Configurar e verificar a solução FlexVPN

Contents

Introdução

Este documento descreve o ambiente Flex Virtual Private Network, apresenta seus recursos e explica como configurar cada topologia FlexVPN.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco IOS e Cisco IOS XE
- Internet Key Exchange (IKE) versão 2
- Segurança de Protocolo Internet (IPsec)
- FlexVPN

Componentes Utilizados

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

- Cisco IOS XE Amsterdam-17.3.6

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 FlexVPN é uma solução VPN versátil e abrangente fornecida pela Cisco, projetada para oferecer uma estrutura unificada para vários tipos de conexões VPN. Desenvolvido com base no protocolo IKEv2 (Internet Key Exchange versão 2), o FlexVPN foi projetado para simplificar a configuração, o gerenciamento e a implantação da VPN, aproveitando um conjunto consistente de ferramentas, os mesmos comandos e etapas de configuração se aplicam a diferentes tipos de VPN (site a site, acesso remoto e assim por diante). Essa consistência ajuda a reduzir erros e torna o processo de implantação mais intuitivo.

IKEV2 VS IKEV1

O FlexVPN aproveita o IKEv2, que suporta algoritmos criptográficos modernos como AES (Advanced Encryption Standard) e SHA-256 (Secure Hash Algorithm). Esses algoritmos fornecem criptografia forte e integridade de dados, protegendo os dados transmitidos pela VPN contra interceptação ou adulteração.

O IKEv2 oferece mais métodos de autenticação em comparação ao IKEv1. Além da Chave Pré-Compartilhada (PSK) e dos tipos de autenticação híbrida e baseada em certificado, o IKEv2 permite que o respondente utilize o Protocolo de Autenticação Extensível (EAP) para a autenticação do cliente.

No FlexVPN, o EAP é usado para a autenticação do cliente, o roteador atua como um relay, passando mensagens EAP entre o cliente e o servidor EAP de back-end, normalmente um servidor RADIUS. O FlexVPN suporta vários métodos EAP, incluindo EAP-TLS, EAP-PEAP, EAP-PSK e outros, para proteger o processo de autenticação.

A tabela mostra as diferenças entre as funções IKEv1 e IKEv2:

	IKEv2	IKEv1
Mensagens de estabelecimento	4 mensagem	6 mensagem

de protocolo		
Suporte a EAP	Sim (2 mensagens extras)	No
Negociação para associações de segurança	2 mensagens extras	3 mensagem extra
Executar sobre UDP 500/4500	Yes	Yes
NAT Traversal (NAT-T)	Yes	Yes
Funções de retransmissão e confirmação	Yes	Yes
Fornece proteção de identidade, um mecanismo de proteção contra DoS e Perfect Forward Secrecy (PFS)	Yes	Yes
Suporte a cifras de próxima geração	Yes	No

Escalabilidade

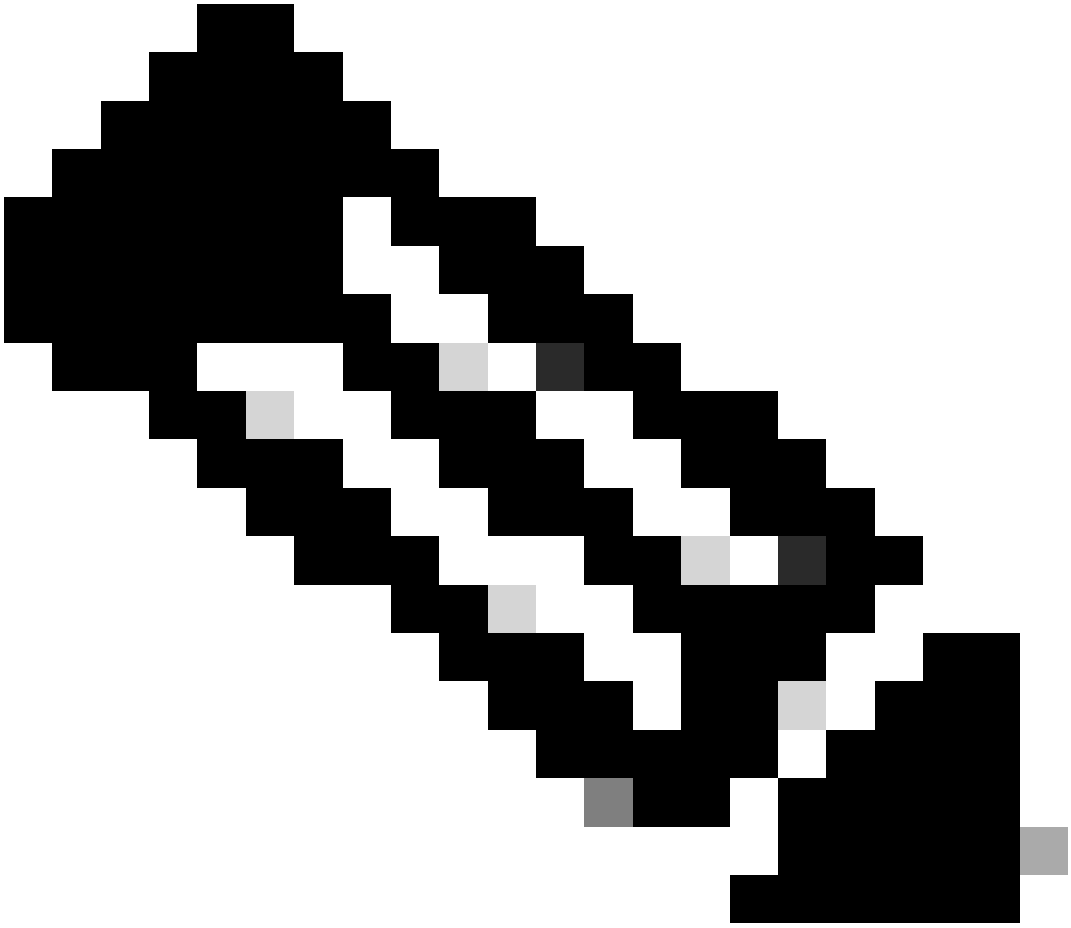
A FlexVPN pode ser facilmente expandida de pequenos escritórios para redes de grandes empresas. Isso o torna a escolha ideal para empresas com um número significativo de usuários remotos que exigem acesso seguro e confiável à rede.

Recursos Principais

- Configuração dinâmica e túneis sob demanda:
  - A conexão FlexVPN é iniciada, o sistema gera uma interface de acesso virtual com base em um modelo pré-configurado. Essa interface atua como o ponto final do túnel durante a conexão. Quando o túnel não for mais necessário, a interface de acesso virtual será desativada, liberando os recursos do sistema.

- Flexibilidade na implantação:
  - Modelo Hub-and-Spoke: Um hub central se conecta a várias filiais. O FlexVPN simplifica a configuração dessas conexões com uma única estrutura, tornando-a ideal para redes grandes.
  - Topologias de malha completa e de malha parcial: Todos os locais podem se comunicar diretamente sem passar por um hub central, reduzindo o atraso e melhorando o desempenho.

- Alta disponibilidade e redundância:
  - Hubs redundantes: Oferece suporte a vários hubs para backup. Se um hub falhar, as filiais podem se conectar a outro hub, garantindo conectividade contínua.
  - Balanceamento de carga: Isso distribui conexões VPN em vários dispositivos para evitar que um único dispositivo fique sobrecarregado, o que é crucial para manter o desempenho em grandes implantações.



Note: O próximo guia fornece mais informações sobre a configuração do balanceamento de carga para a conexão de Hubs.

Configurando o Balanceador de Carga IKEv2

- Autenticação e autorização escaláveis:
  - Integração AAA: Funciona com servidores AAA, como Cisco ISE ou RADIUS, para o gerenciamento centralizado de credenciais e políticas de usuário, essenciais para o uso em larga escala.
  - PKI e certificados: Suporta Public Key Infrastructure (PKI) e certificados digitais para autenticação segura, que é mais escalável do que usar chave pré-compartilhada, especialmente em grandes ambientes.

Roteamento

A funcionalidade de roteamento no FlexVPN foi projetada para aprimorar a escalabilidade e para gerenciar com eficiência várias conexões VPN e permitir uma maneira dinâmica de rotear o

tráfego para cada uma delas. Os próximos componentes e mecanismos principais que tornam o roteamento FlexVPN eficiente:

- Interface de Modelo Virtual: Este é um modelo de configuração que inclui todas as configurações necessárias para uma conexão VPN, como atribuição de endereço IP, origem do túnel e configurações de IPsec. Nessa interface, é configurado o comando`ip unnumbered`para emprestar um endereço IP, normalmente de um loopback, em vez de configurar um endereço IP específico como origem do túnel. Isso permite que o mesmo modelo seja usado por cada spoke, permitindo que cada spoke use seu próprio endereço IP de origem.

- Interface de acesso virtual: Essas são interfaces criadas dinamicamente que herdam suas configurações da interface do modelo virtual. Cada vez que uma nova conexão VPN é estabelecida, uma nova interface de acesso virtual é criada com base no modelo virtual. Isso significa que cada sessão VPN tem sua própria interface exclusiva, o que simplifica o gerenciamento e o dimensionamento.

- Protocolos de roteamento dinâmico: Ele funciona com protocolos de roteamento como OSPF, EIGRP e BGP sobre túneis VPN. Isso mantém as informações de roteamento atualizadas automaticamente, o que é importante para redes grandes e dinâmicas.

- O IKEv2 anuncia rotas permitindo que o servidor FlexVPN envie atributos de rede para o cliente, que instala essas rotas na interface do túnel. O cliente também comunica suas próprias redes ao servidor durante a troca do modo de configuração, permitindo atualizações de rotas em ambas as extremidades.

- O NHRP (Next Hop Resolution Protocol) é um protocolo de resolução de endereços dinâmico usado em topologias de hub e spoke para mapear endereços IP públicos para terminais VPN privados. Ele permite que os spokes descubram outros IPs de spokes para comunicação direta.

Política de Autorização

Uma política de autorização IKEv2 para FlexVPN pode ser configurada para controlar vários aspectos da conexão VPN. Uma política de autorização IKEv2 define a política de autorização local e contém atributos locais e/ou remotos:

- Atributos locais, como roteamento e encaminhamento de VPN (VRF) e a política de QOS, são aplicados localmente.
- Atributos remotos, como rotas, são enviados para o peer por meio do modo de configuração.
- Use o comando crypto ikev2 authorization policy para definir a política local.
- A política de autorização IKEv2 é referenciada do perfil IKEv2 através do comando AAA authorization.

Esta tabela fornece uma visão geral dos parâmetros-chave que podem ser configurados sob a política de autorização IKEv2.

Parâmetro	Descrição

AAA	Integração com servidores AAA para validar credenciais de usuário, autorizar acesso e conta para uso. A política pode especificar se a validação é feita localmente no roteador ou remotamente, por meio de um servidor RADIUS.
Configuração do Cliente	Envia definições de configuração para o cliente, como valores de tempo limite ocioso, keepalives, atribuição de servidor DNS e WINS, etc.
Configuração específica do cliente	Permite configurações diferentes para clientes diferentes com base em sua identidade ou associação de grupo.
Conjunto de rotas	Essa configuração permite que determinado tráfego passe pelo túnel VPN. Isso executa a injeção de rota que é enviada para o cliente VPN em uma conexão bem-sucedida.

FlexVPN versus outras tecnologias

A FlexVPN oferece uma variedade de benefícios que a tornam uma opção atraente para ambientes de rede modernos. Ao fornecer uma estrutura unificada, o FlexVPN simplifica a configuração e o gerenciamento, melhora a segurança, suporta escalabilidade, garante interoperabilidade e reduz a complexidade.

	Mapa de Criptografia	DMVPN	FlexVPN
Roteamento dinâmico	No	Yes	Yes
Direto spoke-to-spoke dinâmico	No	Yes	Yes
VPN de acesso remoto	Yes	No	Yes
Envio de configuração	No	No	Yes
Configuração Ponto a Ponto	No	No	Yes
Qos peer-peer	No	Yes	Yes
Integração de servidor AAA	No	No	Yes

Diagrama de Rede

O FlexVPN permite a criação de túneis entre dispositivos, estabelecendo a comunicação entre o hub e os spokes. Ele também permite a criação de túneis para comunicação direta entre os spokes e conexão para usuários de VPN de acesso remoto, como mostrado no diagrama.

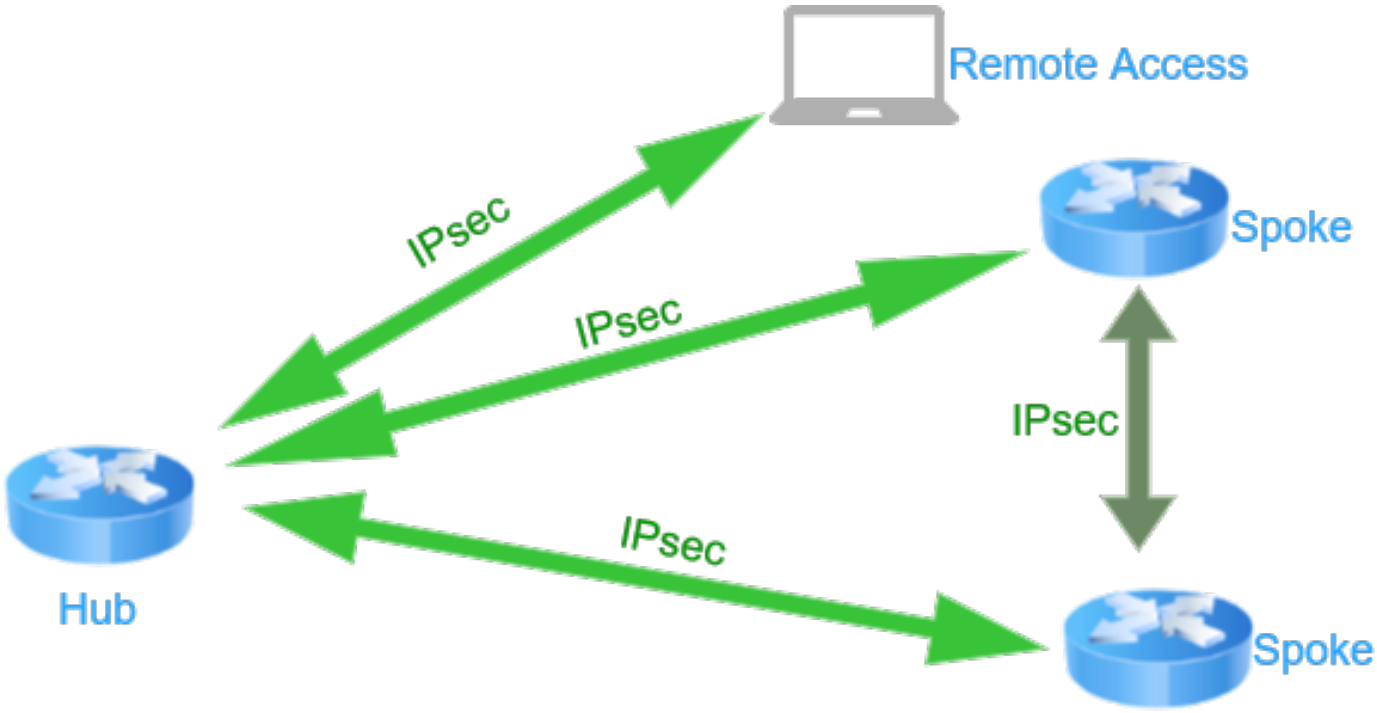
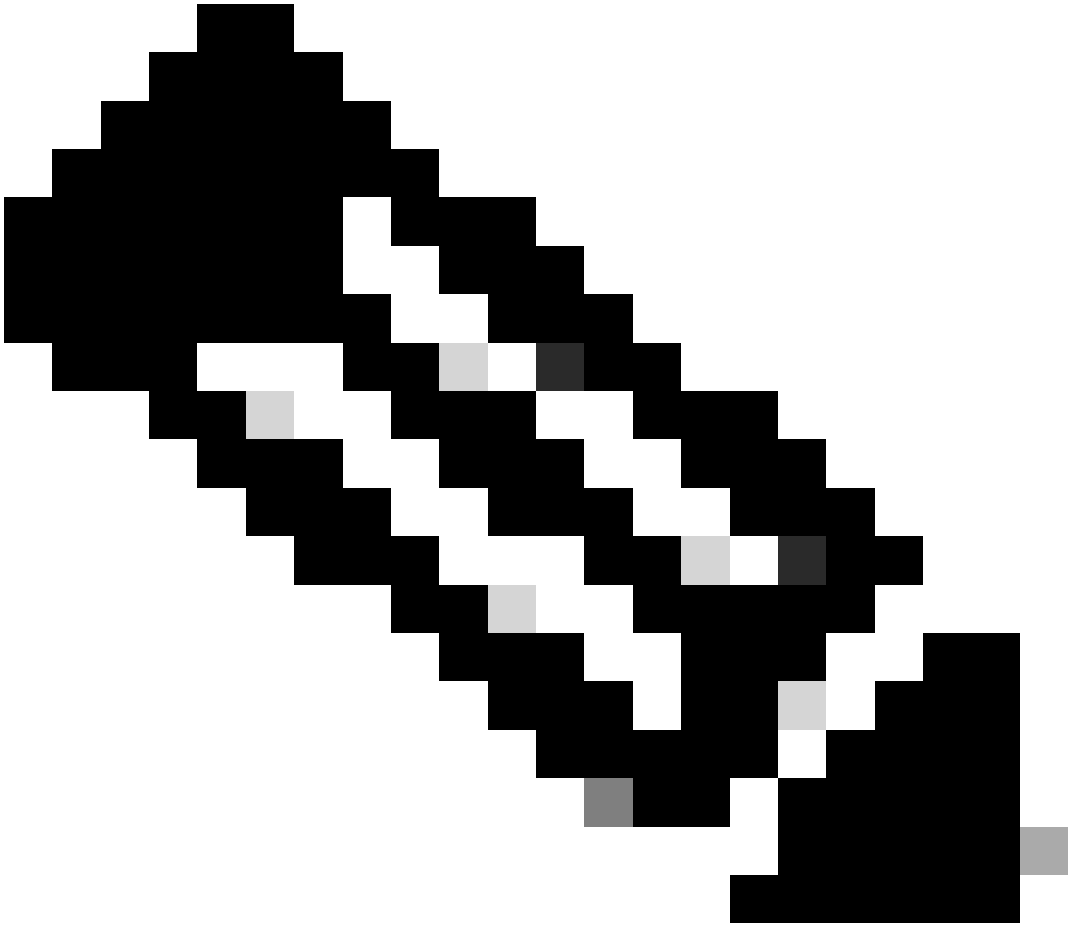


Diagrama FlexVPN



Note: A configuração da VPN de acesso remoto não é abordada neste guia. Para obter detalhes sobre sua configuração, consulte o guia:

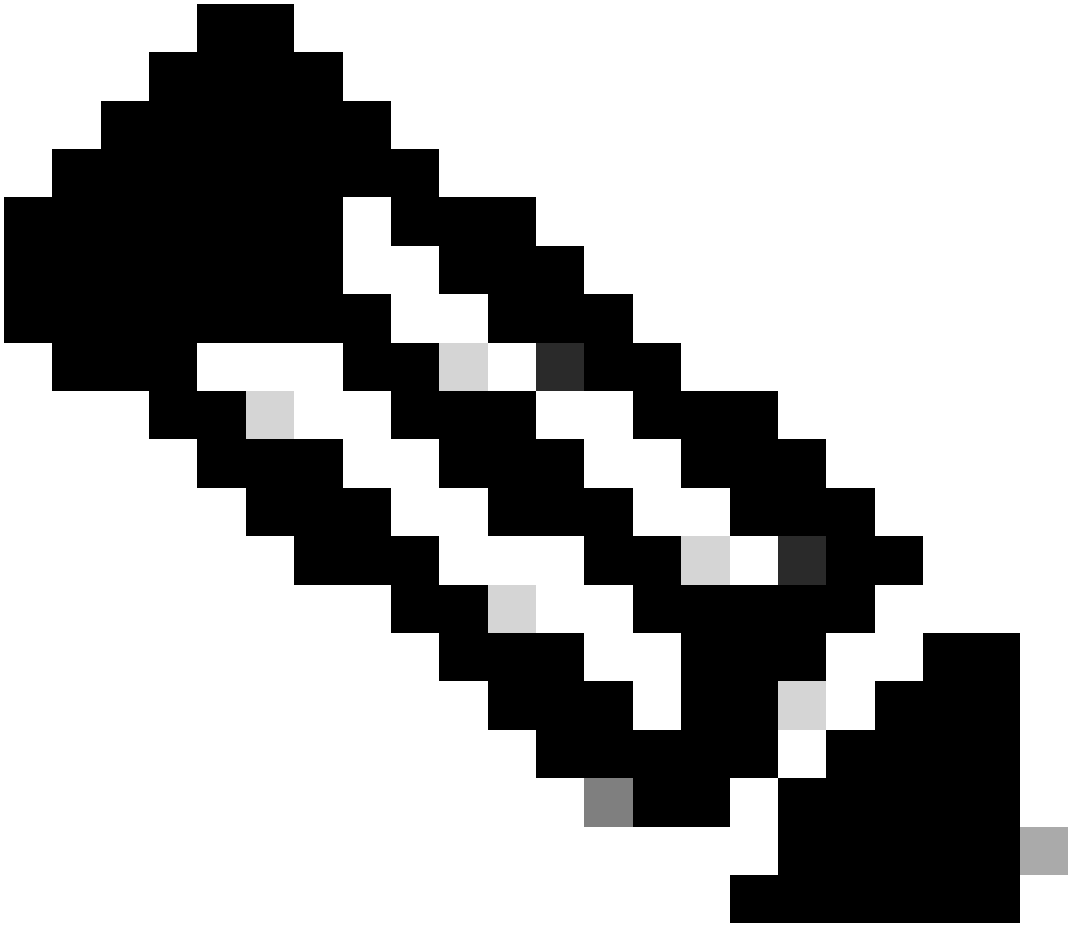
Configurar o FlexVPN Headend para acesso remoto IKEv2 de cliente seguro (AnyConnect) usando o banco de dados de usuário local

Configurar

O FlexVPN se caracteriza pela simplicidade de sua configuração. Essa simplicidade é evidente nos blocos de configuração consistentes usados para vários tipos de VPNs. O FlexVPN fornece blocos de configuração diretos que são geralmente aplicáveis, com configurações opcionais ou etapas adicionais disponíveis, dependendo dos recursos ou requisitos específicos da topologia:

- Proposta IKEv2: Define os algoritmos usados na negociação da Associação de Segurança (SA) IKEv2. Depois de criada, anexe esta proposta a uma política IKEv2 para que ela seja selecionada durante a negociação.

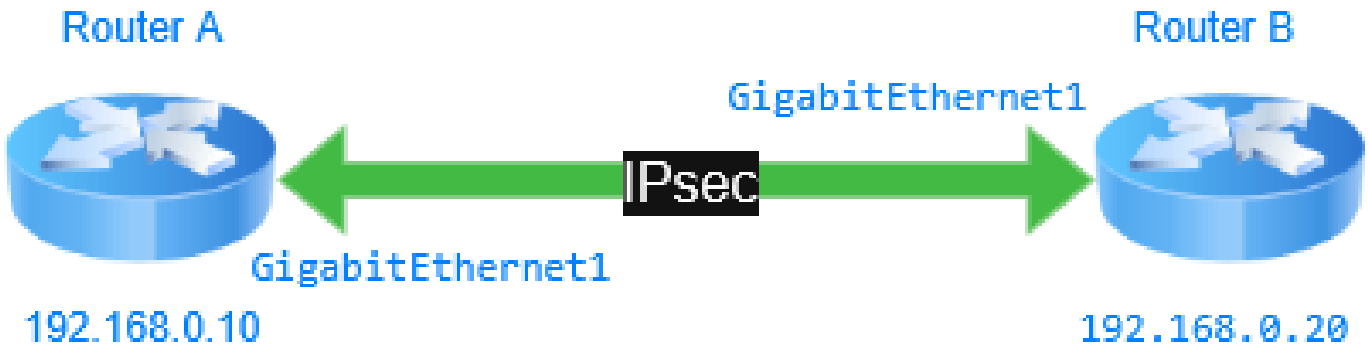
- Política IKEv2: Vincula a proposta a uma instância de Virtual Routing and Forwarding (VRF) ou endereço IP local. O link de política para a proposta IKEv2.
- Toque de chave IKEv2: Especifica Chaves pré-compartilhadas (PSKs), que podem ser assimétricas se usadas para autenticação de mesmo nível.
- Ponto confiável (opcional): Configura os atributos de identidade e de Autoridade de Certificação (CA) para autenticação de mesmo nível ao usar a infraestrutura de chave pública (PKI) como método de autenticação.
- Integração AAA (opcional): O FlexVPN integra servidores AAA, como o Cisco ISE (Identity Services Engine) ou servidores RADIUS como método de autenticação.
- Perfil IKEv2: Armazena parâmetros não negociáveis do SA IKE, como o endereço do par VPN e os métodos de autenticação. Não há perfil IKEv2 padrão, portanto, você deve configurar um e anexá-lo a um perfil IPsec no iniciador. Se a autenticação PSK for usada, o perfil IKEv2 fará referência ao chaveiro IKEv2. Se a autenticação PKI ou o método de autenticação AAA for usado, ele fará referência aqui.
- Conjunto de Transformação IPsec: Especifica uma combinação de algoritmos aceitáveis para o SA IPsec.
- Perfil IPsec: Consolida as configurações do FlexVPN em um único perfil que pode ser aplicado a uma interface. Este perfil faz referência ao conjunto de transformação IPsec e ao perfil IKEv2.



Note: Os exemplos de configuração utilizam Chaves pré-compartilhadas para fornecer uma demonstração direta da configuração e da simplicidade da FlexVPN. Embora as chaves pré-compartilhadas possam ser empregadas para fácil implantação e pequenas topologias, os métodos AAA ou PKI são mais adequados para topologias maiores.

Configuração FlexVPN site a site

A topologia site a site do FlexVPN foi projetada para conexões VPN diretas entre dois sites. Cada local é equipado com uma interface de túnel que estabelece um canal seguro sobre o qual o tráfego pode fluir. A configuração explica como estabelecer uma conexão VPN direta entre dois sites, como mostrado no diagrama.



Site_to_Site_Diagram

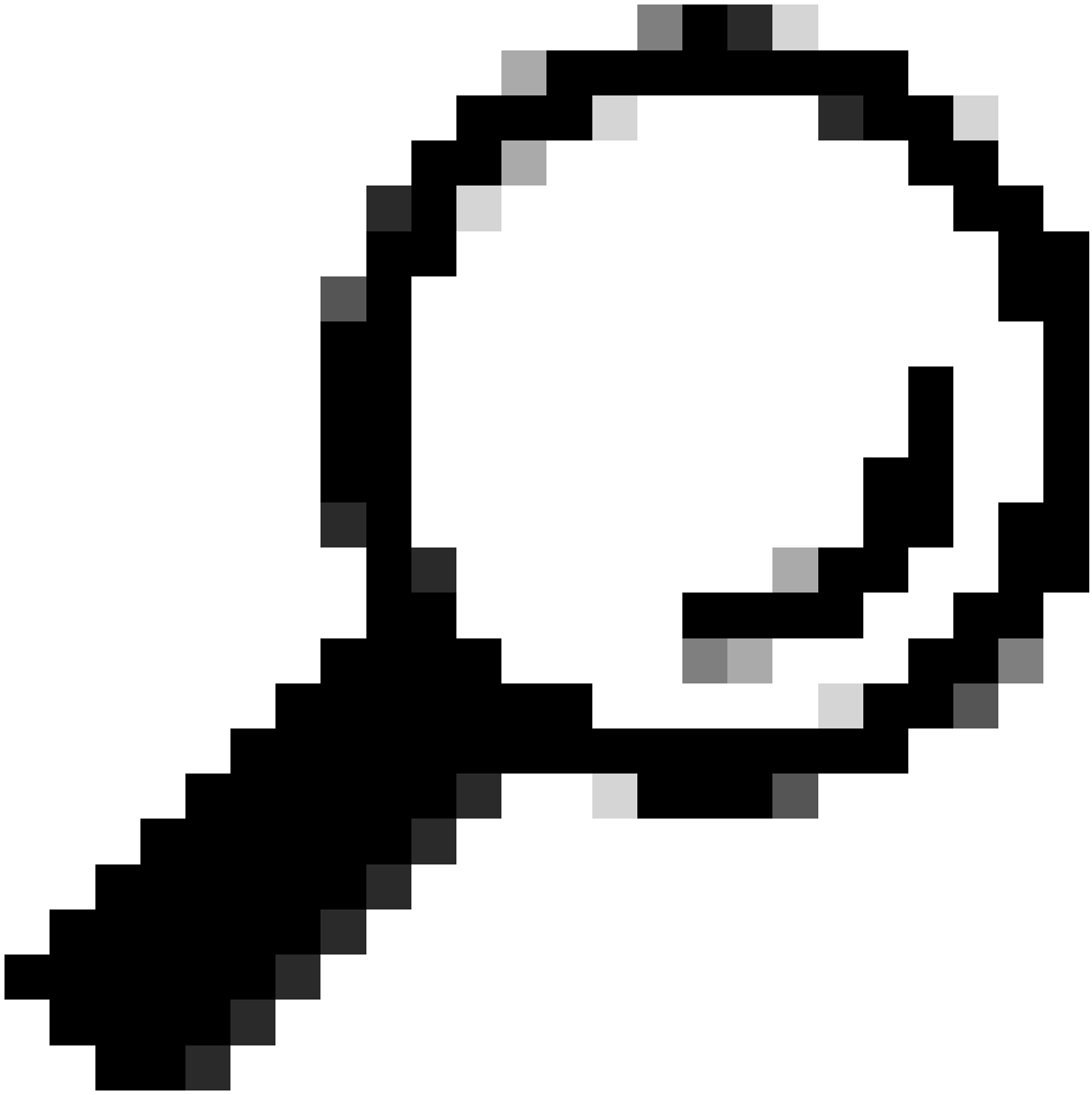
Passo 1: Configuração de Roteador A

a. Definir proposta e política de IKEv2.

b. Configure um chaveiro e insira um Pre-Shared Key que seja usado para autenticar o peer.

c. Crie um IKEv2 profile e atribua o keyring.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.20
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
crypto ikev2 profile FLEXVPN_PROFILE
match identity remote address 192.168.0.20
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```



Tip: O recurso **IKEv2 Smart Defaults** minimiza a configuração,FlexVPNcobrindo a maioria dos casos de uso. Você pode personalizar **IKEv2 Smart Defaults** para casos de uso específicos, embora a Cisco não recomende essa prática.

---

d. Crie um Transport Set e defina os algoritmos de criptografia e hash usados para proteger os dados.

e. Crie um **IPsec profile.**

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
```

```
 set ikev2-profile FLEXVPN_PROFILE
!
```

f. Configure a interface do túnel.

```
!
interface Tunnel0
 ip address 10.1.120.10 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.20
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.10 255.255.255.0
!
```

g. Configure o roteamento dinâmico para anunciar a interface do túnel. Depois disso, ele pode anunciar outras redes que devem passar pelo túnel.

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

Passo 2: Configuração do Roteador B

a. Definir proposta e política de IKEv2.

b. Configure um keyring e insira um Pre-Shared Key que seja usado para autenticar o peer.

c. Crie um IKEv2 profile e atribua o keyring.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.10
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
crypto ikev2 profile FLEXVPN_PROFILE
```

```
match identity remote address 192.168.0.10
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```

d. Crie um Transport Set e defina os algoritmos de criptografia e hash usados para proteger os dados.

e. Crie um IPsec profile e atribua o perfil IKEv2 e o conjunto de transformações criado anteriormente.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

f. Configure o Tunnel interface.

```
!
interface Tunnel0
 ip address 10.1.120.20 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.20 255.255.255.0
!
```

g. Configure o roteamento dinâmico para anunciar a interface do túnel. Depois disso, ele pode anunciar outras redes que devem passar pelo túnel.

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

Verificar

- Use o comando show ip interface brief para revisar o status da interface de túnel e verificar

se o túnel está em um status up/up.

<#root>

```
RouterB#
```

show ip interface brief

```
Interface              IP-Address      OK?   Method    Status   Protocol
GigabitEthernet1       192.168.0.20    YES   NVRAM     up       up
Tunnel0                10.1.120.11     YES   manual
```

up

```
 up
```

1. Use o comando show crypto ikev2 sa para confirmar se a conexão segura entre os roteadores está estabelecida.

<#root>

```
RouterB#
```

show crypto ikev2 sa

```
IPv4 Crypto IKEv2 SA

Tunnel-id  Local                Remote               fvrf/ivrf   Status
2          192.168.0.20/500     192.168.0.10/500     none/none
```

READY

```
    Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
```

Life/Active Time: 86400/3139 sec

```
IPv6 Crypto IKEv2 SA
```

- Use o comando show crypto ipsec sa para confirmar se o tráfego está criptografado e passando pelo túnel, verificando se os contadores encaps e decaps estão aumentando.

<#root>

```
RouterB#
```

show crypto ipsec sa

```
interface: Tunnel0
```

```
    Crypto map tag: Tunnel0-head-0, local addr 192.168.0.20

   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
   current_peer 192.168.0.10 port 500
     PERMIT, flags={origin_is_acl,}


#pkts encaps: 669, #pkts encrypt: 669, #pkts digest: 669




#pkts decaps: 668, #pkts decrypt: 668, #pkts verify: 668


    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

      local crypto endpt.: 192.168.0.20, remote crypto endpt.: 192.168.0.10
      plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
      current outbound spi: 0x93DCB8AE(2480715950)
      PFS (Y/N): N, DH group: none

      inbound esp sas:


spi: 0x89C141EB(2311143915)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5578, flow_id: CSR:3578, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0


sa timing: remaining key lifetime (k/sec): (4607913/520)


         IV size: 16 bytes
         replay detection support: Y


Status: ACTIVE(ACTIVE)



      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:


spi: 0x93DCB8AE(2480715950)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5577, flow_id: CSR:3577, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0


sa timing: remaining key lifetime (k/sec): (4607991/3137)
```

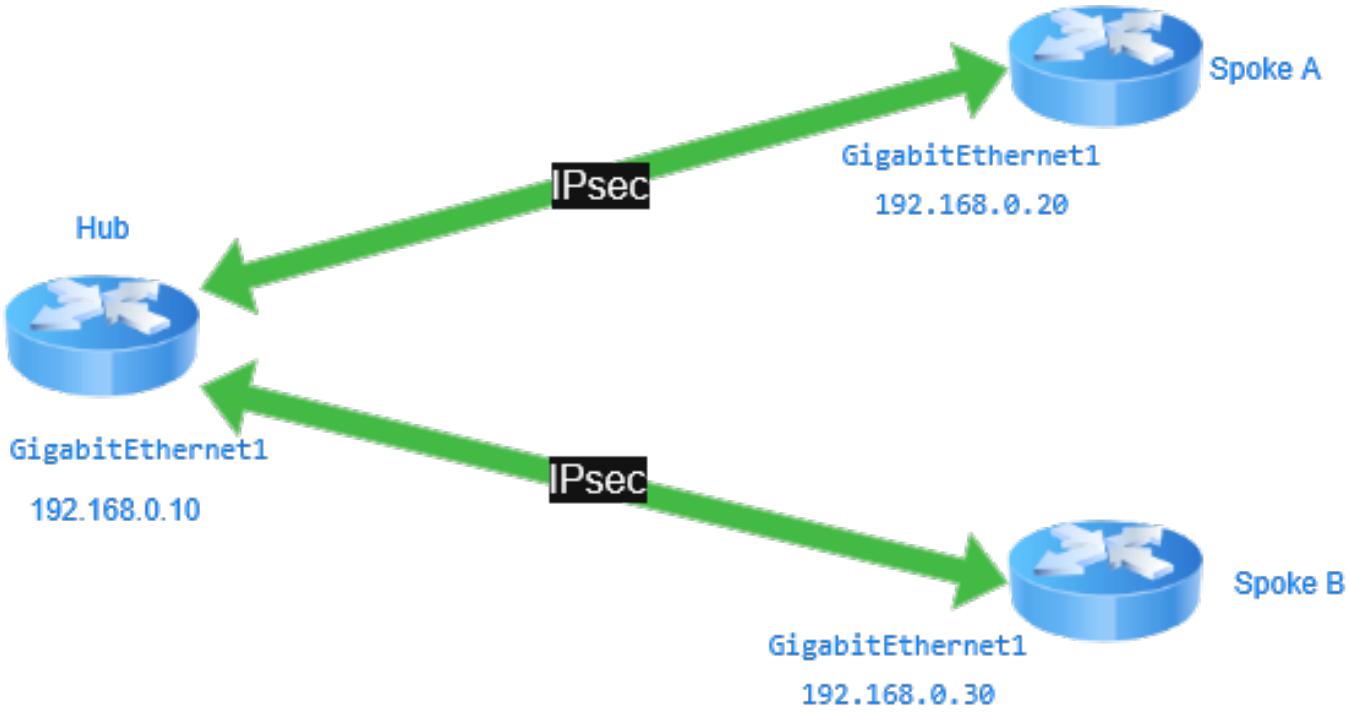
```
         IV size: 16 bytes
         replay detection support: Y

Status: ACTIVE(ACTIVE)


      outbound ah sas:

      outbound pcp sas:
```

- Use o comando show ip eigrp neighbors para confirmar se a adjacência do EIGRP está estabelecida com o outro site.

```
RouterB#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface              Hold  Uptime     SRTT    RTO    Q   Seq
                                                   (sec)            (ms)          Cnt  Num
0   10.1.120.10             Tu0                     13   00:51:26    3      1470   0   2
```

FlexVPN hub-and-spoke

Na topologia hub-and-spoke, vários roteadores spoke se conectam a um roteador de hub central. Essa configuração é ideal para cenários em que os spokes se comunicam principalmente com o hub. No FlexVPN, os túneis dinâmicos podem ser configurados para melhorar a eficiência da comunicação. O hub emprega o roteamento IKEv2 para distribuir rotas para roteadores spoke, garantindo conectividade contínua. Como é referenciado no diagrama, a configuração explica a conexão VPN entre um Hub e Spoke e como o Hub é configurado para estabelecer conexão dinâmica com vários Spokes e é capaz de adicionar mais Spokes.



Diagrama_Hub_and_Spoke

Passo 1: Configuração do Hub

a. Definir proposta e política de IKEv2.

b. Configure um keyring e insira um Pre-Shared Key que seja usado para autenticar os spokes.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Ative os serviços AAA no roteador Hub e, em seguida, defina uma lista de autorização de rede denominadaFlexAuthque especifique as políticas da configuração do dispositivo local.

```
!
aaa new-model
```

```
 aaa authorization network FlexAuth local
!
```

d. Defina um IP address pool nomeado FlexPool, que contenha os endereços de 10.1.1.2 a 10.1.1.254. Esse pool é usado para atribuir automaticamente um endereço IP à interface de túnel dos spokes.

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

e. Defina uma lista de acesso IP padrão que seja nomeada FlexTraffic e permita que a rede 10.10.1.0/24. Essa ACL define as redes que são enviadas aos spokes FlexVPN para acessá-las através do túnel.

```
!
ip access-list standard FlexTraffic
 permit 10.10.1.0 0.0.0.255
!
```

A lista de acesso e o pool de endereços IP são mencionados no **IKEv2 Authorization Policy**.

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

f. Crie um IKEv2 profile, atribua o grupo de autorização keyring e AAA.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

g. Crie um Transport Set, defina os algoritmos de criptografia e hash usados para proteger os dados.

h. Crie um IPsec profile, atribua o IKEv2 profile e o Transport Set criado anteriormente.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

i. Configure o **virtual-template 1** as **type tunnel**. Faça referência à interface como umIP unnumbered addresse aplique o **IPsec profile**

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

Passo 2: Configuração do raio

a. Definir proposta e política de IKEv2.

b. Configure um chaveiro e insira uma chave pré-compartilhada que é usada para autenticar no hub.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Ative os serviços AAA no roteador Hub e defina uma lista de autorização de rede nomeada **FlexAuth** que especifique as políticas da configuração do dispositivo local. Em seguida, configure a política de configuração do modo para enviar o endereço IP e as rotas para os spokes FlexVPN.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Defina uma lista de acesso IP padrão que seja nomeada **FlexTraffic** e permita que a rede 10.20.2.0/24. Essa ACL define as redes que são compartilhadas por esse spoke passem pelo túnel.

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

A lista de acesso é atribuída no **IKEv2 Authorization Policy**.

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. Crie um IKEv2 profile, atribua o grupo de autorização keyring e AAA.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
!
```

f. Crie um conjunto de transporte e defina os algoritmos de criptografia e hash usados para proteger os dados.

g. Crie um perfil IPsec, atribua o perfil IKEv2 e o conjunto de transporte criado anteriormente.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. Configure a interface túnel com a propriedade de endereço IP negociado, que é obtida do pool que ele configurou no hub.

```
!
interface tunnel 0
 ip address negotiated
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

Verificar

Use o comando show ip interface brief para revisar o status do túnel, do modelo virtual e do acesso virtual:

- No hub, o modelo virtual tem um status ativado/desativado, o que é normal. Um Acesso Virtual é criado para cada Spoke que estabelece uma conexão com o Hub e mostra um status up/up.
- No spoke, a interface do túnel recebeu um endereço IP e mostra um status up/up.

<#root>

FlexVPN_HUB#

show ip interface brief

```
Interface              IP-Address      OK? Method Status           Protocol
GigabitEthernet1       192.168.0.10    YES NVRAM  up               up
GigabitEthernet2       10.10.1.10      YES manual up               up
Loopback1              10.1.1.1        YES manual up               up
```

Virtual-Access1 10.1.1.1 YES unset up up

```
 <<<<<<< This Virtual-Access has been created and is up/up
Virtual-Template1      10.1.1.1        YES unset  up
```

```
FlexVPN_Spoke#
```

show ip interface brief

```
Interface              IP-Address      OK? Method  Status            Protocol
GigabitEthernet1       192.168.0.20    YES NVRAM   up                up
GigabitEthernet2       10.20.2.20      YES manual  up                up
```

Tunnel0 10.1.1.8 YES manual up up <<<<<<

```
The tunnel interface received an IP address from pool defined
```

- Use o comando show crypto ikev2 sa para confirmar que a conexão segura entre o Hub e o Spoke está estabelecida.

<#root>

```
FlexVPN_HUB#
```

show crypto ikev2 sa

```
 IPv4 Crypto IKEv2 SA

Tunnel-id Local                 Remote                fvrf/ivrf                Status
1         192.168.0.10/500      192.168.0.20/500      none/none
```

READY

```
 Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
 Life/Active Time: 86400/587 sec


 IPv6 Crypto IKEv2 SA
```

- Use o comando show crypto ipsec sa para confirmar se o tráfego está criptografado e passando pelo túnel, verificando se os contadores encaps e decaps estão aumentando.

<#root>

```
FlexVPN_HUB#
```

show crypto ipsec sa

interface: Virtual-Access1

Crypto map tag: Virtual-Access1-head-0, local addr 192.168.0.10

```
   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
   current_peer 192.168.0.20 port 500
     PERMIT, flags={origin_is_acl,}

    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10



    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10


    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.0.10, remote crypto endpt.: 192.168.0.20
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0xAFC2F841(2948790337)
     PFS (Y/N): N, DH group: none

     inbound esp sas:


spi: 0x7E780336(2121794358)


        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 5581, flow_id: CSR:3581, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-h


sa timing: remaining key lifetime (k/sec): (4607998/3010)


        IV size: 16 bytes
        replay detection support: Y


Status: ACTIVE(ACTIVE)



      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:


spi: 0xAFC2F841(2948790337)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5582, flow_id: CSR:3582, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-


sa timing: remaining key lifetime (k/sec): (4607998/3010)


         IV size: 16 bytes
         replay detection support: Y
```

```
Status: ACTIVE(ACTIVE)


      outbound ah sas:

      outbound pcp sas:
```

- Use o comando show ip route para verificar se as rotas foram enviadas aos spokes:
  - A rota para 10.1.1.1/32 foi enviada por meio de payloads de configuração de IKEv2 devido à instrução de interface do conjunto de rotas na configuração de HUB.
  - A rota para 10.10.1.0/24 foi enviada por payloads de configuração IKEv2 devido à instrução FlexTraffic route set access-list na configuração de HUB.

<#root>

```
FlexVPN_Spoke#show ip route
<<< Omitted >>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S        10.1.1.1/32 is directly connected, Tunnel0   <<<<<<<


C        10.1.1.8/32 is directly connected, Tunnel0
S        10.10.1.0/24 is directly connected, Tunnel0  <<<<<<<


C        10.20.2.20/32 is directly connected, GigabitEthernet2
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.20/32 is directly connected, GigabitEthernet1
```

- Use o comando ping para verificar a conectividade com as redes anunciadas.

<#root>

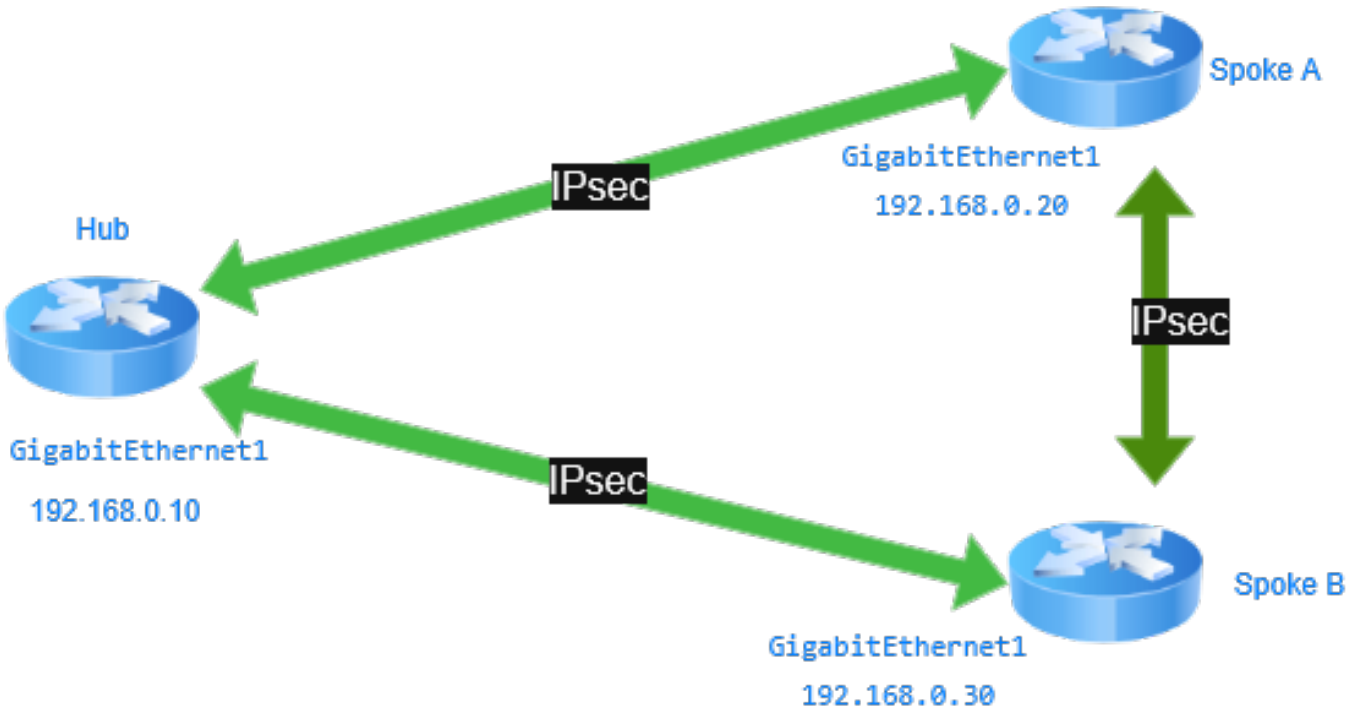
```
FlexVPN_HUB#

ping 10.20.2.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.2.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
FlexVPN_Spoke#

ping 10.10.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

FlexVPN spoke to spoke

A FlexVPN em uma topologia Hub and Spoke com conectividade Spoke to Spoke permite comunicação VPN dinâmica, escalável e segura. O hub atua como um ponto de controle centralizado onde o NHRP permite que os spokes consultem o hub quanto a outros endereços IP de spokes, permitindo túneis IPsec de spoke a spoke para comunicação eficiente e latência reduzida.

ip nhrp redirect No hub, o comando é usado para notificar os spokes de que a comunicação direta entre spoke e spoke é possível, otimizando o fluxo de tráfego, ignorando o hub para o tráfego do plano de dados. **ip nhrp shortcut** Nos spokes, o comando permite que eles estabeleçam dinamicamente túneis diretos com outros spokes após receberem o redirecionamento do hub. O diagrama faz referência ao tráfego entre o hub e o spoke e a comunicação spoke para spoke.



Spoke_to_Spoke_Diagram

Passo 1: Configuração do Hub

a. Defina políticas e perfis de IKEv2.

b. Configure um keyring e insira um Pre-Shared Key que seja usado para autenticar os spokes.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Ative os serviços AAA no roteador Hub, defina uma lista de autorização de rede nomeada **FlexAuth** que especifique políticas da configuração do dispositivo local e configure a política de configuração do modo para enviar o endereço IP e as rotas para os spokes FlexVPN.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Defina umIP address poolnome **FlexPool**, que contenha os endereços 10.1.1.2 a 10.1.1.254. Esse pool é usado para atribuir automaticamente um endereço IP à interface de túnel dos spokes.

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

e. Defina uma lista de acesso IP padrão que seja nomeadaFlexTraffice permita a rede 10.0.0.0/8. Essa ACL define as redes que são enviadas aos spokes FlexVPN, incluindo as redes para outros spokes conectados ao Hub, para que os spokes saibam que essas redes são alcançadas primeiro pelo Hub.

```
!
ip access-list standard FlexTraffic
 permit 10.0.0.0 0.255.255.255
!
```

As listas de acesso e IP address pool os são atribuídos no **IKEv2 Authorization Policy.**

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

f. Crie um IKEv2 profile, atribua o grupo de autorização keyring e AAA.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

g. Crie um Transport Set e defina os algoritmos de criptografia e hash usados para proteger os dados.

h. Crie um IPsec profile, atribua o IKEv2 profile e o Transport Set criado anteriormente.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

i. Configure o **virtual-template 1** as **type tunnel**. Faça referência à interface como um **IP unnumbered address** e aplique o **IPsec profile.**

O comando **ip nhrp redirect** é configurado no Modelo virtual para informar aos spokes para estabelecer uma conexão direta com outros spokes para acessar suas redes.

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

Passo 2: Configuração Do Spoke A

a. Defina políticas e perfis de IKEv2.

b. Configure um keyring e insira um Pre-Shared Key que seja usado para autenticar os spokes.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Ative os serviços AAA no roteador Hub e defina uma lista de autorização de rede nomeada **FlexAuth** que especifique as políticas da configuração do dispositivo local. Em seguida, configure a política de configuração do modo para enviar o endereço IP e as rotas para os spokes FlexVPN.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Defina uma lista de acesso IP padrão que seja nomeada **FlexTraffic** e permita que a rede 10.20.2.0/24. Essa ACL define as redes que são compartilhadas por esse spoke passem pelo túnel.

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

A lista de acesso é atribuída na **IKEv2 Authorization Policy.**

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. Crie um IKEv2 profile, atribua o grupo de autorização keyring e AAA.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

f. Crie um Transport Set e defina os algoritmos de criptografia e hash usados para proteger os dados.

g. Crie um perfil IPsec, atribua o perfil IKEv2 e o conjunto de transporte criado anteriormente.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. Configure a interface de túnel e o modelo virtual. Especifique **Virtual-Template1** para dVTIs que são criados para oferecer suporte a **NHRP shortcuts**. Além disso, defina tunnel0 como um endereço não numerado no virtual-template.

O **ip nhrp shortcut** comando é configurado nos Spokes para permitir que eles estabeleçam dinamicamente túneis diretos para outros spokes com base nas mensagens de redirecionamento

NHRP do hub.

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

Passo 3: Configuração do spoke B

a. Defina políticas e perfis de IKEv2.

b. Configure um keyring e insira um Pre-Shared Key que seja usado para autenticar os spokes.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Ative os serviços AAA no roteador Hub, defina uma lista de autorização de rede nomeada **FlexAuth** que especifique políticas da configuração do dispositivo local e configure a política de configuração do modo para enviar o endereço IP e as rotas para os spokes FlexVPN.

```
!
```

```
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Defina uma lista de acesso IP padrão nomeada **FlexTraffic** e que permita que a rede 10.30.3.0/24. Essa ACL define as redes que são compartilhadas por esse spoke passem pelo túnel.

```
!
ip access-list standard FlexTraffic
 permit 10.30.3.0 0.0.0.255
!
```

A lista de acesso é referenciada no IKEv2 Authorization Policy.

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. Crie um IKEv2 profile, atribua o grupo de autorização keyring e AAA.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

f. Crie um Transport Set e defina os algoritmos de criptografia e hash usados para proteger os dados.

g. Crie um IPsec profile, atribua o IKEv2 profile e o Transport Set criado anteriormente.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
```

```
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. Configure o tunnel interface e o virtual template. Especifique **Virtual-Template1** para dVTIs que são criados para oferecer suporte a NHRP shortcuts. Além disso, defina tunnel0 como um endereço não numerado no virtual-template.

O **ip nhrp shortcut** comando é configurado nos Spokes para permitir que eles estabeleçam dinamicamente túneis diretos para outros spokes com base nas mensagens de redirecionamento NHRP do hub.

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.30 255.255.255.0
!
```

Verificar

Use o comando show ip interface brief para revisar o status do túnel, do modelo virtual e do acesso virtual. Agora, é uma conexão direta de spoke para spoke:

- Nos Spokes, o Modelo Virtual tem um status ativo/inativo que é normal. Um acesso virtual é criado para conexão no estado up/up.

<#root>

```
FlexVPN_Spoke#

show ip interface brief


Interface                IP-Address      OK?  Method  Status                Protocol
GigabitEthernet1         192.168.0.30    YES  NVRAM   up                    up
GigabitEthernet2         10.20.2.20      YES  manual  up                    up

Tunnel0                  10.1.1.12       YES  manual  up                    up
```

```
Virtual-Access1          10.1.1.12      YES  unset   up                    up

Virtual-Template1        10.1.1.12      YES  unset   up                    down
```

- Use o comando show crypto ikev2 sa para confirmar que a conexão segura entre cada dispositivo está estabelecida.
- Use o comando show crypto ipsec sa para confirmar se o tráfego está criptografado e passando pelo túnel, verificando se os contadores encaps e decaps estão aumentando.
- Use o comando show ip nhrp para verificar o redirecionamento de tráfego entre os spokes.

<#root>

```
FlexVPN_Spoke#

show ip nhrp


10.1.1.10/32 via 10.1.1.10
   Virtual-Access1 created 00:00:13, expire 00:09:46
   Type:

dynamic

, Flags: router nhop rib nho
   NBMA address: 192.168.0.30

10.30.3.0/24 via 10.1.1.10


   Virtual-Access1 created 00:00:13, expire 00:09:46
   Type:

dynamic

, Flags: router rib nho
   NBMA address: 192.168.0.30
```

Use o comando show ip route para verificar se as rotas foram enviadas para o spoke:

- As duas rotas associadas à interface Virtual-Access1 são novas e associadas aos atalhos NHRP.
- O caractere % indica uma substituição do próximo salto.

<#root>

```
FlexVPN_Spoke#sh ip route
<<<< Omitted >>>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
S        10.0.0.0/8 is directly connected, Tunnel0
S        10.1.1.1/32 is directly connected, Tunnel0
```

```
S  %     10.1.1.10/32 is directly connected, Virtual-Access1


C        10.1.1.12/32 is directly connected, Tunnel0
C        10.20.2.20/32 is directly connected, GigabitEthernet2
S  %     10.30.3.0/24 is directly connected, Virtual-Access1


      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.30/32 is directly connected, GigabitEthernet1
```

- Use o comando ping para verificar a conectividade com as redes anunciadas.

<#root>

```
FlexVPN_Spoke#

ping 10.30.3.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.3.30, timeout is 2 seconds:

.!!!!


Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração. Use estes comandos para depurar o processo de negociação do túnel:

debug crypto interface

debug crypto ikev2
debug crypto ikev2 client flexvpn
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ikev2 packet

debug crypto ipsec
debug crypto ipsec error
debug crypto ipsec message
debug crypto ipsec states

As depurações de NHRP podem ajudar na solução de problemas das conexões spoke-to-spoke.

```
debug nhrp
debug nhrp detail
debug nhrp event
debug nhrp error
debug nhrp packet
debug nhrp routing
```

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.