FlexVPN: Ejemplo de Configuración de la Implementación de IPv6 en un Hub y Spoke

Contenido

Introducción

Este documento describe una configuración común que utiliza un Cisco IOS® FlexVPN spoke e implementación de hub en un entorno IPv6. Se expande sobre los conceptos tratados en FlexVPN: Configuración básica de LAN a LAN IPv6.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco IOS FlexVPN
- Protocolos de ruteo

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Routers de servicios integrados de segunda generación (ISR G2) de Cisco
- Versión 15.3 del software del IOS de Cisco (o versión 15.4T para túneles dinámicos de radio a radio con 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

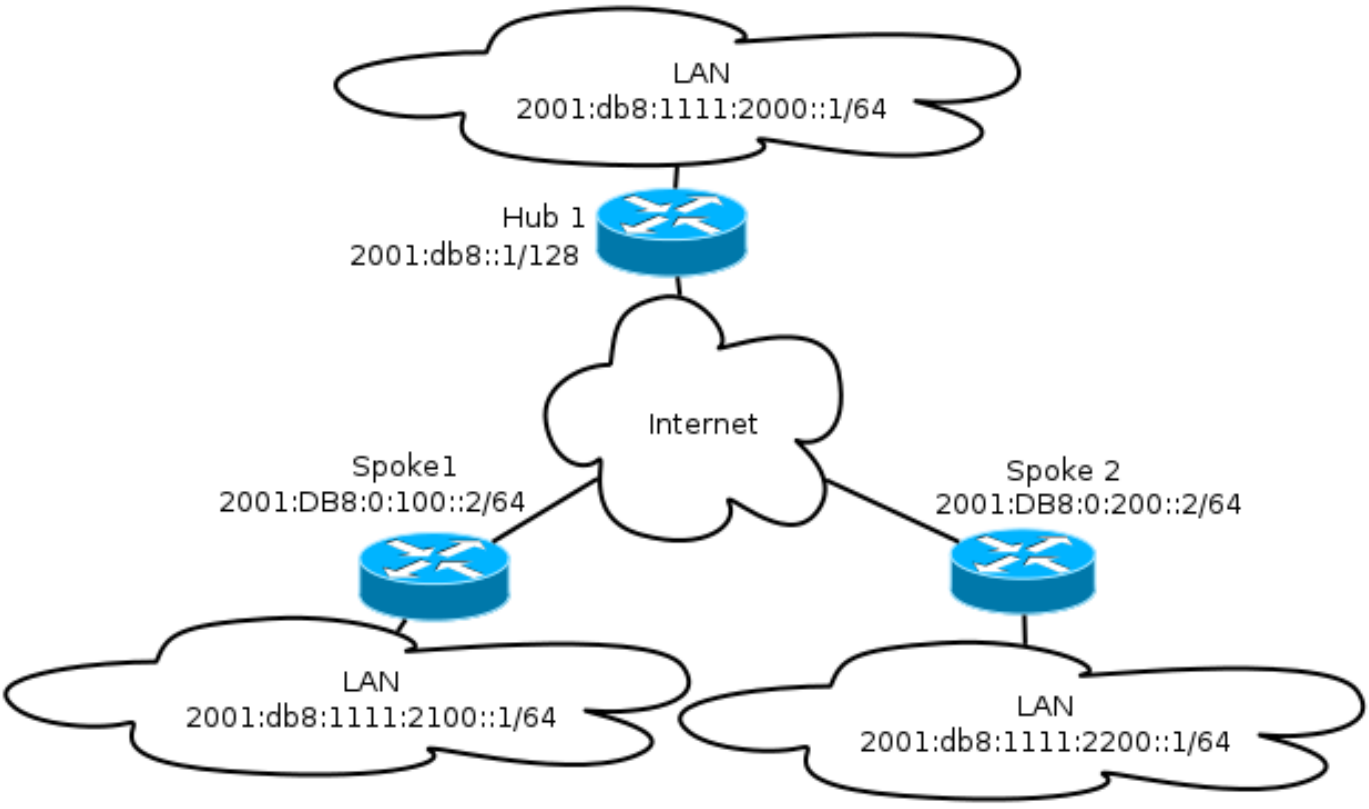
> **Nota:** Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Mientras que este ejemplo de configuración y el diagrama de red utilizan IPv6 como red de transporte, la encapsulación de routing genérico (GRE) se suele utilizar en implementaciones FlexVPN. El uso de GRE en lugar de IPsec permite a los administradores ejecutar IPv4 o IPv6 o ambos en los mismos túneles, independientemente de la red de transporte.

Diagrama de la red

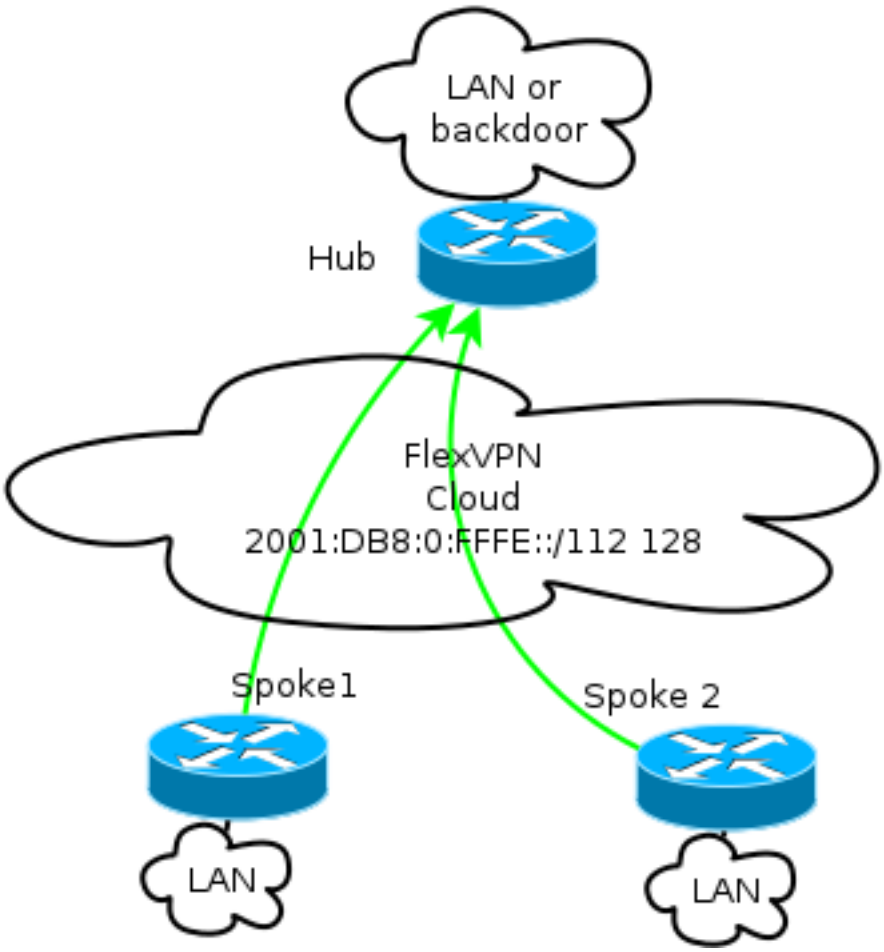
Red de transporte

Este es un diagrama de la red de transporte utilizada en este ejemplo:



Red superpuesta

Este es un diagrama de la topología básica de red superpuesta utilizada en este ejemplo:



Cada radio se asigna desde un conjunto de direcciones de /112, pero recibe una dirección /128. Por lo tanto, la notación '/112 128' se utiliza en la configuración del conjunto IPv6 del hub.

Configuraciones

Esta configuración muestra una superposición de IPv4 e IPv6 que funciona sobre una estructura básica de IPv6.

Cuando se compara con ejemplos que utilizan IPv4 como estructura básica, observe que debe utilizar el comando **tunnel mode** para cambiar el nodo y acomodar el transporte IPv6.

La función de túnel de radio a radio sobre IPv6 se introducirá en la versión 15.4T del software del IOS de Cisco, que aún no está disponible.

Protocolos de ruteo

Cisco recomienda que utilice el protocolo de gateway fronterizo interno (iBGP) para el peering entre radios y concentradores para implementaciones de gran tamaño porque iBGP es el protocolo de routing más escalable.

El intervalo de escucha del protocolo de gateway fronterizo (BGP) no admite el intervalo IPv6, pero simplifica el uso con un transporte IPv4. Aunque es factible utilizar BGP en un entorno de este tipo, esta configuración ilustra un ejemplo básico, por lo que se eligió el protocolo de routing de gateway interior mejorado (EIGRP).

Configuración del hub

En comparación con ejemplos anteriores, esta configuración incluye el uso de nuevos protocolos de transporte.

Para configurar el hub, el administrador necesita:

- Habilite el ruteo de unidifusión.
- Aprovisione el routing de transporte.
- Aprovisione un nuevo conjunto de direcciones IPv6 para asignarlo dinámicamente. La piscina es 2001:DB8:0:FFFE::/112; Los 16 bits permiten el direccionamiento de 65 535 dispositivos.
- Habilite IPv6 para la configuración del protocolo de resolución de salto siguiente (NHRP) para permitir IPv6 en la superposición.
- Cuenta para el direccionamiento IPv6 en el llenado de claves, así como el perfil en la configuración de criptografía.

En este ejemplo, el hub anuncia un resumen EIGRP para todos los radios.

Cisco no recomienda el uso de una dirección de resumen en la interfaz de plantilla virtual en la implementación de FlexVPN; sin embargo, en una VPN multipunto dinámica (DMVPN), esto no solo es común, sino que también se considera una práctica recomendada. Consulte Migración de FlexVPN: Cambio difícil de DMVPN a FlexVPN en los mismos dispositivos: Actualización de la configuración del hub para obtener más detalles.

```
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
```

Configuración de Spoke

Al igual que en la configuración del hub, el administrador necesita aprovisionar el direccionamiento IPv6, habilitar el ruteo IPv6 y agregar la configuración de NHRP y criptografía.

Es factible utilizar EIGRP y otros protocolos de ruteo para el peering de spoke a spoke. Sin embargo, en un escenario típico, los protocolos no son necesarios y pueden afectar a la escalabilidad y estabilidad.

En este ejemplo, la configuración de ruteo mantiene solamente la adyacencia EIGRP entre el spoke y el hub, y la única interfaz que no es pasiva es la interfaz 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 recomendaciones cuando cree entradas de protocolo de ruteo en un spoke:

1. Permita que el protocolo de ruteo establezca una relación a través de la conexión (en este caso, la interfaz Tunnel1) al hub. Por lo general, no es deseable establecer adyacencia de

ruteo entre radios porque esto aumenta significativamente la complejidad en la mayoría de los casos.

2. Anuncie solamente las subredes LAN locales y habilite el protocolo de ruteo en una dirección IP asignada por el hub. Tenga cuidado de no anunciar una subred grande porque podría afectar a la comunicación de radio a radio.

Este ejemplo refleja ambas recomendaciones para EIGRP en 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
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

> **Nota:** La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Sesión de Spoke a Hub

Una sesión configurada correctamente entre dispositivos radiales y concentradores tiene una sesión de Intercambio de claves de Internet versión 2 (IKEv2) activa y tiene un protocolo de routing que puede establecer adyacencia. En este ejemplo, el protocolo de ruteo es EIGRP, por lo que hay dos 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
```

En IPv4, EIGRP utiliza una dirección IP asignada al par; en el ejemplo anterior, es la dirección IP del hub de 10.1.1.1.

IPv6 utiliza una dirección local de link; en este ejemplo, el hub es FE80::A8BB:CCFF:FE00:6600. Utilice el comando **ping** para verificar que se pueda alcanzar el hub a través de su IP local de link:

```
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
```

Sesión de radio a radio

Las sesiones de radio a radio se activan dinámicamente a demanda. Utilice un simple comando **ping** para activar una sesión:

```
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 la conectividad directa de spoke a spoke, el administrador necesita:

- Verifique que una sesión dinámica de radio a radio active una nueva interfaz de acceso 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 el estado de la sesión 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
```

Tenga en cuenta que hay disponibles dos sesiones: un spoke a hub y otro spoke a spoke.

- Verifique 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
```

El resultado muestra que 2001:DB8:1111:2200::/64 (la LAN para Spoke2) está disponible a través de 2001:DB8:0:FFFE::, que es la dirección IPv6 negociada en la interfaz Tunnel1 para Spoke2. La interfaz Tunnel1 está disponible a través de la dirección de acceso múltiple sin difusión (NBMA) de 2001:db8:0:200::2 , que es la dirección IPv6 asignada estáticamente a Spoke2.

- Verifique que el tráfico esté pasando a través de esa interfaz:

```
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 la ruta de ruteo y la configuración 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

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

> **Nota:** Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

Estos comandos debug le ayudan a resolver problemas:

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

Consulte Lista de Comandos Principal de Cisco IOS, Todas las Versiones para obtener más información sobre estos comandos.