Exemplo de configuração do FlexVPN Spoke no design de hub redundante com uma abordagem de nuvem dupla

Contents

Introduction

Este documento descreve como configurar um spoke em uma rede FlexVPN com o uso do bloco de configuração de cliente FlexVPN em um cenário em que vários hubs estão disponíveis.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- FlexVPN
- Protocolos de roteamento da Cisco

Componentes Utilizados

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

- Roteador de serviços integrados (ISR) Cisco G2 Series
- Cisco IOS® versão 15.2M

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Para fins de redundância, um spoke pode precisar se conectar a vários hubs. A redundância no lado do spoke permite operação contínua sem um único ponto de falha no lado do hub.

Os dois designs de hub redundante FlexVPN mais comuns que usam a configuração de spoke são:

- **Abordagem de nuvem dupla**, em que um spoke tem dois túneis separados ativos para ambos os hubs o tempo todo.
- **Abordagem de failover**, em que um spoke tem um túnel ativo com um hub em um determinado momento.

Ambas as abordagens têm um conjunto único de prós e contras.

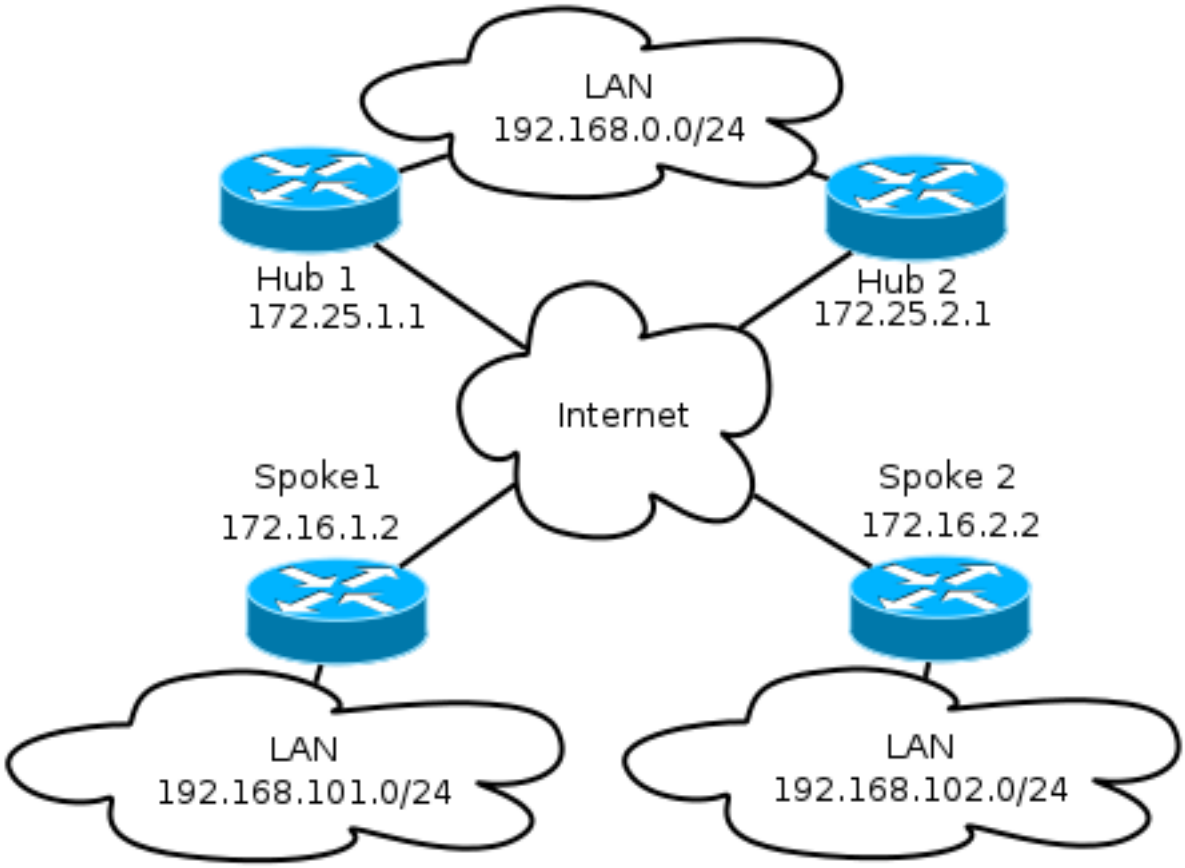
Abordagem	Pros	Cons
Nuvem dupla	• Recuperação mais rápida durante a falha, com base nos temporizadores do protocolo de roteamento • Mais possibilidades de distribuir o tráfego entre os hubs, já que a conexão com ambos os hubs está ativa	• O Spoke mantém a sessão em ambos hubs ao mesmo tempo, o que consom recursos em ambos os hubs
Failover	• Configuração fácil - integrada ao FlexVPN • Não depende do protocolo de roteamento em caso de falha	• Tempo de recuperação mais lento - co base no rastreamento de objeto Dead Detection (DPD) ou (opcional) • Todo o tráfego é forçado a viajar para hub de cada vez.

Este documento descreve a primeira abordagem. A abordagem a essa configuração é semelhante à configuração de nuvem dupla de VPN multiponto dinâmica (DMVPN). A configuração básica de hub e spoke é baseada em documentos de migração de DMVPN para FlexVPN. Consulte a Migração do FlexVPN: Hard Move from DMVPN to FlexVPN on Same Devices (Transferência forçada de DMVPN para FlexVPN nos mesmos dispositivos) para obter uma descrição dessa configuração.

Diagrama de Rede

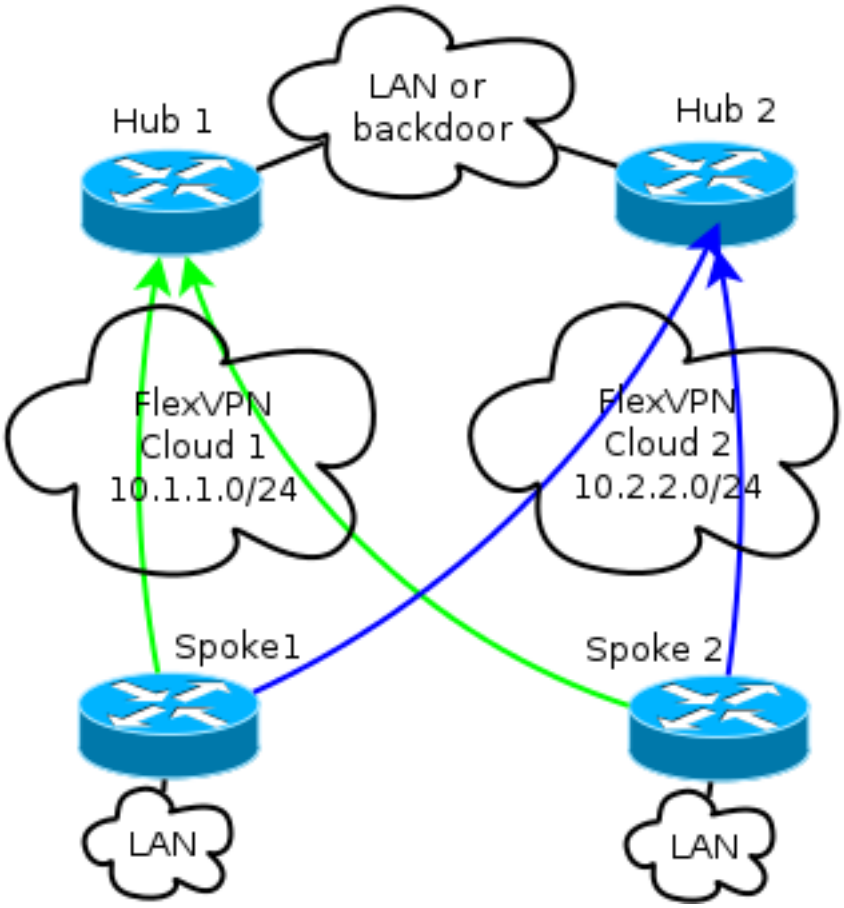
Rede de transporte

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



Sobreposição de rede

O diagrama ilustra a rede sobreposta com conectividade lógica que mostra como o failover deve funcionar. Durante a operação normal, o Spoke 1 e o Spoke 2 mantêm um relacionamento com ambos os hubs. Em caso de falha, o protocolo de roteamento muda de um hub para outro.



Note: No diagrama, as linhas verdes mostram a conexão e a direção das sessões de Internet Key Exchange Version 2 (IKEv2)/Flex para o Hub 1 e as linhas azuis indicam a conexão com o Hub 2.

Ambos os hubs retêm endereçamento IP separado em nuvens sobrepostas. O endereçamento **/24** representa o pool de endereços alocados para essa nuvem, não o endereçamento de interface real. Isso ocorre porque o hub FlexVPN normalmente aloca um endereço IP dinâmico para a interface spoke e depende de rotas inseridas dinamicamente através de comandos de rota no bloco de autorização FlexVPN.

Configurações de Spoke

Configuração de interface de túnel spoke

A configuração típica usada neste exemplo é simplesmente duas interfaces de túnel com 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
```

Para permitir que túneis spoke-to-spoke se formem corretamente, um Modelo Virtual (VT) é necessário.

```
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 indica a interface LAN no Virtual Routing and Forwarding (VRF), que é global nesse caso. No entanto, pode ser melhor referenciar uma interface de loopback. Isso ocorre porque as interfaces de loopback permanecem on-line sob quase todas as condições.

Configuração do Protocolo de Gateway de Borda de Spoke (BGP - Spoke Border Gateway Protocol)

Como a Cisco recomenda o iBGP como o protocolo de roteamento a ser usado na rede de sobreposição, este documento menciona somente esta configuração.

> **Note**: Os spokes devem manter a acessibilidade de BGP para ambos os hubs.

```
router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
neighbor 10.1.1.1 fall-over
neighbor 10.2.2.1 remote-as 65001
neighbor 10.2.2.1 fall-over
```

O FlexVPN nesta configuração não tem um conceito de hub primário ou secundário. O administrador decide se o protocolo de roteamento prefere um hub a outro ou, em alguns cenários, executa o balanceamento de carga.

Considerações sobre failover de spoke e convergência

Para minimizar o tempo que um spoke leva para detectar uma falha, use estes dois métodos

típicos.

- Reduza os temporizadores BGP. O tempo de espera padrão causa failover.
- Configure o fallover do BGP, que é discutido neste artigo, Suporte BGP para Desativação de Sessão de Peering Rápido.
- Não use a BFD (Bidirectional Forwarding Detection), pois ela não é recomendada na maioria das implantações de FlexVPN.

Túneis spoke-to-spoke e failover

Os túneis spoke-to-spoke usam switching de atalho Next Hop Resolution Protocol (NHRP). O Cisco IOS indica que esses atalhos são rotas NHRP, por exemplo:

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

192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks
H 192.168.102.0/24 [250/1] via 10.2.2.105, 00:00:21, Virtual-Access1
```

Essas rotas não expiram quando a conexão BGP expira; em vez disso, eles são mantidos para o tempo de espera do NHRP, que é de duas horas por padrão. Isso significa que os túneis spoke-to-spoke ativos permanecem em operação mesmo em uma falha.

Configurações de hub

Pools locais

Conforme discutido na seção **Diagrama de Rede**, ambos os hubs mantêm endereçamento IP separado.

Hub1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

Hub2

```
ip local pool FlexSpokes 10.2.2.100 10.2.2.254
```

Configuração do BGP do hub

A configuração do BGP do hub permanece semelhante aos exemplos anteriores.

Esta saída vem do Hub 1 com um endereço IP de LAN de **192.168.0.1**.

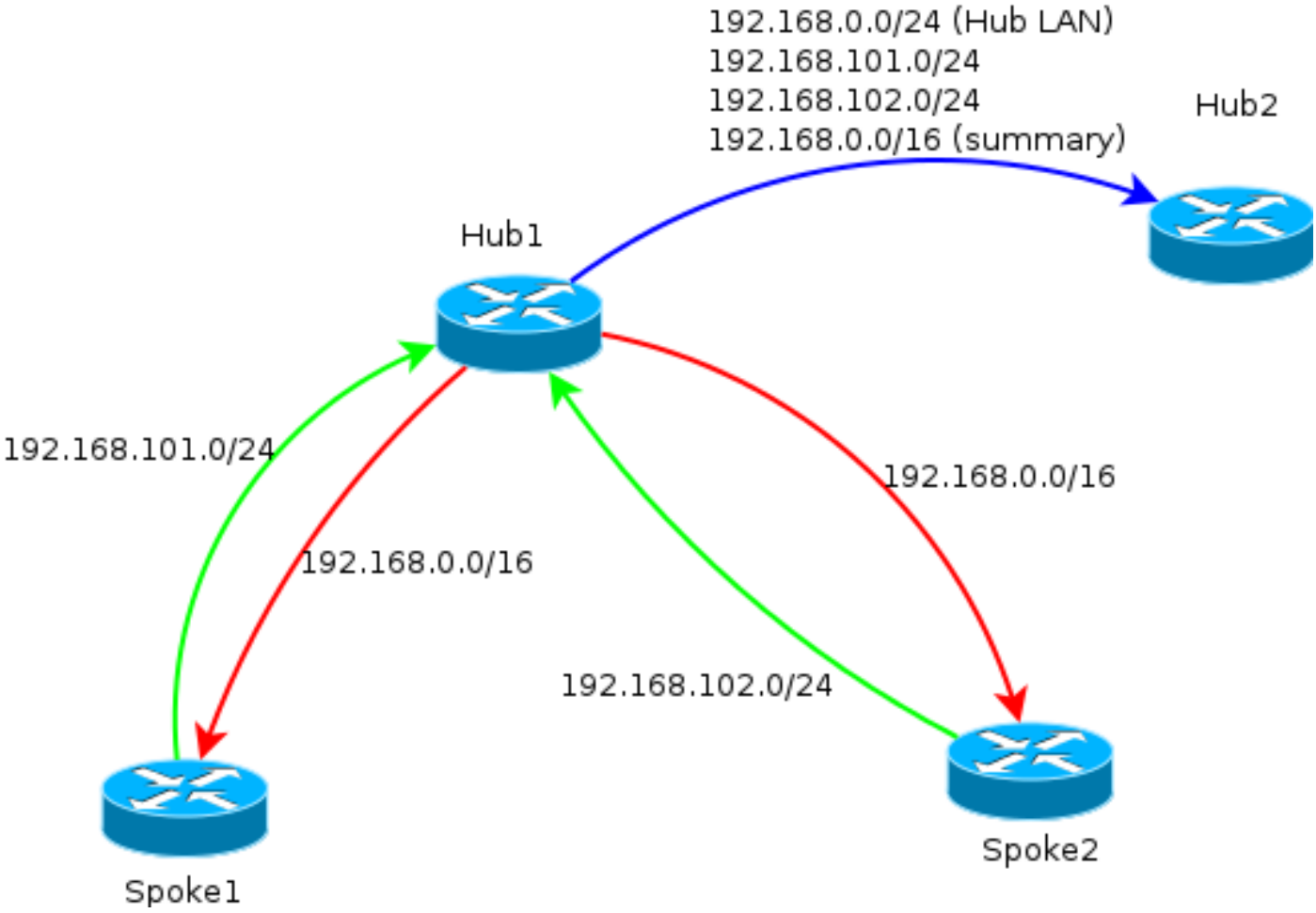
```
router bgp 65001
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
aggregate-address 192.168.0.0 255.255.0.0 summary-only
neighbor Spokes peer-group
```

```
neighbor Spokes remote-as 65001
neighbor Spokes fall-over
neighbor 192.168.0.2 remote-as 65001
neighbor 192.168.0.2 route-reflector-client
neighbor 192.168.0.2 next-hop-self all
neighbor 192.168.0.2 unsuppress-map ALL

route-map ALL permit 10
match ip address 1

ip access-list standard 1
permit any
```

Essencialmente, é isso que se faz:

- O pool de endereços FlexVPN local está no intervalo de escuta BGP.
- A rede local é 192.168.0.0/24.
- Um resumo é anunciado somente para spokes. A configuração de endereço agregado cria uma rota estática para esse prefixo através da interface null0, que é uma rota de descarte usada para evitar loops de roteamento.
- Todos os prefixos específicos são anunciados para o outro hub. Como também é uma conexão iBGP, ela requer uma configuração de refletor de rota.

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



Note: No diagrama, a linha verde representa as informações fornecidas pelos spokes para o hub, a linha vermelha representa as informações fornecidas por cada hub para os spokes (apenas um resumo) e a linha azul representa prefixos trocados entre os hubs.

Verificar

Como cada spoke retém associação com ambos os hubs, duas sessões IKEv2 são vistas com o comando **show crypto ikev2 sa**.

```
IPv4 Crypto IKEv2 SA

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
```

Para visualizar as informações do protocolo de roteamento, insira estes comandos:

show bgp ipv4 unicast

show bgp summary

Nos spokes, você deve ver que o prefixo de resumo é recebido dos hubs e que as conexões aos dois hubs estão 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
```

Troubleshoot

Há dois blocos principais para solucionar problemas:

- Internet Key Exchange (IKE)
- Internet Protocol Security (IPsec)

Aqui estão os comandos show relevantes:

```
show crypto ipsec sa

show crypto ikev2 sa
```

Aqui estão os comandos debug relevantes:

```
debug crypto ikev2 [internal|packet]

debug crypto ipsec

debug vtemplate event
```

Este é o protocolo de roteamento relevante:

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

show bgp summary
```