Описание Trend Micro Interscan Messaging Security Virtual Appliance (IMSVA)

Trend Micro IMSVA – Высокопроизводительное шлюзовое решение для обеспечения многоуровневой фильтрации спама и вирусов в почтовом трафике (POP3/SMTP), блокирования писем с небезопасными гиперссылками, сохранения конфиденциальности при переписке и отслеживания активности в реальном времени с последующим формированием детальной отчетности.

Trend Micro IMSVA решает следующие ключевые задачи:

1. Гибридная система проверки почтового трафика, включающая фильтрацию и очистку потока сообщений как локально, так и в режиме SaaS на базе глобальной системы обеспечения безопасности Smart Protection Network с высоким уровнем SLA (опционально) с единой системой управления.
2. Блокирование спама как на уровне источников его распространения (на основе репутации IP адресов и подсетей) до попадания нежелательной корреспонденции в сеть компании при помощи глобальной системы обеспечения безопасности Trend Micro Smart Protection Network, так и за счет локального анализа по спам сигнатурам тех сообщений, которые прошли репутационную проверку.
3. Защита от угроз, нацеленных на отказ в обслуживании и проникновение в корпоративные почтовые системы обеспечивается за счет блокирования DHA и bounce атак, а также предварительной очистки трафика в облаке (опционально).
4. Блокирование писем, содержащих гиперссылки, ведущие в конечном итоге на опасные или зараженные Интернет-ресурсы (в реальном времени проверяется вся цепочка переадресаций URL из писем).
5. Очистка входящего и исходящего трафика от огромного количества вредоносного ПО (включая вирусы, шпионские программы, элементы бот сетей, утилиты для создания туннелей и др.)
6. Наличие контентной фильтрации и шифрования писем, обеспечивающих соблюдение политик безопасности по почтовой переписке и защиту от утечки информации.
7. Поддержка глобальной службы каталогов LDAP (Active Directory) позволяющая настроить политики с привязкой к пользователям/группам.
8. Поддержка интеграции со сторонними системами через SNMP, позволяющая осуществлять мониторинг состояния системы.

9. Формирование подробных отчетов позволяет детализировать статистику по работе системы, найденных угрозах и другие сведения, представленные как в виде графиков, так и в обычном тексте.

Основные особенности IMSVA

- **Форм-фактор virtual appliance.** IMSVA поставляется в виде virtual appliance (виртуальный модуль с интегрированной операционной системой), который может быть установлен как в виртуальной среде (VMware и Hyper-V), так и на физических серверах.

- **Гибридная система защиты.** Основной задачей IMSVA является блокирование попадания спама и вредоносного кода в корпоративную сеть предприятия через почтовые системы. Работа этих механизмов обеспечивается за счет использования смешанной системы проверки потока сообщений, работающих как в локальном режиме, так и на уровне т.н. «облачного» сервиса Trend Micro (Smart Protection Network). Что может быть реализовано благодаря этому:
    - в случае использования гибридного механизма, уровень нагрузки на локальную сеть предприятия существенно снижается, т.к. основные проверки (антиспам, антивирус) производятся на ЦОД Trend Micro и локально проверяется только та часть корреспонденции, которая прошла первый эшелон защиты.
    - гибридная схема проверки обеспечивает значительное снижение рисков, связанных с отказом в обслуживании в случае распределенных атак, а также проникновения вредоносного кода. Уровень SLA соответствует лучшим практикам в индустрии (детали см в отдельном документе).

- **Антиспам фильтрация.** Основой антиспам фильтрации является использование почтового репутационного сервиса, являющегося частью глобальной распределенной системы безопасности Smart Protection Network (SPN), созданной Trend Micro. Главной особенностью этого механизма является возможность блокирования спама на уровне источников его распространения (на уровне IP адресов и подсетей) без необходимости анализировать сами письма. Поток сообщений, проходящих внутрь сети предприятия, в этом случае заметно снижается; за анализ этих писем отвечает локальный антиспам движок, работающий на основе сигнатур и эвристического анализа. Общий уровень эффективной фильтрации спама достигает 95% (по оценке WestCoast). Также система обеспечивает:
    - Настройку индивидуальных белых списков (доменов и IP адресов), обеспечивающих прозрачное хождение легитимных писем от проверенных отправителей;

- Гибкую настройку параметров локального антиспам движка, позволяющую оптимизировать сканирование писем в соответствии с условиями.

- **Блокирование опасных URL в письмах.** IMSVA обеспечивает блокирование различных веб ресурсов в реальном времени в том случае, если по глобальной репутационной базе Trend Micro они проходят как опасные. При этом проверку проходит не только ссылка, представленная в письме, но и конечная ее цель, т.е. система проверяет всю цепочку переадресаций.

- **Защита входящего и исходящего трафика от вирусов и прочего вредоносного контента.** Защита от вирусов, шпионских приложений, элементов бот сетей, скриптов и прочего опасного содержимого позволяет решить следующие задачи:
  - Снижение рисков, связанных с утратой контроля над системой благодаря контролю вложений и удалению писем, содержащих приложения для массовых рассылок (например, макровирусы);
  - Защита репутации предприятия благодаря возможностям защиты, снижающим вероятность распространения вредоносного контента;
  - Предотвращение потерь, связанных с проникновением или рассылкой шпионских приложений или утилит, осуществляющих кражу данных.

- **Фильтрация содержимого.** Благодаря наличию функций контентной фильтрации, система избежать возможной утечки нежелательной информации и обеспечить сохранность данных предприятия, а именно:
  - Запрет отправки файлов и сообщений, содержащих определенные слова и словосочетания, регулярные выражения;
  - Запрет выгрузки файлов определенного типа (MIME) и размера позволяет ограничить отправку и выгрузку нежелательных документов и снизить нагрузку на шлюз;
  - Политики могут быть созданы как на групповой основе, так и индивидуально в привязке к доменным пользователям Active Directory.

- **Поддержка шифрования.** Для дополнительной защиты конфиденциальности предприятия IMSVA содержит встроенные средства шифрования на основе личностной криптографии (IBE). Такой способ шифрования писем позволяет решить следующие задачи:
  - Зашифрованная переписка не требует подготовки инфраструктуры (KPI) ни на стороне отправителя, ни на стороне получателя, что минимизирует затраты с внедрением и обслуживанием;
  - Риски, связанные с перехватом сообщений нецелевыми получателями, сведены к минимуму.

- Почта зашифровывается автоматически на основе политик.

- **Поддержка различных механизмов идентификации.** Для применения политик в режиме максимальной совместимости с существующей инфраструктурой, система поддерживает следующие режиме идентификации объектов и субъектов:
  - IP адреса клиентский систем;
  - Имена клиентских хостов;
  - Пользователи из LDAP и группы, на их основе.

- **Контроль в реальном времени.** Контроль соблюдения политик и защиты от угроз обеспечивается в режиме реального времени как в режиме мониторинга, так и через уведомления (в т.ч. через SNMP и e-mail).

- **Балансировка нагрузки и катастрофоустойчивость.** Система обладает встроенными средствами балансировки нагрузки, а также механизмами защиты от аварий:
  - IMSVA поддерживает высокую доступность за счет дублирования, обеспечивая переключение активный/пассивный для работы в режиме моста;
  - Система масштабируется для распределенных сетей и поддерживает развертывание в многоуровневом режиме.

- **Система отчетности.** Генерация отчетов обеспечивает наглядное представление работы системы в рамках всей инфраструктуры предприятия.

- **Поддержка большого количества платформ.** IMSVA может работать как на физических платформах (перечень сертифицированных систем доступен на сайте), так и в виртуальной среде. Версии поддерживаемых виртуальнеых платформ:
  - VMware ESX/ESXi 3.5 или выше
  - Microsoft Hyper-V 2.0 или выше.

Архитектура IMSVA

IMSVA поставляется как virtual appliance, в который интегрировано само решение и операционная система (CentOS). Система может быть установлена в сетевой инфраструктуре одним из методов, перечисленных в руководстве по развертыванию.

Сертификация

- **ФСТЭК России**

  В настоящее время решения Trend Micro, в том числе продукт IMSVA, имеют сертификаты ФСТЭК России (ТУ и НДВ на производство). Подробности можно найти на сайте.

Загрузить тестовую версию

IMSVA: http://ru.trendmicro.com/ru/products/enterprise/interscan-messaging-security-virtual-appliance/download/index.php

Дополнительная информация по продукту

http://ru.trendmicro.com/ru/products/enterprise/interscan-messaging-security-virtual-appliance/

http://docs.trendmicro.com/en-us/enterprise/interscan-web-security-virtual-appliance.aspx (руководства пользователя)