

Трафик UDP через Сбои ASA после Ссылки Основного поставщика услуг Интернет Возвращается Онлайн в Двойной Настройке интернет-провайдера

Содержание

[Введение](#)

[Перед началом работы](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Проблема](#)

[Решение](#)

[Дополнительные сведения](#)

Введение

Если Устройство адаптивной защиты (ASA) имеет два исходящих интерфейса на подсеть назначения, и предпочитаемый маршрут назначению удаляется из таблицы маршрутизации в течение некоторого времени, связи Протокола UDP могут прерваться, когда предпочитаемый маршрут становится повторно добавленным к таблице маршрутизации. На TCP - подключения могла бы также влиять проблема, но так как TCP обнаруживает потерю пакета, эти соединения разъединены автоматически окончательными точками и восстановили использование большего количества оптимальных маршрутов после изменения маршрутов.

Эта проблема может также быть замечена, если протокол маршрутизации используется, и изменение топологии инициирует изменение в таблице маршрутизации на ASA.

Перед началом работы

Требования

Для обнаружения с этой проблемой таблица маршрутизации ASA должна измениться. Это распространено с двойными каналами поставщика избыточной формой или когда ASA учится, направляет через IGP (OSPF, EIGRP, RIP).

Эта проблема происходит, когда ссылка основного поставщика услуг Интернет возвращается онлайн, или упомянутый IGP видит повторное схождение, из-за который меньше предпочитаемого маршрута, который использовался ASA, заменен предпочтительным более низким метрическим маршрутом. Вы тогда видели бы

долговечные соединения, такие как регистрации SIP UDP, GRE, и т.д., отказывая однажды основной, или предпочитаемый маршрут повторно установлен в таблицу маршрутизации ASA.

Используемые компоненты

Сведения в документе приведены на основе данных версий аппаратного и программного обеспечения:

- Любое многофункциональное устройство защиты Cisco ASA серии 5500
- Версии ASA 8.2 (5), 8.3 (2) 12, 8.4 (1) 1, 8.5 (1) и позже

Условные обозначения

[Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.](#)

Проблема

Если запись таблицы маршрутизации удалена из таблицы маршрутизации ASA и нет никаких маршрутов из интерфейса для достижения назначения, соединения, созданные через межсетевой экран, с которым внешнее назначение будет удалено ASA. Это происходит так, чтобы соединения могли быть созданы снова с помощью другого интерфейса с записями маршрутизации для целевого подарка.

Однако, если уточненные маршруты будут добавлены назад к таблице, то соединения не будут обновлены для использования новых, уточненных маршрутов и продолжат использовать менее - оптимальный интерфейс.

Например, полагайте, что межсетевой экран имеет два интерфейса, которые стоят перед Интернетом - "снаружи" и "резервная копия" - и эти два маршрута существуют в конфигурации ASA:

```
route outside 0.0.0.0 0.0.0.0 10.1.1.1 1 track 1
route backup 0.0.0.0 0.0.0.0 172.16.1.1 254
```

Если и внешняя сторона и резервные интерфейсы будут подключены, то соединения, созданные исходящий через межсетевой экран, будут использовать внешний интерфейс, поскольку это имеет предпочтительную метрику 1. Если внешний интерфейс закрыт (или функция мониторинга SLA, которая отслеживает обнаружение маршрута потеря подключения к отслеженному IP), соединения с помощью внешнего интерфейса были бы разъединены и восстановили использование резервного интерфейса, поскольку резервный интерфейс является единственным интерфейсом с маршрутом назначению.

Проблема происходит, когда внешний интерфейс принесен резервное копирование, или отслеживаемый маршрут становится привилегированным маршрутом снова. Таблица маршрутизации обновлена для предпочтения исходного маршрута, но существующие соединения продолжают существовать на ASA и пересекать резервный интерфейс и НЕ удалены и воссозданы на внешнем интерфейсе с более предпочтенной метрикой. Это вызвано тем, что резервный маршрут по умолчанию все еще существует в интерфейсно-специфичной таблице маршрутизации ASA. Соединение продолжает использовать интерфейс с меньшим количеством предпочитаемого маршрута, пока не удалено

соединение; в случае UDP это могло бы быть неопределенно.

Эта ситуация может вызвать проблемы с долговечными соединениями, такими как внешние регистрации SIP или другие UDP - подключения.

Решение

Для рассмотрения этой определенной проблемы новая характеристика была добавлена к ASA, который заставит соединения быть разъединенными и восстановленными на новом интерфейсе, если больше предпочитаемого маршрута назначению будет добавлено к таблице маршрутизации. Для активирования опции (она отключена по умолчанию), установите ненулевой таймаут в команду **timeout floating-conn**. Этот таймаут (заданный в HH:MM:SS) задает время, ASA ждет, прежде чем это разъединит соединение однажды, больше предпочитаемого маршрута добавлено назад к таблице маршрутизации:

Это - пример CLI активации опции. С этим CLI, если пакет получен на существующем соединении, для которого существует теперь другое, больше предпочитаемого маршрута назначению, соединение будет разъединено 1 минуту спустя (и восстановил использование нового, большего количества предпочитаемого маршрута):

```
ASA# config terminal ASA(config)# timeout floating-conn 0:01:00 ASA(config)# end ASA# show run
timeout conn 1:00:00 half-closed 0:10:00 udp 0:50:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00
sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:01:00
absolute timeout tcp-proxy-reassembly 0:01:00 timeout xlate 0:01:00 timeout pat-xlate 0:00:30
timeout floating-conn 0:01:00 ASA#
```

Эта опция добавлена к платформе ASA в версиях 8.2 (5), 8.3 (2) 12, 8.4 (1) 1, и 8.5 (1), включая более поздние версии программного обеспечения ASA.

Если вы выполняете версию кода ASA, который не реализует эту опцию, обходной путь к проблеме должен был бы вручную сбросить UDP - подключения, которые продолжают брать меньше предпочитаемого маршрута несмотря на лучший маршрут, сделанный доступный через ясный `<ip> local-host` или `<ip> clear conn`.

Справочник по командам перечисляет эту новую характеристику под разделом [таймаута](#).

Дополнительные сведения

- [Cisco Systems – техническая поддержка и документация](#)