Пример базовой конфигурации FWSM

Содержание

Введение

В этом документе описан порядок базовой настройки модуля служб брандмауэра (FWSM), установленного либо на коммутаторах серии Cisco 6500, либо на маршрутизаторах серии Cisco 7600. Сюда входит настройка IP-адресов, маршрутизации по умолчанию, статической и динамической трансляции сетевых адресов (NAT), а также списков контроля доступа (ACL) для фильтрации нежелательного трафика. Кроме того, описывается настройка серверов приложений (таких как Websense) для проверки локального интернет-трафика и веб-серверов для интернет-пользователей.

Предварительные условия

Требования

Для данного документа нет особых требований.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного и аппаратного обеспечения:

- Модуль служб брандмауэра с ПО 3.1 или более поздней версии.
- Коммутаторы серии Catalyst 6500 с требуемыми компонентами, как показано:
  1. Модуль Supervisor engine с ПО Cisco IOS®, также называемый супервизором Cisco IOS, либо операционной системой (ОС) Catalyst. См. Таблицу со списком поддерживаемых выпусков ПО и модуля supervisor engine.
  2. Плата MSFC 2 с программным обеспечением Cisco IOS. См. Таблицу со списком поддерживаемых версий ПО Cisco IOS.

	Модули Supervisor Engine[1]
Версия ПО Cisco IOS	

ПО Cisco IOS версии 12.2(18)SXF и выше	720, 32
ПО Cisco IOS версии 12.2(18)SXF2 и выше	2, 720, 32
Модульное ПО Cisco IOS	
ПО Cisco IOS версии 12.2(18)SXF4	720, 32
Операционная система Catalyst[2]	
версии 8.5(3) и выше	2, 720, 32

[1] FWSM не поддерживает модуль supervisor engine версии 1 или 1A.

[2] При использовании ОС Catalyst на модуле supervisor engine на плате MSFC можно использовать любую поддерживаемую версию ПО Cisco IOS. При использовании ПО Cisco IOS на модуле supervisor engine на плате MSFC должна быть установлена та же версия ПО.

Данные сведения были получены в результате тестирования приборов в специфической лабораторной среде. В качестве начальной конфигурации для всех описанных в документе устройств использовались стандартные (заводские) настройки. В условиях реально действующей сети при использовании каждой команды необходимо четко понимать, какие последствия может иметь применение той или иной команды.

Сопутствующие продукты

Эти настройки также справедливы для маршрутизаторов серии Cisco 7600 с требуемыми компонентами, как показано:

- Модуль supervisor engine с программным обеспечением Cisco IOS. См. Таблицу со списком поддерживаемых выпусков ПО Cisco IOS и модуля supervisor engine.
- Плата MSFC 2 с программным обеспечением Cisco IOS. См. Таблицу со списком поддерживаемых версий ПО Cisco IOS.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в статье Cisco Technical Tips Conventions (Условные обозначения, используемые в технической документации Cisco).

Общие сведения

FWSM представляет собой высокопроизводительный, компактный, отслеживающий состояние модуль брандмауэра, который устанавливается на коммутаторы серии Catalyst 6500 и маршрутизаторы серии Cisco 7600.

Брандмауэры защищают локальные сети от доступа неавторизованных пользователей извне. Брандмауэр также может защитить локальные сети друг от друга, например, если сеть с кадровой информацией работает отдельно от пользовательской сети. Если часть сетевых ресурсов необходимо открыть для внешнего доступа, например веб-сервер или FTP-сервер, можно поместить эти ресурсы в отдельную сеть, защищенную брандмауэром, которую называют "демилитаризованной" зоной (DMZ). Брандмауэр предоставляет ограниченный доступ к DMZ, а так как DMZ включает в себя только публичные серверы, при атаке пострадают только они, в то время как внутренняя локальная сеть не пострадает. Вы также можете контролировать доступ локальных пользователей к внешним ресурсам, например, к Интернету; вы можете разрешить доступ только к указанным сайтам, потребовать аутентификации или авторизации, либо

настроить удаленный фильтр URL-адресов.

FWSM включает множество дополнительных функций, например "несколько контекстов безопасности", похожие на виртуализованные брандмауэры, прозрачный (Слой 2) или маршрутизируемый (Слой 3) режимы работы брандмауэра, сотни интерфейсов и многие другие функции.

Итак, подключенные к брандмауэру сети работают следующим образом: внешняя сеть находится перед брандмауэром; внутренняя сеть защищена и находится за брандмауэром, при этом к зоне DMZ, которая защищена брандмауэром, имеется ограниченный доступ извне. В связи с тем, что FWSM позволяет настроить много интерфейсов с разными политиками безопасности, включающими различные внутренние интерфейсы, зоны DMZ и даже при желании внешние интерфейсы, данные инструкции описывают только стандартные ситуации.

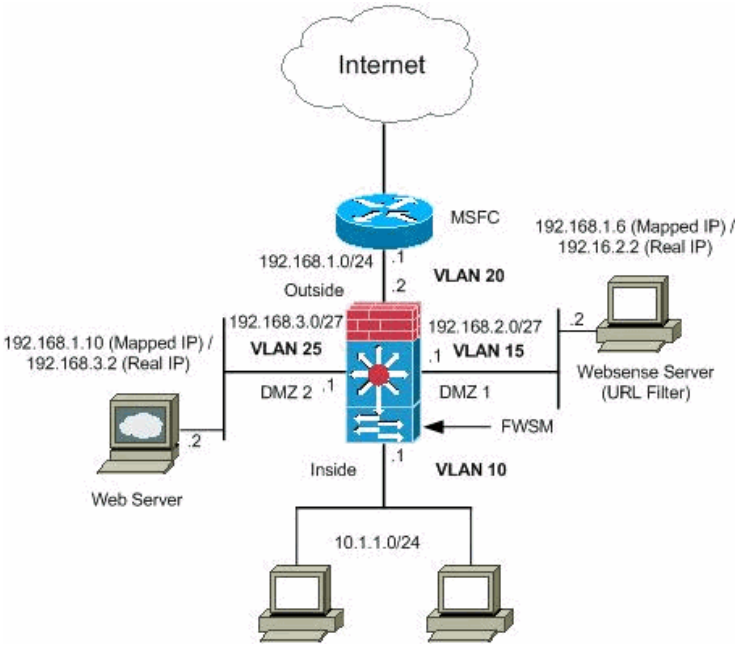
Конфигурация

В этом разделе приводится информация по настройке функций, описанных в данном документе.

Примечание: Используйте Средство поиска команд (registered customers only) для получения дополнительной информации по используемым в данном разделе командам.

Сетевой график

В данном документе используется следующая настройка сети:



Примечание: Использованные в этой конфигурации схемы IP-адресов даны для примера и не годятся для использования в Интернете. Это адреса RFC 1918, которые использовались в лабораторной среде.

Конфигурации

Этот документ использует следующие конфигурации:

- Настройка коммутатора серии Catalyst 6500
- Настройка модуля FWSM

Настройка коммутатора серии Catalyst 6500

1. Вы можете установить плату FWSM в коммутаторы серии Catalyst 6500, или в маршрутизаторы серии Cisco 7600. Конфигурация обеих серий идентична и в данном документе серии упоминаются под общим названием **коммутатор**.

   Примечание: Необходимо правильно настроить коммутатор перед конфигурацией FWSM.

2. **Назначение сети VLAN модулю FWSM** — раздел описывает процесс назначения сети VLAN модулю FWSM. Модуль FWSM не включает в себя каких-либо внешних физических интерфейсов. Вместо этого он использует интерфейсы сетей VLAN. Назначение сети VLAN модулю FWSM схоже с процедурой назначения сети VLAN порту коммутатора; в модуль FWSM входит внутренний интерфейс подключения к модулю фабрик коммутации (при наличии) либо общая шина.

   Примечание: Дополнительные сведения о сетей VLAN и назначении их портам коммутатора см. в разделе Настройка сети VLAN руководства по настройке ПО коммутаторов серии Catalyst 6500.

   1. **Рекомендации по использованию сетей VLAN:**

      1. Вы можете использовать частные сети VLAN вместе с FWSM. Назначьте первичную сеть VLAN модулю FWSM; после чего FWSM автоматически сможет работать с трафиком вторичной сети VLAN.

      2. Зарезервированные сети VLAN использовать нельзя.

      3. Нельзя использовать сеть VLAN с идентификатором "1".

      4. Если вы используете резервный FWSM в корпусе того же коммутатора, не назначайте сети VLAN, которые предназначены для резерва и отслеживания состояния, порту коммутатора. Однако, если вы используете обеспечение отказоустойчивости устройств, сеть VLAN необходимо включить в магистральный порт между устройствами.

      5. Если вы не добавите сети VLAN в коммутатор перед их назначением модулю FWSM, они будут храниться в базе данных модуля Supervisor Engine и переданы в модуль FWSM сразу после добавления в коммутатор.

      6. Назначьте сети VLAN модулю FWSM перед тем, как назначить их модулю MSFC.

         При несоблюдении этого условия, сети VLAN будут исключены из списка на назначение модулю FWSM.

   2. **Назначение сетей VLAN модулю FWSM в ПО Cisco IOS:**

      В ПО Cisco IOS создайте до 16 защищенных брандмауэром групп сетей VLAN и затем назначьте эти группы модулю FWSM. Например, можно назначить все сети VLAN одной группе, либо можно создать внешнюю и внутреннюю группы, либо по отдельной группе на каждого клиента. Каждая группа может содержать неограниченное число сетей VLAN.

      Вы не можете назначить одну и ту же сеть VLAN нескольким защищенным брандмауэром группам; тем не менее, можно назначить несколько таких групп модулю FWSM, либо назначить одну группу нескольким модулям FWSM. Сети VLAN, которые назначены нескольким модулям FWSM, к примеру, могут находиться в отдельной группе по сравнению с виртуальными ЛВС, которые уникальны для каждого модуля FWSM.

      1. Для назначения сетей VLAN модулю FWSM выполните следующую процедуру:

         ```
         Router(config)#firewall vlan-group firewall_group vlan_range
         ```

         `vlan_range` может обозначать одну или несколько сетей VLAN, например от 2 до 1000 или от 1025 до 4094, обозначенных либо одним числом (n), например 5, 10, 15, либо в виде диапазона (n-x), например 5-10, 10-20.

         Примечание: Маршрутизируемые порты и WAN-порты потребляют ресурсы внутренних сетей VLAN, так что сети VLAN в диапазоне 1020-1100 могут уже использоваться.

         Пример:

         ```
         firewall vlan-group 1 10,15,20,25
         ```

      2. Для назначения защищенных брандмауэром групп модулю FWSM выполните следующую процедуру:

         ```
         Router(config)#firewall module module_number vlan-group firewall_group
         ```

Значение `firewall_group` представляет собой один или несколько номеров групп, как отдельных цифр (n) типа 5, так и диапазонов типа 5-10.

Пример:

```
firewall module 1 vlan-group 1
```

3. **Назначение сетей VLAN модулю FWSM в операционной системе Catalyst ПО**—В ПО Catalyst OS следует назначить список сетей VLAN модулю FWSM. При желании вы можете назначить одну и ту же сеть VLAN нескольким модулям FWSM. Список может содержать неограниченное число сетей VLAN.

   Для назначения сетей VLAN модулю FWSM выполните следующую процедуру:

```
Console> (enable)set vlan vlan_list firewall-vlan mod_num
```

   Значение `vlan_list` может содержать один или несколько номеров сетей VLAN, к примеру, от 2 до 1000 и от 1025 до 4094, обозначенных как отдельными цифрами (n) типа 5, 10, 15, так и диапазонами типа 10-20.

3. **Добавление виртуальных интерфейсов SVI к модулю MSFC**— сеть VLAN, заданная на модуле MSFC, называется виртуальным интерфейсом коммутатора (SVI). Если вы назначите сеть VLAN, используемую для SVI, модулю FWSM, то MSFC начнет маршрутизацию между модулем FWSM и другими виртуальными ЛВС третьего уровня (L3).

   По соображениям безопасности, по умолчанию только один SVI может существовать между MSFC и модулем FWSM. К примеру, при неправильной настройке системы с несколькими SVI трафик может пойти в обход модуля FWSM, если вы назначите модулю MSFC как внутренние, так и внешние сети VLAN.

   Для настройки SVI выполните следующую процедуру

```
Router(config)#interface vlan vlan_number
Router(config-if)#ip address address mask
```

   Пример:

```
interface vlan 20
ip address 192.168.1.1 255.255.255.0
```

Настройка коммутатора серии Catalyst 6500

`!--- Output Suppressed`
 	
`firewall vlan-group 1 10,15,20,25`
`firewall module 1 vlan-group 1`
 	
`interface vlan 20`
`ip address 192.168.1.1 255.255.255.0`
`!--- Output Suppressed`

Примечание: При помощи соответствующей команды операционной системы коммутатора установите сеанс его работы с модулем FWSM:

- ПО Cisco IOS:

```
Router#session slot <number>processor 1
```

- ПО Catalyst OS:

```
Console> (enable) session module_number
```

Настройка модуля FWSM

1. **Настройка интерфейсов для модуля FWSM**—Перед тем как пустить трафик через модуль FWSM, необходимо настроить имя интерфейса и IP-адрес. Необходимо также изменить уровень безопасности, установив его отличным от стандартного (который имеет значение "0"). Если вы укажете в качестве имени интерфейса `inside` и не укажете уровень безопасности явным образом, то модуль FWSM установит этот уровень равным 100.

   Примечание: Каждый интерфейс должен иметь уровень безопасности, от 0 (самый низкий) до 100 (самый высокий). Например, для самой важной сети, такой как внутренняя основная сеть, следует задать уровень безопасности равным 100, в то время как внешняя сеть, имеющая доступ к Интернету, может иметь уровень 0. Прочие сети, такие как DMZ могут иметь разные уровни в указанном диапазоне.

   Вы можете добавить в настройки любые идентификаторы VLAN, но только сети VLAN, назначенные модулю FWSM коммутатором, например, 10, 15, 20 и 25, смогут пропускать трафик. Используйте команду **show vlan** для того, чтобы просмотреть все сети VLAN, назначенные модулю FWSM.

```
interface vlan 20
   nameif outside
   security-level 0
   ip address 192.168.1.2 255.255.255.0
interface vlan 10
   nameif inside
   security-level 100
   ip address 10.1.1.1 255.255.255.0
interface vlan 15
   nameif dmz1
   security-level 60
   ip address 192.168.2.1 255.255.255.224
interface vlan 25
   nameif dmz2
   security-level 50
   ip address 192.168.3.1 255.255.255.224
```

   Подсказка: В команде **nameif *<name>*** значение *name* является текстовым параметром, который может содержать до 48 символов и не является чувствительным к регистру. Чтобы изменить имя, введите эту команду еще раз с новым значением. Не оставляйте имя пустым, так как все команды, которые используют это имя, будут в таком случае удалены.

2. **Настройка стандартной маршрутизации:**

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1
```

   Стандартная маршрутизация включает в себя определение IP-адреса шлюза (192.168.1.1), на который модуль FWSM посылает все IP-пакеты, не имеющие полученных или статических правил маршрутизации. Стандартная маршрутизация представляет собой статический адрес 0.0.0.0/0 в роли целевого IP-адреса. Указанные явным образом правила маршрутизации имеют более высокий приоритет, чем стандартный адрес.

3. **Динамический NAT** преобразует группу местных адресов (10.1.1.0/24) в пул отображаемых адресов (192.168.1.20-192.168.1.50), которые могут использоваться для маршрутизации в целевой сети. В отображаемом пуле может быть меньше адресов, чем в реальной группе. Когда компьютер, который нужно перенаправить, получает доступ к целевой сети, модуль FWSM назначает ему IP-адрес из отображаемого пула. Перенаправление включается только когда реальный компьютер создает соединение. Перенаправление действует только на время соединения, а пользователь при этом не сохраняет свой IP-адрес после прекращения перенаправления.

```
nat (inside) 1 10.1.1.0 255.255.255.0
global (outside) 1 192.168.1.20-192.168.1.50 netmask 255.255.255.0
access-list Internet extended deny ip any 192.168.2.0 255.255.255.0
access-list Internet extended permit ip any any
access-group Internet in interface inside
```

Необходимо создать ACL для того, чтобы запретить прохождение трафика из внутренней сети 10.1.1.0/24 в сеть DMZ1 (192.168.2.0) и разрешить для других типов трафика выход в Интернет через ACL *Internet*, который применяется к внутреннему интерфейсу в качестве средства перенаправления входящего трафика.

4. **Статический NAT** создает фиксированное правило для преобразование местных адресов в отображаемые. Благодаря динамическому NAT и PAT, каждый компьютер использует различные адреса или порты для каждого перенаправления. Из-за того, что отображаемый адрес не меняется при каждом соединении со статическим NAT, а также из-за того, что существует приоритетное правило перенаправления, статический NAT позволяет компьютерам в целевой сети перенаправлять трафик согласно этому правилу, если для этого есть соответствующие права.

   Основным отличием между динамическим NAT и диапазоном адресов для статического NAT является то, что статический NAT позволяет удаленному компьютеру создавать соединение с использованием перенаправления (при наличии соответствующих прав), в то время как динамический NAT не позволяет это делать. Кроме того, число необходимых отображаемых адресов должно быть равно числу реальных адресов со статическим NAT.

```
static (dmz1,outside) 192.168.1.6 192.168.2.2 netmask 255.255.255.255
static (dmz2,outside) 192.168.1.10 192.168.3.2 netmask 255.255.255.255
access-list outside extended permit tcp any host 192.168.1.10 eq http
access-list outside extended permit tcp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-data
access-list outside extended permit udp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-status
access-group outside in interface outside
```

   Ниже показаны две инструкции статического NAT. Первая из них нужна для транслирования местного IP 192.168.2.2 внутреннего интерфейса в отображаемый IP 192.168.1.6 внешней подсети в случае, если ACL разрешает прохождение трафика от исходного IP-адреса 192.168.1.30 к отображаемому 192.168.1.6 для доступа к серверу Websense в сети DMZ1. Похожим образом вторая инструкция статического NAT нужна для транслирования местного IP 192.168.3.2 внутреннего интерфейса в отображаемый IP 192.168.1.10 внешней подсети в случае, если ACL разрешает прохождение трафика из Интернета по отображаемому IP 192.168.1.10 для доступа к веб-серверу в сети DMZ2.

5. Команда **url-server** определяет сервер, на котором запущено приложение фильтрации URL-адресов Websense. Всего можно определить 16 URL-серверов в режиме одного контекста и 4 URL-сервера в мультирежиме, однако одновременно можно использовать только одно приложение, либо N2H2, либо Websense. Дополнительно, если вы измените настройки безопасности, то настройки на сервере приложений не будут обновлены автоматически. Это следует сделать отдельно, в соответствии с указаниями поставщика.

   Команда **url-server** должна быть настроена перед запуском команды **filter** для адресов HTTP и FTP. Если все серверы URL будут удалены из списка сервера, то все фильтрующие команды, связанные с URL, будут также удалены.

   После определения сервера, включите службу фильтрации URL с помощью команды **filter url** .

```
url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1 connections 5
```

   Команда **filter url** предотвращает доступ исходящих пользователей к интернет-адресам, которые вы указали в приложении фильтрации Websense.

```
filter url http 10.1.1.0 255.255.255.0 0 0
```

Настройка модуля FWSM
!--- Output Suppressed

```
interface vlan 20
   nameif outside
   security-level 0
   ip address 192.168.1.2 255.255.255.0
interface vlan 10
   nameif inside
   security-level 100
   ip address 10.1.1.1 255.255.255.0
interface vlan 15
   nameif dmz1
   security-level 60
   ip address 192.168.2.1 255.255.255.224
interface vlan 25
   nameif dmz2
   security-level 50
   ip address 192.168.3.1 255.255.255.224
passwd fl0wer
enable password treeh0u$e
route outside 0 0 192.168.1.1 1
url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1 connections 5
url-cache dst 128
filter url http 10.1.1.0 255.255.255.0 0 0
!--- When inside users access an HTTP server, FWSM consults with a
!--- Websense server in order to determine if the traffic is allowed.

nat (inside) 1 10.1.1.0 255.255.255.0
global (outside) 1 192.168.1.20-192.168.1.50 netmask 255.255.255.0
!--- Dynamic NAT for inside users that access the Internet

static (dmz1,outside) 192.168.1.6 192.168.2.2 netmask 255.255.255.255
!--- A host on the subnet 192.168.1.0/24 requires access to the Websense
!--- server for management that use pcAnywhere, so the Websense server
!--- uses a static translation for its private address.


static (dmz2,outside) 192.168.1.10 192.168.3.2 netmask 255.255.255.255
!--- A host on the Internet requires access to the Webserver, so the Webserver
!--- uses a static translation for its private address.


access-list Internet extended deny ip any 192.168.2.0 255.255.255.0
access-list Internet extended permit ip any any
access-group Internet in interface inside
!--- Allows all inside hosts to access the outside for any IP traffic,
!--- but denies them access to the dmz1



access-list outside extended permit tcp any host 192.168.1.10 eq http
!--- Allows the traffic from the internet with the destination IP address
!--- 192.168.1.10 and destination port 80


access-list outside extended permit tcp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-data
access-list outside extended permit udp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-status

!--- Allows the management host 192.168.1.30 to use
!--- pcAnywhere on the Websense server

access-group outside in interface outside


access-list WEBSENSE extended permit tcp host 192.168.2.2 any eq http
access-group WEBSENSE in interface dmz1
!--- The Websense server needs to access the Websense
!--- updater server on the outside.
!--- Output Suppressed
```

Проверка

Используйте этот раздел для проверки работоспособности ваших настроек.

Интерпретатор выходных данных (registered customers only) (OIT) поддерживает команды **show** . Используйте OIT для просмотра анализа вывода команды **show** .

1. Чтобы убедиться, что коммутатор распознал модуль FWSM и предоставил ему выход в сеть, просмотрите информацию о модуле

(выберите команду для вашей ОС):

- ПО Cisco IOS:

```
Router#show module
Mod Ports Card Type                              Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
 1    2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-SUP2-2GE    SAD0444099Y
 2   48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD03475619
 3    2  Intrusion Detection System             WS-X6381-IDS       SAD04250KV5
  4    6  Firewall Module                         WS-SVC-FWM-1       SAD062302U4
```

- ПО Catalyst OS:

```
Console>show module [mod-num]
The following is sample output from the show module command:

Console> show module
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- ------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
4   4    2     Intrusion Detection Syste WS-X6381-IDS        no  ok
5   5    6     Firewall Module           WS-SVC-FWM-1        no  ok
6   6    8     1000BaseX Ethernet        WS-X6408-GBIC       no  ok
```

Примечание: Команда **show module** показывает адреса шести портов для модуля FWSM. Это внутренние порты, которые сгруппированы в один канал EtherChannel.

2.

```
Router#show firewall vlan-group
Group vlans
----- ------
  1 10,15,20
  51 70-85
  52 100
```

3.

```
Router#show firewall module
Module Vlan-groups
 5    1,51
 8    1,52
```

4. Введите команду для вашей операционной системы для просмотра текущего загрузочного раздела:

- ПО Cisco IOS:

```
Router#show boot device [mod_num]
```

Пример:

```
Router#show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

- ПО Catalyst OS:

```
Console> (enable) show boot device mod_num
```

Пример:

```
Console> (enable) show boot device 6
Device BOOT variable = cf:5
```

Устранение неполадок

Этот раздел содержит сведения, которые можно использовать для устранения неполадок в вашей конфигурации.

1. **Установка загрузочного раздела по умолчанию**—По умолчанию, модуль FWSM загружается с раздела приложений **cf:4**. Однако, вы можете задать загрузку с раздела приложений **cf:5**, либо в служебный раздел **cf:1**. Для того, чтобы изменить загрузочный раздел по умолчанию, введите команду для вашей операционной системы:

   - ПО Cisco IOS:

   ```
   Router(config)#boot device module mod_num cf:n
   ```

   Где n может равняться 1 (служебный), 4 (приложение), или 5 (приложение).

   - ПО Catalyst OS:

   ```
   Console> (enable) set boot device cf:n mod_num
   ```

   Где n может равняться 1 (служебный), 4 (приложение), или 5 (приложение).

2. **Сброс модуля FWSM в ПО Cisco IOS**—Для того, чтобы сбросить модуль FWSM, введите указанную ниже команду:

   ```
   Router#hw-module module mod_num reset [cf:n] [mem-test-full]
   ```

   Аргумент **cf:n** обозначает дисковый раздел, 1 (служебный), 4 (приложение), или 5 (приложение). Если вы не укажете раздел, то будет использован раздел по умолчанию, обычно это **cf:4**.

   Параметр **mem-test-full** запускает полный тест памяти, который длится примерно шесть минут.

   Пример:

   ```
   Router#hw-mod module 9 reset
   Proceed with reload of module? [confirm] y
   % reset issued for module 9
   Router#
   00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
   00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
   ```

   Для ПО **Catalyst OS**:

   ```
   Console> (enable) reset mod_num [cf:n]
   ```

Где **cf:n** обозначает раздел, 1 (служебный), 4 (приложение), или 5 (приложение). Если вы не укажете раздел, то будет использован раздел по умолчанию, обычно это **cf:4**.

Примечание: NTP нельзя настроить на модуле FWSM, потому что он использует настройки коммутатора напрямую.

Дополнительные сведения

- **Cisco Страница поддержки модуля служб брандмауэра для серии Catalyst 6500**
- **Cisco Страница поддержки коммутаторов серии Catalyst 6500**
- **Cisco Страница поддержки маршрутизатора серии 7600**
- **Cisco Systems — техническая поддержка и документация**

Дата генерации PDF файла: Jan 05, 2010

---

http://www.cisco.com/support/RU/customer/content/10/105388/fwsm-basic-config.shtml

---