Configurar BGP sobre DMVPN Fase 3

Contents

Introdução

Este documento descreve a configuração e a operação da Fase 3 do DMVPN usando o BGP, incluindo a solução de problemas em camadas para túneis IPsec sobre DMVPN.

Pré-requisitos

Para os comandos de configuração e debug neste documento, você precisa de dois roteadores Cisco que executem o Cisco IOS® versão 15.3(3)M ou posterior. Em geral, uma Dynamic Multipoint VPN (DMVPN) Fase 3 básica requer o Cisco IOS versão 12.4(6)T, embora os recursos e depurações vistos neste documento não sejam totalmente suportados.

Requisitos

A Cisco recomenda que você tenha conhecimento básico destes tópicos:

- IKEV1/IKEV2 e IPsec
- Componentes DMVPN:

- Protocolo de Resolução de Próximo Salto (NHRP - Next Hop Resolution Protocol): Cria um banco de dados de mapeamento distribuído (NHRP) de todos os túneis spoke's para

endereços reais (interface pública)
- Interface de túnel de encapsulamento de roteamento genérico multiponto (mGRE): Interface única de encapsulamento de roteamento genérico (GRE - Generic Routing Encapsulation) para suportar vários túneis GRE/IPsec, simplifica o tamanho e a complexidade da configuração e suporta a criação de túnel dinâmico.
- Proteção de túnel IPsec: Cria e aplica dinamicamente políticas de criptografia
- Roteamento: Redes dinâmicas; quase todos os protocolos de roteamento (Enhanced Interior Gateway Routing Protocol (EIGRP), Routing Information Protocol (RIP), Open Shortest Path First (OSPF), BGP, ODR) são suportados

Componentes Utilizados

As informações neste documento são baseadas nos Cisco ASR1000 Series Aggregation Services Routers, versão 17.6.5(MD).

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.

Informações de Apoio

O que é DMVPN?

O DMVPN é uma solução de software Cisco IOS para criar VPNs IPsec+GRE de forma fácil, dinâmica e escalável. É uma solução para criar uma rede VPN com vários locais sem ter que configurar todos os dispositivos estaticamente. É uma rede 'hub and spoke' em que os spokes podem se comunicar diretamente entre si sem precisar passar pelo hub. A criptografia é suportada por IPsec, o que torna o DMVPN uma opção popular para conectar diferentes sites usando conexões de Internet regulares.

Como funciona o DMVPN?

- Os spokes criam um túnel GRE/IPsec permanente dinâmico para o hub, mas não para outros spokes. Eles se registram como clientes do servidor NHRP (hub).
- Quando um spoke precisa enviar um pacote para uma sub-rede de destino (privada) atrás de outro spoke, ele consulta via NHRP o endereço real (externo) do spoke de destino.
- Agora, o spoke de origem pode iniciar um túnel GRE/IPsec dinâmico para o spoke de destino (porque ele conhece o endereço do peer).
- O túnel spoke-to-spoke dinâmico é construído sobre a interface mGRE.
- Quando o tráfego é interrompido, o túnel spoke-to-spoke é removido.

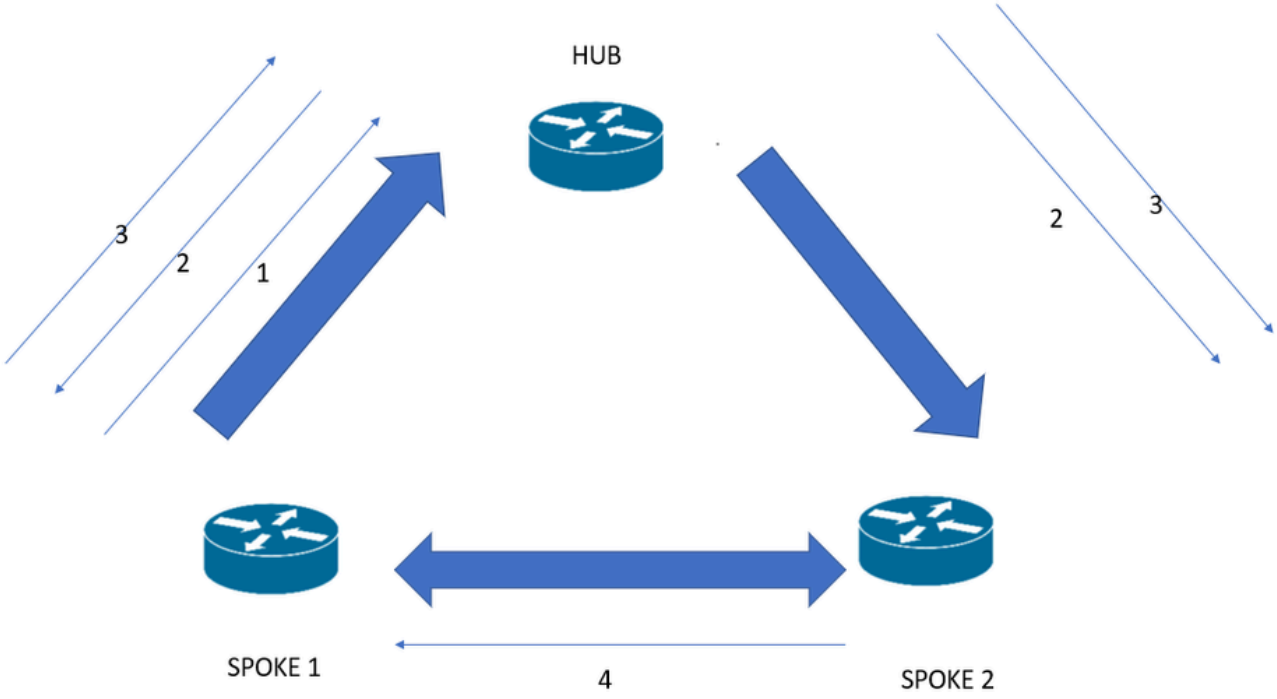
Quais são os diferentes tipos de DMVPN?

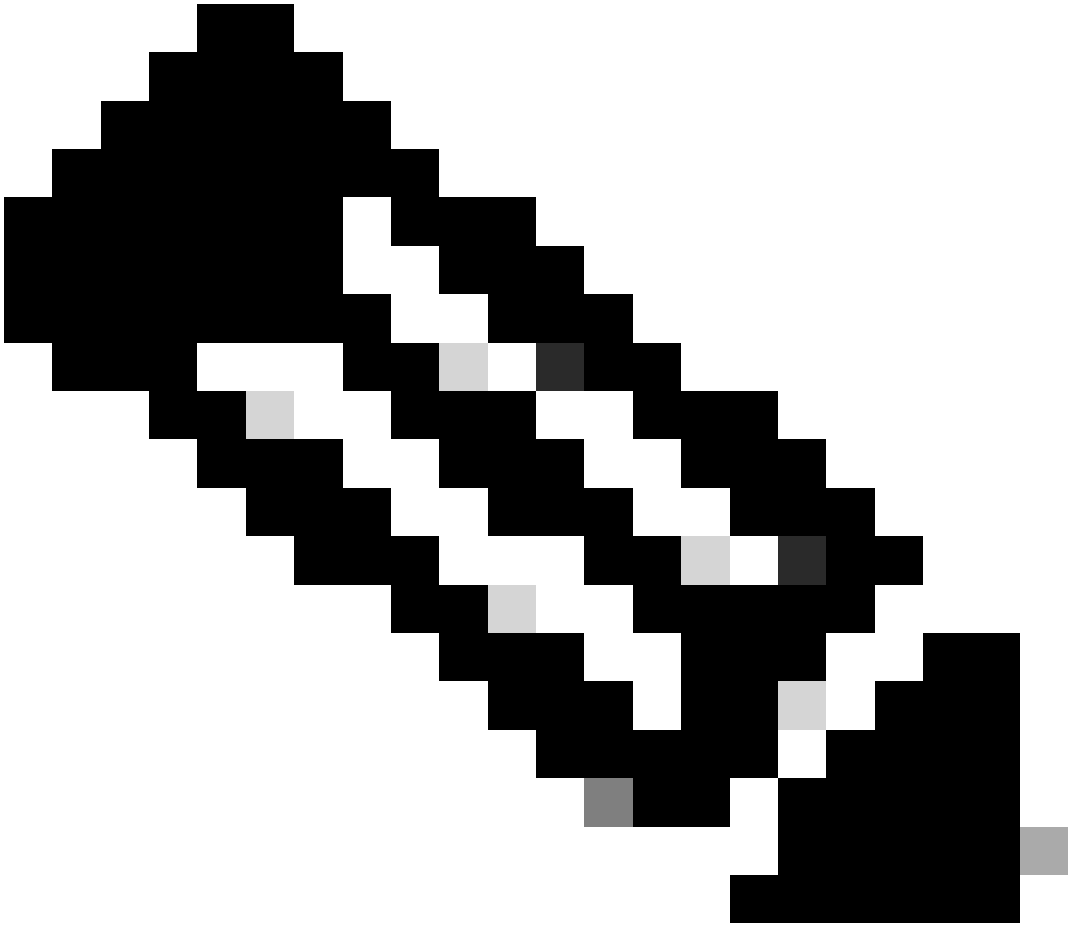
1. DMVPN Fase I: Essa fase envolve uma única interface mGRE no hub e todos os spokes ainda são túneis estáticos, de modo que você não obtém nenhuma conectividade dinâmica

de spoke para spoke.
2. DMVPN Fase II: Essa fase envolve a configuração de cada local com uma interface mGRE para que você obtenha a conectividade dinâmica spoke-to-spoke.
3. DMVPN Fase III: essa fase se expande na escalabilidade da rede DMVPN. Isso envolve o resumo na nuvem DMVPN. Junto com a configuração de redirecionamentos de NHRP e switching de atalho de NHRP. Os redirecionamentos de NHRP instruem a origem a encontrar um caminho melhor para o destino que está tentando alcançar. Os atalhos do NHRP permitem que o DMVPN aprenda sobre outras redes atrás de outros roteadores DMVPN.

Fluxo de tráfego para DMVPN Fase 3

1. O pacote é enviado da rede 1 de Spoke para as 2 redes de Spoke via Hub (de acordo com a tabela de roteamento).
2. O hub roteia o pacote para Spoke2, mas, paralelamente, envia de volta a mensagem de redirecionamento de NHRP para Spoke1, contendo informações sobre o caminho não ideal para Spoke2 e o IP do túnel de Spoke2.
3. Spoke1 envia então a solicitação de Resolução NHRP do endereço IP 2 NBMA (Nonbroadcast Multiaccess) do Spoke para o NHS (Next Hop Server) com o IP destino do túnel 2 do Spoke. Essa solicitação de resolução de NHRP é enviada para Spoke2 via NHS (de acordo com a tabela de roteamento) - é um processo normal de encaminhamento de NHRP salto por salto.
4. Spoke2 depois de receber a solicitação de resolução incluindo o IP NBMA de Spoke1 envia a resposta de Resolução NHRP diretamente para Spoke1 - A resposta não atravessa o Hub!
5. Spoke1 depois de receber o IP NBMA correto de Spoke2 regrava a entrada CEF para o prefixo de destino - esse procedimento é chamado de Atalho NHRP.
6. Os spokes não acionam o NHRP por adjacências de coleta, mas as respostas do NHRP atualizam o CEF.


HUB
3
2
1
2
3
SPOKE 1
4
SPOKE 2

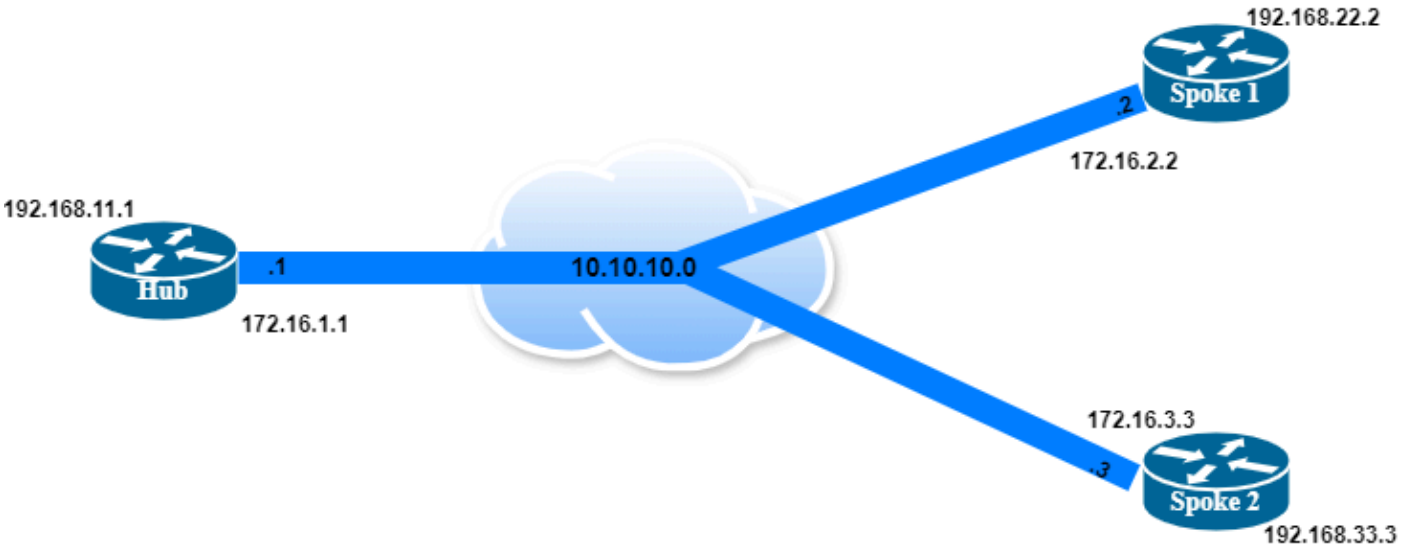


Note:

Fase 2 da DMVPN: Nessa fase, o pacote spoke-to-spoke inicial é, de fato, comutado por processo, pois a adjacência CEF está no estado 'glean'. Isso significa que o roteador não tem informações suficientes para encaminhar o pacote usando o CEF e deve usar uma comutação de processo com uso mais intensivo de recursos para resolver o próximo salto usando o NHRP (Next Hop Resolution Protocol).

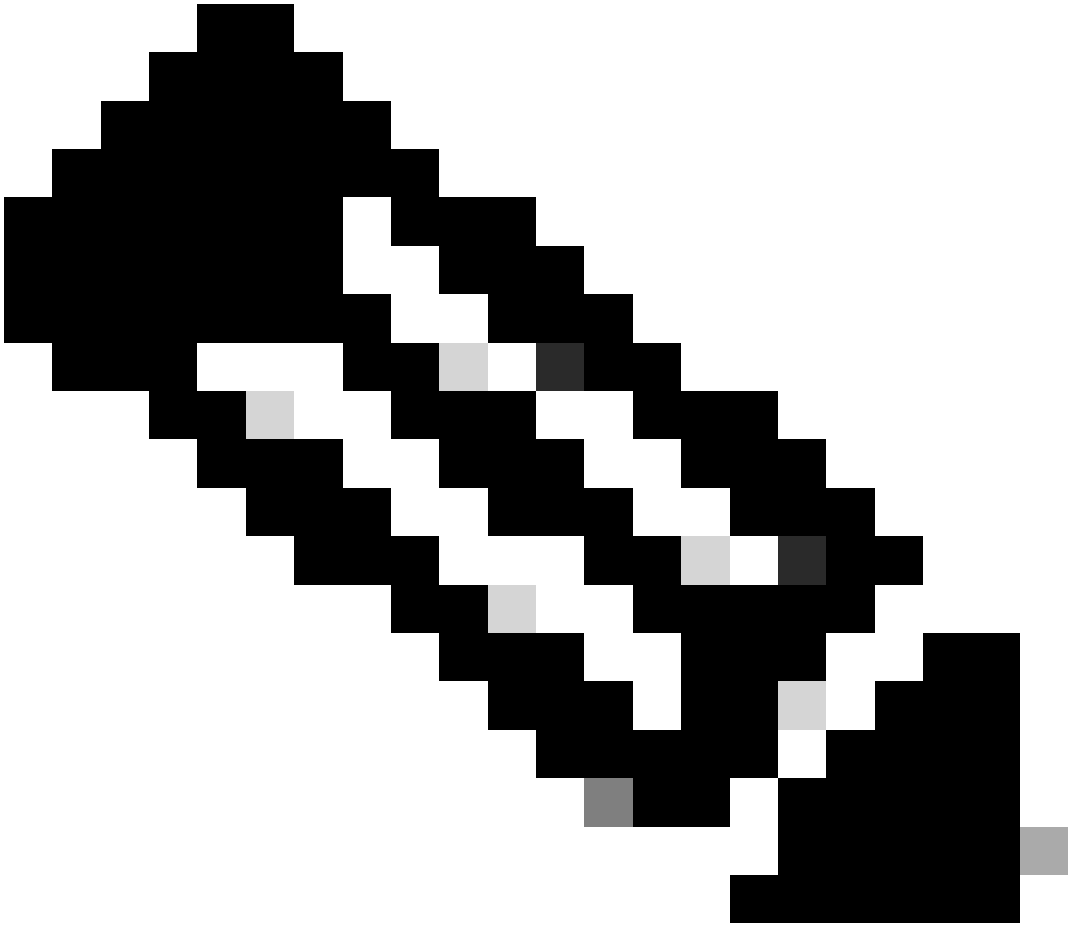
Fase 3 da DMVPN: Essa fase melhora a Fase 2, permitindo que o pacote spoke-to-spoke inicial seja comutado usando CEF desde o início. Isso é obtido com o uso dos recursos de Redirecionamento NHRP e Atalho NHRP, que ajudam a estabelecer rapidamente túneis spoke-to-spoke diretos. Como resultado, o CEF é usado de forma mais consistente, reduzindo a dependência na comutação de processos.

Diagrama de Rede



Configurações

Configurações de criptografia



Note: Isso é o mesmo no hub e em todos os spokes.

1. Configure uma proposta e um chaveiro Ikev2.

```
crypto ikev2 proposal DMVPN
encryption aes-cbc-256
integridade sha256
grupo 14
crypto ikev2 keyring IKEV2-KEYRING
peer any
address 0.0.0.0 0.0.0.0
CISCO123 de chave pré-compartilhada
!
```

2. Configure o perfil Ikev2 que contém todas as informações relacionadas à conexão.

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

match address local interface GigabitEthernet0/0/0
match identity remote address 0.0.0.0
pré-compartilhamento local de autenticação
pré-compartilhamento remoto de autenticação
keyring local IKEV2-KEYRING

Estes são os detalhes dos comandos usados no perfil ikev2:

- match address local interface GigabitEthernet0/0/0: Interface externa local onde a VPN termina, neste caso, GigabitEthernet0/0/0
- match identity remote address 0.0.0.0: Como o peer remoto pode ser múltiplo, usando 0.0.0.0, que indica qualquer peer
- pré-compartilhamento local de autenticação: O modo de autenticação no site local é pré-compartilhado
- pré-compartilhamento remoto de autenticação: O modo de autenticação no site local é pré-compartilhado
- chaveiro local IKEV2-KEYRING: Use o mesmo chaveiro que você criou anteriormente.

3. Configure o perfil IPsec.

crypto ipsec transform-set T-SET esp-aes 256 esp-sha256-hmac
túnel de modo

crypto ipsec profile IPSEC-IKEV2

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

Crie um conjunto de transformação para a negociação de túnel IPsec e chame o conjunto de transformação e o perfil Ikev2 no perfil IPsec.

Configuração de DMVPN

1. Configure a interface externa.

interface GigabitEthernet0/0/0

endereço ip 172.16.1.1 255.255.255.0
negotiation auto
cdp enable

2. Configure o roteador de hub para integração mGRE e IPsec (isto é, associe o túnel ao perfil IPsec configurado no procedimento anterior)

interface Tunnel0
endereço 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 <-------- Obrigatório para habilitar a fase 3 do DMVPN no roteador hub
tunnel source GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel protection ipsec profile IPSEC-IKEV2
!
```

Estes comandos são usados na configuração da interface do túnel:

- ip nhrp authentication DMVPN: Nesse caso, a cadeia de autenticação 'DMVPN' deve ter o mesmo valor em todos os hubs e spokes que fazem parte da mesma rede DMVPN.
- ip nhrp map multicast dynamic: Permite que o NHRP adicione spokes ao mapeamento multicast do NHRP dinamicamente.
- ip nhrp network-id 1: Identificador de rede de 32 bits que ativa o NHRP em uma interface.
- ip nhrp redirect: Habilita a indicação de tráfego de redirecionamento se o tráfego for encaminhado com a rede NHRP.
- origem de túnel GigabitEthernet0/0/0: Define o endereço de origem para uma interface de túnel, onde você está usando o endereço IP GigaEthernet 0/0/0.
- tunnel mode gre multipoint: Define o modo de encapsulamento como mGRE para essa interface de túnel.
- tunnel protection ipsec profile IPSEC-IKEV2: Associa uma interface de túnel ao perfil IPsec que já foi criado em configurações de criptografia.

3. Configurar roteadores spoke para integração de mGRE e IPsec com uma interface externa e loopback para testar a conectividade do Border Gateway Protocol (BGP).

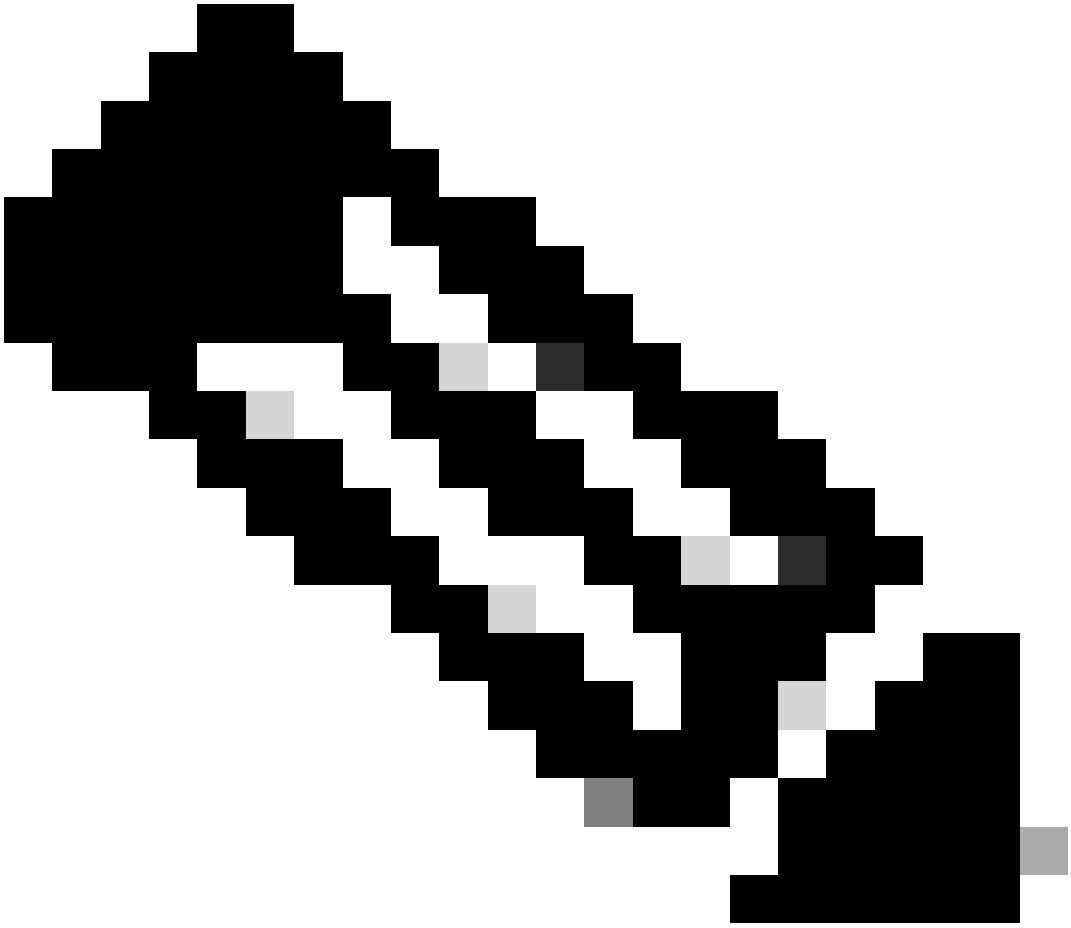
RAIO X: (Uma configuração semelhante pode ser usada em todos os spokes)

```
interface GigabitEthernet0/0/0
endereço ip 172.16.3.3 255.255.255.0
velocidade 1000
no negotiation auto

!

interface Loopback10
endereço ip 192.168.33.3 255.255.255.0
!
interface Tunnel0
endereço ip 10.10.10.3 255.255.255.0
no ip redirects
ip nhrp authentication DMVPN
ip nhrp map 10 10 10 172 16 1 1 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 <-------- Obrigatório para habilitar DMVPN Fase 3 no Spoke Router
```

tunnel source GigabitEthernet0/0/0
tunnel mode gre multipoint
tunnel protection ipsec profile IPSEC-IKEV2

Estes comandos são usados na configuração da interface do túnel:

- ip nhrp authentication DMVPN: Nesse caso, a cadeia de autenticação 'DMVPN' deve ter o mesmo valor em todos os hubs e spokes que fazem parte da mesma rede DMVPN.
- ip nhrp map 10.10.10.1 172.16.1.1: Mapeia manualmente o endereço IP NBMA do hub com o endereço IP da interface do túnel.
- ip nhrp map multicast 172.16.1.1: Redireciona todo o tráfego multicast para o hub.
- ip nhrp network-id 1: Identificador de rede de 32 bits que ativa o NHRP em uma interface.
- ip nhrp nhs 10.10.10.1: O servidor do próximo salto, que é nosso hub, é configurado com esse comando.
- atalho ip nhrp: Ativa a comutação de atalhos NHRP em uma interface.
- origem de túnel GigabitEthernet0/0/0: Define o endereço de origem para uma interface de túnel, onde você está usando o endereço IP GigaEthernet 0/0/0.
- tunnel mode gre multipoint: Define o modo de encapsulamento como mGRE para essa interface de túnel.
- tunnel protection ipsec profile IPSEC-IKEV2: Associa uma interface de túnel ao perfil IPsec que já foi criado em configurações de criptografia.



Note: O comando ip nhrp redirect envia a mensagem para os Spokes que diz "Há uma rota melhor para o Spoke de destino do que através do Hub" e o atalho ip nhrp impõe a instalação dessa rota na Base de Informações de Encaminhamento (FIB) nos Spokes.

Configuração de BGP

Há várias variações que podem ser escolhidas:

- eBGP com um número AS diferente em cada spoke
- eBGP com o mesmo número AS em cada spoke
- iBGP

Explicar todos os três cenários está fora do escopo deste documento.

Um eBGP com um número AS diferente em todos os spokes é configurado, de modo que os vizinhos dinâmicos não podem ser usados. Portanto, você deve configurar os vizinhos manualmente.

eBGP com AS diferente nos raios

1. Configuração de BGP no HUB:

Hub(config)#router bgp 65010

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

Hub(config-router)#network 192.168.11.1 máscara 255.255.255.255

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

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

!

Estes comandos são usados na configuração do BGP no Hub:

- router bgp 65010: Configura um processo de roteamento BGP. Use o argumento 'autonomous-system-number' que identifica o dispositivo para outros alto-falantes BGP.
- rede 192.168.11.1 máscara 255.255.255.255: Especifica uma rede como local para este sistema autônomo e a adiciona à tabela de roteamento BGP.
- neighbor 10.10.10.2 remote-as 65011: Adiciona o endereço IP do vizinho Spoke 1 no sistema autônomo especificado à tabela de vizinhos BGP multiprotocolo IPv4 do dispositivo local.
- neighbor 10.10.10.3 remote-as 65012: Adiciona o endereço IP do vizinho Spoke 2 no sistema autônomo especificado à tabela de vizinhos BGP multiprotocolo IPv4 do dispositivo local.

2. Configuração de BGP no Spoke X:

Spoke2(config)#router bgp 65012

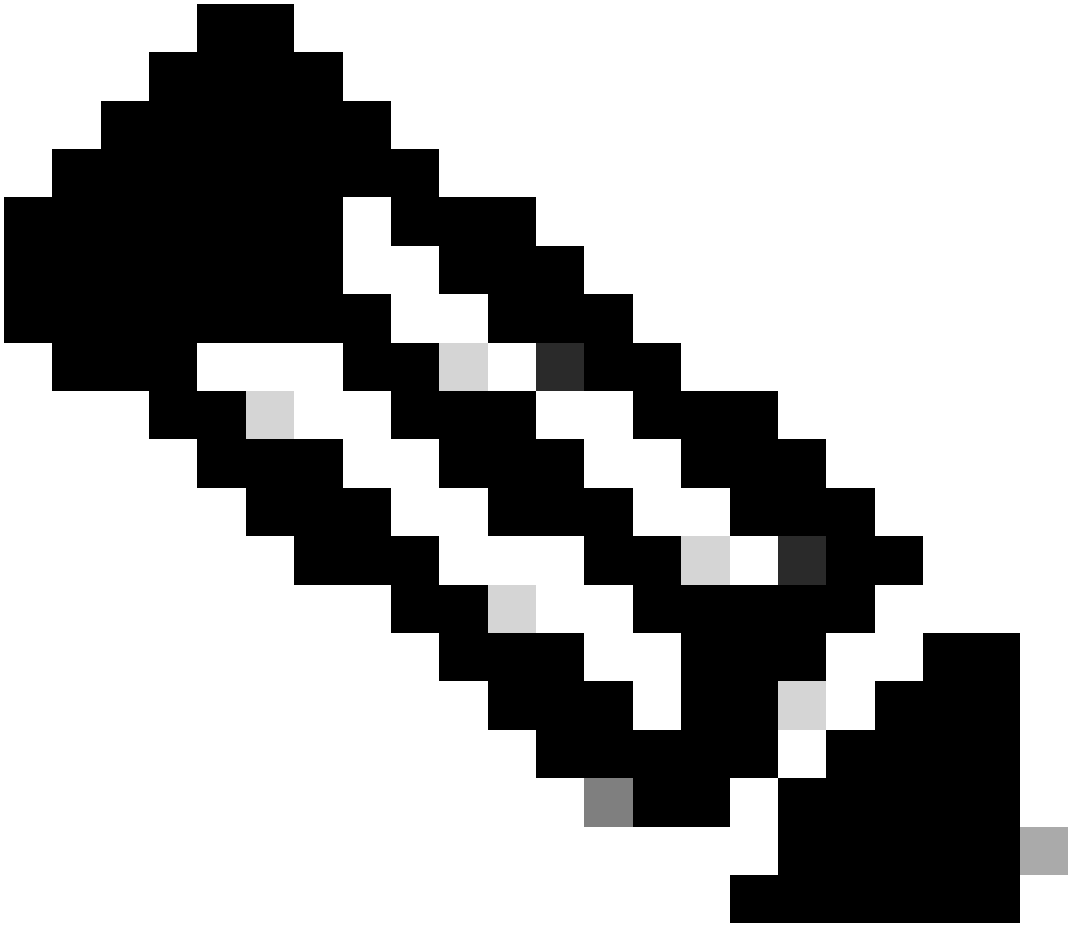
Spoke2(config-router) #bgp log-neighbor-changes

Spoke2(config-router)# network 192.168.33.3 mask 255.255.255.255

Spoke2(config-router)# neighbor 10.10.10.1 remote-as 65010

Estes comandos são usados na configuração do BGP no Spoke X:

- router bgp 65012: Configura um processo de roteamento BGP. Use o argumento 'autonomous-system-number' que identifica o dispositivo para outros alto-falantes BGP.
- rede 192.168.33.3 máscara 255.255.255.255: Especifica uma rede como local para este sistema autônomo e a adiciona à tabela de roteamento BGP.
- neighbor 10.10.10.1 remote-as 65010: Adiciona o endereço IP do Hub no sistema autônomo especificado à tabela de vizinhos BGP multiprotocolo IPv4 do dispositivo local.



Note: Uma configuração semelhante deve ser feita em todos os spokes na rede DMVPN.

Verificar

1. Comandos de verificação no dispositivo Hub:

HUB#sh dmvpn

Exibe informações de sessão específicas de DMVPN.

Legenda: Attrb —> S - Estático, D - Dinâmico, I - Incompleto
N - NATed, L - Local, X - Sem soquete
T1 - Rota Instalada, T2 - Nexthop-override
C - Compatível com CTS
Ent —> Número de entradas NHRP com o mesmo peer NBMA
Status do NHS: E —> Esperando Respostas, R —> Respondendo, W —> Aguardando
Tempo de Atividade —> Tempo de Atividade ou Inatividade para um Túnel

==========

Interface: Detalhes de Tunnel0, IPv4 NHRP
Tipo:Hub, NHRP Peers:2, <<<<<<<<<<<<<<<<<<<<<<< Informa que o dispositivo está atuando como Hub e 2 peers NHRP estão conectados a este 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 <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< Os dois peers foram registrados dinamicamente com o hub e estão no estado UP.
1 172.16.3.3 10.10.10.3 ATIVO 01:08:58 D

HUB#sh ip nhrp

Mostra o mapeamento de endereço NBMA para IP de interface de túnel de todos os pares NHRP conectados ao Hub. O hub mantém o banco de dados de todos os spokes.

10.10.10.2/32 via 10.10.10.2
Tunnel0 criado 01:47:22, expirar 01:32:27
Digite: dinâmico, Sinalizadores: unique registered used nhop
Endereço NBMA: 172.16.2.2
10.10.10.3/32 via 10.10.10.3
Tunnel0 criado 01:09:11, expirar em 01:29:58
Digite: dinâmico, Sinalizadores: unique registered used nhop
Endereço NBMA: 172.16.3.3

HUB#sh ip nhrp multicast

Exibe informações de mapeamento multicast NHRP.

Endereço NBMA I/F
Sinalizadores Tunnel0 172.16.2.2: dynamic (Enabled) (Dinâmico (Ativado))
Sinalizadores Tunnel0 172.16.3.3: dynamic (Enabled) (Dinâmico (Ativado))

HUB#sh crypto sockets

Número de conexões do soquete de criptografia 2

Pares Tu0 (local/remoto): 172.16.1.1/172.16.2.2
Identificação local (endereço/máscara/porta/porta): (172.16.1.1/255.255.255.255/0/47)
Identificação remota (endereço/máscara/porta/porta): (172.16.2.2/255.255.255.255/0/47)
Perfil de IPSec: "IPSEC-IKEV2"
Estado do soquete: Abrir
Cliente: "TUNNEL SEC" (Estado do Cliente: Ativo)
Pares Tu0 (local/remoto): 172.16.1.1/172.16.3.3
Identificação local (endereço/máscara/porta/porta): (172.16.1.1/255.255.255.255/0/47)
Identificação remota (endereço/máscara/porta/porta): (172.16.3.3/255.255.255.255/0/47)

Perfil de IPSec: "IPSEC-IKEV2"
Estado do soquete: Abrir
Cliente: "TUNNEL SEC" (Estado do Cliente: Ativo)
Soquetes de criptografia no estado de escuta:
Cliente: Perfil "TUNNEL SEC": "IPSEC-IKEV2" Nome do mapa: "Tunnel0-head-0"

HUB#sh cry ikev2 sa

IPv4 Crypto IKEv2 SA

Status remoto FVRF/IVRF de Tunnel-id
1 172.16.1.1/500 172.16.2.2/500 nenhum/nenhum PRONTO
Encr.: AES-CBC, tamanho da chave: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Sinal de autenticação: PSK, verificação de autenticação: PSK
Vida/Tempo Ativo: 86400/6524 seg

Status remoto FVRF/IVRF de Tunnel-id
2 172.16.1.1/500 172.16.3.3/500 nenhum/nenhum PRONTO
Encr.: AES-CBC, tamanho da chave: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Sinal de autenticação: PSK, verificação de autenticação: PSK
Vida/Tempo Ativo: 86400/4234 seg

IPv6 Crypto IKEv2 SA

HUB#sh ip bgp summary

Exibe o estado atual da sessão BGP/o número de prefixos que o roteador recebeu de um vizinho ou grupo de peer.

Identificador de roteador BGP 192.168.11.1 número AS local 65010
A versão da tabela de BGP é 4, a versão da tabela de roteamento principal é 4.
3 entradas de rede usando 432 bytes de memória
3 entradas de caminho usando 252 bytes de memória
3/3 entradas de atributo de caminho/melhor caminho BGP usando 480 bytes de memória
2 entradas AS-PATH BGP usando 48 bytes de memória
0 entradas de cache de mapa de rota BGP usando 0 bytes de memória
0 entradas de cache de lista de filtros BGP usando 0 bytes de memória
BGP usando 1212 bytes totais de memória
Prefixos 3/0 de atividade do BGP, caminhos 3/0, intervalo de verificação de 60 segundos

Vizinho V AS MsgRcvd MsgSent TblVer Estado Up/Down InQ OutQ/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

Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvel, B - BGP
D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas
N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2

E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2
i - IS-IS, su - resumo IS-IS, L1 - IS-IS nível 1, L2 - IS-IS nível 2
ia - IS-IS inter-área, * - candidato padrão, U - rota estática por usuário
o - ODR, P - rota estática baixada periodicamente, H - NHRP, l - LISP
a - rota de aplicativo
+ - rota replicada, % - substituição do próximo salto, p - substituições de PfR

O gateway de último recurso é 172.16.1.2 para a rede 0.0.0.0

192.168.0.0/16 tem sub-redes variáveis, 4 sub-redes, 2 máscaras
B 192.168.22.0/24 [20/0] via 10.10.10.2, 00:29:15 <<<<<<<<<<<<Entrada para Spoke 1 rotas anunciadas
B 192.168.33.0/24 [20/0] via 10.10.10.3, 00:18:37 <<<<<<<<<<<<Entrada para Spoke 2 rotas anunciadas

2. Comandos de verificação no spoke 1:

Spoke1#sh dmvpn

Legenda: Attrb —> S - Estático, D - Dinâmico, I - Incompleto
N - NATed, L - Local, X - Sem soquete
T1 - Rota Instalada, T2 - Nexthop-override
C - Compatível com CTS, I2 - Temporário
Ent —> Número de entradas NHRP com o mesmo peer NBMA
Status do NHS: E —> Esperando Respostas, R —> Respondendo, W —> Aguardando
Tempo de Atividade —> Tempo de Atividade ou Inatividade para um Túnel
==========

Interface: Detalhes de Tunnel0, IPv4 NHRP
Tipo:Spoke, NHRP Peers: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 <<<<<<<<<<<<O hub está sendo mostrado como S- static desde que o configuramos como uma entrada estática na interface do túnel
1 172.16.3.3 10.10.10.3 UP 00:19:34 D <<<<<<<<<<<<Túnel sob demanda dinâmico spoke-to-spoke criado após o envio de tráfego para spoke 2

Spoke1#sh ip bgp summary

Identificador do roteador BGP 192.168.22.2, número AS local 65011
A versão da tabela de BGP é 4, a versão da tabela de roteamento principal é 4.
3 entradas de rede usando 744 bytes de memória
3 entradas de caminho usando 432 bytes de memória
3/3 entradas de atributo de caminho/melhor caminho BGP usando 864 bytes de memória
2 entradas AS-PATH BGP usando 64 bytes de memória
0 entradas de cache de mapa de rota BGP usando 0 bytes de memória

0 entradas de cache de lista de filtros BGP usando 0 bytes de memória
BGP usando 2104 bytes totais de memória
Prefixos 3/0 de atividade do BGP, caminhos 3/0, intervalo de verificação de 60 segundos
3 redes atingiram o pico às 08:16:54 jun 2 2022 UTC (01:11:51.732 atrás)

Vizinho V AS MsgRcvd MsgSent TblVer Estado Up/Down InQ OutQ/PfxRcd
10.10.10.1 4 65010 85 85 4 0 0 01:12:21 2 <<<<<<<<<<<<<<<<< Recebemos 2 prefixos do Hub, cada um para loopback de hub e loopback de Spoke2

Spoke1#sh ip route bgp

Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvel, B - BGP
D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas
N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2
E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2, m - OMP
n - NAT, Ni - NAT interno, Não - NAT externo, Nd - NAT DIA
i - IS-IS, su - resumo IS-IS, L1 - IS-IS nível 1, L2 - IS-IS nível 2
ia - IS-IS inter-área, * - candidato padrão, U - rota estática por usuário
H - NHRP, G - NHRP registrado, g - resumo de registro NHRP
o - ODR, P - rota estática baixada periodicamente, l - LISP
a - rota de aplicativo
+ - rota replicada, % - substituição do próximo salto, p - substituições de PfR

O Gateway de último recurso é 172.16.2.10 para a rede 0.0.0.0

B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:16 >>>>>>>>>>>>>>> Rede de hub acessível diretamente via hub

B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:46 >>>>>>>>>>>>>>>> Rede spoke diretamente acessível via IP de túnel spoke.

Spoke1#sh ip route

Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvel, B - BGP
D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas
N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2
E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2, m - OMP
n - NAT, Ni - NAT interno, Não - NAT externo, Nd - NAT DIA
i - IS-IS, su - resumo IS-IS, L1 - IS-IS nível 1, L2 - IS-IS nível 2
ia - IS-IS inter-área, * - candidato padrão, U - rota estática por usuário
H - NHRP, G - NHRP registrado, g - resumo de registro NHRP
o - ODR, P - rota estática baixada periodicamente, l - LISP
a - rota de aplicativo
+ - rota replicada, % - substituição do próximo salto, p - substituições de PfR

O Gateway de último recurso é 172.16.2.10 para a rede 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.2.10
172.16.2.0/24 tem sub-redes variáveis, 2 sub-redes, 2 máscaras
C 172.16.2.0/24 está conectado diretamente, GigabitEthernet2
L 172.16.2.2/32 está conectado diretamente, GigabitEthernet2
10.0.0.0/8 tem sub-redes variáveis, 2 sub-redes, 2 máscaras
C 10.10.10.0/24 está conectado diretamente, Tunnel0
L 10.10.10.2/32 está conectado diretamente, Tunnel0
B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:13:21
192.168.22.0/24 tem sub-redes variáveis, 2 sub-redes, 2 máscaras
C 192.168.22.0/24 está conectado diretamente, Loopback10
L 192.168.22.2/32 está conectado diretamente, Loopback10
B 192.168.33.0/24 [20/0] via 10.10.10.3, 01:12:51

Spoke1#sh ip nhrp nhs

Legenda: E=Esperando respostas, R=Respondendo, W=Aguardando, D=Dinâmico
Túnel0:
10.10.10.1 RE priority = 0 cluster = 0 **>>>>>>>>>>** Somente um servidor de próximo salto é configurado

Spoke1#sh ip nhrp traffic

Túnel0: Limite máximo de envio:10000Pacotes/10 segundos, Uso:0%
Enviado: Total 52
1 Solicitação de Resolução 0 Resposta de Resolução 51 Solicitação de Registro **<<<<<<<<**
Número de vezes que as solicitações de registro foram enviadas ao Hub
0 Resposta de Registro 0 Solicitação de Expurgação 0 Resposta de Expurgação
0 Indicação de erro 0 Indicação de tráfego 0 Supressão de redirecionamento
Rec.: Total 25
0 Solicitação de resolução 1 Resposta de resolução 0 Solicitação de registro **<<<<<<<<<<<<**
Número de vezes que recebemos respostas a essas solicitações de registro
24 Resposta de Registro 0 Solicitação de Expurgação 0 Resposta de Expurgação
0 Indicação de erro 0 Indicação de tráfego 0 Supressão de redirecionamento

Spoke1#sh ip nhrp multicast

Endereço NBMA I/F
Sinalizadores Tunnel0 172.16.1.1: static (Enabled) **<<<<<<<<<<<** O tráfego multicast é configurado para ser encaminhado para o hub NBMA

Soquetes de criptografia Spoke1#sh

Número de conexões do soquete de criptografia 2

Pares Tu0 (local/remoto): 172.16.2.2/172.16.1.1

Identificação local (endereço/máscara/porta/porta): (172.16.2.2/255.255.255.255/0/47)
Identificação remota (endereço/máscara/porta/porta): (172.16.1.1/255.255.255.255/0/47)
Perfil de IPSec: "IPSEC-IKEV2"
Estado do soquete: Abrir <<<<<<<<<<<<<<<<<<<< Status do soquete para este par em particular
Cliente: "TUNNEL SEC" (Estado do Cliente: Ativo)
Pares Tu0 (local/remoto): 172.16.2.2/172.16.3.3
Identificação local (endereço/máscara/porta/porta): (172.16.2.2/255.255.255.255/0/47)
Identificação remota (endereço/máscara/porta/porta): (172.16.3.3/255.255.255.255/0/47)
Perfil de IPSec: "IPSEC-IKEV2"
Estado do soquete: Abrir
Cliente: "TUNNEL SEC" (Estado do Cliente: Ativo)
Soquetes de criptografia no estado de escuta:
Cliente: Perfil "TUNNEL SEC": "IPSEC-IKEV2" Nome do mapa: "Tunnel0-head-0"

Spoke1#sh cry ikev2 sa

IPv4 Crypto IKEv2 SA

Status remoto FVRF/IVRF de Tunnel-id
2 172.16.2.2/500 172.16.3.3/500 nenhum/nenhum PRONTO
Encr.: AES-CBC, tamanho da chave: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Sinal de autenticação: PSK, verificação de autenticação: PSK
Vida/Tempo Ativo: 86400/287 seg

Status remoto FVRF/IVRF de Tunnel-id
1 172.16.2.2/500 172.16.1.1/500 nenhum/nenhum PRONTO
Encr.: AES-CBC, tamanho da chave: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Sinal de autenticação: PSK, verificação de autenticação: PSK
Vida/Tempo Ativo: 86400/4643 seg

IPv6 Crypto IKEv2 SA

Spoke1#traceroute 192.168.33.3 source lo10

Digite a seqüência de escape para cancelar.
Rastreando a rota para 192.168.33.3
Informações de VRF: (vrf em nome/id, vrf fora nome/id)
1 10.10.10.3 3 msec 4 msec * <<<<<<<<<<<< O tráfego vai diretamente para o roteador Spoke 2 sem passar pelo hub.

Spoke2#sh dmvpn

Legenda: Attrb —> S - Estático, D - Dinâmico, I - Incompleto
N - NATed, L - Local, X - Sem soquete
T1 - Rota Instalada, T2 - Nexthop-override
C - Compatível com CTS, I2 - Temporário

Ent —> Número de entradas NHRP com o mesmo peer NBMA
Status do NHS: E —> Esperando Respostas, R —> Respondendo, W —> Aguardando
Tempo de Atividade —> Tempo de Atividade ou Inatividade para um Túnel
==========

Interface: Detalhes de Tunnel0, IPv4 NHRP
Tipo:Spoke, NHRP Peers:2,

Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.16.1.1 10.10.10.1 ATÉ 01:20:26 S
1 172.16.2.2 10.10.10.2 ATIVIDADE 00:07:51 D

3. Comandos de verificação no spoke 2:

Spoke2#sh ip nhrp

10.10.10.1/32 via 10.10.10.1
Tunnel0 criado 01:36:06, nunca expira
Digite: static, Sinalizadores:
Endereço NBMA: 172.16.1.1
10.10.10.2/32 via 10.10.10.2
Tunnel0 criado às 00:08:09, expira às 00:01:50
Digite: dinâmico, Sinalizadores: roteador implícito
Endereço NBMA: 172.16.2.2
10.10.10.3/32 via 10.10.10.3
Tunnel0 criado às 00:08:09, expira às 00:01:50
Digite: dinâmico, Sinalizadores: local exclusivo do roteador
Endereço NBMA: 172.16.3.3
(sem soquete)
Spoke2#sh ip nhrp mul
Spoke2#sh ip nhrp multicast
Endereço NBMA I/F
Sinalizadores Tunnel0 172.16.1.1: static (Enabled)
Spoke2#

Spoke2#sh crypto sockets

Número de conexões do soquete de criptografia 2

Pares Tu0 (local/remoto): 172.16.3.3/172.16.1.1
Identificação local (endereço/máscara/porta/porta): (172.16.3.3/255.255.255.255/0/47)
Identificação remota (endereço/máscara/porta/porta): (172.16.1.1/255.255.255.255/0/47)
Perfil de IPSec: "IPSEC-IKEV2"
Estado do soquete: Abrir <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<< Status do soquete para este par em particular
Cliente: "TUNNEL SEC" (Estado do Cliente: Ativo)

Pares Tu0 (local/remoto): 172.16.3.3/172.16.2.2
Identificação local (endereço/máscara/porta/porta): (172.16.3.3/255.255.255.255/0/47)
Identificação remota (endereço/máscara/porta/porta): (172.16.2.2/255.255.255.255/0/47)
Perfil de IPSec: "IPSEC-IKEV2"
Estado do soquete: Abrir
Cliente: "TUNNEL SEC" (Estado do Cliente: Ativo)
Soquetes de criptografia no estado de escuta:
Cliente: Perfil "TUNNEL SEC": "IPSEC-IKEV2" Nome do mapa: "Tunnel0-head-0"

Spoke2#sh cry ikev2 sa

IPv4 Crypto IKEv2 SA

Status remoto FVRF/IVRF de Tunnel-id
2 172.16.3.3/500 172.16.2.2/500 nenhum/nenhum PRONTO
Encr.: AES-CBC, tamanho da chave: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Sinal de autenticação: PSK, verificação de autenticação: PSK
Vida/Tempo Ativo: 86400/509 seg

Status remoto FVRF/IVRF de Tunnel-id
1 172.16.3.3/500 172.16.1.1/500 nenhum/nenhum PRONTO
Encr.: AES-CBC, tamanho da chave: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Sinal de autenticação: PSK, verificação de autenticação: PSK
Vida/Tempo Ativo: 86400/4866 s

IPv6 Crypto IKEv2 SA

Spoke2#sh ip bgp summary

Identificador do roteador BGP 192.168.33.3, número AS local 65012
A versão da tabela de BGP é 4, a versão da tabela de roteamento principal é 4.
3 entradas de rede usando 744 bytes de memória
3 entradas de caminho usando 432 bytes de memória
3/3 entradas de atributo de caminho/melhor caminho BGP usando 864 bytes de memória
2 entradas AS-PATH BGP usando 64 bytes de memória
0 entradas de cache de mapa de rota BGP usando 0 bytes de memória
0 entradas de cache de lista de filtros BGP usando 0 bytes de memória
BGP usando 2104 bytes totais de memória
Prefixos 3/0 de atividade do BGP, caminhos 3/0, intervalo de verificação de 60 segundos
3 redes atingiram o pico às 08:16:54 jun 2 2022 UTC (01:20:43.775 atrás)

Vizinho V AS MsgRcvd MsgSent TblVer Estado Up/Down InQ OutQ/PfxRcd
10.10.10.1 465010 97 94 4 0 0 01:21:07 2 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>. Recebemos 2 prefixos do Hub, cada um para loopback de hub e loopback de Spoke2

Spoke2#sh ip route

Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvel, B - BGP

D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas
N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2
E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2, m - OMP
n - NAT, Ni - NAT interno, Não - NAT externo, Nd - NAT DIA
i - IS-IS, su - resumo IS-IS, L1 - IS-IS nível 1, L2 - IS-IS nível 2
ia - IS-IS inter-área, * - candidato padrão, U - rota estática por usuário
H - NHRP, G - NHRP registrado, g - resumo de registro NHRP
o - ODR, P - rota estática baixada periodicamente, l - LISP
a - rota de aplicativo
+ - rota replicada, % - substituição do próximo salto, p - substituições de PfR

O Gateway de último recurso é 172.16.3.10 para a rede 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.3.10
172.16.3.0/24/8 tem sub-redes variáveis, 2 sub-redes, 2 máscaras
C 172.16.3.0/24 está conectado diretamente, GigabitEthernet3
L 172.16.3.3/32 está conectado diretamente, GigabitEthernet3
10.0.0.0/8 tem sub-redes variáveis, 2 sub-redes, 2 máscaras
C 10.10.10.0/24 está conectado diretamente, Tunnel0
L 10.10.10.3/32 está conectado diretamente, Tunnel0
B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:47:08
B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:46:45
192.168.33.0/24 tem sub-redes variáveis, 2 sub-redes, 2 máscaras
C 192.168.33.0/24 está conectado diretamente, Loopback10
L 192.168.33.3/32 está conectado diretamente, Loopback10

Spoke2#sh ip route bgp

Códigos: L - local, C - conectado, S - estático, R - RIP, M - móvel, B - BGP
D - EIGRP, EX - EIGRP externo, O - OSPF, IA - OSPF entre áreas
N1 - OSPF NSSA externo tipo 1, N2 - OSPF NSSA externo tipo 2
E1 - OSPF tipo externo 1, E2 - OSPF tipo externo 2, m - OMP
n - NAT, Ni - NAT interno, Não - NAT externo, Nd - NAT DIA
i - IS-IS, su - resumo IS-IS, L1 - IS-IS nível 1, L2 - IS-IS nível 2
ia - IS-IS inter-área, * - candidato padrão, U - rota estática por usuário
H - NHRP, G - NHRP registrado, g - resumo de registro NHRP
o - ODR, P - rota estática baixada periodicamente, l - LISP
a - rota de aplicativo
+ - rota replicada, % - substituição do próximo salto, p - substituições de PfR

O Gateway de último recurso é 172.16.3.10 para a rede 0.0.0.0

B 192.168.11.0/24 [20/0] via 10.10.10.1, 01:21:11 >>>>>>>>>>>>>>>>Rede de hub acessível diretamente via hub
B 192.168.22.0/24 [20/0] via 10.10.10.2, 01:20:48 >>>>>>>>>>>>>>>> Rede spoke diretamente acessível via IP de túnel spoke.

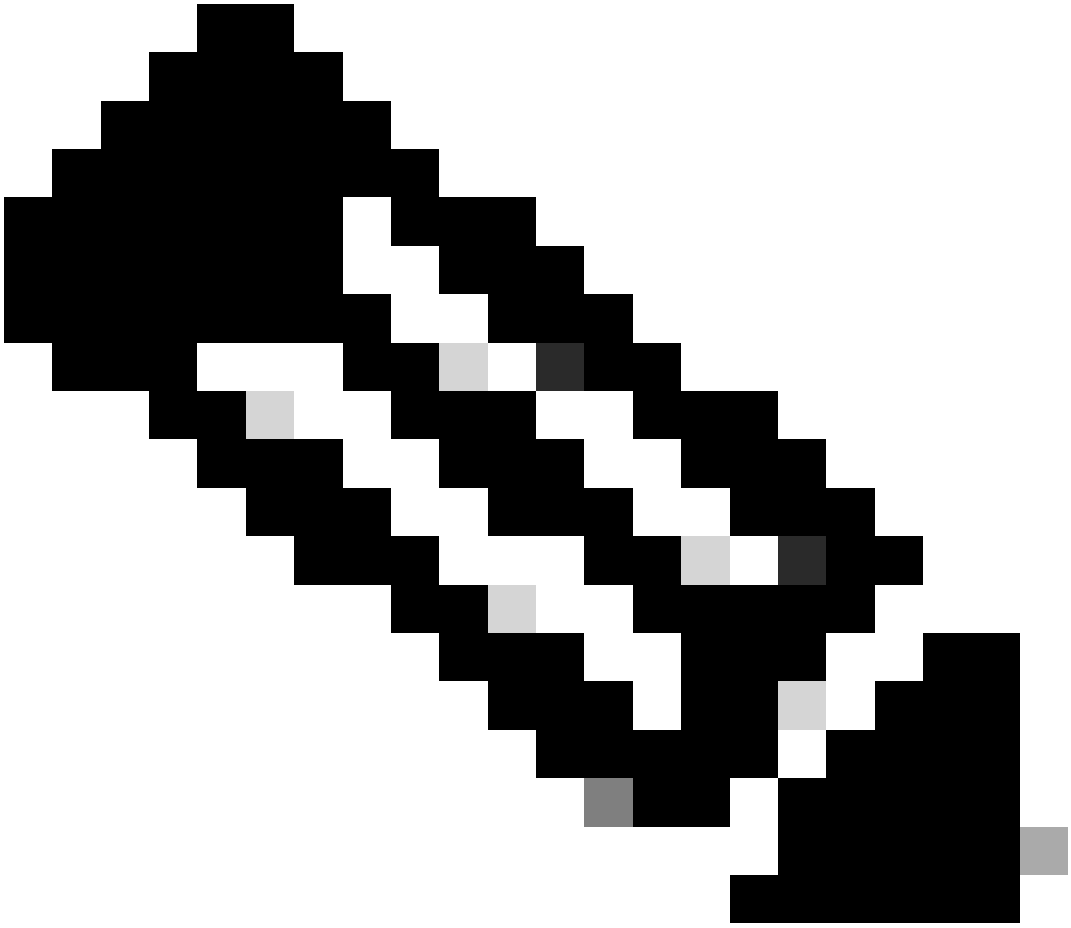
Spoke2#sh ip nhrp nhs

Legenda: E=Esperando respostas, R=Respondendo, W=Aguardando, D=Dinâmico
Túnel0:
10.10.10.10.1 RE priority = 0 cluster = 0 **>>>>>>>>>>>>>>** Somente um servidor de próximo salto é configurado

Spoke2#traceroute 192.168.22.2 loopback de origem 10

Digite a seqüência de escape para cancelar.
Rastreando a rota para 192.168.22.2
Informações de VRF: (vrf em nome/id, vrf fora nome/id)
1 10.10.10.2 4 msec 4 msec * **<<<<<<<<<<<<** O tráfego vai diretamente para o roteador Spoke 1 sem passar pelo hub.

Troubleshooting



Note: É sempre sugerido usar depurações condicionais, pois executar depurações não condicionais pode afetar o processador e, portanto, o ambiente de produção. O endereço NBMA corresponde ao "endereço IP externo" (endereço IP usado para originar a interface do túnel) e o IP do túnel corresponde ao "endereço IP lógico, isto é, o endereço IP da interface do túnel".

debug dmvpn condition peer <nmbma/tunnel> <NMBA IP or Tunnel IP address of peer>
debug crypto condition peer ipv4 <WAN IP of the Peer>
debug nhrp condition peer <nbma/tunnel> <NBMA or Tunnel IP address of Peer>

Para solucionar problemas de DMVPN, você deve adotar uma abordagem em camadas:

debug dmvpn detail all

1. Camada de criptografia: Depois de confirmar a conectividade física entre dois peers, a criptografia precisa ser verificada. Essa camada criptografa/descriptografa pacotes GRE.

Comandos de depuração comuns usados para verificar a parte de criptografia:

debug crypto condition peer ipv4 <Endereço IP WAN do Peer>

debug crypto ikev2

debug crypto ikev2 error

debug crypto ikev2 internal

debug crypto ikev2 packet

debug crypto ipsec

debug crypto ipsec error

OU

debug dmvpn condition peer <nmbma/tunnel> <NMBA IP or Tunnel IP address of peer>

debug crypto condition peer ipv4 <WAN IP of the Peer>

debug dmvpn detail crypto

Para obter uma compreensão detalhada da solução de problemas da Camada de Criptografia, consulte o link externo:

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

2. GRE/NHRP: Alguns problemas comuns incluem falhas de registro de NHRP e alterações de endereço NBMA dinâmico no spoke, levando a um mapeamento NHRP inconsistente no hub.

Comandos de depuração comuns usados para verificar o mapeamento de NHRP:

debug nhrp condition peer <nbma/tunnel> <NBMA or Tunnel IP address of Peer>

debug nhrp cache

debug nhrp packet

debug nhrp detail

debug nhrp error

Para obter informações sobre as soluções de problemas de DMVPN mais comuns, consulte o link externo:

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

3. Roteamento: O protocolo de roteamento não monitora o estado dos túneis spoke-spoke sob demanda.

As atualizações de roteamento IP e os pacotes de dados multicast IP atravessam apenas os túneis hub-and-spoke.

Os pacotes de dados IP unicast passam pelos túneis spoke-spoke hub-and-spoke e por demanda.

Debug: Vários comandos debug, dependendo do protocolo de roteamento.

Para o aprofundamento do roteamento BGP, consulte o link externo:

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

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.