Сообщения поддержки активности туннеля с общей инкапсуляцией маршрутов (GRE)

Содержание

Введение

Этот документ объясняет, что пакеты Keepalive Универсальной инкапсуляции маршрутизации (GRE) и как они работают.

> **Примечание:** Сообщения поддержки активности GRE не поддерживаются вместе с защитой Туннеля IPSec ни при каких обстоятельствах. Этот документ обсуждает эту проблему.

Туннели GRE

Туннель GRE — это расположенный на маршрутизаторе Cisco логический интерфейс, который предоставляет механизм для инкапсулирования пакетов, переносимых внутри транспортного протокола (passenger packet). Это - архитектура, разработанная для предоставления сервисов для реализации схемы инкапсуляции соединения типа точка-точка.

Функциональность туннелей GRE не зависит от состояния. Это значит, что конечная точка каждого туннеля не хранит никаких данных о состоянии или доступности другой удаленной конечной точки этого туннеля. Вследствие этого маршрутизатор локальной конечной точки туннеля не в состоянии отключить линейный протокол интерфейса туннеля GRE, если удаленный конец туннеля недоступен. Возможность помечать интерфейс, как отключенный, когда удаленный конец соединения недоступен, используется для удаления маршрутов (а именно, статических маршрутов) в таблице маршрутизации, которая используется интерфейсом исходящей связи. В частности, если линейный протокол интерфейса отключается, то любые статические маршруты, которые указывают на этот интерфейс,

удаляются из таблицы маршрутизации. Это обеспечивает установку альтернативного (плавание) статический маршрут или для Маршрутизации на основе политик (PBR) для выбора альтернативного следующего перехода или интерфейса.

Обычно интерфейс туннеля GRE включается сразу после настройки и остается активным до тех пор, пока имеется действительный адрес источника туннеля или интерфейс в активном состоянии. IP-адрес назначения туннеля также должен быть доступным для маршрутизации. Это обязательно даже в том случае, если не задана конфигурация для другого конца туннеля. Это означает, что статический маршрут или PBR-пересылка пакетов через интерфейс туннеля GRE работает даже в том случае, если пакеты туннеля GRE не достигают другого конца туннеля.

Прежде чем сообщения поддержки активности GRE были внедрены, были только способы определить локальные проблемы на маршрутизаторе и никаком способе определить проблемы в промежуточной сети. Например, случай, в котором туннельные пакеты GRE успешно переданы, но потеряны, прежде чем они достигнут другого конца туннеля. Такие сценарии вызвали бы пакеты данных, которые проходят Туннель GRE, чтобы быть "черные перфорируемый", даже при том, что альтернативный маршрут, который использует PBR или плавающий статический маршрут через другой интерфейс, мог бы быть доступным. Сообщения поддержки активности в интерфейсе туннеля GRE используются для того, чтобы решить проблему аналогично тому, как сообщения используются на физических интерфейсах.

Принципы работы сообщений поддержки активности туннеля

Механизм поддержки активности Туннеля GRE подобен сообщениям проверки активности PPP, в которых он дает способность к одной стороне, чтобы инициировать и получить пакеты keepalive к и от удаленного маршрутизатора, даже если удаленный маршрутизатор не поддерживает сообщения поддержки активности GRE. Поскольку GRE является механизмом туннелирования пакетов для IP-туннелирования внутри IP-протокола, пакет IP-туннеля GRE может быть создан внутри другого пакета IP-туннеля GRE. Для сообщений поддержки активности GRE отправитель предварительно создает пакет ответа на сообщение поддержки активности в исходном keepalive пакете запроса так, чтобы удаленный конец только сделал стандартное расформирование GRE внешнего IP - заголовка GRE и затем вернуться внутренний пакет GRE IP к отправителю. На примере ниже представлены концепции IP-туннелирования, где GRE — протокол инкапсуляции, а IP — транспортный протокол. Инкапсулируемый протокол является также IP (невзирая на то, что это может быть другой протокол как Decnet, Межсетевой пакетный обмен (IPX) или AppleTalk).

Стандартный пакет:

IP - заголовок	Заголовок TCP	Telnet

Туннелируемый пакет:

IP - заголовок	GRE	IP - заголовок	Заголовок TCP	Telnet

- IP является транспортным протоколом.

- GRE является протоколом инкапсуляции.
- IP является протоколом переноса.

Вот пример пакета keepalive, который происходит из маршрутизатора A и предназначен для маршрутизатора B. Ответ на сообщение поддержки активности, который маршрутизатор B возвращает к маршрутизатору A, уже во Внутреннем IP - заголовке. Маршрутизатор Router B просто декапсулирует пакеты поддержки активности и отправляет их обратно на физический интерфейс (S2). Тот, в свою очередь, обрабатывает пакеты поддержки активности GRE подобно любым другим IP-пакетам данных GRE.

Сообщения поддержки активности GRE:

IP - заголовок GRE		GRE	IP - заголовок		GRE
Источник A	Назначение Б.	PT=IP	Источник B	Назначение A.	PT=0

Из-за особенностей данного механизма ответные сообщения поддержки активности передаются не по туннельному, а по физическому интерфейсу. Это означает, что на ответный пакет сообщения поддержки активности GRE не влияют никакие **функции обработки исходящих данных** на туннельном интерфейсе, такие как 'tunnel protection...', QoS, Виртуальная маршрутизация и Передача (VRF), и т.д.

> **Примечание:** Если Контрольный список входящего доступа (ACL) на Туннельном интерфейсе GRE настроен, то пакет keepalive Туннеля GRE, который должны быть разрешены противоположные передачи устройства. В противном случае Туннель GRE противоположного устройства не работает. (`gre <number> access-list < > < >`)

Другой атрибут пакетов Keepalive Туннеля GRE - то, что таймеры поддержки активности на каждой стороне независимы и не должны совпадать, подобный сообщениям проверки активности PPP.

> **Совет:** Проблема конфигурации сообщений поддержки активности на одной стороне туннеля заключается в том, что только один маршрутизатор, у которого настроены сообщения поддержки активности, помечает свой туннельный интерфейс как отключенный, если время ожидания счетчика сообщений поддержки активности истекло. Интерфейс туннеля GRE на другой стороне, где отсутствует конфигурация сообщений поддержки активности, остается активным, даже если другая сторона туннеля отключена. Туннель может стать черной дырой для пакетов, направленных в туннель стороной, не имеющей конфигурации сообщений поддержки активности.

> **Совет:** В большой сети туннелей GRE с топологией "звезда" следует выполнить только настройку конфигурации сообщений поддержки активности на стороне оконечных устройств, но не стороне концентратора. В большинстве случаев для оконечных устройств более важна возможность определять недостижимость концентратора и переключаться на резервный путь (например, для резервирования соединений).

Сообщения поддержки активности туннеля с общей инкапсуляцией маршрутов (GRE)

В ПО Cisco IOS® версии 12.2(8)T можно задавать конфигурацию сообщений поддержки активности в интерфейсе туннеля GRE типа "точка-точка". Это изменение, в свою очередь, позволяет динамически отключать интерфейс, если сообщения поддержки активности отсутствуют в течение некоторого периода времени.

Для получения дополнительной информации о том, как другие формы пакетов Keepalive работают, ссылаются на Обзор Механизмов поддержки активности на Cisco IOS.

> **Примечание:** Пакеты Keepalive туннеля GRE только поддерживаются на Туннелях GRE "точка-точка". Сообщения поддержки активности туннеля могут быть настроены на многоточечных туннелях GRE (mGRE), однако это не даст ощутимого эффекта.

> **Примечание:** В целом проверки подлинности туннеля не будут работать, когда VRF будут использоваться на туннельном интерфейсе и FVRF (‘tunnel vrf...’), и iVRF (‘ip vrf forwarding...’ на туннельном интерфейсе) не совпадают. Это важно на оконечной точке туннеля, которая "отражает" поддержку активности назад к запрашивающей стороне. Когда запрос поддержки активности получен, он получен в FVRF и декапсулирован. Это показывает предварительно изготовленный ответ поддержки активности, который тогда должен быть передан назад отправителю, BUT, что передача находится в контексте iVRF на туннельном интерфейсе. Поэтому, если iVRF и FVRF не совпадают тогда, пакет ответа поддержки активности не передан назад отправителю. Это истинно даже при замене iVRF и/или FVRF с "глобальным".

Ниже показаны выходные данные команд, используемых для конфигурации сообщений поддержки активности в туннелях GRE.

```
Router# configure terminal
Router(config)#interface tunnel0
Router(config-if)#keepalive 5 4

!--- The syntax of this command is keepalive [seconds [retries]].


!--- Keepalives are sent every 5 seconds and 4 retries.
!--- Keepalives must be missed before the tunnel is shut down.
!--- The default values are 10 seconds for the interval and 3 retries.
```

Для более полного понимания общих механизмов функционирования сообщений поддержки активности GRE ниже рассматриваются пример туннельной топологии и конфигурации:

Маршрутизатор A

```
Router# configure terminal
Router(config)#interface tunnel0
Router(config-if)#keepalive 5 4

!--- The syntax of this command is keepalive [seconds [retries]].



!--- Keepalives are sent every 5 seconds and 4 retries.
!--- Keepalives must be missed before the tunnel is shut down.
!--- The default values are 10 seconds for the interval and 3 retries.
```

Маршрутизатор B

```
Router# configure terminal
Router(config)#interface tunnel0
Router(config-if)#keepalive 5 4

!--- The syntax of this command is keepalive [seconds [retries]].



!--- Keepalives are sent every 5 seconds and 4 retries.
!--- Keepalives must be missed before the tunnel is shut down.
!--- The default values are 10 seconds for the interval and 3 retries.
```

В этом сценарии маршрутизатор A выполняет эти шаги:

1. Создает внутренний IP - заголовок каждые пять секунд где:

   источник установлен как локальная переменная назначение туннеля, которое является 192.168.1.2назначение установлено как локальная точка начала туннеля, которая является 192.168.1.1

   и заголовок GRE добавлен с Типом протокола (PT) 0

   Пакет, генерируемый маршрутизатором A, но не передаваемый:

2. Передает тот пакет из его туннельного интерфейса, который приводит к инкапсуляции пакета с внешним IP - заголовком где:

   источник установлен как локальная переменная точка начала туннеля, которая является 192.168.1.1назначение установлено как локальное назначение туннеля, которое является 192.168.1.2

   и заголовок GRE добавлен с PT = IP.

   Пакет, переданный от маршрутизатора A до маршрутизатора B:

3. Инкрементно увеличивает счетчик проверки подлинности туннеля одним.

4. Учитывая, что существует способ достигнуть оконечной точки туннеля дальнего конца,

и линейный туннельный протокол не не работает из-за других причин, пакет поступает в маршрутизатор B. С этим тогда совпадают против Туннеля 0, становится декапсулированным, и передано IP - адресу назначения, который является IP-адресом точки начала туннеля на маршрутизаторе A.

Передаваемый от маршрутизатора B до маршрутизатора A:

5. По прибытию в маршрутизатор A пакет становится декапсулированным и проверка результатов PT в 0. Это показывает, что это - пакет keepalive. Происходит сброс значения счетчика сообщений проверки активности на 0 и пакет отбрасывается.

Если маршрутизатор B недостижим, маршрутизатор A продолжает создавать и передавать пакеты keepalive, а также обычный трафик. Если пакеты Keepalive не возвращаются, линейный туннельный протокол не ложится спать, пока счетчик проверки подлинности туннеля является меньше, чем количество повторных попыток, которое в этом случае равняется четырем. Если данное условие не соблюдено, то в следующий раз при попытке маршрутизатора Router A отправить пакет поддержки активности маршрутизатору Router B, линейный протокол отключается.

Примечание: Во включенном или выключенном состоянии туннель не передает и не обрабатывает какой-либо трафик данных. Однако он продолжает отправлять пакеты поддержки активности. При получении ответов сообщений поддержки активности, означающих доступность конечной точки туннеля, счетчик сообщений поддержки активности сбрасывается на 0, а линейный протокол в туннеле активируется.

Для наблюдения пакетов Keepalive в действии включите **туннель отладки** и **отладьте проверку подлинности туннеля**.

Примеры отладки от маршрутизатора A:

```
debug tunnel keepalive
Tunnel keepalive debugging is on
01:19:16.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=15
01:19:21.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=16
01:19:26.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=17
```

Сообщения поддержки активности GRE и одноадресная пересылка по обратному пути

RPF индивидуальной рассылки (Одноадресная пересылка по обратному пути) является характеристикой безопасности, которая помогает обнаруживать и отбрасывать имитировавший IP - трафик с проверкой адреса источника пакетов против таблицы маршрутизации. Когда RPF Индивидуальной рассылки выполнен в строгом режиме (**rx ip verify unicast source reachable-via**), пакет должен быть получен на интерфейсе, который маршрутизатор использовал бы для передачи возвращаемого пакета. Если строгий режим или свободный RPF Индивидуальной рассылки режима будут включены на туннельном интерфейсе маршрутизатора, который получает пакеты сообщения поддержки активности GRE, то пакеты пакетов Keepalive будут отброшены RPF после туннельной декапсуляции,

так как маршрут к адресу источника пакета (собственный адрес точки начала туннеля маршрутизатора) не через туннельный интерфейс. Отбрасывание пакета RPF может наблюдаться в **выходных данных show ip traffic** следующим образом:

```
Router#show ip traffic | section Drop
Drop: 0 encapsulation failed, 0 unresolved, 0 no adjacency
0 no route, 156 unicast RPF, 0 forced drop
0 options denied
```

В результате инициатор проверок подлинности туннеля переведет туннель в нерабочее состояние из-за пропущенных возвращаемых пакетов пакетов Keepalive. Таким образом, RPF Индивидуальной рассылки не должен быть настроен в строгом или свободном режиме для пакетов Keepalive Туннеля GRE для работы. Для получения дополнительной информации о RPF Индивидуальной рассылки, обратитесь к Пониманию Одноадресной пересылки по обратному пути.

IPsec и сообщения поддержки активности GRE

Туннели GRE с IPSec

В некоторых случаях туннели GRE совмещаются с IPSec, поскольку IPSec не поддерживает многоадресную рассылку IP-пакетов. Из-за этого протоколы динамической маршрутизации не могут работать успешно по сети IPsec VPN. Поскольку туннели GRE поддерживают многоадресную рассылку IP-пакетов, протокол динамической маршрутизации может быть реализован в туннеле GRE. Пакеты одноадресного IP - трафика GRE, что результат может быть зашифрован IPsec.

Существует два способа выполнения шифрования IPSec пакетов GRE:

- Один путь с использованием **криптокарты**. Криптокарта применяется к исходящему физическому интерфейсу (интерфейсам) для пакетов туннеля GRE. В этом случае последовательность шагов следующие:

  Зашифрованный пакет достигает физического интерфейса.Пакет дешифрован и передан к туннельному интерфейсу.Пакет декапсулирован и затем передан к IP - адресу назначения в открытом тексте.

- Другой путь состоит в том, чтобы использовать **tunnel protection**. **Если используется команда tunnel protection, она настраивается в интерфейсе туннеля GRE. Команда tunnel protection доступна в ПО Cisco IOS версии 12.2(13)T**. В этом случае последовательность шагов следующие:

  Зашифрованный пакет достигает физического интерфейса.Пакет передан к туннельному интерфейсу.Пакет дешифрован и декапсулирован и затем передан к IP - адресу назначения в открытом тексте.

Особенность обоих методов состоит в выполнении шифрования IPSec после добавления инкапсуляции GRE. Существуют два основных отличия в использовании криптокарты и команды защиты туннеля:

- Криптокарта IPSec привязана к физическому интерфейсу и проверяется при отправке из него пакетов.

Туннель GRE уже имеет GRE, инкапсулировал пакет этой точкой.
- Защита туннеля привязывает функцию шифрования к туннелю GRE; она проверяется после GRE-инкапсуляции пакета, но до того, как пакет передан на физический интерфейс.

Проблемы с сообщениями поддержки активности при совмещении IPSec и GRE

Учитывая эти два способа добавить шифрование к Туннелям GRE, существует три отдельных способа установить зашифрованный Туннель GRE:

1. В то время как Узлу B настроили криптокарту на физическом интерфейсе, узлу A настроили tunnel protection на туннельном интерфейсе.
2. В то время как Узлу B настроили tunnel protection на туннельном интерфейсе, узлу A настроили криптокарту на физическом интерфейсе.
3. Обоим Узлам настроили tunnel protection на туннельном интерфейсе.

Конфигурация, описанная в Сценариях 1 и 2, часто реализовывается в схеме звезды. Защита туннеля устанавливается на концентраторе-маршрутизаторе с целью уменьшения размера конфигурации, и статическая криптокарта используется на каждом их оконечных устройств.

Считайте каждый из этих сценариев с сообщениями поддержки активности GRE включенным на Узле B (луч) и где туннельный режим используется для шифрования.

Сценарий 1

Установка:

- Взаимодействуйте с Tunnel Protection использования.
- Взаимодействуйте с Криптокартами использования B.
- Пакеты Keepalive включены на Узле B.
- IP - безопасное шифрование сделано в туннельном режиме.

В этом сценарии, так как сообщения поддержки активности GRE настроены на Узле B, события последовательности, когда поддержка активности генерируется, следующие:

1. Узел B генерирует пакет keepalive, который является инкапсулировавшим GRE и затем переданным физическому интерфейсу, где это зашифровано и переслано к назначению туннеля, Узел A.

   Пакет, переданный от Узла B для Пиринга с A:

2. В Узле A, сообщение поддержки активности GRE получено дешифрованное:

   декапсулированный:

Затем внутренний ответный пакет сообщения поддержки активности GRE маршрутизируется на основе его адреса назначения (DA), который является Узлом B. Это означает на Узле A, пакет сразу поднят с постели назад физический интерфейс для Пиринга с B. Начиная с Узла tunnel protection использования на **туннельном интерфейсе** не зашифрован пакет keepalive.

Поэтому пакет, переданный от Узла для Пиринга с B:

Примечание: Поддержка активности не зашифрована.

3. Взаимодействуйте с B, теперь получает ответ сообщения поддержки активности GRE, который не зашифрован на его физическом интерфейсе, но из-за криптокарты, настроенной на физическом интерфейсе, это ожидает зашифрованный пакет и так отбрасывает его.

Поэтому даже при том, что Узел A отвечает на пакеты Keepalive и исходящий маршрутизатор, Узел B получает ответы, это никогда не обрабатывает их, и в конечном счете изменяет протокол линии связи туннельного интерфейса к нерабочему состоянию.

Результат:

Пакеты Keepalive включили на Узле B, заставляют состояние туннеля на Узле B изменяться на/вниз.

Сценарий 2

Установка:

- Взаимодействуйте с Криптокартами использования.
- Взаимодействуйте с Tunnel Protection использования B.
- Пакеты Keepalive включены на Узле B.
- IP - безопасное шифрование сделано в туннельном режиме.

В этом сценарии, так как сообщения поддержки активности GRE являются onfigured на Узле B, события последовательности, когда поддержка активности генерируется, следующие:

1. Узел B генерирует пакет keepalive, который является инкапсулировавшим GRE и затем зашифрованным tunnel protection на туннельном интерфейсе и затем переданным физическому интерфейсу.

   Пакет, переданный от Узла B для Пиринга с A:

2. В Узле A, сообщение поддержки активности GRE получено дешифрованное:

декапсулированный:

Затем внутренний ответный пакет сообщения поддержки активности GRE маршрутизируется на основе его адреса назначения (DA), который является Узлом B. Это означает на Узле A, пакет сразу поднят с постели назад физический интерфейс для Пиринга с B. Начиная с Узла криптокарты использования на **физическом интерфейсе**, это сначала зашифрует этот пакет перед ним вперед это на.

Поэтому пакет, переданный от Узла для Пиринга с B:

Примечание: Ответ на сообщение поддержки активности зашифрован.

3. Взаимодействуйте с B, теперь получает зашифрованный ответ сообщения поддержки активности GRE, назначение которого передано туннельному интерфейсу, где это дешифровано:

Так как Тип Protocal установлен в 0, Узел B знает, что это - ответ на сообщение поддержки активности и обрабатывает его как таковой.

Результат:

Пакеты Keepalive включили на Узле B, успешно определяют то, что состояние туннеля должно основываться на доступности назначения туннеля.

Ситуация 3

Установка:

- Оба Узла используют Tunnel Protection.
- Пакеты Keepalive включены на Узле B.
- IP - безопасное шифрование сделано в туннельном режиме.

Этот сценарий подобен Сценарию 1 в том, что, когда Узел A получает зашифрованную поддержку активности, это дешифрует и декапсулирует его. Однако, когда ответ передан, отступают, он не зашифрован начиная с Узла tunnel protection использования на **туннельном интерфейсе**. Таким образом Узел B отбрасывает незашифрованный ответ на сообщение поддержки активности и не обрабатывает его.

Результат:

Пакеты Keepalive включили на Узле B, заставляют состояние туннеля на Узле B изменяться на/вниз.

Обходной путь

В таких ситуациях, где пакеты GRE должны быть зашифрованы, существует три возможных решения:

1. **Используйте криптокарту на Узле A, tunnel protection на Узле B, и включите пакеты Keepalive на Узле B.**

   Так как данный тип конфигурации главным образом используется в осевых настройках и потому что в таких настройках для луча более важно знать о достижимости концентратора, решение состоит в том, чтобы использовать динамическую криптокарту на концентраторе (Узел A) и tunnel protection на луче (Узел B) и включить сообщения поддержки активности GRE на луче. Таким образом, невзирая на то, что Туннельный интерфейс GRE на концентраторе остается, сосед по маршруту и маршруты через туннель потеряны, и альтернативный маршрут может быть установлен. На луче факт, что туннельный интерфейс выключился, может инициировать его для внедрения интерфейса номеронабирателя и обратного вызова к концентратору (или другой маршрутизатор в концентраторе), затем установить новое соединение.

2. **Используйте что-то другое, чем сообщения поддержки активности GRE для определения доступности однорангового узла**.

   Если оба маршрутизатора настроены с tunnel protection, то пакеты Keepalive Туннеля GRE не могут использоваться ни в одном направлении. В этом случае единственная опция должна использовать протокол маршрутизации или другой механизм, такой как Service Assurance Agent, чтобы обнаружить, достижим ли узел или нет.

3. **Используйте криптокарты на Узле A и Узле B.**

   Если и маршрутизаторы настроены с криптокартами, проверки подлинности туннеля могут пройти в обоих направлениях и Туннельных интерфейсах GRE, может завершить работу или в или в оба направления и инициировать резервное подключение, которое будет сделано. Данный вариант обеспечивает наибольшую гибкость.

Дополнительные сведения

- RFC 1701, Общая инкапсуляция маршрутов (GRE)
- RFC 2890, Расширения GRE "ключ" и "порядковый номер"
- Поддержка рабочего состояния туннеля с общей инкапсуляцией маршрутов (GRE)
- Фрагментация IP и PMTUD
- Обзор механизмов поддержки активности на Cisco IOS
- Техническая поддержка - Cisco Systems