Configurazione di BGP su DMVPN fase 3

Sommario

Introduzione

In questo documento viene descritta la configurazione e il funzionamento di DMVPN fase 3 con BGP, con la risoluzione dei problemi su più livelli per i tunnel IPsec su DMVPN.

Prerequisiti

Per i comandi di configurazione e debug illustrati in questo documento, sono necessari due router Cisco con Cisco IOS® versione 15.3(3)M o successive. In generale, una VPN DMVPN (Dynamic Multipoint VPN) di base fase 3 richiede Cisco IOS versione 12.4(6)T, anche se le funzionalità e i debug illustrati in questo documento non sono completamente supportati.

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- IKEV1/IKEV2 e IPsec
- Componenti VPN:

- Protocollo NHRP (Next Hop Resolution Protocol): Crea un database di mapping distribuito (NHRP) di tutti gli indirizzi del tunnel spoke a quelli reali (interfaccia pubblica)

- Interfaccia tunnel Multipoint Generic Routing Encapsulation (mGRE): Interfaccia GRE (Single Generic Routing Encapsulation) per supportare più tunnel GRE/IPsec, semplificare le dimensioni e la complessità della configurazione e supportare la creazione dinamica del tunnel
- Protezione tunnel IPsec: Creazione e applicazione dinamica di regole di crittografia
- Instradamento: reti dinamiche; sono supportati quasi tutti i protocolli di routing (Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), BGP, ODR)

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco ASR serie 1000 Aggregation Services Router, versione 17.6.5(MD).

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.

Premesse

Che cos'è DMVPN?

DMVPN è una soluzione software Cisco IOS per creare VPN IPsec+GRE in modo facile, dinamico e scalabile. È una soluzione per creare una rete VPN con più siti senza dover configurare tutti i dispositivi in modo statico. Si tratta di una rete "hub and spoke" in cui gli spoke possono comunicare direttamente tra loro senza dover passare attraverso l'hub. La crittografia è supportata tramite IPsec, che rende DMVPN una scelta diffusa per la connessione di siti diversi tramite connessioni Internet regolari.

Come funziona DMVPN?

- Gli spoke creano un tunnel GRE/IPsec permanente dinamico per l'hub, ma non per altri spoke. Si registrano come client del server NHRP (hub).
- Quando un spoke deve inviare un pacchetto a una subnet di destinazione (privata) dietro un spoke diverso, richiede tramite NHRP l'indirizzo reale (esterno) del spoke di destinazione.
- Ora il spoke di origine può avviare un tunnel GRE/IPsec dinamico per il spoke di destinazione (perché conosce l'indirizzo del peer).
- Il tunnel spoke dinamico è costruito sull'interfaccia mGRE.
- Quando il traffico cessa, il tunnel spoke-to-spoke viene rimosso.

Quali sono i diversi tipi di DMVPN?

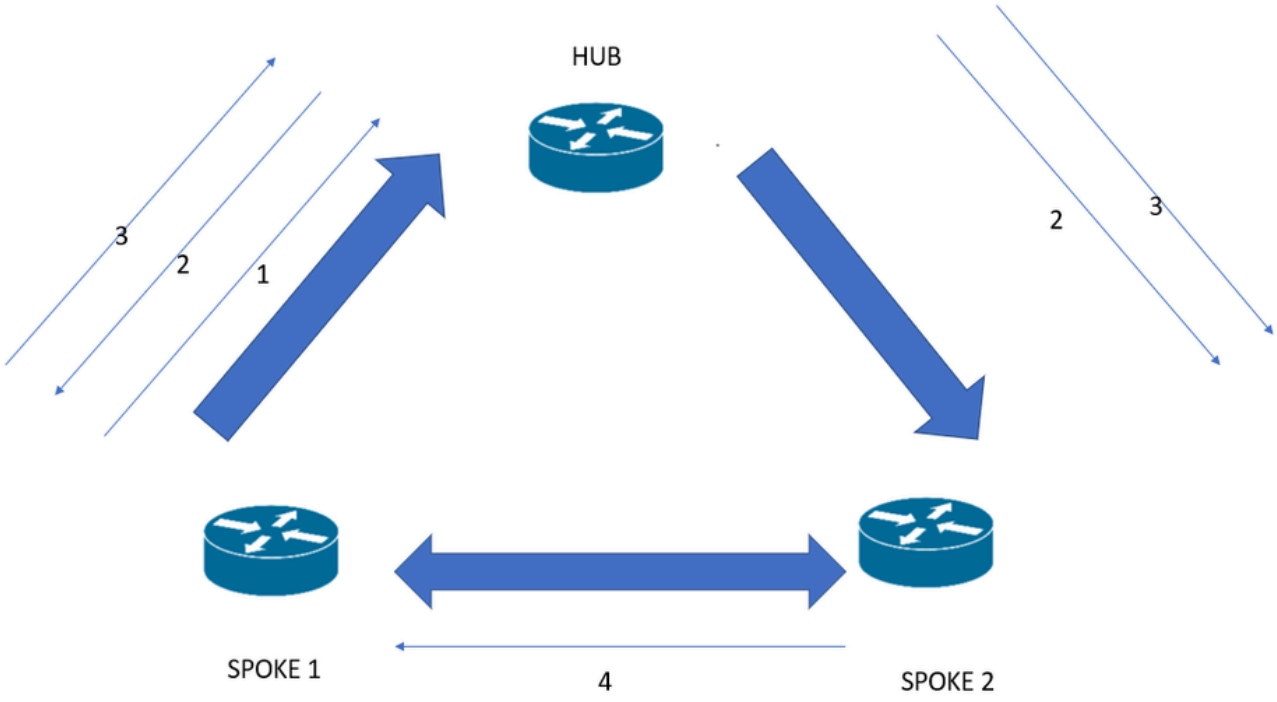
1. DMVPN fase I: Questa fase comporta una singola interfaccia mGRE sull'hub e tutti gli spoke sono ancora tunnel statici, quindi non si ottiene alcuna connettività dinamica spoke-to-spoke.
2. DMVPN fase II: Questa fase prevede la configurazione di tutti i siti con un'interfaccia mGRE

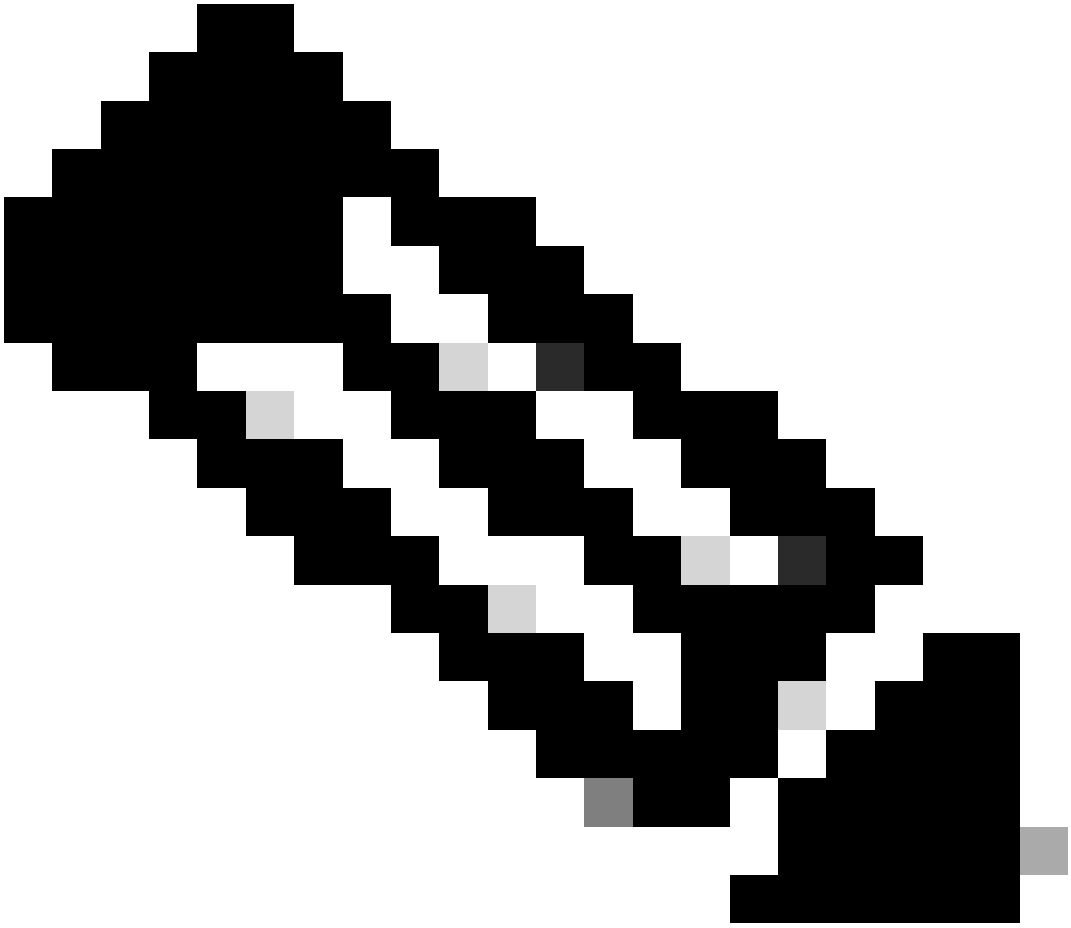
in modo da ottenere la connettività dinamica spoke-to-spoke.

3. DMVPN Fase III: questa fase amplia la scalabilità della rete DMVPN. Questo implica il riepilogo nel cloud DMVPN. Oltre alla configurazione dei reindirizzamenti NHRP e della commutazione dei collegamenti NHRP. I reindirizzamenti NHRP indicano all'origine di trovare un percorso migliore verso la destinazione che si sta cercando di raggiungere. I collegamenti NHRP consentono a DMVPN di ottenere informazioni su altre reti dietro altri router DMVPN.

Flusso del traffico per DMVPN fase 3

1. Il pacchetto viene inviato dalla rete 1 di Spoke alle reti 2 di Spoke tramite Hub (in base alla tabella di routing).
2. L'hub instrada il pacchetto a Spoke2 ma invia parallelamente il messaggio di reindirizzamento NHRP a Spoke1 contenente informazioni sul percorso non ottimale di Spoke2 e l'IP del tunnel di Spoke2.
3. Spoke1 invia quindi la richiesta di risoluzione NHRP dell'indirizzo IP 2 Nonbroadcast Multiaccess (NBMA) di Spoke al server dell'hop successivo (NHS) con l'IP di destinazione del tunnel 2 di Spoke. Questa richiesta di risoluzione NHRP viene inviata indirizzata a Spoke2 tramite NHS (in base alla tabella di routing) - si tratta di un normale processo di inoltro NHRP hop-by-hop.
4. Spoke2 dopo aver ricevuto la richiesta di risoluzione che include l'indirizzo IP NBMA di Spoke1 invia la risposta di risoluzione NHRP direttamente a Spoke1 - Reply non attraversa l'hub!
5. Spoke1 dopo aver ricevuto l'indirizzo IP NBMA corretto di Spoke2, riscrive la voce CEF per il prefisso di destinazione - questa procedura è denominata collegamento NHRP.
6. I raggi non attivano NHRP mediante l'evidenziazione delle adiacenze, ma le risposte NHRP aggiornano l'MCE.



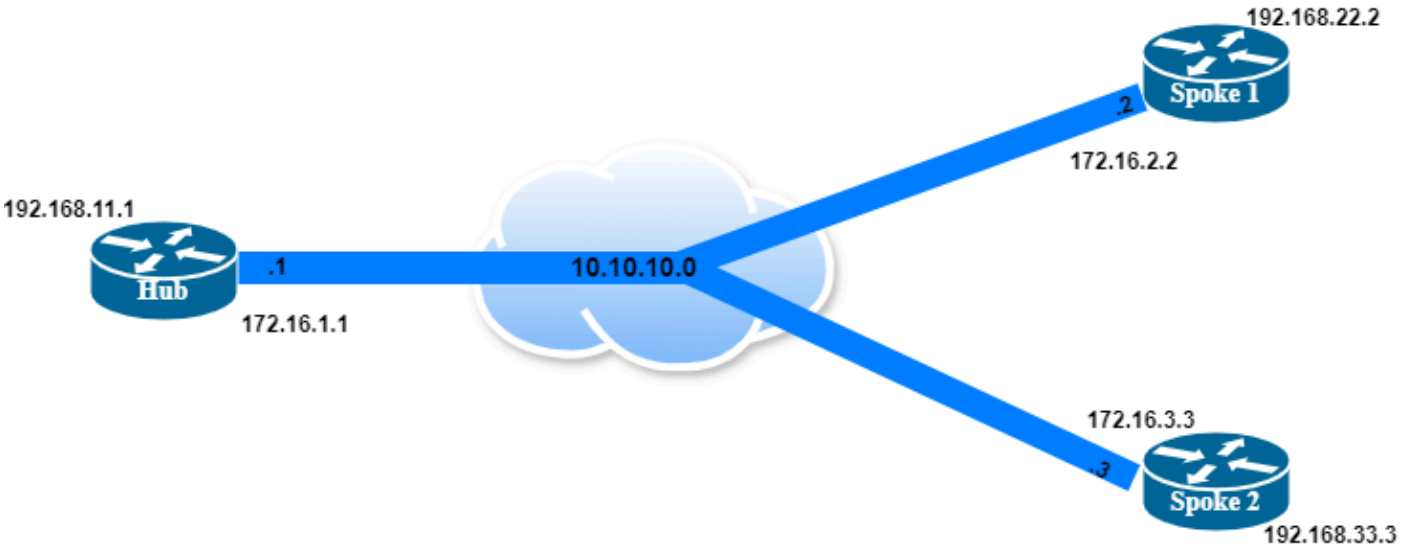


Nota:

DMVPN Fase 2: In questa fase, il pacchetto spoke-to-spoke iniziale è in effetti a commutazione di contesto perché l'adiacenza CEF è in stato "glan". Ciò significa che il router non dispone di informazioni sufficienti per inoltrare il pacchetto utilizzando il protocollo CEF e deve utilizzare una commutazione di processo che richieda un uso più intensivo delle risorse per risolvere l'hop successivo utilizzando il protocollo NHRP (Next Hop Resolution Protocol).

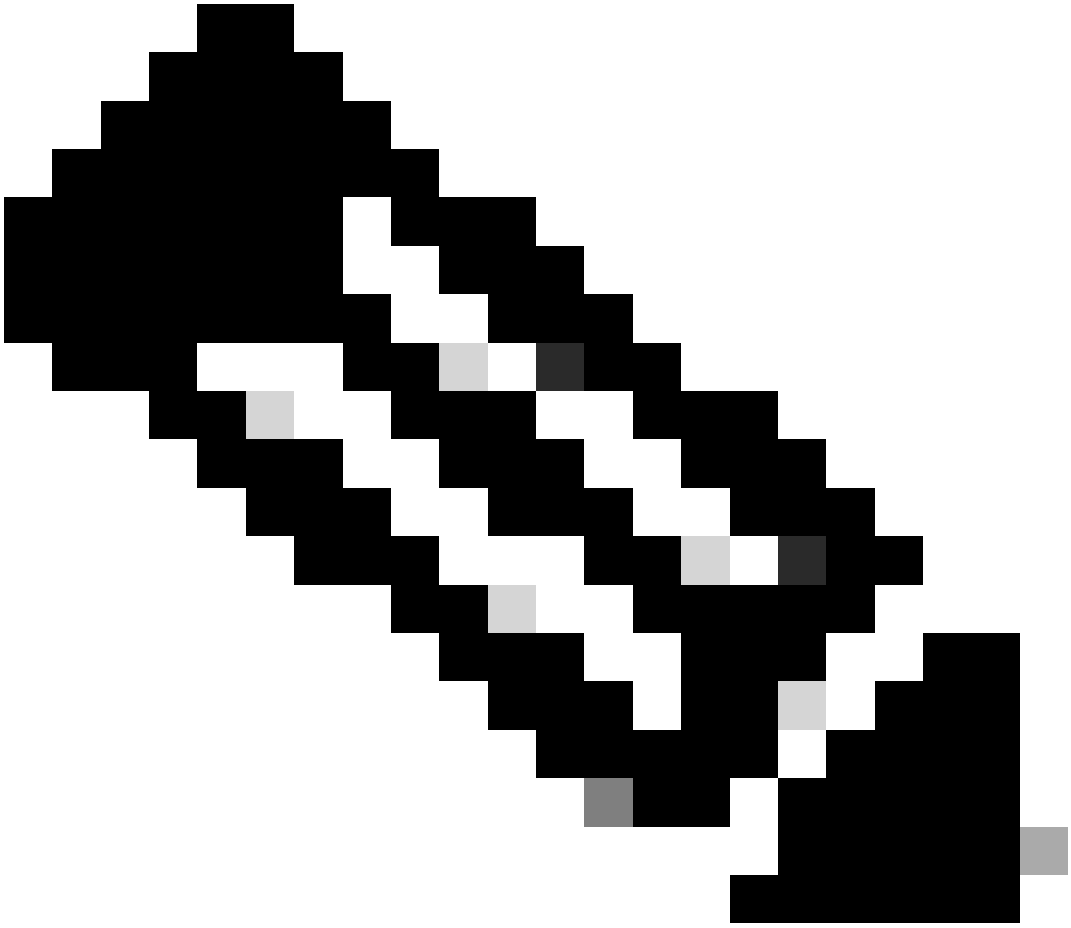
DMVPN Fase 3: Questa fase migliora la Fase 2 consentendo al pacchetto spoke iniziale di essere commutato utilizzando CEF dall'inizio. Questo risultato viene ottenuto tramite le funzionalità di reindirizzamento NHRP e di collegamento NHRP, che consentono di stabilire rapidamente tunnel spoke diretti. Di conseguenza, l'CEF viene utilizzato in modo più coerente, riducendo la dipendenza dal processo di commutazione.

Esempio di rete



Configurazioni

Configurazioni crittografiche



Nota: Questo è lo stesso sull'hub e tutti i raggi.

1. Configurare una proposta Ikev2 e un keyring.

```
crypto ikev2 proposta DMVPN
crittografia aes-cbc-256
integrità sha256
gruppo 14
crypto ikev2 keyring IKEV2-KEYRING
peer any
indirizzo 0.0.0.0 0.0.0.0
chiave già condivisa CISCO123
!
```

2. Configurare il profilo Ikev2 che contiene tutte le informazioni relative alla connessione.

```
crypto ikev2 profile IKEV2-PROF
```

corrispondenza indirizzo interfaccia locale Gigabit Ethernet0/0/0
corrispondenza indirizzo remoto identità 0.0.0.0
pre-condivisione locale di autenticazione
pre-condivisione remota per l'autenticazione
keyring locale IKEV2-KEYRING

Di seguito sono riportati i dettagli dei comandi utilizzati nel profilo ikev2:

- match address local interface Gigabit Ethernet0/0/0: Interfaccia esterna locale dove termina la VPN, in questo caso Gigabit Ethernet0/0/0
- corrispondenza identità indirizzo remoto 0.0.0.0: poiché il peer remoto può essere multiplo, utilizzare 0.0.0.0 che indica qualsiasi peer
- pre-condivisione locale di autenticazione: La modalità di autenticazione nel sito locale è precondivisa
- pre-condivisione remota di autenticazione: La modalità di autenticazione nel sito locale è precondivisa
- keyring locale IKEV2-KEYRING: Usare lo stesso keyring creato in precedenza.

3. Configurare il profilo IPSec.

crypto ipsec transform-set T-SET esp-aes 256 esp-sha256-hmac
tunnel in modalità

profilo ipsec crypto IPSEC-IKEV2

set transform-set T-SET
set ikev2-profile IKEV2-PROF

Creare un set di trasformazioni per la negoziazione del tunnel IPsec e chiamare il set di trasformazioni e il profilo Ikev2 nel profilo IPsec.

Configurazione DMVPN

1. Configurare l'interfaccia esterna.

interfaccia Gigabit Ethernet0/0/0

indirizzo ip 172.16.1.1 255.255.255.0
negoziazione automatica
cdp enable

2. Configurare il router hub per l'integrazione di GRE e IPSec, ovvero associare il tunnel al profilo IPSec configurato nella procedura precedente

interface Tunnel0
indirizzo ip 10.10.10.1 255.255.255.0
no ip redirects
IP nhrp authentication DMVPN

```
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp redirect <— Obbligatorio per abilitare DMVPN fase 3 sul router hub
origine tunnel Gigabit Ethernet0/0/0
modalità tunnel gre multipoint
protezione tunnel profilo ipsec IPSEC-IKEV2
!
```

Questi comandi sono utilizzati nella configurazione dell'interfaccia del tunnel:

- DMVPN autenticazione ip nhrp: In questo caso, la stringa di autenticazione 'DMVPN' deve avere lo stesso valore su tutti gli hub e gli spoke appartenenti alla stessa rete DMVPN.
- multicast dinamico mappa ip nhrp: Consente a NHRP di aggiungere raggi al mapping multicast NHRP in modo dinamico.
- ip nhrp network-id 1: Identificatore di rete a 32 bit che abilita NHRP su un'interfaccia.
- reindirizzamento ip nhrp: Abilita l'indicazione del traffico di reindirizzamento se il traffico viene inoltrato con la rete NHRP.
- origine tunnel Gigabit Ethernet0/0/0: Imposta l'indirizzo di origine per un'interfaccia tunnel, in questo caso si utilizza l'indirizzo IP GigaEthernet 0/0/0.
- modalità tunnel gre multipoint: Imposta la modalità di incapsulamento su mGRE per questa interfaccia del tunnel.
- profilo ipsec di protezione del tunnel IPSEC-IKEV2: Associa un'interfaccia tunnel al profilo IPsec già creato nelle configurazioni crittografiche.

3. Configurare i router Spoke per l'integrazione di GRE e IPsec insieme a un'interfaccia esterna e al loopback per verificare la connettività Border Gateway Protocol (BGP).

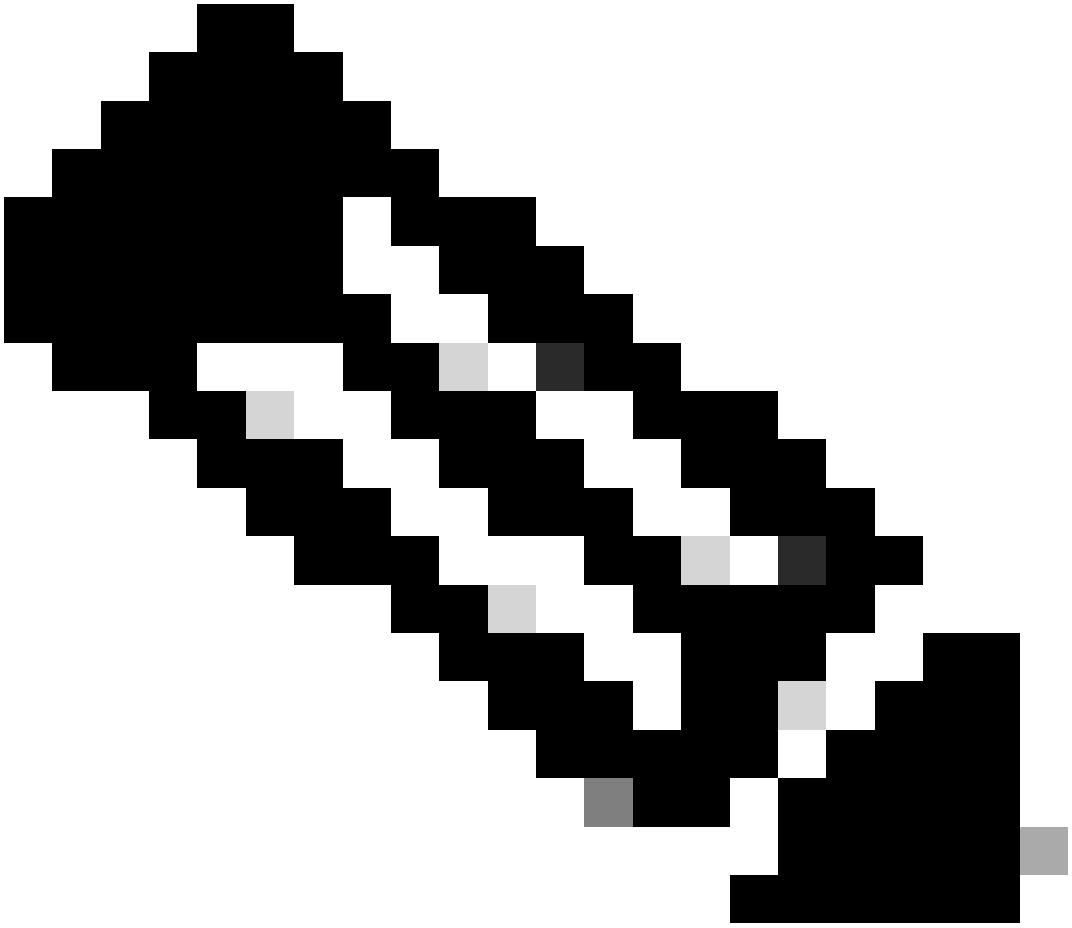
SPOKE X (Una configurazione simile può essere utilizzata in tutti i raggi)

```
interfaccia Gigabit Ethernet0/0/0
indirizzo ip 172.16.3.3 255.255.255.0
speed 1000
nessuna negoziazione automatica

!

interfaccia Loopback10
indirizzo ip 192.168.33.3 255.255.255.0
!
interface Tunnel0
indirizzo ip 10.10.10.3 255.255.255.0
no ip redirects
IP nhrp authentication DMVPN
ip nhrp map 10.10.10.1 172.16.1.1
ip nhrp map multicast 172.16.1.1
ip nhrp network-id 1
ip nhrp nhs 10.10.10.1
ip nhrp shortcut <: obbligatorio per abilitare DMVPN fase 3 su router spoke
```

origine tunnel Gigabit Ethernet0/0/0
modalità tunnel gre multipoint
protezione tunnel profilo ipsec IPSEC-IKEV2

Questi comandi sono utilizzati nella configurazione dell'interfaccia del tunnel:

- DMVPN autenticazione ip nhrp: In questo caso, la stringa di autenticazione 'DMVPN' deve avere lo stesso valore su tutti gli hub e gli spoke appartenenti alla stessa rete DMVPN.
- ip nhrp map 10.10.10.1 172.16.1.1: Esegue manualmente il mapping dell'indirizzo IP NBMA dell'hub con l'indirizzo IP dell'interfaccia del tunnel.
- ip nhrp map multicast 172.16.1.1: Reindirizza tutto il traffico multicast verso l'hub.
- ip nhrp network-id 1: Identificatore di rete a 32 bit che abilita NHRP su un'interfaccia.
- ip nhrp nhs 10.10.10.1: Il server dell'hop successivo corrispondente all'hub viene configurato utilizzando questo comando.
- collegamento ip nhrp: Abilita il passaggio rapido NHRP su un'interfaccia.
- origine tunnel Gigabit Ethernet0/0/0: Imposta l'indirizzo di origine per un'interfaccia tunnel, in questo caso si utilizza l'indirizzo IP GigaEthernet 0/0/0.
- modalità tunnel gre multipoint: Imposta la modalità di incapsulamento su mGRE per questa interfaccia del tunnel.
- profilo ipsec di protezione del tunnel IPSEC-IKEV2: Associa un'interfaccia tunnel al profilo IPsec già creato nelle configurazioni crittografiche.



Nota: Il comando ip nhrp redirect invia il messaggio agli spoke indicante che "il percorso verso lo spoke di destinazione è migliore di quello attraverso l'hub" e il collegamento ip nhrp impone l'installazione di questa route nella base di informazioni per l'inoltro (FIB) sugli spoke.

Configurazione BGP

È possibile scegliere tra diverse varianti:

- eBGP con un numero AS diverso su ciascun spoke
- eBGP con lo stesso numero AS su ciascun spoke
- iBGP

La spiegazione di tutti e tre gli scenari esula dall'ambito del presente documento.

È stato configurato un eBGP con un numero AS diverso su tutti i spoke. Impossibile utilizzare router adiacenti dinamici. Pertanto, è necessario configurare manualmente i router adiacenti.

eBGP con AS diverso sui spoke

1. Configurazione BGP sull'HUB:

Hub(config)#router bgp 6501

Hub(config-router)#bgp log-neighbor-changes

Hub(config-router)#network 192.168.11.1 mask 255.255.255.255

Hub(config-router)#neighbors 10.10.10.2 remote-as 65011

Hub(config-router)#neighbors 10.10.10.3 remote-as 65012

!

Questi comandi vengono utilizzati nella configurazione BGP sull'hub:

- router bgp 65010: Configura un processo di routing BGP. Utilizzare l'argomento 'independent-system-number' che identifica il dispositivo per gli altri altoparlanti BGP.
- network mask 192.168.11.1 255.255.255.255: Specifica una rete locale per questo sistema autonomo e la aggiunge alla tabella di routing BGP.
- neighbors 10.10.10.2 remote-as 65011: Aggiunge l'indirizzo IP del router adiacente Spoke 1 nel sistema autonomo specificato alla tabella dei router adiacenti BGP multiprotocollo IPv4 del dispositivo locale.
- neighbors 10.10.10.3 remote-as 65012: Aggiunge l'indirizzo IP del router adiacente Spoke 2 nel sistema autonomo specificato alla tabella dei router adiacenti BGP multiprotocollo IPv4 del dispositivo locale.

2. Configurazione BGP su spoke X:

Spoke2(config)#router bgp 65012

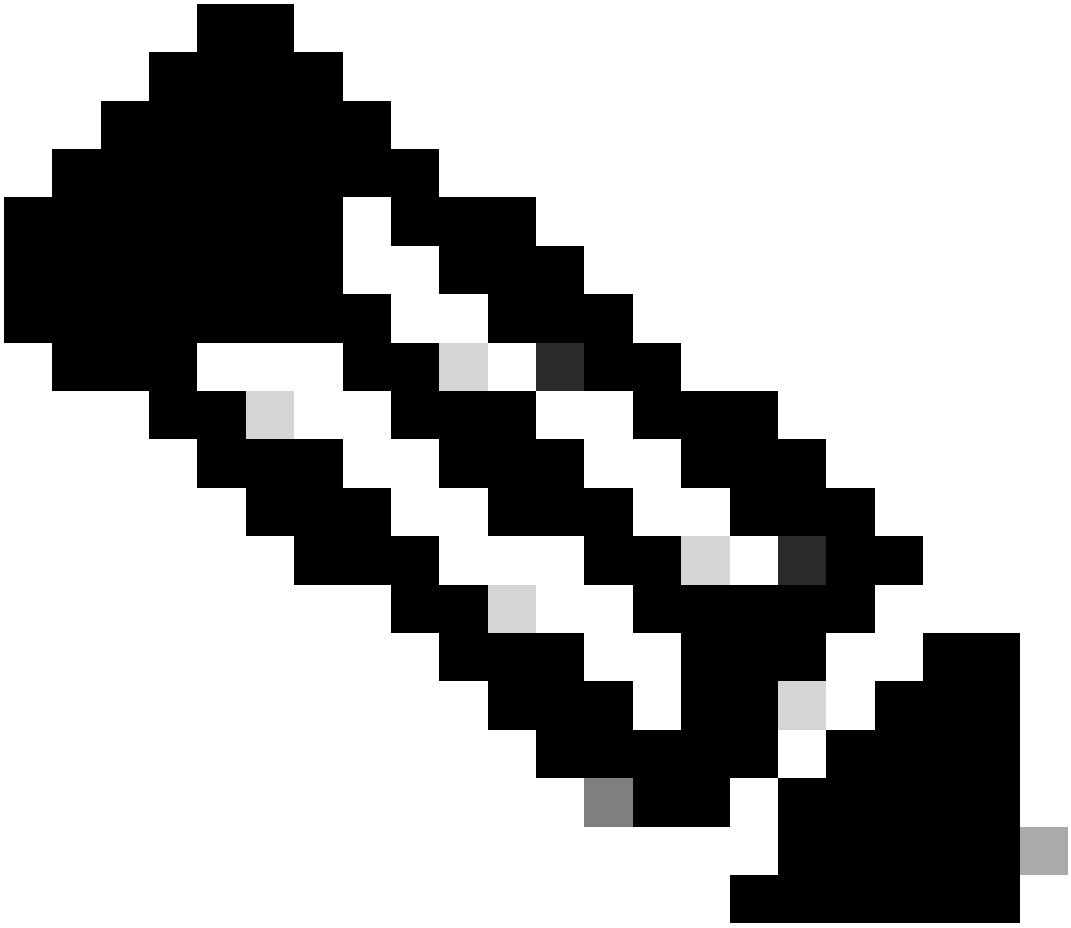
Spoke2(config-router) #bgp log-neighbors-changes

Spoke2(config-router)# rete 192.168.33.3 maschera 255.255.255.255

Spoke2(config-router)# router adiacente 10.10.10.1 remoto-as 65010

Questi comandi vengono utilizzati nella configurazione BGP del spoke X:

- router bgp 65012: Configura un processo di routing BGP. Utilizzare l'argomento 'independent-system-number' che identifica il dispositivo per gli altri altoparlanti BGP.
- network mask 192.168.33.3 255.255.255.255: Specifica una rete locale per questo sistema autonomo e la aggiunge alla tabella di routing BGP.
- router adiacente 10.10.10.1 remoto-as 65010: Aggiunge l'indirizzo IP dell'hub nel sistema autonomo specificato alla tabella dei nodi adiacenti BGP multiprotocollo IPv4 del dispositivo locale.



Nota: Una configurazione simile deve essere eseguita su tutti gli spoke nella rete DMVPN.

Verifica

1. Comandi di verifica sul dispositivo Hub:

HUB#sh dmvpn

Visualizza le informazioni sulla sessione specifica di DMVPN.

Legenda: Attrb —> S - Statico, D - Dinamico, I - Incompleto
N - NATed, L - Locale, X - Senza socket
T1 - Route installata, T2 - Next-Thop-Override
Compatibilità con CTS
Ent —> Numero di voci NHRP con lo stesso peer NBMA
Stato NHS: E —> Risposte Previste, R —> Risposta, W —> In Attesa
Tempo di attività —> Tempo di attività o inattività per un tunnel

==========

Interfaccia: Dettagli NHRP Tunnel0, IPv4
Tipo:Hub, Peer NHRP:2, **<<<<<<<<<<<<<<<<<<<< <>>** Indica che il dispositivo funge da Hub e che due peer NHRP sono connessi all'HUB.

Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
— — — —
1 172.16.2.2 10.10.10.2 UP 01:47:08 D **<<<<<<<<<<<<<<<<<<<<<<<<<<<< << << << <> < < < < < < <>** I peer sono registrati in modo dinamico con l'hub e sono nello stato UP.
1 172.16.3.3 10.10.10.3 UP 01:08:58 D

HUB#sh ip nhrp

Mostra il mapping degli indirizzi NBMA all'IP dell'interfaccia tunnel di tutti i peer NHRP connessi all'hub. Hub gestisce il database di tutti i raggi.

10.10.10.2/32 via 10.10.10.2
Tunnel0 creato 01:47:22, scadenza 01:32:27
Tipo: dinamico, Flag: nhop utilizzato registrato univoco
Indirizzo NBMA: 172.16.2.2
10.10.10.3/32 via 10.10.10.3
Tunnel0 creato 01:09:11, scadenza 01:29:58
Tipo: dinamico, Flag: nhop utilizzato registrato univoco
Indirizzo NBMA: 172.16.3.3

HUB#sh ip nhrp multicast

Visualizza le informazioni sul mapping multicast NHRP.

Indirizzo NBMA I/F
Flag Tunnel0 172.16.2.2: dinamico (abilitato)
Flag Tunnel0 172.16.3.3: dinamico (abilitato)

HUB#sh crypto sockets

Numero di connessioni socket di crittografia 2

Tu0 Peer (locale/remoto): 172.16.1.1/172.16.2.2
Rientro locale (addr/mask/port/port): (172.16.1.1/255.255.255.255/0/47)
Rientro remoto (addr/mask/port/port): (172.16.2.2/255.255.255.255/0/47)
Profilo IPSec: IPSEC-IKEV2
Stato socket: Open (Aperto)
Client: "TUNNEL SEC" (stato client: Attiva)
Tu0 Peer (locale/remoto): 172.16.1.1/172.16.3.3
Rientro locale (addr/mask/port/port): (172.16.1.1/255.255.255.255/0/47)
Rientro remoto (addr/mask/port/port): (172.16.3.3/255.255.255.255/0/47)

Profilo IPSec: IPSEC-IKEV2
Stato socket: Open (Aperto)
Client: "TUNNEL SEC" (stato client: Attiva)
Socket di crittografia in stato di ascolto:
Client: Profilo "TUNNEL SEC": Nome mappa "IPSEC-IKEV2": "Tunnel0-head-0"

HUB#sh cry ikev2 sa

SA IPv4 Crypto IKEv2

Stato fvrf/ivrf remoto locale ID tunnel
1 172.16.1.1/500 172.16.2.2/500 nessuna/nessuna PRONTA
Encr: AES-CBC, dimensione chiave: 256, PRF SHA512, Hash: SHA512, DH Grp:5, segno di autenticazione: PSK, verifica autenticazione: Chiave primaria
Durata/Durata: 8640/6524 sec.

Stato fvrf/ivrf remoto locale ID tunnel
2 172.16.1.1/500 172.16.3.3/500 nessuna/nessuna PRONTA
Encr: AES-CBC, dimensione chiave: 256, PRF SHA512, Hash: SHA512, DH Grp:5, segno di autenticazione: PSK, verifica autenticazione: Chiave primaria
Durata/Durata: 8640/4234 sec.

SA IPv6 Crypto IKEv2

Riepilogo bgp ip HUB#sh

Visualizza lo stato corrente della sessione BGP/il numero di prefissi che il router ha ricevuto da un router adiacente o da un gruppo peer.

Identificatore router BGP 192.168.11.1 locale, numero AS 65010
La versione della tabella BGP è 4, la versione della tabella di routing principale è 4.
3 voci di rete che utilizzano 432 byte di memoria
3 voci di percorso con 252 byte di memoria
3/3 voci dell'attributo path/bestpath BGP che utilizzano 480 byte di memoria
2 voci BGP AS-PATH con 48 byte di memoria
0 voci della cache route-map BGP che utilizzano 0 byte di memoria
0 voci della cache dell'elenco filtri BGP che utilizzano 0 byte di memoria
BGP che utilizza 1212 byte totali di memoria
Prefissi attività BGP 3/0, percorsi 3/0, intervallo di scansione 60 secondi

Adiacente V AS MsgRcvd MsgSent TblVer InQ OutQ Stato Up/Down/PfxRcd
10.10.10.2 4 65011 33 33 4 0 0 00:25:35 1
10.10.10.3 4 65012 21 25 4 0 0 00:14:58 1

Hub#sh ip route bgp

Codici: L - locale, connesso tramite C, S - statico, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP esterno, O - OSPF, IA - OSPF interarea
N1 - Tipo esterno NSSA OSPF 1, N2 - Tipo esterno NSSA OSPF 2

E1 - OSPF tipo esterno 1, E2 - OSPF tipo esterno 2
i - IS-IS, su - IS-IS riepilogo, L1 - IS-IS livello-1, L2 - IS livello-2
ia - IS-IS inter area, * - valore predefinito candidato, U - route statica per utente
o - ODR, P - percorso statico scaricato periodicamente, H - NHRP, l - LISP
a - percorso di applicazione
+ - route replicata, % - override hop successivo, p - override da PfR

Il gateway di ultima istanza è 172.16.1.2 per la rete 0.0.0.0

192.168.0.0/16 è subnet in modo variabile, 4 subnet, 2 maschere
B 192.168.22.0/24 [20/20] via 10.10.10.2, 00:29:15 <<<<<<<<<<< << <<
B 192.168.33.0/24 [20/20] via 10.10.10.3, 00:18:37 <<<<<<<<<<< <<<Voce per route annunciate spoke 2

2. Comandi di verifica nel raggio 1:

Spoke1#sh dmvpn

Legenda: Attrb —> S - Statico, D - Dinamico, I - Incompleto
N - NATed, L - Locale, X - Senza socket
T1 - Route installata, T2 - Next-Thop-Override
C - CTS, I2 - Temporaneo
Ent —> Numero di voci NHRP con lo stesso peer NBMA
Stato NHS: E —> Risposte Previste, R —> Risposta, W —> In Attesa
Tempo di attività —> Tempo di attività o inattività per un tunnel
==========

Interfaccia: Dettagli NHRP Tunnel0, IPv4
Tipo:Spoke, Peer NHRP:2,

Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
— — — —
1 172.16.1.1 10.10.10.1 UP 01:32:09 S <<<<<<<<<<<<<<> L'hub è contrassegnato come S-static perché è stato configurato come entry statico nell'interfaccia del tunnel
1 172.16.3.3 10.10.10.3 UP 00:19:34 D <<<<<<<<<<<<<Tunnel Spoke-to-Spoke dinamico su richiesta creato dopo l'invio del traffico al Spoke 2

Spoke1#sh ip bgp summary

Identificatore router BGP 192.168.22.2, numero AS locale 65011
La versione della tabella BGP è 4, la versione della tabella di routing principale è 4.
3 voci di rete che utilizzano 744 byte di memoria
3 voci di percorso con 432 byte di memoria
3/3 voci dell'attributo path/bestpath BGP che utilizzano 864 byte di memoria
2 voci BGP AS-PATH con 64 byte di memoria
0 voci della cache route-map BGP che utilizzano 0 byte di memoria
0 voci della cache dell'elenco filtri BGP che utilizzano 0 byte di memoria

BGP che utilizza 2104 byte totali di memoria
Prefissi attività BGP 3/0, percorsi 3/0, intervallo di scansione 60 secondi
3 reti hanno raggiunto l'apice alle 08:16:54 giu 2 2022 UTC (01:11:51.732 ago)

Adiacente V AS MsgRcvd MsgSent TblVer InQ OutQ Stato Up/Down/PfxRcd
10.10.10.1 4 65010 85 85 4 0 0 01:12:21 2 <<<<<<<<<<<<<<<<<<<<<< Abbiamo ricevuto 2 prefissi da Hub, ciascuno per il loopback hub e il loopback Spoke2

Spoke1#sh ip route bgp

Codici: L - locale, connesso tramite C, S - statico, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP esterno, O - OSPF, IA - OSPF interarea
N1 - Tipo esterno NSSA OSPF 1, N2 - Tipo esterno NSSA OSPF 2
E1 - OSPF tipo esterno 1, E2 - OSPF tipo esterno 2, m - OMP
N - NAT, Ni - NAT interno, No - NAT esterno, Nd - NAT DIA
i - IS-IS, su - IS-IS riepilogo, L1 - IS-IS livello-1, L2 - IS livello-2
ia - IS-IS inter area, * - valore predefinito candidato, U - route statica per utente
H - NHRP, G - NHRP registrato, g - NHRP riepilogo registrazione
o - ODR, P - percorso statico scaricato periodicamente, l - LISP
a - percorso di applicazione
+ - route replicata, % - override hop successivo, p - override da PfR

Il gateway di ultima istanza è 172.16.2.10 alla rete 0.0.0.0

B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:16 **>>>>>>>>>>** Rete hub raggiungibile direttamente tramite hub

B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:46 **>>>>>>>>>>** Raggiungibile direttamente tramite IP tunnel spoke.

Spoke1#sh route ip

Codici: L - locale, connesso tramite C, S - statico, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP esterno, O - OSPF, IA - OSPF interarea
N1 - Tipo esterno NSSA OSPF 1, N2 - Tipo esterno NSSA OSPF 2
E1 - OSPF tipo esterno 1, E2 - OSPF tipo esterno 2, m - OMP
N - NAT, Ni - NAT interno, No - NAT esterno, Nd - NAT DIA
i - IS-IS, su - IS-IS riepilogo, L1 - IS-IS livello-1, L2 - IS livello-2
ia - IS-IS inter area, * - valore predefinito candidato, U - route statica per utente
H - NHRP, G - NHRP registrato, g - NHRP riepilogo registrazione
o - ODR, P - percorso statico scaricato periodicamente, l - LISP
a - percorso di applicazione
+ - route replicata, % - override hop successivo, p - override da PfR

Il gateway di ultima istanza è 172.16.2.10 alla rete 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.2.10

172.16.2.0/24 è subnet in modo variabile, 2 subnet, 2 maschere
C 172.16.2.0/24 è connesso direttamente, Gigabit Ethernet2
L 172.16.2.2/32 è connesso direttamente, Gigabit Ethernet2
10.0.0.0/8 è subnet in modo variabile, 2 subnet, 2 maschere
C 10.10.10.0/24 è connesso direttamente, Tunnel0
L 10.10.10.2/32 è connesso direttamente, Tunnel0
B 192.168.11.0/24 [20/20] via 10.10.10.1, 01:13:21
192.168.22.0/24 è subnet in modo variabile, 2 subnet, 2 maschere
C 192.168.22.0/24 è connesso direttamente, Loopback10
L 192.168.22.2/32 è connesso direttamente, Loopback10
B 192.168.33.0/24 [20/20] via 10.10.10.3, 01:12:51

Spoke1#sh ip nhrp nhs

Legenda: E=Previste risposte, R=In risposta, W=In attesa, D=Dinamiche
Tunnel0:
10.10.10.1 Priorità RE = 0 cluster = 0 **>>>>>>>** È configurato un solo server dell'hop successivo

Traffico Spoke1#sh ip nhrp

Tunnel0: Limite massimo di invio:10000Pkts/10Sec, Utilizzo:0%
Inviato: Totale 52
1 Richiesta di risoluzione 0 Risposta di risoluzione 51 Richiesta di registrazione **<<<<<<<** <
Numero di volte in cui le richieste di registrazione sono state inviate all'hub
0 Risposta registrazione 0 Richiesta rimozione 0 Risposta rimozione
0 Indicazione di errore 0 Indicazione di traffico 0 Reindirizzamento Soppressione
Ricevuto: Totale 25
0 Richiesta di risoluzione 1 Risoluzione Risposta 0 Richiesta di registrazione **<<<<<<<<<<<<**
Numero di volte in cui abbiamo ricevuto risposte a tali richieste di registrazione
24 Registrazione Risposta 0 Rimozione Richiesta 0 Rimozione Risposta
0 Indicazione di errore 0 Indicazione di traffico 0 Reindirizzamento Soppressione

Spoke1#sh ip nhrp multicast

Indirizzo NBMA I/F
Bandiere Tunnel0 172.16.1.1: static (Enabled) **<<<<<<<<<<<<>** Il traffico multicast è configurato per essere inoltrato verso l'NBMA dell'hub

Spoke1#sh crypto sockets

Numero di connessioni socket di crittografia 2

Tu0 Peer (locale/remoto): 172.16.2.2/172.16.1.1
Rientro locale (addr/mask/port/port): (172.16.2.2/255.255.255.255/0/47)
Rientro remoto (addr/mask/port/port): (172.16.1.1/255.255.255.255/0/47)

Profilo IPSec: IPSEC-IKEV2
Stato socket: Apri <<<<<<<<<<<<<<<<<< < < < <> stato del socket per il peer specifico
Client: "TUNNEL SEC" (stato client: Attiva)
Tu0 Peer (locale/remoto): 172.16.2.2/172.16.3.3
Rientro locale (addr/mask/port/port): (172.16.2.2/255.255.255.255/0/47)
Rientro remoto (addr/mask/port/port): (172.16.3.3/255.255.255.255/0/47)
Profilo IPSec: IPSEC-IKEV2
Stato socket: Open (Aperto)
Client: "TUNNEL SEC" (stato client: Attiva)
Socket di crittografia in stato di ascolto:
Client: Profilo "TUNNEL SEC": Nome mappa "IPSEC-IKEV2": "Tunnel0-head-0"

Spoke1#sh cry ikev2 sa

SA IPv4 Crypto IKEv2

Stato fvrf/ivrf remoto locale ID tunnel
2 172.16.2.2/500 172.16.3.3/500 nessuna/nessuna PRONTA
Encr: AES-CBC, dimensione chiave: 256, PRF SHA512, Hash: SHA512, DH Grp:19, segno di autenticazione: PSK, verifica autenticazione: Chiave primaria
Durata/Durata: 8640/287 sec.

Stato fvrf/ivrf remoto locale ID tunnel
1 172.16.2.2/500 172.16.1.1/500 nessuna/nessuna PRONTA
Encr: AES-CBC, dimensione chiave: 256, PRF SHA512, Hash: SHA512, DH Grp:19, segno di autenticazione: PSK, verifica autenticazione: Chiave primaria
Durata/Durata: 8640/4643 sec.

SA IPv6 Crypto IKEv2

Spoke1#traceroute 192.168.33.3 source lo10

Digitare la sequenza di escape da interrompere.
Tracciamento del percorso fino a 192.168.33.3
Informazioni VRF: (vrf in nome/id, vrf out nome/id)
1 10.10.10.3 3 msec 4 msec * <<<<<<<<<<<<<<<<> Il traffico si dirige direttamente al router Spoke 2 senza passare attraverso l'hub.

Spoke2#sh dmvpn

Legenda: Attrb —> S - Statico, D - Dinamico, I - Incompleto
N - NATed, L - Locale, X - Senza socket
T1 - Route installata, T2 - Next-Thop-Override
C - CTS, I2 - Temporaneo
Ent —> Numero di voci NHRP con lo stesso peer NBMA
Stato NHS: E —> Risposte Previste, R —> Risposta, W —> In Attesa
Tempo di attività —> Tempo di attività o inattività per un tunnel

==========

Interfaccia: Dettagli NHRP Tunnel0, IPv4
Tipo:Spoke, Peer NHRP:2,

Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
— — — —
1 172.16.1.1 10.10.10.1 FINO A 01:20:26 S
1 172.16.2.2 10.10.10.2 UP 00:07:51 D

3. Comandi di verifica su spoke 2:

Spoke2#sh ip nhrp

10.10.10.1/32 via 10.10.10.1
Tunnel0 creato 01:36:06, senza scadenza
Tipo: statico, Flag:
Indirizzo NBMA: 172.16.1.1
10.10.10.2/32 via 10.10.10.2
Tunnel0 creato 00:08:09, scadenza 00:01:50
Tipo: dinamico, Flag: implicito del router
Indirizzo NBMA: 172.16.2.2
10.10.10.3/32 via 10.10.10.3
Tunnel0 creato 00:08:09, scadenza 00:01:50
Tipo: dinamico, Flag: router locale univoco
Indirizzo NBMA: 172.16.3.3
(senza socket)
Multicast Spoke2#sh ip nhrp
Spoke2#sh ip nhrp multicast
Indirizzo NBMA I/F
Flag Tunnel0 172.16.1.1: statico (attivato)
Spoke2#

Socket crittografici Spoke2#sh

Numero di connessioni socket di crittografia 2

Tu0 Peer (locale/remoto): 172.16.3.3/172.16.1.1
Rientro locale (addr/mask/port/port): (172.16.3.3/255.255.255.255/0/47)
Rientro remoto (addr/mask/port/port): (172.16.1.1/255.255.255.255/0/47)
Profilo IPSec: IPSEC-IKEV2
Stato socket: Apri <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< <> lo stato del socket per il peer specifico
Client: "TUNNEL SEC" (stato client: Attiva)
Tu0 Peer (locale/remoto): 172.16.3.3/172.16.2.2
Rientro locale (addr/mask/port/port): (172.16.3.3/255.255.255.255/0/47)
Rientro remoto (addr/mask/port/port): (172.16.2.2/255.255.255.255/0/47)

Profilo IPSec: IPSEC-IKEV2
Stato socket: Open (Aperto)
Client: "TUNNEL SEC" (stato client: Attiva)
Socket di crittografia in stato di ascolto:
Client: Profilo "TUNNEL SEC": Nome mappa "IPSEC-IKEV2": "Tunnel0-head-0"

Spoke2#sh cry ikev2 sa

SA IPv4 Crypto IKEv2

Stato fvrf/ivrf remoto locale ID tunnel
2 172.16.3.3/500 172.16.2.2/500 nessuna/nessuna PRONTA
Encr: AES-CBC, dimensione chiave: 256, PRF SHA512, Hash: SHA512, DH Grp:19, segno di autenticazione: PSK, verifica autenticazione: Chiave primaria
Durata/Durata: 8640/509 sec.

Stato fvrf/ivrf remoto locale ID tunnel
1 172.16.3.3/500 172.16.1.1/500 nessuna/nessuna PRONTA
Encr: AES-CBC, dimensione chiave: 256, PRF SHA512, Hash: SHA512, DH Grp:19, segno di autenticazione: PSK, verifica autenticazione: Chiave primaria
Durata/Durata: 8640/4866 sec.

SA IPv6 Crypto IKEv2

Spoke2#sh ip bgp summary

Identificatore router BGP 192.168.33.3, numero AS locale 65012
La versione della tabella BGP è 4, la versione della tabella di routing principale è 4.
3 voci di rete che utilizzano 744 byte di memoria
3 voci di percorso con 432 byte di memoria
3/3 voci dell'attributo path/bestpath BGP che utilizzano 864 byte di memoria
2 voci BGP AS-PATH con 64 byte di memoria
0 voci della cache route-map BGP che utilizzano 0 byte di memoria
0 voci della cache dell'elenco filtri BGP che utilizzano 0 byte di memoria
BGP che utilizza 2104 byte totali di memoria
Prefissi attività BGP 3/0, percorsi 3/0, intervallo di scansione 60 secondi
3 reti hanno raggiunto l'apice alle 08:16:54 giu 2 2022 UTC (01:20:43.775 ago)

Adiacente V AS MsgRcvd MsgSent TblVer InQ OutQ Stato Up/Down/PfxRcd
10.10.10.1 465010 97 94 4 0 0 01:21:07 2 **>>>>>>>>>>>>>**. Sono stati ricevuti 2 prefissi da Hub, ciascuno per il loopback hub e il loopback Spoke2

Router Spoke2#sh ip

Codici: L - locale, connesso tramite C, S - statico, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP esterno, O - OSPF, IA - OSPF interarea
N1 - Tipo esterno NSSA OSPF 1, N2 - Tipo esterno NSSA OSPF 2
E1 - OSPF tipo esterno 1, E2 - OSPF tipo esterno 2, m - OMP

N - NAT, Ni - NAT interno, No - NAT esterno, Nd - NAT DIA
i - IS-IS, su - IS-IS riepilogo, L1 - IS-IS livello-1, L2 - IS livello-2
ia - IS-IS inter area, * - valore predefinito candidato, U - route statica per utente
H - NHRP, G - NHRP registrato, g - NHRP riepilogo registrazione
o - ODR, P - percorso statico scaricato periodicamente, l - LISP
a - percorso di applicazione
+ - route replicata, % - override hop successivo, p - override da PfR

Il gateway di ultima istanza è 172.16.3.10 alla rete 0.0.0.0

S* 0.0.0.0/0 [1/0] tramite 172.16.3.10
172.16.3.0/24/8 è subnet in modo variabile, 2 subnet, 2 maschere
C 172.16.3.0/24 è connesso direttamente, Gigabit Ethernet3
L 172.16.3.3/32 è connesso direttamente, Gigabit Ethernet3
10.0.0.0/8 è subnet in modo variabile, 2 subnet, 2 maschere
C 10.10.10.0/24 è connesso direttamente, Tunnel0
L 10.10.10.3/32 è connesso direttamente, Tunnel0
B 192.168.11.0/24 [20/20] via 10.10.10.1, 01:47:08
B 192.168.22.0/24 [20/20] via 10.10.10.2, 01:46:45
192.168.33.0/24 è subnet in modo variabile, 2 subnet, 2 maschere
C 192.168.33.0/24 è connesso direttamente, Loopback10
L 192.168.33.3/32 è connesso direttamente, Loopback10

Spoke2#sh ip route bgp

Codici: L - locale, connesso tramite C, S - statico, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP esterno, O - OSPF, IA - OSPF interarea
N1 - Tipo esterno NSSA OSPF 1, N2 - Tipo esterno NSSA OSPF 2
E1 - OSPF tipo esterno 1, E2 - OSPF tipo esterno 2, m - OMP
N - NAT, Ni - NAT interno, No - NAT esterno, Nd - NAT DIA
i - IS-IS, su - IS-IS riepilogo, L1 - IS-IS livello-1, L2 - IS livello-2
ia - IS-IS inter area, * - valore predefinito candidato, U - route statica per utente
H - NHRP, G - NHRP registrato, g - NHRP riepilogo registrazione
o - ODR, P - percorso statico scaricato periodicamente, l - LISP
a - percorso di applicazione
+ - route replicata, % - override hop successivo, p - override da PfR

Il gateway di ultima istanza è 172.16.3.10 alla rete 0.0.0.0

B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:21:11 >>>>>>>>>>>>>Rete hub raggiungibile direttamente tramite hub
B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:20:48 >>>>>>>>>>> Raggiungibile direttamente tramite IP tunnel spoke.

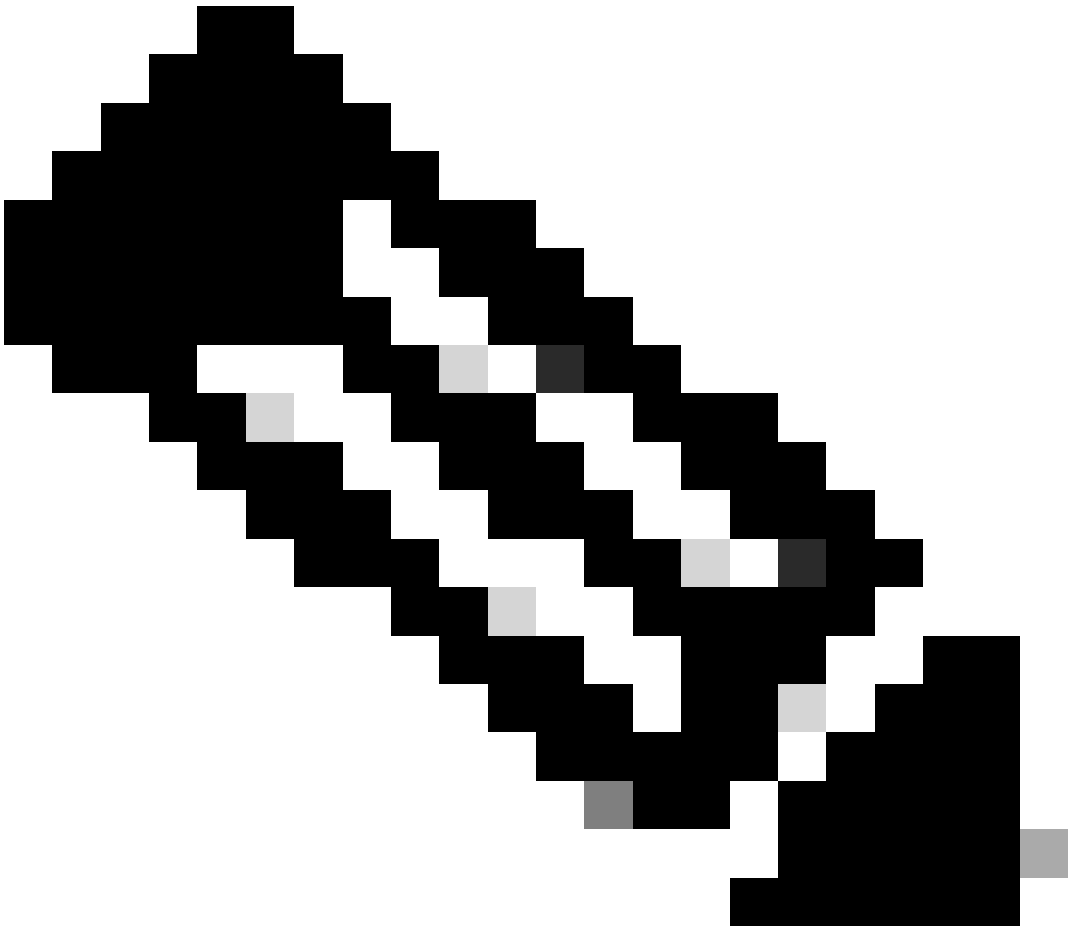
Spoke2#sh ip nhrp nhs

Legenda: E=Previste risposte, R=In risposta, W=In attesa, D=Dinamiche
Tunnel0:
10.10.10.1 Priorità RE = 0 cluster = 0 **>>>>>>>>>>>>** È configurato un solo server dell'hop successivo

Spoke2#traceroute 192.168.22.2 source loopback 10

Digitare la sequenza di escape da interrompere.
Tracciamento del percorso fino a 192.168.22.2
Informazioni VRF: (vrf in nome/id, vrf out nome/id)
1 10.10.10.2 4 msec 4 msec * **<<<<<<<<<<<<<<<<<** Il traffico si dirige direttamente al router Spoke 1 senza passare attraverso l'hub.

Risoluzione dei problemi



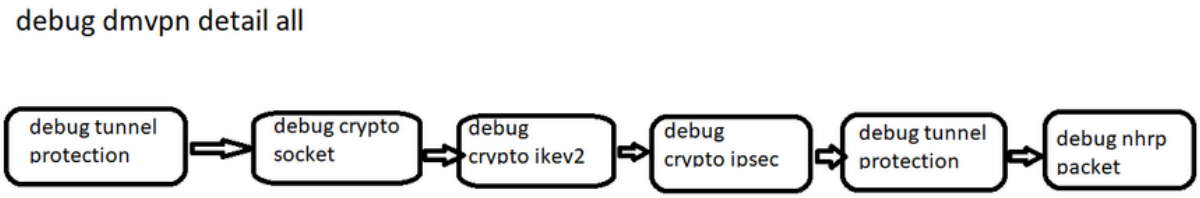
> Nota: Si consiglia sempre di utilizzare i debug condizionali, in quanto l'esecuzione dei debug non condizionali può influire sul processore e quindi sull'ambiente di produzione.

L'indirizzo NBMA corrisponde all'indirizzo IP esterno (indirizzo IP utilizzato per l'origine dell'interfaccia del tunnel) e l'indirizzo IP del tunnel corrisponde all'indirizzo IP logico, ovvero l'indirizzo IP dell'interfaccia del tunnel.

---

debug dmvpn condition peer <nmbma/tunnel> <indirizzo IP NMBA o indirizzo IP tunnel del peer>
debug crypto condition peer ipv4 <IP WAN del peer>
debug nhrp condition peer <nbma/tunnel> <indirizzo IP tunnel o NBMA del peer>

Per risolvere i problemi relativi a DMVPN, è necessario adottare un approccio su più livelli:



1. Livello crittografia: Dopo aver verificato la connettività fisica tra due peer, è necessario verificare la crittografia. Questo livello cripta/decripta i pacchetti GRE.

Comandi di debug comuni utilizzati per verificare la parte relativa alla crittografia:

debug crypto condition peer ipv4 <indirizzo IP WAN del peer>

debug crypto ikev2

errore debug crypto ikev2

debug crypto ikev2 internal

debug crypto ikev2 packet

debug crypto ipsec

errore debug crypto ipsec

O

debug dmvpn condition peer <nmbma/tunnel> <indirizzo IP NMBA o indirizzo IP tunnel del peer>

debug crypto condition peer ipv4 <IP WAN del peer>

debug dmvpn detail crypto

Per ulteriori informazioni sulla risoluzione dei problemi relativi a Encryption Layer, fare riferimento al collegamento esterno:

https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html.

2. GRE/NHRP: Alcuni problemi comuni includono errori di registrazione NHRP e modifiche dinamiche dell'indirizzo NBMA in spoke che portano a mapping NHRP incoerenti nell'hub.

Comandi di debug comuni utilizzati per verificare il mapping NHRP:

debug nhrp condition peer <nbma/tunnel> <indirizzo IP tunnel o NBMA del peer>

debug nhrp cache

debug nhrp packet

debug nhrp detail

errore debug nhrp

Per una comprensione delle soluzioni di risoluzione dei problemi DMVPN più comuni, fare riferimento al collegamento esterno:

https://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html.

3. Instradamento: Il protocollo di routing non monitora lo stato dei tunnel spoke su richiesta.

Gli aggiornamenti del routing IP e i pacchetti di dati multicast IP attraversano solo i tunnel hub e spoke.

I pacchetti di dati IP unicast attraversano sia i tunnel hub e spoke che quelli su richiesta.

Debug: Vari comandi di debug a seconda del protocollo di routing.

Per l'unità profonda del routing BGP, fare riferimento al collegamento esterno:

https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html.

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).