Exemplo de configuração de spoke FlexVPN no design de hub redundante com bloco de cliente FlexVPN

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.

Informações de Apoio

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 em uma falha, com base nos temporizadores do protocolo de roteamento • Mais possibilidades de distribuir tráfego entre os hubs, já que as conexões a ambos os hubs estão ativas	• 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 segunda abordagem.

Configurar

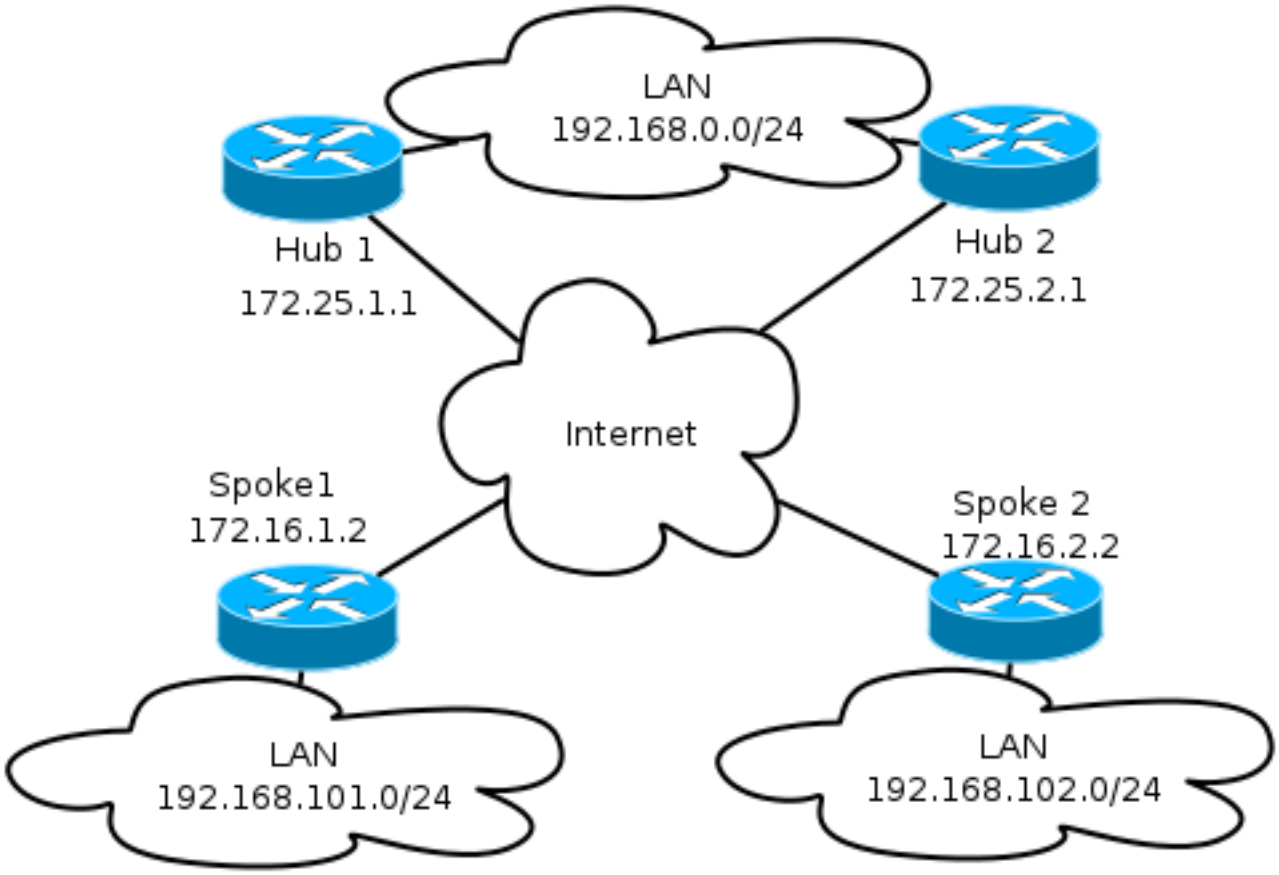
Note: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagramas de rede

Esses diagramas mostram os diagramas de topologia de transporte e de sobreposição.

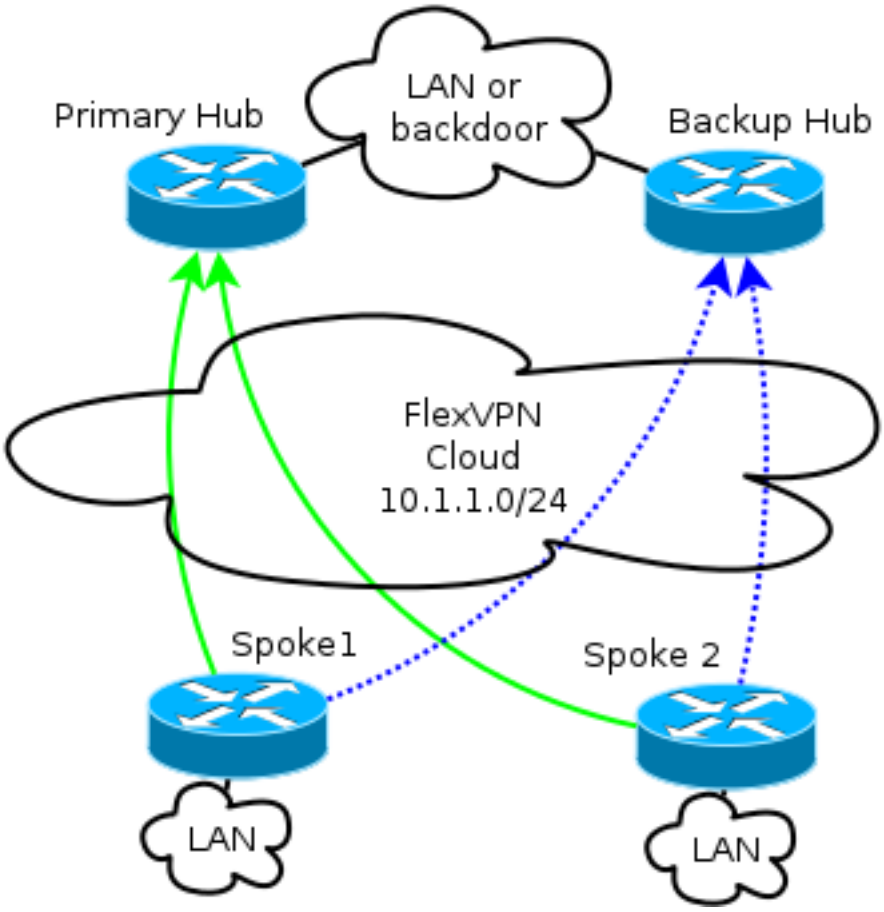
Rede de transporte

Este diagrama ilustra a rede de transporte básica que é normalmente usada em redes FlexVPN.



Sobreposição de rede

Este 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 apenas com um hub.



Note: No diagrama, as linhas verdes sólidas mostram a conexão e a direção das sessões primárias do Internet Key Exchange Version 2 (IKEv2)/Flex e as linhas azuis pontilhadas indicam a conexão de backup caso a sessão do Internet Key Exchange (IKE) para o hub principal falhe.

O endereçamento **/24** representa o pool de endereços alocados para essa nuvem, e não o endereçamento real da interface. 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.

Configuração básica de spoke e hub

A configuração básica do hub e do spoke é baseada em documentos de migração do Dynamic Multipoint VPN (DMVPN) para FlexVPN. Essa configuração é descrita na [Migração do FlexVPN: Artigo Hard Move from DMVPN to FlexVPN on Same Devices (Movimentação forçada do DMVPN para o FlexVPN nos mesmos dispositivos)](#).

Ajuste de configuração de spoke

Configuração de Spoke - Bloco de Configuração do Cliente

A configuração de spoke deve ser estendida pelo bloco de configuração do cliente.

Na configuração básica, vários peers são especificados. O peer com a maior preferência (número mais baixo) é considerado antes de outros.

```
crypto ikev2 client flexvpn Flex_Client
peer 1 172.25.1.1
peer 2 172.25.2.1
client connect Tunnel1
```

A configuração do túnel deve ser alterada para permitir que o destino do túnel seja escolhido dinamicamente, com base no bloco de configuração do cliente FlexVPN.

```
interface Tunnel1
 tunnel destination dynamic
```

Écrucial lembrar que o bloco de configuração do cliente FlexVPN está vinculado a uma interface, e não ao IKEv2 ou ao perfil de Segurança de Protocolo Internet (IPsec).

O bloco de configuração do cliente fornece várias opções para ajustar o tempo de failover e as operações, que incluem o rastreamento do uso de objetos, backup de discagem e funcionalidades de grupos de backup.

Com a configuração básica, o spoke confia em DPDs para detectar se um spoke não responde e dispara uma alteração quando o peer é declarado morto. A opção de usar DPD não é rápida, por causa de como os DPDs funcionam. Um administrador pode querer aprimorar a configuração com rastreamento de objeto ou aprimoramentos semelhantes.

Para obter mais informações, consulte o capítulo **Configuração do Cliente FlexVPN** do guia de configuração do Cisco IOS, que está vinculado na seção **Informações Relacionadas** no final deste documento.

Configuração completa de spoke - referência

```
crypto logging session

crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco

crypto ikev2 profile Flex_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
 aaa authorization group psk list default default
 virtual-template 1

crypto ikev2 dpd 30 5 on-demand

crypto ikev2 client flexvpn Flex_Client
 peer 1 172.25.1.1
 peer 2 172.25.2.1
 client connect Tunnel1
```

```
crypto ipsec transform-set IKEv2 esp-gcm
 mode transport

crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

interface Tunnel1
 description FlexVPN tunnel
 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
 delay 2000
 tunnel source Ethernet0/0
 tunnel destination dynamic
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
```

Configuração do hub

Embora a maioria da configuração do hub permaneça a mesma, vários aspectos devem ser abordados. A maioria deles está relacionada a uma situação em que um ou mais spokes estão conectados a um hub, enquanto outros permanecem em relação a outro hub.

Endereços spoke

Como os spokes obtêm endereços IP de hubs, normalmente se deseja que os hubs atribuam endereços de sub-redes diferentes ou de uma parte diferente de uma sub-rede.

Por exemplo:

Hub1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.175
```

Hub2

```
ip local pool FlexSpokes 10.1.1.176 10.1.1.254
```

Isso evita a criação de sobreposição, mesmo que os endereços não sejam roteados para fora da nuvem FlexVPN, o que pode prejudicar a solução de problemas.

Endereço de sobreposição de hub

Ambos os hubs podem manter o mesmo endereço IP em uma interface de modelo virtual; no entanto, isso pode afetar a solução de problemas em alguns casos. Essa escolha de design facilita a implantação e o planejamento, já que o spoke deve ter apenas um endereço de peer para o Border Gateway Protocol (BGP).

Em alguns casos, ele pode não ser desejado ou necessário.

Roteamento

Énecessário que os hubs troquem informações sobre os spokes conectados.

Os hubs devem ser capazes de trocar as rotas específicas dos dispositivos conectados e ainda fornecer um resumo dos spokes.

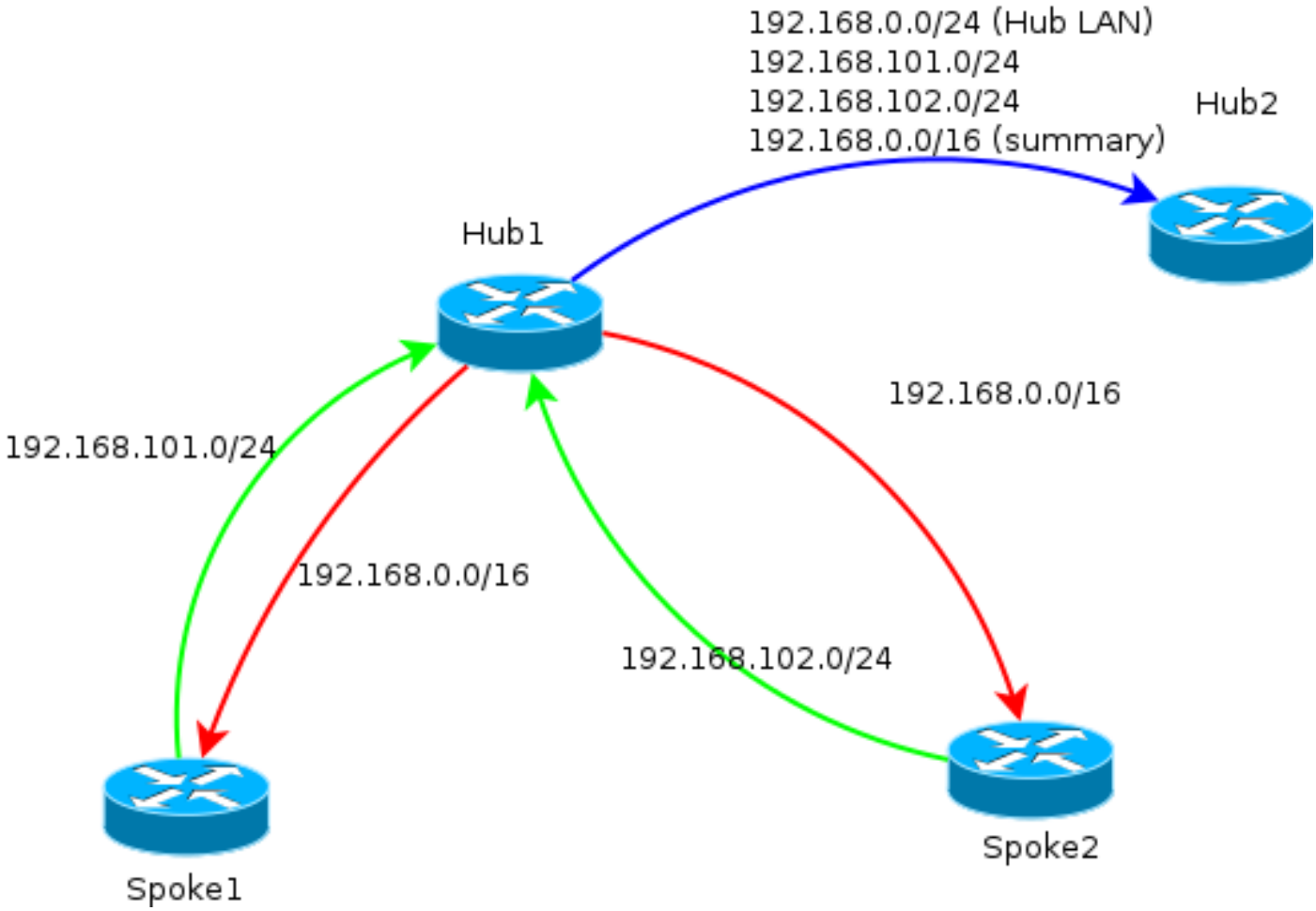
Como a Cisco recomenda que você use o iBGP com FlexVPN e DMVPN, somente esse protocolo de roteamento é mostrado.

```
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
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

access-list 1 permit any

route-map ALL permit 10
match ip address 1
```

Essa configuração permite:

- Ouvinte dinâmico de endereços atribuídos a spokes
- Rede de publicidade de 192.168.0.0/24
- Rota resumida de anúncios de 192.168.0.0/16 para todos os spokes. A configuração aggregate-address cria uma rota estática para esse prefixo por meio da interface null0, que é uma rota de descarte usada para evitar loops de roteamento.
- Encaminhamento de prefixos específicos para o outro hub
- Cliente refletor de rota para garantir que os hubs trocam informações aprendidas de spokes entre si

Este diagrama representa a troca de prefixos no BGP nesta configuração, da perspectiva de um dos hubs.



Note: Neste 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 os prefixos trocados entre os hubs.

Os resumos de rede usam

Os resumos podem não ser aplicáveis ou desejados em alguns cenários. Tenha cuidado ao designar o IP de destino em prefixos, pois o iBGP não substitui o salto seguinte por padrão.

Os resumos são recomendados em redes que mudam de estado frequentemente. Por exemplo, conexões instáveis com a Internet podem exigir resumos para: evite a remoção e a adição de prefixos, limite o número de atualizações e permita que a maioria das configurações seja dimensionada corretamente.

Túneis spoke-to-spoke

No cenário e na configuração mencionados na seção anterior, os spokes em diferentes hubs não conseguem estabelecer túneis spoke-to-spoke diretos. O tráfego entre spokes conectados a hubs diferentes flui sobre os dispositivos centrais.

Há uma solução fácil para isso. No entanto, exige que o Next Hop Resolution Protocol (NHRP) com o mesmo ID de rede esteja ativado entre os hubs. Isso pode ser feito, por exemplo, se você criar um túnel GRE (Generic Routing Encapsulation) ponto a ponto entre os hubs. Em seguida, o

IPsec não é necessário.

Verificar

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

O comando **show crypto ikev2 sa** informa sobre onde o spoke está conectado no momento.

O comando **show crypto ikev2 client flexvpn** permite que um administrador compreenda o estado atual da operação do cliente FlexVPN.

```
Spoke2# show crypto ikev2 client flexvpn

Profile : Flex_Client
Current state:ACTIVE
Peer : 172.25.1.1
Source : Ethernet0/0
ivrf : IP DEFAULT
fvrf : IP DEFAULT
Backup group: Default
Tunnel interface : Tunnel1
Assigned IP address: 10.1.1.111
```

Um failover bem-sucedido com o comando **show logging** configuration registra essa saída no dispositivo spoke:

```
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is DOWN.  Peer 172.25.1.1:500
Id: 172.25.1.1
%FLEXVPN-6-FLEXVPN_CONNECTION_DOWN: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.1.1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.  Peer 172.25.2.1:500
Id: 172.25.2.1
%FLEXVPN-6-FLEXVPN_CONNECTION_UP: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.2.1 Assigned_Tunnel_v4_addr = 10.1.1.177
```

Nesta saída, o spoke desconecta do **hub 172.25.1.1**, o bloco de configuração do cliente Flex_Client detecta falha e força uma conexão com **172.25.2.1** onde um túnel é ativado, e um spoke recebe um IP de **10.1.1.177**.

Troubleshoot

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

> **Note**: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.**

Aqui estão os comandos debug relevantes:

- **debug crypto ikev2**
- **debug radius**

Informações Relacionadas

- Guia de configuração do FlexVPN e Internet Key Exchange versão 2, Cisco IOS versão 15 M&T
- Suporte Técnico e Documentação - Cisco Systems