Solución de problemas habituales de DMVPN

Contenido

Introducción

Este documento describe las soluciones más comunes a los problemas de Dynamic Multipoint VPN (DMVPN).

Prerequisites

Requirements

Cisco recomienda que conozca la configuración de DMVPN en los routers CISCO IOS®.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- IOS de Cisco

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Este documento describe las soluciones más comunes a los problemas de Dynamic Multipoint VPN (DMVPN). Muchas de estas soluciones se pueden implementar antes de que se produzca cualquier resolución de problemas detallada de la conexión DMVPN. Este documento se presenta como una lista de verificación de procedimientos comunes que puede intentar antes de comenzar a resolver problemas de una conexión y llamar al Soporte Técnico de Cisco.

Para obtener más información, refiérase a la Guía de Configuración de Dynamic Multipoint VPN, Cisco IOS Release 15M&T.

Consulte Comprensión y Uso de los Comandos Debug para Resolver Problemas de IPsec para proporcionar una explicación de los comandos debug comunes que se utilizan para resolver problemas de IPsec.

La configuración de DMVPN no funciona

Problema

Una solución de DMVPN configurada o modificada recientemente no funciona.

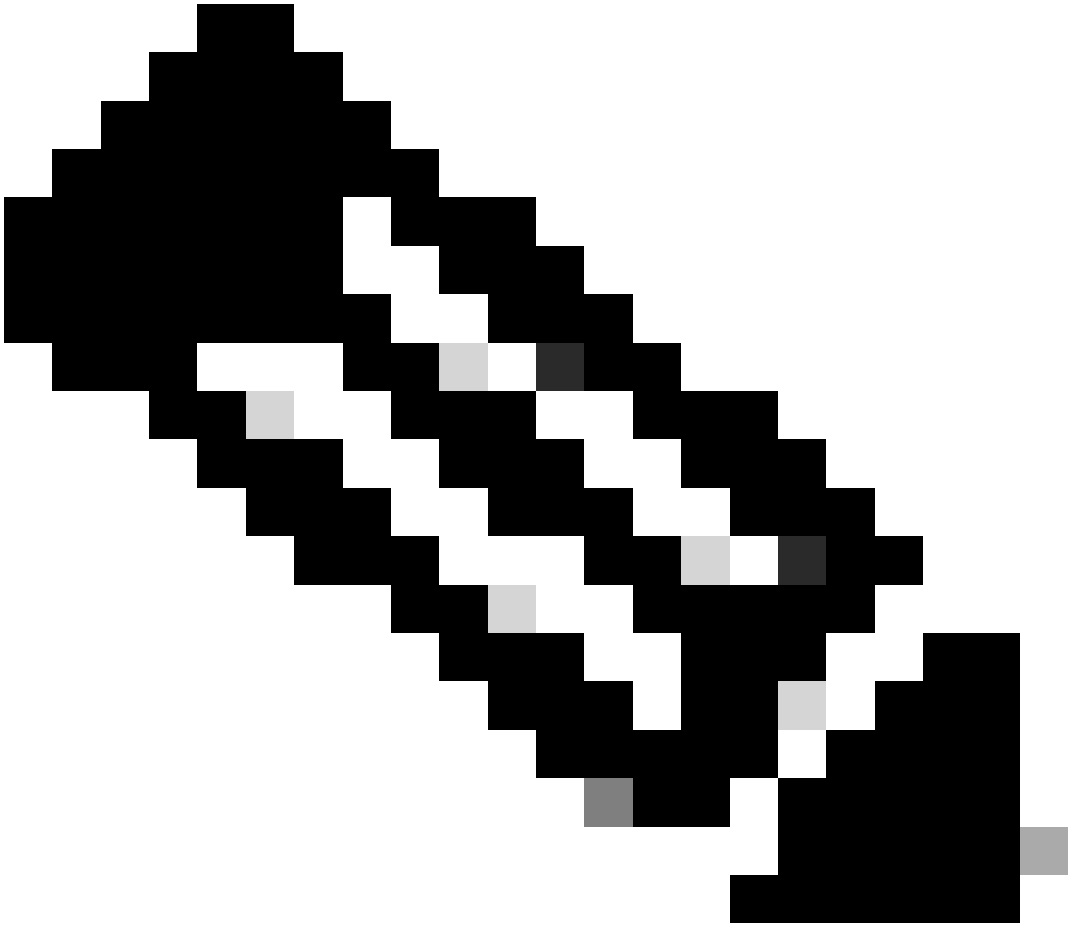
Una configuración de DMVPN actual ya no funciona.

Soluciones

Esta sección contiene soluciones para los problemas de DMVPN más comunes.

Estas soluciones (sin ningún orden en particular) se pueden utilizar como una lista de verificación de elementos para verificar o probar antes de resolver problemas en profundidad :

- Problemas comunes
- Compruebe si los paquetes de Asociación de seguridad de Internet y Protocolo de administración de claves (ISAKMP) están bloqueados en el proveedor de servicios de Internet (ISP).
- Verifique si Generic Routing Encapsulation (GRE) funciona cuando se elimina la protección del túnel.
- Error de registro en el protocolo de resolución de próximo salto (NHRP).
- Verifique si las longitudes están configuradas correctamente.
- Verifique si el tráfico fluye en una sola dirección.
- Verifique que el vecino de protocolo de ruteo esté establecido.



Nota: Antes de empezar, compruebe los siguientes pasos:

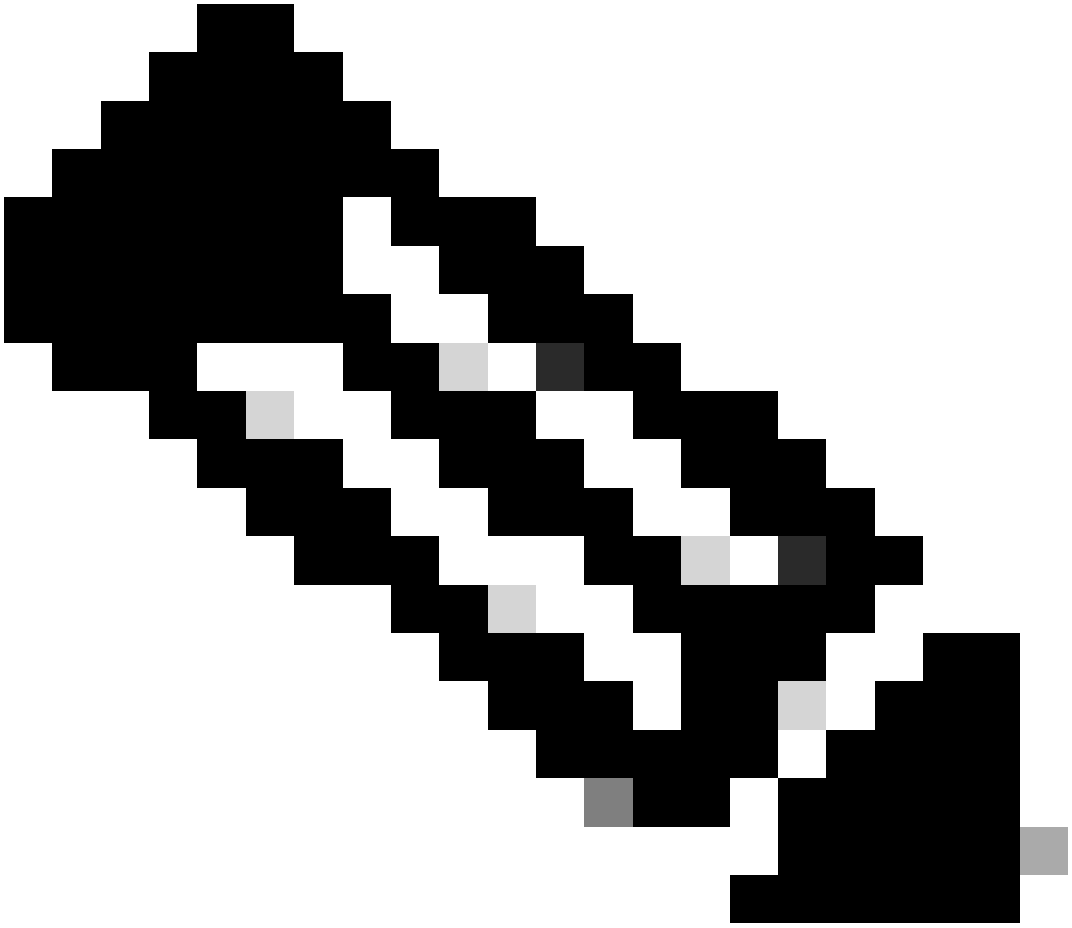
1. Sincronice las marcas de hora entre el concentrador y el dispositivo radial
2. Habilite la depuración de msec y las marcas de hora de registro:

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

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

3. Habilite terminal exec prompt timestamp para las sesiones de depuración:

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



Nota: De esta manera, puede correlacionar fácilmente la salida de debug con la salida del comando show.

Problemas comunes

Compruebe la conectividad básica

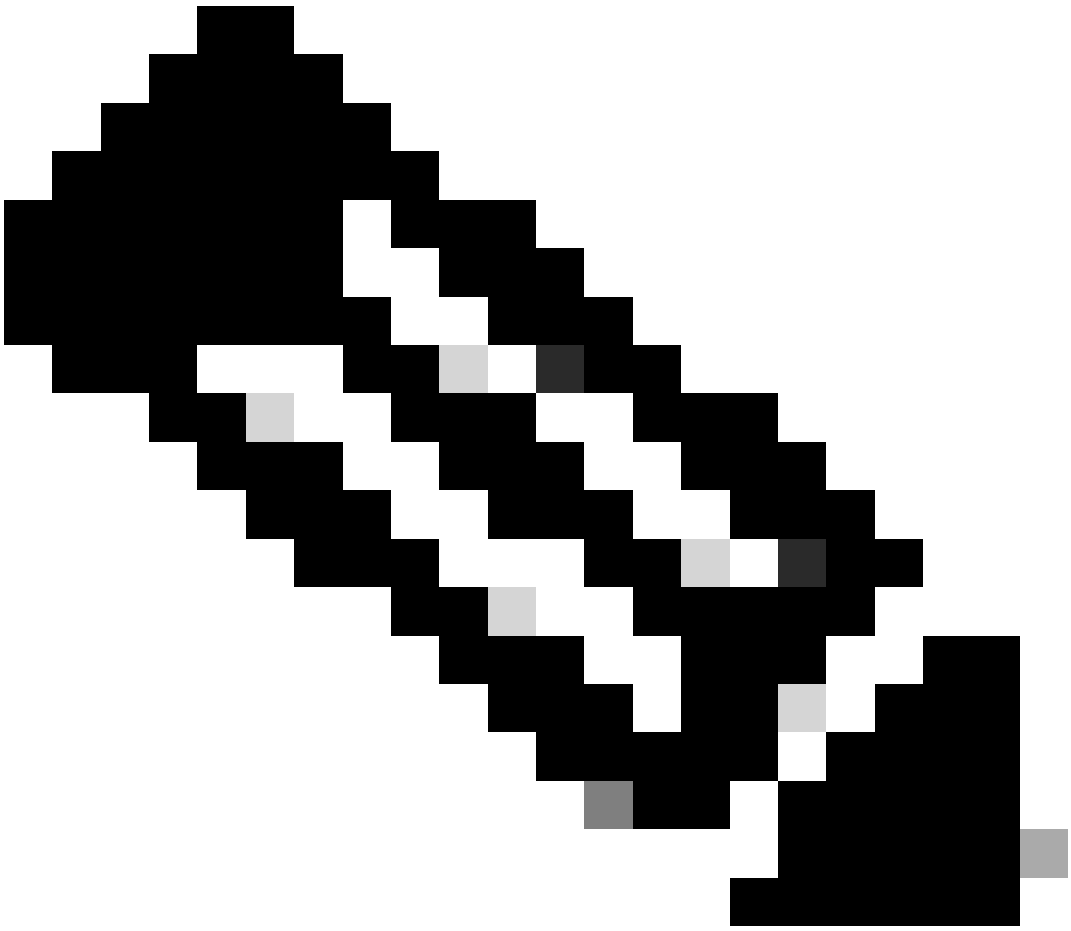
1. Haga ping desde el hub al spoke con las direcciones NBMA y al revés.

   Estos pings deben salir directamente de la interfaz física, no a través del túnel DMVPN. Se espera que no haya un cortafuegos que bloquee los paquetes de ping. Si esto no funciona, compruebe el enrutamiento y los cortafuegos entre los routers de concentrador y de dispositivos radiales.

2. Además, utilice traceroute para verificar la trayectoria que toman los paquetes de túnel cifrado.

3. Use los comandos debug y show para verificar que no haya conectividad:

   - debug ip icmp
   - debug ip packet



> Nota: El comando debug ip packet genera una cantidad sustancial de salida y utiliza una cantidad sustancial de recursos del sistema. Este comando se debe utilizar con precaución en las redes de producción. Siempre debe usarse con el comando access-list. Para obtener más información sobre cómo utilizar la lista de acceso con debug ip packet, consulte Troubleshooting con Listas de Acceso IP.

Compruebe si hay políticas de ISAKMP incompatibles

Si las políticas ISAKMP configuradas no coinciden con la política propuesta por el peer remoto, el router intenta la política predeterminada de 65535. Si esto tampoco coincide, se produce un error en la negociación de ISAKMP.

El comando show crypto isakmp sa muestra que ISAKMP SA está en MM_NO_STATE, lo que significa que el modo principal falló.

Compruebe que la clave secreta compartida previamente sea incorrecta

Si los secretos previamente compartidos no son los mismos en ambos lados, la negociación falla.

El router devuelve el mensaje de verificación de integridad fallida.

Compruebe si el conjunto de transformación de IPsec es incompatible

Si el conjunto de transformación IPSec no es compatible o no coincide en los dos dispositivos IPSec, la negociación IPSec falla.

El router devuelve el mensaje atts not accept para la propuesta de IPSec.

Compruebe si los paquetes de ISAKMP se bloquean en el 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)
```

El ejemplo anterior muestra el túnel VPN inestable.

Además, verifique debug crypto isakmp que el router spoke envíe el paquete 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
```

El debug resultado anterior muestra que el router de radio envía el paquete udp 500 cada 10 segundos.

Verifique con el ISP si el router spoke está conectado directamente con el router ISP para asegurarse de que permiten el tráfico udp 500.

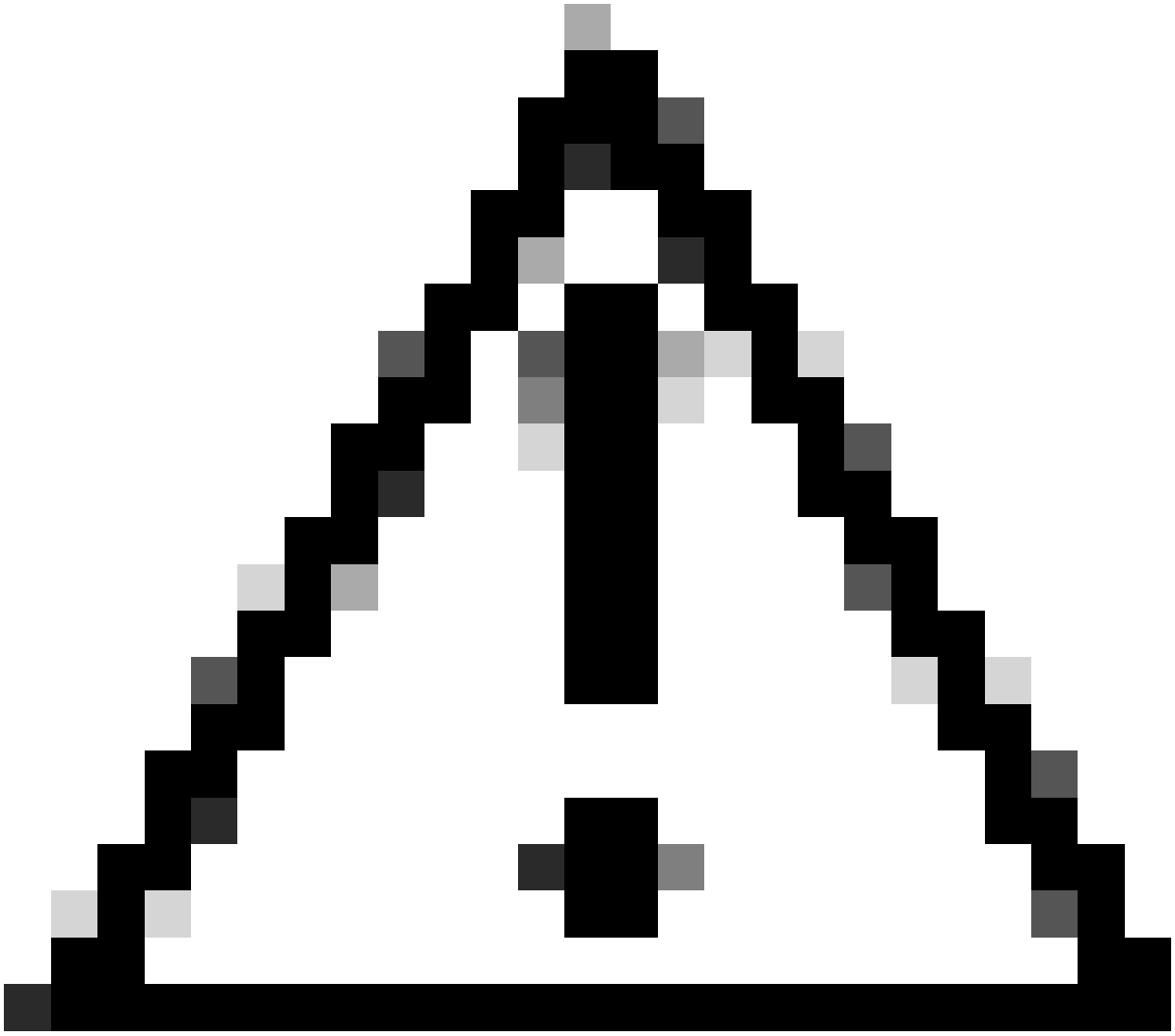
Una vez que el ISP permitió udp 500, agregue la ACL entrante en la interfaz de salida, que es el origen del túnel para permitir que udp 500 se asegure de que el tráfico udp 500 ingrese al router. Utilice el show access-list comando para verificar si se incrementan los recuentos de visitas.

<#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)



Precaución: Asegúrese de que ip any any esté permitido en su lista de acceso. De lo contrario, el resto del tráfico se puede bloquear como una lista de acceso aplicada de forma entrante en la interfaz de salida.

Verifique si GRE funciona cuando se elimina la protección del túnel

Cuando DMVPN no funcione, antes de solucionar problemas con IPsec, verifique que los túneles GRE funcionen correctamente sin cifrado IPsec.

Para obtener más información, consulte Cómo configurar un túnel GRE.

Error de registro NHRP

El túnel VPN entre el concentrador y los dispositivos radiales está activo, pero no deja pasar el tráfico de datos:

```
    <#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 !---
```

Muestra que el tráfico de retorno no regresa desde el otro extremo del túnel.

Compruebe la entrada de NHS en el router de dispositivos radiales:

```
    <#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
```

Muestra que se ha producido un error en la solicitud NHS. Para resolver este problema, asegúrese de que la configuración de la interfaz de túnel del router de dispositivos radiales es correcta.

Ejemplo de configuración:

<#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 !---

Ejemplo de configuración con la entrada correcta del 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 !---

Ahora, compruebe la entrada de NHS y los contadores de cifrado/descifrado 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 !---
```

Verificar si las longitudes están configuradas correctamente

Use estos comandos para comprobar la vida útil actual de SA y la hora de la siguiente renegociación:

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

Observe los valores de vida útil de SA. Si están cerca de la vida útil configurada (el valor predeterminado es 24 horas para ISAKMP y 1 hora para IPsec), esto significa que estas SA se han negociado recientemente. Si mira un poco más tarde y se han negociado de nuevo, entonces el ISAKMP y/o IPSec pueden estar rebotando hacia arriba y hacia abajo.

```
<#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
```

Compruebe si el tráfico fluye en un solo sentido

El túnel VPN entre el router de dispositivos radiales está activo, pero no deja pasar el tráfico de datos.

```
   <#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 !---
```

No hay paquetes de decap en spoke1, lo que significa que los paquetes de esp se descartan en algún punto de la ruta de retorno de spoke2 a spoke1.

El router spoke2 muestra encap y decap, lo que significa que el tráfico ESP se filtra antes de que llegue a spoke2. Puede ocurrir en el extremo del ISP en spoke2 o en cualquier firewall en la trayectoria entre el router spoke2 y el router spoke1. Una vez que permiten ESP (protocolo IP 50), spoke1 y spoke2 muestran incrementos en los contadores encaps y 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 que el vecino de protocolo de ruteo esté establecido

Los dispositivos radiales no pueden establecer la relación de vecino de protocolo de routing:

```
    <#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
```

Compruebe si la asignación de multidifusión de NHRP está configurada correctamente en el concentrador.

En el concentrador, la asignación dinámica de multidifusión de nhrp debe estar configurada en la interfaz de túnel del concentrador.

Ejemplo de configuración:

```
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 !---
```

Ejemplo de configuración con la entrada correcta para la asignación dinámica de multidifusión de nhrp:

<#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 !---
```

Esto permite que NHRP agregue automáticamente los routers de los dispositivos radiales a las asignaciones de NHRP de multidifusión.

Para obtener más información, refiérase al ip nhrp map multicast dynamic comando en la Referencia de Comandos de IP Addressing Services de 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
```

Las rutas a los dispositivos radiales se aprenden a través del protocolo eigrp.

Problema con VPN de acceso remoto con integración DMVPN

Problema

La DMVPN funciona correctamente, pero no puede establecer la RAVPN.

Solución

Para ello, use perfiles de ISAKMP y perfiles de IPsec. Cree perfiles independientes para DMVPN y RAVPN.

Para obtener más información, consulte el Ejemplo de configuración de DMVPN y Easy VPN Server con perfiles de ISAKMP.

Problema con dual-hub-dual-dmvpn

Problema

Problema con dual-hub-dual-dmvpn. Específicamente, los túneles se desactivan y no pueden renegociarse.

Solución

Utilice la palabra clave shared en la protección IPSec de túnel para las interfaces de túnel en el hub y también en el spoke.

Ejemplo de configuración:

```
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 obtener más información, refiérase al **tunnel protection** comando en la Referencia de Comandos de Seguridad de Cisco IOS (A-C).

Problemas al iniciar sesión en un servidor a través de DMVPN

Problema

No se puede acceder al tráfico del problema a través del servidor de red DMVPN.

Solución

El problema podría estar relacionado con el tamaño de MTU y MSS del paquete que utiliza GRE e IPsec.

Ahora, el tamaño del paquete podría ser un problema para la fragmentación. Para eliminar este problema, use estos comandos:

<#root>

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

También puede configurar el **tunnel path-mtu-discovery**comando para detectar dinámicamente el tamaño de MTU.

Para obtener una explicación más detallada, consulte Resolución de problemas de fragmentación de IP, MTU, MSS y PMTUD con GRE e IPSEC.

No se pudo acceder a los servidores en DMVPN a través de determinados puertos

Problema

No se puede acceder a los servidores en DMVPN a través de puertos específicos.

Solución

Para verificar, inhabilite el conjunto de funciones del firewall del IOS de Cisco y vea si funciona.

Si funciona correctamente, el problema está relacionado con la configuración del firewall del IOS de Cisco, no con la DMVPN.

Información Relacionada

- **Dynamic Multipoint VPN (DMVPN)**
- **Negociación IPSec/Protocolos IKE**
- **Soporte técnico y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).