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.**

2. Выберите **Enable Signature, и Обновления Механизма от** флажка **Cisco.com** справа разделяют на области и щелкают по синему названию **Настроек сервера Cisco.com** чтобы к выпадающему область конфигурации.

3. Введите имя пользователя и пароль CCO.

   Вот URL в качестве примера для Версий Cisco IPS 7.0 (8) и 7.1 (6):

   https://72.163.4.161//cgi-bin/front.x/ida/locator/locator.pl

   Вот URL в качестве примера для Версий Cisco IPS 7.2 (1), 7.3 (1), и позже:

   https://www. cisco . com//cgi-bin/front.x/ida/locator/locator.pl

   Примечание: Не изменяйте URL Cisco.com. Это не должно должно быть быть изменено от его настройки по умолчанию.//является намеренным и не опечатка. В Версиях Cisco IPS 7.2 (1), 7.3 (1), и позже, датчик делает запрос сервера DNS, который определен в конфигурации сенсорной сети для решения www. cisco . URL com к интернет-маршрутизируемому IP - адресу.

4. Настройте время начала и частоту для планирования обновления подписи. Рекомендуется установить время начала в произвольный момент времени, который не находится на вершине часа. В данном примере время установлено в 23:15:00. Частота может быть настроена для поддержки почасовых или ежедневных попыток обновления. Нажмите **Apply** для применения изменений конфигурации.

Усовершенствования автоматического обновления подписи

Много улучшений функции Автоматического обновления включены в Версии Cisco IPS 7.2 (1) и позже. Улучшения дополнительных мер безопасности также добавлены к Версиям Cisco IPS 7. 3.2 и более поздние версии . См. параметры конфигурации, описанные в этом разделе для дополнительных сведений.

Обновление теперь функция

Версия 7.2 (1) Cisco IPS представила новую возможность GUI IPS и CLI, который позволяет администраторам сразу инициировать Автоматическое обновление подписи, которое обходит потребность ждать в течение запланированного времени для появления.

Для обхода списка автоматического обновления и обновления сразу, перейдите к IDM/IME и выберите **Configuration> Sensor Management > Auto / Auto/Cisco.com Update.** Пока Автоматическое обновление правильно настроено и применено, можно нажать кнопку **Update Now** в верхнем правом угле экрана для инициирования попытки обновления.

Можно также ввести **autoupdatenow** команду в CLI датчика для инициирования попытки обновления. Например:

```
SSP-60# autoupdatenow
Warning: Executing this command will perform an auto-upgrade on the sensor immediately.
Before executing this command, you must have a valid license to apply the Signature
AutoUpdates and auto-upgrade settings configured.After executing this command please
disable user-server/cisco-server inside 'auto-upgrade' settings, if you don't want
scheduled auto-updates
Continue? []: yes
Automatic Update for the sensor has been executed.Use 'show statistics host' command
to check the result of auto-update.Please disable user-server/cisco-server in
auto-upgrade settings, if you don't want scheduled auto-updates
```

Автоматическое обновление через интернет-Прокси

Для инициирования автоматического обновления через интернет-прокси перейдите к IDM/IME и выберите **Configuration> Sensor Setup> Network**. Введите DNS и (дополнительно) IP-адрес Прокси-сервера HTTP и порт:

Проверьте сертификаты доверенного корня

Когда обновления загружены, версия 7.3 (2) Cisco IPS представила способность к IPS для проверки цепочки корневого сертификата сервера средства обновления. С этой активированной опцией IPS проверяет, подписан ли корневой сертификат в цепочке сертификатов CA. Trusted Root, Например, корневые сертификаты TLS, которые получены в процессе обновления подписи из сервера Cisco и глобального сервера корреляции, проверены. Эта опция в настоящее время отключается по умолчанию в Версии 7.3 (2) Cisco IPS; однако, это могло бы быть включено по умолчанию в будущем выпуске. См. *Чтение* IPS *Меня* файл для получения дополнительной информации.

Просмотрите локальное хранилище надежного сертификата

Для просмотра текущего списка установленных сертификатов доверенного корня в Версиях IPS 7.3 (2) и позже, перейдите к **Конфигурации> менеджмент Датчика> Сертификаты> Сертификаты доверенного корня**:

Включите строгую проверку серверного сертификата TLS

Выполните эти шаги для активации Строгой опции Проверки Сервера TLS:

1. Перейдите к **Конфигурации> Настройка Датчика> Сеть**.
2. Разверните **HTTP, FTP, Telnet, SSH, CLI и Другое** выпадающее меню **Опций**.
3. Проверьте флажок **Enable Strict TLS Server Validation**.
4. Нажмите **Apply** для применения конфигурации к датчику.

Добавьте/Обновите Корневые сертификаты к Локальному Хранилищу Надежного сертификата

Поскольку сертификаты истекают на серверах средства обновления, Cisco оставляет за собой право использовать цепочку корневого сертификата кроме GeoTrust и Thawte. Если обновленный сертификат не существует в текущем образе программного обеспечения IPS, то обновленная цепочка корневого сертификата может быть вручную установлена в локальное хранилище надежного сертификата датчика. Закодированные DER сертификаты могут быть расположены на файловый сервер и получены датчиком через SCP или HTTPS. Следующий пример использует SCP для демонстрации установки сертификатов / процесс обновления.

1. От IDM/IME перейдите к **Конфигурации> менеджмент Датчика> SSH> Известные Ключи RSA Хоста**.
2. **Нажмите Add** и введите IP-адрес сервера SCP.
3. Нажмите **Retrieve Host Key** для имения датчика, автоматически получают открытый ключ из сервера.
4. Нажмите **OK** дважды и затем **Применитесь** для применения конфигурации к датчику. **Примечание:** Если размер ключа, представленный сервером SCP, меньше, чем 2,048 битов, предупреждение появляется.
5. Нажмите **Yes** для добавления ключа к известной таблице хостов или **No** для возврата к экрану **Add Known Host RSA Key**.

6. Перейдите к **Конфигурации> менеджмент Датчика> Сертификаты доверенного корня**.

7. Нажмите **Add/Update** для добавления нового закодированного DER файла сертификата от сервера SCP. Гарантируйте, что файл сертификата предварительно расположен на сервер и доступный для удаленного извлечения через SSH.

8. Выберите **SCP** как протокол и введите URL, имя пользователя и пароль.

9. Нажмите **OK** для начала передачи файла сертификата и установки.

10. Нажмите **Yes** для добавления сертификата к IPS локальное хранилище Trusted Root и затем **OK** для выхода.

Проверка

От IDM/IME выберите **Configuration> Sensor Management > Auto / Auto/Cisco.com Update.** Разверните **информационный** раздел **Автоматического обновления** для рассмотрения статуса последней попытки загрузки. Нажмите **Refresh** для обновления **информационных** данных **Автоматического обновления**.

Для проверки статуса процесса Автоматического обновления через CLI введите **команду show statistics host** :

```
IPS# show statistics host
<Output truncated>
Auto Update Statistics
lastDirectoryReadAttempt = 16:55:03 GMT-06:00 Wed Jun 27 2012
= Read directory: http://CCOUser@72.163.7.55//swc/esd/06/273556262/guest/
= Success
lastDownloadAttempt = 16:55:03 GMT-06:00 Wed Jun 27 2012
= Download: http://CCOUser@72.163.7.55//swc/esd/06/273556262/guest/
IPS-sig-S654-req-E4.pkg
= Success
nextAttempt = 17:55:00 GMT-06:00 Wed Jun 27 2012
lastInstallAttempt = 16:55:46 GMT-06:00 Wed Jun 27 2012
= Success
<Output truncated>
```

От IDM/IME обратитесь к Лицензированию гаджета на информационной панели Дом для просмотра Статуса лицензии и в настоящее время устанавливаемой версии подписи. Та же информация может быть получена через CLI с **командой Show version**.

```
SSP-60# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.3(2)E4

Host:
Realm Keys key1.0
Signature Definition:
Signature Update S805.0 2014-06-03
Threat Profile Version 7
```

```
OS Version: 2.6.29.1
Platform: ASA5585-SSP-IPS60
Serial Number: JAF1527CPNK
Licensed, expires: 21-Jun-2014 UTC
Sensor up-time is 39 days.
Using 46548M out of 48259M bytes of available memory (96% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 86.6M out of 377.5M bytes of available disk space (24% usage)
boot is using 63.4M out of 70.5M bytes of available disk space (95% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)

MainApp C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500
Running
AnalysisEngine C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500
Running
CollaborationApp C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500
Running
CLI C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500

Upgrade History:

* IPS-sig-S802-req-E4 16:07:23 UTC Thu May 29 2014
IPS-sig-S805-req-E4.pkg 16:18:51 UTC Mon Jun 09 2014

Recovery Partition Version 1.1 - 7.3(2)E4

Host Certificate Valid from: 15-Jul-2013 to 16-Jul-2015
```

Устранение неполадок

После корректной конфигурации Автоматического Обновления подписи выполните эти шаги, чтобы изолировать и исправить проблемы, с которыми обычно встречаются:

1. Для всех устройств IPS и модулей за исключением AIM и IDSM, гарантируйте, что интерфейс команд и управления связан с локальной сетью, назначил действительный IP - адрес / маска/шлюз подсети и имеет возможности IP - доступы к Интернету. Для AIM и модулей IDSM, действительный интерфейс команд и управления используется, как определено в конфигурации. Для подтверждения рабочего состояния интерфейса от CLI введите эту **команду показа**:

   ```
   IPS# show interfaces
   <Output truncated>
   MAC statistics from interface Management0/0
   Interface function = Command-control interface
   Description = Media Type = TX
   Default Vlan = 0
   Link Status = Up <---
   <Output truncated>
   ```

2. Чтобы проверить, имеет ли учетная запись пользователя CCO необходимые привилегии загрузить пакеты обновления подписи, открыть web-браузер и войти к Cisco.com с этой той же учетной записью CCO. После того, как аутентифицируемый, вручную загрузите последний пакет подписи IPS. Неспособность вручную загрузить пакет является вероятной причиной к отсутствию ассоциации учетной записи пользователя к допустимой подписке услуг Cisco для IPS. Кроме того, доступ к защитному программному обеспечению на CCO ограничен авторизованными

пользователями, которые приняли ежегодное соглашение о шифровании/экспорте. Сбой для утверждения этого соглашения, как было известно, предотвратил загрузки подписи от IDM/IME/CSM. Чтобы проверить, было ли это соглашение принято, открывает браузер и входит к Cisco.com с той же учетной записью CCO. После того, как аутентифицируемый, попытка вручную загрузить Cisco IOS? пакет ПО с набором функций K9.

3. Проверьте, существует ли там, прокси для Интернета связал трафик (все версии кроме 7.2 (1) и позже). Если трафик от порта командования и управления проходит этот прокси, функция Автоматического обновления не работает. Реконфигурируйте сеть так, чтобы в трафик порта командования и управления не проникали прокси и тест снова.

4. Для датчиков, которые выполняют программное обеспечение Версий 7.2 или 7.3, гарантируйте, что настроены один или несколько серверов DNS. Это требуется так, чтобы датчик был в состоянии решить www. cisco . средство обновления com FQDN к Интернет-маршрутизируемому IP-адресу.

5. Проверьте, существуют ли какие-либо приложения фильтрации содержимого или формирования трафика или устройства в пути к Интернету. Если подарок, настройте исключение, чтобы позволить IP-адресу интерфейса команд и управления обращаться к Интернету без ограничения.

6. Если трафик ICMP разрешен к Интернету, откройте CLI сенсора IPS и попытки пропинговать открытый IP - адрес.

   Этот тест может использоваться, чтобы проверить, настроены ли необходимая маршрутизация и правила NAT (если используется) правильно. Если тест ICMP успешно выполняется, все же Автоматические обновления продолжают отказывать, гарантировать, что сетевые устройства, такие как маршрутизаторы и межсетевые экраны вдоль пути разрешают HTTPS и сеансы HTTP от IP интерфейса команд и управления IPS. Например, если IP-адрес командования и управления 10.1.1.1, простая запись ACL на межсетевом экране ASA может быть похожей на данный пример:

   ```
   access-list INSIDE-TO-INTERNET extended permit tcp host 10.1.1.1 any eq www
   access-list INSIDE-TO-INTERNET extended permit tcp host 10.1.1.1 any eq https
   ```

7. Имя пользователя CCO не должно содержать специальные символы, например. См. идентификатор ошибки Cisco CSCsq30139 для получения дополнительной информации.

8. Когда сбои автоматического обновления подписи происходят, используйте следующую таблицу для соответствия с связанными кодами ошибки HTTP.

   ```
   IPS# show statistics host
   Auto Update Statistics
   lastDirectoryReadAttempt = 19:31:09 CST Thu Nov 18 2010
   = Read directory: https://72.163.4.161//cgi-bin/front.x/ida/locator/locator.pl
   ```

```
= Error: AutoUpdate exception: HTTP connection failed [1,110] <--
lastDownloadAttempt = 19:08:10 CST Thu Nov 18 2010
lastInstallAttempt = 19:08:44 CST Thu Nov 18 2010
nextAttempt = 19:35:00 CST Thu Nov 18 2010
```

Сообщение	Значение
Ошибка: Исключение AutoUpdate: Соединение HTTP отказало [1,110]	Аутентификация отказала. Проверьте имя пользователя и пароль.
исключение AutoUpdate status=false: Получите Ответ HTTP, подведенный [3,212]	Запрос к Auto Update Server испытал таймаут.
Ошибка: ответ ошибки HTTP: 400	Удостоверьтесь, что значение URL Cisco принято значение по умолчанию. Если ИДЕНТИФИКАТОР CCO больше, чем 32 символа в длине, попробуйте другой ИДЕНТИФИКАТОР CCO. Это может быть ограничением на сервер загрузки Cisco.
Ошибка: Исключение AutoUpdate: Соединение HTTP отказало [1,0]	Сетевая проблема предотвратила загрузку или существует потенциальная проблема с серверами загрузки.