# FlexVPN falou no projeto redundante do hub com um exemplo de configuração duplo da aproximação da nuvem

## Índice



## Introdução

Este documento descreve como configurar um spoke em uma rede de FlexVPN com uso do bloco da configuração de cliente de FlexVPN em uma encenação onde o Hubs múltiplo esteja disponível.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- FlexVPN
- Protocolos de roteamento de Cisco

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Roteador do serviço integrado do G2 Series de Cisco (ISR)
- Versão 15.2M do ® do Cisco IOS

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

# Configurar

Para fins de redundância, um spoke pôde precisar de conectar ao Hubs múltiplo. A Redundância no lado de raio permite a operação contínua sem um ponto de falha único no lado de hub.

Os dois projetos redundantes os mais comuns do hub de FlexVPN que usam a configuração de raio são:

- **Aproximação dupla da nuvem**, onde um spoke tem dois túneis separados ativos a ambo o Hubs em todas as vezes.
- **Aproximação do Failover**, onde um spoke tem um túnel ativo com o um hub em algum ponto dado a tempo.

Ambas as aproximações têm um conjunto exclusivo de profissionais - e - contra.

| Aproximação | Pros | Cons |
|---|---|---|
| Nuvem dupla | • Recuperação mais rápida durante a falha, com base em temporizadores do protocolo de roteamento<br>• Mais possibilties para distribuir o tráfego entre o Hubs, desde que a conexão a ambo o Hubs é ativa | • O spoke mantém a sessão a ambo o Hu ao mesmo tempo, que consome recurso ambo o Hubs |
| Failover | • Configuração fácil - construída em FlexVPN<br>• Não confia no protocolo de roteamento em uma falha | • Tempo de recuperação mais lento - bas no Dead Peer Detection (DPD) ou (opcionalmente) no Rastreamento de ob<br>• Todo o tráfego é forçado para viajar a u hub de cada vez. |

Este documento descreve a primeira aproximação. A aproximação a esta configuração é similar à configuração dupla da nuvem do Dynamic Multipoint VPN (DMVPN). A configuração básica do hub and spoke é baseada em documentos da migração do DMVPN a FlexVPN. Refira a migração de FlexVPN: Movimento duro do DMVPN a FlexVPN no mesmo artigo dos dispositivos para uma descrição desta configuração.

### Diagrama de Rede

### Rede de transporte

Este diagrama ilustra a rede de transporte básica usada tipicamente em redes de FlexVPN.

### Rede de folha de prova

O diagrama ilustra a rede de folha de prova com conectividade lógica que mostra como o Failover deve trabalhar. Durante a operação normal, Spoke1 e Spoke2 mantêm um relacionamento com ambo o Hubs. Em cima de uma falha, o protocolo de roteamento comuta de um hub a outro.

> **Note**: No diagrama, as linhas verde mostram a conexão e o sentido da versão 2 do intercâmbio de chave de Internet (as sessões IKEv2)/Flex a Hub1, e das linhas azul indicam a conexão a Hub2.

Ambo o Hubs retém o endereçamento de IP separado em nuvens da folha de prova. O endereçamento de **/24** representa o conjunto de endereço atribuído para esta nuvem, não o endereçamento real da relação. Isto é porque o hub de FlexVPN atribui tipicamente um endereço IP dinâmico para a relação do spoke, e confia nas rotas introduzidas dinamicamente através dos comandos route no bloco da autorização de FlexVPN.

## Configurações de raio

### Configuração da interface de túnel do spoke

A configuração típica usada neste exemplo é simplesmente duas interfaces de túnel com os dois endereços de destino separados.

```
interface Tunnel1
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default

interface Tunnel2
ip address negotiated
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel destination 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

A fim permitir que os túneis spoke-to-spoke formem corretamente, um molde virtual (VT) é precisado.

```
interface Virtual-Template1 type tunnel
ip unnumbered ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

O spoke usa uma interface não numerada que indique a interface de LAN no roteamento virtual e na transmissão (VRF), que é global neste caso. Contudo, pôde ser melhor prover uma interface de loopback. Isto é porque as interfaces de loopback permanecem em linha sob quase todas as circunstâncias.

### Configuração do Border Gateway Protocol (BGP) do spoke

Desde que Cisco recomenda o iBGP como o protocolo de roteamento a ser usado na rede de folha de prova, menções deste documento somente esta configuração.

> **Note**: O spokes deve reter a alcançabilidade BGP a ambo o Hubs.

```
interface Virtual-Template1 type tunnel
ip unnumbered ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

FlexVPN nesta configuração não tem um conceito preliminar ou secundário do hub. O administrador decide se o protocolo de roteamento prefere um hub sobre outro ou, em algumas encenações, executa a função de balanceamento de carga.

### Considerações do Failover e da convergência do spoke

A fim minimizar o tempo onde toma para falou para detectar a falha, usa estes dois métodos típicos.

- Encurte os temporizadores BGP. O Failover das causas do hold-time do padrão.
- Configurar o BGP queda-sobre, que discused neste artigo, suporte do BGP para a desativação rápida da sessão de peer.
- Não use a detecção bidirecional da transmissão (BFD), porque não se recomenda na maioria de disposições de FlexVPN.

### Túneis spoke-to-spoke e Failover

Interruptor spoke-to-spoke do atalho do Next Hop Resolution Protocol (NHRP) do uso dos túneis. O Cisco IOS indica que aqueles atalhos são rotas NHRP, por exemplo:

```
Spoke1#show ip route nhrp
(...)
```

```
Spoke1#show ip route nhrp
(...)
```

Aquelas rotas não expiram quando a conexão BGP expira; em lugar de, são guardados para o tempo de contenção de NHRP, que é duas horas à revelia. Isto significa que os túneis spoke-to-spoke ativos permanecem na operação mesmo em uma falha.

## Configurações do hub

### Conjuntos locais

Como discutido na seção do **diagrama da rede**, ambo o Hubs retém o endereçamento de IP separado.

Hub1

```
Spoke1#show ip route nhrp
(...)
```

Hub2

```
Spoke1#show ip route nhrp
(...)
```

### Configuração de BGP do hub

A configuração de BGP do hub permanece similar aos exemplos anteriores.

Esta saída vem de Hub1 com um endereço IP de Um ou Mais Servidores Cisco ICM NT LAN de **192.168.0.1**.

```
Spoke1#show ip route nhrp
(...)
```

```
Spoke1#show ip route nhrp
(...)
```

Essencialmente, este é o que é feito:

- O conjunto de endereços local de FlexVPN está no BGP escuta escala.
- A rede local é 192.168.0.0/24.
- Um sumário é anunciado somente ao spokes. a configuração do Agregado-endereço cria uma rota estática para esse prefixo através da relação do null0, que é uma rota rejeitada que seja usada a fim impedir loop de roteamento.
- Todos os prefixos específicos são anunciados ao outro hub. Desde que é igualmente uma conexão do iBGP, exige uma configuração do refletor de rota.

Este diagrama representa a troca de prefixos BGP entre o spokes e o Hubs em uma nuvem de FlexVPN.

> **Note**: No diagrama, a linha verde representa a informação fornecida pelo spokes ao hub, a linha vermelha representa a informação fornecida por cada hub ao spokes (um sumário somente), e a linha azul representa os prefixos trocados entre o Hubs.

# Verificar

Desde que cada spoke retém a associação com ambo o Hubs, duas sessões IKEv2 são consideradas com o comando **cripto ikev2 sa da mostra**.

```
Spoke1#show ip route nhrp
(...)

Tunnel-id Local Remote fvrf/ivrf Status
3 172.16.1.2/500 172.16.2.2/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3147 sec

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.2/500 172.25.2.1/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3256 sec
```

A fim ver a informação do protocolo de roteamento, incorpore estes comandos:

```
show bgp ipv4 unicast

show bgp summary
```

No spokes, você deve ver que o prefixo sumário está recebido do Hubs, e que as conexões a ambo o Hubs são ativas.

```
Spoke1#show bgp ipv4 unicast
BGP table version is 4, local router ID is 192.168.101.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*>i 192.168.0.0/16 10.1.1.1 0 100 0 i
* i 10.2.2.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
Spoke1#show bgp summa
Spoke1#show bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
BGP table version is 4, main routing table version 4
2 network entries using 296 bytes of memory
3 path entries using 192 bytes of memory
3/2 BGP path/bestpath attribute entries using 408 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
```

```
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 896 total bytes of memory
BGP activity 2/0 prefixes, 3/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 7 7 4 0 0 00:00:17 1
10.2.2.1 4 65001 75 72 4 0 0 01:02:24 1
```

# Troubleshooting

Há dois blocos principais a pesquisar defeitos:

- Internet Key Exchange (IKE)
- Segurança de protocolo do Internet (IPsec)

Estão aqui os comandos show relevantes:

```
show crypto ipsec sa

show crypto ikev2 sa
```

Estão aqui os comandos relevant debug:

```
debug crypto ikev2 [internal|packet]

debug crypto ipsec

debug vtemplate event
```

Está aqui o protocolo de roteamento relevante:

```
show bgp ipv4 unicast (or show ip bgp)

show bgp summary
```