Поймите, как работает Cisco IPS автоматическая функция обновления подписи

Содержание

Введение

Этот документ предоставляет обзор системы предотвращения вторжений Cisco (IPS) (IPS) функция Автоматического обновления и ее операция.

Функция Автоматического обновления IPS была представлена в версии 6.1 IPS и предоставляет администраторам простой способ для обновления подписей IPS на регулярно запланированном интервале.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Обновления подписи требуют допустимой подписки услуг Cisco для IPS и лицензионного ключа. Перейдите к http://www. cisco . com/движение/лицензия и нажимает **IPS Signature Subscription Service** для просьбы лицензионного ключа.
- Cisco.com (CCO) учетная запись пользователя, которая привязана к активной подписке услуг Cisco для IPS.
- Привилегии загрузить криптографическое программное обеспечение . Перейдите : http://программные средства. cisco . com/legal/k9/controller/do/k9Check. x? eind=Y , чтобы проверить, есть ли у вас доступ.

Используемые компоненты

Сведения в документе приведены на основе данных версий аппаратного и программного обеспечения:

- Версии Cisco IPS 6.1 и позже
- Определенные функции Версий Cisco IPS 7.2 (1), 7.3 (1), и позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

Требование к сети

1. Интерфейс команд и управления IPS требует прямого доступа к Интернету с помощью HTTPS (TCP 443) и HTTP (TCP 80).
2. Технология NAT и Списки контроля доступа (ACL) на периферийных устройствах, таких как маршрутизаторы и межсетевые экраны должны быть настроены для разрешения подключения IPS к Интернету.
3. Исключите IP-адрес интерфейса команд и управления из всех фильтров контента и формирователей сетевого трафика.
4. Прокси-серверы поддержек характеристик Автоматического обновления в 7.2 (1)

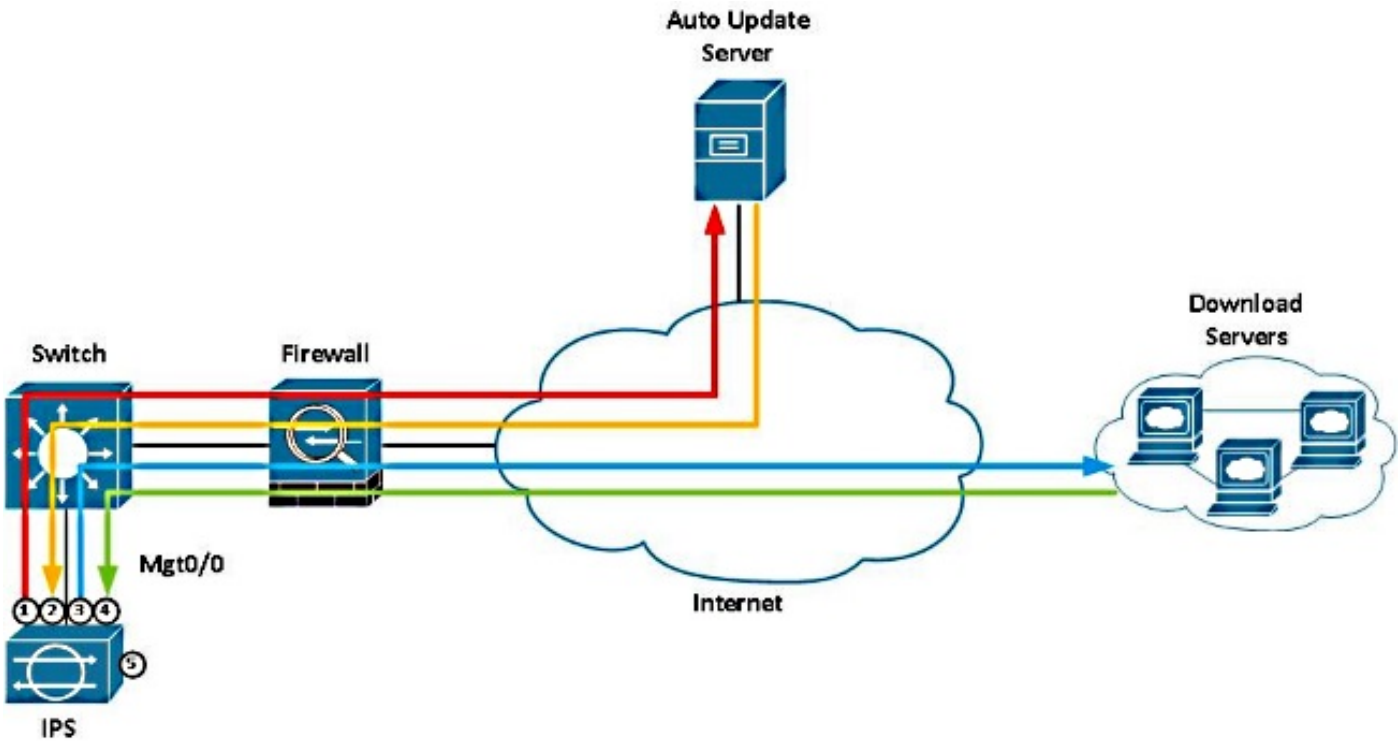
FIPS/CC сертифицировали выпуск. Все прочие 6.x и 7.x выпуски ПО не поддерживают Автоматическое обновление через прокси-сервер в это время. 7.2 (1) выпуск включает много изменений в Secure Shell (SSH) по умолчанию и параметры настройки HTTPS. См. Комментарии к выпуску для системы предотвращения вторжений Cisco (IPS) 7.2 (1) E4 перед обновлением к 7.2 (1).

% Warning: В Версии 7.0 (8) E4 Cisco IPS значение по умолчанию для IP-адреса сервера Cisco изменено от 198.133.219.25 до 72.163.4.161 в конфигурации URL Автоматического обновления. Если ваш датчик настроен для автоматических обновлений, вы, возможно, должны были бы обновить правила межсетевого экрана, чтобы позволить датчику соединяться с новым IP-адресом. Для Версий Cisco IPS 7.2 и позже, жестко закодированный IP-адрес сервера автоматического обновления заменен именованным Полным доменным именем (FQDN) и Поиском в системе доменных имен (DNS). См. Раздел конфигурации этого документа для дополнительных сведений.

Обходные предупреждения

Некоторые обновления подписи требуют, чтобы таблицы регулярного выражения были перекомпилированы за это время, IPS может войти в транзитный режим программного обеспечения. Для встроенных датчиков с набором транзитного режима к Автоматическому Аналитический Механизм обойден, позволив трафику течь через встроенные интерфейсы и встроенных пар VLAN без контроля. Если транзитный режим установлен в Выключено, встроенный датчик останавливает проходящий трафик, в то время как применено обновление.

Процесс автоматического обновления подписи



1. IPS аутентифицируется на Auto Update Server в 72.163.4.161 HTTPS использования

(TCP 443).

2. IPS передает клиентскую декларацию к Auto Update Server, который включает ID платформы и зашифрованный общий секретный ключ что использование сервера для проверки подлинности датчика Cisco IPS.

3. После того, как аутентифицируемый, сервер обновления отвечает декларацией сервера, которая содержит список опций файла загрузки, привязанных к ID платформы. Данные, содержавшие здесь, включают информацию, отнесенную в версию обновления, расположение загрузки и поддерживаемые протоколы передачи файлов. На основе этих данных логика автоматического обновления IPS определяет, допустима ли какая-либо из опций загрузки, и затем выбирает лучший пакет обновления для загрузки. При подготовке к загрузке сервер предоставляет IPS ряд ключей, которые будут использоваться для дешифрования файла обновления.

4. IPS устанавливает новое соединение к серверу загрузки, определенному в декларации сервера. IP-адрес сервера загрузки варьируется, который зависит от местоположения. IPS использует протокол передачи файлов, определенный в URL данных загрузки файла, изученном в декларации сервера (в настоящее время HTTP использования (TCP 80)).

5. IPS использует ранее загруженные ключи для дешифрования пакета обновления и затем применяет Файлы цифровой подписи к датчику.

Настройка

Основная конфигурация автоматического обновления подписи

Функция Автоматического обновления может быть настроена от диспетчера устройств IPS (IDM) или IPS Manager Express (IME). Выполните следующие действия:

1. От IDM/IME выберите **Configuration> Sensor Management > Auto / Auto/Cisco.com Update.**