La mayoría de las soluciones comunes del troubleshooting DMVPN

Contenido

Introducción

Este documento contiene la mayoría de las soluciones comunes a los problemas del Dynamic Multipoint VPN (DMVPN). Muchas de estas soluciones se pueden implementar antes del troubleshooting profundizado 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.

Si usted necesita los documentos del ejemplo de configuración para el DMVPN, refiera a los ejemplos de configuración y lista de notas técnicas DMVPN.

Note: Refiera al Troubleshooting de IPSec - Entendiendo y con los comandos debug de proporcionar los **comandos debug de una** explicación de común que se utilizan para resolver problemas los problemas del IPSec.

prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de la configuración DMVPN en el Routers del ® del 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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

La configuración DMVPN no trabaja

Problema

Una solución DMVPN recientemente configurada o modificada no trabaja.

Trabajos actuales de una configuración DMVPN no más.

Soluciones

Esta sección contiene las soluciones a los problemas mas comunes DMVPN.

Estas soluciones (en ningún orden particular) se pueden utilizar como lista de verificación de elementos para verificar o de intento antes de que usted enganche al troubleshooting profundizado:

- Problemas comunes
- Verifique si los paquetes ISAKMP se bloquean en el ISP

- Verifique si el GRE está trabajando muy bien quitando la protección del túnel
- El registro NHRP está fallando
- Verifique si los cursos de la vida estén configurados correctamente
- Verifique si los flujos de tráfico en solamente una dirección
- Verifique que establezcan al vecino del Routing Protocol

Note: Antes de que usted comience, marque éstos:

1. Sincronización-para arriba los grupos fecha/hora entre el hub and spoke
2. **Grupos fecha/hora del debug y del registro milisegundo del** permiso:`Debug de los grupos fecha/hora de Router(config)#service datetime msecRegistro de los grupos fecha/hora de Router(config)#service datetime msec`
3. **Grupo fecha/hora terminal del prompt exec del** permiso para las sesiones de debugging:`Grupo fecha/hora del prompt exec de Router#terminal`

Note: Esta manera, usted puede correlacionar fácilmente la **salida de los debugs** con la **salida del comando show**.

Problemas comunes

Verifique la conectividad básica

1. Haga ping del concentrador al rayo usando los direccionamientos NBMA e invierta.Estos ping deben pasar directamente hacia fuera la interfaz física, no a través del túnel DMVPN. Esperanzadamente, no hay un Firewall que bloquea los paquetes ping. Si esto no trabaja, marque la encaminamiento y cualquier Firewall entre el Routers del hub and spoke.
2. También, **traceroute del** uso para marcar la trayectoria que los paquetes del túnel encriptado están tomando.
3. Utilice los **comandos debug and show** de no verificar ninguna Conectividad:**haga el debug del ICMP del IPhaga el debug del paquete del IPNote**: **El comando debug ip packet** genera una cantidad sustancial de salida y utiliza a una cantidad sustancial de recursos del sistema. Este comando se debe utilizar con cautela en las redes de producción. Utilice siempre con el **comando access-list**.**Note**: Para más información sobre cómo utilizar la **lista de acceso** con el **paquete del IP del debug**, refiera al Troubleshooting con las listas de acceso IP.

Verifique para la política isakmp incompatible

Si las políticas ISAKMP configuradas no coinciden con la política propuesta por el peer remoto, el router intenta la política predeterminada de 65535. Si eso no hace juego tampoco, falla la negociación ISAKMP.

El comando show crypto isakmp sa muestra ISAKMP SA para estar adentro **MM_NO_STATE**, significando al modo principal fallado.

Verifique para el secreto incorrecto de la clave previamente compartida

Si los Secretos previamente compartidos no son lo mismo en los ambos lados, la negociación fallará.

El router vuelve el mensaje **fallado "verificación de integridad"**.

Verifique para el IPSec incompatible transforman el conjunto

Si el transforme el conjunto del IPSec no es compatible o unido mal en los dos dispositivos del IPSec, el IPSec Negotiation fallará.

El router vuelve el mensaje **no aceptable de los "atts"** para la oferta del IPSec.

Verifique si los paquetes ISAKMP se bloquean en el 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)
```

El antedicho muestra el cambio del túnel VPN.

Además, **isakmp del debug crypto del** control a verificar que el router radial esté enviando el paquete 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
```

El router radial antedicho de las demostraciones de la **salida de los debugs** está enviando el paquete UDP 500 en cada 10 segundos.

Marque con el ISP para ver si el router radial está conectado directamente con el router del ISP para aseegurarse los está permitiendo el tráfico UDP 500.

Después de que el ISP permitiera UDP 500, agregue el ACL entrante en la interfaz de egreso, que es origen de túnel para permitir que el UDP 500 se aseegure el tráfico UDP 500 está entrando en al router. Utilice el comando show access-list de verificar si las cuentas del golpe están incrementando:

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

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

Caution: Aseegurese le tener **cualquier del IP** permitido en su lista de acceso. Si no, el resto del tráfico será bloqueado como entrante aplicado **lista de acceso** en la interfaz de egreso.

Verifique si el GRE está trabajando quitando la protección del túnel

Cuando el DMVPN no está trabajando, antes de resolver problemas con el IPSec, verifique que los túneles GRE estén funcionando muy bien sin la encripción de IPSec.

Para más información, refiera a la configuración el túnel GRE.

El registro NHRP está fallando

El túnel VPN entre el hub and spoke está para arriba, pero incapaz de pasar el tráfico de datos:

```
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 !---
```

Muestra que el tráfico de retorno no se está volviendo del otro extremo del túnel.

Entrada del control NHS en el router radial:

```
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 la petición NHS está fallando. Para resolver este problema, aseegurese la configuración en el router radial que la interfaz del túnel está correcta.

Ejemplo de configuración:

```
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 para el servidor 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 !---
```

Ahora, verifique la entrada NHS y el IPSec cifra/los contadores del 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 si los cursos de la vida estén configurados correctamente

Utilice estos comandos de verificar el curso de la vida actual SA y la época para la renegociación siguiente:

- **muestre el detalle crypto isakmp sa**
- **muestre el *<NBMA-address-peer>* crypto del par IPSec sa**

Note los valores del curso de la vida SA. Si están cercanos a los cursos de la vida configurados (el valor por defecto es 24 horas para el ISAKMP y 1 hora para el IPSec), después ese significa que estos SA se han negociado recientemente. Si usted mira un poco mientras que más adelante y se han renegociado otra vez, después el ISAKMP y/o el IPSec pueden despedir hacia arriba y hacia abajo.

```
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 si los flujos de tráfico en solamente una dirección

El túnel VPN entre el router del spoke al spoke está para arriba, pero incapaz de pasar el tráfico de datos:

```
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 del decap en spoke1, que significa que especialmente los paquetes están caídos en alguna parte en la vuelta de la trayectoria de spoke2 hacia spoke1.

El router spoke2 muestra el encap y el decap, así que significa que el tráfico ESP está filtrado antes de spoke2 que alcanza. Puede suceder en el extremo ISP en spoke2 o en cualquier Firewall en la trayectoria entre el router spoke2 y el router spoke1. Después de permitir ESP (protocolo IP 50), spoke1 y spoke2 muestran que el encaps y los contadores de los decaps estén 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 establezcan al vecino del Routing Protocol

El spokes no puede establecer la relación del vecino del Routing Protocol:

```
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 si el mapeo multidifusión NHRP se configura correctamente en el concentrador.

En el concentrador, se requiere para tener mapeo multidifusión dinámico del nhrp configurado en la interfaz del túnel del concentrador.

Ejemplo de configuración:

```
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
```

Ejemplo de configuración con la entrada correcta para el mapeo multidifusión dinámico del 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 !---
```

Esto permite que el NHRP agregue automáticamente a los routeres radiales a los mapeos NHRP del Multicast.

Para más información, refiera a la sección **dinámica del Multicast de la correspondencia del nhrp del IP de los** 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
```

Las rutas al spokes son doctas con el protocolo del eigrp.

Problema con el VPN de acceso remoto de integración con el DMVPN

Problema

El DMVPN está trabajando muy bien, pero incapaz de establecer el RAVPN.

Solución

Utilice los perfiles y los perfiles de ipsec ISAKMP para alcanzar esto.

Cree los perfiles separados para el DMVPN y el RAVPN.

Para más información, refiera al DMVPN y al Easy VPN Server con el ejemplo de configuración de los perfiles ISAKMP.

Problema con el dual-concentrador-dual-DMVPN.

Problema

Problema con el dual-concentrador-dual-DMVPN. Específicamente, los túneles van abajo e incapaz de renegociar.

Solución

Utilice la palabra clave compartida en el túnel protección IPSec para ambas las interfaces del túnel en el concentrador, y en el spoke también.

Ejemplo de configuración:

```
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 más información, refiera a la sección de la **protección del túnel** en la referencia de comandos de la Seguridad de Cisco IOS.

Preocupe el registro en un servidor con el DMVPN

Problema

Publique con acceder un servidor a través de la red DMVPN.

Solución

El problema se podría relacionar con el tamaño MTU y MSS del paquete que está utilizando el GRE y el IPSec.

Ahora, el tamaño de paquetes podía ser un problema con la fragmentación. Para eliminar este problema, utilice estos comandos:

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

Usted podría también configurar el **comando tunnel path-mtu-discovery** de descubrir dinámicamente la talla del MTU.

Para una más explicación detallada, refiera a la resolución fragmentación de IP, los problemas MTU, MSS, y PMTUD con el GRE y el IPSEC.

Incapaz de acceder los servidores en el DMVPN a través de los ciertos puertos

Problema

Incapaz al Access Servers en el DMVPN a través de los puertos específicos.

Solución

Verifique inhabilitando al conjunto de características del escudo de protección IOS y vea si trabaja.

Si trabaja muy bien, después el problema se relaciona con los config del escudo de protección IOS, no con el DMVPN.

Información Relacionada

- Dynamic Multipoint VPN (DMVPN)
- IPSec Negotiation/IKE Protocols
- Soporte Técnico y Documentación - Cisco Systems