WatchGuard System Manager 11

Руководство администратора (пользователя)

WatchGuard XTM 1050

WatchGuard XTM 8

Firebox X Peak e-Series

Firebox X Core e-Series

Firebox X Edge e-Series

Пользователям

Информацию, представленную в этом документе, нельзя изменять без соответствующего разрешения. Имена компаний и данные, которые используются в данном документе являются вымышленными и не имеют никакого отношения к реальности. Ни одна глава, ни один раздел данного документа не может быть скопирован или передан любыми электронными или механическими средствами без соответствующего письменного разрешения компании WatchGuard Technologies Inc.

Версия документа: 05/05/2009

Авторские права, торговые марки и информация о патентах

Аббревиатуры, используемые в документе

3DES	Triple Data Encryption Standard	IPSec	Internet Protocol Security	SSL	Secure Sockets Layer
BOVPN	Branch Office Virtual Private Network	ISP	Internet Service Provider	TCP	Transfer Control Protocol
DES	Data Encryption Standard	MAC	Media Access Control	UDP	User Datagram Protocol
DNS	Domain Name Service	NAT	Network Address Translation	URL	Uniform Resource Locator
DHCP	Dynamic Host Configuration Protocol	PPP	Point-to-Point Protocol	WAN	Wide Area Network
IP	Internet Protocol	PPPoE	Point-to-Point protocol over Ethernet	WSM	WatchGuard System Manager

О компании WatchGuard

Начиная с 1996 года занималась разработкой решений по сетевой безопасности, которые включали в себя брандмауэры, VPN и устройства безопасности, которые использовались для защиты сетей и их ресурсов. Недавно был выпущен новый продукт XTM (eXtensible Threat Management), который выполняет все задачи по безопасности электронной почты и веб-доступа, которые требуются различным компаниям. Продуктами WatchGuard пользуются более 15000 клиентов в 120 странах мира. Более полумиллиона решений безопасности WatchGuard работают сейчас во всем мире в различных отраслях, включая торговлю, образование и здравоохранение. Главный офис компании находится в г. Сиэтл, Вашингтон

Для более подробной информации звоните по телефону 206.613.6600 или заходите на сайт: www.watchguard.com

Адрес

Rainbow Security

129343, Москва, Проезд Серебрякова 14

(495) 66-323-66

Техническая поддержка

techsupport@rainbow.msk.ru

Содержание

Глава 1 - Введение в сетевую безопасность

Сети и сетевая безопасность

Сеть – это группа компьютеров и других устройств, соединенных между собой. Это могут быть 2 компьютера , которые соединяются серийным кабелем , или множество компьютеров во всем мире, объединенных через Интернет. Компьютеры одной сети могут работать вместе и обмениваться данными.

Несмотря на то, что сеть Интернет позволяет получить доступ к большому количеству информации и увеличивает возможности ведения дел через сеть, это влечет за собой проникновение хакеров в вашу сеть.

Многие люди думают, что их компьютеры не содержат важную информацию. Они не подозревают, что их компьютер является мишенью для хакеров. Это заблуждение.

Хакер может использовать ваш компьютер как платформу для атаки других компьютеров или сетей, а также использовать вашу учетную запись для отправки спама. Ваша персональная информация и данные учетной записи также уязвимы и ценны для хакеров.

WatchGuard устройство и подписка LiveSecurity помогут вам отразить атаки такого типа. Хорошая политика сетевой безопасности или набор правил доступа для пользователей также помогут вам эффективно обнаруживать и отражать атаки на ваш компьютер и вашу сеть. Мы рекомендуем вам настроить ваш Firebox в соответствие с вашей политикой безопасности и подумать о потенциальных внешних и внутренних угрозах для вашей компании.

Интернет подключения

ISP (Internet service providers) – это компании, которые предоставляют пользователям доступ в сеть Интернет. Скорость, с которой данные передаются по сети, называется пропускная способность: например 3 Мбит/с (Mbps).

Высокоскоростное соединение, такое как например кабельный модем или DSL (Digital Subscriber Line), также известно как широкополосное соединение.

Широкополосные соединения значительно быстрее dial-up соединений. Пропускная способность dial-up соединения меньше .1 Мбит/с , в то время как пропускная способность кабельного модема может быть более 5 Мбит/с .

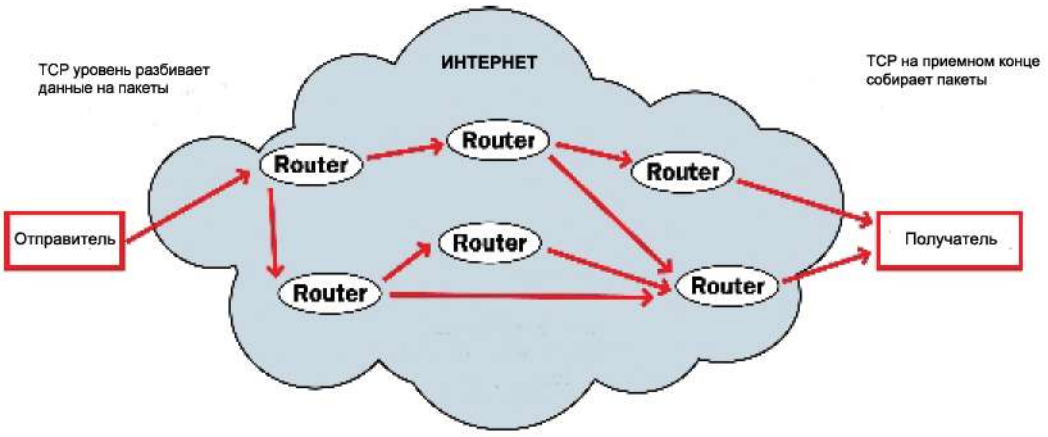
Обычно скорость передачи данных несколько меньше, чем максимальная скорость, так как каждый компьютер является частью одной сети и использует некоторую часть пропускной способности. Поэтому скорость передачи данных по кабельному модему может значительно снизится при наличии большого количества пользователей в сети.

DSL соединения обеспечивают постоянную величину пропускной способности, но скорость передачи данных в таких соединениях меньше, чем скорость передачи через кабельные модемы. Также следует помнить, что пропускная способность величина постоянная только между вашим домом или офисом и центральным офисом, в котором установлен DSL модем.

Передача информации в сети Интернет

Данные по сети Интернет передаются в виде пакетов. Каждый пакет содержит адрес пункта назначения. Пакеты, которые передаются по сети, могут попадать в пункт назначения разными

путями, или маршрутами. В пункте назначения порядок этих пакетов восстанавливается. Для того чтобы гарантировать доставку всех пакетов в пункт назначения в них добавляется информации об адресе назначения.



Протоколы

Протокол – это совокупность правил, которое используется устройствами для обмена данными в сети. Протоколы являются грамматикой языка, на котором общаются устройства в сети. Стандартным протоколом сети Интернет является протокол IP (Internet Protocol). Этот протокол используется компьютерами в сети Интернет для общения друг с другом. Этот протокол определяет, каким образом данные будут передаваться по сети. Наиболее часто используемые транспортные протоколы это TCP (Transmission Control Protocol) и UDP (User Datagram Protocol). TCP/IP – основной стек протоколов, который используется компьютерами для подключения к сети Интернет.

При настройке устройства WatchGuard вам необходимо будет знать некоторые параметры стека протоколов TCP/IP. Для более подробной информации см. “Ваши настройки TCP/IP ”

IP адреса

Для того чтобы отправить обычное письмо кому –либо, вам необходимо знать координаты. Для передачи данных по сети Интернет от одного компьютера к другому необходимо знать адрес этого компьютера. Компьютерный адрес известен как IP-адрес (Internet Protocol Address) . Все устройства в сети Интернет имеют уникальный IP адрес, который позволяет другим устройствам находить их и обмениваться с ними данными. IP адрес состоит из четырех октетов (8-битных двоичных последовательностей), представленных в десятичном формате и разделенных точками. Каждое значение между точками должно лежать в диапазоне от 0 до 255.

Некоторые примеры IP адресов:

- 206.253.208.100
- 4.2.2.2
- 10.0.4.1

Внутренние адреса и шлюзы

Большинство компаний создают так называемые внутренние сети со своим собственным адресным пространством. Диапазон адресов 10.x.x.x и 192.168.x.x зарезервирован для внутренних IP-адресов. Компьютеры, подключенные к сети Интернет не могут использовать эти адреса. Если компьютер находится во внутренней (частной) сети, то к сети Интернет вы подключаетесь через *шлюз* – устройство, которое имеет публичный IP адрес.

Обычно *шлюзом по умолчанию* (*default gateway*) является маршрутизатор, находящийся между вашей внутренней сетью и сетью Интернет. После того, как вы подключите устройство Firebox к вашей сети, то оно становится вашим шлюзом по умолчанию для всех компьютеров, подключенных к Trusted или Optional интерфейсам.

Маски подсети

Для безопасности и увеличения эффективности сети обычно разделяют на более мелкие части, называемые подсетями. Все устройства подсети имеют схожие IP адреса. Например, все устройства, имеющие IP адреса, у которых первые три октета 50.50.50 – принадлежат одной и той же подсети. Сеть IP адресов масок подсети или сетевая маска – это последовательность битов, которую маска делит на IP адреса, показывающая количество доступных адресов и количество уже используемых. Маску подсети также как и IP адрес или в slash или CIDR нотации.

Slash-нотация

Slash-нотация используется устройством Firebox для многих целей, включая настройку политик. Slash-нотация, также известна как CIDR (Classless Inter-Domain Routing) нотация – это более удобный способ записи маски подсети.

При использовании slash-нотации вы записываете IP-адрес, затем прямую косую черту (/), и затем номер маски подсети. Для того чтобы определить номер маски подсети:

1. Конвертируйте маску подсети в двоичный вид.

2. Посчитайте количество единиц в маске подсети. Это количество и будет номером маски подсети

Например, вы хотите записать IP-адрес 192.168.42.23 с маской подсети 255.255.255.0, используя slash-нотацию.

1. Приведение маски подсети к двоичному представлению. Например, двоичное представление 255.255.255.0. - *11111111.11111111.11111111.00000000.*

2. Подсчет количества единиц в маске подсети. Приведенный выше пример имеет двадцать четыре единицы.

3. Затем к IP адресу из пункта 2 добавляется число, отделяемое от основного IP адреса слешом (/).
В результате получим 192.168.42.23/24.

Приведенная таблица показывает общие сетевые маски и их эквиваленты в slash-нотации.

Маска подсети	Эквивалент маски в slash-нотации
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26

255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30

Ввод IP-адресов

К этому типу IP адресов относятся - ваш IP адрес в мастере Setup Wizard или диалоговом окне управления программным обеспечением в Firebox, типом цифр и периодами в правильной последовательности. Для того, чтобы не использовать клавишу TAB, клавиши со стрелками, клавишу пробела, или мышь для перевода курсора после периодов.

Например, если ваш IP адрес 172.16.1.10 не относится к типу пространства после 16. Не пытайтесь перевести курсор после следующего периода к типу 1.

Тип периода непосредственно следующий после 16 и затем типы 1.10. Нажмите «/» для перемещения к сетевой маске.

Статические и Динамические IP адреса

ISP (Internet service providers – поставщик Интернет услуг) определяет IP адрес каждого устройства сети. IP адрес может быть статическим или динамическим. Статический IP адрес не меняет своего значения. Если у вас есть web-сервер, FTP-сервер или другие Интернет ресурсы, которые не могут менять своего адреса, вы можете получить статический IP адрес от вашего ISP. Статический IP адрес обычно более дорогой, чем динамический, и некоторые Интернет-провайдеры не предоставляют статические IP адреса.

В этом случае вам следует сформировать статический IP адрес вручную. Динамические IP адреса ISP выделяют для вашего временного пользования. Если динамический адрес не используется, он может быть автоматически присвоен другому устройству. Динамический IP адрес устанавливает использование либо DHCP, либо PPPoE.

Протокол DHCP

DHCP (Dynamic Host Configuration Protocol) Интернет протокол, который компьютер сети использует для получения IP адресов и другой информации, такой как шлюз по умолчанию. Когда вы подключаетесь к Интернету, DHCP сервер автоматически присваивает IP адрес вашему компьютеру

Это может быть IP адрес, который вы использовали ранее, либо новый, еще не использованный вами IP адрес. Когда вы закрываете Интернет соединение, которое использует динамический IP адрес, Интернет-провайдер может назначить этот IP адрес другому клиенту.(пользователю) Вы можете сконфигурировать Firebox как DHCP сервер для сетей, подключенных к нему. Вы можете назначить диапазон, из которого DHCP сервер сможет выбрать адрес.

Протокол PPPoE

Некоторые Интернет-провайдеры назначают свои IP адреса через протокол Point-to-point over Ethernet (PPPoE). PPPoE расширяет возможности стандартных dial-up - соединений, добавляя некоторые функциональные возможности Ethernet и PPP. Этот сетевой протокол позволяет ISP использовать биллинг, аутентификацию и системы безопасности dial-up-инфраструктур с DSL или кабельным модемами

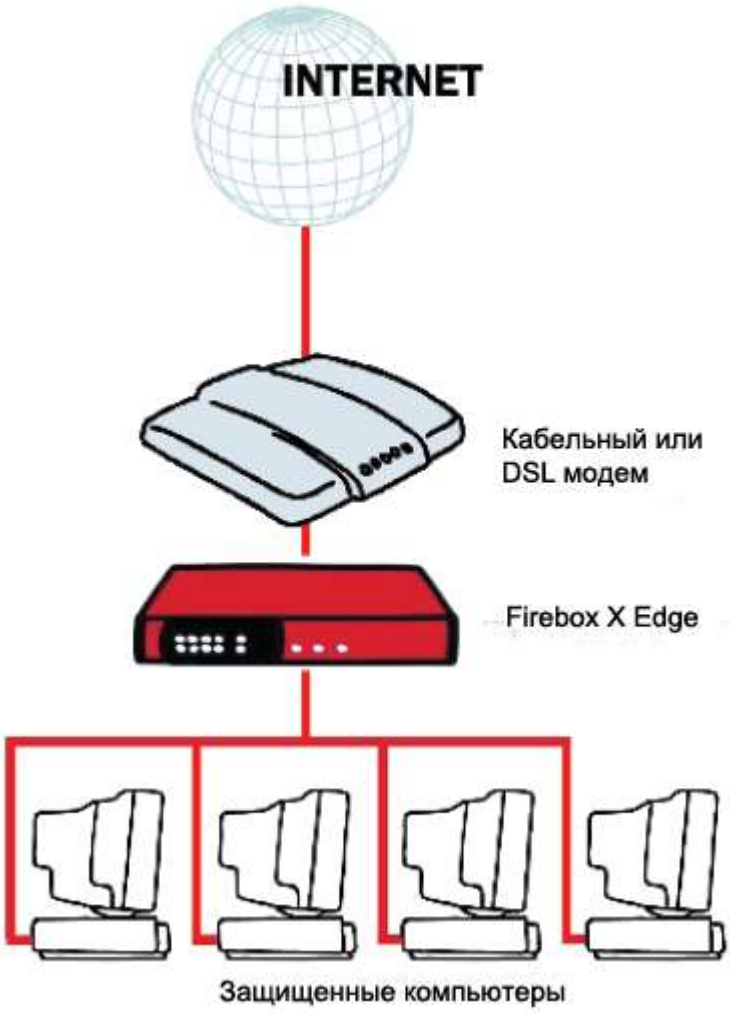
DNS (Domain Name System)

Для поиска адреса нужного вам человека вы зачастую пользуетесь телефонным справочником. В сети Интернет эквивалентом телефонного справочника является DNS (Domain Name System). DNS – это набор серверов, которые преобразуют числовые IP адреса в читаемые Интернет адреса и наоборот. DNS получает от вас запрос на подключение, например к сайту www.example.com, и находит его IP-адрес - 50.50.50.1.

Для подключения к сайтам сетевым устройствам необходим его реальный IP адрес, однако доменные имена легче запомнить. DNS сервер – это сервер, который выполняет это преобразование. Многие компании имеют внутренние DNS серверы в своей сети, которые также занимается обработкой DNS запросов. Вы также можете использовать внешние DNS серверы, например DNS сервер, предоставленный вашим ISP

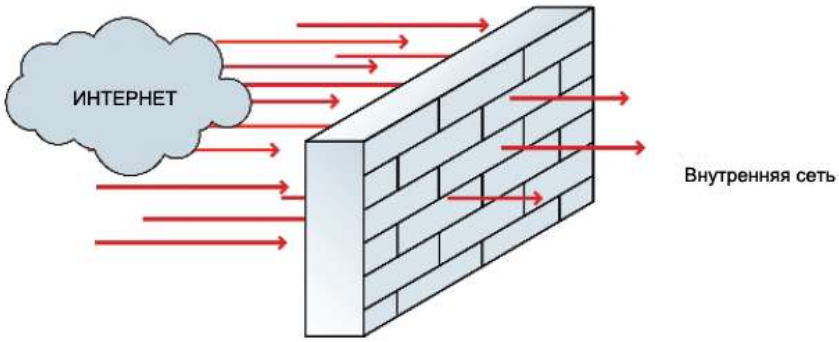
Брандмауэры

Брандмауэр – это устройство, которое используется для защиты вашей внутренней сети от внешних атак. На рисунке ниже показано, каким образом брандмауэр защищает компьютеры, подключенные к Trusted сети.



Брандмауэры используют политики доступа для идентификации и фильтрации данных различных типов. Они также могут определять какие порты и политики могут быть использованы пользователями при подключении к сети Интернет (исходящий доступ). Например многие брандмауэры имеют политики безопасности, которые разрешают только определенные типы трафика. Пользователи имеют возможность выбирать политики, которые подходят им больше

всего. Другие брандмаэуры, как например WatchGuard устройства, позволяют пользователю самому настраивать эти политики



Брандмауэры могут программными и аппаратными. Брандмауэр защищает сеть от несанкционированного доступа из сети Интернет. Входящий и исходящий трафик анализируется брандмауэром, если трафик не удовлетворяет политике безопасности, то он блокируется. В некоторых закрытых или *default-deny* брандмауэрах, все подключения запрещены, только если нет специального правила, которое разрешает это подключение. Для того чтобы использовать такой тип брандмауэром вам необходимо иметь очень подробную информацию о приложениях, которые необходимо использовать в вашей сети. Другой тип брандмауэров разрешают весь сетевой трафик, который не заблокирован в настройках. Такой тип брандмауэров легче эксплуатировать, но они менее безопасны.

Сервисы и политики

Вы используете *сервисы* для отправки определенные типов данных (электронная почта, файлы или команды) с одного компьютера на другой через сеть или другие сети. Эти сервисы используют протоколы. Чаще всего используются следующие Интернет сервисы:

- Доступ в сеть Интернет (World Wide Web) осуществляется по протоколу HTTP(HyperText Transfer Protocol);
- Для передачи электронной почты используется протоколы SMTP или POP3;
- Для передачи файлов используется протокол FTP;
- Для поиска IP адреса по доменному имени используется DNS,
- Для удаленного доступа к терминалу используются протоколы Telnel или SSH (Secure Shell).

Когда вы разрешаете или запрещаете сервис, вы должны добавить политику в конфигурацию вашего Firebox. Каждая созданная вами политика может создать брешь в вашей системе безопасности. Для того чтобы передавать и получать данные вам необходимо будет открывать доступ к вашему компьютеру, что несет в себе потенциальную угрозу вашей сети. Мы рекомендуем добавлять только те политики, которые вам необходимы для вашей деловой деятельности.

Пример использования политики: предположим, что ваш системный администратор хочет разрешить подключение Windows терминала к публичному серверу компании на Optional интерфейсе. Администратор при помощи Remote Desktop администрирует этот сервер. Он не хочет, чтобы другие пользователи могли использовать Remote Desktop сервисы через Firebox. Администратору необходимо добавить политику, которая разрешает RDP соединения только с IP-адреса компьютера администратора на IP-адрес публичного web-сервера.

Во время настройки вашего WatchGuard устройства при помощи мастера Quick Setup Wizard, мастер создает политики для ограниченного исходящего доступа. Если у вас используется другие приложения, то для того чтобы разрешить им доступ вам необходимо выполнить следующее:

- Настроить политики на Firebox, которые разрешат необходимый трафик
- Создать список хостов, к которым будет применяться эта политика, и выполнить все необходимые настройки параметров политики
- Создать такую политику доступа, которая одновременно не создаст потенциальной бреши в вашей системе защиты, и которая предоставит пользователям доступ к необходимым сервисам

Порты

Порты, помимо физических портов, которые используются для физического подключения устройств друг к другу, но также и специальные номера, которые используются для привязки трафика к определенным процессам на компьютере. Если IP адрес похож на адрес улицы, то порт представляет собой номер квартиры или здания на этой улице. Когда компьютер передает данные на другой удаленный компьютер, он указывает IP адрес устройства, которое эти данные будет получать, и номер порта, который определяет какой процесс на этом устройстве эти данные будет обрабатывать.

Например, вы хотите посмотреть страницу на Интернет сайте. Ваш браузер пытается создать подключение через порт 80 (порт для HTTP трафика) для каждого элемента страницы. После того, как браузер получит все запрашиваемые с сервера данные, он закроет соединение.

Большинство портов используются только для определенного типа трафика, например порт 25 используется только для SMTP (Simple Mail Transfer Protocol) трафика. Некоторые протоколы, как SMTP, имеют закрепленные за ними номера портов. Другие программы для каждого подключения используют различные номера портов. Специальная организация IANA (Internet Assigned Numbers Authority) содержит список известных портов. Для того чтобы посмотреть список портов зайдите на сайт:

http://www.iana.org/assignments/port-numbers

Большинство политики, которые вы создаете на устройстве Firebox, имеют номера портов от 0 и 1024

Порты можно закрыть или открыть. Если порт открыт, то ваш компьютер принимает данные по этому порту и использует этот порт для соединения с другими устройствами. Однако открытый порт это угроза вашей системе безопасности. Для того чтобы защитить вашу сеть от атак вам необходимо решить, какие порты необходимо заблокировать, а какие необходимо открыть. Для более подробной информации см. “Заблокированные порты”.

Вы также можеть блокировать попытки хакеров сканировать порты на вашем компьютере: процедура сканирования портов используется для того, чтобы определить, какие порты открыты на вашем компьютере. Для более подробной информации см. “Сканирование портов и адресного пространства”.

Глава 2 - Fireware XTM

Введение в Fireware XTM

Fireware XTM предоставляет пользователям простой и эффективный инструмент для просмотра, управления и мониторинга всех устройств Firebox, которые находятся в вашей сети.

Fireware XTM включает в себя четыре приложения:

- WatchGuard System Manager (WSM)
- Веб интерфейс Fireware XTM Web UI
- Fireware XTM Command Line Interface (CLI)
- WatchGuard Server Center

Для настройки сети, которая будет отвечать требованиям безопасности в вашей организации, вам возможно придется использовать несколько приложений Fireware XTM. Например, если у вас в сети работает только один Firebox X Edge e-Series, то для его администрирования вам понадобится только Fireware XTM Web UI или Fireware XTM Command Line Interface. Однако для того чтобы вести журнал и генерировать разнообразные отчеты вам понадобится WatchGuard Server Center.

Если у вас в сети работает несколько устройств WatchGuard или вы приобрели Fireware XTM с обновлением Pro, мы рекомендуем вам использовать WatchGuard System Manager (WSM).

Для более подробной информации о подключении Firebox к Fireware XTM Web UI или Fireware XTM Command Line Interface см. online help или руководства пользователей для этхи продуктов. Вы можете посмотреть или загрузить самую последнюю документацию по этми продуктам по следующей ссылке:

http://www.watchguard.com/help/documentation/xtm.asp

Термины Firebox и устройство WatchGuard, которые используются в данной документации, относятся в устройствам WatchGuard, которые используют Fireware XTM (например, Firebox X Edge e-Series).

Компоненты Fireware XTM

Для того чтобы запустить WatchGuard System Manager или WatchGuard Server Center в ОС Windows нажмите на соответствующий ярлык в меню Start. Вы также можете запустить WatchGuard Server Center из панели задач, нажав на соответствующую иконку. Из этих приложений вы можете запускать другие утилиты управления сетью.

WatchGuard System Manager

WatchGuard System Manager (WSM) – это основное приложение для подключения к устройству Firebox и серверам управления WatchGuard и управления ими. WSM поддерживает смешанные окружения. Вы можете управлять устройствами Firebox, которые работают под управления различных версий программного обеспечения. WSM включает набор утилит, которые позволят вам управлять сетевым трафиком.

Policy Manager

Policy Manager – утилита для конфигурации межсетевого экрана. Policy Manager включает полный набор предварительно настроенных пакетных фильтров и прокси. Вы также можете создать свой собственный пакетный фильтр, в котором вы можете настроить порты, протоколы и другие параметры. Другие компоненты утилиты Policy Manager помогут вам отразить атаки типа «SYN Flood», «spoofing» и сканирование портов и адресного пространства. Для более подробной информации см. “Policy Manager”.

Firebox System Manager (FSM)

Firebox System Manager предоставляет вам интерфейс для мониторинга всех компонентов устройства Firebox. При помощи Firebox System Manager вы можете в режиме реального времени посмотреть состояние вашего устройства Firebox и его конфигурации. Для более подробной информации, см. “Firebox System Manager (FSM)”.

HostWatch

HostWatch – утилита мониторинга трафика между интерфейсами Firebox в режиме реального времени. HostWatch также содержит информацию о пользователях, подключениях, портах и устройствах.Для более подробной информации см. “Утилита HostWatch”.

LogViewer

LogViewer – утилита для просмотра файлов журналов. Для более подробной информации см. “Глава 21 - Журналы и Уведомления”.

Report Manager

При помощи утилиты Report Manager вы можете генерировать отчеты по данных, собранным с ваших Серверов Журналов для всех ваших устройств WatchGuard. Для более подробной информации см. “Утилита Report Manager”

CA Manager

Утилита Certificate Authority (CA) Manager содержит список сертификатов безопасности, установленных на вашу станцию управления с установленной Fireware XTM. При помощи этой утилиты вы можете импортировать, настраивать и генерировать сертификаты для VPN туннелей и других задач.

WatchGuard Server Center

WatchGuard Server Center – приложения для мониторинга и настройки всех ваших серверов WatchGuard.Для более подробной информации см. “Установка серверов WatchGuard System Manager”

Management Server

Сервер Управления работает на компьютере под управлением ОС Windows. При помощи этого сервера вы можете управлять работой всех брандмауэров в вашей сети, а также создавать VPN туннели при помощи процедуры drag-n-drop. Основными функциями Сервера Управления являются:

- Центр сертификации для генерации сертификатов для IPSec туннелей
- Централизованное управление конфигурациями VPN туннелей
- Централизованное управление устройствами Firebox и Firebox X Edge. Для более подробной информации о Сервере Управления, см. “Сервер Управления”.

Сервер Журналов (Log Server)

Сервер Журналов собирает сообщения журнала с каждого устройства WatchGuard Firebox. Сообщения передаются на Сервер Журналов в зашифрованном виде. Для шифрования сообщений используется формат XML (открытый текст). Информация, которая собирается с брандмауэров включает в себя сообщения по трафику, события, тревоги и диагностические сообщения. Для более подробной информации о Сервере Журналов, см. “Серверы Журналов”.

Сервер WebBlocker

Сервер WebBlocker работает с HTTP прокси устройства Firebox для того чтобы закрывать пользователям доступ к определенным категориям web-сайтов. Список разрешенных и заблокированных сайтов составляются администратором во время процедуры настройки устройства Firebox. Для более подробной информации об WebBlocker и сервере WebBlocker.

Сервер Карантина (Quarantine Server)

Сервер Карантина собирает и изолирует электронные сообщения, которые помечаются как спам специальной программой анализа электронной почты - spamBlocker.

Сервер Отчетов (Report Server)

Сервер Отчетов с определенной периодичностью собирает данные, которые были получены Серверами Журналов с устройств Firebox, и затем с определенной периодичностью генерирует отчеты. После того как данные попадают на Сервер Отчетов, вы можете посмотреть их при помощи утилиты Report Manager

Web-интерфейс Fireware XTM и Интерфейс командной строки (Command Line Interface)

Web-интерфейс Fireware XTM Web UI и Интерфейс командной строки (Command Line Interface) являются альтернативой основным приложениям и могут выполнять те же самые задачи, что и WatchenGuard System Manager и Policy Manager. Некоторые дополнительные настройки и компоненты, как FireCluster или настройки политики прокси, недоступны в Fireware XTM Web UI или Command Line Interface.

Fireware XTM с обновлением Pro

Обновление Pro для Fireware XTM предоставляет несколько дополнительных компонентов для опытных клиентов – балансировка нагрузки на сервер и дополнительные SSL VPN туннели. Компоненты, доступные в Pro, зависят от модели вашего Firebox:

Для того чтобы приобрести Fireware XTM with с Pro обновлением свяжитесь с вашим локальным представителем.

Компонент	Core e-Series	Core/Peak e-s и XTM 1050 (Pro)	Edge e-Series	Edge e-Series (Pro)
FireCluster	X			
Поддержка VLAN	75 max	75 max (Core) 200 max (Peal/XTM 1050)	20 max	50 max
Протоколы динамической маршрутизации (OSPF и BGP)		X		X
Маршрутизация на базе политик (Policy-Based Routing)		X		X
Балансировка нагрузки на сервер (Server Load Balancing)		X		
Максимальное количество SSL VPN туннелей		X		X
Multi-WAN переключение при отказе канала (Multi-WAN Failover)	X	X		X
Балансировка нагрузки multi-WAN		X		X

Глава 3 - Сервис и поддержка

Техническая поддержка WatchGuard

Компания WatchGuard® прекрасно понимает важность технической поддержки для своих клиентов, которые используют решения компании для защиты своих сетей. Нашим клиентам необходимо больше информации и помощи в мире, где вопросы безопасности являются критичными.

Сервис LiveSecurity® Service предоставляет вам всю необходимую информацию. Для этого необходимо получить подписку на этот сервис сразу после регистрации вашего WatchGuard устройства.

Сервис LiveSecurity Service

Ваше WatchGuard устройство включает подписку на наш сервис LiveSecurity Service, которая активируется в режиме online сразу после регистрации вашего устройства в сети. После активации подписки LiveSecurity Service вы получите доступ полный доступ к программе поддержки. Использование LiveSecurity Service дает следующие преимущества:

Гарантия на оборудование и возможность замены необходимого оборудования

Активная подписка LiveSecurity расширяет гарантийный срок вашего устройства WatchGuardю Эта подписка также позволяет вам значительно минимизировать время замены оборудования в случае аппаратного сбоя. Если ваше оборудование вышло из строя, то компания WatchGuard отправит вам замену еще до того, как вы отправите нам вышедшее из строя оборудование.

Обновления программ

Ваша подписка LiveSecurity Service дает вам доступ к последним обновлениям ПО, а также доступ к новым функциональным возможностям WatchGuard устройств.

Техническая поддержка

Если вам нужна помощь, то наши эксперты готовы вам помочь:

- Наши эксперты работают 12 часов в день, 5 дней в неделю*
- Максимальное время ответа не более 4 часов
- Доступ к форумам, модераторами которых являются наши опытные инженеры

Обучающие материалы и Тревоги

Ваша подписка LiveSecurity Service предоставляет вам доступ к различным обучающим видеоматериалам, online курсам, а также специальным программам, которые были разработаны для того чтобы ответить на все интересующие вас вопросы о сетевой безопасности, а также вопросы по поводу установки, конфигурации и эксплуатации продуктов компании WatchGuard.

Наша Rapid Response Team, группа технических экспертов в области сетевой безопасности, постоянно следят за последними угрозами, информация о которых появляется в сети Интернет. Собрав определенное количество информации, они создают для вас специальные рассылки LiveSecurity Broadcasts, в которых вы сможете найти всю необходимую информацию о методах борьбы с новыми угрозами. Вы можете настроить о каких угрозах вы хотите знать, а какие просто игнорируются.

Подписка LiveSecurity Service Gold

Подписка LiveSecurity Service Gold доступна для компаний, которым необходима 24-часовая поддержка. Данная подписка обеспечивает расширенные временные рамки решения определенной проблемы, а также меньшее время первого ответа на ваш запрос. Для более полной технической поддержки подписка LiveSecurity Service Gold необходима для каждого устройства.

Истечение срока действия сервиса

Для обеспечения высокого уровня безопасности вашей сети мы рекомендуем иметь активную подписку. Если срок вашей подписки истекает, вы теряете возможность получать информацию о последних угрозах, а также доступ к последним обновлениям ПО. Стоимость обновления подписки значительно ниже, чем стоимость восстановления сети после атаки. Если вы обновите вашу подписку в течение 30 дней, то восстановление подписки будет бесплатным.

Глава 4 - Начало

Перед тем как начать

Перед тем как вы начнете процедуру установки, убедитесь, что вы выполнили все указания, приведенные ниже.

При описании процедур установки, мы предполагаем, что ваше устройство Firebox имеет один Trusted, один External и один Optional-интерфейсы. Для того чтобы настроить дополнительные интерфейсы воспользуйтесь утилитами конфигурации и процедурами, описание которых приведено в разделах Network Setup и Configuration.

Проверка базовых компонент

Убедитесь, что у вас есть следующие компоненты:

- Компьютер с сетевой картой 10/100BaseT Ethernet и установленным web браузером
- Устройство WatchGuard Firebox или XTM
- Последовательный кабель (синего цвета)
  Только для Firebox X Core, Peak и WatchGuard XTM
- Один кроссовер кабель (красного цвета)
  Только для Firebox X Core, Peak и WatchGuard XTM
- Один прямой Ethernet кабель (зеленого цвета)
- Силовой кабель или источник питания AC

Загрузка ключа функций WatchGuard

После того, как вы получите устройство Firebox вам необходимо активировать его на сайте LiveSecurity и получить ваш ключ функций. Этот ключ позволяет вам использовать все компоненты устройства Firebox.

Если вы зарегистрировали ваш Firebox перед тем, как запустить Quick Setup Wizard, вы можете скопировать ключ и вставить его в соответствующее поле в мастере.

Мастер затем применит его к вашему Firebox. Если вы не вставите этот ключ в соответствующее поле, вы можете завершить работу мастера, однако при этом вам будет разрешено только одно подключение к сети Интернет. После приобретения дополнительных продуктов, вам необходимо получить новый лицензионный ключ. После того как вы зарегистрируете ваш Firebox или любой новый продукт, вы можете в любое время синхронизировать ключ вашего Firebox с ключами, которые хранятся на сайте LiveSecurity в вашем профиле, при помощи пользовательского интерфейса WSM. Для более подробной информации о ключах функции см. “Ключи функций (Feature Keys)”

Сетевые адреса

При настройке Firebox мы рекомендуем создать две таблицы. В первую таблицу запишите сетевые IP-адреса перед тем, как подключите устройство Firebox к сети. Для записи масок подсети WatchGuard использует slash-нотацию. Для более подробной информации см. “Slash-нотация”. Для более подробной информации об IP-адресах см. “IP адреса”

Таблица 1. Сетевые адреса без устройства Watchguard	
WAN сеть	_____._____._____._____ / ____
Шлюз по умолчанию	_____._____._____._____
Локальная сеть	_____._____._____._____ / ____
Вторичная сеть (если используется)	_____._____._____._____ / ____
Публичные серверы (если используются)	_____._____._____._____
	_____._____._____._____
	_____._____._____._____

Во вторую таблицу запишите сетевые IP-адреса после того, как вы подключите устройство Firebox к сети

External интерфейс

Для подключения к внешней сети (обычно сеть Интернет), которая не является доверенной сетью.

Trusted интерфейс

Для подключения к частной LAN (local area network) или внутренней сети, которые вы хотите защитить

Optional интерфейс

Обычно используется для подключения к DMZ или к сегменту вашей сети, которые имеет смешанное доверие. При помощи интерфейсов Optional вы можете создавать сегменты сети с различным уровнем доступа.

Таблица 2. Сетевые адреса с устройством Watchguard	
Шлюз по умолчанию	_____._____._____._____ / ____
External интерфейс	_____._____._____._____
Trusted интерфейс	_____._____._____._____ / ____
Optional интерфейс	_____._____._____._____ / ____
Вторичная сеть (если используется)	_____._____._____._____

Режим конфигурации брандмауэра

Перед тем как устанавливать WatchGuard System Manager вам необходимо решить, как вы будете подключать устройство Firebox к вашей сети. Способ подключения устройства Firebox к сети определяет конфигурацию интерфейса. Для того чтобы подключить устройство Firebox к вашей сети вам необходимо выбрать режим конфигурации — routed или drop-in — которые удовлетворяет требованиям вашей сети.

Многие сети работают лучше с routed-конфигурацией, но мы рекомендуем вам использовать режим **drop-in** в случае если:

- Вы используете большое количество статических IP-адресов и не хотите менять конфигурацию вашей сети.
- Вы не можете присвоить компьютерам, подключенным к Trusted или Optional сетям, которые имеют публичные IP-адреса, внутренние IP-адреса

Ниже приводится таблица, информация в которой поможет вам выбрать режим конфигурации брандмауэра.

Режим смешанной маршрутизации (Mixed Routing Mode)	Режим Drop-In
Все интерфейсы Firebox находятся в разных сетях	Все интерфейсы Firebox находятся в одной сети и имеют один и тот же IP-адрес
Trusted и Optional интерфейсы должны находиться в разных сетях. Каждый интерфейс имеет IP-адрес в своей сети	Компьютеры, подключенные к интерфейсам Trusted или Optional могут иметь публичные IP-адреса.
Для того чтобы преобразовать публичные IP-адреса компьютеров, подключенных к интерфейсам Trusted и Optional, в частные используйте статическую NAT (Network Address Translation)	Так как компьютеры с публичным доступом имеют публичные IP-адреса, нет необходимости использовать NAT

Для более подробной информации о режиме drop-in см. “Конфигурация сети в режиме drop-in”

Для более подробной информации о режиме смешанной маршрутизации см. “Режим смешанной маршрутизации (Mixed Routing Mode)”

Также устройство WatchGuard поддерживает третий режим конфигурации – режим моста. Этот режим используется довольно редко. Для более подробной информации о режиме моста см. “Конфигурация сети в режиме моста”

Вы можете использовать мастера Web Setup Wizard или WSM Quick Setup Wizard для того чтобы создать первоначальную конфигурацию. После того, как вы запустите мастер Web Setup Wizard, автоматически будет включен режим смешанной маршрутизации. Если вы запустите мастер WSM Quick Setup Wizard, то вы можете настроить режим работы брандмауэра.

Каталог для установки серверных компонентов

Во время установки вы можете установить сервер управления и WatchGuard System Manager на один компьютер. Или вы можете при помощи той же самой процедуры установки установить компоненты Сервера Управления, Сервера Журналов, Сервера Отчетов, Сервера WebBlocker или Сервера Карантина на другие компьютеры для того чтобы снизить нагрузку на один компьютер и обеспечить резервирование. Сервер Управления не будет работать нормально на компьютере, на

котором не установлено WSM. Для того чтобы решить куда устанавливать серверное программное обеспечение, вам необходимо проверить дисковое пространство вашей станции управления и выбрать метод установки, который вам подходит.

Если вы устанавливаете серверное ПО на компьютер с включенным межсетевым экраном другого производителя (не Windows), вам необходимо будет открыть порты для подключения через этот межсетевой экран. Пользователям Windows Firewall нет необходимости изменять конфигурацию своего межсетевого экрана, так как программа установки автоматически откроет необходимые порты. Для более подробной информации см. “Установка Серверов WatchGuard на компьютеры с установленными программными брандмауэрами”

Установка WatchGuard System Manager

Вы можете установить WatchGuard System Manager (WSM) на компьютер, который вы выбрали в качестве *станции управления*. Для получения информации на устройстве Firebox (состояние подключения и туннелей, статистика по трафику, сообщения журнала) вы можете воспользоваться утилитами, которые устанавливаются на станцию управления. Выберите компьютер под управлением ОС Windows, который будет работать как станция управления, и установите на него необходимое программное обеспечение управления. Для того чтобы установить WatchGuard System Manager вам необходимо иметь права администратора. После установки вы можете работать с правами Power User (Windows XP или Windows 2003).

На одну станцию управления вы можете установить несколько версий WatchGuard System Manager. За одну процедуру установки вы можете установить только одну версию серверного ПО.

Создание резервной копии вашей предыдущей конфигурации

Если у вас установлена предыдущая версия WatchGuard System Manager, то перед тем как устанавливать новую версию ПО сделайте резервную копию конфигурации вашей политики безопасности. Для более подробной информации о том, как сделать резервную копию вашей конфигурации, см. “Резервные копии образов flash-дисков Firebox”.

Загрузка WatchGuard System Manager

Последнюю версию ПО WatchGuard System Manager вы можете загрузить на этом сайте https:// www.watchguard.com/archive/softwarecenter.asp.

Для загрузки вам необходимо будет войти под своей учетной записью LiveSecurity. Если вы являетесь новым пользователем, то для того чтобы загрузить WSM вам необходимо создать профиль пользователя и активировать ваш продукт здесь:

http:// www.watchguard.com/activate

ПО станции управления доступна в двух уровнях шифрования. Выберите правильный уровень шифрования. Для более подробной информации см. “Уровни шифрования программного обеспечения”

Если вы устанавливаете серверное ПО на компьютер с включенным межсетевым экраном другого производителя (не Windows), вам необходимо будет открыть порты для подключения через этот межсетевой экран. Для того чтобы разрешить подключения к серверу WebBlocker вам необходимо открыть UDP порт 5003. Пользователям Windows Firewall нет необходимости изменять конфигурацию своего межсетевого экрана. Для более подробной информации см. “Установка Серверов WatchGuard на компьютеры с установленными программными брандмауэрами”

Для того чтобы установить Сервер Управления выполните следующее:

1. Загрузите последнюю версию WatchGuard System Manager на компьютер, который вы используете как станцию управления.

2. На этот же компьютер загрузите последнюю версию Fireware

3. Запустите файл и выполните все необходимые инструкции. Программа установки включает окно, в котором вы выбираете компоненты и обновления, которые вы хотите установить. Для установки некоторых компонентов потребуется другая лицензия

4. Запустите мастер Quick Setup Wizard. Мастер можно запустить из Web или как обычное Windows приложение.

   * Для более подробной информации о запуске мастера через Web см. ”Мастер Quick Setup Wizard”.

   * Для более подробной информации о запуске мастера как обычное Windows приложение, см. “Запуск мастер WSM Quick Setup”.

Уровни шифрования программного обеспечения

Программное обеспечение станции управления доступно в двух уровнях шифрования:

Base

Поддерживает 40-битное шифрование для Mobile VPN с PPTP туннелями. Вы не можете создать IPSec VPN туннель с этим уровнем шифрования.

Strong

Поддерживает 40-битное и 128-битное шифрования для Mobile VPN с PPTP. Также поддерживает 56-битный и 168-битный DES, и 128-битный, 192-битный и 256-битный AES. Для того чтобы использовать VPN с IPSec вам необходимо загрузить ПО с уровнем шифрования Strong. На экспорт программного обеспечения такого типа накладываются определенные ограничения. Возможно в вашем регионе загрузка такого программного обеспечения запрещена

Мастер Quick Setup Wizard

При помощи мастера Quick Setup Wizard вы можете создавать базовую конфигурацию вашего Firebox X. При первом запуске устройство Firebox использует базовый конфигурационный файл. Это позволяет устройству Firebox работать как обычный межсетевой экран. Вы можете использовать эту же процедуру каждый раз, когда вы хотите перезагрузить Firebox с новой конфигурацией с целью восстановления или по другим причинам.

При настройке Firebox при помощи мастера Quick Setup Wizard, вы настраиваете только базовые политики (Исходящий TCP и UDP, пакетный фильтр FTP, пинг и WatchGuard) и IP-адреса интерфейсов. Если вы хотите проверить работу приложений или хотите посмотреть сетевой трафик, вам необходимо сделать следующее:

- Настроить политики для того чтобы разрешить необходимый трафик
- Для каждой политики настроить хосты и параметры
- Сбалансировать политику защиты вашей сети с требованиями ваших пользователей по доступу к внешним ресурсам

Мастер Quick Setup Wizard можно запустить из web или как обычное Windows-приложение.

Для более подробной информации о запуске мастера из Web, см. “Мастер Quick Setup Wizard”.

Для более подробной информации о запуске мастера как обычное Windows-приложения, см. ”Запуск мастер WSM Quick Setup”

Запуск мастера Web Setup Wizard

Это инструкции для мастера Web Setup Wizard на устройстве Firebox с установленным Fireware XTM версии v11.0 или выше. Если ваше устройство WatchGuard использует более раннюю версию ПО, то перед тем как использовать эти инструкции, вам необходимо обновить версию до Fireware XTM. Для более подробной информации см. Release Notes.

При помощи мастера Web Setup Wizard вы можете создать базовую конфигурацию для любого устройства Firebox X e-Series или WatchGuard XTM. Мастер Web Setup Wizard автоматически выбирает в качестве режима работы устройства режим смешанной маршрутизации. Для того чтобы использовать мастер Web Setup Wizard, вам необходимо напрямую подключиться к устройству WatchGuard и при помощи браузера запустить мастер. После того, как вы настроите ваше устройство WatchGuard, оно по протоколу DHCP пришлет новый IP адрес вашей станции управления.

Перед тем, как запустить мастер Web Setup Wizard, убедитесь, что вы выполнили следующее:

- Зарегистрировали ваш Firebox в LiveSecurity Service
- Сохранили копию лицензионного ключа Firebox в текстовом файле на вашей станции управления

Запуск мастера Web Setup Wizard

1. При помощи красного кроссовер-кабеля, который входит в комплект устройства Firebox, соедините Ethernet порт вашей станции управления с Trusted интерфейсом вашего устройства Firebox.
    - Для устройств Firebox X Core, Peak e-Series или XTM Trusted интерфейс – это интерфейс номер 1
    - Для Firebox X Edge e-Series Trusted интерфейс – это интерфейс LAN0
2. При помощи силового кабеля подключите Firebox к источнику питания.
3. Запустите Firebox в режиме по умолчанию. Для устройств Core, Peak и XTM – это безопасный режим. Для более подробной информации см. “Запуск Firebox X Core или Peak e-Series, или WatchGuard XTM в безопасном режиме”
4. Убедитесь, что ваша станция управления разрешает использование IP-адресов, присвоенных DHCP-сервером. Например, если ваша станция управления работает под управлением ОС, то выполните следующее:

- Выберите **Start > All Programs > Control Panel > Network Connections > Local Area Connections**.
- Нажмите **Properties**.
- Выберите **Internet Protocol (TCP/IP)** и нажмите **Properties**.
- Убедитесь, что опция **Obtain an IP Address Automatically** включена.

5. Если ваш браузер использует HTTP прокси сервер, вам необходимо временно отключить настройки HTTP прокси в вашем браузере. Для более подробной информации см. “Отключение HTTP прокси в браузере”

6. Откройте браузер и в адресной строке браузера введите IP адрес интерфейса 1.

   Для Firebox X Core или Peak, или устройства WatchGuard XTM он равен: *https://10.0.1.1:8080*.

   Для Firebox X Edge: *https://192.168.111.1:8080*.

   Если вы используете Internet Explorer, то убедитесь, что ваш адрес начинается с `https://`. При этом создается защищенное HTTP соединение между вашей станцией управления и устройством WatchGuard.
   Мастер Web Setup Wizard запустится автоматически.

7. Войдите в систему, используя следующие данные доступа:

   Имя пользователя: `admin`
   Пароль: `readwrite`

8. Выполните все необходимые инструкции мастера. Мастер Web Setup Wizard содержит следующие страницы. При этом важно понимать, что список страниц, отображаемых в мастере, зависит от выбранных способов конфигурации:

   Login

   Войдите в систему под учетной записью администратора. Имя пользователя: *admin*, Пароль: *readwrite*

   Welcome

   На первой странице содержится информация о мастере.

   Select a configuration type

   Выберите, создавать ли новую конфигурацию или восстановить конфигурацию из сохраненного резервного файла.

   License agreement

   Для того чтобы продолжить работу с мастером вам необходимо принять условия лицензионного соглашения.

   Retrieve Feature Key, Apply Feature Key, Feature key options

   Если ваш Firebox на данный момент не имеет ключа функций, то мастер предоставит необходимые опции для загрузки или импорта необходимого ключа функций. Загрузить ключ функций мастер сможет только при наличии активного подключения к сети Интернет. Если вы загрузили локальную копию ключа функций на ваш компьютер, вы можете вставить его в соответствующее окно мастера. Если устройство Firebox не имеет активного подключения к сети Интернет, и вы, перед тем как запустить мастер вы не загрузили ключ функций и не зарегистрировали свое устройство, то на данном этапе вы можете не

использовать этот ключ.

Если в мастере Web Setup Wizard вы выбрали не использовать ключ функций, то вам необходимо будет зарегистрировать ваше устройство и применить ключ функций в web-интерфейсе Fireware XTMWeb UI. До тех пор, пока вы не импортируете ключ функций на ваше устройство, его функционал будет ограничен.

Configure the External Interface of your Firebox

Выберите способ получения IP адреса у вашего ISP: DHCP, PPPoE или Static (Статический).

Configure the External Interface for DHCP

Введите DHCP данные, предоставленные вашим ISP.

Configure the External Interface for PPPoE

Введите PPPoE данные, предоставленные вашим ISP.

Configure the External Interface with a static IP address

Введите статические данные, предоставленные вашим ISP.

Configure the DNS and WINS Servers

Введите IP адреса Domain DNS и WINS серверов

Configure the Trusted Interface of the Firebox

Введите IP адрес Trusted интерфейса. Дополнительно, вы можете включить DHCP сервер для Trusted интерфейса.

Wireless (Только для Firebox X Edge e-Series Wireless)

Выберите рабочий регион, канал и режим работы беспроводной сети. Рабочий регион зависит от того, где вы приобрели вашFirebox. Для более подробной информации см.

Create passphrases for your device

Введите пароли для учетных записей - status (только чтение) и admin (чтение/запись).

Enable remote management

Включить удаленное управление устройством.

Add contact information for your device

Введите имя устройства, его местоположение и контактные данные для сохранения данных управления на этом устройстве. По умолчанию в качестве имени устройства используется номер модели вашего Firebox. Мы рекомендуем использовать уникальное имя, которое поможет быстро идентифицировать устройство, особенно при управлении с удаленного ресурса.

Set the Time Zone

Выберите часовой пояс региона, в котором находится Firebox.

The Quick Setup Wizard is complete

После того, как вы завершите работу мастера, устройство WatchGuard перезагрузится.

Если вы в течение 15 или больше минут вы не выполните никаких действий в мастере Web Setup Wizard, вам необходимо будет вернуться к п. 3 и повторить всю процедуру снова.

Если вы измените IP адрес Trusted интерфейса, то вам необходимо проверить, принадлежит ли этот IP адрес адресному пространству Trusted сети. Если вы используете DHCP, то перезагрузите ваш компьютер.

После того, как мастер завершит работу

После того, как вы выполните все инструкции мастера, устройство Firebox будет настроено при помощи базовой конфигурации, которая включает в себя 4 политики (Исходящий TCP и UDP, пакетный фильтр FTP, пинг и WatchGuard) и указанные IP-адреса интерфейсов. Для изменения конфигурации устройства Firebox вы можете использовать утилиту Policy Manager.

- Для более подробной информации о том, как запустить устройство Firebox после того, как мастер Quick Setup Wizard завершит работу, см. “Завершение установки”

- Для более подробной информации о том, как запустить WatchGuard System Manager и его утилиты, см. ”Запуск WatchGuard System Manager”

Если у вас возникли проблемы при работе с мастером

Если мастер Web Setup Wizard не может установить Fireware XTM на устройство WatchGuard, то мастер сгенерирует таймаут. Если у вас возникли проблемы с мастером, то проверьте следующее:

- Файл Fireware XTM, который вы загрузили с сайта LiveSecurity, может быть поврежден. Если этот файл поврежден, то на LCD дисплее устройств Firebox X Core, Peak или XTM вы увидите сообщение: *File Truncate Error*.

  Если появится это сообщение, попробуйте загрузить файл и запустить мастер снова.

- Если вы используете Internet Explorer 6, то очистите кэш файлов и попробуйте снова. Для того чтобы очистить кэш в Internet Explorer выберите **Tools > Internet Options > Delete Files**.

Запуск мастер WSM Quick Setup

Это инструкции для мастера Web Setup Wizard на устройстве Firebox с установленным Fireware XTM версии v11.0 или выше. Если ваше устройство WatchGuard использует более раннюю версию ПО, то перед тем как использовать эти инструкции, вам необходимо обновить версию до Fireware XTM. Для более подробной информации см. Release Notes.

Мастер Quick Setup Wizard запускается, как обычное Windows приложение и используется для создания базового конфигурационного файла. Вы можете использовать мастер Quick Setup Wizard с любой моделью Firebox X Core или Peak. Firebox использует этот файл при первом запуске. Это позволяет устройству Firebox работать как обычный брандмауэр. После того, как вы настроите Firebox при помощи базового конфигурационного файла, вы можете при помощи утилиты Policy Manager изменить конфигурацию устройства. Для поиска устройств, которые необходимо настроить, мастер Quick Setup Wizard использует процедуру поиска устройств. Эта процедура использует широковещательный UDP-запрос. При использовании процедуры поиска устройств могут возникнуть проблемы с программными брандмауэрами, включая брандмауэр Microsoft Windows XP SP2.

Перед тем, как запустить мастер Web Setup, убедитесь, что вы выполнили следующее:

- Зарегистрировали свое устройство WatchGuard в LiveSecurity Service

- Скопировали ключ функций в текстовый файл на вашей станции управления

- Загрузили WSM и Fireware XTM с сайта LiveSecurity Service на вашу станцию управления

- Скопировали исполняемый файл Fireware XTM на вашу станцию управления

Запуск мастера Quick Setup Wizard

1. При помощи красного кроссовер-кабеля, который входит в комплект устройства Firebox, соедините Ethernet порт вашей станции управления с Trusted интерфейсом вашего устройства Firebox.

   Для устройств Firebox X Core, Peak e-Series или XTM Trusted интерфейс – это интерфейс номер 1

   Для Firebox X Edge e-Series Trusted интерфейс – это интерфейс LAN0

2. В ОС Windows выберите **Start > All Programs > WatchGuard System Manager 11.0 > Quick Setup Wizard**
   Или в WatchGuard System Manager выберите **Tools > Quick Setup Wizard**.
   Запустится мастер Quick Setup Wizard.

3. Выполните все инструкции мастера.

Настройка режима маршрутизации в мастере Quick Setup Wizard

Вы можете использовать мастер WSM Quick Setup Wizard для настройки режима работы устройства Firebox – режим смешанной маршрутизации или режим drop-in. Режим drop-in вы можете выбрать только в том случае, когда вашему External интерфейсу присвоен статический IP адрес.

Для того чтобы выбрать режим смешанной маршрутизации выполните следующее:

- На странице **Configure the External Interface** выберите **Static IP Addressing**.
- Введите статический IP адрес и шлюз по умолчанию для External интерфейса.
- На странице **Configure the internal interfaces of your device** выберите **Use the same IP address as the external interface**.

Для более подробной информации о режиме drop-in см. “Конфигурация сети в режиме drop-in”

Настройка ключа шифрования

В мастере Quick Setup Wizard вам необходимо будет для устройства Firebox создать пароли состояния и конфигурации. После того, как вы настроите Сервер Журналов для сбора сообщений журнала с устройства WatchGuard, в качестве ключа шифрования по умолчанию используйте созданный вами в мастере Quick Setup Wizard пароль состояния. После того, как вы настроите ваш Сервер Журналов, вы можете изменить ключ шифрования. Для более подробной информации см. “Изменение ключа шифрования Сервера Журнала”

После того, как мастер завершит работу

После того, как вы запустили мастер Quick Setup Wizard, вам возможно придется подождать некоторое время, пока устройство Firebox не будет готово к работе. Это характерно для моделей Firebox X Peak - 5500e, 6500e, 8500e, and 8500e-F. После того, как вы выполните все инструкции мастера, устройство Firebox будет настроено при помощи базовой конфигурации, которая включает в себя 4 политики (Исходящий TCP и UDP, пакетный фильтр FTP, пинг и WatchGuard) и указанные IP-адреса интерфейсов. Для изменения конфигурации устройства Firebox вы можете использовать утилиту Policy Manager.

- Для более подробной информации о том, как запустить устройство Firebox после того, как мастер Quick Setup Wizard завершит работу, см. “Завершение установки”
- Для более подробной информации о том, как запустить WatchGuard System Manager и его утилиты, см. “Запуск WatchGuard System Manager”

Завершение установки

Для того чтобы подключить устройство Firebox к сети, вам необходимо выполнить следующее.

1. Поместить устройство Firebox в его постоянное местонахождение.

2. Убедиться что станция управления и другие компьютеры используют IP-адрес Trusted интерфейса устройства Firebox в качестве своих шлюзов.

3. В WatchGuard System Manager выберите **File > Connect To Device** для того чтобы подключить станцию управления к устройству Firebox.
   Для подключения к устройству WatchGuard используйте пароль состояния

4. Если вы используете routed конфигурацию, то вам необходимо, чтобы шлюз по умолчанию на всех компьютерах, подключенных к устройству WatchGuard совпадал с IP адресом Trusted интерфейса устройства WatchGuard.

5. Выполните необходимые настройки, которые будут соответствовать требованиям вашей системы безопасности. Для более подробной информации см. *Customize your security policy*.

6. Если вы установили несколько WatchGuard серверов, то см. "Установка серверов WatchGuard System Manager"

Если вы устанавливаете серверное ПО на компьютер с включенным межсетевым экраном другого производителя (не Windows), вам необходимо будет открыть порты для подключения через этот межсетевой экран. Пользователям Windows Firewall нет необходимости изменять конфигурацию своего межсетевого экрана.

Настройка вашей политики безопасности

Ваша политика безопасности определяет, какие пользователи могут подключаться к сети, к каким компьютерам сети они могут получать доступ и какие пользователи могут получать доступ к внешним ресурсам. Конфигурационный файл вашего Firebox создает политику безопасности. Конфигурационный файл, созданный при помощи мастера Quick Setup Wizard, это только базовая конфигурация.

Вы можете создать конфигурационный файл, который настроит политику безопасности в соответствие с требованиями вашей системы безопасности. Для того чтобы определить типы исходящего и входящего трафиков, которые вы хотите запретить или разрешить, вам необходимо в конфигурационный файл добавить пакетные фильтры и политики прокси.

Каждая политика влияет на работу вашей сети. Политики, которые увеличивают уровень безопасности вашей сети, могут значительно ограничить доступ к ней. Политики, которые облегчают доступ к вашей сети снижают уровень ее безопасности. При выборе политик безопасности вам необходимо выбрать набор сбалансированных политик, в зависимости от того, какое оборудование вы хотите защитить.

Если вы устанавливаете систему в первый раз, то мы рекомендуем вам использовать только пакетные фильтры до того момента, когда система начнет нормально функционировать. При необходимости вы можете добавить политики прокси.

Сервис LiveSecurity Service

В комплект поставки устройства Firebox входит подписка на сервис LiveSecurity Service. Ваша подписка предоставляет вам следующие возможности:

- Вы сможете загружать последние обновления ПО для обеспечения наилучшей защиты вашей сети

- Возможность получать квалифицированную помощь по техническим вопросам с предоставлением всех ресурсов технической поддержки
- Обеспечивает бесперебойную работу устройств посредством предоставления самой последней информации по вопросам безопасности
- Предоставляет доступ к справочной информации по различным вопросам безопасности сетей
- Улучшает систему защиты вашей сети при помощи дополнительного ПО и другиз компонентов
- Расширяет вашу аппаратную гарантию с возможностью замены вышедшего из строя оборудования

Для более подробной информации о сервисе LiveSecurity Service см. “Техническая поддержка WatchGuard”

Запуск WatchGuard System Manager

Для того чтобы запустить WatchGuard System Manager выполните следующее:

Выберите **Start** > **All Programs** > **WatchGuard System Manager 11.0** > **WatchGuard System Manager**.
Откроется WatchGuard System Manager.

Для более подробной информации о работе с WatchGuard System Manager (WSM) см. “Глава 19 - Управление устройствами и VPN”

Подключение к устройству WatchGuard

1. Откройте WatchGuard System Manager.
2. Нажмите  .
   Или выберите **File > Connect to Device**.
   Или правой кнопкой нажмите на любое место окна WSM (закладка **Device Status**) и выберите **Connect to Device**.
   Откроется диалоговое окно Connect to Firebox.

3. В выпадающем списке **Name / IP Address** введите имя или IP адрес устройства WatchGuard. При последующих подключениях вы сможете выбрать необходимый Firebox из выпадающего списка **Name / IP Address**.

4. В поле **Passphrase** Введите пароль состояния Firebox (только для чтения). Пароль состояния используется для мониторинга трафика и состояния устройства Firebox. При сохранении новой конфигурации вам необходимо будет ввести пароль конфигурации

5. (Дополнительно) При необходимости измените значение в поле **Timeout**. Это поле устанавливает промежуток времени (в секундах), в течение которого станция управления ждет данные от устройства Firebox перед тем как отправить сообщение о том, что она не может получить данные. Если у вас невысокая скорость работы сети или Интернет подключения, то вам необходимо увеличить это значение. Уменьшение этого значения уменьшает время ожидания таймаут-сообщения при попытке подключения к устройству Firebox, которое недоступно.

6. Нажмите **Login**.
Устройство WatchGuard появится в окне WatchGuard System Manager.

Отключение от устройства WatchGuard

1. Выберите закладку **Device Status**.

2. Выберите устройство.

3. Нажмите  .
Или выберите **File** > **Disconnect**.
Или нажмите правой кнопкой и выберите **Disconnect**.

Отключение от всех устройств WatchGuard

Если вы подключены к нескольким устройствам Firebox, вы можете одновременно отключиться от их всех.

1. Выберите закладку **Device Status**.

2. Выберите **File > Disconnect All**.
Или нажмите правой кнопкой и выберите **Disconnect All**.

Запуск утилиты безопасности

Вы можете в WatchGuard System Manager запустить следующие утилиты безопасности.

Policy Manager

При помощи утилиты Policy Manager вы можете устанавливать, настраивать и изменять политику безопасности сети для устройства Firebox

Для того чтобы запустить утилиту Policy Manager нажмите  . Или выберите **Tools > Policy Manager**.

Firebox System Manager

Утилита WatchGuard Firebox System Manager используется для запуска различных утилит безопасности при помощи простого интерфейса. Также при помощи утилиты Firebox System Manager вы можете выполнять мониторинг трафика, который проходит через межсетевой экран, в режиме реального времени.

Для того чтобы запустить Firebox System Manager, нажмите  . Или выберите **Tools** > **Firebox System Manager**.

HostWatch

Утилита HostWatch показывает соединения через устройство Firebox из доверенной сети во внешнюю сеть, или через другие интерфейсы или VLAN. Утилита может показывать текущие соединения, а также историю соединений, информация о которых берется из файла журнала

Для того чтобы запустить HostWatch, нажмите  . Или выберите **Tools > HostWatch**

LogViewer

Утилита LogViewer используется для отображения файлов журнала. Утилита предоставляет пользователям следующие возможности:

- Применять фильтр по типу данных
- Искать слова и поля
- Печатать и сохранять в файл

Для более подробной информации об утилите LogViewer, см. Use LogViewer to see log files. Для того чтобы запустить утилиту LogViewer, нажмите  . Или выберите **Tools > Logs > LogViewer**.

Report Manager

Это итоговая информация по данным, которые вы собрали из файлов журналов устройства Firebox. Для более подробной информации об утилите WatchGuard Reports, см. About the Report Manager.

Для того чтобы запустить Report Manager, нажмите  . Или выберите **Tools > Logs > Report Manager**.

Мастер Quick Setup Wizard

При помощи мастера Quick Setup Wizard вы можете создавать базовую конфигурацию для вашего устройства Firebox. Firebox использует эту конфигурацию при первом запуске. Это позволяет устройству Firebox работать изначально как обычный межсетевой экран. Вы можете использовать ту же самую процедуру в любое время когда вы хотите перезагрузить устройство Firebox с новой конфигурацией с целью восстановления или по другим причинам

Для того чтобы запустить мастер Quick Setup Wizard, нажмите  .

Или выберите **Tools** > **Quick Setup Wizard**.

CA Manager

В системе WatchGuard System Manager, компьютер, на котором настроен Сервер Управления, также выполняет функции Центра Сертификации (далее ЦС)(CA). ЦС выдает сертификаты пользователям Firebox когда они подключаются к Серверу Управления для получения обновлений конфигурации. Перед тем как использовать Сервер Управления в качестве Центра Сертификации, вам необходимо настроить его на Сервере Управления

Для того чтобы настроить или изменить параметры центра сертификации нажмите  . Или выберите **Tools > CA Manager**.

Дополнительно

Установка WSM и сохранение старой версии

Вы можете установить новую версию WSM (WatchGuard System Manager), не удаляя старую версию. Так как вы можете установить только одну версию серверного ПО, вам необходимо или удалить серверные компоненты из старой версии WSM или установить новую версию WSM без серверных компонентов. Мы рекомендуем перед установкой новой версии WSM удалить серверные компоненты предыдущей версии.

Установка Серверов WatchGuard на компьютеры с установленными программными брандмауэрами

Программные межсетевые экраны могут заблокировать порты, которые необходимы для работы серверов WatchGuard. Перед тем как установить Серверы Управления, Журналов, Отчетов, Карантина и сервер WebBlocker на компьютер с установленными программными межсетевыми экранами, вам необходимо будет открыть соответствующие порты. Пользователям Windows Firewall нет необходимости менять свою конфигурацию, так как программа установки автоматически откроет необходимые порты.

В таблице приведены номера портов, которые необходимо открыть.

Тип сервера/ Серверный компонент	Протокол/порт
Сервер Управления	TCP 4109, TCP 4110, TCP 4112, TCP 4113
Сервер Журналов с установленным Fireware	TCP 4115
Сервер Журналов с установленным WFS	TCP 4107
Сервер WebBlocker	TCP 5003, UDP 5003
Сервер Карантина	TCP 4119, TCP 4120
Сервер Отчетов	TCP 4122
Сервер Журналов	TCP 4121

Поддержка Динамического IP адреса на External интерфейсе

Если вы хотите использовать динамические IP адреса, вам необходимо настроить ваше устройство WatchGuard в режиме routed. Если вы выберете DHCP, ваше устройство WatchGuard для получения IP адреса, шлюза по умолчанию и маски подсети будет подключаться к DHCP серверу под управлением вашего ISP. Этот сервер также может предоставить информацию о DNS сервере. Если DHCP сервер не предоставляет вам информации о DNS, то вам необходимо добавить ее вручную. При необходимости вы можете изменить IP адрес, выданный вашим ISP.

Вы также можете использовать PPPoE.

Как и в случае с DHCP, Firebox подключается по протоколу PPPoE к серверу PPPoE вашего ISP. Это подключение автоматически настраивает ваш IP-адрес, шлюз и маску подсети.

Если вы используете PPPoE на External интерфейсе, то при настройке сети вам необходимо будет ввести имя пользователя и пароль PPP. Если ваш ISP выдал вам доменное имя, то при работе с мастером Quick Setup Wizard введите это имя в формате «пользователь@домен».

Статический IP-адрес необходим устройству Firebox для выполнения некоторых функций. Если вы настроили динамическое получение IP-адресов, то устройство Firebox не сможет использовать эти функции:

- FireCluster
- Drop-in режим
- 1-to-1 NAT на External интерфейсе
- Mobile VPN с PPTP

Если ваш ISP для выдачи статического IP адреса использует PPPoE, то WatchGuard устройство позволяет вам включить Mobile VPN with PPTP.

Подключение кабелей Firebox

- Подключите Firebox к источнику питания при помощи силового кабеля.
- Для подключения вашей станции управления к концентратору или коммутатору мы рекомендуем использовать прямой Ethernet-кабель зеленого цвета.
- Для подключения устройства Firebox к концентратору или коммутатору используйте такой же кабель.
- Вы также можете использовать красный кроссовер-кабель для подключения интерфейса Trusted к Ethernet-порту станции управления.

Подключение к Firebox через Firefox v3

Web браузеры используют сертификаты для того чтобы идентифицировать устройство, которое пытается установить HTTP соединение. В случае если сертификат является самоподписанным сертификатом или если запрашиваемые IP адрес или имя хоста отличаются от IP адреса или имени хоста, указанного в сертификате, пользователи увидят предупреждение. По умолчанию ваш Firebox использует самоподписанные сертификаты, которые используются для оперативной настройки вашей сети. Однако при попытке подключиться к Firebox через браузер пользователь видит сообщение *Secure Connection Failed*.

Для того чтобы избежать такой ситуации, мы рекомендуем установить валидный сертификат, подписанный Центром Сертификации (Certificate Authority). Этот сертификат ЦС можно также использовать для увеличения уровня безопасности VPN аутентификации.

Если вы хотите и дальше использовать самоподписанный сертификат, то вам необходимо создать исключение для Firebox на каждом компьютере пользователей. Текущие версии браузеры в окне предупреждения выводят также ссылку, по которой пользователь может перейти и продолжить подключение. Если в вашей компании используется браузер Mozilla Firefox v3, вашим пользователям необходимо создать исключение для сертификата перед тем как они смогут подключаться к устройству Firebox.

Действия, для которых необходимо создать исключение:

- Аутентификация пользователя
- Установка и подключение Mobile VPN with SSL-клиента
- Запуск мастера Web Setup Wizard

- Подключение к Web интерфейсу Fireware XTM Web UI
- Edge (v10.x и выше) и SOHO устройства, как управляемые клиенты

URL, для которых необходимо создать исключение:

- https://IP адрес или имя хоста интерфейса Firebox:8080
- https://IP адрес или имя хоста интерфейса Firebox:4100
- https:// адрес или имя хоста Firebox:4100/sslvpn.html

Создание исключения сертификата в Mozilla Firefox v3

Для того чтобы при последующих подключениях пользователь не видел сообщение предупреждения, вам необходимо в Firefox v3 создать исключение для сертификата Firebox. Создать исключение вам необходимо для каждого IP адреса, имени хоста и номера порта, которые используются для подключения к Firebox. Например, исключение, которое будет использовать только имя хоста, будет работать некорректно если вы, например, будете подключаться по IP адресу. Аналогично, исключение для порта 4100 не будет применяться для подключений, в которых не указан номер порта.

Созданное исключения для сертификата не снижает уровень безопасности, так как весь трафик между вашим компьютером и устройством WatchGuard зашифрован средствами SSL.

Есть два способа создания исключений.

- Нажать на ссылку в окне **Secure Connection Failed**.
- Создать исключения при помощи Firefox v3 Certificate Manager.

В окне **Secure Connection Failed**:

1. Нажмите **Or you can add an exception**.
2. Нажмите **Add Exception**.
   Откроется диалоговое окно Add Security Exception
3. Нажмите **Get Certificate**.
4. Включите опцию **Permanently store this exception**.
5. Нажмите **Confirm Security Exception**.

Для того чтобы создать несколько исключений выполните следующее:

1. В Firefox выберите **Tools > Options**.
   Откроется диалоговое окно Options.
2. Выберите **Advanced**.
3. Выберите закладку **Encryption** и нажмите **View Certificates**.
   Откроется диалоговое окно Certificate Manager.
4. Выберите закладку **Servers** и нажмите **Add Exception**.
5. В поле **Location** введите URL для подключения к Firebox. Наиболее часто используемые URL приведены выше.
6. Когда в разделе **Certificate Status** появится информация о сертификате нажмите **Confirm Security Exception**.

7. Нажмите **OK**. Для того чтобы добавить еще несколько исключений повторите п. 4–6.

Отключение HTTP прокси в браузере

Многие web браузеры используют HTTP прокси сервер для увеличения скорости загрузки страниц. Для управления устройством Firebox через web интерфейс вам необходимо к нему подключаться напрямую. Если вы используете HTTP прокси сервер, то вам необходимо временно его отключить в настройках браузера.

После того, как вы выполните необходимые настройки на Firebox, вы можете заново включить HTTP прокси сервер. Для того чтобы отключить HTTP прокси в Firefox, Safari или Internet Explorer см. нижеприведенные инструкции. Если вы используете другой браузер, используйте его справочную систему. Большинство браузеров автоматически отключают использование HTTP прокси сервера.

Отключение HTTP прокси в Internet Explorer 6.x or 7.x

1. Откройте Internet Explorer

2. Выберите **Tools** > **Internet Options**.
   Откроется диалоговое окно Internet Options.

3. Выберите закладку **Connections** tab.

4. Выберите **LAN Settings**.
   Откроется диалоговое окно Local Area Network (LAN) Settings.

5. Отключите опцию **Use a proxy server for your LAN**.

6. Нажмите **OK** Для того чтобы закрыть диалоговое окно **Local Area Network (LAN) Settings**.

7. Нажмите **OK** для того чтобы закрыть диалоговое окно **Internet Options**.

Отключение HTTP прокси в Firefox 2.x

1. Откройте Firefox.

2. Выберите **Tools** > **Options**.
   Откроется диалоговое окно Options.

3. Нажмите на иконку **Advanced**.

4. Выберите закладку **Network**. Нажмите **Settings**.

5. Нажмите **Connection Settings**.
   Откроется диалоговое окно Connection Settings.

6. Включите опцию **Direct Connection to the Internet**.

7. Нажмите **OK** для того чтобы закрыть диалоговое окно **Connection Settings**.

8. Нажмите **OK** для того чтобы закрыть диалоговое окно **Options**.

Отключение HTTP прокси в Safari 2.0

1. Откройте Safari

2. Выберите **Preferences**
   Откроется диалоговое окно Safari preferences.

3. Нажмите на иконку **Advanced**.

4. Нажмите на кнопку **Change Settings**.
   Откроется диалоговое окно System Preference.

5. Отключите опцию **Web Proxy (HTTP)**.

6. Нажмите **Apply Now**.

Ваши настройки TCP/IP

Для того чтобы получить информацию о настройках вашей сети, вы можете посмотреть настройки TCP/IP любого из компьютеров, подключенного к этой сети. Для того чтобы подключить ваше устройство WatchGuard вам необходимо следующее:

- IP адрес
- Маска подсети
- Шлюз по умолчанию
- Статический или динамический IP адрес

Если ваш ISP присвоил вам IP адрес, который начинается с 10, 192.168, или с 172.16 до 172.31, это значит, что ваш ISP использует NAT (Network Address Translation) и ваш IP адрес является внутренним адресом. Для External интерфейса мы рекомендуем использовать публичный IP адрес. Если External интерфейсу будет присвоен внутренний IP адрес, то у вас могут возникнуть проблемы с некоторым функционалом, например cVPN.

Для того чтобы посмотреть настройки TCP/IP для вашего компьютера, см. Следующий раздел данной главы.

Настройки TCP/IP в Microsoft Windows Vista

1. Выберите Start > Programs > Accessories > Command Prompt.
   Откроется диалоговое окно Command Prompt.

2. В командной строке введите `ipconfig /all` и нажмите **Enter**.

3. Запишите параметры для основного сетевого адаптера (primary network adapter).

Настройки TCP/IP в Microsoft Windows 2000, Windows 2003 и Windows XP

1. Выберите **Start** > **All Programs** > **Accessories** > **Command Prompt**.
   Откроется диалоговое окно Command Prompt.

2. В командной строке введите `ipconfig /all` и нажмите **Enter**.

3. Запишите параметры для основного сетевого адаптера (primary network adapter).

Настройки TCP/IP в Microsoft Windows NT

1. Выберите **Start** > **Programs** > **Command Prompt**.
   Откроется диалоговое окно Command Prompt.

2. В командной строке введите `ipconfig /all` и нажмите **Enter**.

3. Запишите параметры для основного сетевого адаптера (primary network adapter).

Настройки TCP/IP в Macintosh OS 9

1. Выберите **Apple menu** > **Control Panels** > **TCP/IP**.
   Откроется диалоговое окно TCP/IP.

2. Запишите параметры для основного сетевого адаптера (primary network adapter).

Настройки TCP/IP в Macintosh OS X 10.5

1. Выберите **Apple** > **System Preferences** или нажмите на иконку в **Dock**.
   Откроется диалоговое окно System Preferences.

2. Нажмите на иконку **Network**.
   Откроется панель Network preference.

3. Выберите адаптер, который используется для подключения к сети Интернет.

4. Запишите параметры для основного сетевого адаптера.

Настройки TCP/IP в других операционных системах (Unix, Linux)

1. Для того чтобы найти настройки TCP/IP см. Документацию по вашей ОС.

2. Запишите параметры для основного сетевого адаптера.

Глава 5 - Настройка и управление

Базовая настройка и управление

После подключения вашего устройства WatchGuard в сеть и его настройки при помощи базового конфигурационного файла, вы можете приступить к его конфигурации в соответствие с требованиями системы безопасности вашей компании.

Конфигурационные файлы

Конфигурационный файл Firebox включает данные конфигурации, опции, IP-адреса и другую информацию, которая формирует вашу политику безопасности. Конфигурационные файлы имеют расширение .xml.

Policy Manager для Fireware или Fireware Pro – утилита WatchGuard при помощи которой вы может создавать, изменять и сохранять конфигурационные файлы. При работе с Policy Manager на экране вы можете увидеть версию конфигурационного файла, которую легко проверить и изменить. С помощью Policy Manager, вы можете выполнять следующее:

- Открыть конфигурационный файл: или конфигурационный файл, который на данный момент используется вашим Firebox, или локальный конфигурационный файл, который хранится на вашем жестком диске и не используется)
- Создавать новый конфигурационный файл
- Сохранить конфигурационный файл
- Редактировать существующие конфигурационные файлы

Открытие конфигурационного файла

Сетевым администраторам иногда необходимо вносить изменения в политику безопасности сети. Например, ваша компания приобрела новое приложение и вам необходимо открыть порт и протокол для доступа к серверу на сайте производителя. Ваша компания также может приобрести новый компонент для Firebox или наняла нового сотрудника, которому необходим доступ к ресурсам сети.

Для того чтобы выполнить все эти, и многие другие задачи, вам необходимо открыть ваш конфигурационный файл, при помощи утилиты Policy Manager внести необходимые изменения и сохранить конфигурационный файл.

Открытие конфигурационного файла в WatchGuard System Manager

1. В ОС Windows выберите **Start > All Programs > WatchGuard System Manager 10 > WatchGuard System Manager**. WatchGuard System Manager 10 является по умолчанию названием каталога для иконок меню Start. Вы не можете изменить это имя во время установки, но вы можете изменить его через ОС Windows.

2. Нажмите  . Или выберите **File > Connect To Device**.
   Откроется диалоговое окно Connect to Firebox.

3. Из выпадающего списка выберите ваш Firebox или введите IP-адрес его интерфейса Trusted. Введите пароль состояния. Нажмите **OK**.
   Устройство появится в закладке Device Status системы WatchGuard System Manager

4. В закладке **Device Status** выберите необходимый Firebox. Затем нажмите . Или выберите **Tools > Policy Manager**. Откроется утилита Policy Manager, которая в свою очередь откроет конфигурационный файл выбранного Firebox. Для того чтобы сделанные вами изменения вступили в силу необходимо сохранить конфигурационный файл на Firebox.

Открытие локального конфигурационного файла

Вы можете открывать конфигурационные файлы, которые находятся на любом сетевом диске, доступ к которому имеет ваша станция управления. Если вы хотите использовать конфигурационный файл, который был создан по умолчанию, мы рекомендуем вам запустить мастер Quick Setup Wizard, при помощи него создать базовый конфигурационный файл и затем открыть существующий конфигурационный файл. Однако, если вы откроете конфигурационный файл, который был производителем создан по умолчанию, убедитесь, что вы изменили пароли состояний и конфигурации.

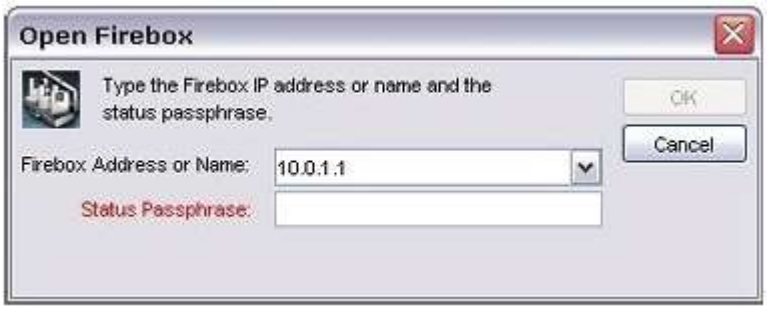
1. В WatchGuard System Manager нажмите . Или выберите **Tools > Policy Manager**.
   Откроется окно Policy Manager.

2. Выберите **Open Configuration File** и нажмите **Browse**

3. При помощи диалогового окна **Open** найдите и откройте необходимый конфигурационный файл. Нажмите **Open**.
   Policy Manager откроет конфигурационный файл и отобразит необходимые параметры

Открытие конфигурационного файла при помощи Policy Manager

1. В Policy Manager выберите **File > Open > Firebox**.
   Откроется диалоговое окно Open Firebox. Если появится сообщение об ошибке подключения, попробуйте еще раз.



2. Из выпадающего списка **Firebox Address or Name** выберите необходимый Firebox.
   Вы также можете ввести IP-адрес или имя хоста.

3. В поле **Status Passphrase** введите пароль состояния Firebox. Также пароль состояния используется для сохранения нового конфигурационного файла на Firebox.

4. Нажмите **OK**.
   Policy Manager откроет конфигурационный файл и отобразит все необходимые параметры.

Если вы не можете открыть Policy Manager, попробуйте выполнить следующее:

- Если диалоговое окно **Connect to Firebox** открывается сразу после того, как вы введете пароль, убедитесь, что клавиша Caps Lock отключена, и что пароль вы ввели правильно. Помните, что пароль чувствителен к регистру

- Если наступает таймаут диалогового окна **Connect to Firebox**, проверьте подключение к интерфейсу Trusted и на вашем компьютере. Также убедитесь, что вы ввели правильный IP – адрес интерфейса Trusted. Также убедитесь, что IP-адрес вашего компьютера находится в той же сети, что и IP-адрес интерфейса Trusted устройства Firebox.

Создание конфигурационного файла

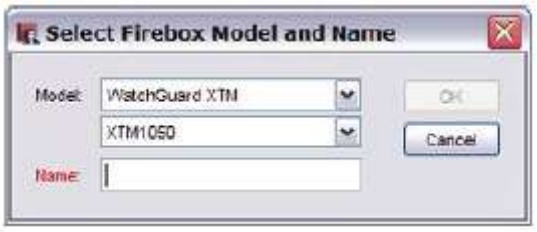
Мастер Quick Setup Wizard создает базовый конфигурационный файл для вашего Firebox. Мы рекомендуем его использовать как основу для всех остальных конфигурационных файлов. Также создать конфигурационный файл с параметрами по умолчанию вы можете при помощи утилиты Policy Manager

1. В WatchGuard System Manager нажмите  . Или выберите **Tools > Policy Manager**.
   Откроется Policy Manager

2. В Policy Manager выберите **Create a new configuration file for**

3. В выпадающем списке **Firebox** выберите тип конфигурации

4. Нажмите **OK**.
   Откроется диалоговое окно Select Firebox Model and Name



5. Из выпадающего списка **Model** выберите модель вашего Firebox. Так как для каждой модели существует набор уникальных параметров, то вам необходимо выбрать именно модель вашего Firebox.

6. В поле **Name** введите имя, которое будет использоваться как имя конфигурационного файла. Оно также будет использоваться для идентификации вашего Firebox, если он находится под управления Сервера Управления, а также в сообщениях журнала и отчетов

7. Нажмите **OK**.

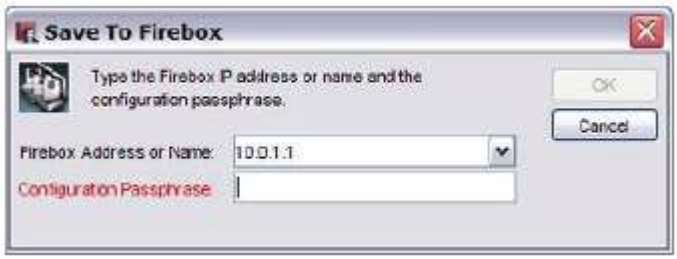
Утилита Policy Manager создаст новый конфигурационный файл с именем <*name*>*.xml*, где <*name*> - это имя, которые вы присвоили вашему Firebox.

Сохранение конфигурационного файла

После того как вы создали новый конфигурационный или внесли изменения в текущий конфигурационный файл, вы можете сохранить его прямо в Firebox. Если вы внесли изменения в рабочий конфигурационный файл и хотите, чтобы ваши изменения вступили в силу, вам необходимо сохранить конфигурационный файл в Firebox. Вы также можете сохранить текущий конфигурационный файл на жесткий диск. Если вы планируете внести какие-либо изменения в конфигурационный файл, мы рекомендуем сначала сохранить копию старого конфигурационного файла на жесткий диск. Если у вас возникнут проблемы с новой конфигурацией, вы всегда можете восстановить старую конфигурацию

Сохранение конфигурации на Firebox

1. В окне Policy Manager нажмите **File > Save > To Firebox**.
   Откроется диалоговое окно Save to Firebox.



2. Из выпадающего списка **Firebox Address or Name** выберите необходимый Firebox, или введите его имя или IP-адрес. Если вы используете имя Firebox – это имя должно быть прописано на DNS-сервере.

   При вводе IP-адреса вводите все цифры и точки. Не используйте клавишы со стрелками или клавишу Tab.

3. Введите пароль конфигурации. Для сохранения конфигурационного файла в Firebox необходимо использовать пароль конфигурации.

4. Нажмите **OK**.

Сохранение конфигурации на локальный жесткий или сетевой диски

1. В окне Policy Manager выберите **File** > **Save** > **As File**. Вы также можете использовать комбинацию CTRL-S.
   Откроется стандартное диалоговое Windows-окно сохранения файла

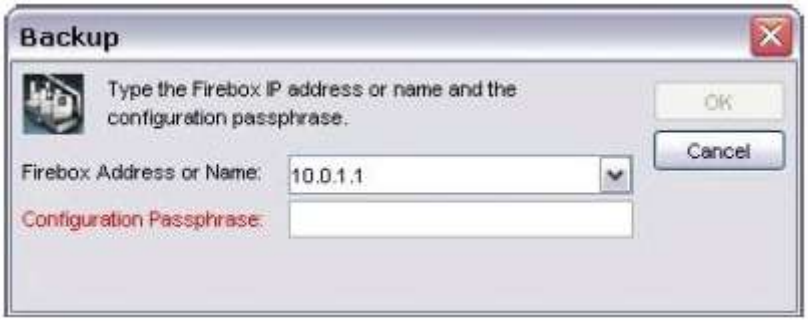
2. Введите имя файла. По умолчанию файл сохраняется в каталог *My Documents\My WatchGuard\configs*. Вы также можете сохранять конфигурационный файл в любой каталог, к которому вы можете подключиться с вашей станции управления. Для повышения уровня безопасности, мы рекомендуем сохранять конфигурационный файл в специальный каталог, недоступный для других пользователей.

3. Нажмите **Save**.
   Файл конфигурации будет сохранен на жесткий диск.

Резервные копии образов flash-дисков Firebox

Резервная копия – это зашифрованная и сохраненная копия образа flash-диска Firebox. Она включает в себя программно-аппаратное обеспечение, конфигурационный файл, лицензии и сертификаты. Вы может сохранять резервную копию на вашу станцию управления и в любой сетевой каталог. Мы рекомендуем регулярно делать резервные копии образа flash-диска Firebox. Мы также рекомендуем делать резервные копии перед тем, как вносить изменения в конфигурацию Firebox или обновлять Firebox или его программно-аппаратное обеспечение

1. В окне Policy Manager выберите File > Backup.
   Откроется диалоговое окно Backup.



2. Введите пароль конфигурации для вашего Firebox.
   Откроется вторая часть окна Backup.

3. Введите ключ шифрования и его подтверждение. Это ключ используется для шифрования резервного файла. Если вы потеряете или забудете ключ шифрования, то вы не сможете восстановить резервный файл.

4. Выберите каталог, в который вы хотите сохранить резервный файл. Нажмите **OK**. По умолчанию каталог сохранения резервного файла (с расширением ".fxi"):

   C:\Documents and Settings\All Users\Shared WatchGuard\backups\<IP-адрес Firebox> - <дата><версия_WSM>.fxi.

5. Нажмите **OK**.

Восстановление копии образа flash-диска Firebox

1. В окне Policy Manager выберите **File > Restore**.

2. Введите пароль конфигурации для вашего Firebox. Нажмите **OK**.

3. Введите ключ шифрования, который вы использовали при создании резервной копии. Firebox восстановит копию образа flash-диска и перезагрузится. При перезагрузке он будет использовать копию образа flash-диска.

   По умолчанию каталог сохранения резервного файла (с расширением ".fxi"):

C:\Documents and Settings\All Users\Shared WatchGuard\backups\<IP-адрес Firebox> - <дата><версия_WSM>.fxi.

Подождите две минуты перед тем, как подключаться к Firebox. Если вы не можете восстановить образ flash-диска вашего Firebox, вы можете перезагрузить Firebox.

В зависимости от имеющейся у вас в наличие модели Firebox, вы можете перезагрузить Firebox для восстановления заводских настроек или запустить мастер Quick Setup Wizard для того чтобы создать новую конфигурацию.

Для более подробной информации см. “Перезагрузка Firebox с предыдущей или новой конфигурациями”

Использование существующей конфигурации для новой модели Firebox

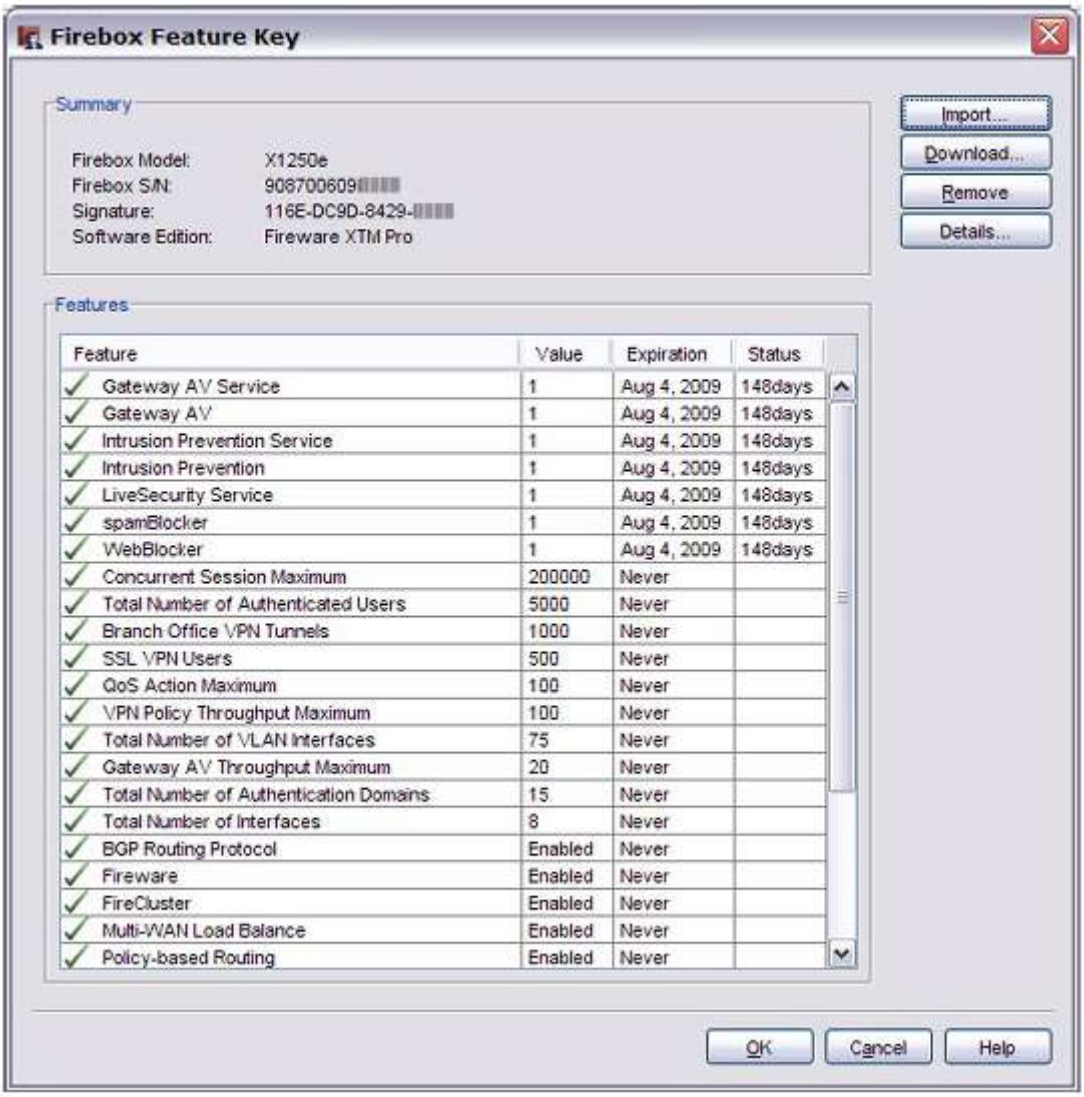
При обновлении модели вашего Firebox вы можете продолжать использовать ваш старый конфигурационный файл. Во время импорта нового ключа функций Firebox может автоматически изменить ваш существующий конфигурационный файл для его корректной работы с новой моделью Firebox. Для этого выполните следующее:

1. Получите ключ функций для вашего нового Firebox.

2. Если у вашего нового Firebox имеет больше интерфейсов, чем у старого, то вам необходимо будет отключить дополнительные интерфейсы. Например, если хотите обновить Firebox с шестью интерфейсами до Firebox с восемью интерфейсами, то вам необходимо на новом Firebox отключить два интерфейса. Для того чтобы узнать количество интерфейсов, используемых вашим Firebox см. ниже.

3. На вашем текущем Firebox откройте Policy Manager.

4. Выберите **Setup** > **Feature Keys**.
Откроется диалогое окно Firebox Feature Key.



5. Нажмите **Remove** для того чтобы удалить текущий ключ функций

6. Нажмите **Import**.
   Откроется диалогое окно Import Firebox Feature Key

7. Когда вы получили лицензионный ключ для вашего нового Firebox, вы сохранили этот ключ в файле. Откройте этот файл и скопируйте его содержимое для нового Firebox в диалоговом окнеthe **Import Firebox Feature Key**.

8. Нажмите **OK**. Policy Manager при помощи нового лицензионного ключа заменить модель в конфигурационном файле. Для того чтобы проверить в Policy Manager выберите **Setup > System**.

9. Выберите **File > Save > To Firebox** для того чтобы сохранить конфигурацию.

Определение количества интерфейсов на вашем Firebox

Если вы не уверены в количестве интерфейсов на вашем Firebox см. страницу со сравнительной характеристикой продуктов:

http://www.watchguard.com/products/compare.asp

Настройка нового Firebox

Если ваш Firebox выходит из строя в течение гарантийного срока, компания WatchGuard может заменить его согласно RMA (Return Merchandise Agreement) на ту же самую модель. При замене Firebox служба WatchGuard Customer Care переносит лицензии со старого Firebox на новый. Весь функционал, включенный в лицензии старого Firebox, будет работать в новом Firebox.

Для того чтобы настроить ваш новый Firebox для работы со старой конфигурацией, вам необходимо выполнить все инструкции, приведенные ниже.

Сохраните конфигурации старого Firebox в файл

Файл конфигурации по умолчанию сохраняется в каталог *My Documents\My WatchGuard\configs*. Для более подробной информации см. “Сохранение конфигурационного файла”

Получение ключа функций для нового Firebox

Так как серийный номер нового Firebox отличается от серийного номера вашего Firebox, то вам необходимо получить новый лицензионный ключ на сайте WatchGuard, в разделе Support. Новый Firebox будет в вашем списке активированных продуктов с таким же именем, как и старый Firebox, но с другим серийным номером.

Для более подробной информации о получении лицензионного ключа см. “Получение ключа функций от LiveSecurity”

Базовая настройка при помощи мастера Quick Setup Wizard

Также как и для любого нового устройства, для нового Firebox вам необходимо создать при помощи мастера Quick Setup Wizard создать базовый конфигурационный файл. Мастер Quick Setup Wizard может быть запущен, как Web, так и как обычное приложения.

- Для более подробной информации о запуске мастера, как Web-приложение, см. “Мастер Quick Setup Wizard”
- Для более подробной информации о запуске мастера, как обычное приложение, см. “Запуск мастер WSM Quick Setup”

Обновление лицензионного ключа в конфигурационном файле старого Firebox и сохранение его на новом Firebox

1. В WatchGuard System Manager выберите **Tools > Policy Manager**.
2. Выберите **Open configuration file**.
3. Нажмите **Browse** и выберите сохраненный конфигурационный файл старого Firebox.
4. Нажмите **Open**. Нажмите **OK**.
5. В Policy Manager выберите **Setup > Feature Keys**.
6. Нажмите **Remove** для того чтобы удалить старый лицензионный ключ.
7. Нажмите **Import** для того чтобы импортировать новый лицензионный ключ.
8. Нажмите **Browse** и выберите новый лицензионный ключ, который вы загрузили с сайта LiveSecurity.

   Или нажмите **Paste** для того чтобы вставить содержимое ключа в соответствующее текстовое поле.
9. Нажмите два раза **OK** для того чтобы закрыть диалоговые окна **Firebox Feature Key**.
10. Выберите **File > Save > To Firebox** для того чтобы сохранить конфигурацию на новый Firebox.

Конфигурация нового Firebox успешно завершена. С этого момента новый Firebox будет использовать все политики и настройки старого Firebox.

Перезагрузка Firebox с предыдущей или новой конфигурациями

Если у вашего Firebox возникли проблемы с конфигурацией, исправить которые вы не в состоянии, вы можете перезагрузить его с заводскими настройками. Например, если вы не знаете пароля администратора или перебои с электроэнергией нанесли вред програмнно-аппаратному ПО, вы

можете запустить Firebox с заводскими настройками, установленными по умолчанию и затем при помощи мастера Quick Setup Wizard создать новую конфигурацию или восстановить сохраненную.

Для более подробной информации о заводских настройках см. “Заводские настройки”

Запуск Firebox X Core или Peak e-Series, или WatchGuard XTM в безопасном режиме

Для того чтобы запустить Firebox X Core или Peak e-Series, или WatchGuard XTM с заводскими настройками вам необходимо запустить их в безопасном режиме.

1. Выключите устройство WatchGuard.
2. Нажмите на кнопку со стрелкой вниз на передней панели устройства.
3. Не отпускайте кнопку со стрелками пока на LCD дисплее не появится надпись:

   Для устройств Firebox X Core или Peak device на LCD дисплее появится надпись `WatchGuard Technologies`.

   Для устройств WatchGuard XTM на LCD дисплее появится надпись `Safe Mode Starting....`

   Если устройство работает в безопасном режиме, то на дисплее после номера модели идет слово `safe`.

Если вы запустите устройство в безопасном режиме то:

- Устройство временно использует заводские настройки сети и безопасности.
- Лицензионный ключ, который использовался до этого, не удаляется. Если вы запустите мастер Quick Setup Wizard для того чтобы создать новую конфигурацию, мастер будет использовать ранее импортированный ключ.
- Содержимое Старого конфигурационного файла не перезаписывается до тех пор, пока вы не сохраните новую конфигурацию. Если вы перезапустите Firebox, не сохранив новую конфигурацию, то устройство будет использовать текущую конфигурацию.

Перезагрузка Firebox X Edge e-Series с заводскими настройками

При перезагрузке Firebox X Edge ваши настройки заменяются на установленные по умолчанию заводские. Для того чтобы перезагрузить Firebox X Edge e-Series с заводскими настройками:

1. Отключите питание.
2. Зажмите кнопку **Reset** на задней панели Edge.
3. Продолжайте удерживать кнопку **Reset** и подключите питание.
4. Удерживайте кнопку **Reset** до того, как не загорится индикатор **Attn.** Перезагрузка Edge с заводскими настройками завершена.
   Этот процесс может занять 45 и более секунд.
5. Отпустите кнопку **Reset**.

   *Не пытайтесь подключиться к Edge в этот момент. Перед тем, как подключиться к Edge, вам необходимо его запустить еще раз. В противном случае при попытке подключения к Edge откроется web страница со следующим сообщением: Your WatchGuard Firebox X Edge is running from a backup copy of firmware. Вы также можете увидеть это сообщение в случае если кнопка **Reset** осталась в нажатом положении. Если вы продолжаете получать это сообщение, то вам необходимо проверить кнопку Reset или перезагрузить Edge.*

6. Отключите питание и подключите его снова.
   Загорится индикатор Power Indicator и ваш Edge запустится в безопасном режиме.

Запуск мастера Quick Setup Wizard

После того как вы запустите Firebox с установленными по умолчанию заводскими настройками, вы можете при помощи мастера Quick Setup создать базовую конфигурацию для Firebox или восстановить резервную копию образа Firebox.

Заводские настройки

Заводские настройки по умолчанию – это первоначальная конфигурация устройства WatchGuard. Вы всегда можете вернуться к этим настройкам, перезагрузив Firebox, как описано в "Перезагрузка Firebox с предыдущей или новой конфигурациями"

По умолчанию используются следующие настройки:

Trusted сеть (Firebox X Edge e-Series)

По умолчанию для Trusted сети используется IP-адрес 192.168.111.1, маска подсети - 255.255.255.0.

IP-адрес и порт по умолчанию для Fireware XTM Web UI - *https://192.168.111.1:8080*.

По умолчанию Firebox выдает компьютерам, подключенным к trusted сети, IP-адреса по протоколу DHCP.

По умолчанию диапазон IP-адресов - 192.168.111.2 - 192.168.111.254.

Trusted сеть (Firebox X Core and Peak e-Series и WatchGuard XTM)

По умолчанию для Trusted сети используется IP-адрес 10.0.1.1, маска подсети - 255.255.255.0.

Для Fireware XTM Web UI используются следующие IP-адрес и порт - https://10.0.1.1:8080.

По умолчанию Firebox выдает компьютерам, подключенным к trusted сети, IP-адреса по протоколу DHCP.

По умолчанию диапазон IP-адресов 10.0.1.2 - 10.0.1.254.

External сеть

Firebox получает IP адрес по DHCP.

Optional сеть

Optional сеть отключена.

Настройки брандмауэра

Все политики для входящего трафика заблокированы. Политика для исходящего трафика разрешает весь исходящий трафик. Ping-запросы, полученные из External сети заблокированы.

Система безопасности

Firebox имеет встроенную учетную запись администратора *admin* (чтение-запись) и учетную запись *status* (только чтение). При первоначальной настройки устройства при помощи Quick Setup Wizard вам необходимо будет создать пароли состояния и конфигурации. После завершения настройки устройства при помощи мастера Quick Setup Wizard вы можете подключиться к Fireware XTM Web UI под учетной записью «admin» или «status». Для того чтобы получить полный доступ, вам необходимо использовать имя пользователя *admin* и пароль конфигурации. Для того, чтобы

получить доступ только с правами чтения в вам необходимо использовать имя пользователя *status* и ввести read-only пароль.

По умолчанию администрирование Firebox осуществляется только из Trusted сети. Для того чтобы получить доступ к Firebox из External сети вам необходимо выполнить определенные настройки.

Параметры обновления

Для того чтобы включить WebBlocker, spamBlocker и Gateway AV/IPS вам необходим ключ функций или вы можете использовать команду **Get Feature Key**. Если вы запускаете Firebox в безопасном режиме, то вам нет необходимости повторно импортировать ключ функций.

Ключи функций (Feature Keys)

Ключ функций представляет собой специальную лицензию, которая разрешает вам использовать определенные функциональные компоненты на вашем Firebox.

После того, как вы приобрели новый компонент, выполните следующее

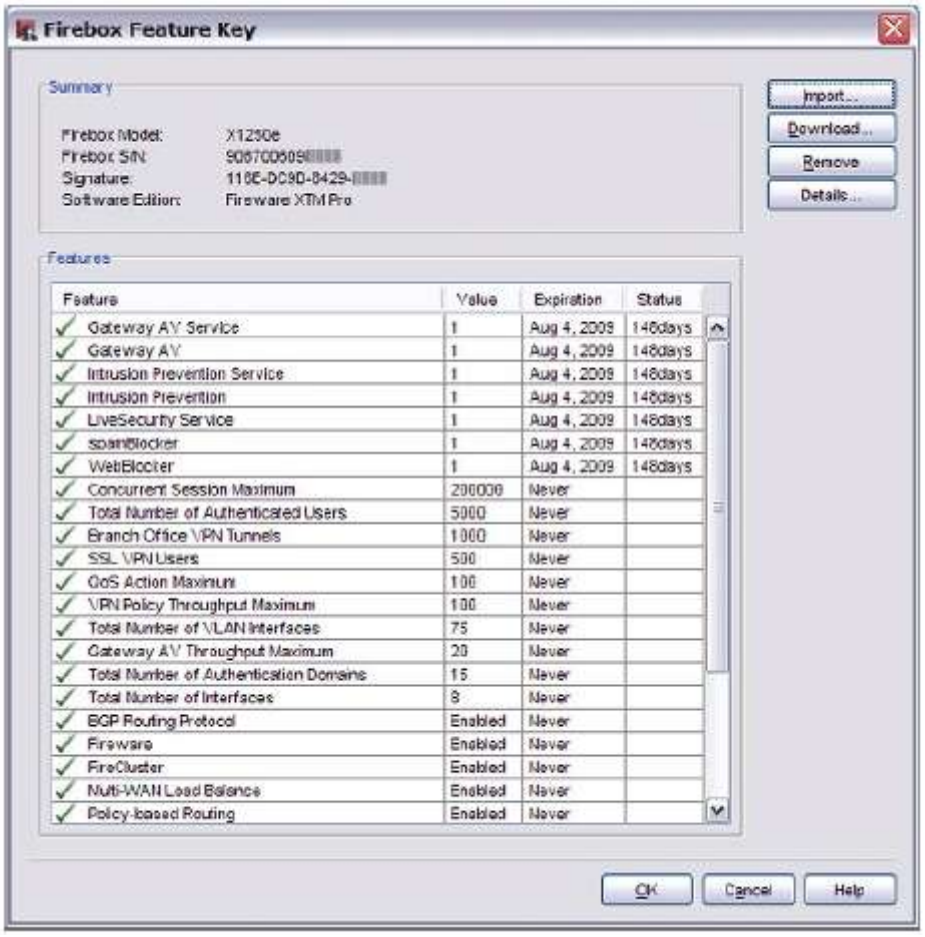
- Получите лицензионный ключ
- Импортируйте ключ в Firebox

Просмотр компонентов доступных с текущим лицензионным ключом

Для того чтобы посмотреть компоненты, доступ к которым предоставляет лицензионный ключ выполните следующее:

1. Откройте Policy Manager.

2. Выберите **Setup** > **Feature Keys**.
Откроется диалоговое окно Firebox Feature Key.



В этом окне вы найдете следующую информацию:

- Список доступных компонентов
- Включен ли или отключен компонент
- Значение, присвоенное компоненту, как например количество разрешенных интерфейсов VLAN
- Дата истечения срока действия компонента
- Текущее состояние по срокам. Например количество дней, которое осталось до истечения срока действия компонента
- Версия ПО, к которой применяется этот ключ

Проверка соответствия ключа функций

Для того чтобы проверить, что все компоненты Firebox корректно были активированы лицензионным ключом, выполните следующее:

1. Откройте Policy Manager
2. Нажмите  .
*Откроется диалоговое окно **Feature Key Compliance**. В поле Description содержится информация о том, все ли компоненты соответствующие лицензионному ключу*.

Для того чтобы получить ключ функций выполните следующее:

1. В диалоговом окне **Feature Key Compliance** нажмите **Add Feature Key**. *Откроется диалоговое окно Firebox Feature Key*.

2. Выберите, хотите ли вы импортировать или загрузить ключ функций. Для более подробной информации см. “Импорт ключа на Firebox” или “Загрузка ключа функций”

Получение ключа функций от LiveSecurity

Перед тем, как активировать новый компонент, или обновить подписку, вам необходим сертификат лицензионного ключа от компании WatchGuard, который еще не зарегистрирован на сайте LiveSecurity. При активации этого ключа, вы можете получить специальный лицензионный ключ, который включит необходимый компонент на вашем Firebox. Вы также можете получить уже существующий ключ.

Активация ключа для компонента

Для того чтобы активировать лицензионный ключ и получить специальный лицензионный ключ для активации компонента выполните следующее:

1. Зайдите на страницу https://www.watchguard.com/activate.
   Если вы еще не вошли в систему, то откроется страница LiveSecurity Log In.

2. Введите ваши имя пользователя и пароль для входа в систему LiveSecurity.
   Откроется страница Activate Products.

3. Введите серийный номер или ключ для вашего продукта (ключ вы можете найти на вашем печатном сертификате), включая дефисы. Для регистрации нового Firebox используйте серийный номер, а для регистрации дополнительных компонентов – лицензионный ключ.

4. Нажмите **Continue**.
   Откроется страница Choose Product to Upgrade.

5. В выпадающем списке выберите ваш Firebox. Если при регистрации вашего Firebox вы ввели его имя, то это имя будет в списке устройств.

6. Нажмите **Activate**.
   Откроется страница Retrieve Feature Key.

7. Скопируйте лицензионный ключ и сохраните его в текстовом файле на вашем компьютере.

8. Нажмите **Finish**.

Получение текущего ключа

Получить ваш текущий ключ вы можете двумя способами:

- Через сайт LiveSecurity и загрузить его оттуда

- Через Firebox System Manager

Через сайт вы можете загрузить один или сразу несколько ключей, собранных в одном файле. Если вы выберете несколько устройств, то этот файл будет содержат лицензионные ключи для каждого устройства.

Для того чтобы получить лицензионный ключ через сайт LiveSecurity выполните следующее:

1. Зайдите на страницу *https://www.watchguard.com/archive/manageproducts.asp*.
   Если вы еще не вошли в систему, то откроется страница LiveSecurity Log In.

2. Введите ваши имя пользователя и пароль для входа в систему LiveSecurity.
   Откроется страница Manage Products.

3. Выберите **Feature Keys**.
   Откроется страница Retrieve Feature Key со списком продуктов.

4. Из выпадающего списка выберите ваш Firebox.

5. Нажмите **Get Key**.
   Откроется список ваших зарегистрированных устройств.

6. Выберите **Show feature keys on screen**.

7. Нажмите **Get Key**.
   Откроется страница Retrieve Feature Key.

8. Скопируйте ключ в текстовый файл и сохраните его на вашем компьютере.

Для того чтобы получить ваш текущий ключ при помощи Firebox System Manager (FSM) выполните следующее:

1. Откройте FSM.

2. Выберите **Tools** > **Synchronize Feature Key**.
   Откроется диалоговое окно Synchronize Feature Key.

3. Нажмите **Yes** для синхронизации вашего лицензионного ключа.
   Firebox загрузит лицензионный ключ с сайта LiveSecurity.

Импорт ключа на Firebox

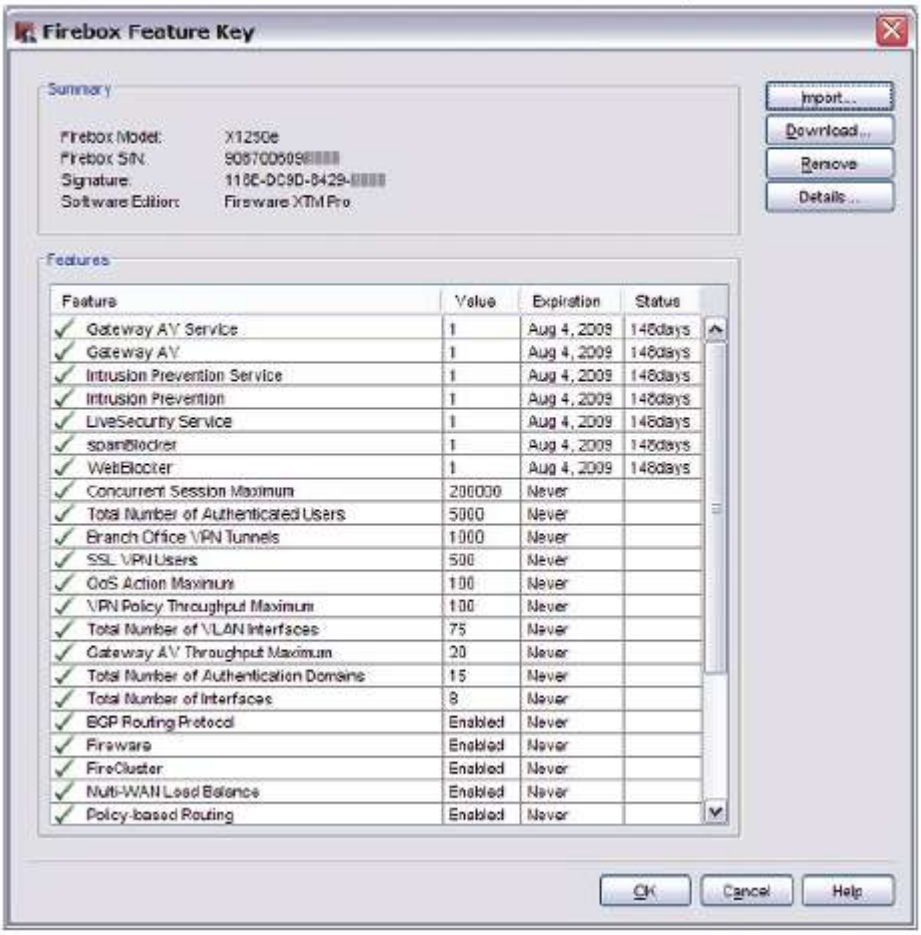
Если вы приобрели новый функционал или обновление для вашего Firebox, то для того чтобы использовать этот функционал или обновление вам необходимо импортировать ключ функций. Перед тем, как импортировать новый ключ, вам необходимо полностью удалить старый ключ.

1. В Policy Manager выберите **Setup > Feature Keys**.
   Откроется диалоговое окно Firebox Feature Keys.

   В окне вы увидите список доступных компонентов. Также это диалоговое окно содержит следующую информацию:

   - Включенные и отключенные компоненты

- Значение, присвоенное компоненту, как например количество разрешенных интерфейсов VLAN
- Дата истечения срока действия компонента
- Текущее состояние по срокам. Например количество дней, которое осталось до истечения срока действия компонента



2. Нажмите **Remove** для того чтобы удалить старый лицензионный ключ.
   Текущий ключ функций будет удален из диалогового окна.

3. Нажмите **Import**.
   Откроется диалоговое окно Import Firebox Feature Key

4. Нажмите **Browse** и выберите файл с новым ключом функций. Или, скопируйте содержимое ключа и нажмите **Paste** для того чтобы вставить его в соответствующее текстовое поле.

5. Нажмите **OK**.
   Диалоговое окно Import a Firebox Feature Key закроется и новый ключ функций появится в диалоговом окне Firebox Feature Key.

6. Нажмите **OK**.

7. Сохраните конфигурационный файл.
   Ключ функций не будет работать до тех пор, пока вы не сохраните конфигурационный файл.

Удаление ключа функций

1. В Policy Manager выберите **Setup** > **Feature Keys**.
   Откроется диалоговое окно Firebox Feature Keys.

2. Нажмите **Remove**.

3. Нажмите **OK**.

4. Сохраните конфигурационный файл.

Просмотр информации о ключе

Вы можете посмотреть следующую информацию о вашем лицензионном ключе: серийный номер Firebox, Firebox ID, имя и модель устройства, номер версии, а также список доступных компонентов. Для того чтобы посмотреть информацию о вашем ключе выполните следующее:

1. В Policy Manager выберите **Setup** > **Feature Keys**.
   Откроется диалоговое окно Firebox Feature Key.

2. Нажмите **Details**.
   Откроется диалоговое окно Feature Key Details.

3. В этом окне вы можете посмотреть всю необходимую информацию о вашем ключе.

Загрузка ключа функций

Вы можете загрузить копию вашего ключа на вашу станцию управления.

1. Выберите **Setup** > **Feature Keys**.
   Откроется диалоговое окно Feature Keys.

2. Нажмите **Download**.
   Откроется диалоговое окно Get Firebox Feature.

3. Введите пароль состояния.

4. Нажмите **OK**.

Если вы уже создали учетную запись LiveSecurity, то вы можете загрузить ключ функций при помощи Firebox System Manager.

1. Откройте Firebox System Manager.

2. Выберите **Tools** > **Synchronize Feature Key**.
   Firebox загрузит с сайта LiveSecurity текущий ключ функций.

Включение NTP и добавление NTP серверов

Протокол NTP (Network Time Protocol) используется для синхронизации часов компьютеров сети. Firebox может при помощи протокола NTP получить корретное значение времени с NTP серверов в сети Internet.

Из-за того Firebox добавляет время в каждое сообщение журнала, вам необходимо корректно его настроить. Вы можете изменить NTP сервер, который используется вашим Firebox. Вы также, помимо основного NTP сервера, вы можете добавить еще несколько NTP серверов (при необходимости их удалить), или вообще установить время вручную.

Для того чтобы использовать NTP конфигурация вашего Firebox должна разрешать DNS. По умолчанию DNS разрешен в конфигурации политикой Outgoing. Перед настройкой NTP вам необходимо настроить DNS серверы для интерфейса External. Для более подробной информации см. “Добавление WINS и DNS серверов”

1. Выберите **Setup > NTP**.
   Откроется диалоговое окно NTP Setting

2. Включите опцию **Enable NTP**.

3. Для того чтобы добавить NTP сервер, в текстовом поле введите IP-адрес или имя хоста NTP сервера и нажмите **Add**.
   Вы можете настроить максимум 3 NTP сервера

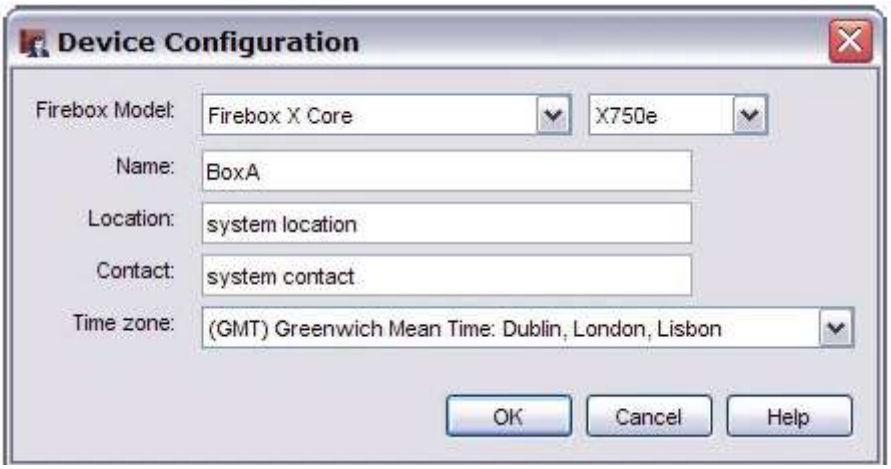
4. Для того чтобы удалить сервер в списке **NTP Server Names/IPs** выберите необходимый сервер и нажмите **Remove**.

5. Нажмите **OK**.

Настройка часового пояса и базовых параметров устройства

1. Откройте Policy Manager.

2. Выберите **Setup > System**.
   Откроется диалоговое окно Device Configuration



3. Вы можете настроить следующие параметры:

   Firebox model

   Модель Firebox и ее номер автоматически определяется мастером Quick Setup Wizard. Вам нет необходимости изменять эти параметры. Если вы добавите новый лицензионный ключ, информация о модели и ее номере автоматически обновится.

   Name

   Имя устройства Firebox. Имя, присвоенное вашему устройству, будет отображаться в файлах журналов и отчетах. В противном случае в файлах журналов и отчетах отображается IP-адрес External интерфейса устройства Firebox. Многие клиенты в качестве имени устройства используют Fully Qualified Domain Name, так как это имя зарегистрировано на DNS сервере. Если вы используете Сервер Управления для настройки VPN туннелей и сертификатов вам необходимо присвоить устройству Firebox имя.

   Location, Contact

   Здесь введите любую информацию, которая позволит идентифицировать и эффективно администрировать устройство Firebox. Если вы ввели эту информацию в мастере Quick Setup Wizard, то эта информация будет отображаться здесь. Эта информация содержится в закладке **Front Panel** программы Firebox System Manager.

   Time zone

   Выберите часовой пояс для устройства Firebox. Часовой пояс определяет дату и время, которые отображаются в файле журнала и таких утилитах, как LogViewer, WatchGuard Reports и WebBlocker.

4. Нажмите **OK**.

SNMP протокол

Протокол SNMP (Simple Network Management Protocol) используется для мониторинга устройств в вашей сети. SNMP использует специальные информационные базы MIB (Management Information Base) для того чтобы определять, какие события и какую информацию необходимо мониторить. Для сбора и анализа SNMP данных вам необходимо установить специальное приложение.

Существует два типа MIB: Standard и Enterprise. Standard MIB содержат описания событий, которые происходят в сети и внутри оборудования, и которые используются многими устройствами. Enterprise MIB используются для предоставления информации о событиях, которые характерны только для определенного оборудования.

Ваш Firebox поддерживает восемь стандартных MIB: IP-MIB, IF-MIB, TCP-MIB, UDPMIB, SNMPv2-MIB, SNMPv2-SMI, RFC1213-MIB и RFC1155 SMI-MIB, а также 2 корпоративные MIB:

WATCHGUARD-PRODUCTS-MIB и WATCHGUARD-SYSTEM-CONFIG-MIB.

SNMP опросы и ловушки

Вы можете настроить Firebox для обработки SNMP опросов от SNMP сервера. Firebox сообщает серверу SNMP разнообразную информацию, включая количество трафика на каждом интерфейсе, время работы устройства, количество полученных и отправленных TCP пакетов и дату последнего обновления интерфейса Firebox.

SNMP ловушка – это уведомление о событии, которое Firebox отправляет системе управления SNMP. Ловушка определяет наступление определенного события, как например превышение какого-нибудь порогового значения. Вы можете настроить Firebox таким образом, что для каждой политики в Policy Manager Firebox будет отправлять ловушки. SNMP-запрос информации похож на

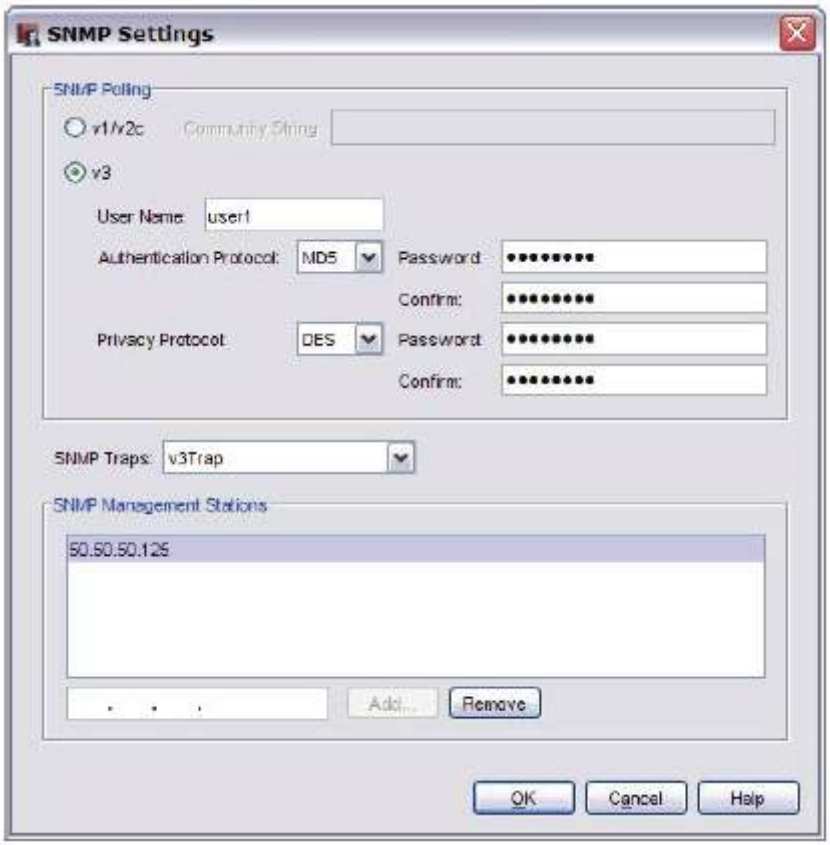
ловушку, но принимающая сторона отправляет ответ на него. Если устройство Firebox не получает ответа, оно отправляет запрос снова до тхе пор, пока SNMP менеджер не ответит.

Ловушка отправляется только один раз и принимающая сторона не отправляет никаких ответов. Запрос на информацию более надежен в отличие от ловушки, так как Firebox знает был ли запрос доставлен до адресата или нет.

Включение SNMP опросов

Вы можете настроить ваш Firebox для обработки SNMP опросов с SNMP сервера. В ответ на опросы Firebox отправляет SNMP серверу такую информацию, как количество трафика на каждом интерфейсе, время работы устройства, количество входящих и исходящих TCP пакетов, и дату последнего обновления сетевых интерфейсов.

1. Выберите **Setup > SNMP**.



2. Выберите версию SNMP, которую вы хотите использовать: **v1/v2c** or **v3**. Если вы выберите **v1/v2c**, то в поле **Community String** введите community строку, которая будет использоваться для подключения к SNMP серверу. Если вы выберите **v3,** то вам необходимо ввести следующую информацию:

   User Name — имя пользователя для аутентификации SNMPv3.

   Authentication Protocol — протокол аутентификации (**MD5** (Message Digest 5) или **SHA** (Secure Hash Algorithm).

   Authentication Password — пароль аутентификации.

   Privacy Protocol — протокол шифрования (**DES** (Data Encryption Standard) или **None** для отключения шифрования SNMP трафика.

   Privacy Password — Пароль для шифрования исходящих сообщений и расшифрования входящих сообщений.

3. Нажмите **OK**. Для того чтобы Firebox мог получать SNMP опросы, вам необходимо добавить политику SNMP. Policy Manager автоматически попросит вас это сделать.

В диалоговом окне **New Policy Properties** выполните следующее:

1. В секции **From** нажмите **Add**
   Откроется диалоговое окно Add Address

2. Нажмите **Add Other**.
   Откроется диалоговое окно Add Member.

3. Из выпадающего списка **Choose Type** выберите **Host IP**.

4. В поле **Value** введите IP-адрес сервера SNMP.

5. Нажмите два раза **OK** для того чтобы закрыть диалоговые окна **Add Member** и **Add Address**.
   Для новой политики появится закладка Policy.

6. Под полем **To** нажмите **Add**.
   *Откроется диалоговое окно **Add Address**.*

7. В поле **Available Members** выберите **Firebox**. Нажмите **Add**.
   Firebox появится в поле Selected Members and Addresses.

8. Нажмите два раза **OK** для того чтобы закрыть диалоговые окна **Add Address** and **New Policy Properties**.

9. Нажмите **Close**.

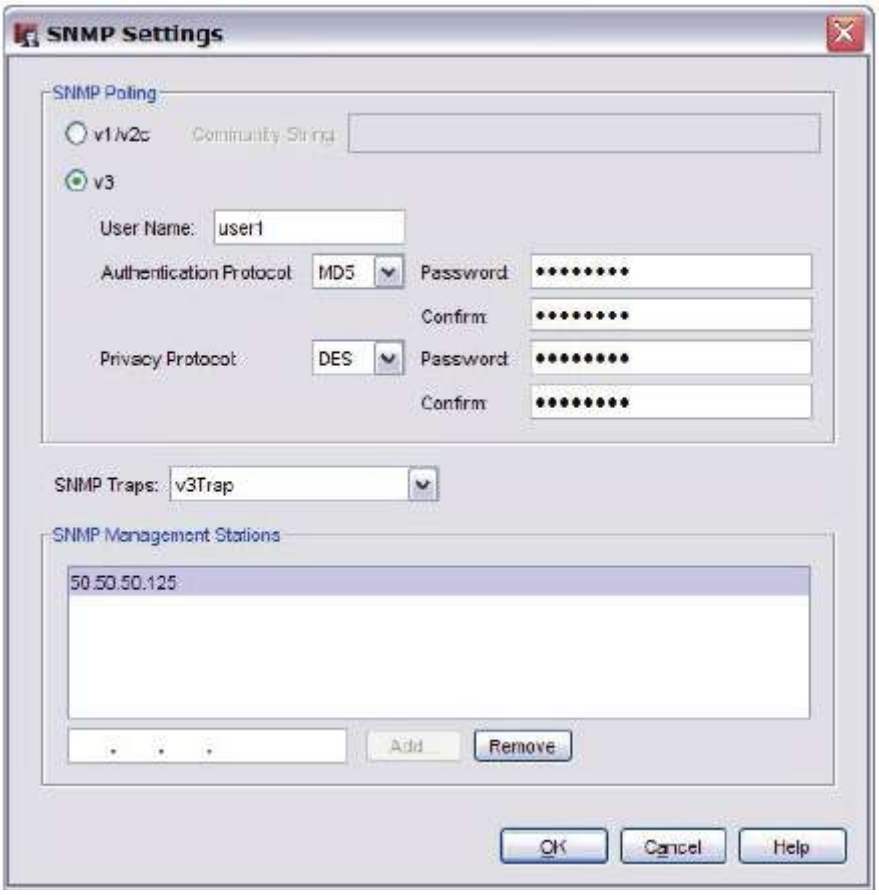
Включение станций управления SNMP и ловушек

SNMP ловушка – это специальный тип уведомления, которое ваше WatchGuard устройство отправляет SNMP серверу. Ловушка отправляется в случае наступления определенного события (например, значение какой-то величины превысило пороговое значение). Ваше WatchGuard устройство может отправлять ловушки для любых политик.

Информационный SNMP запрос похож на ловушку, но в отличие от нее на этот запрос получатель должен отправить ответ. Если ваше WatchGuard устройство не получает ответ, оно повторно отправляет информационный запрос и будет отправлять его до тех пор, как SNMP сервер не пришлет ответ. Ловушка отправляется только один раз, и получатель этой ловушки в ответ на нее не отправляет никакого ответа. Информационный запрос более надежен по сравнению с ловушкой, однако он более ресурсоемкий. Они хранятся в памяти до тех пор, пока не придет ответ на них. Повторная отправка информационных запросов увеличивает трафик в сети. Для того чтобы использовать информационные SNMP запросы вам необходимо использовать SNMPv2 or SNMPv3. SNMPv1 поддерживает только ловушки.

Настройка SNMP серверов

1. Выберите **Setup > SNMP**.
   Откроется диалоговое окно SNMP Settings.



2. В выпадающем списке **SNMP Traps** выберите версию ловушек или информационных запросов. SNMPv1 поддерживает только ловушки.

3. В текстовом поле SNMP Management Stations введите IP-адрес вашего SNMP сервера. Нажмите **Add**.
   Повторите п. 2-3 для того чтобы добавить еще несколько SNMP серверов.

4. Нажмите **OK**.

Добавление политики SNMP

Для того чтобы ваш Firebox мог получать SNMP запросы, вам необходимо создать политику SNMP.

1. Нажмите .
   Или выберите **Edit > Add Policy**.
   Откроется диалоговое окно Add Policies

2. Откройте **Packet Filters**, выберите **SNMP**, и нажмите **Add**.
   Откроется диалоговое окно New Policy Properties.

3. В секции **From** нажмите **Add**.
   Откроется диалоговое окно Add Address.

4. Нажмите **Add Other**.
   Откроется диалоговое окно Add Member.

5. Из выпадающего списка **Choose Type** выберите **Host IP**. В поле **Value** введите IP-адрес сервера SNMP.

6. Нажмите два раза **OK** для того чтобы закрыть диалоговые окна **Add Member** и **Add Address**.
   Для новой политики появится закладка Policy.

7. Под полем **To** нажмите **Add**. Откроется диалоговое окно **Add Address**.

8. В поле **Available Members** выберите **Firebox**. Нажмите **Add**.
   Firebox появится в поле Selected Members and Addresses.

9. Нажмите два раза **OK** для того чтобы закрыть диалоговые окна **Add Address** and **New Policy Properties**.

10. Сохраните конфигурацию.

Отправка SNMP ловушки для политики

Firebox может отправлять SNMP ловушку в случае если трафик был отфильтрован политикой. Для этого вам необходимо наличие хотя бы одного SNMP сервера.

1. Два раза нажмите на политику SNMP
   В диалоговом окне Edit Policy Properties выполните следующее.

2. Выберите закладку **Properties**.

3. Нажмите **Logging**.
   Откроется диалоговое окно Logging and Notification.

4. Включите опцию **Send SNMP Trap**.

5. Нажмите **OK** для того чтобы закрыть диалоговое окно **Logging and Notification**.

6. Нажмите **OK** для того чтобы закрыть диалоговое окно **Edit Policy Properties**.

MIB (Management Information Bases)

Fireware XTM поддерживает два типа MIB:

Standard MIB

Standard MIB содержат описания событий, которые происходят в сети и внутри оборудования, и которые используются многими устройствами. Ваше устройство WatchGuard поддерживает восемь Standard MIB:

- IP-MIB
- IF-MIB
- TCP-MIB
- UDP-MIB
- SNMPv2-MIB
- SNMPv2-SMI
- RFC1213-MIB
- RFC1155 SMI-MIB

Эти MIB содержат общую информацию о настройках сети (например, IP адреса и настройки сетевых интерфейсов).

Enterprise MIB

Enterprise MIB предоставляют информацию о событиях, характерных только для определенного оборудования.

Ваш Firebox поддерживает следующие Enterprise MIBs:

- WATCHGUARD-PRODUCTS-MIB
- WATCHGUARD-SYSTEM-CONFIG-MIB
- UCD-SNMP-MIB

Эти MIB включают более специфичную информацию об устройстве (загрузка CPU, время работы оборудования и др.).

При установке WatchGuard System Manager MIB устанавливаются в каталог:

\My Documents\My WatchGuard\Shared WatchGuard\SNMP

Пароли, Ключи Шифрования и Общие ключи (Shared Keys)

Пароли, ключи шифрования и общие ключи являются одним из компонентов вашей системы безопасности. В данном разделе приводится информации о паролях, ключах шифрования и общих ключах, которые используются для администрирования устройств WatchGuard.

Также в данном разделе вы сможете найти информацию об ограничениях, накладываемых на пароли, ключи шифрования и общие ключи.

Создание пароля, ключа шифрования или общего ключа

При создании безопасного пароля, ключа шифрования или общего ключа мы вам рекомендуем следовать следующим требованиям:

- Использовать комбинацию ASCII символов верхнего и нижнего регистра, числа и специальные символы (например, Im4e@tiN9).
- Не использовать слова из словарей, даже если вы записываете его наоборот или на другом языке.
- Не использовать имена.

В качестве дополнительной меры безопасности мы рекомендуем вам с определенной периодичностью менять пароли и ключи.

Пароли Firebox

Firebox использует два пароля:

Пароль состояния (Status passphrase)

Пароль только для чтения, который разрешает доступ к устройству Firebox. Если вы подключитесь к устройству Firebox с этим паролем, то вы сможете только просматривать конфигурацию, не имея возможности вносить какие-либо изменения. Пароль состояния привязан к имени пользователя *status*.

Пароль конфигурации (Configuration passphrase)

read-write пароль или парольная фраза, которые предоставляют администратору полный доступ к Firebox. Для того чтобы вносить изменения в конфигурацию и сохранять их вам необходимо для подключения к Firebox использовать этот пароль. Этот пароль также используется во время процедуры смены паролей. Пароль конфигурации привязан к пользователю *admin*.

Длина каждого пароля Firebox должна быть не меньше 8 символов.

Пользовательские пароли

Вы можете создавать имена пользователей и пароли, которые будут использоваться для аутентификации и администрирования на базе прав доступа.

Пользовательские пароли для Firebox аутентификации

После создания этого пароля, символы этого пароля будут скрыты и вы больше никогда не сможете его посмотреть в открытом виде. Если вы забыли или потеряли этот пароль, вам необходимо будет создавать новый пароль. Длина этого пароля 8–32 символов.

Пользовательские пароли для администрирования на базе ролей

После создания этого пароля, вы больше никогда не сможете его посмотреть в диалоговом окне **User and Group Properties**. Если пароль был утерян, вам необходимо создать новый. Длина пароля не менее 8 символов.

Серверные пароли

Пароль Администратора (Administrator passphrase)

Пароль Администратора используется для управления доступом к WatchGuard Server Center. Для того чтобы подключиться к Серверу Управления из WatchGuard System Manager (WSM) вам необходимо использовать этот пароль. Длина пароля должна быть не менее 8 символов. Пароль администратора привязан к пользователю *admin*.

Ключ сервера аутентификации

Специальный ключ, который используется Firebox и сервер аутентификации для защиты передаваемой между ними информации. Этот ключ зависит от регистра и должен быть одинаковым на Firebox и на сервере аутентификации. Серверы аутентификации RADIUS, SecurID и VASCO используют этот специальный ключ.

Ключи шифрования и общие ключи

Ключ шифрования Сервера Журналов

Ключ шифрования, который используется для создания защищенного соединения между Серверами Журналов и Firebox. Длина ключа шифрования - 8–32 символов. Вы можете использовать все символы, за исключением пробелов и косой черты (/ или \).

Ключ шифрования для резервирования и восстановления

Этот ключ шифрования используется для создания зашифрованной копии конфигурационного файла вашего Firebox. Для расшифрования конфигурационного файл вам необходимо тот же ключ, которым этот файл был зашифрован. В случае потери этого ключа вы не сможете восстановить информацию из зашифрованного файла. Длина этого ключа шифрования – 8-15 символов.

Ключ шифрования VPN

Ключ шифрования представляет собой пароль, который используется двумя устройствами для шифрования и расшифрования данных, передающихся по туннелю. Оба устройства должны использовать один и тот же пароль

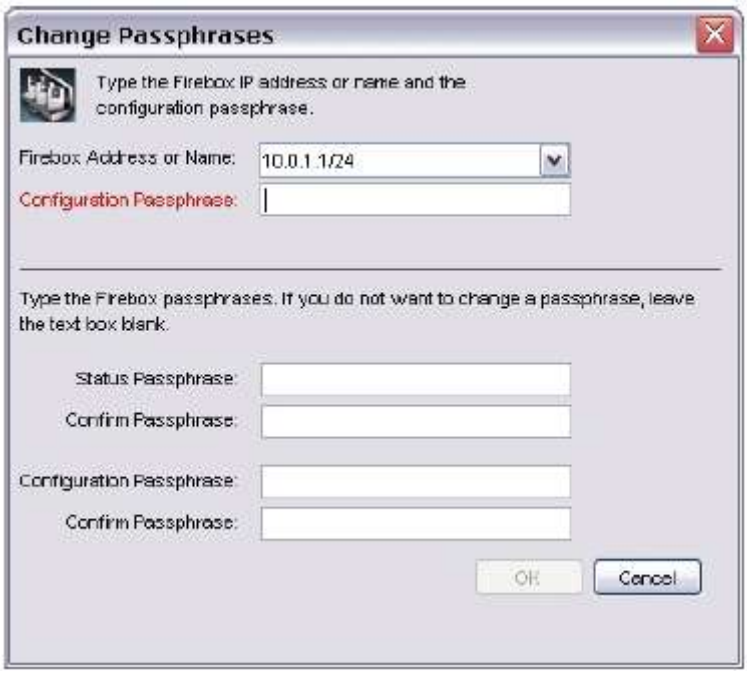
Смена паролей Firebox

A Firebox uses two passphrases:

- Пароль состояния. Пароль только для чтения, который разрешает доступ к устройству Firebox
- Пароль конфигурации – (read-write) пароль, который предоставляет полный доступ к Firebox

Для того чтобы сменить пароли выполните следующее:

1. Откройте конфигурационный файл Firebox.
2. Нажмите **File** > **Change Passphrases**.
   Откроется диалоговое окно Change Passphrases.



3. В выпадающем списке **Firebox Address or Name** выберите IP или имя устройства Firebox.
4. В текстовом поле **Configuration Passphrase** введите пароль конфигурации.
5. Введите и подтвердите пароль состояния (read-only) и пароль конфигурации (read/write). Пароль состояния должен отличаться от пароля конфигурации.
6. Нажмите **OK**.

Псевдонимы

Псевдоним – это ярлык, который идентифицирует группу хостов, сетей или интерфейсов. Если вы используете псевдоним, то вам будет легко создать политику безопасности, так как Firebox разрешает использование псевдонимов при создании политик. По умолчанию вы можете использовать следующие псевдонимы:

- **Any** - Псевдонимы, которые соответствуют интерфейсам Firebox(например *Trusted* или *External*.
- **Firebox** — псевдоним для всех интерфейсов Firebox.

- **Any-Trusted** — Псевдоним для всех интерфейсов Firebox, которые настроены как Trusted, и для любой сети, доступ к которым вы можете получить через эти интерфейсы.

- **Any-External** — Псевдоним для всех External интерфейсов устройства Firebox (как указано в Policy Manager: выберите **Network > Configuration**), и любой сети, доступ к которым вы можете получить через эти интерфейсы

- **Any-Optional** — Псевдоним для всех Optional интерфейсов устройства Firebox (как указано в Policy Manager: выберите **Network > Configuration**), и любой сети, доступ к которым вы можете получить через эти интерфейсы.

- **Any-BOVPN** — Псевдоним для любого BOVPN (IPSec) туннеля.

Если вы используете мастер BOVPN Policy для создания политики, которая разрешает трафик через BOVPN туннель, то мастер автоматически создает псевдонимы .in и .out для входящего и исходящего туннелей.

Имена псевдонимов отличаются от имен пользователей и групп пользователей, которые используются при аутентификации. При использовании аутентификации вы можете выполнять мониторинг подключения по имени, а не по IP-адресу. При аутентификации пользователь вводит имя пользователя и пароль. Для более подробной информации об аутентификации пользователя см. “Аутентификация пользователя”

Компоненты псевдонима

К псевдониму вы можете добавить следующие компоненты:

- IP-адрес хоста

- IP-адрес сети

- Диапазон IP-адресов хостов

- DNS имя для хоста

- Адрес туннеля: определяется пользователем или группой, адресом и именем туннеля

- Произвольный адрес: состоит из имени пользователя или группы, адреса и интерфейса Firebox

- Другой псевдоним

- Авторизованный пользователь или группа

Создание псевдонима

1. В Policy Manager выберите **Setup > Aliases**.
   Откроется диалоговое окно Aliases. Предварительно-настроенные псевдонимы отображаются синим цветм, а пользовательские псевдонимы отображаются черным.

2. Нажмите **Add**.
   Откроется диалоговое окно Add Alias.

3. В поле **Alias Name** введите уникальное имя, которое будет использоваться для идентификации псевдонима. *Это имя появляется в списках при настройке политики безопасности.*

4. В поле **Description** введите описание псевдонима

5. Нажмите **ОК**

Добавление к псевдониму адреса, диапазона адресов, DNS имени или другого псевдонима

1. В диалоговом окне **Add Alias** нажмите **Add**.
   Откроется диалоговое окно Add Member.

2. Из выпадающего списка выберите тип компонента, который вы хотите добавить

3. В поле **Value** введите адрес или имя.

4. Нажмите **OK**.
   Новый компонент появится в секции Alias Members диалогового окна Add Alias.

5. Если к псевдониму вы хотите добавить еще компонентов повторите п. 1–3. Для добавления пользователей или группы см. процедуру ниже.

6. После того, как вы добавите все необходимые компоненты, нажмите **OK**.

Добавление к псевдониму авторизованного пользователя или группы пользователей

1. Нажмите **User**.
   Откроется диалоговое окно Add Authorized Users or Groups.

2. Из выпадающего списка **Type** выберите тип добавляемого пользователя или группы: **Firewall user**, **PPTP user** или **SSL VPN user**.

3. Если вы хотите добавить пользователя, то в выпадающем списке **Type** выберите **User,** если группу – то **Group**.

4. Если пользователь или группа появляется в списке в нижней части диалогового окна **Add Authorized Users or Groups** выберите пользователя или группу и нажмите **Select**. Если пользователя или группы нет в списке, то это значит, что они еще не добавлены, как авторизованный пользователь или авторизованная группа. Перед тем как добавить пользователя или группу, вам необходимо настроить их как авторизованного пользователя или авторизованную группу.

5. Если вы хотите добавить дополнительные компоненты, повторите шаги 1–4. Или выполните предыдущую процедуру для добавления адреса, диапазона адресов, имя DNS или другой псевдоним.

6. Нажмите **OK**.

Для более подробной информации см.:

- Создание нового пользователя для аутентификации Firebox
- Создание новой группы для аутентификации Firebox
- Использование в политиках пользователей и групп

Для того чтобы удалить элемент из списка, выберите его и нажмите **Remove**.

Настройка глобальных параметров Firebox

В Policy Manager вы можете выбрать параметры, которые управляют работой различных компонентов Firebox. Вы можете настроить базовые параметры для:

- Обработки ICMP ошибок
- Проверки TCP SYN
- Максимальный размер TCP
- Управления трафиком и QoS

- Web UI порт

Для того чтобы изменить глобальные параметры выполните следующее:

1. Выберите **Setup** > **Global Settings**.
   Откроется диалоговое окно Global Settings.

2. Выполните настройку необходимых параметров, используя процедуры описанные ниже.\

Настройка глобальных параметров обработки ICMP ошибок

Протокол ICMP (Internet Control Message Protocol) управляет ошибками, которые происходят во время передачи данных по сети. Протокол используется для двух типов операций:

- Сообщений хостам клиентов об ошибке.

- Сканирования сети для поиска общих параметров сети.

Firebox отправляет ICMP сообщение каждый раз, когда происходит событие, которое соответствует указанным вами параметрам. Такие сообщения являются очень полезными при диагностике проблем работы сети, а также снижают уровень безопасности вашей сети, так как содержат информацию о конфигурации вашей сети. Если вы запретите ICMP сообщение, то вы увеличите уровень безопасности вашей сети, но при этом вы также создадите возможность для задержек сообщений о таймауте подключений, что может привести к проблемам в работе приложений.

Глобальные параметры обработки ошибок средствами ICMP:

Fragmentation Req (PMTU)

Включите эту опцию для того чтобы разрешить сообщения **ICMP Fragmentation Req**. Firebox использует эти сообщения для корректной передачи пакета данных

Time Exceeded

Включите эту опцию для того чтобы разрешить сообщения **ICMP Time Exceeded**. Маршрутизатор обычно отправляет эти сообщение, когда происходит зацикливание маршрута.

Network Unreachable

Включите эту опцию для того чтобы разрешить сообщения **ICMP Network Unreachable**. Маршрутизатор обычно отправляет это сообщение когда сетевое соединение не работает.

Host Unreachable

Включите эту опцию для того чтобы разрешить сообщения **ICMP Host Unreachable**. Ваша сеть обычно отправляет эти сообщения, когда она не может использовать хост или сервис

Port Unreachable

Включите эту опцию для того чтобы разрешить сообщения **ICMP Port Unreachable**. Хост или межсетевой экран обычно отправляют эти сообщения когда сетевой сервис недоступен или доступ к нему запрещен

Protocol Unreachable

Включите эту опцию для того чтобы разрешить сообщения **ICMP Protocol Unreachable**.

Вы можете изменить глобальные параметры ICMP для политики. Для этого выполните следующее:

1. В закладке Advanced диалогового окна **New/Edit Policy Properties** из выпадающего списка **ICMP Error Handling** выберите **Specify setting**.

2. Выберите **ICMP Setting**.

3. В диалоговом окне **ICMP Error Handling Settings** при помощи флагов укажите необходимые параметры.

4. Нажмите **OK**.

Включение TCP SYN checking

Процедура TCP SYN Checking проверяет было ли выполнена процедура TCP three-way handshake перед тем, как Firebox разрешит обмен данными.

Настройка глобальных параметров максимального размера TCP сегмента

Вы можете указать фиксированный размер сегмента TCP для соединения, которое использует дополнительные поля TCP/IP(например PPPoE, ESP, AH и т.д). Если этот размер будет некорректно настроен, пользователи не смогут получить доступ к некоторым сайтам.

Ниже приведены глобальные параметры максимального размера сегмента TCP:

Auto Adjustment

Firebox проверяет максимальный размер сегментов (MSS) и изменяет их размер на необходимую величину.

No Adjustment

Firebox не изменяет значение MSS.

Limit to

Вы устанавливает предел для изменения размера.

Включение и отключение Traffic Management и QoS

Для того чтобы отключить эти компоненты включите опцию **Disable all traffic management and QoS features**. Вы возможно захотите отключить эти компоненты при отладке сети или выполнении тестов на производительность.

Изменение порта Web UI

По умолчанию Fireware XTM Web UI использует порт 8080. Для того чтобы изменить порт Fireware XTM Web UI выполните следующее:

1. В текстовом поле **Web UI Port** введите или выберите другой номер порта.

2. Подключитесь к Web UI через новый порт.

Автоматическая перезагрузка

Некоторые компании используют плановые автоматические перезагрузки своих WatchGuard устройств

Для того чтобы настроить устройство для автоматической перезагрузки выполните следующее:

1. Включите опцию **Schedule time for daily reboot**.

2. В соответствующих текстовых полях введите время (в формате 24 часа) автоматическиой перезагрузки оборудования.

Опция External Console

Эта опция доступна только для устройств Edge. Включите опцию если вы хотите использовать последовательный порт для консольных подключений (например, Fireware XTM CLI). Если эта опция включена, то вы не можете использовать последовательный порт для переключения модемов. Для того чтобы изменить значение этой опции вам необходимо перезагрузить устройство.

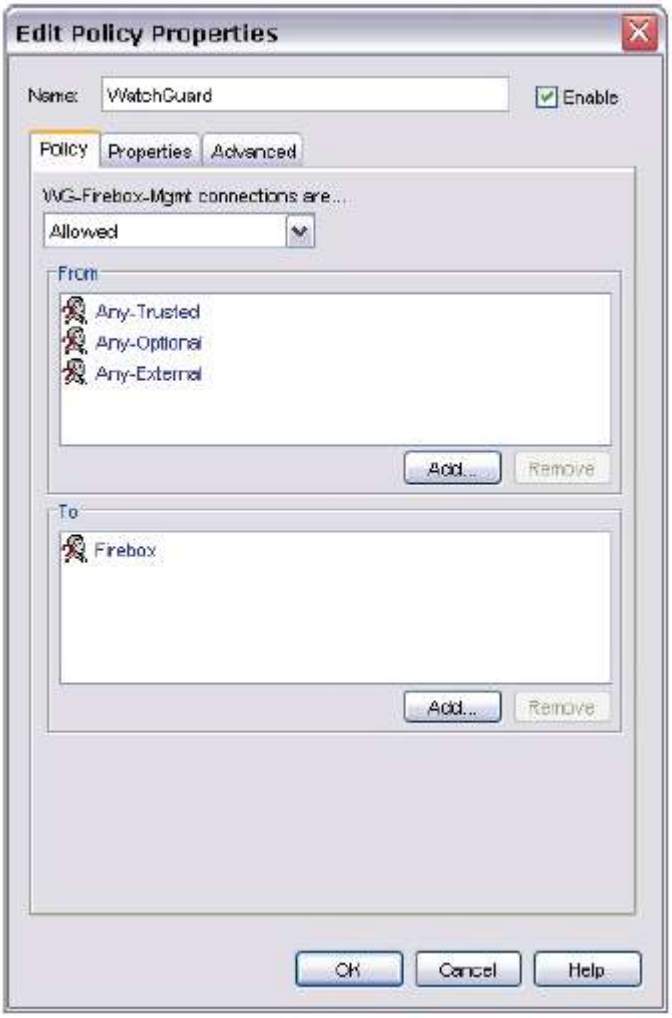
Удаленное управление Firebox

При настройке Firebox мастер Quick Setup Wizard автоматически создает политику с именем **WatchGuard**. Эта политика позволяет вам подключаться к устройству Firebox с любого компьютера, подключенного к Trusted или Optional сетям. Если вы хотите удаленно администрировать Firebox вам необходимо в политике WatchGuard разрешить административное подключение с вашего удаленного IP адреса.

Политика WatchGuard управляет доступом к Firebox по этим четырем портам: 4103, 4105, 4117, 4118. Если в политике WatchGuard вы разрешаете подключения, то вы разрешаете подключения по этим четырем портам.

Перед тем как вносить изменения в политику WatchGuard, мы рекомендуем создать подключение к Firebox по VPN, что обеспечит безопасность этого соединения. Если создать VPN не представляется возможным, то вам необходимо разрешить доступ к Firebox только определенным авторизованным пользователям и как можно меньшему количеству компьютеров. Например для того чтобы повысить безопасность системы, вы можете разрешить удаленный доступ к Firebox только одному компьютеру (вместо “Any-External”).

1. Два раза нажмите на политику **WatchGuard**. Или правой кнопкой нажмите на политику WatchGuard и выберите **Edit**.
   Откроется диалоговое окно Edit Policy Properties.



2. В секции **From** выберите **Add**.
   Откроется диалоговое окно Add Address.

3. Нажмите **Add Other**, выберите тип **Host IP** и введите IP адрес компьютера, с которого вы будете удаленно подключаться к Firebox.

4. Если вы хотите предоставить доступ авторизованному пользователю, в диалоговом окне **Add Address** нажмите **Add User**.
   Откроется диалоговое окно Add Authorized Users or Groups.

Для более подробной информации см. “Создание псевдонима”

Файлы WatchGuard System Manager

В приведенной ниже таблице представлены каталоги, в которых хранятся файлы WatchGuard System Manager. Так как вы можете поместить эти файлы в разные каталоги, вам необходимо знать, в каком каталоге они должны находиться. Вы можете хранить файлы журнала отдельно от остальных файлов установки

Если вы не используете неанглийскую версию ОС, то вам необходимо изменить имена каталогов на соответствующие имена каталогов вашей ОС (“Documents and Settings” или “Program Files”)

Тип файла	Каталог
Данные, созданные пользователем (общие)	C:\Documents and Settings\All Users\Shared WatchGuard
Сертификаты	My Documents\My WatchGuard\certs\<IP_Сервера_Управления>
Приложения WatchGuard	C:\Program Files\WatchGuard\wsm11.0

Общие библиотеки приложений	C:\Program Files\Common Files\WatchGuard\wsm11.0
Данные Сервера Управления	C:\Documents and Settings\WatchGuard\wmserver
Данные Сервера Карантина	C:\Documents and Settings\WatchGuard\wqserver
Данные Центра Сертификации (ЦС)	C:\Documents and Settings\WatchGuard\wgca
Данные Сервера Отчетов	C:\Documents and Settings\WatchGuard\wrserver
Данные Сервера Журналов	C:\Documents and Settings\WatchGuard\wlogserver
Данные Сервера WebBlocker	C:\Documents and Settings\WatchGuard\wbserver
Образы будущих обновлений продукта	C:\Program Files\Common Files\WatchGuard\resources\FirewareXTM\11.0
Справочные файлы (Fireware & WSM)	C:\Program Files\WatchGuard\wsm11.0\help\fireware
Справочные файлы (WFS)	C:\Program Files\WatchGuard\wsm11.0\help\wfs

Файлы приложений и пользовательские файлы

В приведенных ниже таблицах приводится информация о каталогах, в которых хранятся файлы приложений WatchGuard и пользовательские файлы (например, конфигурационные файлы Firebox). В случае если приложение открыло похожий файл в другом каталоге, то оно запоминает этот каталог и при следующей попытке открыть файл приложение ищет этот файл в каталоге, в котором этот файл был последний раз открыт.

Policy Manager для Fireware

Операция	Тип файла	Каталог по умолчанию
Чтение/запись	Резервные копии Firebox	C:\Documents and Settings\All Users\Shared WatchGuard\backups
Чтение	Образы обновлений продукта	C:\Program Files\Common es\WatchGuard\resources\FirewareXTM\11.0
Чтение	Список Blocked Sites	My Documents\My WatchGuard
Чтение	Исключения списка Blocked Sites	My Documents\My WatchGuard

Чтение/запись	Конфигурационные файлы Firebox	My Documents\My WatchGuard/configs
Чтение/запись	Файлы лицензий Firebox	My Documents\My WatchGuard/configs
Чтение	Файл импорта воначальной лицензии	My Documents\My WatchGuard
Запись	Конфигурационные лы программы клиента obile VPN (*.wgx и *.ini)	C:\Documents and Settings\All Users\Shared WatchGuard\muvpn

WFS

Операция	Тип файла	Каталог по умолчанию
Чтение	Журналы с уведомлениями	Текущий рабочий каталог
Чтение	Импорт правил спама	Текущий рабочий каталог
Запись	Сохраненные резервные копии	C:\Documents and Settings\All Users\Shared WatchGuard\backups
Запись	MUVPN SPDs (.wgx)	C:\Documents and Settings\All Users\Shared WatchGuard\muvpn
Чтение	Импорт Blocked Sites	Текущий рабочий каталог
Чтение/Запись	Резервная копия образа	C:\Documents and Settings\All Users\Shared WatchGuard\ backups

Report Manager

Тип файла	Каталог по умолчанию
Журнал отчетов	C:\Documents and Settings\<user name>\Application Data\WatchGuard\wgreports
Файлы отчетов	C:\Documents and Settings\<user name>\Application Data\WatchGuard\wgreports

LogViewer

Тип файла	Каталог по умолчанию
Файлы конфигурации LogViewer	C:\Documents and Settings\<user name>\Application Data\WatchGuard\enhanced_logviewer
Файлы журнала отладки LogViewer	C:\Documents and Settings\<user name>\Application Data\WatchGuard\enhanced_logviewer
Экспортированные файлы LogViewer	C:\Documents and Settings\WatchGuard\logs
Сохраненные файлы журнала LogViewer	C:\Documents and Settings\WatchGuard\reports
Файлы поисковых запросов LogViewer	C:\Documents and Settings\<user name>\Application Data\WatchGuard\enhanced_logviewer\searches

Обновление Fireware XTM

Периодически компания WatchGuard выпускает новые версии WatchGuard System Manager (WSM) и Fireware XTM, которые доступны пользователям Firebox с активной подпиской LiveSecurity. Для того чтобы обновить версию WSM с Fireware XTM см. следующие разделы этой главы.

Установите обновление на вашу станцию управления

1. Загрузите новое обновление Fireware XTM и WatchGuard System Manager с сайта http://www.watchguard.com.

2. Создайте резервные копии вашего текущего конфигурационного файла и файлов конфигурации Сервера Управления. Для более подробной информации см. “Резервные копии образов flash-дисков Firebox”

   Для более подробной информации о создании резервной копии настроек вашего Сервера Управления см. “Создание резервной копии или восстановление конфигурации Сервера Управления”

3. При Windows Add or Remove Programs удалите все существующие версии WatchGuard System Manager и WatchGuard Fireware XTM. Вы можете иметь несколько установленных версий клиентского ПО и только одну версию серверного ПО. Для более подробной информации см. “Дополнительно”

4. Запустите файл установки, который вы загрузили с сайта LiveSecurity.

5. Выполните все необходимые инструкции мастера для установки файла обновления Fireware XTM в ваш каталог установки WatchGuard.

Обновление Firebox

1. Для того чтобы сохранить обновление на Firebox, откройте конфигурационный файл при помощи Policy Manager.

   WatchGuard System Manager автоматически определит, что это конфигурационный файл для более старой версии, и открывает диалоговое окно обновления.

2. Нажмите **Yes** для того чтобы обновить конфигурационный файл. Выполните все необходимые инструкции мастера.

Диалоговое окно обновления для разных версий выглядит по разному

Если при открытии Policy Manager вы не увидите диалогового окна обновления, то выполните следующее:

1. Выберите **File** > **Upgrade**.

2. Введите пароль конфигурации.
Откроется диалоговое окно Upgrade — Enter the path to the upgrade image

3. Автоматически выбирается каталог по умолчанию. Если вы установили обновление в другой каталог, то нажмите **Browse** и выберите необходимый каталог.

4. Нажмите **OK**.

Процедура обновления займет примерно минут 15 и затем устройство WatchGuard будет автоматически перезагружено. Если ваше WatchGuard устройство до установки обновления работало в течение определенного периода времени, то вам необходимо будет до установки обновления его перезагрузить для того чтобы очистить временную память.

Использование нескольких версий Policy Manager

В WatchGuard System Manager v11 если вы откроете конфигурационный файл, созданный более ранней версией Policy Manager, и если более ранняя версия WatchGuard System Manager также установлена на вашем компьютере, то откроется диалоговое окно **Upgrade Available**. Вы можете запустить более раннюю версию Policy или обновить конфигурационный файл для работы с новой версией. Если вы не хотите чтобы WatchGuard System Manager открывал это диалоговое окно в следующий раз, когда вы откроете конфигурационный файл более ранней версии, выберите опцию **Do not show this message again**.

Для того чтобы снова включить отображение диалогового окна **Upgrade Available** выполните следующее:

1. В WatchGuard System Manager выберите **Edit > Options**.
Откроется диалоговое окно Options.

2. Включите опцию **Show upgrade dialog when launching Policy Manager**.

3. Нажмите **OK**.

Опции обновления

Вы можете устанавливать обновления на ваше устройство WatchGuard для того чтобы включить дополнительные сервисы подписки, компоненты и получить дополнительную емкость.

Список доступных опций обновлений см. здесь: www.watchguard.com/products/options.asp.

Обновления сервисов безопасности

WebBlocker

Обновление WebBlocker позволяет вам управлять доступом к web содержимому

spamBlocker

spamBlocker используется для фильтрации спама и bulk почты

Gateway AV/IPS

Gateway AV/IPS используется для защиты от вирусов и обнаружения несанкционированных проникновений в сеть

Обновления ПО

Pro

Обновление Pro позволяет вам использовать некоторые дополнительные компоненты Fireware XTM для опытных клиентов – балансировка нагрузки на сервер и дополнительные SSL VPN туннели. Список компонентов, доступных с обновлением Pro, зависят от типа и модели вашего Firebox

Обновление модели устройства

Для некоторых моделей Firebox вы можете приобрести лицензионный ключ, который позволит вам обновить ваше устройство до более новой модели, что позволит использовать функционал, реализованный в этой новой модели устройства. Для более подробной информации о возможностях различных моделей устройства Firebox см.

http://www.watchguard.com/products/compare.asp.

Как установить обновление

После того, как вы приобрели необходимое обновление, вам необходимо зарегистрировать его на сайте WatchGuard LiveSecurity. Затем вам необходимо загрузить лицензионный ключ, который позволит установить обновление на ваше устройство WatchGuard. Для более подробной информации о ключах см.”Ключи функций (Feature Keys)”

Обновление сервисов безопасности

Для эффективной работы сервисов безопасности WatchGuard (Gateway AntiVirus, Intrusion Prevention Service, WebBlocker и spamBlocker) их необходимо регулярно обновлять.

Устройство WatchGuard создает специальные уведомления о том, что сервис безопасности необходимо обновить. Когда вы сохраняете изменения в конфигурационный файл, WatchGuard System Manager сообщает вам о том, сколько осталось дней до истечения срока действия обновления. Если срок действия ваших сервисов истек вы не сможете сохранять изменения в конфигурационный файл до тех пор, пока не обновите сервисы безопасности или совсем их не отключите.

1. В Policy Manager выберите **File > Save > To Firebox**.
   Вы увидите сообщение об необходимости обновления лицензионного ключа.

2. Нажмите **OK**.
   Откроется диалоговое окно Feature Key Compliance

3. Выберите подписку с истекшим сроком действия.

4. Если у вас уже есть новый лицензионный ключ, то нажмите **Add Feature Key**. Вставьте содержимое вашего ключа в соответствующее текстовое поле (CTRL-V или нажмите **Paste**). Если у вас нет лицензионного ключа, нажмите **Disable** даже если вы планируете обновить позже. Если вы отключите подписку, вы не потеряете все ваши настройки. Если вы потом обновите вашу подписку, то вы можете заново активировать ваши настройки и сохранить на Firebox.

5. Нажмите **OK**.

Обновление подписок из Firebox System Manager

Если срок действия вашей подписки подходит к концу, то на передней панели Firebox System Manager появится предупреждение и кнопка **Renew Now** в верхнем правом углу окна Нажмите кнопку **Renew Now** для того чтобы обновить вашу подписку на сайте LiveSecurity Service

Глава 6 - Настройка сети

Настройка сетевого интерфейса

Основным компонентом настройки WatchGuard Firebox является настройка IP адресов интерфейсов. При работе с мастером Quick Setup Wizard вы выполняете настройку интерфейсов External и Trusted чтобы по ним мог передаваться трафик.

В разделах этой главы приводится описание процедуры изменения конфигурации интерфейсов после того, как вы завершили работу с мастером, или добавления других компонентов сети к вашей конфигурации.

Например, вы можете настроить интерфейс Optional для публичных серверов, например web-сервера. Межсетевой экран физически отделяет сети в вашей LAN от сетей в WAN.

Для передачи трафика из защищенной сети во внешние сети ваш Firebox использует маршрутизацию. Для того чтобы маршрутизировать трафик из одной сети в другую вашему устройству необходимо знать, какие сети подключены к его интерфейсам.

Поэтому мы рекомендуем вам записать всю информацию о настройках вашей сети и VPN. Эта информация понадобится нашей службе технической поддержки для оперативного решения возникших проблем

Режимы сети

Ваше устройство WatchGuard поддерживает несколько режимов сети:

Mixed routing mode (Смешанный режим маршрутизации)

В этом режиме вы можете настроить ваш Firebox для передачи трафика в различные логические и физические сети. Этот режим используется по умолчанию и предоставляет наибольшую гибкость для различных конфигураций сети. Однако вам необходимо отдельно настроить каждый интерфейс. А также вам возможно придется менять сетевые настройки для каждого компьютера, подключенного к защищенной сети. Для передачи информации между интерфейсами Firebox использует NAT (Network Address Translation)

Основные требования для режима смешанной маршрутизации:

- IP-адреса всех интерфейсов устройства WatchGuard должны лежать в разных подсетях. Минимальная конфигурация включает в себя Trusted и External интерфейсы. Вы также можете настроить один или несколько Optional интерфейсов.

- Все компьютеры, подключенные к интерфейсам, должны иметь IP-адреса из соответствующей подсети.

Режим Drop-in

В этом режиме интерфейсы устройства WatchGuard имеют один и тот же IP адреса. Вы можете поместить ваше устройство между маршрутизатором и LAN, при этом вам не надо будет изменять сетевые настройки компьютеров, подключенных к LAN. Этот режим называется *drop-in* потому что ваше устройство подключается прямо в существующую сеть. Некоторые сетевые компоненты, как мосты и VLAN (Virtual Local Area Networks) в этом режиме недоступны.

Для реализации конфигурации drop-in вам необходимо выполнить следующее:

- Устройству WatchGuard присвоить статический внешний IP адрес.

- Использовать одну логическую сеть для всех интерфейсов.
- Не использовать multi-WAN в режимах Round-robin или Failover.

Для более подробной информации см. “Конфигурация сети в режиме drop-in”

Режим моста (Bridge mode)

Режим моста позволяет вам подключать ваше WatchGuard устройство между существующей сетью и ее шлюзом для того чтобы обеспечить фильтрацию сетевого трафика. Если вы включите этот режим то устройство WatchGuard будет обрабатывать трафик и направлять его на указанный IP адреса шлюза. На шлюзе трафик обрабатывается так, как будто он был послан с первоначального источника. В этом режиме ваше WatchGuard устройство не сможет определенный функционал, для которого необходим публичный и уникальный IP адрес. Например вы не можете использовать устройство в режиме моста в качестве конечной точки VPN (Virtual Private Network).

Для более подробной информации см. About network configuration in bridge mode.

Типы интерфейсов

Для настройки вашей сети в режимах смешанной маршрутизации или drop-in вы можете использовать следующие типы интерфейсов:

External интерфейсы

Внешний интерфейс, который используется для подключения вашего WatchGuard устройства в нешней сети. Часто через этот интерфейс устройство Firebox подключается к сети Интернет. Вы можете настроить до 4 физических External интерфейсов. При настройке external интерфейса вам необходимо будет выбрать, какой IP-адрес будет присвоен вашему интерфейсу. Для более подробной информации обратитесь к вашему ISP или системному администратору.

Trusted интерфейсы

Trusted интерфейсы используются для подключения частных LAN (local area network) или внутренних сетей вашей организации. Trusted интерфейс используется для предоставления вашим сотрудниками доступа в Интернет и защиты вашей внутренней сети.

Optional интерфейсы

Интерфейсы Optional – это сети со смешанным доверия или DMZ, которые отделены от вашей сети Trusted. Примером компьютеров, которые можно подключить к интерфейсам Optional, являются публичные web-серверы, FTP серверы и серверы электронной почты. Для более подробной информации о настройке интерфейсов Optional см. “Общие настройки интерфейса”.

Вы можете добавить к вашей сети дополнительные компоненты: При настройке интерфейсов Firebox для обозначения маски подсети вам необходимо использовать slash-нотацию. Например если у нас адрес сети 192.168.0.0 и маска подсети 255.255.255.0, то, используя slash-нотацию, вы можете записать - 192.168.0.0/24.

Интерфейс с IP адресом 10.0.1.1/16 имеет маску подсети 255.255.0.0.

Режим смешанной маршрутизации (Mixed Routing Mode)

В этом режиме вы можете настроить ваш Firebox для передачи трафика между различными физическими и логическими сетями. Этот режим используется по умолчанию. Несмотря на то, что большинство сетевых компонентов, а также компонентов безопасности, доступны в этом режиме, вам необходимо для обеспечения корректной работы сети аккуратно проверить конфигурации каждого устройства, подключенного к вашему Firebox.

Базовая конфигурация сети в режиме смешанной маршрутизации включает по крайней мере два интерфейса. Например, вы можете подключить External интерфейс к кабельному модему, а Trusted интерфейс к внутреннему роутеру, к которому подключены сотрудники вашей компании. В этой базовой конфигурации вы можете добавить Optional сеть, которая защищает ваши серверы, но предоставляет более полный доступ с внешних сетей, настроить VLAN и другой дополнительный функционал, или создать определенные ограничения, например ограничения MAC адресов. Вы также можете определить, каким образом трафик будет передаваться между интерфейсами.

Перед тем, как начать настройку интерфейсов в режиме смешанной маршрутизации, см. “Общие настройки интерфейса”

При использовании сети в режиме смешанной маршрутизации довольно легко забыть IP адреса и точки подключений в сети, особенно если вы используете VLAN (Virtual Local Area Networks), вторичные сети и другой дополнительный функционал. Поэтому мы рекомендуем вам записать всю информацию о настройках вашей сети и VPN. Эта информация понадобится нашей службе технической поддержки для оперативного решения возникших проблем

Настройка External интерфейса

External интерфейс используется для подключения вашего WatchGuard устройства к внешней сети. Часто через этот интерфейс устройство Firebox подключается к сети Интернет. Вы можете настроить до 4 физических External интерфейсов. При настройке external интерфейса вам необходимо будет выбрать, какой IP-адрес будет присвоен вашему интерфейсу. Для более подробной информации обратитесь к вашему ISP или системному администратору.

Статический IP адрес

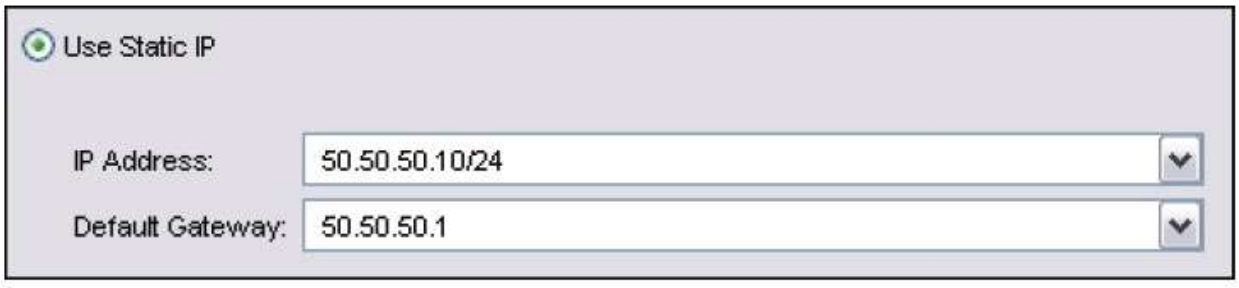
1. Выберите **Network > Configuration**.
   Откроется диалоговое окно Network Configuration.

2. Выберите интерфейс External. Нажмите **Configure**.

3. В диалоговом окне **Interface Settings** выберите **Static**.

4. В поле **IP address в**ведите IP адрес интерфейса.

5. В поле **Default Gateway** введите IP адрес шлюза по умолчанию



6. Нажмите **OK**.

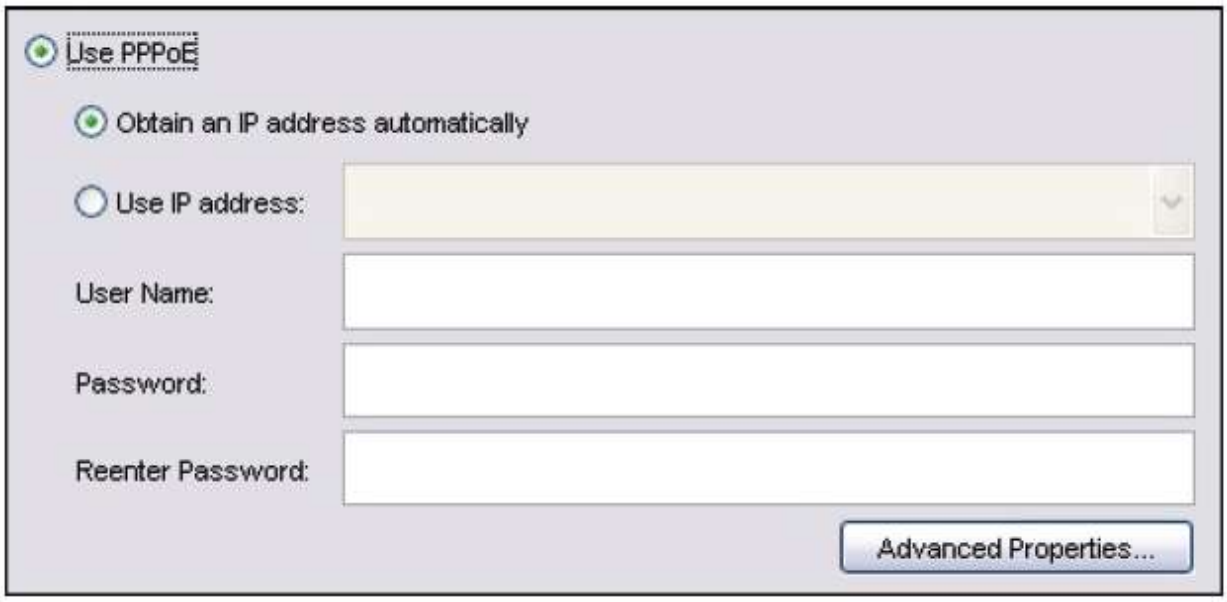
PPPoE аутентификация

Если ваш Интернет-провайдер использует PPPoE, то перед тем как передавать трафик через External интерфейс, вам необходимо для Firebox ввести параметры PPPoE.

1. Выберите **Network** > **Configuration**.
   Откроется диалогое окно Network Configuration.

2. Выберите External интерфейс. Нажмите **Configure**.

3. В диалоговом окне **Interface Settings** выберите **Use PPPoE**



4. Выберите необходимую опцию:

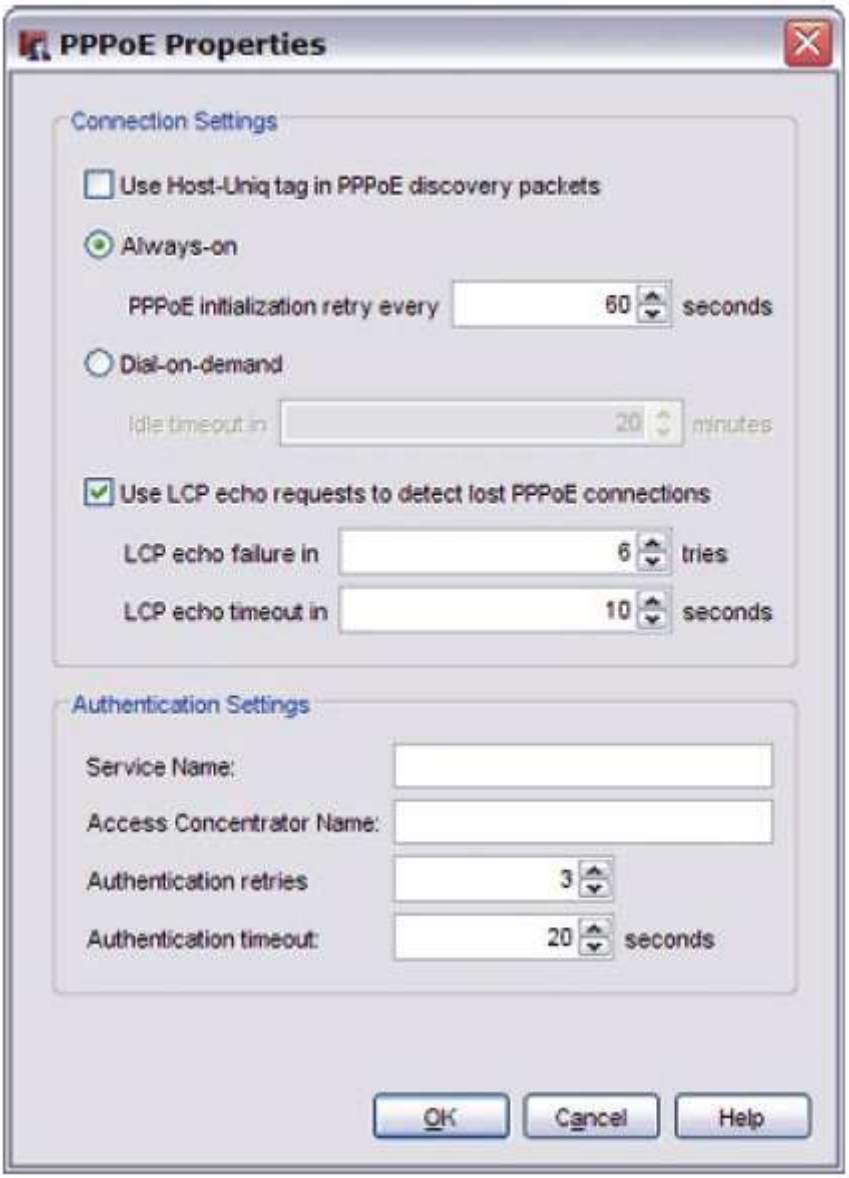
   * **Obtain an IP address automatically**

   * **Use IP address** (информация, предоставленная вашим ISP)

5. Если вы выберете **Use IP Address** в соответствующем поле введите IP-адрес.

6. В текстовых полях **User Name** и **Password** введите имя пользователя и пароль соответственно. Пароль вам необходимо будет ввести два раза.
   Для имен пользователей ISP используют формат электронной почты: user@example.com.

7. Выберите **Advanced Properties** для настройки PPPoE.
Откроется диалогое окно PPPoE Properties. Ваш ISP также сообщит вам о необходимости изменить значения таймаута или LCP



8. Включите опцию **Use Host-Uniq tag in PPPoE discovery packets** если вашему ISP необходимо тэг Host-Uniq для обнаружения пакетов PPPoE.

9. Выберите режим подключения Firebox к PPPoE серверу:

   * **Always-on** — Firebox постоянно подключен к PPPoE серверу. Сетевой трафик необязательно передавать через External интерфейс. Если вы включите эту опцию, то вам необходимо будет в **PPPoE Initialization Retry Interval** ввести время в секундах, в течение которого PPPoE пытается инициализировать перед тем как сгенерирует таймаут.

   * **Dial-on-Demand** —Firebox подключается к серверу PPPoE только при получении запроса передачи трафика через External интерфейс. Если ваш ISP с определенной периодичностью разрывает, а затем восстанавливает соединения, то включите эту опцию. В поле **Idle Timeout** введите промежуток времени, в течение которого клиент может оставаться подключенным даже при отсутствии трафика. Если вы не включите опцию, то при каждом разрыве и восстановлении соединений, вам необходимо будет вручную перезагрузить.

10. В поле **LCP echo failure in** выберите количество неудачных LCP echo запросов, после которого PPPoE соединение будет считаться неактивным и будет закрыто.

11. В поле **LCP echo timeout in** выберите промежуток времени (в секундах), по истечение которого запрос для каждого таймаута

12. В поле **Service Name** введите имя сервиса PPPoE. Это либо имя ISP или класс сервиса, настроенный на сервере PPPoE. Обычно эта опция не используется. Используйте эту опцию только если у несколько концентраторов доступа или вы знаете, что вам необходимо использовать определенное имя сервиса.

13. В поле **Access Concentrator Name** введите имя концентратора доступа PPPoE, также известного как PPPoE сервер. Используйте эту опцию только в том случае, если у вас есть несколько концентраторов.

14. В поле **Authentication retries** выберите количество попыток соединения.
По умолчанию количество попыток равняется 3.

15. В поле **Authentication timeout** введите время между попытками подключения.
По умолчанию - 20 секунд.

16. Нажмите **OK**.

17. Сохраните вашу конфигурацию.

Использование DHCP

1. В диалоговом окне **Interface Settings** выберите **Use DHCP Client**

2. Если ваш ISP или внешний DHCP сервер требует идентификатор клиента (MAC-адрес например), то в поле **Client** введите значение этого идентификатора.

3. Для того чтобы для идентификации использовать имя хоста, в поле **Host Name** введите имя хоста

4. Для того чтобы включить получение IP-адреса для Firebox через DHCP, в секции **Host IP** выберите опцию **Obtain an IP automatically**. Для того чтобы ввести IP-адрес и использовать DHCP для формальной выдачи этого адреса устройству Firebox выберите опцию **Use IP address** и введите IP адрес в соответствующее поле. По умолчанию IP адреса, выданные DHCP сервером действуют в течение одного дня.

5. Для того чтобы изменить время действия выданного IP адреса, включите опцию **Leasing Time** и в соответствующем выпадающем списке выберите необходимое значение.

Настройка DHCP в режиме смешанной маршрутизации

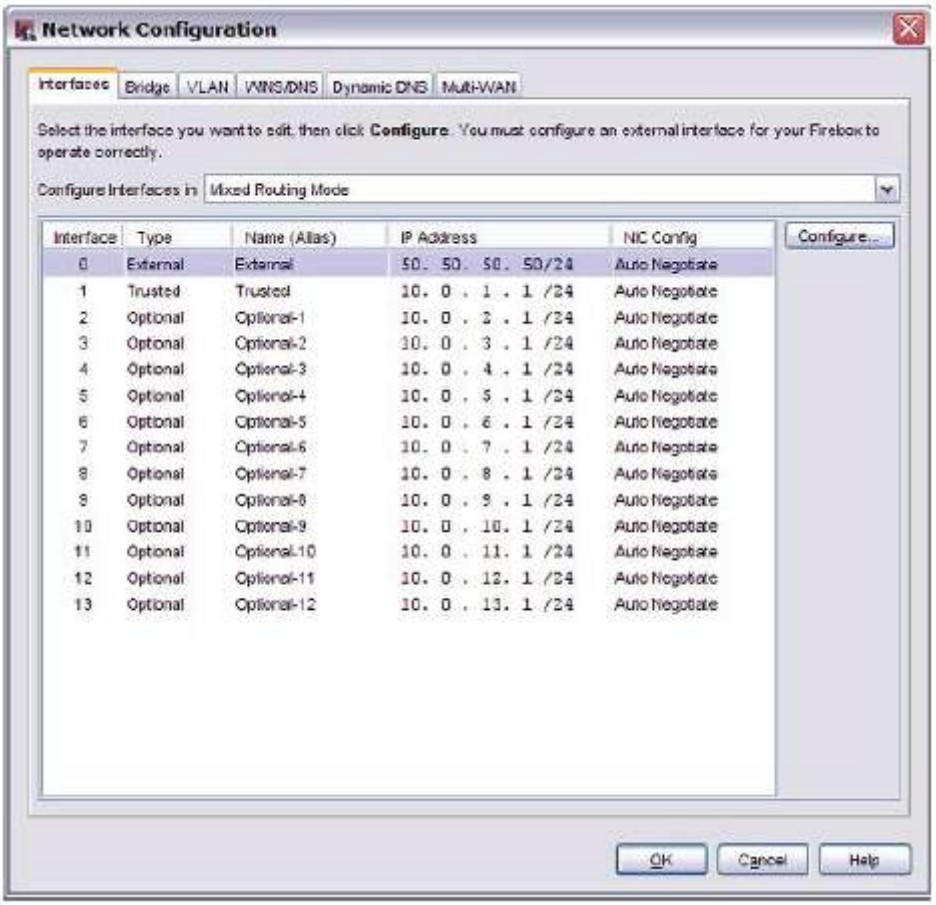
DHCP (Dynamic Host Configuration Protocol) – протокол, который используется для автоматического присвоения IP адресов устройствам сети. Вы можете настроить на вашем WatchGuard устройстве DHCP сервер, который будет использоваться для защищенных сетей. Если у вас есть DHCP сервер, мы рекомендуем вам продолжать использовать этот сервер. Если ваше устройство WatchGuard в режиме drop-in то см. “Настройка DHCP в режиме drop-in”

Вы не можете настроить DHCP на интерфейсах, для которых включен FireCluster.

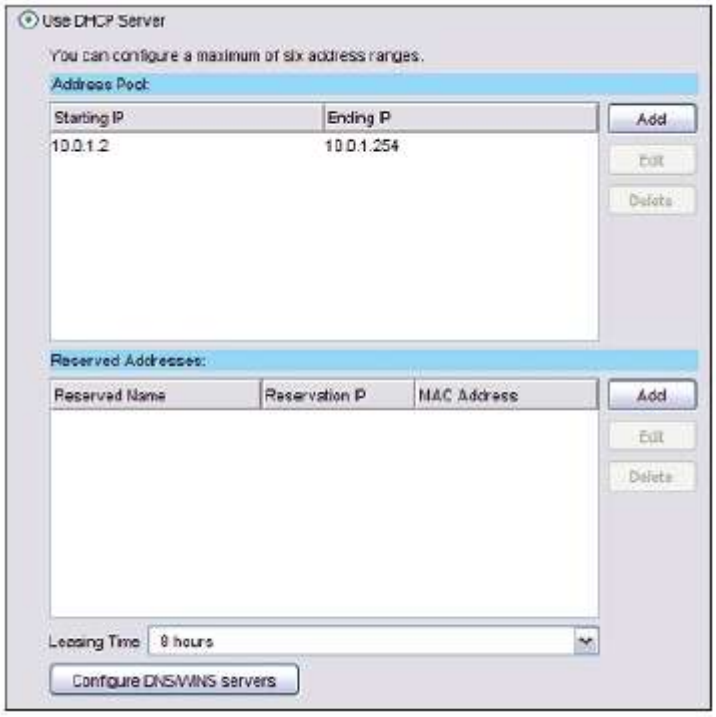
Настройка DHCP

1. Выберите **Network** > **Configuration**.

2. Выберите Trusted или Optional интерфейсы. Нажмите **Configure**. Для того чтобы настроить DHCP сервер для гостевой беспроводной сети выберите **Network > Wireless** и нажмите **Configure** для гостевой беспроводной сети



3. Включите опцию **Use DHCP Server**. Для гостевой беспроводной сети включите опцию **Enable DHCP Server on Wireless Guest Network**



4. Для того чтобы добавить диапазон IP-адресов, которые будут присваиваться пользователям, подключенным к этому интерфейсу, в разделе **Address Pool** нажмите **Add**. Укажите начальный и конечный адрес диапазона, и затем нажмите **OK**. Диапазон адресов должен принадлежать основной или вторичной IP подсети интерфейса.

   Вы можете настроить до 6 диапазонов адресов. Диапазоны адресов используются в порядке от первой к последней. Адресам в диапазонах присваиваются номера.

5. Для того чтобы изменить величину срока действия IP адреса, выданного DHCP сервером, в выпадающем списке **Leasing Time** выберите необходимую величину.

   Это промежуток времени, в течение которого DHCP клиент может использовать IP адрес, полученный от DHCP сервера. Когда срок действия адреса подходит к концу, клиент отправляет DHCP серверу запрос на продление срока действия IP-адреса.

6. По умолчанию если ваше WatchGuard устройство настроено как DHCP сервер, то, помимо IP адресов, оно передает клиенту информацию о DNS и WINS серверах (**Network Configuration > WINS/DNS)**. Для того чтобы указать, какую информацию ваш DCHP сервер будет передавать клиентам нажмите **Configure DNS/WINS servers**.

   * В поле **Domain Name** введите имя домена.

   * Для того чтобы добавить DNS или WINS сервер нажмите на кнопку **Add,** введите IP адрес и нажмите **OK**.

   * Для того чтобы изменить IP адрес выбранного сервера нажмите на кнопку **Edit**.

   * Для того чтобы удалить выбранный сервер из списка нажмите на кнопку **Delete**.

Настройка DHCP резерваций

Для того чтобы зарезервировать определенный IP-адрес для клиента выполните следующее:

1. Нажмите **Add** рядом с полем **Reserved Addresses**. Для гостевой беспроводной сети нажмите **DHCP Reservations** и затем нажмите **Add**.

2. Введите имя резервации, IP адрес, который вы хотите зарезервировать и MAC-адрес сетевой карты клиента

3. Нажмите **OK**.

Динамический DNS

Вы можете зарегистрировать внешний IP-адрес вашего Firebox® при помощи сервиса динамического DNS.

Динамический DNS гарантирует вам, что при выдаче вам Интернет-провайдером нового IP-адреса, IP-адрес, прикрепленный к вашему доменному имени, тоже изменится. Этот функционал доступен как в режиме смешанной маршрутизации, так и в режиме drop-in.

Firebox при запуске получает IP адрес сервера members.dyndns.org. Он гарантирует, что при каждой перезагрузке и в течение 20 дней IP-адрес будет корректным. Если вы измените конфигурацию DynDNS вашего Firebox или если вы измените IP-адрес шлюза по умолчанию, настроенного на Firebox, то при этом произойдет мгновенное обновление DynDNS.com. Для более подробной информации о динамическом DNS, см. http://www.dyndns.com.

Использование динамического DNS

Вы можете зарегистрировать внешний IP адрес вашего WatchGuard устройства при помощи специального сервиса - Dynamic Network Services (DynDNS). Максимум для пяти имен хостов этот сервис бесплатный. WatchGuard System Manager на данный момент не поддерживает других провайдеров динамического DNS.

Сервис динамического DNS гарантирует, что в случае если ваш ISP выдает вам новый IP адрес, IP-адрес привязанный к имени домена тоже изменится. Ваше устройство проверяет IP адрес members.dyndns.org при запуске. Ваше WatchGuard гарантирует корректность IP адреса при каждой перезагрузке или в течение каждых дней. Если вы внесете какие-либо изменения в конфигурацию DynDNS, или если вы измените IP адрес шлюза по умолчанию, то ваша конфигурация на DynDNS.com тут же обновится.

Для более подробной информации см. http://www.dyndns.com.

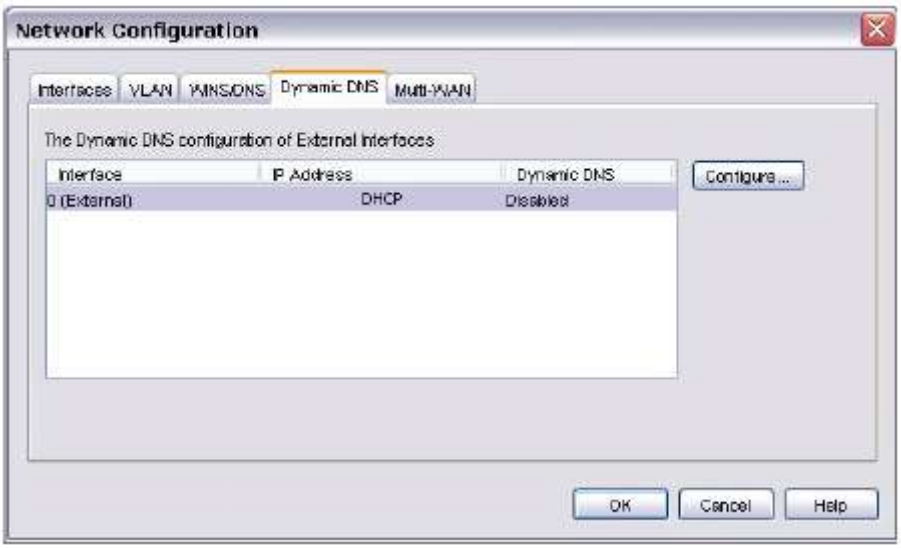
1. Создайте учетную запись dynDNS. Для этого зайдите на сайт DynDNS и выполните все необходимые инструкции.

2. В Policy Manager выберите **Network > Configuration**.

3. Выберите закладку **WIN/DNS**.

4. Убедитесь, что вы ввели хотя бы один DNS сервер.

5. Выберите закладку **Dynamic DNS**



6. Выберите External интерфейс, для которого вы хотите настроить динамический DNS и нажмите **Configure**.
   Откроется диалогое окно Per Interface Dynamic DNS.

7. Для того чтобы включить динамический DNS включите опцию **Enable Dynamic DNS**.

8. Введите имя пользователя, пароль и имя домена, которые вы использовали при создании учетной записи dynDNS.

9. В выпадающем списке **Service Type** выберите систему, которая будет использоваться для этого обновления:

   * **dyndns** — отправляет обновления для имени хоста Динамического DNS. Выберите эту опцию если вы не управляете вашим IP-адресом (например, если он динамический и меняется с определенной периодичностью).

   * **custom** — отправляет обновления для имени хоста произвольного DNS. Эта опция используется клиентами, который платят за регистрацию своего домена в dyndns.com.

   Для более подробной информации см. http://www.dyndns.com/services/.

10. В поле **Options** вы можете ввести любую из приведенных ниже опций. Если вы хотите добавить опцию, то в начале и конце опции необходимо поставить символ “&”. Если вы хотите добавить несколько опций, вам необходимо разделять опции при помощи символа “&”. Например:

    &backmx=NO&wildcard=ON&

    mx=mailexchangerback

    mx=YES|NOwildcard=ON|OFF|NOCHG

    offline=YES|NO

    Для более подробной информации см. http://www.dyndns.com/developers/specs/syntax.html.

11. При помощи стрелок установите временной интервал обновления IP-адреса.

Конфигурация сети в режиме drop-in

В режиме drop-in всем интерфейсам устройства Firebox присваиваются один IP адрес. Режим drop-in распределяет все диапазон логических адресов сети между всеми доступными сетевыми интерфейсами. Вы можете подключить ваш Firebox между машрутизатором и LAN и при этом не вносить каких-либо изменений в конфигурацию локальных компьютеров.

В режиме drop-in:

- Вам необходимо присвоить один IP адрес всем интерфейсам Firebox (External, Trusted, и Optional).
- Вы можете добавить вторичные сети на любом интерфейсе.
- Вы можете оставить без изменений IP-адреса и шлюзы по умолчанию для хостов в Trusted и Optional сетях и подключить вторичную сеть к External интерфейсу таким образом, чтобы Firebox мог корректно передавать трафик между этими сетями.
- Публичные серверы, подключенные к Firebox, могут и дальше использовать публичные IP-адреса. Для маршрутизации трафика из вашей сети на публичные серверы Firebox не использует трансляцию сетевых адресов.

Параметры конфигурации drop-in:

- External интерфейсу вам необходимо присвоить статический IP адрес.
- Использование одной логической сети для всех интерфейсов.
- Вы не можете настроить больше одного External интерфейса в этом режиме. Multi-WAN автоматически отключена. Иногда вам необходимо будет очистить ARP кэш.

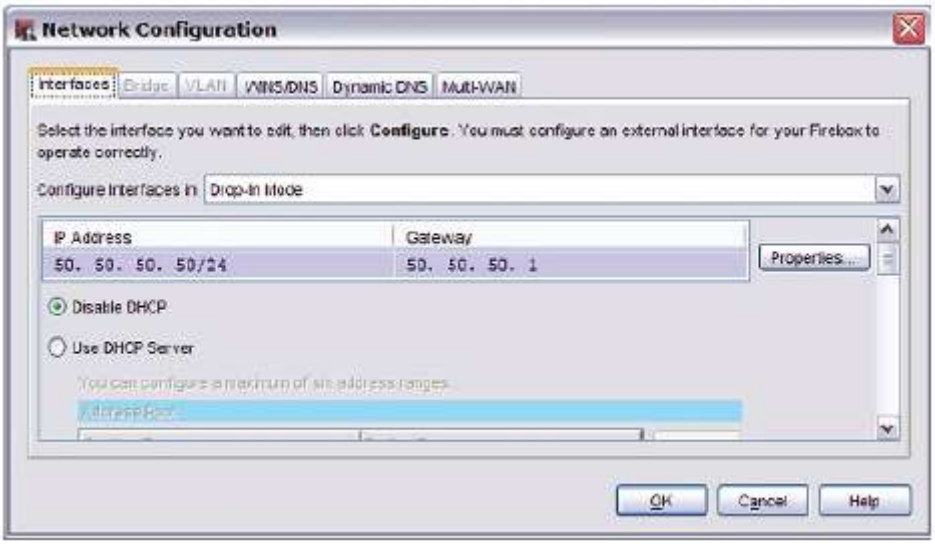
Вы также можете настроить ваши сетевые интерфейсы в режиме drop-in при использовании мастера Quick Setup Wizard. Если вы уже создали конфигурацию сети, то вы можете при помощи Policy Manager переключиться на режим drop-in.

Если вы переместите IP с компьютера, который подключен к одному интерфейсу, на компьютер, подключенный к другому интерфейсу, потребуется несколько минут для того чтобы восстановить передачу трафика. Перед тем как передавать трафик ваш Firebox должен обновить свою внутреннюю таблицу маршрутизации.

Режим drop-in для настройки интерфейса

1. Нажмите  . Или выберите **Network** > **Configuration**.
   Откроется диалогое окно Network Configuration.
2. В выпадающем списке **Configure Interfaces in** выберите **Drop-In Mode**.
3. В поле **IP Address** введите IP-адрес, который будет использоваться для всех интерфейсов Firebox.

4. В поле **Gateway** введите IP адрес шлюза. Этот IP адрес будет автоматически добавлен в список Related Hosts



5. Нажмите **OK**.

6. Сохраните конфигурационный файл.

Настройка связанных хостов

В режимах drop-in или моста все интерфейсы Firebox имеют один и тот же IP-адрес. Firebox автоматически обнаруживает новые устройства, подключенные к этим интерфейсам, и добавляет MAC адреса этих устройств в свою внутреннюю таблицу маршрутизации. Если вы хотите вручную настроить подключения к устройствам или если функция Automatic Host Mapping работает некорректно, вы можете сами добавить связанный хост. Связанный хост создает статический маршрут между IP адресом хоста и сетевым интерфейсом. Мы рекомендуем отключить функцию Automatic Host Mapping для интерфейсов, для которых вы создаете связанные хосты.

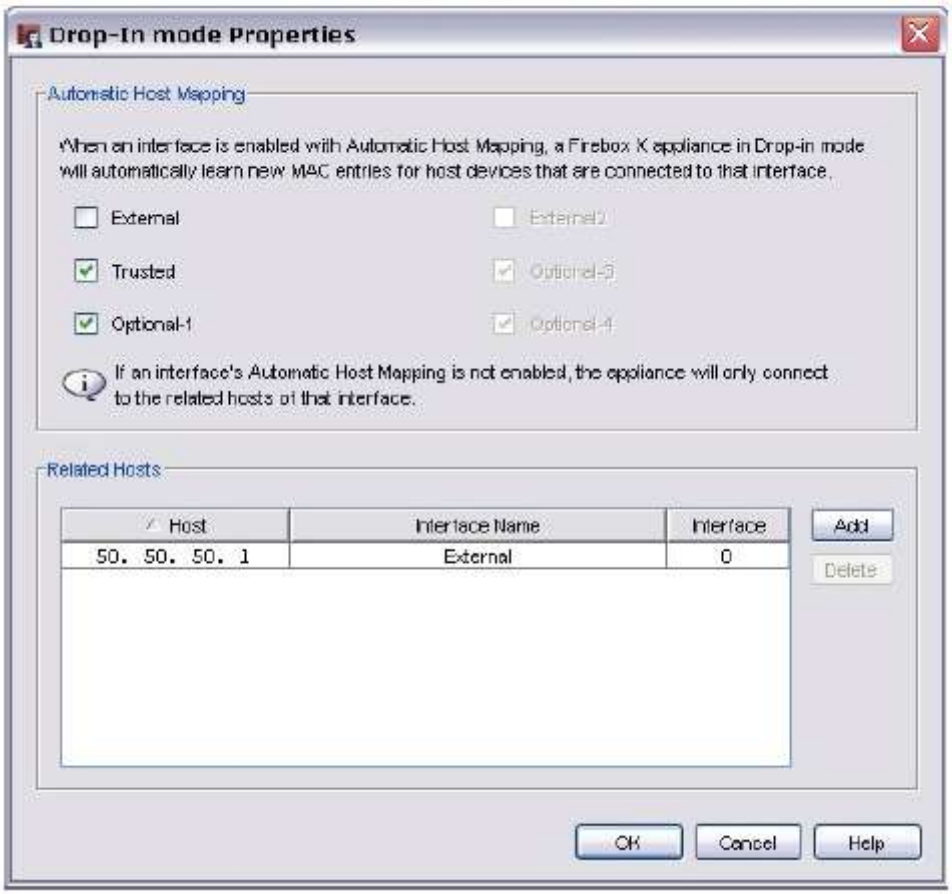
1. Нажмите  . Или выберите **Network** > **Configuration**.
Откроется диалоговое окно Network Configuration.

2. Настройте сетевые интерфейсы в режимах drop-in или моста, затем нажмите **Properties**.
Откроется диалоговое окно Drop-In Mode Properties.

3. Очистите флажок для интерфейсов, для которых вы хотите добавить связанные хосты.

4. Нажмите **Add**. Введите IP адрес устройства, для которого вы хотите создать статический маршрут.

5. В колонке **Interface Name** выберите интерфейс для связанного хоста



6. Нажмите **OK**.

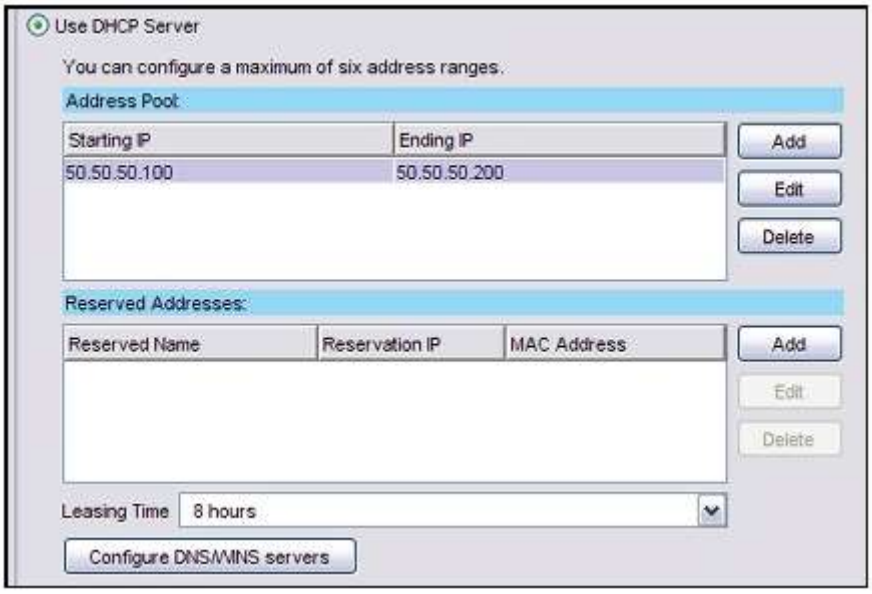
7. Сохраните конфигурационный файл.

Настройка DHCP в режиме drop-in

Если вы используете режим drop-in, то вы можете при помощи Policy Manager настроить Firebox, как DHCP сервер для защищенных сетей, или настроить Firebox в качестве агента DHCP relay. Если у вас уже есть рабочий DHCP сервер, мы рекомендуем продолжать его использовать.

Использование DHCP

1. Нажмите . Или выберите **Network** > **Configuration**.
   Откроется диалогое окно Network Configuration



2. Выберите **Use DHCP Server**.

3. Для того чтобы добавить пул адресов для Firebox, нажмите **Add** рядом с полем **Address Pool** и введите начальный и конечный адреса пула, которые находятся в той же подсети, что drop-in IP адрес. drop-in IP адрес не должен входить в этот пул адресов. Нажмите **OK**.

   Вы можете настроить максимум 6 пулов.

4. Для того чтобы зарезервировать определенный IP адрес для устройства или клиента, рядом с полем **Reserved Addresses** нажмите **Add**. Введите имя резервации, IP адрес, который вы хотите зарезервировать и MAC адрес устройства. Нажмите **OK**.

5. В выпадающем списке **Leasing Time** выберите промежуток времени, в течение которого DHCP клиент может использовать выданный IP адрес

6. По умолчанию если ваше WatchGuard устройство настроено как DHCP сервер, то, помимо IP адресов, оно передает клиенту информацию о DNS и WINS серверах (**Network Configuration > WINS/DNS)**. Для того чтобы указать, какую информацию ваш DCHP сервер будет передавать клиентам нажмите **Configure DNS/WINS servers**.

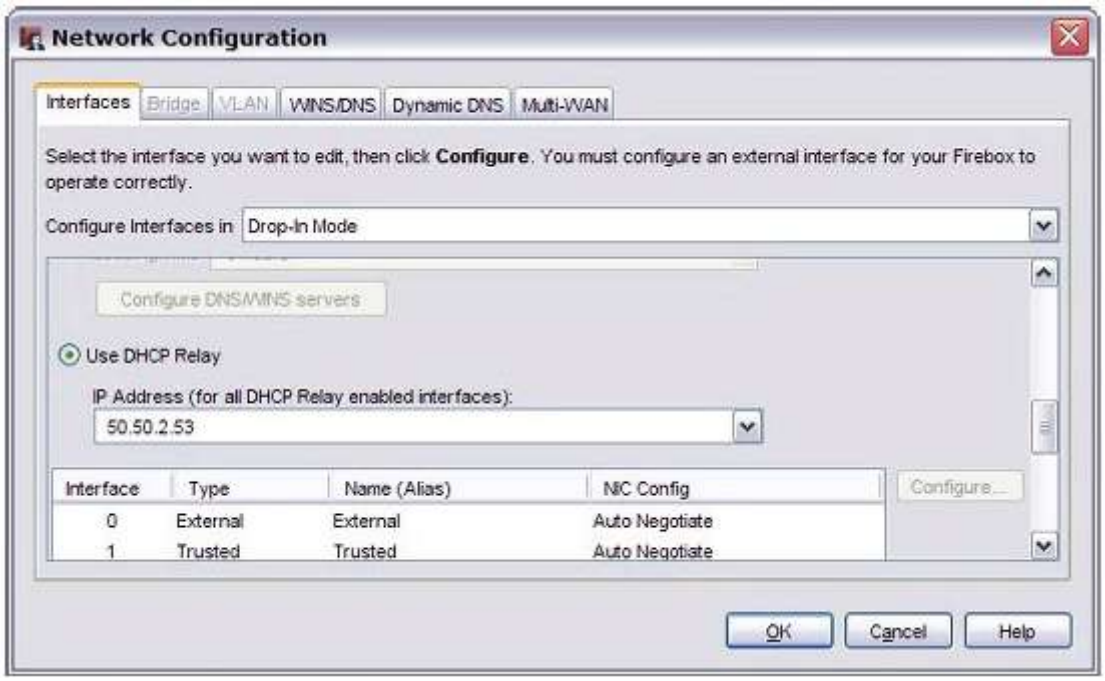
7. Нажмите **OK**.

8. Сохраните конфигурационный файл.

Использование DHCP ретрансляции

1. Нажмите . Или выберите **Network** > **Configuration**.
   Откроется диалогое окно Network Configuration.

2. Выберите **Use DHCP Relay**



3. Введите IP адрес DHCP сервера в соответствующем текстовом поле. При необходимости проверьте наличие маршрута на DHCP сервере.

4. Нажмите **OK**.

5. Сохраните конфигурационный файл.

Настройка параметров DHCP для одного интерфейса

Вы можете настроить различные параметры DHCP для каждого интерфейса Firebox (Trusted или Optional).

1. Нажмите . Или выберите **Network** > **Configuration**.
Откроется диалогое окно Network Configuration.

2. Прокрутите до самого низа диалогового окна **Network Configuration** и выберите интерфейс.

3. Нажмите **Configure**.

4. Настройте необходимые параметры DHCP:

   * Для того чтобы использовать такие же параметры DHCP, которые вы настроили для режима drop-in, выберите **Use System DHCP Setting**.

   * Для того чтобы отключить DHCP для клиентов, подключенных к данному интерфейсу, выберите **Disable DHCP**.

   * Для того чтобы настроить дополнительные параметры DHCP для клиентов, подключенных ко вторичной сети, выберите **Use DHCP Server for Secondary Network**.

5. Нажмите **OK**.

Конфигурация сети в режиме моста

Режим моста позволяет вам подключить ваше WatchGuard устройство между существующей сетью и ее шлюзом для фильтрации и управления сетевым трафиком. При использовании этого режима ваше WatchGuard устройство обрабатывает и перенаправляет весь сетевой трафик на другие шлюзы. Трафик приходит на шлюз с IP адресом устройства, которое этот трафик передавало. Для того чтобы использовать режим моста, вам также необходимо указать IP-адрес, который будет использоваться для управления вашим WatchGuard устройством.

При использовании режима моста вашему WatchGuard устройству не будут доступны следующие функции:

- Multi-WAN
- VLAN (Virtual Local Area Networks)
- Сетевые мосты
- Статические маршруты
- FireCluster
- Вторичные сети
- DHCP сервер или DHCP ретрансляция
- Переключение модемов (только Firebox X Edge)
- 1-to-1, динамическая или статическая NAT
- Динамическая маршрутизация (OSPF, BGP или RIP)
- Любой тип VPN для которого Firebox является конечной точкой или шлюзом
- Некоторые функции прокси, включая HTTP Web Cache Server

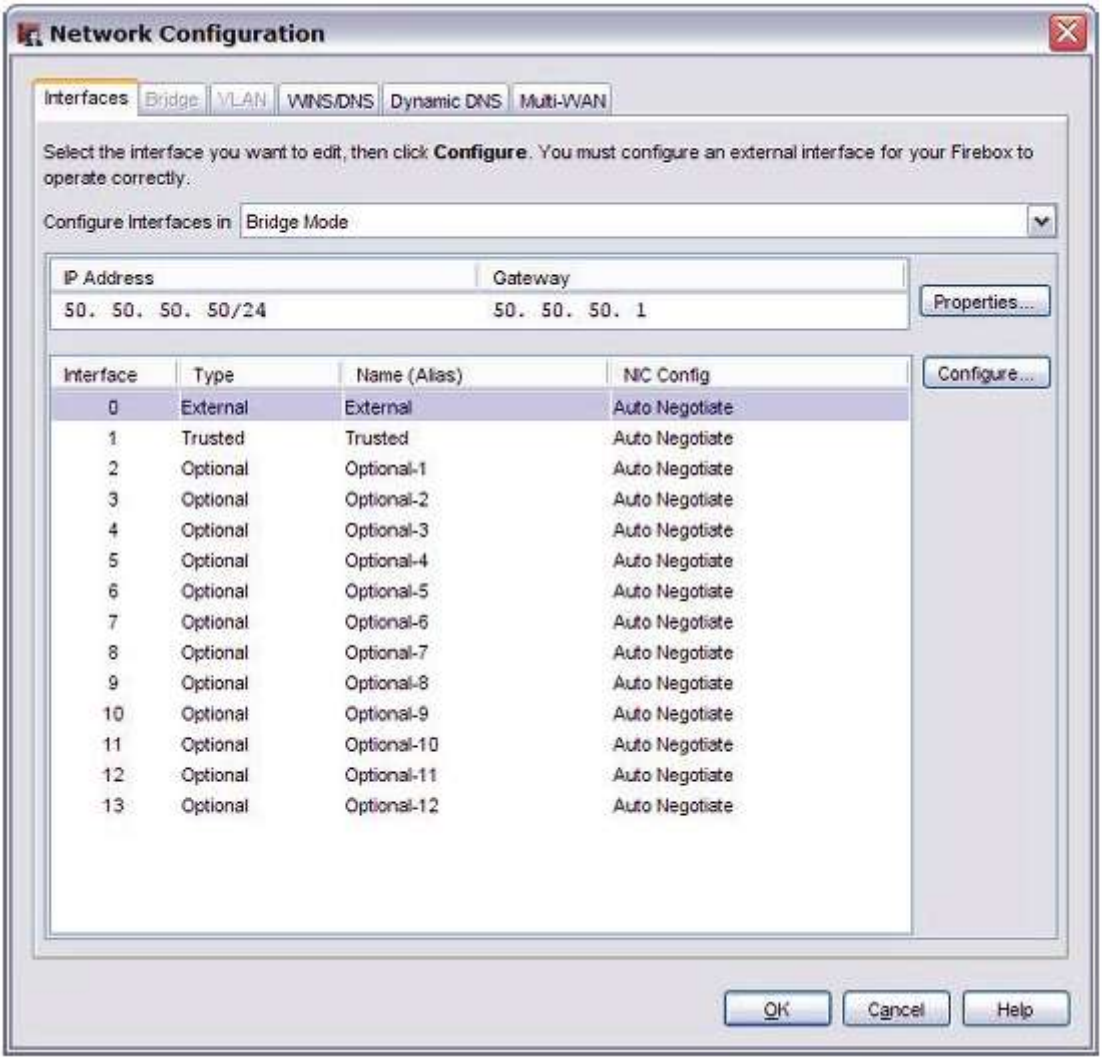
Если вы до этого настроили какие-либо из этих функций, то при включении режима моста эти функции будут отключены. Для того чтобы использовать эти функции вам необходимо использовать другой режим конфигурации сети. Если вы вернетесь снова в режим drop-in или режим смешанной маршрутизации, то вам возможно придется некоторые функции настраивать заново.

Когда вы включите режим моста, все интерфейсы с настроенными сетевыми мостами или VLAN будут отключены. Для того чтобы использовать эти интерфейсы вам необходимо сменить режим конфигурации сети (drop-in или режим смешанной маршрутизации) и настроить эти интерфейсы как External, Optional или Trusted, а затем снова включить режим моста. Функции беспроводной сети при включении режима моста работают корректно.

Для того чтобы включить режим моста:

1. Нажмите  . Или выберите **Network** > **Configuration**.
   Откроется диалогое окно Network Configuration.

2. В выпадающем списке **Configure Interfaces** In выберите **Bridge Mode**



3. Если программа вас попросит отключить интерфейсы, нажмите **Yes** для того чтобы отключить интерфейсы или **No** для того чтобы вернуться к предыдущей конфигурации.

4. В поле **IP Address** введите IP адрес вашего WatchGuard устройства, используя slash-нотацию. Этот IP адрес будет использоваться только для администрирования.

5. В поле **Gateway** введите IP адрес шлюза, который будет получать весь сетевой трафик от вашего устройства

6. Нажмите **OK**.

7. Сохраните вашу конфигурацию.

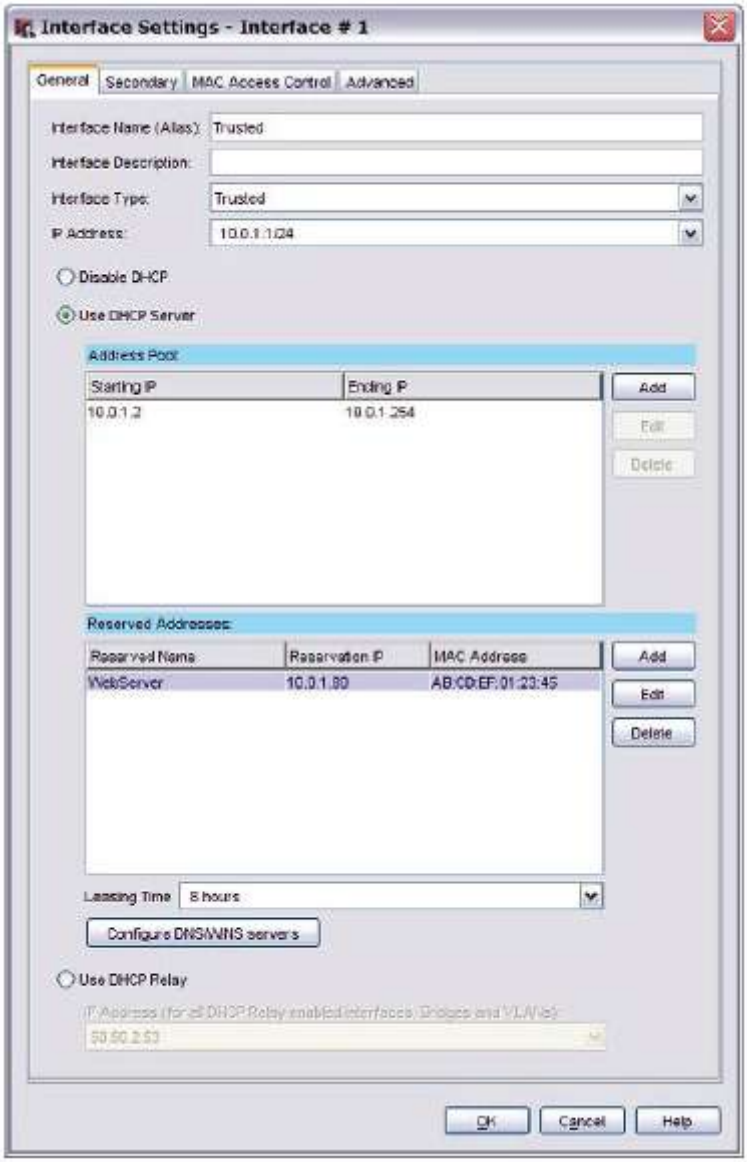
Общие настройки интерфейса

В режиме смешанной машрутизации вы можете настроить ваш Firebox для передачи трафика в различные логические и физические сети. Этот режим используется по умолчанию и предоставляет наибольшую гибкость для различных конфигураций сети. Однако вам необходимо отдельно настроить каждый интерфейс. А также вам возможно придется менять сетевые настройки для каждого компьютера, подключенного к защищенной сети.

Для того чтобы включить режим смешанной маршрутизации выполните следующее:

1. Выберите **Network** > **Configuration**
   Откроется диалогое окно Network Configuration.

2. Выберите интерфейс, который вы хотите настроить, и нажмите **Configure**. Список доступных опций зависит от типа выбранного вами интерфейса.
   Откроется диалогое окно Interface Settings



3. В поле **Interface Name (Alias)** введите имя интерфейса. Это имя должно быть уникальным как среди всех интерфейсов, так и среди имен MVPN групп и туннелей. Затем вы можете использовать это имя для различных целей, например при создании политик прокси, или для управления трафиком на этом интерфейсе.

4. (Дополнительно) В **Interface Description** введите описание интерфейса.

5. В поле **Interface Type** вы можете изменить тип интерфейса. Некоторые типы интерфейсов имеют дополнительные параметры.

   * Для более подробной информации о присвоении IP адресу External интерфейсу см. “Configure an external interface” on page 81.

   * Для автоматического присвоения IP адресов компьютерам, подключенным к Trusted или Optional интерфейсам, см. “Использование DHCP ретрансляции” или “Настройка DHCP в режиме смешанной маршрутизации”

* Для более подробной информации о нескольких IP адресах на одном физическом интерфейсе см. “Configure a secondary network” on page 101.

* Для более подробной информации о настройках VLAN см. “VLAN (Virtual local area networks)”.

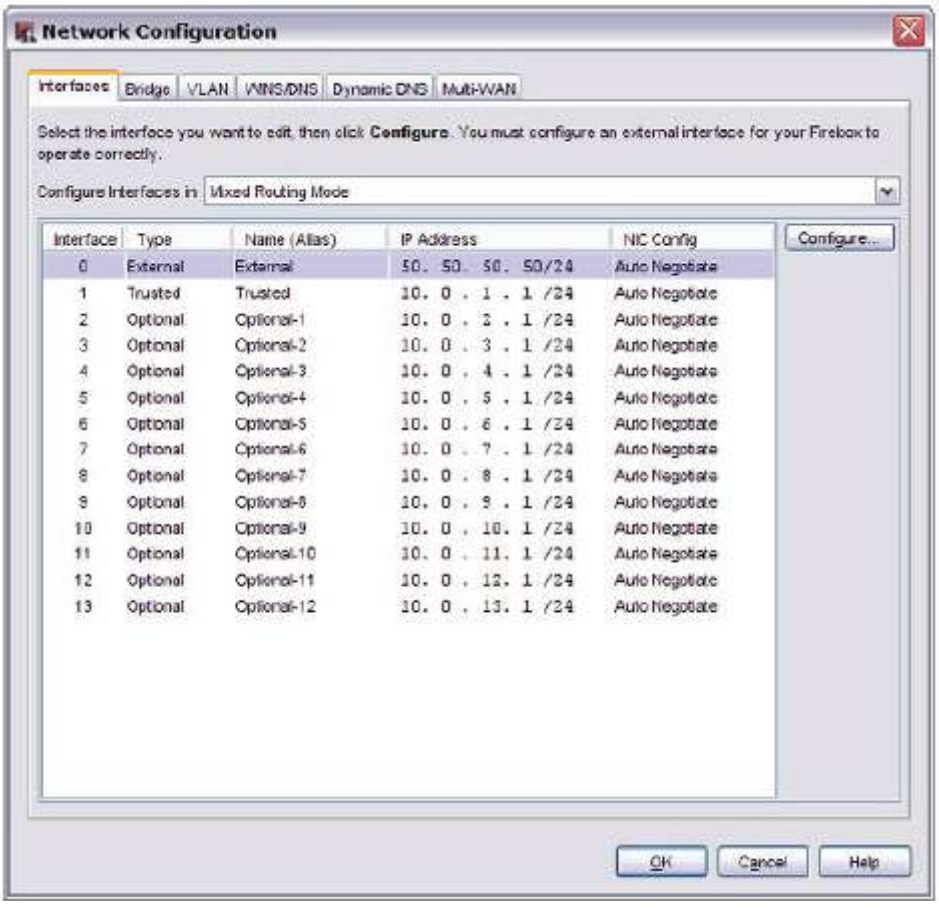
* Для того чтобы удалить интерфейс из вашей конфигурации см. “Общие настройки интерфейса”

6. Выполните необходимую настройку вашего интерфейса.

7. Нажмите **OK**.

Отключение интерфейса

1. Выберите Network > Configuration.
   Откроется диалогое окно Network Configuration



2. Выберите интерфейс, который вы хотите отключить. Нажмите **Configure**.
   Откроется диалогое окно Interface Setting

3. В выпадающем списке **Interface Type** выберите **Disabled**. Нажмите **OK**.

Теперь в диалоговом окне **Network Configuration** этот интерфейс будет отображаться как **Disabled**.

Настройка DHCP ретрансляции

Для получения IP адресов для компьютеров, подключенных к Trusted или Optional сетям, вы можете использовать DHCP ретрансляции. При этом Firebox будет отправлять DHCP запросы в другую сеть.

Вы не можете использовать DHCP ретрансляцию на интерфейсе, на котором включен FireCluster

Для того чтобы настроить DHCP ретрансляцию выполните следующее:

1. Выберите **Network** > **Configuration**.
   Откроется диалогое окно Network Configuration.

2. Выберите Trusted или Optional интерфейс и нажмите **Configure**.

3. Выберите **Use DHCP Relay**.

4. Введите IP адрес DHCP сервера. Убедитесь, что у вас настроен маршрут к DHCP серверу

5. Нажмите **OK**.

Блокировка трафика по MAC адресу

При помощи списка MAC адресов вы можете определять, какие устройства могут передавать трафик через указанный интерфейс. Если вы включите эту функцию, то WatchGuard устройство будет проверять MAC адрес каждого компьютера или устройства, подключенного к указанному интерфейсу. Если MAC адреса устройства нет в списке MAC Access Control для этого интерфейса, то трафик с этого устройства блокируется.

Эта функция используется для предотвращения несанкционированного доступа в вашу сеть из внешней сети. Однако при подключении нового авторизованного устройства к сети, вам необходимо добавлять запись в список MAC Address Control

Если вы хотите использовать функцию управления доступом на базе MAC адресов, то вам необходимо в список разрешенных MAC-адресов добавить адрес компьютера, с которого вы будете администрировать ваше WatchGuard устройство

Для того чтобы включить MAC Access Control для интерфейса выполните следующее:

1. Выберите Network > Configuration.
   Откроется диалогое окно Network Configuration.

2. Выберите интерфейс, для которого вы хотите включить MAC Access Control, и нажмите **Configure**.
   Откроется окно Interface Settings.

3. Выберите закладку **MAC Access Control**.

4. Включите опцию **Restrict access by MAC address**.

5. Нажмите **Add**.
   Откроется окно Add a MAC.

6. В поле **MAC address** введите MAC адрес устройства, доступ которому вы хотите разрешить.

7. (Дополнительно) В поле **Name** введите имя устройства.

8. Нажмите **OK**.
   Для того чтобы добавить устройства в список MAC Access Control см. п. 5–8

Добавление WINS и DNS серверов

Некоторым компонентам Firebox® для корректной необходимо использовать IP-адреса WINS и DNS серверов. Эти компоненты включают в себя DHCP и Mobile VPN.

Доступ к этим серверам необходимо предоставлять с интерфейса Trusted

Эта информация используется для:

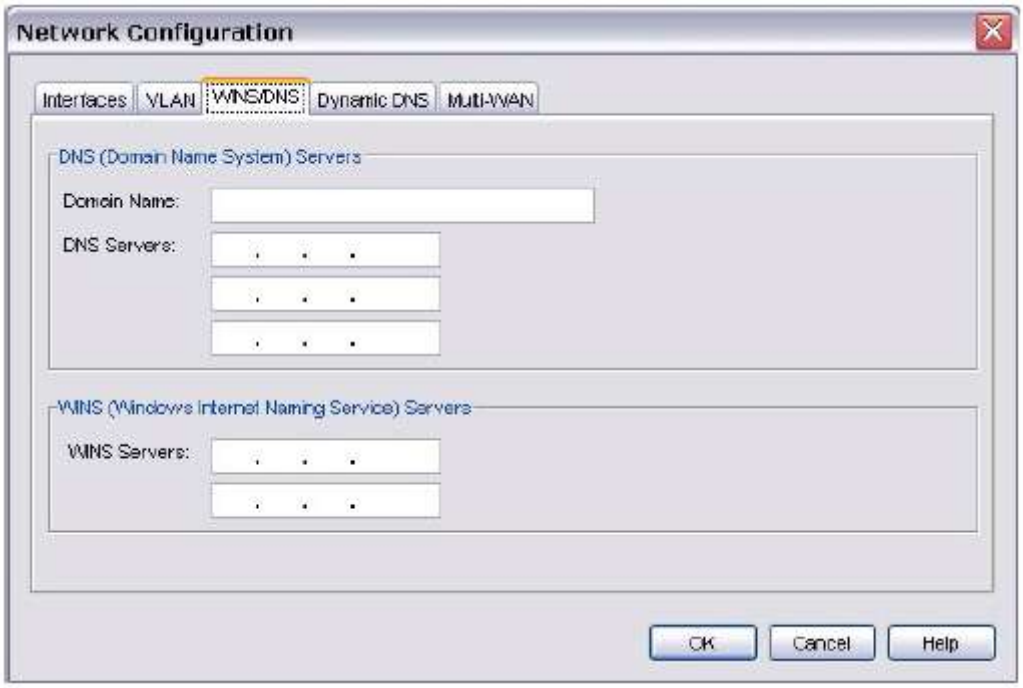
- Firebox использует DNS сервер, показанный здесь, для разрешения имен для IP-адресов для корректной работы IPSec VPN, spamBlocker, GAV и IPS.

- WINS и DNS-записи используются DHCP-клиентами в доверенных и дополнительных сетях пользователями MUVPN, и пользователями PPTP RUVPN для разрешения DNS-запросов.

Убедитесь, что для DHCP и Mobile VPN вы используете только внутренние WINS и DNS серверы. Это гарантирует вам, что вы не создадите политики, конфигурация которых запретит пользователям подключаться к DNS серверу.

1. Выберите **Network** > **Configuration**.
   Откроется диалогое окно Network Configuration.

2. Выберите закладку **WINS/DNS**.
   В закладке WINS/DNS появится информация



3. Введите основной и резервный адреса для WINS и DNS серверов. Вы можете использовать до трех DNS серверов. Для того чтобы DHCP-клиенты могли использовать такие имена как “ watchguard_mail ” в поле **Domain Name** введите суффикс домена

Настройка вторичной сети

Вторичная сеть – это сеть, которая использует одну из физических сетей, как один из интерфейсов Firebox®.

При добавлении вторичной сети вы для интерфейса создаете (или добавляете) IP-псевдоним. Этот IP-псевдоним – это шлюз по умолчанию для всех компьютеров вторичной сети. Вторичная сеть сообщает Firebox, что к интерфейсу Firebox подключена еще одна сеть.

Например, если вы настроили Firebox в режиме drop-in, вы всем интерфейсам Firebox один и тот же IP адрес. Однако для вашей Trusted сети вы используете другую схему IP адресации. Вы можете добавить эту частную сеть, как вторичную сеть, к Trusted интерфейсу вашего Firebox.

Когда вы добавляете вторичную сеть, вы создаете маршрут с IP адреса во вторичной сети к IP адресу интерфейса Firebox. Если вы настроили Firebox со статическим IP-адресом, вы можете добавить IP-адрес в ту же подсеть, что и к вашему основному интерфейсу External в качестве вторичной сети. Затем вы можете настроить статическую NAT для нескольких типов серверов.

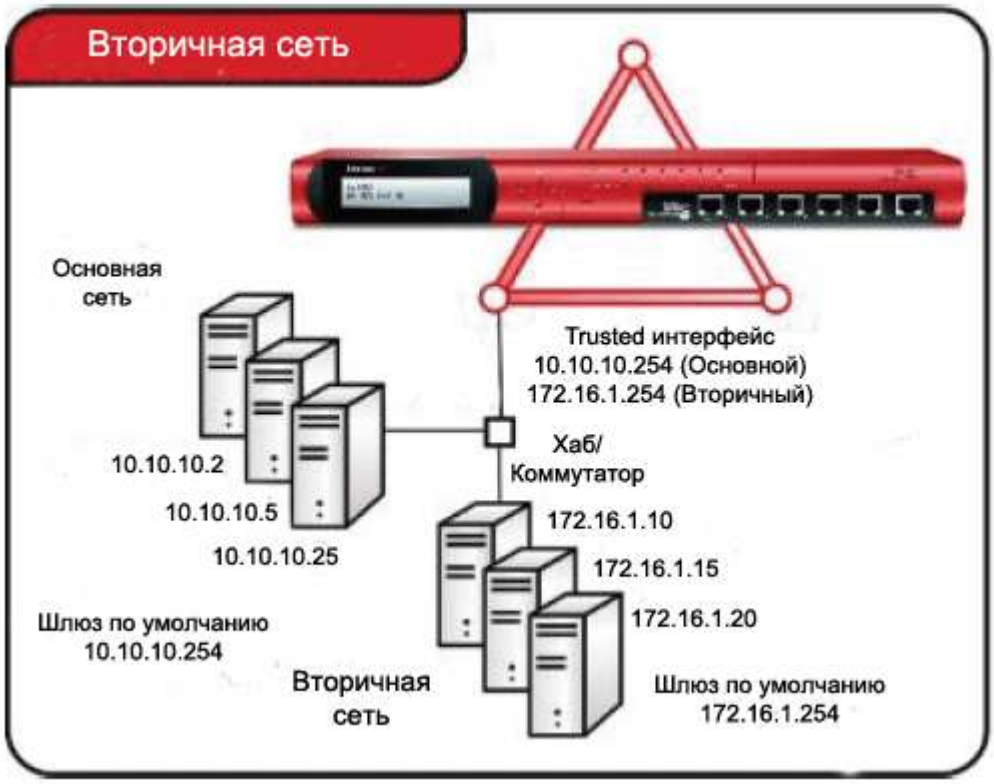
Например, если у вас есть два SMTP-сервера и для каждого вы хотите настроить правило статической NAT, то вы можете настроить вашу внешнюю вторичную сеть со вторым публичным IP-адресом.

Вы можете добавить до 255 вторичных сетей на каждом интерфейсе Firebox. Вторичные сети вы можете использовать как для drop-in, так и для режима смешанной маршрутизации. Если External интерфейс получает IP адрес посредством PPPoE и DHCP, то вы можете к нему добавить вторичную сеть

Для того чтобы создать вторичный IP адрес, вам необходимо следующее:

- Незадействованный IP адрес из вторичной сети, который можно присвоить интерфейсу Firebox

- Незадействованный IP адрес из той же сети, что External интерфейс устройства Firebox



Для того чтобы создать вторичный IP адрес выполните следующее:

1. Выберите **Network** > **Configuration**.
   Откроется диалогое окно Network Configuration.

2. Выберите интерфейс для вторичной сети и нажмите **Configure**.
   Откроется диалогое окно Interface Settings.

3. Выберите закладку **Secondary**.

4. Нажмите **Add**. Введите свободный IP адрес хоста из вторичной сети

5. Нажмите **OK**.

6. Нажмите **OK снова**.

Будьте осторожны при добавлении адресов вторичной сети. Firebox не будет вам сообщать о некорректности введенного адреса. Мы не рекомендуем вам создавать подсеть как вторичную сеть на одном интерфейсе, который является компонент большей сети, подключенной к другому интерфейсу. Если вы так сделаете, то ваша сеть будет некорректно работать, а также будет подвержена атакам типа “spoofing”

Дополнительные настройки интерфейса

Вы можете использовать следующие дополнительные настройки для интерфейсов Firebox:

Настройки параметров сетевой карты

ручная или автоматическая настройка скорости передачи данных и дюплексного режим работы интерфейсов Firebox. Мы рекомендуем для скорости передачи данных использовать автоматическую настройку. Если вы хотите использовать ручную настройку, то тогда вам придется убедиться, что устройство, к которому подключен Firebox, вручную настроен на такие же параметры скорости передачи и дюплексного режима работы. Используйте ручную настройку, только если вам необходимо изменить параметры, установленные автоматически, для работы с другими устройствами сети.

Outgoing Interface Bandwidth

Проверка корректного выделения пропускной способности для политик при использовании Traffic Management. Этот параметр помогает вам сделать так, чтобы гарантированная суммарная пропускная способность не заняла весь канал связи

QoS Marking

Создание различных классификаций сервисов для различных типов сетевого трафика. Вы можете настроить маркирование по умолчанию. Эти параметры могут заменены параметрами, указанными в политике. Для более подробной информации см. ””.

DF bit for IPSec

Настройки бита Don’t Fragment (DF) bit для IPSec.

PMTU Setting for IPSec

(Только для интерфейсов External) Управляет промежутком времени, в течение которого Firebox уменьшает размер MTU для туннеля IPSec VPN при получении запроса ICMP Request to Fragment от маршрутизатора с меньшим значением MTU.

Static MAC/IP address binding

Управляет доступом к интерфейсу Firebox при помощи MAC-адресов.

Настройки параметров сетевой карты (NIC)

1. Выберите **Network > Configuration**.
2. Выберите интерфейс, который вы хотите настроить, и нажмите **Configure**.
3. Выберите закладку **Advanced**.
4. Из выпадающего списка **Link Speed** выберите **Auto Negotiate** если вы хотите, чтобы Firebox автоматически выбирал скорость передачи данных. Вы также можете выбрать одну из полудуплексных или полнодуплексных скоростей, совместимую с вашим оборудованием Мы настоятельно рекомендуем вам самостоятельно не изменять этот параметр. Если вы все-таки захотите изменить значение этого параметра, то обратитесь в Службу Технической Поддержки. Если вы настроите скорость вручную, это может привести к тому, что произойдет конфликт с устройством NIC во время процедуры отката потому, что интерфейс Firebox не сможет повторно подключиться.
5. В поле **Maximum Transmission Unit (MTU)** выберите максимальный размер пакета, который можно передать через интерфейс. Мы рекомендуем использовать значение 1500 байт, только если ваша сетевое оборудование требует другого значения MTU

   Значения MTU могут быть от 68 до 9000 байт.
6. Нажмите **OK**.
7. Сохраните вашу конфигурацию.

Настройка пропускной способности интерфейса (Outgoing Interface Bandwidth)

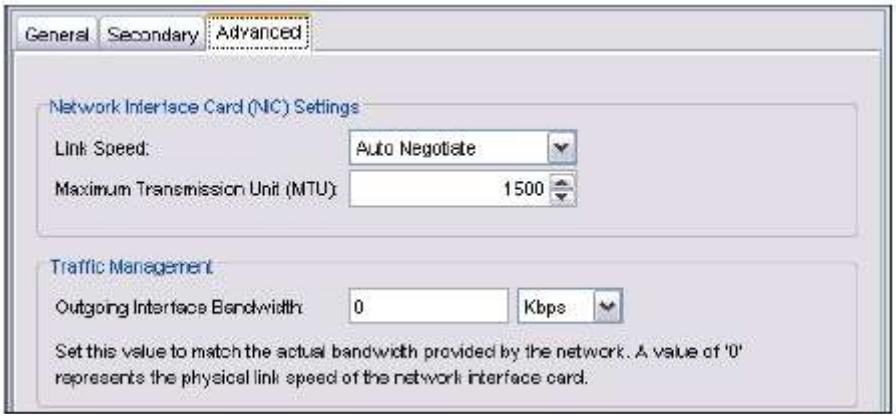
Перед тем как использовать компоненты Traffic Management вам необходимо установить для каждого интерфейса лимит пропускной способности (Outgoing Interface Bandwidth) трафика. После того, как вы настроите эту величину, Fireware будет блокировать пакеты, которые превышают лимит. Также если вы выделяете слишком много пропускной способности утилита Policy Manager

выдаст вам предупреждение. Если значение Outgoing Interface Bandwidth для любого интерфейса равно нулю, то скорость передачи данных через этот интерфейс будет настроена автоматически

1. Выберите **Network** > **Configuration**.
   Откроется диалогое окно Network Configuration.

2. Выберите интерфейс, для которого хотите настроить лимит пропускной способности, и нажмите **Configure**. *Откроется диалоговое окно Interface Settings.*

3. Выберите закладку **Advanced**



4. В поле **Outgoing Interface Bandwidth** введите значение пропускной способности. Для интерфейсов External в качестве лимита пропускной способности используйте скорость вашего подключения к Интернет. Для LAN интерфейсов в качестве лимита используйте величину минимальной скорости подключения, поддерживаемую вашей сетью

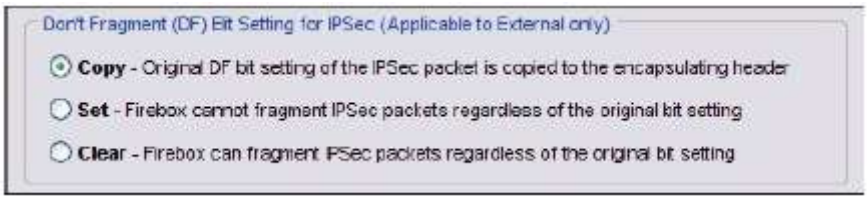
5. Нажмите **OK**.

6. Нажмите **OK** снова.

7. Сохраните конфигурацию.

Установка бита DF для IPSec

При настройке интерфейса External вам необходимо будет выбрать один из переключателей для бита Don't Fragment (DF) для IPSec



Copy

Биты Type of Service (TOS) – набор из четырех флагов(битов) в IP заголовке, которые используются для определения приоритета того или иного трафика. Fireware предоставляет вам опцию, которая разрешает прохождения пакетов с TOS флагами через IPSec туннель. Некоторые ISP сбрасывают все пакеты с установленными битами TOS. Если выбрана опция **Copy,** то при инкапсуляции исходного пакета в IPSec заголовок значения битов не меняется. Если исходный пакет имел обнуленные флаги TOS, то Fireware при инкапсуляции не меняет значения этих битов.

Set:

Выберите опцию **Set** если вы хотите, что Firebox не разбивал фреймы на фрагменты в независимости от исходного значения бита. Если пользователю необходимо подключиться по

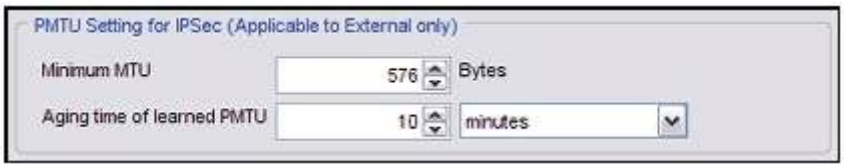
IPSec к Firebox из-за другого Firebox, вам необходимо отключить эту опцию для того чтобы включить компонент IPSec pass-through. Например, если мобильные сотрудники находятся у заказчика, где также стоит Firebox, они могут подключаться к своей сети по IPSec. Для корректной обработки исходящих IPSec соединений на локальном Firebox вам необходимо добавить политику IPSec

Clear

Выберите опцию **Clear** для того чтобы устройство Firebox разбивало фрейм на части, которые по размеру нормально упаковываются в IPSec пакет с ESP или AH заголовком, в независимости от начального состояния бита.

Настройки PMTU для IPSec

Эта дополнительная настройка интерфейса применяется только к интерфейсам External.



Параметр PMTU (Path Maximum Transmission Unit) управляет промежутком времени, в течение которого Firebox уменьшает MTU для IPSec VPN туннеля, когда он получает запрос ICMP Request to Fragment packet от маршрутизатора с более низким значением параметра MTU.

Мы рекомендуем использовать значения по умолчанию. Это позволит вам защититься от машрутизатора в сети Internet с очень низким значением MTU

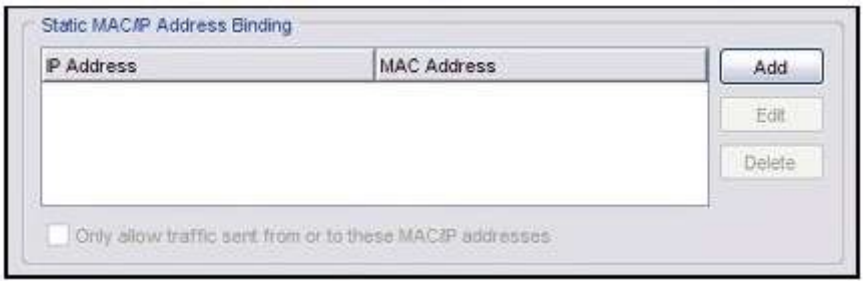
Статическая привязка MAC адреса

Вы можете управлять доступом к интерфейсу Firebox при помощи MAC-адреса. Эта опция позволит вам защитить вашу сеть от атак типа «ARP poisoning», в которых хакеры используют ложные ARP записи для получения доступа к вашей сети. Если эта опция включена и MAC-адрес компьютера, который пытается подключиться к Firebox не включен в конфигурацию, соединение сбрасывается. Если вы ограничиваете доступ к Firebox по MAC-адресу, убедитесь, что вы добавили MAC-адрес компьютера, который используется для администрирования.

Если вы хотите использовать функцию управления доступом на базе MAC адресов, то вам необходимо в список разрешенных MAC-адресов добавить адрес компьютера, с которого вы будете администрировать ваше WatchGuard устройство.

1. Выберите **Network > Configuration**. Выберите интерфейс, который вы хотите настроить и нажмите **Configure**.

2. Выберите закладку **Advanced**



3. Рядом с таблицей **Static MAC/IP Address Binding** нажмите **Add**

4. Введите IP и MAC адреса. Нажмите **OK**.

5. Если вы хотите, чтобы через этот интерфейс проходил только трафик, который совпадает с записями этой таблицы, включите опцию **Only allow traffic sent from or to these MAC/IP addresses**. В противном случае отключите опцию

Сетевые Мосты

Сетевой мосты создает подключения между различными физическими сетевыми интерфейсами на вашем WatchGuard устройстве. Мост можно использовать так же, как и обычный физический сетевой интерфейс. Например, вы можете настроить DHCP для выдачи IP адресов компьютерам, подключенным к мосту, или использовать его как псевдоним в политиках брандмауэра.

Для того чтобы использовать мост, выполните следующее:

1. Создать конфигурацию сетевого моста.

2. Добавить сетевые интерфейсы к мосту.

Если для трафика между двумя интерфейсами вы хотите использовать мост, то мы вам рекомендуем использовать в качестве режима конфигурации сети использовать режим моста.

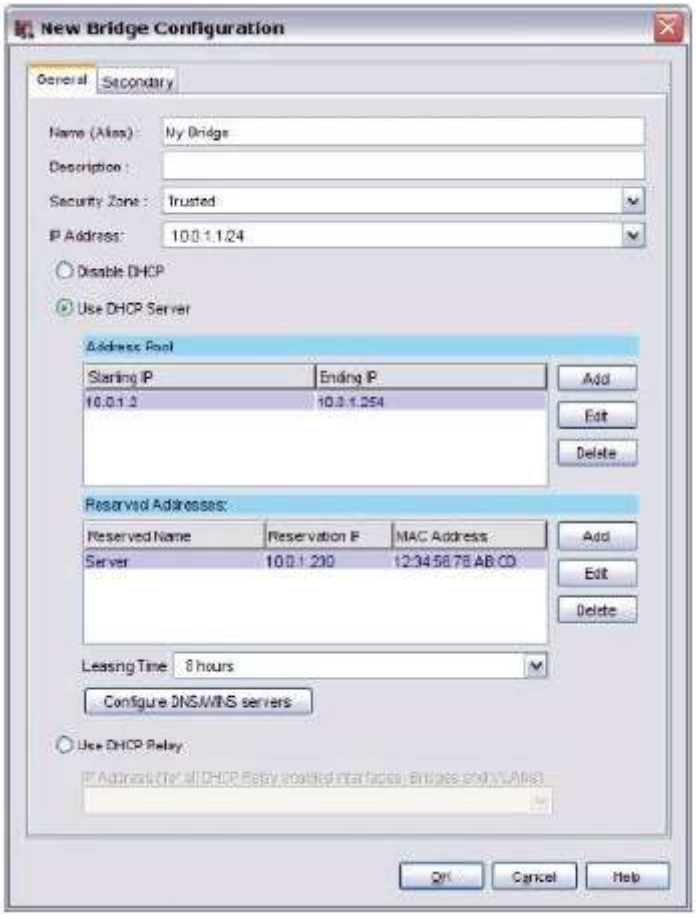
Создание конфигурации сетевого моста

Для того чтобы использовать мост, вам необходимо создать его конфигурацию и добавить к нему один или несколько сетевых интерфейсов.

1. Нажмите  . Или выберите Network > Configuration.
   Откроется диалоговое окно Network Configuration.

2. Выберите закладку **Bridge**.

3. Нажмите **Add**.
   Откроется диалоговое окно New Bridge Configuration



4. В текстовых полях **Name** или **Alias** введите имя или псевдоним для нового моста. Это имя будет использоваться для идентификации моста на сетевом интерфейсе. В поле **Description** вы можете ввести описание моста.

5. В списке **Security Zone** выберите **Trusted**, **Optional**, or **External**. Мост будет добавлен к псевдониму выбранной вами зоны безопасности. Например, если вы выберете зону безопасности Optional, то мост будет добавлен к псевдониму Any-Optional.

6. В поле **IP address** введите IP адрес моста, используя slash-нотацию.

7. Выберите метод получения IP адреса мостом - **Disable DHCP**, **Use DHCP Server** или **Use DHCP Relay**. При необходимости выполните настройку DHCP сервера, DHCP ретрансляции и параметров DNS/WINS серверов.

8. Для того чтобы создать IP адреса вторичных сетей выберите закладку **Secondary**.

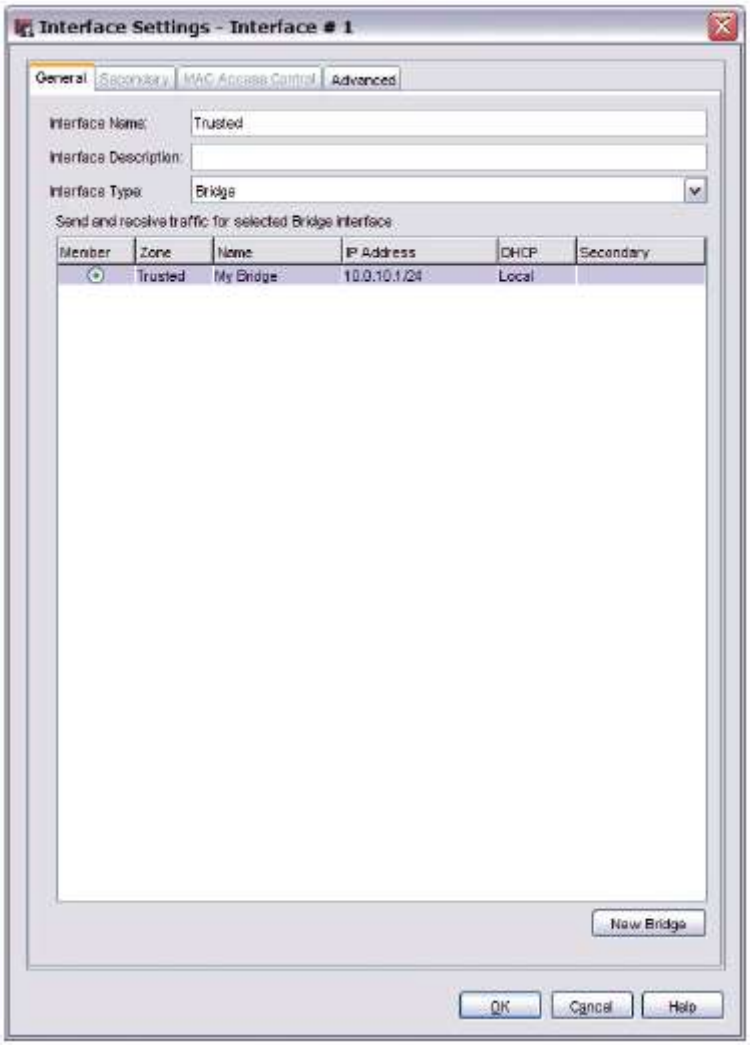
9. Нажмите **OK**.

Добавление интерфейса к мосту

Для того чтобы использовать мост, вам необходимо создать конфигурацию моста и присвоить его к одному или нескольким интерфейсам. Конфигурацию моста вы можете создать в диалоговом окне **Network Configuration** или во время процедуры настройки интерфейса.

1. Нажмите . Или выберите **Network** > **Configuration**.
   Откроется диалоговое окно Network Configuration.

2. Выберите интерфейс, который вы хотите добавить в мост, и нажмите **Configure**.
   Откроется окно Interface Configuration - Interface #



3. В выпадающем списке **Interface Type** выберите **Bridge**.

4. Для того чтобы создать новую конфигурацию моста выберите переключатель рядом с созданной конфигурацией моста или нажмите **New Bridge**.

5. Нажмите **OK**

Маршрутизация

Маршрут это совокупность устройств, которые проходит трафик во время пути до места назначения. Такие устройства, или маршрутизаторы, хранят информацию с сетях, подключенных к ним напрямую в специальной таблице – *таблице маршрутизации*. Информация в этой таблице используется для маршрутизации трафика к следующему маршрутизатору.

При изменении параметров интерфейса, при разрыве связи или при перезагрузке, WatchGuard устройство автоматически обновляет свою таблицу маршрутизации. Для того чтобы обновить таблицу маршрутизации, вам необходимо использовать *динамическую маршрутизацию* или добавить *статический маршрут*.

Статический маршрут повышает производительность, но обладает меньшей гибкостью, так как в случае изменения топологии сети или обрыва связи, трафик не будет автоматически перенаправлен по другому маршруту, и соответственно не сможет попасть в место назначения. Использование протоколов динамической маршрутизации гарантирует доставку трафика в место назначения. Однако в отличие от статических маршрутов, настройка протоколов динамической маршрутизации значительно сложнее.

Добавление статического маршрута

Маршрут – это последовательность устройств, через которые трафик идет от источника до места назначения. *Маршрутизатор* – устройство, который отвечает за маршрутизацию трафика до его места назначения.

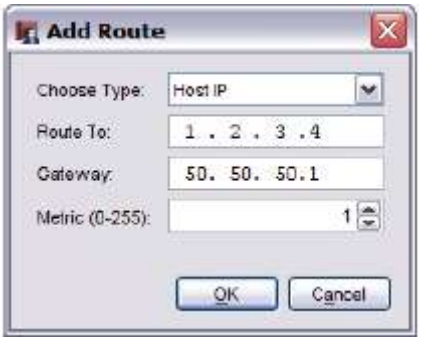
Каждый маршрутизатор подключается минимум к двум сетям. Пакет на своем пути к месту назначения может пройти несколько маршрутизаторов

Для передачи трафика на определенные хосты или в определенные сети вы можете создать *статические маршруты*. Маршрутизатор на базе статического маршрута передает трафик в корректное место назначения. Если к вашему маршрутизатору подключена целая сеть, то вам необходимо создать статический маршрут. Если вы не добавите маршрут к удаленной сети, то весь трафик будет направлен на Firebox шлюз по умолчанию.

Перед тем как начать, вам необходимо понимать разницу между маршрутом к сети и маршрутом к хосту. Маршрут к сети – это маршрут к целой сети, подключенной к маршрутизатору. Если к маршрутизатору подключен только один хост, то вам необходимо создать маршрут к хосту.

1. Выберите **Network** > **Routes**.
   Откроется диалоговое окно Setup Routes.

2. Нажмите **Add**.
   Откроется диалоговое окно Add Route



3. Выберите **Network IP** из выпадающего списка если у вас за маршрутизатором находится целая сеть. Если у вас за маршрутизатором находится только один хост или вы хотите отправлять трафик только одному хосту, то выберите **Host IP**

4. В текстовом поле **Route To** введите адрес сети или адрес хоста. При вводе используйте slash-нотацию.

5. В поле **Gateway** введите IP-адрес маршрутизатора.
   Убедитесь, что вы ввели IP-адрес, который принадлежит той же сети, что и Firebox.

6. В поле **Metric** введите метрику маршрута. Маршруты с более низкой метрикой имеют более высокий приоритет.

7. Нажмите **OK** для того чтобы закрыть диалоговое окно **Add Route**.
   Созданный маршрут появится в диалоговом окне Setup Routes.

8. Нажмите **OK** для того чтобы закрыть диалоговое окно **Setup Routes**.

VLAN (Virtual local area networks)

802.1Q VLAN (virtual local area network) – это совокупность компьютеров в одной или нескольких LAN, которые сгруппированы вместе в один домен трансляции в независимости от их физического расположения. Это позволяет группировать устройства в зависимости от параметров трафика

вместо физического местоположения. Члены VLAN могут иметь общие ресурсы так как будто они подключены к одной и той же LAN.

Вы также можете использовать VLAN для разделения коммутатора на несколько логических сегментов.

Например, предположим ваша компания имеет сотрудников, которые работают полный рабочий день, и работников по контракту, которые подключены к той же локальной сети. Вы хотите работникам по контракту ограничить доступ к некоторому набору ресурсов, которые используются другими сотрудниками. Вы также хотите использовать более строгую политику безопасности по отношению к ним. В этой ситуации вы делите интерфейс на две VLAN.

VLAN позволяют вам разбить сеть на несколько логических сетей. VLAN значительно упрощают проектирование, реализацию и управление вашей сетью. Так как VLAN являются программным функционалом, вы можете достаточно быстро и просто адаптировать свою сеть к различного рода модификациям, перемещениям и реорганизациям.

VLAN использую мосты и коммутаторы, поэтому широковещательные запросы будут получать только пользователи той VLAN, из который этот запрос был отправлен. Следовательно объем трафика через маршрутизатор снижается, что приводит к уменьшению величины задержки. Вы можете настроить ваш Firebox, как DHCP сервер для компьютеров, находящихся в одной VLAN, или использовать DHCP ретрансляцию с отдельным DHCP сервером.

Требования к VLAN и ограничения

- Реализация VLAN в устройствах WatchGuard не поддерживает протокол STP.
- Вы не можете использовать VLAN если ваш Firebox использует конфигурацию drop-in
- Если у вас используется только один VLAN, то физический интерфейс может не тэгировать все входящие пакеты. Например, если External-1 является нетэгированным членом VLAN-1, то он одновременно не может нетэгированным членом другой VLAN. Также External интерфейсы могут принадлежать только одной VLAN.
- Ваши настройки multi-WAN применяются для VLAN трафика. Однако будет значительно проще управлять пропускной способностью, если вы будете в конфигурации multi-WAN вы будете использовать только один физический интерфейс.
- Максимальное количество VLAN, которое вы можете создать, определяется модель вашего устройства и соответствующей лицензией. Для того чтобы посмотреть максимальное количество VLAN, которое вы можете создать на устройстве WatchGuard, откройте Policy Manager и выберите **Setup > Feature Keys**. Найдите строку **Total number of VLAN interfaces**.
- Мы рекомендуем не создавать более 10 VLANов на External интерфейсах.
- Все компьютеры сети, которые вы хотите добавить в VLAN, должны иметь IP-адреса, которые лежат в том же диапазоне, что и остальные члены этой VLAN.

Если вы используете VLAN, то вы можете игнорировать сообщения “802.1d unknown version”. Такие сообщения появляются потому что WatchGuard VLAN не поддерживают протокол STP.

Тэгирование (Tagging)

Для того чтобы использовать VLAN, вам необходимы коммутаторы с поддержкой VLAN. Интерфейс коммутатора в заголовок фрейма вставляет специальный тэг длиной в 4 байта, который обозначает принадлежность этого фрейма к определенному VLAN. Процедура тэгирования описана в стандарте IEEE 802.1Q.

VLAN разделяют понятия тэгированные и нетэгированные фреймы. Вам необходимо настроить на каких интерфейсах будут передаваться тэгированные фреймы, на каких - нетэгированные. Ваше

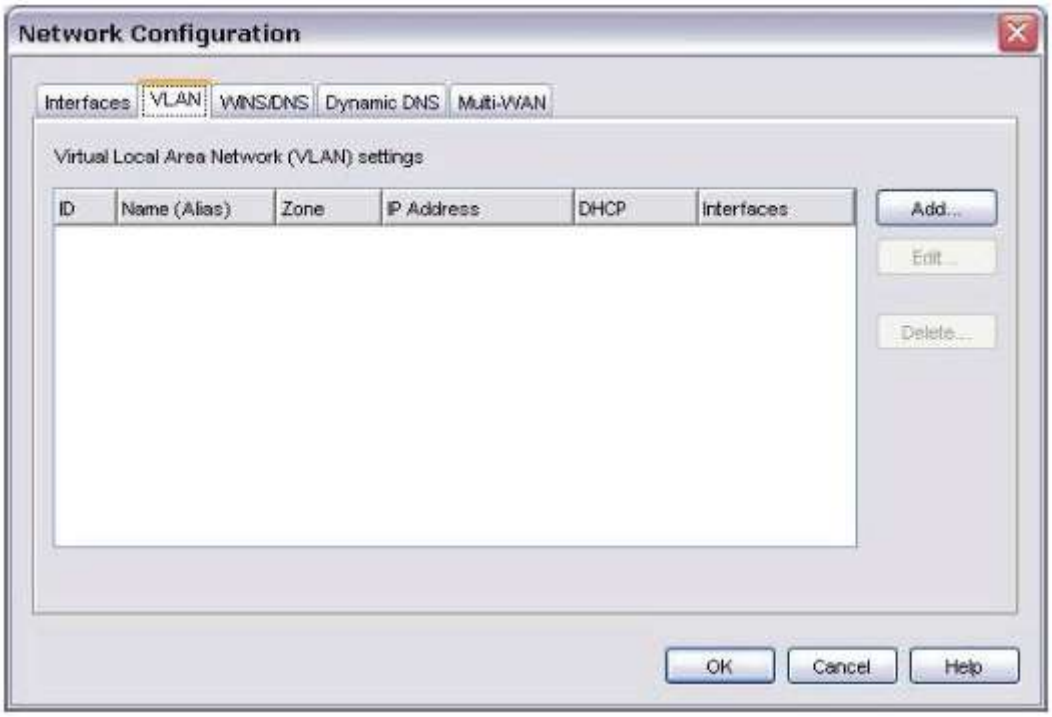
WatchGuard устройство может добавлять тэги к пакетам данных, которые передаются на коммутатор, а также удалять тэги для пакетов данных, которые передаются в сегмент сети, принадлежащий определенному VLAN, и в котором нет коммутатора.

Создание новой VLAN

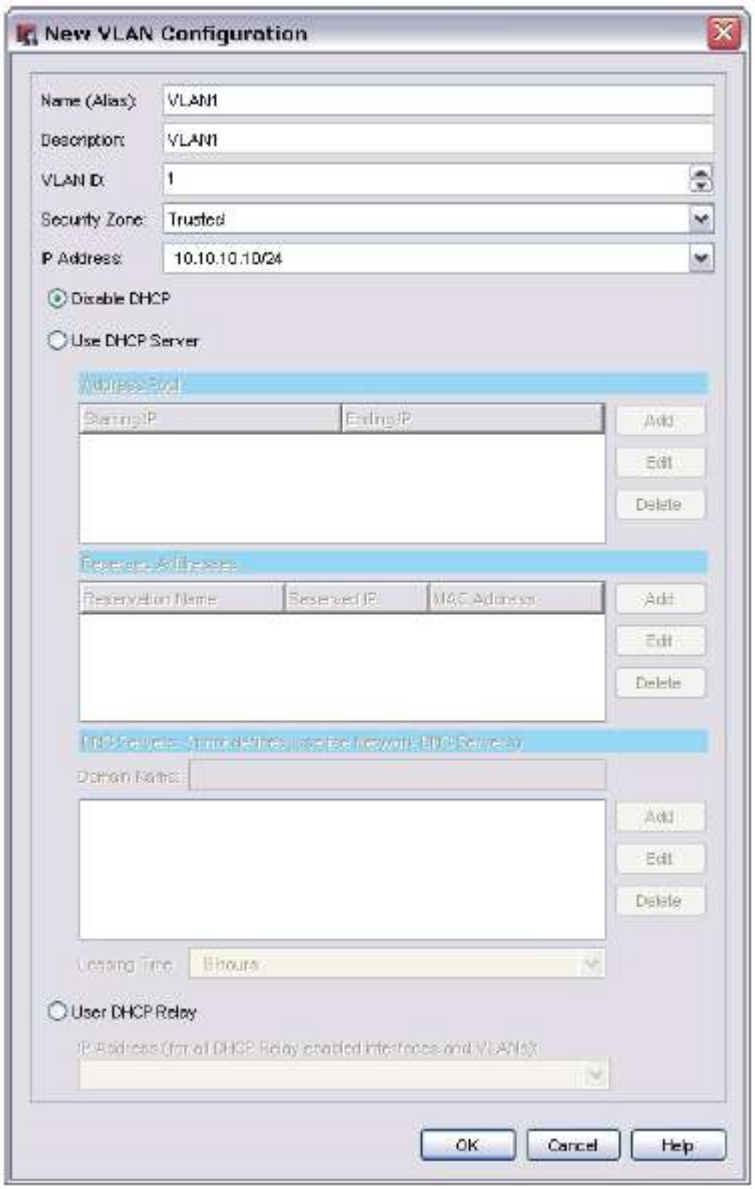
Перед тем как начать создание новой VLAN, убедитесь что вы разбираетесь в теории VLAN и ограничениях, которые на них накладываются.

1. В Policy Manager выберите **Network > Configuration**.
   Откроется диалоговое окно Network Configuration.

2. Выберите закладку **VLAN**. Появится таблица существующих VLAN и их параметров



3. Нажмите **Add**.
   Откроется диалоговое окно New VLAN Configuration



4. В поле **Name (Alias)** введите название для VLAN

5. В поле **Description** введите описание VLAN. Необязательно для ввода.

6. В поле **VLAN ID** введите целое число, которое вы хотите присвоить VLAN.

7. В поле **Security Zone** выберите **Trusted** или **Optional**. Зоны безопасности – это псевдонимы для зон безопасности интерфейсов. Например, VLAN интерфейса Trusted управляются политиками, которые используют псевдоним "any-trusted" в качестве источника или места назначения. VLAN могут быть Trusted или Optional.

8. В поле **IP Address** введите адрес VLAN шлюза

DHCP в VLAN сетях

Вы можете настроить ваш Firebox, как DHCP сервер для компьютеров, которые являются частью одной VLAN.

1. Выберите переключатель **Use DHCP Server** для того чтобы настроить ваш Firebox, как DHCP сервер для указанной VLAN сети.

2. Для того чтобы добавить пул IP адресов нажмите **Add** и введите начальный и конечный IP пула. Нажмите **OK**.
   Вы можете настроить максимум 6 пулов.

3. Для того чтобы зарезервировать определенный IP адрес для клиента, нажмите **Add** рядом с полем **Reserved Addresses**. В поле **Name** введите имя резервации, в поле **IP address** – IP адрес, который вы хотите зарезервировать и в поле **MAC address** MAC-адрес компьютера клиента. Нажмите **OK**.

4. При помощи стрелок **Leasing Time** вы можете изменить срок действия IP адреса по умолчанию.
   Это промежуток времени, в течение которого DHCP клиент может использовать выделенный ему IP адрес. Когда срок действия IP адреса подходит к концу, клиент отправляет запрос на продление срока действия адреса.

5. Для того чтобы добавить DNS или WINS серверы к вашей конфигурации DHCP нажмите на кнопку **DNS/WINS Servers**.

6. Если это необходимо в поле **Domain Name** введите имя домена.

7. Если вы хотите добавить сервер, то рядом со списком серверов.

8. Для того чтобы изменить информацию о сервере, выберите его из списка и нажмите **Edit.**
   Для того чтобы удалить сервер, выберите его из списка и нажмите **Delete**

DHCP ретрансляция в VLAN

1. Выберите переключатель **Use DHCP Relay**.

2. Введите IP-адрес DHCP сервера. Убедитесь, что вы добавили маршрут к DHCP серверу.

Затем подключите интерфейсы к VLAN.

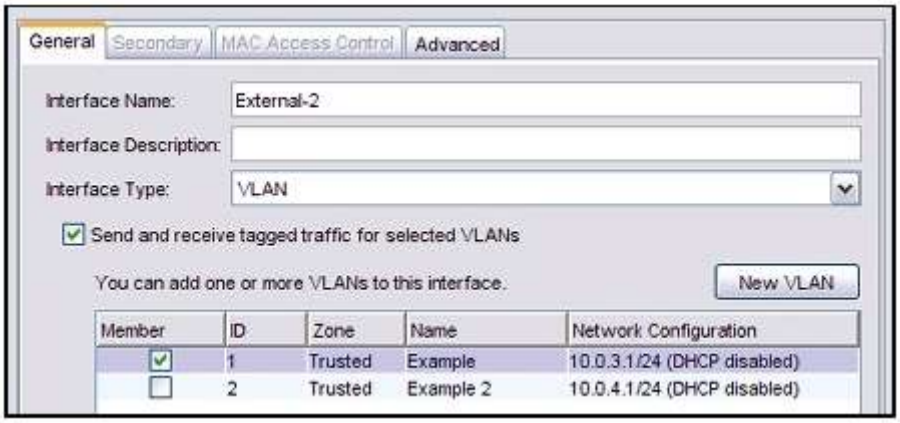
Добавление интерфейсов в VLAN

При создании новой VLAN вы указываете тип данных, который она получает от интерфейсов Firebox. Вы также можете добавить интерфейс в определенную VLAN, а также удалить его из определенной VLAN.

1. В диалоговом окне **Network Configuration** выберите закладку **Interfaces**.

2. Выберите интерфейс и нажмите **Configure**.
   Откроется диалоговое окно Interface Settings.

3. В выпадающем списке **Interface Type** выберите **VLAN**.
   Появится таблица со всеми созданными VLAN



4. Для того чтобы на данном интерфейсе получать тэгированные данные включите опцию **Send and receive tagged traffic for selected VLANs**

5. Напротив всех интерфейсов, которые вы хотите добавить в данный VLAN, отметьте флажок **Member**. Для того чтобы удалить интерфейс из VLAN, очистите флажок **Member** напротив этого интерфейса.

   Интерфейс может принадлежать к одной External VLAN, или нескольким Trusted или Optional VLAN.

6. Для того чтобы данный интерфейс получал нетэгированные данные включите опцию **Send and receive untagged traffic for selected VLAN**.

7. В выпадающем списке выберите конфигурацию VLAN и нажмите **New VLAN** для того чтобы создать новую конфигурацию VLAN

8. Нажмите **OK**.

Глава 7 - Multi-WAN

Использование нескольких External интерфейсов

Firebox предоставляет вам возможность обеспечить резервирование интерфейсов External. Компании часто используют эту опцию если им необходимо постоянное подключение к сети Интернет. Компонент multi-WAN позволяет вам настроить до 4 интерфейсов External, каждый в разной подсети. Это позволит вам подключить Firebox к нескольким ISP. При настройке второго интерфейса компонент multi-WAN автоматически включается.

Требования и условия использования Multi-WAN

Для использования этой опции вам необходимо второе подключение к сети Интернет. При использовании multi-WAN необходимо помнить следующее:

- Если у вас есть политика, настроенная для псевдонима отдельного интерфейса External, вам необходимо изменить псевдоним на “Any-External” или другой псевдоним, который вы настроите для интерфейсов External. Если вы не сделаете этого, то часть трафика может быть заблокирована политиками межсетевого экрана.

- Параметры Multi-WAN не применяются к входящему трафику. При настройке политики для входящего трафика вы можете игнорировать все параметры multi-WAN.

- Вы можете изменить параметры multi-WAN в любой политике. В закладке **Policy** политики включите опцию **Use policy-based routing** и укажите интерфейс External, который будет использоваться устройством Firebox. Для более подробной информации о маршрутизации на базе политики см.”Настройка маршрутизации на базе политик”.

- Присвойте FQDN (Fully Qualified Domain Name) имя вашей компании IP-адресу интерфейса External низшего порядка. Если вы хотите добавить multi-WAN Firebox к конфигурации вашего Сервера Управления, вам необходимо добавить Firebox, используя его интерфейс External низшего порядка, который будет использоваться для его идентификации.

- multi-WAN работает только в режиме смешанной маршрутизации. Эта функция не работает в режимах drop-in или моста.

- Для того чтобы использовать метод Interface Overflow, вам необходимо иметь Fireware XTM с обновлением Pro. Вам также понадобится лицензия Fireware Pro в случае если вы используете метод Round-robin и хотите настроить различные весовые коэффициенты для интерфейсов External устройства

Для управления сетевым трафиком вы можете использовать одну из четырех multi-WAN опций.

Multi-WAN и DNS

Убедитесь, что DNS сервер доступен из любой WAN. В противном случае вам необходимо сделать следующие изменения в вашей политики:

- Список **From** должен содержать Firebox.

- Выберите **Use policy-based routing**. Если DNS сервер доступен только из одной WAN, выберите интерфейс в соответствующем выпадающем списке. Если DNS сервер доступен из нескольких WAN, выберите любую из них, выберите **Failover**, выберите **Configure** и выберите все интерфейсы, которые имеют доступ к DNS серверу. Порядок не имеет значения.

Multi-WAN и FireCluster

Вы можете использовать multi-WAN переключение с FireCluster. При этом настройка каждого компонента осуществляется отдельно. Multi-WAN переключение, причиной которого стало обрыв связи, не запускает процедуру переключения FireCluster. Переключение FireCluster происходит только в случае выхода из строя физического интерфейса или в случае отсутствия ответа на запрос, отправленного на этот интерфейс. Переключение FireCluster является более приоритетным, чем multi-WAN переключение.

Для настройки маршрутизации на базе политик вам необходим Fireware XTM с обновлением Pro.

Опции multi-WAN

При настройке нескольких интерфейсов External у вас есть четыре опции, которые используются для управления интерфейсами для исходящих пакетов. Некоторые опции потребуют наличия установленного Fireware XTM с обновлением Pro.

Multi-WAN в режиме Round-robin

При настройке multi-WAN с методом Round-robin устройство Firebox проверяет свою внутреннюю таблицу маршрутизации на наличие статического или динамического маршрута для каждого подключения. Если указанный маршрут не найден, Firebox распределяет трафик между всеми External интерфейсами.

Для распределения трафика между интерфейсами, которые вы указали в конфигурации Round-Robin, Firebox использует следующие величины: средний объем отправленного (TX) и принятого (RX) трафика. Если вы используете Fireware Pro вы можете присвоить каждому интерфейсу, указанному в конфигурации Round-Robin, весовой коэффициент. По умолчанию для всех пользователей Fireware каждый интерфейс имеет весовой коэффициент 1.

Весовой коэффициент определяет часть трафика, которую Firebox передает через этот интерфейс. Если вы используете Fireware Pro и вы присвоили интерфейсу весовой коэффициент равный 2, то через этот интерфейс будет передаваться в два раза больше трафика, чем через интерфейс с весовым коэффициентом 1. Например если у вас есть три интерфейса External с пропускными способностями 6M, 1.5M и .075M соответственно и вы хотите сбалансировать трафик между тремя интерфейсами, вам необходимо использовать весовые коэффициенты 8, 2 и 1 соответственно.

Fireware попытается распределить трафик следующим образом: через три интерфейса будет проходить 8/11, 2/11 и 1/11 от общего трафика.

Переключение (Failover)

Если вы используете метод переключения для маршрутизации трафика через External интерфейсы устройства Firebox, то вам необходимо выбрать один из интерфейсов в качестве основного. Другие интерфейсы будут использоваться для резервирования. Вы можете выбрать в каком порядке Firebox будет использовать резервные интерфейсы. Firebox выполняет мониторинг основного External интерфейса. Если интерфейс выйдет из строя, Firebox перенаправит весь трафик на следующий External интерфейс, указанный в конфигурации.

В то время, как Firebox передает трафик по резервному интерфейсу, он продолжает выполнять мониторинг основного интерфейса. Как только основной интерфейс снова заработает, Firebox мгновенно перенаправит все новые соединения на него. Вы можете принять решение, что делать с существующими подключениями; эти подключения могут быть немедленно переключены на основной интерфейс или до самого завершения эти подключения будут работать через резервный интерфейс.

Переключения Multi-WAN и FireCluster настраиваются отдельно друг от друга. Multi-WAN Failover, причиной которого стал обрыв связи, не запускает процедуру переключения FireCluster

Переключение FireCluster происходит только когда физический интерфейс вышел из строя или не отвечает. Переключение FireCluster имеет более высокий приоритет по сравнению с переключением multi-WAN.

Метод Interface overflow (Переполнение интерфейса)

Если вы используете метод Interface Overflow, то вам необходимо выбрать порядок использования интерфейсов устройством Firebox для передачи данных и для каждого интерфейса указать пороговую величину пропускной способности. Firebox начинает передавать трафик через первый в списке Interface Overflow интерфейс External. Когда трафик через этот интерфейс достигает пороговой величины Firebox начинает передавать данные по следующему по списку интерфейсу. Такой метод позволяет ограничить объем трафика, передаваемого через каждый интерфейс. Для того чтобы определить пропускную способность Firebox проверяет количество переданных (TX) и принятых (RX) пакетов данных и использует наибольшее число.

При настройке пороговой величины пропускной способности для каждого интерфейса, вам необходимо учитывать интенсивность использования этого интерфейса вашей сетью и устанавливать пороговую величину в зависимости от этого. Например, если ISP асимметричен и вы установили пороговую величину пропускной способности на основе большой скорости TX, то Interface Overflow не будет запущен большой скоростью RX. Если все интерфейсы WAN достигнут предела своей пропускной способности, Firebox для поиска оптимального пути будет использовать протокол ECMP (Equal Cost MultiPath Protocol). Для того чтобы использовать метод маршрутизации multi-WAN у вас должен быть установлен Fireware XTM с обновлением Pro.

Routing Table (Таблица маршрутизации)

Если вы выберете опцию Routing Table для вашей конфигурации multi-WAN, Firebox будет использовать маршруты своей внутренней таблицы маршрутизации или маршруты, которые он получил от динамических процессов маршрутизации, для передачи данных через корректный интерфейс External. Для проверки наличия маршрута для пакета данных Firebox просматривает свою таблицу маршрутизации. В закладке **Status** системы Firebox System Manager вы можете посмотреть список маршрутов.

Опция Routing Table является опцией multi_WAN по умолчанию. Если Firebox не может найти указанный маршрут, то он выбирает маршрут на базе хэша IP-адресов источника и назначения при помощи протокола ECMP (Equal Cost Multipath Protocol): http://www.ietf.org/rfc/rfc2992.txt

При помощи протокола ECMP, Firebox использует алгоритм для решения по какому маршрут отправлять пакет данных. Этот алгоритм не учитывает текущий объем трафика.

Serial модем (только для Firebox X Edge)

Если у вашей компании есть учетная запись для dial-up подключений, то вы можете к последовательному интерфейсу вашего Edge подключить внешний модем и использовать это подключение в случае если все остальные вышли из строя.

Настройка опции Routing Table

Перед тем, как начать

- Для того чтобы использовать компонент multi-WAN у вас должно быть несколько настроенных интерфейсов External. Для более подробной информации о настройке интерфейсов External см. “Настройка External интерфейса”

- Вам необходимо решить является ли метод Routing Table тем методом multi-WAN, который вам необходим. Для более подробной информации см.” Использование нескольких External интерфейсов”

- Убедитесь, что вы действительно понимаете принцип работы и требования к компоненту multi-WAN и выбранному вами методу. Для более подробной информации см. “В каких случаях выбрать режим Routing Table” и “Опции multi-WAN”

Режим Routing Table и балансировка нагрузки

Важно помнить, что опция Routing Table не балансирует нагрузки для подключений к сети Интернет. Firebox считывает данные из внутренней таблицы маршрутизации сверху вниз. Статические и динамические маршруты имеют более высокий приоритет по сравнению с маршрутами по умолчанию. Поэтому они расположены в верхней части таблицы. (Маршрут по умолчанию – это маршрут с адресом назначения 0.0.0.0/0.)

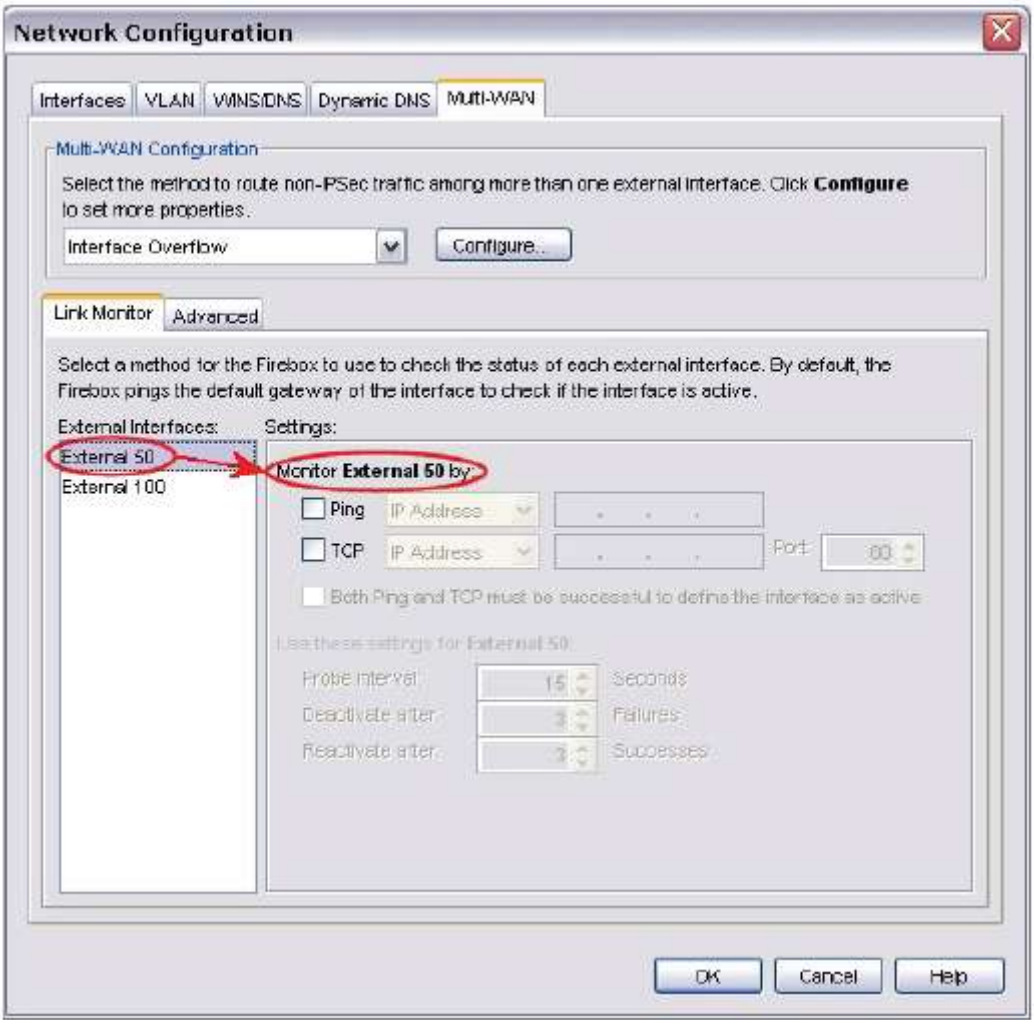
Если для указанного места назначения маршрут не найден, трафик маршрутизируется между External интерфейсами при помощи алгоритма ECMP. Это может привести к распределению пакетов между несколькими External интерфейсами

Настройка интерфейсов

1. В Policy Manager выберите **Network > Configuration**

2. Выберите закладку **Multi-WAN**.

3. Из выпадающего списка выберите **Routing table**. По умолчанию IP-адрес всех интерфейсов External включены в конфигурацию



4. Если вы хотите удалить интерфейс из конфигурации, то нажмите **Configure** и отключите флаг рядом с интерфейсом, который вы хотите удалить. В конфигурации должен быть

минимум один интерфейс External. Это может быть полезно если вы хотите для определенного трафика использовать маршрутизацию на базе политик и оставить только одну WAN для трафика по умолчанию.

5. Для того чтобы завершить процедуру конфигурации, вам необходимо добавить информацию о мониторинге подключения, как описано в “Состояние WAN интерфейса”. Для более подробной информации о дополнительной конфигурации multi-WAN см. “Дополнительные настройки multi-WAN”

Таблица маршрутизации Firebox

Если вы выберете опцию Routing Table, вам полезно будет знать внутренню структуру таблицы маршрутизации Firebox.

1. Откройте Firebox System Manager
2. Выберите закладку **Status Report**.
3. При помощи полосы прокрутки найдите таблицу **Kernel IP routing table**. Это внутренняя таблица маршрутизации Firebox. Под таблицей вы можете найти информацию о группе ECMP.

Таблица маршрутизации Firebox включает следующее:

- Динамические маршруты, созданные протоколами маршрутизации (RIP, OSPF, and BGP) (если вы включили динамическую маршрутизацию)
- Постоянные сетевые маршруты или маршруты хостов, добавленные вами в закладке **Network > Routes** утилиты Policy Manager.
- Маршруты, которые автоматически создаются Firebox при чтении информации о конфигурации сети (**Network > Configuration**).
- Если Firebox обнаруживает, что интерфейс External вышел из строя, он удаляет любые статические или динамические интерфейсы, которые используются этим интерфейсом. Это происходит тогда, когда хосты, указанные в закладке **Link Monitor,** не отвечают и если Ethernet подключение выходит из строя.

Для более подробной информации о состоянии интерфейсов и обновления таблицы маршрутизации см. “Состояние WAN интерфейса”.

Когда использовать методы Multi-WAN и маршрутизацию

Если вы используете динамическую маршрутизацию, то вы можете использовать следующие режимы конфигурации multi-WAN - Routing Table или Round-Robin. Выбранный вами режим конфигурации не распространяется на маршруты, которые используют шлюз по умолчанию во внутренней сети (Optional или Trusted сетях).

В каких случаях выбрать режим Routing Table

Режим Routing Table рекомендуется использовать в следующих ситуациях:

- Вы используете динамическую маршрутизацию (RIP, OSPF или BGP) и маршрутизаторы во внешних сетях присылают на устройство Firebox информацию о маршрутах, таким образом позволяя устройству Firebox выбирать наиболее оптимальные машруты во внешние сети
- Вам необходимо получить доступ к внешнему сайту или внешней сети через определенный маршрут. Например:

  * У вас есть сегмент, который использует маршрутизатор Frame Relay во внешней сети

* Вы хотите, чтобы весь трафик, передаваемый во внешнюю сеть, проходил чееред определенный интерфейс External

Метод Routing Table – самый быстрый метод балансировки нескольких маршрутов в сеть Интернет. После того, как вы включите эту опцию, управления всеми соединениями будет выполнять алгоритм ECMP. Вам нет необходимости выполнять какие-либо дополнительные настройки на Firebox.

В каких случаях использовать метод Round-Robin

Балансировка нагрузки для подключений к сети Интернет при помощи алгоритма ECMP базируется на подключениях, а не на пропускной способности. Статические или динамические маршруты используются до применения алгоритма ECMP. Если у вас установлен Fireware XTM Pro, опция Round-Robin предоставляет вам возможность передавать большее количество через один интерфейс, чем через другой. В то же время алгоритм Round Robin распределяет трафик между External интерфейсами на базе пропускной способности, а не количества подключений. Это предоставляет вам возможность управлять количеством байт, переданных через определенный ISP.

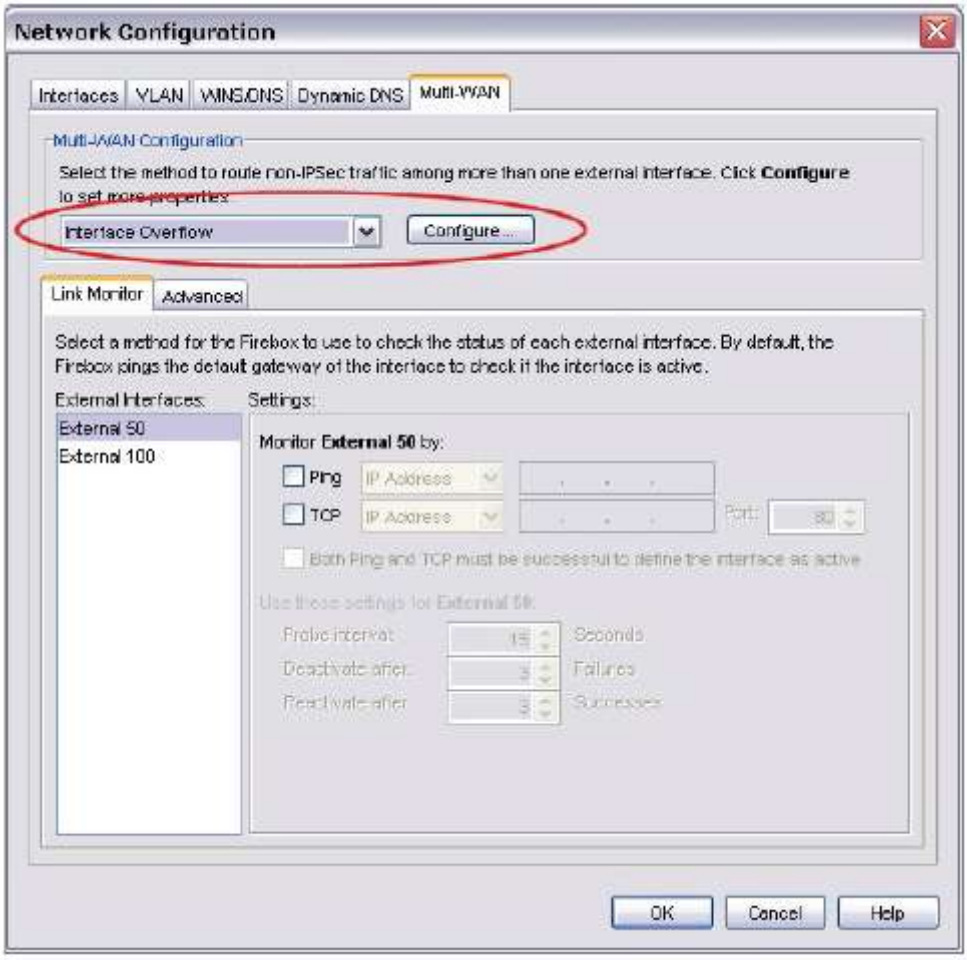
Настройка опции Interface Overflow

Перед тем, как начать

- Для того чтобы использовать компонент WAN у вас должно быть несколько настроенных интерфейсов External
- Убедитесь, что вы действительно понимаете принцип работы и требования к компоненту multi-WAN и выбранному вами методу

Настройка интерфейсов

1. В Policy Manager выберите **Network > Configuration**.
2. Выберите закладку **Multi-WAN**.
3. Из выпадающего списка выберите **Interface Overflow**



4. Нажмите **Configure**.

5. В колонке **Include** отметьте флаг напротив каждого интерфейса, который вы хотите добавить в конфигурацию.

6. Для того чтобы настроить пороговую величину пропускной способности для интерфейса External, выберите необходимый интерфейс из списка и нажмите **Configure**.

7. Из выпадающего списка выберите **Mbps** или **Kbps** в качестве единицы измерения и введите значение пороговой величины пропускной способности для интерфейса. Важно помнить, что Firebox вычисляет пропускную способность на базе большего значения отправленных и принятых пакетов.

8. Нажмите **OK**.

9. Для того чтобы завершить процедуру конфигурации, вам необходимо добавить информацию, как это описано в “Состояние WAN интерфейса”

Для более подробной информации о дополнительной конфигурации multi-WAN, см. “Дополнительные настройки multi-WAN”

Настройка опции multi-WAN Failover

- Для того чтобы использовать компонент multi-WAN у вас должно быть несколько настроенных External интерфейсов. Для более подробной информации о настройке интерфейсов External см. “Настройка External интерфейса”

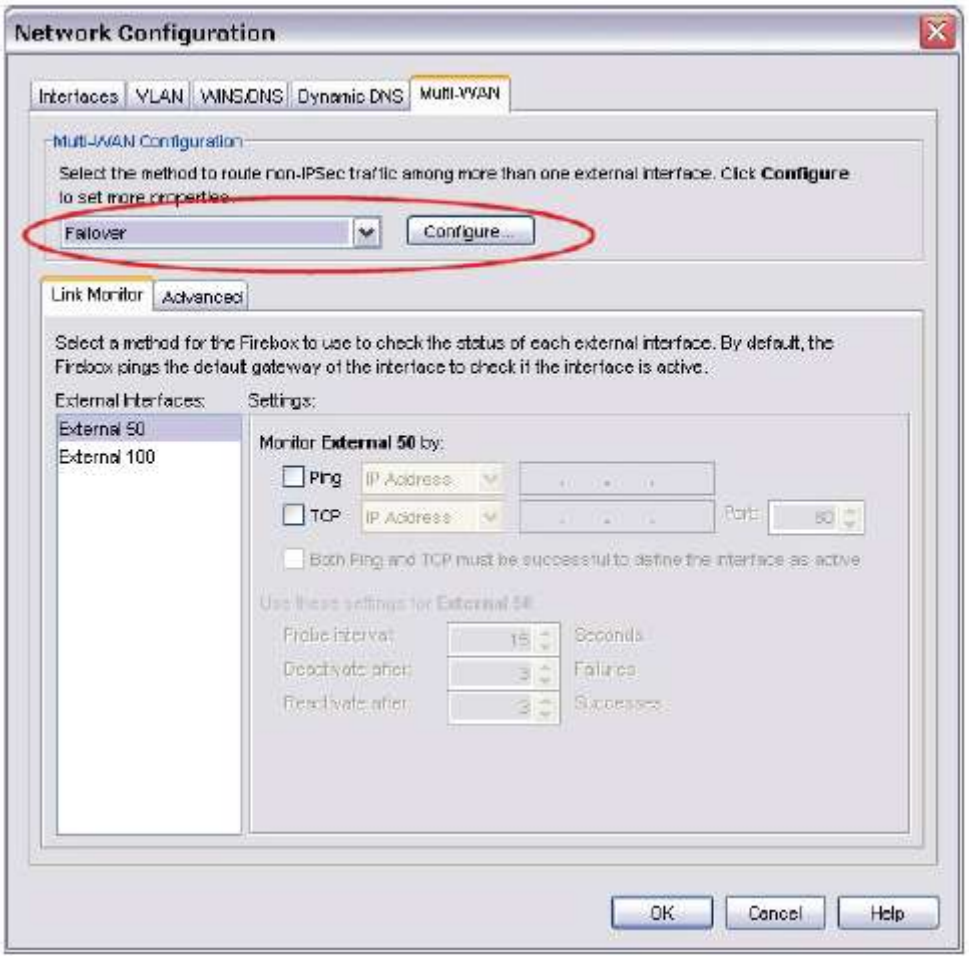
- Убедитесь, что вы действительно понимаете принцип работы и требования к компоненту multi-WAN и выбранному вами методу. См. “Использование нескольких External интерфейсов” и “Опции multi-WAN”

Настройка интерфейсов

1. В Policy Manager выберите **Network > Configuration**.

2. Выберите закладку **Multi-WAN**.

3. Из выпадающего списка выберите **Failover**



4. Нажмите **Configure.** Укажите основной и резервные интерфейсы External. В колонке **Include** отметьте флаг напротив каждого интерфейса, который вы хотите использовать в конфигурации Failover. При помощи кнопок **Move Up** и **Move Down** установите порядок для **failover**. Первый интерфейс в списке будет основным интерфейсом.

5. Нажмите **OK**.

6. Для того чтобы завершить процедуру конфигурации вам необходимо добавить информацию мониторинга подключения как описано в **About WAN Interface status**

7. Нажмите **OK**.

Переключение serial модема

Данная процедура относится только к устройству Firebox X Edge.

Firebox X Edge может передавать через serial модем в случае если он не может передавать данные через External интерфейсы. Для того чтобы использовать serial модем вам необходимы учетная запись dial-up у вашего ISP (Internet Service Provider) и внешний модем, подключенный к последовательному порту Firebox.

Edge тестировался со следующими модемами:

- Hayes 56K V.90 serial fax модем
- Zoom FaxModem 56K модель 2949
- U.S. Robotics 5686 внешний модем
- Creative Modem Blaster V.92 serial модем
- MultiTech 56K Data/Fax Modem International

Включение функции переключения serial модема

1. Выберите **Network** > **Modem**.
2. Включите опцию **Enable Modem for Failover when all external interfaces are down**

3. Выполните все необходимые настройки параметров **Account**, **DNS**, **Dial-Up** и **Link Monitor**
4. Нажмите **OK**.

5. Сохраните вашу конфигурацию.

Параметры учетной записи (Account)

1. В поле **Telephone number** введите номер телефона вашего ISP. В поле **alternate telephone number** при необходимости введите дополнительный номер.

2. В поле **Account name** введите имя учетной записи dial-up.

3. Если для входа в систему вы используете имя домена (например, msn.com), то в поле **Account Domain** введите это имя.

4. В поле **Account password** введите пароль вашей учетной записи.

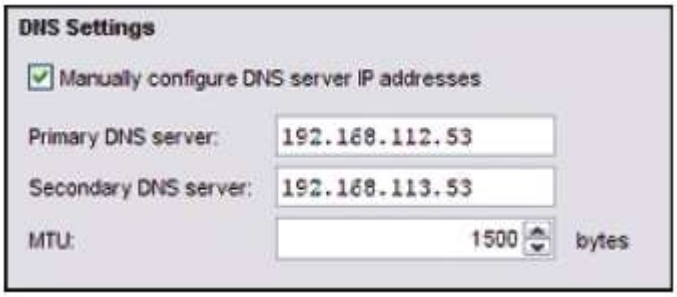
5. Если у вас возникают проблемы с подключением, то включите опцию **Enable modem and PPP debug trace**. Если эта опция включена, то Edge генерирует подробные сообщения в файл журнала событий.

6. Для настройки дополнительных параметров, выберите другие закладки и выполните все необходимые настройки.

7. Нажмите **OK**.

Параметры DNS

Если ваш dial-up ISP не предоставляет информацию о DNS сервере, или вам необходимо использовать другой DNS сервер, то вы можете вручную добавить IP адреса для DNS сервера, которые будут использовать после переключения



1. Включите опцию **Manually configure DNS server IP addresses**.

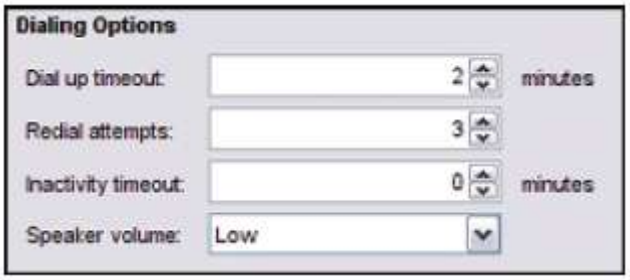
2. В поле **Primary DNS Server** введите IP адрес основного DNS сервера. Если у вас есть второй DNS сервер, то в поле **Secondary DNS server** введите его IP адрес.

3. В поле **MTU** (Maximum Transmission Unit) введите максимальный размер передаваемого сегмента. Большинству пользователей нет необходимости изменять значение этого параметра.

4. Для настройки дополнительных параметров, выберите другие закладки и выполните все необходимые настройки.

5. Нажмите **OK**.

Настройки Dial-up



1. В поле **Dial up timeout** введите величину таймаута при отсутствии подключения через модем. По умолчанию - 2 минуты.

2. В поле **Redial attempts** введите количество попыток подключения устройства Edge к сети Интернет. По умолчанию – 3 попытки.

3. В поле **Inactivity Timeout** введите величину таймаута подключения в случае отсутствия трафика. По умолчанию таймаут не используется.

4. В выпадающем списке **Speaker volume** выберите громкость динамика вашего модема.

5. Для настройки дополнительных параметров, выберите другие закладки и выполните все необходимые настройки.

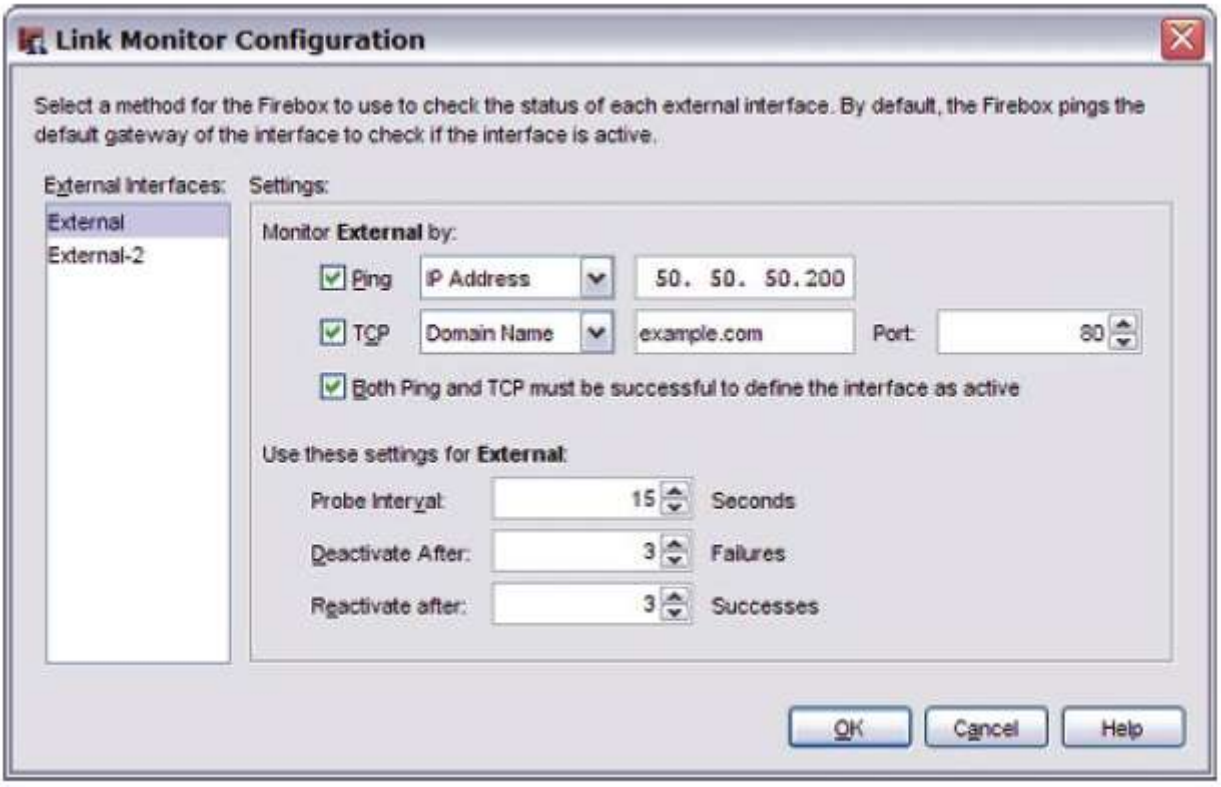
6. Нажмите **OK**.

Настройки Link Monitor

В закладке **Link Monitor** вы можете настроить параметры для тестирования одного или нескольких External интерфейсов для активного подключения.

Когда External интерфейс снова становится активным, Firebox X Edge перенаправляет весь трафик с serial модема на External интерфейс. Вы можете настроить Link Monitor таким образом, чтобы он отправлял ping-запросы на сайт или устройство через External interface,создавал TCP соединение с указанными сайтом или номером порта.

Вы также можете настроить временной интервал между тестами и настроить количество попыток, после которого тест считается неудачным



В списке **External Interfaces** выберите External, который вы хотите настроить. Каждый интерфейс вам придется настраивать отдельно.

Для настройки параметры Link Monitor для интерфейса выполните следующее:

1. Для отправки ping-запросов на определенный сайт или устройство, включите опцию **Ping** и введите IP адрес или имя хоста, на которые будут отправляться ping-запросы.

2. Для того чтобы создать TCP подключение к определенному сайту или устройству включите опцию **TCP** и введите IP адрес или имя хоста. Также в поле **Port** вы можете ввести номер порта.
   По умолчанию используется порт 80 (HTTP).

3. Если вы хотите, чтобы для активации интерфейса были необходимы успешные ping-запросы и TCP подключения, включите опцию **Both Ping and TCP must be successful**.

4. В поле **Probe after** введите значение временного интервала между попытками подключения.
   По умолчанию – 15 секунд.

5. В поле **Deactivate after** введите количество попыток подключения, после которых интерфейс считается неактивным.
   По умолчанию – 3 попытки.

6. В поле **Reactivate after** введите количество успешных подключений, после которых интерфейс будет считаться активным.
   По умолчанию – 3 попытки.

7. Нажмите **OK** для того чтобы закрыть диалоговое окно **Link Monitor**.

8. Для настройки дополнительных параметров, выберите другие закладки и выполните все необходимые настройки.

9. Нажмите **OK**.

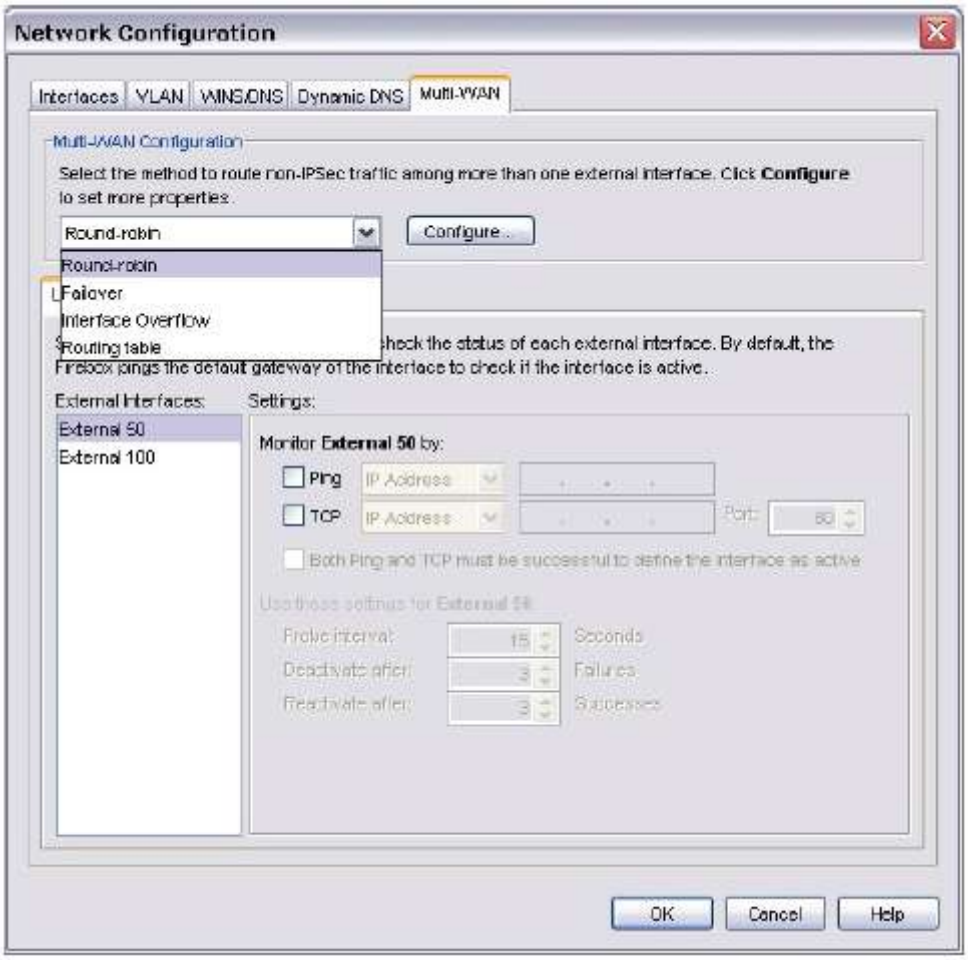
Настройка опции Round-robin

Перед тем как начать

- Для того чтобы использовать компонент WAN у вас должно быть несколько настроенных External интерфейсов
- Убедитесь, что вы действительно понимаете принцип работы и требования к компоненту multi-WAN и выбранному вами методу

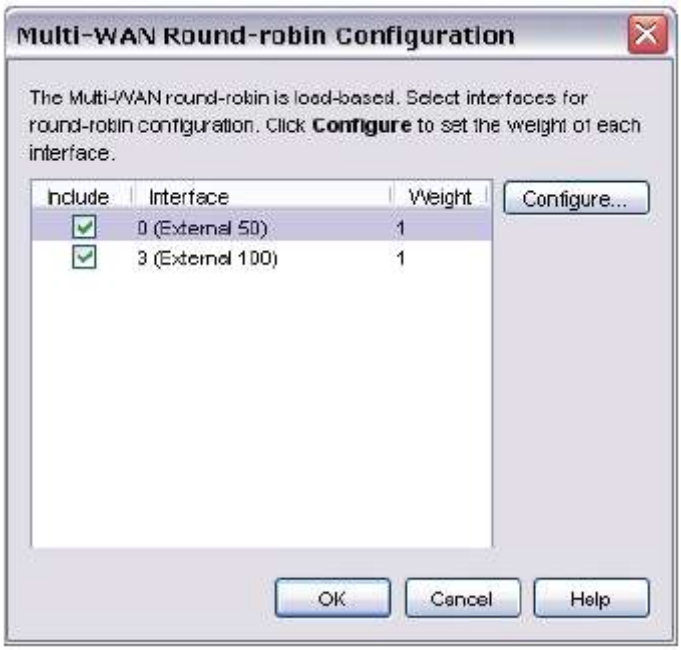
Настройка интерфейсов

1. В Policy Manager выберите **Network > Configuration**.
2. Выберите закладку **Multi-WAN**.
3. Из выпадающего списка выберите **Round-robin**.



4. Нажмите **Configure** (находится рядом с выпадающим списком).

5. В колонке **Include** отметьте флаги напротив каждого интерфейса, который вы хотите использовать в конфигурации round-robin. Нет необходимости в конфигурацию добавлять все External интерфейсы. Например, у вас может быть один интерфейс, который вы хотите использовать для маршрутизации на базе политик, которую вы не хотите в конфигурацию round-robin.



6. Если вы используете Fireware XTM с обновлением Pro на вашем Firebox и вы хотите изменить весовые коэффициенты, присвоенные интерфейсам, нажмите **Configure**.

7. Выберите необходимый весовой коэффициент для интерфейса. Весовой коэффициент интерфейса устанавливает процент нагрузки по трафику на интерфейс.

8. После того, как вы закончите, нажмите **OK**. Для более подробной информации об изменении весовых коэффициентов см. ”Присвоение весовых коэффициентов интерфейсам”

9. Для того завершить вашу конфигурацию, вам необходимо добавить информацию о Link Monitor, как описано в “Состояние WAN интерфейса”. Для более подробной информации о дополнительных настройках multi-WAN см.” Дополнительные настройки multi-WAN”.

10. Нажмите **OK**.

*Изменить весовой коэффициент интерфейса с единицы вы можете только если у вас есть лицензия Fireware Pro. В противном случае при попытке закрытия диалогового окна **Network Configuration** вы получите сообщение об ошибке.*

Присвоение весовых коэффициентов интерфейсам

Если вы используете Fireware XTM с обновлением Pro, то каждому интерфейсу в конфигурации round-robin multi-WAN вы можете присвоить весовой коэффициент. По умолчанию каждый интерфейс имеет коэффициент равный единице. Весовой коэффициент определяет какую часть трафика Firebox передает через этот интерфейс.

В качестве весовых коэффициентов вы можете использовать только целые числа. Для обеспечения оптимальной балансировки нагрузки между интерфейсами, вам необходимо произвести некоторые вычисления для того чтобы понять, какому интерфейсу присвоить какой весовой коэффициент. Используйте общий множитель для того чтобы пропускная способность, присвоенная каждому интерфейсу, соответствовала целому числу.

Например, предположим у вас есть три подключения к сети Интернет. Один ISP дает вам 6 Мбит/с, другой ISP - 1.5 Мбит/с, третий - 768 Кбит/с. Convert the proportion to whole numbers:

- 768 Кбит/с будет примерно равен .75 Мбит/с. Соответственно у вас будут следующие значения: 6, 1.5 и .75 Мбит/с.
- Умножьте каждое значение на 100. Получится соответственно: [6 : 1.5 : .75] будет равно [600 : 150 : 75]
- Найдите наибольший делитель для этих трех чисел. В данном случае 75 это наибольший делитель.
- Разделите каждое число на наибольший делитель.

В результате получите 8, 2 и 1 соответственно. Вы можете использовать эти числа в качестве весовых коэффициентов в конфигурации round-robin multi-WAN.

Дополнительные настройки multi-WAN

Помимо основных параметров, вы можете также настроить такие дополнительные параметры multi-WAN, как sticky соединения, переключение и уведомления о событий. Не все параметры доступны для всех опций конфигурации multi-WAN. Если выбранный вами параметр не используется для опции конфигурации multi-WAN, эти поля неактивны.

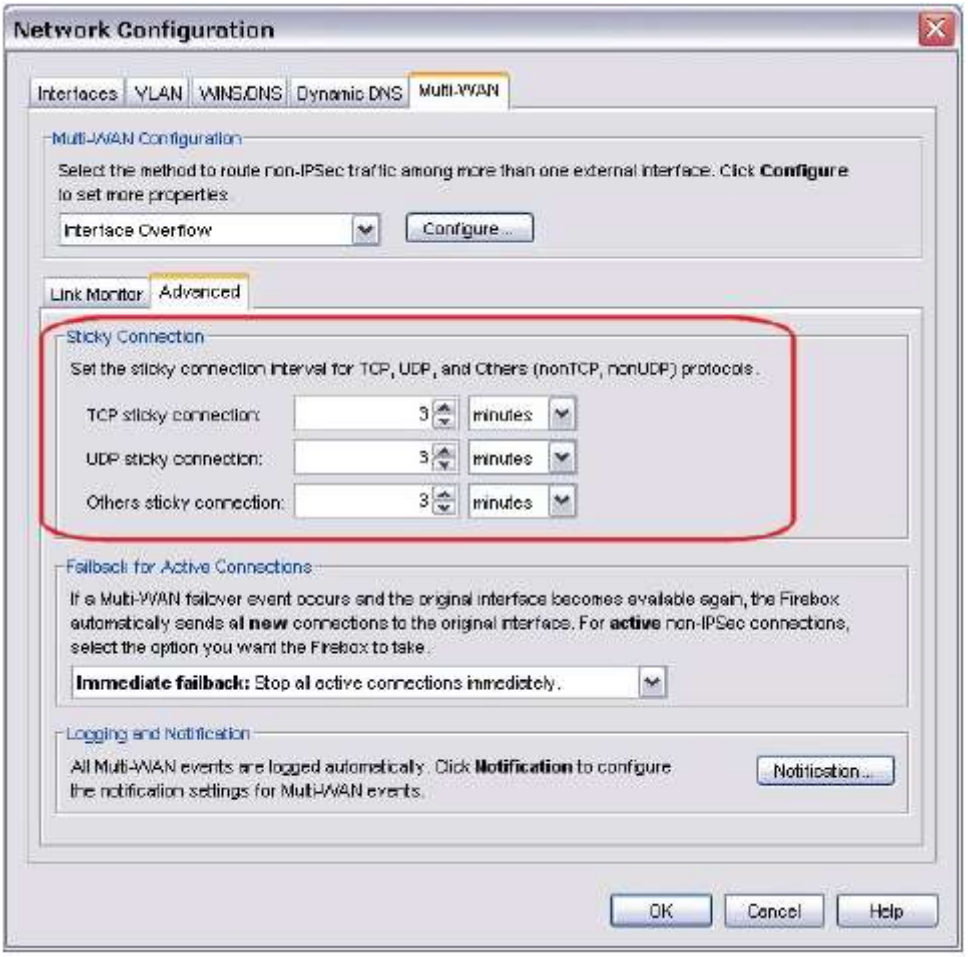
Sticky соединения

Sticky соединение – это соединение, которое использует один и тот же WAN интерфейс в течение какого-то промежутка времени. Вы можете настроить параметры таких соединений если для multi-WAN вы используете опции Round-robin, Interface Overflow.

Параметр «прилипания» гарантирует, что если один пакет пройдет через интерфейс External, то все остальные пакеты будут передаваться через этот же интерфейс в течение определенного промежутка времени. По умолчанию, sticky соединения используют один и тот же интерфейс в течение 3 минут. Если политика содержит параметр sticky-соединения, то этот параметр может заменить все глобальные параметры sticky соединений.

Настройка глобального промежутка времени для sticky соединений

В закладке **Advanced** вы можете настроить промежуток времени для TCP, UDP соединений, а также соединений, которые используют другой протокол. Если вы настроите этот промежуток внутри политики, то это значение заменит значение глобального промежутка времени. Для более подробной информации см. "Настройка длительности sticky соединения для политики".

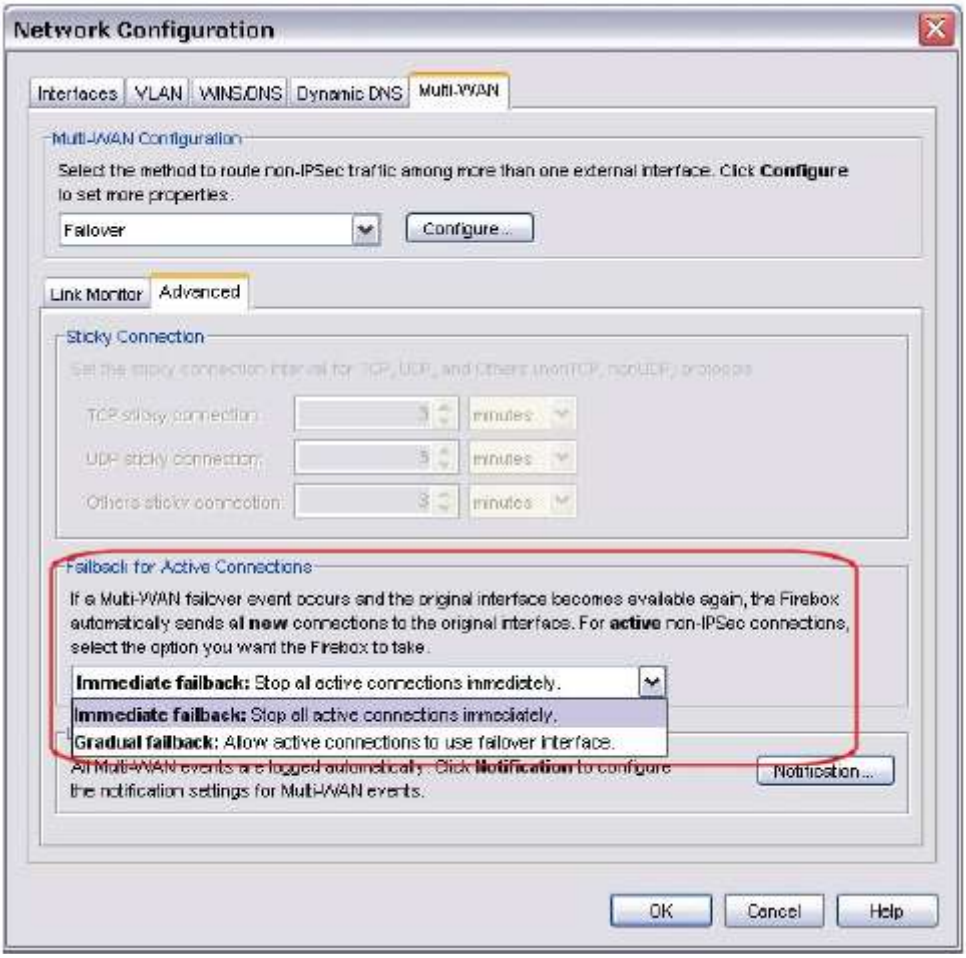


Настройка переключения

Вы можете настроить действие, которое будет выполнять ваше WatchGuard устройство, в случае переключения и последующего восстановления основного External интерфейса. При этом все соединения переносятся на основной external интерфейс. Однако вы можете настроить, каким образом все активные соединения будут переноситься в случае переключения. Эти настройки также применяются к любой маршрутизации на базе политик

1. В диалоговом окне **Network Configuration** выберите закладку Multi-WAN.

2. Выберите закладку **Advanced**



3. В секции **Failback for Active Connections** в выпадающем списке выберите одну из следующих опций:

   * **Immediate failback** — Устройство WatchGuard немедленно закрывает все активные соединения.

   * **Gradual failback** — Устройство WatchGuard для активных подключений до их завершения продолжает использовать резервный интерфейс.

4. Нажмите **OK**.

Состояние WAN интерфейса

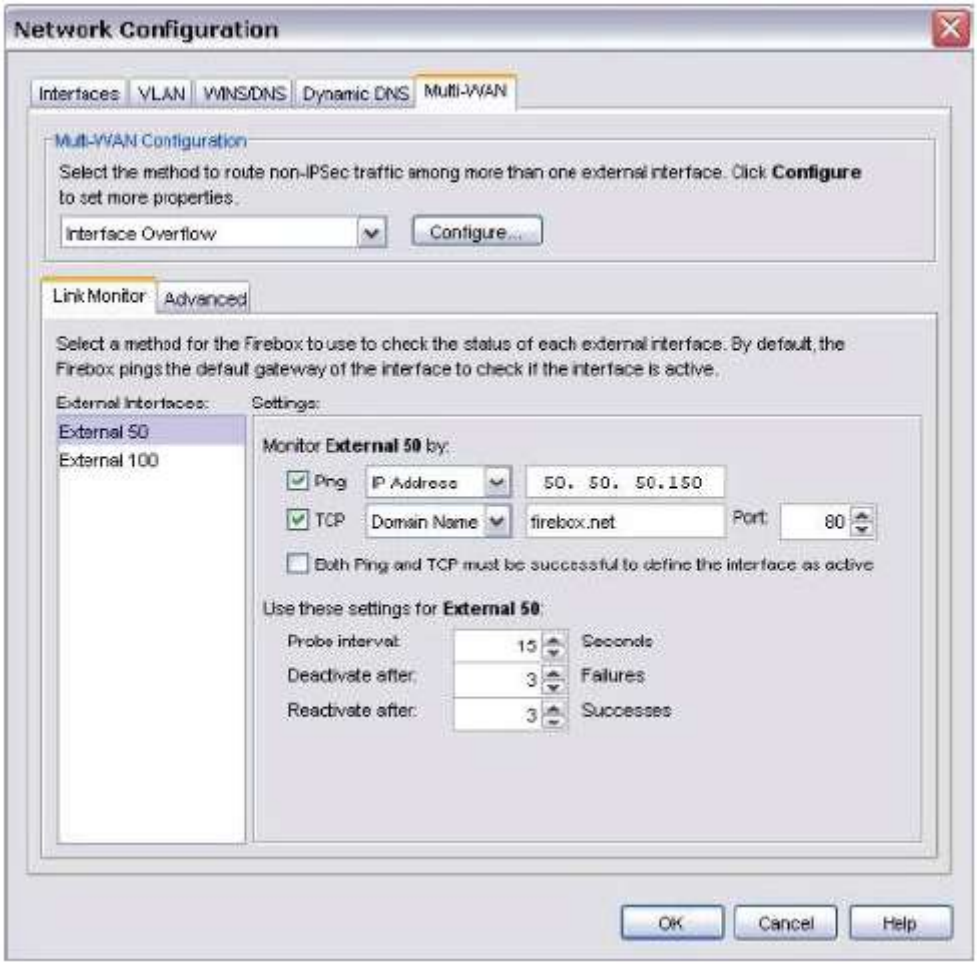
Вы можете настроить метод и частоту проверки устройством Firebox состояния каждого WAN интерфейса. По умолчанию Firebox шлет ping-запросы на шлюз по умолчанию интерфейса для проверки его состояния.

Время обновления таблицы маршрутизации Firebox

Если хост Link Monitor не отвечает, то может понадобится 40-60 секунд для устройства WatchGuard для обновления своей таблицы маршрутизации. Когда хост Link Monitor начинает снова отвечать на запросы, то устройству Firebox для обновления таблицы маршрутизации может понадобится от 1 до 60 секунд. Процесс обновления проходит значительно быстрее в случае если Firebox обнаруживает физическое отключение Ethernet порта. В этом случае WatchGuard устройство мгновенно обновляет свою таблицу маршрутизации. Если физическое подключение восстановлено, то Firebox в течение 20 секунд обновляет свою таблицу маршрутизации.

Создание хоста Link Monitor

1. В диалоговом окне **Network Configuration** выберите закладку **Multi-WAN**, и затем выберите закладку **Link Monitor**



2. В колонке **External Interface** выберите интерфейс. В поле **Settings** появится информация о выбранном интерфейсе

3. Выберите необходимый метод проверки состояния External интерфейса:

   * **Ping** — введите IP адрес или имя домена, на которые Firebox будет отправлять ping-запросы для проверки состояния интерфейса

   * **TCP** — введите IP адрес или имя домена компьютера, с которыми Firebox будет пытаться установить TCP соединение для проверки состояния WAN интерфейса.

   * **Both ping and TCP must be successful to define the interface as active** — Если ping-запрос и TCP-соединение были успешными, то лишь в этом случае интерфейс считается активным. Если External интерфейс входит в FireCluster, переключение multi-WAN failover, причиной которого стало отсутствие связи с хостом мониторинга подключения, не запускает процедуру переключения FireCluster. Переключение FireCluster происходит только в случае выхода из строя физического интерфейса или отсутствия связи с ним. Если вы добавили имя домена, на которое устройство Firebox будет отправлять ping-запросы, и хотя бы один из External интерфейсов имеет статический IP адрес, то вам необходимо настроить DNS сервер

4. В поле **Probe Interval** введите частоту проверки состояний интерфейсов.
   По умолчанию - 15 секунд.

5. В поле **Deactivate after** введите количество неудачных попыток проверки состояния интерфейсов, после чего запускается процедура переключения.

   По умолчанию – 3 попытки. После трех неудачных попыток Firebox начинает передавать трафик через следующий в списке multi-WAN failover интерфейс.

6. В поле **Reactivate after** введите количество удачных попыток проверки состояния интерфейса, после чего интерфейс считается активным.

7. Повторите все вышеуказанные пункты для каждого External интерфейса.

8. Нажмите **OK**

Глава 8 Трансляция сетевых адресов (NAT)

Трансляция сетевых адресов (NAT)

Трансляция сетевых адресов (NAT) – термин, который используется для описания различных преобразований IP-адреса и номера порта. На самом базовом уровне NAT меняет один IP-адрес на другой.

Основная цель NAT – увеличение числа компьютеров, которые могут работать с одним публичным маршрутизируемым адресом, и скрытие информации о внутренних адресах вашей сети. При использовании NAT IP-адрес источника изменяется для всех передаваемых пакетов

Вы можете использовать NAT как общую настройку брандмауэра или как настройку в политике. NAT настройки брандмауэра не используются в политиках BOVPN. Если у вас есть Fireware XTM Pro, то вы можете использовать функцию балансировки нагрузки сервера, как часть правила статической NAT. Балансировки нагрузки на сервер используется для увеличения производительности сети с несколькими публичными серверами и ее масштабируемости.

При помощи функции балансировки нагрузки вы можете управлять подключениями к определенному количеству серверов (максимум 10) для каждой политики брандмауэра. Устройство WatchGuard управляет нагрузкой в зависимости от количества активных сессий на каждом сервере. Устройство WatchGuard не измеряет и не сравнивает пропускную способность, используемую каждым сервером.

Более подробную информацию о балансировке нагрузки на север см. в “Настройка балансировки нагрузки на сервер”.

Типы NAT

Устройство WatchGuard поддерживает 3 типа NAT. Вы можете использовать одновременно несколько типов NAT. Вы можете использовать некоторые типы NAT для всего трафика брандмауэра, а остальные типы – как параметры в политике.

Динамическая NAT

Динамическая NAT так же известна, как IP-маскирование. Устройство WatchGuard может использовать свой публичный IP-адрес для исходящих пакетов на всех соединениях или для определённых сервисов. Это процедура скрывает реальный IP-адрес компьютера, который является источников пакетов во внешней сети. Динамическая NAT, как правило, используется для скрытия IP-адресов внутренних хостов, когда они получают доступ к публичным сервисам.

Более подробную информацию см. в “Динамическая NAT”

Статическая NAT

Статическая NAT, также известная как переадресация портов, настраивается во время настройки параметров политики. Статическая NAT это NAT-соединение «порт-хост». Хост отправляет пакет из внешней сети на порт внешнего интерфейса. Статическая NAT изменяет этот IP-адрес на IP-адрес и порт хоста, который находится за брандмауэром. Более подробную информацию см. в “Статическая NAT”.

1-to-1 NAT

1-to-1 NAT соотносит IP-адреса одной сети и IP-адреса другой сети. Это тип NAT часто используется для того, чтобы предоставить внешним компьютерам доступ к вашим публичным, внутренним серверам. Более подробную информацию см. в “1-to-1 NAT”.

Динамическая NAT

Динамическая NAT - наиболее часто используемый тип NAT. Происходит преобразование IP-адреса источника исходящего соединения в публичный IP-адрес Firebox. Вне Firebox в качестве IP адреса источника всех исходящих пакетов вы видите публичный IP-адрес External интерфейса устройства Firebox.

Многие компьютеры могут подключаться к Internet по одному публичному IP-адресу. Динамическая NAT обеспечивает высокий уровень безопасности внутренних хостов, которые подключаются к сети Интернет, так как при использовании динамической NAT реальные IP адреса хостов скрываются.

При использовании динамической NAT все подключения идут из внутренних сетей, подключенных к Firebox, тем самым хакеры не смогут подключиться к компьютерам во внутренней сети, так как они не знают их реальный IP адрес. В большинстве сетей политика безопасности рекомендуем использовать NAT для всех исходящих пакетов.

В Firebox динамическая NAT включена по умолчанию в диалоговом окне **Network > NAT.** Она так же включена по умолчанию в настройках всех создаваемых вами политик. Вы можете включить использование динамической NAT в отдельных политиках, не включая ее глобально для всего брандмауэра

Добавление записей динамической NAT

Конфигурация динамической NAT по умолчанию включает динамическую NAT для всех внутренних IP-адресов.

По умолчанию конфигурация NAT содержит следующие записи:

- 192.168.0.0/16 – любой внешний IP-адрес
- 172.16.0.0/12 – любой внешний IP-адрес
- 10.0.0.0/8 – любой внешний IP-адрес

Эти три сетевых адреса являются внутренними сетями, зарезервированными организацией Internet Engineering Task Force (IETF), и обычно используются для IP-адресов в локальной сети. Для того, чтобы включить динамическую NAT для других внутренних IP-адресов, вам необходимо добавить соответствующие записи в конфигурацию NAT.

Устройство WatchGuard использует правила динамической NAT в той последовательности, в которой они отображаются в списке записей динамической NAT. Мы рекомендуем использовать правила в зависимости от объема трафика, к которому эти правила применяются.

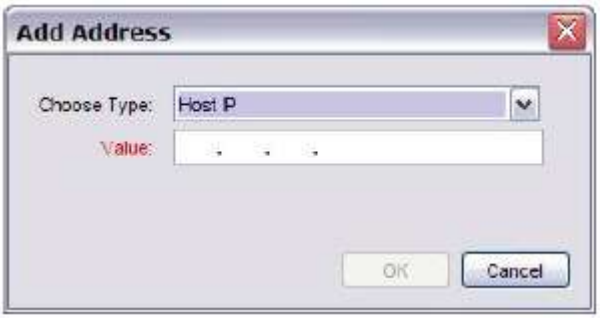
1. Выберите **Network > NAT**.
   Откроется диалоговое окно NAT Setup

2. В закладке **Dynamic NAT** нажмите **Add**.
   Откроется диалоговое окно Add Dynamic NAT

3. В выпадающем списке **From** выберите источник исходящих пакетов. Например, можно использовать доверенный псевдоним хоста для того чтобы включить NAT для трафика из всех Trusted сетей.

4. В выпадающем списке **To** выберите адрес назначения исходящих пакетов.

5. Для того, чтобы добавить IP-адрес хоста или сети, нажмите  .
   Откроется диалоговое окно Add Address



6. В выпадающем списке **Choose Type** выберите тип адреса.

7. В текстовом поле **Value** введите IP-адрес или диапазон IP-адресов. Вы должны ввести адрес сети в slash-нотации. При вводе IP-адреса, вводите все цифры и точки между ними. Не используйте клавиши TAB или клавиши со стрелками.

8. Нажмите **OK**.
   Новая запись появится в списке Dynamic NAT Entries.

Удаление записи о динамической NAT

Вы не можете изменять текущую запись динамической NAT. Если вы хотите изменить существующую запить, вы должны удалить запись и добавить одну новую. Для того, чтобы удалить запись о динамической NAT необходимо:

1. Выбрать запись для удаления.

2. Нажать **Remove**.
   Появится предупреждающее сообщение.

3. Нажмите **Yes**.

Упорядочивание записей динамической NAT

Для того, чтобы изменить порядок записей динамической NAT следует:

1. Выбрать запись для изменения.

2. Нажать **Up** или **Down** для перемещения их в списке.

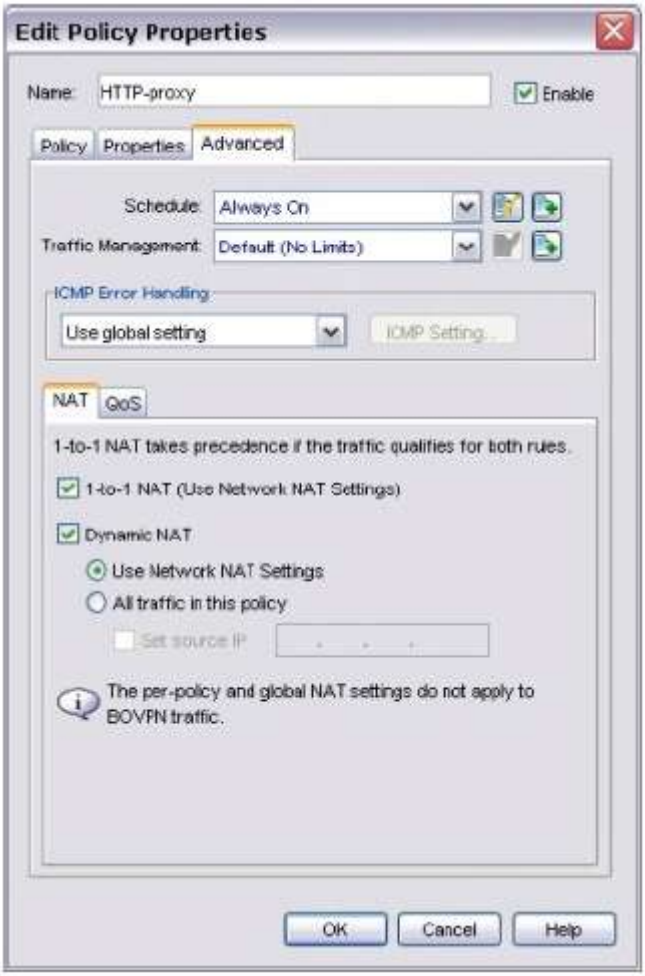
Настройка политике на основе динамической NAT

При использовании динамической NAT на базе политик Firebox преобразовывает внутренние IP-адреса в публичные. Динамическая NAT по умолчанию включена в настройках каждой политики, поэтому включать ее надо, только если вы до этого ее не выключали. Для корректной работы динамической NAT на базе политик используйте вам необходимо проверить в закладке **Policy** диалогового окна **Edit Policy Properties,** что исходящий трафик разрешен только через один интерфейс Firebox.

Правила NAT 1-to-1 имеют более высокий приоритет, чем правила динамической NAT.

1. Щелкните правой кнопкой мыши и выберите **Modify Policy**.
   Откроется диалоговое окно Edit Policy Properties.

2. Нажмите на закладку **Advanced**



3. Если вы хотите использовать правила динамической NAT, установленные на устройство WatchGuard, выберите **Use Network NAT Settings**. Если вы хотите применить NAT для всего трафика в политике, выберите **All traffic in this policy**.

4. Если вы выбрали **All traffic in this policy,** вы можете установить IP-адрес источника динамической NAT для любой политики, которая использует динамическую NAT. Включите опцию **Set source IP**. Если вы выберете IP-адрес источника, то этот в качестве IP адреса источника для всех исходящих пакетов будет использоваться специальный адрес из указанного вами диапазона внешних или публичных адресов. Это используется в основном в случае, когда необходимо чтобы исходящие SMTP пакеты в качестве IP адреса источника содержали адрес MX записи для вашего домена, так как IP адрес вашего External интерфейса и IP адрес вашей MX записи могут отличаться.
Этот адрес источника должен быть в той же подсети, что и указанный интерфейс, для исходящего трафика. Мы рекомендуем вам не использовать опцию **Set source IP** , если у вас не более одного внешнего интерфейса, настроенного на устройстве WatchGuard.

   Если вы не включите опцию **Set source IP,** устройство WatchGuard изменит IP-адрес источника для каждого пакета на IP-адрес интерфейса, с которого пакет передается во внешнюю сеть.

5. Нажмите **OK**.

6. Сохраните конфигурационный файл.

Отключение динамической NAT на базе политик

Динамическая NAT включена в настройки по умолчанию для каждой политики. Для того чтобы отключить динамическую NAT на базе политик выполните следующее:

1. Правой кнопкой мыши выбрать **Modify Policy**.
   Откроется диалоговое окно Edit Policy Properties.

2. Нажать на закладку **Advanced**.

3. Для отключения NAT на трафике, который управляется этой политикой, убрать флажок **Dynamic NAT.**

4. Нажать **OK**.

5. Сохранить конфигурационный файл.

1-to-1 NAT

При включении NAT 1-to-1 ваше устройство WatchGuard изменяет маршруты всех входящих и исходящих пакетов, отправленных с одного диапазона адресов на адреса из другого диапазона. Правило NAT 1-to-1 всегда имеет больший приоритет над динамической NAT.

1-to-1 NAT часто используется, когда у вас есть несколько внутренних серверов с внутренними IP адресами и вы хотите предоставить доступ к этим серверам из внешней сети. При помощи 1-to-1 NAT вы можете создать публичные IP-адреса, которые будут соответствовать внутренним адресам ваших серверов. При этом вам не надо менять IP-адрес ваших внутренних серверов. При наличии группы одинаковых серверов (например, группа серверов электронной почты), 1-to-1 NAT легче настраивается, чем статическая NAT для этой же группы серверов. Для того чтобы понимать, каким образом настраивается 1-to-1 NAT, рассмотрим пример:

У компании ABC есть несколько серверов электронной почты, подключенных к Trusted интерфейсу устройства WatchGuard. Серверы имеют следующие адреса:

10.1.1.1

10.1.1.2

10.1.1.3

10.1.1.4

10.1.1.5

Компания ABC выбирает 5 публичных IP-адресов из того же подсети, что и адрес External интерфейса. Затем прописывает эти адреса на DNS сервере.

Эти адреса следующие:

50.1.1.1

50.1.1.2

50.1.1.3

50.1.1.4

50.1.1.5

Затем компания ABC создает правило 1-to-1 NAT для своих серверов электронной почты. Правило 1-to-1 NAT строит статическую, двунаправленную связь между соответствующей парой IP-адресов. Эта связь выглядит следующим образом:

10.1.1.1 <--> 50.1.1.1

10.1.1.2 <--> 50.1.1.2

10.1.1.3 <--> 50.1.1.3

10.1.1.4 <--> 50.1.1.4

10.1.1.5 <--> 50.1.1.5

В то время, как правило1-to-1 NAT применяется, ваше устройство WatchGuard создает двунаправленный маршрутизацию и NAT-связь между пулом частных IP-адресов и пулом публичных адресов. 1-to-1 NAT так же работает при отправке трафика по сети, которую защищает ваше устройство WatchGuard.

1-to-1 NAT и VPNs

При создании VPN-туннеля сети на каждом конце VPN-туннеля, должны использоваться различные диапазоны сетевых адресов. Вы можете использовать 1-to-1 NAT, в том случае, когда необходимо создать VPN-туннель между двумя сетями, которые используют один и те же диапазоны внутренних адресов. Если диапазон внутренних адресов удаленной сети совпадает с диапазоном локальной сети, на обоих VPN шлюзах вам необходимо настроить 1-to-1 NAT.

1-to-1 NAT для VPN-туннеля настраивается при создании VPN-туннеля (не в диалоговом окне **Network > NAT)**

1. Выберите диапазон IP-адресов, который ваш компьютер будет использовать в качестве IP-адресов источника при передаче трафика из внутренней сети во внешнюю через BOVPN-туннель. Вам необходимо будет связаться с администратором удаленной сети, для того чтобы выбрать диапазон IP адресов, который на данный момент не задействован. Не используйте следующие адреса:

   * Адреса Trusted-, Optional- или внешней сетей, подключенных к вашему устройству

   * Вторичной сети, подключенной к Trusted-, Optional- или внешней сети, подключенной к вашему устройству

   * Маршрутизируемой сети, настроенной в Policy Manager (**Network > Routes**).

   * Сети, для которых же существуют BOVPN-туннели.

   * Пула адресов Mobile VPN пользователей.

   * Сети, доступ к которым IPSec-устройства могут получить через свои интерфейсы, маршруты и VPN-маршруты.

2. Выполните настройку локального и удаленного шлюзов на устройствах WatchGuard

3. Создайте туннели между шлюзами, которые являются конечными точками туннеля. В диалоговом окне **Tunnel Route Settings** для каждого устройства WatchGuard включите опцию **1:1 NAT** и введите маскированный диапазон IP-адресов для устройств WatchGuard. Количество IP-адресов в этом текстовом поле должно быть точно таким же, что и число IP-адресов в текстовом поле **Local** в верхней части диалогового окна. Например, если вы используете slash-нотацию для указания подсети, величина после «\» должна быть такой же, что и в обоих текстовых полях.

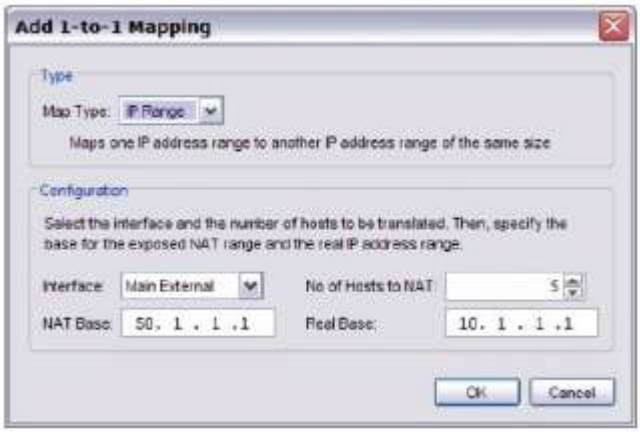
Для более подробной информации см. “1-to-1 NAT через BOVPN туннель”

Настройка 1-to-1 NAT в брандмауэре

1. Выберите **Network > NAT**.
   Откроется диалоговое окно NAT Setup.

2. Нажмите на закладку **1-to-1 NAT**.

3. Нажмите **Add**.
   Откроется диалоговое окно Add 1-to-1 Mapping



4. В выпадающем списке **Map Type** выберите **Single IP** (для одного хоста), **IP range** (для диапазона адресов) или **IP subnet** (для подсети). Если вы выберете **IP range** или **IP subnet,** то эта подсеть или диапазон не должны включать более 256 IP-адресов. Если ваш диапазон или подсеть содержит более 256 адресов, то вам необходимо создать дополнительные правила.

5. Заполните все поля в разделе **Configuration**. Для более подробной информации см. следующий раздел

6. Нажмите **OK**.

После того, как вы настроили глобальное правило 1-to-1 NAT, вы должны добавить IP-адреса NAT в соответствующие политики.

- Если ваша политика управляет исходящим трафиком, необходимо добавить Real Base IP-адрес в секцию **From** в настройках политики.

- Если ваша политика управляет входящим трафиком, добавьте NAT Base IP адрес в секцию **To** в настройках политики.

В предыдущем примере, где для обеспечения доступа к серверам электронной почты мы использовали 1-to-1 NAT, вам необходимо настроить политику SMTP, разрешающую SMTP трафик. Для того чтобы завершить процедуру настройки вам необходимо изменить параметры политики для того чтобы разрешить трафик из внешней сети на указанный диапазон IP-адресов 10.1.1.1- 10.1.1.5.

1. Создайте новую политику или откройте существующую политику.

2. Рядом со списком **From** нажмите **Add**.

3. Выберите псевдоним **Any-External** и нажмите **OK**.

4. Рядом со списком **To** нажмите **Add**. Нажмите **Add Other**.

5. Для того чтобы добавить IP-адреса выберите **Host IP** из выпадающего списка и введите IP-адрес в текстовое поле рядом со списком и нажмите **OK** дважды.

6. Повторите пункты 3-4 для каждого IP-адреса в диапазоне адресов NAT. Для добавления нескольких IP-адресов за один раз выберите **Host Range** в выпадающем списке. Введите первый и последний IP-адреса из диапазона базы NAT и нажмите **OK** дважды.

Для подключения к компьютеру, расположенному на другом интерфейсе и который использует 1-to-1 NAT, вам необходимо использовать публичный (NAT Base) адрес этого компьютера. Если это является проблемой, вы можете отключить 1-to-1 NAT и использовать статическую NAT.

Создание правила 1-to-1 NAT

Для каждого правила 1-to-1 NAT вы можете выбрать хост, диапазон хостов или подсеть. Вы также должны настроить следующие параметры:

Интерфейс

Название Ethernet-интерфейса, для которого применяется 1-to-1 NAT. Ваше устройство применяет 1-to-1 NAT для входящих и исходящих пакетов этого интерфейса. В примере выше правило применяется для внешнего интерфейса.

Базовый IP-адрес NAT

При настройке правила 1-to-1 NAT вам необходимо указать диапазон IP-адресов (диапазоны “**to**” и “**from**”). Базовый IP адрес NAT (NAT Base) это первый доступный IP-адрес в диапазоне “**to**”. Базовый IP-адрес NAT это адрес, на который меняется реальный базовый IP-адрес, при использовании 1-to-1 NAT. Вы не можете в качестве базового IP адреса NAT использовать адрес существующего интерфейса

В примере выше базовый IP-адрес NAT - 50.50.50.1.

Реальный базовый IP-адрес NAT

При настройке правила 1-to-1 NAT вам необходимо указать диапазон IP-адресов (диапазоны “**to**” и “**from**”). Реальный базовый IP-адрес NAT – это первый IP-адрес в диапазоне адресов «**from**». Этот IP-адрес присваивается физическому Ethernet-интерфейсу компьютера, для которого вы будете применять политику 1-to-1 NAT. Когда пакеты с интерфейса с реальным базовым IP-адресом NAT передаются через указанный интерфейс, к ним применяется политика 1-to-1.

В примере выше реальный базовый IP-адрес NAT - 10.0.1.50.

Количество хостов NAT (только для диапазонов)

Количество IP-адресов в диапазоне, для которых применяется правило 1-to-1 NAT. При применении 1-to-1 NAT первый реальный базовый IP-адрес меняется на первый базовый IP-адрес NAT. Второй реальный базовый IP-адрес в диапазоне меняется на второй базовый IP-адрес NAT. Это повторяется до тех пор, пока не будет достигнуто число, равное количеству хостов NAT. Выше в примере количество хостов равно пяти.

Вы можете так же использовать 1-to-1 NAT, при создании VPN-туннеля между двумя сетями, которые используют один и те же внутренние IP адреса. При создании VPN-туннелей сети на обоих концах VPN-туннеля должны использовать различные диапазоны IP адресов.

Если обе сети используют одинаковые диапазоны внутренних IP адресов, вы можете на обоих концах туннеля включить 1-to-1 NAT. Затем, вы можете создать VPN-туннель, не меняя внутренние IP-адреса обоих сетей

Настройка 1-to-1 NAT на базе политик

1-to-1 NAT на базе политик использует все настроенные диапазоны внутренних и внешних адреса, но правила 1-to-1 NAT применяются только в отдельных политиках. 1-to-1 NAT по умолчанию включен в настройках каждой политики. Если трафик совпадает с политиками 1-to-1 NAT и динамической NAT, то политика 1-to-1 NAT имеет более высокий приоритет.

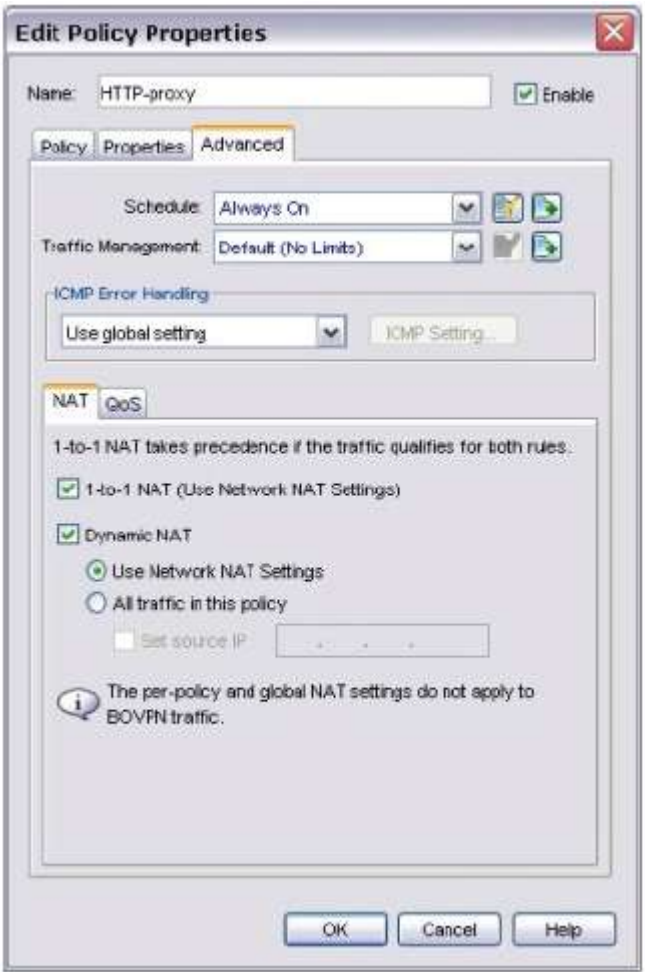
Включение политики, основанной на 1-to-1 NAT

Вам не надо предпринимать никаких действий для включения 1-to-1 NAT на базе политик, так как она включена по умолчанию во всех политиках. Если вы до этого отключали 1-to-1 NAT, то в п.3 вам необходимо включить опцию **1-to-1 NAT**.

Отключение 1-to-1 NAT на базе политик

1. Нажмите правой кнопкой мыши на политику и выберите **Modify Policy**.
   Откроется диалоговое окно Edit Policy Properties.

2. Выберите закладку **Advanced**



3. Отмените флажок **1-to-1 NAT** для того, чтобы отключить NAT для трафика, контролируемого этой политикой.

4. Нажмите **OK**. Сохраните конфигурационный файл.

Настройка NAT loopback с помощью статической NAT

Fireware XTM включает поддержку NAT loopback.

NAT loopback позволяет пользователям Trusted- или Optional-сетей получать доступ к публичному серверу, который подключен к тому же физическому интерфейсу

Для подключений через NAT loopback Firebox изменяет IP-адрес источника соединения на IP-адрес внутреннего интерфейса Firebox (основной IP-адрес для интерфейса, к которому подключенные и сервер, и клиент). Для того чтобы понять, как необходимо настраивать NAT loopback при использовании статической NAT, приведем следующий пример:

У компании ABC есть HTTP-сервер, который подключен к Trusted-интерфейсу Firebox. Компания использует правило 1-to-1 NAT, которое создает соответствие между публичным IP-адресом и внутренним адресом сервера. Компания хочет разрешить пользователям Trusted-сети подключаться к этому серверу, используя его публичный IP-адрес

В этом примере мы предполагаем:

- IP адрес Trusted-интерфейса - 10.0.1.0/24.
- Trusted-интерфейс так же имеет вторичный IP-адрес: 192.168.2.0/24.
- HTTP-сервер физически подключен к сети 10.0.1.0/24. Реальный базовый NAT адрес HTTP-сервера находится в Trusted сети

Добавление политики NAT loopback к серверу

Рассмотрим пример, позволяющий разрешить пользователям вашей trusted- и optional-сети использовать публичный IP-адрес или доменное имя для доступа к публичному серверу, подключенному к Trusted сети. Для этого вы должны добавить HTTP-политику, которая может выглядеть так:

From

- *Any-Trusted*
- *Any-Optional*

To

- *100.100.100.5 --> 10.0.1.5*

Раздел **To** политики содержит статический маршрут NAT от публичного IP-адреса HTTP-сервера к реальному IP-адресу сервера. Более подробную информацию о статической NAT см. в “Статическая NAT”. Если вы используете 1-to-1 NAT для маршрутизации трафика к серверам внутри вашей сети, см. “NAT loopback и 1-to-1 NAT”

NAT loopback и 1-to-1 NAT

NAT loopback позволяет пользователям trusted- и optional-сетей подключаться к публичному серверу со своим публичным IP-адресом или доменным именем, если сервер является физическим Firebox-интерфейсом.

Если вы используете 1-to-1 NAT для маршрутизации трафика к серверам внутренней сети, используйте эти инструкции для настройки NAT loopback от внутренних пользователей к тем серверам. Если вы не используйте 1-to-1 NAT, см. “Настройка NAT loopback с помощью статической NAT”

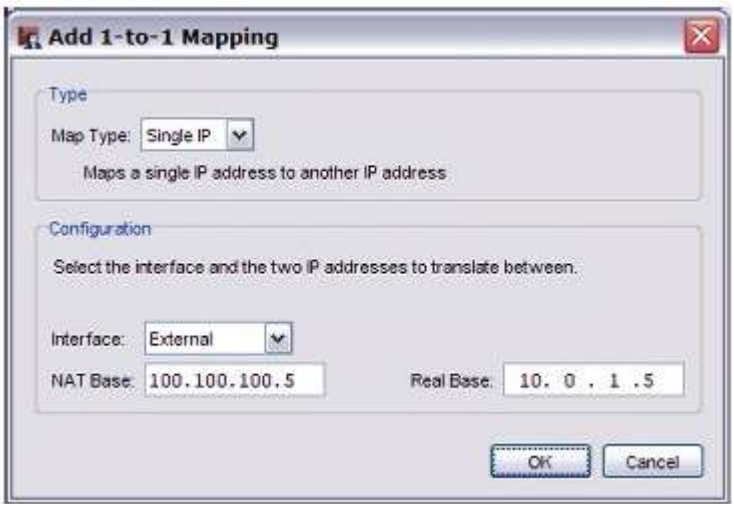
Для понимания, как происходит настройка NAT loopback при использовании 1-to-1 NAT, рассмотрим пример:

У компании ABC есть HTTP-сервер, подключенный к Trusted-интерфейсу устройства Firebox. Компания использует правило 1-to-1 NAT для преобразования публичного IP-адреса сервера в его внутренний адрес. Компания хочет разрешить пользователям, подключенным к trusted-интерфейсу использовать публичный IP-адрес или доменное имя для доступа к этому публичному серверу.

Для этого примера мы предполагаем:

- Сервер с публичным IP-адресом 100.100.100.5 привязан к определенному адресу из внутреннего диапазона. В закладке *1-to-1 NAT* диалогового окна *NAT Setup* выберите эти опции:

  интерфейс — **External**, NAT Base — **100.100.100.5**, Real Base — **10.0.1.5**

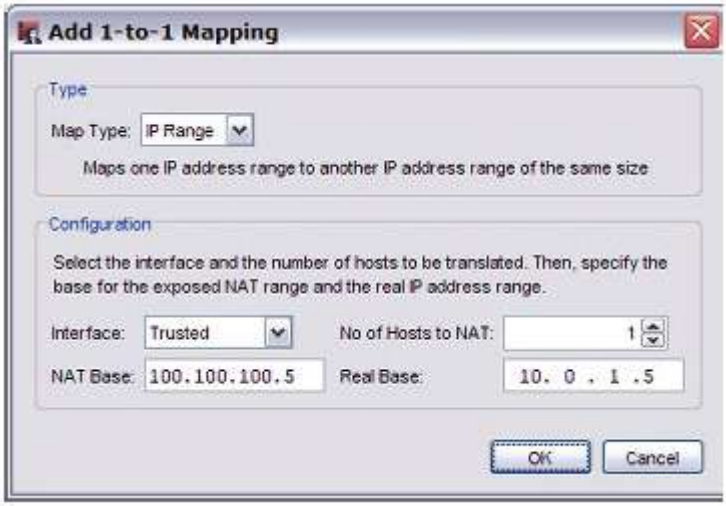


- Trusted-интерфейс настроен с основной сетью 10.0.1.0/24
- HTTP-сервер физически подключен к сети через Trusted интерфейс. **Real Base**-адрес хоста, который является trusted-интерфейсом.
- Trusted интерфейс так же настраивается со вторичной сетью 192.168.2.0/24.

В этом примере для того, чтобы включить NAT loopback для всех пользователей, подключенных к trusted-интерфейсу, следует:

1. Убедиться в том, что у вас есть записи 1-to-1 NAT для каждого интерфейса, через которые передается трафик, когда компьютеры внутренней сети пытаются получить доступ к публичному IP-адресу 100.100.100.5 через NAT loopback

   Вы должны добавить еще одно 1-to1 NAT соответствие для его применения к трафику, который передает Trusted-интерфейса. Новое 1-to-1 преобразование будет таким же, как и предыдущее, кроме параметра **Interface,** который устанавливается в **Trusted** вместо **External**.

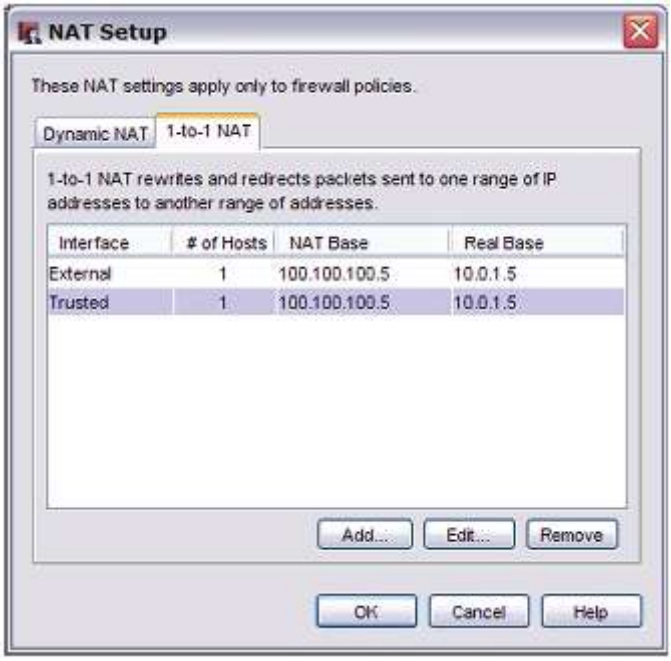


   После того, как вы добавили вторую запись 1-to-1 NAT, закладка **1-to-1 NAT** диалогового окна **NAT Setup** покажет два 1-to-1 NAT преобразования: одно – для External, другое – для Trusted интерфейсов.

   В закладке 1-to-1 NAT диалогового окна NAT Setup добавятся две записи:

   *Интерфейс — **External**, NAT Base — **100.100.100.5**, Real Base — **10.0.1.5***

*Интерфейс — **Trusted**, NAT Base — **100.100.100.5**, Real Base — **10.0.1.5***



2. Добавить запись динамической NAT для каждой сети на интерфейсе, к которому подключен сервер. Поле **From** для записи динамической NAT это сетевой IP-адрес сети, из которой компьютеры получают доступ к IP-адресу 1-to-1 NAT с NAT loopback. Поле **To** для записи динамической NAT это базовый адрес NAT в 1-to-1 NAT преобразовании. В этом примере к Trusted-интерфейсу подключено две сети, и вы хотите разрешить пользователям обоих сетей получать доступ к HTTP-серверу с публичным IP-адресом или именем хоста сервера. Вы должны добавить две записи динамической NAT.

   В закладке Dynamic NAT для настроек NAT (NAT Setup) добавьте:

   10.0.1.0/24 - 100.100.100.5

   192.168.2.0/24 - 100.100.100.5

3. Добавить политику для разрешения пользователям вашей trusted-сети использовать публичный IP-адрес или доменное имя для получения доступа к публичному серверу trusted-сети. Для этого примера:

   From

   Any-Trusted

   To

   100.100.100.5

   Публичный IP-адрес, к которому пользователи хотят подключиться - 100.100.100.5. Этот IP-адрес настраивается как вторичный IP-адрес на внешнем интерфейсе. В разделе **To** политики добавьте 100.100.100.5.

Более подробную информацию о конфигурации статической NAT см. в “Статическая NAT”

Более подробную информацию о том, как настроить 1-to-1 NAT, см. в “1-to-1 NAT”

Статическая NAT

Статическая NAT, так же известная как перенаправление портов, это NAT преобразование «порт-хост». Хост отправляет пакет от внешней сети на порт внешнего интерфейса.

Статическая NAT изменяет IP-адрес получателя на IP-адрес и порт за брандмауэром. Если программное приложение использует несколько портов или эти порты выбираются динамически,

то вам следует использовать 1-to-1 NAT или проверить прокси на вашем устройстве WatchGuard, которое управляет этим типом трафика.

Статическая NAT также применяется для трафика, передаваемого из сети, защищенной вашим WatchGuard устройством. При включении статической NAT вы используете внешний IP-адрес вашего Firebox . Вы можете делать это по своему усмотрению, либо потому, что ваш публичный сервер не имеет публичного IP-адреса. Например, вы можете подключить ваш SMTP сервер к вашему Firebox с внутренним IP-адресом и настроить статическую NAT в SMTP-политике. Ваше устройство WatchGuard устанавливает соединение на 25 порту и любой SMTP-трафик отправляется к реальному SMTP-серверу за Firebox.

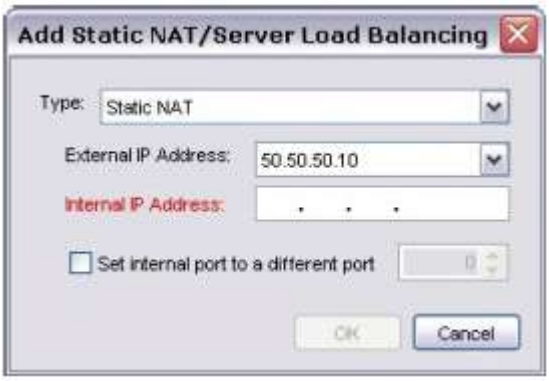
Настройка статической NAT

1. Откройте Policy Manager.

2. Два раза нажмите на политику

3. В выпадающем списке **Connections are** выберите **Allowed**. Для использования статической NAT политика должна разрешать входящий трафик.

4. Ниже списка **To** нажмите **Add.** Нажмите **Add NAT**.
   Откроется диалоговое окно Add Static NAT/Server Load Balancing



   *Статическая NAT доступная только для политик, которые используют заданный порт, включаяя TCP и UDP. Политика, которая использует различные протоколы, не может использовать входящую статическую NAT. Кнопка **NAT** в диалоговом окне **Properties** при настройке политики недоступна.Вы так же не можете использовать статическую NAT с политикой **Any.***

5. В выпадающем списке **Type** выберите **Static NAT**.

6. В выпадающем списке **External IP address** выберите внешний IP-адрес или псевдоним, который вы хотите использовать для этой политики. Например, вы можете применять статическую NAT для этой политики и пакетов, полученных только на одном внешнем IP-адресе. Или вы может использовать статическую NAT для пакетов, полученных на любом внешнем IP-адресе, если вы выберите псевдоним Any-External.

7. В поле **Internal IP Address** введите внутренний адрес. Этот адрес будет адресом назначения в Trusted- или Optional-сети.

8. Если необходимо, установите **Set internal port to a different port than this policy**. Это дает возможность осуществлять трансляцию «порт-адрес» (PAT). Существует возможность изменить получателя пакета не только на указанном хосту, но и на различных портах. Если вы выберете эту опцию, введите номер порта или используйте клавиши со стрелками вверх и вниз для выбора необходимого порта. Данный параметр обычно не используется.

9. Нажмите **OK** для того, чтобы закрыть диалоговое окно **Add Static NAT**.
   Откроется маршрут статической NAT в списке Members и Addresses.

10. Нажмите **OK** для того, чтобы закрыть диалоговое окно **Add Address**.

11. Нажмите **OK** для того, чтобы закрыть диалоговое окно **Policy Properties**.

Настройка балансировки нагрузки на сервер

Для того чтобы использовать балансировку нагрузки на сервер вам необходимо устройство Firebox X Core, Peak или WatchGuard XTM с установленным Fireware XTM Pro

Параметр балансировки нагрузки на сервер в Fireware XTM предназначен для увеличения масштабируемости и производительности высокоскоростной сети с несколькими публичными серверами. При балансировке нагрузки на сервер вы можете при помощи устройства WatchGuard проверять количество активных сессий на не более 10 публичных серверов для каждой политики. Устройство WatchGuard управляет нагрузкой в зависимости от количества активных сессий на каждый сервер

Устройство WatchGuard не измеряет и не сравнивает пропускную способность, которая используется каждым сервером. Вы настраиваете балансировку нагрузки на сервер как часть правила статической NAT. Устройство WatchGuard может балансировать подключения между вашими серверами посредством двух различных алгоритмов

При настройке балансировки нагрузки на сервер вы должны выбрать алгоритм, который будет применяться вашим устройством WatchGuard.

Round-robin

Если вы выберите эту опцию, ваше устройство распределит входящие сеансы между серверами, установленными в политике в циклическом порядке. Первое соединение отправляется на первый сервер, указанный в вашей политике. Следующее соединение отправляется на следующий сервер вашей политики и так далее.

Least Connection

Если вы выберите эту опцию, устройство WatchGuard будет отправлять каждое новое подключение к тому серверу в списке, который теперь имеет наименьшее количество открытых соединений с устройством. Устройство WatchGuard не может сообщить о количестве открытых соединений сервера с другими интерфейсами. Для балансировки нагрузки вы можете использовать специальные весовые коэффициенты интерфейсов. По умолчанию каждый интерфейс имеет весовой коэффициент равный «1». Весовой коэффициент распределяет пропорционально нагрузку между серверами

Если вы серверу присвоили весовой коэффициент равный «2» , то при этом вы увеличиваете в два раза количество сессий, которое будет перенаправлено на этот сервер

При настройке балансировки нагрузки на сервер важно знать:

- Вы можете настраивать балансировку нагрузки на сервер для любой политики, на которой применяется статическая NAT.
- Если вы применяете балансировку нагрузки на сервер для политики, вы не можете использовать маршрутизацию на базе политик и другие правила NAT в этой же политике.
- При использовании балансировки нагрузки на сервер вы можете добавить максимум 10 серверов для одной политики.
- Устройство WatchGuard не может изменять IP-адрес отправителя или источника для трафика, передаваемого на эти устройства. Несмотря на то, что трафик передается с устройства WatchGuard, каждый сервер, нагрузка на которые балансируется, видит реальный IP-адрес источника
- Если вы используете балансировку нагрузки на сервер в кластере «active/passive», то при переключении синхронизации в режиме реального времени не происходит

Когда резервное Master-устройство становиться активным master-устройством, оно перенаправляет все сессия на все серверы в списке балансировки нагрузки для того чтобы проверить их доступность

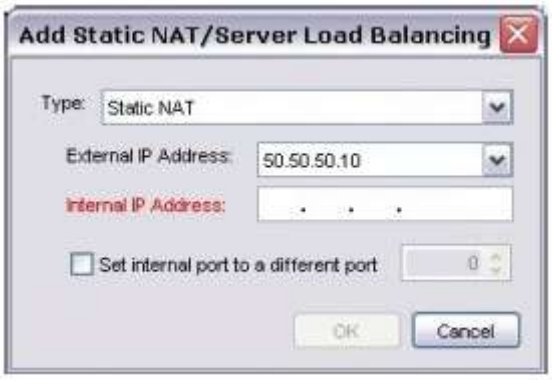
Затем применяется алгоритм балансировки нагрузки на сервер на всех доступных серверах.

Для того чтобы настроить балансировку нагрузки на сервер настройки балансировки нагрузки на сервере:

1. Дважды щелкните на политику, к которой вы хотите применить балансировку нагрузки на сервер. Или выделите политику и выберите **Edit > Modify Policy**. Для создания новой политики и включения балансировки нагрузки на сервер в этой политике выберите **Edit > Add Policy**

2. Ниже поля **To** нажмите **Add**.
Откроется диалоговое окно Add Address

3. Нажмите **Add NAT**.
Откроется диалоговое окно Add Static NAT/Server Load Balancing



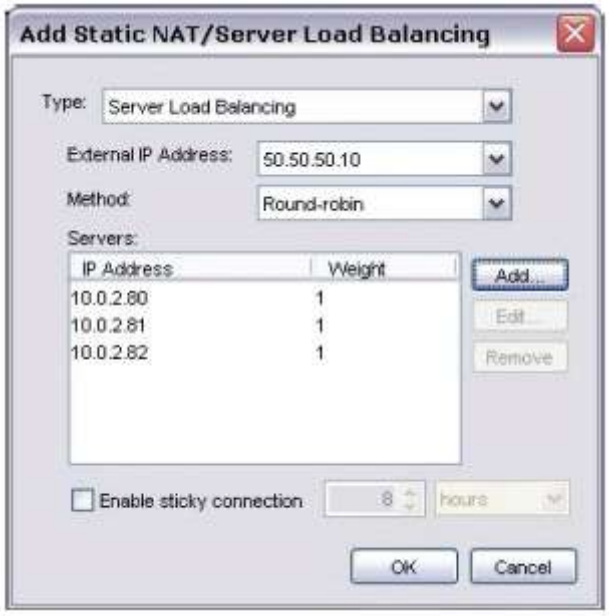
4. В выпадающем списке **Type** выберите **Server Load Balancing**

5. В выпадающем списке **External IP address** выберите внешний IP-адрес или псевдоним, который вы будете использовать для вашей политики. Например, вы можете использовать устройство WatchGuard для балансировки нагрузки на сервер для пакетов, полученных только на одном внешнем IP-адресе. Или вы можете использовать устройство WatchGuard для балансировки нагрузки на сервер к пакетам, полученных на любом внешнем IP-адресе, если вы выберите псевдоним **Any-External**.

6. В выпадающем списке **Method** выберите алгоритм, который будет использовать ваше устройство WatchGuard для балансировки нагрузки на сервер: **Round-robin** или **Least Connection**.

7. Нажмите **Add** для того чтобы добавить в политику IP-адреса внутренних серверов. Вы можете добавить максимум 10 серверов в одной политике. Вы можете так же присвоить серверу весовой коэффициент. По умолчанию весовой коэффициент каждого сервера равен «1». Весовой коэффициент используется для распределения нагрузки между серверами. Если вы серверу присвоите весовой коэффициент 2, то по сравнению с сервером с коэффициентом 1 это сервер может обслуживать в два раза больше соединений

8. Для настройки sticky-соединений для ваших внутренних серверов включите опцию **Enable sticky connection** и в соответствующих полях укажите их длительность**.** Sticky-соединение – это соединение, которое продолжает использовать тот же сервер в течение определенного периода времени. Параметр «прилипания» гарантирует, что все пакеты с источника в место назначения будут передаваться через один сервер в течение определенного промежутка времени



9. Нажмите **OK**.

10. Сохраните конфигурационный файл.

Глава 9 – Настройка беспроводной связи

Настройка беспроводной сети

Когда вы включаете беспроводную связь на устройстве WatchGuard, вы можете настроить внешний интерфейс для работы в беспроводной сети или можете настроить устройство WatchGuard, как беспроводную точку доступа для пользователей, подключенных к вашим Trusted-, Optional- или гостевым сетям. Перед тем, как приступить к настройка беспроводного доступа см. “Перед тем, как начать”

Для того чтобы включить поддержку беспроводной сети, вам необходимо получить ключ функций. Для более подробной информации см. в “Ключи функций (Feature Keys)”

Для включения функции беспроводной сети на вашем устройстве WatchGuard выполните следую выполнить:

1. Выберите **Network** > **Wireless**.
   Откроется диалоговое окно Wireless Configuration

2. Включите опцию **Enable wireless**.

3. В диалоговом окне **Wireless Configuration** выберите конфигурацию беспроводной сети:

   Enable wireless client as external interface.

   Если вы выберете эту конфигурацию, то вы можете настроить внешний интерфейс беспроводного устройства Watchguard для подключения к беспроводной сети. Это используется в областях с ограниченной или не существующей сетевой инфраструктурой

   Enable wireless access points

   Если вы выберете эту конфигурацию, вы можете настроить ваше беспроводное устройство

WatchGuard в качестве точки доступа для пользователей Trusted-, Optional- или гостевой сетей

4. В секции **Radio Settings** выберите ваш рабочий регион (**Operating Region**), канал (**Channel**) и режим беспроводной связи (**Wireless mode**). Более подробную информацию см. в «Радио-параметры беспроводной сети» на с. 182.

5. нажать **OK**.

Настройка беспроводной точки доступа

Любой беспроводное устройство WatchGuard может быть настроено как беспроводная точка доступа с тремя различными зонами безопасности. Вы можете разрешить другим беспроводным устройствам беспроводной сети подключаться к доверенной или опциональной зоне безопасности беспроводного устройства WatchGuard. Также для ващих пользователей вы можете включить беспроводную гостевую сеть. Компьютеры, которые подключаются к гостевой сети, подключаются через беспроводное устройство WatchGuard, но не имеют доступ к компьютерам Trusted- или Optional-сети.

Перед включением беспроводного устройства WatchGuard в качестве беспроводной точки доступа вы должны внимательно изучить пользователей беспроводной сети, которых подключаете к устройству, и определить уровень доступа, необходимый для каждого типа пользователей.

Существует 3 типа доступа к беспроводной сети:

Разрешение беспроводного подключения к Trusted-интерфейсу.

Когда вы разрешаете беспроводные подключения через *Trusted интерфейс ,то* беспроводные устройства имеют полный доступ ко всем компьютерам Trusted- и Optional-сетей и полный доступ в сеть Интернет на базе созданных вами правил. Если вы разрешаете доступ к беспроводной сети через Trusted-интерфейс, мы настоятельно рекомендуем включать и использовать ограничения по MAC-адресам для разрешения доступа через устройство WatchGuard только тем устройствам, которые добавлены в список разрешенных MAC адресов (**Allowed MAC Address**). Более подробную информацию об ограничении доступа по MAC-адресам см. в “Статическая привязка MAC адреса”

Разрешение беспроводного подключения к Optional-интерфейсу

При предоставлении беспроводного подключения через *Optional-интерфейс* беспроводные устройства имеют полный доступ ко всем компьютерам Optional сети и полный доступ в Internet на основе созданных вами правил исходящего доступа

Разрешения беспроводного гостевого подключения через External-интерфейс

Компьютеры, которые подключены к беспроводной гостевой сети, подключаются через устройство WatchGuard к сети Интернет на основе созданных вами правил исходящего доступа. Эти устройства не имеют доступ к компьютерам Trusted- и Optional-сетей. Более подробную информацию о конфигурировании беспроводной гостевой сети см. в “Включение беспроводной гостевой сети”. Для предоставления беспроводного соединения в вашей trusted- или optional-сети см. в “Разрешение беспроводных подключений к trusted- или optional-сети”

Перед тем, как начать

Беспроводные устройства WatchGuard соответствуют рекомендациям 802.11b и 802.11g Institute of Electrical and Electronics Engineers (IEEE).

При установке беспроводного устройства WatchGuard необходимо:

- Убедиться, что беспроводное устройство устанавливается на расстоянии более, чем 20 см от всех людей. Это рекомендации FCC для маломощных передатчиков.

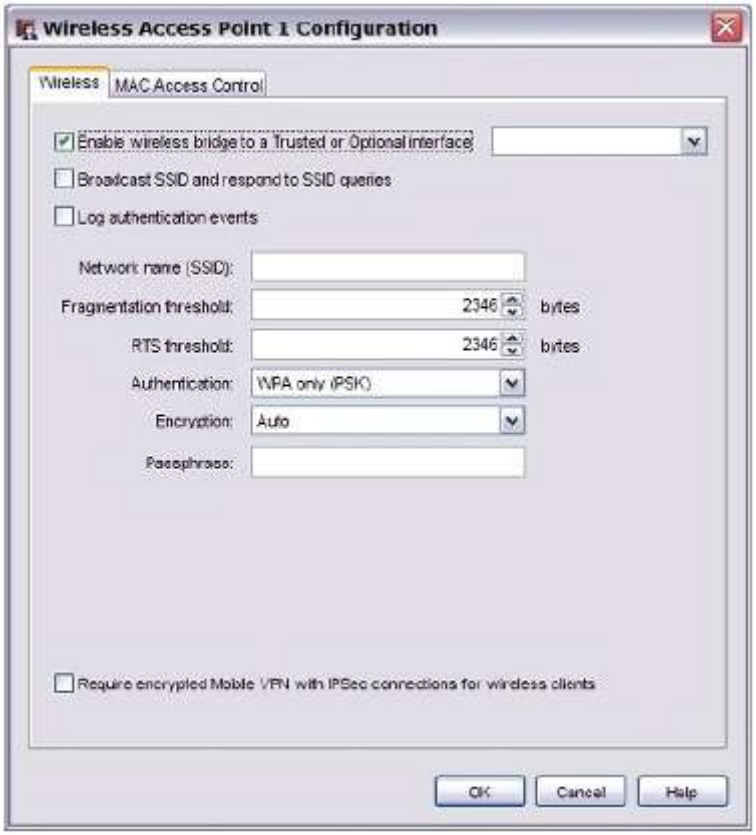
- Так же рекомендуется установить беспроводное устройство вдали от других антенн или передатчиков для уменьшения интерференции.

- По умолчанию беспроводной алгоритм аутентификации, настроенный на каждой зоне безопасности, является не самым надежным. Если беспроводные устройства, подключенные к вашему беспроводному устройству, могут корректно работать с WPA2, то мы рекомендуем его использовать

- Клиент беспроводной сети, подключенный к устройству WatchGuard из trusted- или optional-сети, может быть частью любого Branch Office VPN-туннеля, в котором локальный сетевой компонент настройки Phase 2, включает IP-адреса Trusted- или Optional сетей. Для управления доступом к VPN-туннелю вы можете заставить пользователя в обязательно порядке проходить процедуру аутентификации

Настройка параметров беспроводной сети

При предоставлении беспроводного доступа к Trusted-, Optional- или беспроводной гостевой сетям некоторые настройки устанавливаются одинаково для каждой из трех зон безопасности



Можно установить различные значения для каждой зоны. Более подробную информацию о настройках **Broadcast SSID and respond to SSID queries** см. “Включение/отключение SSID-рассылки”

Для более подробной информации об изменении **Network Name (SSID)** см. в “Изменение SSID”

Для более подробной информации о настройках **Log Authentication Events** см. в “Журнал событий аутентификации”

Для более подробной информации о **Fragmentation Threshold,** см. в “Изменение порогового значения фрагментации”

Для более подробной информации о **RTS Threshold** см. в “Изменение порогового значения RTS”

Более подробную информацию о настройках **Authentication** и **Encryption** см “Настройки безопасности беспроводной сети”

Включение/отключение SSID-рассылки

Компьютеры с картами беспроводной сети отправляют запросы для определения точек беспроводного доступа, к которым они подключены. Для того устройство WatchGuard отвечало на эти запросы включите опцию **Broadcast SSID and respond to SSID queries**. Для обеспечения безопасности включайте эту опцию только во время настройки компьютеров вашей сети для подключения к беспроводному устройству WatchGuard. Отключите эту опцию после того, как все клиентские настройки будет завершены.

Если вы используете беспроводные гостевые сервисы, то возможно понадобится разрешить SSID-рассылки в стандартном режиме.

Изменение SSID

SSID (Service Set Identifier) – это уникальное имя вашей беспроводной сети. Для использования беспроводной сети из компьютера клиента беспроводная сетевая карта должна иметь тот же SSID, что и беспроводное устройство WatchGuard .

Операционная система Fireware XTM автоматически назначает SSID каждой беспроводной сети. Этот SSID использует формат, содержащий имя интерфейса и 5-6 цифр из серийного номера Edge. При изменении SSID на Edge-интерфейсе введите новое имя в поле SSID для уникальной идентификации вашей беспроводной сети.

Журнал событий аутентификации

Событие аутентификации происходит, когда беспроводной компьютер пытается подключиться к беспроводному интерфейсу устройства WatchGuard. Для записи этого события в журнальный файл выберите опцию **Log Authentication Events**.

Изменение порогового значения фрагментации

Fireware XTM позволяет устанавливать максимальный размер кадра, который может отправить беспроводное устройство WatchGuard без его фрагментации. Это максимальный размер кадра называется пороговое значение фрагментации. Значение этого параметра меняется редко.

По умолчанию максимальный размер кадра – 2346, что означает все кадры будут передаваться без фрагментации. Это наиболее оптимальный вариант

Когда необходимо изменить пороговое значение фрагментации

Коллизии происходят в том случае, когда два устройства одновременно используют одну и ту же среду для передачи пакетов. Два пакета могут повредить друг друга и в результате образуется группа нечитаемых блоков данных. Если пакет образуется в результате коллизии, то он отбрасывается и передается снова. Происходит добавление информации к служебным данным сети и может уменьшиться пропускная способность и скорость в сети.

Более крупные пакеты чаще сталкиваются с другими, более мелкими кадрами. Для того чтобы уменьшить размер пакетов, передаваемых по сети, вам необходимо уменьшить пороговое значение фрагментации. При уменьшении размер кадра вы значительно уменьшите количество повторных отправок пакетов из-за возникающих коллизий, тем самым увеличив пропускную способность сети. Однако более мелкие кадры создают большую нагрузку на сеть.

Это особенно справедливо в беспроводных сетях, где каждый отправленный кадр должен быть обработан принимающим устройством, которое в свою очередь отправляет информацию передающему устройству о том, что пакет был успешно принят. Когда количество ошибок при передаче пакетов высоко (больше 5 или 10 процентов коллизий или ошибок), вы можете улучшить производительность беспроводной сети, уменьшив пороговое значение фрагментации

Уменьшение времени передачи данных за счет уменьшения количества повторных отправок пакетов, может быть достаточным для компенсации увеличившейся нагрузки на сеть из-за использования более мелких пакетов, что в свою очередь приведет к увеличению пропускной способности вашей сети

Если количество ошибок при передаче пакетов невелико, то уменьшив пороговое значение фрагментации вы снизите общую производительность вашей сети

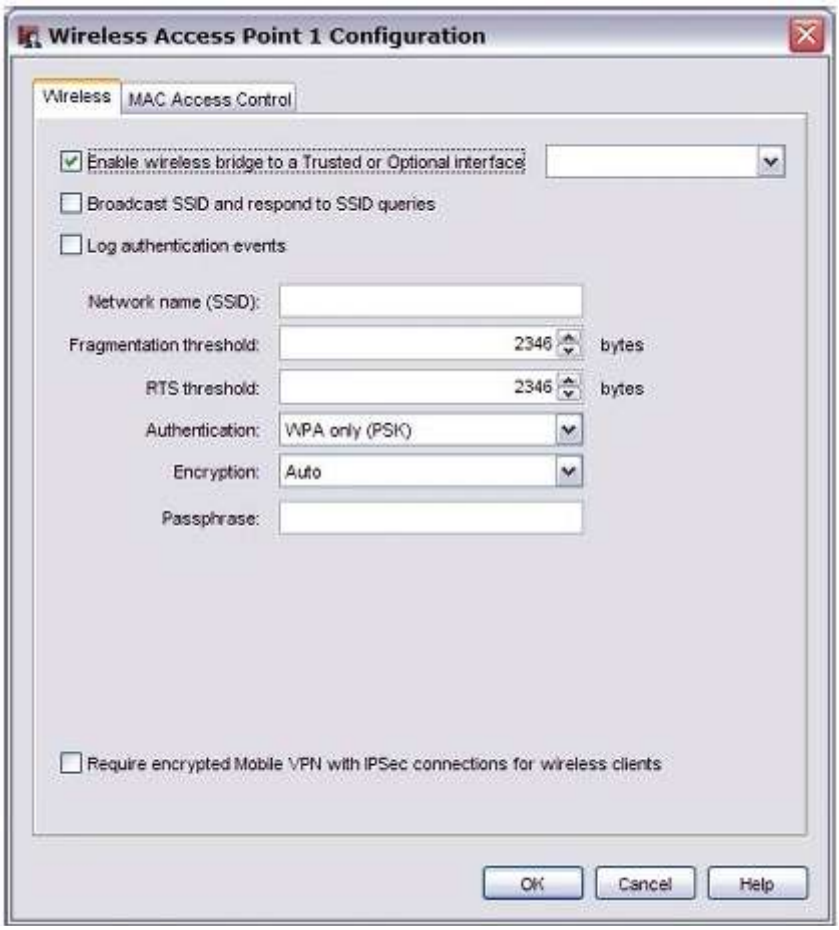
Если вы хотите поэкспериментировать, то мы рекомендуем начать с величины 2346 и постепенно ее уменьшать. Для получения более полной картины общей производительности системы мы рекомендуем выполнять мониторинг вашей сети несколько раз в день

Затем сравните эффект при большом количестве ошибок и при сравнительно небольшом их количестве. В общем, мы рекомендуем не изменять эту величину и оставить ее равной по умолчанию 2346

Изменение порогового значения фрагментации

1. Выберите **Network** > **Wireless**.

2. Выберите беспроводную сеть для настройки. Рядом с **Access point 1** или **Access point 2** или **Wireless Guest** нажмите **Configure**.
   Появится настройка беспроводной сети для данной беспроводной сети



3. Для изменения порогового значения фрагментации в текстовом поле **Fragmentation Threshold** введите или выберите значение между 256 и 2346.

4. Нажмите **OK**.

5. Сохраните конфигурацию.

Изменение порогового значения RTS

RTS/CTS (Request To Send / Clear To Send) помогает предотвратить проблемы, когда клиент беспроводной сети получает сигналы от более чем одной точки доступа беспроводной сети того же канала. Данную проблему называют *hidden node*.

Мы не рекомендует вам изменять значение порога RTS, заданное по умолчанию Когда **RTS Threshold** устанавливается в значение по умолчанию, равное 2346, RTS/CTS выключается. Если вы должны изменить пороговое значение RTS, делайте это постепенно. Уменьшайте только на небольшие величины за один раз. После каждого изменения в течение определенного промежутка наблюдайте работу вашей сети, и только на основе наблюдений принимайте решение, необходимо ли дальше уменьшать ли эту величину

Если вы намного уменьшили эту величину, вы можете внести большую задержку в сеть, как *Requests to Send* увеличивается настолько, что общая среда резервируется чаще, чем это необходимо.

Настройки безопасности беспроводной сети

Беспроводное устройство WatchGuard использует 3 протокола безопасности, стандартизованные для защиты вашей беспроводной сети: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), and WPA2.

Каждый стандарт протокола используется для шифрования данных, передаваемых по беспроводной сети

Они так же могут предотвращать несанкционированный доступ к точкам доступа беспроводной сети. WEP и WPA используют pre-shared- ключи. WPA и WPA2 используют алгоритм для изменения ключа шифрования в определенные интервалы, которые сохраняют данные, отравляемые беспроводным подключением, более защищенными.

Для защиты конфиденциальности вы можете использовать эти функции вместе с другими механизмами защите локальной сети, такими как защита пароля, VPN-туннели и пользовательская аутентификация.

Выбор алгоритма аутентификации для беспроводной сети

В Firebox X Edge e-Series Wireless существуют пять методов аутентификации.

Мы рекомендуем вам использовать WPA2, поскольку он является наиболее безопасным.

Пять доступных методов (от менее безопасных к более):

Открытая система

Открытая система аутентификации позволяет любому пользователю проводить аутентификацию в точке доступа. Этот метод может использоваться без шифрования или с WEP -шифрованием.

Общие ключи

При аутентификации с использованием общих ключей могут подключаться только те клиенты беспроводной сети, которые имеют общий ключ. Общий ключ аутентификации может использоваться только с WEP-шифрованием.

Только WPA (PSK)

При использовании WPA (Wi-Fi Protected Access) с pre-shared-ключами каждому клиенту беспроводной сети выдается одинаковый пароль для аутентификации в точке доступа.

WPA/WPA2 (PSK)

При использовании WPA/WPA2 (PSK) аутентификации Edge принимает подключения от беспроводных устройств, настроенных для использования WPA или WPA2.

Только WPA2 (PSK)

WPA2-аутентификация с pre-shared-ключами реализует полный стандарт 802.11i и является наиболее безопасным методом аутентификации.

Выбор уровня шифрования

В выпадающем списке **Encryption** выберите уровень шифрования для ваших беспроводных подключений. Изменение параметров происходит при использовании различных механизмов аутентификации. Операционная система Fireware XTM автоматически создает случайный ключ шифрования, когда вам необходимо его использовать. Вы может использовать этот ключ или изменить его на другой.

Каждый клиент беспроводной сети должен использовать одинаковый ключ при подключении к устройству WatchGuard.

Открытая система и общие ключи шифрования

Параметры шифрования для открытых систем и общие ключи аутентификации - WEP 64-битные шестнадцатеричные, WEP 40-битные ASCII, WEP 128-битные шестнадцатеричные, и WEP 128-битные ASCII.

Если вы выбираете открытую систему аутентификации, то вы можете так же выбрать *no encryption*.

1. Если вы используете WEP-шифрование в текстовых полях **Key** введите значение в шестнадцатеричном или ASCII виде. Не все беспроводные адаптеры поддерживают символы ASCII. Вы можете иметь максимум 4 ключа.

   * WEP 64-битный шестнадцатеричный ключ должен состоять 10 шестнадцатеричных символов (0-f)

   * WEP 40-битный ASCII ключ должен состоять из 5 символов.

   * WEP 128-битный шестнадцатеричный ключ должен состоять из 26 шестнадцатеричных символов (0-f).

   * WEP 128-битный ASCII ключ должен состоять 13 символов.

2. Если вы ввели несколько ключей, в выпадающем списке **Key Index** выберите ключ, который будет использоваться в качестве ключа по умолчанию. Беспроводное устройство WatchGuard может использовать одновременно только один ключ.

Если вы выберите ключ, отличный от первого в списке, вы должны установить клиента беспроводной сети для использования этого же ключа.

WPA и WPA2 PSK аутентификация

Параметрами шифрования для WPA-PSK и WPA2-PSK аутентификации являются **TKIP**, **AES**, и **Auto**. Рекомендуется устанавливать опцию шифрования в **Auto** для того, чтобы беспроводное устройство WatchGuard имело доступ к настройкам TKIP и AES.

Разрешение беспроводных подключений к trusted- или optional-сети

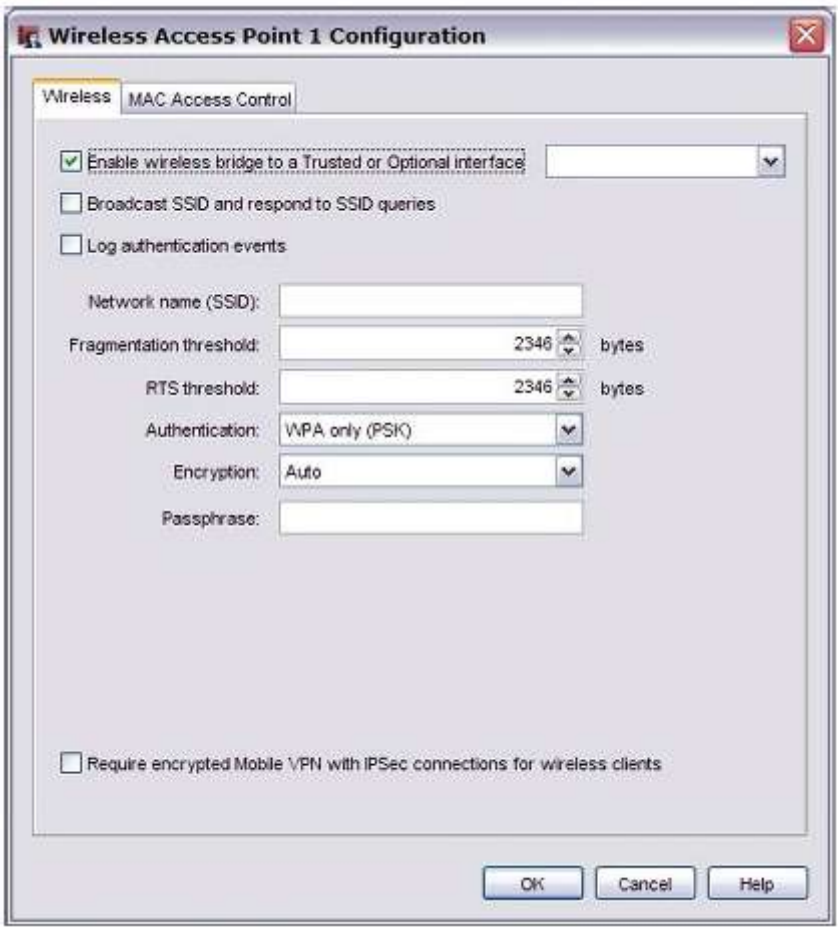
Для обеспечения беспроводных подключений к trusted- или optional-сети:

1. Выберите **Network** > **Wireless**.
   Откроется диалоговое окно Configuration

2. Выберите опцию **Enable wireless**.

3. Выберите **Enable wireless access points**.

4. Рядом с **Access point 1** или **Access point 2** нажмите **Configure**.
   Откроется диалоговое окно Wireless Access Point



5. Выберите опцию **Enable wireless bridge to a Trusted or Optional interface**.

6. В выпадающем списке рядом с **Enable wireless bridge to a Trusted or Optional interface** выберите trusted- или optional-интерфейс.

   Trusted

   Любые клиенты беспроводной сети в trusted-сети имеют полный доступ к компьютерам trusted- или optional-сети и доступ к Internet, как это определено в исходящих правилах брандмауэра на вашем устройстве WatchGuard. Если клиент беспроводной сети получает IP-адрес при помощи DHCP, то вам необходимо настроить и включить DHCP сервер в вашей Optional сети

   Optional

   Любой клиент беспроводной optional-сети имеет полный доступ к компьютерам этой сети и к сети Интернет как это определено в исходящих правилах брандмауэра на вашем устройстве WatchGuard. Если клиент беспроводной сети получает IP-адрес при помощи DHCP, то вам необходимо настроить и включить DHCP сервер в вашей Optional сети

7. При настройке беспроводного интерфейса для отправки и ответов на SSID-запросы включите опцию **Broadcast SSID and respond to SSID queries**. Более подробную информацию об этих настройках см. в “Включение/отключение SSID-рассылки”

8. Выберите опции **Log Authentication Events** если вы хотите, чтобы устройство WatchGuard отправляло сообщения в файл журнала каждый раз, когда беспроводной компьютер подключается к интерфейсу. Более подробную информацию о записи в журнал см. в “Журнал событий аутентификации”

9. При необходимости пользователей беспроводной сети использовать Mobile VPN с IPSec-клиентом выберите опцию **Require encrypted Mobile VPN with IPSec connections for**

wireless clients. При выборе этой опции только пакетам Firebox разрешается передавать по беспроводной сети DHCP, ICMP, IKE (UDP порт 500), ARP и IPSec (IP протокол 50). Если вам необходимо, чтобы пользователи беспроводной сети использовали Mobile VPN с IPSec-клиентом, то для увеличения безопасности клиентов беспроводной сети не рекомендуется использовать WPA или WPA2 в качестве методов аутентификации в беспроводной сети.

10. В текстовом поле **Network name (SSID**) введите уникальное имя для беспроводной optional-сети или используйте имя по умолчанию. Более подробную информацию об изменении SSID см. в "Изменение SSID"

11. Для изменения порогового значения фрагментации в текстовом окне **Fragmentation Threshold** введите значение от 256 до 2346. Мы не рекомендуем изменять эти настройку. Более подробную информацию об этих настройках см. в "Изменение порогового значения фрагментации"

12. В выпадающем списке **Authentication** выберите тип аутентификации для включения беспроводных соединений с optional-интерфейсом. Мы рекомендуем вам использовать WPA2, если беспроводное устройство в вашей сети может поддерживать WPA2. Более подробную информацию об этой настройки см. в "Выбор алгоритма аутентификации для беспроводной сети"

13. В выпадающем списке **Encryption** выберите тип шифрования для использования беспроводного подключения и добавьте ключи или пароли, необходимые для выбранного типа шифрования. Если вы выберете параметры шифрования с pre-shared-ключами, то он будет создан случайным образом для вас. Мы можете использовать этот ключ или свой собственный. Более подробную информацию см. в "Выбор уровня шифрования"

14. Сохраните конфигурационный файл. Для настройки гостевой беспроводной сети без доступа к компьютерам вашей trusted- или optional-сетей см. "Включение беспроводной гостевой сети"

При активации беспроводных подключений на trusted-интерфейсе мы рекомендуем ограничить доступ по MAC-адресам. Это предотвратит подключение пользователей, соединенных с беспроводном устройством WatchGuard, от несанкционированных компьютеров, которые могут содержать вирусы или spyware. Нажмите на закладку ***MAC Access Control*** *для включения контроля по MAC-адресам. Вы можете использовать эту закладку так же в том случае, когда вы ограничиваете сетевой трафик на интерфейсе, как описано в restrict network traffic by MAC address.*

Включение беспроводной гостевой сети

Вы можете активировать беспроводную гостевую сети для предоставления доступа гостевым пользователям беспроводной сети к Internet без доступа к компьютерам вашей trusted- и optional-сети.

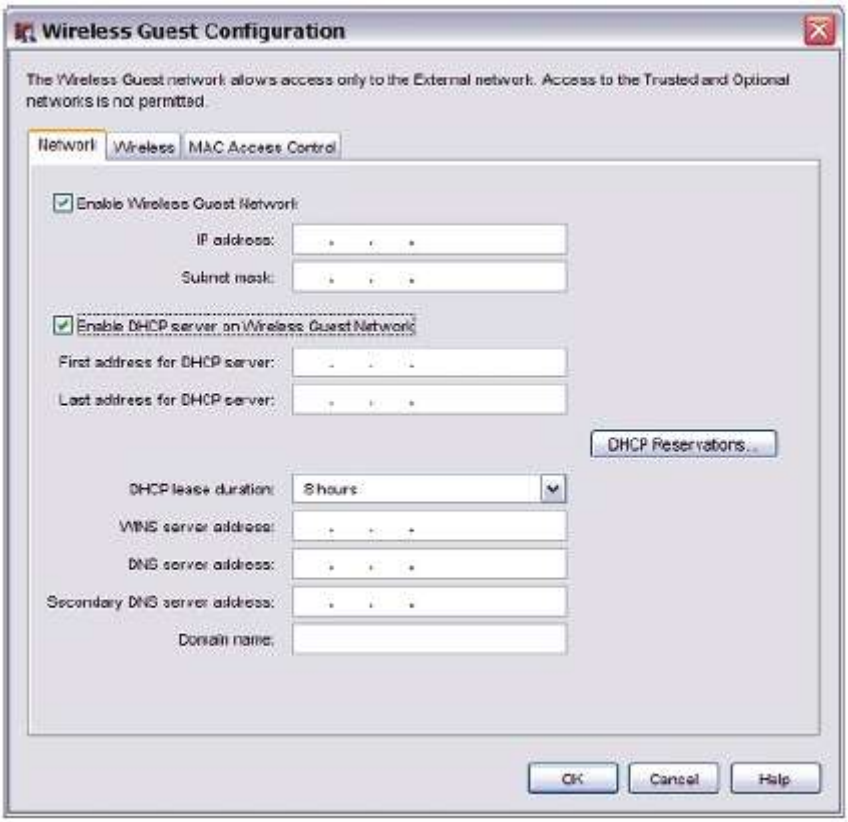
Для установки беспроводной гостевой сети:

1. Выберите **Network > Wireless**.
   Откроется диалоговое окно Wireless Configuration

2. Выберите опцию **Enable wireless**.

3. Выберите **Enable wireless access points**.

4. Рядом с **Wireless guest** нажмите **Configure**.
   Откроется диалоговое окно Wireless Guest Configuration



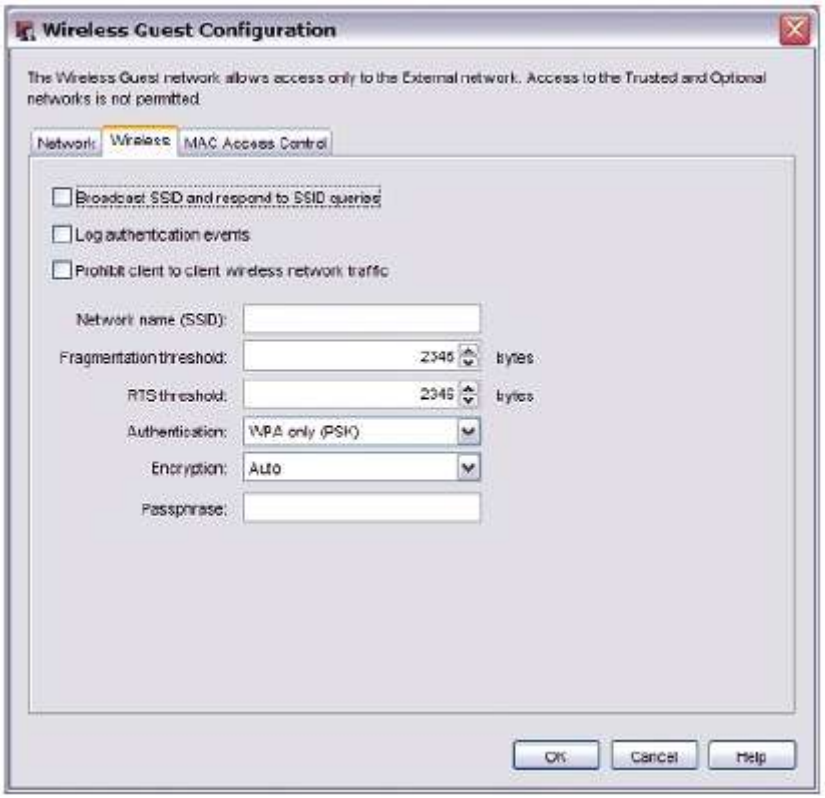
5. Выберите опцию **Enable Wireless Guest Network**. Беспроводные соединения разрешены через устройство WatchGuard к Internet на основе правил, настроенных для исходящего доступа на вашем устройстве. Эти компьютера не имеют доступа к компьютерам trusted- или optional-сети.

6. В текстовом поле **IP Address** введите частный IP-адрес для использования в беспроводной гостевой сети. Это IP-адрес не должен использоваться на каком-либо из сетевых интерфейсов.

7. В текстовом поле **Subnet Mask** введите маску подсети. Обычно используют маску 255.255.255.0.

8. Для настройки устройства WatchGuard в качестве DHCP-сервера, когда беспроводное устройство пытается создать подключение, выберите опцию **Enable DHCP Server on Wireless Guest Network**

9. Нажмите на закладку **Wireless**, чтобы просмотреть настройки безопасности для беспроводной гостевой сети.
Откроются настройки Wireless



10. Выберите опцию **Broadcast SSID and respond to SSID queries** для создания имени вашей беспроводной гостевой сети, которое будут видеть пользователи-гости

11. Для отправки сообщения в файл журнала каждый раз, когда компьютер беспроводной сети пытается подключиться к гостевой беспроводной сети, выберите опцию **Log Authentication Events**

12. Для разрешения пользователям-гостям беспроводной сети отправлять трафик друг другу отключите опцию **Prohibit client to client wireless network traffic**.

13. В текстовом поле **Network name (SSID**) введите уникальное имя для вашей гостевой беспроводной сети или используйте имя по умолчанию

14. Для изменения порогового значения фрагментации в текстовом поле **Fragmentation Threshold** введите значение от 256 до 2346. Мы не рекомендует изменять эти настройки.

15. В выпадающем списке **Authentication** выберите тип аутентификации для включения соединений к беспроводной гостевой сети. Настройка, которую вы выбираете, зависит от типа предоставляемого доступа гостям и того, требуется ли гостям вашей сети применять пароль для использования сети

16. В выпадающем списке **Encryption** выберите тип шифрования, используемый для беспроводного подключения, и добавьте ключи или пароли, необходимые для выбранного типа шифрования. Если вы выберите опцию шифрования с pre-shared-ключами, то он будет сгенерирован для вас случайным образом. Вы можете использовать этот ключ или ввести свой собственный

17. Нажмите **OK**.

18. Сохраните конфигурационный файл.

Вы так же можете ограничить доступ к гостевой сети по MAC-адресам. Нажмите на закладку **MAC Access Control** для включения контроля по MAC-адресам. Вы можете использовать эту закладку в том случае, когда ограничиваете сетевой трафик на интерфейсе

Настройка вашего external-интерфейса в качестве беспроводного интерфейса

В области с ограниченной или не существующей сетевой инфраструктурой вы можете использовать ваше беспроводное устройство WatchGuard для обеспечения безопасного сетевого доступа. Вы должны физически подключить ваши сетевые устройства к устройству WatchGuard. Затем необходимо настроить external-интерфейс для подключения в беспроводной точке доступа, которая соединена с более крупной сетью.

Когда external-интерфейс настроен на работу с беспроводным подключением, устройство WatchGuard не может долго использоваться в качестве точки доступа к беспроводной сети. Для обеспечения доступа к беспроводной сети пользователей подключите беспроводную точку доступа к беспроводному устройству WatchGuard.

Настройка основного external-интерфейс в качестве беспроводного интерфейса

1. Выберите **Network** > **Wireless**.
   Откроется диалоговое окно Wireless Configuration

2. Выберите опцию **Enable wireless**.

3. Выберите **Enable wireless client as external interface**.

4. Нажмите **Configure**.
Откроются настройки external-интерфейса.

5. В выпадающем списке **Configuration Mode** выберите опцию:

Manual Configuration

Для использования статического IP-адреса выберите данную опцию. Введите **IP Address**, **Subnet Mask**, and **Default Gateway**.

DHCP Client

Данная опция используется для настройки external-интерфейса в качестве DHCP-клиента. Введите необходимые параметры DHCP.

6. Нажмите на закладку **Wireless**.
   Откроется диалоговое окно настройки клиента беспроводной сети

7. В текстовом поле **Network name (SSID)** введите уникальное имя для вашей беспроводной external-сети.

8. В выпадающем списке **Authentication** выберите тип аутентификации для включения беспроводных соединений. Мы рекомендуем использовать WPA2, если беспроводные устройства в вашей сети могут его поддерживать

9. В выпадающем списке **Encryption** выберите тип шифрования для использования беспроводного подключения и добавьте ключи или пароли, необходимые для выбранного типа аутентификации. Если вы выберете параметры шифрования с pre-shared-ключами, то он будет создан случайным образом для вас. Мы можете использовать этот ключ или свой собственный.

10. Нажмите **OK**.

Настройка BOVPN-туннеля для дополнительной безопасности

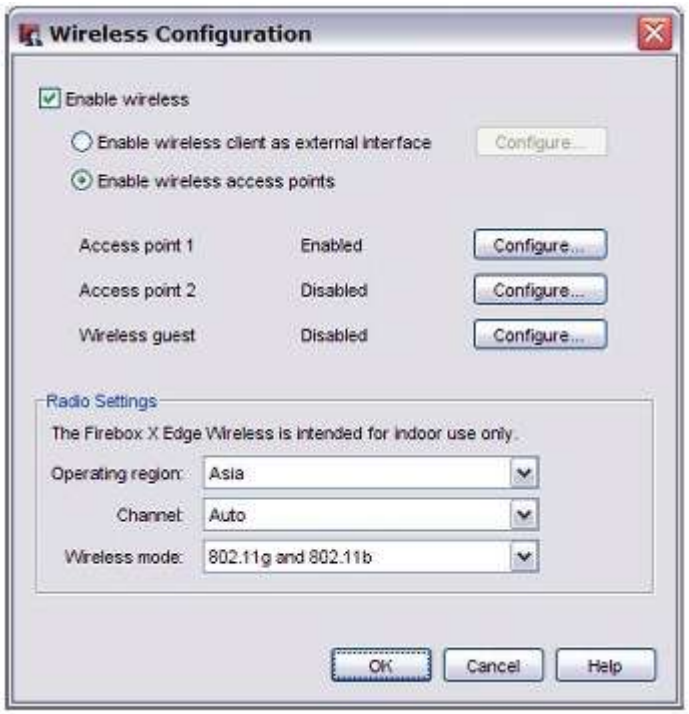
Для создания беспроводного моста и обеспечения дополнительной безопасности добавьте BOVPN-туннель между вашим устройством WatchGuard и внешним шлюзом. Вы должны установить режим **Aggressive Mode** на первой стадии настроек вашей BOVPN-конфигурации на обоих устройствах. Более подробную информацию об установке BOVPN-туннеле см. в “About manual BOVPN tunnels” на с. 736.

Радио-параметры беспроводной сети

Беспроводные устройства WatchGuard используют радиочастотные сигналы для отправки и принятия трафика от компьютеров с беспроводными Ethernet-картами. Некоторые настройки определены для выбора канала. Для отображения или изменения радио-настроек необходимо:

1. Открыть Policy Manager.

2. Выбрать **Network** > **Wireless**.



Radio Settings отображаются в нижней части диалогового окна

Установка рабочего диапазона и канала

При активации беспроводной сети вы должны установить беспроводной рабочий диапазон.

1. В выпадающем списке **Operating region** выберите рабочий диапазон, который лучше всего описывает расположение вашего устройства. Этот список беспроводных рабочих диапазонов, которые вы можете выбрать на Firebox, может быть различным, в зависимости от того, где вы приобрели его.

2. В выпадающем списке **Channel** выберите канал или выберите **Auto**. Если вы установите канал **Auto,** беспроводное устройство WatchGuard автоматически выберет канал с самым сильным сигналом, доступным в этом местоположении.

В связи с нормативными требованиями в различных частях мира не все беспроводные каналы доступны в каждом регионе.

Эта таблица включает каналы, поддерживаемые Firebox X Edge Wireless и доступные для каждого беспроводного региона

Канал	Центр. Частота, МГц	Америка	Азия	Австралия & H.3	EMEA	France	Израиль	Япония	Тайвань	Китай
1	2412	Да	Да	Да	Да			Да	Да	Да
2	2417	Да	Да	Да	Да			Да	Да	Да
3	2422	Да	Да	Да	Да		Да	Да	Да	Да

4	2427	Да	Да	Да	Да		Да	Да	Да	Да
5	2432	Да	Да	Да	Да		Да	Да	Да	Да
6	2437	Да	Да	Да	Да		Да	Да	Да	Да
7	2442	Да	Да	Да	Да		Да	Да	Да	Да
8	2447	Да	Да	Да	Да		Да	Да	Да	Да
9	2452	Да	Да	Да	Да		Да	Да	Да	Да
10	2457	Да	Да	Да	Да	Да		Да	Да	Да
11	2462	Да	Да	Да	Да	Да		Да	Да	Да
12	2467	Да	Да	Да	Да	Да		Да	Да	Да
13	2472	Да	Да	Да	Да	Да		Да	Да	Да
14	2484							Да		

Установка беспроводного режима работы

Большинство беспроводных карт работают только в режиме 802.11b (до 11 Мб/с) или 802.11g (54 МБ/с). Для установки рабочего режима на беспроводном устройстве WatchGuard выберите опцию в выпадающем списке **Wireless Mode**.

Существует 3 беспроводных режима:

Только 802.11b

Этот режим ограничивает беспроводное устройство WatchGuard для подключения к устройствам только в режиме 802.11b.

Только 802.11g

Этот режим ограничивает беспроводное устройство WatchGuard для подключения к устройствам только в режиме 802.11g.

802.11g и 802.11b

Этот режим активирован по умолчанию и является рекомендуемой настройкой. Этот режим позволяет устройству WatchGuard подключаться к устройствам, которые используют 802.11b или 802.11g. Устройство WatchGuard работает в режиме 802.11g, только если все беспроводные карты, подключенные к устройству, используют 802.11g. Если любой клиент, использующий 802.11g, подключен к устройству, то все соединения автоматически переводятся в режим 802.11b.

Настройка карты беспроводной сети на вашем компьютере

Эти инструкции приведены для Windows XP с операционной системой Service Pack 2.

Для установки инструкций на другие операционные системы см. документацию или Help-файлы вашей ОС.

1. Выберите **Start** > **Settings** > **Control Panel** > **Network Connections**.
   Откроется диалоговое окно Network Connections.

2. Правой кнопкой мыши нажмите на **Wireless Network Connection** и выберите **Properties**.
   Откроется диалоговое окно Wireless Network Connection.

3. Выберите закладку **Wireless Networks**.

4. Ниже **Preferred Networks** нажмите **Add**.
   Откроется диалоговое окно Wireless Network Properties.

5. Введите SSID в текстовое поле **Network Name (SSID)**.

6. Выберите сетевую аутентификацию и данные метода шифрования из выпадающего списка. Если необходимо, отключите опцию **The key is provided for me automatically** и введите сетевой ключ 2 раза.

7. Нажмите **OK,** чтобы закрыть диалоговое окно **Wireless Network Properties**.

8. Нажмите **View Wireless Networks**.
   Все доступные беспроводные соединения откроются в текстовом поле Available Networks.

9. Выберите SSID беспроводной сети или нажмите **Connect**. Если сеть использует шифрование, введите сетевой ключ дважды и диалоговом окне Wireless Network Connection и нажмите **Connect** снова.

10. Настройте беспроводной компьютер для использования DHCP

.

Глава 10 - Динамическая маршрутизация

Динамическая маршрутизация

Протокол маршрутизации – это я зык, на котором маршрутизатор общается с другими маршрутизаторами для обмена информацией о состоянии сетевых таблиц машрутизации. При использовании статической маршрутизации, таблицы маршрутизации нельзя изменить. Если маршрутизатор на удаленном конце выходит из строя, то пакет не может попасть в место назначения.

Динамическая маршрутизация позволяет динамически изменять таблицы маршрутизации в зависимости от изменения маршрутов. Если наиболее оптимальный маршрут не может быть использован, протоколы динамической машрутизации при необходимости изменяют таблицы маршрутизации для успешного продвижения трафика.

Некоторые протоколы динамической маршрутизации поддерживаются только в Fireware XTM с обновлением Pro. Динамическая маршрутизация в устройствах Firebox X Edge e-Series не поддерживается.

Fireware XTM с обновлением Pro поддерживает протоколы динамической маршрутизации RIP v1 и v2, OSPF, и BGP v4. Fireware XTM поддерживает только RIP v1 and v2

Конфигурационные файлы демонов маршрутизации

Для того чтобы использовать протоколы динамической машрутизации с Fireware, вам необходимо импортировать или ввести имя конфигурационного файла для демона маршрутизации, который вы хотите использовать. Этот конфигурационный файл содержит информацию, такую как пароль и имя файла журнала. Вы сможете найти шаблоны конфигурации для каждого из протоколов маршрутизации в этом FAQ:

- Пример конфигурационного файла RIP маршрутизации
- Пример конфигурационного файла OSPF маршрутизации
- Пример конфигурационного файла BGP маршрутизации

Команды отображаются в секциях в порядке, в котором они должны идти в конфигурационном файле.

Примечания о конфигурационных файлах:

- Символы “!” и “#” используются для комментариев. Если первый символ в строке – один из символов комментария, то вся строка интерпретируется как комментарий. Если символ комментария не является первым символом в строке, то строка интерпретируется как команда.
- Обычно для отключения какой-либо команды вы можете использовать слово “no” в начале строки. Например, команда “no network 10.0.0.0/24 area 0.0.0.0” отключает определенный сегмент сети.

Протокол RIP (Routing Information Protocol)

Протокол RIP (Routing Information Protocol) используется для управления информацией маршрутизатора в независимых сетях, таких как корпоративная LAN или внутренняя WAN.

При использовании протокола RIP хост шлюза каждые 30 секунд отправляет ближайшему маршрутизатору свою таблицу маршрутизации. Этот маршрутизатор, в свою очередь, отправляет эту таблицу соседним маршрутизаторам.

Протокол RIP оптимально использовать в малых сетях, потому что передача полной таблицы маршрутов каждые 30 секунд создает большую нагрузку на сеть и таблицы RIP ограничены 15 «прыжками». Для больших сетей лучше использовать протокол OSPF

Существует две версии протокола RIP. RIP v1 использует UDP broadcast через порт 520 для отправки обновлений таблиц маршрутизации. RIP v2 для отправки обновлений таблиц маршрутизации использует multicast.

Команды RIP

Для создания и модификации конфигурационного файла ниже приводится таблица поддерживаемых команд маршрутизации. Эти секции должны идти в таком же порядке в конфигурационном файле, как и в этой таблице.

Секция	Команда	Описание
Настройка простого пароля и MD5 аутентификации для интерфейса		
	interface eth [N]	Войти в режим настройки интерфейса
		Алгоритм аутентификации для интерфейса
	ip rip authentication string [PASSWORD]	Установить пароль для ентификации RIP сообщений
	key chain [KEY-CHAIN]	Установить имя цепочки MD5 ключей
	key [INTEGER]	Установить номер MD5 ключа
	key-string [AUTH-KEY]	Установить ключ MD5 аутентификации
	ip rip authentication mode md5	Установить режим аутентификации – MD5
	ip rip authentication mode key-chain [KEYCHAIN]	Установить цепочку MD5 ключей

Настройка демона маршрутизации RIP

router rip	Запустить демона маршрутизации
version [1/2]	Выбрать версию RIP (по олчанию используется RIP v2)
ip rip send version [1/2]	Выбрать версию RIP сообщений, которые будут отправляться другим маршрутизаторам
ip rip receive version [1/2]	Выбрать версию RIP сообщений, которые будут брабатываться устройством
no ip split-horizon	Отключить функцию Split izon (включена по умолчанию)

Настройка интерфейсов и сетей

no network eth[N]

passive-interface eth[N]

passive-interface default

network [A.B.C.D/M]

neighbor [A.B.C.D/M]

Рассылка RIP маршрутов остальным маршрутизаторам и добавление OSPF и BGP маршрутов в таблицу RIP маршрутов

default-information originate	Отправить информацию о ршруте «последней надежды» ршрут по умолчанию) остальным маршрутизаторам
redistribute kernel	Рассылка статических ршрутов брандмауэра остальным маршрутизаторам

redistribute connected	Загрузка маршрутов со всех интерфейсов в таблицу маршрутизации RIP
redistribute connected route-map [MAPNAME]	Загрузить маршруты с ильтром маршрутеой карты (mapname)
redistribute ospf	Загрузка OSPF маршрутов в аблицу маршрутизации RIP
redistribute ospf route-map [MAPNAME]	Загрузка OSPF маршрутов в блицу маршрутизации RIP (с маршрутной картой)
redistribute bgp	Загрузка BGP маршрутов в аблицу маршрутизации RIP
redistribute bgp route-map [MAPNAME]	Загрузка BGP маршрутов в блицу маршрутизации RIP (с маршрутной картой)

Настройка фильтров загрузки маршрутов (маршрутные карты и списки доступа)

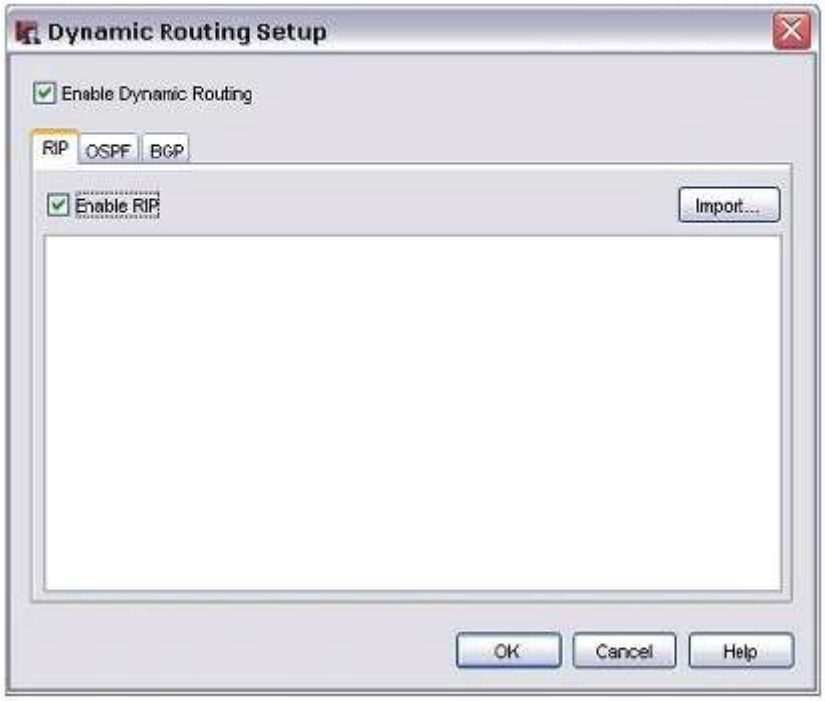
access-list [PERMIT|DENY] ISTNAME] [A,B,C,D/M | ANY]	Создать список доступа, орый разрешит или запретит узку только одного или всех IP адресов
route-map [MAPNAME] permit [N]	Создать маршрутную карту с нным именем и разрешением с приоритетом N
match ip address [LISTNAME]	

Настройка RIP v1 на Firebox

1. В окне Policy Manager выберите **Network** > **Dynamic Routing**.
   Откроется диалоговое окно Dynamic Routing Setup.

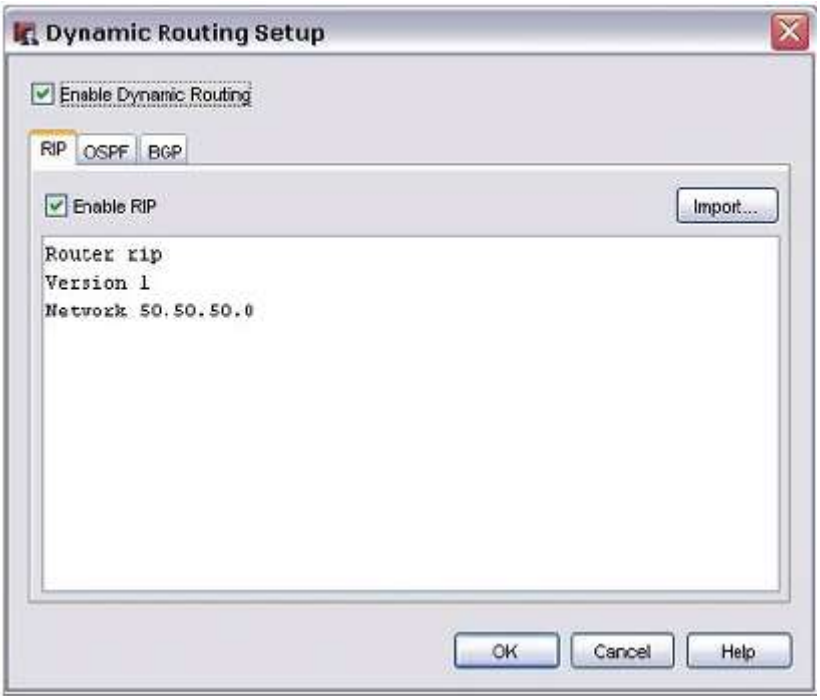
2. Нажмите **Enable Dynamic Routing**

3. Выберите закладку **RIP**



4. Включите опцию **Enable RIP**.

5. Для того импортировать конфигурационный файл демона маршрутизации нажмите **Import** или в текстовом поле введите имя конфигурационного файла



6. Нажмите **OK**.

Для более подробной информации см. “Конфигурационные файлы демонов маршрутизации”

Если вы нажмете Import, вы можете найти шаблон конфигурации демона маршрутизации RIP. Он расположен в каталоге: C:\Documents and Settings\My Documents\My WatchGuard.

Разрешение RIP v1 трафика через Firebox

Для того чтобы разрешить RIP-трансляции вам необходимо создать и настроить политику, которая будет разрешать RIP-трансляции от маршрутизатора к IP-адресам сети.

Вам также необходимо добавить IP-адрес интерфейса Firebox® в поле **To**.

1. Нажмите  . Или выберите **Edit** > **Add Policies**.

2. В окне Policy Manager выберите **Edit** > **Add Policies**. Из списка пакетных фильтров выберите RIP. Нажмите **Add**.
   Откроется окно New Policy Properties для RIP.

3. В диалоговом окне New Policy Properties настройте политику, чтобы она разрешала трафик с IP-адреса и сетевой адрес маршрутизатора, который использует RIP для подключения к интерфейсу Firebox®. Вам также необходимо добавить адрес трансляции

4. Нажмите OK.

5. Выполните необходимые настройки на маршрутизаторе, который вы указали в п. 3.

6. После того, как вы настроите маршрутизатор, откройте отчет Firebox Status Report и посмотрите в секцию динамической маршрутизации для того чтобы проверить, обмениваются ли RIP сообщениями Firebox и маршрутизатор.

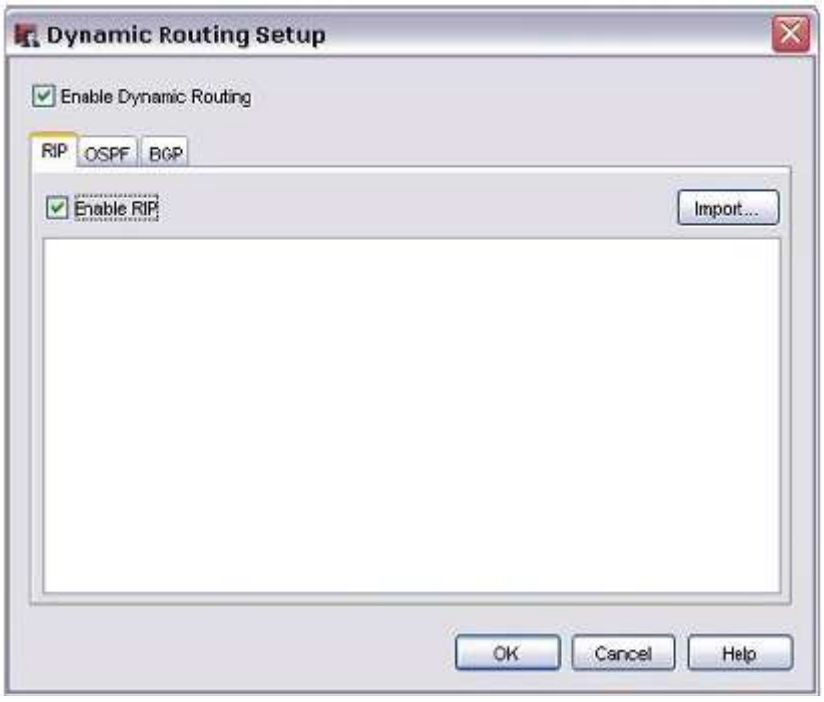
Затем вы можете настроить аутентификацию и политику RIP для того, чтобы она слушала только необходимые интерфейсы

Настройка RIP v2

1. Выберите **Network** > **Dynamic Routing**.
   Откроется диалоговое окно Dynamic Routing Setup

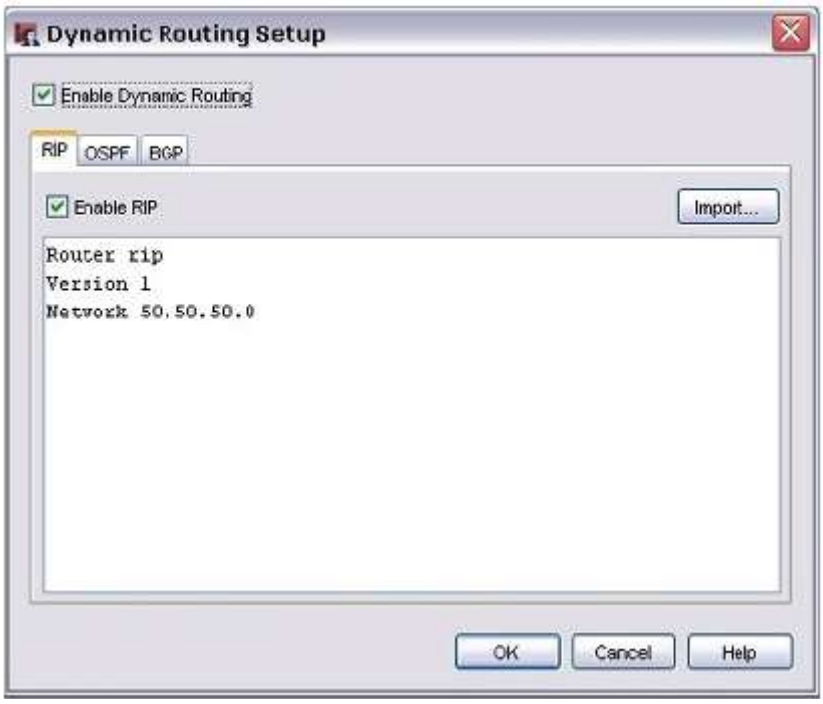
2. Включите опцию **Enable Dynamic Routing**.

3. Выберите закладку **RIP**



4. Включите опцию **Enable RIP**.

5. Для того импортировать конфигурационный файл демона маршрутизации нажмите **Import** или в текстовом поле введите имя конфигурационного файла



6. Нажмите **OK**.

Для более подробной информации см. “Конфигурационные файлы демонов маршрутизации”

Разрешение RIP v2 трафика через Firebox

Вам необходимо создать и настроить политику, которая должна разрешать групповые передачи RIP v2 от маршрутизаторов, на которых используется RIP v2, на зарезервированные IP-адреса групповой передачи для RIP v2.

1. Нажмите . Или выберите **Edit > Add Policies**.

2. Из списка пакетных фильтров выберите **RIP**. Нажмите **Add**.

3. В диалоговом окне New Policy Properties настройте политику, чтобы она разрешала трафик с IP или сетевого адреса машрутизатора, который использует RIP, на IP-адрес групповой передачи 224.0.0.9.

4. Нажмите **OK**.

5. Выполните необходимые настройки на маршрутизаторе, который вы указали в п. 3.

6. После того, как вы настроите маршрутизатор, откройте Firebox Status Report и посмотрите в секцию динамической маршрутизации для того чтобы проверить, обмениваются ли обновлениями Firebox и маршрутизатор.

Затем вы можете настроить аутентификацию и политику RIP для того, чтобы она слушала только необходимые интерфейсы

Пример файла конфигурации RIP маршрутизации

Для того чтобы использовать любой протокол динамической маршрутизации вам необходимо импортировать или скопировать и вставить конфигурационный файл для демона динамической маршрутизации. В этом разделе приводится пример конфигурационного файла для демона маршрутизации RIP. Если вы хотите использовать этот файл в качестве базы для своего собственного конфигурационного файла, то скопируйте содержимое этого файла в текстовое приложение (Notepad или Wordpad) и сохраните его под новым именем.

Дополнительные команды закомментированы при помощи "!". Для того чтобы включить команду, удалите символ "!" и выполните необходимые изменения.

```
!! SECTION 1: Configure MD5 authentication keychains.

! Set MD5 authentication key chain name (KEYCHAIN), key number

(1),

! and authentication key string (AUTHKEY).

! key chain KEYCHAIN

! key 1 ! key-string AUTHKEY

!! SECTION 2: Configure interface properties.

! Set authentication for interface (eth1).

! interface eth1

!

! Set RIP simple authentication password (SHAREDKEY).

! ip rip authentication string SHAREDKEY

!

! Set RIP MD5 authentication and MD5 keychain (KEYCHAIN).

! ip rip authentication mode md5

! ip rip authentication key-chain KEYCHAIN

!

!! SECTION 3: Configure global RIP daemon properties.

! Enable RIP daemon. Must be enabled for all RIP configurations.

router rip

!

! Set RIP version to 1; default is version 2.

! version 1

!

! Set RIP to send or received to version 1; default is version 2.
```

```
! ip rip send version 1
! ip rip receive version 1
!
! Disable split-horizon to prevent routing loop. Default is
enabled.
! no ip split-horizon
!! SECTION 4: Configure interfaces and networks.
! Disable RIP send and receive on interface (eth0).
! no network eth0
!
! Set RIP to receive-only on interface (eth2).
! passive-interface eth2
!
! Set RIP to receive-only on all interfaces.
! passive-interface default
!
! Enable RIP broadcast (version 1) or multicast (version 2) on
! network (192.168.253.0/24). !network 192.168.253.0/24
!
! Set unicast routing table updates to neighbor
(192.168.253.254).
! neighbor 192.168.253.254
!! SECTION 5: Redistribute RIP routes to peers and inject OSPF or
BGP
!! routes to RIP routing table.
! Share route of last resort (default route) from kernel routing
table
! with RIP peers.
! default-information originate
!
! Redistribute firewall static routes to RIP peers.
```

```
! redistribute kernel
!
! Set route maps (MAPNAME) to restrict route redistribution in
Section 6.
! Redistribute routes from all interfaces to RIP peers or with a
route map
! filter (MAPNAME).
! redistribute connected
! redistribute connected route-map MAPNAME
!
! Redistribute routes from OSPF to RIP or with a route map filter
(MAPNAME).
! redistribute ospf !redistribute ospf route-map MAPNAME
!
! Redistribute routes from BGP to RIP or with a route map filter
(MAPNAME).
! redistribute bgp !redistribute bgp route-map MAPNAME
!! SECTION 6: Configure route redistribution filters with route
maps and
!! access lists.
! Create an access list to only allow redistribution of
172.16.30.0/24.
! access-list LISTNAME permit 172.16.30.0/24
! access-list LISTNAME deny any
!
! Create a route map with name MAPNAME and allow with a priority
of 10.
! route-map MAPNAME permit 10
! match ip address LISTNAME
```

Протокол OSPF(Open Shortest Path First)

Этот протокол поддерживается только в Fireware XTM с обновлением Pro.

Протокол OSPF (Open Shortest Path First) - внутренний протокол маршрутизации, который используется в больших сетях. С использованием OSPF маршрутизатор, который видит изменения в своей таблице маршрутизации или обнаруживает изменения в сети, мновенно отправляет групповое обновление все маршрутизаторам сети. OSPF отличается от RIP по следующим причинам:

- OSPF передает только часть измененной таблицы маршрутизации. RIP передает таблицу маршрутизации целиком.
- OSPF отправляет multicast пакет сигнал, только в случае изменения его информации. RIP отправляет таблицу маршрутизации каждые 30 секунд.

Также существует несколько понятий, которые очень важны для понимания протокола OSFP:

- Если у вас есть несколько OSPF сегментов, один сегмент должен быть 0.0.0.0 (базовый сегмент).
- Все остальные сегменты должны располагаться рядом с базовым сегментом. Если же нет, то вам необходимо настроить виртуальное соединение с базовым сегментом.

Команды OSPF

Ниже приводится таблица команд маршрутизации, для того чтобы создать или изменить конфигурационный файл. Эти секции должны идти в таком же порядке в конфигурационном файле, как и в этой таблице

Секция	Команда	Описание
	Настройка интерфейса	
	ip ospf authentication-key [PASSWORD]	Установить пароль аутентификации для OSPF
	interface eth[N]	Войти в режим настройки интерфейса
	ip ospf message-digest-key [KEY-ID] md5 [KEY]	Создать ключ аутентификации и указать его ID
	ip ospf cost [1-65535]	Установить стоимость канала связи (см. ниже таблицу стоимости каналов связи)
	ip ospf hello-interval [1-65535]	Интервал отправки hello-пакетов. По умолчанию 10 секунд
	ip ospf dead-interval [1-65535]	Установить временной интервал, по истечении которого, начиная с отправки последнего hello-пакета, соседнее устройство считается недоступным. По умолчанию

	40 секунд
ip ospf retransmit-interval [1-65535]	Установить временной интервал между отправкой LSA сообщений. По умолчанию 5 секунд
ip ospf transmit-delay [1-3600]	Установить временной интервал для отправки LSA обновления. По умолчанию – 1 секунда
ip ospf priority [0-255]	Установить приоритет маршрута. Если вы укажете большое значение, то с большой вероятностью этот маршрутизатор станет DR (Designated Router)

Настройка демона маршрутизации OSPF

router ospf	Запустить OSPF демон
ospf router-id [A.B.C.D]	Установить ID маршрутизатора вручную. В противном случае маршрутизатор сам определит свой ID
ospf rfc 1583compatibility	Включить совместимость RFC 1583 (может привести к петлям маршрутизации)
ospf abr-type [cisco|ibm|shortcut|standard]	Для более подробной информации см. draft-ietf-abr-o5.txt
passive-interface eth[N]	Отключить OSPF сообщения на интерфейсе eth[N]
auto-cost reference bandwidth[0-429495]	Установить глобальную величину стоимости (см. ниже таблицу стоимости каналов связи). Не используйте эту команду вместе с командой "ip ospf [COST]"
timers spf [0-4294967295][0-4294967295]	Установить величины OSPF Schedule Delay и Hold Time

Включить OSPF в сети. Значение переменной «area» (зона) можно ввести двумя способами:

[W.X.Y.Z] или просто целое число

network [A.B.C.D/M] area [Z]	Включить OSPF для сети [W.X.Y.Z] и зоны 0.0.0.Z

Настройка параметров BackBone и Других Зон. Значение переменной «area» (зона) можно ввести двумя способами: [W.X.Y.Z] или просто целое число

area [Z] range [A.B.C.D/M]	Создать зону 0.0.0.Z и роить «classful » сеть для этой (диапазон адресов и интерфейс а также маска подсети должны совпадать)
area [Z] virtual-link [W.X.Y.Z]	Создать виртуальное соседнее стройство для зоны 0.0.0.Z
area [Z] stub	Сделать зону 0.0.0.Z тупиковой (stub area)
area [Z] stub no-summary	
area [Z] authentication	Включить простую тификацию на базе паролей для зоны 0.0.0.Z
area [Z] authentication message-digest	Включить MD5 ентификацию для зоны 0.0.0.Z

Загрузка OSPF маршрутов

default-information originate	Загрузить маршрут «последней кды» (маршрут по умолчанию) в OSPF таблицу
default-information originate metrics [0-16777214]	Загрузить маршрут по анию в OSPF таблицу и добавить к нему метрику, которая пользовалась для генерации маршрута по умолчанию
default-information originate always	Всегда загружать маршрут по молчанию в OSPF таблицу
default-information originate always metrics [0-16777214]	Всегда загружать маршрут по молчанию в OSPF таблицу и авлять к нему метрику, которая пользовалась для генерации

	маршрута по умолчанию
redistribute connected	Загружать маршруты всех нтерфейсов в OSPF таблицу
redistribute connected metrics	Загружать маршруты во всех терфейсов в OSPF таблицу и авлять к ним метрики, которые ользовались для их создания

Настройка загрузки маршрутов со Списками Доступа и Маршрутными картами

access-list [LISTNAME] permit [A.B.C.D/M]	Создать список доступа, ый разрешит загрузку маршрута [A.B.C.D/M]
access-lists [LISTNAME] deny any	Запретить загрузку любой шрутной карты, не указанной в предыдущей команде
route-map [MAPNAME] permit [N]	Создать маршрутную карту с ем [MAPNAME] и разрешить ее с приоритетом N
match ip address [LISTNAME]	

Таблица OSPF Interface Cost

Протокол OSPF находит наиболее оптимальный путь между двумя точками. Для того чтобы это делать, протокол учитывает такие факторы, как скорость подключения к интерфейсу, количество «прыжков» между точками, и другие метрики. По умолчанию, OSPF использует реальную скорость подключения устройства для подсчета стоимости канала связи.

Вы можете вручную установить стоимости канала к интерфейсам для того чтобы повысить эффективность если, например, ваш гигабайтный брандмауэр к 100-Мбитному маршрутизатору. При помощи чисел в таблице OSPF Interface Cost установите все необходимые стоимости канала связи

Интерфейс	Пропускная ıособность (в бит/с)	Пропускная ɔсобность (байт/сек)	OSPF стоимость канала связи
Ethernet	1G	128M	1
Ethernet	100M	12.5M	10
Ethernet	10M	1.25M	100

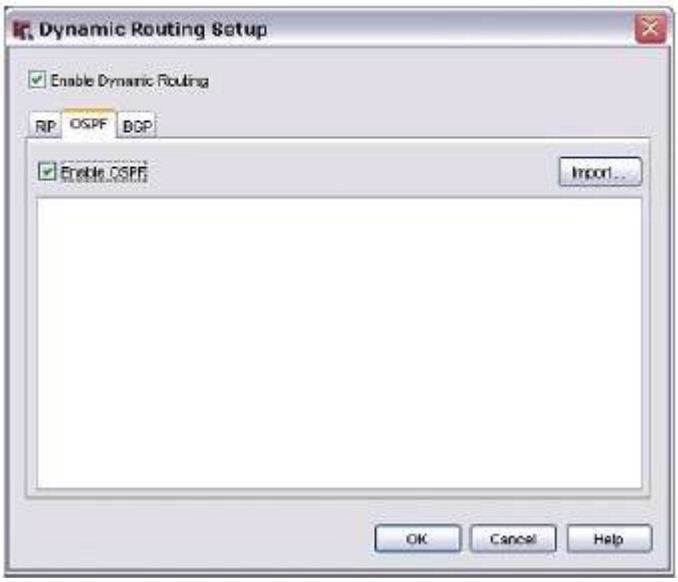
Модем	2M	256K	500
Модем	1M	128K	1000
Модем	500K	62.5K	2000
Модем	250K	31.25K	4000
Модем	125K	15625	8000
Модем	62500	7812	16000
Последовательный (Serial)	115200	14400	10850
Последовательный (Serial)	57600	7200	21700
Последовательный (Serial)	38400	4800	32550
Последовательный (Serial)	19200	2400	61120
Последовательный (Serial)	9600	1200	65535

Настройка OSPF на Firebox

1. В окне **Policy Manager** выберите **Network** > **Dynamic Routing**.
   Откроется диалоговое окно Dynamic Routing Setup.

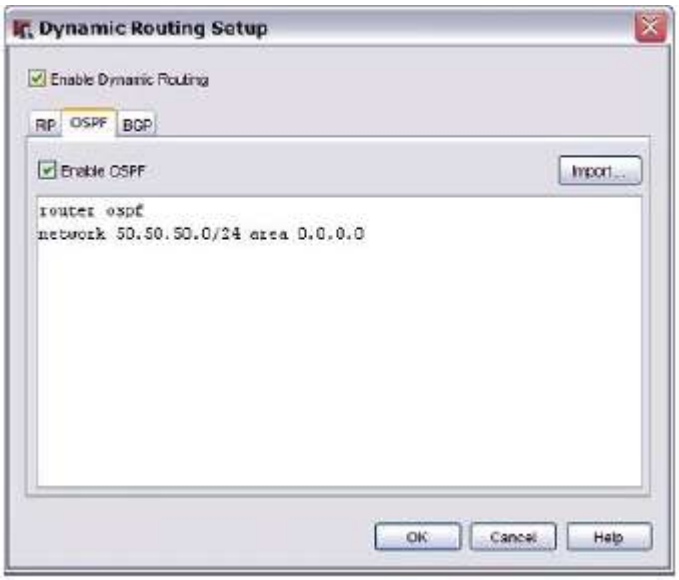
2. Включите опцию **Enable Dynamic Routing**

3. Выберите закладку **OSPF**



4. Включите опцию **Enable OSPF**.

5. Для того импортировать конфигурационный файл демона маршрутизации нажмите **Import** или в текстовом поле введите имя конфигурационного файла



   Для того чтобы начать, вам необходимы только две команды в вашем конфигурационном файле OSPF. Эти команды используются для запуска OSPF процесса:

   `router OSPF`

   `network` <IP адрес интерфейса, на котором будет запущен процесс OSPF > area <ID зоны в формает x.x.x.x>

6. Нажмите **OK**.

Разрешение OSPF трафика через Firebox

Для того чтобы разрешить OSPF multicast трафик вам необходимо создать соответствующую политику. Для этого выполните следующее:

1. Нажмите  . Или выберите **Edit** > **Add Policies**.

2. Из списка пакетных фильтров выберите **RIP**. Нажмите **Add**.

3. В диалоговом окне **New Policy Properties** создайте политику, которая разрешит трафик с IP адреса или адреса сети маршрутизатора на IP-адреса 224.0.0.5 и 224.0.0.6. Для более подробной информации о настройке IP адресов источника и назначения см. “Настройка правил доступа для политики”

4. Нажмите **OK**.

5. Выполните все необходимые настройки на маршрутизаторе, который вы выбрали в п.3

6. После того, как вы настроите маршрутизатор, откройте Firebox Status Report и посмотрите в секцию динамической маршрутизации для того чтобы проверить, обмениваются ли обновлениями Firebox и маршрутизатор. Затем вы можете настроить аутентификацию и политику OSPF для того, чтобы она слушала только необходимые интерфейсы

Пример конфигурационного файла OSPF маршрутизации

Для того чтобы использовать любой протокол динамической маршрутизации вам необходимо импортировать или скопировать и вставить конфигурационный файл для демона динамической маршрутизации. В этом разделе приводится пример конфигурационного файла для демона маршрутизации OSPF. Если вы хотите использовать этот файл в качестве базы для своего собственного конфигурационного файла, то скопируйте содержимое этого файла в текстовое приложение (Notepad или Wordpad) и сохраните его под новым именем. Дополнительные команды закомментированы при помощи "!". Для того чтобы включить команду, удалите символ "!" и выполните необходимые изменения.

```
!! SECTION 1: Configure interface properties.

! Set properties for interface eth1.

! interface eth1

!

! Set simple authentication password (SHAREDKEY).

! ip ospf authentication-key SHAREDKEY

!

! Set MD5 authentication key ID (10) and MD5 authentication key

(AUTHKEY).

! ip ospf message-digest-key 10 md5 AUTHKEY

!

! Set link cost to 1000 (1-65535) on interface eth1.

! for OSPF link cost table. !ip ospf cost 1000

!

! Set hello interval to 5 seconds (1-65535); default is 10

seconds.
```

```
! ip ospf hello-interval 5
!
! Set dead-interval to 15 seconds (1-65535); default is 40
seconds.
! ip ospf dead-interval 15
!
! Set interval between link-state advertisements (LSA)
retransmissions

! to 10 seconds (1-65535); default is 5 seconds.
! ip ospf retransmit-interval 10
!
! Set LSA update interval to 3 seconds (1-3600); default is 1
second.
! ip ospf transmit-delay 3
!
! Set high priority (0-255) to increase eligibility to become the
! designated router (DR).
! ip ospf priority 255
!! SECTION 2: Start OSFP and set daemon properties.
! Enable OSPF daemon. Must be enabled for all OSPF configurations.
router ospf
!
! Set the router ID manually to 100.100.100.20. If not set, the
firewall will
! set its own ID based on an interface IP address.
! ospf router-id 100.100.100.20
!
! Enable RFC 1583 compatibility (increases probability of routing
loops).
! ospf rfc1583compatibility
```

```
!
! Set area border router (ABR) type to cisco, ibm, shortcut, or
standard.
! More information about ABR types is in draft-ietf-ospf-abr-alt-
05.txt.
! ospf abr-type cisco
!
! Disable OSPF announcement on interface eth0.
! passive interface eth0
!
! Set global cost to 1000 (0-429495).
! auto-cost reference bandwidth 1000
!
! Set SPF schedule delay to 25 (0-4294967295) seconds and hold
time to
! 20 (0-4294967295) seconds; default is 5 and 10 seconds. !timers
spf 25 20
!! SECTION 3: Set network and area properties. Set areas with
W.X.Y.Z
!! or Z notation.
! Announce OSPF on network 192.168.253.0/24 network for area
0.0.0.0.
! network 192.168.253.0/24 area 0.0.0.0
!
! Create area 0.0.0.1 and set a classful network range
(172.16.254.0/24)
! for the area (range and interface network settings must match).
! area 0.0.0.1 range 172.16.254.0/24
!
! Set virtual link neighbor (172.16.254.1) for area 0.0.0.1.
! area 0.0.0.1 virtual-link 172.16.254.1
```

```
!
! Set area 0.0.0.1 as a stub on all routers in area 0.0.0.1.
! area 0.0.0.1 stub
!
! area 0.0.0.2 stub no-summary
!
! Enable simple password authentication for area 0.0.0.0.
! area 0.0.0.0 authentication
!
! Enable MD5 authentication for area 0.0.0.1.
! area 0.0.0.1 authentication message-digest
!! SECTION 4: Redistribute OSPF routes
! Share route of last resort (default route) from kernel routing
table
! with OSPF peers.
! default-information originate
!
! Redistribute static routes to OSPF.
! redistribute kernel
!
! Redistribute routes from all interfaces to OSPF.
! redistribute connected
! redistribute connected route-map
! ! Redistribute routes from RIP and BGP to OSPF.
! redistribute rip !redistribute bgp
!! SECTION 5: Configure route redistribution filters with access
lists
!! and route maps.
! Create an access list to only allow redistribution of 10.0.2.0/
24.
! access-list LISTNAME permit 10.0.2.0/24
```

```
! access-list LISTNAME deny any

!

! Create a route map with name MAPNAME and allow with a

priority of 10 (1-199).

! route-map MAPNAME permit 10

! match ip address LISTNAME
```

Протокол BGP(Border Gateway Protocol)

Этот протокол поддерживается только в Fireware XTM с обновлением Pro на устройствах Core e-Series, Peak e-Series или XTM.

Протокол BGP (Border Gateway Protocol) масштабируемый протокол динамической маршрутизации, который используется группой маршрутизаторов для обмена информацией о маршрутах. BGP – это протокол динамической маршрутизации, который используется в сети Интернет. Для определение политик маршрутизации и создания стабильного маршрутизируемого окружения BGP использует параметры или “атрибуты”. BGP позволяет вам создавать несколько маршрутов в и из сети Интернет к вашим сетям и ресурсам. Это дает вам возможность создать отказоустойчивые маршруты и увеличивает время работы системы.

Хосты, на которых используется BGP, используют протокол TCP для отправки информации об изменениях в таблицах маршрутизации, которые они обнаружили. Хост отправляет только часть таблицы маршрутизации, в которой произошли изменения. BGP использует CIDR-маршрутизацию для уменьшения размеров таблиц машрутизации в сети Интернет. Размер таблиц BGP в Fireware XTM равен 32K.

Для обычного WAN клиента наиболее оптимальным решением является использование протокола OSPF. WAN может также использовать протокол EBGP, когда для доступа в Интернет используется несколько шлюзов. EBGP позволяет вам использовать все преимущества возможной отказоустойчивости в сетях с многосетевыми компьютерами

Для того чтобы использовать BGP вам необходимо иметь ASN-номер. Вам необходимо получить ASN от одного из региональных центров из таблицы, приведенной ниже. После того как вы присвоили себе ASN-номер, вам необходимо с каждым Интернет-провайдером, для того чтобы они получили свои ASN-номера и другую необходимую информацию.

Регион	Registry Name	Web сайт
Северная Америка	RIN	www.arin.net
Европа	RIPE	www.ripe.net
Азия	APNIC	www.apnic.net
Латинская Америка	LACNIC	www.lacnic.net
Африка	AfriNIC	www.afrinic.net

Команды BGP

Ниже приводится таблица команд маршрутизации, для того чтобы создать или изменить конфигурационный файл.

Эти секции должны идти в таком же порядке в конфигурационном файле, как и в этой таблице.

Не используйте параметры конфигурации BGP, которые вы получили не от вашего Интернет-провайдера.

Секция	Команда	Описание
Настройка демона маршрутизации BGP		
	router bgp [ASN]	Запустить BGP демон и указать номер автономной системы (ASN). Данные предоставляются вашим ISP
	network [A.B.C.D/M]	Анонсировать BGP на сети A.B.C.D/M
	no network [A.B.C.D/M]	Отключить анонсирование BGP на сети [A.B.C.D/M]
Настройка параметров соседних устройств		
	neighbor [A.B.C.D] remote-as [ASN]	Сделать устройство [A.B.C.D] членом удаленной автономной системы ASN
	neighbor [A.B.C.D] ebgp-multihop	Создать соседнее устройство в другой сети с помощью функции BGP multi-Hop
	neighbor [A.B.C.D] version 4+	Настройка версии BGP (4, 4+,4-) для обмена данными с соседним устройством. По умолчанию - 4
	neighbor [A.B.C.D] update-source [WORD]	Выбрать определенный интерфейс для BGP сессий
	neighbor [A.B.C.D] default-originate	Переслать маршрут по умолчанию соседним BGP устройствам
	neighbor [A.B.C.D] port 189	Настройка порта, по которому BGP устройства будут

	обмениваться данными
neighbor [A.B.C.D] send-community	Настроить send-community
neighbor [A.B.C.D] weight 1000	Установить весовой коэффициент по умолчанию для маршрутов устройства [A.B.C.D]

Community Lists

ip community-list [<1-99>|<100-199>] permit AA:NN	Указать сообщество, которое будет принимать номер автономной системы и номер сети, разделенные двоеточием

Фильтрация устройств (**Peer Filtering**)

neighbor [A.B.C.D] distribute-list [LISTNAME] [IN|OUT]	Настроить список рапределения и направления для конечного устройства
neighbor [A.B.C.D] prefix-list [LISTNAME] [IN|OUT]	Использовать список префиксов для сравнения с входящими и исходящими BGP данными, которые передаются устройству [A.B.C.D]
neighbor [A.B.C.D] filter-list [LISTNAME][IN|OUT]	Для соответсвия путя доступа автономной системы ко входящим и исходящим маршрутам
neighbor [A.B.C.D] route-map [MAPNAME][IN|OUT]	Для применения карты маршрутов ко входящим и исходящим маршрутам

Загрузка маршрутов в BGP таблицу

redistribute kernel	Загрузка статических маршрутов в BGP таблицу
redistribute rip	Загрузка RIP маршрутов в BGP таблицу
redistribute ospf	Загрузка OSPF маршрутов в BGP таблицу

Отражение маршрутов

bgp cluster-id A.B.C.D	Настройка ID кластера, если BGP кластер имеет несколько рефлекторов маршрута
neighbor [W.X.Y.Z] route-reflector-client	Настройка маршрутизатора в качестве рефлектора BGP маршрутов и настроить соседнее устройство в качестве его клиента

Списки доступа и списки IP префиксов

ip prefix-lists PRELIST permit A.B.C.D/E	Создать список префиксов
access-list NAME [deny|allow] A.B.C.D/E	Создать список доступа
route-map [MAPNAME] permit [N]	Вместе с командами «match» и «set», эта команда используется для настройки условий и действий для загрузки маршрутов
match ip address prefix-list [LISTNAME]	Совпадение с определенным списком доступа
set community [A:B]	Создать атрибут BGP сообщества
match community [N]	Совпадение с определенным списком сообществ
set local-preference [N]	Установить значение предпочтения для направления автономной системы

Настройка BGP для Firebox

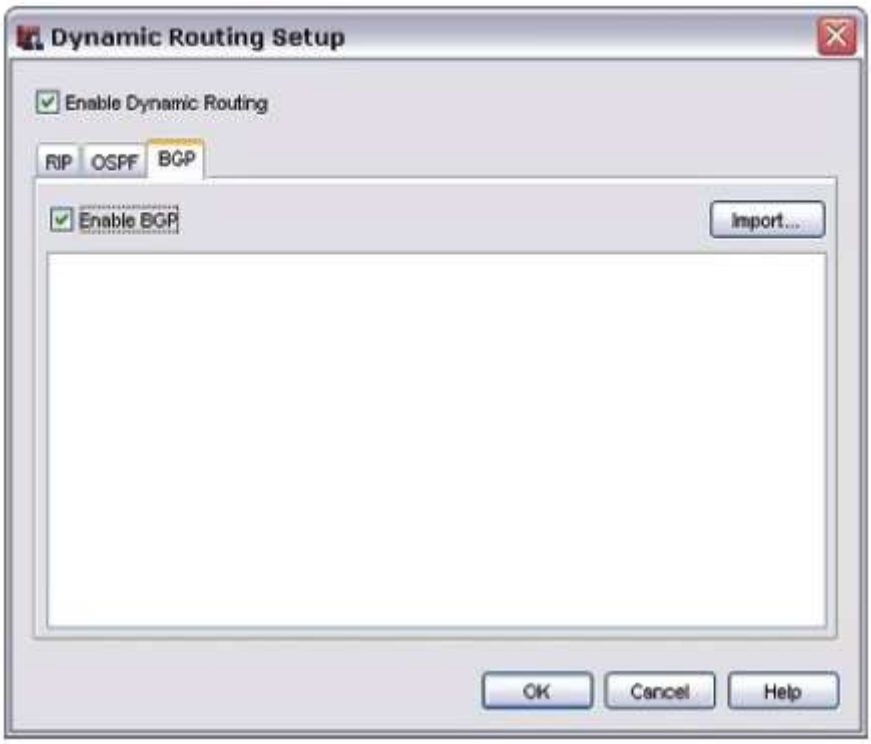
Для того чтобы работать с протоколом BGP, который запущен у вашего ISP, вам необходимо номер автономной системы (ASN).

Для более подробной информации см. “Протокол BGP(Border Gateway Protocol)”

1. Выберите **Network** > **Dynamic Routing**.
   Откроется диалоговое окно Dynamic Routing Setup.

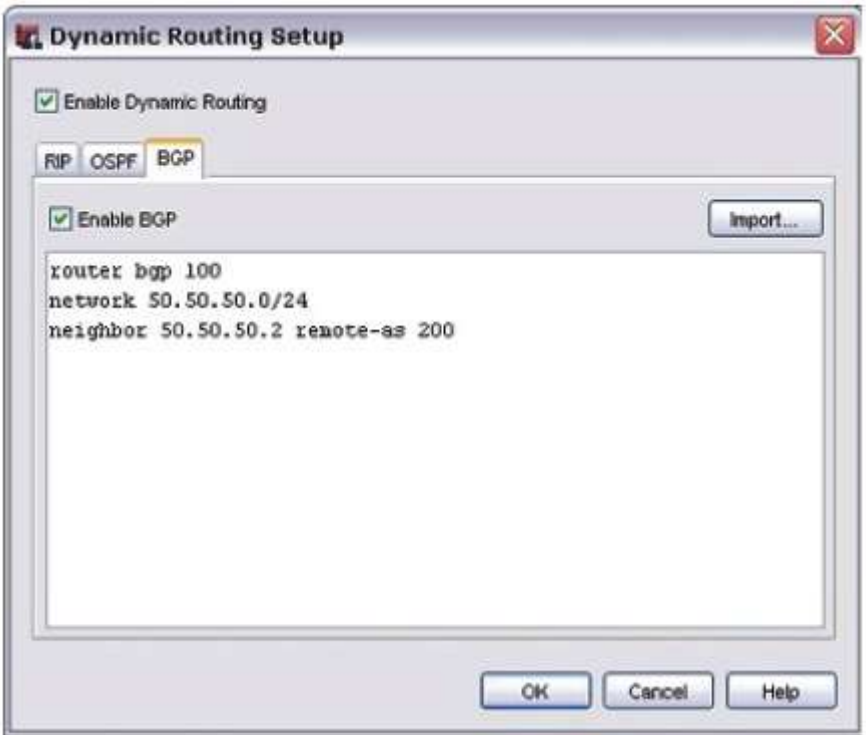
2. Включите опцию **Enable Dynamic Routing**.

3. Выберите закладку **BGP**



4. Включите опцию **Enable BGP**.

5. Для того импортировать конфигурационный файл демона маршрутизации нажмите **Import** или в текстовом поле введите имя конфигурационного файла.



Для того чтобы запустить BGP вам необходимы три команды в вашем конфигурационном файле BGP. Эти команды запускают BGP процесс, устанавливают связь с ISP и создают маршрут в сеть Интернет из вашей локальной сети. Команды необходимо вводить в

следующем порядке.

`router BGP:` Номер автономной системы BGP, выданный вашим ISP

`network:` IP адрес сети, маршрут к которому из сети Интернет, вы будете передавать

`neighbor:` <IP адрес соседнего BGP маршрутизатора> `remote-as` <Номер автономной системы BGP >

6. Нажмите **OK**.

Разрешение BGP трафика через Firebox

Вам необходимо создать и настроить политику, которая должна разрешать BGP-трафик от сетей к Firebox. Эти сети должны быть теми же сетями, которые содержатся в конфигурационном файле

1. Нажмите  . Или выберите **Edit** > **Add Policies**.
2. Из списка пакетных фильтров выберите **BGP**. Нажмите **Add**.
3. В диалоговом окне **New Policy Properties** создайте политику, которая разрешит трафик с IP адреса или адреса сети маршрутизатора, на котором запущен BGP, к IP-адресу интерфейса Firebox. Вам также необходимо добавить сетевой broadcast IP адрес.
4. Нажмите **OK**.
5. Выполните все необходимые настройки на маршрутизаторе, который вы выбрали в п.3
6. После того, как вы настроите маршрутизатор, откройте Firebox Status Report и посмотрите в секцию динамической маршрутизации для того чтобы проверить, обмениваются ли обновлениями Firebox и маршрутизатор. Затем вы можете настроить аутентификацию и политику BGP для того, чтобы она слушала только необходимые маршрутизации

Пример конфигурационного файла BGP маршрутизации

Для того чтобы использовать любой протокол динамической маршрутизации вам необходимо импортировать или скопировать и вставить конфигурационный файл для демона динамической маршрутизации. В этом разделе приводится пример конфигурационного файла для демона маршрутизации BGP. Если вы хотите использовать этот файл в качестве базы для своего собственного конфигурационного файла, то скопируйте содержимое этого файла в текстовое приложение (Notepad или Wordpad) и сохраните его под новым именем. Дополнительные команды закомментированы при помощи "!". Для того чтобы включить команду, удалите символ "!" и выполните необходимые изменения.

```
!! SECTION 1: Start BGP daemon and announce network blocks to BGP

neighbors

! Enable BGP and set local ASN to 100 router bgp 100

! Announce local network 64.74.30.0/24 to all neighbors defined

in section 2

! network 64.74.30.0/24

!! SECTION 2: Neighbor properties

! Set neighbor (64.74.30.1) as member of remote ASN (200)

! neighbor 64.74.30.1 remote-as 200
```

```
! Set neighbor (208.146.43.1) on another network using EBGP multi-hop

! neighbor 208.146.43.1 remote-as 300

! neighbor 208.146.43.1 ebgp-multihop

! Set BGP version (4, 4+, 4-) for communication with a neighbor;default is 4

! neighbor 64.74.30.1 version 4+

! Announce default route to BGP neighbor (64.74.30.1)

! neighbor 64.74.30.1 default-originate

! Set custom TCP port 189 to communicate with BGP neighbor (64.74.30.1).
Default port is TCP 179

! neighbor 64.74.30.1 port 189

! Set peer send-community

! neighbor 64.74.30.1 send-community

! Set a default weight for neighbor's (64.74.30.1) routes

! neighbor 64.74.30.1 weight 1000

! Set maximum number of prefixes allowed from this neighbor

! neighbor 64.74.30.1 maximum-prefix NUMBER

!! SECTION 3: Set community lists

! ip community-list 70 permit 7000:80

!! SECTION 4: Announcement filtering

! Set distribute list and direction for peer

! neighbor 64.74.30.1 distribute-list LISTNAME [in|out]

! To apply a prefix list to be matched to incoming or outgoing advertisements
to that neighbor

! neighbor 64.74.30.1 prefix-list LISTNAME [in|out

! To match an autonomous system path access list to incoming or outgoing
routes

! neighbor 64.74.30.1 filter-list LISTNAME [in|out]

! To apply a route map to incoming or outgoing routes

! neighbor 64.74.30.1 route-map MAPNAME [in|out]

!!SECTION5: Redistribute routes to BGP

! Redistribute static routes to BGP

! Redistribute kernel

! Redistribute rip routes to BGP
```

```
! Redistribute rip

! Redistribute ospf routes to BGP

! Redistribute ospf

!!SECTION6:Route reflection

! Set cluster ID and firewall as a client of route reflector server
51.210.0.254

! bgp cluster-id A.B.C.D

! neighbor 51.210.0.254 route-reflector-client

!! SECTION 7: Access lists and IP prefix lists

! Set prefix list

! ip prefix-list PRELIST permit 10.0.0.0/8

! Set access list!access-list NAME deny 64.74.30.128/25

! access-list NAME permit 64.74.30.0/25

! Create a route map with name MAPNAME and allow with a priority of 10

! route-map MAPNAME permit 10

! match ip address prefix-list LISTNAME

! set community 7000:80
```

Глава 11 – FireCluster

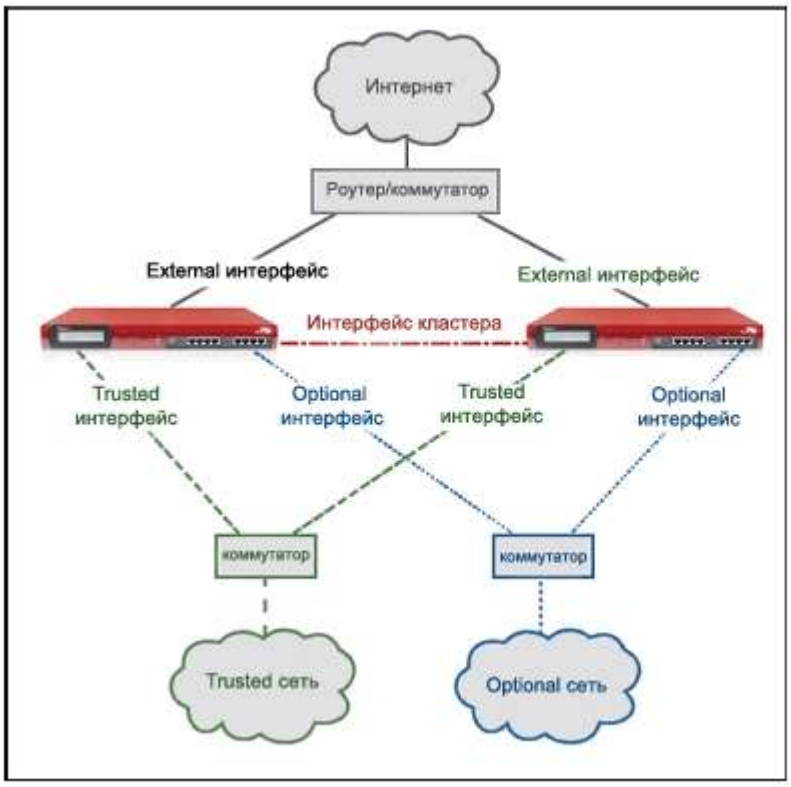
WatchGuard FireCluster

При помощи WatchGuard FireCluster вы можете настроить два устройства WatchGuard как кластер, что позволит вам значительно повысит производительность сети и ее масштабируемость. Существует два варианта конфигурации FireCluster:

active/passive (активный-пассивный) и active/active (активный-активный).

Для того чтобы обеспечить резервирование необходимо создать кластер в режиме «active/passive». Для того чтобы обеспечить резервирование и балансировку нагрузки в вашей сети создайте кластер в режиме «active/active».

После того, как вы создадите и настроите FireCluster, вы сможете управлять работой и выполнять мониторинг двух устройств как одно виртуальное устройство.



После включения FireCluster ваши устройства WatchGuard поддерживают:

- Подключение вторичных сетей на Trusted, External и Optional интерфейсах
- Multi-WAN подключения
  (Ограничение — Переключение внешнего канала, которое произошло по причине ошибки подключения к хосту мониторинга, не приводит к переключению FireCluster. Переключение в кластере FireCluster происходит только тогда, когда физический интерфейс выходит из строя и или не отвечает на запросы)
- VLAN сети

В случае если один из элементов кластера выходит из строя, то происходит переключение на резервный элемент кластера. При этом сохраняются:

- Подключения, обрабатываемые пакетным фильтром
- BOVPN-туннели
- Пользовательские сессии

При переключении следующие соединения могут быть разорваны:

- Подключения через прокси
- Mobile VPN with PPTP
- Mobile VPN with IPSec
- Mobile VPN with SSL

Пользователям Mobile VPN после переключения возможно понадобится переподключиться к VPN туннелю вручную. Для более подробной информации о переключении FireCluster см. "Переключение в кластере FireCluster"

Состояние кластера FireCluster

Для того чтобы посмотреть текущее состояние FireCluster в Firebox System Manager выполните следующее:

1. Загрузите Firebox System Manager.
2. Найдите информацию о FireCluster, как описано в разделе "Firebox, FireCluster и параметры интерфейса".
   Для управления и мониторинга элемента кластера FireCluster вы не сможете использовать web интерфейс Fireware XTM Web UI.

Переключение в кластере FireCluster

Процедура переключения для обоих режимов работы кластера одинакова.

В каждом из режимов работы каждый элемент кластера хранит информацию о состоянии и текущих подключениях всего кластера. При выходе из строя одного элемента кластера происходит переключение на другой элемент и вся информация о соединениях, обрабатываемых пакетным фильтром, BOVPN-туннелях и пользовательских сессиях переносится на второй элемент кластера.

В кластере FireCluster одно устройство является активным устройством, другое – резервным. Через основной интерфейс кластера осуществляется синхронизация данных о подключениях и текущих сессиях между устройствами кластера. Если основной интерфейс кластера выходит из строя, то данные между двумя устройствами начинают передаваться через резервный интерфейс кластера.

Мы рекомендует настраивать как основной, так и резервный интерфейсы кластера. Это гарантирует, что в случае выхода из строя активного устройства, резервное устройство будет иметь всю необходимую информацию для дальнейшего обслуживания исходящих подключений.

События, приводящие к переключению

Существует три типа событий, при наступлении которых произойдет переключение.

Обрыв связи на интерфейсе основного устройства

Если на интерфейсе основного устройства обнаруживается обрыв связи, то происходит переключение на резервное устройство. Для того чтобы посмотреть список интерфейсов, мониторинг состояния которых осуществляется системой, откройте страницу конфигурации FireCluster в Policy Manager.

Основное устройство работает некорректно

Переключение происходит в том случае, если на основном устройстве обнаруживаются программные или аппаратные проблемы, или если на этом устройстве при выполнении критически важного процесса происходит ошибка.

Кластер получает команду Failover Master с Firebox System Manager

Для того чтобы вручную запустить процедуру переключения с основного на резервный элементы кластера в Firebox System Manager выберите **Tools > Cluster > Failover Master**.Для более подробной информации об этой команде см. “Переключение master-устройства”

Что происходит при переключении

Когда происходит переключение, устройство кластера, которое до этого момента выполнял функцию резервного устройства кластера, становится основным устройством кластера. В то время как основное устройство кластера перезагружается и становится резервным. При переключении с одного элемента кластера на другой все данные о соединениях, обрабатываемых пакетным фильтром, BOVPN-туннелях и пользовательских сессиях сохраняются и переносятся на второй элемент кластера. Такое поведение характерно как для режима «active/active», так и для «active/passive». С подключениями через прокси прокси и Mobile VPN сессиями могут возникнуть проблемы, описание которых вы можете найти в таблице далее в этой главе.

В режиме работы кластера «active/active», если резервный элемент кластера выходит из строя, все данные о соединениях пакетного фильтра, BOVPN туннелях и пользовательских сессиях сохраняются и переносятся на основной элемент кластера. С подключениями через прокси прокси и Mobile VPN сессиями могут возникнуть проблемы, описание которых вы можете найти в таблице далее в этой главе.

В режиме работы кластера «active/passive» сбой в работе резервного элемента не приводит к разрыву соединений и пользовательских сессий, так как они все обслуживаются основным активным элементом.

Переключение FireCluster и балансировка нагрузки

Если для ваших внутренних серверов вы используете балансировку нагрузки, то при переключении FireCluster не происходит синхронизации в режиме реального времени. После переключения основной элемент кластера перенаправляет соединения на все серверы в списке серверов для балансировки нагрузки для получения информации о том, какой из серверов доступен на данный момент. Затем кластер использует алгоритм балансировки нагрузки для всех доступных серверов. Для более подробной информации о балансировке нагрузки на сервер см. “Настройка балансировки нагрузки на сервер”

Мониторинг состояния кластера во время переключения

Статус каждого устройства в кластере отображается в закладке **Front Panel** в Firebox System Manager сразу после имени устройства.

Если во время переключения вы посмотрите на закладку **Front Panel**, то вы увидите, как изменяется статус устройств во время переключения:

- Устройство, которое до этого было резервным, становится активным
- Статус устройства, которое было до этого активным, меняется сначала на (inactive), а затем после перезагрузки на (idle)

- Устройство, которое было до этого активным, после перезагрузки становится резервным

Для более подробной информации о мониторинге состояния см. “Мониторинг и управление устройствами FireCluster”

Подключение/сессия	Последствия
Подключения пакетного фильтра	Все подключения переносятся на резервное устройство кластера
BOVPN туннели	Все туннели переключаются на резервное устройство кластера
Пользовательские сессии	Все сессии переносятся на резервный элемент кластера
Подключения через прокси	Подключения, обслуживаемые вышедшим из строя устройством необходимо пересоздать. Подключения, обслуживаемые остальными устройствами кластера, будут продолжать работать
Mobile VPN with IPSec	Если основное устройство кластера выходит из строя, все Mobile VPN with IPSec сессии необходимо будет пересоздать. Если из строя выйдет резервное устройство, то пересоздать необходимо только сессии, обслуживаемые этим устройством. Сессии, обслуживаемые основным устройством, не обрываются
Mobile VPN with SSL	Если выйдет из строя любое из устройств, то все сессии необходимо будет пересоздать
Mobile VPN with PPTP	Все PPTP сессии обслуживаются основным устройством, даже в режиме «active/active». Если основное устройство выйдет из строя все сессии необходимо будет пересоздать. Выход из строя резервного устройства не приведет к сбоям связи

IP адрес управления

В конфигурации FireCluster все устройства используют одни и те же IP-адреса для всех активных интерфейсов.

Когда вы подключаетесь к кластеру в WatchGuard System Manager, вы автоматически подключаетесь к активному устройству кластера, где вы можете посмотреть состояния остальных устройств кластера. Для более подробной информации о мониторинге состояния элементов кластера в Firebox System Manager см. “Мониторинг и управление устройствами FireCluster”

Для более подробной информации о обновлении конфигурации кластера через Policy Manager см. “Обновление конфигурации FireCluster”

Настройка интерфейса управления

Вдобавок к общим IP-адресам для каждого интерфейса, каждый элемент кластера также имеет свой уникальный IP-адрес, который используется для управления. Используя этот IP-адрес вы можете напрямую подключаться к элементу кластера и смотреть информацию о его состоянии, или для непосредственного управления этим интерфейсом.

Этот уникальный IP-адрес называется *IP адрес управления*. При настройке FireCluster вам необходимо будет выбрать интерфейс, который будет использоваться для управления всеми элементами кластера. Этим интерфейсом может быть любой из активных интерфейсов.

Для каждого элемента кластера вам необходимо выбрать свой интерфейс управления

IP адрес управления не используется для каждодневных рутинных задач по администрированию кластера.

Использование интерфейса управления для восстановления образа из резервной копии

Если вы хотите восстановить копию образа FireCluster, то для того чтобы напрямую подключиться к устройству кластера вам необходимо использовать IP адрес управления.

Если вы подключились к устройству кластера через IP адрес управления, то в Firebox System Manager в меню **Tools** вам будут доступны две дополнительные команды: **Cluster > Leave** и **Cluster > Join**. При помощи этих команды вы можете восстановить образ FireCluster из резервной копии. Для более подробной информации см. “Восстановление образа FireCluster”

Интерфейс управления для обновления ОС с внешнего ресурса

WatchGuard System Manager для обновления ОС устройств кластера использует интерфейс управления. Если вы хотите обновить ОС с удаленного ресурса выполните следующее:

- Интерфейсу управления присвойте IP адрес External интерфейса
- IP адрес интерфейса управления для каждого устройства кластера является публичным и маршрутизируемым IP адресом

Для более подробной информации см. “Обновление Fireware XTM для устройств FireCluster”

Если через интерфейс управления вы подключаетесь к резервному master-устройству вы не сможете сохранить изменения конфигурации через Policy Manager.

Настройка FireCluster

FireCluster поддерживает два варианта настройки кластера.

Кластер Active/Passive

В этом режиме одно устройство в кластере является активным, второе - резервным. Через активное устройство проходит весь трафик. Резервное устройство постоянно следит за состоянием активного устройства. Если активное устройство выходит из строя, то резервное устройство переводит весь трафик на себя. После переключения трафик всех активных подключений маршрутизируется на активное устройство.

Кластер Active/Active

В этом режиме устройства в кластере делят весь трафик между собой. Трафик между устройствами кластера распределяется по двум алгоритмам, которые вам необходимо настроить - *round-robin* или *least connections*. Если одно из устройств в кластере выходит из строя, другое

устройство весь его трафик переводит на себя. После переключения трафик всех активных подключений маршрутизируется на активное устройство.

Требования и ограничения FireCluster

Перед тем как приступать к настройке FireCluster, пожалуйста, ознакомьтесь с нижеприведенными требованиями и ограничениями:

- Устройства WatchGuard в кластере должны быть одинаковой модели. Поддерживаются модели Firebox X Core e-Series, Firebox Peak e-Series или WatchGuard XTM.
- Все устройства в кластере должны использовать одну и ту же версию Fireware XTM с обновлением Pro.
- Для каждого устройства в кластере необходимо иметь активную подписку LiveSecurity Service.
- Мы рекомендуем, чтобы для всех устройств в кластере в режиме «active/active» были в наличие активные лицензии для дополнительных сервисов (WebBlocker или Gateway AntiVirus). Для более подробной информации см. “About feature keys and FireCluster” on page 244.
- К каждому активному интерфейсу кластер должен быть подключен коммутатор.
- Для кластера в режиме «active/active» все коммутаторы и маршрутизаторы в broadcast домене должны поддерживать multicast трафик
- Для кластера в режиме «active/active» вам необходимо знать IP и MAC-адреса каждого Layer 3 коммутатора и маршрутизатора, подключенных к кластеру. Затем во время настройки FireCluster вам необходимо будет добавить эти значения в ARP таблицу. Для более подробной информации см. “Добавление записей в ARP таблицу FireCluster для каждого коммутатора”
- FireCluster не поддерживает динамические протоколы маршрутизации.

Синхронизация кластера и мониторинг состояния

При использовании FireCluster вам необходимо выделить по крайней мере один интерфейс, через который все устройства кластера будут обмениваться данными. Этот интерфейс называется **интерфейс кластера** (*cluster interface)*. При настройке устройств кластера вам необходимо подключить устройства кластера друг к другу через основной интерфейс кластера. Для обеспечения резервирования мы рекомендуем вам настроить резервный интерфейс кластера. Используя этот интерфейс устройства, объединенные в кластер, синхронизируют всю информацию, необходимую для балансировки нагрузки и переключения в случае выхода из строя активного устройства.

Функции устройств FireCluster

При объединении устройств в кластер очень важно понимать, какие функции выполняет каждое устройство в кластере.

Основное устройство (Cluster master)

Это устройство распределяет трафик между элементами кластера и осуществляет обработку запросов, поступающих из внешней сети - WatchGuard System Manager, SNMP, DHCP, ARP-запросы, запросы протоколов маршрутизации и IKE. При настройке или изменении настроек кластера все изменения сохраняются на активном устройстве. Устройство, которое будет включено первым, и становится активным устройством в кластере.

Резервное устройство (Backup cluster master)

Это устройство синхронизирует всю необходимую информацию с активным устройством для того чтобы в случае выхода из строя активного устройства, оно могло взять его функции на себя. Резервное master-устройство может быть активным или пассивным.

Активное устройство (Active member)

Любое устройство в кластере, через которое проходит трафик. В кластере «active/active» оба устройства являются активными. В кластере «active/passive» активным является только основное master-устройство.

Пассивное устройство (Passive member)

Устройство в кластере «active/passive», через которое не проходит трафик. В кластере «active/passive» пассивным является резервное master-устройство.

Этапы конфигурации FireCluster

Для того чтобы настроить устройства WatchGuard как FireCluster, вам необходимо выполнить следующее:

1. Спланируйте конфигурацию вашего FireCluster. Для более подробной информации см. “Перед тем, как начать”

2. Подключите устройства FireCluster к сети, как описано в “Подключение оборудования FireCluster”

3. Настроить FireCluster в Policy Manager. Вы можете это сделать одним из следующих способов:

   - “Мастер FireCluster Setup Wizard”

   - “Ручная настройка FireCluster”

Для настройки кластера «active/active» вам также необходимо выполнить следующее:

1. Настройте поддержку multicast MAC-адресов на ваших Layer 3 коммутаторах и маршрутизаторах, которые подключены к FireCluster. Для более подробной информации см. “Требования к коммутаторам и маршрутизаторам при использовании кластера «active/active»”

2. Добавьте в ARP таблицу записи для каждого маршрутизатора и коммутатора, которые подключены к FireCluster

Перед тем, как начать

Перед тем как приступить к настройке FireCluster, вам необходимо выполнить все необходимые инструкции, описанные в дальнейших разделах этой главы.

Проверка основных компонентов

Убедитесь, что у вас имеется следующее:

- Два устройства Firebox X Core, Peak или WatchGuard XTM одной и той же модели

- Одна и та же версия Fireware XTM с обновлением Pro, установленная на каждом устройстве

- Один кроссовер-кабель (красного цвета) для каждого интерфейса кластера (если вы хотите использовать резервный интерфейс кластера, то вам необходимо еще один кроссовер-кабель)

- Один коммутатор для каждого активного интерфейса
- Ethernet-кабели для подключения устройств к портам коммутатора
- Серийные номера для каждого устройства
- Ключи функций ключи для каждого устройства с одинаковыми активированными сервисами. Для более подробной информации см. “Получение ключа функций от LiveSecurity”

Настройка коммутаторов и маршрутизаторов

В кластере «active/active» сетевые интерфейсы используют multicast MAC-адреса. Поэтому вам необходимо настроить маршрутизацию этих MAC-адресов. Для более подробной информации см. “Требования к коммутаторам и маршрутизаторам при использовании кластера «active/active»”

Этот шаг необязателен для кластера «active/passive», так как там multicast MAC-адреса не используются.

Выбор IP-адресов для интерфейсов кластера

Мы рекомендует создать таблицу, которая будет содержать IP-адреса, которые вы хотите присвоить интерфейсам кластера и интерфейсам управления. Мастер установки FireCluster попросит вас настроить эти параметры для каждого устройства в кластера. Если вы заранее спланируете эти IP-адреса, то вам будет значительно легче настроить эти интерфейсы при помощи мастера.

Интерфейсы и IP адреса для интерфейсов кластера			
	Интерфейс	**IP адрес для устройства 1**	**IP адрес для устройства 2**
Основной интерфейс кластера	_____	____.____.____.____ /__	____.____.____.____ /__
Резервный интерфейс кластера	_____	____.____.____.____ /__	____.____.____.____ /__
Интерфейс управления	_____	____.____.____.____ /__	____.____.____.____ /__

Основной интерфейс кластера

Это специальный интерфейс на устройстве WathGuard, который используется для обмена данными между элементами кластера. Если у вас есть интерфейс, который настроен как отдельный VLAN интерфейс, не используйте этот интерфейс в качестве интерфейса кластера. IP-адреса основных интерфейсов кластера для всех устройств должны быть в одной подсети.

Резервный интерфейс кластера (дополнительно, но рекомендуется)

Это второй интерфейс на устройстве WatchGuard, который можно использовать для обмена данными между элементами кластера. Устройства кластера используют этот интерфейс в случае если основной интерфейс вышел из строя. Для обеспечения резервирования мы рекомендуем использовать два интерфейса кластера. IP-адреса резервных интерфейсов кластера для всех устройств должны быть в одной подсети.

Интерфейс управления

Это сетевой интерфейс устройства Firebox, который используется для прямого подключения к устройствам кластера с любого приложения WatchGuard. IP-адреса управления для устройств в кластере могут быть разных в подсетях

Подключение оборудования FireCluster

Устройства, которые объединяются в кластер должны быть одной модели, на них должно быть установлено одна и та же версия Fireware XTM с обновлением Pro

Для того чтобы объединить два устройства WatchGuard в кластер FireCluster выполните следующее:

1. При помощи кроссовер-кабеля (кабель красного цвета) подключите основной интерфейс кластера одного устройства к основному интерфейсу кластера другого устройства.

2. Если вы хотите использовать резервный интерфейс кластера, то вам необходимо второй кроссовер-кабель для подключения. Если у вас есть свободный интерфейс, то мы рекомендуем настроить резервный интерфейс кластера.

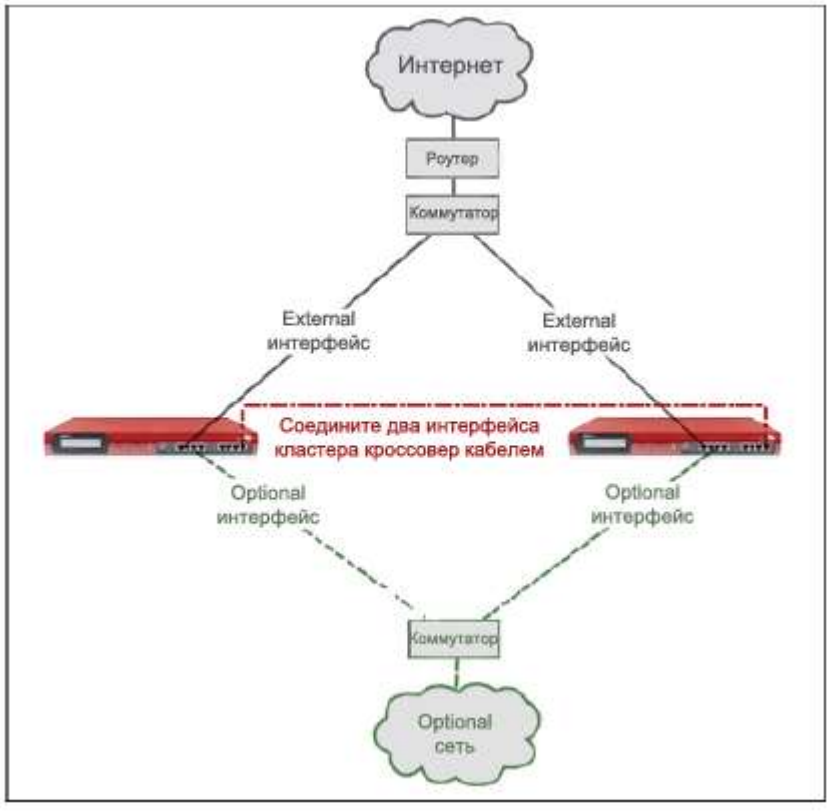
3. Подключите External интерфейс каждого устройства к коммутатору. Если вы используете Multi-WAN, подключите второй External интерфейс каждого устройства к коммутатору.

4. Подключите Trusted интерфейс каждого устройства к вашему внутреннему коммутатору

5. Подключите остальные Trusted и Optional интерфейсы к вашему внутреннему коммутатору. Для более подробной информации о требованиях к коммутатору см. “Требования к коммутаторам и маршрутизаторам при использовании кластера «active/active»”

Вам необходимо подключать каждую пару интерфейсов к отдельному концентратору или коммутатору.

На диаграмме ниже показаны подключения простого кластера FireCluster.



В этом примере FireCluster имеет один External и один Trusted интерфейсы, подключенные к коммутатору. Основные интерфейсы кластера соединены при помощи кроссовер-кабеля.

После того, как вы сделаете все необходимые подключения в FireCluster, вы можете приступить к его настройке в Policy Manager. Вы можете сделать это двумя способами:

- “Мастер FireCluster Setup Wizard”
- “Ручная настройка FireCluster”

Требования к коммутаторам и маршрутизаторам при использовании кластера «active/active»

Кластер «active/active» для передачи данных использует multicast MAC-адреса на всех интерфейсах. Перед тем как использовать кластер «active/active», убедитесь, что ваши коммутаторы, маршрутизаторы и другие сетевые устройства могут обрабатывать multicast MAC адреса.

Broadcast домен – это логическая часть компьютерной сети, в которой все сетевые узлы могут обмениваться данными через Layer 3 устройства (маршрутизатор или управляемый коммутатор).

Кластер «active/active» использует multicast MAC-адреса. Большинство машрутизаторов и управляемых коммутаторов по умолчанию игнорируют трафик от multicast MAC-адресов. Перед тем как использовать кластер «active/active», убедитесь, что ваши Layer-3 устройства могут обрабатывать multicast MAC адреса.

Требования к коммутаторам и маршрутизаторам

Все коммутаторы и маршрутизаторы, которые находятся в одном broadcast-домене вместе с кластером должны удовлетворять следующим требованиям.

1. Все коммутаторы и маршрутизаторы в broadcast-домене не должны блокировать ARP-запросы, которые содержат multicast MAC-адреса.
    - Это требование необходимо соблюдать на всех коммутаторах и маршрутизаторах в broadcast домене, даже если они напрямую не подключены к устройствам FireCluster.
    - Для неуправляемых коммутаторов второго уровня, это требование выполняется по умолчанию.
    - Маршрутизаторы и большинство управляемых коммутаторов по умолчанию блокируют ARP ответы, которые содержат multicast MAC-адреса.
    - Для более подробной информации об обработке ARP сообщений, содержащих multicast MAC-адреса см. документацию по вашему маршрутизатору или управляемому коммутатору.
    - В некоторых маршрутизаторов вы можете добавить multicast MAC-адрес в качестве статического ARP. Если ваш маршрутизатор поддерживает данный функционал, то добавьте в ARP таблицу multicast MAC-адрес и соответствующий ему IP-адрес кластера.
    - Маршрутизатор не должен поддерживать multicast ARP, как указано в RFC 1812, разделе 3.2.2.
2. Коммутаторы, которые подключаются к External и Trusted интерфейсам кластера, должны передавать кадры, в которых в качестве MAC-адреса назначения используется multicast MAC-адрес, во все порты.
    - Для неуправляемых коммутаторов второго уровня, это требование выполняется по умолчанию.
    - Для маршрутизаторов и большинства управляемых коммутаторов вам необходимо выполнить изменения в конфигурации, а именно вручную добавить порты, на

которые будет передаваться кадры с MAC-адресом назначения равным multicast MAC-адресу кластера.

- Multicast MAC-адрес кластера вы можете посмотреть в закладке **Status Report** в Firebox System Manager, или в диалоговом окне конфигурации FireCluster в Policy Manager.Для более подробной информации см. “Find the multicast MAC addresses for an active/active cluster” on page 231.

Для кластера «active/active» вам также необходимо в конфигурации FireCluster в Policy Manager добавить статические ARP записи для вашего Layer 3 маршрутизатора.

Для более подробной информации о настройке двух коммутаторов для кластера «active/active» см. “Пример настройки коммутаторы и ARP таблицы для кластера «active/active»”

Добавление ARP записей в кластер «active/active»

Кластер «active/active» на всех интерфейсах, подключенных к вашей сети, использует multicast MAC-адреса, которые используются для передачи данных

Для некоторых коммутаторов, подключенных к интерфейсам кластера, вам необходимо добавить запись в ARP таблицу. В противном случае возможны проблемы в работе кластера. Добавить ARP запись вы можете при помощи утилиты Policy Manager.

Для того чтобы добавить ARP-запись в конфигурацию вашего Firebox выполните следующее:

1. В WatchGuard System Manager для того чтобы подключиться к кластеру вам необходимо ввести его IP-адрес. Не используйте IP адрес управления.

2. Нажмите  . Или выберите **Tools** > **Policy Manager**.
   Откроется утилита Policy Manager.

3. Выберите **Network** > **ARP Entries**.
   Откроется диалоговое окно Static ARP Entries.

4. Нажмите **Add**.
   Откроется диалоговое окно Add ARP Entry.

5. Из выпадающего списка **Interface** выберите интерфейс, который будет подключаться к layer 3 коммутатору.

6. В текстовом поле **IP Address** введите IP-адрес коммутатора.

7. В текстовом поле **MAC Address** введите MAC-адрес коммутатора. Нажмите **OK**.
   ARP-запись будет добавлена в список Static ARP Entries list.

8. Повторите п. 4–7 для каждого коммутатора, которые напрямую подключены к интерфейсам FireCluster.

9. Нажмите **OK**.

10. Выберите **File > Save > to Firebox** для того чтобы сохранить сделанные изменения.

Также вам необходимо настроить коммутаторы для работы с кластером «active/active». Для более подробной информации см. “Требования к коммутаторам и маршрутизаторам при использовании кластера «active/active»”

Для более подробной информации о настройке двух коммутаторов для работы с кластером «active/active» см. “Пример настройки коммутаторы и ARP таблицы для кластера «active/active»”

Пример настройки коммутаторы и ARP таблицы для кластера «active/active»

Layer 3 коммутаторы по умолчанию нормально обрабатывают multicast трафик. Поэтому FireCluster работает нормально без каких-либо изменений в конфигурации. Layer 3 коммутатор, порты которого находятся в одном VLAN, также работает без каких-либо проблем. Если же порты Layer 3 коммутатора находятся в разных VLAN, то вам необходимо для корректной работы коммутатора с кластером FireCluster выполнить определенные настройки. Layer 3 коммутаторы, которые маршрутизируют VLAN или/и IP-адреса, блокируют multicast трафик от устройств кластера FireCluster. Для того чтобы коммутатор перестал блокировать multicast трафик от устройств FireCluster, вам необходимо на коммутаторе добавить Multicast MAC адрес и соответствующую запись в ARP-таблицу.

После того, как вы настроите кластер «active/active», то для обеспечения корректной работы кластера и коммутаторов вам необходимо выполнить определенные настройки.

Для более подробной информации см.:

- "Требования к коммутаторам и маршрутизаторам при использовании кластера «active/active»"
- "Добавление ARP записей в кластер «active/active»"

Этот раздел содержит пример настройки коммутаторов и кластера «active/active». Приведенный ниже пример не содержит описания остальной процедуры настройки FireCluster. Для более подробной информации о настройке FireCluster см. "Настройка FireCluster"

Перед тем как начать убедитесь, что у вас есть следующая информация:

- IP и multicast MAC адреса интерфейса FireCluster, к которому подключен коммутатор. Для более подробной информации см. "Определение multicast MAC адресов для «active/active» кластера"
- IP и MAC адреса всех коммутаторов и маршрутизаторов, подключенных к интерфейсам FireCluster

Компания WatchGuard предоставляет своим клиентам специальные инструкции, которые помогут настроить продукты WatchGuard для работы с продуктами других компаний. Для более подробной информации о настройке продуктов других компаний см. информацию о технической поддержке в данном документе.

Пример настройки

В этом примере FireCluster имеет один внешний и один внутренний интерфейсы. Внешний интерфейс каждого устройства кластера подключен к коммутатору Cisco 3750. Внутренние интерфейсы кластера подключены к коммутатору Extreme Summit 15040. Для более подробной информации о командах на других моделях коммутаторов см. документацию по соответствующему устройству. В данном примере мы приводим команды для обоих моделей коммутаторов.

В данном примере используются следующие IP адреса:

- **Интерфейс FireCluster (External)**
  IP адрес: 50.50.50.5024
  Multicast MAC адрес: `01:00:5e:32:32:32`
- **Интерфейс 1 FireCluster (Trusted)**
  IP адрес: 10.0.1.1/24
  Multicast MAC адрес: 01:00:5e:00:01:01
- **Cisco 3750 коммутатор, подключенный к External интерфейсу FireCluster**
  IP адрес: 50.50.50.100
  MAC адрес VLAN интерфейса: 00:10:20:3f:48:10

VLAN ID: 1
Интерфейс: gi1/0/11

- **Extreme Summit 15040 коммутатор подключенный к внутреннему интерфейсу FireCluster**
  IP адрес: 10.0.1.100
  MAC адрес: 00:01:30:f3:f1:40
  VLAN ID: Border-100
  Интерфейс: 9

Настройка коммутатора Cisco

В данном примере коммутатор Cisco подключен к интерфейсу 0 (External) кластера FireCluster. Для того чтобы добавить MAC-адрес и соответствующую запись в ARP таблицу вам необходимо воспользоваться командной строкой коммутатора.

1. Откройте командную строку коммутатора Cisco 3750.

2. Для того чтобы добавить запись в ARP таблицу для multicast MAC-адреса интерфейса FireCluster введите следующую команду:

   arp <FireCluster interface IP address> <FireCluster MAC address> arpa

   Для данного примера вам необходимо ввести следующее:

   arp 50.50.50.50 0100.5e32.3232 arpa

3. Для того чтобы добавить MAC-адрес в таблицу MAC адресов введите следующую команду:

   ```
   mac-address-table static <FireCluster interface MAC address> vlan <ID>
   interface <#>
   ```

   Для данного примера вам необходимо ввести следующее:

   ```
   mac-address-table static 0100.5e32.3232 vlan 1 interface gi1/0/11
   ```

Настройка коммутатора Extreme

В данном примере коммутатор Extreme Summit подключен к интерфейсу 1 (Trusted) кластера FireCluster Для того чтобы добавить MAC-адрес и соответствующую запись в ARP таблицу вам необходимо воспользоваться командной строкой коммутатора.

1. Откройте командную строку Extreme 3750.

2. Для того чтобы добавить запись в ARP таблицу для multicast MAC-адреса интерфейса FireCluster введите следующую команду:

   ```
   configured iparp add <ip address> <MAC Address>
   ```

   Для данного примера вам необходимо ввести следующее:

   ```
   configured iparp add 10.0.1.1/24 01:00:5e:00:01:01
   ```

3. Для того чтобы добавить MAC-адрес в таблицу MAC адресов введите следующую команду:

   ```
   create fdbentry <MAC> VLAN <ID> port <#>
   ```

   Для данного примера вам необходимо ввести следующее:

   ```
   create fdbentry 01:00:5e:00:01:01 VLAN Border-100 port 9
   ```

Добавление записей в ARP таблицу FireCluster для каждого коммутатора

1. При помощи WatchGuard System Manager подключитесь к FireCluster. Для подключения используйте IP адрес интерфейса кластера.

2. Нажмите  . Или выберите Tools > Policy Manager.
   Откроется Policy Manager.

3. Выберите **Network** > **ARP Entries**.
   Откроется диалоговое окно Static ARP Entries.

4. Нажмите **Add**.
   Откроется диалоговое окно Add ARP Entry.

5. В выпадающем списке **Interface** выберите **External**.

6. В текстовом поле **IP Address** введите IP адрес интерфейса коммутатора, который подключен к интерфейсу External.
   Для данного пример введите: `50.50.50.100`

7. В поле the **MAC Address** введите MAC адрес VLAN интерфейса коммутатора, который подключен к интерфейсу External.
   Для данного примера введите: `00:10:20:3f:48:10`

8. Нажмите **OK**.
   ARP запись будет добавлена в список Static ARP Entries.

9. Нажмите **Add**.
   Откроется диалоговое окно Add ARP Entry.

10. В выпадающем списке **Interface** выберите **Trusted**.

11. В текстовом поле **IP Address** введите IP адрес интерфейса коммутатора, который подключен к интерфейсу Trusted.
    Для данного примера введите: `10.0.1.100`

12. В поле the **MAC Address** введите MAC адрес VLAN интерфейса коммутатора, который подключен к интерфейсу Trusted.
    В данном примере введите: `00:01:30:f3:f1:40`

13. Нажмите **OK**.
    ARP запись будет добавлена в список Static ARP Entries.

14. Нажмите **OK** для того чтобы закрыть диалоговое окно **Static ARP Entries**.

15. Выберите **File > Save > to Firebox** для того чтобы сохранить сделанные изменения.

Мастер FireCluster Setup Wizard

Настроить FireCluster вы можете вручную или при помощи мастера FireCluster Setup Wizard.

Для более подробной информации о ручной настройке FireCluster см. “Ручная настройка FireCluster”

Перед тем как использовать FireCluster выполните следующее:

- Убедитесь, что вас есть все необходимые компоненты для настройки FireCluster и его спланированная конфигурация. Для более подробной информации см. “Перед тем, как начать”

- Подключите устройства FireCluster друг к другу и к сетевым элементам, как описано в “Подключение оборудования FireCluster”

FireCluster в режиме «active/active» на всех интерфейсах использует multicast MAC адреса. Перед тем, как включить FireCluster в режиме «active/active», убедитесь, что ваши коммутаторы и маршрутизаторы поддерживают multicast трафик. Для более подробной информации см. “Требования к коммутаторам и маршрутизаторам при использовании кластера «active/active»”

Настройка FireCluster

1. При помощи WatchGuard System Manager подключитесь к устройству WatchGuard, конфигурацию которого вы хотите использовать для кластера. После того, как вы включите FireCluster, это устройство станет master-устройством кластера после первого сохранения конфигурации.

2. Нажмите . Или выберите **Tools** > **Policy Manager**.
   В Policy Manager откроется файл конфигурации для данного устройства.

3. Выберите **FireCluster** > **Setup**.
   Запустится мастер FireCluster Setup Wizard

4. Нажмите **Next**.

5. Выберите режим работы кластера:

   Кластер Active/Active

   Такой режим работы кластера используется для обеспечения резервирования и балансировки нагрузки. Если вы выберете этот режим работы кластера, то весь входящий трафик будет равномерно распределяться между двумя устройствами кластера. Вы не можете использовать режим «active/active» если на интерфейсе External вашего WatchGuard устройства включен DHCP или PPPoE.

   Кластер Active/Passive

   Такой режим работы кластер обеспечивает только резервирование. В этом режиме работы активное устройство кластера обрабатывает весь входящий трафик, а резервное устройство постоянно следит за состоянием активного устройства, и в случае выхода его из строя становится активным.

6. Выберите **Cluster ID**. ID кластера уникальным образом идентифицирует кластер в случае если в этом же broadcast домене у вас есть еще несколько кластеров. Если у вас есть только один кластер, то в качестве ID кластера вы можете использовать значение по умолчанию

7. Если вы выберете **Active/Active** кластер, то вам необходимо выбрать метод балансировки нагрузки (**Load-balance method)** между активными устройствами кластера. Вы можете выбрать две опции:

   Least connection

   В этом режиме каждое новое подключение передается устройству кластера, которое на данный момент обслуживает меньшее число подключений. Этот режим используется по умолчанию.

   Round-robin

   В этом режиме новые подключения распределяются между активными устройства кластера в порядке round-robin. Первое подключение передается первому устройству, второе подключение – второму устройству, и т.д.

8. Выберите основной (**Primary)** и резервный (**Backup) интерфейсы кластера**. Интерфейсы кластера используются для обмена данными между устройствами кластера. Вам необходимо настроить Основной интерфейс кластера. Для того чтобы обеспечить резервирование мы также рекомендуем настроить резервный интерфейс кластера.

   Primary

   Основной интерфейс кластера, который используется для обмена данными между устройствами кластера. В качестве основного интерфейса кластера выберите интерфейс, через который устройства кластера подключены друг к другу.

   Backup

   Резервный интерфейс, который используется для обмена данными между устройствами кластера в случае если основной интерфейс выйдет из строя. В качестве резервного интерфейса кластера выберите второй интерфейс, через который устройства кластера подключены друг к другу, если такой существует.

9. Выберите интерфейс управления (**Interface for Management IP address)**. Через этот интерфейс вы можете напрямую подключаться к устройствам кластера для выполнения каких-либо административных задач. Этот интерфейс не является выделенным интерфейсом. Он также не используется для передачи основного трафика

   Если у вас есть интерфейс, который настроен как выделенный VLAN интерфейс, не выбирайте его в качестве выделенного интерфейса кластера.

10. По запросу мастера введите необходимые данные для каждого устройства кластера:

    Feature Key (Ключ функций)

    Для того чтобы активировать весь функционал устройства Watchguard вам необходимо импортировать или загрузить специальный ключ функций. Если вы ранее импортировали этот ключ в Policy Manager, то мастер автоматически будет использовать этот ключ для первого устройства в кластере.

    Member Name (Имя устройства)

    Имя устройства FireCluster.

    Serial Number (Серийный номер)

    Серийный номер устройства. Серийный номер используется как Member ID в диалоговом

окне **FireCluster Configuration**. Мастер автоматически заполнит это поле после того, как вы импортируете лицензионный ключ для данного устройства.

Primary cluster interface IP address

IP-адрес основного интерфейса кластера, посредством которого устройства кластера будут обмениваться данными. IP-адреса основных интерфейсов кластера каждого устройства должны находиться в одной подсети. Если оба устройства загружаются одновременно, то устройство с самым большим IP-адресом основного интерфейса кластера становится master-устройством.

Backup cluster interface IP address

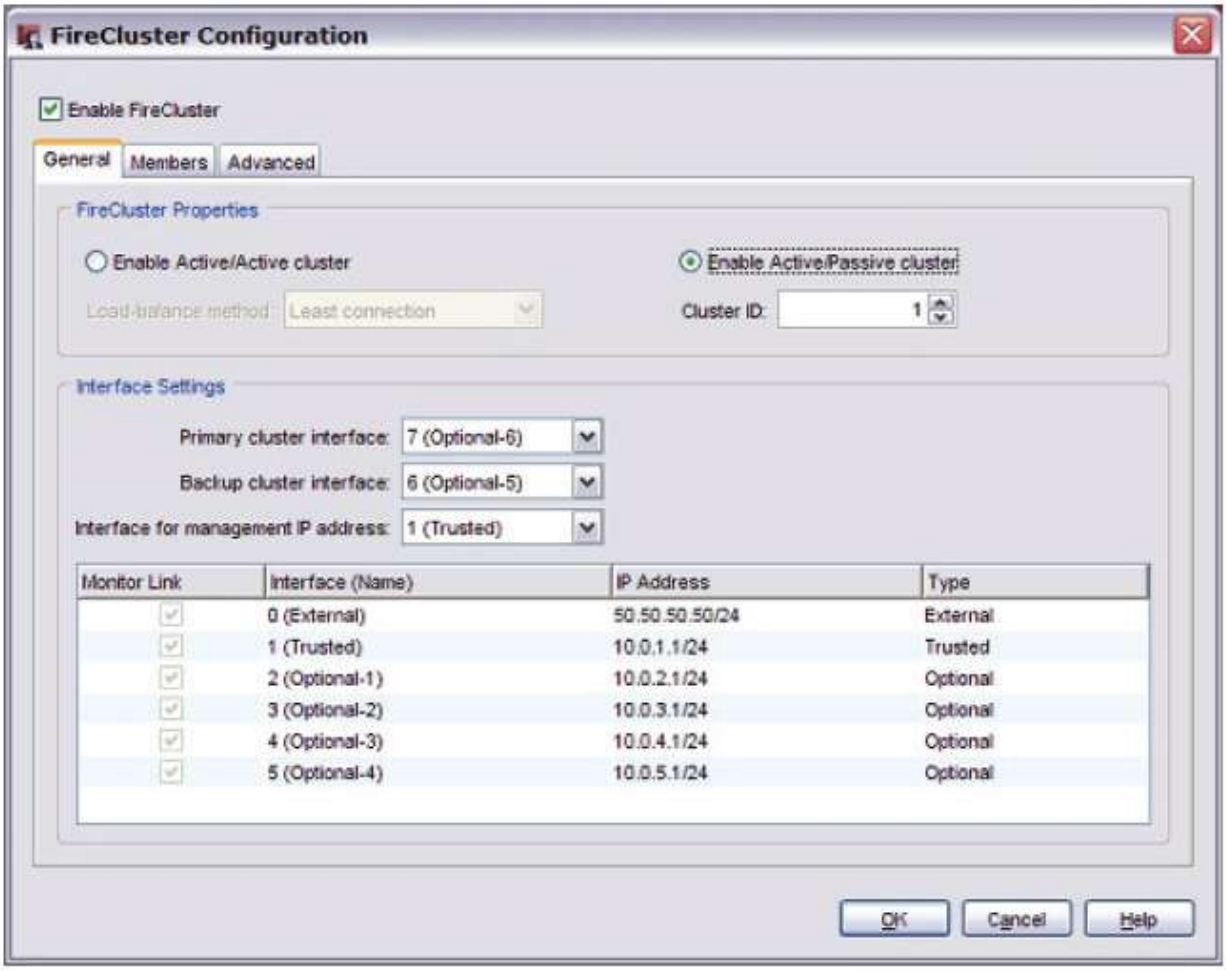
IP-адрес резервного интерфейса кластера, который будет использоваться устройствами кластера для обмена данными в случае если основной интерфейс выйдет из строя. IP-адреса резервных интерфейсов кластера каждого устройства должны находиться в одной подсети.

Management IP address

Уникальный IP-адрес, который используется для прямого подключения к устройству, которое является частью кластера. Для каждого устройства в кластере вам необходимо ввести различные IP-адреса.

11. В последнем окне мастера посмотрите итоговые данные по конфигурации, которые включают параметры интерфейсов, а также список интерфейсов, мониторинг состояния которых будет постоянно выполняться

12. Нажмите **Finish**.
    Откроется диалогое окно FireCluster Configuration



13. В секции **Interface Settings** вы увидите список интерфейсов, состояние которых будет постоянно проверяться системой. Этот список не включает основной и резервный интерфейсы кластера. FireCluster постоянно наблюдает за состоянием подключения на всех включенных интерфейсах. Если master-устройство кластер обнаруживает отсутствие связи на каком-либо из интерфейсах, то для этого устройства запускается процедура переключения.

    Перед тем как сохранить конфигурацию FireCluster вам необходимо отключить все интерфейсы, которые не подключены к вашей сети. Для того чтобы отключить интерфейс выполните следующее:

    - В Policy Manager выберите **Network > Configuration**.
    - Два раза нажмите на интерфейс, который вы хотите отключить и значение **Interface Type** выберите равным **Disabled**.

    Не сохраняйте файл конфигурации до тех пор пока вы не запустите второе устройство в безопасном режиме.

14. Запустите второе устройство WatchGuard в безопасном режиме. Для того чтобы запустить устройство в безопасном режиме, нажмите на кнопку со стрелкой вниз на передней панели устройства

Не отпускайте кнопку со стрелками пока на LCD дисплее не появится надпись `WatchGuard Technologies`. Если устройство работает в безопасном режиме, то на дисплее после номера модели идет слово `safe`.

15. Сохраните конфигурацию на master-устройстве.
Кластер активирован и master-устройство автоматически находит все остальные устройства кластера.

После активации кластера вы можете следить за состоянием устройств кластера в закладке **Front Panel** в Firebox System Manager

Для более подробной информации см. “Мониторинг и управление устройствами FireCluster”

Если второе устройство автоматически не было обнаружено, то вы можете вручную запустить процедуру обнаружения, как описано “Поиск устройств кластера”

Ручная настройка FireCluster

Настроить FireCluster вы можете вручную или при помощи мастера FireCluster Setup Wizard. Для более подробной информации см. “Мастер FireCluster Setup Wizard”

Перед тем как использовать FireCluster выполните следующее:

- Убедитесь, что вас есть все необходимые компоненты для настройки FireCluster, и вы уже спланировали его конфигурацию. Для более подробной информации см. “Перед тем, как начать”

- Подключите устройства FireCluster друг к другу и к сетевым элементам, как описано в “Подключение оборудования FireCluster”

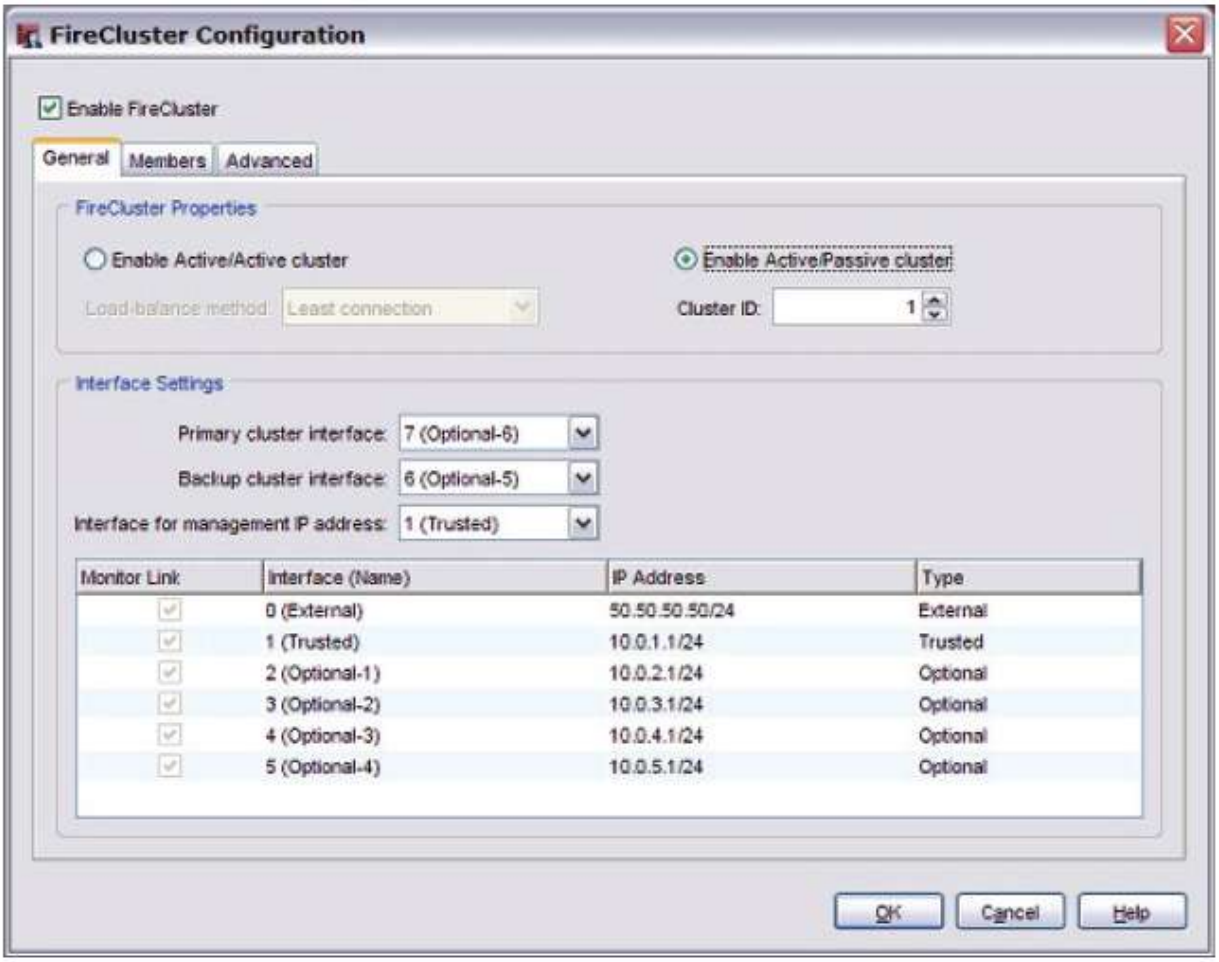
FireCluster в режиме «active/active» на всех интерфейсах использует multicast MAC адреса. Перед тем, как включить FireCluster в режиме «active/active», убедитесь, что ваши коммутаторы и маршрутизаторы поддерживают multicast трафик. Для более подробной информации см. “Требования к коммутаторам и маршрутизаторам при использовании кластера «active/active»”

Активация FireCluster

1. При помощи WatchGuard System Manager подключитесь к устройству WatchGuard, конфигурацию которого вы хотите использовать для кластера. После того, как вы включите FireCluster, это устройство станет master-устройством кластера после первого сохранения конфигурации

2. Нажмите  . Или выберите **Tools** > **Policy Manager**.
Откроется Policy Manager.

3. Выберите **FireCluster** > **Configure**.
   Откроется диалогое окно FireCluster Cluster Configuration



4. Включите опцию **Enable FireCluster**.

5. Выберите режим работы кластера.

   Кластер Active/Active

   Такой режим работы кластера используется для обеспечения резервирования и балансировки нагрузки. Если вы выберете этот режим работы кластера, то весь входящий трафик будет равномерно распределяться между двумя устройствами кластера. Вы не можете использовать режим «active/active» если на External интерфейсе вашего WatchGuard устройства включен DHCP или PPPoE.

   Кластер Active/Passive

   Такой режим работы кластера обеспечивает только резервирование. В этом режиме работы активное устройство кластера обрабатывает весь входящий трафик, а резервное устройство постоянно следит за состоянием активного устройства, и в случае выхода его из строя становится активным.

6. Если вы выберете **Enable Active/Active cluster**, то в выпадающем списке **Load-balance method** выберите метод балансировки нагрузки.

   Least connection

   В этом режиме каждое новое подключение передается устройству кластера, которое на данный момент обслуживает меньшее число подключений. Этот режим используется по умолчанию.

Round-robin

В этом режиме новые подключения распределяются между активными устройства кластера в порядке round-robin. Первое подключение передается первому устройству, второе подключение – второму устройству, и т.д.

7. В выпадающем списке **Cluster ID** выберите идентификатор FireCluster. ID кластера уникальным образом идентифицирует кластер в случае если в этом же broadcast домене у вас есть еще несколько кластеров. Если у вас есть только один кластер, то в качестве ID кластера вы можете использовать значение по умолчанию .

Настройка интерфейсов

Интерфейс FireCluster – это специальный интерфейс, который используется устройствами кластера для обмена данными между собой. Вы можете настроить один или два интерфейсов FireCluster. Для того чтобы обеспечить резервирование мы рекомендуем вам настроить два интерфейса FireCluster. Если у вас есть интерфейс, который настроен как выделенный VLAN интерфейс, не выбирайте его в качестве выделенного интерфейса кластера.

Перед тем как сохранить конфигурацию FireCluster вам необходимо отключить все интерфейсы, которые не подключены к вашей сети.

1. В выпадающем списке **Primary cluster interface** выберите интерфейс, который будет использоваться как основной интерфейс кластера.

2. В выпадающем списке **Backup cluster interface** выберите интерфейс, который будет использоваться как резервный интерфейс кластера.

3. Выберите интерфейс управления (**Interface for management IP address)**. Это интерфейс, через который вы сможете напрямую подключаться к устройству WatchGuard, которое является частью кластера

4. Вы можете посмотреть список интерфейсов, состояние которых с определенной периодичностью проверяется системой. Этот список не включает основной и резервный интерфейсы кластера. FireCluster постоянно наблюдает за состоянием подключения на всех включенных интерфейсах. Если основное устройство кластера обнаруживает отсутствие связи на каком-либо из интерфейсов, то для этого устройства запускается процедура переключения.

5. Для того чтобы отключить интерфейс выберите **Network > Configuration**.

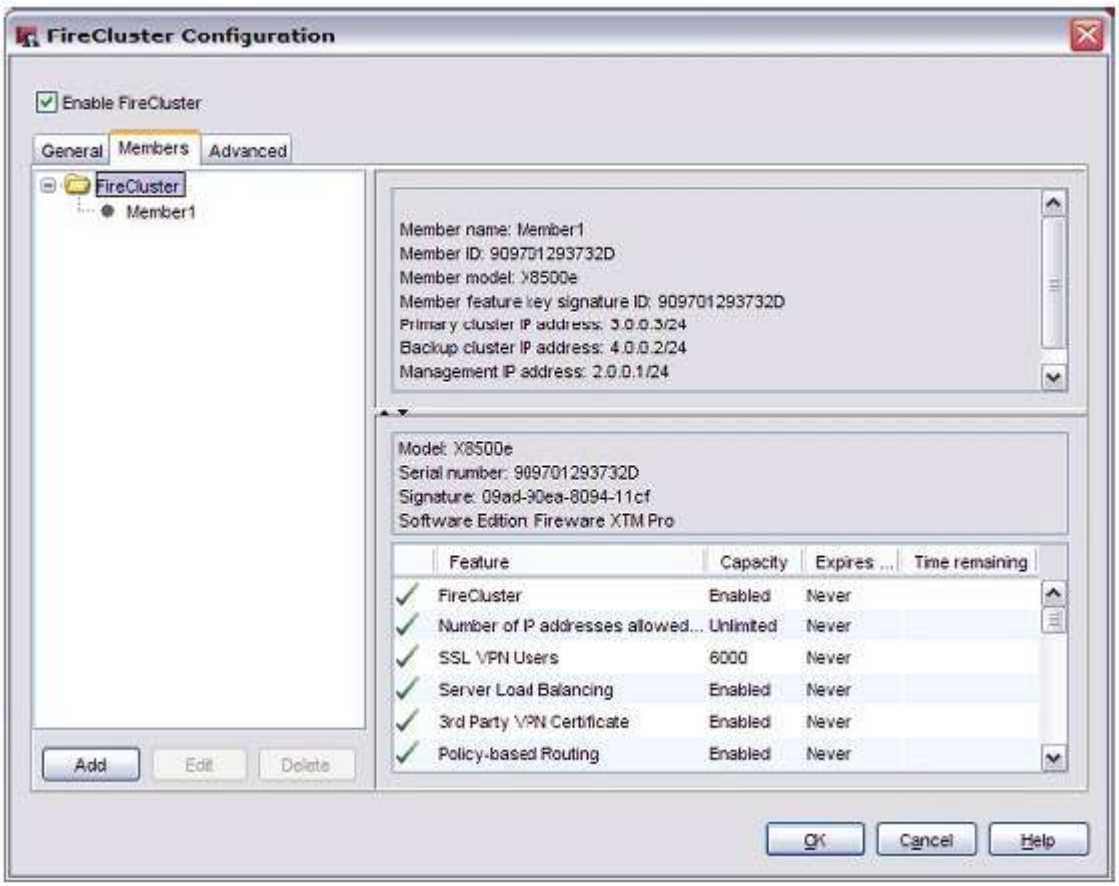
6. Два раза нажмите на интерфейс, который вы хотите отключить

7. Значение **Interface Type** выберите равным **Disabled**.

FireCluster постоянно следит за состоянием всех включенных интерфейсов. Убедитесь, что все интерфейсы в этом списке подключены к коммутатору.

Настройка устройств кластера FireCluster

1. Выберите закладку **Members**.
Откроется страница с конфигурацией всех устройств кластера FireCluster.

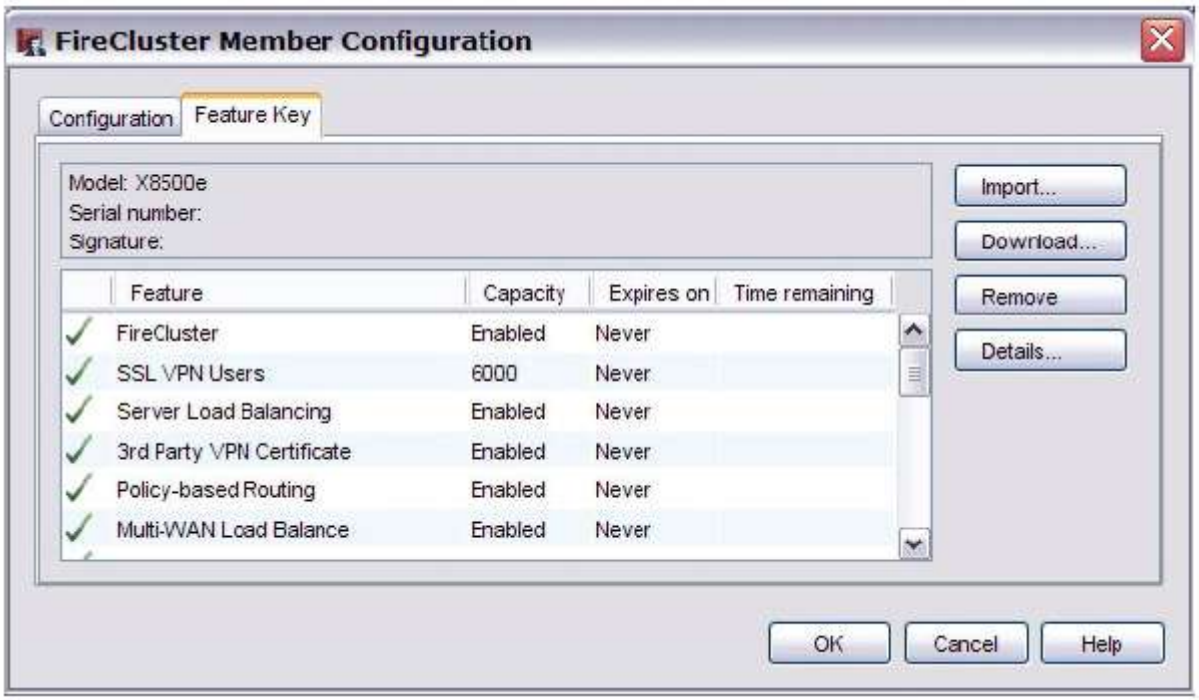


Если ранее импортированный ключ функций находится в этом файле конфигурации, то это устройство автоматически становится Member 1. Если в файле конфигурации нет ключа, то этого устройства в списке устройств кластера не будет. В этом случае вам необходимо добавить каждое устройство вручную и импортировать файл конфигурации для каждого устройства, как описано ниже.

2. Для того чтобы добавить устройство нажмите **Add**.
   Откроется диалогое окно Add member

3. В текстовом поле **Member Name** введите имя устройства. Это имя будет использовать как идентификатор устройства в списке.

4. Выберите закладку **Feature Key**



5. Нажмите **Import**
   Откроется диалоговое окно Import Firebox Feature Key.

6. Для того чтобы найти файл с ключом нажмите **Browse**. Или, скопируйте содержимое файла с ключом в буфер, и затем нажмите **Paste** для того чтобы вставить содержимое буфера в диалоговое окно.

7. Нажмите **OK**.

8. Выберите закладку **Configuration**. В текстовое поле **Serial Number** будет автоматически вставлен серийный номер из лицензионного ключа.

9. В текстовом поле **Interface IP Address** введите IP-адреса, которые вы будете использовать для интерфейсов кластера и интерфейса для IP-адреса управления.

   * В текстовом поле **Primary cluster** введите IP адрес основного интерфейса кластера. IP-адреса основных интерфейсов кластера каждого устройства должны находиться в одной подсети.

   Если оба устройства запустятся одновременно, то master устройством станет устройство с большим IP-адресом основного интерфейса кластера.

   * В текстовом поле **Backup cluster** введите IP адрес резервного интерфейса кластера. Эта опция доступна, только если вы настроили резервный интерфейс кластера. IP-адреса резервных интерфейсов кластера каждого устройства должны находиться в одной подсети.

   * В текстовом поле **Interface for management IP address** введите IP-адрес, который будет использоваться для подключения напрямую к устройствам кластера. Этот интерфейс управления не является выделенным интерфейсом и не используется для основного трафика. IP-адрес этого интерфейса должен быть уникален среди всех устройств в кластере.

10. Нажмите **OK**.
    Добавленное вами устройство появится в закладке Members.

11. Для того чтобы добавить второе устройство в кластер повторите предыдущие пункты.

    Не сохраняйте конфигурацию пока не запустите второе устройство в безопасном режиме.

12. Запустите второе устройство WatchGuard в безопасном режиме. Для того чтобы запустить устройство в безопасном режиме, нажмите на кнопку со стрелкой вниз на передней панели устройства.

    Для устройств Firebox X Core или Peak device, Не отпускайте кнопку со стрелками пока на LCD дисплее не появится надпись `WatchGuard Technologies`. Если устройство работает в безопасном режиме, то на дисплее после номера модели идет слово `safe`..

    Для устройств WatchGuard XTM, Не отпускайте кнопку со стрелками пока на LCD дисплее не появится надпись `Safe Mode Starting...`. Если устройство работает в безопасном режиме, то на дисплее после номера модели идет слово `safe`.

13. Сохраните конфигурацию на master-устройстве.
    Кластер активирован и master-устройство автоматически находит все остальные устройства кластера.

После активации кластера вы можете следить за состоянием устройств кластера в закладке **Front Panel** в Firebox System Manager

Для более подробной информации см. “Monitor and control FireCluster members” on page 234.

Если второе устройство автоматически не было обнаружено, то вы можете вручную запустить процедуру обнаружения, как описано “Поиск устройств кластера”

Определение multicast MAC адресов для «active/active» кластера

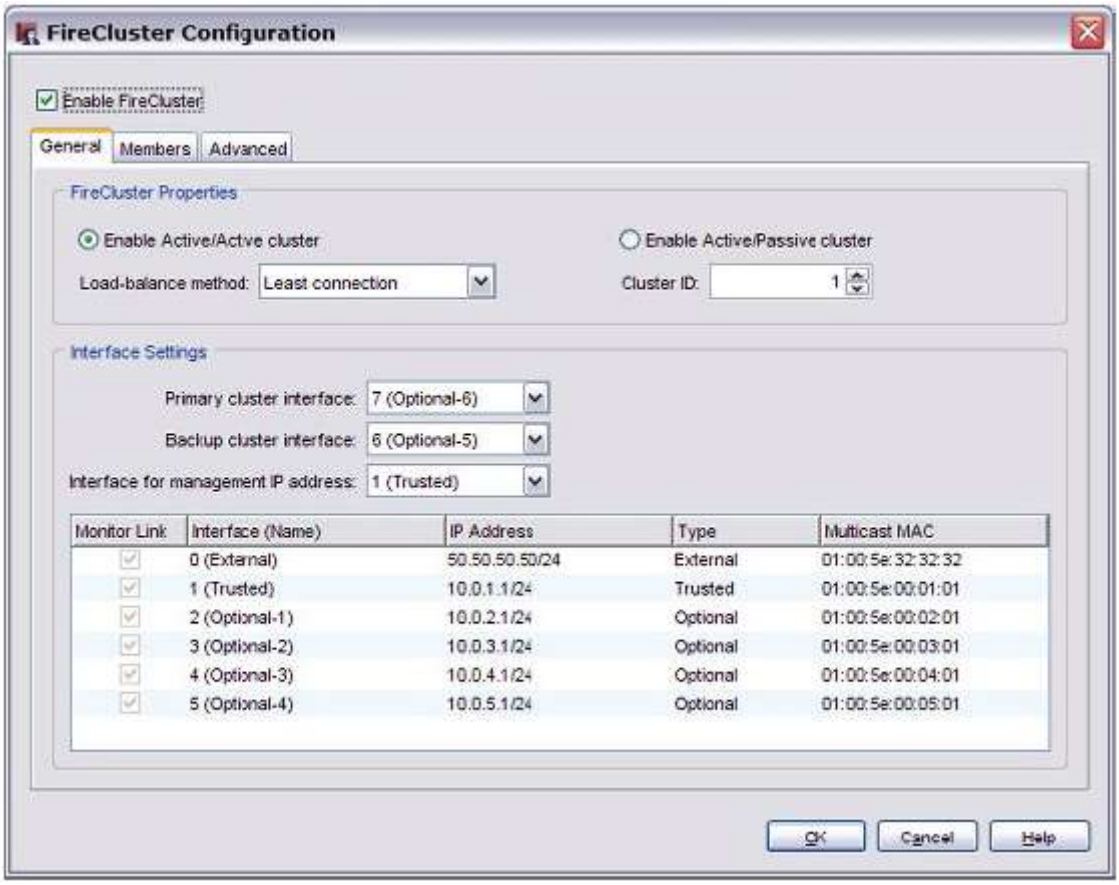
Для того чтобы настроить поддержку multicast MAC-адресов кластера на ваших коммутаторах вам необходимо знать multicast MAC-адреса, которые используются кластером на каждом из интерфейсов.

Поиск MAC адресов в Policy Manager

1. Откройте Policy Manager для «active/active» кластера.

2. Выберите **FireCluster** > **Configure**.
   Откроется диалогое окно FireCluster Configuration.

3. В секции **Interface Settings** вы увидите все необходимые multicast MAC-адреса



Для того чтобы скопировать multicast MAC адрес из конфигурации FireCluster на ваш коммутатор или маршрутизатор выполните следующее:

1. В колонке **Multicast MAC** два раза нажмите на MAC адрес.
   При этом MAC адрес будет выделен.

2. Кликните и поведите курсором в сторону, чтобы выделить MAC адрес более темным цветом.

3. Нажмите Ctrl+C для того чтобы скопировать MAC-адрес в буфер

4. Вставьте MAC-адрес в конфигурацию вашего коммутатора или маршрутизатора.

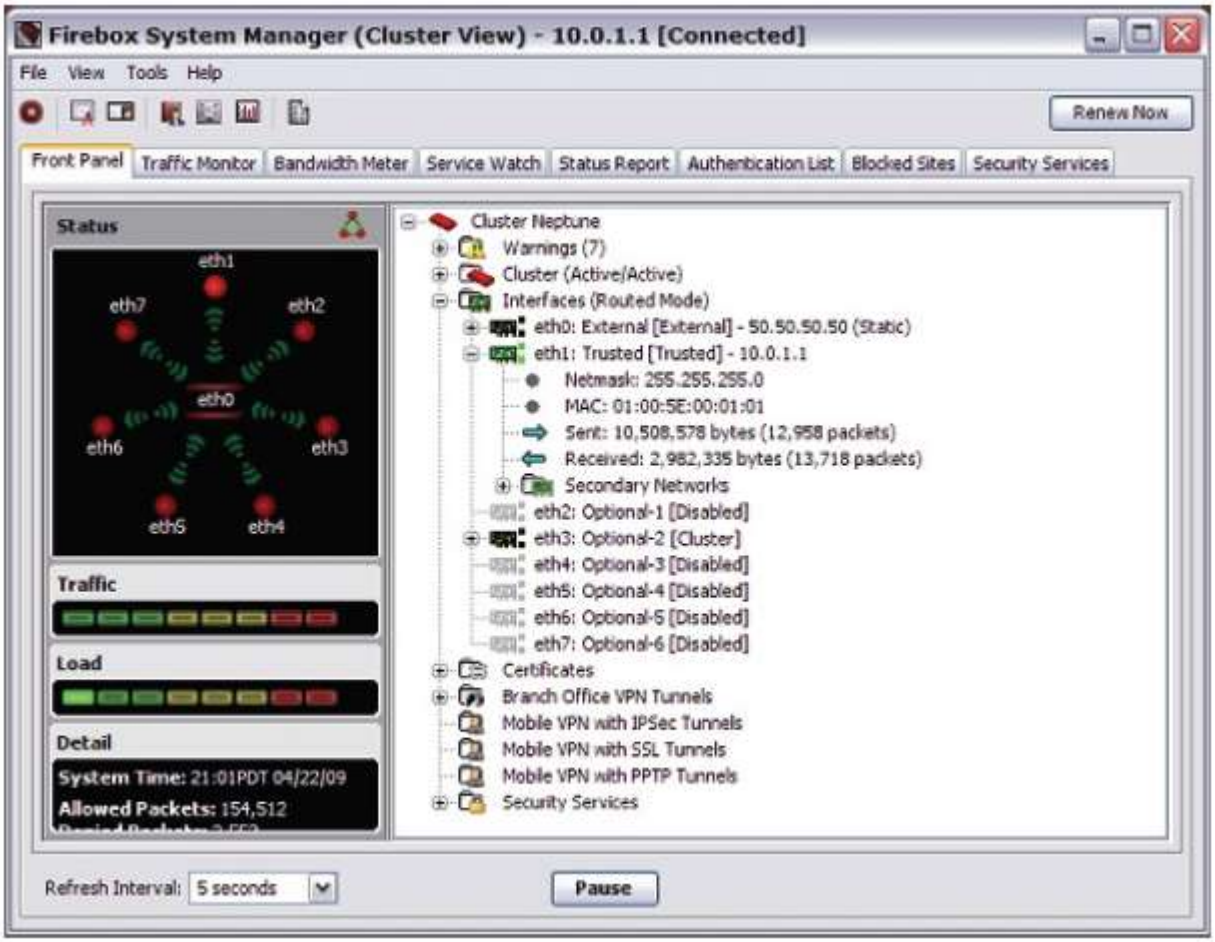
Поиск MAC адреса в Firebox System Manager

Вы также можете посмотреть multicast MAC адреса в Firebox System Manager.

1. Откройте Firebox System Manager

2. Выберите закладку **Front Panel**.

3. Откройте элемент **Interfaces**.
   В списке вы увидите Multicast MAC адрес для каждого интерфейса.



Мониторинг и управление устройствами FireCluster

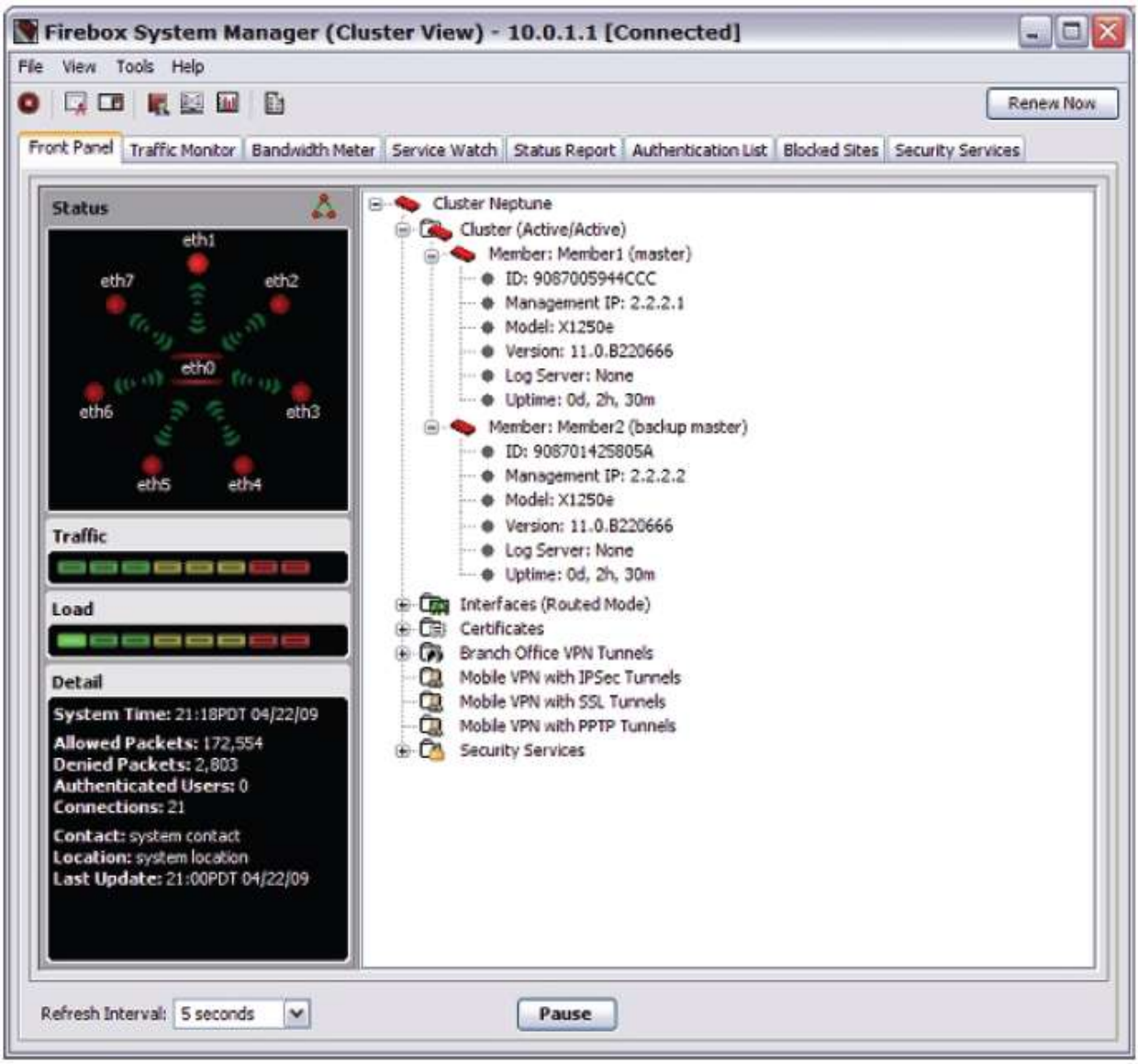
Для мониторинга и управления кластером вы можете использовать IP адрес Trusted интерфейса. В Firebox System Manager вы можете посмотреть всю необходимую информацию об устройствах кластера. В FSM вы можете посмотреть состояние всех устройств кластера так, как будто кластер представляет собой одно устройство.

Для того посмотреть текущее состояние кластера выполните следующее:

1. В Policy Manager подключитесь к Trusted IP-адресу кластера.

2. Нажмите  .
   Откроется Firebox System Manager.

Если вы подключились к Trusted IP-адресу кластера то в закладке **Front Panel** утилиты Firebox System Manager вы можете посмотреть все устройства кластера. Остальные закладки содержат общую информацию для всех устройств кластера



Мониторинг состояния устройств FireCluster

Закладки Firebox System Manager содержат информацию обо всех устройствах кластера. В закладке **Front Pane**l вы можете посмотреть статус каждого устройства кластера. Остальные закладки содержат общую информацию для всех устройств кластера.

Для мониторинга и управления отдельным устройством кластера вы можете использовать интерфейс управления. Если вы хотите посмотреть информацию только для одного устройства кластера, вы не сможете информацию обо всем кластере

Мониторинг и управление устройствами кластера

Вы также при помощи Firebox System Manager может следить за состоянием, а также управлять отдельным устройством кластера. Несмотря на то, что все операции FireCluster выполняются автоматически, вы можете вручную выполнять некоторые функции в Firebox System Manager.

Для того чтобы управлять устройствами кластера, выполните следующее:

1. Выберите **Tools** > **Cluster**.

2. Выберите функцию:

   * Поиск устройств кластера

   * Переключение master-устройства

   * Запуск устройства в безопасном режиме

   * Переключение master-устройства

   * Перезагрузка устройства кластера

   * Выключение устройства

   * Подключение к устройству кластера

   * Отключение устройства от кластера

   * Подключение устройства к кластеру

Поиск устройств кластера

После того, как вы добавите устройство в FireCluster, master-устройство автоматически его обнаружит. При помощи команды *Discover member* вы можете запустить процедуру поиска master-устройством как новых, так и существующих устройств кластера.

Перед тем как начать, убедитесь, что устройство:

- Правильно подключено к сети, как описано в разделе “Подключение оборудования FireCluster”.
- Настроено как элемент кластера. Настроить устройство вы можете двумя способами:

  * Мастер FireCluster Setup Wizard

  * Ручная настройка FireCluster

Для того чтобы запустить процедуру поиска выполните следующее:

1. Если это новое устройство, то загрузите его в безопасном режиме. Для более подробной информации см. ниже.
2. В WatchGuard System Manager подключитесь к master-устройству кластера.
3. Запустите Firebox System Manager.
4. Выберите **Tools** > **Cluster** > **Discover member**.
   Откроется диалогое окно Discover member.

5. Введите пароль конфигурации для кластера.
   Появится сообщение, которое информирует вас о том, что процесс поиска устройств начат.

6. Нажмите **OK**.
   Master устройство будет искать устройства, которые были подключены к кластеру.

Если master устройство обнаруживает новое устройство, то оно проверяет его серийный номер. Ес ли серийный номер совпадает с серийным номером, указанным в конфигурации FireCluster, то оно загружает конфигурацию кластера на него. После этого устройство становится активным устройством. После этого второе устройство синхронизирует все необходимые данные с master-устройством.

После того, как устройство было обнаружено и выполнило первоначальную синхронизацию, оно будет добавлено в закладку **Front Panel** в качестве элемента кластера.

Запуск устройства в безопасном режиме

1. Для того чтобы запустить устройство в безопасном режиме, нажмите на кнопку со стрелкой вниз на передней панели устройства

2. Для устройств Firebox X Core или Peak device, Не отпускайте кнопку со стрелками пока на LCD дисплее не появится надпись `WatchGuard Technologies`. Если устройство работает в безопасном режиме, то на дисплее после номера модели идет слово `safe`..

3. Для устройств WatchGuard XTM, Не отпускайте кнопку со стрелками пока на LCD дисплее не появится надпись `Safe Mode Starting....`

4. Отпустите кнопку. Если устройство работает в безопасном режиме, то на дисплее после номера модели идет слово `safe`.

Переключение master-устройства

При помощи команды **Failover Master** запустить процедуру переключения master-устройства. При этом резервное master-устройство становится активным master-устройством, а активное - резервным.

1. Выберите **Tools** > **Cluster** > **Failover master**.
   Откроется диалоговое окно Failover Master.

2. Введите пароль конфигурации.

3. Нажмите **OK**.
   Активное master устройство становится резервным, а резервное становится активным.

Перезагрузка устройства кластера

Для того чтобы перезагрузить устройство кластера выполните следующее.

1. Выберите **Tools** > **Cluster** > **Reboot member**.
   Откроется диалогое окно Reboot member.

2. Выберите устройство, которое вы хотите перезагрузить

3. Введите пароль конфигурации.

4. Нажмите **OK**.
   Устройство кластера перезагружается.

Если вы перезагрузите master устройство, то происходит переключение. После перезагрузки устройство возвращается в кластер в качестве резервного master устройства.

Выключение устройства

Для того чтобы выключить устройство кластера в Firebox System Manager выполните следующее.

1. Выберите **Tools** > **Cluster** > **Shutdown member**.
   Откроется диалогое окно Shutdown member.

2. Выберите устройство, которое вы хотите выключить.

3. Введите пароль конфигурации.

4. Нажмите **OK**.
Выбранное устройство будет выключено. Трафик, который проходил через это устройство, перенаправляется на другие активные устройства кластера.

Подключение к устройству кластера

Если вы подключитесь к FireCluster через WatchGuard System Manager, то вам будет доступна информация для всех устройств кластера. Для того чтобы посмотреть информацию для отдельного устройства кластера, вы можете напрямую подключиться к нему через Firebox System Manager (FSM). Существует два метода подключения через FSM:

Основное меню FSM или контекстное меню.

Для того чтобы подключиться к устройству кластера через основное меню выполните следующее:

1. Выберите **Tools** > **Cluster** > **Connect to member**.
   Откроется диалогое окно Connect to member.

2. Выберите устройство, к которому вы хотите подключиться.

3. Нажмите **OK**.
   Для выбранного устройства откроется еще одно окно Firebox System Manager.

Для того чтобы подключиться к устройству кластера через контекстное меню выполните следующее:

1. В закладке **Front Panel** выберите устройство, к которому вы хотите подключиться.

2. Нажмите на него правой кнопкой и выберите **Connect to Member**.

Отключение устройства от кластера

Если для подключения к устройству кластера вы используете IP-адрес управления, то в Firebox System Manager вам будет доступна команда **Leave**. Команда **Leave** является частью процедуры восстановления резервного образа FireCluster.

Когда устройство отключается от кластера, оно все еще является частью конфигурации кластера, но не участвует в работе самого кластера. После того, как устройство отключается из кластера, весь его трафик переносится на другие активные устройства кластера.

Для того чтобы отключить устройство от кластера выполните следующее:

1. В WatchGuard System Manager подключитесь к резервному master-устройству (используйте IP адрес управления).

2. Запустите Firebox System Manager для резервного master-устройства.

3. Выберите **Tools** > **Cluster** > **Leave**.
   Резервное master-устройство будет отключено от кластера и перезагрузится.

Для более подробной информации о процедуре восстановления резервной копии образа устройств кластера см. “Восстановление образа FireCluster”

Подключение устройства к кластеру

Команда **Join** доступна в Firebox System Manager только в том случае, если вы подключились к устройству кластера через интерфейс управления, и если вы до этого при помощи команды **Leave**

удалили устройство из кластера. Команды Leave и Join являются частью процедуры восстановления резервной копии образа FireCluster.

1. В WatchGuard System Manager подключитесь к резервному master-устройству через интерфейс управления. Если в восстановленном вами образе настроен другой интерфейс управления или другой пароль конфигурации, то вы можете заново подключиться к устройству, используя данные восстановленного образа.

2. Запустите Firebox System Manager для резервного master-устройства.

3. Выберите **Tools** > **Cluster** > **Join**.
Резервное master-устройство перезагрузится и подключится к кластеру.

Для более подробной информации об интерфейсе управления см. “Настройка интерфейса управления”

Для более подробной информации о процедуре восстановления резервной копии образа устройств кластера см. “Восстановление образа FireCluster”

Добавление или удаление устройства

При помощи Policy Manager вы можете добавлять устройства в кластер, а также удалять их оттуда.

Удаление устройства из FireCluster

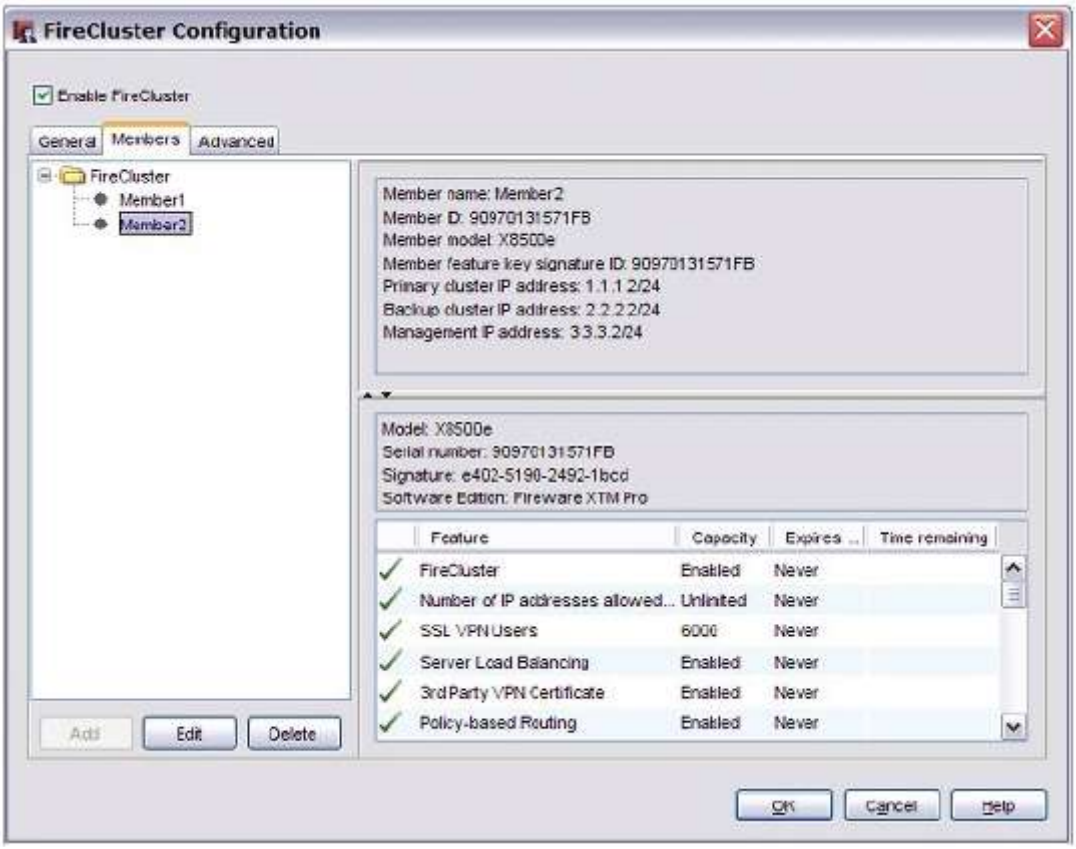
Для того чтобы удалить устройство из FireCluster выполните следующее:

1. В WatchGuard System Manager откройте конфигурацию для master-устройства.

2. Нажмите  . Или выберите **Tools** > **Policy Manager**.
Откроется Policy Manager.

3. Выберите **FireCluster** > **Configure**.
Откроется диалогое окно FireCluster Cluster Configuration.

4. Выберите закладку **Members**.
   Список устройств кластера появится слева



5. Выберите устройство, которое вы хотите удалить.

6. Нажмите **Delete**.
   Устройство будет удалено из списка.

7. Нажмите **OK**.

8. Сохраните файл конфигурации.
   Устройство будет удалено из кластера.

При сохранении файла конфигурации Policy Manager проверяет, является ли текущее master-устройство членом кластера. Если удаленное устройство является текущим master устройством, то Policy Manager пытается запустить процедуру переключения, при этом резервное master-устройство становится новым активным master-устройством кластера. Если процедура переключения происходит успешно, то изменения в конфигурации успешно сохраняются. Если процедура переключения произошла неуспешно, то Policy Manager запрещает вам сохранять конфигурацию.

После того как вы удалите устройство WatchGuard из кластера, при сохранении конфигурации удаленное устройство перезагружается с заводскими настройками. Master-устройством становится другое устройство кластера.

Для более подробной информации о master-устройстве и процедуре переключения см. “Мониторинг и управление устройствами FireCluster”

Добавление устройства в FireCluster

Добавить устройство в кластер вы можете в диалоговом окне **FireCluster Configuration** закладки **Members**. Для того чтобы добавить устройство в кластер выполните следующее:

1. Нажмите **Add**.

2. Выполните все необходимые настройки нового устройства кластера. Для более подробной информации см. “Ручная настройка FireCluster”. При включении FireCluster вам необходимо хотя бы одно устройство в кластере

3. Для того чтобы удалить оба устройства из кластера вам необходимо отключить кластер. Для более подробной информации см. “Отключение FireCluster”

Обновление конфигурации FireCluster

Обновление конфигурации FireCluster происходит также, как и обновление конфигурации на отдельном устройстве WatchGuard. Сохранять изменения конфигурации вы можете только на master-устройстве.

1. В WatchGuard System Manager, нажмите  . Или выберите **File** > **Connect To Device**.
Откроется диалогое окно Connect to Firebox.

2. Выберите или введите Trusted IP адрес для кластера. Введите пароль состояния (read-only). Нажмите **OK**.
Кластер появится как устройство в закладке Device Status.

3. В закладке **Device Status** выберите кластер.

4. Нажмите  . Или выберите **Tools** > **Policy Manager**.
Откроется Policy Manager с текущим файлом конфигурации кластера.

5. Выполните необходимые изменения конфигурации кластера.

6. Сохраните файл конфигурации на Trusted IP адрес кластера.

После того, как вы сохраните конфигурацию кластера, master-устройство автоматически разошлет эту информацию всем остальным устройствам кластера.

Настройка журнала и уведомлений FireCluster

Закладка **Advanced** в диалоговом окне **FireCluster Configuration** содержит настройки журнала и уведомлений. Сообщения журнала всегда создаются для каких-либо событий FireCluster.

Для того чтобы настроить уведомления для процедуры переключения FireCluster выполните следующее:

1. Нажмите **Notification**.

2. Выберите метод уведомлений: SNMP ловушка, электронное сообщение или всплывающее окно

Для того чтобы включить журнал для событий FireCluster в Policy Manager выполните следующее:

1. Выберите **Setup** > **Logging**.

2. Нажмите Diagnostic Log Level.

Ключи функций и FireCluster

Каждое устройство в кластере имеет свой ключ функций. Во время настройки FireCluster, вы импортируете ключи для каждого устройства кластера. FireCluster содержит набор ключей Cluster Features, которые применяются ко всему кластеру. Ключи Cluster Features основаны на лицензионных ключах для всех устройств кластера.

При включении FireCluster для каждого устройства кластера работают следующие сервисы и обновления:

BOVPN и Mobile VPN обновления

Лицензии для Branch Office VPN и Mobile VPN распределяются между всеми устройствами кластера. Если вы приобретете дополнительные BOVPN или Mobile VPN лицензии для каждого устройства в кластере, эта дополнительная емкость будет распределена между всеми устройствами кластера.

Например, если у вас есть два устройства в кластере, и ключ каждого устройства имеет лицензию на 2,000 Mobile VPN пользователей, то лицензия для FireCluster это 4,000 Mobile VPN пользователей.

Подписка на LiveSecurity Service

Подписка LiveSecurity Service привязана к одному устройству, даже если оно работает в кластере. Активная подписка на LiveSecurity Service должна быть для каждого устройства в кластере.

Сервисы безопасности (Subscription Services)

Такие сервисы безопасноси, как WebBlocker, spamBlocker и Gateway AV, работают по-разному для различных режимов работы кластера: «active/active» и «active/passive».

- Active/Active — Вам необходимы одни и те же сервисы, активированные в ключе функций, для обоих устройств. Каждое устройство кластера использует сервисы, активированные в его собственном ключе функций.

- Active/Passive — Вам необходимо активировать сервисы только для одного устройства кластера. Активное устройство кластера использует сервисы, которые активированы в лицензионном ключе любого из устройств.

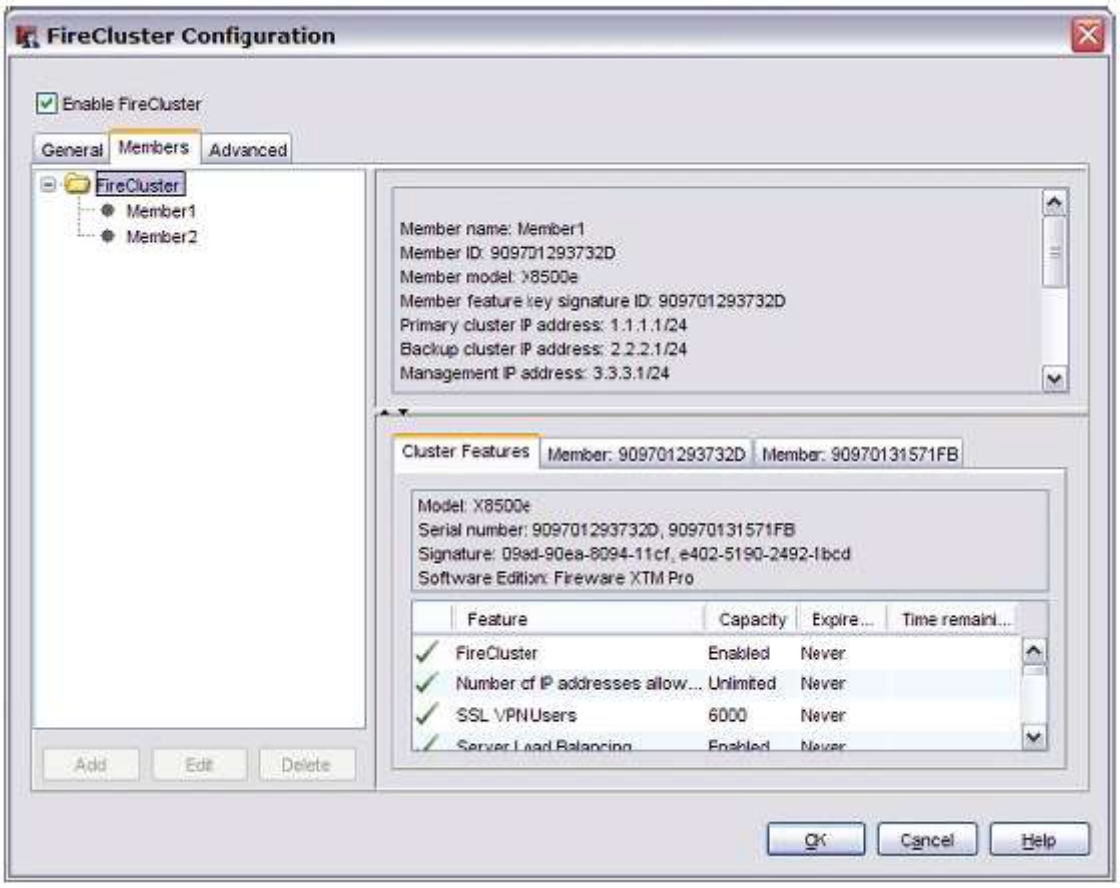
В кластере «active/active» очень важно своевременно обновлять подписку на сервисы для обоих устройств кластера. Если срок действия сервисов истек на одном устройстве кластера «active/active», то эти сервисы не будут работать на этом устройстве. Устройство с истекшей лицензией будет пропускать трафик без применения сервисов.

Просмотр ключей функций и компонентов кластера

1. Откройте Policy Manager для основного устройства.

2. Выберите **FireCluster** > **Configure**.

3. Выберите закладку **Members**



4. Выберите каталог **FireCluster**.
   Закладки с Cluster features и компоненты для каждого устройства появляются в нижней части диалогового окна.

5. Для того чтобы посмотреть лицензионные компоненты выберите закладку **Cluster Features**.

   * В колонках **Expires on** и **Time remaining** указана дату истечения срока действия лицензии и количество дней, которое осталось до истечения срока действия сервиса для всех устройств кластера.

   * В колонке **Capacity** показана емкость кластера.

6. Для того чтобы посмотреть лицензии для каждого устройства кластера выберите закладку **Member**. Проверьте дату истечения срока действия сервисов для каждого устройства кластера.

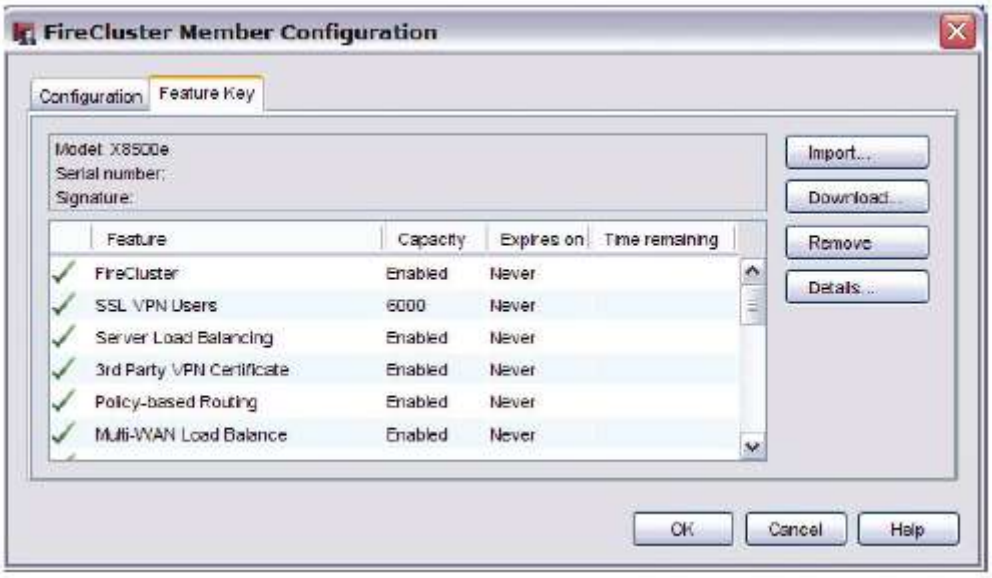
Просмотр или обновление ключа функций для устройств кластера

Для того чтобы посмотреть или обновить ключ функций в Policy Manager выполните следующее.

1. Выберите **FireCluster** > **Configure**.

2. Выберите закладку **Members**.

3. В дереве **FireCluster** выберите устройство. Нажмите **Edit**.
Откроется диалогое окно FireCluster Member Configuration



4. Выберите закладку **Feature Key**. Закладка содержит информацию о компонентах, активированных в этом ключе. Эта закладка включает также следующую информацию:

   * Включен или выключен данный компонент

   * Значение компонента (например количество разрешенных VLAN интерфейсов)

   * Дата истечения срока действия компонента

   * Количество дней, которое осталось до окончания действия компонента

5. Нажмите **Import**.
Откроется диалогое окно Import Firebox Feature Key.

6. Для того чтобы найти ключ функций нажмите **Browse**. Или скопируйте текст ключа и нажмите **Paste** для того чтобы вставить его в диалоговое окно. Нажмите **OK**.

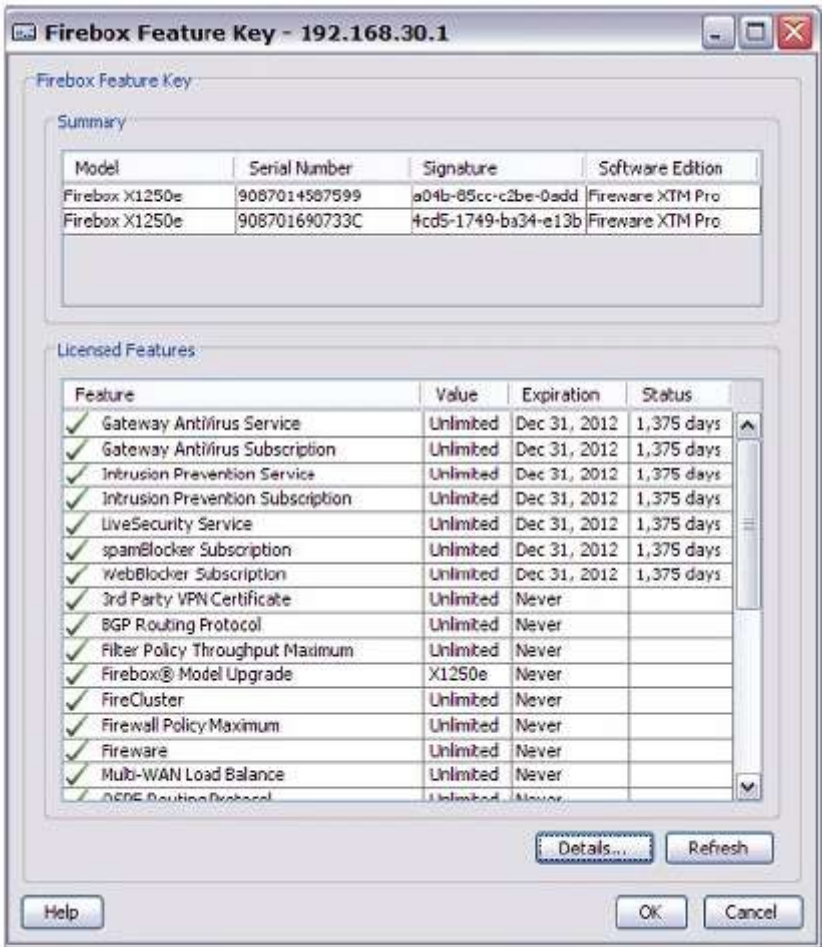
7. Сохраните файл конфигурации.
Лицензионный ключ не будет работать в кластере до тех пор пока не сохраните файл конфигурации на master устройстве.

Для того чтобы посмотреть информацию о ключе функций вы также можете выбрать **Setup > Feature Keys** в Policy Manager

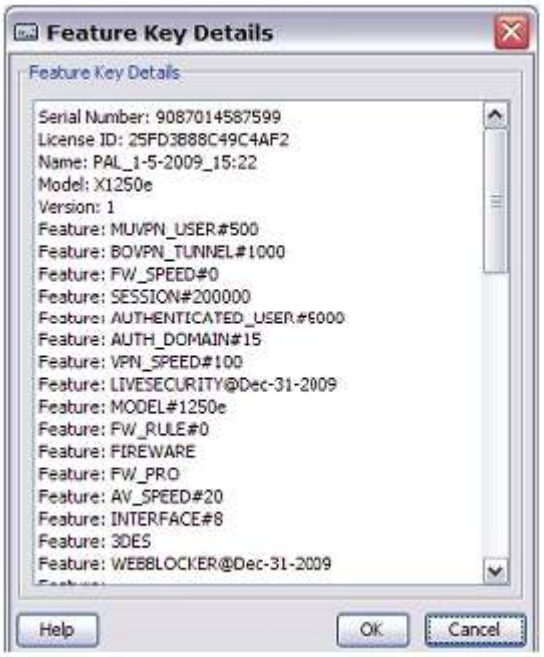
Ключ функций FireCluster в Firebox System Manager

Для того чтобы посмотреть информацию о лицензионном ключе в Firebox System Manager выполните следующее:

1. Выберите **View** > **Feature Keys**.
   Откроется диалогое окно Firebox Feature Key. Секция Licensed Features содержит информацию о лицензионных компонентах для всего кластера



2. Для того чтобы посмотреть более подробную информацию о ключе функций каждого устройства нажмите **Details**



3. Прокрутите вниз для того чтобы посмотреть информацию о ключе функций для второго устройства.

Создание резервной копии образа FireCluster

Так как основное устройство синхронизирует конфигурацию с остальными устройствами кластера, вам необходимо только создать его резервную копию образа FireCluster

Для того чтобы создать резервную копию образа flash памяти (.fxi) master-устройства выполните следующее:

1. В WatchGuard System Manager подключитесь к master-устройству (Trusted IP-адрес).
2. Откройте Policy Manager для master-устройства.
3. Создайте резервную копию образа Firebox.

Для того чтобы создать резервную копию отдельного устройства кластера выполните следующее:

1. В WatchGuard System Manager подключитесь к master-устройству (Trusted IP-адрес).
2. Откройте Policy Manager для устройства кластера.
3. Создайте резервную копию образа Firebox.

Запомните IP-адрес управления и пароль конфигурации в резервной копии образа. Если вы будете восстанавливать FireCluster из этого образа вам понадобится эта информация. После того как резервное master устройство будет отключено от кластера не делайте никаких изменений в конфигурации.

Восстановление образа FireCluster

Для того чтобы восстановить образ Flash-памяти FireCluster, вам необходимо восстановить образ для каждого члена кластера. Резервное master устройство необходимо отключить от кластера перед тем как восстанавливать образ для каждого устройства кластера. После того, как вы

восстановите все образы, вам необходимо заново подключить резервное master устройство к кластеру.

При восстановлении образа подключение к устройствам осуществляется через интерфейс управления. Все остальные интерфейсы неактивны до тех пор, пока процедура восстановления не закончится и резервное устройство не подключится обратно к кластеру.

Отключение резервного устройства от кластера

1. В WatchGuard System Manager через интерфейс управления подключитесь к резервному master-устройству.

2. Запустите для него Firebox System Manager.

3. Выберите **Tools** > **Cluster** > **Leave**.
   Резервное устройство отключится от кластера и перезагрузится.

Восстановление резервной копии образа на резервном master-устройстве

1. В WatchGuard System Manager через интерфейс управления подключитесь к резервному master-устройству.

2. Запустите для него Firebox System Manager.

3. Выберите **File > Restore** для того чтобы восстановить копию образа.
   Устройство перезагрузится и запустится с восстановленной конфигурацией.

После того, как вы восстановите образ на устройстве, то это устройство в WatchGuard System Manager и Firebox System Manager будет отображаться как часть кластера. Кластер не будет работать до тех пор, пока резервное устройство заново не подключится к кластеру

Восстановление резервной копии образа на основном устройстве

1. В WatchGuard System Manager через интерфейс управления подключитесь к основному устройству.

2. Запустите для него Firebox System Manager

3. Выберите **File > Restore** для того чтобы восстановить копию образа.
   Устройство перезагрузится и запустится с восстановленной конфигурацией.

   Для более подробной информации см. “Восстановление образа FireCluster”.

4. В WatchGuard System Manager через интерфейс управления подключитесь к master-устройству.

Если восстановленный образ содержит другой интерфейс управления или другой пароль конфигурации, то вам необходимо в качестве интерфейса управления и паролей использовать интерфейс и пароль, которые содержатся в этом образе.

Подключение резервного master устройства к кластеру

1. В WatchGuard System Manager через интерфейс управления подключитесь к резервному master-устройству. Если восстановленный образ содержит другой интерфейс управления или другой пароль конфигурации, то вам необходимо в качестве интерфейса управления и паролей использовать интерфейс и пароль, которые содержатся в этом образе.

2. Запустите для него Fireware System Manager.

3. Выберите **Tools** > **Cluster** > **Join**.
Резервное устройство перезагрузится и подключится к кластеру.

Обновление Fireware XTM для устройств FireCluster

При помощи Policy Manager вы можете обновить ПО Fireware XTM для всех устройств в кластере FireCluster.

После обновления ПО на устройстве, оно перезагрузится. Когда процедура обновления ПО идет на одном устройстве весь трафик обслуживается другим устройством кластера. После перезагрузки устройство с обновленным ПО снова подключается к кластеру. Так как кластер не может балансировать нагрузку во время перезагрузки, то мы рекомендуем обновление ПО для кластера в режиме «active/active» на время, когда объемы трафика не велики.

Для того чтобы обновить Fireware XTM на устройстве выполните следующее:

1. Откройте файл конфигурации в Policy Manager
2. Выберите **File** > **Upgrade**.
3. Введите пароль конфигурации.
4. Введите или выберите каталог для файла обновления.
5. Для того чтобы создать резервную копию образа нажмите **Yes**.
Откроется список устройств кластера.
6. Выберите устройства, ПО для которых вы хотите обновить.
По окончании обновления каждого устройства на экране появится сообщение об окончании процедуры обновления.

После того, как обновление будет завершено, каждое устройство перезагружается и снова подключается к кластеру. Если вы одновременно обновляете ПО для обоих устройств кластера, то процедура обновления происходит по порядку для каждого устройства. Это позволит не обрывать трафик во время процедуры обновления.

Сначала Policy Manager обновляет резервное устройство. После окончания процедуры обновления, это устройство становится основным активным устройством. Затем Policy Manager обновляет следующее устройство.

Мы рекомендуем использовать одну и ту же версию ПО на обоих устройствах кластера

Если вы хотите обновить ПО удаленно, убедитесь что IP-адрес интерфейса управления настроен на External интерфейсе, и он является публичным и маршрутизируемым IP адресом.

Для более подробной информации см. “IP адрес управления”

Отключение FireCluster

При отключении FireCluster оба устройства одновременно перезагружаются. Поэтому мы рекомендуем вам это делать в часы, когда вы можете позволить небольшие перерывы связи.

Для того чтобы отключить FireCluster выполните следующее:

1. В WatchGuard System Manager откройте конфигурацию master-устройства.
2. Нажмите . Или выберите **Tools** > **Policy Manager**.

3. Выберите **FireCluster** > **Configure**.
   Откроется диалогое окно FireCluster Cluster Configuration.

4. Отключите опцию **Enable FireCluster**.

5. Нажмите **OK**.

6. Сохраните конфигурацию
   Конфигурация сохраняется и оба устройства кластера перезагружаются.

   * Master устройство запускается с IP-адресами, присвоенными кластеру

   * Резервное master устройство запускается с IP-адресами и конфигурацией по умолчанию.

Вы можете удалить одно устройство из кластера и при этом не отключать FireCluster. При этом будет создан кластер с одним устройством и при этом FireCluster не будет отключен и обрывов связи не произойдет.

Глава 12 - Аутентификация

Аутентификация пользователя

Аутентификация пользователя – это процесс определения является ли пользователь тем, кем он представляется, и проверки его прав доступа. На устройстве Firebox учетная запись пользователя состоит из двух частей: имя пользователя и пароль.

Каждая учетная запись пользователя привязывается к IP адресу, что позволяет администратору устройства Firebox выполнять мониторинг всех подключений через Firebox. С использованием аутентификации пользователи могут подключаться к сети с любого компьютера, но получать доступ только с сетевым портам и протоколам, использование которых им разрешено.

Firebox может отслеживать соединения, которые начинаются с определенного IP адреса, и во время аутентификации пользователя также передает имя сеанса.

Вы можете создавать политики брандмауэра, которые будут предоставлять пользователям или группе пользователей доступ к определенным сетевым ресурсам. Это особенно полезно в сетях, в которых несколько пользователей используют один компьютер с одним IP адресом. Вы можете настроить ваш Firebox, как локальный сервер аутентификации, или использовать существующий Active Directory, LDAP или RADIUS сервер аутентификации.

Если вы используете аутентификацию Firebox через порт 4100, права доступа определяются на базе имени пользователя. Если вы используете ПО для аутентификации о стороннего разработчика, права доступа пользователей, аутентификация которых осуществляется на серверах сторонних производителей, базируется на принадлежности к определенной группе.

Аутентификация пользователя WatchGuard разрешает привязку имени пользователя к IP адресу, что позволит вам аутентифицировать и мониторить соединения прямо на устройстве Firebox. Основной вопрос, которым задается каждый администратор, это «Должен ли я разрешить трафик с устройства X на устройство Y?”

Для корректной работы WatchGuard аутентификации IP адрес компьютера пользователя не должен меняться в течение во время процедуры аутентификации.

В большинстве окружений связь между IP-адресом и пользователем стабильна и практически не меняется, и ее можно использовать для аутентификации трафика пользователя. В окружениях, в которых связь между пользователем и IP-адресом не постоянна, например в распределенных или терминальных сетях, использование аутентификации пользователя является нецелесообразным.

На сегодняшний день WatchGuard поддерживает протокол AAA (Authentication, Accounting, and Access control), который основан на стабильной связи между IP-адресом и пользователем. Мы также поддерживаем аутентификацию в домен Active Directory через Single Sign-On, а также поддерживаем наиболее часто используемые серверы аутентификации. Вдобавок мы поддерживаем параметры неактивности и ограничения по времени сеанса.

Это позволяет ограничить промежуток времени, в течение которого IP-адресу будет разрешена передача трафика через Firebox до момента, пока пользователям не придется снова вводить свои пароли.

Если вы управляете SSO доступом при помощи белых списков, управляете таймаутами неактивности пользователей, таймаутами сессий, а также управляете процедурой допуска к аутентификации, вы значительно повышаете уровень управления аутентификацией, ведением учета и доступом. Для того чтобы отключить аутентификацию пользователя, вам необходимо отключить учетную запись пользователя на сервере аутентификации.

Процедура аутентификации пользователей

Для обработки запросов аутентификации в устройстве Firebox запущен HTTPS-сервер. Для того чтобы пройти процедуру аутентификации, пользователь должен подключиться к странице аутентификации устройства Firebox:

https://IP_адрес_интерфейса_ Firebox:4100/

или

https://Имя_хоста_Firebox:4100

На этой странице вы найдете форму для аутентификации. Пользователю необходимо ввести свое имя пользователя и пароль. Firebox по протоколу PAP (Password Authentication Protocol) отправляет эти данные на сервер аутентификации.

После того как пользователь был аутентифицирован, он может использовать сетевые ресурсы.

Так как Fireware XTM по умолчанию для HTTPs использует самоподписанный сертификат, вы увидите предупреждение о безопасности. Вы можете проигнорировать это сообщение. Если вы хотите, чтобы это сообщение больше не появлялось, вам необходимо установить third-party сертификат или сгенерировать свой собственный сертификат, который соответствует IP адресу или имя домена, которые использовались для аутентификации.

Закрытие аутентифицированной сессии вручную

Для того чтобы закрыть аутентифицированную сессию пользователям нет необходимости ждать пока не наступит таймаут. Они могут вручную закрыть свою сессию до того, как наступит таймаут. Для того чтобы закрыть сессию необходимо открыть страницу Authentication. Если страница будет закрыта, то для того чтобы закрыть аутентифицированную сессию пользователю необходимо будет снова аутентифицироваться.

Для того чтобы закрыть аутентифицированную сессию выполните следующее:

1. Зайдите на страницу Authentication:

   ```
   https://[device interface IP address]:4100/
   ```

   или

   ```
   https://[device host name]:4100
   ```

2. Нажмите **Logout**.

Управление аутентифицированными пользователями

При помощи Firebox System Manager вы можете просматривать списки аутентифицированных пользователей и при необходимости закрывать их сессии.

Если страница Authentication настроена для автоматической переадресации на другую страницу, то через несколько секунд после того, как вы откроете страницу портала аутентификации, вы будете переадресованы. Вам необходимо выйти из системы до того, как вы будете перенаправлены на другую страницу

Просмотр аутентифицированных пользователей

Для того чтобы посмотреть аутентифицированных пользователей на вашем Firebox выполните следующее:

1. Запустите Firebox System Manager.

2. Выберите закладку **Authentication List**.
   Откроется список всех аутентифицированных пользователей.

Закрытие сессии пользователя

Для того чтобы закрыть сессию пользователя в Firebox System Manager выполните следующее:

1. Выберите закладку **Authentication List**.
   Откроется список аутентифицированных пользователей.

2. Выберите одного или несколько пользователей.

3. Нажмите правой кнопкой на имя пользователя и выберите **Log Off User**.

Для более подробной информации см.”Аутентифицированные пользователи (закладка Authentication List)”

Использование аутентификации для блокировки входящего трафика

Одной из функций аутентификации является блокировка исходящего трафика. Однако при помощи аутентификации вы также можете блокировать входящий трафик. Если у вас есть учетная запись на Firebox и Firebox имеет внешний публичный IP адрес, вы можете аутентифицироваться на Firebox с внешнего компьютера. Например вы можете ввести следующее:

```
https://<IP address of Firebox external interface>:4100/
```

После того, как вы будете аутентифицированы, вы можете использовать политики, настроенные для вашей учетной записи.

Для того чтобы разрешить удаленному пользователю аутентифицироваться через External интерфейс выполните следующее:

1. В WSM подключитесь к устройству и откройте Policy Manager.

2. Два раза нажмите на политику **WatchGuard Authentication**. Эта политика появится после того, как вы к политике добавите пользователя или группу пользователей.
   Откроется диалоговое окно Edit Policy Properties.

3. В выпадающем списке **WG-Auth connections are** выберите **Allowed**.

4. В секции **From** нажмите **Add**.
   Откроется диалоговое окно Add Address.

5. Из списка выберите **Any** и нажмите **Add**.

6. Нажмите **OK**.
   Any появится в секции From.

7. В секции **To** нажмите **Add**.

8. Из списка выберите **Firebox** и нажмите **Add**.

9. Нажмите **OK**.
   Запись Firebox появится в секции To

10. Нажмите **OK** для того чтобы закрыть диалоговое окно **Edit Policy Properties**.

Аутентификация через Firebox шлюз

Firebox шлюз – это устройство, которое подключается к сети для защиты вашего Сервера Управления от внешних атак из сети Интернет. Для более подробной информации см. “Шлюз Firebox”

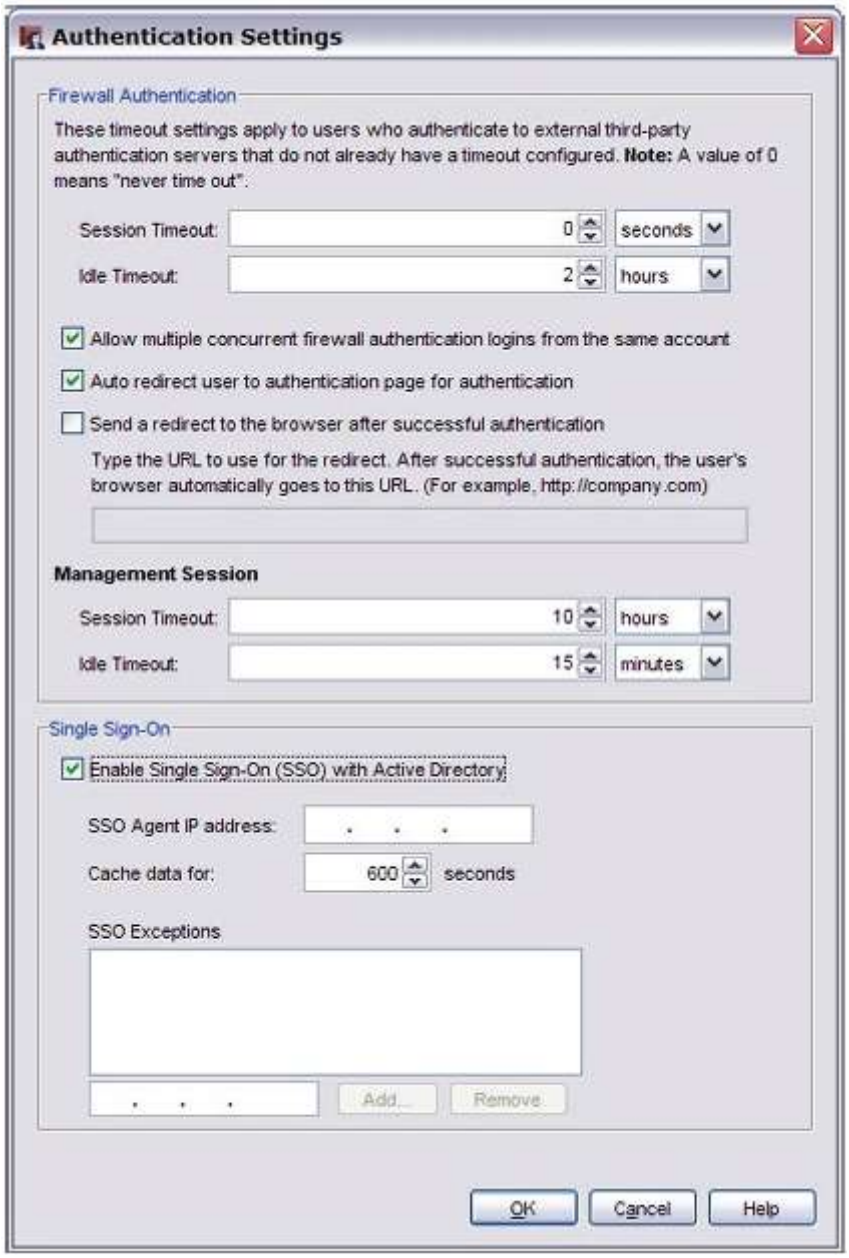
Для того чтобы передавать запросы на аутентификацию через Firebox шлюз на другие устройства, вам необходимо создать политику, которая разрешает передачу трафика аутентификации на шлюзе. Если трафик аутентификации на шлюзе заблокирован, то при помощи Policy Manager добавьте политику WG-Auth. Эта политика управляет трафиком через TCP порт 4100. Эта политика должна разрешать трафика на IP адрес необходимого устройства

Настройка глобальных параметров аутентификации

Для того чтобы настроить глобальные параметры аутентификации (таймауты и перенаправления со страницы аутентификации) и включить Single Sign-On (SSO) выполните следующее:

1. Откройте Policy Manager.

2. Выберите **Setup > Authentication > Authentication Settings**.
Откроется диалоговое окно Authentication Settings



Настройка глобальных таймаутов аутентификации

Этот промежуток времени определяет, как долго пользователь будет оставаться аутентифицированным после закрытия аутентифицированной сессии. Величину этого таймаута вы можете настроить в диалоговых окнах **Authentication Settings** или **Setup Firebox User**.

Для более подробной информации о параметрах аутентификации пользователя и диалоговом окне **Setup Firebox User** см. “Создание нового пользователя для аутентификации Firebox”

Для пользователей, аутентифицированных серверами стороннего производителя, величины таймаутов, настроенные на этих серверах, используются вместо таймаутов, настроенных на Firebox. Таймауты аутентификации не применяются для пользователей Mobile VPN with PPTP.

Session Timeout

Промежуток времени в течение которого пользователь может передавать трафик во внешнюю сеть. Если вы значение этого поля установите равным ноль (0) секунд, минут, часов или дней, то

таймаут сессии не используется и пользователь может оставаться подключенным в течение неограниченного времени.

Idle Timeout

Промежуток времени, в течение которого пользователь может оставаться подключенным в неактивном состоянии (не передает трафик во внешнюю сеть).

Если вы установите значение этого поля равным нулю (0) секунд, минут, часов и дней, то таймаут по неактивности не используется и пользователь может оставаться подключенным в течение неограниченного времени.

Разрешить параллельные подключения

Вы можете разрешить нескольким пользователям аутентифицироваться с использованием одних и тех же атрибутов доступа на одном сервере аутентификации. Это полезно для гостевых учетных записей или в лабораторных условиях. Когда второй пользователей входит в систему под теми же именем пользователя и паролем, сессия первого аутентифицированного пользователя автоматически закрывается.

Если вы выключите эту опцию, пользователь не сможет аутентифицироваться на одном сервере.

1. Откройте диалоговое окно **Authentication Settings**

2. Включите опцию **Allow multiple concurrent firewall authentication logins from the same account**

Для пользователей Mobile VPN with IPSec и Mobile VPN with SSL параллельные подключения с одной и той же учетной записи разрешены в независимости от этой опции. Для параллельного подключения эти пользователи должны подключаться с разных IP адресов. Поэтому если пользователи находятся за Firebox, использующим NAT, они не смогут одновременно подключаться под одной и той же учетной записью. Пользователи Mobile VPN with PPTP не имеют таких ограничений.

Автоматическая переадресация пользователь на страницу аутентификации

Если вы хотите, чтобы ваши пользователи перед тем, как получить доступ в сеть Интернет, проходили процедуру аутентификации, вы можете для неаутентифицированных пользователей настроить автоматическую переадресацию на страницу аутентификации и заставить их самим заходить на страницу аутентификации. Это применяется только к HTTP и HTTPS соединениям.

Auto redirect users to authentication page for authentication

При включении этой опции, все неаутентифицированные пользователи, перед тем как получить доступ к сети Интернет, будут автоматически перенаправлены на страницу аутентификации. При выключении этой опции пользователям необходимо будет самим заходить на страницу аутентификации. Для более подробной информации об аутентификации пользователя см. “Процедура аутентификации пользователей”

Настройка стартовой страницы по умолчанию

Если вы включите опцию **Auto redirect users to authentication page for authentication,** то при попытке открыть какой-либо сайт в браузере пользователь попадет на страницу аутентификации. Если вы хотите, чтобы после успешного входа в систему, пользователь попадал на другую страницу, то выполните следующее.

1. В диалоговом окне **Authentication Settings** включите опцию Send **a redirect to the browser after successful authentication**.

2. В соответствующем текстовом поле введите URI сайта, который браузер будет открывать после того, как пользователь будет успешно аутентифицирован.

Настройка таймаутов Сеанса Управления

Здесь вы можете настроить временные интервалы, в течение которых пользователь с правами чтения/записи будет оставаться аутентифицированным после того, как Firebox закроет сессию.

Session Timeout

Промежуток времени в течение которого пользователь может передавать трафик во внешнюю сеть. Если вы значение этого поля установите равным ноль (0) секунд, минут, часов или дней, то таймаут сессии не используется и пользователь может оставаться подключенным в течение неограниченного времени.

Idle Timeout

Промежуток времени, в течение которого пользователь может оставаться подключенным в неактивном состоянии (не передает трафик во внешнюю сеть). Если вы установите значение этого поля равным нулю (0) секунд, минут, часов и дней, то таймаут по неактивности не используется и пользователь может оставаться подключенным в течение неограниченного времени.

Включение Single Sign-On

Если вы включите использование Single Sign-On (SSO), то пользователи, подключенные к Trusted или Optional сетям будут автоматически аутентифицироваться. Для более подробной информации см. “Single Sign-On (SSO)”.

Политика WatchGuard Authentication (WG-Auth)

Политика WatchGuard Authentication (WG-Auth) создается автоматически на вашем Firebox. Первая созданная вами политика с указанием имени пользователя или группы пользователей в поле **From** (закладка **Policy)** автоматически создает политику WG-Auth. Эта политика управляет доступом к порту 4100, на который пользователи отправляют запросы аутентификации.

Например, для аутентификации на устройстве Firebox с IP-адресом 10.10.10.10, в адресной строке браузера введите *https://10.10.10.10:4100.*

Если вы хотите отправлять запросы аутентификации на определенное устройство через шлюз, то вам придется вручную добавить политику WG-Auth. Если трафик аутентификации на шлюзе заблокирован, то вам необходимо создать политику WG-Auth, которая разрешит трафик аутентификации на IP адреса назначения.

Для более подробной информации см.”Использование аутентификации для блокировки входящего трафика”

Single Sign-On (SSO)

Когда пользователь пытается войти в систему на компьютерах, подключенных к сети, ему необходимо ввести имя пользователя и пароль. Если вы используете аутентификацию Active Directory на вашем Firebox для ограничения исходящего трафика определенных пользователей или групп пользователей, то им потребуется проходить аутентификацию вручную. Вы можете использовать SSO для того, чтобы пользователи доверенной или опциональной сети аутентфицировались автоматически при входе в систему на своем компьютере.

При использовании Single Sign-On (SSO) пользователи, подключенные к Trusted или Optional сетям, после входа в систему на своем компьютере автоматически аутентифицируются на устройстве Firebox. WatchGuard SSO состоит из двух компонентов - SSO агент и клиентские сервисы SSO. Для корректной работы SSO вам необходимо установить SSO агент на компьютеры

в вашем домене. ПО клиента SSO является дополнительным и устанавливается на каждый компьютер.

SSO агент отправляет запрос на компьютер пользователя через 4116 для проверки, кто на данный момент подключен к нему. Если компьютер клиента не отвечает, SSO агент возвращается к предыдущему протоколу из более ранних версий WSM, и отправляет запрос *NetWkstaUserEnum* на компьютер пользователя. Полученную от компьютера информацию SSO агент использует для аутентификации Single Sign-On.

Если SSO клиент не установлен, то SSO может получить от компьютера пользователя несколько ответов на запрос. Это может произойти если к компьютеру подключено на данный момент несколько пользователей, или если под своей учетной записью к компьютеру подключается определенный сервис. SSO агент обрабатывает только первый полученный ответ и передает эту информацию Firebox, в качестве данных пользователя, который на данный момент подключен к компьютеру. Затем устройство может проверить данные пользователя при помощи настроенных для него политик. По умолчанию SSO агент кэширует эти данные примерно на 10 минут для того чтобы для каждого подключения снова не генерировать этот запрос.

Если клиент SSO установлен на компьютере, то при получении запроса от SSO агента и возвращает ему корректную информацию о том, какой пользователь на данный момент подключен к компьютеру. SSO агент не пытается подключиться к серверу Active Directory для получения данных пользователя, так как эти все необходимые данные он получит от клиента SSO, установленного на компьютере пользователя. Если в вашей сети одним компьютером могут пользоваться несколько пользователей, то мы вам рекомендуем установить клиент SSO. В противном случае вам необходимо понимать некоторые ограничения. Например, сервисам, установленным на центральный компьютер, (например клиент антивируса), которые входят в систему с атрибутами доступа учетной записи домена, Firebox предоставляет права доступа пользователя, который вошел в систему первым, а не права доступа пользователя, который только что вошел в систему. Также все сообщения журнала активности пользователя в качестве имени пользователя будут показывать имя учетной записи сервиса.

Если вы не хотите использовать SSO клиент, мы рекомендуем не использовать SSO в сетях, где пользователи подключаются к своим компьютерам под учетными записями сервисов или batch. Если к одному IP адресу привязано несколько пользователей, то сеть может некорректно работать. Это является риском для вашей системы безопасности

Перед тем, как начать

- У вас должен сервер Active Directory в Trusted и Optional сетях.
- Firebox должен использовать аутентификацию Active Directory.
- Каждый пользователь должен иметь учетную запись на сервере Active Directory.
- Для корректной работы SSO каждый пользователь должен подключаться к учетной записи домена. Если пользователи входят в систему под локальной учетной записью, их данные не проверяются и не отправляются на устройство Firebox.
- Если вы используете ПО брандмауэра стороннего производителя на компьютерах вашей сети, убедитесь, что на каждом клиенте открыт TCP порт 445 (Samba/ Windows Networking).
- Убедитесь, что общие принтеры и файлы включены на каждом компьютере, пользователи которых используют SSO для аутентификации.
- Убедитесь, что порты NetBIOS и SMB не заблокированы на компьютерах, пользователи которых используют SSO для аутентификации. NetBIOS использует порты TCP/UDP 137, 138, и 139. SMB использует TCP порт 445.
- Убедитесь, что порт 4116 открыт на всех компьютерах.
- Убедитесь, что компьютеры, пользователи которых используют SSO для аутентификации, являются членами домена с установленными довериями.

Настройка SSO

Для того чтобы использовать SSO, вам необходимо установить SSO агент. Мы также рекомендуем на все компьютеры установить SSO клиент. Несмотря на то, что для того чтобы работать с SSO вам достаточно будет установить SSO агент, для повышения уровня безопасности системы и управления доступом мы также рекомендуем установить SSO клиент

Настройка SSO состоит из 3 этапов:

1. Установка WatchGuard SSO агента.
2. Установка WatchGuard SSO клиента (необязательно, но рекомендуется).
3. Включение SSO на вашем устройстве.

Установка агента WatchGuard Single Sign-On (SSO) agent

Для работы с Single Sign-On (SSO) вам необходимо установить агент WatchGuard SSO. SSO агент – это сервис, который получает запросы на аутентификацию и проверяет статус пользователя на сервере Active Directory. Сервис запускается под именем *WatchGuard Authentication Gateway* на компьютере, на который вы установили SSO агент. Для корректной работы SSO агента, на компьютере должен быть установлен Microsoft .NET Framework 2.0 или выше.

Для того чтобы использовать Single Sign-On с вашим Firebox, вам необходимо установить SSO агент на компьютер домена со статическим IP адресом. Мы рекомендуем установить SSO агент на контроллер домена.

Загрузка SSO агента

1. Зайдите на страницу http://www.watchguard.com/.
2. Войдите в систему, используя имя пользователя и пароль LiveSecurity Service.
3. Нажмите на ссылку **Software Downloads**.
4. Выберите тип и номер модели вашего устройства.
5. Загрузите WatchGuard Authentication Gateway.

Перед тем, как установить

Сервис SSO агента должен быть запущен под учетной записью обычного пользователя, не администратора. Мы рекомендуем специально для агента создать отдельную учетную запись пользователя. Для корректной работы SSO агента вам необходимо настроить учетную запись следующим образом:

- Добавьте учетную запись в группу **Domain Admin**.
- Сделайте группу **Domain Admin** основной группой.
- Разрешите учетной записи подключаться как сервис.
- Сделайте срок действия пароля неограниченным.

Установка сервиса SSO агента

1. Для того чтобы запустить мастер Authentication Gateway Setup Wizard два раза нажмите на файл **WG-Authentication-Gateway.exe**. Для запуска мастера на некоторых других ОС вам возможно придется ввести локальный пароль администратора.

2. Выполните все необходимые инструкции мастера для установки SSO агента.Имя пользователя домена введите в следующем формате: *domain\username*. Имя домена не должно содержать «.com” или «.net». Например, если у вас есть домен *mywatchguard.com* и вы используете учетную запись домена *ssoagent*, то введите `mywatchguard\ssoagent`.

   Также имя пользователя вы можете ввести в формате UPN: username@mywatchguard.com.

   При этом имя домена должно содержать «.com» или «.net».

3. Нажмите **Finish** для того чтобы закрыть мастер.После окончания работы мастера сервис WatchGuard Authentication Gateway автоматически запустится и будет запускаться при каждой перезагрузке компьютера.

Установка клиента WatchGuard Single Sign-On (SSO)

Помимо SSO агента вы также можете установить клиент WatchGuard Single Sign-On (SSO). SSO клиент устанавливается, как сервис Windows, запущенный под учетной записью Local System, и использующийся для проверки данных доступа пользователей, на данный момент подключенных к компьютеру. Когда пользователь пытается аутентифицироваться SSO агент отправляет запрос SSO клиенту для получения пользовательских данных доступа. SSO клиент в ответ возвращает атрибуты доступа пользователя, который на данный момент подключен к компьютеру. SSO клиент слушает порт 4116.

Так как программа установки SSO клиента является MSI файлом, то вы автоматически установить его на компьютеры пользователей, как только они подключаются к вашему домену. Для автоматической установки ПО на компьютеры пользователей вы можете использовать политику Active Directory Group Policy. Для более подробной информации см. Документацию по вашей ОС.

Загрузка SSO клиента

1. Зайдите на страницу http://www.watchguard.com/.
2. Войдите в систему, используя имя пользователя и пароль LiveSecurity Service.
3. Нажмите на ссылку **Software Downloads**.
4. Выберите тип и номер модели вашего устройства.
5. Загрузите WatchGuard Authentication Client.

Установка сервиса SSO клиента

1. Для того чтобы запустить мастер Authentication Client Setup Wizard два раза нажмите на файл **WG-Authentication-Client.msi**. Для запуска мастера на некоторых других ОС вам возможно придется ввести локальный пароль администратора.
2. Выполните все необходимые инструкции мастера для установки ПО. Для того чтобы посмотреть доступных томов для установки и наличие свободного места на каждом нажмите **Disk Cost**.
3. Когда установка будет завершена нажмите **Close**.

После окончания работы мастера сервис WatchGuard Authentication Client автоматически запустится и будет запускаться при каждой перезагрузке компьютера.

Включение Single Sign-On (SSO)

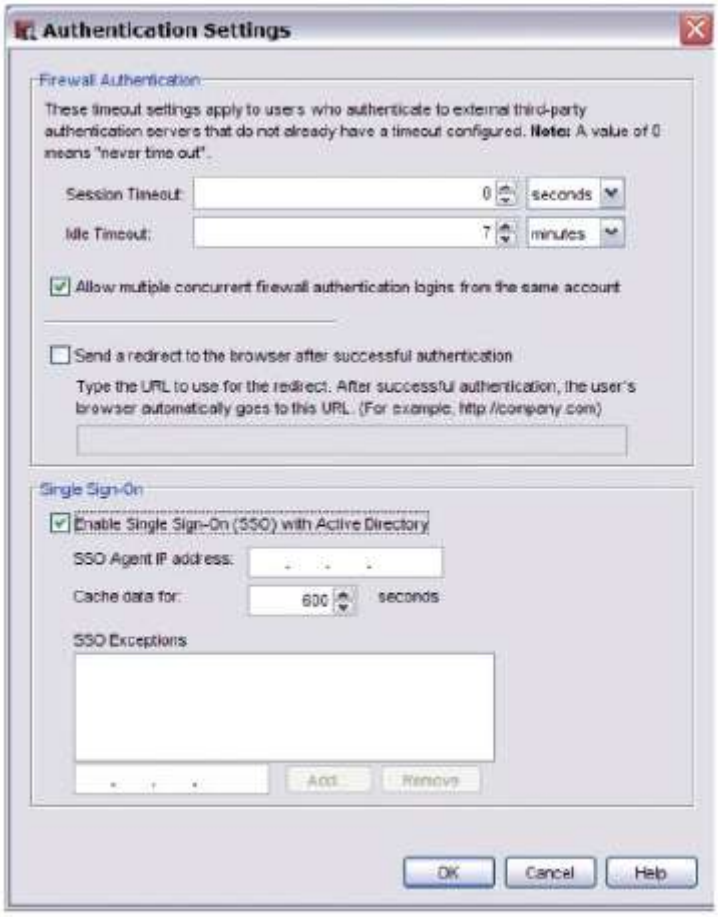
Перед тем как настраивать SSO вам необходимо выполнить следующие действия:

- Настройка сервера Active Directory

- Установка агента SSO
- Установка SSO клиента (дополнительно)

Включение и настройка SSO

1. В Policy Manager выберите **Setup** > **Authentication** > **Authentication Settings**.
   Откроется диалоговое окно Authentication Settings.



2. Включите опцию **Enable Single Sign-On (SSO) with Active Directory**.
3. В поле **SSO Agent IP address** введите IP адрес вашего SSO агента.
4. В поле **Cache data for** введите временной интервал, в течение которого SSO агент будет кэшировать данные.
5. В окне SSO Exceptions добавьте или удалите SSO исключения для IP адресов, на которые Firebox не будет отправлять SSO запросы – различные серверы или компьютеры, которые не являются частью домена. Вы можете ввести IP адрес хоста, IP адрес сети в slash-нотации или диапазон IP адресов. Для более подробной информации об SSO исключениях см. следующий раздел.
6. Нажмите **OK** для того чтобы сохранить сделанные изменения.

Создание SSO исключений

Если ваша сеть содержит устройства с IP –адресами, которым не требуется аутентификация, например принтеры или серверы сети, то их следует добавить в список SSO Exception в конфигурации SSO configuration.

При каждом подключении таких устройств с IP-адресами, которых нет в списке исключений Firebox вызывает агента SSO, чтобы он выполнил привязку IP адреса к имени пользователя. Эта процедура занимает примерно 10 секунд.

При помощи списков исключений вы можете ускорить эту процедуру, а также значительно снизить количество трафика в сети.

Типы Серверов Аутентификации

Firebox поддерживает 6 методов аутентификации:

- Настройка аутентификации RADIUS сервера
- Настройка аутентификации через VASCO сервер
- Настройка SecurID аутентификации
- Настройка аутентификации Active Directory
- Настройка LDAP аутентификации

Вы можете использовать один или несколько способов аутентификации. Если вы будете использовать несколько методов аутентификации, то пользователям во время аутентификации необходимо будет выбирать необходимый метод аутентификации из выпадающего списка.

Серверы аутентификации сторонних производителей

Если вы используете сервер аутентификации стороннего производителя, вам нет необходимости хранить отдельную базу данных пользователей на Firebox. Вы можете настроить этот сервер в соответствие с инструкцией производителя, установить сервер с доступом к Firebox и в целях безопасности поместить его за Firebox.

Затем вам необходимо настроить Firebox для переадресации запросов на аутентификацию на этот сервер. Если вы создаете группу пользователей на Firebox, который аутентифицирует пользователей с помощью сервера аутентификации стороннего производителя, убедитесь, что на этом сервере вы создали точно такую же группу пользователей с таким же названием. Для более подробной информации о настройке серверов аутентификации сторонних производителей см. :

- Настройка аутентификации RADIUS сервера
- Настройка аутентификации через VASCO сервер
- Настройка SecurID аутентификации
- Настройка аутентификации Active Directory
- Настройка LDAP аутентификации

Настройка резервного сервера аутентификации

Вы можете настроить резервный сервер аутентификации с использованием всех способов аутентификации других производителей. Если устройство Firebox не может подключиться к основному серверу аутентификации (после трех попыток), то он помечается как неактивный и генерируется тревога. Затем Firebox подключается у резервному серверу. Если Firebox не может подключиться к резервному серверу аутентификации, он ждет десять минут, и затем пытается повторно подключиться к основному серверу. Этот цикл продолжается до тех пор, пока Firebox не подключится к серверу аутентификации.

Настройка Firebox в качестве сервера аутентификации

Если вы не используете сервер аутентификации других производителей, вы можете использовать Firebox в качестве сервера аутентификации. Эта процедура делит вашу компанию на группы и пользователей для аутентификации. Группа, к которой вы добавите пользователя, управляется при помощи действий, которые они выполняют, и информации, которой они пользуются. Например, у вас может быть бухгалтерская, маркетинговая, исследовательская группа и группа разработчиков. У вас также может быть группа работников с управляемым доступом в интернет.

Для пользователей вы устанавливаете процедуру аутентификации, тип системы и информацию, доступ к которой они могут получить. Пользователем может быть сеть или отдельный компьютер. Если структура вашей компании меняется, то вы можете при необходимости добавлять или удалять пользователей или системы из группы.

Сервер аутентификации Firebox включен по умолчанию.

Типы аутентификации Firebox

Вы можете настроить Firebox для аутентификации пользователей для четырех различных типов аутентификации:

- Аутентификация брандмауэра
- Mobile VPN with PPTP сессии
- Mobile VPN with IPSec сессии
- Mobile VPN with SSL сессии

При успешной аутентификации, Firebox создает соответствия между следующими элементами:

- Имя пользователя
- Группа (или группы) пользователей Firebox, к которой принадлежит пользователь
- IP-адрес компьютера пользователя, с которого пользователь был аутентифицирован
- Виртуальный IP-адрес компьютера пользователя (если пользователь подключен через MUVPN).

Аутентификация брандмауэра

Для аутентификации пользователей вы можете создать учетные записи пользователей или группы пользователей. После того, как пользователь будет аутентифицирован на Firebox, его данные доступа и IP адрес компьютера используются для поиска политики, которая будет обрабатывать трафик, передаваемый этим пользователем.

Для того чтобы создать учетную запись пользователя Firebox вам необходимо выполнить следующее:

1. Создание нового пользователя для аутентификации Firebox.
2. Создание новой группы для аутентификации Firebox и добавление пользователя в эту группу.
3. Создайте политику, которая будет разрешать трафик только для пользователей или группы пользователей, созданных на Firebox. Эта политика применяется только тогда, когда трафик передается с или на IP адрес аутентифицированного пользователя.

Для того чтобы аутентифицировать пользователей через HTTP соединение через порт 4100 выполните следующее:

1. Зайдите на страницу: *https://<IP адрес интерфейса Firebox>:4100/*

2. В текстовых полях **Username** и **Password** введите имя пользователя и пароль соответственно.

3. В выпадающем списке **Domain** выберите домен. Это поле будет активно только в случае если вы можете выбирать из нескольких доменов.

4. Нажмите **Login**.
Если введенные данные верны, то пользователь будет аутентифицирован.

Mobile VPN with PPTP сессии

Вы можете настроить Firebox для работы с сессиями Mobile VPN with PPTP.

Если Firebox настроен для работы с Mobile VPN with PPTP соединениями, пользователи, которые добавляются в группу Mobile VPN with PPTP, могут создавать PPTP подключения при помощи компонента PPTP, который поддерживается их операционной системой.

Так как Firebox разрешает PPTP соединения для любого пользователя Firebox, который предоставит корректные данные доступа, очень важно создать политику для PPTP сессий, которая будет разрешать передавать PPTP трафик только определенным пользователям.

Вы также можете добавить этих пользователей в группу Firebox User и создать политику, которая разрешает трафик только для пользователей этой группы. Firebox создает группу *PPTP-Users* для этих целей.

Для того чтобы настроить Mobile VPN with PPTP выполните следующее:

1. В Policy Manager выберите **VPN > Mobile VPN > PPTP**.

2. Включите опцию **Activate Mobile VPN with PPTP**.

3. Отключите опцию **Use Radius authentication to authenticate Mobile VPN with PPTP users**. Это разрешит устройству Firebox аутентифицировать PPTP сессию. Firebox проверяет совпадает ли имя пользователя и пароль, которые пользователь ввел в окне VPN-подключения с именем пользователя и паролем в Базе Данных пользователей Firebox. Если данные, введенные пользователем совпадают с данными в Базе Данных, пользователь аутентифицируется для PPTP-сеанса.

4. Создайте политику, которая разрешает трафик только для пользователей группы Firebox или группы устройств Firebox. Firebox использует эту политику только тогда, когда трафик идет с виртуального IP-адреса аутентифицированного пользователя.

Mobile VPN with IPSec сессии

При настройке вашего Firebox для работы с сессиями Mobile VPN with IPSec вы создаете политики на вашем устройстве, и затем используете клиент Mobile VPN with IPSec для того чтобы разрешить

пользователям доступ к вашей сети. После настройки Firebox необходимо при помощи ПО клиента Mobile VPN with IPSec настроить каждый компьютер пользователей. После того, как компьютер пользователя будет настроен, пользователь сможет создавать Mobile VPN подключения. Если данные доступа пользователя совпадают с данными в базе данных пользователей Firebox User, и пользователь принадлежит группе Mobile VPN, то Mobile VPN сессия будет аутентифицирована.

Для того чтобы настроить аутентификацию для Mobile VPN with IPSec сессий вам необходимо выполнить следующее:

1. Настройка Mobile VPN with IPSec сессий.

2. Установка ПО клиента Mobile VPN with IPSec.

Mobile VPN with SSL сессии

Вы можете настроить Firebox для работы с Mobile VPN with SSL сессиями. Если Firebox настроен для работы с Mobile VPN with SSL сессиями, пользователи, которые принадлежат группе Mobile VPN with SSL, могут установить и использовать ПО клиента Mobile VPN with SSL для создания SSL подключений.

Так как Firebox разрешает SSL сессии от любого вашего пользователя, который предоставит корректные данные доступа, то очень важно создать политику для SSL VPN сессий, которая будет разрешать их только определенным пользователям. Вы также можете добавить этих пользователей в группу Firebox User Group и создать политику, которая будет разрешать передачу трафика только пользователям этой группы. Для этих целей Firebox сам создает группу *SSLVPN-Users*.

Для настройки Mobile VPN with SSL сессию выполните следующее:

1. В Policy Manager выберите **VPN > Mobile VPN > SSL**.
   Откроется диалогое окно Mobile VPN with SSL Configuration.

2. Выполните все необходимые настройки Mobile VPN with SSL.

Создание нового пользователя для аутентификации Firebox

1. В Policy Manager выберите **Setup** > **Authentication** > **Authentication Servers**.
   Откроется диалогое окно Authentication Servers

2. В закладке **Firebox** диалогового окна **Authentication Servers** под списком **Users** нажмите **Add**.
   Откроется диалогое окно Setup Firebox User.

3. В текстовых полях **Name** и **Description (необязательно)** введите имя пользователя и его описание.

4. В текстовых полях **Passphrase** и **Confirm** введите пароль и его подтверждение.

   Пароль, который вы создали, будет маскирован и больше не будет отображаться в открытом виде. Если вы забудете свой пароль, то вам необходимо создать новый.

5. В поле **Session Timeout** выберите интервал времени, в течение которого пользователь может передавать трафик во внешнюю сеть. По умолчанию значение этого поля равно 1 секунда, минута, час или день. Максимальное значение 365 дней.

6. В поле **Idle Timeout** введите интервал времени, в течение которого пользователь будет оставаться аутентифицированным при отсутствии трафика (трафик не передается во внешнюю сеть). По умолчанию значение этого поля равно 1 секунде, минуте, часу или дню. Максимальное значение – 365 дней.

7. Для того для того, чтобы добавить пользователя в группу **Firebox Authentication Group** выберите пользователя в списке **Available**.

8. Нажмите << для того для того, чтобы переместить пользователя в список **Member**.Или два раза нажмите на имя пользователя в списке **Available**.
   Пользователь будет добавлен в список пользователей.

9. Для того для того, чтобы закрыть диалоговое окно окно **Setup Firebox User** нажмите **OK**.
   Откроется закладка Firebox Users со списком новых пользователей.

Создание новой группы для аутентификации Firebox

1. В Policy Manager выберите **Setup** > **Authentication** > **Authentication Servers**.
   Откроется диалогое окно Authentication Servers.

2. Выберите закладку **Firebox**.

3. Под списком **User Groups** нажмите **Add**.
   Откроется диалогое окно Setup Firebox Group

4. Введите имя группы.

5. (Дополнительно) Введите описание группы.

6. Для того, для того, чтобы добавить пользователя в группу, выберите пользователя в списке **Available**. Нажмите  для того для того, чтобы переместить выбранного пользователя в списке **Member**.
   Вы также можете два раза нажать на имя пользователя в списке Available.

7. После того, как вы добавите всех пользователей в группу, нажмите **OK**.

8. Теперь вы можете настроить политики и аутентификацию для этих пользователей или групп пользователей.

Для более подробной информации см. “Использование в политиках пользователей и групп”.

Настройка аутентификации RADIUS сервера

RADIUS (Remote Authentication Dial-In User Service) используется для аутентификации локальных и удаленных пользователей в сети. RADIUS – это клиент/серверная система, которая хранит аутентификационную информацию для пользователей, серверов удаленного доступа, VPN шлюзов и других ресурсов в одной центральной базе данных.

Для более подробной информации о RADIUS аутентификации см. “Принцип работы аутентификации через RADIUS сервер”

Ключ аутентификации

В сообщениях аутентификации, которые отправляются с и на RADIUS сервер, содержится специальный ключ аутентификации. Этот ключ должен быть одинаковым на RADIUS клиенте и сервере. Без этого ключа клиент и сервер не смогут обмениваться сообщениями.

Способы RADIUS аутентификации

Для web и Mobile VPN with IPSec или SSL аутентификации, RADIUS поддерживает только PAP (Password Authentication Protocol) аутентификацию. Для PPTP аутентификация RADIUS поддерживает только MSCHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2).

Перед тем как начать

Перед тем как настроить Firebox для работы с RADIUS сервером, вам необходима следующая информация:

- Основной RADIUS сервер — IP адрес и порт RADIUS сервера
- Вторичный RADIUS сервер (дополнительно) — IP адрес и порт RADIUS сервера
- Общий ключ — пароль (чувствительный к регистру), который должен быть одинаковым на Firebox и RADIUS сервере
- Методы аутентификации — настройте ваш RADIUS сервер для того для того, чтобы он разрешал используемый вашим Firebox метод аутентификации: PAP или MS CHAP v2

RADIUS аутентификация с вашим Firebox

Для того чтобы использовать RADIUS аутентификацию с вашим Firebox вам необходимо следующее:

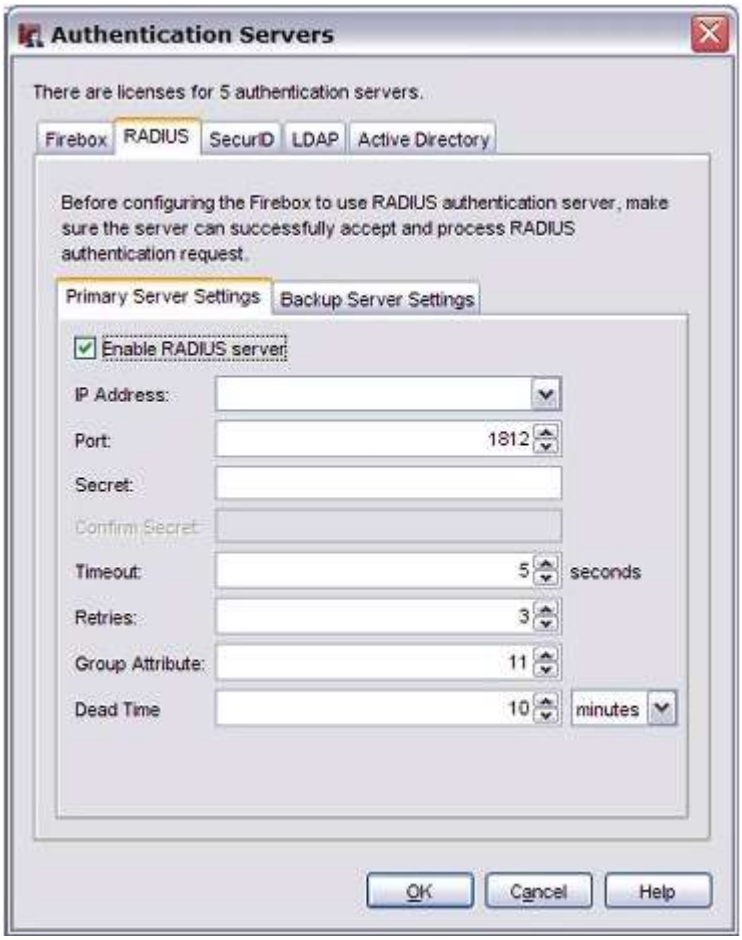
- Добавить IP адрес устройства Firebox на RADIUS сервер. Для более подробной информации см. документацию по RADIUS серверу.
- Включить и настроить RADIUS сервер в вашей конфигурации Firebox.

- Добавить имена пользователей или группы пользователей RADIUS к вашим политикам.

Для того включить и настроить RADIUS сервер(ы) в вашей конфигурации выполните следующее:

1. В Policy Manager нажмите . Или выберите **Setup** > **Authentication** > **Authentication Servers**.
   Откроется диалогое окно Authentication Servers.

2. Выберите закладку **RADIUS Server**



3. Для того чтобы включить RADIUS сервер и активировать поля в этом диалоговом окне включите опцию **Enable RADIUS server**.

4. В поле **IP Address** введите IP адрес RADIUS сервера.

5. В поле **Port** введите номер порта, который используется RADIUS для аутентификации. По умолчанию используется порт 1812. Более ранние версии RADIUS серверов могут использовать порт 1645.

6. В поле **Secret** введите пароль для Firebox и RADIUS сервера. Этот пароль чувствителен к регистру и должен быть одинаковым на Firebox и RADIUS сервере.

7. В поле **Confirm Secret** снова введите пароль.

8. В поле **Timeout** при помощи стрелок установите величину таймаута. Величина таймаута определяет промежуток времени в течение которого Firebox ждет ответа на запрос аутентификации, после чего повторяет запрос снова.

9. В поле **Retries** при помощи стрелок установите количество попыток подключения Firebox к серверу аутентификации. Это количество попыток подключения устройства Firebox к серверу аутентификации, после чего процедура аутентификации считается неуспешной.

10. В поле **Group Attribute** при помощи стрелок установите атрибут группы. По умолчанию атрибут равен FilterID, что соответствует RADIUS атрибуту номер **11**. Атрибут группы используется для настройки атрибута, который будет содержать информацию о User Group. Вам необходимо настроить RADIUS сервер, чтобы он добавлял строку Filter ID в сообщение аутентификации, которое он отправляет Firebox. Например, *engineerGroup* или *financeGroup*. Эта информация затем используется для управления доступом. Firebox сравнивает строку FilterID с именами групп пользователей, настроенных в политиках Firebox.

11. В поле **Dead Time** выберите величину временного интервала, по истечении которого до этого неактивный сервер становится активным. В выпадающем списке выберите единицу измерения: минуты (**minutes)** или часы (**hours)**. Если сервер аутентификации не отвечает в течение какого-либо промежутка времени, то устройство Firebox считает его неактивным. Последующие запросы на аутентификацию не будут отправляться на этот сервер до того момента, пока устройство Firebox не сделает его снова активным.

12. Для того чтобы добавить резервный RADIUS сервер выберите закладку **Secondary Server Settings** и включите опцию **Enable a secondary RADIUS server**.

13. Для настройки всех необходимых параметров см. п. 4–11. Ключ аутентификации (shared secret) должен быть одинаковым на основном и резервном RADIUS серверах

14. Нажмите **OK**.

15. Сохраните конфигурационный файл.

Принцип работы аутентификации через RADIUS сервер

RADIUS – протокол, разработанный для аутентификации пользователей для доступа к dial-in серверу доступа

Сегодня RADIUS сервер используется для разнообразных задач. RADIUS – это клиент-серверный протокол, в котором в качестве клиента выступает устройство Firebox, а в качестве сервера – RADIUS сервер. (RADIUS клиент иногда называют NAS (Network Access Server) сервером) Когда пользователь пытается аутентифицироваться, Firebox отправляет запрос на RADIUS сервер. Если RADIUS сервер настроен для корректной работы с Firebox в качестве клиента, он в ответ на запрос отправляет *accept* или *reject* Сообщения устройству Firebox (Network Access Server).

Процедура аутентификации с использованием RADIUS сервера выглядит следующим образом:

1. Пользователь пытается аутентифицироваться или через HTTPS соединение с Firebox через порт 4100, или через Mobile VPN with PPTP или IPSec сессии. Firebox считывает имя пользователя и пароль.

2. Firebox создает сообщение Access-Request, которое включает в себя ключ аутентификации (shared secret) и зашифрованный пароль, и отправляет его на RADIUS сервер.

3. RADIUS сервер проверяет, что сообщение пришло от известного клиента (Firebox). Если клиент Firebox не настроен на RADIUS сервере, то RADIUS сервер отбрасывает сообщение Access-Request message и не отправляет ничего в ответ.

4. Если клиент Firebox корректно настроен на RADIUS сервере и ключ аутентификации верен, сервер в сообщении Access-Request ищет запрашиваемый метод аутентификации.

5. Если Access-Request использует разрешенный метод аутентификации, RADIUS сервер извлекает из сообщения данные доступа пользователя и ищет совпадения в своей внутренней базе данных. Если RADIUS сервер находит запись с такими именем пользователя и паролем, то он может получить дополнительную информацию о пользователе (разрешение на удаленный доступ, принадлежность к группе, время подключения и т.д).

6. RADIUS сервер проверяет, есть ли у него политика доступа или профиль, соответствующие данным о пользователе. Если такая политика или профиль существуют, то сервер отправляет устройству Firebox ответ.

7. Если сервер не находит записи с указанными именем пользователя и паролем, или у него политики, которая соответствует данным пользователя, то он отправляет сообщение Access-Reject устройству Firebox, сигнализируя об ошибке аутентификации. RADIUS сессия закрывается и Firebox отказывает пользователю в доступе.

8. В противном случае RADIUS отправляет устройству Firebox сообщение Access-Accept.

9. Для всех отправляемых сообщений RADIUS сервер использует ключ аутентификации. Если ключ аутентификации в ответе RADIUS сервера не совпадает с ключом, указанным в запросе, то Firebox отбрасывает этот ответ от RADIUS сервера. Для того чтобы посмотреть сообщения диагностики процедуры аутентификации, вам необходимо установить необходимый уровень этих сообщений и изменить уровень для сообщений журнала категории **Authentication**

10. Firebox считывает значение любого атрибута FilterID в сообщении и подключает пользователя в группу RADIUS.

11. RADIUS сервер в сообщение Access-Accept может добавить большое количество дополнительной информации. Firebox просто игнорирует большую часть этой информации (например, список разрешенных пользователю протоколов - PPP или SLIP, список портов, доступ к которым может получить пользователь, таймауты ожидания и другие атрибуты.

12. Единственный атрибут, обрабатываемый Firebox в сообщении Access-Accept, это атрибут FilterID (RADIUS атрибут номер 11). FilterID необходим Firebox для того чтобы добавить пользователя в группу RADIUS. Для более подробной информации о RADIUS группах, см. следующий раздел.

RADIUS группы

При настройке RADIUS аутентификации вы можете выбрать номер атрибута Group Attribute. Fireware XTM считывает номер атрибута Group Attribute из Policy Manager для того чтобы сообщить в каком атрибуте RADIUS будет передаваться информация о RADIUS группе. Fireware XTM в качестве атрибута группы понимает только номер атрибута RADIUS равный 11, FilterID

При настройке RADIUS сервера не меняйте этот номер.

Когда Firebox получает Access-Accept от RADIUS сервера, он считывает значение атрибута FilterID и использует это значение для привязки пользователя с RADIUS группой. (Настроить FilterID в вашей конфигурации RADIUS вам необходимо будет вручную). Соответственно значение атрибута FilterID это и есть название RADIUS группы, в которую Firebox добавляет пользователя

RADIUS группы, которые вы используете в Policy Manager, это не Windows группы, созданные на вашем контроллере домена, или группы, которые существуют в вашей базе данных пользователей домена. RADIUS группа – это логическая группа пользователей Firebox. Значение FilterID может совпадать с именем локальной группы или группы домена вашей компании, однако это необязательно. Для имен групп мы рекомендуем использовать информативное имя, которое будет содержать информацию о назначении этой группы

Использование RADIUS групп на практике

Если в вашей сети достаточно большое количество пользователей, которых необходимо аутентифицировать, вы можете значительно упросить эту процедуру, заставив RADIUS сервер отправлять один и тот же FilterID для определенных групп пользователей. Firebox будет объединять этих пользователей в логические группы, что значительно упростит управление доступом для этих пользователей. При создании политики в Policy Manager, которая разрешает доступ к сети только аутентифицированным пользователям, вы можете вместо списка пользователей указать имя RADIUS группы, к которой будут принадлежать этот интерфейс.

Например, если Мэри пытается аутентифицироваться, RADIUS сервер в ответ отправляет FilterID=*Sales*. Firebox добавляет Мэри в RADIUS группу *Sales*. Затем Джон и Эллис пытаются также аутентифицироваться и RADIUS в ответ отправляет FilterID=*Sales*. Тем самым Мэри, Джон и Эллис теперь все принадлежат группе *Sales*. Теперь в Policy Manager вы сможете создать политику, которая разрешит пользователям, принадлежащим группе *Sales,* доступ к ресурсам сети.

Вы также можете настроить RADIUS сервер, чтобы он возвращал другой FilterID, например *IT Support* для ваших сотрудников технической поддержки, и затем создать отдельную политику для этой группы.

Например для группы *Sales* вы можете разрешить доступ к сети Интернет, используя политику Filtered-HTTP. Затем вы можете ограничить их доступ к web-сайтам при помощи WebBlocker. А для группы *IT Support* вы можете использовать политику Unfiltered-HTTP, которая разрешает доступ в сеть Интернет без фильтра WebBlocker. В поле **From** при настройке политики вы можете ввести имя RADIUS группы, для того чтобы показать, какая группа будет использовать эту политику.

Таймаут и количество попыток подключения

Если от основного RADIUS сервера не приходит ответа на запрос процедура аутентификация считается неуспешной. После трех неудачных попыток Fireware XTM пытается запросить аутентификацию у резервного RADIUS сервера. Этот процесс называется *переключение*

Это количество попыток аутентификации не равно значению поля Retry. Вы не можете изменить количество попыток аутентификации, после которых будет запущена процедура переключения

Firebox отправляет сообщение Access-Request на первый RADIUS сервер в списке. Если ответа от него нет, то Firebox ждет определенное количество секунд (значение в поле **Timeout)**, и затем снова отправляет сообщение Access-Request.

Это продолжается определенное число раз (значение в поле Retry) (или пока не придет ответ от сервера). Если от RADIUS не получено ответа или если ключ аутентификации RADIUS не совпадает, Fireware XTM считает это неудачной попыткой аутентификаци.

После трех неудачных попыток, Fireware XTM отправляет запрос на второй RADIUS сервер. Если попытка запросить аутентификацию у второго сервера тоже была неудачной, то Fireware XTM ждет в течение 10 минут, пока администратор не исправит проблему. Затем этот цикл повторяется.

Настройка аутентификации через VASCO сервер

Аутентификация сервера VASCO использует ПО VACMAN Middleware для аутентификации удаленных пользователей в локальной сети компании через сервер RADIUS или web сервер

VASCO также поддерживает несколько серверов аутентификации. Система одноразовых паролей VASCO позволяет устранить наиболее уязвимое место в любой системе безопасности — использование статических паролей.

Для того чтобы использовать аутентификации сервера VASCO с Firebox, выполните следующее:

- Добавьте IP-адрес устройства Firebox на сервер VACMAN Middleware, как описано в документации VASCO.
- Включите и настройте сервер VACMAN Middleware в конфигурации Firebox

Добавьте имена пользователей или имена группы в политики Policy Manager. Аутентификации сервера VASCO настраивается при помощи настроек сервера RADIUS.

Диалоговое окно **Authentication Servers** не содержит отдельной закладки для серверов VACMAN Middleware.

1. В Policy Manager нажмите  . Или выберите **Setup** > **Authentication** > **Authentication Servers**.
   Откроется диалогое окно Authentication Servers.

2. Выберите закладку **RADIUS**

3. Для того чтобы включить сервер VACMAN Middleware и поля в диалоговом окне, включите опцию **Enable RADIUS server**

4. В поле **IP Address** введите IP-адрес сервера VACMAN Middleware.

5. Убедитесь, что в поле **Port** используется номер порта, используемый VASCO. По умолчанию используется номер порта 1812.

6. В поле **Secret** введите пароль для Firebox и сервера VACMAN Middleware. В поле **Confirm Secret** повторите ввод пароля. Этот пароль чувствителен к регистру, и должен быть одинаковым на Firebox и сервере RADIUS.

7. В поле **Timeout** введите значение таймаута. Это значение определяет промежуток времени, в течение которого Firebox ждет ответа от сервера аутентификации до тех пор, пока он не попытается снова подключиться.

8. В поле **Retries** введите количество попыток подключения. Это максимальное количество попыток соединения устройством Firebox с сервером аутентификации (используя величину таймаута), после чего Firebox сообщит, что соединение не может быть установлено

9. Для того чтобы настроить атрибут группы используйте элемент управления **Group Attribute**. По умолчанию используется атрибут **FilterID**, который является атрибутом VASCO под номером 11. Значение атрибута группы используется для настройки атрибута, который будет содержать информацию об User Group. Вам необходимо настроить сервер VASCO таким образом, чтобы он при отправке сообщения на Firebox о том, что пользователы был аутентифицирован, он также отправлял строку FilterID; например, engineerGroup или financeGroup. Эта информация затем используется для управления доступом; строка FilterID совпадает с именем группы, настроенной в политиках Firebox

10. Для того чтобы настроить промежуток времени после которого неактивный сервер снова будет считаться активным, введите его в поле **Dead Time.** Если сервер аутентификации не отвечает определенное время, он помечается как неактивный. Последующие попытки аутентификации на этом сервере будут отброшены

11. Для того чтобы добавить резервный сервер VACMAN Middleware, выберите закладку **Secondary Server Settings** и включите опцию **Enable a secondary RADIUS server**. В соответствующих полях введите необходимую информацию. Убедитесь, что используемый пароль (shared secret) один и тот же на основном и резервном серверах аутентификации. Для более подробной информации см.”Настройка резервного сервера аутентификации”.

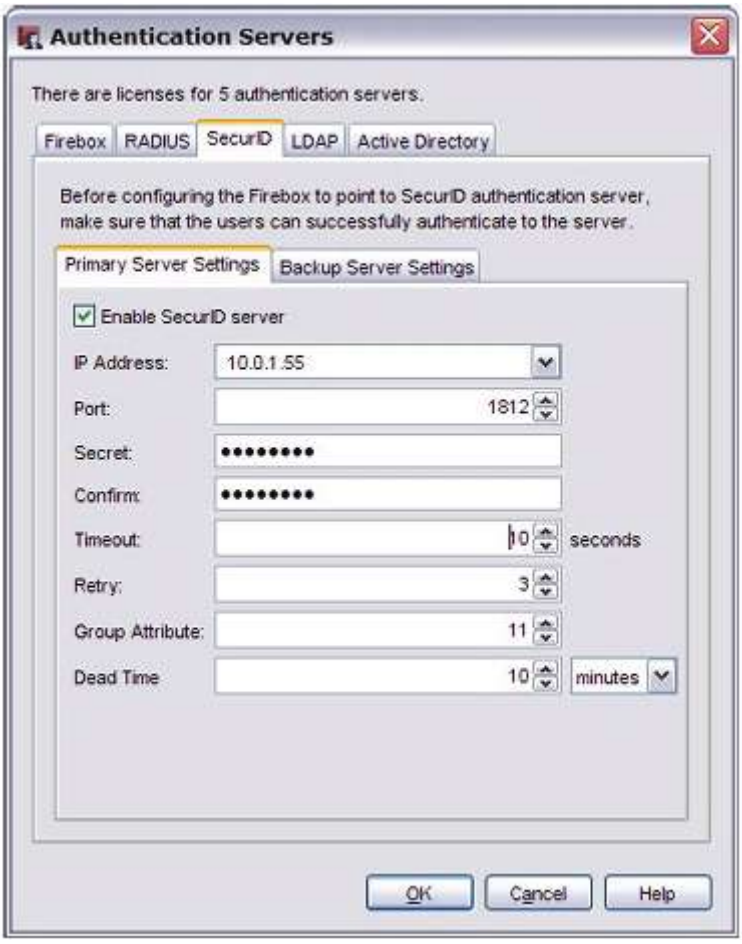
12. Нажмите **OK**. Сохраните конфигурационный файл.

Настройка SecurID аутентификации

Для того чтобы использовать SecurID аутентификацию, вам необходимо правильно настроить серверы RADIUS, VASCO и ACE/Server. Пользователям также необходимо иметь SecurID токен и PIN-код. Для более подробной информации, см. Инструкции по SecurID.

1. В Policy Manager нажмите . Выберите **Setup > Authentication > Authentication Servers**.
   Откроется диалогое окно Authentication Servers.

2. Выберите закладку **SecurID**



3. Для того чтобы включить сервер SecurID и активировать поля в этом окне включите опцию **Enable SecurID server**.

4. В поле **IP Address** введите IP-адрес сервера SecurID.

5. В поле **Port** введите номер порта, который будет использоваться для SecurID аутентификации.
   По умолчанию используется порт номер 1812.

6. В поле **Secret** введите пароль для Firebox® и сервером SecurID.
   Этот пароль чувствителен к регистру, и должен быть одинаковым на Firebox и на сервере SecurID.

7. В поле **Confirm** введите ключ еще раз.

8. В поле **Timeout** устанавливаете величину таймаута.
   Этот параметр устанавливает промежуток времени, в течение которого Firebox ждет ответа от сервера аутентификации перед тем, как повторить подключение.

9. В поле **Retry** установите количество попыток подключения Firebox к серверу аутентификации.
   Это количество попыток подключения Firebox к серверу аутентификации (используя значение таймаута, введенного ранее), перед тем как Firebox сообщит об ошибке при подключении для одной попытки аутентификации

10. В поле **Group Attribute** установите необходимый атрибут группы.
    Атрибут группы используется для того чтобы установить, какие атрибуты несут информацию о Группе Пользователей. Когда сервер RADIUS отправляет Firebox сообщение о том, что пользователь был аутентифицирован, он также отправляет строку Группы Пользователей; например,“engineerGroup” или “financeGroup”. Эта информация затем используется для управления доступом.

11. В поле **Dead Time** укажите промежуток времени по истечении которого неактивный сервер будет помечен как активный. После того как сервер аутентификации не отвечает в течение определенного промежутка, он помечается как неактивный. Последующие запросы не будут поступать на этот сервер до тех пор, пока он снова не станет активным.

12. Для того чтобы добавить резервный сервер SecurID, в закладке **Secondary Server Settings** включите опцию **Enable a secondary SecurID server**. Если вы включите эту опцию, то вам необходимо будет ввести IP-адрес и номер порта резервного сервера SecurID. Для основного и резервного серверов SecurID пароль должен быть одинаковым. Для более подробной информации см.”Настройка резервного сервера аутентификации”

13. Нажмите **OK**.

14. Сохраните конфигурационный файл.

Настройка аутентификации Active Directory

Active Directory - Windows-приложение для работы с LDAP справочником. Active Directory позволяет вам расширить концепцию иерархии доменов, которая используется в DNS, на уровень организации. Вся информация и необходимые параметры хранятся в одной центральной базе данных.

Вы можете использовать сервер аутентификации Active Directory, для того, чтобы пользователи могли аутентифицироваться при помощи своих данных сетевого доступа. Для этого вам необходимо будет настроить как устройство, так и сервер Active Directory.

Перед тем как начать, убедитесь что все ваши пользователи могут аутентифицироваться на сервер Active Directory.

1. В Policy Manager нажмите  . Или выберите **Setup** > **Authentication** > **Authentication Servers**.
   Откроется диалогое окно Authentication Servers.

2. Выберите закладку **Active Directory**

3. Включите опцию **Enable Active Directory server**.

4. В поле **IP Address** введите IP адрес основного сервера Active Directory. Сервер Active Directory может быть подключен к любому интерфейсу Firebox. Вы также можете настроить ваше устройство для использования сервера Active Directory, который доступен через VPN туннель.

5. В поле **Port** выберите номер TCP порта, через который устройство подключается к серверу Active Directory. По умолчанию используется порт 389. Если ваш сервер Active Directory является глобальным справочным сервером, то рекомендуется изменить номер порта по умолчанию. Для более подробной информации см. “Изменение порта по умолчанию сервера Active Directory”

6. В поле **Search Base** введите строку поиска. Стандартный формат строки поиска: ou=<название_департамента_организации>,dc=<первая_часть_уникального_имени_сервера>,dc=<любая_часть_уникального_имени_сервера_которая_записывается_после_точки>. Строка поиска используется для сужения области поиска необходимой информации. Мы рекомендуем строку поиска привязать к корневому элементу домена. Это позволит вам найти всех пользователей и групп, которым этот пользователь принадлежит

7. В поле **Group String** введите атрибут, который будет использоваться для хранения информации о группе пользователя на сервере Active Directory. Если вы не меняли вашу схему Active Directory, то значение этой строки будет `memberOf`.

8. В поле **DN of Searching User** введите DN имя для поиска. Если вы используете атрибут логина `sAMAccountName` вам нет необходимости вводить какие-либо данные в это поле. Если вы измените атрибут логина, вам необходимо добавить значение поля **DN of Searching User в вашу конфигурацию**. Вы можете ввести любое DN пользователя с

правами поиска в LDAP/Active Directory, например Administrator. Более «слабого» DN с правом поиска обычно бывает достаточно.

9. В поле **Password of Searching User** введите пароль, связанный с уникальным именем, для поиска.

10. В поле **Login Attribute** введите атрибут логина LDAP, который будет использоваться для аутентификации. Атрибут логина – это имя, которое используется для привязки к базе данных LDAP. Атрибут логина по умолчанию – это *sAMAccountName*. Если вы используете *sAMAccountName*, то поля **DN of Searching User** и **DN of Searching Password** можно оставить пустыми.

11. В поле **Dead Time** укажите промежуток времени по истечении которого неактивный сервер будет помечен как активный. После того как сервер аутентификации не отвечает в течение определенного промежутка, он помечается как неактивный. Последующие запросы не будут поступать на этот сервер до тех пор, пока он снова не станет активным.

12. Для того чтобы добавить резервный LDAP сервер, выберите закладку **Backup Server Settings** и включите опцию **Enable a secondary LDAP server**. Введите необходимую информацию. Убедитесь, что пароли на основном и резервном серверах одинаковы

13. Нажмите **OK**.

14. Сохраните конфигурационный файл.

Дополнительные параметры Active Directory

Ответ от сервера содержит список атрибутов, из которых Fireware XTM может получить дополнительные данные от сервера LDAP или Active Directory, которые затем можно присвоить аутентифицированным пользовательским сессиям (например, таймауты и Mobile VPN with IPSec адреса). Так как данные, полученные от LDAP сервера, привязаны к отдельным пользователям, то вы не ограничены значениями глобальных параметров. Вы можете использовать эти параметры для каждого отдельного пользователя. Для более подробной информации см. “Настройка дополнительных параметров Active Directory или LDAP”

Определение вашей строки поиска Active Directory

При настройке Firebox для аутентификации через сервер Active Directory server вам необходимо создать *базу поиска (search base)*. Search base определяет, с какого места в иерархической структуре Active Directory начинать поиск. Это позволит значительно ускорит процедуру аутентификации. Для этого вам необходим рабочий сервер Active Directory, который будет содержать всю необходимую информацию о пользователях, которых вы хотите аутентифицировать на устройстве Firebox.

1. На вашем сервере Active Directory выберите **Start** > **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.

2. Найдите свой домен.

3. Откройте его для того, для того, чтобы посмотреть путь к нему.

Компоненты имени домена, имеющие формат *dc=domain name component*, добавляются в конец строки базы поиска и разделены запятой.

В строку базы поиска для каждого уровня в вашем домене, вам необходимо добавить отдельное имя домена. Например, если у вас есть домен *prefix.example.com*, то компонент домена в вашей базе поиска будет выглядеть так: `DC=prefix,DC=example,DC=com`.

Предположим, что ваше имя домена выгляди так:

Тогда строка базы поиска, которую необходимую добавить в конфигурацию Firebox, будет выглядеть так:

```
DC=Kunstlerandsons,DC=com
```

Строка поиска не чувствительна к регистру.

Поля DN of Searching User и Password of Searching User

Если в поле **Login Attribute** вы введете значение, отличное от значения по умолчанию *sAMAccountName,* вам необходимо заполнить эти поля. Большинство компаний, которые используют Active Directory, значения этих полей не меняют. Если вы оставите значение этого поля по умолчанию (*sAMAccountName)*, пользователи для аутентификации будут использовать свои обычные имена пользователей Active Directory. Это имя пользователя вы можете посмотреть в поле **User** закладки **Account** при редактировании информации о пользователях в секции *Users and Computers* сервера Active Directory.

Если вы измените значение поля **Login Attribute**, пользователь для аутентификации использует другой формат имени пользователя. В этом случае в вашей конфигурации вам необходимо указать данные доступа *Searching User credentials*.

Изменение порта по умолчанию сервера Active Directory

Если для аутентификации пользователей ваш Firebox использует сервер аутентификации Active Directory (AD), он подключается к серверу Active Directory через стандартный порт LDAP - TCP порт 389. Если серверы Active Directory в конфигурации вашего Firebox настроены, как глобальные справочные серверы, то для подключения к ним Firebox может использовать порт 3268.

Глобальный справочный сервер – это контроллер домена, который хранит всю необходимую информацию обо всех объектах. Тем самым приложения могут искать необходимую информацию на сервере Active Directory без ссылки на другие контроллеры домена. Если у вас используется только один домен, компания Microsoft рекомендует настроить все контроллеры домена, как глобальные справочные серверы.

Если основной и резервный серверы Active Directory настроены как глобальные справочники, то для увеличения скорости обработки запросов на аутентификацию вы можете изменить порт, по которому Firebox подключается к серверу Active Directory. Однако мы не рекомендуем создавать дополнительные глобальные справочники Active Directory только с целью увеличить скорость обработки запросов на аутентификацию. Процедуры репликации между глобальными справочниками могут использовать значительную часть вашей пропускной способности.

Настройка Firebox для использования порта глобального справочника

1. В Policy Manager нажмите  . Или выберите **Setup** > **Authentication** > **Authentication Servers**.
   Откроется диалогое окно Authentication Servers.

2. Выберите закладку **Active Directory**.

3. В поле **Port** введите **3268**.

4. Нажмите **OK**.

5. Сохраните конфигурационный файл.

Как проверить, является ли ваш сервер Active Directory глобальным справочником

Выберите **Start Menu** > **Administrative Tools** > **Active Directory Sites and Services**.

В левой панели откройте элемент **Sites** и найдите ваш сервер Active Directory.

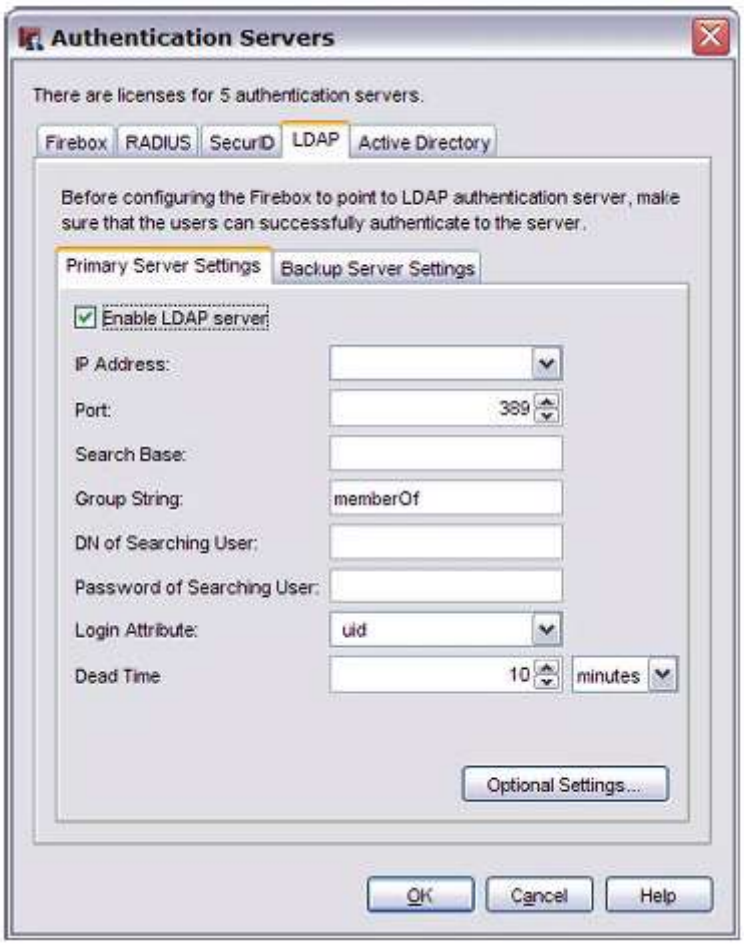
Нажмите правой кнопкой на **NTDS Settings** для вашего сервера Active Directory и выберите **Properties**. Если опция **Global Catalog** включена, то сервер Active Directory используется как глобальный справочник.

Настройка LDAP аутентификации

Для аутентификации пользователей вы также можете использовать LDAP-аутентификацию. LDAP – протокол открытых стандартов, который используется для online directory и работает с транспортными Интернет-протоколами, такими как TCP. Перед тем как приступить к настройке Firebox для LDAP-аутентификации, посмотрите документацию поставщика LDAP решения на предмет поддержки атрибута *memberOf* (или эквивалентный атрибут).

1. В Policy Manager нажмите  . Или выберите **Setup** > **Authentication** > **Authentication Servers**.
   Откроется диалогое окно Authentication Servers.

2. Выберите закладку **LDAP**



3. Для того, чтобы включить LDAP сервер и активировать поля в этом диалоговом окне включите опцию **Enable LDAP server**.

4. В поле IP Address введите IP-адрес основного LDAP-сервера.
LDAP-сервер может быть подключен к любому интерфейсу Firebox interface или доступен через VPN-туннель.

5. Из выпадающего списка Port выберите TCP порт, который будет использовать Firebox для подключения к LDAP-серверу. По умолчанию используется порт 389.
LDAP over TLS не поддерживается.

6. В поле **Search Base** введите строку базы поиска. Стандартный формат строки поиска: ou=название_отдела_организации,dc=первая часть уникального имени сервера,dc=любая часть уникального имени сервера, которая ставится после точки.

   Строка поиска используется для ускорения поиска необходимой информации путем сужения области поиска на сервере. Например, если ваши пользователи принадлежат OU(organizational unit)=*accounts* и имя домена=*example.com*, строка поиска будет выглядеть так:

   ```
   ou=accounts,dc=example,dc=com
   ```

7. В поле **Group String** введите атрибут группы.
Эта строка используется для хранения информации о группе пользователей на LDAP сервере. На многих LDAP серверах, по умолчанию используется строка “uniqueMember”; на других – “member”.

8. В поле **DN of Searching User** введите уникальное имя (DN) для поиска. Вы можете ввести любое DN пользователя с правами поиска в LDAP/Active Directory, например Administrator.

Более «слабое» DN с правом поиска бывает достаточно, и некоторые администраторы создают пользователя с правами поиска, но с ограниченными правами на доступ к этому полю.

9. В поле **Password of Searching User** введите пароль, связанный с уникальным именем, для поиска.

10. В поле **Login Attribute** введите атрибут логина LDAP, который будет использоваться для аутентификации. Атрибут логина – это имя, которое используется для привязки к базе данных LDAP. Атрибут логина по умолчанию – это uid. Если вы используете uid, то поля **DN of Searching User** и **Password of Searching User** можно оставить пустыми.

11. В поле **Dead Time** укажите промежуток времени по истечении которого неактивный сервер будет помечен как активный. После того как сервер аутентификации не отвечает в течение определенного промежутка, он помечается как неактивный. Последующие запросы не будут поступать на этот сервер до тех пор, пока он снова не станет активным.

12. Для того чтобы добавить резервный LDAP сервер, выберите закладку **Backup Server Settings** и включите опцию **Enable a secondary LDAP server**. Введите необходимую информацию. Убедитесь, что пароли на основном и резервном серверах одинаковы. Для более подробной информации см. ”Настройка резервного сервера аутентификации”

13. Нажмите **OK**.

14. Сохраните конфигурационный файл.

Дополнительные параметры LDAP

Ответ от сервера содержит список атрибутов, из которых Fireware XTM может получить дополнительные данные от сервера LDAP или Active Directory, которые затем можно присвоить аутентифицированным пользовательским сессиям (например, таймауты и Mobile VPN with IPSec адреса). Так как данные, полученные от LDAP сервера, привязаны к отдельным пользователям, то вы не ограничены значениями глобальных параметров. Вы можете использовать эти параметры для каждого отдельного пользователя. Для более подробной информации см. “Настройка дополнительных параметров Active Directory или LDAP”

Использование дополнительных параметров Active Directory или LDAP

Ответ от сервера содержит список атрибутов, из которых Fireware XTM может получить дополнительные данные от сервера LDAP или Active Directory, которые затем можно присвоить аутентифицированным пользовательским сессиям (например, таймауты и Mobile VPN with IPSec адреса). Так как данные, полученные от LDAP сервера, привязаны к отдельным пользователям, то вы не ограничены значениями глобальных параметров. Вы можете использовать эти параметры для каждого отдельного пользователя. Для более подробной информации см. “Настройка дополнительных параметров Active Directory или LDAP”

Перед тем как начать

Для того чтобы использовать дополнительные параметры вам необходимо выполнить следующие шаги:

- Расширьте схему директории для добавления новых атрибутов
- Сделайте атрибуты доступными классу объекта, которому принадлежат учетные записи пользователей
- Введите значения атрибутов для объектов пользователей

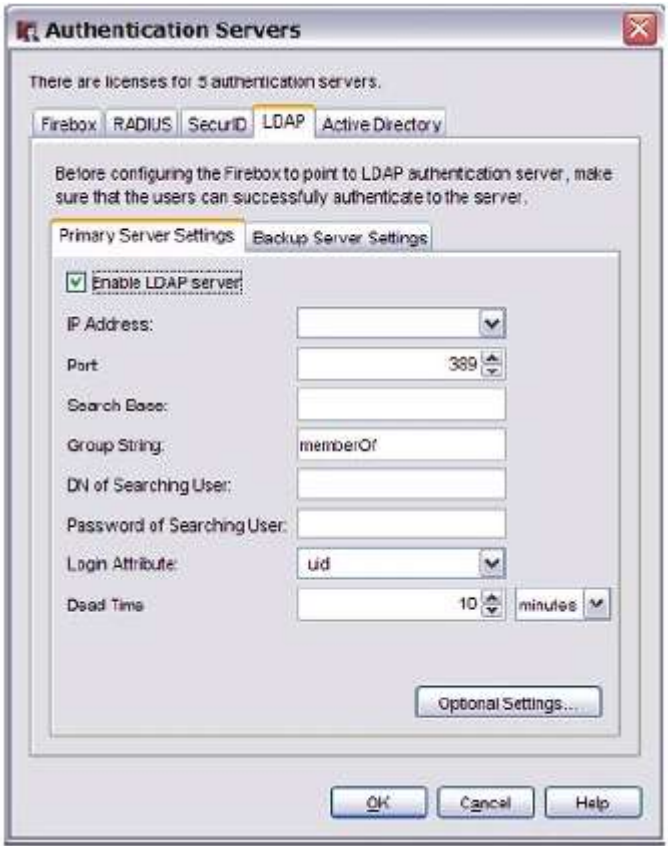
Перед тем как расширять схему вам необходимо выполнить тщательное планирование и тестирование. Изменения схемы Active Directory остаются навсегда и не могут быть отменены. Для более подробной информации о расширении схемы см. информацию на сайте Microsoft. Перед тем как расширять схему для других справочников, посмотрите документацию поставщика LDAP решения

Настройка дополнительных параметров Active Directory или LDAP

Для того, чтобы настроить дополнительные атрибуты, которые будут содержать в ответе сервера и в которых Fireware XTM будет искать дополнительную информацию, выполните следующее:

1. В Policy Manager выберите **Setup** > **Authentication** > **Authentication Servers**.
   Откроется диалоговое окно Authentication Servers

2. Выберите закладки **LDAP** или **Active Directory** для проверки включенности сервера



3. Нажмите Optional Settings.
Откроется диалогое окно Server Optional Settings

4. Введите необходимые атрибуты, которые вы хотите добавить в строку поиска

IP Attribute String

Это поле применяется только для клиентов Mobile VPN. Введите имя атрибута, которое Fireware будет использовать для присвоения клиенту Mobile VPN виртуального IP-адреса. Это должен быть атрибут с одним значением. Значением атрибута должен быть IP-адрес. IP-адрес должен лежать в пуле виртуальных IP адресов, указанный вами при создании группы Mobile VPN. Если Firebox не видит IP атрибута в результате поиска или если вы не указали атрибут в Policy Manager, он присваивает клиенту Mobile VPN виртуальный IP адрес из пула, который вы создали при создании Mobile VPN Group.

Netmask Attribute String

Это поле применяется только для клиентов Mobile VPN. Введите имя атрибута, которое будет использовать Fireware для присвоения маски подсети виртуальному IP-адресу клиента Mobile VPN. Это должен быть атрибут с одним значением. Значение атрибута – нормальная маска подсети. ПО Mobile VPN автоматически присваивает маску подсети если Firebox не видит атрибута маски подсети в результатах поиска или если вы не указали атрибут в Policy Manager.

DNS Attribute String

Это поле применяется только для клиентов Mobile VPN. Введите имя атрибута, которое будет использовать Fireware для присвоения клиенту Mobile VPN одного или нескольких DNS адресов на время сессии Mobile VPN. Этот атрибут может содержать несколько значений. Каждое значение атрибута должно содержать IP-адрес. Если Firebox не видит DNS атрибут в результатах поиска или если вы не указали его в Policy Manager, то он использует WINS адреса, которые вы ввели при настройке WINS и DNS серверов.

WINS Attribute String

Это поле применяется только для клиентов Mobile VPN.

Введите имя атрибута, которое будет использовать Fireware для присвоения клиенту Mobile VPN одного или нескольких WINS адресов на время сессии Mobile VPN. Этот атрибут может содержать несколько значений. Каждое значение атрибута должно содержать IP-адрес. Если Firebox не видит WINS атрибут в результатах поиска или если вы не указали его в Policy Manager, то он использует WINS адреса, которые вы ввели при настройке WINS и DNS серверов.

Lease Time Attribute String

Это поле применяется для клиентов Mobile VPN и клиентов, которые используют аутентификацию межсетевого экрана. Введите имя атрибута, которым Fireware будет управлять промежутком времени в течение которого пользователь может оставаться аутентифицированным (таймаут сессии). После того, как это промежуток времени закончится, Fireware удалит пользователя из списка аутентифицированных пользователей. Это должен быть атрибут с одним значением. Fireware интерпретирует значение атрибута как количество секунд. Ноль интепретируется как отсутствие таймаута.

Idle Timeout Attribute String

Это поле применяется для клиентов Mobile VPN и клиентов, которые используют аутентификацию межсетевого экрана. Введите имя атрибута, который будет использоваться Fireware для управления промежутком времени, в течение которого пользователь может оставаться неактивным. Если во время этого промежутка времени пользователь не передавал трафик, то Fireware удаляет его из списка аутентифицированных пользователей. Это должен быть атрибут с одним значением. Fireware интерпретирует значение атрибута как количество секунд. Ноль интепретируется как отсутствие таймаута.

5. Нажмите **OK**.
Параметры атрибутов будут сохранены.

Аутентификация с использованием локальной учетной записи

Любой пользователь может аутентифицироваться как пользователь Firewall, PPTP пользователь или пользователь Mobile VPN, и создавать PPTP или Mobile VPN туннель, если они включены на Firebox. Однако после того как была выполнена процедура аутентификации или был успешно создан туннель, пользователи могут по туннелю передавать трафик, который разрешен политикой Firebox. Например, пользователь Mobile VPN-only может передавать трафик только через Mobile VPN туннель. Даже если он может создавать PPTP туннель, данные по нему он передавать не может. Если вы используете аутентификацию Active Directory и пользователь группы не

соответствует вашей политике Mobile VPN, вы можете увидеть сообщение об ошибке, в котором говорится что *decrypted traffic does not match any policy*. Если вы увидите это сообщение об ошибке, убедитесь, что пользователь находится в группе с таким же именем, как и у группы Mobile VPN.

Использование в политиках пользователей и групп

Если вы используете Firebox как сервер аутентификации, вы можете использовать пользователей и группы пользователей при создании политик в Policy Manager. Например, вы можете создать политику, которая разрешает соединения только аутентифицированным пользователям. Или вы можете ограничить подключения только для определенных пользователей. Термин *авторизованные пользователи и группы* обозначает пользователей и группы пользователей, которым разрешен доступ к сетевым ресурсам.

Создание пользователей и групп для аутентификации Firebox

Если вы используете Firebox как сервер аутентификации и хотите создать пользователей или группы пользователей, которые будут аутентифицироваться через Firebox, см. “Создание нового пользователя для аутентификации Firebox” и “Создание новой группы для аутентификации Firebox”

Создание пользователей и групп для аутентификации на серверах сторонних производителей

1. На сервере аутентификации создайте группу, которая будет содержать учетные записи всех пользователей

2. В Policy Manager выберите **Setup** > **Authentication** > **Authorized Users/Groups**. *Откроется диалогое окно Authorized Users and Groups*

3. Нажмите **Add**.
   Откроется диалогое окно Define New Authorized User or Group

4. Введите имя пользователя или группы, которых вы создали на сервере аутентификации.

5. (Дополнительно) Введите описание для пользователя или группы.

6. Выберите переключатель **Group** или **User**.

7. В выпадающем списке **Auth Server** выберите тип сервера аутентификации. Выберите **RADIUS** если вы хотите использовать RADIUS или VACMAN Middleware серверы, или **Any** для остальных серверов

8. Нажмите **OK**

Добавление пользователей или групп в политику

Любой пользователь или группа пользователей, которых вы хотите использовать в политике, должны быть в нее добавлены в качестве авторизованных пользователей. Все пользователи и группы, которые вы создали для аутентификации Firebox и все пользователи Mobile VPN автоматически добавляются в список авторизованных пользователей и групп. В этот список вы можете добавить любого пользователя или группу пользователей. Теперь вы готовы добавлять пользователей и группы к вашим политикам

1. В Policy Manager выберите закладку **Firewall**.

2. Два раза нажмите на политику.
   Откроется диалогое окно Edit Policy Properties.

3. В закладке **Policy** под полем **From** нажмите **Add**.
   Откроется диалогое окно Add Address.

4. Нажмите **Add User**.
   Откроется диалогое окно Add Authorized Users or Groups.

5. Слева в выпадающем списке **Type** выберите тип авторизации пользователя или группы: Firewall, PPTP или SSL VPN пользователь

6. Справа в выпадающем списке **Type** выберите **User** или **Group**.

7. Если ваш пользователь или группа появится в списке **Groups**, выберите пользователя или группу и нажмите **Select**.
   Снова откроется диалоговое окно Add Address с пользователем и группой в списке Selected Members or Addresses.

   Нажмите **OK** для того, чтобы закрыть диалоговое окно **Edit Policy Properties**.

8. Если ваши пользователь или группа не появятся в списке в диалоговом окне **Add Authorized Users or Groups**, см. “Создание нового пользователя для аутентификации Firebox”, “Создание новой группы для аутентификации Firebox”, или “Серверы аутентификации сторонних производителей”

После того, как вы добавите пользователя или группу к политике, WatchGuard System Manager автоматически добавляет политику WatchGuard Authentication в конфигурацию Firebox. Эта политика используется для управления доступом к странице аутентификации

Глава 13 - Политики

Политики

Политика безопасности вашей организации – это совокупность правил, которая используется для защиты вашей сети и передаваемого по ней трафика. Firebox блокирует все пакеты, которые запрещены политикой. После того, как вы добавите *политику* в конфигурационный файл вашего Firebox, вы создаете совокупность правил, которые используются Firebox для разрешения или блокировки трафика на базе таких параметров, как IP адрес источника и назначения или TCP/IP порт или протокол.

В качестве примера использования политики рассмотрим следующую ситуацию: администратор сети хочет удаленно подключаться через Remote Desktop к web-серверу, защищенному Firebox. В то же время, администратор хочет, чтобы другие пользователи не могли пользоваться Remote Desktop. Для этого администратор добавляет политику, которая разрешает RDP подключения только с IP адреса компьютера администратора на IP адрес web-сервера.

Политика также дает устройству Firebox дополнительные инструкции по обработке трафика. Например ведение журнала или генерация уведомлений, или NAT (Network Address Translation) для изменения IP адреса источника или порта трафика.

Пакетный фильтр и прокси

Для фильтрации трафика Firebox использует два типа политик: *пакетные фильтры* и *прокси*. Пакетный фильтр проверяет IP и TCP/UDP заголовок каждого пакета и при необходимости блокирует пакет.

Прокси помимо заголовков каждого пакета, также проверяет их содержимое. Этот процесс также называется углубленная проверка пакетов (*deep packet inspection)*. Если заголовок и содержимое пакета не представляют угрозы, то Firebox пропускает его. В противном случае пакет блокируется.

Добавление политик в Firebox

Firebox содержит большое количество предварительно созданных пакетных фильтров и прокси, которые вы можете добавлять в вашу конфигурацию. Например, если вам нужен пакетный фильтр для всего Telnet трафика, вам необходимо добавить политику Telnet. Вы также можете создать свою собственную политику, в которой вы можете настроить необходимые порты, протоколы и другие параметры.

При настройке Firebox при помощи мастера Quick Setup Wizard, сам мастер добавляет несколько пакетных фильтров в вашу конфигурацию: Outgoing (TCP-UDP), FTP, ping и одну или две политики управления WatchGuard. Если вы хотите, чтобы устройство Firebox проверял другие виды трафика, вам необходимо сделать следующее:

- Для этих видов трафик настроить политики на вашем Firebox
- Настроить approved хосты и параметры для этих политик
- Создать баланс между уровнями безопасности вашей сети и доступа ваших пользователей к ресурсам сети

Мы рекомендуем при настройке Firebox установить ограничения на исходящий доступ.

В документации под термином «политики» мы имеем в виду пакетные фильтры и прокси и вся информация, касающаяся политик, относится к пакетным фильтрам и прокси, если нет специальной пометки.

Policy Manager

Fireware XTM Policy Manager - утилита WatchGuard, при помощи которой вы можете создавать, редактировать и сохранять конфигурационные файлы. При работе с утилитой Policy Manager на экране вы можете увидеть версию вашего конфигурационного файла

Окно Policy Manager

Policy Manager имеет две закладки: **Firewall** и **Mobile VPN with IPSec**.

- Закладка **Firewall** показывает политики, которые используются для обычного трафика брандмауэра через Firebox. Закладка **Firewall** также содержит политики BOVPN, тем самым вы можете видеть порядок, в котором Firebox проверяет трафик и применяет правила политики. (Для того чтобы изменить порядок см. ”Порядок следования политик”)

- Закладка **Mobile VPN with IPSec** показывает политики, которые используются с Mobile VPN with IPSec туннелями.

Пользовательский интерфейс Policy Manager имеет два режима отображения: иконки политик (вид Large Icons, используется по умолчанию) или список (вид Details view). Для более подробной информации о переключении между двумя видами см. ”Изменение типа отображения политик в Policy Manager”

Иконки политик

Окно Policy Manager содержит иконки для политик, созданных на Firebox. Для того чтобы редактировать политики просто два раза кликните на необходимой политике. Вид иконок отображает их статус и тип:

- Включенные политики, разрешающие трафик, отображаются с зеленой галочкой или с зеленой полоской и галочкой в Large Icons.

- Включенные политики, которые блокируют трафик, отображаются с красным крестиком или красной полосой (Large Icons).

- Отключенные политики отображаются с черным кругом с линией, или с серой полосой (Large Icons)

- Иконка, которая содержит символ щита, это политика прокси.

Имена политик отображаются в зависимости от их типа:

- Управляемые политики – серый цвет с белым фоном

- BOVPN политики (например BOVPN-allow.out) – зеленый цвет с белым фоном

- Смешанные BOVPN политики и политики брандмауэра (например Ping или Any-PPTP) – голубой цвет с белым фоном.

- Все остальные политики – черный цвет с белым фоном

Для более подробной информации об изменении цвета см. “Смена цвета текста в Policy Manager”

Для более подробной информации о поиске политик в Policy Manager см. “Поиск политики по адресу, порту и протоколу”

Запуск Policy Manager

Для того чтобы запустить Policy Manager в окне WatchGuard System Manager выполните следующее:

- Выберите Firebox для которого вы хотите открыть Policy Manager и нажмите .

  или

- Выберите Tools > Policy Manager.

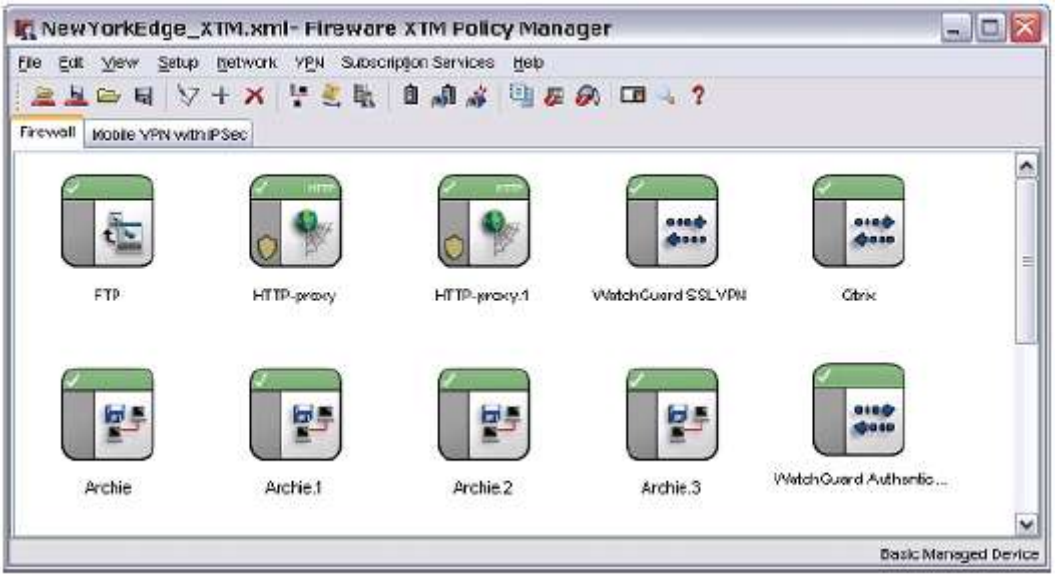
Если выбранный вами Firebox является управляемым устройством, то Policy Manager блокирует устройство в WatchGuard System Manager для того чтобы избежать одновременных изменений его конфигурации в WatchGuard System Manager. Блокировка снимается когда вы закрываете Policy Manager или вы открываете Policy Manager для другого устройства.

Изменение типа отображения политик в Policy Manager

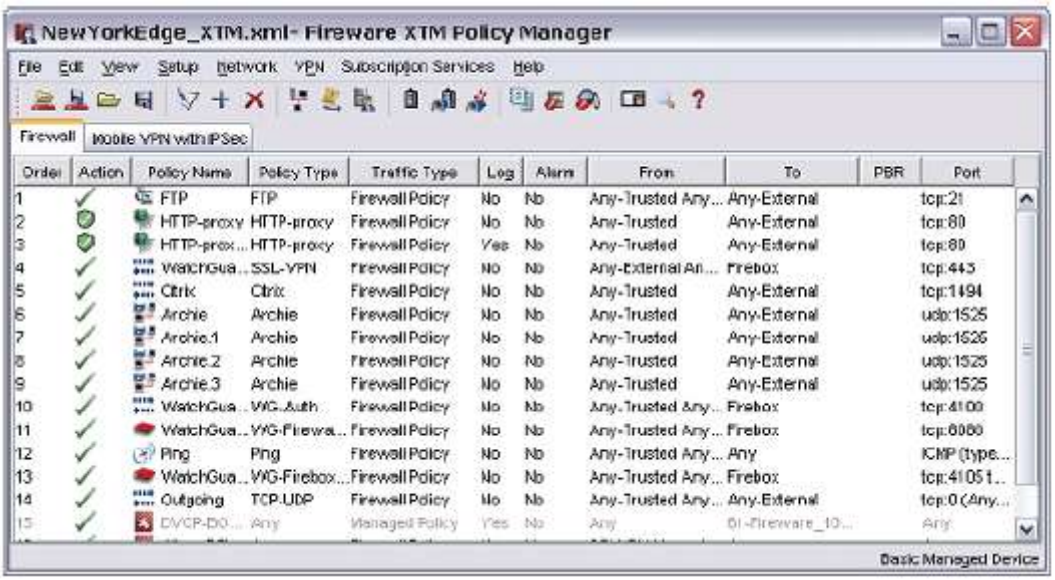
Policy Manager имеет два типа отображения политик: Large Icons и Details.

Политики в используемом по умолчанию Large Icons отображаются в виде иконок. В Details – в виде строк с информацией, разделенной колонками. Здесь вы можете посмотреть различную информацию, начиная с IP-адресов источника и назначения, заканчивая параметрами журнала и уведомления.

Для того чтобы переключиться на вид Details выберите **View > Details**.



Вид Large Icons



Вид Details

Для каждой политики отображается следующая информация:

Order

Порядок, в котором политики обрабатывают проходящий трафик. Policy Manager автоматически сортирует политики от самой специализированной до самой общей. Если вы хотите переключиться на ручной режим сортировки, выберите **View > Auto-order mode**

Затем выберите политику, положение которой вы хотите изменить и перетащите ее в новое положение. Для более подробной информации о порядке расположения политик см. “Порядок следования политик”

Action

Действие, которое применяет политика к трафику, который ее соответствует. Символ в этом поле также определяет, является ли политика пакетным фильтром или прокси.

- Зеленая галочка = пакетный фильтр и трафик разрешен.
- Красный крестик (X) = пакетный фильтр и трафик заблокирован.
- Круг с линией = политика пакетного фильтра и действие для трафика не определено. Зеленый щит с галочкой = политика прокси и трафик разрешен.Красный щит с символом X = политика прокси и трафик запрещен. Серый щит = политика прокси и действие для трафика не определено.

Policy Name

Имя политики (поле **Name** в диалоговом окне **New/Edit Policy Properties**. Для более подробной информации см. “Добавление политики из списка шаблонов”.

Policy Type

Протокол, которым управляет политика. В политиках прокси пишется название протокола плюс "-proxy".

Traffic Type

Тип трафика, который проверяется политикой: брандмауэр или VPN.

Log

Включено или нет ведение журнала для политики.

Alarm

Настроены ли для политики тревоги.

From

Адреса, трафик с которых обрабатывается данной политикой (адреса источников).

To

Адреса, трафик для которых обрабатывается данной политикой (адреса назначения).

PBR

Флаг использования в политике маршрутизации на базе политик. Если в политике используется такая маршрутизация и переключение отключено, то здесь отображается номер интерфейса. Если маршрутизация на базе политик и переключение включены, то здесь отображается список интерфейсов. Для более подробной информации о маршрутизации на базе политик см. “Настройка маршрутизации на базе политик”

Port

Порты и протоколы, используемые политикой.

Смена цвета текста в Policy Manager

По умолчанию цвета имен политик в Policy Manager зависят от типа трафика:

- Управляемые политики – серый цвет на белом фоне
- Политики BOVPN (например BOVPN-allow.out) – зеленый цвет на белом фоне.
- Mixed BOVPN политики и политики межсетевого экрана (например Ping или Any-PPTP) – синим цветом на белом фоне.
- Все остальные политики – черным цветом на белом фоне.

Вы можете использовать цвета по умолчанию или выбрать свои цвета. Вы также можете отключить выделение политик цветом.

1. Выберите **View** > **Policy Highlighting**.
   Откроется диалогое окно Policy Highlighting

2. Для того чтобы включить выделение политики цветом, включите опцию **Highlight Firewall policies based on traffic type**.

3. Для того чтобы изменить цвет текста или фона для имен обычных, управляемых, BOVPN или смешанных политик, нажмите кнопки **Text Color** или **Background Color**.
   Откроется диалоговое окно Select Text Color или Select Background Color

4. При помощи трех закладок **Swatches**, **HSB** или **RGB** выберите необходимый вам цвет:

   * **Swatches** — выберите один из образцов цветов.

   * **HSB** — Выберите переключатель **H** (тон), **S** (насыщенность), или **B** (яркость) и при помощи слайдера или в соответствующем текстовом поле настройте параметры цвета.

   * **RGB** — При помощи ползунков **Red**, **Green** или **Blue** настройте необходимый цвет. После того как вы выберете цвет, пример отображения появится в блоке **Sample** в нижней части диалогового окна. После того, как вы закончите нажмите **OK**.

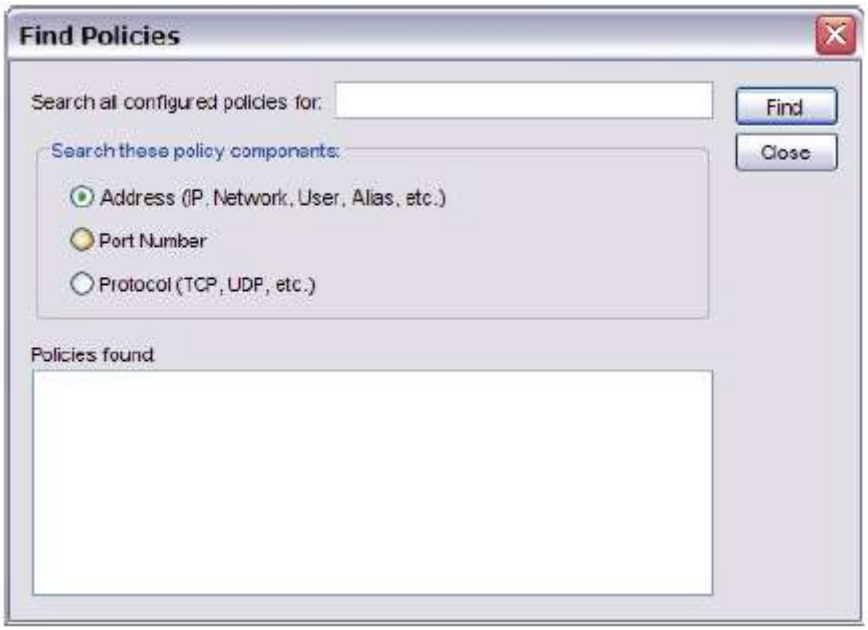
5. После того, как вы закончите, нажмите **OK**.

6. Нажмите **OK** в диалоговом окне **Policy Highlighting** для того чтобы изменения вступили в силу.

Поиск политики по адресу, порту и протоколу

Вы можете искать необходимые политики в Policy Manager в адресу, порту или протоколу.

1. Выберите **Edit > Find**.
   Откроется диалоговое окно Find Policies



2. При помощи переключателей **Address**, **Port Number** или **Protocol** выберите компонент, по которому будет осуществляться поиск.

3. Рядом с **Search all configured policies for** введите строку поиска. Для поисков по адресу и протоколу утилита Policy Manager выполняет поиск частей строки поиска. Вы можете ввести только часть строки и утилита Policy Manager выведет вам политики, которые содержат эту строку.

4. Нажмите **Find**.
   Policy Manager в поле Policies Found выведет политики, которые удовлетворяют вашим условиям поиска

5. Для того чтобы редактировать политику из полученного списка, просто два раза нажмите на нее

Добавление политик в вашу конфигурацию

Для того чтобы добавить политику вы выбираете шаблоны политик из списка. Шаблон политики содержит имя политики, краткое описание политики и порт/протоколы, используемые политикой

- Для того чтобы посмотреть список шаблонов см. “Просмотр списка шаблонов”

- Для того чтобы добавить политику из списка в вашу конфигурацию см. “Добавление политики из списка шаблонов”

- Для того чтобы посмотреть или редактировать шаблон политики см. “Параметры шаблона политики и их изменение”

- Если вы работаете с несколькими Firebox и у вас есть политики для них, вы можете использовать функцию импорта/экспорта для копирования политик с одного Firebox на другой. Для более подробной информации см. “Импорт или экспорт шаблонов политик пользователя”

Для каждой политики Firebox содержит набор настроек, который подходит для большинства конфигураций. Если вы хотите настроить политику специально для вашей конфигурации или если вы хотите добавить к политикам дополнительный функционал (Traffic Management или расписания запусков) вы можете изменять эти параметры.

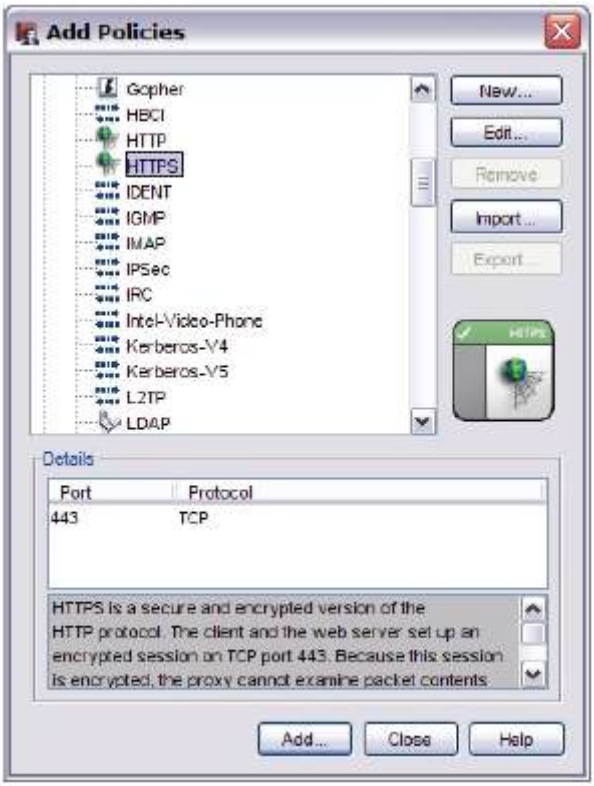
После того, как вы добавите политику, вам необходимо выполнить следующее:

- Настроить разрешенные источники и места назначения сетевого трафика
- Создать правила фильтрации
- Включить или выключить политику
- Настроить дополнительный функционал: Traffic Management, NAT и ведение журнала

Просмотр списка шаблонов

1. Нажмите  . Или выберите Edit > Add Policies.
   Откроется диалоговое окно Add Policies.

2. Нажмите на (+) слева от названия каталога **Packet Filters** или **Proxies**.
   Откроется список шаблонов для пакетных фильтров или прокси



3. Нажмите на шаблон для того чтобы посмотреть общую информацию. Иконка политики появится в правой части окна, а общая информация о шаблоне – в секции **Details**.

Добавление политики из списка шаблонов

Для каждой политики Firebox содержит набор настроек, который подходит для большинства конфигураций. Если вы хотите настроить политику специально для вашей конфигурации или если вы хотите добавить к политикам дополнительный функционал (QoS действия и расписания запусков) вы можете эти параметры изменить.

1. В диалоговом окне **Add Policies** откройте элементы **Packet Filters**, **Proxies** или **Custom**
   Откроется список шаблонов для пакетных фильтров или прокси.

2. Выберите тип политики, которую вы хотите создать. Нажмите **Add**.
   Откроется диалоговое окно New Policy Properties

3. В поле **Name** введите имя политики.

4. Настройте правила доступа и другие параметры политики.

5. Нажмите **OK** для того чтобы закрыть диалоговое окно **Properties**.
   В диалоговом окне Policies вы можете добавить еще несколько политик.

6. Нажмите **Close**.
   Новая политика появится в Policy Manager.

Для более подробной информации см. “Параметры политики”

Добавление нескольких политик одного типа

Если ваша политика безопасности требует этого, то вы можете добавить несколько политики одного типа. Например, вы можете установить ограничение на web-доступ для большинства

пользователей, и одновременно предоставляете полный Web-доступ вашему управлению. Для этого вы создаете две политики с разными параметрами:

1. Добавьте первую политику.

2. Измените имя политики на имя, которая совпадает с вашей политикой безопасности и добавьте необходимую информацию.
   В этом примере вы можете назвать первую политику restricted_web_access.

3. Нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

4. Создайте вторую политику.

5. Нажмите **OK**.
   Откроется диалоговое окно New Policy Properties для этой политики.

Для более подробной информации см. “Параметры политики”

Параметры шаблона политики и их изменение

Информация о шаблоне политики отображается в секции Details диалогового окна **Add Policies**. Если вы хотите более подробную информацию о шаблоне политики, вы можете открыть его в отдельном окне для редактирования. Существует два типа шаблонов политики: предварительно созданные и пользовательские.

Для предварительно созданных политик (в списках Packet Filters и Proxies в диалоговом окне **Add Policies**), вы можете изменять только поле **Description (описание)**. В отличие от пользовательских политик, вы не можете изменять или удалять предварительно созданные политики. Для более подробной информации о пользовательских политиках About custom policies.

Для того чтобы посмотреть информацию о шаблоне политики выполните следующее:

1. В диалоговом окне **Add Policies** выберите шаблон политики.

2. Нажмите **Edit**.

Отключение или удаление политики

Отключить политику в Policy Manager вы можете двумя способами: в закладках **Firewall** или **Mobile VPN with IPSec,** или в диалоговом окне **Edit Policy Properties**.

Для того чтобы отключить политику в закладках **Firewall** или **Mobile VPN with IPSec** выполните следующее:

1. Выберите закладку **Firewall** или **Mobile VPN with IPSec**.

2. Нажмите правой кнопкой на политику и выберите **Disable Policy**.
   Пункт меню изменится на Enable Policy.

Для того чтобы отключить политику в диалоговом окне **Edit Policy Properties** выполните следующее:

1. Два раза нажмите на политику, которую вы хотите отключить.
   Откроется диалоговое окно Edit Policy Properties.

2. Отключите опцию **Enable**.

3. Нажмите **OK**.

Удаление политики

Если ваша политика безопасности изменилась, то иногда вам приходится удалять одну или несколько политик. Для того чтобы удалить политику, сначала ее необходимо удалить в Policy Manager. Затем вы сохраняете новую конфигурацию в Firebox.

1. Выберите политику, которую вы хотите удалить.

2. Нажмите на иконку **Delete**. Или выберите **Edit** > **Delete Policy**.
   Откроется диалоговое окно подтверждения удаления.

3. Нажмите **Yes**.

4. Для того чтобы сохранить конфигурацию выберите **File > Save > To Firebox**.

5. Введите пароль конфигурации и включите опцию **Save to Firebox**.

6. Нажмите **Save**.

7. Перезагрузите Firebox.

Порядок следования политик

Порядок следования политик – это порядок, в котором Firebox проверяет трафик и применяет правила политик. Firebox автоматически сортирует политики от самой подробной до самой общей. Он сравнивает информацию, извлеченную из пакета, со списком правил первой политики в списке. Правило, которое совпадает с информацией, полученной из пакета, применяется к этому пакету. Если совпадения обнаружены в двух политиках, то политика прокси имеет более высокий приоритет.

Автоматическая сортировка политик

Firebox автоматически присваивает наиболее подробной политике самый высокий приоритет. Приоритеты политики определяются на основе списка критериев. Если Firebox не может определить приоритет политики по первому критерию, то он переходит к следующему критерию, и т.д

Ниже приводится список этих критериев

1. Специфичность политики
2. Протоколы политики.
3. Правила для трафика поля **To**.
4. Правила для трафика поля **From**.
5. Действие брандмауэра (Allowed, Denied или Denied (send reset)).
6. Расписания для политик.
7. Буквенно-цифровая последовательность на базе типа политики.
8. Буквенно-цифровая последовательность на базе имени политики.

В следующих разделах приводится описание, каким образом Firebox определяет приоритет политики по вышеперечисленным критериям.

Специфичность политики и протоколы

Firebox использует эти критерии для сравнения двух политик.

1. Политика Any всегда имеет самый низкий приоритет
2. Проверка количества протоколов TCP 0 (any) или UDP 0 (any). Политика с меньшим количеством протоколов имеет более высокий приоритет.
3. Проверка количества уникальных портов для протоколов TCP и UDP. Политика с меньшим количеством портов имеет более высокий приоритет.
4. Проверка уникальных TCP и UDP портов. Политика с меньшим количеством портов будет иметь более высокий приоритет.
5. Подсчет результата на базе значений их IP протоколов. Политика с меньшим результатом имеет более высокий приоритет. Если Firebox на базе этих критериев не может определить приоритеты политик, то он проверяет правила для трафика

Правила для трафика (Traffic rules)

Firebox использует этот критерий для сравнения правил для трафика одной политики с правилами для трафика другой политики. Политика с наиболее детальными правилами имеет более высокий приоритет.

1. Адрес хоста
2. Диапазон IP адресов (меньше, чем сравниваемая подсеть)
3. Подсеть
4. Диапазон IP адресов (больше, чем сравниваемая подсеть)
5. Имя пользователя
6. Группа аутентификации
7. Интерфейс, Firebox
8. Any-External, Any-Trusted, Any-Optional

9. Any

Например, сравним эти две политики:

(HTTP-1) From: Trusted, user1

(HTTP-2) From: 10.0.0.1, Any-Trusted

Trusted – это наиболее общий элемент для HTTP-1. *Any-Trusted* – это наиболее общий элемент для HTTP-2. Так как *Trusted* находится в псевдониме *Any-Trusted*, HTTP-1 является более детализированным правилом для трафика.

Если Firebox по правилам для трафика не может определить приоритет, то он сравнивает политики по следующему критерию – действиям брандмауэра.

Действия брандмауэра (Firewall actions)

На базе этого критерия Firebox сравнивает политики для определения приоритета. Список действий брандмауэра по приоритетам, начиная с самого высокого, выглядит так:

1. Denied или Denied (send reset)
2. Политика прокси Allowed
3. Пакетный фильтр Allowed

Если устройство на основе этих критериев не может определить приоритет, то он сравнивает политики на базе следующего критерия - расписания.

Расписания (Schedules)

Если на основе предыдущего критерия определить приоритет политик не удалось, то устройство Firebox сравнивает политики по расписаниям. Список расписаний работы политики по приоритетам, начиная с самого высокого, выглядит так:

1. Always off (Всегда выключена)
2. Sometimes on (Иногда включена)
3. Always on (Всегда включена)

Если Firebox на основе этих критериев не может определить приоритет, то он сравнивает политики на базе следующего критерия – тип и имя политики.

Типы и имена политик (Policy types and names)

Если на основе предыдущего критерия определить приоритет политик не удалось, то устройство Firebox сравнивает политики по их типам и именам. Сначала сравниваются типы политик, затем их имена. Так как не существует политик одинакового типа с одинаковыми именами, то по этому критерию Firebox окончательно определяет приоритет политик.

Настройка порядка следования политик вручную

Для того чтобы переключиться на ручной режим и изменить порядок следования политик выполните следующее:

1. Выберите **View** > **Auto**-**Order Mode**. Галочка исчезнет и появится сообщение подтверждения.

2. Нажмите **Yes** если вы хотите на ручной режим. При переключении на ручной режим, Policy Manager меняет тип отображения политик на Details. В Large Icons вы не можете изменять порядок следования политик.

3. Для того чтобы изменить порядок следования, выберите любую политики и перетащите в нужное место в списке.

Созданий расписаний для действий Firebox

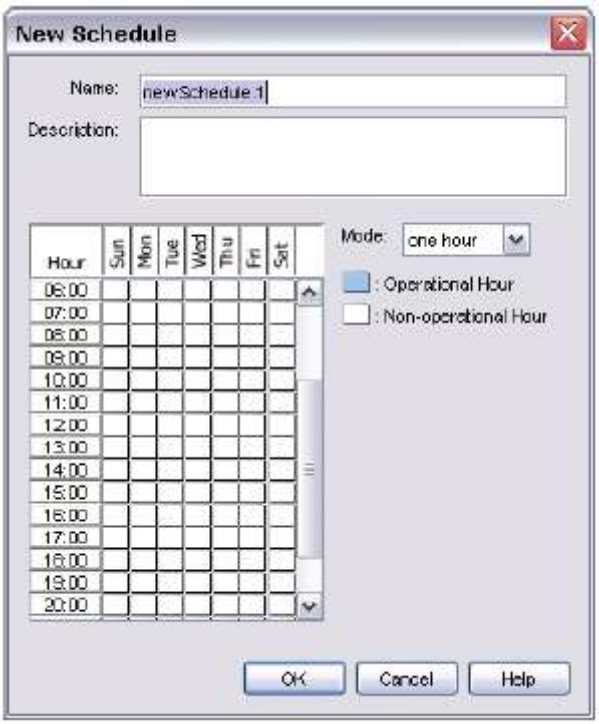
Расписание действий определяет дату и время, когда определенная функция будет выключена или включена. Если вы хотите, чтобы политика или действие WebBlocker автоматически включались или выключались в указанное время, вам необходимо создать для них расписание. Вы также можете создать расписание для нескольких действий или политик.

Например, организация хочет заблокировать определенные виды трафика в рабочее время. Администратор может создать расписание, которое будет активно в рабочие дни, и добавить в него политики, которые будут использоваться для блокировки трафика.

Для того чтобы создать расписание выполните следующее:

1. Выберите **Setup** > **Actions** > **Schedules**.
Откроется диалоговое окно Schedules

2. Для того чтобы редактировать расписание, в диалоговом окне **Schedule** выберите необходимое вам расписание и нажмите **Edit**. Для того чтобы создать новое расписание на основе уже существующего расписания выберите существующее расписание и нажмите **Clone**. Для того чтобы создать новое расписание нажмите **Add**.
Откроется диалоговое окно New Schedule



3. Введите имя расписания и его описание.
Для расписания введите имя, которое будет легко запомнить.Созданное расписание появится в диалоговом окне Schedules.

4. В выпадающем списке **Mode** введите величину инкремента времени для данного расписания: 1 час, 30 или 15 минут.
График в левой части окна New Schedule показывает выбранное значение в выпадающем списке

5. Диаграмма в диалоговом окне по горизонтальной оси показывает дни, а по вертикальной оси – часы и минуты в течение дня. Нажмите на соответствующие блоки, для того чтобы выбрать рабочие (политика активна) и нерабочие часы (политика неактивна)

6. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Schedule**.

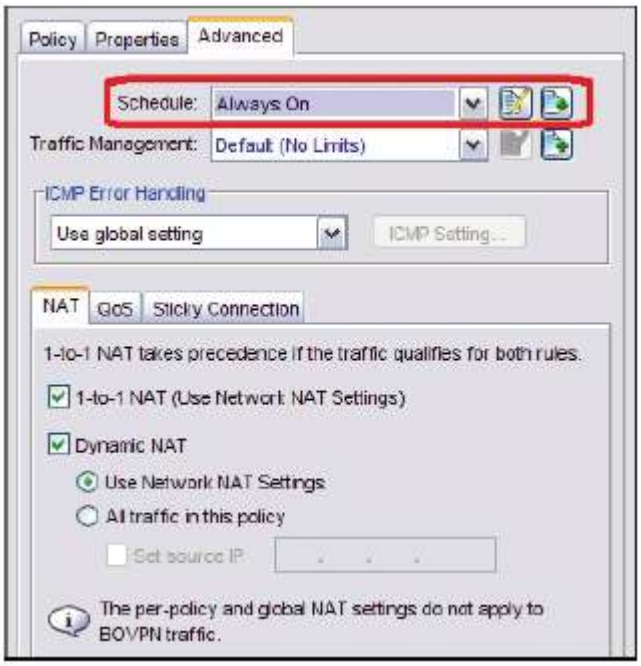
7. Нажмите **Close** для того чтобы закрыть диалоговое окно **Schedules**.

Настройка рабочего расписания

Вы можете создать рабочее расписание для политики, которое будет определять, в какое время политика будет включена. Вы можете рабочие расписания для нескольких политик одновременно.

Для того чтобы изменить расписание для политики выполните следующее:

1. Выберите любую политику и нажмите на нее два раза.
   Откроется диалоговое окно Edit Policy Properties



2. Выберите закладку **Advanced**.

3. В выпадающем списке **Schedule** выберите одно из расписаний. Или нажмите на соответствующую иконку для того чтобы создать ваше расписание.

4. Нажмите **OK**.

Пользовательские политики

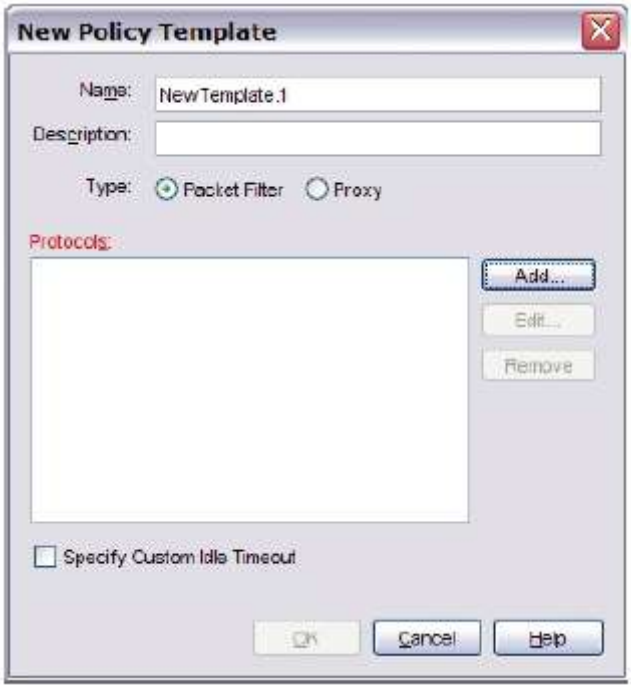
Если протокол не включен в конфигурацию по умолчанию, то вам необходимо создать политику пользователя для того чтобы разрешить передачу трафика по этому протоколу. Вы можете добавить политики пользователя, которые используют:

- TCP порты
- UDP порты
- IP протокол, который не является TCP или UDP. Например GRE, AH, ESP, ICMP, IGMP и OSPF. Для идентификации таких протокол использует номер протокола. Для того чтобы начать процедуру создания политики пользователя вам необходимо сначала создать ее шаблон.

Для более подробной информации см. “Создание или редактирование шаблона политики пользователя”. Или вы можете использовать существующий шаблон. Для добавления политики пользователя используется та же самая процедура, описание которой см. в “Добавление политики из списка шаблонов”

Создание или редактирование шаблона политики пользователя

1. Нажмите  . Или выберите **Edit > Add Policies**.
   Откроется диалоговое окно Add Policies.
   Нажмите **New** или выберите один из шаблонов политик и нажмите **Edit**.
   Откроется диалоговое окно New Policy Template



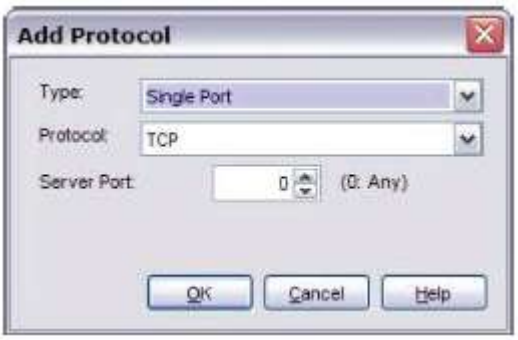
2. В поле **Name** введите имя политики. Имя будет отображаться в Policy Manager в качестве типа политики. Уникальное имя значительно облегчает процедуру поиска политики. Это имя не должно совпадать ни с одним именем в списке в диалоговом окне **Add Policy**.

3. В поле **Description** введите описание политики. Описание появляется в секции Details когда вы нажмете на имя политики в списке User Filters.

4. Выберите тип политики: **Packet Filter** или **Proxy**.

5. Если вы выберете Proxy, выберите протокол прокси из выпадающего списка.

6. Для того чтобы добавить протоколы для этой политики нажмите **Add**.
   Откроется диалоговое окно Add Protocol



7. В выпадающем списке **Type** выберите **Single Port** или **Port Range**.

8. В выпадающем списке **Protocol** выберите протокол для политики. Если выберете **Single Port** вы можете выбрать **TCP**, **UDP**, **GRE**, **AH**, **ESP**, **ICMP**, **IGMP**, **OSP**, **IP**, или **Any**. Если вы

выберете **Port Range** вы можете выбрать **TCP** или **UDP**. Список опций под выпадающим списком меняется в зависимости от выбранного протокола.

Fireware XTM блокирует IGMP multicast трафик через Firebox или между интерфейсами Firebox. Этот трафик разрешен только между интерфейсом и Firebox.

9. В выпадающем списке **Server Port** выберите порт для данной политики. Если вы выбрали **Port Range**, выберите начальный и конечный номер порта.

10. Нажмите **OK**.
Шаблон политики будет добавлен в каталог Custom policies.

Теперь вы можете при помощи этого шаблона создавать пользовательские политики. Для создания используйте ту же самую процедуру, что и для предопределенных политик

Импорт или экспорт шаблонов политик пользователя

Если вы работаете с несколькими Fireboxes и для них используете политики пользователя, то вы можете для того чтобы сэкономить время использовать процедуру экспорта/импорта. Вы можете создать шаблон политики на одном Firebox, экспортировать его в ASCII файл и затем импортировать его на другой Firebox.

На устройствах Firebox, где вы создали политики, должно быть установлена такая же версия WSM, что используется для импорта политик. Вы не можете импортировать шаблон с одной версии на другую версию.

1. На первом Firebox создайте необходимые шаблоны политик

2. Нажмите **Export**. Вам нет необходимости выбирать политики пользователя. Функция экспорта автоматически экспортирует все политики пользователя.

3. В диалоговом окне **Save** выберите куда вы хотите сохранить файл с шаблонами политик. Введите имя файла и нажмите **Save**. *По умолчанию используется каталог My Documents > My WatchGuard.*

4. В Policy Manager на другом Firebox в диалоговом окне **Add Policies** нажмите **Import**.

5. Найдите файл, который вы создали в п. 3 и нажмите **Open**.

6. Если такие шаблоны политик пользователя уже существуют, система спросит вас необходимо заменить ли существующие шаблоны или применить новые шаблоны к существующим. Нажмите **Replace** или **Append**. Если вы нажмете **Replace**, существующие шаблоны будут удалены и заменены новыми. Если вы нажмете **Append**, то новые шаблоны просто добавятся к существующим

Параметры политики

Каждая политика содержит набор параметров по умолчанию, которые могут быть использованы для большинства конфигураций. Однако при необходимости вы можете изменить эти параметры.

Политики Mobile VPN создаются и работают также, как и политики брандмаэура. Однако вам необходимо указать группу Mobile VPN, к которой эта политика применяется.

Для того чтобы настроить параметры политики два раза нажмите на имя политики или на ее иконку.

Закладка Policy

Здесь вы можете настроить базовые параметры политики: блокировать или разрешить трафик, список устройств, которыми она управляет. Также в этой закладке вы можете создать правила

доступа или настроить маршрутизацию на базе политик, статическую NAT или балансировку нагрузки.

Закладка Properties

В этой закладке вы можете посмотреть порт и протокол, к которым применяется политика, а также описание политики. Здесь вы можете настроить параметры ведения журнала для политики, уведомлений, автоматической блокировки и величины таймаутов. Вы также можете настроить действия прокси и ALG.

Закладка Advanced

Эта закладка содержит настройки NAT и Traffic Management (QoS), а также multi-WAN и ICMP опции. Здесь вы также можете настроить рабочее расписание для политики и применить Traffic Management действия.

Параметры прокси

Политики прокси имеют набор правил по умолчанию, которые обеспечивают хороший уровень безопасности и доступа для большинства конфигураций. Если эти наборы правил не удовлетворяют требованиям вашей системы безопасности вы можете создать новые правила, а также удалять и редактировать существующие. Для того чтобы изменить параметры и правила для действия прокси нажмите на иконку **View/Edit Proxy**  (первая иконка справа от выпадающего списка **Proxy action**) и в левой части диалогового окна выберите набор параметров.

Настройка правил доступа для политики

При помощи закладки **Policy** вы можете настроить правила доступа для данной политики.

Поле **Connections are** определяет будет ли трафик, который совпадает с правилами, разрешен или запрещен. При помощи этих параметров вы можете настроить процедуру обработки трафика:

Allowed

Firebox разрешает трафик, который использует эту политику, если он соответствует установленным правилам политики. Вы также можете настроить генерацию сообщения журнала в случае, если трафик был обработан политикой.

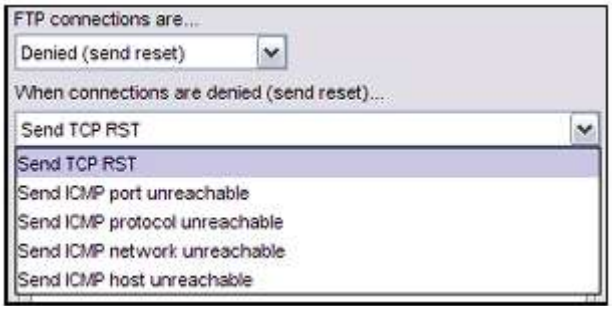
Denied

Firebox запрещает весь трафик, который использует эту политику. Вы можете создавать запись в журнале при попытке компьютера использовать эту политику. Вы также можете настроить автоматическое добавление компьютера, который пытался начать соединение с этой политикой, в список Blocked Sites (см. “Временная блокировка сайтов при помощи политики”).

Denied (send reset)

Firebox запрещает весь трафик, который использует эту политику. Вы также можете настроить автоматическое добавление компьютера, который пытался начать соединение с этой политикой, в список Blocked Sites (см. закладку **Properties**). Firebox также отправляет клиенту RST-пакет для того чтобы сообщить ему что сеанс закрыт или был отклонен.

Вы также можете настроить политику, чтобы она возвращала компьютеру сообщение о том, какие порт, протокол, сеть или хост недоступны. Мы рекомендуем использовать эту опцию только если вы уверены, что ваша сеть корректно работает с остальными сетями



Закладка **Policy** также содержит:

- Список **From** (или **Source**), который определяет кто может передавать (или не передавать) трафик с этой политикой.

- Список **To** (или **Destination**), который определяет кому устройство Firebox будет маршрутизировать трафик, если он совпадает (или не совпадает) со спецификациями политики.

Например, вы можете настроить пакетный ping-фильтр, который будет разрешать трафик от всех компьютеров внешней сети к одному web-серверу в вашей дополнительной сети.

Однако необходимо помнить, что сеть назначения становится уязвимой, если вы откроете порты или порты, которыми управляет политика, для подключений. Будьте аккуратны при настройке ваших политик.

Добавление участников в политику

1. Для того чтобы добавить участника политики, нажмите **Add** для списков **From** или **To**. *Откроется диалоговое окно Add Address*

2. Список **Available Members** содержит псевдонимы, которые вы можете добавить в списки **From** или **To**.

3. Выберите псевдоним и нажмите **Add**, или два раза нажмите на псевдоним. Если вы хотите добавить хосты, пользователей, псевдонимы или туннели к политике, которых нет в списке **Available Members**, см. “Добавление новых участников в политику”

4. Повторите предыдущие пункты для того чтобы добавить еще несколько участников.

5. Нажмите **OK**.

Источник и место назначения могут быть IP адресом хоста, диапазоном хоста, именем хоста, сетевым адресом, именем пользователя, псевдонимом, VPN туннелем или любая комбинация этих объектов. Для более подробной информации о псевдонимах в списках **From** и **To** см. “Псевдонимы”

Для более подробной информации о создании псевдонимов см. “Создание псевдонима”

Добавление новых участников в политику

Если вы хотите добавить хосты, псевдонимы или туннели в список **Available Members** выполните следующий:

1. Нажмите **Add Other**.
   Откроется диалоговое окно Add Member

2. В выпадающем списке **Choose Type** выберите диапазон хостов, IP адрес хоста или IP адрес сети.

3. В поле **Value** введите адрес сети, диапазон или IP адрес

4. Нажмите **OK**.
   Новый участник появится в списке Selected Members and Addresses.

Для того чтобы добавить пользователя или группу в список **Available Members**:

1. Нажмите **Add User**. *Откроется диалоговое окно Add Authorized Users or Groups.*

2. Выберите тип пользователя или группы, сервер аутентификации и кого вы хотите добавить, пользователя или группу

3. Нажмите **Select**.

Если пользователь или группа не появляется в списке, значит они еще не созданы как авторизованные пользователь или группа. Для того чтобы создать новых авторизованных пользователя или группу см. “Использование в политиках пользователей и групп”

Настройка маршрутизации на базе политик

Для передачи трафика по сети маршрутизатор обычно проверяет адрес назначения и в таблице маршрутизации ищет адрес следующего маршрутизатора. В некоторых случаях вы захотите отправлять трафик по другому маршруту, нежели по маршруту по умолчанию, указанному в таблице маршрутизации. Вы можете настроить политику со специальным внешним интерфейсов, который будет использоваться для всего исходящего трафика, который совпадает с этой политикой. Эта процедура известна маршрутизация на базе политик.

Маршрутизация на базе политики имеет более высокий приоритет по сравнению с другими параметрами multi-WAN.

Вы можете использовать маршрутизацию на базе политик если у вас несколько External интерфейсов и ваш Firebox использует multi-WAN. При использовании маршрутизации на базе политик, вы может быть уверены, что весь трафик, обрабатываемый политикой, будет идти через один и тот же интерфейс, даже если в вашей multi-WAN конфигурации данные передаются через интерфейсы в режиме round-robin. Например, если вы хотите, чтобы трафик электронной почты передавался по одному интерфейсу, то вы можете в политике SMTP или POP3 прокси использовать маршрутизацию на базе политик для маршрутизации трафика электронной почты через указанный интерфейс.

Маршрутизация на базе политик, переключение и обратное переключение

Если вы используете маршрутизацию на базе политик с multi-WAN переключением, то вы можете указать, по какому External интерфейсу будет передаваться трафик, соответствующий данной политике, в случае переключения. По умолчанию до того, как интерфейс снова не заработает, трафик блокируется.

Параметры обратного переключения (закладка **Multi-WAN** диалогового окна **Network Configuration**) также применяются к маршрутизации на базе политик. Если происходит переключение, и затем интерфейс, вышедший из строя, снова становится активным, Firebox может для текущих подключений использовать активный в данный момент интерфейс, или переключить их обратно на интерфейс, который снова стал активным. Новые соединения уже идут через интерфейс, вновь ставший активным.

Ограничения маршрутизации на базе политик

- Маршрутизация на базе политик доступна только тогда, когда включена опция multi-WAN. Если вы включите опцию multi-WAN, диалоговое окно **Edit Policy Properties** автоматически добавит поля для настройки маршрутизации на базе политик.

- По умолчанию эта маршрутизация отключена

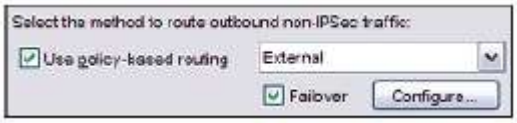
- Маршрутизация на базе политик не применяется к IPSec трафику или к трафику, который передается в доверенную или Optional сети (входящий трафик).

Для использования маршрутизации маршрутизации на базе политик, вам необходим Fireware XTM с обновлением Pro. Вам также необходимо настроить хотя бы два External интерфейса

Добавление маршрутизации на базе политик в политику

1. Откройте Policy Manager.

2. Выберите политику и нажмите  . Или два раза нажмите на политику.
   Откроется диалоговое окно Edit Policy Properties.



3. Включите опцию **Use policy-based routing**.

4. В выпадающем списке выберите интерфейс, который будет использовать для исходящего трафика, который соответствует политике. Этот интерфейс должен быть членом псевдонима или сети, которые вы ввели в поле **To** во время настройки политики.

5. (Дополнительно) Настройте маршрутизацию на базе политик с multi-WAN переключением, как описано ниже. Если вы не выберете **Failover** и интерфейс, который вы выбрали для этой политики, выйдет из строя, то трафик будет заблокирован до того момента, пока интерфейс снова не заработает.

6. Нажмите **OK**.

Маршрутизация на базе политик с переключением

Вы можете сделать интерфейс, который вы выбрали для политики, основным. В то же время создать резервные интерфейсы для всего не-IPSec трафика.

1. В диалоговом окне **Edit Policy Properties** выберите **Failover**.

2. Нажмите **Configure** и укажите резервные интерфейсы для этой политики. Если основной интерфейс для этой политик не активен, трафик передается через резервные интерфейсы. *Откроется диалоговое окно Policy Failover Configuration*

3. В колонке **Include** отметьте флаг для каждого интерфейса, который вы хотите использовать в конфигурации failover. При помощи кнопок **Move Up** и **Move Down** настройте порядок следования интерфейсов. Первый интерфейс в списке – это основной интерфейс

4. Нажмите **OK** для того чтобы закрыть диалоговое окно **Policy Failover Configuration**

5. Нажмите **OK** для того чтобы закрыть диалоговое окно **Edit Policy Properties**

6. Сохраните конфигурационный файл

Настройка таймаута ожидания

Таймаут ожидания (Idle timeout) - это промежуток времени, в течение которого неактивный пользователь может оставаться аутентифицированным (пользователь не передает трафик). По умолчанию Firebox закрывает соединение через 300 секунд (6 минут). Если вы включите таймаут ожидания для вашей политики, то Firebox будет закрывать соединение по истечении указанного вами промежутка времени.

1. В диалоговом окне **Policy Properties** выберите закладку **Properties**.

2. Включите опцию **Specify Custom Idle Timeout**

3. Введите величину таймаута в секундах

Настройка обработки ICMP ошибок

Для политики вы можете настроить параметры обработки ICMP-ошибок. Эти параметры будут использовать вместо глобальных параметров. Для того чтобы изменить параметры обработки ICMP ошибок для данной политики выполните следующее:

1. В выпадающем списке **ICMP Error Handling** выберите **Specify setting**.

2. Нажмите **ICMP Setting**.

3. В диалоговом окне **ICMP Error Handling Settings** выполните все необходимые настройки.

4. Нажмите **OK**.

Применение правил NAT

Вы можете в вашей политике использовать правила NAT:

1. В диалоговом окне **Edit Policy Properties** выберите закладку **Advanced**.

2. Выберите одну из опций, описание которых приведены ниже.

1-to-1 NAT

При использовании этого типа NAT Firebox использует диапазоны внутренних и публичных IP-адресов, как описано в разделе **Ошибка! Источник ссылки не найден.**

Динамическая NAT

При использовании этого типа NAT устройство WatchGuard создает соответствие между внутренними и публичными IP адресами. Динамическая NAT во всех политиках включена по умолчанию. Выберите **Use Network NAT Settings** если вы хотите использовать правила динамической NAT. Выберите **All traffic in this policy** если вы хотите применять NAT ко всему трафику, который соответствует этой политике.

В поле **Set Source IP** вы можете указать IP адрес источника динамической NAT для любой политики, использующей динамическую NAT. При этом весь трафик, который соответствует данной политике, будет в качестве IP адреса источника указывать адрес из вашего публичного или внешнего диапазона IP адресов.

Это делается для того чтобы, в случае, если IP-адрес интерфейса External не совпадает в IP-адресом вашей MX-записи, исходящий SMTP-трафик использовал адрес вашей MX-записи.

Правила 1-to-1 NAT имеют более высокий приоритет, по сравнению с правилами динамической NAT

Настройка длительности sticky соединения для политики

Параметры sticky-соединения для политики используются вместо глобальных параметров sticky-соединений. Для использования sticky-соединений вам необходимо включить multi-WAN.

1. В закладке **Advanced** диалогового окна **Policy Properties** выберите закладку **Sticky Connection**.

2. Не включайте опцию **Override Multi-WAN sticky connection setting** если вы хотите использовать параметры sticky-соединения, настроенные в закладке **Network > Configuration > Multi-WAN**.

3. Для того чтобы настроить параметры sticky соединений для этой политике включите опцию **Enable sticky connection**.

4. В поле **Enable sticky connection** введите количество минут, в течение которого sticky соединение будет активно

Глава 14 - Параметры прокси

Политики прокси и ALG

Политики безопасности WatchGuard (пакетные фильтры, прокси и прикладные шлюзы ALG (Application Layer Gateway)) являются важными инструментами для защиты. Пакетный фильтр проверяет IP и TCP/UDP заголовок каждого пакета, прокси выполняет мониторинг и сканирование всего соединения и ALG, вдобавок к функциональности прокси, обеспечивает прозрачное управление соединением. Политики прокси и ALG проверяют синтаксис и порядок команд, которые используются в соединении, а также используют углубленную проверку пакетов для проверки защищенности соединения.

Политика прокси или ALG последовательно открывают каждый пакет, удаляют заголовок сетевого уровня и проверяют полезную нагрузку пакета. Затем прокси снова добавляет заголовок сетевого уровня и отправляет пакет в место назначения, в то время как ALG восстанавливает исходный заголовок сетевого уровня и передает пакет. В результате прокси или ALG могут находить запрещенные или опасные данные в поле полезной нагрузки. Например, SMTP прокси проверяет все входящие SMTP пакеты (электронная почта) на предмет наличия запрещенного содержимого (исполняемые файлы или скрипты). Хакеры часто используют эти методы для заражения компьютера вирусами. Прокси или ALG могут заблокировать эти типы содержимого, в то время как пакетный фильтр не может обнаруживать такие типы содержимого в поле полезной нагрузки пакета.

Если вы приобрели и включили дополнительные сервисы (Gateway AntiVirus, Intrusion Prevention Service, spamBlocker, WebBlocker), прокси WatchGuard могут применять эти сервисы к трафику.

Настройка прокси

Подобно пакетным фильтрам, политики прокси включают в себя общие параметры управления трафиком, включая Traffic Management и расписания. Однако, политики прокси также включают параметры, характерные только для определенного протокола. Эти параметры настраиваются при помощи *правил*, или групп опций, которые соответствует определенному действию. Например, вы можете настроить правила для блокировки трафика от определенных пользователей или устройств, или разрешать VoIP (Voice over IP) трафик, который соответствует определенным кодекам. Если у вас есть прокси с определенным набором параметров, вы можете сохранить этот набор в вашем созданном прокси и использовать эти параметры с другими прокси.

Fireware XTM поддерживает политики прокси для многих протоколов, включая DNS, FTP, H.323, HTTP, HTTPS, POP3, SIP, SMTP, и TCP-UDP. Для более подробной информации о политике прокси см. раздел соответствующий этой политике.

Тревоги прокси и AV

Тревога – это событие, которое генерирует уведомление, которая представляет собой механизм уведомления администратора о наступлении определенного события в сети. В настройках прокси тревога может быть создана при совпадении трафика с одним из правил политики. Тревога может быть также создана в случае если значение поля **Actions to take** установлено равным не **Allow**.

Например, FTP прокси по умолчанию содержит правило, которое запрещает загрузку файлов со следующими расширениями: .cab, .com, .dll, .exe, and .zip. Вы также можете создавать тревогу в случае если Firebox выполняет действие **Deny**.

Для каждого прокси вы можете выбрать действие, которое Firebox будет выполнять при создании тревоги.

1. В секции **Categories** настроек прокси выберите **Proxy and AV Alarm**.

2. Вы можете настроить Firebox для отправки SNMP ловушки или уведомления администратору сети, или обе сразу. Уведомление может быть в виде электронного письма администратору сети или всплывающего окна на компьютере администратора

3. Если вы хотите изменить параметры одного или нескольких категорий прокси, см. соответствующий раздел далее в этой главе. После того, как вы закончите, нажмите **OK**. Вы не можете вносить изменения в предопределенные действия. Для того для того, чтобы сохранить изменения, сделанные в таких действиях, вам необходимо скопировать (клонировать) эти настройки в новое действие.

4. Введите имя для нового действия и нажмите **OK**.
Откроется диалогое окно New Policy Properties.

Правила и наборы правил

При настройке политики прокси или ALG (application layer gateway) вам необходимо создать новое правило или редактировать существующее правило. Правила – это набор критериев, с которыми прокси сравнивает анализируемый трафик. Правило состоит из типа содержимого, шаблона или выражения и действия, которое выполняет устройство Firebox в случае совпадения трафика с типом содержимого, шаблоном или выражением. Правила также содержат настройки создания тревог и генерации сообщений журнала устройством Firebox. Набор правил (ruleset) – это группа правил на базе одного компонента прокси (тип содержимого, имени файла или электронного вложения).

Для каждого прокси Firebox содержит набор правил по умолчанию.

Отдельные наборы правил используются для защиты пользователей, подключенных к Trusted сети и публичных серверов. Для этих правил вы можете использовать конфигурацию по умолчанию, или настроить необходимые параметры для соответствия вашим требованиям.

Работа с правилами и наборами правил

При настройке прокси в списке **Categories** вы можете посмотреть наборы правил для этого прокси. Эти наборы изменятся если вы измените действие прокси (закладка **Properties** в окне конфигурации прокси).

Например, правила для действия FTP-Client могут иметь параметры отличные от параметров правил действия FTP-Server. WatchGuard прокси содержат предустановленный набор правил, которые обеспечивают хороший уровень уровень защиты и доступности.

Если используемый по умолчанию набор правил не удовлетворяет вашим требованиям, вы можете добавить новый набор. Вы также можете его удалить и редактировать.

Простой и расширенный вид

В настройках прокси правила отображаются в двух видах: простой вид и расширенный вид.

- Простой вид — Простой вид используется для настройки шаблона группового символа, который совпадает с простым регулярным выражением.

- Расширенный вид — Показывает действия для каждого правила. Выберите этот вид если хотите использовать кнопки для редактирования, клонирования (создание нового правила на базе существующего), удаления и перезагрузки правил. Вы также можете использовать расширенный вид для настройки точного совпадения и Perl-совместимые регулярные выражения.

Переключиться с расширенного на простой вид вы можете только если все включенные правила содержат одинаковые действия, тревоги и параметры журналов. Например если у вас есть четыре

правила с действиями **Allow** и одно с действием **Deny**, то вам необходимо продолжать работать с расширенным видом.

Настройка наборов правил и смена вида

Для того для того, чтобы настроить наборы правил в Policy Manager выполните следующее:

1. Два раза нажмите на политику или добавьте новую политику.

2. В диалоговом окне **Policy Properties** выберите закладку **Properties**.

3. Нажмите  .
   Откроется диалогое окно Proxy Action Configuration.

4. Для того чтобы сменить вид нажмите **Change View**.

5. Добавьте, измените при необходимости или удалите все необходимые правила.

Добавление, редактирование или изменение правил

Для того чтобы добавить правила вам необходимо использовать простой или расширенный вид набора правил.

Для настройки шаблона группового символа, который совпадает с простым регулярным выражением, вы можете использовать простой вид, а расширенный вид – для настройки точного совпадения и Perl-совместимых регулярных выражений. Также расширенный вид отображает действия для каждого правила, а также кнопки, которые вы можете использовать для редактирования, клонирования (создание нового правила на базе существующего), удаления или перезагрузки правил.

Во время настройки правил вам необходимо выбрать действия, которое прокси выполняет действия для каждого пакета. Для различных компонентов прокси вы можете выбирать различные действия. Например, действия **Strip** и **Lock** применяются только для действий IPS на базе сигнатур. Ниже приводится список всех доступных действий:

Allow

Разрешает соединение.

Deny

Блокирует определенный запрос, но не разрывает соединение. Клиенту отправляется соответствующее сообщение.

Drop

Блокирует определенный запрос и разрывает соединение. Отправителю не шлется никакого ответа. Firebox клиенту отправляет только TCP reset пакет. Браузер клиента может пользователю отобразить “The connection was reset” или “The page cannot be displayed”, но не сообщит ему по какой причине запрос был заблокирован и разорвано соединение.

Block

Блокирует запрос, разрывает соединение и блокирует сайт. Для более подробной информации о заблокированных сайтах см “Заблокированные сайты”

Весь трафик с IP адреса сайта блокируется на промежуток времени, указанный в Policy Manager (**Setup > Default Threat Protection > Blocked Sites**, закладка **Auto-Blocked**). Используйте это действие только если вы хотите заблокировать трафик на указанный промежуток времени.

Strip

Удаляет вложение из пакета и блокирует его. Другие составляющие пакета данных передаются через Firebox в место назначения.

Lock

Блокирует вложения таким образом, чтобы только администратор мог открыть это его.

AV Scan

Проверяет вложения на предмет наличия вирусов. Если вы выберете эту опцию, то для этой политики будет включен Gateway AntiVirus.

Добавление правил (простой вид)

Для того чтобы добавить новое правило в простом виде выполните следующее:

1. В текстовом поле **Pattern** введите шаблон, который использует синтаксис простого регулярного выражения. Групповой символ для пустой строки или строки из более чем одного символа - “*”. Групповой символ для одного символа - “?”. Нажмите **Add**. *Новое правило появится в поле Rules.*

   Выберите значение в поле **Actions to take**:

   * В выпадающем списке **If matched** выберите действие, которое необходимо выполнить, если содержимое пакета совпадает с одним из правил в списке.

   * В выпадающем списке **None matched** выберите действие, которое необходимо выполнить, если содержимое пакета не совпадает ни с одним правилом в списке.

2. Для того создать тревогу для этого события включите опцию Alarm. Тревога используется для того, для того, чтобы сообщить пользователю о том, к трафику было применено правило прокси. Для того чтобы настроить параметры этой тревоги в списке Categories в левой части окна Proxy Configuration выберите Proxy Alarm. Вы можете отправить SNMP ловушку, отправить электронное письмо или открыть всплывающее окно.

3. Для того чтобы записать это событие в журнал включите опцию **Log**.

Добавление правил (расширенный вид)

При помощи расширенного вида вы настраиваете точное совпадение и Perl-совместимые регулярные выражения. Для более подробной информации о регулярных выражениях см. “Регулярные выражения”

1. В окне **Proxy Action Configuration** нажмите **Add**.
   Откроется диалоговое окно New <ruletype> Rule

2. В поле **Rule Name** введите имя правила. При добавление правила это поле пустое. При клонировании правила вы можете редактировать это поле. При редактировании существующего правила это поле недоступно

3. В выпадающем списке **Rule Settings** выберите одну из следующих опций:

   * **Exact Match** — Для точного совпадения содержимого пакета с текстом правила.

   * **Pattern Match** — Для совпадения содержимого пакета с шаблоном текста, используя групповые символы.

   * **Regular Expression** — Когда содержимое пакета должно совпадать с шаблоном текста с регулярным выражением.

4. В текстовом поле Rule Settings введите текст правила. Если вы выберете Pattern Match, то в качестве групповых символов используйте символы (*), (.) или (?)

5. В секции **Rule Actions** в выпадающем списке **Action** выберите действие, которое прокси будет выполнять для этого правила.

6. Для того чтобы создать тревогу для этого события включите опцию **Alarm**. Тревога сообщает пользователям о том, что правило прокси было применено к сетевому трафику.

7. Для того чтобы записать это событие в журнал включите опцию **Log**.

Копирование и вставка настроек правил

Вы можете скопировать и вставить текст из одного определения прокси в другое. Например, предположим вы можете написать сообщения о запрете для POP3 прокси. Затем вы можете скопировать это сообщение в поле **Deny Message** для SMTP прокси. Когда вы копируете данные между двумя прокси, вам необходимо убедиться, что поле значение которого вы копируете,

совместимо с прокси, в который вы вставляете это значение. Вы можете копировать наборы правил только между прокси или категориями внутри этих 4-х групп. Другие комбинации не совместимы.

Типы содержимого	Имена файлов	Адреса	Аутентификация
HTTP Content Types	FTP Download	SMTP Mail From	SMTP Authentication
SMTP Content Types	FTP Upload	SMTP Mail To	POP3 Authentication
POP3 Content Types	HTTP URL Paths		
	SMTP Filename		
	POP3 Filenames		

Изменение порядка следования правил

Порядок следования правил в списке **Rules** такой же, как и порядок, в котором трафик сравнивается с правилами. Прокси сравнивает трафик с первым правилом сверху вниз. Когда трафик совпадает с правилом Firebox выполняет соответствующее действие. Он не выполняет других действий, даже если трафик совпадает с правилом, которое идет дальше по списку. Для того чтобы изменить порядок следования правил вам необходимо использовать расширенный вид:

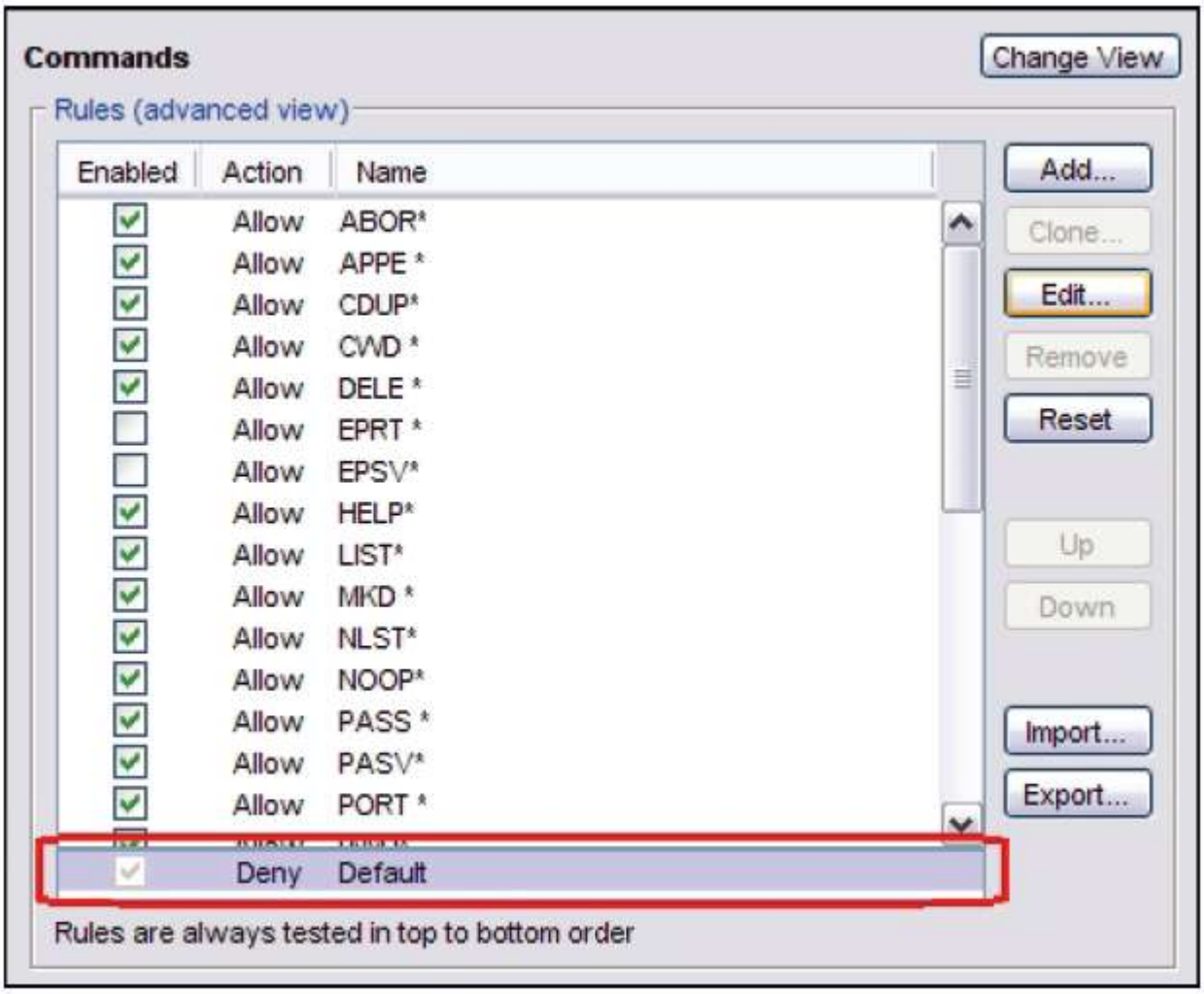
1. Нажмите **Change View** для того чтобы переключиться на расширенный вид.
2. Выберите правило, позицию которого вы хотите изменить. Для изменения позиция правила в списке используйте кнопки **Up** или **Down**.

Изменения правила по умолчанию

Если трафик не совпадает ни с одним правилом прокси, то Firebox использует *правило по умолчанию*. Это правило всегда находится в конце списка правил.

Для того чтобы изменить правило по умолчанию выполните следующее:

1. Выберите правило по умолчанию и нажмите **Edit**.
   Откроется диалоговое окно Edit Default Rule



2. Вы можете изменить действие для правила по умолчанию, а также настроить генерацию тревог и сообщений журнала для этого правила. Для этого правила вы не можете изменять его имя и расположение в списке. Это правило должно быть всегда в конце списка.

3. Нажмите **OK**.

Регулярные выражения

Регулярное выражение – это группа букв, чисел и специальных символов, которые используются для поиска данных. Вы можете использовать Perl-совместимые регулярные выражения (PCRE) в вашей конфигураций для поиска совпадений для определенных типов трафика в действиях прокси. Например, вы можете использовать одно регулярное выражение для блокировки подключений к некоторым web-сайтам и разрешить подключения к другим web сайтам. Вы также можете заблокировать SMTP пакеты в случае если адрес получателя некорректен. Например, если вы хотите заблокировать определенные страницы сайта, которые нарушают вашу политику использования Интернет, вы можете использовать регулярные выражения в категории URL Paths в конфигурации HTTP прокси.

Общая информация

- Регулярные выражения в Fireware чувствительны к регистру — при создании регулярного выражения вам необходимо учитывать регистр символов. Если в начале группы поместить модификатор (?i), то вы можете не обращать внимание на регистр.

- Регулярные выражения в Fireware отличаются от групповых символов MS-DOS и Unix — В MS-DOS или командной строке Windows символы «?» или «*» для поиска имен файлов, которые содержат один или несколько символов. В Fireware эти групповые символы работают по-другому.

Для более подробной информации о групповых символах в Fireware см. следующие разделы.

Создание регулярного выражения

Наиболее простое регулярное выражение – это просто текст, который вы ищете. Регулярное выражение, которое состоит из последовательности букв и чисел, будет использоваться для поиска строк, которые будут содержать только эту последовательность.

Пример: fat будет совпадать с fat, fatuous, infatuated, а также с многими другими последовательностями.

Fireware разрашает использование последовательностей, состоящих из любых символов и включающих регулярное выражение. Очень часто регулярное выражение совпадает с несколькими последовательностями символов. Если вы используете регулярное выражение в качестве источника в правиле Deny, вы можете случайно заблокировать другие типы трафика. Поэтому мы рекомендуем перед тем как добавлять регулярные выражения в конфигурацию тщательно их проверять

Для того для того, чтобы одновременно искать различные последовательности символов вам необходимо использовать специальные символы. Наиболее часто используемым специальным символом является точка (.), которая похоже на групповой символ. Если в регулярном выражении вы введете точку, то оно будет совпадать с любым символом, пробелом или табуляцией. Специальный символ «.» не используется для поиска разрывов (\r\n или \n).

Пример: f..t будет совпадать с foot, feet, f&#t, f –t и f\t3t.

Для того чтобы искать специальный символ в строке, например ту же самую точку, вам необходимо в тексте регулярного выражения перед точкой поставить обратную косую черту (\). Если вы не добавите обратную косую черту, то выражение будет работать некорректно. Для символов, которые уже содержат обратную косую черту, например \t (табуляция), нет необходимости добавлять вторую косую черту. Обратную косую черту необходимо добавлять к следующим символам для их поиска в строке: ? . * | + $ \ ^ ( ) [

Пример: \$9\.99 совпадает с $9.99

Шестнадцатеричные символы

Для поиска шестнадцатеричных символов используйте следующие выражения: \x или %0x%. Модификатор регистра не влияет на шестнадцатеричные символы.

Пример: \x66 или %0x66% совпадает с f, но не с F.

Повторение

Для того чтобы найти переменное количество символов вам необходим модификатор повторений, который вы можете использовать как для одного символа, так и для нескольких. Существует четыре типа модификаторов повторения:

- Цифры внутри фигурных скобок, например {2,4}, будет искать от 2 до 4 символов, идущих подряд.

  Например: 3{2,4} будет совпадать с 33, 333 или 3333, и не будет совпадать с 3 или 33333.

- Знак вопроса (?) после какого-либо символа, класса или группы – ноль или одно вхождение символа, класса, группы в строку.

  Пример: me?et совпадает с met и meet.

- Знак плюс (+) после символа, класса, группы – одно или несколько вхождений символа в строку.

  Пример: me+t совпадает с met, meet и meeeeeeeeet.

- (*) – ноль или несколько вхождений предшествующего ему символа, класса или группы.

  Пример: me*t совпадает mt, met, meet и meeeeeeeeet.

Для того чтобы применить несколько модификаторов к сразу нескольким символам, вам необходимо создать группу. Группа – это последовательность символов, заключенных в скобки.

Пример: ba(na)* будет совпадать с ba, bana, banana и bananananananana.

Классы символов

Для того чтобы найти один символ из группы, вам необходимо использовать квадратные скобки. Группа символов, заключенная в квадратные скобки, называется классом символов

Для классов символов вы можете применять модификаторы повторения. Порядок расположения символов внутри класса не имеет значения.

Специальными символами внутри класса является закрывающаяся скобка (]), обратная косая черта (\), знак вставки (^) и дефис (-).

Пример: gr[ae]y совпадает с gray и grey.

Для того чтобы использовать знак вставки в классе символов, не ставьте его в начале класса. Для того чтобы использовать дефис в классе вам необходимо поставить его первым. Отрицательный класс символов используется для поиска символов, которые не входят в него. Для того чтобы сделать класс отрицательным в его начале поставьте знак вставки (^)

Пример: [Qq][^u] совпадает с Qatar, но не с «question» или Iraq.

Диапазоны

В классах символов часто используют диапазоны символов. Диапазон – это две буквы или цифры, разделенные дефисом (-). Любой символ, который входит в диапазон, будет соответствовать этому регулярному выражению. Если к классу вы добавите модификатор повторения, то предшествующий класс повторяется.

Пример: [1-3][0-9]{2} совпадает с 100 и 399, а также с любым числом, которое находится между 100 и 399.

Некоторые часто используемые диапазоны имеют более короткую запись. Вы можете использовать эти записи внутри других классов. Ниже в таблице приведены нескольких диапазонов и их отрицательные значения.

Class Equivalent to	Negated Equivalent to
\w Any letter or number [A-Za-z0-9]	\W Not a letter or number
\s Any whitespace character [\t\r\n]	\S Not whitespace
\d Any number [0-9]	\D Not a number

Якори

Для поиска начала или конца строки вам необходимо использовать якори. Символ (^) совпадает с началом строки, а символ ($) – с концом строки.

Пример: ^am.*$ совпадает с «ampere», если «ampere» единственное слово в строке. Оно не совпадает с «dame».

При помощи \b вы можете определять границы для символов или \B для поиска символов, которые не являются первым или последним символом в слове.

Есть три вида границ символов:

- Перед первым символом в последовательности, если первый символ – это буква (\w)
- После последнего символа в последовательности, если последний символ это буква (\w)
- Между буквой (\w) и не буквой (\W)

Чередования (Alternation)

Чередования используются для поиска нескольких вариантов в сроке. Чередование в регулярных выражениях похож на булевский оператор OR и обозначается прямой чертой (|).

Пример: m(oo|a|e)n совпадает с первым вхождением «moon», «man» или «men».

Примеры регулярных выражений

Поиск типа содержимого PDF (MIME тип)

^%PDFMatch

Любой валидный IP адрес

(25[0-5]|2[0-4][0-9]\|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]\|[01]?[0-9] [0-9]?)\.(25[0-5]|2[0-4][0-9]\|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]\|[01]? [0-9][0-9]?)

Проверка адреса электронной почты

[A-Za-z0-9._-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,4}

Импорт и экспорт наборов правил

Если у вас есть несколько устройств Fireboxe, вы можете посредством процедур импорта и экспорта переносить наборы правил с одного устройства на другое. Это позволяет сэкономить время, так как создавать правила вам придется только один раз. Вы создаете правил для одного прокси, экспортируете их XML файл и импортируете их в другой прокси.

1. Создайте наборы правил для одного прокси или категории.
2. При необходимости переключитесь на расширенный вид (**Change View)**.
3. Нажмите **Export**.
4. В диалоговом окне **Save** выберите каталог, в который вы сохраните ваш XML файл.
   По умолчанию файл сохраняется в My Documents > My WatchGuard.
5. Введите имя файла и нажмите **Save**.
6. В настройках нового прокси нажмите **Import**.

7. Найдите сохраненный в п. 2 XML файл и нажмите **Open**.

8. Если правила, которые содержатся в файле, уже созданы в новом прокси, то система спросит вам, хотите ли вы сначала удалить старые правила.

   * Нажмите **Yes** если вы хотите удалить существующие правила и заменить их новыми.

   * Нажмите **No** для того чтобы добавить новые правила уже к существующим.

Копирование наборов правил между прокси или категориями

Некоторые наборы правил могут быть использованы в нескольких прокси или категориях. Например вы можете эскпортировать правила Content Types действия HTTP прокси и затем импортировать их в набор правил Content Types действия SMTP прокси. Или вы можете эскпортировать правила SMTP Mail From в набор правил SMTP Mail To

Действия прокси

Действие прокси – это определенный набор параметров, источников и мест назначения для определенного типа прокси. Так как ваша конфигурация может включать несколько экземпляров каждого прокси, вам необходимо подключить каждый экземпляр к определенному действию прокси. Для каждого прокси у вас обычно отдельные действия прокси для клиентов и серверов. Например, вы можете использовать одно действие прокси для пакетов, отправленных на сервер POP3, защищенный Firebox и другое действие прокси для обработки электронных сообщений для клиентов POP3.

Также для клиентов и серверов вы можете создать несколько действий прокси. Например, вы можете создать одну политику HTTP, которая управляет HTTP трафиком от определенной группы пользователей с меньшими привилегиями. В поле **From** в настройках этой политики указаны все IP адреса этих пользователей. Вторая политика HTTP управляет трафиком от группы пользователей с большими привеллегиями. IP адреса этих пользователей также указаны в поле **From** в настройках политики. Вы создаете одно действие HTTP прокси для одной политики и второе действие HTTP прокси для второй политики.

Действие прокси для пользователей с меньшими привилегиями имеет более строгие правила, которые блокируют большее количество URL и типов содержимого, чем действие прокси для второй группы пользователей. Вы можете создать несколько действий прокси и использовать их при необходимости.

Для каждого типа прокси вы можете создать несколько действий прокси, но каждой политике вы можете присвоить только одно действие прокси. Например, иконка POP3 прокси в главном окне Policy Manager привязана только к одному действию прокси; например, действию POP3-Client. Если вы хотите создать POP3 прокси для POP3 сервера или дополнительные прокси для POP3 клиентов, вам необходимо добавить новую политику POP3 в Policy Manager.

Настройка действия прокси

1. В диалоговом окне **Add/Edit Policy Properties** выберите закладку **Properties**.

2. В выпадающем списке **Proxy action** выберите действие прокси.

Редактирование, удаление и клонирование действий прокси

Вы также можете редактировать, удалять или клонировать (копировать) действия прокси:

1. Выберите **Setup** > **Actions**.

2. В диалоговом окне **Proxy Actions** выберите действие прокси, которое вы хотите удалить, редактировать или клонировать.

3. Нажмите **Edit**, **Remove** или **Clone**. Вы не можете удалять предопределенные действия прокси (отображаются синим цветом)

Предопределенные и пользовательские действия прокси

Fireware XTM для каждого прокси имеет набор предопределенных действий прокси для клиента и для сервера. Эти предопределенные действия используются для балансировки уровня безопасности вашей сети и уровня доступа к сетевым ресурсам. Вы не можете изменить параметры предопределенных действий прокси. Если вы хотите внести какие-либо изменения в конфигурацию вам необходимо клонировать параметры предопределенного действия и сохранить их в новом действии прокси. Например, если вы хотите изменить параметры действия прокси HTTP-Client, вам необходимо сохранить это действие под другим именем, например HTTP-Client.1. Это необходимо, только если вы хотите внести изменения в наборе правил. Если вы хотите внести изменения в общие параметры (разрешенные источники и получатели трафика, параметры NAT для политики и др.) вам не нужно сохранять эти настройки под другим именем.

Импорт и экспорт пользовательский действий прокси

Если у вас есть несколько устройств Firebox, то для экономии времени вы можете создать действия прокси на одном устройстве, а затем с помощи функции экспорта/импорта перенести их на другие устройства.

Для успешного импорта действий прокси необходимо, чтобы на устройствах Firebox, с которого вы экспортировали действия в файл, и устройство, на которое вы импортируете действия, были установлены одинаковые версии WSM и Policy Manager.

1. На первом Firebox создайте несколько действий прокси.

2. В диалоговом окне **Proxy Actions** нажмите **Export**. Вам не надо выбирать пользовательские действия, функция эскпорта автоматически скопирует все пользовательские действия в файл.

3. В диалоговом окне **Save** выберите каталог, в который вы хотите сохранить действия прокси.
   По умолчанию используется каталог My Documents > My WatchGuard.

4. Введите имя файла и нажмите **Save**.

5. В Policy Manager на другом Firebox в диалоговом окне **Proxy Actions** нажмите **Import**.

6. Найдите файл, который вы создали в п.3, и нажмите **Open**.

7. Если действия, которые содержатся в файле, уже созданы на этом Firebox, то система попросит вас выбрать, хотите ли вы заменить существующие действия или добавить новые действия к уже существующим.

   * **Replace** — Существующие пользовательские действия прокси удаляются и заменяются на новые.

   * **Append** — Импортированные действия просто добавляются к уже существующим.

Обнаружение проникновений в прокси

Проникновение это прямая атака на ваш компьютер, которая может нанести вред вашему компьютеру, а также с помощью которой хакер может получить доступ к важной информации и использовать ваш компьютер для атаки других компьютеров в сети.

Для того чтобы защитить вашу сеть от проникновений, вы можете приобрести дополнительный сервис - Intrusion Prevention Service (IPS). IPS работает с SMTP, POP3, HTTP, FTP, DNS и TCP-UDP прокси. Для активации и настройки IPS вы можете запустить мастер настройки IPS или использовать набор правил IPS в настройках прокси.

Запуск мастера Activate Intrusion Prevention

1. Откройте Policy Manager.

2. Выберите Subscription **Services** > **Intrusion Prevention** > **Activate**.
   Откроется мастер Activate Intrusion Prevention.

3. Выполните все необходимые инструкции мастера. Для более подробной информации см. Activate Intrusion Prevention Service (IPS).

Набор правил IPS в настройках прокси

1. Загрузите лицензионный ключ для IPS с сайта LiveSecurity Service и добавьте этот ключ в вашу конфигурацию.

2. Добавьте политику прокси к вашей конфигурации Firebox. Или вы можете использовать существующий прокси.

3. В диалоговом окне **New/Edit Policy Properties** выберите закладку **Properties**.

4. Нажмите  .

5. В левой части окна выберите категорию **Intrusion Prevention**.

6. В правой части окна настройте параметры IPS.

Добавление политики прокси

При добавлении политики прокси или ALG (application layer gateway) в вашу конфигурацию, вы указываете устройству Firebox типы содержимого, которые он должен искать при обработке трафика. Если найденное содержимое соответствует критерию, указанному в настройках прокси или ALG, Firebox на базе действий в настройках прокси определяет, блокировать или пропускать этот трафик.

Вы можете использовать параметры политики прокси по умолчанию, а можете внести необходимые изменения. Вы также можете создать отдельные политики прокси или ALG для управления другими сегментами вашей сети.

Важно помнить то, что прокси или ALG требуют больше ресурсов центрального процессора, чем пакетные фильтры. Если вы добавите слишком большое количество политик прокси или ALG, то скорость передачи данных может значительно снизиться. Однако все-таки в отличие от пакетных фильтров, прокси могут перехватывать пакеты, которые содержат потенциально опасные данные. Каждая политика прокси имеет набор параметров, манипулируя которыми вы можете создать баланс между уровнем безопасности вашей сети и скоростью передачи данных.

Для того чтобы добавить политику прокси выполните следующее:

1. В панели инструментов Policy Manager нажмите (+). Или выберите **Edit** > **Add Policies**.
   Откроется диалоговое окно Add Policies.

2. Слева от каталога нажмите на символ (+) для того чтобы открыть каталог **Proxies**.
   Откроется список прокси.

3. Выберите прокси, который вы хотите добавить. Нажмите **Add**.
   Откроется диалоговое окно New Policy Properties.

Политики прокси WatchGuard и ALG имеют предопределенные наборы правил, которые обеспечивают баланс между уровнем безопасности и уровнем доступа. Если используемый по умолчанию набор правил не удовлетворяет всем вашим требованиям вы можете создать свой собственный набор правил

DNS прокси

DNS(Domain Name System) – система серверов, которые преобразуют числовой IP-адрес в читаемые Интернет адреса и обратно. DNS позволяет вашей компьютерной сети понимать, например, что если вы введете в адресной строке браузера www.watchguard.com, то необходимо подключиться к серверу с IP-адресом 200.253.208.100.

Fireware XTM предоставляет вам два способа управления DNS трафиком: пакетный фильтр DNS и политика DNS прокси. Важно понимать, что настройки DNS прокси будут использовать эффективно только если DNS запрост будет маршрутизироваться через ваш Firebox.

Если вы создадите новый конфигурационный файл, то в файл автоматически добавится политика пакетного фильтра Outgoing, которая разрешает все TCP и UDP подключения из ваших Trusted и Optional сетей во внешнюю сеть. Это позволяет вашим пользователям подключаться к внешнему DNS серверу через стандартные порты TCP 53 и UDP 53. Так как Outgoing – это пакетный фильтр, то он не сможет вас защиить от UDP троянов, DNS эксплойтов и других проблем, связанными с разрешением всего UDP трафика из вашей Trusted сети.

Действий прокси DNS-Outgoing имеет средства защиты вашей сети от атак такого типа. Если вы используете внешние DNS серверы для вашей сети, то набор правил DNS-Outgoing предлагает дополнительные способы управления сервисами, доступными пользователям вашей сети. Для того чтобы добавить DNS прокси к вашей конфигурации см. “Добавление политики прокси”

Затем при необходимости в диалоговом окне **New/Edit Policy Properties** вы можете изменить параметры прокси. Поля в этом окне разделены на три закладки: **Policy**, **Properties** и **Advanced**. Вдобавок закладка **Properties** содержит иконку для настройки действия прокси.

Закладка Policy

- **DNS-proxy connections are** — **Allowed** (Разрешены), **Denied** (Заблокированы) или **Denied** (send reset) (Заблокированы, отправлять TCP RESET). Укажите, кто будет в списках From и To (закладка Policy в настройках прокси)
- **Use policy-based routing** — Маршрутизация на базе политики. Для более подробной информации см. “Настройка маршрутизации на базе политик”
- Вы также можете настроить статическую NAT или балансировку нагрузки

Закладка Properties

- Из выпадающего списка **Proxy action** укажите для кого вы создаете действие: клиента или сервера. Для более подробной информации см. “Действия прокси”
- Для настройки журнала нажмите **Logging** и выполните необходимые настройки
- Если в выпадающем списке C**onnections are** (закладка **Policy**) вы выберете Denied или Denied (send reset), вы можете заблокировать сайты, которые пытаются использовать DNS. Для более подробной информации см. “Временная блокировка сайтов при помощи политики”.
- Если вы хотите использовать таймаут ожидания (установленный Firebox или сервером аутентификации) см. “Настройка таймаута ожидания”.

Прокси WatchGuard имеют предустановленные наборы правил, которые обеспечивают необходимый уровень доступности и безопасности для большинства инсталляций. Если набор правил по умолчанию не соответствует вашим требованиям, вы можете создать новый набор правил, или изменить существующий. Для того чтобы изменить параметры правил для действия прокси выполните следующее:

1. Нажмите  .
2. Выберите категорию:

   * DNS proxy: General settings

   * DNS proxy: OPcodes

   * DNS proxy: Query types

   * DNS proxy: Query names

   * Обнаружение проникновений в прокси

   * Тревоги прокси и AV. SNMP ловушки и уведомления отключены по умолчанию.
3. Сохраните сделанные изменения.

Закладка Advanced

В этой закладке вы можете настроить следующее:

- Созданий расписаний для действий Firebox

- Добавление действия Traffic Management к политике
- Настройка обработки ICMP ошибок
- Применение правил NAT
- Включение QoS маркирования или настроек приоритизации для политики
- Настройка длительности sticky соединения для политики

DNS proxy: General settings

На странице **General** (первая страница, которая открываетеся после того, как вы нажмете иконку View/Edit Proxy) вы можете изменить параметры двух правил обнаружения аномалий протокола. Мы не рекомендуем изменять значения по умолчанию.

Not of class Internet

Выберите этот параметр, если вы хотите чтобы действие выполнялось при проверке DNS трафика, который не принадлежит к Интернет-классу. По умолчанию такой трафик не пропускается. Мы рекомендуем не изменять используемое по умолчанию действие.

Badly formatted query

Действие выполняется при проверке DNS трафика, который использует неправильный формат.

Alarm

Тревога – это механизм уведомления пользователей о том, что передаваемый ими трафик был обработан правилом прокси. Для того чтобы настроить тревогу для этого события включите опцию **Alarm**. Для того чтобы настроить параметры тревоги выберите **Proxy Alarm** из списка **Categories** в левой части окна Proxy Configuration. Вы можете использовать SNMP ловушку, электронное письмо или всплывающее окно.

Log

Опция записи события в журнал.

Turn on logging for reports

Создает запись в журнале для каждой транзакции. Эта опция создает большой файл журнала, но эта информация очень важна. Если вы не включите эту опцию, то в отчетах вы не сможете посмотреть подробную информацию об DNS подключениях через прокси.

DNS proxy: OPcodes

DNS OPcodes (operation codes) – это команды, которые даются на DNS сервере для выполнения каких-либо действий: запрос (Query), инверсный запрос (IQuery) и запрос статуса сервера (STATUS). Вы можете разрешить, запретить или заблокировать определенные команды DNS OPcodes.

1. В секции Categories выберите OPCodes.

2. Для того чтобы включить правило, напротив него включите опцию **Enabled**

Если вы используете Active Directory и ваша конфигурации Active Directory требует динамических обновлений, то вам необходимо разрешить DNS OPcodes в правилах ваших действий прокси DNS-Incoming. Это создаст угрозу вашей системе безопасности, однако для корректной работы Active Directory это необходимо.

Добавление правила OPcodes

1. Нажмите **Add**.
   Откроется диалоговое окно New OPCodes Rule.

2. Введите имя для правила.
   Имена правил не должны превышать 200 символов.

3. Значение DNS OPcodes является целым числом. При помощи стрелок установите необходимое значение OPCode.
   Для более подробной информации о значениях DNS OPcodes, см. RFC 1035.

Удаление или изменение правил

1. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

2. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

3. После того, как вы закончите, нажмите **OK**.

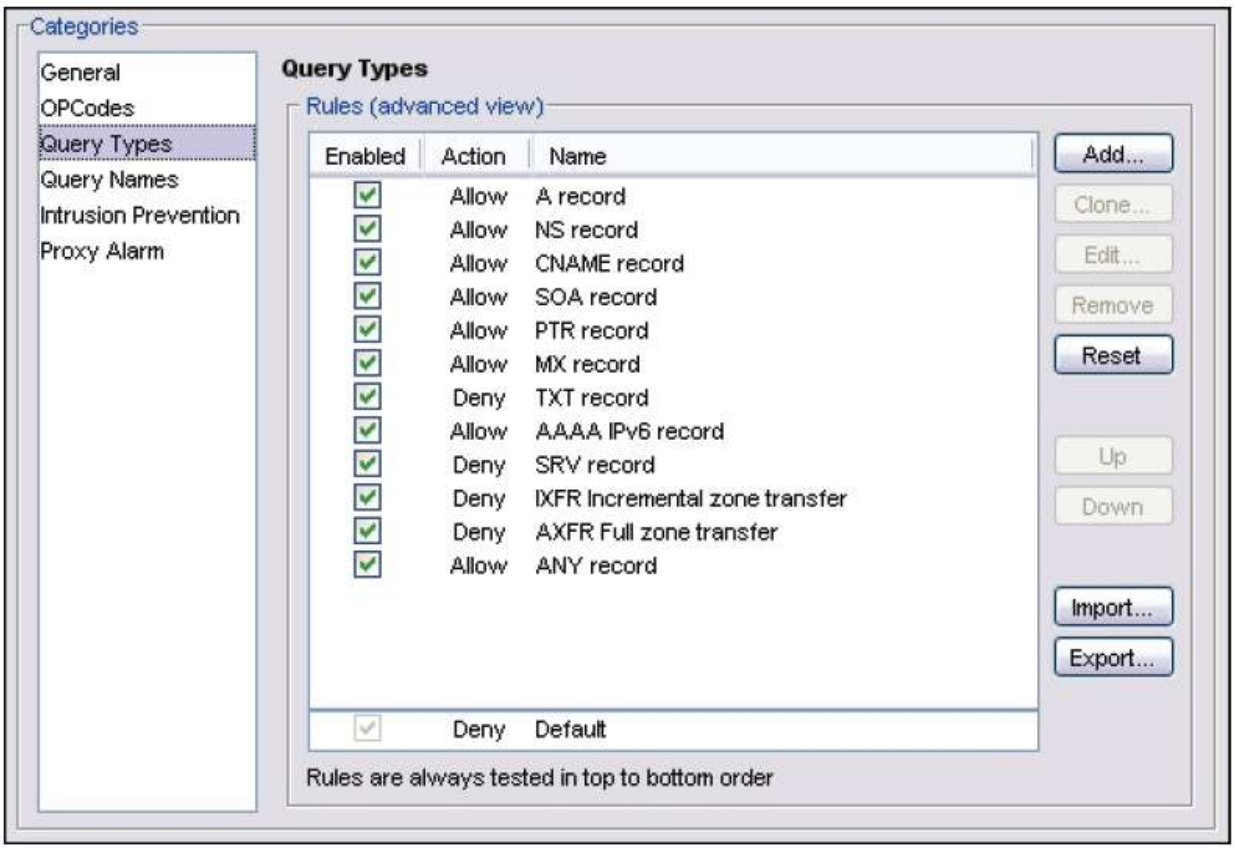
4. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

5. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

DNS proxy: Query types

Здесь вы можете настроить типы DNS запросов – запрос для обычных записей (CNAME или TXT) или специфичный запрос типа AXFR-запрос на трансфер зоны. Здесь вы можете разрешить, запретить, блокировать определенные типы DNS запросов.

1. В секции **Categories** выберите **Query Types**



2. Для того включить правило включите опцию Enabled напротив него.

Добавление нового правила типа запроса

1. Для того чтобы добавить новое правило для типов запроса нажмите **Add**.
   Откроется окно New Query Types Rule.

2. Введите название правила.
   Названия правил могут содержать не более 200 символов.

3. У типов DNS-запросов есть параметр RR(Resource Record – Запись ресурса). При помощи стрелок установите необходимое значение параметра.
   Для более подробной информации о значениях типов DNS-запросов, см. RFC 1035.

4. Добавьте, удалите или измените правила, как описано в “”

5. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

6. После того, как вы закончите, нажмите **OK**.

7. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

8. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

DNS proxy: Query names

Имя DNS-запроса относится к определенному доменному имени, которое отображается как Полное Доменное Имя (FQDN). Вы можете добавлять, удалять и редактировать правила.

1. В секции **Categories** выберите **Query Names**

2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

6. Введите имя нового действия и нажмите **OK**.
Откроется диалоговое окно New Policy Properties.

MX (Mail eXchange) записи

MX (Mail eXchange) запись – это тип DNS записи, которая возвращает один или несколько имен хостов серверов электронной почты, которые отвечают за получение электронной почты в этом домене. Если MX запись содержит несколько имен хостов, то каждому имени присваивается номер, который определяет приоритеты хостов.

Поиск MX записи

Когда сервер электронной почты отправляет письмо, он сначала отправляет DNS запрос на для MX записи домена получателя этого письма. После того, как сервер получит ответ, он будет знать имена авторизованных хостов для обмена почтой в домене получателя письма. Для того чтобы получить IP адрес одного из этих хостов сервер электронной почты отправляет второй DNS запрос для A записи имени хоста. DNS сервер возвращает IP адрес, соответствующий этому имени хоста.

Reverse MX lookup

Большинство анти-спам решений, включая те, которые используются большинством ISP или провайдерами электронной почты (AOL, MSN и Yahoo!) используют реверсивный MX поиск. Используются различные виды реверсивного поиска, однако цель у них одна: сервер получателя хочет проверить, чтобы электронное письмо не пришло с какого-либо постороннего адреса и что сервер, с которого пришло это письмо, является авторизованным хостом для этого домена.

Для проверки является ли сервер отправителя авторизованным сервером электронной почты, сервер получателя пытается найти MX запись, которая соответствует домену отправителя. Если такая запись не найдена, то электронная почта считается спамом и блокируется.

Имя домена, которое ищет сервер получателя, может быть:

- Именем домена в заголовке **From:** электронного письма
- Именем домена в заголовке **Reply-To:** электронного письма
- Имя домена, которое сервер отправителя использует в качестве FROM параметра команды MAIL. (SMTP команда отличается от заголовка электронного письма. Сервер отправителя шлет команду MAIL FROM: серверу получателя для того, чтобы он понял от кого это электронное сообщение)
- Именем домена, которое возвращается в ответ на DNS запрос IP адреса источника. Сервер получателя иногда запрашивает PTR запись, которой соответствует определенный IP адрес. Запись PTR DNS – это запись, которая привязывает IP адрес к имени домена (Обычная *A* запись привязывает имя домена к IP адресу).

Перед тем как продолжить транзакцию сервер получателя отправляет DNS запрос для проверки, существует ли валидная MX запись для домена отправителя. Если для домена отправителя нет валидной DNS MX записи, тогда отправитель считается невалидным и его сообщение считается спамом и блокируется сервером получателя.

MX записи и multi-WAN

Так как при использовании multi-WAN исходящие пакеты устройства Firebox могут содержать различные IP адреса источника, вам необходимо убедиться что ваш DNS записи содержат MX записи для каждого внешнего IP адреса, который используется в качестве адреса источника при отправке электронной почты. Если список хостов в вашей MX записи домена не содержит записи для каждого External интерфейса Firebox, то возможно некоторые удаленные серверы электронной почты будут блокировать вашу почту.

Например, у компании XYZ есть Firebox с несколькими External интерфейсами. Firebox использует метод multi-WAN переключения. Запись MX компании XYZ содержит только одно имя хоста. Это имя хоста имеет *A* запись, которая соответствует IP адресу основного External интерфейса Firebox.

Когда компания XYZ отправляет электронное письмо на test@yahoo.com, оно передается через основной external интерфейс. Это письмо попадает на один серверов электронной почты Yahoo. Этот сервер выполняет реверсивный поиск MX записи для идентификации компании XYZ. Реверсивный поиск MX записи выполнен успешно и электронное письмо доставляется получателю.

В случае WAN переключения на Firebox, все исходящие соединения осуществляться через резервный external интерфейс. В этом случае почтовый сервер Yahoo опять выполняет реверсивный поиск MX и не находит IP адреса компании в MX и A записях компании XYZ. В результате электронное письмо блокируется. Для того чтобы решить эту проблему вам необходимо следующее:

- MX запись содержит несколько имен хостов, по крайней мере один для каждого External интерфейса Firebox.
- По крайней мере одно имя хоста должно иметь DNS *A запись,* которая содержит IP адрес, присвоенный каждому интерфейсу Firebox.

Добавление имени хоста в MX запись

MX записи хранятся, как часть ваших DNS записей домена. Для более подробной информации о настройке MX записей, свяжитесь с вашим хост-провайдером DNS или посмотрите документацию по вашему DNS серверу.

FTP прокси

Протокол FTP (File Transfer Protocol) используется для передачи файлов между компьютерами в TCP/IP сети. FTP клиент это обычно компьютер. FTP сервер может ресурсом, который хранит файлы в той же или другой сетях. FTP клиент может работать в двух режимах передачи данных: активном и пассивном.

В активном режиме сервер инициирует соединение с клиентом через порт 20. В пассивном режиме клиент использует порт, который был до этого согласован с сервером. FTP прокси выполняет мониторинг и сканирование FTP соединений между вашими пользователями и FTP серверами

При помощи политики FTP прокси вы можете:

- Установить максимальную длину имени пользователя, длину пароля, имени файла и командной строки для того, чтобы защитить вашу сеть от атак типа переполнение буфера
- Управлять типами файлов, которые пользователь может выгружать или загружать.

TCP/UDP прокси доступен протоколам на нестандартных портах. Когда FTP использует другой порт (не 20), TCP/UDP прокси транслирует трафик FTP прокси. Для более подробной информации о прокси TCP/UDP см. “TCP-UDP прокси”

Для того чтобы добавить FTP прокси к вашей конфигурации Firebox см. “Добавление политики прокси”. Затем, если вы захотите изменить настройки прокси для того чтобы они соответствовали вашим требованиям, вы можете использовать диалоговое окно **New/Edit Policy Properties**. Поля в этом диалоговом окне разделены на три закладки: **Policy**, **Properties**, и **Advanced**.

Вдобавок закладка **Properties** содержит иконку для настройки действия прокси.

Закладка Policy

В закладке **Policy** вы можете настроить правила доступа и другие опции.

- **FTP-proxy connections are** — выберите одну из опций: **Allowed** (Разрешены), **Denied** (Запрещены) или **Denied (send reset)** (Запрещена, отправка TCP Reset). Вы можете также настроить, кто появится в списках From и To list (закладка Policy в настройках прокси)
- **Use policy-based routing** — См. “Настройка маршрутизации на базе политик”
- Вы также можете настроить статическую NAT или настроить балансировку нагрузки на сервер.

Закладка Properties

- Из выпадающего списка **Proxy action** укажите для кого вы создаете действие: клиента или сервера. Для более подробной информации см. “Действия прокси”
- Для настройки журнала нажмите **Logging** и выполните необходимые настройки
- Если в выпадающем списке **FTP-proxy connections are** (закладка **Policy**) вы выберете Denied или Denied (send reset), вы можете заблокировать сайты, которые пытаются использовать FTP. Для более подробной информации см. “Временная блокировка сайтов при помощи политики”
- Если вы хотите использовать таймаут ожидания (установленный Firebox или сервером аутентификации) см. “Настройка таймаута ожидания”

Прокси WatchGuard имеют предустановленные наборы правил, которые обеспечивают необходимый уровень доступности и безопасности для большинства инсталляций. Если набор

правил по умолчанию не соответствует вашим требованиям, вы можете создать новый набор правил, или изменить существующий.

Для того чтобы изменить параметры правил для действия прокси выполните следующее:

1. Нажмите  .

2. Выберите категорию:

- FTP proxy: General settings
- FTP proxy: Commands— по умолчанию FTP-client прокси разрешает все команды. Прокси FTP-server по умолчанию разрешает следующие команды:

  ABOR DELE* NLST* PORT* REST* RNTO* SYST* XCWD**

  APPE HELP* NOOP* PWD* RETR* STAT* TYPE* XMKD**

  CDUP LIST* PASS* RMD* STOR* USER* XRMD**

  CWD MKD* PASV* QUIT* RNFR* STOU* XCUP**

- FTP proxy: Content — По умолчанию прокси FTP-client запрещает загрузку следующих типов файлов: .cab, .com., .dll, .exe., .zip. Прокси FTP-server разрешает все файлы. Прокси клиента, также как и прокси сервера разрешают выгрузку всех файлов.
- FTP proxy: AntiVirus — Если Gateway AV для FTP прокси включен, то по умолчанию при обнаружении вируса или при сканировании возникла ошибка соединение разрывается.
- Обнаружение проникновений в прокси — Если IPS для FTP прокси включен, то по умолчанию трафик, который соответствует сигнатуре, блокируется.
- Тревоги Proxy and AV — SNMP ловушки и уведомления отключены по умолчанию.

Для переноса набора правил между прокси вы можете использовать функции импорта и экспорта.

Закладка Advanced

В настройках прокси вы можете использовать несколько опций:

- Созданий расписаний для действий Firebox
- Добавление действия Traffic Management к политике
- Настройка обработки ICMP ошибок
- Применение правил NAT
- Включение QoS маркирования или настроек приоритизации для политики
- Настройка длительности sticky соединения для политики

FTP proxy: General settings

На странице **General** вы можете настроить базовые параметры FTP максимальную длину имени пользователя.

1. В секции **Categories** выберите **General**.

2. Для того чтобы установить ограничения на определенные параметры FTP включите соответствующие опции. Настройка этих параметров поможет вам отразить атаки типа «переполнение буфера». При помощи стрелок установите необходимые ограничения:

   Set the maximum user name length to

   Максимальная длина имени пользователя на FTP сайтах.

   Set the maximum password length to

   Устанавливает максимальную длину паролей для входа на FTP сайты.

   Set the maximum file name length to

   Устанавливает максимальные размеры файлов для загрузки или выгрузки.

   Set the maximum command line length to

   Устанавливает максимальную длину командной строки, используемой на FTP сайтах

   Set the maximum number of failed logins per connection to

   Ограничение количества неудачных подключений к вашему ftp сайту. Эта опция позволит вам защититься от атак методом грубой силы

3. Для каждого параметра вы можете включить или отключить опцию **Auto-block**. Если кто-то пытается подключиться к FTP-сайту и превышает установленный предел параметра, для которого включена опция **Auto-block**, компьютер, который отправляет команды добавляется в список Blocked Sites.

4. Для того чтобы записывать в журнал каждую транзакцию включите опцию **Turn on logging for reports**. Вам необходимо включить эту опцию для того чтобы получать подробные отчеты по FTP трафику.

5. Если вы хотите изменить параметры для категории прокси, см. раздел документа, где приводится описание категории, которую вы хотите изменить. Если вы закончили настройку нажмите **OK**. Если действие прокси, параметры которого вы изменили, было предустановлено, то вам необходимо клонировать эти настройки в новое действие Введите имя для нового действия и нажмите **OK**. Откроется диалоговое окно New Policy Properties

FTP proxy: Commands

FTP имеет несколько команд для управления файлами. Вы можете создать правила, которые установят ограничения на использование некоторых команд FTP.

Для того чтобы установить ограничения на команды, которые могут использоваться на FTP сервере, защищенном Firebox, вы можете настроить действие прокси FTP-Server. По умолчанию прокси FTP-Server блокирует следующие команды:

ABOR HELP* PASS* REST* STAT* USER**

APPE LIST* PASV* RETR* STOR* XCUP**

CDUP MKD* PORT* RMD* STOU* XCWD**

CWD NLST* PWD* RNFR* SYST* XMKD**

DELE NOOP* QUIT* RNTO* TYPE* XRMD**

Используйте действие прокси FTP-Client для ограничения команд, которые пользователи, защищенные Firebox, могут использовать для подключения к внешним FTP-серверам. По умолчанию конфигурация FTP-Client разрешает все команды FTP

Вы можете добавлять, удалять и редактировать правила. Ниже приводятся команды, которые необходимы для корректной работы протокола FTP, поэтому их блокировать не надо.

Команда	Команда клиента	Описание
USER	n/a	Отправка имени пользователя
PASS	n/a	Отправка пароля
PASV	n/a	Пассивный режим передачи файлов
SYST	n/a	Вывести информацию об ОС вера и ее версии. FTP клиент ользует эту информацию для ектной обработки ответов FTP сервера

Для того чтобы добавить, удалить и редактировать правило, выполните следующее:

1. В секции **Categories** выберите **Commands**.
2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”
3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.
4. После того, как вы закончите, нажмите **OK**.
5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.
6. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

FTP proxy: Content

Вы можете управлять типом файлов, которые FTP прокси, разрешает загружать. Например, так как многие хакеры для заражения компьютеров вирусами используют исполняемые файлы, вы можете заблокировать запросы на исполняемые файлы (*.exe). Или если вы не хотите, чтобы пользователи загружали файлаы Windows Media files на FTP сервер, вы можете добавить *.wma и заблокировать запросы для этих файлов. В качестве группового символа вы можете использовать (*).

Для управления правилами выгрузки для FTP сервера, защищенного Firebox, используйте действие прокси FTP-Server. Для установки правил выгрузки для пользователей, которые подключаются к внешним FTP серверам, используйте действие прокси FTP-Client.

1. В секции **Categories** выберите **Upload** или **Download**.

2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

6. Введите имя нового действия и нажмите **OK**.
Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

FTP proxy: AntiVirus

Если вы приобрели и включили Gateway AntiVirus, то вам необходимо в секции AntiVirus выбрать действия, которое необходимо предпринять в случае обнаружения вируса в загружаемом/выгружаемом файле.

- Для активации Gateway AntiVirus из настроек прокси см. “Активация Gateway AntiVirus из настроек прокси”

- Для активации Gateway AntiVirus в меню Subsciption Services утилиты Policy Manager см. “Активация Gateway AntiVirus при помощи мастера”

- Для настройки Gateway AntiVirus для FTP прокси см. “Настройка действий Gateway AntiVirus”

Если вы включите Gateway AntiVirus вам необходимо настроить действия, которые будут предприниматься при обнаружении вируса или ошибки в выгружаемом/загружаемом файле. Вы можете выбрать следующие действия:

Allow

Пропускает пакет и отправляет его в место назначения, даже если обнаружен вирус..

Deny

Запретить загрузку файла и отправить сообщение о запрете (Deny-сообщение)

Drop

Блокировка пакета и разрыв соединения. Источнику этого сообщения не отправляется никакого уведомления.

Block

Блокирует пакет и добавление IP-адреса отправителя в список Blocked Sites.

H.323 ALG

Если в вашей сети вы используете Voice-over-IP (VoIP), вы можете добавить H.323 или SIP (Session Initiation Protocol) ALG (Application Layer Gateway) для открытия портов, необходимых для передачи VoIP трафика через ваше WatchGuard устройство. ALG создается также как и политика прокси и предлагает похожий набор параметров. Эти ALG были созданы в работы в сетях с NAT для защиты оборудования для конференций, подключенного к вашему WatchGuard устройству.

H.323 обычно используется в более старом оборудовании для видеоконференций и передачи голоса по IP. Протокол SIP – это более новый стандарт, который чаще используется в сетях, в которых находятся только конечные устройства (например VoIP телефоны), а VoIP провайдер управляет их соединением. При необходимости вы одновременно можете использовать H.323 и SIP ALGs. Для того чтобы понять, какой ALG вам необходимо создать, см. документацию по вашим VoIP оборудованию или приложениям.

Компоненты VoIP

Важно понимать, что вы можете реализовать VoIP следующим образом:

Соединение точка-точка (P2P соединение)

При использовании p2p соединений каждое устройство знает IP адрес другого устройства и напрмяую подключаеткся к нему. Если оба устройства находятся за Firebox, то он может корректно маршрутизировать голосовой трафик.

Hosted соединения

Подключение, которые обслуживаются специальной системой управления - PBX

При использовании H.323 ключевым компонентом системы управления голосовыми вызовами является *привратник (gatekeeper)*. Привратник управляет VoIP звонками для группы пользователей и может находиться в сети, защищенной вашим WatchGuard устройством или где-нибудь во внешней сети. Например, некоторые VoIP провайдеры подключают привратника, к которому вы должны подключиться перед тем, как установить VoIP соединение, к своей сети.

Управление множеством компонентов VoIP сети может представлять довольно непростую задачу. Поэтому перед тем как создавать H.323 или SIP ALG, вам необходимо убедиться, что ваша VoIP сеть корректно работает.

Функции ALG

Если вы включите H.323 ALG, то ваше WatchGuard устройство:

- Автоматически будет отвечать на запросы VoIP приложений и откроет все необходимые порты
- Проверит, что VoIP соединения используют стандартные протоколы H.323
- Генерирует сообщения журнала для аудита

Достаточно большое количество VoIP устройств и серверов используют NAT (Network Address Translation) для автоматического открытия и закрытия портов.

H.323 и SIP ALGs также выполняют эту функцию. Если вы используете H.323 или SIP ALG вам необходимо отключить NAT на ваших VoIP устройствах.

Закладка Policy

- H.323-ALG connections are — выберите одну из опций: Allowed(Разрешены), Denied (Запрещены) или Denied (send reset) (Запрещена, отправка TCP Reset). Вы можете также настроить, кто появится в списках From и To list (закладка Policy в настройках прокси). Для более подробной информации см. Set access rules for a policy.
- **Use policy-based routing** — См. “Настройка маршрутизации на базе политик”
- Вы также можете настроить статическую NAT или настроить балансировку нагрузки на сервер.

Закладка Properties

- Из выпадающего списка **Proxy action** укажите для кого вы создаете действие: клиента или сервера. Для более подробной информации см. “Действия прокси”
- Для настройки журнала нажмите **Logging** и выполните необходимые настройки
- Если в выпадающем списке C**onnections are** (закладка **Policy**) вы выберете Denied или Denied (send reset), вы можете заблокировать сайты, которые пытаются использовать FTP. Для более подробной информации см. “Временная блокировка сайтов при помощи политики”
- Если вы хотите использовать таймаут ожидания (установленный Firebox или сервером аутентификации) см. “Настройка таймаута ожидания”

Прокси WatchGuard имеют предустановленные наборы правил, которые обеспечивают необходимый уровень доступности и безопасности для большинства инсталляций. Если набор правил по умолчанию не соответствует вашим требованиям, вы можете создать новый набор правил, или изменить существующий. Для того чтобы изменить параметры правил для действия прокси выполните следующее:

1. Нажмите  .
2. Выберите категорию:

   * H.323 ALG: General Settings

   * H.323 ALG: Access Control

   * H.323 ALG: Denied Codec

Для переноса набора правил между прокси вы можете использовать функции импорта и экспорта.

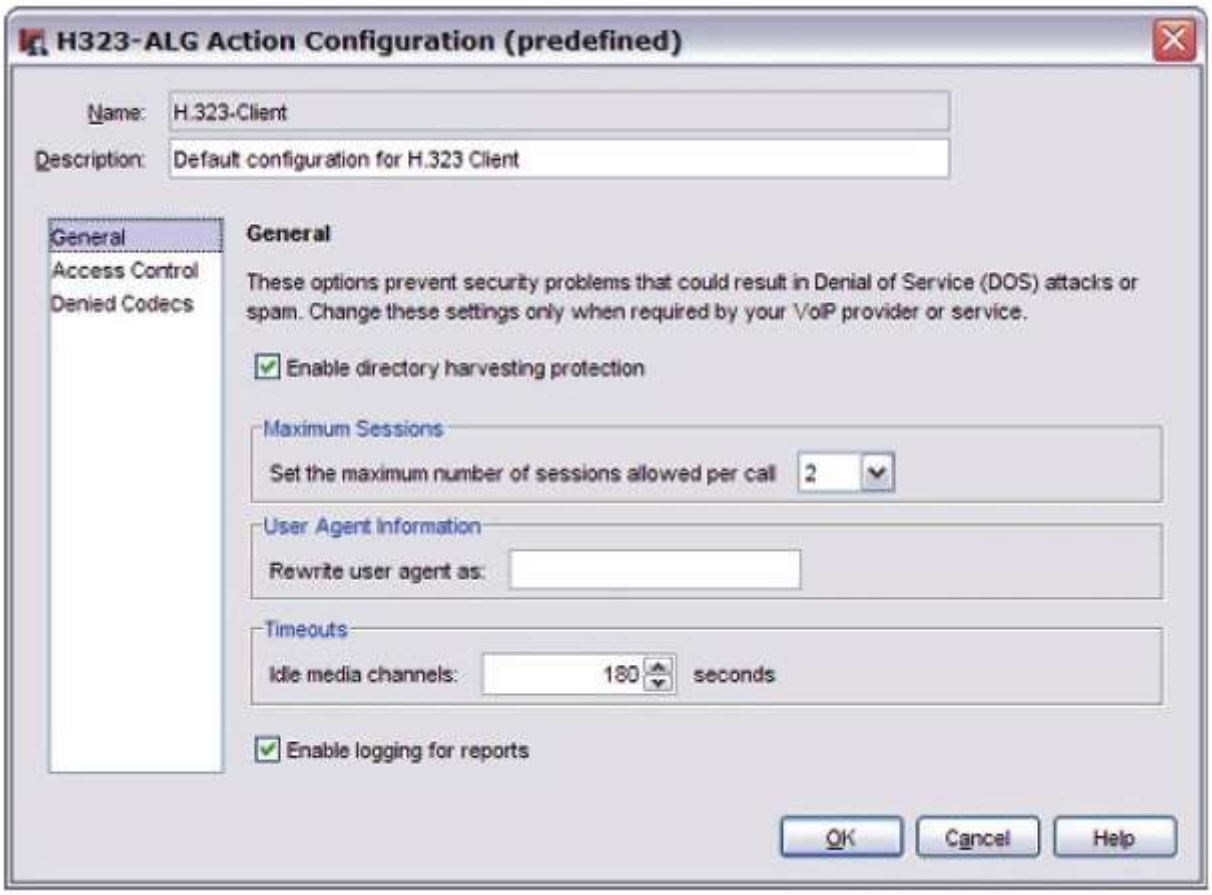
Закладка Advanced tab

В настройках прокси вы можете использовать несколько опций:

- Созданий расписаний для действий Firebox
- Добавление действия Traffic Management к политике
- Настройка обработки ICMP ошибок
- Применение правил NAT
- Включение QoS маркирования или настроек приоритизации для политики
- Настройка длительности sticky соединения для политики

H.323 ALG: General Settings

На странице **General Settings** вы можете настроить параметры безопасности и производительности для H.323 ALG (Application Layer Gateway).



Enable directory harvesting protection

Включите эту опцию для того чтобы защитить информацию о пользователях, которая хранится на VoIP привратниках, защищенных вашим Firebox, от атак хакеров. Эта опция включена по умолчанию.

Maximum sessions

Максимальное количество аудио или видео сессий, которое можно создать в одном VoIP звонке. Например, если вы установите значение этого параметра равное единице и создадите VoIP звонок с аудио и видео, то второе соединения будет блокироваться. По умолчанию максимальное количество сессий равно двум. Для каждой заблокированной сессии Firebox создает запись в журнале.

User agent information

В текстовом поле **Rewrite user agent as** новую строку агента пользователя для идентификации исходящего H.323 трафика. Для того чтобы удалить ложного агента пользователя, очистите это поле.

Timeouts

Если в течение определенного промежутка времени в VoIP аудио, видео канале или канале данных данные не передавались, то Firebox закрывает это соединение. По умолчанию величина таймаута равна 180 секундам (3 минуты), максимальная величина таймаута равна 600 seconds (10 минут). В поле **Idle media channels** введите необходимую величину таймаута.

Включение журнала для отчетов

Включите эту опцию, если вы хотите чтобы для каждого соединения под управлением H.323 ALG создавалась запись в журнале. Это опция необходима для создания подробных отчетов об H.323 трафике. Включена по умолчанию

H.323 ALG: Access Control

На странице **Access Control** вы можете создать список пользователей, которым будет разрешено передавать VoIP трафик

Enable access control for VoIP

Включите эту опцию для того чтобы включить функцию управления доступом.

Default Settings

Включите опцию **Start VoIP calls** для того чтобы разрешить всем пользователям звонить по VoIP.

Включите опцию **Receive VoIP calls** для того чтобы разрешить все пользователям принимать VoIP звонки.

Включите опцию **Log** для того чтобы для отправляемого или принимаемого H.323 VoIP звонка создавалась запись в журнале.

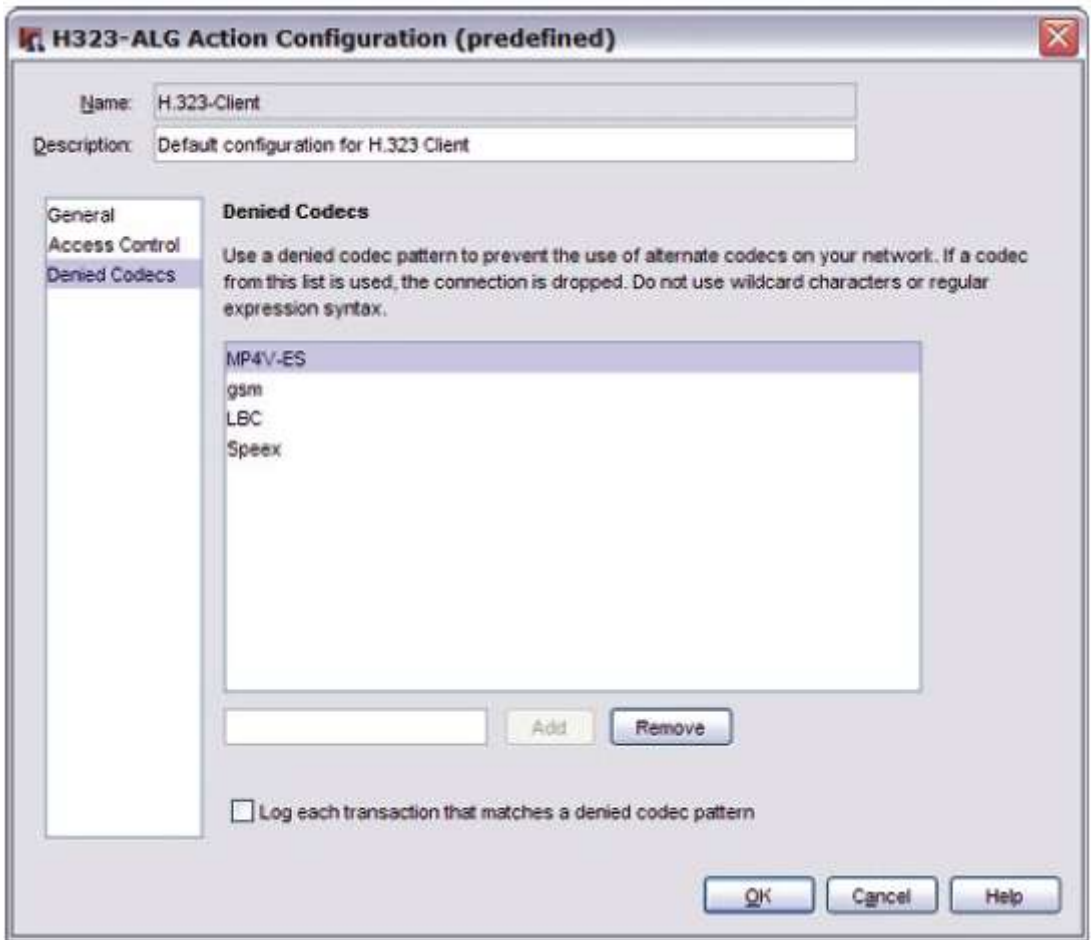
Access Levels

Для того чтобы создать исключения из правил, настроенных выше, введите имя хоста, IP адрес или адрес электронной почты. В выпадающем списке выберите уровень доступа и нажмите **Add**. Вы можете определенным пользователям только звонить (**start calls only)**, только принимать звонки (**receive calls only)**, звонить и принимать звонки (**start and receive calls)** или запретить передачу VoIP трафика (**no VoIP access)**. Эти настройки применяются только для H.323 VoIP трафика. Если вы хотите удалить исключение выберите его из списка и нажмите **Remove**.

Звонки пользователей, у которых есть специальный уровень доступа (исключение), по умолчанию записываются в журнал. Для того чтобы отключить эту функцию для этих пользователей отключите опцию **Log** рядом с исключением.

H.323 ALG: Denied Codec

На странице **Denied Codecs** вы можете настроить VoIP голосовые, видео кодеки и кодеки передачи данных, которые вы хотите заблокировать в вашей сети



Список Denied Codecs

Список запрещенных VoIP кодеков. Если создается H.323 VoIP соединение, которое использует кодек из этого списка, ваше WatchGuard устройство автоматически закрывает это соединение. По умолчанию этот список пуст. В этот список мы рекомендуем добавлять кодеки, которые требуют достаточно большой пропускной способности, представляет определенную угрозу для вашей сети, или из-за которых ваше VoIP решение некорректно работает. Например вы можете запретить G.711 или G.726 кодеки, так как им необходимо больше 32 КБит/с, или вы можете запретить кодек Speex, так как он используется неавторизованным VOIP кодеком.

Для того чтобы добавить кодек в список, в текстовом поле введите название кодека и нажмите кнопку **Add**.

Не используйте групповые символы или регулярные выражения. Названия кодеков чувствительны к регистру. Для того чтобы удалить кодек, выберите его из списка и нажмите **Remove**.

Log each transaction that matches a denied codec pattern

Включите эту опцию, если вы хотите чтобы ваш Firebox создавал запись в журнале каждый раз когда он блокирует H.323 трафик, который содержит кодек из списка запрещенных кодеков.

HTTP прокси

Протокол HTTP (Hyper Text Transfer Protocol) – протокол, который работает по механизму «запрос/ответ». HTTP клиент это обычно web браузер. HTTP сервер – это удаленный ресурс, на котором хранятся HTML файлы, изображения и другое содержимое.

Когда HTTP клиент формирует запрос, он устанавливает TCP соединения через порт 80. HTTP сервер слушает порт 80. Как только он получает запрос от клиента, сервер возвращает запрашиваемый файл, сообщение об ошибке или другую информацию. HTTP прокси – это фильтр

содержимого. Он проверяет web трафик на наличие подозрительного содержимого, которое может представлять собой вирус или другой тип атаки.

Он также может защищать ваш сервер от внешних атак.

При помощи HTTP прокси вы можете:

- Настроить величину таймаутов и ограничения на длину HTTP запросов и ответов для того чтобы избежать значительного использования прокси сетевых ресурсов, а также отразить определенные типы атак.
- Настроить текст сообщения, которое будут видеть пользователи при попытке подключения к заблокированному сайту.
- Фильтровать MIME типы web содержимого.
- Блокировать определенные шаблоны путей и URL.
- Блокировать cookies с определенных web сайтов.

Вы также можете использовать HTTP прокси с WebBlocker. TCP/UDP прокси используется для нестандартных протоколов. Если HTTP использует другой порт (не 80), то TCP/UDP прокси транслирует трафик HTTP прокси. Для более подробной информации о TCP/UDP прокси см. “TCP-UDP прокси”

Для того чтобы добавить HTTP прокси к конфигурации Firebox см. “Добавление политики прокси”. Затем, если вы захотите изменить настройки прокси, вы можете окрыть диалоговое окно **New/Edit Policy Properties** и в нем выполнить все необходимые изменения.Поля этого диалогового окна разделены на три закладки: **Policy**, **Properties**, and **Advanced**. Вдобавок закладка **Properties** содержит иконку для настройки действий прокси.

Закладка Policy

- **HTTP-proxy connections are** — выберите одну из опций: **Allowed** (Разрешены), **Denied** (Запрещены) или **Denied (send reset)** (Запрещена, отправка TCP Reset). Вы можете также настроить, кто появится в списках **From** и **To** (закладка **Policy** в настройках прокси)
- **Use policy-based routing** — См. “Настройка маршрутизации на базе политик”
- Вы также можете настроить статическую NAT или настроить балансировку нагрузки на сервер.

Закладка Properties

- Из выпадающего списка **Proxy action** укажите для кого вы создаете действие: клиента или сервера. Для более подробной информации см. “Действия прокси”
- Для настройки журнала нажмите **Logging** и выполните необходимые настройки
- Если в выпадающем списке C**onnections are** (закладка **Policy**) вы выберете Denied или Denied (send reset), вы можете заблокировать сайты, которые пытаются использовать HTTP. Для более подробной информации см. “Временная блокировка сайтов при помощи политики”
- Если вы хотите использовать таймаут ожидания (установленный Firebox или сервером аутентификации) см. “Настройка таймаута ожидания”

Прокси WatchGuard имеют предустановленные наборы правил, которые обеспечивают необходимый уровень доступности и безопасности для большинства инсталляций. Если набор правил по умолчанию не соответствует вашим требованиям, вы можете создать новый набор

правил, или изменить существующий. Для того чтобы изменить параметры правил для действия прокси выполните следующее:

1. Нажмите  .
2. Выберите категорию:

   * HTTP request: General settings

   * HTTP request: Request methods

   * HTTP request: URL paths

   * HTTP request: Header fields

   * HTTP request: Authorization

   * HTTP Response: General settings

   * HTTP Response: Header fields

   * HTTP Response: Content types

   * HTTP Response: Cookies

   * HTTP Response: Body content types

   * HTTP proxy: Exceptions

   * HTTP proxy: WebBlocker

   * HTTP proxy: Application Blocker

   * HTTP proxy: AntiVirus

   * HTTP proxy: Intrusion prevention

   * HTTP proxy: Deny message

   * Использование кэширующего прокси сервера

Для переноса набора правил между прокси вы можете использовать функции импорта и экспорта.

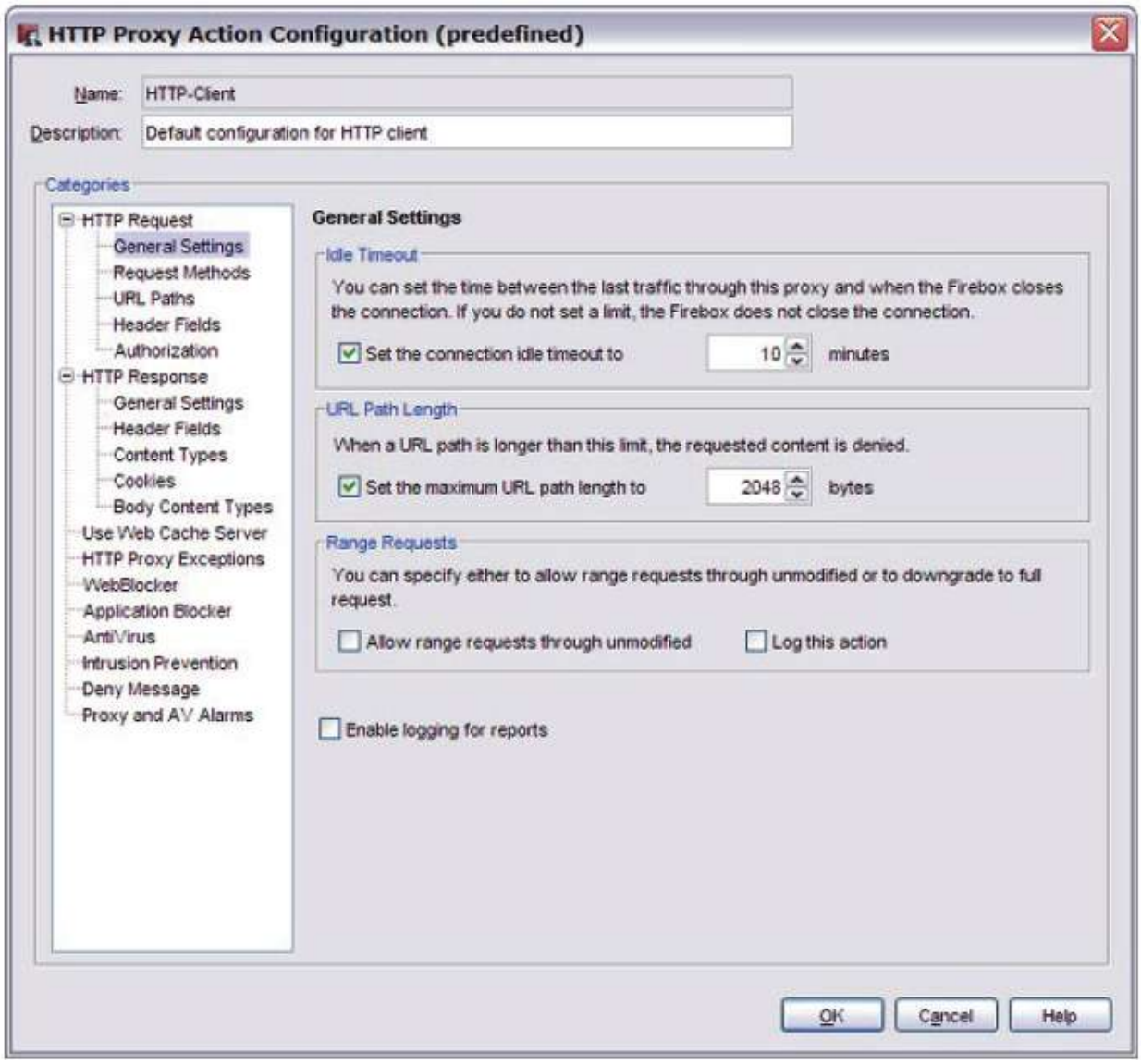
Закладка Advanced

В настройках прокси вы можете использовать несколько опций:

- Созданий расписаний для действий Firebox
- Добавление действия Traffic Management к политике
- Настройка обработки ICMP ошибок
- Применение правил NAT
- Включение QoS маркирования или настроек приоритизации для политики
- Настройка длительности sticky соединения для политики

HTTP request: General settings

На странице **General Settings** вы можете настроить базовые параметры HTTP, например таймаут ожидания и длина URL.



Set the connection idle timeout to

Включите эту опцию для того чтобы закрывать TCP сокет для HTTP трафик в случае если в течение указанного вами промежутка времени данные не передавались. Рядом в текстовом поле введите количество минут, по истечение которых прокси сгенерирует таймаут. Эта опция используется для управления производительностью. Мы рекомендуем не отключать эту опцию, так как каждая открытая TCP сессия использует некоторое количество памяти, и браузеры и серверы не всегда корректно закрывают HTTP сессии. Эта опция позволит корректно закрывать TCP сессии, тем самым освобождая память. Вы можете уменьшить величину таймаута до 5 минут, не теряя при этом в производительности.

Set the maximum URL path length to

Установите максимальное количество символов в URL. В контексте данного прокси, под термином URL понимается все, что идет после имени домена верхнего уровня, включая косую черту, но не имя хоста (www.myexample.com или myexample.com). например URL www.myexample.com/products содержит девять символов - /products. По умолчанию максимальная разрешенная длина URL составляет 2048 символов, что обычно хватает практически для всех запрашиваемых URL . Очень

длинный URL может использовать для атаки на web сервер. Минимальная длина – 15 байт. Мы рекомендуем оставить значение по умолчанию.

Allow range requests through unmodified

Включите эту опцию если вы хотите разрешить range-запросы через Firebox. Range запросы позволяют клиентам вместо всего содержимого запрашивать только определенную его часть. Например, вы можете использовать range запросы, если вы хотите загрузить только определенные страницы большого Adobe файла. Это позволит ускорить загрузку и загрузить только необходимые вам данные.

Range запрос это угроза вашей системе безопасности. Вирусы могут прятаться в любом месте файла, а range запросы позволяют делить любое содержимое на части, тем самым делая невозможным для прокси поиск вирусов в нескольких частях содержимого. Если у вас запущены Gateway AntiVirus (Gateway AV) или IPS на базе сигнатур, Fireware блокирует все range запросы в независимости от того, включена эта опция или нет.

Мы рекомендуем не включать эту опцию если правила, которые вы создали в секции Body Content Types настроек прокси, идентифицируют сигнатуры байтов внутри самого файла, а не в его заголовке.

Включите опцию **Log this action** если вы хотите при каждом выполнении прокси какого-либо действия по range-запросам создавать запись в журнале.

Enable logging for reports

Создать сообщение журнала трафика для каждой транзакции. Эта опция создает большой файл журнала, и эта информации очень важна при отражении атак на ваш брандмауэр.

Если вы не включите эту опцию, то информация о проксируемых HTTP соединениях не будет включена в Отчеты WatchGuard.

HTTP request: Request methods

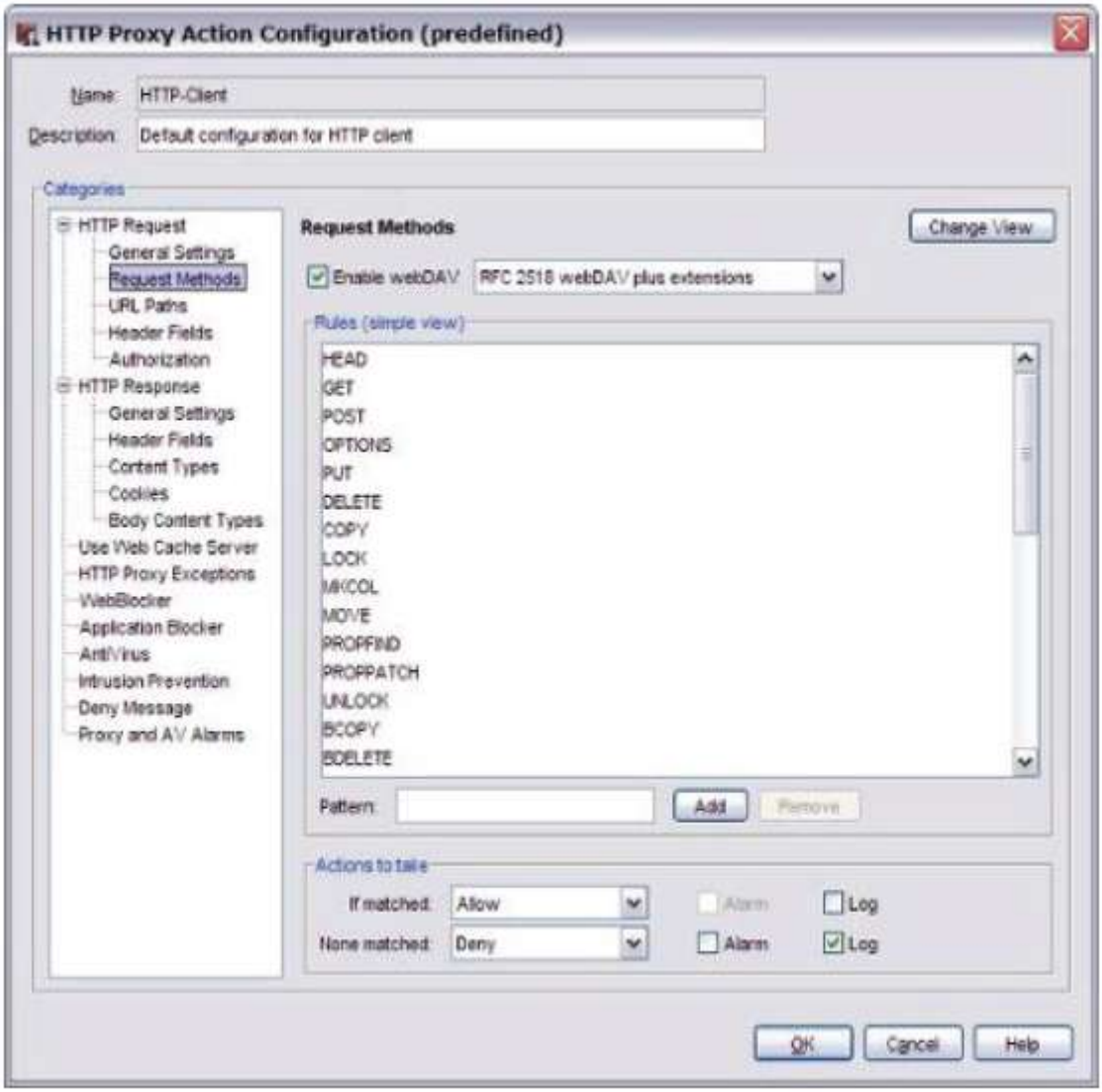
Большинство браузеров используют две метода HTTP-запроса: GET или POST. Для загрузки таких объектов как графика, HTML- или Flash-данные используется метод GET. Так как страницы содержат множество различных элементов, то для каждой страницы клиент отправляет несколько GET-запросовs. Эти элементы объединяются в одну страницу, которая отображается конечному пользователю.

Для отправки данных браузеры используют метод POST. Web-страницы собирают информацию о конечном пользователе (место проживания, адрес электронной почты, имя). Если вы отключите команду POST Firebox будет запрещать все POST-операции для web-серверов во внешней сети. Эти компоненты помогут избежать отправки вашими пользователями информации для web-сайт во внешней сети.

webDAV (Web-based Distributed Authoring and Versioning) – набор HTTP расширений, которые используются для управления файлами на удаленных серверах. WebDAV совместим с Outlook Web Access (OWA). Если webDAV расширения отключены, HTTP прокси поддерживает следующие методы: HEAD, GET, POST, OPTIONS, PUT и DELETE. Для HTTP-Server прокси поддерживает следующие методы: HEAD, GET, and POST. Прокси также поддерживает методы (отключены по умолчанию): OPTIONS, PUT и DELETE.

1. В секции **Categories** выберите **HTTP Request** > **Request Methods**.

2. Включите опцию **Enable webDAV** если вы хотите разрешить пользователям работать с этими расширениями. Протоколу webDAV также доступны некоторые расширения. Если вы включите webDAV, то выберите хотите ли вы включить только рашсирения, описанные в RFC 2518 или включить дополнительный набор расширений для максимизации взаимодействия



3. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

4. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

5. После того, как вы закончите, нажмите **OK**.

6. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

7. Введите имя нового действия и нажмите **OK**.
Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

HTTP request: URL paths

URL (Uniform Resource Locator) используется для уникальной идентификации ресурса на удаленном веб-сервере. Путь URL – это строка, которая идет сразу за доменом верхнего уровня. Вы можете использовать HTTP прокси для того чтобы блокировать сайты, которые содержат специфичный текст в URL.

Если прокси, которое используется по умолчанию, не соответствует вашим требованиям, то вы можете добавить, удалить или изменить шаблоны URL. Ниже приводятся примеры блокировки содержимого при помощи URL-пути HTTP-запроса:

- Для того чтобы заблокировать все страницы с именем хоста www.test.com, введите: www.test.com*
- Для того чтобы заблокировать все пути, которые содержат слово “sex” введите: *sex*
- Для того что заблокировать URL-пути, которые заканчиваются на “*.test”, введите: *.test

Если вы хотите фильтровать URLs при помощи набора правил HTTP request URL path, вам необходимо создать комплексный шаблон, который будет использовать регулярные выражения из расширенного вида набора правил. Намного проще и быстрее будет фильтровать типы содержимого в заголовке или теле сообщения, чем фильтровать по URL.

1. В секции **Categories** выберите **URL paths**.
2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.
3. После того, как вы закончите, нажмите **OK**.
4. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.
5. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

HTTP request: Header fields

Это правило используется для фильтрации содержимого на базе HTTP-заголовка. По умолчанию, Firebox использует правила точного совпадения, которые не пропускают заголовки Via и From, и пропускают все остальные заголовки. Это правило используется для целого заголовка, а не только для имени. Поэтому, для того найти совпадения для всех значений IP-заголовка, введите: “[имя_заголовка]:*”.

Для того чтобы найти совпадения только для некоторых значений заголовка, замените символ (*) необходимым шаблоном. Если ваш шаблон не содержит в начале символа (*), то при вводе шаблона в поле **Pattern** между двоеточием и шаблоном вставьте пробел.

Например, вводите: [*header name*]: [*pattern*], а не [*header name*]:[*pattern*].

Помните что используемые по умолчанию правила не отклоняют заголовок Referer, но содержат отключенное правило для сброса этого заголовка.

Для того чтобы включить правило, выберите **Change View**. Некоторым web-браузерам и приложениям для корректной работы необходим заголовок Referer.

1. В секции **Categories** выберите **Header Fields**.
2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”
3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.
4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

6. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

HTTP request: Authorization

Это правило используется для фильтрации содержимого по значению полей авторизации заголовка HTTP запроса. Когда web-сервер запускает процедуру “WWW-Authenticate”, он отправляет информацию об используемых методах аутентификации. Прокси устанавливает ограничения на тип аутентификации, который отправляется в запросе. При этом используются методы аутентификации, которые поддерживаются web-сервером. По умолчанию Firebox разрешает использование Basic, Digest, NTLM и Passport1.4 аутентификацию, и запрещает использование остальных методов аутентификации. Вы можете удалять, редактировать и добавлять правила в наборе правил по умолчанию.

1. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

2. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

3. После того, как вы закончите, нажмите **OK**.

4. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

5. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

HTTP Response: General settings

При помощи полей General Settings для настройки базовых параметров HTTP, таких как таймаут ожидания, ограничения на длину строки и всю длину.

1. В секции **Categories** выберите **General Settings**.

2. Для настройки ограничений для параметров HTTP включите соответствующие опции и при помощи стрелок выберите необходимые значения:

   Set the timeout to

   Промежуток времени в течение, которого HTTP прокси ожидает отправки web-страницы с сервера. Когда пользователь нажимает на гиперссылку или вводит URL в адресную строку браузера, он отправляет HTTP запрос на удаленный сервер для получения необходимого содержимого. В большинстве браузеров в строке состояния отображается «Contacting site..." или похожее сообщение. Если удаленный сервер не отвечает, HTTP клиент продолжает отправлять запрос, до тех пор пока сервер не ответит или не наступит таймаут запроса. В течение этого времени HTTP прокси продолжает выполнять мониторинг соединения и использовать ценные сетевые ресурсы.

   Set the maximum URL length to

   Устанавливает максимально допустимое число символов в строке заголовков HTTP-ответов. При помощи этого параметра вы можете защититься от атак типа «переполнение

буфера». Так как URL многих коммерческих сайтов удлиняются с течением времени, то вам в будущем придется изменить это значение.

Set the maximum total length to

Устанавливает максимальную длину заголовков HTTP-ответов. Если общая длина заголовков превышает максимальное значение, то HTTP-ответ блокируется.

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

6. Введите имя нового действия и нажмите **OK**.
Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. "Предопределенные и пользовательские действия прокси"

HTTP Response: Header fields

Устанавливает разрешенные поля заголовков HTTP-ответов. RFC 2616 содержит большинство заголовков HTTP-ответов, которые разрешены в используемой по умолчанию конфигурации. Для более подробной информации, см.:

http://www.ietf.org/rfc/rfc2616.txt

1. В секции Categories выберите Header Fields.

2. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

3. После того, как вы закончите, нажмите **OK**.

4. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

5. Введите имя нового действия и нажмите **OK**.
Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. "Предопределенные и пользовательские действия прокси"

HTTP Response: Content types

Когда web-сервер отправляет HTTP-трафик, он обычно добавляет в ответ тип MIME. HTTP-заголовок потока данных содержит тип MIME, который добавляется перед отправкой данных. Формат MIME типа - **тип/подтип**. Например, если вы хотите разрешить загрузку изображений JPEG, вам необходимо добавить `image/jpg` в прокси. Вы также можете использовать (*) в качестве группового символа. Для того чтобы разрешить все изображения, вам необходимо добавить `image/*`.

Определенные типы содержимого, загружаемого пользователями, могут представлять угрозу безопасности вашей сети. Другие типы содержимого могут значительно снизить производительность ваших пользователей. По умолчанию Firebox разрешает некоторые безопасные типы содержимого и запрещает MIME содержимого, которое не имеет типа. Некоторые web-серверы возвращают некорректные MIME типы для того чтобы обойти правила обработки содержимого. Если настройки прокси по умолчанию не соответствуют вашим

требованиям, вы можете выполнить необходимые изменения. Для того чтобы посмотреть список зарегистрированных MIME типов содержимого, зайдите на сайт :

http://www.iana.org/assignments/media-types

Добавление, удаление или редактирование типов содержимого

1. В секции **Categories** выберите **Content Types**.

2. Добавьте, удалите или измените необходимое количество правил

3. Для того чтобы добавить тип содержимого нажмите на кнопку **Predefined**. Откроется диалоговое окно **Select Content Type**.

4. Выберите тип содержимого, которое вы хотите добавить, и нажмите **OK**. Новые типы появятся в поле **Rules**.

5. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

6. После того, как вы закончите, нажмите **OK**.

7. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

8. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

Разрешение web сайтов с отсутствующими типами содержимого

По умолчанию Firebox запрещает MIME содержимое, которое не имеет определенный тип. В большинстве случаев мы рекомендуем не трогать эту опцию. Сайты, которые в своих HTTP ответах не поддерживают стандартные MIME типы, не соответствуют рекомендации RFC и могут представлять серьезную опасность вашей сети. Однако в некоторых компаниях сотрудникам разрешают доступ к сайтам, которые не имеют стандартные типы содержимого. Поэтому вам необходимо внести изменения в конфигурацию вашего прокси

1. В секции **Categories** выберите **Content Types**.

2. Нажмите **Change View**.

3. В списке **Rules** включите опцию рядом с правилом **Allow (none)**.

HTTP Response: Cookies

HTTP cookies – маленькие файлы, которые web-серверы помещают на web-клиента. Cookies используются для мониторинга страниц, которые посещает клиенты, и заставляют web-сервер отправлять клиенту больше страниц в правильной последовательности.

Web-серверы используют cookies для сбора информации о пользователе. Многие web-сайты используют cookies для аутентификации и других операций, и они не могут правильно работать без cookies.

Это правило используется для управления cookies в HTTP-ответов. Вы можете настроить правила для **strip** cookies, в зависимости от требований вашей сети. По умолчанию, правило для прокси-действий HTTP-Server и HTTP-Client разрешает все cookies.

Правило Cookies ищет пакеты на базе домена, которым ассоциируется с cookie. Домен может быть указан в cookie. Если домен в cookie не указан, прокси в первом запросе использует имя хостат.

Поэтому для того чтобы, например, заблокировать все cookies для сайта nosy-adware-site.com, создайте правило с шаблоном: “*.nosyadware-site.com”.

Если вы хотите заблокировать cookies со всех поддоменов сайта, введите (*) перед и после имени домена. Например «`*google.com*`» заблокирует все поддомены google.com (images.google.com и mail.google.com.

Изменение параметров для cookies

1. В секции **Categories** выберите **Cookies**.

2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”.

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

6. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

HTTP Response: Body content types

Это правило используется для управления содержимым HTTP-ответов. Конфигурация Firebox запрещает использование Java-аплеты, Zip архивы, Windows EXE/DLL файлы и CAB-файлы.

Используемое по умолчанию прокси-действие для исходящих HTTP-запросов (HTTP-Client) разрешает все остальные типы содержимого ответа.

Мы рекомендуем вам проверять типы файлов, которые используют в вашей организации, и разрешать использовать только те типы файлов, которые необходимы в вашей сети.

1. В секции **Categories** выберите **Body Content Types**.

2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

3. Если вы хотите типы содержимого нажмите кнопку **Predefined**

4. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

5. После того, как вы закончите, нажмите **OK**.

6. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

7. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

Исключения HTTP прокси

Вы можете использовать исключения HTTP прокси для того чтобы игнорировать правила HTTP прокси для определенных сайтов. Трафик, который совпадает с исключением HTTP прокси, все равно обрабатывается стандартными средствами HTTP прокси. Однако при обработке трафика некоторые параметры прокси игнорируются.

Не включены в настройки Прокси

Следующие параметры прокси игнорируются:

- HTTP request: range-запросы, длина URL, все методы запроса, все URL, заголовки запроса*, совпадения с шаблонами авторизации
- HTTP response: заголовки ответа*, типы содержимого, cookies, типы содержимого тела сообщения

* Заголовки запроса и ответа обрабатываются HTTP прокси даже если трафик совпадает с исключением HTTP прокси. Если во время обработки ошибки не происходит, все заголовки разрешаются. Сканирование антивирусом, IPS сканирование и WebBlocker не применяется к трафику, который совпадает с исключением HTTP прокси.

Включены в настройки Прокси

Следующие параметры не игнорируются:

- HTTP request: таймаут ожидания
- HTTP response: таймаут ожидания, лимит максимальной длины строки, лимит максимальной полной длины

Обработка transfer-encoding все также используется для того чтобы разрешить прокси определять тип содержимого. HTTP прокси запрещает любую некорректную или неправильно сформированную кодировку.

Создание исключений

В качестве исключений HTTP прокси вы можете добавить имена хостов или шаблоны. Например, если вы заблокируете все web-сайты, которые заканчиваются на .test, но хотите разрешить пользователям подключаться к сайту www.abc.test, вы можете добавить сайт www.abc.test в качестве исключения HTTP прокси.

Вам необходимо указать IP-адрес или имя домена сайта, который вы хотите разрешить. Имя домена (хоста) является частью URL, который заканчивается на .com, .net, .org, .biz, .gov или .edu. Имена доменов также могут заканчиваться кодом страны, например .de (Германия) или .jp (Япония). Для того чтобы добавить имя домена введите шаблон URL без "http://". Например, для того чтобы разрешить вашим пользователям подключаться к сайту WatchGuard по адресу http://www.watchguard.com, введите `www.watchguard.com`.

Если вы хотите разрешить все поддомены, которые содержат watchguard.com, вы можете использовать (*) в качестве группового символа. Например для того чтобы разрешить вашим пользователям подключаться к сайту watchguard.com, www.watchguard.com и support.watchguard.com введите `*watchguard.com`.

1. В секции **Categories** выберите **HTTP Proxy Exceptions**.
2. В поле слева от кнопки **Add** введите имя хоста или шаблон имени хоста. Нажмите **Add**. Повторите эту процедуру для всех исключений, которые вы хотите добавить.

3. Если вы хотите генерировать сообщение журнала каждый раз когда HTTP прокси выполняет действие над исключением прокси включите опцию Log each transaction that matches an HTTP proxy exception.

4. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

5. После того, как вы закончите, нажмите **OK**.

6. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

7. Введите имя нового действия и нажмите **OK**.
Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

HTTP proxy: WebBlocker

Вы можете подключить конфигурацию WebBlocker к вашему HTTP прокси.

- Выберите конфигурацию из выпадающего списка.
- Нажмите кнопку для создания новой конфигурации WebBlocker.

Для более подробной информации см. “WebBlocker” и “Приступая к работе с WebBlocker”

HTTP proxy: Application Blocker

Также для обработки и анализа IM (Instant Messaging) и p2p трафика вы можете к вашему прокси подключить конфигурацию Application Blocker.

- Выберите конфигурацию из выпадающего списка.
- Нажмите кнопку для создания новой конфигурации Application Blocker.

HTTP proxy: AntiVirus

Если вы включили Gateway AntiVirus, то вам необходимо настроить действия, которыебудут выполняться если был обнаружен вирус или ошибка в электронном письме (SMTP или POP3 прокси), web-странице (HTTP прокси), загружаемых/выгружаемых файлах (FTP прокси).

- Для активации Gateway AntiVirus из настроек прокси см. “Активация Gateway AntiVirus из настроек прокси”
- Для активации Gateway AntiVirus в меню Subsciption Services утилиты Policy Manager см. “Активация Gateway AntiVirus при помощи мастера”
- Для настройки Gateway AntiVirus для FTP прокси см. “Настройка действий Gateway AntiVirus”

После того, как вы активируете Gateway AntiVirus, вам необходимо выбрать действие, которое будет выполнено в случае обнаружения вируса в загружаемом или выгружаемом файле. Вы можете выбрать следующие действия:

Allow

Разрешить отправку вложения получателю, если даже оно содержит вирус.

Drop

Отбрасывает пакет и разрывает соединение. Источнику пакета не получает никакого уведомления.

Block

Блокирует пакет и добавляет IP адрес отправителя в список Blocked Sites.

HTTP proxy: Intrusion prevention

Если вы включили IPS вам необходимо выбрать действия, которые необходимы для поиска и отражения попыток проникновения в вашу сеть.

Несмотря на то, что вы можете активировать IPS в настройках прокси, будет проще активировать его в меню Subscription Services утилиты Policy Manager

Для активации IPS в настройках HTTP прокси см. “Активация и настройка IPS для TCP-UDP”

HTTP proxy: Deny message

Firebox по умолчанию использует deny-сообщение, которое заменяет запрещенное содержимое. Вы можете изменить текст этого сообщения. Вы можете использовать deny-сообщение в формате HTML. Первая строка deny-сообщения это секция HTTP-заголовка.

Между первой строкой и телом сообщения должна быть пустая строка.

Вы будете видеть deny-сообщение в вашем браузере каждый раз когда вы пытаетесь выполнить запрос, который не разрешен HTTP прокси.

Вы также будете видеть это сообщение, когда ваш запрос разрешен, но HTTP прокси заблокировал ответ с удаленного сервера. Например, если пользователь пытается загрузить файл .exe и вы заблокировали этот тип файла, пользователь увидить deny-сообщение в своем браузере.

Если пользователь пытается загрузить web-страницу, которая содержит неизвестный тип содержимого и политика прокси блокирует неизвестные MIME типы, то он увидит deny-сообщение в своем браузере. Вы можете посмотреть Deny-сообщение по умолчанию в поле **Deny Message**. Для того чтобы изменить текст этого сообщения, используйте следующие переменные:

%(transaction)%

Добавляет Request или Response в зависимости от того, в каком направлении была заблокирована транзакция.

%(reason)%

Причина отклонения содержимого.

%(method)%

Метод заблокированного запроса.

%(url-host)%

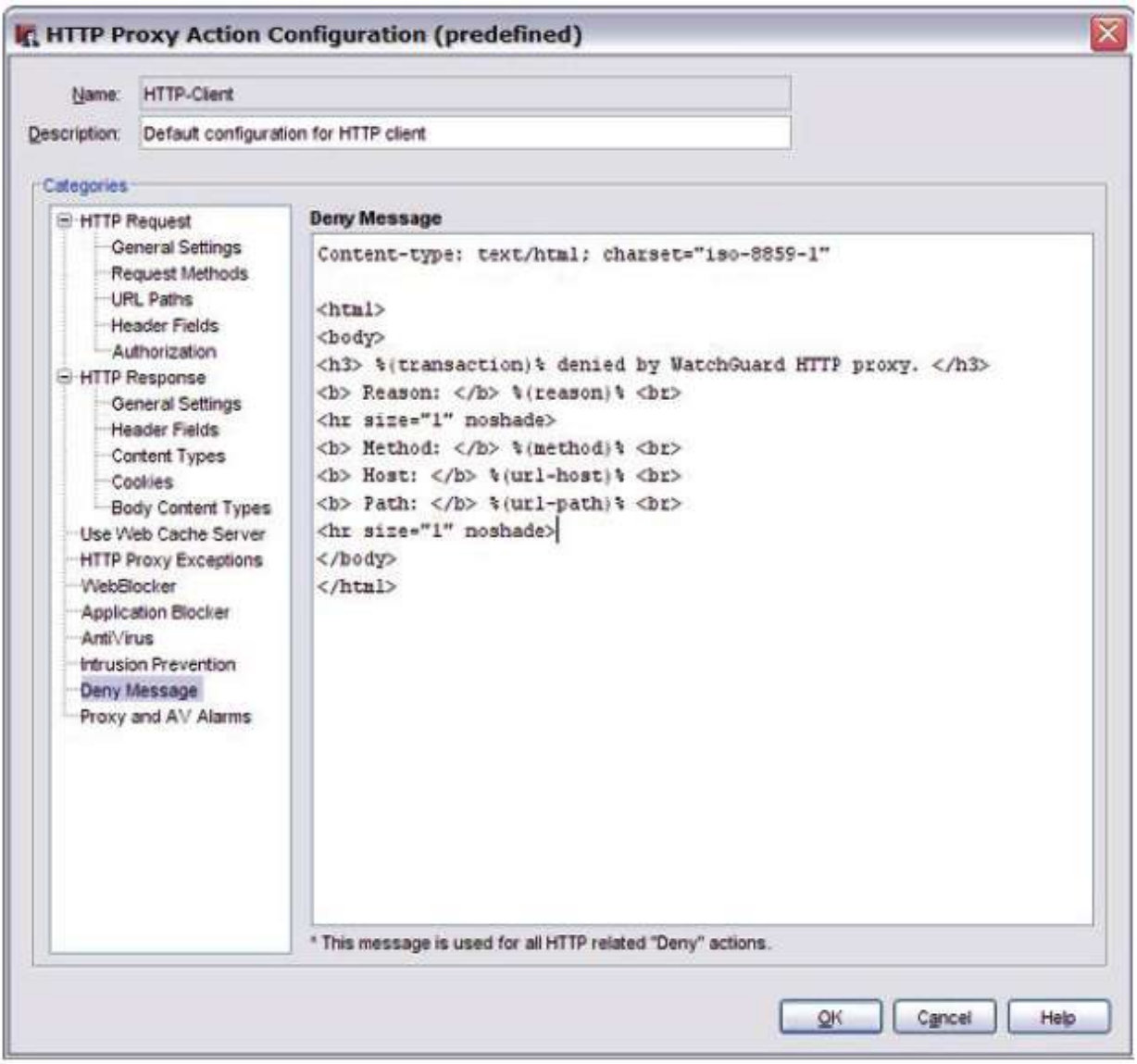
Имя хоста заблокированного URL. Если имя хоста не было включено, то добавляется IP-адрес сервера.

%(url-path)%

Путь заблокированного URL

Для того чтобы настроить deny сообщение выполните следующее:

1. В секции **Categories** выберите **Deny Message**.



2. В поле **Deny Message** введите текст deny-сообщения.

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

6. Введите имя нового действия и нажмите **OK**.
Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

Разрешение Windows обновлений через HTTP прокси

Серверы Windows Update идентифицируют отправляемое ими содержимое, как бинарный поток (поток октетов), который по умолчанию блокируется правилами HTTP прокси. Для того для того, чтобы разрешить Windows обновления через HTTP прокси, вам необходимо в набор правил прокси HTTP-Client добавить исключения для серверов Windows Update.

1. Убедитесь, что ваш Firebox не блокирует исходящие подключения через порт 443 и 80. По этим портам компьютеры подключаются к серверам Windows Update.

2. В секции **Categories** выберите **HTTP Proxy Exceptions**.

3. В текстовом поле слева от кнопки **Add** введите все домены из списка, приведенного ниже, и затем нажмите **Add**:

   windowsupdate.microsoft.com

   download.windowsupdate.com

   update.microsoft.com

   download.microsoft.com

   ntservicepack.microsoft.com

   wustat.windows.com

   v4.windowsupdate.microsoft.com

   v5.windowsupdate.microsoft.com

4. Нажмите **OK**.

Если вы все еще не можете загружать обновления Windows

Если у вас несколько политик HTTP прокси, убедитесь, что вы добавили HTTP исключения в корректную политику и действие прокси. Microsoft не ограничивается только этими доменами. Посмотрите журнал для заблокированного трафика. Если у вас нет Сервера Журналов WatchGuard запустите Windows Update и посмотрите сообщения журнала Firebox (Traffic Monitor). Ищите трафик, который был заблокирован HTTP прокси. Для него в сообщениях журнала будет указан домен. Добавьте этот домен в список исключений HTTP прокси и снова запустите Windows Update.

Использование кэширующего прокси сервера

Так как ваши пользователи могут часто заходить на одни и те же сайты, то кэширующий прокси сервер может значительно увеличить скорость передачи данных и снизить количество данных, передаваемых при установлении соединения с удаленными сайтами. Несмотря на то, что HTTP прокси не кэширует содержимое, вы можете использовать внешний кэширующий прокси сервер. При этом все прокси Firebox и правила WebBlocker продолжают работать.

Подключение Firebox к прокси серверу то же самое, что и подключение к клиенту. Firebox изменяет GET запрос следующим образом:

GET / HTTP/1.1 на GET www.mydomain.com / HTTP/1.1 и отправляет этот запрос на кэширующий прокси сервер. Прокси передает этот запрос дальше на указанный в GET запросе удаленный сайт.

Для того чтобы настроить внешний кэширующий прокси сервер:

1. Настройте внешний прокси сервер (например Microsoft Proxy Server 2.0)

2. Откройте Policy Manager.

3. Два раза нажмите на иконку политики HTTP-proxy.
   Откроется диалогое окно Edit Policy Properties.

4. Выберите закладку **Properties**.

5. Нажмите  .

6. В секции **Categories** выберите **Use Web Cache Server**.

7. Включите опцию **Use external caching proxy server for HTTP traffic**.

8. Введите IP адрес и порт внешнего прокси сервера.

9. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

10. После того, как вы закончите, нажмите **OK**.

11. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

12. Введите имя нового действия и нажмите **OK**.
Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. "Предопределенные и пользовательские действия прокси"

HTTPS прокси

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) – это протокол, работающий по механизму «запрос/ответ», который используется для защищенного обмена данными между клиентом и сервером. Вы можете использовать HTTPS прокси для защиты вашего web сервера, защищенного вашим Firebox, или для проверки HTTPS запросов, отправленных вашими пользователями. По умолчанию когда пользователь создает HTTPS запрос, он сначала устанавливает TCP (Transmission Control Protocol) соединение через порт 443. Большинство HTTPS серверов слушают входящие запросы на порту 443.

HTTPS более защищен чем HTTP, так как он использует цифровые сертификаты для шифрования и расшифрования запросов пользователей и страниц, возвращаемых сервером. Так как HTTPS трафик зашифрован, то для его проверки Firebox должен сначала его расшифровать. После того, как Firebox все проверит, он снова зашифровывает трафик при помощи сертификата и отправляет его получателю.

Для этой функции вы можете экспортировать созданный по умолчанию сертификат или импортировать другой сертификат. Если для проверки трафика вы используете HTTPS прокси, мы вам рекомендуем эскпортировать созданный по умолчанию сертификат и разослать его своим пользователям для того чтобы они не получали предупреждений о недоверенных сертификатах. Если вы используете HTTPS прокси для защиты web-сервер, который обрабатывает запросы из внешней сети, мы рекомендуем импортировать существующий сертификат сервера.

Если HTTPs клиент использует другой порт (не 443), то TCP/UDP прокси транслирует трафик HTTPs прокси. Для более подробной информации см. "TCP-UDP прокси"

Затем, если вы захотите изменить настройки прокси, вы можете окрыть диалоговое окно **New/Edit Policy Properties** и в нем выполнить все необходимые изменения.Поля этого диалогового окна разделены на три закладки: **Policy**, **Properties**, and **Advanced**. Вдобавок закладка **Properties** содержит иконку для настройки действий прокси.

Закладка Policy

- **HTTPS-proxy connections are** — выберите одну из опций: **Allowed** (Разрешены), **Denied** (Запрещены) или **Denied (send reset)** (Запрещена, отправка TCP Reset). Вы можете также настроить, кто появится в списках **From** и **To** list (закладка **Policy** в настройках прокси

- **Use Policy-Based Routing** - См. "Настройка маршрутизации на базе политик"

- Вы также можете настроить статическую NAT или настроить балансировку нагрузки на сервер.

Закладка Properties

- Из выпадающего списка **Proxy action** укажите для кого вы создаете действие: клиента или сервера. Для более подробной информации см. “Действия прокси”
- Для настройки журнала нажмите **Logging** и выполните необходимые настройки
- Если в выпадающем списке C**onnections are** (закладка **Policy**) вы выберете Denied или Denied (send reset), вы можете заблокировать сайты, которые пытаются использовать HTTP. Для более подробной информации см. “Временная блокировка сайтов при помощи политики”
- Если вы хотите использовать таймаут ожидания (установленный Firebox или сервером аутентификации) см. “Настройка таймаута ожидания”

Прокси WatchGuard имеют предустановленные наборы правил, которые обеспечивают необходимый уровень доступности и безопасности для большинства инсталляций. Если набор правил по умолчанию не соответствует вашим требованиям, вы можете создать новый набор правил, или изменить существующий. Для того чтобы изменить параметры правил для действия прокси выполните следующее:

1. Нажмите  .
2. Выберите категорию:

   * HTTPS proxy: Content inspection

   * HTTPS proxy: Certificate names

   * HTTPS proxy: WebBlocker

   * HTTPS proxy: General settings

   * Тревоги прокси и AV

Вы можете переносить правила между прокси посредством функции импорта/ экспорта. Для более подробной информации см. “Импорт и экспорт наборов правил”

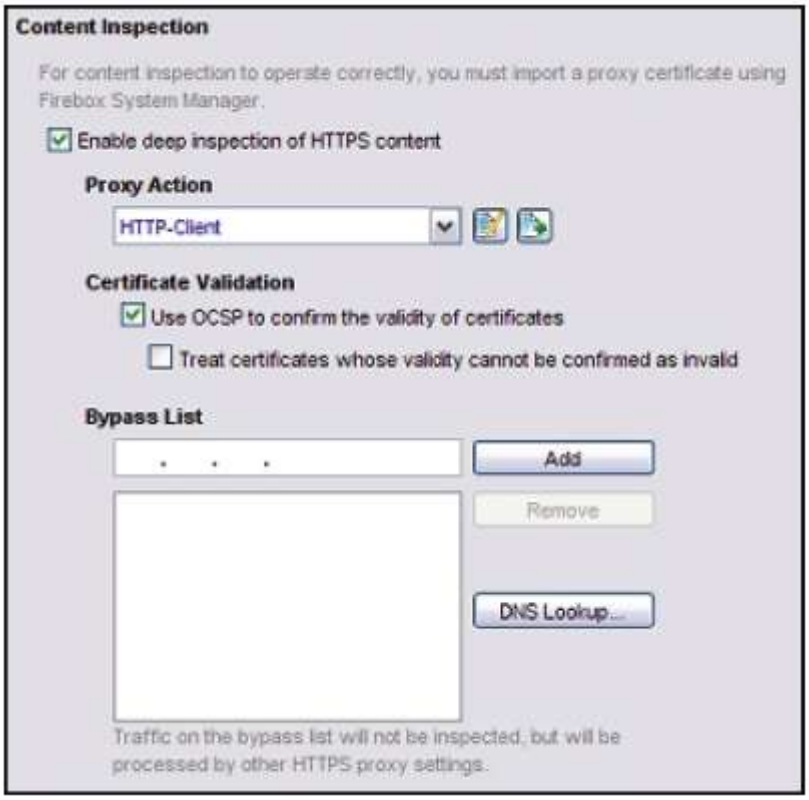
Закладка Advanced

В настройках прокси вы можете использовать несколько дополнительных опций:

- Созданий расписаний для действий Firebox
- Добавление действия Traffic Management к политике
- Настройка обработки ICMP ошибок
- Применение правил NAT
- Включение QoS маркирования или настроек приоритизации для политики
- Настройка длительности sticky соединения для политики

HTTPS proxy: Content inspection

На странице **Content Inspection** вы можете включить и настроить процедуру углубленной проверки HTTPS содержимого



Enable deep inspection of HTTPS content

Если эта опция включена, то Firebox расшифровывает HTTPS трафик, проверяет его содержимое и снова зашифровывает трафик при помощи другого сертификата. Содержимое проверяется выбранной вами политикой HTTP прокси

Если у вас в сети также передается другой трафик, который использует порт HTTPS, например SSL VPN трафик, мы рекомендуем аккуратно использовать эту опцию. HTTPS прокси проверяет весь трафик через TCP порт 443. Для корректной передачи другого трафика, мы рекомендуем добавить источники этого трафика в список Bypass. Для более подробной информации см. Следующие разделы далее в этой главе.

По умолчанию сертификат, который используется для шифрования трафика генерируется автоматически устройством Firebox. Вы также для этого можете загрузить свой сертификат. Если исходный web-сайт или ваш web сервер имеет самоподписанный или невалидный сертификат, или сертификат был подписан Центром Сертификации (ЦС), который Firebox не может распознать, то пользователям откроется предупреждение по поводу сертификата браузера. Сертификаты, которые не могут быть корректно перевыпущены, отображаются следующим образом: *Fireware HTTPS Proxy: Unrecognized Certificate* или просто *Invalid Certificate*.

Мы рекомендуем импортировать используемый вами сертификат, а также другие сертификаты, которым пользователи должны доверять, на компьютер каждого пользователя. Если компьютер пользователя автоматически не доверяет сертификату, который используется для углубленной проверки содержимого HTTPS трафика, то на нем пользователь увидит предупреждение о безопасности, а также определенные сервисы, например Windows Update, будут работать некорректно.

Некоторые программы (например IM клиент), хранит секретные копии необходимых сертификатов и не использует хранилище сертификатов ОС. Если эти программы не умеют импортировать

сертификаты доверенного ЦС, то при включенной функции углубленной проверки содержимого они могут некорректно работать.

Для более подробной информации см. “Certificates and the Certificate Authority” on page 695 or “Use Certificates for the HTTPS Proxy” on page 716.

Proxy action

Действие политики HTTP прокси, которое будет выполнять устройство Firebox при проверке расшифрованного HTTPS содержимого. Если вы включите функции проверки содержимого, параметры WebBlocker действия HTTP прокси будут использоваться вместо параметров действия HTTPS прокси. Если вы добавите IP адреса в список Bypass, трафик с этих IP адресов будет фильтроваться WebBlocker, настройки которого определены в HTTPS прокси

Use OCSP to confirm the validity of certificates

Включите эту опцию, если вы хотите чтобы Firebox по протоколу OCSP (Online Certificate Status Protocol) автоматически проверял состояние сертификатов. Если эта опция включена, Firebox извлекает информацию из сертификата и отправляет ее на OCSP сервер, который хранит текущее состояние этого сертификата. Если OCSP сервер сообщает о том, что этот сертификат был отозван, Firebox этот сертификат отключает.

Если вы включите эту опцию, то при передаче трафика будет небольшая задержка (несколько секунд), необходимая для запроса состояния сертификата на OCSP сервере. Firebox для наиболее часто посещаемых сайтов может хранить от 300 до 3000 ответов от OCSP сервера в кэше. Количество ответов, хранимых в КЭШе, определяется моделью вашего Firebox.

Treat certificates whose validity cannot be confirmed as invalid

Если вы включите эту опцию и OCSP сервер не присылает ответ на запрос о состоянии сертификата, Firebox считает этот сертификат невалидным или отозванным. При включенной опции сертификаты могут быть помечены, как отозванные или невалидные, если у вас возникли проблемы с подключением или возникла ошибка при маршрутизации запроса на сервер.

Bypass list

Список содержит источники, трафик с которых не проверяется устройством Firebox. Для того чтобы добавить web сайт или имя хоста, введите его IP адрес в текстовом поле и нажмите кнопку **Add**.

Если вы включите функции проверки содержимого, параметры WebBlocker действия HTTP прокси будут использоваться вместо параметров действия HTTPS прокси. Если вы добавите IP адреса в список Bypass, трафик с этих IP адресов будет фильтроваться WebBlocker, настройки которого определены в HTTPS прокси

Для оперативного поиска IP адресов сайтов или хостов вы можете использовать функцию DNS Lookup.

1. Нажмите кнопку **DNS Lookup**.

2. Введите имя домена или хоста и нажмите **Lookup**. Если имя домена или хоста валиден, его IP адреса появятся в списке.

3. Выберите все необходимые IP адреса и нажмите **OK**.

4. Для того чтобы выбрать все IP адреса отметьте флаг в верхней части списка.

HTTPS proxy: Certificate names

Имена сертификатов используются для фильтрации содержимого для всего сайта. Если домен HTTPS сертификата совпадает с одной из записей в этом списке, Firebox может заблокировать или разрешить доступ к этому сайту.

Например, если вы хотите запретить трафик с любого сайта в домене *example.com*, добавьте правило Certificate Names с шаблоном *.example.com и в поле **If matched** выберите **Deny**.

1. В секции **Categories** выберите **Certificate Names**.

2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

6. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

HTTPS proxy: WebBlocker

В настройках HTTPs прокси вы можете включить WebBlocker для блокировки определенных типов содержимого.

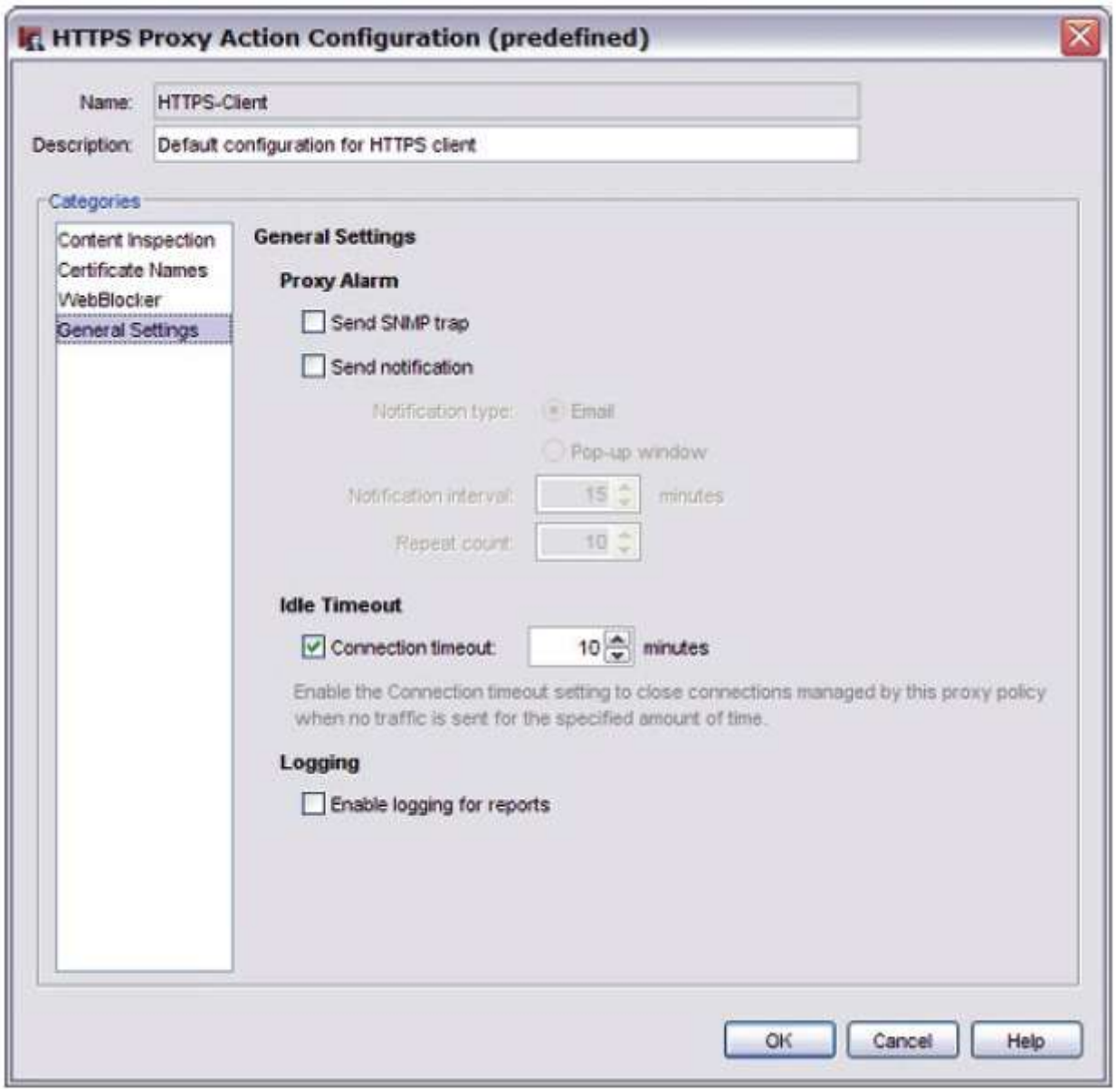
- Выберите конфигурацию из выпадающего списка.

- Нажмите кнопку для создания новой конфигурации WebBlocker.

Для более подробной информации см. “WebBlocker” и “Приступая к работе с WebBlocker”

HTTPS proxy: General settings

На странице **General Settings** вы можете настроить базовые параметры HTTP.



Proxy alarm

Вы можете настроить ваш прокси, чтобы он отправлял SNMP ловушку, уведомление администратору сети, или одновременно и то и другое. Уведомление может быть в виде электронного письма или всплывающего окна на компьютере администратора

Idle timeout

Выберите эту опцию для того чтобы управлять промежутком времени, в течение которого HTTPs прокси ждет от клиента запроса на внешний веб-сервер. Если этот промежуток времени превышает установленное вами значение, HTTP прокси закрывает соединение. В соответствующем поле введите количество минут, по истечение которых прокси сгенерирует таймаут

Enable logging for reports

Создать сообщение журнала трафика для каждой транзакции. Эта опция создает большой файл журнала, и эта информации очень важна при отражении атак на ваш брандмауэр. Если вы не

включите эту опцию, то информация о проксируемых HTTPS соединениях не будет включена в Отчеты WatchGuard Reports.

POP3 прокси

POP3 (Post Office Protocol v.3) – это протокол для передачи электронных писем с сервера электронной почты на почтовый клиент по TCP соединению через порт 110.

Большинство почтовых клиентов используют POP3. При помощи POP3 почтовый клиент подключается к серверу электронной почты и проверяет наличие новых сообщений. Если он находит новое сообщение, он загружает его на локального клиента. После того, как сообщение будет получено клиентом, соединение с сервером закрывается.

При помощи POP3 прокси вы можете:

- Установить ограничения на длину строки и величину таймаута для того чтобы POP3 прокси не использовало слишком много ресурсов сети, а также для защиты от некоторого типа атак.
- Выбрать текст сообщения, которое будут видеть пользователи, в случае если отправленная им почта заблокирована.
- Фильтровать содержимое, включенное в электронное письмо с MIME типами.
- Блокировать определенные URL.

Для того чтобы добавить POP3 прокси к конфигурации Firebox см. “Добавление политики прокси”. Затем, если вы захотите изменить настройки прокси, вы можете окрыть диалоговое окно **New/Edit Policy Properties** и в нем выполнить все необходимые изменения.Поля этого диалогового окна разделены на три закладки: **Policy**, **Properties**, and **Advanced**. Вдобавок закладка **Properties** содержит иконку для настройки действий прокси.

Закладка Policy

- **POP3-proxy connections are** — выберите одну из опций: **Allowed** (Разрешены), **Denied** (Запрещены) или **Denied (send reset)** (Запрещена, отправка TCP Reset). Вы можете также настроить, кто появится в списках From и To list (закладка Policy в настройках прокси)
- **Use policy-based routing —** См. “Настройка маршрутизации на базе политик”
- Вы также можете настроить статическую NAT или настроить балансировку нагрузки на сервер.

Закладка Properties

- Из выпадающего списка **Proxy action** укажите для кого вы создаете действие: клиента или сервера. Для более подробной информации см. “Действия прокси”
- Для настройки журнала нажмите **Logging** и выполните необходимые настройки
- Если в выпадающем списке C**onnections are** (закладка **Policy**) вы выберете Denied или Denied (send reset), вы можете заблокировать сайты, которые пытаются использовать HTTP. Для более подробной информации см. “Временная блокировка сайтов при помощи политики”
- Если вы хотите использовать таймаут ожидания (установленный Firebox или сервером аутентификации) см. “Настройка таймаута ожидания”

Прокси WatchGuard имеют предустановленные наборы правил, которые обеспечивают необходимый уровень доступности и безопасности для большинства инсталляций. Если набор

правил по умолчанию не соответствует вашим требованиям, вы можете создать новый набор правил, или изменить существующий. Для того чтобы изменить параметры правил для действия прокси выполните следующее:

1. Нажмите  .
2. Выберите категорию:

   * POP3 proxy: General settings

   * POP3 proxy: Authentication

   * POP3 proxy: Content types

   * POP3 proxy: File names

   * POP3 proxy: Headers

   * POP3 proxy: AntiVirus responses

   * POP3 proxy: Deny message

   * POP3 proxy: Intrusion prevention

   * POP3 proxy: spamBlocker

   * Тревоги прокси и AV

Вы можете переносить правила между прокси посредством функции импорта/ экспорта. Для более подробной информации см. “Импорт и экспорт наборов правил”

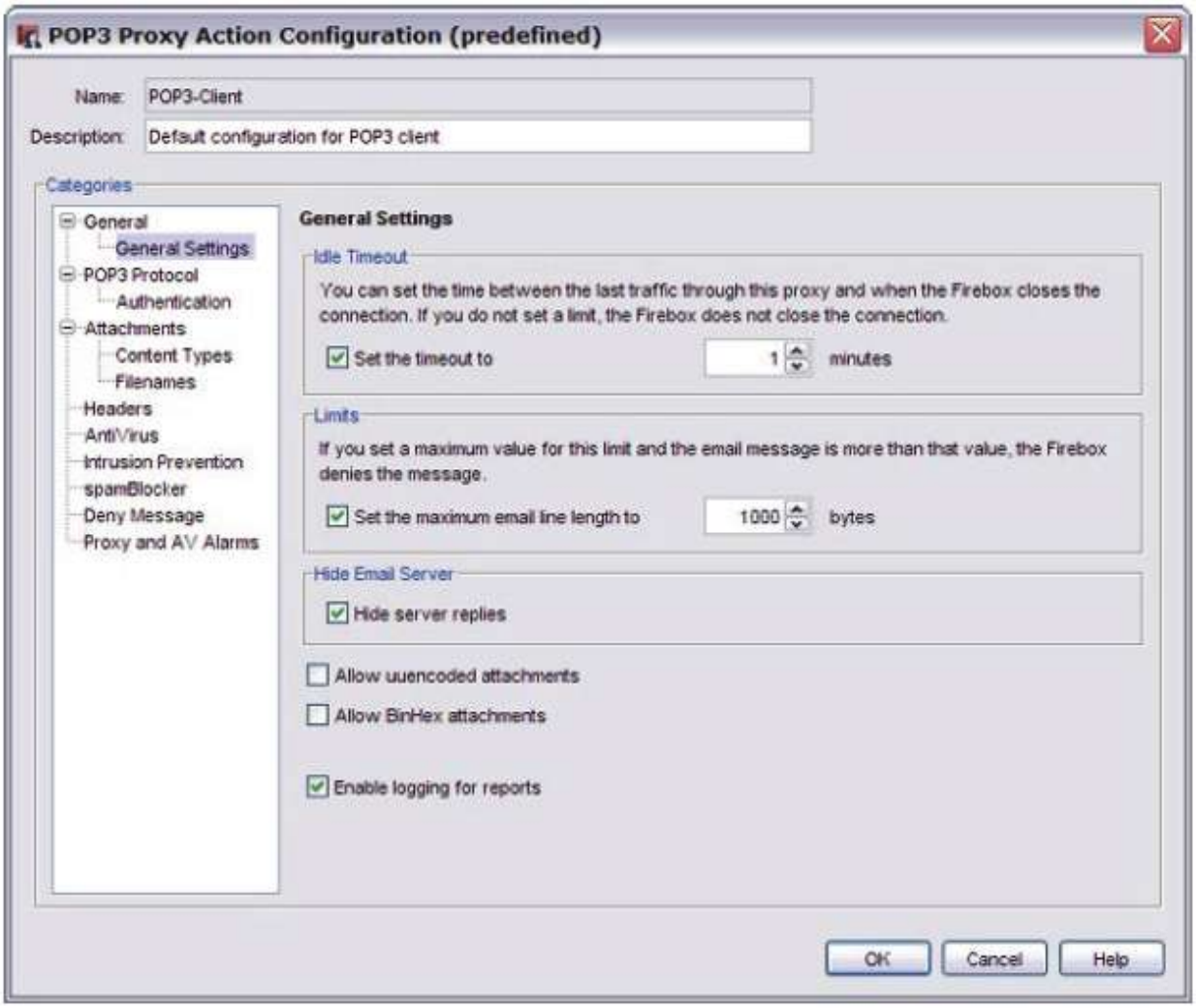
Закладка Advanced

В настройках прокси вы можете использовать несколько дополнительных опций:

- Созданий расписаний для действий Firebox
- Добавление действия Traffic Management к политике
- Настройка обработки ICMP ошибок
- Применение правил NAT
- Включение QoS маркирования или настроек приоритизации для политики
- Настройка длительности sticky соединения для политики

POP3 proxy: General settings

На странице **General Settings** (первая страница, которая открывается после того, как вы нажмете на иконку View/Edit Proxy), вы можете настроить таймаут и длину строки, а также базовые параметры POP3 прокси:



Set the timeout to

При помощи этого параметра вы можете выбрать количество минут, в течение которых почтовый клиент пытается подключиться к серверу электронной почты, после чего соединение будет закрыто. Это не позволяет прокси использоватьбольшое количество ресурсов когда сервер POP3 работает медленно или он недоступен.

Set the maximum email line length to

При помощи этого параметра вы можете защитить свою сеть от атак типа «переполнение буфера». Слишком длинные линии могут привести к переполнению буфера на некоторых почтовых системах. Большинство почтовых клиентов и систем отправляют короткие линии, но некоторые почтовые web-системы отправляют слишком длинные линии. Скорее всего вам не придется изменять значение этого параметра, только если у вас не начнут возникать проблемы с доступом к вашей почте.

Hide server replies

Включите эту опцию если вы хотите заменить строку привествия POP3 в электронных сообщениях. Эти строки могут быть использованы хакерами для определения производителя сервера POP3 и его версию.

Allow uuencoded attachments

Включите эту опцию если вы хотите, чтобы POP3 прокси разрешал вложения, закодированные при помощи UUEncode в электронных сообщениях. Uuencode – это более старая программа, которая использовалась для передачи бинарных файлов в текстовом ASCII формате по сети Интернет. Вложения, закодированные при помощи Uuencoded, могут представлять угрозу безопасности вашей сети, так как они передаются в виде ASCII файлов, которые могут содержать исполняемые файл.

Allow BinHex attachments

Включите эту опцию если вы хотите, чтобы POP3 прокси разрешал BinHex вложения в электронных сообщениях. BinHex (сокращение от binary-to-hexadecimal) – это утилита, которая преобразует файл из бинарного формата в ASCII формат.

Enable logging for reports

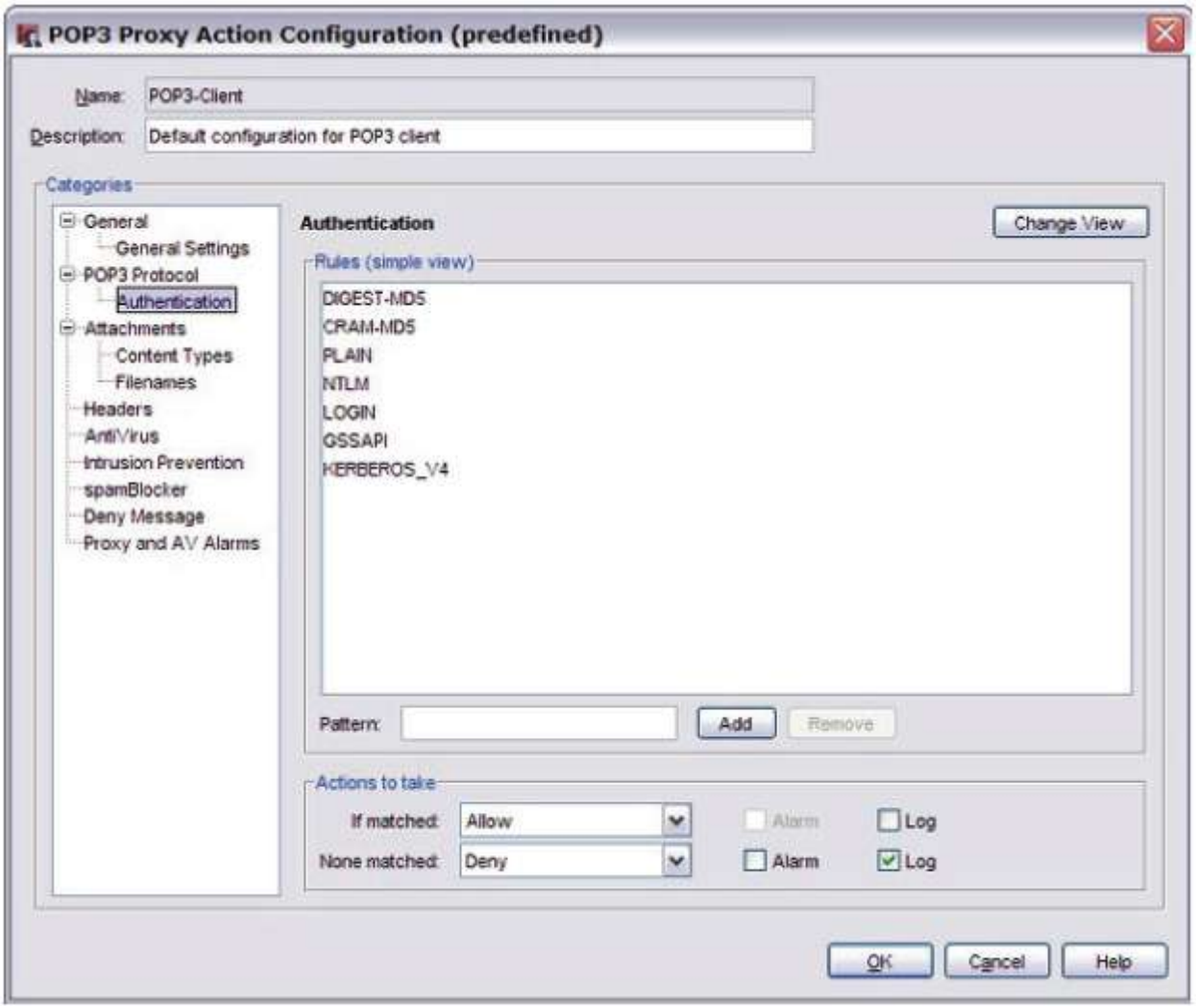
Включите опцию, если вы хотите чтобы POP3 прокси отправлял сообщение журнала для каждого соединения через POP3. Если вы хотите использовать WatchGuard Reports для создания отчетов по POP3 трафику вам необходимо включить эту опцию

POP3 proxy: Authentication

POP3 клиент должен аутентифицироваться на POP3 сервер перед тем, как они смогут обмениваться информацией. На странице **Authentication** вы можете выбрать типы аутентификации для прокси и действие, которые будут выполнены если типы не совпадают с критерием.

Если набор правил по умолчанию не соответствует вашим требованиям, вы можете выполнить необходимые изменения

1. В секции **Categories** выберите **Authentication**.



2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

6. Введите имя нового действия и нажмите **OK**.
Откроется диалоговое окно New Policy Properties.

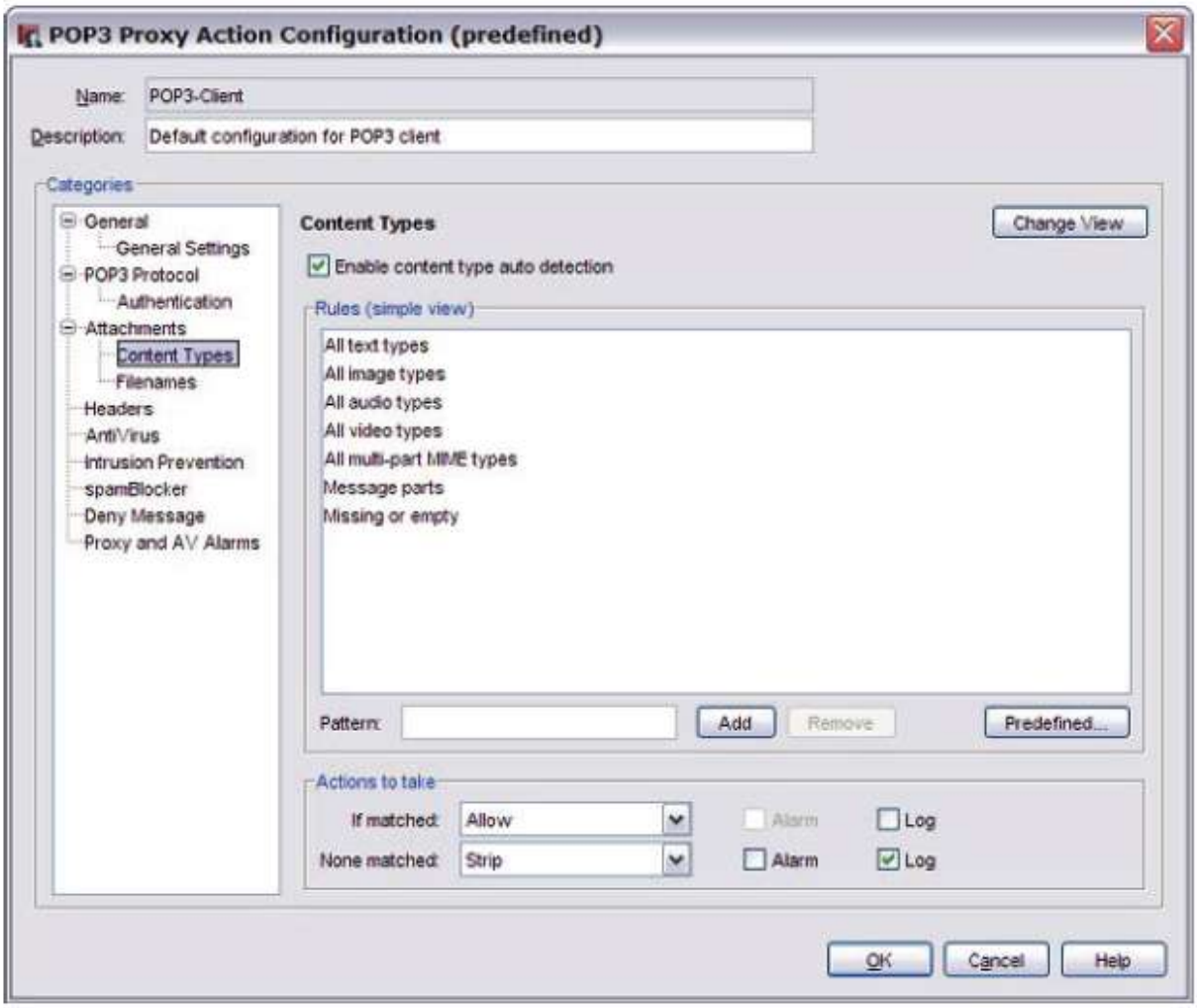
Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

POP3 proxy: Content types

Заголовки электронного письма включает заголовок Content Type, который содержит информацию о MIME типе электронного письма и любых вложений. Тип содержимого или MIME тип сообщает компьютеру тип данных, который содержит электронное письмо. Одни типы содержимого могут представлять угрозу безопасности вашей сети, другие типы могут значительно снизить продуктивность ваших пользователей.

Если набор правил по умолчанию не соответствует вашим требованиям, вы можете выполнить необходимые изменения. На странице **Content Types** вы можете настроить параметры фильтрации контента и действия, которые будут выполнены для типов содержимого, которые не совпадают с критерием. Для действия POP3-server вы можете настроить параметры для фильтрации входящего контента. Для действия POP3-client вы можете настроить параметры для фильтрации исходящего контента.

1. В секции **Categories** выберите **Content Types**



2. Включите опцию **Enable content type auto detection** чтобы POP3 прокси проверял содержимое для определения его типа. В противном случае POP3 прокси будет использовать значение, указанное в заголовке электронного письма, который некоторые клиенты неправильно настраивают. Например, присоединенный .pdf файл может содержать тип содержимого - application/octet-stream. Если вы включите автоматическое определение типа содержимого, POP3 прокси распознает .pdf файл и будет использовать тип содержимого - application/pdf. Если прокси не определит тип содержимого после его проверки, он будет использовать значение, указанное в заголовке электронного письма. Так как хакеры часто пытаются скрыть исполняемые файлы под видом других типов содержимого, мы рекомендуем вам включить автоматическое определение типа содержимого

3. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”. Формат MIME типа - **тип/подтип**. Например, если вы хотите разрешить загрузку изображений JPEG, вам необходимо добавить `image/jpg` в прокси. Вы также можете использовать (*) в качестве группового символа. Для того чтобы разрешить все изображения, вам необходимо добавить `image/*`.

4. Для того чтобы добавить предопределенный тип содержимого нажмите **Predefined**.
   Откроется список типов содержимого с краткими описаниями.

5. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

6. После того, как вы закончите, нажмите **OK**.

7. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

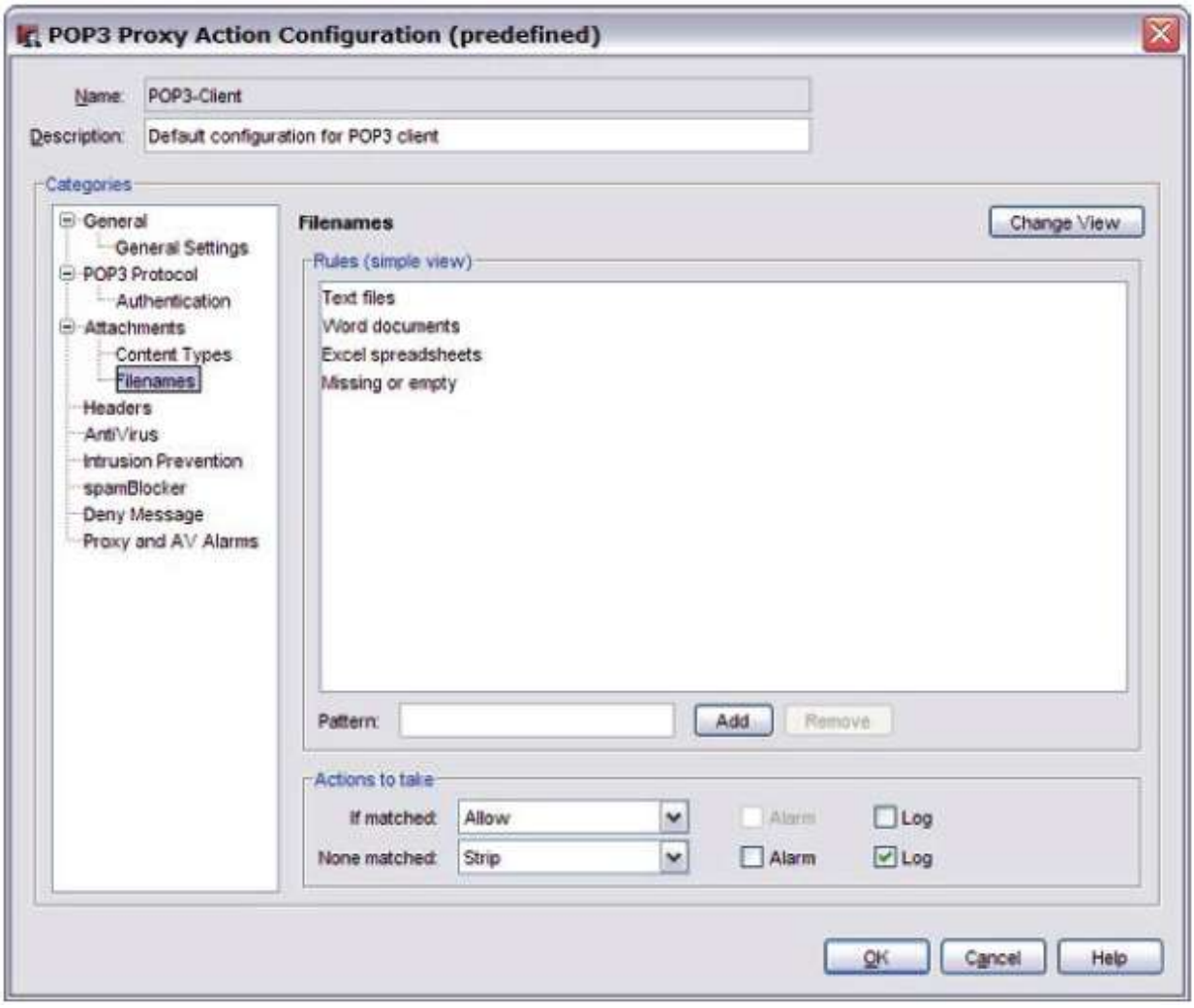
8. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

POP3 proxy: File names

Вы можете использовать эти правила в действии POP3-server для того чтобы наложить ограничения на имена файлов вложений входящих электронных писем. Вы можете использовать правила в действии POP3-client для того чтобы наложить ограничения на имена файлов вложений исходящей почты. Если набор правил, используемый по умолчанию, не соответствует вашим требованиям, вы можете выполнить необходимые изменения.

1. В секции **Categories** выберите **Attachments** > **Filenames**



2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

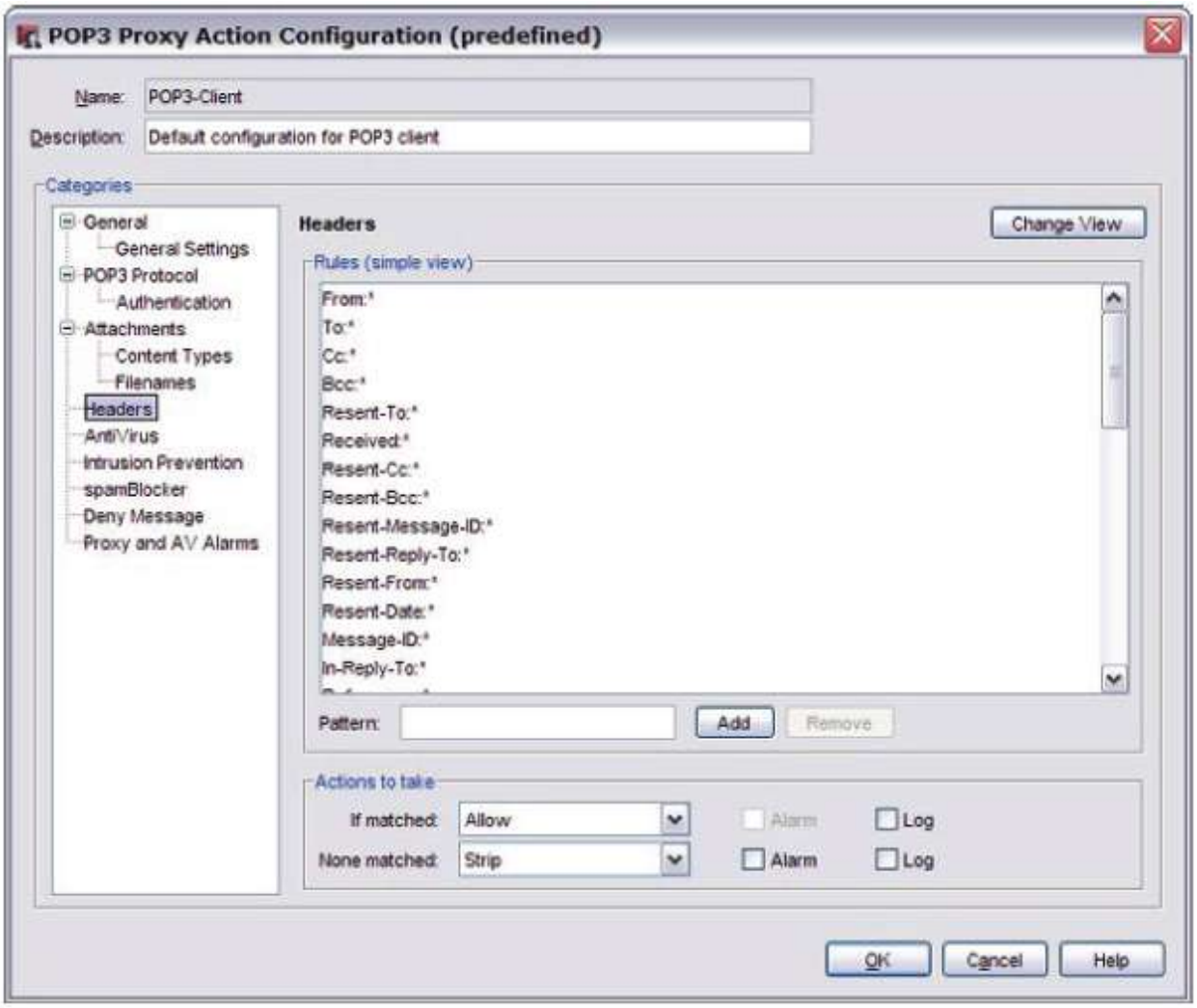
6. Введите имя нового действия и нажмите **OK**.
Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

POP3 proxy: Headers

POP3 прокси проверяет заголовки электронных писем на наличие шаблонов, характерных для злоумышленников. Если набор правил, используемый по умолчанию, не соответствует вашим требованиям, вы можете выполнить необходимые изменения.

1. В секции **Categories** выберите **Headers**



2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

6. Введите имя нового действия и нажмите **OK**.
Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

POP3 proxy: AntiVirus responses

Если вы включили Gateway AntiVirus, то вам необходимо настроить действия, которыебудут выполняться если был обнаружен вирус в загружаемых/выгружаемых файлах.

- Для активации Gateway AntiVirus из настроек прокси см. “Активация Gateway AntiVirus из настроек прокси”

- Для активации Gateway AntiVirus в меню Subsciption Services утилиты Policy Manager см. “Активация Gateway AntiVirus при помощи мастера”

- Для настройки Gateway AntiVirus для FTP прокси см. “Настройка действий Gateway AntiVirus”

После того, как вы активируете Gateway AntiVirus, вам необходимо выбрать действие, которое будет выполнено в случае обнаружения вируса в загружаемом или выгружаемом файле. Вы можете выбрать следующие действия:

Allow

Разрешить отправку пакета получателю, если даже оно содержит вирус.

Lock

Блокирует вложение. Эту опцию необходимо использовать для файлов, которые WatchGuard устройство не может просканировать. Только администратор может открыть заблокированный файл. Администратор может использовать различные приложения для сканирования и проверки файлов вложений

Remove

Удаление вложения и передача сообщения получателю.

Если вы разрешите пользователям передавать вложения, то это снижает уровень безопасности вашей системы.

POP3 proxy: Deny message

Firebox по умолчанию использует deny-сообщение, которое заменяет запрещенное содержимое. Вы можете изменить текст этого сообщения. Вы можете использовать deny-сообщение в формате HTML. Первая строка deny-сообщения это секция HTTP-заголовка.

Между первой строкой и телом сообщения должна быть пустая строка.

В поле **Deny Message** введите текст сообщения, используя следующие переменные:

%(reason)%

Причина отклонения содержимого.

%(filename)%

Имя файла заблокированного содержимого.

%(virus)%

Имя или статус вируса, только для пользователей Gateway AntiVirus.

%(action)%

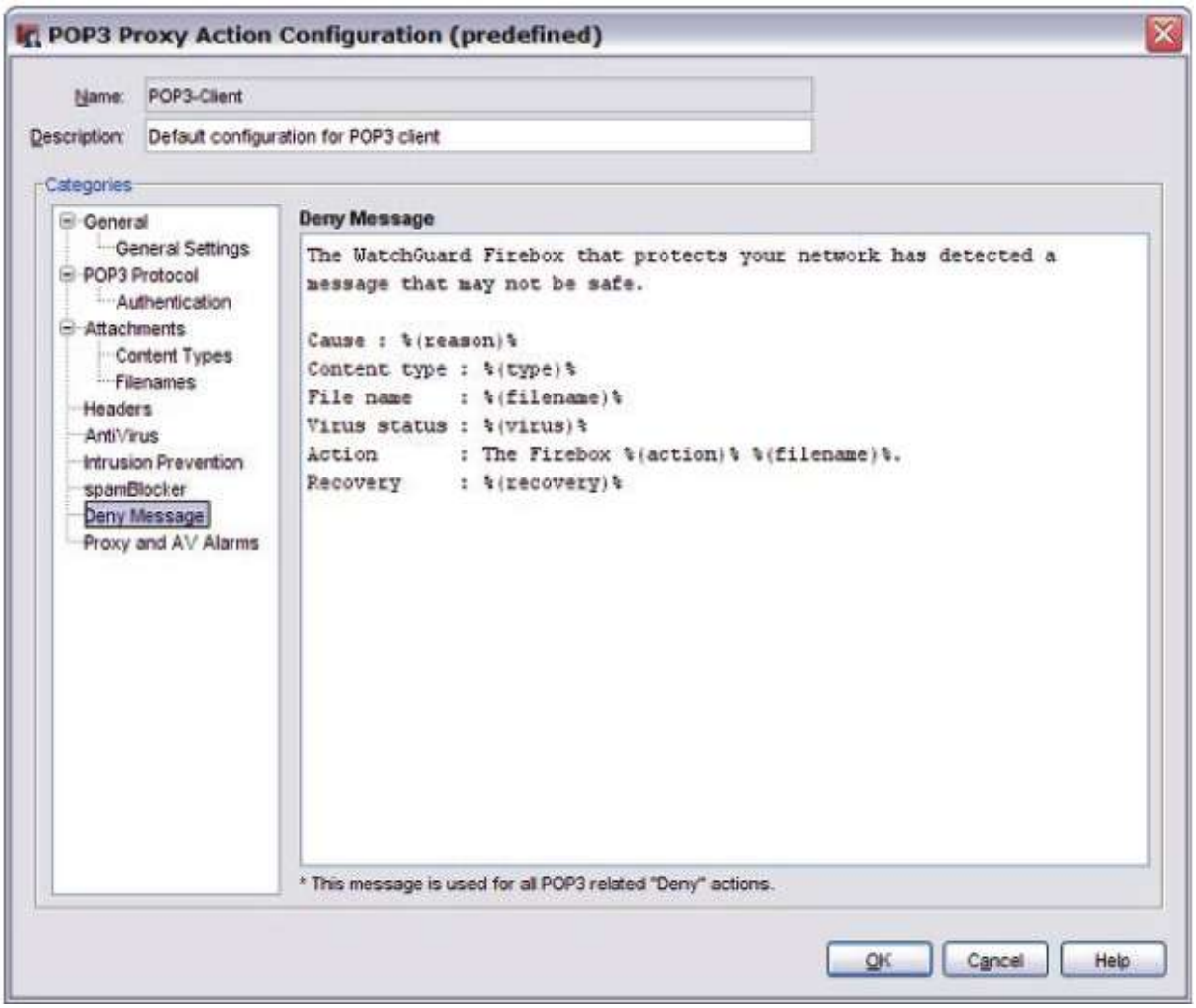
Название выполненного действия: lock, strip и т.д.

%(recovery)%

Флаг восстановления вложения

Для того чтобы настроить deny-сообщение выполните следующее:

1. В секции **Categories** выберите **Deny Message**



2. В поле **Deny Message** введите текст сообщения в формате HTML.

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

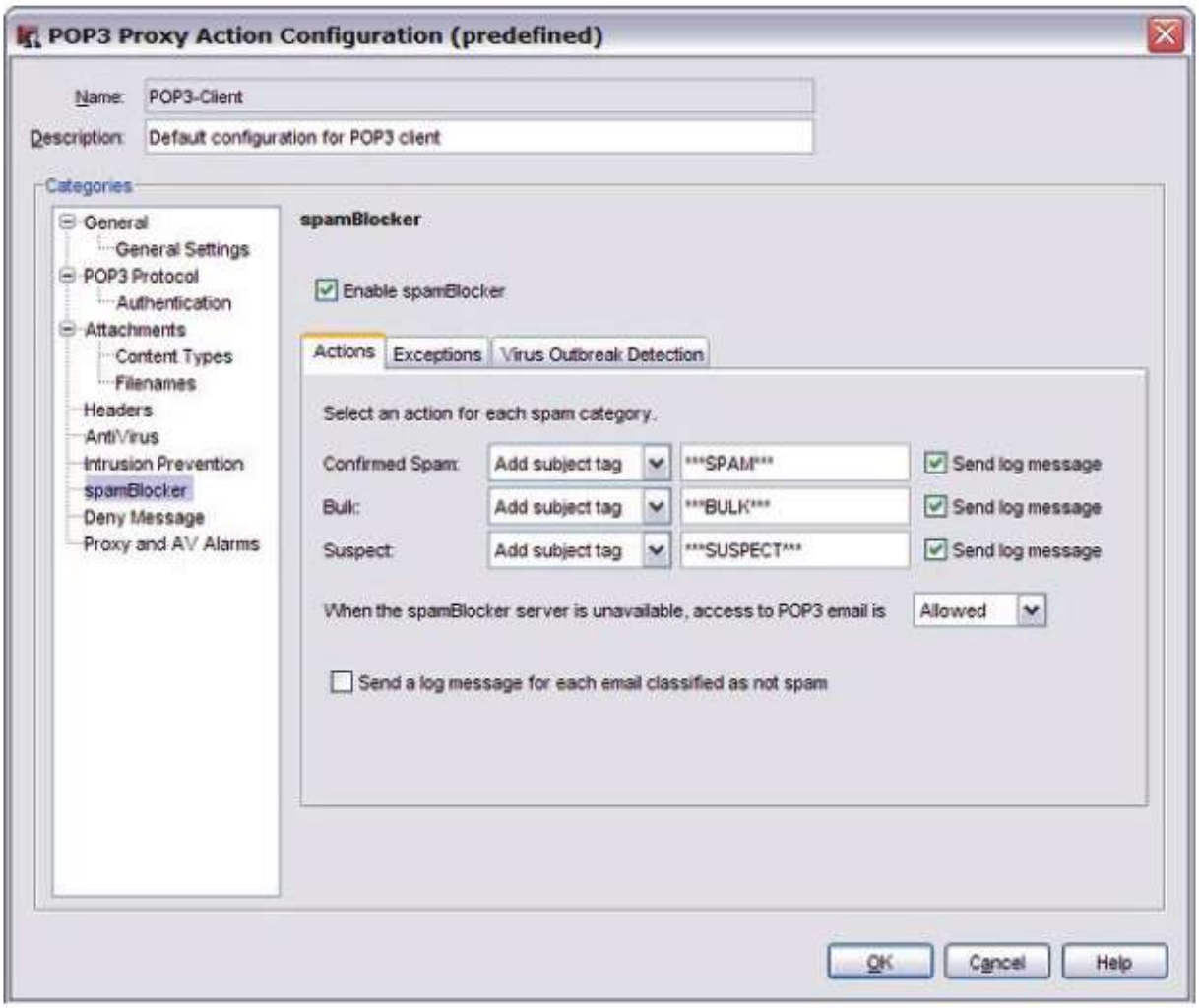
6. Введите имя нового действия и нажмите **OK**.
Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

POP3 proxy: spamBlocker

Нежелательная почта, также известная как спам, заполняет электронные ящики пользователей с огромной скоростью, что приводит к уменьшению пропускной способности, продуктивности работы ваших сотрудников и увеличению использования сетевых ресурсов.

WatchGuard spamBlocker используется для эффективной фильтрации спама. Несмотря на то, что вы можете использовать настройки прокси для активации и конфигурации spamBlocker, намного проще будет использовать меню **Subscription Services** в Policy Manager. Для более подробной информации см. “Глава 31 - spamBlocker”



SIP прокси

Если в вашей сети вы используете Voice-over-IP (VoIP), вы можете добавить H.323 или SIP (Session Initiation Protocol) ALG (Application Layer Gateway) для открытия портов, необходимых для

передачи VoIP трафика через ваше WatchGuard устройство. ALG создается также как и политика прокси и предлагает похожий набор параметров. Эти

ALG были созданы в работы в сетях с NAT для защиты оборудования для конференций, подключенного к вашему WatchGuard устройству.

H.323 обычно используется в более старом оборудовании для видеоконференций и передачи голоса по IP. Протокол SIP – это более новый стандарт, который чаще используется в сетях, в которых находятся только конечные устройства (например VoIP телефоны), а VoIP провайдер управляет их соединением. При необходимости вы одновременно можете использовать H.323 и SIP ALGs. Для того чтобы понять, какой ALG вам необходимо создать, см. документацию по вашим VoIP оборудованию или приложениям.

Компоненты VoIP

Важно понимать, что вы можете реализовать VoIP следующим образом

Соединение точка-точка (P2P соединение)

При использовании p2p соединений каждое устройство знает IP адрес другого устройства и напрмяую подключаеткся к нему. Если оба устройства находятся за Firebox, то он может корректно маршрутизировать голосовой трафик.

Hosted соединения

Подключение, которые обслуживаются специальной системой управления – PBX

В стандарте SIP определены два ключевых компонента – *SIP регистратор (SIP Registrar)* и *SIP прокси*. Вместе эти компоненты выполнют функцию Привратника в H.323 и используются для управления вызовами, обслуживаемыми системой управления вызовами. WatchGuard SIP ALG открывает и закрывает порты, необходимые для работы SIP. В случае если система управления вызовами находится во внешней сети, то WatchGuard SIP ALG может поддерживать и SIP Регистратор и SIP Прокси. В этом релизе мы не поддерживаем протокол SIP в случае если ваша система управления вызовами защищена устройством Firebox.

Координация многих компонентов VoIP системы представляет сложную задачу. Мы рекомендуем вам убедиться, что VoIP соединения работают нормально, перед тем как использовать систему с политиками прокси Firebox. Это поможет вам решать возникающие проблемы.

Функции ALG

Если вы включите H.323 ALG, то ваше WatchGuard устройство:

- Автоматически будет отвечать на запросы VoIP приложений и откроет все необходимые порты
- Проверит, что VoIP соединения используют стандартные протоколы H.323
- Генерирует сообщения журнала для аудита

Достаточно большое количество VoIP устройств и серверов используют NAT (Network Address Translation) для автоматического открытия и закрытия портов.

H.323 и SIP ALGs также выполняют эту функцию. Если вы используете H.323 или SIP ALG вам необходимо отключить NAT на ваших VoIP устройствах.

Для того чтобы добавить SIP ALG в вашу конфигурацию см. “Добавление политики прокси”

Изменить настройки ALG вы можете в диалоговом окне **New/Edit Proxy Policies**. Диалоговое окно содержит три закладки: **Policy**, **Properties** и **Advanced**. В закладке **Properties** вы можете изменить правила для действий прокси.

Закладка Policy

- **SIP-ALG connections are** — выберите одну из опций: **Allowed** (Разрешены), **Denied** (Запрещены) или **Denied (send reset)** (Запрещена, отправка TCP Reset). Вы можете также настроить, кто появится в списках **From** и **To** list (закладка Policy в настройках прокси

- **Use policy-based routing** — См. “Настройка маршрутизации на базе политик”

- Вы также можете настроить статическую NAT или настроить балансировку нагрузки на сервер.

Закладка Properties

- Из выпадающего списка **Proxy action** укажите для кого вы создаете действие: клиента или сервера. Для более подробной информации см. “Действия прокси”

- Для настройки журнала нажмите **Logging** и выполните необходимые настройки

- Если в выпадающем списке C**onnections are** (закладка **Policy**) вы выберете Denied или Denied (send reset), вы можете заблокировать сайты, которые пытаются использовать FTP. Для более подробной информации см. “Временная блокировка сайтов при помощи политики”

- Если вы хотите использовать таймаут ожидания (установленный Firebox или сервером аутентификации) см. “Настройка таймаута ожидания”

Прокси WatchGuard имеют предустановленные наборы правил, которые обеспечивают необходимый уровень доступности и безопасности для большинства инсталляций. Если набор правил по умолчанию не соответствует вашим требованиям, вы можете создать новый набор правил, или изменить существующий. Для того чтобы изменить параметры правил для действия прокси выполните следующее:

1. Нажмите  .
2. Выберите категорию:

   * SIP ALG: General Settings

   * SIP ALG: Access Control

   * SIP ALG: Denied Codecs

Для переноса набора правил между прокси вы можете использовать функции импорта и экспорта.

Закладка Advanced

В настройках прокси вы можете использовать несколько опций:

- Созданий расписаний для действий Firebox

- Добавление действия Traffic Management к политике

- Настройка обработки ICMP ошибок

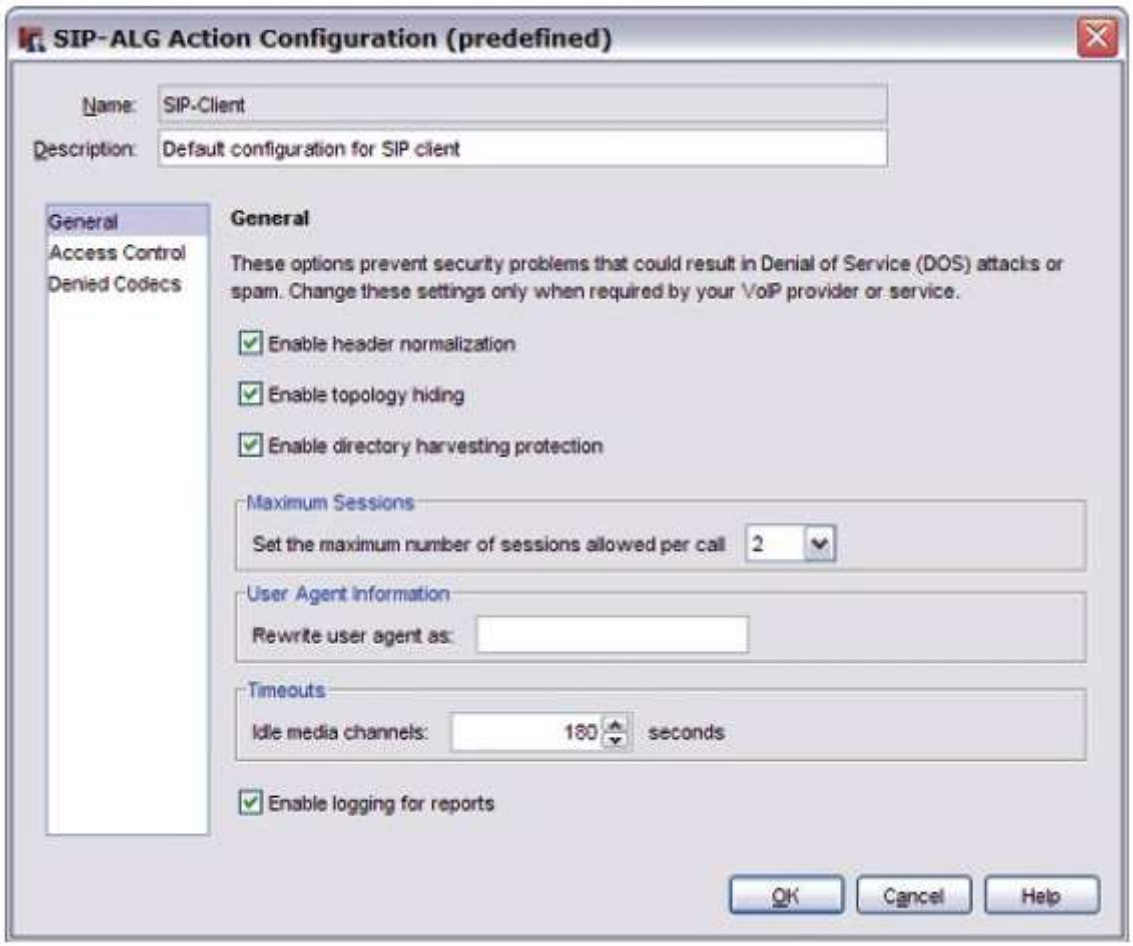
- Применение правил NAT

- Включение QoS маркирования или настроек приоритизации для политики

- Настройка длительности sticky соединения для политики

SIP ALG: General Settings

На странице **General Settings** вы можете настроить параметры безопасности и производительности для SIP ALG (Application Layer Gateway)



Enable header normalization

Включите эту опцию для блокировки некорректных или слишком длинных SIP заголовков. Несмотря на то, что такие заголовки обычно являются признаком атаки на ваш Firebox, вы можете отключить эту опцию если это необходимо для корректной работы вашего VoIP решения.

Enable topology hiding

Эта функция используется для перезаписи заголовков SIP для того чтобы удалить информацию о внутренней сети, например IP адреса. Мы рекомендуем включить эту опцию, только если у вас нет существующего VoIP шлюза.

Enable directory harvesting protection

Включите эту опцию для того чтобы защитить информацию о пользователях, которая хранится на VoIP привратниках, защищенных вашим Firebox, от атак хакеров. Эта опция включена по умолчанию.

Maximum sessions

Максимальное количество аудио или видео сессий, которое можно создать в одном VoIP звонке. Например, если вы установите значение этого параметра равное единице и создадите VoIP звонок с аудио и видео, то второе соединения будет блокироваться. По умолчанию максимальное количество сессий равно двум. Для каждой заблокированной сессии Firebox создает запись в журнале.

User agent information

В текстовом поле **Rewrite user agent as** новую строку агента пользователя для идентификации исходящего H.323 трафика. Для того чтобы удалить ложного агента пользователя, очистите это поле.

Timeouts

Если в течение определенного промежутка времени в VoIP аудио, видео канале или канале данных данные не передавались, то Firebox закрывает это соединение. По умолчанию величина таймаута равна 180 секундам (3 минуты), максимальная величина таймаута равна 600 seconds (10 минут). В поле **Idle media channels** введите необходимую величину таймаута.

Enable logging for reports

Включите эту опцию, если вы хотите чтобы для каждого соединения под управлением SIP ALG создавалась запись в журнале. Это опция необходима для создания подробных отчетов о SIP трафике. Включена по умолчанию

SIP ALG: Access Control

На странице **Access Control** вы можете создать список пользователей, которым будет разрешено передавать VoIP трафик

Enable access control for VoIP

Включите эту опцию для того чтобы включить функцию управления доступом.

Default Settings

Включите опцию **Start VoIP calls** для того чтобы разрешить всем пользователям звонить по VoIP. Включите опцию **Receive VoIP calls** для того чтобы разрешить все пользователям принимать VoIP звонки. Включите опцию **Log** для того чтобы для отправляемого или принимаемого SIP VoIP звонка создавалась запись в журнале.

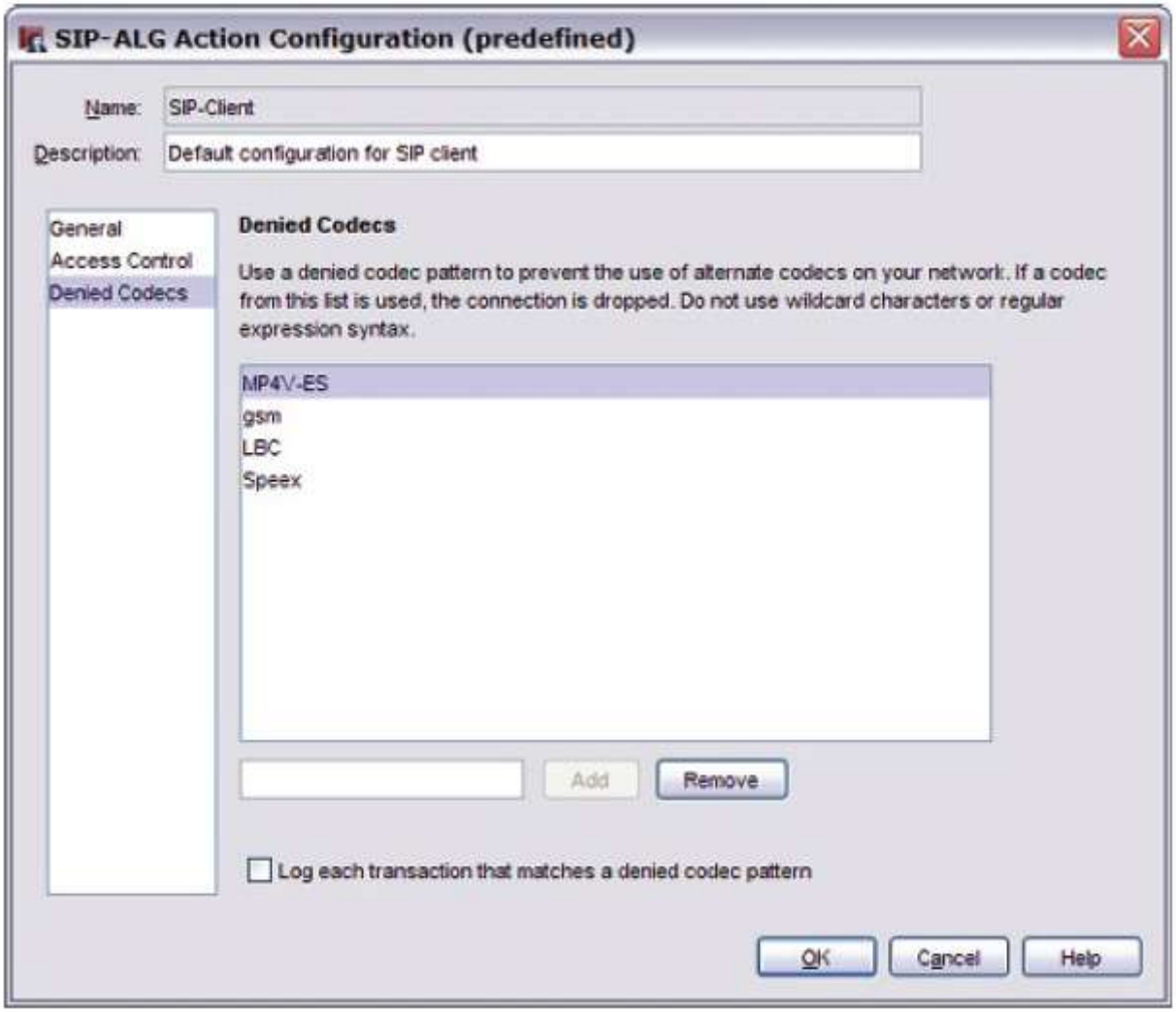
Access Levels

Для того чтобы создать исключения из правил, настроенных выше, введите имя хоста, IP адрес или адрес электронной почты. В выпадающем списке выберите уровень доступа и нажмите **Add**. Вы можете определенным пользователям только звонить (**start calls only)**, только принимать звонки (**receive calls only)**, звонить и принимать звонки (**start and receive calls)** или запретить передачу VoIP трафика (**no VoIP access)**. Эти настройки применяются только для SIP VoIP трафика.

Если вы хотите удалить исключение выберите его из списка и нажмите **Remove**. Звонки пользователей, у которых есть специальный уровень доступа (исключение), по умолчанию записываются в журнал. Для того чтобы отключить эту функцию для этих пользователей отключите опцию **Log** рядом с исключением.

SIP ALG: Denied Codecs

На странице **Denied Codecs** вы можете настроить VoIP голосовые, видео кодеки и кодеки передачи данных, которые вы хотите заблокировать в вашей сети



Denied Codecs list

Список запрещенных VoIP кодеков. Если создается H.323 VoIP соединение, которое использует кодек из этого списка, ваше WatchGuard устройство автоматически закрывает это соединение. По умолчанию этот список пуст. В этот список мы рекомендуем добавлять кодеки, которые требуют достаточно большой пропускной способности, представляет определенную угрозу для вашей сети, или из-за которых ваше VoIP решение некорректно работает. Например вы можете запретить G.711 или G.726 кодеки, так как им необходимо больше 32 КБит/с, или вы можете запретить кодек Speex, так как он используется неавторизованным VOIP кодеком. Для того чтобы добавить кодек в список, в текстовом поле введите название кодека и нажмите кнопку **Add**. Не используйте

групповые символы или регулярные выражения. Названия кодеков чувствительны к регистру. Для того чтобы удалить кодек, выберите его из списка и нажмите **Remove**.

Log each transaction that matches a denied codec pattern

Включите эту опцию, если вы хотите чтобы ваш Firebox создавал запись в журнале каждый раз когда он блокирует H.323 трафик, который содержит кодек из списка запрещенных кодеков.

SMTP прокси

Протокол SMTP (Simple Mail Transport Protocol) – это протокол, который используется для обмена электронными письмами между сервером и клиентом. Обычно он использует TCP соединение через порт 25.

Вы можете использовать SMTP-прокси для управления электронными сообщениями и их содержимым.

SMTP-прокси сканирует SMTP сообщения по определенному числу фильтруемых параметров, и сравнивает их с правилами, установленными в конфигурации прокси

При помощи SMTP прокси вы можете:

- Установить ограничения на длину строки и величину таймаута для того чтобы POP3 прокси не использовало слишком много ресурсов сети, а также для защиты от некоторого типа атак.
- Выбрать текст сообщения, которое будут видеть пользователи, в случае если отправленная им почта заблокирована.
- Фильтровать содержимое, включенное в электронное письмо с MIME типами.
- Установить ограничения на адреса получателей и автоматически блокировать электронную почту от указанных отправителей.

Для того чтобы добавить SMTP прокси к вашей конфигурации см. “Добавление политики прокси”

Затем, если вы захотите изменить настройки прокси, вы можете окрыть диалоговое окно **New/Edit Policy Properties** и в нем выполнить все необходимые изменения.Поля этого диалогового окна разделены на три закладки: **Policy**, **Properties**, and **Advanced**. Вдобавок закладка **Properties** содержит иконку для настройки действий прокси.

Закладка Policy

- **SMTP-proxy connections are** — выберите одну из опций: **Allowed** (Разрешены), **Denied** (Запрещены) или **Denied (send reset)** (Запрещена, отправка TCP Reset). Вы можете также настроить, кто появится в списках **From** и **To** (закладка **Policy** в настройках прокси)
- **Use policy-based routing —** См. “Настройка маршрутизации на базе политик”
- Вы также можете настроить статическую NAT или настроить балансировку нагрузки на сервер.

Закладка Properties

- Из выпадающего списка **Proxy action** укажите для кого вы создаете действие: клиента или сервера. Для более подробной информации см. “Действия прокси”
- Для настройки журнала нажмите **Logging** и выполните необходимые настройки

- Если в выпадающем списке C**onnections are** (закладка **Policy**) вы выберете Denied или Denied (send reset), вы можете заблокировать сайты, которые пытаются использовать FTP. Для более подробной информации см. “Временная блокировка сайтов при помощи политики”

- Если вы хотите использовать таймаут ожидания (установленный Firebox или сервером аутентификации) см. “Настройка таймаута ожидания”

Прокси WatchGuard имеют предустановленные наборы правил, которые обеспечивают необходимый уровень доступности и безопасности для большинства инсталляций. Если набор правил по умолчанию не соответствует вашим требованиям, вы можете создать новый набор правил, или изменить существующий. Для того чтобы изменить параметры правил для действия прокси выполните следующее:

1. Нажмите  .
2. Выберите категорию:

   * SMTP proxy: General settings

   * SMTP proxy: Greeting rules

   * SMTP proxy: ESMTP settings

   * SMTP proxy: Authentication

   * SMTP proxy: Content types

   * SMTP proxy: File names

   * SMTP proxy: Mail From/Rcpt To

   * SMTP proxy: Headers

   * SMTP proxy: AntiVirus responses

   * SMTP proxy: Deny message

   * SMTP proxy: Intrusion Prevention

   * SMTP proxy: spamBlocker

   * Proxy and AV alarms

Для переноса набора правил между прокси вы можете использовать функции импорта и экспорта..

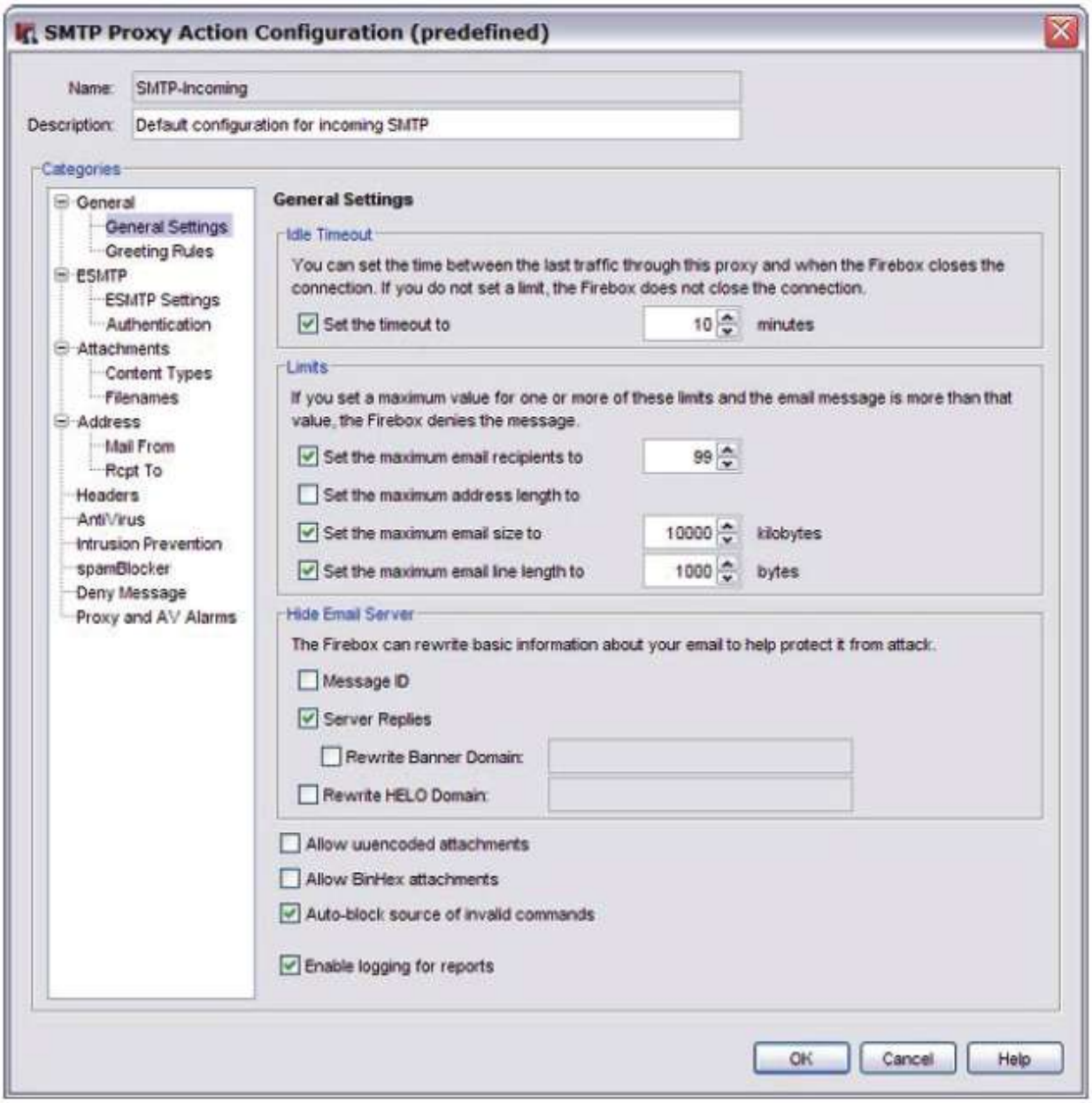
Закладка Advanced

Вы можете использовать следующие опции:

- Созданий расписаний для действий Firebox
- Добавление действия Traffic Management к политике
- Настройка обработки ICMP ошибок
- Применение правил NAT
- Включение QoS маркирования или настроек приоритизации для политики
- Настройка длительности sticky соединения для политики

SMTP proxy: General settings

На странице **General Settings** (первая страница, которая открывается после того, как вы нажмете на иконку View/Edit Proxy), вы можете настроить базовые параметры SMTP прокси, например таймаут ожидания и ограничения, накладываемые на сообщения.



Idle timeout

Вы можете настроить промежуток времени, в течение которого входящее SMTP соединение будет в режим ожидания, после чего наступит таймаут. По умолчанию таймаут ожидания равен 10 минут.

Maximum email recipients

Если вы включите опцию **Set the maximum email recipients to**, то вы можете установить максимальное количество получателей, которым будет отправлено сообщение. Firebox разрешает только определенное количество адресов. Например, максимальное количество адресов равно 50, а в сообщение содержится 52 адреса. Письмо получат первые 50 получателей. Последние два не получат копии сообщения. Список распределения отображается как один электронный адрес (например, support@watchguard.com).

Firebox считает его, как один адрес. Вы можете использовать эту опцию для уменьшения количества спама, так как спамеры часто используют большой список получателей. Будьте осторожны при настройке этого параметра, так как вы можете заблокировать легитимную почту.

Maximum address length

Если вы включите опцию **Set the maximum address length to**, вы можете установить максимальную длину электронного адреса.

Maximum email size

Если вы включите опцию **Set the maximum email size to** вы можете установить максимальный размер входящего SMTP сообщения. Большинство писем отправляются, как 7-bit ASCII текст. Исключения - Binary MIME и 8-bit MIME. 8-bit MIME содержимое (например, MIME вложения) закодированы при помощи стандартных алгоритмов (Base64 или quote-printable encoding) для того чтобы передавать их через 7-bit почтовые системы. Кодирование увеличивает размер файла примерно на треть. Для того чтобы разрешить сообщения размером 10 KB, вам необходимо установить значение этого поля минимум 1334 байта

Maximum email line length

Включив опцию **Set the maximum e-mail line length to** вы можете установить максимальную длину строк SMTP-сообщенийе. Слишком длинные строки могут привести к переполнению буфера на некоторых почтовых системах. Большинство почтовых клиентов и систем отправляют короткие строки, однако некоторые почтовые web-системы отправляют очень большие строки.

Hide Email Server

Включите опции **Message ID** или **Server Replies** для того чтобы в электронных сообщениях заменить границу MIME и SMTP-строку приветствия. Эти параметры используются для идентификации производителя и версии SMTP-сервера.

Если у вас есть почтовый сервер и вы используете действие прокси **SMTP-Incoming**, вы можете заменять имя домена, отображаемое в заголовке вашего SMTP-сервера, на выбранное вами доменное имя.

Для этого включите опцию **Rewrite Banner Domain** и введите доменное имя, которое вы хотите использовать в вашем заголовке. Для этого необходимо еще включить опцию **Server Replies**.

Если вы используете действие **SMTP-Outgoing**, вы можете при помощи SMTP прокси изменять имя домена, отображаемое в полях HELO или EHLO. Поле HELO или EHLO это первая часть SMTP-транзакции, когда ваш почтовый сервер «представляет себя» принимающему почтовому серверу. Для этого включите опцию **Rewrite HELO Domain** и введите имя домена, которые вы хотите использовать в поле HELO или EHLO.

Allow uuencoded attachments

Включите эту опцию если вы хотите, чтобы SMTP прокси разрешал вложения, закодированные при помощи UUEncode в электронных сообщениях. Uuencode – это более старая программа, которая использовалась для передачи бинарных файлов в текстовом ASCII формате по сети Интернет.

Вложения, закодированные при помощи Uuencoded, могут представлять угрозу безопасности вашей сети, так как они передаются в виде ASCII файлов, которые могут содержать исполняемые файлы.

Allow BinHex attachments

Включите эту опцию если вы хотите, чтобы SMTP прокси разрешал BinHex вложения в электронных сообщениях. BinHex (сокращение от binary-to-hexadecimal) – это утилита, которая преобразует файл из бинарного формата в ASCII формата.

Auto-block sources of invalid commands

Включите эту опцию для того чтобы добавить адреса отправителей некорректных команд в список Blocked Sites. Некорректные SMTP команды сигнализируют о том, что ваш SMTP сервер атакован.

Turn on logging for reports

Включите опцию, если вы хотите чтобы SMTP прокси отправлял сообщение журнала для каждого соединения через SMTP. Если вы хотите использовать WatchGuard Reports для создания отчетов по SMTP трафику вам необходимо включить эту опцию

SMTP proxy: Greeting rules

Прокси проверяет HELO/EHLO ответы во время инициализации SMTP-сеанса. Установленные по умолчанию правила для действия прокси SMTP-Incoming гарантируют, что пакеты с длинными приветственными сообщениями или пакеты, которые содержат некорректные символы, отклоняются.

Если набор правил по умолчанию не соответствует вашим требованиям, вы можете выполнить необходимые изменения.

1. В секции **Categories** выберите **Greeting Rules**.

2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

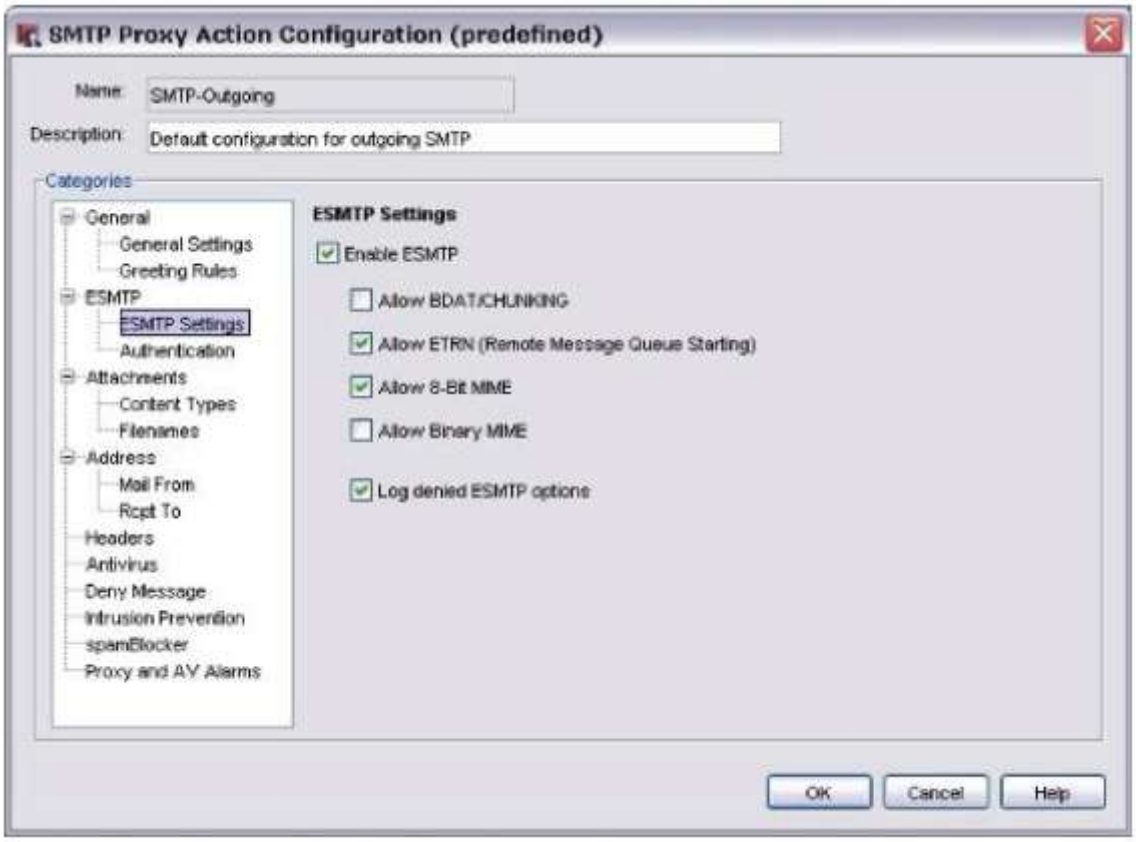
6. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

SMTP proxy: ESMTP settings

При помощей полей **ESMTP Settings** вы можете настроить фильтры для ESMTP-содержимого. Несмотря на то, что SMTP широко применяется, некоторая часть пользователей Интернет посчитали, что необходимо расширить функциональность. ESMTP обеспечивает метод для некоторых функциональных расширений SMTP и для пользователей, которые используют эти расширения для идентификации друг друга

1. В секции **Categories** выберите **ESMTP Settings**



2. Настройте следующие опции:

   Enable ESMTP

   Включите эту опцию, что активировать поля, расположенные ниже.

   Allow BDAT/CHUNKING

   Включить использование BDAT/CHUNKING. Это упрощает процедуру отправки больших сообщений через SMTP-соединения.

   Allow ETRN (Remote Message Queue Starting)

   Это расширение SMTP, которое позволяет SMTP-клиенту и серверу обмениваться очередями сообщений для данного хоста.

   Allow Binary MIME

   Включить использование 8-bit MIME, если клиент и хост поддерживают это расширение. Расширение 8-bit MIME позволяет клиенту и хосту обмениваться сообщениями, которые содержат текст, состоящий из октетов, которые не принадлежат диапазону октетов US-ASCII (hex 00-7F, or 7-bit ASCII), который использует SMTP. Мы не рекомендуем использовать эту опцию, так как это риск.

   Log denied ESMTP options

   Включите эту опцию для того чтобы записывать в журнал неизвестных опций ESMTP, которые удаляются SMTP прокси

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

SMTP proxy: Authentication

Этот набор правил разрешает следующие типы ESMTP-аутентификации: DIGEST- MD5, CRAM-MD5, PLAIN, LOGIN, LOGIN (old style), NTLM, and GSSAPI. Правило, которое используется по умолчанию, не разрешает использование всех других типов аутентификации. RFC, который сообщает о расширении SMTP-аутентификации - RFC 2554

Если набор правил, используемый по умолчанию, не соответствует вашим требованиям, вы можете выполнить необходимые изменения.

1. В секции **Categories** выберите **Attachments** > **Filenames**.

2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

6. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

SMTP proxy: Content types

Определенные типы содержимого электронного письма могут представлять угрозу безопасности вашей сети. Некоторые типы содержимого могут значительно снизить продуктивность ваших пользователей. Вы можете использовать правила для действия прокси **SMTP-Incoming** для того чтобы установить параметры для фильтрации входящего SMTP-содержимого.

Вы можете использовать правила для действия прокси **SMTP-Outgoing** для того чтобы установить параметры для фильтрации исходящего SMTP-содержимого. SMTP разрешает следующие типы содержимого: text/*, image/*, multipart/*, and message/*.

Если набор правил по умолчанию не соответствует вашим требованиям, вы можете удалять и редактировать существующие правила, а также создавать новые правила.

Вы можете настроить автоматическую проверку SMTP прокси содержимого для определения его типа. В противном случае SMTP прокси будет использовать значение, указанное в заголовке электронного письма, который некоторые клиенты неправильно настраивают. Например, присоединенный .pdf файл может содержать тип содержимого - application/octet-stream. Если вы включите автоматическое определение типа содержимого, POP3 прокси распознает .pdf файл и будет использовать тип содержимого - application/pdf. Если прокси не определит тип содержимого после его проверки, он будет использовать значение, указанное в заголовке электронного письма. Так как хакеры часто пытаются скрыть исполняемые файлы под видом других типов содержимого, мы рекомендуем вам включить автоматическое определение типа содержимого

1. В секции **Categories** выберите **Content Types**.

2. Для того чтобы включить проверку содержимого SMTP прокси включите опцию **Enable content type auto detection**.

3. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

4. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

5. После того, как вы закончите, нажмите **OK**.

6. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

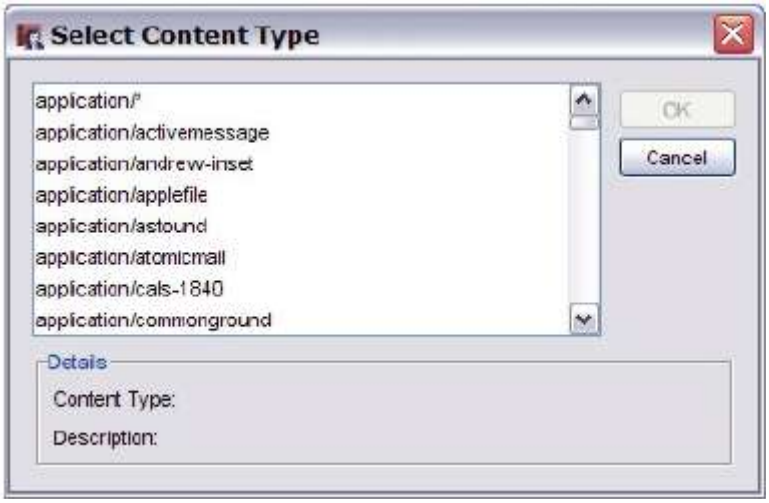
7. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

Добавление общих типов содержимого

Для вашего удобства прокси содержит список типов содержимого, которое вы можете легко добавить в правило Content Type. Для того чтобы открыть список типов содержимого выполните следующее:

1. Нажмите на кнопку **Predefined**.
   Откроется диалоговое окно Select Content Type



2. Выберите один или несколько типов в списке.

3. Нажмите **OK**.

SMTP proxy: File names

Вы можете использовать ruleset для действия прокси **SMTP-Outgoing** для ограничения имен файлов-вложений исходящей почты.

Если набор правил по умолчанию не соответствует вашим требованиям, вы можете удалять и редактировать существующие правила, а также создавать новые правила.

1. В секции **Categories** выберите **Filenames**.

2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

6. Введите имя нового действия и нажмите **OK**.
Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

SMTP proxy: Mail From/Rcpt To

Правило **Mail From** используется для того чтобы разрешать получать электронную почту только от определенных отправителей. Используемая по умолчанию конфигурация разрешает получать электронную почту от всех отправителей.

Правило **Rcpt To** используется для того чтобы разрешать отправлять электронную почту только определенным получателям. Используемая по умолчанию конфигурация разрешает отправлять почту всем отправителям.

В действии SMTP-Incoming, вы можете использовать правило Mail To для того чтобы запретить людям использовать ваш почтовый сервер для ретрансляции электронной почты. Для более подробной информации см. “Защита вашего SMTP сервер от ретрансляции почты”

Вы также можете использовать опцию **Rewrite As** для того чтобы Firebox изменял значения полей From и To вашего электронного адреса. Эта опция известна также как “SMTP маскирование.”

Другие опции доступны в наборах правил **Mail From** и **Rcpt To**:

Block source-routed addresses

Включите эту опцию для того чтобы блокировать сообщение, если адрес получателя или отправителя содержит маршруты источника (source routes). Маршрут источника идентифицирует путь, который должно проделать сообщения при перемещении между хостами. Маршрут может содержать информацию о том, какие роутеры или сайты использовались для передачи этого сообщения. Например, @backbone.com:freddyb@something.com означает, что хост Backbone.com должен быть использован в качестве сервера ретрансляции для доставки почты к freddyb@something.com. По умолчанию эта опция включена для входящих SMTP пакетов и отключена для исходящих SMTP пакетов.

Block 8-bit characters

Включите эту опцию для того чтобы блокировать сообщение, которое содержит 8-битные символы в имени пользователя отправителя или получателя. Это позволяет сделать акцент только на символы алфавита. По умолчанию опция включена для входящих SMTP пакетов и отключена для исходящих SMTP пакетов.

Для настройки ограничений, накладываемых SMTP прокси, на трафик электронной почты выполните следующее:

1. В секции **Categories** выберите **Address**: **Mail From** или **Address: Rcpt To**.

2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

6. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

SMTP proxy: Headers

Правила заголовков позволяют вам установить параметры фильтрации входящих и исходящих SMTP-заголовков

1. В секции **Categories** выберите **Headers**.

2. Добавьте, удалите или измените правила, как описано в “Добавление, редактирование или изменение правил”

3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.

4. После того, как вы закончите, нажмите **OK**.

5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

6. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

SMTP proxy: AntiVirus responses

Если вы включили Gateway AntiVirus, то вам необходимо настроить действия, которыебудут выполняться если был обнаружен вирус в загружаемых/выгружаемых файлах.

- Для активации Gateway AntiVirus из настроек прокси см. “Активация Gateway AntiVirus из настроек прокси”

- Для активации Gateway AntiVirus в меню Subsciption Services утилиты Policy Manager см. “Активация Gateway AntiVirus при помощи мастера”

- Для настройки Gateway AntiVirus для FTP прокси см. “Настройка действий Gateway AntiVirus”

После того, как вы активируете Gateway AntiVirus, вам необходимо выбрать действие, которое будет выполнено в случае обнаружения вируса в загружаемом или выгружаемом файле. Вы можете выбрать следующие действия:

Allow

Разрешить отправку пакета получателю, если даже оно содержит вирус.

Lock

Блокирует вложение. Эту опцию необходимо использовать для файлов, которые WatchGuard устройство не может просканировать. Только администратор может открыть заблокированный файл. Администратор может использовать различные приложения для сканирования и проверки файлов вложений

Quarantine

Если вы используете SMTP прокси со spamBlocker, вы можете отправлять электронные сообщения, которые возможно или точно содержат вирусы, на Сервер Карантина. Для более подробной информации см. “Сервер Карантина”

Remove

Удаление вложения и передача сообщения получателю.

Drop

Отбрасывает пакет и разрывает соединение. Отправитель сообщения не получает никакого уведомления.

Block

Блокирует пакет и добавляет IP отправителя в список Blocked Sites.

Если вы разрешите пользователям передавать вложения, то это снижает уровень безопасности вашей системы.

SMTP proxy: Deny message

Firebox по умолчанию использует deny-сообщение, которое заменяет запрещенное содержимое. Вы можете изменить текст этого сообщения. Вы можете использовать deny-сообщение в формате HTML. Первая строка deny-сообщения это секция HTTP-заголовка. Между первой строкой и телом сообщения должна быть пустая строка.

В поле **Deny Message** введите текст сообщения, используя следующие переменные:

%(reason)%

Причина отклонения содержимого.

%(filename)%

Имя файла заблокированного содержимого.

%(virus)%

Имя или статус вируса, только для пользователей Gateway AntiVirus.

%(action)%

Название выполненного действия: lock, strip и т.д.

%(recovery)%

Флаг восстановления вложения

1. В секции **Categories** выберите **Deny Message**.
2. В поле **Deny Message** введите текст сообщения в формате HTML.
3. Если вы хотите изменить параметры для одной или нескольких категорий, см. раздел по этой категории далее в этом документе.
4. После того, как вы закончите, нажмите **OK**.
5. Если вы внесли изменения в предопределенное действие прокси, то вам необходимо скопировать ваши настройки в новое действие.

6. Введите имя нового действия и нажмите **OK**.
   Откроется диалоговое окно New Policy Properties.

Для более подробной информации о предопределенных действиях пользователя см. “Предопределенные и пользовательские действия прокси”

SMTP proxy: spamBlocker

Нежелательная почта, также известная как спам, заполняет электронные ящики пользователей с огромной скоростью, что приводит к уменьшению пропускной способности, продуктивности работы ваших сотрудников и увеличению использования сетевых ресурсов.

WatchGuard spamBlocker используется для эффективной фильтрации спама. Несмотря на то, что вы можете использовать настройки прокси для активации и конфигурации spamBlocker, намного проще будет использовать меню **Subscription Services** в Policy Manager. Для более подробной информации см. “Глава 31 - spamBlocker”

Настройка SMTP прокси для карантина почты

Сервер Карантина WatchGuard предоставляет безопасный механизм карантина нежелательной почты, также известной как спам. Репозитарий получает электронные сообщения от SMTP прокси. Для того чтобы настроить SMTP прокси для карантина почты выполните следующее:

- Добавьте SMTP прокси в вашу конфигурацию и включите spamBlocker в настройках прокси. Или включите spamBlocker для SMTP прокси.

- При настройке действий, которые spamBlocker будет выполнять для различных категорий почты, убедитесь что вы выбрали действие **Quarantine** для хотя бы одной категории. Если вы выберете это действие, вам необходимо будет настроить Сервер Карантина.

Вы также можете выбрать действие **Quarantine** для электронных писем, идентифицированных системой Virus Outbreak Detection как вирусы

Защита вашего SMTP сервер от ретрансляции почты

Ретрансляция почты, также известная как *почтовый спам* или открытая почтовая ретрансляция, это проникновение на ваш сервер, при котором пользователь использует ваш сервер электронной почты, адрес или другие ресурсы для отправки большого количества спама. Это может привести к выходу из строя системы, повреждению оборудования и финансовым потерям.

Если вы незнакомы с такого типа атаками, или не уверены, уязвим ли ваш сервер элетронной почты для такого рода атак, то мы рекомендуем изучить ваш сервер электронной почты более одробно на предмет уязвимости к атакам типа «ретрансляция почты». Firebox обеспечивает базовую защиту от таких атак..

Для того для того, чтобы защитить ваш сервер, вам необходимо внести изменения в политику SMTP прокси, которая фильтрует трафик из внешней сети на ваш внутренний SMTP сервер, а именно добавить информацию о вашем домене. При вводе имени вашего домена вы можете использовать групповой символ * . При этом любой электронный адрес, который будет заканчиваться на *@ваше-имя-домена* будет разрешен.

Если ваш сервер электронной почты принимает почту с нескольких доменов, то вы можете также добавить их в политику. Например, если вы добавите **@watchguard.com* и **@*.watchguard.com* в список, ваш сервер будет принимать почту, получателем которой является домен верхнего уровня *watchguard.com* и всю почту, получателями которой являются все его поддомены.

Например rnd.watchguard.com.

Перед тем как начать процедуру настройки, вам необходимо знать имена всех ваших доменов, для которых SMTP сервер получает почту.

1. Откройте Policy Manager.

2. Два раза нажмите на политику SMTP прокси, который фильтрует трафик из внешней сети на ваш внутренний SMTP сервер.
   Откроется диалоговое окно Edit Policy Properties.

3. Выберите закладку **Properties**.

4. Нажмите .
   Откроется диалогое окно SMTP Proxy Action Configuration.

5. В секции Categories выберите **Address** > **Rcpt To**.

6. В текстовом поле **Pattern** введите `* @[имя-вашего-домена].`

7. В поле **Actions to Take** нажмите на выпадающий список **None Matched** и выберите **Deny**. Любая почта, предназначенная домену, которого в этом списке нет, будет заблокирована.

8. Нажмите **OK** для того чтобы закрыть диалоговое окно **SMTP Proxy Action Configuration**.

9. Нажмите **OK снова**.

10. Нажмите **Close** для того чтобы закрыть диалоговое окно **Edit Policy Properties**.

11. Сохраните конфигурационный файл.

12. Нажмите **Add**.
    Ваш домен появится в списке Rules.

Вы также можете использовать опцию **Rewrite As** для того чтобы Firebox изменял значения полей From и To вашего электронного адреса. Эта опция известна также как “SMTP маскирование.”

TCP-UDP прокси

TCP-UDP прокси используется для следующих протоколов на нестандартных портах: HTTP, HTTPS, SIP и FTP.

Для этих протоколов TCP-UDP прокси транслирует трафик корректным прокси. Для других протоколов вы можете выбрать, запретить или разрешить трафик. Вы можете также использовать эту политику прокси для разрешения или запрета IM (instant messaging) и P2P (peer-to-peer) трафика.

Для того чтобы добавить TCP-UDP прокси к конфигурации Firebox см. “Добавление политики прокси”

Затем, если вы захотите изменить настройки прокси, вы можете окрыть диалоговое окно **New/Edit Policy Properties** и в нем выполнить все необходимые изменения.Поля этого диалогового окна разделены на три закладки: **Policy**, **Properties**, and **Advanced**. Вдобавок закладка **Properties** содержит иконку для настройки действий прокси.

Закладка Policy

- **TCP-UDP-proxy connections are** — выберите одну из опций: **Allowed** (Разрешены), **Denied** (Запрещены) или **Denied (send reset)** (Запрещена, отправка TCP Reset). Вы можете также настроить, кто появится в списках From и To list (закладка Policy в настройках прокси). Для более подробной информации см. Set access rules for a policy.

- **Use policy-based routing —** См. “Настройка маршрутизации на базе политик”

- Вы также можете настроить статическую NAT или настроить балансировку нагрузки на сервер.

Закладка Properties

- Из выпадающего списка **Proxy action** укажите для кого вы создаете действие: клиента или сервера. Для более подробной информации см. “Действия прокси”

- Для настройки журнала нажмите **Logging** и выполните необходимые настройки

- Если в выпадающем списке C**onnections are** (закладка **Policy**) вы выберете Denied или Denied (send reset), вы можете заблокировать сайты, которые пытаются использовать FTP. Для более подробной информации см. “Временная блокировка сайтов при помощи политики”

- Если вы хотите использовать таймаут ожидания (установленный Firebox или сервером аутентификации) см. “Настройка таймаута ожидания”

Прокси WatchGuard имеют предустановленные наборы правил, которые обеспечивают необходимый уровень доступности и безопасности для большинства инсталляций. Если набор правил по умолчанию не соответствует вашим требованиям, вы можете создать новый набор правил, или изменить существующий. Для того чтобы изменить параметры правил для действия прокси выполните следующее:

1. Нажмите  .
2. Выберите категорию:

   * TCP-UDP proxy: General settings

   * TCP-UDP proxy: Application blocking

   * TCP-UDP proxy: Intrusion prevention

   * Proxy alarm (SNMP ловушки и уведомления отключены по умолчанию)

Для переноса набора правил между прокси вы можете использовать функции импорта и экспорта.

Закладка Advanced

Вы можете использовать следующие опции:

- Созданий расписаний для действий Firebox
- Добавление действия Traffic Management к политике
- Настройка обработки ICMP ошибок
- Применение правил NAT
- Включение QoS маркирования или настроек приоритизации для политики
- Настройка длительности sticky соединения для политики

TCP-UDP proxy: General settings

На странице **General Settings** (первая страница, которая открывается после того, как вы нажмете на иконку View/Edit Proxy), вы можете настроить базовые параметры TCP-UDP прокси.

Proxy actions to redirect traffic

Если трафик передается по нестандартным портам TCP-UDP прокси может передавать его HTTP, HTTPS, SIP и FTP политикам прокси. Для каждого из этих протоколов из выпадающего списка выберите политику прокси, которая будет управлять этим трафиком. Если вы не хотите, что Firebox использовал политику прокси для фильтрации трафика в соответствующих выпадающих списка выберите **Allow** или **Deny**.

Enable logging for reports

Создает запись в журнале для каждой транзакции. Эта опция создает большой файл журнала, но эта информация очень важна. Если вы не включите эту опцию, то в отчетах вы не сможете посмотреть подробную информацию о подключениях прокси.

*Для корректной работы Firebox, вы не можете выбрать опцию **Allow** для протокола FTP.*

TCP-UDP proxy: Application blocking

Вы можете использовать эти правила для создания действий, которые будет выполнять Firebox в случае, когда TCP-UDP прокси обнаруживает Instant Messaging (IM) или Peer to Peer (P2P) сервисы. TCP-UDP прокси обнаруживает следующие IM сервисы: AOL Instant Messenger (AIM), ICQ, IRC, MSN Messenger и Yahoo! Messenger.

Также этот прокси обнаруживает следующие типы P2P сервисов: BitTorrent, eDonkey2000 (Ed2k), Gnutella, Kazaa, Napster, and Phatbot. Для того чтобы использовать блокировку приложения вам не надо приобретать IPS.

1. Откройте Policy Manager.
2. Два раза нажмите на политику TCP-UDP прокси.
   Откроется диалогое окно Edit Policy Properties.
3. Выберите закладку **Properties**.
4. Нажмите  .
   Откроется диалогое окно TCP-UDP Proxy Action Configuration.
5. В секции **Categories** выберите **Application Blocker**.
6. Выберите закладку **IM**.
7. В выпадающем списке выберите действие, которое будет выполнять Firebox при обнаружении Instant Messaging (IM):

   Allow

   Разрешает передачу пакета получателю, даже если содержимое совпадает с сигнатурой

   Deny

   Блокирует пакет и отправляет TCP reset пакет отправителю.
8. Для каждого IM приложения, для которого вы хотите использовать прокси, отметьте соответствующий флаг.
9. Для того для того, чтобы выбрать все IM приложения выберите **All Categories**.
   При этом будут выбраны все приложения.
10. Для настройки действий для P2P приложений выберите закладку **P2P**.
11. Для P2P приложений повторите п. 7–9.

12. Для настройки журнала и уведомлений для IPS нажмите **Logging and Notification**. Для более подробной информации см. Set logging and notification preferences.

13. Если вы хотите изменить параметры для одной или нескольких категорий в этом прокси, см. следующие разделы этого документа.

14. Если вы хотите изменить предустановленное действие прокси, то вам необходимо сначала сделать его копию, и затем выполнить все необходимые изменения для этого действия.

15. Введите имя для нового действия и нажмите **OK**.
    Откроется диалогое окно New Policy Properties.

Глава 15 - Traffic Management и QoS

Traffic Management и QoS

В крупных сетях с большим количеством компьютеров через брандмауэр проходит довольно большой объем трафика. Администратор сети может при помощи действий Traffic Management и Quality of Service (QoS) предотвратить потерю важных данных для критичных бизнес-приложений и обеспечить трафику этих приложений более высокий приоритет.

Traffic Management и QoS обеспечивают целый ряд преимуществ. Вы можете:

- Гарантировать или ограничивать пропускную способность
- Управлять скоростью передачи данных Firebox
- Определять приоритеты трафика

Для того, чтобы использовать Traffic Management в политиках, вам необходимо создать действие Traffic Management, которое представляет собой набор параметров, который вы можете использовать в одной или нескольких политиках. Поэтому нет необходимости настраивать параметры Traffic Management в каждой политике. Если вы хотите к политикам применить другие действия, вы можете создать дополнительные действия Traffic Management

Включение Traffic management и QoS

Из-за возможных проблема с производительностью системы все функции Traffic Management и QoS отключены по умолчанию. Перед тем, как использовать эти функции, вам необходимо их включить:

1. Выберите **Setup** > **Global Settings**.
   Откроется диалоговое окно Global Settings.
2. Включите опцию **Enable all traffic management and QoS features**.
3. Нажмите **OK**.
4. Сохраните конфигурацию.

Гарантия пропускной способности

Резервирование пропускной способности позволяет избежать таймаутов соединений. Очередь Traffic Management с зарезервированной пропускной способностью и низким приоритетом может предоставить приложениям, работающим в режиме реального времени, более высокий приоритет при передаче трафик без необходимости их отключения. Другие очереди Traffic Management могут использовать незадействованную пропускную способность, когда она становится доступной.

Например, у вашей компании есть внешний FTP-сервер, и вы хотите гарантировать, что FTP будет иметь скорость подключения 200 Кбайт/с через интерфейс External. Вы также можете настроить минимальную пропускную способность для Trusted интерфейса, убедившись, что соединение имеет сквозную гарантированную пропускную способность. Для того вам необходимо создать действие Traffic Management, которое установит скорость передачи FTP на External интерфейсе равной минимум 200 кбит/с

Затем вам необходимо создать политику FTP и применить к ней действие Traffic Management.

Скорость ftp put будет равна 200 кбит/с.

Если вы хотите установить скорость ftp get равной 200 кбит/с, вам необходимо настроить FTP трафик на интерфейсе Trusted, чтобы он также имел минимум 200 кбит/с. Другой пример. Предположим, ваша компания использует мультимедиа материалы (потоковые медиа-данные) для проведения курсов обучения внешних заказчиков. Эти потоковые данные используют RTSP через порт 554. Эти потоковые данные используют RTSP через порт 554. На ваших интерфейсах, Trusted и External, имеется большое количество FTP подключений, и вы не хотите, что эти подключения влияли на покупательскую способность при получении потоковых данных. Для того, чтобы гарантировать необходимую пропускную способность, вам необходимо для порта потоковых данных на интерфейсе External применить действие Traffic Management.

Ограничение пропускной способности

Помимо гарантированной пропускной способности используется еще один параметр для External интерфейса - **Outgoing Interface Bandwidth**, который используется для того, чтобы вы не смогли определенному типу трафика выделить пропускной способности больше, чем ее физически существует. Также этот параметр управляет суммарной пропускной способностью, тем самым гарантируя, что посторонний трафик не будет передаваться. Например, у вас есть канал со скоростью 1 Мбит/с, и вы пытаетесь использовать действие Traffic Management, которое гарантирует скорость 973 Кбит/с (0.95 Мбит/с) для политики FTP.

С такими параметрами FTP-трафик занимает весь канал, тем самым не давая другому трафику передаваться по этому каналу. Если вы попытаетесь настроить Firebox таким образом, то Policy Manager предупредит вас, что вы приближаетесь к величине **Outgoing Interface Bandwidth** для этого интерфейса

QoS Маркирование

QoS Маркирование создает различные классы сервисов для различного типа исходящего трафика. Когда вы маркируете трафик, вы изменяете значения 6 бит в заголовках пакета. Внешние устройства с поддержкой QoS могут использовать маркирование и реализовать соответствующую обработку таких пакетов. Вы можете использовать QoS Маркирование для каждого интерфейса или для каждой политики. При создании QoS Маркирования для интерфейса, то каждый пакеты, который передается через этот интерфейс, помечается специальными флагами. QoS Маркирование для политики помечает трафик, к которому эта политика применяется

Приоритет трафика

Вы можете присвоить различные уровни приоритета к политикам или трафику, который передается через определенный интерфейс. Приоритизация трафика на брандмауэре позволяет вам управлять различными очередями классов сервисов (CoS) и резервировать наиболее высокий приоритет для потоковых данных или данных, передающихся в режиме реального времени.

Политика с наивысшим приоритетом может забрать пропускную способность у соединений с более низким приоритетом при насыщении канала связи и в том случае, когда трафик различных типов конкурирует за пропускную способность

Настройка ограничений на скорость передачи данных

Для повышения безопасности вашей сети вы можете создать специальное ограничение, которое будет ограничивать для политики количество фильтруемых подключений в секунду. Если при использовании этого ограничения количество фильтруемых подключений превышает это ограничение, то лишние подключения отбрасываются и создаются соответствующие записи в журнале. Также для данного события вы можете создать тревогу. При этом устройство Firebox может отправить SNMP ловушку на SNMP сервер, или отправить электронное письмо по указанному адресу и или создать всплывающее окно на вашей станции управления

1. Дважды нажмите на политику для ее редактирования.
   Откроется диалоговое окно Edit Policy Properties.

2. Выберите закладку **Advanced**.

3. В выпадающем списке **Connection Rate** выберите максимальное количество соединений в секунду. Настройки по умолчанию не ограничивают скорость соединения.

4. Если вы хотите получить извещение при превышении скорости соединения, выберите опцию **Alarm when capacity exceeded**.

5. Нажмите **Notification** и установите параметры извещения, как описано в “Настройка параметров журнала и уведомлений”

6. Нажмите **OK**.

QoS Маркирование

На сегодняшний день по сетям передаются различные типы трафика, которые конкурируют за пропускную способность.

Весь трафик, в независимости от степени важности, имеет равные шансы быть доставленным в место назначения. Quality of Service (QoS) Маркирование предоставляет наиболее важному трафику возможность быть надежно и быстро доставленным в место назначения.

QoS должен уметь различать типы потоков данных, которые передаются по сети. Затем он должен пометить пакеты данных. QoS Маркирование создает различные классы сервисов для различного типа трафика. Когда вы маркируете трафик, вы изменяете до 6 бит в заголовке пакета данных. Firebox и другое устройство с поддержкой QoS могут использовать маркирование и обеспечить соответствующую обработку пакетов данных. Fireware XTM поддерживает два типа QoS маркирования: IP Precedence-маркирование (так же известное, как Class of Service) и Differentiated Service Code Point (DSCP)-маркирование

Перед тем, как начать

- Убедитесь, что оборудование локальной сети поддерживает QoS маркирование и обработку. Вам так же необходимо убедиться, что ваш ISP поддерживает QoS.

- Использование процедуры QoS в сети требует тщательного планирования. Для начала, Вы можете теоретически определить возможную пропускную способность и затем задать с высоким приоритетом те сетевые приложения, которые могут быть чувствительны к задержкам и джиттеру.

QoS Маркирование на каждый интерфейс и политику

Вы можете использовать QoS Маркирование на каждый интерфейс или политику.

При настройке QoS Маркирования для интерфейса пакеты, которые передаются через этот интерфейс маркируются. QoS Маркирование для политики маркирует трафик, к которому эта политика применяется. QoS Маркирование для политики используется всегда вместо любого QoS Маркирования, настроенного на этом интерфейсе. Например, ваш Firebox получает трафик, маркированный QoS, из внешней сети и отправляет его в Trusted-сеть.

В Trusted-сети уже применяется QoS-маркирование, но вы хотите, чтобы трафик определенной группы пользователей (например руководства) имел более высокий приоритет по сравнению с остальным трафиком, который передается через Trusted-интерфейс. Прежде всего, настройте QoS-маркирование для Trusted-интерфейса и установите все необходимые значения. Затем добавьте политику, в которой при помощи процедуры QoS-маркирования трафику вашего руководства присваивается более высокий приоритет

QoS Маркирование и трафик IPSec

Если вы хотите применить QoS к Ipsec-трафику, вам необходимо создать политику брандмауэра для соответствующей политики IPSec и применить QoS Маркирование для этой политики. Вы так же можете выбрать, сохранять ли исходную маркировку пакета при инкапсуляции его в IPSec-заголовок. Для того чтобы сохранить маркировку пакета выполните следующее:

1. Выберите **VPN** > **VPN Settings**.
   Откроется диалоговое окно VPN Settings.

2. Включите опцию **Enable TOS for IPSec**.

3. Нажмите **OK**.
   Все текущие маркировки сохраняются при инкапсуляции пакетов в IPSec –заголовок.

Для того чтобы удалить маркировку пакета выполните следующее:

1. Выберите **VPN** > **VPN Settings**.
   Откроется диалоговое окно VPN Settings.

2. Отключите опцию **Enable TOS for IPSec**.

3. Нажмите **OK**.
   TOS-биты сбрасываются, и маркирование не сохраняется.

Типы и значения маркирования

Fireware XTM поддерживает два типа QoS Маркирования: Маркирование IP Precedence (также известное как Class of Service) и маркирование Differentiated Service Code Point (DSCP). IP Precedence маркирование изменяет только первые три бита октета TOS. DSCP маркирование использует первые 6 битов октета IP TOS octet.

Оба метода разрешают вам либо оставлять биты в заголовке без изменений, так как они могли быть изменены внешним устройством, или изменять их значения. Значения DSCP могут быть выражены в числовой форме или при помощи специальных ключевых слов, которые соответствуют PHB (per-hop behavior).

Per-hop behavior – это приоритет, который применяется к пакету, который передается из одного места в другое. Fireware DSCP маркирование поддерживает три типа PHB:

Best-Effort

Best-Effort – это тип сервиса установлен по умолчанию и рекомендован для трафика, который является некритичным или передается в режиме реального времени. Если вы не используете QoS маркирование, то весь трафик принадлежит этому типу.

Assured Forwarding (AF)

Assured Forwarding используется для трафика, который требует большей надежности передачи данных , чем Best-Effort. Внутри Assured Forwarding (AF) трафик можно разделить на три класса: Low, Medium и High.

Expedited Forwarding (EF)

Этот тип имеет наивысший приоритет. Обычно используется для критичного трафика или трафика в режиме реального времени. Коды Class-Selector (CSx) обратно совместимы со значениями IP Precedence. Значения CS1-CS7 идентичны значениям IP Precedence от 1 до 7.

Следующая таблица отображает значения DSCP, соответствующие значениям IP Precedence (которые имеют те же значения, что и значение CS) и описание ключевых слов PHB.

Значение DSCP	Эквивалентное значение IP Precedence (CS значения)	Описание: ключевое слово PHB
0		Best-Effort (тоже самое, что отсутствие маркирования)
8	1	Scavenger*
10		AF Class 1 – Low
12		AF Class - Medium
14		AF Class 1 - High
16	2	
18		AF Class 2 - Low
20		AF Class 2 – Medium
22		AF Class 2 - High
24		3
26		AF Class 3 - Low
28		AF Class 3 - Medium
30		AF Class 3 - High
32	4	
34		AF Class 4 - Low
36		AF Class 4 – Medium

38		AF Class 4 - High
40	5	
46		EF
48	6	Internet control
56	7	Network Control

* Класс Scavenger предназначен для трафик с самым низким приоритетом, такой как обмен данными или игры.

Этот трафик имеет приоритет ниже, чем Best-Effort.

Для более подробной информации о значениях DSCP см. в RFC: http://www.rfc-

Включение QoS Маркирование для интерфейса

Вы можете установить значение маркирования по умолчанию для исходящего трафика.

Эти параметры могут быть заменены параметрами, настроенными для политики.

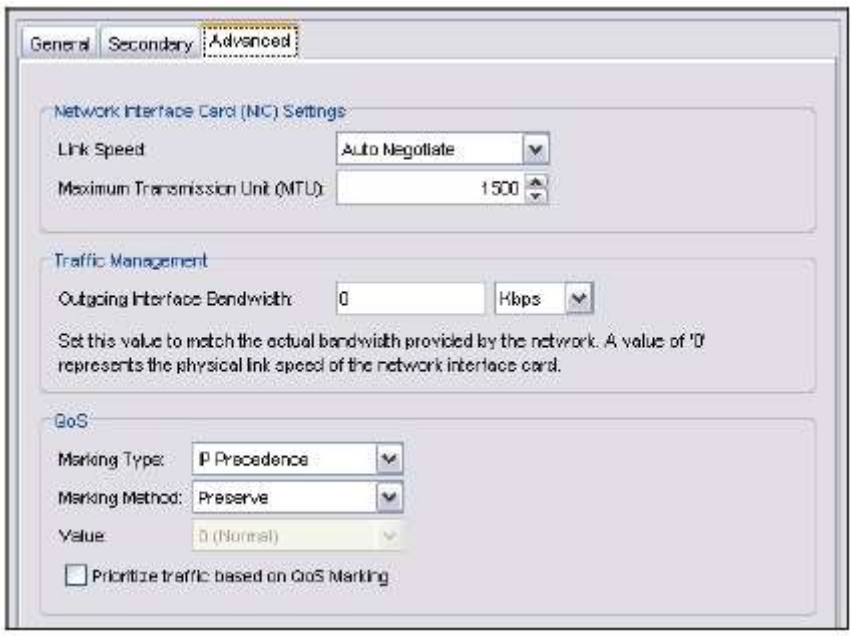
1. Выберите **Setup** > **Global Settings**.
   Откроется диалоговое окно Global Settings.

2. Включите опцию **Enable all traffic management and QoS features**. Нажмите OK.
   Если вы хотите протестировать сеть, то вы можете отключить эти компоненты.

3. Выберите **Network** > **Configuration**.
   Откроется диалоговое окно Network Configuration.

4. Выберите интерфейс, для которого вы хотите включить QoS Маркирование и нажмите **Configure**.
   Откроется диалоговое окно Interface Settings.

5. Нажмите на закладку **Advanced**



6. Из выпадающего списка **Marking Type** выберите **DSCP** или **IP Precedence**.

7. В выпадающем списке **Marking Method** выберите метод маркирования:

   Preserve — не изменять текущее значение битов. Firebox определяет приоритет трафика в зависимости от этого значения.

   Assign — Присвоить биту новое значение.

   Clear — Сбросить бит в ноль.

8. Если вы выбрали **Assign** в предыдущем пункте, установите значение маркирования. Если вы выберете тип маркирования IP Precedence, вы можете выбрать значения от 0 (обычный приоритет) до 7 (наивысший приоритет). Если вы выбрали тип маркирования DSCP, то вы можете выбрать значения от 0 до 56

9. Включите опцию **Prioritize traffic based on QoS Marking**.

10. Нажмите **OK**.

Включение QoS маркирования или настроек приоритизации для политики

Помимо маркирования трафика, который передается через интерфейс Firebox, вы можете маркировать трафик на базе политик. Действие маркирования, которое вы выбрали, применяется ко всему трафику, который использует эту политику.

Несколько политик, которые используют одни и те же действия маркирования, не влияют на работу друг друга. Интерфейсы Firebox могут так же иметь свои собственные настройки QoS маркирования. При использовании QoS маркирования или настроек приоритезации для политики необходимо переопределить для каждого интерфейса настройки QoS маркирования.

1. Дважды нажмите на иконку политики, трафик которой требуется маркировать. *Откроется диалоговое окно Edit Policy Properties.*

2. Нажмите на закладку **Advanced**.

3. Выберите закладку **QoS**.

4. Включите опцию **Override per-interface settings** для включения другого QoS и полей приоритизации.

5. Завершите настройки, как описано в следующем разделе

6. Нажмите **OK**.

7. Сохраните конфигурационный файл

Настройки QoS маркирования

Более подробную информацию о значениях QoS маркирования см. в Marking types and values.

1. В выпадающем списке **Marking Type** выберите один из параметров -- **DSCP** или **IP Precedence**.

2. В выпадающем списке **Marking Method** выберите метод маркирования:

   * **Preserve** — не изменять текущее значение битов. Firebox определяет приоритет трафика в зависимости от этого значения.

   * **Assign** — Присвоить биту новое значение

   * **Clear** — Сбросить бит в ноль.

3. Если вы выбрали **Assign** в предыдущем пункте, установите значение маркирования. Если вы выберете тип маркирования IP Precedence, вы можете выбрать значения от 0 (обычный приоритет) до 7 (наивысший приоритет). Если вы выбрали тип маркирования DSCP, то вы можете выбрать значения от 0 до 56.

4. В выпадающем списке **Prioritize Traffic Based On выберите QoS Marking**.

Настройки приоритизации

Для настройки приоритета трафика используются различные алгоритмы. Fireware использует высокопроизводительный метод на базе алгоритма Hierarchical Token Bucket. Приоритеты в Fireware применяются для каждой политики и эквивалентны уровням CoS (от 0 до 7, где 0 – обычный приоритет и 7 - самый высокий приоритет). При выборе приоритетов используйте информацию, приведенную ниже в таблице. Уровень 5 обычно используется для потоковых данных (VoIP или видеоконференция). Уровень 6 и 7 используйте для политик, которые разрешают административные подключения для того, чтобы избежать интерференции с другим трафиком, который также имеет высокий приоритет. Для того чтобы настроить приоритет трафика для политики выполните следующее:

1. В выпадающем списке **Prioritize Traffic Based On** выберите **Custom Value**.

2. В выпадающем списке **Value** выберите уровень приоритета.

Приоритеты

Мы рекомендуем вам назначать приоритет выше 5, только для административных политик WatchGuard, таких как политика WatchGuard, политика WG-Logging или WG-Mgmt-Server. Для бизнес-трафика выбирайте приоритеты от 0 до 5

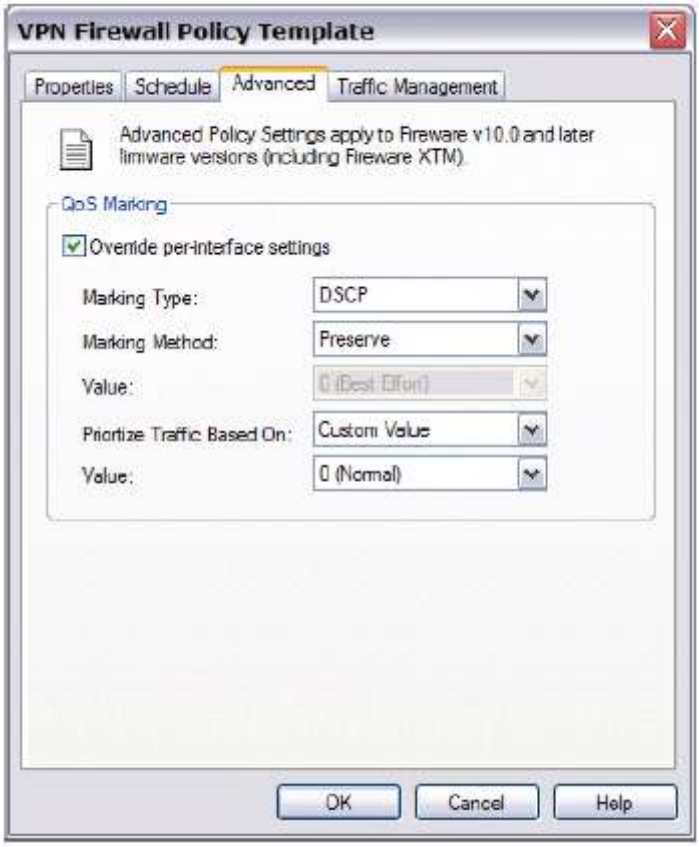
Приоритет	Описание
0	Routine (HTTP, FTP)
1	Priority
2	Immediate (DNS)
3	Flash (Telnet, SSH, RDP)
4	Flash Override
5	Critical (VoIP)
6	Internetwork Control (Настройка удаленного маршрутизатора)
7	Network Control (Управление брандмауэром, маршрутизатором, коммутатором)

Включение QoS маркирования для управляемого BOVPN-туннеля

Для использования QoS с управляемым BOVPN-туннелем необходимо создать шаблон политики VPN-брандмауэра и применить этот шаблон для управляемого BOVPN-туннеля. Вы не можете редактировать политику *Any,* заданную по умолчанию, для управляемого BOVPN-туннеля.

Вы можете использовать QoS маркирование в шаблоне политики VPN брандмауэра для того чтобы устанавливать приоритеты для управляемых BOVPN-туннелей, которые используют различные шаблоны политик. Действие маркирование применяется ко всему трафику, использующему шаблон политики.

1. Откройте Open WatchGuard System Manager и подключитесь к Серверу Управления
2. Выберите закладку **Device Management**.
3. Откройте список **Managed VPNs** и **VPN Firewall Policy Templates**.
4. Выберите необходимый шаблон политики VPN брандмауэра для его редактирования или добавьте шаблон политики VPN брандмауэра.
5. В разделе **Settings** нажмите **Configure**.
   Откроется диалоговое окно VPN Firewall Policy Template.
6. Нажмите на закладку **Advanced**



7. Выберите опцию **Override per-interface settings**.

8. В выпадающем списке **Marking Type** выберите один из двух параметров -- **DSCP** или **IP Precedence**.

9. В выпадающем списке **Marking Method** выберите метод маркирования:

   * **Preserve** — не изменять текущее значение битов. Firebox определяет приоритет трафика в зависимости от этого значения.

   * **Assign** — Присвоить биту новое значение.

   * **Clear** — Сбросить бит в ноль.

10. При выборе типа маркирования – IP Precedence, вы можете выбрать значения от 0 (обычный приоритет) до 7 (наивысший приоритет). Если вы выбрали тип маркирования DSCP, то вы можете выбрать значения от 0 до 56.

11. В выпадающем списке **Prioritize Traffic Based On** выберите метод приоритезации трафика:

    * **Custom Value** — используется величина, заданная пользователем, для назначения приоритета трафику.

    * **QoS Marking** — приоритет трафика на основе QoS маркирования настраивается для шаблона политики.

12. Если вы выберите параметр **Custom Value**, то в выпадающем списке **Value** задайте уровень приоритета

13. Нажмите **OK**.

Управление трафиком и определения политики

Создание действия Traffic Management

Действия Traffic Management используются для ограничения пропускной способности для определенных политик. Действия Traffic Management также могут гарантировать минимальную пропускную способность для групп политик каждого интерфейса. Это позволяет вам управлять величиной пропускной способности, которая выделяется для соединений между Trusted и External интерфейсами, в независимости от соединений между Trusted и Optional интерфейсами, где может быть доступно больше пропускной способности.

Определение доступной пропускной способности

В начале вам необходимо максимально возможную пропускную способность на интерфейсах, для которых используются политики, в настройках которых вы хотите задать гарантированную величину пропускной способности. Для External-интерфейсов эту информацию вы можете узнать у вашего ISP. Вы также можете использовать специальные онлайн программы для измерения скорости передачи данных (в поисковой системе введите *speed test*). Для других интерфейсов можно предположить, что скорость соединения с интерфейсом Firebox является теоретически максимальной полосой пропускания для этой сети.

Вы должны также учитывать пропускную способность интерфейса и в соответствие с этим установить пороговые величины. Если ваш ISP использует асимметричные каналы связи, в качестве порогового значения пропускной способности используйте скорось восходящего потока

Определение суммарной полосы пропускания.

Вам следует так же определить суммарную величину пропускной способности, которую вы хотите гарантировать вашим политикам

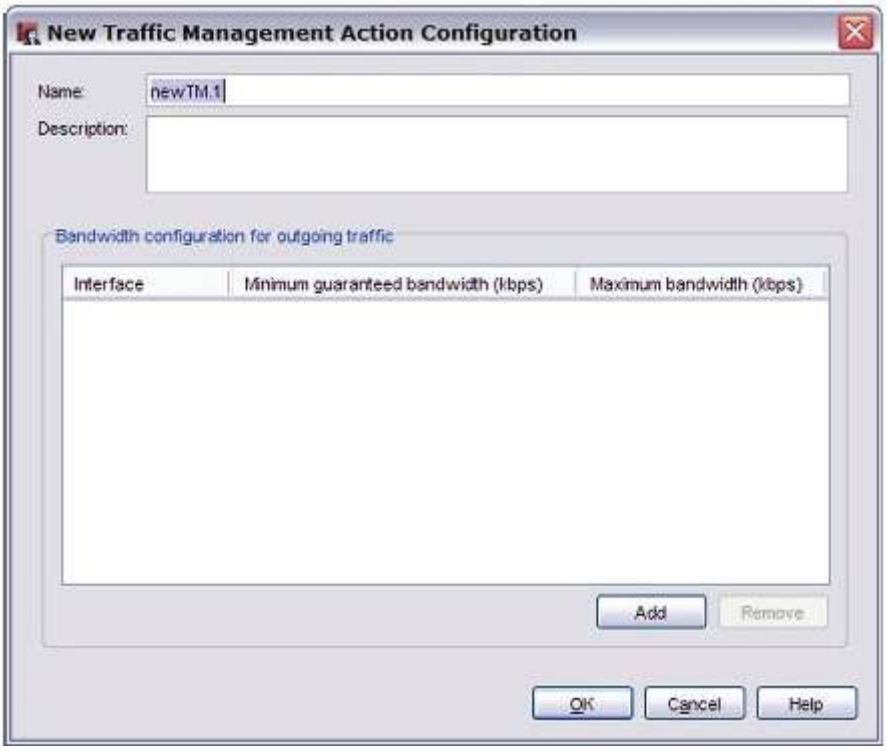
Например, если пропускная способность вашего External интерфейса 1500 кбит/с , то в качестве гарантированной пропускной способности вы можете взять 600 Кбит/с, а 900 кбит/с использовать для остального трафика.

Все политики, использующие данное действие Traffic Management, будут делить скорость передачи данных и величину пропускной способности. После того, как вы создадите политику, она автоматически подключается к действию Traffic Management по умолчанию и не содержит никаких резерваций или ограничений пропускной способности. Если вы создаете действие Traffic Management для установки максимальной пропускной способности в 10 Мбит/с и применяете его к политикам FTP и HTTP, то все FTP и HTTP соединения будут делить эти 10Мбит/с.

Если вы затем добавите то же самое действие в политику SMTP, то после этого FTP, HTTP и SMTP трафик будут делить эти 10 Мбит/с. Такая же логика применяется к скорости передачи данных и гарантированной минимальной пропускной способности. Неиспользуемая гарантированная полосу пропускания, которая резервируется одним действием Traffic Management, может применяться к другим типам трафика.

Создание или изменение действия Traffic Management

1. Дважды нажмите на политику, которой вы хотите гарантировать минимальную пропускную способность. Выберите закладку **Advanced.** Нажмите  **.** Или выберите **Setup > Actions > Traffic Management** и нажмите **Add**.
   Откроется диалоговое окно New Traffic Management Action Configuration



2. В секции **Bandwidth configuration for outgoing traffic** нажмите **Add**.
   Откроется выпадающий список.

3. В колонке **Interface** нажмите на выпадающий список для выбора интерфейса, на котором необходимо установить минимальную пропускную способность.

4. Дважды нажмите на колонки **Minimum guaranteed bandwidth** и **Maximum bandwidth** для редактирования настроек. Введите значение скорости (в кбит/с) для установки минимальной или максимальной пропускной способности.

5. Нажмите **OK**.

6. Если вы создали действие из настроек политики, то теперь новое действие появится в закладке **Advanced** в окне **Traffic Management**. Если создали действие в **Setup > Actions > Traffic Management**, вам необходимо к политике добавить действие Traffic Management.

Добавление действия Traffic Management к политике

После того, как вы создали действие Traffic Management вы можете добавить его к политике

1. Дважды нажмите на политику, для которой необходимо гарантировать минимальную пропускную способность.

2. Нажмите на закладку **Advanced**.

3. В выпадающем списке **Traffic Management** выберите необходимое действие, которое необходимо применить к политике

4. Нажмите **OK** для закрытия диалогового окна **Edit Policy Properties**.Если сумма всех гарантированных пропускных способностей для интерфейсов приближается или превышает пропускную способность, установленную вами на интерфейсе, то откроется предупреждающее сообщение.
   Новое действие откроется в диалоговом окне Traffic Management Actions.

Если вы хотите посмотреть пропускную способность, используемую политикой, выберите закладку **Service Watch** в Firebox System Manager и установите **Bandwidth** вместо **Connections**

Если вы используете multi-WAN, то ограничения пропускной способности применяется отдельно к каждому интерфейсу.

Добавление действия traffic management к нескольким политикам

При добавлении действия Traffic Management к нескольким политикам максимальная и минимальная пропускная способность применяются к каждому интерфейсу в вашей конфигурации. Если две политики используют действие, максимальная пропускная способность для которого равна 100 кбит/с на одном интерфейсе, то весь трафик, который передается через этот интерфейс, и который соответствует этим политикам, будет ограничен до 100 кбит/с.

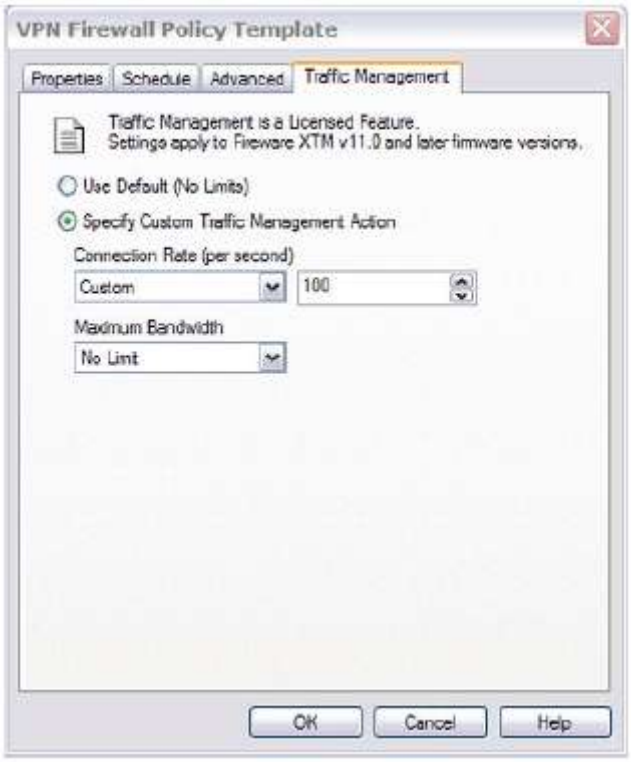
Если вы ограничили пропускную способность на интерфейсе, который используется несколькими приложениями, каждое из которых имеет уникальный порт, то возможно всем подключениям с высоким приоритетом необходимо будет использовать одно действие Traffic Management. Если у вас есть достаточное количество пропускной способности, вы можете создать действие Traffic Management для каждого приложения.

Добавление действия Traffic Management для политики BOVPN брандмауэра

Для того чтобы использовать Traffic Management с управляемым BOVPN-туннелем вам следует создать шаблон политики VPN брандмауэра и применить этот шаблон для управляемого VPN-туннеля.

Вы не можете редактировать политику Any, заданную по умолчанию, для управляемых BOVPN-туннелей. Вы можете использовать Traffic Management в шаблоне политики VPN-брандмауэра для установления различных лимитов пропускной способности для управляемых BOVPN-туннелей, использующих шаблоны различных политик. Действие маркирования применяется для всего трафика, который использует шаблон политики

1. Откройте **WatchGuard System Manager** и подключитесь к управляемому серверу.
2. Нажмите на закладку **Device Management** .
3. Откройте списки **Managed VPNs** и **VPN Firewall Policy Templates**.
4. Добавьте или выберите шаблон политики VPN-брандмауэра
5. В разделе **Settings** нажмите **Configure**.
   Откроется диалоговое окно VPN Firewall Policy Template.
6. Нажмите на закладку **Traffic Management**



7. Выберите опцию **Specify Custom Traffic Management Action**.

8. Создайте действие Traffic Management, как описано в “Создание действия Traffic Management”.

9. Нажмите **OK**.

Глава 16 - Защита от угроз, заданная по умолчанию

Защита от угроз

ОС WatchGuard Fireware XTM и политики, созданные вами, обеспечивают вам строгий контроль доступа к ресурсам сети. Политики доступа помогают защитить вашу сеть от хакеров. Однако, существуют типы атак, от которых политика не сможет защитить. Аккуратная настройка процедуры обработки пакетов, установленная по умолчанию на устройстве WatchGuard, поможет защитить вашу сеть от атак типа «SYN-флуд», «спуфинг» и сканирования портов и адресного пространства

При использовании процедуры обработки пакетов, брандмауэр экран просматривает адрес источника и адрес назначения каждого принимаемого пакета. Он просматривает IP-адрес и номер порта и сравнивает содержимое пакетов с содержимым, которое может нести угрозу для вашей сети.

Если существует угроза, вы можете настроить Firebox для автоматической блокировки возможных атак. Такой способ обнаружения попыток проникновения в сеть помогает защитить вашу сеть от хакеров.

Для более подробной информации о настройке защиты по умолчанию см:

- Опции обработки пакетов по умолчанию
- Заблокированные сайты
- Заблокированные порты

Вы также можете приобрести дополнительный сервис по обнаружению атак на основе сигнатур. Для более подробной информации см. “Gateway AntiVirus и Intrusion Prevention”

Опции обработки пакетов по умолчанию

Когда ваше устройство WatchGuard получает пакет данных, оно проверяет адреса источника и назначения этого пакета, включая IP-адреса и номер порта.

Устройство так же проверяет пакеты на наличие содержимого, которое может нанести вред вашей сети. Эта процедура называется *обработкой пакетов по умолчанию* (*default packet handling*).

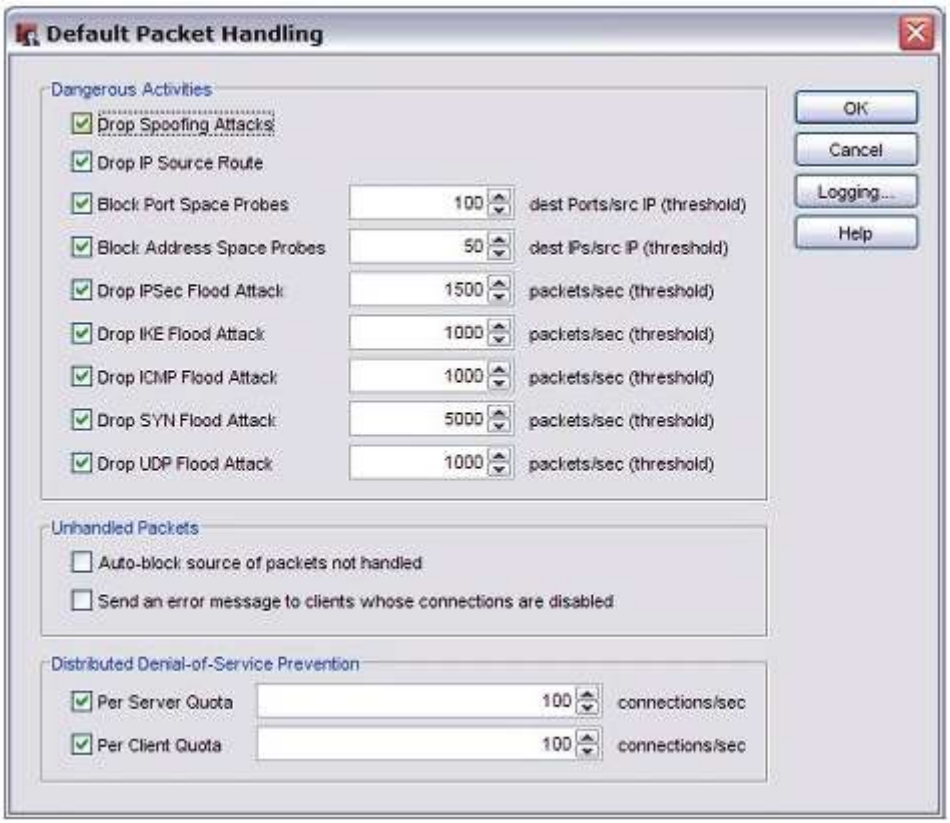
Обработка пакетов по умолчанию может:

- Блокировать пакеты, которые несут потенциальную угрозу, включая пакеты, которые могут быть частью атак типа «SYN flood» и «спуфинг»
- Автоматически блокировать весь трафик от и на определенный IP-адрес
- Добавлять событие в файл журнала
- Отправлять SNMP-ловушку на SNMP-сервер
- Отправлять уведомление о возможных угрозах безопасности

Большинство опций обработки пакетов по умолчанию включены в конфигурацию устройства WatchGuard.Вы можете изменять пороговые величины параметров, по достижении которых устройство WatchGuard предпринимает какое-либо действие

Вы можете так же изменять опции, выбранные для обработки пакетов по умолчанию.

1. В Policy Manager нажмите  . Или выберите **Setup** > **Default Threat Protection** > **Default Packet Handling**.
   Откроется диалоговое окно Default Packet Handling



2. Выберите опции для шаблонов трафика, которые вы хотите применять, как описано в следующих разделах:

   * Атаки типа «Спуфинг»

   * Атаки IP-маршрута источника

   * Сканирование портов и адресного пространства

   * Атаки типа «Флуд»

   * Необработанные пакеты

   * DDos-атаки

Настройка ведения журналов и уведомлений

По умолчанию Firebox при наступлении одного из событий, указанных в диалоговом окне **Default Packet Handing,** создает запись в журнале

Для настройки SNMP ловушек и уведомлений выполните следующее:

1. Нажмите **Logging**.
   Откроется диалоговое окно Logging and Notification.

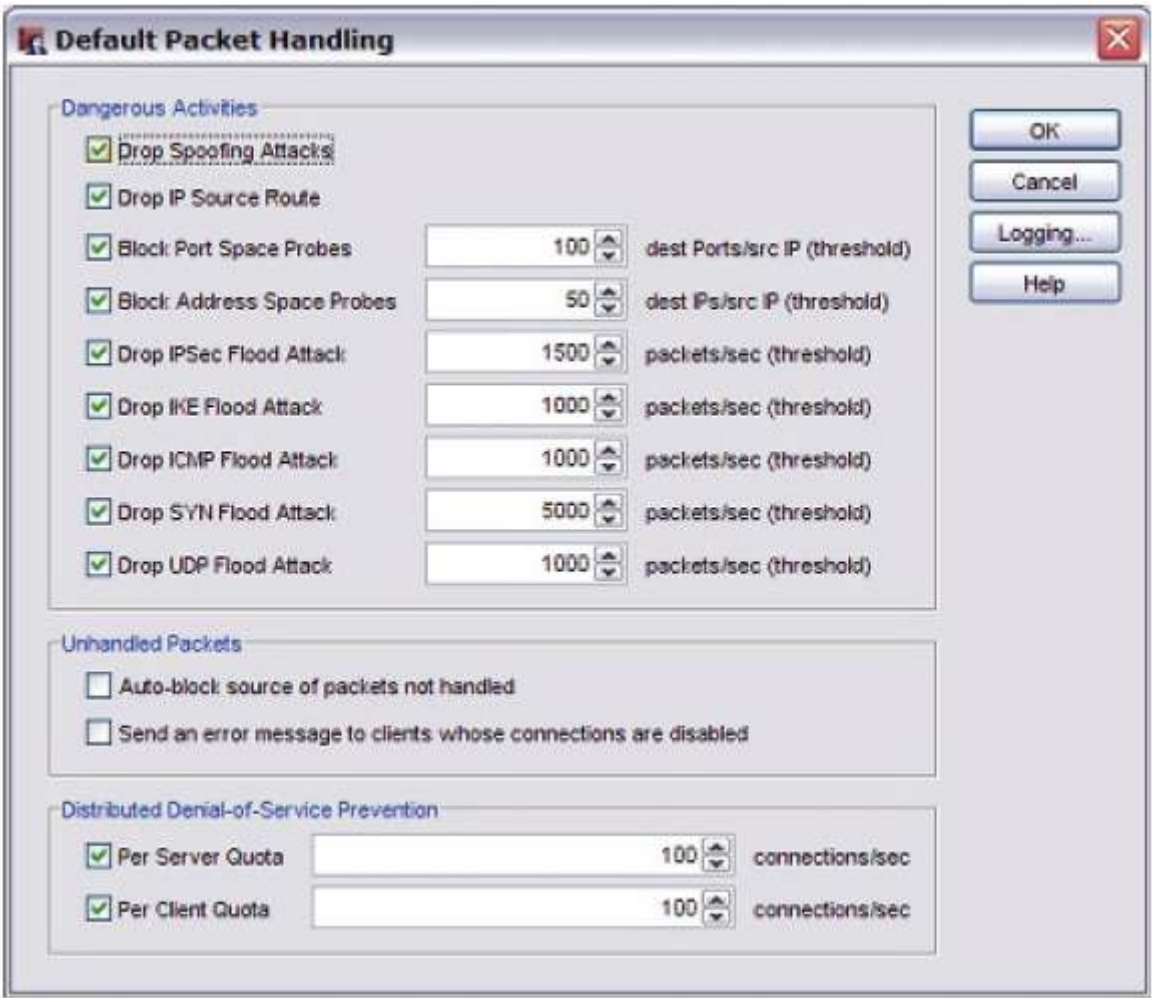
2. Выполните необходимые настройки уведомления, как описано в “Настройка параметров журнала и уведомлений”

Атаки типа «Спуфинг»

Одним из способов получения доступа в вашу сеть является процедура IP спуфинга. При “IP-спуфинге” хакер отправляет TCP/IP пакет, который вместо IP-адреса его реального источника, использует другой IP-адрес. При включении функции анти-спуфинга устройство WatchGuard проверяет, принадлежит ли IP-адрес источника пакета сети, подключенной к этому интерфейсу. По умолчанию устройство WatchGuard отражает атаки типа «спуффинг».

Для того чтобы изменить параметры системы защиты от атак типа “IP спуфинг” выполните следующее:

1. В **Policy Manager** нажмите  . Или выберите **Setup** > **Default Threat Protection** > **Default Packet Handling**.
   Откроется диалоговое окно Default Packet Handling



2. Включите или отключите опцию **Drop Spoofing Attacks** .

3. Нажмите **OK**.

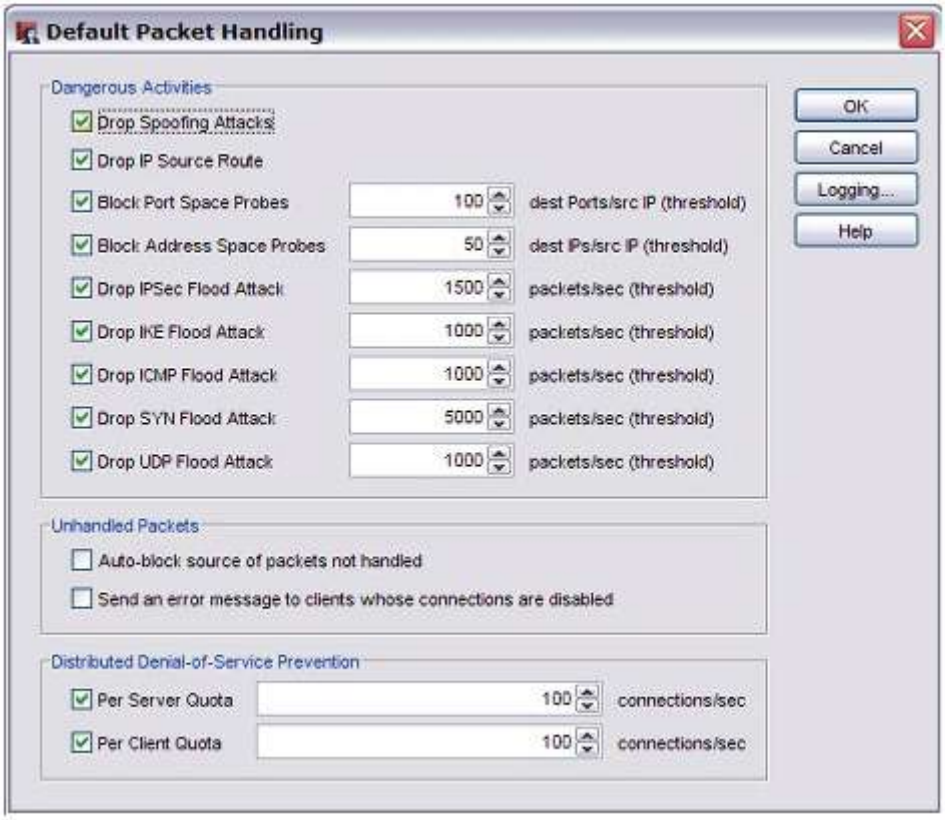
Атаки IP-маршрута источника

Для того чтобы определить маршрута, по которому пакет передавался через сеть, хакер использует атаки IP-маршрута источника. Хакер отправляет IP пакет и использует полученный ответ от вашей сети для того чтобы получить информацию, о том, какая ОС установлена на

компьютере или сетевом устройстве. По умолчанию устройства WatchGuard блокируют атаки IP-маршрута источника.

Для того чтобы изменить параметры защиты от атак маршрута выполните следующее:

1. В Policy Manager нажмите на . Или выберите **Setup** > **Default Threat Protection** > **Default Packet Handling**.
   Откроется диалоговое окно Default Packet Handling



2. Включите или отключите опцию **Drop IP Source Route**.

3. Нажмите **OK**.

Сканирование портов и адресного пространства

Хакеры часто перед тем, как атаковать сеть, собирают информацию об открытых портах на устройствах, подключенных к этой сети. Сканирование портов (*port space probe*) – TCP/UDP-трафик, который отправляется на определенный диапазон портов. Эти порты могут идти по порядку и выбираться случайным образом из диапазона 0 - 65535). Сканирование адресного пространства – TCP/UDP-трафик, который отправляется на определенный диапазон сетевых адресов. Сканирование портов используется для того чтобы определить какие на компьютере запущены сервисы

Сканирование адресного пространства проверяет сеть для просмотра устройств, находящихся в сети. Более подробную информацию о портах см. “Порты”

Как устройство WatchGuard определяет сетевые сканирования

Устройство WatchGuard обнаруживает сканирование портов и адресного пространства только на тех интерфейсах, которые настроены в качестве External.

Сканирование адресного пространства фиксируется, когда компьютер из внешней сети отправляет заданное количество пакетов на IP-адреса, присвоенные External интерфейсам, устройства WatchGuard.

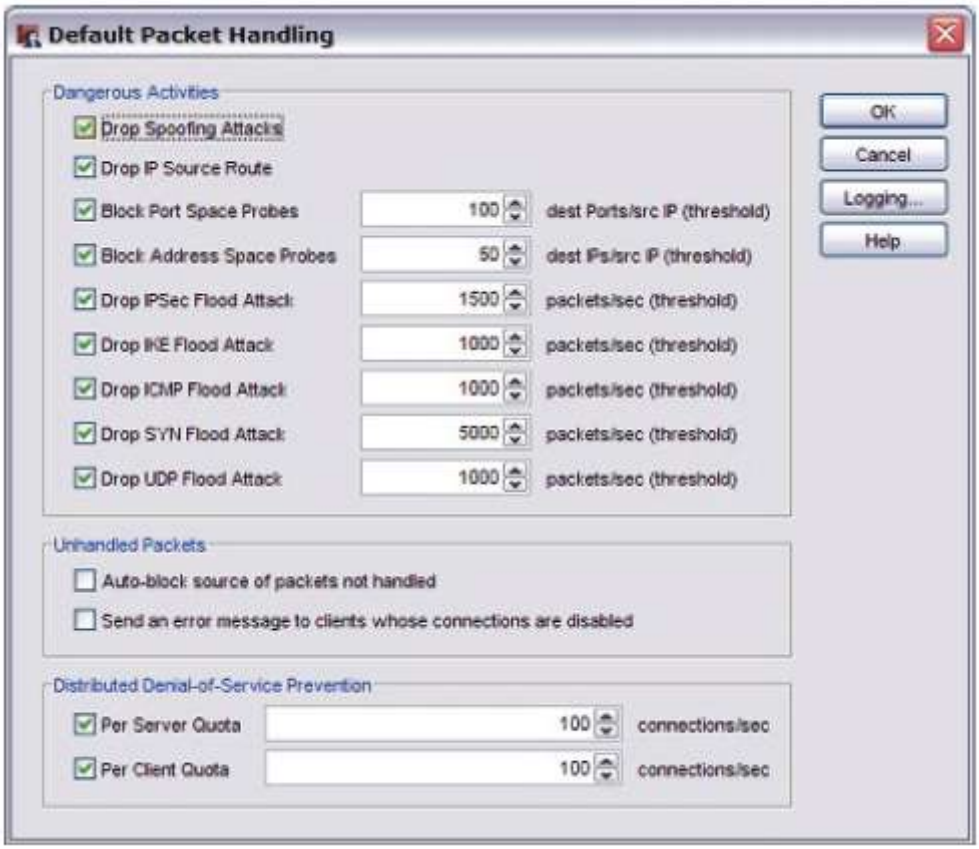
Для обнаружения сканирования портов ваше устройство WatchGuard считает количество пакетов, отправленных от одного IP-адреса на IP-адрес External-интерфейса. Адреса могут включать IP-адрес External интерфейса или вторичные IP-адреса, настроенные на External интерфейсе. Если количество пакетов, отправленных на различные IP-адреса или через определенный диапазон портов за одну секунду больше установленной вами величины, то IP-адрес источника сразу добавляется в список **Blocked Sites**.

Если вы включите опции **Block Port Space Probes** и **Block Address Space Probes ,** то устройство WatchGuard будет проверять весь входящий трафик на всех External интерфейсах. Вы не можете отключать эти опции для определенных IP-адресов или различных периодов времени.

Для защиты от атак типа «сканирования портов и адресного пространства»

По умолчанию устройства WatchGuard блокирует сетевые сканирования. Вы можете изменять настройки этих параметров и изменять максимально допустимое количество сканирований адресов или портов в секунду для каждого IP-адреса источника (по умолчанию данная величина равна 50).

1. В Policy Manager нажмите  . Или выберите **Setup** > **Default Threat Protection** > **Default Packet Handling**.
   Откроется диалоговое окно Default Packet Handling.



2. Выберите или отключите опции **Block Port Space Probes** и **Block Address Space Probes**.

3. Нажмите на кнопку со стрелкой для выбора максимального числа сканирования портов и адресного пространства в секунду с одного и того же IP-адреса. По умолчанию величина **Block Port Space Probes** равна 100, а **Block Address Space Probes** – 50. Это значит, что

источник блокируется, если он инициирует подключение к 100 различным портом или 50 хостам в течении одной секунды.

4. Нажмите **OK**.

Для более оперативного обнаружения попыток сканирования адресного пространства или портов вы можете уменьшить эти пороговые значения. Однако следует учитывать, если вы выберете слишком маленький порог, то вы можете заблокировать нормальный трафик. При использовании более высокого значения существует меньшая вероятность блокировки нормального трафика, но при этом устройство WatchGuard должно будет отправлять пакеты TCP RESET для каждого заблокированного соединения, а это будет влиять на пропускную способность системы и позволит хакерам получить некоторую полезную информацию о вашем брандмауэре

Атаки типа «Флуд»

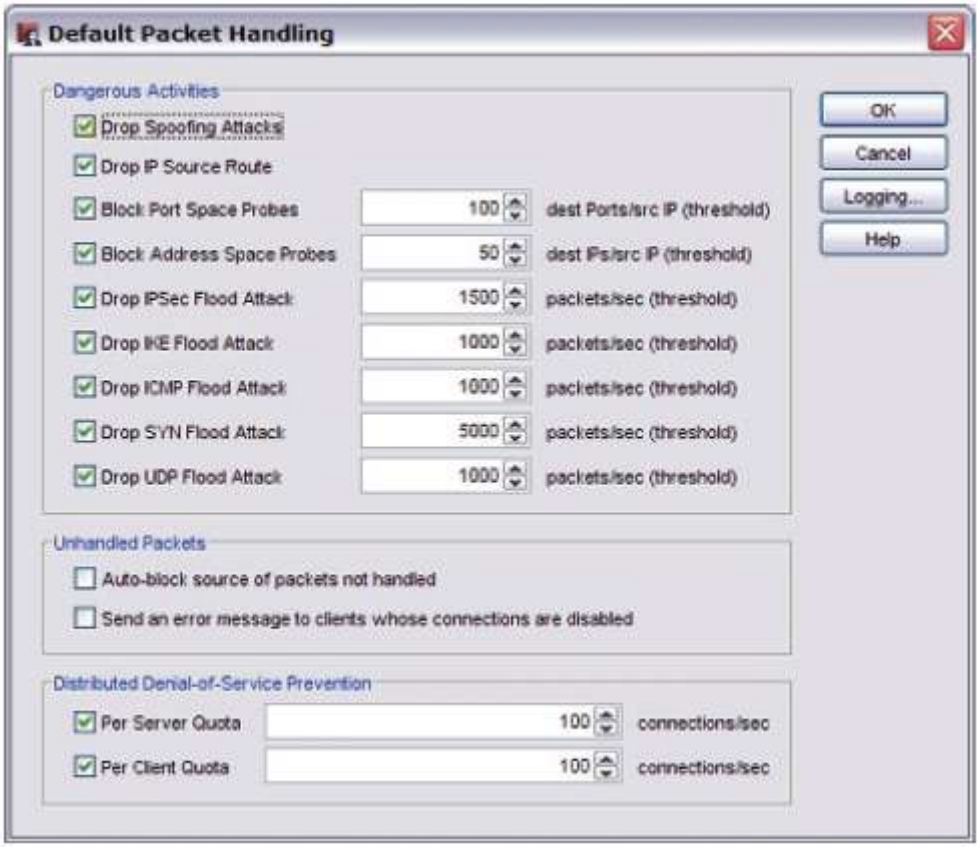
Атаки такого типа подразумевают отправку большого объема трафика на сетевое устройство, которое не будет справляться с такой нагрузкой и начнет блокировать нормальный трафик. Например, атака типа «ICMP flood» заключается в том, что хакер отправляет большое количество ping запросов на указанный хост, который должен использовать все свои ресурсы для того чтобы на каждый ping-запрос присылать ответ

Устройство Firebox может защитить вашу сеть от следующих атак типа «флуд»:

- IPSec флуд
- IKE флуд
- ICMP флуд
- SYN флуд
- UDP флуд

Атаки типа «Флуд» известны также как DoS-атаки. По умолчанию устройство WatchGuard блокирует атаки типа «флуд». Для изменения настроек этой величины или для изменения максимально допустимого числа пакетов в секунду выполните следующее:

1. В Policy Manager нажмите . Или выберите **Setup > Default Threat Protection > Default Packet Handling**.
   Откроется диалоговое окно Default Packet Handling



2. Включите или отключите опции **Flood Attack**.

3. Нажмите на кнопку со стрелкой для выбора максимально допустимого числа пакетов в секунду для каждого IP-адрес источника. Например, если настройка содержит 1000, то Firebox блокирует источник, если он отправляет более чем 1000 пакетов в секунду

4. Нажмите **OK**.

Параметры для атак типа «SYN flood»

Для атак типа «SYN флуд» вы можете установить пороговое значение, при достижении которого устройство WatchGuard, сообщает о возможной атаке типа «SYN флуд», но пакеты при этом не сбрасываются. Если же количество пакетов превышает пороговую величину в два раза, то они сбрасываются устройством WatchGuard. Если количество пакетов находится между пороговой величиной и величиной в два раза большена, и поля src_IP, dst_IP и total_length текущего и предыдущего пакетов совпадают, текущий пакет будет сбрасываться. В противном случае 25 процентов новых пакетов будет сброшено.

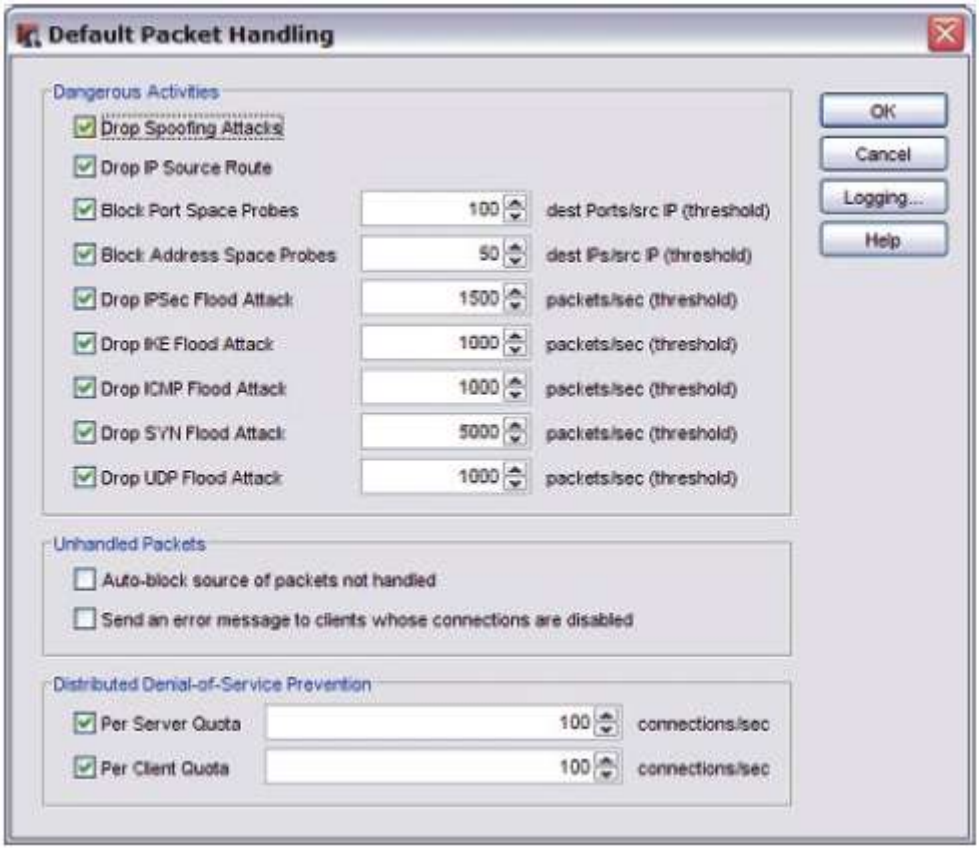
Например, если вы установили порог в 18 пакетов в секунду. Когда устройство получает такое количество пакетов в секунду, то оно предупреждает вас о возможной атаке типа «SYN флуд», но пакеты при этом не отбрасывает. Если устройство начинает получать 20 пакетов в секунду, то оно сбрасывает 25% пакетов (5 пакетов). Если устройство начинает получать 36 и более пакетов в секунду, то последние 18 или больше пакетов обрасываются

Необработанные пакеты

“Необработанный” пакет – это пакет, который не совпадает ни с одним правилом политики.

Firebox всегда блокирует такой пакет. Однако вы можете изменить настройки устройства для защиты вашей сети:

1. В Policy Manager нажмите . Или выберите **Setup** > **Default Threat Protection** > **Default Packet Handling**.
   Откроется диалоговое окно Default Packet Handling



2. Выберите или отключите флажки для этих опций:

   Auto-block source of packets not handled

   Автоматическая блокировка источника необработанных пакетов. Адрес источника добавляется в список Blocked Sites.

   Send an error message to clients whose connections are disabled

   Когда устройство WatchGuard получает необработанный IP-пакет, то клиенту возвращается сообщение TCP reset или ICMP ошибка.

Статистика по необработанным пакетам

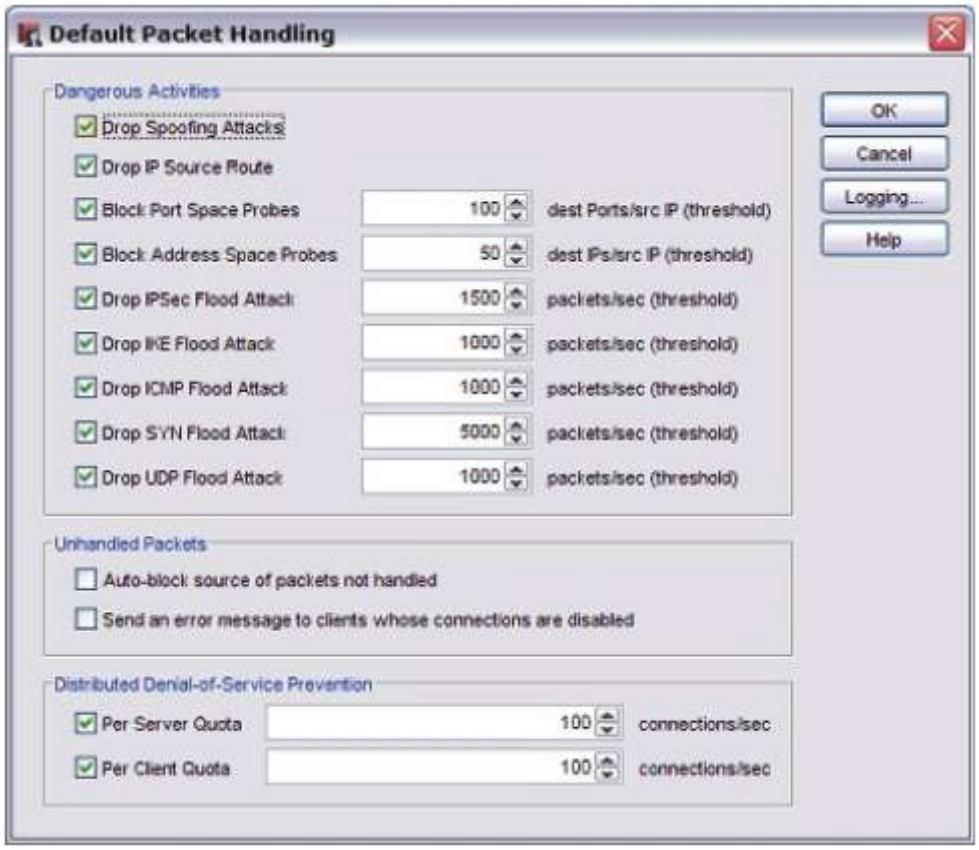
Вы можете просмотреть статистику необработанных пакетов, полученных устройством WatchGuard, в закладке Service Watch в Firebox System Manager. При помощи выпадающего списка **Show connections by** вы можете посмотреть статистику по необработанным пакетам для политик или правил

DDos-атаки

DDoS-атаки напоминают атаки типа «флуд». При DDoS атаке большое количество клиентов и серверов отправляют запросы на одну компьютерную систему с целью ее перегрузить и сделать недоступной для целевых пользователей. Конфигурация по умолчанию устройства WatchGuard

блокирует DDoS-атаки. Вы можете изменять настройки этой величины и максимально допустимого количество соединений в секунду.

1. В Policy Manager нажмите . Или выберите **Setup** > **Default Threat Protection** > **Default Packet Handling**.
   Откроется диалоговое окно Default Packet Handling



2. Выберите или отключите опции **Per Client Quota** or **Per Server Quota**.

3. Нажмите на кнопку со стрелкой для установки максимально допустимого числа соединений в секунду от IP-адреса источника, защищаемого устройством WatchGuard (**Per Client Quota**) или IP-адрес назначения, защищаемого устройством WatchGuard (**Per Server Quota**).

Соединения, которые превышают данное ограничение, отбрасываются.

Заблокированные сайты

Заблокированный сайт – это IP-адрес, который не может подключиться через WatchGuard.

Вы сообщаете устройству WatchGuard о блокировке определенных подозрительных сайтов. При обнаружении подозрительного трафика вы можете заблокировать все соединения с этого IP-адреса. Вы так же можете настроить устройство WatchGuard таким образом, чтобы оно при каждой попытке заблокированного источника к вашей сети. В файле журнала вы можете посмотреть сервисы, которые используются для атак.

Firebox отбрасывает весь трафик от заблокированного IP-адреса.Вы можете создать два типа заблокированных IP адресов: заблокированные на постоянной основе и автоматически заблокированные.

Сайты, заблокированные на постоянной основе

Сетевой трафик с заблокированных сайтов всегда блокируется. Эти IP-адреса хранятся в списке Blocked Sites и добавляются вручную. Например, вы можете добавить IP-адрес, который постоянно пытается просканировать вашу сеть, в список Blocked Sites

Автоматически заблокированные сайты/ Временно заблокированные сайты

Пакеты с автоматически заблокированных сайтов блокируются на протяжении указанного вами промежутка времени. Firebox использует правила обработки пакетов, которые указаны для каждой политики, для того чтобы определить, заблокирован ли сайт или нет.

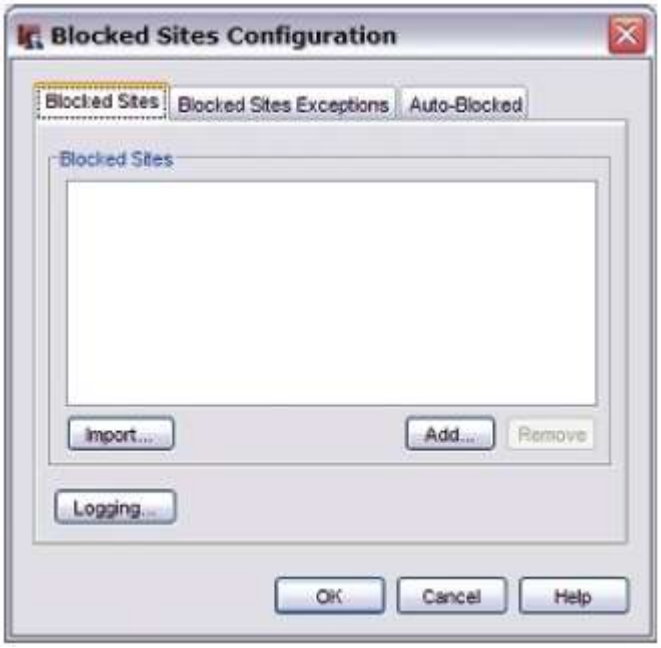
Например, если вы создадите политику, которая запрещает весь трафика через порт 23 (Telnet), то любой IP-адрес, который попытается отправить Telnet трафик через этот порт, будет автоматически заблокирован на указанный вами период времени.

Для более подробной информации об автоматической блокировке сайтов см. “Временная блокировка сайтов при помощи политики”. Вы также можете автоматически блокировать сайты, которые являются источниками пакетов, которые не совпадают ни с одним созданным вами правилом.

Для более подробной информации см. “Необработанные пакеты”

Заблокировать сайт на постоянной основе

1. В Policy Manager нажмите  . Или выберите **Setup > Default Threat Protection > Blocked Sites**.
   Откроется диалоговое окно Blocked Sites Configuration



2. Нажмите **Add**.
   Откроется диалоговое окно Add Site

3. В выпадающем списке **Choose Type** выберите метод идентификации заблокированных сайтов: **Host IP**, **Network IP**, **Host Range**, **or Host Name (DNS lookup)**.

4. Введите значение.
   Значение отображает IP-адрес или диапазон IP-адресов. Если вам необходимо блокировать диапазон адресов, которые включает один или несколько IP-адресов, присвоенных интерфейсам устройства WatchGuard, вам следует, прежде всего, добавить эти IP-адреса в список исключений **Blocked Sites Exceptions**. Для добавления исключений см. в "Создание исключений для списка Blocked Sites"

5. (Дополнительно) Введите дополнительную информацию о заблокированном сайте.

6. Нажмите **OK**.
   Новые сайт появится в списке Blocked Sites.

Настройка журнала для заблокированных сайтов

Вы можете настроить WatchGuard для генерации сообщений журнала, когда хост пытается использовать заблокированный сайт.

В диалоговом окне **Blocked Sites Configuration**:

1. Нажмите Logging.
   Откроется диалоговое окно Logging and Notification.

2. Сконфигурируйте настройки извещения, как описано в "Настройка параметров журнала и уведомлений"

Создание исключений для списка Blocked Sites

При добавлении сайта в список Blocked Site Exceptions трафик с этого сайта не блокируется функцией автоматической блокировки

1. В Policy Manager выберите **Setup** > **Default Threat Protection** > **Blocked Sites**. Нажмите на закладку **Blocked Sites Exceptions**

2. Нажмите **Add**.
Откроется диалоговое окно Add Sit.

3. В выпадающем списке **Choose Type** выберите тип участника: **Host IP**, **Network IP**, **Host Range**, или **Host Name (DNS lookup)**.

4. Введите значение участника.
Поле Member type определяет, используется ли IP-адрес или диапазон IP-адресов. При вводе IP-адреса необходимо вводить все цифры и точки. Не используйте клавиши со стрелками или клавишу Tab.

5. Нажмите **OK**.

Импорт списка заблокированных сайтов или исключений

Если у вас есть несколько WatchGuard, и вы хотите на каждом Firebox заблокировать одни и те же сайты, вы можете создать список сайтов во внешнем файле и импортировать этот файл на каждый WatchGuard. Это должен быть текстовый файл (.txt). IP-адреса в текстовом файле должны быть разделены пробелами или разрывом строки. Для указания сетей используйте slash-нотацию. Для того чтобы записать диапазон адресов, начальный и конечный адреса разделяйте дефисом. Например:

2.2.2.2 5.5.5.0/24

3.3.3.3-3.3.3.8

6.6.6.6 7.7.7.7

Для того чтобы импортировать IP-адреса в список Blocked Sites или Blocked Sites Exceptions для текущего устройства WatchGuard необходимо выполнить:

1. В Policy Manager выбрать **Setup** > **Default Threat Protection** > **Blocked Sites**.
   Откроется диалоговое окно Blocked Sites Configuratio.

2. Для импорта заблокированных сайтов из файла нажать на закладку **Blocked Sites**. Или для импорта исключений нажать на закладку **Blocked Site Exceptions**.

3. Нажать **Import**.
   Откроется диалоговое окно Select a File.

4. Найдите необходимый файл. Нажмите **Select a File**.
   Сайты в файле появятся в списке Blocked Sites или Blocked Sites Exceptions.

5. Нажмите **OK**.

Временная блокировка сайтов при помощи политики

При помощи параметров политики вы можете заблокировать сайты, которые пытаются использовать запрещенный сервис. IP-адреса заблокированных пакетов добавляется в список сайтов Temporary Blocked через 20 минут (по умолчанию).

1. В Policy Manager дважды нажмите на иконку политики для заблокированных сервисов.
   Откроется диалоговое окно Edit Policy Properties.

2. В закладке **Policy** убедитесь, что в выпадающем списке **Connections Are** установлено **Denied** или **Denied (send reset)**.

3. В закладке **Properties** выберите опцию **Auto-block sites that attempt to connect**. По умолчанию. IP-адреса заблокированных пакетов добавляются в список Temporary Blocked Sites за 20 минут.

При включении журнала для временно заблокированных сайтов, вы можете смотреть, какие сайты были временно заблокированы, и решить какие сайты можно заблокировать на постоянной основе

Для включения журнала заблокированных сайтов необходимо:

1. В определении политики нажать на закладку **Properties.**

2. Нажмите **Logging**.

3. Выбрать опцию **Send log message**.

Изменение продолжительности автоматически заблокированных сайтов

Для включения параметров автоматической блокировки необходимо:

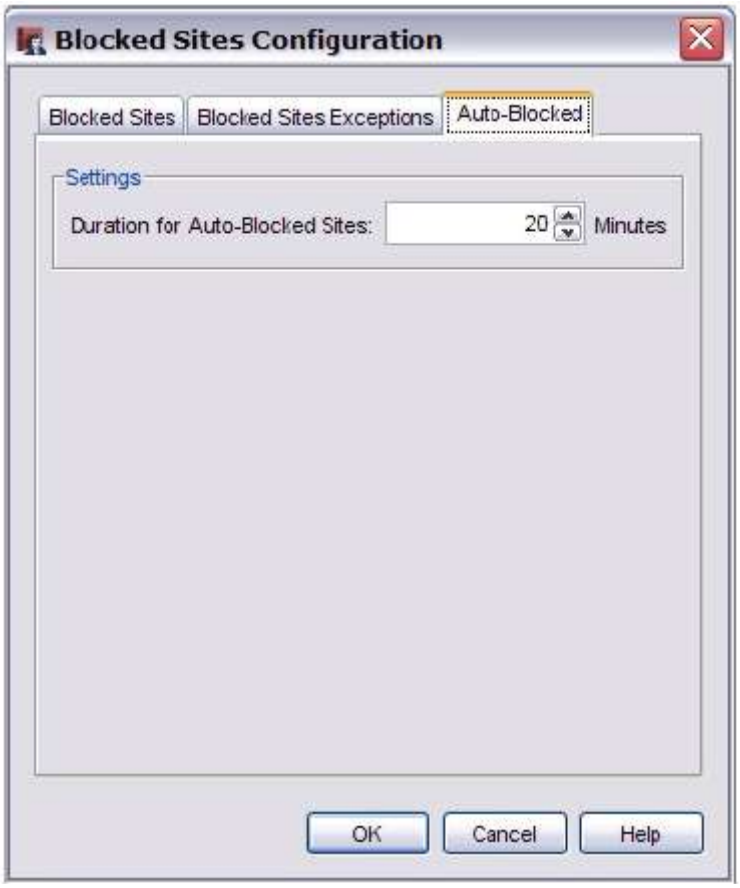
В Policy Manager выбрать **Setup > Default Threat Protection > Default Packet Handling**. Для более подробной информации см. в “Необработанные пакеты”

Вы можете так же использовать настройки политики для автоматической блокировки сайтов, которые пытаются использовать заблокированный сервис. Для более подробной информации см. в “Временная блокировка сайтов при помощи политики”

Для установки продолжительности автоматически заблокированных сайтов необходимо:

1. В Policy Manager выберите **Setup** > **Default Threat Protection** > **Blocked Sites**.

2. Нажмите на закладку **Auto-Blocked**



3. Нажмите на кнопку со стрелкой **Duration for automatically blocked sites** для изменения промежутка времени, в течение которого сайт находится в автоматической блокировке. По умолчанию эта величина равна 20 минутам.

4. Нажмите **OK**.

Заблокированные порты

Вы можете заблокировать порты, которые могут быть использованы для атаки вашей сети. Это приведет к остановке некоторых сетевых сервисов. Блокирующие порты могут защитить ваши наиболее уязвимые сервисы. При блокировке порта вы заменяете все правила в определении вашей политики. Для блокировки порта см. в “Блокировка порта”

Заблокированные по умолчанию порты

По умолчанию WatchGuard блокирует некоторые порты назначения. Это базовая конфигурация, которую вам не надо изменять. TCP и UDP пакеты блокируются для следующих портов:

X Window System (порты 6000-6005)

X Window System (или X-Windows) подключение клиента не шифруется и опасно для использования в сети Интернет.

X Font Server (порт 7100)

Многие версии X-Windows работают с Серверами X Font. На некоторых хостах Серверы X Font обладают правами суперпользователей.

NFS (порт 2049)

NFS – это часто используемый TCP/IP сервис, где несколько пользователей используют одни и те же файлы в сети. Однако новые версии сервиса обладают проблемами, связанными с аутентификацией и безопасностью. Использование NFS в сети Интернет может быть очень опасным.

Portmapper часто использует порт 2049 для NFS. Если вы используете NFS, убедитесь, что NFS использует порт 2049 на всех ваших системах.

rlogin, rsh, rcp (порты 513, 514)

Эти сервисы предоставляют удаленный доступ к компьютерам. Они являются потенциальной угрозой, и хакеры часто используют эти сервисы.

RPC portmapper (порт 111)

Сервис RPC Services использует порт 111 для поиска портов, которые используются данным RPC сервером. Сервисы RPC могут быть легко атакованы из сети Интернет.

порт 8000

Многие компании-разработчики используют этот порт, поэтому с этим портом связаны множеством проблем с безопасностью.

Порт 1

Сервис TCPmux использует Порт 1, но не часто. Для того чтобы усложнить программам процедуру поиска портов, вы можете заблокировать этот порт.

port 0

Этот порт всегда заблокирован устройством WatchGuard. Вы не можете разрешить трафик через порт 0.

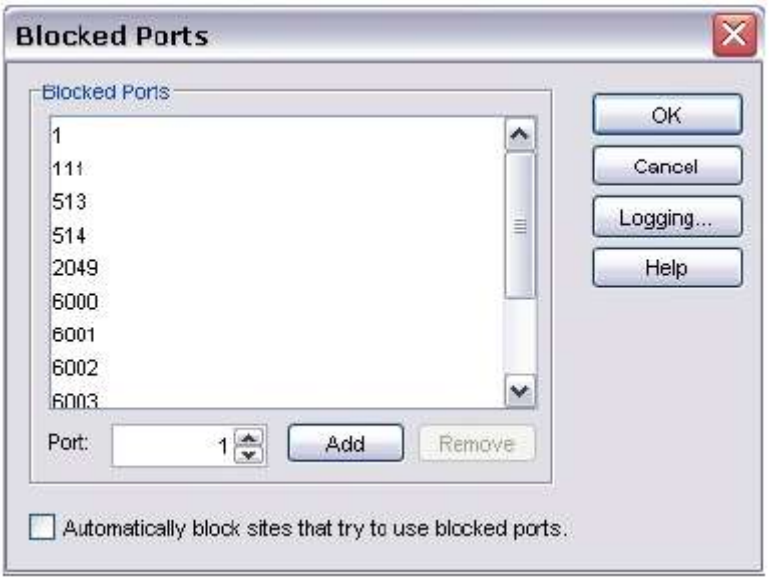
Если вам необходимо разрешить трафик для приложений, которые используют заблокированные по умолчанию порты, мы рекомендуем разрешить трафик для них только через IPSec VPN туннель или использовать ssh для доступа к этому порту.

Блокировка порта

1. В Policy Manager нажмите  . Или выберите **p**.
   Откроется диалоговое окно Blocked Ports.

2. Нажмите на поле со стрелкой **Port** или введите номер порта для блокировки.

3. Нажмите **Add**.
   Номер нового порта появится в списке Blocked Ports.



Блокировка IP-адресов, которые пытаются получить доступ к заблокированным портам

Вы можете настроить WatchGuard для автоматической блокировки external-компьютеров, которые пытаются получить доступ к заблокированным портам.

В диалоговом окне **Blocked Ports** выберите опцию **Automatically block sites that try to use blocked ports**.

Включение журнала и уведомления для заблокированных портов

Вы можете настроить WatchGuard для создания записи в журнале при попытке хоста использовать заблокированный порт. Вы так же можете установить извещение при попытке компьютера получить доступ к заблокированным портам.

В диалоговом окне Blocked Ports необходимо выполнить:

1. Нажать **Logging**.
   Откроется диалоговое окно Logging and Notification.

2. Сконфигурируйте настройку уведомлений, как описано в “Настройка параметров журнала и уведомлений”
   Будьте внимательны при выборе номеров блокирующих портов выше 1023 – клиенты часто используют их в качестве номера порта источника

Глава 17 - Настройка WatchGuard Server

Серверы WatchGuard System Manager

При установке программного обеспечения WatchGuard System Manager вы можете выбрать для установки один или более серверов WatchGuard System Manager. Вы так же можете запустить программу установки и выбрать для установки только один или несколько серверов без необходимости устанавливать WatchGuard System Manager. При установке сервера программа WatchGuard Server Center автоматически устанавливается. WatchGuard Server Center – единственное приложение, которое вы можете использовать для установки, настройки, резервирования и восстановления всех серверов WatchGuard System Manager.

WatchGuard System Manager включает 5 серверов:

- Сервер Управления (Management Server)
- Сервер Журналов (Log Server)
- Сервер Отчетов (Report Server)
- Сервер Карантина (Quarantine Server)
- Сервер WebBlocker (WebBlocker Server)

Для установки серверов WatchGuard System Manager см. в “Установка серверов WatchGuard System Manager”. Инструкции по установке WatchGuard System Manager см. в “Установка WatchGuard System Manager”

Каждый сервер обладает определенными функциями:

Сервер Управления (Management Server)

Сервер Управления работает на компьютере с ОС Windows. Вы можете управлять всеми устройствами-брандмауэрами и создавать частные сетевые (VPN) туннели при помощи процедуры «drag-and-drop». К основным функциям Сервера Управления относятся:

- Центр Сертификации (ЦС), который выдает сертификаты для IPSec туннелей.
- управление конфигурацией VPN–туннелей
- Управление устройствами Fireware XTM и Firebox

Для более подробной информации о Сервере Управления см. см. “Сервер Управления”

Сервер Журналов (Log Server)

Журнал сервера собирает сообщения журнала для каждого Firebox. Сообщения журнала на Сервер Журналов передаются в зашифрованном виде. Формат сообщения журнала – XML (plain text). Собранная информация включает сообщения журнала для трафика, сообщения о событиях, тревоги и сообщения диагностики. Для более подробной информации см. в “Серверы Журналов”

Сервер Отчетов (Report Server)

Сервер отчетов периодически объединяет собранные Серверами Журналов данные от ваших устройств Firebox и генерирует из них отчеты. Данные сервера отчетов можно просмотреть при помощи специальной утилиты Report Manager. Для более подробной информации см. в “Сервер отчетов”

Сервер Карантина (Quarantine Server)

Сервер карантина собирает и изолирует электронную почту, которые были идентифицирована как спам специальной утилитой spamBlocker. Для более подробной информации см. в “Сервер Карантина”

Сервер WebBlocker (WebBlocker Server)

Сервер WebBlocker работает с HTTP-прокси для блокировки пользователям доступа к определенным сайтам. При настройке Firebox вы можете выбрать, какие категории сайтов вы хотите заблокировать, а какие разрешить. Для более подробной информации см. в “WebBlocker”.

Установка серверов WatchGuard System Manager

WatchGuard Server Center – это единственное приложение, используемое для установки, настройки, резервирования и восстановления всех серверов WatchGuard System Manager. После установки WatchGuard System Manager и серверов WatchGuard мастер настройки WatchGuard Server Center создаст серверы WatchGuard, которые были установлены на ваш компьютер

Мастер настройки отобразит только те страницы, которые соответствуют установленным компонентам. Например, если вы установили Сервер Журналов и Сервер Отчетов, но не установили Сервер Карантина, мастер настройки отобразит только те страницы, которые связаны с параметрами Серверов Журналов и Отчетов. Страница, на которой вы создаете списки доменов для Сервера Карантина, в этом мастере не будет

Если вы не установили или не настроили некоторые серверы WatchGuard, вы можете установить или настроить их позже. Вы можете запускать программу установки для сервера, который вы еще не установили, прямо с главной страницы

Вы также можете запустить мастер настроек для настройки Серверов Журналов, которые до этого не были настроены, прямо с главной страницы WatchGuard Server Center

Перед тем как начать

Перед запуском мастера настроек, убедитесь, что у вас есть вся необходимая информация:

- Если вы хотите использовать шлюз Firebox для защиты Сервера Управления, то вам необходимо знать IP-адрес External интерфейса данного Firebox.
- Лицензионный ключ Сервера Управления
- Если вы хотите установить Сервер Карантина, то вам необходимо знать имена доменов, с которых он будет принимать электронные письма
- Если вы хотите установить Сервер Журналов, то вам необходимо знать IP-адрес устройства, которое будет использоваться как Сервер Журналов

Запуск мастера настроек

1. В панели задач правой кнопкой мыши нажмите на  и выберите **Open WatchGuard Server Center**. Если вы не увидели этот значок, вы не установили ни одно из программного обеспечения сервера WatchGuard.
   Запустится мастер настроек WatchGuard Server Center.

2. На странице приветствия убедитесь в наличии информации, необходимой для завершения мастера настроек.

3. Нажмите **Next**.
На странице общих настроек определите название своей организации.

Общие параметры

1. В поле **Organization name** введите имя название вашей организации. Это имя используется для Центра Сертификации на Сервере Управления. Для более подробной информации см. “Настройка Центра Сертификации на Сервере Управления”

2. Нажмите **Next**.
Откроется страница General Settings - Set Administrator passphrase.

3. Введите и подтвердите пароль администратора (поле **Administrator passphrase**). Пароль должен быть не меньше 8 символов. Пароль администратора используется для управления доступом к станции управления (компьютер, на котором установлен WSM).

4. Нажмите **Next**.

Параметры Сервера Управления

Эти настройки откроются в мастере, только если вы установили Сервер Управления

1. Если у вас есть шлюз Firebox для Сервера Управления, нажмите **Yes**. Несмотря на то, что использование шлюза Firebox является необязательным, мы рекомендуем использовать его для защиты Сервера Управления от сети Интернет

2. Введите внешний IP-адрес и пароль для шлюза Firebox.

3. Нажмите **Next**.
Откроется страница Management Server - Enter a license key.

4. Введите лицензионный ключ для Сервера Управления и нажмите **Add**

5. Нажмите **Next**.

Когда интерфейс, IP-адрес которого привязан к Серверу Управления, выходит из строя и затем перезагружается, мы рекомендуем перезагружать заодно и Сервер Управления

Параметры Серверов Журналов и Отчетов

Данные параметры отображаются в мастере только, если вы установили Сервер Журналов

1. Введите и подтвердите ключ шифрования (**Encryption key),** который используется для защищенного соединения между Firebox и Сервером Журналов. Длина ключа шифрования - 8-32 символа. Вы можете использовать все символы, за исключением пробелов и косых черт (/ или \).

2. В поле **Database location,** которое представляет собой папку со всеми файлами журнала, файлами отчетов и файлами настроек отчетов, появится:
C:\Documents and Settings\WatchGuard\logs.

   Тщательно выбирайте каталог. После установки базы данных вы не можете изменять каталог расположения через пользовательский интерфейс Сервера Журналов. Если необходимо изменить местоположение, см. в “Перемещение каталога с данными журнала”.

   Мы рекомендуем использовать этот путь, предложенный по умолчанию. Для изменения этого пути нажмите на **Browse** и выберите новую папку. Убедитесь, что вы выбрали место с достаточным количеством свободной памяти.

3. Нажмите **Next**.

Параметры Сервера Карантина

Эти параметры появятся в мастере настроек, только если вы установили Сервер Карантина. Список доменов определяет имена доменов, с которых Сервер Карантина принимает электронные письма. Сервер оправляет сообщения только тем пользователям, которые находятся в домене, который есть в списке доменов на сервере Сообщения, отправляемые пользователям и которые не содержатся ни в одном из доменов, удаляются.

1. Для добавления домена введите доменное имя в верхней части текстового окна и нажмите **Add**.
   Доменное имя появится в окне.

   Для удаления домена выберите имя из списка и нажмите **Remove**.
   Доменное имя будет удалено из окна.

2. Нажмите **Next**.

Настройки Сервера WebBlocker

Эти параметры отображаются в мастере настроек только при уже установленном сервере WebBlocker. Вы можете установить базу данных WebBlocker сейчас или позже. Размер базы данных WebBlocker - более чем 200 Мб. Загрузка базы данных может больше 30 минут

Убедитесь, что жесткий диск имеет как минимум 250 Мб свободного пространства.

1. Для загрузки базы данных сейчас выберите **Yes** и нажмите **Download**.
   *Для загрузки базы данных позднее нажмите **No**.*

2. Нажмите **Next**.

Обзор и завершение

Проверьте корректность введенных вами параметров

Для того чтобы изменить значения параметров выполните следующее:

1. Нажимайте **Back** до тех пор, пока не попадете на страницу, которая содержит параметры, которые вы хотите изменить

2. Выполните необходимые изменения.

3. Нажимайте **Next** до тех пор, пока не попадете опять на страницу **Review Settings**.

Если ваши настройки правильные:

1. Нажмите **Next**.
   Мастер настроек отобразит процесс конфигурации сервера.

2. Нажмите **Next**.
   Откроется страница завершения мастера настроек WatchGuard Server Center.

3. Нажмите **Finish**.
   Откроется WatchGuard Server Center.

При помощи WatchGuard Server Center вы можете:

- Следить за состоянием серверов WatchGuard

- Установить Сервер Управления

- Устанавливать Сервер Журналов
- Установить Сервер Отчетов
- Установить Сервер Карантина
- Установить сервер WebBlocker
- Изменять пароль администратора

Шлюз Firebox

Шлюз Firebox помогает защищать ваш Сервер управления от сети Интернет. Мы рекомендуем вам использовать шлюз Firebox.

Если вы добавите IP-адрес для вашего шлюза Firebox, мастер выполнит следующие 3 операции:

- Мастер использует этот IP-адрес для настройки шлюза Firebox, чтобы он разрешил подключения к Серверу Управления.

  Если вы здесь не введете IP-адрес, вам следует настроить брандмауэр между Сервером Управления и сетью Интернет, который разрешал подключения к Серверу Управления по TCP портам 4110, 4112, 4113.

- Если у вас установлена более ранняя версия WatchGuard System Manager и Firebox настроен в качестве DVCP-сервера, мастер получает информацию о DVCP-сервере от шлюза Firebox и перемещает эти настройки в ваш Сервер Управления. Более подробную информацию см. в в *Migration Guide*.

- Мастер настроек устанавливает IP-адрес для Списка Отозванных Сертификатов (CRL).

Устройства, которые вы добавляет в качестве управляемых клиентов, используют этот IP-адрес для подключения к Серверу Управления. Этот IP-адрес должен быть публичным адресом вашего Сервера Управления. Если вы здесь не введете IP-адрес, то мастер настроек в качестве IP адрес списка CRL будет использовать текущий IP адрес компьютера, на котором установлен Сервер Управления. Если компьютер, на котором установлен Сервер Управления, подключен к NAT устройству, то вам необходимо изменить CRL и указать публичный IP-адрес вашего Сервера Управления.

Более подробную информацию см. в “Обновление Сервера Управления с новым адресом шлюза”.

Поиск лицензионного ключа вашего Сервера Управления

В большинстве Firebox X Core and Peak приложений WatchGuard System Manager содержит лицензионный ключ, который позволяет вам управлять вашими устройствами (максимум 4 устройства). Исключение составляют только Firebox X 500 и Firebox X 550e.

Если у вас есть лицензионный ключ VPN Manager от предыдущей покупки Firebox, вы можете использовать его для Сервера Управления. Если у вас нет ни одного лицензионного ключа Сервера Управления, который позволяет управлять более чем одним Firebox или отсутствует лицензионный ключ VPN Manager, вы должны приобрести его у официального реселлера компании WatchGuard

Для того чтобы найти лицензионный ключ Сервера Управления или VPN Manager выполните следующее:

1. Открыть браузер и зайдите на следующую страницу:
   https://www.watchguard.com/archive/manageproducts.asp

   При необходимости войдите в систему

2. Перейдите к нижней части страницы.

3. Нажмите на ссылку **View Details** рядом с WatchGuard System Manager или VPN Manager.
   Откроется список доступных лицензионных ключей.

   При появлении нескольких ключей в списке можно использовать любой из них. Лицензионный ключ имеет следующий формат:

   * *WSMMGR-X-000392-yyyyyyyy*

   * *VPNMGR-X-024535-yyyyyyyy*

   Символ «X» отображает количество устройств, управляемых этим ключом.

   Символ «У» -- строка буквенно-цифровых символов.

4. Используйте один из ключей при запуске мастера настроек WatchGuard Server Center для установки Сервера Управления.

Просмотр состояния серверов WatchGuard

Вы можете просмотреть краткую или полную информацию о ваших серверах WatchGuard.

Просмотр запущенных серверов

Для того чтобы посмотреть список запущенных серверов выполните следующее:

1. Нажмите правой кнопкой мыши на в панели задач.

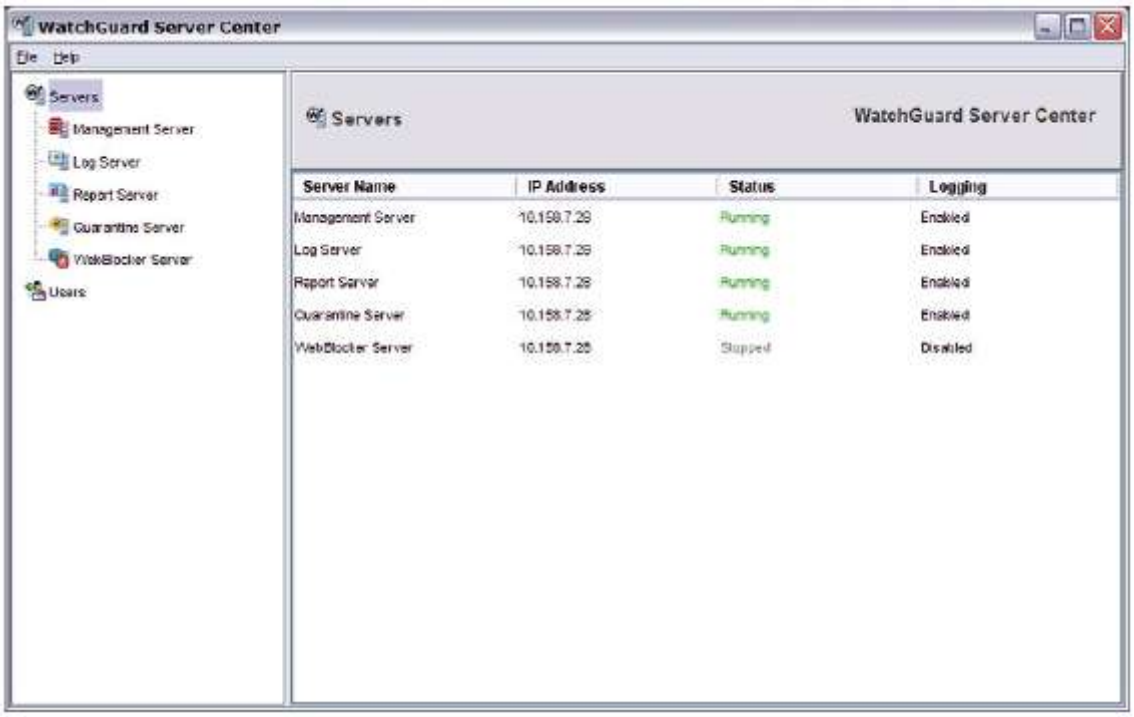
2. Выберите **Server Status**.
   Откроется диалоговое окно WatchGuard Server Center Status со списком установленных и запущенных в данный момент серверов.

Просмотр полной информации о сервере

На компьютере в Серверов Управления:

1. Нажмите правой кнопкой мыши на в панели задач.

2. Выберите **Open WatchGuard Server Center**.
   Откроется диалоговое окно Сервера Управления WatchGuard



Для каждого сервера отобразится страница **Servers**:

- IP-адрес сервера
- состояние: включен/выключен
- состояние журнала: включен/отключен

Настройка вашего сервера WatchGuard

После запуска мастера настроек WatchGuard Server Center для установки ваших серверов вы можете определить каждый сервер более подробно.

Более подробную информацию см. в :

- Сервер Управления
- Серверы Журналов
- Сервер отчетов
- Сервер Карантина
- WebBlocker

Вы так же можете настроить администрирование на базе ролей. Для более подробной информации см. “Администрирование на базе ролей”

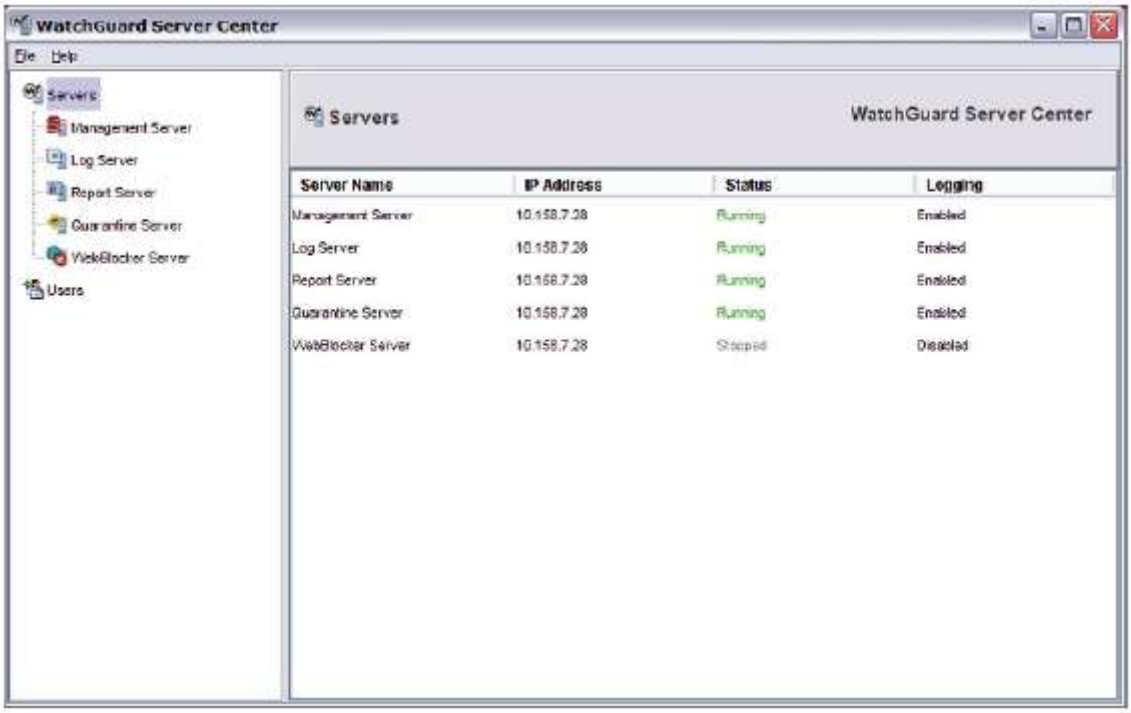
Открытие WatchGuard Server Center

Вы можете использовать WatchGuard Server Center для управления всеми вашими серверами WatchGuard. Для того чтобы открыть WatchGuard Server Center выполните следующее:

1. Нажмите правой кнопкой мыши на  в панели задач или выберите **Open WatchGuard Server Center**.
   Откроется диалоговое окно Connect to WatchGuard Server Center.

2. Введите ваши имя пользователя (**Username**) и пароль (**Administrator passphrase**).

3. Нажать **Login**.
   Откроется диалоговое окно WatchGuard Server Center



4. В меню **Servers** выбрать сервер для настройки.

   - Management Server (Сервер Управления)
   - Log Server (Сервер Журналов)
   - Report Server (Сервер Отчетов)
   - Quarantine Server (Сервер Карантина)
   - WebBlocker Server (Сервер WebBlocker)

Запуск и остановка серверов WatchGuard

Вы можете вручную останавливать и запускать серверы WatchGuard в любое время. При этом вам не надо отключаться от серверов. Для того чтобы остановить сервер в WatchGuard Server Center выполните следующее:

1. В меню **Servers** выберите сервер, который вы хотите остановить. Например, **Log Server (Сервер Журналов)**.

2. Нажмите на сервер правой кнопкой мыши и выберите **Stop Server**.
   Откроется сообщение с предупреждением.

3. Нажмите **Yes** для подтверждения остановки выбранного сервера. Сервер будет остановлен и в верхней части страницы сервера появится сообщение **Stopped**

Например, если вы выключали Сервер Журналов, то появится сообщение вида «Log Server - Stopped».

Для того чтобы запустить сервер в WatchGuard Server Center выполните следующее:

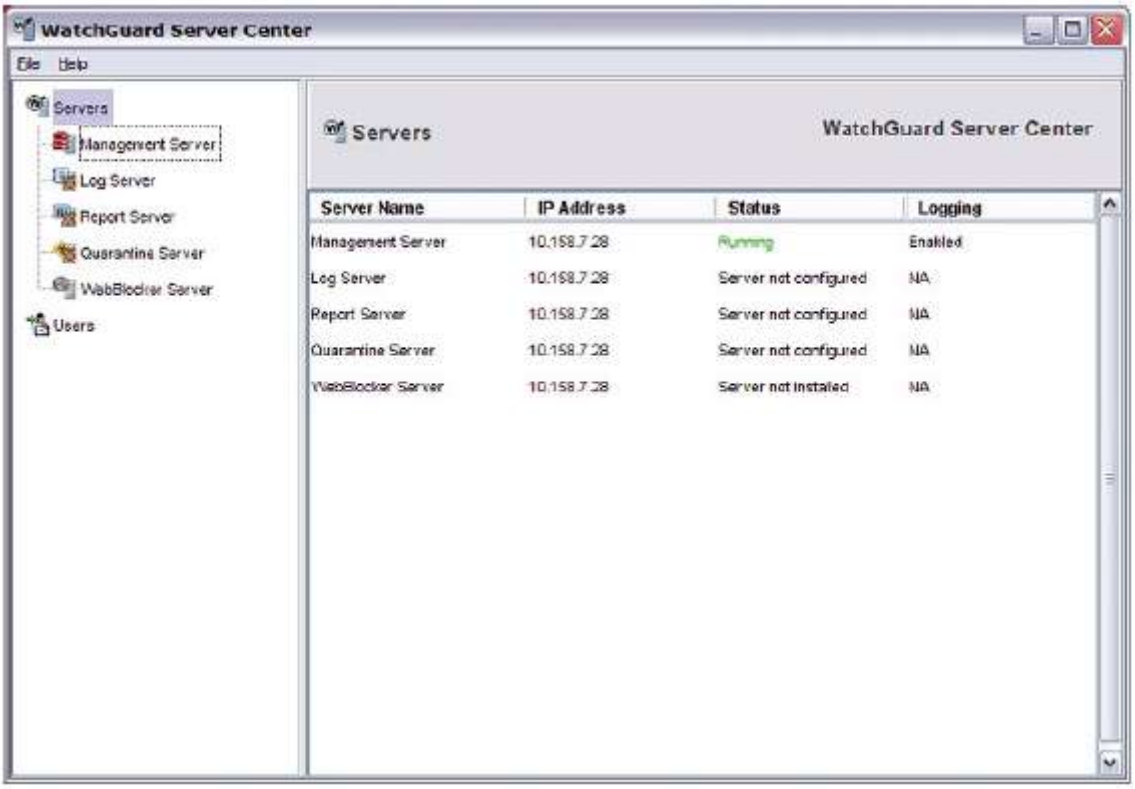
1. В меню **Servers** выберите сервер, который вы хотите запустить. Например, **Log Server**.

2. Правой кнопкой мыши нажмите на сервер и выберите **Start Server**.
Сервис запустится и появится имя сервера в верхней части страницы.
Например, если вы запустили сервер журнала, то появится сообщение о включении Сервера Журнала.

Установка и настройка серверов в WatchGuard Server Center

Если вы уже установили и настроили один или несколько серверов WatchGuard, то вы можете при помощи WatchGuard Server Center (WSC) установить дополнительные серверы или выполнить настройку уже установленных серверов

1. Откройте WatchGuard Server Center.
Откроется главная страница Servers



2. В меню **Servers** выберите сервер для установки или настройки.
Откроется страница выбранного сервера. В примерах ниже вы увидите главную страницу Log Server

Сервер Журнала не установлен

Сервер Журнала не настроен

3. Для установки сервера нажмите **Launch Installer**.
   Откроется диалоговое окно WatchGuard System Manager Installer.

   Для настройки сервера нажмите **Launch Wizard**.
   Откроется мастер настройки WatchGuard Server Center.

4. Если вы хотите установить сервер, то см. инструкции в “Установка WatchGuard System Manager”. Если вы хотите настроить уже установленный сервер, то см. инструкции в “Установка серверов WatchGuard System Manager” для выбранного сервера.

5. Нажмите **Refresh** для обновления страницы сервера.

6. Для настройки установленных серверов повторите пункты 3-5

Открытие или закрытие WatchGuard Server Center

После установки любого сервера WatchGuard значок WatchGuard Server Center автоматически отобразится в панели задач. Это позволяет легко получать доступ к WatchGuard Server Center.

При закрытии WatchGuard Server Center приложение продолжает работать в фоновом режиме, и иконка продолжает отображаться в панели задач. Вы можете закрыть приложение, чтобы оно не продолжало работать в фоновом режиме, а затем снова его включить. При выходе из приложения значок WatchGuard Server Center удаляется из вашей панели задач. Для выхода из WatchGuard Server Center и удаления значка из панели задач:

1. На панели задач нажмите правой кнопкой мыши.

2. Выберите **Exit**.
   Откроется сообщение о подтверждении выхода.

3. Нажмите **Yes**.
   Значок WatchGuard Server Center исчезнет из панели задач.

Для восстановления значка WatchGuard Server Center на панели задач и открытия WatchGuard Server Center:

1. Выберите **Start** > **All Programs** > **WatchGuard System Manager 11.0** > **WatchGuard Server Center**.
   Значок отобразится на панели задач

2. Откройте WatchGuard Server Center.

Глава 18 - Настройка и Администрирование Сервера Управления

Сервер Управления

Сервер Управления WatchGuard позволяет управлять работой нескольких устройств Firebox и VPN-туннелей организаций при помощи одного просто интерфейса управления. Вы можете управлять работой устройств Firebox XTM, Firebox X Core, Firebox X Peak, Firebox X Edge, Firebox III и SOHO 6.

Рабочая станция, настроенная в качестве Сервера Управления, так же выполняет функции Центра Сертификации (CA). Центр Сертификации выдает сертификаты управляемым клиентам, когда они подключаются для загрузки обновлений конфигурации

Установка Сервера Управления

Вы можете установить Сервер Управления на компьютер, который работает под управлением ОС Windows. Настоятельно не рекомендуется использовать для этой цели управляющий компьютер, на котором установлено программное обеспечение WatchGuard System Manager. Мы рекомендуем установить Сервер Управления на компьютер со статическим IP-адресом, который находится за Firebox со статическим внешним IP-адресом. В противном случае, Сервер может неправильно работать.

При запуске программы-установки WatchGuard System Manager вы можете выбрать, какие клиентские и серверные компоненты вы хотите установить. Для того чтобы установить Сервер Управления в списке **Server Components** вам необходимо выбрать **Management Server**

Если вы уже установили WatchGuard System Manager (WSM) и не завершили установку Сервера Управления, вы можете продолжить ее установку.

1. Установите программное обеспечение WatchGuard System Manager.

2. Выберите только **WatchGuard Management Server**. Не выбирайте данную опцию для уже установленных компонентов.

3. Выполните все необходимые инструкции мастера

Настройка Сервера Управления

Инструкции по установки сервера Управления и других серверов WatchGuard см. в “Установка серверов WatchGuard System Manager”

Настройка Сервера Управления

После того, как вы установите Сервер Управления, вы можете выполнять следующие задачи:

- Настройка Центра Сертификации на Сервере Управления

- Настройка параметров управления для Сервера Управления

- Включение и настройка аутентификации на базе Active Directory

- Настройка журналов для Сервера Управления

Настройка параметров для Сервера Управления

При помощи WatchGuard Server Center вы можете настроить параметры вашего Сервера Управления. Вы можете обновить лицензию Сервера Управления, настроить уведомления и параметры журнала. На компьютере, на котором установлен Сервер Управления, выполните следующее:

1. Нажмите правой кнопкой мыши на  в панели задач и выберите **Open WatchGuard Server Center**.
   Откроется диалоговое окно Connect to WatchGuard Server Center.

2. В полях **Username** и **Administrator passphrase** введите имя пользователя и пароль администратора соответственно. Нажмите **Login**.
   Откроется диалоговое окно WatchGuard Server Center.

3. В меню **Servers** выбрать **Management Server**.
   Откроется страница Сервера Управления.

4. Для изменения настроек по умолчанию, которые необходимы для вашей сети необходимо выполнить:

   * Для изменения Центра Сертификации, клиента и отмена списка настроек выберите закладку **Certificates**

   * Для добавления или удаления лицензионного ключа или изменения настроек для уведомления установки выберите закладку **Server Settings**

   * Для включения и настройки параметров Активной Директории выберите закладку **Active Directory**

   * Для изменения параметров журнала выберите закладку Logging

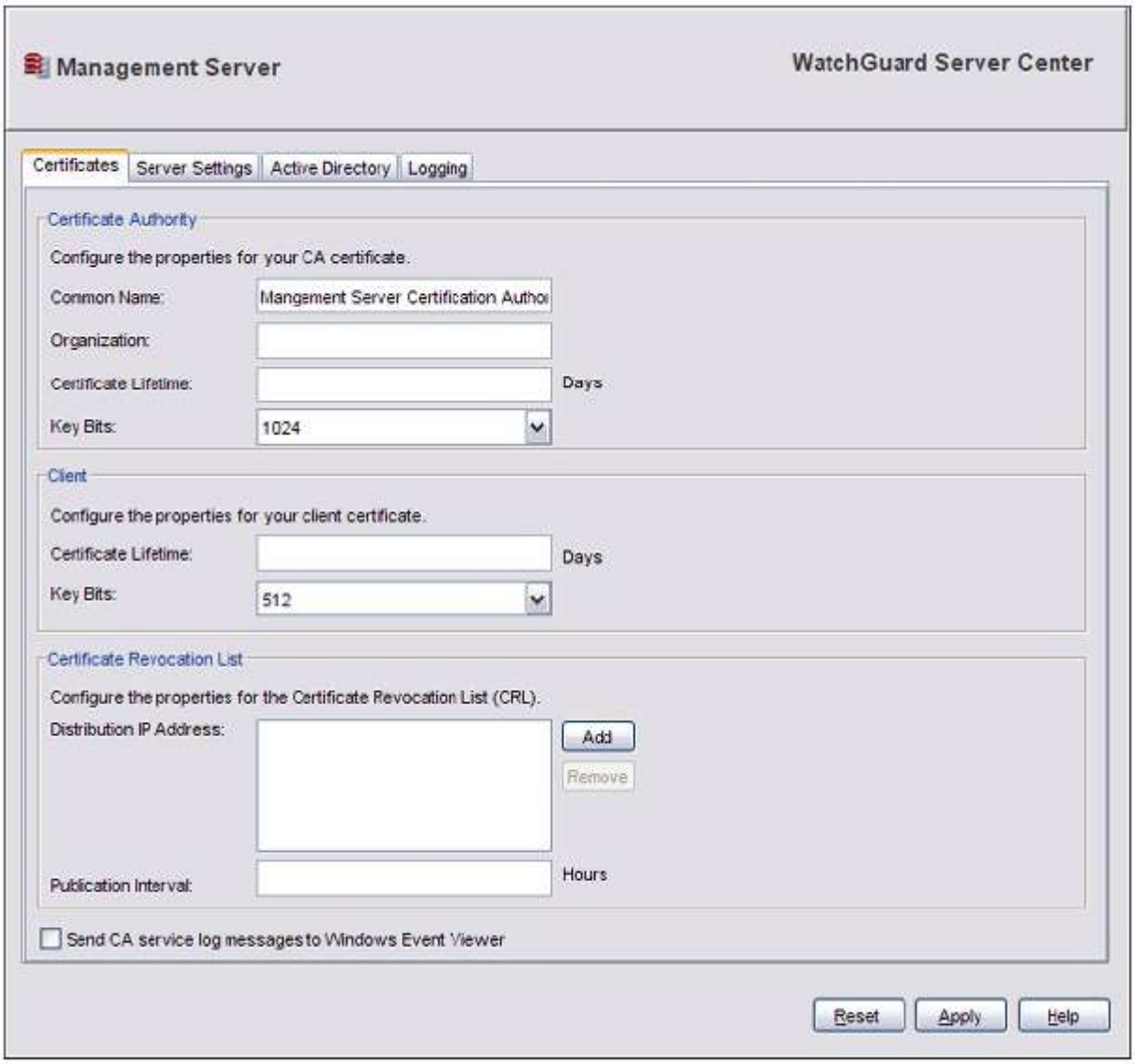
Настройка Центра Сертификации на Сервере Управления

Вы можете настроить Центр Сертификации (далее ЦС) на Сервере Управления. Однако администраторы обычно не меняют параметры сертификатов ЦС

В WatchGuard Server Center выполните следующее:

1. В меню **Servers** выберите **Management Server**.
   Откроется диалогового окна Сервера Управления.

2. Выберите закладку **Certificates**



Установка свойств для Центра Сертификации

В разделе диалогового окна **Certificate Authority** выполните следующие действия:

1. В текстовом поле **Common Name** введите имя, которое будет отображаться в сертификате ЦС

2. В текстовом поле **Organization** введите имя организации для ЦС.

3. В текстовом поле **Certificate Lifetime** введите срок действия сертификата ЦС. Чем длиннее срок действия сертификата ЦС, тем больше времени у хакеров для атаки вашей сети

4. В выпадающем списке **Key Bits** выберите «силу» шифрования для сертификата. Чем выше значение **Key Bits** , тем лучше защита ключа

Настройка параметров для сертификатов клиента

В секции **Client** диалогового окна выполните следующее:

1. В текстовом поле **Certificate Lifetime** введите срок действия сертификата клиента. Чем длиннее срок действия сертификата ЦС, тем больше времени у хакеров для атаки вашей сети

2. В выпадающем списке **Key Bits** выберите «силу» шифрования для сертификата. Чем выше значение **Key Bits** , тем лучше защита ключа

Настройка параметров Списка Отозванных Сертификатов (CRL)

В разделе **Certificate Revocation List** диалогового окна выполните:

1. В окне **Distribution IP Address** выберите IP-адрес из списка или нажмите **Add** для добавления нового адреса. Вы также можете выбрать IP-адрес и удалить его, нажав **Remove**. По умолчанию, используется IP-адреса шлюза Firebox. Это также IP-адрес, по которому клиенты Firebox подключаются к Серверу Управления. Если внешний IP-адрес вашего Firebox изменяется, вам необходимо изменить это значение.

2. Введите значение **Publication Interval** для CRL (в часах). Это период, по истечении которого, CRL автоматически публикуется. По умолчанию это значение равно 0, т.е. CRL публикуется каждые 720 часов (30 дней). CRL также обновляется после того, как сертификат был отозван.

Отправка diagnostic-сообщений журнала для ЦС

Для того чтобы заставить Сервер Управления отправлять diagnostic-сообщения журнала в Windows Event Viewer, выполните следующее:

- Включите опцию **Send CA Service log messages to Windows Event Viewer**.

Для просмотра сообщения журнала откройте Windows Event Viewer:

1. На рабочем столе Windows выберите **Start > Run**.

2. Введите *eventvwr*.

Сообщение журнала появится в разделе **Application** в Event Viewer.

Обновление Сервера Управления с новым адресом шлюза

При использовании мастера установки Серверного Центра на ваш Сервер Управления вы можете выдать IP-адрес шлюзу Firebox, который защищает ваш Сервер Управления от сети Интернет.Этот IP-адрес также используется в качестве IP-адресов **Списка Отозванных Сертификатов (CRL)**. Если вы хотите изменить IP-адрес шлюза Firebox, вы должны прежде всего изменить IP-адрес CRL Distribution вашего Сервера Управления и обновить все управляемые устройства с этой информацией. Если вы не сделаете этого, вы не сможете сохранить подключение к каждому управляемому устройству. Для изменения IP-адреса вашего шлюза Firebox вам следует обновить конфигурацию Сервера Управления, обновить каждый управляемый Firebox и отредактировать NAT-конфигурацию политики WG-Mgmt-Server.

При управлении Branch Office VPN (BOVPN)-туннелей, настроенных на вашем сервере Управления, и шлюза Firebox, который выступает в качестве конечной точки, вам следует удалить эти VPN-туннели до того, как вы начнете эту процедуру. После выполнения этой процедуры вам следует создать VPN-туннель снова.

1. На компьютере с Сервером Управления нажмите правой кнопкой мыши на  и выберите **Open WatchGuard Server Center**.
Откроется диалоговое окно WatchGuard Server Center.

2. В меню **Servers** выберите Management Server.
Откроется страница Сервера Управления.

3. Выберите закладку **Certificate**.

4. В разделе **Certificate Revocation List** добавьте новый IP-адрес для вашего шлюза Firebox и удалите старый. Нажмите **Apply**.

5. На вашей управляющей станции откройте Управление Системой и подключитесь к вашему Серверу Управления.

6. Выберите закладку **Device Management** .

7. Нажмите правой кнопкой на управляющее устройство и выберите **Update Device**.

8. Ниже **Update Client Settings** убедитесь, что выбраны опции **Reset Server Configuration** и **Expire Lease**. Убедитесь, что установлено **Issue/Reissue Firebox's IPSec Certificate and CA's Certificate.**

9. Повторите пункты 3-6 для каждого устройства, управляемого Сервером Управления.

10. Откройте настройку шлюза Firebox в Policy Manager.

11. Выберите **Network > Configuration** и измените IP-адрес external-интерфейса устройства на новый IP-адрес.

12. Дважды нажмите на политику **WG-Mgmt-Server**. При настройке клиента управляемого Firebox вы выдаете IP-адрес управляемого Firebox для шлюза Firebox. Управляемый Firebox использует этот IP-адрес для поиска Сервера Управления. Политика WGMgmt-Server шлюза Firebox настраивает политику NAT для того чтобы любое подключение с управляемого клиента на Сервере Управления направлялось на необходимый External-интерфейс устройства Firebox.

13. Выберите запись NAT в диалоговом окне **To** политики WG-Mgmt-Server и нажмите **Remove**.

14. Ниже диалогового окна **To** нажмите **Add**.
Откроется диалоговое окно Add Address.

15. Нажмите **Add NAT**.
Отроется диалоговое окно Add Static NAT.

16. В выпадающем списке **External IP Address** выберите новый IP-адрес вашего шлюза Firebox.

17. В текстовом окне **Internal IP Address** введите IP-адрес вашего Сервера Управления. Нажмите **OK**.

18. Сохраните конфигурационный файл.

При повторном запуске Firebox соединения между Сервером Управления и клиентами управляемого Firebox будут восстановлены. После этого вы можете заново создать BOVPN-туннели, в которых Firebox используется, как конечная точка

Изменение IP-адреса Сервера Управления

Ваши управляемые устройства Firebox должны всегда иметь возможность подключиться к Серверу Управления. При изменении IP-адреса вашего Сервера Управления или изменении IP-адреса External интерфейса шлюза Firebox клиент управляемого устройства может потерять соединение с Сервером Управления. При изменении IP-адреса вашего Сервера Управления вам следует так же изменять IP-адреса для **Списка Отозванных Сертификатов (CRL)** распределения. и клиентов вашего управляемого Firebox.

IP-адрес распределения списка отозванных сертификатов – IP-адрес, который Сервер Управления выдает для клиентов устройств управляемого Firebox.

Клиенты управляемых устройств затем используют этот IP-адрес для подключения к Серверу Управления. IP-адрес распределения списка отозванных сертификатов должен быть таким же, что и внешний IP-адрес, который клиенты используют для подключения с Серверу Управления. Если Сервер Управления использует внутренние IP-адреса, то IP-адрес распределения списка отозванных сертификатов является IP-адресом External интерфейсом шлюза Firebox. Если Сервер

Управления использует публичный IP-адрес и не располагается за шлюзом Firebox, IP-адрес распределения списка отозванных сертификатов будет публичным, внешним IP-адресом Сервера Управления.

При настройке клиента управляемого Firebox вы выдаете управляемому Firebox IP-адрес для шлюза Firebox. Управляемый Firebox использует данный IP-адрес для поиска Сервера Управления. Политика WG-Mgmt-Server шлюза Firebox устанавливает NAT-политику чтобы убедиться, что любое соединение от клиента управляемого Firebox до Сервера Управления работало через необходимый External-интерфейс устройства Firebox. Для изменения IP-адреса вашего Сервера Управления вам необходимо отредактировать конфигурацию NAT политики WG-Mgmt-Server.

Если Сервер Управления использует внутренний IP адрес

1. В Policy Manager откройте конфигурацию шлюза Firebox, который защищает ваш Сервер Управления от Internet.

2. Дважды нажмите на политику **WG-Mgmt-Server**.
   Откроется диалоговое окно Edit Policy.

3. Выберите запись NAT в диалоговом окне **To** WG-Mgmt-Server политики и нажмите **Remove**.

4. Ниже диалогового окна **To** нажмите **Add**.
   Откроется диалоговое окно Add Address.

5. Нажмите **Add NAT**.
   Откроется диалоговое окно Add Static NAT/Server Load Balancing.

6. В выпадающем списке **External IP Address** убедитесь, что выбран IP-адрес для шлюза Firebox.

7. В текстовом поле **Internal IP Address** введите новый IP-адрес вашего Сервера Управления.

8. Нажмите **OK** для закрытия диалогового окна **Add Static NAT/Sever Load Balancing**.

9. Нажмите **OK** для закрытия диалогового окна **Add Address**.

10. Нажмите **OK** для закрытия диалогового окна **Edit Policy Properties**.

11. Сохраните конфигурационный файл.

Если Сервер Управления использует публичный IP-адрес

1. В Policy Manager откройте конфигурацию шлюза Firebox, который защищает ваш Сервер Управления от сети Интернет

2. Дважды нажмите на политику **WG-Mgmt-Server**.
   Откроется диалоговое окно Edit Policy.

3. Выберите запись NAT в диалоговом окне **To** WG-Mgmt-Server политики и нажмите **Remove**.

4. Ниже диалогового окна **To** нажмите **Add**.
   Откроется диалоговое окно Add Address.

5. Нажмите **Add Other**.
   Откроется диалоговое окно Add Member.

6. В выпадающем списке **Choose Type** выберите **Host IP**.

7. Введите новый публичный IP-адрес Сервера Управления.

8. Нажмите **OK** для закрытия диалогового окна **Add Member**.

9. Нажмите **OK** для закрытия диалогового окна **Add Address**.

10. Нажмите **OK** для закрытия диалогового окна **Edit Policy Properties**.

11. Сохраните конфигурационный файл.

Обновление IP-адреса распределения CRL

Используйте эту процедуру, только если ваш Сервер Управления использует публичным IP-адрес.

1. На компьютере с Сервером Управления правой кнопкой мыши нажмите на  и выберите **Open WatchGuard Server Center**.
   Откроется диалоговое окно Connect to WatchGuard Server Center.

2. Введите пароль администратора и нажмите **Login**.
   Откроется диалоговое окно WatchGuard Server Center.

3. В списке **Servers** выберите **Management Server**.

4. Нажмите на закладку **Certificates**.

5. Если в ней окажется IP-адрес, в разделе **Certificate Revocation List** выберите адрес из списка **Distribution IP Address** и нажмите **Remove**.

6. Нажмите **Add** для добавления нового адреса.
   Откроется диалоговое окно CRL IP Address.

7. Введите новый **IP Address**. нажмите **OK**.
   IP-адрес появится в списке Distribution IP Address.

8. Нажмите **Apply**.
   Откроется диалоговое окно с подтверждением намерения обновить Сервер Управления с вашими изменениями.

9. Нажмите **OK**.
   Откроется диалоговое окно Comments.

10. (Дополнительно) Добавьте комментарий для журналов аудита

11. Нажмите **OK**.
    Сделанные изменения вступят в силу

Обновление управляемых клиентов

Для того чтобы завершить процедуру смены IP адреса вам необходимо обновить все управляемые устройства. Для этого выполните следующее:

1. В WatchGuard System Manager вашей управляющей станции подключитесь в вашему Серверу Управления.

2. Выберите закладку **Device Management** .

3. Правой кнопкой нажмите на управляемый Firebox и выберите **Update Device**.

4. Ниже **Update Client Settings** убедитесь, что выбраны опции **Reset Server Configuration** и **Expire Lease**.

5. Повторите пункты 1-3 для каждого устройства, подключенного к Серверу Управления.

Изменение пароля администратора

Пароль администратора – это главный пароль для всех серверов WatchGuard. В предыдущей версии WatchGuard System Manager в качестве пароля администратора использовались два пароля: главный пароль (Master) и пароль Сервера Управления. В новом релизе эти пароли заменены одним паролем администратора. Пароль администратора – это пароль пользователя *admin.* Этот пользователь автоматически создается мастером установки WatchGuard Server Center. После установки Центра Сервера WatchGuard вы можете изменить пароль администратора в любое время.

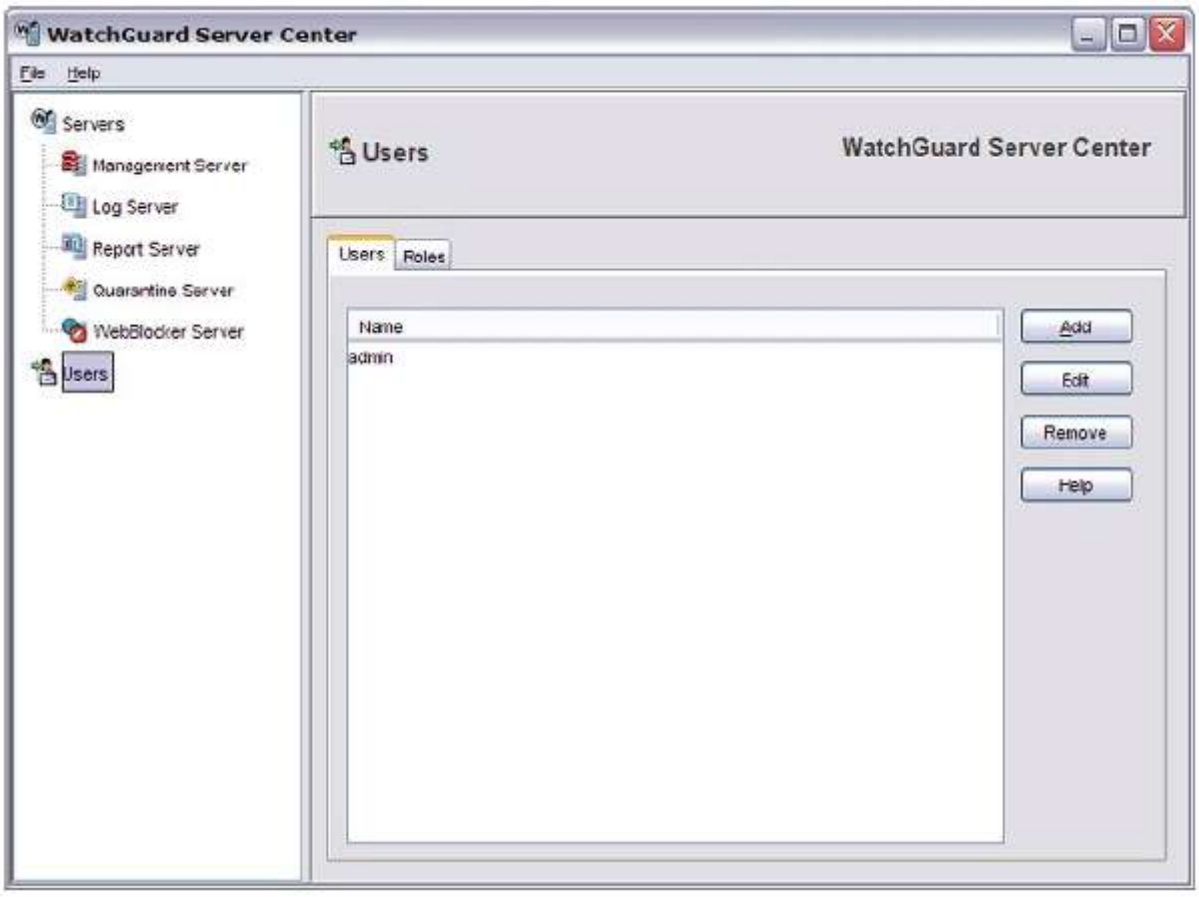
Для более подробной информации о мастере установки WatchGuard Server Center см. в “Установка серверов WatchGuard System Manager”. Более подробную информацию о редактировании пользователей см.в “Создание и удаление пользователей или групп”

Мы рекомендуем вам сделать резервную копию конфигурации Сервера Управления сразу после изменения пароля администратора. При создании резервной копии конфигурационного файла текущий пароль администратора будет храниться в файле. Вы можете использовать этот пароль при восстановлении конфигурационного файла. Если вы изменяете пароль администратора и затем восстанавливаете резервную копию конфигурационного файла со старым паролем администратора, то старый пароль восстановится с конфигурацией сервера.

Перед изменением пароля администратора убедитесь, что пользователь **admin** зарегистрировался на Сервере Управления. Вы не можете изменять имя пользователя **admin.** Вы можете только изменить его пароль.

В WatchGuard Server Center необходимо выполнить:

1. В левой навигационной панели выберите **Users**.
   Откроется страница Users



2. В закладке **Users** в списке **Name** выберите **admin**.

3. Нажмите **Edit**.
   Откроется диалоговое окно User and Group Properties

4. Выберите опцию **Change passphrase**.

5. Введите и подтвердите пароль.

6. Нажмите **OK**.

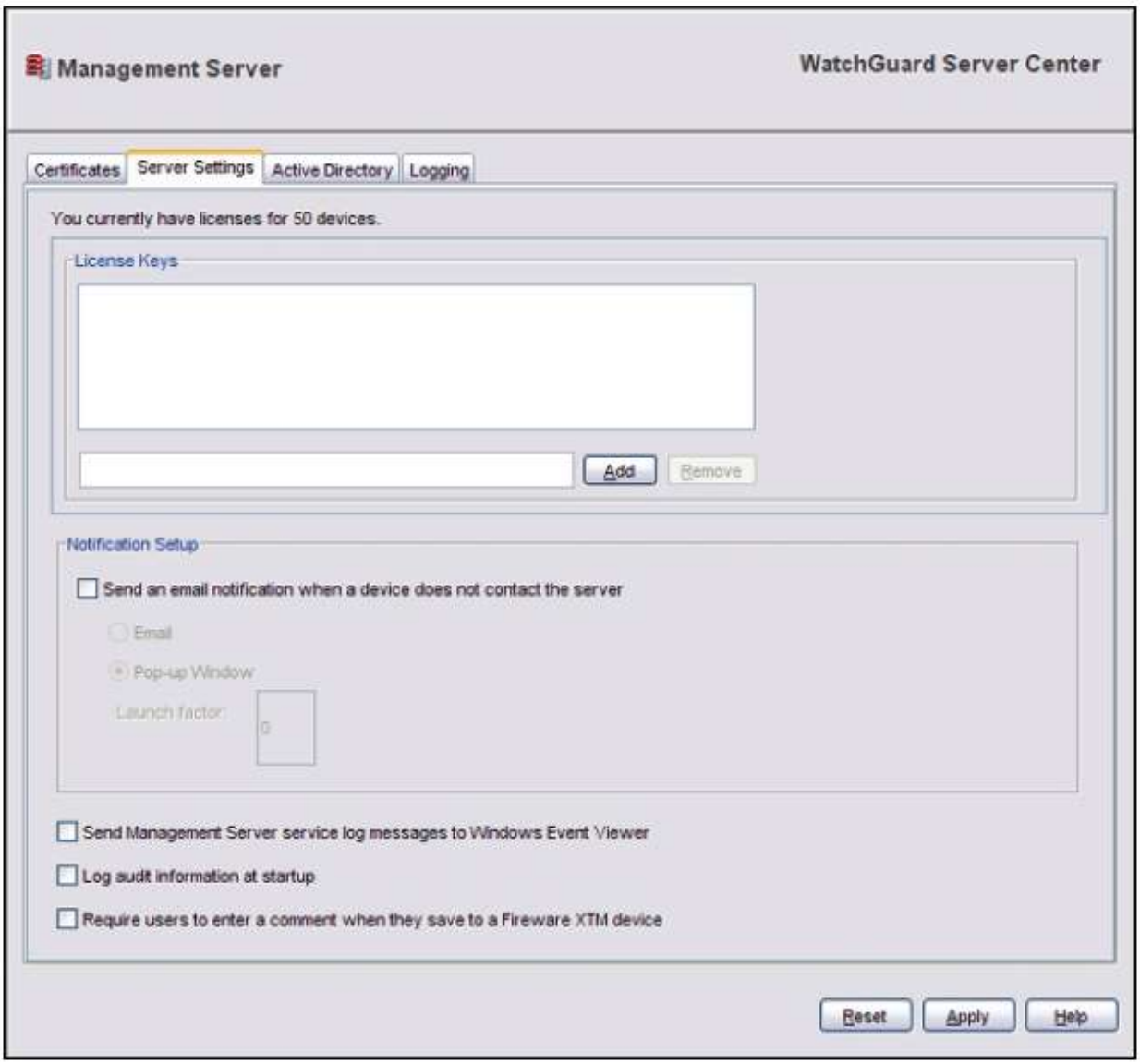
Настройка лицензионного ключа, Уведомлений и параметров конфигурации

Вы можете добавлять или удалять лицензионные ключи, настраивать параметры журнала и уведомлений вашего Сервера Управления

На Сервере Управления выполните:

1. В меню **Servers** выберите **Management Server**.

2. Нажмите на закладку **Server Settings**.
   Откроется страница Server Settings



3. Используйте следующий раздел для настройки параметров вашего Сервера Управления.

4. После завершения нажмите **Apply** для сохранения изменений.

Добавление или удаление лицензии Сервера Управления

Для того чтобы добавить лицензию Сервера Управления выполните следующее:

1. В текстовом окне, ниже окна **License Keys,** введите или вставьте лицензионный ключ Сервера Управления.

2. Нажмите **Add**.
Лицензионный ключ появится в окне License Key.

Для того чтобы удалить лицензию Сервера Управления выполните следующее:

1. В текстовом поле, ниже окна **License Keys** выбрать лицензию для удаления.

2. Нажмите **Remove**.

Настройка уведомления

Выберите опцию **Send notification when the device does not contact the server** и настройте параметры для сообщения уведомления.

- **Email** — при наступлении какого-либо события Сервер Журнала отправляет электронное письмо указанному получателю

- **Pop-up Window** — При наступлении какого-либо события Firebox на станции управления открывает диалоговое окно. Если вы выберете эту опцию, то вам необходимо будет настроить **Launch Factor**.

- **Launch factor** — минимальное время (в минутах) между различными уведомлениями. Этот параметр используется для того, чтобы за короткий промежуток времени для одного и того события не генерировались уведомления

Управление настройками изменения конфигурации

Вы можете настроить несколько глобальных параметров для управления сообщениями журнала, которые отправляются с Сервера Управления на Сервер Журналов.

Send Management Server service log messages to Windows Event Viewer

Включите эту опцию, если вы хотите, чтобы Сервер Управления отправлял diagnostic-сообщения утилите Windows Event Viewer. Вы также можете управлять журналами Сервера Управления в закладке **Logging**

Log audit information at startup

Включите эту опцию, если хотите, чтобы Сервер Управления создавал журналы для управляемых устройств, VPN ресурсов, политик VPN брандмауэра, шаблонов безопасности или шаблонов управления Edge и управляемых туннелей. Для того чтобы получать точную информацию в ваших отчетах вам необходимо включить эту опцию

Require users to enter a comment when they save to a Fireware XTM device

Включите эту опцию, чтобы пользователи вводили комментарии перед тем, как сохранить изменения на Firebox из Policy Manager

Включение и настройка аутентификации Active Directory

Если вы хотите использовать сервер Active Directory для аутентификации пользователей, вам следует использовать закладку **Active Directory** на странице **Management Server** для настройки параметров соединения с сервером Active Directory.

Для использования аутентификации Active Directory в вашем Сервером Управления следует включить LDAPS (LDAP over SSL) в домене Active Directory. Более подробную информацию см. на сайте Microsoft или просмотрите документацию для вашего сервера Active Directory.

Несмотря на то, что основная учетная запись администратора всегда управляется Сервером Управления, вы можете использовать сервер Active Directory для управления другими учетными записями пользователей. Когда пользователь, созданный на сервере аутентификации пытается подключиться к Серверу Управления, Сервер шлет информацию о пользователе на внешний сервер аутентификации

Сервер Active Directory сообщает Серверу Управления о достоверности пользователя и его принадлежности к какой-либо группе. Сервер Управления затем сравнивает пользователя и группу со своим списком пользователей и групп, а так же о роли политики, с которой они связаны.

Для включения и настройки аутентификации Active Directory в WatchGuard Server Center выполните следующее:

1. В меню **Servers** выберите **Management Server**.

2. Нажмите на закладку **Active Directory**.
   Откроется страница Active Directory.

3. Включите опцию **Enable Active Directory authentication**.

4. Для добавления, редактирования или удаления домена в списке **Domain Name** нажмите **Add / Remove.** Вы можете устанавливать несколько доменных имен в этом списке.
   Откроется диалоговое окно Add Domains

5. Для добавления доменного имени в список в текстовом поле **Specify domain name** введите домен Active Directory.
   Контроллер домена Active Directory использует SSL для подключения к серверу Active Directory.

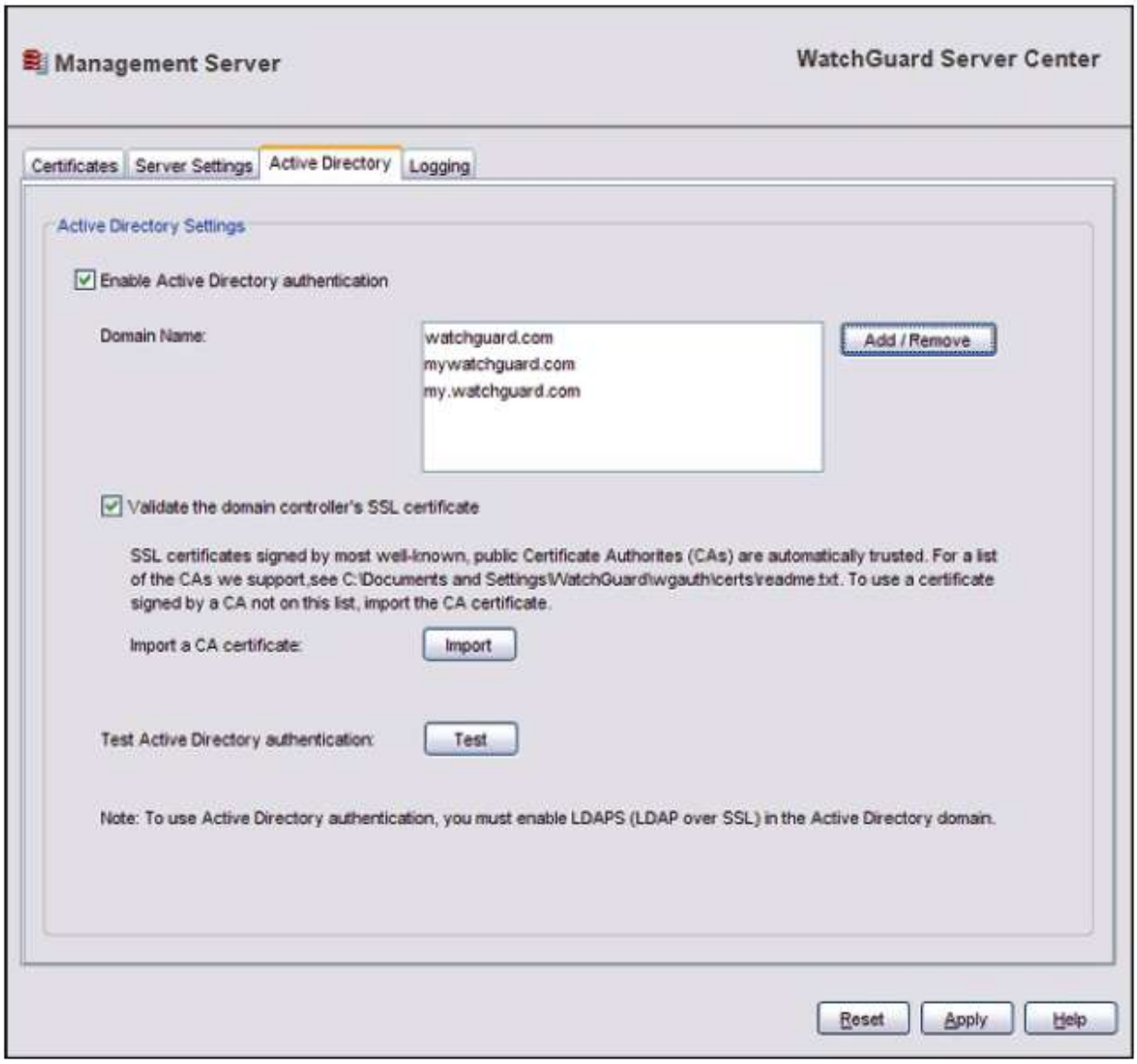
6. Нажмите **Add**.

7. Для добавления имен в список повторите п. 4–6.

8. Для удаления доменного имени из списка выберите его и нажмите **Remove**.

9. После завершения нажмите **OK** для закрытия диалогового окна **Add Domains**.
   Доменные имена появятся в списке Domain Name.

10. Для проверки SSL-сертификата выберите опцию **Validate the domain controller's SSL certificate**



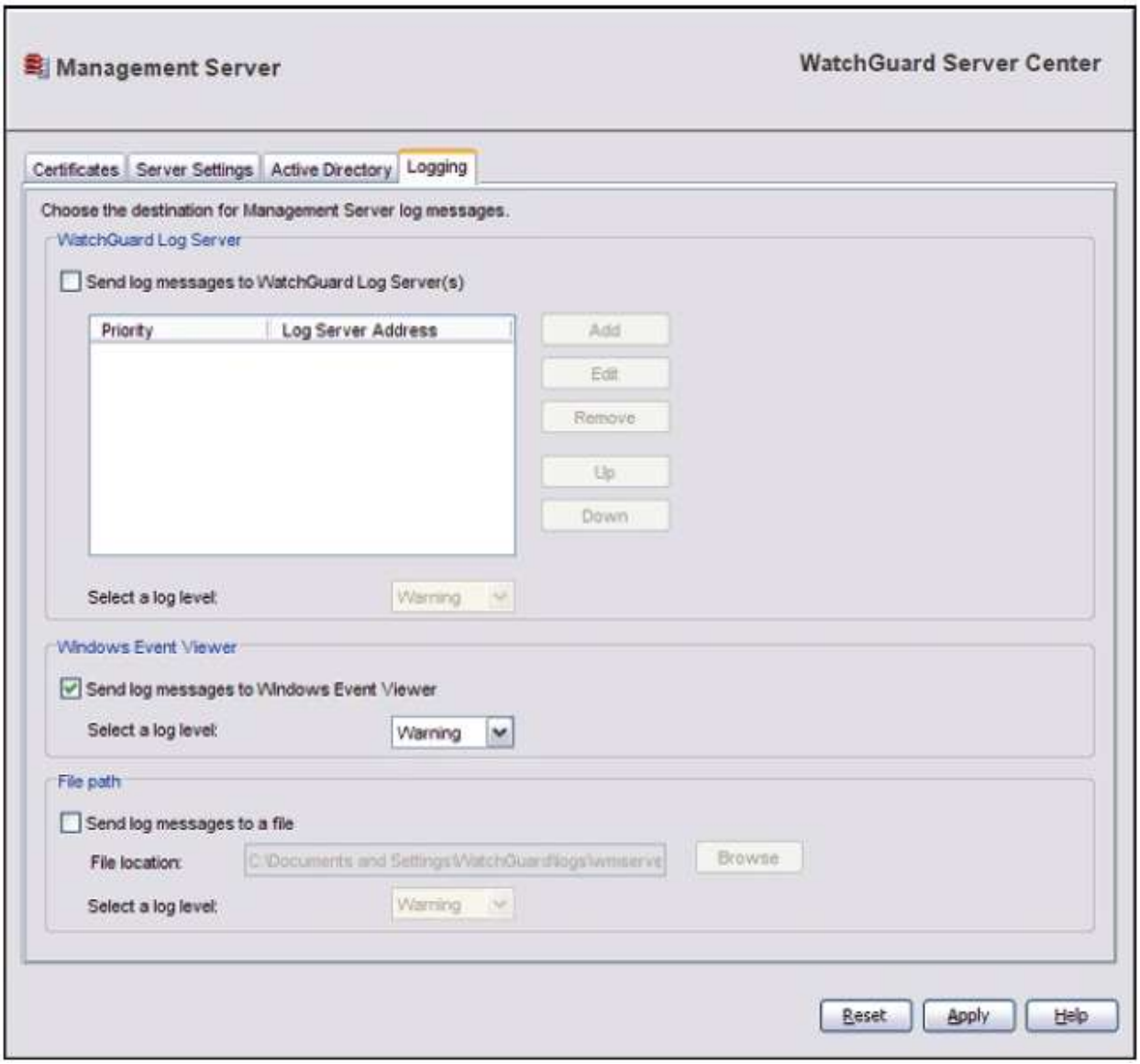
11. Для импорта CA-сертификата нажмите **Import**.
12. Для тестирования вашего соединения с аутентификацией Active Directory нажмите **Test**.
13. Нажмите **Apply** для сохранения изменений.

Настройка параметров Журнала для Сервера Управления

На странице **Logging** Сервера Управления вы можете настроить, куда Сервер Управления будет оправлять сообщения журнала. Вы можете отправлять сообщения на Сервер Журналов, Windows Event Viewer и/или записывать их в файл журнала

В WatchGuard Server Center выполните следующее:

1. В меню **Servers** выберите **Management Server**.
2. Нажать на закладку **Logging**.
   Откроется страница Logging



3. Настройте параметры вашего Сервера Управления

4. После завершения процедуры нажмите **Apply** для сохранения изменений.

Создание резервной копии или восстановление конфигурации Сервера Управления

Сервер Управления содержит конфигурационную информацию для всех управляемых устройств Firebox и VPN-туннелей. Мы рекомендуем периодически создавать копии конфигурации Сервера Управления и копировать их в безопасное место. Затем вы можете использовать эти резервные файлы для восстановления конфигурации Сервера Управления в случае аппаратных проблем. Вы так же можете их использовать при перемещении Сервера Управления на новый компьютер.

При создании резервного конфигурационного файла пароль администратора восстанавливается в файл. Вам следует использовать этот пароль для восстановления конфигурационного файла. Если вы изменили пароль администратора, убедитесь, что вы сохранили пароль на вашем резервном файле. При восстановлении резервного конфигурационного файла со старым паролем администратора пароль будет восстанавливаться с конфигурацией сервера.

Создание резервной копии вашей конфигурации

На компьютере с установленным Сервером Управления выполните следующее:

1. Нажмите правой кнопкой мыши на  и выберите **Backup/Restore**.Или на Сервере Управления WatchGuard выберите **File > Backup/Restore**.
   Запустится мастер настройки WatchGuard Server Center Backup/Restore.

2. Нажмите **Next**.
   Откроется экран Select.

3. Выберите Back up settings.

4. Нажмите **Next**.
   Откроется экран резервного файла Specify.

5. Нажмите **Browse** для выбора каталога, куда будет сохранен конфигурационный файл. Убедитесь, что вы сохранили конфигурационный файл в каталоге, который затем вы сможете в случае необходимости восстановления конфигурации

6. Нажмите **Next**.
   Откроется экран о завершении работы мастера настроек WatchGuard Server Center Backup/Restore.

7. Нажмите **Finish** для выхода из мастера настроек.

Восстановление вашей конфигурации

Перед началом убедитесь, что у текущий пароль администратора хранится в файле.

На компьютере с установленным Сервером Управления выполните следующее:

1. Нажмите правой кнопкой мыши на  и выберите **Backup/Restore**.
   Запустится мастер настроек WatchGuard Server Center Backup/Restore.

2. Нажмите **Next**.
   Откроется экран Select.

3. Выберите **Restore Settings**.

4. Нажмите **Next**.
   Откроется экран резервного файла Specify.

5. Нажмите **Browse** для выбора резервного файла.

6. Введите пароль администратора **Administrator passphrase** для резервного файла.

7. Нажмите **Next**.
   Откроется экран с завершением работы мастера установок WatchGuard Server Center Backup/Restore.

8. Нажмите **Finish** для выхода из мастера установок.

Перенос Сервера Управления на Новый Компьютер

Для перемещения программного обеспечения Сервера Управления на новый компьютер необходимо прежде всего создать резервную копию конфигурации Сервера Управления на текущем компьютере и затем восстановить конфигурацию на новом компьютере.

Убедитесь, что у вас есть пароль администратора из резервной конфигурации. Вам следует так же убедиться, что новый Сервер Управления имеет тот же IP-адрес, что и предыдущий Сервер Управления.

Резервирование, перемещение и восстановление вашего Сервера Управления

На компьютере с установленным Сервером Управления необходимо выполнить:

1. Нажмите правой кнопкой мыши на  и выберите **Backup/Restore**.
   Запустится мастер установки WatchGuard Server Center Backup/Restore.

2. Используйте мастер для резервирования конфигурации вашего Сервера Управления. Убедитесь, что вы сохранили конфигурационный файл в месте, куда позже сможете обратиться из нового компьютера.

3. На новом компьютере запустите программу установки WatchGuard System Manager.

4. Ниже раздела **Server Components** проверьте, что выбран **Management Server**.

5. Правой кнопкой мыши нажмите на новый компьютер и выберите **Backup/Restore**.
   Запустится мастер установок WatchGuard Server Center Backup/Restore.

6. Используйте мастера для восстановления конфигурации вашего Сервера Управления.

Настройка других установленных серверов WatchGuard

При восстановлении конфигурации на вашем новом Сервере Управления для того чтобы открыть WatchGuard Server Center и получить доступ к вашему Серверу Управления вам не надо выполнять все инструкции мастера до конца

Однако, если вы на вашу станцию управления установили другие серверы WatchGuard, то их настройки восстановлены не будут. Для настройки других серверов вам необходимо запустить мастер WatchGuard Server Center Setup.

1. В меню **Servers** выберите любой сервер со статусом **Server not configured**.

2. Нажмите на ссылку **Click here to launch setup wizard for [WatchGuard] Server**. Текст ссылки указывает имя выбранного сервера, но мастер настраивает все установленные сервера WatchGuard.
   Откроется диалоговое окно, в котором сообщается о выполнении мастера установок.

3. Нажмите **OK**.
   Откроется диалоговое окно WatchGuard Server Center Setup Wizard.

4. Нажмите **Next**.

5. Проверьте, что вся необходимая информация настроена на установленных серверах WatchGuard.

6. Для более подробной информации, о том что необходимо для завершения мастера установки Server Center Setup Wizard см. в ”Установка серверов WatchGuard System Manager”.

7. Завершите работу мастер Server Center Setup Wizard.

8. Нажмите **Refresh** на странице выбранного сервера. Появится информация о сервере и запуске его работы.

9. В списке **Servers** выберите другой установленный сервер.

10. Откроется ссылка **Click here to launch setup wizard for [WatchGuard] Server** на странице сервера. НЕ нажимайте на ссылку. Сервер уже установлен.

11. Нажмите **Refresh**.
    Откроется информация о сервере и о начале его работы.

12. Повторите пункты 7-8 для каждого сервера WatchGuard, который вы устанавливали.

Использование WSM для подключения к Серверу Управления

Для подключения к Серверу Управления из WatchGuard System Manager выполните следующее:

1. Нажмите  . Или выберите **File** > **Connect to Server**. Или нажмите правой кнопкой мыши где-либо в окне WatchGuard System Manager и выберите **Connect to > Server**.
   Откроется диалоговое окно Connect to Management Server

2. В выпадающем списке **Management Server** выберите сервер по имени хоста или IP-адресу. Или введите IP-адрес или имя хоста. При этом вводите все точки и цифры. Не используйте клавишу Tab или клавиши со стрелками.

3. Введите ваше имя пользователя для вашей учетной записи на Сервере Управления.

4. Введите пароль для вашей учетной записи пользователя. Если вы используете учетной запись администратора по умолчанию, используйте пароль администратора.

5. При необходимости измените величину **Timeout**. Эта величина устанавливает время (в секундах), в течение которого WatchGuard System Manager ждет данные от Сервера Управления, после чего отправляет сообщение о том, что подключиться не может. Если скорость работы вашей сети невысока, то вам необходимо увеличить это значение

6. Нажмите **Login**.
   Появится сервер в окне WatchGuard System Manager.

В некоторых предыдущих версиях продуктов безопасности WatchGuard Сервер Управления назывался DVCP-сервер.

Отключение от Сервера Управления

1. Выберите Сервер Управления

2. Нажмите  . Или выберите **File** > **Disconnect**. Или выберите правой кнопкой мыши t **Disconnect**.

Импорт и экспорт конфигурации сервера Управления

Вы можете использовать WatchGuard System Manager (WSM) для экспорта файла вашей конфигурации Сервера Управления в DVCP-файл. Вы можете затем использовать текстовый редактор для открытия файла и его просмотра. Вы можете так же импортировать сохраненный конфигурационный DVCP-файл для вашего Сервера Управления. Сохраненный конфигурационный файл не замещается на резервную копию вашего Сервера Управления. Более подробную информацию о резервировании конфигурации вашего Сервера Управления см. в “резервирование или восстановление конфигурации Сервера Управления” на с. 473.

Экспорт конфигурации

1. Откройте WSM и подключитесь к Серверу Управления.

2. Выберите **File** > **Export to File**.
   Откроется диалоговое окно Save As. Имя по умолчанию - [IP-адрес Сервера Управления].dvcp.

3. Для выбора различного имени для файла введите имя в текстовом поле **File name**.

4. Выберите директорию для сохранения файла.

5. Нажмите **Save**.

Импорт конфигурации

1. Откройте WSM и подключитесь к Серверу Управления

2. Выберите **File** > **Import from File**.
   Откроется диалоговое окно Open.

3. Обзор для выбора файла конфигурации.

Нажмите **Open**.

Глава 19 - Управление устройствами и VPN

WatchGuard System Manager

Окно WatchGuard System Manager содержит меню и иконки, которые вы можете использовать для запуска других программ.

Окно WatchGuard® System Manager содержит две закладки, которые вы можете использовать для управления и мониторинга вашей сети: **Device Status** и **Device Management**.

Закладка Device status

В этой закладке отображается состояние всех устройств, подключенных к системе WatchGuard System Manager. Здесь отображается статус, IP- и MAC-адрес каждого интерфейса Ethernet и все установленные сертификаты, а также статус всех VPN-туннелей, настроенных с помощью утилиты System Manager. Более подробная информация для каждого Firebox включает IP-адрес и маску подсети каждого интерфейса Firebox. Она также включает:

- IP-адрес и маску сети шлюза по умолчанию (только для интерфейсов External).
- MAC-адрес интерфейса.
- Количество отправленных и принятых пакетов с момента последней перезагрузки.

Каждое устройство может находиться в 4 различных состояниях:

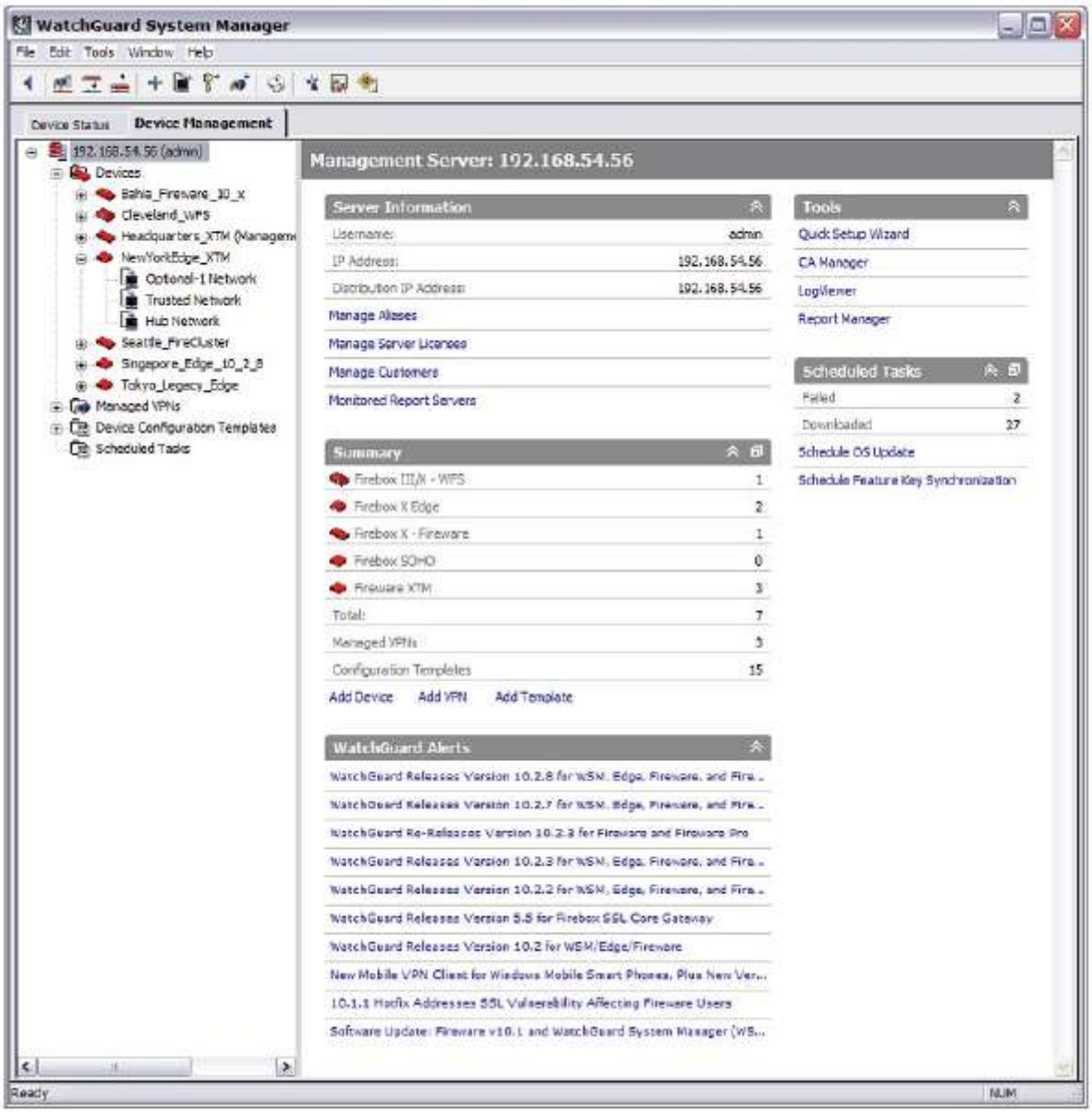
-  - Обычный режим работы. Устройство обменивается данными с WatchGuard System Manager.
-  - Устройство обладает динамическим IP-адресом и еще не подключилось к Серверу Управления.
-  - WatchGuard System Manager в данный момент не может подключиться к устройству Firebox.
-  - Первое подключение к устройству или соединение с устройством еще не установлено.

Закладка **Device Status** также содержит информацию о BOVPN и MUVPN туннелях

Закладка Device management

*Закладка **Device Management** появится только после успешного подключения к Серверу Управления*

В левой части закладки **Device Management** находится панель навигации, в правой – информационная панель. В навигационной панели отображаются подключенные Серверы Управления и их управляемые устройства, управляемые VPN, шаблоны политик VPN Firewall, шаблоны безопасности, шаблоны конфигурации устройств и Запланированные задания. Если вы откроете список устройств, то вы увидите список VPN сетей, подключенных к нему.



В информационной панели отображается информация по каждому элементу, выбранному в панели навигации.

Management Server

Для того чтобы посмотреть или изменить информацию о Сервере Управления, в панели навигации нажмите на **Management Server**. Информация о выбранном Сервере Управления появится в информационной панели справа:

- Имя пользователя и IP-адрес
  Это имя пользователя отображается в панели навигации после IP адреса Сервера Управления (в скобках).

- Псевдонимы для устройств Firebox

- Лицензии сервера

- Customers — Клиенты. Вы можете изменить список контактов как описано в “Настройка параметров управления устройством”

- Серверы Отчетов

- Список управляемых устройств, VPN туннели и Шаблоны Конфигурации

- Тревоги: Последние трансляции LiveSecurity, которые являются информационными тревогами. Если вы нажмете на тревогу, то для того чтобы посмотреть ее полный текст вам необходимо подключиться к LiveSecurity Service.

- Запуск утилит WatchGuard System Manager

- Посмотреть, отменить или удалить Запланированных задач

Devices

Для того чтобы посмотреть список управляемых устройств для Сервера Управления, в панели навигации нажмите **Devices**. Откроется страница **Devices,** на которой вы можете посмотреть список устройств, управляемых этим Сервером Управления. Для того чтобы посмотреть информацию по отдельному управляемому устройству нажмите на необходимое устройство в списке **Devices**, или два раза нажмите на устройство на странице **Devices**. Для выбранного устройства откроется страница **Device Page**.

Managed VPNs

Для того чтобы посмотреть список существующих VPN туннелей и создать новые VPN туннели в панели навигации нажмите **Managed VPNs**. На странице **Managed VPNs** вы можете посмотреть обшую информацию о ваших управляемых VPN туннелях.

Два раза нажмите на управляемый туннель из списка для того чтобы открыть страницу **Managed VPN** для этого туннеля. Для того чтобы создать новый туннель нажмите **Add**.

Для того чтобы посмотреть информацию о существующем управляемом VPN туннеле нажмите на него в меню **Managed VPNs**. На странице **Managed VPN** вы можете посмотреть его параметры. Для того чтобы внести какие-либо изменения нажмите **Configure**

Страница Device Management

На этой странице вы можете настроить параметров управления устройств.

1. Запустите WatchGuard System Manager и подключитесь к Серверу Управления.

2. В закладке **Device Management** выберите **Devices**.
   Откроется страница Devices.

3. Два раза нажмите на устройство в списке. Или откройте список **Devices**, и нажмите на устройство в списке.
   Откроется страница управления для выбранного устройства.

На этой странице **Device Management** вы можете следующее:

- Посмотреть, не заблокирован ли конфигурационный файл устройства. Если конфигурационный файл был открыт с другого Сервера Управления, то конфигурационный файл блокируется для доступа. В верхней части страницы появляется тревога, которая сообщает о том, чтобы конфигурационный файл заблокирован. Вы не можете вносить какие-либо изменения, пока конфигурационный файл устройства не будет разблокирован (будет закрыта утилита Policy Manager для этого устройства).

- Посмотреть общую информацию об устройстве

- Посмотреть, создать, редактировать или удалить VPN туннели для этого устройства

- Смотреть, создавать, редактировать и удалять VPN ресурсы для данного устройства

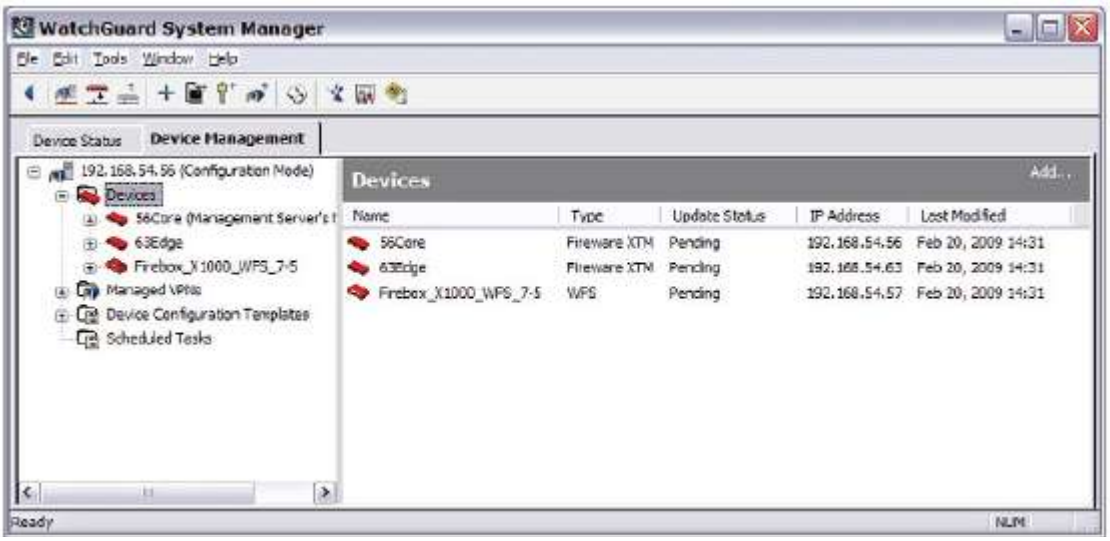
- Запускать утилиты мониторинга, настройки или управления этим устройством

Общая информация об управляемых устройствах

В WatchGuard System Manager вы можете список управляемых устройств, а также при необходимости более подробную информацию о каждом из них. Для этого выполните следующее.

1. Откройте WSM и подключитесь к Серверу Управления.

2. Выберите устройство или каталог в списке **Devices**.
   Информация для выбранного устройства появится на странице Devices.



Name

Имя управляемого устройства.

Type

Тип устройства или ПО, установленное на него.

Update Status

Плановые обновления устройства и текущий статус.

* **Never** — Устройства никогда не обновлялось.

* **Pending** — Было внесено изменение, которое еще не синхронизировано с устройством, или на данный момент идет процедура обновления.

* **Scheduled** — Обновления было запланировано, но еще не началось.

* **Complete** — Устройство было успешно обновления. В скобках указаны дата и время последнего обновления.

IP Address

IP адрес, который используется для идентификации устройства Firebox. Если устройство Firebox не подключилось к Серверу Управления, то в этом поле будет **n/a**

Last Modified

Время и дата последнего изменения конфигурационного файла на сервере.

Режимы Централизованного Управления

Централизованное управление позволяет вам управлять конфигурацией и параметрами ваших устройств Firebox с вашего Сервера Управления. Централизованное управление включает два режима: *Basic Managed Mode u Fully Managed Mode*. Режим Basic Managed доступен для всех моделей Firebox, которыми вы можете управлять при помощи вашего Сервера Управления. Режим Fully Managed доступен только для Firebox X Edge и Fireware XTM.

Для более подробной информации о том, какие режимы доступны для каких устройств см. "Добавление управляемых устройств на Сервер Управления"

В режиме Basic Managed вы можете использовать Сервер Управления для:

- Мониторинга вашего Firebox
- Управления и мониторинга VPN туннелей
- Синхронизации вашего ключа функций
- Обновление ОС вашего Firebox

В режим Fully Managed вы можете использовать Сервер Управления для:

- Мониторинга вашего Firebox
- Управления и мониторинга VPN туннелей
- Синхронизации вашего ключа функций
- Обновление ОС вашего Firebox
- Управления конфигурацией вашего Firebox
- Создавать расписания обновлений конфигураций управляемых
- Управления шаблонами устройств
- Создавать расписания обновлений ваших шаблонов конфигурации устройств (Device Configuration Templates)

Когда вы при помощи WatchGuard System Manager (WSM) добавляете управляемое устройство на Сервер Управления, то оно автоматически будет управляться в режиме Basic Managed. Для того чтобы изменить режим на Fully Managed, вы можете подключить устройство к Шаблону КОнфигурации, или использовать секцию **Device Mode** на странице **Device** вашего Firebox.

Если Firebox находится в режиме Basic Managed, вы можете подключиться к нему напрямую и локально внести необходимые изменения в конфигурационный файл при помощи Policy Manager. When a Firebox is in Fully Managed Mode, you can only make changes to the configuration from the Management Server. If you connect directly to the Firebox, the connection and configuration are set to read-only, and you cannot make changes to the configuration locally.

Для более подробной информации о том, как подключить устройство к шаблону конфигурации, см. "Подключение устройств к Шаблону Конфигурации Устройств"

Для более подробной информации об изменении режима управления см. "Изменение режима Централизованного управления для вашего Firebox"

Для более подробной информации об использовании WSM для управления вашими устройствами см. "Глава 19 - Управление устройствами и VPN"

Изменение режима Централизованного управления для вашего Firebox

Когда вы добавляете устройство на Сервер Управления, оно автоматически добавляется в режиме *Basic Managed*. Вы можете при помощи WatchGuard System Manager (WSM) изменить режим управления на *Fully Managed* и подключить его к Шаблону Конфигурации.

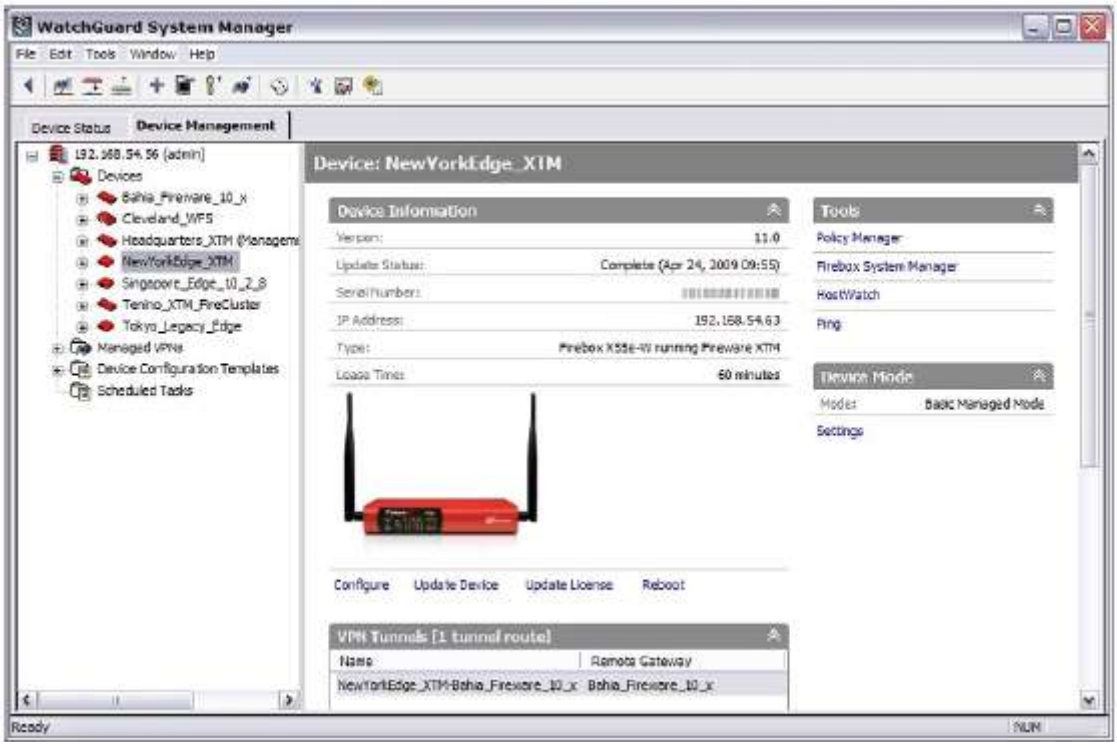
Для более подробной информации о режимах управления см. “Режимы Централизованного Управления”

Для более подробной информации о Шаблонах Конфигурации Устройств см. “Создание шаблонов конфигурации и подключение к Шаблонам Конфигурации Устройства (Device Configuration Templates)”

Для того чтобы изменить режим управления выполните следующее:

1. Откройте WSM и подключитесь к Серверу Управления.

2. Откройте список **Devices** и выберите Firebox X Edge или Fireware XTM.
   Для выбранного устройства откроется страница Device. Текущий режим устройства появится в секции Device Mode.



3. В секции **Device Mode** нажмите **Settings**.
   Откроется диалоговое окно Device Mode.

4. Выполните инструкции, описание которых приведены далее.

Изменение режима управления на Basic Managed

При изменении режима управления устройством с Fully Managed Mode на Basic Managed Mode, если ваше устройство Firebox подключено к Шаблону Конфигурации, то все политики и настройки, входящие в этот шаблон будут удалены из конфигурации устройтсва.

В диалоговом окне Device Mode выполните следующее:

1. Выберите **Basic Managed Mode**.

2. Нажмите **OK**.
   Basic Managed Mode появится в секции Device Mode.

Изменение режима управления на Fully Managed

При смене режима управления устройством с Basic Managed Mode на Fully Managed Mode, вы можете подключить устройство к определенному шаблону конфигурации

В диалоговом окне Device Mode:

1. Выберите Fully Managed Mode.

2. To subscribe to a configuration template, select the **Use Configuration Template** check box and select a template in the drop-down list.

3. Нажмите **OK**.
   Появится сообщения подтверждения.

4. Нажмите **Yes**.
   Сервер Управления загрузит конфигурационный файл. Если вы выбрали шаблон конфигурации, то устройство будет к нему подключено

Использование параметров Device Mode для подключения устройства к шаблону конфигурации

Если вы включили для вашего Firebox режим управления Fully Managed , но не подключили его к определенному шаблону конфигурации, вы можете при помощи диалогового окна Device Mode выбрать необходимый шаблон

1. В секции **Device Mode** нажмите **Settings**.
   Откроется диалоговое окно Device Mode

2. Включите опцию Use **Configuration Template**.

3. Выберите шаблон из выпадающего списка.

4. Нажмите **OK**.
   Появится confirmation message appears.

5. Если вы не хотите перезагружать устройство Firebox отключите опцию **Restart device now to expire lease and download new configuration**.

6. Нажмите **Yes**.
   Устройство будет подключено к шаблону.

Добавление управляемых устройств на Сервер Управления

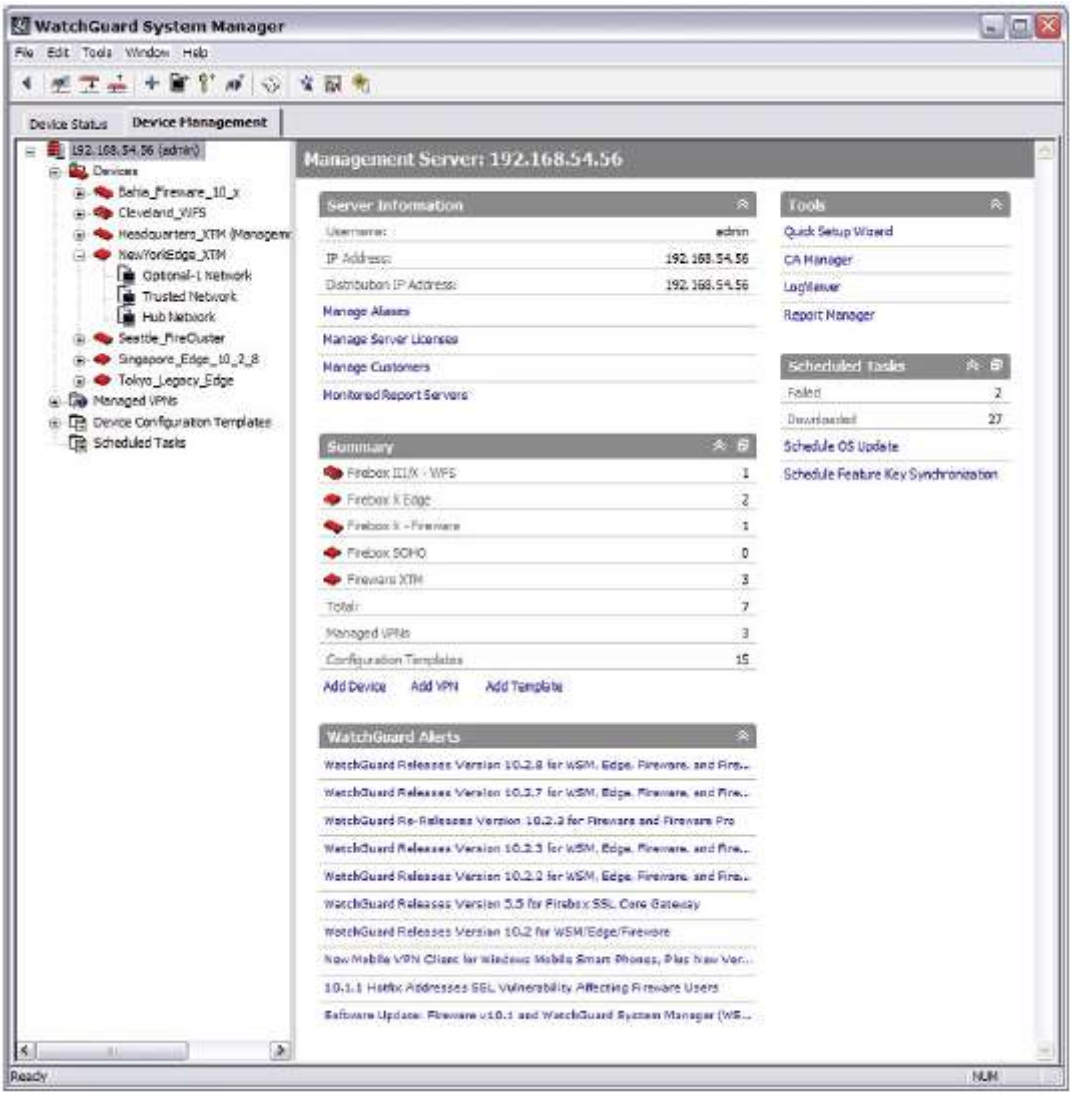
При помощи Сервера Управления вы можете управлять устройствами Firebox, включая устройства Firebox X, на которых установлен Fireware XTM, устройства Firebox X с Fireware, Firebox X Edge, Firebox III и Firebox X Core с установленным WFS и устройства Firebox SOHO. Если вы при помощи Policy Manager настроили устройство как управляемый клиент, то вы можете управлять устройством с динамическим IP адресом. Если у вашего устройства есть несколько внешних интерфейсов, то не меняйте их конфигурацию до тех пор, пока не добавите устройство на Сервер Управления.

В WatchGuard System Manager:

1. Нажмите  для того чтобы подключиться к Серверу Управления. Или выберите **File** > **Connect to Server**. Или нажмите правой кнопкой на любую область окна и выберите **Connect to > Server**.
   Откроется диалоговое окно Connect to Management Server.

2. Введите или выберите IP адрес Сервера Управления и введите пароль конфигурации.

3. Нажмите **Login**.
   Откроется страница Management Server



4. Нажмите  для того чтобы добавить устройство. Или на странице **Management Server** page, в секции **Summary** нажмите **Add Device**.
Запустится мастер Add Device.

5. Нажмите **Next**.
Откроется первая страница конфигурации

6. Выберие опцию:

   * **I know the device's current IP address**

   *** I don't know the device's current dynamically allocated IP address**

7. Выполните все необходимые инструкции в зависимости от выбранной вами опции.

If you know the current IP address of the device

1. В полях **Hostname/IP Address**, **Status Passphrase** и **Configuration Passphrase** введите имя хоста/IP адрес, пароль состояния и пароль конфигурации соответственно. Если вы выберете устройство, которое уже управляется другим сервером, появится предупреждение. Нажмите **Yes**

2. Нажмите **Next**.
Мастер запустит процедуру поиска устройства.

3. В поле **Client Name** введите имя устройства.

4. В выпадающем списке **Device Type** выберите тип устройства.

5. Введите и подтвердите ключ шифрования (**Shared Secret**). Имя и ключ шифрования, которые вы ввели здесь, должны совпадать с именем и ключом шифрования, которые вы ввели при настройке устройства в качестве управляемого клиента.

6. Нажмите **Next**.

7. В полях **Status Passphrase** и **Configuration Passphrase** введите и подтвердите пароли состояния и конфигурации соответственно. Нажмите **Next**.

8. Выберите алгоритм аутентификации туннеля для этого устройства. Нажмите **Next**.
Откроется страница Configure the Device.

9. Нажмите **Next**.
   Откроется страница Add Device Wizard is complete.

10. Проверьте введенную вами информацию. Нажмите **Close**.
    Мастер Add Device Wizard закроется и устройство появится в соответствующей категории устройство в WSM в списках Summary и Devices.

If you do not know the IP address of the device

После того, как мастер завершит работу, вы можете вручную настроить устройство для управления. Когда устройство настроено для управления, он попытается соединиться с Сервером Управления

1. Нажмите **Next**.
   Мастер не запустит процедуру поиска устройства и откроется страница с полем для ввода имени устройства.

2. В поле **Client Name** введите имя для устройства.

3. В выпадающем списке **Device Type** выберите тип устройства.

4. Введите и подтвердите ключ шифрования (**Shared Secret**). Имя и ключ шифрования, которые вы ввели здесь, должны совпадать с именем и ключом шифрования, которые вы ввели при настройке устройства в качестве управляемого клиента.

5. Нажмите **Next**.

6. В полях **Status Passphrase** и **Configuration Passphrase** введите и подтвердите пароли состояния и конфигурации соответственно. Нажмите **Next**.
   Откроется страница Select the tunnel authentication method.

7. Выберите алгоритм аутентификации туннеля для этого устройства. Нажмите **Next**.
   Откроется страница Configure the Device.

8. Нажмите **Next**.
   Откроется страница Add Device Wizard is complete.

9. Проверьте введенную вами информацию. Нажмите **Close**.
   Мастер Add Device Wizard закроется и устройство появится в соответствующей категории устройство в WSM в списках Summary и Devices.

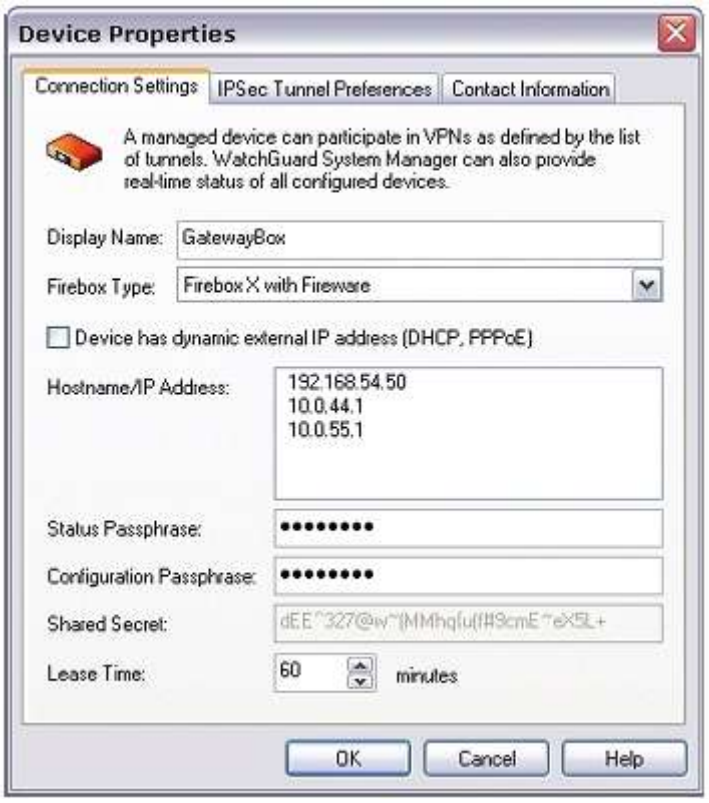
Если во время попытки подключения мастера к устройству по сети передается довольно большой объем трафик, то соединение может быть закрыто по таймауту. В этом случае запустите мастер снова и повторите все процедуры, описанные выше, когда трафика в сети будет меньше.

Настройка параметров управления устройством

На странице Device Management для вашего Firebox вы можете настроить три категории параметров управления: параметры соединения, параметры IPSec туннеля и контактную информацию.

Параметры соединения

1. На странице Device Management в секции **Device Information** нажмите **Configure**.
   Откроется диалоговое окно Device Properties



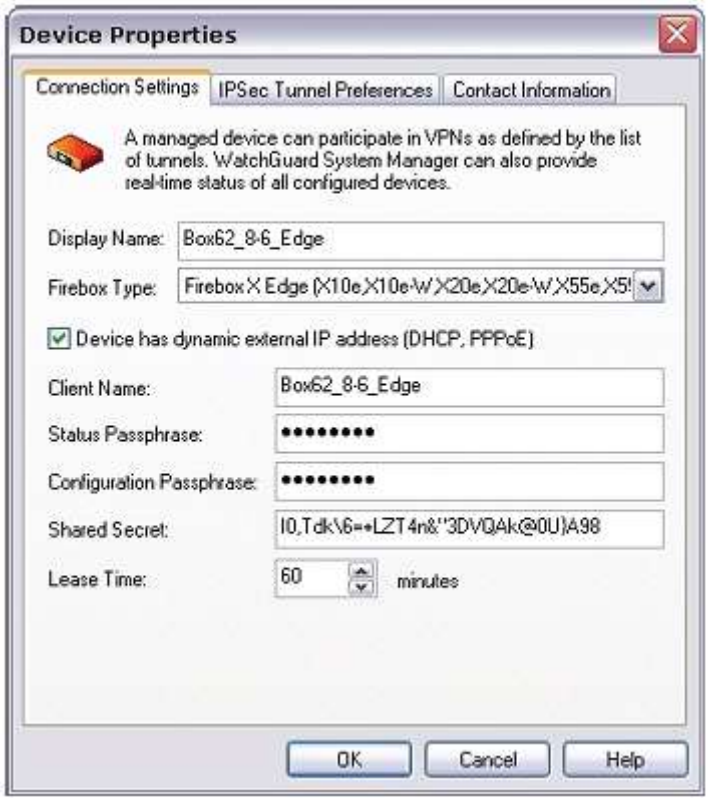
2. В поле **Display Name** введите имя устройства, которое будет отображаться в WSM.

3. В выпадающем списке **Firebox Type** выберите тип устройства и, если доступно, версию установленного ПО.

4. Если устройству присвоен статический IP адрес, то в поле **Hostname/IP Address** введите или выберите адрес для вашего устройства. Это поле содержит список внешних IP адресов, которые WSM использует для поиска устройств и создания VPN туннелей

5. Если устройству присвоен динамический IP адрес включите опцию **Device has dynamic external IP address**.

6. В поле **Client Name** введите имя устройства. Для более подробной информации о том, как вручную настроить устройство для управления см. “Настройка Firebox, как управляемое устройство”



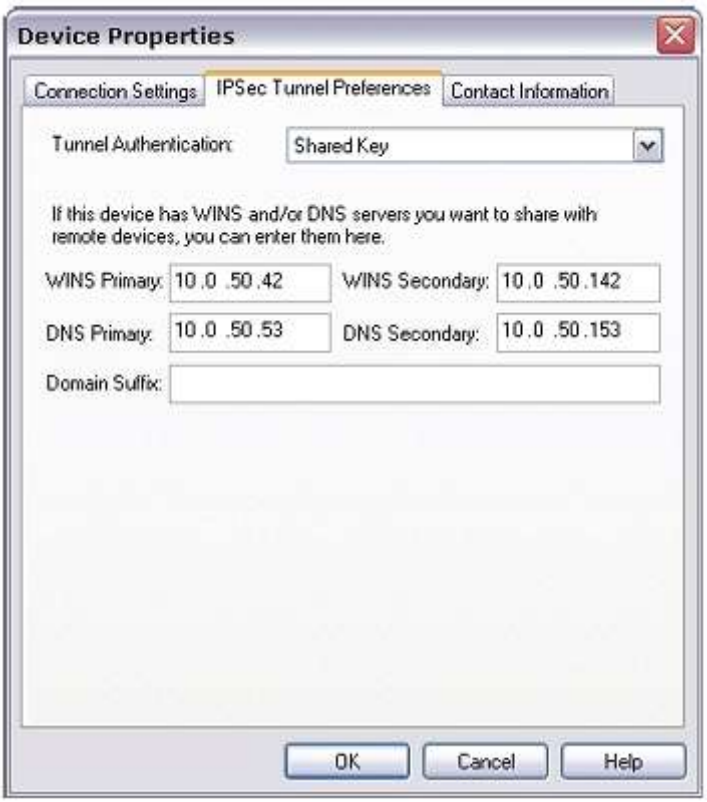
7. Введите пароли состояния и конфигурации для Firebox.

8. В поле **Shared Secret** введите ключ шифрования, который будет использоваться устройством и Сервером Управления.

9. При помощи стрелок **Lease Time** выберите значение интервала обновлений. Это временной интервал определяет, как часто управляемое устройство будет подключаться к Серверу Управления для загрузки обновлений. По умолчанию – 60 минут

Параметры IPSec туннеля

1. В диалоговом окне **Device Properties** выберите закладку **IPSec Tunnel Preferences**



2. (Не появляется в Edge версии v10.0 или ниже) В выпадающем списке **Tunnel Authentication** выберите **Shared Key** или **IPSec Firebox Certificate**

3. Если вы хотите, чтобы ваш управляемый клиент получал параметры WINS и DNS через IPSec BOVPN туннель, введите основной и резервный адреса **WINS и DNS** серверов. В противном случае оставьте эти поля пустыми. Вы также в поле **Domain Name** можете ввести суффикс домена для DHCP клиента, который он будет использовать с такими именами, как *kunstler_mail*.

Контактная информация

На странице Device Management для вашего Firebox вы можете посмотреть текущие записи в Contact List и при необходимости их изменить. Если вы хотите в Contact List для вашего устройства добавить запись, то вам необходимо сначала добавить ее в список контактов Сервера Управления.

Для более подробной информации см. “Manage customer contact information” on page 501.

1. В диалоговом окне **Device Properties** выберите закладку **Contact Information**.
   Откроется список удаленных устройств с их контактной информацией.

2. Для того чтобы посмотреть записи в списке контактов и при необходимо внести какие-либо изменения нажмите **Contact List**.
   Откроется список Contact List.

3. Для того чтобы изменить какую-нибудь запист, нажмите на ней два раза.
Откроется диалоговое окно Contact Information

4. Выполните необходимые изменения и нажмите **OK**.
Измененная запись появится в диалоговом окне Contact List.

5. Нажмите **OK**.

Создание расписания для обновлений ОС и синхронизации ключей функций

При помощи WatchGuard System Manager (WSM) вы можете создать расписание для двух типов задач для ваших управляемых устройств: обновления ОС и Синронизацию Ключей Функций. Обновления ОС для устройств Firebox должны быть установлены на Сервере Управления. Эти обновления вы можете загрузить с LiveSecurity при обновлении WSM.

При создании расписания для выполнения определенной процедуры, вы можете начать ее немедленно или установить время ее запуска в будущем. Вы также можете при помощи WSM загрузить самый последний ключ функций для всех управляемых устройств с сайта LiveSecurity. Например, вы можете сделать так, чтобы обновления ОС загружались каждую пятницу в полночь, а ключи функций синхронизировались в последний день каждого месяца.

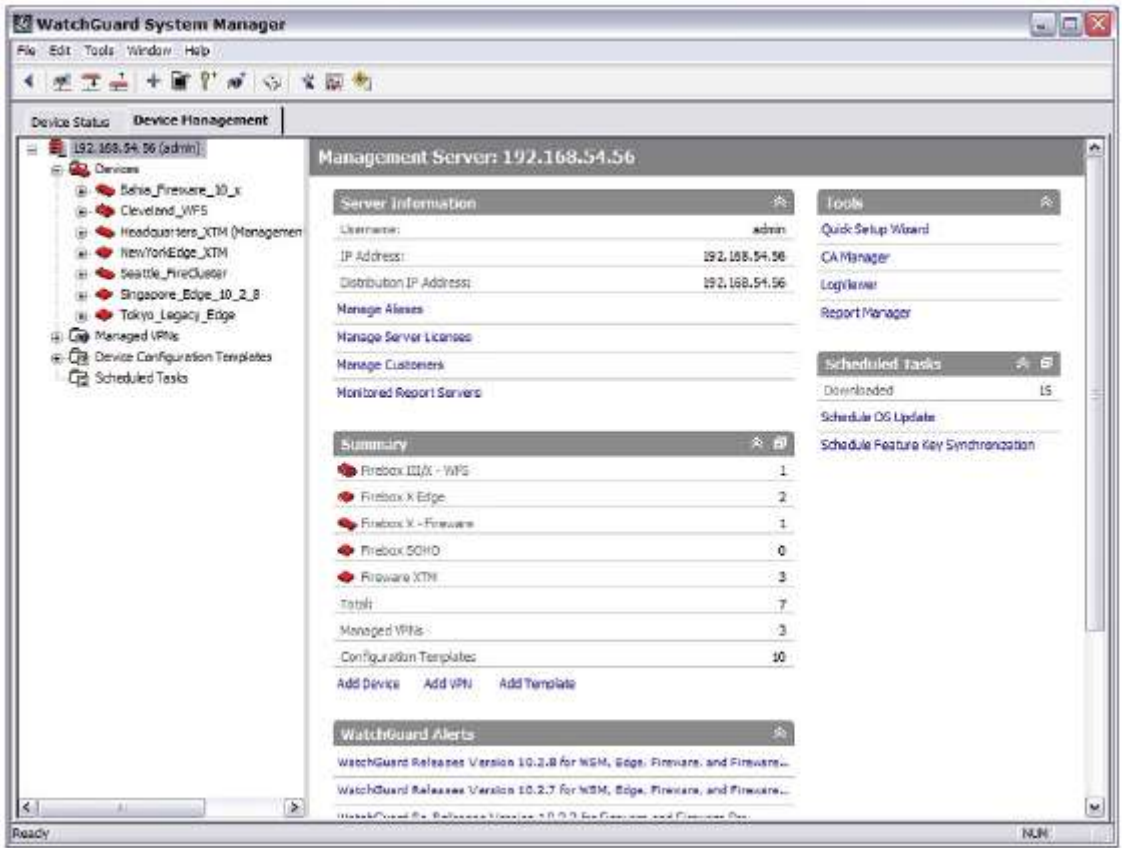
Также при помощи WSM вы также можете настроить регулярные обновления для устройств, управляемых в режиме Fully Managed. Эти обновления конфигурации настраиваются в Policy Manager

Текущий статус все запланированных задач отображается в закладке **Device Management**, на странице **Scheduled Tasks**.

Для того чтобы создать расписание для выполнения определенной процедуры в WatchGuard System Manager выполните следующее:

1. Выберите закладку **Device Management**.

2. В панели навигации слева выберите Сервер Управления, устройства которого вы хотите обновить.
Откроется страница Management Server. В разделе Scheduled Tasks в правой части страницы отображается количество задач по расписанию



3. В секции **Scheduled Tasks** выберите процедуру, для которой вы хотите создать расписание.

4. Выполните все инструкции, описание которых приведено ниже.

Расписание для обновлений ОС для вашего Firebox

Если для Firebox вы создадите расписание обновлений ОС, то перед тем, как процедура обновления будет завершена, Firebox должен перезагрузиться.

В разделе **Scheduled Tasks**:

1. Нажмите **Schedule OS Update**.
Запустится мастер Update OS.

2. Прочитайте сообщение приветствия и нажмите **Next**.
Откроется страница Select the device.

3. В выпадающем списке **Device Type** выберите тип устройства и нажмите **Next**.
Откроется страница Select the devices.

4. Отметьте флаги для устройств Firebox, для которых вы хотите создать расписание обновлений, и нажмите **Next**.
Откроется страница Select the OS version page.

5. В выпадающем списке **OS Version** выберите версию ОС и нажмите **Next**.
Откроется страница Select the Time and Date

6. Для того чтобы запустить процедуру обновления прямо сейчас выберите **Update OS immediately**. Для того чтобы отложить процедуру обновления на будущее выберите **Schedule OS update**.

7. Если вы выбрали **Schedule OS update**, то в поле **Date** и **Time** введите дату и время соответственно.

8. Нажмите **Next**.
Откроется страница Schedule the OS update.

9. Нажмите **Next**.
Откроется страница Update OS Wizard is complete.

10. Нажмите **Close** для того чтобы завершить работу мастера.
*Если вы выбрали **Update OS immediately** – ОС будет обновлена тут же, если вы выбрали Schedule OS update – то обновление ОС произойдет в указанные вами дату и время. Количество процедур по расписанию в секции Scheduled Tasks.*

При обновлении ОС по расписанию, Сервер Управления обновляет ОС устройства Firebox и затем перезагружает его.

Создание расписания для синхронизации ключей функций для управляемых Firebox

В секции **Scheduled Tasks** выполните следующее:

1. Нажмите **Schedule Feature Key Synchronization**.
Запустится мастер Synchronize Feature Keys.

2. Прочитайте приветственное сообщение и нажмите **Next**.
Откроется страница Select the devices.

3. Отметьте флаги для устройств Firebox, для которых вы хотите создать расписание синхронизаций, и нажмите **Next**.
   Откроется страница Select the Time and Date

4. Для того чтобы запустить процедуру синхронизации прямо сейчас выберите **Synchronize Feature Keys immediately**. Для того чтобы запустить процедуру синхронизации позже по расписанию, выберите **Schedule feature keys sync**.

5. Если вы выбрали **Schedule feature keys sync**, то в поле **Date** и **Time** введите дату и время соответственно.

6. Нажмите **Next**.
   Откроется страница Schedule the Feature Keys Synchronization.

7. Нажмите **Next**.
   Откроется страница Synchronize Feature Keys Wizard.

8. Нажмите **Close** для того чтобы завершить мастер
   Если вы выбрали Synchronize Feature Keys immediately – то процедура синхронизации ключей будет запущена прямо сейчас, а если вы выбрали Schedule feature keys sync – то процедура синхронизации будет в указанные вами дату и время. . Количество процедур по расписанию в секции Scheduled Tasks.

Для того чтобы посмотреть информацию для всех процедур по расписанию, или отменить процедуру или удалить ее совсем см. “Просмотр, отмена и удаление процедур по расписанию”

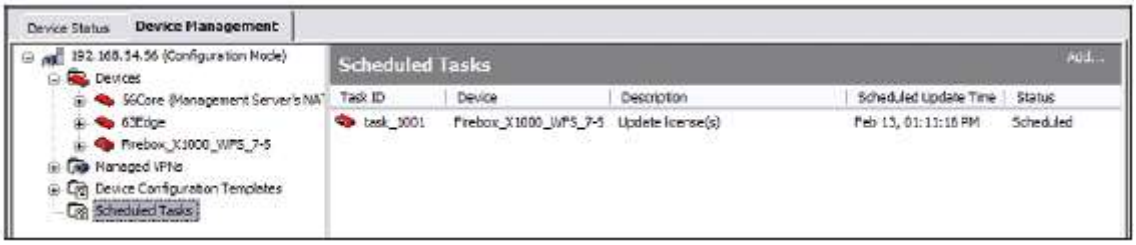
Просмотр, отмена и удаление процедур по расписанию

После того, как вы настроили процедуры обновлений ОС и синхронизации ключей для ваших управляемых устройств, вы можете их посмотреть более подробно или удалить их совсем. Редактировать процедуру по расписанию вы не можете. Если вы хотите изменить параметры процедуры по расписанию, вам необходимо ее удалить и создать новую с необходимыми параметрами.

Для более подробной информации о создании новой процедуры по расписанию см. “Создание расписания для обновлений ОС и синхронизации ключей функций”

1. Откройте WSM и подключитесь к Серверу Управления

2. В закладке **Device Management** нажмите **Scheduled Tasks**.
   Откроется страница Scheduled Tasks



3. Посмотрите информацию по каждой процедуре в списке **Scheduled Tasks**. Каждое обновление имеет уникальный Task ID и отображается в отдельной строчке для каждого устройства, даже если в одно обновления включены несколько устройств. Поэтому когда вы выбираете устройство в списке **Scheduled Tasks**, то выбираются все устройства, включенные в это обновление.

4. При необходимо отмените, удалите или создайте новые процедуры.

   * Для того чтобы удалить процедуру нажмите правой кнопкой на устройство и выберите **Remove Scheduled Update**.
   Процедура будет удалена для всех устройств, включенных в это обновление.

   * Для того чтобы отменить процедуру нажмите правой кнопкой на устройство и выберите **Cancel Scheduled Update**.
   Процедура останется в списке, но ее статус поменяется на Cancelled. Вы можете удалить эту процедуру позже. Активировать эту процедуру снова вы не можете.

   * Для того чтобы создать новую процедуру нажмите **Add** и выберите **Add OS Update**. Или нажмите правой кнопкой и выберите **Add OS Update**.
   Запустится мастер Update OS Wizard.

   * Для того чтобы создать процедуру синхронизации ключей нажмите **Add** и выберите **Add Feature Key Synchronization**. Или нажмите правой кнопкой и выберите **Add Feature Key Synchronization**.
   Запустится мастер Synchronize Feature Keys Wizard.

Удаление процедур по расписанию

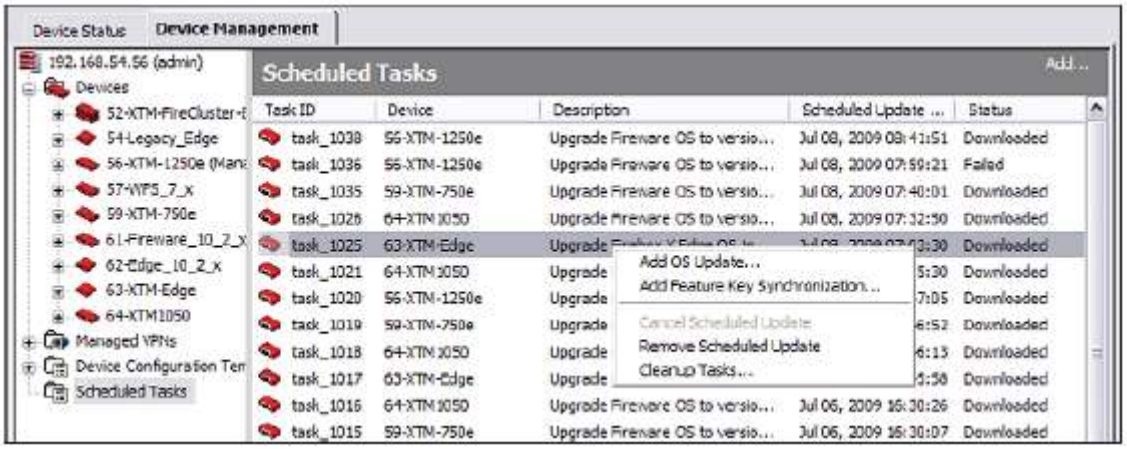
Список Scheduled Tasks list содержит все процедуры обновления ОС и синхронизации ключей функций для вашего Сервера Управления. Если список Scheduled Tasks содержит процедуры, которые имеют статус **Cancelled**, **Downloaded**, **Installed** или **Failed**, вы можете удалить их по отдельности (см. предыдущий раздел) или можете удалить их сразу все.

Для того чтобы удалить все процедуры выполните следующее:

1. Откройте WSM и подключитесь к Серверу Управления

2. В закладке **Device Management** нажмите **Scheduled Tasks**.
   Откроется страница Scheduled Tasks.

3. В окне **Scheduled Tasks** нажмите правой кнопкой на любую область окна.
   Появится контекстное меню



4. Выберите **Cleanup Tasks**.
   Появится сообщение предупреждения

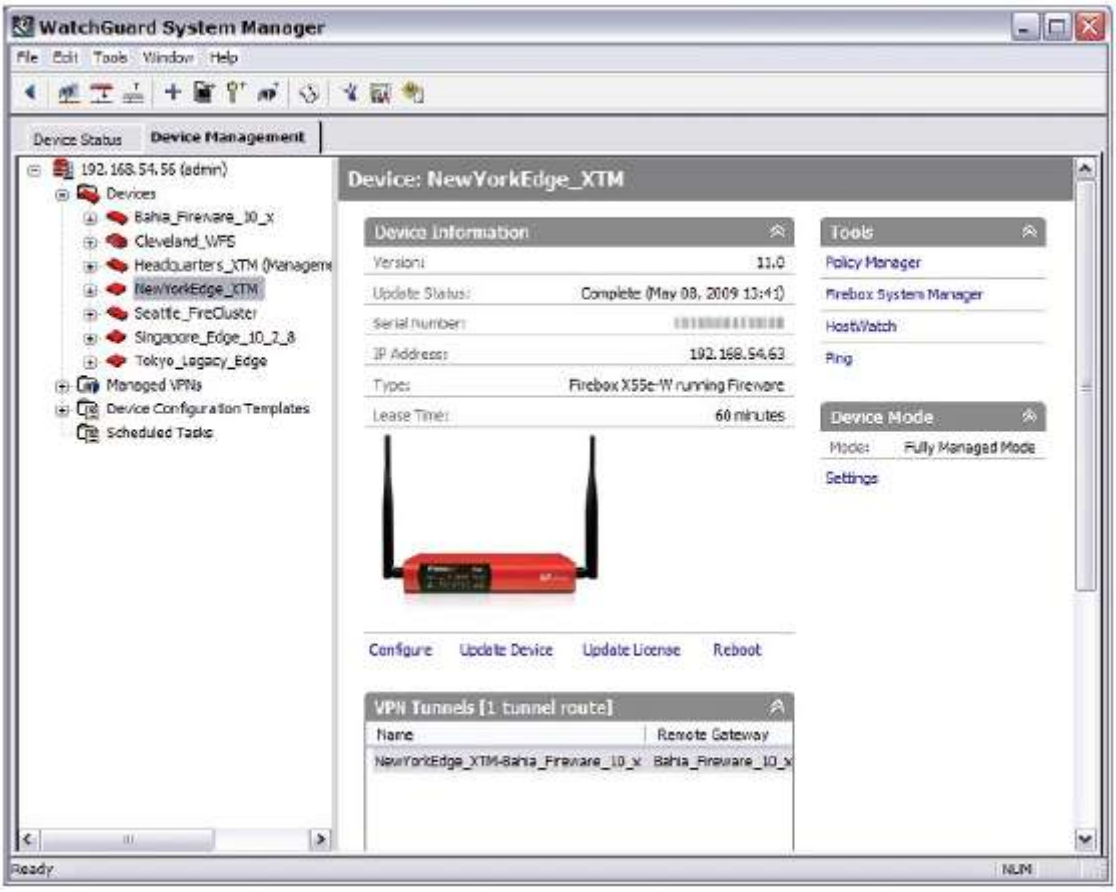
5. Нажмите **Yes**.
   Все процедуры, кроме процедур со статусом Scheduled будут удалены из списка

Обновление конфигурации для устройства в режиме Fully Managed

Для того чтобы изменить конфигурацию устройств в режиме Fully Managed, вам необходимо в закладке Device Management утилиты WatchGuard System Manager запустить Policy Manager для этого устройства.

1. Откройте WSM и подключитесь к Серверу Управления.

2. Откройте список **Devices** и выберите Firebox X Edge или Fireware XTM.
Откроется страница Device для выбранного устройства



3. В разделе **Tools** нажмите **Policy Manager**.
Policy Manager откроет конфигурационный файл для выбранного вами устройства.

4. Внесите необходимые изменения в конфигурационный файл.

5. Сохраните конфигурацию в файл или на Сервер Управления. Для более подробной информации об опциях сохранения конфигурации см. следующие разделы данной главы.

Для того чтобы сохранить конфигурацию в файл выполните следующее:

1. Нажмите . *Откроется диалоговое окно Save.*

2. В **File name** введите имя конфигурационного файла.

3. Выберите каталог, в который вы хотите этот файл сохранить.

4. Нажмите **Save**.
Конфигурация будет сохранена в файл в указанный каталог.

Для того чтобы сохранить конфигурацию прямо на Сервер Управления выполните следующее:

1. Нажмите .
Запустится мастер Schedule Configuration Update.

2. Нажмите **Next**.
Откроется страница Select the Time and Date.

3. Выберите опцию, когда вы хотите обновить конфигурационный файл.

   * **Update configuration immediately (Обновить файл прямо сейчас)**

   * **Schedule configuration update (Обновить конфигурационный файл по расписанию)**

4. Если вы выбрали обновление по расписанию, в полях **Date** и **Time** выберите дату и время обновления.

5. Нажмите **Next**.
   Откроется страница Schedule Configuration Update.

6. Нажмите **Finish** для того чтобы завершить работу мастера.
   Появится сообщение о том, чтобы конфигурация была сохранена на Сервере Управления. Если вы создадите расписание для обновления, дата следующего обновления появится в поле Update Status на странице Device для устройства и на главной странице Devices.

Управление лицензиями сервера

Вы можете при помощи WatchGuard System Manager (WSM) управлять лицензиями Сервера Управления. Вы можете добавлять или удалять лицензионные ключи, а также смотреть информацию о текущем лицензионном ключе, включая количество устройств, работой которой вы можете управлять.

Просмотр информации о текущем лицензионном ключе

1. Откройте WSM и подключитесь к Серверу Управления
   Откроется страница Management Server.

2. В секции **Server Information** нажмите **Manage Server Licenses**. Или выберите **File** > **Manage Server Licenses**.
   Откроется диалоговое окно Management Server Licenses

Добавление или удаление лицензионных ключей

Для того чтобы добавить лицензионный ключ выполните следующее:

1. В диалоговом окне **Management Server Licenses** нажмите **Add**.
   Откроется диалоговое окно Add License Key

2. В текстовом поле **License Key** введите и вставьте лицензионный ключ.

3. Нажмите **OK**.
   Новый ключ появится в окне License Keys. При этот изменится количество лицензированных устройств.

Для того чтобы удалить лицензионный ключ выполните следующее:

1. В окне **License Keys** выберите ключ, который вы хотите удалить.

2. Нажмите **Remove**.
   Ключ будет удален в окне License Keys. При этом количество лицензированных устройств обновится.

Сохранение или отмена сделанных изменений

После того, как вы добавили или удалили лицензионный ключ, вы можете эти изменения сохранить или отменить.

В диалоговом окне **Management Server Licenses** выполните следующее:

- Для того чтобы сохранить изменения нажмите **OK**.

- Для того чтобы закрыть диалоговое окно и отменить сделанные изменения нажмите **Cancel**.

Управление контактной информацией о клиенте

При помощи WatchGuard System Manager (WSM) вы можете управлять контактной информацией, которая отображается для вашего Сервера Управления. После того, как вы добавите данные в список Contact List, вы можете для контактов каждого управляемого устройства добавить необходимую информацию

Добавление контакта на Сервер Управления

В любое время вы можете добавить новый контакт в список Contact List на Сервере Управления.

1. Откройте WSM и подключитесь к Серверу Управления.
   Откроется страница Management Server.

2. В секции **Server Information** нажмите **Manage Customers**.
   Откроется диалоговое окно Contact List.

3. Для того чтобы добавить контакт в список нажмите **Add**.
   Откроется диалоговое окно Contact Information.

4. Введите необходимую информацию. Эта информация необязательна

5. Нажмите **OK**.
   Новый контакт появится в списке Contact List.

6. Для того чтобы добавить контакт повторите п. 3–5.

7. Нажмите **OK** после того, как вы завершите.

Редактирование контакта в списке Contact List

Вы можете изменить любую информацию для выбранног контакта в списке Contact List.

1. Подключитеь к Серверу Управления.
   Откроется страница Management Server.

2. В секции **Server Information** нажмите **Manage Customers**.
   Откроется диалоговое окно Contact List.

3. В диалоговом окне **Contact List** выберите контакт, информацию которого вы хотите изменить.

4. Нажмите **Edit**.
   Откроется диалоговое окно Contact information

5. Внесите необходимые изменения.

6. Нажмите **OK**.
   Обновленная запись появится в диалоговом окне Contact List.

7. Для того чтобы изменить информацию для другого контакта повторите п. 1–5.

8. Нажмите **OK**

Просмотр и управление списком Monitored Report Servers

Список Monitored Report Servers используется для настройки списка Серверов Отчетов, которые установлены на разные компьютеры. Если вы установите Сервер Журналов и Сервер Отчетов на разные компьютеры, ваш Сервер Управления для поиска Серверов Журнала будет отправлять запросы на Серверы Отчетов в списке Report Server. Затем, если вы подключаетесь к Report Manager через WatchGuard System Manager (WSM), он подключится к соответствующему Серверу Отчетов.

При помощи WSM вы можете смотреть и управлять информацией о соединениях для ваших Серверов Отчетов. Вы можете добавить новый Сервер Отчетов, изменить IP адрес или номер порта для существующего Сервера Отчетов, или удалить Сервер Отчетов из списка.

1. Откройте WSM и подключитесь к Серверу Управления.
   Откроется страница Management Server.

2. В секции **Server Information** нажмите **Monitored Report Servers**.
   Откроется диалоговое окно Report Server List

3. Выполните все необходимые инструкции, описание которых приведено в следующих разделах.

Добавление Сервера Отчетов

1. В диалоговом окне **Report Server List** нажмите **Add**.
   Откроется диалоговое окно Report Server

2. В поле **IP Address** введите IP адрес Сервера Отчетов.

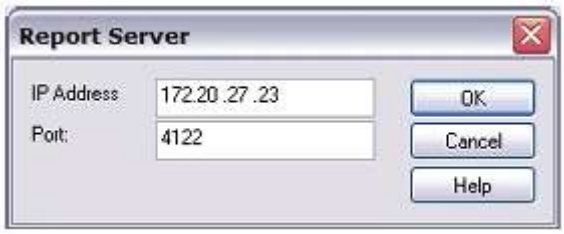
3. В поле **Port** введите номер порта для подключения к Серверу Отчетов.

4. Нажмите **OK**.

5. Повторите п. 1–4 для того чтобы добавить несколько Серверов Отчетов.

Изменение информации для существующего Сервера Отчетов

1. В диалоговом окне **Report Server List** нажмите **Edit**.
   Откроется диалоговое окно Report Server



2. В поле **IP Address** или **Port** введите IP адрес или номер порта для Сервера Отчетов.

3. Нажмите **OK**.

Удаление Сервера Отчетов из списка

1. В диалоговом окне **Report Server List** выберите Сервер Отчетов, который вы хотите удалить.

2. Нажмите **Remove**.
Выбранный Сервер Отчетов будет удален из списка.

Добавление и управление VPN туннелями и ресурсами

В WatchGuard System Manager вы можете управлять VPN туннелями и ресурсами ваших управляемых Firebox. В разделе **VPN Tunnels** страницы **Device** вы можете посмотреть все туннели, которые включают выбранное устройство Firebox..

Просмотр VPN туннелей

В WatchGuard System Manager:

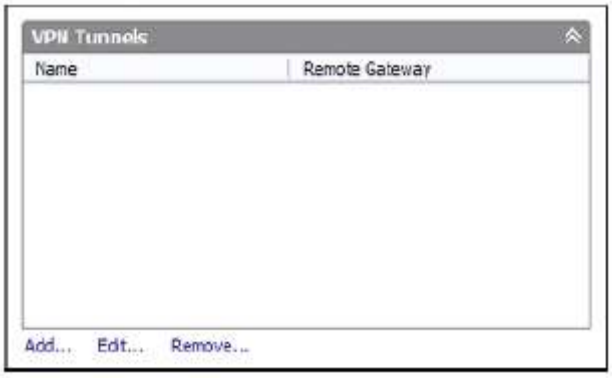
1. Подключитесь к Серверу Управления.

2. Выберите закладку **Device Management**.

3. Откройте список **Devices**.

4. Выберите Firebox.
   Для выбранного Firebox откроется страница Device Management

5. Найдите секцию **VPN Tunnels**.
В этой секции отображаются все туннели, для которых выбранное устройство является конечной точкой



Добавление VPN туннеля

В секции **VPN Tunnels** выполните следующее:

1. Нажмите **Add** для того чтобы добавить новый VPN туннель.
Запустится мастер Add VPN Wizard.

2. Выполните все необходимые инструкции мастер **Add VPN Wizard**

Если вы попытаетесь добавить количество туннелей, которое превышает установленный лицензией максимальный лимит, то появится предупреждение о том, что максимальное количество туннелей превышено.

После того, как вы добавите VPN туннель к вашей конфигурации, этот туннель появится в списке и общее количество VPN туннелей появится в секции **VPN Tunnels**

Редактирование VPN туннеля

После того, как вы добавили VPN туннель, вы можете при помощи WSM внести изменения в его конфигурацию. Вы не можете изменять конфигурацию обеих конечных точек туннеля. Если вы хотите внести в конфигурацию устройства Firebox, которое является конечной точкой туннеля, то вам необходимо будет создать новый туннель.

В секции **VPN Tunnels** выполните следующее:

1. В списке **Name** выберите VPN туннель.

2. Нажмите **Edit**.
Откроется диалоговое окно VPN Properties.

3. Выполните все необходимые изменения в настройках VPN туннеля

4. Нажмите **OK**.
   VPN туннель появится в списке Name.

Удаление VPN туннеля

В секции **VPN Tunnels** выполните следующее:

1. В списке **Name** выберите туннель.

2. Нажмите **Remove**.
   Появится сообщение подтверждения.

3. Если вы хотите, чтобы изменения конфигурации, сразу же не вступали в силу отключите опцию **Restart devices now to expire leases and download new configuration**.

4. Нажмите **Yes**.
   VPN туннель будет удален из списка и устройство будет перезагружено.

Добавление VPN ресурса

Вы можете создать ресурсы, доступ к которым пользователь может получить через VPN туннели. Создавать VPN между хостами или сетями. Вы также можете настроить VPN ресурсы для настройки сетей, которые доступны через данное VPN устройство.

В закладке **Device Management** вы можете посмотреть список созданных VPN ресурсов.

Настройка Firebox, как управляемое устройство

Если ваш Firebox имеет динамический IP адрес, или если Сервер Управления не может подключиться к нему по какой-то причине, вы можете, перед тем, как добавлять устройство на Сервер Управления, настроить Firebox как управляемый клиент. Затем вы можете добавить устройство на Сервер Управления.

Редактирование политики WatchGuard

1. Откройте Policy Manager для Firebox, который вы хотите настроить как управляемое устройство.

2. Два раза нажмите на политику **WatchGuard**.
   Откроется диалоговое окно Edit Policy Properties для политики WatchGuard

3. Убедитесь, что в выпадающем списке **WatchGuard-Firebox-Mgmt connections are** выбран параметр **Allowed**.

4. Под элементом **From**, нажмите **Add**. Нажмите **Add Other**.
   Откроется диалоговое окно Add Address.

5. Нажмите **Add Other**.
   Откроется диалоговое окно Add Member

6. Убедитесь, что в выпадающем списке **Choose Type** выбран параметр **Host IP**.

7. В поле **Value** введите IP-адреса интерфейса External шлюза Firebox. Если у вас нет Firebox шлюза, который защищает Сервер Управления от сети Интернет, введите статический IP адрес вашего Сервера Управления.

8. Нажмите **OK** для того чтобы закрыть диалоговое окно **Add Member**.

9. Нажмите **OK** для того чтобы закрыть диалоговое окно **Add Address**.

10. Убедитесь, что диалоговое окно **To** содержит параметр **Firebox** или **Any**.

11. Сохраните конфигурационный файл.

Теперь вы можете добавить устройство в конфигурацию Сервера Управления, как описано в “Добавление управляемых устройств на Сервер Управления”. После того, как вы добавите Firebox на Сервер Управления, сервер автоматически подключится к статическому IP адресу и настроит устройство Firebox, как управляемый клиент.

Настройка управляемого устройства

(Дополнительно)

Если ваш Firebox имеет динамический IP адрес, или если ваш Сервер Управления по какой-то причине не может найти IP адрес Firebox, вы можете использовать эту процедуру для подготовки вашего Firebox в качестве управляемого устройства.

1. В Policy Manager выберите **Setup** > **Managed Device Settings**.
   Откроется диалоговое окно Managed Device Settings

2. Для того чтобы настроить Firebox, как управляемое устройство, включите опцию **Centralized Management**.

3. В поле **Managed Device Name** введите имя устройства. Это имя чувствительно к регистру и должно совпадать с именем устройства, которое вы ввели при добавлении устройства в конфигурацию Сервера Управления.

4. В случае если Firebox имеет публичный IP адрес в окне **Management Server IP Address(es)** выберите IP адрес Сервера Управления. Или выберите публичный IP адрес Firebox шлюза для Сервера Управления.

5. Для того чтобы добавить нажмите **Add**. Firebox, который защищает Сервер Управления, автоматически следит за портами, которые используются Сервером Управления, и переадресует все подключения по этим портам на Сервер Управления. Если вы используете мастер Management Server Setup, то мастер для обработки этих подключений создает политику *WG-Mgmt-Server*. В противном случае вам необходимо создать эту политику вручную

6. В полях **Shared Secret** и **Confirm** введите ключ шифрования. Ключ шифрования, который вы введете здесь, должен совпадать с ключом шифрования, который вы ввели при добавлении устройства Firebox в конфигурацию Сервера Управления.

7. Нажмите на кнопку Import и импортируйте файл CA-Admin.pem, как ваш сертификат. Этот файл находится в каталоге *My Documents\My WatchGuard\certs\[firebox_ip]*.

8. Нажмите **OK**.

При сохранении конфигурации Firebox будет настроен, как управляемое устройство. Управляемый Firebox пытается подключиться к IP адресу Сервера Управления через TCP порт 4110. Трафик управления разрешены с Сервера Управления на управляемое устройство.

Теперь вы можете добавить устройство в конфигурацию Сервера Управления, как описано в "Добавление управляемых устройств на Сервер Управления"

Также при помощи WSM вы можете настроить режим управления вашим устройством, как описано в "Режимы Централизованного Управления"

Настройка Firebox III или Firebox X Core с WFS, как управляемые клиенты

1. Откройте Policy Manager для Firebox, который вы хотите настроить как управляемый клиент.

2. Два раза нжамите на сервис **WatchGuard**.
Откроется диалоговое окно Edit Service Properties.

3. В закладке **Incoming** убедитесь, что для входящих соединений WatchGuard установлен параметр **Enabled and Allowed**.

4. Под элементом **From**, нажмите **Add**.
Откроется диалоговое окно Add Address

5. Нажмите **Add Other**.
Откроется диалоговое окно Add Member.

6. Убедитесь, что в выпадающем списке **Choose Type** выбран параметр **Host IP Address**.

7. В поле **Value** введите IP-адреса интерфейса External шлюза Firebox, который защищает Сервер Управления от сети Интернет. Если у вас нету шлюза Firebox, который защищает Сервер Управления из сети Интернет, введите статический IP-адрес вашего Сервера Управления.

8. Нажмите **OK** для того чтобы закрыть диалоговое окно **Add Member**.

9. Нажмите **OK** для того чтобы закрыть диалоговое окно **Add Address**.

10. Убедитесь, что диалоговое окно **To** содержит параметр **Firebox** или **Any**

    Если интерфейс External устройства Firebox, которым вы хотите управлять, имеет статический IP-адрес, то на данном этапе вы можете остановиться. Сохраните вашу конфигурацию в Firebox. Теперь вы можете добавлять устройство к конфигурации вашего Сервера Управления. После того, как вы добавите этот Firebox к конфигурации Сервера Управления, Сервер автоматически подключается к статическому IP-адресу и настраивает Firebox как управляемого клиента Если Firebox, которым вы хотите управлять, имеет динамический IP-адрес, см. п. 11.

11. В окне **Policy Manager** выберите **Network** > **DVCP Client**.

12. Включите опцию **Enable this Firebox as a DVCP Client**.

13. В поле **Firebox Name** введите имя для **Firebox**.
    Это имя чувствительно к регистру и должно совпадать с именем, которое вы использовали при добавлении устройства к Серверу Управления

14. Для того чтобы отправлять сообщения журнала для управляемого клиента включите опцию **Enable debug log messages for the DVCP Client.** Мы рекомендуем выбрать эту опцию только в случае решения каких-либо проблем.

15. Нажмите **Add** для того чтобы добавить Сервер Управления, в которому будет подключаться устройство Firebox.
    Откроется диалоговое окно DVCP Server Properties.

16. В поле **IP address** введите IP адрес Сервера Управления (если он использует публичный IP адрес). Или введите публичный IP адрес устройства Firebox, который защищает Сервер Управления.

    Firebox, который защищает Сервер Управления, автоматически выполняет мониторинг всех портов, используемых Сервером и переадресует любые подключения через эти порты на Сервер Управления. Вы можете настроить Firebox, который защищает Сервер Управления, при помощи мастера Management Server Setup Wizard. Если вы использовали мастер Management Server Setup Wizard,или, если вы пропустили этап “Gateway Firebox”, настройте шлюз Firebox для переадресации TCP портов 4110, 4112 и 4113 на внутренний IP-адрес Сервера Управления.

17. В поле **Shared Secret** введите ключ шифрования, который будет использоваться для подключения к Firebox. Ключ шифрования, которые вы введете здесь, должен совпадать с ключом шифрования, который вы ввели при добавлении устройства на Сервере Управления. Устройство Firebox может быть клиентом только одного Сервера Управления.

18. Нажмите **OK** для того чтобы закрыть диалоговое окно **DVCP Server Properties**.

19. Нажмите **OK** для того чтобы закрыть диалоговое окно **DVCP Client Setup**.

20. Сохраните конфигурационный файл. После того, как вы сохраните конфигурацию, Firebox станет управляемым клиентом. Управляемый Firebox пытается подключиться к IP адресу Сервера Управления через порт TCP 4110. Трафик управления разрешены с Сервера Управления на управляемое устройство.

Теперь вы можете добавить устройство в конфигурацию Сервера Управления, как описано в “Добавление управляемых устройств на Сервер Управления”

Edge (v10.x и выше) и SOHO устройства, как управляемые клиенты

Для того чтобы разрешить трафик между станцией управления и Сервером Управления для устройств Firebox X Edge (версии v10.x или ниже), вам необходимо добавить пакетный фильтр WG-SmallOffice-Mgmt в конфигурацию на вашем Firebox шлюзе. Если у вас есть другой брандмауэр, то на нем необходимо политику, которая разрешала бы трафик с управляемых устройств Edge через TCP порт.Если вы создали этот пакетный фильтр и все еще испытываете проблемы с подключением к Web Manager устройства Edge из WSM, то скорее всего проблема с сертификатом в кэше браузера. Удалите все сертификаты WatchGuard и все cookies из хранилища сертификатов вашего web браузера, подключитесь к Серверу Управления, и затем снова попробуйте подключиться к Web Manager устройства Edge.

При помощи Сервера Управления вы можете настраивать и управлять работой устройств Firebox X Edge и SOHO. Для устройств Firebox X Edge (версии 10.x или выше), вы можете включить режим Fully Managed. При этом вы можете управлять политиками, обновлениями и VPN многих устройств Edge, которые расположены в различных местах. Вы можете использовать устройства Edge и SOHO в качестве конечных точек управляемых BOVPN туннелей.

Для того чтобы управлять Firebox X Edge device (версии 10.x и выше) через Сервер Управления, вам необходимо:

1. Установить устройство Edge — Физически подключить его к Ethernet интерфейсу вашего компьютера и запустить мастер Quick Setup Wizard.

2. Добавить устройство Edge на Сервер Управления — Вы можете импортировать сразу несколько устройств Edge.

3. Выполните настройку параметров доступа WSM на устройстве Edge — Первые три этапа описаны в “Подготовка Firebox X Edge (версии v10.x и ниже) для управления”

4. Настройте значения, которые будут использоваться для идентификации устройства на Сервере Управления — “Добавление управляемых устройств на Сервер Управления”

Подготовка Firebox X Edge (версии v10.x и ниже) для управления

В своей конфигурации по умолчанию устройства Firebox X Edge версии до 11.x нельзя добавить на Сервер Управления, как управляемые устройства. Перед тем, как добавить Firebox на Сервер Управления вам необходимо убедиться, что устройство может быть под управлением Сервера Управления. Только после этого вы можете добавить устройство Firebox X Edge на Сервер Управления.

Для того чтобы подготовить устройство Firebox X Edge с ПО версии 10.x или ниже для управления через Сервер Управления, вам необходимо физическое подключение устройства Firebox X Edge к сетевому интерфейсу вашего компьютера. Мы рекомендуем перед началом процедуры подготовки перезагрузить устройство Edge.

Установка устройства Firebox X Edge

1. На компьютере, на котором запущен WatchGuard System Manager, измените IP адрес на: *192.168.111.x/24*.

2. Запустите WatchGuard System Manager и выберите **Tools > Quick Setup Wizard**. *Запустится мастер Quick Setup Wizard.*

3. Прочитайте информацию на странице **Welcome** и нажмите **Next**.

4. Выберите тип устройства - **Firebox X Edge** и нажмите **Next**.

5. Подключите сетевой интерфейс вашего компьютера к любому сетевому порту устройства Firebox X Edge, и нажмите **Next**.

6. Для подключения используйте один из Ethernet кабелей зеленого цвета, который входит в комплект поставки Firebox X Edge. (Если кабеля зеленого цвета в комплекте поставки нет, то попробуйте использовать кабель красного цвета)

7. Выполните инструкции на следующих страницах мастера для того чтобы перезагрузить Firebox X Edge в безопасном режиме.

8. Выполните все необходимые инструкции и нажмите **Next**.

9. Выполните все необходимые инструкции на страницах **Wait for the Firebox** и **The Wizard found this Firebox**. Нажмите **Next**

10. Примите условия лицензионного соглашения и нажмите **Next**.

11. Настройте External (WAN 1) интерфейс устройства Firebox X Edge. Выберите **DHCP**, **PPPoE** или **Static IP addressing**, и нажмите **Next**

12. Нажмите **Next** после того, как вы настроите интерфейс.

13. Настройте внутренний интерфейс устройства Edge и нажмите **Next**.

14. Введите пароли состояния и конфигурации для вашего устройства Edge и нажмите **Next**. Каждый пароль вам необходимо ввести два раза. Это пароли, которые используются WatchGuard System Manager для подключения и настройки устройства.

15. Введите имя пользователя и пароль для устройства и нажмите **Next**. Пароль вам необходимо ввести два раза. Эти данные используются для подключения и настройки устройства через web браузер.

16. Выберите часовой пояс и нажмите **Next**.

17. Настройте параметры Сервера Управления. Введите IP адрес Firebox шлюза, который защищает Сервер Управления, имя, которое будет использоваться для идентификации устройства Firebox на Сервере Управления, и ключ шифрования. Нажмите **Next**. Ключ шифрования используется Сервером Управления для создания VPN туннелей между устройствами Fireboxes. Вам необязательно помнить этот ключ.

18. Проверьте конфигурацию еще раз и нажмите **Next**. 18. Для того чтобы настроить еще одно устройство Edge, включите опцию. Нажмите **Finish**.

Если вы включите эту опцию, то мастер Quick Setup заполните все поля этими же значениями. Тем самым вы можете настроить несколько устройств Edge.

Импорт устройств Firebox X Edge на Сервер Управления

Устройства Firebox X Edge, настроенные при помощи мастера Quick Setup Wizard, можно импортировать на Сервер Управления.

1. Запустите WatchGuard System Manager и подключитесь к Серверу Управления, для которого вы настроили устройства Edge.

2. Выберите **File** > **Import Device**.
   Откроется диалоговое окно WatchGuard System Manager.

3. Включите опции для тех устройств Edge, которые вы хотите импортировать.

4. Нажмите **Import**.

Устройства Firebox X Edge будут импортированы на Сервер Управления. Устройства отображаются в каталоге **Imported Devices** на Сервере Управления.

Настройка параметров доступа WSM на устройстве Edge

1. Для того чтобы подключиться к странице System Status введите *https://* и IP адрес Trusted интерфейса устройства Edge.
   По умолчанию URL: https://192.168.111.1

2. В панели навигации выберите **Administration > WSM Access**.
   Откроется страница WatchGuard Management Access

3. Включите опцию **Enable remote management**.

4. В выпадающем списке **Management Type** выберите **WatchGuard System Manager**.

5. Для того чтобы включить режим Fully Managed включите опцию **Use Centralized Management**. Когда устройство Firebox X Edge находится в режиме Fully Managed, доступ к его страницам конфигурации – только чтение. Исключение – доступ к странице WSM Access. Если вы отключите функцию удаленного управления, то вы снова получите права чтения-записи конфигурации Edge.

   *Не включайте эту опцию **Use Centralized Management** если вы используете WatchGuard System Manager только для управления VPN туннелями*

6. В поле **Status Passphrase** введите пароль состояния. Введите пароль состояния еще раз.

7. В поле **Configuration Passphrase** введите пароль конфигурации. Введите пароль конфигурации еще раз. Эти пароли должны совпадать с паролями, которые вы ввели при добавлении устройства на Сервер Управления

   Если интерфейс External устройства Firebox, которым вы хотите управлять, имеет статический IP-адрес, то на данном этапе вы можете остановиться. Сохраните вашу конфигурацию в Firebox. Теперь вы можете добавлять устройство к конфигурации вашего Сервера Управления. После того, как вы добавите этот Firebox к конфигурации Сервера Управления, Сервер автоматически подключается к статическому IP-адресу и настраивает Firebox как управляемого клиента Если Firebox, которым вы хотите управлять, имеет динамический IP-адрес см. следующий шаг

8. В поле **Management Server Address** введите IP адрес Сервера Управления – если у него есть публичный IP адрес. Если Сервер Управления имеет внутренний IP адрес, то введите публичный IP адрес устройства Firebox, к которому подключен Сервер Управления. Firebox, к которому подключен Сервер Управления, автоматически следит за портами,

которые используются Сервером Управления, и автоматически перенаправляет соединения по этим портам на Сервер Управления

9. В поле **Client Name** введите имя устройства, которое будет использоваться для его идентификации. Это имя чувствительно к регистру и должно совпадать с именем, которое вы ввели при добавлении устройства на Сервере Управления.

10. В поле **Shared Key** введите ключ шифрования. Этот ключ шифрования будет использовать для шифрования данных между Сервером Управления и устройством Firebox X Edge. Ключи на устройстве Edge и на Сервере Управления должны быть одинаковыми. Поэтому ключ шифрования получите у администратора Сервера Управления.

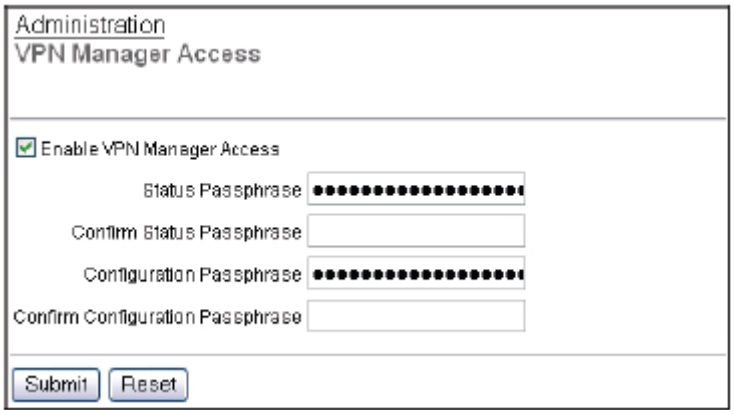
11. Нажмите **Submit** для того чтобы сохранить конфигурацию. После того, как вы сохраните конфигурацию, Firebox X Edge станет управляемым клиентом. Управляемый Firebox пытается подключиться к IP адресу Сервера Управления через порт TCP 4110. Трафик управления разрешены с Сервера Управления на управляемое устройство. Теперь вы можете добавить устройство в конфигурацию Сервера Управления, как описано в “Добавление управляемых устройств на Сервер Управления”.

Настройка Firebox SOHO 6, как управляемый клиент

1. Запустите ваш web-браузер. Введите IP-адрес SOHO 6.

2. При необходимости введите имя пользователя и пароль для подключения к SOHO 6.

3. Под секцией **Administration** нажмите **VPN Manager Access**.
Откроется страница VPN Manager Access



4. В панели навигации слева выберите **Managed VPN**.

5. Включите опцию **Enable VPN Manager Access**.

6. Введите пароль состояния. Введите подтверждение пароля состояния.

7. Введите пароль конфигурации. Введите подтверждение пароля конфигурации.

   *Если External интерфейс Firebox SOHO, которым вы хотите управлять, имеет статический IP адрес, то вы можете остановиться здесь. Нажмите **Submit** для того чтобы сохранить конфигурацию. Теперь вы можете добавить устройство на Сервер Управления. После того, как вы добавите устройство SOHO на Сервер Управления, Сервер Управления автоматически подключится к статическому IP адресу и настроит SOHO, как управляемый клиент. Если SOHO имеет динамический IP адрес, то вы можете продолжить с п. 7.*

8. Включите опцию **Enable Managed VPN**

9. Из выпадающего списка **Configuration Mode** выберите **SOHO**.

10. В поле **DVCP Server Address** введите IP-адрес Сервера Управления, если у него есть публичный IP-адрес. Введите публичный IP-адрес Сервера Управления. Если у Сервера Управления внутренний IP-адрес, введите публичный IP-адрес Firebox, который защищает Сервер Управления. Firebox, который защищает Сервер Управления, автоматически защищает все порты, используемые Сервером Управления, и будет переадресовывать все подключения на эти порты настроенного Сервера Управления. Для этого нет необходимости в специальной конфигурации.

11. В поле **Client Name** введите имя клиента для вашего Firebox SOHO. Это имя чувствительно к регистру и должно совпадать с именем, которое вы ввели для Edge при его добавлении к конфигурации Сервера Управления.

12. В поле **Shared Key** введите ключ. Этот ключ используется для шифрования соединения между Сервером Управления и SOHO. Этот ключ должен быть одним и тем же на SOHO и Сервере Управления. Вам необходимо получить ключ от администратора Сервера Управления.

13. Нажмите **Submit**. После того, как вы сохраните конфигурацию на SOHO, Edge будет работать как управляемый клиент. Управляемый клиент Firebox пытается подключиться к IP-адресу Сервера Управления. Соединения управления между Сервером Управления и управляемым клиентов разрешены. Теперь вы можете добавить устройство к конфигурации вашего Сервера Управления, как описано “Добавление управляемых устройств на Сервер Управления”

Запуск WatchGuard System Manager tools

В закладке **Device Management** вы можете запустить утилиты для конфигурации и мониторинга устройств. Для устройств Firebox вы можете запустить:

- Quick Setup Wizard
- CA Manager
- LogViewer
- Report Manager

Для устройств Firebox и WFS вы можете запустить:

- Policy Manager
- Firebox System Manager
- HostWatch
- Ping
- Expire Lease

Для устройств Edge вы можете запустить:

- Policy Manager (Edge versions 11.x and later)
- Edge Web Manager (Edge versions before 11.0)
- Firebox System Manager
- HostWatch
- Ping

Для того чтобы запустить утилиты WatchGuard System Manager выполните следующее:

1. Выберите закладку **Device Management**.

2. Откройте список **Devices**.

3. Выберите устройство, за состоянием которого вы хотите следить, или которое вы хотите настроить.
   Откроется страница Device Management.

4. В секции **Tools** выберите утилиту, которую вы хотите запустить.
   Запустится выбранная утилита.

Если вы выберете **Expire Lease**, то срок действия управляемого клиента на Сервера Управления автоматически истекает и он загружает последние обновления конфигурации. При этом никакого диалогового окна для подтверждения не появляется

Если вы подключены с Серверу Управления под учетной записью пользователя с правами администратора, то при запуске WSM вам не надо вводить пароли состояния или конфигурации

Настройка параметров сети (только для устройств Edge версии v10.x и ниже)

При помощи Сервера Управления вы можете настроить уникальные параметры сети для устройств Firebox X Edge (версии 10.x и ниже). Процедура загружает текущие настройки сети и включает для устройства режим Fully Managed Mode.

Все параметры сети устройств Firebox X Edge можно настроить при помощи утилиты Edge Web Manager.

В WatchGuard System Manager выполните следующее:

1. Выберите закладку **Device Management**.

2. Откройте список **Devices**

3. Выберите устройство Firebox X Edge.
   Откроется страница Device Management.

4. В секции **Network Settings** нажмите **Configure**.
   Откроется диалоговое окно Network Settings.

5. Выполните все необходимые настройки параметров сети.

6. Нажмите **OK**.

Секция Configuration Template

*Страница управления для устройств SOHO 6 не содержит секцию **Policy***

В этой секции отображаются шаблоны конфигурации устройства, к которым подключено устройство Firebox X Edge. Если устройство не подключено к шаблону, то вы можете сделать это, просто перетащив устройство на соответствующий шаблон конфигурации устройств. Также для того чтобы подключить устройство к шаблону конфигурации вы можете нажать **Configure**

Для более подробной информации о шаблонах конфигурации устройств см. “Создание шаблонов конфигурации и подключение к Шаблонам Конфигурации Устройства (Device Configuration Templates)”

Обновление или перезагрузка устройства, или удаление устройства с Сервера Управления

На странице Device вашего управляемого устройства, вы можете изменить параметры сервера и клиента, обновить IPSec сертификаты и сертификаты ЦС, или перезагрузить устройствоFirebox. Вы также можете удалить устройство с Сервера Управления.

Обновление устройства

На странице **Device Management** выполните следующее:

1. Откройте список **Devices**.

2. Выберите устройство, которое вы хотите обновить.
   Откроется страница Device Management для этого устройства.

3. В секции **Device Information** нажмите **Update Device**.
   Откроется диалоговое окно Update Device

4. Для того чтобы загрузить политики управляемого устройства на Сервер Управления для trusted и optional сетей включите опцию **Download Trusted and Optional Network Policies**. Мы рекомендуем вам это сделать для того чтобы при работе с устройством к вас были самые последние политики.

5. Для того чтобы обновить конфигурацию Сервера Управления на устройстве после обновления (IP адрес Сервера Управления, имя хоста, ключ шифрования и lease time), включите опцию **Reset Server Configuration**. Если вы изменили какие-нибудь параметры устройства, то проверьте, что эта опция включена.

6. Для того чтобы закончить срок действия управляемого клиента на Сервере Управления и загрузить на него последние обновления конфигурации включите опцию **Expire Lease**

7. (Отсутствует для устройств Edge версии ниже 11.0) Для того чтобы сгенерировать или повторно сгенерировать сертификат IPSec для Firebox и сертификат ЦС, включите опцию **Issue/Reissue Firebox's IPSec Certificate and CA's Certificate**.

8. Нажмите **OK**.

Перезагрузка устройства

На странице **Device Management** выполните следующее:

1. Откройте список **Devices**.

2. Выберите устройство, которое вы хотите перезагрузить.
   Для выбранного устройства откроется страница Device Management.

3. В секции **Device Information** нажмите **Reboot**.
   Появится сообщение подтверждения.

4. Нажмите **Yes**.

Удаление устройства с Сервера Управления

Для того чтобы удалить устройство с Сервера Управления выполните следующее:

1. Откройте список **Devices**.

2. Выберите устройство, которое вы хотите удалить.

3. Нажмите правой кнопкой на устройство и нажмите **Remove**. Или выберите **Edit > Remove**.
   Появится сообщение подтверждения.

4. Нажмите **Yes**.

5. Откройте Policy Manager для этого устройства.

6. Выберите **VPN > Managed Client**, и отключите опцию **Enable this Firebox as a Managed Client**.

7. Сохраните конфигурационный файл.

Создание шаблонов конфигурации и подключение к Шаблонам Конфигурации Устройства (Device Configuration Templates)

Шаблон Конфигурации Устройства (Device Configuration Template) – это набор параметров, который может быть использован несколькими устройствами. Для устройств Firebox вы можете на Сервере Управления создать Шаблоны Конфигурации устройства.

Затем вы можете подключить ваши устройства к этим шаблонам. При этом все политики и настройки шаблона конфигурации добавляются в конфигурационный файл отдельного устройства. Вы можете посмотреть эти политики и настройки в конфигурационном файле этого устройства, однако их изменить вы можете только в шаблоне конфигурации устройства.

Если вы создали политику в отдельном конфигурационном файле для вашего устройства, и подключите это устройство к шаблону конфигурации, в котором есть политика с таким же именем, обе политики будут добавлены в конфигурационный файл. Политики с одинаковыми именами не будут друг друга перезаписывать.

Убедитесь, политики с одинаковыми именами не используют параметры, которые могут конфликтовать друг с другом. Мы рекомендуем вам удалить все политики и параметры из вашего конфигурационного файла, имена которых совпадают с именами политик и параметров в шаблонах конфигурации, к которому подключено ваше устройство.

Вы можете использовать шаблоны конфигурации для настройки стандартных фильтров брандмауэра, изменения списка Blocked Sites, изменения конфигурации WebBlocker, настройки параметров журнала или изменить другие параметры политики для одного или несколько управляемых устройств Firebox.

Шаблоны Конфигурации имеют следующие ограничения:

- Шаблоны конфигурации Edge могут использоваться только для устройств Firebox X Edge.

- Каждое устройство можно подключить к одному шаблону конфигурации.
- Для работы с шаблоном конфигурации на устройстве Edge должно быть установлено программно-аппаратное обеспечение версии 7.5 или выше.
- Для устройств Edge с различными версиями ОС 7.5, 8.0, 8.5, 8.6 или 10.x вам необходимо использовать различные шаблоны конфигурации.

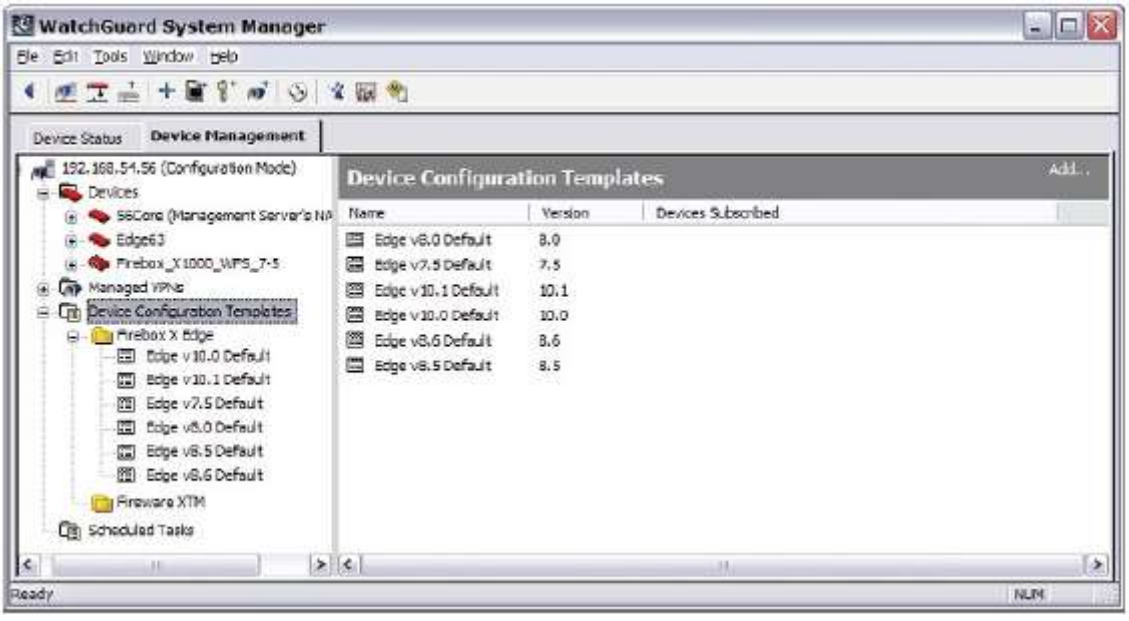
Доступные шаблоны конфигурации включают:

- Firebox X Edge — версии 7.5, 8.x, 10.x
- Fireware XTM — Firebox X Edge e-Series, Core e-Series, Peak e-Series и XTM 1050 версии 11.x

Для всех устройств версии v11.x вы можете использовать один шаблон конфигурации Fireware XTM

Вы можете вносить изменения в шаблон конфигурации устройства, или напрямую в конфигурацию устройств, подключенных к этому шаблону. После того, как вы внесете какие-либо изменения в настройки шаблона конфигурации, Сервер Управления автоматически обновит все устройства, подключенные к этому шаблону.

1. Откройте WatchGuard System Manager и подключитесь к Серверу Управления.
2. Выберите закладку **Device Management**.
   Откроется страница Management Server.
3. Выберите **Device Configuration Templates** в панели навигации слева.
   Откроется страница Device Configuration Templates со списком доступных шаблонов конфигурации



4. Откройте список **Device Configuration Templates** для того чтобы посмотреть список доступных шаблонов. Список **Device Configuration Templates** по умолчанию включает только Шаблоны конфигурации устройств Edge версии 10.1 или ниже. Вы можете добавить шаблоны конфигурации для других устройств Firebox.
5. Нажмите правой кнопкой на **Device Configuration Templates** и выберите **Insert Device Configuration Template**. Или нажмите **Add** в верхней правой части страницы **Device Configuration Templates**.
   Откроется диалоговое окно Product Version.

6. Выберите продукт и версию в выпадающем списке. Нажмите **OK**.
   Если вы выбрали устройство Edge, то откроется окно Edge Configuration: Edge Template.
   Если вы выбрали устройство Fireware XTM, вы сначала выбираете имя шаблона, и затем Fireware XTM Policy Manager откроет пустой конфигурационный файл.

7. Выполните все необходимые инструкции для настройки шаблона конфигурации для выбранного устройства.

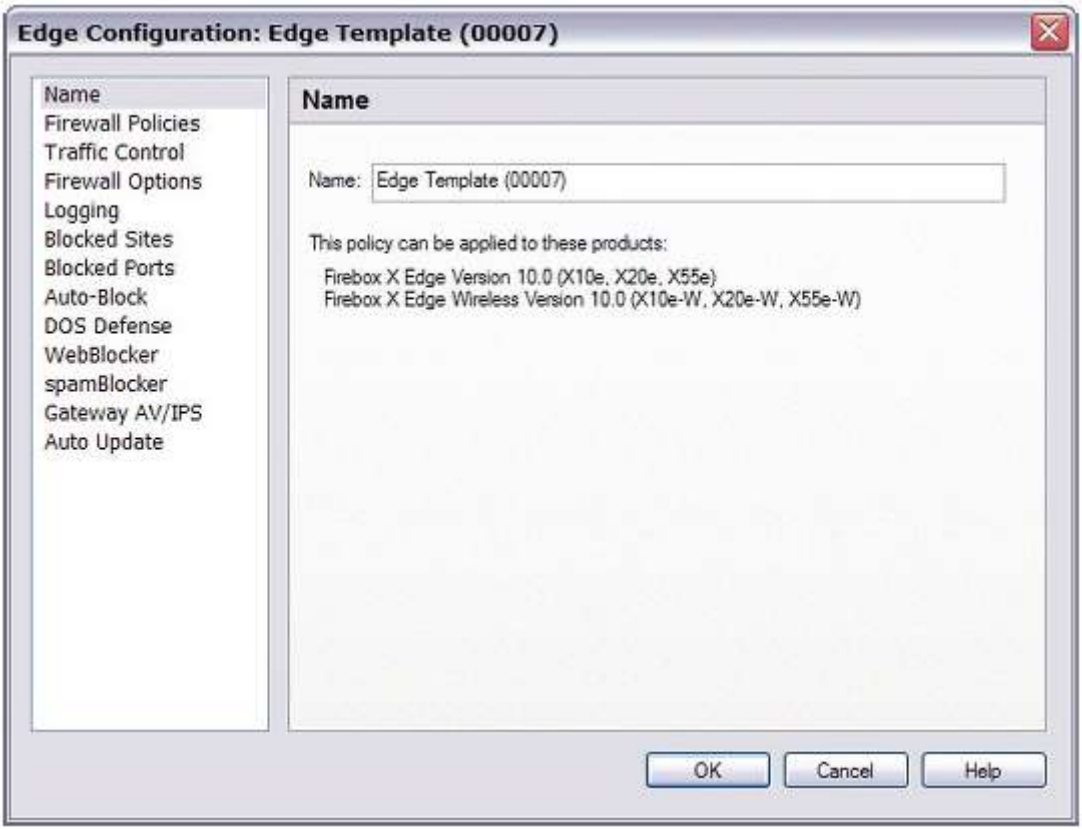
Настройка шаблона для управляемого устройства Edge

В диалоговом окне **Edge Configuration: Edge Template** вы можете настроить параметры вашего шаблона конфигурации Edge

Шаблон будет сохранен на Сервер Управления и обновление отправляется на все устройства Firebox X Edge, подключенные к этому шаблону. Если вы хотите использовать Edge Web Manager для прямого подключения к вашему Edge устройству (вместо ссылки Edge Web Manager в WSM), вам необходимо добавить политику HTTPS в шаблон конфигурации Edge. Эта политика HTTPS должна разрешать трафик с External на Alias, on the Edge over TCP port 443.

Для того чтобы настроить шаблон для устройства Edge выполните следующее:

1. Введите имя шаблона



2. Для того чтобы настроить шаблон, выберите категорию из списка и для нее введите необходимую информацию.
   Список категорий зависит от версии выбранного устройства Edge.

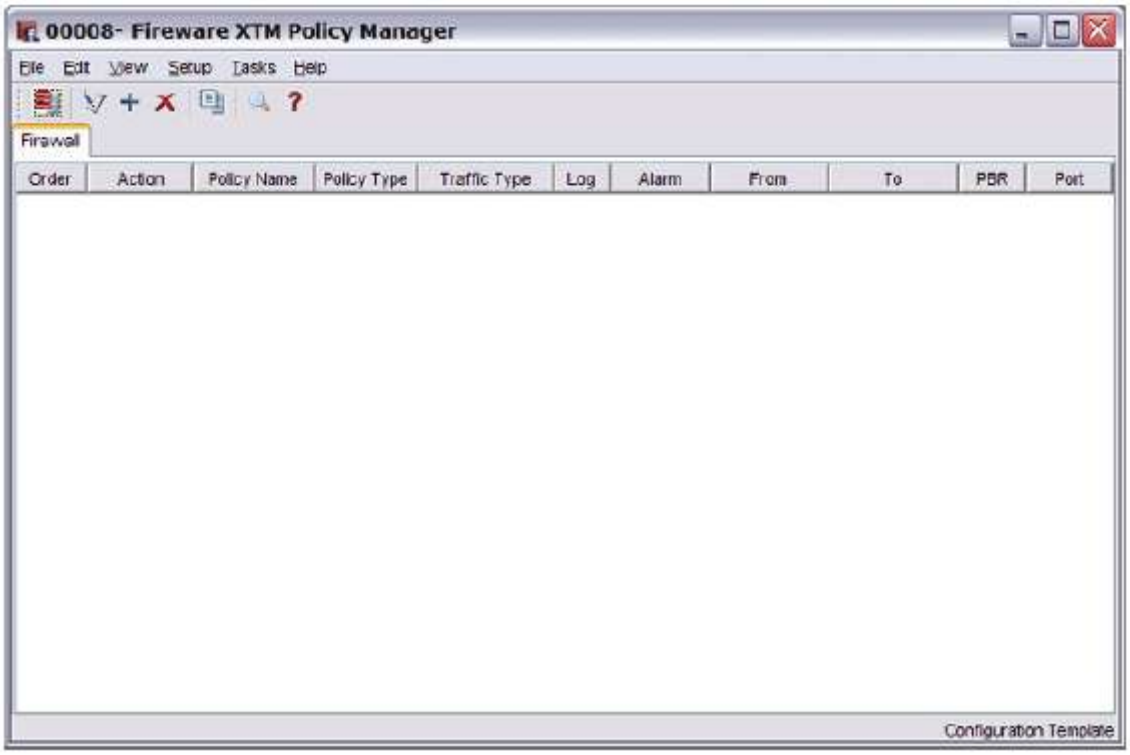
   Для более подробной информации о доступных категориях см. *Help* or *User Guide*.

   Для более подробной информации о том, как добавить политики брандмауэра к шаблону, см. “Добавление предопределенной политики в шаблон конфигурации устройства Edge” или “Добавление политики пользователя к шаблону конфигурации устройства Edge”

3. Нажмите **OK** для того чтобы закрыть диалоговое окно **Edge Configuration: Edge Template**.

Настройка шаблонов конфигурации для других устройств Firebox XTM

Если вы хотите создать шаблон конфигурации для других устройств Firebox XTM (не Edge), то вам необходимо использовать Policy Manager. Это модернизированная версия Policy Manager, при помощи которой вы можете создавать шаблоны конфигурации.



При настройке шаблона вы можете:

- Создавать, изменять или удалять политики
- Настраивать Псевдонимы и параметры журнала
- Настраивать действия прокси, Application Blockers и расписания
- Настраивать spamBlocker, Gateway AntiVirus, Intrusion Prevention, WebBlocker и Сервер Карантина

Для того чтобы настроить новый шаблон для вашего Firebox, в Policy Manager вам необходимо выполнить следующее:

1. Нажмите + в панели инструментов Policy Manager. Или выберите **Edit** > **Add Policy**.
   Откроется диалоговое окно Add Policies.
2. Два раза нажмите на каталог для выбранного типа политики.
   Откроется список выбранных политик.
3. Выберите политику.
4. Нажмите **Add**.
   Откроется диалоговое окно New Policy Properties.
5. Выполните необходимые настройки политики
6. Для того чтобы добавить несколько политики повторите п. 3–5.

7. Нажмите  для того чтобы сохранить конфигурацию на Сервер Управления. Или выберите **File** > **Save** > **To Management Server**.
Запустится мастер Schedule Template Update.

8. Click **Next** to start the wizard.
*Откроется страница **Select the Time and Date**.*

9. Выберите **Update the template immediately (Обновить шаблон прямо сейчас)** или **Schedule template update (Обновить шаблон по расписанию)**.

10. Если вы выберете **Schedule template update**, то в полях **Date** и **Time** введите дату и время, когда вы хотите запустить процедуру обновления.

11. Нажмите **Next**.
Откроется страница Schedule Template Update Wizard is complete

12. Нажмите **Finish** для того чтобы завершить мастер.
Если конфигурация вашего Сервера Управления требует того, чтобы вы добавили комментарий при сохранении конфигурации, то откроется диалоговое окно Save Comment.

13. Если откроется диалоговое окно **Save Comment,** то в нем введите комментарий.

14. Нажмите **OK**.
Новый шаблон появится в списке Device Configuration Templates.

Для того чтобы изменить политику в шаблоне конфигурации выполните следующее:

1. Откройте ваш шаблон конфигурации в Policy Manager.

2. Выберите политику, которую вы хотите изменить

3. Нажмите  в панели инструментов Policy Manager. Или выберите **Edit** > **Modify Policy**.
Откроется диалоговое окно Edit Policy Properties.

4. Выполните необходимые настройки политики

5. Нажмите  для того чтобы сохранить конфигурацию на Сервере Управления. Или выберите **File** > **Save** > **To Management Server**.
Запустится мастер Schedule Template Update.

6. Нажмите **Next** для того чтобы запустить мастер.
Откроется страница Select the Time and Date.

7. Выберите **Update the template immediately или Schedule template update**.

8. Если вы выбрали **Schedule template update** выберите дату и время, когда вы хотите запустить процедуру обновления.

9. Нажмите **Next**.
Откроется страница Schedule Template Update Wizard is complete.

10. Нажмите **Finish** для того чтобы завершить работу мастера.

    Если конфигурация вашего Сервера Управления требует того, чтобы вы добавили комментарий при сохранении конфигурации, то откроется диалоговое окно Save Comment.

11. Если откроется диалоговое окно **Save Comment,** то в нем введите комментарий.

12. Нажмите **OK**.
Новый шаблон появится в списке Device Configuration Templates.

Добавление предопределенной политики в шаблон конфигурации устройства Edge

Вы можете использовать мастер WatchGuard System Manager Add Policy для того чтобы добавить предопределенную политику в шаблон конфигурации устройства Firebox X Edge.

1. В закладке **Device Management** выберите **Device Configuration Templates**.
Откроется страница Device Configuration Templates.

2. Нажмите правой кнопкой на **Device Configuration Templates** и выберите **Insert Device Configuration Template**. *И*ли нажмите **Add** в верхней правой части страницы.
Откроется диалоговое окно Product Version.

3. В выпадающем списке выберите устройство Edge. Нажмите **OK**.
Откроется диалоговое окно Edge Configuration: Edge Template.

4. В панели навигации слева выберите **Firewall Policies**.
Откроется страница Firewall Policies.

5. Нажмите **Add**.
Запустится мастер Add Policy Wizard.

6. Нажмите **Next**.
Откроется страница Select a service for this policy

7. Выберите **Choose a predefined service from this list** и выберите политику из списка.

8. Нажмите **Next**.
Откроется страница Select the traffic direction.

9. Выберите направление трафика — **Outgoing**, **Incoming** или **Optional**.

10. Нажмите **Next**.
Откроется страница Configure the network resources.

11. В выпадающем списке **Filter** выберите **Deny (Заблокировать)** или **Allow (Разрешить)**.

12. В полях **From** и **To** укажите адрес источника и назначения. Для того чтобы добавить новый ресурс нажмите **Add** под элементами **From** или **To.** Затем добавьте необходимую информацию.

13. Нажмите **Next**.
Откроется страница Add Policy Wizard is complete.

14. Нажмите **Finish** для того чтобы завершить работу мастера.

Добавление политики пользователя к шаблону конфигурации устройства Edge

При помощи мастера Add Policy Wizard вы можете создать политику пользователя в шаблоне конфигурации устройства для Firebox X Edge.

1. В закладке **Device Management** выберите **Device Configuration Templates**.
Откроется страница Device Configuration Templates.

2. Нажмите правой кнопкой на **Device Configuration Templates** и выберите **Insert Device Configuration Template**. Или нажмите **Add** в верхней правой части страницы.
Откроется диалоговое окно Product Version.

3. Выберите устройство Edge и версию в выпадающем списке. Нажмите **OK**.
Откроется диалоговое окно Edge Configuration: Edge Template.

4. В панели навигации выберите **Firewall Policies**.
Откроется страница Firewall Policies.

5. Нажмите **Add**.
Запустится мастер Add Policy Wizard.

6. Нажмите **Next**.
Откроется страница Select a service for this policy

7. Выберите **Create and use a new custom service**.

8. Нажмите **Next**.
   Откроется страница Specify Protocols

9. Введите имя протокола

10. Для того чтобы добавить протокол нажмите **Add**.
    Откроется диалоговое окно Add protocol

11. В выпадающем списке **Type** выберите будет ли протокол использовать один порт - **Single Port,** или диапазон портов - **Port Range**.

12. В выпадающем списке **Protocol** выберите протокол, который будет фильтроваться — **TCP**, **UDP**, or **IP**.

13. В поле **Server Port** введите номер порта или номера портов сервера, или в поле **IP Protocol** введите номер протокола.

14. Нажмите **OK** для того чтобы добавить протокол.

15. Повторите п. 10–14 для того чтобы добавить другой протокол.

16. Нажмите **Next** после того, как вы добавите все протоколы.
    Откроется страница Select the traffic direction.

17. Выберите направление трафика — **Outgoing**, **Incoming**, or **Optional**.

18. Нажмите **Next**.
    Откроется страница Configure the network resources.

19. В выпадающем списке **Filter** выберите **Deny (Заблокировать)** или **Allow (Разрешить)**

20. В полях **From** и **To** введите адрес источника и назначения. Для того чтобы добавить новый ресурс нажмите **Add** под полями **From** или **To** и введите всю необходимую информацию.

21. Нажмите **Next**.
    Откроется страница Add Policy Wizard is complete.

22. Нажмите **Finish** для того чтобы завершить работу мастера.

Клонирование шаблона конфигурации устройства

Если у вас есть несколько устройств с похожими конфигурациями, вы можете клонировать (копировать) шаблон и затем внести необходимые изменения в шаблон для каждого устройства. Это позволяет вам создать один Шаблон конфигурации, создать копию для каждого устройства и внести необходимые изменения в каждый экземпляр шаблона. Вы не можете редактировать шаблон по умолчанию. Вы можете сделать копию (клонировать) шаблон по умолчанию и затем для каждого устройства настроить свой шаблон. В закладке **Device Management** утилиты WatchGuard System Manager выполните следующее:

1. Откройте список **Device Configuration Templates**.

2. Нажмите правой кнопкой на шаблон конфигурации, который вы хотите клонировать, и выберите **Clone**.
   Копия шаблона появится в списке с тем же именем плюс «(Cloned)».

3. Откройте политику в Policy Manager и настройте ее для выбранного устройства

4. Сохраните изменения в вашем шаблоне конфигурации.

Изменение имени Шаблона Конфигурации

При создании шаблона конфигурации устройства вы указываете его имя, которое затем вы можете поменять.

1. В закладке **Device Management** откройте список **Device Configuration Templates**.
   Откроется список шаблонов конфигурации.

2. Откройте каталог для типа шаблона конфигурации, имя которого вы хотите изменить.

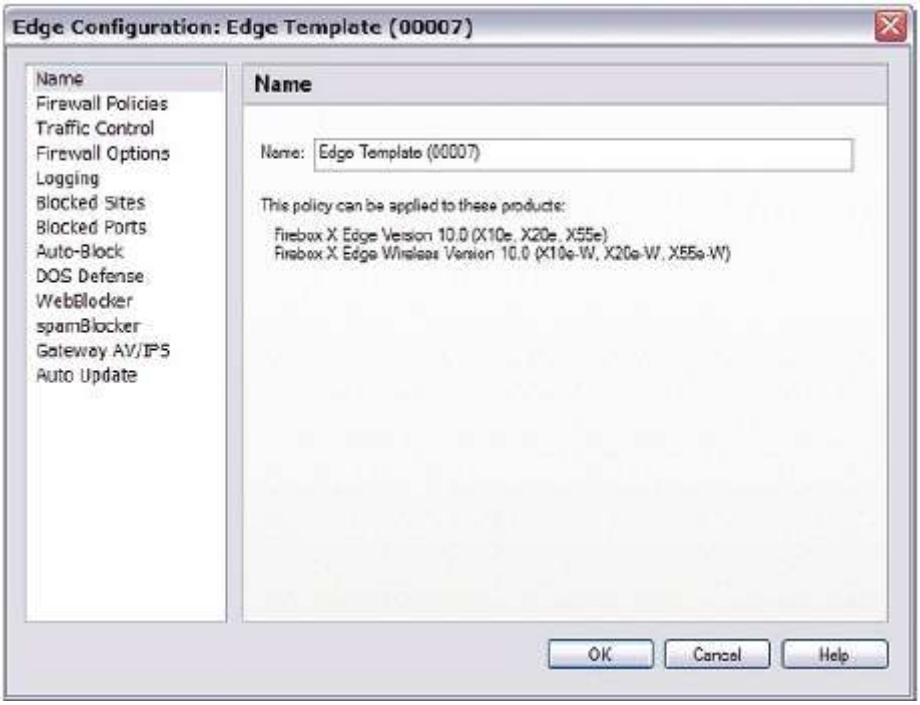
3. Выберите шаблон, имя которого вы хотите изменить.

4. Выполните все необходимые инструкции.

Изменение имени шаблона Firebox X Edge

1. Нажмите правой кнопкой на шаблон и выберите **Properties**.
   Откроется диалоговое окно Edge Configuration.

2. В панели навигации слева выберите **Name**.
   Откроется страница Name



3. В поле **Name** введите новое имя для шаблона

4. Нажмите **OK**.
   Имя шаблона будет изменено.

Изменение имени шаблона Fireware XTM

1. Нажмите правой кнопкой на шаблон и выберите **Rename**.
   Откроется диалоговое окно Change Name.

2. В поле **Name** введите новое имя для шаблона

3. Нажмите **OK**.
   Имя шаблона будет изменено.

Подключение устройств к Шаблону Конфигурации Устройств

При помощи Шаблона конфигурации устройства вы можете создать набор политик и параметров, которые затем вы можете использовать для нескольких устройств Firebox. Вы можете подключить любое из управляемых устройств к соответствующему Шаблону Конфигурации. Одно устройство можно подключить только к одному шаблону. Для того чтобы подключить устройство к шаблону, вы можете просто перетащить шаблон на устройство или использовать страницу Device Configuration. Вы можете подключать устройства к шаблонам такого же типа. Например, если вы перетащите шаблон конфигурации устройств Edge на каталог **Devices**, к нему будут подключены только Edge устройства.

Подключение к шаблону при помощи Drag-and-drop

При помощи процедуры drag-and-drop вы можете подключить к шаблону конфигурации любое устройство Firebox, или сразу список устройств.

1. В закладке **Device Management** откройте список **Devices**

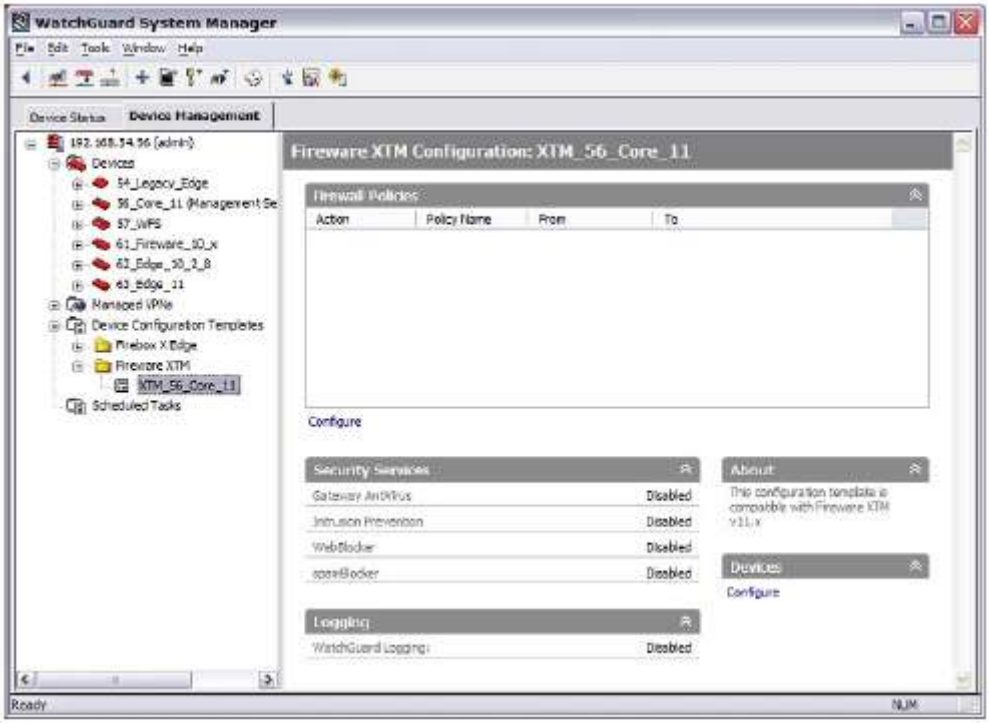
2. Выберите устройство и каталог с устройствами, которые вы хотите подключить к шаблону конфигурации, и перетащите выбранное устройство или выбранный каталог на шаблон конфигурации в списке **Device Configuration Templates**.
   Или перетащите выбранный шаблон конфигурации на устройство или каталог.

   Устройство будет подключено к шаблону.

Подключение устройства к шаблону в окне Manage Device List

В диалоговом окне **Manage Device List** вы можете подключить одно или несколько устройств к шаблону конфигурации.

1. В списке **Device Configuration Templates** выберите шаблон, к которому вы хотите подключить устройство.
   Появится шаблон выбранного устройства



2. Нажмите **Configure** в секции **Devices**
   Откроется список Manage Device List

3. Нажмите **Add**.
   Откроется диалоговое окно Select Devices

4. Отметьте флаг для каждого устройства, которое вы хотите подключить к шаблону конфигурации.

5. Нажмите **OK** для того чтобы закрыть диалоговое окно **Select Devices**

6. Нажмите **Close** для того чтобы закрыть диалоговое окно **Manage Device List**
Выбранные устройства будут подключены к шаблону конфигурации.

Псевдонимы и устройства Firebox

Псевдонимы используются для указания общего направления конфигурации политики на Сервере Управления. Например, при помощи псевдонимов вы можете создать шаблон конфигурации для сервера электронной почты, и создать политику, которая будет работать с этим сервером. Так как серверы электронной почты могут иметь различные IP адреса, вы можете создать псевдоним с именем *MailServer* на Сервере Управления.

При создании шаблона конфигурации для сервера электронной почты, вы можете использовать этот псевдоним в качестве адреса назначения. Затем вы можете создать псевдоним, в качестве адреса источника или назначения, который будет использовать для определенного направления передачи трафика, управляемого этой политикой

В этом примере вы можете настроить входящую политику ***SMTP Allow*** с псевдонимом *MailServer* в качестве адреса назначения.

Для корректной работы шаблона конфигурации на устройствах, на которых запущена эта политика, вам необходимо настроить псевдоним *MailServer* в настройках сети для каждого устройства Firebox X Edge.

Для того чтобы настроить псевдоним выполните следующее:

1. Измените имя псевдонима.

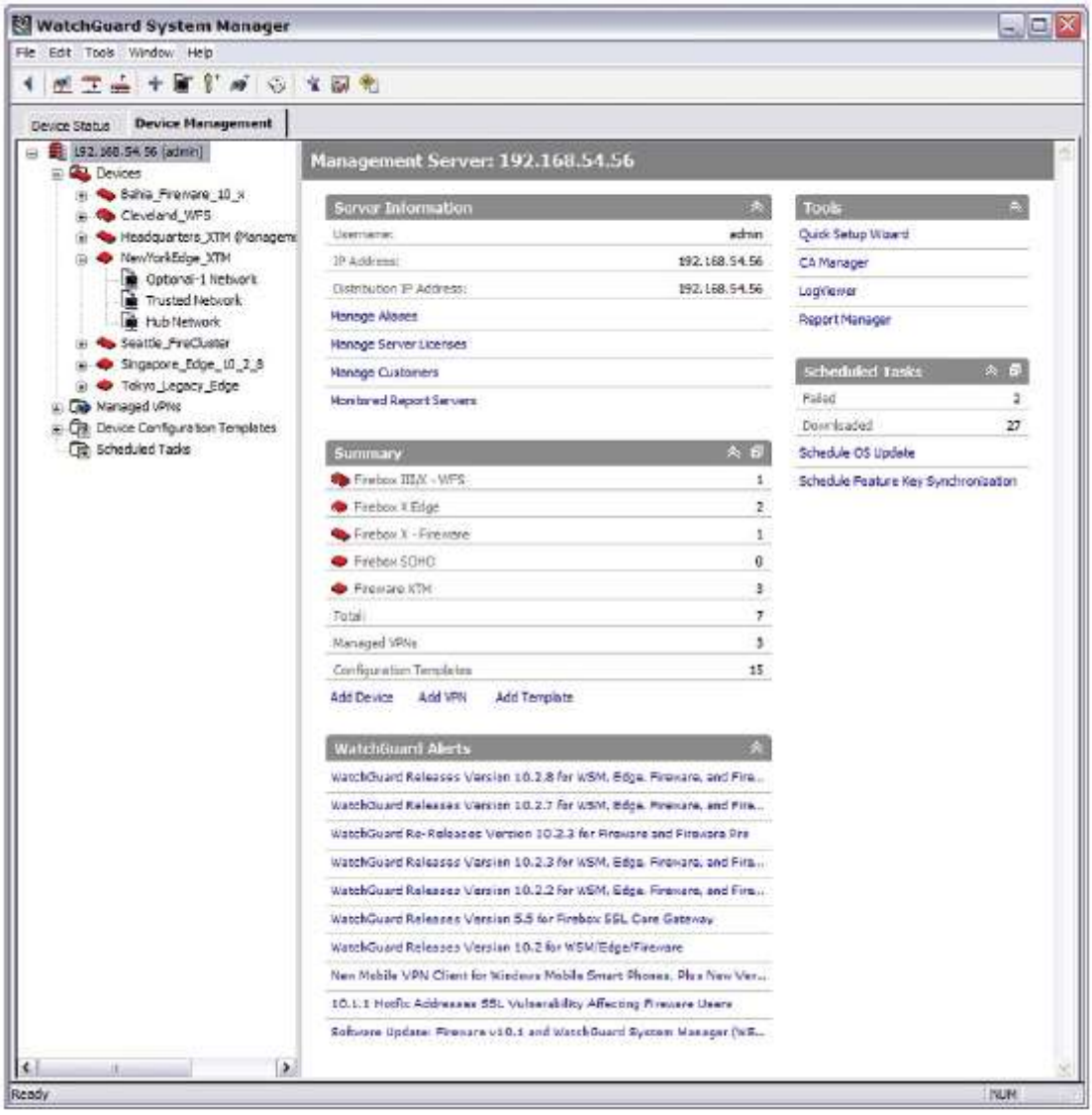
2. Создайте псевдонимы на устройстве Firebox.

Изменение имени псевдонима

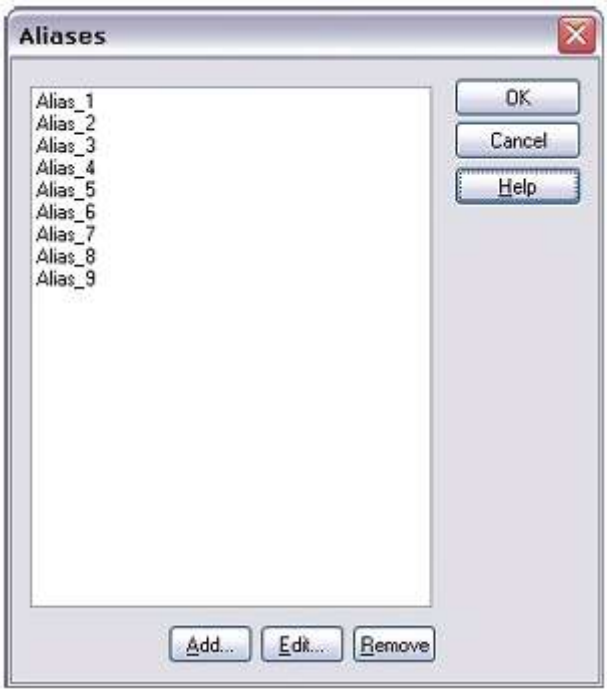
Сервер Управления содержит стандартный набор псевдонимов, которые вы можете использовать в ваших политиках. Вы можете создать новый псевдоним или изменить имя существующего псевдонима. Перед тем, как добавить псевдоним к политике, вам необходимо его создать на Сервере Управления.

В WatchGuard System Manager выберите закладку **Device Management**:

1. В панели навигации слева выберите Сервер Управления.
   Откроется страница Management Server settings



2. Нажмите  . Или в секции **Server Information** нажмите **Manage Aliases**.
   Откроется диалоговое окно Aliases



3. Для того чтобы добавить псевдоним нажмите **Add**.
   Откроется диалоговое окно Add Alias.

   Для того чтобы изменить существующий псевдоним, выберите его и нажмите **Edit**.
   Откроется диалоговое окно Edit Alias Name.

4. В поле **Name** введите имя псевдонима и нажмите **OK**.

5. Если вы хотите добавить еще несколько псевдонимов повторите п.3–4

6. Нажмите **OK**.

Затем вы можете присвоить псевдонимам IP адреса

Создание псевдонимов на устройстве Firebox

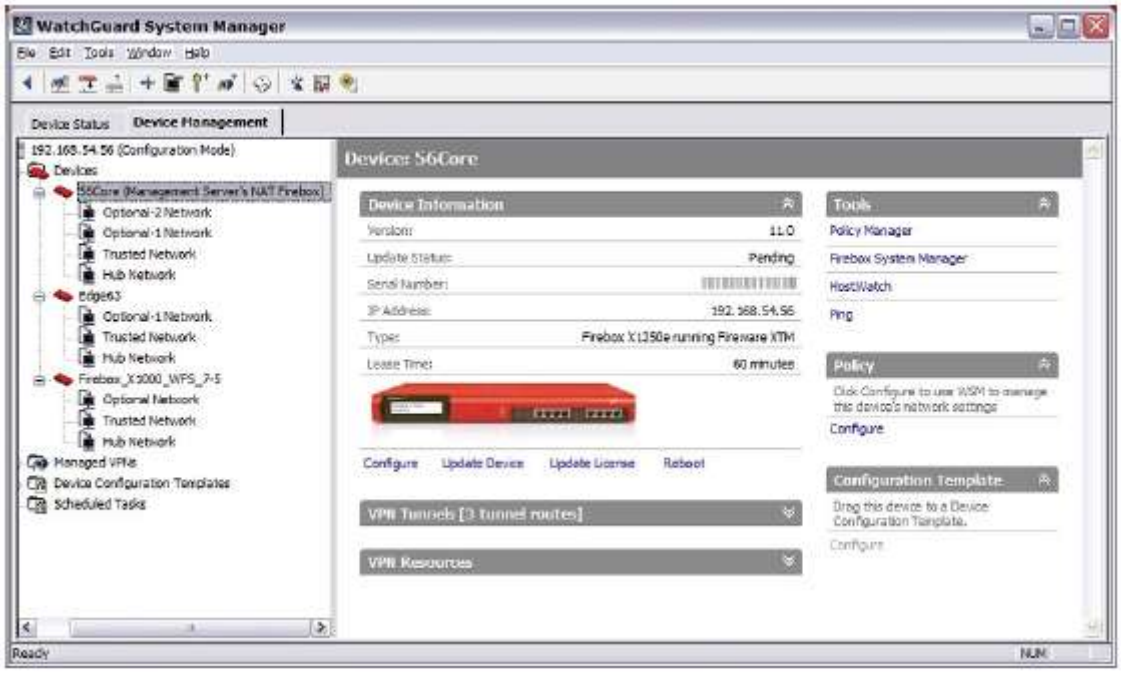
После того, как вы обновили список псевдонимов на вашем Сервере Управления, вы можете создать псевдонимы, которые будут использоваться с вашими устройствами Firebox X Edge. Процедура создания псевдонима зависит от тип и версии вашего устройства. Для более подробной информации см. следующие разделы.

Настройка псевдонима для устройства Fireware XTM Edge

При помощи этой процедуры вы можете создать псевдонимы для всех устройств Fireware XTM Edge. Для других устройств используйте процедуры, описание которых приведено в следующей главе.

В закладке **Device Management** утилиты WatchGuard System Manager выполните следующее:

1. Откройте список **Devices** и выберите устройство Fireware XTM
   Откроется страница Device settings



2. В секции **Policy** выберите **Configure**.
   Откроется Fireware XTM Policy Manager

3. Для более подробной информации о том, как добавить псевдоним в вашу конфигурацию см. “Создание псевдонима”

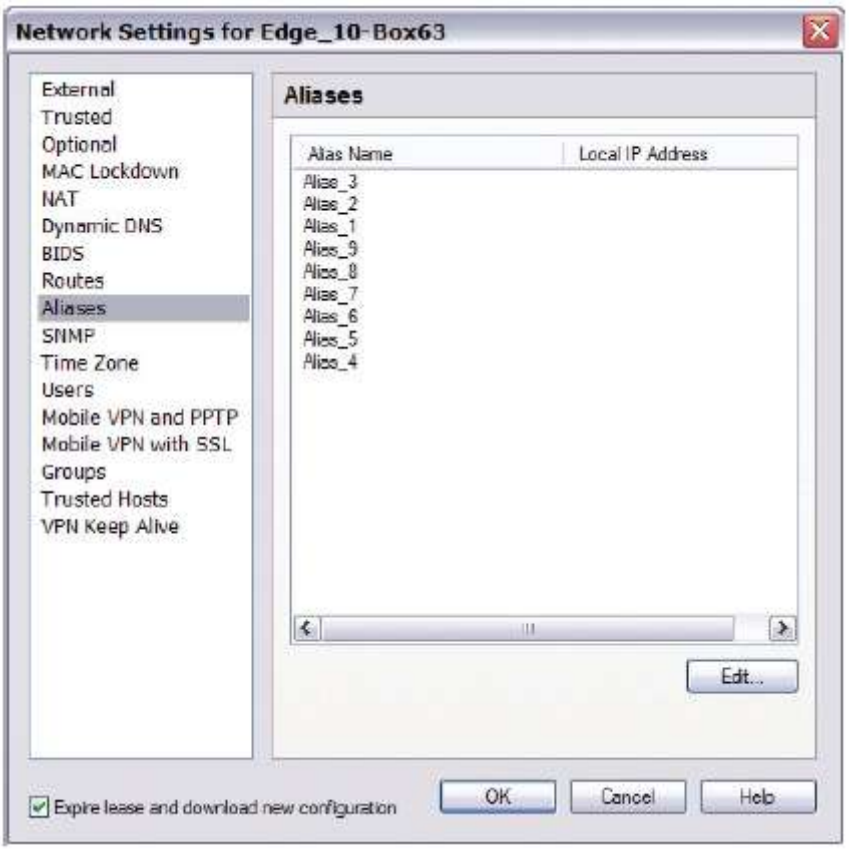
Настройка псевдонима для устройств Edge версии 10.x или ниже

В закладке **Device Management** утилиты WatchGuard System Manager выполните следующее:

1. Откройте список **Devices** и выберите устройство Fireware Edge
   Откроется страница Device settings

2. В секции **Network Settings** нажмите **Configure**.
   Откроется диалоговое окно Network Settings

3. Нажмите **Aliases**.
   Откроется список псевдонимов. Этот список включает псевдонимы, созданные на Сервере Управления, а также псевдонимы по умолчанию



4. Выберите псевдоним, который вы хотите настроить, и нажмите **Edit**.
   Откроется диалоговое окно Local Alias Setting

5. Введите IP адрес для локального псевдонима в сети данного устройства Firebox X Edge. Нажмите **OK**.

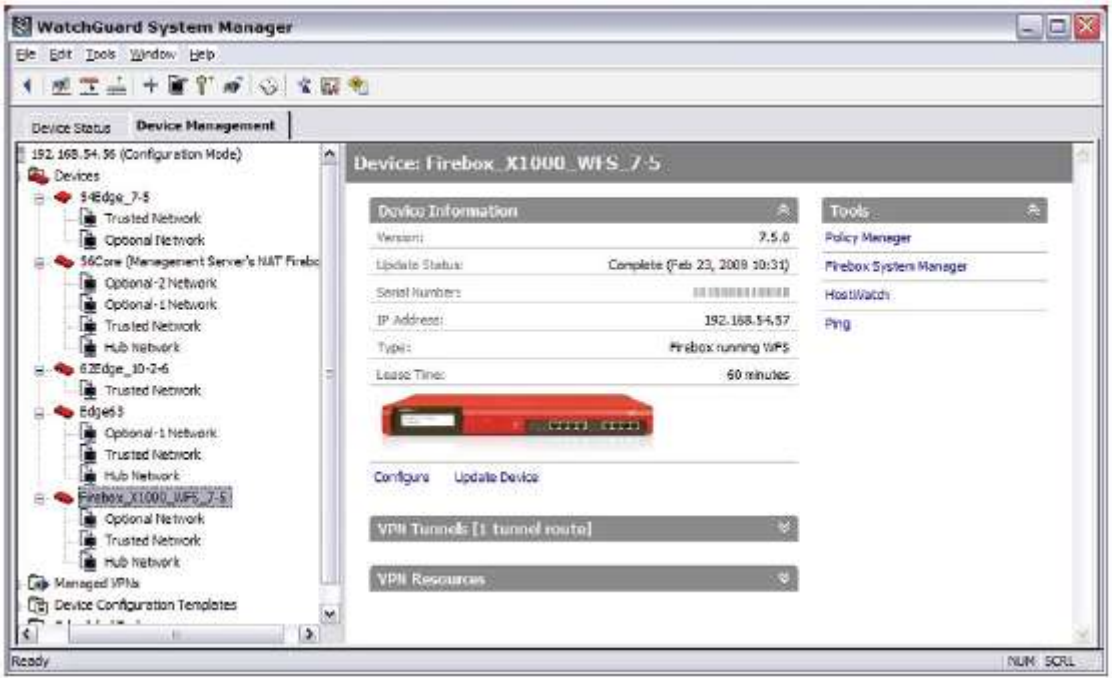
6. Повторите эту процедуру для всех псевдонимов.

7. Нажмите **OK**

Настройка псевдонима для устройства WFS Edge

В закладке **Device Management** утилиты WatchGuard System Manager выполните следующее:

- Откройте список **Devices** и выберите устройство WSF Edge
  Откроется страница Device settings



- В секции **Tools** нажмите **Policy Manager**.
  Откроется WFS Policy Manager.

Удаление устройства из режима Fully Managed

Вы можете переключить режим управления вашим устройством с Fully Managed на Basic Managed. После того, как вы это сделаете, ссылка на шаблон конфигурации будет удалена и все политики, определенные в шаблоне конфигурации, будут удалены из конфигурационного файла.

Если вы хотите удалить устройство с Сервера Управления см. “Удаление устройства с Сервера Управления”

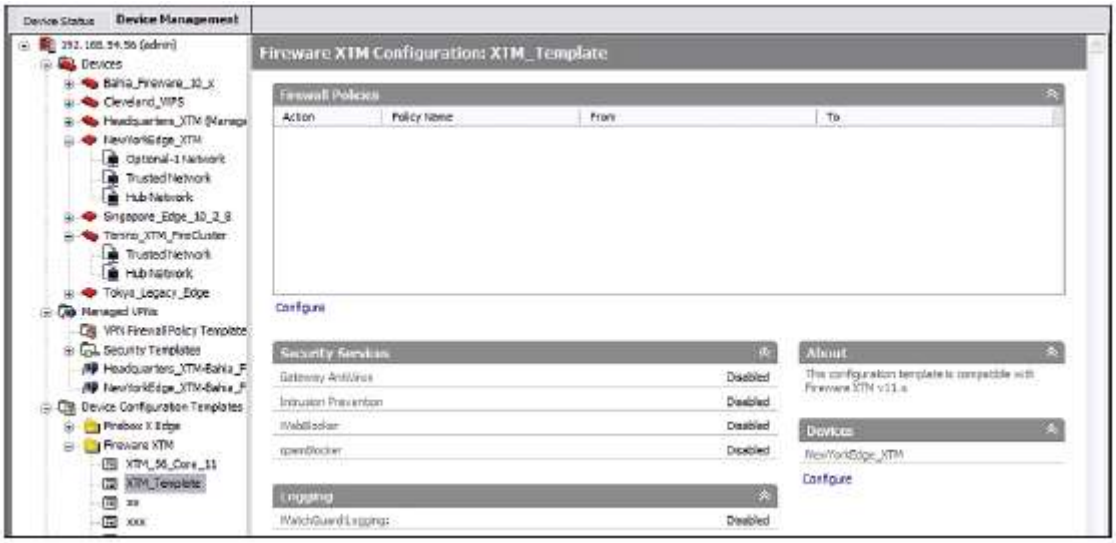
Существует два способа удаления устройства из режима Fully Managed. Вы можете просто изменить режим управления для устройства, или вы можете удалить устройство из списка Manage Devices List шаблона конфигурации, к которому устройство подключено.

Для более подробной информации о смене режима управления см. “Изменение режима Централизованного управления для вашего Firebox”

Для того чтобы удалить устройство из списка Manage Devices List:

1. Выберите закладку **Device Management**.
2. Откройте список **Device Configuration Templates** для вашего Сервера Управления.
3. Откройте каталог для типа шаблонов устройства: **Firebox X Edge** or **Fireware XTM**.

4. Из списка выберите шаблон, к которому подключено устройство.
Откроется страница конфигурации для выбранного шаблона



5. В секции **Devices** нажмите **Configure**
Откроется список Manage Device List.

6. Выберите устройство, которое вы хотите удалить из режима Fully Managed, и нажмите **Remove**.

7. Нажмите **Close**.
Устройство переключится в режим Basic Managed и все политики, созданные в шаблоне конфигурации, будут удалены из конфигурационного файла устройства.

8. Сохраните конфигурационный файл. До тех пор пока вы не сохраните изменения в конфигурационный файл, сделанные изменения не вступят в силу.

Глава 20 - Администрирование на базе ролей

Администрирование на базе ролей

Администрирование на базе ролей позволяет вам разделить административные функции (мониторинг, конфигурация) между несколькими пользователями. Один или несколько ведущих администраторов могут иметь полный доступ ко всем устройствам, в то же время менее опытные будут иметь ограниченные права доступа к устройствам.

Например, один администратор может полный доступ для конфигурации и мониторинга работы устройств Firebox в регионе Eastern и доступ только для мониторинга устройств в Central и Western регионах. Другой администратор может иметь полный доступ к устройствам Central региона и только права мониторинга устройств в Western и Eastern регионах region.

При помощи WatchGuard System Manager (WSM) и WatchGuard Server Center вы можете создать различные так называемые роли для администраторов в вашей организации. Все настройки администрирования на базе ролей хранятся на Сервере Управления, поэтому доступ к ним получить только через WSM или WatchGuard Server Center.

Если вы внесли какое-либо изменения в настройки ролей, эти изменения автоматически появятся на WatchGuard Server Center.

Роли и политики ролей

Роль состоит из двух частей: набор задач и набор устройств, на которых эти задачи можно выполнять. Каждому администратору присваивается одна или несколько ролей - Super Administrator, Mobile User VPN Administrator или User Authentication Administrator.

WatchGuard System Manager (WSM) содержит несколько предопределенных ролей, которые вы можете использовать. Вы также можете создавать свои собственные роли. Эти роли распознаются всеми утилитами WSM и серверами WatchGuard. Например, если вы подключитесь к WSM с правами записи/чтения и откроете Firebox System Manager (FSM), система не попросит вас ввести пароль конфигурации, так как FSM уже идентифицировал как пользователя с достаточными правами.

Политики ролей соединяют набор задач и устройств, на которых эти задачи можно выполнять.

Аудит

Для того чтобы следить за действиями каждого администратора, WSM хранит все изменения, которые произошли на устройстве. Эти изменения записываются в сообщения журнала Сервера Управления. WSM также ведет аудит всех изменений системы: администратор, который внес эти изменения и дату этого изменения

Предопределенные роли

Ваш Firebox содержит несколько предопределенных ролей. Вы также можете создать свои собственные роли

Ниже в таблице содержится список всех предопределенных ролей и разрешенных им действий.

Роль	Разрешенные действия
Super Administrator (Супер Администратор)	Создание пользователей, политик ролей, устройств, каталогов, шаблонов безопасности, VPN политик брандмауэра Имеет доступ к Центру Сертификации Создание отчетов и просмотр журналов аудита любого пользователя Создание отчета для любого устройства
Management Server Administrator (Администратор Сервера Управления)	Создание устройств, каталогов, шаблонов безопасности, VPN политик брандмауэра и информации о клиентах Имеет доступ к Центру Сертификации Создание отчетов и просмотр журналов аудита любого пользователя Создание отчета для любого устройства
Device Administrator (Администратор Устройства)	Просмотр и перемещение каталогов и устройств в WSM Просмотр/изменение каталогов и параметров управления устройствами Просмотр журналов устройств Создание отчета для любого устройства Создание паролей устройств
Network Administrator (Администратор Сети)	Просмотр каталогов и устройств в WSM Просмотр журналов устройств Просмотр/создание отчетов устройств Настройка сети, к которой подключены устройства
Security Administrator (Администратор по вопросам безопасности)	Просмотр каталогов и устройств в WSM Просмотр журналов устройств Просмотр/создание отчетов устройств Настройка сети, политик и параметров QoS Обновление сигнатур Gateway AV / IPS

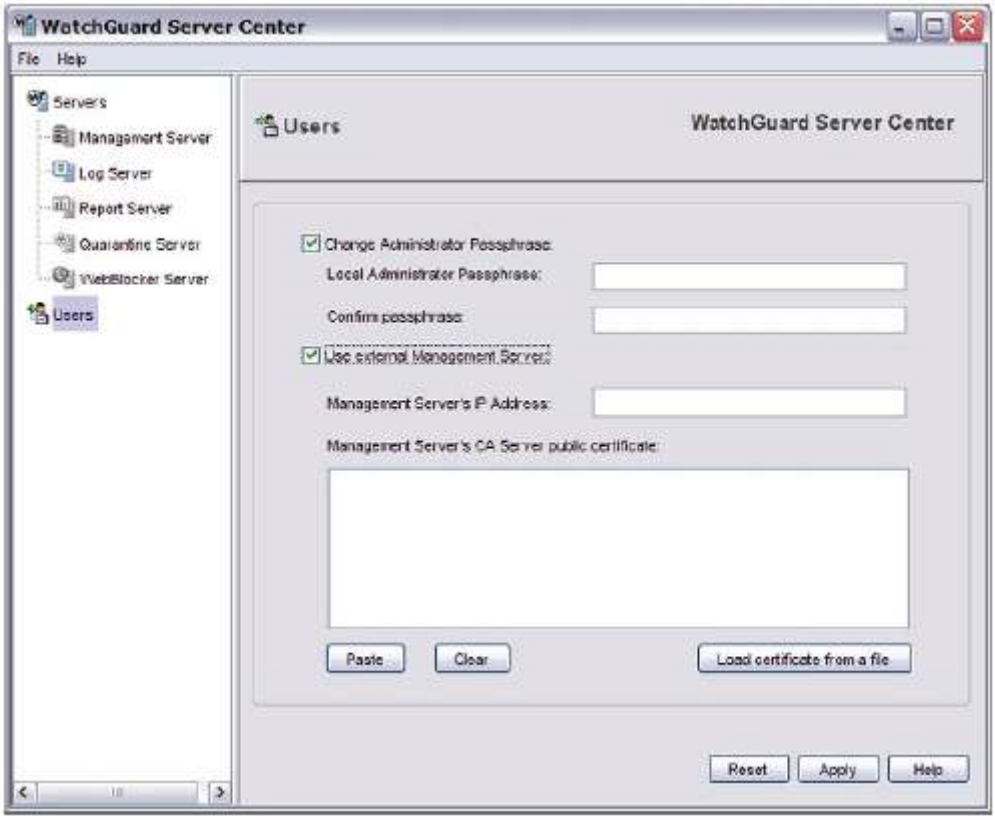
Branch Office VPN Administrator (Администратор BOVPN туннелей)	Просмотр каталогов и устройств в WSM Просмотр журналов устройств Просмотр/создание отчетов устройств Настройка сети, политик и BOVPN туннелей Запуск процедуры повторной генераций ключей для туннеля
Mobile User VPN Administrator (Администратор MUVPN туннелей)	Просмотр каталогов и устройств в WSM Просмотр журналов устройств Просмотр/создание отчетов устройств Настройка сети и MUVPN туннелей Отключение активных туннелей Создание пользователей и групп Повторная генерация ключей для BOVPN туннелей
User Authentication Administrator (Администратор Аутентификации пользователя)	Просмотр каталогов и устройств в WSM Просмотр журналов устройств Просмотр/создание отчетов устройств Настройка внешней аутентификации Создание пользователей и групп
User Services Administrator (Администратор по Сервисам Пользователя)	Просмотр каталогов и устройств в WSM Просмотр журналов устройств Просмотр/создание отчетов устройств Настройка параметров WebBlocker, spamBlocker и Сервера Карантина для устройства
Device Monitor Administrator (Администратор мониторинга работы устройства)	Просмотр каталогов и устройств в WSM Просмотр журналов и отчетов устройств Просмотр конфигурационного файла для устройства

Администрирование на базе ролей и внешний Сервер Управления

Если ваш Сервер Журналов WatchGuard или Сервер Отчетов установлены не на том же компьютере, что и Сервер Управления, вы можете использовать WatchGuard Server Center для настройки данных Сервера Управления, который вы хотите использовать для администрирования на базе ролей. После того, как вы настроите все необходимые данные, Сервер Журналов или Сервер Отчетов могут подключиться к выбранному Серверу Управления для получения информации о ролях удаленных пользователей.

Для того чтобы настроить параметры для внешнего Сервера Управления выполните следующее:

1. В левой навигационной панели выберите **Users**.
   Откроется страница Users



2. Для того чтобы сменить пароль локального администратора включите опцию **Change Administrator Passphrase**.

3. Введите и подтвердите новый пароль для локального администратора.

4. Включите опцию Use **external Management Server**.

5. В поле **Management Server's IP address** введите IP адрес внешнего Сервера Управления.

6. В поле **Management Server's CA Server public certificate** вставьте содержимое сертификата Сервера Управления. Или нажмите **Load certificate from a file to select and upload the certificate**.

7. Нажмите **Apply**.

Создание и удаление пользователей или групп

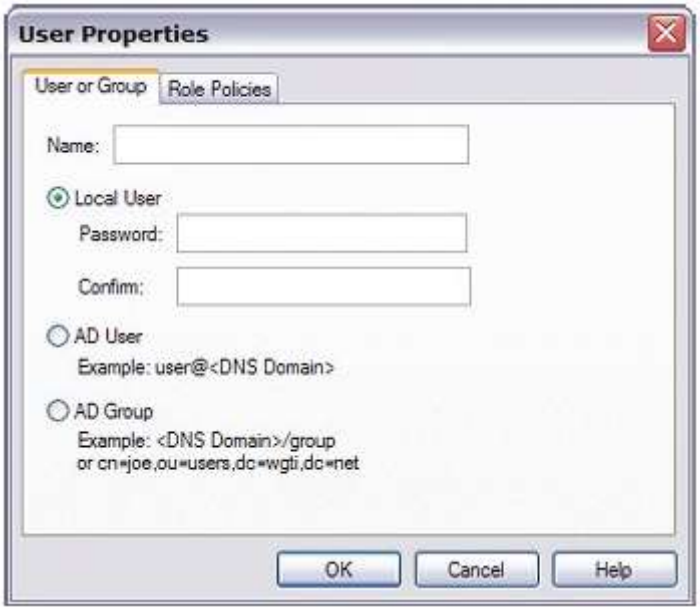
При помощи WatchGuard System Manager (WSM) и WatchGuard Server Center вы можете создавать, редактировать и удалять пользователей или группы пользователей, которые будут использоваться для администрирования на базе ролей. Вы можете выбрать способ аутентификации пользователя или группы, а также создать пароль для локального пользователя.

Использования WatchGuard System Manager для настройки пользователей или групп

1. Откройте WatchGuard System Manager и подключитесь к вашему Серверу Управления.

2. Выберите **File** > **Manage Users**.
   Откроется диалогое окно Manage Users

3. Для того чтобы добавить нового пользователя нажмите **Add**. Для того чтобы изменить информацию о пользователе выберите его из списка и нажмите **Edit**. Вы не можете изменять имена пользователя или группы. Сначала вам необходимо удалить пользователя или группу, а затем добавить нового пользователя или группу с новым именем.
   Откроется диалогое окно User Properties



4. В закладке **User or Group** в поле **Name** введите имя пользователя или группы.

5. Для локальной аутентификации пользователя выберите **Local User**. Для аутентификации пользователя на серверах Active Directory или LDAP нажмите **AD User**. Для аутентификации группы на серверах Active Directory или LDAP нажмите **AD Group**.

   Если вы хотите для аутентификации пользователей использовать сервер Active Directory, то перед тем как создавать пользователей, вам необходимо включить аутентификацию Active Directory

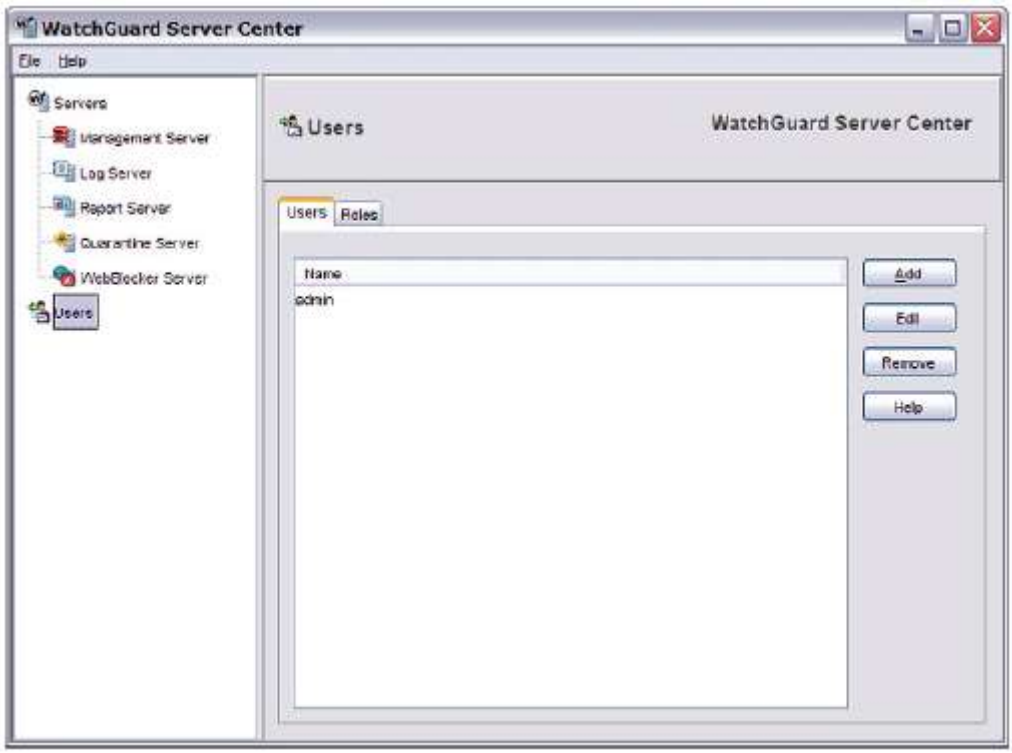
6. Если вы создаете или редактируете локального пользователя, в поле **Password** введите новый пароль.

7. В поле **Confirm Password** введите пароль снова.

8. Если вы редактировали существующих пользователя или группу нажмите **OK**. Если вы создаете нового пользователя или группу выберите закладку **Role Policy** и присвойте роль этому пользователю или группе.

Создание и настройка пользователей и групп в WatchGuard Server Center

1. В левой панели навигации нажмите **Users**.
   Откроется страница Users



2. Для того чтобы добавить нового пользователя нажмите **Add**. Для того чтобы изменить информацию о пользователе выберите его из списка и нажмите **Edit**. Вы не можете изменять имена пользователя или группы. Сначала вам необходимо удалить пользователя или группу, а затем добавить нового пользователя или группу с новым именем.
   Откроется диалогое окно User Properties.

3. В поле **Name** введите имя пользователя или группы.

4. Для локальной аутентификации пользователя выберите **Local User**. Для аутентификации пользователя на серверах Active Directory или LDAP нажмите **AD User**. Для аутентификации группы на серверах Active Directory или LDAP нажмите **AD Group**.

Если вы хотите для аутентификации пользователей использовать сервер Active Directory, то перед тем как создавать пользователей, вам необходимо включить аутентификацию Active Directory

5. Если вы создаете или редактируете локального пользователя, в поле **Password** введите новый пароль.

6. В поле **Confirm Password** введите пароль снова.

7. Если вы редактировали существующих пользователя или группу нажмите **OK**

*Если вы создаете нового пользователя или группу выберите закладку **Role Policy** и присвойте роль этому пользователю или группе.*

Удаление пользователя или группы

Вы не можете удалять предопределенных пользователей или группы. Для того чтобы удалить пользователя или группу выполните следующее:

1. В списке **Users** выберите пользователя или группу, которую вы хотите удалить.

2. Нажмите **Remove**.
   Появится сообщение о подтверждение удаления пользователя или группы.

3. Нажмите **Yes**.
   Пользователь или группа будут удалены из списка.

Создание ролей

При помощи WatchGuard Server Center и WatchGuard System Manager вы можете создавать и редактировать роли на вашем Сервере Управления. Редактировать вы можете только роли, созданные пользователем. Если вы хотите изменить предопределенную роль, скопируйте ее параметры в новую роль, выполните все необходимые изменения и сохраните новую роль.

Создание ролей в WatchGuard Server Center

1. В левой панели навигации нажмите **Users**.
   Откроется страница Users.

2. Выберите закладку **Roles**.
   Предопределенные роли будут отображаться синим цветом, а роли, созданные пользователем – черным

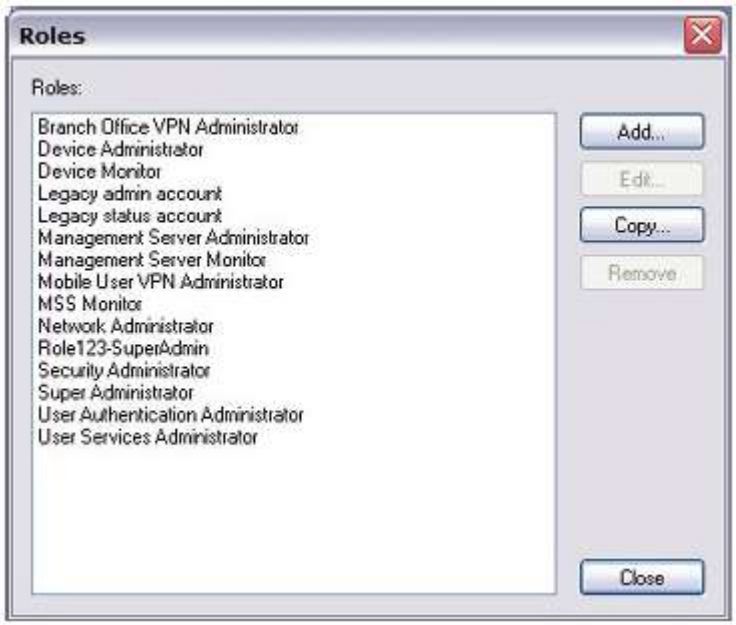
3. Выполните все необходимые инструкции, описанные в разделе “Настройка ролей и политик ролей”

Создание ролей в WatchGuard System Manager

1. Откройте WatchGuard System Manager и подключитесь к вашему Серверу Управления.

2. Выберите **File** > **Manage Users**.
   Откроется диалогое окно Manage Users

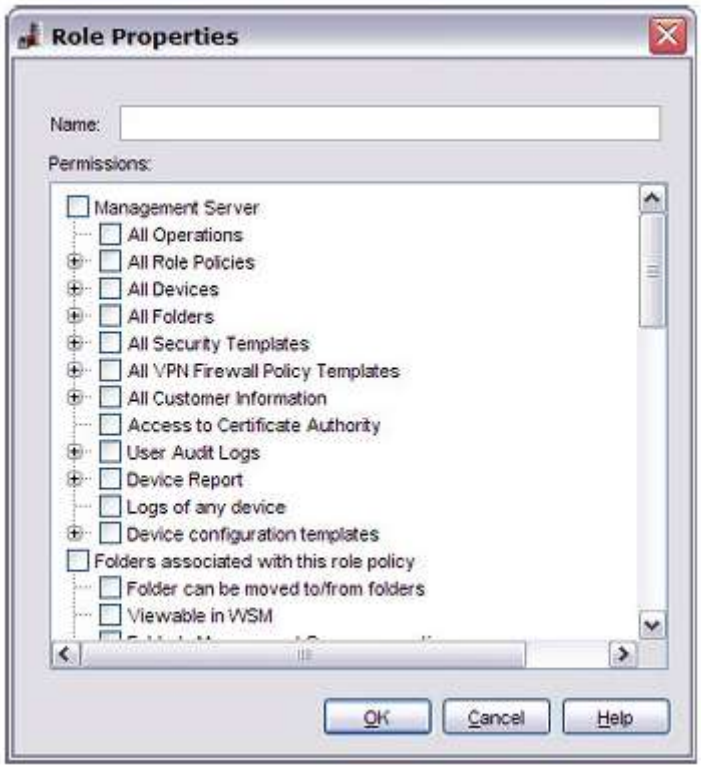
3. Нажмите **Roles**.
   Откроется диалогое окно Roles



4. Выполните все необходимые инструкции, описанные в разделе “Настройка ролей и политик ролей”

Настройка ролей и политик ролей

1. Для того чтобы создать новую роль нажмите **Add**. Для того чтобы редактировать существующую роль, выберите ее из списка и нажмите **Edit**. Редактировать вы можете только роли, созданные пользователем. Если вы хотите создать новую роль на базе существующей предопределенной роли, выберите необходимую предопределенную роль и нажмите **Copy**.
   Откроется диалогое окно Role Properties



2. В поле **Name** введите имя роли.

3. В окне **Permissions** выберите набор прав, который вы хотите предоставить этой роли.

4. Нажмите **OK**.

Удаление ролей

Вы не можете удалять предопределенные роли. Для того чтобы удалить роль выполните следующее:

1. Выберите роль в списке.

2. Нажмите **Remove**.
   Появится сообщение подтверждения удаления роли.

3. Нажмите **Yes**.
   Роль удаляется из списка.

Присвоение ролей пользователю или группе

Политики ролей соединяют набор задач и устройств, на которых эти задачи можно выполнять. При помощи WatchGuard System Manager или WatchGuard Server Center вы можете присвоить одну или несколько ролей пользователю или группе пользователей. Если вы пользователя или группе присваиваете несколько ролей, то пользователь или группа пользователей могут выполнять все задачи на всех устройствах, описанные в этих ролях.

Присвоение ролей в WatchGuard System Manager

Для того для того, чтобы присвоить новую роль пользователю или группе пользователей, или изменить существующие роли, выполните следующее:

1. Откройте WatchGuard System Manager и подключитесь к вашему Серверу Управления.

2. Выберите **File** > **Manage Users**.
   Откроется диалогое окно Manage Users.

3. Создайте пользователя и нажмите **Add**. Или выберите пользователя из списка **Users** и нажмите **Edit**.
   Откроется диалоговое окно User Properties.

4. Выберите закладку **Role Policies**.

5. Для того чтобы добавить новую роль нажмите **Add**. Для того чтобы редактировать существующую роль, выберите необходимую роль из списка **Role** и нажмите **Edit**.
   Откроется диалоговое окно Role Policy

6. В выпадающем списке **Role** выберите существующую роль. Или нажмите **New** для создания новой роли

7. В списке **Devices** отметьте флаг напротив каждого Firebox, который вы хотите добавить в политику роли.

8. Нажмите **OK**.
   Роль появится в списке в закладке Role Policies.

9. Нажмите **OK**.

Для того чтобы удалить роль из настроек пользователя или группы выполните следующее:

1. В диалоговом окне **User Properties** из списка **Role** выберите необходимую роль.

2. Нажмите **Remove**.
   Появится сообщения подтверждения.

3. Нажмите **Yes** для того чтобы удалить роль из списка **Role**.

Присвоение ролей в WatchGuard Server Center

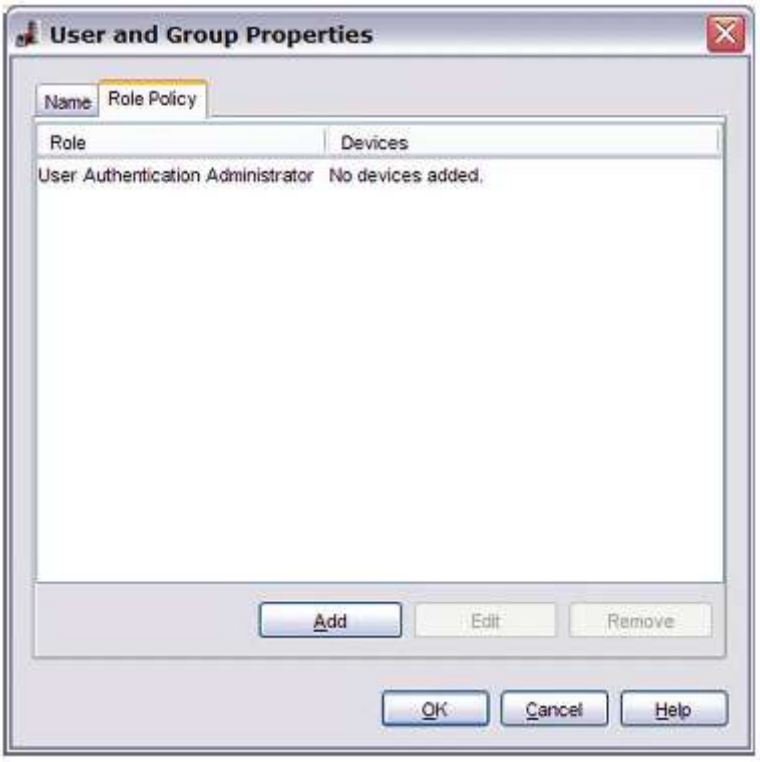
Для того для того, чтобы присвоить новую роль пользователю или группе пользователей, или изменить существующие роли, выполните следующее:

1. В левой панели навигации выберите **Users**.
   Откроется страница Users.

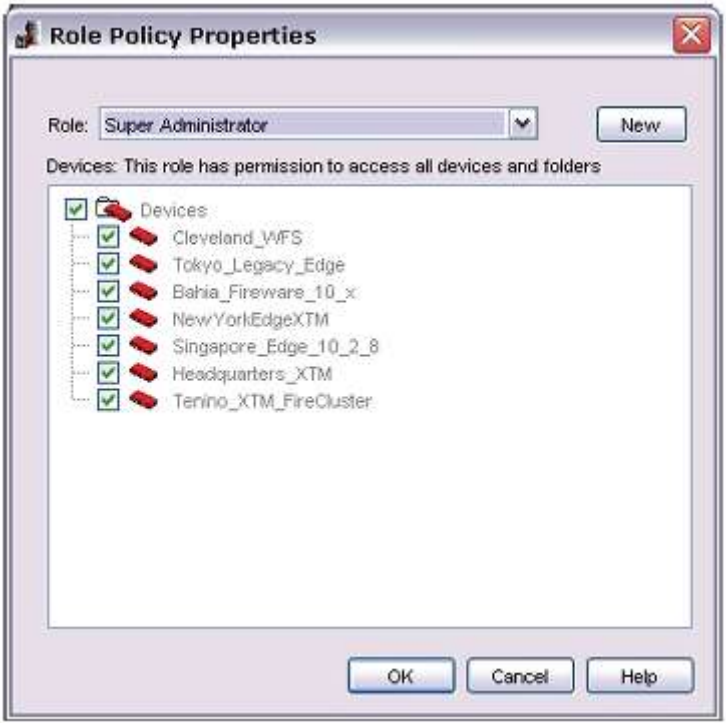
2. Выберите закладку **Users**.

3. Нажмите **Add**.
   Откроется диалогое окно User and Group Properties.

4. Выберите закладку **Role Policy**.
Откроется список ролей, присвоенных данному пользователю. Имя роли отображается в колонке Role, список устройств, разделенных запятой, - в колонке Devices



5. Для того чтобы добавить новую политику роли для пользователя или группы нажмите **Add**. Для изменения существующей политики роли выберите ее и нажмите **Edit**.
Откроется диалогое окно Role Policy Properties



6. В выпадающем списке **Role** выберите роль. Или нажмите **New** для создания новой роли

7. В списке **Devices** отметьте флаги напротив устройств и каталогов, которые вы хотите присвоить этому пользователю и роли.

8. Нажмите **OK**.

Для того чтобы удалить роль из настроек пользователя или группы:

1. В диалоговом окне **User and Group Properties** в списке **Role** выберите роль.

2. Нажмите **Remove**.
   Появится сообщение подтверждения.

3. Нажмите **Yes** для того чтобы удалить роль из списка **Role**.

Глава 21 - Журналы и Уведомления

Ведение журнала и файлы журнала

Важным компонентом любой политики безопасности сети является возможность сбора информации с ваших систем безопасности, периодическая проверка и хранение этой информации.

Система ведения журнала WatchGuard создает файлы журнала, которые содержат информацию о событиях, которые помогут вам следить за состоянием вашей системы безопасности и при необходимости устранять потенциальные угрозы

Файл журнала – список событий и информация о них. Событие – это действие, произошедшее на устройстве Firebox.

Например, блокировка пакета – это событие .

Ваш Firebox также может перехватывать информацию о разрешенных событиях для того, чтобы предоставить более полную картину активности в вашей сети.

Система ведения журналов состоит из нескольких компонентов.

Серверы Журналов

Сервер Журналов собирает сообщения журналов с каждого устройства Firebox. Серверы журнала получают информацию по TCP порту 4107 и 4115. Каждое устройство, которое подключается к Серверу Журналов прежде всего отправляет свое имя, серийный номер, часовой пояс и версию программного обеспечения, и только потом отправляются данные журнала. Серийный номер (SN) Firebox используется как уникальный идентификатор устройства в базе данных Сервера Журналов. Сервер Журналов использует несколько копий базы данных PostgreSQL для управления своей глобальной базой данных.

Каждая копия базы данных PostgreSQL отображаться в Windows Task Manager, как отдельный процесс PostgreSQL. Сервер журнала использует несколько процессов и режимов для сбора и восстановления данных журнала сообщений.

wlcollector.exe - это процесс, который занимается сбором данных журнала

Ваш Firebox подключается к этому процессу по TCP-порту 4115/4107. Программа wlcollector.exe использует два модуля: *ap_collector и ap_notify.*

ap_collector- получает сообщения журнала от Firebox и помещает их в базу данных Сервера Журналов. ap_notify получает тревоги от устройства Firebox и генерирует соответствующие уведомления. Сообщения журнала зашифровываются и отправляются на Сервер Журнала в формате XML (плоский текст).

Информация, которая собирается с брандмауэров, включает в себя сообщения о трафике, тревогах, событиях, сообщения об отладке и статистические сообщения

Вы можете установить Сервер Журналов на компьютер, который вы используете как станцию управления. Или вы можете установить Сервер Журналов на другой компьютер.

Вы можете так же установить дополнительный Сервер Журналов для резервирования и масштабируемости. Для этого используйте программу-инсталлятор WatchGuard System Manager

(WSM) и выберите для установки компоненты Сервера Журналов. После того, как ваш Сервер Журналов собрал данные с устройств Firebox, Сервер Отчетов через определенные промежутки времени собирает эту информацию и генерирует отчеты.

LogViewer

LogViewer - утилита WatchGuard System Manager для просмотра файла журнала. Утилита предоставляет пользователям возможность постраничного вывода информации из файлов журнала, а также функцию поиска и отображения по ключевым или указанным полям.

Ведение журналов и уведомления в приложениях и на серверах

Сервер Журналов может принимать сообщения журнала от вашего Firebox или сервера WatchGuard. После того, как вы настроили ваш Firebox и Сервер Журналов, Firebox начинает отправлять сообщения журнала на Сервер Журналов. Включить ведение журналов вы можете в различных приложениях WSM и политиках, которые вы создали для управления уровнем отображаемых сообщений журнала. Если вы хотите, чтобы сообщения журнала отправлялись на Сервер Журналов с другого сервера WatchGuard, вам необходимо на этом сервере настроить ведение журнала

Сообщения журнала

Firebox отправляет сообщения журнала на Сервер Журналов. Он также может отправлять сообщения на сервер syslog или сохранять их локально. Вы можете выбрать любой из предложенных вариантов.

Для того чтобы посмотреть сообщения журнала выберите закладку **Traffic Monitor** в Firebox System Manager

Вы также можете посмотреть сообщения журнала при помощи утилиты LogViewer. На Сервере Журналов сообщения хранятся в каталоге WatchGuard в файле базы данных SQL с расширением .wgl.xml. Для более подробной информации о типах сообщений журнала см. “Типы сообщений журнала”

Файлы журнала

Сервер Журналов WatchGuard использует файлы *wlcollector.log u ap_collector.log* для хранения информации об подключениях к устройству и базе данных. Эта информация включает ошибки аутентификации, несоответствия запросов и откликов, ошибки доступа к базе данных

Эти файлы восстанавливаются по умолчанию в:
C:\Documents and Settings\WatchGuard\logs\wlogserver\wlcollector

Базы данных

Информация журнала хранится в базе данных PostgreSQL. Каждый Сервер Журнала имеет 4 главных таблицы, которые хранят сообщения журнала для всех устройств Firebox. Эти 4 таблицы управляются специальной (master) таблицей, которая предоставляет доступ к этим 4 таблицам . Сервер Журнала создает новую таблицу каждый день для хранения информации, которая была получена в этот день. Для того чтобы внести изменения в базу данных вручную вы можете использовать PostgreSQL скрипты или специальные утилиты управления, например *pgadmin*.

При первом подключении Firebox к Серверу Журнала, Сервер Журнала обновляет глобальную базу данных информацией о новом устройстве. Сообщения журнала от каждого устройства отправляются к одной из 4 таблиц базы данных Сервера Журнала.

Данные в этих таблицах используются при просмотре журналов в WatchGuard Log Viewer или создании отчета с помощью WatchGuard Report Manager. Эти приложения используют XMLRPC-запросы для общения с Сервером Журнала.

Сгенерированные Сервером Отчетов WatchGuard отчеты сохраняются как XML-файлы в: *C:\Documents and Settings\WatchGuard\wrserver\reports*

Производительность и дисковое пространство

Вы можете настроить несколько устройств Firebox для отправки информации журнала к одному Серверу Журналов. Количество подключаемых устройств строго ограничено доступным дисковым пространством. Однако, точное число устройств, которые вы можете подключать к Серверу Журналов, зависит от размера и скорости его жестких дисков, количества доступной оперативной памяти, количества процессоров и суммы всего трафика журналов, который отправляется на Сервер Журналов с каждого устройства

Вы можете значительно увеличить производительность вашего Сервера Журналов, добавив более скоростные жесткие диски, больше памяти или другие процессоры. Сервер Журналов включает настройку, которая может автоматически удалять старые сообщения журнала из базы данных. При первой установки Сервера Журнала мы рекомендуем определить, сколько дискового пространства используется в среднем за день.

Оцените количество дней, в течение которых дисковое пространство Сервера Журналов будет заполнено и выполните все необходимые настройки в соответствие со значением этого интервала. Дисковое пространство снова используется при создании новой записи журнала и удалении сообщения из базы данных.

Утилита *reindexdb* перестраивает индексы в одной или более таблиц базы данных PostgreSQL для увеличения производительности. Утилиту следует устанавливать только по рекомендации представителя технической поддержки компании WatchGuard.

Типы сообщений журнала

Firebox может отправлять пять типов сообщений журнала. Тип сообщения отображается в тексте сообщения

Пять типов сообщений журнала:

- Traffic-сообщения
- Alarm-сообщения
- Event-сообщения
- Debug-сообщения
- Statistic-сообщения

Traffic-сообщения

Firebox отправляет traffic-сообщение при обработке трафика, проходящего через него, фильтром пакетов и правилами прокси.

Alarm-сообщения

Alarm-сообщения отправляются на Сервер при наступлении события, которое заставляет устройство Firebox выполнять команду. Когда выполняется условие тревоги, то устройство Firebox отправляет Alarm-сообщение утилите Traffic Monitor и на Сервер Журналов, а затем выполняет необходимые действия. Вы можете установить несколько типов Alarm-сообщений. Например, вы можете при помощи утилиты Policy Manager настроить генерацию тревоги, когда какое-то значение совпадает с установленным значением или превышает пороговое. Остальные типы alarm-сообщений отправляются программно-аппаратным обеспечением, и вы не можете изменять значения.

Например, Firebox отправляет Alarm-сообщение, когда произошел сбой при подключении к одному из интерфейсов Firebox или обнаружена атака типа «Denial of Service»

Существует восемь категорий alarm-сообщений: System, IPS, AV, Policy, Proxy, Counter, Denial of Service и Traffic. Firebox за 15 минут отправляет не более 10 alarm-сообщений, которые удовлетворяют одному и тому же условию.

Event-сообщения

Firebox отправляет event-сообщения по причине пользовательской активности. Firebox генерирует event-сообщения при выполнении следующих действий:

- Включение и выключение Firebox
- Firebox и VPN-аутентификация
- Запуск или остановка процесса
- Проблемы с аппаратными компонентами Firebox
- Любое действие, выполненное администратором Firebox

Debug-сообщения

Debug-сообщения содержат информацию, полезную для решения возникших проблем. Всего 27 различных компонентов, которые могут генерировать Debug -сообщения. Вы можете настроить отображение diagnostic-сообщений в утилите Traffic Monitor

Statistic-сообщения

Statistic-сообщения содержат информацию о производительности Firebox. По умолчанию Firebox отправляет сообщения журнала о работе интерфейса External и статистике использования пропускной способности VPN. Вы можете использовать эти сообщения при изменении настроек вашего Firebox для улучшения производительности

Уровни сообщений журнала

При настройке ведения журнала для любого сервера WatchGuard вы можете установить уровень, назначенный сообщению журнала для каждого сервера.

Это позволяет выбирать тип сообщения, который будет включаться в файл журнала.Возможные уровни сообщения журнала:

Off

Diagnostic-сообщения не отправляются на Сервер Журнала для это категории.

Error
(Уровень: низкий)

Включает только сообщения о серьезных ошибках, которые привели к остановке сервиса или процесса

Warning
(Уровень: средний)

Включает информацию об обычных операциях. Так же содержит всю информацию о сообщениях с уровнем *Error.*

Information
(Уровень: высокий)

Включает информацию об успешном выполнении операции, а так же все детали из уровней *Error* и *Warning*.

Debug
(Уровень: повышенный)

Включает детализированные сообщения журнала из всех уровней. Мы рекомендуем выбирать данный пункт только по требованию представителя технической поддержки Watch Guard для выяснения конкретных проблем с конфигурацией.

Уведомления

Уведомление – это сообщение, которое устройство Firebox отправляет администратору в ответ на какое-то событие, которое представляет потенциальную угрозу. Уведомление может быть в виде электронного письма или всплывающего окна. Уведомления также могут быть отправлены средствами SNMP ловушки

Администратор помимо файлов журнала, может проверить информацию, которая содержится в уведомлении для того, чтобы принять решение насчет улучшения системы безопасности. Например, компания WatchGuard рекомендует настроить опцию обработки пакетов таким образом, чтобы она отправляла уведомление каждый раз, когда Firebox обнаруживает попытку сканирования портов. Firebox обнаруживает попытку сканирования портов путем подсчета количества пакетов, отправленных с одного IP-адреса на все IP-адреса интерфейсов External устройства Firebox. Если это количество превышает установленную величину, хост журналов отправляет уведомления администратору сети с информацией об отклоненных пакетах.

При обнаружении попытки сканирования портов, администратор может предпринять следующие шаги

- Блокировать порты, которые пытались просканировать
- Блокировать IP-адрес, с которого были отправлены пакеты
- Отправить уведомления в форме электронного письма вашему администратору сети

Firebox отправляет уведомления только при их включении и настройке на Сервере Журналов, который используется на вашем устройстве.

Настройка журналов для вашей сети

При помощи Сервера Журналов WatchGuard и параметров уведомлений вы можете настроить ведение журнала в вашей сети. Данные журнала, которые собирают устройства Firebox и Сервер Журнала, позволят вам управлять работой вашей сети

Этот раздел содержит общую информацию по настройке журнала для вашей сети. Для более подробной информации по каждому из пунктов, см. соответствующие ссылки в конце каждого раздела

Шаг 1 — Запуск мастера установки WatchGuard Server Center

На компьютере, на котором установлен Сервера Журналов, выполните следующее:

1. Нажмите правой кнопкой мыши на  в панели задач и выберите **Open WatchGuard Server Center**.
   Откроется мастер установки WatchGuard Server Center Setup Wizard.

2. Просмотрите первую страницу мастера, чтобы убедиться в наличии всей необходимой информации для выполнения мастера настроек. Нажмите **Next**.

3. Введите имя вашей организации. Нажмите **Next**.

4. Введите и подтвердите пароль администратора (**Administrator passphrase**) для использования всех серверов WatchGuard. Нажмите **Next**.

5. (Дополнительно) Введите IP-адрес вашего шлюза Firebox. Нажмите **Add**. Нажмите **Next**.

6. (Дополнительно) Введите лицензионный ключ вашего Сервера Управления. Нажмите **Next**.

7. Введите **Log Server Encryption key** и нажмите **Browse** для выбора расположения базы данных Сервера Журнала. Нажмите **Next**.

8. Введите доменное имя Сервера Карантина. Нажмите **Add**. Нажмите **Next**.

9. (Дополнительно) загрузите и установите базу данных WebBlocker. Нажмите **Next**.
   Процедура займет продолжительное количество времени для загрузки и установки базы данных. Вы можете установить базу данных позже, если выберите отказ от установки в мастере.

10. Просмотрите выбранные вами параметры. Нажмите **Next**.
    Мастер установки настроит ваши сервера.

11. Нажмите **Finish** для завершения работы мастера.

Более подробную информацию см. в разделе "Установка серверов WatchGuard System Manager"

Шаг 2 — Настройка вашего Сервера Журналов

На компьютере, на котором установлен Сервера Журналов, выполните следующее:

1. Нажмите правой кнопкой мыши на  в панели задач и выберите **Open WatchGuard Server Center**.
   Откроется диалоговое окно WatchGuard Server Center.

2. Введите имя пользователя в поле **Username** и пароль администратора в поле **Administrator passphrase**.

3. В меню **Servers** выберите **Log Server**.
   Откроется страница Log Server.

4. Измените настройки по умолчанию в соответствии с вашей сетью.

   * для изменения настроек по умолчанию выберите закладку **Server Settings**

   * для изменения параметров резервирования файла журнала, его удаления и настройки уведомлений выберите закладку **Database Maintenance**.

   * для изменения параметров ведения журнала выберите закладку **Logging**

5. При завершении работы нажмите **OK**.

Шаг 3 — Выбор приложения, которому Firebox будет отправлять данные журнала

На компьютере с установленным WSM откройте Policy Manager для выбранного Firebox.

1. В Policy Manager, выберите **Setup > Logging**.

2. Настройте параметры журнала для Сервера Журнала WatchGuard, сервера syslog и внутреннего хранилища Firebox.

Шаг 4 — Настройка Сервера Журналов на вашем Firebox

1. В Policy Manager выберите **Setup > Logging**.
   Откроется диалоговое окно Logging Setup.

2. Нажмите **Configure**.

3. Выберите Сервер Журнала в списке. Если в списке более одного сервера, вы можете нажать **Up** или **Down** для изменения порядка текущего выбранного сервера.

4. Нажмите **OK**.
   Новый приоритет Сервера Журнала появится в списке Сервера Журнала WatchGuard.

Шаг 5 — установки уведомления в вашей политике

1. В Policy Manager добавьте политику или дважды нажмите на политике для ее редактирования.

2. Нажмите на закладку **Properties** и нажмите **Logging**.

3. Установите параметры для политики безопасности.

Шаг 6 — использование LogViewer для просмотра сообщений данных

1. Для открытия LogViewer нажмите на  в панели инструментов WatchGuard System Manager.
   Откроется диалоговое окно WatchGuard LogViewer.

2. Для подключения к устройству нажмите  в панели LogViewer.
   Откроется диалоговое окно Connect to Log Server.

3. Введите IP-адрес и пароль для вашего Сервера Журнала и нажмите **OK**.
   Откроется диалоговое окно Select Firebox/Server.

4. Выберите Сервер Журнала или Firebox из списка и нажмите **OK**. Для подключения к нескольким устройствам одновременно выберите более одного Firebox или Сервера Журнала.
   Окно устройства появится для каждого выбранного устройства. IP-адрес появится в заголовке окна. Содержание окон для Firebox и Сервера Журнала будет различными.

5. Выберите сообщения журнала для просмотра более подробной информации о нем.
   Подробная информация о сообщении журнала появится на правой нижней части окна Details.

Если детализированная информация не отображается, выберите **View > Details Pane**.

Настройка Сервера Журналов

Сервер Журналов осуществляет сбор данных журнала для каждого Firebox, управляемого WatchGuard System Manager. Вы можете можете установить Сервер Журналов на вашу станцию управления или установить его на другой компьютер. Вы можете так же добавить еще один Сервер Журналов для обеспечения резервирования

Если вы установили сервер WatchGuard на компьютере с брандмауэром, отличным от Windows Firewall, вам следует открыть порты, необходимые для подключения серверов через брандмауэр. Пользователи Windows Firewall не должны изменять эти настройки

Установка Сервера Журнала

Для установки Сервера Журналов на ваш компьютер или другую управляющую станцию выполните следующее:

1. Выполните программу установки WatchGuard System Manager.

2. Выберите компоненты только для **Log Server**.

3. Завершите работы мастера установки.

Перед тем как начать

Перед выполнением настройки Сервера Журналов вам следует завершить работу мастера установки WatchGuard Server Center Setup Wizard. В мастере установки вы добавляете детали о зашифрованном ключе Сервера Журнала, о расположении базы данных Сервера Журнала и пути к каталогу для данных журнала.

Настройка системных параметров

Перед настройкой вашего Сервера Журналов убедитесь, что на компьютере с установленным Сервером Журналов отключен переход в спящий режим и установлено тоже время, что и на Firebox.

1. Нажмите **Start** > **Control Panel**.

2. Выберите **Power Options**.

3. Выберите закладку **Hibernate** для отключения перехода в «спящий режим». Это необходимо, чтобы удостовериться, что Сервер Журналов не выключится при переходе компьютера в спящий режим.

4. Убедитесь, что на Сервера Журнала и Firebox установлено одинаковое время.
   Для синхронизации времени на Firebox с системным временем откройте Firebox System Manager и выберите **Tools > Synchronize Time**.

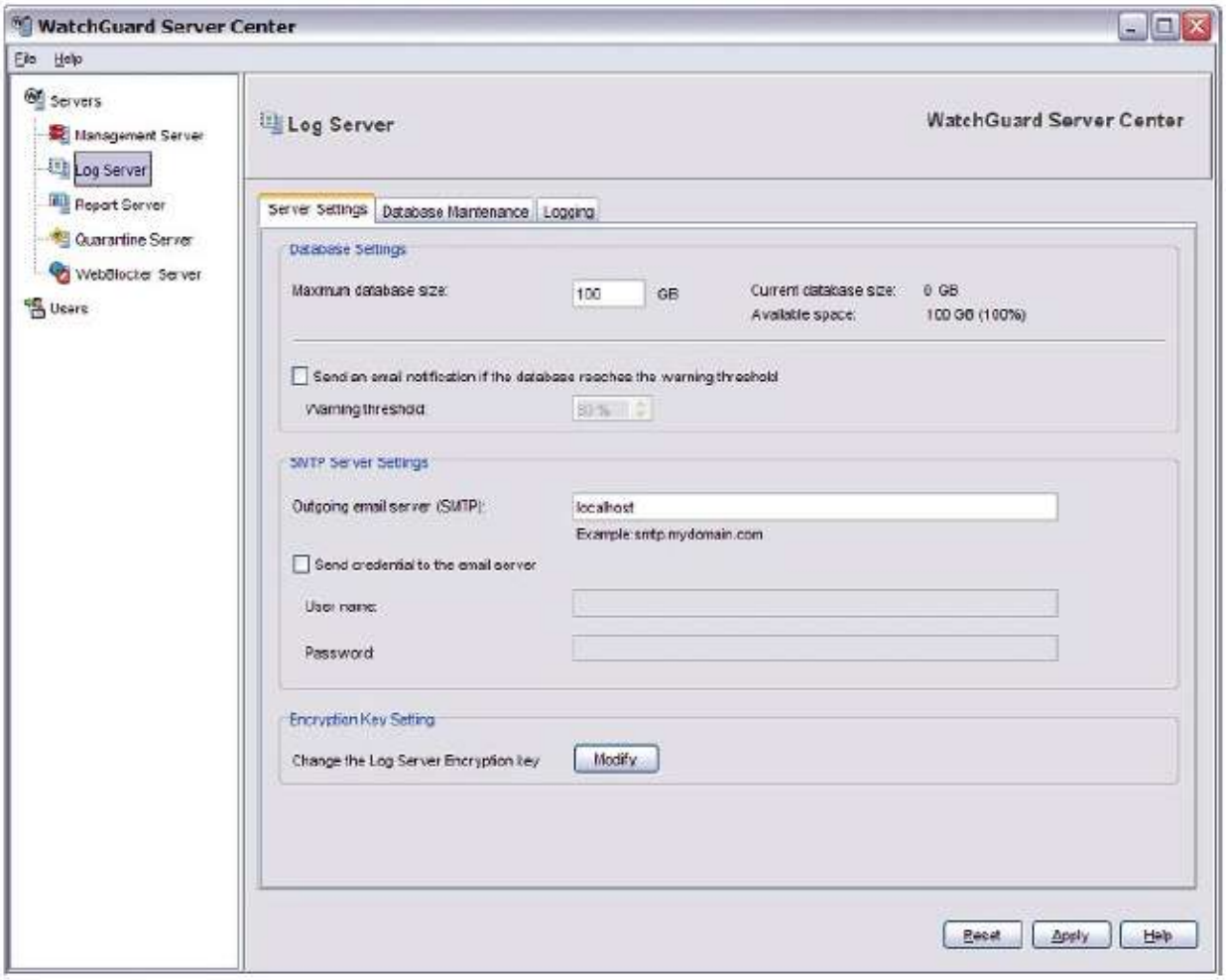
Настройка Сервера Журналов

На компьютере с установленным Сервером Журналов необходимо выполнить:

1. Нажмите правой кнопкой на  в панели задач и выберите **Open WatchGuard Server Center**.
   Откроется диалоговое окно Connect to WatchGuard Server Center.

2. Введите ваше имя пользователя в **Username** и пароль администратора в **Administrator passphrase**. Нажмите **Login**.
   Откроется диалоговое окно WatchGuard Server Center.

3. В списке **Servers** выберите **Log Server**.
Откроется диалоговое окно Log Server



4. Измените настройки по умолчанию в соответствии с вашей сетью:

   * для изменения настроек сервера по умолчанию выберите закладку **Server Settings** .

   * для изменения параметров резервирования файла, удаления и уведомления выберите закладку **Database Maintenance**.

   * для изменения параметров ведения журнала выберите закладку Logging.

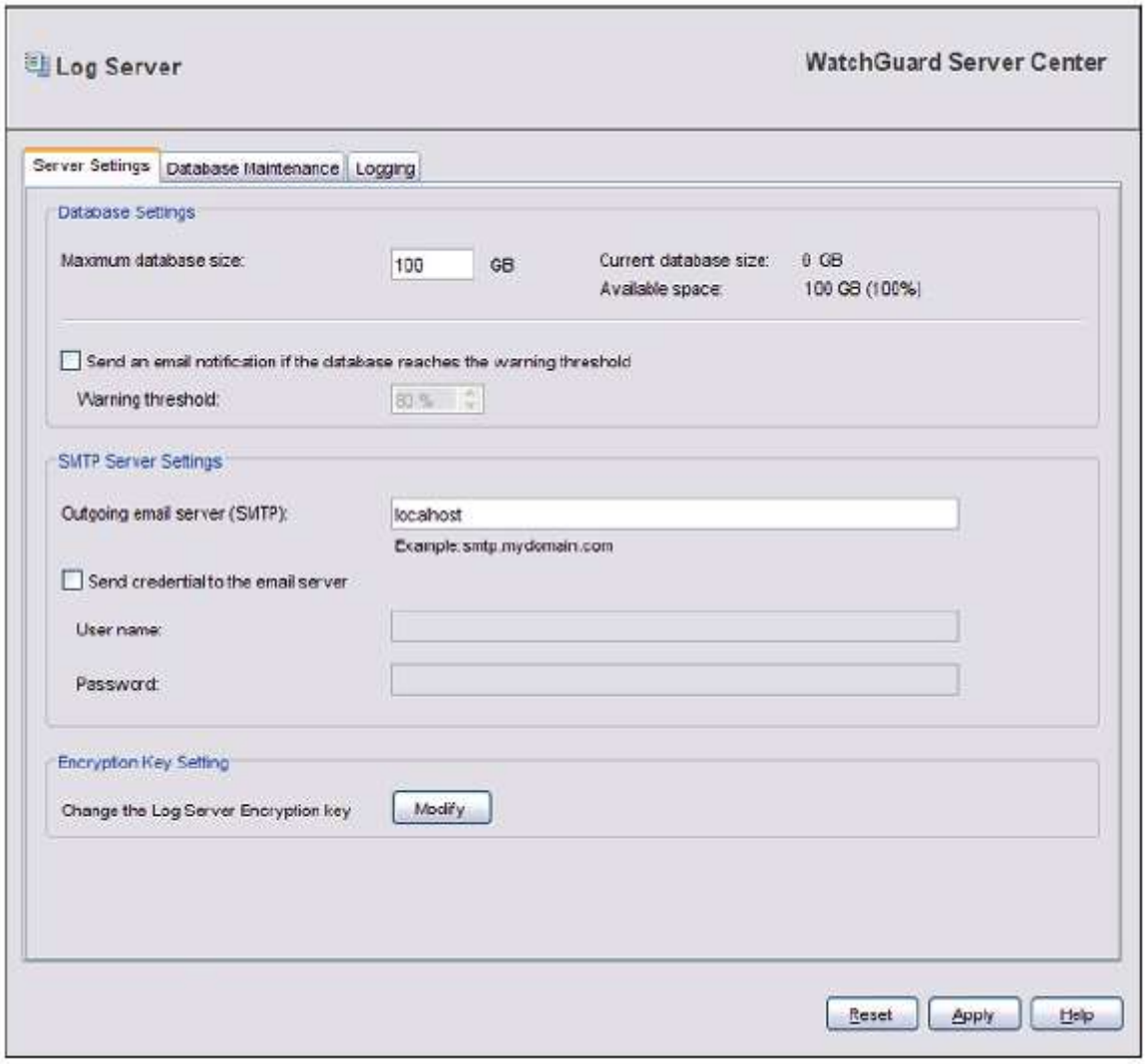
Настройка параметров базы данных, SMTP-сервера и ключа шифрования

Вы можете выбрать базу данных и параметры SMTP-сервера, ключа шифрования для вашего Сервера Журнала WatchGuard.

В WatchGuard Server Center необходимо выполнить:

1. В меню **Servers** выберите **Log Server**.

2. Нажмите на закладку **Server Settings**.
   Откроется диалоговое окно Server Settings



3. Используйте следующий раздел для настройки параметров вашего Сервера Журнала.

4. При завершении нажмите **Apply** для сохранения изменений.

Настройка параметров базы данных Сервера Журнала

Вы можете выбрать максимальный размер базы данных Сервера Журнала и получать сообщения уведомление о приближении размера базы данных к максимальному, заданному вами значению. Когда размер сервера достигает максимально заданного значения, то происходит очистка самых старых сообщений журнала для создания свободного места новым сообщениям.

В разделе **Database Settings** необходимо выполнить:

1. В поле **Maximum database size** введите максимальный размер базы данных Сервера Журнала. Установите значение от 1 до 10 000 Гб.
   Текущий размер базы данных и количество Гб отображается рядом с этим полем.

2. Для получения предупреждающего сообщения при приближении размера базы данных к предельному значению выберите опцию **Send an email notification if the database reaches the warning threshold**.

3. Для определения времени, когда база данных отправит вам предупреждающее сообщение о пороговом значении, нажмите стрелками вверх или вниз на **Warning threshold.**

Например, если вы хотите получать предупреждение, установили значение пороговой величины равным 90% и максимальный размер базы данных равным 1000 Гб, то Сервер Журналов отправит вам предупреждение, когда будет занято 900 Гб дискового пространства.

Параметры SMTP сервера

Вы можете задавать адрес сервера исходящих электронных сообщений SMTP и устанавливать учетные записи пользователей для доступа к SMTP-серверу, если ваш email-сервер требует проверки подлинности.

В разделе **SMTP Server Settings** необходимо выполнить:

1. В поле **Outgoing email server (SMTP)** введите адрес вашего SMTP-сервера.

2. Если ваш email-сервер требует аутентификации, следует:

   * включить опцию **Use login information for the email server**.

   * в поле **User name** ввести имя пользователя для email-сервера. Если имя пользователя не предусмотрено для вашего SMTP-сервера, вы можете оставить это поле пустым.

   * в поле **Password** ввести пароль для email-сервера.

Если пароль не предусмотрен для вашего SMTP-сервера, вы можете оставить это поле пустым.

Изменение ключа шифрования Сервера Журнала

Вы можете изменять ключ шифрования Сервера Журнала при установке мастера настроек в WatchGuard Server Center Wizard.

В разделе **Encryption Key Setting**:

1. Нажмите **Modify**.
   Откроется диалоговое окно Log Server Encryption Key.

2. В поле **New key** введите новый ключ шифрования для Сервера Журнала.

3. Нажмите **OK**.
   Закроется диалоговое окно Log Server Encryption Key и ключ шифрования обновится до новой. заданной величины.

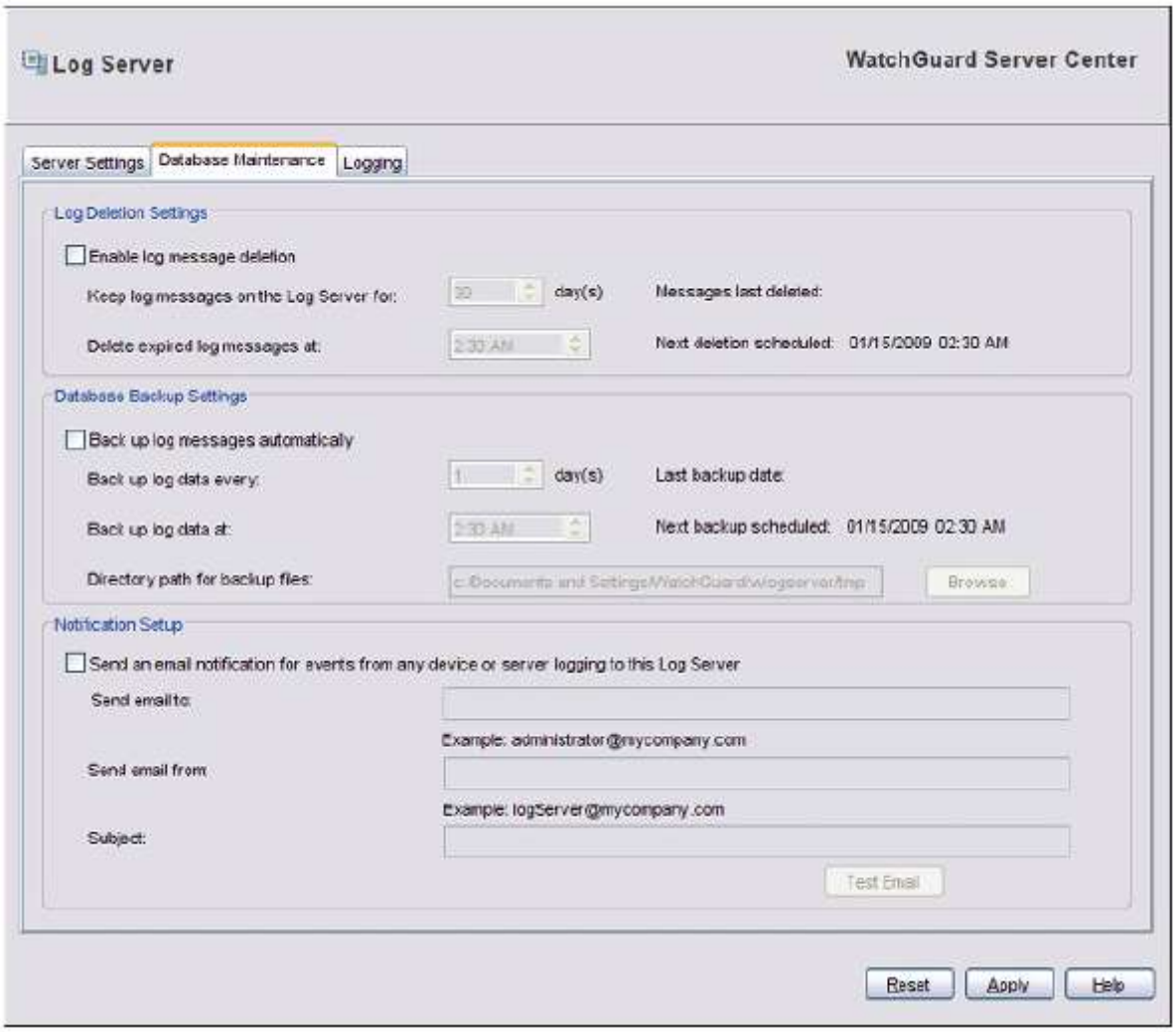
Настройка удаления журнала, резервной копии базы данных и параметров уведомления о событиях

Вы можете выбрать параметры удаления журнала, резервирования базы данных и уведомления для вашего Сервера Журнала WatchGuard.

В WatchGuard Server Center:

1. В меню **Servers** выберите **Log Server**.

2. Нажмите на закладку **Database Maintenance**.
   Откроется диалоговое окно Database Maintenance



3. Используйте следующий раздел для настройки параметров вашего Сервера Журнала.

4. Для завершения работы и сохранения изменений нажмите **Apply.**

Настройка параметров удаления сообщений журнала

Вы можете включить ваш Сервера Журналов для удаления сообщений журнала из вашего устройства и задать время удаления сообщений.

В разделе **Log Deletion Settings**:

1. Выберите опцию **Enable log message deletion**.

2. Для задания количества дней, в течение которых сообщения остаются на Сервере Журналов, нажмите стрелку вверх/вниз **Retain log messages for**.
   Данные сообщения, удаленные позже всех, появятся в диалоговом окне

   Для уменьшения размера базы данных Сервера Журналов выберите наименьшее количество дней. Это позволяет вашему Серверу Журналов удалять сообщения более часто.

3. Для установки времени дня, когда будут удалены сообщения с истекшим сроком, нажмите стрелки вверх/вниз **Delete expired log messages at.**
   Дата и время следующего запланированного удаления появятся в диалоговом окне.

Настройка параметров для резервирования базы данных Сервера Журнала

Вы можете настроить Сервер Журналов для автоматического создания резервной копии сообщений журнала, и определить, когда и как часто будут резервироваться данные журнала, а также выбрать каталог для сохранения резервной копии.

В разделе **Database Backup Settings**:

1. Включите опцию **Back up log messages automatically**.

2. Для того чтобы задать, как часто будут резервироваться данные журнала, при помощи стрелок **Back up log data every** выберите необходимое значение
   Диалоговое окно отображает дату последней резервной копии

3. Для выбора времени создания резервной копии данных при помощи стрелок **Back up log data at** выберите необходимые значения.
   Диалоговое окно отобразит дату и время следующего запланированного создания резервной копии.

4. Рядом с полем **Directory path for backup files** нажмите **Browse** и выберите каталог для сохранения резервной копии файла.
   Выбранный каталог появится в поле Directory path for backup files

Из-за того копия данных находится на том же, компьютере что и база данных Сервера Журналов, то мы рекомендуем сохранять копии данных Сервера в внешнем диске

Настройка параметров уведомления о событии

Вы можете настраивать Сервер Журнала для отправки сообщений-уведомлений для событий, которые настроены в Policy Manager. Вы можете так же выбрать учетную запись электронной почты для получения и отправки сообщений-уведомлений о событии.

В разделе Notification Setup:

1. Для включения уведомления выберите опцию **Send an email notification for events from any device or server logging to this Log Server**. Рекомендуется выбрать эту опцию для уведомления о событиях, которые настроены в Policy Manager.

2. В поле **Send email to** введите полный адрес электронной почты вашей учетной записи, на которой вы хотите получать уведомления.

3. В поле **Send email from** введите адрес электронной почты, от которого вы хотите получать уведомления.

4. В поле **Subject** введите тему, которая будет отображаться получателю при поступлении уведомления в электронном письме.

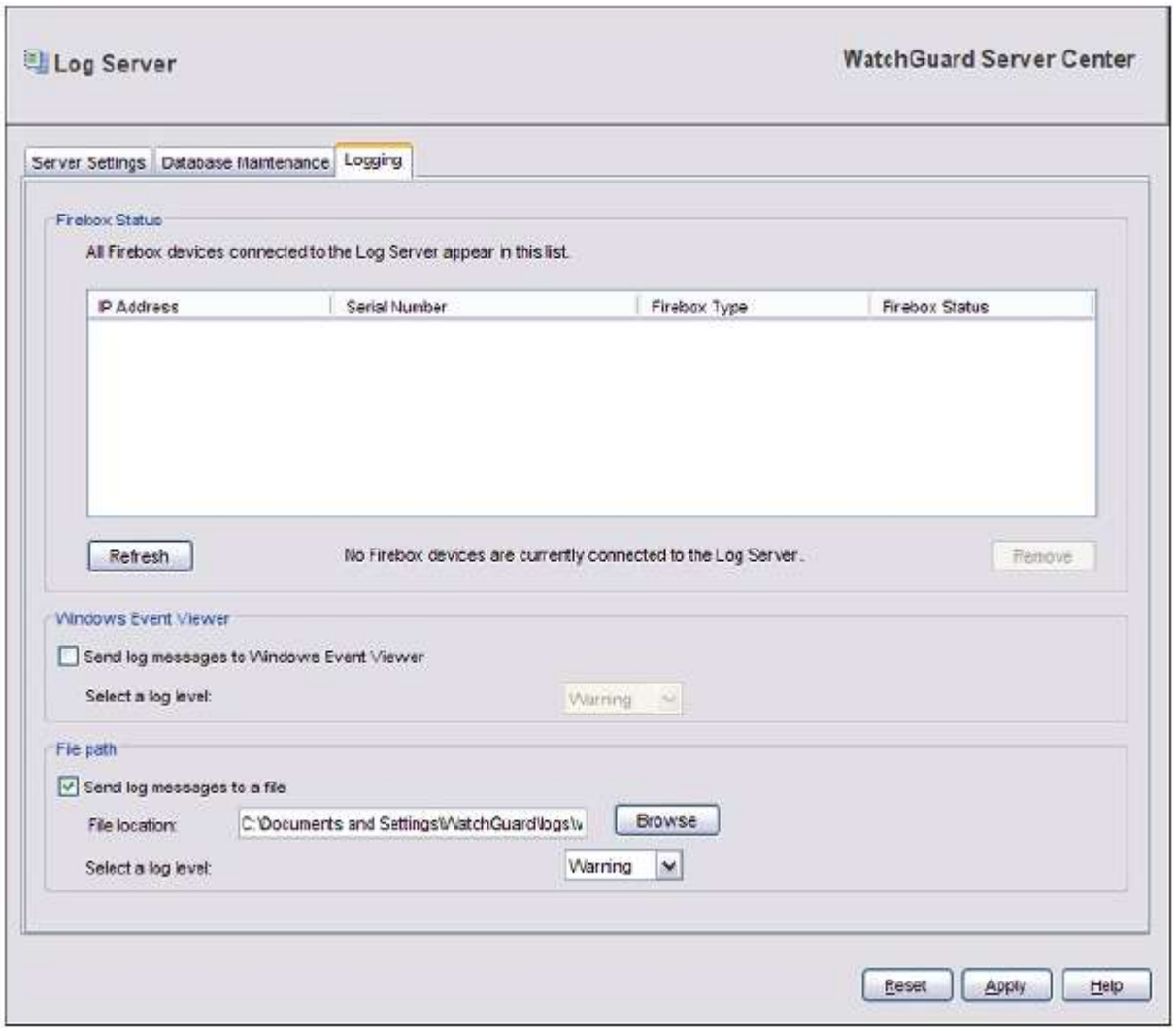
Настройка статуса Firebox и параметров ведения журнала

В закладке **Logging** вы можете настроить параметры состояния вашего Firebox, Windows Event Viewer, а также каталоги для хранения файлов журнала

В WatchGuard Server Center:

1. В списке **Servers** выберите **Log Server**.

2. Нажмите на закладку **Logging**.
   Откроется страница Logging



3. Используйте следующий раздел для настройки параметров вашего Сервера Журнала.

4. При завершении работы нажмите **Apply** для сохранения изменений.

Проверка состояния устройств Firebox

Окно **Firebox Status** отображает список всех устройств Firebox, подключенных к Серверу Журнала. Вы можете обновить список или удалить устройства из списка. Для просмотра текущего статуса подключенных устройств:

1. Убедитесь, что выбрана закладка **Logging**.

2. Нажмите **Refresh**.
   Откроется сообщение, если ни одно из устройств Firebox не подключено к Серверу Журнала.

Для удаления устройства из списка:

1. Выберите устройство в списке **Firebox Status** .

2. Нажмите **Remove** для удаления устройства из списка.

Настройка ведения журнала для Windows Event Viewer

Вы можете выбирать сообщения журнала для отправки к программе Windows Event Viewer.

1. В разделе **Windows Event Viewer** выберите опцию **Send log messages to Windows Event Viewer**.

2. Нажмите на выпадающий список **Select a log level** для выбора уровня, назначаемому сообщениям журнала:

   * **Error (ошибка)**

   *** Warning (предупреждение)**

   *** Information (информация)**

   *** Debug (отладка)**

Сохранение сообщений журнала в файл

Вы можете сохранить сообщения журнала в файл. Эта опция включена по умолчанию

Для изменения параметров файла журнала:

1. Если вы хотите сохранять сообщения журнала в файл, то убедитесь, что опция **Send log messages to a file** включена

2. Нажмите **Browse** для выбора каталога, в котором вы хотите сохранить файл

3. Нажмите на выпадающий список **Select a log level** для выбора уровня, назначаемого сообщениям:

   Error (ошибка)

   Warning (предупреждение)

   Information (информация)

   Debug (отладка)

Перемещение каталога с данными журнала

Вы можете использовать мастер установки WatchGuard Server Center Setup Wizard для выбора нового каталога, в котором будут сохраняться файлы журнала. Сервер Журналов затем сохраняет все файлы данных в этот каталог. После этого мастер завершит свою работу, и вы не сможете изменить этот каталог из приложений WatchGuard Server Center.

Для того чтобы изменить каталог, в который будут сохраняться файлы журнала, вам необходимо снова запустить мастер настройки Сервера Журналов. Для этого внесите необходимые изменения в файл *wlserver.ini* и откройте мастер WatchGuard Server Center Setup Wizard

В мастере вы можете указать новый каталог, в котором будут сохраняться файлы журнала. После этого Сервер Журналов будет сохранять данные в журнала в новый каталог, однако вам необходимо еще вручную перенести данные из старого каталога.

Мастер WatchGuard Server Center Setup Wizard содержит набор страниц, который зависит от того, какие серверные компоненты у вас уже установлены

Инструкции, описанные ниже, рассчитаны, что на вашем компьютере установлены только Сервер Журналов, Сервер Управления и Сервер Отчетов.

Если у вас уже установлены другие сервера WatchGuard, то дополнительные опции могут появиться в мастере установок.

Более подробную информацию об этих страницах см. Set up WatchGuard System Manager Servers

Сервер Журналов и Сервер Отчетов используют базу данных PostgreSQL. Если они у вас установлены на одном компьютере, то при перемещении базы данных для Сервера Журналов, вы также переместите базу данных для Сервера Отчетов

Шаг 1 — Остановка сервисов

1. Откройте WatchGuard Server Center.
2. Остановите и запустите серверы WatchGuard.
3. Закройте WatchGuard Server Center.
4. Остановите сервисы PostgreSQL-8.2.
5. В Панели Управления Windows выберите **Administrative Tools > Services**.
   Откроется окно Services.
6. Выберите **PostgreSQL-8.2** и нажмите **Stop**.
   Сервисы остановятся.

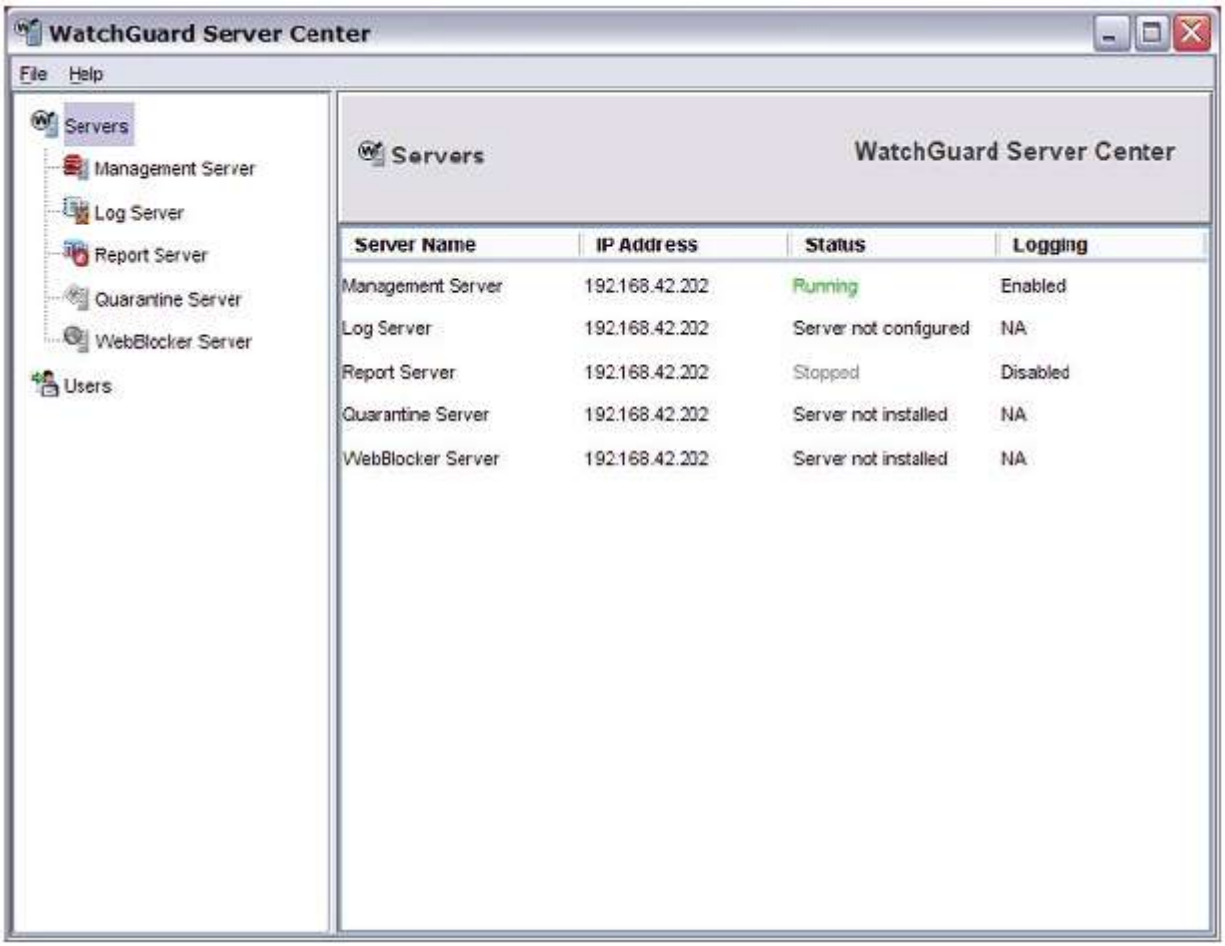
Шаг 2 — Перемещение данных файла

1. Создайте новый каталог для данных журнала. Например, *E:\WatchGuard\log_directory\logs*.
2. Перейдите к текущему каталогу данных журнала и скопируйте целиком папку. Убедитесь, что все папки и файлы были включены в каталог. Например, перейдите в каталог *C:\Documents and Settings\WatchGuard\logs* и скопируйте подкаталог *\data* и все его файлы
3. Вставьте скопированные файлы в новый каталог. Убедитесь, что вы скопировали все необходимые данные

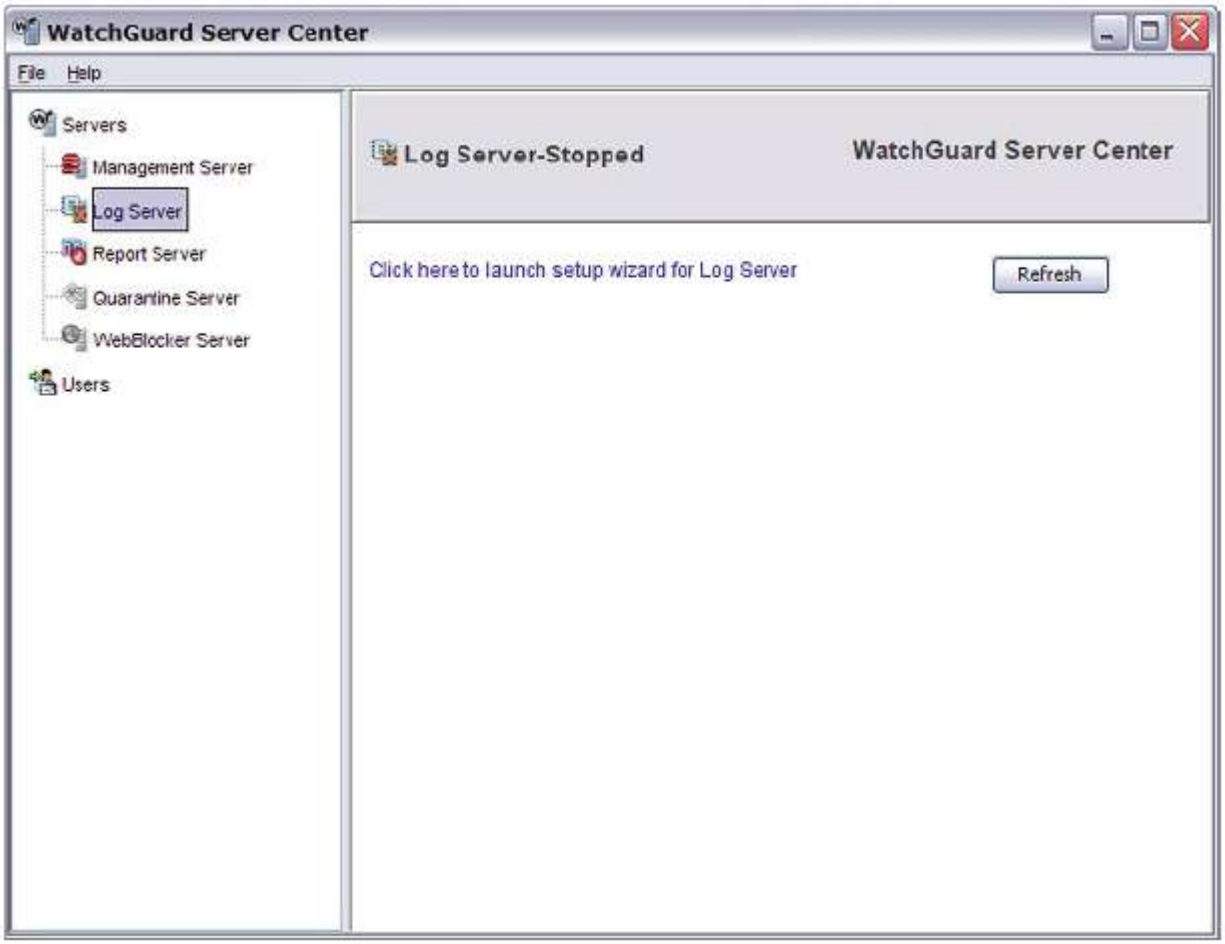
Шаг 3 — Запуск мастера Setup Wizard

1. Откройте файл *C:\Documents and Settings\WatchGuard\wlogserver\wlogserver.ini* и измените значение **WizardSuccess** на **“0”**.
2. Удалите файл: *\Program Files\WatchGuard\wsm11.0\postgresql\install\pg_install.ini*.

3. Откройте WatchGuard Server Center. **Status** для Сервера Журнала – **Server not configured**



4. В меню **Servers** выберите **Log Server**.
   Откроется диалоговое окно Log Server



5. Для запуска мастера установок WatchGuard Server Center Setup Wizard для Сервера Журнала нажмите **Click here to launch setup wizard for Log Server**.
   Откроется сообщение WatchGuard Server Center Setup Wizard.

6. Нажмите **OK** для запуска мастера установок.
   Откроется диалоговое окно WatchGuard Server Center Wizard.

7. Нажмите **Next** для начала работы с мастером установок.
   Откроется страница Log Server.

8. Введите и подтвердите тот же ключ шифрования **Encryption key,** который вы установили при первоначальном завершении WatchGuard Server Center Setup Wizard.

9. В поле **Database location** выберите новую директорию расположения данных журнала, созданную в шаге 2, описанном выше. Не включайте папку *\data*.
   Например, E:\WatchGuard\log_directory\logs.

10. Нажмите **Next**.

11. Завершите работу мастера WatchGuard Server Center Wizard.
    Мастер установит программу PostgreSQL и настроит Сервера Журнала с новой директорией расположения Сервера Журнала.

Финальный шаг

1. На странице **Log Server** нажмите **Refresh**.
   Сервер Журнала запустится и откроется страница конфигурации Сервера Журнала.

2. Перезагрузите Сервер Отчета.

Запуск и остановка Сервера Журнала

Вы можете вручную запускать или останавливать сервисы Сервера Журнала в любое время. Вам не следует отключаться от вашего Сервера Журнала. Для запуска сервиса в WatchGuard Server Center необходимо выполнить:

1. Выберите **Log Server** в меню **Servers**.

2. Нажмите правой кнопкой на **Log Server** и выберите **Start Server**.
Сервисы запустятся, и Сервер Журнала откроется в верхней части страницы Сервер Журнала

Для остановки работы сервисов в WatchGuard Server Center:

1. Выберите Log Server в меню Servers.

2. Правой кнопкой мыши нажмите на **Log Server** и выберите **Stop Server**.
Откроется предупреждающее сообщение.

3. Нажмите **Yes** для подтверждения намерения остановить сервис Сервера Журнала.
Сервис остановится, и сообщение об остановки Сервера Журнала появится в верхней части страницы.

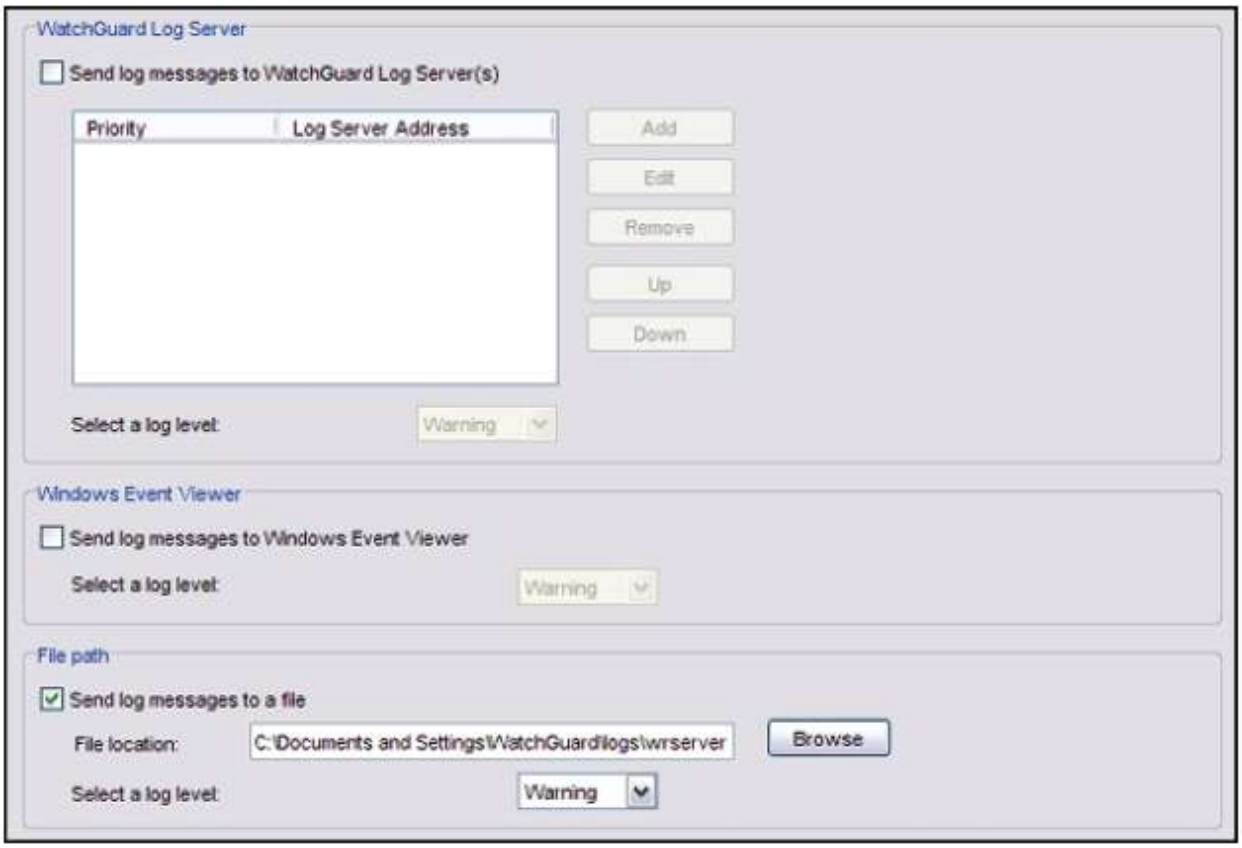
Настройка параметром ведения журнала для серверов WatchGuard

На страницах **Logging** WatchGuard Server Center для Сервера Управления, Сервера Отчета и Сервера Карантина вы можете выбрать место, куда будут отправлять данные журнала: Сервер Журналов, Windows Event Viewer и/или файл

В WatchGuard Server Center:

1. В меню **Servers** выберите сервер для настройки.

2. Нажмите на закладку **Logging**.
   Откроется страница Logging.



3. Используйте следующий раздел для настройки параметров вашего сервера.

4. При завершении работы нажмите **Apply** для сохранения изменений.

Настройка ведения журнала на Сервере Журнала WatchGuard

Вы можете выбрать для отправки сообщения от ваших серверов к одному или более Серверам Журнала WatchGuard.

При добавлении одного и более Серверов Журнала вы можете использовать список приоритетов Сервера Журнала для определения порядка, в котором сервер будет подключаться к каждому Серверу Журнала.

Если сервер не может подключиться к Серверу Журнала с наивысшим приоритетом (Приоритет 1), то происходит переход к следующему Серверу Журнала в списке.

Если сервер просматривает каждый Сервер Журнала в списке и не может подключиться, то происходит попытка подключения снова и снова к первому в списке Серверу Журнала.

Для определения ведения журнала:

1. В разделе **WatchGuard Log Server** выберите опции **Send log messages to WatchGuard Log Server(s)**.

2. Нажмите **Add** для добавления Сервера Журнала в список.
   Откроется диалоговое окно Add Log Server.

3. Введите IP-адрес. Введите и подтвердите ключ шифрования для Сервера Журнала.

4. Нажмите **OK**.
   Сервер Журнала появится в списке.

5. Для добавления другого Сервера Журнала повторите шаги 2-4.

6. Для изменения информации для Сервера Журнала выберите сервер из списка и нажмите **Edit**.

7. Для изменения приоритета сервера в списке выберите сервер и нажмите **Up** или **Down**.
   Выбранный Сервер Журнала переместится вверх/вниз в списке Приоритет.

8. Для удаление сервера из списка выберите сервер и нажмите **Remove**.

9. Нажмите на выпадающий список **Select a log level** для выбора уровня, назначаемого сообщениям журнала:

   * **Error (ошибка)**

   *** Warning (предупреждение)**

   *** Information (информация)**

   *** Debug (отладка)**

Для отключения ведения журнала в Сервере Журнала WatchGuard отключите опцию **Send log messages to WatchGuard Log Server(s)**

Настройка ведения журнала в Windows Event Viewer

Вы можете выбрать сообщения журнала для отправки в Windows Event Viewer.

1. В разделе **Windows Event Viewer** выберите опцию **Send log messages to Windows Event Viewer**.

2. Нажмите на выпадающий список **Select a log level** для выбора уровня, назначаемого сообщениям журнала:

   Error (ошибка)

   Warning (предупреждение)

   Information (информация)

   Debug (отладка)

Сохранение сообщений журнала в файл журнала

Вы можете выбирать сообщения журнала для сохранения в файл, доступ к которому может осуществляться позже.

Это опция включена по умолчанию.

Для изменения параметров файла журнала:

1. Убедитесь, что выбрана опция **Send log messages to a file** , если вы хотите сохранить сообщения журнала в файл.

2. Нажмите **Browse** для выбора каталога, куда сохраняется файл журнала.

3. Нажмите выпадающий список **Select a log level** для выбора уровня, назначаемого сообщениям журнала:

Error (ошибка)

Warning (предупреждение)

Information (информация)

Debug (отладка)

Выбор места, куда Firebox будет отправлять данные журнала

Вы можете настраивать ваш Firebox для записи в журнал событий, которое произошло на устройстве. Затем анализируя файлы журнала вы можете значительно повысить уровень безопасности вашей системы. Вам необходимо указать, куда Firebox будет отправлять сообщения журналов.

1. В Policy Manager выберите **Setup > Logging**.
   Откроется диалоговое окно Logging Setup

2. Настройте необходимые параметры для Сервера Журнала, syslog сервера и внутреннего хранилища Firebox Internal Storage. Ниже приводится описание доступных опций.

   WatchGuard Log Server

   Для того чтобы устройство Firebox отправляло сообщения журнала на Серверы Журналов включите опцию **Send log messages to the log servers at these IP addresses**. Firebox может одновременно отправлять сообщения на Сервер Журналов и syslog сервер. Нажмите **Configure** и введите IP-адреса ваших Серверов Журналов

   Syslog Server

Для того чтобы устройство Firebox отправляло сообщения журнала на syslog сервер включите опцию **Send log messages to the Syslog server at this IP address**. Firebox может одновременно отправлять сообщения на Сервер Журналов и syslog сервер. Нажмите **Configure** и введите IP-адреса ваших syslog серверов

Firebox Internal Storage

Для того чтобы устройство Firebox сохраняло сообщения журнала во внутреннем хранилище включите опцию **Send log messages in Firebox internal storage**.

Performance Statistics

По умолчанию Firebox отправляет сообщения журнала с информацией о работе интерфейсов External и статистике использования пропускной способности VPN

Diagnostic Log Level

Для более подробной информации о том, как установить необходимый уровень сообщений диагностики, которые будут записываться в журнал и в Traffic Monitor см. “Установка уровня диагностики ведения журнала”

3. Для отправки сообщения журнала при изменениях конфигурации устройства включите опцию **Send log messages when the configuration for this Firebox is changed**.

4. Нажмите **OK**.

Добавление Сервера Журнала

Если вы включите опцию **Send log messages to the log servers at these IP addresses,** при определении места отправки сообщений журнала Firebox, вы можете добавить несколько дополнительных Серверов Журналов.

1. В Policy Manager выберите **Setup** > **Logging**.
   Откроется диалоговое окно Logging Setup

2. В разделе Сервер Журнала WatchGuard включите опцию **Send log messages to the log servers at these IP-адрес addresses**.

3. Нажмите **Configure**.
Откроется диалоговое окно Configure Log Servers

4. Нажмите **Add**.
Откроется диалоговое окно Add Event Processor

5. В поле **Log Server Address** введите IP-адрес Сервера Журнала, который необходимо добавить.

6. В текстовых полях **Encryption Key** и **Confirm Key** введите ключ шифрования Сервера Журналов, который вы создали при его настройке. Допустимый диапазон для ключа шифрования составляет 8-32 символа. Вы можете использовать все символы, кроме пробелов и косых черт (/ или \)

7. Нажмите **OK**.
Откроется диалоговое окно Add Event Processor.

Сохранение изменений и проверка ведения журнала

1. Нажмите **OK** для закрытия диалогового окна **Configure Log Servers**.

2. Нажмите **OK** для закрытия диалогового окна **Logging Setup**.

3. Сохраните конфигурационный файл

4. Для проверки того, что Firebox отправляет сообщений журнала корректно от WSM. Выберите **Tools > Firebox System Manager**.

В разделе **Detail** рядом с **Log Server** появится IP-адрес хоста журнала.

Установка приоритетов Сервера Журнала

Список приоритетов Сервера Журнала включает выбранный вами порядок, в котором Firebox подключается к вашим Серверам Журнала.

Вы можете назначить один Сервер Журнала в качестве основного (с приоритетом 1), а другие сервера – в качестве запасных. Если устройство Firebox не может подключиться к Серверу Журналов с наивысшим приоритетом, он подключается к следующему Серверу из списка с более низким приоритетом. Если Firebox не может подключиться ни к одному серверу в списке, он снова пытается подключится к первому Серверу Журналов. Когда основной Сервер Журнала не доступен, и Firebox подключается к резервному Серверу Журнала, Firebox пытается снова подключиться в основному Серверу Журнала каждые 6 минут.

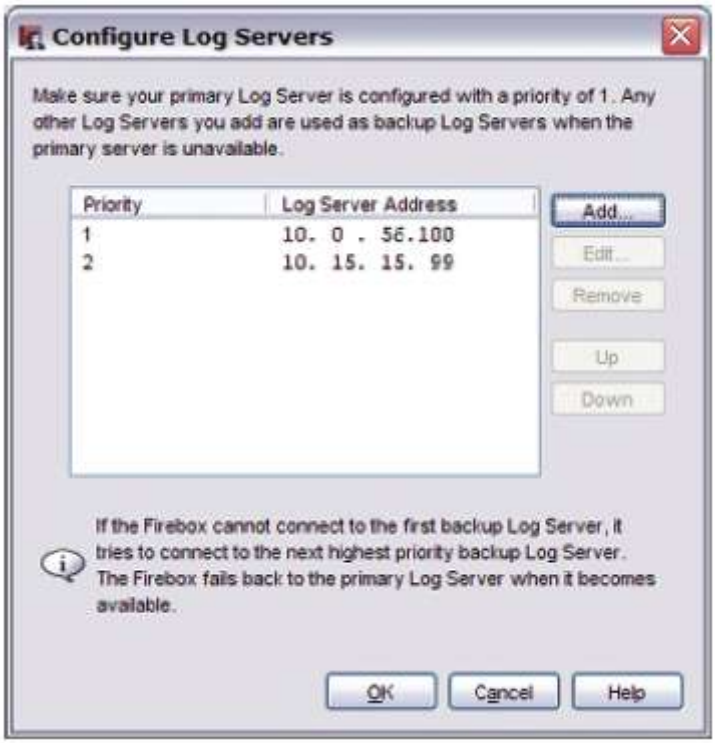
Неэффективным является тот случай, когда Firebox подключен к резервному Серверу Журнала в то время, когда основной Сервер Журнала доступен для подключения.

Для создания списка приоритетов Сервера Журнала:

1. В Policy Manager выберите **Setup > Logging**.
Откроется диалоговое окно Logging Setup.

2. В разделе Сервера Журнала WatchGuard выберите опцию **Send log messages to the Log Servers at these IP addresses**.

3. Нажмите **Configure**.
   Откроется диалоговое окно Configure Log Servers



4. Выберите Сервера Журнала из списка и нажмите **Up** или **Down** для изменения порядка.

5. Нажмите **OK**.
   Откроется диалоговое окно Logging Setup. Новый порядок приоритетов Сервера Журнала появится в списке Сервера Журнала WatchGuard.

Настройка syslog

Syslog - интерфейс, разработанный для UNIX, но также используется в других компьютерных системах. Вы можете настроить Firebox для отправки журналов на syslog-сервер. Firebox может одновременно отправлять журналы на Сервер Журналов и syslog-сервер, или отправлять журналы отдельно каждому серверу. Журналы Syslog передаются в незашифрованном виде.

Мы не рекомендуем использовать хост syslog на интерфейсе External.

1. В окне Policy Manager выберите **Setup** > **Logging**. Откроется диалоговое окно **Logging Setup**

2. В разделе Syslog Server выберите опцию **Send Log Messages to the Syslog server at this IP address**.

3. В адресном поле введите IP-адрес syslog-сервера.

4. Нажмите **Configure**.
   Откроется диалоговое окно Configure Syslog

5. Для того чтобы в сообщение журнала добавить время с вашего Firebox включите опцию **Include timestamp in Syslog message**.

6. Для того чтобы в сообщение журнала добавить серийный номер устройства Firebox включите опцию **Include the serial number of Firebox in the Syslog messages**.

7. Для каждого типа сообщения журнала выберите тип источника (“facility”), к которому вы хотите присвоить сообщение. Если вы выберите **NONE,** информация для этого типа сообщений не будет отправляться на syslog -хост. Для более подробной информации о типах сообщений журнала, см. Типы сообщений журнала. Тип источника (“facility”) syslog - это поле в syslog-пакете и файл, которому отправляются syslog-сообщения. Для сообщений с более высоким приоритетом используйте Local0, например для срочных оповещений. Для сообщений с более низким приоритетом используйте значения Local1-Local 7 (чем меньше цифра, тем выше приоритет). Для более подробной информации о типе источника (“facility”), см. документацию по серверу syslog.

8. Для отмены ваших параметров и восстановления параметров по умолчанию для syslog нажмите **Restore Defaults**.

9. Нажмите **OK** для закрытия диалогового окна **Configure Syslog**.

10. Нажмите **OK** для закрытия диалогового окна **Logging Setup**.

11. Сохраните конфигурационный файл.

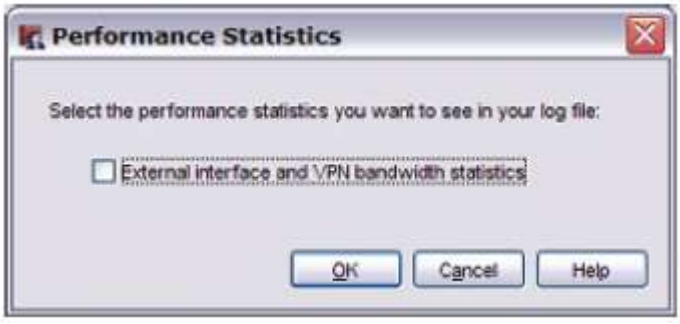
Настройка журнала для статистике по производительности

Вы можете выбрать, будут ли отображаться данные по производительности в закладке **Traffic Monitor** в Firebox System Manager. Для того чтобы посмотреть эти данные необходимо включить функцию ведения журнала для статистики. При выборе этой опции Firebox отправляет данные о производительности External интерфейса и пропускной способности VPN туннелей на ваш Сервер Журналов

Включение или отключение ведения журнала для статистики по производительности

1. В Policy Manager выберите **Setup > Logging**.
   Откроется диалоговое окно Logging Setup

2. Нажмите **Performance Statistics**.
   Откроется диалоговое окно Performance Statistics



3. Для включения ведения журнала статистики по производительности выберите опцию **External interface and VPN bandwidth statistics.**

   Для отключения ведения журнала статистики по производительности отключите опцию **External interface and VPN bandwidth statistics.**

4. Нажмите **OK**.

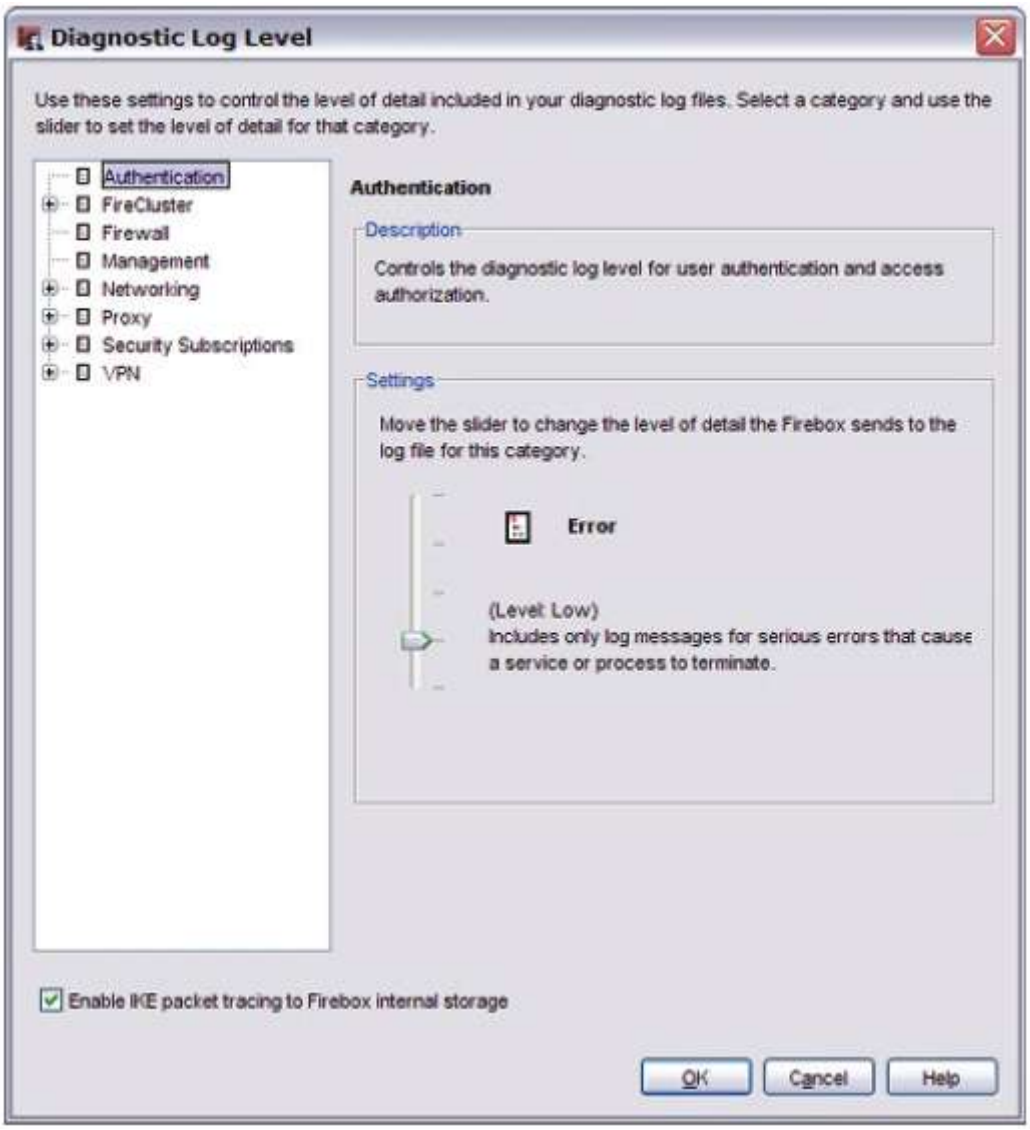
5. Сохраните конфигурационный файл.

Установка уровня диагностики ведения журнала

Вы можете выбрать уровень журналов диагностики, которые будут записываться в файл журнала или в Traffic Monitor. Мы не рекомендуем устанавливать самый высокий уровень, если только специалист службы технической поддержки не попросить вас это сделать для исправления проблемы. Установка высокого уровня для журналов диагностики приведет к быстрому заполнению файла журнала, а также создаст дополнительную нагрузку на Firebox.

1. В Policy Manager выберите **Setup > Logging**.
   Откроется диалоговое окно Logging Setup

2. Нажмите **Diagnostic Log Level**.
Откроется диалоговое окно Diagnostic Log Level



3. Выберите категорию из списка.
Описание категории появится в поле Description.

4. Используйте бегунок **Settings** для установки уровня детализации, включенной в сообщения журнала каждой категории. При выбранном **Off** (наименьший уровень) , сообщения диагностики для этой категории отключаются.

5. При включении Firebox для сбора trace пакета для IKE-пакетов выберите опцию **Enable IKE packet tracing to Firebox internal storage**.

6. Нажмите **OK** для сохранения изменений.
Откроется диалоговое окно Logging Settings.

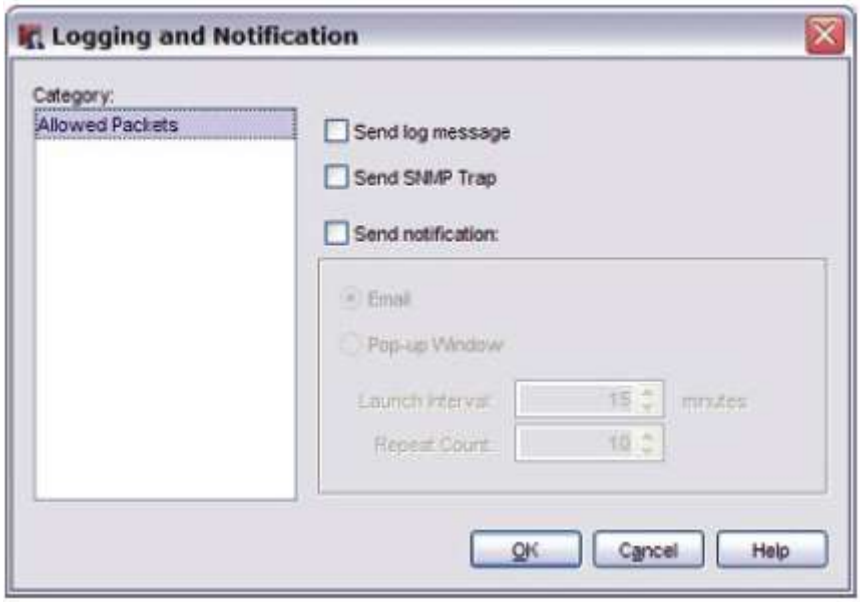
Настройка ведения журнала и уведомления для политики

Вы можете использовать Policy Manager для настройки ведения журнала и параметры уведомления для каждой политики вашей конфигурации.

1. В Policy Manager добавьте политику или дважды нажмите на политику для ее редактирования.
   Откроется диалоговое окно New Policy Properties или Edit Policy Properties

2. Нажмите на закладку **Properties**.

3. Нажмите **Logging**.
   Откроется диалоговое окно Logging and Notification

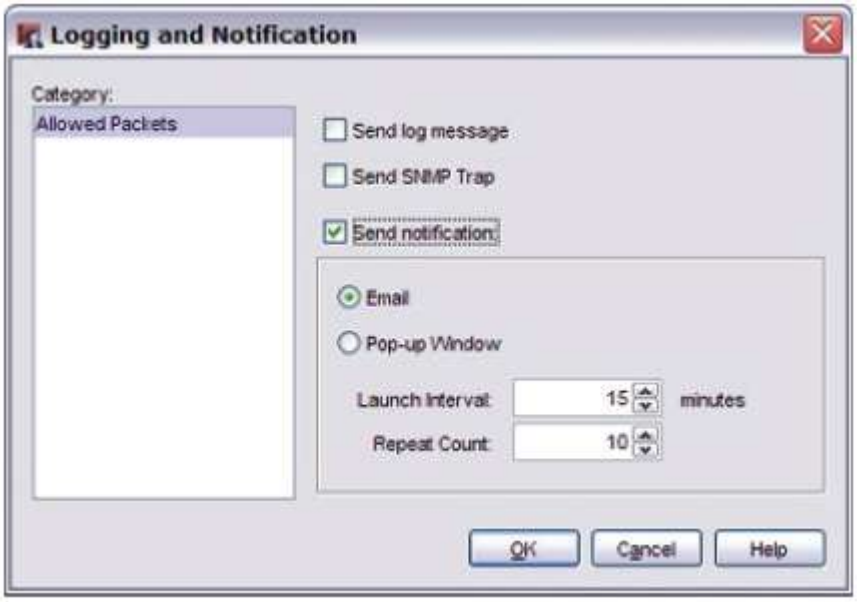


4. Установите параметры для политики безопасности

5. Нажмите **OK** для сохранения изменений.

Настройка параметров журнала и уведомлений

Параметры журнала и уведомлений одинаковы в конфигурации Firebox. Для каждого места, в котором вы определили ведение журнала и уведомления, большинство или все поля описаны ниже.



Send log message

Если вы включите эту опцию, Firebox будет отправлять сообщение при наступлении какого-либо события. Вы можете выбрать для отправки сообщений журнала на Сервер Журнала WatchGuard, Syslog-сервер или внутреннее хранилище Firebox

Send SNMP trap

Если вы включите эту опцию, то Firebox будет отправлять уведомление о событии системе управления SNMP. Протокол SNMP (Simple Network Management Protocol) – это набор утилит для мониторинга и управления сетями. SNMP ловушка – это уведомление о событии, которое Firebox отправляет системе управления SNMP

*При выборе опции **Send SNMP Trap** и при ненастроенном SNMP появится диалоговые окна, и система спросит, хотите ли вы это настроить SNMP. Нажмите **Yes,** чтобы перейти к диалоговому окну **SNMP Settings.** Вы не можете отправлять SNMP-ловушки при ненастроенном SNMP.*

Send notification

Если вы включите эту опцию, то Firebox будет отправлять уведомление после каждой блокировки пакета данных. Для более подробной информации о настройке уведомлений см. About notification. Вы можете настроить ваш Firebox для выполнения одного из следующий действий:

- **Email** — При наступлении какого-либо события Сервер Журналов отправляет электронное письмо.
- **Pop-up Window** — При наступлении какого-либо события Firebox генерирует всплывающее окно на станции управления.
- **Launch Interval** — Минимальное время (в минутах) между различными уведомлениями. Варьируя значением этого параметра, вы можете избегать ситуаций, когда для одного и того же события сгенерируется более одного уведомления.
- **Repeat Count** — Этот параметр отслеживает частоту возникновения события. Когда количество событий достигает выбранной величины, запускается специальное повторное уведомление. Это уведомление создает запись повтора в журнале с информацией об этом уведомлении.

Уведомление повторяется снова после того, как количество событий опять достигнет этой величины. Пример использования этих двух параметров. Значения параметров следующие:

- Launch interval = 5 минут
- Repeat count = 4

Сканирование портов начинается в 10:00 часов утра и повторяется каждую минуту. Это запускает процедуры ведения журнала и уведомлений. Ниже приводятся время и произошедшие события:

1. 10:00— Первая попытка сканирования портов (первое событие)
2. 10:01— Первое уведомление (одно событие)
3. 10:06— Второе уведомление (сообщает о 5 событиях)
4. 10:11— Третье уведомление (сообщает о 5 событиях)
5. 10:16— Четвертое уведомление (сообщает о 5 событиях)

Параметр **Launch Interval** управляет интервалами между событиями 1, 2, 3, 4 и 5. Значение параметра равно 5 минутам. Умножьте значение параметра Repeat Count на значение Launch Interval. Это и будет промежуток времени.ю после которого будет запущено уведомление повторения.

Использование скриптов, утилит и стороннего программного обеспечения с Сервером Журналов

Вы можете использовать некоторые скрипты, утилиты и приложения из командной стоки для совершения точных заданий Сервера Журнала. Вы можете так же использовать некоторые

сторонние программы с Сервером Журнала. Эти задачи разработаны для помощи в проблемах, которые влияют на нормальную работу Сервера Журнала. WatchGuard не поддерживает использование этих скриптов и утилит для процедур. Используйте их с осторожностью.

Вы можете использовать скрипты, утилиты, приложения и сторонние программы для:

- резервирование и восстановления базы данных Сервера Журнала
- восстановления резервной копии файла журнала
- импорт файла журнала на Сервера Журнала
- использование Crystal Reports с Сервером Журнала

В коде примеров, показанных в этой теме, *backup.db* используется в качестве имени по умолчанию для файла содержимого вашей базы данных. Вы можете выбрать различные имена файлов при выполнении процедуры. Дополнительно, буквы X используется в пути имени для обозначения букв и имен, которые могут быть различны для каждого пользователя.

Например, если путь имени содержит каталог *wsm11.x,* вам следует искать каталог в похожим именем, таким, как *wsm11.0.* Если у вас есть несколько версий WatchGuard System Manager и установлен Fireware XTM, вы можете повторить процедуры для каждой версии.

Резервирование и восстановления базы данных Сервера Журнала

Вы можете использовать утилиту *pg_dump* для создания файла, который содержит базу данных Сервера Журнала. Этот файл называется *dump-файл.* Вы можете использовать этот файл для восстановления базы данных текущего сервера или перемещать Сервер Журнала на другой сервер.

1. Откройте командную строку. Введите *cd \Program Files\WatchGuard\wsm10.x\postgresql\bin* И нажмите **Enter** для изменения вашего рабочего каталога.
   Используйте соответствующую версию для вашего установленного WSM.

2. Введите *pg_dump -v -f "c:\db.backup" -F c -Z 5 -U wguser wglog* и нажмите **Enter**.

3. По требованию введите пароль администратора.
   Содержимое вашей базы данных Сервера Журнала сохраняется в определенном пути и имени файла в рабочем каталоге (выбранном в шаге 1).

4. Если вы хотите переместить базу данных Сервера Журнала на другой компьютер, переместите каталог данных журнала и установите Сервера Журнала. Скопируйте резервный файл на новый компьютер Сервера Журнала и остановите Сервер Журнала.

5. В командной строке измените ваш рабочий каталог на каталог, в котором находится файл *backup.db*. Например, вы можете сохранить dump-файл базы данных в корневом каталоге C: drive, введите *cd* \ и нажмите **Enter** для изменения вашего рабочего каталога на расположение файла.

6. Для восстановления резервной базы данных на новом компьютере с Сервером Журнала, на котором не создана база данных, введите pg_restore -U wguser -v "c:\db.backup" -C -d wglog и нажмите **Enter**. Если понадобиться, введите пароль администратора и снова нажмите **Enter**. База данных создается и содержание резервного файла импортируется в новый Сервер Журнала. Для восстановления резервной базы данных на текущем компьютере с Сервером Журнала с уже имеющейся базой данных введите pg_restore -U wguser -v "c:\db.backup" -c -d wglog и нажмите **Enter**. При необходимости введите пароль администратора и нажмите **Enter**.
   База данных Сервера Журнала запишется вновь с содержанием dump-файла базы данных.

7. Запустите Сервер Журнала.

Восстановление резервной копии файла журнала

Вы можете восстановить резервную копию файла журнала на ваш Сервер Журналов. Для того чтобы восстановить данные журнала вам необходимо будет предварительно настроить ваш Сервер Журналов.

Если вы включите автоматическое резервирование сообщений журнала, то Сервер Журнала будет сохранять содержимое базы данных в CSV файл в указанном каталоге. Для каждого устройства, которое генерирует журналы и отправляет их на Сервер Журналов, создается набор из 4 файлов. При восстановлении файлов журналов с резервного сервера, вам необходимо конвертировать и импортировать весь набор файлов .

Для того чтобы восстановить ваши данные журнала на Сервере Журналов необходимо сперва преобразовать файл CSV в XML при помощи утилиты `wlconvert.exe`.

Если у вас настроен вторичный Сервер Журналов, то файлы журнала с каждого сервера находятся в отдельном файле CSV

wlconvert.exe – утилита командной строки. Перед тем как преобразовать файлы при помощи утилиты `wlconvert` вам необходимо знать следующие два параметра: -d (directory) и -f (filename). directory - это каталог, в котором хранятся резервные файлы. Является дополнительным аргументом. Filename - sn_timestamp часть имени файла для каждого из четырех файлов, где sn – серийный номер устройства и timestamp – дата в формате *YYYYMMDDhhmmss*.

Например, если резервные файлы Сервера Журналов находятся в каталоге **C:\old_logs** и значение параметра sn_timestamp для файла равно **209188121122_0070731000006**. Тем самым аргументы можно записать так: **-d C:\old_logs -f 209188121122_0070731000006**.

Для того чтобы преобразовать эти файлы в необходимый формат, выполните следующее:

1. Для изменения вашей текущей директории в командной сроке введите *cd \Program Files\WatchGuard\wsm11.0\wlcollector\bin* и нажмите Enter.

2. Введите *wlconvert -d <directory> and -f <filename>*.
   Используйте каталог и информацию об имени файла для вашего Сервера Журнала.

3. Нажмите **Enter** на вашей клавиатуре. Набор четырех файлов преобразуется в один XML файл, имя которого равно значению параметра sn_timestamp. Например, 209188121122_0070731000006.xml. Новый XML файл появляется в том же каталоге, что и CSV-файлы.

После того как вы преобразовали файлы в XML формат, вы можете импортировать XML файл на Сервер Журналов при помощи утилиты `wlimport.exe`.

Импорт файла журнала на Сервер Журналов

Вы можете импортировать XML файлы журнала на Сервер Журналов при помощи утилиты `wlimport.exe`. Резервные файлы Сервера Журнала могут быть в CSV –формате.

Если вы хотите восстановить ваши резервные копии файлов журнала, сначала необходимо преобразовать CSV файлы в XML

`wlimport.exe` – это утилита командной строки. Для импорта файлов журнала вам необходимо ввести значения двух аргументов:

-e (ключ шифрования журналов) и -i (значение поля **Display Name** для Сервера Журналов). Для импорта XML файла журнала:

1. Для изменения текущего рабочего каталога в командной строке введите *cd \Program Files\WatchGuard\wsm11.x\wlcollector\bin* и нажмите Enter. Замените .x в пути, указанном выше, на версию установки WSM.

2. Введите *wlimport -e <log encryption key> -I <log server display name>*. Используйте ключ шифрования и отображаемое имя для вашего Сервера Журнала.

3. Нажмите **Enter** на вашей клавиатуре.

XML файл будет импортирован на ваш Сервер Журналов, и откроется счетчик, который покажет количество импортированных записей. Процедура импорта займет несколько минут. Количество времени зависит от размера файлов журнала.

После того, как импорт файла будет завершен, вы можете при помощи утилиты LogViewer посмотреть файлы журнала

Использование Crystal Reports с Сервером Журнала

Если ваша организация использует Crystal Reports, вы можете применять базы данных Сервера Журнала в качестве источника информации. Вам следует установить программное обеспечение от сторонней фирмы для этого функционала. Так же мы рекомендуем устанавливать Crystal Reports на отдельном компьютере от Сервера Журнала для лучшей производительности.

В этих процедурах мы использует IP-адрес Сервера Журнала - 192.168.0.1, и IP-адрес удаленного клиента - 192.168.0.2. Это только пример IP-адресов. Убедитесь, что вы заменили их на корректные IP-адреса вашего Сервера Журнала и удаленного клиента при завершении этих процедур.

Вам необходим только аргумент информации *–i* для импорта XML-файлов из старого Сервера Журнала в новый.

Если вы хотите импортировать резервные файлы из вашего текущего Сервера Журнала, то аргумент –i не требуется.

Настройка компьютера для вашего Сервера Журнала

1. Остановите Сервер Журнала и сервисы базы данных PostgreSQL.

2. Откройте файл конфигурации PostgreSQL в текстовом редакторе.
   C:\Documents and Settings\WatchGuard\logs\data\postgresql.conf

3. Для обеспечения соединения с базами данных других компьютеров в файле измените параметры Сервера Журнала **listen_addresses** на:

   listen_addresses = '*'

   или

   listen_addresses = 'localhost, 192.168.0.1'

   если необходимо, переместите символ комментария (#) от начала строки.

4. Сохраните **postgresql.conf**.

5. Откройте файл **pg_hba.conf**.

6. Добавьте строку, похожую на:
   host all all 192.68.0.2/32 md5

   в примере 192.168.0.2 – это адрес удаленного клиент, от которого вы хотите получить доступ.

7. Перезагрузите PostgreSQL и сервисы Сервера Журнала.

Настройка компьютера с Crystal Reports

1. Установите Crystal Reports на отдельном от Сервера Журнала компьютере.

2. Загрузите и установите драйвер ODBC для PostgreSQL.
3. В меню Windows Start выберите **Control Panel** > **Administrative Tools** > **Data Sources** (**ODBC**).
4. В закладке **User DSN** нажмите **Add**.
5. Выберите **PostgreSQL Unicode**.
6. настройте соединение со следующими параметрами:

   Data Source — PostgreSQL30W

   Database — wglog

   Server — 127.0.0.1

   Port — 5432

   User name — wguser

   Password — [пароль сервера управления]
7. Нажмите **Test** для проверки соединения.
8. Откройте Crystal Reports.
9. Выберите **Database** > **Log On or Off Server** > **Create New Connection** > **ODBC (RDO)**.
10. Выберите источник данных, созданный в шага- 3-7 и создайте соединение.

Использование LogViewer для просмотра файлов журнала

LogViewer – утилита WatchGuard System Manager для просмотра файлов журналов. Утилита предоставляет пользователю возможность просматривать данные постранично, выполнять поиск и отображать данные в зависимости от указанных ключевых слов или имен полей

Открытие LogViewer

1. Откройте WatchGuard System Manager.

2. Нажмите на  в панели инструментов WatchGuard System Manager. Или выберите **Tools > Logs > LogViewer**.
Откроется диалоговое окно WatchGuard LogViewer

Подключение к устройству

Вы можете подключаться к устройствам Firebox, FireClusters или Серверам Журналов. При подключении к Firebox вы можете фильтровать данные по типу сообщений, времени и дате, и также выполнять поиск по ключевым словам.

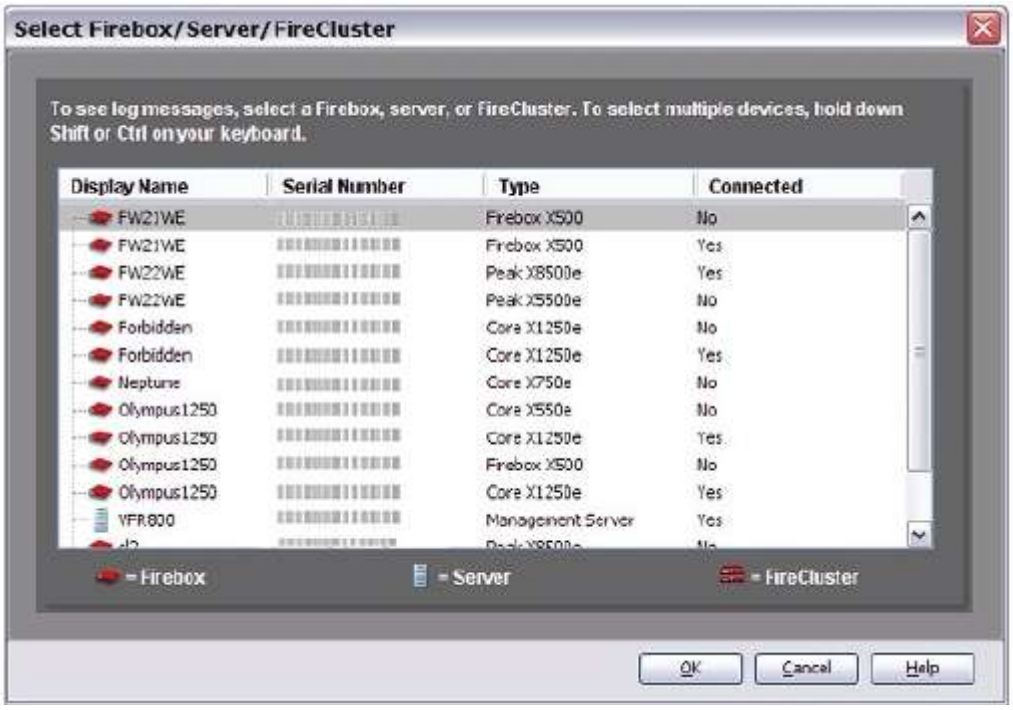
При подключении к Серверу Журнала, вы можете фильтровать данные по времени и дате или выполнять простой поиск по ключевым словам

1. Нажмите на  в панели инструментов LogViewer. Или выберите **File** > **Connect to Log Server**.
Откроется диалоговое окно Connect to Log Server.

2. Введите IP-адрес, имя пользователя и пароль для вашего Сервера Журнала.

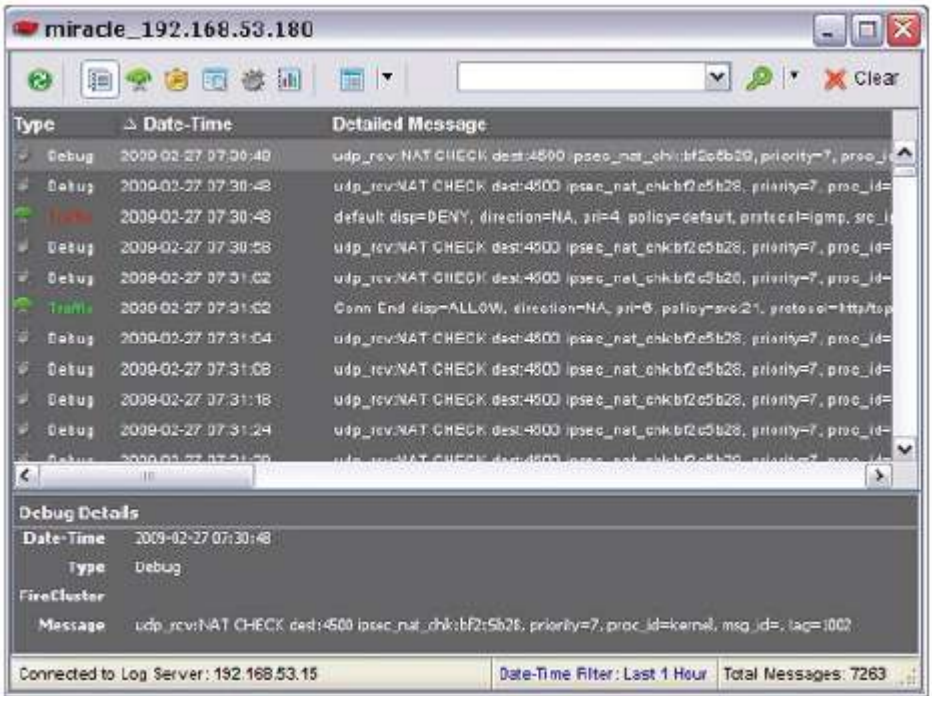
3. Нажмите **Login**.
Диалоговое окно Connect to Log Server закроется. Откроется диалоговое окно Select Firebox/Server/FireCluster

   Если вы впервые подключаетесь к этому устройству, серверу или кластеру, то появится Certificate Warning. Вам следует принять сертификат для продолжения и подключения.



4. Выберите один или более устройств Firebox , Сервера Журнала или FireClusters из списка и нажмите **OK**. Для выбора нескольких устройств удерживайте Shift или Control на вашей клавиатуре. Окно устройства откроется для каждого выбранного устройства. IP-адрес устройства появится в заголовке меню.

   Содержание окна Firebox и окна Server – отличаются



5. Выберите сообщение журнала для просмотра более подробной информации о нем. *Выбранное сообщение журнала появится на панели Details в нижней части окна устройства.*

6. Если панель Details не отображается, выберите **View > Details Pane,** чтобы ее включить.

Открытие журналов для Основного Сервера Журналов

Если вы указали Основной Сервер Журналов, вы можете открыть файлы журнала для этого сервера прямо из LogViewer без подключения к нему. Вы также можете посмотреть список устройств Firebox, которые в данный момент отправляют свои журналы на Основной Сервер Журналов.

Для того чтобы использовать эту опцию вам необходимо выбрать Основной Сервер Журналов

Для того чтобы открыть журналы для основного Сервера Журналов, выполните следующее:

1. Откройте Open Log Viewer.

2. Нажмите на  в панели инструментов LogViewer. Или выберите **File** > **Open Logs For**.
   Откроется диалоговое окно Select Firebox/Server/FireCluster со списком подключенных устройств.

Настройка параметров пользователей LogViewer

Вы можете настроить содержимое и формат окна LogViewer. Вы можете выбрать основной Сервер Журнала LogViewer для автоматического подключения и настройки содержимого в параметрах величины Search. Вы можете так же настроить появление окна LogViewer, выбрать типы журналов для появления и деталей, включенных для каждого типа сообщения.

Для установки параметров пользователя LogViewer:

1. В LogViewer выберите **View > Preferences**.
   Откроется диалоговое окно User Preferences.

2. Выберите закладку для настройки окна LogViewer .

   * закладка **General** включает опции для параметров основного Сервера Журнала и параметров поиска.

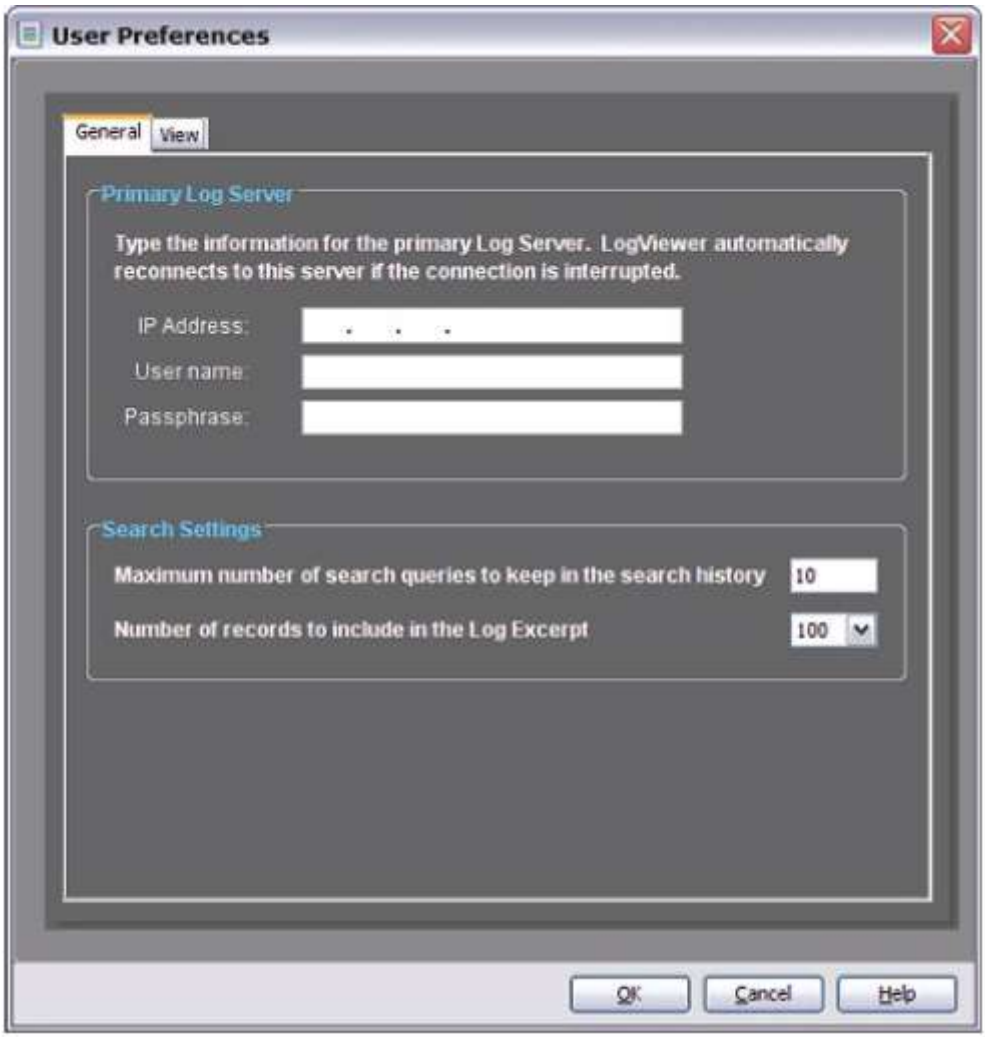
   * закладка **View** включает опции для настройки окна LogViewer и колонки параметров для поиска типа сообщения журнала.

Настройка основного Сервера Журнала и параметров Поиска

Вы можете определить Сервер Журнала для автоматического переподключения LogViewer и настроить параметры для величины Search в LogViewer.

В диалоговом окне **User Preferences**:

1. Выберите закладку **General**



2. Если вы хотите автоматически переподключать LogViewer к определенному Серверу Журналов, в разделе **Primary Log Server** введите IP адрес (**IP Address)**, имя пользователя (**User name**) и пароль (**Passphrase**) для вашего основного Сервера Журналов. Если вы не хотите указывать основной Сервер Журналов, оставьте поле пустым.

3. В разделе **Search Settings** введите максимальное количество поисковых запросов в вашей истории поиска.

4. Выберите **Number of records to include in the Log Excerpt** из выпадающего списка.

Настройка окна LogViewer и параметров колонки

Вы можете так же определить информацию, которая будет отображаться в окне LogViewer. В диалоговом окне **User Preferences**:

1. Выберите закладку **View**

2. В выпадающем списке **Default log type** выберите тип сообщений журнала, который вы хотите добавить по умолчанию.

3. Выберите, требуется ли отображать параметры сообщений журнала (опция **Show log message details**)

4. Выберите размер шрифта, который вы хотите использовать для записей журнала из выпадающего списка **Log table entry font size.**

5. Выберите **Column Settings** для включения каждого типа сообщения журнала. Каждая закладка включает список доступных деталей для данного типа сообщения. Используйте эти закладки, чтобы выбрать, какие столбцы с деталями появятся для каждого сообщения. Нажмите **Up** или **Down** для изменения порядка столбцов.

6. Нажмите **OK**.

Поля сообщений журнала

При помощи колонок вы можете выбрать, какие параметры сообщения необходимо будет включить в сообщение журнала. Ниже приводится список доступных колонок. Для некоторых типов сообщений отображаться будут не все колонки.

Колонка сообщения журнала	Описание
Additional Info	Дополнительная информация о сообщении для журналов прокси. Например: hostname, filename, rule_name, content_type.

Alarm ID	Номер тревоги.
Alarm Name	Категория тревоги (System, IPS, AV, Policy, Proxy, Probe, Denial of service, or Traffic).
Alarm Type	Тип тревоги (email, popup).
Application Provider	Имя сервер, который предоставляет данные.
Bytes Received	Количество байт, полученных устройством (WAN или Tunnel).
Bytes Sent	Количество байт, отправленных устройством (WAN или Tunnel) в период генерации статистики по журналам
Connection ID	Идентификатор подключения.
DateTime	Дата и время (на сервере) получения сообщения журнала.
Destination Interface	Имя интерфейса назначения.
Destination IP	IP-адрес назначения.
Destination IP-NAT	Способ обработки NAT (network address translation) для IP-адреса данного пакета.
Destination Port	Порт назначения для данного пакета.
Destination Port-NAT	Способ обработки NAT (network address translation) для порта назначения этого пакета.
Detailed Message	Все поля сообщения, разделенные запятыми
Device	Имя устройства, которое отправило журнал производительности (WAN или Tunnel).
Direction	Направление действия: входящее или исходящее.
Disposition	Диспозиция пакета: deny или allow.

Message	Поле сообщения.
Message Code	Код типа сообщения.
Message Timestamp (s.ms)	Временная метка для сообщения в формате «секундах.миллисекунды».
Misc. Details	Дополнительная информация о выбранных колонках. Например: RC (return code – код возврата), длина пакета и TTL (время жизни пакета в секундах).
Policy	Имя политики в Policy Manager, которая отвечает за обработку этого пакета.
Priority	Уровень приоритета сообщения.
Process ID	ID процесса, который был выполнен в действии сообщения.
Protocol	Протокол, используемый в пакете.
Proxy Action	Имя действия прокси, которое обрабатывает данный пакет. Действие прокси – это набор правил для прокси, которые можно применить для нескольких политик.
Request ID	ID серверного процесса, запрошенного в сообщении.
Return Code	Код возврата пакета.
Source Interface	Имя интерфейса источника для данного пакета (см. в Policy Manager).
Source IP	IP-адрес источника.
Source IP-NAT	Способ обработки NAT (network address translation) для IP адреса источника для этого пакета
Source Port	Порт источника.
Source Port-NAT	Способ обработки NAT (network address translation) для порта источника для этого

	пакета
Type	Тип сообщения журнала. Все сообщения журнала содержат тип сообщения: "al" для тревог, "ev" для событий, "db" для отладки, "pe" для сообщений статистики, “tr” для Traffic.

Утилита Search Manager

При помощи утилита LogViewer Search Manager вы можете создавать правила для поиска данных LogViewer. Вы можете создавать свое собственное правило и затем многократно его использовать. Вы также можете удалять или редактировать правила и очищать историю поиска.

Запуск Search Manager

1. Откройте LogViewer.

2. Нажмите на  в панели инструментов LogViewer. Или выберите **Tools** > **Search Manager**. *Откроется диалоговое окно Search Manager*

Создание Search Query

1. Нажмите на **Add Search** на панели **Tasks**.

2. Введите имя для вашего поиска в поле **Name**.

3. Выберите **Search Parameters**.

Сохранение поиска

После того, как вы создали запрос поиска, вы можете сохранить его для запуска вновь. Нажмите **Save Search** на панели **Tasks**.
Имя поиска появится в списке My Searches.

Удаление поиска

Если вы не хотите сохранять уже использованные поиски в списке **My Searches,** вы можете удалить их. Вы можете удалить только один сохраненный поиск за раз.

1. Выберите поиск в списке **My Searches**.

2. Нажмите **Remove Search** на панели **Tasks**.
Имя поиска исчезнет их списка My Searches.

Редактирование поиска

Вы можете редактировать сохраненные поиски для изменения их параметров.

1. Выберите имя поиска в списке **My Searches**.
Выбранное имя поиска появится в поле Name.

2. Измените параметры поиска.

3. Нажмите **Save Search** на панели **Tasks**.
Откроется сообщение Save Search.

Запуск поиска

Вы можете запустить сохраненный или новый запрос поиска. Для запуска сохраненного поиска:

1. Выберите имя запроса в списке **My Searches**.

2. Нажмите **Run Search** на панели **Tasks**.
Сообщения журнала, которые соответствуют параметрам сохраненного поиска, отобразится в окне LogViewer.

Для запуска нового запроса:

1. Следуйте инструкциям в разделе *Create a Search Query* для определения запросов поиска.

2. Нажмите **Run Search** на панели **Tasks**.
Сообщения журнала, которые соответствуют параметрам сохраненного поиска, появятся в окне LogViewer.

Очищение истории поиска

Вы можете удалить все последние запросы поиска в истории поиска. На панели **Tasks** нажмите **Clear Search History**.

Параметры поиска

Выберите один из существующих вариантов для каждого поля при создании поискового запроса.

Для настройки **Search Parameters**:

1. Выберите тип сообщения, для которого вы хотите выполнить поиск, из выпадающего списка **Log message type.**

   *** All Logs** *** Debug**

   *** Traffic** *** Statistic**

   *** Alarm** *** Server**

   *** Event**

2. Для применения столбцов, оператора и правил для вашего поискового запросы нажмите **Add** или **Edit**.

   Column — выберите столбец для поиска из выпадающего списка.

   Operator — выберите операцию для поиска: EQUAL TO, NOT EQUAL TO, GREATER THAN (>), LESS THAN (<), CONTAINS.

   Value — введите значение для оператора поиска.

3. Нажмите **OK** для сохранения параметров правила поиска.

4. Из выпадающего списка **Order By** выберите порядок для отображения результатов поиска и просмотра результатов в восходящем (**ascending**) или (**descending**) порядке. Вы можете выбрать любой столбец, который может быть сортирован и доступен для выбранного типа сообщения.

5. Выберите отображение **Options** для правила поиска.

   Rule — Если вы выберете **AND**, то на экране появятся результаты, которые удовлетворяют всем правилам. Если вы выберете **OR**, то на экране появятся результаты, которые удовлетворяют любому правилу. Если в вашем поиске есть только одно правило, то этот параметр не используется.

   Matches — Выберите ,будут ли включены сообщения журнала **Include** или **Exclude,** которые совпадают с критериями поиска, в конечный результат

Фильтрация сообщений журнала по типу и времени или запущенной строке поиска

LogViewer включает тип и время фильтров, которые вы можете использовать для отображения определенных типов сообщений журнала для заданного периода времени. Вы можете так же использовать значение строки поиска для нахождения сообщений журнала, которые содержат особенные символы.

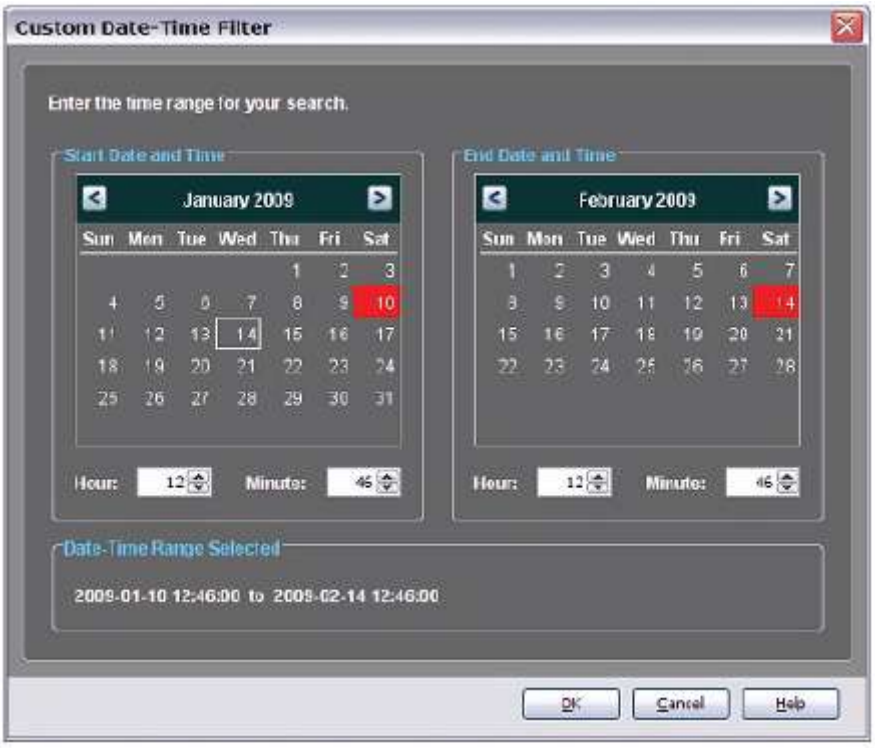
Это может быть удобным при отладке.

Фильтрация сообщений по типу и времени

1. Нажмите на кнопку тип для фильтрации сообщения журнала по типу.
   LogViewer сортирует сообщения журнала и отображает только те сообщения, которые соответствуют выбранному типу журнала.

   * **All logs**
   * **Event**
   * **Traffic**
   * **Debug**
   * **Alarm**
   *

2. Нажмите и выберите **Custom Filter**.
   Откроется диалоговое окно Custom Date-Time Filter



3. Выберите **Start Date and Time** и **End Date and Time**.

   * Нажмите на календари для выбора периода времени.

   * Нажмите на **Hour** и **Minute** стрелками для выбора периода времени.

4. Нажмите **OK**.
   Данные сообщения журнала для выбранного периода времени отобразятся в окне LogViewer.

Запуск строки поиска

Вы можете использовать Search Manager для поиска сообщений журнала по определенным деталям или запускать строку поиска из LogViewer.

1. В выпадающем списке в верхней правой части окна LogViewer введите определенную текстовую стоку для поиска в журналах.

   Например, введите HTTP Proxy для поиска всех сообщений журнала с HTTP Proxy.

2. Нажмите  . Для выбора того, каким образом появятся результаты в LogViewer, нажмите на выпадающий список и выберите опцию:

   Show only results

   Исключает все сообщения журнала, которые не совпадают в параметрами писка в окне LogViewer. Исходные сообщения, которые вы выбрали, будут выделены.

   Highlight results

   Включает все сообщения журнала в окно, но выделяет только те, которые соответствуют поиску.

   Recent Saved Searches

   Включает поиски, которые вы сохранили в Search Manager. Выбранные результат поиска из списка для работы в текущем окне Device.

   LogViewer ищет через сообщения журнала и применяет выбранные параметры.

Использование Log Excerpt для фильтрации результатов поиска

Log Viewer включает опции поиска, которые вы можете использовать для поиска заданного события, произошедшего на вашем Firebox. После нахождения заданного сообщения журнала вы может использовать Log Excerpt для просмотра сообщений журнала, которые Сервера Журнала записал до или после того, как вы выбрали сообщение журнала.

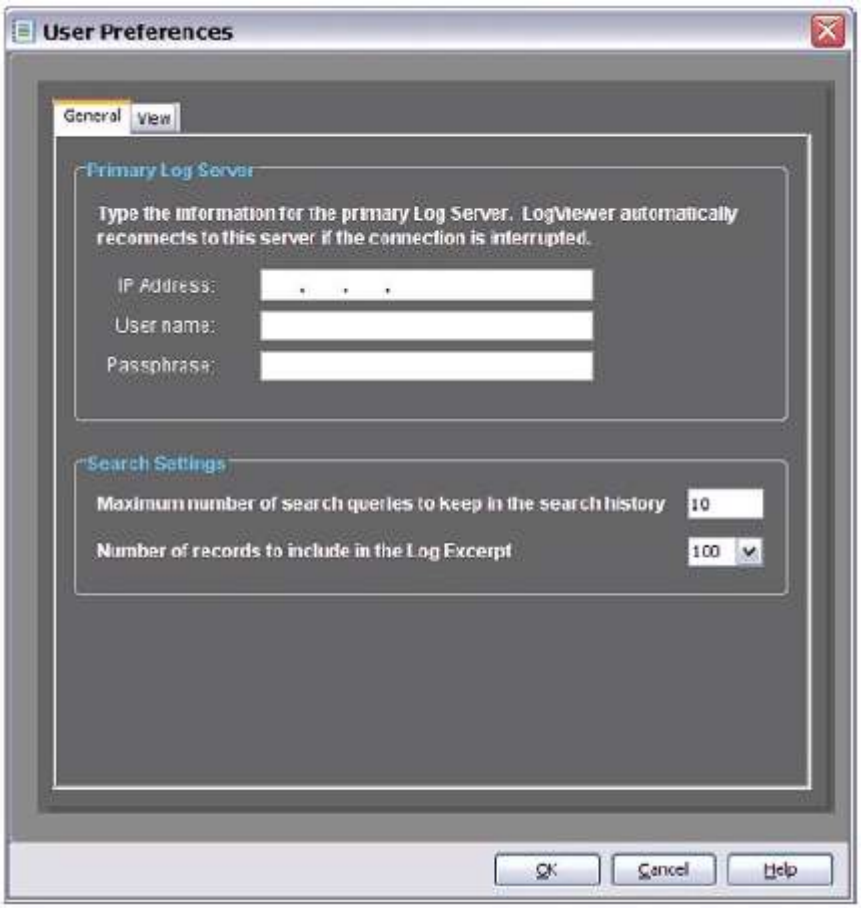
Вы можете так же выбрать количество журналов (50-250), которое вы хотите просматривать дополнительно с выбранным сообщением.

Это может помочь вам просмотреть другие события, которые произошли во время отладки сетевой проблемы. Вы можете так же использовать Log Excerpt для сравнения сообщений журнала двух различных устройств при отладке. Например, вы можете использовать это значение для просмотра сообщений журнала от устройства, которое является конечной точкой, при неполадках с VPN-туннелем.

Установка количества Log Excerpts

1. В LogViewer выберите **View > Preferences**.
   Откроется диалоговое окно User Preferences.

2. Выберите закладку **General**



3. В разделе **Search Settings** выберите **Number of records to be included in the Log Excerpt** из соответствующего выпадающего списка.
   По умолчанию установлено 100.

4. Нажмите **OK**.

Использование Log Excerpt для очистки результатов поиска

Для использования Log Excerpt вам следует запустить поисковый запрос в текстовой строке внутри сообщений журнала

1. В LogViewer подключитесь к Серверу Управления и Firebox.

2. Выберите тип сообщения журнала и запустите строку поиска или создайте свой собственный запрос

3. Выберите сообщения журнала в окне **LogViewer**.

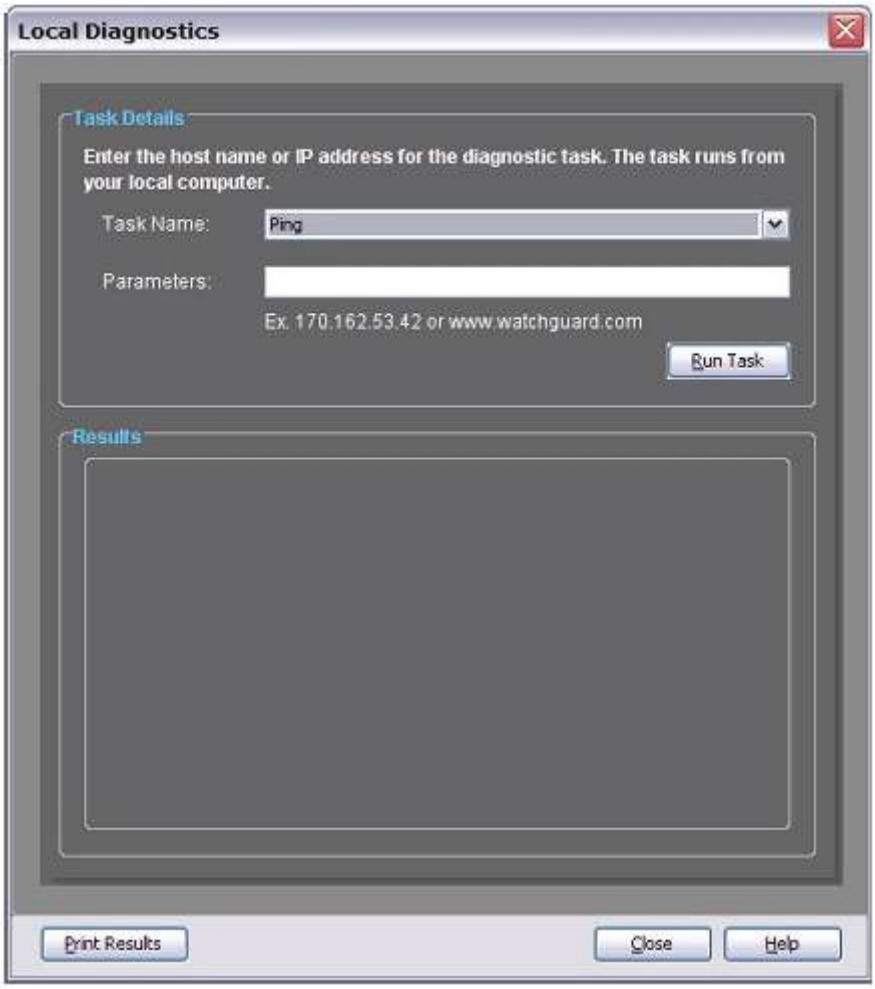
4. Правой кнопкой мыши нажмите на сообщения журнала и выберите **Show Log Excerpt**. Или нажмите кнопку **F5**.
   LogViewer фильтрует результаты поиска и отображает количество журналов, которое окружают метку для выбранного сообщения.

5. Нажмите Clear , чтобы удалить фильтры и вернуться к первоначальному вида окна LogViewer.

Запуск локальных задач диагностики

При помощи утилиты LogViewer вы можете запускать процедуры диагностики на любом IP адресе или хосте. Процедуры диагностики включают **Ping**, **Tracert** или **NSLookup**.

1. Нажмите на  в панели инструментов LogViewer . Или выберите **Tools > Local Diagnostics** и выберите процедуру.
   Откроется диалоговое окно Local Diagnostics.



2. Из выпадающего списка **Task name** выберите процедуру

   * **Ping** - Убедитесь, что IP адрес или хост активны

   * **Tracert** - Трассировка маршрута к IP-адресу или хосту.

   * **NSLookup** - Проверка имени сервера и актуального IP адреса выбранного IP-адреса или хоста

3. Введите IP-адрес или имя хоста в поле **Parameters**

4. Нажмите **Run Task**. Результаты выполнения процедуры появятся в поле **Results**

5. Для того чтобы распечатать результаты работы процедуры нажмите Print Results.
   Откроется диалоговое окно Prints.

6. Настройте параметры принтера и нажмите Print.

Импорт и экспорт данных в LogViewer

При помощи LogViewer вы можете посмотреть данные из файлов журналов базы данных или экспортировать выбранные данные в файл базы данных.

Импорт данных

1. В панели инструментов **LogViewer** нажмите  .
   Или выберите **File** > **Import Data**.
   Откроется диалоговое окно Import Data.

2. Найдите необходимый файл базы данных.

3. Нажмите **Import**.
   Выбранные данные появятся в новом окне Server.

Экспорт данных

1. Выберите сообщения, которые вы хотите экспортировать в LogViewer Firebox или в окне Server.

2. На панели инструментов LogViewer нажмите. Или выберите **File** > **Export Selected Data**.
   Откроется диалоговое окно Export Selected Data. В поле File name будет указано имя файла по умолчанию.

3. Выберите каталог, куда вы хотите сохранить файл базы данных

4. При необходимости введите новое имя файла в поле **File name**.

5. Нажмите **Export**.
   Файл базы данных сохранится в выбранном каталоге.

Отправка сообщений журнала по электронной почте, печать или сохранение сообщений журнала

После того, как вы выберете одно или несколько сообщений журнала в LogViewer, вы можете их отправить по электронной почте, распечатать или сохранить

Отправка сообщения по электронной почте

1. Откройте LogViewer.

2. Выберите **File > Send Selection As** и выберите опции от следующего списка:

   * Comma Separated Values (*.csv)

   * Portable Document Format (*.pdf)

   Откроется электронное письмо с присоединенным файлом в выбранном формате.

Печать сообщения

1. Откройте LogViewer.

2. Выберите **File** > **Print Selection**.
   Откроется диалоговое окно Print.

3. Выберите принтер и его опции.

4. Нажмите **Print**.

Сохранение сообщения

1. Откройте LogViewer.
2. Выберите **File > Save Selection as** и выберите опции от следующего списка:

   * Comma Separated Values (*.csv)

   * Web Page (*.htm, *.html)

   * Portable Document Format (*.pdf)

   * Extensible Markup Language (*.xml)

   Откроется диалоговое окно Save.
3. Выберите каталог и введите имя файла.

Нажмите **Save**

Глава 22 - Мониторинг состояния Firebox

Firebox System Manager (FSM)

WatchGuard Firebox System Manager (FSM) предоставляет вам интерфейс для мониторинга всех компонентов Firebox и выполняемых ими функции.

При помощи FSM вы можете посмотреть следующее:

- Базовое состояние Firebox и сети (закладка Front Panel)
- Сообщения журнала Firebox (закладкаTraffic Monitor)
- Визуальное отображения использования пропускной способности (Закладка Bandwidth Meter)
- Визуальное отображение использования политики (Закладка Service Watch)
- Статистика по трафику и производительности (Закладка Status Report)
- Список аутентифицированных пользователей (закладка Authentication List)
- Список заблокированных сайтов (закладка Blocked Sites)
- Подписки по сервисам безопасности (закладка Security Services)

Вы также можете запустить эти приложения из Firebox System Manager:

- **HostWatch** – графический пользовательский интерфейс, который показывает все соединения между различными интерфейсами Firebox
- **Performance Console** – утилита Firebox, которая используется для построения графиков, которые показывают работу различных компонентов Firebox.
- **Communication log** – хранить сообщения о подключениях между Firebox и Firebox System Manager.
- **Policy Manager** – инструмент, который вы можете использовать для создания, изменения и сохранения файлов конфигурации для ваших устройств Firebox.

При помощи Firebox System Manager вы можете выполнять следующие функции:

- Управление сертификатами
- Отключение или переподключение к Firebox
- Перезагрузка или выключение Firebox
- Расчет контрольной суммы Fireware XTM
- Просмотр и синхронизация ключей функции

- Синхронизация времени
- Очистка ARP кэша
- Удаление тревог
- BOVPN туннели
- Управление кластером FireCluster
- Изменение паролей

Запуск Firebox System Manager

Вы можете использовать Firebox System Manager (FSM) для просмотра статуса подключенного Firebox. Перед использованием Firebox System Manager, вам необходимо открыть WatchGuard System Manager и вы должны быть подключены к устройству

1. В WatchGuard System Manager выберите закладку **Device Status**.
2. Выберите Firebox, состояние которого вы хотите посмотреть при помощи Firebox System Manager.
3. Нажмите . Или выберите **Tools** > **Firebox System Manager**.
   Откроется диалоговое окно Firebox System Manager.

Информация о состоянии устройства появится через несколько секунд, так как Firebox System Manager должен подключиться к устройству Firebox

Отключение или повторное подключение к Firebox

Когда окно FSM открыто вы можете закрывать или снова создавать подключение к устройству Firebox

Для отключения FSM от Firebox и закрытия соединения между ними выполните следующее:

1. Запустите FSM.
2. Нажмите . Или выберите **File** > **Disconnect**.
   Статус устройства изменится на Not Monitored.

Для того чтобы заново подключить FSM к Firebox выполните следующее:

1. Запустите FSM.
2. Нажмите . Или выберите **File > Connect**.
   Статус устройства изменится на Connected.

Настройка интервала обновления и остановка дисплея

Все закладки Firebox System Manager в нижней части содержат выпадающий список, в котором указаны значения интервалов обновления и кнопка Pause для остановки дисплея.

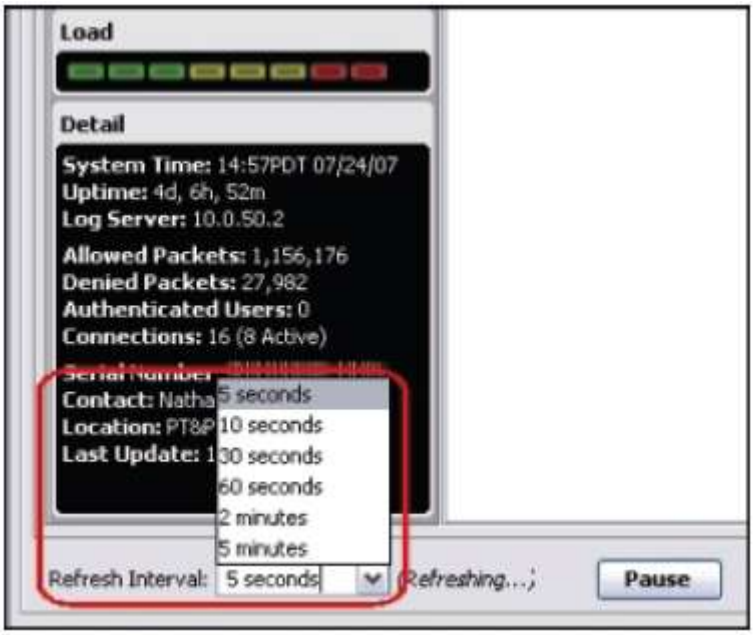
Интервал обновления

Интервал обновления – это интервал опроса; промежуток времени между обновлениями дисплея. Вы можете изменить промежуток времени (в секундах), по истечении которого FSM получит информацию от Firebox и отправит ее пользовательскому интерфейсу.

Частоту, с которой вы будете получать данные от устройства Firebox, необходимо сбалансировать с нагрузкой на Firebox.

Проверьте значения интервалов обновления в каждой закладке. Когда закладка получит новую информацию для дисплея, рядом с выпадающим списком **Refresh Interval** появляется текст Refreshing.... Более короткие промежутки времени дают более точное отображение на дисплее, но создают большую нагрузку на Firebox.

В окне Firebox System Manager из выпадающего списка **Refresh Interval** выберите интервал обновления. Также в этом поле вы можете ввести свое значение



Pause/Continue

Для временной остановки обновления данного окна системой Firebox System Manager нажмите на кнопку **Pause**. После того, как вы нажмете кнопку **Pause,** она превратится в кнопку **Continue**. Для того чтобы возобновить процедуру обновления окна нажмите **Continue.** Кнопка изменится на Pause.

Базовый статус Firebox и сети (Закладка Front Panel)

Закладка **Front Panel** Firebox System Manager содержит базовую информацию о вашем Firebox, вашей сети и сетевом трафике. Закладка всегда отображает предупреждения об устройстве Firebox или его компонентах.

Инструкции по открытию Firebox System Manager см. в “Запуск Firebox System Manager”. Более подробную информацию о Firebox и статусе сети см. следующие разделы:

- Визуальное отображение трафика между интерфейсами
- Объем трафика, загрузка процессора и базовое состояние
- Состояние Firebox
- Состояние VPN туннеля и сервисы безопасности

Предупреждения

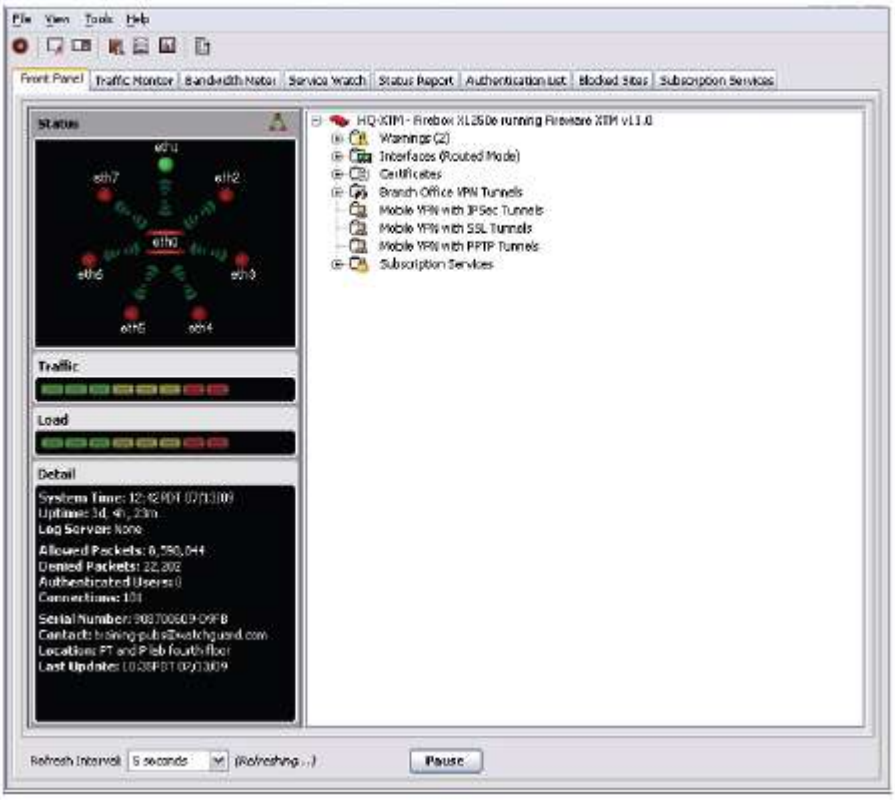
Любое предупреждение появляется всегда в верхней части списка:

Activate Now

Если устройство не было активировано, появляется предупреждение в списке **Warnings** и кнопка **Activate Now** в правом верхнем углу становится видимой. Нажмите на нее, чтобы зайти на сайт LiveSecurity Service, где вы сможете получить ключ функций для вашего Firebox.

Renew Now

Если срок действия любых WSM сервисов заканчивается, появляется предупреждение в списке **Warnings** и кнопка **Renew Now** становится видимой. Нажмите на эту кнопку для того, чтобы обновить ваши сервисы.



Открытие и закрытие деревьев

Для того чтобы открыть часть дисплея, нажмите на символ (+) рядом с параметром, или два раза нажмите на имя параметра. Для того чтобы закрыть часть дисплея нажмите на символ (–) рядом с параметром. Если рядом с параметром нет символов (+) или (-), то это значит, что по нему нет больше информации.

Визуальное отображение трафика между интерфейсами

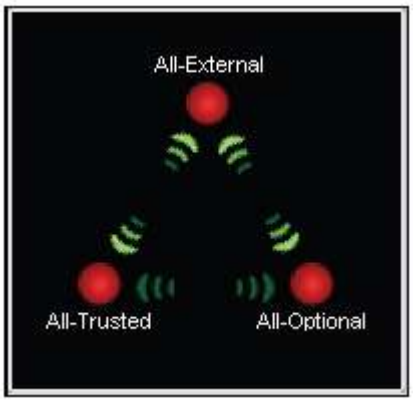
В верхнем левом углу окна, Firebox System Manager находится дисплей, который показывает трафик между интерфейсами Firebox. Дисплей также показывает, запрещен или разрешен ли трафик на каждом интерфейсе.

Дисплей может быть в форме треугольника или звезды. Вершины звезды и треугольника показывают перемещение трафика, который идет через интерфейсы. Зеленая стрелка показывает, что трафик на данном интерфейсе разрешен. Красная стрелка показывает, что трафик определенного типа на данном интерфейсе запрещен. Каждая вершина показывает

входящее и исходящее соединения разными стрелками. Когда трафик передается между двумя интерфейсами, то в направлении трафика зажигаются стрелки

Дисплей в форме треугольника

В треугольнике сетевой трафик показан точками треугольника. Точки показывают только те случаи, когда соединение неактивно или запрещено. Исключение составляет тот случай, когда передается большой объем **default-route** VPN трафика. Под default-route VPN трафиком понимают пакеты, которые передаются через VPN к Firebox, который настроен как шлюз по умолчанию для VPN сети. В этом случае индикатор уровня трафика Firebox System Manager может показать высокий уровень трафика, но вы не увидите зеленых огней при увеличении количества default-route VPN трафика, который передается через один и тот же интерфейс.



Если у Firebox есть три настроенных интерфейса, то каждая вершина треугольника представляет собой отдельный интерфейс. Если у устройства Firebox более трех интерфейсов, то каждая вершина треугольника обозначает тип интерфейса. Например, если у вас есть шесть настроенных интерфейсов (один External, один Trusted и 4 интерфейса Optional), вершина “All-Optional” треугольника представляет все четыре интерфейса Optional.

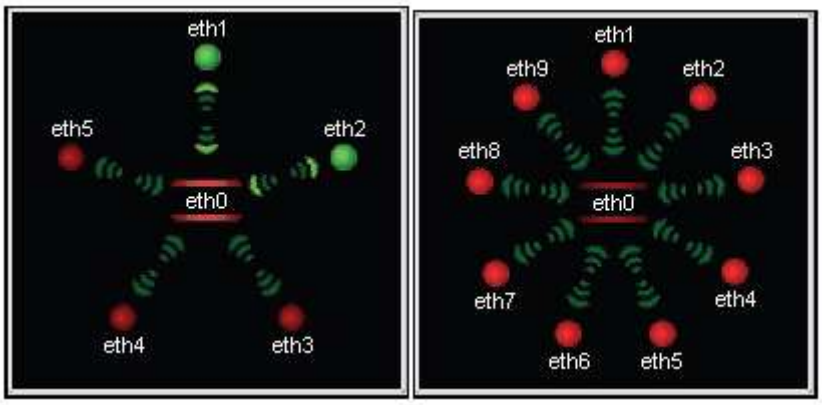
Дисплей в форме звезды (Star display)

В звезде место, где вершины сходятся, может символизировать следующее:

- Red (запрещен)— Firebox запрещает подключение через этот интерфейс.
- Green (разрешен)—Между этим интерфейсом и другим интерфейсом (не в центре звезды) передается трафик. Когда есть трафик между этим интерфейсом и центром, точки между этими интерфейсами показаны как зеленые стрелки, которые постоянно мигают.

Этот дисплей показывает весь трафик, проходящий через центральные интерфейсы. Стрелка, которая движется от центрального интерфейса к боковым, показывает прохождение трафика через устройство Firebox. Трафик проходит через центральный интерфейс и затем идет к боковым интерфейсам.

Например, если интерфейс eth1 находится в центре звезды, а интерфейс eth2 является боковым, то зеленая стрелка показывает, что трафик идет от интерфейса eth1 к интерфейсу eth2. Дисплей в форме звезды имеет несколько представлений, в зависимости от типа подключенных к Firebox устройств. Количество углов в звезде изменяется в зависимости от количества интерфейсов на вашем устройстве. Один интерфейс расположен в центре звезды, а остальные дополнительные интерфейсы отображаются по углам звезды. Например, если на устройстве есть 6 интерфейсов, звезда содержит 5 углов и, если устройство имеет 10 интерфейсов, то звезда имеет 9 углов.

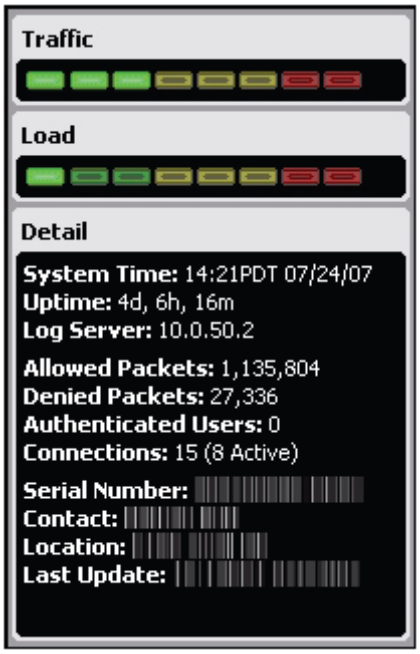


Если вы используете дисплей в форме звезды, то вы можете настроить интерфейс, который будет находиться в центре. Нажмите на название интерфейса или его точку. Интерфейс переместится в центр звезды. Все интерфейсы перемещаются по часовой стрелке. Если вы переместите интерфейс в центр звезды, то вы сможете увидеть весь трафик между этим и остальными интерфейсами. По умолчанию в центре находится интерфейс External.

Для того чтобы изменить дисплей, нажмите на него правой кнопкой и выберите **Triangle Mode** или **Star Mode.**

Объем трафика, загрузка процессора и базовое состояние

Firebox System Manager показывает объем трафика, загрузку процессора и базовое состояние на своей передней панели. Под **Security Traffic Display** находятся индикатор объема трафика **Traffic**, индикатор загрузки процессора и информацию о базовом состоянии (Detail). Две гистограммы показывают объем трафика и емкость устройства Firebox

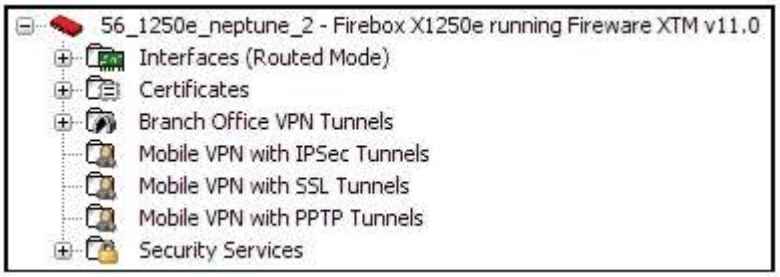


Состояние Firebox

В правой части передней панели **Front Panel** Firebox System Manager находится информация о базовом состоянии.

Состояние и предупреждения

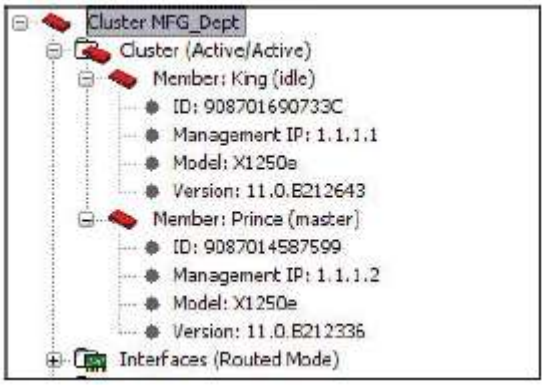
- Состояние устройства Firebox. Включает версию Fireware и **patch string**.
- **Предупреждения**: Появляются при обновлении сервисов безопасности и становятся доступными , когда срок действия сервисов безопасности или других компонентов истекает. Для того чтобы обновить, нажмите на кнопку **Renew Now,** которая появляется в правой верхней части окна FSM.



Firebox, FireCluster и параметры интерфейса

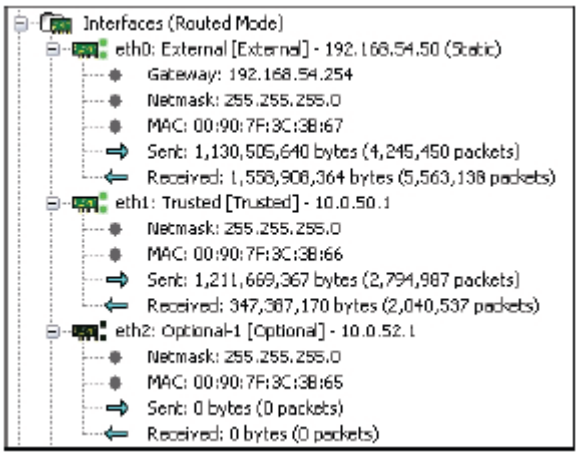
В закладке **Front Panel** системы Firebox System Manager (закладка доступна при первом запуске FSM) вы можете открыть параметры для того чтобы посмотреть следующее:

- IP-адрес каждого интерфейса Firebox и режим конфигурации интерфейса External.
- Доступны ли устройства FireCluster. Также здесь отображается дата последнего обновления устройства кластера.



Если вы откроете список для каждого интерфейса, то вы можете посмотреть следующую информацию:

- IP-адрес, шлюз и маску сети каждого настроенного интерфейса.
- MAC адрес каждого интерфейса
- Количество байт и пакетов, полученных с последней перезагрузки Firebox
- Состояние физического соединения (подсвеченный значок интерфейса или соединения обозначает о настроенном интерфейсе или соединении, затемненный значок соответствует нерабочему состоянию интерфейса или соединения)



Сертификаты и их текущий статус

FSM показывает сертификаты, которые есть на устройстве Firebox, и их текущий статус. Для валидных сертификатов FSM показывает период их действия и их отпечаток

Сообщения журнала Firebox (Traffic Monitor)

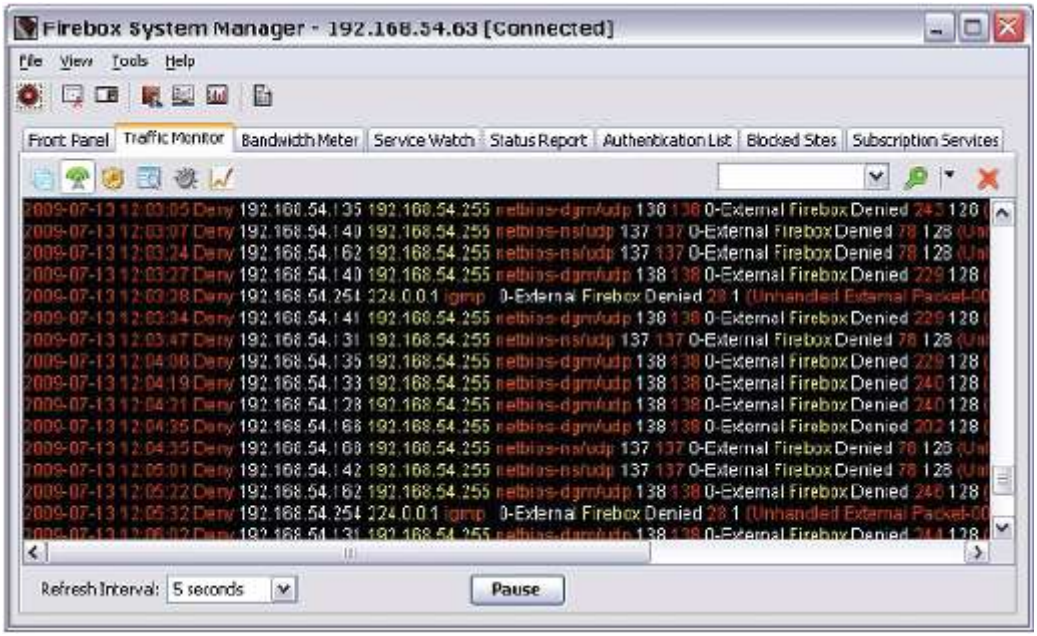
Вы можете использовать Firebox System Manager (FSM) для просмотра сообщений журнала по мере их возникновения на вашем устройстве Firebox. В некоторых сетях может возникнуть небольшая задержка при отправке сообщения журнала.

1. Запустите Firebox System Manager.
2. Нажмите на закладку **Traffic Monitor**.

Traffic Monitor можно использовать для решения проблем, связанных с производительностью системы

Вы можете настроить Traffic Monitor для:

- Изменения параметров Traffic Monitor
- Копирования сообщений в другие приложения
- Получения более подробной информации о сообщении
- Включения уведомление для определенных сообщений
- Использования иконок Traffic Monitor для отображения определенных типов сообщений журнала
- просмотра diagnostic -сообщения в Traffic Monitor (при диагностике проблем)



Сортировка и фильтрация сообщений журнала в Traffic Monitor

Вы можете использовать кнопки Traffic Monitor для сортировки информации, которая отображается в Traffic Monitor. При помощи кнопок Traffic Monitor вы можете смотреть только определенные типы сообщения. Вы можете так же использовать поле фильтра для поиска и очистки списка сообщений

Для того чтобы сортировать сообщения по типу выполните следующее:

1. В FSM выберите закладку **Traffic Monitor**.

2. Нажмите кнопку для выбора типа сообщения для просмотра в Traffic Monitor.

   *  - все журналы

   *  - журналы трафика

   *  - тревоги

   *  - журналы событий

   *  - журналы отладки

   *  - журналы со статистикой производительности

   FSM сортирует сообщения журнала и отображает только выбранный тип сообщений.

Для фильтрации сообщений по определенным полям выполните следующее:

1. В FSM выберите закладку**Traffic Monitor**

2. В выпадающем списке введите или выберите информацию, которую вы хотите найти. Вы можете ввести значение в поле фильтра или выбрать предыдущее введенное значение в выпадающем списке.

3. Нажмите на выпадающий список  и выберите **Highlight Search Results** или **Filter Search Results**.
   Сообщения журнала, которые соответствуют поисковому запросу, появятся в окне Traffic Monitor.

4. Для удаления фильтра нажмите  .

Изменение параметров Traffic Monitor

Вы можете настроить внешний вид утилиты Traffic Monitor. Вы можете выбрать цвет фона для окон, цвет текста для типов сообщений, а также выбрать отображать ли сообщения в цвете, показывать имена полей сообщений. Вы также можете установить максимальное количество отображаемых сообщений журнала.

Для того чтобы изменить параметры Traffic Monitor выполните следующее:

1. Запустите Firebox System Manager.

2. В Firebox System Manager выберите **File > Settings**. Или нажмите где-либо на экране правой кнопкой мыши и выберите **Settings**.
   Откроется диалоговое окно Settings.

Установка максимального количества сообщений журнала

Вы можете изменить максимальное количество сообщений журнала, которые хранятся и отображаются в Traffic Monitor. При достижении максимального количества новые сообщения журнала будут заменять первые записи. Если у вас медленный процессор или недостаточное количества памяти, то большое количество сообщений может привести к замедлению работы вашей системы управления

Если вам необходимо посмотреть большое количество сообщений журнала, то вы можете использовать утилиту LogViewer

1. В диалоговом окне **Settings**

2. В выпадающем списке **Maximum Log Messages** выберите максимальное количество сообщений журнала, которое будет отображаться в Traffic Monitor

3. Нажмите **OK**.

Отображение имена полей в сообщениях журнала

Traffic Monitor в сообщения журнала может добавлять специальные метки для полей сообщения: *src_ip*, *dst_ip* и *src_port*.

В диалоговом окне **Settings** выполните следующее:

1. Включите опцию **Show Log Field Names**.

2. Нажмите **OK**.

Использование цвета для сообщений журнала

Вы можете настроить Traffic Monitor для отображения сообщений в указанном вами цвете. При помощи цветов вы можете различать типы выводимой информации. В закладках **Alarm**, **Traffic Allowed**, **Traffic Denied**, **Event**, **Debug** и **Performance** вы можете выбрать цвет для каждого поля.

1. В диалоговом окне **Settings** выберите закладку **Traffic Monitor**

2. Для того чтобы отключить все цвета на экране отключите опцию **Show Logs in Color**

3. Выберите закладку (**Alarm**, **Traffic Allowed**, **Traffic Denied**, **Event**, **Debug** или **Performance**).

4. Из списка выберите категорию информации сообщения журнала. В окне **Text Color** отображается текущий цвет для выбранной категории.

5. Для изменения цвета нажмите на окно управления цвета **Text Color**.
Откроется диалоговое окно Traffic Monitor Field Color.

6. Выберите цвет. Образец цвета появится в окне *Sample* в верхней части диалогового окна.

7. Нажмите **OK** для закрытия диалогового окна или **Reset** для использования предыдущего цвета.

8. Нажмите **OK** для закрытия диалогового окна **Settings**.

Выбор цвета фона для Traffic Monitor

1. В диалоговом окне **Settings** нажмите на закладку **Traffic Monitor**.

2. Нажмите на окно управления цветом **Background Color**.
Откроется диалоговое окно Traffic Monitor Background Color.

3. Выберите цвет. Образец цвета появится в окне *Sample* в верхней части диалогового окна.

4. Нажмите **OK,** чтобы закрыть диалоговое окно или **Reset** для перехода к предыдущему цвету.

5. Для отмены ваших изменений и возврата к первоначальному фоновому цвету нажмите **Restore Defaults**.

6. Нажмите **OK** для закрытия диалогового **Settings**.

Копирование сообщений в другие приложения

Вы можете копировать сообщения журнала в Firebox System Manager и вставлять их в различные программы.

1. В закладке **Traffic Monitor** выберите одно или более сообщений.

2. Правой кнопкой нажмите на сообщение (-я) и выберите **Copy Selection** или **Copy All**. Если вы выбрали **Copy All**, то Firebox System Manager скопирует все видимые сообщения журнала.

3. Откройте другую программу и вставьте сообщение (-я). Вы можете так же использовать LogViewer для открытия файла журнала.

LogViewer – инструмент WatchGuard System Manager для просмотра подробной информации данных файла журнала.

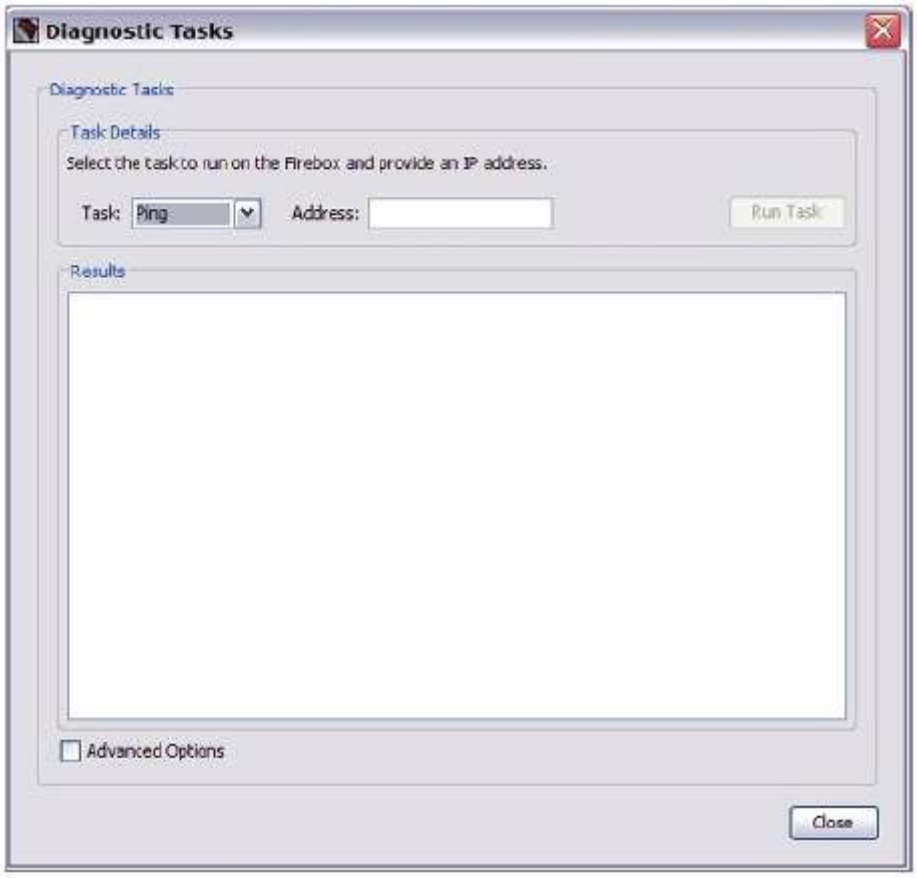
Получение более полной информации о сообщении

Вы можете использовать Firebox System Manager (FSM) Traffic Monitor Diagnostic Tasks для получения более подробной информации о сообщении журнала трафика или просмотра информации в сообщениях журнала вашего устройства. Вы можете пинговать IP-адреса источника или отправителя, проследить маршрут к IP-адресу источника или получателя, искать DNS-информацию для IP-адреса или просматривать информацию о пакетах, переданных через вашу сеть (TCP dump). Для того чтобы фильтровать выводимые результаты вы можете использовать специальные аргументы

Запуск Diagnostic Tasks

Вы можете запустить diagnostic-задачи для просмотра информации во всех сообщениях журнала из вашего устройства. Это может помочь при решении проблем в сети.

1. В закладке FSM **Traffic Monitor** нажмите правой кнопкой мыши на сообщение и выберите **Diagnostic Tasks**.
   Откроется диалоговое окно Diagnostic Tasks



2. В выпадающем списке **Task** выберите задачу, которую вы хотите запустить.

   * Ping

   * Trace Route

   * DNS Lookup

   * TCP Dump

   Если вы выберите Ping, Trace Route или DNS Lookup, то откроется поле Address .

   Если вы выберите TCP Dump, откроется поле Interface.

3. В текстовом поле **Address** введите IP-адрес. Или в выпадающем списке **Interface** выберите интерфейс

4. Для фильтрации результатов включите опцию **Advanced Options**.
   Откроется поле Arguments.

5. В поле **Arguments** введите аргументы, которые вы хотите включить в поиск. Проверьте, что вы включили в список аргументов значение поля **Address** или интерфейс, выбранный в выпадающем списке **Interface**. Если вы в список аргументов не добавили какую-либо из этих величин, то поиск не будет запущен. Для того чтобы посмотреть список аргументов наведите свой курсор на поле **Arguments** или оставьте поле аргументов пустым и нажмите **Run Task**.

6. После того, как вы ввели все необходимые аргументы, нажмите **Run Task**.
   Информация о задаче появится в окне Results и появится кнопка Stop Task.

7. Для остановки diagnostic –задачи нажмите **Stop Task**.

8. Нажмите **Close** для закрытия диалогового окна **Diagnostic Tasks** и вернитесь в Traffic Monitor.

Ping или Trace Route трафика для сообщений журнала

Для того чтобы получить более подробную информацию об IP адресе источника или назначения, который содержится в сообщения журнала, вы можете для него запустить процедуры ping или traceroute.

1. В закладке FSM **Traffic Monitor** выберите сообщение журнала.

2. Правой кнопкой мыши нажмите и выберите задачу:

   * **Source IP address > Ping**

   *** Source IP address > Trace Route**

   *** Destination IP address > Ping**

   *** Destination IP address > Trace Route**

   Откроется диалоговое окно Diagnostic Tasks в текстовом поле которого будет информацию о выбранном сообщении и информации о выбранной процедуре диагностики. Выбранная процедура запустится автоматически.

3. Для фильтрации полученных результатов включите опцию **Advanced Options**. *Откроется поле Arguments.*

4. В поле **Arguments** введите аргументы, которые вы хотите включить в поиск. Проверьте, что вы включили в список аргументов значение поля **Address** или интерфейс, выбранный в выпадающем списке **Interface**. Если вы в список аргументов не добавили какую-либо из этих величин, то поиск не будет запущен. Для того чтобы посмотреть список аргументов наведите свой курсор на поле **Arguments** или оставьте поле аргументов пустым и нажмите **Run Task**.

5. После того, как вы ввели все необходимые аргументы, нажмите на **Run Task**. *Информация о задаче появится в окне Results и появится кнопка Stop Task.*

6. Для того чтобы остановить процедуру диагностики нажмите **Stop Task**.

7. Нажмите **Close** для закрытия диалогового окна **Diagnostic Tasks** и возвращения к Traffic Monitor.

Копирование IP-адреса сообщений журнала

Вы можете копировать IP-адрес источника или получателя, указанных в сообщениях журнала, в другое приложение

1. В закладке FSM **Traffic Monitor** выберите сообщение журнала.

2. Нажмите правой кнопкой мыши на сообщение и выберите задачу:

   * **Source IP address > Copy Source IP address**

   *** Destination IP address > Copy Destination IP address**

   Выбранный IP-адрес скопируется в системный буфер обмена.

Включение уведомлений для определенных типов сообщений

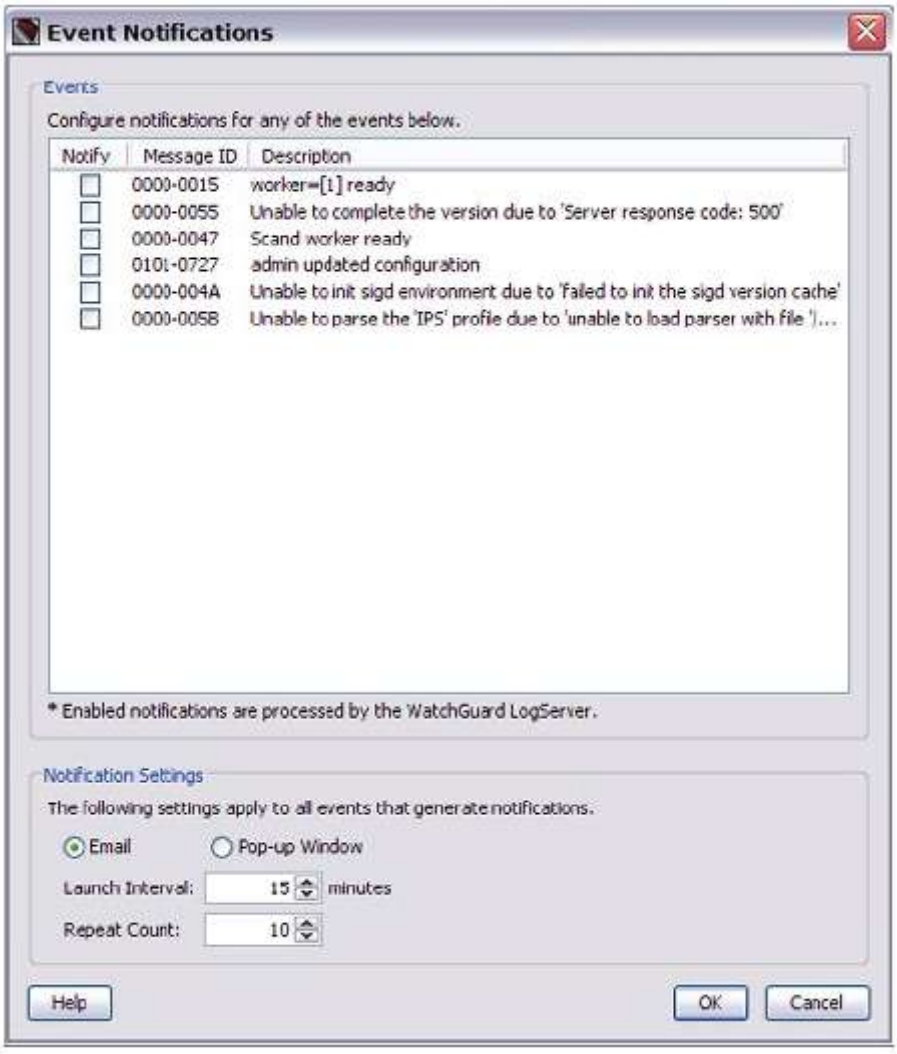
Если вы хотите осуществлять мониторинг определенных событий Firebox, то вам необходимо включить уведомления для сообщений журнала, указанных в Traffic Log. Последующие сообщения с таким идентификатором будут генерировать уведомления.

Идентификатор сообщений появится в диалоговом окне **Event Notifications** для событий, которые уже настроены для уведомлений или для событий, которые действительно произошли на Firebox. Фактическое событие сообщения Firebox показано в столбце **Description**.

В Firebox System Manager выполните следующее:

1. Выберите закладку **Traffic Monitor**.

2. Правой кнопкой мыши нажмите и выберите **Event Notifications**.
   Откроется диалоговое окно Event Notifications с Message ID и Description для всех допустимых событий



3. Для того чтобы сортировать информацию по столбцам нажмите на заголовок столбца.

4. Для получения уведомления о сообщении включите опцию **Notify**.

5. Выберите **Notification Settings**. **Notification Settings** в нижней части диалогового окна применяется для всех уведомлений о событии

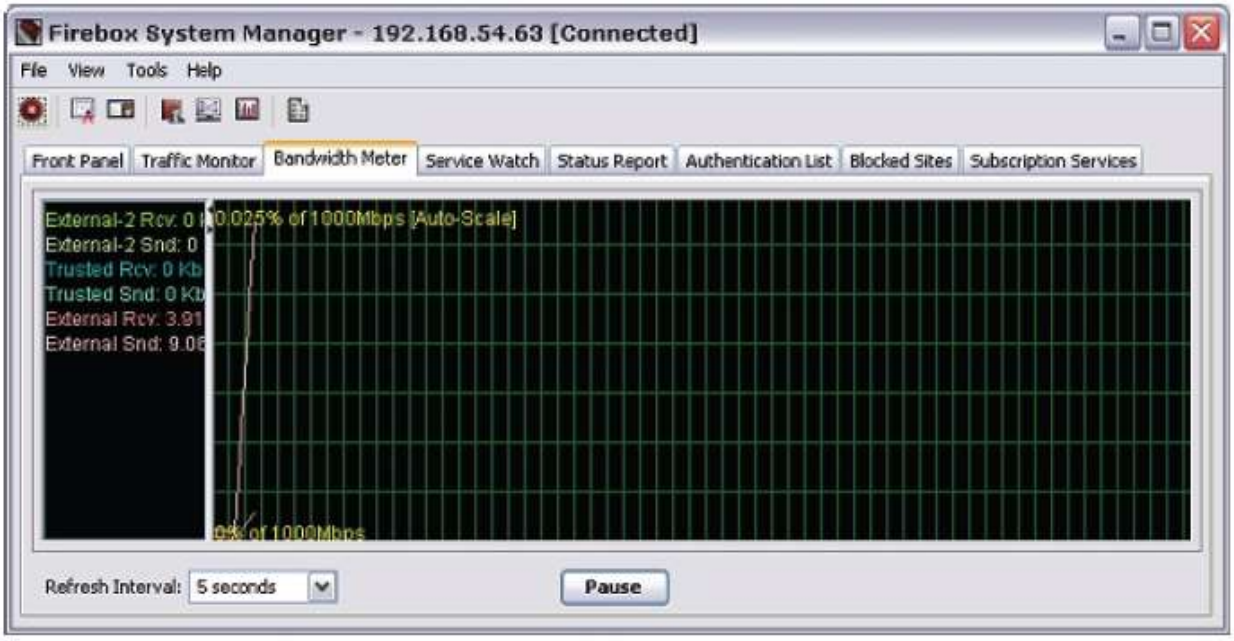
6. Нажмите **OK** для сохранения изменений.
   Откроется диалоговое окно Configure Event Notifications с запросом пароля вашей конфигурации.

7. Введите пароль конфигурации (**Configuration passphrase**) для вашего Firebox и нажмите **OK**.
   Отобразится сообщение, которое вы настроили для уведомления о событии обновится.

Визуальное отображение использования пропускной способности (закладка Bandwidth Meter)

Для того чтобы посмотреть пропускную способность всех интерфейсов Firebox в режиме реального времени выберите закладку **Bandwidth Meter**. Ось Y показывает поток трафика от/к выбранного интерфейса. Ось X (горизонтальная) показывает время.

Если вы нажмете на любую область графика, то откроется окно, в котором вы можете посмотреть более подробную информацию о пропускной способности в этот момент времени. Вдобавок к физическим интерфейсам счетчик также показывает интерфейсы VLAN.



Изменение параметров Bandwidth Meter

Вы можете определять появление Bandwidth Meter, а так же выбирать параметры цвета для текста и разметку, появление меток для интерфейса и устанавливать масштаб для графиков.

Для изменения параметров отображения пропускной способности:

1. В Firebox System Manager выберите закладку **Bandwidth Meter**.

2. Выберите **File** > **Settings**. Или нажмите в любом месте на экране и выберите **Settings**.
   Откроется диалоговое окно Settings

3. Из закладки **Bandwidth Meter** вы можете настроить параметры отображении, а также опции, описание которых приводится в следующих разделах

4. При завершении работы нажмите **OK** для сохранения ваших изменений и возврата к FSM.

Изменение масштаба

Вы можете использовать диалоговое окно **Settings** для изменения масштаба отображения графиков или вы можете нажать правой кнопкой мыши в любом месте закладки Bandwidth Meter и выбрать **Graph Scale** для установки масштаба.

Вы можете изменить масштаб закладки **Bandwidth Meter**. Из выпадающего списка **Graph Scale** выберите значение, которое наиболее подходит для вашей сети.

Для установки произвольного масштаба:

1. В выпадающем списке **Graph Scale** выберите **Custom Scale**.

2. В текстовом поле **Custom Scale** введите значение в килобайтах для каждой секунды.

Добавление и удаление линий

Для добавления линии в закладке **Bandwidth Meter:**

1. В разделе **Color Settings** выберите интерфейс из списка **Hide**.

2. Нажмите на окно управления цветом **Text Color** для выбора цвета линии.

3. Нажмите **Add**.
Имя интерфейса появится в списке Show с выбранным вами цветом.

Для удаление линии в закладке **Bandwidth Meter**:

1. В разделе **Color Settings** выберите интерфейс из списка **Show**.

2. Нажмите **Remove**.
Имя интерфейса появится в списке Hide

Смена цветов

Для изменения цветов экрана в закладке **Bandwidth Meter**:

1. Нажмите на окно управления цветом **Background** и **Grid Line** для выбора новых цветов.
   Откроются диалоговые окна Select Background Color или Select Grid Line.

2. Нажмите на закладку **Swatches**, **HSB** или **RGB** и выберите цвет.
   Пример выбранного цвета появится в разделе Preview.

3. Нажмите **OK** для подтверждения вашего выбора и возврата в диалоговое окно **Settings**.

Изменение способа отображения интерфейсов

Имена интерфейсов появляются в левой части закладки **Bandwidth Meter.** Имена интерфейсов могут отображаться в виде списка. Дисплей также может отображать имя интерфейса рядом с линией, идентифицирующей его.

Для изменения способа отображения имен интерфейсов:

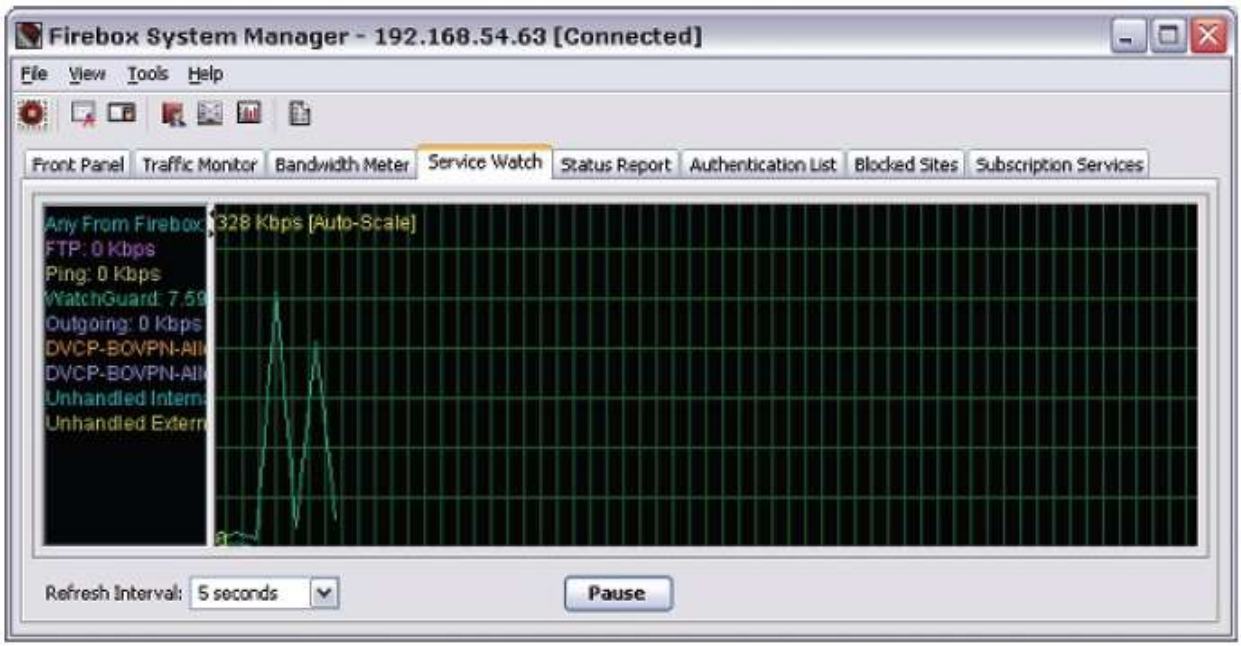
Нажмите на выпадающий список **Show the interface labels as** и выберите **List** или **Tags.**

Для просмотра пропускной способности, используемой политикой вместо интерфейса, см. закладку **Service Watch**

Визуальное отображение использование политики (Закладка Service Watch)

Вы можете использовать Firebox System Manager для просмотра графиков политик, настроенных на Policy Manager.

В закладке **Service Watch** ось Y (вертикальная) показывает количество подключений. Ось X (горизонтальная) показывает время. Если вы нажмете на любую область графика, то откроется окно, в котором вы можете посмотреть более подробную информацию об использовании политики в данный момент времени. Вы можете так же настроить появление закладки **ServiceWatch.**



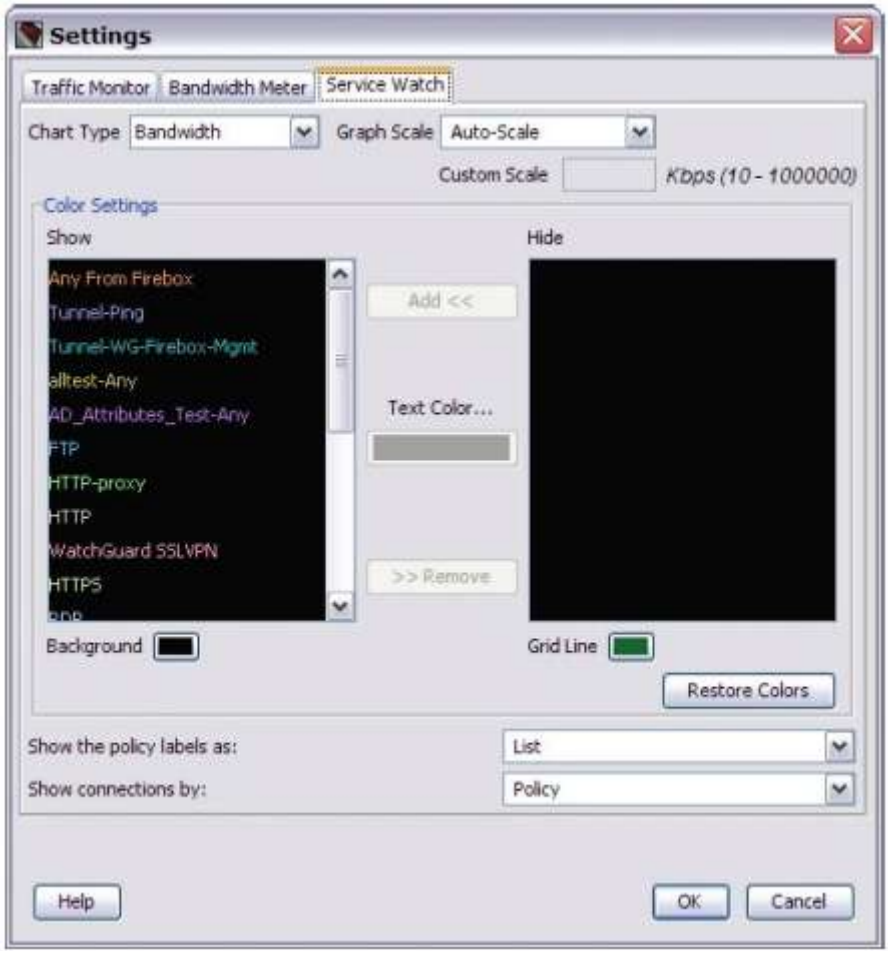
Изменение параметров Service Watch

Вы можете настроить внешний вид Service Watch. Вы можете выбрать параметры цвета для текста и строк таблиц, представление меток политики и установить тип и масштаб для графика.

Для изменения параметров отображения политики:

1. В Firebox System Manager выберите закладку **Service Watch** .

2. Выберите **File** > **Settings**. Или нажмите правой кнопкой мыши в любом месте на экране и выберите **Settings**.
   Откроется диалоговое окно Settings



3. В закладке **Service Watch** вы можете изменить параметры отображения Service Watch с опциями из следующего раздела.

4. При завершении работы нажмите **OK** для сохранения изменений и возвращения к FSM.

Изменение масштаба

Вы можете изменить масштаб закладки **Service Watch**. Из выпадающего списка **Graph Scale** выберите значение, которое наиболее подходит для объема трафика, передаваемого по вашей сети.

1. Из выпадающего списка **Graph Scale** выберите **Custom Scale**.

2. В текстовом поле **Custom Scale** введите количество соединений.

Отображение пропускной способности, которая используется политикой

Для того чтобы показать количество байт в секунду, которые используются политикой вместо количества подключений, из выпадающего списка **Chart Type** выберите **Bandwidth**. Для того чтобы посмотреть использование пропускной способности интерфейсом вместо политики, см. закладку **Bandwidth Meter**

Добавление и удаление линий

Для того чтобы добавить линию в закладке **Service Watch**:

1. Из выпадающего списка **Hide** (секция **Color Settings**)
2. При помощи элемента управления **Text Color** выберите цвет отображения линии.
3. Нажмите **Add**. Имя интерфейса появится в списке **Show** с выбранным вами цветом.

Для того чтобы удалить линию из закладки Service Watch:

1. В разделе **Settings** выберите политику из списка **Show**.
2. Нажмите **Remove**. Имя интерфейса появится в списке Hide

Изменение цвета

Для изменения цветов экрана в закладке **Service Watch**:

1. Нажмите на элементы управления цветом **Background и Grid Line** для выбора новых цветов.
Откроется диалоговое окно Select Background Color или Select Grid Line.

2. Нажмите **Swatches**, **HSB** или **RGB** и выберите цвет.
Пример выбранного цвета появится в разделе Preview.

3. Нажмите **OK** для подтверждения вашего выбора и возврата к диалоговому окну **Settings**.

Изменение способа отображения имен политик

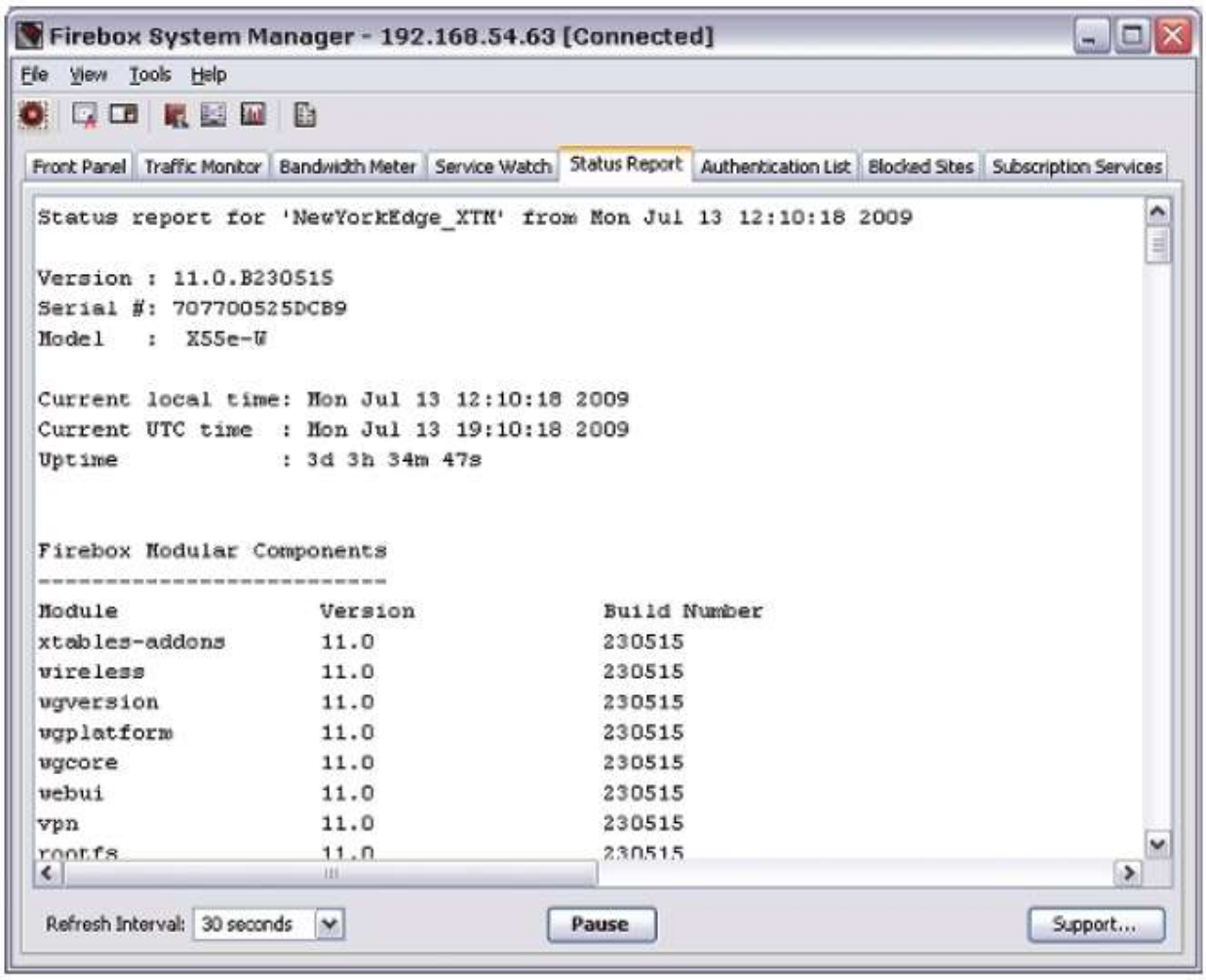
Вы можете изменить способ отображения имен политик (в левой части закладки **Service Watch**). Имена могут отображаться в виде списка, а также могут отображаться рядом с линией, которую они идентифицируют.

Для отображения имен политики:

Из выпадающего списка **Show the policy labels as** выберите необходимый способ отображения: **List** или **Tags**

Статистика по трафику и производительности (закладка Status Report)

Закладка **Status Report** предоставляет вам статистику по трафику и производительности Firebox.



Для просмотра Status Report:

1. Запустите Firebox System Manager.
2. Выберите закладку **Status Report** .

Status Report включает информацию:

Uptime and version information

Время работы Firebox, версию ПО WatchGuard Firebox System, модель Firebox, версию аппаратного ПО, патч (если используется). Также здесь приведен список компонентов Firebox, их состояния и версии.

Log Servers

IP-адреса всех настроенных Серверов Журналов.

Logging options

Опции сообщений журнала, настроенные при помощи Quick Setup Wizard или Policy Manager.

Memory and load average

Статистика использования памяти (в байтах) и средняя нагрузка на Firebox. Нагрузка состоит их трех значений, которые показывают среднюю нагрузку на устройство за последнюю минуту, последние пять минут и последние 15 минут соответственно. Значения, которые превышают 1.00 (100%), показывают, что некоторые запросы из-за недостатка ресурсов поставлены в очередь (Если нагрузка превышает 1.00, то это не значит, что система перегружена.)

Processes

ID процесса, имя и состояние процесса.

Network configuration

Информация о сетевых картах устройства Firebox: имя интерфейса, его аппаратный и IP-адреса, и его маска подсети. Дисплей также включает информацию о локальной маршрутизации, IP псевдонимы и зарезервированные DHCP lease.

Blocked Sites list, Blocked Sites exceptions

Список заблокированных сайтов и исключений. Временно заблокированные сайты появляются в закладке **Blocked Sites**.

Interfaces

Интерфейсы Firebox, их типы (External, Trusted или Optional), его состояние и количество пакетов, счетчик пакетов.

Routes

Таблица маршрутизации ядра Firebox. Вы можете использовать эти таблицы для того, чтобы определить какой из интерфейсов Firebox используется для каждого адреса назначения. Здесь также вы можете найти ECMP группы и динамические маршруты, добавленные демоном маршрутизации.

ARP table

ARP таблица устройства Firebox. ARP таблица используется для преобразования IP-адресов в аппаратные. (Если устройство работает в режиме drop-in, то используйте таблицу ARP только для диагностики проблем с подключением вторичных сетей)

Total Dynamic Network Address Translation (DNAT) entries

Количество использованных и доступных элементов.

Multi-WAN status

Информация по шлюзам и sticky-соединениям, так же содержит таблицу sticky-соединений.

DHCP client leases

Информация по выдаче IP-адресов DHCP сервером клиентам на определенный срок.

Dynamic Routing

Компоненты динамической маршрутизации, которые используются устройством Firebox.

DNS Servers

Адресная информация для DNS-серверов.

Refresh interval

Частота обновления дисплея.

Support

Если вы устраняете неполадки с помощью представителя тех.поддержки, вы можете нажать **Support** для создания файла, который может быть использован для более оперативного решения проблемы

Изменение значения интервала обновления (Refresh Interval)

Содержание Status Report автоматически обновляется в соответствии с интервалом обновления.

Для изменения интервала обновления:

1. В выпадающем списке **Refresh Interval** выберите интервал.

2. Для остановки автоматического обновления экрана нажмите **Pause**.
   Пока экран приостановлен, обновление не происходит.

3. Для запуска автоматического обновления экрана вновь нажмите **Continue**.
   Экран сразу же обновится и затем, через указанный период времени.

Захват (Трассировка) пакетов для устранения неполадок

Для того чтобы посмотреть о перехваченных пакетах на устройстве Firebox выполните следующее:

1. Запустите Firebox System Manager и нажмите на закладку **Status Report**.

2. Нажмите **Support**.
   Откроется диалоговое окно Support Logs.
   Firebox System Manager получит информацию о перехваченных пакетах

3. Нажмите **Browse** для выбора места сохранения файлов журнала диагностики.
   Файлы поддержки сохраняются в формате tarzipped (.tgz).*

4. Нажмите **Retrieve**.
   Support Log сохранится в заданном месте.

5. Просмотрите подробную информацию о packet trace в файле поддержки.

6. После того, как вы закончите отключите diagnostic сообщения

Аутентифицированные пользователи (закладка Authentication List)

Закладка **Authentication List** системы Firebox System Manager предоставляет вам информацию о всех пользователях, аутентифицированных устройством Firebox. Вы можете сортировать информацию в списке Authentication List по любым столбцам. Вы можете так же закрыть сеанс аутентификации пользователя.

Для просмотра **Authentication List**:

1. Запустите Firebox System Manager.

2. Выберите закладку **Authentication List**

Информация о каждом пользователе, который прошел аутентификацию, появится в этих 4 столбцах:

User

Имя пользователя, которое он (она) используется при аутентификации.

Type

Тип аутентифицированного пользователя: пользователи брандмауэра (Firewall users) или Мобильные пользователи (Mobile User).

IP Address

Внутренний IP-адрес пользователя. Для мобильных пользователей IP-адрес – это IP-адрес, присвоенный им устройством Firebox.

From Address

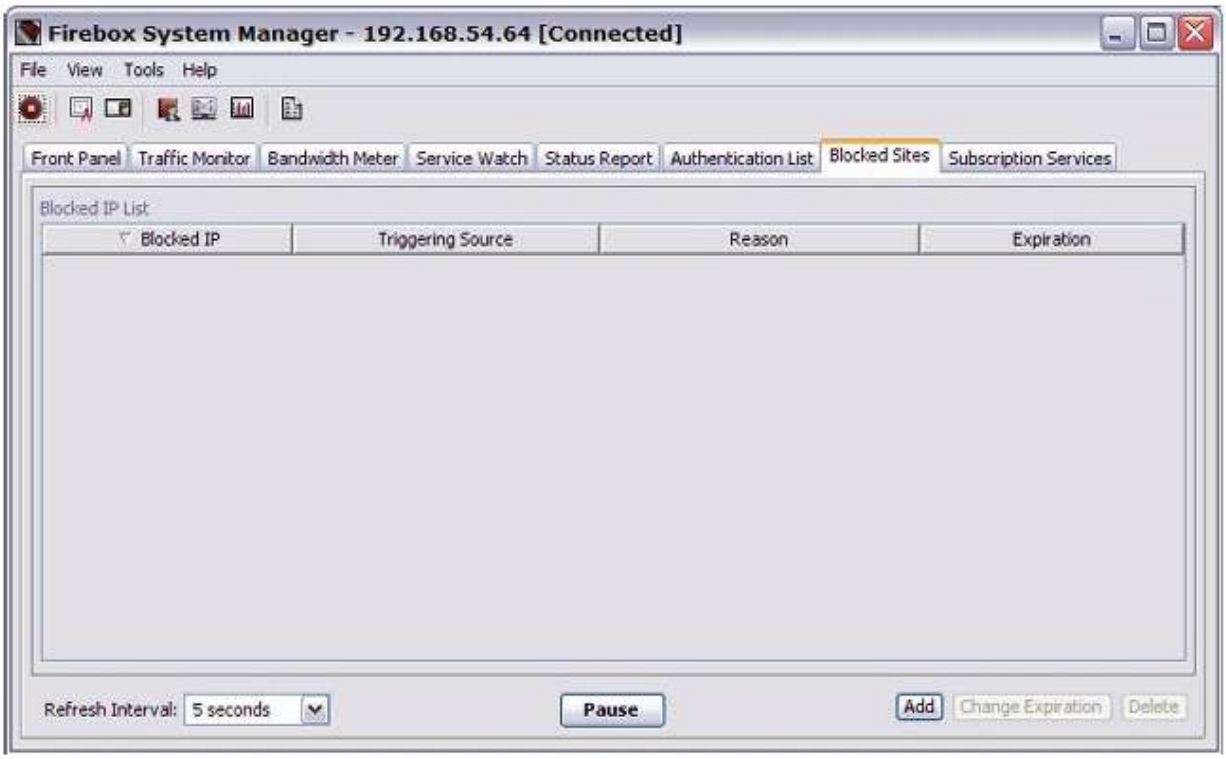
IP-адреса компьютера, с которого пользователя проходил процедуру аутентификации. Для мобильных пользователей этот IP-адрес – это IP-адрес компьютера, который использовался для подключения к устройству Firebox. Для пользователей межсетевого экрана IP-адрес и адрес, указанный в колонке From, совпадают.

Для сортировки пользователей нажмите на заголовки каждой из колонок. Вы также можете отключать пользователей от Firebox. Для того чтобы отключить пользователя от Firebox нажмите правой кнопкой на имя пользователя и выберите **Log Off User**.

Просмотр или изменение списка Blocked Sites (закладка Blocked Sites)

Закладка **Blocked Sites List** системы Firebox System Manager содержит все временно заблокированные внешние IP-адреса. Причиной блокировки внешнего IP-адреса может быть много: сканирование портов, атака типа «спуфинг», сканирование адресного пространства, или любое настроенное вами событие.

Столбец **Expiration** для каждого IP-адреса показывает время, когда адрес должен быть удален из закладки **Blocked Sites.**



Рядом с каждым IP-адресом отображается время, в течение которого сайт будет находиться в списке **Blocked Sites**. Более подробную информацию см. в "Временная блокировка сайтов при помощи политики"

Изменение списка Block Sites

В закладке Firebox System Manager Blocked Sites вы можете временно изменять параметры определенных IP-адресов в списке **Blocked IP List**. Вы можете добавить сайт в список, изменить срок нахождения этого сайта в списке или удалить сайт из списка.

Для того чтобы временно добавить сайт в список **Blocked IP List** выполните следующее:

1. Нажмите **Add**.
   Откроется диалоговое окно Add Temporary Blocked Site

2. Введите IP-адрес для блокировки.

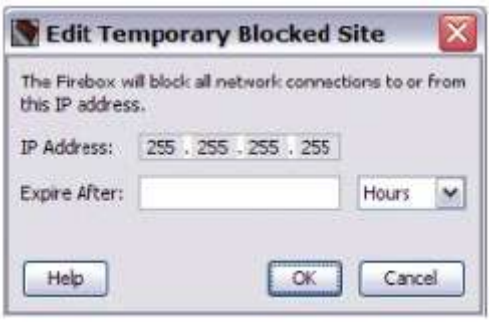
3. Введите значение в поле **Expire After** и выберите **Hours**, **Minutes**, или **Seconds** из выпадающего списке для установки времени блокировки сайта.

4. Нажмите **OK**.
   Откроется диалоговое окно Add Blocked Site.

5. Введите пароль конфигурации для вашего Firebox и нажмите **OK**.
   IP-адрес появится в списке Blocked IP List.

Для изменения времени, в течение которого сайт будет удален из списка **Blocked IP List**:

1. Выберите сайт в **Blocked IP List** и нажмите **Change Expiration**.
   Откроется диалоговое окно Edit Temporary Blocked Site для выбранного IP-адреса.



2. Проверьте значение **IP Address**.

3. Введите новый срок действия в поле **Expire After** и выберите **Hours**, **Minutes**, или **Seconds** из выпадающего списка.

4. Нажмите **OK**.
   Откроется диалоговое окно Update Site.

5. Введите пароль конфигурации для вашего Firebox и нажмите **OK**.

Для удаления сайта из **Blocked IP List**:

1. Выберите сайт из **Blocked IP List** и нажмите **Delete**.
   Откроется диалоговое окно Delete Site(s).

2. Введите пароль конфигурации для вашего Firebox и нажмите **OK**.
   IP-адрес удалится из списка Blocked IP List.

Вам следует открыть Firebox с паролем конфигурации для удаления сайта из списка.

Заблокированные сайты и Traffic Monitor

Когда IP-адрес находится в списке Blocked Sites, сообщения журнала о трафике, которое включает в себя это адрес, отображает интерфейс назначения в качестве *unknown.*

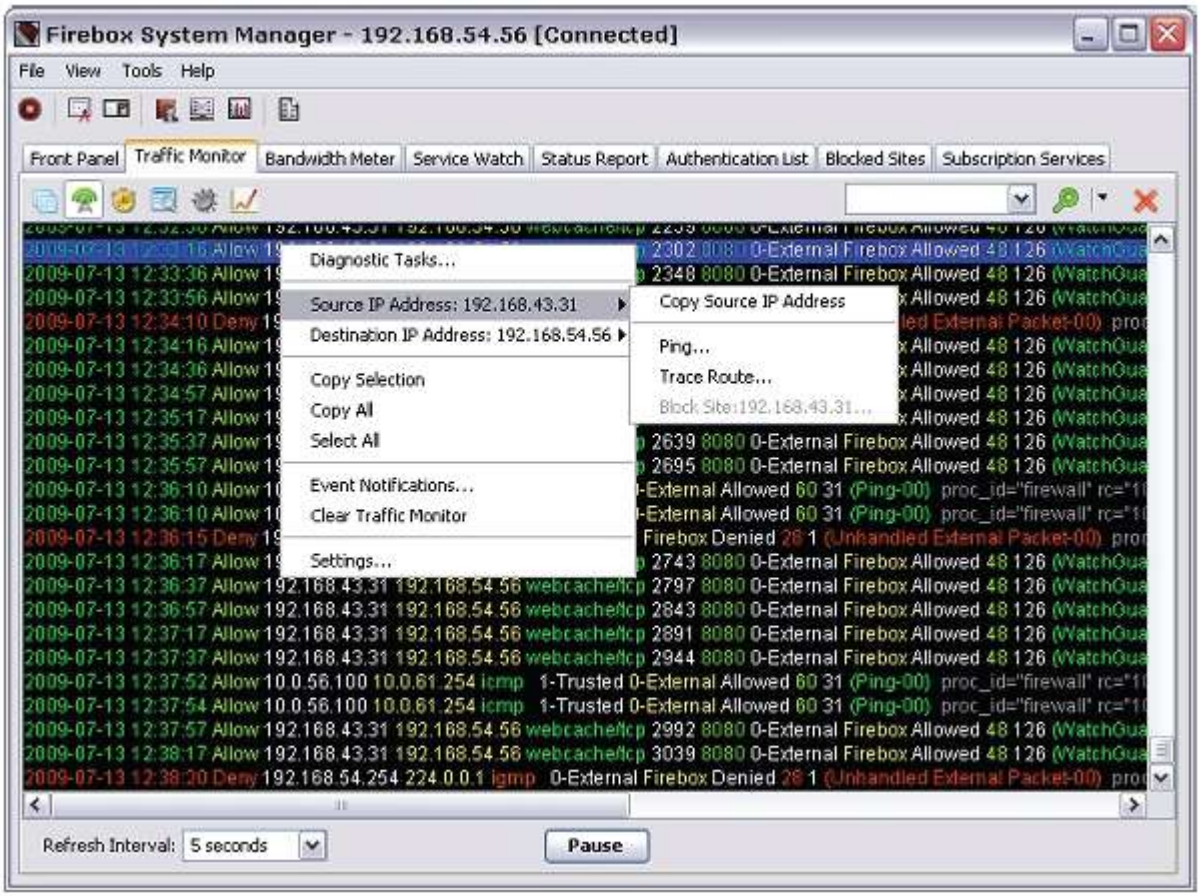
В Firebox System Manager (FSM) вы можете видеть интерфейс назначения и добавить IP-адрес в список временно заблокированных сайтов.

Для того чтобы посмотреть интерфейс назначения выполните следующее:

1. Выберите закладку **Traffic Monitor**.

2. Выберите сообщение.

3. Нажмите правой кнопкой мыши на сообщение и выберите **Destination IP Address**.
   Откроется диалоговое окно Destination IP address и меню опции



Для сохранения циклов вычисления Fireware не идентифицирует интерфейс назначения для пакетов, если IP-адрес источника или назначения блокируется.

Для блокировки IP-адреса интерфейса назначения:

1. Выберите закладку **Traffic Monitor**.

2. Выберите сообщение.

3. Нажмите правой кнопкой мыши на сообщение и выберите **Destination IP Address**.
   Откроется диалоговое окно Destination IP address и меню опции.

4. Выберите **Block Site**.
   Откроется диалоговое окно Choose Expiration

5. Введите необходимое значение в поле **Expire After** и выберите **Hours**, **Minutes**, или **Seconds и**з выпадающего списка.

6. Нажмите **OK**.
   Откроется диалоговое окно Update signature.

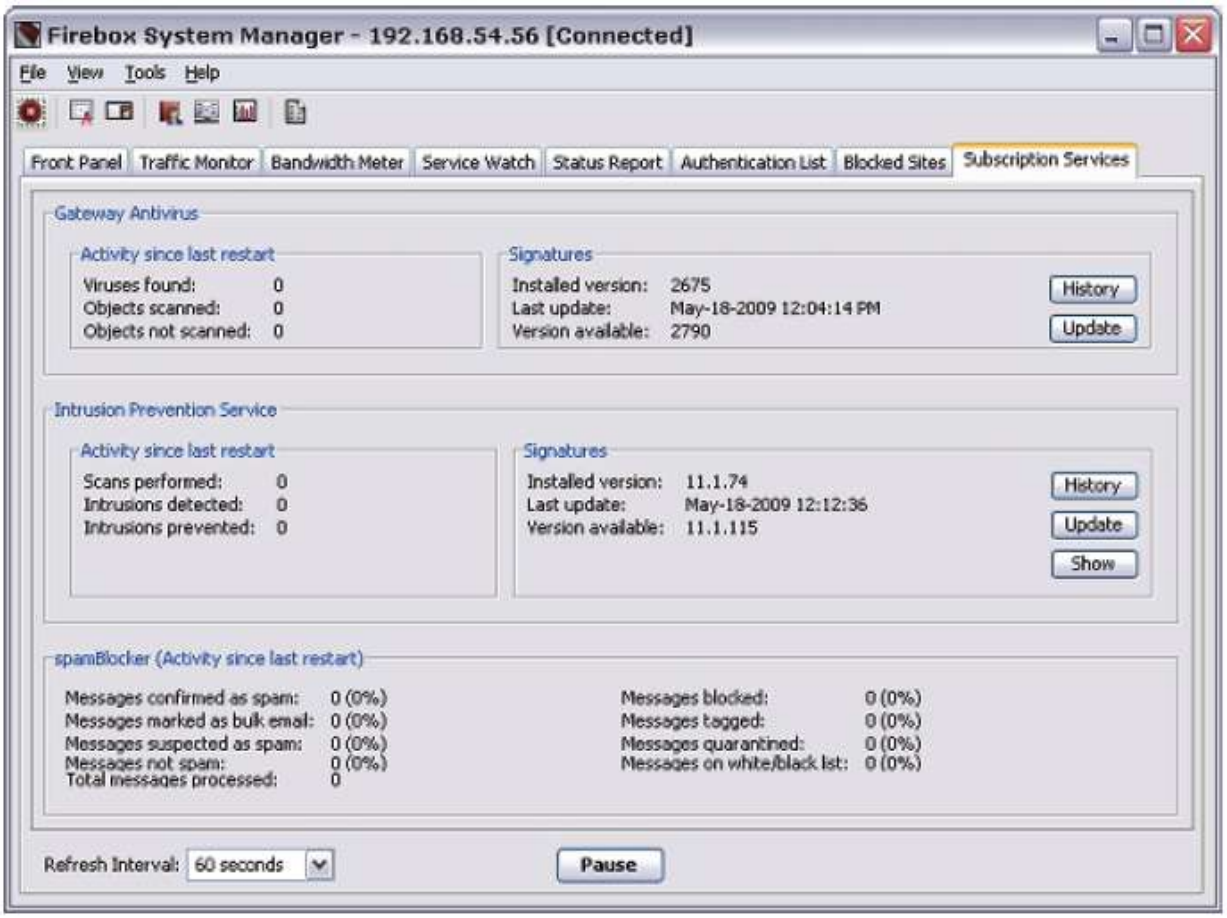
7. Введите пароль конфигурации вашего Firebox и нажмите **OK**.
   IP-адрес временно добавляется в список Blocked Sites на некоторое время.

Статистика по сервисам безопасности (закладка Subscription Services)

Закладка Firebox System Manager **Subscription Services** включает текущую статистику Firebox об сервисах, если установлено:

- Статистика Gateway AntiVirus
- Статистика Intrusion Prevention Service
- Статистика spamBlocker

Вы можете так же использовать эту страницу для обновления подписей для Gateway AntiVirus и подписей для IntrusionPrevention Service



Статистика Gateway AntiVirus

Закладка **Security Services** системы Firebox System Manager содержит статистику по Gateway AntiVirus.

Activity since last restart

- **Viruses found**: Количество найденных вирусов с момента последней перезагрузки Firebox.
- **Objects scanned/not scanned**: Количество просканированных и непросканированных файлов с момента последней перезагрузки Firebox.

Signatures

- **Installed version**: Номер версии установленных сигнатур.
- **Last update**: Дата последнего обновления сигнатур
- **Version available**: Если доступна новая версия сигнатур.
- **Server URL**: URL к которому подключается Firebox для поиска сигнатур и URL, откуда устройство Firebox загружает сигнатуры.
- **History**: Список всех обновлений сигнатур. Вы можете скопировать информацию об одном обновлении или можете скопировать весь список.

- **Update**: Обновление сигнатур. Эта кнопка активна, только если доступна новая версия сигнатур.

Статистика по Intrusion Prevention Service

Закладка **Security Services** Firebox System Manager содержит статистическую информацию о сервисе IPS (Intrusion Prevention Service)

Activity since last restart

- **Scans performed**: Количество просканированных файлов с момента последней перезагрузки Firebox.
- **Intrusions detected**: Количество обнаруженных проникновений с момента последней перезагрузки Firebox.
- **Intrusions prevented**: Количество зараженных файлов, которые были удалены, начиная с момента последней перезагрузки Firebox.

Signatures

- **Installed version**: Версия сигнатур
- **Last update**: Дата последнего обновления сигнатур
- **Version available**: Если доступна новая версия сигнатур
- **Server URL**: URL к которому подключается Firebox для поиска сигнатур и URL, откуда устройство Firebox загружает сигнатуры.
- **History**: Список всех обновлений сигнатур. Вы можете скопировать информацию об одном обновлении или можете скопировать весь список.
- **Update**: Обновление сигнатур. Эта кнопка активна, только если доступна новая версия сигнатур.
- **Show**: Нажмите на эту кнопку для того чтобы загрузить и посмотреть список всех сигнатур IPS. После того, как вы загрузите все сигнатуры, вы можете найти необходимую сигнатуру по ее ID.

Статистика по spamBlocker

Закладка **Security Services** системы Firebox System Manager содержит статистическую информацию по активности spamBlocker, которая наблюдалась после последней перезагрузки устройства.

Статистика включает количество и процентное соотношение для каждого типа сообщения в выбранной категории:

- Сообщения, которые после последней перезагрузки были установлены, как:

  * bulk-почта

  * спам

  * подозрительный спам

  * не спам

- Сообщения после последней перезагрузки:

  * заблокированные

  * помеченные

  * отправленные на Сервера Карантина

- Количество сообщений, которые были заблокированы или разрешены списком исключений, которые вы создали в spamBlocker

  * исключения, которые вы создали для блокировки отдельных сайтов называется черным списком

  * исключения, которые были созданы для разрешения доступа к определенным сайтам, называются белым списком.

Если вы перезагрузите Firebox, все счетчики обнулятся.

Утилита HostWatch

Утилита HostWatch представляет собой графический интерфейс, который показывает соединения между различными интерфейсами Firebox. HostWatch также предоставляет информацию о пользователях, соединениях, портах и другую информацию.

Окно HostWatch

Верхняя часть окна HostWatch разделена на две части. В левой части вы можете настроить интерфейс, за работой которого вы хотите следить. В правой части будут показаны все входящие и исходящие подключения интерфейса, который вы поместили в левую часть.

Линии, соединяющие хосты-источники с хостами назначения, обозначены цветом, который показывает тип соединения. Вы можете изменить эти цвета. По умолчанию используются следующие цвета:

- **Red** — Firebox запрещает подключение.
- **Blue** — Соединение использует прокси.
- **Green** — Для соединения Firebox использует NAT
- **Black** — Нормальное соединение (соединение установлено и оно не использует ни прокси, ни NAT).

Иконки, которые показывают тип сервиса, появляются рядом с серверами.

DNS разрешение и HostWatch

DNS (Domain name server) разрешение не происходит сразу после запуска HostWatch. Если HostWatch настроен для DNS разрешения, он заменяет IP-адреса именами хостов или пользователей.

Если Firebox не может идентифицировать хост или имя пользователя, в окне HostWatch отображается IP-адрес. Если вы используете DNS разрешение с утилитой HostWatch, то станция управления будет отправлять большое количество NetBIOS пакетов (UDP 137) через Firebox. Единственный способ отключить его – это выключить NetBIOS over TCP/IP в ОС Windows.

Запуск HostWatch

Для запуска приложения HostWatch:

1. Откройте Firebox System Manager.

2. Нажмите  . Или выберите **Tools** > **HostWatch**.
   Экран автоматически запустится.

Приостановки и запуск экрана HostWatch

Для приостановки экрана HostWatch выполните следующие действия:

В окне HostWatch нажмите  .

Или выберите **File > Pause**.

Для запуска экрана HostWatch выполните следующее:

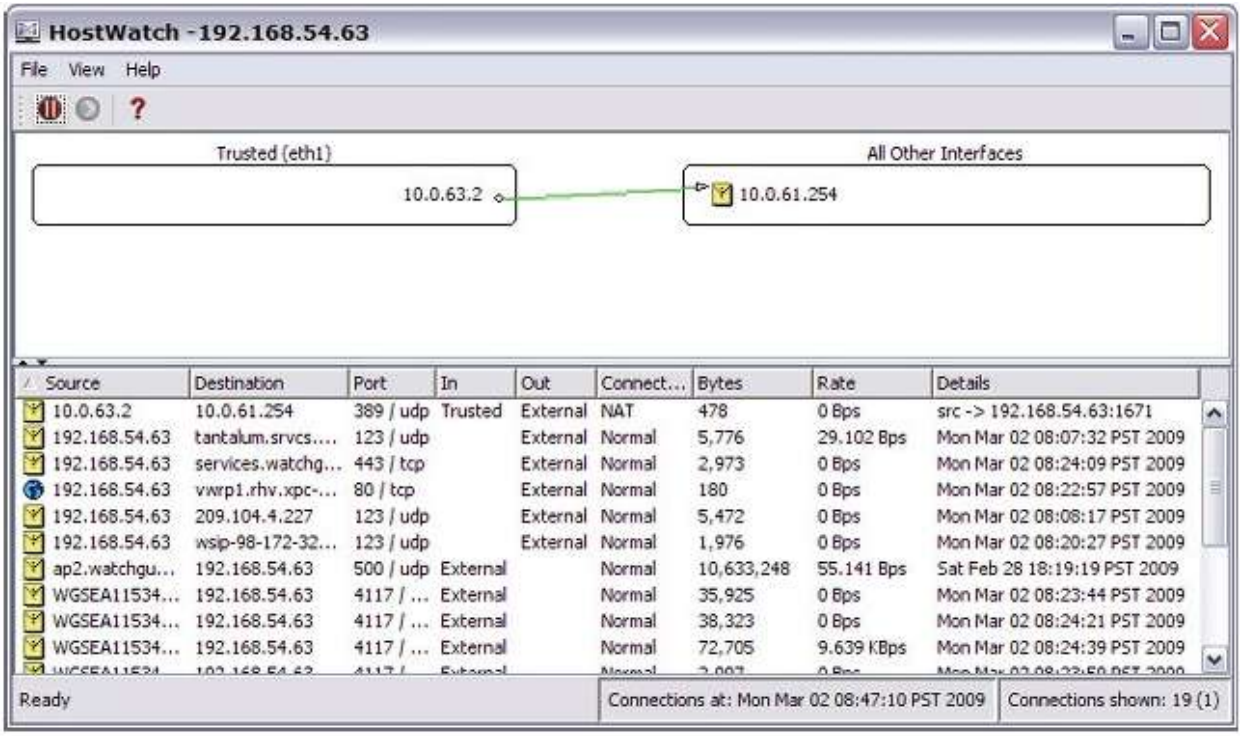
В окне HostWatch нажмите  .

Или выберите **File > Continue**.

Выбор соединений и интерфейсов для мониторинга

При первом запуске HostWatch в левом верхней части окна вы видите внутренние интерфейсы Firebox и соединения через эти интерфейсы в верхнем правом углу.

Подключения к/от этих интерфейсов появится в верхнем правом углу окна в списке **All Other Interfaces.**



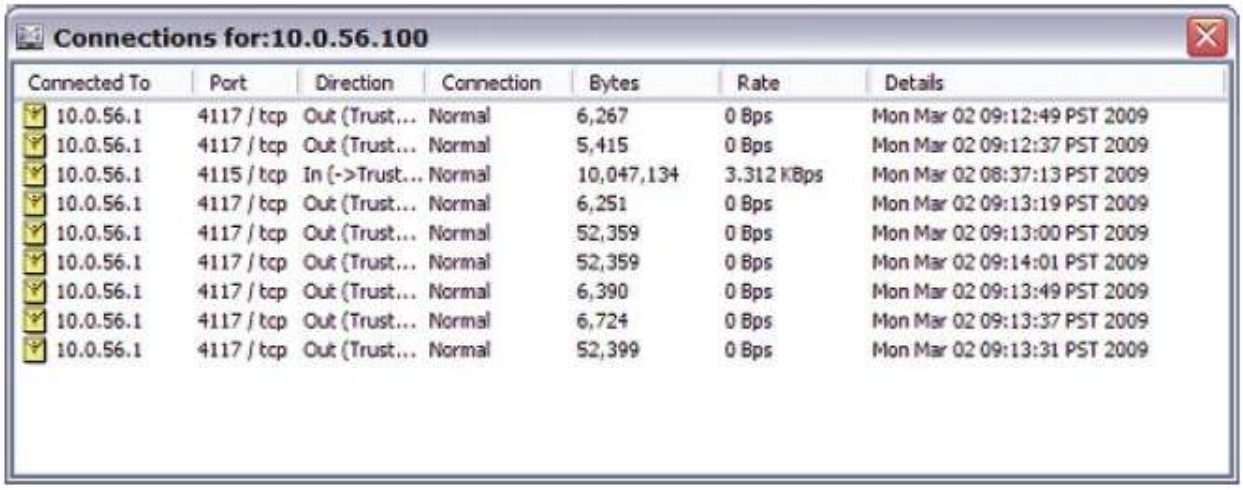
Просмотр подключений

Вы можете подключить HostWatch для просмотра информации о соединении и включить IP адреса, номер порта, время, тип и направление соединения. В нижней части окна HostWatch показаны все соединения через все интерфейсы. Информация, представленная в таблице, включает:

- Источник и место назначения
- Номер порта
- Используемый интерфейс Firebox и тип трафика (входящий или исходящий)
- Тип соединения (нормальное, через прокси, заблокированное)
- Такие параметры, как время создания соединения или команда, которая использовалась для создания соединения

Для просмотра соединений интерфейса необходимо выполнить:

Дважды нажмите на пункт в любой – левом или правом списке.
Откроется диалоговое окно *Connections For .*



Выбор нового интерфейса для мониторинга

Для выбора нового интерфейса из HostWatch:

1. Выберите **View** > **Interface**. Или нажмите правой кнопкой на имя интерфейса.
2. Выберите новый интерфейс для мониторинга.

Для точного определения имени интерфейса или использования регулярных выражений для нескольких интерфейсов:

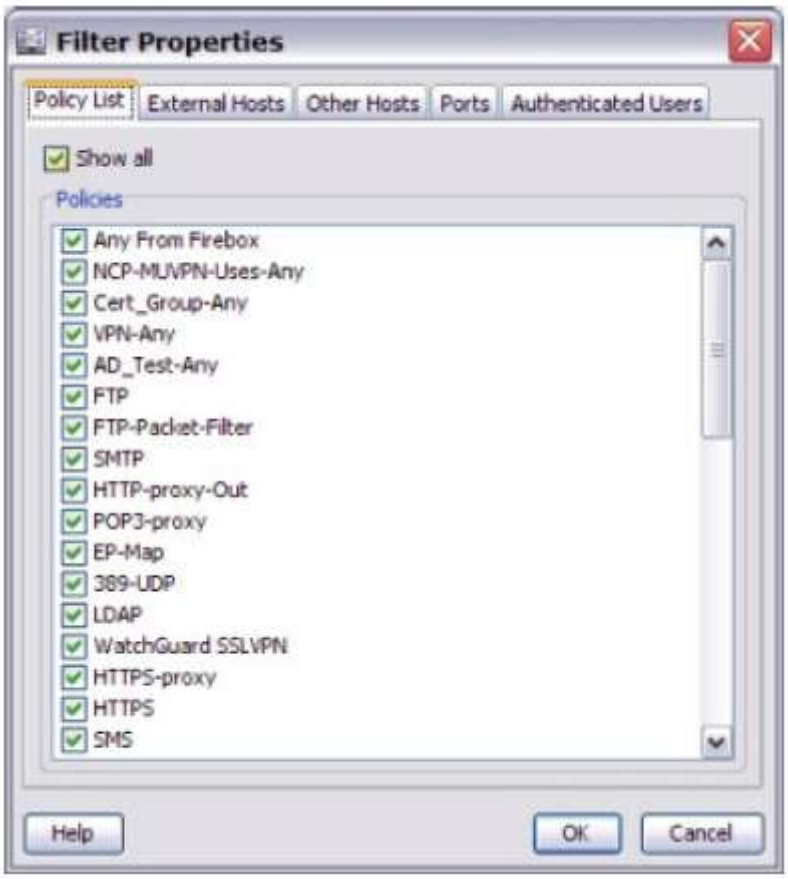
1. Выберите **View** > **Interface**. Или нажмите правой кнопкой на текущее имя интерфейса.
2. Выберите **Other** из списка интерфейсов.

Вы можете использовать эту опцию для просмотра VLAN в HostWatch.

Фильтрация содержимого окна HostWatch

По умолчанию HostWatch показывает все политики, хосты, порты и аутентифицированных пользователей. Вы можете настроить окно HostWatch таким образом, чтобы оно отображало только необходимое вам содержимое. Вы можете использовать эту функцию для мониторинга определенных политик, хостов, портов или пользователей.

1. В HostWatch выберите **View > Filter**.
   Откроется диалоговое окно Filter Properties.
   Имя вторичной закладки изменится для сопоставления выбранного интерфейса при мониторинге



2. Нажмите на закладку для мониторинга.

3. В закладке для каждого пункта, которые вы хотите просмотреть, в поле Hosts или Authenticated Users введите IP-адрес, номер порта или имя пользователя для мониторинга. Нажмите Add.

4. Для фильтрации по политике выберите закладку **Policy List** и отметьте опцию для каждой политики, которую вы хотите использовать для мониторинга.

5. Для отображения всех пунктов в категории выберите опцию **Show all** на каждой закладке.

6. Нажмите **OK**.

Изменение параметров отображения HostWatch

Вы можете изменить способ отображения информации утилитой HostWatch. Например, вы можете вместо IP адресов отображать имена хостов.

1. В HostWatch выберите **View > Settings**.

2. Выберите закладку **Display** для изменения отображения хостов в окне HostWatch

3. Выберите закладку **Line Color** для изменения цветов линии для подключений **NAT**, **Proxy**, **Blocked Normal**

4. Нажмите **OK** для закрытия диалогового окна **Settings**.

Открыть или заблокировать сайт при помощи утилиты HostWatch

Вы можете открыть сайт для отображения в HostWatch.

1. На нижней панели окна нажмите правой кнопкой на сайт и выберите **Visit Proxied Website**.

2. В всплывающем окне введите адрес сайта.

Вы так же можете заблокировать IP-адрес и добавить его в список Blocked Sites:

1. В верхней части панели нажмите правой кнопкой на IP-адрес и выберите **Block Site: [адрес сайта]**. Или нажмите правой кнопкой на соединение в нижней части панели выберите одно из двух: **Block Site: [адрес отправителя]** или **Block Site: [адрес назначения]**.
   Откроется диалоговое окно Choose Expiration

2. В поле **Expire After** введите период времени для сайта на время блокировки. Вы можете выбрать **Hours**, **Minutes** или **Seconds** из выпадающего списка.

3. При необходимости введите пароль вашей конфигурации.

Firebox блокирует все сетевые подключения к/от этого IP-адреса.

Консоль Performance Console

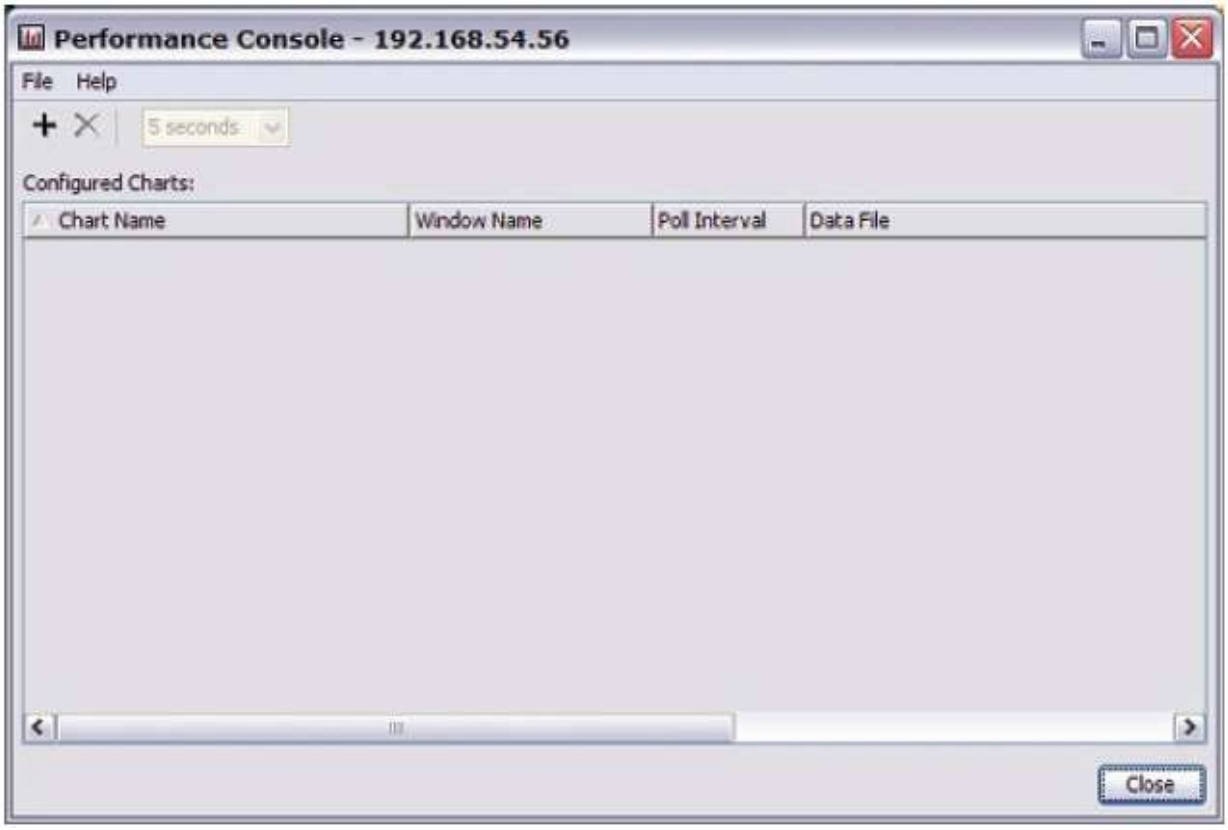
Performance Console – это утилита, которая используется для построения графиков, которые показывают работу различных компонентов Firebox. Для того чтобы получить необходимую информацию вы создает счетчики, которые идентифицируют информацию, использующуюся для построения графиков.

Запуск консоли Performance Console

Для того чтобы запустить консоль Performance Console в Firebox System Manager:

1. Нажмите . Или выберите **Tools** > **Performance Console**.
   Откроется диалоговое окно Add Chart.

2. Для закрытия диалогового окна Add Chart и просмотра Performance Console нажмите **Cancel**.
   Откроется диалоговое окно Performance Console.



3. Или добавьте и задайте счетчики, который идентифицируют информацию.

Более подробную информацию о Performance Console и счетчиках см. в Define performance counters.

Создание графиков при помощи Performance Console

Для создания графиков в Performance Console:

1. Создайте счетчики производительности. Счетчики сгруппированы по категориям, список которых приведен в "Types of counters" ниже.

2. Измените график или добавьте новый график

Типы счетчиков

Вы можете использовать следующие счетчики производительности:

System Information

Отображает использование процессора.

Interfaces

Мониторинг работы выбранных интерфейсов и событий, связанных с ними. Например, вы можете создать счетчик, который отслеживает количество пакетов, получаемых определенным интерфейсом.

Policies

Мониторинг выбранных политик и событий, связанных с ними. Например, вы можете создать счетчик, который отслеживает число пакетов, обрабатываемых политикой.

VPN Peers

Мониторинг выбранных VPN-политик и событий связанных с ними.

Tunnels

Мониторинг выбранных VPN-туннелей и событий связанных с ними.

Остановка мониторинга или закрытие окна

Вы можете остановить мониторинг для сохранения ресурсов и перезапустить их в другое время.

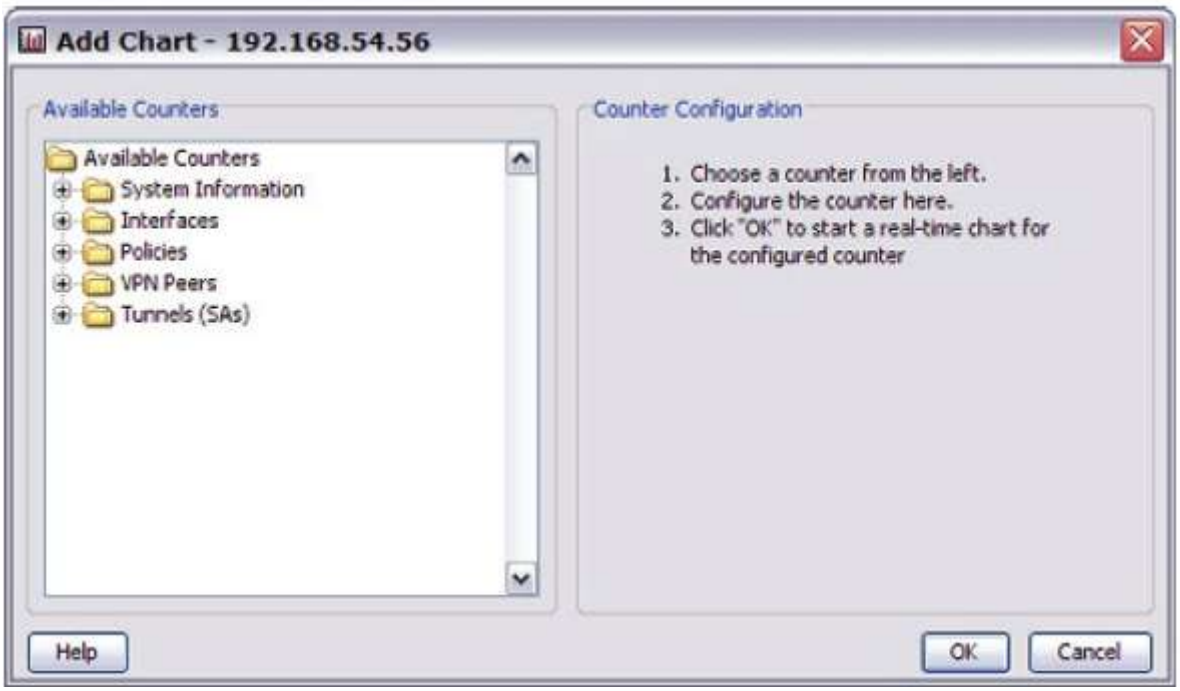
1. Нажмите **Stop Monitoring**.
   Performance Console больше не получает данные для данного счетчика.

2. Нажмите **Close** для закрытия окна с графиком.

Создание счетчиков производительности

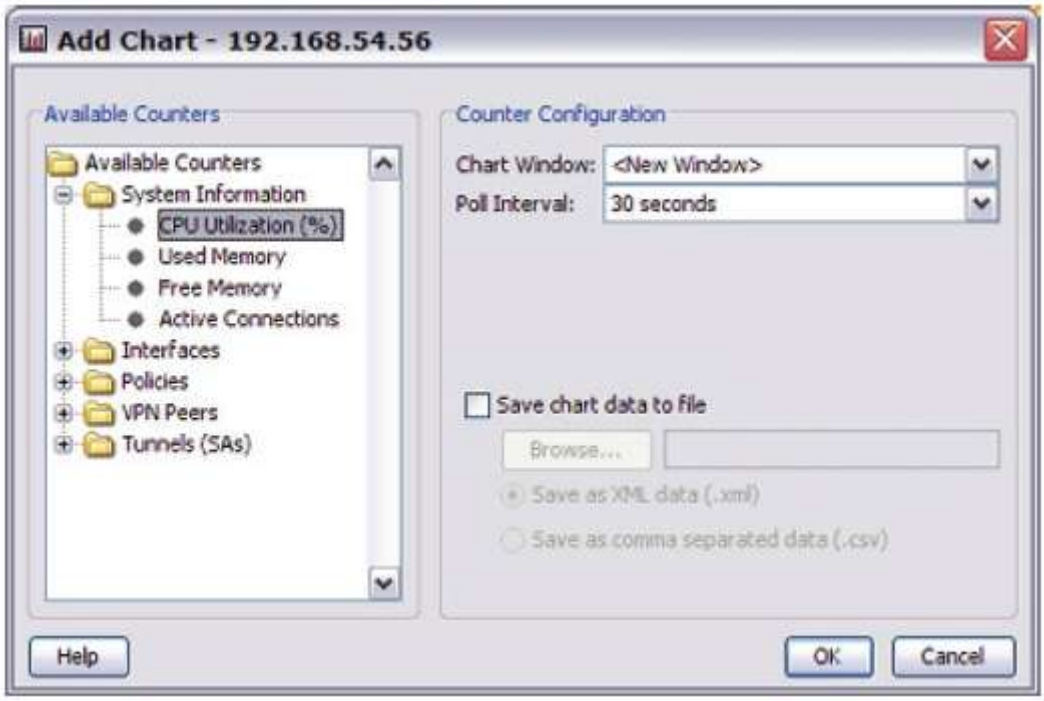
Для того чтобы создать счетчик для любой из этих категорий в списке Available Counters выполните следующее:

1. В Firebox System Manager нажмите . Или выберите **Tools** > **Performance Console**.
   Откроется диалоговое окно Add Chart



2. В списке **Available Counters** откройте категорию счетчика.
   Откроются допустимые счетчики для данной категории.

3. Выберите счетчик такой, как **CPU Utilization**. Поля Counter Configuration автоматически обновятся в зависимости от выбранного счетчика



4. В выпадающем списке **Chart Window** выберите **<New Window>** для появления графика в новом окне. Или выберите имя в открытом окне для добавления графика в это окно.

5. В выпадающем списке **Poll Interval** выберите временной интервал. Это частота, с которой консоль Performance Console загружает обновленную информацию с Firebox.

6. Добавьте необходимую конфигурационную информацию по выбранному счетчику. Эти поля конфигурации соответствуют счетчику, и разные счетчики имеют различные поля.

   Допустимые поля включают:

   Type

   Из выпадающего списка выберите тип создаваемого графика: **Rate**, **Difference**, или **Raw Value**. Например, вы хотите построить график для значения value_1 в момент времени time_1, value_2 в момент времени time_2 и т.д.

   * Если вы создаете график типа **Rate**, вы используете следующие значения: (value_2-value_1)/ (time_2-time_1), (value_3-value_2)/(time_3-time_2) и т.д.

   * Если тип графика - **Difference**, вы используете следующие значения: value_2-value_1, value_3-value_2, и т.д.

   * Если тип графика - **Raw Value**, вы используете следующие значения: value_1, value_2, и т.д. Эти значения являются обычными счетчиками контента (байтов или пакетов). Такие значения могут только увеличиваться

   Interface

   Выпадающий список для выбора интерфейса, для которого вы хотите построить график.

   Policy

   (Если вы выберете Policy counter) Выпадающий список для выбора политики, для которого вы хотите построить график. Вы можете обновить список политики, который появится в Performance Console при нажатии на кнопку **Refresh Policy List.**

Peer IP

(Если выберете счетчик VPN Peers) Выпадающий список для выбора IP-адреса конечной точки VPN, для которой вы хотите построить график. Если вы выберете счетчик VPN Peers, то, нажав на кнопку **Refresh Peer IP List**, вы можете обновлять список политик, который отображается в консоли Performance Console.

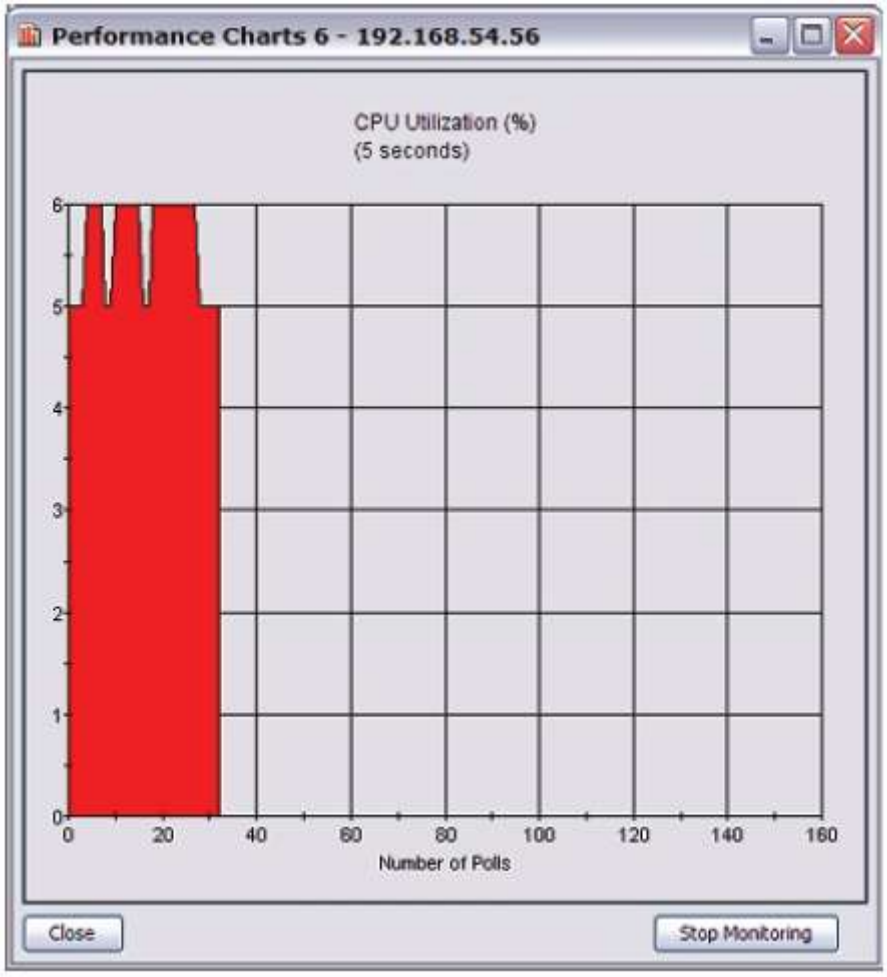
Tunnel ID

(Если вы выберете счетчик Tunnels) Выпадающий список для выбора VPN-туннеля, для которого вы хотите построить график. Вы можете обновить список VPN –туннелей, которые появляются в Performance Console, нажав на кнопку Refresh Tunnel ID List. Если вы не знаете ID вашего VPN-туннеля, посмотрите в закладке Front Panel Firebox System Manager.

7. Выберите опцию **Save Chart Data to File** для сохранения данных, собранных Performance Console.

8. Нажмите **Browse** для выбора расположения при сохранении файла и выбора формата сохраняемых данных – XML или CSV. Например, вы можете открыть XML-файл в Microsoft Excel для того, чтобы посмотреть каждое значение, записанное для каждого интервала опроса. Вы можете использовать другие программы для того, чтобы объединять данные с нескольких файлов.

9. Нажмите **OK** для запуска графика в реальном времени для данного счетчика. Графики появятся в реальном времени окна. Вы можете просмотреть один/несколько графиков в каждом окне.

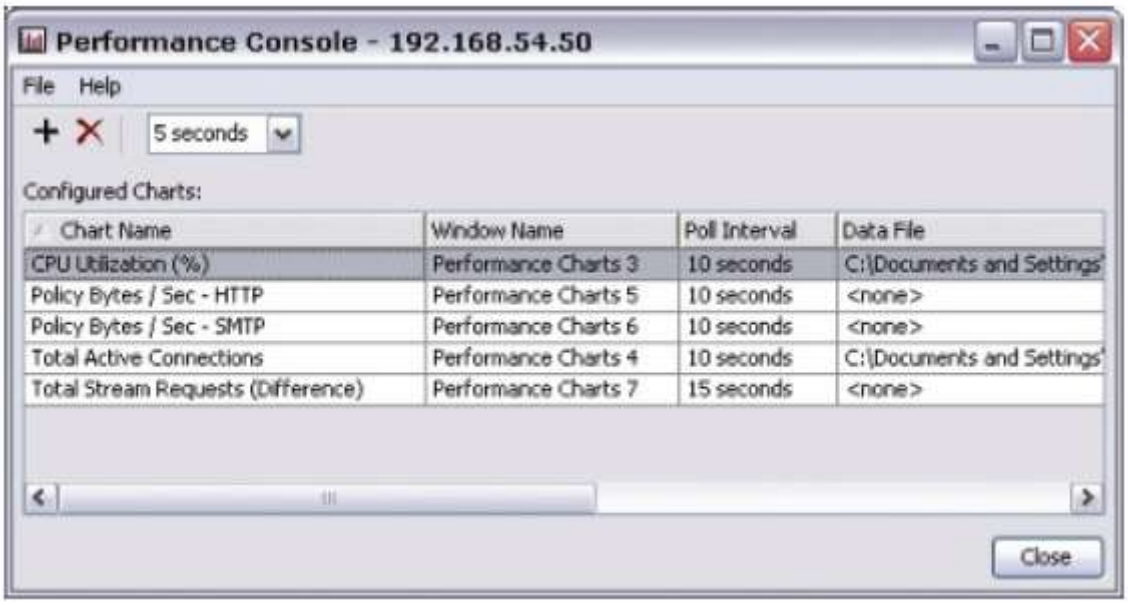


Графики автоматически масштабируются для соответствия данным и обновляются каждые 5 секунд.

Этот график показывает использование CPU. Для других функций вы создаете графики, используя ту же самую процедуру

Добавление графиков и изменение интервалов опроса

Основное окно консоли Performance Console показывает таблицу, которая содержит все активные и настроенные счетчики производительности. В этом окне вы можете создавать новые графики или изменять интервал опроса для каждого счетчика.



Добавление нового графика

Для добавления нового графика необходимо выполнить:

1. Нажмите . Или выберите **File** > **Add Chart**.
   Откроется диалоговое окно Add Chart.

2. Определите счетчик производительности для графика.

Изменение интервала опроса

Для изменения интервала опроса для одной консоли производительности выполните следующее:

1. Выберите имя графика из списка.

2. Нажмите на интервал опроса в выпадающем списка на панели инструментов Performance Console и выберите новый период между опросами.
   *Новая частота появится в столбце **Poll Interval**.*

Удаление графика

Для удаления графика:

1. Выберите имя графика из списка и нажмите. Или выберите **File > Delete Chart**.
   Откроется диалоговое окно подтверждения.

2. Нажмите **Yes** для удаления графика.

Просмотр и управление сертификатами Firebox

Firebox System Manager (FSM) включает диалоговое окно **Certificates** , из которого вы можете определять различные задания, связанные с вашими сертификатами.

Вы можете:

- Посмотреть список текущих сертификатов Firebox и данные о каждом сертификате
- Удалить сертификат из устройства Firebox.
- Создавать запрос на генерацию сертификата.
- Импортировать сертификат стороннего Центра Сертификации и хранить его в списке доверенных сертификатов.

Для открытия диалогового окна **Certificates** в Firebox System Manager необходимо выполнить:

1. Запустите Firebox System Manager.

2. Нажмите  . Или выберите **View** > **Certificates**.
   Откроется диалоговое окно Certificates.

Более подробную информацию о заданиях для сертификатов для в FSM см.в See and manage Firebox certificates.

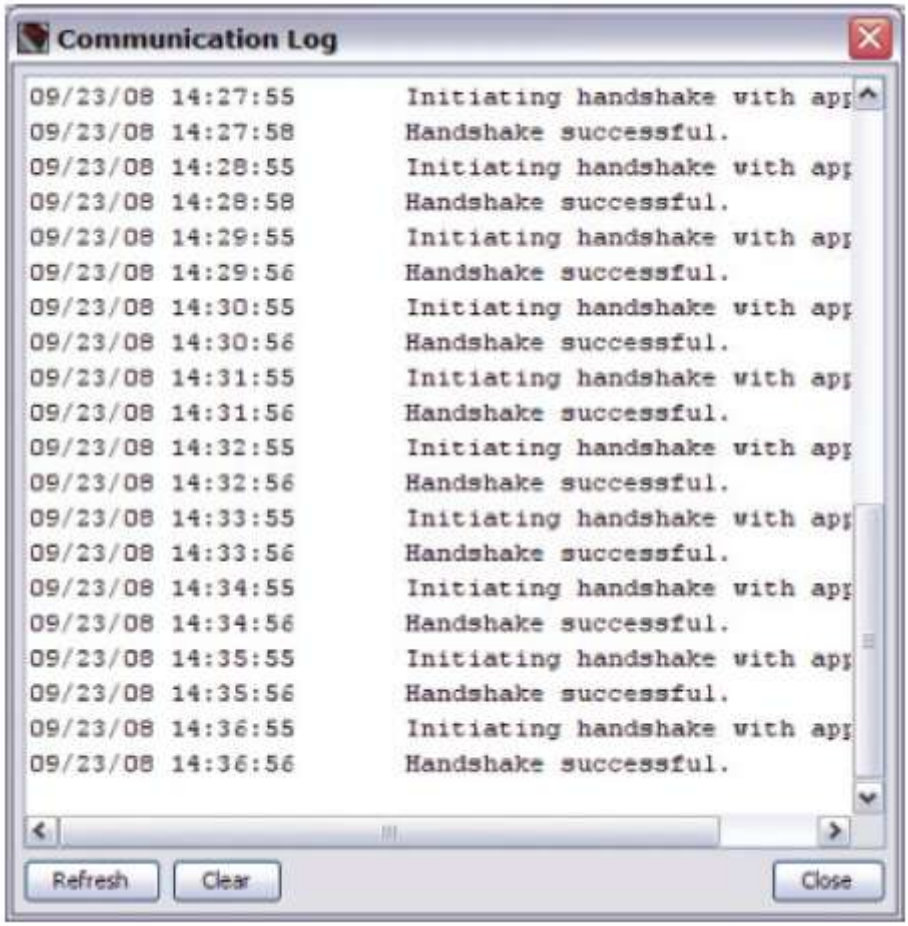
Журнал коммуникаций (Communication log)

Журнал коммуникаций содержит такую информацию, как количество удачных и неудачных попыток входа в систему, квитирование и т.д.

Это подключения между Firebox и Firebox System Manager. Для того чтобы посмотреть журнал в Firebox System Manager:

1. Запустите Firebox System Manager.

2. Нажмите . Или выберите **View > Communication Log**.
   Откроется диалоговое окно Communication Log



3. Этот журнал запускается при первом удачном входе в систему и показывает информацию о текущей сессии.

4. Перезагрузите информацию журнала в диалоговое окно, нажав **Refresh**.

5. Для удаления всей информации из Журнала коммуникаций нажмите **Clear**.
   Вся информация удалиться из журнала коммуникаций и не подлежит восстановлению.

Выполнение операций в Firebox System Manager

Вы можете использовать инструменты Firebox System Manager для выполнения различных задач на вашем Firebox.

Эти задачи включают:

- Синхронизация системного времени
- Перезагрузка или выключение вашего Firebox
- Очистка ARP кэша

- Просмотр и синхронизация ключей функций
- Синхронизация ключей функции
- Расчет контрольной суммы Fireware XTM
- Отчистка тревог
- Повторное создание ключей для BOVPN туннелей
- Управление FireCluster

Синхронизация системного времени

Эта команда используется для синхронизации времени Firebox с системным временем.

1. В Firebox System Manager выберите **Tools > Synchronize Time**.
   Откроется диалоговое окно Synchronize Firebox Time

2. Введите пароль конфигурации вашего устройства.
3. Нажмите **OK**.
   Появится сообщение о синхронизации времени устройства с управляющей станцией.

Перезагрузка или выключение вашего Firebox

Вы можете использовать Firebox System Manager (FSM) для удаленной перезагрузки или выключения вашего Firebox.

Для перезагрузки вашего Firebox необходимо выполнить:

1. Подключиться к Firebox.
2. Запустить Firebox System Manager.
3. Выбрать **File** > **Reboot**.
   Появится сообщение о подтверждении.
4. Нажать **Yes**.
   Firebox выполнит перезагрузку.

Для выключения вашего Firebox:

1. Подключиться к Firebox.
2. Запустить Firebox System Manager.
3. Выбрать **File** > **Shutdown**.
4. Нажать **Yes**.
   Firebox выключится.

Очистка ARP кэша

ARP (Address Resolution Protocol) кэш содержит аппаратные адреса (также известные как MAC-адреса) TCP/IP хостов. Перед началом ARP запроса, система проверяет наличие адреса в кэше. Если ваша сеть имеет drop-in конфигурацию, то после подключения устройства Firebox вам необходимо будет очистить ARP кэш.

1. В Firebox System Manager выберите **Tools > Clear ARP Cache**.

2. Введите пароль конфигурации вашего устройства.

3. Нажмите **OK**.
   Все записи кэша сбросятся.

В режиме drop-in на Firebox эта процедура очищает только содержимое ARP-таблицы, но не таблицу MAC-адресов. Самые старые записи в таблице MAC-адресов удаляются при наличии более 2000 записей. Если вы хотите очистить таблицу MAC, вам необходимо перезагрузить Firebox.

Просмотр и синхронизация ключей функций

Вы можете использовать ключи функции, установленные на вашем Firebox из Firebox System Manager.

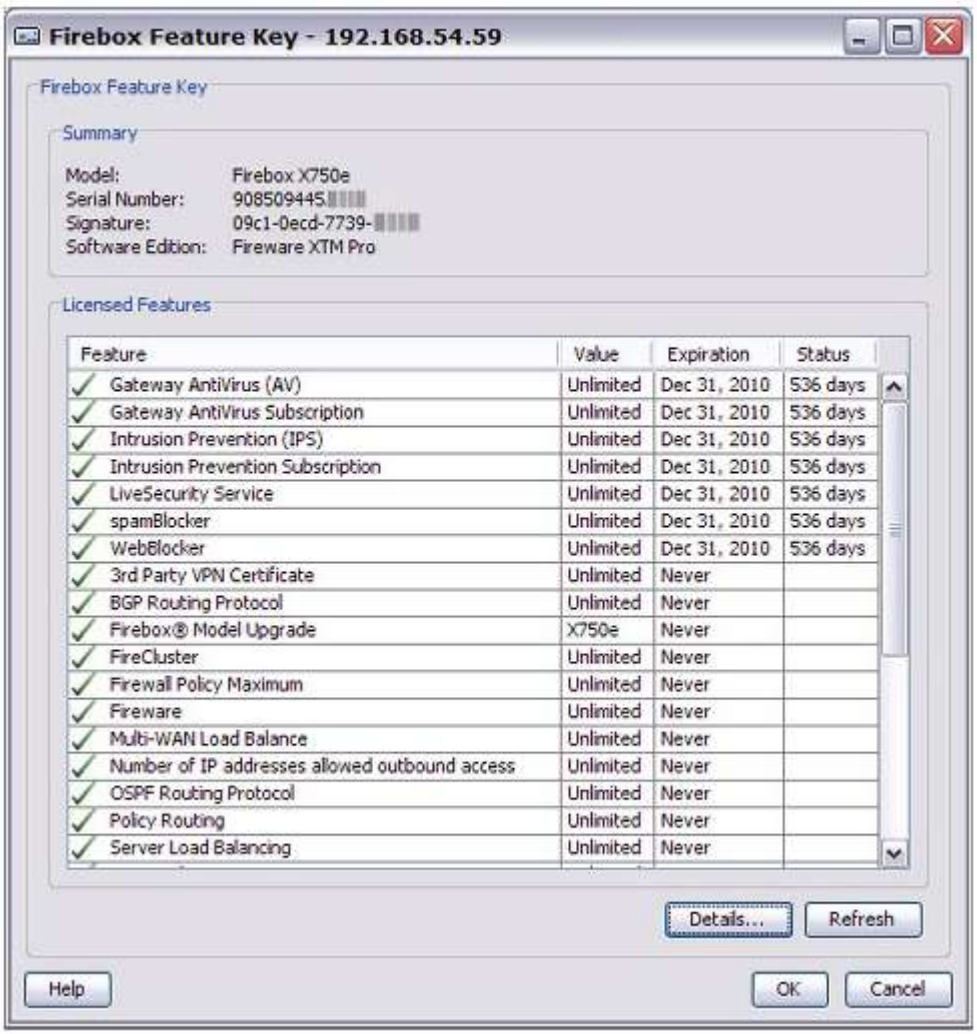
Вы можете так же получить новый функциональный ключ из LiveSecurity.

Просмотр ключей функций

Вы можете просмотреть функциональные ключи:

1. Запустите Firebox System Manager.

2. Нажмите . Или выберите **View > Feature Keys**.
   Откроется диалоговое окно Firebox Feature Key.



Feature

Название компонента, например подписка на spamBlocker.

Value

Например, количество разрешенных VLAN интерфейсов или BOVPN туннелей

Expiration

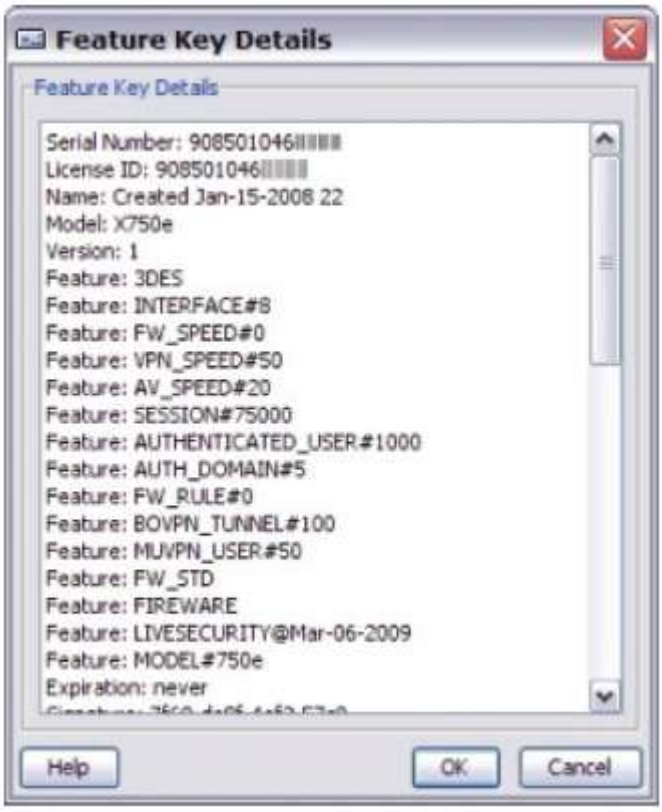
Дата истечения срока действия. Если компонент не имеет срока действия, то в этом поле - **Never**.

Status

Для компонентов с определенным сроком действия, количество оставшихся дней

Details

Просмотр подробной информации о лицензионном ключе.



Refresh

Нажмите для перезагрузки информации функционального ключа в диалоговом окне.

Синхронизация ключей функции

Если вы уже создали учетную запись LiveSecurity, то вы можете получить текущий функциональный ключ:

1. В Firebox System Manager выберите **Tools > Synchronize Feature Key**.
   Откроется диалоговое окно Synchronize Feature Key

2. Введите пароль конфигурации устройства.

3. Нажмите **OK**.
   Firebox подключится в сайте LiveSecurity и загрузит текущий функциональный ключ на ваш Firebox.

Расчет контрольной суммы Fireware XTM

Контрольная сумма используется для проверки целостности данных при передаче и хранении.

Вы можете использовать эту проверку, чтобы убедиться, что Firebox OS не была изменена или повреждена с момента создания на WatchGuard и моментом установки ее на ваш Firebox. Контрольная сумма осуществляется для записей пакета Fireware XTM, но не для каждого файла в пакете. Для нахождения опубликованной контрольной суммы для вашей версии Fireware XTM обратитесь к *Release Notes* для установленной версии Fireware XTM.

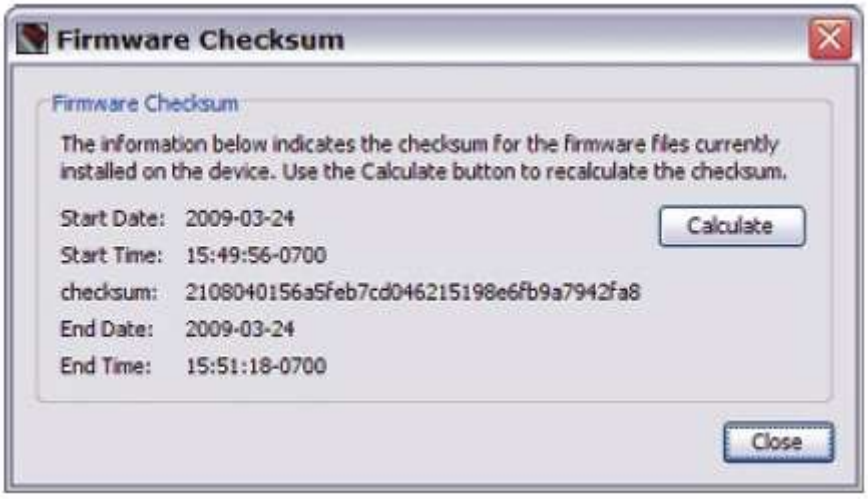
Вы можете использовать Firebox System Manager (FSM) для расчета контрольной суммы для версии установленного Fireware XTM на вашем Firebox, и затем, вы можете сравнить эту величину с контрольной суммой загруженного вами пакета Fireware XTM.

Вам следует подключиться к члену HA-кластера для использования функции на узле HA – кластера.

Более подробную информацию о “Connect to a cluster member” см. на с. 239.

1. Запустите Firebox System Manager.

2. Выберите **Tools** > **Firmware Checksum**.
   Откроется диалоговое окно Firmware Checksum и FSM автоматически начнет рассчитывать контрольную сумму. Это может занять некоторое время для завершения



3. Для еще одного расчета контрольной суммы нажмите **Calculate**.

4. Откройте *Release Notes* для установленных версий Fireware XTM и найдите величину контрольной суммы.

5. Сравните найденную величину со значением контрольной суммы, рассчитанной в диалоговом окне **Firmware Checksum**.

Если контрольные суммы совпадают, то ваши пакеты встроенного ПО не изменялись, в противном случае, они могут быть повреждены.

Отчистка тревог

Эта команда очищает список тревог устройства Firebox.

1. Запустите Firebox System Manager.

2. Выберите **Tools** > **Clear Alarm**.
   Откроется диалоговое окно Clear Alarm

3. Введите пароль конфигурации на Firebox.

4. Нажмите **OK**.

Повторное создание ключей для BOVPN туннелей

Обычно конечные точки шлюза BOVPN туннелей должны генерировать и обмениваться новыми ключами после определенного промежутка времени или количества переданного трафика. Иногда вам понадобится срочно сгенерировать новые ключи. Опция повторного создания ключей в Firebox System Manager завершает действие BOVPN туннеля.

Это может быть использовано при устранении неполадок. Туннели начинают работу при начале передаче трафика по ним; они пересоздаются, как только по ним начинается передаваться трафик. Если вы создадите новые ключи для туннеля и по нему трафик передаваться не будет, то этот туннель не будет автоматически пересоздан.

Повторное генерация ключей для одного BOVPN туннеля

1. В Firebox System Manager выберите закладку **Front Panel**.

2. В списке **Branch Office VPN Tunnels** выберите туннель для повторного создания ключа.

3. Нажмите правой кнопкой мыши и выберите **Rekey Selected BOVPN Tunnel**.
   Откроется диалоговое окно Rekey BOVPN Tunnels.

4. Введите пароль конфигурации устройства.

5. Нажмите **OK**.

Повторная генерация ключей для всех BOVPN туннелей

1. В Firebox System Manager, выберите закладку **Front Panel**.

2. Нажмите правой кнопкой мыши в любом месте окна Front Panel.

3. Выберите **Rekey All BOVPN Tunnels**.
   Откроется диалоговое окно Rekey All BOVPN Tunnels.

4. Введите пароль конфигурации устройства.

5. Нажмите **OK**.

или

1. В Firebox System Manager выберите **Tools > Rekey All BOVPN Tunnels**.
   Откроется диалоговое окно Rekey All BOVPN Tunnels.

2. Введите пароль конфигурации Firebox.

3. Нажмите **OK**.

Управление FireCluster

Вы можете выполнять несколько FireCluster операций в Firebox System Manager

Смена паролей

Мы рекомендуем периодически изменять пароли Firebox для дополнительной безопасности. Вы можете изменить состояние и конфигурацию пароля для вашего Firebox из Firebox System Manager.

Вы можете изменять оба пароль одновременно или только один пароль. Для этого вам следует войти под своей учетной записью на Firebox с паролем конфигурации

1. Запустите Firebox System Manager.

2. Выберите **Tools** > **Change Passphrases**.
   Откроется диалоговое окно Change Passphrases

3. Введите и подтвердите новое состояние пароля **Status Passphrase**.

4. Введите и подтвердите новый пароль конфигурации **Configuration Passphrase**.

Нажмите **OK**.
Пароли состояния и конфигурации должны состоять не меньше, чем из 8 символов.

Глава 23 - Отчеты WatchGuard

Сервер отчетов

Сервер отчетов объединяет данные, собранные Серверами Журналов с устройств Firebox, и генерирует из них отчеты. После того, как данные попадают на Сервер Отчетов, вы можете при помощи утилиты Report Manager посмотреть доступные отчеты. Для более подробной информации о Report Manager см. “Утилита Report Manager”. Для более подробной информации об отчетах см. “Список предопределенных отчетов”

Более подробную информацию о настройке вашего Сервера Отчетов см. в “Настройка Сервера Отчетов”

Настройка Сервера Отчетов

При помощи программы установки WatchGuard System Manager вы можете установить Сервер Отчетов на компьютер, который является Сервером управления, или вы можете установить Сервер Отчетов на другой компьютер.

Вы также можете создать резервные Серверы Отчетов. Если вы устанавливаете Сервер Отчетов на компьютер с установленным межсетевым экраном (не Windows Firewall), то вам необходимо открыть соответствующие порты для корректной работы сервера. Пользователям Windows Firewall нет необходимости изменять конфигурацию своего межсетевого экрана

Установка Сервера Отчетов

Вы можете установить Сервер Отчетов на ваш управляющий компьютер или на любой другой компьютер.

Если вы выбрали для установки Сервера Отчетов другой компьютер необходимо выполнить:

1. Установите программное обеспечение WatchGuard System Manager.

2. Выберите для установки только компоненты **Report Server**.

Перед тем, как начать

Перед настройкой Сервера Отчетов вам необходимо запустить мастер WatchGuard Server Center Setup Wizard для установки WatchGuard Server Center.

Для Сервера Отчетов вы добавляете базу данных сервера Журнала и пароль администратора для мастера установок Setup Wizard.

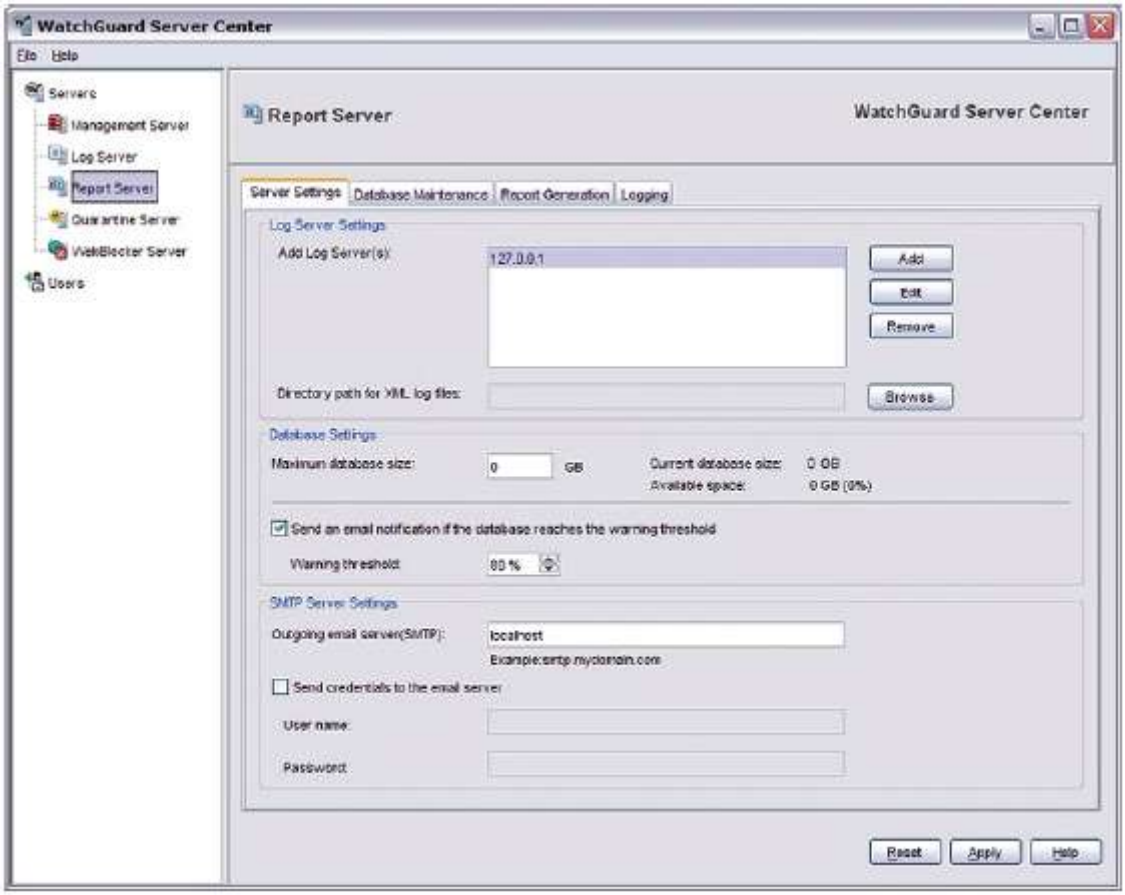
Настройка Сервера Отчетов

На компьютере, на котором установлен Сервер Отчетов, выполните следующее:

1. Нажмите правой кнопкой мыши на  в панели задач и выберите **Open WatchGuard Server Center**.
   Откроется диалоговое окно Connect to WatchGuard Server Center.

2. Введите ваше имя пользователя (**Username**) и пароль администратора (**Administrator passphrase**). Нажмите **Login**.
   Откроется диалоговое окно WatchGuard Server Center.

3. Выберите **Report Server** в меню **Servers**.
   Откроется страница Report Server



4. Измените параметры по умолчанию в соответствии с вашей сетью.

   * Для изменения параметров сервера по умолчанию нажмите на закладку **Server Settings**

   * Для изменения параметров резервного файла Журнала и Удаления, событий Уведомления нажмите **Database Maintenance**

   * Для изменения параметров для генерации отчета выберите закладку **Report Generation**.

   * Для изменения параметров ведения журнала выберите закладку **Logging**

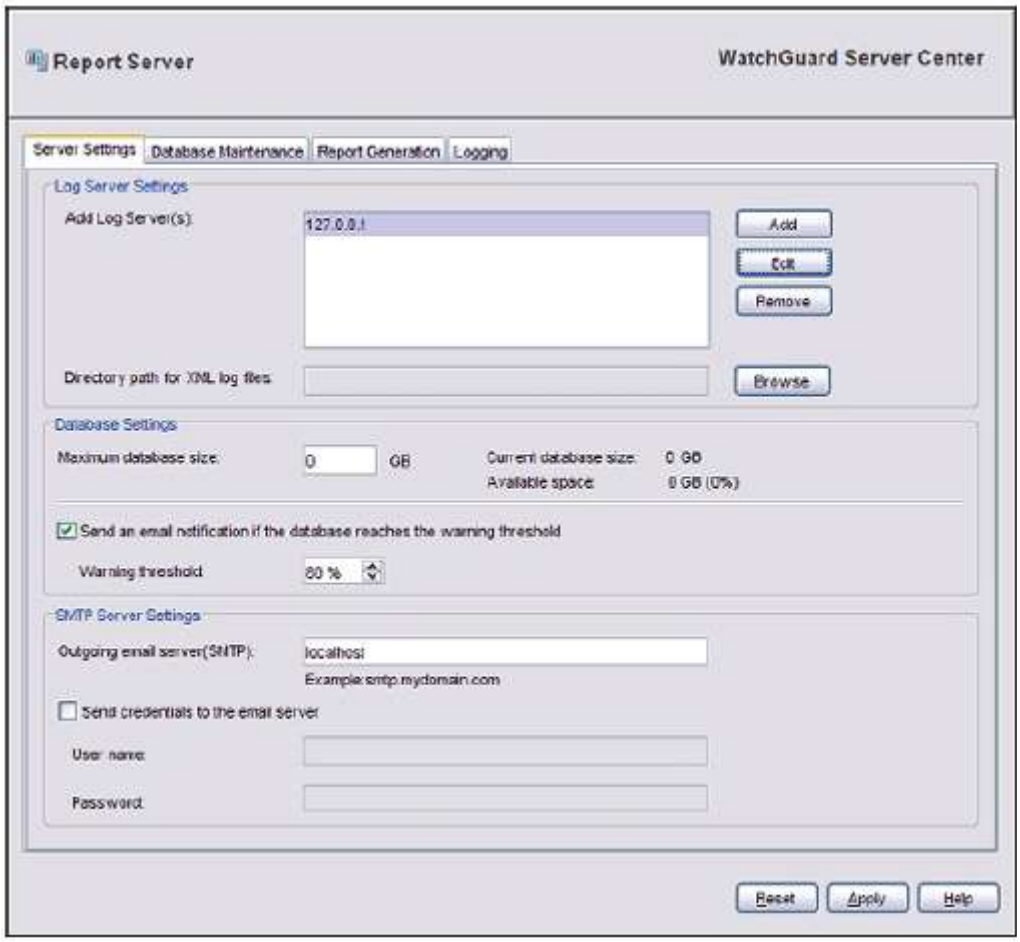
Настройка параметров Сервера

Сервер Отчетов получает данные от вашего Сервера Журналов и использует их для создания отчетов активности сети. В закладке **Server Settings** вы назначаете сервер Журнала, к которому может подключиться ваш Сервер Отчетов, и настраиваете параметры для базы данных Сервера Отчетов и SMTP-сервера.

В WatchGuard Server Center выполните следующее:

1. В меню **Servers** выберите **Report Server**.

2. Выберите закладку **Server Settings**.
   Откроется диалоговое окно Server Settings



3. Используйте следующий раздел для настройки параметров вашего Сервера Отчетов.

4. При завершении работы нажмите **Apply** для сохранения изменений.

Настройка параметров Сервера Журналов

Сервер Отчетов может собирать данные от нескольких Серверов Журналов, которые затем будут добавлены в отчет. Сервер Отчетов может так же хранить созданные вами файлы отчетов в формате XML.

1. Измените список **Add Log Server(s)**.

   * Для того чтобы добавить Сервер Журналов в список нажмите **Add**.

   * Для того чтобы изменить информацию о Сервере Журналов, выберите сервер из списка и нажмите **Edit**.

   * Для того чтобы удалить сервер из списка, выберите его и нажмите **Remove**.

2. Нажмите **Browse** для того чтобы выбрать каталог, в котором будут сохраняться файлы журнала **(Directory Path for XML log files)**

Настройка параметров базы данных

Вы можете выбрать максимальный размер вашей базы данных Сервера Отчетов.

Вы можете так же выбрать получение уведомлений при приближении размера базы данных к выбранному максимальному размеру. При достижении размера базы данных к выбранному максимальному размеру самые старые отчеты удаляются для освобождения места новым отчетам.

В разделе **Database Settings** выполните следующее:

1. В поле **Maximum database size** введите максимальный размер для базы данных Сервера Журнала. Вы можете установить размер от 1 до 10 000 Гб.
   Текущий размер базы данных и количество доступных Гб отображается рядом с этим полем.

2. Для получения сообщения о тревоге при приближении размера базы данных к максимальному включите опцию **Send an email notification if the database reaches the warning threshold**.

3. Для того чтобы настроить пороговую величину размера базы данных по достижении которого вы получите предупреждение, при помощи стрелок установите необходимое значение в поле **Warning threshold.**

Например, если вы установите лимит предупреждения для базы данных равным 90%, и максимальный размер базы данных равен 1000 Гб, то Сервер Отчетов сгенерирует предупреждение, когда размер базы данных будет равен 900 Гб

*Если база данных Сервера Отчетов регулярно очищается, и количество записей, отправляемых на сервер, остается практически неизменным, свободное пространство повторно используется для следующих отчетов.Однако, если интервал очистки (определенный в поле **Retain log messages for** в закладке Database Maintenance) уменьшается, или ведение журнала отладки отключено после периода времени, мы рекомендуем использовать утилиту командной строки vacuumdb для повторного использования дискового пространства*

Параметры SMTP-сервера

Вы можете задать адрес исходящего SMTP-сервера и настроить данные доступа к серверу, если он требует аутентификации

В разделе **SMTP Server Settings** необходимо выполнить:

1. В поле **Outgoing email server (SMTP)** введите адрес вашего SMTP-сервера.

2. Если ваш почтовый сервер запрашивает аутентификацию необходимо выполнить:

   * Включить опцию **Use login information for the email server**

   ***** В поле **User name** ввести имя пользователя для почтового сервера.

   * В поле **Password** ввести пароль для почтового сервера.

Если имя пользователя и пароль не требуются для вашего SMTP-сервера, вы можете оставить это поле пустым.

Настройка Сервера Журнала для Сервера Отчетов

Вы можете настроить несколько Серверов Журналов, данные с которых будут собираться Сервером Отчетов для последующего включения их в отчеты. Вы можете добавить, удалить Серверы Журналов, а также изменить пароли для Сервера Журналов

Добавление Сервера Журнала

На странице WatchGuard Server Center **Report Server** выполните следующее:

1. Выберите закладку **Server Settings**.

2. В разделе **Log Server Settings** нажмите **Add**.
   Откроется диалоговое окно Add Log Server.

3. Введите IP-адрес (**IP Address**) и пароль (**Password**) для Сервера Журналов

4. Нажмите **OK**.

Удаление Сервера журнала

На странице WatchGuard Server Center **Report Server** выполните следующее:

1. Выберите закладку **Server Settings**.

2. В окне **Log Server Settings** выберите Сервер Журналов, который вы хотите удалить

3. Нажмите **Remove**.
   Сервер Журнала будет удален из списка

Изменение пароля Сервера Журнала

Если вы изменяете пароль для вашего Сервера Журнала, вам также следует обновить пароль, используемый Сервером Отчетов для подключения к Серверу Журналов

На странице WatchGuard Server Center **Report Server** выполните следующее:

1. Выберите закладку **Server Settings**.

2. В окне **Log Server Settings** выберите Сервер Журналов

3. Нажмите **Edit**.
   Откроется диалоговое окно Edit Log Server

4. Введите новый пароль в поле **New Passphrase** для Сервера Журналов

5. Нажмите **OK**.
   Пароль Сервера Журнала будет обновлен

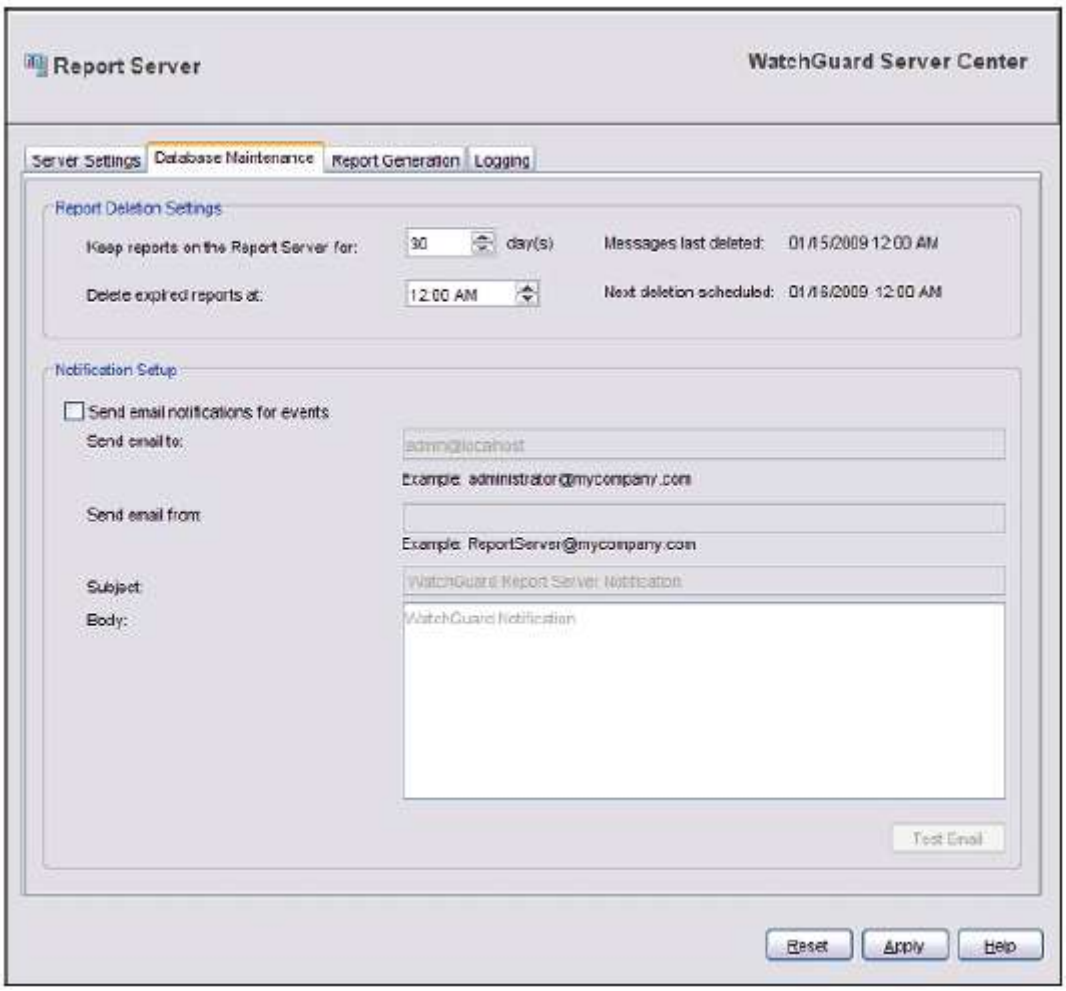
Настройка параметров Удаления отчетов и Уведомлений о событиях

Вы можете настроить параметры удаления отчетов и уведомлений для вашего Сервера Отчетов.

В WatchGuard Server Center выполните следующее:

1. В меню **Servers** выберите **Report Server**.

2. Нажмите на закладку **Database Maintenance**.
   Откроется диалоговое окно Database Maintenance



3. Используйте следующий раздел для настройки параметров вашего Сервера Отчетов .

4. При завершении работы нажмите **Apply** для сохранения ваших изменений.

Настройка параметров удаления отчета

Сервер Отчетов может автоматически удалять отчеты в указанное вами время. Вы можете выбрать срок хранения отчетов на сервере (от 1 до 356 дней). По умолчанию – отчет хранится 14 дней (2 недели).

В разделе Report Deletion Settings выполните следующее:

1. Нажмите на стрелки вверх/вниз **Retain Report messages for** для задания количества дней, в течение которых сообщение будет храниться на Сервере отчетов.
   Диалоговое окно отображает дату, когда сообщение было удалено в последний раз

   Для сохранения малого размера вашей базы данных выберите меньшее количество дней.

2. Нажмите стрелки вверх/вниз **Delete expired Report messages at** для установки времени дня, когда сообщение будет удалено.
   Диалоговое окно отображает дату и время следующего установленного удаления.

Настройка параметров для уведомления о событиях

Вы можете настроить Сервер Отчетов для отправки сообщения уведомления о событиях. Вы можете так же выбрать учетную запись электронной почты, от/к которой будут отправляться сообщения.

В разделе **Notification Setup** необходимо выполнить:

1. Для включения функции уведомления выберите опцию **Send email notifications for events**. Вам следует выбрать эту опцию для уведомления о случившихся событиях.

2. В поле **Send email to** введите полый адрес электронной почты, учетная запись вы хотите использовать для отправки уведомлений сообщений.

3. В поле **Send email from** введите полный адрес электронной почты, с которого будут отправляться сообщения уведомления.

4. В поле **Subject** введите темы, которая будет отображаться пользователям при получении уведомления о событии по электронной почте.

5. В поле **Body** введите сообщение, которые будет видеть пользователь при получении уведомления по электронной почте. Вы можете использовать простой текст или HTML в сообщении.

6. Если вы выберите включение уведомлений, вы можете нажать **Test Email** для проверки уведомления по email для указанного адреса. Сообщение откроется и сообщит о результатах доставки (УСПЕШНОЕ/неудачное).

Настройка параметров Генерации отчетов

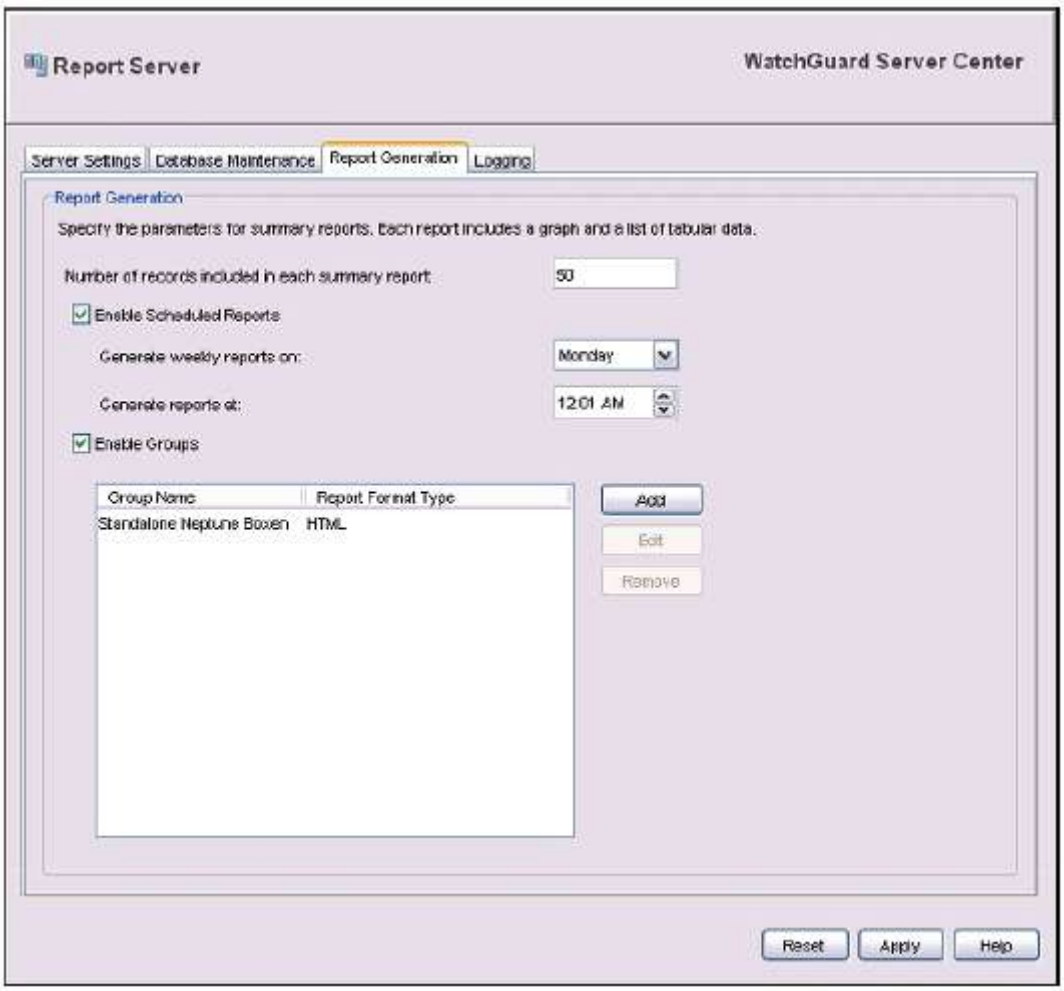
Вы можете настроить параметры Генерации отчета для вашего Сервера Отчетов. Это применяется только для кратких данных отчета. Отчеты генерируются в XML-файлы, которые вы можете просмотреть с помощью Report Manager. При создании группы устройств вы можете так же выбрать форматы для генерации отчетов: PDF или HTML.

В группе отчетов вы можете так же выбрать определенные типы отчетов для включения и каталог, куда будут сохранять сгенерированные отчеты.

В WatchGuard Server Center необходимо выполнить:

1. В меню **Servers** выберите **Report Server**.

2. Нажмите закладку **Report Generation**.
   Откроется диалоговое окно Report Generation



3. Используйте следующий раздел для настройки параметров вашего Сервера Отчетов.

4. При завершении нажмите **Apply** для сохранения изменений.

Определение параметров для генерации отчетов

Вы можете включить Сервера Отчетов для генерации еженедельных отчетов и выбора дня и времени.

1. В текстовом поле **Number of records included in summary report** введите количество записей, которые будут появляться в Итоговом отчете. Допустимый диапазон – 25-100 записей. Эти параметры применяются только для Итоговых отчетов.

2. Выберите опцию **Enable Scheduled Reports**. Эта опция выбрана по умолчанию. Если опция не выбрана, Сервера Отчетов не генерирует отчеты автоматически.

3. В выпадающем списке **Generate weekly reports on** выберите день, в течение которого отчет сгенерируется.

4. При помощи стрелок вверх/вниз выберите время дня начала отчета (поле **Generate reports at)**.

5. Для сохранения групп устройств Firebox для включения в отчетах выберите опцию **Enable Groups**.

   * для создания группы нажмите **Add**.

   * для изменения текущей группы выберите групп из списка и нажмите **Edit**.

* для удаления группы из списка выберите и нажмите **Remove**.

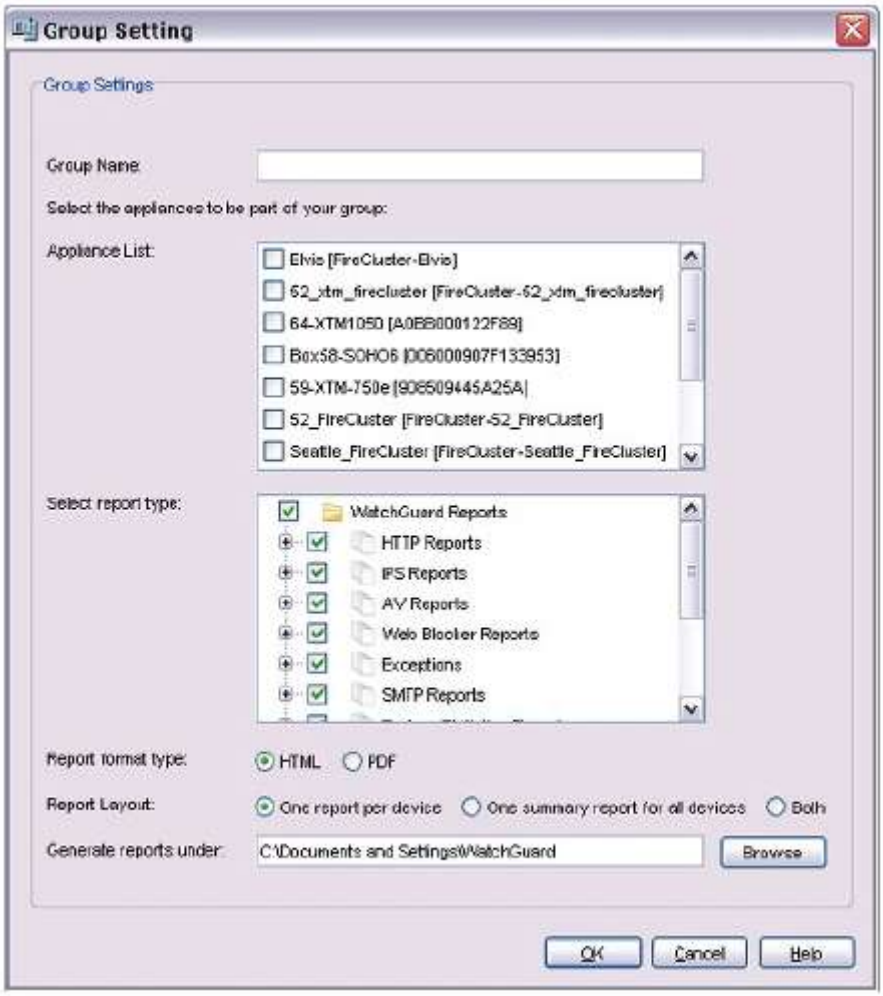
Более подробную информацию о добавлении или изменении групп см. в следующем разделе.

Создание групп и отчетов по расписанию

Вы можете создать группы устройств Firebox для включения в отчеты генерации Сервера Отчетов и расписание отчетов, которые будут отображаться в списке **Archived Reports**.

Для создания групп и отчетов по расписанию необходимо выполнить:

1. В закладке Сервера Отчетов **Report Generation** выберите опцию **Enable Groups**.
2. Нажмите **Add**.
   Откроется диалоговое окно Group Setting



3. В поле **Group Name** введите соответствующее имя для определения группы.
4. В **Appliance List**, выберите устройства для включения в группы.
5. В окне **Select report type** выберите опцию рядом с каждым отчетом, который будет отображаться при генерации отчета.
6. Выберите **Report format type** для формата выводимого отчета. Вы можете выбрать для просмотра отчетов в **HTML** или **PDF** -формате.

7. Выберите **Report Layout**. Вы можете выбрать для просмотра One report per device, One summary report for all devices, или Both.

8. В поле **Generate reports under** введите путь к каталогу , где будут храниться сгенерированные отчеты. Или нажмите **Browse** для выбора каталога.

9. Нажмите **OK**.

Для изменения параметров текущей группы необходимо выполнить:

1. В окне **Enable Groups** выберите группу для изменения.

2. Нажмите **Edit**.
Откроется диалоговое окно Group Setting.

3. Сделайте необходимые изменения параметров для группы.

4. Нажмите **OK**.

Настройка параметров ведения журнала для Сервера Отчетов

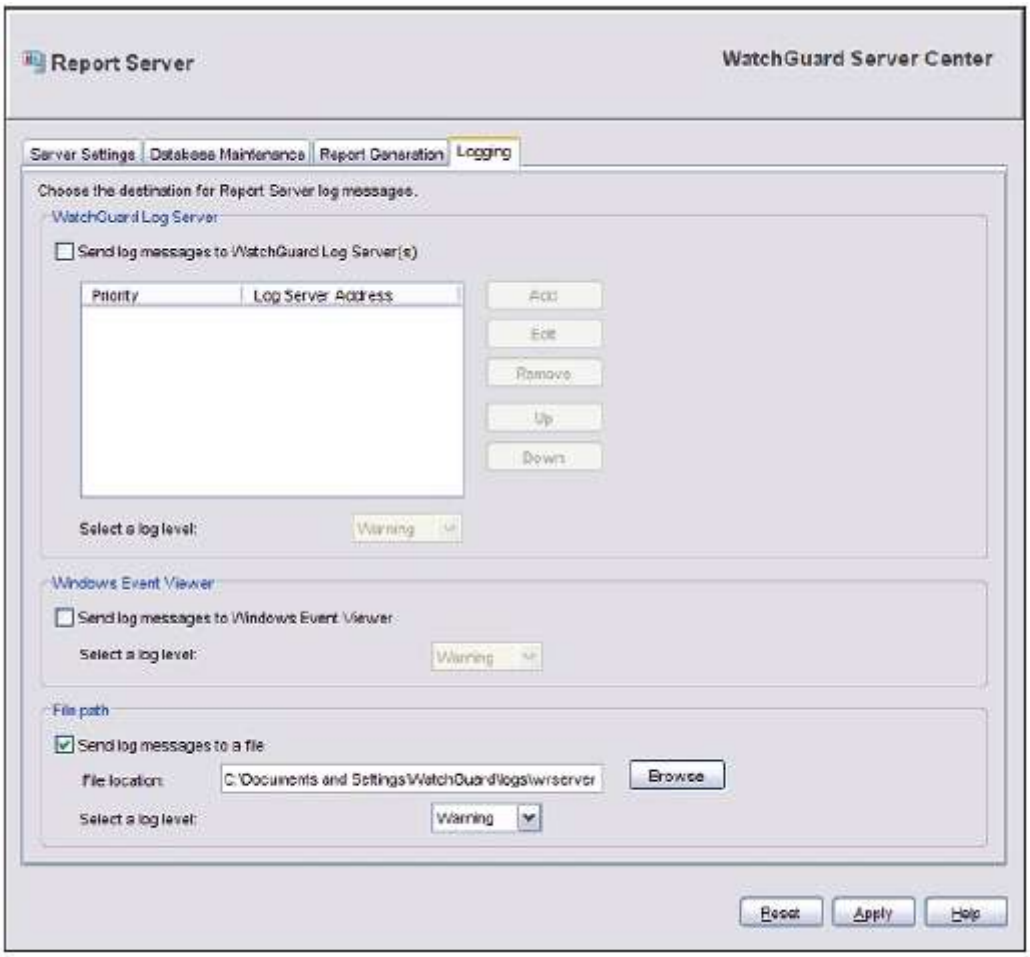
На странице Сервер Отчетов **Logging** вы можете настроить место, куда Сервер Отчетов будет отправлять данные сообщения.

Вы можете выбрать для отправки сообщений журнала одну или более опций: WatchGuard Сервер Журнала, Windows Event Viewer или файл журнала.

В WatchGuard Server Center необходимо выполнить:

1. В меню **Servers** выберите **Report Server**.

2. Нажмите на закладку **Logging**.
   Откроется диалоговое окно Logging



3. Настройте параметры для вашего Сервера Отчетов. Более подробную информацию о настройке параметров Logging см. в Configure Logging Settings for your WatchGuard servers.

4. При завершении нажмите **Apply** для сохранения ваших изменений.

Перемещение каталога отчета

Вы можете использовать WatchGuard Server Center Setup Wizard для выбора каталога, где храниться файлы данных каталога.

Сервер Отчетов хранит все файлы данных в этом каталоге. После завершения работы мастера установок вы не сможете изменять каталог данных в приложении WatchGuard Server Center. Сервер Отчетов хранит XML-файлы отчетов в различных местах, которые могут быть изменены в WatchGuard Server Center.

Для изменения расположения хранения отчетов Сервера Отчетов вам следует установить Сервер Отчетов повторно. Для этого вы можете изменить файл *wrserver.ini* и запустить повторно WatchGuard Server Center Setup Wizard. При повторном запуске мастера вы задаете новое расположение каталога, но данные при этом не переносятся в новый каталог. Вы можете вручную переместить данные из старого каталога в новый перед использованием мастера установок для задания нового каталога Сервера Отчетов.

При запуске мастера установок WatchGuard Server Center Setup Wizard для реконфигурирования вашего Сервера Отчетов страница, отображаемая в мастере, может отличаться от страниц, описанных в следующих разделах.

Дальнейшее описание применимо, если у вас установлены только Сервер Отчетов, Сервер Управления и Сервер Журнала.

Если у вас установлены другие сервера WatchGuard, то в мастере могут появиться дополнительные страницы

Из-за совместного использования Сервером Журнала и Сервером Отчета базы данных PostgreSQL, то в случае, когда эти серверы установлены на один и тот же компьютер, то при перемещении базы данных это произойдет для обоих серверов.

Шаг 1 — Остановка сервисов

1. Откройте WatchGuard Server Center.

2. Остановите и запустите ваши серверы WatchGuard.

3. Закройте WatchGuard Server Center.

4. Остановите сервисы PostgreSQL-8.2.

   * В Windows Control Panel выберите **Administrative Tools > Services**.
   Откроется диалоговое окно Services.

   * Выберите **PostgreSQL-8.2** и нажмите **Stop**.
   Сервисы остановятся.

Шаг 2 — Перемещение данных отчета

1. Создайте новый каталог для файлов отчета.
   Например, *E:\WatchGuard\report_directory\reports*.

2. Перейдите в каталог, в котором сейчас хранятся отчеты, и скопируйте весь каталог. Убедитесь, что вы скопировали все файлы и каталоги. Например, перейдите в каталог *C:\Documents and Settings\WatchGuard\reports*.

   Скопируйте подкаталог *\data* и все его файлы

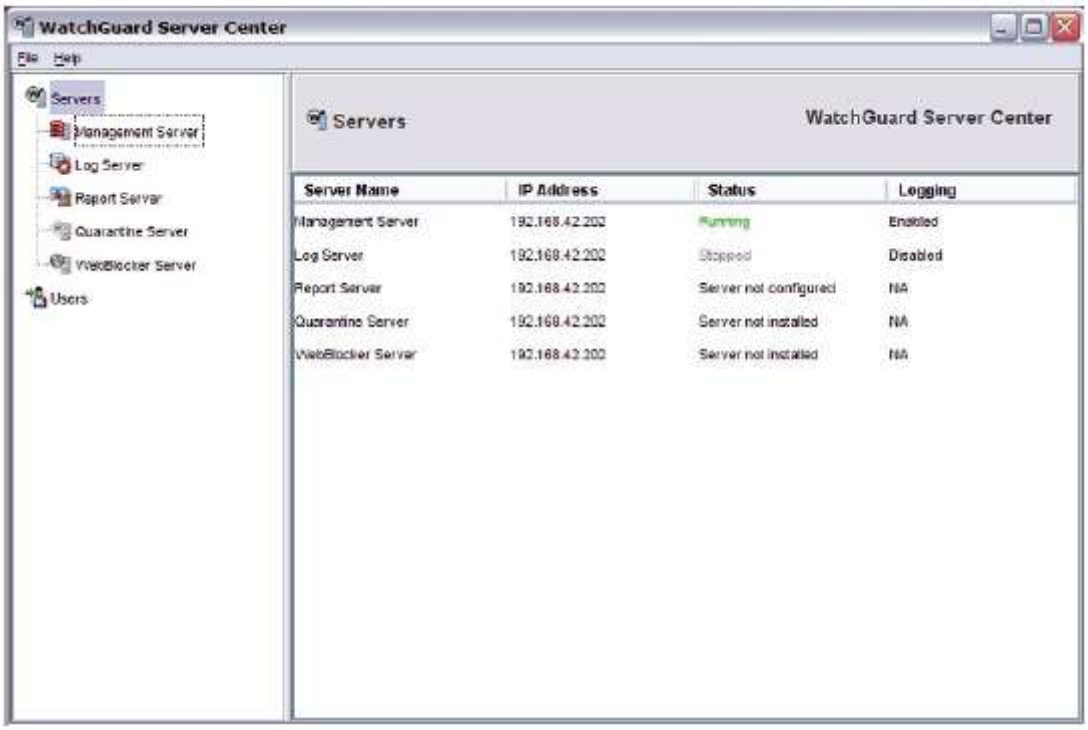
3. Вставьте скопированный каталог отчетов в новый каталог.
   Например, в каталог *E:\WatchGuard\report_directory\reports*. Убедитесь, что вы вставили все записи отчета в каталог. Для данного примера это будет папка `\data`.

Шаг 3 — запуск Setup Wizard

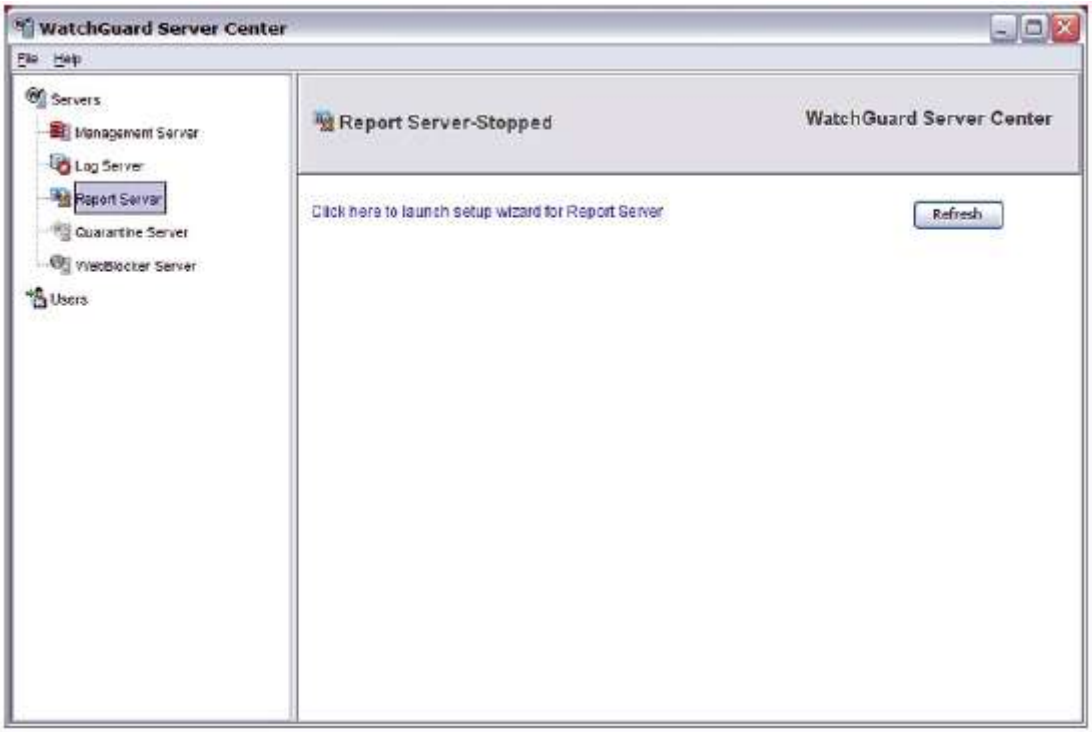
1. Откройте папку *C:\Documents and Settings\WatchGuard\wrserver\wrserver.ini* и измените величину WizardSuccess на “0”.

2. Удалите файл: *\Program Files\WatchGuard\wsm11.0\postgresql\install\pg_install.ini.*

3. Откройте WatchGuard Server Center. Состояние (**Status)** для Сервера Отчетов - **Server not configured**.



4. В меню **Servers** выберите **Report Server**.
   Откроется диалоговое окно Report Server



5. Для запуска WatchGuard Server Center Setup Wizard для Сервера Отчетов нажмите **Click here to launch setup wizard for Report Server**.
   Откроется сообщение о запуске WatchGuard Server Center Setup Wizard.

6. Нажмите **OK** для запуска мастера.
   Откроется диалоговое окно WatchGuard Server Center Wizard.

7. Нажмите **Next**.
   Откроется диалоговое окно Review Settings.

8. Просмотрите **Report Server Settings**.

9. Нажмите **Next**.

10. Завершите работу мастера WatchGuard Server Center Wizard.
Мастер установит программу PostgreSQL и настроит Сервер Отчетов.

Завершающие шаги

1. На странице **Report Server** нажмите **Refresh**. Сервер Отчетов запустится, и откроется страница его конфигурации.

2. Перезапустите Сервер Журнала.

Запуск и остановка Сервера Отчетов

Вы можете запускать или останавливать сервисы Сервера Отчетов в любое время, при этом сохраняя подключении с вашим Сервером Отчетов.

Для запуска сервисов в WatchGuard Server Center необходимо выполнить:

1. Выберите **Report Server** в меню **Servers**.

2. Нажмите правой кнопкой мыши на **Report Server** и выберите **Start Server**. Сервисы остановятся, и Сервер Отчетов появится в верхней части страницы Сервера Отчетов .

Для остановки сервисов в WatchGuard Server Center необходимо выполнить:

1. Выберите **Report Server** в меню **Servers**.

2. Нажмите правой кнопкой мыши на **Report Server** и выберите **Stop Server**.
Откроется предупреждающее сообщение.

3. Нажмите **Yes** для подтверждения намерения об остановки Сервера Отчетов.
Сервисы остановятся, и откроется Report Server-Stopped в верхней части страницы Сервера Отчетов.

Утилита Report Manager

При помощи утилиты Report Manager вы можете посмотреть данные, собранные с ваших Серверов Журналов. При помощи Report Manager вы можете посмотреть все доступные отчеты для Firebox, FireCluster , серверовWatchGuard или нескольких устройств.

Отчеты WatchGuard Reports – это итоговые данные по сообщениям журнала. Report Manager объединяет данные журнала в отчеты различного типа. В закладке **Archived Reports** Report Manager вы можете просмотреть отчеты, которые запланированы для запуска Сервером Отчетов.

Вы так же можете выбрать для запуска отчетов в реальном времени в закладке **On-demand Reports.** Firebox. При помощи дополнительных компонентов утилиты Report Manager вы можете:

- Настроить опции отчета, например цвет фона, максимальное количество записей в файле и каталог, в котором вы будете хранить отчеты.

- Выбрать параметры отчета, например диапазоны дат для отчетов и групп Firebox для которых вы хотите создать отчеты.

- Изменить типа отчета с HTML на PDF и обратно
- Отправить отчет по электронной почте, распечатать и сохранить отчет

Для того чтобы использовать отчеты WatchGuard, у вас должен быть установлен Internet Explorer 6.0 или выше или Firefox.При испольовании другого браузера, установленного у вас по умолчанию, отчет не отобразится в окне Report Manager. Для просмотра отчетов другими браузерами вам следует вручную выбрать отчет в окне браузера. Более подробную информацию см. в "Select the Report format" on page 694.

Открытие Report Manager

Откройте Report Manager на главном интерфейсе WatchGuard System Manager (WSM) .

1. На панели инструментов WSM нажмите . Или выберите **Tools** > **Logs** > **Report Manager**.
   Откроются диалоговые окна WatchGuard Report Manager и Connect to Report Server.

2. Введите IP-адрес для вашего Сервера Отчетов и имя пользователя и пароль администратора. Пароль администратора задается при завершении работы WatchGuard Server Center Setup Wizard.

3. Нажмите **Login**.
   Report Manager подключится в Серверу Отчетов и данные появятся в окне навигации WatchGuard Reports.

При первом подключении к Серверу Отчетов появится диалоговое окно **Accept Certificate.** Вам следует принять сертификат для продолжения действий.

Подключение к различным Серверам Отчета

Для подключения к различным Серверам Отчета с помощью Report Manager, прежде всего, следует отключиться от текущего Сервера Отчетов.

1. Выберите **File** > **Disconnect**.

2. Нажмите на в панели инструментов Report Manager для подключения к различным Серверам Отчетов.

Настройка опций отчета

Вы можете изменить настройки вывода отчета по умолчанию, а также изменить шаблон отчета по умолчанию.

1. Нажмите на в панели инструментов Report Manager. Или выберите **View** > **Options**.
   Откроется диалоговое окно Options в выбранной закладкой General.

2. Используйте последующие разделы для настройки параметров.

3. При завершении нажмите **OK** для сохранения изменений.

Настройка параметров для графиков и диалоговых окон

Вы можете установить темный/светлый фон для графиков и диалоговых окон. Темный фон установлен по умолчанию. Для применения светлого фона в графиках и диалоговых окнах необходимо выполнить:

1. Выберите закладку **General**.

2. Отключите опцию **Use dark background for charts and dialogs**.

Настройка параметров для Report Output

1. Выберите закладку **General**.

2. Для задания каталога для файлов (**Specify the directory for the report files**) нажмите **Browse** и выберите папку для сохранения файла отчетов Report Manager на вашем локальном жестком диске.

3. Для задания вида по умолчанию для вывода отчета выберите **Report file type**:

   * HTML

   * PDF

   При использовании Report Manager отчет автоматически отображается в выбранном формате.

4. Для установки максимального количества записей, включенных в каждый HTML-файл, нажмите стрелками вверх/вниз на **Maximum records per HTML file**.

5. Чтобы настроить Report Manager для создание новых версий выбранных отчетов выберите опцию **Always recreate the report file when I open it**.

   Генерация больших отчетов занимает значительно времени. Эта опция может занять больше времени, но она содержит самый последние данные.

   Отключите эту опцию, чтобы включить Report Manager для открытия существующей версии выбранных отчетов. Эта опция уменьшает количество времени, занимаемое для просмотра отчета. Информация, включенная в предыдущих отчетах, может не содержать последние данные.

6. Для удаления всех созданных вами отчетов выберите опцию **Always delete report files I created when Report Manager closes**. Чтобы оставить файлы отчета в каталоге отключите эту опцию.

7. Для настройки уведомления об удалении файлов для Report Manager выберите опцию **Ask me before deleting report files**. Если вы хотите удалять файлы без уведомления, отключите эту опцию.

Выбор каталог для шаблонов отчетов (Report Template)

Чтобы задать каталог для определенных файлов отчета необходимо выполнить:

1. Выберите закладку **General**.

2. В разделе **Report Template** нажмите **Browse** и выберите каталог для сохранения файлов отчета.

Добавление дополнительной информации в ваш отчет

Вы можете использовать Report Options для добавления в отчет логотипа вашей компании, сайта с перенаправлением на него при нажатии на логотип и определенного количества отчетов, включенных в итоговую таблицу Report.

1. Выберите закладку **Report**

2. Для добавления логотипа вашей компании в верхнюю часть вашего отчета в текстовом поле **Specify the company logo used in report header with a full path name** введите полный путь к файлу изображения или нажмите **Browse** для выбора файла.

3. Для добавления сайта с перенаправлением на него при нажатии на логотип компании в отчете в поле **Specify the web address when a user clicks on the company logo** и введите полный адрес сайта.

4. Для добавления ссылки с адресом сайта в отчет выберите опцию **Add link and automatically generate linked files**.

5. Чтобы установить, когда Report Server будет перемещать записи из итоговой таблицы отчетов нажмите на поле с помощью стрелок вверх/вниз **The maximum entries in the report summary table**.

Список предопределенных отчетов

Report Manager содержит предопределенные отчеты, которые вы можете использовать для отображения данных, собранных Firebox.

Тип отчета	Название отчета	Описание
Web Traffic Summary	Web activity trend	Направления, активные иенты, наиболее популярные ы, информация по WebBlocker и eb-сайты, заблокированные правилами прокси Графики включены для более обных отчетов. Для того чтобы отреть более подробный отчет

		нажмите на график.
	Web trend summary	Данные по направлениям в час
	Most active clients	Top 50 клиентов по количеству подключений
	Most popular domains	Top 50 сайтов, посещенных клиентами
	WebBlocker service	Статистика и сайты, аблокированные сервисом WebBlocker
	URL details by time	Все URL в хронологическом порядке
	URL details by client	Все URL по клиентам
	URL details by domain	Все URL по доменам
	Web activity audit	Если вы включите флаг аудита HTTP в Policy Manager, то этот будет содержать разрешенные подключения
Intrusion Prevention Summary	Intrusion Prevention Summary	Все действия IPS
	Detail by protocol	Данные по IPS, сортированные по протоколу
	Detail by severity	Данные по IPS, тсортированные по уровню серьезности проблемы
	Detail by source IP	Данные по IPS, сортированные по IP-адресу источника
	Detail by signature	Данные по IPS, ортированные по сигнатурам
AntiVirus Summary	AntiVirus summary	Отчет по действиям AntiVirus
	Detail by protocol	Параметры действий AntiVirus по протоколам

	Detail by host (HTTP)	Параметры действий AntiVirus по хостам
	Detail by virus	Параметры действий AntiVirus по вирусам
	Detail by email sender	Параметры действий AntiVirus правителям. Доступна для SMTP or POP3
spamBlocker Summary	spamBlocker summary	Статистика по типу спама, гвиям и топ источников спама и получателей
	spamBlocker by sender	Статистика по отправителям
Proxy Reports	Host summary	Статистика проксируемого трафика по хостам
	Proxy Summary	Статистика проксируемого трафика по прокси
	Time Summary / Daily Trend	Статистика проксируемого трафика по времени
	Session Summary	Статистика проксируемого трафика по сессиям
SMTP Proxy Summary	SMTP server summary	Отчет по активности сервера ГР(для внутренних и внешних почтовых учетных записей)
	SMTP email summary	Отчет по активности SMTP ты (для внутренних и внешних адресов)
	SMTP proxy detail	Записи действий SMTP прокси по времени
	Email account summary	Внешние и внутренние учетные записи электронной почты
	Email server summary	Внутренние и внешние серверы электронной почты
POP3 Proxy	Email account summary	Внутренние и внешние

		почтовые учетные записи
	Email server summary	Внутренние и внешние серверы
	POP3 detail	Все записи по времени
Packet-Filtered Reports	Host summary	Отчет по данным пакетного фильтра
	Service Summary	Отчет по данным пакетного фильтра по сервисам
	Time Summary / Daily Trend	Отчет по данным пакетного фильтра по времени
	Session Summary	Отчет по данным пакетного фильтра по сессиям
Firebox Statistics	Firebox statistics	Статистика по пропускной обности для всех интерфейсов Firebox.
	Denied User Authentication	Подробный список ошибок нтификации. Список содержит емя, дату и причину ошибки
	User Authentication Report	Подробный список тифицированных пользователей, чая время подключения, время чения и информации о способе подключения
	External interface bandwidth	Статистика по пропускной собности интерфейса External. Период извлечения данных еделяется временем отчета. нимальный интервал равен 1 нуте. Опубликованный отчет вляет данные каждые 10 минут
	VPN tunnel bandwidth	Отчет по трафику VPN туннеля
	Audit Trail	Список изменений в конфигурации

Exceptions	Denied packet summary	Отчет по журналам для всех заблокированных пакетов
	Denied incoming packets detail	Подробный журнал для аждого входящего действия
	Denied outgoing packet detail	Подробный журнал для ждого исходящего действия
	Alarms	Все тревоги
Management Server Audit	Server audit summary	Отчет по аудиту сервера
	Server audit detail	Вся информация по аудиту сервера
	Server Authentication Report	Все неудачные попытки аутентификации
Management Reports	Boxes Under Management Report	Отчет для всех устройств box, подключенных к Серверу Управления

Выбор параметров отчетов

После того, как вы подключитесь к Серверу Отчетов, вы можете при помощи утилиты Report Manager посмотреть данные журнала. Для того чтобы посмотреть отчеты, вам необходимо выбрать устройства Firebox и диапазон даты, которые будут включены в отчет. В отчет вы можете включить один или несколько Firebox.

Для просмотра отчетов вам следует выбрать устройства и диапазон времени/даты для включения в отчет и выбрать **архивный отчет** или создать отчет по запросу (**on-demand report).**

Архивные отчеты – это отчеты, которые создаются по расписанию вашим Сервером Отчетов. Вы можете выбрать данные, которые будут включены в отчет

Отчет по запросу - это отчеты, которые создаются по запросу WatchGuard

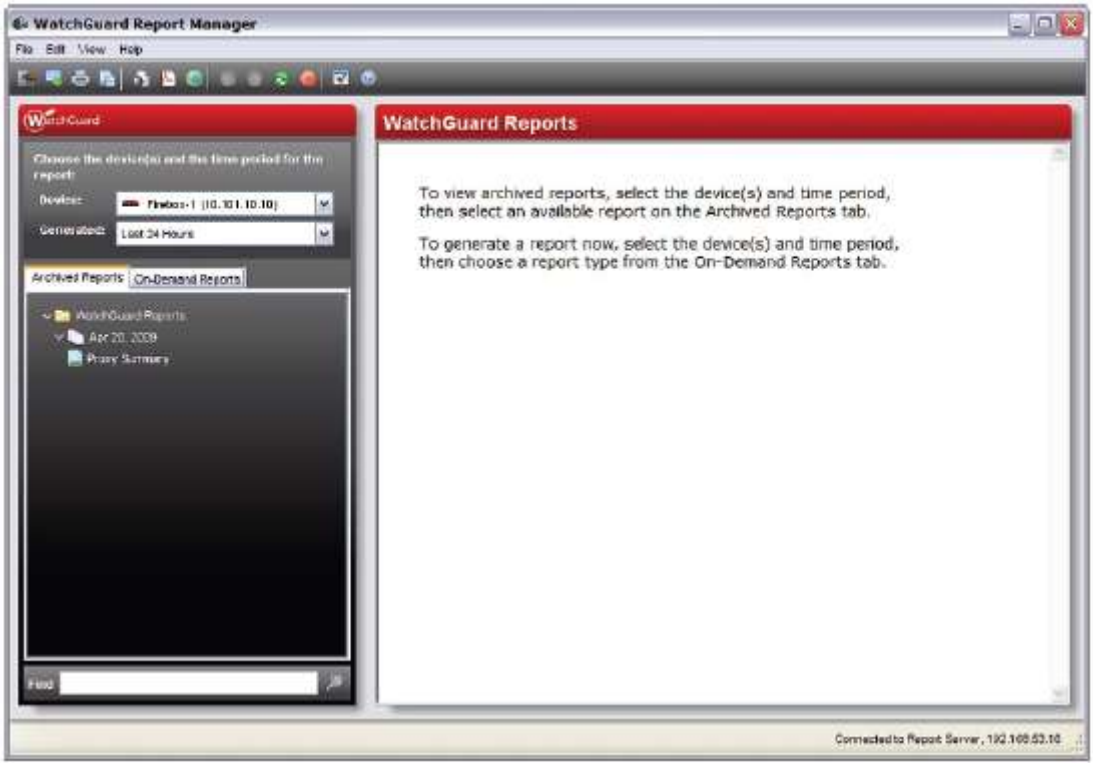
В зависимости от выбранной закладки, **Archived Reports** или **On-Demand Reports,** метка поля периода времени/даты изменяется. Если вы выбрали **Archived Reports,** метка **Generated** информирует, что в течение выбранного периода времени создался архивный отчет на Сервере Отчетов. Если вы выбрали **On-Demand Reports,** метка **Generate** свидетельствует о периоде времени, для которого сообщения журнала включаются в ваш отчет.

Выбор устройства, периода времени и списка отчетов

Вы можете просмотреть детальную информацию для Firebox, сервера или FireCluster в вашем отчете. Вы можете так же получить отчеты только для одного устройства FireCluster.

Для просмотра отчеты вам нужно выбрать устройство, период времени и тип отчета- архивный или по запросу.

1. Откройте Report Manager и подключитесь к Серверу Отчетов.
   Откроется диалоговое окно Report Manager



2. В выпадающем списке **Device** выберите устройство, сервера или FireCluster для создания отчета.

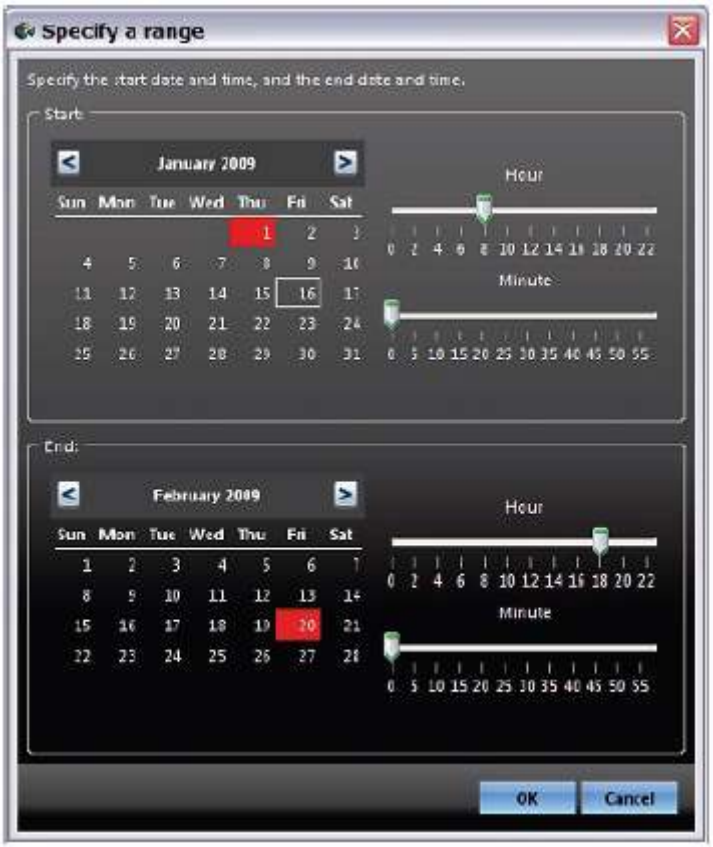
3. В выпадающем списке **Generate** или **Generated** выберите период времени для отчета. Для выбора отображения отчетов на определенный период времен и даты перейдите к разделу *Specify a date range.*

4. Для выбора списка отчета нажмите закладку **Archived Reports** или **On-Demand Reports**.
   Доступные отчеты появятся в выбранном списке отчетов.

Выбор диапазона дат

Вы можете выводить ваши отчеты для определенной даты или времени в одном списке отчетов.

1. Нажмите на выпадающий список **Generate** или **Generated** и выберите **Specify a range**.
   Или выберите **Edit** > **Specify a range**.
   Откроется диалоговое окно Specify a range



2. В разделе **Start** выберите дату и время запуска.

3. В разделе **End** выберите дату и время окончания.

4. Нажмите **OK**.
   Диапазон появится в выпадающем списке Generate или Generated.

Некоторые диапазоны дат не могут быть сохранены от сеанса к сеансу. При закрытии Сервера Управления все выбранные вами диапазоны исчезнут.

Редактирование диапазона дат

Вы можете изменить параметры выбранного диапазона времени и дат.

1. Выберите диапазон дат для изменения в выпадающих списках **Generate или Generated .**

2. Нажмите  .
   Откроется диалоговое окно Specify a range.

3. Измените дату и время начала и окончания.

4. Нажмите **OK**.
   Обновленный диапазон появится в выпадающем списке Generate или Generated.

Выбор отчетов для генерации

После подключения в Серверу Отчетов, выбора устройства(в) и периода времени для вашего отчета вы можете выбрать типы отчетов для их включения в Отчеты WatchGuard.

Отчеты, которые отображаются в списке **Reports available on the server list,** заполняются на основе параметров журнала и ваших серверов, событий, произошедших на вашем устройстве.

Выбранный вами тип отчета для данных журнала и тип события отобразится в списке.Если вы не можете просмотреть особые отчеты в списке, вы можете изменить вашу конфигурацию при сборе данных журнала для этих отчетов

Создание отчетов

В Report Manager выполните следующее:

1. Выберите **Edit** > **Create reports**.
   Откроется диалоговое окно Create Report

2. Для изменения каталога хранения файлов отчета нажмите **Browse**.

3. Выберите **HTML** или **PDF** в качестве типа файла отчета **Report file type**.
   Report Manager автоматически отобразит отчеты в выбранном формате.

4. Выберите опции и списке для каждого создаваемого отчета. Для того чтобы выбрать все отчеты включите опцию **Reports available on the server**.

5. Если вы хотите чтобы диалоговое окно **Create Report** не закрывалось после того, как все отчеты будут сгенерированы, отключите опцию **Automatically close this dialog box after all reports generate successfully.**

6. Нажмите **Start**.
   Report Manager сгенерирует выбранные отчеты.

Отображение отчета

После того как вы настроили параметры отчета и выбрали отчеты для генерации, вы можете их показать. Отчеты сгруппированы по дате и по типу для всех выбранных устройств.

Для того чтобы посмотреть отчет в Report Manager выполните следующее:

1. Откройте Report Manager и подключитесь к вашему Серверу Отчетов.

2. Выберите параметры отчета для устройства и периода времени/даты.

3. Выберите закладку **Archived Reports** или **On-Demand Reports**.

4. Нажмите на имя отчета в списке **WatchGuard Reports**.
   Откроется диалоговое окно Progress, затем выбранный отчет появится справа.Если вы выбрали для просмотра отчета браузер по умолчанию, то отчет откроется в окне браузера.

   Некоторые отчеты включают ссылки на данные устройства. Вы можете выбрать отчет с ссылками на данные устройства, нажав для ссылку для просмотра этих данных. Откроется диалоговое окно с данными устройства.

5. Для остановки процесса генерации отчета нажмите  .

6. Для обновления выбранного отчета нажмите  .
   Или выберите **Edit** > **Update report list**.

Поиск отчета в списке

Вы можете использовать поле **Find** Report Manager для поиска определенного отчета в списке.

1. Выберите раздел в отчете для включения его в поиск. Например, для поиска всех отображаемых отчетов нажмите WatchGuard Reports вверху списка.

2. В поле **Find** внизу Report Manager введите фразу для поиска

3. Нажмите  . Или нажмите **Enter** на вашей клавиатуре. Если фраза будет найдена в списке отчетов, то первый отчет, в котором была найдена указанная строка, появится на экране и будет подсчечен

4. Нажмите снова на  для нахождения отчетов в списке. Если фраза не содержится в отображаемом отчете, ниже поле Find появится сообщение “Phrase not found”.

Поиск информации в отчете

Вы можете использовать диалоговое окно для поиска информации в отчете.

1. В списке **WatchGuard Reports** выберите отчет.
   Откроется диалоговое окно с данными отчета.

2. Нажмите **Ctrl + F** на вашей клавиатуре.
   Откроется диалоговое окно Find.

3. В поле **Find** введите фразу для поиска.

4. Выберите опцию для дополнительных параметров поиска. Опции включают **Case sensitive**, **Wrap Search**, и **Backward**.

5. Нажмите **Find**.

Просмотр отчетов об использовании клиентом Web-ресурсов

Отчеты клиента составляют один из многих типов отчетов, доступных на вашем Сервере Отчетов, в качестве отчетов по запросу. Они могут содержать информацию от прокси -сообщений об аутентификации пользователя, имени хоста или IP-адресе для выбранного устройства или группы.

Существует 2 типа отчетов клиента: *Top Client* и *Per Client*.

Запуск отчета Top Client

Сообщения журнала для отчетов Top Client включают только информацию об IP-адресе. Из-за того, что сообщения журнала не содержат параметры имени хоста и имени пользователя, отчеты Top Client разделяются на 3 типа:

- Top Client по IP-адресу
- Top Client по имени хоста
- Top Client по аутентификации пользователя

Для просмотра отчета Top Client в Report Manager необходимо выполнить:

1. Подключитесь к вашему Серверу Отчетов.
2. В выпадающем списке **Device** выберите устройства, сервер или FireCluster.
3. В выпадающем списке **Generate** выберите диапазон даты для отчетов.
4. Выберите закладку **On-Demand Reports**.
5. В списке **WatchGuard Reports** выберите **Top Client Report by** [тип отчета].
   Откроется диалоговое окно выбранного отчета.

Запуск отчета Per Client

Отчет Per Client содержит подробное резюме деятельности для определенных клиентов на устройствах и для диапазонов времени. Вы можете выбрать один или более параметров для включения в этот отчет.

Опции включают:

- имя пользователя и ID
- IP-адрес
- имя пользователя

Вы можете так же выбрать домен для выбранных параметров.

Для просмотра отчета Per Client в Report Manager необходимо выполнить:

1. Подключитесь к вашему Серверу Отчетов.
2. В выпадающем списке **Device** выберите устройство, сервер или FireCluster.
3. В выпадающем списке **Generate** выберите диапазон дат для отчета.
4. Выберите закладку **On-Demand Reports**.
5. В списке **WatchGuard Reports** выберите **Per Client Web Activity Report**.
   Откроется диалоговое окно Per Client Report Configuration

6. Введите **User Name**, **IP Address**, и/или **Host Name,** которые вы хотите включить в отчет.

7. В выпадающем списке **Domain** выберите сервер аутентификации для домена.

8. Нажмите **OK**.
   Отчет появится с определенной информацией.

После выбора параметров для отчета Per Client вы можете нажать на выпадающий список и выбрать параметры другого отчета. При закрытии Report Manager история параметров автоматически удаляется. Вы можете так же вручную удалить историю.

В диалоговом окне **Per Client Report Configuration** необходимо выполнить:

1. Нажмите на выпадающий список для удаления истории параметров.

2. Выберите **Clear history**.
   История для выбранных параметров удалится.

Фильтрация данных отчета

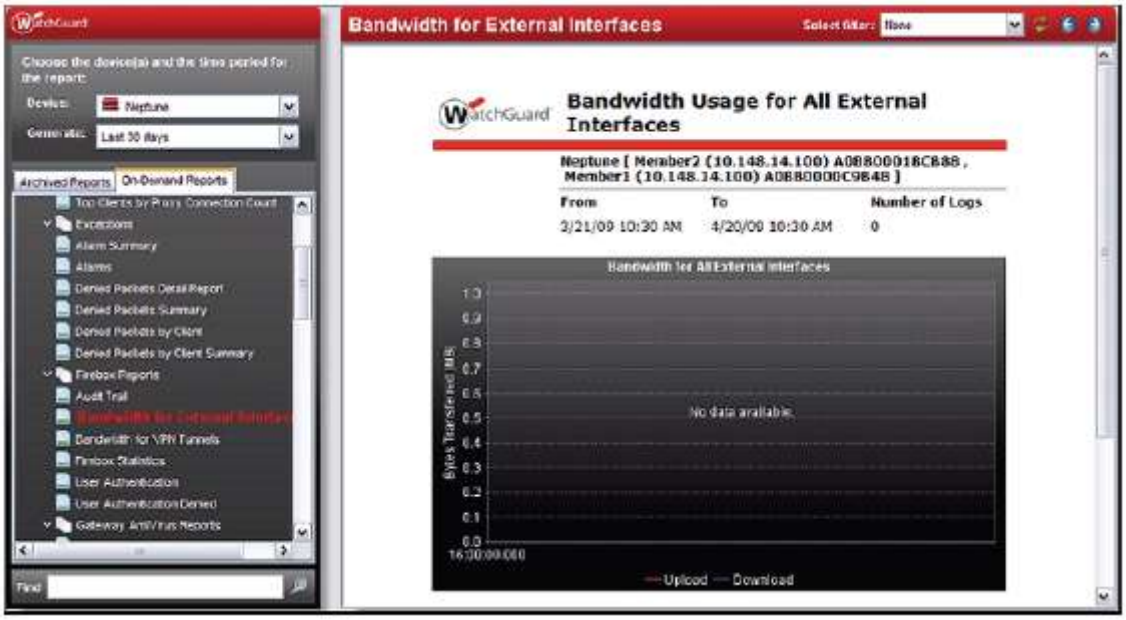
Вы можете создать файлы для очистки информации, включенной в отчет. Данные категории, заданные для каждого фильтра, можно объединить для обеспечения гибкости выводимых данных в отчете. При закрытии Report Manager ваши фильтры сохраняются, так что вы можете применить их для последующих отчетов. Вы можете так же изменять величины, указанные в ваших фильтрах, для того чтобы выводить только необходимые данные. Фильтры не доступны для всех отчетов.

Вы можете фильтровать данные отчета при его просмотре в Report Manager. Если вы просматриваете ваши отчеты в браузере, то фильтрация данных невозможна.

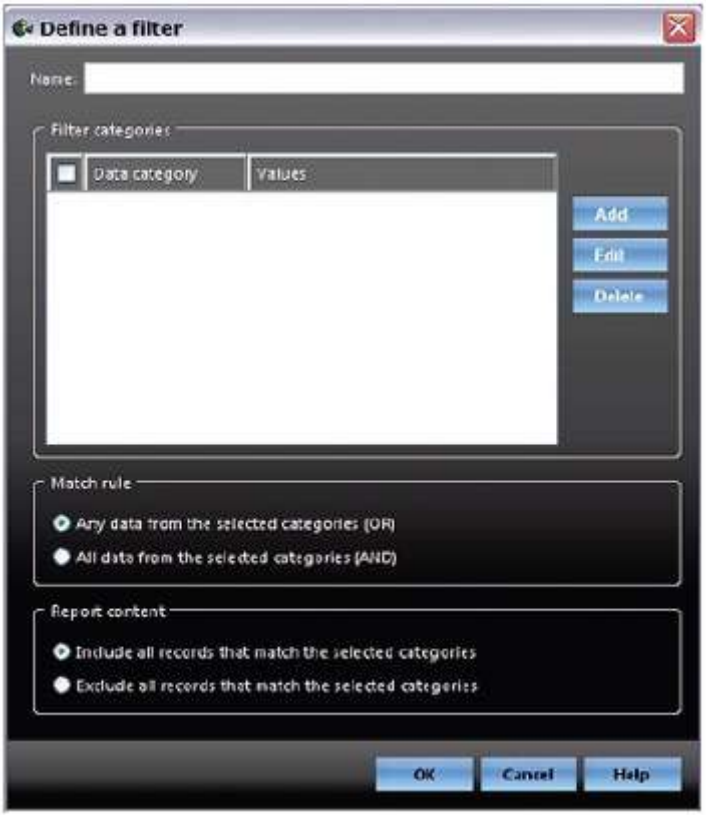
Создание фильтра

Вы можете создать фильтр в Report Manager после выбора отчета.

1. Выберите параметры отчета и отображение отчета.
   Откроется отчет



2. В выпадающем списке **Select filter** выберите **Define a filter**.
   Откроется диалоговое окно Define



3. В поле **Name** введите имя для фильтра.

4. Нажмите **Add** для создания категории данных для фильтра.
   Откроется диалоговое окно Define

5. Выберите **Data category** из выпадающего списка.

   Source IP/Host Name

   IP-адрес источника или имя хоста, включенного в запись журнала.

   Port Number

   Порт Источника или получателя, включенного в запись журнала.

   User Name

   Имя пользователя, включенного в запись журнала. Величина для этой категории чувствительна к регистру.

   Destination IP/Host Name

   IP-адрес назначения или имя хоста, включенного в запись журнала.

6. В поле **Values** введите значение для категории данных.

7. Нажмите **Add**.
   Величина появится в окне Values.

8. Выберите **Match rule** для категории фильтра.

9. Нажмите **OK**.
   Категория фильтра появится в списке Filter categories list.

10. Выберите **Match rule** для фильтра.

11. Выберите опцию **Report content** для включения или исключения отфильтрованного содержания.

12. Нажмите **OK**.
    Фильтр откроется в выпадающем списке Select filter.

Применение или удаление фильтра

Для применения фильтра в отчете необходимо выполнить:

1. В списке **WatchGuard Reports** выберите отчет.

2. В выпадающем списке **Select** выберите фильтр или создайте его вручную

Если фильтр применяется к отчету и выбраны различные отчеты в списке **WatchGuard Reports,** однотипные фильтры автоматически применятся к новому отчету. Вы можете применять или удалять различные фильтры для отчетов. Для удаления фильтров из отчетов необходимо выполнить:

В выпадающем списке **Select filter** выберите **None**.
Нефильтрованные данные отчета появятся в выбранном отчете.

Изменение фильтра

Вы можете изменить любые детали фильтра после его создания.

1. В выпадающем списке **Select filter** выберите фильтр для изменения.

2. Нажмите  .
Откроется диалоговое окно Modify a filter

3. Для создания фильтра другой категории данных нажмите **Add**.
Откроется диалоговое окно Define a filter category.

4. Заполните все необходимые поля и нажмите **OK**.

5. Для изменения категории данных выберите ее и нажмите **Edit**.
Откроется диалоговое окно Modify a filter category.

6. Совершите любые необходимые изменения и нажмите **OK**.

7. Для изменения имени фильтра введите новое имя в поле **Name**.

8. Сделайте все необходимые изменения в **Match rule** в **Report content**.

9. Нажмите **OK**.
Измененный фильтр появится в выпадающем списке Select filter.

Удаление фильтров

Вы можете отключить все фильтры в списке, но не более одного за один раз.

1. Нажмите на выпадающий список **Select filters** и выберите **Clear filters**.
   Откроется сообщение с подтверждением.

2. Нажмите **OK**.
   Все фильтры удалятся из списка.

Выбор формата отчета

Вы можете просмотреть ваш отчет в HTML или PDF-формате или в вашем браузере по умолчанию.

1. Откройте ваш отчет.

2. Выберите соответствующий формат для отчета:

   * для просмотра отчета в HTML-формате нажмите  .

   * для просмотра отчета в PDF -формате нажмите  .

   * для просмотра отчета в браузере по умолчанию нажмите  .

Отправка отчета по электронной почте, печать и сохранение отчета

После того, как вы выбрали отчет, вы можете его отправить по почте, распечатать или сохранить его прямо из Report Manager.

Отправка отчета по электронной почте

1. Отобразите отчет.

2. Нажмите  . Или выберите **File > Send to**.
   Если отчет в HTML формате, откроется электронное письмо с ссылкой на HTML файл.
   Если отчет в формате PDF, электронное письмо откроется с вложением.

Печать отчета

1. Отобразите отчет.

2. Нажмите  . Или выберите **File > Print**.

3. Если отчет в формате HTML, откроется диалоговое окно **Print**. Выберите необходимые параметры принтера и нажмите **Print**. Если отчет в формате PDF, отчет появляется в отдельном окне. Распечатайте отчет прямо из этого окна

Сохранение отчета

1. Отобразите отчет.

2. Нажмите  . Или выберите **File > Save as**.
   Откроется диалоговое окно Save.

3. Выберите расположение, имя файла и его тип.

Нажмите **Save**.
Если ваш браузер по умолчанию не Internet Explorer или Firefox, вам для просмотра лучше выбрать браузер

Глава 24 - Сертификаты и Центр Сертификации

Сертификаты

Сертификаты используются для аутентификации пользователя или организации. Сертификаты используют пару ключей, которая состоит из двух математически связанных чисел. У пользователя хранится один ключ - секретный ключ.

Пользователь может передавать другим пользователям второй (открытый) ключ. Ключи в паре ключей идут вместе. Секретные ключи, используемые для подписи сертификата, могут быть из той же пары ключей, что и ключи, которые использовались для генерации сертификата, или из другой пары ключей

Если применяется м ключ, используемый для создания сертификата, результатом будет самоподписанный сертификат. Если секретный ключ применяется из другой пары ключей, результатом является обыкновенный сертификат.

Сертификаты с секретными ключами, которые используются для подписи других сертификатов, называются сертификатами ЦС (Центр Сертификатов). Центр Сертификатов – это организация или приложение, которое подписывает или отзывает сертификаты. Если в вашей компании используется PKI инфраструктура, то вы можете самостоятельно подписывать сертификаты

Большинство приложений и устройств автоматически принимают сертификаты от доверенных ЦС. Сертификаты, которые не подписаны известным ЦС, например самоподписанные сертификаты, автоматически не принимаются многими серверами или программами и некорректно работают с некоторыми функциями Fireware XTM.

Использование нескольких сертификатов для установления доверия

Некоторые сертификаты могут использоваться вместе для создания цепи доверия. Например, сертификат ЦС в начале цепочки – это сертификат известного ЦС и используется для подписи сертификатов более мелких ЦС. Сертификаты более мелких ЦС могут затем подписывать другие сертификаты ЦС, используемые вашей организацией. Наконец, ваша организация может использовать сертификат ЦС для подписи других сертификатов, которые используются в HTTPS-прокси.

Однако для того чтобы использовать этот последний сертификат в цепочке, вам необходимо импортировать сертификаты всех ЦС в этой цепочке в следующем порядке:

1. Сертификат ЦС от известного ЦС (как тип «Other»)
2. Сертификат ЦС от более мелкого ЦС (в качестве «Other»)
3. Сертификат ЦС от организации (в качестве «Other»)
4. Сертификат, используемый для повторного шифрования содержимого HTTPS-прокси после проверки (в качестве «Центра HTTPS-прокси»).

Это может понадобиться для импорта всех сертификатов на каждое устройство клиента, чтобы последний сертификат так же доверялся пользователями

Как Firebox использует сертификаты

Ваш Firebox использует сертификаты для нескольких целей:

- Данные сеансов управления защищаются сертификатами.
- BOVPN или Mobile VPN with IPSec туннели могут использовать сертификаты для аутентификации.
- При проверки содержимого HTTPS-прокси использует сертификат для повторного шифрования входящего HTTPS-трафика после расшифровки.
- Вы можете использовать сертификаты с HTTPS-прокси для защиты веб-сервера в вашей сети.
- При аутентификации пользователя Firebox с какой-либо целью, например изменение параметров WebBlocker, соединение шифруется с сертификатом.

По умолчанию ваш Firebox создает самоподписываемые сертификаты для защиты данных сеанса управления и попытки аутентификации для Fireware XTM Web UI и для проверки содержимого HTTPS-прокси.

Для того чтобы убедиться в уникальности сертификата, который используется для углубленной проверки содержимого HTTPS прокси, его имя содержит серийный номер и дату создания. Из-за этого, что эти сертификаты не подписаны доверенным ЦС, пользователи вашей сети увидят предупреждение о том, что сертификат не подписан доверенным ЦС

У вас есть 3 опции для удаления предупреждения:

1. Вы можете импортировать сертификаты, которые подписаны доверенным ЦС Мы рекомендуем по возможности выбирать эту опцию
2. Вы можете создать самоподписанный сертификат, которое будет соответствовать имени и расположению вашей организации.
3. Вы можете использовать самоподписанные сертификаты по умолчанию.

Если вы хотите использовать вторую и третью опции вам необходимо попросить ваших пользователей принять этот сертификат во время подключения к устройству Firebox. Или вы можете экспортировать сертификат в файл и разослать его всем пользователям. Вам следует установить WatchGuard System Manager для экспорта сертификатов.

Время жизни сертификата и CRL

Каждый сертификат имеет время жизни. После окончания времени жизни (срока действия) сертификата его нельзя использовать. Вы можете так же удалять сертификаты вручную из Firebox System Manager (FSM).

Иногда сертификаты могут быть отозваны. Firebox хранит список отозванных сертификатов - Certificate Revocation List (CRL) – список, который используется для проверки валидности сертификатов, которые используются для VPN аутентификации. Если вы установили WatchGuard System Manager, этот список может быть обновлен вручную с помощью Firebox System Manager (FSM) или автоматически с помощью информации сертификата.

Каждый сертификат содержит уникальный номер, используемый для идентификации сертификата. Если уникальный номер Web Server, BOVPN, или Mobile VPN with IPSec сертификата есть в списке CRL, Firebox этот сертификат отключает

Если в настройках HTTPS-прокси включена проверка содержимого, то Firebox при помощи протокола OCSP (Online Certificate Status Protocol) проверяет статус сертификата, который использовался для подписи HTTPS содержимого. OCSP сервер отправляет устройству Firebox

статус сертификата. Firebox принимает OCSP ответ, если он подписан сертификатом, которому устройство Firebox доверяет Если OCSP-ответ не подписан сертификатом, которому доверяет Firebox или если OCSP сервер не прислал ответ, то вы можете настроить Firebox таким образом, чтобы он либо отклонял, либо принимал этот сертификат

Центры Сертификации и подпись запросов

Для создания самоподписывающегося сертификата вы помещаете часть зашифрованной пары ключей в CSR (Certificate Signing Request) запрос, который отправляется Центру Сертификации. Для каждого CSR запроса необходимо использовать новую пару ключей. После того, как ЦС проверит CSR запрос и идентифицирует вас, он выдаст вам сертификат

Если у вас есть программное обеспечение FSM или Сервер Управления, вы можете использовать эти программы для создания CSR на вашем Firebox. Вы можете так же использовать другие инструменты, такие как OpenSSL или the Microsoft CA Server, которые идут в комплекте с большинством ОС Windows Server. Если вы хотите создать сертификат для использования функции проверки содержимого HTTPS-прокси, необходимо, чтобы сертификат ЦС мог повторно подписать другие сертификаты. Если вы создали CSR запрос с помощью Firebox System Manager и подписали его у известного ЦС, то вы можете использовать этот сертификат в качестве сертификата ЦС. Если вы не хотите устанавливать PKI в вашей организации, вы рекомендуем выбрать известный ЦС для подписи CSR, кроме сертификатов ЦС для HTTPS-прокси.

Если известный ЦС подписал ваши сертификаты, то они этим сертификатам автоматически доверяют большинство пользователей. WatchGuard имеет несколько протестированных сертификатов, подписанных VeriSign, Microsoft CA Server, Entrust, и RSA KEON. Вы можете так же импортировать сертификаты других ЦС, чтобы ваш Firebox им доверял

В WatchGuard System Manager Сервер Управления так же работает качестве ЦС. ЦС выдает сертификаты для устройств управляемого Firebox при их контакте с Сервером Управлении для получения обновлений конфигурации

Просмотр и управление сертификатами Firebox

В Firebox System Manager вы можете:

- просматривать список текущих сертификатов Firebox и и параметры
- удалять сертификаты из Firebox.
- Создавать CSR запросы.
- импортировать сертификат или CRL (список отключенных сертификатов).
- экспортировать сертификаты для повторной подписи или рассылки.

Просмотр текущих сертификатов

Для просмотра текущего списка сертификатов:

1. Откройте Firebox System Manager.
2. Выберите **View** > **Certificates**.
   Откроется диалоговое окно Certificates

В этом диалоговом окне вы можете увидеть список всех сертификатов и CSR-запросы. В список включены:

* состояние и тип сертификата

* используемый сертификатом алгоритм

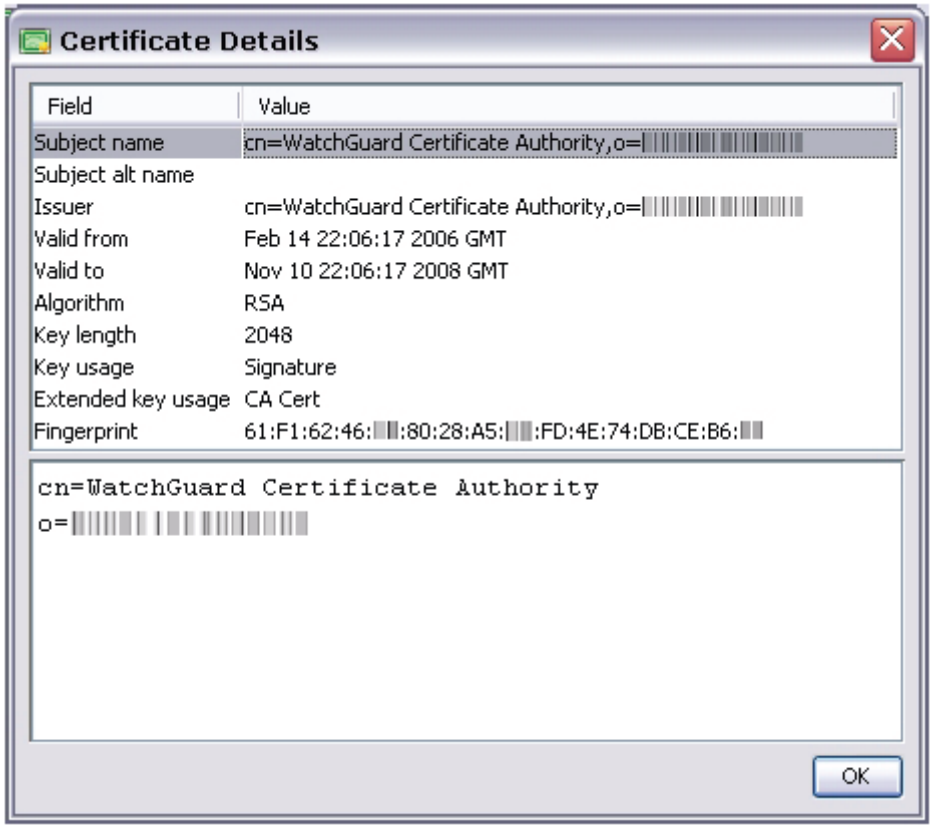
* Subject или идентификатор сертификата.

Вы умолчанию сертификаты доверенного ЦС не отображаются в этом списке. Вы можете просмотреть все сертификаты от доверенных ЦС.

3. Для просмотра всех сертификатов от доверенных ЦС включите опцию **Show Trusted CAs for HTTPS Proxy.**

4. Для того чтобы скрыть отображение сертификатов от доверенных ЦС отключите опцию **Show Trusted CAs for HTTPS Proxy**.

5. Для просмотра дополнительной информации о сертификате в списке выберите сертификат и нажмите **Details**.
Диалоговое окно Certificate Details отобразится с информацией о подписанном сертификате ЦС и отпечатке сертификата. Вы можете использовать эту информацию для устранения неполадок или однозначно идентифицировать сертификаты.



Удаление сертификатов

При удалении сертификатов он больше не может быть использованным для аутентификации.

Если вы удалите один из автоматически созданных сертификатов, например самоподписанный сертификат, используемый по умолчанию для HTTPS-прокси, ваш Firebox создает новый самоподписанный сертификат при следующей перезагрузке. Если вы импортировали другой сертификат, Firebox автоматически не будет создавать новый самоподписанный сертификат

Для того чтобы удалить сертификат выполните следующее:

1. Выберите сертификат в диалоговом окне **Certificates**.

2. Нажмите **Delete**.
Откроется диалоговое окно Remove Certificate.

3. Введите пароль конфигурации Firebox (чтение/запись)

4. Нажмите **OK**.
Сертификат будет удален.

Импортирование CRL из файла

Вы можете импортировать CRL, который вы до этого загрузили из своего локального компьютера.

CRL используется только для проверки состояния сертификатов, используемых для VPN-аутентификации.

1. Выберите **View** > **Certificates**.
   Откроется диалоговое окно Certificates.

2. Нажмите **Import Certificate/CRL**.

3. Выберите закладку **Import a CRL**

4. Нажмите **Browse** для поиска файлов.

5. Нажмите **Import CRL**.
   Откроется диалоговое окно Import CRL.

6. Введите пароль конфигурации.

7. Нажмите **OK**.
   Заданный вами CRL добавится в CRL на вашем Firebox.

Импорт сертификата из файла

Вы можете импортировать сертификат из буфера обмена Windows или из файла на вашем локальном компьютере. Сертификаты должны быть в формате PEM (base64).

Перед тем, как импортировать сертификата, которые будет использоваться HTTPS-прокси, вам необходимо импортировать все сертификаты из цепочки доверия для того чтобы устройство Firebox им также доверяло

1. Выберите **View** > **Certificates**.
   Откроется диалоговое окно Certificates.

2. Нажмите **Import Certificate/CRL**.

3. Выберите переключатель, который соответствует функции сертификата:

   * Если сертификаты используются политикой HTTPS прокси, которая управляет web-трафиком пользователей, подключенных к Trusted или Optional сетям, то выберите **HTTPS Proxy Authority (for deep packet inspection).** Сертификат, который вы импортируете для этой цели, должен быть сертификатом ЦС. Перед тем, как импортировать сертификат, который будет использоваться для шифрования HTTPS трафика, вам необходимо импортировать сертификат, который будет использоваться для подписи этого

сертификата, с категорией “**Other**”

* Если сертификат используется для политики HTTPS-прокси, которая управляет трафиком с внешней сети на веб-сервер, защищенный устройством Firebox, выберите **HTTPS Proxy Server.**

***** Убедитесь, что вы импортировали сертификат ЦС, используемый ля подписи сертификата с категорией «Другой» до импорта сертификата ЦС, использующего повторную подпись их веб-сервера HTTPS.

* Для сертификата, который будет использоваться для проверки HTTPS трафика, который не шифруется HTTPS-прокси – например, корневой сертификат или сертификат промежуточного ЦС, который используется для подписи сертификата внешнего web сервера - выберите **Trusted CA for HTTPS Proxy**.

* Если сертификат используется для аутентификации или других целей выберите **IPSec, Web Server, Other**. Выберите эту категорию, если вы хотите импортировать сертификат для создания цепи доверия к сертификату, который используется для повторного шифрования сетевого трафика

4. Нажмите **Paste** для вставки содержимого буфера обмена. Или **Load from File** для выбора файла на вашем локальном компьютере, содержащем сертификат. Если файл так же содержит секретный ключ, то введите пароль для его расшифровки.

5. Нажмите **Import Certificate**.
Сертификат будет добавлен в Firebox.

Экспорт сертификата

Вы можете экспортировать сертификат для повторной подписи доверенным ЦС или для рассылки его вашим пользователям

1. Выберите **View** > **Certificates**.

2. Выберите сертификат и нажмите **Export**.

3. Выберите расположение и введите имя для сертификата.
Сертификат сохраняется в формате PEM

Просмотр и управление сертификатами Сервера Управления

Вы можете посмотреть список сертификатов на Сервере Управления. Для этого обычно используется web-приложение CA Manager. Вы также можете выполнить некоторые функции из окна WatchGuard System Manager

Использование web-приложение CA Manager

1. Откройте WatchGuard System Manager.

2. Подключитесь к Серверу Управления.
Вам следует ввести пароль конфигурации для подключения

3. Нажмите закладку **Device Management** .

4. Нажмите  . Или выберите **Tools** > **CA Manager**.

web-приложения CA Manager имеют несколько страниц, которые могут использоваться для управляемых сертификатов.

- **Certificate Authority CA Certificate —** Показывает сертификат ЦС. Вы можете сохранить сертификат в файл или скопировать его содержимое в буфер обмена Window

- **Management Server CA Certificate** — Показывает сертификат ЦС Сервера Управления. Вы можете сохранить сертификат в файл или скопировать его содержимое в буфер обмена Windows

- **Generate a New Certificate** — Опция для создания нового сертификата

- **Find and Manage Certificates** — На этой странице вы можете искать сертификаты по серийному номеру, параметру Common Name или OU. Затем вы можете просмотреть детали для отмененных, восстановленных или поврежденных сертификатов, возвращенных в результате поиска.

- **List and Manage Certificates** - Для того чтобы посмотреть полную информацию о сертификате выберите его номер в колонке **Serial**. Эта страница показывает подробную информацию о сертификате, например его алгоритм подписи и издателя.

    - *Для того чтобы изменить статус одного или нескольких сертификатов,* напротив каждого сертификата отметьте флаг. В нижней части страницы выберите действие из выпадающего списка и нажмите **Go**.

    - *При отзыве сертификата* он добавляется в список Certificate Revocation List (CRL) и не может быть использован для аутентификации.

    - *Если вы восстановите сертификат*, он удаляется из CRL и его можно снова использовать. Если вы удалите или уничтожите сертификат, он не добавляется в CRL, но его все равно нельзя использовать для аутентификации. CRL публикуется для каждого Firebox при подключении его к Серверу Управления

- **Upload Certificate Request** — На этой странице вы можете подписать запрос на сертификат от другого сервиса. Введите Common Name и OU, которые используются в сертификате, и затем нажмите **Browse** для того, чтобы найти CSR (Certificate Signing Request) файл. После того как вы закончите, нажмите **Upload**.

- **Publish a Certificate Revocation List (CRL)** —Эта опция используется для публикации CRL на каждом Firebox, подключенном к Серверу Управления. Любые VPN туннели, которые используют сертификат из нового списка CRL, прекращают свою работу, как только устройство получает этот новый CRL

Управление сертификатами при помощи WSM

Вы можете использовать WSM для того, чтобы посмотреть сертификаты, которые используются Сервером Управления, и удалить ненужные сертификаты.

1. Откройте WatchGuard System Manager.

2. Подключитесь в Серверу Управления.
   Необходимо ввести пароль конфигурации для подключения.

3. Выберите **File** > **Certificates**.
   Откроется диалоговое окно Certificate Maintenance со списком сертификатов, используемых WatchGuard System Manager. WatchGuard автоматически получит необходимые сертификаты

4. Для удаления сертификата выберите его и нажмите **Remove**. Если сертификат на данный момент используется Сервером Управления, вам следует прежде всего отключится от сервера до удалении сертификата.

5. Нажмите **OK**.
При удалении сертификата Сервера Управления не удаляйте сертификаты в Microsoft Internet Explorer.

Создание сертификата при помощи FSM или Сервера Управления

До создания сертификата вы можете выполнить CSR-запрос при помощи Firebox System Manager (FSM). Вы также можете создать новый сертификат для Mobile VPN при помощи встроенного Certificate Authority (CA) Manager на вашем Сервере Управления.

Создание сертификата с помощью FSM

1. Подключитесь к вашего Firebox и откройте FSM.

2. Выберите **View** > **Certificates**.

3. Нажмите **Create Request**.
Запустится Certificate Request Wizard.

4. Нажмите **Next**.

5. Выберите для каких целей будет использоваться этот сертификат

   * Если сертификат должен использоваться для повторного шифрованию содержимого при помощи HTTPS прокси выберите **HTTPS Proxy Authority**.

   * Если сертификат должен использоваться для повторного шифрования содержимого для защищенного веб-сервера при помощи HTTPS-прокси выберите **HTTPS Proxy Server**.

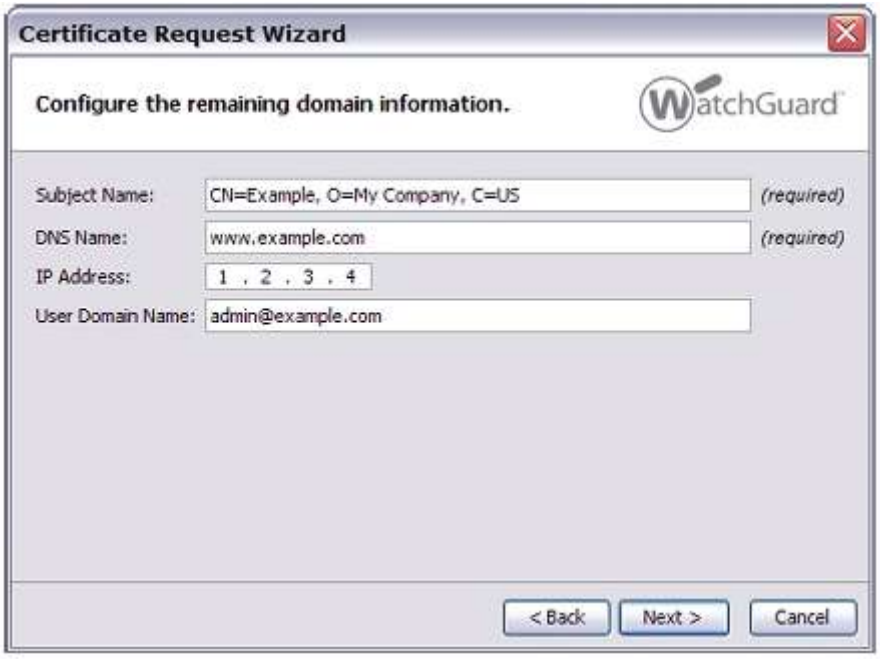
   * для других целей, включая аутентификацию VPN, Firebox, или Сервера Управления выберите **IPSec, Device, Web Server, Other**.

6. Нажмите **Next**.

7. Введите ваше имя , адрес и название вашей компании, город, штат или провинцию и страну, в которой вы работаете. Эти записи используются для создания названия темы

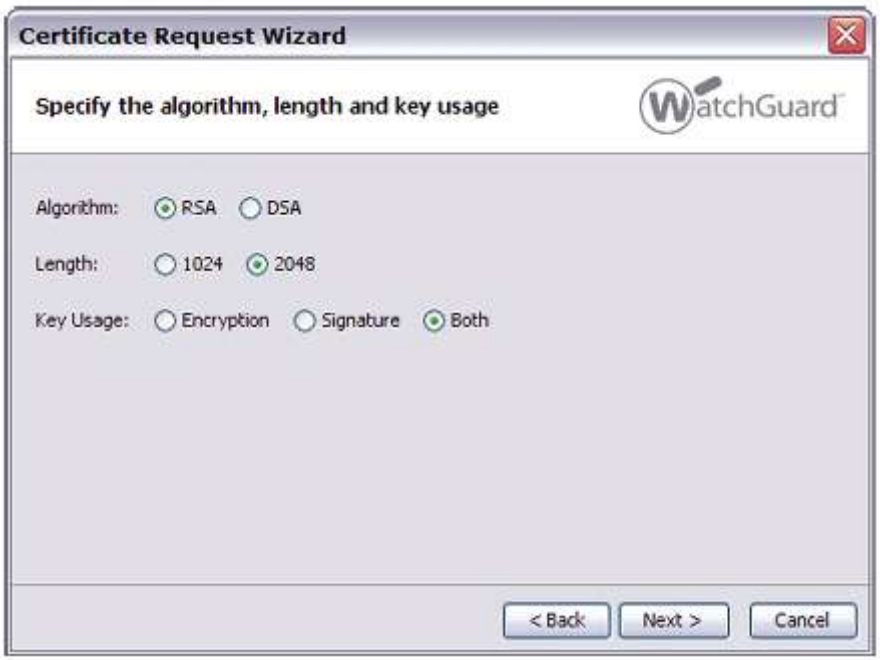
8. Нажмите **Next**.
Мастер создаст название темы на основании записей предыдущего окна.

9. Введите соответствующую информацию в поля **DNS name**, **IP address**, и **user domain name**



10. Нажмите **Next**.

11. По умолчанию сертификаты используют RSA-шифрование, 1024-битную длину ключа и шифрование и подписи для используемый ключей. Совершите все необходимые изменения для этих настроек. Нажмите **Next**.
Сертификаты центра HTTPS-прокси и сервера HTTPS-прокси не имеют опций для используемых ключей.



12. Нажмите **Next**. Введите тип пароля конфигурации.

13. Нажмите **OK** для просмотра завершенных CSR

14. Нажмите **Copy** для копирования **Certificate Signing Request** в буфер обмена Windows. Вам следует отправить этот CSR в ЦС для подписи до использования вашего Firebox. При импорте завершенных сертификатов вам следует, прежде всего, импортировать сертификат ЦС для подписи нового сертификата с категорией «Other».

15. Нажмите **Next**.

16. На последнем экране wizard вы можете:

    * Нажать **Import Now** для импорта сертификата.
    Откроется диалоговое окно Import Certificate/CRL

    * Нажмите **Finish ,** чтобы закрыть мастер установок.

Создание самоподписанного сертификата с помощью CA Manager

1. Откройте WatchGuard System Manager.

2. Подключитесь к Серверу Управления.
   Вам следует ввести пароль конфигурации для подключения.

3. Нажмите на закладку **Device Management** для Сервера Управления.

4. Нажмите  . Или выберите **Tools** > **CA Manager**.

5. Нажмите **Generate a New Certificate**.

6. Введите общее имя, пароль и время жизни сертификата в тему.

   * для пользователей Mobile VPN общее имя должно совпадать с именем удаленного пользователя.

   * для пользователей Firebox общее имя должно совпадать с информацией, идентифицирующей Firebox (обычно это IP-адрес).

   * для общих сертификатов общее имя – имя пользователя.

7. Если сертификат используется только для пользователей Mobile VPN введите организационную группу для темы. Организационная группа должна быть представлена в формате *GW:<vpn gateway name>.* Если вы не знаете имя шлюза VPN, используйте значение config.watchguard.id в файле конфигурации шлюза Firebox.

8. Для загрузки сертификата после его создания выберите опцию **Download Cert**.

9. Нажмите **Generate**.

Создание CSR с помощью OpenSSL

Для создания сертификата прежде всего необходимо создать Certificate Signing Request (CSR). Вы можете отправить CSR в ЦС или использовать его для создания сертификатов, подписанных самостоятельно.

Использование OpenSSL для создания CSR

OpenSSL устанавливается с большинством GNU/Linux. Для загрузки кода источника или бинарного файла Windows перейдите к http://www.openssl.org/ и следуйте инструкциям по установке ОС. Вы можете использовать OpenSSL, чтобы конвертировать сертификаты и CSR из одного формата в другой.

Более подробную информацию см. руководства по OpenSSL или online-документацию.

1. Откройте терминал командной строки.

2. Для создания частного ключа, называемого privkey.pem, в вашем текущем каталоге введите:
   openssl genrsa -out privkey.pem 1024

3. Введите:
   openssl req -new -key privkey.pem -out request.csr
   Эта команда создает CSR в формате PEM в вашем текущем каталоге.

4. Когда система вас попросит ввести x509 Common Name, то введите полное имя домена (FQDN)

5. Следуйте инструкциям вашего ЦС для отправки CSR.

Для создания временного, собственного сертификата в то время, как ЦС возвращает ваш подписанный сертификат:

1. Откройте командную строку.

2. Введите:
   openssl x509 -req -days 30 -in request.csr -key privkey.pem -out sscert.cert

эта команда создает сертификат внутри вашего текущего каталога, сроком в 30 дней с частным ключом и CSR, созданным вами в предыдущей процедуре.

Вы не можете использовать собственный сертификат для аутентификации удаленного шлюза VPN. Мы рекомендуем использовать сертификаты, подписанные доверенным ЦС.

Создание сертификата при помощи Microsoft CA

Вы можете сами создать сертификат при помощи Microsoft Certificate Authority (CA). Каждый CSR(certificate signing request) должен быть подписан ЦС перед тем, как использовать его для аутентификации.

При выполнении этой процедуры вы выступаете в качестве ЦС и сами подписываете свой запрос. Для обеспечения совместимости мы рекомендуем вам отправить CSR-запрос в такие ЦС, как Verisign или GeoTrust. Так как корневые сертификаты этих организаций по умолчанию установлены в большинстве Интернет браузеров, вам не надо вручную пересылать сертификат. Для завершения CSR-запроса вы можете использовать Windows Server 2003

Отправка запроса на сертификат

1. Откройте ваш web-браузер. В адресной строке введите IP-адрес сервера, на котором установлен ЦС, и *certsrv*. Например: *http://10.0.2.80/certsrv*.

2. Нажмите на ссылку **Request a Certificate**.

3. Нажмите **Advanced certificate request**.

4. Нажмите **Submit a certificate**.

5. В поле **Saved Request** вставьте содержимое вашего CSR запроса. Нажмите **OK**.

6. Закройте web-браузер.

Выдача сертификата

1. Подключитесь к серверу, на котором установлен ЦС.

2. Выберите **Start** > **Control Panel** > **Administrative Tools** > **Certification Authority**.

3. В дереве **Certification Authority** (Local) в панели навигации слева, выберите **Your Domain Name** > **Pending Requests**.

4. В правой навигационной панели выберите **CSR**

5. В меню Action выберите **All Tasks > Issue**.

6. Закройте окно ЦС.

Загрузка сертификата

1. В адресной строке введите IP-адрес сервера, на котором установлен ЦС, и *certsrv*. Например: *http://10.0.2.80/certsrv*

2. Нажмите **View the status of a pending certificate request**.

3. Выберите ваш запрос сертификата с временем и датой, предоставленной вами.

4. Выберите переключатель **Base 64 encoded** для того, чтобы выбрать формат PKCS10 или PKCS7.

5. Нажмите **Download certificate** для того, чтобы сохранить сертификат на жесткий диск.

Центр Сертификации является компонентом Windows Server 2003. Если ЦС не установлен в секции Administrative Tools Панели Управления, см. инструкцию производителя

Использование сертификатов для аутентификации

Вы можете использовать сертификаты для:

- Mobile VPN with IPSec tunnel authentication
- BOVPN tunnel authentication

Вы также можете настроить сертификат web-сервера для аутентификации Firebox. Сертификат web-сервера – этот сертификат, который используется устройством Firebox для HTTPS соединений, отмены WebBlocker или других целей.

После того, как вы выполните эти процедуры, мы рекомендуем вам подключиться к Firebox, чтобы Policy Manager смог загрузить список установленных сертификатов. Если сохраненные изменения с локального конфигурационного файла и новые настройки не совпадают с сертификатами на вашем Firebox, то Firebox может некорректно работать.

Использование сертификатов для аутентификации Mobile VPN with IPSec туннелей

Когда создается Mobile VPN туннель, протокол IPSec проверяет идентичность каждой конечной точки туннеля при помощи PSK (pre-shared key).Этот ключ может быть использован как пароль на обеих точках подключений или сертификат с Сервера Управления. Для того чтобы использовать сертификат для Mobile VPN аутентификации Firebox должен быть настроен как управляемый клиент. Для того чтобы использовать сертификат для нового туннеля Mobile VPN with IPSec выполните следующее:

1. В Policy Manager, выберите **VPN > Mobile VPN > IPSec**.
   Откроется диалоговое окно Mobile VPN with IPSec Configuration.

2. Нажмите **Add**.
   Откроется Mobile VPN with IPSec Wizard.

3. Нажмите **Next**.

4. Завершите страницу **Select a user authentication server**. Нажмите **Next**.

5. Выберите **Use an RSA certificate issued by your WatchGuard Management Server**.

6. Введите IP-адрес и пароль администратора вашего Сервера Управления.

7. Завершите работу мастера.

Для изменения существующего Mobile VPN-туннеля и использования сертификата при аутентификации необходимо выполнить:

1. В Policy Manager выберите **VPN > Mobile VPN > IPSec**.

2. Выберите Mobile VPN-туннель для изменения. Нажмите **Edit**.

3. Нажмите на закладку **IPSec Tunnel** .

4. Выберите **Use a certificate**.

5. Введите **IP address** Сервера Управления или ЦС. При необходимости установите timeout соединения.

6. Нажмите **OK**.

При использовании сертификатов вам следует выдать каждому пользователю Mobile VPN 3 файла:

- Профиль конечного пользователя (.wgx)
- Сертификат клиента (.p12)
- Корневой сертификат ЦС (.pem)

Когда пользователь Mobile VPN открывает файл .wgx, корневой и пользовательский сертификаты, которые содержатся в файлах cacert.pem и .p12, будут автоматически загружены

Для аутентификации Mobile VPN вы не можете использовать самоподписанные сертификаты или сертификаты сторонних производителей

Проверки VPN-сертификатов с помощью LDAP-сервера

Вы можете использовать LDAP-сервер для автоматической проверки сертификатов, используемых для VPN-аутентификации при доступе на сервер. Вам необходимо иметь учетную запись LDAP, предоставленную сторонним сервисом ЦС для использования этой функции.

1. В Policy Manager выберите **VPN > VPN Settings**.
   Откроется диалоговое окно VPN Settings

2. Выберите опцию **Enable LDAP server for certificate verification**.

3. В текстовом поле **Server** введите имя или адрес LDAP-сервера.

4. (дополнительно) введите или выберите номер порта **Port**.

5. Нажмите **OK**
   Ваш Firebox проверяет CRL, сохраненный на LDAP-сервере при запросе аутентификации туннеля.

Использование сертификата для аутентификации BOVPN туннеля

После того, как BOVPN туннель был создан, протокол IPSec идентифицирует каждую конечную точку туннеля при помощи PSK(Pre-Shared Key) или сертификата, который был импортирован на Firebox. Для того чтобы использовать сертификат для аутентификации BOVPN туннеля выполните следующее:

1. Выберите **VPN** > **Branch Office Gateways**.

2. Нажмите **Add** для создания нового шлюза. Или выберите существующий шлюз и нажмите **Edit**.

3. Выберите **Use IPSec Firebox Certificate**.

4. Выберите сертификат для использования.

5. Установите другие параметры, если это необходимо.

6. Нажмите **OK**.

Если вы используете сертификат для BOVPN-аутентификации необходимо выполнить:

- Необходимо импортировать сертификат
- Firebox System Manager должен опознавать сертификат как IPSec-сертификат.
- Убедитесь, что сертификат для устройств каждого шлюза конечной точки использует тот же алгоритм. Обе конечные точки должны использовать DSS или RSA. Алгоритм для сертификатов появится в таблице диалогового окна **New Gateway** в WatchGuard System Manager и в диалоговом окне **Certificates** на Firebox System Manager.
- Если у нас нет самоподписывающегося сертификата или сертификата стороннего производителя, вам следует использовать ЦС на WatchGuard Management Server.

Более подробную информацию см. Configure the certificate authority on the Management Server.

Проверки сертификата с помощью FSM

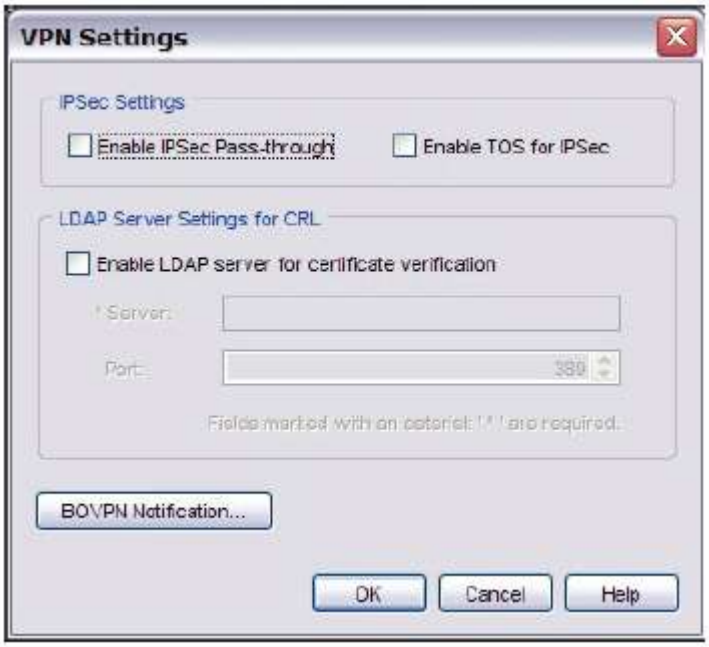
1. Выберите **View** > **Certificates**.
   Откроется диалоговое окно Certificates.

2. В колонке **Type** появится проверка *IPSec* или *IPSec/Web*.

Проверка VPN-сертификатов с помощью LDAP-сервера

Вы можете использовать LDAP-сервер для автоматической проверки сертификатов, используемых для VPN-аутентификации при доступе на сервер. Вам необходимо иметь учетную запись LDAP, предоставленную сторонним сервисом ЦС для использования этой функции.

1. Выберите **VPN** > **VPN Settings**.
   Откроется диалоговое окно VPN Settings



2. Выберите опцию **Enable LDAP server for certificate verification**.

3. В текстовом поле **Server** введите имя или адрес LDAP-сервера.

4. (дополнительно) введите номер порта **Port**.

5. Нажмите **OK**.
   Ваш Firebox проверяет CRL, сохраненные на LDAP-сервере при запросе аутентификации туннеля.

Настройка сертификата web-сервера для аутентификации Firebox

При подключении пользователя к устройству WatchGuard с помощью web-браузера часто появляется предупреждение о безопасности. Это предупреждение происходит из-за того, что сертификат по умолчанию не является доверенным или не соответствует IP-адресу или доменному имени, используемому при аутентификации. Если у вас есть обновление Fireware XTM with a Pro, вы можете использовать самоподписывающийся сертификат или сертификат стороннего производителя, который соответствует IP-адресу или доменному имени, необходимому при аутентификации.

Необходимо импортировать сертификат на каждый браузер клиента или устройство для предотвращение появления предупреждения.

Для просмотра сертификата текущего веб-браузера необходимо выполнить:

1. Откройте Firebox System Manager.

2. Выберите **View > Certificates**. Сертификат веб-сервера помечается астериксом (*).

При настройке сертификата веб-сервера для аутентификации Firebox :

1. Выберите **Setup** > **Authentication** > **Web Server Certificate**

2. Для использования сертификата по умолчанию выберите **Default certificate signed by Firebox**. См. п. 7

3. Для использования уже импортированного сертификата выберите **Third-party certificate**.

4. Выберите сертификат из выпадающего списка. См. п 7.
   Этот сертификат должен быть признанным как Web -сертификат Firebox System Manager.

5. Если вы хотите создать сертификат пользователя, подписанный вашим Firebox выберите **Custom certificate signed by Firebox**.

6. Введите общее имя **common name** для вашей организации. Обычно, это доменное имя. (Дополнительно) вы можете так же ввести **organization name** и **organization unit name** для идентификации части вашей организации, создающей сертификат.

7. Нажмите **Add Domain Names** или **Add Interface IP Addresses**

8. В текстовом поле внизу диалогового окна введите доменное имя или IP-адрес интерфейса на вашем Firebox.

9. Нажмите **Add**.

10. Повторите шаги 8-9 для добавления доменных имен.

11.нажмите **OK**.

Использование сертификатов для HTTPS-прокси

Многие веб-сайты используют оба протокола - HTTP и HTTPS – для отправки информации к пользователям. В то время, пока http-трафик может быть легко проверен, HTTPS-трафик – зашифрован.

Для просмотра HTTPS-трафика, запрашиваемого пользователями вашей сети, вам следует настроить ваш Firebox для расшифровки HTTPS трафика и затем повторно ее зашифровать при помощи сертификата, подписанного доверенным ЦС

По умолчанию Firebox повторно шифрует содержимое, проверяемое автоматически созданным самоподписанным сертификатом. Пользователи без копии этого сертификата увидят предупреждение при подключении к защищенному веб-сайту по HTTPS.

Если удаленный веб-сайт использует сертификат с истекшим сроком действия или сертификат подписан ЦС, которому Firebox не доверяет, Firebox подписывает содержимое как *Fireware HTTPS Proxy: Unrecognized Certificate* или просто *Invalid Certificate*.

Эта секция содержит информацию о процедуре эскпорта сертификата и его импорта в ОС Microsoft Windows или Mac OS X для его использования с HTTPS-прокси. Для более подробной информации об импорта сертификата на другие устройства, ОС или приложение см. соответствующую документацию

Защита внутреннего HTTPS-сервера

Для защиты HTTPS-сервера вашей сети необходимо прежде всего импортировать сертификат ЦС, используемый для подписи сертификата HTTPS-сервера, и затем импортировать сертификат HTTPS-сервера с его соответствующим ключом.

Если сертификат ЦС, используемый для подписи сертификата HTTPS-сервера не является автоматически доверенным, необходимо импортировать каждый доверенный сертификат последовательно для корректной работы этой функции. После импорта всех сертификатов настройте HTTPS-прокси необходим выполнить:

В Policy Manager необходимо выполнить:

1. Выберите **Edit** > **Add Policy**.
   Откроется диалоговое окно Add Policies.

2. Откройте категорию **Proxies** и выберите запись **HTTPS-proxy**. Нажмите **Add**.
   Откроется диалоговое окно New Policy Properties.

3. Выберите закладку **Properties** .

4. Нажмите  .

5. В категории **Content Inspection** (выбрана по умолчанию), выберите опцию **Enable deep inspection of HTTPS content**.

6. Выберите действие http-прокси для проверки содержимого HTTPS или создайте новое действие HTTPS-прокси для использования этой политики.

7. Отключите две опции для OCSP-подтверждения.

8. В **Bypass List**, введите IP-адреса веб-сайтов для отключения проверки трафика.

9. Нажмите дважды **OK**

10. Нажмите **Close**.

Более подробную информацию см. See and manage Firebox certificates.

Проверка содержимого для внешних HTTPS-серверов

Если ваша организация уже создала PKI (Public Key Infrastructure) с доверенным ЦС, вы можете импортировать сертификат на Firebox, подписанный ЦС вашей организации. Если сертификаты ЦС не являются автоматически доверенными , необходимо импортировать каждый предыдущий сертификат в цепи доверия для корректной работы этой функции

Если у вас есть другой трафик, использующий порт HTTPS, например SSL VPN-трафик, рекомендуется более тщательно проверять содержимое. SSL VPN-прокси пытается проверить весь трафик на том же пути, что и порт 443 TCP.Для проверки корректной работы других источников трафика, рекомендуется добавлять эти IP-адреса с список Bypass.

Перед тем, как включить эту функцию, вам необходимо разослать сертификаты, которые будут использоваться для подписи HTTPS-трафика, всем пользователям вашей сети.

Вы можете прикрепить сертификат в электронному письму с необходимыми инструкциями или автоматически его установить на всех компьютерах вашей сети. Так же мы рекомендуем сперва проверять работу HTTPS-прокси для малого количества пользователей

Если ваша организация не имеет PKI, вам необходимо скопировать сертификат по умолчанию или самоподписанный сертификат с устройства Firebox на компьютеры пользователей

В Policy Manager выполните следующее:

1. Выберите **Edit** > **Add Policy**.
   Откроется диалоговое окно Add Policies.

2. Откройте категорию **Proxies** и выберите запись **HTTPS-proxy**. Нажмите **Add**.
   Откроется диалоговое окно New Policy Properties.

3. Выберите закладку **Properties**.

4. Нажмите  .

5. В категории **Content Inspection** (выбрана по умолчанию) выберите опцию **Enable deep inspection of HTTPS content**

6. Выберите действие http-прокси для использования проверки содержимого HTTPS ли создайте новое действие http-прокси для использования этой политики.

7. Выберите опции для OCSP –подтверждения сертификата.

8. В списке **Bypass List**, введите IP-адрес веб-сайтов, трафик которых не проверяется.

9. Нажмите дважды **OK** .

10. Нажмите **Close**.

При включении проверки содержимого параметры WebBlocker действия HTTP -прокси отменяют параметры WebBlocker HTTPS-прокси. При добавлении IP-адресов в список Bypass трафик от этих сайтов фильтруется с помощью параметров WebBlocker в HTTPS-прокси. Более подробную информацию о настройке WebBlocker см. About WebBlocker.

Экспорт сертификата проверки содержимого HTTPS

Эта процедура экспортирует один сертификат из вашего Firebox в формате PEM.

1. Откройте Firebox System Manager и подключитесь к вашему Firebox.

2. Выберите **View** > **Certificates**.

3. Выберите сертификат ЦС **HTTPS Proxy Authority** из списка и нажмите **Export**.

4. Введите имя и выберите место для локального сохранения сертификата.

5. Скопируйте сохраненный сертификат для машин клиентов.

Если сертификат HTTPS прокси, который используется для проверки содержимого, требует наличия сертификата корневого или промежуточного ЦС, то вам также необходимо эскпортировать и эти сертификаты

Если вы ранее импортировали сертификата на компьютер клиента, то вы можете экспортировать сертификат прямо из хранилища сертификатор браузера или ОС. В большинстве случает сертификат экспортируется в формате x.509. Для того чтобы импортировать сертификат в ОС Windows и Mac OS X пользователям необходимо два раза нажать на сертификат

Импорт сертификата на устройства клиентов

Для использования сертификатов на устройстве клиентов с установленным Firebox необходимо экспортировать эти сертификаты из FSM, затем импортировать сертификаты на компьютер каждого пользователя

Устранение неполадок с помощью проверки содержимого HTTPS

Firebox часто создает сообщения журнала при проблемах с сертификатами, которые используются для проверки содержимого HTTPS. Мы рекомендуем проверять эти сообщения журнала для получения большей информации.

Если у вас проблемы с подключениями к удаленному серверу, то вам необходимо проверить, были ли импортированы все сертификаты, необходимые для доверия сертификату ЦС, который используется для повторного шифрования HTTPS содержимого, а также сертификаты, которые необходимы для доверия сертификату web сервера. Для успешной работы Вам следует импортировать все эти сертификаты на Firebox и на каждое устройство клиента.

Глава 25 - Управляемые BOVPN туннели

Управляемые BOVPN туннели

VPN (Virtual Private Network) создает защищенное подключение между географически разделенными компьютерами или сетями. Каждое отдельное подключение называется *туннелем*. Когда создается VPN туннель, то конечные точки туннеля должны аутентифицировать друг друга. Данные в туннеле передаются в зашифрованном виде. Только отправитель и получатель могут прочитать передаваемые данные.

BOVPN(Branch Office Virtual Private Networks) сеть позволяет организациям создать защищенные соединения между географически разделенными офисами. Сетями или хостами в VPN туннеле могут главный офис, филиалы, удаленные пользователи или удаленный работник. Технология BOVPN позволяет организациям передавать конфиденциальные данные по зашифрованным каналам связи между офисами. Это позволяет упростить связь, снижает стоимость выделенных линий и обеспечивают необходимый уровень безопасности на каждом конце туннеля.

При помощи WatchGuard System Manager вы можете быстро и просто настраивать IPSec туннели, использующие аутентификацию и шифрование. Такие туннели называются *управляемыми BOVPN туннелями*. Другой тип туннеля называется *BOVPN туннель, созданный вручную*, который в отличие от управляемого туннеля, создается при помощи нескольких диалоговых окон. Для более подробной информации о туннелях, создаваемых вручную, см. “BOVPN туннели, созданные вручную”.

Создание управляемого BOVPN туннеля

Вы можете быстро создать туннель между устройства при помощи процедуры drag-and-drop и простого мастера

Однако, перед тем создавать управляемые туннели, вам необходимо выполнить следующие процедуры:

1. Добавить устройства WatchGuard, которые будут использоваться как конечные точки туннеля, на Сервер Управления

2. Если для VPN аутентификации вы используете сертификат, вам необходимо его импортировать. Этот сертификат должен быть идентифицирован Firebox System Manager как сертификат IPSec. Для того чтобы это проверить, откройте Firebox System Manager, выберите **View > Certificates** и проверьте значение колонки **Type** в диалоговом окне **Certificates.** Ее значение должно быть равным "IPSec" или "IPSec/Web." Если у вас нет стороннего или самоподписанного сертификатов, вам необходимо использовать Центр Сертификации, который входит в Сервер Управления

Опции туннеля

Вы можете использовать несколько опций для настройки управляемых VPN туннелей:

- Если trusted сеть, подключенная к одному из устройств, содержит большое количество маршрутизируемых и вторичных сетей, данные которых вы хотите также передавать через туннель, вам необходимо добавить их к устройству, в качестве VPN ресурсов. Для более подробной информации см. “Создание VPN ресурсов”

- Если вы хотите заблокировать передачу определенных типов трафик через управляемый BOVPN туннель, или если вы хотите заблокировать трафик передачи данных журнала на Сервер Журналов, вам необходимо использовать шаблоны политики VPN Firewall. Или вы можете использовать шаблон политики, созданный на Сервере Управления. Для более подробной информации см. “Создание шаблонов политики VPN брандмауэра”

- Мастер, при помощи которого вы можете создавать управляемые BOVPN туннели, позволяет вам выбрать алгоритмы шифрования, которые подходят для большинства конфигураций VPN туннелей. Однако вы при необходимости можете создать свои собственные настройки, которые будут удовлетворять требованиям вашей сети. Для более подробной информации см. “Создание шаблонов безопасности”

VPN переключение

VPN переключение, описание которой приведено в “VPN переключение”, также поддерживается в управляемых BOVPN туннелях. Если вы используете multi-WAN и вы создаете управляемые туннели, WSM автоматически настраивает пару шлюзов, которые включают в себя внешние интерфейсы на обоих концах туннеля. Дополнительного конфигурации не требуется.

Глобальные параметры VPN

Глобальные параметры VPN на вашем Firebox применяются ко всем ручным BOVPN туннелям, управляемым туннелям и Mobile VPN туннелям. Вы можете использовать эти параметры для:

- Включения опции IPSec pass-through.

- Управления пакетов с установленными битами ToS (Type of Service).

- Использования сервера LDAP для проверки сертификатов.

Настройки Firebox для отправки уведомления в случае выхода из строя туннеля BOVPN (только для BOVPN туннелей).

Для того чтобы изменить эти параметры в Policy Manager выберите **VPN > VPN Settings**

Состояние BOVPN туннеля

Вы можете при помощи Firebox System Manager посмотреть текущее состояние BOVPN туннелей. Эта информация также отображается в закладке **Device Status** системы WatchGuard System Manager

Повторная генерация ключей для BOVPN туннеля

При помощи Firebox System Manager вы можете мгновенно сгенерировать новую пару ключей для BOVPN туннелей вместо того, чтобы ждать истечения их срока действия

Создание VPN ресурсов

VPN ресурс – это сеть, устройствам которой разрешается передавать данные через указанный VPN туннель. Если конечное VPN устройство имеет статический IP адрес, всем устройствам trusted сетей, подключенных к устройству, автоматически разрешается передача данных по туннелю. Сервер Управления создает VPN ресурс по умолчанию для устройства, который включает в себя все trusted-сети

Однако, если trusted сеть, подключенная к устройству, содержит большое количество маршрутизируемых и вторичных сетей, устройствам которых вы хотите разрешить передачу данных по туннелю, вам необходимо их вручную добавить в качестве VPN ресурсов. Если конечное устройство имеет динамический IP адрес, вам необходимо информацию о его текущих ресурсах, как описано ниже, или добавить любые сети, подключенные к этому устройству в

качестве VPN ресурсов. Сервер Управления автоматически не будет создавать VPN ресурсы для этих сетей.

Получение информации о текущих ресурсах устройства

Если конечное устройство имеет динамический IP адрес, получите информацию о политиках, которые применяются для сетей, подключенных к этому устройству. Или вы можете пропустить эту процедуру и добавить сети в качестве VPN ресурсов.

1. В WatchGuard System Manager выберите управляемое устройство в закладке **Device Management**, затем выберите **Edit > Update Device**.
   Откроется диалоговое окно Update Device

2. Включите опцию **Download Trusted and Optional Network policies**

3. Нажмите **OK**.

Создание нового VPN ресурса

Для того чтобы создать новый VPN ресурс в закладке **Device Management** выполните следующее:

1. Выберите устройство, для которого вы хотите создать VPN ресурс, и нажмите . Или нажмите правой кнопкой на устройство и выберите **Insert VPN Resource**.
   Откроется диалоговое окно VPN Resource для этого устройства

2. В поле **Policy Name** введите имя политики. Это имя будет отображаться в окне Device Management и в мастере Add VPN Wizard.

3. В выпадающем списке **Disposition** выберите одну из следующих опций:

   secure

   Шифровать трафик, передаваемый с и на этот ресурс. Эта наиболее часто используемая опция.

   Bypass

   Передавать трафик в открытом виде. Вы можете использовать эту опцию, если один из Firebox работает в режиме drop-in и туннель маршрутизирует трафик в сеть drop-in. В этом случае drop-in IP адрес должен быть разрешен, а не заблокирован, иначе туннель не будет создан

   Block

   Заблокировать трафик через VPN. Вы можете это сделать, если вы хотите заблокировать трафик с одного или нескольких IP адресов, которые принадлежат подсети, которой передача трафика разрешена

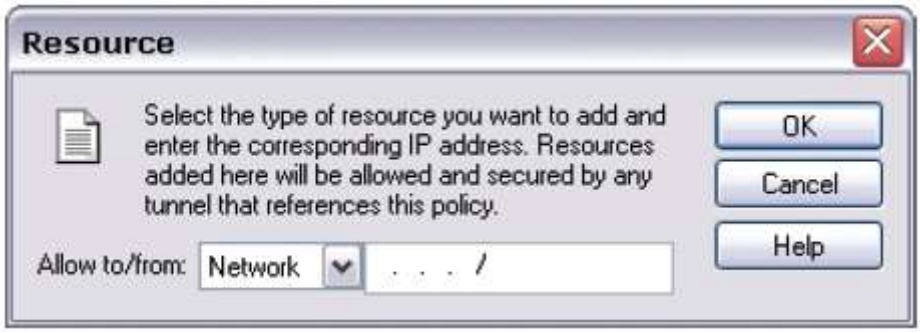
   *Если вы хотите создать VPN ресурс для Firebox X Edge, который не использует Fireware XTM версии 11.0 или выше, то поле **Disposition** не появится, так как поддерживается только опция **secure**.*

4. Создайте, измените или удалите ресурсы. Нажмите **Add** для того чтобы добавить IP адрес устройства или адрес сети. Нажмите **Edit** для того чтобы редактировать существующий ресурс. Для того чтобы удалить ресурс, выберите его в списке **Resources** и нажмите **Remove**

5. Нажмите **OK**.

Добавление хоста или сети

1. В диалоговом окне **VPN Resource** нажмите **Add**.
   Откроется диалоговое окно Resource



2. В выпадающем списке **Allow to/from** выберите тип ресурса и затем в соответствующих текстовых полях введите IP адрес или адрес сети.

3. Нажмите **OK**.

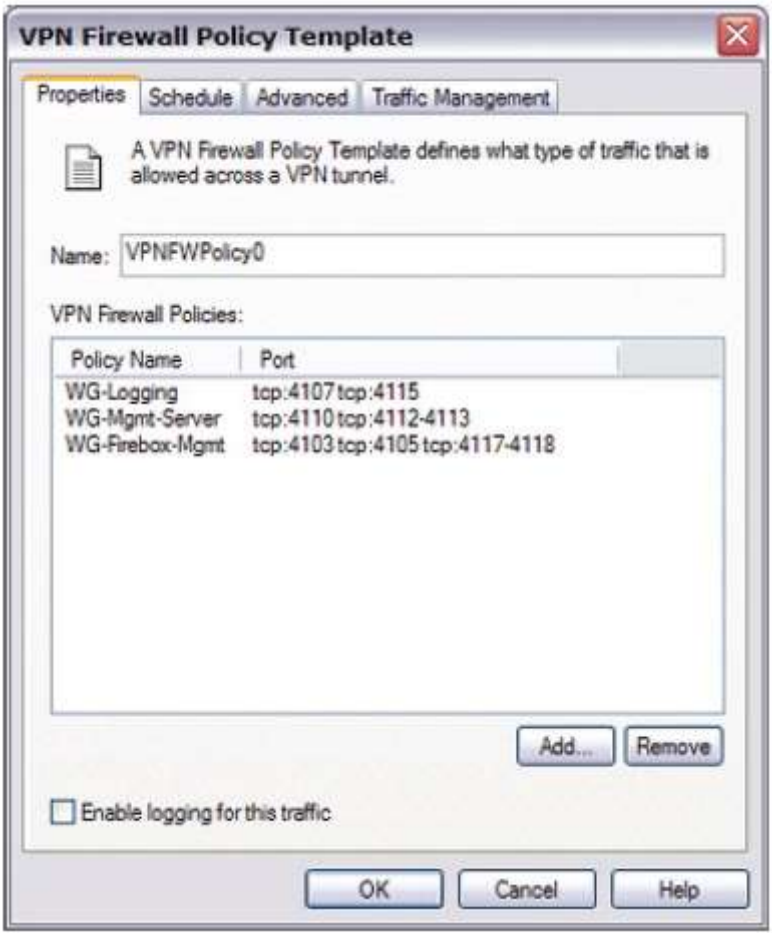
Создание шаблонов политики VPN брандмауэра

При помощи шаблонов политики VPN Firewall вы можете создать набор политик для межсетевого экрана, которые запрещают определенные типы трафика через VPN. Необходимо отметить, что шаблоны политик не поддерживают политики прокси. Если вы будете использовать политику Any VPN, для всего трафика, передаваемого по управляемому VPN туннелю, будут генерироваться сообщения журнала. Если вы хотите управлять процедурой записи трафика в журнал, вам необходимо создать свой собственный шаблон политики VPN Firewall и включить опцию **Enable logging for this traffic**. Для политики Any VPN вы не можете отключить ведение журнала

Для того чтобы создать шаблон политики VPN Firewall выполните следующее:

1. В левой части (дерево) закладки **Device Management** откройте каталог **Managed VPNs**, и нажмите **VPN Firewall Policy Templates**. *Откроеися список текущих шаблонов политик*

2. В правом верхнем углу окна нажмите **Add**.
   Откроется диалоговое окно VPN Firewall Policy Template



3. В поле **Name** введите имя для шаблона политики. Это имя будет отображаться в дереве Device Management и мастере Add VPN

4. Для того чтобы добавить политику к шаблону нажмите **Add**. *Запустится мастер Add Policy.*

5. Выберите одну из предустановленных политик или создайте свою собственную. Если вы захотите создать свою собственную политику, то в следующих окна мастера введите имя, порт и протокол для этой политики.

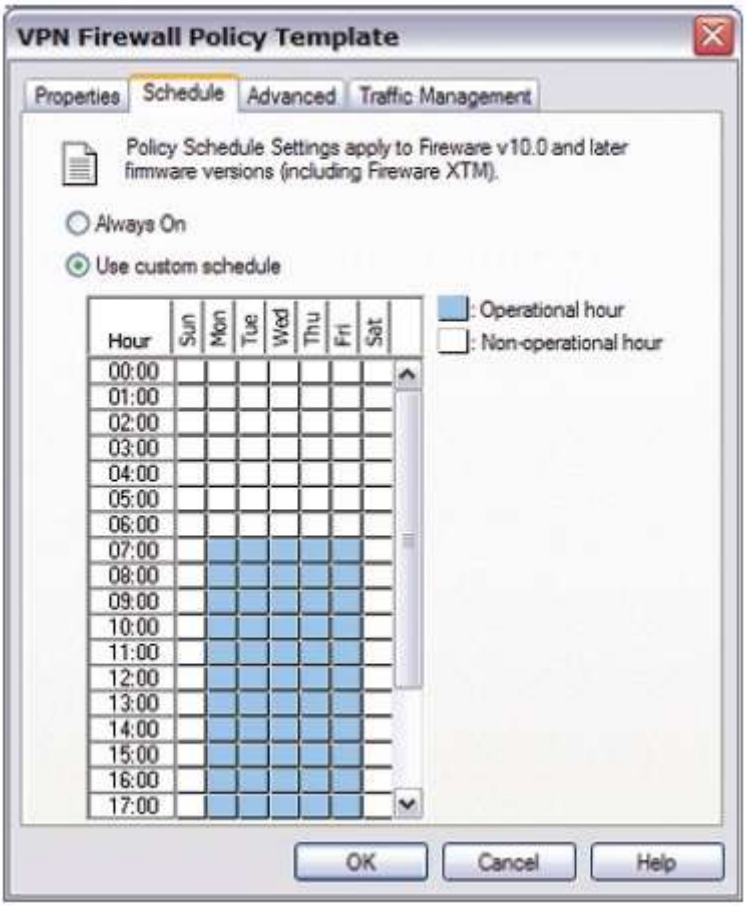
6. После того, как вы добавите политику, вы можете повторить эту процедуру для добавления новых политик. Нажмите **OK**

Настройка расписания для шаблона политики

По умолчанию шаблон политики применяется в любое время (**Always On)**. Если вы хотите выключить шаблон политики в определенные часы, вы можете настроить расписание работы шаблона политики.

1. Выберите закладку **Schedule**
   Откроется окно Policy Schedule Settings.

2. Для того чтобы изменить рабочие часы шаблона политики выберите **Use custom schedule**. *Откроется расписание*



3. Ось X на графике показывает дни недели. Ось Y показывает часы. Для того чтобы выбрать рабочие часы шаблона политики нажмите на соответствующие блоки.

QoS маркирование в шаблоне политики

При помощи QoS Маркирования вы можете помечать трафик, который использует шаблон политики VPN брандмауэра. Маркирование применяется для всего трафик, который использует политику.

1. Выберите закладку **Advanced**
2. Включите опцию **Override per-interface settings**
3. Настройте параметры QoS Маркирования, как описано в “Включение QoS маркирования для управляемого BOVPN-туннеля”

Настройка Traffic Management в шаблоне политики

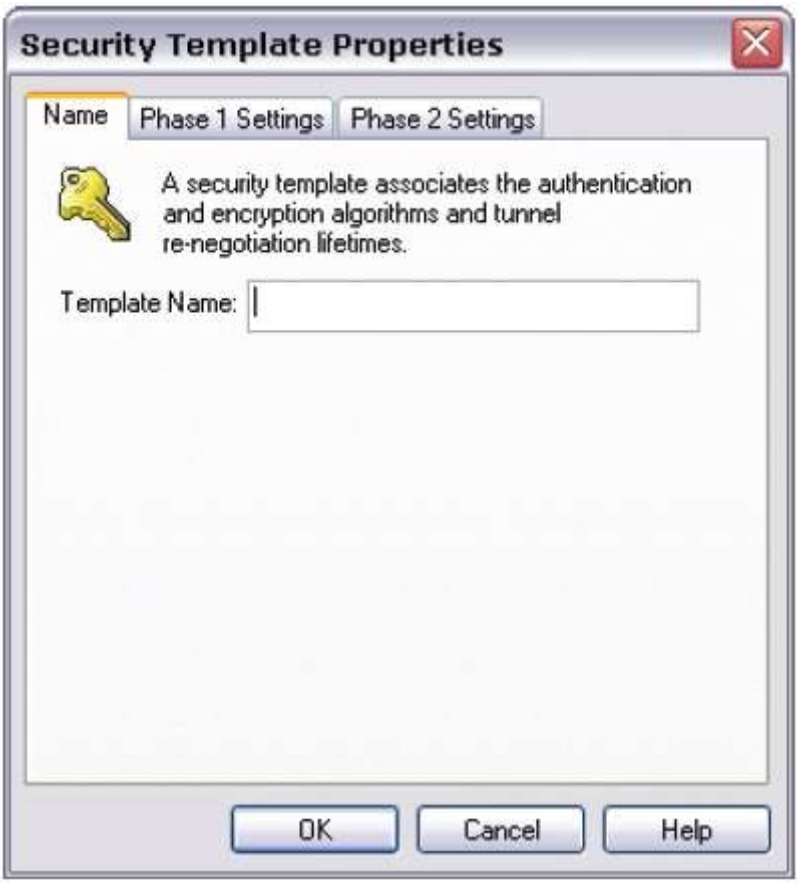
1. Выберите закладку **Traffic Management**
2. Выберите переключатель **Specify Custom Traffic Management Action**
3. Настройте параметры Traffic Management, как описано в “Добавление действия Traffic Management для политики BOVPN брандмауэра”

Создание шаблонов безопасности

Шаблон безопасности – это коллекция параметров, которую вы можете использовать при создании туннеля. При использовании Шаблонов Безопасности, вам не надо при каждом создании туннеля заново его настраивать. Эти шаблоны включают параметры Phase 1 и Phase 2

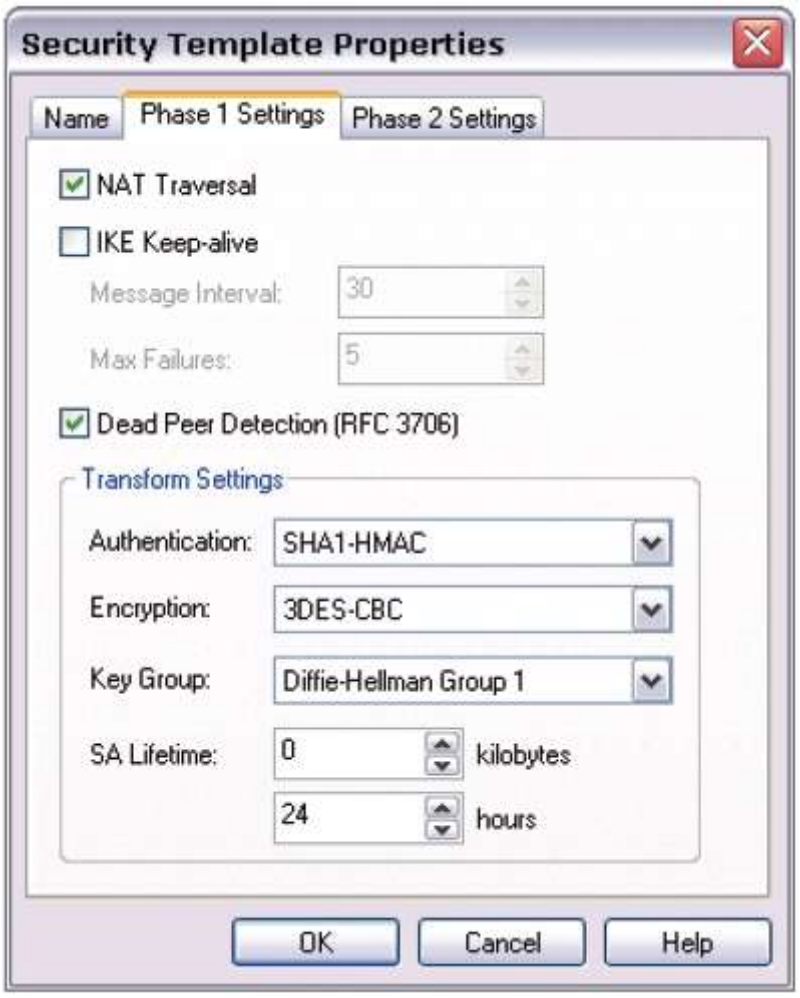
Для доступных типов шифрования используются предустановленные Шаблоны безопасности. При помощи этих параметров вы можете создавать защищенные туннели, которые будут корректно работать во всех сетях. Однако, если к вашей сети выдвигаются особые требования, вы можете изменить существующие шаблоны безопасности или создать новые. Для того чтобы создать шаблон безопасности выполните следующее:

1. В закладке **Device Management** выберите **Edit** > **Insert Security Template** или нажмите 
   Откроется диалоговое окно Security Template



2. В текстовом поле **Template Name** введите имя шаблона. Это имя будет отображаться в дереве Device Management и мастере Add VPN.

3. Выберите закладку **Phase 1 Settings**



4. Если вы хотите создать BOVPN туннель между Firebox и другим устройством, которое подключено к NAT устройству включите опцию **NAT Traversal**. NAT Traversal, или UDP Икапсуляция, позволяет трафику доходить до места назначения, когда у устройства нет публичного IP адреса.

5. Если другое конечное VPN устройство поддерживает Dead Peer Detection, то включите опцию **Dead Peer Detection**

6. Если оба устройства не поддерживают Dead Peer Detection, и если оба устройства – это устройства Firebox, включите опцию **IKE Keep-alive**.

   * В поле **Message Interval** укажите количество секунд

   * Для того чтобы установить максимальное количество раз, когда Firebox пытается отправить сообщение IKE keep-alive, перед тем как начать Phase 1 снова, введите необходимое количество в поле **Max failures**

   Не включайте опции IKE Keep-alive и Dead Peer Detection одновременно.

7. Из выпадающих списков **Authentication** и **Encryption** выберите методы аутентификации и шифрования.

8. Из выпадающего списка Key Group выберите группу Diffie-Hellman. Группа Diffie-Hellman определяет силу главного ключа, который использует в процессе обмена информацией о ключах. Чем выше номер группы, тем выше уровень безопасности, но тем больше времени требуется для генерации ключа. Для более подробной информации см. “Группы Diffie-Hellman”

9. Для того чтобы изменить период действия SA (security association) в поле **SA Life** введите время или объем трафика. Если вы введете ноль, то период действия SA будет бесконечным

10. Выберите закладку **Phase 2 Settings**

11. Из выпадающего списка **Authentication** выберите метод аутентификации для Phase 2.

12. В выпадающем списка Encryption выберите метод шифрования.

13. Для того установить дату истечения срока ключа, включите опцию Force key expiration и выберите необходимое количество килобайт или часов. Если опция **Force Key Expiration** отключена, или она включена и количество часов и килобайтов равны нулю, то Firebox будет пытаться использовать значение срока действия ключа, установленного для оконечного устройства. Если и эта опция отключена, то Firebox будет использовать срок действия ключа по умолчанию, равный 8 часам. Максимальный срок действия ключа равен 1 год.

14. Нажмите **OK**.

Создание управляемых туннелей между устройствами

Вы можете настроить туннель при помощи мастера Add VPN.

Перед тем как использовать эту процедуру необходимо, чтобы Динамические Firebox и Firebox® X Edge или SOHO имели настроенные сети. Вам также необходимо получить политики от любого нового динамического устройства перед тем как создавать «drag-and-drop» туннели (Для этого используйте процедуру **Ошибка! Источник ссылки не найден.**).

В закладке Device Management выполните следующее:

1. На одном конце туннеля нажмите на название устройства. Перетащите это название к названию устройства на другом конце туннеля.
   Запустится мастер **Add VPN**. Или в закладке Device Management выберите Edit > Create a new VPN или нажмите на иконку  .
   Запустится мастер Add VPN.

2. Если в п.1 вы использовали процедуру drag-and-drop, то мастер покажет две конечные точки туннеля и VPN ресурсы, которые используются туннелем. Если вы не использовали процедуру drag-and-drop выберите конечные устройства в выпадающем списке **Device**.

3. В выпадающем списке VPN Resource списка выберите VPN-ресурс для каждого устройства. Выберите **Hub Network** для того чтобы null-route VPN туннель передавал трафик через VPN. Используйте этот параметр в качестве VPN ресурса для устройства, которое содержит null-route VPN. Удаленное устройство затем будет отправлять весь трафик через VPN на устройство, который в качестве локального ресурса имеет **Hub Network**.

4. Нажмите **Next**.

5. Выберите необходимый шаблон безопасности. Для более подробной информации см. Add Security Templates . При помощи флагов выберите DNS и WINS серверы, которые вы хотите использовать. Нажмите Next.

6. Выберите шаблон политики VPN Firewall, который применим к типу трафика, который вы хотите разрешить через этот туннель. Если вы не создали ни одного шаблона политику VPN Firewall, для этого туннеля будет использовать политика **Any**

7. Нажмите **Next**.
   Мастер покажет вам конфигурацию.

8. Включите опцию **Restart devices now to download VPN configuration**. Нажмите **Finish** для того чтобы перезапустить устройства и создать VPN-туннель.

Изменение параметров туннеля

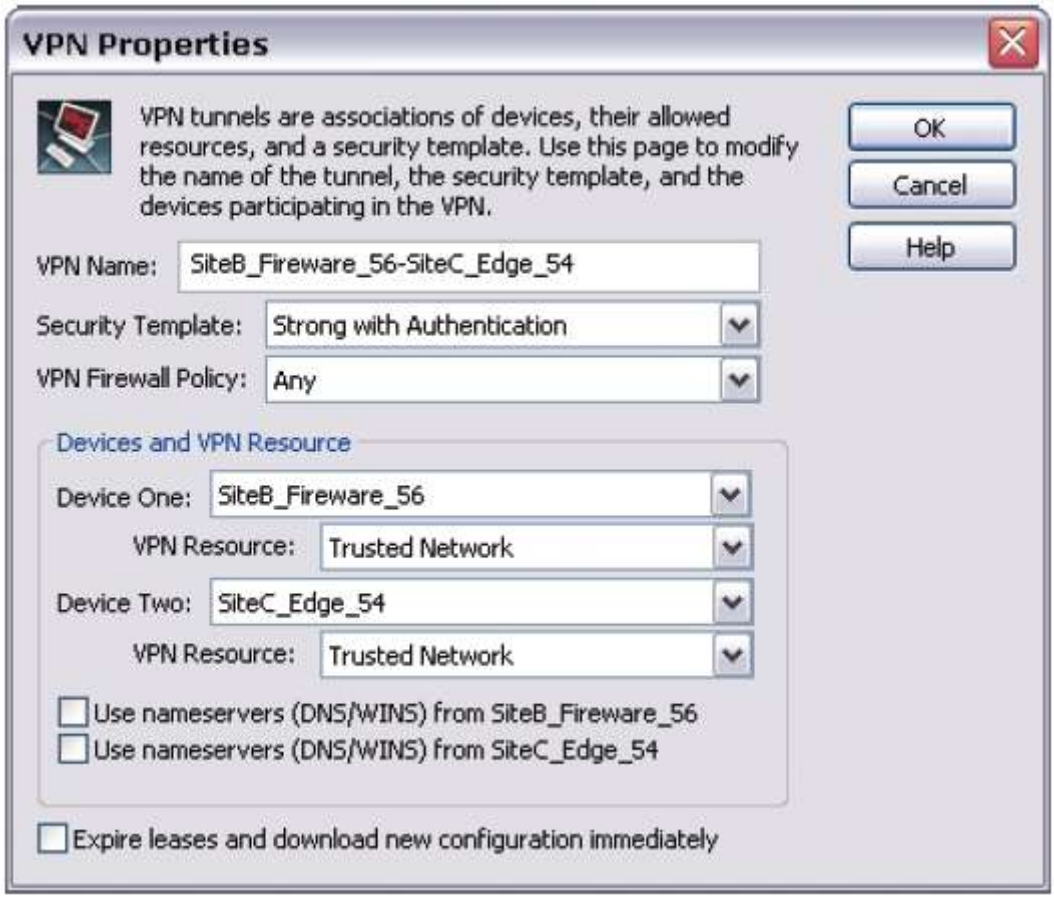
Вы можете видеть все ваши туннели в закладке Device Management WatchGuard® System Manager (WSM). WSM позволяет вам изменять название туннеля, шаблон безопасности, конечные точки и политику. Если вы хотите изменить шаблон политики или шаблон безопасности для туннеля, вы можете перетащить имя соответствующего шаблона из меню в левой части закладки Device Management на имя туннеля в меню. После этого новый шаблон будет применен. Для того чтобы изменить другие параметры туннеля выполните следующее:

1. В закладке **Device Management** откройте меню устройства.

2. Нажмите правой кнопкой на туннель, параметры которого вы хотите изменить, и выберите **Properties**.
   Откроется диалоговое окно VPN Properties

3. Выполните все необходимые изменения параметров туннеля.

4. Нажмите **OK** для того чтобы сохранить изменения.
   Изменения будут применены после следующего создания туннеля



Удаление туннелей и устройств

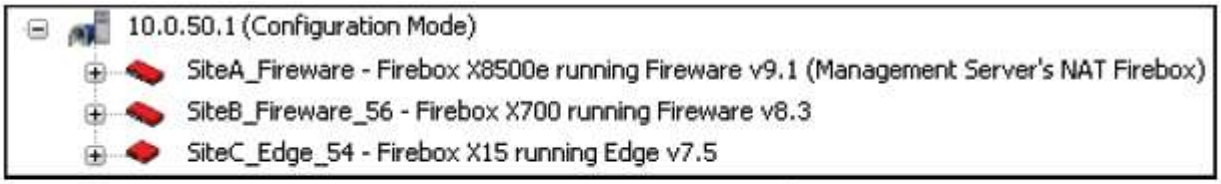
Для того чтобы удалить устройство из WatchGuard® System Manager (WSM), вам сначала необходимо удалить туннели, для которых это устройство является конечной точкой.

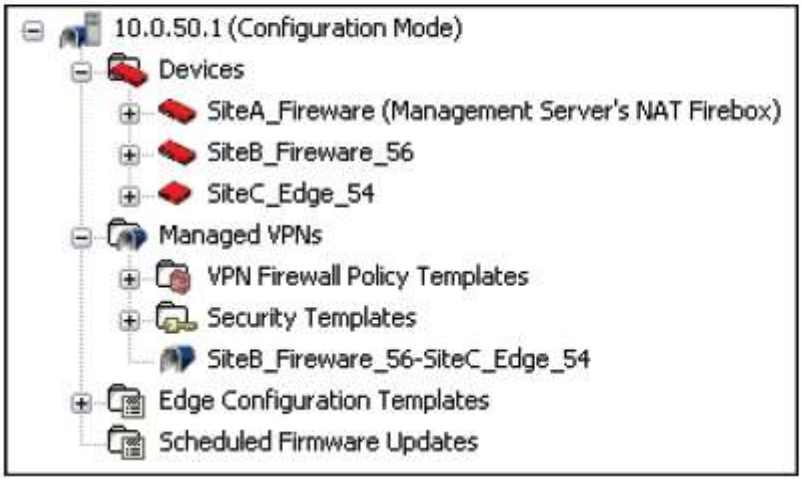
Удаление туннеля

1. В WSM выберите закладку **Device Management**
2. Откройте каталог **Managed VPNs** для того чтобы показать туннель, который вы хотите удалить.
3. Правой кнопкой нажмите на туннель
4. Выберите **Remove**. Нажмите Yes для подтверждения
5. После необходимо перезагрузить устройства, которые вы хотите удалить. Нажмите **Yes**.

Удаление устройства

1. В окне System Manager выберите закладку Device Status или Device Management. Откроется закладка Device Status (см. ниже рисунок слева) или закладка Device Management (см. ниже рисунок справа).





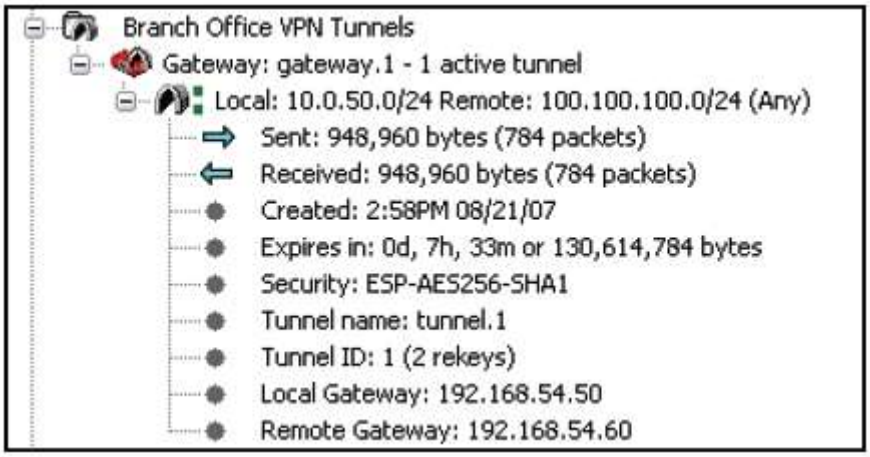
2. Если вы используете закладку Device Management, откройте каталог Devices.
3. Правой кнопкой нажмите на устройство.
4. Выберите Remove. Нажмите Yes.

Состояние VPN туннеля и сервисы безопасности

Передняя панель Firebox System Manager включает статистику по VPN туннелям.

Под секцией Firebox Status в правой части окна находится секция BOVPN туннелей.

Firebox System Manager отображает текущее состояние туннеля, информацию по шлюзу для каждого VPN туннеля, объем переданных и принятых данных, дата создания и информация об истечение сроков действия, тип аутентификации и шифрования, и количество повторных генераций ключей.



Каждый BOVPN туннель имеет три состояния:

Active

BOVPN туннель работает нормально и передает данные.

Inactive

BOVPN туннель создан, но не настроен. Через него не передается трафик.

Expired

BOVPN туннель был активным, но теперь не работает, так как через него не передается трафик или соединение между шлюзами потеряно. Эта информация также отображается в закладке **Device Status** системы WatchGuard System Manager.

Состояние Mobile VPN туннелей

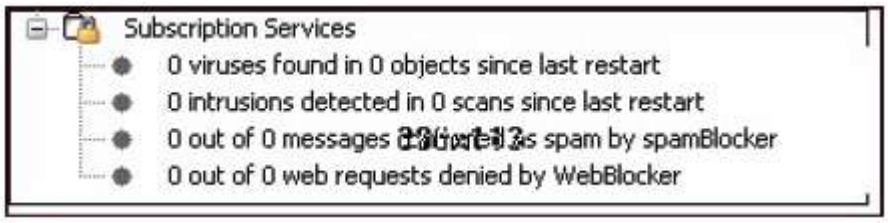
Firebox System Manager показывает имя пользователя, IP-адрес и количество отправленных/принятых пакетов для трех типов Mobile VPN туннелей:

- Mobile VPN with IPSec
- Mobile VPN with SSL
- Mobile VPN with PPTP

Для того чтобы отключить пользователей Mobile VPN нажмите правой кнопкой на пользователе и выберите **Logoff selected user**.

Состояние Сервисов Безопасности (Security Services)

В секции Security Services, Firebox System Manager показывает количество найденных вирусов, количество проникновений, количество спама и количество заблокированных web-запросов с момента последней перезагрузки.



Глава 26 - BOVPN туннели, созданные вручную

Что необходимо для создания VPN

Перед тем, как начать настройку BOVPN сети на вашем WatchGuard устройстве, изучите внимательно нижеприведенные требования:

- У вас должно быть два устройства WatchGuard, или одно WatchGuard устройство и устройство, которое поддерживает протокол IPSec. На обоих устройствах необходимо включить VPN.

- У вас должно быть подключение к Интернету.

- Интернет-провайдер (ISP) для каждого VPN устройства должен разрешить передачу IPSec трафика.

- Некоторые Интернет -провайдеры не разрешают создавать VPN туннели в своих сетях, без специального уведомления или оплаты. Поговорите со специалистами вашего Интернет-провайдера, чтобы они разрешили следующие порты и протоколы:

  * UDP порт 500 (IKE)

  * UDP порт 4500 (NAT traversal)

  * IP протокол 50 (ESP)

- Если на другом конце туннеля стоит управляемое WatchGuard устройство, то для создания VPN туннеля вы можете использовать опцию Managed VPN. Managed VPN значительно проще, чем Manual VPN. Для того чтобы использовать эту опцию, вам необходимо получить необходимую информацию от администратора, который занимается устройством на другом конце VPN туннеля.

- Вам необходимо знать, какой IP-адрес присвоен вашему External интерфейсу – статический или динамический

- Ваше WatchGuard устройство сообщит вам о максимальном количество туннелей, которое вы можете создать. Если вашу модель Firebox можно обновить, то вы можете приобрести обновление, которое увеличивает максимальное количество VPN туннелей.

- Если вы соединяете две сети Microsoft Windows NT, они должны быть в одном и том же домене Microsoft Windows, или они должны быть в доверенных доменах. Это ошибка в Microsoft Networking, а не ошибка Firebox.

- Если вы хотите использовать DNS и WINS серверы из сети на другом конце VPN туннеля, вам необходимо знать IP адреса этих серверов. Firebox может присвоить компьютерам, подключенным к Trusted сети, IP адреса серверов WINS и DNS если компьютеры получают свои IP адреса через DHCP.

- Если вы хотите компьютерам присвоить IP адреса WINS и DNS сервером на другом конце VPN, вы можете ввести эти адреса в настройках DHCP при настройке Trusted сети

- Вам необходимо знать адреса внутренних (Trusted) сетей, подключенных к вашему Firebox, и сетей, подключенных к другому VPN устройству, и их маски подсети

Внутренние IP адреса компьютеров, подключенных к вашему Firebox, не должны совпадать с IP адресами компютерами на другом конце VPN туннеля. Если компьютеры вашей Trusted сети используют такие же IP адреса, что и компьютеры в сети на другом конце VPN туннеля, то для избежания конфликта IP адресов вам необходимо изменить IP адреса в вашей или в сети на другом конце туннеля.

BOVPN туннели, созданные вручную

VPN (Virtual Private Network) создает защищенное подключение между географически разделенными компьютерами или сетями. Каждое отдельное подключение называется туннелем. Когда создается VPN туннель, то конечные точки туннеля должны аутентифицировать друг друга. Данные в туннеле передаются в зашифрованном виде. Только отправитель и получатель могут прочитать передаваемые данные.

BOVPN(Branch Office Virtual Private Networks) сеть позволяет организациям создать защищенные соедиения между географически разделенными офисами. Сетями или хостами в VPN туннеле могут главный офис, филиалы, удаленные пользователи или удаленный работник. Технология BOVPN позволяет организациям передавать конфиденциальные данные по зашифрованным каналам связи между офисами. Это позволяет упростить связь, снижает стоимость выделенных линий и обеспечивают необходимый уровень безопасности на каждом конце туннеля.

BOVPN туннели, созданные вручную предоставляют пользователям различные опции туннелирования. Другим типом туннеля является управляемый BOVPN туннель, которая представляет собой BOVPN туннель, который создается при помощи drag-and drop и шаблонов. Для более подробной информации см. “Управляемые BOVPN туннели”

Что необходимо для создания VPN

Вдобавок к требованиям VPN, для создания вручную VPN туннеля вам необходима следующая информация:

- Вам необходимо знать, является ли IP адрес, присвоенный другому VPN устройству, статическим или динамическим. Если VPN устройство на другом конце туннеля имеет динамический IP адрес, ваш Firebox должен искать это устройство по имени домена или использовать сервис Динамического DNS.

- Вам необходимо знать ключ шифрования данных в туннеле. Этот ключ должен использоваться на обоих устройствах туннеля.

- Вам необходимо знать метод шифрования данных, использующийся в туннеле (DES, 3DES, AES-128 bit или AES-192 bit или AES-256 bit). Устройства VPN на обоих концах туннеля должны использовать один и тот же метод.

- Вам необходимо знать метод аутентификации на каждом конце туннеля (MD5 или SHA-1). Устройства VPN на обоих концах туннеля должны использовать один и тот же метод аутентификации.

Мы рекомендуем записать всю необходимую информацию для обоих устройств. Для более подробной информации см. “Пример таблицы с адресами для VPN туннеля”.

Создание BOVPN туннеля вручную

Процедура создания туннеля вручную состоит из следующих этапов:

1. Настройка шлюзов—точек подключения на локальном и удаленном концах туннеля

2. Создание туннеля между шлюзами—настройка маршрутов для туннеля, настройка процедуры управления безопасносмтью и создание политики для туннеля. В следующиз разделах приведено описание остальных опций.

Пользовательские политики туннеля

Firebox автоматически добавляет новые VPN туннели к политикам BOVPN-Allow.in и BOVPN-Allow.out. Эти политики разрешают передачу всего трафика по туннелю. Вы можете не использовать эту политику и создать свою собственную политику VPN для того, чтобы разрешать только определенные типы политик в туннеле

Однонаправленные туннели

Если вы хотите туннель был открыт только в одну сторону, настройте динамическую NAT через BOVPN-туннель. Это может быть полезно, когда вы создаете туннель к удаленному сайту, где весь VPN трафик идет от одного публичного IP-адрес

VPN переключение

VPN туннели автоматически переключаются на резервный WAN интерфейс во время WAN переключения. Вы также можете настроить BOVPN туннели для переключения на резервную конечную точку туннеля, если основная точка выйдет из строя или будет недоступна. Для этого вам необходимо настроить хотя бы одну резервную конечную точку туннеля

Глобальные настройки VPN

Глобальные параметры VPN на вашем Firebox применяются ко всем ручным BOVPN туннелям, управляемым туннелям и Mobile VPN туннелям. Вы можете использовать эти параметры для:

- Включения опции IPSec pass-through.
- Управления пакетов с установленными битами ToS (Type of Service).
- Использования сервера LDAP для проверки сертификатов.

Настройки Firebox для отправки уведомления в случае выхода из строя туннеля BOVPN (только для BOVPN туннелей). Для того чтобы изменить эти параметры в Policy Manager выберите **VPN > VPN Settings**

Состояние BOVPN туннеля

Вы можете при помощи Firebox System Manager посмотреть текущее состояние BOVPN туннелей. Эта информация также отображается в закладке **Device Status** системы WatchGuard System Manager

Повторная генерация ключей для туннеля

При помощи Firebox System Manager вы можете мгновенно сгенерировать новую пару ключей для BOVPN туннелей вместо того, чтобы ждать истечения их срока действия

Пример таблицы с адресами для VPN туннеля

Элемент	Описание	Назначается
Внешний IP адрес	IP адрес IPSec устройства в нтернет Пример: Сайт A: 207.168.55.2	ISP

	Сайт B: 68.130.44.15	
Адрес локальной сети	Адрес локальной сети. Это IP компьютеров, которым ено передавать трафик через ь. Мы рекомендуем зовать адреса из известных онов: * 10.0.0.0/8—255.0.0.0 * 172.16.0.0/12—255.240.0.0 * 192.168.0.0/16—255.255.0.0 Номера после косых черт – это подсети. /24 – это маска подсети 5.255.0 Пример: Сайт A: 192.168.111.0/24 Сайт B: 192.168.222.0/24	Вами
Ключ шифрования (Shared Key)	Ключ шифрования – альный ключ, который зуется двумя IPSec устройства шифрования данных, аваемых по туннелю. Оба ства должны использовать один же пароль. В противном случае ование и расшифрование х будет работать некорректно. ь должен состоять из цифр, лов, букв нижнего и верхнего ра. Например лучше зовать пароль “Gu4c4mo!3” “guacamole” Пример: Сайт A: OurSharedSecret Сайт B: OurSharedSecret	Вами
Алгоритм шифрования	DES использует 56-битное вание. 3DES использует 168- шифрование. AES может зовать 128-битное, 192-битное и тное шифрование. Оба ства на концах туннеля должны зовать один и тот же метод вания Пример:	Вами

	Сайт A: 3DES; Сайт B: 3DES	
Аутентификация	Два устройства должны ›зовать один и тот же метод ификации Пример: Сайт A: MD5 (or SHA-1) Сайт B: MD5 (or SHA-1)	Вами

Настройка шлюзов

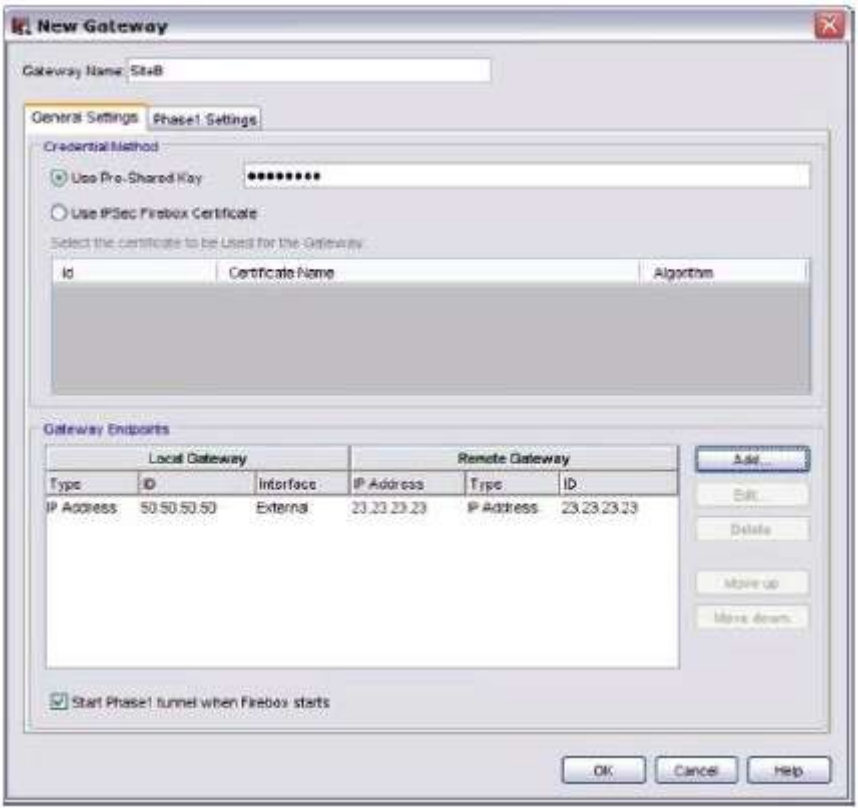
Шлюз – это точка подключения для одного или нескольких туннелей. Для того чтобы создать туннель, вам необходимо настроить шлюзы на локальном и удаленном устройствах. Для того чтобы настроить шлюзы, вам необходимо указать следующее:

- Данные доступа — ключи и сертификат IPSec. Для более подробной информации об использовании сертификатов для BOVPN аутентификации, см. “Использование сертификата для аутентификации BOVPN туннеля”
- Местоположение конечных точек локального и удаленного шлюзов (IP-адрес или информация о домене)
- Настройки Phase 1 процедуры IKE(Internet Key Exchange). Во время этой фазы создается SA (Security Association) — протоколы и настройки, которые будут использовать конечными точками шлюзов для обмена данными — для защиты данных, которые передаются во время этапа согласования параметров безопасности.

Для того чтобы настроить шлюзы для ваших конечных устройств, выполните следующее:

1. В Policy Manager выберите **VPN > Branch Office Gateways**.
   Откроется диалоговое окно Gateways.

2. Для того чтобы добавить новый шлюз нажмите **Add**.
   Откроется диалоговое окно New Gateway



3. В поле **Gateway Name** введите имя, которое будет использоваться для идентификации шлюза в конфигурации Firebox.

4. Теперь вы можете настроить данные доступа или шлюзы.

Отключение автоматического запуска туннеля для шлюза

BOVPN туннели автоматически создаются каждый раз при включении устройства WatchGuard. Вы можете изменить это, например в случае если процедуру создания туннеля должно инициировать устройство на другом конце туннеля. Для того чтобы отключить автоматическое создание туннелей для этого шлюза, отключите опцию **Start Phase1 tunnel when Firebox starts**.

Редактирование и удаление шлюзов

Для того чтобы изменить настройки шлюза выберите **VPN > Branch Office Gateways**. Или нажмите правой кнопкой на иконку туннеля в закладке **BOVPN** утилиты Policy Manager, и выберите **Gateway Property**.

1. Выберите шлюз, настройки которого вы хотите изменить, и нажмите **Edit**.
   Откроется диалоговое окно Edit Gateway.

2. Выполните необходимые изменения и нажмите **OK**. Для того чтобы удалить шлюз, выберите его и нажмите **Remove**. Вы также можете выбрать несколько шлюзов и нажать **Remove** для того чтобы удалить их всех.

Настройка данных доступа

В диалоговом окне **New Gateway** выберите **Use Pre-Shared Key** или **Use IPSec Firebox Certificate** для того чтобы выбрать процедуру аутентификации, которая будет использоваться в туннеле.

Если вы выбрали Use Pre-Shared Key

Введите или вставьте ключ шифрования. Устройства на обоих концах туннеля должны использовать один и тот же ключ шифрования. Ключ шифрования должен состоять только из ASCII символов.

Если вы выбрали Use IPSec Firebox Certificate

В таблице под переключателем вы можете посмотреть список сертификатов, установленных на устройстве Firebox. Выберите необходимый сертификат. Для более подробной информации см. “Использование сертификата для аутентификации BOVPN туннеля”

Настройка конечных точек шлюза

Конечные точки шлюза – это локальный и удаленный шлюз, которые соединены BOVPN туннелем. Эта информация используется вашим WatchGuard устройством для обмена информацией с устройством на другом конце туннеля при создании BOVPN туннеля. Также эта информация используется для идентификации устройства WatchGuard на другом конце туннеля.

Любой External интерфейс может быть конечной точкой шлюза. Если у вас есть несколько External интерфейсов, то вы можете настроить несколько конечных точек шлюза

Локальный шлюз

В разделе Local Gateway вы можете настроить ID шлюза и интерфейс, к которому подключается BOVPN туннель. В качестве ID шлюза вы можете использовать статический IP адрес. Для этого выберите опцию **By IP Address**. Выберите опцию **By Domain Information** если у вас есть домен, соответствующий IP адресу, к которому подключается BOVPN туннель.

1. В разделе **Gateway Endpoints** диалогового окна **New Gateway** нажмите **Add**.
   Откроется диалоговое окно New Gateway Endpoints Settings

2. Укажите ID шлюза.

   By IP address— Выберите переключатель **By IP Address**. Введите IP адрес интерфейса устройства Firebox или выберите его из выпадающего списка, который содержит все настроенные интерфейсы устройства.

   By Domain Information—Выберите переключатель **By Domain Information**. Нажмите **Configure** и выберите метод конфигурации домена. Выберите **By Domain Name** или **By User ID on Domain**.

   By Domain Name—Введите имя вашего домена и нажмите **OK**.

   By User ID on Domain—Введите имя пользователя и имя домена в формате *UserName@DomainName* и нажмите **OK**.

3. В выпадающем списке **External Interface** выберите интерфейс Firebox, IP адрес или имя домена которого вы выбрали в качестве ID шлюза.

Удаленный шлюз

В разделе Remote Gateway вы можете настроить IP адрес шлюза и его ID для удаленного шлюза. IP адрес шлюза может быть статическим (**Static IP address**) или динамическим (**Dynamic IP address**). ID шлюза может быть именем домена (**By Domain Name**)**,** ID пользователя в домене (**By User ID on Domain)** или x500 именем (**By x500 Name**). Администратор удаленного шлюза сообщит вам всю необходимую информацию.

1. Выберите IP адрес удаленного шлюза.

* **Static IP address**—Выберите опцию если удаленное устройство имеет статический IP адрес. Введите IP адрес или выберите его из выпадающего списка.

* **Dynamic IP address**—Выберите эту опцию, если удаленное устройство имеет динамический IP адрес.

2. Выберите ID шлюза.

   By IP address—Выберите переключатель **By IP Address**. Введите IP адрес или выберите его из выпадающего списка.

   By Domain Information— Выберите переключатель **By Domain Information**. Нажмите **Configure** и выберите метод конфигурации домена**.** Выберите **By Domain Name** или **By User ID on Domain** или **By x500 Name** и введите имя пользователя, ID пользователя и домен, или x500 имя. Нажмите **OK**.

*Если удаленная конечная точка VPN туннеля использует DHCP или PPPoE для получения внешнего IP-адреса, то в качестве типа идентификатора удаленного шлюза используйте значение поля **Domain Name**. В качестве имени участника используйте полное имя домена удаленной VPN точки. Firebox использует IP-адрес и имя домена для поиска VPN точки. Убедитесь, что DNS-сервер, который используется Firebox, сможет идентифицировать имя.*

Нажмите **OK** для того чтобы закрыть диалоговое окно **New Gateway Endpoints Settings**. Откроется диалоговое окно New Gateway. Пара созданных вами шлюзов появится в списке шлюзов. Если вы хотите использовать параметры Phase 1 то см. “Настройка режима и преобразований (Параметры Phase 1)”. В противном случае нажмите OK.

Настройка режима и преобразований (Параметры Phase 1)

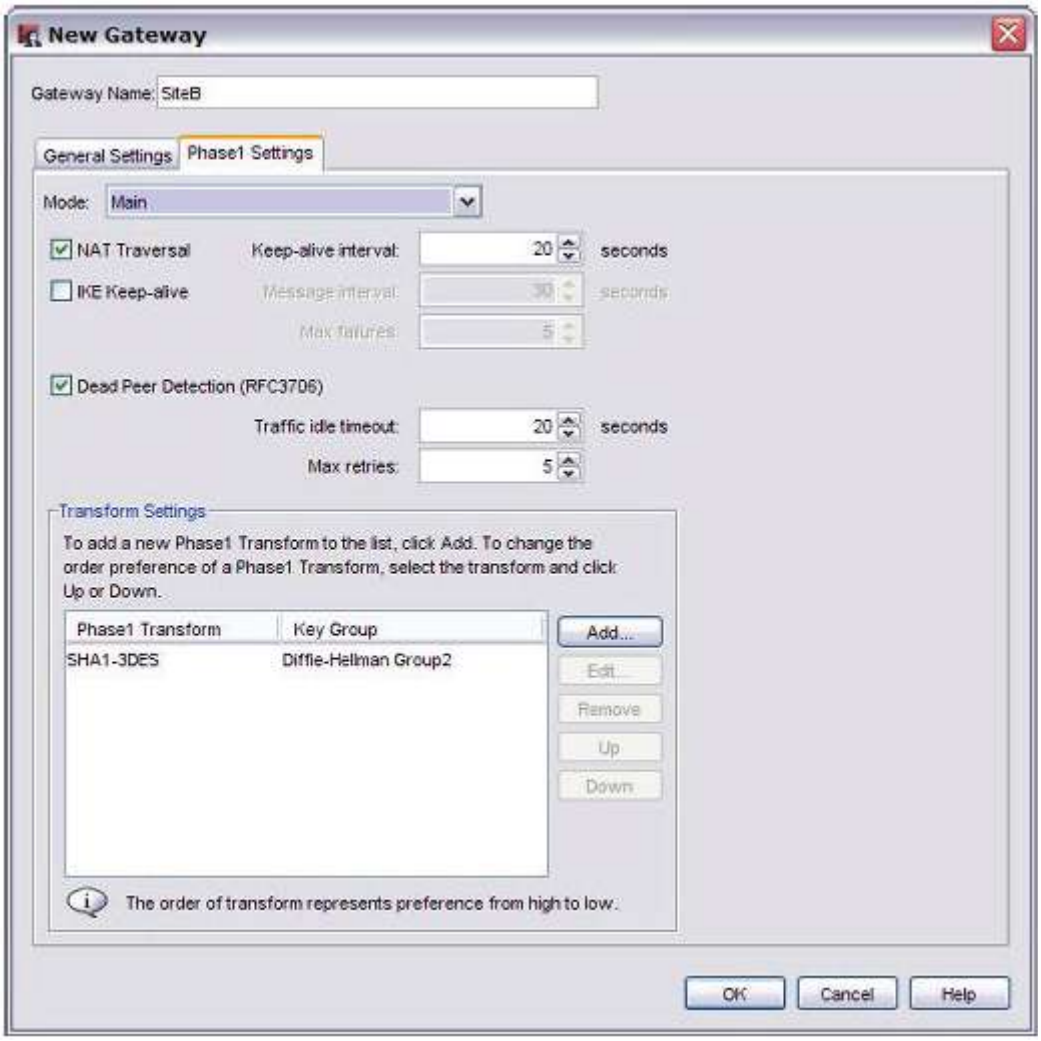
Phase 1 IPSec соединения – это фаза создания защищенного, аутентифицированного канала связи. Этот канал связи называется ISAKMP Security Association (SA).

Обмен данными во время Phase 1 может идти в двух режимах: Основной режим (*Main Mode)* или Агрессивный режим (*Aggressive Mode)*. Режим определяет тип и количество сообщений, которым обмениваются устройства во время этой фазы.

Преобразование – это набор протоколов и алгоритмов безопасности, которые используются для защиты передаваемых данных. Во время согласования IKE конечные точки туннеля «договариваются» об использовании определенного преобразования.

Вы можете настроить туннель таким образом, чтобы при создании туннеля вы могли выбрать несколько преобразований. Для более подробной информации см. “Добавление преобразования Phase 1”

1. В диалоговом окне **New Gateway** выберите закладку **Phase1 Settings**



2. В выпадающем списке **Mode** выберите **Main**, **Aggressive** или **Main fallback to Aggressive**.

   Main Mode

   Более безопасный; Использует 6 сообщений. В первых двух стороны договариваются о политике; в следующих двух обмениваются данными Diffie-Hellman, и последние два для аутентификации обмена Diffie-Hellman. Основной режим поддерживает следующие группы Diffie-Hellman: 1, 2 и 5. Этот режим также позволяет вам использовать несколько преобразований, как описано в “Добавление преобразования Phase 1”

   Aggressive Mode

   Более быстрый, так как использует только три сообщения, которые используются для обмена данными Diffie-Hellman и идентификации двух конечных точек VPN-туннеля. Менее безопасен.

   Main fallback to aggressive

   Firebox осуществляет обмен Phase 1 в режиме Main Mode. Если согласование будет неудачным, он будет использовать Агрессивный Режим

3. Если вы хотите создать BOVPN туннель между Firebox и другим устройством, который находится за устройством NAT, включите опцию NAT Traversal. NAT Traversal, или UDP Encapsulation, позволяет трафику попадать в правильные места назначения.

4. Для того чтобы Firebox отправляла сообщения своему IKE-пользователю для того, чтобы туннель был открытым, включите опцию **IKE Keepalive**. Для того установить значение параметра **Message Interval**, введите количество секунд

IKE Keep-alive используется только устройствами WatchGuard. Не включайте эту опцию, если устройство на другом конце туннеля это IPSec устройство другого производителя или WatchGuard устройство, которое поддерживает Dead Peer Detection.

5. Для того чтобы установить максимальное количество попыток устройства Firebox отправить IKE keep-alive сообщение, перед тем оно попытается повторить Фазу 1, в поле **Max failures** введите необходимое значение.

6. Опция **Dead Peer Detection** используется для включения/отключения процедуры обнаружения неактивного участника. Если вы включите эту процедуру, Firebox будет отправлять запрос участнику, если в течение определенного промежутка времени от участника не поступал трафик. Процедура обнаружения неактивного IPSec участника более масштабируем, чем сообщения IKE keep-alive. В поле **Traffic idle timeout** укажите количество секунд, по истечение которых участнику будет отправлен запрос. В поле **Max retries** введите количество запросов для участника после чего он будет считаться неактивным. Dead Peer Detection это промышленный стандарт, который используется большинством IPSec устройств. Если устройства на обоих концах туннеля поддерживают технологию Dead Peer Detection, то мы вам рекомендуем ее использовать на обоих устройствах.

   Если вы настроили VPN переключение, вам необходимо включить DPD. Для более подробной информации см. “Configure VPN Failover” on page 785.

7. Firebox содержит один набор преобразований, который отображается в списке **Transform Settings**. Параметры преобразования: SHA1 аутентификация, 3DES шифрования и группа Diffie-Hellman 1. Вы также можете выполнить следующее:

   * Использовать эти параметры по умолчанию

   * Удалить эти параметры и создать новые

   * Создать дополнительные параметры, как описано в “Добавление преобразования Phase 1”

Добавление преобразования Phase 1

Вы можете создать туннель, которые позволяет участникам использовать несколько преобразований. Например, одно преобразование может использовать SHA1-DES-DF1 ([метод_аутентификации]-[метод_шифрования]-[группа_ключей]) и второе преобразование использует MD5-3DES-DF2. Приоритет SHA1-DES-DF1 выше, чем у MD5-3DES-DF2. Когда трафик передается по туннелю, SA может использовать, как SHA1- DES-DF1 (первый приоритет) или MD5-3DES-DF2 (второй приоритет) в зависимости от преобразований, которые совпадают с преобразованиями участников

Вы можете использовать максимум 9 преобразований. Для того чтобы использовать несколько преобразований, в п. 2 вам необходимо выбрать Основной Режим.

1. В закладке **Phase 1 Settings** диалогового окна **New Gateway** найдите секцию **Transform Settings** в его нижней части. Нажмите **Add**.
   Откроется диалоговое окно Phase1 Transform

2. В выпадающем списке **Authentication** выберите метод аутентификации: **SHA1** или **MD5**.

3. В выпадающем списке **Encryption** выберите метод шифрования: **AES (128-bit**), **AES (192-bit)**, **AES (256-bit)**, **DES**, or **3DES**

4. Для того чтобы изменить время жизни SA (Security Association) в поле **SA Life** введите количество часов (**Hour** в выпадающем списке) или минут (**Minute** в выпадающем списке).

5. В выпадающем списке **Key Group** выберите группу Diffie-Hellman. Fireware XTM поддерживает группы 1, 2 и 5. Группы Diffie-Hellman определяют «силу» ключа шифрования, который используется в процедуре обмена ключами. Чем выше номер группы, тем выше уровень безопасности и больше времени необходимо для генерации ключей

6. Вы можете добавить максимум 9 преобразований. Вы можете выбрать преобразование и при помощи кнопок **Up** или **Down** изменить приоритет этого преобразования в списке

7. Нажмите **OK**.

Если ваш Firebox подключено к NAT устройству

Firebox может использовать NAT Traversal, что позволяет вам создавать VPN туннели в случае если ваш ISP использует NAT (Network Address Translation) или External интерфейс вашего Firebox подключен к NAT устройству. Мы рекомендуем чтобы External интерфейсу устройства Firebox был присвоен публичный IP адрес. В противном случае см. следующие разделы.

NAT устройства обычно имеют некоторые базовые функции брандмауэра. Для того чтобы создать VPN туннель к устройству Firebox, вам необходимо чтобы NAT устройство пропускало трафик к Firebox. На NAT устройстве необходимо открыть следующие порты и протоколы:

- UDP порт 500 (IKE)
- UDP порт 4500 (NAT Traversal)
- IP протокол 50 (ESP)

Для более подробной информации см. документацию по вашему устройству NAT. Если External интерфейс вашего Firebox имеет внутренний IP адрес, то в качестве локального ID в настройках Phase 1 вы не можете использовать этот IP адрес.

- Если NAT устройство, к которому подключено устройство Firebox, имеет динамический публичный IP адрес:

    - Сначала выберите режим работы устройства – режим моста. В этом режиме устройство Firebox получает публичный IP адрес на External интерфейсе. Для более подробной информации см. документацию по вашему NAT устройству.

    - Настройте сервис Динамического DNS на устройстве Firebox. В настройках Phase 1 Manual VPN, в качестве локального ID выберите **Domain Name**. В качестве Local ID введите имя домена DynDNS. Удаленное устройство должно идентифицировать ваш Firebox по имени домена и использовать имя домена DynDNS, которое соответствует имени домена, которое соответствует устройству Firebox в настройках Phase 1.

- Если NAT устройство, к которому подключен Firebox, имеет статический публичный IP адрес:

    - В настройках Phase 1 Manual VPN в качестве Local ID из выпадающего списка выберите **Domain Name**. В качестве Local ID введите публичный IP адрес внешнего интерфейса NAT устройства. Удаленное устройство должно идентифицировать ваш Firebox по имени домена и должно использовать такой же публичный IP адрес в качестве имени домена в его настройках Phase 1.

Группы Diffie-Hellman

Группы Diffie-Hellman (DH) определяют «силу» ключа, который используется в процедуре обмена ключами. Чем выше номер группы, тем выше уровень безопасности и больше времени необходимо для генерации ключей.

WatchGuard устройства поддерживают группы Diffie-Hellman 1, 2 и 5:

- DH Group 1: 768-bit group
- DH Group 2: 1024-bit group
- DH Group 5: 1536-bit group

Оба устройства при обмене ключами должны использовать одну и ту же группу DH, которая устанавливается во время Phase 1. При создании ручного BOVPN туннеля, вам необходимо в качестве параметров Phase 1 указать группу Diffie-Hellman. Во время Phase 1 устройства создают защищенный, аутентифицированный канал связи.

DH группы и Perfect Forward Secrecy (PFS)

Вдобавок к Phase 1 вы можете указать группу Diffie-Hellman в настройках Phase 2 IPSec соединения. Конфигурация Phase 2 включает настройка параметров SA. Настроить группу Diffie-Hellman для Phase 2 вы можете только при включенной опции Perfect Forward Secrecy (PFS).

PFS обеспечивает более высокий уровень защиты ключей, так как новые ключи не создаются на основе предыдущих. Если ключ был скомпрометирован, новые сеансовые ключи также хорошо защищены. Если вы включите PFS в настройках Phase 2 обмен по Diffie-Hellman происходит каждый раз, когда оба устройства создают новую SA.

Группа DH для Phase 2 не должна совпадать с группой для Phase 1.

Выбор группы Diffie-Hellman

По умолчанию для Phase 1 и Phase 2 используется группа Diffie-Hellman номер 1. Эта группа обеспечивает базовый уровень безопасности и достаточно неплохую производительность. Если скорость инициализации туннеля и повторной генерации ключей для вам не играет важной роли, используйте Group 2 или Group 5. Реальная скорость инициализации и повторной генерации ключей зависит от целого ряда факторов.

Анализ производительности

В таблице приведены данные, полученные приложением, которое генерирует 2000 значений Diffie-Hellman. These figures are for a 1.7GHz Intel Pentium 4 CPU.

DH группа	Количество пар ключей	Необходимое время	Время на генерацию каждой пары ключей
Группа 1	2000	43 секунды	21 мс
Группа 2	2000	84 секунды	42 мс
Группа 5	2000	246 секунд	123 мс

Создание туннелей между конечными точками шлюза

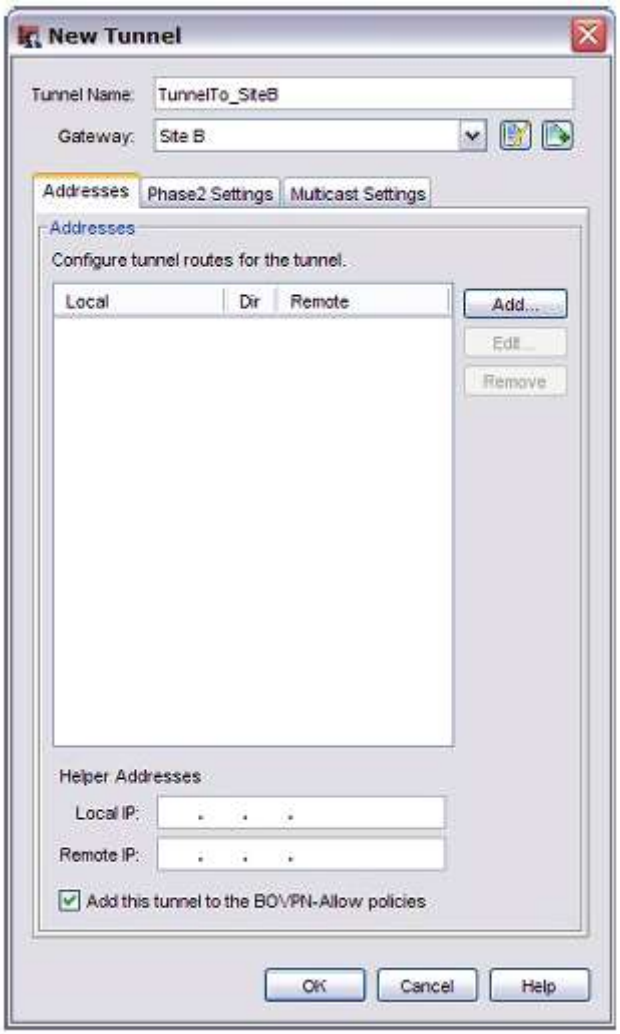
После того, как вы настроите точки шлюза, вы можете между ними создать туннель. Для того чтобы создать туннель, вам необходимо выполнить следующее:

- Создать туннель
- Настроить параметры Phase 2 для IKE. Во время этой фазы создаются ассоциации безопасности (SA) для шифрования пакетов данных.

Создание туннеля

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.
   Откроется диалоговое окно Branch Office IPSec Tunnels

2. Нажмите **Add**.
   Откроется диалоговое окно New Tunnel



3. В поле **Tunnel Name** введите уникальное имя туннеля (Это имя должно быть уникальным среди имен туннелей, имен групп Mobile VPN и интерфейсов.

4. В списке **Gateway** выберите шлюз для туннеля. Если вы хотите изменить параметры уже существующего шлюза, выберите его и нажмите  . Выполните все процедуры, описание которых см. в “Настройка шлюзов”. Если вы хотите добавить новый шлюз нажмите  . Выполните все процедуры, описание которых см. в “Настройка шлюзов”

5. Включите опцию **Add this tunnel to the BOVPN-Allow policies** если вы хотите добавить туннель в политики BOVPN-Allow.in и BOVPN-Allow.out. Эти политики разрешают весь трафик, маршрут которого совпадает с маршрутами туннеля. Если вы хотите запретить передачу трафика по туннелю, отключите эту опцию и при помощи мастера BOVPN Policy создайте свои политики, которые будут разрешать передачу определенного типа трафика по туннелю.

Теперь вы можете добавить маршруты к туннелю, настроить параметры Phase 2 или настроить параметры Multicast

Редактирование и удаление туннеля

Для того чтобы изменить параметры туннеля выберите **VPN > Branch Office Tunnels**. Или нажмите правой кнопкой на иконку туннеля в закладке **Branch Office VPN** утилиты Policy Manager и выберите **Tunnel Property**.

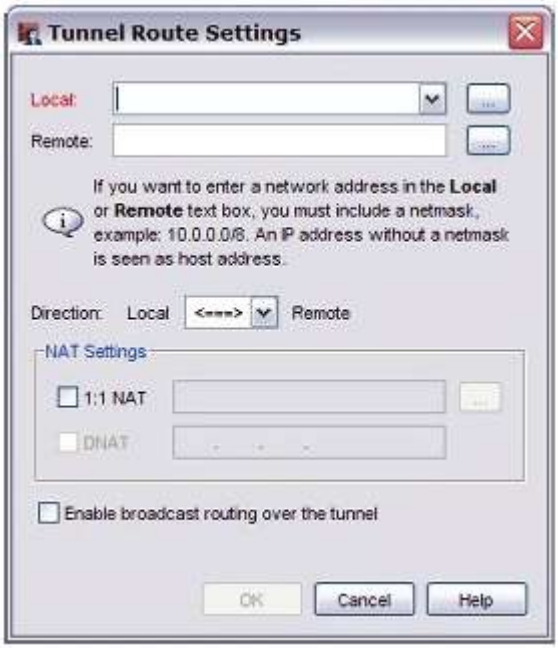
1. Выберите туннель и нажмите **Edit**.
   Откроется диалоговое окно Edit Tunnel.

2. Выполните все необходимые изменения и нажмите **OK**.

Для того чтобы удалить туннель в диалоговом окне **Branch Office IPSec Tunnels** выберите туннель, который вы хотите удалить, и нажмите **Remove**. Вы также можете удалить несколько туннелей сразу.

Создание маршрутов для туннеля

1. В закладке **Addresses** диалогового окна **New Tunnel** нажмите **Add**.
   Откроется диалоговое окно Tunnel Route Settings



2. В выпадающем списке **Local** выберите необходимый локальный адрес. Вы также можете нажать на кнопку рядом с выпадающим списком **Local** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя.

3. В поле **Remote** введите адрес удаленной сети. Вы также можете нажать на кнопку рядом с полем **Remote** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя.

4. В выпадающем списке **Direction** выберите направление для туннеля. Направление определяет, какая конечная точка начнет первой передачу данных по VPN туннелю.

5. Если типы адресов и направление туннеля совместимы вы можете включить 1-to-1 NAT и динамическую NAT для туннеля. Для более подробной информации см.”Настройка исходящей динамической NAT через BOVPN туннель” и “1-to-1 NAT через BOVPN туннель”

6. Нажмите **OK**.

Настройка параметров Phase 2

Параметры Phase 2 включают параметры SA, которая определяет способ защиты пакетов, передаваемых по туннелю. SA хранит всю необходимую информацию, которую Firebox использует для обработки трафика, передаваемого по защищенному туннелю. Параметры SA могут включать:

- Алгоритмы шифрования и аутентификации.

- Время жизни SA (в секундах или в количестве байт, или одновременно в обоих).

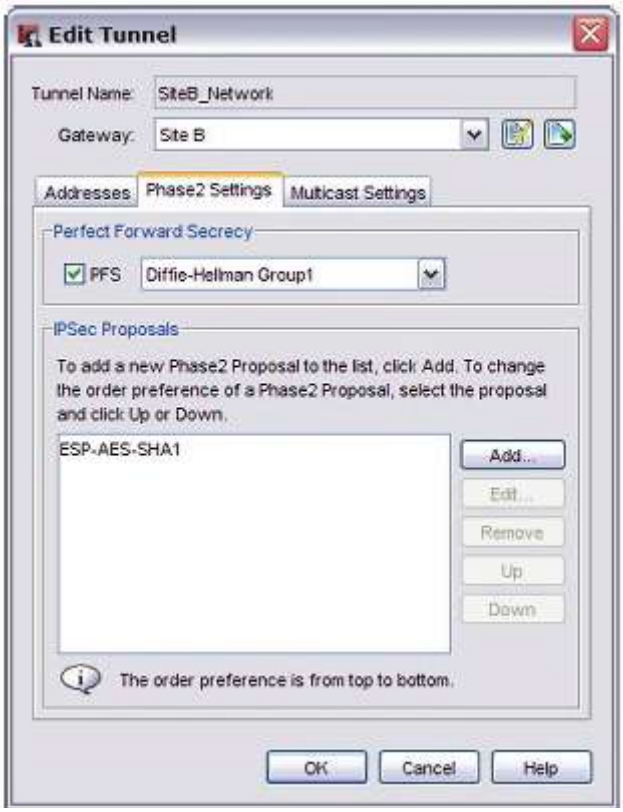
- IP адрес устройства, для которого была создана SA (устройство, выполняющее IPSec шифрования и расшифрование на другом конце VPN туннеля. Этим устройство не может быть компьютер, который передает или получает трафик).

- IP адреса источника и назначения трафика, для которого была создана SA.

- Направление трафик, к которому применяется SA (Для каждого направления передачи трафика создается по одной SA – для исходящего и входящего).

Для того чтобы настроить параметры Phase 2 выполните следующее:

1. В диалоговом окне **New Tunnel** выберите закладку **Phase2 Settings**



2. Включите опцию **PFS** если вы хотите включить Perfect Forward Secrecy (PFS). Если вы включите использование PFS выберите группу Diffie-Hellman. Perfect Forward Secrecy обеспечивает более высокий уровень защиты ключей, которые создаются во время установления соединения. Ключи, созданные с использованием PFS, не создаются на основе предыдущих ключей. Если предыдущий сеансовый был скомпрометирован, то ваш не стоит волноваться по поводу компрометации новых ключей

3. Firebox содержит одно предложение по умолчанию в списке **IPSec Proposals**. Предложение (Proposal) содержит алгоритм ESP для защиты данных, AES шифрование и SHA-1 аутентификацию. Вы можете сделать следующее:

   * Использовать предложение по умолчанию

   * Удалить предложение по умолчанию и создать новое

   * Создать новое предложение

   В закладке Phase 2 Settings вы можете создать несколько предложений Phase 2. Однако к одной и той же конфигурации Phase 2 вы не можете добавить AH и ESP предложения.

   Если вы планируете использовать IPSec pass-through, вам необходимо создать ESP

предложение, так как IPSec pass-through поддерживает только ESP. Для более подробной информации об IPSec pass-through см. “Глобальные параметры VPN”

Создание Phase 2 предложения

Вы можете создать несколько Phase 2 предложений для одного туннеля. Например, вы можете создать два предложения: одно с параметрами ESP-3DES-SHA1 и второе с параметрами ESP-DES-MD5. При передаче трафика по туннелю, SA может использовать или ESP-3DES-SHA1 или ESP-DES-MD5.

Вы можете создать максимум девять предложений.

Для того чтобы создать новое предложение выберите закладку **Phase 2 Settings** в диалоговых окнах **New Tunnel** или **Edit Tunnel** и в разделе **IPSec Proposals** нажмите на кнопку **Add**

Создание существующего предложения

Вы можете выбрать одно из шести предопределенных предложений. Название предложений имеют следующий формат: <Тип>-<Метод_Аутентификации>-<Метод_Шифрования>. Для всех шести предложений Force Key Expiration равен 8 часам или 128000 килобайт.

Для того чтобы использовать одно из шести предопределенных предложений выполните следующее:

1. Выберите **Use an existing Phase 2 proposal**.

2. В выпадающем списке выберите необходимое предложение и нажмите **OK**.

Создание нового предложения

1. В диалоговом окне **New Phase2 Proposal** включите опцию **Create a new Phase 2 proposal**. Или в Policy Manager выберите **VPN > Phase2 Proposals**. Откроется диалоговое окно **Phase2 Proposals**. Нажмите **Add**.

2. В поле **Name** введите имя нового предложения. Если вы открыли диалоговое окно из **VPN > Phase 2 Proposals**, то появится дополнительное поле **Description**. В поле **Description** введите описание предложения (дополнительно)

3. В выпадающем списке **Type** выберите метод предложения: **ESP** или **AH**. Мы рекомендуем использовать ESP (Encapsulating Security Payload). Основные отличия между ESP и AH (Authentication Header):

   * ESP использует аутентификацию с шифрованием.

   * AH использует только аутентификацию. ESP аутентификация, в отличие от AH, не включает защиту IP заголовка.

   * IPSec pass-through поддерживает только ESP. Если вы хотите использовать IPSec pass-though вам в качестве метода предложения необходимо использовать ESP. Для более подробной информации об IPSec pass-through см. “Глобальные параметры VPN”

4. В выпадающем списке **Authentication** выберите алгоритм аутентификации: **SHA1**, **MD5** или **None**.

5. (Если вы выбрали **ESP** в выпадающем списке **Type**) В выпадающем списке **Encryption** выберите алгоритм шифрования: DES, 3DES и AES 128, 192, or 256 bit

6. Для того чтобы конечные точки туннеля инициировали процедуру генерации новых ключей через определенный промежуток времени, включите опцию **Force Key Expiration** в соответствующем поле введите время и количество байт, по истечении которых будет инициирована процедура генерации нового ключа. Если опция **Force Key Expiration** отключена, или она включена и значения времени и количество килобайтов равны нулю, Firebox попытается использовать срок действия ключа, установленный для устройства. Если и этот параметр отключен или равен нулю, то Firebox будет использовать установленный по умолчанию временной промежуток равный 8 часам. Максимальный срок действия ключ – 1 год.

7. Нажмите **OK**.

Редактирование или создание предложения на базе существующего (клонирование)

При создании предложение на базе существующего предложения (клонирование) вы копируете существующее предложение и сохраняете его под новым именем. Вам необходимо будет это сделать, если вы хотите редактировать предопределенные предложения.

1. В Policy Manager выберите **VPN > Phase2 Proposals**.
   Откроется диалоговое окно Phase2 Proposals.

2. Выберите предложение и нажмите **Edit** или **Clone**.

3. Выполните все необходимые изменения, как описано в разделе **Create a new proposal**. Нажмите **OK**.

Редактирование предложения

Редактировать вы можете только предложения, созданные пользователями.

1. В Fireware XTM Web UI выберите **VPN > BOVPN**

2. В разделе **Phase 2 Proposals** выберите предложение и нажмите **Edit**.

3. Выполните все необходимые изменения, как описано в разделе **Create a new proposal**.

Изменение порядка следования туннелей

Порядок следования туннелей в списке крайне важен, когда несколько туннелей используют один и тот же маршрут или когда маршруты перекрывают друг друга. Туннель, который находится выше по списку в диалоговом окне **Branch Office IPSec Tunnels** будет иметь более высокий приоритет в случае если трафик будет соответствовать маршруту нескольких туннелей.

Для того чтобы изменить порядок следования туннелей в списке выполните следующее:

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.
   Откроется диалоговое окно Branch Office IPSec Tunnels.

2. Выберите туннель и при помощи кнопок **Move Up** или **Move Down** переместите его в необходимую позицию.

Глобальные параметры VPN

Вы можете настроить глобальные параметры, которые будут использоваться для ручных BOVPN туннелей, управляемых BOVPN и Mobile VPN with IPSec туннелей.

1. В Policy Manager выберите **VPN > VPN Settings**.
   Откроется диалоговое окно VPN Settings

2. Настройте необходимые параметры для ваших VPN туннелей.

Enable IPSec Pass-through

Для того чтобы пользователь смог создать IPSec подключение к Firebox, которое находится за другим Firebox, вам необходимо включить опцию **Enable IPSec Pass-through**. Например, если ваши мобильные сотрудники находятся в офисе заказчика, у которого стоит Firebox, то они могут подключиться к своей сети через IPSec туннель. Для разрешения исходящих IPSec подключений вам необходимо на локальном Firebox создать политику IPSec. Если вы хотите создать Phase 2 предложение и использовать функцию IPSec pass-through, вам в качестве метода предложение необходимо указать ESP (Encapsulating Security Payload), так как IPSec pass-through поддерживает только его.

После того, как вы включите IPSec pass-through в Policy Manager будет автоматически создана политика *WatchGuard IPSec*. Политика разрешает трафик из любой Trusted или Optional сетей в любое направление. Если вы отключите IPSec pass-through, то политика *WatchGuard IPSec* будет удалена.

Enable TOS for IPSec

Type of Service (TOS) – это 4 бита в IP заголовке, который используется маршрутизаторами для определения приоритета трафика. Fireware предоставляет вам возможность разрешить IPSec туннелям удалять или оставлять эти биты без изменений. Некоторые ISP блокируют все пакеты с установленными TOS флагами.

Если вы не включите опцию **Enable TOS for IPSec,** то все IPSec пакеты будут передаваться без TOS флагов. Если TOS флаги были установлены до этого, то Fireware удалит их при инкапсуляции пакета в IPSec заголовок. Если опция **Enable TOS for IPSec** включена и передаваемый пакет имеет установленные TOS флаги, то Fireware при инкапсуляции пакета в IPSec заголовок оставит эти флаги без изменений. Если у исходного пакета этих флагов не было, то при инкапсуляции пакета в IPSec заголовок Fireware не добавляет эти флаги. Обратите внимание на эту опцию, если вы хотите использовать QoS маркирование для IPSec трафика traffic. QoS маркирование может изменять флаги TOS

Enable LDAP server for certificate verification

При создании VPN шлюза вы указываете данные доступа для обеих конечных точек VPN туннеля, которые будут использованы во время создания туннеля. Если вы хотите использовать IPSec сертификат Firebox, вы можете указать LDAP сервер, который будет использоваться для проверки валидности сертификата. Введите IP адрес LDAP сервера в соответствующем текстовом поле. Вы также можете указать порт.

BOVPN Notification

Выберите эту опцию для того чтобы Firebox отправлял уведомления в случае если туннель вышел из строя. Откроется диалоговое окно, в котором вы можете настроить все необходимые параметры уведомлений. Эта опция не используется Mobile VPN with IPSec туннелями.

Создание пользовательской политики туннеля

Политики туннеля – это набор правил, которые применяются к подключениям через туннель. По умолчанию новый VPN туннель автоматически добавляется в политики BOVPN-Allow.in и BOVPN-Allow.out, которые разрешают передачу трафика по туннелю. Вы можете настроить туннель, чтобы он не добавлялся в эти политики. Убедитесь, что вы отключили опцию **Add this tunnel to the BOVPN-Allow policie**.

Затем создайте VPN политику для того чтобы разрешить определенные типы трафика.

1. В Policy Manager выберите **VPN > Create BOVPN Policy**.
   Запустится мастер BOVPN Policy Wizard.

2. Выполните все необходимые инструкции мастера. Мастер содержит следующие страницы:

Choose a name for the policies

Введите имя политики, к которому мастер добавит .in и .out для входящих и исходящих туннелей соответственно. Например, если вы введете имя «williams», то мастер создаст политики «williams.in» и «williams.out».

Select the policy type

Укажите тип трафика, который будет разрешен через BOVPN туннель

Select the BOVPN tunnels

Выберите BOVPN туннели, к которым будут применяться политики, созданные в этом мастере.

Create an alias for the tunnels

(Дополнительно) Как и в случае с именем, введите имя туннеля, к которому мастер добавит .in и .out для создания псевдонимов для входящих и исходящих туннелей соответственно. Вы также можете использовать эти псевдонимы в других политиках. Если вы создаете политики для большого количества BOVPN туннелей, рекомендуем вам создать псевдоним

The BOVPN Policy Wizard has completed successfully

Последнее окно сообщит вам о том, какие политики и псевдонимы были созданы мастером.

Настройка исходящей динамической NAT через BOVPN туннель

В BOVPN туннелях вы можете использовать динамическую NAT (DNAT). Динамическая NAT работает, как однонаправленная NAT, и держит VPN туннель открытым только в одном направлении. Это может быть полезно если вы создаете BOVPN туннель к удаленному сайту, где весь VPN трафик идет с одного публичного IP адреса.

Например, предположим вы хотите создать BOVPN туннель к сайту вашего бизнес-партнера, через который вы можете подключиться к серверу баз данных, и вы не хотите, чтобы эта компания могла получить доступ к вашим ресурсам. Ваш бизнес-партнер хочет предоставить вам доступ только с одного IP-адреса. Для этого вам необходимо иметь внешний IP-адрес и адрес доверенной сети каждой конечной точки туннеля VPN. Если вы включите динамическую NAT в BOVPN туннеле, то для этого туннеля вы не можете использовать функцию VPN переключения

Нижеприведенная инструкция подходит для любого BOVPN туннеля, который использует динамическую NAT для того чтобы весь трафик из одной точки туннеля шел с одного IP адреса. На изображениях, приведенных далее в этой главе, будут отображены параметры для BOVPN, где весь трафик с Site A должен идти с одного публичного IP сайта Site A.

Site A

Публичный IP—50.50.50.50

Trusted сеть—10.0.1.1/24

Site B

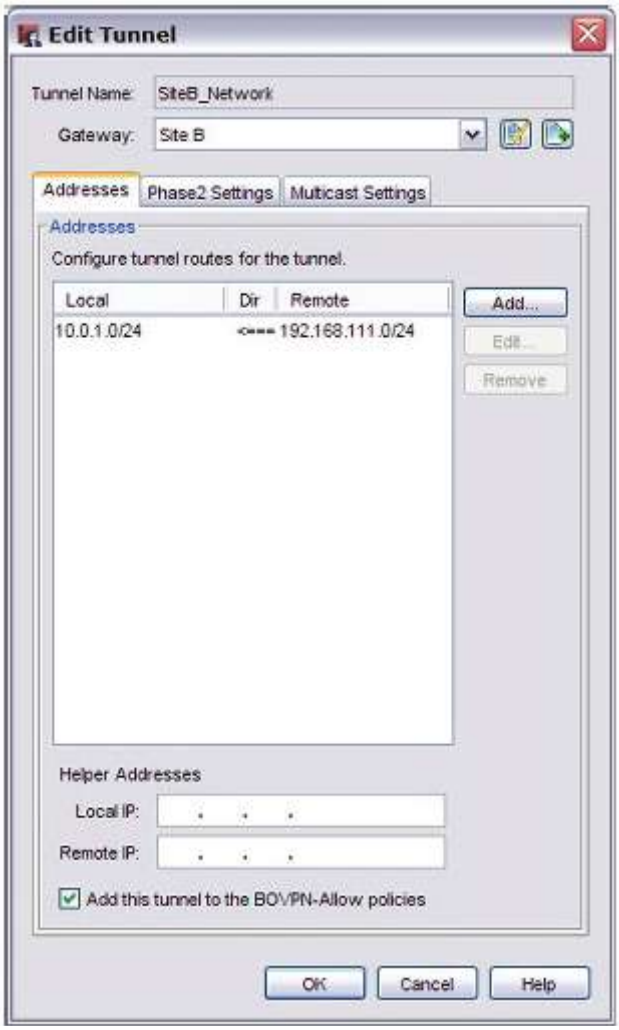
Публичный IP—23.23.23.23

Trusted сеть—192.168.111.1/24

Настройка конечной точки для использования одного IP адреса для всего исходящего трафика (Site A)

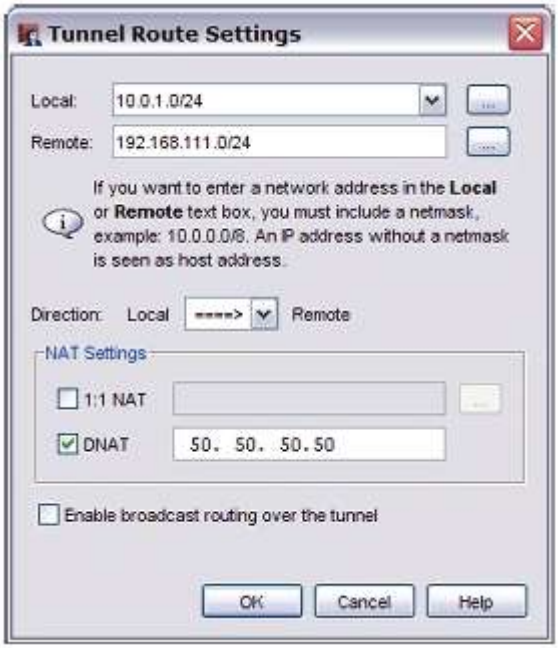
1. В Policy Manager настройте шлюз для BOVPN

2. Выберите **VPN > Branch Office Tunnels**. Нажмите **Add** для того чтобы добавить новый туннель или выберите существующий туннель и нажмите **Edit**.
   Откроется диалоговое окно Add Tunnel или Edit Tunnel



3. В выпадающем списке **Gateway** выберите необходимый шлюз.

4. В закладке **Addresses** нажмите **Add**.
Откроется диалоговое окно Tunnel Route Settings



5. В выпадающем списке **Local** выберите необходимый адрес. Вы также можете нажать кнопку рядом с выпадающим списком **Local** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя.

6. В поле **Remote** введите адрес удаленной сети. Вы также можете нажать кнопку рядом с полем **Remote** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя.

7. В выпадающем списке **Direction** выберите опцию, в которой стрелочки указывают на **Remote**.

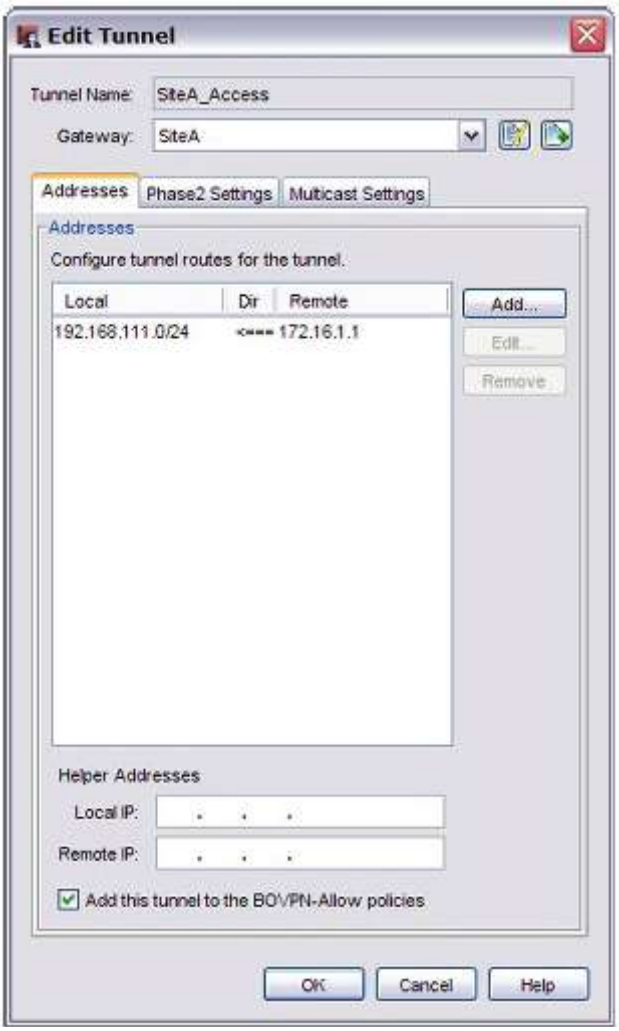
8. В секции **NAT Settings** включите опцию **DNAT**. В поле рядом введите IP адрес, который будет использоваться в качестве IP адреса источника для всего трафика, передаваемого по туннелю.

9. Нажмите два раза **OK**, нажмите **Close** и затем сохраните все сделанные изменения.

Настройка конечной точки, которая получает трафик с одного IP адреса (Site B)

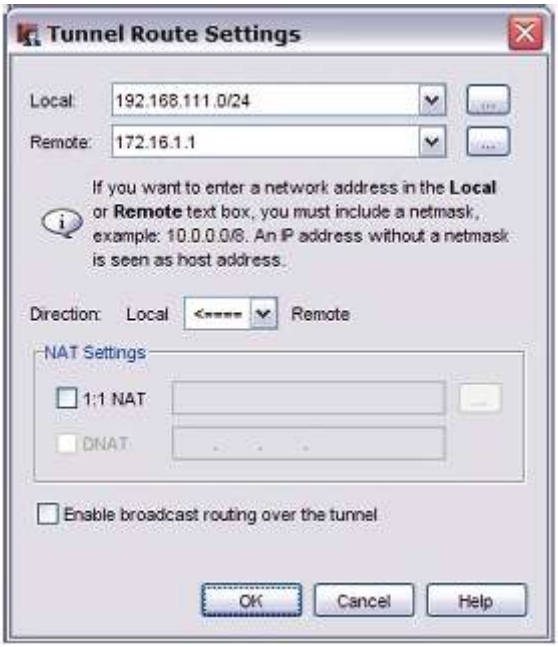
1. В Policy Manager настройте шлюз для BOVPN

2. Выберите **VPN > Branch Office Tunnels**. Нажмите **Add** для того чтобы добавить новый туннель или выберите существующий туннель и нажмите **Edit**.
Откроется диалоговое окно Add Tunnel или Edit Tunnel



3. В выпадающем списке **Gateway** выберите необходимый шлюз.

4. В закладке **Addresses** нажмите **Add**.
   Откроется диалоговое окно Tunnel Route Settings



5. В выпадающем списке **Local** выберите необходимый адрес. Вы также можете нажать кнопку рядом с выпадающим списком **Local** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя. Этот адрес должен совпадать с адресом, который вы указали в поле **Remote** в настройках Сайта A (см п.6 предыдущего раздела)

6. В поле **Remote** введите адрес удаленной сети. Вы также можете нажать кнопку рядом с полем **Remote** и ввести IP адрес хоста. Этот адрес должен совпадать с DNAT адресом, который вы указали в настройках Сайта A (см. п.8 в предыдущем разделе.

7. В выпадающем списке **Direction** выберите опцию, в которой стрелочки указывают на **Local.**

8. В секции **NAT Settings** ничего не включайте.

9. Нажмите два раза **OK**, нажмите **Close** и затем сохраните все сделанные изменения.

Если устройство Firebox на удаленном сайте будет перезагружено, то два устройства Firebox на обоих концах будут создавать туннель заново. Первый Firebox применяет динамическую NAT ко всему трафику, передаваемому из Trusted сети на Firebox на удаленном сайте. Удаленный сайт получает весь трафик с одного DNAT IP адреса.

1-to-1 NAT через BOVPN туннель

Когда вы создаете BOVPN туннель между сетями, которые используют один и тот же диапазон внутренних IP адресов, то происходит конфликт IP адресов. Для того чтобы этого избежать, обе сети должны использовать 1-to-1 NAT. 1-to-1 NAT меняет IP адреса трафика, передаваемого по VPN туннелю.

1-to-1 NAT меняет IP адреса из одного диапазона на IP адреса другого диапазона такого же размера. Каждый IP адрес в первом диапазоне соответствует IP адресу из второго диапазона. В этом документе под первым диапазоном мы имеем в виду диапазон реальных IP адресов, а под вторым диапазоном – маскированные IP адреса

1-to-1 NAT и VPN

Если вы используете 1-to-1 NAT через BOVPN туннель:

- Когда компьютер в вашей сети отправляет пакет компьютеру в удаленной сети, Firebox меняет IP адрес источника на IP адрес из диапазона маскированных IP адресов. Удаленная сеть получает пакет с IP адресом источника равным маскированному IP адресу.

- Когда компьютер из удаленной сети отправляет пакет компьютеру в вашей сети через VPN, то он отправляет его на адрес из диапазона маскированных IP адресов. Firebox меняет IP адрес назначения на реальный IP адрес и передает пакет истинному получателю.

1-to-1 NAT через VPN влияет только на трафик, который передается по VPN. Правила, которые вы можете посмотреть в Policy Manager, выбрав **Network > NAT,** на трафик, передающийся по VPN не влияют.

Другие причины использовать 1-to-1 NAT через VPN

Вдобавок к предыдущей ситуации, вы можете использовать 1-to-1 NAT через VPN если сеть, к которой вы создаете VPN туннель, содержит VPN к сети, которая использует такой же диапазон IP адресов, что и ваша сеть. IPSec устройство не может маршрутизировать трафик между двумя удаленными сетями, которые используют одинаковые диапазоны IP адресов. При использовании 1-to-1 NAT ваши компьютеры будут отправлять пакеты с маскированными IP адресами. Однако в отличие от предыдущей ситуации, вам необходимо будет использовать NAT только на вашей конечной точке туннеля.

Подобная ситуация также наблюдается в случае, если два удаленных офиса с одинаковыми диапазонами, пытаются создать VPN туннели к вашему Firebox. В этом случае один из офисов должен использовать NAT.

Альтернатива NAT

Если ваша офисная сеть используется диапазон внутренних адресов 192.168.0.x или 192.168.1.x, то скорее всего у вас возникнут проблемы с конфликтом IP адресов. Эти IP адреса часто используются широкополосными маршрутизаторами или другими электронными устройствами в домах или офисах. При возможности вам необходимо будет изменить используемый в вашей сети диапазон на 10.x.x.x или 172.16.x.x.

Как настроить VPN

1. Выберите диапазон IP адресов, которые будут использоваться компьютерами вашей сети в качестве IP адресов источника при передаче трафика через BOVPN туннель. Проконсультируйтесь с администратором удаленной сети по поводу используемых диапазонов IP адресов. Не используйте адреса из:

   * Trusted, Optional или внешних сетей, подключенных к вашему Firebox

   * Вторичных сетей, подключенных к Trusted, Optional или External интерфейсам вашего Firebox

   * Маршрутизируемых сетей, настроенные в политике вашего Firebox (**Network > Routes**)

   * Сетей, для которых у вас уже есть BOVPN туннель

   * Виртуального Пула IP адресов Mobile VPN

   * Сети, подключенные у интерфейсам удаленного IPSec устройства, и сети, для которых на VPN устройстве настроены сетевые или VPN машруты

2. Настройте шлюзы для локального и удаленного Firebox.

3. Создайте туннель между конечными точками. В диалоговых окнах Tunnel Route Settings на каждом Firebox, включите опцию 1:1 NAT и в текстовом поле введите диапазон маскированных IP адресов. Количество IP адресов в диапазоне должно равняться количеству адресов в поле Local в верхней части диалогового окна. Например, если для

записи подсети вы используете slash-нотацию, то значение маски подсети должно быть одинаковым в обоих текстовых полях.

Настройки NAT в **Network > NAT** утилиты Policy Manager менять не надо. Эти параметры не влияют на VPN трафик.

Пример

Возьмем для пример две компании - Site A и Site B. Эти компании хотят создать BOVPN туннель между своими Trusted сетями. Обе компании используют Firebox с установленной Fireware XTM и используют один и тот же внутренний диапазон IP адресов, 192.168.1.0/24. Firebox каждой компании использует 1-to-1 NAT через VPN. Site A отправляет пакеты на на IP адреса Site B из диапазона маскированных адресов. Также Site B отправляет пакеты на IP адреса Site A из маскированного диапазона. При этом не происходит конфликта IP адресов. Обе компании используют следующие настройки:

- Пакеты с Site A передаются по VPN туннелям с IP адресами источника из диапазона 192.168.100.0/24. Это маскированный диапазон Site A для этого VPN туннеля.

- Пакеты с Site B передаются по VPN туннелю с IP адресами источника из диапазона 192.168.200.0/24. Это маскированный диапазон Site B.

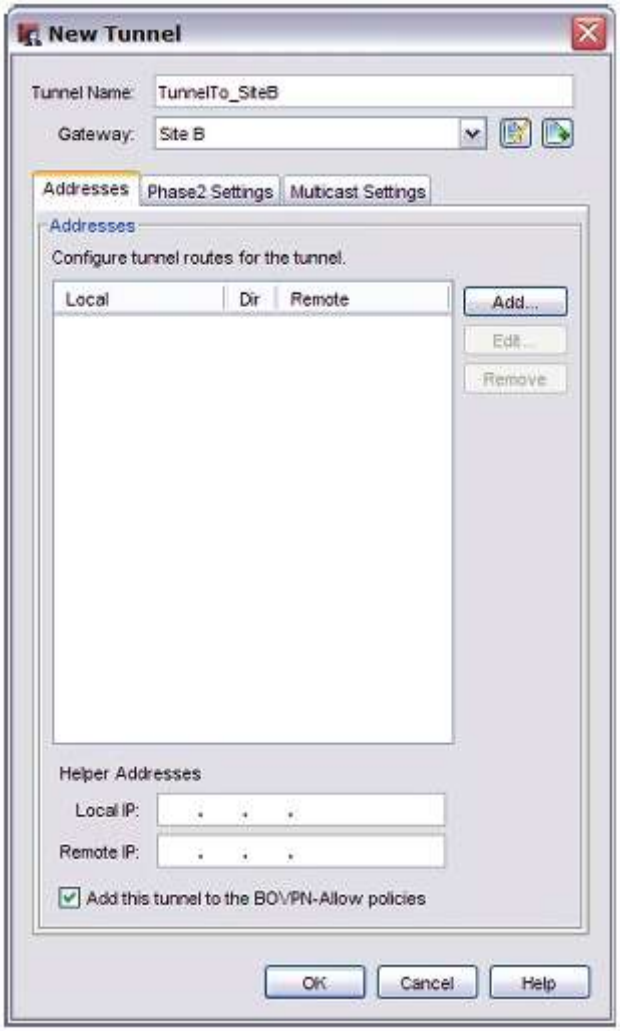
Настройка BOVPN шлюза на каждом Firebox

Первым этапом будет создание шлюза, который будет использоваться для идентификации удаленного IPSec устройства. После того, как вы создатите шлюз, он появится в списке шлюзов в Policy Manager. Для того чтобы посмотреть список шлюзов в Policy Manager выберите **VPN > Branch Office Gateways**

Настройка локального туннеля

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.
   Откроется диалоговое окно Branch Office IPSec Tunnels

2. Нажмите **Add**.
   Откроется диалоговое окно New Tunnel



3. Введите имя туннеля. В этом примере назовем туннеля "TunnelTo_SiteB".

4. В выпадающем списке **Gateway** выберите шлюз, который указывает на удаленное IPSec устройство. В этом примере будем использовать шлюз с именем "SiteB".

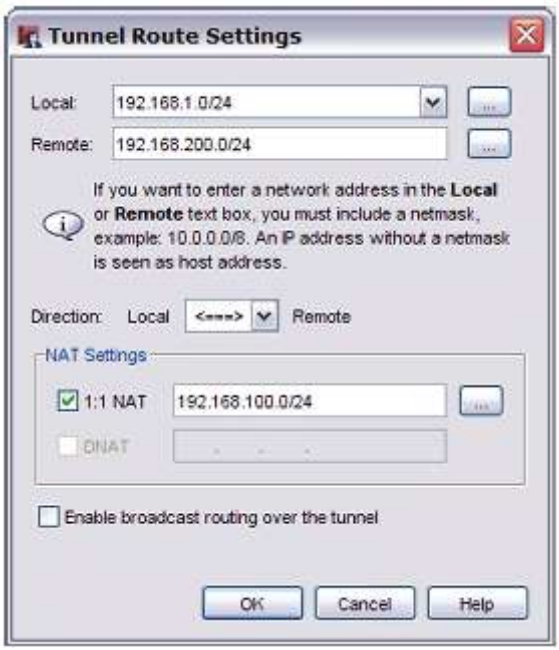
5. Откройте закладку **Phase 2 Settings**. Убедитесь, что параметры Phase 2 в вашей сети совпадают с параметрами Phase 2 удаленной сети.

6. Выберите закладку **Addresses** и нажмите **Add** для того чтобы добавить пару локальный-удаленный шлюзы.
Откроется диалоговое окно Tunnel Route Settings.

7. В поле **Local** введите диапазон реальных IP адресов вашей локальной сети, который будет использоваться для VPN. В этом примере - 192.168.1.0/24.

8. В поле **Remote** введите диапазона внутренних IP адресов, на которые локальные компьютеры будут передавать трафик. В этом примере удаленная сеть на Site B использует 1-to-1 NAT. Соответственно, пакеты, идущие с компьютеров Site B будут передаваться по туннеля с IP адресами источника из маскированного диапазона Site B - 192.168.200.0/24. Компьютеры локальной сети на Site A отправляют пакеты на IP адреса из маскированного диапазона адресов Site B . Если удаленная сеть не использует NAT, то в поле **Remote** введите реальный диапазон IP адресов.

9. Включите опцию **1:1 NAT** и введите маскированный диапазон IP адресов для данного офиса. Эти IP адреса будут использоваться в качестве IP адресов источника при передаче пакетов из сети, защищенной этим Firebox, по VPN туннелю. (Опция **1:1 NAT** будет включена после того, как вы введете корректный IP адрес хоста, адрес сети или диапазон IP адресов в поле **Local**). Site A использует маскированный диапазон IP адресов - 192.168.100.0/24



10. Нажмите **OK**. Firebox создаст новый туннель в политиках BOVPN-Allow.out и BOVPN-Allow.in

11. Сохраните конфигурационный файл. Если вы хотите использовать 1-to-1 NAT только на вашей стороне VPN, вы можете пропустить следующий раздел и завершить настройку. Устройство на удаленном необходимо настроить таким образом, чтобы оно разрешало трафик с IP адресов вашего маскированного диапазона.

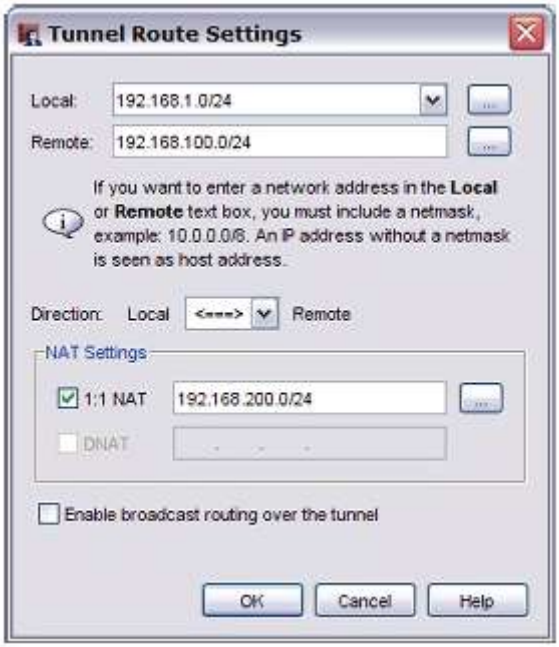
Настройка туннеля на удаленном устройстве

1. Для того чтобы создать туннель на удаленном Firebox повторите п. 1–6 предыдущего раздела. Убедитесь, что параметры Phase 2 совпадают.

2. В поле **Local** введите диапазон реальных IP адресов вашей локальной сети, который будет использоваться для VPN. В этом примере - 192.168.1.0/24.

3. В поле **Remote** введите диапазона внутренних IP адресов, на которые локальные компьютеры будут передавать трафик. В этом примере удаленная сеть на Site A использует 1-to-1 NAT. Соответственно, пакеты, идущие с компьютеров Site A будут передаваться по туннеля с IP адресами источника из маскированного диапазона Site A - 192.168.100.0/24. Компьютеры локальной сети на Site B отправляют пакеты на IP адреса из маскированного диапазона адресов Site A

4. Включите опцию **1:1 NAT** и введите маскированный диапазон IP адресов для данного офиса. Эти IP адреса будут использоваться в качестве IP адресов источника при передаче пакетов из сети, защищенной этим Firebox, по VPN туннелю. Site B использует маскированный диапазон - 192.168.200.0/24



5. Нажмите **OK**. Firebox создаст новый туннель в политиках BOVPN-Allow.out и BOVPN-Allow.in

Создание маршрута для всего Интернет трафика

После того, как вы разрешите удаленным пользователям подключаться к сети Интернет через VPN туннель, наиболее безопасной опцией будет маршрутизация всего Интернет трафика пользователей через VPN туннель на Firebox. С устройства Firebox трафик будет отправляться обратно в сеть Интернет.

В этой конфигурации (также известной как hub route или default-route VPN), Firebox имеет возможность проверять весь трафик и обеспечивать необходимый уровень безопасности. Однако следует учесть, что использование такой конфигурации требует больше ресурсов процессора и пропускной способности Firebox. Если вы используете default-route VPN, политика динамической NAT должна включать весь исходящий трафик из удаленных сетей. Это позволит удаленным пользователям подключаться к сети Интернет, отправляя весь трафик на Firebox.

После того, как вы создадите маршрут по умолчанию через BOVPN туннель, вам необходимо сделать три вещи:

- Настроить BOVPN на удаленном Firebox (чей трафик, вы хотите передавать по туннелю) отправлять весь трафик на адрес 0.0.0.0/0.

- Настроить BOVPN на центральном Firebox для того чтобы разрешить передачу трафика с него на удаленный Firebox.

- Добавить маршрут на центральном Firebox из сети 0.0.0.0/0 в сеть удаленного Firebox.

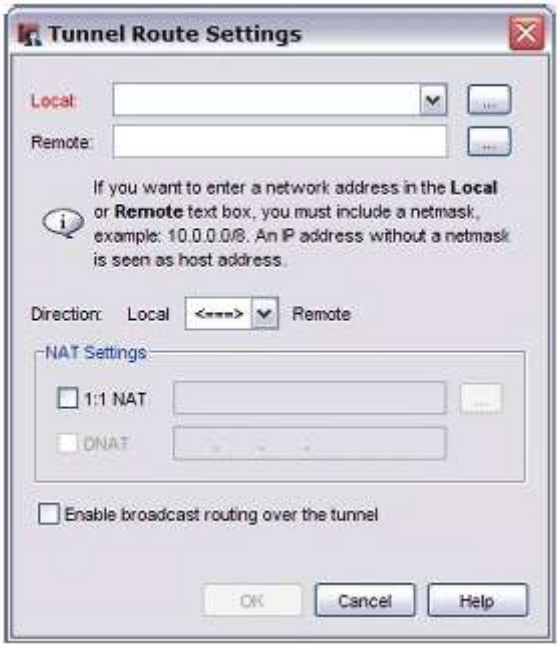
Перед тем, как начать, вам необходимо создать BOVPN туннель между центральным и удаленным Firebox. Для более подробной информации см. “BOVPN туннели, созданные вручную”

Настройка BOVPN туннеля на удаленном Firebox

1. В Policy Manager откройте конфигурационный файл удаленного Firebox.

2. Выберите **VPN > Branch Office Tunnels**. Найдите туннель к центральному Firebox и нажмите **Edit**.
   Откроется диалоговое окно Edit Tunnels.

3. Нажмите **Add**.
   Откроется диалоговое окно Tunnel Route Settings



4. В выпадающем списке **Local** выберите или введите адрес Trusted-сети удаленного Firebox.

5. В поле **Remote**, введите 0.0.0.0/0 и нажмите **OK**.

6. Выберите любой туннель к центральному Firebox и нажмите **Remove**.

7. Нажмите **OK** и сохраните конфигурационный файл.

Настройка BOVPN туннеля на центральном Firebox

1. В Policy Manager откройте конфигурационный файл центрального Firebox.

2. Выберите **VPN > Branch Office Tunnels**. Найдите туннель к центральному Firebox и нажмите **Edit**.
   Откроется диалоговое окно Edit Tunnels.

3. Нажмите **Add**.
   Откроется диалоговое окно Tunnel Route Settings.

4. Нажмите на кнопку рядом с выпадающим списком **Local**. Выберите **Network IP** из выпадающего списка **Choose Type**. В поле **Value** введите 0.0.0.0/0 и нажмите **OK**.

5. В поле **Remote** введите адрес Trusted сети удаленного Firebox и нажмите **OK**.

6. Выберите любой туннель к удаленному Firebox и нажмите **Remove**.

7. Нажмите **OK** и сохраните конфигурационный файл.

Добавление записи динамической NAT на центральном Firebox

Для того чтобы разрешить компьютеру с внутренним IP адресом получить доступ к сети Интернет через Firebox, вам необходимо на центральном Firebox настроить динамическую NAT. При помощи динамической NAT Firebox меняет внутренние IP адреса пакетов, отправленных компьютерами сети, подключенной к Firebox, на публичный IP адрес устройства Firebox. По умолчанию динамическая NAT включена и активна для следующих диапазонов внутренних адресов:

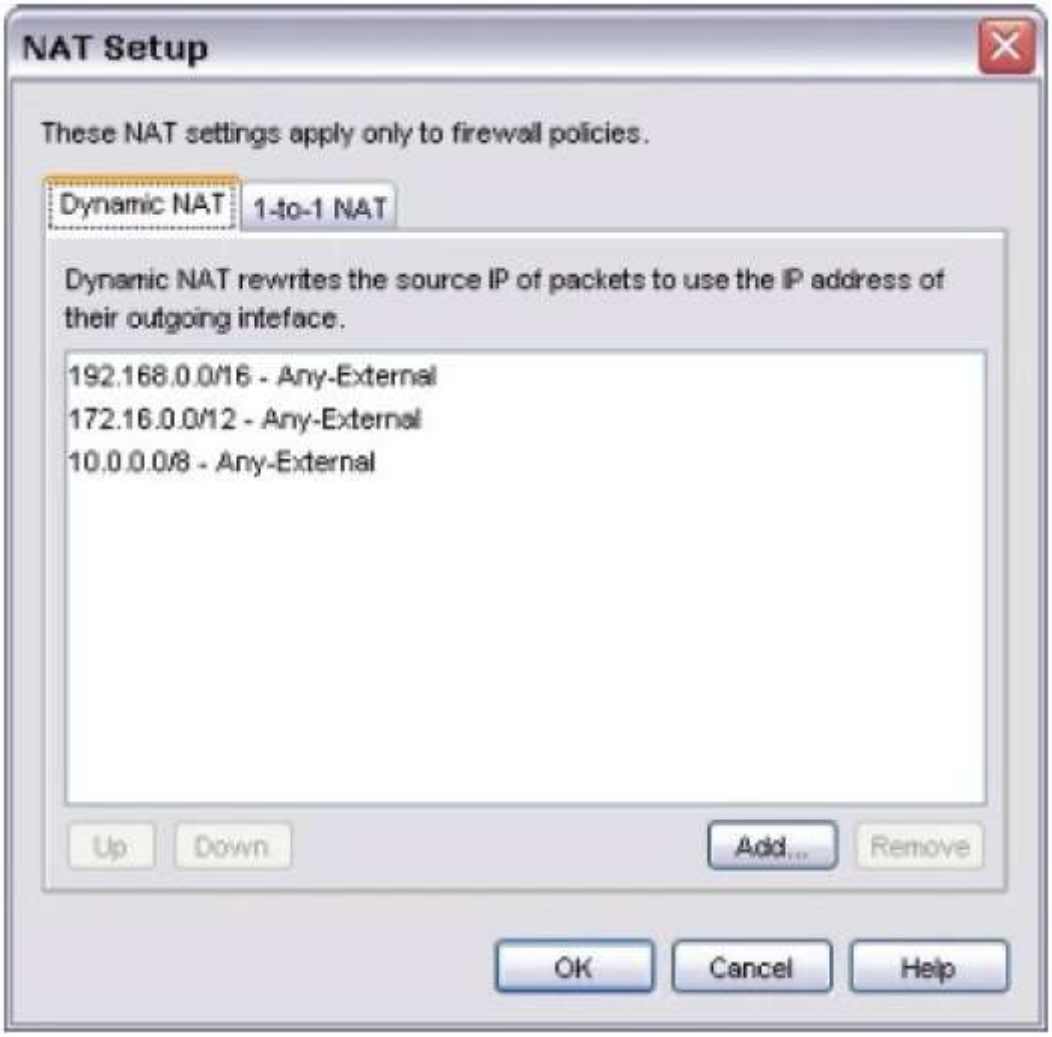
192.168.0.0/16 - Any-External

172.16.0.0/12 - Any-External

10.0.0.0/8 - Any-External

Во время настройки маршрута по умолчанию через BOVPN туннель к удаленному Firebox, если IP адреса сети, подключенной к удаленному Firebox, не входят в эти три диапазона, то вам необходимо эту подсеть добавить в настройки динамической NAT.

1. В Policy Manager выберите **Network > NAT**.
   Откроется диалоговое окно NAT Setup



2. В закладке **Dynamic NAT** диалогового окна **NAT Setup** нажмите **Add**.
   Откроется диалоговое окно Add Dynamic NAT

3. Нажмите  рядом с выпадающим списком **From**.

4. В выпадающем списке **Choose Type** выберите **Network IP**. В поле **Value** введите IP адрес сети, подключенной к удаленному Firebox и нажмите **OK**.

5. В выпадающем списке **To** выберите **Any-External**.

6. Нажмите **OK** для того чтобы закрыть диалоговое окно **Add Dynamic NAT**.

7. Нажмите **OK**. Сохраните конфигурацию на центральном Firebox.

Включение multicast маршрутизации через BOVPN туннель

Вы можете включить multicast маршрутизацию через BOVPN туннель для того чтобы поддерживать односторонние multicast потоки данных между сетями, защищенными устройствами WatchGuard. Например, вы можете использовать multicast маршрутизацию через BOVPN туннель для передачи потоковых данных с сервера VOD(Video On Demand) пользователям на другом конце BOVPN туннеля.

Multicast маршрутизация через BOVPN туннель поддерживается только между устройствами WatchGuard.

После того, как вы включите multicast маршрутизацию через BOVPN туннель, то туннель будет передавать multicast трафик с одного IP адреса на IP Multicast Group адрес. Вам необходимо настроить передачу multicast трафика через туннель на этот IP Multicast Group адрес. На одном Firebox вам необходимо настроить передачу multicast трафика по туннелю, а на втором обработку multicast трафика, передаваемого по туннелю. Для одного туннеля вы можете использовать только один IP адрес источника.

После того, как вы включите multicast маршрутизацию через BOVPN туннель, устройство WatchGuard создаст GRE туннель внутри IPSec VPN туннеля между сетями. Firebox будет передавать multicast трафик по этому GRE туннелю. Для создания GRE туннеля необходим неиспользованный IP адрес на каждом конце туннеля. Вам необходимо настроить специальные «справочные» IP адреса на каждом конце туннеля

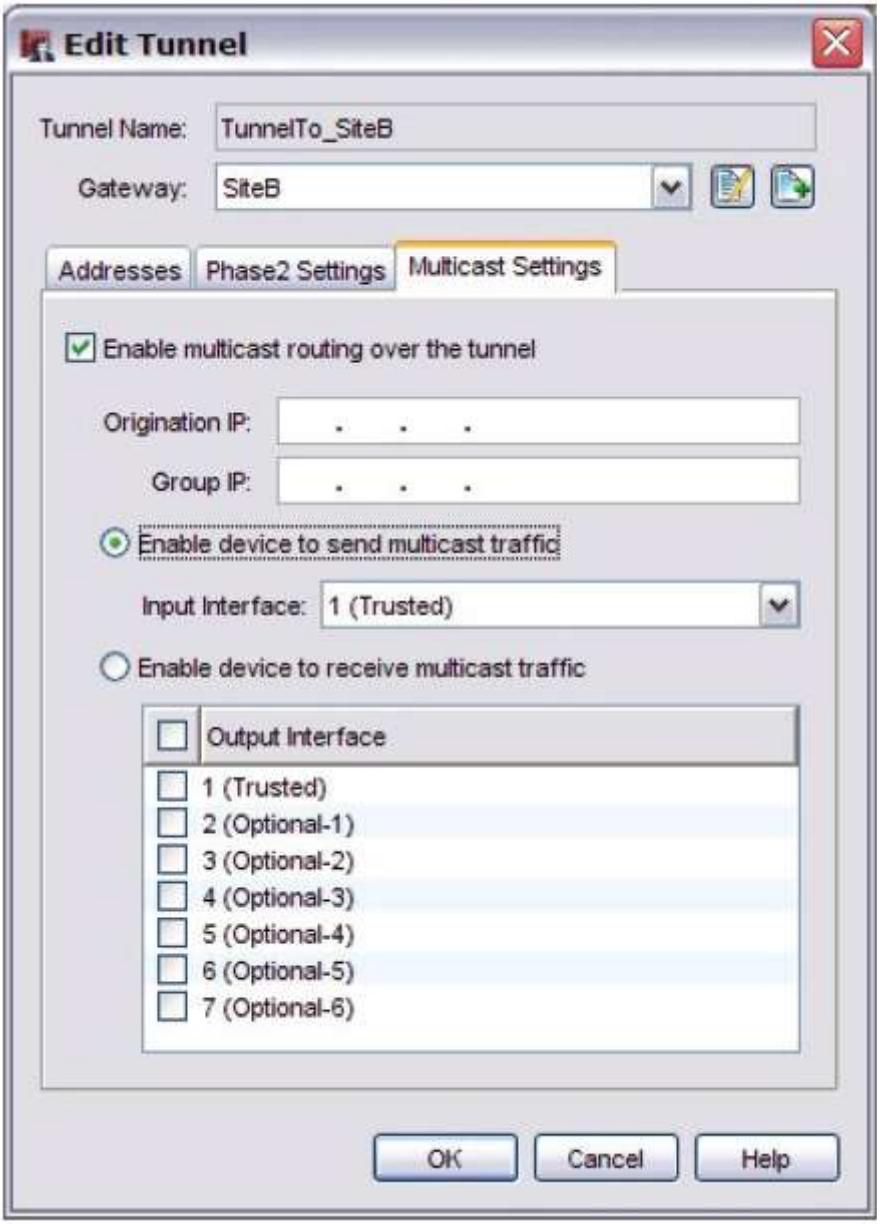
Настройка передачи multicast трафика по туннелю

Для того чтобы передавать multicast трафик по туннелю, вам необходимо на Firebox, который передает трафик, включить передачу multicast трафика по BOVPN туннелю.

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.

2. Выберите туннель и нажмите **Edit**.

3. В диалоговом окне **Edit Tunnel** выберите закладку **Multicast Settings**



4. Включите опцию **Enable multicast routing over the tunnel**.

5. В текстовом поле **Origination IP** введите IP адрес источника multicast трафика.

6. В поле **Group IP** введите multicast IP адрес, на который будет передаваться multicast трафик.

7. Выберите переключатель **Enable device to send multicast traffic**.

8. В выпадающем списке **Input Interface** выберите интерфейс, который будет передавать multicast трафик.

9. Выберите закладку **Addresses**.
   В нижней части закладки Addresses появятся настройки Broadcast/Multicast Tunnel Endpoints

10. В поле **Helper Addresses** введите IP адрес для каждой конечной точки multicast туннеляъ. Firebox будет использовать эти адреса в качестве конечных точек broadcast/multicast GRE туннеля внутри IPSec BOVPN туннеля. В качестве Local IP и Remote IP вы можете использовать любой незадействованный IP адрес. Мы рекомендуем использовать IP адреса, которых нет ни в одной сети, подключенной к Firebox или сети, о котором устройство Firebox знает.

    * В поле **Local IP** введите IP адрес локальной конечной точки туннеля

    * В поле **Remote IP** введите IP адрес удаленной конечной точки туннеля.

Включение обработки multicast трафика на удаленном устройстве WatchGuard

Для того чтобы получать и обрабатывать multicast трафик вам необходимо на удаленном устройстве Firebox включить обработку multicast трафик, передаваемого через туннель.

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.

2. Выберите туннель и нажмите **Edit**.

3. В диалоговом окне **Edit Tunnel** выберите закладку **Multicast Settings**

4. Включите опцию **Enable multicast routing over the tunnel**.

5. В поле **Origination IP** введите IP источника multicast трафика.

6. В поле **Group IP** введите IP адрес получателя трафика

7. Выберите переключатель **Enable device to receive multicast traffic**.

8. При помощи флагов выберите интерфейсы, которые будут получать и обрабатывать multicast трафик.

9. Выберите закладку **Addresses**.
В нижней части закладки Addresses появятся настройки Broadcast/Multicast Tunnel Endpoints

10. В разделе **Helper Addresses** введите IP адрес, противоположный тому, что вы ввели в конфигурации другой конечной точке туннеля.

    * В поле **Local IP** введите IP адрес, который вы ввели в поле **Remote IP** на Firebox другой точке туннеля.

    * В поле **Remote IP** введите IP адрес, который вы ввели в поле **Local IP** на Firebox другой точке туннеля..

Пример: Multicast маршрутизация через BOVPN туннель

Рассмотрим пример настройки BOVPN туннеля и включения multicast маршрутизации с устройства на Сайте A в trusted сеть Сайта B. Предположим, что туннель уже создан

Параметры

САЙТ A (Firebox with Fireware XTM 11.x)

IP адрес Trusted сети: **10.0.50.0/24**

Существующий туннель: **Tunnel_to_SiteB**

Существующий маршрут туннеля: **10.0.50.0/24 <==> 192.168.100.0/24**

САЙТ B (Firebox with Fireware XTM 11.x)

IP адрес Trusted сети: **192.168.100.0/24**

Существующий туннель: **Tunnel_to_SiteA**

Существует маршрут туннеля: **192.168.100.0/24 <==> 10.0.50.0/24**

Multicast устройство на Сайте A

IP адрес сети Multicast устройства: **10.0.50.3**

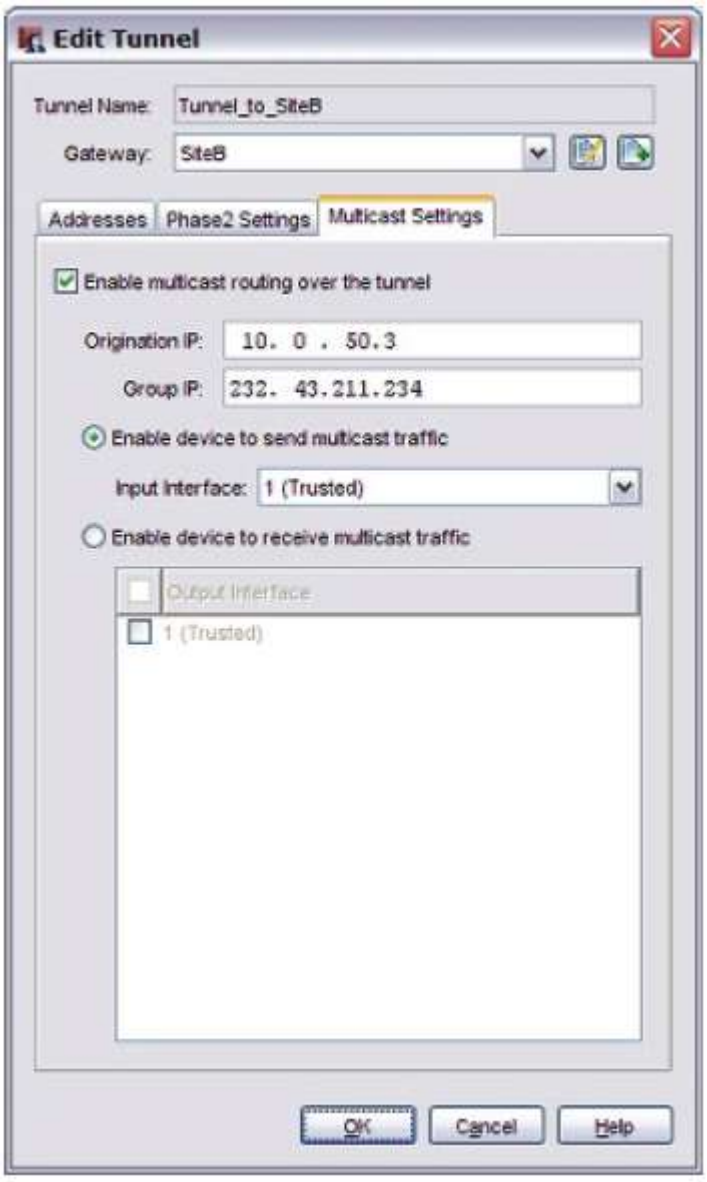
Multicast group IP адрес: **232.43.211.234**

Настройка multicast маршрутизации для BOVPN туннеля на Сайте A

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.
Откроется диалоговое окно Branch Office IPSec Tunnels.

2. Выберите закладку **Tunnel_to_SiteB**. Нажмите **Edit**.
   Откроется диалоговое окно Edit Tunnel.

3. Выберите закладку **Multicast Settings**



4. Включите опцию **Enable multicast routing over the tunnel**.

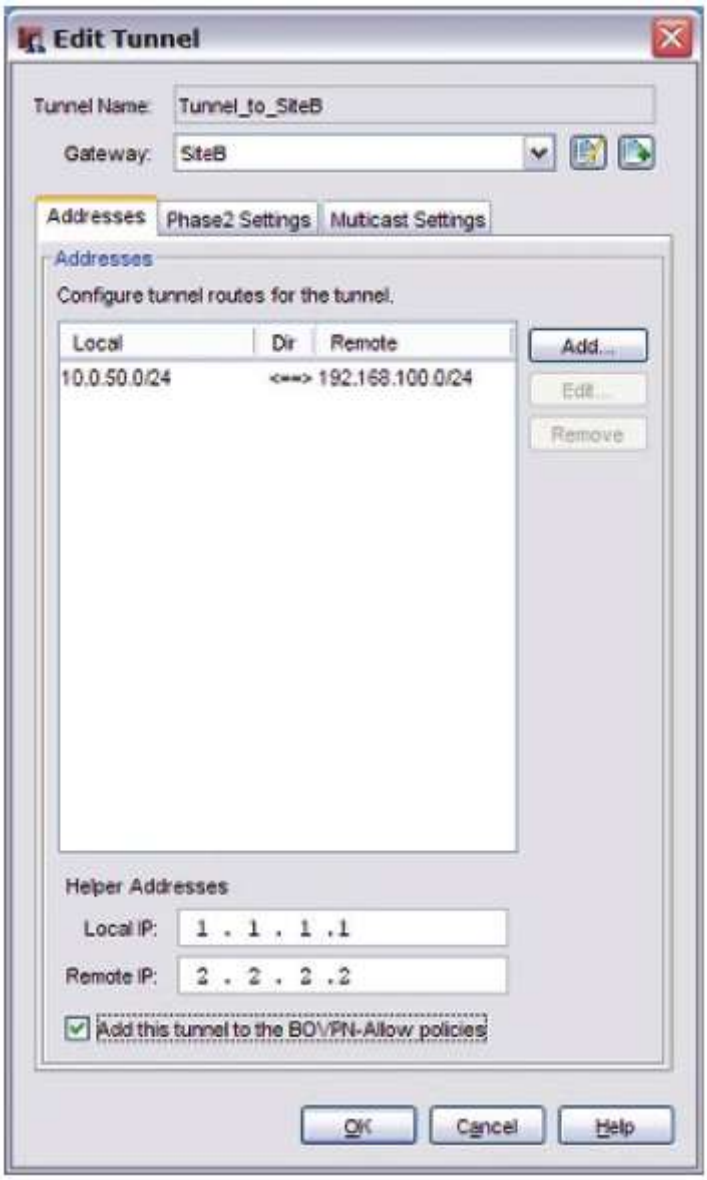
5. В поле **Origination IP** введите IP адрес источника трафика: *10.0.50.3*.

6. В поле **Group IP** введите multicast IP адрес, на который будет отправляться multicast трафик: *232.43.211.234*.

7. Выберите переключатель **Enable device to send multicast traffic**.

8. В выпадающем списке **Input Interface** выберите интерфейс, который будет передавать multicast трафик: **1 (Trusted)**.

9. Выберите закладку **Addresses**
   В нижней части закладки появятся настройки helper Addresses



10. Выберите маршрут туннеля. В разделе **Helper Addresses**, введите еще не задействованные IP адреса для каждой конечной точки туннеля. В качестве Local IP и Remote IP вы можете использовать любой незадействованный IP адрес. Мы рекомендуем использовать IP адреса, которых нет ни в одной сети, подключенной к Firebox или сети, о котором устройство Firebox знает. Для данного примера:

    * В поле **Local IP** на сайте Site A введите 1.1.1.1.

    * В поле **Remote IP** на сайте Site A введите 2.2.2.2.

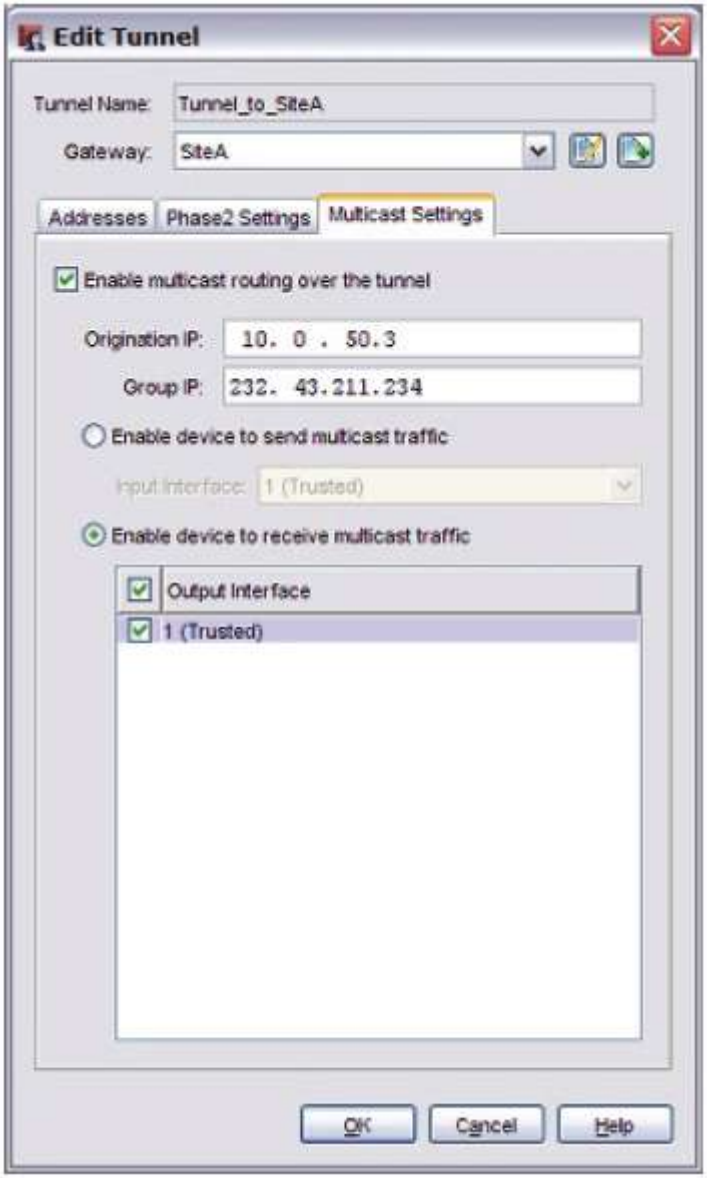
11. Сохраните конфигурацию на Firebox.

Настройка multicast маршрутизации для BOVPN туннеля на Сайте B

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.
Откроется диалоговое окно Branch Office IPSec Tunnels.

2. Выберите закладку **Tunnel_to_SiteA**. Нажмите **Edit**.
Откроется диалоговое окно Edit Tunnel.

3. Выберите закладку **Multicast Settings**



4. Включите опцию **Enable multicast routing over the tunnel**.

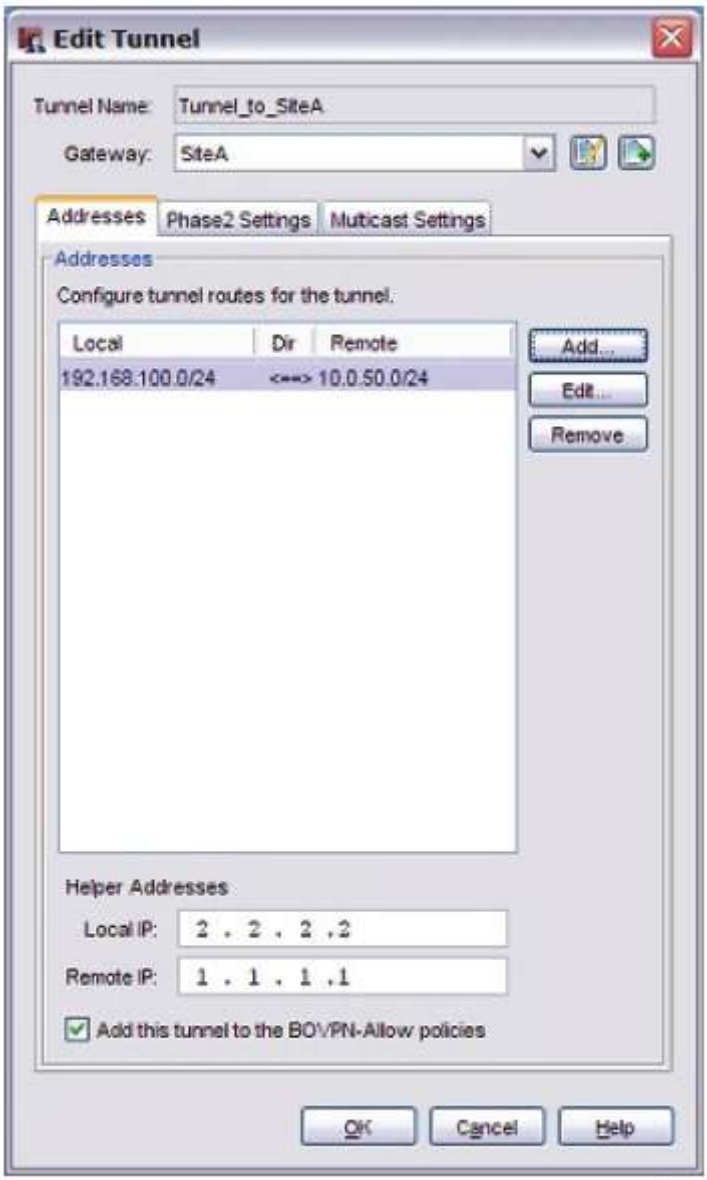
5. В поле Origination IP введите IP адрес источника трафика: *10.0.50.3*.

6. В поле **Group IP** введите multicast IP адрес, на который будет отправляться multicast трафик: *232.43.211.234*.

7. Выберите переключатель **Enable device to receive multicast traffic**.

8. В выпадающем списке **Output Interface** выберите интерфейсы, которые будут получать и обрабатывать multicast трафик. Для данного пример выберите: **1 (Trusted)**.

9. Выберите закладку **Addresses** tab.
Справочные IP адреса появятся в нижней части закладки Addresses



10. Выберите маршрут туннеля. В разделе **Helper Addresses**, введите еще не задействованные IP адреса для каждой конечной точки туннеля. В качестве Local IP и Remote IP вы можете использовать любой незадействованный IP адрес. Мы рекомендуем использовать IP адреса, которых нет ни в одной сети, подключенной к Firebox или сети, о котором устройство Firebox знает. Для данного примера:

    * В поле **Local IP** на сайте Site A введите: 2.2.2.2

    * В поле **Remote IP** введите 1.1.1.1

11. Сохраните конфигурацию Firebox.

Включение broadcast маршрутизации через BOVPN туннель

Broadcast маршрутизация через BOVPN туннель поддерживается только между устройствами WatchGuard.

Также на вашем Firebox вы можете настроить broadcast маршрутизацию через BOVPN туннель. После того, как вы включите broadcast маршрутизацию, туннель будет поддерживать broadcast трафик на broadcast IP адрес - 255.255.255.255.

Локальный broadcast трафик подсети не маршрутизируется через туннель. Broadcast маршрутизация поддерживает передачу broadcast трафика из одной сети в другую через BOVPN туннель.

Broadcast маршрутизация через BOVPN туннель не поддерживает следующие типы broadcast трафика:

- DHCP/ Bootstrap Protocol (bootp) broadcast
- NetBIOS broadcast
- Server Message Block (SMB) broadcast

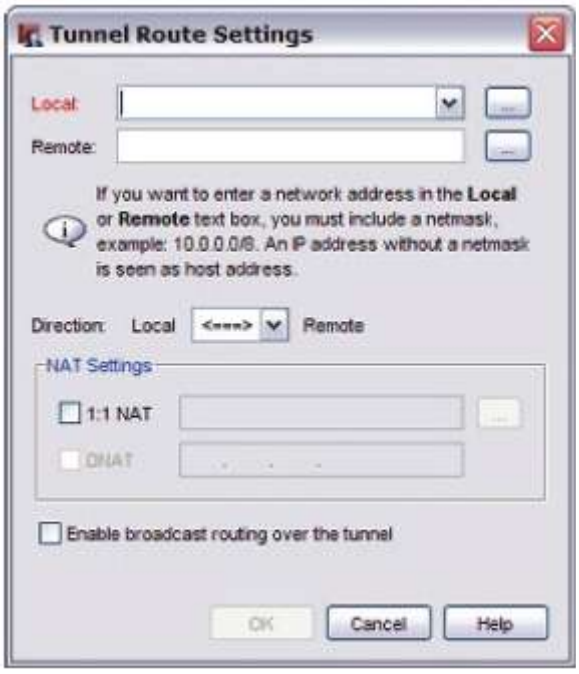
Для более подробной информации о типах broadcast трафика, которые могут переданы через BOVPN туннель см. “Example: Broadcast routing through a BOVPN tunnel” on page 780.

Некоторым приложениям для работы необходимо генерировать broadcast трафик. Если устройства, которым необходимо обмениваться данными, находятся в разных концах BOVPN туннеля, то для того чтобы приложения смогли обнаруживать другие устройства, вам необходимо включить broadcast маршрутизацию через туннель.

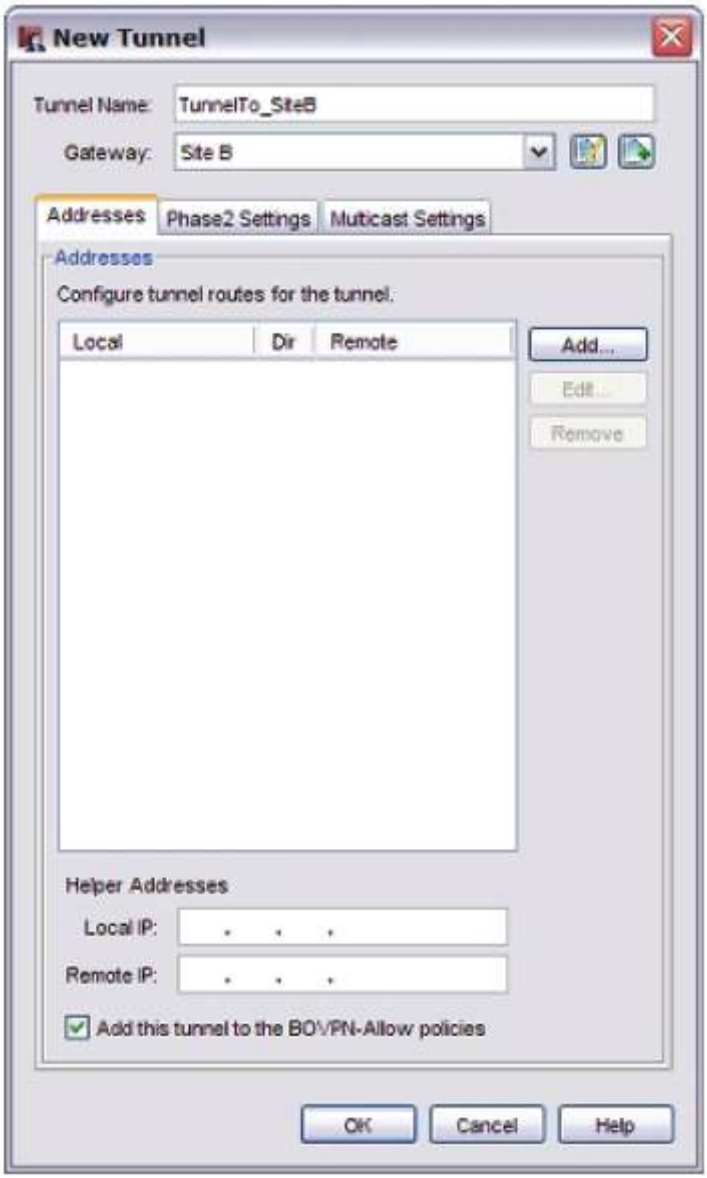
После того, как вы включите broadcast маршрутизацию через BOVPN туннель, устройство WatchGuard создает GRE туннель внутри IPSec VPN туннеля между сетями. Firebox передает broadcast трафик через GRE туннель. Для создания GRE туннеля вам необходим незадействованный IP адрес на каждом конце туннеля. Также вам необходимо настроить helper IP адреса на каждом конце туннеля.

Включение broadcast маршрутизации для локального Firebox

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.
2. Выберите туннель и нажмите **Edit**.
3. В диалоговом окне **Edit Tunnel** выберите маршрут туннеля и нажмите **Edit**.
   Откроется диалоговое окно Tunnel Route Settings



4. Включите опцию **Enable broadcast routing over the tunnel**. Нажмите **OK**.
   Вы вернетесь обратно в диалоговое окно Edit Tunnel. helper адрес появятся в нижней части закладки Addresses



5. В разделе **Helper Addresses** введите IP адреса для каждой конечной точки broadcast туннеля. В разделе **Helper Addresses**, введите еще не задействованные IP адреса для каждой конечной точки туннеля. В качестве Local IP и Remote IP вы можете использовать любой незадействованный IP адрес. Мы рекомендуем использовать IP адреса, которых нет ни в одной сети, подключенной к Firebox или сети, о котором устройство Firebox знает.

   * В поле **Local IP** введите IP адрес для локальной конечной точки туннеля.

   * В поле **Remote IP** введите IP адрес для удаленной конечной точки туннеля.

Настройка маршрутизации broadcast трафика для Firebox на другом конце туннеля

1. Повторите п. 1-4 из предыдущего раздела.

2. В разделе **Helper Addresses** введите IP адрес, противоположный тому, что вы ввели в конфигурации другой конечной точке туннеля.

   * В поле **Local IP** введите IP адрес, который вы ввели в поле **Remote IP** на Firebox другой точке туннеля.

   * В поле **Remote IP** введите IP адрес, который вы ввели в поле **Local IP** на Firebox другой точке туннеля.

Пример: Маршрутизация broadcast трафика через BOVPN туннель

Рассмотрим пример настройки BOVPN туннеля и включения broadcast маршрутизации с устройства на Сайте A в trusted сеть Сайта B.

Параметры

САЙТ A (Firebox with Fireware XTM 11.x)

IP адрес Trusted сети: **10.0.50.0/24**

Существующий туннель: **Tunnel_to_SiteB**

Существует маршрут туннеля: **10.0.50.0/24 <==> 192.168.100.0/24**

САЙТ B (Firebox with Fireware XTM 11.x)

IP адрес Trusted сети: **192.168.100.0/24**

Существующий туннель: **Tunnel_to_SiteA**

Существует маршрут туннеля: **192.168.100.0/24 <==> 10.0.50.0/24**

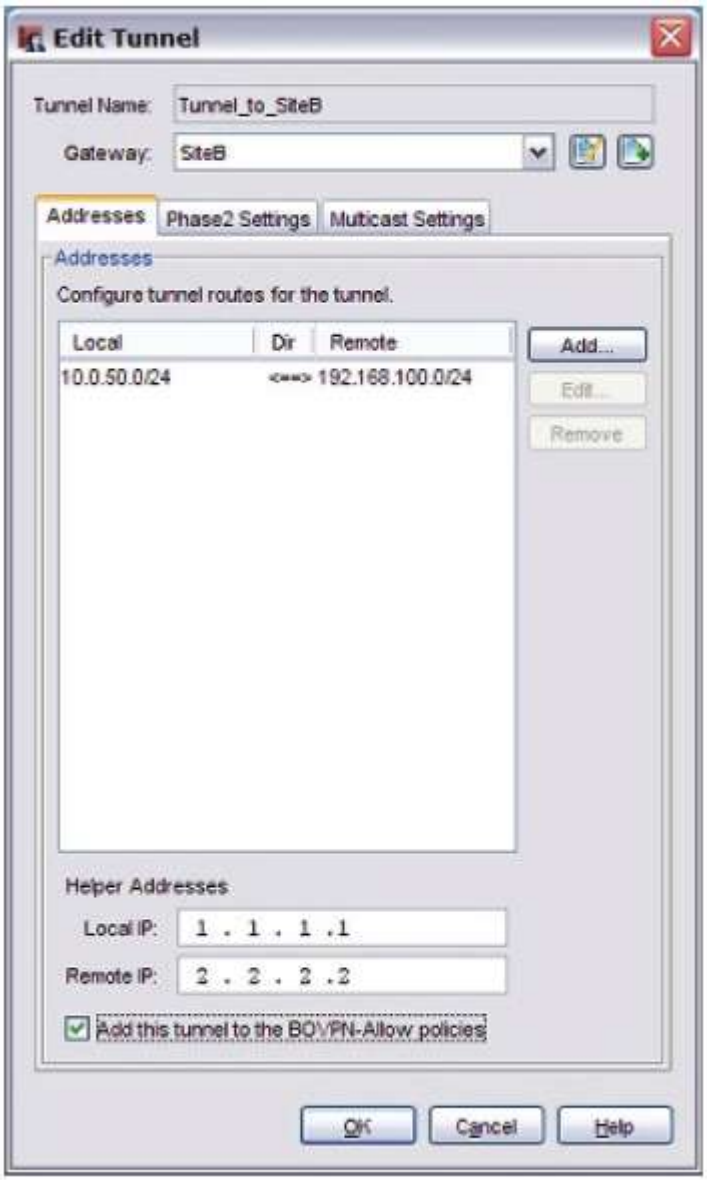
Broadcast устройство на Сайте A

IP адрес сети: **10.0.50.3**

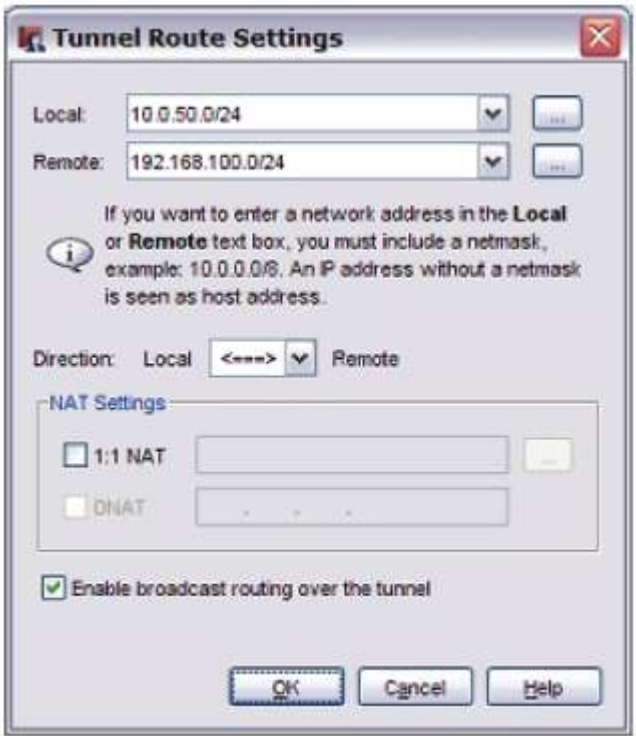
Настройка broadcast маршрутизации для BOVPN туннеля на Сайте A

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.
   Откроется диалоговое окно Branch Office IPSec Tunnels.

2. Выберите закладку **Tunnel_to_SiteB**. Нажмите **Edit**.
Откроется диалоговое окно Edit Tunnel



3. В диалоговом окне **Edit Tunnel** выберите маршрут туннеля и нажмите **Edit**.
Откроется диалоговое окно Tunnel Route Settings



4. Включите опцию **Enable broadcast routing over the tunnel**. Нажмите OK.
Вы вернетесь в диалоговое окно Edit Tunnel. Helper адреса появятся в нижней части закладки Addresses

5. В разделе **Helper Addresses** введите IP адреса для каждой конечной точки broadcast туннеля. В разделе **Helper Addresses**, введите еще не задействованные IP адреса для каждой конечной точки туннеля. В качестве Local IP и Remote IP вы можете использовать любой незадействованный IP адрес. Мы рекомендуем использовать IP адреса, которых нет ни в одной сети, подключенной к Firebox или сети, о котором устройство Firebox знает. Для данного примера:

   * В поле **Local IP** для Сайта A введите 1.1.1.1.

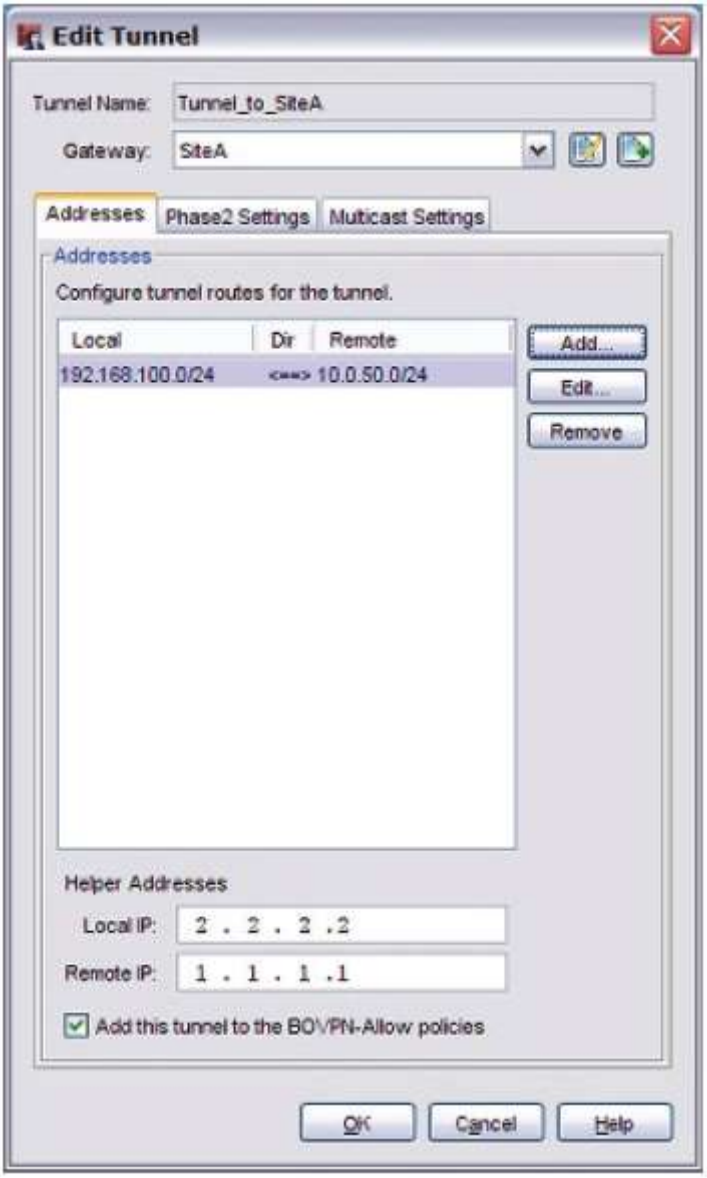
   * В поле **Remote IP** для Сайта A введите 2.2.2.2.

6. Сохраните конфигурацию на Firebox.

Настройка broadcast маршрутизации для BOVPN туннеля на Сайте B

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.
Откроется диалоговое окно Branch Office IPSec Tunnels.

2. Выберите закладку **Tunnel_to_SiteB**. Нажмите **Edit**.
Откроется диалоговое окно Edit Tunnel



3. В диалоговом окне **Edit Tunnel** выберите маршрут туннеля и нажмите **Edit**.
Откроется диалоговое окно Tunnel Route Settings.

4. Включите опцию **Enable broadcast routing over the tunnel**. Нажмите OK.
Вы вернетесь в диалоговое окно Edit Tunnel. Helper адреса появятся в нижней части закладки Addresses

5. В разделе **Helper Addresses** введите IP адреса для каждой конечной точки broadcast туннеля. В разделе **Helper Addresses**, введите еще не задействованные IP адреса для каждой конечной точки туннеля. В качестве Local IP и Remote IP вы можете использовать любой незадействованный IP адрес. Мы рекомендуем использовать IP адреса, которых нет ни в одной сети, подключенной к Firebox или сети, о котором устройство Firebox знает.

   * В поле **Local IP** для Сайта B введите 2.2.2.2

   * В поле **Remote IP** для Сайта B введите 1.1.1.1

6. Сохраните конфигурацию на Firebox.

Примеры broadcast трафика:

В этом примере BOVPN туннель маршрутизирует следующие broadcast:

10.0.50.x/24 -> 192.168.100.255 (адрес назначения – это broadcast адрес удаленной сети)

10.0.50.x/24 -> 255.255.255.255

192.168.100.x/24 -> 10.0.50.255 (адрес назначения – это broadcast адрес удаленной сети)

192.168.100.x/24 -> 255.255.255.255

В этом примере BOVPN туннель не маршрутизирует следующие broadcast адреса:

0.0.0.0 -> 255.255.255.255 (dhcp/bootp broadcast)

10.0.50.x/24 -> 10.0.50.255 (netbios broadcast: not the directed broadcast address of the remote network)

192.168.100.x/24 -> 192.168.100.255 (netbios broadcast: не прямой broadcast адрес удаленной сети)

100.100.100.x/24 -> 10.0.50.255 (IP адрес источника не совпадает с адресом сети)

100.100.100.x/24 -> 192.168.100.255 (IP адрес источника не совпадает с адресом локальной сети)

Настройка VPN переключения(VPN Failover)

Эта тема относится только к VPN туннелям, созданным вручную. Если вы настроили multi-WAN и создали управляемый туннель, то WSM автоматически настроит пары шлюзов, которые включают внешние интерфейсы на обоих концах туннеля. Нет необходимо в дополнительной конфигурации.

Переключение – очень важная функция для сетей, для которых резервирование является критичным.

Если вы настроили и используете multi-WAN переключение, VPN туннели в случае выхода из строя основного External интерфейса, автоматически будут переключаться на резервный External интерфейс. Вы также можете настроить переключение VPN туннелей с основной точки на резервную, в случае если основная точка станет недоступна.

Триггерами VPN переключения являются следующие события:

- Физический канал вышел из строя. Firebox выполняет мониторинг VPN шлюза и устройств, указанных в настройках multi-WAN link monitor. Если физический канал выходит из строя, то происходит VPN переключение.

- Firebox обнаруживает, что VPN устройство не доступно.

При переключении, если туннель использовал IKE keep-alive пакеты, то он продолжает их отправлять этому устройству. После того, как придет ответ на эти пакеты, IKE переключится обратно на основной VPN шлюз. Если туннель использует Dead Peer Detection, обратное переключение происходит после того, как будет получен ответ от основного VPN шлюза.

При переключении, большинство существующих и новых подключений автоматически переключатся. Например, если вы запустите команду FTP “PUT” и основной шлюз выйдет из строя, передача данных по FTP продолжится через резервный VPN маршрут. При этом произойдет лишь небольшая задержка. Помните, что VPN переключение будет работать только если:

- Firebox на каждом конце туннеля имеют установленной Fireware v11.0 или выше.

- Настроено Multi-WAN переключение

- Интерфейсы вашего Firebox есть в списке пар шлюзов на удаленном Firebox. Если вы уже настроили multi-WAN переключение, то ваши VPN туннели при необходимости будут автоматически переключатся на резервный интерфейс.

- DPD включена в настройках Phase 1 на каждом конце туннеля.

VPN переключение не работает для BOVPN туннелей с динамической NAT, которая используется как часть конфигурации туннеля. Для BOVPN туннелей, которые не используют NAT, VPN переключение работает и BOVPN сессии не обрываются.

Сессии Mobile VPN туннелей обрываются, и вам заново аутентифицировать свой Mobile VPN клиент для того чтобы создать новый Mobile VPN туннель.

Создание нескольких пар шлюзов

Если вы настроили multi-WAN и создали управляемый туннель, то WSM автоматически настроит пары шлюзов, которые включают внешние интерфейсы на обоих концах туннеля. Нет необходимо в дополнительной конфигурации..

Для того чтобы ручные BOVPN туннели переключались на резервную точку подключения, вам необходимо создать несколько локальных и удаленных точек подключения для каждого шлюза. Для полнофункционального failover для конфигурации VPN, вам необходимо создать пары шлюзов для каждой комбинации внешних интерфейсов на каждом конце туннеля. Например, предположим что ваша основная локальная точка подключения - 205.122.1.1/24 и резервная - 205.122.2.1/24. Ваша основная удаленная точка подключения - 50.50.1.1/24 + резервная - 50.50.2.1/24.

Для того чтобы использовать VPN Failover, вам необходимо создать следующие пары шлюзов:

23.23.1.1 - 50.50.1.1

23.23.1.1 - 50.50.2.1

23.23.2.1 - 50.50.1.1

23.23.2.1 - 50.50.2.1

1. Выберите **VPN > Branch Office Gateways**. Для того чтобы добавить новый шлюз нажмите **Add**. Введите имя для шлюза и настройте данные доступа

2. В секции Gateway Endpoints диалогового окна **New Gateway** нажмите **Add**
Откроется диалоговое окно New Gateway Endpoints Settings

3. Укажите местоположение локального и удаленного шлюзов. Выберите имя внешнего интерфейса, который совпадает с IP-адресом локального шлюза или имени домена. Для удаленного шлюза вы можете добавить IP-адрес и ID шлюза. Это необходимо если удаленный шлюз находится за устройством NAT и требует больше информации для аутентификации.

4. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Gateway Endpoints**
Откроется диалоговое окно New Gateway. Созданная вами пара шлюзов появится в списке шлюзов. Повторите эту процедуру для того чтобы добавить еще пары шлюзов. Вы можете добавить максимум 9 пар шлюзов. Вы можете выбрать пару и при помощи кнопок **Up** или **Down** измените порядок следования пары шлюзов.

5. Нажмите **OK**.

Повторная генерация ключей для BOVPN туннеля

Обычно шлюзы должны генерировать и обмениваться новыми ключами после определенного промежутка времени или после определенного объема трафика (поле **Force Key Expiration** в диалоговом окне **Phase2 Proposals**).

Иногда вам необходимо будет мгновенно сгенерировать новую пару ключей.

Повторная генерация ключей для одного BOVPN туннеля

Вы можете сгенерировать новую пару ключей для туннеля на передней панели Firebox System Manager и в закладке **Device Status** системы WatchGuard System Manager.

Под **Branch Office VPN Tunnels** выберите туннель, для которого вы хотите сгенерировать новую пару ключей. Нажмите правой кнопкой и выберите *Rekey Selected BOVPN Tunnel*.

Введите пароль конфигурации для Firebox, к которому подключен Firebox System Manager

Повторная генерация ключей для всех BOVPN туннелей

В Firebox System Manager нажмите правой кнопкой на любое место окна и выберите **Rekey All BOVPN Tunnels**.

Введите пароль конфигурации для Firebox, к которому подключен Firebox System Manager. Или в Firebox System Manager выберите **Tools > Rekey All BOVPN Tunnels**.

Введите пароль конфигурации для Firebox, к которому подключен Firebox System Manager. Или в закладке **Device Status** системы WatchGuard System Manager, нажмите правой кнопкой на заголовок **Branch Office VPN Tunnels** или на любой туннель под заголовком. Выберите **Rekey All BOVPN Tunnels**.

Вопросы

Зачем мне нужен внешний статический IP address?

Для того чтобы создать VPN соединение, каждое устройство должно знать IP адрес другого устройства. Если устройство имеет динамический IP адрес, то он естественно может меняться. Если IP адрес одного из устройств меняется, то второе устройство его не может найти и соответственно не может установить VPN соединение. Для того чтобы создать VPN соединение между такими устройствами эти устройства должны знать, как друг друга найти. Если вы не можете получить внешний статический IP адрес, вы можете воспользоваться сервисом Dynamic DNS

Как мне получить внешний статический IP адрес?

Вы можете получить внешний статический IP адрес для вашего компьютера у вашего ISP или администратора сети. Большинство ISP используют динамические IP адрес для упрощения конфигурации сети. Некоторые ISP могут выделить вам статический IP адреса, в качестве дополнительной опции.

Как мне решить проблемы с подключением?

Если вы можете пинговать Trusted интерфейс удаленного Firebox и компьютеры в удаленной сети, то VPN туннель работает нормально. Возможные причины проблем с подключением – это ПО, установленное на сетевые устройства.

Почему не работает ping?

Если вы не можете пинговать IP адрес локального интерфейса удаленного Firebox, выполните следующее:

1. Попробуйте пропинговать адрес удаленного Firebox. Например, с Сайта A попробуйте пропинговать IP адрес Сайта B. Если вы не получаете ответ на ваши ping-запросы, проверьте настройки сети на Сайте B. Сайт B должен отвечать на ping-запросы на этом интерфейсе. Если все корректно настроено, проверьте подключение компьютеров Сайта B к сети Интернет. Если компьютеры Сайта B не могут подключиться к Интернету, поговорите с вашим ISP или администратором сети.

2. Если вы можете пинговать внешний адрес каждого Firebox, попробуйте пропинговать какой-нибудь локальный адрес в удаленной сети. С компьютера на Сайте A попробуйте пропинговать внутренний интерфейс удаленного Firebox. Если туннель работаем нормально, то вам придет ответ. Если вы не получили ответ, то проверьте ваши локальные настройки. Проверьте, не входят ли используемые в обоих сетях IP адреса в диапазон DCHP адресов. Две сети, соединенные через VPN туннель, не должны использовать одни и те же IP адреса.

Как я могу создать больше VPN туннелей, чем разрешено на устройстве Edge?

Количество VPN туннелей, которое вы можете создать на Firebox X Edge e-Series, определяется моделью устройства. Для того чтобы создавать большее количество туннелей вам необходимо приобрести обновление для вашей модели у реселлера или на сайте компани WatchGuard:

http://www.watchguard.com/products/purchaseoptions.asp

WatchGuard VPN совместимость: Fireware XTM с Fireware XTM

BOVPN туннель предоставляет вам защищенный метод передачи данных по незащищенной сети Интернет. В этом документе приводится информация о том, как создать BOVPN туннель вручную.

В этом разделе вы не найдете подробной информации о том, какие параметры используются в диалоговых окнах настроек BOVPN и как они могут повлиять на трафик, передаваемый через туннель. Для более подробной информации о каждом из этих параметров см. Соответствующий раздел:

- “BOVPN туннели, созданные вручную
- Настройка шлюзов
- Создание туннелей между конечными точками шлюза

IP адреса и параметры туннелей

Перед тем, как создавать вручную BOVPN туннель, первым делом вам необходимо определить все необходимые IP адреса и параметры, которые будут использоваться на каждом конце туннеля. Вы также можете распечатать этот документ, заполнить все необходимые поля и затем использовать эту информацию при настройке параметров в Policy Manager.

Для этого документа каждая конечная точка туннеля должна иметь внешний статический IP адрес

Если вы являетесь администратором одного из устройств, то вы можете передать эту таблицу со всей необходимой информацией администратору устройства на другом конце туннеля, для того чтобы он ввел корректные параметры

Проверьте конфигурацию обоих конечных точек VPN туннеля. Убедитесь, что их настройки, а также настройки Phase 1 и Phase 2 одинаковые. Если эти настройки не совпадают, туннель не будет создан.

Параметры BOVPN туннеля:

САЙТ A (Firebox с Fireware XTM 11.x)

Публичный IP адрес: _____

Внутренний IP адрес: _____

САЙТ B (Firebox с Fireware XTM 11.x)

Публичный IP адрес: _____

Внутренний IP адрес: _____

Параметры PHASE 1 (обе стороны должны использовать одинаковые параметры)

*Для BOVPN туннеля между двумя Fireboxe с Fireware XTM, мы рекомендуем включить **Dead Peer Detection (RFC3706)** и не включать **IKE Keep-Alive**. Не включайте сразу две опции. Если на обоих концах туннеля функция Dead Peer Detection поддерживается, то вам всегда необходимо ее включать.*

Данные доступа: Выберите **Use Pre-Shared Key**.

Mode (choose one): Main____ Aggressive____

Ключ шифрования (pre-shared key): _____

NAT Traversal: Yes ____ No ____

интервал NAT Traversal Keep-alive: _____

IKE Keep-alive: Yes ____ No ____

интервал IKE Keep-alive Message: _____

Максимальное количество неудачных попыток IKE Keep-alive: _____

Dead Peer Detection (RFC3706): Yes ____ No ____

Таймаут ожидания Dead Peer Detection Traffic: _____

Максимальное количество попыток Dead Peer Detection: _____

Алгоритм аутентификации (выберите один): SHA1____ MD5____

Алгоритм шифрования(выберите один): DES____ 3DES____ AES-128____ AES-192____ AES-256____

Время жизни SA _____

Выберите **Hours** в качестве единицы измерения времени жизни SA.

Группа Diffie-Hellman (выберите одну): 1____ 2____ 5____

Параметры PHASE 2 (обе стороны должны использовать одинаковые параметры)

Тип: AH ____ ESP ____

Алгоритм аутентификации (выберите один): None____ MD5____ SHA1____

Алгоритм шифрования (выберите один): DES____ 3DES____ AES-128____ AES-192____ AES-256____

Force Key Expiration (выберите один): Enable____ Disable____

Perfect Forward Secrecy (Группа Diffie-Hellman): Disable____ Group1____ Group2____ Group5____

Phase 2 Key Expiration (В часах) _____

Phase 2 Key Expiration (В килобайтах) _____

Пример настроек туннеля

На этой странице показан пример настроек туннеля. Значения всех параметров, приведенных ниже, будут дальше использоваться в описании процедур настройки

САЙТ A (Firebox с Fireware XTM 11.x)

Публичный IP адрес: **50.50.50.50**

Внутренний IP адрес сети: **10.0.50.1/24**

САЙТ B (Firebox with Fireware XTM 11.x)

Публичный IP адрес: **100.100.100.100**

Внутренний IP адрес сети: **192.168.100.1/24**

Параметры PHASE 1 (обе стороны должны использовать одинаковые параметры)

Данные доступа: Выберите **Use Pre-Shared Key**.

Mode (выберите один): Main

Ключ шифрования (Pre-shared key): SiteA2SiteB

NAT Traversal: Yes

Интервал NAT Traversal Keep-alive: 20 seconds

IKE Keep-alive: No

Интервал IKE Keep-alive Message: None

Максимальное количество неудачных попыток IKE Keep-alive: None

Dead Peer Detection (RFC3706): Yes

Таймаут ожидания Dead Peer Detection Traffic: 20 seconds

Максимальное количество попыток Dead Peer Detection: 5

Алгоритм аутентификации (выберите один): SHA1

Алгоритм шифрования(выберите один): 3DES

Время жизни: 8

Выберите Hours в качестве единицы измерения времени жизни SA.

Группа Diffie-Hellman (выберите одну): 2

Параметры PHASE 2 (обе стороны должны использовать одинаковые параметры)

Тип: ESP

Алгоритм аутентификации (выберите один): SHA1

Алгоритм шифрования (выберите один): AES (256 bit)

Force Key Expiration (выберите один): Enable

Perfect Forward Secrecy (Группа Diffie-Hellman): Disable

Phase 2 Key Expiration (В часах): 8

Phase 2 Key Expiration (В килобайтах): 128000

Если вы используете WSM 11.x, то примеры настроек Phase 1 и Phase 2 совпадают с настройками по умолчанию. Они также совпадают с настройками по умолчанию в WSM версии 10.2.2 и выше, также Edge версии 10.2.2 и выше. Они не совпадают с настройками по умолчанию в других версиях Fireware или Edge.

Настройка Сайта A, Fireware XTM 11.x

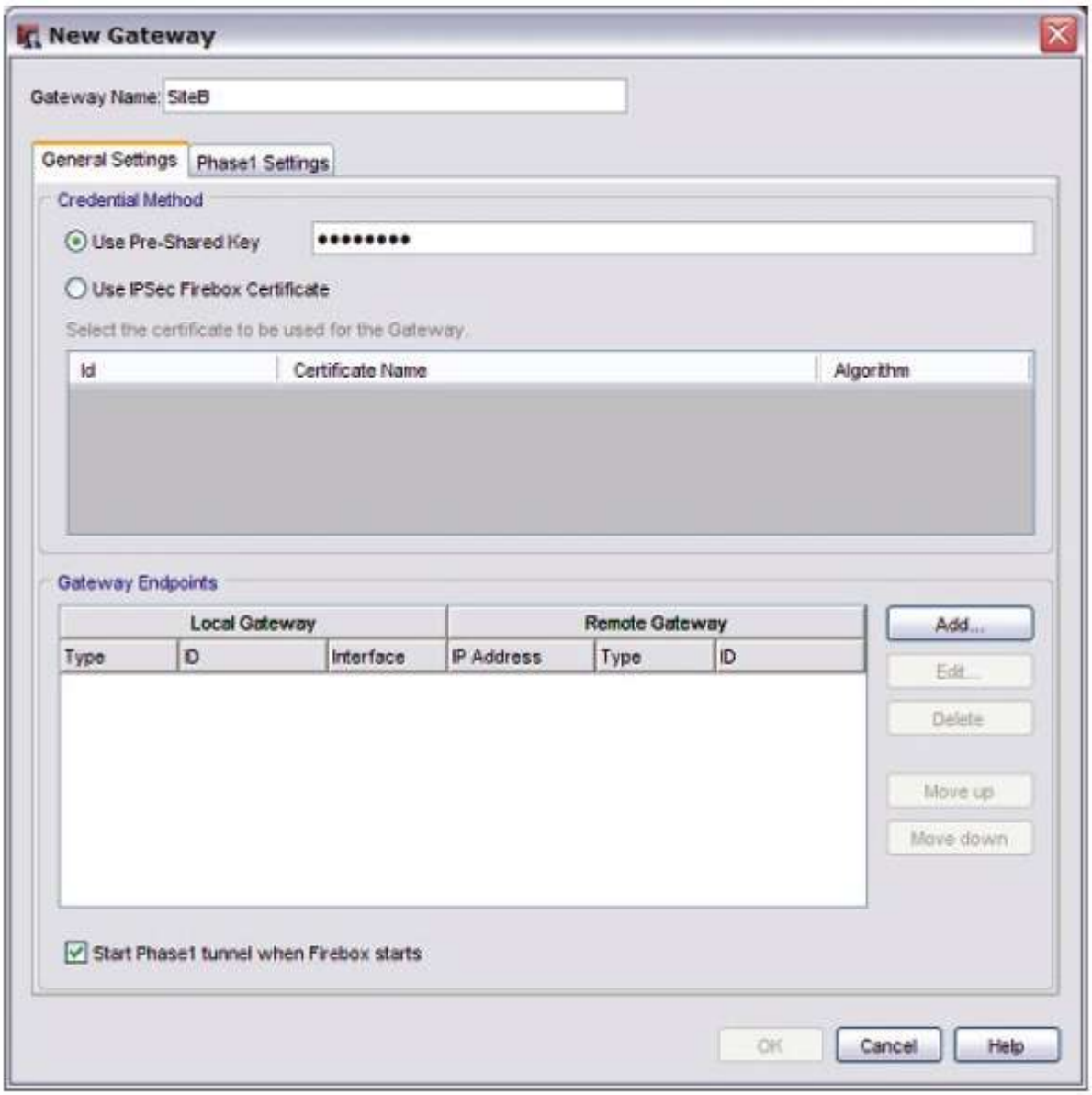
В данном разделе приводится описание настройки шлюза на Сайте A, в котором стоит Firebox с Fireware XTM 11.x. Шлюз – это точка подключения для одного или нескольких туннелей. Для того чтобы настроить шлюз, вам необходимо указать:

- Данные доступа (ключи шифрования или IPSec сертификаты Firebox)
- Местоположение локального и удаленного шлюзов: IP адрес или имя домена
- Параметры Phase 1 для IKE согласования

Создание VPN шлюза

1. В Policy Manager выберите **VPN > Branch Office Gateways**.
   Откроется диалоговое окно Gateways.

2. Для того чтобы добавить новый шлюз нажмите **Add**.
Откроется диалоговое окно New Gateway.

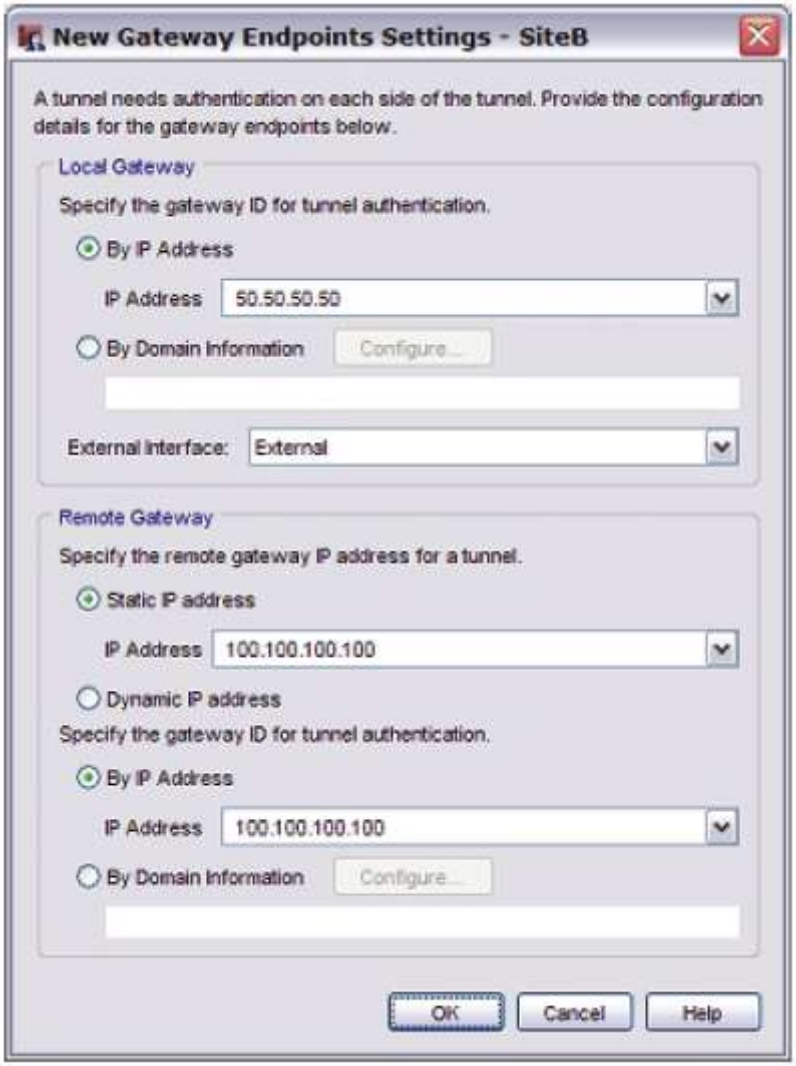


3. В поле **Gateway Name** введите имя, которое будет использоваться для идентификации шлюза в конфигурации Firebox.

4. Выберите закладку **General Settings**.

5. В секции **Credential Method** выберите **Use Pre-Shared Key**. В текстовом поле введите ключ шифрования.
Ключ шифрования должен состоять только из стандартных ASCII символов.

6. В секции **Gateway Endpoints** нажмите **Add**.
   Откроется диалоговое окно New Gateway Endpoints Settings



7. В секции **Local Gateway** выберите **By IP Address**.

8. В выпадающем списке **IP Address** выберите внешний (публичный) IP адрес для Сайта A. В этом списке содержатся все IP адреса интерфейсов.

9. В поле **External Interface** выберите интерфейс, которому присвоен внешний (публичный) IP адрес Сайта A.

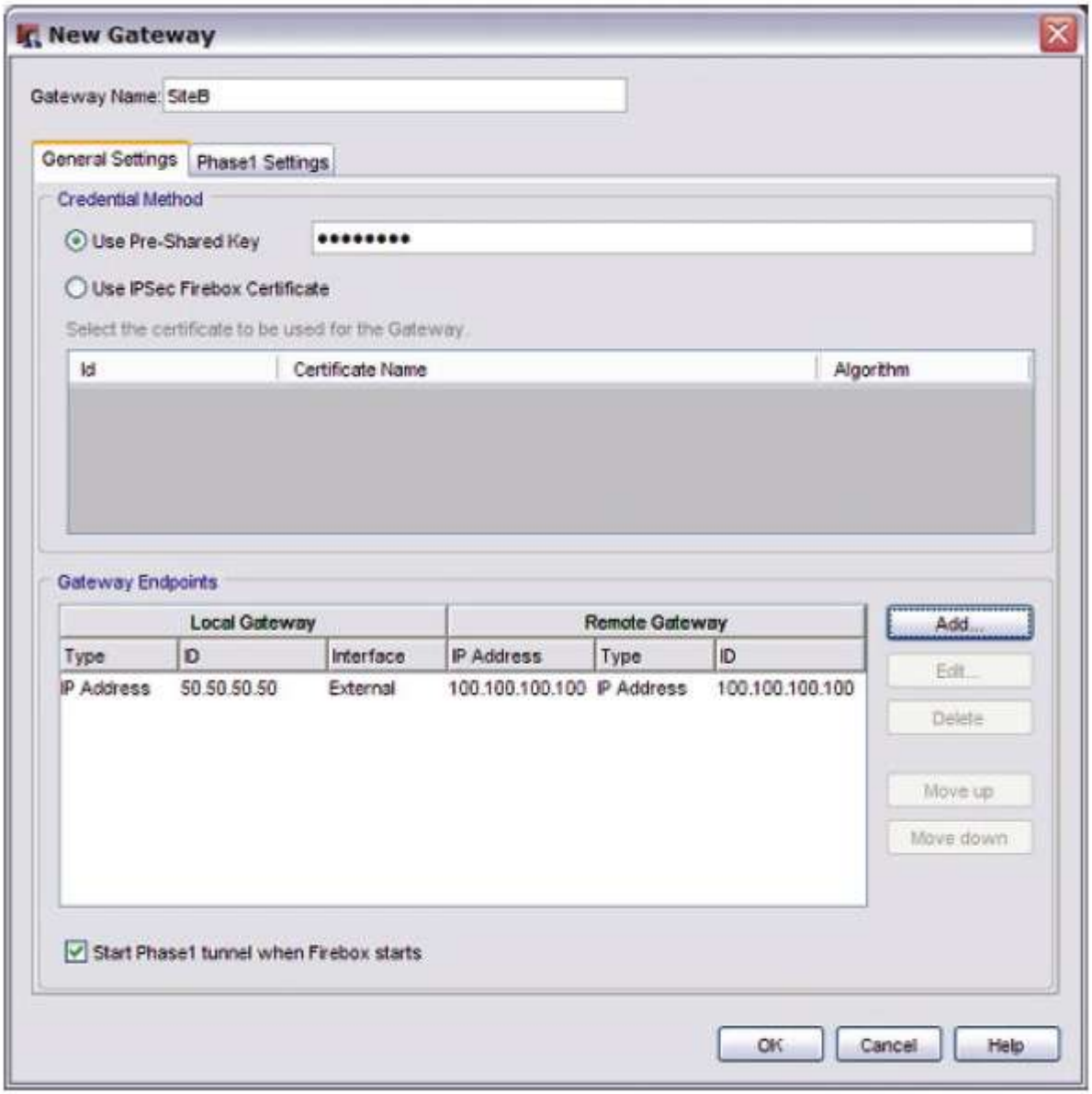
10. В секции **Remote Gateway** для **Specify the remote gateway IP address for a tunnel**, выберите **Static IP Address**.

11. Для **IP Address**, введите внешний (публичный) IP адрес устройства Firebox на Сайте B

12. Выберите **By IP Address** для **Specify the gateway ID for the tunnel authentication**.

13. В поле **IP Address**, введите внешний (публичный) IP адрес устройства Firebox на сайте B.

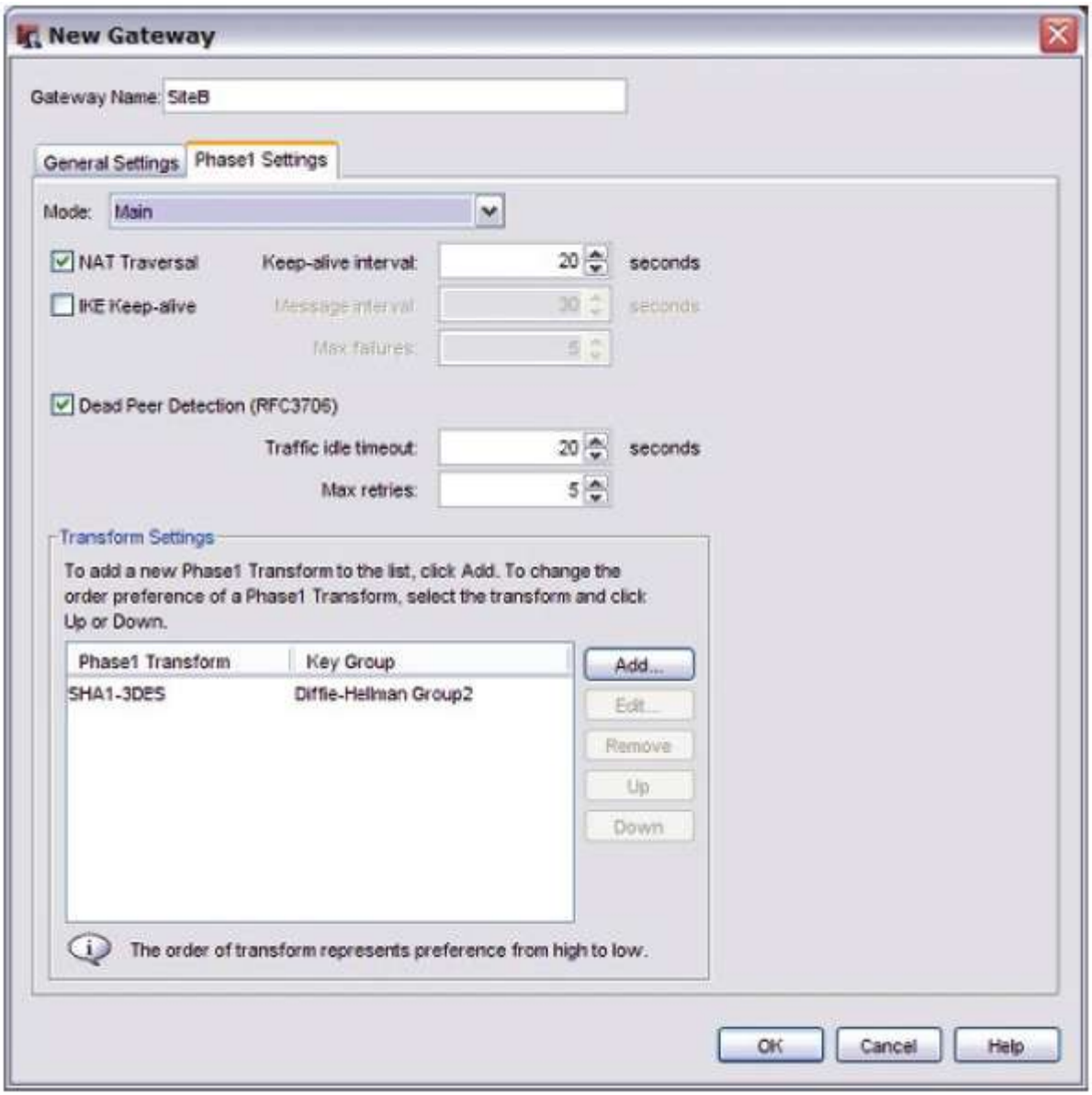
14. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Gateway Endpoints Settings**. *Пара созданных вами шлюзов появится в списке.*



Настройка параметров Phase 1

Phase 1 IPSec соединения – это фаза создания защищенного, аутентифицированного канала связи. Этот канал связи называется ISAKMP Security Association (SA)

- Выберите закладку **Phase 1 Settings**



- В выпадающем списке **Mode** выберите **Main** или **Aggressive**.
  В примере используется режим Main Mode, так как обе конечные точки туннеля имеют статические IP адреса. Если одна из точек имеет динамический IP адрес, то вам необходимо использовать режим Aggressive mode.

- На основе информации о параметрах BOVPN туннеля определите, будете ли вы использовать **NAT Traversal**, **IKE Keep-alive** или **Dead Peer Detection (RFC3706)**. Для BOVPN туннеля между двумя Firebox с Fireware XTM, мы рекомендуем выбрать **NAT Traversal** и **Dead Peer Detection**.

- В секции **Transform Settings** выберите преобразование по умолчанию и нажмите **Edit**

- В выпадающих списках **Authentication** и **Encryption** выберите алгоритмы аутентификации и шифрования соответственно.

- В поле **SA Life** введите время жизни **SA** и в выпадающем списке выберите **Hours**, чтобы в качестве единицы измерения времени жизни использовать часы.

- В выпадающем списке **Key Group** выберите группу Diffie-Hellman.

- Нажмите **OK**. Все остальные параметры Phase 1 оставьте без изменений.

- Нажмите **OK** для того чтобы закрыть диалоговое окно **New Gateway**.
  Созданный вами шлюз появится в списке Gateways

- Нажмите **Close** для того чтобы закрыть диалоговое окно **Gateways**.

Создание VPN туннеля

После того, как вы настроите точки шлюза, вы можете между ними создать туннель. Для того чтобы создать туннель, вам необходимо выполнить следующее:

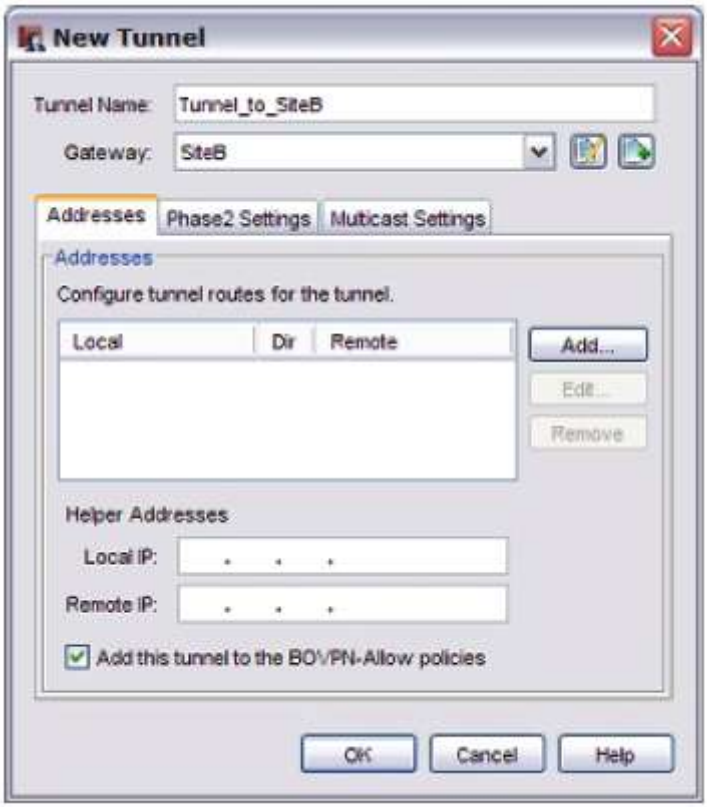
- Создать маршруты (для локальной и удаленной точек туннеля)

- Настроить параметры Phase 2 для IKE. Во время этой фазы создаются ассоциации безопасности (SA) для шифрования пакетов данных.

Для того чтобы создать туннель выполните следующее:

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.
   Откроется диалоговое окно Branch Office IPSec Tunnels.

2. Нажмите **Add**.
   Откроется диалоговое окно New Tunnel



3. В поле **Tunnel Name** введите уникальное имя туннеля (Это имя должно быть уникальным среди имен туннелей, имен групп Mobile VPN и интерфейсов.

4. В списке **Gateway** выберите шлюз для туннеля.

5. Включите опцию **Add this tunnel to the BOVPN-Allow policies** если вы хотите добавить туннель в политики BOVPN-Allow.in и BOVPN-Allow.out. Эти политики разрешают весь трафик, маршрут которого совпадает с маршрутами туннеля. Если вы хотите запретить передачу трафика по туннелю, отключите эту опцию и при помощи мастера BOVPN Policy создайте свои политики, которые будут разрешать передачу определенного типа трафика по туннелю

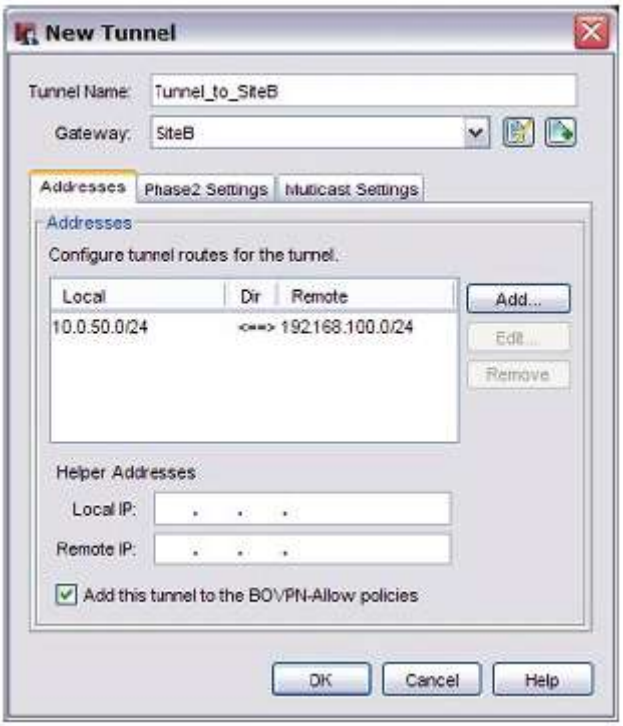
6. В секции **Addresses** нажмите **Add**.
Откроется диалоговое окно Tunnel Route Settings

7. В выпадающем списке **Local** выберите локальный (внутренний) адрес сети. Это внутренний адрес сети Сайта A. Вы также можете нажать на кнопку рядом с выпадающим списком **Local** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя. Это устройства, подключенные к локальному Firebox, которые смогут передавать данные по туннелю.

8. В поле **Remote** введите адрес удаленной сети. Это внутренний адрес сети Сайта B. Вы также можете нажать на кнопку рядом с полем **Remote** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя. Это устройства, подключенные к удаленному Firebox, которые смогут передавать данные по туннелю.

9. В выпадающем списке **Direction** выберите направление для туннеля. Направление определяет, какая конечная точка начнет первой передачу данных по VPN туннелю.

10. Нажмите **OK**.
Маршрут туннеля появится в закладке Addresses диалогового окна New Tunnel.



Настройка параметров Phase 2

Параметры Phase 2 включают параметры SA, которая определяет способ защиты пакетов, передаваемых по туннелю. SA хранит всю необходимую информацию, которую Firebox использует для обработки трафика, передаваемого по защищенному туннелю.

1. В диалоговом окне **New Tunnel** выберите закладку **Phase2 Settings**

2. Включите опцию **PFS** если вы хотите включить Perfect Forward Secrecy (PFS). Если вы включите использование PFS выберите группу Diffie-Hellman.

3. В секции **IPSec Proposals** выберите предложение по умолчанию и нажмите **Remove**.

4. Нажмите **Add**.
   Откроется диалоговое окно New Phase 2 Proposal

5. Выберите **Create a new Phase 2 proposal**.

6. В поле **Name** введите имя нового предложения.

7. В выпадающем списке **Type** выберите **ESP** или **AH**.

8. Выберите алгоритмы аутентификации и шифрования.

9. Вы можете настроить срок действия ключа шифрования. Для того чтобы включить функцию срока действия ключа выберите Enable в выпадающем списке **Force Key Expiration**. В соответствующих текстовых полях введите временной интервал или количество килобайт, по истечении которых срок действия ключа истечет. Если в одном из полей вы введете ноль, то этот счетчик будет игнорироваться. Если опция **Force Key Expiration** отключена или количество часов и килобайт равны нулю, то Fireware будет использовать по умолчанию ноль килобайт и 8 часов.

10. Два раза нажмите **OK** для того чтобы вернуться в диалоговое окно **Branch Office IPSec Tunnel**.
    Созданный вами туннель появится в списке Branch Office IPSec Tunnels

11. Нажмите **Close** и сохраните изменения.

Firebox на Сайте A настроен.

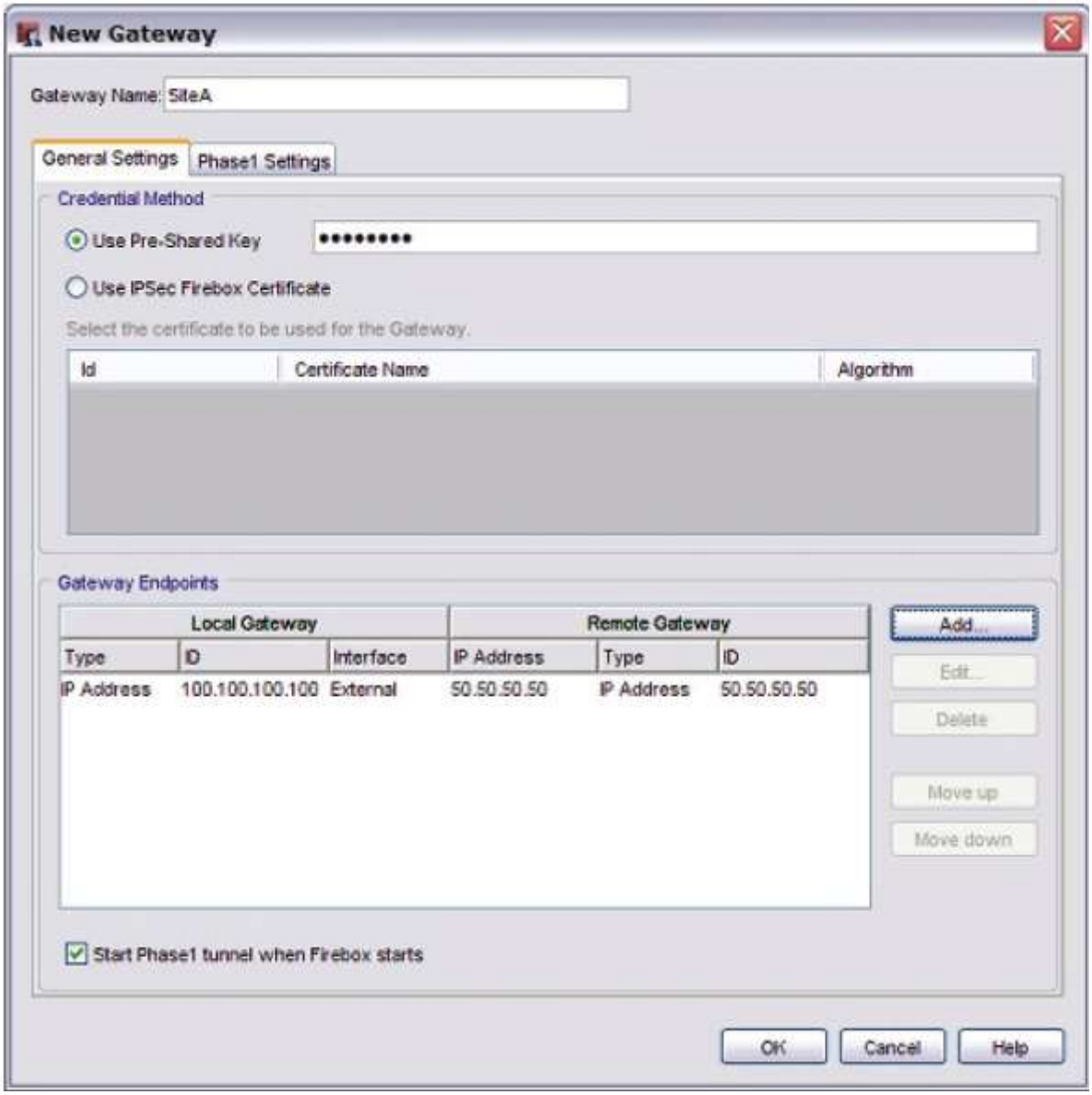
Настройка Сайта B, Fireware XTM 11.x

Теперь вы можете настроить шлюз на Сайте B, на котором стоит Firebox с Fireware 11.x.

Создание VPN шлюза

1. В Policy Manager выберите **VPN > Branch Office Gateways**.
   Откроется диалоговое окно Gateways.

2. Для того чтобы добавить новый шлюз нажмите **Add**.
   Откроется диалоговое окно New Gateway



3. В поле **Gateway Name** введите имя, которое будет использоваться для идентификации шлюза в конфигурации Firebox.

4. Выберите закладку **General Settings**.

5. В секции **Credential Method** выберите **Use Pre-Shared Key**. В текстовом поле введите ключ шифрования.
   Ключ шифрования должен состоять только из стандартных ASCII символов.

6. В секции **Gateway Endpoints** нажмите **Add**.
   Откроется диалоговое окно New Gateway Endpoints Settings

7. В секции **Local Gateway** выберите **By IP Address**.

8. В выпадающем списке **IP Address** выберите внешний (публичный) IP адрес для Сайта B. В этом списке содержатся все IP адреса интерфейсов.

9. В поле **External Interface** выберите интерфейс, которому присвоен внешний (публичный) IP адрес Сайта B.

10. В секции **Remote Gateway** для **Specify the remote gateway IP address for a tunnel**, выберите **Static IP Address**.

11. Для **IP Address**, введите внешний (публичный) IP адрес устройства Firebox на Сайте A.

12. Выберите **By IP Address** для **Specify the gateway ID for the tunnel authentication**.

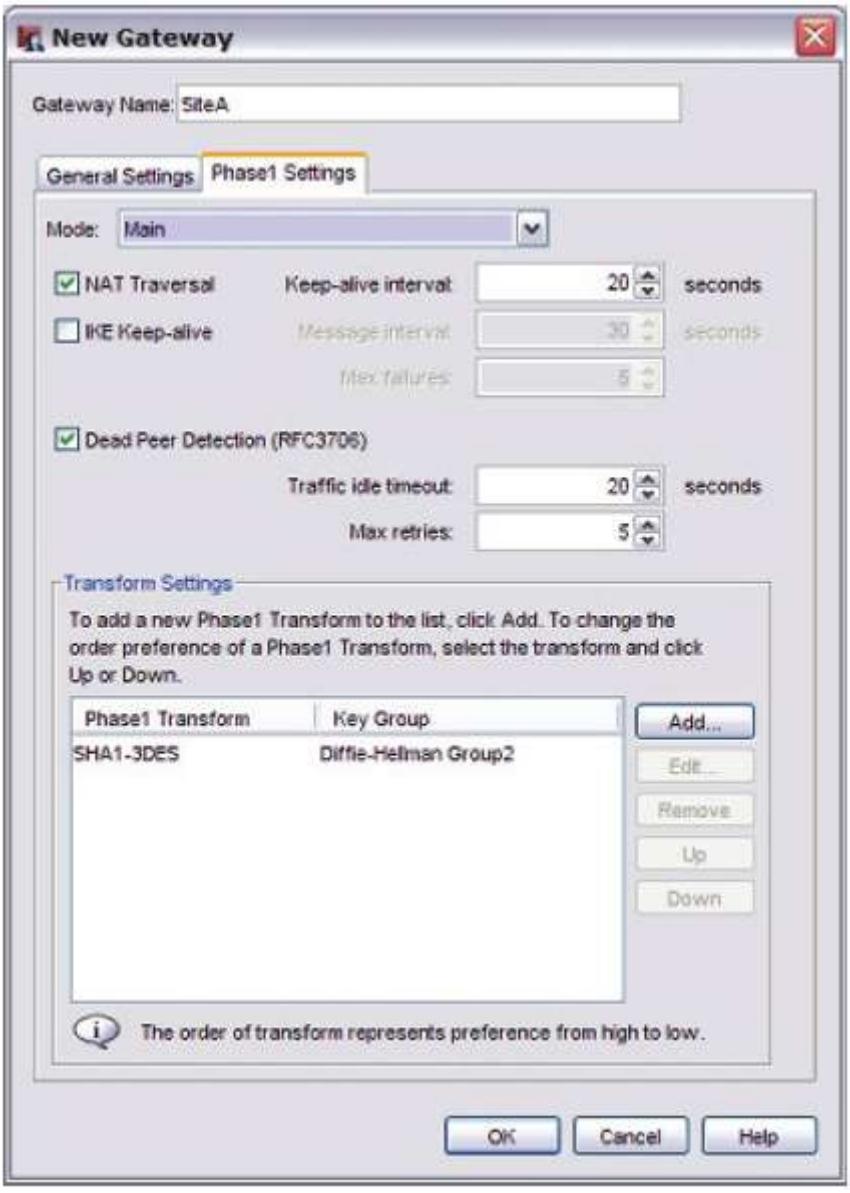
13. В поле **IP Address**, введите внешний (публичный) IP адрес устройства Firebox на сайте A.

14. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Gateway Endpoints Settings**.
Пара созданных вами шлюзов появится в списке.

Настройка параметров Phase 1

Phase 1 IPSec соединения – это фаза создания защищенного, аутентифицированного канала связи. Этот канал связи называется ISAKMP Security Association (SA)

1. Выберите закладку **Phase 1 Settings**



2. В выпадающем списке **Mode** выберите **Main** или **Aggressive**.

3. На основе информации о параметрах BOVPN туннеля определите, будете ли вы использовать **NAT Traversal**, **IKE Keep-alive** или **Dead Peer Detection (RFC3706)**. Выберите значения, которые вы указали в BOVPN Tunnel Settings.

4. В секции **Transform Settings** выберите преобразование по умолчанию и нажмите **Edit**

5. В выпадающих списках **Authentication** и **Encryption** выберите алгоритмы аутентификации и шифрования соответственно.

6. В поле SA Life введите время жизни SA и в выпадающем списке выберите Hours, чтобы в качестве единицы измерения времени жизни использовать часы.

7. В выпадающем списке **Key Group** выберите группу Diffie-Hellman.

8. Нажмите **OK**. Все остальные параметры Phase 1 оставьте без изменений.

9. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Gateway**.
Созданный вами шлюз появится в списке Gateways.

10. Нажмите **Close** для того чтобы закрыть диалоговое окно **Gateways**.

Создание VPN туннеля

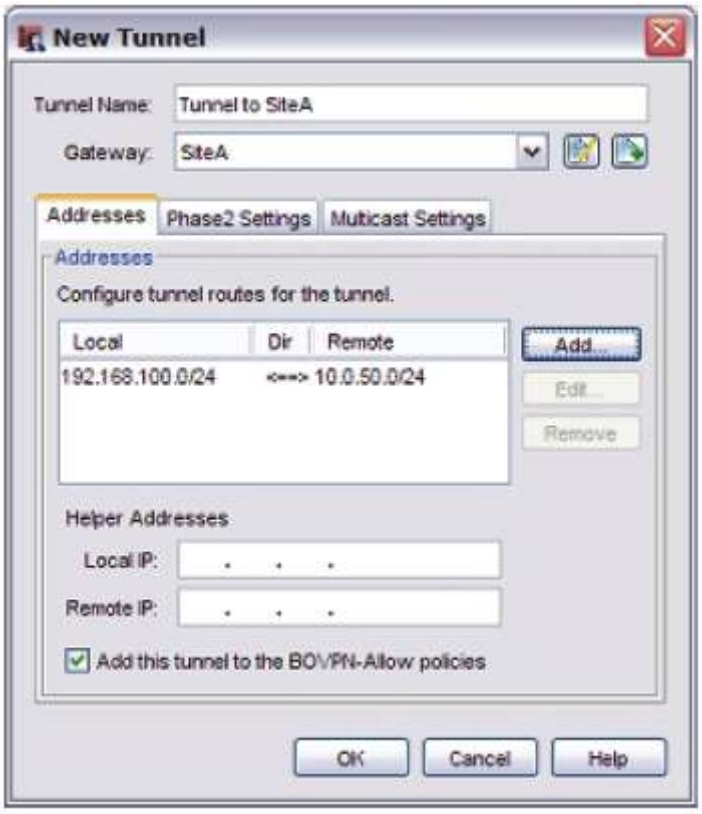
После того, как вы настроите точки шлюза, вы можете между ними создать туннель. Для того чтобы создать туннель, вам необходимо выполнить следующее:

- Создать маршруты (для локальной и удаленной точек туннеля)
- Настроить параметры Phase 2 для IKE. Во время этой фазы создаются ассоциации безопасности (SA) для шифрования пакетов данных

Для того чтобы добавить VPN туннель выполните следующее:

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.
Откроется диалоговое окно Branch Office IPSec Tunnels.

2. Нажмите **Add**.
Откроется диалоговое окно New Tunnel



3. В поле **Tunnel Name** введите уникальное имя туннеля (Это имя должно быть уникальным среди имен туннелей, имен групп Mobile VPN и интерфейсов.

4. В списке **Gateway** выберите шлюз для туннеля.

5. Включите опцию **Add this tunnel to the BOVPN-Allow policies** если вы хотите добавить туннель в политики BOVPN-Allow.in и BOVPN-Allow.out. Эти политики разрешают весь трафик, маршрут которого совпадает с маршрутами туннеля. Если вы хотите запретить передачу трафика по туннелю, отключите эту опцию и при помощи мастера BOVPN Policy создайте свои политики, которые будут разрешать передачу определенного типа трафика по туннелю

6. В секции **Addresses** нажмите **Add**.
   Откроется диалоговое окно Tunnel Route Settings

7. В выпадающем списке **Local** выберите локальный (внутренний) адрес сети. Это внутренний адрес сети Сайта A. Вы также можете нажать на кнопку рядом с выпадающим списком **Local** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя. Это устройства, подключенные к локальному Firebox, которые смогут передавать данные по туннелю.

8. В поле **Remote** введите адрес удаленной сети. Это внутренний адрес сети Сайта B. Вы также можете нажать на кнопку рядом с полем **Remote** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя. Это устройства, подключенные к удаленному Firebox, которые смогут передавать данные по туннелю.

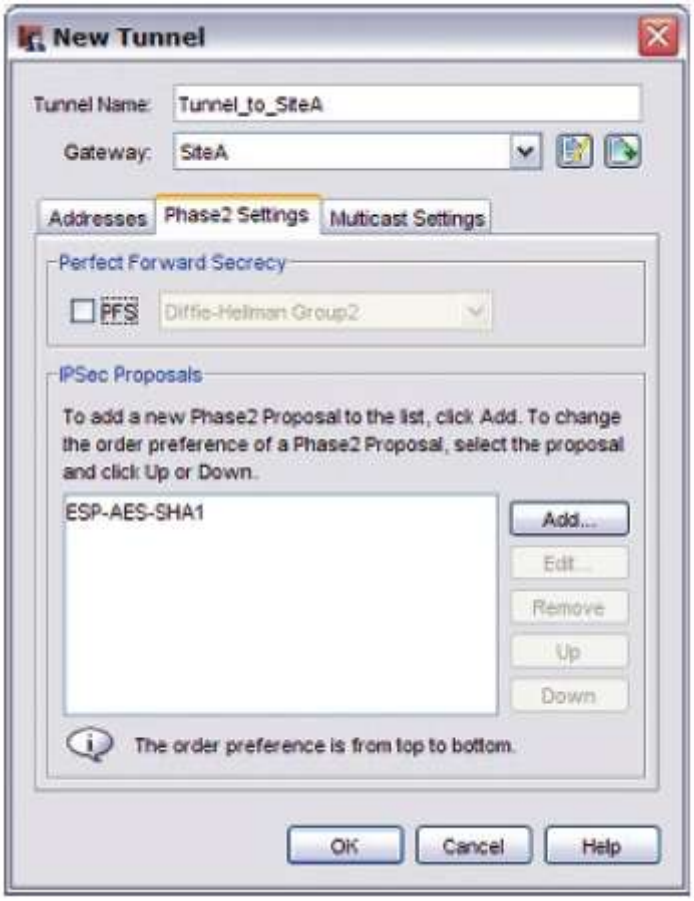
9. В выпадающем списке **Direction** выберите направление для туннеля. Направление определяет, какая конечная точка начнет первой передачу данных по VPN туннелю.

10. Нажмите **OK**.
    Маршрут туннеля появится в закладке Addresses диалогового окна New Tunnel.

Настройка параметров Phase 2

Параметры Phase 2 включают параметры SA, которая определяет способ защиты пакетов, передаваемых по туннелю. SA хранит всю необходимую информацию, которую Firebox использует для обработки трафика, передаваемого по защищенному туннелю.

1. В диалоговом окне **New Tunnel** выберите закладку **Phase2 Settings**



2. Включите опцию **PFS** если вы хотите включить Perfect Forward Secrecy (PFS). Если вы включите использование PFS выберите группу Diffie-Hellman.

3. В секции **IPSec Proposals** выберите предложение по умолчанию и нажмите **Remove**.

4. Нажмите **Add**.
   Откроется диалоговое окно New Phase 2 Proposal

5. Выберите **Create a new Phase 2 proposal**.

6. В поле **Name** введите имя нового предложения.

7. В выпадающем списке **Type** выберите **ESP** или **AH**.

8. Выберите алгоритмы аутентификации и шифрования.

9. Вы можете настроить срок действия ключа шифрования. Для того чтобы включить функцию срока действия ключа выберите Enable в выпадающем списке **Force Key Expiration**. В соответствующих текстовых полях введите временной интервал или количество килобайт, по истечении которых срок действия ключа истечет. Если в одном из полей вы введете ноль, то этот счетчик будет игнорироваться. Если опция **Force Key Expiration** отключена или количество часов и килобайт равны нулю, то Fireware будет использовать по умолчанию ноль килобайт и 8 часов.

10. Два раза нажмите **OK** для того чтобы вернуться в диалоговое окно **Branch Office IPSec Tunnel**.
Созданный вами туннель появится в списке Branch Office IPSec Tunnels

11. Нажмите **Close** и сохраните изменения.

Firebox на Сайте B настроен.

После того, как вы настроили шлюзы и создали туннели на обеих конечных точках туннеля, вы можете по туннелю передавать трафик. Если туннель не работает, проверьте файлы журнала на обоих Firebox за период времени, в течение которого вы пытались создать туннель. В файлах журнала вы должны увидеть, по какой причине туннель не был создан. Вы также можете посмотреть файлы журнала в режиме реального времени в Firebox System Manager.

WatchGuard VPN совместимость: Fireware XTM с Fireware 10.x

BOVPN туннель предоставляет вам защищенный метод передачи данных по незащищенной сети Интернет. В этом документе приводится информация о том, как создать BOVPN туннель вручную.

В этом разделе вы не найдете подробной информации о том, какие параметры используются в диалоговых окнах настроек BOVPN и как они могут повлиять на трафик, передаваемый через туннель. Для более подробной информации о каждом из этих параметров см. Соответствующий раздел:

- BOVPN туннели, созданные вручную
- Настройка шлюзов
- Создание туннелей между конечными точками шлюза

IP адреса и параметры туннеля

Перед тем, как создавать вручную BOVPN туннель, первым делом вам необходимо определить все необходимые IP адреса и параметры, которые будут использоваться на каждом конце туннеля. Вы также можете распечатать этот документ, заполнить все необходимые поля и затем использовать эту информацию при настройке параметров в Policy Manager.

Для этого документа каждая конечная точка туннеля должна иметь внешний статический IP адрес

Если вы являетесь администратором одного из устройств, то вы можете передать эту таблицу со всей необходимой информацией администратору устройства на другом конце туннеля, для того чтобы он ввел корректные параметры \

Если какого-либо параметра нет в списке, значит вам не надо менять его значение по умолчанию.

Проверьте корректность настройки конечных точек VPN туннеля, а также проверьте, чтобы параметры Phase 1 и Phase 2 на обоих устройствах были одинаковы. В противном случае туннель не будет работать.

Параметры BOVPN туннеля:

САЙТ A (Firebox с Fireware XTM 11.x)

Публичный IP адрес: _____

Внутренний IP адрес: _____

САЙТ B (Firebox с Fireware 10.x)

Публичный IP адрес: _____

Внутренний IP адрес: _____

Параметры PHASE 1 (обе стороны должны использовать одинаковые параметры)

*Для BOVPN туннеля между двумя Fireboxe с Fireware XTM, мы рекомендуем включить **Dead Peer Detection (RFC3706)** и не включать **IKE Keep-Alive**. Не включайте сразу две опции. Если на обоих концах туннеля функция Dead Peer Detection поддерживается, то вам всегда необходимо ее включать.*

Данные доступа: Выберите **Use Pre-Shared Key**.

Ключ шифрования (pre-shared key): _____

NAT Traversal: Yes ____ No ____

интервал NAT Traversal Keep-alive: _____

IKE Keep-alive: Yes ____ No ____

интервал IKE Keep-alive Message: _____

Максимальное количество неудачных попыток IKE Keep-alive: _____

Dead Peer Detection (RFC3706): Yes ____ No ____

Таймаут ожидания Dead Peer Detection Traffic: _____

Максимальное количество попыток Dead Peer Detection: _____

Алгоритм аутентификации (выберите один): SHA1____ MD5____

Алгоритм шифрования(выберите один): DES____ 3DES____ AES-128____ AES-192____ AES-256____

Время жизни SA _____

Выберите Hours в качестве единицы измерения времени жизни SA.

Группа Diffie-Hellman (выберите одну): 1____ 2____ 5____

Параметры PHASE 2 (обе стороны должны использовать одинаковые параметры)

Тип: AH ____ ESP ____

Алгоритм аутентификации (выберите один): None____ MD5____ SHA1____

Алгоритм шифрования (выберите один): DES____ 3DES____ AES-128____ AES-192____ AES-256____

Force Key Expiration (выберите один): Enable____ Disable____

Perfect Forward Secrecy (Группа Diffie-Hellman): Disable____ Group1____ Group2____ Group5____

Phase 2 Key Expiration (В часах) _____

Phase 2 Key Expiration (В килобайтах) _____

Пример настроек туннеля

На этой странице показан пример настроек туннеля. Значения всех параметров, приведенных ниже, будут дальше использоваться в описании процедур настройки

САЙТ A (Firebox с Fireware XTM 11.x)

Публичный IP адрес: **50.50.50.50**

Внутренний IP адрес сети: **10.0.50.1/24**

САЙТ B (Firebox с Fireware 10.x)

Публичный IP адрес: **100.100.100.100**

Внутренний IP адрес сети: **192.168.100.1/24**

Параметры PHASE 1 (обе стороны должны использовать одинаковые параметры)

Данные доступа: Выберите **Use Pre-Shared Key**.

Mode (выберите один): Main

Ключ шифрования (Pre-shared key): SiteA2SiteB

NAT Traversal: Yes

Интервал NAT Traversal Keep-alive: 20 секунд

IKE Keep-alive: No

Интервал IKE Keep-alive Message: None

Максимальное количество неудачных попыток IKE Keep-alive: None

Dead Peer Detection (RFC3706): Yes

Таймаут ожидания Dead Peer Detection Traffic: 20 seconds

Максимальное количество попыток Dead Peer Detection: 5

Алгоритм аутентификации (выберите один): SHA1

Алгоритм шифрования(выберите один): 3DES

Время жизни: 8

Выберите Hours в качестве единицы измерения времени жизни SA.

Группа Diffie-Hellman (выберите одну): 2

Параметры PHASE 2 (обе стороны должны использовать одинаковые параметры)

Тип: ESP

Алгоритм аутентификации (выберите один): SHA1

Алгоритм шифрования (выберите один): AES (256 bit)

Force Key Expiration (выберите один): Enable

Perfect Forward Secrecy (Группа Diffie-Hellman): Disable

Phase 2 Key Expiration (В часах): 8

Phase 2 Key Expiration (В килобайтах): 128000

Если вы используете WSM 11.x, то примеры настроек Phase 1 и Phase 2 совпадают с настройками по умолчанию. Они также совпадают с настройками по умолчанию в WSM версии 10.2.2 и выше, также Edge версии 10.2.2 и выше. Они не совпадают с настройками по умолчанию в других версиях Fireware или Edge.

Настройка Сайта A, Fireware XTM 11.x

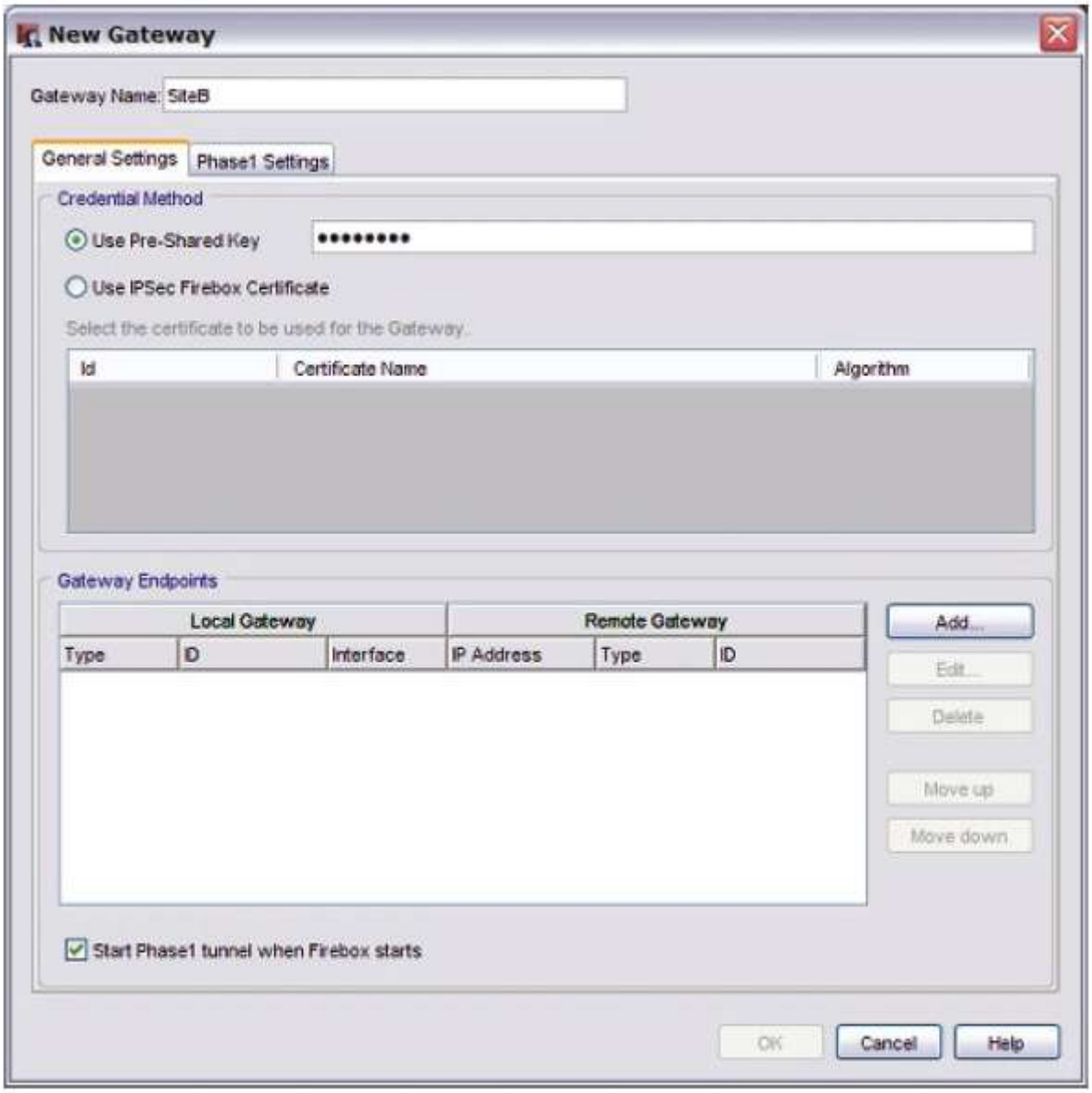
В данном разделе приводится описание настройки шлюза на Сайте A, в котором стоит Firebox с Fireware XTM 11.x. Шлюз – это точка подключения для одного или нескольких туннелей. Для того чтобы настроить шлюз, вам необходимо указать:

- Данные доступа (ключи шифрования или IPSec сертификаты Firebox)
- Местоположение локального и удаленного шлюзов: IP адрес или имя домена
- Параметры Phase 1 для IKE согласования

Создание VPN шлюза

1. В Policy Manager выберите **VPN > Branch Office Gateways**.
   Откроется диалоговое окно Gateways.

2. Для того чтобы добавить новый шлюз нажмите **Add**.
   Откроется диалоговое окно New Gateway



3. В поле **Gateway Name** введите имя, которое будет использоваться для идентификации шлюза в конфигурации Firebox.

4. Выберите закладку **General Settings**.

5. В секции **Credential Method** выберите **Use Pre-Shared Key**. В текстовом поле введите ключ шифрования.
   Ключ шифрования должен состоять только из стандартных ASCII символов.

6. В секции **Gateway Endpoints** нажмите **Add**.
   Откроется диалоговое окно New Gateway Endpoints Settings

7. В секции **Local Gateway** выберите **By IP Address**.

8. В выпадающем списке **IP Address** выберите внешний (публичный) IP адрес для Сайта A. В этом списке содержатся все IP адреса интерфейсов.

9. В поле **External Interface** выберите интерфейс, которому присвоен внешний (публичный) IP адрес Сайта A.

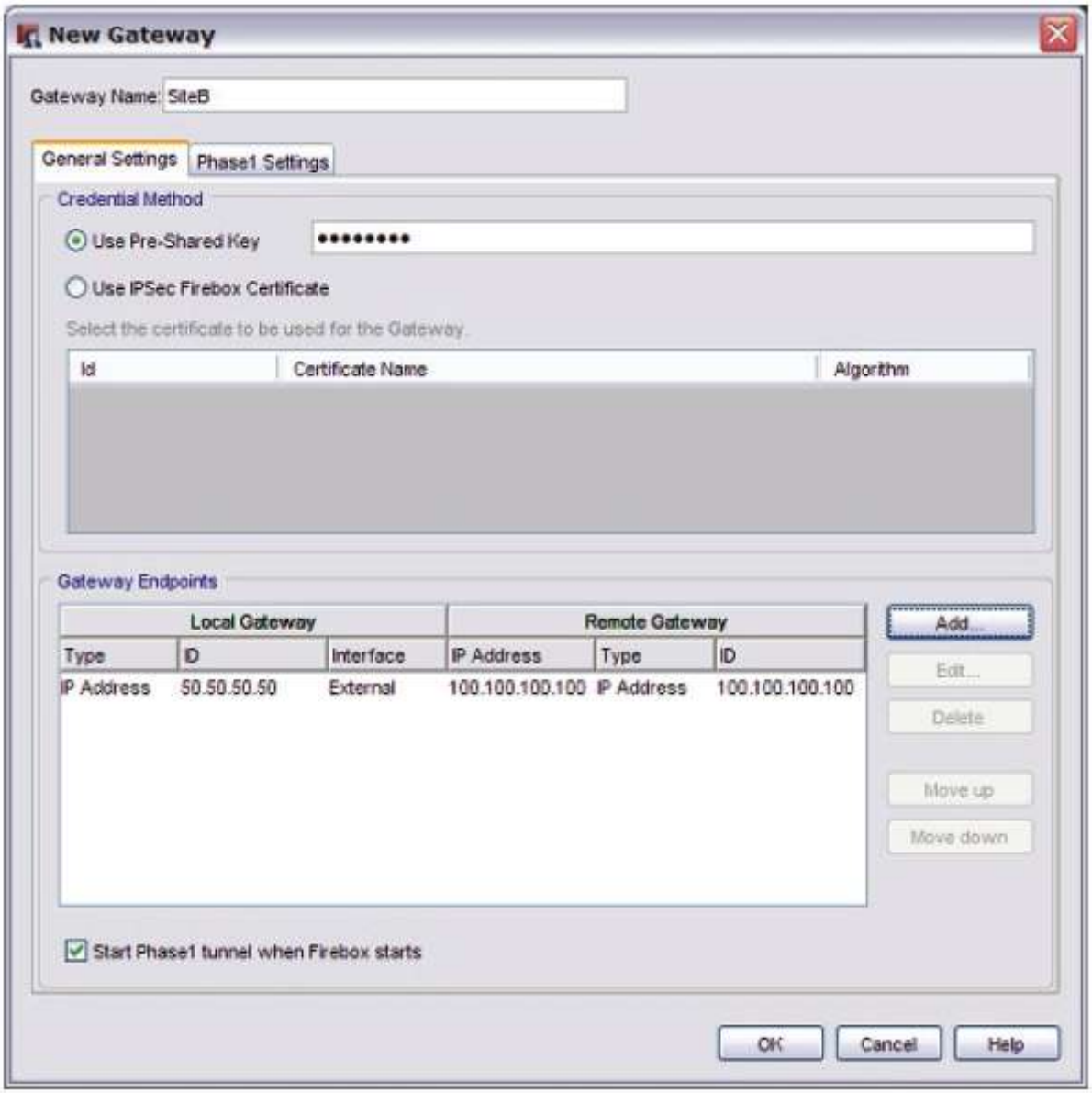
10. В секции **Remote Gateway** для Specify **the remote gateway IP address for a tunnel**, выберите **Static IP Address**.

11. Для **IP Address**, введите внешний (публичный) IP адрес устройства Firebox на Сайте B

12. Выберите **By IP Address** для **Specify the gateway ID for the tunnel authentication**.

13. В поле **IP Address**, введите внешний (публичный) IP адрес устройства Firebox на сайте B.

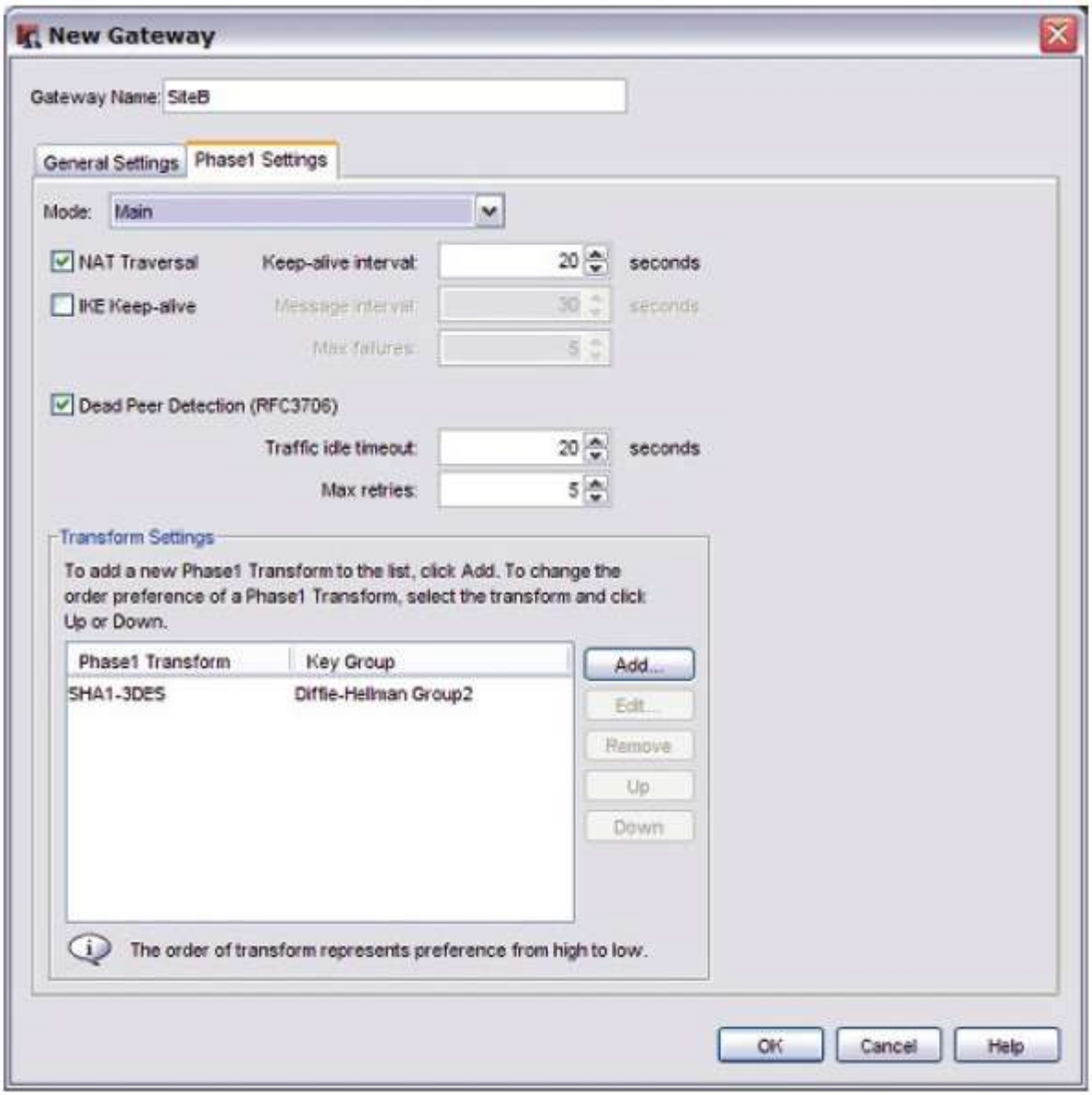
14. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Gateway Endpoints Settings**.
Пара созданных вами шлюзов появится в списке



Настройка параметров Phase 1

Phase 1 IPSec соединения – это фаза создания защищенного, аутентифицированного канала связи. Этот канал связи называется ISAKMP Security Association (SA)

1. Выберите закладку **Phase 1 Settings**.



2. В выпадающем списке **Mode** выберите **Main** или **Aggressive**.
   В примере используется режим Main Mode, так как обе конечные точки туннеля имеют статические IP адреса. Если одна из точек имеет динамический IP адрес, то вам необходимо использовать режим Aggressive mode.

3. На основе информации о параметрах BOVPN туннеля определите, будете ли вы использовать **NAT Traversal**, **IKE Keep-alive** или **Dead Peer Detection (RFC3706)**. Для BOVPN туннеля между Firebox с Fireware XTM, мы рекомендуем выбрать **NAT Traversal** и **Dead Peer Detection**.

4. В секции **Transform Settings** выберите преобразование по умолчанию и нажмите **Edit**

5. В выпадающих списках **Authentication** и **Encryption** выберите алгоритмы аутентификации и шифрования соответственно.

6. В поле SA Life введите время жизни SA и в выпадающем списке выберите Hours, чтобы в качестве единицы измерения времени жизни использовать часы.

7. В выпадающем списке **Key Group** выберите группу Diffie-Hellman.

8. Нажмите **OK**. Все остальные параметры Phase 1 оставьте без изменений.

9. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Gateway**.
Созданный вами шлюз появится в списке Gateways

10. Нажмите **Close** для того чтобы закрыть диалоговое окно **Gateways**.

Создание VPN туннеля

После того, как вы настроите точки шлюза, вы можете между ними создать туннель. Для того чтобы создать туннель, вам необходимо выполнить следующее:

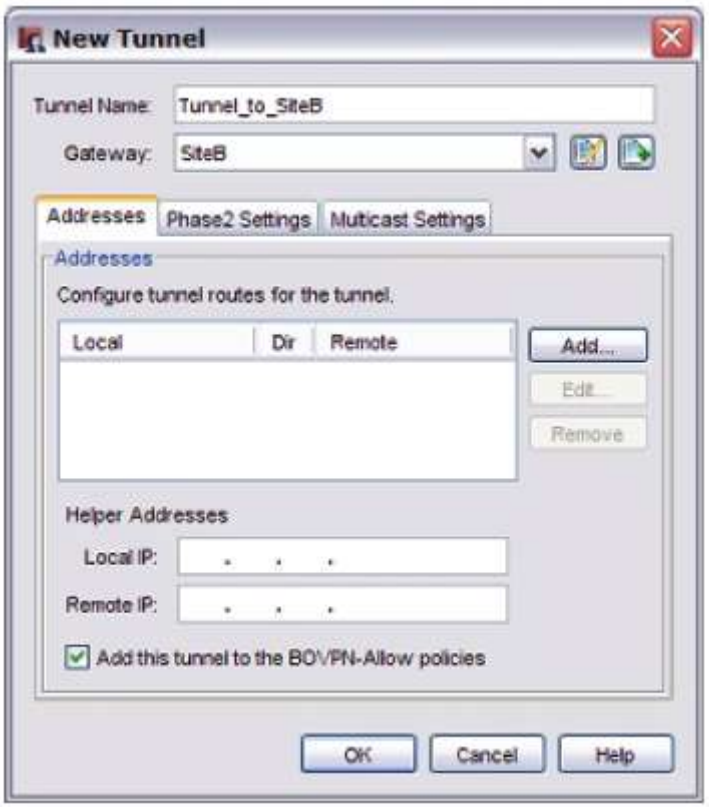
- Создать маршруты (для локальной и удаленной точек туннеля)

- Настроить параметры Phase 2 для IKE. Во время этой фазы создаются ассоциации безопасности (SA) для шифрования пакетов данных:

Для того чтобы создать VPN туннель выполните следующее:

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.
   Откроется диалоговое окно Branch Office IPSec Tunnels.

2. Нажмите **Add**.
   Откроется диалоговое окно New Tunnel



3. В поле **Tunnel Name** введите уникальное имя туннеля (Это имя должно быть уникальным среди имен туннелей, имен групп Mobile VPN и интерфейсов.

4. В списке **Gateway** выберите шлюз для туннеля.

5. Включите опцию **Add this tunnel to the BOVPN-Allow policies** если вы хотите добавить туннель в политики BOVPN-Allow.in и BOVPN-Allow.out. Эти политики разрешают весь трафик, маршрут которого совпадает с маршрутами туннеля. Если вы хотите запретить передачу трафика по туннелю, отключите эту опцию и при помощи мастера BOVPN Policy создайте свои политики, которые будут разрешать передачу определенного типа трафика по туннелю

6. В секции **Addresses** нажмите **Add**.
   Откроется диалоговое окно Tunnel Route Settings

7. В выпадающем списке **Local** выберите локальный (внутренний) адрес сети. Это внутренний адрес сети Сайта A. Вы также можете нажать на кнопку рядом с выпадающим списком **Local** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя. Это устройства, подключенные к локальному Firebox, которые смогут передавать данные по туннелю.

8. В поле **Remote** введите адрес удаленной сети. Это внутренний адрес сети Сайта B. Вы также можете нажать на кнопку рядом с полем **Remote** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя. Это устройства, подключенные к удаленному Firebox, которые смогут передавать данные по туннелю.

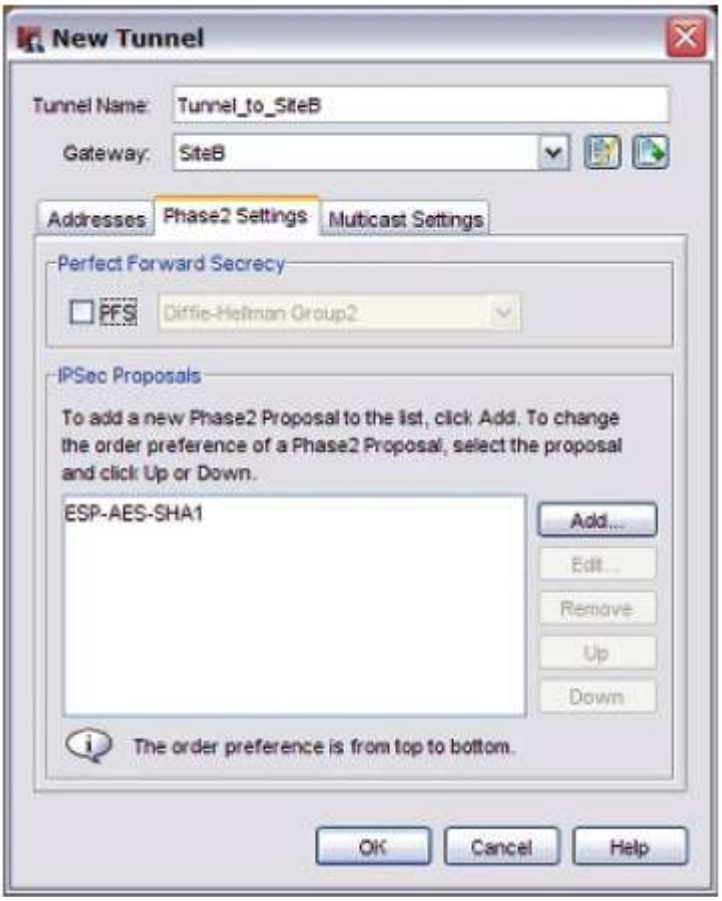
9. В выпадающем списке **Direction** выберите направление для туннеля. Направление определяет, какая конечная точка начнет первой передачу данных по VPN туннелю.

10. Нажмите **OK**.
Маршрут туннеля появится в закладке Addresses диалогового окна New Tunnel.

Настройка параметров Phase 2

Параметры Phase 2 включают параметры SA, которая определяет способ защиты пакетов, передаваемых по туннелю. SA хранит всю необходимую информацию, которую Firebox использует для обработки трафика, передаваемого по защищенному туннелю.

1. В диалоговом окне **New Tunnel** выберите закладку **Phase2 Settings**



2. Включите опцию **PFS** если вы хотите включить Perfect Forward Secrecy (PFS). Если вы включите использование PFS выберите группу Diffie-Hellman.

3. В секции **IPSec Proposals** выберите предложение по умолчанию и нажмите **Remove**.

4. Нажмите **Add**.
   Откроется диалоговое окно New Phase 2 Proposal

5. Выберите **Create a new Phase 2 proposal**.

6. В поле **Name** введите имя нового предложения.

7. В выпадающем списке **Type** выберите **ESP** или **AH**.

8. Выберите алгоритмы аутентификации и шифрования.

9. Вы можете настроить срок действия ключа шифрования. Для того чтобы включить функцию срока действия ключа выберите Enable в выпадающем списке **Force Key Expiration**. В соответствующих текстовых полях введите временной интервал или количество килобайт, по истечении которых срок действия ключа истечет. Если в одном из полей вы введете ноль, то этот счетчик будет игнорироваться. Если опция **Force Key Expiration** отключена или количество часов и килобайт равны нулю, то Fireware будет использовать по умолчанию ноль килобайт и 8 часов.

10. Два раза нажмите **OK** для того чтобы вернуться в диалоговое окно **Branch Office IPSec Tunnel**.
    Созданный вами туннель появится в списке Branch Office IPSec Tunnels

11. Нажмите **Close** и сохраните изменения.

Firebox на Сайте A настроен.

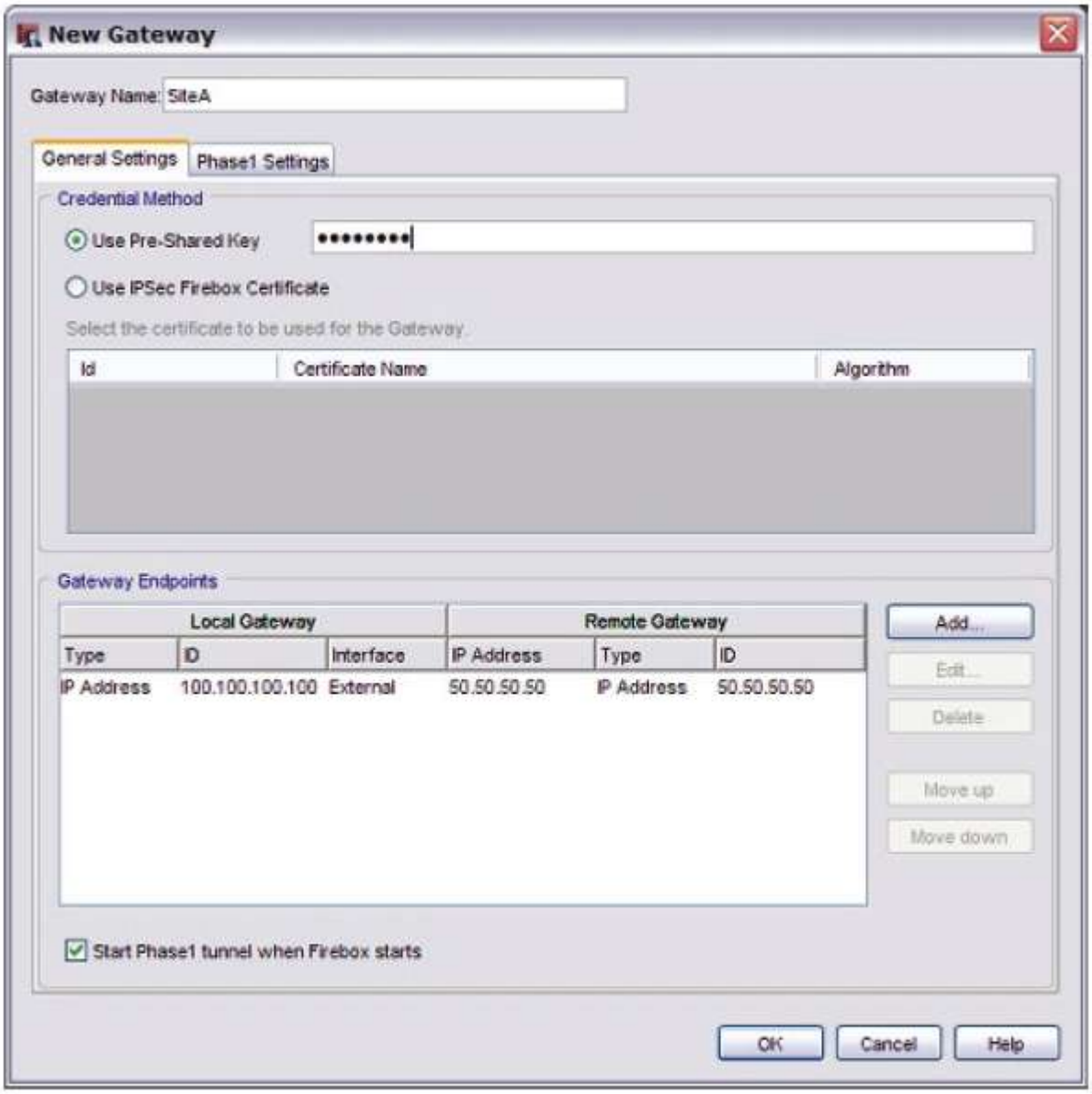
Настройка Сайта B, Fireware 10.x

Теперь вы можете настроить шлюз на Сайте B, на котором стоит Firebox с Fireware 10.x.

Создание VPN шлюза

1. В Policy Manager выберите **VPN > Branch Office Gateways**.
   Откроется диалоговое окно Gateways.

2. Для того чтобы добавить новый шлюз нажмите **Add**.
   Откроется диалоговое окно New Gateway



3. В поле **Gateway Name** введите имя, которое будет использоваться для идентификации шлюза в конфигурации Firebox.

4. Выберите закладку **General Settings**.

5. В секции **Credential Method** выберите **Use Pre-Shared Key**. В текстовом поле введите ключ шифрования.
   Ключ шифрования должен состоять только из стандартных ASCII символов.

6. В секции **Gateway Endpoints** нажмите **Add**.
   Откроется диалоговое окно New Gateway Endpoints Settings

7. В секции **Local Gateway** выберите **By IP Address**.

8. В выпадающем списке **IP Address** выберите внешний (публичный) IP адрес для Сайта B. В этом списке содержатся все IP адреса интерфейсов.

9. В поле **External Interface** выберите интерфейс, которому присвоен внешний (публичный) IP адрес Сайта B.

10. В секции **Remote Gateway** для **Specify the remote gateway IP address for a tunnel**, выберите **Static IP Address**.

11. Для **IP Address**, введите внешний (публичный) IP адрес устройства Firebox на Сайте A.

12. Выберите **By IP Address** для **Specify the gateway ID for the tunnel authentication**.

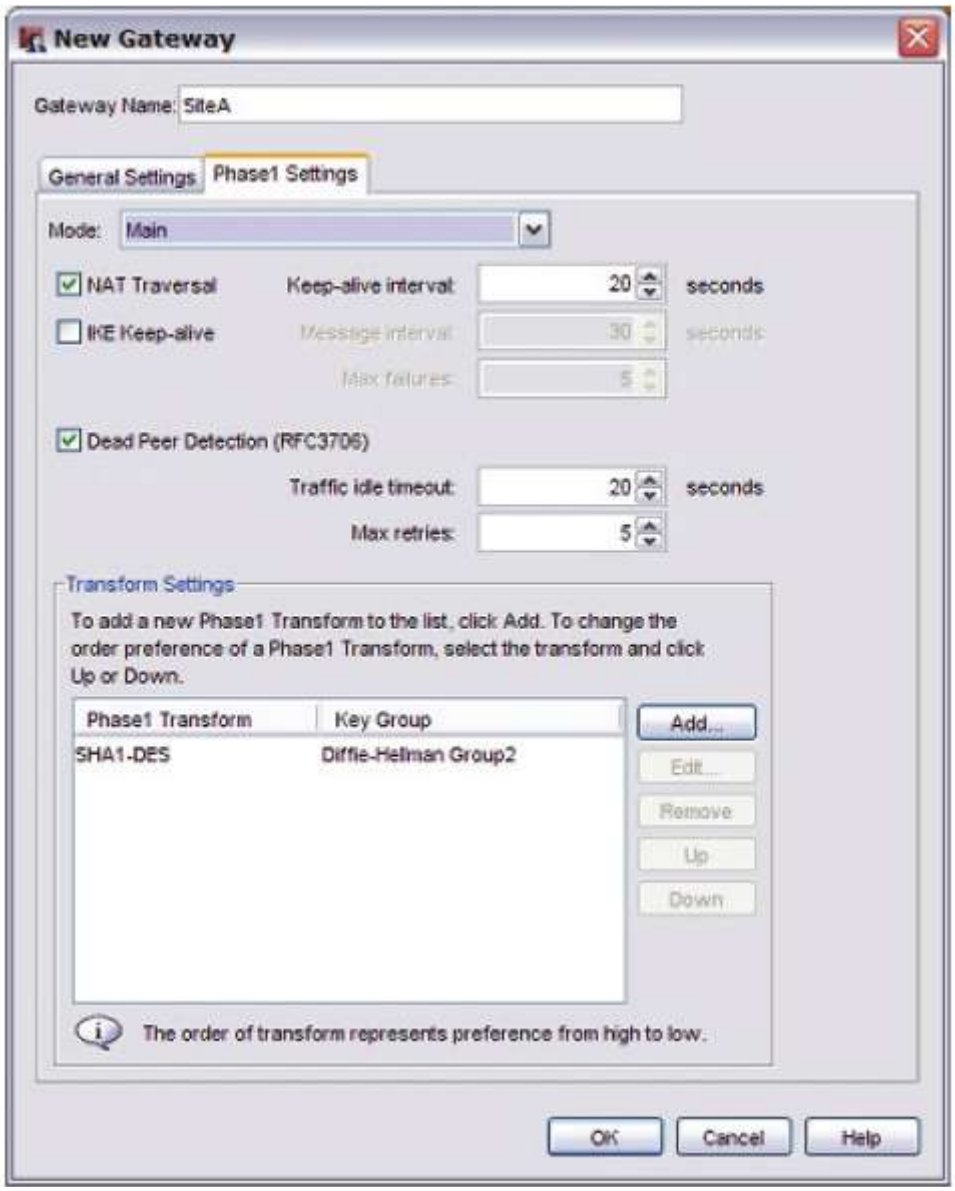
13. В поле **IP Address**, введите внешний (публичный) IP адрес устройства Firebox на сайте A.

14. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Gateway Endpoints Settings**.
   Пара созданных вами шлюзов появится в списке.

Настройка параметров Phase 1

Phase 1 IPSec соединения – это фаза создания защищенного, аутентифицированного канала связи. Этот канал связи называется ISAKMP Security Association (SA)

1. Выберите закладку **Phase 1 Settings**



2. В выпадающем списке **Mode** выберите **Main** или **Aggressive**.

3. На основе информации о параметрах BOVPN туннеля определите, будете ли вы использовать **NAT Traversal**, **IKE Keep-alive** или **Dead Peer Detection (RFC3706)**. Выберите значения, которые вы указали в BOVPN Tunnel Settings.

4. В секции **Transform Settings** выберите преобразование по умолчанию и нажмите **Remove**.

5. Нажмите **Add** для того чтобы добавить новое преобразование

6. В выпадающих списках **Authentication** и **Encryption** выберите алгоритмы аутентификации и шифрования соответственно.

7. В поле **SA Life** введите время жизни SA и в выпадающем списке выберите **Hours**, чтобы в качестве единицы измерения времени жизни использовать часы.

8. В выпадающем списке **Key Group** выберите группу Diffie-Hellman.

9. Нажмите **OK**. Все остальные параметры Phase 1 оставьте без изменений.

10. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Gateway**.

11. Нажмите **Close** для того чтобы закрыть диалоговое окно **Gateways**.

Создание VPN туннеля

После того, как вы настроите точки шлюза, вы можете между ними создать туннель. Для того чтобы создать туннель, вам необходимо выполнить следующее:

- Создать маршруты (для локальной и удаленной точек туннеля)
- Настроить параметры Phase 2 для IKE. Во время этой фазы создаются ассоциации безопасности (SA) для шифрования пакетов данных

Для того чтобы создать VPN туннель выполните следующее:

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.
   Откроется диалоговое окно Branch Office IPSec Tunnels.

2. Нажмите **Add**.
   Откроется диалоговое окно New Tunnel

3. В поле **Tunnel Name** введите уникальное имя туннеля (Это имя должно быть уникальным среди имен туннелей, имен групп Mobile VPN и интерфейсов.

4. В списке **Gateway** выберите шлюз для туннеля.

5. Включите опцию **Add this tunnel to the BOVPN-Allow policies** если вы хотите добавить туннель в политики BOVPN-Allow.in и BOVPN-Allow.out. Эти политики разрешают весь трафик, маршрут которого совпадает с маршрутами туннеля. Если вы хотите запретить передачу трафика по туннелю, отключите эту опцию и при помощи мастера BOVPN Policy создайте свои политики, которые будут разрешать передачу определенного типа трафика по туннелю

6. В секции **Addresses** нажмите **Add**.
   Откроется диалоговое окно Tunnel Route Settings

7. В выпадающем списке **Local** выберите локальный (внутренний) адрес сети. Это внутренний адрес сети Сайта A. Вы также можете нажать на кнопку рядом с выпадающим списком **Local** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя. Это устройства, подключенные к локальному Firebox, которые смогут передавать данные по туннелю.

8. В поле **Remote** введите адрес удаленной сети. Это внутренний адрес сети Сайта B. Вы также можете нажать на кнопку рядом с полем **Remote** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя. Это устройства, подключенные к удаленному Firebox, которые смогут передавать данные по туннелю.

9. В выпадающем списке **Direction** выберите направление для туннеля. Направление определяет, какая конечная точка начнет первой передачу данных по VPN туннелю.

10. Нажмите **OK**.

Настройка параметров Phase 2

Параметры Phase 2 включают параметры SA, которая определяет способ защиты пакетов, передаваемых по туннелю. SA хранит всю необходимую информацию, которую Firebox использует для обработки трафика, передаваемого по защищенному туннелю.

1. В диалоговом окне **New Tunnel** выберите закладку **Phase2 Settings**

2. Включите опцию **PFS** если вы хотите включить Perfect Forward Secrecy (PFS). Если вы включите использование PFS выберите группу Diffie-Hellman.

3. В секции **Security Associations (SA)** нажмите **Settings**

4. В секции **Address Selector** опция **Create one SA that includes all tunnel routes** определяет, создается ли уникальная SA для каждой пары Локальный/Удаленный в настройка VPN туннеля. Мы не рекомендуем включать эту опцию.

5. В секции **Service Selector** выберите **Create one SA that includes all ports and protocols**. Если вы отключите эту опцию, то для каждой уникальный пары порт/протокол будет создаваться SA. Если вам необходимо управлять портами и протоколами, разрешенными в туннеле, мы рекомендуем использовать политику BOVPN. Для более подробной информации см. Define a custom tunnel policy.

6. Нажмите **OK**.
Откроется закладка Phase2 Settings.

7. В секции **IPSec Proposals** выберите предложение по умолчанию и нажмите **Remove**.

8. Нажмите **Add**.
   Откроется диалоговое окно New Phase 2 Proposal

9. Выберите **Create a new Phase 2 proposal**.

10. В поле **Name** введите имя нового предложения.

11. В выпадающем списке **Type** выберите **ESP** или **AH**.

12. Выберите алгоритмы аутентификации и шифрования.

13. Вы можете настроить срок действия ключа шифрования. Для того чтобы включить функцию срока действия ключа выберите Enable в выпадающем списке Force Key Expiration. В соответствующих текстовых полях введите временной интервал или количество килобайт, по истечении которых срок действия ключа истечет. Если в одном из полей вы введете ноль, то этот счетчик будет игнорироваться. Если опция Force Key Expiration отключена или количество часов и килобайт равны нулю, то Fireware будет использовать по умолчанию ноль килобайт и 8 часов.

14. Два раза нажмите **OK** для того чтобы вернуться в диалоговое окно **Branch Office IPSec Tunnel**.
Созданный вами туннель появится в списке Branch Office IPSec Tunnels.

15. Нажмите **Close** и сохраните изменения.

Firebox на Сайте B настроен.

После того, как вы настроили шлюзы и создали туннели на обеих конечных точках туннеля, вы можете по туннелю передавать трафик. Если туннель не работает, проверьте файлы журнала на обоих Firebox за период времени, в течение которого вы пытались создать туннель. В файлах журнала вы должны увидеть, по какой причине туннель не был создан. Вы также можете посмотреть файлы журнала в режиме реального времени в Firebox System Manager.

WatchGuard VPN interoperability: Fireware XTM to Edge 10.x

BOVPN туннель предоставляет вам защищенный метод передачи данных по незащищенной сети Интернет. В этом документе приводится информация о том, как создать BOVPN туннель вручную. В этом разделе вы не найдете подробной информации о том, какие параметры используются в диалоговых окнах настроек BOVPN и как они могут повлиять на трафик, передаваемый через туннель. Для более подробной информации о каждом из этих параметров см. Соответствующий раздел:

- BOVPN туннели, созданные вручную
- Настройка шлюзов
- Создание туннелей между конечными точками шлюза

IP адреса и параметры туннеля

Перед тем, как создавать вручную BOVPN туннель, первым делом вам необходимо определить все необходимые IP адреса и параметры, которые будут использоваться на каждом конце туннеля. Вы также можете распечатать этот документ, заполнить все необходимые поля и затем использовать эту информацию при настройке параметров в Policy Manager.

Для этого документа каждая конечная точка туннеля должна иметь внешний статический IP адрес

Если вы являетесь администратором одного из устройств, то вы можете передать эту таблицу со всей необходимой информацией администратору устройства на другом конце туннеля, для того чтобы он ввел корректные параметры

Если какого-либо параметра нет в списке, значит вам не надо менять его значение по умолчанию.

Проверьте корректность настройки конечных точек VPN туннеля, а также проверьте, чтобы параметры Phase 1 и Phase 2 на обоих устройствах были одинаковы. В противном случае туннель не будет работать.

Параметры BOVPN туннеля:

САЙТ A (Firebox с Fireware XTM 11.x)

Публичный IP адрес: _____

Внутренний IP адрес: _____

САЙТ B (Firebox with Edge 10.x)

Публичный IP адрес: _____

Внутренний IP адрес: _____

Параметры PHASE 1 (Должны совпадать на обоих концах туннеля):

Данные доступа: Выберите **Use Pre-Shared Key**.

Ключ шифрования (pre-shared key): _____

NAT Traversal: Yes ____ No ____

интервал NAT Traversal Keep-alive: _____

интервал IKE Keep-alive Message: _____

Максимальное количество неудачных попыток IKE Keep-alive: _____

Dead Peer Detection (RFC3706): Yes ____ No ____

Таймаут ожидания Dead Peer Detection Traffic: _____

Максимальное количество попыток Dead Peer Detection: _____

Алгоритм аутентификации (выберите один): SHA1____ MD5____

Алгоритм шифрования(выберите один): DES____ 3DES____ AES-128____ AES-192____ AES-256____

Время жизни SA _____

Выберите Hours в качестве единицы измерения времени жизни SA.

Группа Diffie-Hellman (выберите одну): 1____ 2____ 5____

Параметры PHASE 2 (обе стороны должны использовать одинаковые параметры)

Тип: AH ____ ESP ____

Алгоритм аутентификации (выберите один): None____ MD5____ SHA1____

Алгоритм шифрования (выберите один): DES____ 3DES____ AES-128____ AES-192____ AES-256____

Force Key Expiration (выберите один): Enable____ Disable____

Perfect Forward Secrecy (Группа Diffie-Hellman): Disable____ Group1____ Group2____ Group5____

Phase 2 Key Expiration (В часах) _____

Phase 2 Key Expiration (В килобайтах) _____

*Мы рекомендуем включить одну из опций: или **IKE Keep-alive** или **Dead Peer Detection (RFC3706)**. Если оконечные устройства туннеля поддерживают Dead Peer Detection, то включите ее. Если на обоих концах туннеля стоят устройства Watchguard, но одно из них не поддерживает Dead Peer Detection , то включите опцию IKE Keep-alive. IKE Keep-alive используется только устройствами WatchGuard. Не включайте IKE Keep-alive, если одно из устройств на конце туннеля от другого производителя.*

Пример настроек туннеля

На этой странице показан пример настроек туннеля. Значения всех параметров, приведенных ниже, будут дальше использоваться в описании процедур настройки.

САЙТ A (Firebox с Fireware XTM 11.x)

Публичный IP адрес: **50.50.50.50**

Внутренний IP адрес сети: **10.0.50.1/24**

САЙТ B (Firebox с Edge 10.x)

Публичный IP адрес: **100.100.100.100**

Внутренний IP адрес сети: **192.168.100.1/24**

Параметры PHASE 1 (обе стороны должны использовать одинаковые параметры)

Данные доступа: Выберите **Use Pre-Shared Key**.

Mode (выберите один): Main

Ключ шифрования (Pre-shared key): SiteA2SiteB

NAT Traversal: Yes

Интервал NAT Traversal Keep-alive: 20 секунд

IKE Keep-alive: No

Интервал IKE Keep-alive Message: None

Максимальное количество неудачных попыток IKE Keep-alive: None

Dead Peer Detection (RFC3706): Yes

Таймаут ожидания Dead Peer Detection Traffic: 20 seconds

Максимальное количество попыток Dead Peer Detection: 5

Алгоритм аутентификации (выберите один): SHA1

Алгоритм шифрования(выберите один): 3DES

Время жизни: 8

Выберите Hours в качестве единицы измерения времени жизни SA.

Группа Diffie-Hellman (выберите одну): 2

Параметры PHASE 2 (обе стороны должны использовать одинаковые параметры)

Тип: ESP

Алгоритм аутентификации (выберите один): SHA1

Алгоритм шифрования (выберите один): AES (256 bit)

Perfect Forward Secrecy (Группа Diffie-Hellman): Disable

Phase 2 Key Expiration (В часах): 8

Phase 2 Key Expiration (В килобайтах): 128000

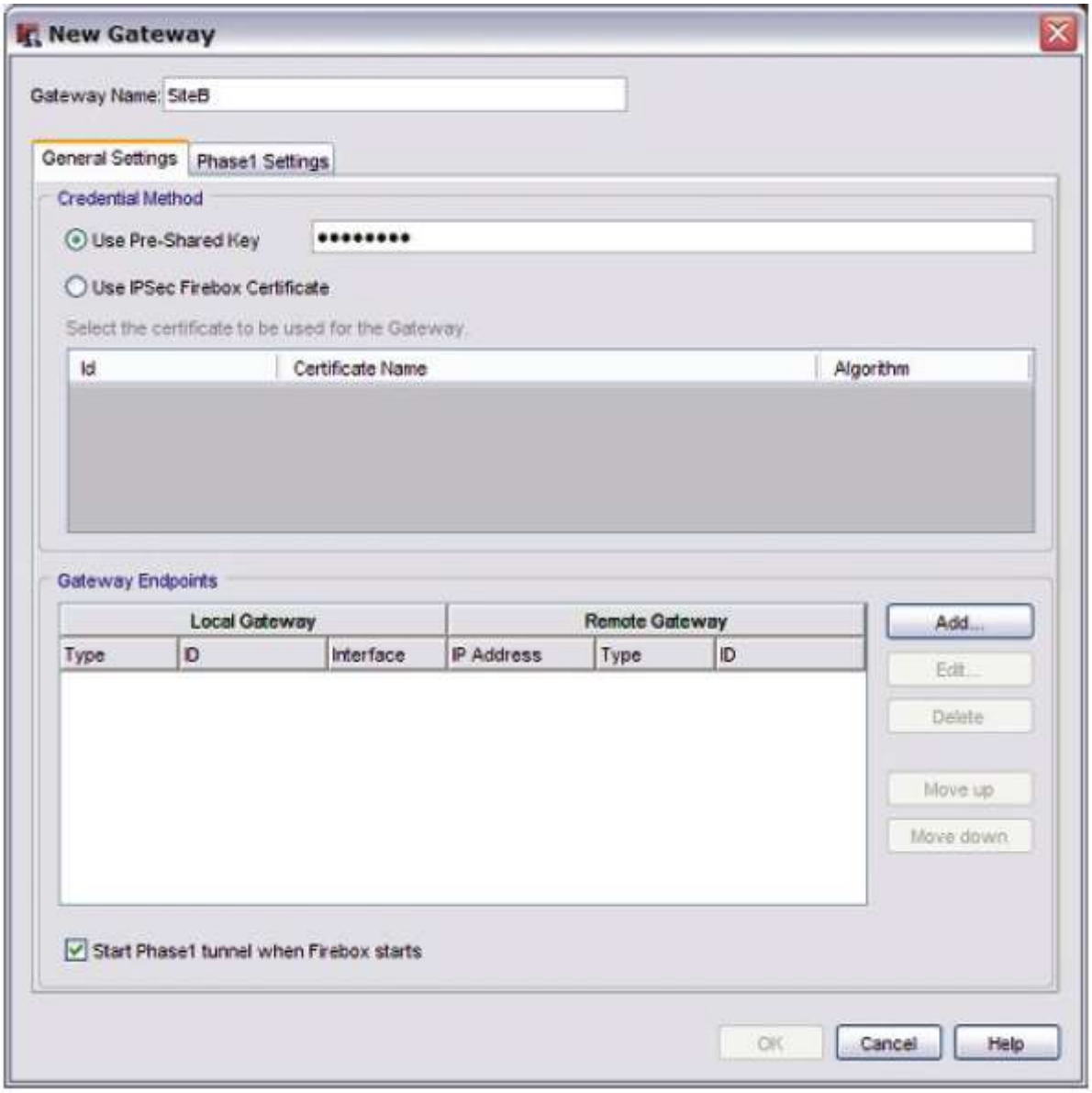
Если вы используете WSM 11.x, то примеры настроек Phase 1 и Phase 2 совпадают с настройками по умолчанию. Они также совпадают с настройками по умолчанию в WSM версии 10.2.2 и выше, также Edge версии 10.2.2 и выше. Они не совпадают с настройками по умолчанию в других версиях Fireware или Edge.

Настройка Сайта A, Fireware 11.x

Для того чтобы создать VPN шлюз выполните следующее:

1. В Policy Manager выберите **VPN > Branch Office Gateways**.
   Откроется диалоговое окно Gateways.

2. Для того чтобы добавить новый шлюз нажмите **Add**.
   Откроется диалоговое окно New Gateway

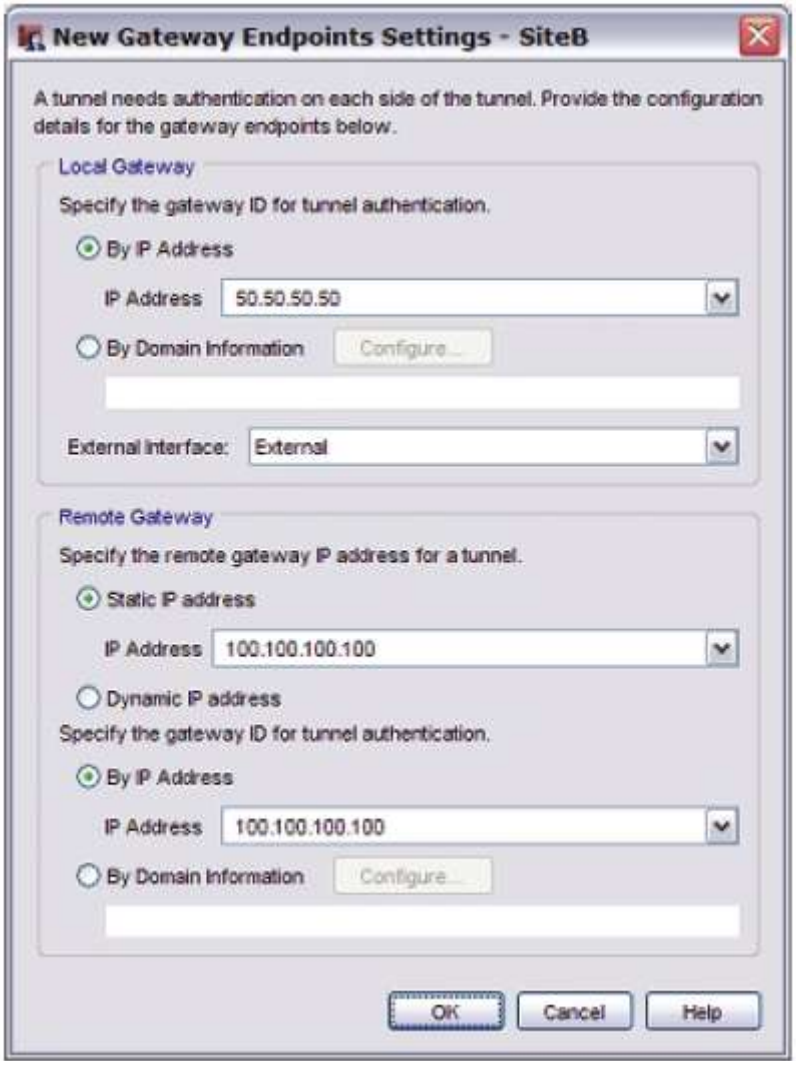


3. В поле **Gateway Name** введите имя, которое будет использоваться для идентификации шлюза в конфигурации Firebox.

4. Выберите закладку **General Settings**.

5. В секции **Credential Method** выберите **Use Pre-Shared Key**. В текстовом поле введите ключ шифрования.
   Ключ шифрования должен состоять только из стандартных ASCII символов.

6. В секции **Gateway Endpoints** нажмите **Add**.
Откроется диалоговое окно New Gateway Endpoints Settings



7. В секции **Local Gateway** выберите **By IP Address**.

8. В выпадающем списке **IP Address** выберите внешний (публичный) IP адрес для Сайта A. В этом списке содержатся все IP адреса интерфейсов.

9. В поле **External Interface** выберите интерфейс, которому присвоен внешний (публичный) IP адрес Сайта A.

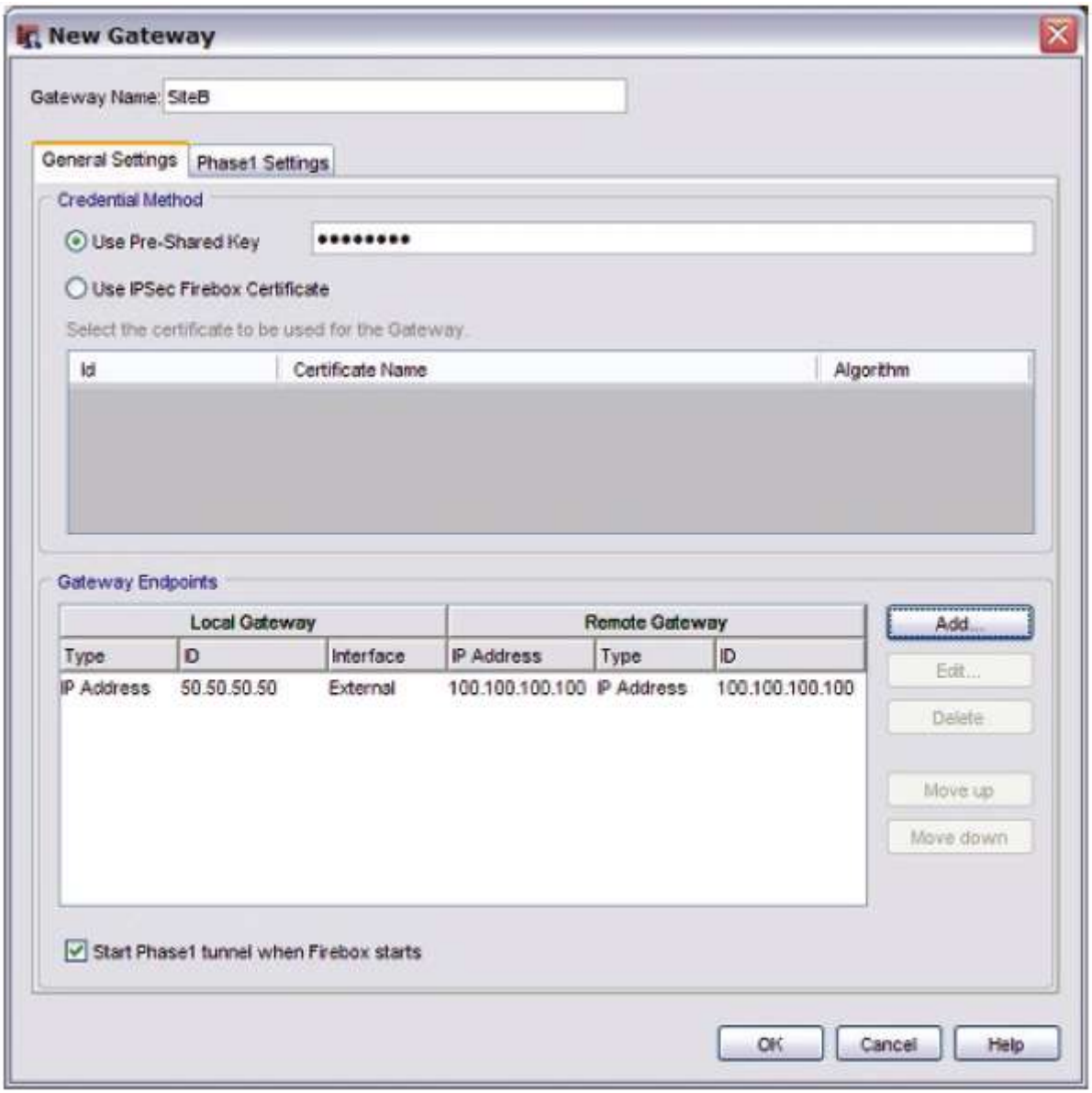
10. В секции **Remote Gateway** для **Specify the remote gateway IP address for a tunnel**, выберите **Static IP Address**.

11. Для **IP Address**, введите внешний (публичный) IP адрес устройства Firebox на Сайте B .

12. Выберите **By IP Address** для **Specify the gateway ID for the tunnel authentication**.

13. В поле **IP Address**, введите внешний (публичный) IP адрес устройства Firebox на сайте B.

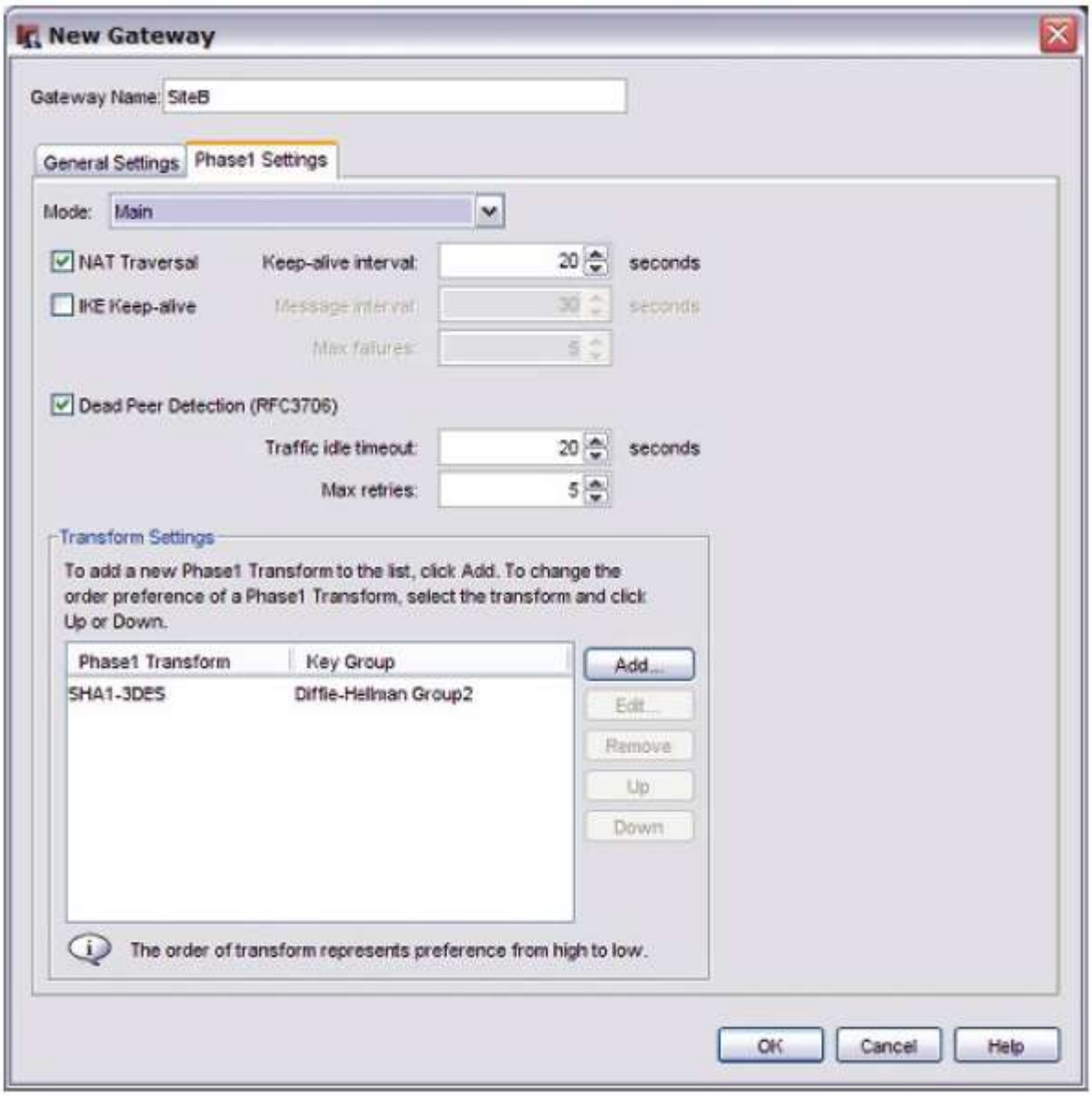
14. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Gateway Endpoints Settings**. *Пара созданных вами шлюзов появится в списке*



Настройка параметров Phase 1

Phase 1 IPSec соединения – это фаза создания защищенного, аутентифицированного канала связи. Этот канал связи называется ISAKMP Security Association (SA)

1. Выберите закладку **Phase 1 Settings**



2. В выпадающем списке **Mode** выберите **Main** или **Aggressive**.
   В примере используется режим Main Mode, так как обе конечные точки туннеля имеют статические IP адреса. Если одна из точек имеет динамический IP адрес, то вам необходимо использовать режим Aggressive mode.

3. На основе информации о параметрах BOVPN туннеля определите, будете ли вы использовать **NAT Traversal**, **IKE Keep-alive** или **Dead Peer Detection (RFC3706)**. Для BOVPN туннеля между Firebox с Fireware XTM и Edge 10.2.2 и выше, мы рекомендуем выбрать **NAT Traversal** и **Dead Peer Detection**.

4. В секции **Transform Settings** выберите преобразование по умолчанию и нажмите **Edit**

5. В выпадающих списках **Authentication** и **Encryption** выберите алгоритмы аутентификации и шифрования соответственно.

6. В поле SA Life введите время жизни SA и в выпадающем списке выберите Hours, чтобы в качестве единицы измерения времени жизни использовать часы.

7. В выпадающем списке **Key Group** выберите группу Diffie-Hellman.

8. Нажмите **OK**. Все остальные параметры Phase 1 оставьте без изменений.

9. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Gateway**.
Созданный вами шлюз появится в списке Gateways

10. Нажмите **Close** для того чтобы закрыть диалоговое окно **Gateways**.

Создание VPN туннеля

После того, как вы настроите точки шлюза, вы можете между ними создать туннель. Для того чтобы создать туннель, вам необходимо выполнить следующее:

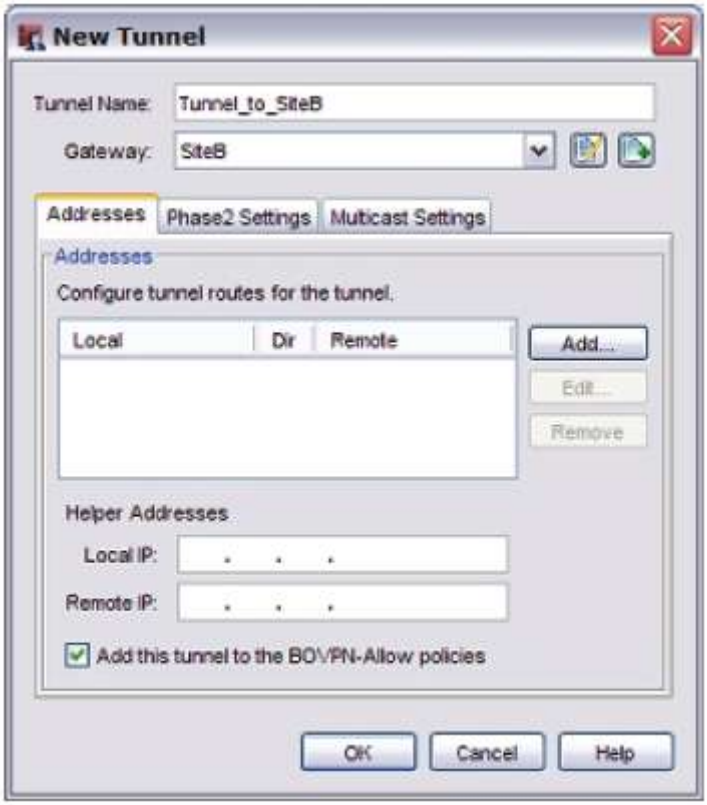
- Создать маршруты (для локальной и удаленной точек туннеля)

- Настроить параметры Phase 2 для IKE. Во время этой фазы создаются ассоциации безопасности (SA) для шифрования пакетов данных:

Для того чтобы создать VPN туннель выполните следующее:

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.
   Откроется диалоговое окно Branch Office IPSec Tunnels.

2. Нажмите **Add**.
   Откроется диалоговое окно New Tunnel



3. В поле **Tunnel Name** введите уникальное имя туннеля (Это имя должно быть уникальным среди имен туннелей, имен групп Mobile VPN и интерфейсов.

4. В списке **Gateway** выберите шлюз для туннеля.

5. Включите опцию **Add this tunnel to the BOVPN-Allow policies** если вы хотите добавить туннель в политики BOVPN-Allow.in и BOVPN-Allow.out. Эти политики разрешают весь трафик, маршрут которого совпадает с маршрутами туннеля. Если вы хотите запретить передачу трафика по туннелю, отключите эту опцию и при помощи мастера BOVPN Policy создайте свои политики, которые будут разрешать передачу определенного типа трафика по туннелю

6. В секции **Addresses** нажмите **Add**.
   Откроется диалоговое окно Tunnel Route Settings

7. В выпадающем списке **Local** выберите локальный (внутренний) адрес сети. Это внутренний адрес сети Сайта A. Вы также можете нажать на кнопку рядом с выпадающим списком **Local** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя. Это устройства, подключенные к локальному Firebox, которые смогут передавать данные по туннелю.

8. В поле **Remote** введите адрес удаленной сети. Это внутренний адрес сети Сайта B. Вы также можете нажать на кнопку рядом с полем **Remote** и ввести IP адрес хоста, адрес сети, диапазон IP адресов или DNS имя. Это устройства, подключенные к удаленному Firebox, которые смогут передавать данные по туннелю.

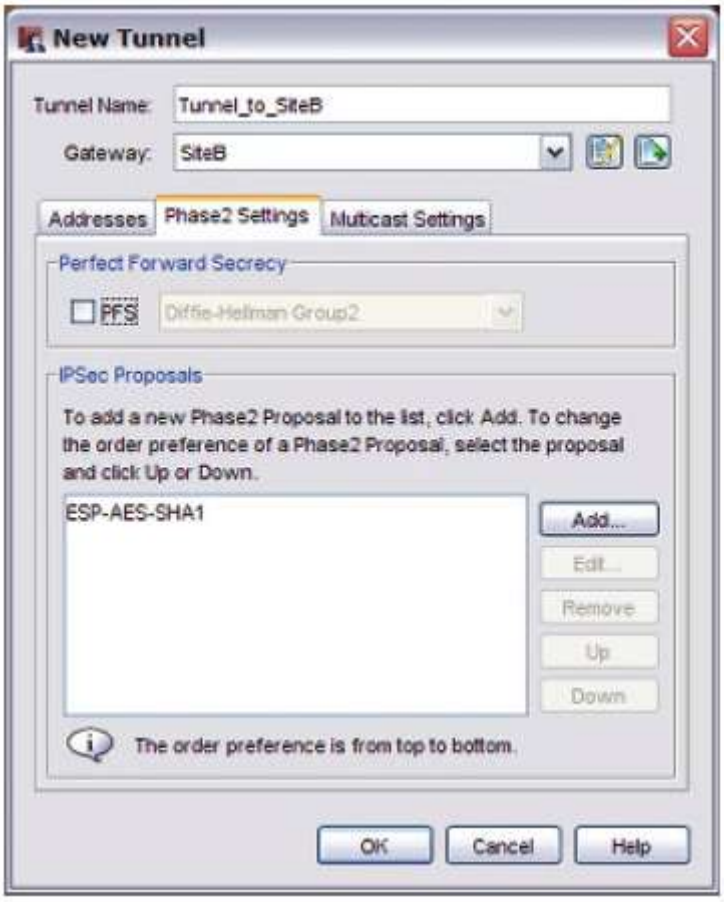
9. В выпадающем списке **Direction** выберите направление для туннеля. Направление определяет, какая конечная точка начнет первой передачу данных по VPN туннелю.

10. Нажмите **OK**.
    Маршрут туннеля появится в закладке Addresses диалогового окна New Tunnel.

Настройка параметров Phase 2

Параметры Phase 2 включают параметры SA, которая определяет способ защиты пакетов, передаваемых по туннелю. SA хранит всю необходимую информацию, которую Firebox использует для обработки трафика, передаваемого по защищенному туннелю.

1. В диалоговом окне **New Tunnel** выберите закладку **Phase2 Settings**



2. Включите опцию **PFS** если вы хотите включить Perfect Forward Secrecy (PFS). Если вы включите использование PFS выберите группу Diffie-Hellman.

3. В секции **IPSec Proposals** выберите предложение по умолчанию и нажмите **Remove**.

4. Нажмите **Add**.
   Откроется диалоговое окно New Phase 2 Proposal

5. Выберите **Create a new Phase 2 proposal**.

6. В поле **Name** введите имя нового предложения.

7. В выпадающем списке **Type** выберите **ESP** или **AH**.

8. Выберите алгоритмы аутентификации и шифрования.

9. Вы можете настроить срок действия ключа шифрования. Для того чтобы включить функцию срока действия ключа выберите Enable в выпадающем списке Force Key Expiration. В соответствующих текстовых полях введите временной интервал или количество килобайт, по истечении которых срок действия ключа истечет. Если в одном из полей вы введете ноль, то этот счетчик будет игнорироваться. Если опция Force Key Expiration отключена или количество часов и килобайт равны нулю, то Fireware будет использовать по умолчанию ноль килобайт и 8 часов.

10. Два раза нажмите **OK** для того чтобы вернуться в диалоговое окно **Branch Office IPSec Tunnel**.
    Созданный вами туннель появится в списке Branch Office IPSec Tunnels

11. Нажмите **Close** и сохраните изменения.

Firebox на Сайте A настроен.

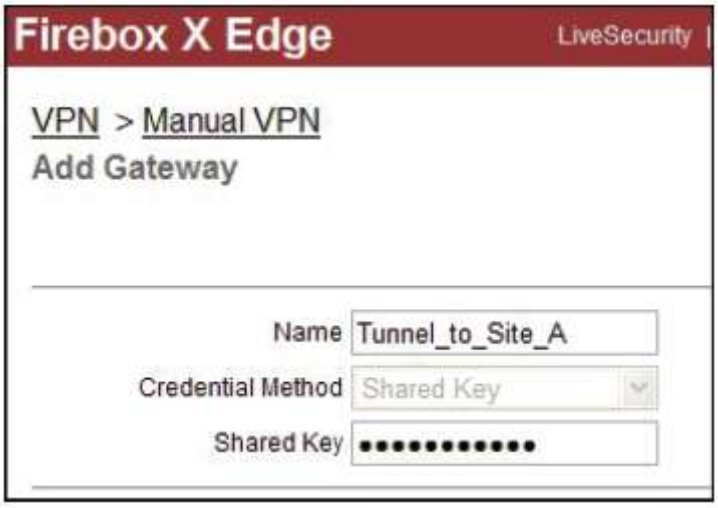
Настройка Сайта B, Edge 10.x

Теперь вы можете настроить шлюз на Сайте B, на котором стоит Firebox X Edge.

1. Через браузер зайдите на страницу System Status устройства Edge.
   По умолчанию IP адрес равен: 192.168.111.1.

2. В панели навигации слева выберите **VPN > Manual VPN**.
   Откроется страница Manual VPN

3. Нажмите на кнопку **Add**.
   Откроется страница Add Gateway

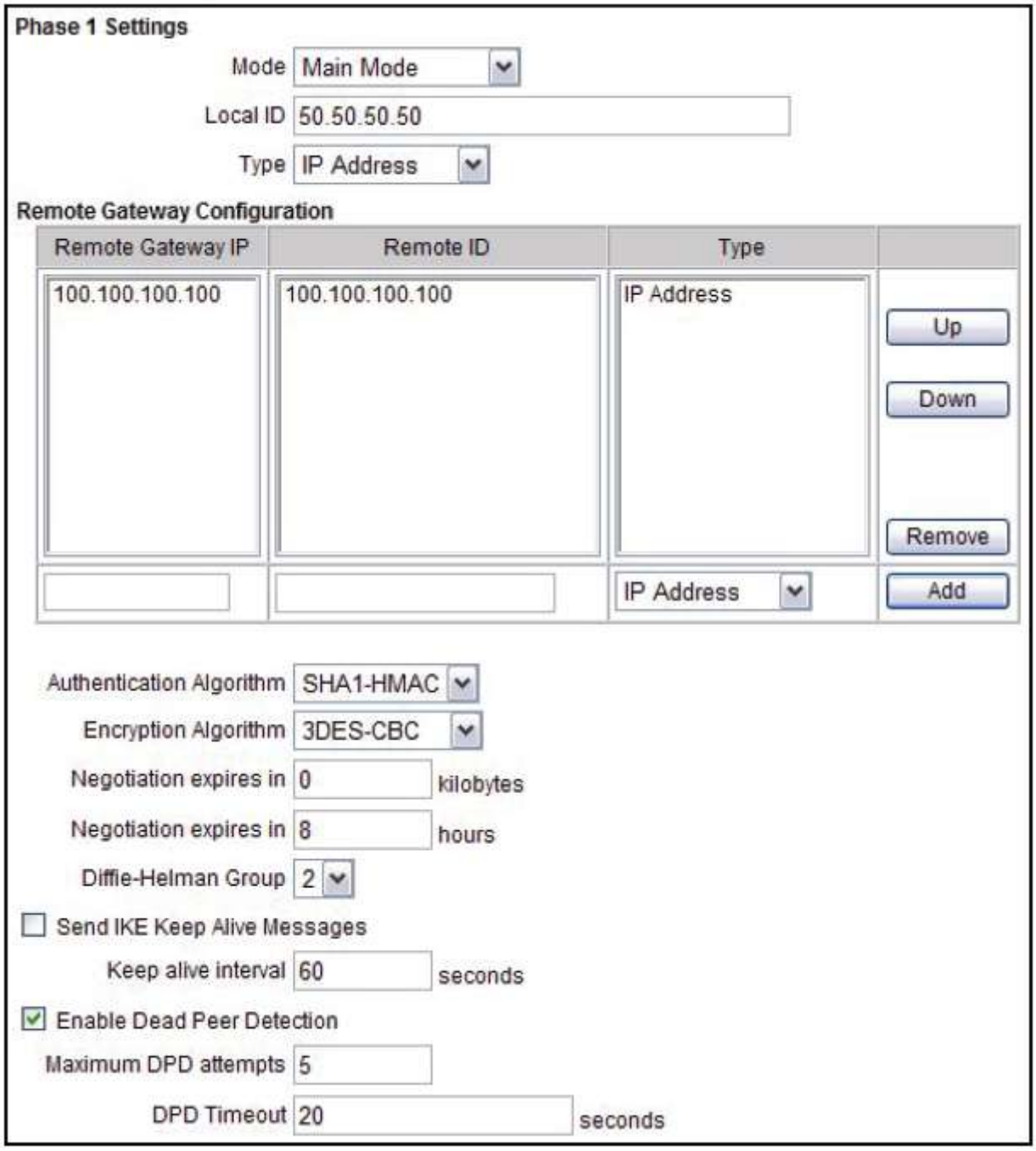


4. Введите имя для IPSec туннеля. При вводе используйте только стандартные ASCII символы без пробелов.
   Это имя необязательно должно совпадать с именем туннеля на Fireware Firebox.

5. В поле **Credential Method** выберите **Shared Key**.

6. В поле **Shared Key**, введите тот же ключ шифрования, который вы ввели в конфигурации Сайта A.

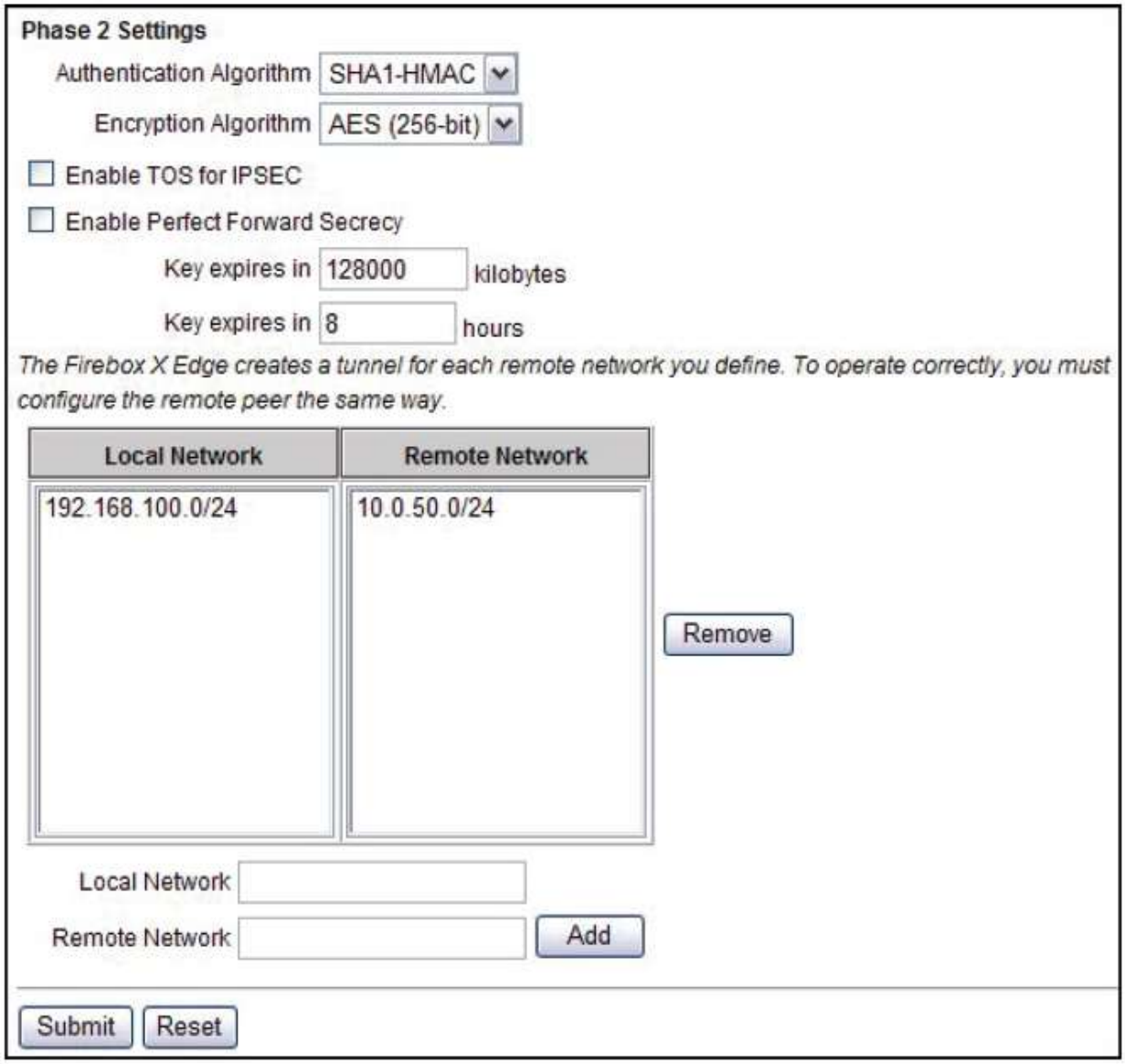
Настройка параметров Phase 1



1. Выберите режимы **Main Mode** или **Aggressive Mode**.
2. Рядом с полем **Local ID**, введите публичный IP адрес устройства Edge.
3. Рядом с полем **Type** выберите **IP Address**.
4. В секции **Remote Gateway Configuration** в нижней части колонки **Type** выберите **IP Address**.
5. В нижней части колонок **Remote Gateway IP** и **Remote ID** введите публичный IP адрес устройства Firebox на Сайте A.
6. Нажмите на кнопку **Add**.
7. Выберите алгоритмы аутентификации и шифрования.

8. В полях **Negotiation expires in** введите количество часов и килобайт.
9. Выберите группу Diffie-Hellman (**Diffie-Hellman Group**): **1**, **2** или **5**.
10. В зависимости от настроек вашего BOVPN туннеля выберите **Send IKE Keep-alive Messages** или **Dead Peer Detection**.

Настройка параметров Phase 2



1. Выберите алгоритм аутентификации и шифрования.
2. НЕ включайте опцию **Enable TOS for IPSec**.
3. Не включайте опцию **Enable Perfect Forward Secrecy**.
4. В полях **Key expires in** введите количество килобайт (**kilobytes**) и часов(**hours**).
5. В поле **Local Network** введите адрес сети внутренней сети Сайта B.
6. В поле **Remote Network** введите адрес внутренней сети Сайта A.
7. Нажмите на кнопку **Add**.

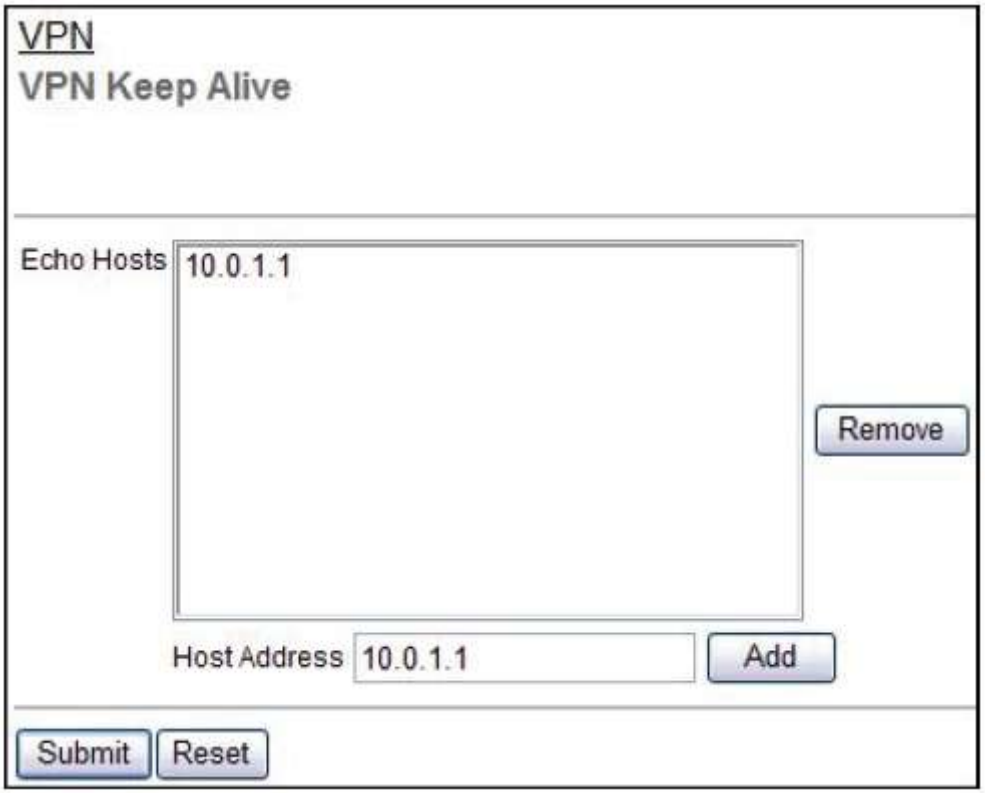
8. Для того чтобы сохранить все выполненные изменения нажмите на кнопку **Submit**.

Настройка VPN Keep Alive

Для того чтобы держать VPN туннель открытым, даже при отсутствии трафика через него, вы можете использовать IP адрес устройства на другом конце в качестве echo хоста, на который Firebox будет каждую минуту отправлять ping-запрос. В качестве echo хоста используйте устройство, которое постоянно включено и может отвечать на ping запросы. Вы можете использовать несколько IP адресов, на которые Firebox будет отправлять ping-запросы разным хостам через различные туннели.

1. Для того чтобы подключиться к странице System Status введите `https://` и IP адрес trusted интерфейса Firebox X Edge.
   По умолчанию используется следующий URL is: https://192.168.111.1

2. В панели навигации выберите **VPN > VPN Keep Alive**.
   Откроется страница VPN Keep Alive



3. Введите IP адрес echo хоста. Нажмите **Add**.

4. Повторите п. 3 для того чтобы добавить еще несколько echo хостов.

5. Нажмите **Submit**.

Устройство Edge на Сайте B теперь настроено.

После того, как вы настроили шлюзы и создали туннели на обеих конечных точках туннеля, вы можете по туннелю передавать трафик. Если туннель не работает, проверьте файлы журнала на обоих Firebox за период времени, в течение которого вы пытались создать туннель. В файлах журнала вы должны увидеть, по какой причине туннель не был создан. Вы также можете посмотреть файлы журнала в режиме реального времени в Firebox System Manager. Для того чтобы посмотреть сообщения журнала на устройстве Edge, нажмите **Logging** в Firebox X Edge Web Manager.

Улучшение работы BOVPN туннелей

Бывают случаи, когда BOVPN туннель корректно настроен, но не всегда работает так как надо. В этом разделе содержится информация, которая поможет вам решить проблемы, связанные с проблемами передачи трафика по BOVPN туннелям. Информация, приведенная в этом разделе, не используется для улучшения производительности BOVPN туннеля.

Существует основные три причины некорректной работы BOVPN туннелей:

- Одна или обе конечные точки туннеля имеют нестабильное подключение к внешней сети. Большая задержка, высокая степень фрагментации пакетов и большие потери пакетов приводят к нестабильности соединения. Эти факторы оказывают значительное влияние на BOVPN трафик, так как в отличие от обычного трафика, BOPVN пакеты передаются в зашифрованном виде, на приемном конце их необходимо расшифровывать, а затем собирать по порядку, и затем только отправлять получателю.

- Одно из устройств на конце туннеля не WatchGuard устройство, или устройство WatchGuard с более старым ПО. Тесты совместимости между новыми продуктами WatchGuard и более старыми версиями устройств выполнялись с использованием последних версий ПО, которое доступно для более старых устройств. Если вы используете более старое ПО, то у вас возникнуть проблемы, которые были устранены в более новых релизах ПО. WatchGuard устройства используют стандарт IPSec, тем самым они совместимы с многими другими IPSec устройствами. Однако, существуют устройства, которые работают не по стандарту, соответственно с этими устройствами могут возникнуть проблемы.

- Если по туннелю передается небольшое количество или в течение достаточного длительного промежутка времени трафик по туннелю не передавался, некоторые устройства могут закрыть VPN соединение. WatchGuard устройства, на которых установлен Fireware и устройства WatchGuard Edge не закрывают VPN соединение, однако некоторые IPSec устройства и устройства WatchGuard с ранними версиями WFS в случае отсутствия трафика в течение определенного промежутка времени, будут закрывать соединение.

Вы можете установить последние версии ОС и ПО управления на все устройства WatchGuard, однако все равно это не исключает возможности возникновения такой ситуации. Однако вы можете предпринять некоторые действия по улучшению работы BOVPN туннеля.

IKE Keep-alive или Dead Peer Detection

Обе опции, IKE Keep-alive и Dead Peer Detection, используются для проверки включенности туннеля. Если они обнаруживают, что туннель не работает, они запускают процедуру Phase 1 согласования. Если вы включите обе опции, то начало процедуры Phase 1 согласования может привести к тому, что вторая опция обнаружит, что туннель перестал работать, и запустить вторую процедуру Phase 1 согласования. При этом трафик через туннель не будет передаваться до тех пор, пока параметры туннеля заново не будут согласованы. Для того чтобы обеспечить стабильную работу туннеля, выберите только одну из опций.

Важно помнить следующее:

*Опция **IKE Keep-alive** используется только устройствами WatchGuard. Если какое-либо из оконечных устройств туннеля эту опцию не поддерживают, то не используйте эту опцию.*

После того, как вы включите опцию IKE Keep-alive, Firebox будет с определенной периодичностью отправлять сообщения на удаленный шлюз и ждать на них ответа. Значение **Message interval** определяет частоту отправки этих сообщений. Значение **Max Failures** определяет максимальное количество запросов, ответ на которые не были получены, после чего конечные устройства туннеля запускают процедуру Phase 1 согласования.

Dead Peer Detection – это промышленный стандарт, который используется большинством IPSec устройств. Если оконечные устройства туннеля поддерживают опцию Dead Peer detection, то включите ее.

После того, как вы включите опцию Dead Peer Detection, Firebox будет выполнять мониторинг трафик, передаваемого по туннелю. Если от удаленного устройства в течение определенного промежутка (поле **Traffic idle timeout**) времени трафик не приходит, то Firebox на удаленный шлюз отправляет запрос. Если на определенное количество запросов (поле **Max retries**) не было получено ответа, то Firebox запускает процедуру Phase 1 согласования. Для более подробной информации о Dead Peer Detection см. http://www.ietf.org/rfc/rfc3706.txt.

Настройка IKE Keep-alive и Dead Peer Detection является частью процедуры настройки параметров Phase 1.

1. В Policy Manager выберите **VPN > Branch Office Gateways**.
2. Выберите шлюз и нажмите **Edit**.
3. Выберите закладку **Phase 1 Settings**.

Настройки по умолчанию

Настройки BOVPN по умолчанию обеспечивают оптимальный уровень безопасности и скорости передачи данных. При возможности используйте эти настройки. Если удаленное устройство не поддерживает какой-либо из параметров, установленных по умолчанию, то выполните необходимые настройки. Для WSM 11.0 используются следующие настройки по умолчанию:

Если параметр не отображается в WSM, то его значение вы изменить его не можете.

Общие параметры (General Settings)	
Mode	Режим Main (Выберите Aggressive если одно из ройств имеет динамический внешний IP адрес)
NAT Traversal	Да
Интервал NAT Traversal Keep-alive	20 секунд
IKE Keep-alive	Отключен
Интервал сообщений IKE Keep-alive	-
Максимальное количество неудачных попыток IKE Keep-alive	-
Dead Peer Detection (RFC3706)	Включен
Таймаут ожидания трафика Dead Peer Detection	20 секунд
Максимальное количество попыток Dead Peer Detection	5
Параметры Phase 1 преобразования	

Алгоритм аутентификации	SHA-1
Алгоритм шифрования	3DES
Время жизни SA (в часах)	8
Время жизни SA (в килобайтах)	0
Группа Diffie-Hellman	2
Параметры Phase 2 предложения	
Тип	ESP
Алгоритм аутентификации	SHA-1
Алгоритм шифрования	3DES
Force Key Expiration	Включен
Срок действия ключа Phase 2 (в часах)	8
Срок действия ключа Phase 2 (в килобайтах)	128000
Perfect Forward Secrecy	Отключен
Группа Diffie-Hellman	-

Передача файлов журнала через туннель

Если через туннель в течение определенного промежутка времени не передается трафик, конечное устройство может решить, что второе устройство недоступно, и не запускать немедленно процедуру пересоздания VPN туннел. Одним из способов проверить, передается ли трафик по туннелю, это попытаться передать файлы журнала по туннелю. При этом вам не нужен Сервер Журналов для получения и записи данных журнала в файл. В этом случае Firebox будет отправлять данные журнала на несуществующий Сервер Журнала, что позволит создать небольшую нагрузку на туннель и обеспечить стабильность его работы.

Существует два типа данных журнала: журналы WatchGuard и syslog. Если Firebox отправляет данные журнала на Сервер Журнала WatchGuard и syslog сервер, то вы не можете использовать этот метод для передачи трафика через туннель.

Вам необходимо выбрать IP адрес Сервер Журнала, на который будут отправлять данные журнала. Для того чтобы выбрать IP адрес выполните следующее.

- IP адрес Сервера Журнала должен быть указан в настройках маршрутов туннеля на удаленном устройстве

- IP адрес Сервера Журнала не должен использоваться реальным устройством.

Два типа журналов создают различное количество трафика.

WatchGuard журналы

По туннелю не будет передаваться никаких данных, до тех пор пока Firebox не подключится к Серверу Журналов. Единственный тип трафика, который передается через туннель, это попытки подключения к Серверу Журналов. Этого трафика будет достаточно для стабильной работы туннеля.

Syslog журналы

Данные сразу отправляются на syslog сервер. Объем передаваемых данных зависит от объема трафика, обслуживаемого Firebox. Syslog генерирует достаточное количество трафика для обеспечения стабильной работы туннеля.

Для обеспечения стабильности и наименьшего влияния на реальный трафик, сначала попробуйте использовать WatchGuard журналы. Если это не поможет, то попробуйте syslog журналы. е

В приведенных ниже процедурах подразумевается, что оконечными устройствами туннеля являются WatchGuard Firebox и ни одно из устройств не отправляет данные журнала на Сервер Журнала WatchGuard или syslog сервер. Если одна и конечных точек туннеля отправляет данные журнала на один из серверов, то не меняйте эти настройки.

Вы можете использовать следующие варианты:

- Одно из устройств на конце туннеля будет отправлять данные журнала WatchGuard через туннель.

- Другое устройство будет отправлять данные журнала WatchGuard через туннель.

- Оба устройства отправляют данные журнала WatchGuard через туннель.

- Одно из устройств на конце туннеля будет отправлять syslog трафик через туннель.

- Другое устройство будет отправлять syslog трафик через туннель.

- Оба устройства отправляют syslog трафик через туннель..

Передача данных журнала WatchGuard через туннель

1. В Policy Manager выберите **Setup > Logging**.

2. Выберите Send log messages to the log servers at these IP addresses и нажмите Configure.

3. Нажмите **Add**.
   Откроется диалоговое окно Add Event Processor.

4. В поле **Log Server Address** введите IP адрес Сервера Журналов.

5. В поле **Encryption Key** введите ключ шифрования. В поле **Confirm Key** введите ключ шифрования еще раз.
   Длина ключа шифрования - 8–32 символов. Вы можете использовать все символы, кроме пробелов и косых черт (/ or \).

6. Нажмите **OK** три раза.

Передача syslog трафика через туннель

1. В Policy Manager выберите **Setup > Logging**.
2. Выберите **Send log messages to the Syslog server at this IP addresses**.
3. Введите IP адрес syslog сервера в текстовом поле.
4. Нажмите **OK**

Глава 27 - Mobile VPN with PPTP

Mobile VPN with PPTP

Mobile VPN для создания безопасного соединения использует протокол PPTP(Point-to-Point Tunneling Protocol). Для каждого Firebox он поддерживает одновременно до 50 пользователей. Пользователи Mobile VPN могут аутентифицироваться на устройство Firebox или на сервер аутентификации RADIUS. Вам необходимо настроить Firebox и компьютеры-хосты удаленных пользователей

Требования к Mobile VPN with PPTP

Перед тем, как настраивать WatchGuard устройство для работы с Mobile VPN with PPTP, убедитесь, что у вас вся необходимая информация, приведенная ниже:

IP адреса удаленных пользователей, которые будут использовать для Mobile VPN with PPTP сессий.

- Для Mobile VPN with PPTP туннелей устройство WatchGuard выдает каждому удаленному пользователя виртуальный IP адрес. Эти виртуальные IP адрес не должны принадлежать диапазону адресов, который используется в вашей внутренней сети, защищенной устройством WatchGuard. Наиболее безопасным вариантом выдачи адресов для пользователей Mobile VPN будет установка "placeholder" вторичной сети. Затем из этого диапазона выбрать IP-адрес. Например, вы можете создать подсеть, которая будет вторичной сетью для вашей доверенной сети 10.10.0.0/24. Выберите IP-адреса в этой подсети для диапазона PPTP адресов.

- IP адреса WINS и DNS серверов, которые используются для поиска IP адресов по именам хостов

- Имена пользователей и пароли пользователей, которым разрешено подключаться к Firebox с использованием Mobile VPN.

Уровни шифрования

Для Mobile VPN with PPTP вы можете выбрать 128-битное или 40-битное шифрование. Американские версии Windows XP поддерживают 128-битное шифрование. Для остальных версий Windows вы можете получить у компании Microsoft специальный патч. Firebox сначала пытается использовать 128-битное шифрование. Если клиент не может использовать 128-битное шифрования, то Firebox использует 40-битное (если оно включено)

Если вы живете за пределами США и вам необходимо разрешение использовать «сильное» шифрование для вашей учетной записи LiveSecurity Service, то на адрес supportid@watchguard.com отправьте электронное письмо, в котором должна содержаться следующая информация:

- Номер ключа Сервиса LiveSecurity

- Дата приобретения

- Название вашей компании

- Почтовый адрес компании

- Номер телефона и контактное лицо

- Адрес электронной почты

Если вы живете в США и не используете WatchGuard System Manager (WSM) с поддержкой «сильного» шифрования, то вам необходимо загрузить соответствующее ПО на странице Software Downloads на сайте LiveSecurity Service.

1. Зайдите на сайт www.watchguard.com.

2. Войдите в систему под вашей учетной записью LiveSecurity Service.

3. Нажмите **Support**.
   Откроется ваш WatchGuard Support Center.

4. В секции **Managing Your Products** выберите **Software Downloads**.

5. В выпадающем списке **Choose product family** выберите ваше устройство WatchGuard.
   Откроется страница Software Downloads.

6. Загрузите версию **WatchGuard System Manager с поддержкой «сильного» шифрования**.

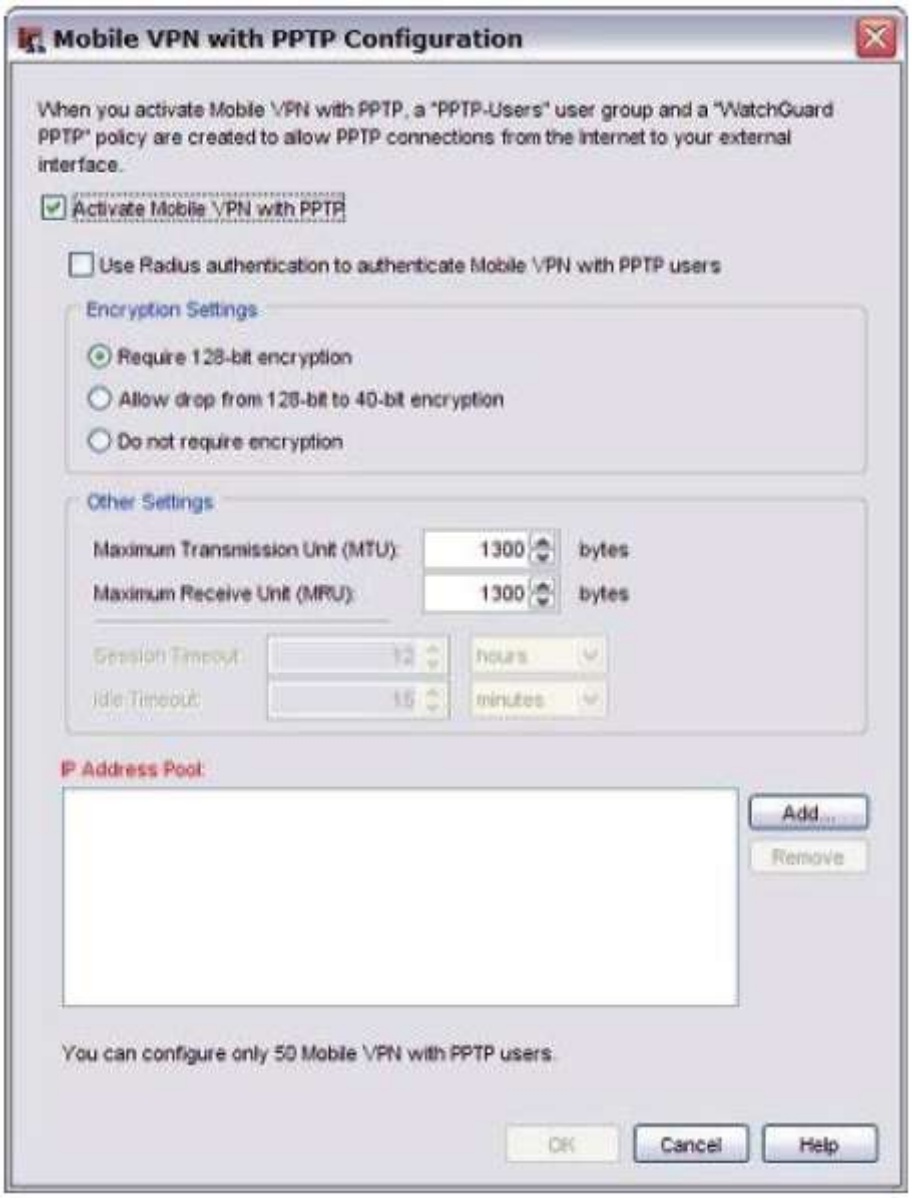
Перед установкой WatchGuard System Manager с поддержкой «сильного» шифрования, вам необходимо все установленные версии WatchGuard System Manager.

Если вы хотите сохранить вашу текущую конфигурацию, то для установки не используйте мастер Quick Setup Wizard. Откройте WatchGuard System Manager, подключитесь к устройству и сохраните конфигурационный файл. Конфигурации с различными уровнями шифрования совместимы.

Настройка Mobile VPN with PPTP

Для того чтобы настроить ваше WatchGuard устройство для работы с PPTP сессиями вам необходимо сначала активировать Mobile VPN with PPTP и настроить все необходимые параметры.

1. В Policy Manager выберите **VPN > Mobile VPN > PPTP**.
   Откроется диалоговое окно Mobile VPN with PPTP Configuration



2. Включите опцию **Activate Mobile VPN with PPTP**. Эта опция позволит вам изменять данные ваших удаленных PPTP пользователей и автоматически создаст политику WatchGuard PPTP, которая будет разрешать передачу PPTP трафика. Мы не рекомендуем вносить изменения в политику WatchGuard PPTP.

3. Для того чтобы настроить все необходимые параметры PPTP см. следующие разделы далее в этой главе.

Аутентификация

Mobile VPN with PPTP пользователи могут аутентифицироваться на устройстве Firebox, или использовать расширенную аутентификацию через серверы RADIUS или VACMAN Middleware. Инструкции по работе с сервером VACMAN Middleware абсолютно идентичны инструкциям по работе с RADIUS сервером. Для того чтобы для аутентификации использовать внутреннюю базу данных устройства WatchGuard, не включайте опцию **Use RADIUS authentication to authenticate Mobile VPN with PPTP users**.

Для того чтобы для аутентификации использовать серверы RADIUS или VACMAN Middleware выполните следующее:

1. Включите опцию **Use RADIUS Authentication to authenticate Mobile VPN with PPTP users**.

2. В диалоговом окне **Authentication Servers** выполните необходимые настройки RADIUS или VASCO серверов. Для более подробной информации см. “Настройка аутентификации RADIUS сервера” и “Настройка аутентификации через VASCO сервер”

3. На RADIUS сервере создайте группу *PPTP-Users* и добавьте в нее пользователей

Для того чтобы установить PPTP соединение, пользователь должен быть членом группы PPTP-Users. После того, как пользователь будет аутентифицирован, вы можете для этого пользователя создать группы и настроить для этой группы политики, которые будут управлять доступом пользователя к сетевым ресурсам.

Настройка шифрования для PPTP туннелей

Американская версия Windows XP использует 128-битное шифрование. Вы можете загрузить патч для использования «сильного» шифрования с сайта Microsoft для других версий Windows.

- Выберите **Require 128-bit encryption** если для всех PPTP туннелей вы хотите использовать 128-битное шифрование. Мы рекомендуем использовать 128-битное шифрование для VPN.

- Выберите **Allow Drop from 128-bit to 40-bit** для того чтобы для менее надежных подключений использовать 40-битное шифрование. Firebox всегда сначала пытается использовать128-битное шифрование. Если клиент не может использовать 128-битное шифрование, то используется 40-битное шифрование. Эта опция используется только клиентами, которые находятся за пределами США

- Включите опцию **Do not require encryption** для того чтобы разрешить незашифрованный трафик через VPN.

MTU и MRU

Параметры MTU (Maximum Transmission Unit) или MRU (Maximum Receive Unit) отправляются клиенту в качестве параметров PPTP во время установления PPTP сессий. Мы не рекомендуем изменять значения этих параметров, только если вы точно уверены, что изменение значений этих параметров решит возникшую проблему. Некорректные MTU или MRU могут привести к потерям PPTP VPN трафика.

Настройка таймаутов для PPTP туннелей

Вы можете настроить два параметра таймаута для PPTP туннелей:

Session Timeout

Максимальное количество времени, в течение которого пользователь может передавать трафик во внешнюю сеть. Если значение равно нулю, то пользователь может оставаться подключенным неограниченное количество времени.

Idle Timeout

Промежуток времени, в течение которого пользователь может оставаться аутентифицированным в режиме ожидания (пользователь не передает трафик во внешнюю сеть). Если значение равно нулю, то пользователь может оставаться в режиме ожидания неограниченное количество времени.

Если вы не настроите эти параметры, будут использованы глобальные параметры

Добавление IP адреса в IP Address Pool

Mobile VPN with PPTP поддерживает до 50 параллельных сессий (пользователей). WatchGuard устройство каждому Mobile VPN пользователю выдает открытый IP адрес из пула доступных

адресов. Когда пользователь закрывает сессию, его IP адрес снова становится доступным в пуле. Для корректной работы PPTP вам необходимо настроить два или более IP адресов.

1. В секции **IP Address Pool** нажмите **Add**.
   Откроется диалоговое окно Add Address

2. В выпадающем списке **Choose Type** выберите **Host IP** (для одного IP адреса) или **Host Range** (для диапазона IP адресов). Вы можете создать максимум 50 адресов. Если вы выберете **Host IP** вам необходимо создать минимум два IP адреса. Если вы выберете **Host Range** и создадите диапазон, состоящий из более 50 адресов, Mobile VPN with PPTP будет использовать первые 50 адресов из этого диапазона.

3. В поле **Value** введите IP адрес хоста. Если вы выбрали **Host Range**, в поле **Value** введите первый IP адрес диапазона и в поле **To** – последний IP адрес диапазона. Проверьте, что введенные вами IP адреса, не используются другими устройствами, подключенными к вашему Firebox. Созданный вами IP адрес или диапазон адресов появятся в списке доступных адресов для удаленных пользователей.

4. Нажмите **OK**.

5. Повторите п. 1–4 для того чтобы добавить все необходимые адреса для Mobile VPN with PPTP.

Сохранение изменений

После того, как вы закончили нажмите **OK**. Сохраните все сделанные изменения.

Настройка WINS и DNS серверов

Mobile VPN клиенты используют адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System) серверов. DNS изменяет имена хостов на IP-адреса, в то время как WINS изменяет имя NetBIOS на IP-адреса. Интерфейс Trusted устройства Firebox® должен иметь доступ к этим серверам

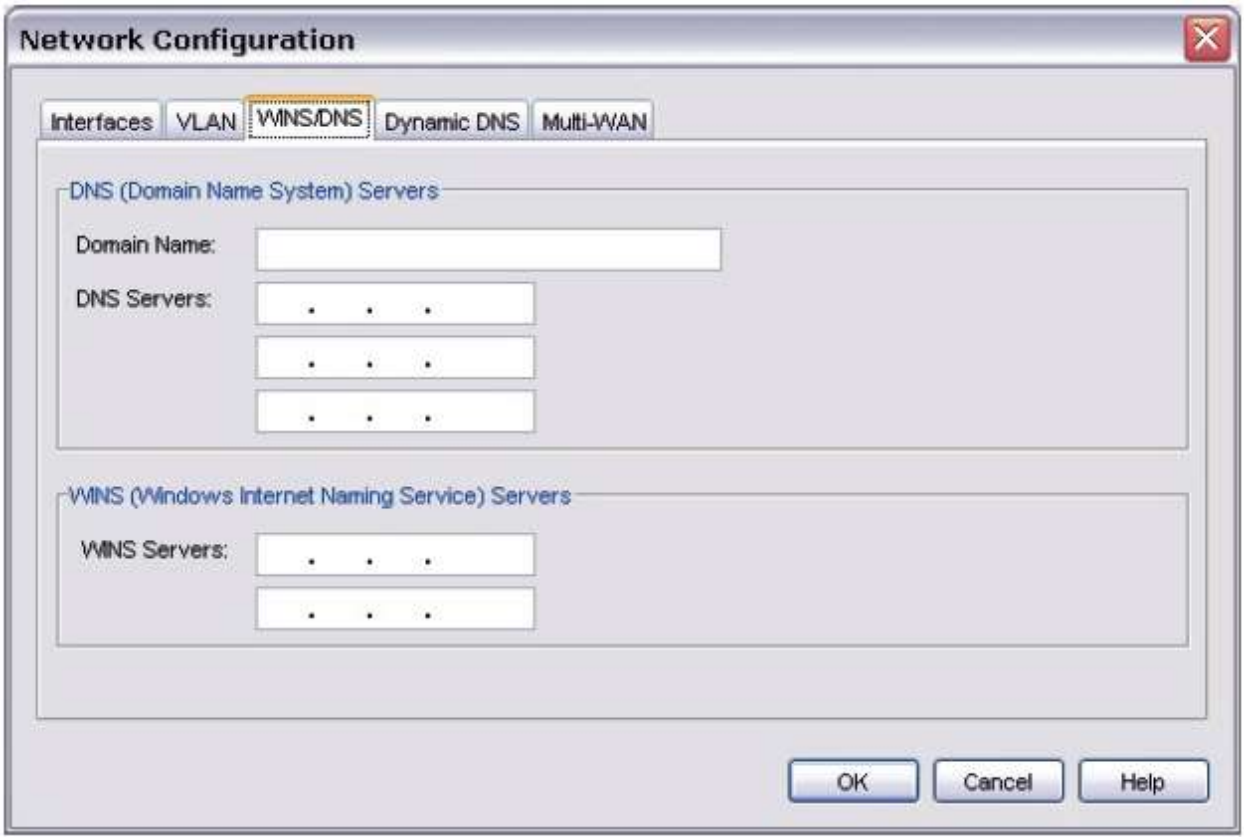
1. В Policy Manager выберите **Network > Configuration**.

2. Выберите закладку **WINS/DNS**.
   Закладка содержит информацию о WINS и DNS серверах.

3. В поле **Domain Name** введите имя домена для DNS сервера.

4. В текстовых полях **DNS Servers** введите адреса DNS серверов. Вы можете добавить максимум 3 сервера.

5. В текстовых полях **WINS Servers** введите IP адреса WINS серверов. Вы можете добавить максимум два WINS сервера



Добавление новых пользователей в группу PPTP-Users

Для того подключиться к устройству Firebox через PPTP VPN туннель, пользователям необходимо для аутентификации ввести имя пользователя и пароль. WatchGuard устройство использует введенные данные для аутентификации пользователя на устройстве WatchGuard.

Если на устройстве WatchGuard вы включите PPTP, то автоматически будет создана группа под названием *PPTP-Users*. Для того чтобы создавать PPTP подключения пользователь должен принадлежать этой группе.

Для более подробной информации см. “Настройка Firebox в качестве сервера аутентификации”

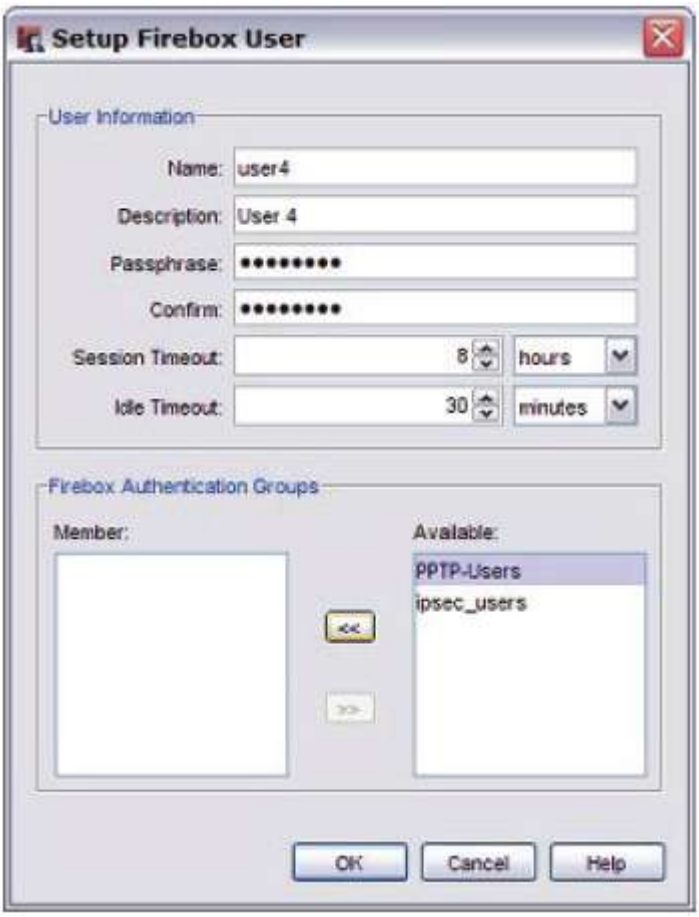
Если для аутентификации вы используете серверы RADIUS или VACMAN middleware, то вам необходимо создать на серверах аутентификации создать группу PPTP-Users и добавить в нее необходимых пользователей. Для более подробной информации см. Документацию по вашему серверу аутентификации.

Если для аутентификации вы используете ваше WatchGuard устройство, то вам необходимо всех пользователей добавить в группу PPTP-Users.

1. В Policy Manager выберите **Setup** > **Authentication** > **Authentication Servers**.
   Откроется диалоговое окно Authentication Servers.

2. Выберите закладку **Firebox**

3. Для того чтобы добавить нового пользователя в группу под списком **Users** нажмите кнопку **Add**. Для того чтобы изменить данные выбранного пользователя нажмите **Edit**



4. Для нового пользователя введите имя пользователя и пароль. Введите пароль еще раз. Если пользователь был создан ранее, то вы можете пропустить этот шаг.
Описание вводить не обязательно. Мы не рекомендуем вам менять значения параметров Session Timeout и Idle Timeout, установленные по умолчанию.

5. Для того чтобы добавить пользователя в группу Firebox Authentication Group выберите пользователя в списке **Available**.

6. Нажмите  для того чтобы переместить пользователя в список **Member**. Или два раза нажмите на имени пользователя в списке Available.
Пользователь будет добавлен в список пользователей. Для того чтобы добавить еще несколько пользователей см. п. 3–6.

7. Нажмите **OK** для того чтобы закрыть диалоговое окно **Setup Firebox User**.
Откроется закладка Firebox Users со списком новых пользователей.

Опция для Интернет-доступа через Mobile VPN with PPTP туннель

Вы можете разрешить удаленным пользователям доступ в сеть Интернет через туннель Mobile VPN. Эта опция влияет на вашу безопасность, так как Интернет трафик не фильтруется и не зашифровывается. Для маршрутов туннеля Mobile VPN у вас есть две опции: default-route VPN и split tunnel VPN.

Default-route VPN

Наиболее безопасная опция – весь Интернет трафик удаленных пользователей маршрутизируется через VPN туннель на Firebox. С Firebox трафик отправляется в сеть Интернет. В этой конфигурации (default-route VPN), Firebox проверяет весь трафик и обеспечивает более высокий уровень безопасности. Однако при этом увеличивается нагрузка на процессор и используется больше пропускной способности. При использовании default-route VPN, политика динамической NAT должна включать исходящий трафик с удаленной сети. Это позволяет удаленным пользователям получать доступ в сеть Интернет, когда они отправляют весь трафик на Firebox.

Если после создания Mobile VPN туннеля на компьютере под управлением ОС Windows вы введете команды "route print" или "ipconfig", то вы увидите некорректные данные о шлюзе по умолчанию. Корректные данные вы можете посмотреть в закладке ***Details*** *диалогового окна* ***Virtual Private Connection Status****.*

Split tunnel VPN

Опция раздельного туннелирования трафика. Эта опция позволит пользователям получать доступ к сети Интернет без необходимости отправки Интернет трафика через VPN туннель. Раздельное туннелирование позволяет повысить скорость передачи данных в сети, но уменьшает уровень ее безопасности, так как созданные вами политики не обрабатывают передаваемый Интернет трафик. Если вы хотите использовать раздельное туннелирование, то необходимо чтобы на компьютере каждого пользователя стоял программный брандмауэр.

Настройка Default-route VPN для Mobile VPN with PPTP

В ОС Windows Vista, XP и 2000 для PPTP по умолчанию используется опция Default Route VPN. Для того чтобы получать трафик от PPTP пользователя вам необходимо на вашем Firebox настроить динамическую NAT. Любая политика, которая управляет исходящим трафиком в сеть Интернет должна разрешать PPTP трафик.

При настройке default-route VPN вам необходимо следующее:

- Убедитесь, что IP-адреса, которые вы добавили в пул PPTP адресов, включены в вашу конфигурацию динамической NAT на устройстве WatchGuard. В Policy Manager выберите **Network > NAT**.

- Ваша политика должна разрешать передачу трафика пользователям, принадлежащим группе PPTP-Users, через External интерфейс. Например, если для управления доступом к web-сайтам вы используете WebBlocker, то вам необходимо добавить группу PPTP-Users в политику прокси с включенным WebBlocker.

Настройка Split tunnel VPN для Mobile VPN with PPTP

На компьютере клиента необходимо настроить PPTP таким образом, чтобы весь трафик не шел через VPN.

1. Для Windows Vista, XP или 2000, выберите **Control Panel > Network Connections** и правой кнопкой нажмите на VPN соединение.

2. Выберите **Properties**.
   Откроется диалоговое окно VPN properties.

3. Выберите закладку **Networking**.

4. В списке выберите **Internet Protocol (TCP/IP)** и нажмите **Properties**.
   Откроется диалоговое окно Internet Protocol (TCP/IP) Properties.

5. В закладке **General** выберите **Advanced**.
   Откроется диалоговое окно Advanced TCP/IP Settings.

6. Для Windows XP и Windows 2000 — В закладке **General** (XP и Windows 2000), отключите опцию **Use default gateway on remote network**.

   Для Windows Vista — В закладке **Settings** (XP и Windows 2000) отключите опцию **Use default gateway on remote network**.

Настройка политик для управления доступом пользователей Mobile VPN with PPTP

У пользователей Mobile VPN with PPTP по умолчанию нет прав доступа через устройство WatchGuard. Вам необходимо создать или настроить политики, которые будут предоставлять пользователям PPTP доступ к сетевым ресурсам.

Перед тем, как настроить политику PPTP доступа, вам необходимо включить Mobile VPN with PPTP

После того, как вы включите Mobile VPN for PPTP, Policy Manager создаст группу PPTPUsers, которую вы использовать в настройках политики PPTP доступа

Если вы PPTP пользователям присвоили IP адреса из Trusted сети, то трафик PPTP пользователей будет заблокирован. Весь Mobile VPN with PPTP трафик заблокирован по умолчанию. Поэтому вам необходимо создать политики, которые разрешат PPTP пользователям получать доступ к ресурсам сети.

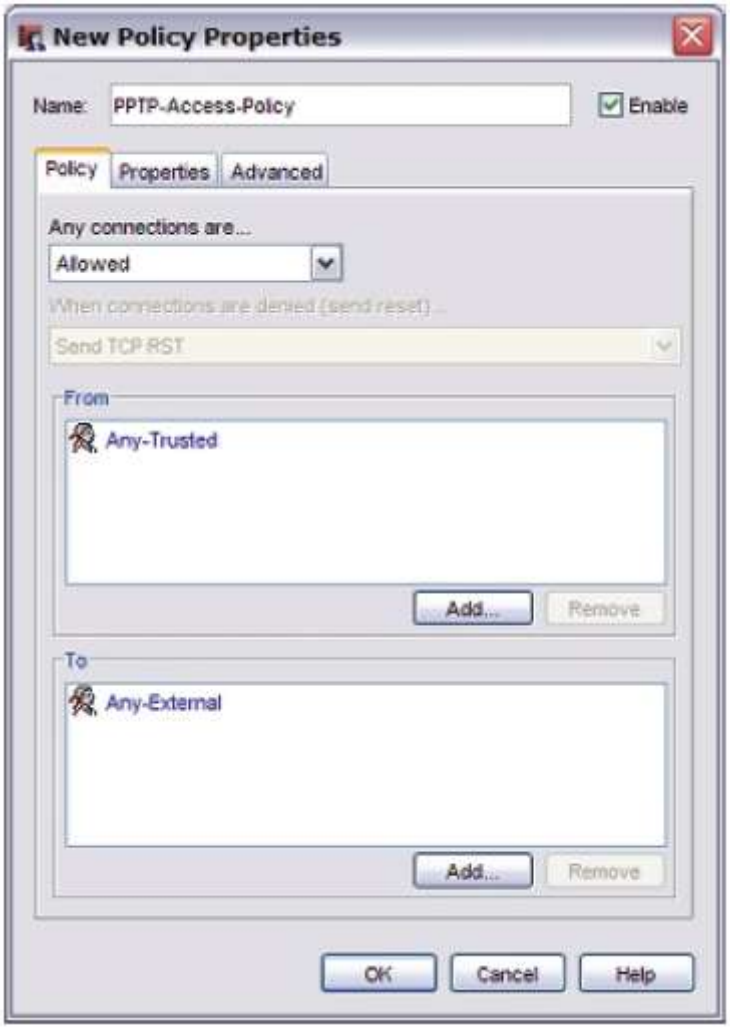
Разрешение доступа PPTP пользователям в Trusted сеть

В этом примере вы добавляете политику Any для того чтобы предоставить пользователям группы PPTP-Users полный доступ к ресурсам всех ваших Trusted сетей.

1. В Policy Manager нажмите  в панели инструментов Policy Manager. Или выберите **Edit** > **Add Policies**.
   Откроется диалоговое окно Add Policies.

2. Откройте элемент **Packet Filters** (нажмите знак (+)).
   Откроется список пакетных фильтров.

3. Выберите **Any** и нажмите **Add**.
Откроется диалоговое окно New Policy Properties



4. В поле **Name** введите имя политики. Введите такое имя, по которому будет достаточно легко идентифицировать политику в вашей конфигурации.

5. В закладке **Policy** в секции **From** нажмите **Add**.
Откроется диалоговое окно Add Address.

6. В секции **Selected Members and Addresses** выберите **Any-Trusted** и нажмите **Remove**.

7. Нажмите **Add User**.
Откроется диалоговое окно Add Authorized Users or Groups

8. В выпадающем списке **Type** выберите **PPTP**.

9. Во втором выпадающем списке **Type** выберите **Group**.

10. В окне **Groups** выберите **PPTP-Users** и нажмите **Select**.
Группа PPTP-Users появится в качестве имени метода аутентификации

11. Нажмите **OK** для того чтобы закрыть диалоговое окно **Add Address**.

12. В диалоговом окне **New Policy Properties** в секции **To** нажмите **Add**.
Откроется диалоговое окно Add Address.

13. В списке **Selected Members and Addresses** выберите **Any-External** и нажмите **Remove**.

14. В списке **Available Members** выберите **Any-Trusted** и нажмите **Add**.
Any-Trusted появится в окне Selected Members and Addresses

15. Нажмите **OK** для того чтобы закрыть диалоговое окно **Add Address**.
Откроется диалоговое окно New Policy Properties

16. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Policy Properties**.

17. Нажмите **Close**.

18. Сохраните ваши изменения.

Другие группы или пользователи в политике PPTP

Для создания PPTP подключения пользователь должен принадлежать группе *PPTP-Users*. При настройке политики, которая предоставляет PPTP пользователям доступ к ресурсам сети, вы можете ввести имя пользователя или имя группы, которой этот пользователь принадлежит.

Для того чтобы выбрать другого пользователя или группу выполните следующее:

1. В Policy Manager два раза нажмите на политику, к которой вы хотите добавить пользователя или группу.

2. В закладке **Policy** нажмите **Add** в секции **From**.
Откроется диалоговое окно Add Address.

3. Нажмите **Add User**.
Откроется диалоговое окно Add Authorized Users or Groups.

4. В первом выпадающем списке **Type** выберите **PPTP**.

5. Во втором выпадающем списке **Type** выберите **Group** или **User**.

6. Выберите пользователя или группу, которых вы хотите добавить и нажмите **Select**.
Выбранный пользователь или группа появится в диалоговом окне Add Address окна Selected Members and Addresses.

7. Нажмите **OK** для того чтобы закрыть диалоговое окно **Add Address**.

8. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Policy Properties**.

Подготовка компьютеров клиента для PPTP

Вам сначала необходимо подготовить каждый компьютер, который будет использоваться как удаленный хост Mobile VPN with PPTP с доступом в Интернет.

Выполните нижеприведенные процедуры, используя инструкции, описание которых приводится в следующих разделах:

- Установите необходимую версию Microsoft Dial-Up Networking и необходимые пакеты обновлений (service pack)

- Подготовка ОС для VPN-подключений

- Установите VPN-адаптер (необходим не во всех ОС).

Подготовка компьютера клиента с установленной ОС Windows NT или 2000: Установка MSDUN и пакетов обновлений

Для корректной конфигурации Mobile VPN with PPTP вам возможно понадобится установить нижеприведенные компоненты:

- Обновления MSDUN (Microsoft Dial-Up Networking)

- Другие расширения

- Пакеты обновлений

Для Mobile VPN with PPTP необходимо установить эти обновления:

Шифрование	Платформа	Приложение
Base	Windows NT	40-bit SP4
Strong	Windows NT	128-bit SP4
Base	Windows 2000	40-bit SP2*
Strong	Windows 2000	128-bit SP2*

*40-bit шифрование используется по умолчанию в Windows 2000. Если вы будете обновлять с Windows 98 с «сильным» шифрованием, Windows 2000 автоматически установит сильное шифрование для новой инсталляции.

Для того чтобы установить пакеты обновлений, посетите сайт Microsoft Download Center: http://www.microsoft.com/downloads/

Процедура настройки и установление PPTP соединения отличаются для разных версий Microsoft Windows.

Для настройки PPTP соединения в ОС Windows Vista, см. “Создание и подключение PPTP Mobile VPN для Windows Vista”

Для настройки PPTP соединения в ОС Windows XP см. “Создание и подключение PPTP Mobile VPN дл Windows XP”

Для настройки PPTP соединения в ОС Windows 2000, см. “Создание и подключение PPTP Mobile VPN для Windows 2000”

Создание и подключение PPTP Mobile VPN для Windows Vista

Создание PPTP подключения

Для того чтобы подготовить компьютер клиента с установленной Windows Vista, вам необходимо настроить PPTP подключение:

1. Выберите **Start > Settings > Control Panel**.
   Кнопка Start в Windows Vista находится в нижнем левом углу экрана.

2. Нажмите **Network and Internet**.
   Откроется окно Network and Sharing Center.

3. В левой колонке, под **Tasks** нажмите **Connect to a network**.
   Запустится мастер New Connection Wizard.

4. Выберите **Connect to a workplace** и нажмите **Next**.
   Откроется диалоговое окно Connect to a workplace.

5. Выберите **No, create a new connection** и нажмите **Next**.
   Откроется диалоговое окно How do you want to connect.

6. Нажмите **Use my Internet connection (VPN)**.
   Откроется диалоговое окно Type the Internet address to connect.

7. Введите имя хоста и IP-адрес интерфейса External устройства Firebox в поле **Internet address**.

8. Введите имя для Mobile VPN (например "PPTP to Firebox") в поле **Destination name**.

9. Выберите, смогут ли другие пользователи использовать это подключение.

10. Включите опцию **Don't connect now; just set it up so I can connect later** чтобы компьютер клиента не пытался подключиться в данный момент.

11. Нажмите **Next**.
Откроется диалоговое окно Type your user name and password.

12. В полях **User name** и **Password** введите имя пользователя и пароль соответственно.

13. Нажмите **Create**.
Откроется диалоговое окно The connection is ready to uses.

14. Для того чтобы проверить подключение нажмите **Connect now**.

Установление PPTP соединения

Для того чтобы подключить компьютер клиента с Windows Vista, замените параметр **[name of the connection]** реальным именем подключения, которое вы ввели при настройке PPTP соединения. Имя пользователя и пароль указывают на одного из пользователей группы PPTP-Users. Убедитесь, что у вас есть активное подключение к сети Интернет.

1. Нажмите **Start > Settings > Network Connections > [name of the connection]**.
Кнопка Start в Windows Vista находится в нижнем левом углу экрана.

2. Введите имя пользователя и пароль для соединения и нажмите **Connect**.

3. При первом подключении вам необходимо выбрать месторасположение сети. Выберите Public Location.

Создание и подключение PPTP Mobile VPN дл Windows XP

Для того чтобы подготовить удаленный хост, который работает под управлением Windows XP, вам необходимо настроить сетевое подключение.

Создание PPTP Mobile VPN

На рабочем столе компьютера клиента:

1. Выберите **Start** > **Control Panel** > **Network Connections**.

2. В меню слева нажмите **Create a new connection**. Или нажмите **New Connection Wizard** в классическом виде Windows.
Запустится мастер New Connection.

3. Нажмите **Next**.

4. Нажмите **Connect to the network at my workplace**. Нажмите **Next**.

5. Нажмите **Virtual Private Network Connection**. Нажмите **Next**.

6. Введите имя для подключения, например "Connect with Mobile VPN." Нажмите **Next**.

7. Выберите одну из следующих опций:

   * Для широкополосного подключения выберите **Do not dial the initial connection**.

Или,

* Для модемного подключения выберите **Automatically dial this initial connection**, и затем в выпадающем списке выберите соответствующее имя подключения.

8. Нажмите **Next**.
   Откроется страница VPN Server Selection. Мастер отображает эту страницу, если вы используете Windows XP SP2. Не все пользователи Windows XP смогут увидеть эту страницу

9. Введите имя хоста или IP-адрес External интерфейса устройства Firebox. Нажмите Next.
   Откроется окно Smart Cards.

10. Выберите, будете ли вы использовать смарт-карту для данного подключения и нажмите **Next**.
    Откроется окно Connection Availability.

11. Выберите, кто может пользоваться этим соединением и нажмите **Next**.

12. Выберите **Add a shortcut to this connection to my desktop**.

13. Нажмите **Finish**.

Подключение с помощью PPTP Mobile VPN

1. Запустите подключение к сети Интернет через dial-up сеть или напрямую через LAN или WAN.

2. Два раза нажмите на ярлык нового подключения на вашем рабочем столе. Или выберите **Control Panel > Network Connections** и выберите ваше созданное подключение из списка Virtual Private Network

3. Введите имя пользователя и пароль

4. Нажмите **Connect**.

Создание и подключение PPTP Mobile VPN для Windows 2000

Для того чтобы подготовить удаленный хост, который работает под управлением Windows 2000, вам необходимо настроить сетевое подключение.

Создание PPTP Mobile VPN

На рабочем столе компьютера клиента:

1. Выберите **Start** > **Settings** > **Network Connections** > Create a New Connection.
   Запустится мастер New Connection.

2. Нажмите Next.

3. Нажмите **Connect to the network at my workplace**. Нажмите **Next**.

4. Нажмите **Virtual Private Network Connection**. Нажмите **Next**.

5. Введите имя для подключения, например “**Connect with Mobile VPN**.” Нажмите Next.

6. Выберите опции для этого подключения (не использовать набор номера (для широкополосного подключения), или автоматический набор номера (для подключение через модем). Нажмите Next.

7. Введите имя хоста или IP-адрес интерфейса External устройства Firebox. Нажмите **Next**.

8. Выберите **Add a shortcut to this connection to my desktop**. Нажмите **Finish**

Подключение через PPTP Mobile VPN

1. Запустите подключение к сети Интернет через dial-up сеть или напрямую через LAN или WAN.

2. Два раза нажмите на ярлык нового подключения на вашем рабочем столе. Или выберите **Control Panel > Network Connections** и выберите ваше созданное подключение из списка Virtual Private Network

3. Введите имя пользователя и пароль

4. Нажмите **Connect**.

Исходящие PPTP подключения из сети, защищенной Firebox

При необходимости вы можете создавать PPTP подключение к одному Firebox из сети, защищенной другим Firebox. Например, один из ваших удаленных пользователей едет к заказчику в офис, в котором есть Firebox. При этом этот пользователь не сможет подключиться к вашей сети через PPTP. Необходимо на локальном Firebox разрешить исходящие PPTP соединения, добавив политику, которая разрешит трафик из сети, к которой на данный момент подключен пользователь на псевдоним *Any-External*.

Глава 28 - Mobile VPN with IPSec

Mobile VPN with IPSec

WatchGuard Mobile VPN with IPSec – это клиентское приложение, которое устанавливается на удаленный компьютер. Клиент создает защищенное подключение с удаленного компьютера к вашей защищенной сети по незащищенному каналу связи. Клиент Mobile VPN использует протокол IPSec для защиты соединения. Информация, представленная в этой главе, поможет вам настроить Mobile VPN туннель между клиентом WatchGuard Mobile VPN with IPSec и Firebox X Core или Firebox X Peak, на которых установлено Fireware XTM.

Настройка Mobile VPN with IPSec подключения

Вы можете использовать устройство WatchGuard, в качество конечной точки Mobile VPN with IPSec туннелей.

В Policy Manager выберите **VPN > Mobile VPN > IPSec**.

Для того чтобы создавать Mobile VPN with IPSec соединения пользователь должен принадлежать группе Mobile VPN. Эта группа создается при помощи мастера Add Mobile VPN with IPSec. После того, как мастер завершит работу, Policy Manager делает следующее:

- Создает профиль конфигурации клиента (.wgx файл) и копирует его на станцию управления, которая создала учетную запись Mobile VPN. Для настройки компьютера клиента Mobile VPN вам необходимо иметь этот .wgx файл. Если для аутентификации вы используете сертификат, то генерируются файлы .p12 и cacert.pem. Эти файлы создаются в том же каталоге, что и .wgx файл.

- Автоматически создает политику Any в закладке Mobile VPN, которая разрешит трафик для аутентифицированного Mobile VPN пользователя.

Для того чтобы ограничить доступ Mobile VPN клиенту, удалите политику *Any* и создайте политики, которые будут разрешать доступ только к определенным ресурсам сети. Для более подробной информации см. “Policy Manager”

После того, как устройство WatchGuard будет настроено, на компьютере пользователя необходимо установить клиент Mobile VPN with IPSec. Для более подробной информации об установке клиента Mobile VPN with IPSec см. “Инструкции для установки клиента Mobile VPN with IPSec”

После того, как компьютер будет настроен для корректной работы, пользователь сможет создавать Mobile VPN соединения. Если данные доступа, предоставленные пользователем, совпадают с данными доступа в базе данных устройства WatchGuard, и если пользователь принадлежит группе Mobile VPN, то тогда Mobile VPN сессия будет аутентифицирована.

Системные требования

Перед тем, как приступить к настройке устройства WatchGuard, вам необходимо понять системные требования для устройства WatchGuard и компьютеру с установленным клиентом Mobile VPN with IPSec.

WatchGuard System Manager with strong encryption

Так как на экспорт программных продуктов, использующих шифрование, накладываются определенные ограничения, WatchGuard System Manager доступен с двумя уровнями шифрования. При использовании Mobile VPN with IPSec вам необходимо загрузить WatchGuard

System Manager с «сильным» шифрованием, так как стандарт IPSec требует минимум 56-битное шифрование.

Mobile user client computer

Вы можете установить клиента Mobile VPN with IPSec на любой компьютер под управлением следующих ОС: Windows 2000 Professional, Windows XP (32-bit), Windows Vista (32-bit and 64-bit).

Перед установкой ПО клиента, убедитесь, что на удаленном компьютере никакого другого ПО для Mobile VPN with IPSec туннелей. Вам также необходимо с компьютеров пользователей удалить любые программные брандмауэры (кроме брандмауэра Microsoft).

Опции доступа в Интернет через Mobile VPN туннель

Вы можете разрешить в сеть Интернет доступ удаленным пользователям через Mobile VPN туннель. Эта опция влияет на вашу систему безопасности, так как Интернет трафик передается в открытом виде и не фильтруется. Вы можете использовать две опции для маршрутов Mobile VPN туннеля: default-route VPN и split tunnel VPN.

Default-route VPN

Наиболее безопасная опция – весь Интернет трафик удаленных пользователей маршрутизируется через VPN туннель на Firebox. С Firebox трафик отправляется в сеть Интернет. В этой конфигурации (default-route VPN), Firebox проверяет весь трафик и обеспечивает более высокий уровень безопасности. Однако при этом увеличивается нагрузка на процессор и используется больше пропускной способности. При использовании default-route VPN, политика динамической NAT должна включать исходящий трафик с удаленной сети. Это позволяет удаленным пользователям получать доступ в сеть Интернет, когда они отправляют весь трафик на Firebox.

Split tunnel VPN

Опция раздельного туннелирования трафика. Эта опция позволит пользователям получать доступ к сети Интернет без необходимости отправки Интернет трафика через VPN туннель. Раздельное туннелирование позволяет повысить скорость передачи данных в сети, но уменьшает уровень ее безопасности, так как созданные вами политики не обрабатывают передаваемый Интернет трафик. Если вы хотите использовать раздельное туннелирование, то необходимо чтобы на компьютере каждого пользователя стоял программный брандмауэр.

Конфигурационные файлы клиента Mobile VPN

При помощи Mobile VPN with IPSec администратор сетевой безопасности управляет профилями конечных пользователей. Policy Manager используется для создания группы Mobile VPN with IPSec и создавать профили конечных пользователей в виде файлов с расширениями .wgx или .ini. Файлы .wgx и .ini содержат ключ шифрования, идентификационные данные пользователя, IP адреса и настройки, которые используются для создания защищенного туннеля между удаленным компьютером и устройством WatchGuard.

Файл .wgx зашифрован паролем, длина которого от 8 символов. Администратор и удаленный пользователь должны знать этот пароль. Если вы хотите импортировать этот файл на клиенте Mobile VPN with IPSec вам необходимо будет ввести пароль для его расшифрования. Файл .wgx не используется для настройки параметров Line Management.

Конфигурационный файл .ini не зашифровывается. Его необходимо использовать только в случае, если вы изменили параметры **Line Management** (любое значение, кроме **Manual**).

Для более подробной информации о **Line Management** в закладке **Advanced** см. “Редактирование профиля Mobile VPN with IPSec группы”

После того, как вы выполнили все инструкции мастера Add Mobile User VPN, вы можете создавать файл .wgx бесконечное число раз. Для более подробной информации см. “Конфигурационные файлы клиента Mobile VPN”. Если вы хотите заблокировать профили мобильных пользователей,

вы можете сделать их только для чтения. Для более подробной информации см. “Блокировка профиля пользователя”

Настройка Firebox для Mobile VPN with IPSec

Вы можете включить Mobile VPN with IPSec для существующей группы пользователей или вы можете создать новую группу. Пользователи группы могут аутентифицироваться на локальном сервере аутентификации Firebox, или на сервере аутентификации стороннего производителя, который включен в вашу конфигурацию Firebox. Для более подробной информации см. “Добавление пользователей к группе Mobile VPN”

Если вы используете сервер аутентификации стороннего производителя, см. документацию по этому продукту.

1. В Policy Manager выберите **VPN > Mobile VPN > IPSec**.
   Откроется диалоговое окно Mobile VPN with IPSec Configuration

2. Нажмите **Add**.
Откроется мастер Add Mobile User VPN with IPSec

3. Нажмите **Next**.
Откроется диалоговое окно Select a user authentication server

4. В выпадающем списке **Authentication Server** выберите сервер аутентификации. Вы можете выбрать - Firebox (Firebox-DB), RADIUS, VASCO, SecurID, LDAP или Active Directory. Проверьте включенность выбранного способа аутентификации в Policy Manager. Для этого выберите **Setup > Authentication > Authentication Servers**.

5. В поле **Group Name** введите имя группы. Вы можете ввести имя уже созданной группы Mobile VPN, или ввести имя новой группы. Проверьте, что имя группы уникально среди остальных имен VPN групп, а также среди интерфейсов и имен туннелей. Для более подробной информации об аутентификации VPN группы

6. Нажмите **Next**.
Откроется страница Select a tunnel authentication method

7. Выберите способ аутентификации туннеля:

   Use this passphrase - Введите пароль.

   Use an RSA certificate issued by your WatchGuard Management Server - Введите **IP Address** вашего Сервера Управления и пароль администратора (**Administration Passphrase**)

8. Нажмите **Next**.
Откроется страница Direct the flow of Internet traffic

9. Выберите опцию для Интернет трафика:

   No, allow Internet traffic to go directly to the mobile user's ISP.
   (Раздельное туннелирование)

   Yes, force all Internet traffic to flow through the tunnel.
   (Default-route VPN)
   Нажмите **Next**.
   Откроется страница Identify the resources accessible through the tunnel

10. Нажмите **Add** для того чтобы указать IP адреса хостов и сетей, к которым пользователи смогут подключаться через VPN туннель

11. Нажмите **Next**.
Откроется страница Create the virtual IP address pool

12. Нажмите **Add** для того чтобы добавить один IP адрес или диапазон адресов. Для того чтобы добавить еще несколько виртуальных IP адресов, повторите эту процедуру. Пользователям Mobile VPN при подключении к вашей сети присваиваются адреса из этого диапазона. Количество IP адресов должно соответствовать количеству пользователей. Если вы используете High Availability, вам необходимо для каждого Mobile VPN пользователя выделить по два виртуальных IP адреса. Эти IP адреса нельзя использовать для любых других целей.

13. Нажмите **Next**.
Откроется страница Add Mobile VPN with IPSec Wizard. Конфигурационный файл группы Mobile VPN with IPSec будет создан в каталоге, указанном на этой странице

14. Для того чтобы добавить пользователей в новую группу Mobile VPN with IPSec включите опцию **Add users to**.

15. Нажмите **Finish**.

Настройка внешнего сервера аутентификации

Если вы создаете группу пользователей Mobile VPN, которая аутентифицируется через сервер аутентификации стороннего производителя, убедитесь, что вы создали группу на сервере, имя которой совпадает с именем группы Mobile VPN. Для RADIUS, VASCO или SecurID, убедитесь, что сервер RADIUS отправляет атрибут Filter-Id (RADIUS attribute #11) при успешной аутентификации пользователя, для того чтобы сообщить Firebox какой группе принадлежить пользователь. Значение атрибута Filter- Id должно совпадать с именем группы Mobile VPN. Все пользователи Mobile VPN, которые аутентифицируются через этот сервер, должны принадлежать этой группе

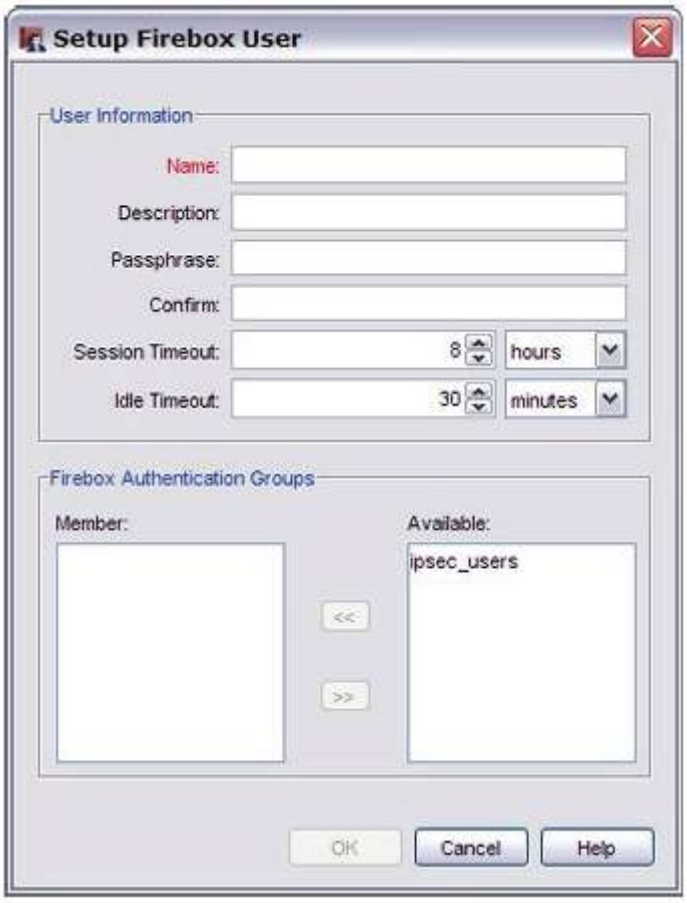
Добавление пользователей к группе Mobile VPN

Для того чтобы создать Mobile VPN туннель с Firebox, удаленным пользователям необходимо ввести имя пользователя и пароль для аутентификации. WatchGuard System Manager используею введенные данные для аутентификации пользователя. Для того чтобы аутентифицироваться, пользователи должны принадлежать группе Mobile VPN. Если вы используете аутентификацию Firebox, см. инструкции ниже. Если вы используете сервер аутентификации стороннего производителя, то см. документацию по этому продукту

1. В Policy Manager выберите **Setup** > **Authentication** > **Authentication Servers**.
   Откроется диалоговое окно Authentication ServersОткроется диалоговое окно

2. Выберите закладку **Firebox**.

3. Для того чтобы добавить нового пользователя нажмите на кнопку **Add** под списком **Users**.
   Откроется диалоговое окно Setup Firebox User



4. Введите имя пользователя и пароль для нового пользователя. Введите пароль снова для подтверждения.
   Описание пользователя вводить необязательно. Значения Session Timeout и Idle Timeout изменяйте только при необходимости.

5. В окне **Firebox Authentication Groups** при помощи стрелок сделайте пользователя членом группы, которую вы создали при помощи мастер

6. Нажмите **OK**.
   Новый пользователь появится в списке Users в диалоговом окне Authentication Servers. Вы можете добавить еще пользователей.

7. Нажмите **OK** для того чтобы закрыть диалоговое окно **Authentication Servers**

Редактирование профиля Mobile VPN with IPSec группы

После того, как вы при помощи мастера Mobile User VPN создали новый .wgx, вы можете редактировать профиль:

- Изменить ключ шифрования (shared key)
- Добавить доступ к большему количеству хостов или сетей
- Ограничить доступ к единственному порту назначения, порту источника или протоколу
- Изменить параметры Phase 1 или Phase 2.

Для того чтобы изменить профиль группы Mobile VPN with IPSec:

1. В Policy Manager выберите **VPN > Mobile VPN > IPSec**.
   Откроется диалоговое окно Mobile VPN with IPSec Configuration

2. Из списка выберите группу, которую вы хотите изменить.

3. Нажмите **Edit**.
Откроется диалоговое окно Edit Mobile VPN with IPSec

4. Для редактирования профиля группы используйте следующие поля:

Authentication Server

Выберите сервер аутентификации, который будет использоваться для этой группы Mobile VPN. Для настройки сервера аутентификации выберите **Setup > Authentication > Authentication Servers** в меню Policy Manager.

Passphrase

Введите пароль для шифрования профиля Mobile VPN (.wgx файл). Ключ шифрования должен состоять из стандартных ASCII символов. Если для аутентификации вы используете сертификат, то введите PIN для сертификата.

Confirm

Введите пароль снова.

Primary

Выберите или введите основной внешний IP, к которому пользователи этой группы могут подключаться

Backup

Выберите или введите резервный внешний IP-адрес, к которому могут подключаться пользователи этой группы. Этот IP-адрес является необязательным. Если вы введет резервный IP-адрес, убедитесь, что это IP-адрес, присвоенный интерфейсу External.

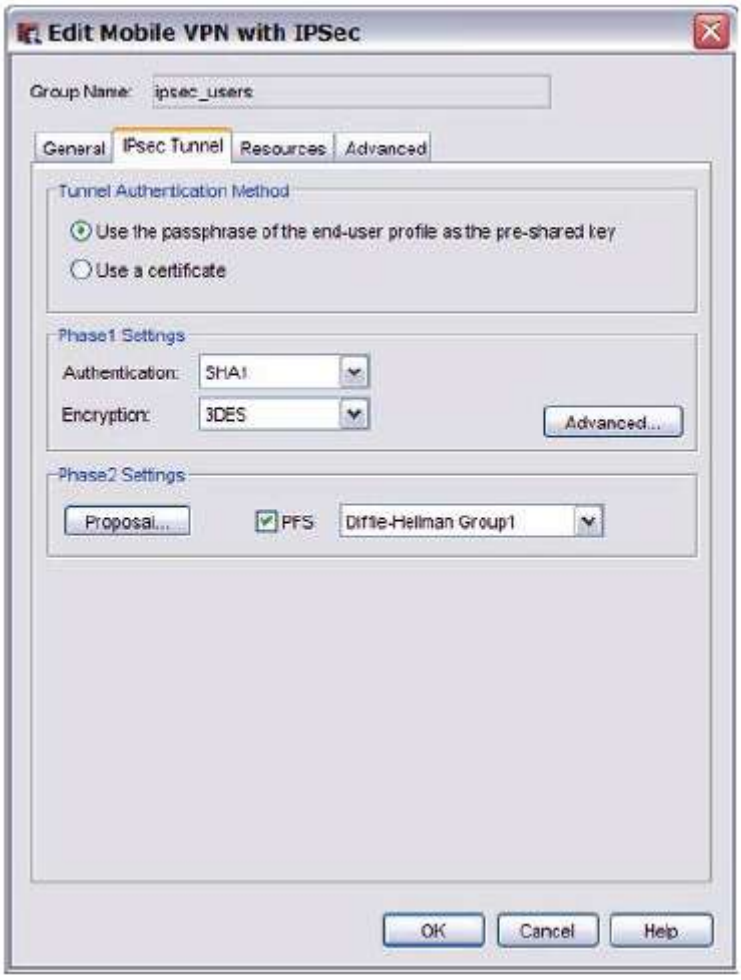
Session

Выберите промежуток времени в минутах, в течение которого Mobile VPN сессия может быть активной

Idle

Введите промежуток времени, по истечении которого Firebox закроет сессию Mobile VPN. Таймаут сессии и таймаут ожидания – это значения по умолчанию, если только сервер аутентификации не использует свои значения. Если вы используете сервер аутентификации Firebox, значения таймаутов для группы Mobile VPN всегда игнорируются, так как вы их настраиваете для отдельных учетных записей Firebox. Значения таймаутов не могут превышать значения, указанного в поле **SA Life**. Для того чтобы изменить значение этого поля, в закладке **IPSec Tunnel** диалогового окна **Edit MUVPN Extended Authentication Group** нажмите **Advanced**. По умолчанию значение **SA Life** равно 8 часов

5. Выберите закладку **IPSec Tunnel**



6. Для настройки параметров туннеля используйте следующие поля:

Use the passphrase of the end-user profile as the pre-shared key

Выберите этот параметр, если вы хотите использовать пароль профиля конечного пользователя в качестве ключа шифрования для аутентификации туннеля. Вам

необходимо использовать тот же самый ключ на удаленном устройстве, и этот ключ должен содержать только стандартные ASCII символы.

Use a certificate

Выберите эту опцию, если для аутентификации туннеля вы хотите использовать сертификат.

CA IP address

(Это поле появится, только если для аутентификации вы используете сертификат) Выберите этот параметр, если вы хотите для аутентификации туннеля использовать сертификат.

Timeout

(Это поле появится, только если для аутентификации вы используете сертификат) Введите промежуток времени в секундах, по истечение которого Центр Сертификации генерирует.

Phase1 Settings

Выберите методы аутентификации и шифрования для Mobile VPN туннеля. Эти параметры должны быть идентичными на обоих концах туннеля. Для того чтобы настроить дополнительные параметры, такие как NAT Traversal или группы ключей, нажмите на кнопку **Advanced** и см. процедуру, описанную в “Настройка параметров Phase 2”. Ниже приведен список алгоритмов шифрования.

* DES

* 3DES

* AES (128 bit)

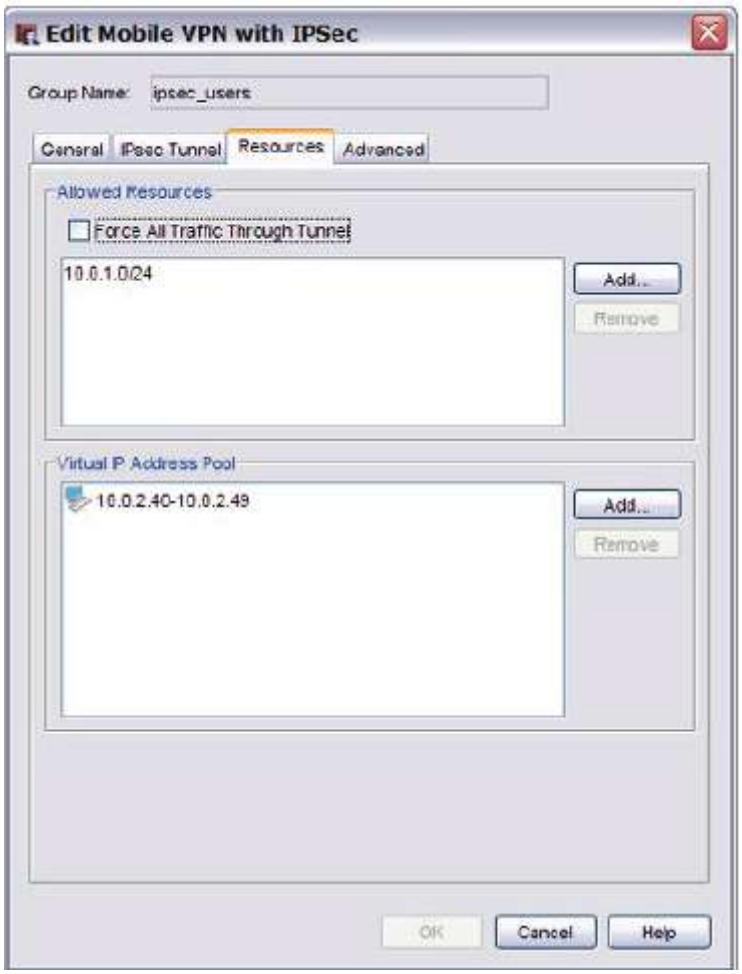
* AES (192 bit)

* AES (256 bit)

Phase2 Settings

Выберите предложение и параметры истечения срока действия ключа для Mobile VPN туннеля. ВЫ также можете включить Perfect Forward Secrecy (PFS) или настроить группы Diffie-Hellman. Для того чтобы изменить другие параметры предложения нажмите на кнопку **Proposal**, и см. процедуру, описанную в “Настройка параметров Phase 2”

7. Выберите закладку **Resources**



8. Используйте следующие поля для того чтобы добавить или удалить разрешенные сетевые ресурсы и виртуальные IP-адреса:

   Allowed Resources list

   Список ресурсов, доступ к которым могут получить пользователи группы Mobile VPN. Для того чтобы добавить в список IP-адрес или диапазон IP-адресов нажмите **Add**. Нажмите **Remove** для того чтобы удалить выделенные IP-адрес или диапазон IP-адресов

   Force All Traffic Through Tunnel

   Включите эту опцию для того чтобы передавать весь трафик пользователей Mobile VPN через VPN туннель. Если эта опция включена, Интернет трафик пользователя Mobile VPN передается по туннелю, при этом скорость загрузки сайтов снизится. Если опция отключена, трафик пользователей Mobile VPN передается в открытом виде, но сайты для этих пользователей будут грузиться быстрее

   Virtual IP Address Pool

   Список внутренних IP-адресов, которые используются пользователями Mobile VPN в туннеле. Эти адреса используются только при необходимости. Нажмите **Add** для того чтобы добавить IP-адрес или диапазон IP-адрес в пул виртуальных IP-адресов. Нажмите **Remove** для того чтобы удалить IP-адрес или диапазон IP-адресов из пула адресов.

9. Выберите закладку **Advanced**

10. Настройте параметры **Line Management**:

    Connection mode

    Manual — В этом режиме клиент не пытается автоматически пересоздать VPN туннель, если он вышел из строя. Этот режим используется по умолчанию. Для того чтобы пересоздать туннель вам необходимо нажать на кнопку **Connect** в Connection Monitor, или нажать правой кнопкой на иконку Mobile VPN в панели инструментов Windows и выбрать **Connect**.

    Automatic — В этом режиме клиент пытается создать VPN соединение когда конечная точка доступна через VPN. Также клиенты после выхода из строя VPN туннеля пытаются его автоматически пересоздать.

    Variable — В этом режиме клиент пытается автоматически пересоздать VPN туннель до тех пор, пока вы не нажмете **Connect**.

    Inactivity timeout

    Если Connection Mode равен **Automatic** или **Variable**, клиент Mobile VPN with IPSec в течение указанного вами промежутка времени не пытается пересоздать VPN подключение.

    *По умолчанию используется режим **Manual** и **0 seconds**. Если вы измените какой-нибудь параметр, то для настройки ПО клиента вам необходимо .ini файл*

11. Нажмите **OK**.

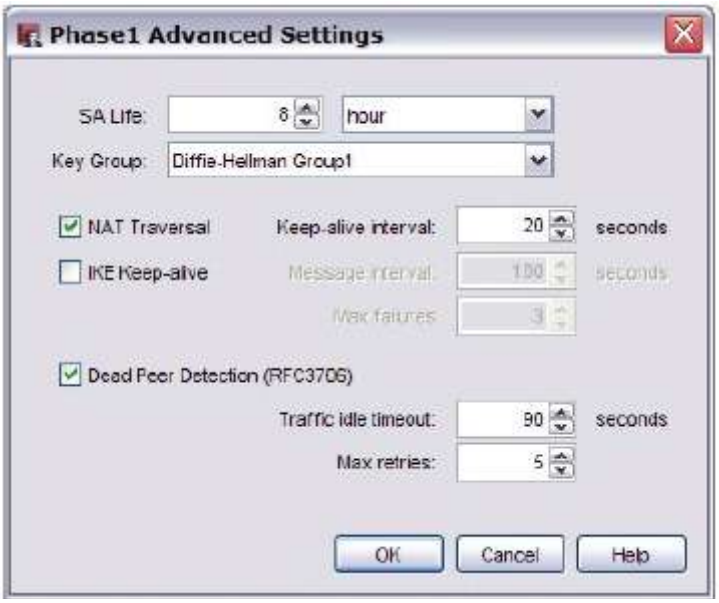
После этого вам необходимо сохранить вашу конфигурацию Firebox. Конечные пользователи, которые принадлежат группе, не смогут подключаться до тех пор, пока они не получат новый

конфигурационный файл и не импортируют его в свой Mobile VPN with IPSec клиент. Вам необходимо сгенерировать конфигурационный файл и разослать его вашим пользователям

Настройка дополнительных параметров Phase 1

Вы можете настроить дополнительные параметры Phase 1 для профиля Mobile VPN пользователя.

1. В закладке **IPSec Tunnel** диалогового окна **Edit Mobile VPN with IPSec**, выберите **Advanced**.
   Откроется диалоговое окно Phase1 Advanced Settings



2. Настройте необходимые опции для вашего профиля. Мы рекомендуем вам использовать настройки по умолчанию.

   SA Life

   Введите время жизни SA (security association) и из выпадающего списка выберите **Hour** или **Minute**. После того как время жизни SA истечет, начнется новая процедура Phase 1 согласования. Тем меньше время жизни SA, тем выше уровень безопасности. Но при этом новая процедура согласования параметров SA закроет все существующие соединения.

   Key Group

   Выберите необходимую группу Diffie-Hellman. WatchGuard поддерживает группы 1, 2 и 5. Группы Diffie-Hellman определяют силу основного ключа (master), который используется в процессе обмена ключами. Группы с большим номером обеспечивают более высокий уровень безопасности, но для генерации ключей требуется больше времени.

   NAT Traversal

   Включите эту опцию для того чтобы создать Mobile VPN туннель между Firebox и другим устройством, который находится за NAT устройством. NAT Traversal, или UDP инкапсуляция, разрешает маршрутизацию трафика в корректное место назначения.

   IKE Keep-alive

   Включите эту опцию, если пользователи из вашей группы, подключаются к устройству WatchGuard, которое не поддерживает Dead Peer Detection. Все устройства WatchGuard с Fireware v9.x или ниже, Edge v8.x или ниже и все версии WFS не поддерживают Dead Peer Detection. Для этих устройств включите опцию. Не включайте IKE Keep-alive и Dead Peer Detection одновременно.

Message interval

Введите количество секунд для интервала сообщения keep-alive

Max failures

Максимальное количество раз, которое Firebox пытается отправлять сообщение IKE keep-alive, перед тем как начать процедуру согласования Phase 1 снова.

Dead Peer Detection

Включите опцию для того чтобы включить Dead Peer Detection (DPD). Ваше устройство WatchGuard должно поддерживать эту опцию. Все устройства WatchGuard с Fireware v10.x или выше, и Edge v10.x или выше поддерживают DPD. Не включайте IKE Keep-alive и Dead Peer Detection одновременно. DPD основана на RFC 3706 и использует шаблоны IPSec трафика для того чтобы определить существование соединения. Если вы выберете DPD, одному из участников (peer) отправляется сообщение are-you-there после того, как от него не поступало трафика в течение определенного периода времени. Если DPD определяет что peer неактивен, следующие попытки подключения не выполняются.

Traffic Idle Timeout

Количество секунд, по истечении которых устройство WatchGuard повторяет попытку подключения к удаленному устройству.

Max retries

Максимальное число попыток подключения, после чего Firebox считает, что удаленное устройство недоступно, закрывает текущее VPN соединение и запускает снова процедуру Phase 1.

3. Нажмите **OK**.

Настройка параметров Phase

Вы можете настроить параметры Phase 2 для вашего профиля Mobile VPN пользователя.

1. В закладке **IPSec Tunnel** диалогового окна **Edit Mobile VPN with IPSec**, выберите **Proposal**.
   Откроется диалоговое окно Phase2 Proposal

2. Настройте необходимые параметры для вашего профиля. Мы рекомендуем использовать настройки по умолчанию

Type

ESP или **AH** – две опции для методов предложений. На данный момент поддерживается только ESP

Authentication

Выберите **SHA1** или **MD5** в алгоритма аутентификации.

Encryption

Выберите алгоритм шифрования в выпадающем списке.

* DES

* 3DES

* AES (128 bit)

* AES (192 bit)

* AES (256 bit)

Force Key Expiration

Включите эту опцию для того, чтобы по истечении определенного срока происходила повторная процедура генерации ключей. В полях под **Force Key Expiration**, выберите количество времени и количество байт, по истечении или по достижении которых срок действия ключа истечет. Если опция **Force Key Expiration** отключена, или она включена и значения времени и количества байт равны нулю, Firebox пытается использовать значение времени для срока действия ключа, установленного для одного из участников. Если и это значение равно нулю и опция отключена, то Firebox по умолчанию использует значение равное 8 часам. Вы можете установить промежуток до года.

3. Нажмите **OK**.

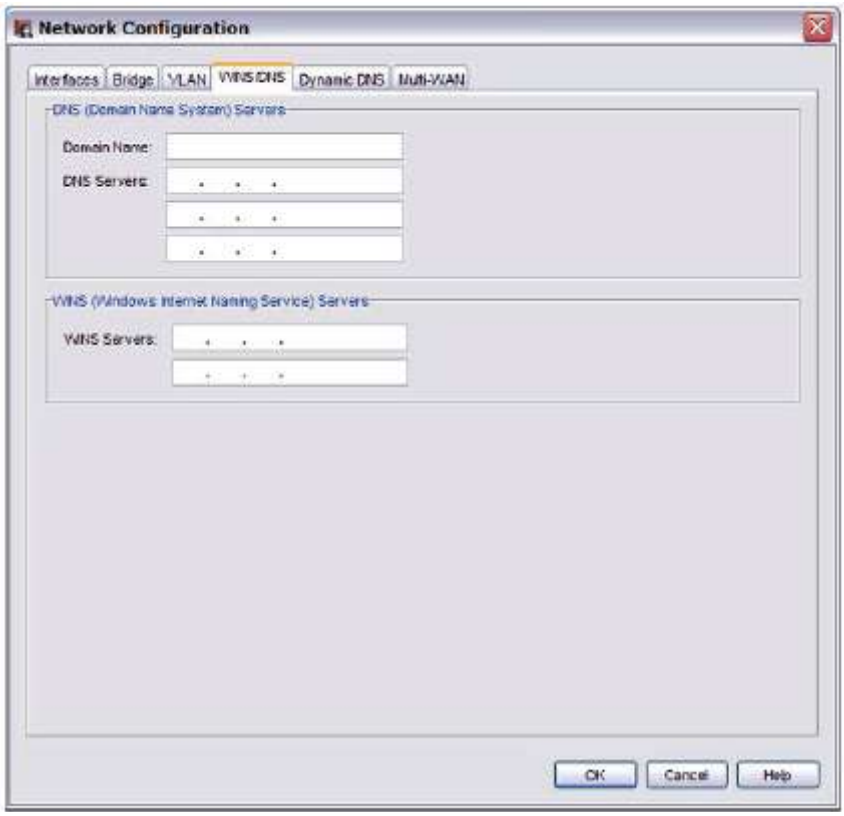
Настройка WINS и DNS серверов

Mobile VPN клиенты используют адреса WINS (Windows Internet Naming Service) и DNS (Domain Name System) серверов. DNS изменяет имена хостов на IP-адреса, в то время как WINS изменяет имя NetBIOS на IP-адреса. Интерфейс Trusted устройства Firebox® должен иметь доступ к этим серверам.

Убедитесь, что вы используете только внутренний DNS сервер. Не используйте внешние DNS серверы.

1. В Policy Manager выберите **Network > Configuration**.
Откроется диалоговое окно Network Configuration.

2. Выберите закладку **WINS/DNS**.
   Появится информация для WINS и DNS серверов



3. Введите имя домена для DNS сервера.

4. В текстовых полях **DNS Servers** и **WINS Servers** введите IP адреса WINS и DNS серверов.

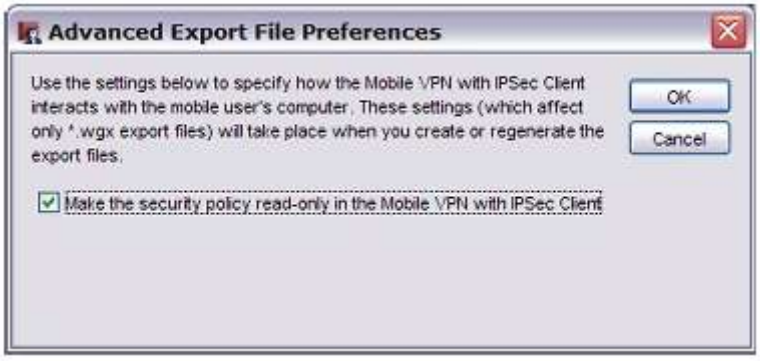
5. Нажмите **OK**.

Блокировка профиля пользователя

Вы можете заблокировать профиль конечного пользователя так, что пользователи могут только просматривать параметры профиля, но не менять их. Мы рекомендуем вам заблокировать все профили, чтобы пользователи не могли вносить какие-либо изменения в них. Эта функция доступна только для .wgx файлов профиля пользователя. Вы не можете сделать файлы .ini только для чтения.

1. В Policy Manager выберите **VPN > Mobile VPN > IPSec**.
   Откроется диалоговое окно Mobile VPN with IPSec Configuration.

2. Нажмите **Advanced**. Откроется диалоговое окно Advanced Export File Preferences



3. Для того чтобы мобильным пользователям предоставить только read-only доступ к своим профилям включите опцию **Make the security policy read-only in the MUVPN Client**.

4. Нажмите **OK**.

Сохранение профиля на Firebox

Для того чтобы активировать новый профиль пользователя Mobile VPN, вам необходимо сохранить конфигурационный файл на Firebox.

В Policy Manager, нажмите  .

Или выберите **File** > **Save** > **To Firebox**.

Конфигурационные файлы Mobile VPN with IPSec

Для того чтобы настроить клиент Mobile VPN with IPSec вам необходимо импортировать конфигурационный файл. Конфигурационный файл также называется файл профиля пользователей. Существует два типа конфигурационных файлов.

.wgx

.wgx файлы хранятся в зашифрованном виде. Вы также можете ограничить пользователям доступ к этим файлам.

.wgx файл не используется для настройки параметров Line Management в ПО клиента. Если вы в параметрах **Line Management** выбрали значение, не равное **Manual**, то вам необходимо использовать .iniф файл.

.ini

.ini файл используется только тогда, когда вы поменяли настройки **Line Management** (выбрали не **Manual**). .ini файл хранится в незашифрованном виде.

После того, как вы первый раз настроили Mobile VPN with IPSec группу, или сделали какие-либо изменения в существующей группе, то вам необходимо заново сгенерировать конфигурационный файл для группы и передать его пользователям. Конфигурационные файлы Mobile VPN, или профили, хранятся в каталоге:

C:\Documents and Settings\All Users\Shared Watchguard\muvpn\ip_address\config_name\wgx\config_name.wgx

и

C:\Documents and Settings\All Users\Shared Watchguard\muvpn\ip_address\config_name\ini\config_name.ini

Если для аутентификации вы используете сертификаты, то файлы сертификата также создаются.

Для того чтобы сгенерировать конфигурационный файл в Policy Manager выполните следующее:

1. В Policy Manager выберите **VPN >Mobile VPN > IPSec**.

2. Выберите группу Mobile VPN и нажмите **Generate.**

Теперь вы можете передать этот файл пользователям.

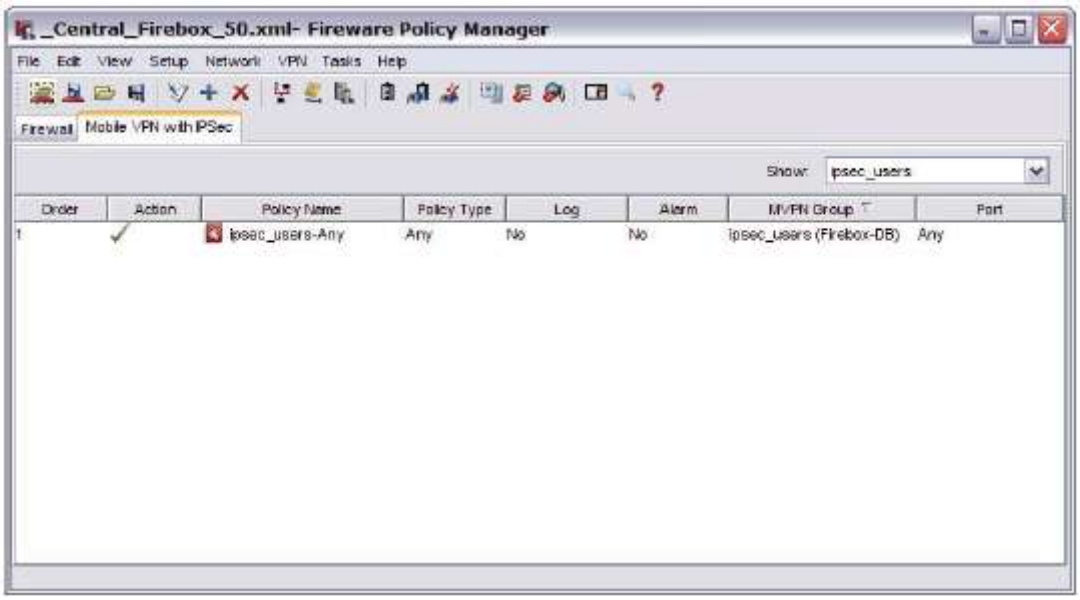
Настройка политик для фильтрации Mobile VPN трафика

В конфигурации по умолчанию пользователи Mobile VPN with IPSec имеют полный доступ к ресурсам Firebox с политикой *Any*.

Политика *Any* policy разрешает трафик на всех портах и все протоколы между Mobile VPN пользователем и ресурсами сети, доступной через Mobile VPN туннель. Для того чтобы заблокировать определенные порты и протоколы, политику Any можно удалить и заменить ее своими политиками, которые будут управлять доступом Mobile VPN пользователей к ресурсам сети.

Создание политик

1. В Policy Manager выберите закладку **Mobile VPN with IPSec**



2. В выпадающем списке **Show** выберите Mobile VPN группу, для которой вы хотите создать политику. Перед тем, как создать политику, вам необходимо выбрать группу, для которой эта политика будет создана.

3. Добавьте, удалите политики и сделайте необходимые изменения в настройках политики

4. Сохраните ваш конфигурационный файл.

Изменение вида

Вы можете смотреть списки политики двумя способами: Large icons или Detailed.

- Для того включить вид Large Icons выберите View > Large Icons.

- Для того включить вид Detailed выберите **View > Details**.

Под разделом **MVPN Group**, Policy Manager отобразит сервер аутентификации для Mobile VPN группы (в скобках)

Рассылка ПО и профилей

WatchGuard рекомендуем рассылать профили конечных пользователей при помощи зашифрованной почты или другим защищенным методом.

Для работы с Mobile VPN на каждом компьютере клиента должно находиться следующее:

- **Пакет установки ПО**

  Пакеты установки вы можете найти на сайте WatchGuard LiveSecurity Service: http://www.watchguard.com/support

  Войдите в систему под вашим именем пользователя и паролем учетной записи LiveSecurity Service.

  Нажмите на ссылку **Latest Software**, слева нажмите **Add-ons/Upgrades** и затем нажмите **Mobile VPN with IPSec**.

- **Профиль конечного пользователя**

  Этот файл содержит имя группы, ключ шифрования, и параметры, необходимые компьютеру для подключения к удаленной защищенной сети по незащищенному каналу связи. Имя файла профиля - **groupname.wgx**. По умолчанию файл .wgx находится в следующем каталоге:

  C:\Documents and Settings\All Users\Shared WatchGuard \muvpn\<IP address of Firebox>\<Mobile VPN with IPSec group name\wgx

- **Два файла сертификата, если вы используете сертификаты для аутентификации**

  Это .p12 файл – зашифрованный файл, которые содержат сертификат; и cacert.pem, который содержит сертификат ЦС (корневой сертификат). Файлы .p12 и cacert.pem находятся в том же каталоге, что и файл профиля пользователя.

- **Документация пользователя**

  Документация помогает удаленному пользователю установить клиент Mobile VPN и импортировать конфигурационный файл Mobile VPN

- **Ключ шифрования**

  Для того чтобы импортировать профиль пользователя, пользователю необходимо будет ввести ключ шифрования. Этот ключ используется для расшифрования файла и импортирует политику безопасности в клиента Mobile VPN. Ключ создается во время создания файла в Policy Manager

Пароль профиля пользователя, имя пользователя и пароль пользователя являются очень важной информацией. С целью обеспечения безопасности, мы не рекомендуем рассылать эту информацию средствами электронной почты. Эти данные лучше сообщить пользователю лично, или использовать другой способ, при котором неавторизованное лицо не сможет перехватить эту информацию.

Дополнительная информация по Mobile VPN

В этом разделе приводится дополнительная информация по Mobile VPN with IPSec.

Создание исходящих IPSec соединений через Firebox

Бывают ситуации, когда пользователю необходимо создать IPSec соединение с Firebox с устройства, которое находится за другим Firebox. Например, если мобильный сотрудник находится на сайте, где установлен Firebox, то он может создать IPSec подключение к своей сети . Для того чтобы локальный Firebox корректно обрабатывал исходящие IPSec соединения, вам необходимо настроить политику IPSec, которая включает пакетный фильтр IPSec

Так политика IPSec включает туннель к IPSec серверу и не выполняет никаких проверок на межсетевом экране, то вам необходимо к этой политике добавить только пользователей, которым вы доверяете

Закрытие IPSec соединений

Для того чтобы полностью закрыть VPN соединения, вам необходимо перезагрузить Firebox. Удаление политики IPSec не закрывает текущие соединения.

Глобальные настройки VPN

Глобальные **настройки** VPN на вашем Firebox применяются ко всем ручным BOVPN и Mobile VPN туннелям. Вы можете использовать эти настройки для:

- Включения IPSec pass-through
- Удаления или сохранения значений битов Type of Service (TOS)
- Использования LDAP сервера для проверки сертификатов

Для того чтобы изменить эти параметры в Policy Manager выберите **VPN > VPN Settings**

Просмотр количества Mobile VPN лицензий

Вы можете посмотреть количество лицензий Mobile VPN, установленных из Policy Manager.

1. Выберите **Setup > Feature Keys**.
   Откроется диалоговое окно Firebox Feature Key.

2. Найдите **Mobile User VPN Users** в колонке **Features**, и посмотрите число в колонке **Capacity**. Это количество установленных лицензий Mobile VPN.

Приобретение дополнительных Mobile VPN лицензий

WatchGuard Mobile VPN with IPSec является дополнительным компонентом. Каждое устройство Firebox X device содержит определенное количество лицензий Mobile VPN. Вы можете приобрести дополнительные лицензии для Mobile VPN. Лицензии вы можете приобрести у вашего локального реселлера или на сайте: http://www.watchguard.com/sales

Добавление ключей функций

Для более подробной информации о ключах функций см. “Ключи функций (Feature Keys)”

Mobile VPN и VPN переключение

Вы можете настроить VPN туннели для переключения на резервные точки подключения, если основная точка становится недоступной

Если VPN failover настроен и происходит сбой, сессии Mobile VPN закрываются. Для того чтобы создать новый Mobile VPN туннель вам необходимо снова аутентифицировать пользователя. Для того чтобы настроить VPN failover для Mobile VPN туннелей выполните следующее:

1. В Policy Manager выберите **VPN > Mobile VPN > IPSec**. Откроется диалоговое окно Mobile VPN with IPSec Configuration.

2. Выберите группу мобильных пользователей и нажмите **Edit**.
   Откроется диалоговое окно Edit Mobile VPN with IPSec.

3. Выберите закладку **General**.

Введите IP-адрес резервного WAN интерфейса в поле **Backup** секции **Firebox IP Addresses**. Вы можете указать только один интерфейс

Настройка Mobile VPN with IPSec для использования динамического IP адреса

Для устройства Firebox, который используется как конечная точка VPN туннеля, мы рекомендуем использовать статический IP адрес или использовать сервис Динамического DNS

Если вы не можете использовать обе из вышеприведенных опций и внешний IP адрес Firebox является динамическим, то при каждом изменении IP адреса Firebox вам необходимо генерировать новый конфигурационный файл профиля пользователя и рассылать его всем Mobile VPN пользователям, или сообщать пользователям о том, что необходимо изменить конфигурационный файл. В противном случае, IPSec пользователи не смогут установить соединение.

Ниже приведены инструкции, как настроить Firebox и IPSec клиенты в случае если Firebox имеет внешний динамический IP адрес и вы не можете использовать Динамический DNS.

Как узнать текущий IP адрес

Для того чтобы узнать текущий IP адрес External интерфейса устройства Firebox выполните следующее:

1. В Policy Manager выберите **Network > Configuration**.

2. IP адрес интерфейса вы можете посмотреть в колонке IP интерфейса **External**.

Это IP адрес, который сохраняется в конфигурационном .wgx файле. Если удаленные пользователи не могут подключиться, то вам необходимо проверить, не изменился ли внешний IP адрес.

Настройка Firebox и компьютеров клиентов IPSec

Перед тем, как загрузить .wgx файлы, устройство Firebox должно иметь IP адрес, присвоенный External интерфейсу. Это единственное отличие от нормальной конфигурации устройства Firebox и IPSec клиентов

Обновление конфигурации клиентов после изменения внешнего IP адреса Firebox

После того, как внешний IP адрес устройства Firebox меняется, удаленные Mobile VPN with IPSec пользователи не смогут подключаться до тех пор, пока они не получат информацию о новом IP адресе. Изменить IP адрес вы можете сделать двумя способами.

- Передать пользователям новый .wgx файл для импорта.

- Предоставить пользователям возможность вручную изменять конфигурацию IPSec клиента. Для того чтобы использовать эту опцию, вам необходимо настроить Firebox таким образом, чтобы удаленные пользователи могли сами редактировать конфигурацию

Для того чтобы передать пользователям новый .wgx файл:

1. В Policy Manager выберите **VPN >Mobile VPN > IPSec**.

2. Выберите группу Mobile VPN и нажмите **Generate** для создания и загрузки .wgx файлов.

3. Передайте .wgx файлы удаленным пользователям.

4. Сообщите удаленным пользователям, что им необходимо импортировать профиль пользователя.

Для того чтобы пользователи могли сами редактировать конфигурацию клиентов выполните следующее:

1. Сообщите пользователям новый внешний IP адрес Firebox. Затем попросите пользователей выполнить следующие пять шагов
2. На компьютере, на котором установлен IPSec клиент, выберите **Start** > **All Programs** > **WatchGuard Mobile VPN** > **Mobile VPN Monitor**.
3. Выберите **Configuration** > **Profile Settings**.
4. Выберите профиль и нажмите **Configure**.
5. В левой колонке выберите **IPSec General Settings**.
6. Для **Gateway** введите новый внешний IP адрес устройства Firebox.

Клиент Mobile VPN with IPSec

Клиент WatchGuard Mobile VPN with IPSec устанавливается на компьютер пользователя. Пользователь через Интернет активирует клиент Mobile VPN. Клиент Mobile VPN создает зашифрованный туннель к вашим доверенной и Optional сетям, которые защищены WatchGuard Firebox. Клиент Mobile VPN разрешает вам предоставлять удаленный доступ к вашим внутренним сетям.

Требования к клиенту

Перед тем как установить клиента, посмотрите приведенные ниже требования и рекомендации.

Вы можете устаноить клиент Mobile VPN with IPSec на любой компьютер под управлением Windows 2000 Professional, Windows XP (32-bit) или Windows Vista (32-bit and 64-bit). Перед тем как установить клиент, убедитесь, что на удаленном компьютере не установлено никакого другого ПО Mobile User VPN. Вам также необходимо удалить любой программный межсетевой экран (кроме Microsoft firewall) с каждого удаленного компьютера.

- Если на компьютере клиента установлена Windows XP, вам необходимо войти в систему под учетной записью, у которой есть администраторские права для установки клиента и импорта конфигурационного файла. После того, как вы установили и настроили клиент, для подключения администраторские права уже не нужны.
- Если на компьютере клиента установлена Windows Vista, вам необходимо войти в систему под учетной записью, у которой есть администраторские права для установки клиента и импорта конфигурационного файла.
- Перед тем как установить клиент Mobile VPN проверьте, установлены ли все доступные пакеты обновлений на компьютере
- Настройки WINS и DNS для клиента Mobile VPN client извлекаются из профиля клиента, импортированного во время настройки клиента Mobile VPN.

Мы рекомендуем вам не менять конфигурацию клиента Mobile VPN, если это не описано в данной документации

Установка клиента Mobile VPN with IPSec

Процедура установки клиента состоит из двух частей: установка клиента на удаленном компьютере и импорт профиля конечного пользователя. Перед тем как начать установку, убедитесь, что у вас все необходимые компоненты для установки, которые вы можете получить у вашего администратора:

- Файл установки Mobile VPN
- Профиль пользователя с файлом .wgx
- Ключ шифрования
- файл сертификата .p12 (Если вы подключаетесь к Firebox X Core и Peak и для аутентификации используете сертификаты)
- Имя пользователя и пароль

Запишите пароль и храните его в безопасном месте. Пароль вам необходимо будет ввести в конце установки.

Для того чтобы установить клиент выполните следующее:

1. Скопируйте файл установки Mobile VPN на удаленный компьютер и извлеките содержимое файла архива.
2. Скопируйте профиль пользователя (файл .wgx) в корневой каталог на удаленном компьютере (клиент или пользователь).
   Если для аутентификации вы используете сертификаты, в корневой каталог также скопируйте .p12 файл.
3. Запустите исполняемый файл Mobile VPN Запустится мастер WatchGuard Mobile VPN Installation. После того, как мастер завершит работу, вам необходимо перезагрузить ваш компьютер.

Импорт профиля пользователя

После того, как компьютер перезагрузится, откроется диалоговое окно WatchGuard Mobile VPN Connection Monitor. При первом запуске программы вы увидите следующее сообщение:

```
There is no profile for the VPN dial-up! Do you want to use the Configuration Assistant for generating a profile now?
```

Нажмите **No**.

Для того чтобы отключить автоматический запуск Connection Monitor, выберите **Window > AutoStart > No Autostart**. Для того чтобы импортировать конфигурационный файл или .ini файл Mobile VPN выполните следующее:

1. Выберите **Start** > **All Programs** > **WatchGuard Mobile VPN** > **Mobile VPN Monitor**.
2. Выберите **Configuration > Profile Import**.
   Запустится мастер Profile Import Wizard.
3. В окне **Select User Profile** найдите файлы .wgx или .ini. Нажмите **Next**.
4. Нажмите **Next**.
5. Если вы используете .wgx файл, то на странице **Decrypt User Profile** введите пароль. Пароль зависим от регистра символов.
6. Нажмите **Next**.
7. На странице **Overwrite or add Profile** вы можете выбрать, перезаписать ли текущий профиль с таким же именем.
8. Нажмите **Next**.

9. В окне **Authentication** вы можете выбрать, вводить ли имя пользователя и пароль для аутентификации туннеля. Если вы оставите эти поля пустыми, при каждом подключении к VPN вам необходимо будет вводить имя пользователя и пароль. Если вы введете ваше имя пользователя и пароль здесь, Firebox сохранит эту информацию и вам не надо будет вводить ее при каждом подключении. Однако, это потенциальная угроза безопасности. Вы также можете ввести только имя пользователя, оставив поле пароля пустым.

10. Нажмите **Next**.

11. Нажмите **Finish**.
Теперь компьютер готов для работы с Mobile VPN with IPSec.

Выбор сертификата и ввод PIN кода

Если для аутентификации вы используете сертификаты, вам необходимо выбрать корректный сертификат. У вас должен быть cacert.pem и .p12 файл.

1. Выберите **Configuration** > **Certificates**.

2. В закладке **User Certificate** в выпадающем списке **Certificate** выберите **from PKS#12 file**.

3. Рядом с полем **PKS#12 Filename** нажмите на кнопку и найдите файл .p12.

4. Нажмите **OK**.

5. Выберите **Connection** > **Enter PIN**.

6. Введите PIN и нажмите **OK**.
PIN – это пароль, который используется для шифрования файла при работе с мастером Add Mobile User VPN Wizard.

Удаление клиента Mobile VPN

В некоторых ситуациях вам возможно понадобится удалить клиент Mobile VPN. Для удаления клиента Mobile VPN мы рекомендуем использовать утилиту Windows Add/Remove Programs. Перед тем как начать процедуру удаления, отключите все туннели и закройте Mobile VPN Connection Monitor. Затем выполните следующее:

1. Выберите **Start** > **Settings** > **Control Panel**.
Откроется окно Control Panel.

2. Два раза нажмите на иконку **Add/Remove** Programs.
Откроется окно Add/Remove Programs.

3. Выберите **WatchGuard Mobile VPN** и нажмите **Change/Remove**.
Откроется окно InstallShield Wizard.

4. Нажмите **Remove** и нажмите **Next**.
Откроется диалоговое окно Confirm File Deletion.

5. Нажмите **OK** для того чтобы полностью удалить все компоненты.

Если вы не включите эту опцию в конце процедуры удаления, то при следующей установке Mobile VPN клиента все настройки соединения, которые использовались в этой установке, будут использовать для новой установки.

Подключение и отключение клиента Mobile VPN

Клиент WatchGuard Mobile VPN with IPSec создает защищенное подключение с удаленного компьютера к вашей защищенной сети через Интернет. Для того чтобы создать такое подключение, вам необходимо подключиться к сети Интернет и использовать клиент Mobile VPN

для подключения к защищенной сети. Настройте подключение к сети Интернет через Dial-Up Networking или LAN. Затем выполните приведенные ниже инструкции или выберите ваш профиль. Для того чтобы подключить или отключить клиент нажмите правой кнопкой мыши на иконку Mobile VPN в панели инструментов Windows.

1. Выберите **Start** > **All Programs** > **WatchGuard Mobile VPN** > **Mobile VPN Monitor**.

2. Из выпадающего списка **Profile** выберите профиль, который вы создали для ваших Mobile VPN соединений. Нажмите **Connect**.

3. Нажмите **Connect**

Отключение Mobile VPN клиента

В диалоговом окне Mobile VPN Monitor нажмите **Disconnect**.

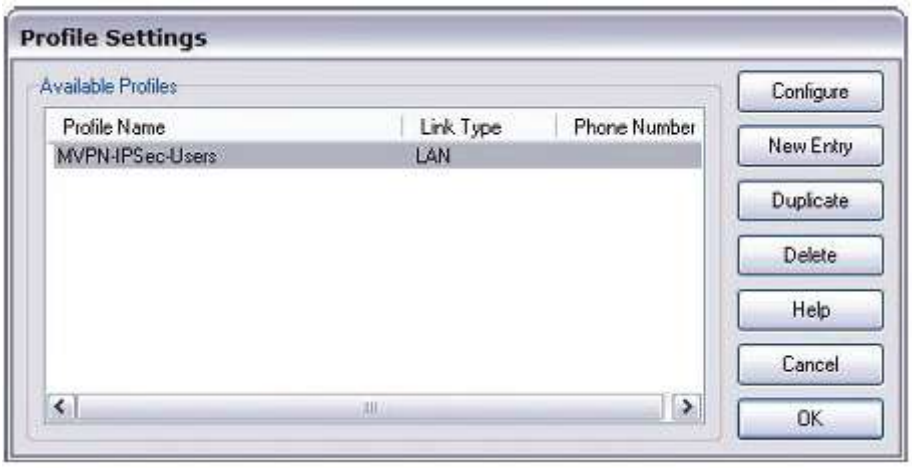
Управление соединением

Для каждого импортированного профиля, вы можете настроить действие, которое будет выполнять Mobile VPN клиент в случае если VPN туннель по какой-то причине становится недоступным. Вы можете настроить эти параметры на устройстве WatchGuard и сохранить их в .ini файл, и затем с помощью этого файла настроить программу клиента. .wgx не используется для изменения этих параметров.

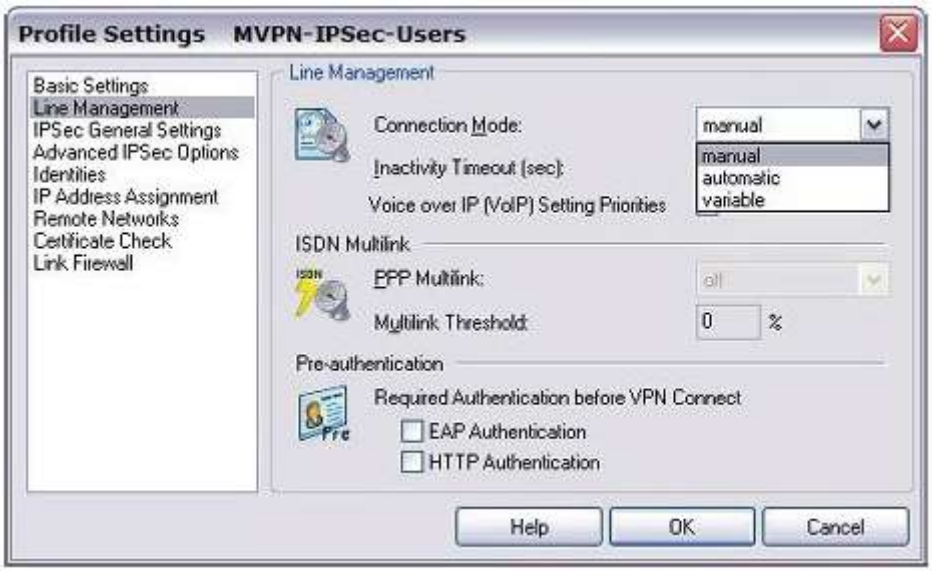
Для того чтобы настроить поведение клиента Mobile VPN при выходе из строя VPN туннеля выполните следующее:

1. В WatchGuard Mobile VPN Connection Monitor выберите **Configuration > Profile Settings**.

2. Выберите имя профиля и нажмите **Configure**



3. В левой панели выберите **Line Management**



4. Из выпадающего списка **Connection Mode** выберите необходимый режим.

   Manual — если вы выберете режим **manual**, клиента не будет автоматически перезагружать туннель при его выходе из строя. Для того чтобы перезапустить туннель вам необходимо нажать кнопку **Connect** в Connection Monitor или нажать правой кнопкой на иконку Mobile VPN в панели инструментов Windows и нажать **Connect**.

   Automatic — Если вы выберете режим **automatic**, то клиент попытается начать соединение, когда ваш компьютер передает трафик в место назначение, доступ к которому вы можете получить через VPN. Также клиент пытается автоматически перезагрузить VPN туннель, если он вышел из строя.

   Variable — Если вы выберете режим **variable**, клиент пытается автоматически перезапустить VPN туннель до тех пока, пока вы не нажмете **Disconnect**. Клиент не будет пытаться перезагрузить VPN туннель после того, как в следующий раз вы нажмете **Connect**.

5. Нажмите **OK**.

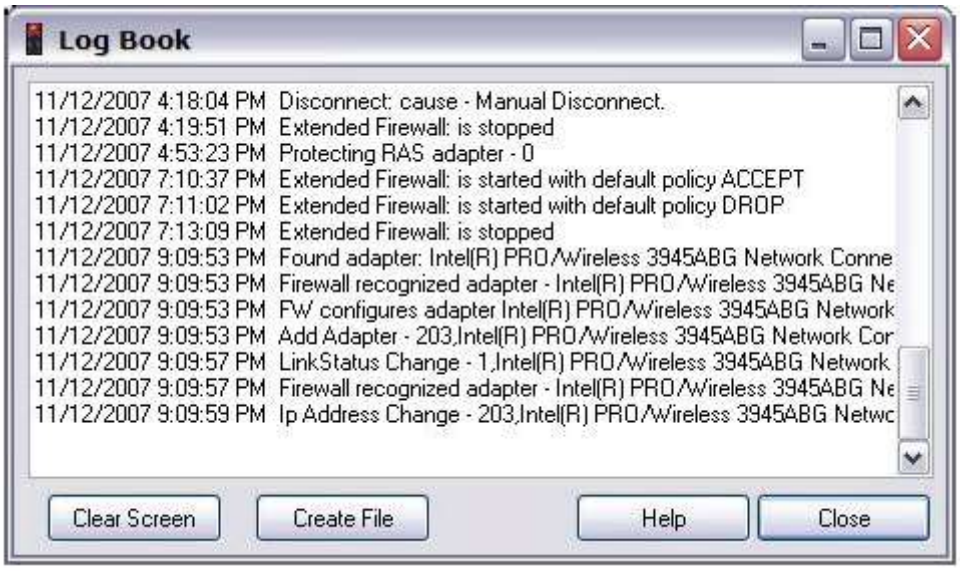
Иконка программы клиента Mobile User VPN

Иконка Mobile User VPN появляется в панели задач Windows и показывает статус межсетевого экрана, **link firewall** и VPN сети. Для того чтобы отключить или подключить клиента, или посмотреть какой профиль используется на данный момент, нажмите на иконку правой кнопкой и выберите соответствующий пункт меню.

Просмотр сообщений журнала Mobile VPN

Вы можете использовать файл журналов клиента Mobile VPN для решения проблем, которые возникают в процессе создания VPN подключения.

Для того чтобы посмотреть файлы журналов Mobile VPN выберите **Log > Logbook** в Connection Monitor.
Откроется диалоговое окно Log Book



Защита вашего компьютера с помощью брандмауэра Mobile VPN

Клиент WatchGuard Mobile VPN with IPSec содержит два компонента брандмауэра:

Link firewall

link firewall не включен по умолчанию. Когда link firewall включен, ваш компьютер будет блокировать все пакеты, которые поступают с других компьютеров. Вы можете включать link firewall только если Mobile VPN туннель активен.

Desktop firewall

Этот межсетевой экран может управлять всеми подключениями вашего компьютера. Вы можете настроить дружественные сети и настроить правила доступа отдельно для дружественных и неизвестных сетей.

Включение link firewall

Если link firewall включен, клиент Mobile VPN блокирует любые пакеты, отправленные вашему компьютеру с других хостов. Он разрешает только пакеты, которые были отправлены в ответ на запрос, отправленный вашим компьютером. Например, если вы отправляете запрос на HTTP сервер через туннель с вашего компьютера, то трафик, который будет передаваться в ответ на ваш запрос будет разрешен. Если хост пытается отправить HTTP запрос на ваш компьютер через туннель, то этот запрос блокируется. Для того чтобы включить link firewall выполните следующее:

1. В WatchGuard Mobile VPN Connection Monitor выберите **Configuration > Profile Settings**.

2. Выберите профиль, для которого вы хотите включить Link Firewall и выберите **Configure**.

3. В левой панели выберите **Link Firewall**

4. Из выпадающего списка **Stateful Inspection** выберите **when connected** или **always**. Если вы выберете **when connected**, то link firewall будет работать при наличии активного туннеля для этого профиля. Если вы выберете **always**, то link firewall всегда работает в независимости от того, активен туннель или нет.

5. Нажмите **OK**.

Desktop Firewall

Когда вы включаете **правило** в вашей конфигурации брандмауэра, вам необходимо указать к какому типу сети это правило будет применяться. В клиенте Mobile VPN client определены три типа сетей:

VPN networks

Сети, определенные для клиента в импортированном профиле.

Unknown networks

Любая сеть, не указанная в брандмауэре.

Friendly networks

Любая сеть в межсетевом экране, которая определена как известная

Включение Desktop Firewall

Для того чтобы включить desktop firewall выполните следующее:

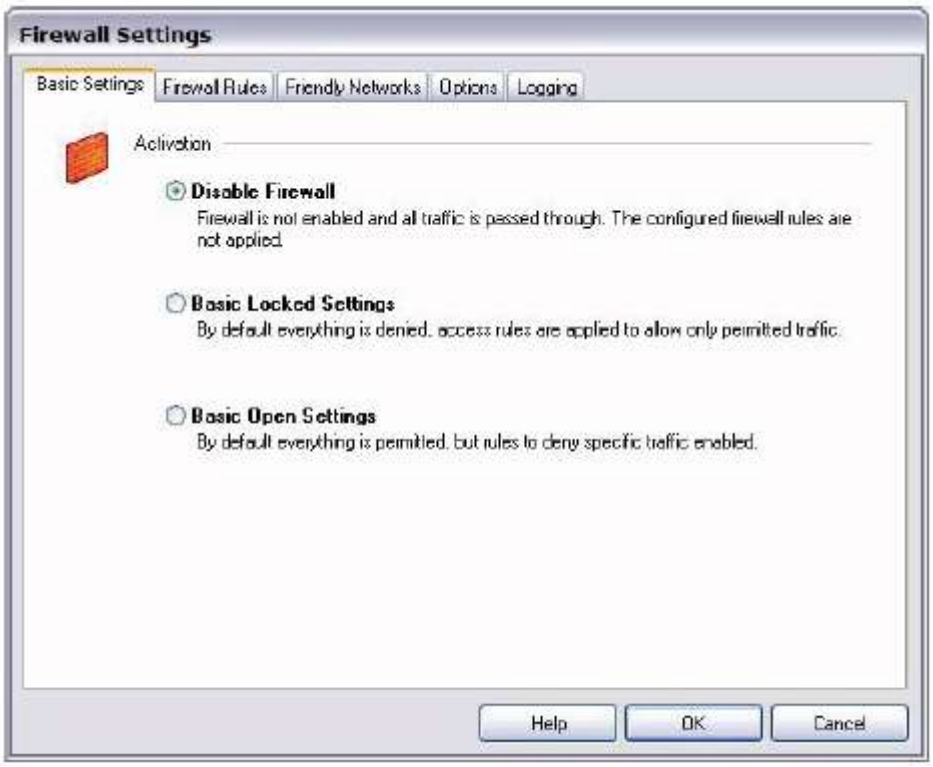
1. В WatchGuard Mobile VPN Connection Monitor выберите **Configuration > Firewall Settings**. *Межсетевой экран отключен по умолчанию.*

2. После того, как вы включите межсетевой экран, вам необходимо выбрать два режима:

   Basic Locked Settings — в этом режиме межсетевой экран блокирует все исходящие и

входящие соединения вашего компьютера, только если вы не создали правило, которое разрешает эти соединения.

Basic Open Settings — в этом режиме межсетевой экран разрешает все соединения, только если вы не создали правило, которое запрещает эти соединения



3. Нажмите **OK**.

После того, как вы включили desktop firewall, вы можете настроить параметры вашего межсетевого экрана

Создание дружественных сетей

Вы можете сгенерировать правило межсетевого экрана для известных вам сетей. Например, если вы хотите использовать клиент Mobile VPN в локальной сети, где ваш компьютер будет доступен другим компьютерам сети, вы можете добавить адрес этой сети в качестве дружественной сети. При этом правила брандмауэра для этой LAN будут отличаться от правил брандмауэра, которые вы создали для подключений к сети Интернет и удаленных VPN сетей.

1. В диалоговом окне **Firewall Settings** выберите закладку **Friendly Networks**.

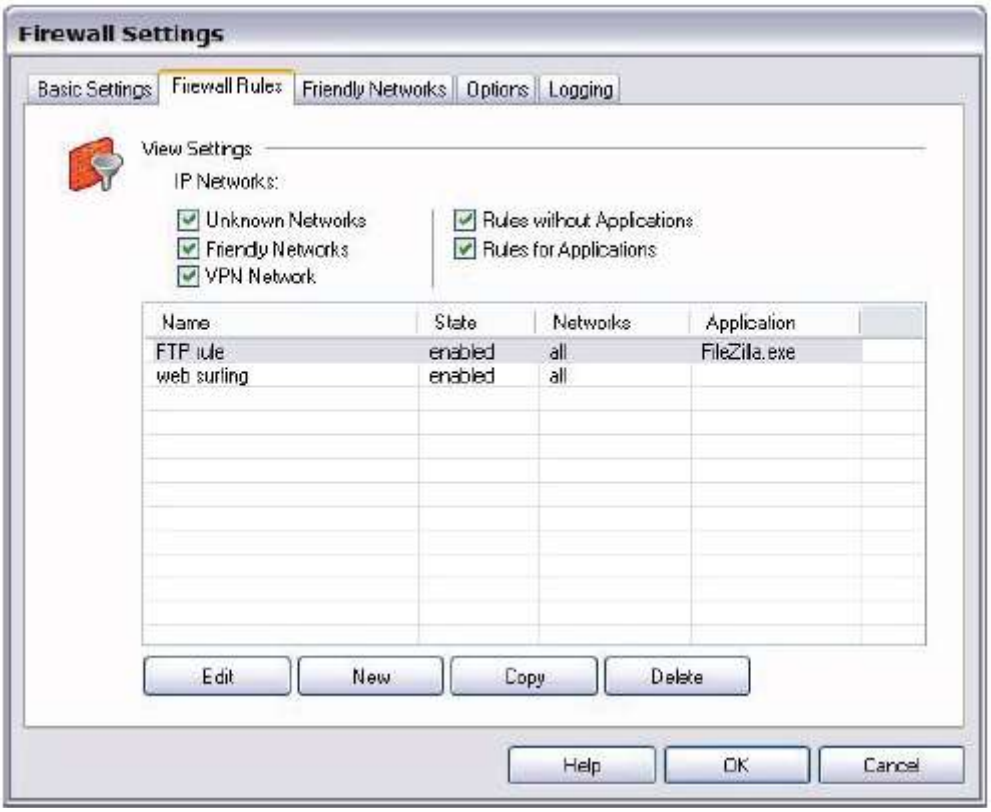
2. Нажмите **New** для того чтобы добавить дружественную сеть.

В этом релизе компонент **Automatic Friendly Network Detection** не работает.

Создание правил брандмауэра

Вы можете создать исключения для режима межсетевого экрана, который вы выбрали при включении межсетевого экрана в закладке **Firewall Rules** диалогового окна **Firewall Settings**. Например, после того как вы включили межсетевой экран и выбрали режим **Basic Locked Settings**, то правила, созданные здесь, будут разрешать трафик. Если вы выбрали **Basic Open Settings**, то правила, созданные здесь будут запрещать трафик.

Правила межсетевого экрана могут включать несколько номеров портов от одного протокола. Для того чтобы показать категории правил межсетевого экрана отметьте необходимые флаги под секцией **View Settings**.



Для того чтобы создать правило нажмите **New**. Для настройки трафика, которым вы хотите управлять, вы можете использовать четыре закладки диалогового окна **Firewall Rule Entry**:

- Закладка General
- Закладка Local
- Закладка Remote
- Закладка Applications

Закладка General

В этой закладке вы можете настроить базовые параметры правил брандмауэра

Rule Name

Введите имя для правила. Например, вы можете создать правило Web surfing, которое будет включать трафик через TCP порты 80 (HTTP), 8080 (alternate HTTP) и 443 (HTTPS).

State

Для того чтобы отключить правило, выберите **Disabled**. Новые правила включены по умолчанию.

Direction

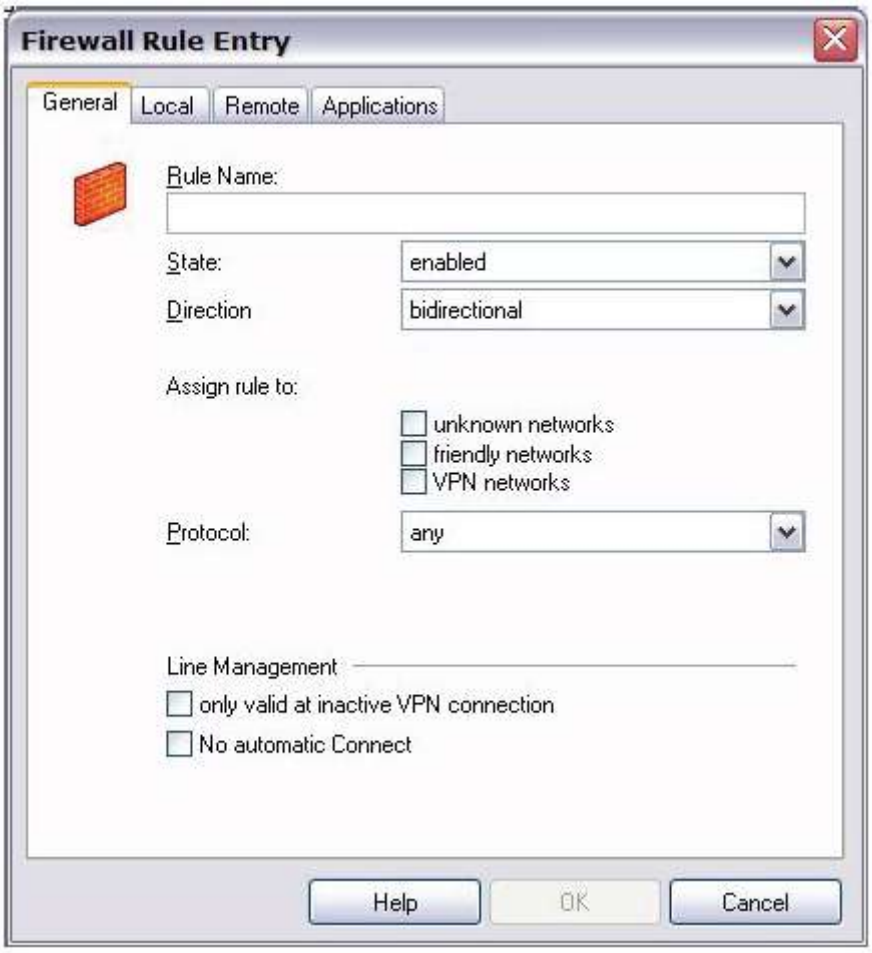
Для того чтобы применять правило к входящему трафику выберите **outgoing**. Для того чтобы применить правило к исходящему трафику выберите **incoming**. Для того чтобы применить правило к обеим направлениям выберите **bidirectional**.

Assign rule to

Напротив типов сетей, для которых вы хотите применить правило, отметьте флаги.

Protocol

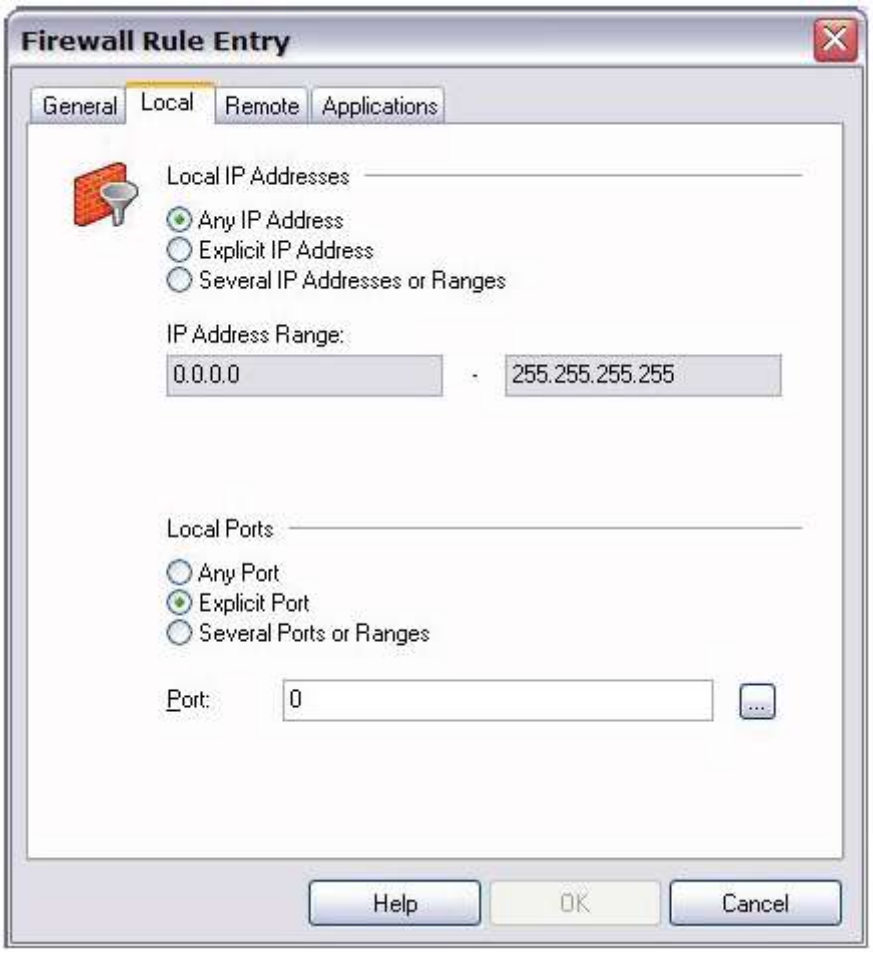
При помощи выпадающего списка выберите тип трафика, которым вы хотите управлять



Закладка Local

В закладке **Local** вы можете указать любые IP-адреса и порты, которые будут управляться вашим правилом межсетевого экрана. Мы рекомендуем в любом правиле при настройке значения **Local IP Addresses** выбирать переключатель **Any IP address**. Если вы настраиваете входящую политику, вы можете добавить порты, которые будут управлять этой политикой. Если вы хотите в одной политике управлять несколькими портами, выберите **Several Ports or Ranges**. Для того чтобы добавить новый порт нажмите **New**.

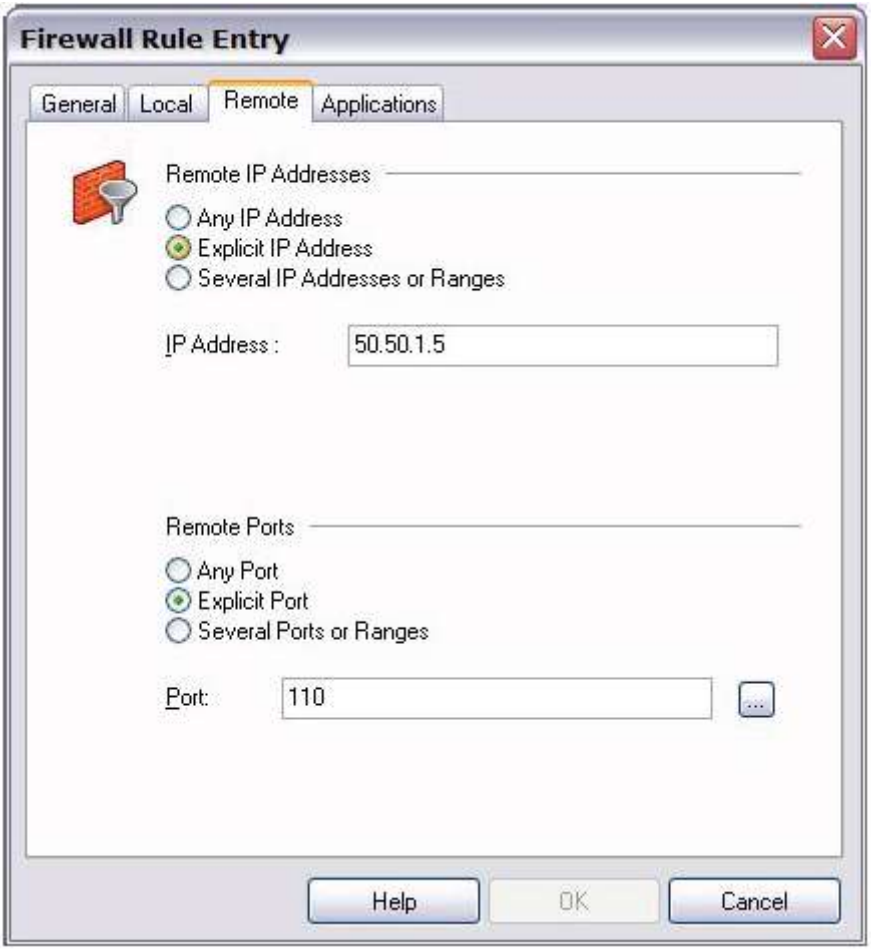
Если вы выберете переключатель **Explicit IP Address**, не забудьте указать IP-адрес. IP-адрес не должен быть равен 0.0.0.0



Закладка Remote

Здесь вы можете указать любое количество удаленных IP-адресов, которые будут управлять данным правилом. Например, если ваш межсетевой экран блокирует весь трафик и вы хотите создать правило для того чтобы разрешить исходящий POP3 трафик, добавьте IP-адрес вашего сервера POP3 в качестве **Explicit IP Address** в диалоговом окне **Remote IP Addresses**. Затем в секции **Remote Ports**, укажите порт 110 в качестве **Explicit Port** для этого правила.

Если вы выберете переключатель **Explicit IP Address**, не забудьте указать IP-адрес. IP-адрес не должен быть равен 0.0.0.0



Закладка Applications

Вы можете ограничить правило межсетевого экрана таким образом, что оно будет применяться для определенного приложения

1. В закладке **Applications** диалогового окна Firewall Rule Entry включите опцию **Bind Rule To Application below**.

2. Выберите **Select Application** для того чтобы найти необходимые приложения на вашем компьютере.

3. Нажмите **OK**

Инструкции для установки клиента Mobile VPN with IPSec

Эти инструкции написаны для пользователей программы клиента Mobile VPN with IPSec. В них пользователям рекомендуют обращаться к администратору сети для информации по установке программного брандмауэра или его настройки, как часть процедуры установки программы клиента, и для настройки параметров, которые управляют подключением, если не используется файл .ini. Вы можете распечатать эти инструкции или использовать их для создания списка инструкций для ваших конечных пользователей.

Клиент Mobile VPN with IPSec создает зашифрованное соединение между вашим компьютером и Firebox через стандартный Интернет канал. Программа клиента Mobile VPN предоставляет вам доступ к ресурсам защищенной сети из любого места, где есть подключение к сети Интернет.

Перед тем как установить программу клиента, убедитесь, что вы понимаете эти требования и рекомендации:

- Вы можете установить программу клиента Mobile VPN with IPSec на любой компьютер с установленной Windows 2000 Pro, Windows XP (32-bit and 64-bit) или Windows Vista (32-bit and 64-bit).
- Проверьте, не установлено ли на ваш компьютер других программ клиента IPSec mobile user VPN.
- Удалите любой программный брандмауэр (кроме Microsoft firewall) с вашего компьютера.
- Если на компьютере установлена ОС Windows XP, то для того чтобы установить программу клиента Mobile VPN и импортировать конфигурационный файл, вам необходимо войти в систему под правами администратора. Права администратора не нужны для подключения, только для установки и настройки.

- Если на компьютере установлена ОС Windows Vista, то для того чтобы установить программу клиента Mobile VPN и импортировать конфигурационный файл, вам необходимо войти в систему под правами администратора. Права администратора не требуются для импорта .wgx или .ini файлы, или для подключения.

- Вы рекомендуем перед установкой программы клиента Mobile VPN вам проверить все установленные пакеты обновлений.

- Мы не рекомендуем изменять параметры клиента Mobile VPN, если их описания нет в этой документации.

Перед тем, как запустить процедуру установки, то убедитесь, что у вас есть следующие компоненты:

- Файл установки программы клиента Mobile VPN with IPSec

- Профиль пользователя (.wgx или .ini файл)

- Пароль (если конечный пользователь использует .wgx файл или при подключении для аутентификации используются сертификаты)

- Имя пользователя и пароль

- cacert.pem и .p12 файлы сертификата (если при подключении для аутентификации используются сертификаты)

Установка программы клиента

1. Скопируйте .zip файл Mobile VPN на удаленный компьютер и извлеките содержимое файла архива. Не запускайте файл установки с CD или другого внешнего накопителя.

2. Скопируйте профиль пользователя (.wgx или .ini файлы) в корневой каталог.
   Если для аутентификации вы используете сертификаты, скопируйте файлы cacert.pem и .p12 в корневой каталог.

3. Два раза нажмите на файл .exe. При этом запустится мастер WatchGuard Mobile VPN Installation Wizard. После окончания работы мастера, вам необходимо будет перезагрузить ваш компьютер.

4. Выполните все необходимые инструкции мастера (не меняйте значения параметров по умолчанию).

5. После того, как мастер завершит работу, вам необходимо перезагрузить компьютер.

6. После того, как компьютер перезагрузится, откроется диалоговое окно WatchGuard Mobile VPN Connection Monitor.

   Если вы запускаете программу клиента в первый раз, вы увидите следующее сообщение:

   ```
   There is no profile for the VPN dial-up!

   Do you want to use the Configuration Assistant for generating a profile now?
   ```

7. Нажмите **No**.

8. Выберите **Window > Autostart > No Autostart.** После этого программа не будет запускаться автоматически.

После того, как вы установили программу клиента, установите заново ваш программный брандмауэр или настройте брандмауэр, который устанавливается, как часть программы клиента.

Если вы используете программный брандмауэр стороннего производителя, то убедитесь, что он разрешит трафик для создания VPN туннеля и другого трафика, который передается по туннелю. Для более подробной информации обратитесь к вашему администратору сети.

Импорт профиля пользователя

Файл профиля пользователя используется для настройки параметров программы клиента Mobile VPN, которые используются для работы с VPN туннелями. Для того чтобы импортировать .wgx или .ini файлы выполните следующее:

1. Выберите **Start** > **All Programs** > **WatchGuard Mobile VPN** > **Mobile VPN Monitor**.
2. В WatchGuard Mobile VPN Connection Monitor выберите **Configuration > Profile Import**. *Откроется мастер Profile Import Wizard.*
3. На странице **Select User Profile** найдите файлы .wgx или .ini.
4. Нажмите **Next**.
5. Если вы используете .wgx файл, то на странице **Decrypt User Profile** введите пароль. Этот пароль зависит от регистра.
6. Нажмите **Next**.
7. На странице **Overwrite or add Profile** вы можете выбрать, перезаписать ли текущий профиль с таким же именем.
8. Нажмите **Next**.
9. В окне **Authentication** вы можете выбрать, вводить ли имя пользователя и пароль для аутентификации туннеля. Если вы оставите эти поля пустыми, при каждом подключении к VPN вам необходимо будет вводить имя пользователя и пароль. Если вы введете ваше имя пользователя и пароль здесь, Firebox сохранит эту информацию и вам не надо будет вводить ее при каждом подключении. Однако, это потенциальная угроза безопасности. Вы также можете ввести только имя пользователя, оставив поле пароля пустым.
10. Нажмите **Next**.
11. Нажмите **Finish**.

Выбор сертификата и ввод пароля

Выполните инструкции, приведенные в этом разделе, если у вас есть cacert.pem и .p12 файлы.

1. Выберите **Configuration** > **Certificates**.
2. В закладке **User Certificate** В выпадающем списке **Certificate** выберите **from PKS#12 file**.
3. Рядом с полем **PKS#12 Filename** нажмите на кнопку и найдите файл .p12.
4. Нажмите **OK**.
5. Выберите **Connection** > **Enter PIN**.
6. Введите пароль и нажмите **OK**.

Подключение и отключение программы клиента Mobile VPN

Настройте подключение к сети Интернет через Dial-Up Networking или LAN. Затем выполните приведенные ниже инструкции для выбора профиля, подключения или отключения.

Для того чтобы выбрать ваш профиль и подключить программу клиента Mobile VPN:

1. Выберите **Start** > **All Programs** > **WatchGuard Mobile VPN** > **Mobile VPN Monitor**.
   Откроется диалоговое окно WatchGuard Mobile VPN

2. В выпадающем списке **Profile** выберите импортированный профиль

3. Нажмите **Connect**.
   Если вы успешно подключитесь, то иконка программы клиента Mobile User VPN появится в панели задач Windows.

Для того чтобы отключить клиент Mobile VPN:

1. Откройте диалоговое окно Mobile VPN Monitor.

2. Нажмите **Disconnect**.

Управление соединением

Для каждого импортированного профиля, вы можете настроить действие, которое будет выполнять Mobile VPN клиент в случае если VPN туннель по какой-то причине становится недоступным. Вы можете настроить эти параметры на устройстве WatchGuard и сохранить их в .ini файл, и затем с помощью этого файла настроить программу клиента. .wgx не используется для изменения этих параметров.

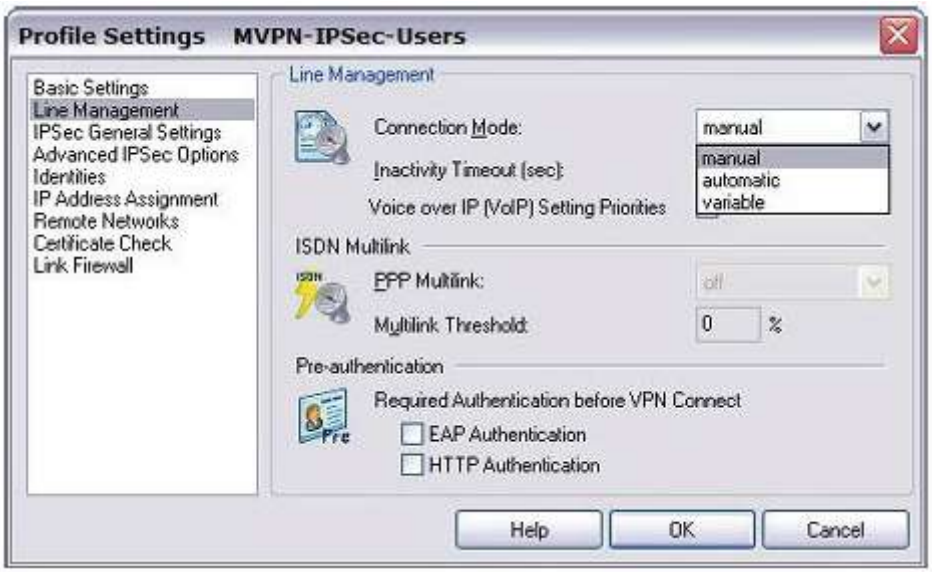
Если вы импортировали файл .ini для настройки программы клиента, не меняйте параметры Line Management. Файл .ini используется для настройки этих параметров.

Для того чтобы настроить поведение клиента Mobile VPN при выходе из строя VPN туннеля выполните следующее:

1. В WatchGuard Mobile VPN Connection Monitor выберите **Configuration > Profile Settings**.

2. Выберите имя профиля и нажмите **Configure**

3. В левой панели выберите **Line Management**



4. Из выпадающего списка **Connection Mode** выберите необходимый режим.

   Manual — если вы выберете режим **manual**, клиента не будет автоматически перезагружать туннель при его выходе из строя. Для того чтобы перезапустить туннель вам необходимо нажать кнопку **Connect** в Connection Monitor или нажать правой кнопкой на иконку Mobile VPN в панели инструментов Windows и нажать **Connect**.

   Automatic — Если вы выберете режим **automatic**, то клиент попытается начать соединение, когда ваш компьютер передает трафик в место назначение, доступ к которому вы можете получить через VPN. Также клиент пытается автоматически перезагрузить VPN туннель, если он вышел из строя.

   Variable — Если вы выберете режим **variable**, клиент пытается автоматически перезапустить VPN туннель до тех пока, пока вы не нажмете **Disconnect**. Клиент не будет пытаться перезагрузить VPN туннель после того, как в следующий раз вы нажмете **Connect**.

5. Нажмите **OK**.

Иконка программы клиента Mobile User VPN

Иконка Mobile User VPN появляется в панели задач Windows и показывает статус межсетевого экрана, **link firewall** и VPN сети. Для того чтобы отключить или подключить клиента, или посмотреть какой профиль используется на данный момент, нажмите на иконку правой кнопкой и выберите соответствующий пункт меню.

Настройка Mobile VPN для Windows Mobile

WatchGuard Mobile VPN для Windows Mobile используется на мобильных устройствах с установленной ОС Windows Mobile для создания защищенного подключения к сетям, подключенным к Firebox, который поддерживает Mobile VPN with IPSec. Mobile VPN для Windows Mobile состоит из двух компонентов:

- **WatchGuard Mobile VPN WM Configurator** запускается на компьютере, который может подключиться к мобильному устройству через Microsoft ActiveSync. Утилита Configurator выполняет необходимые настройки и загружает программу клиента Mobile VPN на мобильное устройство.

- Программа клиента WatchGuard Mobile VPN запускается на мобильном устройстве с установленной ОС Windows Mobile. Для создания VPN соединения на мобильном устройстве должен быть запущен сервис **WatchGuard Mobile VPN Service. WatchGuard Mobile VPN Monitor** позволяет вам выбрать загруженный профиль пользователя и подключиться к VPN сети.

- Mobile VPN для Windows Mobile использует такой же .wgx файл, который используется для настройки программ клиента Mobile VPN with IPSec. Для более подробной информации о профиле пользователя см. Configure the Firebox for Mobile VPN with IPSec.

Требования к Mobile VPN WM Configurator и клиенту Windows Mobile IPSec

Перед тем, как установить программу клиента, убедитесь, что вы понимаете требования и рекомендации для работы с Mobile VPN with IPsec. Если же нет, то см. соответствующие разделы, в которых приводится описание процедуры настройки Firebox для использования Mobile VPN.

Вам необходимо настроить Firebox для работы с Mobile VPN with IPSec. По окончании этой процедуры будет создан профиль пользователя, который будет использовать для настройки программы клиента Windows Mobile.

Системные требования Mobile VPN WM Configurator:

Операционная система	Версия Microsoft ActiveSync
Windows 2000	4.5 или выше
Windows XP (32-битная или 64-битная)	4.5 или выше
Windows Vista	6.1

Требования к программе клиента Windows Mobile IPSec:

- Windows Mobile 5.0
- Windows Mobile 6.0

Поддерживаются также устройства:

- Symbol MC70 (Windows Mobile 5 Premium Phone)
- T-Mobile Dash (Windows Mobile 6 Smartphone)
- Samsung Blackjack (Windows Mobile 5 Smartphone)

Для того чтобы установить Windows Mobile VPN WM Configurator и импортировать файл профиля на некоторые ОС, вам необходимы права Администратора. Права администратора не нужны для загрузки программы клиента и настройки мобильного устройства.

Устройства, приведенные в этом списке, были проверены с WatchGuard Mobile VPN для Windows Mobile. Для более подробной информации см. http://forum.watchguard.com/.

Установка Mobile VPN WM Configurator

Утилиту Mobile VPN WM Configurator необходимо установить на компьютер, который может подключиться к мобильному устройстве через ActiveSync. Перед тем, как приступить к установке утилиты, убедитесь, что у вас есть следующие компоненты:

- Файл установки WatchGuard Mobile VPN WM Configurator
- Файл профиля пользователя
- Ключ шифрования
- .p12 файл сертификата(если VPN подключается к Firebox X Core или Peak и для аутентификации использует сертификаты)
- Имя пользователя и пароль(если VPN подключается к Firebox X Core и Peak и использует Extended Authentication)

Для того чтобы установить Configurator выполните следующее:

1. Скопируйте .zip файл Mobile VPN WM Configurator .zip на компьютер и извлеките его содержимое.
2. Скопируйте файл профиля пользователя (.wgx файл) в корневой каталог на удаленный компьютер.
3. Два раза нажмите на .exe файл, извлеченный в п. 1. После этого запустится мастер WatchGuard Mobile VPN WM Installation Wizard.
4. Выполните все инструкции мастера. В диалоговом окне **InstallShield Wizard Complete** включите опцию **Start PDA Installation** если мобильное устройство подключено через ActiveSync.

Выбор сертификата и ввод PIN

Если для аутентификации вы используете сертификаты, вам необходимо выбрать корректный сертификат. У вас должен быть cacert.pem и .p12 файл.

1. Выберите **Configuration** > **Certificates**.
2. В закладке **User Certificate** в выпадающем списке **Certificate** выберите **from PKS#12 file**.

3. Рядом с полем **PKS#12 Filename** нажмите на кнопку и найдите файл .p12.

4. Нажмите **OK**.

5. Выберите Connection > Enter PIN.

6. Введите PIN и нажмите **OK**.
   PIN – это пароль, который используется для шифрования файла при работе с мастером Add Mobile User VPN Wizard.

Импорт профиля пользователя

Для того чтобы импортировать файл .wgx выполните следующее:

1. Выберите **Start** > **All Programs** > **WatchGuard Mobile VPN** > **WatchGuard Mobile VPN WM**.

2. Выберите **Configuration** > **Profile Import**.
   Запустится мастер Profile Import Wizard.

3. На странице **Select User Profile** выберите каталог, в котором находится файл .wgx. Нажмите **Next**.

4. На странице **Decrypt User Profile** введите пароль или ключ шифрования, полученный от администратора сети. Этот пароль или ключ зависит от регистра. Нажмите **Next**.

5. На странице **Overwrite or add Profile** вы можете выбрать, перезаписать ли текущий профиль с таким же именем. Нажмите **Next**.

6. В окне **Authentication** вы можете выбрать, вводить ли имя пользователя и пароль для аутентификации туннеля. Если вы оставите эти поля пустыми, при каждом подключении к VPN вам необходимо будет вводить имя пользователя и пароль. Если вы введете ваше имя пользователя и пароль здесь, Firebox сохранит эту информацию и вам не надо будет вводить ее при каждом подключении. Однако, это потенциальная угроза безопасности. Вы также можете ввести только имя пользователя, оставив поле пароля пустым. Это поможет снизить объем данных, необходимых для VPN соединения. Если вы оставите эти поля пустыми, то вам необходимо ввести имя пользователя и пароль при первом подключении к VPN. При следующем подключении, поля имени пользователя и пароля будут автоматически заполнены данными последнего сеанса связи.

7. Нажмите **Next**.

8. Нажмите **Finish**.

Если выбранный пароль – это пароль на Active Directory или LDAP серверах и вы выбрали его хранение на этих серверах, то при смене пароля на сервере аутентификации, этот пароль становится недействительным.

Установка программы клиента Windows Mobile на мобильное устройство

После того, как вы импортируете профиль пользователя в Configurator, подключите Configurator к мобильному устройству. Компьютер и мобильное устройство должны быть подключены друг к другу через ActiveSync.

После того, как программа клиента WatchGuard Mobile VPN будет установлена на ваше мобильное устройство вам необходимо его перезагрузить

1. Подключите мобильное устройство к вашему компьютеру через Microsoft ActiveSync

2. Для того чтобы запустить Configurator выберите **Start** > **All Programs** > **WatchGuard Mobile VPN** > **WatchGuard Mobile VPN WM**.

3. Если WatchGuard Mobile VPN WM не был установлен на устройство, то откроется окно **Confirmation**. Нажмите **Yes**

4. Откроется диалоговое окно информации. Нажмите **OK**.

5. WatchGuard Mobile VPN WM будет установлен на ваше мобильное устройство. Нажмите **OK**

6. Перезагрузите мобильное устройство.

Загрузка профиля пользователя на мобильное устройство

После того, как вы установили на мобильное устройство необходимое ПО, то вам необходимо на него загрузить профиль пользователя.

1. Подключите мобильное устройство к вашему компьютеру через Microsoft ActiveSync.
2. Выберите **Start** > **All Programs** >**WatchGuard Mobile VPN** >**WatchGuard Mobile VPN WM**
3. В выпадающем списке **Profile** выберите профиль, который вы загрузить на мобильное устройство

4. Нажмите **Upload**.

5. После того, как процедура загрузки будет завершена, в секции состояния Configurator будет показано **Upload completed successfully!**

Если VPN для аутентификации используется сертификат, то вам необходимо загрузить файл этого сертификата на мобильное устройство. Перед тем, как загрузить сертификат, вам необходимо настроить Configurator для работы с сертификатами.

Для того чтобы загрузить сертификат выполните следующее:

1. В утилите Configurator выберите **Configuration > Upload PKS#12 File**.

2. Выберите PKS#12 файл. Нажмите **Open**.

Подключение и отключение Mobile VPN для Windows Mobile клиента

Программа клиента WatchGuard Mobile VPN для Windows Mobile на основе данных на мобильном устройстве создает защищенное подключение к удаленным сетям, подключенным к Firebox. Мобильные устройства должны иметь доступ в сеть Интернет.

1. На вашем мобильном устройстве выберите **Start** > **Programs** > **WatchGuard Mobile VPN Monitor**. Если сервис WatchGuard Mobile VPN Service не запущен, то откроется диалоговое окно. Нажмите **Yes** для того чтобы запустить сервис

2. Откроется диалоговое окно WatchGuard Mobile VPN. В выпадающем списке в верхней части окна выберите профиль

3. Нажмите **Connect** и введите свое имя пользователя и пароль. Нажмите **OK**

*После первого успешного VPN соединения, программа клиента сохраняет имя пользователя и при следующем подключении спрашивает только пароль. Для того чтобы изменить имя пользователя нажмите **OK** при пустом поле с паролем. После этого откроется диалоговое окно, в котором вы сможете ввести новые имя пользователя и пароль.*

4. В диалоговом окне между телефоном и компьютером появится желтая линия с надписью **Connecting**. После того, как туннель будет создан, цвет линии меняется на зеленый

Для того чтобы отключить Mobile VPN клиент выполните следующее:

1. На вашем мобильном устройстве выберите **Start** > **Programs** > **WatchGuard Mobile VPN Monitor**

2. Нажмите **Disconnect**. Зеленая линия снова станет желтой. Если между телефоном и компьютером линия отсутствует, то VPN отключен.

Защита вашего мобильного устройства с помощью брандмауэра Mobile VPN

Программа клиента WatchGuard Mobile VPN для Windows Mobile состоит из двух компонентов брандмауэра:

Link firewall

link firewall не включен по умолчанию. Когда link firewall включен, ваш компьютер будет блокировать все пакеты, которые поступают с других компьютеров. Вы можете включать link firewall только если Mobile VPN туннель активен.

Desktop firewall

Этот межсетевой экран может управлять всеми подключениями вашего компьютера. Вы можете настроить дружественные сети и настроить правила доступа отдельно для дружественных и неизвестных сетей.

Остановка сервиса WatchGuard Mobile VPN Service

Для того чтобы создавать VPN туннели на мобильном устройстве должен быть запущен сервис WatchGuard Mobile VPN Service. Если вы закроете Monitor сервис не будет остановлен. Вам необходимо сделать это вручную.

1. На мобильном устройстве выберите **Start** > **Programs** > **WatchGuard Mobile VPN Service**

2. Откроется диалоговое окно WatchGuard Mobile VPN. Нажмите **Yes** для того чтобы остановить сервис.

Удаление Configurator, Service and Monitor

Для того чтобы удалить WatchGuard Mobile VPN for Windows Mobile, вам необходимо удалить все ПО с вашего компьютера и мобильного устройства.

Удаление Configurator с вашего компьютера

1. На вашем компьютере выберите **Start > Control Panel**.
2. Два раза нажмите **Add or Remove Programs**.
3. Выберите **WatchGuard Mobile VPN WM** и нажмите **Change/Remove**.
4. Нажмите **Yes** Для того чтобы удалить приложение.
5. Нажмите **OK** после того, как процедура удаления завершится.

Удаление WatchGuard Mobile VPN Service и Monitor с вашего мобильного устройства

1. На вашем мобильном устройстве выберите **Start > Settings**.
2. В секции Settings выберите закладку **System** и два раза нажмите **Remove Programs**.
3. Выберите **WatchGuard Mobile VPN** и нажмите **Remove**.

4. Откроется диалоговое окно **Remove Program**. Нажмите **Yes** для того чтобы удалить приложение.

Откроется диалоговое окно, которое спросит вам, надо ли перезагружать устройство. Нажмите **Yes** для того чтобы перезагрузить устройство. Нажмите **No** если вы хотите перезагрузить устройство позже. Программа будет полностью удалена с вашего мобильного устройства после его перезагрузки

Глава 29 - Mobile VPN with SSL

Mobile VPN with SSL

Технология Mobile VPN with SSL-программа клиента, которое устанавливается на удаленному компьютере. Клиент создает безопасное подключение от удаленного компьютера к вашей защищенной сети через небезопасную сеть, такую, как сеть Интернет. Mobile VPN-клиент использует SSL (Secure Sockets Layer) для обеспечения безопасности соединения.

Настройка Firebox для Mobile VPN with SSL

При включении Mobile VPN with SSL группа пользователей *SSLVPN-Users* и политика WatchGuard SSLVPN создаются для разрешения SSL VPN-подключений из сети Интернет до вашего External интерфейса.

Настройка параметров аутентификации и соединения

1. В Policy Manager выберите **VPN > Mobile VPN > SSL**.
   Откроется диалоговое окно Mobile VPN with SSL Configuration

2. Выберите опцию **Activate Mobile VPN with SSL**.

3. В выпадающем списке **Authentication Server** выберите сервер аутентификации. Вы можете аутентифицировать пользователей при помощи внутренней базе данных (Firebox-DB) устройства WatchGuard или с помощью серверов RADIUS, VACMAN Middleware, SecurID, LDAP или Active Directory. Убедитесь, что выбранный способ аутентификации включен (выберите **Setup > Authentication >мAuthentication Servers**)

4. Если вы выберете RADIUS или SecurID аутентификацию, вы можете включить опцию **Force users to authenticate after a connection is lost** для того, чтобы пользователи снова аутентифицировались после того, как Mobile VPN with SSL сессия была закрыта. Мы рекомендуем включить эту опцию, если вы используете двухфакторную аутентификацию, которая использует одноразовый пароль, как SecurID или Vasco.

   Если эту опцию вы не включите, то после того, как SSL сессия была закрыта, повторная попытка подключения может быть неудачной. Mobile VPN with SSL клиент после того, как соединение было разорвано, автоматически снова пытается установить соединение, используя введенный ранее одноразовый пароль, который уже недействителен

5. В выпадающем списке **Primary** выберите или введите публичный IP-адрес или доменное имя. Mobile VPN with SSL-клиенты подключаются к этому IP-адресу или доменному имени по умолчанию.

6. Если ваш Firebox имеет несколько WAN соединений, в выпадающем списке **Backup** выберите другой IP-адрес**.** Программа клиента Mobile VPN with SSL подключается к резервному IP-адресу в случае, когда не удается установить соединение с основным IP адресом

Настройка параметров Networking и IP Address Pool

В секции **Networking and IP address pool** вы можете настроить ресурсы сети, доступ к которым могут получать клиенты Mobile VPN with SSL

1. Из выпадающего списка в разделе **Networking and IP Address Pool** выберите метод, который Firebox использует для передачи трафика через VPN-туннель.

   * Выберите **Bridge VPN Traffic** для пробрасывания SSL VPN-трафика в указанную сеть. Данные настройки являются настройками по умолчанию для Firebox X Edge.

   * Выберите **Routed VPN Traffic** для маршрутизации VPN-трафика к указанной сети или ресурсам. Данные настройки являются настройками по умолчанию для устройств Firebox X Core, Peak и WatchGuard XTM.

2. Включите или отключите опцию **Force all client traffic through the tunnel**.

   Включите опцию если вы хотите передавать трафик из внутренней сети и сети Интернет через туннель. Эта опция отправляет весь внешний трафик через ваши политики Firebox и обеспечивает необходимый уровень безопасности мобильных пользователей. Однако при этом требуется больше ресурсов процессора, то приведет к невысокой скорости доступа в сеть Интернет для мобильных пользователей. Для более подробной информации о доступе мобильных пользователей в сеть Интернет при включенной опции **Force all client traffic through tunnel** см. “Опции для доступа в Интернет через Mobile VPN with SSL-туннель”

   * Отключите опцию **Force all client traffic through tunnel** для передачи через туннель только трафика внутренних сетей. Эта опция обеспечивает более высокую скорость передачи данных посредством маршрутизации через устройство Firebox только необходимого трафика. Но при этом ваши политики не управляют доступом пользователей в сеть Интернет. Для того чтобы ограничить доступ Mobile VPN with SSL клиентов только к определенным устройствам вашей внутренней сети, выберите переключатель **Specify allowed resources**. Введите IP-адрес ресурса в slash-нотации и нажмите **Add**.

3. Выберите IP-адрес, которые устройство Firebox будет присваивать Mobile VPN with SSL клиентам. Виртуальные IP-адреса в этом адресном пуле не могут быть частью сети, защищаемой устройством WatchGuard, любой сети, доступной через маршрут или BOVPN, адресами назначенными DCHP устройствам, подключенным к устройству WatchGuard, или адресами пулов для Mobile VPN with IPSec или Mobile VPN with SSL.

   Routed VPN traffic

   Для пула виртуальных адресов оставьте настройки по умолчанию - 192.168.113.0/24 или выберите другой диапазон. Введите IP-адрес подсети в slash-нотации. IP-адреса из этой подсети автоматически назначаются подключенным клиентам Mobile VPN with SSL. Вы не можете присвоить IP-адрес пользователю. Виртуальные IP-адреса в этом адресном пуле не могут быть частью сети, защищаемой устройством WatchGuard, любой сети, доступной через маршрут или BOVPN, адресами назначенными DCHP устройствам, подключенным к устройству WatchGuard, или адресами пулов для Mobile VPN with IPSec или Mobile VPN with PPTP..

   Bridge VPN traffic

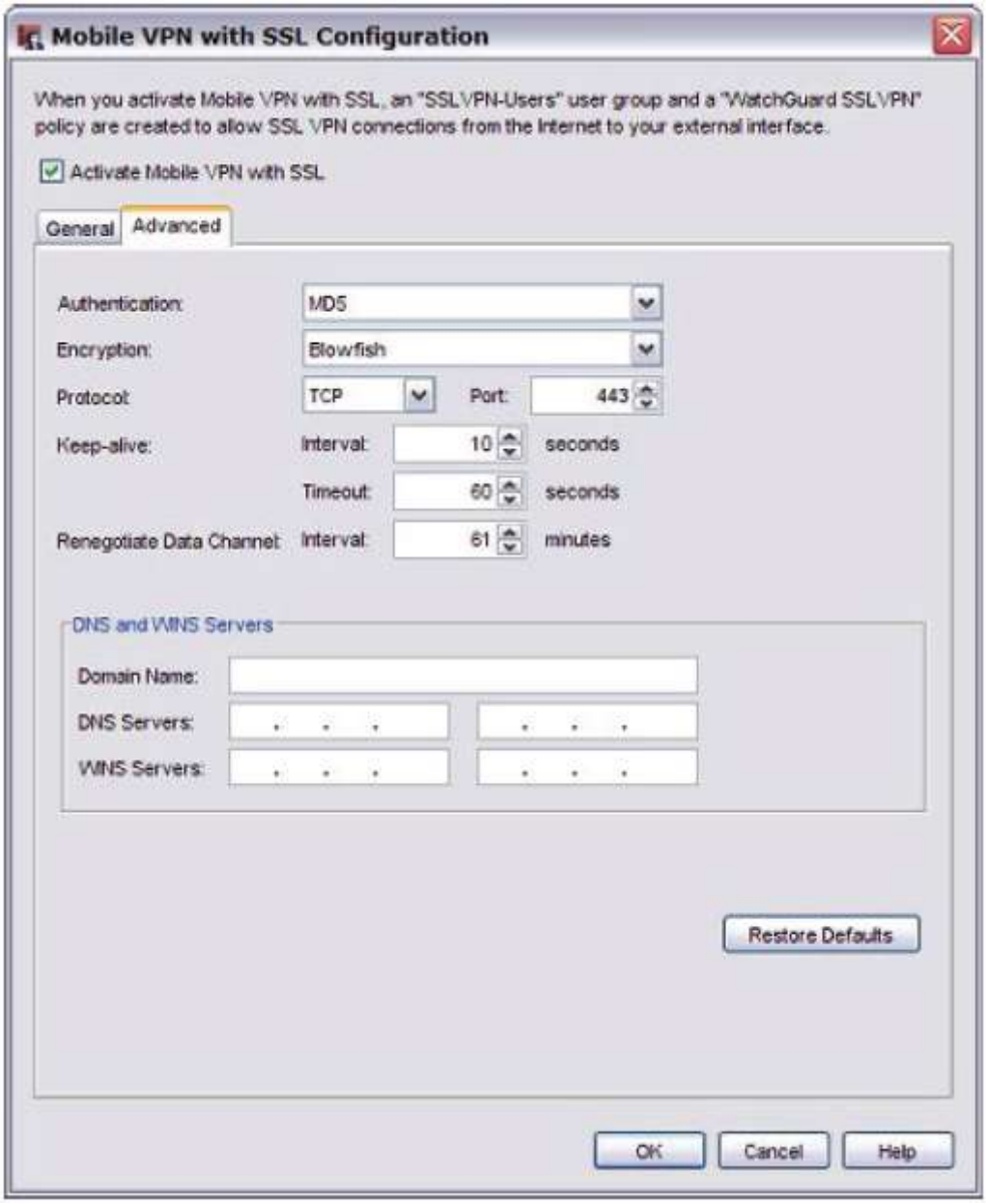
   В выпадающем списке **Bridge to interface** выберите имя интерфейса, куда будет пробрасываться трафик. В полях **Start** и **End** введите первый и последний IP-адрес диапазона, который присваивается подключенным клиентам Mobile VPN with SSL. Первый и последний IP-адреса должны находиться в одной подсети для интерфейса, в который они пробрасываются.

4. Нажмите **OK**.

После того, как вы сохраните изменения, вам необходимо будет, перед тем как пользователи смогут загрузить и установить программное обеспечение, настроить аутентификацию пользователя для Mobile VPN with SSL. Любые изменения, которые вы сделали, будут автоматически разосланы клиентам Mobile VPN with SSL при следующем их подключении

Настройка дополнительных параметров для Mobile VPN with SSL

1. В Policy Manager выберите **VPN > Mobile VPN > SSL**.
   Откроется диалоговое окно Mobile VPN with SSL Configuration



2. Нажмите на закладку **Advanced**. Поля закладки описаны далее.

   Authentication

   Метод аутентификации, используемый для установления соединения. Опции **MD5**, **SHA**, **SHA-1**, **SHA-256**, и **SHA-512**.

   Encryption

   Алгоритм, используемый для шифрования трафика. Опции Blowfish, DES, 3DES, AES (128 bit), AES (192 bit), или AES (256 bit). Алгоритмы отображены в порядке от самых слабых до сильных, за исключением Blowfish, который использует 128-битный ключ для «сильного» шифрования. Для лучшей эффективности с высоким уровнем шифрования мы рекомендуем выбрать MD5 аутентификацию с Blowfish-шифрованием.

   Protocol and Port

   Протокол по умолчанию и порт для Mobile VPN with SSL – TCP-порт 443. Это так же стандартный протокол и порт для HTTPS-трафика. Mobile VPN with SSL может поддерживать порт 443 с HTTPS.

Keep-alive

Частота передачи трафика устройством WatchGuard через туннель для того чтобы туннель при отсутствии трафика через него не закрывался.

Timeout

Промежуток времени, в течение которого устройство WatchGuard будет ожидать ответ от удаленного устройства. Если в течение промежутка времени, указанного в этом поле, ответа не будет, то туннель будет закрыт и удаленный пользователь должен будет создать туннель заново

Renegotiate Data Channel

Если соединение Mobile VPN with SSL активно в течение времени, указанного в текстовом поле **Renegotiate Data Channel**, клиент Mobile VPN with SSL должен создать новый туннель. Минимальное значение – 60 минут.

DNS and WINS Servers

DNS и WINS могут быть использованы для разрешения IP-адресов ресурсов, которые защищены устройством WatchGuard. Для того, чтобы клиенты Mobile VPN with SSL использовали DNS или WINS-серверы за устройством WatchGuard вместо серверов, назначенных удаленной сетью, к которой они подключены, введите доменное имя и IP-адреса DNS и WINS серверов вашей сети

Restore Defaults

Нажмите на закладку **Advanced** для сброса настроек в значения по умолчанию**.** Вся информацию о DNS и WINS-сервере в закладке **Advanced** будет удалена.

Настройка аутентификации пользователя для Mobile VPN with SSL

Для того чтобы аутентифицировать пользователя на устройстве WatchGuard и разрешить ему подключение через Mobile VPN with SSL туннель вам необходимо настроить аутентификацию пользователя на устройстве WatchGuard. Вы можете настроить ваше устройство WatchGuard в качестве сервера аутентификации или использовать сторонний сервер аутентификации. При включении Mobile VPN with SSL группа SSLVPN-Users создается автоматически.

Пользователи должны принадлежать непосредственно группе SSLVPN-Users. Если пользователи принадлежат группе, которая является частью SSLVPN-Users, они не смогут создавать Mobile VPN with SSL сессии

Настройка политик для управления доступом клиентов Mobile VPN with SSL

После того, как вы включите Mobile VPN with SSL, будет автоматически создана политика ***Allow SSLVPN-Users.*** Эта политика не ограничивает доступ клиентов Mobile VPN with SSL к ресурсам вашей сети. Для того чтобы ограничить доступ клиентов Mobile VPN with SSL вам необходимо создать несколько политик или добавить группу с Mobile VPN with SSL доступом в секцию **From** в настройках текущей политики.

Если вы пользователям Mobile VPN with SSL присваиваете адрес из Trusted-сети, их трафик не будет считаться доверенным. Весь трафик Mobile VPN with SSL является доверенным по умолчанию. Независимо от назначенного IP-адреса политики должны быть созданы для доступа пользователей Mobile VPN with SSL к ресурсам сети.

Разрешение доступа к Trusted сети пользователям Mobile VPN with SSL

В этом примере вы добавляете любую политику для разрешения полного доступа к ресурсам всех Trusted сетей пользователям группы SSLVPN-Users.

1. Нажмите на иконку плюс (+) на панели инструментов Policy Manager. Вы можете так же выбрать **Edit > Add Policies**.
   Откроется диалоговое окно Add Policies.

2. Нажмите на иконку плюс (+) слева от **Packet Filters**.
   Откроется список шаблонов для пакетного фильтра.

3. Выберите **Any** и нажмите **Add**.
   Откроется диалоговое окно New Policy Properties.

4. Введите имя для политики в текстовое поле **Name**. Выберите имя, которое будет помогать вам определять эту политику в вашей конфигурации.

5. В закладке **Policy** в поле **From** выберите **Any-Trusted** и нажмите **Remove**.

6. В разделе **From** нажмите **Add**.
   Откроется диалоговое окно Add Address. Откроется диалоговое окно Add Member.

7. Нажмите **Add User**. Для двух выпадающих списков **Type** выберите **SSL VPN** для первого и **Group** для второго.

8. Выберите **SSLVPN-Users** и нажмите **Select**.
   После надписи SSLVPN-Users появится название аутентификации в скобках.

9. Нажмите **OK** для закрытия диалогового окна **Add Address**.

10. В секции **From** выберите **Any-External** и нажмите **Remove**.

11. В разделе **To** нажмите **Add**.
    Откроется диалоговое окно Add Address.

12. В списке **Available Members** выберите **Any-Trusted** нажмите **Add**.

13. Нажмите **OK** дважды и нажмите **Close**.

14. Сохраните изменения в устройстве WatchGuard. Более подробную информацию о политиках см. в Add policies to your configuration.

Использование другой группы или пользователей в политике Mobile VPN with SSL

Пользователи должны быть членами группы SSLVPN-Users для создания Mobile VPN with SSL-соединения. Вы можете использовать политики с другими группам для ограничения доступа к ресурсам после того, как пользователь подключился. Для того чтобы выбрать пользователя, который не принадлежит группе SSLVPN-Users, выполните следующее:

1. В Policy Manager дважды нажмите на политику для добавления пользователя или группы.

2. В закладке Policy нажмите **Add** в разделе **From**.
   Откроется диалоговое окно Add Address.

3. Нажмите **Add User**.
   Откроется диалоговое окно Add Authorized Users or Groups.

4. Для двух выпадающих списков **Type** выберите **Firewall** для первого и одно их двух **(User** или **Group)** для второго**.**

5. Нажмите на имя пользователя или группы для добавления и нажмите **Select**.

6. Дважды нажмите **OK**.

Опции для доступа в Интернет через Mobile VPN with SSL-туннель

Разрешение прямого доступа в сеть Интернет

При активации Mobile VPN with SSL на вашем Firebox вы должны выбрать ресурсы, доступ к которым будет разрешен пользователям SSL VPN. Если вы выберете **Specify allowed resources** или **Allow access to networks connected through Trusted, Optional and VLANs,** то только трафик для этих ресурсов будет передаваться через VPN-туннель.

Весь остальной трафик будет передаваться прямо в сеть Интернет и сеть, к которой удаленно подключен пользователь. Эта опция может влиять на безопасность, так как любой трафик, передаваемый в сеть Интернет или удаленную сеть клиента, передается в незашифрованном виде и не обрабатывается политиками Firebox.

Принудительная передача трафика через туннель

Данная опция обеспечивает наибольшую безопасность для **Allowed Resources**. Для этого необходимо, чтобы весь удаленный трафик от пользователей сети Интернет маршрутизировался через VPN-туннель к Firebox. С устройства Firebox трафик передается обратно в сеть Интернет. С этой конфигурацией (так же известной как default-route VPN) Firebox проверяет весь трафик, тем самым обеспечивая высокий уровень безопасности.

Однако это потребует больше ресурсов процессора и пропускной способности устройства Firebox, что в случае довольно большого количества VPN пользователей может значительно снизить скорость работы вашей сети. По умолчанию политика, называемая *Allow SSLVPNUsers ,* предоставляет доступ ко всем внутренним ресурсам и сети Интернет

Использование HTTP-прокси для управления доступом в Интернет для пользователей Mobile VPN with SSL

По умолчанию *Allow SSLVPN-Users* политика не имеет ограничений на трафик, который разрешен от клиентов SSL к Internet.

Для ограничения доступа в Internet вы можете использовать HTTP-прокси, который вы уже настроили, или добавить новую политику HTTP-прокси для SSL-клиентов.

1. Дважды нажмите на политику для открытия диалогового окна **Edit Policy Properties**.
2. В закладке **Policy** нажмите **Add** в разделе **From**.
3. Нажмите **Add User**.
4. Для **Type** выберите **SSL VPN** и **Group**.
5. Выберите **SSLVPN-Users** и нажмите **Select**.
6. Нажмите **OK** для возвращение к диалоговому окну **Edit Policy Properties**.
7. Нажмите **OK**. Сохраните конфигурационный файл.

Политика HTTP-прокси имеет больший приоритет над политикой **Any**.

Вы можете оставить политику Any для обработки трафика, отличного от HTTP или можете использовать те же действия в другой политике для управления трафика, поступающего от SSL-клиента.

Разрешения имен для Mobile VPN with SSL

Цель Mobile VPN соединения заключается в разрешении пользователям подключаться к сетевым ресурсам в качестве локальных пользователей. В локальной сети NetBIOS позволяет вам подключаться к устройствам, используя имя устройства

Необязательно знать IP-адрес каждого сетевого устройства. Однако, Mobile VPN-туннель не может передавать broadcast трафик, а протоколу NetBIOS необходимо broadcast для корректной работы. Вы должны использовать другой метод.

Методы разрешения имен через Mobile VPN with SSL-соединения.

Вы должны выбрать один из двух методов для разрешения имен:

WINS/DNS (Windows Internet Name Service/Domain Name System)

WINS-сервер содержит базу данных имен NetBIOS для локальной сети. DNS работает аналогично. Если ваше доменное имя используется Active Directory, вы должны использовать DNS для разрешения имен.

Файл LMHOSTS

Файл LMHOSTS , созданный вручную файл, которые вы устанавливает на все компьютеры с установленной программой клиента Mobile VPN with SSL.Файл содержит список разрешенных имен и их IP-адреса.

Выбор наилучшего метода для вашей сети

Из-за ограничения администраторских требований и информации, которую он предоставляет, WINS/DNS сервер является более предпочтительным решением для разрешения имен через MVPN-туннель. WINS сервер постоянно сканирует сеть и обновляет свою информацию. Если ресурс изменил свой IP-адрес или был добавлен новый ресурс, то на клиенте SSL ничего не надо менять. При попытке клиента получить доступ к ресурсам по имени запрос отправляется к WINS/DNS-серверу и предоставляется самая последняя информация.

При отсутствии WINS-сервера файл LMHOSTS быстро предоставит информацию о разрешении имен клиентам Mobile VPN with SSL. Данный файл является статическим и при каждом изменении вам необходимо редактировать этот файл вручную. Пары разрешенных имен/IP-адресов в файле LMHOSTS используются не только для Mobile VPN with SSL-соединений, но и для всех сетевых соединений.

Настройка WINS или DNS для разрешения имен

Каждая сеть является уникальной в рамках имеющихся ресурсов и квалификации администраторов. Лучшим источником информации о настройке WINS-сервера для вашего сервера является документация, например официальная документация на сайте Microsoft. При настройке вашего WINS- или DNS-сервера необходимо учесть:

- WINS-сервер должен быть настроен как клиент
- Firebox должен быть шлюзом по умолчанию для WINS- и DNS-сервера.
- Необходимо убедиться, что сетевой ресурс не имеет более одного IP-адреса, присвоенного единственному сетевому интерфейсу.

NetBIOS способен только распознавать первый IP-адрес, присвоенный NIC. Более подробную информацию см .в http://support.microsoft.com/kb/q131641/.

Добавление WINS- и DNS-серверов к настройке Mobile VPN with SSL

1. В программе Policy Manager выберите **VPN > Mobile VPN > SSL**.
2. Выберите **Advanced**.
3. Введите основной и второстепенный адреса для WINS- и DNS-сервером. Вы должны также ввести суффикс домена в текстовое поле **Domain Name** для клиента, использующего неполные доменные имена.

4. Нажмите **OK**. Сохраните конфигурационный файл.

5. Новые настройки будут использованы для подключения тогда, когда компьютер SSL-клиента аутентифицируется на Firebox.

Настройка LMHOSTS-файла для использования разрешенных имен

При использовании LMHOSTS-файла для разрешения имен на вашем MUVPN-клиенте нет необходимости изменять программное обеспечение Firebox или MUVPN. Основные инструкции о создании LMHOSTS-файла см. в http://support.microsoft.com/kb/q150800/.

Редактирование LMHOSTS-файла

1. Найдите LMHOSTS-файл на компьютере MUVPN-клиента. LMHOSTS-файл (иногда называется lmhosts.sam) обычно находится в каталоге: *C:\WINDOWS\system32\drivers\etc*

2. Если вы найдете LMHOSTS-файл в этом каталоге, откройте его в текстовом редакторе, например Notepad. Если вы не можете найти LMHOSTS-файл, создайте новый в текстовом редакторе.

3. Для создания записи в LMHOSTS-файле введите IP-адрес сетевого ресурса, пять пробелов и затем имя ресурса. Имя ресурса должно содержать не более 15 символов.

   Например, 192.168.42.252 server_name

4. Если вы начали работать с более старым LMHOSTS-файлом, сохраните его с первоначальным именем. Если вы создали новый файл в Notepad, сохраните его с именем lmhost в репозитории *C:\WINDOWS\system32\drivers\etc*. Вы должны так же выбрать тип "All Files" в диалоговом окне **Save** или добавьте к имени файла расширение .txt при работе с Notepad.

5. Перезагрузите компьютер SSL-клиента для того, чтобы активизировать LMHOSTS-файл.

Установка и подключение Mobile VPN with SSL-клиента

Программное обеспечение Mobile VPN with SSL позволяет пользователям подключаться, отключаться, получать информацию о соединении и осуществлять выход клиента.

Mobile VPN with SSL-клиент добавляет иконку на панели задач операционной системы Windows или иконку в панели меню Mac OS X. Вы можете использовать эту иконку для управления программным обеспечением клиента.

Для использования Mobile VPN with SSL необходимо:

1. Проверить соответствие системным требованиям

2. Загрузить программное обеспечение клиента.

3. Установить программное обеспечение клиента.

4. Подключиться к вашей внутренней сети.

Если пользователь не устанавливает соединение с устройством WatchGuard по номеру 4100 TCP-порта или не может загрузить инсталлятор от устройства WatchGuard, необходимо вручную установить программное обеспечение Mobile VPN with SSL-клиент и настроить файл.

Требования к компьютеру клиента

Вы можете установить программное обеспечение Mobile VPN with SSL-клиент на компьютеры со следующей операционной системой:

- Microsoft Windows Vista (32 bit)
- Microsoft Windows XP (32 bit)
- Microsoft Windows 2000 Pro
- Mac OS X 10.3 (Panther), 10.4 (Jaguar), or 10.5 (Leopard)

Если на компьютере клиента установлена ОС Windows Vista или Windows XP, вы должны войти под учетной записью администратора для установки программного обеспечения Mobile VPN with SSL-клиент. Административные права не требуются для подключения после того, как SSL-клиент был установлен и настроен. В операционной системе Windows XP Professional пользователь должен быть членом группы Network Configurations Operators для запуска SSL-клиента.

Если на компьютере установлена ОС Mac X, административные права не требуются для установки и использования SSL-клиента. Если на компьютере установлено программное обеспечение брандмауэра, то он должен быть настроен на разрешения исходящих соединений с номером 4100 TCP-порта.

Загрузка программного обеспечения клиента

1. Подключитесь к IP-адресам, введя в веб-браузере:

   https://<IP_адрес_интерфейса_устройства_WatchGuard>:4100/sslvpn.htm

   или

   https://<Имя_хоста_устройства_WatchGuard>:4100/sslvpn.html

2. Введите имя пользователя и пароль для аутентификации на устройстве WatchGuard. *Откроется страница загрузки SSL VPN-клиента*

3. Нажмите кнопку **Download** для инсталлятора, который вы планируете использовать. Существует две доступные версии: Windows (WG-MVPN-SSL.exe) и Mac OS X (WG-MVPN-SSL.dmg).

4. Сохраните файл на вашем рабочем столе или в другом месте по вашему усмотрению.

Установка программного обеспечения клиента

Для операционной системы Microsoft Windows:

1. Дважды нажмите на **WG-MVPN-SSL.exe**.
   Запустится мастер настройки клиента Mobile VPN with SSL.

2. Примите настройки по умолчанию, предложенные на экране мастера настроек.

3. Если вы хотите добавить иконку на рабочий стол или иконку для быстрого запуска (Quick Launch), выберите опцию в мастере настроек, соответствующую данному параметру. Установка иконки на рабочем столе или в меню быстрого запуска является необязательной.

4. Завершите работу мастера настроек.

Для операционной системы Mac OS X:

1. Дважды нажмите на **WG-MVPN-SSL.dmg**.
   Том с именем WatchGuard Mobile VPN будет создан на вашем рабочем столе.

2. В томе WatchGuard Mobile VPN дважды нажмите на **WatchGuard Mobile VPN with SSL Installer V15.mpkg**.
   Начнется выполнение инсталлятора клиента.

3. Примите настройки по умолчанию на каждом экране инсталлятора.

4. Завершите работу инсталлятора.

После загрузки и установки программного обеспечения клиента программа Mobile VPN client автоматически подключиться к устройству WatchGuard. Каждый раз при подключении к устройству WatchGuard программное обеспечение клиента проверяет обновления для конфигурации.

Подключение к вашей внутренней сети

Для подключения к частной сети в операционной системе Microsoft Windows необходимо:

1. Использовать один из трех способов запуска программного обеспечения клиента:

   * Выберите **Start** > **All Programs** > **WatchGuard** > **Mobile VPN with SSL client** > **Mobile VPN with SSL client**.

   * Дважды нажмите на иконку **Mobile VPN with SSL** на вашем рабочем столе.

   * Нажмите на иконку **Mobile VPN with SSL** на панели инструментов быстрого запуска.

2. Ввести информацию для устройства WatchGuard, к которому необходимо подключиться, а так же имя и пароль для пользователя. Server- IP-адрес основного внешнего интерфейса устройства WatchGuard. Если вы настраиваете Mobile VPN with SSL для использования порта, номер которого отличен от значения по умолчанию 443, в поле Server введите IP-адрес основного внешнего интерфейса, затем двоеточие и номером порта. Например, если Mobile VPN with SSL настраивается для использования порта 444 и основной внешний IP-адрес - 50.50.50.1, то запись Server будет выглядеть следующим образом: 50.50.50.1:444.

3. Нажмите **Connect**.

Для подключения к внутренней сети в операционной системе Mac OS X необходимо:

1. Открыть окно Finder. Затем **Applications > WatchGuard** и дважды нажать на приложение **WatchGuard Mobile VPN with SSL**.
   Откроется иконка WatchGuard Mobile VPN with SSL в меню.

2. Нажать на иконку в меню и выбрать **Connect**.

3. Ввести информацию для устройства WatchGuard, к которому необходимо подключиться, а так же имя и пароль для управления сервером пользователя. Server- IP-адрес основного внешнего интерфейса устройства WatchGuard. Если вы настраиваете Mobile VPN with SSL для использования порта, отличного от номера порта 443, заданному по умолчанию, в поле Server введите IP-адрес основного внешнего интерфейса, затем двоеточие и номером порта. Например, если Mobile VPN with SSL настраивается для использования порта 444 и основной внешний IP-адрес - 50.50.50.1, то запись Server будет выглядеть следующим образом: 50.50.50.1:444.

4. Нажать **Connect**. SSL-клиент должен ввести свои данные для входа в систему. Mobile VPN with SSL не поддерживает Single Sign-On (SSO)-сервисы. Если соединение между SSL-клиентом и устройством WatchGuard временно потеряно, SSL-клиент пытается установить связь снова.

Элементы управления Mobile VPN with SSL-клиента

При запуске Mobile VPN with SSL-клиента иконка Mobile VPN with SSL появится в системной панели задач (в операционной системе Windows) или в меню (Mac OS X).

Статус VPN-соединения отображается в виде иконки с увеличительным стеклом. Возможные варианты статуса:

-  - VPN-соединение не установлено.
-  - VPN-соединение установлено. Вы можете безопасно подключаться к ресурсам за устройством WatchGuard.
-  - Клиенты находятся в процессе подключения или отключения.

Для того, чтобы просмотреть список клиентов управления нажмите правой кнопкой мыши на иконку Mobile VPN with SSL на панели задач (для ОС Windows) или в меню (для Mac OS X).

Вы можете выбрать следующие действия:

Connect/Disconnect

Запуск/остановка SSL VPN-соединения.

View Logs

Открытие журнального файла соединения.

Properties

Для ОС Windows: выберите **Launch program on startup** для запуска клиента при загрузке Windows. Введите номер уровня **Log level** для изменения уровня детализации, включенной в журналах. Для ОС Mac X: Отображение детализированной информации о SSL VPN-соединении. Вы так же можете устанавливать уровень детализации.

About

Диалоговое окно Mobile VPN открывается для отображения информации о программном обеспечении клиента.

Exit (Windows) или Quit (Mac OS X)

Отключение от устройства WatchGuard и выключение клиента.

Рассылка и установка программного обеспечения Mobile VPN with SSL-клиента и конфигурационного файла вручную

Если вы не можете использовать TCP-порт 4100 для соединения с Firebox из-за блокировки брандмауэром или ISP-ограничений, вы можете вручную разослать пользователям программу клиента и конфигурационный файл.

Вы можете загрузить программное обеспечение SSL-клиента в разделе **Software Downloads** на веб-сайте LiveSecurity. Важно понимать, что клиенты, которые не могут подключиться по TCP-порту 4100, могут организовать VPN-соединение, но при этом автоматическое изменение конфигурации происходить не будет.

При подключении пользователя появится диалоговое окно с предложением загрузки самой последней конфигурации из сервера, при положительном ответе (Yes) устанавливается VNP-соединение без изменений настроек Mobile VPN with SSL. Если изменения проведены, вы должны установить новый конфигурационный файл для пользователей, которые не могут подключиться по TCP-порту 4100.

Загрузка конфигурационного файла с устройства Firebox

Необходимо настроить Firebox для использования Mobile VPN with SSL до проведения этой процедуры, для этого:

1. Запустите Start Firebox System Manager.
2. Выберите закладку **Status Report** и нажмите **Support**.
3. Выберите место для сохранения *support.tgz* файла и нажмите Retrieve.
4. Извлеките содержимое support.tgz в директорию на вашем компьютере.

Конфигурационный файл Mobile VPN with SSL располагается в *var\sslvpn\client.wgssl*.

Доступ по FTP на устройство Firebox осуществляется через командную строку Windows

Установка и настройка SSL-клиента с использованием установочного программного обеспечения и конфигурационного файла

Для проведения установки и настройки SSL-клиента необходимо наличие двух файлов:

- Установочное программное обеспечение Mobile VPN with SSL VPN-клиент WG-MVPN-SSL.exe (для ОС Microsoft Windows) или WG-MVPN-SSL.dmg (для ОС Mac X)
- Конфигурационный файл Mobile VPN with SSL VPN - sslvpn_client.wgssl

Для ОС Microsoft Windows:

1. Дважды нажмите на **WG-MVPN-SSL.exe**.
   Запустится мастер установки Mobile VPN with SSL-клиента.
2. Примите настройки по умолчанию, предложенные на экранах мастера установки.

3. Для добавления иконки на рабочий стол или иконки на панели быстрого запуска выберите опцию для этой операции.
   Появление иконки на рабочем столе или на панели быстрого запуска – необязательно. Иконка клиента добавляется в меню Windows Start по умолчанию.

4. Завершите работу мастера настроек.

5. Используйте один из трех методов для запуска программного обеспечения клиента:

   Выберите **Start** > **All Programs** > **WatchGuard** > **Mobile VPN with SSL client** > **Mobile VPN with SSL client**. Запустится инсталлятор клиента.

   * Дважды нажмите на иконку Mobile VPN with SSL-клиент на рабочем столе.

   * Нажмите на иконку Mobile VPN with SSL-клиент в панели инструментов быстрого запуска.

6. Дважды нажмите на **sslvpn-client.wgssl** для настройки программного обеспечения Mobile VPN with SSL-клиент.

Для ОС Mac X:

1. Двойным щелчком нажмите на **WG-MVPN-SSL.dmg**.
   Том с именем WatchGuard Mobile VPN будет создан на рабочем столе.

2. В томе WatchGuard Mobile VPN дважды нажмите на **WatchGuard Mobile VPN with SSL Installer V15.mpkg**.
   Начнется выполнениеThe client installer starts.

3. Примите настройки по умолчанию, предложенные на экранах мастера установки.

4. Завершите работу мастера настроек.

5. Начнется выполнение программного обеспечения. Откройте окно Finder и перейдите к **Applications > WatchGuard**.

6. Дважды нажмите на приложение **WatchGuard Mobile VPN with SSL**.
   Откроется логотип Mobile VPN with SSL в меню.

7. Двойным щелчком нажмите на **sslvpn-client.wgssl** для настройки программного обеспечения Mobile VPN with SSL-клиента.

Обновление конфигурации компьютера, который не может подключиться к устройству WatchGuard

Вы должны установить файл обновления sslvpn-client.wgssl

1. Дважды щелкните на **sslvpn-client.wgssl**.
   Запустится SSL-клиент.

2. Введите имя пользователя и пароль управления сервером. Нажмите **Connect**.SSL VPN будет использоваться с новыми настройками.

Удаление Mobile VPN with SSL-клиента

Вы можете использовать приложение деинсталлятор для удаления Mobile VPN with SSL-клиента из компьютера.

Windows Vista и Windows XP

1. Выберите **Start > All Programs > WatchGuard > Mobile VPN with SSL client > Uninstall Mobile VPN with SSL client.**
   Запустится программа-деинсталлятор Mobile VPN with SSL-клиента.

2. Нажмите **Yes** для удаления Mobile VPN with SSL-клиента и всех его компонентов.

3. При завершении программы нажмите **OK**.

Mac OS X

1. В окне Finder перейдите к полю **Applications > WatchGuard**.

2. Двойным щелчком нажмите на приложение **Uninstall WG SSL VPN** для выполнения программы-деинсталлятора.
   Запустится программа-деинсталлятор Mobile VPN with SSL-клиент.

3. Нажмите **OK** в диалоговом окне **Warning**.

4. Нажмите **OK** в диалоговом окне **Done**.

5. В окне Finder перейдите в поле **Applications**.

Переместите папку **WatchGuard** в корзину.

Глава 30 - WebBlocker

WebBlocker

Если вы предоставите вашим пользователям неограниченный доступ в Интернет, то вы рискуете получить значительное снижение пропускной способности вашей сети и ее производительности. Неуправляемое посещение Интернет сайтов может представлять серьезную угрозу для вашей системы безопасности. Сервис WebBlocker предоставляет вам возможность управлять доступом ваших пользователей к различным Интернет сайтам.

WebBlocker использует базу данных с адресами Интернет сайтов, доступ к которым управляется SurfControl, компанией-лидеров в области web фильтрации.

Когда пользователь пытается подключиться к определенному сайту WatchGuard устройство проверяет базу данных WebBlocker. Если запрашиваемого сайта в базе данных нет или он не заблокирован, пользователь без проблем открывает запрашиваемые страницы этого сайта. Если же запрашиваемый найден в базе данных и он заблокирован, пользователь видит уведомление и доступ к сайту блокируется. Для фильтрации web содержимого WebBlocker использует HTTP и HTTPS.

Если вы еще не настроили HTTP или HTTPS прокси, то их автоматическая настройка происходит после включения WebBlocker.

Для фильтрации web содержимого устройство WatchGuard использует базу данных WebBlocker, расположенную на сервере WebBlocker. Если вы хотите использовать WebBlocker на не-Edge устройстве WatchGuard, вам сначала необходимо настроить локальный сервер WebBlocker на вашей станции управления. WebBlocker на устройстве Edge по умолчанию использует сервер WebBlocker, который установлен на устройстве WatchGuard.

Сервер WebBlocker устанавливается, как часть процедуры установки WatchGuard System Manager.

Для настройки WebBlocker на устройстве WatchGuard вам нужен лицензионный ключ WebBlocker, зарегистрированный на сайте LiveSecurity. После регистрации этого лицензионного ключа, LiveSecurity выдаст вам новый ключ.

Настройка сервера WebBlocker Server

Установка сервера WebBlocker

Проверьте, что сервер WebBlocker установлен на вашей станции управления. Вы выбираете установку сервера в окне выбора компонентов для установки при установке WatchGuard System Manager Installer. Если сервер у вас не установлен, то см. “Установка WatchGuard System Manager”. В окне выбора компонентов для установки выберите только сервер WebBlocker.

Управление сервером WebBlocker

Управление сервером WebBlocker осуществляется в WatchGuard Server Center. Для того чтобы посмотреть общие настройки сервера WebBlocker выполните следующее:

1. Нажмите правой кнопкой  в панели задач и выберите **Open WatchGuard Server Center**. *Откроется диалоговое окно Connect to WatchGuard Server Center.*

2. В полях **Username** и **Administrator passphrase** введите имя пользователя и пароль администратора соответственно.

3. Нажмите **Login**.
   Откроется WatchGuard Server Center.

4. В секции **Servers** выберите **WebBlocker Server**.
   Откроется страница WebBlocker General Settings.

На этой странице вам будут доступны кнопки в зависимости от того, загрузили ли вы полную базу данных WebBlocker

- Если базу данных вы не загрузили, появится кнопка **Download**

- После того, как вы загрузите базу данных WebBlocker, появится кнопка **Update**

Вы можете использовать следующие кнопки для управления сервером.

- Нажмите на кнопку **Download** для того чтобы загрузить полную базу данных WebBlocker.
- Нажмите на кнопку **Update** для обновления базы данных WebBlocker.
- Нажмите на кнопку **Status** для того чтобы посмотреть дату и время последнего обновления базы данных WebBlocker, а также другую полезную информацию.
- Нажмите на кнопку Change Port для того чтобы изменить порт, который слушает сервер WebBlocker. Мы не рекомендуем менять номер порта

Загрузка базы данных WebBlocker

После первой установки сервера WebBlocker вам необходимо загрузить полную базу данных WebBlocker.

База Данных WebBlocker содержит более 240 MB данных. Скорость загрузки определяется скоростью подключения и сама загрузка может занять более 30 минут. Убедитесь, что на вашем жестком диске имеется минимум 250MB свободного места.

Для этого выполните следующее:

1. Нажмите правой кнопкой на  в панели задач и выберите **Open WatchGuard Server Center**.
   Откроется диалоговое окно Connect to WatchGuard Server Center.

2. В полях **Username** и **Administrator passphrase** введите имя пользователя и пароль администратора соответственно.

3. Нажмите **Login**.
   Откроется WatchGuard Server Center.

4. В секции **Servers** выберите **WebBlocker Server**.
   Откроется страница WebBlocker General Settings

5. Для того чтобы загрузить полную базу данных WebBlocker нажмите **Download**.
   Откроется диалоговое окно Download WebBlocker Database

6. Для того выбрать, в который будет загружена база данных нажмите **Browse** и выберите необходимый каталог.

   По умолчанию база данных загружается в каталог C:\Documents and Settings\WatchGuard\wbserver\db.

   Вы не можете загрузить базу данных в корневой каталог, например c:\.

7. Для того чтобы загрузить новую базу данных нажмите **Download**.
   В отдельном диалоговом окне появится строка состояния загрузки.

8. Нажмите два раза **OK**.

9. Для того чтобы запустить WebBlocker сервер, нажмите правой кнопкой **WebBlocker Server** в WatchGuard Server Center и выберите **Start Server**

База данных WebBlocker не обновляется автоматически. Для того чтобы постоянно обновлять вашу базу данных WebBlocker, мы рекомендуем использовать Планировщик Задач (Windows Task Scheduler).

Обновление базы данных WebBlocker

База данных WebBlocker не обновляется автоматически. Обновлять базу данных WebBlocker вы можете в любое время. Для того чтобы загрузить полную базу данных см. процедуру загрузки в разделе “Загрузка базы данных WebBlocker”

Для того чтобы постоянно обновлять вашу базу данных WebBlocker, мы рекомендуем использовать Планировщик Задач (Windows Task Scheduler).

Загрузка частичного обновления

1. Нажмите правой кнопкой в панели задач и выберите **Open WatchGuard Server Center**.
   Откроется диалоговое окно Connect to WatchGuard Server Center.

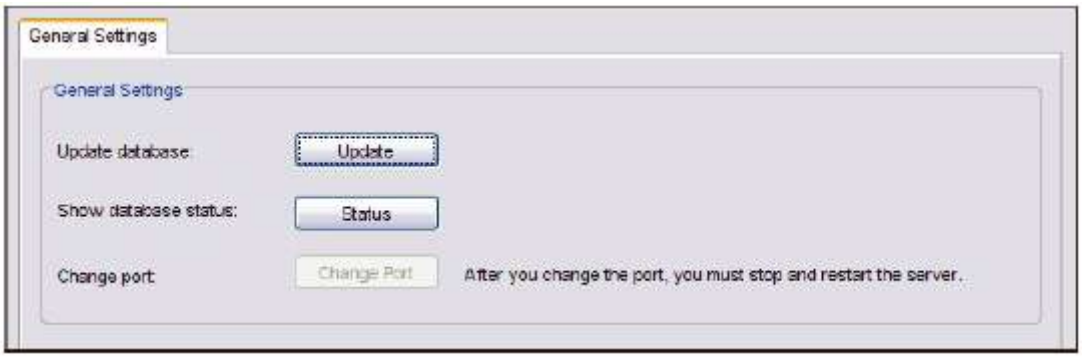
2. В полях **Username** и **Administrator passphrase** введите имя пользователя и пароль администратора соответственно.

3. Нажмите **Login**.
   Откроется WatchGuard Server Center.

4. В секции **Servers** нажмите правой кнопкой на **WebBlocker Server** и выберите **Stop Server**.
   Появится сообщение подтверждения.

5. Нажмите **Yes**.

6. В закладке **General Settings** нажмите **Update**



7. Для того чтобы запустить сервер, нажмите правой кнопкой на **WebBlocker Server** и выберите **Start Service**.

Автоматическая загрузка базы данных WebBlocker

Для того чтобы ваши базы постоянно обновлялись используйте Планировщик Заданий Windows (Windows Task Scheduler). Вы можете использовать планировщик для чтобы составить расписание для процесса “updatedb.bat”, который создается автоматически в каталоге WSM8/bin.

1. Откройте **Scheduled Tasks**. Для того чтобы открыть планировщик в Windows XP, нажмите **Start**, нажмите **All Programs**, выберите **Accessories**, выберите **System Tools**, и нажмите **Scheduled Tasks**.

2. Нажмите **Add Scheduled Task**.

3. Запустится мастер Scheduled Tasks. Нажмите **Next**.

4. Экран покажет список программ. Нажмите **Browse**.

5. В каталоге C:\Program Files\WatchGuard\wsm8\bin выберите **updatedb.bat**.

6. Выберите временной интервал для задания. Мы рекомендуем обновлять ваши базы данных каждый день. Если у вас низкая скорость работы сети Интернет, то обновлять базы вы можете реже. Нажмите **Next**.

7. Введите время и частоту для запуска процедуры. Так как для обновления вам необходимо останавливать сервер WebBlocker, то мы рекомендуем вам производить обновления в нерабочее время.

8. Выберите начальную дату. Нажмите **Next**.

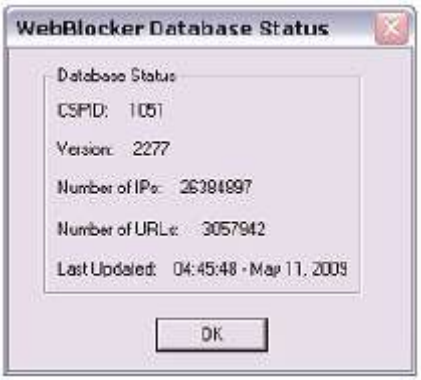
9. Для использования процедуры введите имя пользователя и пароль. Убедитесь, что этот пользователь имеет доступ к необходимым файлам. Нажмите **Next**.

10. Нажмите **Finish**.

Состояние базы данных

1. В секции **Servers** выберите **WebBlocker Server**.
   Откроется страница WebBlocker Server General Settings.

2. Нажмите **Status**.
   Откроется диалоговое окно WebBlocker Database Status.



3. Посмотрите состояние вашей базы данных.

4. Нажмите **OK**.

Изменение порта сервера WebBlocker

WatchGuard устройство отправляет запросы на ваш сервер WebBlocker через UDP порт 5003. По умолчанию Firebox использует TCP порт 5003 для проверки соединения с вашим сервером WebBlocker. Ваш сервер WebBlocker слушает входящие данные от WatchGuard устройства на этих портах. Мы не рекомендуем менять значения этих портов. Единственной причиной, по которой вы можете изменить значения порта по умолчанию, это если на вашем компьютере, на котором установлен сервер WebBlocker, имеется программа, которая также использует TCP или UDP порт 5003 (например, Filemaker Pro).

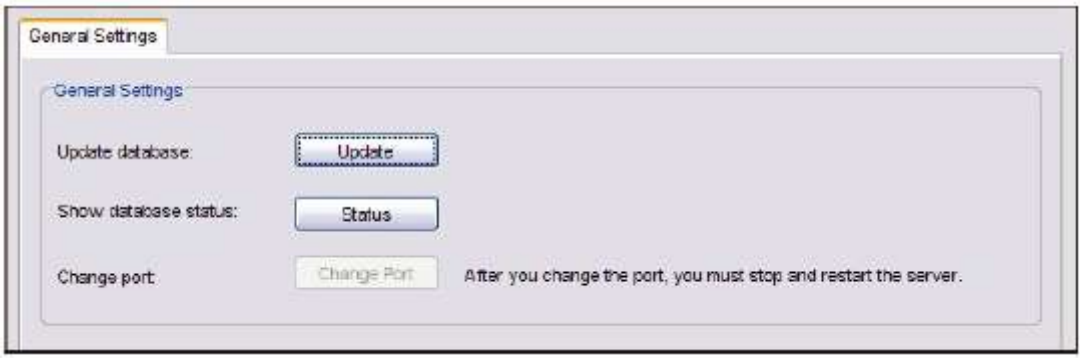
Изменения порта, который слушает сервер WebBlocker Server

1. Нажмите правой кнопкой на  в панели задач и выберите **Open WatchGuard Server Center**.
   Откроется диалоговое окно Connect to WatchGuard Server Center.

2. В полях **Username** и **Administrator passphrase** введите имя пользователя и пароль администратора соответственно.

3. Нажмите **Login**.
   Откроется WatchGuard Server Center.

4. В секции **Servers** выберите **WebBlocker Server**.
   Откроется страница WebBlocker General Settings



5. Нажмите **Change Port**.
   Откроется диалоговое окно WebBlocker Configuration

6. В текстовом поле **Server Listen Port** введите или выберите новый порт. Нажмите **OK**.
   Значение порта будет изменено. Изменения вступят в силу только после того, как вы перезапустите сервер WebBlocker.

7. Для того чтобы остановить сервер в секции **Servers** нажмите правой кнопкой **WebBlocker Server** и выберите **Stop Server**.

8. Для того чтобы перезапустить сервер в секции **Servers** нажмите правой кнопкой **WebBlocker Server** и выберите **Start Server**.

Изменение порта сервера WebBlocker, который используется Firebox

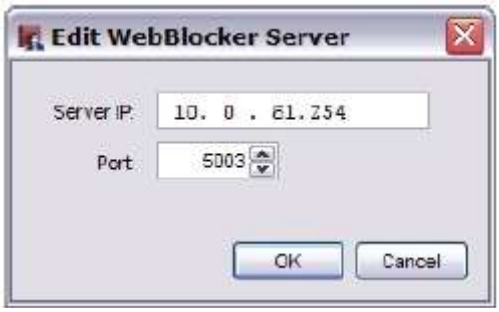
После того, как вы изменили номер порта для сервера WebBlocker, вам необходимо внести изменения на каждом устройстве Firebox, использующем WebBlocker.

1. Откройте Policy Manager.

2. Выберите **Setup** > **Actions** > **WebBlocker**.
   Откроется диалоговое окно WebBlocker Configurations.

3. Выберите конфигурацию WebBlocker. Нажмите **Edit**.
   Откроется диалоговое окно Edit WebBlocker Configuration.

4. Выберите сервер WebBlocker. Нажмите **Edit**.
   Откроется диалоговое окно Edit WebBlocker Server



5. В поле **Port** введите или выберите номер порта, который вы указали в настройках сервера WebBlocker.

6. Нажмите **OK** для того чтобы закрыть все диалоговые окна.

7. Сохраните конфигурационный файл.

Копирование базы данных WebBlocker с одного сервера WebBlocker на другой

После того как вы установили сервер WebBlocker, вам необходимо загрузить полную базу данных WebBlocker. Если у вас уже есть сервер WebBlocker, то вы можете скопировать базу данных с него на новый сервер. База данных WebBlocker занимает около 250 Мб. В зависимости от скорости передачи по сети Интернет, возможно будет быстрее загрузить базу с локального сервера.

Перед тем как начать

Перед тем, как копировать базу данных WebBlocker, вам необходимо установить сервер WebBlocker на второй сервер. Вы выбираете установку сервера в окне выбора компонентов для установки при установке WatchGuard System Manager Installer. Если сервер у вас не установлен, то см. ““Установка WatchGuard System Manager””. В окне выбора компонентов для установки выберите только сервер WebBlocker. В этих инструкциях используется каталог по умолчанию для установки WatchGuard System Manager 11.0. Номер версии также входит в название каталога, куда будет установлена программа. Если вы используете другую версию, то вам необходимо изменить имя каталога в соответствии с вашей версией ПО.

На обоих серверах вам необходимо установить сервер WebBlocker в один и тот же каталог.

Копирование базы данных WebBlocker и конфигурационных файлов

1. Скопируйте содержимое каталога *\documents and settings\watchguard\wbserver\db* с одного сервера в тот же каталог на другом сервере.

2. Скопируйте файл *\documents and settings\watchguard\wbserver\conf\CSPConfig.ini* с одного сервера в тот же каталог на другом сервере.

3. На новом сервере откройте *\documents and settings\watchguard\wbserver\wbserver.ini* в текстовом редакторе (например, Блокнот).

4. В конец файла добавьте следующие две строки:

   SurfConfigFile = "\C:\\Documents and Settings\\WatchGuard\\wbserver\\conf\\CSPConfig.ini"

   Если вы не выполните эту процедуру, сервер WebBlocker не сможет открыть конфигурационный файл и запуститься

5. На новом сервере скопируйте файл *\program files\watchguard\wsm11.0\wbserver\conf\license.ini* в каталог *\documents and settings\watchguard\wbserver\conf* на сервере.

Запуск утилиты для установки сервиса WebBlocker

Обычно эта процедура выполняется автоматически после загрузки базы данных. Если вы скопировали локальную базу данных, то вам необходимо вручную запустить эту процедуру.

1. Выберите **Start > Run**.

2. Введите (включая кавычки) следующую строку:

   "C:\program files\watchguard\wsm11.0\wbserver\bin\wbserver" -config

Запуск сервера WebBlocker на новом сервере

1. Нажмите правой кнопкой на  в панели задач и выберите **Open WatchGuard Server Center**.
   Откроется диалоговое окно Connect to WatchGuard Server Center.

2. В полях **Username** и **Administrator passphrase** введите имя пользователя и пароль администратора соответственно.

3. Нажмите **Login**.
   Откроется WatchGuard Server Center.

4. В секции **Servers** выберите **WebBlocker Server**.

5. Нажмите **Start Server**.
   Сервер WebBlocker запустится с новой базой данных.

Для того чтобы постоянно обновлять вашу базу данных WebBlocker, мы рекомендуем использовать Планировщик Задач (Windows Task Scheduler).

Приступая к работе с WebBlocker

Перед тем как начать

- Выполните процедуру настройки сервера WebBlocker.

- Загрузите базу данных WebBlocker для сервера WebBlocker. Для более подробной информации см. “Загрузка базы данных WebBlocker”

- Загрузите лицензионный ключ для WebBlocker и импортируйте его на ваше WatchGuard устройство.

Активация WebBlocker на устройстве WatchGuard

При помощи Policy Manager вы можете активировать сервис WebBlocker на вашем устройстве WatchGuard.

1. Откройте Policy Manager.

2. Выберите **Subscription Services** > **WebBlocker** > **Activate**.
   Откроется мастер Activate WebBlocker Wizard.

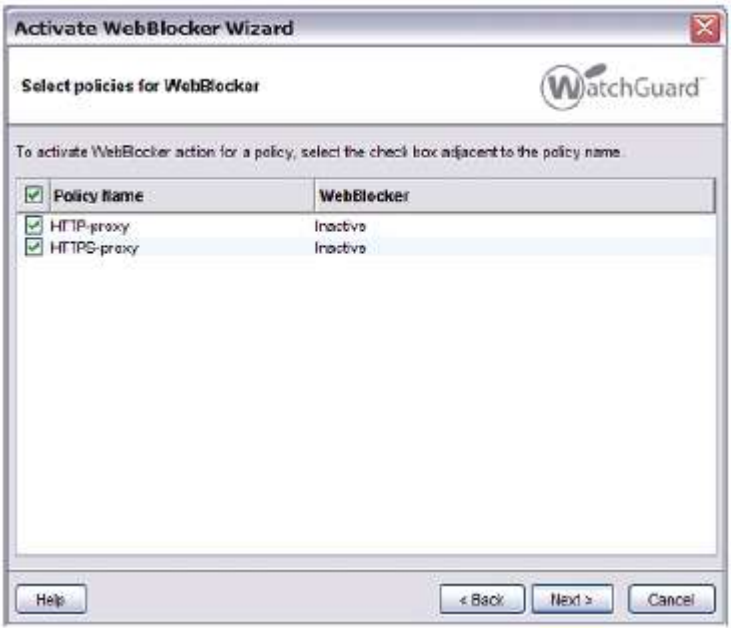
3. Нажмите **Next**.
   Откроется первая страница мастера. Список страниц мастера, которые вы можете увидеть, зависит от вашей конфигурации.

4. Выполните все необходимые инструкции мастера. Мастер содержит три страницы, описание которых приводится далее в этой главе.

Настройка политик для WebBlocker

Эта страница не открывается если вы не создали ни одной политики HTTP proxy. В этом случае мастер создаст политику HTTP прокси для вас.

Если вы создали политики HTTP прокси, то на странице будет список этих политик. Из списка выберите политики прокси, которые вы хотите использовать для WebBlocker. Если вы не выберете ни одной политики, то при помощи действия WebBlocker будет создана новая политика HTTP прокси.



Идентификация серверов WebBlocker

Если у вас устройство Firebox X Core или Peak или устройство WatchGuard XTM, вам необходимо настроить по крайней мере один сервер WebBlocker.

Для того чтобы добавить сервер WebBlocker выполните следующее:

1. Нажмите **Add**.
2. В поле **Server IP** введите IP адрес сервера WebBlocker.
3. При необходимости измените номер порта.

Вы также можете добавить резервный сервер WebBlocker, который будет использоваться в случае если основной сервер выйдет из строя. Основным является сервер, который идет первым в списке

Для того чтобы переместить сервер по списку выполните следующее:

1. Выберите сервер.
2. Нажмите **Move Up** или **Move Down**.

Если вы используете Firebox X Edge, то сервис WebBlocker по умолчанию использует сервер WebBlocker, обслуживаемый компанией WatchGuard. Вы можете настроить сервис WebBlocker таким образом, чтобы он использовал локальный сервер WebBlocker:

1. Выберите **Custom WebBlocker server**.
2. Нажмите **Add**.
3. В поле **Server IP** введите IP адрес сервера WebBlocker
4. При необходимости измените номер порта

Для того чтобы добавить сервер WebBlocker после завершения работы мастера, выполните следующее:

1. Откройте Policy Manager.
2. Выберите **Setup** > **Actions** > **WebBlocker**.
3. Нажмите **Add**.
4. Выберите закладку **Servers**.

Выбор категорий, которые вы хотите заблокировать

- Для того чтобы заблокировать определенные категории сайтов, отметьте флаг напротив тех категорий сайтов, которые вы хотите заблокировать. Категория **Other** заблокирована по умолчанию

- Для того чтобы прочитать описание категории просто нажмите на нее и описание категории появится в нижней части страницы

- Если вы хотите заблокировать доступ к сайтам всех категорий, то включите опцию **Deny All Categories**.

- Для того чтобы убедиться, что пользователи не могли попасть на сайты, которые скрывают реальную информацию о себе или пытаются обойти сервис WebBlocker, заблокируйте категорию **Proxies & Translators**.

Правила исключений для ограничения доступа к сайтам

Вместо категорий вы можете использовать специальные правила исключения.

1. Очистите флаги для всех категорий.

2. Выберите **Deny website access**

Настройка WebBlocker

После активации сервера WebBlocker и создания базового конфигурационного файла, вы можете настроить параметры WebBlocker.

Настройка параметров WebBlocker для политики

1. В Policy Manager выберите **Subscription Services** > **WebBlocker** > **Configure**.
   Откроется диалоговое окно Configure WebBlocker со списком созданных HTTP или HTTPS политик

2. Выберите политику, которую вы хотите настроить, и нажмите **Configure**.
Откроется диалоговое окно WebBlocker Configuration для этой политики

Диалоговое окно **WebBlocker Configuration** содержит следующие закладки:

- Add new servers or change their order
- Change categories to block
- Add exceptions
- Define advanced WebBlocker options
- Define WebBlocker alarms

Копирование параметров WebBlocker из одной политику в другую\

Если у вас есть несколько политик WebBlocker, вы можете при помощи кнопок **Copy** и **Paste** копировать параметры из одной политики в другую.

1. Выберите политику, которую вы хотите настроить, и нажмите **Copy**.
   Кнопка Paste станет активной

2. Выберите политику, в которую вы хотите скопировать параметры, и нажмите **Paste**.
   Параметры WebBlocker будут скопированы в выбранную вами политику.

3. Нажмите **Configure** для того чтобы посмотреть параметры политики.
   Параметры этой политики будут идентичны параметрам политики, из которой вы их скопировали.

Добавление новых серверов WebBlocker или изменение порядка их следования

Вы можете добавить максимум 5 серверов WebBlocker. Если устройство WatchGuard не может подключиться к первому серверу в списке, то оно пытается подключиться к следующему и т.д. Первый сервер в списке является основным сервером.

Добавление сервера

1. В закладке **Servers** диалогового окна **WebBlocker Configuration** нажмите **Add**.
   Откроется диалоговое окно Add WebBlocker Server.

2. Рядом с полем **Server IP** введите IP адрес сервера WebBlocker. При необходимости измените номер порта. Нажмите **OK**.

Изменение порядка следования серверов

1. Вы можете изменить порядок следования серверов, для того чтобы определить порядок, в котором устройство Firebox будет подключаться к резервным серверам. Для изменения положения сервера в списке используйте кнопки **Move Up и Move Down**.

2. Нажмите **OK**.

Если вы используете Firebox X Edge, то сервис WebBlocker по умолчанию использует сервер WebBlocker, обслуживаемый компанией WatchGuard. Вы можете настроить сервис WebBlocker таким образом, чтобы он использовал локальный сервер WebBlocker

Категории WebBlocker

База данных WebBlocker содержит 9 групп категорий с 54 категориями web-сайтов. Сайт добавляется в категорию, если его содержимое соответствует необходимому критерию. Например, категория **Illegal Drugs** блокирует сайты, на которых рассказано как курить марихуану. Эта категория не блокирует сайты, который посвящен истории марихуаны. Категория **Other** включает новые сайты и категории, выпущенные SurfControl, которые не являются частью программного обновления Firebox X Edge. Категория **Uncategorized** содержит сайты, которые не подходят ни к одной категории.

Изменение категорий для блокировки

При использовании мастера Activate WebBlocker wizard вы выбрали категории сайтов, которые вы хотите заблокировать. Выберите закладку **Categories в диалоговом окне WebBlocker Configuration** для того чтобы изменить вашу исходнуб конфигурацию. Это окно очень похоже на окно мастера, описание которого приведено в “Приступая к работе с WebBlocker”. Отличие только в том, что категории сгруппированы под заголовками. Например заголовок Shopping включает Advertisements, Food & Drink, Motor Vehicles, Real Estate, and Shopping. Если вы хотите выбрать все категории под заголовком Shopping рядом с этим заголовоком отметьте флаг. Сайты под этим заголовком будут автоматически выбраны. Если вы хотите выбрать отдельную категорию, то снимите этот флаг и выберите только необходимую вам категорию

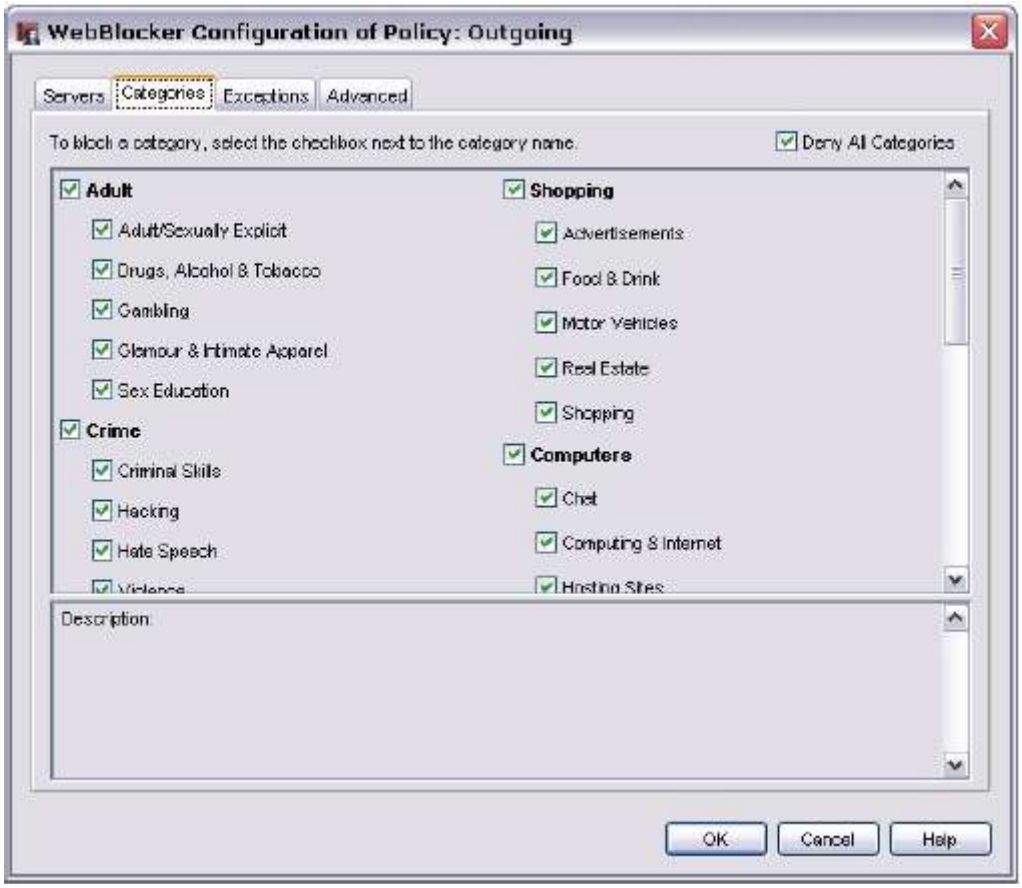
При блокировке сайта отправлять тревогу

Вы можете настроить WebBlocker для отправки тревоги если пользователь пытается подключиться к запрещенному сайту. В секции **Actions to Take** в нижней части диалогового окна выберите **Alarm if denied**.

Для того чтобы настроить параметры тревоги выберите закладку **Alarm**

Запись действий WebBlocker в журнал

Вы можете настроить WebBlocker таким образом, чтобы он записывал в журнал каждую попытку пользователя подключиться к заблокированному сайту. В разделе **Actions to Take** в нижней части диалогового окна выберите **Log this action**



Проверка, добавлен ли сайт в какую-либо категорию

Для того чтобы проверить, добавлен ли сайт, заблокированный WebBlocker, в какую-либо категорию, зайдите на страницу Test-a-Site на сайте SurfControl.

1. Зайдите на страницу: *http://mtas.surfcontrol.com/mtas/WatchGuardTest-a-Site.asp*
   Откроется страница WatchGuard Test-a-Site

2. Введите URL или IP адреса сайта, который вы хотите проверить.

3. В выпадающем списке **Additional Test-a-Site Versions** выберите **54 Category**.

4. Нажмите **Test Site**.
Откроется страница WatchGuard Test-a-Site Results

Добавление, удаление или изменение категории

Если вы получите сообщение о том, что введенного вами URL нет в списке SurfControl, вы можете сообщить об этом прямо на этой странице.

1. На странице **Test Results** нажмите **Submit A Site**.
Откроется страница Submit A Site

2. Выберите, что вы хотите сделать: Добавить сайт (**Add a site**)**,** Удалить сайт **(Delete a site)** или Изменить категорию **(Change the category)**.

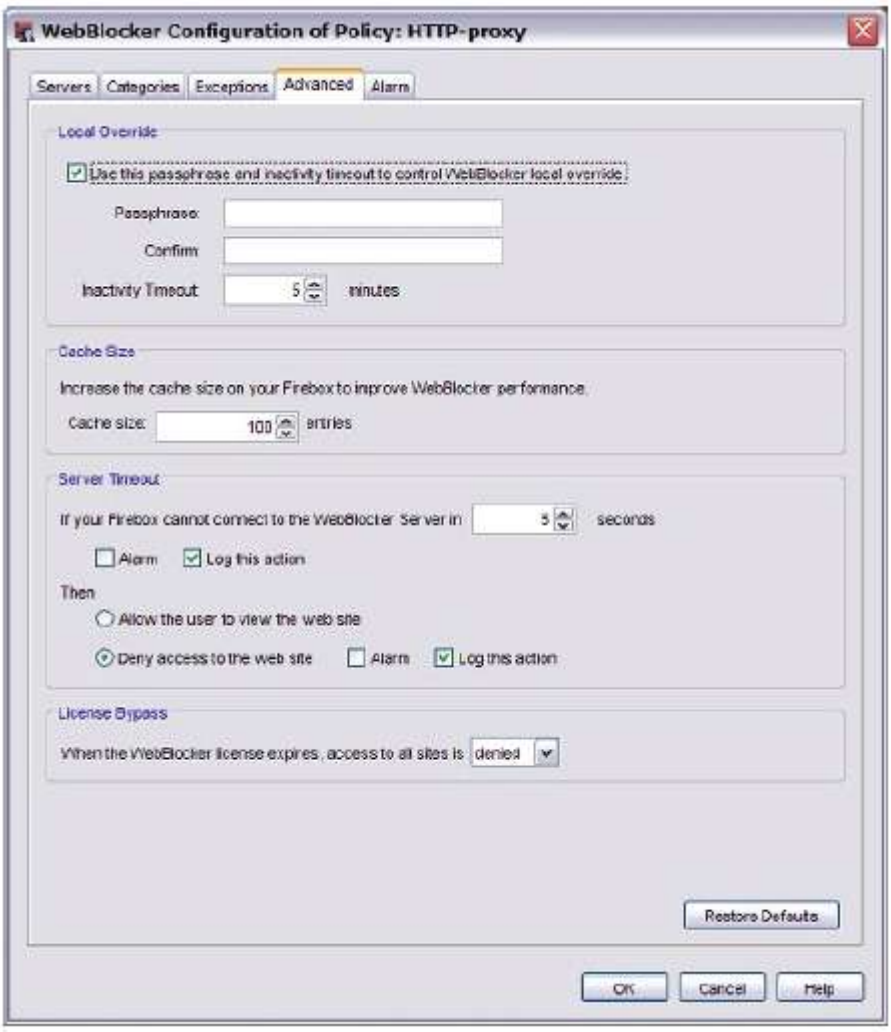
3. Введите URL сайта.

4. Если вы хотите изменить категорию сайта, то в выпадающем списке выберите новую категорию.

5. Нажмите **Submit**.

Настройка дополнительных параметров WebBlocker

Выберите закладку **Advanced** для того, чтобы настроить дополнительные параметры WebBlocker.



Секция Local Override

Если вы хотите, чтобы пользователи обходили систему фильтрации WebBlocker если они знают пароль, включите опцию **Use this passphrase and inactivity timeout to enable WebBlocker local override**. В поле **Passphrase** введите пароль, в поле **Confirm** введите его еще раз. При необходимости вы можете изменить значения поля **Inactivity Timeout**.

После того, как вы включили эту опцию, пользователю для того чтобы подключиться к сайту, заблокированному WebBlocker, необходимо будет ввести пароль. Если пользователь введет правильный пароль, то сервис WebBlocker разрешит пользователю доступ к запрашиваемому сайту. Пользователь сможет пользоваться ресурсами сайта до того, как истечет таймаута неактивности или пользователь закроет аутентифицированный сеанс. Эта опция работает с политиками HTTP прокси

Секция Cache size

Этот параметр используется для увеличения производительности WebBlocker.

Cache Size

При помощи стрелок выберите или введите количество записей в кэше.

Секция Server timeout

If your Firebox cannot connect to the WebBlocker server in

Введите количество секунд, в течение которых Firebox пытается подключиться к серверу.

Alarm

Выберите эту опцию для того чтобы отправлять тревогу каждый раз когда Firebox не может подключиться к серверу WebBlocker. Для того чтобы настроить параметры для тревоги выберите закладку **Alarm**

Log this action

Запись сообщения журнала если Firebox генерирует таймаут

Allow the user to view the website

Опция используется для разрешения пользователю просматривать сайт, Firebox генерирует таймаут и не может подключиться к серверу WebBlocker.

Deny access to the website

Запрет доступа если Firebox генерирует таймаут.

Устройство WatchGuard пытается подключиться к серверу WebBlocker даже, если он недоступен. Если вы разрешите пользователю передачу трафика, когда сервер недоступен, то при отправке запроса вынужден будет ждать некоторое количество времени пока ваше устройство Watchguard будет пытаться подключиться к серверу WebBlocker и сгенерирует таймаут. После этого пользователь сможет подключиться к запрашиваемому сайту. После того, как связь с сервером WebBlocker восстановится, правила WebBlocker снова начнут применяться к трафику.

Секция License Bypass

Эта опция используется в случае, если пользователь запрашивает подключение к сайту, WebBlocker включен и срок действия подписки на сервис WebBlocker истек.

В выпадающем списке **When the WebBlocker license expires, access to all sites is** выберите одну из опций:

denied

Если срок действия лицензии WebBlocker истек, то заблокировать все сайты

allowed

Разрешить доступ к сайтам, даже если срок действия лицензии WebBlocker истек

По умолчанию если срок действия лицензии истек, то доступ ко всем сайтам блокируется

Создание тревог WebBlocker

Для того чтобы настроить параметры уведомлений для тревог WebBlocker выберите закладку **Alarm**. Вы можете отправлять тревогу, каждый раз когда устройство Firebox не может подключиться к серверу WebBlocker и генерирует таймаут, или когда Firebox генерирует таймаут и доступ к сайту закрыт.

Исключения WebBlocker

WebBlocker может заблокировать сайт, который необходим для вашего бизнеса. Вы можете создать *исключение,* которое разрешит пользователям доступ к этому сайту

Например, представим, что сотрудники вашей фирмы часто используют медицинский сайт. Некоторые из таких сайтов могут заблокированы WebBlocker, так как они входят в категорию по сексуальному образованию. Для того чтобы разблокировать этот сайт для доступа, вам необходимо IP-адрес или имя домена этого сайта. Вы также можете заблокировать сайты, которые по умолчанию разрешены WebBlocker.

Исключения применяются только HTTP-трафика.

Если вы заблокируете доступ к сайту при помощи WebBlocker, сайт автоматически не будет добавлен в список Blocked Sites

Создание действия для сайтов, которые не совпадают с исключениями

В секции **Use category list** под списком правил исключений, вы можете настроить действие, которое будет выполнено, если URL не совпадает с вашими исключениям. По умолчанию выбран переключатель **Use the WebBlocker category list to determine accessibility**, and WebBlocker сравнивает сайты с категориями, указанными вами в закладке.

Вы также можете не использовать категории и вместо этого использовать правила исключения для запрета доступа к web сайту.

Для этого выберите переключатель **Deny website access**.

Alarm

Выберите эту опцию для того чтобы отправлять тревогу в случае когда Firebox запрещает исключение WebBlocker. Для того чтобы настроить параметры тревоги выберите закладку **Alarm**

Log this action

Выберите эту опцию для того чтобы записывать в журнал сообщение о том, что Firebox запретил исключение WebBlocker.

Компоненты правила исключения

Исключения основаны на URL-шаблонах, а не на IP-адресах. Вы можете блокировать URL при точном совпадении. Обычно, более удобно использовать поиск шаблонов URL. URL шаблоны не содержат "http://". Для того чтобы шаблон совпадал со URL-путями на всех сайтах, он должен содержать в начале “/*”.

Хост, указанный в URL, может быть именем хоста, которое содержится в HTTP-запросе, или IP-адресом сервера.

На данном этапе сетевые адреса не поддерживаются, хотя в шаблоне вы можете использовать подсети (например, 10.0.0.*).

Для серверов на порту 80, не включайте этот порт. Для серверов на других портах, добавьте “ :port”, например:

10.0.0.1:8080. Вы также можете использовать групповой символ для порта — например, 10.0.0.1:*— но это не применяется для порта 80.

Исключения с частью URL

Вы можете создать исключения WebBlocker с использованием любой части URL. Вы можете установить номер порта, имя пути, или строку, которая должна быть заблокирована для определенного сайта. Например, если необходимо заблокировать только www.sharedspace.com/~dave, потому что там содержатся несоответствующие фотографии, вы введете “www.sharedspace.com/~dave/*”. Это дает возможность пользователю заходить на страницу www.sharedspace.com/~julia, где находится содержимое, которое вы хотите показать пользователям.

Для того чтобы заблокировать URL, которые содержат слово “sex” , вы можете ввести “*/*sex*”. Для того чтобы блокировать URL, которые содержат слово “sex” в пути или в имени хоста, введите “*sex*”.

Вы также можете блокировать порты в URL. Например, взгляните на URL http://www.hackerz.com/warez/index.html:8080.

Этот URL заставляет браузер использовать HTTP-протокол на TCP порту 8080 вместо метода по умолчанию, который использует порт 80. Вы можете заблокировать порт, введя *8080.

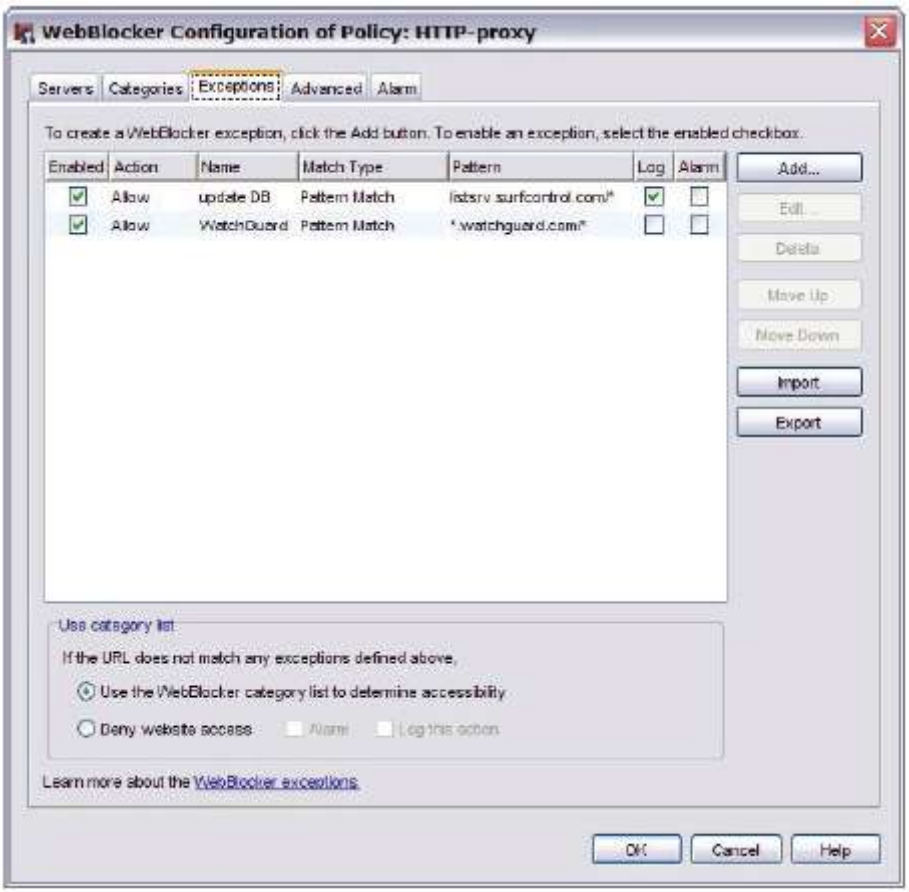
Добавление исключений WebBlocker

Вы можете добавить исключение, которое будет точно совпадать с URL, или вы можете использовать групповой символ "*" в URL. Например, если вы добавите "www.somesite.com" в список Allowed Sites и пользователь введет "www.somesite.com/news", то этот запрос будет заблокирован. Если вы добавите "www.somesite.com/*" в список Allowed Sites, WebBlocker разрешит подключение к этому URL и всем его путям.

Для того чтобы добавить исключения выполните следующее:

Вы также можете отказать от категорий вообще и для запрета доступа к определенным сайтам использовать исключения. Для этого выберите переключатель **Deny website access**.

1. Для того чтобы создать исключения для категорий WebBlocker, выберите закладку **Exceptions**



2. Для того чтобы добавить новое правило исключения нажмите **Add**.
Откроется диалоговое окно New WebBlocker Exception

3. В выпадающем списке **Match Type** выберите одну из следующих опций:

   Pattern match

   Поиск определенного шаблона в URL или адресе сайта, например “pattern” в «www.pattern.com»

   Не забудьте удалить “http://” вначале и добавить “/* в конце. В одном шаблоне вы можете использовать несколько групповых символов. Например шаблон «www.somesite.com/*» будет соответствовать всем URL-путям на сайте www.somesite.com. Для того чтобы ввести адрес используйте шаблон, который заканчивается групповым символом.

   Например для поиска всех сайтов по адресу 1.1.1.1 и порт 8080 введите “*”.

   Exact match

   Поиск полного совпадения шаблона с URL или IP адресом. Здесь вы не можете использовать групповые символы. Например, если вы создадите исключение для «www.yahoo.com» и будете использовать шаблон для полного совпадения, то запрос пользователя на подключение к сайту www.yahoo.com/news будет заблокирован.

   Regular expression

   Регулярные выражения используют синтаксис Perl-совместимых регулярных выражений для поиска. Например шаблон «\.[onc][eor][gtm]» будет соответствовать .org, .net, .com и любой другой комбинации из трех букв, каждая из которых будет совпадать с символом, заключенным в скобки. Не забудьте удалить “http://”

   Групповые символы, использующиеся в shell скрипте, поддерживаются.

   Например выражение “(www)?\.watchguard\.[com|org|net]” будет соответствовать URL, включая www.watchguard.com, www.watchguard.net и www.watchguard.org.

   Выражение «1.1.1.[1-9]» будет соответствовать IP адресам от 1.1.1.1 до 1.1.1.9. Для более подробной информации о регулярных выражениях см. “Регулярные выражения”

4. В выпадающем списке **Type** выберите тип сайта: **URL** или **Host IP Address**.

5. Если вы выберете **URL** в предыдущем поле, введите шаблон, значение или выражение в зависимости от значения в поле **Match Type.** Если вы выберете **Host IP Address** в предыдущем поле, введите адрес, порт и каталог

6. Нажмите **OK** для того чтобы закрыть диалоговое окно **New WebBlocker Expression**.

7. Нажмите на колонку **Action** для того чтобы получить доступ к выпадающему списку **Action**. Выберите необходимое действие.

8. В поле **Name** введите название исключения. По умолчанию используется следующее имя: WB Rule[номер]. Для исключений WebBlocker вы можете использовать следующие опции:

   * Если вы хотите изменить настройки, которые вы сделали в диалоговом окне **New WebBlocker Exception,** вы можете использовать выпадающие списки для полей **Match Type** и **Pattern**.

   * Если вы хотите чтобы при выполнении действия над исключением генерировалось сообщение журнала включите опцию **Log**.

   * Для того чтобы выключить использование исключений отключите опцию **Enabled**.

   * В секции **Use category list** под списком правил исключений, вы можете настроить действие, которое будет выполнено, если URL не совпадает с вашими исключениям. По умолчанию выбран переключатель **Use the WebBlocker category list to determine accessibility**, and WebBlocker сравнивает сайты с категориями, указанными вами в

закладке.

* Вы также можете не использовать категории и вместо этого использовать правила исключения для запрета доступа к web сайту. Для этого выберите переключатель **Deny website access**.

Изменение порядка следования правил исключения

Порядок следования правил исключений в списке – это порядок, в котором к сайтам применяются правила. WebBlocker сравнивает сообщение с первым правилом в списке, и если сообщение не удовлетворяет этому правилу, сравнивает со следующим правилом в списке, и т.д. WebBlocker выполняет действие, указанное в первом правиле, которому удовлетворит сайт. Если сайт удовлетворяет правилам далее по списку, то они игнорируются.

Для того чтобы изменить порядок следования правил в списке, выберите правило и при помощи кнопок **Up** или **Down** переместите правило в необходимую позицию.

Импорт или экспорт правил исключений WebBlocker

Если у вас есть несколько Firebox или вы используете WebBlocker с несколькими прокси, вы можете импортировать или экспортировать правила исключений. Это позволяет вам сэкономить время, так как вам необходимо создать только одно правило. Вы можете перемещать правила между прокси или устройствами Firebox двумя способами.

Вы можете создать ASCII файл, который содержит правила, и импортировать его на остальные Firebox или прокси. Или вы можете использовать пользовательский интерфейс WebBlocker для создания правил исключений, экспортировать их в файл и затем импортировать этот файл на другой Firebox или прокси

Запись наборов правил в ASCII файл

Вы можете записать правила в обычный ASCII файл, который использует стандартную UTF-8 кодировку. В каждой строчке необходимо указать только одно правило.

[rule_name, action, **enabled|disabled, log|no log**, match_type,] pattern_value

где:

rule_name это имя правила в списке исключений.

По умолчанию используется правило **WB Rule** *n*.

action = **Allow** или **Deny**. По умолчанию - **Allow**.

enabled|disabled = Включено или отключено правило. По умолчанию - **enabled**

log|no log = Включение или выключение записи действия в журнал. По умолчанию - **no log**.

match_type = Тип совпадения: точное совпадение (exact match), регулярное выражение (regular expression) и совпадение по шаблону (pattern match).

По умолчанию - **pattern match**.

value = значение для совпадения.

Поля в скобках необязательны. Если вы их не будете использовать, то использованы будут значения по умолчанию.

Комментарии в файле начинаются с символа (#).

Ниже приведен пример файла правил исключений.

```
#

# Here are five exception rules

#

AllowFB, allow, enabled, No Log,*.firebox.net/*

deny, disabled, Log, very.badsite.com/*

ExceptionRule1,*.goodsite.com/"

exact match, 10.0.0.1

*.xyz.*/
```

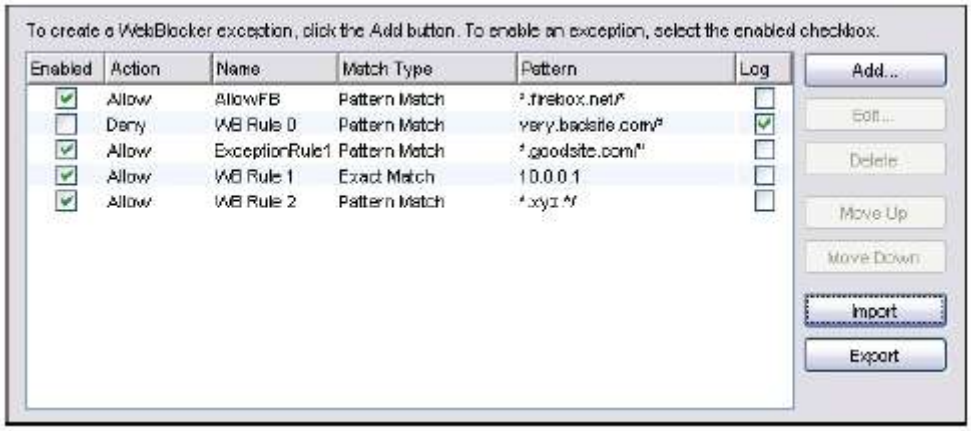
Следующая секция, показывает как будет выглядеть файл после импорта в WebBlocker

Импорт ASCII файла исключений

1. В закладке **Exceptions** диалогового окна **WebBlocker Configuration** нажмите **Import**.

2. Найдите необходимый файл и нажмите **Open**.

3. Если такие исключения уже существуют, система попросит вас подтвердить – хотите ли вы заменить существующие исключения в WebBlocker или добавить эти. Если вы хотите изменить порядок следования правил см. “Изменение порядка следования правил исключения”. Если вы импортируете файл примера в WebBlocker, то он будет выглядеть следующим образом



Экспорт правил в ASCII файл

Если вы экспортируете правила исключений из прокси, Firebox сохраняет текущие правила в текстовый ASCII файл в формате, описанном в “Импорт или экспорт правил исключений WebBlocker”

1. В закладке **Exceptions** диалогового окна **WebBlocker Configuration**, создайте необходимые исключения.

2. Нажмите **Export**.

В диалоговом окне **Open** выберите каталог, куда вы хотите сохранить исключения и нажмите **Save**. Теперь вы можете открыть другой HTTP прокси в этом же или в другом конфигурационном файле и импортировать файл исключений

Предоставление доступа пользователям к определенному набору сайтов

Вы можете настроить WebBlocker таким образом, для того, чтобы он пользователям предоставлял доступ только к одному сайту или набору сайтов. Для каждого сайта, доступ к которому вы хотите предоставить пользователям, в список исключений вам необходимо добавить разрешенное исключение. Затем вам необходимо настроить WebBlocker, чтобы он блокировал доступ к сайтам, которых нет в этом списке. В такой конфигурации WebBlocker для предоставления доступа к сайтам не использует список категорий. Для того чтобы разрешить пользователям доступ к определенному сайту на базе шаблона URL выполните следующее:

1. В Policy Manager выберите **Subscription Services** > **WebBlocker** > **Configure**.
   Откроется диалоговое окно Configure WebBlocker со списком созданных HTTP или HTTPS политик.

2. Выберите политику, которую вы хотите настроить. Нажмите **Configure**.
   Откроется диалоговое окно WebBlocker Configuration.

3. Выберите закладку **Exceptions**.
Закладка Exceptions содержит список созданных исключений

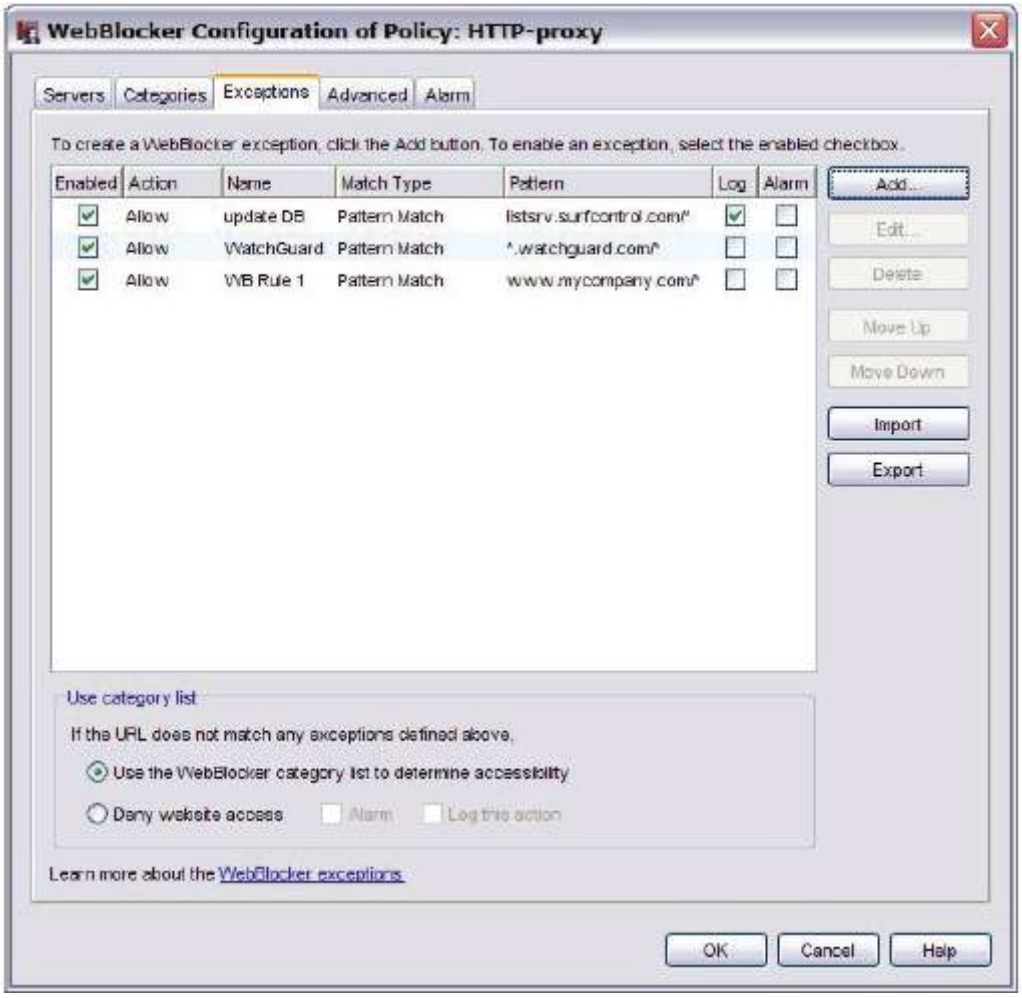
4. Для того чтобы добавить новое правило исключения нажмите **Add**.
Откроется диалоговое окно New WebBlocker Exception

5. В выпадающем списке **Match Type** выберите **Pattern Match**.

6. В выпадающем списке **Type** выберите **URL**.

7. В поле Pattern введите шаблон URL. Например, шаблон `www.mycompany.com/*` разрешит доступ ко всем URL путям на сайте www.mycompany.com. При вводе шаблона URL не вводите http:// в начале строки. Для того чтобы разрешить доступ ко всем URL путям введите прямую косую черту (/) в конце шаблона. Групповой символ (*) используется для поиска любого символа. В тексте шаблона вы можете использовать несколько групповых символов

8. Нажмите **OK** для того чтобы закрыть диалоговое окно **New WebBlocker Exception**.
   В окне WebBlocker Configuration вы увидите созданное вами исключение.



9. Если вы хотите редактировать какое-либо исключение нажмите на колонку **Name** этого исключения. По умолчанию используется следующее имя `WB Rule[number]`.

10. Для того чтобы добавить исключения для других сайтов, доступ к которым вы хотите разрешить вашим пользователям, см. п. 2 – 7.

11. После того, как вы добавите все необходимые сайты в список исключений, выберите переключатель **Deny website access**. После этого сервис WebBlocker будет блокировать доступ к сайтам, которых нет в этом списке.

12. Нажмите **OK**. Сохраните конфигурационный файл.

Действия WebBlocker в настройках прокси

Базовая конфигурация, которую вы создаете в **Tasks > WebBlocker > Configure** – это действие WebBlocker—набор параметров WebBlocker—которое вы можете применить для HTTP или HTTPS прокси. Вы можете создать дополнительные действия WebBlocker.

Создание дополнительных действий WebBlocker

1. В Policy Manager выберите **Setup > Actions > WebBlocker**.
   Откроется диалоговое окно WebBlocker Configurations.

2. Нажмите **Add**. Или если вы хотите создать новое действие, на базе уже существуюещего, выберите это действие и нажмите **Clone**.

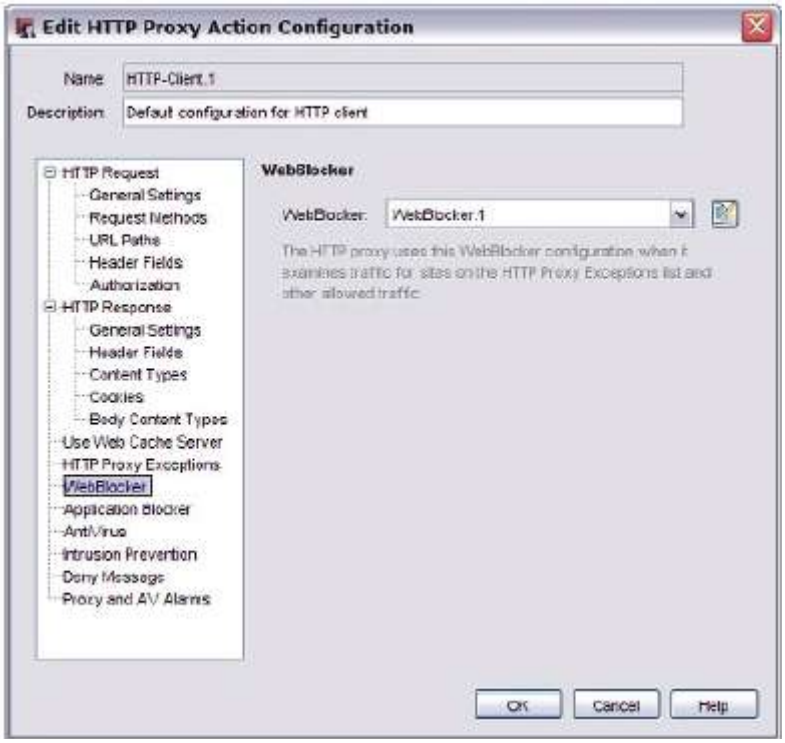
3. Настройте параметры действия WebBlocker

Добавление действий WebBlocker к политике

1. Два раза нажмите на иконку политики HTTP для того чтобы открыть диалоговое окно **Edit Policy Properties**.

2. Выберите закладку **Properties**.

3. Нажмите на иконку **View/Edit Proxy**.
   Откроется диалоговое окно HTTP Proxy Action Configuration



4. Выберите WebBlocker из списка категорий

5. Из выпадающего списка **WebBlocker** выберите действие **WebBlocker**.

Расписание действий WebBlocker

Для политики вы можете создать рабочее расписание. Вы можете использовать предопределенные параметры в выпадающем списке или создать новое расписание. Вы можете использовать эти периоды времени для установки правил для блокировки сайтов. Например, вы можете запретить спортивные сайты в рабочее время, но разрешить использовать эти сайты во время ланча, в вечернее время, на выходных.

Для того чтобы создать расписание для политики, выполните следующее

1. Откройте политику для редактирования и выберите закладку **Advanced**.

2. Из выпадающего списка выберите расписание, или нажмите на иконку New/Clone для создания нового расписания

Настройте HTTP-политику, которая использует расписание. Вы также можете настроить две HTTP-политики, но создать расписание только для одной. Каждая политика использует одно из действий HTTP proxy. Каждое из действий HTTP proxy указывает на одно из хотя бы двух действий Web-Blocker

Истечение срока действия сервиса WebBlocker

Если ваш сайт использует WebBlocker, вам необходимо обновить или отключить сервис WebBlocker после того как истечет срок его действия. WebBlocker по умолчанию блокирует весь трафик, когда все подключения к серверу были закрыты по причине таймаута. Когда срок действия сервиса WebBlocker истек, то он больше не сможет подключаться к серверу, что в результате для Firebox выльется в таймаут сервера. Весь HTTP трафик будет заблокирован. Поэтому мы вам рекомендуем изменить настройки WebBlocker по умолчанию еще од истечения срока его действия.

Для этого откройте диалоговое окно **WebBlocker Configuration** и выберите закладку **Advanced**. В разделе **License Bypass** значение поля установите в **Allowed**.

Примеры

Использование локального пароля WebBlocker

Локальный пароль WebBlocker – это опция, которая позволяет пользователю, зная локальный пароль, получить доступ к сайту, который заблокирован политикой WebBlocker. Например в школе учитель может использовать локальный пароль для того чтобы разрешить ученикам доступ к сайту, который заблокирован WebBlocker. Если пользователь при включенной опции локального пароля пытается подключиться к сайту, который заблокирован политикой WebBlocker, то он увидит в браузере deny-сообщение

Если для аутентификации устройство WatchGuard использует самоподписанные сертификаты, пользователь также может увидеть предупреждение о безопасности. Для этого мы рекомендуем установить доверенный сертификат на Firebox или импортировать самоподписанный сертификат на компьютер каждого пользователя.

Для того чтобы получить доступ к запрашиваемому сайту пользователю необходимо ввести значения **override destination** и **override password**.

1. В поле **Override destination** введите URL, доступ к которому вы хотите разрешить. По умолчанию значение поля **Override destination** равно заблокированному URL. При вводе значения Override Destination вы можете использовать групповые символы. Например:

   **.amazon.com*

   Разрешает доступ ко всем поддоменам amazon.com

   **amazon.com*

   Разрешает доступ ко всем доменам, имя которых заканчивается на «amazon.com». Например «images-amazon.com»

   *www.amazon.com/books-used-books-textbooks/**

   Разрешает доступ только страницам этого пути.

2. В поле **Override Password** введите локальный пароль, который был создан в профиле WebBlocker.

3. Нажмите **Submit**.

После того, как пользователь введет корректный пароль, Firebox разрешит доступ к сайту, указанному в поле **Override destination** на промежуток времени, который определяется аутентифицированным сеансом пользователя или величиной таймаута неактивности WebBlocker.

Вы можете включить функцию **local override** и установить значение таймаута неактивности в закладке Advanced в конфигурации WebBlocker.

Настройка политик WebBlocker для группы пользователей

Многие организации хотят каждой определенной группе пользователей предоставлять различные уровни доступа к различным сайтам в сети Интернет. Для этого вам необходимо:

- Создать группы пользователей на вашем сервере аутентификации.
- Создать политику HTTP прокси для каждой группы пользователей. Политика включает настройки WebBlocker для данной группы.
- Создайте политику HTTP прокси для неаутентифицированных пользователей, которые будут автоматически перенаправлены на страницу аутентификации WatchGuard authentication.

Пример

В качестве примера возьмем две группы, для которых мы хотим настроить различные уровни доступа:

- Группа Students (более ограниченный доступ)
- Группа Teachers (менее ограниченный доступ)

Создание групп на сервере аутентификации

Сначала вам необходимо настроить аутентификацию пользователей: Active Directory, локальная аутентификация, Radius или LDAP. В этом примере мы будем использовать аутентификацию на сервере Active Directory.

На сервере аутентификации вам необходимо создать две группы: Teachers и Students

Создание политики HTTP для группы с более ограниченным доступом

1. В Policy Manager в панели инструментов нажмите (+). ли выберите **Edit** > **Add Policies**.
   Откроется диалоговое окно Add Policies.
2. Откройте каталог **Proxies** (нажмите (+) слева от каталога)
   Откроется список прокси.

3. Выберите прокси **HTTP**. Нажмите **Add**.
   Откроется диалоговое окно New Policy Properties

4. В поле **Name** введите имя политики. В этом примере мы назовем политику просто **HTTP-proxy-Students**.

5. В закладке **Policy** в разделе **From** нажмите **Any-Trusted**. Затем нажмите **Remove**.

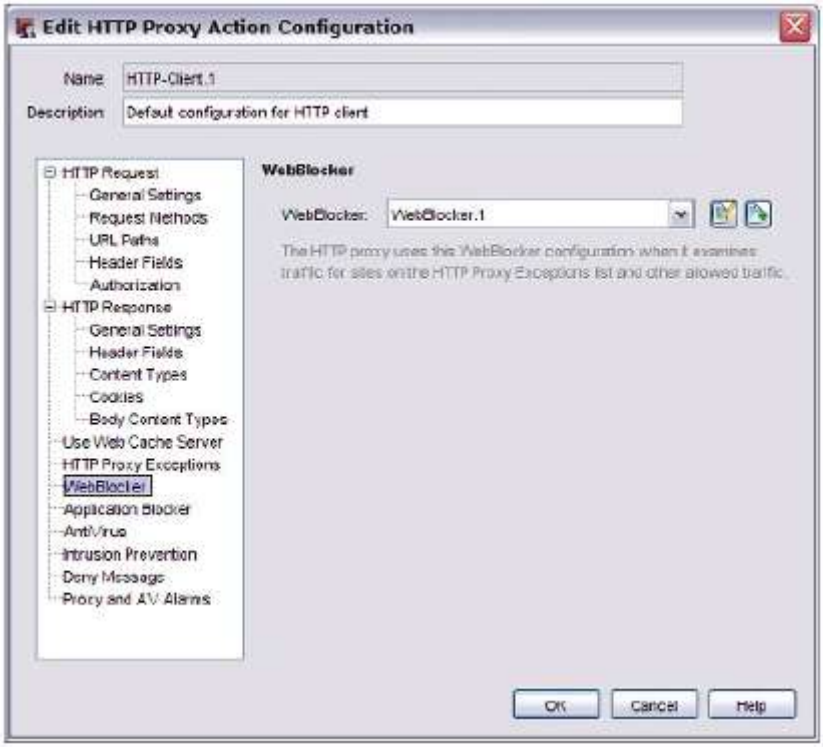
6. В секции **From** нажмите **Add** для того, чтобы добавить группу пользователей к этой политике.
   Откроется диалоговое окно Add Address.

7. Нажмите **Add User**. Для **Type** выберите **Firewall** или **Group**.
   Откроется диалоговое окно Authorized Users or Groups

8. Выберите группу, для которой вы хотите настроить наиболее ограниченный доступ. Нажмите **Select**. Затем нажмите **OK**. В этом примере мы добавим группу Active Directory под названием **Students**.

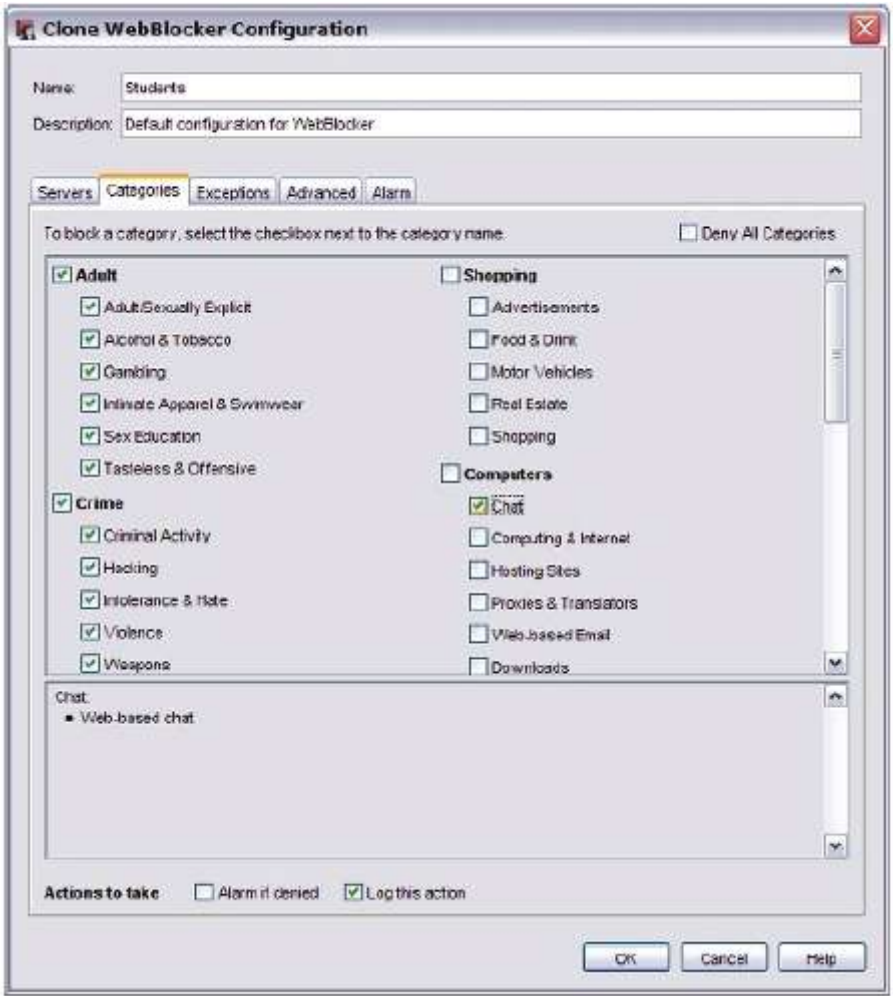
9. Выберите закладку **Properties**.

10. Нажмите на иконку **View/Edit Proxy**. 
Откроется диалоговое окно HTTP Proxy Action Configuration



11. В списке слева выберите **WebBlocker**.
Откроется страница конфигурации WebBlocker.

12. Рядом с выпадающим списком **WebBlocker** нажмите иконку **New/Clone**.
Откроется диалоговое окно WebBlocker Configuration



13. В поле **Name** введите имя конфигурации WebBlocker. В этом примере - **Students**.

14. В закладке **Servers** нажмите **Add**, и введите IP адрес сервера WebBlocker.

15. Выберите закладку **Categories** для того чтобы посмотреть категории содержимого, которое вы можете заблокировать.

16. Напротив каждой категории, которую вы хотите заблокировать для группы **Students**, отметьте флаг.

17. Нажмите **OK** для того чтобы закрыть диалоговое окно **WebBlocker Configuration**.

18. Нажмите **OK** для того чтобы закрыть диалоговое окно **HTTP Proxy Action Configuration**.

19. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Policy Properties**.

Создание политики HTTP для группы с менее ограниченным доступом

Политика для группы **Teachers** создается аналогично группе **Students**.

1. В Policy Manager в панели инструментов нажмите (+). Или выберите Edit > Add Policies.
Откроется диалоговое окно Add Policies.

2. Откройте каталог **Proxies** (нажмите (+) слева от каталога)
Откроется список прокси.

3. Выберите прокси **HTTP**. Нажмите **Add**.
   Откроется диалоговое окно New Policy Properties.

4. В поле **Name** введите имя политики. В этом примере мы назовем политику просто **HTTP-proxy-Teachers**.

5. В закладке **Policy** в разделе **From** нажмите **Any-Trusted**. Затем нажмите **Remove**.

6. В секции **From** нажмите **Add** для того, чтобы добавить группу пользователей к этой политике.
   Откроется диалоговое окно Add Address.

7. Выберите группу, для которой вы хотите настроить наиболее ограниченный доступ. Нажмите **Select**. Затем нажмите **OK**. В этом примере мы добавим группу Active Directory под названием **Teachers**.

8. Нажмите на иконку **View/Edit Proxy**. 
   Откроется диалоговое окно HTTP Proxy Action Configuration.

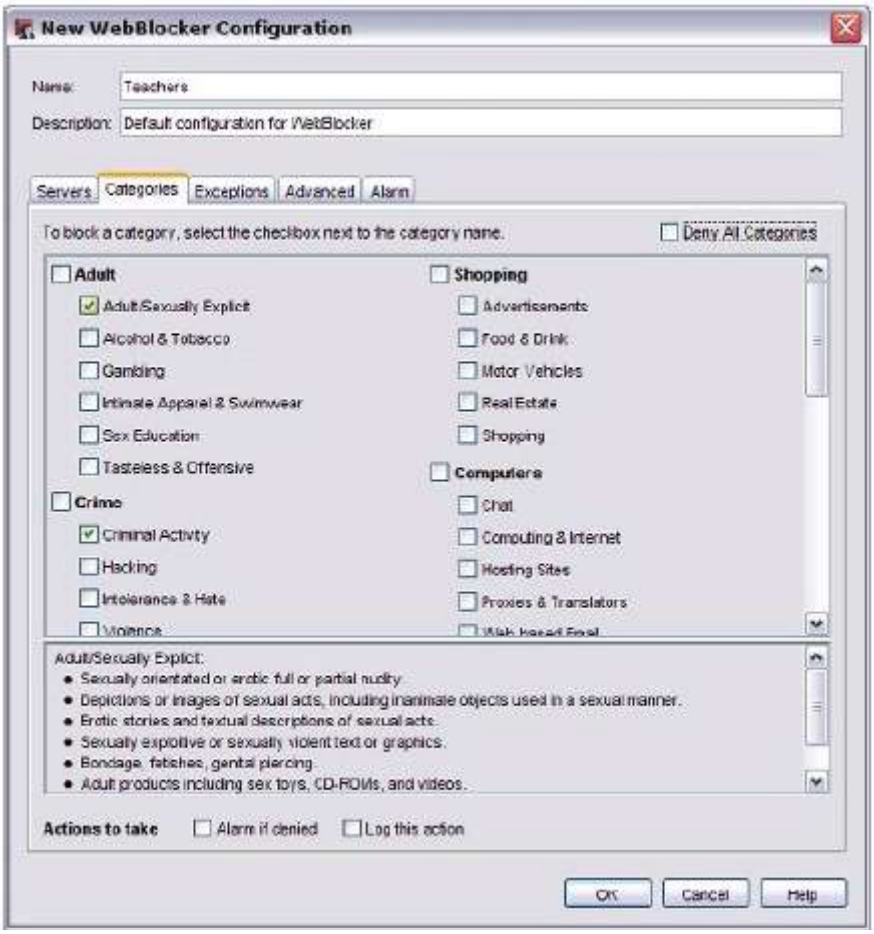
9. В списке слева выберите **WebBlocker**.
   Откроется страница конфигурации WebBlocker.

10. Рядом с выпадающим списком **WebBlocker** нажмите иконку **New/Clone**. 
    Откроется диалоговое окно New WebBlocker Configuration.

11. В поле **Name** введите имя конфигурации WebBlocker. В этом примере - **Teachers**.

12. В закладке **Servers** нажмите **Add**, и введите IP адрес сервера WebBlocker.

13. Выберите закладку **Categories** для того чтобы посмотреть категории содержимого, которое вы можете заблокировать



14. Напротив каждой категории, которую вы хотите заблокировать для группы **Students**, отметьте флаг.

15. Нажмите **OK** для того чтобы закрыть диалоговое окно **WebBlocker Configuration**.

16. Нажмите **OK** для того чтобы закрыть диалоговое окно **HTTP Proxy Action Configuration**.

17. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Policy Properties**.

Создание HTTP прокси для блокировки исходящего HTTP доступа и переадресация пользователей на страницу аутентификации

1. В Policy Manager в панели инструментов нажмите (+). Или выберите **Edit** > **Add Policies**.
   Откроется диалоговое окно Add Policies.

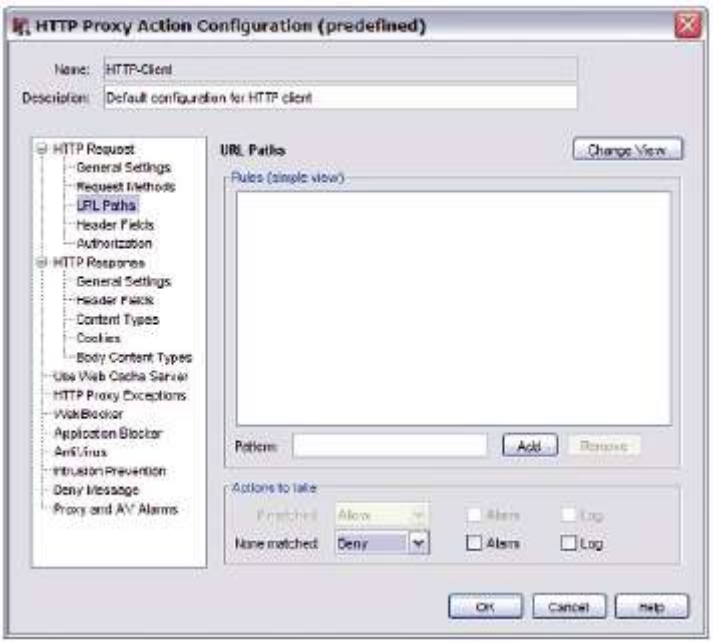
2. Откройте каталог **Proxies** (нажмите (+) слева от каталога)
   Откроется список прокси.

3. Выберите прокси **HTTP**. Нажмите **Add**.
   Откроется диалоговое окно New Policy Properties

4. В поле **Name** введите имя политики. В этом примере мы назовем политику просто **HTTP-proxy-redirect**.

5. Выберите закладку **Properties**.

6. Нажмите на иконку **View/Edit Proxy**. 
   Откроется диалоговое окно HTTP Proxy Action Configuration



7. В списке слева выберите **URL Paths**.

8. В выпадающем списке **None matched** выберите **Deny**.

9. В списке слева выберите **Deny Message**

10. Скопируйте нижеприведенный текст и скопируйте его в поле **Deny Message**. Этот текст содержит XML команды, которые автоматически переадресуют пользователя на страницу аутентификации

```
https://<your firebox IP address>:4100.
Content-type: text/html; charset="iso-8859-1"
<html>
<META HTTP-EQUIV="Refresh" CONTENT="10;url=https://?.?.?.?:4100/">
<h3> %(transaction)% denied by WatchGuard HTTP proxy. </h3>
<b> Reason: </b> %(reason)% <br>
<hr size="1" noshade>
<b> Method: </b> %(method)% <br>
<b> Host: </b> %(url-host)% <br>
<b> Path: </b> %(url-path)% <br>
<hr size="1" noshade>
<p>You have not authenticated yet. You will be redirected to the WatchGuard
device Authentication page in 15 seconds.</p>
<p>To go there immediately, click <a href="https://?.?.?.?:4100/">here</a>.</p>
</body>
</html>
```

11. Текст `"?.?.?.?"` замените IP адресом вашего WatchGuard устройства.

12. Нажмите **OK** для того чтобы закрыть диалоговое окно **Edit HTTP Proxy Action Configuration**.

13. Нажмите **OK** для того чтобы закрыть диалоговое окно **New Policy Properties**.

14. В Policy Manager выберите **File > Save > To Firebox** для того чтобы сохранить вашу конфигурацию.

Теперь WebBlocker будет использовать различные политики для различных групп аутентифицированных пользователей, и автоматически будет перенаправлять неаутентифицированных пользователей на страницу аутентификации устройства WatchGuard.

Сервер WebBlocker, защищенный другим WatchGuard устройством

Если у вас есть несколько географически разделенных WatchGuard устройств, вы можете настроить WebBlocker в офисе филиала таким образом, для того, чтобы он использовать сервер WebBlocker, подключенный к WatchGuard устройству в центральном офисе. Существует два способа настройки такой конфигурации.

- Передавать трафик WebBlocker через BOVPN туннель. Этот трафик будет передаваться в зашифрованном виде.

- Передавать трафик WebBlocker в открытом виде по сети Интернет. Этот трафик будет передаваться в открытом виде.

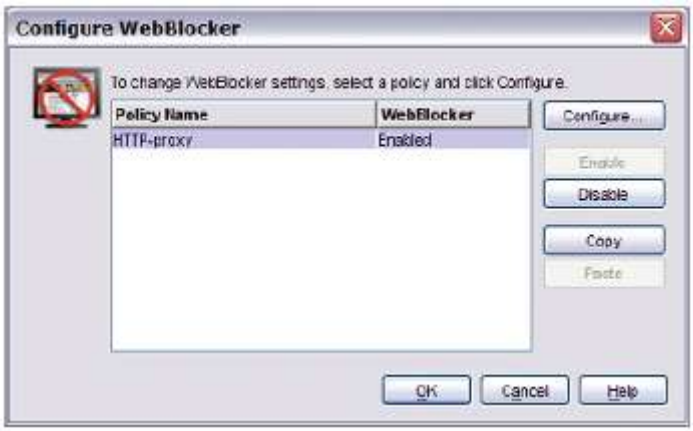
В этой конфигурации под **центральным устройством WatchGuard** подразумевается устройство, которое защищает сервер WebBlocker, **устройство WatchGuard филиала** – это устройство, которое будет подключаться к серверу WebBlocker, защищенного центральным устройством.

Передача трафика WebBlocker через BOVPN

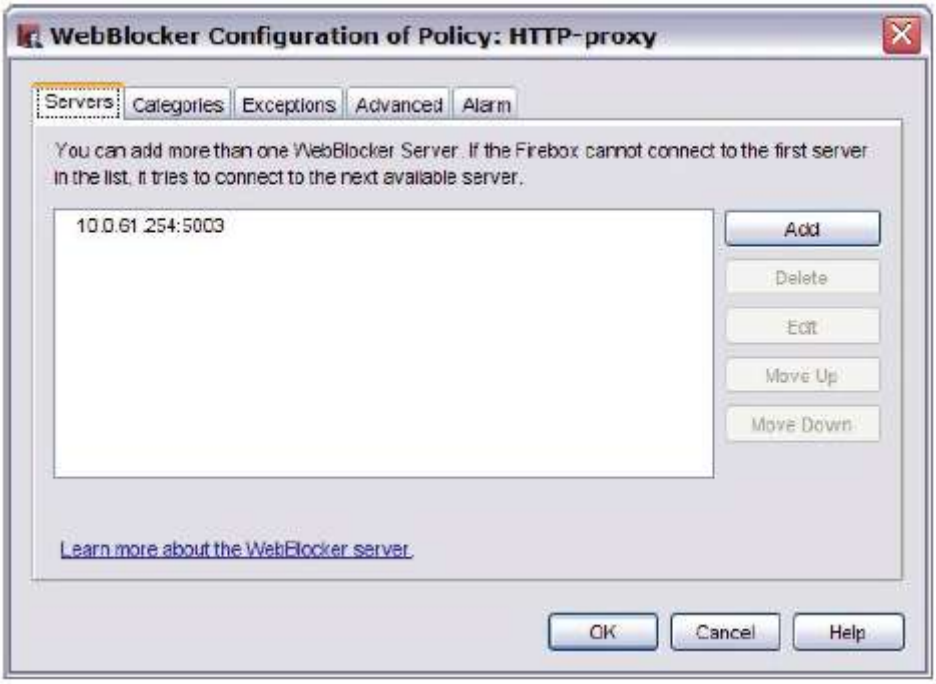
Если у вас между двумя устройствами WatchGuard создан BOVPN туннель, то вы можете настроить передачу трафика WebBlocker через него. Мы рекомендуем использовать именно эту конфигурацию, так как трафик между двумя устройствами будет передаваться в зашифрованном виде.

На каждом устройстве WatchGuard филиала вам необходимо настроить IP адрес сервера WebBlocker:

1. В Policy Manager выберите **Subscription Services** > **WebBlocker** > **Configure**.
   Откроется диалоговое окно Configure WebBlocker



2. Выберите политику и нажмите **Configure**.
Откроется диалоговое окно WebBlocker Configuration of Policy для этой политики



3. Нажмите **Add** для того чтобы добавить IP адрес сервера WebBlocker. Или выберите существующий IP адрес и нажмите **Edit**.
Откроется диалоговое окно Edit WebBlocker Server.

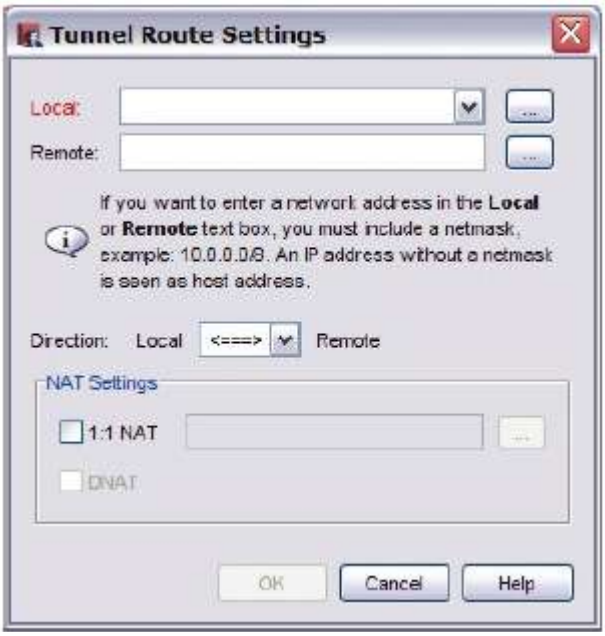
4. В поле **Server IP** введите реальный (внутренний) IP адрес центрального сервера WebBlocker.

На каждом устройстве WatchGuard филиала добавьте маршрут туннеля на сервер WebBlocker:

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.
Откроется диалоговое окно Branch Office IPSec Tunnels

2. Выберите туннель к центральному устройству WatchGuard и нажмите **Edit**.
Откроется диалоговое окно Edit Tunnel.

3. В закладке **Addresses** нажмите **Add**.
Откроется диалоговое окно Tunnel Route Settings



4. Для **Local** введите внешний IP адрес устройства WatchGuard филиала.

5. Для **Remote** введите внутренний IP адрес сервера WebBlocker.

6. Сохраните конфигурацию на устройстве.

На центральном устройстве WatchGuard добавьте маршрут туннеля с сервера WebBlocker к каждому устройству филиала:

1. В Policy Manager выберите **VPN > Branch Office Tunnels**.

2. Выберите туннель к устройству WatchGuard в филиале и нажмите **Edit**.

3. В закладке **Addresses** выберите **Add**.

4. Для **Local** введите внутренний IP адрес сервера WebBlocker.

5. Для **Remote** введите внешний IP адрес устройства WatchGuard филиала.

6. Если у вас есть несколько филиалов, то вам необходимо повторить эту процедуру для каждого

7. Сохраните конфигурацию.

Теперь устройство WatchGuard, находящееся в филиале, может обмениваться данными с центральным сервером WebBlocker по зашифрованному VPN туннель.

Передача трафика WebBlocker в открытом виде по сети Интернет

Мы не рекомендуем передавать трафик WebBlocker по сети Интернет в открытом виде. Вы можете использовать такую конфигурацию, когда вам необходимо запасной путь в случае если VPN туннель станет недоступным

На каждом устройстве WatchGuard филиала вам необходимо настроить IP адрес сервера WebBlocker:

1. В Policy Manager выберите **Subscription Services > WebBlocker > Configure**.
   Откроется диалоговое окно Configure WebBlocker

2. Выберите политику и нажмите **Configure**.
   Откроется диалоговое окно WebBlocker Configuration of Policy для этой политики

3. Нажмите **Add** для того чтобы добавить IP адрес сервера WebBlocker. Или выберите существующий IP адрес и нажмите **Edit**.
   Откроется диалоговое окно Edit WebBlocker Server.

4. В поле **Server IP** введите внешний IP адрес центрального устройства WatchGuard, которое защищает сервер WebBlocker.

5. Нажмите **OK**.

6. Сохраните конфигурацию.

На центральном устройстве WatchGuard создайте политику WB-WebBlocker:

1. В Policy Manager выберите **Edit > Add Policy**.

2. Откройте каталог **Packet Filters (нажмите** (+) слева от него).

3. Два раза нажмите на политику **WB-WebBlocker**.
Откроется диалоговое окно New Policy Properties

4. В разделе **From** выберите **Any-Trusted**. Нажмите **Remove**.

5. В разделе **From** нажмите **Add**.
Откроется диалоговое окно Add Address

6. Если устройство филиала имеет динамический внешний IP адрес, в списке **Available Members.** Выберите **Any-External**. Нажмите **Add**.

7. Если устройство филиала WatchGuard имеет внешний статический IP адрес, см. инструкцию по добавлению IP адреса хоста для каждого устройства WatchGuard, которое будет использовать сервер WebBlocker.

* Нажмите **Add Other**.

* В выпадающем списке **Choose type** выберите **Host-IP**.

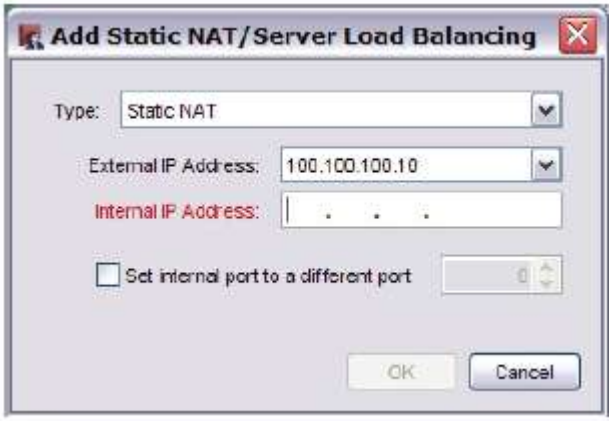
* В текстовом поле **Value** введите внешний IP адрес устройства филиала. Нажмите **OK**.

8. Нажмите **OK** для того чтобы закрыть диалоговое окно **Add Address**.

9. В диалоговом окне **New Policy Properties** в разделе **To** выберите **Any-External**. Нажмите **Remove**.

10. Нажмите **Add**.
Откроется диалоговое окно Add Address.

11. Нажмите **Add NAT**.
Откроется диалоговое окно Add Static NAT/Server Load Balancing



12. В выпадающем списке **Type** выберите **Static NAT**.

13. В выпадающем списке **External IP Address** выберите IP адрес External интерфейса.

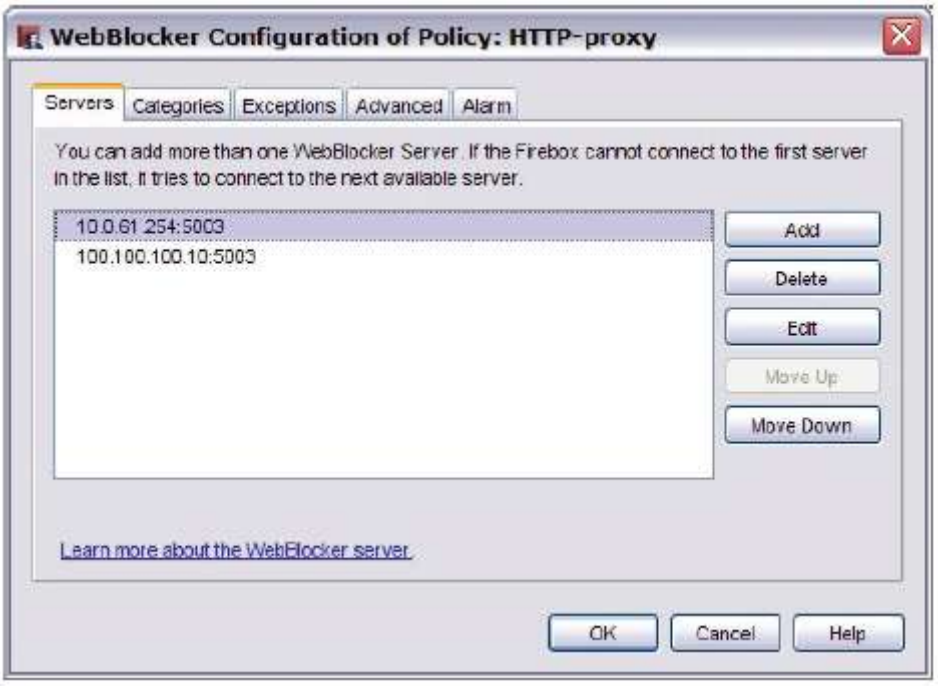
14. В поле **Internal IP Address** введите внутренний IP адрес сервера WebBlocker. Нажмите **OK**.

15. Сохраните конфигурацию.

Теперь устройство филиала может использовать центральный сервер WebBlocker

Настройка резервного подключения к серверу WebBlocker

Если для передачи WebBlocker трафика вы используете VPN туннель и он выйдет из строя, то сервис WebBlocker не сможет получить доступ к серверу WebBlocker. Для обеспечения резервирования, вы можете использовать сеть Интернет, как резервный путь для передачи трафика на сервер WebBlocker. Если вы хотите настроить два подключения, то убедитесь, что сервис WebBlocker на устройстве филиала использует внутренний IP адрес сервера WebBlocker в качестве первого сервера в списке.



В этой конфигурации сервис WebBlocker на устройстве сначала пытается подключиться к центральному серверу WebBlocker через VPN туннель. Если подключение неудачно, то он пытается подключиться к серверу через сеть Интернет.

Глава 31 - spamBlocker

spamBlocker

Нежелательная почта, также известная как спам, заполняет электронные ящики пользователей с огромной скоростью, что приводит к уменьшению пропускной способности, продуктивности работы ваших сотрудников и увеличению использования сетевых ресурсов.

WatchGuard spamBlocker использует ведущую мировую технологию от компании Commtouch для блокировки спама на вашем Интернет шлюзе и предотвращает его попадание на ваш сервер электронной почты.

Коммерческие фильтры электронной почты используют различные методы для поиска спама. В черном списке хранится список доменов, которые используются источниками спама или используются для трансляции спама. Фильтры содержимого ищут ключевые слова в заголовке и теле письма. Процедура обнаружения URL сравнивает список доменов, которые используюся источниками спама, с URL, который содержится в теле электронного письма.

Однако, все эти процедуры сканируют каждое электронное письмо. Хакеры могут легко обойти эти алгоритмы защиты. Для обхода черного списка они могут маскировать адрес отправителя, изменить ключевые слова, встроить слова в изображение, или использовать несколько языков. Они также могут создать цепь прокси для того чтобы скрыть URL.

spamBlocker использует технологию Recurrent-Pattern Detection (RPD), созданную компанией Commtouch, для обнаружения этих типов атак. RPD – это инновационный метод поиска эпидемий спама в сети Интернет в режиме реального времени. RPD находит шаблоны эпидемии, не только шаблоны отдельных сообщений. Так как он не использует содержимое и заголовок письма, то он может идентифицировать эпидемию на любом языке, в любом формает или кодировке. Для того чтобы посмотреть анализ эпидемии спама в режиме реального времени зайдите на сайт Commtouch Outbreak Monitor:

http:// www.commtouch.com/Site/ResearchLab/map.asp.

spamBlocker также предоставляет пользователям опции обнаружения вирусных эпидемий. Для более подробной информации см. “Включение и настройка параметров для Virus Outbreak Detection (VOD)”

Вы можете посмотреть статистику по активности spamBlocker на Firebox, как описано в “Статистика по spamBlocker”

Требования к spamBlocker

Перед установкой spamBlocker вам необходимо иметь:

- Лицензионный ключ spamBlocker. Для того чтобы получить лицензионный ключ, обратитесь к реселлеру WatchGuard или зайдите на сайт WatchGuard LiveSecurity: http://www.watchguard.com/store.

- Сервер электронной почты POP3 или SMTP. spamBlocker работает с WatchGuard POP3 и Incoming SMTP прокси. Если вы не настроили POP3 или SMTP прокси, то они будут включены при настройке сервиса spamBlocker. Если у вас несколько политик прокси для POP3 или для SMTP, spamBlocker будет работать с ими всеми

- Настроенный DNS на Firebox, который будет применять правила spamBlocker. В Policy Manager выберите **Network > Configuration**. Выберите закладку **WINS/DNS и** введите IP-адреса DNS серверов для Firebox

- Подключение к сети Интернет

Действия, тэги и категории spamBlocker

Firebox использует действия spamBlocker для принятия решения по поводу доставки электронной почты. Когда сообщению присваивается определенная категория, применяется соответствующая опция.

При использовании spamBlocker с POP3 прокси поддерживаются не все опции.

Allow

Пропускает почту через Firebox.

Add subject tag

Пропускает электронное сообщение через Firebox и вставляет текст в поле Subject электронного сообщения метку (тэг). Вы можете использовать тэги по умолчанию, а можете создать свои тэги. Вы также можете создать правила в вашем почтовом клиенте для автоматической сортировки спама, как описано в “Создание правил в вашем почтовом клиенте”

Quarantine (SMTP only)

Отправляет электронное сообщение на Сервер Карантина. Необходимо отметить, что опция **Quarantine** поддерживается только тогда, когда вы используете spamBlocker с SMTP прокси. POP3 прокси не поддерживает эту опцию.

Deny (SMTP only)

Блокировка электронного сообщения. Firebox отправляет это 571 SMTP сообщение на сервер электронной почты, с которого пришло данное письмо: D*elivery not authorized, message refused*.

Опция **Deny** поддерживается только если вы используете spamBlocker с SMTP прокси. POP3 прокси не поддерживает эту опцию.

Drop (SMTP only)

Закрывает соединение. Firebox не отправляет на сервер источника никаких сообщений. Опция **Drop** поддерживается только если вы используете spamBlocker с SMTP прокси. POP3 прокси не поддерживает эту опцию.

Тэги spamBlocker

Firebox добавляет тэг в поле Subject электронного письма. Вы можете настроить добавляемые тэги. В этом примере показано поле Subject электронного письма, которое помечено как спам. По умолчанию добавляется тэг: ***SPAM***.

```
Subject: ***SPAM*** Free auto insurance quote
```

В этом примере показано использование произвольного тэга: [SPAM]

```
Subject: [SPAM] You’ve been approved!
```

Категории spamBlocker

Commtouch Recurrent-Pattern Detection (RPD) классифицирует спам атаки в своей базе данных Anti-Spam Detection Center в зависимости от уровня серьезности. spamBlocker формирует запрос в базу данных и каждому письму присваивает определенную категорию. spamBlocker содержит три категории:

Confirmed Spam – электронные сообщения от известных спамеров. Для такого типа электронной почты мы рекомендуем использовать действие **Deny** если вы используете spamBlocker с SMTP прокси, или **Add subject tag** если вы используете spamBlocker с POP3 прокси.

Bulk – электронные сообщения, которые не приходят от известных спаммеров, но совпадают с некоторыми шаблонами спама. Для этого типа электронной почты мы рекомендуем использовать действие **Add subject tag**, или действие **Quarantine** если вы используете spamBlocker с SMTP прокси.

Suspect – электронные сообщения, которые можно интепретировать как спам. Часто такие письма не являются спамом. Мы рекомендует интепретировать такие письма как "false positive". Для этого типа электронной почты мы рекомендуем использовать действие **Allow или действие Quarantine, если вы используете SMTP прокси**

Просмотр категории spamBlocker для сообщения

После того как spamBlocker присвоит сообщению определенную категорию, он добавляет категорию сообщения в его заголовок в качестве spam-результата.

Для того чтобы посмотреть spam результат для сообщения, откройте его заголовки.

Если у вас Microsoft Outlook откройте сообщение, выберите **View > Options** и откройте диалоговое окно **Internet headers**.

Spam результат отображается в этой строке:

```
X-WatchGuard-Spam_Score:
```

Например:

```
X-WatchGuard-Spam-Score: 3, bulk; 0, no virus
```

Первое число в этой строке – это категория спама. Это число принимает следующие значения:

0 - clean

1 - clean

2 - suspect

3 - bulk

4 - spam

Если в вашей конфигурации вы включите Virus Outbreak Detection (VOD), spam результат в заголовке сообщения будет содержат еще одну цифру, VOD категорию:

0 - no virus

1 - no virus

2 - virus threat possible

3 - virus threat high

Активация spamBlocker

You use a wizard to enable the spamBlocker feature in the SMTP proxy, the POP3 proxy, or both. You can also use this wizard to add a new SMTP proxy or POP3 proxy to your WatchGuard device configuration.

1. Убедитесь, что у вас есть все необходимое для работы со spamBlocker
2. Загрузите лицензионный ключ для spamBlocker на устройство WatchGuard
3. В WatchGuard System Manager выберите устройство WatchGuard, которое будет использовать spamBlocker.
4. Нажмите на иконку Policy Manager . Или выберите **Tools** > **Policy Manager**.
5. В Policy Manager выберите **Subscription Services** > **spamBlocker** > **Activate**.
   Запустится мастер Activate spamBlocker

6. Все необходимые инструкции мастера. Мастер содержит следующие страницы.

Apply spamBlocker settings to your policies

Эта страница откроется, если у вас уже есть несколько политик SMTP, но для них не включен spamBlocker. Выберете политики прокси, для которых вы хотите включить spamBlocker. Любые политики, для которых spamBlocker уже включен, будут затемнены.

Create new proxy policies

Эта страница откроется если на устройстве WatchGuard не создано ни одной политики SMTP или POP3, или создана только из этих политик. Мастер создаст одну или сразу две политики. Для этого Вам необходимо иметь по крайней мере один интерфейс External со статическим IP-адресом.

- Для того чтобы создать политику POP3 включите опцию **POP3**.
- Для того чтобы создать политику SMTP включите опцию **Incoming SMTP**. Введите IP адрес сервера электронной почты.
- Политика SMTP, созданная этим мастером, содержит “Any-External” для поля **From** и параметр статической NAT в поле **To**. Параметр статической NAT использует первый внешний статический IP-адрес, настроенный на устройстве Firebox. Он включает статическую NAT для IP-адреса сервера электронной почты, который вы ввели в мастере. Если эта созданная по умолчанию политика не удовлетворяет требованиям вашей организации, то вы можете при помощи Policy Manager создать свою политику SMTP.

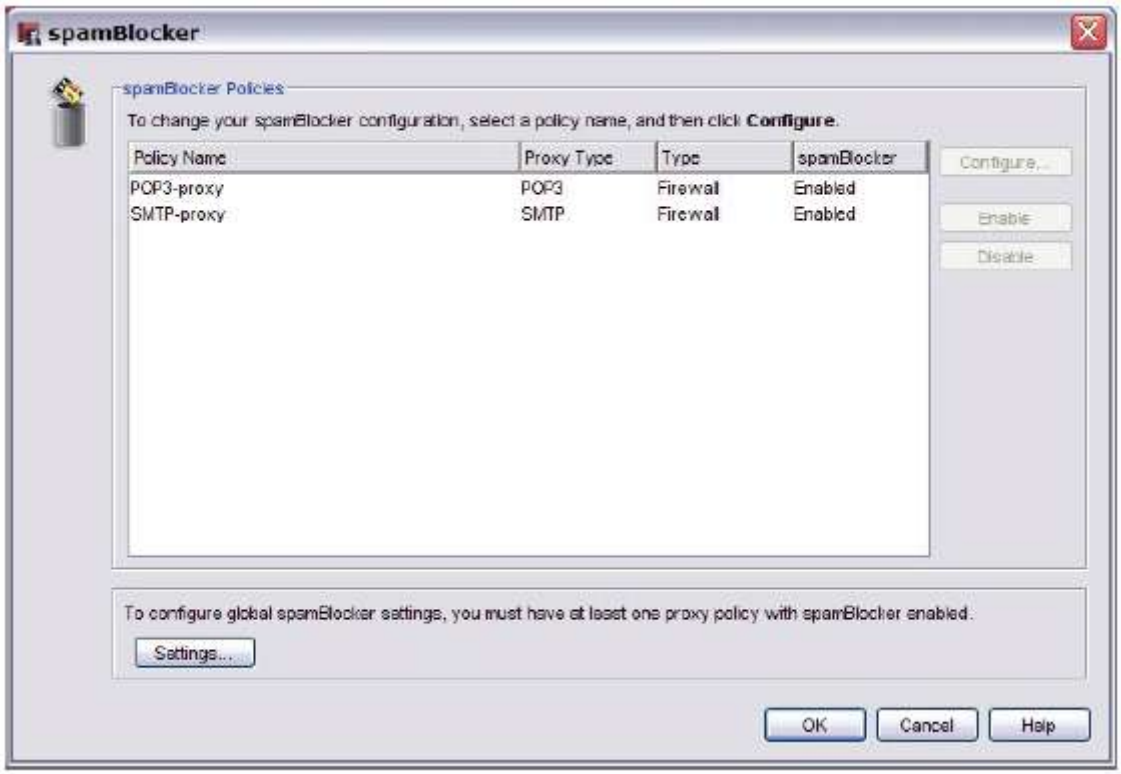
Для более подробной информации см. Add a policy from the list of templates.

После того, как вы закончите работу с мастером, вы можете выбрать флаг в нижней части экрана для того чтобы начать настройку spamBlocker.

Настройка spamBlocker

После того как вы при помощи мастера Activate spamBlocker активировали spamBlocker и создали базовую конфигурацию, вы можете настроить другие параметры spamBlocker.

1. В окне Policy Manager, выберите **Tasks > spamBlocker > Configure**. Откроется диалоговое окно spamBlocker со списком политик SMTP и POP3. В окне показывается доступность spamBlocker для каждой политики



2. Выберите политику, которую вы хотите настроить и нажмите **Configure**.
Откроется страница spamBlocker Configuration для этой политики

3. Включите опцию **Enable spamBlocker**.

4. Выберите действия, которые spamBlocker будет выполнять для каждой категории, в выпадающих списках рядом с **Confirmed spam**, **Bulk**, и **Suspect**. Если вы выберете **Add subject tag** для любой категории, вы измените тэг по умолчанию, который появляется в текстовом поле справа от выпадающего списка

5. Если вы хотите чтобы каждый раз при выполнении действия spamBlocker, генерировалось сообщение журнала включите опцию **Send log message**.

6. Диалоговое окно **When the spamBlocker server is unavailable, access to POP3/SMTP email is** определяет как Firebox будет обрабатывать входящую почту, когда сервер spamBlocker не работает. Мы рекомендуем использовать действие по умолчанию - **Allowed**.

   * Если вы настроите spamBlocker для блокировки POP3 или SMTP почты, когда он не может подключиться к серверу spamBlocker, то это приведет к конфликту с Microsoft Outlook. Когда Outlook открывает соединение с сервером электронной почты, spamBlocker пытается подключиться к серверу spamBlocker. Если сервер spamBlocker недоступен, spamBlocker останавливает загрузку почты. Когда это происходит, запускается цикл. Outlook пытается загрузить почту, а spamBlocker останавливает эту процедуру. Это продолжается до тех пор, пока Firebox не сможет подключиться к серверу spamBlocker, или запрос не будет отклонен по причине таймаута прокси, или пока вы не отмените запрос.

   * Если вы выберете значение этой опции равное **Denied** с SMTP прокси, то Firebox отправит сообщение 450 SMTP на сервер источника: Mailbox is temporarily unavailable.

7. Если вы включите опцию **Send log message for each email classified as not spam,** то если при проверке электронного письма, оно не было идентифицировано как спам, bulk или подозрительное, это записывается в журнал. Включите эту опцию если вы хотите записать это в журнал.

8. (Дополнительно) Добавьте правила исключений spamBlocker, как описано в “Исключения spamBlocker”

9. Настройте действия Virus Outbreak Detection, как описано в “Включение и настройка параметров для Virus Outbreak Detection (VOD)”

10. Нажмите **OK**.

Если у вас есть межсетевой экран по периметру между Firebox, который использует spamBlocker, и сетью Интернет, он не должен блокировать HTTP трафик. Протокол HTTP используется для отправки запросов с Firebox на сервер spamBlocker

Вы можете настроить глобальные параметры spamBlocker, которые применяются к spamBlocker в независимости от используемой прокси. Для более подробной информации см. “Настройка глобальных параметров spamBlocker”

Исключения spamBlocker

Вы можете создать список исключений для основных действий spamBlocker на базе адреса отправителя. Например, если вы хотите разрешить рассылку, которую spamBlocker идентифицирует как Bulk, вы можете добавить адрес этого отправителя в список исключений и использовать действие **Allow** в независимости от того, к какой категории принадлежит отправитель.

Или, если вы хотите применить тэг к отправителю, которого spamBlocker определил как безопасного, то вы можете добавить этого отправителя в список исключений.

Убедитесь, что вы добавили настоящий адрес отправителя, который указан в поле Mail-From. Для того чтобы получить реальный адрес для исключения, откройте полный заголовок электронного письма (в Microsoft Outlook выберите **View > Options** и посмотрите в секцию **Internet headers**). Адреса отправителя и получателя находятся в этих полях:

X-WatchGuard-Mail-From:

X-WatchGuard-Mail-Recipients:

Аккуратно используйте групповые символы в шаблоне. Спамеры могут перехватить информацию, которая содержится в заголовке.

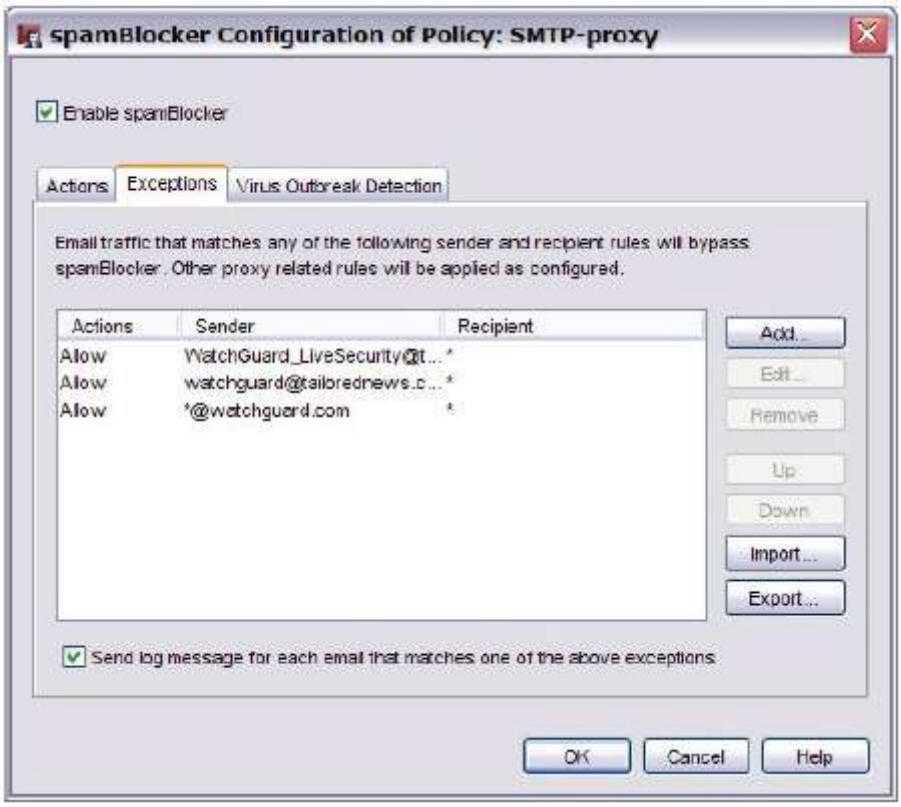
Чем специфичнее адреса в списке исключений, тем труднее их будет перехватить. Для того чтобы добавить правило исключения см. “Добавление правил исключений spamBlocker”. Для того чтобы изменить порядок следования правил в диалоговом окне см. “Изменение порядка следования исключений”. Вы также можете добавить, записав их в файл и затем импортировать этот файл на ваш Firebox. Для более подробной информации см. “Импорт и экспорт правил исключений spamBlocker”

Добавление правил исключений spamBlocker

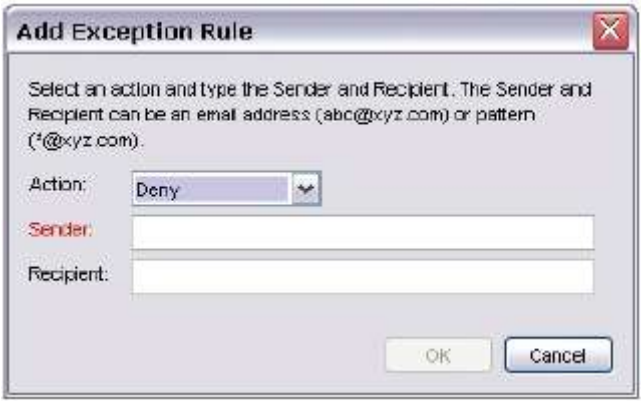
После того, как вы включите spamBlocker, вы можете создать исключения, которые разрешат получать почту от определенных отправителей, минуя spamBlocker.

1. В Policy Manager выберите **Subscription Services** > **spamBlocker** > **Configure**.

2. Выберите политику прокси и нажмите **Configure**. Выберите **Exceptions**



3. Нажмите **Add**. Выберите действие: **Allow**, **Add subject tag**, **Quarantine**, **Deny**, or **Drop**. (Помните, что POP3 прокси поддерживает только **Allow** и **Add subject tag**.)



4. Введите адрес отправителя или адрес получателя, или оба. Вы можете ввести полный электронный адрес или использовать групповые символы. Убедитесь, что вы добавили настоящий адрес отправителя, который указан в поле Mail-From. Для того чтобы получить реальный адрес для исключения, откройте полный заголовок электронного письма (в Microsoft Outlook выберите **View > Options** и посмотрите в секцию **Internet headers**). Адреса отправителя и получателя находятся в этих полях:

   X-WatchGuard-Mail-From:

   X-WatchGuard-Mail-Recipients:

   Аккуратно используйте групповые символы в шаблоне. Спамеры могут перехватить информацию, которая содержится в заголовке. Чем специфичнее адреса в списке исключений, тем труднее их будет перехватить.

5. Нажмите **OK**.
   Исключение будет добавлено в список исключений.

6. Если вы хотите чтобы каждое совпадении электронного сообщения с одним из исключений записывалось в журнал включите опцию **Send log message for each email that matches one of the above exceptions**. Исключения обрабатываются в том порядке, в котором они идут в списке. При помощи кнопок **Up** и **Down** вы можете изменить порядок следования исключений в списке

Изменение порядка следования исключений

Порядок, в котором правила исключений располагаются в списке, показывает в каком порядке электронные письма сравниваются с ними. Прокси сравнивает сообщение с первым правилом в списке и так далее вниз по списку. Если сообщение совпадает с правилом, Firebox выполняет соответствующее действие. Если сообщение совпадет с правилами ниже по списку, то Firebox не будет выполнять. Для того чтобы изменить порядок следования правил, выберите правило, которое вы хотите переместить, и при помощи кнопок **Up** или **Down** переместите его в необходимое место.

Импорт и экспорт правил исключений spamBlocker

Если у вас есть несколько Firebox или вы используете spamBlocker с несколькими прокси, вы можете импортировать или экспортировать правила исключений. Это позволяет вам сэкономить время, так как вам необходимо создать только одно правило. Вы можете перемещать правила между прокси или устройствами Firebox двумя способами.

Вы можете создать ASCII файл, который содержит правила, и импортировать его на остальные Firebox или прокси. Или вы можете использовать пользовательский интерфейс WebBlocker для создания правил исключений, экспортировать их в файл и затем импортировать этот файл на другой Firebox или прокси

Запись наборов правил в ASCII файл

Вы можете записать правила в обычный ASCII файл, который использует стандартную UTF-8 кодировку. В каждой строчке необходимо указать только одно правило.

Синтаксис: [action, <tag>,] sender [, recipient]

где:

action = Allow, Add subject tag <tag>, Quarantine, Deny или Drop. (Quarantine, Deny, и Drop не поддерживаются POP3 прокси)

По умолчанию используется действие Allow.

tag = Идентификатор, который вы хотите добавить к электронному письму. Идентификатор необходимо заключить в угловые скобки.

sender = Электронный адрес (abc@mywatchguard.com) или шаблон (*@firebox.net). По умолчанию используются все отправители.

recipient = Электронный адрес (abc@mywatchguard.com) или шаблон (*@firebox.net).

По умолчанию используются все получатели. Все поля, заключенные в скобки, являются дополнительными. Если вы их не введете, будут использоватья значения по умолчанию. Комментарии в файле начинаются с символа (#). Ниже приведен пример правила исключения spamBlocker:

```
# allow all email from firebox.net *@firebox.net
```

```
# use **SPAM** tag on all email from xyz.com Add subject tag, <**SPAM**>,
*@xyz.com

# deny all email from unknown.com to abc@mywatchguard.com Deny,
*@unknown.com,

abc@mywatchguard.com
```

Импорт файла исключений

1. В закладке **Exceptions** диалогового окна **spamBlocker Configuration** нажмите **Import**.

2. Найдите необходимый файл и нажмите **Open**.

Если такие исключения уже существуют, система попросит вас подтвердить – хотите ли вы заменить существующие исключения в spamBlocker или добавить эти. Выберите **Replace** или **Append**. Если вы нажмете **Append**, импортированные правила появятся в секции **Exceptions**. Если вы хотите порядок следования правил исключений см. “Изменение порядка следования исключений”

*Если вы хотите импортировать правило с исключением **Deny** в POP3 прокси, то произойдет ошибка.*

Экспорт правил в ASCII файл

Если вы экспортируете правила исключений из прокси, Firebox сохраняет текущие правила в текстовый ASCII файл в формате.

1. В закладке **Exceptions** диалогового окна **spamBlocker Configuration**, создайте необходимые исключения.

2. Нажмите **Export**.

В диалоговом окне **Open** выберите каталог, куда вы хотите сохранить исключения и нажмите **Save**. Теперь вы можете открыть другой SMTP или POP3 прокси в этом же или в другом конфигурационном файле и импортировать файл исключений.

Запись исключений в журнал

Включите опцию **Send log message for each email that matches one of the above exceptions** если вы хотите для каждого электронного письма, которое совпадает с правилом исключения генерировать сообщение журнала. Если вы импортируете правило с **Deny** исключением в POP3 прокси, вы увидите сообщение об ошибке

Настройка действий Virus Outbreak Detection для политики

Virus Outbreak Detection (VOD) - это технология, которая использует технологию анализа трафика для идентификации эпидемий вирусов в течение нескольких минут и предоставляет защиту против этих эпидемий. Разработанная компанией Commtouch технология VOD интегрирована в систему безопасности spamBlocker. Для того чтобы настроить действия Virus Outbreak Detection выполните следующее:

1. В Policy Manager выберите **Subscription Services** > **spamBlocker** > **Configure**.

2. Убедитесь, что Virus Outbreak Detection включен:

   * В диалоговом окне **spamBlocker** нажмите **Settings**.

   * В диалоговом окне **spamBlocker Settings** выберите закладку **General Settings**.

   * Включите опцию **Enable Virus Outbreak Detection (VOD).** Для более подробной информации см. “Enable and set parameters for Virus Outbreak Detection (VOD)” on page

1007.

* Нажмите **OK**.

3. В диалоговом окне **spamBlocker** выберите политику прокси и нажмите **Configure**. Выберите закладку **Virus Outbreak Detection**

4. В выпадающем списке **When a virus is detected** выберите действие, которое выполнит WatchGuard устройство если VOD обнаружит вирус в электронном письме

5. Из выпадающего списка **When a scan error occurs** выберите действие, которое выполнит Firebox в случае если VOD не может просканировать электронное письмо или вложение. Вложения, которые нельзя просканировать, содержат сообщения закодированные в двоичношестнадцатеричном виде, зашифрованные файлы или файлы, которые используют определенные алгоритмы сжатия, которые нами не поддерживаются (Zip файлы).

6. Включите опции **Log this action** для того чтобы записывать в журнал обнаружение вируса или ошибку при сканировании.

7. Включите опции **Alarm** для того чтобы создавать тревогу в случае обнаружения вируса или ошибки сканирования. SMTP прокси поддерживает действия **Allow**, **Lock**, **Remove**, **Quarantine**, **Drop** и **Block**. POP3 прокси поддерживает только действия **Allow**, **Lock** и **Remove**.

Для более подробной информации см. spamBlocker actions, tags, and categories.

Настройка spamBlocker для карантина почты

Сервер Карантина WatchGuard предоставляет безопасный механизм карантина для электронных писем, идентифицированных как спам, или которые содержат вирусы. Этот репозитарий получает электронные письма от SMTP прокси, которые фильтруются spamBlocker.

Для того чтобы настроить карантин для spamBlocker выполните следующее:

1. Когда вы запустите мастер Activate spamBlocker Wizard , вам необходимо убедиться, что вы используете spamBlocker с SMTP прокси. POP3 прокси не поддерживает Сервер Карантина.

2. При выборе действий, которые spamBlocker применяет для различных категорий электронной почты, убедитесь, что вы выбрали действие **Quarantine** хотя бы для одной категории.

Если вы выберете это действие вам необходимо настроить Сервер Карантина. Вы также можете выбрать действие **Quarantine** для электронных писем, которые были идентифицированы Virus Outbreak Detection как вирусы

Использование spamBlocker с несколькими прокси

Вы можете настроить несколько SMTP или POP3 прокси для работы со spamBlocker. Это позволит вам создать свои правила для различных групп внутри организации. Например, вы можете разрешить всю почту для вашей администрации и использовать тэги спама для отдела маркетинга. Если вы хотите использовать более одного сервиса прокси со spamBlocker, ваша сеть должна использовать одну из этих конфигураций:

- Каждая политика прокси должна отправлять почту на различные внутренние серверы электронной почты.

  Или

- Вам необходимо использовать внешний источник или источники, которые могут оптравлять почту для каждой политики прокси

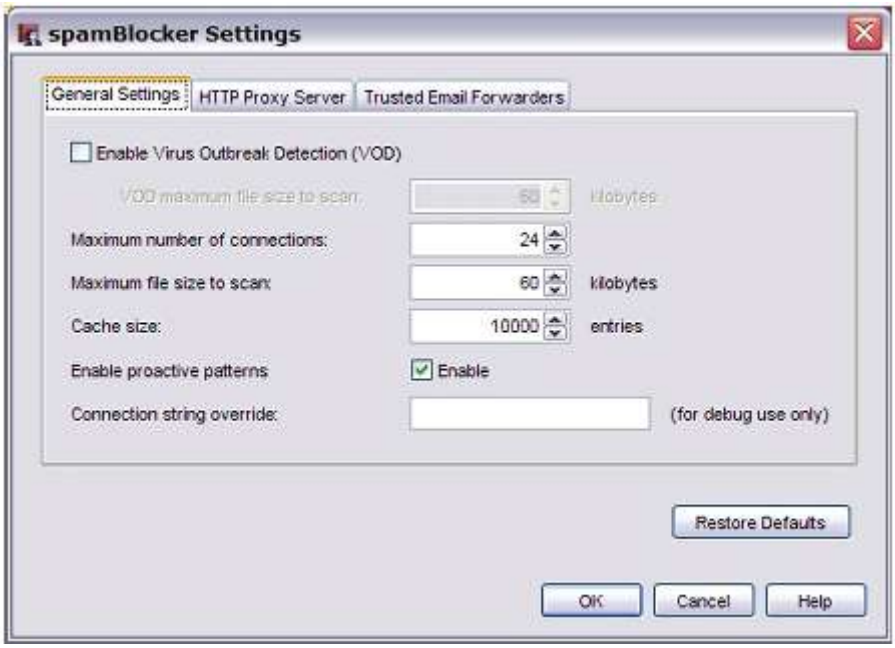
Настройка глобальных параметров spamBlocker

Для настройки глобальных параметров spamBlocker вам необходимо включить spamBlocker хотя бы для одной политики прокси.

Вы можете использовать глобальные параметры spamBlocker для оптимизации его работы. Так как большинство этих параметров используют определенное количество памяти, вам необходимо сбалансировать производительность spamBlocker с требованиями к функционалу Firebox.

1. В Policy Manager выберите **Subscription Services** > **spamBlocker** > **Configure**.

2. Нажмите **Settings**.
   Откроется диалоговое окно spamBlocker Settings



3. spamBlocker создает подключение для каждого обрабатываемого сообщения. Это подключение включает информацию о сообщение, которое используется для генерации его spam результата. spamBlocker устанавливает максимальное количество подключений, которые могут одновременно помещены в буфер, в зависимости от модели вашего встроенного ПО. В поле **Maximum number of connections** вы можете указать максимальное количество подключений. Если количество трафика, обрабатываемого вашими политиками прокси низкое, вы можете увеличить количество подключений без снижения производительности. Если у вас возникают проблемы с выделением памяти для ваших прокси вы можете уменьшить количество подключений.

4. В поле **Maximum file size to scan** выберите количество байт электронного письма, которое будет просканировано spamBlocker. Для корректного обнаружения спама значения 20–40K будет вполне достаточно. Однако если спам в виде изображений является проблемой для вашей компании, вы можете увеличить это значение для блокировки спама в виде изображений

5. В поле **Cache size** введите количество кэшируемых записей для сообщений, которые были идентифицированы как спам или bulk. Локальный кэш может увеличить производительность, так как нет необходимости отправлять трафик Commtouch. Обычно вам нет необходимости изменять это значение. Вы можете установить значение этого поля равным нулю для того чтобы вся почта, отправлялась в Commtouch. Обычно это используется для решения проблем.

6. Отключите опцию **Enabled** рядом с **Proactive Patterns** если вы хотите отключить Commtouch CT Engine Proactive Patterns. Этот компонент автоматически включается на e-Series и Firebox X Peak. Для работы этого компонента при обновлении локальной базы данных требуется большое количество свободного дискового пространства. Если у вас проблемы с памятью или скоростью процессора, отключите этот компонент.

7. Поле **Connection string override** используется только тогда, когда вам необходимо решить проблемы, возникающие в работе spamBlocker. Не изменяйте это значение, только если вас не попросят об этом представители службы технической поддержки.

8. (Дополнительно) Для настройки дополнительных параметров вы можете использовать закладки диалогового окна **spamBlocker Settings**:

   * Use an HTTP proxy server for spamBlocker

* Use trusted email forwarders to improve spam score accuracy

* Enable and set parameters for Virus Outbreak Detection (VOD)

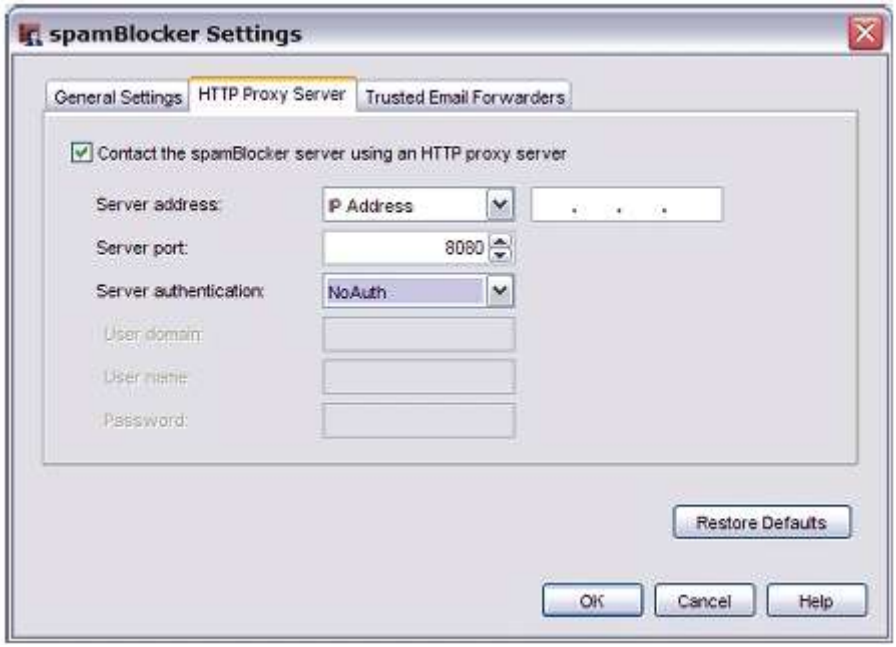
9. Нажмите **OK**. Если вы хотите восстановить параметры spamBlocker по умолчанию, нажмите **Restore Defaults**.

Использование HTTP прокси сервера для spamBlocker

Если для подключения к серверу CommTouch через Интернет сервису spamBlocker необходим HTTP прокси сервер, вам необходимо в диалоговом окне **spamBlocker Settings** настроить параметры HTTP прокси сервера.

1. В диалоговом окне spamBlocker нажмите **Settings**.

2. Выберите закладку **HTTP Proxy Server**

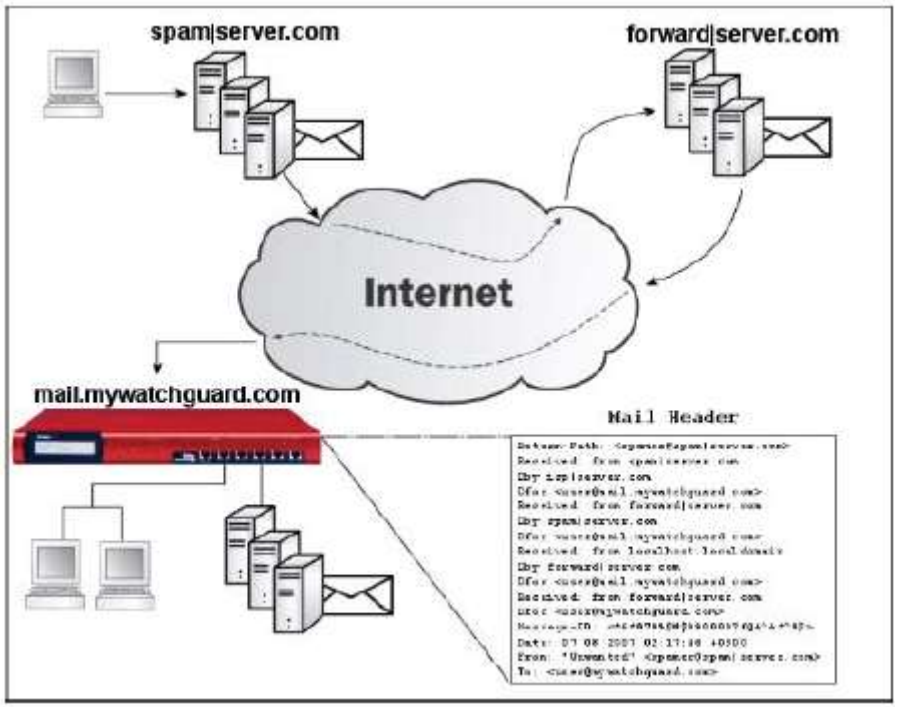


3. В закладке **HTTP Proxy Server** включите опцию **Contact the spamBlocker using an HTTP Proxy server**.

4. Выполните настройку остальных параметров прокси сервера, включая адрес прокси сервера, порт, через который устройство WatchGuard подключается к прокси серверу и данные аутентификации, которые используются устройством WatchGuard для подключения к прокси серверу (если аутентификация необходима на прокси сервере)

Создание доверенных серверов-ретрансляторов электронной почты для повышения точности spam результат

Часть spam результата для электронного сообщения считается с использованием IP адреса, откуда это сообщение было получено. Если используется пересылка почты, то для подсчета spam результата используется IP адрес сервера пересылки. Так как сервер пересылки не является источником электронной почты, расчет spam результат может быть неточным.



Для того чтобы улучшить подсчет spam результата, вы можете ввести несколько имен хостов или доменных имен серверов электронной почты, которым доверяете пересылку почты на ваш почтовый сервер. Если вы используете SMTP введите одно или несколько имен хостов или доменов SMTP серверов, которым вы доверяете пересылку почты на ваш сервер. Если вы используете POP3 введите имена доменов известных или наиболее часто используемых POP3 провайдеров, которым вы доверяете, для загрузки электронной почты. После того, как вы добавите один или несколько серверов переадресации почты, spamBlocker будет игнорировать сервер переадресации в заголовках электронных сообщений. Spam результат расчитывается при помощи IP-адрес исходного сервера электронной почты.

1. В диалоговом окне **spamBlocker Settings** выберите закладку **Trusted Email Forwarders**.
2. Введите имя хоста или домена в текстовом поле в нижней части диалогового окна и нажмите **Add**. Если вы хотите добавить имя домена, то не забудьте в начале имени поставить точку, например .firebox.net.
3. (Дополнительно) Повторите п. 2 для того чтобы добавить еще серверов переадресации.
4. Нажмите **OK**.

Включение и настройка параметров для Virus Outbreak Detection (VOD)

Virus Outbreak Detection (VOD) - это технология, которая использует технологию анализа трафика для идентификации эпидемий вирусов в течение нескольких минут и предоставляет защиту против этих эпидемий. Разработанная компанией Commtouch, признанным мировым лидером в области спама и защиты от вирусов, технология VOD ловит вирусы быстрее, чем системы на базе сигнатур.

Для того чтобы включить и настроить VOD выполните следующее:

1. В диалоговом окне **spamBlocker Settings** выберите закладку **General Settings**
2. Включите опцию **Enable Virus Outbreak Detection (VOD)**.
3. По умолчанию, VOD сканирует входящие электронные письма размером вплоть до максимального оптимального размера для устройства Firebox. Вы можете изменить этот лимит при помощи стрелок рядом с полем **VOD maximum file size to scan**

Для более подробной информации о максимальном размере и размере по умолчанию для сканирования для различных моделей WatchGuard см. “About spamBlocker and VOD scan limits” on page 1007.

Если глобальное значение spamBlocker поля **Maximum file size to scan** настроено в диалоговом окне spamBlocker Settings больше чем значение **VOD maximum file size to scan**, VOD будет использовать глобальное значение spamBlocker.

В прокси для spamBlocker вы можете настроить действия, которые будет выполнять spamBlocker при обнаружении вируса, как описано в “Включение и настройка параметров для Virus Outbreak Detection (VOD)”

Ограничения на сканирование spamBlocker и VOD

spamBlocker сканирует каждый файл до определенного количество килобайт. Любые дополнительные байты файла не сканируются. Это позволяет прокси сканировать большие файлы по частям без влияния на скорость работы системы. Максимальный размер и размер по умолчанию могут быть разными для разных моделей WatchGuard.

Максимальные размеры сканирования для различных моделей устройств WatchGuard (в килобайтах)

Для более подробной информации о настройке максимального размер файла для сканирования spamBlocker и VOD см. “Настройка глобальных параметров spamBlocker” и “Включение и настройка параметров для Virus Outbreak Detection (VOD)”

Модель	Минимально	Максимально	По умолчанию
Firebox X Edge e-Series: X10e, X20e, X55e, X10e-W, X20e-W, X55e-W	1	40	40
Firebox X Core e-Series: X550e, X750e, X750e-4, X1250e, X1250e-4	1	2000	60
Firebox X Peak e-Series: X5500e, X6500e, X8500e, X8500e-F	1	2000	100
WatchGuard XTM1050	1	2000	100

Подключения spamBlocker

Для каждого обрабатываемого сообщения spamBlocker создает подключение. Это соединение содержит информацию с ооообщение, которое используется для подсчета spam результата. spamBlocker устанавливает максимальное количество соединение, которые могут одновременно буферизованы в соответствие с моделью вашего WatchGuard устройства.

Максимальное количество подключений в зависимости от модели устройства WatchGuard

Модель	Минимально	Максимально	По умолчанию
Firebox X Edge e-Series: X10e, X20e, X55e, X10e-W, X20e-W, X55e-W	4	4	4
Firebox X Core e-Series: X550e	4	16	16
Firebox X Core e-Series: X750e, X750e-4, X1250e, X1250e-4	4	24	24
Firebox X Peak e-Series: X5500e, X6500e, X8500e, X8500e-F	4	80	32
WatchGuard XTM1050	4	80	32

Для более подробной информации о настройке максимального размера файла для сканирования spamBlocker и VOD, см. “Настройка глобальных параметров spamBlocker”

Создание правил в вашем почтовом клиенте

Для того чтобы использовать действие **Tag** в spamBlocker вам необходимо настроить ваш почтовый клиент для сортировки сообщений. Большинство почтовых клиентов, таких как Outlook, Thunderbird и Mac Mail, позволяют вам настроить правила для автоматической отправки сообщений с тэгами в подкаталоги. Некоторые почтовые клиенты позволяют вам создать правило для автоматического удаления сообщений. Так как вы можете использовать различные теги для каждой категории spamBlocker, вы можете для каждой категории настроить различные правила. Например, вы можете настроить одно правило для перемещения электронных сообщений с тэгами ***BULK*** в подкаталог Bulk, и другое правило для удаления всех сообщений с тэгом ***SPAM***

Если вы используете spamBlocker с SMTP прокси, то вы можете отправлять ваши электронные письма на Сервер Карантина

Отправка спама и bulk в специальные каталоги в Outlook

Эта процедура описывает этапы создания правила для bulk и подозрительной почты в Microsoft Outlook. Вы можете помещать электронную почту, помеченную тэгом “spam” или “bulk”, в специальные каталоги Outlook. Когда вы создаете такие каталоги, вы можете хранить спам в отдельных каталогах и при необходимости получать доступ к ним.

Если вы используете другого почтового клиента, см. документацию по этому продукту.

Перед тем как начать, убедитесь, что вы создали действия для спама или bulk-сообщений в **Add Subject Tag**. Вы можете использовать тэги по умолчанию или создать свои тэги. Ниже приводится описание процедуры создания каталогов с тэгами по умолчанию.

1. В вашем Outlook Inbox выберите **Tools** > **Rules and Alerts**.
2. Нажмите **New Rule.** Запустится мастер **Rules**.
3. Выберите **Start from a blank rule**.
4. Выберите **Check messages when they arrive**. Нажмите **Next**.
5. Включите опцию условия: **when specific words in the subject**. Затем в нижней панели, отредактируйте описание правила.
6. В диалоговом окне **Search Text** , введите тэг *****SPAM*****. Если вы хотите использовать свой тэг, то введите его здесь.
7. Нажмите **Add**. Нажмите **OK**.
8. Нажмите **Next**
9. Мастер спросит вас о том, что делать с сообщением. Выберите опцию **move it to the specified folder.** Затем в нижней панели нажмите **specified** для того чтобы выбрать каталог для сохранения.
10. В диалоговом окне **Choose a Folder** нажмите **New**.
11. В поле имени каталога, введите **Spam**. Нажмите **OK**.
12. Нажмите **Next** два раза.
13. Для того чтобы завершить настройку правила, введите имя для вашего правила. Нажмите **Finish**.
14. Нажмите **Apply**.

Повторите эту процедуру для создания правила для bulk-сообщений, при помощи тэга bulk. Вы можете помещать bulk-сообщения в этот же каталог, или создать новый каталог.

Отправка отчета о «false positive» или «false negatives»

«false positive» сообщение – это легитимное сообщение, которое spamBlocker неправильно идентифицировал как спам. «false negative» сообщение – это спам, который spamBlocker некорректно идентифицировал как спам. Если вы обнаружите «false positive» или «false negative» сообщение, то вы можете отправить отчет прямо компании Commtouch. Вы также можете отправить отчет о «false positive» для писем, входящих в полезные массовые рассылки. Это сообщение, которое spamBlocker идентифицировал как bulk почту, в то время как пользователь запрашивал электронное сообщение

Не отправляйте отчет о «false positive», когда электронному сообщению была присвоена категория Suspect. Так как эта категория не является постоянной, Commtouch не рассматривает отчеты для сообщений из категории Suspected.

Для того чтобы отправить отчет компании Commtouch вам необходим доступ к электронному сообщению. Вам также необходимо знать категорию (Confirmed Spam, Bulk), которую присвоил ему spamBlocker. Если вы не знаете категорию см. раздел "Find the category a message is assigned to" далее в этой главе.

1. Сохраните ваше сообщение в .msg или .eml. Вы не можете переслать исходное сообщение, так как компании Commtouch необходим заголовок сообщения. Если вы используете почтовые клиенты Microsoft Outlook или Mozilla Thunderbird, вы можете перетащить электронное сообщение на ваш рабочий стол. В противном случае вам

необходимо выбрать **File > Save As** для того чтобы сохранить сообщение в указанном каталоге.

2. Создайте новое сообщение, адресованное:

   reportfp@blockspam.biz для false positives

   reportfn@blockspam.biz для false negatives

   reportso@blockspam.biz для false positive solicited bulk почты

3. В поле Subject введите следующее:

   `FP Report` <Название_вашей_компании> <Дата_отправки> для false positives

   `FN Report` <Название_вашей_компании> <Дата_отправки> для false negatives

   `FP Report` <Название_вашей_компании> <Дата_отправки> для false positive solicited bulk email

4. Приложите файл .msg или .eml к сообщению и отправьте его.

Если вы хотите отправить несколько сообщений, то вы можете отправить их в одном Zip файле. Не помещайте Zip файл в другой Zip архив. Zip файл может быть сжат только на один уровень для автоматического анализа его компанией Commtouch.

Использование RefID записи вместо текста сообщения

Если вы хотите отправить отчет компании Commtouch, но не можете отправить исходное сообщение, так как информация в этом сообщении является конфиденциальной, то вы можете вместо заголовка сообщения использовать RefID запись. RefID запись – это номер транзакции между Firebox и Commtouch Detection Center. spamBlocker добавляет X-WatchGuard-Spam-ID заголовок к каждому сообщению. Этот заголовок выглядит следующим образом:

X-WatchGuard-Spam-ID: 0001.0A090202.43674BDF.0005-G-gg8BuArWNRyK9/VKO3E51A==

Длительная последовательность цифр и букв после `X-WatchGuard-Spam-ID:` - это RefID запись. Вместо прикрепления исходного сообщения, скопируйте RefID в тело сообщения. Если у вас есть несколько сообщений, отчет о которых вы хотите отправить, то в каждую строку тела сообщения поместите RefID для каждого сообщения.

Для того чтобы посмотреть заголовки электронного сообщения в Microsoft Outlook выполните следующее:

1. Откройте электронное сообщение в новом окне или выберите его в Outlook.

2. Если вы открыли сообщение в отдельном окне, то выберите **View > Options**. Если вы выделили сообщение в Outlook нажмите правой кнопкой на него и нажмите **Options**. Заголовки сообщения вы можете посмотреть в нижней части окна Message Options.

Для того чтобы посмотреть заголовки электронного сообщения в Microsoft Outlook Express выполните следующее:

1. Откройте электронное сообщение в новом окне или выберите его в Outlook Express.

2. Если вы открыли сообщение в отдельном окне, то выберите **File > Properties**. Если вы выделили сообщение в Outlook Express нажмите правой кнопкой на него и нажмите **Properties**.

3. Выберите закладку **Details** для того чтобы посмотреть заголовки сообщения

Для того чтобы посмотреть заголовки электронного сообщения в Mozilla Thunderbird выполните следующее:

1. Откройте электронное сообщение в новом окне.

2. Выберите **View** > **Headers** > **All**.

Поиск категории, присвоенной сообщению

Тэги сообщения – это единственный способ определения категории, присвоенной сообщению. Измените действие на **Add subject tag** и используйте уникальную последовательность символов, которая будет добавляться в поле Subject электронного письма. Для более подробной информации об использовании тэгов spamBlocker.

Глава 32 - Gateway AntiVirus и IPS (Intrusion Prevention Service)

Gateway AntiVirus и Intrusion Prevention

Хакеры используют достаточно большое количество способов для атаки компьютеров, подключенных к сети Интернет. Существует две основные категории атак: вирусы и проникновения.

Вирусы, включая червей и троянов, это небольшие программы, которые создают копии себя и помещают их в исполняемый код или документы на вашем компьютере. Вирус, который попал на компьютер, может нанести серьезный вред вашему компьютеру, например удалить важные файлы.

Проникновения – это прямые атаки на ваш компьютер. Обычно эти атаки используют какие-либо уязвимости в ПО, установленном на вашем компьютере. Эти атаки предназначены для нанесения вреда вашей сети, получения важной информации, а также использования одних компьютеров для атаки других компьютеров или сетей.

Для того чтобы защитить свою сеть от таких атак вы можете приобрести сервис Gateway AntiVirus/Intrusion Prevention Service (Gateway AV/IPS) для вашего WatchGuard устройства.

IPS и Gateway AntiVirus работают с SMTP, POP3, HTTP, FTP и TCP-UDP прокси. При обнаружении новой атаки, ее уникальные параметры, по которым ее можно идентифицировать, записываются в специальных записей, называемых сигнатурами. Gateway AV/IPS использует эти сигнатуры для поиска вирусов и попыток проникновения в вашу сеть во время сканирования входящего трафика каким-либо прокси. Если вы включите Gateway AV/IPS для прокси, он будет сканировать типы содержимого этого прокси.

На устройствах Firebox X Edge e-Series Gateway AV/IPS не сканирует следующие типы содержимого для HTTP прокси: text/, image/*, audio/*, and video/*. Gateway AV не сканирует эти типы содержимого для увеличения скорости работы системы. На устройствах Edge эти типы содержимого не сканируются даже в том случае, если они присутствуют в списке Content Types в настройках политики HTTP прокси.*

Gateway AV/IPS может сканировать следующие типы файлов: .zip, .gzip, .tar, .jar, .rar, .chm, .lha, .pdf, XML/HTML контейнер, OLE контейнер (Microsoft Office документы), MIME (в основном электронные письма в формате EML), .cab, .arj, .ace, .bz2 (Bzip), .swf (flash; ограниченная поддержка).

WatchGuard не гарантирует, что Gateway AV/IPS сможет обнаружить все известные вирусы и заблокировать все попытки проникновения в сеть.

Для того чтобы использовать эти сервисы вам необходимо приобрести обновление Gateway AV/IPS. Для более подробной информации зайдите на сайт WatchGuard LiveSecurity: http://www.watchguard.com/store

Или свяжитесь с вашим дистрибьютором WatchGuard. В любое время вы можете посмотреть статистику Gateway AntiVirus и Intrusion Prevention Service на устройстве WatchGuard

Установка и обновление Gateway AV/IPS

Для того чтобы установить Gateway AntiVirus или Intrusion Prevention Service, вам необходимо получить лицензионный ключ от LiveSecurity Service и добавить его на Firebox. Новые вирусы и методы проникновения появляются в Интернете довольно часто. Для того чтобы обеспечить надежную защиту GAV/IPS, вам необходимо часто обновлять сигнатуры. Вы можете настроить

Firebox для автоматического обновления сигнатур. Вы также можете обновлять сигнатуры вручную.

Для более подробной информации см. “Configure the Gateway AV/IPS update server” on page 1025 и “See subscription services status and update signatures manually” on page 1026.

Gateway AntiVirus/Intrusion Prevention и политики прокси

Gateway AV может работать с SMTP, POP3, HTTP, FTP и TCP-UDP прокси. IPS может работать с этими прокси плюс к DNS прокси. Когда вы включите Gateway AV или Intrusion Prevention, эти прокси будут проверять различные типы трафика и выполнять заданные вам действия, например сброс соединения или блокировка пакета и добавление его источника в список Blocked Sites.

Gateway AV и IPS сканируют различные типы трафика в зависимости от того, какие прокси вы используете:

- SMTP или POP3 прокси: Gateway AV/IPS ищет вирусы и проникновения, закодированные с помощью популярных методов вложений. Вы также можете использовать Gateway AV и SMTP прокси для отправки зараженной почты на Сервер Карантина

- HTTP прокси: Gateway AV/IPS ищет вирусы и проникновения на web страницах, которые загружаются пользователями.

- TCP-UDP прокси: Этот прокси сканирует трафик на динамических портах. Этот прокси распознает трафик для различных типов прокси, включая HTTP и FTP. TCP-UDP прокси затем отправляет трафик соответствующей прокси для сканирования на наличие вирусов или проникновений. Вы можете использовать TCP-UDP прокси для блокировки Instant Messaging (IM) или Peer to Peer (P2P) сервисов

- FTP прокси: Gateway AV/IPS ищет вирусы и проникновения и загружаемых или выгружаемых файлов

- DNS прокси: Gateway AV/IPS ищет вирусы и проникновения в DNS пакетах.

Каждый прокси, который использует Gateway AV/IPS, имеет опции характерные только для этого прокси. Например, список элементов, которые вы можете просканировать отличаются для разных прокси.

Для всех прокси вы можете ограничить размер сканируемых данных до определенного количества килобайт. Максимальные размеры сканируемых данных и размер по умолчанию отличаются для различных моделей устройства WatchGuard. Firebox сканирует в файле определенное количество килобайт. Это позволяет пропускать лишь частично просканированные файлы.

Для того чтобы всегда иметь самую последнюю версию сигнатур вы можете включить автоматическое обновление для сервера Gateway AV

Активация Gateway AntiVirus

Существует два способа активации Gateway AntiVirus:

- Activate Gateway AntiVirus with a wizard from Policy Manager

- Activate Gateway AntiVirus wizard from proxy definitions

При использовании мастера Activate Gateway AntiVirus вы можете создавать прокси за один шаг и включать Gateway AntiVirus одновременно для нескольких прокси. Если вы планируете использовать Gateway AntiVirus для нескольких прокси, то рекомендуем для экономии времени использовать мастер

Активация Gateway AntiVirus при помощи мастера

1. В окне WatchGuard System Manager, выберите Watchguard устройство, на котором вы хотите использовать Gateway AntiVirus.

2. Нажмите . Или выберите **Tools** > **Policy Manager**.

3. В Policy Manager выберите **Subscription Services** > **Gateway AntiVirus** > **Activate**. *Откроется мастер Activate Gateway AntiVirus*

4. Нажмите **Next**.

5. Выполните все необходимые инструкции мастера. Мастер отображает страницы в зависимости, есть ли в вашей конфигурации политики прокси. Например, если в вашей конфигурации нет политик прокси, мастер поможет вам создать ее. Затем вы можете снова запустить мастер для настройки GAV или вы можете посмотреть инструкции в следующих секциях. Мастер содержит следующие страницы.

Применение настроек Gateway AntiVirus к вашим политикам

На этой странице содержится список политик прокси, которые уже созданы на вашем Firebox. Из списка выберите политики прокси, для которых вы хотите включить Gateway AntiVirus. Политики Any, для которых Gateway AntiVirus уже включен, затенены.

Вы также можете в настройках прокси автоматически включить Gateway AntiVirus для SMTP, POP3, HTTP, FTP или TCP прокси

Создание новых политик прокси

Эта страница открывается, если у вас еще нету политик для SMTP или HTTP.

Для того чтобы создать политику, отметьте соответствующую опцию. Если вы выбрали SMTP, то введите IP-адрес сервера электронной почты. Этот мастер по умолчанию создает политику SMTP, которая является политикой статической NAT. Для того чтобы создать эту политику SMTP, у вас должен по крайней мере один интерфейс External со статическим IP-адресо или PPPoE. Если у вас несколько интерфейсов, то создается только одна политика.

Поле **To** политик содержит параметр статической NAT (статический IP-адрес первого интерфейса External к опредленному IP-адресу почтового сервиса). Если эта политика не удовлетворяет вашим требованиям, вы можете перед тем как запустить мастер создать свою политику SMTP.

Активация Gateway AntiVirus из настроек прокси

Вы можете активировать Gateway AntiVirus из настроек прокси. Для этого выполните следующее.

1. Добавьте SMTP, POP3, HTTP, FTP или TCP-UDP прокси, который вы хотите использовать с Gateway AntiVirus

2. Два раза нажмите на политику в Policy Manager.
   Откроется диалоговое окно Edit Policy Properties.

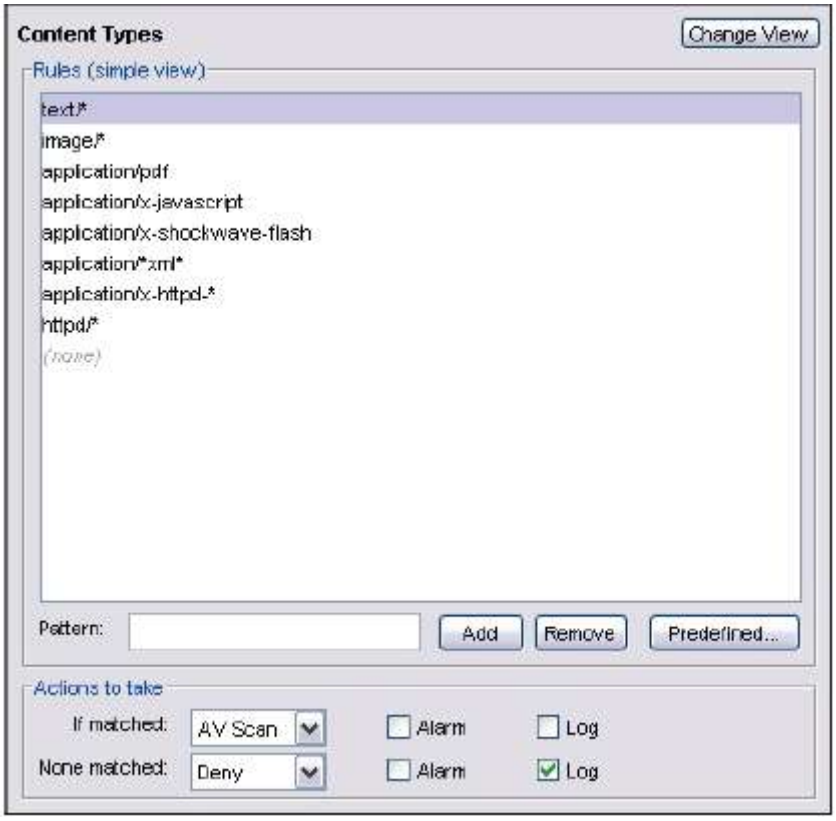
3. Выберите закладку **Properties**.

4. Нажмите на иконку **View/Edit Proxy**  (иконка справа от выпадающего списка **Proxy action**).

5. Gateway AV может сканировать трафик, который соответствует правилам нескольких категорий каждого прокси. Например для SMTP и POP3 прокси сервис Gateway AV может сканировать трафик, который совпадает с правилами категорий **Content Types** и **File Names**. В списке **Categories** в левой части окна **Proxy Action Configuration** нажмите на одну из категорий.

FTP прокси	SMTP прокси	POP3 прокси	HTTP прокси	TCP-UDP прокси (HTTP/SMTP трафик на динамических портах)
Download	Content-Types	Content-Types	Requests: URL Paths	Requests: URL Paths
Upload	File Names	File Names	Response: Content Types, Body Content Types	Response: Content Types, Body Content Types

6. В выпадающих списках **If matched** или **None matched** выберите **AV Scan.** При этом сервис Gateway будет сканировать трафик, который соответствует или не соответствует правилам указанных категорий



7. Нажмите **OK**. Gateway AntiVirus будет автоматически активирован и включен для соответствующего прокси. Если вы хотите включить Gateway AntiVirus для других прокси, то вам необходимо повторить эту процедуру для этих прокси.

На устройствах Firebox X Edge e-Series Gateway AV/IPS не сканирует следующие типы содержимого для HTTP прокси: text/, image/*, audio/*, and video/*. Gateway AV не сканирует эти типы содержимого для увеличения скорости работы системы. На устройствах Edge эти типы содержимого не сканируются даже в том случае, если они присутствуют в списке Content Types в настройках политики HTTP прокси.*

Настройка действий Gateway AntiVirus

Когда вы включите Gateway AntiVirus, вам необходимо настроить действия, которые будут выполняться в случае обнаружения вирусов и ошибки в электронном сообщении (SMTP или POP3 прокси), web страница (HTTP прокси), или выгружаемые/загружаемые файлы (FTP прокси).

Вы можете выбрать следующие действия:

Allow

Разрешить передачу пакета получателю, даже если он содержит вирус.

Deny (только для FTP прокси)

Заблокировать передачу файла и отправить deny сообщение.

Lock (SMTP and POP3 proxies only)

Блокировать вложение. Эта опция лучше использовать когда размер вложения слишком большой для Gateway AntiVirus или когда Firebox не может его просканировать. Пользователь не может открыть заблокированный файл. Разблокировать файл может только администратор.

Администратор при помощи другого антивирусного ПО может просканировать файл и проверить содержимое вложения. Для более подробной информации о том, как разблокировать заблокированный файл см. “Разблокировка файла, заблокированного Gateway AntiVirus”

Quarantine (SMTP proxy only)

Если вы используете SMTP прокси со spamBlocker, вы можете отправлять электронные сообщения, содержащие вирусы, или возможные вирусы на Сервер Карантина. Для более подробной информации о Сервере Карантина см. “Сервер Карантина”. Для более подробной информации о настройке Gateway AntiVirus для работы с Сервером Карантина см. “Настройка Gateway AntiVirus для карантина почты”

Remove (только для SMTP и POP3 прокси)

Удаляет вложения и отправляет сообщение получателю.

Drop (не поддерживается в POP3 прокси)

Отбрасывает пакет и разрывает соединение. Источнику сообщения не получает никакого уведомления.

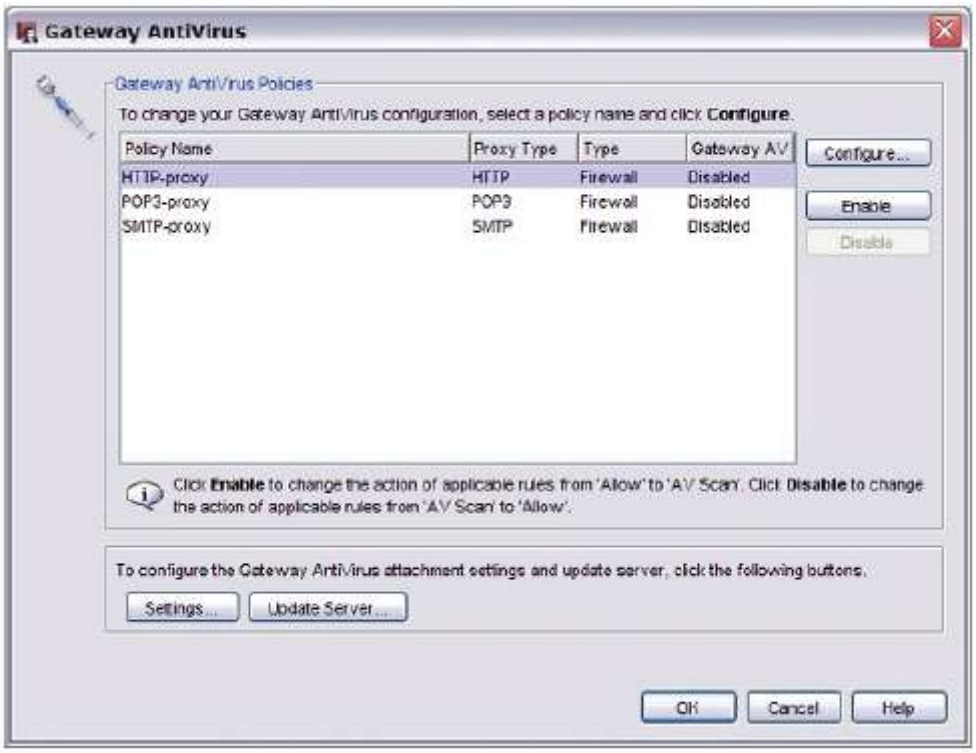
Block (не поддерживается в POP3 прокси)

Блокирует пакет и добавляет IP адрес отправителя в список Blocked Sites.

Если вы разрешите передавать вложения, это значительно снизит уровень вашей безопасности.

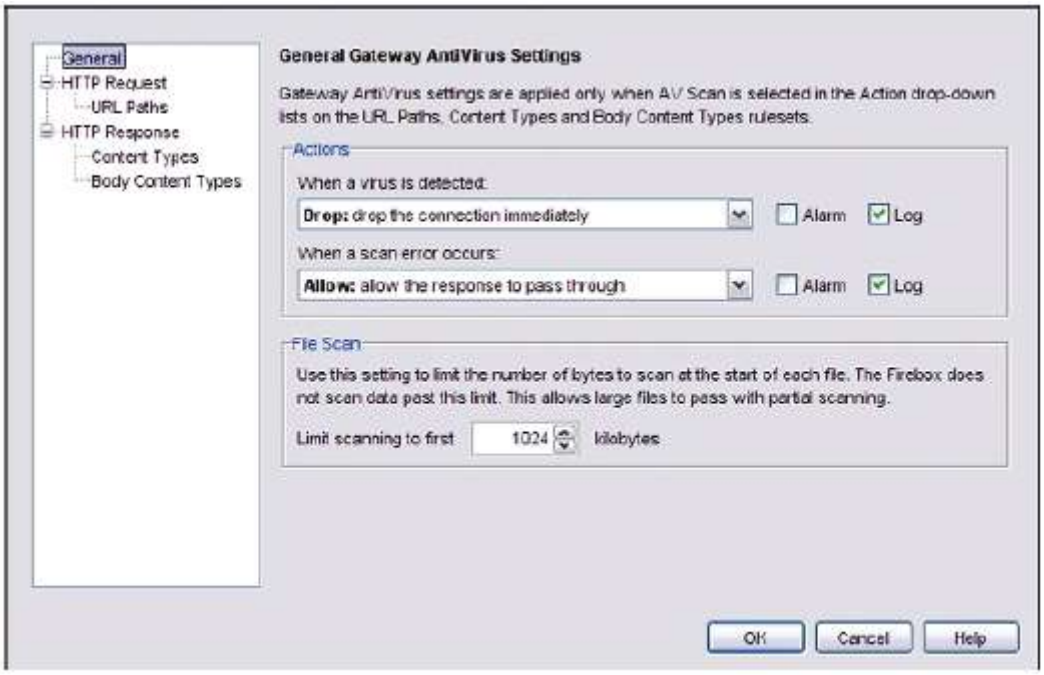
Настройка действий Gateway AntiVirus для действия прокси

1. В Policy Manager выберите **Subscription Services** > **Gateway AV** > **Configure**.
   Откроется диалоговое окно Gateway AntiVirus



2. Выберите политику, для которой вы хотите включить Gateway AntiVirus, и нажмите **Enable**.
   Статус Gateway AV изменится на Enabled.

3. Нажмите **Configure**.
   Откроется страница с параметрами Gateway AntiVirus для этой политики.



4. Из выпадающего списка **When a virus is detected** выберите действие, которое будет выполнено при обнаружении вируса в электронном письме, файле или на web странице.

5. Из выпадающего списка **When a scan error occurs** выберите действие, которое будет выполнено если Firebox не может просканировать объект или вложение. Вложения, которые Gateway не может просканировать, включают binhex сообщения, определенные зашифрованные файлы или файлы, которые используют сжатие, которое не поддерживается Gateway AV, как например Zip файлы, защищенные паролем files. Для более подробной информации информации о действиях Gateway AV см. начало этой главы.

6. Если вы хотите записывать каждое действие в журнал, включите опцию **Log**.

7. Если вы хотите для каждого создавать тревогу, включите опцию **Alarm**.

8. Вы можете ограничить размер сканируемого файла до определенного количества килобайт. Остальные байты в файле не сканируются. Это позволяет прокси сканировать только часть больших файлов, не оказывая заметного влияния на производительность. В поле **Limit scanning to first** введите необходимое количество килобайт

Вы также можете настроить действия Gateway AntiVirus в диалоговом окне **Edit Policy Properties**.

1. Два раза нажмите на политику в Policy Manager.

2. Выберите закладку **Properties**.

3. Нажмите на иконку **View/Edit Proxy**. 

4. Выберите **AntiVirus** из списка **Categories**.

Настройка уведомлений для действий антивируса

Тревога – это механизм оповещения пользователей о том, что правило прокси было применено к передаваемому им трафику. Если вы включите тревоги для действий антивируса в прокси, вам также необходимо настроить тип тревоги.

Для того чтобы настроить тип тревоги для политики прокси выполните следующее:

1. В Policy Manager два раза нажмите на политику.
2. Выберите закладку **Properties**.
3. Нажмите на иконку **View/Edit Proxy**. 
4. Выберите категорию **Proxy and AV Alarms**
5. Выполните настройку параметров тревог в категории Proxy/AV Alarms

Разблокировка файла, заблокированного Gateway AntiVirus

WatchGuard System Manager предоставляет вам утилиту для разблокировки вложений, заблокированных Gateway AntiVirus:

C:\Program Files\WatchGuard\wsm8\bin\unlock.exe

Для того чтобы открыть заблокированный файл, выполните следующее:

1. Откройте командную строку.
2. Введите: Unlock <путь_к_заблокированному файлу>

Настройка Gateway AntiVirus для карантина почты

Сервер Карантина WatchGuard предоставляет безопасный механизм карантина электронных писем, которые были идентифицированы как спам, или которые содержат вирусы. Этот репозитарий получает электронные сообщения от SMTP прокси.

Для того чтобы настроить Gateway AntiVirus для карантина почты выполните следующее:

1. При запуске мастера Activate Gateway AntiVirus Wizard, вам необходимо убедиться, что вы используете Gateway AntiVirus с SMTP прокси. POP3 прокси не поддерживает Сервер Карантина.
2. При настройке действий spamBlocker для различных категорий почты (как описано в процедуре настройки spamBlocker), убедитесь, что хотя бы для одной категории вы выбрали действие **Quarantine**. Когда вы выберете это действие, вам необходимо настроить Сервер Карантина. Вы также можете выбрать действие **Quarantine** для электронных сообщений, идентифицированных Virus Outbreak Detection, как содержащие вирусы

Настройка ограничений на сканирование файлов сервисом Gateway AntiVirus

Gateway AntiVirus сканирует каждый файл до определенного количество килобайт. Любые дополнительные байты файла не сканируются. Это позволяет прокси сканировать большие файлы по частям без влияния на скорость работы системы. Максимальный размер и размер по умолчанию могут быть разными для разных моделей WatchGuard.

Максимальные размеры сканирования для различных моделей устройств WatchGuard (в килобайтах)

Модель	Минимум	Максимум	По умолчанию
Firebox X Edge e-Series: X10e, X20e,	250	1024	250

X55e, X10e-W, X20e-W, X55e-W			
Firebox X Core e-Series: X550e, X750e, X750e-4, X1250e, X1250e-4	250	20480	1024
Firebox X Peak e-Series: X5500e, X6500e, X8500e, X8500e-F	250	30720	1024
WatchGuard XTM1050	250	30720	1024

Для более подробной информации о настройке максимального размер файла для сканирования см. “Настройка действий Gateway AntiVirus”

Обновление параметров Gateway AntiVirus/IPS

Устройство WatchGuard имеет несколько параметров для сервиса Gateway AntiVirus в независимости от того, с каким прокси он используется. Для более подробной информации см. “Настройка параметров восстановления Gateway AV”

Для обеспечения высокого уровня безопасности важно иметь самую последнюю версию сигнатур для Gateway AntiVirus/Intrusion Prevention Service. Обновить сигнатуры вы можете двумя способами:

- Настроить сервер обновлений Gateway AV/IPS для автоматического обновления
- Обновить сигнатуры вручную в Firebox System Manager. Для более подробной информации см. “Обновление сервисов вручную”

Если вы используете антивирус другого производителя

Если на компьютерах, защищенных устройством WatchGuard, установлен антивирус другого производителя, у вас могут возникнуть проблемы с обновлением сигнатур. Когда этот антивирус пытается обновить сигнатуры через порт 80, сервис WatchGuard Gateway AV/IPS, который работает с HTTP прокси, распознает сигнатуры и удаляет их из пакета еще до того, как они попадут на компьютер клиента. Тем самым антивирус не может обновить свои базы данных. Для того чтобы этого избежать, вам необходимо создать исключение в HTTP прокси. Для этого вам необходимо знать имя сервера, с которого антивирус пытается загрузить обновления. После вы можете добавить этот сервер, как исключение в настройки HTTP прокси.

Для того чтобы создать исключение на устройстве WatchGuard, которое защищает компьютер, антивирус которого хочет обновить свои базы данных, выполните следующее:

1. Откройте настройки политики HTTP прокси, которая заблокировала обновления антивируса.
2. В секции **Categories** выберите **HTTP Proxy Exceptions**.
3. В поле рядом с кнопкой **Add** введите имя хоста сервера обновлений. Если вы хотите разрешить подключение ко всем его поддоменам, вставьте групповой символ (*) до и после имени хоста сервера.

Например, *watchguard.com* разрешает все поддомены сайта watchguard.com - antivirus.watchguard.com или updates.watchguard.com.

4. Нажмите **Add**. Повторите п. 4 и 5, если вы хотите добавить еще несколько исключений.

5. Нажмите два раза **OK**. Сохраните конфигурационный файл.

Настройка параметров восстановления Gateway AV

1. В Policy Manager выберите **Subscription Services** > **Gateway AntiVirus** > **Configure**.
Откроется диалоговое окно Gateway AntiVirus.

2. В диалоговом окне **Gateway AntiVirus** нажмите **Settings**.
Откроется диалоговое окно Gateway AV Decompression Settings

3. Для сканирования внутри сжатых вложений включите опцию **Enable Decompression**. Выберите или введите количество уровней сжатия для сканирования. Мы рекомендуем оставить три уровня по умолчанию. Если вы укажите большее число уровней, то это может повлиять на скорость передачи трафика. Gateway AntiVirus поддерживает максимум шесть уровней.

   Если Gateway AntiVirus обнаруживает, что глубина архива больше значения, установленного в этом поле, он сгенерирует ошибку сканирования.

   Сжатые файлы, которые Gateway AV сканировать не может, включают в себя зашифрованные файлы или файлы, использующие типы сжатия, которые нами не поддерживаются, например Zip файлы, защищенные паролем.

   Для того чтобы настроить действие, которое будет выполнять Firebox при обнаружении сообщения, которое он не может просканировать, выберите действие для **When a scan error occurs** в категории **General** настроек политики.

4. Нажмите **Restore Defaults** для того чтобы восстановить значения по умолчанию.

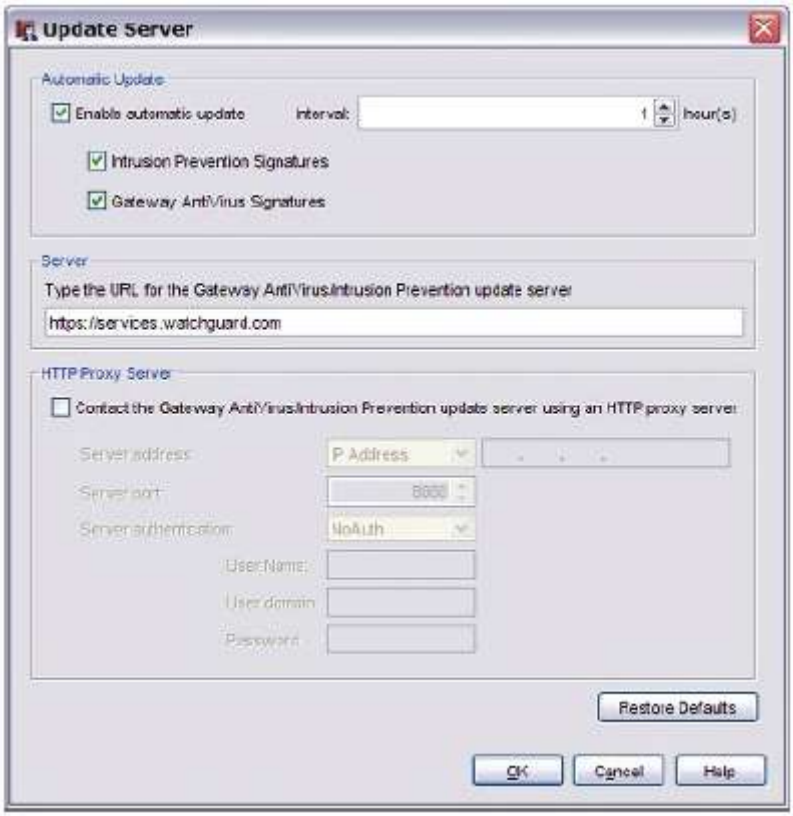
5. Нажмите **OK**.

Настройка сервера обновлений Gateway AV/IPS

Gateway AV и IPS используют один и тот же сервер обновления.

1. В Policy Manager выберите **Subscription Services** > **Gateway AntiVirus** > **Configure**. Или выберите **Subscription Services** > **Intrusion Prevention** > **Configure**.

2. Нажмите **Update Server**.
Откроется диалоговое окно Update Server



3. Для того чтобы включить автоматическое обновление сигнатур, включите опцию **Automatic update**. Введите количество минут между автоматическими обновлениями в выпадающем списке **Interval**.

   * Если вы хотите, чтобы Firebox загружал новые сигнатуры Gateway AV с указанным интервалом включите опцию **Gateway AV Signatures**.

   * Если вы хотите, чтобы Firebox загружал новые сигнатуры Gateway AV с указанным интервалом включите опцию **IPS Signatures**

4. Не изменяйте URL сервера обновлений для Gateway AV или IPS. Если вы случайно или неправильно введете URL, нажмите **Restore Defaults** для того чтобы вернуть значение по умолчанию.

5. Нажмите **OK**.

Подключение к серверу обновлений через HTTP прокси сервер

Если ваш Firebox должен подключаться к серверу обновлений Gateway AV/IPS через HTTP прокси, вам необходимо добавить информацию об HTTP прокси сервере к вашей конфигурации Gateway AV/IPS.

1. В диалоговых окнах **Gateway AntiVirus** или **Intrusion Prevention** нажмите **Update Server**

2. Включите опцию **Contact the Gateway AV/IPS update server using an HTTP proxy server**.

3. Из выпадающего списка **Server address** выберите, будете или вы идентифицировать ваш HTTP прокси сервер при помощи имени хоста или IP-адреса. В соответствующем поле введите IP-адрес или имя хоста.

4. Большинство HTTP прокси серверов получают запросы через порт 8080. Если ваш HTTP прокси использует другой порт, введите его в поле **Server port**.

5. Из выпадающего списка **Server authentication** выберите тип аутентификации, который будет использоваться на вашем HTTP прокси сервере. Выберите **NoAuth** если ваш HTTP прокси не требует аутентификации. Если ваш HTTP прокси сервер требует аутентификацию **NTLM** или **Basic**, введите имя пользователя, домен пользователя и пароль в соответствующих полях.

6. Нажмите **OK**.

Блокировка доступа из Trusted сети к серверу обновлений

Если вы не хотите, чтобы пользователи, подключенные к вашей Trusted сети, не могли получить доступ к серверу обновлений, вы можете использовать внутренний сервер для загрузки обновлений. Вы можете создать новую политику HTTP прокси с исключениями или политику пакетного фильтра HTTP, которая разрешает трафик только с IP адреса вашего внутреннего сервера на внешний сервер обновлений.

Состояния сервисов безопасности и обновление сигнатур вручную

Вы можете настроить сервисы безопасности для автоматического обновления сигнатур. Вы также обновлять сигнатуры вручную. Если вы не будете обновлять сигнатуры на вашем Firebox, вы не будете надежно защищены от самых последних вирусов и атак. Вы можете посмотреть статус и получить обновления в закладке **Security Services системы** Firebox System Manager.

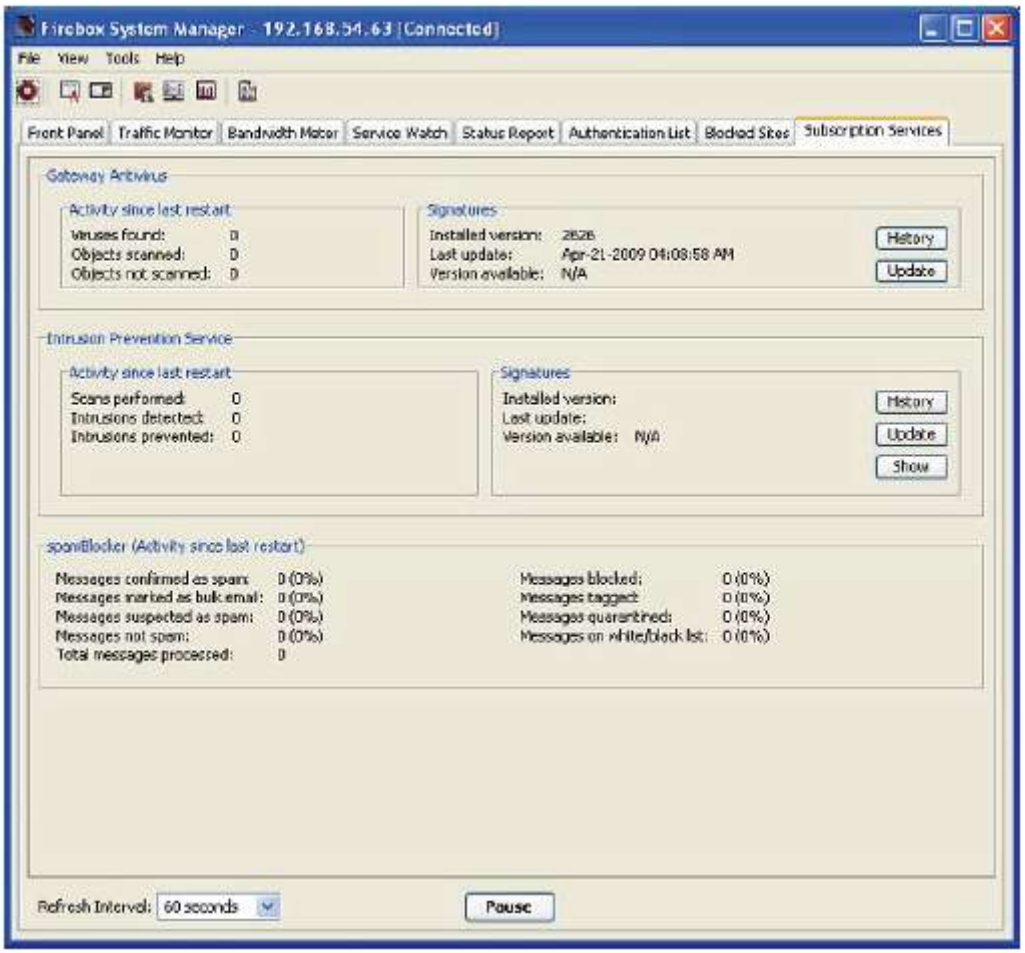
Статус сервиса

Закладка **Subscription Services** показывает – включена ли ваша защита или нет. ВЫ также сожете посмотреть информацию о версии сигнатур

Для того чтобы посмотреть статус сервиса выполните следующее:

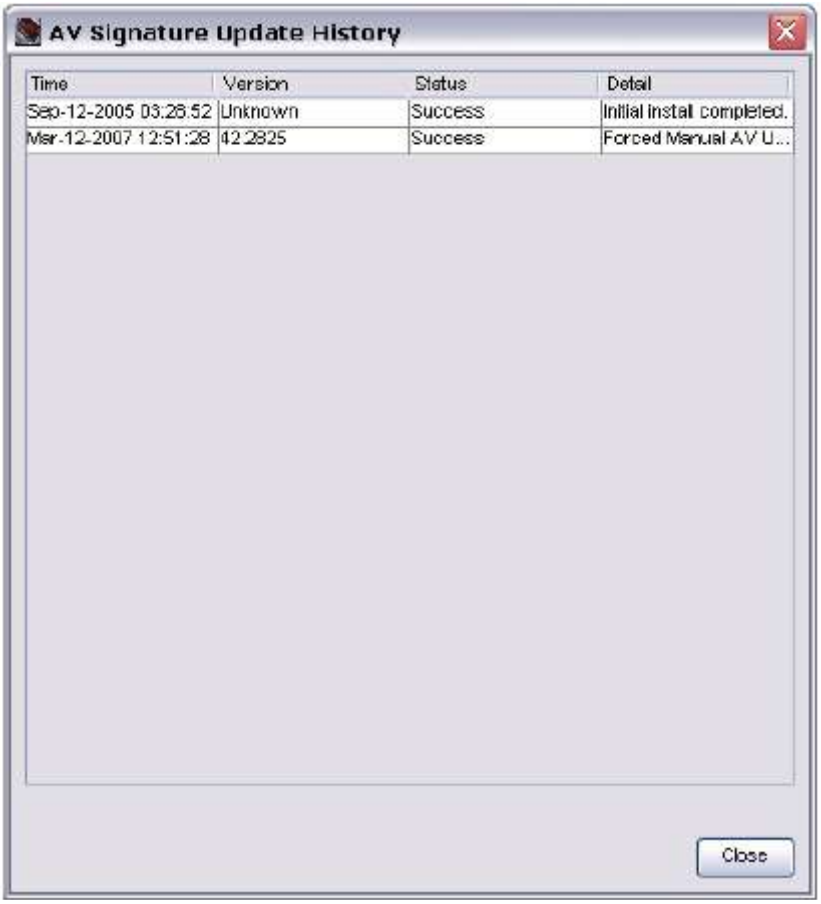
1. Откройте Firebox System Manager.

2. Выберите закладку **Security Services**. В окне отображается статус установленных сервисов безопасности. Для того чтобы посмотреть информации о состоянии вам необходимо установить соответствующие лицензии



Просмотр истории обновлений

В закладке **Subscription Services** нажмите **History** для того чтобы посмотреть список обновлений сервисов



Обновление сервисов вручную

В закладке **Subscription Services** нажмите **Update** для сервиса, который вы хотите обновить. Вам необходимо ввести пароль конфигурации. Firebox загружает самые последние доступные версиии сигнатур для Gateway AntiVirus или Intrusion Protection Service.

Активация Intrusion Prevention Service (IPS)

Хакеры используют множество методов для атаки компьютеров в сети Интрнет. Эти атаки предназначены для повреждения работы вашей сети, получения важной информации и использования ваших компьютеров для атаки других сетей. Такие атаки называются *проникновениями*.

Вы используете IPS для поиска и отражения атак при помощи прокси WatchGuard. IPS проверяет DNS, FTP, HTTP и SMTP трафик. IPS использует TCP proxy для сканирования FTP или HTTP трафика через нестандартные порты

Так как TCP-UDP прокси имеет дополнительный набор опций для IPS, вы не можете использовать эту процедуру для этого прокси. Вы также можете использовать TCP-UDP для обнаружения и разрешения/запрета Instant Messaging (IM) или Peer to Peer (P2P) сервисов. Однако этот компонент является частью базового продукта. Вам не надо приобретать Intrusion Prevention Service для его использования

Перед как использовать IPS в политике прокси, вам необходимо его активировать и создать базовую конфигурацию. Для этого вы можете запустить мастер Activate Intrusion Prevention или использовать набор правил Intrusion Prevention в настройках прокси. Мы рекомендуем

использовать мастер. Для того чтобы запустить мастер Activate Intrusion Prevention выполните следующее:

1. Получите лицензионный ключ для IPS от LiveSecurity Service и добавьте его на Firebox

2. В WatchGuard System Manager выберите устройство WatchGuard, который будет использовать IPS, и откройте Policy Manager.

3. В Policy Manager выберите **Subscription Services** > **Intrusion Prevention** > **Activate**. *Запустится мастер Activate Intrusion Prevention*

4. Нажмите **Next**.

5. Выполните все необходимые операции в мастере. Мастер отображает страницы в зависимости от того, есть ли в вашей конфигурации политики прокси. Например, если в вашей конфигурации нет политик прокси, мастер поможет вам создать ее. Затем вы можете снова запустить мастер для настройки IPS или вы можете посмотреть инструкции в следующих секциях.

Select proxy policies to enable

На этой странице отображается список политик прокси, созданных для вашего Firebox. Из списка выберите политики прокси, для которых вы хотите включить IPS. Вы не можете выбрать политики с уже включенным сервисом IPS.

Create new proxy policies

В этой странице отображаются типы прокси, для которых не существует политик. Если, например, вы создали политику SMTP, она не появится в списке.

Для того чтобы создать политику, отметьте соответствующую опцию. Если вы выберете SMTP, введите IP-адрес сервера электронной почты. Этот мастер создает по умолчанию политику SMTP, которая является политикой статической NAT. Для того чтобы создать эту политику SMTP, у вас должен по крайней мере один интерфейс External со статическим IP-адресо или PPPoE. Если у вас несколько интерфейсов, то создается только одна политика.

Поле **To** политик содержит параметр статической NAT (статический IP-адрес первого интерфейса External к опредeнному IP-адресу почтового сервиса). Если эта политика не удовлетворяет вашим требованиям, то, перед тем, как запустить мастер, вы можете создать свою политику SMTP

Select advanced Intrusion Prevention settings.

Если вы активируете IPS для прокси HTTP client Откроется диалоговое окно страница **Select advanced Intrusion Prevention settings**. Эти параметры будут применяться к трафику, который передается через HTTP прокси. Список опций зависит от конфигурации используемых вами прокси.

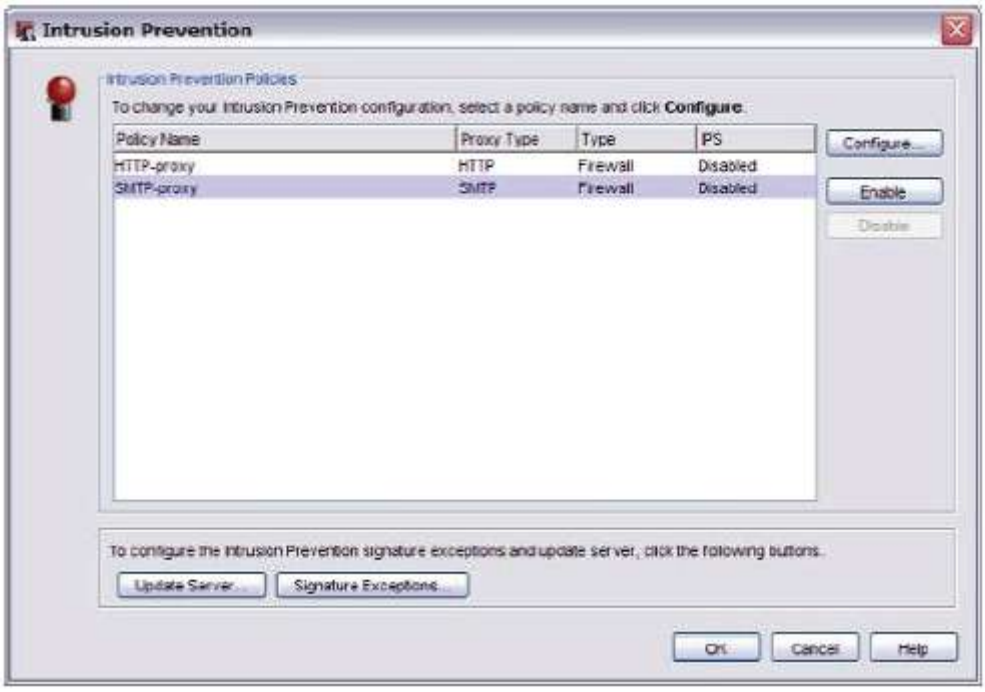
После того, как мастер завершит работу, вы можете настроить IPS для выбранных вами прокси.

Настройка Intrusion Prevention Service (IPS)

После того, как вы активировали IPS и создали базовую конфигурацию, вы можете настроить параметры IPS.

Если вы включили IPS в настройках прокси, эту процедуру можно пропустить. В настройках прокси вы уже выполнили все необходимые настройки IPS. Однако при помощи этой процедуры вы можете при необходимости внести изменения.

1. В Policy Manager выберите **Subscription Services > Intrusion Prevention > Configure**.
   Откроется диалоговое окно Intrusion Prevention



2. Выберите политику, которую вы хотите настроить, и нажмите **Configure**.
   Откроется диалоговое окно IPS Configuration для этой политики.

3. Настройте необходимые параметры для IPS.

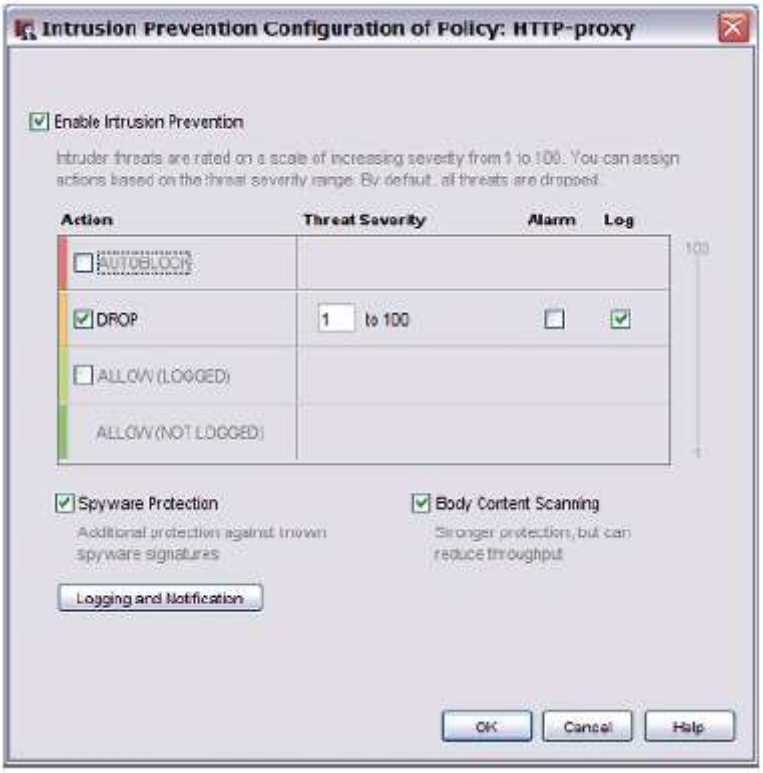
Настройка параметров для Intrusion Prevention Service (IPS)

Для настройки параметров IPS для политики прокси выполните следующее.

1. В Policy Manager выберите **Subscription Services** > **Intrusion Prevention** > **Configure**.

2. Выберите прокси и нажмите **Configure**.

3. Включите опцию **Enable Intrusion Prevention**



4. Выберите одно из следующих действий:

   * **AUTOBLOCK**: разрыв соединения и добавление IP адреса отправителя в список Blocked Sites если содержимое совпадает с сигнатурой, уровень критичности которой равен или больше установленного вами уровня. Вы не можете выбрать действие AUTOBLOCK для SMTP прокси.

   * **DROP**: Разрыв соединения если содержимое совпадает с сигнатурой на уровне критичности, который находится в установленном вами диапазоне. Отправитель сообщения не получает никакого уведомления

   * **ALLOW (LOGGED)**: Разрешает транзакцию даже если содержимое совпадает с сигнатурой на уровне критичности, который попадает в установленный вами диапазон. Разрешенные транзакции в этом диапазоне уровней критичности, автоматически записываются в журнал.

   * **ALLOW (NOT LOGGED)**: Если вы разрешите угрозы, уровень критичности которых не превышает минимальный уровень, транзакции, которые совпадают с уровнем критичности ниже минимального будут автоматически разрешены и не будут записываться в журнал. Числа, которые появляются в колонке **Threat Severity** для данного действия изменить нельзя.

*Если вы сделаете минимальный порог уровня критичности для действия **ALLOW (LOGGED)** больше единицы, то все транзакции, которые совпадают с сигнатурой на более низком уровне критичности будут разрешены и не будут записываться в журнал*

5. Для того чтобы установить минимальный уровень критичности для действий **AUTOBLOCK**, **DROP**, or **ALLOW (LOGGED)** выберите число в колонке **Threat Severity**. Все угрозы имеют уровни критичности от 1 до 100. По умолчанию все угрозы блокируются и записываются в файл.

6. Если вы хотите записывать в журнал действия прокси включите опцию **Log** для каждого действия IPS.

7. Если для каждого действия прокси создать тревогу включите опцию **Alarm**

8. (Только HTTP и TCP-UDP прокси) Включите опцию **Enable spyware protection** для защиты от spyware. После того, как вы включите защиту от spyware сервис IPS помимо обычных сигнатур будет использовать сигнатуры защиты от spyware (Emerging Threats). Для более подробной информации о проекте Emerging Threats см. http://www.emergingthreats.net.

9. (только для HTTP и TCP-UDP прокси) Включите опцию **Body Content Scanning**. Это обеспечивает более надежную защиту, однако снижает пропускную способность.

10. Нажмите **Logging and Notification** для того чтобы настроить журнал и уведомления для IPS

Также действия IPS вы можете настроить в диалоговом окне **Edit Policy Properties**.

1. В Policy Manager два раза нажмите на политику.

2. Выберите закладку **Properties**.

3. Нажмите  .

4. Выберите Intrusion Prevention в списке Categories.

5. Настройте параметры IPS.

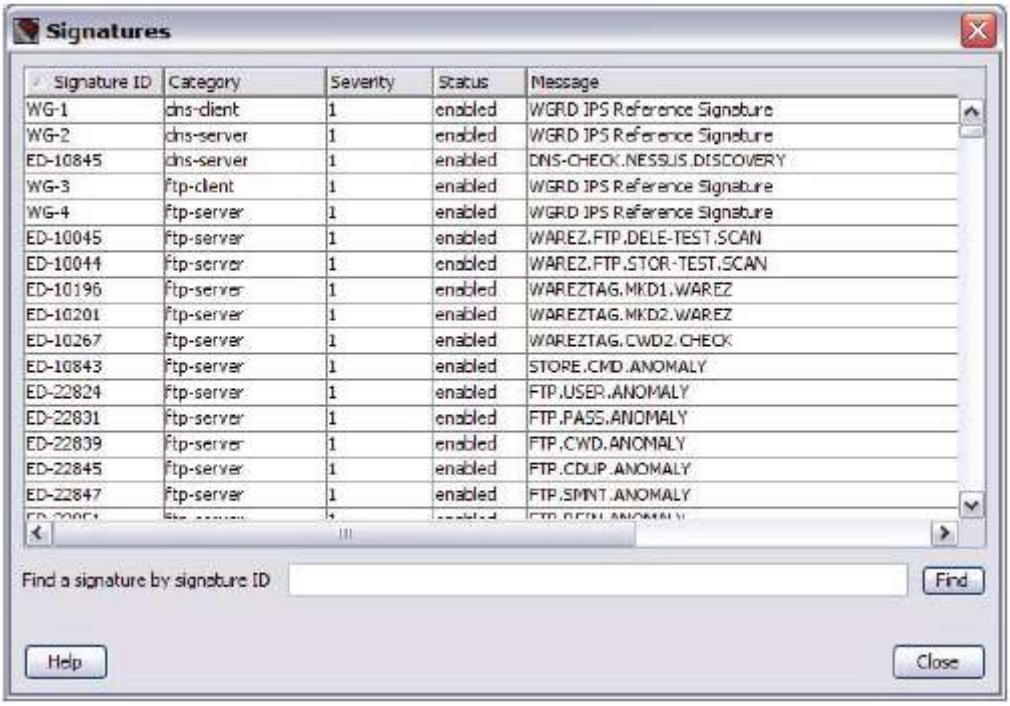
Настройка исключений сигнатур

После того, как вы включите IPS в политике прокси, она будет проверять трафик на наличие определенных шаблонов, которые совпадают с известными сигнатурами. Когда происходит совпадение шаблона трафика с IPS сигнатурой, устройство WatchGuard запрещает загрузку содержимого и потенциальная попытка проникновения блокируется. Если вы хотите разрешить трафик, заблокированный IPS, вы можете идентификационный номер сигнатуры и добавить эту сигнатуру в список исключений IPS. Каждая сигнатура IPS имеет свой уникальный ID. Вы можете найти ID каждой сигнатуры при помощи Firebox System Manager.

Поиск ID сигнатуры

1. Откройте Firebox System Manager. Выберите закладку **Subscription Services**.

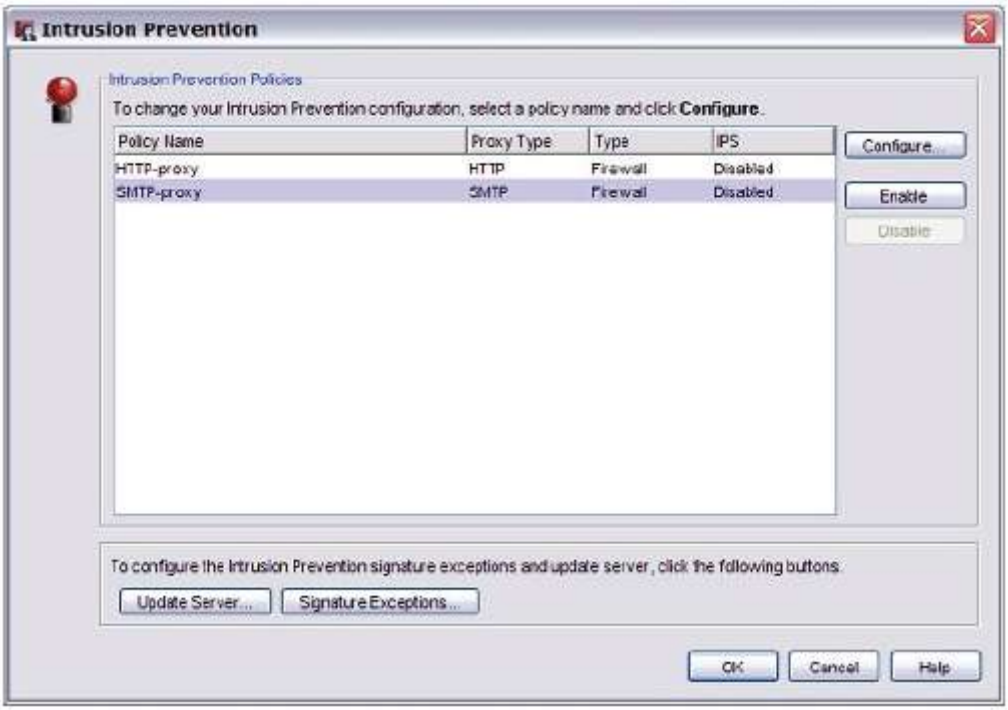
2. В разделе **Intrusion Prevention** нажмите **Show**.
Откроется диалоговое окно Signatures.



3. Для добавления сигнатуры исключения используйте Signature ID

Добавление исключения IPS сигнатуры

1. В Policy Manager выберите **Subscription Services** > **Intrusion Prevention** > **Configure**
Откроется диалоговое окно Intrusion Prevention



2. Нажмите **Signature Exceptions**.
   Откроется диалоговое окно Signature ID Exception

3. В поле **Signature ID** введите ID сигнатуры, которую вы хотите отключить. Нажмите **Add**.

4. Нажмите **OK**.

Копирование параметров IPS в другие политики

После настройки IPS для одного прокси, вы можете скопировать эту конфигурацию в другие прокси. Однако, вы можете копировать настройки IPS только между политиками с совместимыми конфигурациями IPS.

- Между политиками FTP, DNS, POP3 и SMTP
- Между политиками TCP
- Между политиками HTTP

Для того чтобы скопировать параметры IPS из одной политики в другую выполните следующее:

В окне **Intrusion Prevention** выберите прокси, конфигурацию которого вы хотите скопировать, нажмите правой кнопкой на него и выберите **Copy IPS Configuration**.

В этом же диалоговом окне, выберите прокси, в которые вы хотите скопировать конфигурацию, нажмите правой кнопкой и выберите **Paste IPS Configuration**

Активация и настройка IPS для TCP-UDP

Так как TCP-UDP прокси имеет несколько дополнительных параметров IPS, то вы не можете использовать мастер Activate IPS Wizard для настройки IPS для TCP-UDP.

1. Если вы еще не добавили TCP прокси к конфигурации Firebox, откройте Policy Manager, нажмите (+) в панели инструментов Policy Manager, откройте каталог **Proxies**, и два раза нажмите **TCP-proxy**.

2. В диалоговом окне **New Policy Properties** выберите **Properties** и нажмите  .

3. В секции Categories выберите Intrusion Prevention.

4. Настройте параметры для IPS(IPS).

5. Для настройки TCP-UDP прокси для блокировки Instant Messaging (IM) и Peer to Peer (P2P) сервисов, см. “TCP-UDP proxy: Application blocking”

Глава 33 - Сервер Карантина

Сервер Карантина

Сервер Карантина компании WatchGuard предоставляет вам безопасный механизм карантина любых электронных сообщений, идентифицированных как спам или как содержащие вирусы. Сервер Карантина – это репозитарий для электронных сообщений, которые были помещены в карантин SMTP прокси на основе данных, полученных после их анализа сервисом spamBlocker или Gateway AntiVirus.

Тщательный контроль позволяет вам настроить порядок размещения электронной почты, процедуру выделения свободного места и другие параметры. Сервер Карантина предоставляет все необходимые утилиты как пользователям, так и администраторам. Пользователь периодически получает по электронной почте уведомления от Сервера Карантина о том, что пользователь имеет электронную почту на Сервере Карантина. Для того чтобы подключиться к Серверу Карантина пользователю необходимо нажать на URL, который содержится в электронном письме. На этом сайте пользователи могут посмотреть информацию об отправителях и темах всех подозрительных писем, помещенных в карантин. Пользователи могут выбрать те сообщения, которые будут загружены в их почтовые ящики, или удалить ненужные сообщения.

Администратор может сконфигурировать Сервер Карантина для автоматического удаления будущих сообщений с определенных доменов и от определенных отправителей, те сообщения, которые содержат определенный текст в поле Subject..

Администратор может всегда посмотреть статистику по активности Сервера Карантина, включая количество изолированных сообщений за определенный промежуток времени, а также количество сообщений, которые предположительно является спамом. SMTP прокси на основе данных, полученных после анализа сервисами spamBlocker и Gateway AntiVirus, распределяет сообщения по нескольким категориям:

- Предположительно спам (Suspected spam): Сообщение может быть спамом, однако для точной идентификации не хватает данных.
- Подтвержденный спам(Confirmed spam): сообщения является спамом.
- Bulk: сообщение является коммерческим bulk сообщением.
- Virus: Сообщение содержит вирус.
- Possible virus: Возможно, что сообщение содержит вирус, однако для точной идентификации не хватает информации.

Прокси SMTP нужен Сервер Карантина только в случае, если в настройках прокси вы указали помещать в карантин сообщения, которые были идентифицированы как спам, или если вы настроили Gateway AntiVirus для карантина сообщений из определенной категории.

Настройка Сервера Карантина

Установка Сервера Карантина

Убедитесь, что Сервер Карантина установлен на вашей станции управления. Сервер Карантина устанавливается, как серверный компонент при установке WatchGuard System Manager. Если Сервер Карантина у вас не установлен, то вы можете снова запустить мастер установки, и в окне выбора серверных компонентов для установки выбрать только Сервер Карантина

Запуск мастера WatchGuard Server Center Setup

Мастер WatchGuard Server Center Setup используется для настройки Сервера Карантина и других установленных серверных компонентов. Мастер WatchGuard Server Center Setup запускается автоматически после первого запуска WatchGuard Server Center.

На компьютере, на который вы установили Сервер Карантина, выполните следующее:

1. Нажмите правой кнопкой на  в панели задач и выберите **Open WatchGuard Server Center**.
   Откроется мастер WatchGuard Server Center Setup.

2. Внимательно прочитайте информацию на первой странице и убедитесь, что вас есть вся необходимая информация. Нажмите **Next**.

3. Введите название вашей организации. Нажмите **Next**.

4. Введите и подтвердите пароль администратора (**Administrator passphrase**)**,** который будет использоваться для всех серверов WatchGuard. Нажмите **Next**.

5. (Дополнительно) Введите IP вашего Firebox шлюза. Нажмите **Add**. Нажмите **Next**.

6. (Дополнительно) Введите лицензионный ключ вашего Сервера Управления. Нажмите **Next**.

7. Введите ключ шифрования Сервера Журналов (**Log Server Encryption key)**. Нажмите **Next**.

8. Введите имя домена, сообщения с которого вы хотите поместить в карантин. Нажмите **Add**. Нажмите **Next**.

9. (Дополнительно) Загрузите и установите базу данных WebBlocker. Нажмите **Next**.
   Загрузка и установка базы данных может занять много времени. Вы также можете установить ее позже.

10. Проверьте выполненные вами настройки. Нажмите **Next**.
    Мастер выполнит настройку ваших серверов.

11. Нажмите **Finish** для того чтобы закрыть мастер.

Если вы установили Сервер Карантина после того, как вы настроили другие Серверы WatchGuard, мастер не запустится автоматически после запуска WatchGuard Server Center.Вы можете запустить мастер, нажав на иконку Сервера Карантина в WatchGuard Server Center.

Настройка параметров Сервера Карантина

На компьютере, на который вы установили Сервер Карантина, выполните следующее:

1. Нажмите правой кнопкой на  в панели задач и выберите **Open WatchGuard Server Center**.
   Откроется WatchGuard Server Center.

2. В текстовых полях **Username** и **Administrator passphrase** введите имя пользователя и пароль администратора соответственно.

3. В меню **Servers** выберите **Quarantine Server**.
   Откроется страница Quarantine Server.

4. Выполните необходимые настройки параметров сервера.

   * Для того чтобы изменить параметры сервера см. “Настройка параметров Сервера Карантина”

* Для того чтобы изменить параметры администрирования базы данных см. “Изменение параметров удаления и списка доменов”

* Для того чтобы изменить параметры уведомлений см. “Изменение параметров уведомления”

* Для того чтобы изменить параметры журнала см. “Настройка журнала для Сервера Карантина”

* Для настройки правил карантина почты см. “Правила Сервера Карантина”

5. После того, как вы закончите все необходимые настройки, нажмите **OK**.

Настройка Firebox для карантина почты

После того, как вы установили Сервер Карантина, вам необходимо обновить конфигурацию вашего Firebox для отправки почты на Сервер Карантина.

Вы можете сделать это двумя способами:

1. Настройте IP адрес Сервера Карантина, как описано в “Установка Сервера Карантина”

2. Создайте действия spamBlocker и Gateway AntiVirus для SMTP прокси для карантина почты. Для более подробной информации см. “Настройка Gateway AntiVirus для карантина почты” и “Настройка spamBlocker для карантина почты”

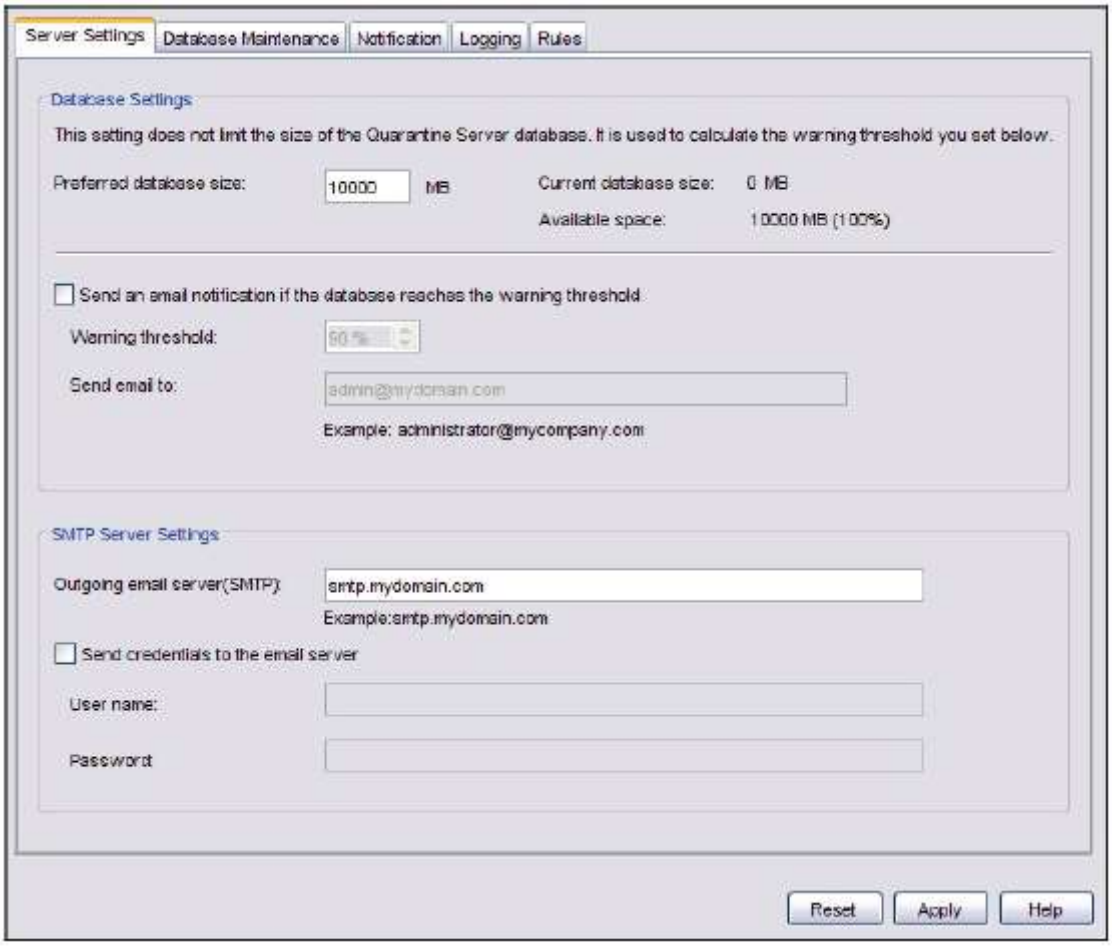
Настройка Сервера Карантина

Для того чтобы открыть страницу параметров Сервера Карантина выполните следующее:

1. Нажмите правой кнопкой на  в панели задач Windows и выберите **Open WatchGuard Server Center**.

2. Введите пароль администратора.
Откроется WatchGuard Server Center.

3. Нажмите на иконку Сервера Карантина .
Откроется страница Quarantine Server Configuration



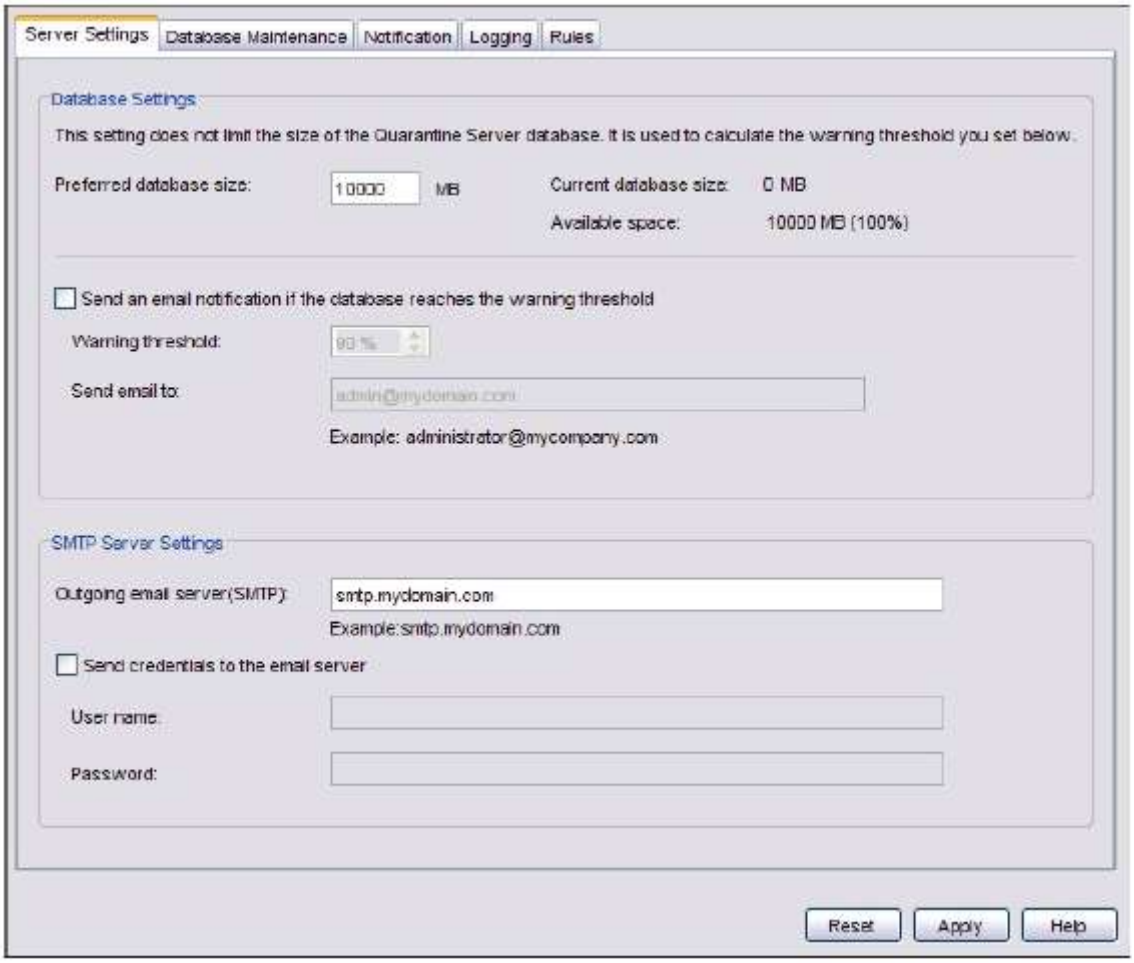
Вы можете настроить следующие параметры:

- Общие параметры сервера.
- Срок хранения сообщений или настройки домена пользователя: на протяжении какого времени хранить сообщения в карантине, добавление и удаление доменов пользователей. На Сервер Карантина будет отправляться почта только пользователей, которые принадлежать доменам в списке.
- Параметры уведомлений: Уведомление пользователю о том, что его почта была отправлена на Сервер Карантина.
- Параметры журнала.
- Правила Сервера Карантина

Настройка общих параметров сервера

1. Нажмите правой кнопкой на в панели задач Windows и выберите **Open WatchGuard Server Center**.
2. Введите пароль администратора
Откроется WatchGuard Server Center.

3. Нажмите .
Откроется страница Quarantine Server Configuration



Параметры базы данных

Preferred database size

Этот параметр используется для уведомлений. Он не ограничивает размер базы данных Сервера Карантина. Он используется для подсчета порогового размер базы данных для уведомлений. Размер базы данных варьируется от 1 до 10000 Мб. По умолчанию - 10000 Мб. Диалоговое окно показывает текущий размер базы данных и количество свободного места.

Send an email notification if the database reaches the warning threshold

Включите эту опцию для того чтобы получать предупреждение в случае если размер базы данных скоро достигнет своего предела.

Warning threshold

Выберите размер базы данных, по достижении которого вы получите предупреждение.

Send warning message to

Введите адрес электронной почты, на который будут отправляться уведомления. Например, предположим вы выбрали получение предупреждения, установили пороговую величину равной 90%, и установили предпочтительный размер базы данных равным 1000 Мб, Сервер Карантина отправит предупреждение, когда размер базы данных достигнет 900 Мб.

Настройки SMTP сервера

Outgoing email server (SMTP)

Адрес исходящего SMTP сервера.

Use login information for the email server

Если ваш сервер требует аутентификацию, то включите эту опцию.

User name

Введите имя пользователя для сервера электронной почты. Если для подключения к SMTP серверу вам не нужно имя пользователя, вы можете оставить это поле пустым.

Password

Введите пароль для сервера электронной почты. Если для подключения к SMTP серверу вам не нужен пароль, вы можете оставить это поле пустым.

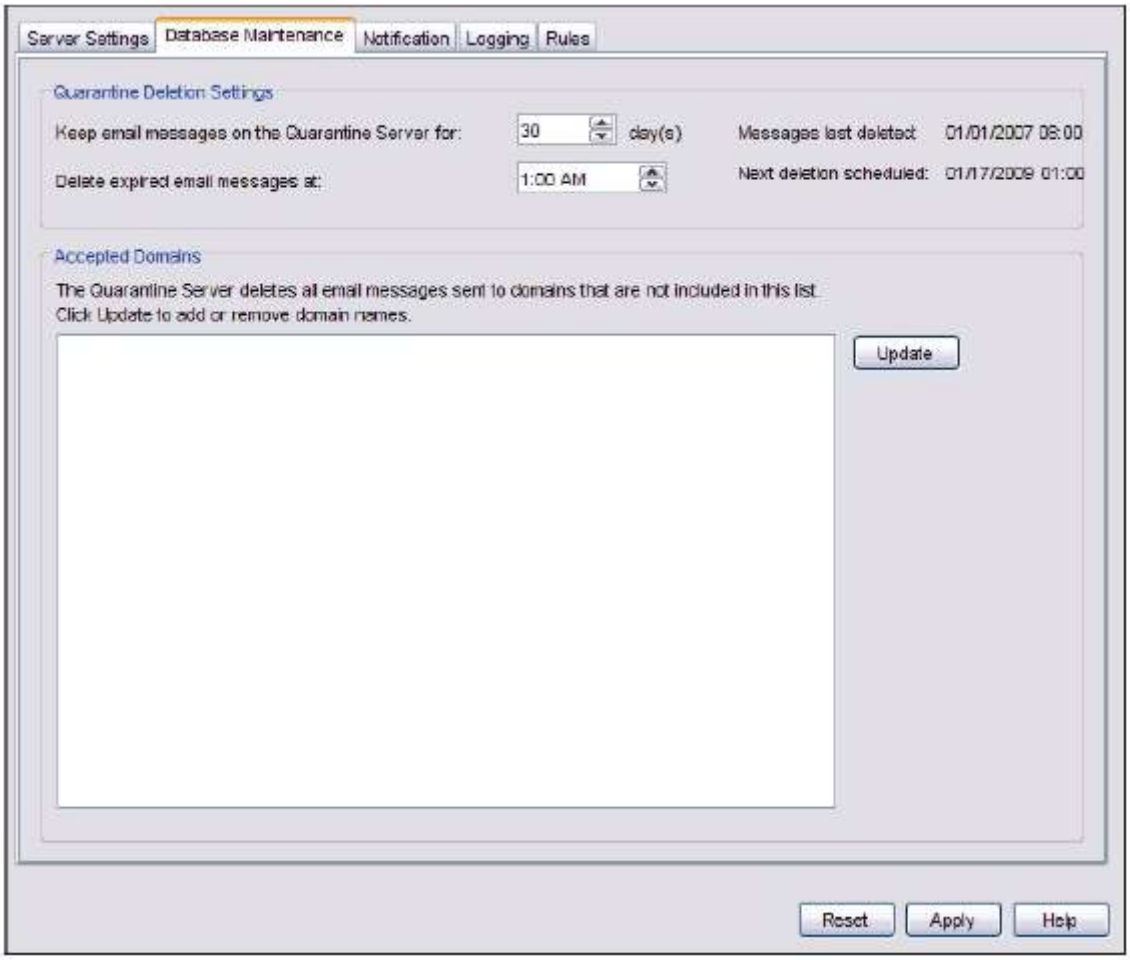
Изменение параметров удаления и списка доменов

1. Нажмите правой кнопкой на  в панели задач Windows и выберите **Open WatchGuard Server Center**.

2. Введите пароль администратора
   Откроется WatchGuard Server Center.

3. Нажмите  .
   Откроется страница Quarantine Server Configuration.

4. Выберите закладку **Database Maintenance**



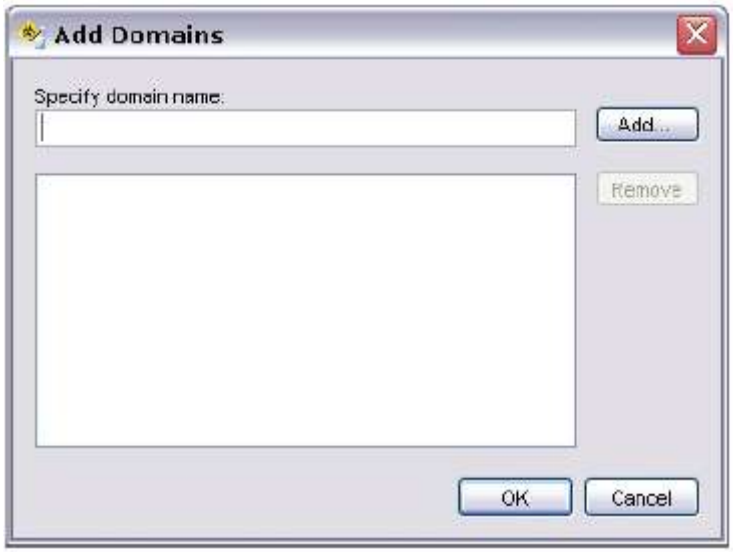
5. В поле **Keep email messages on the Quarantine Server for** введите количество дней, в течение которых сообщение будет храниться на Сервере Карантина. По умолчанию сообщения хранятся 30 дней.

6. В поле **Delete expired messages at** введите время дня, когда сообщения, срок хранения которых уже истек, будут удалены.

Добавление или удаление доменов

Закладка **Database Maintenance** диалогового окна **Quarantine Server Configuration** показывает имена доменов, электронная почта которых будет приниматься Сервером Карантина. Только те пользователи домена, которые занесены в список, смогут отправлять сообщения для Сервера Карантина. Сообщения, отправляемые пользователями вне списка, будут удалены.

1. Для добавления или удаления имени домена на сервере нажмите Update. Откроется диалоговое окно *Add Domains.*



2. Для того чтобы добавить домен введите его имя в поле **Specify domain name** и нажмите **Add**.

3. Для того чтобы удалить домен из списка, выберите его и нажмите **Remove**.

Изменение параметров уведомления

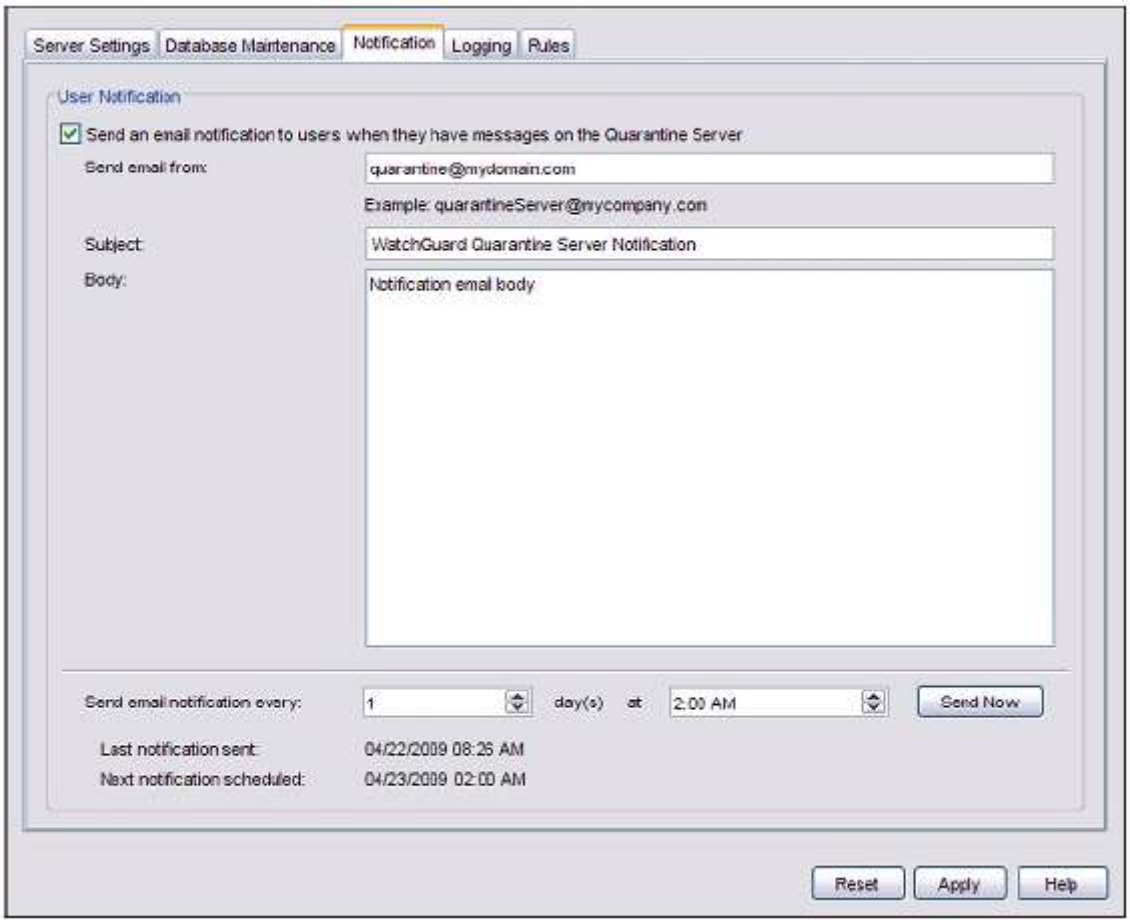
Пользователь периодически получает сообщения по электронной почте, которые содержат список сообщений, хранящихся в настоящее время на Сервере Карантина. Вы можете настроить учетную запись, с которой будут приходить эти сообщения. Вы также можете определить заголовок и содержание сообщения. Вы можете настроить интервал, в течении которого Сервер Карантина будет отправлять уведомления, несмотря на то, что он не может превышать одного дня. Вы также можете настроить точное время.

1. Нажмите правой кнопкой на  в панели задач Windows и выберите **Open WatchGuard Server Center**.

2. Введите пароль администратора
Откроется WatchGuard Server Center.

3. Нажмите  .
Откроется страница Quarantine Server Configuration.

4. Выберите закладку **Notification**



5. Для того включить или выключить уведомления (и поля в этом диалоговом окне) включите или выключите опцию **Send an email notification to users when they have messages on the Quarantine Server**.

6. В поле **Send email from** введите полный адрес электронной почты, с которого вы хотите отправить сообщении.

7. В поле Subject введите тему сообщения. По умолчанию в качестве темы письма используется строка «*WatchGuard Quarantine Server Notification*»

8. В поле Body введите содержание сообщения. Вы можете ввести текст или HTML в основную часть сообщения.

   Письмо с уведомлением всегда отправляется в формате HTML с указанием ссылок на сообщения, помещенные в карантин. Уведомления будут некорректно отображаться в почтовых клентах, которые не поддерживают HTML в теле сообщения.

9. Рядом с полем **Send email notification every**, введите временной интервал для уведомлений и время дня, в течение которого вы хотите отправить предупреждение. Если вы хотите непосредственно отправить сообщение для всех пользователей, кликните Send Now.

Некоторые почтовые клиенты могут пометить уведомления от Сервера Карантина как мошенничество или фишинг. Дело в том, что клиенты классифицируют такие URL, использующие IP адреса, как подозрительные. URL, предоставляющие пользователям доступ к Серверу Карантина, включают IP адреса Сервера Карантина вместо имени хоста.

Настройка журнала для Сервера Карантина

На странице **Logging** в настройках Сервера Карантина вы можете указать, куда он будет отправлять сообщения журнала. Сервер Карантина может отправлять сообщения журнала на Сервер Журналов WatchGuard, Просмотрщик Событий Window и/или, файл журнала.

В WatchGuard Server Center выполните следующее:

1. В списке **Servers** выберите **Quarantine Server**.

2. Выберите закладку **Logging**.
   Откроется страница Logging

3. Настройте необходимые параметры для вашего сервера

4. После того, как вы закончили, нажмите **Apply** для того сохранить выполненные изменения.

Правила Сервера Карантина

Вы можете настроить правила, которые будут автоматически удалять сообщения, которые приходят с определенных доменов или от определенных отправителей, или если они содержат указанный вами текст в поле Subject.

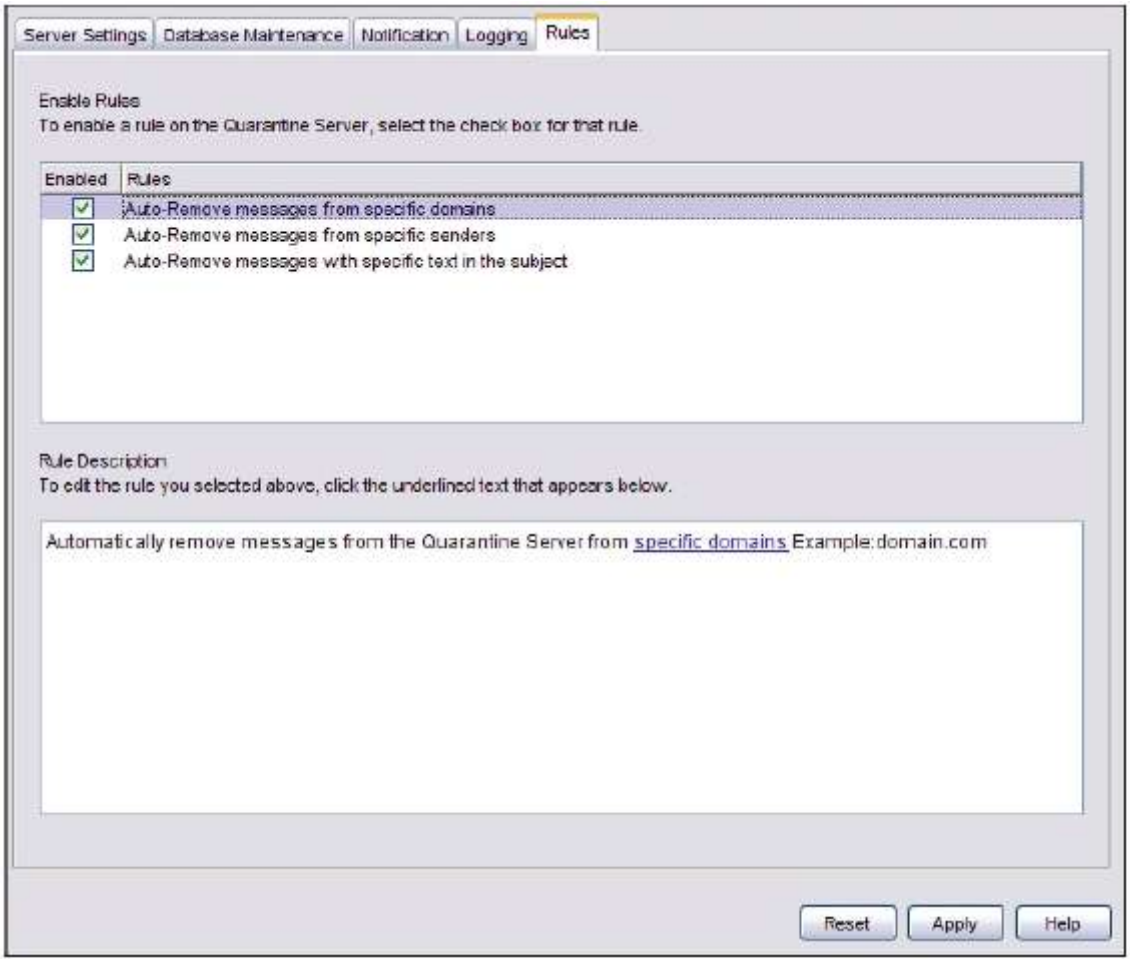
1. Нажмите правой кнопкой на в панели задач Windows и выберите **Open WatchGuard Server Center**.

2. Введите пароль администратора
   Откроется WatchGuard Server Center.

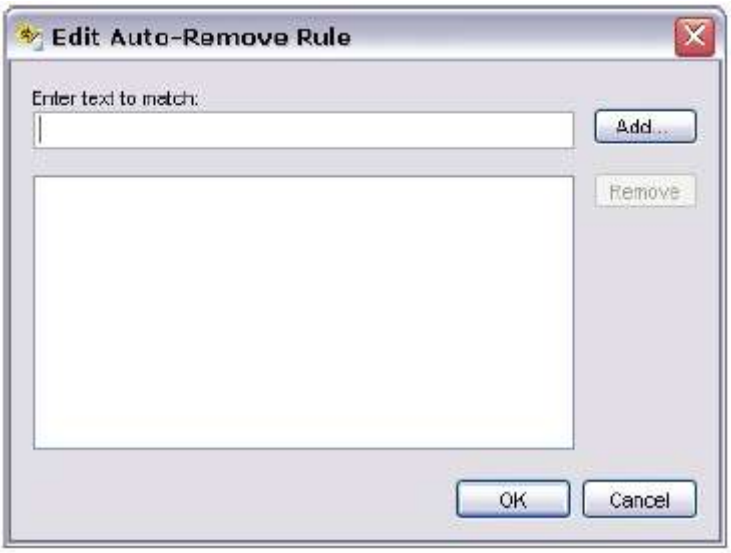
3. Нажмите  .
   Откроется страница Quarantine Server Configuration.

4. Выберите закладку **Rules**.

5. Для того чтобы изменить правило просто нажмите на него.
   Описание правила появится в разделе Rule Description



6. Кликните на подчеркнутые слова в правиле, для того чтобы добавить определенные домены, отправителей или строку в поле темы сообщения. Откроется диалоговое окно Edit Auto-Remove Rule



7. Для того чтобы добавить новый домен, отправителя или строку, введите его в поле **Enter text to match** и нажмите **Add**.

Обратите внимание на следующие ограничения в корректировке правил:

- Правила не поддерживают групповые символы. Например, вы не можете использовать правило Auto-Remove - *.gov” для автоматического удаления всех доменов с расширением *.gov.

- При удалении домена, отправителя или строки, Сервер Карантина удаляет только последующие сообщения электронной почты, удовлетворяющие этому правилу. Т.е. не удаляет те сообщения, которые находятся в настоящее время в базе данных.

Правила для автоматической блокировки сообщений со специфической строкой применяются только для текста, находящегося в строке темы сообщения. Если указанный текст находится в информационной части сообщения, т.е. не в строке темы сообщения, оно не будет удалено.

Настройка Сервера Карантина на Firebox

Вам необходимо настроить IP адрес Сервера Карантина, куда Firebox будет отправлять сообщения.

1. В Policy Manager выберите **Subscription Services** > **Quarantine Server**.
   Откроется диалоговое окно Quarantine Server

2. Введите IP адрес Сервера Карантина. Мы не рекомендуем изменять порт, который используется Сервером Карантина по умолчанию, только если вас не попросит это сделать представитель службы технической поддержки компании WatchGuard.

3. Для того чтобы отправлять все сообщения, обрабатываемые spamBlocker или Gateway AntiVirus, на Сервер Карантина включите опцию **Enable debugging for SMTP**. Если электронное сообщение не было обработано spamBlocker, так как оно является исключением spamBlocker, то оно не отправляется на Сервер Карантина.

4. Если вы хотите отменить все сделанные изменения и вернуть настройки по умолчанию нажмите **Restore Defaults**.

Клиент Сервера Карантина

Клиент Сервера Карантина предоставляет вам возможность управлять сообщениями и пользователями на сервере. Запустить клиент вы можете из WatchGuard System Manager.

1. В WatchGuard System Manager нажмите  . Или выберите **Tools** > **Quarantine Server Client**.

2. В поле **Name/IP Address** введите или выберите IP адрес или имя хоста сервера. Если ваш Сервер Карантина установлен на том же компьютере, что и WatchGuard System Manager, вы можете ввести **localhost**.

3. В поле **Username** введите имя пользователя. Этот пользователь должен иметь права Супер Администратора (Super Administrator). Для более подробной информации об администрировании на базе ролей см. “Администрирование на базе ролей”

4. В поле **Password** введите пароль пользователя Super Administrator.

5. Нажмите **OK**.
   Откроется диалоговое окно Quarantine Server Message and User Management.

В этом диалоговом окне вы можете:

- Управлять сообщениями карантина
- Управлять пользователями Сервера Карантина
- Смотреть статистику активности Сервера Карантина

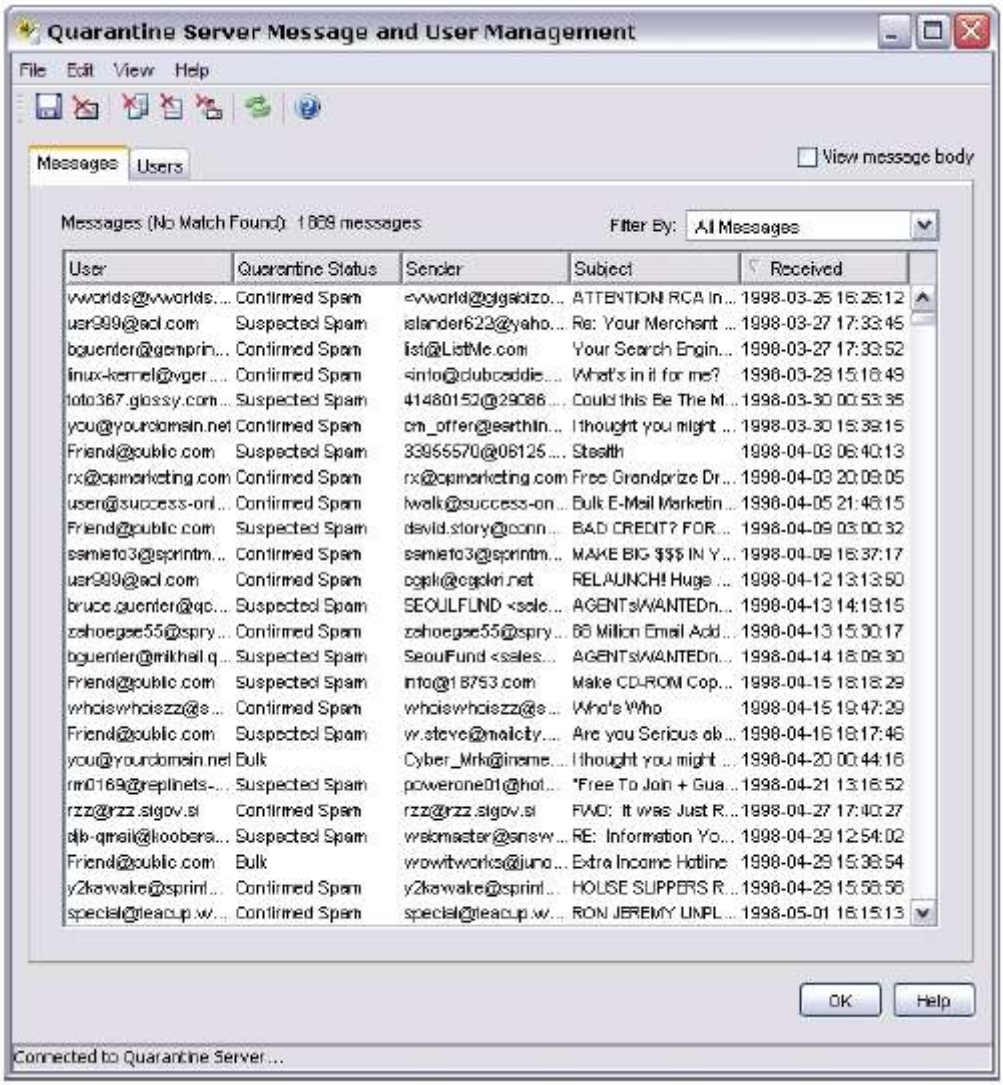
Управление сообщениями карантина

У вас существует возможность просмотра всех сообщений от Сервера Карантина в диалоговом окне. Вы можете сортировать сообщения по пользователям, статусу карантина, отправителям, темам, дате/времени получения.

Просмотр сообщений карантина

Для того чтобы запустить клиент Сервера Карантина из WatchGuard System Manager выберите **Tools > Quarantine Server Client**

Откроется диалоговое окно **Quarantine Server Message and User Management**. Список сообщений карантина вы можете посмотреть в закладке **Messages**



Настройка опций просмотра сообщений

Вы можете использовать выпадающий список **Filter By** для просмотра всех сообщений или только тех, которые имеют специфичный статус карантина. Для просмотра основной части сообщения выберите опцию **View message body.** Выберите какое-либо сообщение. Вторая панель появится в нижней части диалогового окна. Вы также можете выбрать любое сообщение и нажать **Edit > View Message Body,** либо нажать правой кнопкой мыши на сообщение и выбрать **View Message Body.**

Сохранение сообщений в файл

Вы можете сохранить копию сообщения в файл.

1. В закладке Messages диалогового окна **Quarantine Server Message and User Management,** выберите сообщения для сохранения. За один раз вы можете хранить только одно сообщение.

2. Кликните или выберите **File > Save As**.
   Либо кликните правой кнопкой мыши на сообщении и выберите **Save As.**

3. Выберите или введите каталог, в который вы хотите сохранить файл. Нажмите Save.

Передача сообщения получателю

Вы можете передать сообщение, помещенное в карантин, получателю. Вы не можете передавать сообщения, которые содержат или предположительно содержат вирусы.

1. В закладке **Messages** выберите сообщение или сообщения, которые вы хотите передать из получателям.

   * Для того чтобы выбрать несколько сообщений, нажмите на первое сообщение, зажмите клавишу `Shift` и нажмите на последнее сообщение списка.

   * Для того чтобы выбрать несколько сообщений, которые идут не по порядку, зажмите клавишу `Ctrl` и выберите все необходимые сообщения.

   * Для того чтобы выбрать все сообщения выберите **Edit >Select All**. Или нажмите правой кнопкой на любое сообщение и выберите **Select All**.

2. Выберите **Edit > Release Message**. Или нажмите правой кнопкой на выбранное сообщение и выберите **Release Message**.

После того, как сообщение будет отправлено пользователю, оно будет удалено из закладки Messages.

Удаление сообщений вручную

1. В закладке **Messages** диалогового окна **Quarantine Server Message and User Management,** выберите сообщение или сообщения для удаления.

2. Выберите диапазон сообщений, кликнув на первом сообщении в диапазоне, зажав клавишу shift, и кликните на последнем сообщении в диапазоне. Для выборочного выделения сообщений, которые не входят в диапазон, нажимайте клавишу Ctrl по мере выделения сообщения. Для выделения всех сообщений выберите **Edit >Select All.** Кликните правой кнопкой мыши на любое сообщение и выберите **Select All.**

3. Нажмите  .
   Или выберите **Edit > Delete.**

Автоматическое удаление сообщений

Вы можете настроить автоматическое удаление всех будущих сообщений, поступивших от особых доменов или отправителей, или содержащих текст в строке темы сообщения. Все последующие электронные письма от таких пользователей с определенными характеристиками будут автоматически удалены до того, как отправятся на Сервер Карантина.

1. В закладке **Messages** диалогового окна **Quarantine Server Message and User Management** выберите сообщение или сообщения, объединенные этой характеристикой, для автоматического удаления.

   * Для того чтобы выбрать диапазон сообщений, нажмите на первом сообщении в списке, нажав клавишу Shift, и нажмите на последнем сообщении в списке.

   * Для выборочного выделения сообщений, которые не входят в диапазон, нажимайте клавишу Ctrl по мере выделения сообщения.

   * Для выделения всех сообщений выберите **Edit >Select All.** Кликните правой кнопкой мыши на любое сообщение и выберите **Select All.**Нажмите. Или выберите **Edit > Delete.**

2. Выбор соответствующих опций для удаления. В меню Edit выберите **Auto-Remove > Sender Domain**, **Auto-Remove > Sender**, или **Auto-Remove > Subject**. Этими опциями можно воспользоваться контекстным меню правой кнопкой мыши.

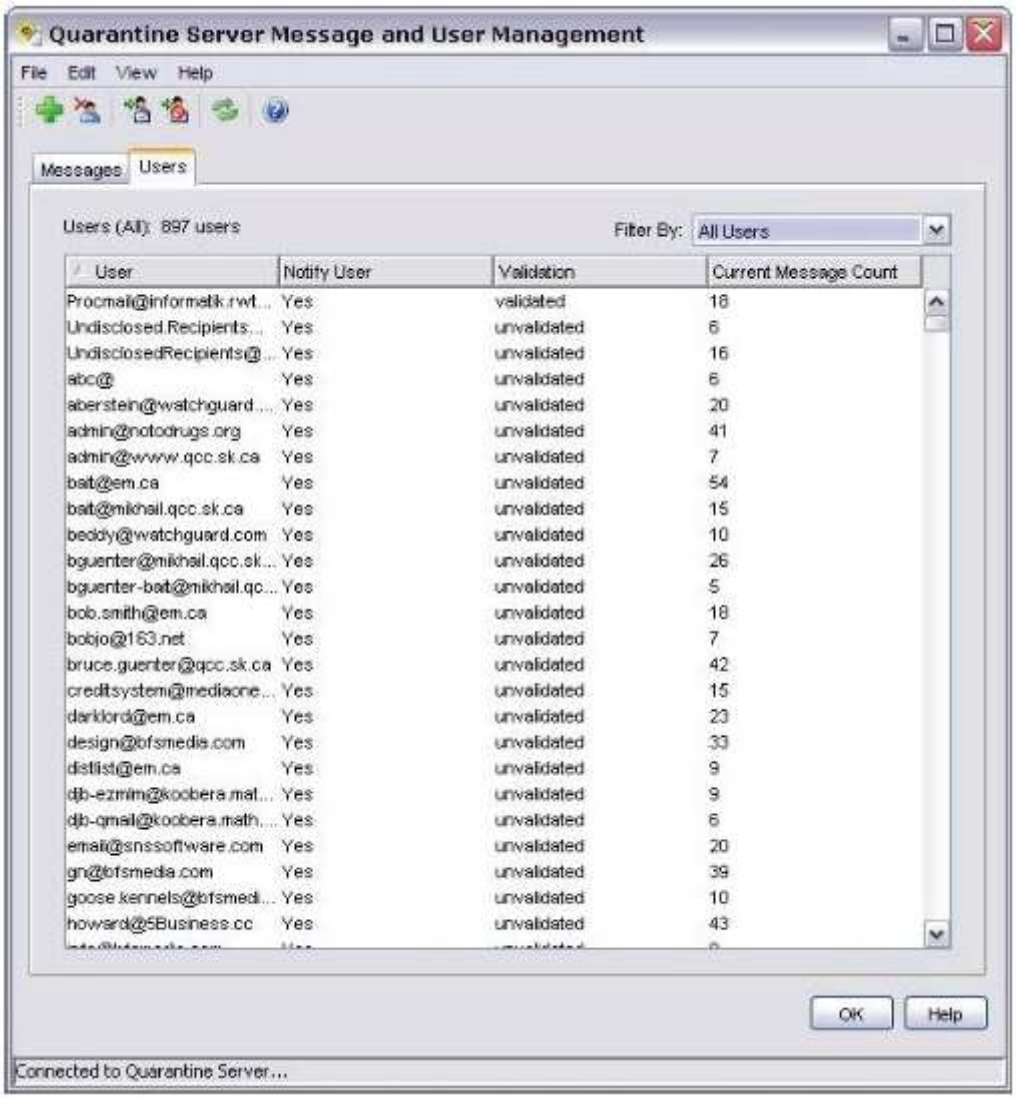
Вы также можете использовать соответствующие иконки для этих опций.

Управление пользователями

Сервер Карантина содержит список пользователей, сообщения которых были помещены в карантин. При помощи клиента Сервера Карантина вы можете просматривать список пользователей, удалять их и изменять их параметры уведомлений.

Просмотр списка пользователей Сервера Карантина

Для того чтобы запустить клиент Сервера Карантина выберите в WatchGuard System выберите **Tools > Quarantine Server Clien**t. В диалоговом окне **Quarantine Server Message and User Management** выберите закладку **Users**.



Закладка **Users** содержит следующую информацию:

- Электронные адреса пользователей, сообщения которых были помещены в карантин.
- Настройки уведомлений пользователей.
- Список валидных и невалидных пользователей. Пользователь утвержден в том случае, если он имеет сообщение о том, что он имеет сообщения на Сервере Карантина в своем почтовом клиенте, и пользователи, имеющие ссылку для перехода на Сервер Карантина. Некоторые пользователи shown on Серверу Карантина никогда не будут утверждены,

потому что их электронные адреса созданы спамером или являются существующими(реальными) пользователями.

Число сообщений на данный момент на Сервере Карантина, адресованных этим пользователям. Если вы хотите просмотреть только утвержденных/неутвержденных пользователей в выпадающем списке **Filter by** выберите **Validated Users** или **Unvalidated Users**.

Добавление пользователей

Пользователи, сообщения которых были помещены в карантин, автоматически добавляются в базу Сервера Карантина. Для добавления пользователей вручную см. процедуру, приведенную ниже.

1. Запустите клиент Сервера Карантина.
   Откроется диалоговое окно Quarantine Server Message and User Management.

2. В диалоговом окне **Quarantine Server Message and User Management** выберите закладку **Users**.

3. Выберите **Edit** > **Add User**.
   Откроется диалоговое окно Add User

4. Введите полный адрес электронной почты пользователя, например as name@example.com.

5. Выберите переключатель **Send notification for this user** или **Do not send notification** для того чтобы уведомлять или не уведомлять пользователя о том, что его Сервер Карантина получил сообщение, предназначенное ему.

6. Нажмите **OK**.

Удаление пользователей

После того, как вы удалите пользователя, все его сообщения также будут удалены с сервера.

1. В диалоговом окне **Quarantine Server Message and User Management** выберите закладку **Users**.

2. Выберите пользователя, которого вы хотите удалить, и нажмите  . Или выберите **Edit > Delete**.

Изменение параметров уведомлений пользователя

Вы можете автоматически уведомлять пользователей, когда их сообщение попадает на Сервер Карантина.

1. В диалоговом окне **Quarantine Server Message and User Management** выберите закладку **Users**.

2. Для того чтобы включить уведомления для пользователя, выберите его из списка и нажмите . Или выберите **Edit** > **Notify User** > **Yes**.

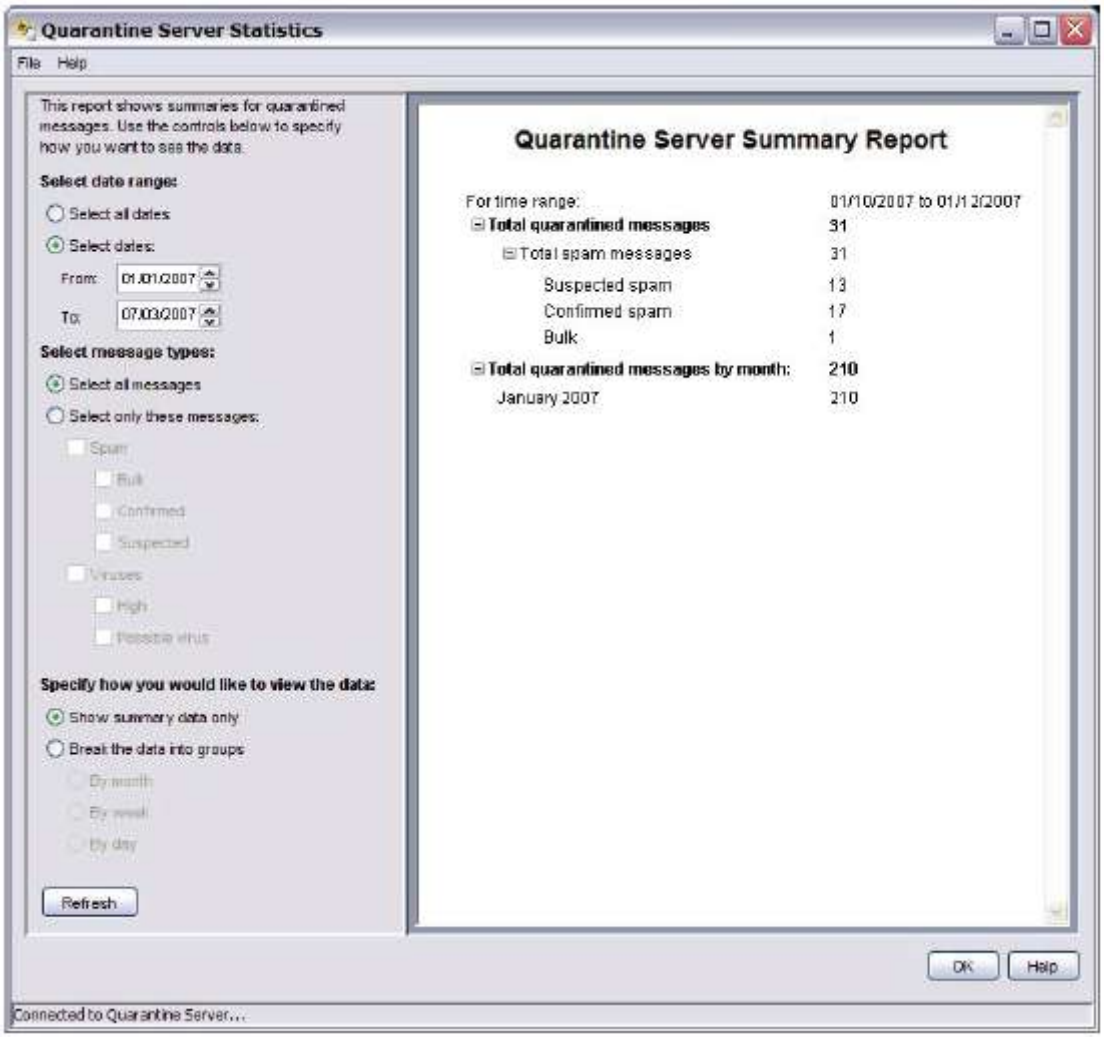
3. Для того чтобы отключить уведомления для пользователя, выберите его из списка и нажмите . Или выберите **Edit** > **Notify User** > **No.**

Статистика по работе Сервера Карантина

Статистика Сервер Карантина включает общее количество сообщений, причины, по которым сообщения были помещены в карантин и количество сообщений, которые были удалены автоматически или вручную. Посмотреть эту статистику вы можете при помощи клиента Сервера Карантина.

1. Для того чтобы запустить клиент Сервера Карантина выберите в WatchGuard System выберите **Tools > Quarantine Server Clien**t
   Откроется диалоговое окно Quarantine Server Message and User Management.

2. В диалоговом окне **Quarantine Server Message and User Management** выберите **View** > **Statistics**.



Просмотр статистики за определенные даты

Вы можете установить отграничение статистики в определенном промежутке времени:

1. Из диалогового окна **Quarantine Server Statistics** выберите переключатель **Select dates.**

2. Введите даты начала и окончания в полях **From и To.**

Просмотр статистики по определенным типам сообщений

Вы можете установить просмотр статистики только таких сообщений, как: подозрительные на спам, подтвержденный спам, часть рекламного предложение, а также содержащие или возможно содержащие вирусы. Выберите переключатель **Select only these messages, затем** выберите тип или типы сообщений, которые необходимо просмотреть.

Группировка статистики по месяцу, неделе или дню

По умолчанию отображаются только краткие данные. Вы можете сгруппировать данные за месяц, неделю или день.

1. Из диалогового окна Quarantine Server Statistics выберите переключатель **Break the data into groups**.

2. Выберите один из переключателей: **By Month**, **By Week**, или **By Day.**

Экспорт и печать статистических данных

Для экспорта статистики Сервера Карантина в таблицу Microsoft Excel (формат .xls) необходимо из диалогового окна **Quarantine Server Statistic**s выбрать **File > Export to Excel.**

Для экспорта статистики Сервера Карантина в CSV формат – из диалогового окна **Quarantine Server Statistics** выберите **File > Export to Csv**.

Печать статистики Сервера Карантина осуществляется таким образом: из диалогового окна **Quarantine Server Statistics** выберите **File > Print.**