

McAfee® Secure Firewall (Sidewinder)

Старых брандмауэров на основе правил и сигнатур больше недостаточно — новые угрозы сочетают атаки по нескольким направлениям, возникают как за пределами, так и внутри корпоративной сети, и даже используют зашифрованные протоколы. Сегодня хакеры играют на уязвимостях приложений. Программно-аппаратный комплекс Secure Firewall (ранее Sidewinder) — это межсетевой экран нового поколения, обеспечивающий управление безопасностью приложений и многоуровневую защиту в сочетании с высочайшей производительностью обработки сетевого трафика.

Защита от ботнетов и комбинированных атак

Технология TrustedSource представляет собой первый в истории отрасли и самый мощный на сегодня механизм предупреждающего детектирования угроз на основе ретроспективного анализа поведения узлов и устройств (репутации).

Глобальная сеть TrustedSource открывает поистине экстрасенсорные возможности — мы видим то, чего не замечают другие. Именно поэтому мы блокируем более 70% нежелательного трафика на периметре корпоративных сетей, уменьшая нагрузку на IT-инфраструктуру наших клиентов и снижая риски атак. TrustedSource блокирует попытки установления соединений со стороны заведомо «плохих» узлов-отправителей, обращения к инфицированным web-страницам и трафик компьютеров, входящих в состав «зомби-сетей» (ботнетов). По аналогии с банковской системой оценки кредитоспособности клиента, TrustedSource рассчитывает репутацию сетевых ресурсов в реальном времени с учетом текущего уровня и характера угроз в Интернете, что обеспечивает точную идентификацию подозрительных узлов и предупреждающую блокировку соответствующего трафика.

В центре внимания — приложения

Главной игровой площадкой злоумышленников сегодня стали приложения. По последним оценкам от 70 до 80% новых атак используют уязвимости в приложениях и успешно обходят традиционные технологии контекстной/глубокой инспекции пакетов. Анализ пакетов на прикладном уровне сам по себе не гарантирует безопасность. Secure Firewall, как истинный брандмауэр прикладного уровня, расширяет границы контроля приложений, позволяя отслеживать, кто и как использует электронную почту, web-трафик (HTTP/S), интернет-конференции (H.323), приложения Oracle, Citrix, SQL, VoIP (SIP), протоколы SSH, FTP и многие другие распространенные сервисы.

Фильтрация зашифрованного трафика

Другим излюбленным инструментом современных хакеров является зашифрованный трафик, который пропускается большинством брандмауэров без какой-либо проверки. И здесь на сцену выходит еще одно важное отличие Secure Firewall — дешифрация и фильтрация трафика SSH, SFTP, SCP и SSL/HTTPS, позволяющая блокировать атаки на серверы предприятия на дальних подступах.

Оптимизация управления и соблюдение стандартов

Хорошей системой защиты легко управлять. Помимо удобного и понятного интерфейса, позволяющего создать любое правило на одном экране, Secure Firewall также предлагает целый ряд инструментов, облегчающих управление.

- **Secure Firewall Reporter** — штатное встроенное средство управления событиями безопасности (SEM — Security Event Management), обеспечивающее централизованный мониторинг, корреляцию событий и формирование отчетов, превращающих данные аудита безопасности в информацию для принятия решений.
- **Secure Firewall CommandCenter** — система централизованного управления устройствами Secure Firewall. Приобретается отдельно и обеспечивает централизованное управление политиками сотен программно-аппаратных брандмауэров McAfee.
- **Функциональные обновления** — автоматически распространяются через Интернет. Secure Firewall самостоятельно выполняет проверку подлинности, тестирование и установку системных обновлений по заданному администратором расписанию.
- **Средства мониторинга и контроля сетевой активности сотрудников и подрядчиков**, позволяющие перехватить шпионские приложения и другое вредоносное содержание, загружаемое по незнанию или по злому умыслу.



Модель	410	510	1100	2100	2150	4150
Форм-фактор	Small 1U	Small 1U	Enterprise 1U	Enterprise 2U	Enterprise 2U	Enterprise 5U
Неограниченное число пользователей	Да	Да	Да	Да	Да	Да
Рекомендованное число пользователей	300	600	Средние и крупные организации	Средние и крупные организации	Крупные организации	Корпоративный сегмент
RAID	—	—	RAID 1	RAID 1	RAID 5	RAID 5
Источники питания	Один	Один	Два	Два	Два	Два
Порты RJ-45 (штатно/макс)	4/8 1 Гбит	4/10 1 Гбит	8/14 1 Гбит	8/20 1 Гбит	8/20 1 Гбит	14/24 1 Гбит
Опволоконные порты (макс)	—	4	4	6	6	6
Оptionальный 10-гигабитный порт (макс)	—	—	—	2	2	2
Дешифрация и фильтрация SSL/HTTPS	—	Да	Да	Да	Да	Да
Сертификаты	ICSA Labs IPSec VPN, Common Criteria EAL4+ с Application Protection Profile (единственный брандмауэр, обладающим таким сертификатом EAL4+), FIPS 140-2					
Производительность						
Фильтрация пакетов (TCP)	275 Мбит/с	650 Мбит/с	1,9 Гбит/с	1,9 Гбит/с	3,1 Гбит/с	3,8 Гбит/с
Контекстная фильтрация	250 Мбит/с	600 Мбит/с	1,8 Гбит/с	1,8 Гбит/с	2,9 Гбит/с	3,6 Гбит/с
Число одновременных подключений	100 000	500 000	1 000 000	1 000 000	1 600 000	2 000 000
Фильтрация прикладного уровня	230 Мбит/с	250 Мбит/с	1,4 Гбит/с	1,4 Гбит/с	2,2 Гбит/с	2,7 Гбит/с
IPSec VPN	160 Мбит/с	160 Мбит/с	240 Мбит/с	240 Мбит/с	350 Мбит/с	400 Мбит/с
Размеры, масса, электропитание						
Ширина	54,6 см	54,6 см	42,6 см	44,43 см	44,43 см	44,27 см
Глубина	42,54 см	57,6 см	77,2 см	74,4 см	74,4 см	67,43 см
Высота	4,2 см	4,2 см	4,26 см	8,64 см	8,64 см	21,77 см
Масса	11,8 кг	11,8 кг	16,3 кг	23 кг	28,85 кг	45,36 кг
Электропитание	345 ватт 110/220 В	345 ватт 110/220 В	2 x 670 ватт 110/220 В	2 x 750 ватт 110/220 В	2 x 750 ватт 110/220 В	2 x 930 ватт 110/220 В