Пример миграции формата подписи системы защиты от атак от версии 4.x к версии 5.x

Содержание

Введение

В Cisco IOS® Release 12.4 (11) T и позже, система предотвращения вторжений (IPS) Cisco IOS оказывает поддержку для формата подписи версии программного обеспечения 5.x Cisco IPS. 5.x формат подписи является основанным на версии форматом XML определения подписи, также используемым другой Cisco основанные на устройстве продукты IPS. Поддержка подписей и файлов определения подписи (SDFs) в версии 4.x Cisco IPS прекращена в этом и дальнейшем T-train Cisco IOS выпуски ПО.

Клиенты, которые выполняют IPS Cisco IOS с SDFs формата подписи Версии 4.x, могут реконфигурировать IPS Cisco IOS для использования предопределенных категорий подписи Cisco, Основных и Усовершенствованных наборов подписи или утилиты миграции IPS Cisco IOS для миграции файлов SDF предыдущей версии 4.x в наборы подписи формата Версии 5.x Cisco IPS.

Этот документ описывает, как мигрировать от Cisco IPS 4.x SDF формата и включить перемещенный набор подписи в Cisco IOS Release 12.4 (11) T или позже. Для получения дополнительной информации о том, как настроить IPS Cisco IOS в Cisco IOS Release 12.4 (11) T или позже, обратитесь к IPS 5.x Поддержка Формата Подписи и Усовершенствования Удобства пользования.

Примечание: Cisco рекомендует выполнить миграцию IPS Cisco IOS перед обновлением к Cisco IOS Release 12.4 (11) T или более поздний образ.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Cisco IOS Release 12.4 (11) T или 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.

Шаги для миграции файлов SDF версии 4.x

Сценарий миграции требует Cisco IPS 4.x файл SDF формата и (дополнительно) файл конфигурации интерфейса командой строки, который содержит сведения о конфигурации IPS Cisco IOS, используемые на маршрутизаторе thatrunsa, освобождают ранее, чем Cisco IOS Release 12.4 (11) T.

Сценарий миграции ищет команды, которые содержат **ip ips signature** *<sigid> [<sigsubid>]* **отключенный** в файле конфигурации маршрутизатора. Если файл конфигурации не содержит эту команду CLI, нет никакой потребности в сценарии миграции для чтения файла конфигурации интерфейса командой строки. Преобразование подписей, как таковых, базируется исключительно на SDF.

При выполнении сценария миграции, прежде чем вы обновите IPS Cisco IOS к Cisco IOS Release 12.4 (11) T или позже, придержитесь, процесс в Выполняют Сценарий Миграции IPS Cisco IOS.

При выполнении сценария миграции после того, как вы обновите IPS Cisco IOS к Cisco IOS Release 12.4 (11) T или позже, выполните эти шаги:

1. Проверьте любую потребность преобразовать команды CLI, **ip ips signature** *<sigid> [<sigsubid>]* **отключенный**, как упомянуто выше.
2. Используйте **команду copy running-config flash:ipscfg.cfg** для сохранения конфигурации интерфейса командой строки маршрутизатора в файл.Эта команда выполняет резервное копирование конфигурация существующего маршрутизатора для мигания в файле, названном *ipscfg.cfg*. Процесс переноса использует этот файл для полного 4.x к 5.x преобразование формата подписи.
3. Продолжите выполнять сценарий миграции IPS Cisco IOS.

Выполните сценарий миграции IPS Cisco IOS

Сценарий миграции доступен от Cisco.com в этом URL: http://www. cisco . com/cgi-bin/tablebuild.pl/ios-v5sigup. Сохраните сценарий миграции к флэш-памяти маршрутизатора или к доступному для маршрутизатора местоположению, такому как сервер упрощенного

протокола передачи файлов (TFTP).

Сценарий миграции преобразовывает SDF от формата Версии 4.x Cisco IPS до формата Версии 5.x. Сценарий миграции поддерживает только эти параметры подписи:

- severity
- действие
- включенный

Кроме того, сценарий миграции может также читать из конфигурации IPS IOS fileand, перемещают отключенные подписи, которые были настроены **командой ip ips signature <sigid> <sigsubid> disabled** CLI в версиях ранее, чем Cisco IOS Release 12.4 (11) T.

Примечание: Пользовательский (non Cisco) подписи не преобразованы с этим сценарием.

Данный пример показывает, как переместить IPS 4.x отформатированный файл *sdmips.sdf* к IPS Cisco IOS в Cisco IOS Release 12.4 (11) T с IPS Cisco IOS 5.x поддержка формата подписи.

```
C2821#tclsh flash:ios-ips-migrate.tbc
This migration script will migrate Signature Definition Files
     from 4.x format to 5.x format.
The migration script will migrate only the following signature
     parameters - severity, action, enabled - for Cisco (non-custom) signatures.
Do you want to continue? [y/n] y
Please choose an IOS config file from which to migrate IOS IPS configuration.
Config File: [startup-config]
The following SDF locations were found configured in startup-config:
  flash://sdmips.sdf
Please provide SDF to migrate from the above list or of your own
     choice: flash:// sdmips.sdf
Migrating following SDF file (this will a take few minutes):
  flash://sdmips.sdf
Time Elapsed: 0:02:23
Migration completed successfully. The migrated file is
  C2821-sigdef-delta.xml
C2821#
```

Во-первых, сценарий миграции отображает краткий текст о своей функции. Затем, сценарий предоставляет возможность выбирать местоположение из того, где считать ток (предварительная миграция) конфигурация для IPS Cisco IOS. По умолчанию читает из загрузочной конфигурации. При предыдущем сохранении конфигурации к серверу TFTP или флэш-памяти маршрутизатора задайте местоположение в приглашении.

Пример:

Используйте **tftp://192.168.1.5 / <***конфигурация интерфейса командой строки маршрутизатора***>** для уведомления сценария для загрузки конфигурации интерфейса командой строки из сервера TFTP 192.168.1.5.

Используйте **flash://<***сохраненная конфигурация***>** для чтения из файла, экономил на флэш-памяти.

Загрузите перемещенные подписи в IPS Cisco IOS в программном обеспечении Cisco IOS версии 12.4(11)T

После того, как миграция подписи завершена, обновите образ маршрутизатора к Cisco IOS

Release12.4 (11) T, если вы уже не сделали так. Как только маршрутизатор повторно загружен, выполните эти шаги.

1. Включите IPS Cisco IOS.Эти выходные данные показывают, как включить IPS Cisco IOS на маршрутизаторе Cisco 2821. Для получения дополнительной информации о том, как настроить IPS Cisco IOS, обратитесь к IPS 5.x Поддержка Формата Подписи и Усовершенствования Удобства пользования.C2821#**mkdir ips**
```
Create directory filename [ips]?
Created dir flash:ips
C2821#conf t
Enter configuration commands, one per line. End with CNTL/Z.
C2821(config)#ip ips name MYIPS
C2821(config)#ip ips config location ips
C2821(config)#ip ips signature-category
C2821(config-ips-category)#category all
C2821(config-ips-category-action)#retired true
C2821(config-ips-category-action)#exit
C2821(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
C2821(config)#
```
2. Скопируйте и вставьте этот ключ в маршрутизатор для настройки крипто-открытого ключа подписи.C2821#**mkdir ips**
```
Create directory filename [ips]?
Created dir flash:ips
C2821#conf t
Enter configuration commands, one per line. End with CNTL/Z.
C2821(config)#ip ips name MYIPS
C2821(config)#ip ips config location ips
C2821(config)#ip ips signature-category
C2821(config-ips-category)#category all
C2821(config-ips-category-action)#retired true
C2821(config-ips-category-action)#exit
C2821(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
C2821(config)#
```
3. Включите IPS Cisco IOS на интерфейсах как показано в данном примере:C2821(config)#
```
C2821(config)#interface gigabitEthernet 0/0
C2821(config-if)#ip ips MYIPS in
C2821(config-if)#ip ips MYIPS out
C2821(config-if)#exit
```
4. Используйте команду **копии** для загрузки последнего пакета подписи:C2821#**copy tftp://192.168.1.5/IOS-S253-CLI.pkg idconf**
   Эта команда загружает подписи из пакета подписи *IOS-S253-CLI.pkg* в IPS Cisco IOS.**Примечание: категория подписи ips iOS все** было настроено в шаге 1, который исключает все подписи. После того, как пакет подписи успешно загружен, никакие подписи не выбраны и скомпилированы.
5. Используйте эту команду для загрузки перемещенного XML-файла в IPS Cisco IOS:*<имя хоста маршрутизатора>*-sigdef-delta.xmlПример:
   copy flash:C2821-sigdef-delta.xml idconf
   Как только маршрутизатор анализирует отформатированный Файл цифровой подписи версии 5.x, миграция завершена.
6. Используйте **команду show ip ips signature count**, чтобы проверить сводное состояние подписи, и затем использовать **команду show ip ips signature details**, чтобы посмотреть определенные детали на всех подписях.

Дополнительные сведения

- Cisco Intrusion Prevention System
- Уведомления о дефекте для специалистов по продуктам безопасности (включая обнаружение несанкционированного доступа CiscoSecure)
- Техническая поддержка - Cisco Systems