

McAfee® Email Gateway (IronMail)



Системы электронной почты являются основным объектом кибер-угроз, причем как внешних, таких как спам, вирусы, попытки взлома, программные черви и трояны, так и внутренних, наподобие утечек данных и нарушения внутренних или нормативно-законодательных регламентов доступа к информации. Сегодня, когда эпидемии компьютерных вирусов спама распространяются по миру в считанные минуты, защита систем электронной почты требует новых, гораздо более адаптивных и оперативных методов защиты. Именно такие методы и реализует программно-аппаратный комплекс Secure Mail (ранее IronMail), который устанавливается перед почтовым сервером организации и обеспечивает оперативную нейтрализацию любых входящих и исходящих угроз.

Защита входящего трафика

Технология TrustedSource рассчитывает интегральную репутацию каждого сообщения по IP-адресам, доменным именам, URL-ссылкам и вложенным файлам. Используются результаты аналитической обработки более трети общемирового корпоративного почтового трафика. Технология способна блокировать до 80% нежелательных подключений к почтовой системе только на основе репутационных данных.

99% точность распознавания спама. Технология SpamProfiler анализирует каждое сообщение по нескольким тысячам контрольных признаков и рассчитывает вероятность того, что сообщение является спамом, содержит признаки фишинг-атаки или иные угрозы.

Технология OutbreakDefender – объединяет сразу несколько механизмов защиты от угроз во входящих и исходящих сообщениях, гарантирующих что, такие сообщения никогда не будут рассылаться клиентам и партнерам:

- механизм T-X Days: мультипротокольная перекрестная репутация TrustedSource идентифицирует угрозы еще до их появления;
- механизмы прогнозирования: функции обнаружения аномалий Anomaly Detection Engine и поведенческого анализа файлов File Behavior Analysis идентифицируют угрозы на ранних стадиях;
- механизмы упреждения: автоматическая изоляция подозрительных вложений с помощью функции Dynamic Quarantine и правила блокировки вложенных файлов;
- механизмы реагирования: поиск угроз по ключевым словам, оценка репутации отправителя и получателя, антивирусная проверка с одновременным применением до трех анти-вирусных механизмов.

Защита исходящего трафика

Предотвращение утечек информации. Секретные сведения могут быть как структурированными (номера кредитных карт, паспортные данные и т.д.), так и неструктурированными (интеллектуальная собственность, сведения, представляющие коммерческую тайну или попадающие по действия нормативно-регулирующих требований, закрытая техническая информация и т.д.). Secure Mail предлагает средства проверки почтовых сообщений, позволяющие надежно защитить обе указанные категории и обеспечить выполнение отраслевых стандартов защиты информации. В комплект поставки входят готовые настройки для поддержки регламентов HIPAA, GLBA и SOX, а также инструменты контроля на уровне ключевых слов и документов в целом.

Прозрачное шифрование на основе политик. Устройства Secure Mail поддерживают целый ряд технологий шифрования и позволяют реализовать криптозащиту электронной переписки в прозрачном для конечного пользователя режиме:

- схема «организация–организация»: Secure Mail может выполнять шифрование трафика между почтовыми шлюзами с использованием отраслевого стандарта TLS или унаследованных технологий, наподобие S/MIME и OpenPGP;
- схемы «организация–клиент»: в случае отсутствия возможности использовать технологии шифрования, заказчик может получать сообщения, отправляемые через Secure Mail, с помощью web-интерфейса.

Масштабируемость

Линейка из четырех моделей устройств Secure Mail позволяет выбрать оптимальное решение для любой организации.

Модель	E5200	E2200	S120	S10D
Целевая аудитория	Телеком-операторы, провайдеры, крупные предприятия	Средние и крупные предприятия	Малые и средние предприятия	Малые предприятия, филиалы
Форм-фактор	Для монтажа в стойку, 2U	Для монтажа в стойку, 1U	Для монтажа в стойку, 1U	Для монтажа в стойку, 1U
Процессорных ядер	8	4	2	1
Память	4 Гбайт	4 Гбайт	4 Гбайт	1 Гбайт
Диск	600 Гбайт	150 Гбайт	150 Гбайт	80 Гбайт
Сетевые интерфейсы	4	2	2	1