Configurazione e risoluzione dei problemi di FlexVPN Spoke to Spoke tramite EIGRP

Sommario

Introduzione

In questo documento viene descritta la distribuzione e la risoluzione dei problemi di Cisco FlexVPN spoke-to-spoke con IKEv2 e NHRP per tunnel con crittografia client diretta.

Prerequisiti

- Configurazione hub VPN Flex e client VPN Flex

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- IKEv2
- VPN basata sul percorso
- VTI (Virtual Tunnel Interfaces)
- NHRP
- IPSec
- EIGRP
- VRF-Lite

Componenti usati

Le informazioni fornite in questo documento si basano su:

- Cisco IOS XE 17.9.4a

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.

Scalabilità

FlexVPN può essere facilmente espansa dalle reti dei piccoli uffici a quelle delle grandi aziende. È in grado di gestire molte connessioni VPN senza richiedere un lavoro aggiuntivo, il che è ottimo per le organizzazioni in crescita o con molti utenti remoti.

Caratteristiche principali:

- Configurazione dinamica e tunnel on-demand:
  - VTI (Virtual Tunnel Interfaces): FlexVPN utilizza VTI che possono essere create e rimosse in base alle esigenze. Ciò significa che i tunnel VPN vengono configurati solo quando c'è traffico e rimossi quando non sono necessari, risparmiando risorse e migliorando la scalabilità.
  - Protocolli di routing dinamico: Funziona con protocolli di routing come OSPF, EIGRP e BGP su tunnel VPN. In questo modo le informazioni di routing vengono aggiornate automaticamente, un aspetto importante per le reti grandi e dinamiche.
- Flessibilità nell'implementazione:
  - Modello hub e spoke: Un hub centrale si connette a più filiali. FlexVPN semplifica la configurazione di queste connessioni con un unico framework, rendendolo ideale per reti di grandi dimensioni.
  - Topologie Mesh completa e Mesh parziale: Tutti i siti possono comunicare direttamente senza passare attraverso un hub centrale, riducendo i ritardi e migliorando le prestazioni.
- Alta disponibilità e ridondanza:
  - Hub ridondanti: Supporto di più hub per il backup. In caso di guasto di un hub, le filiali possono connettersi a un altro hub, garantendo una connettività continua.

    - Bilanciamento del carico: Distribuisce le connessioni VPN su più dispositivi per evitare che un singolo dispositivo diventi sovraccarico, il che è fondamentale per mantenere le prestazioni in installazioni di grandi dimensioni.
- Autenticazione e autorizzazione scalabili:
    - Integrazione AAA: Funziona con server AAA come Cisco ISE o RADIUS per la gestione centralizzata di credenziali e policy utente, essenziali per l'utilizzo su larga scala.
    - PKI e certificati: Supporta PKI (Public Key Infrastructure) e certificati digitali per un'autenticazione sicura, più scalabile rispetto all'utilizzo di chiavi già condivise, soprattutto in ambienti di grandi dimensioni.

Premesse

FlexVPN e NHRP

Il server FlexVPN fornisce la funzionalità sul lato server di FlexVPN. Il client FlexVPN stabilisce un tunnel VPN IPsec sicuro tra un client FlexVPN e un altro server FlexVPN.

NHRP è un protocollo simile al protocollo ARP (Address Resolution Protocol) che riduce i problemi di rete non broadcast multiaccess (NBMA). Con NHRP, le entità NHRP collegate a una rete NBMA apprendono dinamicamente l'indirizzo NBMA delle altre entità che fanno parte di tale rete, consentendo a tali entità di comunicare direttamente senza richiedere al traffico di utilizzare un hop intermedio.

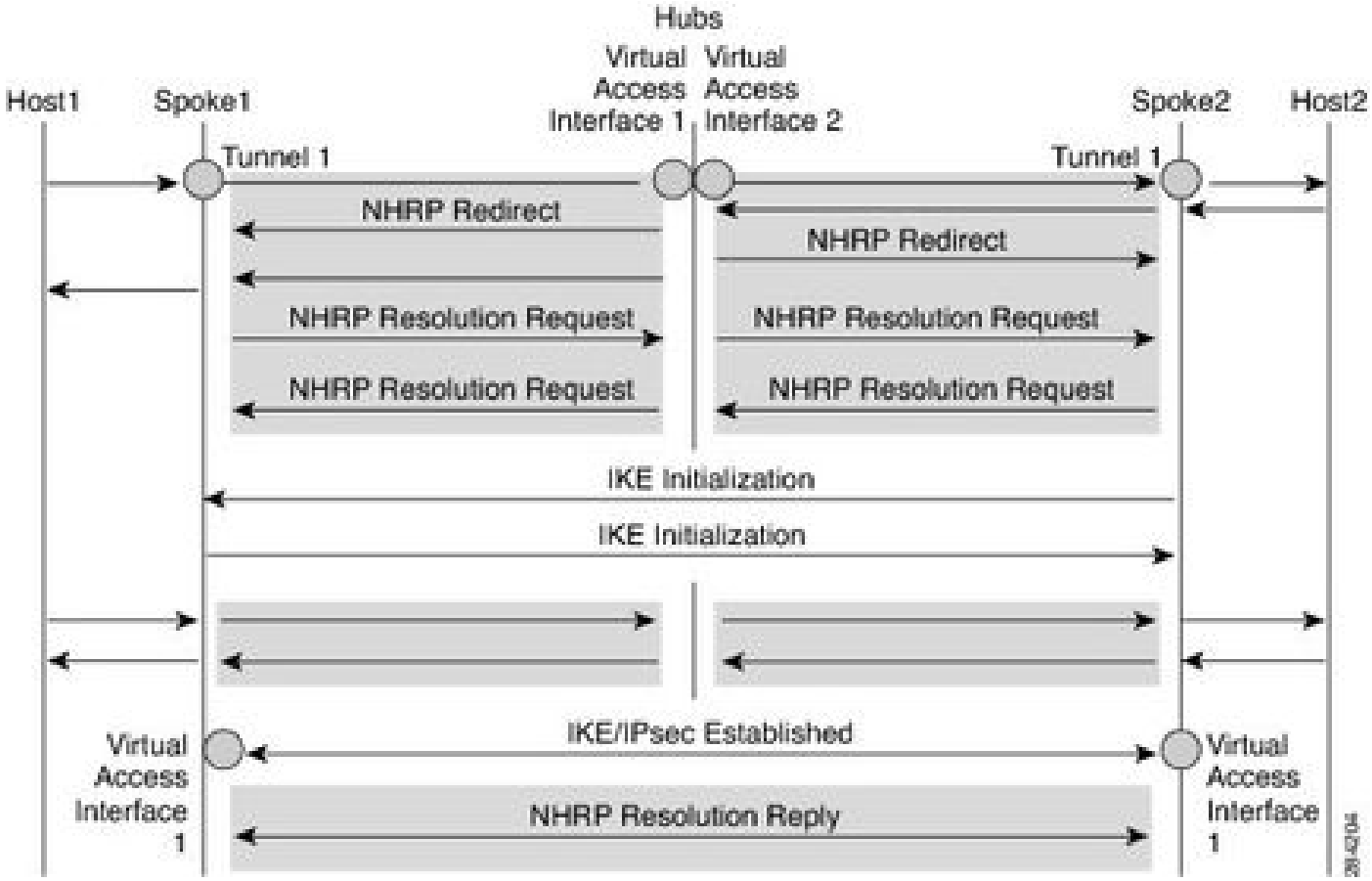
La funzione Spoke-to-Spoke di FlexVPN integra NHRP e il client FlexVPN (spoke) per stabilire un canale di crittografia diretto con un altro client in una rete FlexVPN esistente. Le connessioni vengono create utilizzando interfacce tunnel virtuali (VTI), IKEv2 e NHRP, dove NHRP viene utilizzato per risolvere i client FlexVPN nella rete.

Cisco consiglia di garantire:

- Le voci di routing non vengono scambiate tra i raggi. Una considerazione chiave, illustrata più avanti, è il progresso nella risoluzione dei problemi relativi alla topologia basata su EIGRP.

- Per gli spoke vengono utilizzati profili diversi e il comando config-exchange non è configurato per gli spoke.

Processo NHRP



L'illustrazione mostra il flusso del traffico tra lo Spoke 1 e lo Spoke 2, con le reti 198.51.100.0/29/24 e 198.51.100.8/29, entrambe pubblicizzate tramite l'EIGRP che effettuano il peering diretto agli Spoke attraverso l'hub. Di seguito viene riportato l'aspetto del flusso del traffico quando viene stabilita la comunicazione tra la spoke 1 (198.51.100.0/29/24) e la spoke 2 (198.51.100.8/29).

1. L'host 1 invia il traffico destinato all'host 2. La ricerca della route sull'host 1 comporta l'inoltro all'interfaccia del tunnel hub perché l'hub annuncia la rete tramite EIGRP.
2. Quando il traffico raggiunge l'hub, la ricerca dell'estremità hub del percorso conferma che la rete spoke 2 198.51.100.8/29 viene appresa tramite l'accesso virtuale spoke 2.
3. L'hub avvia il reindirizzamento NHRP poiché entrambe le interfacce di accesso virtuale (spoke 1 e spoke 2) fanno parte della stessa rete NHRP con lo stesso ID di rete NHRP.
4. Alla ricezione del reindirizzamento, Spoke1 avvia una richiesta di risoluzione per la rete spoke 2 tramite l'interfaccia tunnel (la stessa interfaccia su cui ha ricevuto il reindirizzamento). Spoke 2 ripete la stessa procedura per la richiesta di risoluzione della rete spoke 1.
5. Spoke2 riceve la richiesta di risoluzione sull'interfaccia del tunnel e recupera il numero di modello virtuale definito nella configurazione. Il numero di modello virtuale viene utilizzato per creare l'interfaccia di accesso virtuale per stabilire una sessione crittografica tra due spoke. Una volta attivate le SA crittografiche tra i due spoke, entrambi gli spoke installano percorsi di indirizzi IP dell'hop successivo appresi tramite IPSEC post-definizione di interfacce di accesso virtuale.
6. Entrambi gli spoke quindi procedono a verificare la raggiungibilità dell'hop successivo prima di inviare la risposta di risoluzione attraverso l'interfaccia di accesso virtuale appena creata

per la connettività spoke-to-spoke.
7. Quando l'hop successivo è raggiungibile, entrambi gli spoke si inviano una risposta di risoluzione a vicenda.
8. Entrambi gli spoke possono ora sostituire l'indirizzo IP dell'hop successivo della rete di destinazione dell'altro per l'accesso virtuale tramite NHO.
9. Spoke1 installa le voci della cache necessarie per l'IP dell'hop successivo di Spoke2 e la relativa rete. Spoke1 elimina anche la voce temporanea della cache che punta all'hub per risolvere la rete in tunnel interface1.
10. Lo stesso passaggio viene ripetuto da spoke 2, vengono installate le voci della cache per l'IP dell'hop successivo spoke 1 e la sua rete procede nell'eliminazione della voce dell'hub precedente tramite il tunnel.
11. NHRP aggiunge route di collegamento come route NHO (Next-Hop Override) o NHRP (Next-Hop Override).

Configurazione di FlexVPN Spoke to Spoke con EIGRP

Considerazioni fondamentali per la topologia basata su EIGRP

Prima di procedere con la configurazione, è necessario comprendere alcuni concetti chiave,

- Per qualsiasi distribuzione EIGRP, se gli spoke ricevono una tabella di routing completa di altri spoke o solo route di riepilogo, è necessario installare un elenco di prefissi sul lato hub per gli aggiornamenti del routing in uscita al fine di filtrare gli indirizzi IP tunnel degli spoke da annunciare l'uno all'altro.

- L'orizzonte di divisione in EIGRP funziona in modo diverso rispetto a IBGP. L'EIGRP impedisce solo alle reti pubblicitarie di uscire da un'interfaccia da cui sono state apprese. Ad esempio, l'hub dispone di due spoke, uno connesso tramite l'accesso virtuale 1 e l'altro tramite le interfacce di accesso virtuale 2. Le route apprese dall'hub tramite VA 1 dal spoke 1 vengono pubblicizzate nuovamente in spoke 2 tramite VA 2 e viceversa poiché VA 1 e VA 2 sono interfacce diverse. Nel caso di IBGP, non pubblicizza le reti apprese dal peer di ritorno a un altro peer. In un esempio simile, un hub configurato con IBGP non annuncia le reti posteriori apprese da VA 1 a VA 2 e viceversa.

- Questo comportamento in EIGRP crea un conflitto nell'adiacenza CEF per l'indirizzo IP dell'hop successivo (un indirizzo IP dell'interfaccia di accesso virtuale per un tunnel spoke-to-spoke) poiché viene appreso prima tramite EIGRP utilizzando un'interfaccia del tunnel hub e poi tramite IPsec utilizzando un'interfaccia di accesso virtuale. Ciò causa un routing asimmetrico per il traffico NHRP e produce anche una voce NHRP duplicata nella tabella NHRP e voci NHO duplicate nella tabella di routing, nonché per entrambe le interfacce hop successivo (tunnel tramite hub) e (accesso virtuale tramite spoke).

- Questo comportamento è stato rilevato negli ID bug Cisco CSCwn54813 e Cisco CSCwn54758. Cisco consiglia di attenersi alla soluzione alternativa fornita per il filtro degli indirizzi del tunnel sull'hub per gli aggiornamenti in uscita.

- Il modello virtuale del lato hub deve avere un indirizzo IP da un pool diverso rispetto alle

interfacce del tunnel Spokes, in quanto si desidera filtrare gli aggiornamenti EIGRP in uscita per assicurarsi che il peer EIGRP Hub and Spokes non sia influenzato.

Di seguito sono riportati due esempi che mostrano come configurare FlexVPN spoke con EIGRP sul server FlexVPN e sul client FlexVPN. Abbiamo seguito le best practice per segregare il traffico di sovrimpressione e sovrapposizione inserendole in VRF specifici. VRF A è per l'underlay, mentre B è utilizzato per l'overlay.

Esempio 1 - Utilizzo Di NHO (Next-Hop-Override) Per La Comunicazione Spoke-To-Spoke

Server FlexVPN

```
ip local pool FLEXPOOL 192.0.2.129 192.0.2.254

crypto ikev2 authorization policy CISCO_FLEX
 pool FLEXPOOL
 def-domain cisco.com
 route set interface

crypto ikev2 proposal CISCO_PROP
 encryption aes-gcm-256
 prf sha256
 group 21

crypto ikev2 policy CISCO_POL
 match fvrf A
 proposal CISCO_PROP

crypto ikev2 profile CISCO_IKEV2
 match fvrf A
 match identity remote fqdn domain cisco.com
 identity local fqdn hub.cisco.com
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list default CISCO_FLEX
 virtual-template 1

crypto ipsec transform-set CISCO_TRANSFORM esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile CISCO_PROF
 set transform-set CISCO_TRANSFORM
 set pfs group19
 set ikev2-profile CISCO_IKEV2

interface Loopback0
 ip vrf forwarding B
 ip address 192.0.2.1 255.255.255.255

interface GigabitEthernet1
 ip vrf forwarding A
 ip address 203.0.113.2 255.255.255.252

interface Virtual-Template1 type tunnel
 ip vrf forwarding B
```

```
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF

ip prefix-list CISCO_PREFIX seq 5 deny 192.0.2.128/25 le 32
ip prefix-list CISCO_PREFIX seq 6 permit 0.0.0.0/0 le 32

router eigrp B
!
address-family ipv4 unicast vrf B autonomous-system 1
!
af-interface default
hello-interval 2
hold-time 10
exit-af-interface
!
topology base
distribute-list prefix CISCO_PREFIX out
exit-af-topology
network 192.0.2.128 0.0.0.127
network 192.0.2.1 0.0.0.0
exit-address-family
```

FlexVPN Client 1

```
ip host vrf A hub.cisco.com 203.0.113.2

crypto ikev2 authorization policy CISCO_FLEX
 route set interface

crypto ikev2 proposal CISCO_PROP
 encryption aes-gcm-256
 prf sha256
 group 21

crypto ikev2 policy CISCO_POL
 match fvrf A
 proposal CISCO_PROP

crypto ikev2 client flexvpn CISCO_CLIENT
 peer 1 fqdn hub.cisco.com dynamic
 client connect Tunnel1

crypto ikev2 profile CISCO_IKEV2
 match fvrf A
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke1.cisco.com
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list default CISCO_FLEX
 virtual-template 1

crypto ipsec transform-set CISCO_TRANSFORM esp-aes 256 esp-sha256-hmac
 mode transport
```

```
crypto ipsec profile CISCO_PROF
 set transform-set CISCO_TRANSFORM
 set pfs group19
 set ikev2-profile CISCO_IKEV2

interface Tunnel1
 ip vrf forwarding B
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination dynamic
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF
end

interface GigabitEthernet1
 ip vrf forwarding A
 ip address 203.0.113.6 255.255.255.252

interface Loopback1
 ip vrf forwarding B
 ip address 198.51.100.1 255.255.255.248

interface Virtual-Template1 type tunnel
 ip vrf forwarding B
 ip unnumbered Tunnel1
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF

router eigrp B
 address-family ipv4 unicast vrf B autonomous-system 1

 af-interface default
  hello-interval 2
  hold-time 10
  passive-interface
 exit-af-interface

 af-interface Tunnel1
  no passive-interface
 exit-af-interface

  topology base
  exit-af-topology
  network 198.51.100.0 0.0.0.7
  network 192.0.2.128 0.0.0.127
 exit-address-family
```

FlexVPN Client 2

```
ip host vrf A hub.cisco.com 203.0.113.2

crypto ikev2 authorization policy CISCO_FLEX
 route set interface
```

```
crypto ikev2 proposal CISCO_PROP
 encryption aes-gcm-256
 prf sha256
 group 21

crypto ikev2 policy CISCO_POL
 match fvrf A
 proposal CISCO_PROP

crypto ikev2 client flexvpn CISCO_CLIENT
 peer 1 fqdn hub.cisco.com dynamic
 client connect Tunnel1

crypto ikev2 profile CISCO_IKEV2
 match fvrf A
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke2.cisco.com
 authentication remote pre-share key cisco
 authentication local pre-share key cisco
 aaa authorization group psk list default CISCO_FLEX
 virtual-template 1

crypto ipsec transform-set CISCO_TRANSFORM esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile CISCO_PROF
 set transform-set CISCO_TRANSFORM
 set pfs group19
 set ikev2-profile CISCO_IKEV2

interface Tunnel1
 ip vrf forwarding B
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination dynamic
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF
end

interface GigabitEthernet1
 ip vrf forwarding A
 ip address 203.0.113.10 255.255.255.252

interface Loopback1
 ip vrf forwarding B
 ip address 198.51.100.9 255.255.255.248

interface Virtual-Template1 type tunnel
 ip vrf forwarding B
 ip unnumbered Tunnel1
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel vrf A
 tunnel protection ipsec profile CISCO_PROF

router eigrp B
 address-family ipv4 unicast vrf B autonomous-system 1

 af-interface default
```

```
 hello-interval 2
 hold-time 10
 passive-interface
exit-af-interface

af-interface Tunnel1
 no passive-interface
exit-af-interface

 topology base
 exit-af-topology
 network 198.51.100.8 0.0.0.7
 network 192.0.2.128 0.0.0.127
exit-address-family
```

Esempio 2 - Utilizzo Di Route Installate NHRP Per La Comunicazione Spoke-To-Spoke

Server FlexVPN

L'unica modifica nella configurazione EIGRP consiste nell'introduzione di route di riepilogo anziché di una tabella di routing completa per gli spoke. Assicurarsi di ridurre il modello virtuale per inserire la configurazione di riepilogo nella topologia EIGRP. Fare riferimento all'ID bug Cisco CSCwn84303.

```
router eigrp B
!
address-family ipv4 unicast vrf B autonomous-system 1
!
af-interface default
hello-interval 2
hold-time 10
exit-af-interface
!
af-interface Virtual-Template1
summary-address 198.51.100.0 255.255.255.0 <<<<<<<<<<< Summary address
exit-af-interface
!
topology base
distribute-list prefix CISCO_PREFIX out
exit-af-topology
network 192.0.2.128 0.0.0.127
network 192.0.2.1 0.0.0.0
exit-address-family
```

Verifica e risoluzione dei problemi

Esempio 1 - Utilizzo Di NHO (Next-Hop-Override) Per La Comunicazione Spoke-To-Spoke

Spoke 1 (prima della risoluzione NHRP Spoke to Spoke e della definizione del tunnel)

```
Spoke1#show ip route vrf B

Routing Table: B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.0.2.0/32 is subnetted, 2 subnets
S        192.0.2.1 is directly connected, Tunnel1
C        192.0.2.130 is directly connected, Tunnel1
      198.51.100.0/24 is variably subnetted, 3 subnets, 2 masks
C        198.51.100.0/29 is directly connected, Loopback1
L        198.51.100.1/32 is directly connected, Loopback1
D        198.51.100.8/29 [90/102451840] via 192.0.2.1, 00:01:46
```

Spoke 2 (prima della risoluzione NHRP Spoke to Spoke e della definizione del tunnel)

```
Spoke2#show ip route vrf B

Routing Table: B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.0.2.0/32 is subnetted, 2 subnets
S        192.0.2.1 is directly connected, Tunnel1
C        192.0.2.129 is directly connected, Tunnel1
      198.51.100.0/24 is variably subnetted, 3 subnets, 2 masks
D        198.51.100.0/29 [90/102451840] via 192.0.2.1, 00:04:01
C        198.51.100.8/29 is directly connected, Loopback1
L        198.51.100.9/32 is directly connected, Loopback1
Spoke2#
```

Spoke 1 (dopo la risoluzione NHRP Spoke to Spoke e la definizione del tunnel)

Avvio di ICMP per l'attivazione del tunnel spoke-to-spoke.

```
Spoke1#ping vrf B 198.51.100.9 source 198.51.100.1 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 198.51.100.1
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 111/111/111 ms
```

Verifica del collegamento NHRP.

```
Spoke1#show ip nhrp vrf B detail
192.0.2.129/32 via 192.0.2.129
   Virtual-Access1 created 00:00:18, expire 00:09:41
   Type: dynamic, Flags: router nhop rib nho
   NBMA address: 203.0.113.10
   Preference: 255
198.51.100.8/29 via 192.0.2.129
   Virtual-Access1 created 00:00:17, expire 00:09:41
   Type: dynamic, Flags: router rib nho
   NBMA address: 203.0.113.10
   Preference: 255
```

Verifica creazione collegamento post route NHO.

```
Spoke1#show ip route vrf B next-hop-override

Routing Table: B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.0.2.0/32 is subnetted, 3 subnets
S        192.0.2.1 is directly connected, Tunnel1
S   %    192.0.2.129 is directly connected, Virtual-Access1
                     [NHO][1/255] via 192.0.2.129, Virtual-Access1
C        192.0.2.130 is directly connected, Tunnel1
      198.51.100.0/24 is variably subnetted, 3 subnets, 2 masks
C        198.51.100.0/29 is directly connected, Loopback1
L        198.51.100.1/32 is directly connected, Loopback1
D   %    198.51.100.8/29 [90/102451840] via 192.0.2.1, 00:07:13
                         [NHO][90/255] via 192.0.2.129, 00:00:45, Virtual-Access1
```

Verifica dei contatori NHRP.

```
Spoke1#show ip nhrp traffic
Tunnel1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 2
         2 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
   Rcvd: Total 3
         2 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  1 Traffic Indication  0 Redirect Suppress
Virtual-Access1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 3
         0 Resolution Request  1 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         2 Error Indication  0 Traffic Indication  0 Redirect Suppress
   Rcvd: Total 1
         0 Resolution Request  1 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
Virtual-Template1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
   Rcvd: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
```

Spoke 2 (dopo la risoluzione NHRP Spoke to Spoke e la definizione del tunnel)

Verifica del collegamento NHRP.

```
Spoke2#show ip nhrp vrf B detail
192.0.2.130/32 via 192.0.2.130
   Virtual-Access1 created 00:04:42, expire 00:05:18
   Type: dynamic, Flags: router nhop rib nho
   NBMA address: 203.0.113.6
   Preference: 255
198.51.100.0/29 via 192.0.2.130
   Virtual-Access1 created 00:04:40, expire 00:05:18
   Type: dynamic, Flags: router rib nho
   NBMA address: 203.0.113.6
   Preference: 255
```

Verifica creazione collegamento post route NHO.

```
Spoke2# show ip route vrf B next-hop-override

Routing Table: B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.0.2.0/32 is subnetted, 3 subnets
S        192.0.2.1 is directly connected, Tunnel1
C        192.0.2.129 is directly connected, Tunnel1
S   %    192.0.2.130 is directly connected, Virtual-Access1
                     [NHO][1/255] via 192.0.2.130, Virtual-Access1
      198.51.100.0/24 is variably subnetted, 3 subnets, 2 masks
D   %    198.51.100.0/29 [90/102451840] via 192.0.2.1, 00:11:20
                         [NHO][90/255] via 192.0.2.130, 00:04:52, Virtual-Access1
C        198.51.100.8/29 is directly connected, Loopback1
L        198.51.100.9/32 is directly connected, Loopback1
```

Verifica dei contatori NHRP.

```
Spoke2#show ip nhrp traffic
Tunnel1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 2
         2 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
   Rcvd: Total 3
         2 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  1 Traffic Indication  0 Redirect Suppress
Virtual-Access1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 3
         0 Resolution Request  1 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         2 Error Indication  0 Traffic Indication  0 Redirect Suppress
   Rcvd: Total 1
         0 Resolution Request  1 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
Virtual-Template1: Max-send limit:10000Pkts/10Sec, Usage:0%
   Sent: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
   Rcvd: Total 0
         0 Resolution Request  0 Resolution Reply  0 Registration Request
         0 Registration Reply  0 Purge Request  0 Purge Reply
         0 Error Indication  0 Traffic Indication  0 Redirect Suppress
```

Di seguito viene riportata una spiegazione dettagliata di come impostare un tunnel spoke diretto con l'aiuto di debug da uno dei spoke.

- Il raggio 1 ha avviato ICMP.

```
Spoke1#ping vrf B 198.51.100.9 source 198.51.100.1 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 198.51.100.1
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 111/111/111 ms
```

- L'hub ha ricevuto un messaggio ICMP e ha avviato il reindirizzamento (indicazione del traffico) a entrambi i spoke.

```
*Feb 3 16:15:35.280: NHRP: Receive Traffic Indication via Tunnel1 vrf: B(0x4), packet size: 104
*Feb 3 16:15:35.280: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 3 16:15:35.280: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 3 16:15:35.280: pktsz: 104 extoff: 88
*Feb 3 16:15:35.280: (M) traffic code: redirect(0)
```

```
*Feb 3 16:15:35.280: src NBMA: 203.0.113.2
*Feb 3 16:15:35.280: src protocol: 192.0.2.1, dst protocol: 198.51.100.1
*Feb 3 16:15:35.280: Contents of nhrp traffic indication packet:
*Feb 3 16:15:35.281: 45 00 00 64 00 19 00 00 FE 01 68 0E C6 33 64 01
*Feb 3 16:15:35.281: C6 33 64 09 08 00 F3 F6 00 0D 00 00 00 00 00 00
*Feb 3 16:15:35.281: 3A 53 4F F3 AB CD AB CD AB CD AB CD AB CD AB CD
*Feb 3 16:15:35.281: NHRP-DETAIL: netid_in = 1, to_us = 0
*Feb 3 16:15:35.281: NHRP-DETAIL: NHRP traffic indication for afn 1 received on interface Tunnel1 , for
```

- Entrambi gli spoke hanno attivato una richiesta di risoluzione passata attraverso il tunnel1.

```
*Feb 3 16:15:35.295: NHRP: Sending NHRP Resolution Request for dest: 198.51.100.9 to nexthop: 198.51.10
*Feb 3 16:15:35.295: NHRP: Attempting to send packet through interface Tunnel1 via DEST dst 198.51.100.
*Feb 3 16:15:35.295: NHRP-DETAIL: First hop route lookup for 198.51.100.9 yielded 192.0.2.1, Tunnel1
*Feb 3 16:15:35.295: NHRP: Send Resolution Request via Tunnel1 vrf: B(0x4), packet size: 72
*Feb 3 16:15:35.295: src: 192.0.2.130, dst: 198.51.100.9
*Feb 3 16:15:35.295: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 3 16:15:35.295: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 3 16:15:35.295: pktsz: 72 extoff: 52
*Feb 3 16:15:35.296: (M) flags: "router auth src-stable nat ", reqid: 10
*Feb 3 16:15:35.296: src NBMA: 203.0.113.6
*Feb 3 16:15:35.296: src protocol: 192.0.2.130, dst protocol: 198.51.100.9
*Feb 3 16:15:35.296: (C-1) code: no error(0), flags: none
*Feb 3 16:15:35.296: prefix: 0, mtu: 9934, hd_time: 600
*Feb 3 16:15:35.296: addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 255
*Feb 3 16:15:35.296: NHRP: 96 bytes out Tunnel1
```

- Entrambi gli spoke hanno ricevuto una richiesta di risoluzione tramite Tunnel1.

```
*Feb 3 16:15:35.392: NHRP: Receive Resolution Request via Tunnel1 vrf: B(0x4), packet size: 92
*Feb 3 16:15:35.392: (F) afn: AF_IP(1), type: IP(800), hop: 254, ver: 1
*Feb 3 16:15:35.392: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 3 16:15:35.392: pktsz: 92 extoff: 52
*Feb 3 16:15:35.392: (M) flags: "router auth src-stable nat ", reqid: 10
*Feb 3 16:15:35.392: src NBMA: 203.0.113.10
*Feb 3 16:15:35.392: src protocol: 192.0.2.129, dst protocol: 198.51.100.1
*Feb 3 16:15:35.392: (C-1) code: no error(0), flags: none
*Feb 3 16:15:35.392: prefix: 0, mtu: 9934, hd_time: 600
*Feb 3 16:15:35.392: addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 255
*Feb 3 16:15:35.392: NHRP-DETAIL: netid_in = 1, to_us = 0
*Feb 3 16:15:35.392: NHRP-DETAIL: Resolution request for afn 1 received on interface Tunnel1 , for vrf:
```

- Entrambi gli spoke hanno eseguito una ricerca del percorso per le loro reti locali 198.51.100.0/29/24 e 198.51.100.8/29.

```
*Feb 3 16:15:35.392: NHRP-DETAIL: Multipath IP route lookup for 198.51.100.1 in vrf: B(0x4) yielded Loo
*Feb 3 16:15:35.392: NHRP: Route lookup for destination 198.51.100.1 in vrf: B(0x4) yielded interface L
*Feb 3 16:15:35.392: NHRP-DETAIL: netid_out 0, netid_in 1
```

```
*Feb 3 16:15:35.392: NHRP-ATTR: smart spoke and attributes are not configured
*Feb 3 16:15:35.392: NHRP: We are egress router. Process the NHRP Resolution Request.
*Feb 3 16:15:35.393: NHRP: Cache radix tree head is not initialized for vrf: B(0x4)
*Feb 3 16:15:35.393: NHRP-DETAIL: Multipath IP route lookup for 198.51.100.1 in vrf: B(0x4) yielded Loo
*Feb 3 16:15:35.393: NHRP: nhrp_rtlookup for 198.51.100.1 in vrf: B(0x4) yielded interface Loopback1, p
*Feb 3 16:15:35.393: NHRP-DETAIL: netid_out 0, netid_in 1
*Feb 3 16:15:35.393: NHRP: We are egress router for target 198.51.100.1, recevied via Tunnel1 vrf: B(0x
```

- La risposta di risoluzione è stata accodata e l'impostazione di IPSec è stata avviata poiché entrambi gli spoke sono ora a conoscenza l'uno dell'altro indirizzi NBMA.

```
*Feb 3 16:15:35.393: NHRP: Checking for delayed event 192.0.2.129/198.51.100.1 on list (Tunnel1 vrf: B(
*Feb 3 16:15:35.393: NHRP: No delayed event node found.
*Feb 3 16:15:35.394: NHRP-DETAIL: Updated delayed event with ep src:203.0.113.6 dst:203.0.113.10 ivrf:B
*Feb 3 16:15:35.394: NHRP: Enqueued Delaying resolution request nbma src:203.0.113.6 nbma dst:203.0.113
*Feb 3 16:15:35.394: NHRP: Interface: Tunnel1 configured with FlexVPN. Deferringcache creation for nhop
*Feb 3 16:15:35.406: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to
*Feb 3 16:15:35.456: NHRP: Virtual-Access1: Tunnel mode changed from
'Uninitialized tunnel mode' to 'GRE over point to point IPV4 tunnel mode'
*Feb 3 16:15:35.456: NHRP: Virtual-Access1: NHRP not enabled in delay_if_up
*Feb 3 16:15:35.511: NHRP: Registration with Tunnels Decap Module succeeded
*Feb 3 16:15:35.511: NHRP: Rejecting addr type 1
*Feb 3 16:15:35.511: NHRP: Adding all static maps to cache
*Feb 3 16:15:35.511: NHRP-DETAIL: Adding summary-prefix entry: nhrp router block not configured
*Feb 3 16:15:35.512: NHRP:
*Feb 3 16:15:35.512: Instructing NHRP to create Virtual-Access from Virtual template 1 for interface Vi
*Feb 3 16:15:35.537: %SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as
*Feb 3 16:15:35.539: NHRP-CACHE: Virtual-Access1: Cache add for target 192.0.2.130/32 vrf: B(0x4) label
*Feb 3 16:15:35.540: 203.0.113.6 (flags:0x20)
*Feb 3 16:15:35.540: NHRP-DETAIL: self_cache: Unable to get tableid for swidb:Virtual-Access1 proto:NHR
*Feb 3 16:15:35.540: NHRP-DETAIL: self_cache: Unable to get tableid for swidb:Virtual-Access1 proto:UNK
*Feb 3 16:15:35.548: NHRP: Updating delayed event with destination 203.0.113.10 on interfaceTunnel1 wit
*Feb 3 16:15:35.788: NHRP:
*Feb 3 16:15:35.788: Fetched address from underlying IKEv2 for interfaceVirtual-Access1. Pre-NATed = 20
*Feb 3 16:15:35.788: %DMVPN-5-CRYPTO_SS: Virtual-Access1: local address : 203.0.113.6 remote address :
```

- Durante la definizione di IPSEC e il processo di creazione dei collegamenti NHRP, entrambi gli spoke hanno individuato e installato gli altri indirizzi IP del tunnel nella relativa tabella di routing come route IPSEC e hanno sondato la raggiungibilità dell'hop successivo.

```
*Feb 3 16:15:35.788: NHRP: Processing delayed event on interface Tunnel1 with NBMA 203.0.113.10
*Feb 3 16:15:35.789: NHRP: Could not find instance node for vrf: B(0x4)
*Feb 3 16:15:35.789: NHRP-DETAIL: Cache INIT: NHRP instance root is NULL
*Feb 3 16:15:35.789: NHRP: Inserted instance node for vrf: B(0x4)
*Feb 3 16:15:35.789: NHRP-DETAIL: Initialized remote cache radix head for vrf: B(0x4)
*Feb 3 16:15:35.789: NHRP-DETAIL: Initialized local cache radix head for vrf: B(0x4)
*Feb 3 16:15:35.789: NHRP-RT: Attempting to create instance PDB for vrf: B(0x4)(0x4)
*Feb 3 16:15:35.789: NHRP-CACHE: Virtual-Access1: Cache add for target 192.0.2.129/32 vrf: B(0x4) label
*Feb 3 16:15:35.789: 203.0.113.10 (flags:0x2080)
*Feb 3 16:15:35.789: NHRP-RT: Adding route entry for 192.0.2.129/32 via 192.0.2.129, Virtual-Access1 vr
*Feb 3 16:15:35.791: NHRP-RT: Route addition to RIB Successful
*Feb 3 16:15:35.791: NHRP-EVE: NHP-UP: 192.0.2.129, NBMA: 203.0.113.10
```

```
*Feb 3 16:15:35.791: %DMVPN-5-NHRP_NHP_UP: Virtual-Access1: Next Hop NHP : (Tunnel: 192.0.2.129 NBMA: 2
*Feb 3 16:15:35.791: NHRP-CACHE:
*Feb 3 16:15:35.791: Next-hop not reachable for 192.0.2.129
*Feb 3 16:15:35.791: %NHRP-5-NHOP_UNREACHABLE: Nexthop address 192.0.2.129 for 192.0.2.129/32 is not ro
```

- Fino al completamento dell'installazione dei collegamenti e NHO, Spoke A ha eseguito la ricerca hop successiva degli indirizzi IP di accesso virtuale di Spoke B e viceversa, ma la ricerca hope successiva ha restituito "N/A restituito" a causa del quale Spoke A ha inviato un'indicazione di errore a Spoke B confermando che l'hop successivo non è raggiungibile. È possibile fare riferimento alla ricerca specifica come ricerca a percorsi multipli.

```
*Feb 3 16:15:35.791: NHRP-DETAIL: Multipath recursive nexthop lookup(if_in:, netid:1) for 192.0.2.129 i
*Feb 3 16:15:35.791: NHRP: Sending error indication. Reason: 'Cache pak failure' LINE: 13798
*Feb 3 16:15:35.791: NHRP: Attempting to send packet through interface Virtual-Access1 via DEST dst 192
*Feb 3 16:15:35.791: NHRP-DETAIL: Multipath recursive nexthop lookup(if_in:, netid:1) for 192.0.2.129 i
*Feb 3 16:15:35.791: NHRP: Send Error Indication via Virtual-Access1 vrf: B(0x4), packet size: 132
*Feb 3 16:15:35.791: src: 192.0.2.130, dst: 192.0.2.129
*Feb 3 16:15:35.791: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 3 16:15:35.791: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 3 16:15:35.791: pktsz: 132 extoff: 0
*Feb 3 16:15:35.791: (M) error code: protocol address unreachable(6), offset: 0
*Feb 3 16:15:35.791: src NBMA: 203.0.113.6
*Feb 3 16:15:35.791: src protocol: 192.0.2.130, dst protocol: 192.0.2.129
*Feb 3 16:15:35.792: Contents of error packet:
*Feb 3 16:15:35.792: 00 01 08 00 00 00 00 00 00 FE 00 5C A2 22 00 34
*Feb 3 16:15:35.792: 01 01 04 00 04 04 C8 02 00 00 00 0A CB 00 71 0A
*Feb 3 16:15:35.792: C0 00 02 81 C6 33 64 01
*Feb 3 16:15:35.792:
```

- Una volta che la NHO è entrata per l'hop successivo ed è stata creata la scorciatoia, entrambi gli spoke hanno inviato nuovamente richieste di risoluzione per la rete dell'altro.

```
*Feb 3 16:15:35.813: NHRP: No need to delay processing of resolution event nbma src:203.0.113.6 nbma ds
*Feb 3 16:15:35.813: NHRP-CACHE: Virtual-Access1: Cache update for target 192.0.2.129/32 vrf: B(0x4) la
*Feb 3 16:15:35.813: 203.0.113.10 (flags:0x2280)
*Feb 3 16:15:35.813: NHRP-RT: Adding route entry for 192.0.2.129/32 via 192.0.2.129, Virtual-Access1 vr
*Feb 3 16:15:35.814: NHRP-RT: Route addition to RIB Successful
.
*Feb 3 16:15:35.841: NHRP-RT: Route entry 192.0.2.129/32 via 192.0.2.129 (Vi1) clobbered by distance
*Feb 3 16:15:35.847: NHRP-RT: Unable to stop route watch for 192.0.2.129/32 interface Virtual-Access1 .
*Feb 3 16:15:35.847: NHRP-RT: Adding route entry for 192.0.2.129/32 via 192.0.2.129, Virtual-Access1 vr
*Feb 3 16:15:35.847: NHRP-RT: Route addition failed (admin-distance)
*Feb 3 16:15:35.847: NHRP-RT: nexthop-override added to RIB
.
*Feb 3 16:15:37.167: NHRP: Sending NHRP Resolution Request for dest: 198.51.100.9 to nexthop: 198.51.10
*Feb 3 16:15:37.167: NHRP: Attempting to send packet through interface Tunnel1 via DEST dst 198.51.100.
*Feb 3 16:15:37.167: NHRP-DETAIL: First hop route lookup for 198.51.100.9 yielded 192.0.2.1, Tunnel1
*Feb 3 16:15:37.167: NHRP: Send Resolution Request via Tunnel1 vrf: B(0x4), packet size: 72
*Feb 3 16:15:37.167: src: 192.0.2.130, dst: 198.51.100.9
*Feb 3 16:15:37.167: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 3 16:15:37.167: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 3 16:15:37.167: pktsz: 72 extoff: 52
```

```
*Feb 3 16:15:37.167: (M) flags: "router auth src-stable nat ", reqid: 10
*Feb 3 16:15:37.167: src NBMA: 203.0.113.6
*Feb 3 16:15:37.167: src protocol: 192.0.2.130, dst protocol: 198.51.100.9
*Feb 3 16:15:37.167: (C-1) code: no error(0), flags: none
*Feb 3 16:15:37.167: prefix: 0, mtu: 9934, hd_time: 600
*Feb 3 16:15:37.167: addr_len: 0(NSAP), subaddr_len: 0(NSAP), proto_len: 0, pref: 255
*Feb 3 16:15:37.167: NHRP: 96 bytes out Tunnel1
```

- Una volta che entrambi gli spoke hanno ricevuto richieste di risoluzione per le rispettive reti, NHO ha sostituito la route EIGRP tramite tunnel (HUB) con accesso virtuale.

```
*Feb 3 16:30:57.768: NHRP-CACHE: Virtual-Access1: Cache add for target 198.51.100.8/29 vrf: B(0x4) labe
*Feb 3 16:30:57.768: 203.0.113.10 (flags:0x1000)
*Feb 3 16:30:57.768: NHRP-RT: Adding route entry for 198.51.100.8/29 via 192.0.2.129, Virtual-Access1 v
*Feb 3 16:30:57.769: NHRP-RT: Route addition failed (admin-distance)
*Feb 3 16:30:57.769: NHRP-RT: nexthop-override added to RIB
*Feb 3 16:30:57.769: NHRP-EVE: NHP-UP: 192.0.2.129, NBMA: 203.0.113.10
*Feb 3 16:30:57.769: %DMVPN-5-NHRP_NHP_UP: Virtual-Access1: Next Hop NHP : (Tunnel: 192.0.2.129 NBMA: 2
*Feb 3 16:30:57.769: NHRP-CACHE: Deleting incomplete entry for 198.51.100.9/32 interface Tunnel1 vrf: B
*Feb 3 16:30:57.769: NHRP-EVE: NHP-DOWN: 198.51.100.9, NBMA: 198.51.100.9
```

- In seguito, entrambi gli spoke inviano una risposta di risoluzione attraverso l'interfaccia di accesso virtuale.

```
*Feb 3 16:30:57.436: NHRP-CACHE: Virtual-Access1: Internal Cache add for target 198.51.100.0/29 vrf: B(
*Feb 3 16:30:57.436: 203.0.113.6 (flags:0x20)
*Feb 3 16:30:57.436: NHRP: Attempting to send packet through interface Virtual-Access1 via DEST dst 192
*Feb 3 16:30:57.436: NHRP-DETAIL: Multipath recursive nexthop lookup(if_in:, netid:1) for 192.0.2.129 i
*Feb 3 16:30:57.436: NHRP: Send Resolution Reply via Virtual-Access1 vrf: B(0x4), packet size: 120
*Feb 3 16:30:57.436: src: 192.0.2.130, dst: 192.0.2.129
*Feb 3 16:30:57.436: (F) afn: AF_IP(1), type: IP(800), hop: 255, ver: 1
*Feb 3 16:30:57.436: shtl: 4(NSAP), sstl: 0(NSAP)
*Feb 3 16:30:57.436: pktsz: 120 extoff: 60
*Feb 3 16:30:57.437: (M) flags: "router auth dst-stable unique src-stable nat ", reqid: 11
*Feb 3 16:30:57.437: src NBMA: 203.0.113.10
*Feb 3 16:30:57.437: src protocol: 192.0.2.129, dst protocol: 198.51.100.1
*Feb 3 16:30:57.437: (C-1) code: no error(0), flags: none
*Feb 3 16:30:57.437: prefix: 29, mtu: 9976, hd_time: 599
*Feb 3 16:30:57.437: addr_len: 4(NSAP), subaddr_len: 0(NSAP), proto_len: 4, pref: 255
*Feb 3 16:30:57.437: client NBMA: 203.0.113.6
*Feb 3 16:30:57.437: client protocol: 192.0.2.130
*Feb 3 16:30:57.437: NHRP: 144 bytes out Virtual-Access1
```

Esempio 2 - Utilizzo Di Route Installate NHRP Per La Comunicazione Spoke-To-Spoke

Server FlexVPN

È stata introdotta la verifica della topologia EIGRP per la route di riepilogo.

```
FLEX-HUB#show ip eigrp vrf B topology 198.51.100.0
EIGRP-IPv4 VR(B) Topology Entry for AS(1)/ID(192.0.0.1)
          Topology(base) TID(0) VRF(B)
EIGRP-IPv4(1): Topology base(0) entry for 198.51.100.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 9837035520, RIB is 76851840
  Descriptor Blocks:
  0.0.0.0 (Null0), from 0.0.0.0, Send flag is 0x0
      Composite metric is (9837035520/0), route is Internal
      Vector metric:
        Minimum bandwidth is 100 Kbit
        Total delay is 50101250000 picoseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1476
        Hop count is 0
        Originating router is 192.0.0.1
```

Client FlexVPN

Verifica della presenza della route di riepilogo.

```
Spoke1#show ip route vrf B eigrp

Routing Table: B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      198.51.100.0/24 is variably subnetted, 4 subnets, 3 masks
D        198.51.100.0/24 [90/102451840] via 192.0.2.1, 00:00:04
```

Provare a stabilire un tunnel spoke-to-spoke iniziando il traffico.

```
Spoke1#ping vrf B 198.51.100.9 source 198.51.100.1 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 198.51.100.1
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 13/13/13 ms
```

Nuova verifica.

```
Spoke1#show ip route vrf B next-hop-override

Routing Table: B
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.0.2.0/32 is subnetted, 3 subnets
S        192.0.2.1 is directly connected, Tunnel1
H        192.0.2.129 is directly connected, 00:02:18, Virtual-Access1
C        192.0.2.132 is directly connected, Tunnel1
      198.51.100.0/24 is variably subnetted, 4 subnets, 3 masks
D        198.51.100.0/24 [90/102451840] via 192.0.2.1, 00:02:13
C        198.51.100.0/29 is directly connected, Loopback1
L        198.51.100.1/32 is directly connected, Loopback1
H        198.51.100.8/29 [250/255] via 192.0.2.129, 00:02:18, Virtual-Access1
```

L'output dei debug per l'installazione della rete Spokes è stato modificato in modo molto lieve. L'installazione della rete Spokes ha avuto esito positivo, invece dell'errore RIB, e l'aggiunta di NHO è stata completata.

```
*Feb 3 16:43:38.957: NHRP-CACHE: Virtual-Access1: Cache add for target 198.51.100.8/29 vrf: B(0x4) labe
*Feb 3 16:43:38.957: 203.0.113.10 (flags:0x1000)
*Feb 3 16:43:38.957: NHRP-RT: Adding route entry for 198.51.100.8/29 via 192.0.2.131, Virtual-Access1 v
*Feb 3 16:43:38.957: NHRP-RT: Route addition to RIB Successful
*Feb 3 16:43:38.957: NHRP-EVE: NHP-UP: 192.0.2.131, NBMA: 203.0.113.10
```

Informazioni correlate

- Configurazione di FlexVPN Spoke to Spoke
- Esempio di configurazione del blocco client FlexVPN Spoke in un hub ridondante con FlexVPN

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).