FWSM : Сбои вследствие трафика устранения неполадок к неправильному Xlates

Содержание

Введение

Из-за дизайна Модуля Сервисов межсетевого экрана (FWSM) пакетная обработка, xlates, созданный неправильно пакетами для маршрутизации, может вызвать сбои трафика для соединений через межсетевой экран. Для выбора исходящего интерфейса для входящего пакета первые проверки FWSM, чтобы видеть, совпадает ли IP - адрес назначения входящего пакета с каким-либо существующим глобальным IP - адресом / Сеть в преобразовании NAT (xlate) для того интерфейса в его таблице xlate. Если соответствие найдено, исходящий интерфейс просто выбран на основе локального интерфейса в записи xlate, и межсетевой экран не консультируется с таблицей маршрутизации для принятия решения исходящего интерфейса.

Поведение по умолчанию FWSM должно создать запись xlate для source IP любого разрешенного пакета, который получен на одном из его интерфейсов. Если пакет маршрутизируется через сеть неправильно (для какого-либо количества причин) и поступает входящий в неверный интерфейс FWSM, xlate создан для отражения этого. Когда это происходит, записи в таблице xlate могут отвергнуть записи в таблице маршрутизации и вызвать сбои трафика для назначений, на которые влияют.

Этот документ описывает признаки и триггеры для этой проблемы, как диагностировать его

и предоставляет решения для того, чтобы препятствовать тому, чтобы он произошел.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с FWSM.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Признаки

Логическая топология

Соответствующая конфигурация

```
interface Vlan1
 nameif outside
 security-level 0
 ip address 192.168.100.50 255.255.255.0
!
interface Vlan10
 nameif inside
 security-level 100
 ip address 10.10.1.50 255.255.255.0
!
interface Vlan20
 nameif dmz
 security-level 50
 ip address 10.20.1.50 255.255.255.0
!
same-security-traffic permit intra-interface
access-list outside_in extended permit tcp any host 10.30.1.1 eq www
access-list inside_in extended permit ip any any
access-group inside_in in interface inside
access-group outside_in in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.100.254
route dmz 10.30.1.0 255.255.255.0 10.20.1.254
```

Наблюдаемые состояния

Соединения от клиентского компьютера в 172.16.1.10 на Web-сервер в 10.30.1.1 сбоях.

Захват пакета на **внешнем интерфейсе** показывает SYN TCP от клиентского компьютера, поступающего в интерфейс FWSM.

```
FWSM# show capture outside
3 packets seen, 3 packets captured
   1: 13:58:09.280752960 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
   2: 13:58:12.280755950 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
   3: 13:58:18.280761960 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
3 packets shown
```

Захват пакета на интерфейсе **dmz** не показывает что пакет, оставляя межсетевой экран.

```
FWSM# show capture dmz
0 packet seen, 0 packet captured
0 packet shown
```

Никакая запись не создана в таблице подключений FWSM, и системные журналы не показывают информации, отнесенной клиенту или IP-адресам сервера.

Триггеры

На фундаментальном уровне эта проблема вызвана записью в таблице xlate FWSM, которая была создана неправильно пакет для маршрутизации. Из-за пути разработана пакетная обработка FWSM, межсетевой экран проверяет таблицу xlate, прежде чем это проверит таблицу маршрутизации для определения исходящего интерфейса. В результате, если пакет совпадет с существующим xlate, то исходящий интерфейс будет выбран на основе той записи, даже если запись будет конфликтовать с тем, что перечислено в таблице маршрутизации. Другими словами, таблица xlate имеет приоритет по таблице маршрутизации.

Для диагностирования этой проблемы проверьте выходные данные **команды show xlate debug**:

```
FWSM# show xlate debug
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       o - outside, r - portmap, s - static
3 in use, 3 most used
NAT from inside:10.30.1.1 to outside:10.30.1.1 flags Ii idle 0:00:00 timeout 3:00:00 connections
0
NAT from inside:10.30.1.1 to inside:10.30.1.1 flags Ii idle 0:00:07 timeout 3:00:00 connections
0

NAT from dmz:10.30.1.1 to outside:10.30.1.1 flags Ii idle 0:00:10 timeout 3:00:00 connections 0
```

Примечание: Ключевое слово отладки в show xlate крайне важно. Без него записи xlate не будут включать имена интерфейсов, к которым привязана запись.

Таблица xlate показывает, что существует 3 xlates, созданные для Web-сервера. Первый xlate создан между **внутренним интерфейсом** и **внешним интерфейсом**. Второй xlate создан как hairpinned или u-turned xlate на **внутреннем интерфейсе**. Третий xlate создан между **dmz** и **внешним интерфейсом**. Я отмечает, указывает, что это - идентификационный xlate, и IP фактически не преобразовывается.

Первый интерфейс, перечисленный в записи, является "реальным" или "локальным" интерфейсом, где IP, как предполагается, фактически существует. Второй перечисленный интерфейс является "сопоставленным" или "глобальным" интерфейсом, где преобразовывается IP. Ни один из них показанный xlates не корректен. Это вызвано тем, что Web-сервер (10.30.1.1) фактически существует позади интерфейса **dmz**. Третий xlate

корректен для этой организации сети.

Ошибка подключения происходит из-за первого xlate, перечисленного в таблице. Когда Пакет TCP SYN клиента поступает во внешний интерфейс, предназначенный к 10.30.1.1, FWSM проверяет таблицу xlate и совпадает с первой записью. Эта запись указывает, что пакет должен выход на **внутреннем интерфейсе**, который является неправильным, и пакет помещен в черный список.

По умолчанию FWSM автоматически создаст идентификационный xlate для любого трафика, который не совпадает с явно настроенным правилом NAT. Из-за этого, даже если пакет ошибочно поступает в неверный интерфейс, будет создан xlate. В частности для этого случая, пакеты из источника от 10.30.1.1 поступили входящие во **внутренний интерфейс** вместо того, чтобы поступить в интерфейс **dmz**, как ожидается.

Когда Web-сервер пытался пропинговать несуществующий IP-адрес (10.199.199.1), первый xlate (**внутри> снаружи**) был создан. Запрос эха оставил Web-сервер предназначенным его шлюзу по умолчанию (маршрутизатор DMZ). Маршрутизатор DMZ передал пакет к внутреннему маршрутизатору на его статический маршрут:

```
S       10.0.0.0/8 [1/0] via 10.50.1.254
```

Поскольку 10.199.199.0/24 сеть фактически не существует нигде, внутренний маршрутизатор просто придерживается своего маршрута по умолчанию и передает пакет к **внутреннему интерфейсу** FWSM:

```
S*   0.0.0.0/0 [1/0] via 10.20.1.50
```

Аналогично, FWSM также не имеет маршрута для сети назначения. Поэтому это выбирает внешний интерфейс как исходящий интерфейс и создает идентификационный xlate **изнутри> снаружи**:

```
S    0.0.0.0 0.0.0.0 [1/0] via 192.168.100.254, outside
```

Второй xlate (**внутри> внутри**) был создан, когда Web-сервер пытался обратиться к серверу DNS, в то время как 10.40.1.254 интерфейса внутреннего маршрутизатора временно не работали из-за откидной створки ссылки. Запрос DNS оставил Web-сервер предназначенным его шлюзу по умолчанию (маршрутизатор DMZ). Маршрутизатор DMZ передал пакет к внутреннему маршрутизатору на его статический маршрут:

```
S       10.0.0.0/8 [1/0] via 10.50.1.254
```

Однако интерфейс внутреннего маршрутизатора, связанный с 10.40.1.0/24 сетью, временно не работал, и ее маршрут прямого соединения для этой сети отсутствовал. Поэтому единственный подходящий маршрут в таблице маршрутизации был маршрутом по умолчанию назад к FWSM:

```
S*   0.0.0.0/0 [1/0] via 10.20.1.50
```

Пакет маршрутизировался к **внутреннему интерфейсу** FWSM. Таблица маршрутизации FWSM указала, что сеть назначения 10.40.1.0/24 существовала позади того же **внутреннего интерфейса**:

```
S    10.40.1.0 255.255.255.0 [1/0] via 10.10.1.254, inside
```

Поскольку **команда same-security-traffic permit intra-interface** включена, FWSM позволит u-turned xlate быть созданным.

Для суммирования первый xlate был инициирован:

- Широкий маршрут 10.0.0.0/8 настроен на маршрутизаторе DMZ
- **ACL permit ip any any** настроен на внутреннем интерфейсе FWSM

Второй xlate был инициирован:

- Интерфейс переброски на Внутреннем маршрутизаторе
- **внутриинтерфейс разрешения на same-security-traffic** настроен на FWSM

Решения

Существует много других возможных решений к этой проблеме. Прежде всего удаление xlate от таблицы должно позволить трафику начинать работать снова, пока не восстановлен xlate. Это может быть сделано с **командой clear xlate**. Пример:

```
FWSM# clear xlate interface inside local 10.30.1.1 global 10.30.1.1
```

Примечание: Любые соединения, которые используют удаленный xlate, будут также разъединены.

Как только это завершено, фокус должен быть на препятствовании тому, чтобы возвратился xlates. Часто времена, большая часть рекомендуемого способа, чтобы сделать это должно исправить настройку маршрутизации в среде, чтобы препятствовать тому, чтобы трафик поступил в неправильный интерфейс FWSM. FWSM также предлагает ряд параметров конфигурации для решения этих проблем.

Решите конфигурации неправильной маршрутизации

Это решение берет тщательное планирование и глубокое понимание сетевой среды. В первом приведенном выше примере маршрут 10.0.0.0/8 на маршрутизаторе DMZ является технически неправильным, так как вся/8 сеть не существует вне своих 10.50.1.253 интерфейсов. Вместо этого некоторые опции, которые существуют:

- Устраните 10.50.1.0/24 сеть все вместе и просто направьте весь трафик через FWSM. Это также предоставляет лучшую сегментацию и безопасность между Внутренней частью и сетями DMZ.
- Настройте статический маршрут на DMZ для только 10.40.1.0/24 и удалите маршрут 10.0.0.0/8.
- Используйте протокол динамической маршрутизации между Внутренней частью и маршрутизаторами DMZ для корректного объявления только сетей, которые фактически существуют.

Часто существует много возможностей для регулировки настройки маршрутизации, но конечная цель должна гарантировать, что трафик от данного хоста в состоянии поступить только в одиночный интерфейс FWSM.

Отключите внутриинтерфейс разрешения на same-security-traffic

Команда same-security-traffic permit intra-interface позволяет FWSM развороту или трафику шпильки на интерфейсе. Это означает, что пакет может ввести межсетевой экран в тот же интерфейс, на котором это уезжает. Эта функциональность отключена по умолчанию и имеет очень мало использования в большинстве дизайнов FWSM. Поскольку FWSM использует интерфейсы виртуальной локальной сети (VLAN), трафик, который остается в

той же VLAN, никогда не должен обрабатываться FWSM.

Во втором приведенном выше примере **команда same-security-traffic permit intra-interface** позволила пакету и вводить и оставлять **внутренний интерфейс**. Отключение **внутриинтерфейса разрешения на same-security-traffic** предотвратило бы это поведение и отбросило бы пакет, прежде чем когда-либо создавался xlate:

```
FWSM(config)# no same-security-traffic permit intra-interface
```

Пакеты отбрасывания, которые Поступают в Неверный интерфейс (ACL или uRPF)

Когда пакет от Web-сервера неправильно поступил во **внутренний интерфейс,** в обоих приведенных выше примерах был создан xlates. Для предотвращения проблемы все вместе, FWSM может быть настроен для отбрасывания пакетов, которые поступают в неверный интерфейс.

FWSM требует, чтобы весь трафик был разрешен ACL, прежде чем это сможет пройти. Поэтому эта функциональность может быть достигнута, только разрешив трафик от соответствующих исходных сетей на каждом интерфейсе. В приведенных выше примерах **внутренний интерфейс** разрешает весь IP - трафик:

```
access-list inside_in extended permit ip any any
```

Вместо этого это должно быть изменено, чтобы только разрешить трафик от 10.10.1.0/24 и 10.40.1.0/24 подсетей:

```
access-list inside_in extended permit ip 10.10.1.0 255.255.255.0 any

access-list inside_in extended permit ip 10.40.1.0 255.255.255.0 any
```

В некоторых средах это не подходящий параметр из-за размера и/или масштаба других сетей, проходящих через FWSM. Однако эта функциональность может быть достигнута, проще использовав функцию под названием Одноадресная пересылка по обратному пути (uRPF).

Когда опция uRPF будет активирована, FWSM сравнит IP - адрес источника первого пакета каждого соединения против его таблицы маршрутизации. Если маршрут, который найден, не совпадет с интерфейсом, в который поступил пакет, то тот пакет будет отброшен из-за Ошибки переадресации по обратному пути.

В приведенном выше примере FWSM имеет статический маршрут, который использует интерфейс **dmz** для достижения 10.30.1.0/24 сети. Поэтому, если uRPF будет включен на **внутреннем интерфейсе**, пакетах из источника от Web-сервера (10.30.1.1), которые поступают неправильно во **внутренний интерфейс**, то будет отброшен.

Для включения uRPF примените **команду ip verify reverse-path** к каждому рассматриваемому интерфейсу. Пример:

```
FWSM(config)# ip verify reverse-path interface inside
```

Включите обход xlate

В обоих из приведенных выше примеров xlates создан с флагами Ii. Эти флаги указывают, что xlate является идентификационной трансляцией (I), которая произошла на интерфейсе высокого уровня безопасности (i). По умолчанию FWSM создаст их xlates для любого

трафика, который не совпадает с явным правилом NAT/PAT. Для отключения этого поведения **команда xlate-bypass** может быть включена в FWSM 3.2 (1) и позже:

```
FWSM(config)# xlate-bypass
```

Эта функция будет препятствовать тому, чтобы FWSM создал идентификационный xlates во-первых. Таким образом трафик в приведенных выше примерах не был бы перенаправлен к неверному интерфейсу из-за элемента таблицы xlate. Однако трафик все еще пройдет через непреобразованный FWSM.

Сводка

Для определения исходящего интерфейса для пакета FWSM будет всегда консультироваться со своей таблицей xlate перед рассмотрением его таблицы маршрутизации. Если тот пакет совпадает с существующим xlate, исходящий интерфейс выбран на основе связанного интерфейса xlate. Это происходит независимо от любых противоречий, которые могли бы быть найдены в таблице маршрутизации. Таким образом таблица xlate имеет приоритет по таблице маршрутизации.

Поскольку FWSM будет всегда создавать запись xlate для всех новых соединений по умолчанию, это может вызвать сбои трафика в случаях, где неправильно пакеты для маршрутизации заставляют FWSM создавать xlate. Как выделено выше, существует много возможных сценариев, где это может произойти, но все относятся назад к пакету, получаемому на неверном интерфейсе. Этот документ покрыл эти возможные проблемы:

- Широкий config маршрутизации передает пакеты в неверном направлении
- FWSM настроен для разрешения трафика от неправильных исходных сетей
- FWSM настроен к трафику шпильки/поворота на 180 градусов

Для быстрого восстановления подключения для соединений, которые отказывают из-за неправильного xlate, удаляют запись с **командой clear xlate**. Этот документ также покрыл множественные решения для того, чтобы препятствовать тому, чтобы они xlates возвратились в будущем, включая:

- Решите конфигурации неправильной маршрутизации с помощью уточненных маршрутов
- Отключите внутриинтерфейс разрешения на same-security-traffic
- Пакеты отбрасывания, которые поступают в неверный интерфейс с помощью ACL или uRPF
- Включите обход xlate

Дополнительные сведения

- Справочник по командам: ip проверяет обратный путь
- Справочник по командам: обход xlate
- Cisco Systems – техническая поддержка и документация