FlexVPN: IPv6 en un ejemplo de la configuración de despliegue del hub and spoke

Contenido

Introducción

Este documento describe una configuración común que utilice el Cisco IOS que el ® FlexVPN habló y despliegue del concentrador en un entorno del IPv6. Se amplía en los conceptos discutidos en [FlexVPN: IPv6 LAN básico a la configuración LAN](#).

Prerrequisitos

Requisitos

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.

- Generación 2 (ISR G2) del Routers de los Servicios integrados de Cisco
- Versión de Cisco IOS Software 15.3 (o versión 15.4T para los túneles dinámicos del spoke al spoke con el IPv6)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

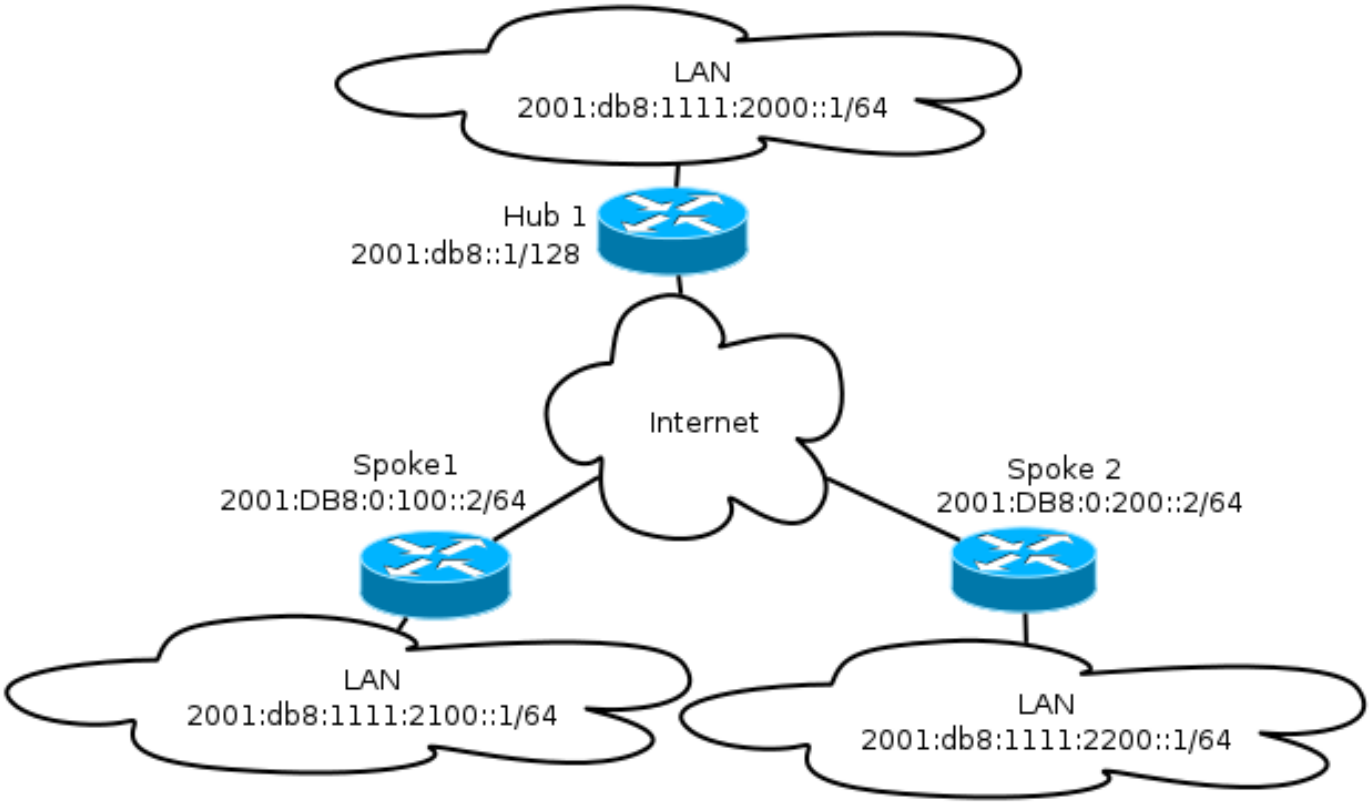
> Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Mientras que este ejemplo de configuración y diagrama de la red utilizan el IPv6 como la red de transporte, el Generic Routing Encapsulation (GRE) se utiliza típicamente en las implementaciones de FlexVPN. El uso del GRE en vez del IPSec permite que los administradores ejecuten el IPv4 o IPv6 o ambos sobre los mismos túneles, sin importar la red de transporte.

Diagrama de la red

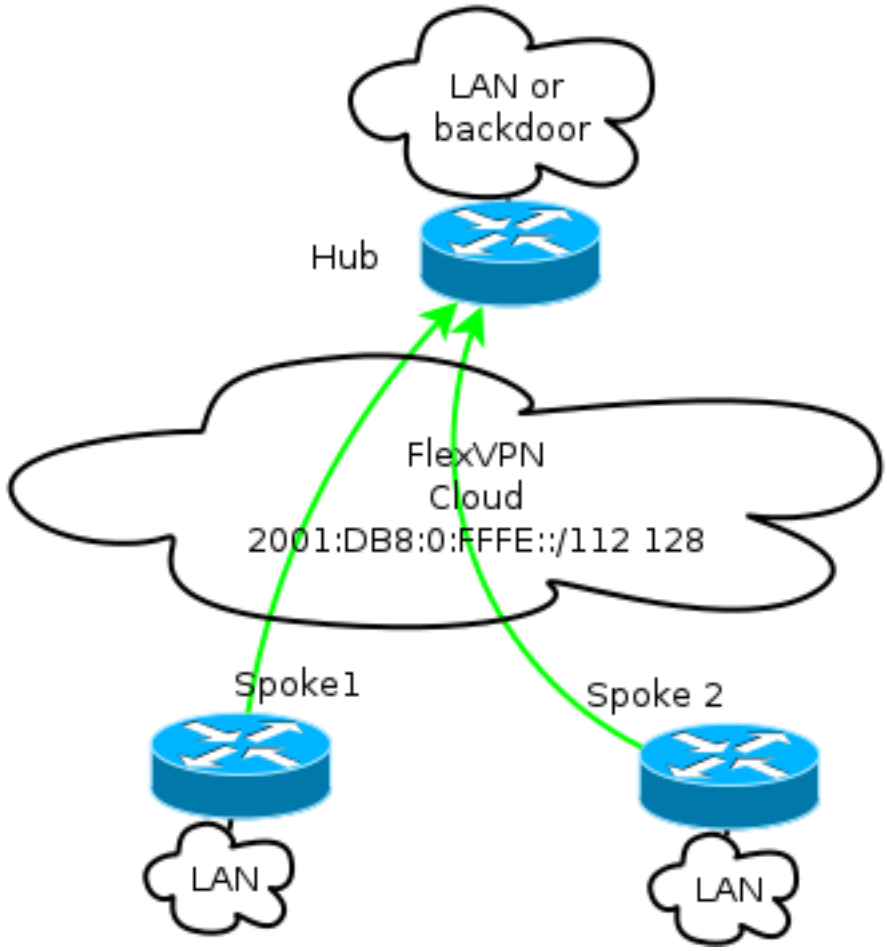
Red de transporte

Éste es un diagrama de la red de transporte usada en este ejemplo:



Red de recubrimiento

Éste es un diagrama de la topología de red básica del recubrimiento usada en este ejemplo:



Cada spoke se asigna de una agrupación de direcciones de /112, pero recibe un direccionamiento de /128. Así, la notación '/112 128' se utiliza en configuración de agrupación del IPv6 del concentrador.

Configuraciones

Esta configuración muestra un IPv4 y el IPv6 cubiertos que trabaja sobre una estructura básica del IPv6.

Cuando está comparado a los ejemplos que utilizan el IPv4 como estructura básica, observe que usted debe utilizar el cambio del nodo del **comando tunnel mode** para y acomodar el transporte del IPv6.

La característica del túnel del spoke al spoke sobre el IPv6 será introducida en el Cisco IOS Software Release 15.4T, que no está todavía disponible.

Protocolos de ruteo

Cisco recomienda que usted utiliza el Internal Border Gateway Protocol (iBGP) para mirar entre el spoke y el Hubs para las implementaciones grandes porque el iBGP es la mayoría del protocolo del ruteo escalable.

El Border Gateway Protocol (BGP) escucha rango no soporta el rango del IPv6, pero simplifica el uso con un transporte del IPv4. Aunque sea posible utilizar el BGP en tal entorno, esta configuración ilustra un ejemplo básico, así que el Enhanced Interior Gateway Routing Protocol (EIGRP) fue elegido.

Configuración del hub

Comparado a más viejos ejemplos, esta configuración incluye el uso de los nuevos protocolos de transporte.

Para configurar el concentrador, el administrador necesita:

- Unicast Routing del permiso.
- Encaminamiento del transporte de la disposición.
- Provision un nuevo pool de los direccionamientos del IPv6 que se asignarán dinámicamente. El pool es 2001:DB8:0:FFFE::/112; 16 bits permiten para que 65,535 dispositivos sean dirigidos.
- Permita al IPv6 para la configuración del Next Hop Resolution Protocol (NHRP) para permitir el IPv6 en el recubrimiento.
- Explique el IPv6 que dirige en el llavero así como el perfil en la configuración de criptografía.

En este ejemplo, el concentrador hace publicidad de un resumen del EIGRP a todo el spokes.

Cisco no recomienda el uso de una dirección de resumen en la interfaz de plantilla virtual en el despliegue de FlexVPN; sin embargo, en un Dynamic Multipoint VPN (DMVPN), esto es no sólo común pero también se considera una mejor práctica. Vea la migración de FlexVPN: Movimiento duro del DMVPN a FlexVPN en los mismos dispositivos: Configuración del hub actualizada para

los 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 radial

Como en la Configuración del hub, el administrador necesita provision la dirección del IPv6, el IPv6 del permiso ruteando, y agrega el NHRP y la configuración de criptografía.

Es posible utilizar el EIGRP y otros Routing Protocol para el peering del spoke al spoke. Sin embargo, en un escenario típico, los protocolos no son necesarios y pudieron afectar el scalability y la estabilidad.

En este ejemplo, la configuración de ruteo guarda solamente la adyacencia del EIGRP entre el spoke y el concentrador, 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 usted crea las entradas del Routing Protocol en un spoke:

1. Permita que el Routing Protocol establezca una relación vía la conexión (en este caso, la interfaz Tunnel1) al concentrador. No es generalmente deseable establecer la adyacencia de la encaminamiento entre el spokes porque éste aumenta perceptiblemente la complejidad en la mayoría de los casos.

2. Haga publicidad de las subredes del LAN local solamente, y habilite el Routing Protocol en una dirección IP asignada por el concentrador. Tenga cuidado de no hacer publicidad de una subred grande porque puede ser que afecte la comunicación del spoke al spoke.

Este ejemplo refleja ambas recomendaciones para el EIGRP en el Spoke1:

```
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
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

> Nota: La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Sesión del spoke a hub

Una sesión correctamente configurada entre el spoke y los dispositivos del concentrador tiene una sesión del intercambio de claves de Internet versión 2 (IKEv2) que sea ascendente y tiene un Routing Protocol que pueda establecer la adyacencia. En este ejemplo, el Routing Protocol es EIGRP, tan allí es dos comandos eigrp:

- muestre ikev2 crypto sa
- muestre al vecino del eigrp 65001 del IPv6
- muestre al vecino del eigrp 65001 del IP

```
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 el IPv4, el EIGRP utiliza un IP Address asignado para mirar; en el ejemplo anterior, es la dirección IP del concentrador de 10.1.1.1.

El IPv6 utiliza a una dirección local del link; en este ejemplo, el concentrador es FE80::A8BB:CCFF:FE00:6600. Utilice el comando ping para verificar que el concentrador se puede alcanzar a través de su IP del local de la conexión:

```
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 del spoke al spoke

Se sacan a colación las sesiones del spoke al spoke dinámicamente a pedido. Utilice un comando de ping simple para accionar una sesión:

```
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
```

Para confirmar la Conectividad directa del spoke al spoke, el administrador necesita:

- Verifique que una sesión dinámica del spoke al spoke accione 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 al 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 secObserve que dos sesiones están disponibles: un spoke a hub y un spoke al spoke.
```

- Verifique el 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::2La salida muestra que 2001:DB8:1111:2200::/64 (el LAN para el Spoke2) está disponible vía 2001:DB8:0:FFFE:: , que es el direccionamiento negociado del IPv6 en la interfaz Tunnel1 para el Spoke2. La interfaz Tunnel1 está disponible vía el direccionamiento del acceso múltiple sin broadcast (NBMA) de 2001:db8:0:200::2, que es el direccionamiento del IPv6 asignado al Spoke2 estáticamente.
```

- Verifique que el tráfico esté pasando vía 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 trayectoria de ruteo y las configuraciones 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
```

Troubleshooting

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 los problemas:

- FlexVPN/IKEv2 y IPSec: **debug crypto ipsecdebug crypto ikev2 [paquete|interno]**
- NHRP (spoke al spoke):
  - **paquete del nhrp del debug**
  - **extensión del nhrp del debug**
  - **caché del nhrp del debug**
  - **ruta del nhrp del debug**

Refiera al Cisco IOS comando list principal, todas las versiones para más información sobre estos comandos.