Configurar e Solucionar Problemas do FlexVPN Spoke to Spoke via EIGRP

Contents

Introdução

Este documento descreve a implantação e a solução de problemas do Cisco FlexVPN spoke-to-spoke usando IKEv2 e NHRP para túneis de criptografia de cliente direto.

Pré-requisitos

- Configuração de hub do Flex VPN e cliente do Flex VPN

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- IKEv2
- VPN de rota
- Interfaces de túnel virtual (VTI)
- NHRP
- IPSec
- EIGRP
- VRF-Lite

Componentes Utilizados

As informações neste documento são baseadas em:

- Cisco IOS XE 17.9.4a

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Escalabilidade

A FlexVPN pode ser facilmente expandida de pequenos escritórios para redes de grandes empresas. Ele pode gerenciar muitas conexões VPN sem precisar de muito trabalho extra, o que é ótimo para organizações que estão crescendo ou têm muitos usuários remotos.

Recursos Principais:

- Configuração dinâmica e túneis sob demanda:
  - Interfaces de túnel virtual (VTI): O FlexVPN usa VTIs que podem ser criadas e removidas conforme necessário. Isso significa que os túneis VPN são configurados somente quando há tráfego e removidos quando não são necessários, economizando recursos e melhorando a escalabilidade.
  - Protocolos de roteamento dinâmico: Ele funciona com protocolos de roteamento como OSPF, EIGRP e BGP sobre túneis VPN. Isso mantém as informações de roteamento atualizadas automaticamente, o que é importante para redes grandes e dinâmicas.
- Flexibilidade na implantação:
  - Modelo Hub-and-Spoke: Um hub central se conecta a várias filiais. O FlexVPN simplifica a configuração dessas conexões com uma única estrutura, tornando-a ideal para redes grandes.
  - Topologias de malha completa e de malha parcial: Todos os locais podem se comunicar diretamente sem passar por um hub central, reduzindo o atraso e melhorando o desempenho.
- Alta disponibilidade e redundância:
  - Hubs redundantes: Oferece suporte a vários hubs para backup. Se um hub falhar, as filiais podem se conectar a outro hub, garantindo conectividade contínua.

    - Balanceamento de carga: Distribui conexões VPN em vários dispositivos para evitar que um único dispositivo fique sobrecarregado, o que é crucial para manter o desempenho em grandes implantações.
- Autenticação e autorização escaláveis:
    - Integração AAA: Funciona com servidores AAA, como Cisco ISE ou RADIUS, para o gerenciamento centralizado de credenciais e políticas de usuário, essenciais para o uso em larga escala.
    - PKI e certificados: Suporta Public Key Infrastructure (PKI) e certificados digitais para autenticação segura, que é mais escalável do que usar chaves pré-compartilhadas, especialmente em grandes ambientes.

Informações de Apoio

FlexVPN e NHRP

O servidor FlexVPN oferece a funcionalidade do servidor do FlexVPN. O cliente FlexVPN estabelece um túnel IPsec VPN seguro entre um cliente FlexVPN e outro servidor FlexVPN.

O NHRP é um protocolo semelhante ao Address Resolution Protocol (ARP) que alivia os problemas de rede de multiacesso sem broadcast (NBMA). Com o NHRP, as entidades NHRP conectadas a uma rede NBMA aprendem dinamicamente o endereço NBMA das outras entidades que fazem parte dessa rede, permitindo que essas entidades se comuniquem diretamente sem exigir tráfego para usar um salto intermediário.

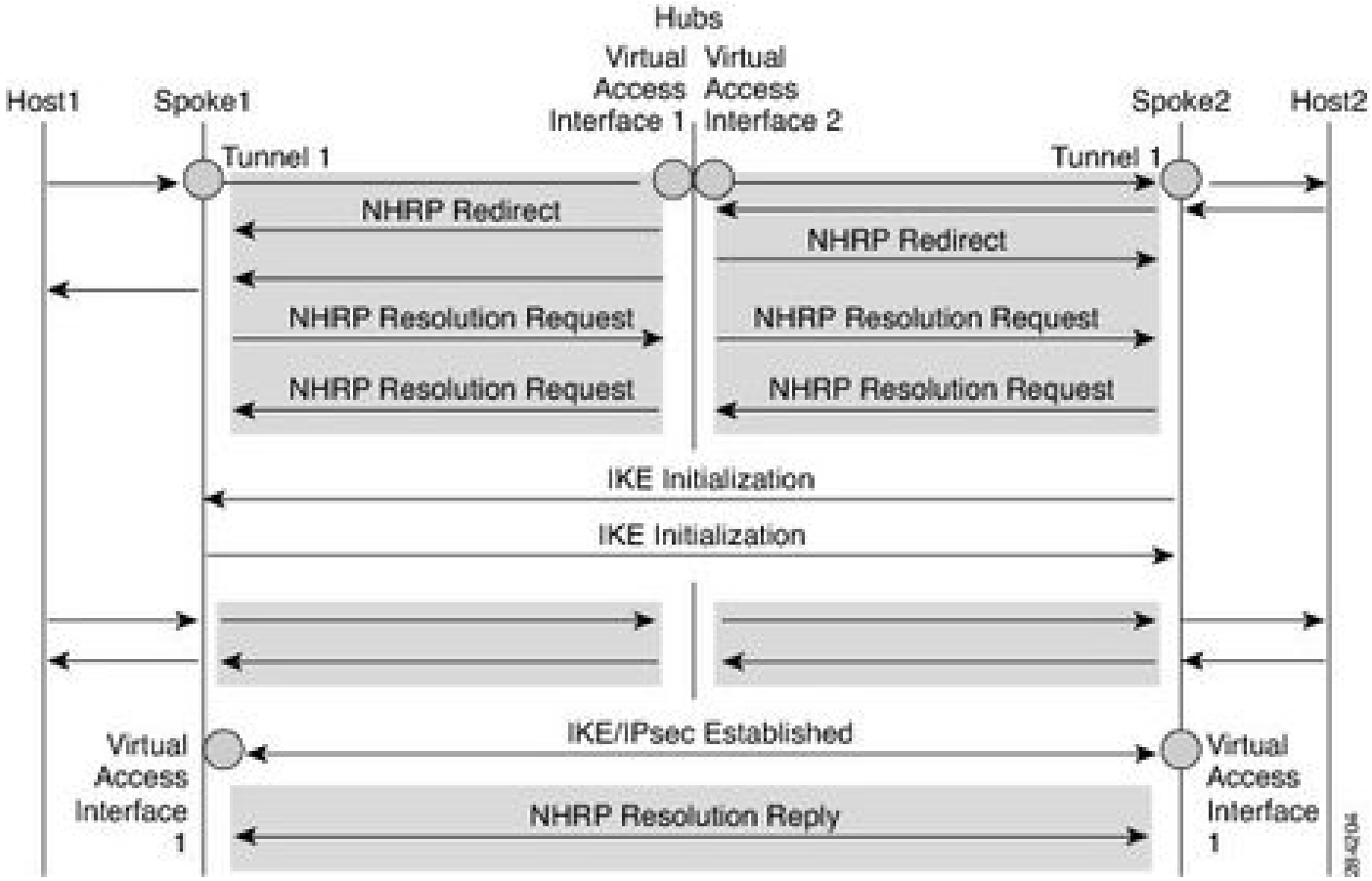
O recurso Spoke to Spoke do FlexVPN integra NHRP e cliente FlexVPN (spoke) para estabelecer um canal de criptografia direto com outro cliente em uma rede FlexVPN existente. As conexões são criadas usando interfaces de túnel virtual (VTI), IKEv2 e NHRP, onde o NHRP é usado para resolver os clientes FlexVPN na rede.

A Cisco recomenda garantir:

- As entradas de roteamento não são trocadas entre os spokes. Uma consideração importante, explicada posteriormente à medida que avançamos para solucionar problemas de topologia baseada em EIGRP.

- Perfis diferentes são usados para os spokes e o comando config-exchange não está configurado para os spokes.

Processo NHRP



A ilustração demonstra o fluxo de tráfego entre Spoke 1 e Spoke 2, com as redes 198.51.100.0/29/24 e 198.51.100.8/29, ambas anunciadas através do peering EIGRP diretamente para os spokes através do hub. Esta é a aparência do fluxo de tráfego quando a comunicação é estabelecida entre Spoke 1(198.51.100.0/29/24) e Spoke 2 (198.51.100.8/29).

1. O Host 1 envia o tráfego destinado ao Host 2. A pesquisa de rota no Host 1 resulta no seu encaminhamento para a interface de túnel de hub, pois o hub está anunciando essa rede via EIGRP.
2. Quando o tráfego chega ao hub, a consulta de rota final do hub confirma que a rede 198.51.100.8/29 do spoke 2 é aprendida por meio do acesso virtual do spoke 2.
3. O hub inicia o redirecionamento de NHRP, pois as interfaces de acesso virtual (spoke 1 e spoke 2) fazem parte da mesma rede NHRP com o mesmo ID de rede NHRP.
4. Ao receber o redirecionamento, Spoke1 inicia uma solicitação de resolução para a rede spoke 2 pela interface de túnel (a mesma interface pela qual recebeu o redirecionamento). Spoke 2 repete o mesmo processo para a solicitação de resolução da rede spoke 1.
5. Spoke2 recebe a solicitação de resolução na interface de túnel e recupera o número do modelo virtual conforme definido na configuração. O número do modelo virtual é usado para criar a interface de acesso virtual para estabelecer uma sessão de criptografia entre dois spokes. Quando as SAs de criptografia entre os dois spokes estiverem ativadas, ambos os spokes instalam rotas do endereço IP do próximo salto aprendidas via IPSEC após o estabelecimento de interfaces de acesso virtual.
6. Os dois spokes então continuam a verificar a acessibilidade do próximo salto antes de enviar a resposta de resolução através da recém-criada interface virtual-access para conectividade spoke-to-spoke.

7. Quando o próximo salto estiver acessível, ambos os spokes enviarão uma resposta de resolução um ao outro.
8. Agora, ambos os spokes podem substituir o endereço IP do próximo salto da rede destino um do outro para acesso virtual via NHO.
9. Spoke1 instala as entradas de cache necessárias para o IP do próximo salto do Spoke2 e sua rede. Spoke1 também exclui a entrada de cache temporária que aponta para o hub para resolver a rede na interface1 do túnel.
10. O mesmo passo é repetido pelo spoke 2, ele também instala entradas de cache para o IP do próximo salto do spoke 1 e sua rede avança na exclusão da entrada antiga do hub pelo túnel.
11. O NHRP adiciona rotas de atalho como a rota de substituição do próximo salto (NHO) ou a rota H (NHRP).

Configuração do FlexVPN spoke to spoke usando EIGRP

Considerações importantes para a topologia baseada em EIGRP

Antes de prosseguir para a configuração, há alguns conceitos-chave que devemos entender,

- Para qualquer implantação do EIGRP, se os spokes estiverem recebendo uma tabela de roteamento completa de outros spokes ou apenas rotas de sumarização, uma lista de prefixos precisa ser instalada no lado do hub para atualizações de roteamento de saída para filtrar endereços IP de túnel de spokes a serem anunciados uns nos outros.

- O split horizon no EIGRP funciona de forma diferente do IBGP. O EIGRP apenas interrompe o anúncio de redes fora de uma interface na qual elas foram aprendidas. Por exemplo, o hub tem dois spokes, um conectado através de interfaces de acesso virtual 1 e o outro através de acesso virtual 2. As rotas aprendidas pelo hub via VA 1 do spoke 1 são anunciadas de volta para spoke 2 via VA 2 e vice-versa, já que VA 1 e VA 2 são interfaces diferentes. No caso do IBGP, ele não anuncia nenhuma rede aprendida de seu peer de volta para outro peer. Em um exemplo semelhante, um hub configurado com o IBGP não anuncia redes de volta que aprendeu de VA 1 para VA 2 e vice-versa.

- Esse comportamento no EIGRP cria um conflito na adjacência CEF para o endereço IP do próximo salto (um endereço IP de interface de acesso virtual para um túnel spoke-to-spoke), pois ele é aprendido primeiro via EIGRP usando uma interface de túnel de hub e depois via IPsec usando uma interface de acesso virtual. Isso causa roteamento assimétrico para o tráfego NHRP e também resulta em uma entrada NHRP duplicada na tabela NHRP e entradas NHO duplicadas na tabela de roteamento, bem como para as interfaces do próximo salto (túnel via hub) e (acesso virtual via spoke).

- Rastreamos esse comportamento no bug da Cisco ID CSCwn54813 e no bug da Cisco ID CSCwn54758. A Cisco aconselharia seguir a solução fornecida para a filtragem de endereços de túnel no hub para atualizações de saída.

- O modelo virtual do lado do hub precisa ter IP de um pool diferente das interfaces de túnel de spokes, já que queremos filtrar as atualizações de saída do EIGRP para garantir que o

peering do EIGRP de hub e spoke não seja afetado.

Aqui estão dois exemplos que mostram como configurar o spoke do FlexVPN usando EIGRP no servidor FlexVPN e no cliente FlexVPN. Seguimos as práticas recomendadas para segregar o tráfego subjacente e de sobreposição colocando-os em VRFs específicos. O VRF A é para a subjacência, enquanto o B é usado para a sobreposição.

Exemplo 1 - Utilização de NHO (Next-Hop-Override) para comunicação spoke-to-spoke

Servidor 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
```

Cliente FlexVPN 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
```

Cliente FlexVPN 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
```

Exemplo 2 - Utilização de Rotas Instaladas de NHRP para Comunicação Spoke to Spoke

Servidor FlexVPN

A única alteração na configuração do EIGRP é introduzir rotas de sumarização em vez da tabela de roteamento completa nos spokes. Certifique-se de desativar o modelo virtual para enviar a configuração de resumo para a topologia EIGRP. Consulte o bug da Cisco ID 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
```

Verificação e solução de problemas

Exemplo 1 - Utilização de NHO (Next-Hop-Override) para comunicação spoke-to-spoke

Spoke 1 (antes da resolução e do estabelecimento de túnel Spoke to Spoke NHRP)

```
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 (antes da resolução e do estabelecimento de túnel do NHRP spoke to spoke)

```
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 (após a resolução e o estabelecimento de túnel do NHRP Spoke to Spoke)

Iniciando o ICMP para disparar o túnel 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
```

Verificando o atalho 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
```

Verificando a criação do atalho de postagem das rotas 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
```

Verificando contadores 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 (após o estabelecimento da resolução e do túnel spoke to spoke NHRP)

Verificando o atalho 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
```

Verificando a criação do atalho de postagem das rotas 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
```

Verificando contadores NHRP.

Aqui está uma explicação passo a passo de como um túnel spoke-to-spoke direto é estabelecido com a ajuda de depurações de um dos spokes.

- O spoke 1 iniciou o 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
```

- O hub recebeu o ICMP e iniciou o redirecionamento (indicação de tráfego) para ambos os spokes.

```
*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
```

- Ambos os spokes acionaram uma solicitação de resolução que passou por 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
```

- Ambos os spokes receberam uma solicitação de resolução via 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:
```

- Ambos os spokes realizaram pesquisa de rota para suas redes locais 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
```

- A resposta de resolução foi enfileirada e o estabelecimento de IPsec foi iniciado, pois ambos os spokes agora estão cientes dos endereços NBMA um do outro.

```
*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 o estabelecimento de IPSEC e o processo de criação de atalhos NHRP, ambos os spokes aprenderam e instalaram uns aos outros endereços ip de túnel em sua tabela de roteamento como rota IPSEC e sondaram a acessibilidade do próximo salto.

```
*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
```

- Até a conclusão da instalação do atalho e do NHO, o spoke A executou a consulta do próximo salto de endereços IP de acesso virtual do spoke B e vice-versa, mas a consulta da próxima esperança retornou "N/A rendado", devido ao qual o spoke A enviou uma indicação de erro para o spoke B confirmando que o próximo salto está inacessível. A pesquisa específica pode ser chamada de pesquisa de vários caminhos.

```
*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:
```

- Quando o NHO é acionado para o próximo salto e o atalho é criado, ambos os spokes enviam solicitações de resolução para a rede um do outro novamente.

```
*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
```

- Quando ambos os spokes receberam solicitações de resolução para as redes um do outro, o NHO substituiu a rota EIGRP via túnel (HUB) por acesso virtual.

```
*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
```

- Depois, ambos os spokes enviam uma resposta de resolução através da interface de acesso virtual.

```
*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
```

Exemplo 2 - Utilização de Rotas Instaladas de NHRP para Comunicação Spoke to Spoke

Servidor FlexVPN

Verificação da topologia do EIGRP para a rota sumarizada introduzida.

```
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
```

Clientes FlexVPN

Verificando a presença de rota sumarizada.

```
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
```

Tente estabelecer um túnel spoke-to-spoke iniciando o tráfego.

```
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
```

Verificando novamente.

```
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
```

Há uma alteração muito pequena na saída de depurações para a instalação de rede de spokes, onde ela mostra a instalação bem-sucedida da rota em vez de falha de RIB e a adição de NHO.

```
*Feb 3 16:43:38.957: NHRP-CACHE: Virtual-Access1: Cache add for target 198.51.100.8/29 vrf: B(0x4) label
*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
```

Informações Relacionadas

- Configurando o FlexVPN spoke to spoke
- Exemplo de configuração de spoke do FlexVPN no design de hub redundante com bloco de cliente do FlexVPN

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.