Наиболее распространенные решения для устранения проблем DMVPN

Содержание

Введение

Этот документ содержит наиболее распространенные решения проблем Динамической многоточечной VPN (DMVPN). Многие из этих решений могут быть внедрены до всестороннего устранения проблем соединения 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.

При необходимости в документах примера конфигурации для DMVPN обратитесь к Примерам конфигурации и технические примечания DMVPN.

Примечание: См. Устранение проблем протокола IPSec - Понимание и Использование команд отладки для обеспечения объяснения распространенных команд отладки **команды отладки**, которые используются для решения проблем IPsec.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с конфигурацией DMVPN на маршрутизаторах 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 модифицированное решение DMVPN не работает.

Текущая конфигурация DMVPN больше не работает.

Решения

Этот раздел содержит решения наиболее распространенных проблем DMVPN.

Эти решения (без определенного порядка) могут использоваться в качестве чек-листа элементов, чтобы проверить или попробовать перед привлечением во всестороннем устранении проблем:

- Распространенные проблемы
- Проверьте, заблокированы ли Пакеты ISAKMP в интернет-провайдере
- Проверьте, хорошо работает ли GRE путем удаления tunnel protection

- Регистрация NHRP отказывает
- Проверьте, настроены ли сроки службы должным образом
- Проверьте ли трафики только в одном направлении
- Проверьте, что установлен сосед по протоколу маршрутизации

Примечание: Перед началом проверьте их:

1. Syncup метки времени между концентратором и лучом
2. Включите **отладку msec и регистрируйте метки времени**:`Router(config)#service timestamps debug datetime msec Router(config)#service timestamps log datetime msec`
3. Включите **метку времени приглашения terminal exec** для сеансов отладки:`Router#terminal exec prompt timestamp`

Примечание: Таким образом, можно легко коррелировать **выходные данные отладки** с **выходными данными команды show**.

Распространенные проблемы

Проверьте основное подключение

1. Эхо-запрос от концентратора до адресов и реверса NBMA использования луча.Эти эхо-запросы должны пойти непосредственно физический интерфейс, не через туннель DMVPN. Хотелось бы надеяться, нет межсетевого экрана, который блокирует ping - пакеты. Если это не работает, проверьте маршрутизацию и любые межсетевые экраны между концентратором и маршрутизаторами на конце луча.
2. Кроме того, используйте **traceroute** для проверки пути, который берут пакеты зашифрованного туннеля.
3. Используйте **команды debug и show** для проверки подключения:**debug ip icmpdebug ip packetПримечание: Команда debug ip packet** генерирует значительное количество выходных данных и использует значительное количество ресурсов системы. Эта команда должна использоваться с осторожностью в рабочих сетях. Всегда используйте с **командой access-list.Примечание:** Для получения дополнительной информации о том, как использовать **access-list** с **debug ip packet**, обратитесь для Устранения проблем со списками доступа IP.

Проверьте для несовместимой Политики ISAKMP

Если настроенная Политика ISAKMP не совпадает с предложенной политикой удаленным узлом, маршрутизатор пробует политику по умолчанию 65535. Если это не совпадает также, это отказывает согласование ISAKMP.

Команда show crypto isakmp sa показывает ISAKMP SA, чтобы быть в **MM_NO_STATE**, означая подведенный основной режим.

Проверьте для неправильной тайны предварительного общего ключа

Если предварительные общие ключи не будут тем же с обеих сторон, то согласование откажет.

Маршрутизатор возвращает **"проверку работоспособности подведенное"** сообщение.

Проверьте для несовместимой команды IPsec transform set

Если команда IPsec transform set не будет совместимой или несогласованной на этих двух Устройствах IPSec, то согласование IPsec откажет.

Маршрутизатор возвращается **"atts не приемлемое"** сообщение для предложения по Ipsec.

Проверьте, заблокированы ли Пакеты ISAKMP в интернет-провайдере

```
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)
```

Вышеупомянутое показывает переброску VPN-туннеля.

Далее, проверьте **debug crypto isakmp**, чтобы проверить, что маршрутизатор на конце луча передает 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
```

Вышеупомянутые **выходные данные отладки** показывают, что маршрутизатор на конце луча передает пакет udp 500 через каждые 10 секунд.

Согласуйте с интернет-провайдером, чтобы видеть, напрямую подключается ли маршрутизатор на конце луча к маршрутизатору ISP, чтобы удостовериться, что они позволяют трафик udp 500.

После того, как интернет-провайдер позволил udp 500, добавьте входящий ACL в исходящем интерфейсе, который является точкой начала туннеля, чтобы позволить udp 500 удостоверяться, что трафик udp 500 входит в маршрутизатор. Используйте команду show access-list, чтобы проверить, инкрементно увеличивается ли пораженное количество:

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

Внимание. : Удостоверьтесь, что у вас есть **ip любой любой** разрешенный в вашем access-

list. В противном случае весь другой трафик будет заблокирован, поскольку **access-list** применился входящий на исходящий интерфейс.

Проверьте, работает ли GRE путем удаления tunnel protection

Когда DMVPN не работает, прежде, чем устранить неполадки с IPsec, проверьте, что Туннели GRE хорошо работают без IP - безопасного шифрования.

Для получения дополнительной информации обратитесь для Настройки Туннеля GRE.

Регистрация NHRP отказывает

VPN-туннель между концентратором и лучом подключен, но неспособный передать 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    ACTIVERouter#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 !---
```

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

Проверьте запись NHS в маршрутизаторе на конце луча:

```
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
```

Это показывает, что отказывает запрос NHS. Для решения этой проблемы удостоверьтесь, что конфигурация на туннельном интерфейсе маршрутизатора на конце луча корректна.

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 корректной 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, что запись NHS и IPsec шифруют/дешифруют счетчики:

```
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, настроены ли сроки службы должным образом

Используйте эти команды для проверки текущего срока действия SA и время для следующего пересмотра:

- **show crypto isakmp sa detail**
- **узел show crypto ipsec sa** *<адресный узел NBMA>*

Заметьте значения срока действия SA. Если они близко к настроенным срокам службы (по умолчанию составляет 24 часа для ISAKMP и 1 час для IPsec), то это означает, что об этих SA недавно выполнили согласование. Если вы смотрите немного позже, и они были пересмотрены снова, то ISAKMP и/или IPsec могут возвращаться вверх и вниз.

```
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 ли трафики только в одном направлении

VPN-туннель между маршрутизатором конечного маршрутизатор - конечного маршрутизатора подключен, но неспособный передать 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 spoke1 нет никаких decap пакетов, что означает, что пакеты ESP отброшены где-нибудь в пути, возвращаются из spoke2 к spoke1.

spoke2 маршрутизатор показывает и encap и decap, что означает, что ESP трафик фильтруется прежде, чем достигнуть spoke2. Это может произойти в конце интернет-провайдера в spoke2 или в любом межсетевом экране в пути между spoke2 маршрутизатором и spoke1 маршрутизатором. После разрешения ESP (Протокол "IP" 50), инкрементно увеличиваются spoke1 и spoke2 и показать encap и счетчики decaps.

```
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, что установлен сосед по протоколу маршрутизации

Спицы неспособны установить отношение соседа 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, настроено ли составление карты групповой адресации NHRP должным образом в концентраторе.

В концентраторе это требуется, чтобы настраивать динамическое nhrp составление карты групповой адресации в туннельном интерфейсе концентраторов.

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 корректной записью для динамического nhrp составления карты групповой адресации:

```
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 на конце луча к NHRP - маршрутизациям групповой адресации.

Для получения дополнительной информации обратитесь к разделу **ip nhrp map multicast dynamic** Команд 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
```

Маршруты к лучам изучены через протокол eigrp.

Проблема с интегрирующейся VPN удаленного доступа с DMVPN

Проблема

DMVPN хорошо работает, но неспособный установить RAVPN.

Решение

Используйте профили ISAKMP и Профили IPSEC для достижения этого.

Создайте отдельные профили для DMVPN и RAVPN.

Для получения дополнительной информации обратитесь к DMVPN и Серверу Easy VPN с Примером конфигурации Профилей ISAKMP.

Проблема с dual-hub-dual-dmvpn.

Проблема

Проблема с dual-hub-dual-dmvpn. В частности туннели выключаются и неспособные пересмотреть.

Решение

Используйте совместно используемое ключевое слово в туннельной Защите IPsec и для туннельных интерфейсов на концентраторе, и на луче также.

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
```

Для получения дополнительной информации обратитесь к разделу **tunnel protection** в Справочнике по командам Безопасности Cisco IOS.

Проблема, входящая в сервер через DMVPN

Проблема

Проблема с доступом к серверу через сеть DMVPN.

Решение

Проблема могла быть отнесена к MTU и размеру MSS пакета, который использует GRE и IPsec.

Теперь, размер пакета мог быть проблемой с фрагментацией. Для устранения этой проблемы используйте эти команды:

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

Вы могли также настроить **команду tunnel path-mtu-discovery** для динамичного обнаружения максимального размера передаваемого блока данных.

Для большего количества подробного объяснения обратитесь для Решения Фрагментации ip, MTU, MSS и Проблем PMTUD с GRE и IPSEC.

Неспособный обратиться к серверам на DMVPN через

определенные порты

Проблема

Неспособный к серверам доступа на DMVPN через определенные порты.

Решение

Проверьте путем отключения набора функций межсетевого экрана IOS и посмотрите, работает ли он.

Если это хорошо работает, то проблема отнесена к config межсетевого экрана IOS, не с DMVPN.

Дополнительные сведения

- Динамическая многоточечная VPN (DMVPN)
- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация