Установите и настройте сервисный модуль FirePOWER на платформе ASA

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Общие сведения
Перед началом работы
Установить
Установите модуль SFR на ASA
Установите ASA образ загрузки SFR
Настройка
Настройте программное обеспечение FirePOWER
Настройте центр управления FireSIGHT
Трафик перенаправления к модулю SFR
Проверка
Устранение неполадок
Дополнительные сведения

Введение

Этот документ описывает, как установить и настроить (SFR) модуль Cisco FirePOWER, который работает на устройстве адаптивной защиты Cisco (ASA) и как зарегистрировать модуль SFR в Центре управления Cisco FireSIGHT.

Предварительные условия

Требования

Cisco рекомендует, чтобы ваша система удовлетворила эти требования перед попыткой процедур, которые описаны в этом документе:

- Гарантируйте, что у вас есть по крайней мере 3 ГБ свободного места на флэш-накопителе (disk0), в дополнение к размеру загрузочного программного обеспечения.
- Гарантируйте, что у вас есть доступ к привилегированному режиму EXEC. Для доступа к привилегированному режиму EXEC введите **команду enable** в CLI. Если пароль был "not set", то нажмите **Enter**:

```
ciscoasa> enable
Password:
ciscoasa#
```

Используемые компоненты

Для установки FirePOWER Services на Cisco ASA эти компоненты требуются:

- Версия программного обеспечения 9.2.2 Cisco ASA или позже
- Платформы Cisco ASA, 5512-X через 5555-X
- Версия программного обеспечения 5.3.1 FirePOWER или позже

Примечание: Если вы хотите установить FirePOWER (SFR) Сервисы на ASA 5585-X Модуль оборудования, считайте Установку FirePOWER (SFR) Сервисы на ASA 5585-X Модуль оборудования.

Эти компоненты требуются на Центре управления Cisco FireSIGHT:

- Версия программного обеспечения 5.3.1 FirePOWER или позже
- Центр управления FireSIGHT FS2000, FS4000 или виртуальное устройство

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.

Общие сведения

Cisco ASA модуль FirePOWER, также известный как ASA SFR, предоставляет Сервисы межсетевого экрана следующего поколения, такие как:

- Система предотвращения вторжений следующего поколения (NGIPS)
- Видимость приложения и контроль (AVC)
- Фильтрация URL-адресов
- Усовершенствованная вредоносная защита (AMP)

Примечание: Можно использовать ASA модуль SFR в Одиночном или Многоконтекстном режиме, и в Направленном или Прозрачном режиме.

Перед началом работы

Рассмотрите эту важную информацию перед попыткой процедур, которые описаны в этом документе:

- Если у вас есть политика активного сервиса, которая перенаправляет трафик к Системе предотвращения вторжений (IPS) / С учетом контекста (CX) модуль (что вы заменили ASA SFR), необходимо удалить его перед настройкой ASA политика обслуживания SFR.

- Необходимо завершить работу любых других модулей ПО, которые это в настоящее время выполняет. Устройство может выполнить одиночный модуль ПО за один раз. Необходимо сделать это от CLI ASA. Например, эти команды завершение работы и удаление модуль ПО IPS, и затем повторно загружают ASA:
```
ciscoasa# sw-module module ips shutdown
ciscoasa# sw-module module ips uninstall
ciscoasa# reload
```
Команды, которые используются для удаления модуля CX являются тем же, кроме **cxsc**

ключевого слова используется вместо **ips**:

```
ciscoasa# sw-module module cxsc shutdown
ciscoasa# sw-module module cxsc uninstall
ciscoasa# reload
```

- Когда вы повторно захватываете образ модуль, используйте то же **завершение** и **деинсталлируйте** команды, которые используются для удаления старого образа SFR. Например:

```
ciscoasa# sw-module module sfr uninstall
```

- Если ASA, модуль SFR используется в Многоконтекстном режиме, выполняют процедуры, которые описаны в этом документе в системном поле выполнения.

Совет: Для определения статуса модуля на ASA введите **команду show module**.

Установить

В этом разделе описывается установить модуль SFR на ASA и как установить ASA образ загрузки SFR.

Установите модуль SFR на ASA

Выполните эти шаги для установки модуля SFR на ASA:

1. Загрузите ASA системное программное обеспечение SFR от Cisco.com до HTTP, HTTPS или сервера FTP, который доступен от ASA интерфейс управления SFR.
2. Загрузите образ загрузки к устройству. Можно использовать или Cisco Adaptive Security Device Manager (ASDM) или CLI ASA для загрузки образа загрузки к устройству. **Примечание:** Не передавайте системное программное обеспечение; это загружено позже к Твердотельному диску (SSD).Выполните эти шаги для загрузки образа загрузки через ASDM: Загрузите образ загрузки к своей рабочей станции или разместите его в FTP, TFTP, HTTP, HTTPS, Блок сообщений сервера (SMB) или сервер Протокола SCP.Выберите **Tools> File Management** в ASDM.Выберите соответствующую команду File Transfer, или *Между Локальным компьютером и Флэшем* или *Между Удаленным сервером и Флэшем*.Передайте загрузочное программное обеспечение флэш-накопителю (disk0) на ASA.Выполните эти шаги для загрузки образа загрузки через CLI ASA:Загрузите образ загрузки на FTP, TFTP, HTTP или сервере HTTPS.Введите команду **копии** в CLI для загрузки образа загрузки к флэш-накопителю. Вот пример, который использует HTTP - протокол (замените **<HTTP_Server>** вашим IP-адресом сервера или именем хоста):`ciscoasa# copy http://<HTTP_SERVER>/asasfr-5500x-boot-5.3.1-152.img disk0:/asasfr-5500x-boot-5.3.1-152.img`
3. Введите эту команду для настройки ASA местоположение образа загрузки SFR во флэш-накопителе ASA:

```
ciscoasa# sw-module module sfr recover configure image disk0:/file_path
```

   Например:

```
ciscoasa# sw-module module sfr recover configure image disk0:
 /asasfr-5500x-boot-5.3.1-152.img
```

4. Введите эту команду для загрузки ASA образ загрузки SFR:

```
ciscoasa# sw-module module sfr recover boot
```

   В это время при включении **загрузки модуля отладки** на ASA эти отладки распечатаны:

```
ciscoasa# sw-module module sfr recover boot
```

5. Ждите приблизительно 5 - 15 минут ASA модуль SFR, чтобы загрузить, и затем

открыть сеанс консоли для в рабочем состоянии ASA образ загрузки SFR.

Установите ASA образ загрузки SFR

Выполните эти шаги для устанавливания недавно установленного ASA образ загрузки SFR:

1. Нажмите **Enter** после открытия сеанса для достижения приглашения регистрации. **Примечание:** Имя пользователя по умолчанию является **admin**, и пароль по умолчанию является **Admin123**.Например:
```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```
Совет: Если ASA, который загрузка модуля SFR не завершила, сбои команды сеанса и сообщение, кажется, указывает, что система неспособна соединиться по TTYS1. Если это происходит, ждите загрузки модуля, чтобы завершить и попробовать еще раз.
2. Введите команду **настройки** для настройки системы так, чтобы можно было установить пакет системного программного обеспечения:
```
asasfr-boot> setup
Welcome to SFR Setup
[hit Ctrl-C to abort]
Default values are inside []
```
Вам тогда предлагают для этой информации:**Имя хоста** - имя хоста может быть до 65 алфавитно-цифровых знаков без пробелов. Использование дефисов позволено.**Сетевой адрес** - сетевой адрес может быть или статическим IPv4 или адресами IPv6. Можно также использовать DHCP для IPv4 или IPv6 автоматическая конфигурация не сохраняющая состояние.**Информация DNS** - необходимо определить по крайней мере один сервер Системы доменных имен (DNS), и можно также установить доменное имя и область поиска.**Информация NTP** - можно включить Протокол NTP и настроить серверы NTP для установки системного времени.
3. Введите **системную** команду **установки** для установки образа программного обеспечения системы:
```
asasfr-boot >system install [noconfirm] url
```
Включайте **noconfirm** опцию, если вы не хотите отвечать на подтверждающие сообщения. Замените ключевое слово **URL** местоположением **.pkg** файла. Например:
```
asasfr-boot >system install http://<HTTP_SERVER>/asasfr-sys-5.3.1-152.pkg
Verifying
Downloading
Extracting

Package Detail
Description: Cisco ASA-FirePOWER 5.3.1-152 System Install
Requires reboot: Yes

Do you want to continue with upgrade? [y]: y
Warning: Please do not interrupt the process or turn off the system. Doing so
might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image
Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
```

```
(press Enter)

Broadcast message from root (ttyS1) (Mon Jun 23 09:28:38 2014):
The system is going down for reboot NOW!
Console session with module sfr terminated.
```

Примечание: Когда установка завершена, системные перезагрузки. Позвольте десяти или больше минутам для установки компонента приложения и для ASA сервисы SFR запускаться. Выходные данные **команды "show module" sfr** команда должны указать, что все процессы подключены.

Настройка

В этом разделе описывается настроить программное обеспечение FirePOWER и Центр управления FireSIGHT, и как перенаправить трафик к модулю SFR.

Настройте программное обеспечение FirePOWER

Выполните эти шаги для настройки программного обеспечения FirePOWER:

1. Откройте сеанс для ASA модуль SFR.
   Примечание: Другое приглашение регистрации теперь появляется, потому что вход в систему происходит на полностью-функциональном-модуле.Например:
   ```
   ciscoasa# session sfr
   Opening command session with module sfr.
   Connected to module sfr. Escape character sequence is 'CTRL-^X'.
   Sourcefire ASA5555 v5.3.1 (build 152)
   Sourcefire3D login:
   ```
2. Войдите с **именем пользователя admin** и **паролем Admin123**.
3. Завершите конфигурацию системы, как предложено, которая происходит в этом заказе: Считайте и примите Лицензионное соглашение с конечным пользователем (EULA).Измените пароль администратора.Настройте адрес управления и параметры настройки DNS, как предложено. **Примечание:** Можно настроить и IPv4 и адреса управления IPv6.Например:
   ```
   ciscoasa# session sfr
   Opening command session with module sfr.
   Connected to module sfr. Escape character sequence is 'CTRL-^X'.
   Sourcefire ASA5555 v5.3.1 (build 152)
   Sourcefire3D login:
   ```
4. Ждите системы для реконфигурирования себя.

Настройте центр управления FireSIGHT

Для управления ASA модуль SFR и политика безопасности, необходимо зарегистрировать его в Центре управления FireSIGHT. Вы не можете выполнить эти действия с Центром управления FireSIGHT:

- Настройте ASA интерфейсы модуля SFR
- Завершение работы, перезапуск, или иначе управляют ASA процессы модуля SFR
- Создайте резервные копии от или восстановите резервные копии к, ASA модульные устройства SFR
- Контроль за доступом с правом записи управляет для соответствия с трафиком с

использованием условий тега VLAN

Трафик перенаправления к модулю SFR

Для перенаправления трафика к ASA модуль SFR необходимо создать политику обслуживания, которая определяет определенный трафик. Выполните эти шаги для перенаправления трафика к ASA модуль SFR:

1. Выберите трафик, который должен быть определен с **командой access-list**. В данном примере перенаправлен весь трафик от всех интерфейсов. Можно сделать это для определенного трафика также.
   ```
   ciscoasa(config)# access-list sfr_redirect extended permit ip any any
   ```
2. Создайте class-map для соответствия с трафиком на списке доступа:
   ```
   ciscoasa(config)# class-map sfr
   ciscoasa(config-cmap)# match access-list sfr_redirect
   ```
3. Задайте режим развертываний. Можно настроить устройство или в пассивном или во встроенном (обычном) режиме развертываний (только для монитора).
   Примечание: Вы не можете настроить обоих пассивный режим и встроить режим в то же время на ASA. Только один тип политики безопасности позволен.Во встроенных развертываниях, после того, как нежелательный трафик отброшен и любые другие действия, которые применены политикой, выполнены, трафик возвращен к ASA для дальнейшей обработки и окончательной передачи. Данный пример показывает, как создать policy-map и настроить ASA модуль SFR во встроенном режиме:
   ```
   ciscoasa(config)# policy-map global_policy
   ciscoasa(config-pmap)# class sfr
   ciscoasa(config-pmap-c)# sfr fail-open
   ```

   В пассивных развертываниях копия трафика передается сервисному модулю SFR, но это не возвращено к ASA. Пассивный режим позволяет вам просматривать действия, которые модуль SFR завершил бы в отношении трафика. Это также позволяет вам оценивать содержание трафика без влияния к сети.

   Если вы хотите настроить модуль SFR в пассивном режиме, используйте ключевое слово **только для монитора** (как показано в следующем примере). Если вы не включаете ключевое слово, трафик передается во встроенном режиме.
   ```
   ciscoasa(config-pmap-c)# sfr fail-open monitor-only
   ```
   % Warning: Режим **только для монитора** не позволяет сервисному модулю SFR запрещать или блокировать вредоносный трафик.**Внимание. :** Могло бы быть возможно настроить ASA в режиме *только для монитора* с использованием интерфейсного **форварда трафика sfr** команда **только для монитора**; однако, эта конфигурация просто для демонстрационной функциональности и не должна использоваться на производственном ASA. Любые проблемы, которые найдены в этой демонстрационной функции, не поддерживаются Центром технической поддержки Cisco (TAC). Если вы желаете развернуть ASA сервис SFR в пассивном режиме, настройте его с использованием *policy-map*.
4. Задайте местоположение и примените политику. Можно применить политику глобально или на интерфейсе. Для переопределения глобальной политики на интерфейсе можно применить политику обслуживания к тому интерфейсу.

   Глобальное ключевое слово применяет карту политик ко всем интерфейсам, и

интерфейсное ключевое слово применяет политику к одному интерфейсу . Допускается только одна глобальная политика. В данном примере политика применена глобально:

```
ciscoasa(config)# service-policy global_policy global
```

Внимание. : Карта политик **global_policy** является политикой по умолчанию. При использовании эту политику и хотите удалить ее на вашем устройстве для целей устранения проблем, гарантировать понимание его результата.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Зарегистрируйте устройство в центре управления FireSIGHT
- Развертывания центра управления FireSIGHT на VMware ESXi
- Сценарии конфигурации управления IPS на 5500-X модуле ips
- Cisco Systems – техническая поддержка и документация