A maioria de soluções comuns do Troubleshooting DMVPN

Índice

Introdução

Este documento contém a maioria de soluções comum aos problemas do Dynamic Multipoint VPN (DMVPN). Muitas destas soluções podem ser executadas antes do Troubleshooting detalhado da conexão DMVPN. Este documento é apresentado como uma lista de verificação de procedimentos comuns a serem tentados antes de você iniciar o troubleshooting de uma conexão e chamar o Suporte Técnico da Cisco.

Se você precisa documentos do exemplo de configuração para o DMVPN, refira exemplos de configuração e TechNotes DMVPN.

Nota: Refira o Troubleshooting de IPSec - Compreendendo e usando comandos debug fornecer os **comandos debug de uma** explicação comun que são usados para pesquisar defeitos edições do IPsec.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento da configuração DMVPN no Roteadores do ® do Cisco IOS.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco IOS

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

A configuração DMVPN não trabalha

Problema

Uma solução de DMVPN recentemente configurada ou alterada não trabalha.

Trabalhos atuais de uma configuração DMVPN já não.

Soluções

Esta seção contém soluções aos problemas os mais comuns DMVPN.

Estas soluções (em nenhum pedido específico) podem ser usadas como uma lista de verificação de artigos para verificar ou de tentativa antes que você contrate no Troubleshooting detalhado:

- Problemas comuns
- Verifique se os pacotes ISAKMP são obstruídos no ISP
- Verifique se o GRE está trabalhando muito bem removendo a proteção do túnel
- O registro NHRP está falhando

- Verifique se as vidas estão configuradas corretamente
- Verifique se os fluxos de tráfego em somente um sentido
- Verifique que o vizinho de protocolo de roteamento está estabelecido

Nota: Antes que você comece, verifique estes:

1. Sincronização-acima os timestamps entre o hub and spoke
2. Permita o **milissegundo debugam e registram timestamps**:`Os timestamps de Router(config)#service debugam o datetime msecOs timestamps de Router(config)#service registram o datetime msec`
3. Permita o **timestamp terminal do prompt de exec** para os sessão de debugging:`Timestamp do prompt de exec de Router#terminal`

Nota: Esta maneira, você pode facilmente correlacionar o **resultado do debug** com o **show command output (resultado do comando show)**.

Problemas comuns

Verifique a conectividade básica

1. Sibile do hub aos endereços de utilização NBMA do raio e inverta.Estes sibilos devem atravessar diretamente para fora a interface física, não o túnel DMVPN. Esperançosamente, não há um Firewall que obstrua pacotes de ping. Se isto não trabalha, verifique o roteamento e todos os Firewall entre o Roteadores do hub and spoke.
2. Também, **traceroute do** uso para verificar o trajeto que os pacotes do túnel criptografado estão tomando.
3. Use os **comandos debug and show** não verificar nenhuma Conectividade:**debugar o ICMP IPdebugar o pacote IPNota: O comando debug ip packet** gerencie um montante substancial de saída e usa um montante substancial de recursos de sistema. Este comando deve ser usado com cuidado nas redes de produção. Use sempre com o **comando access-list**.**Nota:** Para obter mais informações sobre de como usar a **lista de acesso** com **debugar o pacote IP**, consultam para pesquisar defeitos com listas de acesso IP.

Verifique para a política de ISAKMP incompatível

Se as políticas de ISAKMP configuradas não combinam a política proposta pelo peer remoto, o roteador tenta a política padrão de 65535. Se isso não combina tampouco, falha a negociação de ISAKMP.

O comando show crypto isakmp sa mostra ISAKMP SA para estar em **MM_NO_STATE**, significando o modo principal falhado.

Verifique para o segredo incorreto da chave pré-compartilhada

Se os segredos pré-compartilhados não são os mesmos em ambos os lados, a negociação falhará.

O roteador retorna a mensagem **falhada "verificação de sanidade"**.

Verifique para o IPsec incompatível transformam o grupo

Se o conjunto de transformação do IPsec não é compatível ou combinado mal nos dois dispositivos IPSec, a negociação de IPSec falhará.

O roteador retorna dos **"a** mensagem **não aceitável atts"** para a proposta do IPsec.

Verifique se os pacotes ISAKMP são obstruídos no ISP

```
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)
```

O acima mostra o flapping do túnel VPN.

Mais, **isakmp do debug crypto da** verificação para verificar que o roteador do spoke está enviando o pacote 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
```

O roteador acima do spoke das mostras do **resultado do debug** está enviando o pacote UDP 500 nos segundos cada 10.

Verifique com o ISP para ver se o roteador do spoke é conectado diretamente ao roteador ISP para se certificar que estão permitindo o tráfego UDP 500.

Depois que o ISP permitiu UDP 500, adicionar o ACL de entrada na interface de saída, que é origem de túnel para permitir que o UDP 500 se certifique do tráfego UDP 500 está entrando o roteador. Use o comando show access-list verificar se as contagens da batida estão incrementando:

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

Cuidado: Certifique-se de você ter o **algum IP** permitido **em** sua lista de acesso. Se não, todo tráfego restante será obstruído como um de entrada aplicado **lista de acesso na** interface de saída.

Verifique se o GRE está trabalhando removendo a proteção do túnel

Quando o DMVPN não está trabalhando, antes de pesquisar defeitos com IPsec, verifique que os túneis GRE estão funcionando muito bem sem criptografia IPSec.

Para mais informação, consulte para configurar o túnel GRE.

O registro NHRP está falhando

O túnel VPN entre o hub and spoke está acima, mas incapaz de passar o tráfego de dados:

```
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 !---
```

Mostra que o tráfego de retorno não está voltando da outra extremidade do túnel.

Verifique a entrada de NHS no roteador do spoke:

```
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
```

Mostra que o pedido de NHS está falhando. Para resolver este problema, certifique-se que a configuração na interface de túnel do roteador do spoke está correta.

Exemplo de configuração:

```
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 !---
```

Exemplo de configuração com a entrada correta para o server de 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 !---
```

Agora, verifique que a entrada de NHS e o IPsec cifram/contadores do decrypt:

```
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 !---
```

Verifique se as vidas estão configuradas corretamente

Use estes comandos verificar a vida atual SA e o momento para a negociação nova seguinte:

- **mostre o detalhe cripto isakmp sa**
- **mostre o <*NBMA-address-peer*> cripto do par IPsec sa**

Observe valores da vida SA. Se são próximos às vidas configuradas (o padrão é 24 horas para o ISAKMP e 1 hora para o IPsec), a seguir esse significa que estes SA têm sido negociados recentemente. Se você olha por pouco tempo mais atrasado e estiveram renegociados outra vez, a seguir o ISAKMP e/ou o IPsec podem saltar para cima e para baixo.

```
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
```

Verifique se os fluxos de tráfego em somente um sentido

O túnel VPN entre o roteador spoke-to-spoke está acima, mas incapaz de passar o tráfego de dados:

```
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 !---
```

Não há nenhum pacote do decap em spoke1, que significa que os pacotes estão deixados cair esp em algum lugar no retorno do trajeto de spoke2 para spoke1.

O roteador spoke2 mostra o encap e o decap, assim que significa que o tráfego ESP está filtrado antes de spoke2 de alcance. Pode acontecer na extremidade ISP em spoke2 ou em todo o Firewall no trajeto entre o roteador spoke2 e o roteador spoke1. Após ter permitido ESP (50 pés do protocolo IP), spoke1 e spoke2 mostram que os encaps e os contadores dos decaps estão incrementando.

```
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 !---
```

Verifique que o vizinho de protocolo de roteamento está estabelecido

O spokes é incapaz de estabelecer o relacionamento do vizinho de protocolo de roteamento:

```
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
```

Verifique se o mapeamento de multicast NHRP é configurado corretamente no hub.

No hub, exige-se para ter o mapeamento de multicast dinâmico do nhrp configurado na interface de túnel do hub.

Exemplo de configuração:

```
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
```

Exemplo de configuração com a entrada correta para o mapeamento de multicast dinâmico do 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 !---
```

Isto permite que o NHRP adicione automaticamente o Roteadores do spoke aos mapeamentos NHRP do Multicast.

Para mais informação, refira a seção **dinâmica do Multicast do mapa do nhrp IP de** comandos 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
```

As rotas ao spokes são instruídas com o protocolo do eigrp.

Problema com o acesso remoto VPN de integração com DMVPN

Problema

O DMVPN está trabalhando muito bem, mas incapaz de estabelecer o RAVPN.

Solução

Use perfis e perfis IPSec ISAKMP para conseguir isto.

Crie perfis separados para o DMVPN e o RAVPN.

Para mais informação, refira o DMVPN e o Easy VPN Server com exemplo de configuração dos perfis ISAKMP.

Problema com duplo-hub-duplo-DMVPN.

Problema

Problema com duplo-hub-duplo-DMVPN. Especificamente, os túneis estão indo para baixo e incapaz de renegociar.

Solução

Use a palavra-chave compartilhada na proteção IPSec do túnel para ambas as interfaces de túnel no hub, e no spoke igualmente.

Exemplo de configuração:

```
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
```

Para mais informação, refira a seção da **proteção do túnel na** referência de comandos do Cisco IOS Security.

Incomode o registro em um server com o DMVPN

Problema

Emita com acesso de um server através da rede de DMVPN.

Solução

O problema poderia ser relacionado ao tamanho MTU e MSS do pacote que está usando o GRE e o IPsec.

Agora, o tamanho do pacote podia ser uma edição com a fragmentação. Para eliminar este problema, use estes comandos:

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

Você poderia igualmente configurar o **comando tunnel path-mtu-discovery** descobrir dinamicamente o tamanho do MTU.

Para mais explicação detalhada, refira a fragmentação de IP da resolução, as edições MTU, MSS, e PMTUD com GRE e IPSEC.

Incapaz de alcançar os server no DMVPN através das determinadas portas

Problema

Incapaz aos servidores de acesso no DMVPN através das portas específicas.

Solução

Verifique desabilitando o conjunto de recursos do firewall de IOS e veja se trabalha.

Se trabalha muito bem, a seguir o problema está relacionado à configuração do firewall de IOS, não com o DMVPN.

Informações Relacionadas

- Dynamic Multipoint VPN (DMVPN)
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems