Пример настройки Firewall Service Module в режиме прозрачного брандмауэра

Содержание

Введение

Межсетевой экран традиционно организуется как маршрутизируемый переход, функционирующий как шлюз по умолчанию для хостов, подключенных к одной из защищенных им подсетей. *Прозрачный межсетевой экран, с другой стороны, является межсетевым экраном 2-уровня, который действует как невидимый межсетевой экран или как «врезка в линию» и незаметен для подключенных устройств как переход через маршрутизатор.* Внутренние и наружные интерфейсы служебного модуля межсетевого экрана (FWSM) соединяются с одной и той же сетью. Поскольку межсетевой экран не является переходом через маршрутизатор, можно легко ввести прозрачный межсетевой экран в существующую сеть. Переадресация IP не требуется.

Его поддержка значительно облегчается, так как не требуется устранять проблемы, связанные со сложными шаблонами маршрутизации или настройкой NAT.

Несмотря на то что функционирование в режиме прозрачности напоминает работу моста, трафик уровня 3, например IP-трафик, не может проникнуть сквозь модуль FWSM, если не было явно заданного разрешения на выполнение этого действия, сопровожденного расширенным списком доступа. Единственный трафик, для которого возможно прохождение через прозрачный межсетевой экран без списка доступа, — это трафик ARP. Проверка ARP-трафика осуществляется с помощью функции инспектирования ARP.

В маршрутизируемом режиме некоторые виды трафика не могут быть пропущены модулем FWSM, даже если они разрешены списком доступа. Кроме того, прозрачный межсетевой экран пропускает любой трафик из расширенного списка доступа (IP-трафик) или списка доступа EtherType (трафик, отличный от IP-трафика).

Например, с помощью прозрачного межсетевого экрана можно установить смежности протокола маршрутизации; также можно разрешить прохождение трафика VPN (IPSec), OSPF, RIP, EIGRP или BGP на основании расширенного списка доступа. Аналогичным образом можно пропускать через модуль FWSM такие протоколы, как HSRP или VRRP.

Пропускание трафика, отличного от IP (например, AppleTalk, IPX, BPDU и MPLS), можно настроить при помощи списка доступа EtherType.

Если какие-либо функции не поддерживаются прозрачным межсетевым экраном, можно разрешить прохождение трафика через него, чтобы вышестоящие или нижестоящие маршрутизаторы смогли обеспечить необходимую функциональность. Например, можно разрешить прохождение DHCP-трафика в расширенном списке доступа (вместо неподдерживаемой функции переключения DHCP) или трафик групповой адресации, который создается IP/TV.

Если модуль FWSM защиты работает в прозрачном режиме, то исходящий интерфейс пакета определяется путем поиска MAC-адреса, а не через поиск маршрута. Инструкции маршрута можно настроить, однако они будут действовать только для трафика, источником которого является модуль FWSM. Например, если сервер системного журнала расположен в удаленной сети, необходимо использовать статический маршрут, чтобы модуль FWSM мог достичь данной подсети.

Исключение из этого правила — случай, когда используется анализ голосовых пакетов, а оконечное устройство отстоит от FWSM как минимум на один переход. Например, если прозрачный межсетевой экран используется между CCM и шлюзом H.323 и на участке между прозрачным межсетевым экраном и шлюзом H.323 присутствует маршрутизатор, то для успешного завершения вызовов необходимо добавить на FWSM статический маршрут для шлюза H.323.

Примечание: FWSM прозрачного режима не передает пакеты CDP или любые пакеты, которые не имеют допустимого EtherType больше, чем или равняются 0x600. Например, невозможно прохождение пакетов IS-IS. Исключение составляют блоки данных протокола моста (BPDU), которые поддерживаются.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Данный документ составлен для модуля FWSM с микропрограммой версии 3.x.

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.

Прозрачный межсетевой экран

Группы мостов

Если требуется избежать накладных расходов, связанных с контекстами безопасности, или использовать контексты безопасности в максимально возможной мере, можно настроить до восьми пар интерфейсов, называемых группами мостов. Каждая группа мостов подключается к отдельной сети. Трафик одной группы мостов изолирован от других групп мостов. Маршрутизация трафика в другие группы мостов в пределах FWSM не осуществляется: трафик должен покинуть маршрутизатор FWSM и только после этого может быть возвращен внешним маршрутизатором на другую группу мостов в модуле FWSM. Несмотря на то что функции мостового соединения для каждой группы мостов независимы, множество прочих функций распространяются одновременно на все группы мостов. Например, все группы мостов совместно используют сервер системного журнала или конфигурацию сервера AAA. Для полного разделения политики безопасности следует использовать контексты безопасности, назначая каждому контексту одну группу мостов.

Поскольку межсетевой экран не является переходом через маршрутизатор, можно легко ввести прозрачный межсетевой экран в существующую сеть. Переадресация IP не требуется. Его поддержка значительно облегчается, так как не требуется устранять проблемы, связанные со сложными шаблонами маршрутизации или настройкой NAT.

Примечание: Каждая группа мостов требует управления IP-адресами. FWSM использует этот IP-адрес в качестве адреса источника для пакетов, создаваемых в группе мостов. Управляющий IP-адрес должен принадлежать той же подсети, что подключенная сеть.

Рекомендации

Следуйте данным рекомендациям при планировании сети с прозрачным межсетевым экраном:

- Каждой группе мостов необходим IP-адрес управления.В отличие от маршрутизируемого режима, в котором IP-адрес требуется каждому интерфейсу, в прозрачном межсетевом экране IP-адрес назначается группе мостов в целом. Модуль

FWSM использует этот IP-адрес в качестве исходного адреса для пакетов, создаваемых модулем FWSM, таких как системные сообщения или сообщения авторизации, аутентификации и учета (AAA).Управляющий IP-адрес должен принадлежать той же подсети, что подключенная сеть. Не допускается устанавливать подсеть равной подсети хоста (255.255.255.255). FWSM не поддерживает трафик во вторичных сетях. Поддерживается только трафик в той сети, к которой относится IP-адрес управления. Управление IP-подсетями описано в документе Назначение IP-адреса группе мостов.
- Каждая группа мостов использует только внутренний и внешний интерфейс.
- Каждая напрямую подключенная сеть должна быть расположена в той же подсети.
- IP-адрес управления для группы мостов не должен указываться в качестве шлюза по умолчанию для подключенных устройств. В качестве шлюза по умолчанию для устройств должен быть указан маршрутизатор с другой стороны модуля FWSM.
- Маршрут по умолчанию для прозрачного межсетевого экрана, необходимый для обеспечения возвратного пути трафика управления, действует только для трафика управления из сети одной группы мостов. Это ограничение обусловлено тем, что маршрут по умолчанию определяет как интерфейс в группе мостов, так и IP-адрес маршрутизатора в сети группы мостов, а задать несколько маршрутов по умолчанию нельзя. Если трафик управления поступает сразу из нескольких групп мостов, то необходимо задать статический маршрут для определения сети, из которой ожидается трафик управления.
- В многоконтекстном режиме каждый контекст должен использовать различные интерфейсы, несколько контекстов не могут использовать один интерфейс.
- В многоконтекстном режиме для каждого контекста обычно используются разные подсети. Можно использовать перекрывающиеся подсети, однако с точки зрения осуществимости маршрутизации это требует наличия маршрутизатора и конфигурации NAT в топологии сети.Чтобы разрешить прохождение трафика 3-го уровня (например, IP-трафика), необходимо использовать расширенный список контроля доступа. Также можно использовать список доступа EtherType для разрешения пропуска трафика, отличного от IP.

Разрешенные MAC-адреса

Эти MAC-адреса получателей разрешены для прохождения трафика через прозрачный межсетевой экран. Любые MAC-адреса, не указанные в данном списке отбрасываются.

- Реальный широковещательный MAC-адрес получателя, равный FFFF.FFFF.FFFF
- MAC-адреса групповой адресации IPv4 с 0100.5E00.0000 по 0100.5EFE.FFFF
- MAC-адреса групповой адресации IPv6 с 3333.0000.0000 по 3333.FFFF.FFFF
- Адрес групповой адресации BPDU, равный 0100.0CCC.CCCD
- Многоадресные MAC-адреса AppleTalk с 0900.0700.0000 по 0900.07FF.FFFF

Неподдерживаемые функции

Следующие функции не поддерживаются в прозрачном режиме:

- NAT/PATNAT выполняется в вышестоящем маршрутизаторе.**Примечание:** NAT/PAT поддерживается в прозрачном межсетевом экране для версии FWSM 3.2 и более поздних версий.

- Протоколы динамической маршрутизации (RIP, EIGRP, OSPF)Допускается добавление статических маршрутов для трафика, созданного модулем FWSM. Также можно разрешить прохождение трафика протоколов динамической маршрутизации через модуль FWSM с помощью расширенных списков контроля доступа.
- IPv6 для IP-адреса группы мостов.Тем не менее, при помощи списка контроля доступа EtherType можно разрешить пропускание идентификаторов EtherType для IPv6.
- Ретрансляция DHCPПрозрачный межсетевой экран может выступать в качестве DHCP-сервера, но при этом он не поддерживает выполнение команд ретрансляции DHCP. Ретрансляция DHCP не требуется, поскольку для пропуска DHCP-трафика можно использовать расширенный список доступа.
- Качество обслуживания (QOS)
- Групповая адресацияПосредством расширенного списка контроля доступа можно разрешить пропускание многоадресного трафика через устройство защиты. Дополнительные сведения см. в разделе Сквозное пропускание трафика.
- Оконечная обработка VPN-сеансов для сквозного трафикаПрозрачный межсетевой экран поддерживает VPN-туннели типа «узел-узел» только для соединений управления. Он не осуществляет оконечную обработку VPN-сеансов для трафика, проходящего через модуль FWSM. Можно разрешить прохождение трафика VPN через модуль FWSM с помощью расширенного списка контроля доступа, однако оконечная обработка соединений, не относящихся к управлению, выполняться не будет.
- Функция LoopGuard на коммутатореПри работе FWSM в прозрачном режиме включать функцию LoopGuard глобально на коммутаторе не следует. Функция LoopGuard автоматически действует для внутреннего трафика EtherChannel между коммутатором и FWSM, поэтому при переключении и восстановлении после отказа функция LoopGuard вызывает отключение вторичного модуля из-за перехода EtherChannel в состояние «err-disable».

Настройка

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

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

На схеме сети представлена типичная сеть с прозрачным межсетевым экраном, в которой внешние устройства расположены в той же подсети, что и внутренние. Внутренний маршрутизатор и хосты подключены напрямую к внешнему маршрутизатору.

Конфигурации

Каждый контекст можно настроить для работы в режиме маршрутизируемого межсетевого экрана по умолчанию или в режиме прозрачного межсетевого экрана.

При смене режимов модуль FWSM очищает конфигурацию, так как многие команды поддерживаются только в одном из режимов. Если уже имеется сформированная

конфигурация, то перед изменением режима следует создать ее резервную копию. На основе этой резервной копии можно создать новую конфигурацию.

При загрузке в модуль FWSM текстовой конфигурации, изменяющей режим посредством команды firewall transparent, убедитесь, что эта команда стоит в начале конфигурации. FWSM изменяет режим в момент чтения этой команды, после чего продолжает считывать загруженную конфигурацию. Если команда будет расположена в тексте конфигурации дальше, то модуль FWSM удалит все предыдущие строки конфигурации.

Для установки прозрачного режима введите в каждом контексте следующую команду:

```
hostname(config)#firewall transparent
```

Для установки маршрутизируемого режима введите в каждом контексте следующую команду:

```
hostname(config)#no firewall transparent
```

Различные сценарии перемещения данных в прозрачном межсетевом экране

Получение доступа к внешнему серверу электронной почты внутренним пользователем

Пользователь внутренней сети получает доступ к серверу электронной почты в Интернете (снаружи сети). Модуль FWSM получает пакет и, если необходимо, добавляет MAC-адрес источника в таблицу MAC-адресов. Поскольку данный сеанс — новый, модуль проверяет, разрешен ли пакет в соответствии с условиями политики безопасности (списками доступа, фильтрами или AAA-аутентификацией).

Примечание: Для многоконтекстного режима FWSM сначала классифицирует пакет в соответствии с уникальным интерфейсом.

Модуль FWSM регистрирует создание сеанса. Если MAC-адрес получателя присутствует в таблице, то модуль FWSM передает пакет за пределы внешнего интерфейса. В качестве MAC-адреса назначения используется адрес вышестоящего маршрутизатора, 192.168.1.2. Если MAC-адрес получателя отсутствует в таблице модуля FWSM, то модуль пытается его обнаружить при отправке запроса ARP и эхо-запроса. Первый пакет отбрасывается.

Сервер электронной почты отвечает на запрос. Поскольку сеанс уже выполняется, пакет не обходит множество поисков, связанных с новым соединением. Модуль FWSM пересылает пакет внутреннему пользователю.

Внутренний пользователь посещает почтовый сервер с NAT

При включении NAT на маршрутизаторе, подключенном к Интернету, поток направляемых через него пакетов незначительно изменяется.

Пользователь внутренней сети получает доступ к серверу электронной почты в Интернете (снаружи сети). Модуль FWSM получает пакет и, если необходимо, добавляет MAC-адрес источника в таблицу MAC-адресов. Поскольку данный сеанс — новый, модуль проверяет, разрешен ли пакет в соответствии с условиями политики безопасности (списками доступа, фильтрами или AAA-аутентификацией).

Примечание: Для многоконтекстного режима FWSM сначала классифицирует пакет в соответствии с уникальным интерфейсом.

Маршрутизатор Интернета преобразует фактический адрес хоста A (192.168.1.5) в сопоставленный адрес маршрутизатора Интернета (172.16.1.1). Поскольку сопоставленный адрес не принадлежит к той же сети, что и внешний интерфейс, необходимо убедиться в том, что у вышестоящего маршрутизатора есть статический маршрут к сопоставленной сети, который ведет к модулю FWSM.

Модуль FWSM регистрирует установление сеанса и пересылает пакет с внешнего интерфейса. Если MAC-адрес получателя присутствует в таблице, то модуль FWSM передает пакет за пределы внешнего интерфейса. В качестве MAC-адреса получателя используется адрес вышестоящего маршрутизатора, 172.16.1.1. Если MAC-адрес получателя отсутствует в таблице модуля FWSM, то модуль пытается его обнаружить при отправке запроса ARP и эхо-запроса. Первый пакет отбрасывается.

Сервер электронной почты отвечает на запрос. Поскольку сеанс уже выполняется, пакет не обходит множество поисков, связанных с новым соединением. Посредством NAT модуль преобразует сопоставленный адрес в фактический адрес, 192.168.1.5.

Посещение внутреннего web-сервера внутренним пользователем

Если Хост A пытается обратиться к внутреннему Web-серверу (10.1.1.1), Хост A (192.168.1.5) передает пакет запроса к Интернет-маршрутизатору (так как это - шлюз по умолчанию) через FWSM от внутренней части до внешней стороны. Затем пакет перенаправлен на Web-сервер (10.1.1.1) через FWSM (снаружи к внутренней части) и встроенный маршрутизатор.

Примечание: Пакет запроса возвращается к Web-серверу, только если FWSM имеет список доступа для разрешения трафика от внешней стороны до внутренней части.

Чтобы устранить эту проблему, необходимо назначить в качестве шлюза по умолчанию для хоста A (10.1.1.1) внутренний маршрутизатор (192.168.1.3) вместо маршрутизатора Интернета (192.168.1.2). Это предотвращает передачу любого ненужного трафика на внешний шлюз, а если такой трафик появляется — перенаправляет его на внешний маршрутизатор (маршрутизатор Интернета). Он также производит обратное разрешение адресов, когда web-сервер или любой другой хост (10.1.1.0/24), представленный во внутренней среде внутреннего маршрутизатора, выполняет попытку доступа к хосту A (192.168.1.5).

Посещение внешним пользователем web-сервера внутренней сети

Ниже приводится описание перемещения данных через модуль FWSM:

1. Пользователь внешней сети выполняет запрос web-страницы с внутреннего web-сервера. Модуль FWSM получает пакет и, если необходимо, добавляет MAC-адрес источника в таблицу MAC-адресов. Поскольку данный сеанс — новый, модуль проверяет, разрешен ли пакет в соответствии с условиями политики безопасности (списками доступа, фильтрами или AAA-аутентификацией).**Примечание:** Для многоконтекстного режима FWSM сначала классифицирует пакет в соответствии с уникальным интерфейсом.

2. Модуль FWSM регистрирует установление сеанса только в том случае, если внешнему пользователю разрешен доступ на внутренний web-сервер. Доступ на web-сервер должен быть разрешен для внешнего пользователя с помощью списка доступа.
3. Если MAC-адрес получателя присутствует в таблице, то модуль FWSM отправляет пакет с внутреннего интерфейса. В качестве MAC-адреса получателя используется адрес нижестоящего маршрутизатора, 192.168.1.3.
4. Если MAC-адрес получателя отсутствует в таблице модуля FWSM, то модуль пытается его обнаружить при отправке запроса ARP и эхо-запроса. Первый пакет отбрасывается.
5. Веб-сервер отвечает на запрос. Поскольку сеанс уже выполняется, пакет обходит множество поисков, связанных с новым соединением. Модуль FWSM пересылает пакет внешнему пользователю.

Получение доступа для внешнего пользователя к внутреннему хосту

Пользователь внешней сети выполняет попытку доступа к внутреннему хосту. Модуль FWSM получает пакет и, если необходимо, добавляет MAC-адрес источника в таблицу MAC-адресов. Поскольку данный сеанс — новый, система проверяет, разрешен ли пакет в соответствии с условиями политики безопасности (списками доступа, фильтрами или AAA-аутентификацией).

Примечание: Для многоконтекстного режима FWSM сначала классифицирует пакет в соответствии с уникальным интерфейсом.

Пакет отклоняется и модуль FWSM отбрасывает его, поскольку у внешнего пользователя отсутствуют права доступа к внутреннему хосту. В случае атаки внешнего пользователя на внутреннюю сеть модуль FWSM при помощи ряда методов определяет, допустим ли данный пакет в уже установленном сеансе.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

```
cisco(config)#show firewall Firewall mode: Transparent
```

Устранение неполадок

Сквозное пропускание трафика

В прозрачном режиме межсетевого экрана для передачи многоадресного трафика сверху вниз и снизу вверх необходимы списки контроля доступа. В обычных межсетевых экранах при передаче сверху вниз этого не требуется.

Примечание: Адрес многоадресной рассылки (224.0.0.9) ни при каких обстоятельствах не может являться исходным адресом для возвратного трафика, поэтому в обратном

направлении такой трафик впущен не будет, и необходимы два списка контроля доступа: на выход и на вход.

Например, список контроля доступа прозрачного межсетевого экрана для пропускания RIP-трафика будет иметь вид, аналогичный следующему примеру:

RIP

Внешний список контроля доступа (на вход):

```
access-list outside permit udp host (outside source router) host 224.0.0.9 eq 520
access-group outside in interface outside
```

Внутренний список контроля доступа (на выход):

```
access-list inside permit udp host (inside source router) host 224.0.0.9 eq 520
access-group inside in interface inside
```

Выполнение EIGRP:

```
access-list inside permit eigrp host (inside source) host 224.0.0.10
 access-group inside in interface inside
access-list outside permit eigrp host (outside source) host 224.0.0.10
access-group outside in interface outside
```

Для OSPF:

```
access-list inside permit ospf host ( inside source ) host 224.0.0.5
( this access-list is for hello packets )
access-list inside permit ospf host ( inside source ) host 224.0.0.6
( dr send update on this port )
access-list inside permit ospf host ( inside source ) host ( outside source )
access-group inside in interface inside
 access-list outside permit ospf host ( outside source ) host 224.0.0.5
access-list outside permit ospf host ( outside source ) host 224.0.0.6
access-list outside permit ospf host ( outside sourec ) host ( inside source )
access-group outside in interafce outside
```

Соответствие между сетями VLAN для платы MSFC и модуля FWSM

В прозрачном режиме не требуется назначать одинаковые сети VLAN на интерфейсе платы MSFC и в модуле FWSM, поскольку данный режим представляет собой разновидность моста.

Дополнительные сведения

- Cisco PIX Firewall Software
- Запросы комментариев (RFC)
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- PIX/ASA: Пример конфигурации прозрачного межсетевого экрана
- Cisco Systems – техническая поддержка и документация