



Сетевая безопасность
 Решения компании Check Point лидируют на рынке средств защиты сетевой инфраструктуры.

Устройства UTM-1

Устройства Check Point UTM-1™ содержат все необходимое для обеспечения безопасности Вашей сети и обеспечивают наиболее комплексную и мощную защиту. Устройства представляют собой универсальные и не требующие сложной настройки решения. В каждое устройство встроено централизованное управление. Предложение Check Point по аппаратному устройству для заказчика включает обновления ПО, гарантию на аппаратное устройство и сервисное обслуживание.



UTM-1 выпускаются с предустановленным комплексным и гибким программным решением. Все устройства UTM-1 могут включать такие программные блейды, как: межсетевой экран, VPN, систему предотвращения вторжений, SSL VPN, защиту от вирусов, программ-шпионов и спама, специализированный межсетевой экран для защиты web-приложений и web-фильтрацию. По желанию, можно добавить другие программные блейды.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

- Проверенные технологии, пользующиеся доверием компаний из списка Fortune 500
- Все необходимое для защиты Вашей сети: функционал, обновления и управление безопасностью
- Защита сетей, систем и пользователей от множества видов атак из Интернета
- Обеспечение конфиденциальности путем защиты удаленного доступа и связи между узлами
- Быстрое и простое развертывание системы безопасности и ее администрирование благодаря наличию многих функций безопасности в одном устройстве и широкой линейке устройств для компаний любого размера - от малого офиса до крупного предприятия
- Защита от появляющихся новых угроз при помощи службы обновлений Check Point Update Service

ВСЕОБЪЕМЛЮЩАЯ ЗАЩИТА

Гибкая архитектура “Программные блейды”:

В UTM-1 применяется революционная архитектура Check Point “Программные блейды”. Данная архитектура - первая и единственная в отрасли, обеспечивающая комплексную, гибкую и управляемую защиту для компаний любого размера. Уникальная способность архитектуры Check Point гибко и быстро расширять возможности системы безопасности обеспечивает заказчикам пониженную совокупную стоимость средств безопасности и рентабельное решение, которое отвечает требованиям сетевой среды сейчас и в будущем.

Программный блейд Firewall: надежный контроль приложений и защита от атак

UTM-1 использует популярный в отрасли межсетевой экран и уже в состоянии поставки обеспечивает проверку тысяч приложений, протоколов и сервисов, в т.ч. систем интернет-сообщений и одноранговых сетей (P2P).

Программный блейд IPSec VPN: простая организация защищенных каналов и удаленный доступ

Применение устройств UTM-1 упрощает создание VPN-туннелей для связи между объектами и удаленного доступа. Вместо ручной настройки каждого туннеля в отдельности и защиты всей VPN-сети можно задать необходимые параметры безопасности всего за один шаг, при этом новые узлы и удаленные пользователи добавляются автоматически. Устройства UTM-1 позволяют Вам предоставлять удаленный доступ в сеть собственным сотрудникам и деловым партнерам с гибким выбором протокола и клиентского приложения VPN.

Программный блейд IPS: передовая система предотвращения вторжений

Программный блейд Check Point IPS обеспечивает лучшую в отрасли комплексную защиту, новые динамичные возможности управления системы предотвращения вторжений и многогигабитную производительность, превосходящие остальные системы IPS. Программный блейд IPS защищает клиента, сервер и операционную систему от угроз, вредоносного кода, «червей» и др., а повышенная производительность Check Point R70 дает заказчикам уникальную возможность упреждающей защиты от угроз при установке блейда IPS на каждый шлюз безопасности. Мощный механизм использует множество различных методов обнаружения и анализа, в том числе: использование сигнатур уязвимостей и попыток их использования, анализ протоколов, выявление аномалий, анализ поведения объектов. Механизм IPS проводит быструю фильтрацию 90% входящего трафика, не требующего тщательной проверки. Глубокий анализ с целью выявления угроз проводится в оставшихся 10% трафика, что снижает нагрузку и повышает эффективность работы системы.

Программный блейд Anti-Virus & Anti Malware: защита от вирусов и шпионского ПО на рубеже шлюза

Средства защиты от вирусов и шпионского ПО на рубеже шлюза являются ключевыми компонентами UTM-1 и дополняют средства защиты настольных рабочих станций. Чтобы остановить вирусы и другое вредоносное ПО на рубеже шлюза, UTM-1 применяет новейший список сигнатур для борьбы с вирусами и шпионскими программами, а также защиту на основе ано-

малий. Трафик служб протоколов POP3, SMTP, FTP и HTTP подвергается антивирусному сканированию в реальном времени для выявления вредоносных элементов, возможно, скрытых среди полезной информации.

Программный блейд Anti-Spam and Email Security: комплексная защита сообщений

Многоуровневый подход, используемый в Check Point UTM-1, обеспечивает безопасность инфраструктуры электронной почты и ее эффективную защиту от спама, вирусов и другого вредоносного ПО.

Защита от нежелательной почты благодаря проверке репутации IP-адреса	Блокировка спама и вредоносного ПО на уровне соединения благодаря проверке репутации отправителя в постоянно обновляемой базе данных IP-адресов
Защита от нежелательных сообщений на основании содержимого	Обеспечивается защита от сложных форм нежелательных сообщений, в том числе сообщений с использованием изображения или текста на иностранном языке
Черные и белые списки	Для запрета отправителей нежелательной почты и для получения почты от надежных отправителей используются списки разрешения или блокирования
Средство защиты от вирусов в электронной почте	Обеспечивается защита от широкого ряда вирусов и вредоносного ПО, включая сканирование содержимого сообщений и вложений
Превентивная защита	Обеспечивается защита от атак с использованием новых нежелательных сообщений и вредоносного ПО с помощью передового механизма сопоставления схем и анализа распределения
IPS для электронной почты	Обеспечивается защита от широкого спектра угроз, включая DoS-атаки и атаки, основанные на переполнении буфера, нацеленные на саму инфраструктуру системы обмена сообщениями

Программный блейд URL Filtering:

Устройства UTM-1 препятствуют посещению сотрудниками посторонних и нежелательных web-сайтов. В UTM-1 встроены средства web-фильтрации, использующие базу данных, насчитывающую свыше 20 миллионов URL-адресов по различным категориям угроз. Предусмотрена возможность задания наиболее подходящей для политики защиты Вашей компании.

Добавление новых программных блейдов Check Point: быстрая адаптация к новым угрозам безопасности

Устройства UTM-1 выпускаются с предустановленным набором программных блейдов. Для соответствия новым и постоянно меняющимся требованиям безопасности, функционал UTM-1 может быть легко и быстро расширен после установки дополнительных программных блейдов, например, таких, как: Web, VoIP, Advanced Networking и Acceleration & Clustering.

ПРОСТОТА И ГИБКОСТЬ

Комплексное готовое решение

С устройством UTM-1 Вы получаете все необходимое для обеспечения сетевой безопасности, в том числе:

- обновления системы безопасности,
- управление безопасностью,
- гарантию на аппаратное устройство.

Встроенное централизованное управление

Устройства Check Point UTM-1 поставляются со встроенной системой управления, которая позволяет управлять несколькими шлюзами Check Point централизованно, с помощью единой консоли. Устройства содержат контейнер управления безопасностью (Security Management container) и следующие программные блейды: Network Policy Management, Endpoint Policy Management и Logging & Status.

Централизованная автоматизированная схема распространения обновлений

Служба Update Services позволяет Вам использовать устройство UTM-1 как упреждающее решение в области безопасности, способное обеспечить защиту сетей от новых атак за счет постоянного и автоматического обновления средств защиты.

Быстрая настройка

Устройства Check Point UTM-1 можно легко настроить с помощью мастера первоначальной настройки. Работа по конфигурированию устройства будет простой:

- подключение кабелей и включение питания,
- выполнение указаний мастера настройки,
- запуск интерфейса средства управления

Технические характеристики устройств

Характеристики безопасности	Подробные сведения о защите
Программный блейд Firewall	
Поддержка протоколов/приложений	Более 200
Защита VoIP	SIP, H.323, MGCP и SCCP с поддержкой NAT
Управление обменом мгновенными сообщениями	MSN, Yahoo, ICQ и Skype
Блокирование подключений «точка-точка»	Kazaa, Gnutella, BitTorrent
Преобразование сетевых адресов (NAT)	Поддержка статической/скрытой трансляции NAT с задаваемыми вручную и автоматически правилами
Программный блейд IPSec VPN	
Поддержка шифрования	AES 128-256 бит, 3DES 56-168 бит
Методы проверки подлинности	Пароль, RADIUS, TACACS, X.509, SecurID
Источник сертификатов	Встроенный удостоверяющий центр (X.509)
Сообщества сетей VPN	Соединения между узлами настраиваются автоматически по мере создания объектов
Поддерживаемые топологии	Звезда и полносвязная сеть
Сеть VPN на основе маршрутов	Используются интерфейсы виртуальных туннелей; нумерованные/ненумерованные интерфейсы
Поддержка клиента VPN	Полная безопасность рабочих станций при помощи VPN и межсетевого экрана для настольных ПК

Характеристики безопасности	Подробные сведения о защите
Удаленный доступ на основе технологии SSL	Полностью встроенный шлюз сети VPN на основе SSL обеспечивает по требованию доступ на основе технологии SSL
Сканирование подключенных конечных точек сети на основе технологии SSL	Перед допуском в сеть выполняется сканирование подключенных рабочих станций для проверки соответствия требованиям/наличия вредоносного ПО
Программный блейд IPS	
Защита на сетевом уровне	Блокируются такие атаки, как DoS, сканирование портов, а также связанные с протоколами IP/ICMP/TCP атаки
Защита на уровне приложений	Блокируются такие атаки, как искажение кэша службы DNS, скрытые атаки по протоколу FTP и недопустимые команды
Методы обнаружения	На основе сигнатур, аномалий поведения и протоколов
Программный блейд Antivirus & Anti-Malware	
Защита от вирусов	Защита протоколов HTTP, FTP, POP3 и SMTP
Блокирующие средства защиты от шпионского ПО	Блокирование шпионского ПО на основе известных схем на шлюзе
Обновления	Централизованное ежедневное обновление
Программный блейд URL Filtering	
База данных с URL-адресами	Свыше 20 миллионов URL-адресов охватывают свыше 3 миллиардов web-страниц
Поддерживаемые языки	Свыше 70 языков в 200 странах
Обновления	Централизованное ежедневное обновление (свыше 100 000 новых сайтов в неделю)
Программный блейд Anti-Spam & Email Security	
Служба IPS для электронной почты	Защита от атак по протоколам SMTP, POP3 и IMAP
Защита от нежелательных сообщений с помощью определенных схем	Обнаружение нежелательных сообщений на основе динамической базы данных сигнатур
Проверка репутации IP-адреса	Блокирование отправителя нежелательных сообщений и вредоносного ПО
Средства защиты от вирусов на основе сигнатур	Первый уровень защиты от вирусов и вредоносного ПО
Защита от вновь появляющихся вирусов без задержки	Дополнение защиты на основе сигнатур для блокирования вновь появляющихся вирусов
Списки блокирования/разрешения	Обеспечивает контроль над отдельными доменами и пользователями
Управление и составление отчетов	
Централизованное управление	Включает централизованное управление
Наблюдение/регистрация	SmartView Tracker™ позволяет осуществлять усовершенствованное наблюдение и регистрацию
Составление отчетов ¹	Быстрое составление отчетов
Интерфейс командной строки	Telnet, SSH
Сетевые возможности	
Поддержка DHCP	Сервер SecurePlatform™ DHCP и рестранслятор
Резервный поставщик услуг Интернета ¹	Принятие решений в отношении маршрута на основе протокола, источника и узла назначения, а также порта
Поддержка маршрутизации ¹	OSPF, BGP, RIP v1/2, многоадресная передача
Поддержка моста 2-го уровня	Незаметная интеграция в существующую сеть
Рабочие характеристики и доступность	
Высокая доступность	Варианты восстановления после отказа по схеме «активный/пассивный» и «активный/активный»
Распределение нагрузки ¹	ClusterXL® обеспечивает практически линейное масштабирование
Качество обслуживания ¹	FloodGate-1® обеспечивает детальное управление качеством обслуживания
Резервный поставщик услуг Интернета ¹	Автоматически пересылает трафик на второй интерфейс

¹ Приобретается дополнительно в R70

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ УСТРОЙСТВ УТМ-1

	УТМ-1 130, 132, 136	УТМ-1 270, 272, 276	УТМ-1 570, 572, 576	УТМ-1 1070, 1073, 1076	УТМ-1 2070, 2073, 2076	УТМ-1 3070, 3073, 3076
Версия ПО	R65, R70	R65, R70	R65, R70	R65, R70	R65, R70	R65, R70
Число портов 10/100	1	—	—	—	—	—
Число портов 10/100/1000	4	4	6	6	8	10
Пропускная способность межсетевого экрана	400 Мбит/с	600 Мбит/с	1,1 Гбит/с	2 Гбит/с	3 Гбит/с	4,5 Гбит/с
Пропускная способность сети VPN	100 Мбит/с	100 Мбит/с	250 Мбит/с	250 Мбит/с	280 Мбит/с	1,1 Гбит/с
Число одновременных сеансов	300 000	600 000	800 000	1,1 миллиона	1,1 миллиона	1,1 миллиона
Пропускная способность IPS	300 Мбит/с ¹	380 Мбит/с ¹	700 Мбит/с ¹	900 Мбит/с ¹	1 Гбит/с ¹	4 Гбит/с ¹
Число лицензированных пользователей	Неограниченное	Неограниченное	Неограниченное	Неограниченное	Неограниченное	Неограниченное
Рекомендованное число пользователей	до 75	до 125	до 250	до 500	до 1000	до 1500
Число сетей VLAN	1024 ²	1024 ²	1024 ²	1024 ²	1024 ²	1024 ²
УТМ без предварительной настройки	Да	Да	Да	Да	Да	Да
Ускорение защиты	Нет	Нет	Нет	Нет	Нет	Да
Встроенное управление несколькими узлами	Standalone	Да	Да	Да	Да	Да
Емкость устройства хранения данных	80 ГБ	160 ГБ	160 ГБ	160 ГБ	160 ГБ	160 ГБ
Корпус	Настольный вариант/ занимает одно отделение стойки	Занимает одно отделение стойки	Занимает одно отделение стойки	Занимает одно отделение стойки	Занимает одно отделение стойки	Занимает одно отделение стойки
Габаритные размеры (стандартные)	10,6 x 5,7 x 1,6 дюйма	16,8 x 10 x 1,73 дюйма	16,8 x 10 x 1,73 дюйма	16,8 x 10 x 1,73 дюйма	17,4 x 15 x 1,73 дюйма	17,4 x 15 x 1,73 дюйма
Габаритные размеры (метрические)	270 x 145 x 40 мм	429 x 255 x 44 мм	429 x 255 x 44 мм	429 x 255 x 44 мм	443 x 381 x 44 мм	443 x 381 x 44 мм
Масса	1,6 кг (3,52 фунта)	3,7 кг (8,1 фунта)	3,7 кг (8,1 фунта)	3,7 кг (8,1 фунта)	6,5 кг (14,3 фунта)	6,5 кг (14,3 фунта)
Условия окружающей среды	Температура: от 5 до 40 °С, влажность: от 10 до 85 % без конденсации, высота над уровнем моря: 2 500 м					
Входное питание	100 - 240 В перем. тока, 50 - 60 Гц	100 - 240 В перем. тока, 50 - 60 Гц	100 - 240 В перем. тока, 50 - 60 Гц	100 - 240 В перем. тока, 50 - 60 Гц	100 - 240 В перем. тока, 50 - 60 Гц	100 - 240 В перем. тока, 50 - 60 Гц
Потребляемая мощность	60 Вт (макс.)	65 Вт (макс.)	65 Вт (макс.)	65 Вт (макс.)	250 Вт (макс.)	250 Вт (макс.)
Соответствие стандартам	UL 60950; FCC часть 15, подчасть В, класс А; EN 55024; EN 55022; VCCI V-3; AS/NZS 3548:1995; CNS 13438 класс А (испытания успешно проведены; ожидается утверждение государственными органами); KN22, серия KN61000-4, ТТА; IC-950; ROHS					

¹Тесты проведены с использованием шаблона реального трафика и стандартным профилем безопасности («Default»)

² Максимальное число VLAN-сетей на интерфейс составляет 256

АДРЕСА И ТЕЛЕФОНЫ CHECK POINT

Международная штаб-квартира

5 Ha'Solelim Street, Tel Aviv 67897, Israel | Телефон: +972-3-753-4555 | Факс: +972-3-624-1100 | Эл. почта: info@checkpoint.com

Представительство в России и СНГ

Check Point Software Technologies (Russia) OOO | 109240, Москва, ул. Николаямская, д.13, стр.17 | Тел./факс: +7 495 967 7 444 | http://rus.checkpoint.com