Сообщения поддержки активности туннеля с общей инкапсуляцией маршрутов (GRE)

Содержание

Введение

В данном документе содержится описание принципов работы сообщений поддержки активности (keepalive). В документации Сообщения поддержки активности туннеля общей инкапсуляции маршрутов (GRE) утверждается, что использование сообщений поддержки активности туннеля GRE совместно с командой **tunnel protection ipsec profile** не поддерживается. Данная проблема, а также один случай совместного использования, и является предметом обсуждения в данном документе.

Предварительные условия

Требования

Настоящий документ не предъявляет каких-либо специфических требований.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к устройству или какой-либо версии ПО.

Условные обозначения

Дополнительные сведения о применяемых в документе обозначениях см. в статье Условные обозначения, используемые в технической документации Cisco.

Механизм сообщений поддержки активности туннеля GRE

Туннели GRE

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 позволяет выбрать альтернативный следующий переход (участок) или интерфейс при установке альтернативного (плавающего) маршрута или при использовании маршрутизации на основе политик (PBR).

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.

До внедрения сообщений активности GRE туннель GRE отключался по трем причинам:

- Отсутствует маршрут, соответствующий адресу назначения туннеля.
- Отключен интерфейс, привязанный к источнику туннеля.
- Маршрут по адресу назначения туннеля проходит по данному туннелю.

Эти три правила (отсутствие маршрута, отключение интерфейса и несоответствие туннельного маршрута назначения) являются локальными проблемами маршрутизатора на конечных точках туннеля, и проблемы работоспособности промежуточных сетей ими не ограничиваются. Например, эти правила не объясняют случай, когда пакеты успешно передаются по туннелю GRE, но теряются до прихода на конечную точку туннеля. Из-за этого пакеты данных, проходящие через туннель GRE, попадают в "черные дыры", даже если альтернативный маршрут, использующий PBR, или плавающий статический маршрут через другой интерфейс потенциально доступен. Сообщения поддержки активности в интерфейсе туннеля GRE используются для того, чтобы решить проблему аналогично тому, как сообщения используются на физических интерфейсах.

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. В последующих разделах общие механизмы функционирования сообщений поддержки активности GRE рассматриваются более подробно.

Общие механизмы сообщений поддержки активности

Сообщения поддержки активности отправляются сетевым устройством по физическому или виртуальному каналу связи для информирования другого сетевого устройства о том, что канал связи между ними сохраняет работоспособность. Интервалы сообщений поддержки активности — это период времени от отправки устройством сообщения поддержки активности до отправки следующего сообщения тем же сетевым устройством. Повторы сообщений поддержки активности — это количество отправленных устройством сообщений, на которых не последовало ответа до выключения интерфейса.

Сообщения поддержки активности Ethernet

В широковещательной среде, такой как Ethernet, сообщения поддержки активности немного отличаются. Поскольку количество возможных соседей в Ethernet велико, сообщения поддержки активности не предусматривают определения доступности пути по кабелю к какому-то определенному соседу. Данные сообщения позволяют только выполнить проверку доступа локальной системы к кабелю Ethernet для чтения и записи. Маршрутизатор создает Ethernet-пакет, который содержит MAC-адрес источника и назначения самого маршрутизатора и специальный код Ethernet, равный 0x9000. Оборудование Ethernet отправляет этот пакет по кабелю Ethernet и затем немедленно получает этот пакет обратно. Таким образом, выполняется проверка аппаратных средств приема и передачи в адаптере Ethernet, а также проверка целостности кабеля.

Source MAC	Destination MAC	Protocol Type	Data	Layer-2 Padding
00-00-0C-04-EF-04	00-00-0C-04-EF-04	9000	0000 0100	0000 ... 0000

Сообщения поддержки активности HDLC

Другой хорошо известный механизм сообщений поддержки активности — серийные сообщения для HDLC. Серийные сообщения поддержки активности пересылаются от одного маршрутизатора к другому (и обратно) и подтверждаются. Каждый маршрутизатор отслеживает отправленные и подтвержденные пакеты поддержки активности с помощью последовательных номеров. Таким образом, удаленные маршрутизаторы могут проанализировать сообщения поддержки активности друг друга и определить, получены ли отправленные сообщения.

На рисунке показано, как работают серийные сообщения поддержки активности: маршрутизатор 1 (Router 1) и маршрутизатор 2 (Router 2) подключены напрямую через интерфейсы Serial0/0 и Serial2/0, соответственно. В выходных данных маршрутизатора Router 1 интерфейс Serial 0/0 отключен намеренно. Это вынуждает маршрутизатор Router 2 пропустить три сообщения поддержки активности, для того, чтобы показать, как вследствие этой ошибки маршрутизатор Router 2 отключает интерфейс Serial2/0, если не поступают сообщения поддержки активности.

Здесь приведен пример выходных данных команды **debug serial interface** для соединения HDLC, когда сообщения поддержки активности включены. Когда разность значений в полях myseq и mineseen на маршрутизаторе Router 2 превышает 3, линия отключается и интерфейс перезагружается.

Маршрутизатор Router 1

```
17:21:09.685: Serial0/0: HDLC myseq 0, mineseen 0*, yourseen 1, line up
17:21:19.725: Serial0/0: HDLC myseq 1, mineseen 1*, yourseen 2, line up
17:21:29.753: Serial0/0: HDLC myseq 2, mineseen 2*, yourseen 3, line up
17:21:39.773: Serial0/0: HDLC myseq 3, mineseen 3*, yourseen 4, line up
17:21:49.805: Serial0/0: HDLC myseq 4, mineseen 4*, yourseen 5, line up
17:21:59.837: Serial0/0: HDLC myseq 5, mineseen 5*, yourseen 6, line up
17:22:09.865: Serial0/0: HDLC myseq 6, mineseen 6*, yourseen 7, line up
17:22:19.905: Serial0/0: HDLC myseq 7, mineseen 7*, yourseen 8, line up
17:22:29.945: Serial0/0: HDLC myseq 8, mineseen 8*, yourseen 9, line up
Router1 (config-if)#shut
17:22:39.965: Serial0/0: HDLC myseq 9, mineseen 9*, yourseen 10, line up
17:22:42.225: %LINK-5-CHANGED: Interface Serial0/0, changed state
to administratively down

17:22:43.245: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to down
```

Маршрутизатор Router 2

```
*Sep 24 17:21:04.929: Serial2/0: HDLC myseq 0, mineseen 0, yourseen 0, line up
*Sep 24 17:21:14.941: Serial2/0: HDLC myseq 1, mineseen 1*, yourseen 1, line up
*Sep 24 17:21:24.961: Serial2/0: HDLC myseq 2, mineseen 2*, yourseen 2, line up
*Sep 24 17:21:34.981: Serial2/0: HDLC myseq 3, mineseen 3*, yourseen 3, line up
*Sep 24 17:21:45.001: Serial2/0: HDLC myseq 4, mineseen 4*, yourseen 4, line up
*Sep 24 17:21:55.021: Serial2/0: HDLC myseq 5, mineseen 5*, yourseen 5, line up
*Sep 24 17:22:05.041: Serial2/0: HDLC myseq 6, mineseen 6*, yourseen 6, line up
*Sep 24 17:22:15.061: Serial2/0: HDLC myseq 7, mineseen 7*, yourseen 7, line up
*Sep 24 17:22:25.081: Serial2/0: HDLC myseq 8, mineseen 8*, yourseen 8, line up
*Sep 24 17:22:35.101: Serial2/0: HDLC myseq 9, mineseen 9*, yourseen 9, line up
*Sep 24 17:22:45.113: Serial2/0: HDLC myseq 10, mineseen 10*, yourseen 10, line up
*Sep 24 17:22:55.133: Serial2/0: HDLC myseq 11, mineseen 10, yourseen 10, line up
*Sep 24 17:23:05.153: HD(0): Reset from 0x203758
*Sep 24 17:23:05.153: HD(0): Asserting DTR
*Sep 24 17:23:05.153: HD(0): Asserting DTR and RTS
*Sep 24 17:23:05.153: Serial2/0: HDLC myseq 12, mineseen 10, yourseen 10, line up
*Sep 24 17:23:15.173: HD(0): Reset from 0x203758
*Sep 24 17:23:15.173: HD(0): Asserting DTR
*Sep 24 17:23:15.173: HD(0): Asserting DTR and RTS
*Sep 24 17:23:15.173: Serial2/0: HDLC myseq 13, mineseen 10, yourseen 10, line down
17:23:16.201: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0,
changed state to down
```

```
Router2#
17:23:25.193: Serial2/0: HDLC myseq 14, mineseen 10, yourseen 10, line down
```

Сообщения поддержки активности туннеля с общей инкапсуляцией маршрутов (GRE)

Механизм сообщений поддержки активности туннеля GRE немного отличается от механизма Ethernet или последовательных интерфейсов. Он позволяет одной из сторон отправлять пакеты поддержки активности удаленному маршрутизатору и получать их от него даже в том случае, 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 ответный пакет внутри исходного пакета-запроса сообщения поддержки активности, таким образом, удаленной стороне необходимо только выполнить стандартную декапсуляцию GRE внешнего IP-заголовка GRE и затем передать внутренний IP-пакет GRE. Из-за особенностей данного механизма ответные сообщения поддержки активности передаются не по туннельному, а по физическому интерфейсу. Это означает, что функции на выходе туннельного интерфейса, такие как "защита туннеля ...", качество обслуживания (QoS) и так далее, не оказывают влияния на ответный пакет поддержки активности GRE. Если имеется ACL входящего трафика в интерфейсе туннеля GRE, в нем должно быть разрешены пакеты поддержки активности туннеля GRE (`access-list <number> permit gre host <tunnel-source> host <tunnel-destination>`).

Другой атрибут сообщений поддержки активности туннеля GRE — независимость счетчиков сообщений поддержки активности и отсутствие необходимости их соответствия друг другу. 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. 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).

Принципы работы сообщений поддержки активности туннеля

Туннель GRE — это расположенный на маршрутизаторе Cisco логический интерфейс, который предоставляет механизм для инкапсулирования пакетов, переносимых внутри транспортного протокола (passenger packet). Данный механизм предоставляет службы, которые позволяют реализовать схему инкапсуляции "точка-точка".

На примере ниже представлены концепции IP-туннелирования, где GRE — протокол инкапсуляции, а IP — транспортный протокол. Протокол переноса также является IP-протоколом (однако он может быть другим протоколом, например Decnet, IPX или Appletalk).

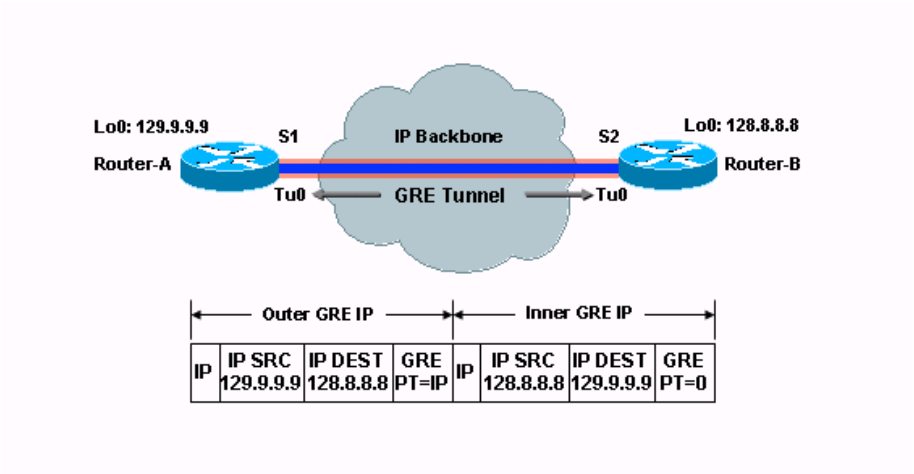
Normal Packet

Tunnel Packet

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

Для более полного понимания общих механизмов функционирования сообщений поддержки активности GRE ниже рассматриваются пример туннельной топологии и конфигурации. Физические интерфейсы маршрутизаторов Router A и Router B обозначены соответственно как S1 и S2, туннельные интерфейсы обозначены Tu0. Имеется магистральная IP-сеть между двумя конечными маршрутизаторами туннеля GRE.

Это пример пакета поддержки активности, который отправлен из маршрутизатора Router A и назначен маршрутизатору Router B. Ответ на сообщение поддержки активности, который маршрутизатор Router B возвращает маршрутизатору Router A, уже находится 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.



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
!--- Синтаксис данной команды keepalive [секунды [повторы]].


!--- Сообщения поддержки активности отправляются каждые 5 секунд и 4 секунды.
!--- Сообщения поддержки активности должны отсутствовать перед отключением туннеля.
!--- По умолчанию интервал ожидания равен 10 секундам, а количество повторов — 3.
```

Примечание. Сообщения поддержки активности туннеля GRE поддерживаются только в туннелях GRE типа "точка-точка". Сообщения поддержки активности туннеля могут быть настроены на многоточечных туннелях GRE (mGRE), однако это не даст ощутимого эффекта.

В таблице показана конфигурация маршрутизаторов Router A и Router B, на каждом из которых присутствует конфигурация **сообщений поддержки активности туннеля**.

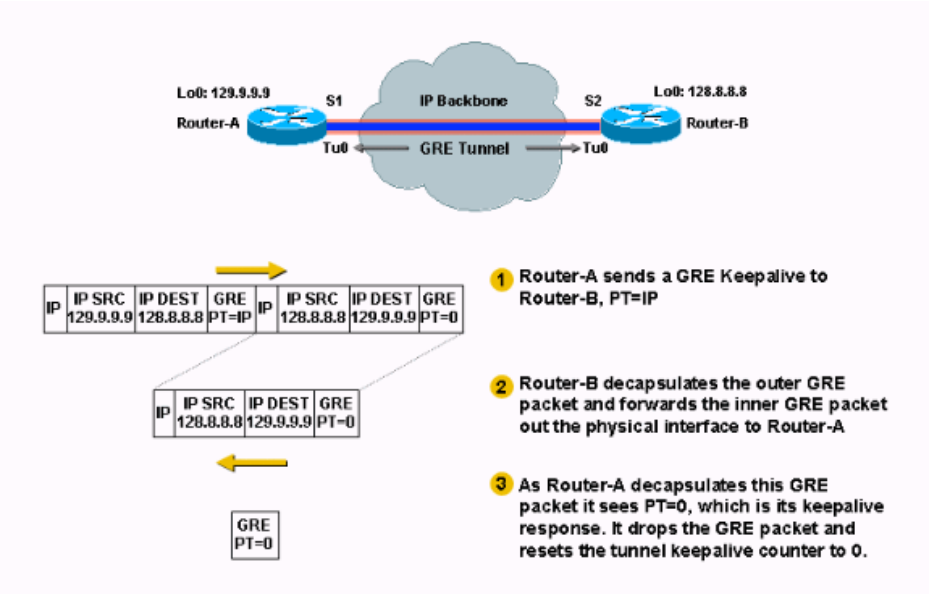
Имя хоста маршрутизатора Router-A	Имя хоста маршрутизатора Router-B
interface loopback 0 ip address 129.9.9.9 255.255.255.255 interface tunnel 0 ip address 1.1.1.1 255.255.255.240 tunnel source loopback0 tunnel destination 128.8.8.8 keepalive 5 4	interface loopback 0 ip address 128.8.8.8 255.255.255.255 interface tunnel 0 ip address 1.1.1.2 255.255.255.240 tunnel source loopback0 tunnel destination 129.9.9.9 keepalive 5 4

Если сообщения поддержки активности на конечной точке туннеля маршрутизатора Router A включены, маршрутизатор в каждом интервале <период> создает внутренний IP-заголовок и заголовок GRE с нулевым типом протокола (PT). Затем он отправляет этот пакет туннельному интерфейсу, в результате чего происходит инкапсуляция пакета с внешним IP-заголовком и заголовком GRE с PT, равным IP. Маршрутизатор Router A увеличивает значение счетчика сообщений поддержки активности туннеля на единицу. Если предположить, что способ достижения конечной точки туннеля на дальнем конце существует, а линейный туннельный протокол по каким-то причинам не отключен, то пакет поступает на маршрутизатор Router B. Затем он сопоставляется с туннелем 0, декапсулируется и направляется по IP-адресу назначения, который является IP-адресом источника туннеля на маршрутизаторе Router A. Когда пакет поступает на маршрутизатор Router A, он декапсулируется, и проверка PT дает в результате 0. Это означает, что данный пакет является пакетом поддержки активности. Происходит сброс значения счетчика сообщений проверки активности на 0 и пакет

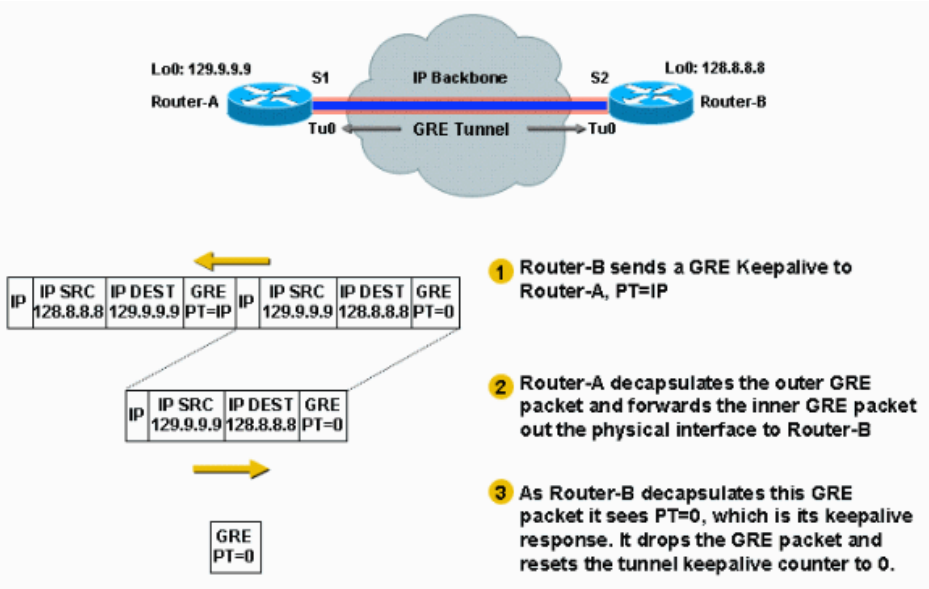
отбрасывается.

В случае если маршрутизатор Router B недоступен, маршрутизатор Router A продолжает создавать и отправлять пакеты поддержки активности, а также обычный трафик. Если сообщение поддержки активности не возвращается, линейный протокол туннеля остается включенным до тех пор, пока значение счетчика сообщений поддержки активности меньше, чем число <попыток>. Если данное условие не соблюдено, то в следующий раз при попытке маршрутизатора Router A отправить пакет поддержки активности маршрутизатору Router B, линейный протокол отключается.

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. На схеме показан пример сценария, когда маршрутизатор Router A отправляет сообщения поддержки активности GRE маршрутизатору Router B:



На схеме показан пример сценария, когда маршрутизатор Router B отправляет сообщения поддержки активности GRE маршрутизатору Router A:



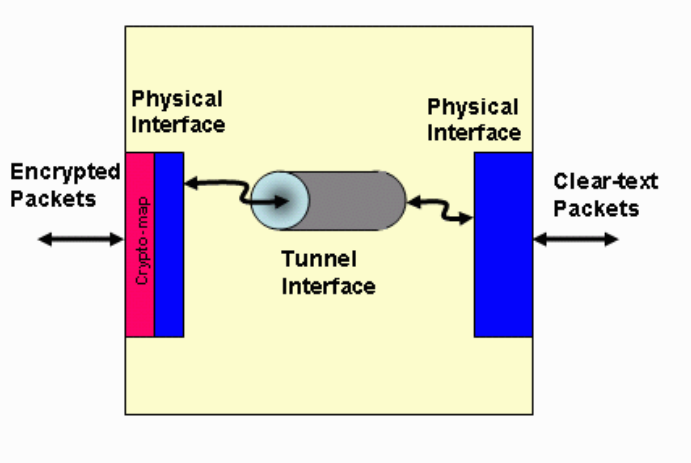
IPsec и сообщения поддержки активности GRE

Туннели GRE с IPSec

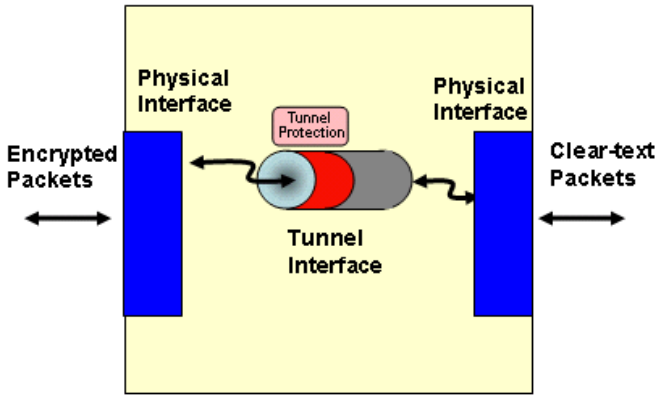
В некоторых случаях туннели GRE совмещаются с IPSec, поскольку IPSec не поддерживает многоадресную рассылку IP-пакетов. Это не позволяет протоколам динамической маршрутизации успешно работать в сетях VPN IPSec. Поскольку туннели GRE поддерживают многоадресную рассылку IP-пакетов, протокол динамической маршрутизации может быть реализован в туннеле GRE. Соответственно, для IP-пакетов одноадресной рассылки GRE может применяться шифрование IPSec.

Существует два способа выполнения шифрования IPSec пакетов GRE. Один из них заключается в использовании **криптокарты**, другой — в использовании команды **tunnel protection**. Особенность обоих методов состоит в выполнении шифрования IPSec после добавления инкапсуляции GRE. Криптокарта применяется к исходящему физическому интерфейсу (интерфейсам) для пакетов туннеля GRE. Если используется команда **tunnel protection**, она настраивается в интерфейсе туннеля GRE. Команда **tunnel protection** доступна в ПО Cisco IOS версии 12.2(13)T.

На данной схеме показаны зашифрованные пакеты, поступившие на маршрутизатор через интерфейс туннеля GRE. Маршрутизатор имеет криптокарту, которая применяется на физическом интерфейсе. Дешифрованные и декапсулированные пакеты передаются по IP-адресу назначения как открытый (незашифрованный) текст.



На следующей схеме показан случай применения команды **tunnel protection** на интерфейсе туннеля GRE. Пакеты поступают через интерфейс туннеля на маршрутизатор зашифрованными, дешифруются и декапсулируются, а затем передаются по IP-адресу назначения как открытый (незашифрованный) текст.



Существуют два основных отличия в использовании криптокарты и команды защиты туннеля:

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

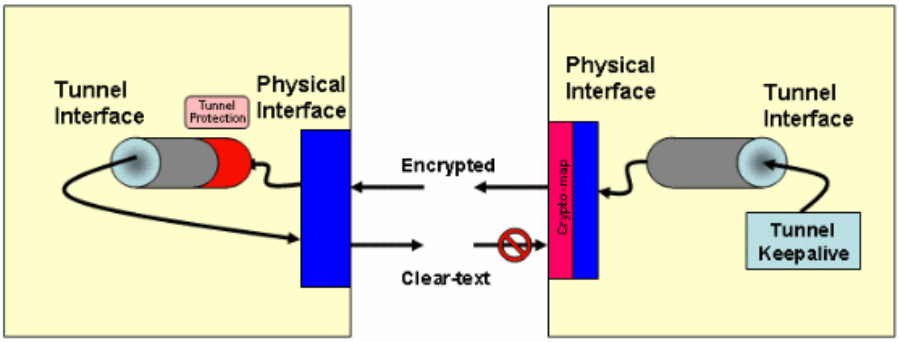
  Примечание. В туннеле GRE к этому моменту уже имеется GRE-инкапсулированный пакет.

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

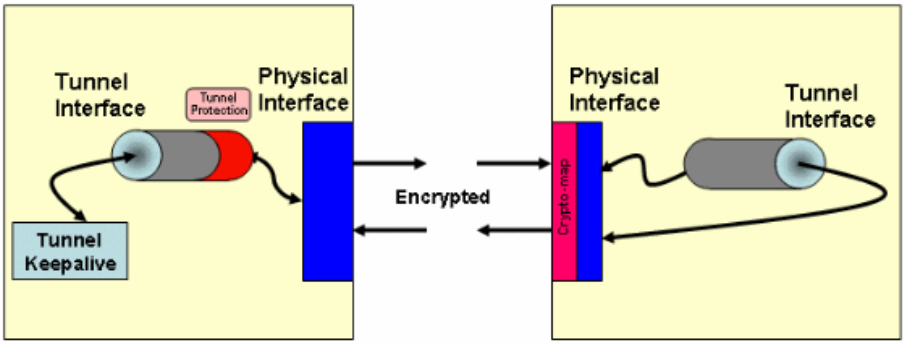
Проблемы с сообщениями поддержки активности при совмещении IPSec и GRE

Проблема возникает, если используется криптокарта (настроенная в физическом интерфейсе) на одной стороне туннеля GRE IPSec, а защита туннеля установлена на другой стороне. При этом конфигурация защиты туннеля присутствует только в интерфейсе (не физическом) туннеля. Такой тип конфигурации может быть установлен в топологии типа "звезда". Защита туннеля устанавливается на концентраторе-маршрутизаторе с целью уменьшения размера конфигурации, и статическая криптокарта используется на каждом их оконечных устройств. Если выполнить настройку сообщений поддержки активности туннеля GRE на оконечном устройстве в данном сценарии, передача этих сообщений не выполняется. Причина заключается в том, что ответное сообщение поддержки активности от КОНЦЕНТРАТОРА проходит через физический интерфейс, в котором криптокарта не настроена. Поэтому ответное сообщение поддержки активности не шифруется и принимающий маршрутизатор (который отправил данный пакет) отбрасывает ответные сообщения, так как они не имеют защиты IPSec (незашифрованы).

Представленная схема иллюстрирует данную проблему:



Этой проблемы можно избежать, если настроить сообщения поддержки активности GRE на маршрутизаторе с установленной защитой туннеля. Это показано на следующей схеме:



Если на концентраторе используются динамические криптокарты, а на оконечных устройствах — защита туннеля, следует настроить сообщения поддержки активности GRE на оконечном маршрутизаторе для запуска резервного интерфейса и выполнения вызова концентратора при отключении интерфейса туннеля на оконечном устройстве.

Хотя интерфейс туннеля GRE на концентраторе остается активным, соседи по маршрутам и сами маршруты потеряны, а установка альтернативных маршрутов невозможна. Отключение туннельного интерфейса может запустить на оконечном устройстве интерфейс номеронабирателя, после чего будет выполнен вызов концентратора (или другого маршрутизатора в концентраторе) и установлено новое соединение.

Если на обоих маршрутизаторах установлены криптокарты, сообщения поддержки активности туннеля будут проходить в обоих направлениях, а интерфейсы туннеля GRE смогут отключаться для одного или обоих направлений, таким образом, делая возможным запуск резервного соединения. Данный вариант обеспечивает наибольшую гибкость.

Дополнительные сведения

- **RFC 1701, Общая инкапсуляция маршрутов (GRE)**
- **RFC 2890, Расширения GRE "ключ" и "порядковый номер"**
- **Сообщения поддержки активности туннеля с общей инкапсуляцией маршрутов (GRE)**
- **Фрагментация IP и PMTUD**
- **Техническая поддержка — Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/10/107704/gre-tunnel-keepalive.shtml