Risoluzione dei problemi comuni di DMVPN

Sommario

Introduzione

Questo documento descrive le soluzioni più comuni ai problemi della VPN dinamica con multipunto (DMVPN).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della configurazione di DMVPN sui router Cisco IOS®.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IOS

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Questo documento descrive le soluzioni più comuni ai problemi della VPN dinamica con multipunto (DMVPN). Molte di queste soluzioni possono essere implementate prima di qualsiasi risoluzione approfondita dei problemi della connessione DMVPN. Questo documento viene presentato come un elenco di controllo delle procedure comuni da provare prima di iniziare a risolvere i problemi di una connessione e chiamare il supporto tecnico Cisco.

Per ulteriori informazioni, fare riferimento alla Guida alla configurazione di Dynamic Multipoint VPN, Cisco IOS release 15M&T.

Per una spiegazione dei comandi di debug comuni utilizzati per risolvere i problemi relativi a IPSec, consultare il documento sulla descrizione e l'uso dei comandi di debug per la risoluzione dei problemi relativi a IPSec.

La configurazione di DMVPN non funziona

Problema

Una soluzione DMVPN configurata o modificata di recente non funziona.

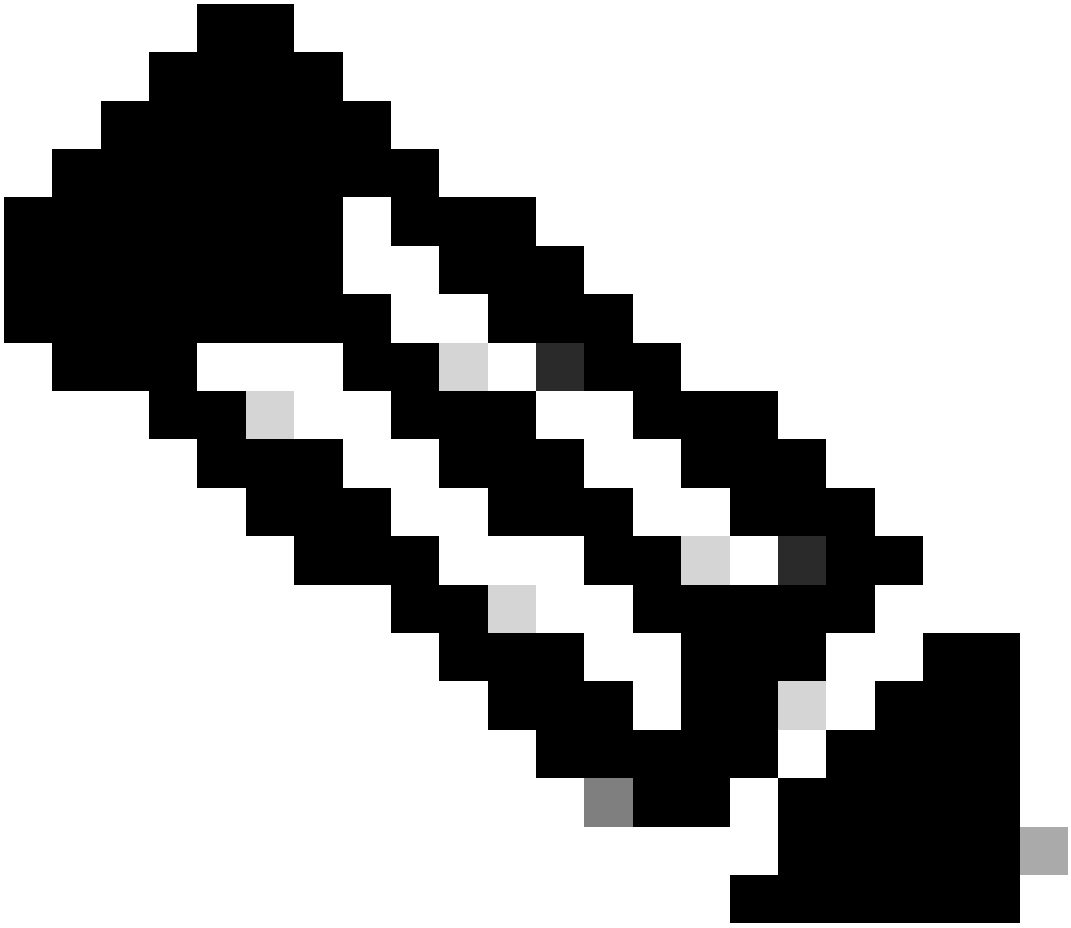
Una configurazione DMVPN corrente non funziona più.

Soluzioni

Questa sezione contiene le soluzioni ai problemi DMVPN più comuni.

Queste soluzioni (nell'ordine indicato) possono essere utilizzate come elenco di controllo degli elementi da verificare o provare prima di procedere con la risoluzione dei problemi:

- Problemi comuni
- Verificare se i pacchetti ISAKMP (Internet Security Association and Key Management Protocol) sono bloccati presso il provider di servizi Internet (ISP)
- Verificare il funzionamento del GRE (Generic Routing Encapsulation) quando viene rimossa la protezione del tunnel
- Registrazione NHRP (Next-Hop Resolution Protocol) non riuscita
- Verifica della corretta configurazione delle durate
- Verifica se il traffico scorre in una sola direzione
- Verificare che il protocollo di routing adiacente sia stato stabilito



Nota: Prima di iniziare, verificare i passaggi successivi:

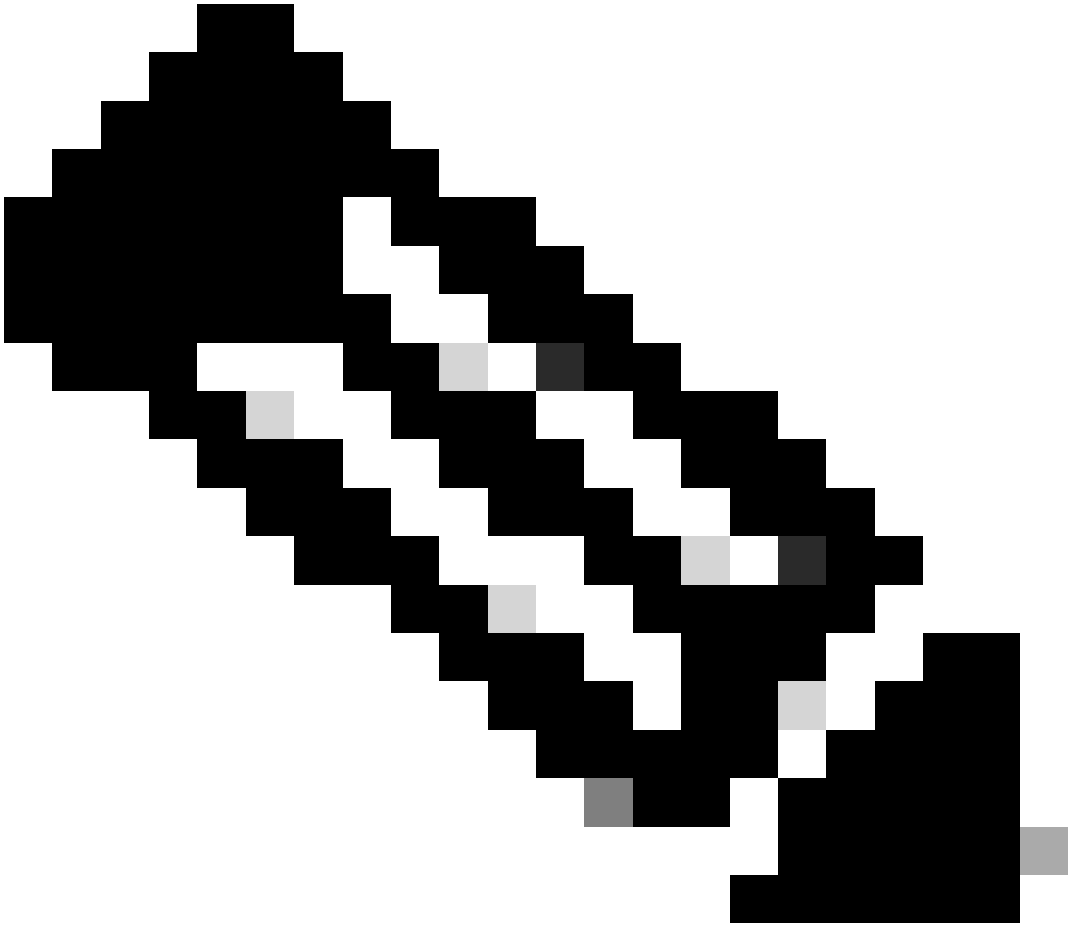
1. Sincronizza i timestamp tra hub e spoke
2. Abilita timestamp log e debug msec:

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

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

3. Abilitare il timestamp del prompt di esecuzione del terminale per le sessioni di debug:

```
Timestamp del prompt Router#terminal
```



Nota: In questo modo, è possibile correlare facilmente l'output del comando debug all'output del comando show.

Problemi comuni

Verifica della connettività di base

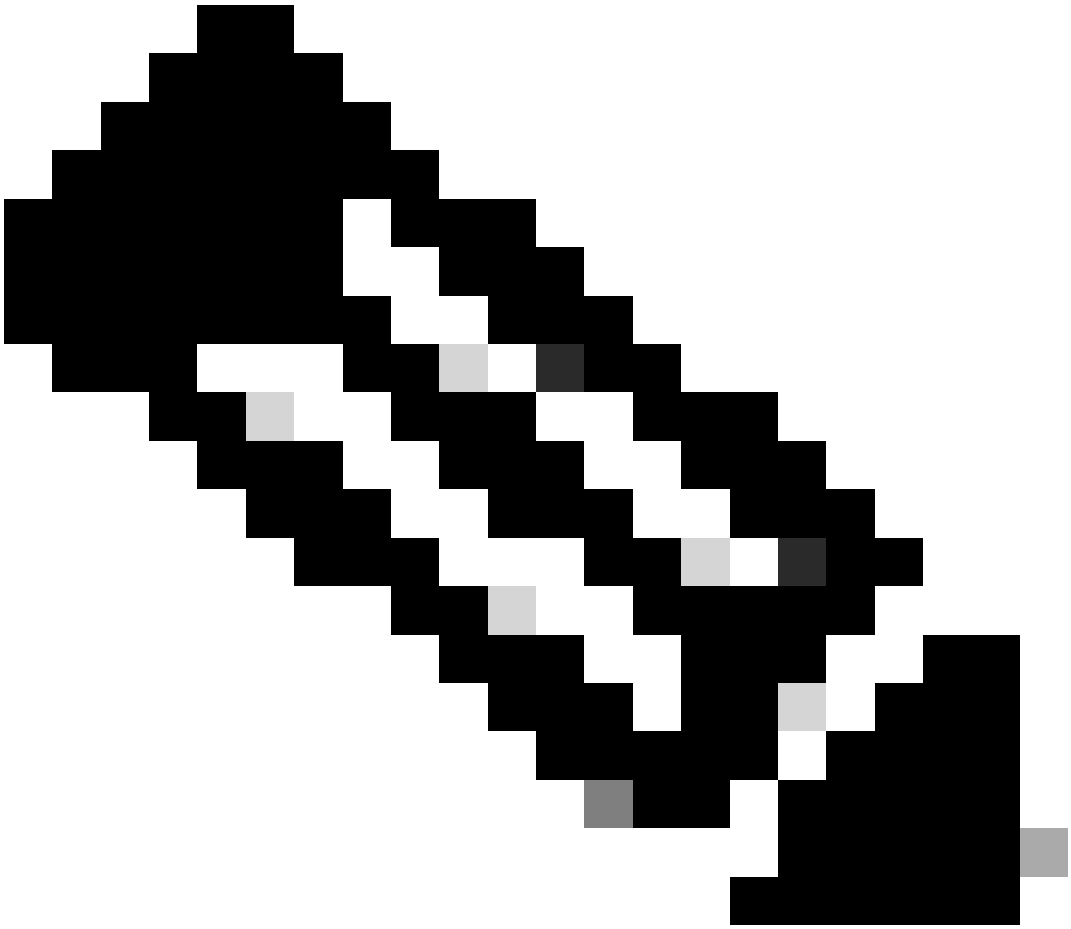
1. Eseguire il ping tra l'hub e il spoke con indirizzi NBMA e inversione.

   I ping devono uscire direttamente dall'interfaccia fisica, non tramite il tunnel DMVPN. Si spera che non vi sia un firewall che blocchi i pacchetti ping. Se l'operazione non riesce, controllare il routing e gli eventuali firewall tra i router hub e spoke.

2. Inoltre, usare traceroute per controllare il percorso dei pacchetti del tunnel crittografati.

3. Per verificare l'assenza di connettività, usare i comandi debug e show:

- debug ip icmp
- debug ip packet



Nota: Il comando debug IP packet genera una quantità sostanziale di output e utilizza una quantità sostanziale di risorse di sistema. Questo comando deve essere utilizzato con cautela nelle reti di produzione. Da utilizzare sempre con il comando access-list. Per ulteriori informazioni su come utilizzare l'elenco degli accessi con il pacchetto IP di debug, consultare il documento sulla risoluzione dei problemi relativi agli elenchi degli accessi IP.

Verifica criteri ISAKMP incompatibili

Se i criteri ISAKMP configurati non corrispondono ai criteri proposti dal peer remoto, il router tenta di utilizzare il criterio predefinito 65535. Se non corrisponde a nessuno dei due, la negoziazione ISAKMP non riesce.

Il comando show crypto isakmp sa mostra che l'associazione di sicurezza ISAKMP è in

MM_NO_STATE, ossia la modalità principale non è riuscita.

Verifica del segreto della chiave già condivisa non corretto

Se i segreti già condivisi non sono gli stessi su entrambi i fronti, la negoziazione fallisce.

Il router restituisce il messaggio di controllo integrità mentale non riuscito.

Verifica set di trasformazioni IPSec incompatibili

Se il set di trasformazioni IPSec non è compatibile o non corrisponde sui due dispositivi IPSec, la negoziazione IPSec non riuscirà.

Il router restituisce il messaggio atts non accettabile per la proposta IPSec.

Verificare se i pacchetti ISAKMP sono bloccati presso l'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)
```

Nell'esempio precedente viene mostrato lo sfarfallio del tunnel VPN.

Inoltre, verificare`debug crypto isakmp` che il router spoke invii un pacchetto 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
```

L'debug output precedente mostra che il router spoke invia un pacchetto UDP 500 ogni 10 secondi.

Verificare con l'ISP se il router spoke è collegato direttamente al router ISP per accertarsi che autorizzi il traffico UDP 500.

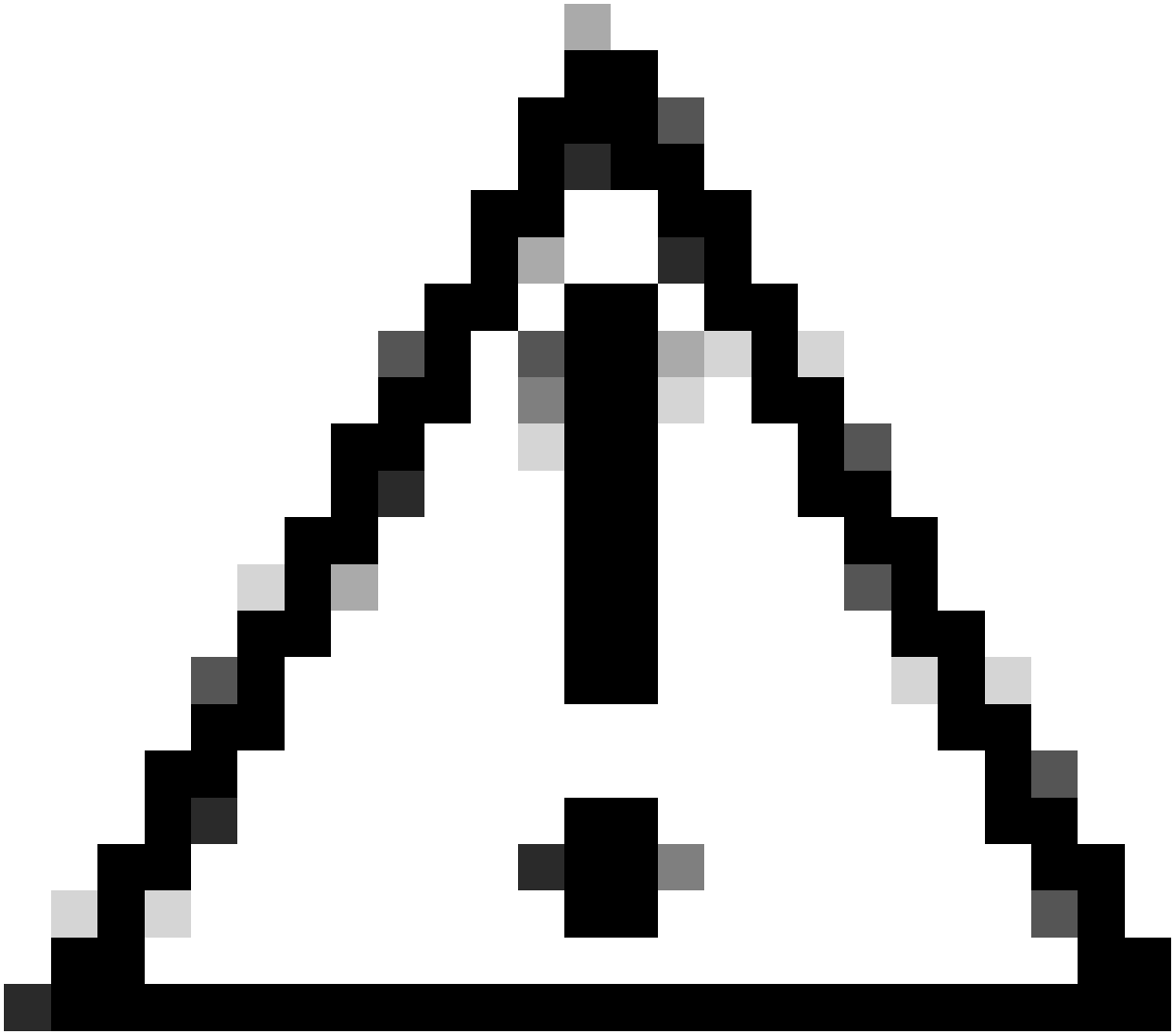
Dopo che l'ISP ha concesso l'UDP 500, aggiungere l'ACL in entrata nell'interfaccia di uscita, che è l'origine del tunnel, in modo da consentire all'UDP 500 di verificare che il traffico UDP 500 entri nel router. Utilizzare ilshow access-listcomando per verificare se il conteggio visite aumenta.

<#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)
```



Attenzione: Verificare che nell'elenco degli accessi sia presente qualsiasi indirizzo IP consentito. In caso contrario, tutto il resto del traffico può essere bloccato come elenco degli accessi applicato in entrata sull'interfaccia di uscita.

Verifica del funzionamento del GRE quando viene rimossa la protezione del tunnel

Se DMVPN non funziona, prima di risolvere i problemi con IPsec, verificare che i tunnel GRE funzionino correttamente senza crittografia IPsec.

Per ulteriori informazioni, consultare il documento sulla configurazione di un tunnel GRE.

Registrazione NHRP non riuscita

Il tunnel VPN tra hub e spoke è attivo, ma non è in grado di passare il traffico di dati:

<#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 !---
```

Mostra che il traffico di ritorno non ritorna dall'altra estremità del tunnel.

Controllare la voce NHS nel router 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
```

Indica che la richiesta NHS non è riuscita. Per risolvere il problema, verificare che la configurazione sull'interfaccia del tunnel del router spoke sia corretta.

Esempio di configurazione:

<#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 !---
```

Esempio di configurazione con la voce corretta per il server 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 !---
```

Verificare quindi la voce NHS e i contatori di crittografia/decrittografia 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 !---
```

Verifica della corretta configurazione delle durate

Utilizzare questi comandi per verificare la durata corrente dell'associazione di protezione e l'ora della successiva rinegoziazione:

- visualizzare i dettagli di crypto isakmp sa
- show crypto ipsec sa peer<NBMA-address-peer>

Notare i valori di durata SA. Se la durata si avvicina a quella configurata (il valore predefinito è 24 ore per ISAKMP e 1 ora per IPsec), le associazioni di protezione sono state negoziate di recente. Se dopo qualche istante vengono nuovamente negoziati, è possibile che il protocollo ISAKMP e/o IPsec sia in aumento o in diminuzione.

<#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
```

Verifica se il traffico scorre in una sola direzione

Il tunnel VPN tra il router spoke-to-spoke è attivo, ma non è in grado di passare il traffico di dati.

<#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 !---
```

Non ci sono pacchetti decap in spoke1, il che significa che i pacchetti esp vengono scartati da qualche parte nel percorso di ritorno da spoke2 verso spoke1.

Il router spoke2 mostra sia l'encap che il decap, ossia il traffico ESP viene filtrato prima di raggiungere spoke2. Può verificarsi all'estremità ISP in spoke2 o in qualsiasi firewall nel percorso tra router spoke2 e router spoke1. Dopo aver consentito l'uso di ESP (IP Protocol 50), spoke1 e spoke2 mostrano entrambi l'incremento dei contatori 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 !---
```

Verificare che il protocollo di routing adiacente sia stato stabilito

Spoke: impossibile stabilire una relazione di protocollo di routing con il router adiacente:

<#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
```

Verificare che il mapping multicast NHRP sia configurato correttamente nell'hub.

Nell'hub è necessario che il mapping multicast NHRP dinamico sia configurato nell'interfaccia del tunnel hub.

Esempio di configurazione:

```
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 !---
```

Esempio di configurazione con la voce corretta per il mapping multicast NHRP dinamico:

<#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 !---
```

Ciò consente a NHRP di aggiungere automaticamente router spoke ai mapping NHRP multicast.

Per ulteriori informazioni, consultare il ip nhrp map multicast dynamic comando nella guida di riferimento dei comandi di Cisco IOS IP Addressing Services.

<#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
```

I percorsi agli spoke vengono appresi attraverso il protocollo Eigrp.

Problema con la VPN ad accesso remoto con integrazione DMVPN

Problema

DMVPN funziona correttamente, ma non è in grado di stabilire la RAVPN.

Soluzione

A tale scopo, utilizzare i profili ISAKMP e IPsec. Creare profili distinti per la VPN DMVPN e la VPN RAVPN.

Per ulteriori informazioni, fare riferimento agli esempi di configurazione di DMVPN e Easy VPN Server con profili ISAKMP.

Problema con la dmvpn dual-hub

Problema

Problema con dmvpn dual-hub. In particolare, i tunnel si interrompono e non possono essere rinegoziati.

Soluzione

Usare la parola chiave shared nella protezione IPsec del tunnel sia per le interfacce tunnel sull'hub sia per lo spoke.

Esempio di configurazione:

```
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 !---
```

Per ulteriori informazioni, consultare il**tunnel protection** comando nella guida di riferimento dei comandi di Cisco IOS Security (A-C).

Problemi di accesso a un server tramite DMVPN

Problema

Impossibile accedere al traffico di uscita attraverso il server di rete DMVPN.

Soluzione

Il problema potrebbe essere correlato alle dimensioni MTU e MSS del pacchetto che usa GRE e IPsec.

Ora, le dimensioni del pacchetto potrebbero essere un problema con la frammentazione. Per risolvere il problema, utilizzare i seguenti comandi:

<#root>

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

È inoltre possibile configurare il **tunnel path-mtu-discovery** comando in modo da individuare dinamicamente le dimensioni dell'MTU.

Per una spiegazione più dettagliata, fare riferimento alla sezione Risoluzione dei problemi di frammentazione IP, MTU, MSS e PMTUD con GRE e IPSEC.

Impossibile accedere ai server su DMVPN tramite alcune porte

Problema

Impossibile accedere ai server su DMVPN tramite porte specifiche.

Soluzione

Per verificare che le funzionalità del firewall di Cisco IOS siano impostate e controllare se funzionano.

Se funziona correttamente, il problema è relativo alla configurazione del firewall di Cisco IOS, non alla DMVPN.

Informazioni correlate

- DMVPN (Dynamic Multipoint VPN)
- Negoziazione IPSec/protocolli IKE
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).