Solucionar problemas comuns de DMVPN

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
  - Conventions
- Informações de Apoio
- Configuração de DMVPN não funciona
  - Problema
  - Soluções
  - Problemas comuns
    - Verificar a conectividade básica
    - Verifique a política de ISAKMP incompatível
    - Verifique se há um segredo de chave incorreto pré-compartilhado
    - Verifique se há o conjunto de transformação IPsec compatível
  - Verifique se os pacotes ISAKMP são bloqueados no ISP
  - Verifique se o GRE funciona quando a proteção de túnel é removida
  - Falha no registro de NHRP
  - Verifique se os tempos de vida estão configurados corretamente
  - Verifique se os fluxos de tráfego estão em apenas uma direção
  - Verifique se o vizinho do protocolo de roteamento está estabelecido
  - Problema com VPN de acesso remoto com integração de DMVPN
  - Problema
  - Solução
  - Problema com dual-hub-dual-dmvpn
  - Problema
  - Solução
- Problema com o logon em um servidor por meio de DMVPN
  - Problema
  - Solução
  - Não é possível acessar os servidores no DMVPN por determinadas portas
  - Problema
  - Solução
- Informações Relacionadas

Introdução

Este documento descreve as soluções mais comuns para problemas de VPN Multiponto Dinâmico (DMVPN).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento de configuração de DMVPN nos roteadores 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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

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

Informações de Apoio

Este documento descreve as soluções mais comuns para problemas de VPN Multiponto Dinâmico (DMVPN). Muitas dessas soluções podem ser implementadas antes de qualquer solução de problemas detalhada 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.

Para obter mais informações, consulte o Guia de Configuração de VPN Multiponto Dinâmico, Cisco IOS Release 15M&T .

Consulte Compreender e Usar Comandos de Depuração para Identificar e Solucionar Problemas do IPsec para fornecer uma explicação dos comandos debug comuns usados para solucionar problemas do IPsec.

Configuração de DMVPN não funciona

Problema

Uma solução DMVPN recentemente configurada ou modificada não funciona.

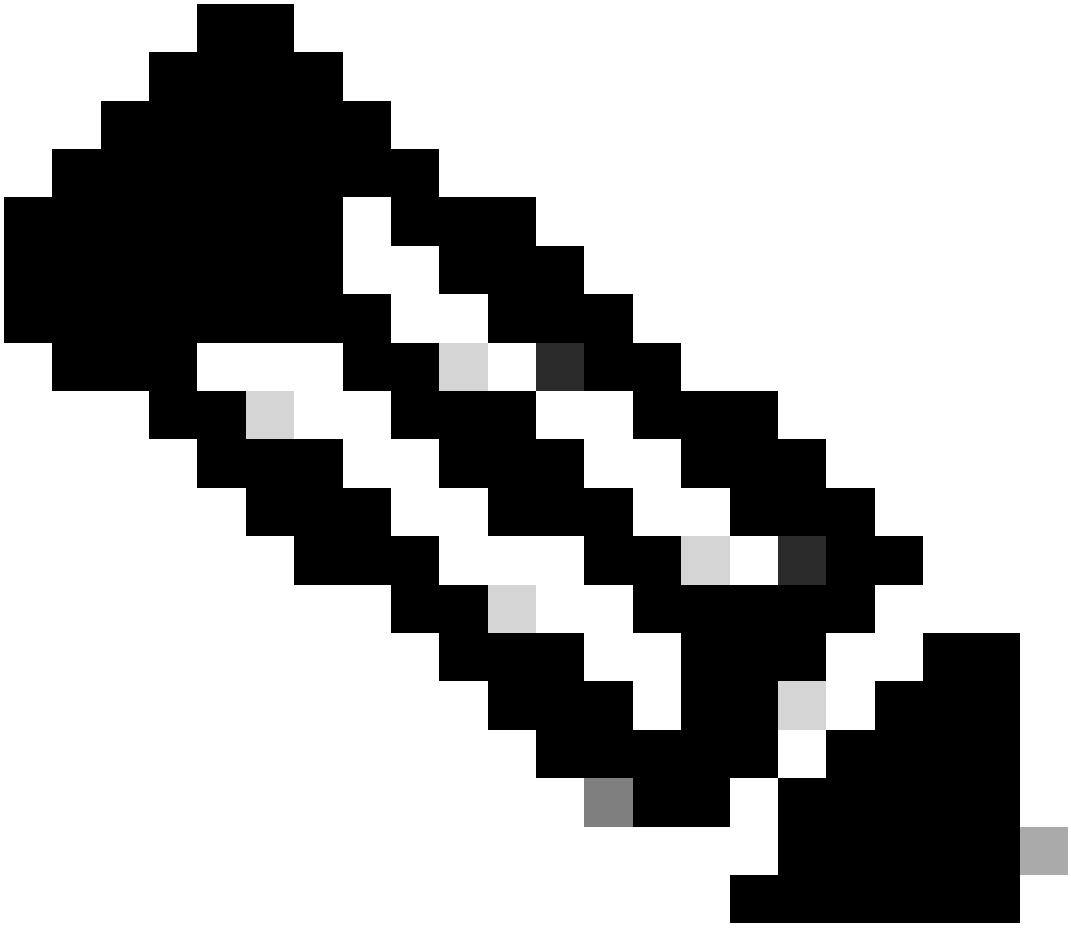
Uma configuração DMVPN atual não funciona mais.

Soluções

Esta seção contém soluções para os problemas mais comuns de DMVPN.

Essas soluções (em nenhuma ordem em particular) podem ser usadas como uma lista de verificação de itens a serem verificados ou tentados antes de você solucionar problemas detalhados :

- Problemas comuns
- Verifique se os pacotes ISAKMP (Internet Security Association and Key Management Protocol) estão bloqueados no ISP (Internet Service Provider).
- Verifique se o GRE (Generic Routing Encapsulation) funciona quando a proteção de túnel é removida.
- Falha no registro do Next-Hop Resolution Protocol (NHRP).
- Verifique se os tempos de vida estão configurados corretamente.
- Verifique se o tráfego flui em apenas uma direção.
- Verifique se o vizinho do protocolo de roteamento está estabelecido.



Observação: antes de começar, verifique as próximas etapas:

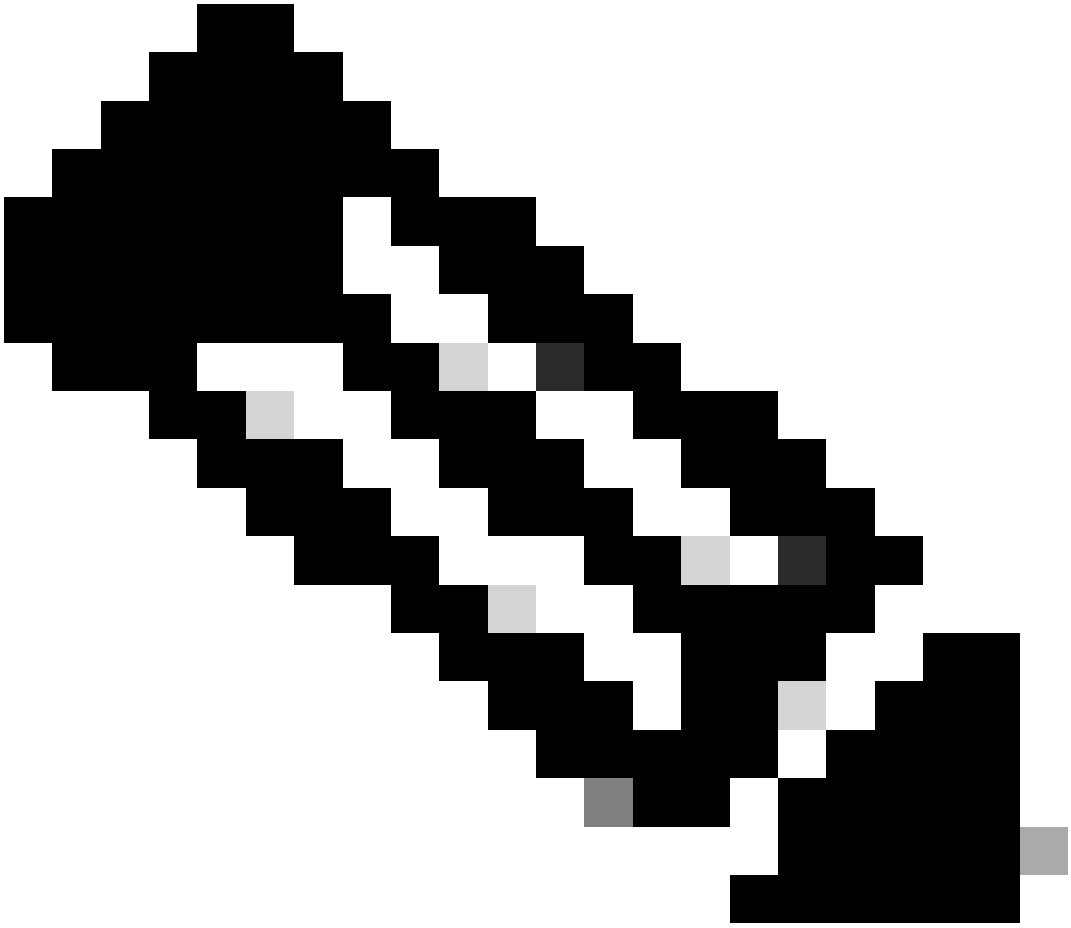
1. A sincronização dos carimbos de hora entre hub e spoke
2. Ativar msec debug e carimbos de hora de log:

```
Router(config)#service timestamps debug datetime msec

Router(config)#service timestamps log datetime msec
```

3. Ativar terminal exec prompt timestamp para sessões de depuração:

```
Router#terminal exec prompt timestamp
```



Observação: dessa forma, você pode correlacionar facilmente a saída do comando debug com a saída do comando show.

Problemas comuns

Verificar a conectividade básica

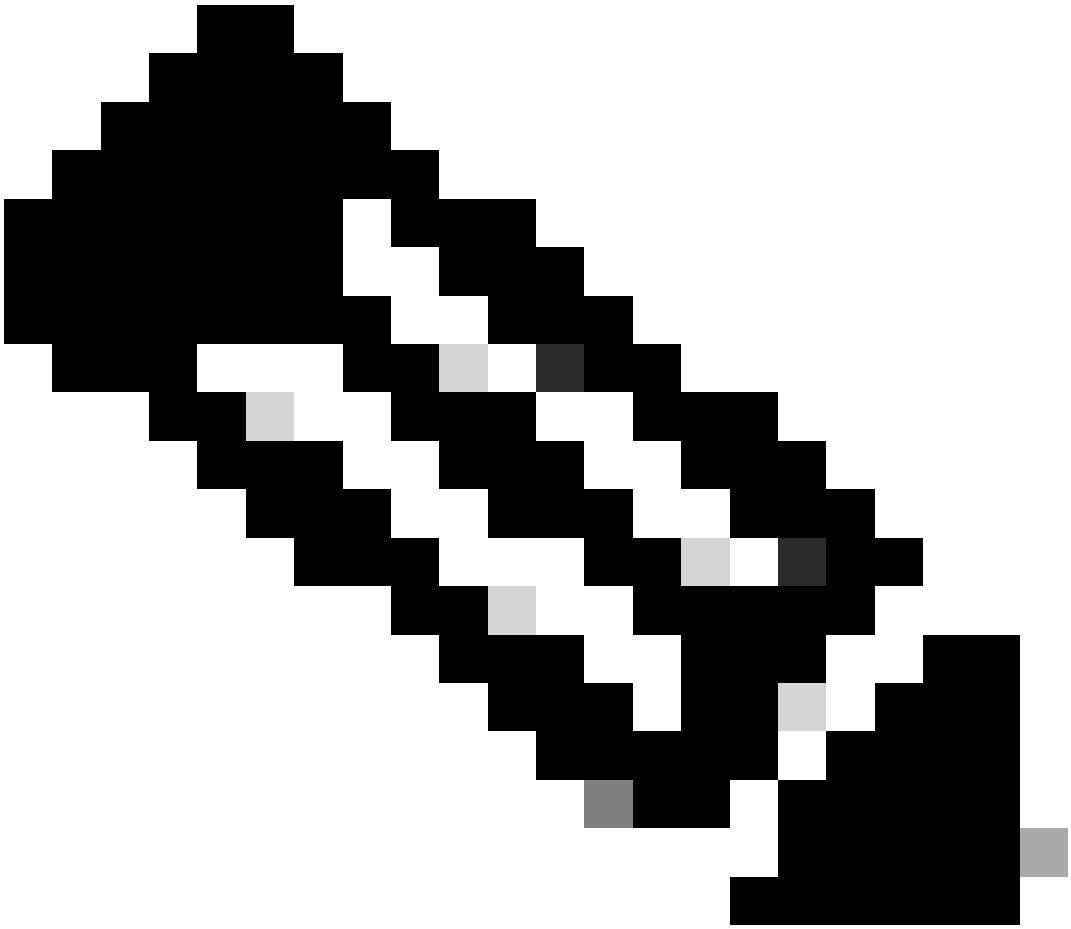
1. Faça ping do hub para o spoke com endereços NBMA e reverta.

   Esses pings devem sair diretamente da interface física, não pelo túnel DMVPN. Espera-se que não seja um firewall que bloqueia os pacotes de ping. Se isso não funcionar, verifique o roteamento e possíveis firewalls entre os roteadores hub and spoke.

2. Além disso, use traceroute para verificar o caminho que os pacotes de túnel criptografados percorrem.

3. Use os comandos debug e show para verificar se não há conectividade:

- debug ip icmp
- debug ip packet



Observação: o comando debug ip packet gera uma quantidade substancial de saída e usa uma quantidade substancial de recursos do sistema. Esse comando deve ser usado com cuidado em redes de produção. Sempre use o comando access-list. Para obter mais informações sobre como usar a lista de acesso com debug ip packet, consulte Solução de problemas com listas de acesso IP.

Verifique se há política ISAKMP incompatível

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

O comando show crypto isakmp sa mostra que a ISAKMP SA está em MM_NO_STATE, o que significa que o modo principal falhou.

Verifique se há um segredo de chave incorreto pré-compartilhado

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

O roteador retorna a mensagem sanity check failed.

Verifique se há o conjunto de transformação IPsec compatível

Se o conjunto de transformação IPsec não for compatível ou não corresponder nos dois dispositivos IPsec, a negociação IPsec falhará.

O roteador retorna a mensagem atts not accept para a proposta IPsec.

Verifique se os pacotes ISAKMP são bloqueados no ISP

<#root>

```
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 exemplo anterior mostra a oscilação de túnel VPN.

Além disso, verifique debug crypto isakmp se o roteador spoke envia o pacote udp 500:

<#root>

```
Router#
```

debug crypto isakmp

<#root>

```
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
```

A debug saída anterior mostra que o roteador spoke envia pacote udp 500 a cada 10 segundos.

Verifique com o ISP se o roteador spoke está conectado diretamente ao roteador ISP para certificar-se de que eles permitam o tráfego udp 500.

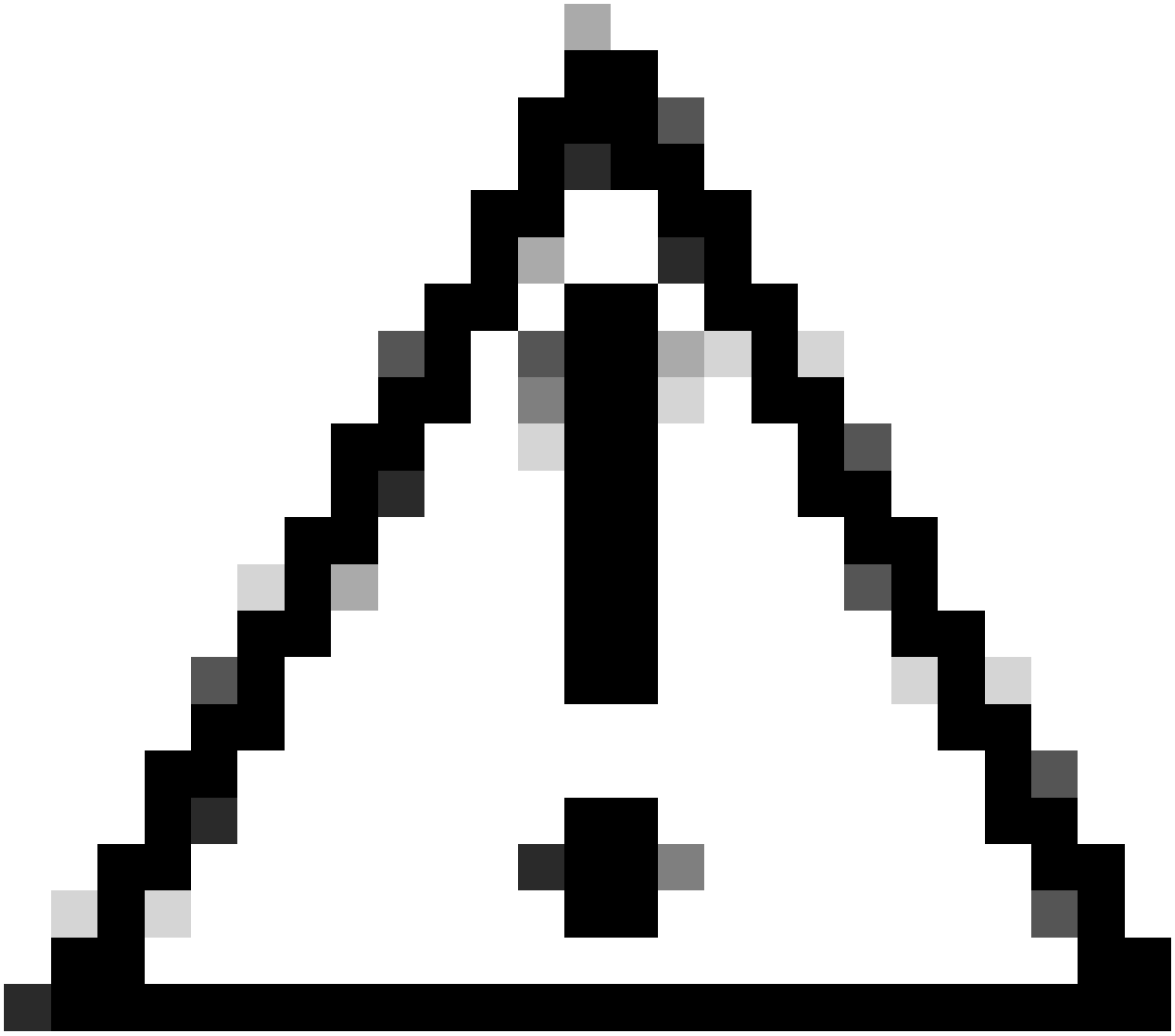
Depois que o ISP permitiu o udp 500, adicione a ACL de entrada na interface de saída, que é a origem do túnel para permitir que o udp 500 verifique se o tráfego udp 500 entra no roteador. Use o show access-listcomando para verificar se as contagens de ocorrências aumentam.

```
    <#root>

Router#


show access-lists 101


Extended IP access list 101
    10 permit udp host 172.17.0.1 host 172.16.1.1 eq isakmp log (4 matches)
    20 permit udp host 172.17.0.5 host 172.16.1.1 eq isakmp log (4 matches)
    30 permit ip any any (295 matches)
```



Cuidado: verifique se você tem ip any any permitido em sua lista de acesso. Caso contrário, todo o tráfego restante pode ser bloqueado como uma lista de acesso aplicada na entrada na interface de saída.

Verifique se o GRE funciona quando a proteção de túnel é removida

Quando o DMVPN não funcionar, antes de solucionar problemas com o IPsec, verifique se os túneis GRE funcionam bem sem a criptografia IPsec.

Para obter mais informações, consulte Como configurar um túnel GRE.

Falha no registro de NHRP

O túnel VPN entre hub e spoke está estabelecido, mas não consegue passar tráfego de dados:

```
<#root>

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


<#root>

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 !---
```

Ele mostra que o tráfego de retorno não volta da outra extremidade do túnel.

Verificar a entrada de NHS no roteador spoke:

```
    <#root>

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 a solicitação NHS falhou. Para resolver esse problema, garanta que a configuração na interface do túnel do roteador spoke está correta.

Exemplo de configuração:

<#root>

```
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 !---

O exemplo de configuração com a entrada correta para o servidor NHS:

<#root>

```
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 a entrada de NHS e contadores de descriptografia/criptografia de IPsec:

<#root>

```
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 os tempos de vida estão configurados corretamente

Use esses comandos para verificar o tempo de vida atual de SA e o momento da próxima renegociação:

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

Observe valores de tempo de vida de SA. Se estiverem perto dos tempos de vida configurados (o padrão é 24h para ISAKMP e 1h para IPsec), então isso significa que esses SAs foram negociados recentemente. Se você olhar um pouco mais tarde e eles tiverem sido negociados novamente, o ISAKMP e/ou IPsec pode estar pulando para cima e para baixo.

<#root>

```
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 estão em apenas uma direção

O túnel VPN entre o roteador spoke-to-spoke está estabelecido, mas não consegue passar tráfego de dados.

<#root>

```
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 pacotes decap no spoke1, o que significa que os pacotes esp foram descartados em algum ponto do caminho voltam do spoke2 para o spoke1.

O roteador spoke2 mostra encap e decap, o que significa que o tráfego ESP é filtrado antes de alcançar spoke2. Isso pode acontecer na extremidade do ISP no spoke2 ou em qualquer firewall no caminho entre o roteador spoke2 e o roteador spoke1. Depois de permitirem ESP (IP Protocol 50), spoke1 e spoke2 mostram incrementos de contadores encaps e decaps.

<#root>

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 se o vizinho do protocolo de roteamento está estabelecido

Spokes não conseguem estabelecer o relacionamento de vizinho do protocolo de roteamento:

<#root>

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 está configurado apropriadamente no hub.

No hub, é necessário que o mapeamento de multicast nhrp dinâmico seja configurado na interface do túnel hub.

Exemplo de configuração:

```
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 network-id 10
 no ip split-horizon eigrp 10
 tunnel mode gre multipoint

!--- !--- Output is truncated !---
```

Exemplo de configuração com a entrada correta do mapeamento de multicast nhrp dinâmico:

<#root>

```
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 !---
```

Isso permite ao NHRP adicionar automaticamente roteadores spoke aos mapeamentos NHRP multicast.

Para obter mais informações, consulte o ip nhrp map multicast dynamic comando na Referência de Comandos de Serviços de Endereçamento IP do Cisco IOS.

<#root>

```
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 para os spokes são aprendidas pelo protocolo eigrp.

Problema com VPN de acesso remoto com integração de DMVPN

Problema

O DMVPN funciona bem, mas não consegue estabelecer o RAVPN.

Solução

Use perfis ISAKMP e IPsec para conseguir isso. Crie perfis separados para DMVPN e RAVPN.

Para obter mais informações, consulte Servidor VPN fácil e DMVPN com exemplo de configuração de perfis ISAKMP.

Problema com dual-hub-dual-dmvpn

Problema

Problema com dual-hub-dual-dmvpn. Especificamente, os túneis são desativados e não podem renegociar.

Solução

Use a palavra-chave compartilhada na proteção IPsec de túnel para as interfaces de túnel no hub e também no spoke.

Um exemplo de configuração:

```
interface Tunnel43
 description <<tunnel to primary cloud>>
 tunnel source interface vlan10
 tunnel protection IPSec profile myprofile shared

!--- !--- Output is truncated !---

interface Tunnel44
 description <<tunnel to secondary cloud>>
 tunnel source interface vlan10
 tunnel protection IPSec profile myprofile shared

!--- !--- Output is truncated !---
```

Para obter mais informações, consulte o **tunnel protection** comando na Cisco IOS Security Command Reference (A-C).

Problema com o logon em um servidor por meio de DMVPN

Problema

O tráfego de saída através do servidor de rede DMVPN não pode ser acessado.

Solução

O problema pode estar relacionado ao tamanho de MTU e MSS do pacote que usa GRE e IPsec.

Agora o tamanho do pacote pode ter um problema com fragmentação. Para eliminar o problema, use estes comandos:

<#root>

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

Você também pode configurar o **tunnel path-mtu-discovery**comando para descobrir dinamicamente o tamanho da MTU.

Para obter uma explicação mais detalhada, consulte Resolver problemas de fragmentação de IP, MTU, MSS e PMTUD com GRE e IPSEC.

Não é possível acessar os servidores no DMVPN por determinadas portas

Problema

Não é possível acessar servidores no DMVPN por portas específicas.

Solução

Para verificar, desative o conjunto de recursos do firewall do Cisco IOS e veja se ele funciona.

Se funcionar bem, o problema está relacionado à configuração do firewall do Cisco IOS, não ao DMVPN.

Informações Relacionadas

- **Dynamic Multipoint VPN (DMVPN)**
- **Negociação IPsec/Protocolos IKE**
- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.