Пример базовой конфигурации FWSM

Содержание

Введение

В этом документе описан порядок базовой настройки модуля служб сетевого экрана (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.

Примечание: Когда лицензионные ключи являются точно тем же между модулями, в сценарии Высокой доступности (HA) FWSM аварийное переключение может только успешно синхронизировать. Поэтому аварийное переключение не может работать между FWSM с другими лицензиями.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Модуль служб сетевого экрана 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.Плата MSFC 2 с программным обеспечением Cisco IOS. Посмотрите Таблицу для поддерживаемых Cisco IOS Software Release.

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.

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.

Родственные продукты

Эта конфигурация может также использоваться для маршрутизаторов Cisco серии 7600 с требуемыми компонентами как показано:

- Supervisor Engine с программным обеспечением Cisco IOS. См. Таблицу со списком поддерживаемых выпусков ПО Cisco IOS и модуля supervisor engine.
- MSFC 2 с программным обеспечением Cisco IOS. Посмотрите Таблицу для поддерживаемых Cisco IOS Software Release.

Условные обозначения

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

Общие сведения

FWSM является высокоэффективным, экономящим место, модулем самонастраивающегося межсетевого экрана, который устанавливает в Коммутаторах серии Catalyst 6500 и маршрутизаторах Cisco серии 7600.

Межсетевые экраны защищают внутренние сети от неавторизованный доступа пользователями на внешней сети. Например, когда вы разделяете сеть кадр от пользовательской сети, межсетевой экран может также защитить внутренние сети друг от друга. Если часть сетевых ресурсов необходимо открыть для внешнего доступа, например веб-сервер или FTP-сервер, можно поместить эти ресурсы в отдельную сеть, защищенную сетевым экраном, которую называют "демилитаризованной" зоной (DMZ). Межсетевой экран предоставляет ограниченный доступ к DMZ, но потому что DMZ включает только общие серверы, атака там влияет только на серверы и не влияет на другие внутренние сети. Можно также управлять, когда внутренние пользователи обращаются к внешним сетям, например, доступ к Интернету при разрешении только определенных адресов требует аутентификации или авторизации или координаты с внешним сервером фильтрации URL-адресов.

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

Во время обсуждения сетей, связанных с межсетевым экраном, внешняя сеть перед межсетевым экраном, внутренняя сеть защищена и позади межсетевого экрана и DMZ, в то время как позади межсетевого экрана, предоставляет ограниченный доступ внешним пользователям. Поскольку FWSM позволяет вам настроить много интерфейсов с различной политикой безопасности, который включает много внутренних интерфейсов, много DMZs, и даже много внешних интерфейсов при желании, эти термины использованы в общем смысле только.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:

Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

Конфигурации

Эти конфигурации используются в данном документе:

- Конфигурация коммутатора серии Catalyst 6500
- Конфигурация FWSM

Конфигурация коммутатора серии Catalyst 6500

1. Можно установить FWSM в Коммутаторах серии Catalyst 6500 или маршрутизаторах Cisco серии 7600. Конфигурация и серии идентична и серия, упомянуты в общем в этом документе как **коммутатор**.**Примечание:** Необходимо настроить коммутатор соответственно перед настройкой FWSM.
2. **Назначьте VLAN на Модуль Сервисов межсетевого экрана** — В этом разделе описывается назначить VLAN на FWSM. FWSM не включает внешних физических интерфейсов. Вместо этого это использует интерфейсы виртуальной локальной сети (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:** См. раздел VLAN Настройки Руководства по конфигурации программного обеспечения Коммутаторов Catalyst 6500 для получения дополнительной информации о том, как создать VLAN и назначить его на порты коммутатора.**VLAN Рекомендации:**Можно использовать частные VLAN с FWSM. Назначьте основной VLAN (виртуальная локальная сеть) на FWSM; FWSM автоматически обрабатывает вторичный VLAN трафик.Вы не можете использовать зарезервированные VLAN.Вы не можете использовать VLAN 1.При использовании аварийного переключения FWSM в том же шасси коммутаторов не назначайте VLAN, которую вы резервировали для аварийного переключения и связи с отслеживанием состояния к порту коммутатора. Но при использовании аварийного переключения между шасси необходимо включать VLAN в магистральный порт между шасси.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.Назначьте VLAN на FWSM перед присвоением их на MSFC.От VLAN, которые не удовлетворяют это условие, сбрасывают из диапазона VLAN, которые вы пытаетесь назначить на FWSM.**Назначьте VLAN на FWSM в программном обеспечении Cisco IOS:**В программном обеспечении Cisco IOS создайте до 16 Групп VLAN межсетевого экрана, и затем назначьте группы на FWSM. Например, можно назначить все VLAN на одну группу, или можно создать внутреннюю группу и внешнюю группу, или можно создать группу для каждого клиента. Каждая группа может содержать неограниченные VLAN.Вы не можете назначить ту же VLAN на множественные группы межсетевого экрана; однако, можно назначить множественные группы межсетевого экрана на FWSM, и можно назначить одиночную группу межсетевого экрана на множественные FWSM. VLAN, которые вы хотите назначить на множественные FWSM, например, могут находиться в отдельной группе от VLAN, которые уникальны для каждого FWSM.Выполните шаги для присвоения VLAN на FWSM:`Router(config)#` **`firewall vlan-group firewall_group vlan_range`** `Vlan_range VLAN, 2 1000 1025 4094, (n), 5, 10, 15, (n-x), 5-10, 10-20.`**Примечание:** Маршрутизируемые порты и порты глобальной сети (WAN) используют внутренние виртуальные сети, таким образом, возможно, что могут уже использоваться VLAN в диапазоне 1020-1100.**Пример:** **`firewall vlan-group 1 10,15,20,25`** Выполните шаги для присвоения групп межсетевого экрана на FWSM.`Router(config)#` **`firewall module module_number vlan-group firewall_group`** `firewall_group` является одним или более номерами группы или как одиночным номером (n) как 5 или как диапазоном как 5-10.**Пример:** **`firewall module 1 vlan-group 1`** **Назначьте VLAN на FWSM в Операционной системе Catalyst** — В Программном обеспечении операционной системы Catalyst, вы назначаете список VLAN к FWSM. Можно назначить ту же VLAN на множественные FWSM при желании. Список может содержать неограниченные VLAN.Выполните шаги

для присвоения VLAN на FWSM.`Console> (enable)`**`set vlan vlan_list firewall-vlan mod_num`** `vlan_list` может быть одной или более VLAN, например, 2 - 1000 и от 1025 до 4094, определенный или как одиночный номер (n) как 5, 10, 15 или как диапазон (n-x) как 5-10, 10-20.

3. **Добавление виртуальных интерфейсов SVI к модулю MSFC— сеть VLAN, заданная на модуле MSFC, называется виртуальным интерфейсом коммутатора (SVI).** Если вы назначаете VLAN, используемую для SVI к FWSM, то маршруты MSFC между FWSM и другими VLAN Уровня 3.Из соображений безопасности, по умолчанию, только один SVI может существовать между MSFC и 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.Выполните шаги для настройки SVI`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`

Конфигурация 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: Сеанс в к FWSM от коммутатора с командой, соответствующей вашей операционной системе коммутатора:

- ПО Cisco IOS):`Router#`**`session slot <number> processor 1`**
- Программное обеспечение операционной системы Catalyst:`Console> (enable)` **`session module_number`**

(Необязательно) Совместно используя VLAN с другими Сервисными модулями — Если коммутатор имеет другие сервисные модули, например, ядро управления приложениями (ACE), возможно, что необходимо совместно использовать некоторые VLAN с этими сервисными модулями. См. Дизайн Сервисного модуля с ACE и FWSM для получения дополнительной информации о том, как оптимизировать конфигурацию FWSM, когда вы работаете с такими другими модулями.

Конфигурация FWSM

1. **Настройте Интерфейсы для FWSM** — Прежде чем можно будет позволить трафик через FWSM, необходимо настроить имя интерфейса и IP-адрес. Необходимо также изменить уровень безопасности, установив его отличным от стандартного (который имеет значение "0"). Если вы называете интерфейсный `inside`, и вы делаете "not set" уровень безопасности явно, то FWSM устанавливает уровень безопасности в 100.**Примечание:** Каждый интерфейс должен иметь уровень безопасности от 0 (самый низкий) к 100 (самый высокий). Например, в то время как внешняя сеть, связанная с Интернетом, может быть уровнем 0, необходимо назначить большую часть защищенной сети, такой как сеть внутреннего хоста, к уровню 100. Другие сети, такие как DMZs, могут быть промежуточными.Можно добавить любой ИДЕНТИФИКАТОР VLAN к конфигурации, но только VLAN, например, 10, 15, 20 и 25, которые назначены на FWSM коммутатором, могут передать трафик. Используйте **команду show vlan** для просмотра всех VLAN, назначенных на 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
```

Совет: В команде *<name>* **nameif** *название* является текстовой строкой до 48 символов и не регистрозависимо. Можно поменять имя при возвращении в эту команду с новым значением. Не вводите форму, потому что та команда вызывает все команды, которые обращаются к тому названию, которое будет удалено.

2. **Конфигурирование маршрута по умолчанию:**
   `route outside 0.0.0.0 0.0.0.0 192.168.1.1` Маршрут по умолчанию определяет IP-адрес шлюза (192.168.1.1), к которому FWSM передает все пакеты IP, для которых это не имеет изученного или статического маршрута. Маршрут по умолчанию является просто статическим маршрутом с 0.0.0.0/0 как IP - адрес назначения. Маршруты, которые определяют определенное назначение, имеют приоритет по маршруту по умолчанию.
3. **Динамический NAT** преобразовывает группу действительных адресов (10.1.1.0/24) к пулу сопоставленных адресов (192.168.1.20-192.168.1.50), которые маршрутизуемы на сети назначения. Сопоставленный пул может включать меньше адресов, чем реальная группа. Когда хост, который вы хотите преобразовать, обращается к сети назначения, FWSM назначает его IP-адрес от сопоставленного пула. Трансляция добавлена только, когда реальный хост инициирует соединение. Трансляция существует только на время соединения, и данный пользователь не поддерживает тот же IP-адрес после таймаутов трансляции.
   ```
   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, чтобы запретить, что трафик от внутренней сети 10.1.1.0/24 входит в сеть DMZ1 (192.168.2.0) и позволяет другие виды трафика к Интернету через приложение *Интернета* ACL к внутреннему интерфейсу как входящее направление для входящего трафика.
4. **Статический NAT** создает неподвижную трансляцию действительного адреса (адресов) к сопоставленному адресу (адресам).With динамический NAT и PAT, каждый хост использует другой адрес или порт для каждой последующей трансляции. Поскольку сопоставленный адрес является тем же для каждого последовательного соединения со статическим NAT, и персистентное правило трансляции существует, статический NAT позволяет хостам на сети назначения инициировать трафик к преобразованному хосту, если существует список доступа, который позволяет его.Главное различие между динамическим преобразованием NAT и диапазоном адресов для статического преобразования NAT заключается в том, что статическое преобразование NAT позволяет удаленному хосту инициировать соединение с преобразуемым хостом (если список доступа разрешает это), в то время как динамическое преобразование NAT не позволяет этого. Вам также нужно равное число сопоставленных адресов как действительные адреса 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-list inbound extended permit udp
   any host 216.70.55.69 range 8766 30000 access-group outside in interface outside
   ```
   Это эти две показанные статических инструкции NAT. Первый предназначается для перевода реального IP 192.168.2.2 на внутреннем интерфейсе к сопоставленному IP 192.168.1.6 на внешней подсети при условии, что ACL позволяет трафик из источника 192.168.1.30

к сопоставленному IP 192.168.1.6 для доступа к Серверу Websense в сети DMZ1. Точно так же вторая статическая инструкция NAT означала преобразовывать реального IP 192.168.3.2 на внутреннем интерфейсе к сопоставленному IP 192.168.1.10 на внешней подсети при условии, что ACL позволяет трафик от Интернета до сопоставленного IP 192.168.1.10, чтобы обратиться к веб-серверу в сети DMZ2 и иметь номер порта UDP в диапазоне 8766 - 30000.

5. **Команда url-server** определяет сервер, который запускает приложение фильтрации URL-адресов Websense. Предел является 16 серверами URL в одиночном режиме контекста и четырьмя серверами URL в многорежимном, но можно использовать только одно приложение, или N2H2 или Websense, за один раз. Кроме того, при изменении конфигурации на устройстве безопасности это не обновляет конфигурацию на сервере приложений. Это следует сделать отдельно, в соответствии с указаниями поставщика.**Команда url-server** должна быть настроена перед запуском **команды фильтрации** для HTTPS и FTP. Если все серверы URL удалены из списка серверов, то все команды фильтрации, отнесенные к фильтрации URL-адресов, также удалены.Как только вы определяете сервер, включаете сервис фильтрации URL-адресов с **командой filter url**.
   `url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1 connections 5` **Команда filter url** позволяет предотвращение доступа исходящих пользователей от URL Всемирной паутины, которые вы определяете с приложением фильтрации Websense.
   `filter url http 10.1.1.0 255.255.255.0 0 0`

Конфигурация 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-list inbound extended permit
udp any host 216.70.55.69 range 8766 30000 !--- Allows
udp port number in the range of 8766 to 30000. 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

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Используйте OIT для просмотра анализа выходных данных команды show.**

1. Просмотрите сведения о модуле в соответствии с вашей операционной системой, чтобы проверить, что коммутатор подтверждает FWSM и принес его онлайн: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` Программное обеспечение операционной системы Catalyst:`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 шесть портов для FWSM. Это внутренние порты, которые группируются как 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 своей операционной системы для просмотра текущего раздела начальной загрузки: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 ]:`Программное обеспечение операционной системы Catalyst:`Console> (enable) show boot device mod_num` **Пример:**`Console> (enable) show boot device 6 Device BOOT variable = cf:5`

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

1. **Устанавливая Раздел начальной загрузки По умолчанию** — По умолчанию, FWSM загружается от **cf:4** раздела установки приложения. Но, можно принять решение загрузиться от **cf:5** раздела установки приложения или в **cf:1** разделение обслуживания. Для изменения раздела начальной загрузки по умолчанию введите команду для операционной системы:ПО Cisco IOS):`Router(config)#boot device module mod_num cf:n` Где n 1 (обслуживание), 4 (приложение), или 5 (приложение).Программное обеспечение операционной системы Catalyst:`Console> (enable) set boot device cf:n mod_num` Где n 1 (обслуживание), 4 (приложение), или 5 (приложение).
2. **При сбросе FWSM в программном обеспечении Cisco IOS** — для сброса FWSM, введите команду как показано:`Router#hw-module module mod_num reset [cf:n] [mem-test-full]` **cf:n** аргумент является разделением, или 1 (обслуживание), 4 (приложение), или 5 (приложение). Если вы не задаете разделение, раздел по умолчанию используется, который, как правило, является **cf:4**.**mem-test-full** опция запускает тест полной памяти, который занимает приблизительно 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 **программного обеспечения операционной системы Catalyst**:`Console> (enable) reset mod_num [cf:n]` Где **cf:n** является разделением, или 1 (обслуживание), 4 (приложение), или 5 (приложение). Если вы не задаете разделение, раздел по умолчанию используется, который, как правило, является **cf:4**.

Примечание: NTP не может быть настроен на FWSM, потому что это берет свои параметры настройки от Коммутатора.

Проблема: Неспособный передать трафик виртуальной локальной сети (VLAN) от FWSM до Сенсора IPS 4270

Вы неспособны передать трафик от FWSM до Сенсоров IPS.

Решение

Для принуждения трафика через IPS прием должен создать дополнительную VLAN, чтобы эффективно сломать одну из текущих VLAN в два и затем соединить их вместе. Проверьте данный пример с VLAN 401 и 501 для разъяснения:

- Если вы хотите просмотреть трафик на основном **VLAN 401**, создайте другой **vlan VLAN 501** (вспомогательная VLAN). Затем отключите интерфейс виртуальной локальной сети (VLAN) 401, который хосты в 401 в настоящее время использование в качестве их шлюза по умолчанию.
- Затем включите интерфейс VLAN 501 с *тем же* адресом, который вы ранее отключили на интерфейсе VLAN 401.
- Разместите один из интерфейсов IPS в VLAN 401 и другого в VLAN 501.

Все, что необходимо сделать, должно переместить шлюз по умолчанию для VLAN 401 на VLAN 501. Необходимо сделать подобные изменения к VLAN если подарок. Обратите внимание на то, что VLAN по существу походят на сегменты LAN. У вас может быть шлюз по умолчанию на другой части провода, чем хосты, которые используют его.

Поврежденные пакеты выходят в FWSM

Как я могу решить проблему поврежденных пакетов в FWSM?

Решение

Выполните sysopt np команда модуля завершения в режиме глобальной конфигурации для решения вопроса Поврежденного пакета в FWSM. Эта команда была представлена в Версии FWSM 3.2 (5) и гарантирует, что пакеты переданы в том же заказе, они были получены.

Проблема: Неспособный передать асимметрично пакеты для маршрутизации через межсетевой экран

Вы неспособны передать асимметрично пакеты для маршрутизации через межсетевой экран.

Решение

Выполните команду обхода состояния TCP расширенных настроек соединения набора в режиме конфигурации класса для передачи асимметрично пакетов для маршрутизации через межсетевой экран. Эта команда была представлена в Версии FWSM 3.2 (1).

Поддержка netflow в FWSM

FWSM поддерживает Netflow?

Решение

Netflow не поддерживается в FWSM.

Дополнительные сведения

- Страница поддержки модуля служб межсетевого экрана для коммутаторов Cisco Catalyst серии 6500
- Страница технической поддержки коммутаторов Cisco Catalyst серии 6500
- Страница технической поддержки маршрутизатора Cisco серии 7600
- Перехват TCP FWSM и cookie SYN объяснены
- Cisco Systems – техническая поддержка и документация