

FlexVPN falou no projeto redundante do hub com o exemplo de configuração do bloco do cliente de FlexVPN

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagramas da rede](#)

[Rede de transporte](#)

[Rede de folha de prova](#)

[Configuração básica do spoke e do hub](#)

[Ajuste da configuração de raio](#)

[Configuração de raio - Bloco da configuração de cliente](#)

[Configuração de raio completa - Referência](#)

[Configuração do hub](#)

[Endereços do spoke](#)

[Endereço da folha de prova do hub](#)

[Roteamento](#)

[Uso dos sumários da rede](#)

[Túneis spoke-to-spoke](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

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.

Informações de Apoio

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

- | | |
|-------------|--|
| | <ul style="list-style-type: none">• Recuperação mais rápida em uma falha, com base em temporizadores do protocolo de roteamento• Mais possibilidades para distribuir o tráfego entre o Hubs, desde que as conexões a ambo o Hubs são ativas |
| Nuvem dupla | |
| Failover | <ul style="list-style-type: none">• Configuração fácil - construída em FlexVPN• Não confia no protocolo de roteamento em uma falha |

Cons

- O spoke mantém a sessão a ambo o Hubs ao mesmo tempo, que consome recursos em ambo o Hubs
- Tempo de recuperação mais lento - baseado no Dead Peer Detection (DPD) (opcionalmente) no Rastreamento de objetos
- Todo o tráfego é forçado para viajar a hub de cada vez

Este documento descreve a segunda aproximação.

Configurar

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

Diagramas da rede

Estes diagramas mostram o transporte e os diagramas de topologia da folha de prova.

Rede de transporte

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

Rede de folha de prova

Este 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 um hub somente.

Note: No diagrama, as linhas verde contínuas mostram a conexão e o sentido da versão 2 preliminar do intercâmbio de chave de Internet (as sessões IKEv2)/Flex, e das linhas azul pontilhadas indicam a conexão de backup se a sessão do Internet Key Exchange (IKE) à falha preliminar do hub.

O endereçamento de **/24** representa o conjunto de endereço atribuído para esta nuvem, e 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.

Configuração básica do spoke e do hub

A configuração básica do hub and spoke é baseada em documentos da migração do Dynamic Multipoint VPN (DMVPN) a FlexVPN. Esta configuração é descrita na [migração de FlexVPN: Movimento duro do DMVPN a FlexVPN no mesmo](#) artigo dos [dispositivos](#).

Ajuste da configuração de raio

Configuração de raio - Bloco da configuração de cliente

A configuração de raio deve ser estendida pelo bloco da configuração de cliente.

Na configuração básica, os peer múltiplos são especificados. O par com a preferência mais elevada (o mais baixo número) é considerado antes de outro.

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

A configuração de túnel deve mudar a fim permitir que o destino de túnel seja escolhido dinamicamente, com base no bloco da configuração de cliente de FlexVPN.

```
interface Tunnell
 tunnel destination dynamic
```

É crucial recordar que o bloco da configuração de cliente de FlexVPN está amarrado a uma relação, e não a IKEv2 ou ao perfil da segurança de protocolo do Internet (IPsec).

O bloco da configuração de cliente fornece as opções múltiplas a fim ajustar o tempo e as operações do Failover, que incluem o seguimento do uso dos objetos, do Dial backup, e das funcionalidades dos grupos do backup.

Com configuração básica, o spoke confia em DPD a fim detectar se um spoke é sem resposta, e provoca uma mudança uma vez que o par é declarado absolutamente. A opção para usar o DPD não é rápida, devido a como os DPD trabalham. Um administrador pôde querer aumentar a configuração com Rastreamento de objetos ou realces similares.

Para mais informação, refira o capítulo da **configuração de cliente de FlexVPN** do guia de configuração do IOS da Cisco, que é ligado na **seção Informação Relacionada** na extremidade deste documento.

Configuração de raio completa - Referência

```
interface Tunnell
 tunnel destination dynamic
```

Configuração do hub

Quando a maioria da configuração do hub permanecer a mesma, diversos aspectos devem ser endereçados. A maioria deles referem-se uma situação em qual ou mais spokes estão conectados a um hub, quando outro permanecer no relacionamento a um outro hub.

Endereços do spoke

Desde que o spokes obtém endereços IP de Um ou Mais Servidores Cisco ICM NT do Hubs, deseja-se normalmente que o Hubs atribua endereços das sub-redes diferentes ou de um diferente parte de uma sub-rede.

Por exemplo:

Hub1

```
interface Tunnell
 tunnel destination dynamic
```

Hub2

```
interface Tunnell
 tunnel destination dynamic
```

Isto impede a criação da sobreposição, mesmo se os endereços não são distribuídos fora da nuvem de FlexVPN, que pôde danificar o Troubleshooting.

Endereço da folha de prova do hub

Ambo o Hubs pode reter o mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT em uma interface de molde virtual; contudo, isto pode impactar a pesquisa de defeitos em alguns casos. Esta escolha do projeto facilita distribuir e planejar, desde que o spoke deve ter somente um endereço de peer para o Border Gateway Protocol (BGP).

Em alguns casos, não pôde ser desejada ou precisado.

Roteamento

Énecessário que o Hubs troque a informação sobre o spokes que é conectado.

O Hubs deve poder trocar as rotas específicas dos dispositivos que conectou, e fornecer ainda um sumário ao spokes.

Desde que Cisco recomenda que você usa o iBGP com FlexVPN e DMVPN, simplesmente esse protocolo de roteamento é mostrado.

```
interface Tunnell
 tunnel destination dynamic
```

```
interface Tunnell
 tunnel destination dynamic
```

Esta configuração reserva:

- Ouvinte dinâmico dos endereços atribuídos ao spokes
- Anunciando uma rede de **192.168.0.0/24**
- Anunciando uma rota sumária de **192.168.0.0/16** a todo o 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.
- Transmissão de prefixos específicos ao outro hub
- Cliente de refletor da rota para certificar-se de que o Hubs troca a informação aprendida do spokes entre se

Este diagrama representa a troca do prefixo no BGP nesta instalação, da perspectiva de um do Hubs.

Note: Neste 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.

Uso dos sumários da rede

Os sumários não puderam ser aplicáveis ou desejados em algumas encenações. Use o cuidado quando você designa o IP de destino nos prefixos, porque o iBGP não cancela o salto seguinte à revelia.

Os sumários são recomendados nas redes que mudam o estado frequentemente. Por exemplo, as conexões com o Internet instáveis puderam exigir sumários: evite a remoção e a adição de prefixos, limite o número de atualizações, e permita que a maioria de instalações escalem corretamente.

Túneis spoke-to-spoke

Na encenação e na configuração mencionadas na seção anterior, o spokes no Hubs diferente não pode estabelecer túneis spoke-to-spoke diretos. O tráfego entre o spokes conectado ao Hubs diferente flui sobre os dispositivos centrais.

Há uma ação alternativa fácil para esta. Contudo, exige que o Next Hop Resolution Protocol (NHRP) com o mesmo rede-ID está permitido entre o Hubs. Isto pode ser conseguido, por exemplo, se você cria um túnel de encapsulamento de roteamento genérico (GRE) ponto a ponto entre o Hubs. Então, o IPsec não é exigido.

Verificar

[A ferramenta Output Interpreter](#) ([clientes registrados somente](#)) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

O comando **cripto ikev2 sa da mostra** informa-o sobre onde o spoke é conectado atualmente.

O comando **cripto do flexvpn do cliente ikev2 da mostra** permite que um administrador compreenda o estado atual da operação de cliente de FlexVPN.

```
Spoke2# show crypto ikev2 client flexvpn
```

```
Spoke2# show crypto ikev2 client flexvpn
```

Um failover bem-sucedido com a **configuração de registro da mostra** registra esta saída no dispositivo do spoke:

```
Spoke2# show crypto ikev2 client flexvpn
```

Nesta saída, as desconexões do spoke do **hub 172.25.1.1**, o bloco da configuração de cliente de Flex_Client detectam a falha e forçam uma conexão a **172.25.2.1** aonde um túnel vem acima, e um spoke é atribuído um IP de **10.1.1.177**.

Troubleshooting

[A ferramenta Output Interpreter \(clientes registrados somente\)](#) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Note: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

Estão aqui os comandos relevant debug:

- debug crypto ikev2
- debug radius

Informações Relacionadas

- [FlexVPN e manual de configuração da versão 2 do intercâmbio de chave de Internet, Cisco IOS Release 15 M&T](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)