

Миграция FlexVPN: твердое перемещение от DMVPN до FlexVPN на другом концентраторе

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Процедура миграции](#)

[Трудная миграция между двумя другими концентраторами](#)

[Пользовательский подход](#)

[Топология сети](#)

[Топология транспортной сети](#)

[Топология оверлейной сети](#)

[!--- конфигурацию](#)

[Конфигурация DMVPN](#)

[Лучевая конфигурация DMVPN](#)

[Конфигурация DMVPN концентратора](#)

[Конфигурация FlexVPN](#)

[Говорил конфигурацию FlexVPN](#)

[Конфигурация концентратора FlexVPN](#)

[Миграция трафика](#)

[Мигрируйте на BGP как \[рекомендуемый\] протокол маршрутизации наложения](#)

[Лучевой BGP - конфигурация](#)

[BGP - конфигурация концентратора](#)

[Переместите трафик на BGP/FlexVPN](#)

[Мигрируйте на новые туннели с EIGRP](#)

[Обновленная конфигурация оконечного устройства](#)

[Обновленная конфигурация концентратора FlexVPN](#)

[Концентратор DMVPN - обновленный BGP - конфигурация](#)

[Концентратор FlexVPN - обновленный BGP - конфигурация](#)

[Переместите трафик на FlexVPN](#)

[Этапы проверки](#)

[Дополнительные замечания](#)

[Туннели конечного маршрутизатор - конечного маршрутизатора, которые Уже Существуют](#)

[Очистите записи NHRP](#)

[Известные предупреждения](#)

[Дополнительные сведения](#)

Введение

Этот документ предоставляет сведения о том, как мигрировать от сети Динамической многоточечной VPN (DMVPN), которая в настоящее время существует к FlexVPN на других устройствах концентратора. Конфигурации для обеих платформ сосуществуют на устройствах. В этом документе только наиболее распространенный сценарий показывают - DMVPN с использованием общего ключа для аутентификации и Протокола EIGRP как протокол маршрутизации. В этом документе продемонстрирована миграция к Протоколу BGP, который является рекомендуемым протоколом маршрутизации, и менее - выбираемый EIGRP.

Предварительные условия

Требования

Cisco рекомендует иметь базовые знания об этих темах:

- DMVPN
- FlexVPN

Используемые компоненты

Примечание: Не вся вторая версия протокола Internet Key Exchange (IKEv2) поддерживает программных и аппаратных средств. См. [Cisco Feature Navigator](#) для получения дополнительной информации.

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия 15.2 (4) M1 маршрутизатора с интеграцией служб (ISR) Cisco или более новый
- Маршрутизатор агрегации Cisco, серии 1000 (ASR1K) 3.6.2 Выпусков 15.2 (2) S2 или более новый

Один преимущества более новой платформы и программного обеспечения способность использовать Криптографию Следующего поколения, такую как Расширенный стандарт шифрования (AES) Режим Галуа/Счетчика (GCM) для шифрования в протоколе IPSEC (Internet Protocol Security) (IPsec), как обсуждено в Запросе на комментарий (RFC) 4106. AES GCM позволяет вам достигать намного более быстрой скорости шифрования на некоторых аппаратных средствах. Для наблюдения Рекомендаций Cisco на использовании и миграции к Криптографии Следующего поколения, обратитесь к [статье Encryption Следующего поколения](#).

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Процедура миграции

В настоящее время рекомендуемый метод для миграции от DMVPN до FlexVPN для этих двух платформ для не работы в то же время. Это ограничение планируется, чтобы быть удаленным из-за новых функций миграции, которые будут представлены в Выпуске ASR 3.10, отслеженном под multiple запросами на расширение на стороне Cisco, которые включают идентификатор ошибки Cisco [CSCuc08066](#). Те функции должны быть доступными в конце июня 2013.

Миграция, где обе платформы сосуществуют и воздействуют в то же время на те же устройства, упоминается как **мягкая миграция**, которая указывает на минимальное воздействие и плавное аварийное переключение от одной платформы до другого. Миграция, где конфигурации для обеих платформ сосуществуют, но не работают в то же время, упоминается как **трудная миграция**. Это указывает что переключатель с одной платформы на другое средство отсутствие связи по VPN, даже если минимальный.

Трудная миграция между двумя другими концентраторами

В этом документе обсуждена миграция от концентратора DMVPN, который в настоящее время используется к новому концентратору FlexVPN. Эта миграция уже позволяет общение между лучами, перемещенными на FlexVPN и тех, которые все еще работают на DMVPN и могут быть выполнены во множественных фазах на каждом луче отдельно.

При условии, что сведения о маршрутизации должным образом заполнены, связь между перемещенными и неперемещенными лучами должна остаться возможной. Однако дополнительная задержка может наблюдаться, потому что перемещенные и неперемещенные лучи не создают туннели конечного маршрутизатор - конечного маршрутизатора друг между другом. В то же время перемещенные лучи должны быть в состоянии установить прямые туннели конечного маршрутизатор - конечного маршрутизатора между собой. То же применяется к неперемещенным лучам.

Пока эта новая функция миграции не доступна, выполните эти шаги для выполнения миграций с другим концентратором от DMVPN и FlexVPN:

1. Проверьте подключение по DMVPN.
2. Добавьте конфигурацию FlexVPN и завершите работу туннеля, который принадлежит новой конфигурации.
3. (Во время периода технического обслуживания) На каждом луче, один за другим, завершает работу туннеля DMVPN.
4. На том же луче как в Шаге 3, незакрытом туннельные интерфейсы FlexVPN.
5. Проверьте подключение оконечного устройства - концентратора.
6. Проверьте подключение конечного маршрутизатор - конечного маршрутизатора в FlexVPN.
7. Проверьте подключение конечного маршрутизатор - конечного маршрутизатора с DMVPN от FlexVPN.
8. Повторите Шаги 3 - 7 для каждого луча отдельно.
9. Если вы встречаетесь с какими-либо проблемами с проверками, описанными в Шагах 5, 6, или 7, завершаете работу интерфейса FlexVPN, и незакрытый интерфейсы DMVPN для возвращения к DMVPN.

10. Проверьте связь оконечного устройства - концентратора по выполнившей резервное копирование DMVPN.
11. Проверьте связь конечного маршрутизатор - конечного маршрутизатора по выполнившей резервное копирование DMVPN.

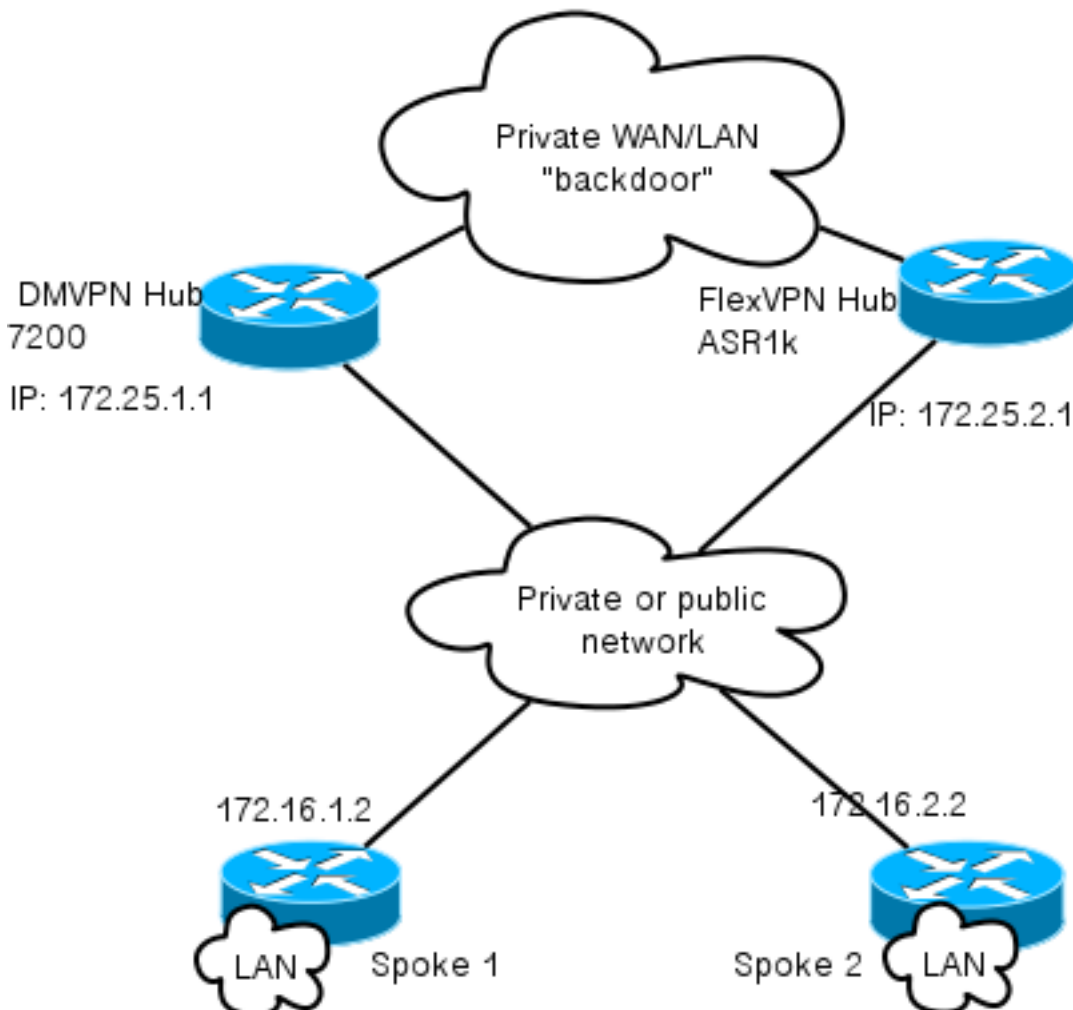
Пользовательский подход

Если предыдущий подход не мог бы быть лучшим решением для вас из-за вашей сети или сложностей маршрутизации, запустите обсуждение со своим представителем Cisco перед миграцией. Лучший человек, с которым можно обсудить пользовательский процесс переноса, является вашим Системным инженером или Инженером Расширенных сервисов.

Топология сети

Топология транспортной сети

Эта схема показывает типичную топологию соединения хостов в Интернете. IP-адрес концентратора `loopback0` (`172.25.1.1`) используется для завершения Сеанса IPsec DMVPN. IP-адрес на новом концентраторе (`172.25.2.1`) используется для FlexVPN.

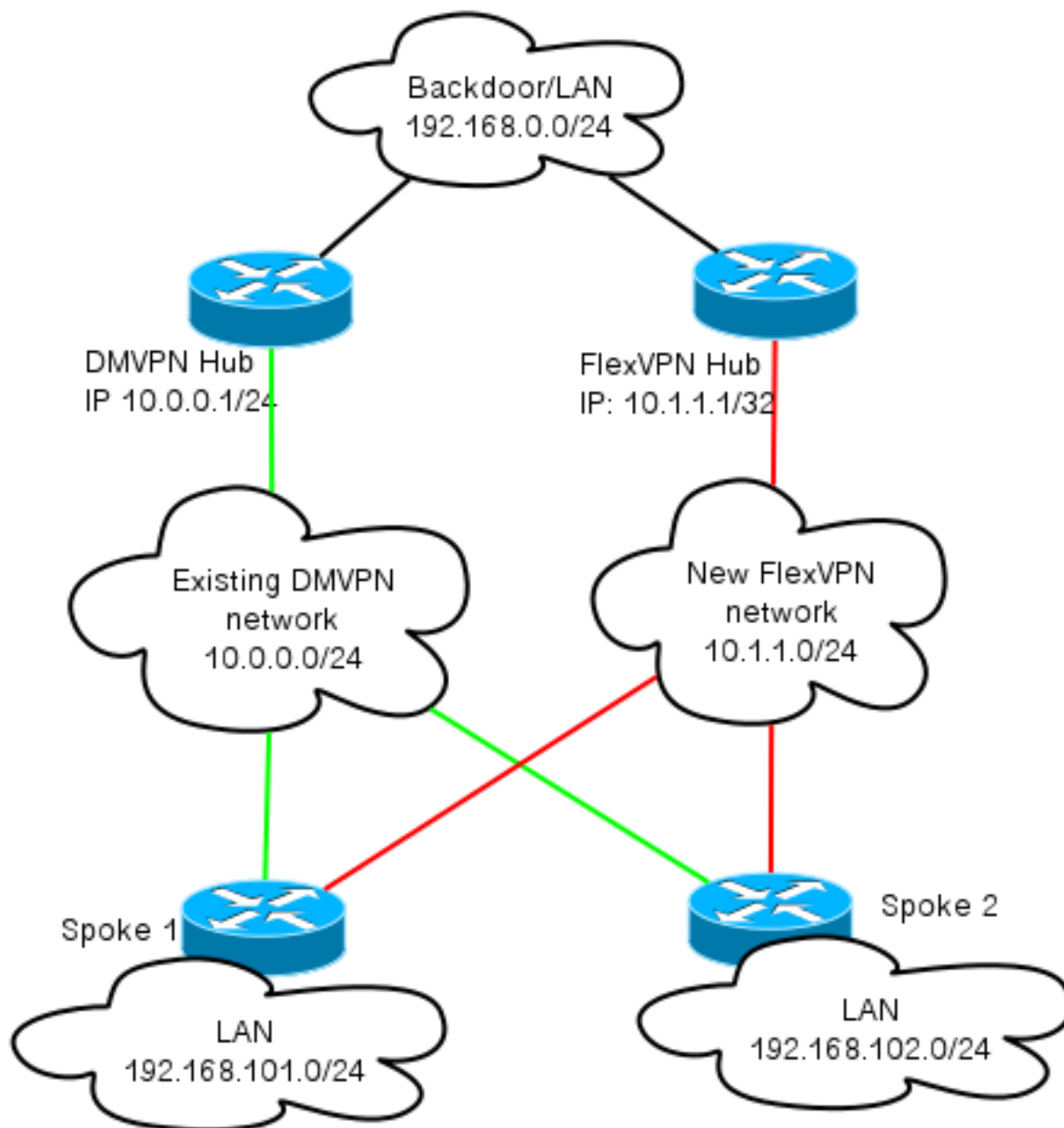


Заметьте ссылку между двумя концентраторами. Эта ссылка крайне важна для разрешения подключения между FlexVPN и облаками DMVPN во время миграции. Это позволяет лучам,

уже перемещенным на FlexVPN связываться с сетями DMVPN и наоборот.

Топология оверлейной сети

Эта схема топологии показывает два отдельных облака, используемые для наложения: DMVPN (зеленые соединения) и FlexVPN (красные соединения). Префиксы LAN показывают для соответствующих узлов. 10.1.1.0/24 подсеть не представляет реальную подсеть с точки зрения интерфейсной адресации, но представляет блок пространства IP, выделенного облаку FlexVPN. Объяснение позади этого обсуждено позже в **Разделе конфигурации FlexVPN**.



!--- конфигурацию

В этом разделе описываются DMVPN и конфигурации FlexVPN.

Конфигурация DMVPN

В этом разделе описываются базовую конфигурацию для концентратора DMVPN и луча.

Предварительный общий ключ (PSK) используется для аутентификации IKEv1. Как только IPsec установлен, регистрация Протокола NHRP от оконечного устройства - концентратора выполнена так, чтобы концентратор мог изучить Нешироковещательный множественный доступ лучей (NBMA), обращающийся динамично.

Когда NHRP выполняет регистрацию на луче, и концентратор, направляя смежность может установить, и маршрутами можно обменяться. В данном примере EIGRP используется в качестве протокола базовой маршрутизации для оверлейной сети.

Лучевая конфигурация DMVPN

Здесь можно найти конфигурацию базового примера DMVPN с аутентификацией PSK и EIGRP как протокол маршрутизации.

```
crypto isakmp policy 10
  encr aes
  authentication pre-share

crypto isakmp key cisco address 0.0.0.0

crypto isakmp keepalive 30 5

crypto isakmp profile DMVPN_IKEv1
  keyring DMVPN_IKEv1
  match identity address 0.0.0.0

crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
  mode transport

crypto ipsec profile DMVPN_IKEv1
  set transform-set IKEv1
  set isakmp-profile DMVPN_IKEv1

interface Tunnel0

ip address 10.0.0.101 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map 10.0.0.1 172.25.1.1
ip nhrp map multicast 172.25.1.1
ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp nhs 10.0.0.1
ip nhrp shortcut
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN_IKEv1

router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.102.0
passive-interface default
no passive-interface Tunnel0
```

Конфигурация DMVPN концентратора

В конфигурации концентратора туннель получен от **loopback0** с IP-адресом **172.25.1.1**. Остальное - стандартное развертывание концентратора DMVPN с EIGRP как протокол маршрутизации.

```
crypto isakmp policy 10
encr aes
authentication pre-share

crypto isakmp key cisco address 0.0.0.0

crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
mode transport
crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1

interface Tunnel0
ip address 10.0.0.1 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp server-only
ip nhrp redirect
ip summary-address eigrp 100 192.168.0.0 255.255.0.0
ip tcp adjust-mss 1360
tunnel source Loopback0
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN_IKEv1

router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel0
```

Конфигурация FlexVPN

FlexVPN основывается на этих тех же фундаментальных технологиях:

- **IPSec:** В отличие от по умолчанию в DMVPN, IKEv2 используется вместо IKEv1 для согласования о Сопоставлениях безопасности IPSec (SA). IKEv2 предлагает улучшения по сравнению с IKEv1, такие как упругость и количество сообщений, которые необходимы для установления канала защищенных данных.
- **GRE:** В отличие от DMVPN, статические и динамические интерфейсы точка-точка используются, а не только один статический multipoint интерфейс GRE. Эта конфигурация позволяет добавленную гибкость, специально для per-spoke/per-hub поведения.
- **NHRP:** В FlexVPN NHRP прежде всего используется для установления связи конечного маршрутизатор - конечного маршрутизатора. Слицы не регистрируются к концентратору.
- **Маршрутизация:** Поскольку лучи не выполняют регистрацию NHRP к концентратору, необходимо полагаться на другие механизмы для проверки, концентратор и лучи могут

связаться двунаправленным образом. Similiar к DMVPN, протоколы динамической маршрутизации могут использоваться. Однако FlexVPN позволяет вам использовать IPsec для представления сведений о маршрутизации. По умолчанию должен представить как /32 маршрут для IP-адреса с другой стороны туннеля, который позволяет прямое соединение оконечного устройства - концентратора.

В трудной миграции от DMVPN до FlexVPN два frameworks не работают в то же время на те же устройства. Однако рекомендуется разделить их.

Разделите их на нескольких уровнях:

- NHRP - Использование другой ID сети NHRP (рекомендовано).
- При маршрутизации - (рекомендованы) процессы отдельной маршрутизации Использования.
- Виртуальная маршрутизация и Передача (VRF) - Разделение VRF позволяет добавленную гибкость, но не обсуждено здесь (дополнительное).

Говорил конфигурацию FlexVPN

Одно из различий в конфигурации оконечного устройства в FlexVPN по сравнению с DMVPN - то, что у вас потенциально есть два интерфейса. Существует требуемый туннель для связи оконечного устройства - концентратора и дополнительный туннель для туннелей конечного маршрутизатор - конечного маршрутизатора. Если бы вы принимаете решение не иметь динамическое туннелирование конечного маршрутизатор - конечного маршрутизатора и предпочли бы, чтобы все прошло устройство концентратора, можно удалить интерфейс виртуального шаблона и удалить ярлык NHRP, переключающийся из туннельного интерфейса.

Заметьте, что статический туннельный интерфейс получает IP-адрес на основе согласования. Это позволяет концентратору предоставлять IP-адрес туннельного интерфейса лучу динамично без потребности создать статическую адресацию в облаке FlexVPN.

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 profile Flex_IKEv2
match identity remote fqdn domain cisco.com
local identity fqdn spoke.cisco.com
authentication remote rsa-sig
authentication local rsa-sig
aaa authorization group cert list default default
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

Примечание: По умолчанию локальная идентичность приведена в порядок для использования IP-адреса. Таким образом, соответствующее сообщение о совпадении на узле должно совпасть на основе адреса также. Если требование должно совпасть на основе Составного имени (DN) в certificate, то соответствие должно быть сделано с использованием карты сертификата.

Cisco рекомендует использовать AES GCM с аппаратными средствами, которые поддерживают его.


```
crypto ipsec transform-set IKEv2 esp-gcm
mode transport
```

```
crypto ipsec profile default
set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
```

```
interface Tunnell
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
shutdown
tunnel source Ethernet0/0
tunnel destination 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

```
interface Virtual-Templatel type tunnel
ip unnumbered Tunnell
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

Инфраструктура открытых ключей (PKI) является рекомендуемым методом для выполнения широкомасштабной аутентификации в IKEv2. Однако можно все еще использовать PSK, пока вы знаете о его ограничениях.

Вот пример конфигурации, который использует Cisco в качестве PSK.

```
crypto ikev2 keyring Flex_key
peer Spokes
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco
pre-shared-key remote cisco
crypto ikev2 profile Flex_IKEv2
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local Flex_key
aaa authorization group psk list default default
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

Конфигурация концентратора FlexVPN

Как правило, концентратор только завершает динамические туннели оконечного устройства - концентратора. Это - то, почему вы не находите статический туннельный интерфейс для FlexVPN в конфигурации концентратора. Вместо этого интерфейс виртуального шаблона используется.

Примечание: На стороне концентратора необходимо указать на адреса пула, которые будут назначены на лучи.

Адреса от этого пула добавлены позже в таблице маршрутизации как/32 маршруты для каждого луча.

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 authorization policy default
pool FlexSpokes
crypto ikev2 profile Flex_IKEv2
match identity remote fqdn domain cisco.com
local identity fqdn hub.cisco.com
authentication remote rsa-sig
authentication local rsa-sig
aaa authorization group cert list default default
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

Cisco рекомендует использовать AES GCM с аппаратными средствами, которые поддерживают его.

```
crypto ipsec transform-set IKEv2 esp-gcm
mode transport
```

Примечание: В этой конфигурации AES была прокомментирована операция GCM.

```
crypto ipsec profile default
set ikev2-profile Flex_IKEv2
! set transform-set IKEv2

interface Loopback0
description DMVPN termination
ip address 172.25.2.1 255.255.255.255
interface Loopback100
ip address 10.1.1.1 255.255.255.255
interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip nhrp network-id 2
ip nhrp redirect
tunnel path-mtu-discovery
tunnel protection ipsec profile default
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

С аутентификацией в IKEv2 тот же принцип применяется на концентратор как на луче. Для масштабируемости и гибкости, используйте сертификаты. Однако можно снова использовать одинаковую конфигурацию для PSK как на луче.

Примечание: IKEv2 предлагает гибкость с точки зрения аутентификации. В то время как другая сторона использует Подпись Ривест-Шамир-Адлемана (RSA-СИГНАЛ), одна сторона может аутентифицироваться с PSK.

Если требование должно использовать общие ключи для аутентификации, то изменения конфигурации подобны описанным для маршрутизатора на конце луча [здесь](#).

Соединение BGP межконцентратора

Удостоверьтесь, что концентраторы знают, где расположены определенные префиксы. Это становится все более и более важным, потому что некоторые лучи были перемещены на

FlexVPN, в то время как некоторые другие лучи остаются на DMVPN.

Вот соединение BGP межконцентратора на основе конфигурации концентратора DMVPN:

```
router bgp 65001
network 192.168.0.0
neighbor 192.168.0.2 remote-as 65001
```

Миграция трафика

Мигрируйте на BGP как [рекомендуемый] протокол маршрутизации наложения

BGP является протоколом маршрутизации, который основывается на обмене индивидуальной рассылки. Из-за его характеристик, это - лучший протокол масштабирования в сетях DMVPN.

В данном примере используется Внутренний BGP (iBGP).

Лучевой BGP - конфигурация

Лучевая миграция состоит из двух частей. Во-первых, включите BGP как динамическую маршрутизацию:

```
router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
```

После того, как Соседний BGP узел подходит (см. следующий раздел), и новые префиксы по BGP изучены, можно качать трафик от текущего облака DMVPN до нового облака FlexVPN.

BGP - конфигурация концентратора

Концентратор FlexVPN - полный BGP - конфигурация

На концентраторе, во избежание хранения конфигурации соседства для каждого луча отдельно, настраивают динамических слушателей. В этой настройке BGP не иницирует новые соединения, но принимает соединения от предоставленного пула IP-адресов. В этом случае упомянутый пул является **10.1.1.0/24**, который является всеми адресами в новом облаке FlexVPN.

Два момента, которых необходимо отметить:

- Концентратор FlexVPN объявляет определенные префиксы к концентратору DMVPN; таким образом неподавлять карта используется.
- Или объявите подсеть FlexVPN **10.1.1.0/24** к таблице маршрутизации или удостоверьтесь, что концентратор DMVPN рассматривает концентратор FlexVPN как

следующий переход.

Этот документ показывает последний подход.

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

router bgp 65001
network 192.168.0.0
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
aggregate-address 192.168.0.0 255.255.0.0 summary-only
neighbor Spokes peer-group
neighbor Spokes remote-as 65001

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

Концентратор DMVPN - полный BGP и конфигурация протокола EIGRP

Конфигурация на концентраторе DMVPN является основной, потому что это только получает определенные префиксы от концентратора FlexVPN и объявляет префиксы, которые это изучает из EIGRP.

```
router bgp 65001
bgp log-neighbor-changes
redistribute eigrp 100
neighbor 192.168.0.2 remote-as 65001
```

Переместите трафик на BGP/FlexVPN

Как обсуждено прежде, необходимо завершить работу функциональности DMVPN и перевести FlexVPN в рабочее состояние для выполнения миграции.

Эта процедура гарантирует минимальное воздействие:

1. На каждом луче, отдельно, введите это:

```
interface tunnel 0
shut
```

На этом этапе удостоверьтесь, что существуют сеансы № IKEv1, установленные к этому лучу. Это может быть проверено при проверке выходных данных **команды show crypto isakmp sa** и сообщений системного журнала монитора, генерируемых командой **сеанса crypto logging**. Как только это подтверждено, можно продолжить переводить FlexVPN в рабочее состояние.

2. На том же луче введите это:

```
interface tunnel 1
no shut
```

Этапы проверки

Устойчивость IPsec

Лучший способ оценить устойчивость IPsec состоит в том, чтобы контролировать sylogs с выполненной командой **конфигурации сеанса crypto logging**. Если вы видите сеансы, которые идут вверх и вниз, это может указать на проблему на уровне IKEv2/FlexVPN, который должен быть исправлен, прежде чем миграция может начаться.

Заполненная информация BGP

Если IPsec стабилен, удостоверьтесь, что таблица BGP заполнена с записями от лучей (на концентраторе) и сводка от концентратора (на лучах). В случае BGP это может быть просмотрено с этими командами:

```
show bgp
! or
show bgp ipv4 unicast
! or
show ip bgp summary
```

Вот пример корректной информации от концентратора FlexVPN:

```
BGP router identifier 172.25.2.1, local AS number 65001
(...omitted...)
```

```
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.100 4 65001 112 123 16 0 0 01:35:58 1
192.168.0.1 4 65001 97 99 16 0 0 01:24:12 4
```

Выходные данные показывают, что концентратор изучил один префикс из каждого из лучей, и оба луча являются динамическими и отмечены звездочкой (*) знак. Это также показывает, что получены в общей сложности четыре префикса от межсоединения концентратора.

Вот пример подобной информации от луча:

```
show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)
```

```
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
```

Луч получил два префикса от концентратора. В случае этой настройки один префикс должен быть сводкой, объявленной на концентраторе FlexVPN. Другой сеть **DMVPN 10.0.0.0/24**, перераспределенная на луче DMVPN в BGP.

Мигрируйте на новые туннели с EIGRP

EIGRP является популярным выбором в сетях DMVPN из-за его относительно простого развертывания и быстрой конвергенции. Однако это масштабируется хуже, чем BGP и не предлагает много усовершенствованных механизмов, которые могут использоваться BGP прямо из коробки. Следующий раздел описывает один из способов переместиться в FlexVPN с новым процессом EIGRP.

Обновленная конфигурация оконечного устройства

Новая Автономная система (AS) добавлена с отдельным процессом EIGRP:

```
router eigrp 200
network 10.1.1.0 0.0.0.255
network 192.168.101.0
passive-interface default
no passive-interface Tunnel1
```

Примечание: Лучше не установить смежность протокола маршрутизации по туннелям конечного маршрутизатор - конечного маршрутизатора. Поэтому только сделайте интерфейс **tunnel1** (оконечное устройство - концентратор) не пассивный.

Обновленная конфигурация концентратора FlexVPN

Точно так же для концентратора FlexVPN, подготовьте протокол маршрутизации в appropriate AS, совпав с одним настроенным на лучах.

```
router eigrp 200
network 10.1.1.0 0.0.0.255
```

Существует два метода, которые используются для обеспечения сводки назад к лучу.

- Перераспределите статический маршрут, который указывает к **null0** (предпочтительный вариант).

```
ip route 192.168.0.0 255.255.0.0 null 0
ip route 10.1.1.0 255.255.255.0 null 0
```

```
ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
ip prefix-list EIGRP_SUMMARY_ONLY seq 10 permit 10.1.1.0/24
```

```
route-map EIGRP_SUMMARY permit 20
match ip address prefix-list EIGRP_SUMMARY_ONLY
```

```
router eigrp 200
distribute-list route-map EIGRP_SUMMARY out Virtual-Template1
redistribute static metric 1500 10 10 1 1500 route-map EIGRP_SUMMARY
```

Эта опция позволяет контроль над сводкой и перераспределением без модификаций к конфигурации Технологии виртуализации (VT) концентратора. Это важно, потому что конфигурация VT концентратора не может модифицироваться, если существует активный виртуальный доступ, привязанный к ней.

- Установите сводный адрес стиля DMVPN на виртуальном шаблоне.

Эта конфигурация *не рекомендуется* из-за внутренней обработки и репликации сказанной сводки к каждому виртуальному доступу. Это показывают здесь для ссылки.

```
interface Virtual-Template1 type tunnel
ip summary-address eigrp 200 192.168.0.0 255.255.0.0
```

Другим аспектом для составления является обмен маршрутизации межконцентратора. Это может быть сделано при перераспределении экземпляров EIGRP к iBGP.

Концентратор DMVPN - обновленный BGP - конфигурация

Конфигурация остается основной. Необходимо перераспределить определенные префиксы от EIGRP до BGP:

```
router bgp 65001

redistribute eigrp 100

neighbor 192.168.0.2 remote-as 65001
```

Концентратор FlexVPN - обновленный BGP - конфигурация

Подобный концентратору DMVPN, в FlexVPN, необходимо перераспределить префиксы нового процесса EIGRP к BGP:

```
router bgp 65001

redistribute eigrp 200 redistribute static

neighbor 192.168.0.1 remote-as 65001
```

Переместите трафик на FlexVPN

Необходимо завершить работу функциональности DMVPN и перевести FlexVPN в рабочее состояние на каждом луче, по одному, для выполнения миграции. Эта процедура гарантирует минимальное влияние:

1. На каждом луче, отдельно, введите это:

```
interface tunnel 0
shut
```

На этом этапе удостоверьтесь, что существуют сеансы № IKEv1, установленные на этом луче. Это может быть проверено при проверке выходных данных **команды show crypto isakmp sa** и сообщений системного журнала монитора, генерируемых командой **сеанса crypto logging**. Как только это подтверждено, можно продолжить переводить FlexVPN в рабочее состояние.

2. На том же луче введите это:

```
interface tunnel 1
no shut
```

Этапы проверки

Устойчивость IPsec

Если IPsec стабилен, как в случае BGP, необходимо оценить. Лучший способ сделать так состоит в том, чтобы контролировать sylogs с выполненной командой **конфигурации сеанса crypto logging**. Если вы видите, что сеансы идут вверх и вниз, это может указать на проблему на уровне IKEv2/FlexVPN, который должен быть исправлен, прежде чем миграция может начаться.

Сведения EIGRP в таблице топологии

Удостоверьтесь, что ваша таблица топологии EIGRP заполнена с лучевыми записями LAN

на концентраторе и сводкой на лучах. Это может быть проверено при вводе этой команды в концентратор (концентраторы) и луч (лучи):

```
show ip eigrp [AS_NUMBER] topology
```

Вот пример вывода от луча:

```
Spokel#show ip eigrp 200 topology
EIGRP-IPv4 Topology Table for AS(200)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 26112000
via Rstatic (26112000/0)
via 10.1.1.1 (26240000/128256), Tunnel1

P 192.168.101.0/24, 1 successors, FD is 281600
via Connected, Ethernet1/0

P 192.168.0.0/16, 1 successors, FD is 26114560
via 10.1.1.1 (26114560/2562560), Tunnel1

P 10.1.1.100/32, 1 successors, FD is 26112000
via Connected, Tunnel1

P 10.1.1.0/24, 1 successors, FD is 26114560
via 10.1.1.1 (26114560/2562560), Tunnel1
```

Выходные данные показывают, что луч знает о его подсети LAN (в *курсиве*) и сводки для тех (полужирным).

Вот пример вывода от концентратора:

```
hub2# show ip eigrp 200 topology
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.2.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 128256
via Connected, Loopback200

P 192.168.101.0/24, 1 successors, FD is 26905600
via 10.1.1.100 (26905600/281600), Virtual-Access1

P 192.168.0.0/16, 1 successors, FD is 2562560
via Rstatic (2562560/0)

P 10.1.1.0/24, 1 successors, FD is 2562560
via Rstatic (2562560/0)
```

Выходные данные показывают, что концентратор знает о подсетях LAN лучей (в *курсиве*), итоговый префикс, который это объявляет (полужирным), и назначенный IP - адрес каждого луча через согласование.

Дополнительные замечания

Туннели конечного маршрутизатор - конечного маршрутизатора, которые Уже Существуют

Поскольку завершение туннельного интерфейса DMVPN заставляет записи NHRP быть удаленными, будут разъединены туннели конечного маршрутизатор - конечного маршрутизатора, которые уже существуют.

Очистите записи NHRP

Концентратор FlexVPN не полагается на процесс регистрации NHRP от луча, чтобы знать, как направить трафик назад. Однако динамические туннели конечного маршрутизатор - конечного маршрутизатора полагаются на записи NHRP.

В DMVPN, если NHRP на концентраторе очищен, это может привести к недолгим неполадкам подключения. В FlexVPN, очищая NHRP на лучах вызовет Сеанс IPSec FlexVPN, отнесенный в туннели конечного маршрутизатор - конечного маршрутизатора, чтобы быть разъединенным. Очистка NHRP на концентраторе не имеет никакого эффекта на сеанс FlexVPN.

Это вызвано тем, что, в FlexVPN по умолчанию:

- Спицы не регистрируются к концентраторам.
- Концентраторы работают только как редиректоры NHRP и не устанавливают записи NHRP.
- Записи ярлыка NHRP установлены на лучах для туннелей конечного маршрутизатор - конечного маршрутизатора и динамические.

Известные предупреждения

На трафик конечного маршрутизатор - конечного маршрутизатора мог бы влиять идентификатор ошибки Cisco [CSCub07382](#) .

Дополнительные сведения

- [DMVPN к FlexVPN мягкий пример конфигурации миграции](#)
- [Cisco Systems – техническая поддержка и документация](#)