FlexVPN: Exemplo de configuração de implantação de IPv6 em hub and spoke

Contents

Introduction

Este documento descreve uma configuração comum que usa uma implantação de hub e spoke FlexVPN do Cisco IOS® em um ambiente IPv6. Ele se expande nos conceitos discutidos no FlexVPN: Configuração básica de LAN para LAN do IPv6.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco IOS FlexVPN
- Protocolos de Roteamento

Componentes Utilizados

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

- Roteadores de Serviços Integrados Cisco 2ª Geração (ISR G2)
- Software Cisco IOS versão 15.3 (ou versão 15.4T para túneis spoke-to-spoke dinâmicos com IPv6)

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

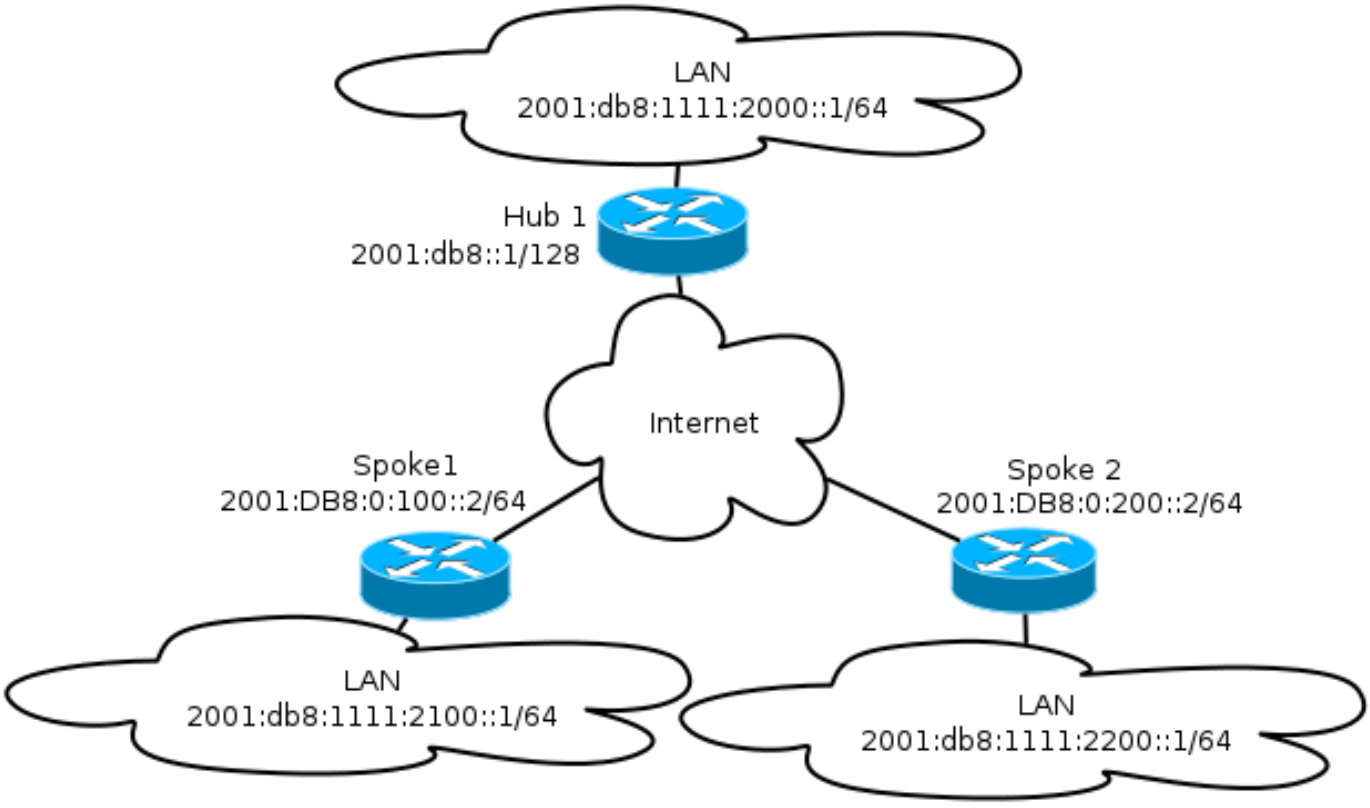
> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Embora esse exemplo de configuração e diagrama de rede usem IPv6 como a rede de transporte, o Generic Routing Encapsulation (GRE) é normalmente usado em implantações de FlexVPN. O uso de GRE em vez de IPsec permite que os administradores executem IPv4 ou IPv6 ou ambos nos mesmos túneis, independentemente da rede de transporte.

Diagrama de Rede

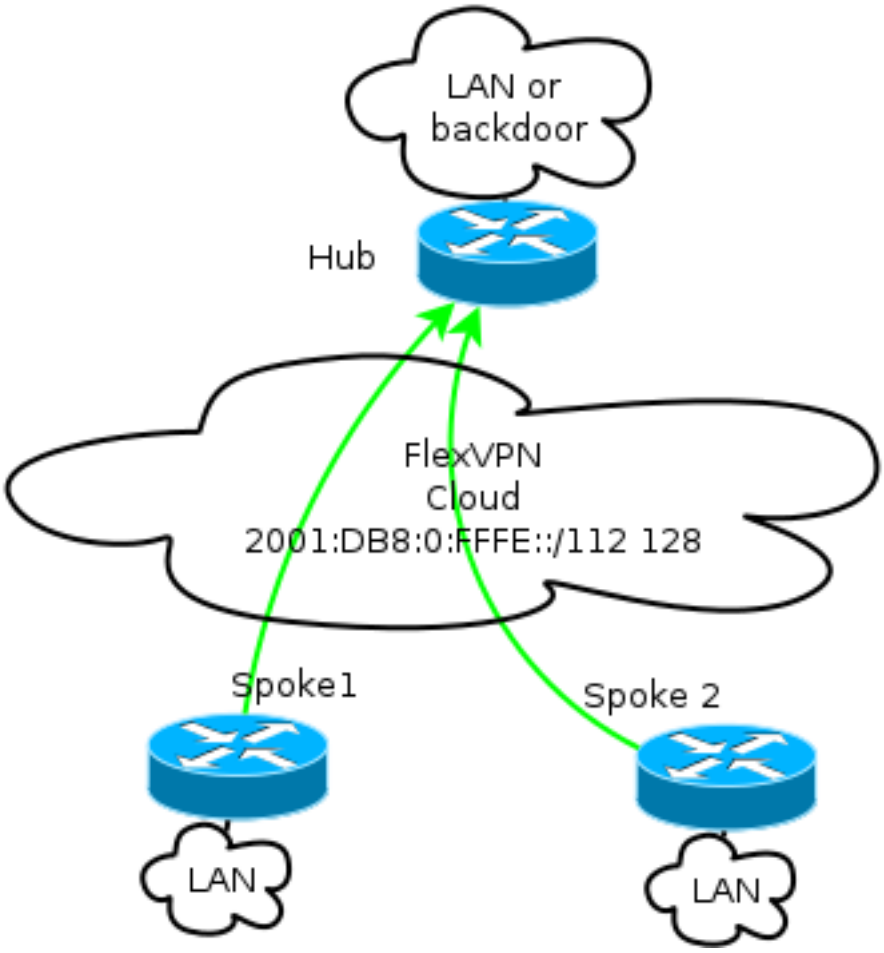
Rede de transporte

Este é um diagrama da rede de transporte usada neste exemplo:



Sobreposição de rede

Este é um diagrama da topologia de rede de sobreposição básica usada neste exemplo:



Cada spoke é atribuído de um pool de endereços /112, mas recebe um endereço /128. Assim, a notação '/112 128' é usada na configuração do pool IPv6 do hub.

Configurações

Essa configuração mostra uma sobreposição IPv4 e IPv6 que funciona em um backbone IPv6.

Quando comparado a exemplos que usam IPv4 como um backbone, observe que você deve usar o comando **tunnel mode** para alterar o nó e acomodar o transporte IPv6.

O recurso de túnel spoke-to-spoke sobre IPv6 será apresentado no Cisco IOS Software Release 15.4T, que ainda não está disponível.

Protocolos de Roteamento

A Cisco recomenda que você use o Border Gateway Protocol (iBGP) interno para peering entre spoke e hubs para grandes implantações, pois o iBGP é o protocolo de roteamento mais escalável.

O intervalo de escuta do Border Gateway Protocol (BGP) não suporta o intervalo de IPv6, mas simplifica o uso com um transporte IPv4. Embora seja viável usar o BGP em um ambiente desse

tipo, essa configuração ilustra um exemplo básico, então o EIGRP (Enhanced Interior Gateway Routing Protocol) foi escolhido.

Configuração do hub

Comparada aos exemplos mais antigos, essa configuração inclui o uso de novos protocolos de transporte.

Para configurar o hub, o administrador precisa:

- Ative o roteamento unicast.
- Provisione roteamento de transporte.
- Provisione um novo pool de endereços IPv6 a serem atribuídos dinamicamente. O pool é 2001:DB8:0:FFFE::/112; 16 bits permitem que 65.535 dispositivos sejam endereçados.
- Ative o IPv6 para a configuração do Next Hop Resolution Protocol (NHRP) para permitir o IPv6 na sobreposição.
- Considere o endereçamento IPv6 no teclado, bem como o perfil na configuração de criptografia.

Neste exemplo, o hub anuncia um resumo do EIGRP para todos os spokes.

A Cisco não recomenda o uso de um endereço de sumarização na interface Virtual-Template na implantação do FlexVPN; no entanto, em uma VPN multiponto dinâmica (DMVPN), isso não é apenas comum, mas também é considerado uma prática recomendada. Consulte Migração do FlexVPN: Transferência forçada de DMVPN para FlexVPN nos mesmos dispositivos: Configuração do hub atualizada para obter detalhes.

```
ipv6 unicast-routing
ipv6 cef

ip local pool FlexSpokes 10.1.1.176 10.1.1.254
ipv6 local pool FlexSpokesv6 2001:DB8:0:FFFE::/112 128

crypto ikev2 authorization policy default
 ipv6 pool FlexSpokesv6
pool FlexSpokes
route set interface
crypto ikev2 keyring Flex_key
peer ALL
address ::/0
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/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

interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
```

```
ip mtu 1400
ip nhrp network-id 2
ip nhrp redirect
ip tcp adjust-mss 1360
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
 ipv6 unnumbered Loopback100
ipv6 enable
ipv6 eigrp 65001
 ipv6 nhrp network-id 2
 ipv6 nhrp redirect
 tunnel mode gre ipv6
tunnel protection ipsec profile default

interface Ethernet1/0
description LAN subnet
ip address 192.168.0.1 255.255.255.0
ipv6 address 2001:DB8:1111:2000::1/64
ipv6 enable
ipv6 eigrp 65001

interface Loopback0
ip address 172.25.1.1 255.255.255.255
ipv6 address 2001:DB8::1/128
ipv6 enable

ip route 192.168.0.0 255.255.0.0 Null0
ipv6 route 2001:DB8:1111::/48 Null0

ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
ipv6 prefix-list EIGRP_SUMMARY_v6 seq 5 permit 2001:DB8:1111::/48

router eigrp 65001
 distribute-list prefix EIGRP_SUMMARY_ONLY out Virtual-Template1
 network 10.1.1.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
 redistribute static metric 1500 10 10 1 1500

ipv6 router eigrp 65001
 distribute-list prefix-list EIGRP_SUMMARY_v6 out Virtual-Template1
 redistribute static metric 1500 10 10 1 1500
```

Configuração de Spoke

Como na configuração do hub, o administrador precisa provisionar o endereçamento IPv6, ativar o roteamento IPv6 e adicionar a configuração de NHRP e criptografia.

Éviável usar o EIGRP e outros protocolos de roteamento para peering spoke-to-spoke. No entanto, em um cenário típico, os protocolos não são necessários e podem afetar a escalabilidade e a estabilidade.

Neste exemplo, a configuração de roteamento mantém somente a adjacência do EIGRP entre o spoke e o hub, e a única interface que não é passiva é a interface Tunnel1:

```
ipv6 unicast-routing
ipv6 cef

crypto logging session
```

```
crypto ikev2 authorization policy default
route set interface
crypto ikev2 keyring Flex_key
peer ALL
address ::/0
pre-shared-key local cisco
pre-shared-key remote cisco
!
crypto ikev2 profile Flex_IKEv2
match identity remote address ::/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

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 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
ipv6 address negotiated
 ipv6 enable
 ipv6 nhrp network-id 2
 ipv6 nhrp shortcut virtual-template 1
 ipv6 nhrp redirect
tunnel source Ethernet0/0
 tunnel mode gre ipv6
tunnel destination 2001:DB8::1
tunnel protection ipsec profile default

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
delay 1000
ipv6 mtu 1400
ipv6 tcp adjust-mss 1358
 ipv6 unnumbered Ethernet1/0
ipv6 enable
 ipv6 nhrp network-id 2
 ipv6 nhrp shortcut virtual-template 1
 ipv6 nhrp redirect
tunnel mode gre ipv6
tunnel protection ipsec profile default
```

Siga estas recomendações ao criar entradas de protocolo de roteamento em um spoke:

1. Permita que o protocolo de roteamento estabeleça uma relação através da conexão (neste caso, a interface Tunnel1) com o hub. Geralmente, não é desejável estabelecer adjacência de roteamento entre spokes, pois isso aumenta significativamente a complexidade na maioria dos casos.

2. Anuncie somente sub-redes locais de LAN e ative o protocolo de roteamento em um endereço IP atribuído pelo hub. Tenha cuidado para não anunciar uma sub-rede grande porque ela pode afetar a comunicação spoke-to-spoke.

Este exemplo reflete ambas as recomendações para EIGRP em Spoke1:

```
router eigrp 65001
 network 10.1.1.0 0.0.0.255
 network 192.168.101.0 0.0.0.255
 passive-interface default
 no passive-interface Tunnel1

ipv6 router eigrp 65001
 passive-interface default
 no passive-interface Tunnel1
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

> **Note**: 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..

Sessão spoke-to-hub

Uma sessão corretamente configurada entre dispositivos spoke e hub tem uma sessão IKEv2 (Internet Key Exchange Version 2) que está ativa e tem um protocolo de roteamento que pode estabelecer adjacência. Neste exemplo, o protocolo de roteamento é EIGRP, portanto, há dois comandos EIGRP:

- **show crypto ikev2 sa**
- **show ipv6 eigrp 65001 neighbor**
- **show ip eigrp 65001 neighbor**

```
Spoke1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
1          none/none            READY
Local  2001:DB8:0:100::2/500
Remote  2001:DB8::1/500
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth
verify: PSK
     Life/Active Time: 86400/1945 sec

Spoke1#sh ipv6 eigrp 65001 neighbor
EIGRP-IPv6 Neighbors for AS(65001)
H   Address                 Interface          Hold Uptime   SRTT   RTO  Q  Seq
```

```
                                          (sec)         (ms)       Cnt Num
0   Link-local address:     Tu1                 14 00:32:29   72  1470  0  10
   FE80::A8BB:CCFF:FE00:6600

Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(65001)
H   Address                 Interface          Hold Uptime   SRTT   RTO  Q  Seq
                                          (sec)         (ms)       Cnt Num
0   10.1.1.1                Tu1                11 00:21:05   11  1398  0  26
```

No IPv4, o EIGRP usa um endereço IP atribuído ao peer; no exemplo anterior, é o endereço IP do hub 10.1.1.1.

O IPv6 usa um endereço de link local; neste exemplo, o hub é FE80::A8BB:CCFF:FE00:6600. Use o comando **ping** para verificar se o hub pode ser alcançado através do IP link local:

```
Spoke1#ping FE80::A8BB:CCFF:FE00:6600
Output Interface: tunnel1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to FE80::A8BB:CCFF:FE00:6600, timeout is
2 seconds:
Packet sent with a source address of FE80::A8BB:CCFF:FE00:6400%Tunnel1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/5 ms
```

Sessão spoke-to-spoke

As sessões spoke-to-spoke são criadas dinamicamente sob demanda. Use um comando **ping** simples para disparar uma sessão:

```
Spoke1#ping  2001:DB8:1111:2200::100 source e1/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:1111:2200::100, timeout is 2 seconds:
Packet sent with a source address of 2001:DB8:1111:2100::1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/8/10 ms
```

Para confirmar a conectividade direta spoke-to-spoke, o administrador precisa:

- Verifique se uma sessão spoke-to-spoke dinâmica aciona uma nova interface de acesso virtual:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed
state to up
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.
Peer 2001:DB8:0:200::2:500       Id: 2001:DB8:0:200::2
```

- Verifique o estado da sessão IKEv2:

```
Spoke1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

 IPv6 Crypto IKEv2  SA

Tunnel-id    fvrf/ivrf              Status
1          none/none             READY
```

```
Local  2001:DB8:0:100::2/500
Remote  2001:DB8::1/500
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
     Life/Active Time: 86400/3275 sec

Tunnel-id    fvrf/ivrf              Status
2          none/none            READY
Local  2001:DB8:0:100::2/500
Remote  2001:DB8:0:200::2/500
     Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK,
Auth verify: PSK
     Life/Active Time: 86400/665 sec
```

Observe que duas sessões estão disponíveis: um spoke-to-hub e um spoke-to-spoke.

- Verificar o NHRP:

```
Spoke1#show ipv6 nhrp
2001:DB8:0:FFFE::/128 via 2001:DB8:0:FFFE::
Virtual-Access1 created 00:00:10, expire 01:59:49
Type: dynamic, Flags: router nhop rib nho
NBMA address: 2001:DB8:0:200::2
2001:DB8:1111:2200::/64 via 2001:DB8:0:FFFE::
Virtual-Access1 created 00:00:10, expire 01:59:49
Type: dynamic, Flags: router rib nho
NBMA address: 2001:DB8:0:200::2
```

A saída mostra que 2001:DB8:111:2200::/64 (a LAN para Spoke2) está disponível via 2001:DB8:0:FFFE::, que é o endereço IPv6 negociado na interface Tunnel1 para Spoke2. A interface Tunnel1 está disponível através do endereço NBMA (nonbroadcast multiaccess) de 2001:db8:0:200::2 , que é o endereço IPv6 atribuído estaticamente ao Spoke2.

- Verifique se o tráfego está passando por essa interface:

```
Spoke1#sh crypto ipsec sa peer 2001:DB8:0:200::2

interface: Virtual-Access1
   Crypto map tag: Virtual-Access1-head-0, local addr 2001:DB8:0:100::2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (2001:DB8:0:100::2/128/47/0)
  remote ident (addr/mask/prot/port): (2001:DB8:0:200::2/128/47/0)
  current_peer 2001:DB8:0:200::2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 196, #pkts encrypt: 196, #pkts digest: 196
   #pkts decaps: 195, #pkts decrypt: 195, #pkts verify: 195
(...)
```

- Verifique o caminho de roteamento e as configurações de CEF:

```
Spoke1#show ipv6 route
(...)
D   2001:DB8:1111:2200::/64 [90/27161600]
    via 2001:DB8:0:FFFE::, Virtual-Access1 [Shortcut]
    via FE80::A8BB:CCFF:FE00:6600, Tunnel1
(...)
Spoke1#show ipv6 cef 2001:DB8:1111:2200::
2001:DB8:1111:2200::/64
 nexthop 2001:DB8:0:FFFE:: Virtual-Access
```

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

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

Esses comandos debug ajudam a solucionar problemas:

- FlexVPN/IKEv2 e IPsec: **debug crypto ipsecdebug crypto ikev2 [pacote|interno]**
- NHRP (spoke-to-spoke):
  - **debug nhrp pack**
  - **debug nhrp extension**
  - **debug nhrp cache**
  - **debug nhrp route**

Consulte a Lista de Comandos Mestre do Cisco IOS, Todas as Versões para obter mais informações sobre esses comandos.