RAINBOW SECURITY

ОПИСАНИЕ ПРОДУКЦИИ
компании WatchGuard

Версия документа 1.02 (май 2010)

Оглавление:

1. О компании WatchGuard

Компания WatchGuard Technologies начала свою деятельность в 1996 году, выпустив первое в мире аппаратное решение для защиты межсетевого пространства, во многом предопределив понятие Интернет-защиты. Спустя всего год в программно-аппаратных комплексах WatchGuard впервые стала использоваться технология Application Proxy (прокси-фильтрация), которая в отличие от пакетной фильтрации позволяет анализировать все семь уровней модели OSI (включая сеансовый, прикладной и уровень представления).

В 2003 году WatchGuard реализовал в своем оборудовании концепцию UTM (Unified Threat Management, или «Объединенное Управление Угрозами») – защиты путем объединения в одном «ящике» функций разных устройств: межсетевого экрана, системы обнаружения и предотвращения вторжений в сеть, а также функций антивирусного шлюза. За три года WatchGuard стал уверенным лидером отрасли UTM-устройств.

Постоянно совершенствуя свои продукты, в 2009 году WatchGuard предложил рынку новый стандарт безопасности – XTM (Extensible Threat Management) устройства, в которых улучшен и расширен ряд функциональных характеристик UTM-устройств, например, добавлена возможность анализировать пакеты протокола HTTPS и осуществлять поддержку VoIP.

Сегодня штат сотрудников компании составляет боле 500 человек, центральная штаб-квартира располагается в городе Сиэтл (США, шт. Вашингтон) с дополнительными офисами в Северной Америке, Европе, Азии и Латинской Америке. Основной принцип работы WatchGuard с клиентами – четко отлаженный трехступенчатый канал дистрибуции, в котором взаимодействует сам производитель, дистрибьютор и реселлер. География распространения решений WatchGuard насчитывает более 150 стран по всему миру. На территории России и стран СНГ с 1999 года официальным дистрибутором WatchGuard является компания Rainbow Technologies.

Официальный сайт компании WatchGuard: http://www.watchguard.com/

Официальный сайт Rainbow Technologies: http://www.rnbo.ru/

2. Описание продуктов

2.1 Мультифункциональные устройства WatchGuard XTM-Series

WatchGuard XTM 1050

Бизнесу, который полагается на высокую производительность и постоянную доступность, обычно приходилось платить высокую цену за то, чтобы сделать компьютерные сети безопасными. Так было до тех пор, пока не появилось новое высокопроизводительное устройство WatchGuard XTM 1050, способное обеспечить полностью расширяемую защиту корпоративного уровня по доступной цене. Это устройство рекомендовано для крупных корпоративных сетей с объемом до 10 000 пользователей! Решения сетевой безопасности «все-в-одном» (XTM) совмещают в себе полную и максимально надежную защиту, сокращение временных затрат и иных вложений, связанных с управлением множества отдельностоящих продуктов безопасности.

С WatchGuard Firebox XTM 1050 ваша сеть это:

Безопасность

- Анализ содержимого на прикладном уровне и блокирование угроз, которые не могут обнаружить межсетевые экраны с сохранением состояния пакетов.
- Защита прокси обеспечивает надежную защиту для протоколов HTTP, HTTPS, FTP, SMTP, POP3, DNS, TCP/UDP.
- Подписки безопасности увеличивают защиту в критических областях для обеспечения всесторонней защиты.
- Интегрированный SSL VPN для простого сетевого доступа откуда угодно, когда угодно.

Высокая мощность

- Межсетевой экран с пропускной способностью 10 Гб/с и производительностью туннелей VPN 2 Гб/с.
- 12 потоковых гигабитных портов Ethernet, с вариантом установки дополнительных 4-х гигабитных оптоволоконных портов.
- Любые из 12-ти портов могут быть настроены на внутреннюю, внешнюю или опциональную (ДМЗ) зону для максимального использования сетевых ресурсов.
- Управление кластером из двух устройств как единой логической единицей, с вариантами установки отказоустойчивости и балансировки нагрузки, которая почти удваивает производительность одного устройства.

Эффективность

- Интерфейс командной строки CLI с поддержкой скриптов позволяет упростить интеграцию в существующую инфраструктуру для быстрого подключения.
- Интерактивный мониторинг и построение отчетов в режиме реального времени – без дополнительных вложений – позволяет достичь беспрецедентной наглядности

сетевой безопасности, для того чтобы вы могли незамедлительно предпринять превентивные и корректирующие действия.
- Интуитивная консоль управления позволяет централизованно управлять всеми функциями безопасности.
- Контроль доступа на основе ролей (RBAC) позволяет администратору создавать специализированные роли для усиления контроля.
- Создание VPN соединений типа «офис-офис» - три клика мышью и удаленный офис подключен.

Гибкость
- Безопасность голосовых звонков VoIP означает, что вам не надо «тянуть провода в обход межсетевого экрана» для извлечения выгоды из использования VoIP.
- Динамическая маршрутизация и управление формой трафика позволяют максимально увеличить гибкость и эффективность вашей сети.
- Маршрутизация на основе политик позволяет указать исходящий интерфейс для каждой службы, для контроля над пропускной способностью канала и снижения затрат.
- Балансировка нагрузки между серверами позволяет с легкостью защитить публичные коммерческие «фермы серверов».
- Выравнивание нагрузки между двумя внешними соединениями, отказоустойчивый кластер (Активный/Пассивный и Активный/Активный), переключение резервных каналов WAN и туннелей VPN в случае отказа способствуют повышению производительности, отказоустойчивости и надежности.
- Различные виды VPN для гибкости при удаленном доступе.

Исчерпывающая защита
- Многоуровневая, взаимосвязанная безопасность призвана защитить вашу сеть.
- Мощность и производительность позволяет обрабатывать огромные объемы трафика.
- Интуитивное централизованное управления предоставляет необходимый контроль для эффективного управления.
- Расширенные сетевые функции, которые позволяют вам убедиться, что сеть гладко работает.

Технические спецификации XTM 1050

Межсетевой экран	Межсетевой экран с запоминанием состояния, глубокая проверка на уровне приложений, прокси-фильтры прикладного уровня
Фильтры прикладного уровня	HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3
Защита от угроз	Блокирование шпионских приложений, атак на отказ в обслуживании, фрагментированных и искаженных сетевых пакетов и многое другое
VoIP	H.323. SIP, безопасность размещения и сессий
SpamBlocker	Доступно в комплектации Security Bundle
WebBlocker	Доступно в комплектации Security Bundle
Шлюзовой антивирус	Доступно в комплектации Security Bundle
Система защиты от вторжений	Доступно в комплектации Security Bundle

VPN и аутентфиикация	
Шифрование	DES, 3DES, AES 128-, 192-, 256-бит
IPSec	SHA-1, MD5, общий ключ IKE, сторонние сертификаты
SSL	Наличие тонкого клиента
PPTP	Сервер и транзитная передача
Режим переключения VPN	Да
Single Sign-on	XAUTH Radius, LDAP, Windows Active Directory Сквозная аутентификация в Active Directory
Other User Authentication	VASCO, RSA SecurID, Web-based, Local
Производительность МЭ	10 Гб/с
Производительность VPN	2 Гб/с
Количество одновременных сессий	2,500,000
Количество IP адресов хостов в сети (LAN IP)	Без ограничений
VPN Офис – Офис (BOVPN)	7,000
MU VPN – IPSec (вкл/макс)	15,000
Сетевые функции	
Операционная система	Fireware® XTM Pro
Назначение IP-адресов	Статическое, DynDNS, PPPoE, DHCP (сервер, клиент, ретрансляция)
Маршрутизация	Статическая, динамическая (BGP4, OSPF, RIP v1/2), на основе политик (PBR)
Поддержка VLAN	500 VLAN: режимы моста, тегирования, маршрутизации
Режим работы в кластере	Активный/Пассивный, Активный/Активный с распределением нагрузки
NAT	Статический, динамический, 1:1, на основе политик, транзит IPSec, виртуальные IP-адреса для балансировки нагрузки на сервера
Другие функции	Независимость портов, прозрачный режим работы, режим переключения канала WAN при отказе основного, балансировка нагрузки на сервера, балансировка нагрузки между несколькими каналами WAN
Платформа управления	WatchGuard System Manager (WSM) v11
Уведомления	SNMP v2/v3, e-mail, оповещения системы управления

Сервера	Логирование, Отчеты, Карантин, WebBlocker, Централизованное управление
WEB-интерфейс	Для управления с помощью самых распространенных браузеров с Windows, Mac, Linux и Solaris OS
Интерфейс командной строки	Для прямого подключения и создания скриптов

WatchGuard XTM 8 Series

Новая линейка устройств XTM-8 идеально подходит для крупных офисов и штаб-квартир с общим числом пользователей до 5000 человек. У устройств WatchGuard XTM 8 Series пропускная способность МЭ достигает 5 Гб/с, встроено 10 интерфейсов 10/100/1000. Также этим устройствам присущи свойства XTM-класса: полноценная контентная инспекция HTTPS, опциональные URL фильтрация, антиспам, шлюзовой антивирус и система предотвращения вторжений. Гибкие инструменты централизованного управления позволяют администраторам контролировать множество устройств, проводить мониторинг в реальном масштабе времени и создавать огромный спектр отчетов. Отказоустойчивый кластер (active/active), горячее переключение между WAN соединениями, балансировка нагрузки и технологии виртуализации позволяют достичь максимальной надежности и производительности.

Безопасность

- Анализ содержимого на прикладном уровне и блокирование угроз, которые не могут обнаружить межсетевые экраны с сохранением состояния пакетов.
- Полноценная защита прокси обеспечивает надежную защиту для протоколов HTTP, HTTPS, FTP, SMTP, POP3, DNS, TCP/UDP.
- Набор подписок безопасности увеличивает защиту в критических областях для обеспечения полного управления угрозами.
- Интегрированный SSL VPN для простого сетевого доступа: откуда угодно, когда угодно.

Высокая мощность и эффективность

- Межсетевой экран с пропускной способностью 5 Гб/с и производительностью туннелей VPN 1,7 Гб/с.
- Даже со всеми включенными подписками безопасности XTM пропускная способность достигает отличного показателя по отрасли – 1,2 Гбит/с.
- 10 гигабитных портов Ethernet поддерживают высокую скорость сетевой инфраструктуры и гигабитные подключения WAN.
- Активный/Активный отказоустойчивый кластер с функцией балансировки нагрузки гарантирует максимальное время работы без простоя.
- Интерфейс командной строки CLI с поддержкой скриптов позволяет упростить интеграцию в существующую инфраструктуру.

- Интерактивный мониторинг и построение отчетов в режиме реального времени. Без дополнительных вложений позволяет достичь беспрецедентной наглядности сетевой безопасности, для того, чтобы Вы могли незамедлительно предпринять превентивные и корректирующие действия.
- Интуитивная консоль управления позволяет централизованно управлять всеми функциями безопасности.
- Контроль доступа на основе ролей (RBAC) позволяет администратору создавать специализированные роли для разграничения контроля.
- Создание VPN соединений типа «офис-офис» - три клика мышью и удаленный офис подключен.

Гибкость

- Безопасность голосовых звонков VoIP означает, что Вам не надо «тянуть провода в обход межсетевого экрана» для извлечения выгоды из использования VoIP.
- Переключение резервных каналов WAN и VPN в случае отказа способствуют повышению производительности, отказоустойчивости и надежности.
- Различные виды VPN для гибкости при удаленном доступе.
- Любые из 10 портов могут быть настроены на внутреннюю, внешнюю или опциональную (DMZ) зону для максимального использования сетевых ресурсов.
- Такие расширенные сетевые функции, как режим прозрачного моста и широковещание на канале VPN позволяет наращивать безопасность без необходимости изменения существующей сетевой инфраструктуры.

Масштабируемость

- Простое добавление лицензии позволяет обновить программно-аппаратный комплекс до старшей модели в рамках продуктовой линейки, что ведет к увеличению производительности и пропускной способности.
- Добавление дополнительных подписок безопасности для блокирования спама, контроля опасных и недопустимых сетевых ресурсов, защиты от сетевых вторжений и предотвращения попадания в локальную сеть вирусов, троянов, шпионских средств и других вредоносных приложений на уровне шлюза.

Будьте готовы к перспективам нового дня

- Нет необходимости жертвовать безопасностью ради высокой производительности или наоборот. Многоуровневая совместимая безопасность защищает сеть, не снижая производительность.
- Расширенные сетевые функции гарантируют надежность и гибкость, необходимые бизнесу.
- Безопасное удаленное подключение позволяет мобильным рабочим станциям оставаться в режиме онлайн и поддерживать работоспособность.

Инструменты безопасности и построения отчетов, включенные в комплект поставки, без дополнительных затрат, позволяют поддержать отраслевые и нормативные стандарты.

Модельный ряд и детализированные спецификации

Характеристики	XTM 810	XTM 820	XTM 830
Пропускная способность межсетевого экрана	3 Гб/с	4 Гб/с	5 Гб/с
Пропускная способность VPN*	1 Гб/с	1.4 Гб/с	1.7 Гб/с
Пропускная способность XTM	850 Мб/с	1 Гб/с	1.2 Гб/с
Интерфейсы 10/100/1000	10	10	10
Количество одновременных сессий	500.000	750.000	1.000.000
Число поддерживаемых LAN IP-адресов	неогр.	неогр.	неогр.
Количество поддерживаемых VLAN*	200	300	400
Число туннелей офис-офис BOVPN	1000	2000	6000
Число туннелей Mobile VPN IPSec *(вкл/макс)*	600/2000	700/6000	800/8000
Число туннелей Mobile VPN SSL	1000	4000	6000
Число туннелей Mobile VPN PPTP	50	50	50
Максимальное число локальных аутентифицированных пользователей	400	500	600
Возможность модернизации до старшей модели	да	да	нет

Безопасность

Межсетевой экран — Межсетевой экран с запоминанием состояния, глубокая проверка на уровне приложений, прокси-фильтры прикладного уровня

Фильтры прикладного уровня — HTTP, HTTPS, SMTP, FTP, DNS, TCP, POP3, TCP-UDP

Защита от угроз — Блокирование шпионских приложений, атак на отказ в обслуживании, фрагментированных и искаженных сетевых пакетов, смешенных угроз и многое другое

VoIP — H.323. SIP, безопасность размещения и сессий

SpamBlocker — Доступно в комплектации Security Bundle

WebBlocker — Доступно в комплектации Security Bundle

Шлюзовой антивирус — Доступно в комплектации Security Bundle

Система защиты от вторжений — Доступно в комплектации Security Bundle

VPN и аутентификация

Шифрование — DES, 3DES, AES 128-, 192-, 256-бит

IPSec — SHA-1, MD5, общий ключ IKE, сторонние сертификаты

SSL — Наличие тонкого клиента, web exchange

PPTP — Сервер и транзитная передача

Режим переключения VPN	Да
Single Sign-on	Сквозная аутентификация в Active Directory
XAUTH	Radius, LDAP, Windows Active Directory
Другая аутентификация Пользователей	VASCO, RSA SecurID, Web-based, локальная база

Сетевые функции

Операционная система	Fireware XTM Pro
Назначение IP-адресов	Статическое, DynDNS, PPPoE, DHCP (сервер, клиент, ретрансляция)
Маршрутизация	Статическая, динамическая (BGP4, OSPF, RIP v1/2), на основе политик (PBR)
Поддержка VLAN	VLAN: режимы моста, тегирования, маршрутизации
Режим работы в кластере	Активный/Пассивный, Активный/Активный с распределением нагрузки
NAT	Статический, динамический, 1:1, на основе политик, транзит IPSec, виртуальные IP-адреса для балансировки нагрузки на сервера
Другие функции	Независимость портов, прозрачный режим работы, режим переключения канала WAN при отказе основного, балансировка нагрузки на сервера, балансировка нагрузки между несколькими каналами WAN

Управление

Платформа управления	WatchGuard System Manager (WSM) v11 или выше
Сигналы и Уведомления	SNMP v2/v3, e-mail, оповещения системы управления
Серверы	Сервер логирования, отчетов, карантина, централизованного управления и база WebBlocker
WEB-интерфейс	Для управления с помощью самых распространенных браузеров с Windows, Mac, Linux и Solaris OS
Интерфейс командной строки	Для прямого подключения и создания скриптов

WatchGuard XTM 5 Series

Устройства WatchGuard XTM 5 Series предоставляют новый класс высокопроизводительной безопасности для растущих предприятий среднего бизнеса.

- Производительность – 2.3 Gb/s МЭ и до 800 Mb/s XTM.
- 7 Ethernet портов включая 6 GbE
- 4 модели в линейке.
- ОС – Fireware XTM 11.2.1 – с возможностью блокирования Skype.
- Управление – WSM 11.2.1, включая улучшения MSSP.
- Лучшая цена на рынке!

Модельный ряд и детализированные спецификации

	XTM 505	XTM 510	XTM 520	XTM 530
Пропускная способность межсетевого экрана*	850 Mbps	1.4 Gbps	1.9 Gbps	2.3 Gbps
Пропускная способность VPN*	210 Mbps	350 Mbps	550 Mbps	750 Mbps
Пропускная способность XTM*	275 Mbps	400 Mbps	600 Mbps	800 Mbps
Интерфейсы 10/100	1 copper	1 copper	1 copper	1 copper
Интерфейсы 10/100/1000	6 copper	6 copper	6 copper	6 copper
Интерфейсы I/O	1 Serial, 2 USB	1 Serial, 2 USB	1 Serial, 2 USB	1 Serial, 2 USB
Число поддерживаемых LAN IP-адресов	неогр.	неогр.	неогр.	неогр.
Количество одновременных сессий (bi-directional)	40,000	50,000	100,000	350,000
Число VLAN (bridging, tagging, routed mode)	75	75	75	75
Максимальное число локальных аутентифицированных пользователей	500	500	1,000	2,500
VPN туннели				
VPN для филиалов	65	75	200	600
Mobile VPN IPSec (incl/max)	5/75	25/100	50/300	400/1,000
Mobile VPN SSL (included/max)	1/65**	1/75**	1/300**	1/600**
PPTP	50	50	50	50

* Значения пропускной способности может варьироваться в зависимости от конкретной среды и конфигурации.

* * Возможное максимальное число при апгрейде на Fireware XTM Pro

WatchGuard XTM 2 Series

Устройства WatchGuard® XTM 2 Series firewall/VPN предоставляют высокую степень безопасности для малого бизнеса и удаленных филиалов без серьезных затрат на оборудование.

- Лучшее решение для небольших офисов и малого бизнеса.
- 6 Ethernet портов, включая 3 GbE
- Двухдиапазонный Wireless-N (802.11 a/b/g/n)
- Производительность до 190 Mb/s МЭ и 40 Mb/s XTM.

Модельный ряд и детализированные спецификации

	XTM 21/21-W	XTM 22/22-W	XTM 23/23-W
Пропускная способность межсетевого экрана *	110 Mbps	150 Mbps	195 Mbps
Пропускная способность VPN*	35 Mbps	55 Mbps	55 Mbps
Пропускная способность XTM*	18 Mbps	30 Mbps	40 Mbps
Интерфейсы 10/100	3 copper	3 copper	3 copper
Интерфейсы 10/100/1000	3 copper	3 copper	3 copper
I/O интерфейсы	2 USB	2 USB	2 USB
Число поддерживаемых LAN IP-адресов	неогр.	неогр.	неогр.
Количество одновременных сессий (bi-directional)	10,000	20,000	30,000
Число VLAN (bridging, tagging, routed mode)	20, upgradeable to 50 with Fireware XTM Pro upgrade	20, upgradeable to 50 with Fireware XTM Pro upgrade	50
Максимальное число локальных аутентифицированных пользователей	100	200	200
VPN туннели			
VPN для филиалов	5	20	50
Mobile VPN IPSec (incl/max)	1/11	5/25	5/55
Mobile VPN SSL (included/max)	1/11**	1/25**	55/55
PPTP	50	50	50

* Значения пропускной способности может варьироваться в зависимости от конкретной среды и конфигурации.
* * Возможное максимальное число при апгрейде на Fireware XTM Pro.

2.2 Мультифункциональные устройства e-Series

Firebox X Edge e-Series

Аппаратно-программный комплекс создан специально для обеспечения надежной защиты сетей предприятий малого бизнеса и удаленных офисов/филиалов и сотрудников. Рекомендуемая производителем максимальная емкость сетевых подключений составляет 50 пользователей. Пропускная способность межсетевого экрана составляет 100 мегабит в секунду. Линейка Edge представлена проводными и беспроводными моделями. Беспроводные модели включают в себя весь функционал аналогичных проводных моделей и имеют дополнительную функцию WAP (802.11b/g) для подключения беспроводных пользователей с помощью технологии Wi-Fi. Такие возможности Firebox серии Edge особенно актуальны в современном бизнесе, где виртуализация офисов уже не дань моде, а жизненная необходимость.

Firebox X Edge - решение на основе расширяемой платформы, адаптируемое к растущим потребностям информационной безопасности. Firebox X Edge позволяет использовать лицензионные ключи для своей модернизации, то есть получить большую производительность, пропускную способность и функционал старших моделей внутри линейки без дорогостоящей замены оборудования. Firebox серии Edge легко использовать даже тем, у кого небольшой опыт эксплуатации сетей!

Модельный ряд

Характеристики	Firebox X10e/X10e-W	Firebox X20e/X20e-W	Firebox X55e/X55e-W
Возможность модернизации до старшей модели	до X20e или X55e/ до X20e-W или X55e-W	до X55e/ до X55e-W	N/A N/A
Пропускная способность межсетевого экрана	100 Mbps	100 Mbps	100 Mbps
Пропускная способность VPN*	35 Mbps	35 Mbps	35 Mbps
Шлюзовой антивирус / Система предотвращения вторжений *(GAV/IPS)*	дополнительно	дополнительно	дополнительно
Фильтрация URL *(WebBlocker)*	дополнительно	дополнительно	дополнительно
Блокирование спама *(SpamBlocker)*	дополнительно	дополнительно	дополнительно
Последовательный порт	1	1	1
Интерфейсы 10/100	6	6	6
Количество одновременных сессий	6 000	8 000	10 000
Число поддерживаемых LAN IP-адресов	15 (расш. до 20)	30	неогр.

Число туннелей офис-офис BOVPN *(вкл/макс)*	5	15	25
Число туннелей Mobile VPN IPSec *(вкл/макс)*	1/11	5/25	5/55
Число туннелей Mobile VPN SSL *(вкл/макс)*	1/11	1/25	55/55
Число туннелей Mobile VPN PPTP *(вкл/макс)*	10/10	10/10	10/10
Максимальное число аутентифицированных пользователей	200	200	200
Улучшенный функционал Edge Pro *(*)*	дополнительно	дополнительно	включительно

* пропускная способность будет зависеть от конфигурации и окружения.

Проводные модели:

- **Firebox® X55e** предназначен для удалённых офисов и сетей предприятий малого бизнеса до 50 пользователей и включает в себя лучший в своём классе межсетевой экран, VPN, фильтрацию URL (дополнительно) и улучшенные возможности управления сетью.

- **Firebox® X20e** предназначен для малых сетей до 30-ти пользователей. Это устройство является идеальным выбором для создания VPN тоннеля в филиале, соединенном с центральным офисом, использующим Firebox® X Core™ или Peak™. Такое подключение позволяет дистанционно централизованно управлять функционалом Edge при помощи системы управления WatchGuard System Manager. Модель предусматривает модернизацию до Firebox X55e путем загрузки лицензионного ключа.

- **Firebox® X10e** предназначен для малых сетей до 20-ти пользователей, которым необходим элементарно устанавливаемый межсетевой экран и VPN для быстрого и легкого соединения с центральным офисом. Он обладает лучшей в своем классе производительностью и возможностью разделять домашнюю и рабочую сеть. Модель предусматривает модернизацию до Firebox X20e или X55e путем загрузки лицензионного ключа.

Функциональные характеристики

Firebox X Edge e-Series включает в себя:

- Динамический пакетный межсетевой экран (Firewall) с запоминанием состояний и функциями VPN.
- Функция поддержки VoIP.
- Простую систему установки и управления политиками безопасности, основанную на приложениях.
- Функцию фильтрации сетевого трафика на прикладном уровне (опционально).
- Шлюзовой антивирус (опционально).
- Блокирование спама (опционально).
- Систему предотвращения вторжений
- Расширенные сетевые функции, такие как: WAN failover, приоритезация и управление трафиком.
- Защита сети при помощи входящих в комплект IPSec VPN клиентов, а так же WPA или WEP (только беспроводные модели).
- Систему разделения домашних/рабочих сетей для домашних офисов.
- Поддержку DNAT, NAT 1 к 1 и PAT.
- Поддержка различных способов аутентификации.

- Шесть сетевых портов для соединения с различными устройствами в сети.
- Возможность централизованного управления WatchGuard System Manager.
- Продлеваемую 90-дневную подписку на службу LiveSecurity Service.

VPN
- Шифрование (DES, 3DES)
- IPSec
- SHA-1, MD5
- IKE - Pre-Shared Key, сертификат Firebox
- IPSec транзит
- PPTP транзит
- Определение неработающего соединения (Dead Peer Detection)

Аутентификация пользователя
- XAUTH
  - ✓ LDAP
  - ✓ Windows Active Directory
- Локальная аутентификация
- Windows NT
- Windows 2000
- Windows 2003

Распределение IP-адресов
- Статически
- PPPoE клиент
- DHCP клиент
- DHCP сервер
- Сервис DHCP Relay
- DDNS

Избыточная характеристика
- Горячая замена провайдера
- Число портов - 1

Управление и приоритезация трафика
- Приоритезация трафика
- Приоритезация трафика/QoS
- 4 уровня приоритезации

Трансляция адресов
- PAT, применимый к политикам
- DNAT
- 1:1 NAT
- IPSec T-NAT
- Статический NAT
- До 8 внешних IP-адресов
- Статические маршруты до 100

Логирование / Отчеты
- Syslog
- WebTrends сравнительные отчеты (WELF) (при использовании WSM)
- HTML - отчеты (при использовании WSM)
- Зашифрованный канал логирования (при использовании WSM)

Управляющее ПО
- WatchGuard System Manager (WSM) v. 8.3.1 или выше

- Win32 управляющий интерфейс

ПО на устройстве
- v.10.x и выше

Беспроводные возможности обеспечения безопасности
- Беспроводные гостевые сервисы
- Стандарт 802.11
- WPA, WEP ключи

Firebox X Core e-Series

Firebox серии Core представляет собой следующую после Edge ступень многофункциональной защиты. Рекомендуемая производителем ёмкость сети составляет 50 – 300 компьютеров. Устройства этой серии идеально подходят для предприятий малого, среднего бизнеса и государственных учреждений.
Firebox X Core обеспечивает надежную защиту компьютерной сети, основанную на применении технологии прокси фильтрации. Эта технология позволяет проактивно защищать сеть от различных типов атак, например, переполнение буфера, подделка DNS, DoS, DDoS. В устройствах серии Core действует защита от атак Zero Day, шлюзовой антивирус, программы, противостоящие шпионскому программному обеспечению, блокирование спама, URL-фильтрация и другие. Мощные сервисы безопасности благодаря архитектуре Intelligent Layered Security позволяют организовывать дополнительные уровни сетевой безопасности, обеспечивая целостное, унифицированное решение управления угрозами.

Средства централизованного управления, мониторинга в режиме реального времени, создания единых политик безопасности, централизованного сбора статистики и генерации отчетов существенно упрощают администрирование устройства. Firebox X Core сертифицирован ФСТЭК по 3 классу защищенности.

Модельный ряд

Характеристики	Firebox X550e	Firebox X750e	Firebox X1250e
Пропускная способность МЭ*	300+ Mbps	750 Mbps	1.5Gbps
Пропускная способность VPN	35 Mbps	50 Mbps	100 Mbps
Пропускная способность AV	50 Mbps	70 Mbps	100 Mbps
Шлюзовой антивирус / Система предотвращения вторжений *(GAV/IPS)*	дополнительно	дополнительно	дополнительно
Фильтрация URL *(WebBlocker)*	дополнительно	дополнительно	дополнительно
Блокирование спама *(SpamBlocker)*	дополнительно	дополнительно	дополнительно
Интерфейсы 10/100	4	8	0
Интерфейсы 10/100/1000	0	0	8

Количество поддерживаемых VLAN*	25	25	25
Количество одновременных сессий	25 000	75 000	200 000
Число поддерживаемых LAN IP-адресов	неогр.	неогр.	неогр.
Число туннелей офис-офис BOVPN *(вкл/макс)*	35/45	100/100	600/600
Число туннелей Mobile VPN IPSec *(вкл/макс)*	5/75	50/100	400/400
Число туннелей Mobile VPN SSL *(вкл/макс)*	1/75	1/300	1/500
Число туннелей Mobile VPN PPTP *(вкл/макс)*	50	50	50
Максимальное число аутентифицированных локальных пользователей	250	1 000	5 000
Возможность модернизации до следующей модели	да	да	нет
Улучшенный функционал ОС Fireware Pro	дополнительно	дополнительно	дополнительно

Функциональные характеристики

Firebox® X Core™ e-Series включает в себя:

- Динамический пакетный межсетевой экран (Firewall)с запоминанием состояний;
- VPN.
- Адаптируемую к изменяющимся угрозам архитектуру Intelligent Layered Security.
- Защиту от атак Zero Day.
- Систему предотвращения вторжений (дополнительно).
- Шлюзовой антивирус (дополнительно).
- Систему противодействия шпионскому ПО (дополнительно).
- Анти-спам (дополнительно).
- Фильтрацию URL (дополнительно).
- Систему блокирования спама (дополнительно);
- Операционная система Fireware (с возможностью расширения до Fireware Pro).
- Управляемую антивирусную защиту рабочего места.
- Системный диспетчер WatchGuard® (WSM).
- Продлеваемую 90-дневневную подписку на службу LiveSecurity Service.

Функции безопасности

- МЭ с запоминанием состояний
- Глубокий анализ прокси фильтрами прикладного уровня для протоколов: HTTP, SMTP, FTP, DNS, TCP, POP3, SIP, H323
- Защита от шпионского ПО
- Защита от атак DoS, DDoS, Progressive DoS
- Выявление аномалий протокола
- Поведенческий анализ
- Анализ на соответствие шаблону
- Защита от пересборки фрагментированных пакетов
- Защита от неверно сформированных пакетов
- Статический и динамический списки блокировки ресурсов
- Правила основанные на времени действия
- Управление работой систем обмена мгновенными сообщениями (IM) и контроль работы файлообменных сетей (P2P)

Организация защищенных каналов VPN

- Алгоритмы шифрования (DES, 3DES, AES128, 192, 256-bit)
- IPSec
- SHA-1, MD5
- IKE – Pre-Shared Key, внутренний сертификат Firebox, сторонний сертификат (X.509)
- IPSec транзит
- Доступ мобильных пользователей через тонкий клиент SSL VPN
- PPTP сервер/транзит
- Определение неработающего соединения (RFC 3706)
- Создание VPN соединение методом “Drag-and-Drop”
- Аппаратное шифрование

Аутентификация пользователей

- Прозрачная аутентификация пользователей, SSO клиент
- XAUTH
- LDAP, Windows Active Directory, RADIUS
- ActivIdentity
- VASKO
- RSA SecurID
- Аутентификация на основе Web-формы
- Внутренняя база пользователей

Управление назначением IP адресов

- Статически
- PPoE клиент
- DHCP сервер, клиент, Relay

Функции избыточности и резервирования (HA)**

- Отказоустойчивый кластер (активно/пассивный)
- Автоматическая синхронизация конфигураций
- Автоматическая синхронизация сессий
- Автоматическая синхронизация VPN туннелей

Обход отказа WAN (Multi WAN)

- VPN failover
- Балансировка нагрузки между портами
- Режимы работы Multi WAN (до 4-х портов)
- Переполнение интерфейса **
- Карусельное распределение
- Обход отказа (failover)
- ECMP
- Взвешенное карусельное распределение **

Управление трафиком и приоритезация

- Приоритезация трафика на основе политик
- Маркировка трафика
- IP Services
- Управление качеством обслуживания (QoS)
- 8 очередей приоритета
- Diffserv
- Управление приоритетом очередей

Маршрутизация
- Статическая
- Динамическая **
- BGP4, OSPF, RIP v1, v2
- Маршрутизация на основе политик**

Расширенные сетевые возможности
- Независимое конфигурирование портов
- VLAN (802.11Q) (Bridging, Tagging, Routed Mode)
- Балансировка нагрузки MultiWAN
- Балансировка нагрузки на сервера
- Поддержка VoIP телефонии и видеоконференций H323

Возобновляемые сервисы безопасности
- SpamBlocker – спам фильтрация (POP3, SMTP)
- Карантин спам сообщений
- Защита от вспышек вирусной активности (VOD)
- Шлюзовой антивирус/Система предотвращения вторжений - Gateway AV/IPS, защита от шпионского ПО
- WebBlocker – URL фильтрация (HTTP, HTTPS)

Режимы работы
- Прозрачный/Drop-in (Layer 2)
- Режим маршрутизации (Layer 3)

Трансляция адресов (NAT)
- Статический NAT (Порт форвардинг)
- Динамический NAT
- 1:1 NAT
- Пересылка IPSec через NAT шлюзы (NAT Traversal)
- NAT на основе политик
- Виртуальный IP для балансировки нагрузки на ферму серверов

Журналирование событий / Отчетность
- Сбор и агрегация логов с нескольких устройств
- Форма отчета WebTrends (WELF)
- Отчеты в формате HTML, PDF
- Хранение событий в базе данных SQL
- Шифрование канала передачи событий
- Syslog
- SNMP v2, v3
- Отчет о событиях безопасности и активности пользователей
- Отчет по трафику

Предупреждения / Уведомления
- SNMP v2, v3
- Email
- Через систему управления

Управляющее ПО
- WatchGuard System Manager

Сертификаты
- Common Criteria EAL4
- ICSA

- West Coast Labs
- ФСТЭК по 3-му классу для МЭ

Firebox X Core e-Series

UTM-устройство Firebox® X Peak ™ e-Series обладает наивысшей производительностью среди всех моделей Firebox и отвечает запросам наиболее требовательных политик безопасности. Пропускная способность межсетевого экрана у Peak достигает 2.3 Гбит/сек, а канала VPN – 600 Мбит/сек, поэтому устройства этой серии способны обеспечить надежной защитой сеть, состоящую из более 300 компьютеров. Восемь гигабитных Ethernet-портов обеспечивают бесперебойную работу локальной сети с высокоскоростными каналами передачи данных. Существующая возможность построения защищенных каналов VPN по протоколу SSL позволяет поддерживать круглосуточный доступ удаленных пользователей к сети. Firebox X Peak – это совершенные функции защиты и расширенные сетевые возможности по более привлекательной цене, чем аналогичные продукты, и это идеальный выбор для обеспечения безопасности сложных, разветвлённых высокоскоростных сетей. Все модели серии Peak управляются операционной системой Fireware® XTM Pro, которая позволяет использовать отказоустойчивый кластер в режиме «активный/активный» с распределением нагрузки, обладает поддержкой протоколов динамической маршрутизации, поддержкой VLAN и режимом переключения канала в случае отказа для максимального повышения уровня надежности сети.

Модельный ряд

Характеристики	Firebox X5500e	Firebox X6500e	Firebox X8500e	Firebox X8500e-F
Пропускная способность межсетевого экрана	2.0+ Gbps	2.3 Gbps	2.3 Gbps	2.3 Gbps
Пропускная способность VPN*	400 Mbps	600 Mbps	600 Mbps	600 Mbps
Пропускная способность AV	140 Mbps	170 Mbps	200 Mbps	200 Mbps
Шлюзовой антивирус / Система предотвращения вторжений *(GAV/IPS)*	доп-но	доп-но	доп-но	доп-но
Фильтрация URL *(WebBlocker)*	доп-но	доп-но	доп-но	доп-но
Блокирование спама *(SpamBlocker)*	доп-но	доп-но	доп-но	доп-но
Интерфейсы 10/100/1000	8	8	8	8 (4 - RJ45, 4 - SFP GBIC)
Количество поддерживаемых VLAN*	200	200	200	200
Количество одновременных сессий	500 000	750 000	1 000 000	1 000 000
Число поддерживаемых LAN IP-адресов	неогр.	неогр.	неогр.	неогр.
Число туннелей офис-офис BOVPN *(вкл/макс)*	750/750	750/750	750/750	750/750
Число туннелей Mobile VPN IPSec	600	600	600	600

(вкл/макс)				
Число туннелей Mobile VPN SSL (вкл/макс)	1000/1000	4000/4000	6000/6000	6000/6000
Число туннелей Mobile VPN PPTP *(вкл/макс)*	50	50	50	50
Максимальное число аутентифицированных локальных пользователей	5 000	6 000	8 000	8 000
Возможность модернизации до старшей модели	да	да	нет	нет

- **Firebox® X8500e** предназначен для крупных или распределенных сетей предприятий, которым требуется надежная защита цифровых данных и возможность организации удаленного доступа.
- **Firebox® X8500e-F** применяется в крупных или распределенных сетях предприятий, которые используют оптоволоконные линии.
- **Firebox® X6500e** предназначен для предприятий, которым требуется несколько уровней защиты с централизованным управлением.
- **Firebox® X5500e** используется при построении систем информационной безопасности некрупных предприятий или филиалов, которым требуется интегрированное устройство, имеющее возможность модернизации в соответствии с меняющимися потребностями.

Функциональные характеристики:

Firebox® X Peak™ включает в себя:

- Динамический пакетный межсетевой экран (Firewall) с запоминанием состояний;
- Фильтрацию трафика на уровне приложений (Application Intelligence);
- VPN;
- Защиту от атак Zero Day;
- ILS;
- Предустановленную продвинутую операционную систему FirewarePro;
- Шлюзовой антивирус (дополнительно);
- Систему предотвращения вторжений (дополнительно);
- Систему противодействия шпионскому ПО (дополнительно);
- Анти-спам (дополнительно);
- Фильтрацию URL (дополнительно);
- 10/100/1000 –гигабитную производительность;
- Балансировку нагрузки и/или горячую замену между Интернет провайдерами;
- Динамическую маршрутизацию;
- Систему управления и приоритезации трафика;
- Помощники в настройке конфигураций;
- Оптимальные настройки по умолчанию;
- Логирование и построение отчетов;
- Интерактивный мониторинг в режиме реального времени;
- Возможность создания VPN с помощью пошагового drag-and-drop;
- Продлеваемую 90-дневную подписку на службу LiveSecurity Service.

Функции безопасности

- МЭ с запоминанием состояний
- МЭ с фильтрацией уровня приложений
- Прокси приложения: HTTP, SMTP, FTP, DNS, TCP
- Предотвращение атак DoS и DDoS
- Предотвращение progressive DDoS атак

- Обнаружение аномалий протокола
- Поведенческий анализ атак
- Соответствие образцам атак
- Защита от Fragmented Packet Reassembly
- Защита от неправильно сформированных пакетов
- Статический список блокированных ресурсов
- Динамический список блокированных ресурсов
- Правила, основанные на времени

VPN

- Шифрование (DES, 3DES, AES 128, 192, 256-bit)
- IPSec
  SHA-1, MD5
  IKE - Pre-Shared Key, сертификат Firebox
- PPTP Сервер
- PPTP транзит
- Определение неработающего соединения
- Аппаратное шифрование

Аутентификация пользователя

- XAUTH
  - RADIOS
  - LDAP
- Windows Active Directory
- RSA SecurlID
- WEB - форма
- Локальная аутентификация

Распределение IP- адресов

- Независимо от портов
- Статическое
- PPPoE клиент
- DHCP клиент
- DHCP сервер
- Сервис DHCP Relay
- DDNS клиент

Избыточные характеристики

- Отказоустойчивый кластер*
  в режиме активный/пассивный
  сихронизация конфигурации
  сессионнная синхрогизация
  синхронизация тоннелей VPN
- Горячая замена провайдера
  число портов - 1
  активный/пассивный режимы

Распределение загруженности

- Карусельная схема распределения загруженности
- До 4-х портов

Управление и приоритезация трафика

- Максимальная ширина полос пропускания
- Максимальное количество соединений/сек.
- Приоритезация трафика/QoS*
- 2 уровня приоритезации

Маршрутизация
- Статические маршруты
- RIP v.1, v.2
- BGP4*
- OSPF*

Режим работы
- Прозрачный/drop-in (layer 2)
- Маршрутизируемый (layer 3)

Трансляция адресов
- PAT
- DNAT
- 1:1 NAT
- IPSec T-NAT
- NAT, применимый к политикам

Логирование / Отчеты
- Сбор налогов с нескольких устройств
- WebTrends-совместимые отчеты (WELF)
- HTML - отчеты
- XML - форматы логов
- Зашифрованный канал логирования
- Syslog
- SNMP

Сигналы и уведомления
- SNMP
- По электронной почте
- Сигналы в системе управления
- Сигналы отдельных программ
- Offline конфигурация с графическим интерфейсом пользователя

Управление ПО
- WSM

2.3. Устройства XCS series

WatchGuard XCS 170 и XCS 370

Решения WatchGuard Extensible Content Security (XCS) обеспечивают надежную безопасность на основе стратегии глубокой защиты трафика электронной почты и веб-служб, а также предотвращает утечки данных, расширяя возможности управления рисками. Устройства XCS представлены в шести различных модификациях, в соответствии с требованиями защиты электронной почты для различных по масштабам компаний, и включают в себя решения для обеспечения безопасности наиболее сложных сред электронной почты и Интернет-сетей.

Повышение уровня безопасности при помощи многопротокольной защиты

Устройства WatchGuard XCS обеспечивают масштабируемую защиту данных для почтового и веб-контента. Они гарантируют высочайший уровень безопасности и контроль входящего и исходящего трафика в системах электронной почты и Интернет-сетях. Вы сможете защитить периметр своей сети при помощи комбинации устройств и технологий:

- **WatchGuard Reputation Authority** — это служба мониторинга в режиме реального времени на базе сетевого облака, которая блокирует более 98% нежелательного трафика и угроз с точностью 99,9%;
- **Передовые средства защиты от спама и вредоносного ПО** для фильтрации URL на основе HTTP и HTTPS;
- **Оперативная защита от угроз нулевого часа** обеспечивает самую быструю реакцию на новые угрозы;
- **Постоянная защита электронной почты** предотвращает потерю сообщений;
- **Технология администрирования по принципу «Set It and Forget It» (Установи и забудь)** дает возможность применять одну политику для управления трафиком;
- **Детальная отчетность** предоставляет сведения об уязвимостях в системе безопасности и настраиваемые отчеты для требований аудита.

WatchGuard XCS 170 и XCS 370 это - экономичная технология защиты от спама и вредоносного ПО

Пользователи: компании малого и среднего бизнеса — не более 1000 пользователей.

Вам нужна комплексная защита от спама, вирусов и вредоносного ПО по доступной цене?
Устройства WatchGuard XCS 170 и 370 предлагают наиболее передовую технологию защиты электронной почты для компаний малого и среднего бизнеса. Вы получите мощную систему защиты от спама и угроз в одном удобном устройстве. Подход на основе стратегии глубокой защиты обеспечивает самую высокую эффективность защиты от спама в отрасли (блокируется более 98% спама с точностью 99,9%), а также защиту от вирусов,

комплексных угроз, спуфинга, фишинг-атак и вредоносного ПО. Когда серверы электронной почты обрабатывают только законные, безвредные сообщения, можно сохранить ресурсы полосы пропускания и повысить производительность труда персонала.

Компаниям малого и среднего бизнеса не придется платить высокую цену за эффективную защиту электронной почты.
Устройства WatchGuard XCS 170 и 370 — это доступные по цене комплексные решения, которые защищают от угроз, поступающих вместе с электронной почтой, включая вирусы, спам, комплексные угрозы, фишинг, вредоносное ПО и сетевые атаки. Они блокируют 98% нежелательного трафика по периметру сети, улучшают безопасность электронной почты и повышают производительность без существенных издержек.

Ценность и экономичность в сочетании с глубокой защитой и производительностью.
Устройства WatchGuard XCS обеспечивают лучшую в отрасли защиту от угроз, связанных с электронной почтой, основанной на стратегии глубокой защиты. Надежная, инновационная и высокоэффективная защита электронной почты по доступной цене.

Блокировка 98% угроз и спама по периметру сети WatchGuard Reputation Authority — первая мощная линия обороны от нежелательного и вредоносного входящего трафика, которая предусмотрена во всех устройствах XCS. Она позволяет оптимизировать пропускную способность и освободить сетевые ресурсы для обработки только законного и безвредного трафика.

Многоуровневая защита от спама
Фильтр спама использует многоуровневую технологию анализа входящего трафика для категоризованной взвешенной оценки, предусматривая адаптивные интеллектуальные возможности для блокировки спама с точностью более 99%.

Эффективная защита от вредоносного ПО
Гарантированная защита от вирусов, фишинг-атак, комплексных угроз и вредоносного кода, проникающих в сеть через электронную почту, в режиме реального времени.

Оперативная защита от угроз нулевого часа
Мгновенная блокировка новых и возникающих угроз и самая оперативная защита от атак нулевого часа.

Принцип «Set It and Forget It» (Установи и забудь)
Настройте всего одну политику, и устройство XCS сделает все остальное. Защитите свою электронную почту и позвольте себе сосредоточиться на других приоритетных ИТ-задачах.

Служба LiveSecurity Service
Устройства WatchGuard XCS 170 и 370 предусматривают подписку на инновационную услугу **LiveSecurity Standart Service**, которая активируется через Интернет во время регистрации продукта и предусматривает техническую поддержку только в рабочее время – 12 часов 5 дней в неделю. Она может быть модернизирована до **LiveSecurity Plus Service** , которая предоставляет круглосуточную ежедневную техническую поддержку, обновления и исправления программного обеспечения, а также доступ к информационным ресурсам.

Функции	**XCS 170**	**XCS 370**
	До 500 пользователей	**До 1000 пользователей**
Защита от угроз		
Антиспам	+	+
Блокирование фишинга	+	+
Антивирус/Блокирование вредоносного ПО	+	+
Сервис репутации	+	+

Защита от массовых угроз	+	+
Словари спама	+	+
Фильтры сообщений на основе шаблонов	+	+
Карантин сообщений	+	+
Контроль входящих вложений	+	+
Предотвращение утраты данных		
Контентные правила на основе шаблонов	+	+
Словари соответствия	-	-
Фильтрация нежелательного контента	-	-
Контроль исходящих вложений	-	-
Сканирование исходящего контента и вложений	-	-
Классификация слепков документов и данных	-	-
Шифрование TLS	+	+
Шифрование на уровне сообщений	-	-
Управление и построение отчетов		
Архивирование (стороннее)	+	+
Встроенная система отчетов	+	+
Логирование сообщений	+	+
Настраиваемые подробные политики	+	+
Настраиваемые подробные отчеты	+	+
Централизованное управление	-	-
Отказоустойчивость		
Отказоустойчивость сообщений	-	-
Географическая отказоустойчивость	-	-
Синхронизация почтовых очередей	-	-
Кластеризация по требованию	-	-
Поддержка и обслуживание		
Служба LiveSecurity	стандартная	стандартная
Технические спецификации		
Шасси/процессор		
Форм-фактор	1U Shallow, Для монтажа в стойку	1U Shallow, Для монтажа в стойку
Размеры	1,7”x16,8”x14”	1,7”x16,8”x14”
Вес	17 фунтов	17 фунтов
ЦПУ	Процессор Intel Celeron	Процессор Intel Celeron
Питание	Фиксированное 220 W, универсальное 100/240V	Фиксированное 220 W, универсальное 100/240V
Память		
ОЗУ	2Гб (2 x 1Гб) DDR2 667 МГц	2Гб (2 x 1Гб) DDR3 1066 МГц
Жесткий диск	160 Гб SATA, 7.2K RPM	160 Гб SATA, 7.2K RPM
Возможности подключения		
Сетевые порты	2 Intel Gigabit Ethernet	2 Intel Gigabit Ethernet
Последовательный порт	1 RS-232 (DB-9)	1 RS-232 (DB-9)

WatchGuard XCS 570

Решения WatchGuard Extensible Content Security (XCS) обеспечивают надежную безопасность на основе стратегии глубокой защиты трафика электронной почты и веб-служб, а также предотвращает утечки данных, расширяя возможности управления рисками. Устройства XCS представлены в шести различных модификациях, в соответствии с требованиями защиты электронной почты для различных по масштабам компаний, и включают в себя решения для обеспечения безопасности наиболее сложных сред электронной почты и Интернет-сетей.

Повышение уровня безопасности при помощи многопротокольной защиты

Устройства WatchGuard XCS обеспечивают масштабируемую защиту данных для почтового и веб-контента. Они гарантируют высочайший уровень безопасности и контроль входящего и исходящего трафика в системах электронной почты и интернет-сетях. Вы сможете защитить периметр своей сети при помощи комбинации устройств и технологий:

- **WatchGuard Reputation Authority** — это служба мониторинга в режиме реального времени на базе сетевого облака, которая блокирует более 98% нежелательного трафика и угроз с точностью 99,9%;
- **Передовые средства защиты от спама и вредоносного ПО** для фильтрации URL на основе HTTP и HTTPS;
- **Оперативная защита от угроз нулевого часа** обеспечивает самую быструю реакцию на новые угрозы;
- **Постоянная защита электронной почты** предотвращает потерю сообщений;
- **Технология администрирования по принципу «Set It and Forget It» (Установи и забудь)** дает возможность применять одну политику для управления трафиком;
- **Детальная отчетность** предоставляет сведения об уязвимостях в системе безопасности и настраиваемые отчеты для требований аудита.

WatchGuard XCS 570 это - Защита входящей и исходящей электронной почты и предотвращение утечки данных

Пользователи: компании малого и среднего бизнеса — не более 1000 пользователей

Компании, озабоченные проблемой безопасности входящего и исходящего трафика в своих почтовых сетях, могут воспользоваться преимуществами надежного устройства WatchGuard XCS 570 для защиты от угроз, поступающих вместе с электронной почтой, и обеспечения безопасности контента. Доступное по цене и простое в использовании решение для обеспечения безопасности электронной почты, конфиденциальности и соответствия нормативным требованиям, XCS 570 защищает серверы электронной почты от спама, вирусов, спуфинга, фишинг-атак и шпионского ПО и гарантирует конфиденциальность исходящих почтовых сообщений благодаря мощным средствам предотвращения утечки данных. Централизованное администрирование и отчетность обеспечивают полную прозрачность и контроль всего почтового трафика, снижая общую стоимость владения и упрощая работу.

Комплексное решение для защиты электронной почты, созданное с учетом потребностей компаний среднего бизнеса.
Устройство WatchGuard XCS 570 предоставляет простую в использовании передовую технологию защиты от спама, вирусов, вредоносного ПО, комплексных угроз, шпионских программ, фишинга и сетевых атак. Автоматическое применение политик, обеспечение конфиденциальности и соответствия требованиям предельно упрощаются благодаря готовым словарям соответствия и централизованному управлению, которые предотвращают утечку данных через почтовые каналы.

Блокировка 98% угроз и спама по периметру сети
WatchGuard **Reputation Authority** — первая мощная линия обороны от нежелательного и вредоносного входящего трафика, которая предусмотрена во всех устройствах XCS. Она позволяет оптимизировать пропускную способность и освободить сетевые ресурсы для обработки только законного и безвредного трафика.

Стратегия глубокой защиты для улучшения безопасности
Тщательная проверка контента и контекстный анализ каждого сообщения гарантируют самую надежную защиту почтовой сети от угроз.

Сочетание прозрачности и контроля
Получение комплексного представления о входящем и исходящем почтовом трафике сети для принятия обоснованных решений в области безопасности и устранения уязвимостей в системе защиты электронной почты.

Оперативные средства предотвращения утечки данных для обеспечения конфиденциальности и соответствия нормативным требованиям
Защита важнейших бизнес-ресурсов при помощи автоматизированной технологии предотвращения утечки информации, включающей прозрачное восстановление политик, защиту данных и готовые словари соответствия.

Централизованное администрирование
Централизованная защита, контроль и управление двусторонним почтовым трафиком с единой консоли управления. Обеспечение согласованного применения политик во всей глобальной почтовой сети для усиления защиты и упрощения администрирования.

Постоянная надежная защита
Несколько уровней резервирования и кластеризация по требованию предотвращают потерю сообщений и гарантируют непрерывную и безотказную работу системы защиты электронной почты. Устранение единой точки отказа, уменьшение требований администрирования и обеспечение неограниченного повышения уровней обслуживания.

Служба LiveSecurity Service
Устройства WatchGuard XCS 570 предусматривают подписку на инновационную услугу **LiveSecurity Plus Service**, которая активируется через Интернет во время регистрации продукта. Она предоставляет круглосуточную техническую поддержку, обновления и исправления программного обеспечения, а также доступ к информационным ресурсам.

Функции	**XCS 570**
	До 1000 пользователей
Защита от угроз	
Антиспам	+
Блокирование фишинга	+
Антивирус/Блокирование вредоносного ПО	+
Сервис репутации	+
Защита от массовых угроз	+
Словари спама	+

Фильтры сообщений на основе шаблонов	+
Карантин сообщений	+
Контроль входящих вложений	+
Предотвращение утраты данных	
Контентные правила на основе шаблонов	+
Словари соответствия	+
Фильтрация нежелательного контента	+
Контроль исходящих вложений	+
Сканирование исходящего контента и вложений	+
Классификация слепков документов и данных	+
Шифрование TLS	+
Шифрование на уровне сообщений*	+
Реагирование в прозрачном режиме	+
Управление и построение отчетов	
Архивирование (стороннее)	+
Встроенная система отчетов	+
Логирование сообщений	+
Настраиваемые подробные политики	+
Настраиваемые подробные отчеты	+
Централизованное управление	+
Отказоустойчивость	
Отказоустойчивость сообщений	+
Географическая отказоустойчивость	+
Синхронизация почтовых очередей	+
Кластеризация по требованию	+
Поддержка и обслуживание	
Служба LiveSecurity	LiveSecurity Plus
Технические спецификации	
Шасси/процессор	
Форм-фактор	1U Shallow, Для монтажа в стойку
Размеры	1,7”x16,8”x14”
Вес	17 фунтов
ЦПУ	Процессор Intel Celeron
Питание	Фиксированное 220 W, универсальное 100/240V
Память	
ОЗУ	4Гб (2 x 2Гб) DDR2 667 МГц
Жесткий диск	160 Гб SATA, 7.2K RPM
Возможности подключения	
Сетевые порты	3 Intel Gigabit Ethernet
Последовательный порт	1 RS-232 (DB-9)

*Доступно с WatchGuard XCS Email Encription Subscription

WatchGuard XCS 770, 970 и 1170

Решения WatchGuard Extensible Content Security (XCS) обеспечивают надежную безопасность на основе стратегии глубокой защиты трафика электронной почты и веб-служб, а также предотвращает утечки данных, расширяя возможности управления рисками. Устройства XCS представлены в шести различных модификациях, в соответствии с требованиями защиты электронной почты для различных по масштабам компаний, и включают в себя решения для обеспечения безопасности наиболее сложных сред электронной почты и Интернет-сетей.

Повышение уровня безопасности при помощи многопротокольной защиты

Устройства WatchGuard XCS обеспечивают масштабируемую защиту данных для почтового и веб-контента. Они гарантируют высочайший уровень безопасности и контроль входящего и исходящего трафика в системах электронной почты и интернет-сетях. Вы сможете защитить периметр своей сети при помощи комбинации устройств и технологий:

- **WatchGuard Reputation Authority** — это служба мониторинга в режиме реального времени на базе сетевого облака, которая блокирует более 98% нежелательного трафика и угроз с точностью 99,9%;
- **Передовые средства защиты от спама и вредоносного ПО** для фильтрации URL на основе HTTP и HTTPS;
- **Оперативная защита от угроз нулевого часа** обеспечивает самую быструю реакцию на новые угрозы;
- **Постоянная защита электронной почты** предотвращает потерю сообщений;
- **Технология администрирования по принципу «Set It and Forget It» (Установи и забудь)** дает возможность применять одну политику для управления трафиком;
- **Детальная отчетность** предоставляет сведения об уязвимостях в системе безопасности и настраиваемые отчеты для требований аудита.

WatchGuard XCS 770, 970 и 1170 это - комплексная защита электронной почты и предотвращение утечки данных

Пользователи: крупные предприятия и поставщики услуг Интернета с числом пользователей от 4 000 до 10 000 и более человек

Ориентированные на самые требовательные сети обмена сообщениями, устройства WatchGuard XCS 770, 970 и 1170 XCS представляют собой простые в использовании, комплексные решения для защиты электронной почты, обеспечения конфиденциальности и соответствия нормативным требованиям. Они защищают от угроз, поступающих вместе с электронной почтой, и контролируют исходящий трафик, предотвращая утечку данных. Сеть получает защиту от спама, вирусов, вредоносного ПО, комплексных угроз, шпионских программ, фишинга и сетевых атак, а также автоматизированные возможности защиты контента для контроля и предотвращения утечки информации. Централизованное

администрирование и отчетность снижают затраты на управление, а также обеспечивают полную прозрачность и контроль входящего и исходящего почтового трафика.

Ориентированные на самые требовательные сети обмена сообщениями, устройства WatchGuard XCS 770, 970 и 1170 Extensible Content Security представляют собой простые в использовании решения корпоративного класса для защиты электронной почты, обеспечения конфиденциальности и соответствия нормативным требованиям. Они защищают от угроз, поступающих вместе с электронной почтой, и контролируют исходящий трафик, предотвращая утечку данных. Эти устройства предоставляют самую эффективную технологию защиты электронной почты от спама, вирусов, вредоносного ПО, комплексных угроз, шпионских программ, фишинга и сетевых атак на уровне предприятия, а также автоматизированные возможности защиты контента исходящих сообщений для предотвращения утечки данных электронной почты и веб-служб.

Блокировка 98% угроз и спама по периметру сети
WatchGuard **Reputation Authority** блокирует спам и угрозы прежде, чем они нанесут вред Вашей сети. Эта первая мощная линия обороны от нежелательного и вредоносного входящего трафика предусмотрена во всех устройствах XCS. Препятствуя проникновению спама и Интернет-угроз в сеть, можно оптимизировать пропускную способность и освободить сетевые ресурсы для обработки только законного, безвредного трафика.

Устранение уязвимостей защиты в почтовых и WEB-службах с использованием подписки
Устранение уязвимостей без необходимости в дополнительном оборудовании при помощи XCS **Web Security Subscription (подписка на услуги Интернет-безопасности)**. Объединение защиты входящей и исходящей электронной почты и веб-служб на базе одной платформы. Уменьшение ответственности, связанной с использованием Интернета, и предоставление усовершенствованных средств Интернет-безопасности для обеспечения комплексной защиты электронной почты.

Сочетание прозрачности и контроля
Получение комплексного представления о входящем и исходящем почтовом трафике сети для принятия обоснованных решений в области безопасности и устранения уязвимостей в системе защиты электронной почты.

Оперативные средства предотвращения утечки данных для обеспечения конфиденциальности и соответствия нормативным требованиям
Защита важнейших бизнес-ресурсов при помощи автоматизированной технологии предотвращения утечки информации, включающей прозрачное восстановление политик, защиту данных и готовые словари соответствия.

Централизованное администрирование
Централизованная защита, контроль и управление двусторонним почтовым трафиком с единой консоли управления. Обеспечение согласованного применения политик во всей глобальной почтовой сети для усиления защиты и упрощения администрирования.

Постоянная надежная защита
Несколько уровней резервирования и кластеризация по требованию предотвращают потерю сообщений и гарантируют непрерывную и безотказную работу системы защиты электронной почты. Устранение единой точки отказа, уменьшение требований администрирования и обеспечение неограниченного повышения уровней обслуживания.

Служба LiveSecurity Service
Устройства WatchGuard XCS 770, 970 и 1170 предусматривают подписку на инновационную услугу **LiveSecurity Plus Service**, которая активируется через Интернет во время регистрации продукта. Она предоставляет круглосуточную техническую поддержку,

обновления и исправления программного обеспечения, а также доступ к информационным ресурсам.

Функции	XCS 770 До 4000 пользователей	XCS 970 До 7000 пользователей	XCS 1170 До и более 10 000 польз.
Защита от угроз			
Антиспам	+	+	+
Антивирус/Блокирование вредоносного ПО	+	+	+
Защита от смешанных угроз	+	+	+
Сервис репутации	+	+	+
Защита от массовых угроз	+	+	+
Словари спама	+	+	+
Фильтры сообщений на основе шаблонов	+	+	+
Карантин сообщений	+	+	+
Контроль входящих вложений	+	+	+
Фильтрация URL*	+	+	+
Фильтрация web-контента, не входящего в общепринятые категории*	+	+	+
Предотвращение утраты данных			
Контентные правила на основе шаблонов	+	+	+
Шифрование TLS	+	+	+
Шифрование на уровне сообщений**	+	+	+
Словари соответствия	+	+	+
Фильтрация нежелательного содержимого (Email)	+	+	+
Фильтрация нежелательного содержимого (Web)	+	+	+
Контроль исходящих вложений	+	+	+
Сканирование исходящего контента и вложений	+	+	+
Классификация слепков документов и данных	+	+	+
Реагирование в прозрачном режиме	+	+	+
Управление и построение отчетов			
Архивирование (стороннее)	+	+	+
Встроенная система отчетов	+	+	+
Логирование сообщений	+	+	+
Настраиваемые подробные политики	+	+	+
Настраиваемые подробные отчеты	+	+	+
Централизованное управление	+	+	+
Допустимое использование web-ресурсов*	+	+	+
Контроль web-приложений*	+	+	+
Возможности web-защиты (доступно с Subscription*)			
Фильтрация URL	+	+	+
Фильтрация web-контента, не входящего в общепринятые категории	+	+	+
Допустимое использование web-ресурсов	+	+	+
Контроль web-приложений	+	+	+
Web-кэширование	+	+	+
Загрузки больших файлов с быстрым сканированием	+	+	+
Контроль потокового медиа-контента	+	+	+

Управление web-трафиком и кластеризация	+	+	+
Отказоустойчивость			
Отказоустойчивость на уровне сообщений	+	+	+
Аппаратная отказоустойчивость	-	+	+
Кластеризация по требованию	+	+	+
Синхронизация почтовых очередей	+	+	+
Географическая отказоустойчивость	+	+	+
Поддержка и обслуживание	LiveSecurity Plus	LiveSecurity Plus	LiveSecurity Plus
Технические спецификации			
Шасси/процессор			
Форм-фактор	1U Shallow, Для монтажа в стойку	1U Deep, Для монтажа в стойку	1U Deep, Для монтажа в стойку
Размеры	1,7”x16,8”x14”	1,7”x17,2”x25,6”	1,7”x17,2”x25,6”
Вес	17 фунтов	42 фунта	42 фунта
ЦПУ	Intel Xeon Quad-Core Processor	Intel Xeon Quad-Core Processor	Два Intel Xeon Quad-Core Processor
Питание	Фиксированное 220 W, универсальное 100/240V	Два с горячей заменой, 650W, универсальное 100/240V	Два с горячей заменой, 650W, универсальное 100/240V
Память			
RAID	-	RAID 1	RAID 10
ОЗУ	4Гб (2 x 2Гб) DDR2 667 МГц	4Гб (2 x 2Гб) DDR3 1066 МГц	4Гб (2 x 2Гб) DDR3 1066 МГц
Жесткий диск	160 Гб SATA, 7.2K RPM	Два 160 Гб SATA-II, 7.2K RPM	Четыре 146 Гб SAS, 15K RPM
Возможности подключения			
Сетевые порты	3 Intel Gigabit Ethernet	3 Intel Gigabit Ethernet	3 Intel Gigabit Ethernet
Последовательный порт	1 RS-232 (DB-9)	1 RS-232 (DB-9)	1 RS-232 (DB-9)

* Доступно с WatchGuard XCS Web Security Subscription

**Доступно с WatchGuard XCS Email Encryption Subscription

2.4. Устройство WatchGuard SSL

WatchGuard SSL 100 это доступное, легкое в использование устройство для организации защищенного удаленного доступа, предоставляющее надежную дистанционную работу с корпоративными данными и ресурсами в любое время и в любом месте.

Рекомендовано для предприятий малого и среднего бизнеса с одновременной поддержкой до 100 удаленных пользователей.

Производительность

- Удаленные сотрудники имеют доступ к самым необходимым корпоративным ресурсам, включая e-mail, web-конференции и CRM с любого устройства, поддерживающего web
- Опциональные приложения, включая SSH и RDP могут быть подключены через web-браузер удаленного пользователя для достижения максимальной продуктивности
- Основная конфигурация позволяет конечным пользователям пройти аутентификацию простым двойным щелчком по иконке, далее происходит автоматическая загрузка программы клиента доступа и установка SSL-тоннеля для полного доступа к сетевым базам данных
- Двунаправленное тоннельное соединение позволяет вашей службе поддержки установить соединение с устройством, используемым при доступе удаленным пользователем для устранения возможных технических проблем или обновления программного обеспечения

Простота использования

- Устройство типа «все в одном» - просто подключи и работай – не требует покупки и установки дополнительного программного обеспечения
- После первого подключения пользователи имеют доступ ко всем имеющимся данным на портале - нет необходимости тратить время на повторные аутентификации
- ИТ администраторы получают устройство, которое может быть установлено и готово к работе в кратчайшие сроки
- Функция консолидированного аудита собирает все информацию по доступу, идентификации и системным процессам в центральном хранилище данных для быстрого детального просмотра пользовательской активности

Безопасность

- Комплексная проверка надежности конечной точки доступа гарантирует защиту сети, позволяя конфигурировать и усиливать надежность программной проверкой на вирусы, шпионское ПО, firewall и многими другими функциями устройства
- Очистка сессии удаляет все следы соединения с удаленной точкой доступа, включая удаление файлов и очистку КЭШа, с целью предотвращения утечки данных при следующем входе пользователя в сеть

- Поддержка локальной и сторонней аутентификации, включая усиленную аутентификацию, что гарантирует вход в сеть только авторизированным пользователям и предотвращает проникновение нарушителей

Гибкость

- Возможность входа, как с помощью программы-клиента, так и без, включая поддержку Win 7 и Vista 32-бит. и 64-бит.
- Возможность использования устройства в самой простой конфигурации или ИТ администраторы могут воспользоваться преимуществами проверки чистоты конечной точки доступа, опциональной возможностью отправки JAVA-приложений, двусторонним тоннельным соединением и многим другим.
- Уникальная поддержка любого класса приложений. Администратор может выбирать между публикацией только web-приложений, созданием тоннелей к отдельным ресурсам сети либо отправлять опциональные приложения на компьютер пользователя для более сложного использования
- ИТ администраторы могут интегрировать устройство с существующими сторонними аутентификационными решениями, такими как Microsoft Active Directory, или использовать встроенный LDAP сервер для конфигурации локальной аутентификации, также есть возможность использования встроенной двухфакторной аутентификации включая sms-токены и web-клавиатуры для подтверждения личности пользователя.
- Вся информация, собираемая в логах аудита, может быть представлена в разнообразных графических форматах для текущей или архивной отчетности, а также может быть экспортирована в сторонние программы (Excel, Crystal Reports) для дальнейшего поиска данных и управления активами.

2.5. WatchGuard QMS 500 & 1000

WatchGuard® Quarantine Management Server (QMS) это автоматизированное, интеллектуальное и удобное в использование решение карантина электронной почты, работающее вместе с устройством безопасности электронной почты WatchGuard XCS или любым другим почтовым шлюзом безопасности. Это позволяет перенаправлять сообщения, содержащие нежелательную информацию (спам, фишинг, большие сообщения или сообщения, содержащие вложения) на локальный сервер карантина. Предоставляя безопасное пространство для хранения электронных сообщений, содержащих потенциальные угрозы или спам, WatchGuard QMS дает возможность гибкого контроля и максимальной защиты, позволяя также конечным пользователям самостоятельно регулировать индивидуальные параметры защиты от спама.

Рекомендовано для предприятий средних и больших размеров, а также является идеальным решением для MSSP провайдеров и поставщиков Интернет услуг. Доступны две модели: QMS 500 и QMS 1000.

Спецификация

	QMS 500	**QMS 1000**
Количество пользователей	до 90,000	до 180,000
Пропускная способность	10 млн. сообщений	20 млн. сообщений
Корпус/Процессорr		
Форм-фактор	1U Shallow, Rack-Mountable	1U Deep, Rack-Mountable
Размеры	1.7" (h) x 16.8" (w) x 14" (d)	1.7" (h) x 17.2" (w) x 25.6" (d)
Вес	17 lbs.	42 lbs.
CPU	Intel Dual-Core Processor	Intel Xeon Quad-Core Processor
Питание	Fixed, 200W, universal 100/240V	Two redundant hot-plug, 650W, universal 100/240V
Хранение		
RAID	-	RAID 1
Память	4GB DDR2 RAM	4GB DDR2 RAM
HDD	1 x 500GB SATA	2 x 1TB SATA
Возможности соединения		
Intel Gigabit Ethernet	3 Intel Gigabit Ethernet	4 Intel Gigabit Ethernet
Serial Ports	1 RS-232 (DB-9) Serial Port	1 RS-232 (DB-9) Serial Port
Температура		
Функционирование	32°F to 113°F / 0°C to 45°C	32°F to 113°F / 0°C to 45°C

Хранение	-40°F to 158°F / -40°C to 70°C	-40°F to 158°F / -40°C to 70°C
Относительная влажность		
Функционирование	10% to 85% без конденсации	10% to 85% без конденсации
Хранение	5% to 95% без конденсации	10% to 95% без конденсации
Абсолютная высота		
Функционирование	0 to 9,843 ft (3,000 m)	0 to 9,843 ft (3,000 m)
Хранение	0 to 15,000 ft (4,570 m)	0 to 15,000 ft (4,570 m)