Миграция FlexVPN: твердое перемещение от DMVPN до FlexVPN на тех же устройствах

Содержание

Введение

Этот документ предоставляет сведения о том, как мигрировать от существующей сети DMVPN до FlexVPN на тех же устройствах.

Конфигурации обеих платформ будут сосуществовать на устройствах.

В этом документе только показывают наиболее распространенный сценарий: DMVPN с помощью предварительного общего ключа для аутентификации и EIGRP как протокол маршрутизации.

Этот документ демонстрирует миграцию BGP (рекомендуемый протокол маршрутизации) и менее выбираемый EIGRP.

Предварительные условия

Требования

Этот документ предполагает, что читатель знает базовые понятия DMVPN и FlexVPN.

Используемые компоненты

Обратите внимание на то, что не все поддержки программных и аппаратных средств IKEv2. См. Cisco Feature Navigator для получения информации. Идеально, версии программного обеспечения, которые будут использоваться:

- ISR - 15.2 (4) M1 или более новый
- ASR1k - 3.6.2 выпусков 15.2 (2) S2 или более новый

Среди преимуществ более новой платформы и программного обеспечения возможность использования Криптографии Следующего поколения, например, AES GCM для шифрования в IPsec. Это обсуждено в RFC 4106.

AES GCM позволяет достигать намного более быстрой скорости шифрования на некоторых аппаратных средствах.

Для наблюдения Рекомендаций Cisco при использовании и миграции на Криптографию Следующего поколения, обратитесь к:

http://www. cisco . com/web/about/security/intelligence/nextgen_crypto.html

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Процедура миграции

В настоящее время рекомендуемый способ мигрировать от DMVPN до FlexVPN для этих двух платформ для не работы в то же время.

Это ограничение будет удалено из-за новых функций миграции, которые будут

представлены в выпуске ASR 3.10, отслеженном под множественными запросами на расширение под стороной Cisco, включая 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, будет упоминаться как мягкая миграция, которая указывает на минимальное влияние и плавное аварийное переключение от одной платформы до другого.

Миграция, где конфигурация 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 на тех же устройствах

В этом документе обсуждена миграция от существующей сети DMVPN до новой сети FlexVPN на тех же устройствах.

Эта миграция требует, чтобы обе платформы не воздействовали в то же время на устройства, по существу требуя, чтобы функциональность DMVPN была отключена через плату прежде, чем включить FlexVPN.

Пока новая функция миграции не доступна, способ выполнить миграции с помощью тех же устройств к:

1. Проверьте подключение по DMVPN.
2. Добавьте конфигурацию FlexVPN на месте и завершите работу Туннеля и Интерфейсов виртуального шаблона, принадлежащих новой конфигурации.
3. (Во время периода технического обслуживания) Завершение работы все туннельные интерфейсы DMVPN на всех лучах и концентраторах прежде, чем переместиться в шаг 4.
4. Незакрытые туннельные интерфейсы FlexVPN.
5. Проверьте луч для концентрации подключения.
6. Проверьте луч к лучевому подключению.
7. *Если проверка в точке 5 или 6 не пошла, должным образом возвращаются назад к DMVPN путем завершения интерфейса FlexVPN и незакрытия интерфейсов DMVPN.*
8. *Проверьте луч для концентрации связи.*
9. *Проверьте луч к лучевой связи.*

Пользовательский подход

Если, из-за вашей сети или сложностей маршрутизации, подход не мог бы быть лучшей идеей для вас, запустите обсуждение со своим представителем Cisco перед миграцией. Лучший человек для обсуждения пользовательского процесса переноса является Системным инженером или Инженером Расширенных сервисов.

Топология сети

Топология транспортной сети

Эта схема показывает типичную топологию соединений хостов в Интернете. В этом документе IP-адрес концентратора loopback0 (172.25.1.1) используется для завершения Сеанса IPSec.

Топология оверлейной сети

Эта схема топологии показывает два отдельных облака, используемые для наложения: DMVPN (зеленые соединения) и соединения FlexVPN.

Префиксы Локальной сети показывают для соответствующих сторон.

10.1.1.0/24 подсеть не представляет реальную подсеть с точки зрения интерфейсной адресации, а скорее блок пространства IP, выделенного облаку FlexVPN. Объяснение позади обсуждено позже в Разделе конфигурации FlexVPN.

!--- конфигурацию

Конфигурация DMVPN

Этот раздел содержит базовую конфигурацию концентратора DMVPN и луча.

Предварительный общий ключ (PSK) используется для аутентификации IKEv1.

Как только IPsec был установлен, регистрация NHRP выполнена от луча для концентрации, так, чтобы концентратор мог изучить адресацию NBMA динамично лучей.

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

Лучевая конфигурация DMVPN

Это - конфигурация базового примера DMVPN с аутентификацией предварительного общего ключа 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 контекстах безопасности IPSec. IKEv2 предлагает улучшения по сравнению с IKEv1, начиная с упругости и заканчивающийся тем, сколько сообщений необходимо для установления канала защищенных данных.
- GRE: В отличие от DMVPN, статические и динамические интерфейсы "точка-точка" используются, и не только на статических многоточечных интерфейсах GRE. Эта

конфигурация позволяет добавленную гибкость, специально для per-spoke/per-hub поведения.
- NHRP: В FlexVPN NHRP прежде всего используется для установления луча к лучевой связи. Спицы не регистрируются для концентрации.
- Маршрутизация: Поскольку лучи не выполняют регистрацию NHRP для концентрации, необходимо полагаться на другие механизмы для проверки, концентратор и лучи могут связаться двунаправленным образом. Simliar 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 позволит прямое соединение оконечного устройства - концентратора.

В трудной миграции от DMVPN до FlexVPN два framemworks 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.
- VRF - разделение VRF может позволить добавленную гибкость, но не будет обсуждено здесь (дополнительное).

Говорил конфигурацию FlexVPN

Одно из различий в конфигурации оконечного устройства в FlexVPN по сравнению с DMVPN, то, что у вас есть потенциально два интерфейса.

Существует необходимый туннель для луча для концентрации связи и дополнительного туннеля для луча в лучевые туннели. Если вы принимаете решение не иметь динамический луч к лучевому туннелированию и быть бы, что все проходит устройство концентратора, можно удалить виртуальный интерфейс и удалить ярлык NHRP, переключающийся из туннельного интерфейса.

Вы также заметите, что статическому туннельному интерфейсу получили IP-адрес на основе согласования. Это позволяет концентратору предоставлять IP 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
 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 в аппаратных средствах, 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 Tunnel1
 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 172.25.1.1
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel1
 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
```

PKI является рекомендуемым способом выполнить широкомасштабную аутентификацию в IKEv2.

Однако можно все еще использовать предварительный общий ключ, пока вы знаете, это - ограничения.

Вот пример конфигурации с помощью "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
```

Конфигурация концентратора FlexVPN

Как правило, концентратор только завершит динамические туннели оконечного устройства - концентратора. Это - то, почему в конфигурации концентратора вы не найдете статический туннельный интерфейс для FlexVPN, вместо этого виртуальный интерфейс используется. Это породит интерфейс виртуального доступа для каждого соединения.

Обратите внимание на то, что на стороне концентратора необходимо указать на адреса пула, которые будут назначены на лучи.

Адреса от этого пула будут 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
 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 в аппаратных средствах, которые поддерживают его.

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

Обратите внимание на то, что в конфигурации ниже AES операция GCM была прокомментирована.

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
interface Loopback0
 description DMVPN termination
 ip address 172.25.1.1 255.255.255.255
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
 shutdown
 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. Одна сторона может PSK используемой аутентификации в то время как другой RSA-СИГНАЛ.

Миграция трафика

Миграция на BGP как [Рекомендуемый] протокол маршрутизации наложения

BGP является протоколом маршрутизации на основе обмена индивидуальной рассылки. Из-за он - характеристики, это был лучший протокол масштабирования в сетях DMVPN.

В данном примере используется iBGP.

Лучевой BGP - конфигурация

Лучевая миграция состоит из двух частей. Включение BGP как динамическая маршрутизация.

```
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. BGP - конфигурацию Концентратора в этом разделе миграции), и новые префиксы по BGP изучены, можно качать трафик от существующего облака DMVPN до нового облака FlexVPN.

BGP - конфигурация концентратора

На концентраторе, чтобы избежать поддерживать конфигурацию соседства для каждого луча отдельно, настроены динамические слушатели.

В этой настройке BGP не будет инициировать новые соединения, но примет соединение от предоставленного пула IP-адресов. В этом случае упомянутый пул является 10.1.1.0/24, который является всеми адресами в новом облаке FlexVPN.

```
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
```

Миграция трафика к FlexVPN

Как упомянуто, прежде чем миграция должна быть сделана путем завершения функциональности DMVPN и внедрения FlexVPN.

Эта процедура гарантирует минимальное влияние.

1. На всех лучах:`interface tunnel 0`
   `shut`
2. На концентраторе:`interface tunnel 0`
   `shut`На этом этапе удостоверьтесь, что существуют сеансы № IKEv1, установленные к этому концентратору от лучей.Это может быть проверено путем проверки выходных данных **команды show crypto isakmp sa** и мониторинга сообщений системного журнала, генерируемых сеансом crypto logging.Как только это было подтверждено, можно продолжиться к внедрению FlexVPN.
3. Продвигаясь концентратор:`interface Virtual-template 1`
   `no shut`
4. На лучах:`interface tunnel 1`
   `no shut`

Этапы проверки

Устойчивость IPsec

Лучший способ оценить устойчивость IPsec путем мониторинга sylogs с этой включенной командой настройки:

```
crypto logging session
```

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.

Информация BGP заполнена

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 путем выполнения:

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

Пример корректной информации от концентратора:

```
Hub#show bgp
BGP router identifier 172.25.1.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.101 4 65001 83 82 13 0 0 01:10:46 1 *10.1.1.102 4 65001 7 7 13 0 0 00:00:44 1
```

Вы видите, что концентратор узнал, что 1 префикс от каждого из лучей и обоих лучей является динамичным (отмеченный звездочкой (*) знак).

Пример подобной информации от луча:

```
Spoke1#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 11 11 6 0 0 00:03:43 1
```

Луч получил один префикс от концентратора. В случае этой настройки этот префикс должен быть сводкой, объявленной на концентраторе.

Миграция на новые туннели с помощью EIGRP

EIGRP является популярным выбором в сетях DMVPN из-за, он - относительно простое развертывание и быстрая конвергенция.

Это, однако, масштабирует хуже, чем BGP и не предлагает многие усовершенствованные механизмы, которые могут использоваться BGP прямо из коробки.

Этот следующий раздел описывает один из способов переместиться в FlexVPN с помощью нового процесса EIGRP.

Обновленная конфигурация оконечного устройства

В данном примере новый AS добавлен 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: Необходимо избежать устанавливать смежность протокола маршрутизации по лучу в лучевые туннели, таким образом только сделайте интерфейс tunnel1 (луч к концентратору) не пассивный.

Обновленная конфигурация концентратора

Так же на концентраторе, DMVPN должна остаться рекомендуемым способом для обмена трафиком. Однако FlexVPN должен объявить и уже изучить те же префиксы.

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

Существует два способа предоставить сводку назад к лучу.

- Перераспределение статического маршрута, указывающего на null0 (Предпочтительный вариант).`ip route 192.168.0.0 255.255.0.0 null 0`
  ```
  ip access-list standard EIGRP_SUMMARY
   permit 192.168.0.0 0.0.255.255
  router eigrp 200
   distribute-list EIGRP_SUMMARY out Virtual-Template1
  ```
  `redistribute static metric 1500 10 10 1 1500`Эта опция позволяет управлять сводкой и перераспределением без конфигурации VT касающегося концентратора.
- Или, можно установить сводный адрес стиля DMVPN на Virtual-template. 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 200 172.16.1.0 255.255.255.0
   ip summary-address eigrp 200 192.168.0.0 255.255.0.0 delay 2000
  ```

Миграция трафика к FlexVPN

Миграция должна быть сделана путем завершения функциональности DMVPN и внедрения FlexVPN.

Следующая процедура гарантирует минимальное влияние.

1. На всех лучах:`interface tunnel 0`
   `shut`
2. На концентраторе:`interface tunnel 0`
   `shut`На этом этапе удостоверьтесь, что существуют сеансы № IKEv1, установленные к этому концентратору от лучей.Это может быть проверено путем проверки выходных данных **команды show crypto isakmp sa** и мониторинга сообщений системного журнала, генерируемых сеансом crypto logging.Как только это было подтверждено, можно продолжиться к внедрению FlexVPN.
3. Продвигаясь концентратор:`interface Virtual-template 1`
   `no shut`
4. На всех лучах:`interface tunnel 1`
   `no shut`

Этапы проверки

Устойчивость IPsec

Если IPsec стабилен, как в случае BGP, необходимо оценить. Лучший способ сделать так путем мониторинга sylogs с этой включенной командой настройки:

```
crypto logging session
```

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 вам действительно заполняли вашу таблицу топологии EIGRP с лучевыми записями LAN на концентраторе и сводкой на лучах. Это может быть проверено путем выдачи этой команды на концентраторе (концентраторах) и луче (лучах).

```
show ip eigrp topology
```

Пример надлежащих выходных данных от луча:

```
Spoke1#sh ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
(...omitted as output related to DMVPN cloud ...)
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)


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 (26114560/1709056), Tunnel1 P 10.1.1.107/32, 1
successors, FD is 26112000 via Connected, Tunnel1
```

Вы заметите, что луч знает о его подсети LAN (в курсиве) и сводки для тех **(полужирным)**.

Пример надлежащих выходных данных от концентратора.

```
Hub#sh ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(172.25.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
(...omitted, related to DMVPN...)
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.1.1)
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, Loopback100


P 192.168.101.0/24, 1 successors, FD is 1561600 via 10.1.1.107 (1561600/281600), Virtual-Access1
P 192.168.0.0/16, 1 successors, FD is 1709056 via Rstatic (1709056/0) P 10.1.1.107/32, 1
successors, FD is 1709056 via Rstatic (1709056/0) P 10.1.1.106/32, 1 successors, FD is 1709056
via Rstatic (1709056/0) P 0.0.0.0/0, 1 successors, FD is 1709056 via Rstatic (1709056/0) P
192.168.102.0/24, 1 successors, FD is 1561600 via 10.1.1.106 (1561600/281600), Virtual-Access2
```

Вы обратите внимание, 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

Существующий луч в лучевые туннели

Поскольку завершение туннельного интерфейса DMVPN заставляет записи NHRP быть удаленными, существующий луч в лучевые туннели будет разъединен.

Очистка записей NHRP

Как упомянуто прежде, концентратор FlexVPN не будет полагаться на процесс регистрации NHRP от луча, чтобы знать, как направить трафик назад. Однако динамический луч в лучевые туннели полагается на записи NHRP.

В DMVPN, где очистка NHRP на концентраторе, возможно, привела к недолгим неполадкам подключения.

В FlexVPN, очищающем NHRP на лучах, вызовет Сеанс IPSec FlexVPN, отнесенный к лучу в лучевые туннели, чтобы быть разъединенным. В очищающемся NHRP никакой концентратор не будет иметь эффект на сеанс FlexVPN.

Это то, вследствие того, что в FlexVPN по умолчанию:

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

Известные предупреждения

На луч к лучевому трафику мог бы влиять CSCub07382.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация