Динамические многоточечные виртуальные частные сети IPSec (с применением протокола GRE/NHRP для масштабирования сети VPN IPSec)

Содержание

Введение

В документе описаны динамические многоточечные виртуальные частные сети IPSec (DMVPN) и причины, побуждающие компании проектировать или переходить на новое решение IPsec VPN в ПО Cisco IOS® .

Общие сведения

При шифровании трафика для его защиты компаниям бывает нужно связывать много узлов с основным узлом, а также друг с другом, через Интернет. Например, системе розничной продажи, которой нужно подключиться к штаб-квартире компании для инвентаризации и подачи заказов, может также потребоваться подключение к другим магазинам компании, чтобы проверить наличие продукта. Раньше единственным способом установить соединение было использование сети уровня 2, такой как ISDN или Frame Relay, для объединения всех компонентов. Настройка и себестоимость этих жестко проложенных каналов для внутреннего IP-трафика может быть трудоемка и дорога. Если все узлы (включая основной) уже имеют доступ к недорогому Интернет-трафику, его можно использовать для передачи внутреннего IP-трафика между магазинами и головным офисом с применением туннелей IPsec для обеспечения конфиденциальности и целостности данных.

Для построения больших сетей IPsec с взаимодействием узлов через Интернет для различных компаний, нужна возможность масштабирования сети IPsec. IPsec шифрует трафик между двумя адресуемыми конечными точками вызова, и шифрование выполняется между этими двумя конечными точками с использованием общего "секрета". Так как секрет разделен только между этими двумя конечными точками, шифрованные сети изначально являются набором каналов связи "точка-точка". Поэтому IPsec, в сущности, является туннельной сетью "точка-точка". Наиболее подходящим способом является масштабирование больших сетей "точка-точка" для организации их в сеть с топологией "звезда" или полную (частичную) объединенную сеть. В большинстве сетей почти весь трафик IP приходится на обмен данными между оконечными узлами и концентратором, и лишь самая малая его часть - на трафик между самими оконечными узлами, поэтому звездообразная топология, как правило, оказывается оптимальным вариантом. Кроме того, такая архитектура соответствует топологии старых сетей Frame Relay, в которых ее применение объяснялось запретительно высокой стоимостью установки прямых линий между всеми узлами сетей.

При использовании Интернета в качестве посредника между концентратором и лучами, лучи также имеют прямой доступ друг к другу без дополнительных материальных затрат, но до настоящего времени было практически невозможно установить и/или управлять полной (частичной) объединенной сетью. Сети с полностью или частично ячеистой структурой часто являются более предпочтительными, так как в них могут быть применены методы сбережения стоимости если трафик между двумя оконечными устройствами можно передать напрямую, а не через концентратор. Трафик между двумя лучами, проходящий через концентратор, использует ресурсы концентратора и может вызвать дополнительную задержку, особенно при использовании шифрования IPsec, т.к. концентратору придется расшифровывать приходящие пакеты от посылающих лучей, а затем вновь шифровать трафик для передачи его на получающий луч. Еще один пример, где полезен прямой трафик между лучами, - случай, когда два конца луча находятся в одном городе, а концентратор – на другом конце страны.

Из-за развертывания и увеличения в размерах звездообразных сетей IPsec все чаще возникает необходимость в максимально динамичной маршрутизации IP-пакетов. В старых звездообразных сетях Frame Relay это достигалось с помощью протоколов динамической маршрутизации, таких как OSPF или EIGRP, работающих через каналы Frame Relay. Это

использовалось для динамического объявления доступности оконечных сетей и обеспечения резервирования сетей с IP-маршрутизацией. Если в сети потерян центральный маршрутизатор, резервный центральный маршрутизатор может автоматически занять его место, чтобы сохранить сетевые подключения к сетям-лучам.

Это основная проблема с туннелями IPsec и протоколами динамической маршрутизации. Протоколы динамической маршрутизации рассчитаны на использование многоадресных или широковещательных пакетов, но IPsec не поддерживает шифрование этих пакетов. Текущим способом для решения этой проблемы является использование туннелей общей маршрутной инкапсуляции GRE в комбинации с шифрованием IPsec.

Туннели GRE поддерживают передачу многоадресных и широковещательных IP-пакетов на другой конец туннеля GRE. Туннельный пакет GRE представляет собой однонаправленный пакет IP, поэтому пакет GRE может шифроваться посредством IPsec. В этом сценарии для поддержки сети VPN GRE выполняет туннелирование, а IPsec - шифрование. **Когда туннели GRE настроены, IP-адреса для конечных точек туннеля (tunnel source ..., tunnel destination ...) должны быть известны на другом конце туннеля и иметь возможность передачи через Интернет.** Это означает, что концентратор и маршрутизаторы всех лучей в этой сети должны иметь статические, не частные IP-адреса.

Для подсоединения к Интернету небольших узлов внешний IP-адрес луча обычно меняется при каждом подключении к Интернету, т.к. каждый раз, когда в канале появляется луч (асимметричная цифровая абонентская линия (ADSL) и абонентский кабельный ввод), поставщик Интернет-услуг (ISP) динамично предоставляет адрес внешнего интерфейса (через протокол динамической настройки узла (DHCP)). Такое динамическое выделение "внешнего адреса" маршрутизатора позволяет ISP реализовывать избыточную подписку для адресного пространства в Интернете, так как одновременно не все пользователи будет подключены к сети. Выделение статического адреса для оконечного маршрутизатора может стоить значительно дороже. Для использования протокола динамической маршрутизации поверх IPsec VPN необходимы туннели GRE, но теряется возможность использования периферийных серверов с динамически выделяемыми IP-адресами на внешних физических интерфейсах.

Все упомянутые, а также дополнительные ограничения, сводятся к следующим пунктам:

- IPsec использует список контроля доступа (ACL) для определения данных, которые должны быть зашифрованы. Каждый раз, когда добавляется новая сеть (подсеть) после луча или концентратора, необходимо изменить список управления доступом и на центральном маршрутизаторе и на маршрутизаторе на конце луча. Если SP управляет маршрутизатором, то пользователь должен уведомить SP, чтобы получить список ACL IPsec. Это список изменен таким образом, чтобы новый трафик стал зашифрованным.
- В больших звездообразных сетях размер настройки на маршрутизаторе концентратора можеть достигнуть такой величины, что его уже нельзя будет использовать. Например, центральному маршрутизатору понадобится около 3900 строк конфигурации для поддержки 300 оконечных маршрутизаторов. При таком большом количестве трудно отобразить конфигурацию и найти ее раздел, относящийся к текущей проблеме, отладка которой выполняется. Кроме того, это настройка размера может быть слишком большой, чтобы уместиться в энергонезависимом ЗУПВ, поэтому ее следует сохранить во Flash-памяти.
- GRE + IPsec должен знать адрес однорангового узла конечной точки. IP-адреса маршрутизаторов на конце луча подключены напрямую к Интернету через собственного

ISP, и они зачастую настроены так, что адреса их внешних интерфейсов не являются фиксированными. IP-адреса могут изменяться каждый раз, когда узел подключается к сети (по DHCP).
- Если необходимо прямое соединение между лучами через IPsec VPN, тогда звездообразная сеть должна стать полностью объединенной сетью. Так как еще неизвестно, между какими лучами необходимо установить соединение, то требуется полная объединенная сеть, даже если соединение всех лучей друг с другом не понадобится. Также, невозможно настроить IPsec на маленьком маршрутизаторе луча так, чтобы он имел прямое соединение со всеми другими маршрутизаторами лучей в сети; для этого необходимо иметь более мощные маршрутизаторы лучей.

Решение для сети DMVPN

Чтобы исправить перечисленные проблемы методом масштабирования, решение DMVPN использует Multipoint GRE (mGRE) и протокол разрешения последующего узла (NHRP) с IPsec и некоторыми новыми усовершенствованиями.

Запуск автоматического шифрования IPsec

Если не с помощью решения DMVPN, Зашифрованный туннель IPSec не инициируется, пока нет трафик данных, который требует использования этого Туннеля IPSec. Для запуска туннеля IPsec и отбрасывания трафика требуется от 1 до 10 секунд. **При использовании GRE с IPsec настройка туннеля GRE уже содержит адрес одноранговового узла туннеля GRE (tunnel destination), который одновременно является адресом одноранговового узла IPsec**. Оба адреса настраиваются предварительно.

Если вы используете алгоритм обнаружения конечной точки туннеля (TED) и динамические криптокарты на маршрутизаторе концентратора, то вы можете избежать необходимости предварительной настройки адресов одноранговового узла IPsec на концентраторе, но перед началом работы протокола ISAKMP необходимо провести тестовую отправку и получение TED. Это необязательно, так как при использовании GRE одноранговые адреса источника и назначения известны заранее. Они либо внесены в конфигурацию, либо приведены в NHRP (для многоточечных туннелей GRE).

При использовании решения для сетей DMVPN, IPsec запускается одновременно для двухточечных и многоточечных туннелей GRE. Также, нет необходимости конфигурировать любой криптографический ACL, так как они будут автоматически поставлены от GRE туннельных адресов источника или пункта назначения. Для определения параметров шифрования IPsec используются следующие команды. **Обратите внимание на то, что команды set peer ... или match address ... не требуются, так как данная информация поступает прямо из связанного туннеля GRE или сопоставлений NHRP.**

```
crypto ipsec profile <profile-name> set transform-set <transform-name>
```

Следующая команда связывает интерфейс туннеля с профилем IPsec.

```
interface tunnel<number> ... tunnel protection ipsec profile <profile-name>
```

Динамическое создание туннелей для каналов с топологией "звезда"

Никакой GRE или Информация IPSec о луче не настроены на маршрутизаторе концентратора в сети DMVPN. Туннель GRE маршрутизатора луча содержит (посредством команд NHRP) информацию о маршрутизаторе концентратора. Когда маршрутизатор на конце луча запускается, он автоматически устанавливает туннель IPsec с маршрутизатором-концентратором, как описано выше. Затем он использует NHRP, чтобы сообщить центральному маршрутизатору текущий IP-адрес физического интерфейса. Это полезно по трем причинам:

- Если IP-адрес физического интерфейса оконечного маршрутизатора был присвоен динамически (например, с помощью ADSL или кабельного модема), то для центрального маршрутизатора нельзя использовать эти данные, так как при каждой перезагрузке оконечный маршрутизатор будет получать новый IP-адрес физического интерфейса.
- Конфигурация центрального маршрутизатора сокращается и упрощается, поскольку ему не нужна информация GRE или IPsec об одноранговых маршрутизаторах. Вся информация постоянно запоминается посредством NHRP.
- Изменять настройку на концентраторе или других текущих маршрутизаторах луча при добавлении в сеть DMVPN нового маршрутизатора луча не потребуется. Новый маршрутизатор луча настраивается на основе информации концентратора, и при включении маршрутизатор концентратора автоматически его регистрирует. Протокол динамической маршрутизации передает маршрутную информацию для этого луча на концентратор. Концентратор передает эти новые данные маршрутизации другим периферийным устройствам. Кроме этого, он передает маршрутную информацию всех остальных лучей на этот новый луч.

Создание динамического туннеля для трафика между краевыми маршрутизаторами

Как отмечалось выше, сейчас в ячеистой сети на каждом маршрутизаторе необходимо настраивать все двухточечные туннели IPsec (или IPsec+GRE), даже если какие-либо из них или их большинство действуют не все время. Используя решение DMVPN, один маршрутизатор становится концентратором, а другие маршрутизаторы (лучи) настраиваются на концентратор с помощью туннелей. Туннели с топологией "звезда" постоянно включены, и конфигурирование лучей для определения туннелей для любых других лучей не требуется. Напротив, когда один луч хочет передать пакет на другой луч (как подсеть за другим лучом), он использует NHRP для динамического определения необходимого адреса луча назначения. Центральный маршрутизатор действует в качестве сервера NHRP и обрабатывает этот запрос для исходного оконечного устройства. Затем два конечных устройства динамически создают между собой туннель IPsec (через единый интерфейс mGRE), обеспечивающий прямую передачу данных. Данный динамический туннель между двумя оконечными устройствами будет автоматически разорван после окончания (настроенного) периода бездействия.

Поддержка протоколов динамической маршрутизации

Решение DMVPN основывается на Туннелях GRE, которые поддерживают туннелирующие пакеты групповой адресации/широковещательного IP, таким образом, решение DMVPN также поддерживает протоколы динамической маршрутизации, работающие на основе туннелей IPsec+mGRE. Ранее протокол NHRP требовал явной настройки широковещательного/многоадресного сопоставления для IP-адресов назначения туннеля

для поддержки GRE-туннеллирования многоадресных и широковещательных IP-пакетов. Например, в концентраторе вам был бы нужен **ip nhrp map multicast <spoke-n-addr>** строка настройки для каждого луча. Для решения DMVPN адреса на конце лучей заранее неизвестны, поэтому эта конфигурация невозможна. **NHRP можно настроить на автоматическое добавление каждого луча в список многоадресного назначения на концентраторе с помощью команды ip nhrp map multicast dynamic** . При помощи этой команды, когда маршрутизаторы лучей регистрируют одноадресное сопоставление NHRP при помощи сервера NHRP (концентратора), NHRP также создаст многоадресное сопоставление для этого луча. Это освобождает от необходимости заранее знать адреса оконечных устройств.

Быстрая коммутация Cisco Express Forwarding для mGRE

В настоящий момент трафик в интерфейсе mGRE коммутируется процессом, что приводит к снижению производительности. Решение DMVPN обеспечивает коммутацию с механизмом переадресации Cisco для трафика mGRE, увеличивая быстродействие. Необязательно использовать команды конфигурации для включения этой функции. Если коммутация Cisco Express Forwarding разрешена на интерфейсе туннеля GRE и входящих/исходящих физических интерфейсах, то многоточечные туннельные пакеты GRE будут переключаться с помощью Cisco Express Forwarding.

Использование динамической маршрутизации в виртуальных частных сетях (VPN), защищенных спецификацией IPsec

В данном разделе рассматривается сложившаяся ситуация (предшествующие DMVPN решения). IPsec внедрен на маршрутизаторах Cisco через ряд команд, которые определяют шифрование и затем **команду crypto map <map-name>**, примененную на внешний интерфейс маршрутизатора. Из-за такой архитектуры и отсутствия стандарта, описывающего порядок использования IPsec для шифрования многоадресных/широковещательных IP-пакетов, пакеты протокола IP маршрутизации невозможно передать через туннель IPsec, и информация о любых изменениях маршрутизации достигнет другого конца туннеля IPsec не сразу.

Примечание: Все протоколы динамической маршрутизации кроме BGP используют пакеты IP-адреса групповой адресации или широковещание. Для решения этой проблемы используются туннели GRE в комбинации с IPsec.

Туннели GRE внедрены на маршрутизаторах Cisco при помощи виртуального туннельного интерфейса (**interface tunnel <#>**). Протокол тоннелирования GRE разработан для многоадресных/широковещательных IP пакетов, поэтому протокол динамической маршрутизации можно «запустить» через туннель GRE. Туннельные пакеты GRE являются одноадресными пакетами IP, инкапсулирующими исходный много- или одноадресный пакет IP. Затем можно использовать Ipsec для шифрования туннельного пакета GRE. Можно запустить IPsec в режиме передачи и сэкономить 20 байт, т. к. GRE уже инкапсулировал исходный пакет данных и IPsec нет необходимости инкапсулировать IP-пакет GRE в другом IP-заголовке.

При использовании IPSec в транспортном режиме предусмотрено следующее ограничение: подлежащие шифрованию IP-адреса источника и назначения пакета должны соответствовать одноранговым адресам IPSec (самого маршрутизатора). В данном случае это означает, что конечная точка GRE-туннеля и адрес узла IPsec должны совпадать. Это

не представляет трудности, т. к. одни и те же маршрутизаторы являются конечными точками туннелей IPsec и GRE. Совмещая туннели GRE с шифрованием IPsec, можно использовать протокол динамической IP маршрутизации для обновления таблиц маршрутизации на обоих концах зашифрованного туннеля. Элементы таблицы IP маршрутизации для сетей, которые были записаны через зашифрованный туннель, будут воспринимать противоположный конец туннеля (IP-адрес интерфейса туннеля GRE) как IP следующего перехода. Таким образом, если на каком-либо конце туннеля меняются параметры сети, то на другом конце эти изменения динамически отразятся; соединение при этом не будет нарушено, и дополнительные настройки маршрутизаторов не понадобятся.

Базовая конфигурация

Ниже представлена стандартная двухточечная конфигурация IPsec+GRE. Затем приведено несколько примеров конфигураций, в которых отдельные элементы решения DMVPN добавлены в выполняемые действия, чтобы показать различные возможности DMVPN. Каждый пример построен на предыдущих примерах для демонстрации использования решения DMVPN в усложняющихся структурах сети. Эту серию примеров можно использовать в качестве шаблона для переноса текущей сети VPN IPsec+GRE в DMVPN. В любой момент «перенос» можно остановить, если конкретный пример настройки соответствует требованиям к вашей сети.

Звезда IPsec + GRE (n = 1,2,3,...),...)

Центральный маршрутизатор

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0 crypto map
vpnmap1 10 ipsec-isakmp set peer 172.16.1.1 set
transform-set trans2 match address 101 crypto map
vpnmap1 20 ipsec-isakmp set peer 172.16.2.1 set
transform-set trans2 match address 102 . . . crypto map
vpnmap1 <10*n> ipsec-isakmp set peer 172.16.<n>.1 set
transform-set trans2 match address <n+100> ! interface
Tunnel1 bandwidth 1000 ip address 10.0.0.1
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.16.1.1 ! interface
Tunnel2 bandwidth 1000 ip address 10.0.0.5
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.16.2.1 ! . . . !
interface Tunnel<n> bandwidth 1000 ip address
10.0.0.<4n-3> 255.255.255.252 ip mtu 1400 delay 1000
tunnel source Ethernet0 tunnel destination 172.16.<n>.1
! interface Ethernet0 ip address 172.17.0.1
255.255.255.0 crypto map vpnmap1 ! interface Ethernet1
ip address 192.168.0.1 255.255.255.0 ! router eigrp 1
network 10.0.0.0 0.0.0.255 network 192.168.0.0 0.0.0.255
no auto-summary ! access-list 101 permit gre host
172.17.0.1 host 172.16.1.1 access-list 102 permit gre
host 172.17.0.1 host 172.16.2.1 ... access-list <n+100>
```

```
permit gre host 172.17.0.1 host 172.16.<n>.1
```

Маршрутизатор Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1 authentication pre-share crypto
isakmp key cisco47 address 0.0.0.0 ! crypto ipsec
transform-set trans2 esp-des esp-md5-hmac mode transport
! crypto map vpnmap1 local-address Ethernet0 crypto map
vpnmap1 10 ipsec-isakmp set peer 172.17.0.1 set
transform-set trans2 match address 101 ! interface
Tunnel0 bandwidth 1000 ip address 10.0.0.2
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 ! interface
Ethernet0 ip address 172.16.1.1 255.255.255.252 crypto
map vpnmap1 ! interface Ethernet1 ip address 192.168.1.1
255.255.255.0 ! router eigrp 1 network 10.0.0.0
0.0.0.255 network 192.168.1.0 0.0.0.255 no auto-summary
! access-list 101 permit gre host 172.16.1.1 host
172.17.0.1
```

Маршрутизатор Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0 crypto map
vpnmap1 10 ipsec-isakmp set peer 172.17.0.1 set
transform-set trans2 match address 101 ! interface
Tunnel0 bandwidth 1000 ip address 10.0.0.6
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 ! interface
Ethernet0 ip address 172.16.2.1 255.255.255.252 crypto
map vpnmap1 ! interface Ethernet1 ip address 192.168.2.1
255.255.255.0 ! router eigrp 1 network 10.0.0.0
0.0.0.255 network 192.168.2.0 0.0.0.255 no auto-summary
! access-list 101 permit gre host 172.16.2.1 host
172.17.0.1
```

Маршрутизатор Spoke <n>

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport ! crypto map vpnmap1 local-address
Ethernet0 crypto map vpnmap1 10 ipsec-isakmp set peer
172.17.0.1 set transform-set trans2 match address 101 !
interface Tunnel0 bandwidth 1000 ip address 10.0.0.<4n-
2> 255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 ! interface
```

```
Ethernet0 ip address 172.16.<n>.1 255.255.255.252 crypto
map vpnmap1 ! interface Ethernet1 ip address
192.168.<n>.1 255.255.255.0 ! router eigrp 1 network
10.0.0.0 0.0.0.255 network 192.168.<n>.0 0.0.0.255 no
auto-summary ! access-list 101 permit gre host
172.16.<n>.1 host 172.17.0.1
```

В приведенной выше настройке списки ACL используются для определения трафика, который должен быть зашифрован. И на центральном, и на маршрутизаторе на конце луча список управления доступом должен соответствовать IP пакетам туннеля GRE. Не важно, как меняются сети на концах туннеля, IP пакеты туннеля GRE не изменятся, т.е. этот список ACL не требует изменений.

Примечание: При использовании версий программного обеспечения Cisco IOS до 12.2 (13) T, необходимо применить команду настройки **vpnmap1 криптокарты** к обоим Туннельные интерфейсы GRE (Туннель <x>) и физический интерфейс (Ethernet0). **При использовании Cisco IOS версии 12.2(13)T или более поздней команда crypto map vpnmap1 configuration применяется только к физическому интерфейсу (Ethernet0).**

Примеры таблиц маршрутизации концентраторов и оконечными маршрутизаторами

Таблицы маршрутизации на концентраторе

```
172.17.0.0/24 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 C       10.0.0.0 is directly connected, Tunnel1
 C       10.0.0.4 is directly connected, Tunnel2
 ...
 C       10.0.0.<4n-4> is directly connected, Tunnel<n>
 C    192.168.0.0/24 is directly connected, Ethernet1
 D    192.168.1.0/24 [90/2841600] via 10.0.0.2,
18:28:19, Tunnel1
 D    192.168.2.0/24 [90/2841600] via 10.0.0.6, 2d05h,
Tunnel2
 ...
 D    192.168.<n>.0/24 [90/2841600] via 10.0.0.<4n-2>,
2d05h, Tunnel<n>
```

Таблица маршрутизации для маршрутизатора оконечного устройства 1

```
172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.1.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 C       10.0.0.0 is directly connected, Tunnel1
 D       10.0.0.4 [90/2841600] via 10.0.0.1, 23:00:58,
Tunnel0
 ...
 D      10.0.0.<4n-4> [90/2841600] via 10.0.0.1,
23:00:58, Tunnel0
 D    192.168.0.0/24 [90/2841600] via 10.0.0.1,
23:00:58, Tunnel0
 C    192.168.1.0/24 is directly connected, Loopback0
 D    192.168.2.0/24 [90/3097600] via 10.0.0.1,
23:00:58, Tunnel0
 ...
 D    192.168.<n>.0/24 [90/3097600] via 10.0.0.1,
23:00:58, Tunnel0
```

Таблица маршрутизации на маршрутизаторе Spoke <n>
172.16.0.0/24 is subnetted, 1 subnets C 172.16.<n>.0 is directly connected, Ethernet0 10.0.0.0/30 is subnetted, <n> subnets D 10.0.0.0 [90/2841600] via 10.0.0.1, 22:01:21, Tunnel0 D 10.0.0.4 [90/2841600] via 10.0.0.1, 22:01:21, Tunnel0 ... C 10.0.0.<4n-4> is directly connected, Tunnel0 D 192.168.0.0/24 [90/2841600] via 10.0.0.1, 22:01:21, Tunnel0 D 192.168.1.0/24 [90/3097600] via 10.0.0.1, 22:01:21, Tunnel0 D 192.168.2.0/24 [90/3097600] via 10.0.0.1, 22:01:21, Tunnel0 ... C 192.168.<n>.0/24 is directly connected, Ethernet0

Это базовая работающая конфигурация, которая используется в качестве отправной точки по сравнению с более сложными конфигурациями с возможностью использования решения DMVPN. Первое изменение уменьшит размер настройки на маршрутизаторе концентратора. Это не имеет значения при небольшом количестве оконечных маршрутизаторов, но если количество маршрутизаторов составляет 50–100 устройств, это становится важным фактором.

Уменьшение размера конфигурации центрального маршрутизатора

В следующем примере конфигурация центрального маршрутизатора изменена минимально: с многоканального туннельного интерфейса GRE "точка-к-точке" на одноканальный многоточечный туннельный интерфейс. Это первый шаг к решению DMVPN.

Маршрутизатор концентратора содержит уникальный блок строк настройки, необходимый для определения характеристик криптокарты для каждого маршрутизатора луча. Данная часть конфигурации определяет шифрованный ACL и интерфейс туннеля GRE для маршрутизатора на конце луча. **Эти характеристики чаще всего одинаковы для всех лучей, исключения составляют IP-адреса (set peer ..., tunnel destination ...).**

Из приведенной выше настройки маршрутизатора концентратора видно, что для каждого маршрутизатора луча необходимо как минимум 13 строк настройки; четыре для криптокарты, одна для зашифрованного ACL и восемь для интерфейса туннеля GRE. Общее количество строк конфигурации при 300 оконечных маршрутизаторах равно 39000. Необходимо также 300 (/30) подсетей для адресации каждого канала туннеля. Настройкой такого размера сложно управлять, особенно при устранении неполадок в сети VPN. Для уменьшения этого значения можно использовать динамические криптокарты, которые сократят указанное выше значение на 1200 строк, и оставят 2700 строк в сети с 300 лучами.

Примечание: При использовании динамических криптокарт зашифрованный туннель IPSec должен быть инициирован лучевым маршрутизатором. Можно также использовать **IP ненумерованный <interface>** для сокращения количества подсетей, необходимых для Туннелей GRE, но это может сделать устранение проблем более трудным позже.

Решение DMVPN позволяет настроить одиночный многоадресный туннельный интерфейс GRE и одиночный профиль IPsec на маршрутизаторе-концентраторе для обработки всех маршрутизаторов на конце луча. Это позволяет размеру конфигурации на маршрутизаторе-концентраторе оставаться постоянной, вне зависимости от количества оконечных маршрутизаторов, добавленных в сеть VPN.

Решение DMVPN предлагает следующие новые команды:

```
crypto ipsec profile <name> <ipsec parameters> tunnel protection ipsec profile <name> ip nhrp map multicast dynamic
```

Команда crypto ipsec profile <name> используется как динамическая криптокарта, и это специально разработано для туннельных интерфейсов. Эта команда используется для определения параметров шифрования IPsec в VPN туннелях от конечного устройства к концентратору и от одного конечного устройства к другому. Единственный необходимый параметр в этом профиле - это набор для преобразования. **Адрес одноранговой узла IPsec и условие match address ... для прокси IPsec автоматически извлекаются из NHRP-сопоставлений для туннеля GRE.**

Команда tunnel protection ipsec profile <name> настроена под Туннельным интерфейсом GRE и используется для соединения Туннельного интерфейса GRE к Профилю IPSEC. Кроме того, **команда tunnel protection ipsec profile <name>** может также использоваться с Туннелем GRE "точка-точка". **В этом случае получаются данные о сервере IPsec и модуле доступа из точки начала туннеля… и точке назначения туннеля… конфигурации**. Это позволяет упростить процесс конфигурации, так как отпадает необходимость использования одноранговых узлов IPSec и зашифрованных списков ACL.

Примечание: Tunnel protection … команда указывает, что IP - безопасное шифрование будет сделано после того, как GRE-инкапсуляция была добавлена к пакету.

Эти первые две новых команды подобны настройке криптокарты и присвоению криптокарты к интерфейсу с помощью **команды crypto map <name>**. Существенное отличие заключается в том, что при использовании новых команд нет необходимости указывать адрес равноправного пользователя протокола IPSec или список ACL, чтобы отобрать пакеты, подлежащие шифрованию. Эти параметры определяются автоматически из отображений NHRP для туннельного интерфейса mGRE.

Примечание: При использовании **tunnel protection …** команда на туннельном интерфейсе, **криптокарта...** команда не настроена на физическом исходящем интерфейсе.

Последняя новая команда, ip nhrp map multicast dynamic, позволяет NHRP автоматически добавлять лучевые маршрутизаторы к многоадресным сопоставлениям NHRP, когда эти маршрутизаторы инициируют туннель mGRE+IPsec и регистрируют их одноадресные соответствия NHRP. Это необходимо для возможности работы протокола динамической маршрутизации в туннелях mGRE+IPsec между концентратором и лучами. Если эта команда недоступна, то маршрутизатор концентратора должен иметь отдельный канал настройки для многоадресного сопоставления с каждым лучом.

Примечание: С этой конфигурацией маршрутизаторы оконечных устройств должны инициировать соединение с туннелированием mGRE+IPsec, поскольку конфигурация маршрутизатора концентратора не содержит данных об оконечных устройствах. Однако проблем не возникает, поскольку при использовании DMVPN при запуске оконечного маршрутизатора автоматически инициируется и постоянно остается активным туннель

mGRE+IPsec.

Примечание: Следующий пример демонстрирует двухточечный туннельный интерфейс GRE на оконечных маршрутизаторах и линиях конфигурации NHRP, добавленный на обоих концентраторах и оконечных маршрутизаторах для поддержки туннеля mGRE на маршрутизаторе-концентраторе. Изменения конфигурации изложены ниже.

Маршрутизатор концентратора (старый)

```
crypto map vpnmap1 10 IPsec-isakmp set peer 172.16.1.1
set transform-set trans2 match address 101 crypto map
vpnmap1 20 IPsec-isakmp set peer 172.16.2.1 set
transform-set trans2 match address 102 . . . crypto map
vpnmap1 <10n> IPsec-isakmp set peer 172.16.<n>.1 set
transform-set trans2 match address <n+100> ! interface
Tunnel1 bandwidth 1000 ip address 10.0.0.1
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.16.1.1 ! interface
Tunnel2 bandwidth 1000 ip address 10.0.0.5
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.16.2.1 ! . . . !
interface Tunnel<n> bandwidth 1000 ip address
10.0.0.<4n-1> 255.255.255.252 ip mtu 1400 delay 1000
tunnel source Ethernet0 tunnel destination 172.16.<n>.1
! interface Ethernet0 ip address 172.17.0.1
255.255.255.0 crypto map vpnmap1 ! access-list 101
permit gre host 172.17.0.1 host 172.16.1.1 access-list
102 permit gre host 172.17.0.1 host 172.16.2.1 . . .
access-list <n+100> permit gre host 172.17.0.1 host
172.16.<n>.1
```

Маршрутизатор концентратора (новый)

```
crypto ipsec profile vpnprof set transform-set trans2 !
interface Tunnel0 bandwidth 1000 ip address 10.0.0.1
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map multicast dynamic ip nhrp network-id 100000 ip
nhrp holdtime 600 no ip split-horizon eigrp 1 delay 1000
tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address 172.17.0.1
255.255.255.0
```

(Старый) маршрутизатор Spoke <n>

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<4n-2> 255.255.255.252 ip mtu 1400
delay 1000 tunnel source Ethernet0 tunnel destination
172.17.0.1 ! interface Ethernet0 ip address 172.16.<n>.1
255.255.255.252 crypto map vpnmap1 ! . . . ! access-list
101 permit gre host 172.16.<n>.1 host 172.17.0.1 !
```

(Новый) маршрутизатор Spoke <n>

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
```

```
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<n+1> 255.255.255.0 ip mtu 1400 ip
nhrp authentication test ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000 ip nhrp holdtime 300 ip nhrp
nhs 10.0.0.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.1 tunnel key 100000 ! interface
Ethernet0 ip address 172.16.<n>.1 255.255.255.252 crypto
map vpnmap1 ! . . . ! access-list 101 permit gre host
172.16.<n>.1 host 172.17.0.1 !
```

На лучевых маршрутизаторах изменилась маска подсети, и на туннельный интерфейс были добавлены команды NHRP. Команды NHRP необходимы, т.к. маршрутизатор концентратора теперь использует NHRP для сопоставления IP-адреса туннельного интерфейса луча с IP-адресом физического интерфейса луча.

ip address 10.0.0.<n+1> 255.255.255.0 ip mtu 1400 ip nhrp authentication test ip nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000 ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 ... tunnel key 100000

Подсеть теперь /24 вместо /30, поэтому все узлы находятся в одной подсети, а не в разных. Периферийные сервера по-прежнему передают трафик между краевыми маршрутизаторами через концентратор, поскольку они используют туннельный интерфейс GRE "точка-точка". **Команды ip nhrp authentication ..., ip nhrp network-id ... и tunnel key ... используются для сопоставления туннельных пакетов и пакетов NHRP с правильным широковещательным туннельным интерфейсом GRE и сетью NHRP при их получении концентратором. Ip nhrp map...** и **ip nhrp nhs**... команды используются NHRP на луче для объявления NHRP - маршрутизации лучей (10.0.0. <n+1>-> 172.16. <n>.1) к концентратору. 10.0.0. <n+1> адрес получен из **IP-адреса...** команда на туннельном интерфейсе и 172.16. <n>.1 адресов получен из **назначения туннеля...** команда на туннельном интерфейсе.

В случае 300 лучевых маршрутизаторов это изменение уменьшит число строк настройки на концентраторе с 3 900 до 16 (на 3 884 строки). Размер настройки на каждом лучевом маршрутизаторе увеличится на 6 строк.

Поддержка динамических адресов на оконечных устройствах

Перед установлением туннельного соединения по протоколу IPSec на маршрутизаторе Cisco для каждого одноранговового узла необходимо задать IP-адрес другого одноранговового узла. При выполнении этого может возникнуть проблема, если маршрутизатор на конце луча имеет динамический адрес физического интерфейса, как это часто бывает у маршрутизаторов, подключенных через DSL или кабельную линию.

TED позволяет одноранговому пользователю IPSec найти другого одноранговового пользователя с помощью отправки специального пакета протокола ISAKMP (Протокол управления ключами Ассоциации безопасности Интернет) на IP-адрес назначения исходного пакета данных, который должен быть зашифрован. Предполагается, что этот пакет пройдет через промежуточную сеть, следуя по тому же пути, что и туннельный пакет IPsec. Этот пакет будет подхвачен одноранговым узлом IPsec на другом конце, о чем он сообщит первому одноранговому узлу. Затем выполняется сопоставление безопасности IPsec и ISAKMP и создание туннеля IPsec. Это сработает только в том случае, если пакеты данных, которые необходимо зашифровать, имеют маршрутизируемые IP-адреса.

TED можно использовать в сочетании с GRE туннелями, как конфигурировано в предыдущем разделе. Это было успешно протестировано, хотя в ранних версиях ПО Cisco IOS возникали большие проблемы, когда TED вынужденно шифровал не только туннельные пакеты GRE, но и весь IP трафик между двумя одноранговыми узлами IPsec. Решение DMVPN предоставляет эту и другие дополнительные возможности, при этом хостам не требуется использовать маршрутизируемые IP-адреса Интернета и отправлять тестовые и ответные пакеты. С небольшими изменениями конфигурация из последнего раздела может использоваться для поддержки маршрутизаторов спицы с динамическими IP-адресами на внешних физических интерфейсах.

Центральный маршрутизатор (без изменений)

```
crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
```

(Старый) маршрутизатор Spoke <n>

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 ...
 !
 access-list 101 permit gre host 172.16.<n>.1 host
172.17.0.1
```

(Новый) маршрутизатор Spoke <n>

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  set security-association level per-host match address
101 ! ... ! access-list 101 permit gre any host
172.17.0.1
```

В новой конфигурации оконечного узла поддерживаются следующие функциональные возможности.

- Когда появляется интерфейс туннеля GRE, он запускает отсылку регистрационных пакетов NHRP маршрутизатору концентратора. Эти регистрационные пакеты NHRP инициируют IPsec. На маршрутизаторе на конце луча настроен узел набора <адрес партнера (peer)> и **команды match ip access-list <ACL>**. ACL определяет GRE как протокол: любой в качестве источника, IP-адрес концентратора в качестве адреса

назначения.**Примечание:** Следует отметить, что любой используется в качестве источника в ACL, и это должно иметь место, так как IP-адрес маршрутизатора на конце луча является динамичным и, поэтому, не известный, прежде чем физический интерфейс будет активен. Подсеть IP может использоваться как источник в ACL, если адрес динамического интерфейса "звезды" ограничивается адресом в данной подсети.

- **Была использована команда set security-association level per-host , благодаря чему источник IP на IPsec прокси периферийного оборудования будет адресом текущего физического интерфейса периферийного оборудования (/32), а не адресом из ACL.** Если какие-либо списки ACL использовались в качестве источника в IPsec-прокси, то другой краевой маршрутизатор не сможет настроить с помощью этого концентратора туннель IPsec+GRE. **Это объясняется тем, что итоговый прокси IPsec на концентраторе идентичен команде permit gre host 172.17.0.1 any.** Это означает, что все туннельные пакеты GRE, предназначенные для любого конечного устройства, зашифровываются и отправляются на первое конечное устройство, установившее туннель с концентратором, так как прокси-сервер IPSEC согласовывает пакеты GRE для каждого конечного устройства.
- Как только туннель IPsec настроен, пакет регистрации протокола NHRP передается от оконечного маршрутизатора на заданный сервер следующего узла. NHS является центральным маршрутизатором в сети с топологией "звезда". Пакет регистрации протокола NHRP содержит данные, позволяющие центральному маршрутизатору создавать отображение NHRP для оконечного маршрутизатора. С этим отображением центральный маршрутизатор может пересылать одноадресные IP-пакеты данных для конечного маршрутизатора через туннель mGRE+IPsec. Кроме этого, концентратор добавляет лучевой маршрутизатор в список многоадресного соответствия NHRP. После этого концентратор начнет отправку групповых пакетов динамической IP маршрутизации конечным устройствам (если настроен динамически маршрутизируемый протокол). Луч затем станет соседом протокола маршрутизации концентратора, и они обменяются обновлениями маршрутизации.

Топология "звезда" с использованием инкапсуляции mGRE и IPsec

Центральный маршрутизатор

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map multicast dynamic ip
nhrp network-id 100000 ip nhrp holdtime 600 no ip split-
horizon eigrp 1 delay 1000 tunnel source Ethernet0
tunnel mode gre multipoint tunnel key 100000 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
```

```
ip address 172.17.0.1 255.255.255.0 ! interface
Ethernet1 ip address 192.168.0.1 255.255.255.0 ! router
eigrp 1 network 10.0.0.0 0.0.0.255 network 192.168.0.0
0.0.0.255 no auto-summary !
```

Обратите внимание, что в вышеприведенной конфигурации концентратора IP-адреса оконечных маршрутизаторов не настроены. IP-адреса внешнего физического интерфейса оконечного устройства и туннельного интерфейса сопоставления оконечного устройства определяются концентратором динамически по протоколу NHRP. Это позволяет динамически назначать IP-адрес внешнего физического интерфейса spokevЪ™.

Маршрутизатор Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set security-association level per-host set transform-
set trans2 match address 101 ! interface Tunnel0
bandwidth 1000 ip address 10.0.0.2 255.255.255.0 ip mtu
1400 ip nhrp authentication test ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp network-id 100000 ip nhrp holdtime
300 ip nhrp nhs 10.0.0.1 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 tunnel key
100000 ! interface Ethernet0 ip address dhcp hostname
Spoke1 crypto map vpnmap1 ! interface Ethernet1 ip
address 192.168.1.1 255.255.255.0 ! router eigrp 1
network 10.0.0.0 0.0.0.255 network 192.168.1.0 0.0.0.255
no auto-summary ! access-list 101 permit gre 172.16.1.0
0.0.0.255 host 172.17.0.1
```

Маршрутизатор Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set security-association level per-host set transform-
set trans2 match address 101 ! interface Tunnel0
bandwidth 1000 ip address 10.0.0.3 255.255.255.0 ip mtu
1400 ip nhrp authentication test ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp network-id 100000 ip nhrp holdtime
300 ip nhrp nhs 10.0.0.1 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 tunnel key
```

```
100000 ! interface Ethernet0 ip address dhcp hostname
Spoke2 crypto map vpnmap1 ! interface Ethernet1 ip
address 192.168.2.1 255.255.255.0 ! router eigrp 1
network 10.0.0.0 0.0.0.255 network 192.168.1.0 0.0.0.255
no auto-summary ! access-list 101 permit gre 172.16.2.0
0.0.0.255 host 172.17.0.1
```

Основные параметры конфигурации, на которые необходимо обратить внимание:

- Внешний физический интерфейс (Ethernet0) использует динамический IP-адрес через DHCP.**ip address dhcp hostname Spoke2**
- Крипто-ACL (101) задает подсеть как источник для IPSEC прокси.**список доступа 101 допускает gre 172.16.2.0 0.0.0.255 хост 172.17.0.1**
- Следующая команда в криптокарте IPsec служит для настройки сопоставлений безопасности для отдельных хостов.**set security-association level per-host**
- Все туннели входят в одну подсеть, т. к. все они соединяются через один многоточечный интерфейс GRE концентратора.**ip адрес 10.0.0.2 255.255.255.0**

Комбинация этих трех команд делает не нужной настройку IP-адреса внешнего физического интерфейса оконечного устройства. Используемый прокси-сервер IPsec будет основан скорее на узле, а не подсети.

Конфигурация на маршрутизаторах на конце луча обязательно имеет заданный IP-адрес маршрутизатора-концентратора, поскольку он должен инициировать туннель IPsec+GRE. Отметьте подобие настроек Spoke1 и Spoke2. Похожие настройки будут на всех лучевых маршрутизаторах. В большинстве случаев каждому лучу необходимо просто присвоить уникальный IP-адрес для их интерфейсов; остальные настройки будут одинаковы у всех лучей. Такой подход позволяет быстро настраивать и развертывать много оконечных маршрутизаторов.

Данные NHRP в звездообразной сети выглядят следующим образом.

Центральный маршрутизатор

```
Hub#show ip nhrp 10.0.0.2/32 via 10.0.0.2, Tunnel0
created 01:25:18, expire 00:03:51 Type: dynamic, Flags:
authoritative unique registered NBMA address: 172.16.1.4
10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:06:02,
expire 00:04:03 Type: dynamic, Flags: authoritative
unique registered NBMA address: 172.16.2.10 ...
10.0.0.<n>/32 via 10.0.0.<n>, Tunnel0 created 00:06:00,
expire 00:04:25 Type: dynamic, Flags: authoritative
unique registered NBMA address: 172.16.<n>.41
```

Маршрутизатор Spoke1

```
Spoke1#sho ip nhrp 10.0.0.1/32 via 10.0.0.1, Tunnel0
created 4d08h, never expire Type: static, Flags:
authoritative NBMA address: 172.17.0.1
```

Динамическая сеть типа "звезда" с несколькими узлами

Настройка на лучевых маршрутизаторах, описанная выше, не основывается на возможностях решения DMVPN, поэтому на них может быть запущено ПО Cisco IOS версий ранее 12.2(13)T. Настройка маршрутизатора концентратора зависит от функций DMVPN, поэтому на нем необходимо использовать Cisco IOS версии 12.2(13)T и выше. Это позволяет более гибко определять время обновления уже развернутых лучевых

маршрутизаторов. Если на ваших маршрутизаторах также установлено программное обеспечение Cisco IOS версии 12.2(13)T или более поздней, тогда вы можете упростить конфигурацию следующим образом.

Маршрутизатор Spoke <n> (до Cisco IOSR 12.2 (13) T)
crypto map vpnmap1 10 IPsec-isakmp set peer 172.17.0.1 set security-association level per-host set transform-set trans2 match address 101 ! interface Tunnel0 bandwidth 1000 ip address 10.0.0.<n+1> 255.255.255.0 ip mtu 1400 ip nhrp authentication test ip nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000 ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000 tunnel source Ethernet0 tunnel destination 172.17.0.1 tunnel key 100000 ! interface Ethernet0 ip address dhcp hostname Spoke<n> **crypto map vpnmap1** ! . . . ! **access-list 101 permit gre any host 172.17.0.1**

Маршрутизатор Spoke <n> (после Cisco IOSR 12.2 (13) T)
crypto ipsec profile vpnprof set transform-set trans2 ! interface Tunnel0 bandwidth 1000 ip address 10.0.0.<n+1> 255.255.255.0 ip mtu 1400 ip nhrp authentication test ip nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000 ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000 tunnel source Ethernet0 tunnel destination 172.17.0.1 tunnel key 100000 **tunnel protection ipsec profile vpnprof** ! interface Ethernet0 ip address dhcp hostname Spoke<n> !

Обратите внимание, что было сделано следующее:

1. **Команда crypto map vpnmap1 10 ipsec-isakmp заменена командой crypto ipsec profile vpnprof.**
2. **Команда crypto map vpnmap1 была удалена из интерфейса Ethernet0, и команда tunnel protection ipsec profile vpnprof добавлена на интерфейс Tunnel0.**
3. **Удаленный ACL шифрования, список адресов 101 разрешает туннель GRE для любого хоста 172.17.0.1.**

В этом случае адреса равноправных пользователей и прокси протокола IPSec автоматически выводятся из конфигурации источника и пункта назначения туннеля. Одноранговые узлы и прокси-серверы (в результате команды show crypto ipsec sa):

```
...
local ident (addr/mask/prot/port):    (172.16.1.24/255.255.255.255/47/0)
remote ident (addr/mask/prot/port):   (172.17.0.1/255.255.255.255/47/0)
...
local crypto endpt.: 172.17.1.24, remote crypto endpt.:172.17.0.1
...
```

[В общих словах, следующие полные конфигурации включают все изменения, сделанные в базовой конфигурации (концентратор IPsec+GRE и оконечное устройство) вплоть до этого момента.]

Центральный маршрутизатор
version 12.3 !

```
hostname Hub
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco47 address 0.0.0.0
!
crypto ipsec transform-set trans2 esp-des esp-md5-hmac
 mode transport
!
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 100000
 ip nhrp holdtime 600
 no ip split-horizon eigrp 1
 delay 1000
 tunnel source Ethernet0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
!
interface Ethernet0
 ip address 172.17.0.1 255.255.255.0
!
interface Ethernet1
 ip address 192.168.0.1 255.255.255.0
!
router eigrp 1
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.0.255
 no auto-summary
!
```

Нет изменений конфигурации концентратора.

Маршрутизатор Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof set transform-set trans2 !
interface Tunnel0 bandwidth 1000 ip address 10.0.0.2
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000
ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000
tunnel source Ethernet0 tunnel destination 172.17.0.1
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke2 ! interface Ethernet1 ip address 192.168.1.1
```

```
255.255.255.0 ! router eigrp 1 network 10.0.0.0
0.0.0.255 network 192.168.1.0 0.0.0.255 no auto-summary
!
```

Маршрутизатор Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof set transform-set trans2 !
interface Tunnel0 bandwidth 1000 ip address 10.0.0.3
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000
ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000
tunnel source Ethernet0 tunnel destination 172.17.0.1
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke2 ! interface Ethernet1 ip address 192.168.2.1
255.255.255.0 ! router eigrp 1 network 10.0.0.0
0.0.0.255 network 192.168.2.0 0.0.0.255 no auto-summary
!
```

Динамическая многоточечная VPN с поддержкой IPsec

В этом разделе концепции и конфигурация показывают все возможности динамической многоточечной виртуальной частной сети (DMVPN). NHRP дает возможность лучевым маршрутизаторам динамически запоминать адреса внешних физических интерфейсов других лучевых маршрутизаторов в сети VPN. Это означает, что оконечный маршрутизатор получает достаточный объем информации для динамического создания туннеля IPsec+mGRE к другим оконечным маршрутизаторам. Эта возможность является преимуществом, если трафик данных между двумя оконечными устройствами передается через центральный маршрутизатор. Затем трафик должен быть зашифрован/расшифрован, при этом время задержки и нагрузка на центральном маршрутизаторе увеличиваются вдвое. Для использования этой функции оконечные маршрутизаторы должны быть скоммутированы от GRE "точка-точка" (p-pGRE) до туннельных интерфейсов многоточечной GRE (mGRE). Им тоже нужно знать (под)сети, доступные за другими оконечными устройствами с помощью IP следующего перехода IP-адреса туннеля другого маршрутизатора оконечного устройства. Лучевые маршрутизаторы запоминают эти (под)сети с помощью динамического протокола IP маршрутизации через туннель IPsec+mGRE с концентратором.

Динамический протокол IP-маршрутизации, запущенный на центральном маршрутизаторе можно настроить для отображения маршрутов, обнаруженных на одном оконечном маршрутизаторе, восстанавливая тот же интерфейс на остальных оконечных маршрутизаторах, однако следующим IP-узлом в таких маршрутах, как правило, является центральный, а не оконечный маршрутизатор, на котором был обнаружен этот маршрут.

Примечание: Протокол динамической маршрутизации работает только на концентраторе и линиях спиц. Он не работает в динамических каналах между спицами.

Протоколы динамической маршрутизации (RIP, OSPF и EIGRP) должны быть настроены на концентраторе для декларации обратных маршрутов из интерфейса туннеля mGRE и для задания вызывающего оконечного маршрутизатора в качестве следующего IP-узла для маршрутов, полученных от одного оконечного устройства при декларации маршрута другим устройствам.

Это требования для конфигураций протокола маршрутизации.

RIP

Необходимо выключить расщепленный горизонт на туннельном интерфейсе MGRE на концентраторе, иначе RIP не даст объявление, маршруты, изученные через интерфейс mGRE, отступают тот же самый интерфейс.

no ip split-horizon
В других изменениях нет необходимости. RIP автоматически использует оригинальный IP следующего перехода на объявленных маршрутах, на которых он восстанавливает тот же интерфейс, откуда они были получены.

EIGRP

Нужно отключить разделение горизонтов на туннельном интерфейсе mGRE концентратора, иначе EIGRP не поместит маршруты, полученные по интерфейсу mGRE, обратно в этот интерфейс.

no ip split-horizon eigrp <as>
По умолчанию EIGRP назначит следующий узел IP маршрутизатором концентратора для маршрутов, которые он объявляет, даже если объявление этих маршрутов восстанавливает тот же интерфейс, откуда они были получены. Поэтому в данном случае необходима следующая команда конфигурации, чтобы предписать EIGRP использовать исходный IP-адрес следующего перехода при объявлении этих маршрутов.

no ip next-hop-self eigrp <as>
Примечание: Команда no ip next-hop-self eigrp <as> будет доступным началом в Cisco IOS Release 12.3 (2). Для Cisco IOS версий от 12.2(13)T до 12.3(2) выполните следующие действия:

- Если создание динамических туннелей между оконечными устройствами нежелательно, использовать указанную выше команду нет необходимости.
- Если необходимы динамические туннели между лучами, то необходимо использовать коммутирование туннельного интерфейса на лучевых маршрутизаторах.
- В противном случае вам придется использовать другой протокол маршрутизации для DMVPN.

OSPF

Так как OSPF является протоколом маршрутизации на основе состояния каналов, проблемы с разделением диапазонов не возникают. Обычно при использовании многоточечных

интерфейсов для соединений точка-множество точек настраивается сеть типа OSPF, однако это приведет к тому, что OSPF добавит маршруты хоста в таблицы маршрутизации на оконечных маршрутизаторах. Маршруты этих хостов являются причиной того, что пакеты, предназначенные для сетей за другими оконечными маршрутизаторами, будут перенаправлены через концентратор вместо направления непосредственно к другой оконечной точке. Чтобы обойти эту проблему, настройте тип сети OSPF в качестве широковещательного с помощью команды.

ip ospf network broadcast

Необходимо также убедиться, что маршрутизатор концентратора является выделенным маршрутизатором (DR) для сети IPsec+mGRE. Чтобы сделать это, установите для приоритета OSPF такие значения: на концентраторе — больше 1, а на оконечных сторонах — 0.

- Концентратор: **ip ospf priority 2**
- Луч: **ip ospf priority 0**

Одиночный концентратор DMVPN

Центральный маршрутизатор

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  ip ospf network broadcast ip ospf priority 2 delay
1000 tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address 172.17.0.1
255.255.255.0 ! interface Ethernet1 ip address
192.168.0.1 255.255.255.0 ! router ospf 1 network
10.0.0.0 0.0.0.255 area 0 network 192.168.0.0 0.0.0.255
area 0 !
```

Единственное изменение конфигурации концентратора – это протокол маршрутизации OSPF вместо EIGRP. Обратите внимание, что тип сети OSPF - широковещательный, уровень приоритета - 2. Установка широковещательного типа сети OSPF вынудит OSPF установить маршруты для сетей за лучевыми маршрутизаторами с помощью IP-адреса следующего перехода как туннельного адреса GRE для данного лучевого маршрутизатора.

Маршрутизатор Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.2 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp network-id 100000 ip nhrp holdtime
300 ip nhrp nhs 10.0.0.1 ip ospf network broadcast ip
ospf priority 0 delay 1000 tunnel source Ethernet0
tunnel mode gre multipoint tunnel key 100000 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
ip address dhcp hostname Spoke1 ! interface Ethernet1 ip
address 192.168.1.1 255.255.255.0 ! router ospf 1
network 10.0.0.0 0.0.0.255 area 0 network 192.168.1.0
0.0.0.255 area 0 !
```

Конфигурация для оконечных маршрутизаторов теперь очень похожа на конфигурацию для концентратора. Различия:

- Приоритет OSPF установлен на 0. Маршрутизаторы в топологии «звезда» не могут стать выделенным маршрутизатором для нешироковещательной сети с множественным доступом (NBMA) на основе протокола mGRE. Прямое статическое соединение со всеми оконечными маршрутизаторами предусмотрено только для центрального маршрутизатора. DR должен иметь доступ ко всем участникам сети NBMA.
- Для центрального маршрутизатора настроены одноадресное и многоадресное сопоставления NHRP.
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1 172.17.0.1 **В предыдущей конфигурации команда ip nhrp map multicast ... не использовалась, т. к. туннель GRE был двухточечным.** В этом случае многоадресные пакеты автоматически инкапсулируются через туннель в единственно возможное место назначения. Теперь необходимо использовать эту команду, т.к. туннель между лучами GRE стал многоточечным, и однозначного места назначения не существует.
- Когда оконечный маршрутизатор активируется, он должен инициировать туннель с концентратором, поскольку центральный маршрутизатор не имеет изначально какой-либо информации об оконечных маршрутизаторах, которые могут иметь динамические IP-адреса. Оконечные маршрутизаторы тоже настроены таким образом, что концентратор является их NHRP NHS.`ip nhrp nhs 10.0.0.1`При использовании вышеуказанной команды оконечный маршрутизатор отправляет пакеты регистрации NHRP через туннель mGRE+IPsec на центральный маршрутизатор через равные промежутки времени. Эти пакеты регистрации обеспечивают данные отображения

NHRP для оконечного устройства, необходимые маршрутизатору концентратора для туннелирования пакетов обратно маршрутизаторам оконечных устройств.

Маршрутизатор Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.3 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  ip ospf network broadcast ip ospf priority 0 delay
1000 tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke1 ! interface Ethernet1 ip address 192.168.3.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 0 network 192.168.2.0 0.0.0.255 area 0 !
```

Маршрутизатор Spoke <n>

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<n+1> 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  ip ospf network broadcast ip ospf priority 0 delay
1000 tunnel source Ethernet0 tunnel mode gre multipoint
```

```
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke<n> ! interface Ethernet1 ip address 192.168.<n>.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 0 network 192.168.<n>.0 0.0.0.255 area 0 !
```

Обратите внимание, что конфигурации всех оконечных маршрутизаторов схожи. Единственное различие - это IP-адреса локальных интерфейсов. Это помогает при разворачивании большого количества лучевых маршрутизаторов. Все конечные маршрутизаторы могут быть настроены одинаково, необходимо только добавить адреса локального IP-интерфейса.

На этом этапе обратите внимание на таблицы маршрутизации и таблицы соответствий NHRP на маршрутизаторах концентратора, луча1 и луча 2 для получения начальных условий (сразу после включения луча 1 и 2), а также условий после установления динамической связи между лучами 1 и 2.

Начальные условия

Информация по центральному маршрутизатору

```
Hub#show ip route 172.17.0.0/24 is subnetted, 1 subnets
C 172.17.0.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 C 192.168.0.0/24 is directly
connected, Ethernet1 O 192.168.1.0/24 [110/2] via
10.0.0.2, 00:19:53, Tunnel0 O 192.168.2.0/24 [110/2] via
10.0.0.3, 00:19:53, Tunnel0 Hub#show ip nhrp 10.0.0.2/32
via 10.0.0.2, Tunnel0 created 00:57:27, expire 00:04:13
Type: dynamic, Flags: authoritative unique registered
NBMA address: 172.16.1.24 10.0.0.3/32 via 10.0.0.3,
Tunnel0 created 07:11:25, expire 00:04:33 Type: dynamic,
Flags: authoritative unique registered NBMA address:
172.16.2.75 Hub#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 204
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 205
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 2628
Tunnel0 10.0.0.1 set HMAC_MD5 0 402 2629 Tunnel0
10.0.0.1 set HMAC_MD5 357 0 2630 Tunnel0 10.0.0.1 set
HMAC_MD5 0 427 2631 Tunnel0 10.0.0.1 set HMAC_MD5 308 0
```

Информация о маршрутизаторе Spoke1

```
Spoke1#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.1.24 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 O 192.168.0.0/24 [110/2] via
10.0.0.1, 00:31:46, Tunnel0 C 192.168.1.0/24 is directly
connected, Ethernet1 O 192.168.2.0/24 [110/2] via
10.0.0.3, 00:31:46, Tunnel0 Spoke1#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:42:00,
never expire Type: static, Flags: authoritative used
NBMA address: 172.17.0.1 Spoke1#show crypto engine
connection active ID Interface IP-Address State
Algorithm Encrypt Decrypt 2 Ethernet0 172.16.1.24 set
HMAC_SHA+DES_56_CB 0 0 2064 Tunnel0 10.0.0.2 set
HMAC_MD5 0 244 2065 Tunnel0 10.0.0.2 set HMAC_MD5 276 0
```

Сведения маршрутизатора Spoke2

```
Spoke2#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.2.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
```

```
directly connected, Tunnel0 O 192.168.0.0/24 [110/2] via
10.0.0.1, 00:38:52, Tunnel0 O 192.168.1.0/24 [110/2] via
10.0.0.2, 00:38:52, Tunnel0 C 192.168.2.0/24 is directly
connected, Ethernet1 Spoke2#show ip nhrp 10.0.0.1/32 via
10.0.0.1, Tunnel0 created 01:32:10, never expire Type:
static, Flags: authoritative used NBMA address:
172.17.0.1 Spoke2#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
17 Ethernet0 172.16.2.75 set HMAC_SHA+DES_56_CB 0 0 2070
Tunnel0 10.0.0.3 set HMAC_MD5 0 279 2071 Tunnel0
10.0.0.3 set HMAC_MD5 316 0
```

На этом шаге проверяется доступность адресата от 192.168.1.2 на 192.168.2.3. Эти адреса предназначены для хостов за маршрутизаторами Spoke1 и Spoke2 соответственно. Приведенная далее последовательность событий обеспечивает организацию прямого туннеля mGRE+IPsec между лучами.

1. Маршрутизатор Spoke1 получает пакет эхо-запроса с адресом назначения 192.168.2.3. Он ищет место назначения в таблице маршрутизации и обнаруживает, что должен передать этот пакет за пределы интерфейса Tunnel0 на IP-адрес следующего перехода, 10.0.0.3.
2. Оконечный маршрутизатор 1 проверяет таблицу коммутации NHRP для 10.0.0.3 и обнаруживает отсутствие входа. Маршрутизатор луча 1 создаёт ответный пакет разрешения NHRP и посылает его на NHS (маршрутизатор концентратора).
3. Маршрутизатор-концентратор проверяет по таблице сопоставления NHRP адрес назначения 10.0.0.3 и обнаруживает, что он сопоставлен с адресом 172.16.2.75. Маршрутизатор Hub создаёт ответный пакет разрешения NHRP и посылает его на маршрутизатор Spoke1.
4. Маршрутизатор Spoke1 получает ответ решения NHRP, и это вводит 10.0.0.3 —> 172.16.2.75 сопоставления в его таблице NHRP - маршрутизации. Включение IPSec-триггеров сопоставления NHRP для инициации туннельного соединения с одноранговым узлом 172.16.2.75.
5. Маршрутизатор луча 1 активизирует ISAKMP с адресом 172.16.2.75 и настраивает связь между ISAKMP и IPsec SAs. IPSEC прокси получен из **команды tunnel source <address>** Tunnel0 и NHRP - маршрутизации.
   local ident (addr/mask/prot/port): (172.16.1.24/255.255.255.255/47/0) remote ident (addr/mask/prot/port): (172.16.2.75/255.255.255.255/47/0)
6. При завершении организации туннеля IPsec все последующие пакеты данных, поступающие к подсети 192.168.2.0/24, будут передаваться напрямую к лучу 2.
7. После пересылки на узел пакета, предназначенного для 192.168.2.3, этот хост вышлет обратный пакет на 192.168.1.2. Когда маршрутизатор Spoke2 получает этот пакет, предназначенный для 192.168.1.2, он будет искать этот адрес в таблице маршрутизации и обнаружит, что необходимо переадресовать этот пакет через интерфейс Tunnel0 на следующий IP-адрес пересылки, 10.0.0.2.
8. Маршрутизатор Spoke2 проверяет таблицу коммутации NHRP для 10.0.0.2 и обнаруживает отсутствие записи. Маршрутизатор луча 2 создаёт ответный пакет разрешения NHRP и посылает его на NHS (маршрутизатор концентратора).
9. Маршрутизатор концентратора проверяет по таблице сопоставления NHRP адрес назначения 10.0.0.2 и обнаруживает, что он сопоставлен с адресом 172.16.1.24. Центральный маршрутизатор создает пакет ответа NHRP разрешение и отсылает его маршрутизатору на конце луча 2.

10. Маршрутизатор Spoke2 получает ответ решения NHRP, и это вводит 10.0.0.2 —> 172.16.1.24 сопоставления в его таблице NHRP - маршрутизации. Добавление сопоставления NHRP инициирует создание туннеля IPsec с узлом 172.16.1.24, но такой туннель уже существует, поэтому дальнейшие действия не требуются.
11. Лучи 1 и 2 могут теперь пересылать друг другу пакеты напрямую. Если для пересылки пакетов на протяжении периода удержания сопоставление NHRP не используется, сопоставление NHRP будет удалено. Удаление записи сопоставления NHRP инициирует удаление IPsec SA для этого прямого подключения.

Условия после установки динамического канала между оконечными устройствами Spoke1 и Spoke2

Информация о маршрутизаторе Spoke1

```
Spoke1#show ip nhrp 10.0.0.1/32 via 10.0.0.1, Tunnel0
created 02:34:16, never expire Type: static, Flags:
authoritative used NBMA address: 172.17.0.1 10.0.0.3/32
via 10.0.0.3, Tunnel0 created 00:00:05, expire 00:03:35
Type: dynamic, Flags: router unique used NBMA address:
172.16.2.75 Spoke1#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
2 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB 0 0 3
Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB 0 0 2064
Tunnel0 10.0.0.2 set HMAC_MD5 0 375 2065 Tunnel0
10.0.0.2 set HMAC_MD5 426 0 2066 Tunnel0 10.0.0.2 set
HMAC_MD5 0 20 2067 Tunnel0 10.0.0.2 set HMAC_MD5 19 0
```

Сведения маршрутизатора Spoke2

```
Spoke2#show ip nhrp 10.0.0.1/32 via 10.0.0.1, Tunnel0
created 02:18:25, never expire Type: static, Flags:
authoritative used NBMA address: 172.17.0.1 10.0.0.2/32
via 10.0.0.2, Tunnel0 created 00:00:24, expire 00:04:35
Type: dynamic, Flags: router unique used NBMA address:
172.16.1.24 Spoke2#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
17 Ethernet0 172.16.2.75 set HMAC_SHA+DES_56_CB 0 0 18
Ethernet0 172.16.2.75 set HMAC_SHA+DES_56_CB 0 0 2070
Tunnel0 10.0.0.3 set HMAC_MD5 0 407 2071 Tunnel0
10.0.0.3 set HMAC_MD5 460 0 2072 Tunnel0 10.0.0.3 set
HMAC_MD5 0 19 2073 Tunnel0 10.0.0.3 set HMAC_MD5 20 0
```

Из приведенного выше примера видно, что Spoke1 и Spoke2 получили NHRP-сопоставления друг друга от маршрутизатора Hub, и они построили и используют туннель mGRE+IPsec. Срок действия сопоставлений NHRP закончится через пять минут (текущее значение времени хранения NHRP = 300 секунд). Если сопоставления NHRP используются в течение последней минуты, то будет послан запрос и ответ разрешения NHRP для обновления значения до его удаления. Иначе, схема NHRP будет уничтожена и будет инициирована IPsec очистка.

VPN с динамическим многоточечным IPsec с двумя концентраторами

Добавив несколько строк настройки на лучевые маршрутизаторы, можно установить маршрутизаторы двух (и больше) концентраторов (для избыточности). Существует 2 способа настроить DMVPN с двумя концентраторами.

- Одиночная сеть DMVPN, в которой каждый луч использует одиночный одноточечный интерфейс туннеля GRE и которая указывает на два разных концентратора как на ее сервер следующего перехода (NHS).На маршрутизаторе с функциями концентратора предусмотрен только один многоточечный туннельный интерфейс GRE.
- Двойные сети DMVPN, где у каждой есть оконечное оборудование с двумя туннельными интерфейсами GRE (или двухточечный, или многоточечный), а каждый туннель GRE подключен к различным маршрутизаторам-концентраторам.Снова, на маршрутизаторе концентратора предусмотрен только один многоточечный туннельный интерфейс GRE.

В следующих примерах приведены настройки этих двух сценариев для сетей DMVPN с двумя концентраторами. В обоих случаях выделены отличия от конфигурации DMVPN с одним концентратором.

Схема "Двойной концентратор – одинарный DMVPN"

Система с двумя концентраторами и одной сетью DMVPN достаточно проста в настройке, однако в ней не обеспечивается управление маршрутизацией по сети DMVPN такого уровня, как в системах с двумя концентраторами и двумя сетями DMVPN. Главная идея заключается в том, чтобы иметь единое «облако» DMVPN со всеми концентраторами (в данном случае с двумя) и подключить все лучи к этой одиночной сети («облаку»). Статическое NHRP-сопоставление оконечных устройств и концентраторов определяет статический канал IPsec+mGRE, в котором выполняется протокол динамической маршрутизации. Динамический протокол маршрутизации не будет выполняться в динамической линии связи IPsec+mGRE между оконечными устройствами. Поскольку лучевые маршрутизаторы маршрутизируют соседей с маршрутизаторами концентраторов через тот же туннельный интерфейсй mGRE, то нельзя использовать различия настройки интерфейсов (такие как полоса пропускания, стоимость и задержка) и канала для изменения метрики протокола динамической маршрутизации, чтобы предпочесть один концентратор другому, когда они работают оба. Если это предпочтение необходимо, следует использовать внутренние методы для настройки протокола маршрутизации. Поэтому в качестве протокола динамической маршрутизации лучше использовать EIGRP или RIP, а не OSPF.

Примечание: Эта проблема характерна только для расположенных рядом концентраторов. В противном случае при стандартной динамической маршрутизации будет выбран правильный маршрутизатор-концентратор, даже если доступ к сети назначения возможен и через другой маршрутизатор-концентратор.

Схема "Двойной концентратор – одинарный DMVPN"

Центральный маршрутизатор
version 12.3 ! hostname Hub1 ! crypto isakmp policy 1 authentication pre-share crypto isakmp key cisco47 address 0.0.0.0 ! crypto ipsec transform-set trans2 esp-des esp-md5-hmac mode transport ! crypto ipsec profile vpnprof set transform-set trans2 !

```
 interface Tunnel0
  bandwidth 1000 ip address 10.0.0.1 255.255.255.0 ip
mtu 1400 ip nhrp authentication test ip nhrp map
multicast dynamic ip nhrp network-id 100000 ip nhrp
holdtime 600 ip ospf network broadcast ip ospf priority
2 delay 1000 tunnel source Ethernet0 tunnel mode gre
multipoint tunnel key 100000 tunnel protection ipsec
profile vpnprof ! interface Ethernet0 ip address
172.17.0.1 255.255.255.0 ! interface Ethernet1 ip
address 192.168.0.1 255.255.255.0 ! router ospf 1
network 10.0.0.0 0.0.0.255 area 1 network 192.168.0.0
0.0.0.255 area 0 !
```

Маршрутизатор-концентратор2

```
version 12.3
 !
 hostname Hub2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 900 ip address 10.0.0.2 255.255.255.0 ip mtu
1400 ip nhrp authentication test ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp map multicast 172.17.0.1 ip nhrp map
multicast dynamic ip nhrp network-id 100000 ip nhrp
holdtime 600 ip nhrp nhs 10.0.0.1 ip ospf network
broadcast ip ospf priority 1 delay 1000 tunnel source
Ethernet0 tunnel mode gre multipoint tunnel key 100000
tunnel protection ipsec profile vpnprof ! interface
Ethernet0 ip address 172.17.0.5 255.255.255.0 !
interface Ethernet1 ip address 192.168.0.2 255.255.255.0
! router ospf 1 network 10.0.0.0 0.0.0.255 area 1
network 192.168.0.0 0.0.0.255 area 0 !
```

Единственное различие в настройке концентратора 1 - это использование OSPF двух областей. Область 0 закреплена за сетью, находящейся позади двух концентраторов, а область 1 – за сетью DMVPN и сетями позади лучевых маршрутизаторов. OSPF мог бы использовать одну область, но для демонстрации конфигурации для нескольких областей OSPF в этом примере использовались две области.

Конфигурация концентратора 2 в основном совпадает с конфигурацией концентратора 1 при изменениях соответствующего IP-адреса. Главное отличие состоит в том, что концентратор 2 также является лучом (или клиентом) концентратора 1; т.е. концентратор 1 является главным, а концентратор 2 - дополнительным. Это сделано для того, чтобы концентратор 2 стал соседом OSPF, и концентратор 1 работал черех туннель mGRE. Поскольку концентратор 1 – это выделенный маршрутизатор OSPF DR, он должен иметь прямое соединение со всеми другими маршрутизаторам OSPF через интерфейс mGRE (сеть NBMA). Без наличия прямой связи между концентраторами 1 и 2 концентратор 2 не сможет участвовать в маршрутизации OSPF при работающем концентраторе 1. Когда отключается концентратор 1, концентратор 2 выступает в роли OSPF DR для DMVPN (сеть NBMA). При повторном включении концентратора 1 он снова станет главным, будучи маршрутизатором назначения OSPF для сети DMVPN.

Маршрутизаторы за концентратором 1 и концентратором 2 будут использовать концентратор 1 для передачи пакетов лучевым сетям, поскольку пропускная способность интерфейса туннеля GRE установлена на 1000 Кб/сек, что больше, чем у концентратора 2. Оконечные маршрутизаторы, напротив, отправляют пакеты, предназначенные для сетей за маршрутизаторами, на Hub1 и Hub2, т. к. на каждом оконечном маршрутизаторе есть только один туннельный интерфейс mGRE и два равноценных маршрута. Использование балансировки нагрузки по пакетам может привести к нарушению последовательности пакетов.

Маршрутизатор Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp map multicast 172.17.0.5 ip nhrp map
10.0.0.2 172.17.0.5 ip nhrp network-id 100000 ip nhrp
holdtime 300 ip nhrp nhs 10.0.0.1 ip nhrp nhs 10.0.0.2
ip ospf network broadcast ip ospf priority 0 delay 1000
tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke1 ! interface Ethernet1 ip address 192.168.1.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 1 network 192.168.1.0 0.0.0.255 area 1 !
```

Различие в конфигурации оконечных маршрутизаторов следующее:

- Оконечный маршрутизатор в новой конфигурации настроен со статическими сопоставлениями NHRP для концентратора 2, и концентратор 2 добавлен как сервер следующего перехода.Исходный:
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1 172.17.0.1 ip nhrp nhs 10.0.0.1
  Новый:
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1 172.17.0.1 ip nhrp map multicast 172.17.0.5 ip nhrp map 10.0.0.2 172.17.0.5 ip nhrp nhs 10.0.0.1 ip nhrp nhs 10.0.0.2
- Области OSPF для оконечных маршрутизаторов были изменены на область 1.

Как вы помните, определение статического отображения NHRP и сервера NHS на маршрутизаторе оконечного узла для концентратора необходимо для того, чтобы обеспечить работу протокола динамической маршрутизации в этом туннеле. Это определяет концентратор и оконечную маршрутизацию или соседнюю сеть. Учтите, что концентратор 2 используется для всех конечных устройств и сам является конечным устройством для концентратора 1. Это облегчает проектирование, настройку и изменение

сетей со структурой "звезда" при использовании решений DMVPN (динамических многоотводных виртуальных частных сетей).

Маршрутизатор Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.12 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp map multicast 172.17.0.5 ip nhrp map
10.0.0.2 172.17.0.5 ip nhrp network-id 100000 ip nhrp
holdtime 300 ip nhrp nhs 10.0.0.1 ip nhrp nhs 10.0.0.2
ip ospf network broadcast ip ospf priority 0 delay 1000
tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke1 ! interface Ethernet1 ip address 192.168.2.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 0 network 192.168.2.0 0.0.0.255 area 0 !
```

Маршрутизатор Spoke <n>

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<n+10> 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp map multicast 172.17.0.5 ip nhrp map
10.0.0.2 172.17.0.5 ip nhrp network-id 100000 ip nhrp
holdtime 300 ip nhrp nhs 10.0.0.1 ip nhrp nhs 10.0.0.2
ip ospf network broadcast ip ospf priority 0 delay 1000
tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
```

```
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke<x> ! interface Ethernet1 ip address 192.168.<n>.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 0 network 192.168.<n>.0 0.0.0.255 area 0 !
```

На этом этапе обратите внимание на таблицы маршрутизации, таблицы соответствий NHRP и соединения IPsec на маршрутизаторах концентратора 1 и 2, луча1 и 2 для получения начальных условий (сразу после включения луча 1 и 2).

Начальные условия и изменения

Информация маршрутизатора концентратора 1

```
Hub1#show ip route 172.17.0.0/24 is subnetted, 1 subnets
C 172.17.0.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 C 192.168.0.0/24 is directly
connected, Ethernet1 O 192.168.1.0/24 [110/2] via
10.0.0.11, 00:02:17, Tunnel0 O 192.168.2.0/24 [110/2]
via 10.0.0.12, 00:02:17, Tunnel0 Hub1#show ip nhrp
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 1w3d, expire
00:03:15 Type: dynamic, Flags: authoritative unique
registered NBMA address: 172.17.0.5 10.0.0.11/32 via
10.0.0.11, Tunnel0 created 1w3d, expire 00:03:49 Type:
dynamic, Flags: authoritative unique registered NBMA
address: 172.16.1.24 10.0.0.12/32 via 10.0.0.12, Tunnel0
created 1w3d, expire 00:04:06 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.2.75 Hub1#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 4
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 5
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 6
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 3532
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 232 3533
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 212 0 3534
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 18 3535
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 17 0 3536
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 7 3537 Tunnel0
10.0.0.1 set HMAC_MD5+DES_56_CB 7 0
```

Данные о концентраторе 2 маршрутизатора

```
Hub2#show ip route 172.17.0.0/24 is subnetted, 1 subnets
C 172.17.0.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 C 192.168.0.0/24 is directly
connected, Ethernet1 O 192.168.1.0/24 [110/2] via
10.0.0.11, 00:29:15, Tunnel0 O 192.168.2.0/24 [110/2]
via 10.0.0.12, 00:29:15, Tunnel0 Hub2#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 1w3d, never
expire Type: static, Flags: authoritative used NBMA
address: 172.17.0.1 10.0.0.11/32 via 10.0.0.11, Tunnel0
created 1w3d, expire 00:03:15 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.1.24 10.0.0.12/32 via 10.0.0.12, Tunnel0 created
00:46:17, expire 00:03:51 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.2.75 Hub2#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 4
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 5
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 6
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 3520
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 0 351 3521
```

```
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 326 0 3522
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 0 311 3523
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 339 0 3524
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 0 25 3525
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 22 0
```

Информация о маршрутизаторе Spoke1

```
Spoke1#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.1.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 O IA 192.168.0.0/24 [110/11]
via 10.0.0.1, 00:39:31, Tunnel0 [110/11] via 10.0.0.2,
00:39:31, Tunnel0 C 192.168.1.0/24 is directly
connected, Ethernet1 O 192.168.2.0/24 [110/2] via
10.0.0.12, 00:37:58, Tunnel0 Spoke1#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 00:56:40,
never expire Type: static, Flags: authoritative used
NBMA address: 172.17.0.1 10.0.0.2/32 via 10.0.0.2,
Tunnel0 created 00:56:40, never expire Type: static,
Flags: authoritative used NBMA address: 172.17.0.5
Spoke1#show crypto engine connection active ID Interface
IP-Address State Algorithm Encrypt Decrypt 1 Ethernet0
172.16.1.24 set HMAC_SHA+DES_56_CB 0 0 2 Ethernet0
172.16.1.24 set HMAC_SHA+DES_56_CB 0 0 2010 Tunnel0
10.0.0.11 set HMAC_MD5+DES_56_CB 0 171 2011 Tunnel0
10.0.0.11 set HMAC_MD5+DES_56_CB 185 0 2012 Tunnel0
10.0.0.11 set HMAC_MD5+DES_56_CB 0 12 2013 Tunnel0
10.0.0.11 set HMAC_MD5+DES_56_CB 13 0
```

Сведения маршрутизатора Spoke2

```
Spoke2#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.2.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 O IA 192.168.0.0/24 [110/11]
via 10.0.0.1, 00:57:56, Tunnel0 [110/11] via 10.0.0.2,
00:57:56, Tunnel0 O 192.168.1.0/24 [110/2] via
10.0.0.11, 00:56:14, Tunnel0 C 192.168.2.0/24 is
directly connected, Ethernet1 Spoke2#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 5w6d, never
expire Type: static, Flags: authoritative used NBMA
address: 172.17.0.1 10.0.0.2/32 via 10.0.0.2, Tunnel0
created 6w6d, never expire Type: static, Flags:
authoritative used NBMA address: 172.17.0.5 Spoke2#show
crypto engine connection active ID Interface IP-Address
State Algorithm Encrypt Decrypt 2 Ethernet0 172.16.2.75
set HMAC_SHA+DES_56_CB 0 0 3 Ethernet0 172.16.2.75 set
HMAC_SHA+DES_56_CB 0 0 3712 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 0 302 3713 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 331 0 3716 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 0 216 3717 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 236 0
```

Существует несколько интересных пунктов по таблицам маршрутизации на Hub1, Hub2, Spoke1 и Spoke2:

- У обоих маршрутизаторов-концентраторов стоимости маршрутов к сетям после оконечных маршрутизаторов равны.Hub1:`O 192.168.1.0/24 [110/2] via 10.0.0.11, 00:02:17, Tunnel0`

  `O 192.168.2.0/24 [110/2] via 10.0.0.12, 00:02:17, Tunnel0`Hub2:`O 192.168.1.0/24 [110/2] via 10.0.0.11, 00:29:15, Tunnel0`

  `O 192.168.2.0/24 [110/2] via 10.0.0.12, 00:29:15, Tunnel0`Это означает, что Hub1 и

Hub2 будут объявлять одну и ту же стоимость для сетей с оконечными маршрутизаторами тем маршрутизаторам, которые входят в сеть с концентраторами. Например, таблица маршрутизации на маршрутизаторе R2, который связан непосредственно с локальной сетью 192.168.0.0/24, выглядит следующим образом:R2:O IA 192.168.1.0/24 [110/12] via 192.168.0.1, 00:00:26, Ethernet1/0/3
[110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/3O O IA 192.168.2.0/24 [110/12] via 192.168.0.1, 00:00:27, Ethernet1/0/3
[110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/3

- Оконечные маршрутизаторы имеют равные стоимости маршрутов через оба маршрутизатора-концентратора к сетям после маршрутизаторов-концентраторов.Spoke1:O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:39:31, Tunnel0
[110/11] via 10.0.0.2, 00:39:31, Tunnel0Spoke2:O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:57:56, Tunnel0
[110/11] via 10.0.0.2, 00:57:56, Tunnel0Выполнение оконечными маршрутизаторами попакетного распределения нагрузки может привести к появлению поврежденных пакетов.

Чтобы избежать асимметричной маршрутизации или попакетного распределения нагрузки через связи к двум концентраторам, нужно так настроить протокол маршрутизации, чтобы был предпочтительным один путь к от оконечного устройства к концентратору в обоих направлениях. Если необходимо настроить концентратор 1 в качестве основного и концентратор 2 в качестве резервного, необходимо установить различные значения стоимости OSPF для туннельных интерфейсов концентраторов.

Hub1:

```
interface tunnel0
...
ip ospf cost 10
...
```

Hub2:

```
interface tunnel0
...
ip ospf cost 20
...
```

Теперь маршруты выглядят следующим образом:

Hub1:

```
O     192.168.1.0/24 [110/11] via 10.0.0.11, 00:00:28, Tunnel0
O     192.168.2.0/24 [110/11] via 10.0.0.12, 00:00:28, Tunnel0
```

Hub2:

```
O     192.168.1.0/24 [110/21] via 10.0.0.11, 00:00:52, Tunnel0
O     192.168.2.0/24 [110/21] via 10.0.0.12, 00:00:52, Tunnel0
```

R2:

```
O     IA 192.168.1.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
O     IA 192.168.2.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
```

Два маршрутизатора-концентратора имеют различные стоимости на маршрутах для сетей за конечными маршрутизаторами. Это означает, что концентратор 1 будет более предпочтительным для передачи трафика на лучевые маршрутизаторы, что видно на маршрутизаторе R2. Это решит описанную выше проблему асимметричной маршрутизации.

Здесь по-прежнему используется асимметричная маршрутизация в другом направлении, как описано во втором пункте выше. **При использовании OSPF в качестве динамического протокола маршрутизации, эту проблему можно решить обходным путем, воспользовавшись командой distance ... в маршрутизаторе ospf1 на оконечных устройствах для оказания предпочтения маршрутам, полученным через концентратор Hub1, а не маршрутам, полученным через концентратор Hub2.**

Spoke1:

```
router ospf 1
 distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

Spoke2:

```
router ospf 1
 distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

Теперь маршруты выглядят следующим образом:

Spoke1:

```
O     192.168.0.0/24 [110/11] via 10.0.0.1, 00:00:06, Tunnel0
```

Spoke2:

```
O     192.168.1.0/24 [110/11] via 10.0.0.1, 00:00:10, Tunnel0
```

Вышеописанная конфигурация маршрутизатора обеспечивает защиту от асимметричной маршрутизации, при этом разрешая аварийное переключение на Hub2 при отказе Hub1. Это означает, что при двух работающих концентраторах используется только Hub1. Если вы хотите использовать оба концентратора путем балансировки оконечных устройств по концентраторам, с функцией обхода отказа и без асимметричной маршрутизации, то конфигурация маршрутизации может усложниться, особенно при использовании OSPF. Поэтому рекомендуется предпочесть следующий двойной концентратор с двойной DMVPN.

Системы с двумя концентраторами – топология двойной динамической многоточечной виртуальной частной сети (DMVPN)

Систему с двумя коммутаторами с топологией двойной динамической многоточечной виртуальной частной сети (DMVPN) несколько сложнее настроить, но она дает больший контроль над маршрутизацией через DMVPN. Основная идея заключается в том, чтобы иметь два раздельных «облака» DMVPN. Каждый концентратор (в данном случае два) будет подключен к одной подсети DMVPN ("облаку"), а маршрутизаторы на конце луча будут подключены к обеим подсетям DMVPN ("облакам"). Поскольку оконечные маршрутизаторы маршрутизируют соседей с маршрутизаторами-концентраторами через два туннельных интерфейса GRE, можно использовать различия конфигурации интерфейсов (такие как полоса пропускания, стоимость и задержка), изменяя метрики протокола динамической маршрутизации, чтобы предпочесть один концентратор другому, когда они работают оба.

Примечание: Вышеуказанная проблема возникает только если центральные маршрутизаторы размещены рядом друг с другом. В противном случае при стандартной динамической маршрутизации будет выбран правильный маршрутизатор-концентратор, даже если доступ к сети назначения возможен и через другой маршрутизатор-концентратор.

На оконечных маршрутизаторах можно использовать туннельные интерфейсы - либо p-pGRE, либо mGRE. **Многоточечный интерфейс p-pGRE на лучевом маршрутизаторе может использовать тот же IP-адрес источника туннеля ... Но многоточечные интерфейсы mGRE на лучевом маршрутизаторе должны иметь уникальный IP-адрес источника туннеля ...** IP-адрес. Это связано с тем, что при инициации IPSec первым передается пакет ISAKMP, который должен быть связан с одним из туннелей mGRE. Пакет ISAKMP имеет только IP-адрес назначения (адрес удаленного однорангового узла IPsec), с которым следует выполнять это сопоставление. **Этот адрес сравнивается с адресом источника туннеля, однако поскольку у обоих туннелей один и тот же адрес источника туннеля, интерфейс первого туннеля mGRE всегда будет ему соответствовать.** Это значит, что входящие многоадресные пакеты данных могут быть связаны с неправильным mGRE интерфейсом, разрушая любой протокол динамической маршрутизации.

Сами пакеты GRE лишены этой проблемы, так как используют значение ... туннельного ключа, чтобы различать два интерфейса mGRE. Начиная с Cisco IOS выпуск 12.3(5) и 12.3(7)T, в ПО был добавлен новый параметр для преодоления этого ограничения: **защита туннеля....общая. Слово общая означает, что множественные интерфейсы mGRE будут использовать шифрование IPSec с тем же IP-адресом источника.** При использовании более ранних версий ПО можно использовать туннели p-pGRE в системе с двумя концентраторами с двойной DMVPN. **В случае туннеля p-pGRE источник туннеля и IP-адрес пункта назначения туннеля могут быть использованы для согласования. В этом примере туннели p-pGRE будут использоваться с двумя концентраторами и с двойной DMVPN; классификатор shared не используется.**

Системы с двумя концентраторами – топология двойной динамической многоточечной виртуальной частной сети (DMVPN)

Следующие выделенные изменения связаны с настройками динамического многоточечного концентратора и оконечного устройства, ранее показанными в этом документе.

Маршрутизатор Ядро1

```
version 12.3
 !
 hostname Hub1 ! crypto isakmp policy 1 authentication
pre-share crypto isakmp key cisco47 address 0.0.0.0
0.0.0.0 ! crypto ipsec transform-set trans2 esp-des esp-
md5-hmac mode transport ! crypto ipsec profile vpnprof
set transform-set trans2 ! interface Tunnel0 bandwidth
1000 ip address 10.0.0.1 255.255.255.0 ip mtu 1400 ip
nhrp authentication test ip nhrp map multicast dynamic
ip nhrp network-id 100000 ip nhrp holdtime 600 no ip
split-horizon eigrp 1 delay 1000 tunnel source Ethernet0
tunnel mode gre multipoint tunnel key 100000 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
ip address 172.17.0.1 255.255.255.252 ! interface
Ethernet1 ip address 192.168.0.1 255.255.255.0 ! router
eigrp 1 network 10.0.0.0 0.0.0.255 network 192.168.0.0
0.0.0.255 no auto-summary !
```

Маршрутизатор-концентратор2

```
version 12.3
 !
 hostname Hub2 ! crypto isakmp policy 1 authentication
pre-share crypto isakmp key cisco47 address 0.0.0.0
0.0.0.0 ! crypto ipsec transform-set trans2 esp-des esp-
md5-hmac mode transport ! crypto ipsec profile vpnprof
set transform-set trans2 ! interface Tunnel0 bandwidth
1000 ip address 10.0.1.1 255.255.255.0 ip mtu 1400 ip
```

```
nhrp authentication test ip nhrp map multicast dynamic
ip nhrp network-id 100001 ip nhrp holdtime 600 no ip
split-horizon eigrp 1 delay 1000 tunnel source Ethernet0
tunnel mode gre multipoint tunnel key 100001 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
ip address 172.17.0.5 255.255.255.252 ! interface
Ethernet1 ip address 192.168.0.2 255.255.255.0 ! router
eigrp 1 network 10.0.1.0 0.0.0.255 network 192.168.0.0
0.0.0.255 no auto-summary !
```

В этом случае настройки концентраторов 1 и 2 похожи. Главное отличие состоит в том, что они являются концентраторами разных DMVPN. Каждая DMVPN использует различные:

- Подсеть IP (10.0.0.0/24, 10.0.0.1/24)
- Идентификатор сети NHRP (100000, 100001)
- Ключ туннеля (100000, 100001)

Протокол динамической маршрутизации был переключен с OSPF на EIGRP, поскольку настройка и управление сети NBMA с помощью EIGRP упрощаются, как описано в этом документе в дальнейшем.

Маршрутизатор Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0 bandwidth 1000 ip address 10.0.0.11
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000
ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000
tunnel source Ethernet0 tunnel destination 172.17.0.1
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Tunnel1 bandwidth 1000 ip address
10.0.1.11 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.1.1 172.17.0.5 ip
nhrp network-id 100001 ip nhrp holdtime 300 ip nhrp nhs
10.0.1.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.5 tunnel key 100001 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
ip address dhcp hostname Spoke1 ! interface Ethernet1 ip
address 192.168.1.1 255.255.255.0 ! router eigrp 1
network 10.0.0.0 0.0.0.255 network 10.0.1.0 0.0.0.255
network 192.168.1.0 0.0.0.255 no auto-summary !
```

Каждый из маршрутизаторов оконечного устройства настроен с двумя туннельными интерфейсами p-pGRE, по одному в каждой из двух DMVPN. **Значения ip address ..., ip nhrp network-id ..., tunnel key ... и tunnel destination ... используются для разделения двух туннелей.** Протокол динамической маршрутизации, EIGRP, выполняется на обеих подсетях туннеля p-pGRE и используется для выбора одного интерфейса p-pGRE interface (DMVPN) посредством другого.

Маршрутизатор Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0 bandwidth 1000 ip address 10.0.0.12
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000
ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000
tunnel source Ethernet0 tunnel destination 172.17.0.1
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Tunnel1 bandwidth 1000 ip address
10.0.1.12 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.1.1 172.17.0.5 ip
nhrp network-id 100001 ip nhrp holdtime 300 ip nhrp nhs
10.0.1.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.5 tunnel key 100001 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
ip address dhcp hostname Spoke2 ! interface Ethernet1 ip
address 192.168.2.1 255.255.255.0 ! router eigrp 1
network 10.0.0.0 0.0.0.255 network 10.0.1.0 0.0.0.255
network 192.168.2.0 0.0.0.255 no auto-summary !
```

Маршрутизатор Spoke <n>

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0 bandwidth 1000 ip address
10.0.0.<n+10> 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.0.1 172.17.0.1 ip
nhrp network-id 100000 ip nhrp holdtime 300 ip nhrp nhs
10.0.0.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.1 tunnel key 100000 tunnel
protection ipsec profile vpnprof ! interface Tunnel1
bandwidth 1000 ip address 10.0.1.<n+10> 255.255.255.0 ip
mtu 1400 ip nhrp authentication test ip nhrp map
10.0.1.1 172.17.0.5 ip nhrp network-id 100001 ip nhrp
holdtime 300 ip nhrp nhs 10.0.1.1 delay 1000 tunnel
source Ethernet0 tunnel destination 172.17.0.5 tunnel
key 100001 tunnel protection ipsec profile vpnprof !
interface Ethernet0 ip address dhcp hostname Spoke<x> !
interface Ethernet1 ip address 192.168.<n>.1
```

```
255.255.255.0 ! router eigrp 1 network 10.0.0.0
0.0.0.255 network 10.0.1.0 0.0.0.255 network
192.168.<n>.0 0.0.0.255 no auto-summary !
```

На этом этапе обратите внимание на таблицы маршрутизации, таблицы соответствий NHRP и соединения IPsec на маршрутизаторах концентратора 1 и 2, луча1 и 2 для получения начальных условий (сразу после включения луча 1 и 2).

Начальные условия и изменения

Информация маршрутизатора концентратора 1

```
Hub1#show ip route 172.17.0.0/30 is subnetted, 1 subnets
C 172.17.0.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets C 10.0.0.0 is
directly connected, Tunnel0 D 10.0.1.0 [90/2611200] via
192.168.0.2, 00:00:46, Ethernet1 C 192.168.0.0/24 is
directly connected, Ethernet1 D 192.168.1.0/24
[90/2841600] via 10.0.0.11, 00:00:59, Tunnel0 D
192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:00:34,
Tunnel0 Hub1#show ip nhrp 10.0.0.12/32 via 10.0.0.12,
Tunnel0 created 23:48:32, expire 00:03:50 Type: dynamic,
Flags: authoritative unique registered NBMA address:
172.16.2.75 10.0.0.11/32 via 10.0.0.11, Tunnel0 created
23:16:46, expire 00:04:45 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.1.24 Hub1#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 15
Ethernet0 172.17.63.18 set HMAC_SHA+DES_56_CB 0 0 16
Ethernet0 10.0.0.1 set HMAC_SHA+DES_56_CB 0 0 2038
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 759 2039
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 726 0 2040
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 37 2041
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 36 0
```

Данные о концентраторе 2 маршрутизатора

```
Hub2#show ip route 172.17.0.0/30 is subnetted, 1 subnets
C 172.17.0.4 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets D 10.0.0.0
[90/2611200] via 192.168.0.1, 00:12:22, Ethernet1 C
10.0.1.0 is directly connected, Tunnel0 C 192.168.0.0/24
is directly connected, Ethernet1 D 192.168.1.0/24
[90/2841600] via 10.0.1.11, 00:13:24, Tunnel0 D
192.168.2.0/24 [90/2841600] via 10.0.1.12, 00:12:11,
Tunnel0 Hub2#show ip nhrp 10.0.1.12/32 via 10.0.1.12,
Tunnel3 created 06:03:24, expire 00:04:39 Type: dynamic,
Flags: authoritative unique registered NBMA address:
172.16.2.75 10.0.1.11/32 via 10.0.1.11, Tunnel3 created
23:06:47, expire 00:04:54 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.1.24 Hub2#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 4
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 6
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 2098
Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 0 722 2099
Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 690 0 2100
Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 0 268 2101
Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 254 0
```

Информация о маршрутизаторе Spoke1

```
Spoke1#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.1.0 is directly connected, Ethernet0
```

```
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 C 10.0.1.0 is directly
connected, Tunnel1 D 192.168.0.0/24 [90/2841600] via
10.0.1.1, 00:26:30, Tunnel1 [90/2841600] via 10.0.0.1,
00:26:30, Tunnel0 C 192.168.1.0/24 is directly
connected, Ethernet1 D 192.168.2.0/24 [90/3097600] via
10.0.1.1, 00:26:29, Tunnel1 [90/3097600] via 10.0.0.1,
00:26:29, Tunnel0 Spoke1#show ip nhrp 10.0.0.1/32 via
10.0.0.1, Tunnel0 created 23:25:46, never expire Type:
static, Flags: authoritative NBMA address: 172.17.0.1
10.0.1.1/32 via 10.0.1.1, Tunnel1 created 23:24:40,
never expire Type: static, Flags: authoritative NBMA
address: 172.17.0.5 Spoke1#show crypto engine connection
active ID Interface IP-Address State Algorithm Encrypt
Decrypt 16 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB
0 0 18 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB 0 0
2118 Tunnel0 10.0.0.11 set HMAC_MD5+DES_56_CB 0 181 2119
Tunnel0 10.0.0.11 set HMAC_MD5+DES_56_CB 186 0 2120
Tunnel1 10.0.1.11 set HMAC_MD5+DES_56_CB 0 105 2121
Tunnel1 10.0.1.11 set HMAC_MD5+DES_56_CB 110 0
```

Сведения маршрутизатора Spoke2

```
Spoke2#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.2.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets C 10.0.0.0 is
directly connected, Tunnel0 C 10.0.1.0 is directly
connected, Tunnel1 D 192.168.0.0/24 [90/2841600] via
10.0.1.1, 00:38:04, Tunnel1 [90/2841600] via 10.0.0.1,
00:38:04, Tunnel0 D 192.168.1.0/24 [90/3097600] via
10.0.1.1, 00:38:02, Tunnel1 [90/3097600] via 10.0.0.1,
00:38:02, Tunnel0 C 192.168.2.0/24 is directly
connected, Ethernet1 Spoke2#show ip nhrp 10.0.0.1/32 via
10.0.0.1, Tunnel0 created 1d02h, never expire Type:
static, Flags: authoritative used NBMA address:
172.17.0.1 10.0.1.1/32 via 10.0.1.1, Tunnel1 created
1d02h, never expire Type: static, Flags: authoritative
used NBMA address: 172.17.0.5 Spoke2#show crypto engine
connection active ID Interface IP-Address State
Algorithm Encrypt Decrypt 8 Ethernet0 172.16.2.75 set
HMAC_SHA+DES_56_CB 0 0 9 Ethernet0 172.16.2.75 set
HMAC_SHA+DES_56_CB 0 0 2036 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 0 585 2037 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 614 0 2038 Tunnel1 10.0.1.12 set
HMAC_MD5+DES_56_CB 0 408 2039 Tunnel1 10.0.1.12 set
HMAC_MD5+DES_56_CB 424 0
```

Следует отметить несколько особенностей, касающихся таблиц маршрутизации на маршрутизаторах Hub1, Hub2, Spoke1 и Spoke2:

- У обоих маршрутизаторов-концентраторов стоимости маршрутов к сетям после оконечных маршрутизаторов равны.Hub1:`D 192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:00:59, Tunnel0`

  `D 192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:00:34, Tunnel0`Hub2:`D 192.168.1.0/24 [90/2841600] via 10.0.1.11, 00:13:24, Tunnel0`

  `D 192.168.2.0/24 [90/2841600] via 10.0.1.12, 00:12:11, Tunnel0`Это означает, что Hub1 и Hub2 будут объявлять одну и ту же стоимость для сетей с оконечными маршрутизаторами тем маршрутизаторам, которые входят в сеть с концентраторами. Например, таблица маршрутизации на маршрутизаторе R2, который связан непосредственно с локальной сетью 192.168.0.0/24, выглядит следующим образом:R2:`D 192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:51:51, Ethernet1/0/3`

```
                            [90/2867200] via 192.168.0.2, 00:51:51, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:52:43, Ethernet1/0/3
                    [90/2867200] via 192.168.0.1, 00:52:43, Ethernet1/0/3
```

- Оконечные маршрутизаторы имеют равные стоимости маршрутов через оба маршрутизатора-концентратора к сетям после маршрутизаторов-концентраторов.Spoke1:`D    192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:26:30, Tunnel1`
  `[90/3097600] via 10.0.0.1, 00:26:30, Tunnel0`Spoke2:`D 192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:38:04, Tunnel1`
  `[90/3097600] via 10.0.0.1, 00:38:04, Tunnel0`Выполнение оконечными маршрутизаторами попакетного распределения нагрузки может привести к появлению поврежденных пакетов.

Чтобы избежать асимметричной маршрутизации или попакетного распределения нагрузки через связи к двум концентраторам, нужно так настроить протокол маршрутизации, чтобы был предпочтительным один путь к от оконечного устройства к концентратору в обоих направлениях. Если необходимо настроить концентратор 1 в качестве основного и концентратор 2 в качестве резервного, необходимо установить различные значения задержки для туннельных интерфейсов концентраторов.

Hub1:

```
interface tunnel0
...
delay 1000
...
```

Hub2:

```
interface tunnel0
...
delay 1050
...
```

Примечание: В этом примере к задержке на интерфейсе туннеля на Hub2 было добавлено 50, потому что она меньше задержки на интерфейсе Ethernet1 (100) между этими двумя концентраторами. Сделав это, Hub2 еще будет напрямую пересылать пакеты маршрутизаторам на концах лучей, но он будет менее желательным, нежели маршрут от Hub1 к маршрутизаторам за Hub1 и Hub2. Если задержка увеличится более, чем на 100, то концентратор 2 будет передавать пакеты для лучевых маршрутизаторов с помощью концентратора 1 через интерфейс Ethernet1, хотя маршрутизаторы за концентраторами 1 и 2 будут по-прежнему предпочитать концентратор 1 для передачи пакетов.

Теперь маршруты выглядят следующим образом:

Hub1:

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:01:11, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:01:11, Tunnel0
```

Hub2:

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:00:04, Tunnel0
D    192.168.2.0/24 [90/2854400] via 10.0.1.12, 00:00:04, Tunnel0
```

R2:

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
```

Два центральных маршрутизатора имеют разный приоритет при сетевой маршрутизации к

оконечным маршрутизаторам, в этом случае, Hub1 будет более предпочтителен для пересылки трафика оконечным маршрутизаторам, как можно увидеть на R2. Это решает проблему, описанную выше в первом пункте.

Проблема, описанная выше во втором абзаце, все еще сохраняется, но так как у вас два туннельных интерфейса p-pGRE, вы можете настроить для них различные значения задержки, чтобы изменить метрику EIGRP для маршрутов, сведения о которых поступают от концентратора-1 (Hub1) и от концентратора-2. (Hub2).

Spoke1:

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

Spoke2:

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

Теперь маршруты выглядят следующим образом:

Spoke1:

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:15:44, Tunnel0
D    192.168.2.0/24 [90/3097600] via 10.0.0.1, 00:15:44, Tunnel0
```

Spoke2:

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:13:54, Tunnel0
D    192.168.1.0/24 [90/3097600] via 10.0.0.1, 00:13:54, Tunnel0
```

Вышеописанная конфигурация маршрутизатора обеспечивает защиту от асимметричной маршрутизации, при этом разрешая аварийное переключение на Hub2 при отказе Hub1. Это означает, что при двух работающих концентраторах используется только Hub1.

Если вы хотите использовать оба концентратора путем балансировки лучевых устройств по концентраторам, с функцией обхода отказа и без асимметричной маршрутизации, то настройка маршрутизации может усложниться; но вы можете это сделать при использовании EIGRP. Для выполнения этого установите **задержку...** на туннельных интерфейсах маршрутизаторов концентратора назад к тому, чтобы быть равным и затем используйте **команду offset-list <acl> out <offset> <interface>** на маршрутизаторах на конце луча для увеличения, метрика EIGRP для маршрутов объявила Туннельные интерфейсы GRE к резервному концентратору. **Неравная задержка для интерфейсов Tunnel0 и Tunnel1 оконечного устройства сохраняется, поэтому маршрутизатор оконечного устройства выберет основной концентратор.** На оконечных маршрутизаторах требуются следующие изменения.

Маршрутизатор Spoke1
version 12.3 ! hostname Spoke1 ! ... ! interface Tunnel0

```
  bandwidth 1000
  ip address 10.0.0.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000 tunnel source Ethernet0 tunnel destination
172.17.0.1 tunnel key 100000 tunnel protection ipsec
profile vpnprof ! interface Tunnel1 bandwidth 1000 ip
address 10.0.1.11 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.1.1 172.17.0.5 ip
nhrp network-id 100001 ip nhrp holdtime 300 ip nhrp nhs
10.0.1.1 delay 1500 tunnel source Ethernet0 tunnel
destination 172.17.0.5 tunnel key 100001 tunnel
protection ipsec profile vpnprof ! ... ! router eigrp 1
offset-list 1 out 12800 Tunnel1 network 10.0.0.0
0.0.0.255 network 10.0.1.0 0.0.0.255 network 192.168.1.0
distribute-list 1 out no auto-summary ! access-list 1
permit 192.168.1.0 !
```

Маршрутизатор Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 ...
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.12 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1500 tunnel source Ethernet0 tunnel destination
172.17.0.1 tunnel key 100000 tunnel protection ipsec
profile vpnprof ! interface Tunnel1 bandwidth 1000 ip
address 10.0.1.12 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.1.1 172.17.0.5 ip
nhrp network-id 100001 ip nhrp holdtime 300 ip nhrp nhs
10.0.1.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.5 tunnel key 100001 tunnel
protection ipsec profile vpnprof ! ... ! router eigrp 1
offset-list 1 out 12800 Tunnel1 network 10.0.0.0
0.0.0.255 network 10.0.1.0 0.0.0.255 network 192.168.2.0
distribute-list 1 out no auto-summary ! access-list 1
permit 192.168.2.0 !
```

Примечание: Значение сдвига 12800 (50*256) было добавлено к метрике EIGRP, потому что это меньше, чем 25600 (100*256). Это значение (25600) – то, что добавляется к метрике EIGRP для маршрутов, полученных между маршрутизаторами концентратора. **Используя значение 12800 в команде offset-list , дополнительный маршрутизатор концентратора будет напрямую направлять пакеты лучевым маршрутизаторам посредством Ethernet через главный для этих лучей маршрутизатор концентратора.** Метрика на маршрутах, объявляемых узловыми маршрутизаторами, такова, что предпочтение отдается основному узловому маршрутизатору. Помните, что у половины периферийных устройств основным маршрутизатором является Hub1, а у другой половины основным маршрутизатором

является Hub2.

Примечание: Если значение смещения превысило 25600 (100*256), концентраторы направят пакеты половине маршрутизаторов на конце луча через другой концентратор через интерфейс Ethernet1, даже если маршрутизаторы после концентраторов по-прежнему предпочитают, чтобы пакеты отправлял правильный концентратор.

Примечание: Также была добавлена команда distribute-list 1 out, так как существует вероятность того, что маршруты, полученные от одного центрального концентратора через туннельный интерфейс на оконечном устройстве, могли быть объявлены в обратную сторону для другого концентратора через другой туннель. Команда distribute-list гарантирует, что конечный маршрутизатор может объявлять лишь собственные маршруты.

Примечание: Если вы предпочитаете управлять рекламными объявлениями маршрутизации на маршрутизаторах концентратора, а не на маршрутизаторах на конце луча, то **offset-list <acl1> в <interface> <value>** и **командах distribute-list <acl2> in** может быть настроен на маршрутизаторах концентратора вместо на лучах. <acl2> access-list перечислил бы маршруты из-за всех лучей, и <acl1> access-list перечислит только маршруты из-за лучей, где другой маршрутизатор концентратора должен быть первичным концентратором.

Теперь маршруты выглядят следующим образом:

Hub1:

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:12:11, Tunnel2
D    192.168.2.0/24 [90/2854400] via 10.0.0.12, 00:13:24, Tunnel2
```

Hub2:

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:09:58, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.10.1.12, 00:11:11, Tunnel0
```

R2:

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:13:13, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:14:25, Ethernet1/0/3
```

Spoke1:

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:16:12, Tunnel0
```

Spoke2:

```
D    192.168.0.0/24 [90/2841600] via 10.0.1.1, 00:18:54, Tunnel1
```

Заключение

Решение DMVPN обеспечивает следующую функциональность для лучшего масштабирования больших и малых сетей IPsec VPN.

- DMVPN обеспечивает лучшее масштабирование в полно-связанных и частично-связанных сетях IPsec VPNs.Оно особенно полезно при наличии нерегулярного трафикамежду лучами (например, каждый луч отсылает данные на другие лучи не постоянно). Оно позволяет каждому лучу напрямую посылать данные на любой другой луч при наличии прямого IP-соединения между лучами.
- DMVPN поддерживает узлы IPsec с динамически присвоенными номерами (такие как Cable, ISDN и DSL).Это применимо к сетям как с топологией звезды, так и с ячеистой

топологией. Для DMVPN может понадобиться постоянно установленная связь между оконечными устройствами.

- DMVPN упрощает добавление узлов VPN.Чтобы добавить новый оконечный маршрутизатор, необходимо настроить его и подключить к сети (хотя, может потребоваться добавить информацию авторизации ISAKMP для нового оконечного маршрутизатора на концентраторе). Концентратор динамически запомнит новый луч, протокол динамической маршрутизации распространит информацию о маршрутизации на концентратор и остальные лучи.
- DMVPN уменьшает размер настройки, необходимой для всех маршрутизаторов сети VPN.Это также относится к сетям VPN GRE+IPsec с топологией "только звезда".
- DMVPN использует GRE и, таким образом, поддерживает IP-широковещание и динамическую маршрутизацию трафика через VPN.Это означает, что протокол динамической маршрутизации можно использовать, а избыточные концентраторы могут поддерживаться протоколом. Многоадресные приложения также поддерживаются.
- DMVPN поддерживает раздельное туннелирование на оконечных устройствах.

Дополнительные сведения

- Динамическая многоточечная VPN (DMVPN)
- Страница поддержки IPSec
- Техническая поддержка - Cisco Systems