Пример настройки маршрутизатора, диспетчера устройств безопасности (SDM) и Cisco IOS CLI в системе предотвращения атак (IPS) Cisco IOS

Содержание

Введение

В Cisco Router and Security Device Manager (SDM) 2.2, Cisco конфигурация IOS® IPS интегрирована в рамках приложения SDM. Вы больше не обязаны запускать отдельное окно для настройки IPS Cisco IOS.

В Cisco SDM 2.2 новый мастер настройки IPS ведет, вы посредством необходимых шагов включаете IPS Cisco IOS на маршрутизаторе. Кроме того, можно все еще использовать пункты меню Advanced Configuration Option, чтобы включить, отключить, и настроить IPS Cisco IOS с Cisco SDM 2.2.

Cisco рекомендует выполнить IPS Cisco IOS с предварительно настроенными файлами определения подписи (SDFs): атака-drop.sdf, 128MB.sdf, и 256MB.sdf. Эти файлы созданы для маршрутизаторов с другими количествами памяти. Файлы связаны с SDM Cisco, который рекомендует SDFs, когда вы сначала включаете IPS Cisco IOS на маршрутизаторе. Эти файлы могут также быть загружены от http://www. cisco . com/pcgi-bin/tablebuild.pl/ios-sigup (только зарегистрированные клиенты).

Процесс для включения SDFs по умолчанию детализирован в, Включают IPS Cisco IOS с SDF Заводской настройки. Когда SDFs по умолчанию не достаточны, или вы хотите добавить новые подписи, можно использовать процедуру, описанную в, Добавляют Дополнительные Подписи после Включения SDF По умолчанию.

Предварительные условия

Требования

Версия 1.4.2 Среды исполнения Java (JRE) или позже требуется, чтобы использовать Cisco SDM 2.2. Рекомендуемый Cisco и настроенный Файл цифровой подписи (на основе DRAM) связан с SDM Cisco (загруженный на памяти флэша - памяти маршрутизатора с SDM Cisco).

Используемые компоненты

Сведения в этом документе основываются на Cisco Router and Security Device Manager (SDM) 2.2.

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

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

Включите IPS Cisco IOS с SDF заводской настройки

Процедура CLI

Завершите эту процедуру для использования CLI для настройки Cisco маршрутизатор серии 1800 с IPS Cisco IOS для загрузки 128MB.sdf на флэше - памяти маршрутизатора.

1. Настройте маршрутизатор для включения уведомления о событии стандарта Security Device Event Exchange (SDEE).`yourname#`**`conf t`**
2. Введите команды настройки (один на линию), и затем нажмите Cntl+Z для окончания.`yourname(config)#`**`ip ips notify sdee`**
3. Создайте имя правила IPS, которое используется для соединения к интерфейсам.`yourname(config)#`**`ip ips name myips`**
4. Настройте команду location IPS для определения, от которого регистрируют систему IPS Cisco IOS, считает подписи.Данный пример использует файл на флэш-памяти: 128 Мбайт. sdf. Часть URL местоположения этой команды может быть любым допустимым URL, который использует флэш-память, диск или протоколы через FTP, HTTP, HTTPS, RTP, SCP и TFTP для обращения к файлам.`yourname(config)#`**`ip ips sdf location flash:128MB.sdf`** **Примечание:** Необходимо включить **команду terminal monitor**, если вы настраиваете маршрутизатор через сеанс Telnet, или вы не будете видеть сообщения SDEE, когда устройство для подписи создаст.
5. Включите IPS на интерфейсе, где вы хотите позволить IPS Cisco IOS просмотреть трафик. В этом случае мы включили на обоих направлениях на interface fastEthernet

0.yourname(config)#**interface fastEthernet 0** yourname(config-if)#**ip ips myips in** *Oct 26 00:32:30.297: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from opacl *Oct 26 00:32:30.921: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from flash:128MB.sdf *Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING: OTHER - 4 signatures - 1 of 15 engines *Oct 26 00:32:30.921: %IPS-6-ENGINE_READY: OTHER - 0 ms - packets for this engines will be scanned *Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING: MULTI-STRING - 0 signatures - 2 of 15 engines *Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILD_SKIPPED: MULTI-STRING - there are no new signature definitions for this engine *Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING: STRING.ICMP - 1 signatures - 3 of 15 engines *Oct 26 00:32:30.941: %IPS-6-ENGINE_READY: STRING.ICMP - 20 ms - packets for this engine will be scanned *Oct 26 00:32:30.945: %IPS-6-ENGINE_BUILDING: STRING.UDP - 17 signatures - 4 of15 engines *Oct 26 00:32:31.393: %IPS-6-ENGINE_READY: STRING.UDP - 448 ms - packets for this engine will be scanned *Oct 26 00:32:31.393: %IPS-6-ENGINE_BUILDING: STRING.TCP - 58 signatures - 5 of 15 engines *Oct 26 00:32:33.641: %IPS-6-ENGINE_READY: STRING.TCP - 2248 ms - packets for this engine will be scanned *Oct 26 00:32:33.641: %IPS-6-ENGINE_BUILDING: SERVICE.FTP - 3 signatures - 6 of 15 engines *Oct 26 00:32:33.657: %IPS-6-ENGINE_READY: SERVICE.FTP - 16 ms - packets for this engine will be scanned *Oct 26 00:32:33.657: %IPS-6-ENGINE_BUILDING: SERVICE.SMTP - 2 signatures - 7 of 15 engines *Oct 26 00:32:33.685: %IPS-6-ENGINE_READY: SERVICE.SMTP - 28 ms - packets for this engine will be scanned *Oct 26 00:32:33.689: %IPS-6-ENGINE_BUILDING: SERVICE.RPC - 29 signatures - 8 f 15 engines *Oct 26 00:32:33.781: %IPS-6-ENGINE_READY: SERVICE.RPC - 92 ms - packets for this engine will be scanned *Oct 26 00:32:33.781: %IPS-6-ENGINE_BUILDING: SERVICE.DNS - 31 signatures - 9 of 15 engines *Oct 26 00:32:33.801: %IPS-6-ENGINE_READY: SERVICE.DNS - 20 ms - packets for this engine will be scanned *Oct 26 00:32:33.801: %IPS-6-ENGINE_BUILDING: SERVICE.HTTP - 132 signatures - 10 of 15 engines *Oct 26 00:32:44.505: %IPS-6-ENGINE_READY: SERVICE.HTTP - 10704 ms - packets for this engine will be scanned *Oct 26 00:32:44.509: %IPS-6-ENGINE_BUILDING: ATOMIC.TCP - 11 signatures - 11 of 15 engines *Oct 26 00:32:44.513: %IPS-6-ENGINE_READY: ATOMIC.TCP - 4 ms - packets for this engine will be scanned *Oct 26 00:32:44.513: %IPS-6-ENGINE_BUILDING: ATOMIC.UDP - 9 signatures - 12 of 15 engines *Oct 26 00:32:44.517: %IPS-6-ENGINE_READY: ATOMIC.UDP - 4 ms - packets for this engine will be scanned *Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING: ATOMIC.ICMP - 0 signatures - 13 of 15 engines *Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.ICMP - there are no new signature definitions for this engine *Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING: ATOMIC.IPOPTIONS - 1 signatures - 14 of 15 engines *Oct 26 00:32:44.517: %IPS-6-ENGINE_READY: ATOMIC.IPOPTIONS - 0 ms - packets for this engine will be scanned *Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING: ATOMIC.L3.IP - 5 signatures - 15 of 15 engines *Oct 26 00:32:44.517: %IPS-6-ENGINE_READY: ATOMIC.L3.IP - 0 ms - packets for this engine will be scanned yourname(config-if)#**ip ips myips out** yourname(config-if)#**ip virtual-reassembly** Первоначально правило IPS применено к интерфейсу, IPS Cisco IOS запускает созданные подписи с файла, заданного командой местоположений SDF. Сообщения SDEE зарегистрированы к консоли и переданы серверу системного журнала, если настроено. Сообщения SDEE с *<number>* механизмов *<number>* указывают на процесс построения устройства для подписи. Наконец, когда эти два номера являются тем же, все механизмы созданы.**Примечание:** Действительная повторная сборка IP является интерфейсной функцией, которая (когда включено) автоматически повторно собирает фрагментированные пакеты, которые входят в маршрутизатор через тот интерфейс. Cisco рекомендует включить IP действительный блок на всех интерфейсах, где трафик входит в маршрутизатор. В вышеупомянутом примере, помимо включения "IP действительного блока" на interface fastEthernet 0, мы настраиваем его на внутреннем интерфейсе VLAN 1 также.yourname(config)#**int vlan 1** yourname(config-if)#**ip virtual-reassembly**

Процедура SDM 2.2

Завершите эту процедуру для использования Cisco SDM 2.2 для настройки Cisco маршрутизатор серии 1800 с IPS Cisco IOS.

1. В приложении SDM нажмите **Configure**, и затем нажмите **Intrusion Prevention**.

2. Нажмите вкладку **Create IPS**, и затем нажмите **Launch IPS Rule Wizard**.SDM Cisco требует уведомления о событии IPS через SDEE для настройки функции IPS Cisco IOS. По умолчанию уведомление SDEE не включено. SDM Cisco побуждает вас включать уведомление о событии IPS через SDEE как показано в этом образе:
3. **Нажмите кнопку OK.**Приветствие к Окну мастера Политики IPS диалогового окна IPS Policies Wizard появляется.
4. **Нажмите кнопку Next.**Окно Select Interfaces появляется.
5. Выберите интерфейсы, для которых вы хотите включить IPS и нажать флажок **Inbound или Outbound** для указания на направление того интерфейса.**Примечание:** Cisco рекомендует включить и входящий и исходящие направления при включении IPS на интерфейсе.
6. **Нажмите кнопку Next.**Окно SDF Locations появляется.
7. **Нажмите Add** для настройки местоположения SDF.Добавление диалогового окна Location Подписи появляется.
8. Нажмите **Specify SDF на** кнопке с зависимой фиксацией **флэш-памяти** и выберите 256MB.sdf из **Имени файла на** выпадающем списке **флэш-памяти**.
9. Нажмите флажок **автосохранения** и нажмите **OK**.**Примечание:** Когда существует изменение подписи, опция автосохранения автоматически сохраняет Файл цифровой подписи.Окно SDF Locations отображает новое местоположение SDF.**Примечание:** Можно добавить дополнительные местоположения подписи для обозначения резервной копии.
10. Нажмите **Use Built-In Signatures (как резервная копия)** флажок.**Примечание:** Cisco рекомендует не использовать встроенную опцию подписи, пока вы не задали одно или более местоположений.
11. Нажмите **Next** для продолжения.Окно со сводной информацией появляется.
12. **Нажмите кнопку Finish.**Выводы информации на экран Диалога состояния Доставки Команд статус как механизм IPS компилируют все подписи.
13. Как только процесс завершен, нажмите **OK**.Выводы информации на экран Диалога состояния Компиляции Подписи информация о компиляции подписи.Эта информация показывает, какие механизмы были скомпилированы и количество подписей в том механизме. Для механизмов, которые отображаются *Пропущенный* в столбце состояния, нет никакой подписи, загруженной для того механизма.
14. Нажмите **Close** для закрытия коробки Диалога состояния Компиляции Подписи.
15. Для проверки, какие подписи в настоящее время загружаются на маршрутизаторе, нажмите **Configure**, и затем нажмите **Intrusion Prevention**.
16. Нажмите вкладку **Edit IPS**, и затем нажмите **Signatures**.Список подписи IPS появляется в окне Signatures.

Добавьте Дополнительные Подписи после Включения SDF По умолчанию

Процедура CLI

Нет никакой команды CLI, доступной, чтобы создать подписи или считать данные о подписи из распределенного файла IOS-Sxxx.zip. Cisco рекомендует использовать или SDM или Центр управления сенсорами IPS для управления подписями в системах IPS Cisco IOS.

Для клиентов, которые уже имеют готовый Файл цифровой подписи и хотят объединить этот файл с SDF, который работает на системе IPS Cisco IOS, можно использовать эту команду:

yourname#**show running-config | include ip ips sdf** ip ips sdf location flash:128MB.sdf yourname# Файл цифровой подписи, определенный командой location подписи, - то, где маршрутизатор загружает файлы подписей, когда это перезагружается или когда реконфигурирован IPS IOS маршрутизатора. Для процесса слияния, чтобы быть успешным, должен также быть обновлен файл, определенный командой location Файла цифровой подписи.

1. Используйте **команду показа** для проверки в настоящее время настраиваемых местоположений подписи.Выходные данные показывают настроенные местоположения подписи. Эта команда показывает от того, где загружены текущие рабочие подписи.yourname#**show ip ips signatures** Builtin signatures are configured Подписи были в последний раз загружены из flash:128MB.sdfОкончательный релиз SDF Cisco S128.0Окончательный релиз SDF тенденции V0.0
2. Используйте команду **ips-sdf** ***<url>*** **копии**, наряду с информацией от предыдущего шага, для слияния Файлов цифровой подписи.yourname#**copy tftp://10.10.10.5/mysignatures.xml ips-sdf** Loading mysignatures.xml from 10.10.10.5 (via Vlan1): ! [OK - 1612 bytes] *Oct 26 02:43:34.904: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from opacl No entry found for lport 55577, fport 4714 No entry found for lport 51850, fport 4715 *Oct 26 02:43:34.920: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from tftp://10.10.10.5/mysignatures.xml *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: OTHER - 4 signatures - 1 of 15 engines *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: OTHER - there are no new signature definitions for this engine *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: MULTI-STRING - 0 signatures - 2 of 15 engines *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: MULTI-STRING - there are no new signature definitions for this engine *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.ICMP - 1 signatures - 3 of 15 engines *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.ICMP - there are no new signature definitions for this engine *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.UDP - 17 signatures - 4 of 15 engines *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.UDP - there are no new signature definitions for this engine *Oct 26 02:43:34.924: %IPS-6-ENGINE_BUILDING: STRING.TCP - 59 signatures - 5 of 15 engines *Oct 26 02:43:36.816: %IPS-7-UNSUPPORTED_PARAM: STRING.TCP 9434:0 CapturePacket=False - This parameter is not supported *Oct 26 02:43:37.264: %IPS-6-ENGINE_READY: STRING.TCP - 2340 ms - packets for this engine will be scanned *Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.FTP - 3 signatures - 6 of 15 engines *Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.FTP - there are no new signature definitions for this engine *Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.SMTP - 2 signatures - 7 of 15 engines *Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.SMTP - there are no new signature definitions for this engine *Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.RPC - 29 signatures - 8 of 15 engines *Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.RPC - there are no new signature definitions for this engine *Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILDING: SERVICE.DNS - 31 signatures - 9 of 15 engines *Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.DNS - there are no new signature definitions for this engine *Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILDING: SERVICE.HTTP - 132 signatures - 10 of 15 engines *Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.HTTP - there are no new signature definitions for this engine *Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.TCP - 11 signatures - 11 of 15 engines *Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.TCP - there are no new signature definitions for this engine *Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.UDP - 9 signatures - 12 of 15 engines *Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.UDP - there are no new signature definitions for this engine *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.ICMP - 0 signatures - 13 of 15 engines *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.ICMP - there are no new signature definitions for this engine *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.IPOPTIONS - 1 signatures - 14 of 15 engines *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.IPOPTIONS - there are no new signature definitions for this engine *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.L3.IP - 5 signatures - 15 of 15 engines *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.L3.IP - there are no new signature definitions for this engine yourname# После выдачи команды **копии** маршрутизатор загружает Файл цифровой подписи в память и затем создает устройства для подписи. В консольном выводе сообщений SDEE отображен статус здания для каждого устройства для подписи.%IPS-

6-ENGINE_BUILD_SKIPPED указывает, что нет никаких новых подписей для этого механизма.%IPS-6-ENGINE_READY указывает, что существуют новые подписи, и механизм готов. Как прежде, "15 из 15 механизмов" сообщение указывают, что были созданы все механизмы.IPS-7-UNSUPPORTED_PARAM указывает, что определенный параметр не поддерживается IPS Cisco IOS. Например, CapturePacket и ResetAfterIdle.**Примечание:** Эти сообщения только для информации и не будут иметь никакого влияния на возможности подписи IPS Cisco IOS или производительности. Эти сообщения регистрации могут быть выключены путем установки уровня регистрации выше, чем отладка (уровня 7).

3. Обновите SDF, определенный командой location подписи, такой это, когда перезагрузки маршрутизатора, этому установят объединенную подпись с обновленными подписями. Данный пример показывает различие в размере файла после того, как объединенная подпись будет сохранена к 128MB.sdf флэш - файл.`yourname#`**`show flash:`** `-#- --length-- -----date/time------ path 4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf yourname#`**`copy ips-sdf flash:128MB.sdf`** `yourname#`**`show flash:`** `-#- --length-- -----date/time------ path 4 522656 Oct 26 2005 02:51:32 +00:00 128MB.sdf` **% Warning:** Новое 128MB.sdf теперь содержит объединенные клиентами подписи. Содержание отличается от Cisco по умолчанию 128MB.sdf файл. Cisco рекомендует изменить этот файл на другое имя для предотвращения беспорядка. Если название изменено, команда location подписи должна быть изменена также.

Процедура SDM 2.2

После того, как IPS Cisco IOS был включен, новые подписи могут быть добавлены в маршрутизатор, который выполняет набор подписи с функцией импорта SDM Cisco. Выполните эти шаги для импорта новых подписей:

1. Выберите SDFs по умолчанию или файл обновления IOS-Sxxx.zip для импорта дополнительных подписей.
2. Нажмите **Configure**, и затем нажмите **Intrusion Prevention**.
3. Нажмите вкладку **Edit IPS**, и затем нажмите **Import**.
4. Выберите **From PC** из выпадающего списка Импорта.
5. Выберите файл, из которого вы хотите импортировать подписи.Данный пример использует последнее обновление, загруженное от Cisco.com, и экономил на жестком диске локального компьютера.
6. **Нажмите кнопку Open.% Warning:** Из-за ограничений связанные с памятью, только ограниченное число новых подписей может быть добавлено поверх подписей, которые были уже развернуты. Если слишком много подписей выбраны, маршрутизатор не мог бы быть в состоянии загрузить все новые подписи из-за недостаточно памяти.Как только загрузка Файла цифровой подписи завершает, диалоговое окно IPS Import появляется.
7. Перейдите через левый просмотр дерева и нажмите флажок **Import** рядом с подписями, которые вы хотите импортировать.
8. Нажмите кнопку с зависимой фиксацией **Merge**, и затем нажмите **OK**.**Примечание:** Опция Replace заменяет текущий набор подписи на маршрутизаторе с подписями, которые вы выбираете для импорта.Как только вы нажимаете OK, приложение SDM Cisco отправляет подписи маршрутизатору.**Примечание:** Высокая загрузка ЦП происходит во время компиляции и загрузки подписей. После того, как IPS Cisco IOS включен на интерфейсе, Файл цифровой подписи начинает загружаться. Маршрутизатор занимает приблизительно пять минут для загрузки SDF. Можно

попытаться использовать **команду show process cpu** для просмотра загрузки ЦПУ от CLI программного обеспечения Cisco IOS. Однако не пытайтесь использовать дополнительные команды или загрузить другой SDFs, в то время как маршрутизатор загружает SDF. Это может заставить процесс компиляции подписи занимать больше времени для завершения (так как загрузка ЦПУ близко к 100 процентам загрузки во время загрузки SDF). Вы, возможно, должны были бы просмотреть список подписей и включить подписи, если они не находятся во *включенном* состоянии.Общий номер подписи увеличился до 519. Этот номер включает все подписи, доступные в файл IOS-S193.zip, которые принадлежат подкатегории Общего файла.

Для большего количества сложных вопросов о том, как использовать SDM Cisco для управления функцией IPS Cisco IOS, обратитесь к документации SDM Cisco в этом URL:

Выберите Signatures и Work with Signature Categories

Чтобы определить, как эффективно выбрать корректные подписи для сети, необходимо знать несколько вещей о сети, которую вы защищаете. Обновленная информация о категории подписи в Cisco SDM 2.2 и позже далее помогает клиентам выбирать корректный набор подписей для защиты сети.

Категория является способом сгруппировать подписи. Это помогает сужать выбор подписи к подмножеству подписей, которые относятся друг к другу. Одна подпись могла принадлежать только одной категории, или это могло принадлежать нескольким категорий.

Это пять категорий верхнего уровня:

- ОС — Основанная на операционной системе классификация подписи
- Атака — Основанная на атаке классификация подписи
- Сервис — Основанная на сервисе классификация подписи
- Протокол уровня 2-4 — классификация подписи На уровне протокола
- Версии — Основанная на выпуске классификация подписи

Каждая из этих категорий далее разделена на подкатегории.

Как пример, рассмотрите домашнюю сеть с широкополосным соединением к Интернету и VPN-туннелем к корпоративной сети. Широкополосному маршрутизатору позволили межсетевому экрану Cisco IOS на открытом (не-VPN) соединение с Интернетом препятствовать тому, чтобы любое соединение инициировалось из Интернета и соединялось с домашней сетью. Весь трафик, который происходит от домашней сети до Интернета, разрешен. Предположите, что пользователь использует ПК под управлением Windows приложения и использует приложения как HTTP (просмотр веб - ресурсов) и электронная почта.

Межсетевой экран может быть настроен так, чтобы только приложения, что пользовательским потребностям позволяют течь через маршрутизатор. Это будет управлять потоком нежелательного и потенциально плохого трафика, который может распространиться всюду по сети. Полагайте, что домашний пользователь не нуждается или использует определенный сервис. Если тому сервису позволяют течь через межсетевой экран, существует потенциальная яма, которую атака может использовать для течения всюду по сети. Оптимальные методы только позволяют сервисы, которые необходимы. Теперь, легче выбрать что подписи включить. Необходимо включить подписи только для сервисов, что вы позволяете течь через межсетевой экран. В данном примере сервисы включают электронную почту и HTTP. SDM Cisco упрощает эту конфигурацию.

Для использования категории, чтобы выбрать требуемые подписи, выбрать **Service> HTTP** и включить все подписи. Этот процесс выбора также работает в диалоговом окне импорта подписи, где можно выбрать все подписи HTTP и импортировать их в маршрутизатор.

Дополнительные категории, которые должны быть выбраны, включают DNS, NETBIOS/SMB, HTTPS и SMTP.

Подписи обновления для файлов SDF по умолчанию

Три на - создали SDFs (атака-drop.dsf, 128MB.sdf, и 256MB.sdf) в настоящее время зарегистрированы на Cisco.com в http://www. cisco . com/pcgi-bin/tablebuild.pl/ios-sigup (только зарегистрированные клиенты). Более новые версии этих файлов будут зарегистрированы, как только они доступны. Для обновления маршрутизаторов, которые работают, IPS Cisco IOS с ними принимают значение по умолчанию SDFs, переходят к веб-сайту и загружают последние версии этих файлов.

Процедура CLI

1. Скопируйте загружаемые файлы к местоположению, где маршрутизатор настроен для загрузки этих файлов из. Для обнаружения, где маршрутизатор в настоящее время настраивается используйте **команду show running-config | in ip ips sdf**.`Router#show running-config | in ip ips sdf ip ips sdf location flash://256MB.sdf autosave` В данном примере маршрутизатор использует 256MB.sdf на флэш-памяти. Файл обновлен при копировании нового, загруженного 256MB.sdf к флэшу - памяти маршрутизатора.
2. Повторно загрузите подсистему IPS Cisco IOS для петляния.Существует два способа повторно загрузить IPS Cisco IOS: повторно загрузите маршрутизатор или реконфигурируйте IPS Cisco IOS для инициирования подсистемы IPS IOS для повторной загрузки подписей. Для реконфигурирования IPS Cisco IOS удалите все правила IPS из настраиваемых интерфейсов, и затем повторно примените правила IPS назад к интерфейсам. Это инициирует систему IPS Cisco IOS для повторной загрузки.

Процедура SDM 2.2

Выполните эти шаги для обновления SDFs по умолчанию на маршрутизаторе:

1. Нажмите **Configure**, и затем нажмите **Intrusion Prevention**.
2. Нажмите вкладку **Edit IPS**, и затем нажмите **Global Settings**.Вершина UI показывает глобальные параметры. Нижняя половина UI показывает в настоящее время настраиваемые местоположения SDF. В этом случае 256MB.sdf файл от флэш-памяти настроен.
3. Выберите **File Management** из Меню Файл.Диалоговое окно File Management появляется.
4. Нажмите **файл Load от ПК**.Диалоговое окно Save File появляется.
5. Выберите SDF, который должен быть обновлен, и нажимать **Open**.Предупреждающее сообщение SDM появляется.
6. Нажмите **Yes** для замены существующего файла.Диалоговое окно отображает выполнение процесса загрузки.
7. Как только процесс загрузки завершен, нажмите **Reload Signatures**, расположенный на панели инструментов location SDF. Это действие повторно загружает IPS Cisco IOS.**Примечание:** Пакет IOS-Sxxx.zip содержит все подписи тот IPS Cisco IOS

поддержки. Обновления к этому пакету подписи зарегистрированы на Cisco.com, как только они становятся доступными. Для обновления подписей, содержавшихся в этом пакете, посмотрите Шаг 2.

Дополнительные сведения

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