Когда клиенты VPN разъединяют, ASA имеет высокую загрузку ЦП из-за петли трафика

Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Общие сведения](#)
[Проблема: Пакеты, предназначенные для разъединенной петли клиента VPN во внутренней сети](#)
[Проблема: Направленные (сетевые) Транслируемые пакеты, Генерируемые Клиентами VPN, Циклично выполнены на Внутренней сети](#)
[Решения проблемы](#)
[Статический маршрут решения 1-для интерфейса Null0 (версия ASA 9.2.1 и позже)](#)
[Решение 2 - использует другой пул IP для клиентов VPN](#)
[Решение 3 - делает таблицу маршрутизации ASA более определенной для внутренних маршрутов](#)
[Решение 4 - добавляет уточненный маршрут для подсети VPN Назад из внешнего интерфейса](#)

Введение

Этот документ описывает общую проблему, которая происходит, когда клиенты VPN разъединяют от устройства адаптивной защиты Cisco (ASA), который выполняется как головной узел VPN для удаленного доступа. Этот документ также описывает ситуацию, где петля трафика происходит, когда пользователи VPN разъединяют от межсетевого экрана ASA. Этот документ не покрывает, как настроить или установить удаленный доступ к VPN, только определенная ситуация, которая является результатом определенных общих настроек маршрутизации.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Конфигурация VPN для удаленного доступа на ASA
- Базовый уровень 3 понятия маршрутизации

Используемые компоненты

Сведения в этом документе основываются на Модели 5520 ASA, которая выполняет версию кода 9.1 (1) ASA.

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

Этот документ может использоваться с этими версиями программного и аппаратного обеспечения:

- Любая модель ASA
- Любая версия кода ASA

Общие сведения

Когда пользователь соединяется с ASA как концентратор VPN для удаленного доступа, ASA устанавливает основанный на хосте маршрут в Таблице маршрутизации ASA, которая направляет трафик тому клиенту VPN из внешнего интерфейса (к Интернету). Когда тот пользователь разъединяет, маршрут удален из таблицы, и пакеты на внутренней сети (предназначенный тому разъединенному пользователю VPN) могли бы быть циклично выполнены между ASA и устройством внутренней маршрутизации.

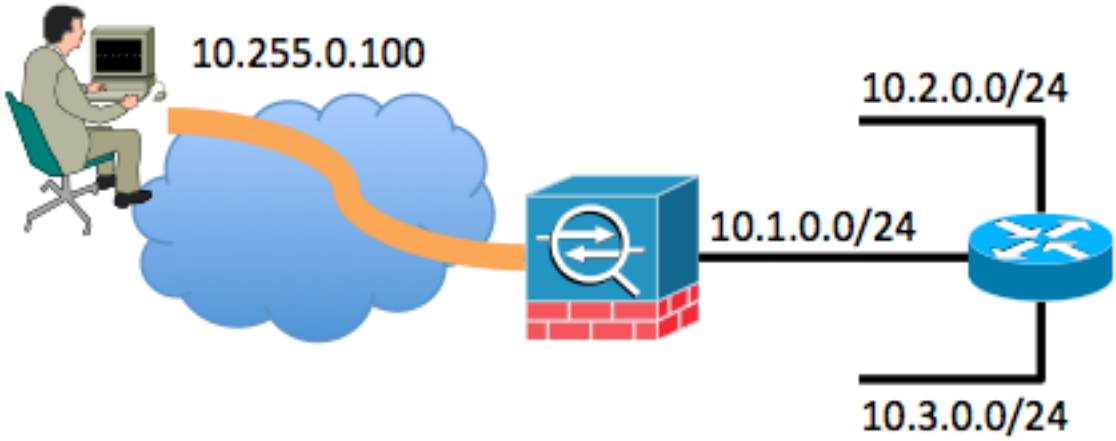
Другая проблема - направленные (сетевые) транслируемые пакеты (генерируемый удалением клиентов VPN) могли бы быть переданы ASA как одноадресный фрейм к внутренней сети. Это могло бы передать его назад ASA, который заставляет пакет быть циклично выполненным, пока не истекает Время жизни (TTL).

Этот документ объясняет эти проблемы и показывает, какие методы настройки могут использоваться для предотвращения проблемы.

Проблема: Пакеты, предназначенные для разъединенной петли клиента VPN во внутренней сети

Когда пользователь VPN для удаленного доступа разъединяет от межсетевого экрана ASA, пакеты все еще представляют на внутренней сети (предназначенный для тех разъединенных пользователей), и адрес VPN назначенного IP - адреса мог бы стать циклично выполненным во внутренней сети. Эти зацикливания пакетов могли бы заставить использование ЦПУ на ASA увеличиваться, пока петля не останавливается или из-за значения IP TTL в Заголовке IP - пакете, постепенно уменьшающемся к 0, или пользователь воссоединяется, и IP-адрес повторно назначен на клиент VPN.

Для понимания этого сценария лучше, рассмотрите эту топологию:



В данном примере клиенту удаленного доступа назначили IP-адрес 10.255.0.100. ASA в данном примере связан с тем же сегментом внутренней сети наряду с маршрутизатором. Маршрутизатор имеет два дополнительных сегмента сети Уровня 3, связанные с ним. Соответствующий интерфейс (маршрутизация) и конфигурации VPN ASA и маршрутизатора показывают в примерах.

Выделение конфигурации ASA показывают в данном примере:

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.0.1 255.255.255.0
!
same-security-traffic permit intra-interface
!
ip local pool VPNpool 10.255.0.1-10.255.0.255
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
route inside 10.0.0.0 255.0.0.0 10.1.0.2
```

Выделение конфигурации маршрутизатора показывают в данном примере:

```
interface FastEthernet0
description connected to the inside interface of the ASA G0/1
ip address 10.1.0.2 255.255.255.0
!
interface FastEthernet1
 description connected to network segment
 ip address 10.2.0.1 255.255.255.0
!
interface FastEthernet2
 description connected to other network segment
 ip address 10.3.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.0.1
```

Таблице маршрутизации маршрутизатора, связанного с внутренней частью ASA просто, указали на маршрут по умолчанию Внутренний интерфейс ASA 10.1.0.1.

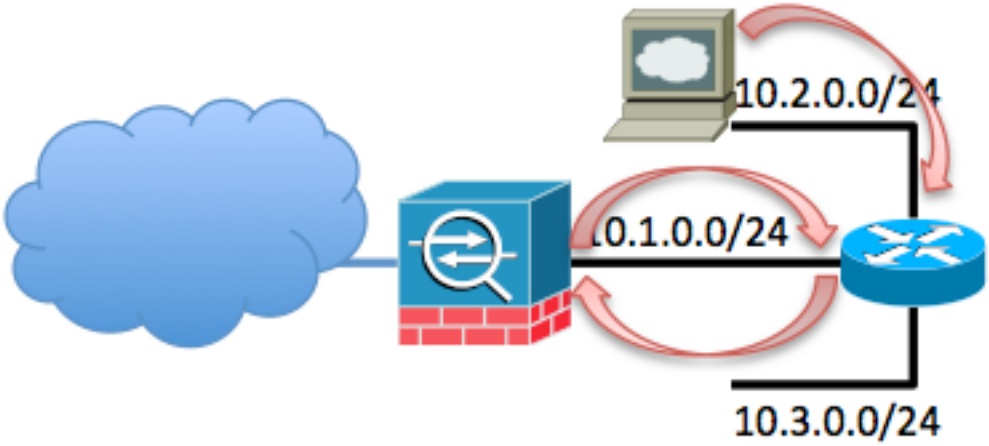
В то время как пользователь связан через VPN с ASA, Таблица маршрутизации ASA показывает следующим образом:

```
ASA# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 198.51.100.1 to network 0.0.0.0
S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Когда пользователь VPN для удаленного доступа разъединяет от VPN, проблема происходит. На этом этапе основанный на хосте маршрут удален из Таблицы маршрутизации ASA. Если хост в сети пытается передать трафик клиенту VPN, тот трафик маршрутизируется к Внутреннему интерфейсу ASA маршрутизатором. Эта серия шагов происходит:

1. Пакет, предназначенный к 10.255.0.100, поступает во внутренний интерфейс ASA.
2. Выполнены стандартные проверки ACL.
3. Таблица маршрутизации ASA проверена для определения исходящего интерфейса для этого трафика.
4. Назначение пакета совпадает с широким маршрутом 10.0.0.0/8, который указывает назад из внутреннего интерфейса к маршрутизатору.
5. ASA проверяет, позволен ли трафик прикрепления - это ищет **внутриинтерфейс разрешения той-же-безопасности** и находит, что позволено.
6. Соединение создано к и из внутреннего интерфейса, и пакет передают обратно в маршрутизатор как следующий переход.
7. Маршрутизатор получает пакет, предназначенный к 10.255.0.100 на интерфейсе, который стоит перед ASA. Маршрутизатор проверяет свою таблицу маршрутизации для подходящего следующего перехода. Маршрутизатор находит, что следующим переходом был бы Внутренний интерфейс ASA, и пакет передан к ASA.
8. Вернитесь к п. 1.

Пример выходных данных команды приводится ниже:



Эта петля происходит до TTL этого пакета декременты к 0. Обратите внимание на то, что Межсетевой экран ASA **не** постепенно уменьшает значение TTL по умолчанию, когда это обрабатывает пакет. Маршрутизатор постепенно уменьшает TTL, поскольку это направляет пакет. Это предотвращает возникновение этой петли неопределенно, но эта петля действительно увеличивает трафик на ASA и заставляет использование ЦПУ пронзать.

Проблема: Направленные (сетевые) Транслируемые пакеты, Генерируемые Клиентами VPN, Циклично выполнены на Внутренней сети

Эта проблема подобна первой проблеме.. Если клиент VPN генерирует пакет адресной трансляции к его подсети назначенного IP - адреса (10.255.0.255 в предыдущем примере), то тот пакет мог бы быть передан как одноадресный фрейм ASA к внутреннему маршрутизатору. Внутренний маршрутизатор мог бы тогда передать его назад ASA, который заставляет пакет циклично выполняться, пока не истекает TTL.

Эта серия событий происходит:

1. Машина клиента VPN генерирует пакет, предназначенный к адресу сетевой широковещательной рассылки 10.255.0.255, и пакет поступает в ASA.
2. ASA рассматривает этот пакет как одноадресный фрейм (из-за таблицы маршрутизации) и вперед это к внутреннему маршрутизатору.

3. Внутренний маршрутизатор, который также рассматривает пакет как одноадресный фрейм, постепенно уменьшает TTL пакета и вперед его назад к ASA.

4. Повторения процесса до TTL пакета уменьшены до 0.

Решения проблемы

Существует несколько возможных решений к этой проблеме. В зависимости от топологии сети и определенной ситуации, одно решение могло бы быть легче внедрить, чем другой.

Статический маршрут решения 1-для интерфейса Null0 (версия ASA 9.2.1 и позже)

При передаче трафика к интерфейсу **Null0** он заставляет пакеты, предназначенные к указанной сети быть отброшенными. Эта функция полезна при настройке Удаленно инициированной черной дыры (RTBH) для Протокола BGP. Если уточненный маршрут (предоставленный Включением ввода обратной маршрутизации) не присутствует, в этой ситуации при настройке маршрута к Null0 для подсети клиента удаленного доступа он вынуждает ASA отбросить трафик, предназначенный к хостам в той подсети.

```
route Null0 10.255.0.0 255.255.255.0
```

Решение 2 - использует другой пул IP для клиентов VPN

Это решение состоит в том, чтобы назначить удаленных пользователей VPN IP-адрес, который не накладывается ни на какую подсеть внутренней сети. Это было бы препятствовать тому, чтобы ASA передал пакеты, предназначенные к той подсети VPN назад к внутреннему маршрутизатору, если не был связан пользователь VPN.

Решение 3 - делает таблицу маршрутизации ASA более определенной для внутренних маршрутов

Это решение состоит в том, чтобы гарантировать, что таблица маршрутизации ASA не имеет никаких очень широких маршрутов, которые накладываются на пул IP VPN. Для этого определенного примера сети удалите маршрут 10.0.0.0/8 из ASA и настройте более определенные статические маршруты для подсетей, которые находятся прочь внутреннего интерфейса. Зависящий от количества подсетей и топологии сети, это могло бы быть большим числом статических маршрутов, и это не могло бы быть возможно.

Решение 4 - добавляет уточненный маршрут для подсети VPN Назад из внешнего интерфейса

Это решение более сложно, что другие, которые описаны в этом документе. Cisco рекомендует попытаться использовать другие решения сначала из-за ситуации, которая описана в Примечании позже в этом разделе. Это решение состоит в том, чтобы препятствовать тому, чтобы ASA передал пакеты из источника IP от IP-подсети VPN назад к встроенному маршрутизатору; если вы добавляете уточненный маршрут для подсети VPN из внешнего интерфейса, можно сделать это. Так как эта IP-подсеть зарезервирована для внешних пользователей VPN, пакеты с IP - адресом источника от этой IP-подсети VPN никогда не должны поступать входящие во Внутренний интерфейс ASA. Самый легкий способ достигнуть этого состоит в том, чтобы добавить маршрут для Пула IP VPN для удаленного доступа из внешнего интерфейса с IP-адресом следующего перехода восходящего маршрутизатора ISP.

В этом примере топологии сети тот маршрут был бы похож на это:

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

В дополнение к этому маршруту добавьте **ip проверяет обратный путь в** команде, чтобы заставить ASA понижаться, любые пакеты получили входящий на внутреннем интерфейсе, полученном от IP-подсети VPN из-за большего количества предпочитаемого маршрута, который существует на внешнем интерфейсе:

```
ip verify reverse-path inside
```

После того, как эти команды внедрены, Таблица маршрутизации ASA выглядит подобной этому, когда связан пользователь:

```
ASA# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 198.51.100.1 to network 0.0.0.0

S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
S 10.255.0.0 255.255.255.0 [1/0] via 198.51.100.1, outside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Когда клиент VPN связан, основанный на хосте маршрут к тому IP-адресу VPN присутствует в таблице и предпочтен. То, когда клиент VPN разъединяет, трафик, полученный от того IP-адреса клиента, который поступает во внутренний интерфейс, проверено против таблицы маршрутизации и отброшено из-за **ip проверяет обратный путь в** команде.

Если клиент VPN генерирует широковещание сети санкционируемой связи к IP-подсети VPN, то тот пакет передан к внутреннему маршрутизатору и передан маршрутизатором назад к ASA, где это отброшено из-за **ip проверяет обратный путь в** команде.

> **Примечание:** После того, как это решение внедрено, если команда **внутриинтерфейса разрешения той-же-безопасности** присутствует в конфигурации, и политика доступа разрешает его, трафик, полученный от пользователя VPN, предназначенного к IP-адресу в пуле IP VPN для пользователя, который не связан, мог бы маршрутизироваться назад из внешнего интерфейса в открытом тексте. Это - нераспространенная ситуация и может быть смягчено с использованием фильтров vpn в политике VPN. Если команда **внутриинтерфейса разрешения той-же-безопасности** присутствует в конфигурации ASA, эта ситуация только происходит.
>
> Аналогично, если внутренние хосты генерируют трафик, предназначенный к IP-адресу в пуле VPN, и тот IP-адрес не назначен на удаленного пользователя VPN, тот трафик мог бы выход за пределами ASA в открытом тексте.