Наиболее распространенные решения для устранения неполадок DMVPN

Содержание

Введение

Этот документ содержит наиболее распространенные решения проблем динамической многоточечной VPN (DMVPN). Многие из этих решений могут быть реализованы перед выполнением всесторонних мероприятий по устранению проблем с соединениями DMVPN. Этот документ составлен в виде контрольного списка общих мер, которые следует предпринять прежде, чем приступать к диагностике соединения и обращаться в службу

технической поддержки Cisco.

Документы с примерами конфигурации для DMVPN приведены на странице Примеры конфигурации и технические примечания по DMVPN.

Примечание. В документе Поиск и устранение неисправностей IPsec — общие сведения и примеры использования команд debug приведено описание распространенных команд debug, которые используются для поиска и устранения неполадок в работе IPsec.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с конфигурацией DMVPN в маршрутизатора с Cisco IOS®.

Используемые компоненты

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

- Cisco IOS

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.

Условные обозначения

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

Конфигурация DMVPN не работает

Проблема

Недавно настроенное или измененное решение DMVPN не работает.

Текущая конфигурация DMVPN больше не работает.

Решения

В этом разделе приведены решения наиболее распространенных проблем DMVPN.

Эти решения (без определенного порядка) могут использоваться в качестве контрольного списка элементов для проверки перед переходом к всесторонним мероприятиям по поиску и устранению неполадок:

- Распространенные проблемы

- Проверка блокировки пакетов ISAKMP поставщиком услуг Интернета
- Проверьте, хорошо ли работает GRE, удалив защиту туннеля
- Ошибка регистрации NHRP
- Проверьте, правильно ли настроены сроки действия
- Проверьте, проходят ли потоки трафика только в одном направлении
- Проверьте, установлены ли отношения соседства в протоколе маршрутизации

Примечание. Перед тем как начать, выполните следующие действия:

1. Синхронизируйте метки времени между концентратором и конечным маршрутизатором
2. **Включите отладку msec и отметки времени в журнале:**`Router(config)#service timestamps debug datetime msec Router(config)#service timestamps log datetime msec`
3. **Включите режим terminal exec prompt timestamp для сеансов отладки:**`Router#terminal exec prompt timestamp`

Примечание. Таким образом можно легко соотнести выходные данные команды debug с выходными данными команды show.

Распространенные проблемы

Проверьте базовые возможности подключения

1. Выполните эхозапрос от концентратора к конечному маршрутизатору, используя адреса NBMA, и в обратном направлении.Эти эхозапросы должны выходить непосредственно из физического интерфейса, а не через туннель DMVPN. Желательно, чтобы между устройствами не было межсетевого экрана, блокирующего пакеты эхозапросов. Если это не работает, проверьте маршрутизацию и наличие межсетевых экранов между центральным и конечными маршрутизаторами.
2. **Кроме того, используйте команду traceroute для проверки пути, по которому проходят пакеты зашифрованного туннеля.**
3. **С помощью команд debug и show проверьте, что связь отсутствует:debug ip icmpdebug ip packet Примечание. Команда debug ip packet формирует выходные данные большого объема и использует значительный объем системных ресурсов.** В рабочих сетях эту команду следует использовать осторожно. **Всегда используйте команду access-list. Примечание. Дополнительные сведения о том, как использовать access-list с debug ip packet, см. в статье Поиск и устранение неполадок с помощью списков доступа IP.**

Проверка наличия несовместимой политики ISAKMP

Если настроенные политики ISAKMP не совпадают с политикой, предложенной удаленным узлом, маршрутизатор пытается использовать политику по умолчанию 65535. Если и эта политика не совпадает, происходит ошибка согласования ISAKMP.

Команда show crypto isakmp sa показывает, что ISAKMP SA находится в MM_NO_STATE, а это значит, что произошел сбой основного режима.

Проверка наличия неправильного секрета предварительного общего ключа

Если предварительные общие ключи не будут одинаковыми на обеих сторонах, произойдет ошибка согласования.

Маршрутизатор возвращает сообщение sanity check failed (ошибка при проверке исправности не пройдена).

Проверка наличия несовместимого набора преобразований IPsec

Если наборы преобразований IPsec несовместимы или не совпадают на двух устройствах IPSec, произойдет ошибка согласования IPsec.

Маршрутизатор возвращает сообщение atts not acceptable (неприменимые параметры) на предложение IPsec.

Проверка блокировки пакетов ISAKMP поставщиком услуг Интернета

```
Router#show crypto isakmp sa


IPv4 Crypto ISAKMP SA
Dst             src               state    conn-id  slot   status
172.17.0.1  172.16.1.1    MM_NO_STATE     0           0   ACTIVE
172.17.0.1  172.16.1.1    MM_NO_STATE     0           0   ACTIVE (deleted)
172.17.0.5        172.16.1.1        MM_NO_STATE      0             0   ACTIVE
172.17.0.5        172.16.1.1        MM_NO_STATE      0             0   ACTIVE (deleted)
```

Приведенные выше данные показывают нестабильность туннеля VPN.

Затем проверьте debug crypto isakmp и удостоверьтесь, что конечный маршрутизатор отправляет пакет udp 500:

```
Router#debug crypto isakmp


04:14:44.450: ISAKMP:(0):Old State = IKE_READY
                        New State = IKE_I_MM1
04:14:44.450: ISAKMP:(0): beginning Main Mode exchange
04:14:44.450: ISAKMP:(0): sending packet to 172.17.0.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:44.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
04:14:54.450: ISAKMP (0:0): incrementing error counter on sa,
              attempt 1 of 5: retransmit phase 1
04:14:54.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
04:14:54.450: ISAKMP:(0): sending packet to 172.17.0.1
              my_port 500 peer_port 500 (I) MM_NO_STATE
04:14:54.450: ISAKMP:(0):Sending an IKE IPv4 Packet.
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE...
04:15:04.450: ISAKMP (0:0): incrementing error counter on sa,
              attempt 2 of 5: retransmit phase 1
04:15:04.450: ISAKMP:(0): retransmitting phase 1 MM_NO_STATE
```

Приведенные выше выходные данные команды debug показывают, что конечный маршрутизатор передает пакет udp 500 через каждые 10 секунд.

Обратитесь к поставщику услуг Интернета и проверьте, подключен ли конечный маршрутизатор напрямую к маршрутизатору этого поставщика, чтобы удостовериться, что

они разрешают трафик udp 500.

После того как поставщик услуг Интернета разрешит пакеты udp 500, добавьте входящий список контроля доступа в выходной интерфейс, который является точкой начала туннеля, чтобы разрешить пакеты udp 500 и обеспечить поступление трафика udp 500 в маршрутизатор. С помощью команды show access-list проверьте, увеличиваются ли счетчики попаданий:

```
Router#show access-lists 101
```

```
Router#show access-lists 101
```

Внимание. : В списке доступа должно быть разрешено ip any any. В противном случае весь остальной трафик будет заблокирован, поскольку access-list применяется на входе в выходном интерфейсе.

Проверьте работу GRE путем удаления защиты туннеля

Когда DMVPN не работает, прежде чем приступать к устранению неполадки с помощью IPsec, проверьте работоспособность туннелей GRE без шифрования IPsec.

Дополнительные сведения см. в статье Настройка туннеля GRE.

Ошибка регистрации NHRP

VPN-туннель между центральным и конечным маршрутизаторами работает, но не может передавать трафик данных:

```
Router#show crypto isakmp sa
        dst             src             state          conn-id  slot   status
        172.17.0.1      172.16.1.1      QM_IDLE           1082    0    ACTIVE

Router#show crypto IPSEC sa
local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
#pkts encaps: 154, #pkts encrypt: 154, #pkts digest: 154
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
inbound esp sas:
spi: 0xF830FC95(4163959957)
outbound esp sas:
spi: 0xD65A7865(3596253285)
!--- !--- Output is truncated !---
```

Он показывает, что ответный трафик не возвращается из другого конца туннеля.

Проверьте запись NHS в конечном маршрутизаторе:

```
Router#show  ip nhrp nhs detail
Legend: E=Expecting replies, R=Responding
Tunnel0: 172.17.0.1  E  req-sent 0  req-failed 30 repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 4371, Ret 64  NHS 172.17.0.1
```

Она показывает, что произошла ошибка запроса NHS. Для решения этой проблемы проверьте правильность конфигурации интерфейса туннеля на конечном маршрутизаторе.

Пример конфигурации:

```
interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
 ip nhrp nhs 172.17.0.1
!--- !--- Output is truncated !---
```

Пример конфигурации с правильной записью для сервера NHS:

```
interface Tunnel0
 ip address 10.0.0.9 255.255.255.0
 ip nhrp map 10.0.0.1 172.17.0.1
 ip nhrp map multicast 172.17.0.1
 ip nhrp nhs 10.0.0.1
!--- !--- Output is truncated !---
```

Теперь проверьте запись NHS и счетчики шифрования/расшифровки Ipsec:

```
Router#show ip nhrp nhs detail
Legend: E=Expecting replies, R=Responding
Tunnel0:        10.0.0.1 RE  req-sent 4  req-failed 0  repl-recv 3 (00:01:04 ago)

Router#show crypto IPSec sa
local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
#pkts encaps: 121, #pkts encrypt: 121, #pkts digest: 121
#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118
inbound esp sas:
spi: 0x1B7670FC(460747004)
outbound esp sas:
spi: 0x3B31AA86(993110662)
!--- !--- Output is truncated !---
```

Проверьте, правильно ли настроены сроки действия

Используйте следующие команды для проверки текущего срока действия SA и времени для следующего согласования:

- **show crypto isakmp sa detail**
- *show crypto ipsec sa peer <NBMA-address-peer>*

Запишите значения сроков действия SA. Если они приблизительно равны настроенным срокам действия (сроки действия по умолчанию: для ISAKMP — 24 часа, для IPsec — 1 час), то это означает, что эти SA были согласованы недавно. Если выполнить проверку немного позже, уже после повторного согласования, то может оказаться, что ISAKMP и/или IPsec то включаются, то выключаются.

```
Router#show crypto ipsec security-assoc lifetime
Security association lifetime: 4608000 kilobytes/3600 seconds

Router#show crypto isakmp policy
```

```
Global IKE policy
Protection suite of priority 1
Encryption algorithm: DES-Data Encryption Standard (65 bit keys)
Hash algorithm: Message Digest 5
Authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
Lifetime: 86400 seconds, no volume limit
Default protection suite
 Encryption algorithm: DES- Data Encryption Standard (56 bit keys)
 Hash algorithm: Secure Hash Standard
 Authentication method: Rivest-Shamir-Adleman Signature
 Diffie-Hellman group: #1 (768 bit)
 Lifetime: 86400 seconds, no volume limit

Router# show crypto ipsec sa
interface: Ethernet0/3
    Crypto map tag: vpn, local addr. 172.17.0.1
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.17.0.1/255.255.255.255/47/0)
   current_peer: 172.17.0.1:500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
    #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0
     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.0.1
     path mtu 1500, media mtu 1500
     current outbound spi: 8E1CB77A

 inbound esp sas:
      spi: 0x4579753B(1165587771)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4456885/3531)
        IV size: 8 bytes
        replay detection support: Y
outbound esp sas:
      spi: 0x8E1CB77A(2384246650)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4456885/3531)
        IV size: 8 bytes
        replay detection support: Y
```

Проверьте, проходят ли потоки трафика только в одном направлении

VPN-туннель между двумя конечными маршрутизаторами работает, но не может передавать трафик данных:

```
Spoke1# show crypto ipsec sa peer 172.16.2.11
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
    #pkts encaps: 110, #pkts encrypt: 110
    #pkts decaps: 0, #pkts decrypt: 0,
local crypto endpt.: 172.16.1.1,
remote crypto endpt.: 172.16.2.11
      inbound esp sas:
      spi: 0x4C36F4AF(1278669999)
      outbound esp sas:
```

```
      spi: 0x6AC801F4(1791492596)
!--- !--- Output is truncated !--- Spoke2#sh crypto ipsec sa peer 172.16.1.1
   local  ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   #pkts encaps: 116, #pkts encrypt: 116,
   #pkts decaps: 110, #pkts decrypt: 110,
local crypto endpt.: 172.16.2.11,
remote crypto endpt.: 172.16.1.1
     inbound esp sas:
     spi: 0x6AC801F4(1791492596)
     outbound esp sas:
     spi: 0x4C36F4AF(1278669999
!--- !--- Output is truncated !---
```

В маршрутизаторе spoke1 отсутствуют пакеты decap, а это означает, что пакеты esp отбрасываются где-то на обратном пути от маршрутизатора spoke2 к маршрутизатору spoke1.

На маршрутизатор spoke2 показывает наличие и пакетов encap, и пакетов decap, а это означает, что трафик ESP фильтруется до того, как достигнет spoke2. Это может произойти на конце поставщика услуг Интернета в spoke2 или любом межсетевом экране в пути между маршрутизаторами spoke2 и spoke1. После разрешения ESP (протокол IP 50) на обоих маршрутизаторах (spoke1 и spoke2) видно, что счетчики encap и decap увеличиваются.

```
spoke1# show crypto ipsec sa peer 172.16.2.11
   local  ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
    #pkts encaps: 300, #pkts encrypt: 300
    #pkts decaps: 200, #pkts decrypt: 200
!--- !--- Output is truncated !--- spoke2#sh crypto ipsec sa peer 172.16.1.1
   local  ident (addr/mask/prot/port): (172.16.2.11/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/47/0)
   #pkts encaps: 316, #pkts encrypt: 316,
   #pkts decaps: 300, #pkts decrypt: 310
!--- !--- Output is truncated !---
```

Проверьте, установлены ли отношения соседства в протоколе маршрутизации

Конечные маршрутизаторы не могут установить отношения соседства по протоколу маршрутизации:

```
Hub# show ip eigrp neighbors
H   Address      Interface   Hold Uptime     SRTT    RTO   Q  Seq
                                (sec)             (ms)  Cnt Num
2   10.0.0.9     Tu0          13  00:00:37     1    5000   1  0
0   10.0.0.5     Tu0          11 00:00:47   1587   5000   0 1483
1   10.0.0.11    Tu0          13 00:00:56     1    5000   1  0
Syslog message:
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10:
Neighbor 10.0.0.9 (Tunnel0) is down: retry limit exceeded

Hub# show ip route eigrp
172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
     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, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

Проверьте, правильно ли настроено составление многоадресной рассылки NHRP в

концентраторе.

В интерфейсе туннеля концентратора должно быть настроено динамическое сопоставление многоадресной рассылки nhrp.

Пример конфигурации:

```
Hub# show ip eigrp neighbors
H   Address     Interface   Hold Uptime     SRTT    RTO   Q  Seq
                              (sec)             (ms)  Cnt Num
2   10.0.0.9     Tu0         13  00:00:37     1    5000   1  0
0   10.0.0.5     Tu0         11 00:00:47   1587   5000   0 1483
1   10.0.0.11    Tu0         13 00:00:56     1    5000   1  0
Syslog message:
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 10:
Neighbor 10.0.0.9 (Tunnel0) is down: retry limit exceeded

Hub# show ip route eigrp
172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
     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, FastEthernet0/1
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

Пример конфигурации с правильной записью для динамического сопоставления многоадресной рассылки nhrp:

```
interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 ip mtu 1400
 no ip next-hop-self eigrp 10
 ip nhrp authentication test
 ip nhrp map multicast dynamic
 ip nhrp network-id 10
 no ip split-horizon eigrp 10
 tunnel mode gre multipoint
!--- !--- Output is truncated !---
```

Это позволяет NHRP автоматически добавлять маршрутизаторы в сопоставления многоадресной рассылки NHRP.

Дополнительные сведения см. в пункте ip nhrp map multicast dynamic раздела Команды NHRP.

```
Hub#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address     Interface   Hold   Uptime   SRTT    RTO     Q     Seq
                                           (sec)    (ms)   Cnt    Num
2   10.0.0.9     Tu0         12   00:16:48   13     200     0     334
1   10.0.0.11    Tu0         13   00:17:10   11     200     0     258
0   10.0.0.5     Tu0         12   00:48:44  1017    5000    0     1495

Hub#show ip route

     172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
D    192.168.11.0/24 [90/2944000] via 10.0.0.11, 00:16:12, Tunnel0
     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, FastEthernet0/1
D    192.168.2.0/24 [90/2818560] via 10.0.0.9, 00:15:45, Tunnel0
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

Для определения маршрутов к конечным маршрутизаторам используется протокол eigrp.

Проблема с интеграцией VPN удаленного доступа с DMVPN

Проблема

DMVPN работает хорошо, но не может установить RAVPN.

Решение

Для достижения этого используйте профили ISAKMP и профили IPsec.

Создайте отдельные профили для DMVPN и RAVPN.

Дополнительные сведения см. в статье Пример настройки DMVPN и сервера Easy VPN Server с помощью профилей ISAKMP.

Проблема с dual-hub-dual-dmvpn.

Проблема

Проблема с dual-hub-dual-dmvpn. В частности, туннели отключаются и не могут выполнить повторное согласование.

Решение

Используйте одинаковое ключевое слово в защите туннеля IPsec для интерфейсов туннеля на концентраторе и на конечном маршрутизаторе.

Пример конфигурации:

```
Hub#show ip eigrp neighbors
IP-EIGRP neighbors for process 10
H   Address      Interface   Hold   Uptime   SRTT    RTO     Q     Seq
                                             (sec)    (ms)   Cnt   Num
2   10.0.0.9     Tu0         12   00:16:48   13     200     0     334
1   10.0.0.11    Tu0         13   00:17:10   11     200     0     258
0   10.0.0.5     Tu0         12   00:48:44  1017    5000    0     1495

Hub#show ip route

     172.17.0.0/24 is subnetted, 1 subnets
C       172.17.0.0 is directly connected, FastEthernet0/0
D    192.168.11.0/24 [90/2944000] via 10.0.0.11, 00:16:12, Tunnel0
     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, FastEthernet0/1
D    192.168.2.0/24 [90/2818560] via 10.0.0.9, 00:15:45, Tunnel0
```

```
S*   0.0.0.0/0 [1/0] via 172.17.0.100
```

Дополнительные сведения см. в разделе о защите туннелей в справочнике команд безопасности Cisco IOS.

Трудности с входом на сервер через DMVPN

Проблема

Проблема с доступом к серверу через сеть DMVPN.

Решение

Проблема может быть связана с MTU и размером MSS пакета, который использует GRE и IPsec.

Размер пакета мог быть причиной проблемы с фрагментацией. Для устранения этой проблемы используйте следующие команды:

```
ip mtu 1400
ip tcp adjust-mss 1360
crypto IPSec fragmentation after-encryption (global)
```

Также можно настроить команду tunnel path-mtu-discovery, чтобы динамически обнаруживать размер MTU.

Более подробное описание см. в разделе Устранение проблем с фрагментацией IP, MTU, MSS и PMTUD в работе GRE и IPSEC.

Невозможно получить доступ к серверам на DMVPN через определенные порты

Проблема

Не удается получить доступ к серверам на DMVPN через определенные порты.

Решение

Отключите набор функций межсетевого экрана IOS и посмотрите, не исчезла ли проблема.

Если все хорошо работает, то проблема связана с настройкой межсетевого экрана IOS, а не с DMVPN.

Дополнительные сведения

- Динамическая многоточечная VPN (DMVPN)
- IPSec Negotiation/IKE

- Cisco Systems – техническая поддержка и документация