Configuración y verificación de la solución FlexVPN

Contenido

Introducción

Este documento describe el entorno de red privada virtual Flex, presenta sus funciones y explica cómo configurar cada topología de FlexVPN.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco IOS y Cisco IOS XE
- Intercambio de claves de Internet (IKE) versión 2
- Seguridad de protocolo de Internet (IPsec)
- FlexVPN

Componentes Utilizados

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

- Cisco IOS XE Amsterdam-17.3.6

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

FlexVPN es una solución de VPN versátil y completa proporcionada por Cisco, diseñada para ofrecer un marco unificado para varios tipos de conexiones VPN. Basada en el protocolo IKEv2 (Intercambio de claves de Internet versión 2), FlexVPN está diseñada para simplificar la configuración, la gestión y la implementación de VPN, aprovechando un conjunto uniforme de herramientas. Los mismos comandos y pasos de configuración se aplican a través de diferentes tipos de VPN (de sitio a sitio, acceso remoto, etc.). Esta coherencia ayuda a reducir los errores y hace que el proceso de implementación sea más intuitivo.

IKEv2 frente a IKEv1

FlexVPN utiliza IKEv2, que admite algoritmos criptográficos modernos como AES (estándar de cifrado avanzado) y SHA-256 (algoritmo hash seguro). Estos algoritmos proporcionan cifrado sólido e integridad de los datos, lo que protege los datos transmitidos a través de la VPN de ser interceptados o manipulados.

IKEv2 ofrece más métodos de autenticación en comparación con IKEv1. Además de los tipos de autenticación híbrida y basada en certificados (PSK) y de clave precompartida, IKEv2 permite al personal de respuesta utilizar el protocolo de autenticación ampliable (EAP) para la autenticación de clientes.

En FlexVPN, EAP se utiliza para la autenticación de clientes; el router actúa como un relé, pasando mensajes EAP entre el cliente y el servidor EAP de back-end, normalmente un servidor RADIUS. FlexVPN admite varios métodos EAP, incluidos EAP-TLS, EAP-PEAP, EAP-PSK y otros, para proteger el proceso de autenticación.

La tabla muestra las diferencias entre las funciones IKEv1 e IKEv2:

	IKEv2	IKEv1
Mensajes de establecimiento de protocolo	4 mensajes	6 mensajes
Compatibilidad con EAP	Sí (2 mensajes adicionales)	No
Negociación para asociaciones de seguridad	2 mensajes adicionales	3 mensajes adicionales
Ejecutar mediante UDP 500/4500	Yes	Yes
NAT transversal (NAT-T)	Yes	Yes
Funciones de retransmisiones y reconocimiento	Yes	Yes
Proporcione protección de identidad, un mecanismo de protección frente a DoS y Perfect Forward Secrecy (PFS)	Yes	Yes
Compatibilidad con cifrado de última generación	Yes	No

Escalabilidad

FlexVPN puede ampliarse fácilmente de pequeñas oficinas a redes de grandes empresas. Esto lo convierte en la opción ideal para organizaciones con un número significativo de usuarios remotos que requieren un acceso a la red seguro y fiable.

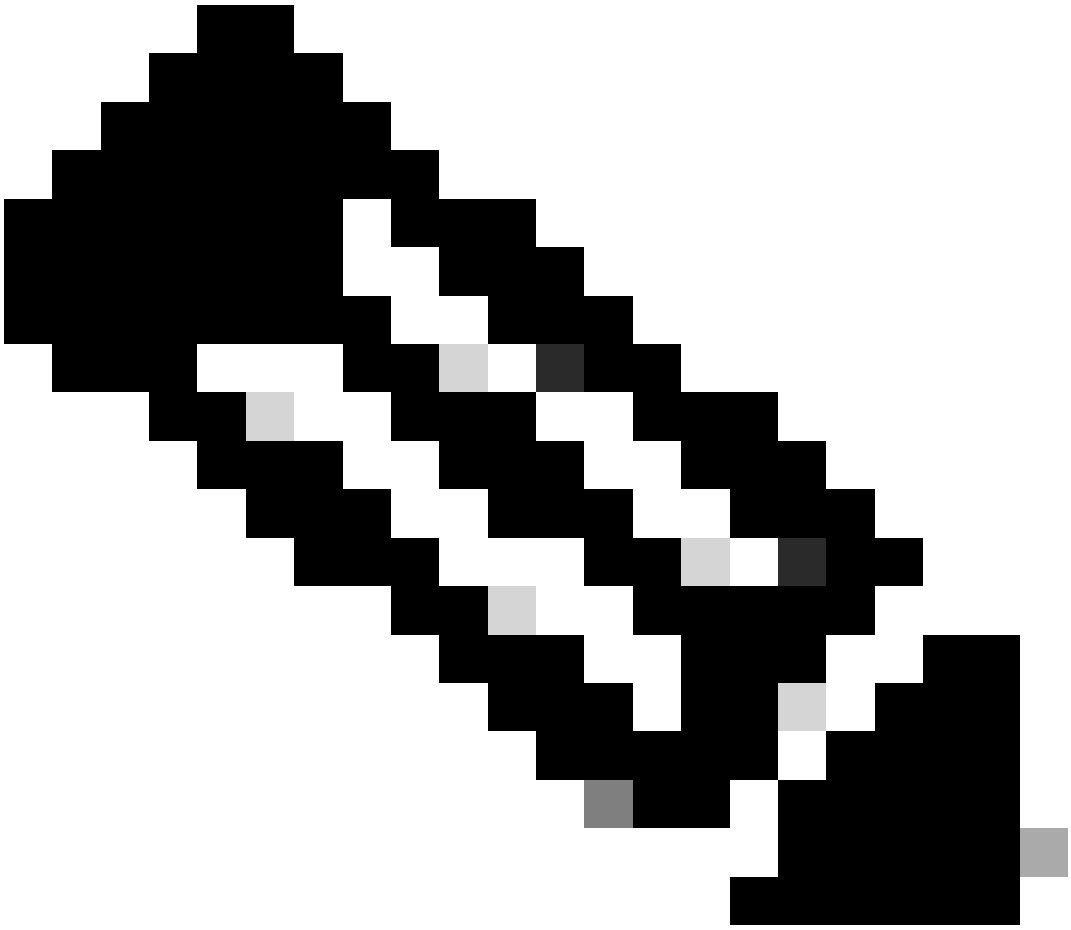
Funciones esenciales

- Configuración dinámica y túneles a demanda:
  - Cuando se inicia la conexión FlexVPN, el sistema genera una interfaz de acceso virtual basada en una plantilla preconfigurada. Esta interfaz actúa como extremo del túnel durante la conexión. Una vez que ya no se necesita el túnel, se desactiva la interfaz de acceso virtual, lo que libera los recursos del sistema.

- Flexibilidad en la implementación:
  - Modelo de hub y radio: Un hub central se conecta a varias sucursales. FlexVPN simplifica la configuración de estas conexiones con una única estructura, lo que la convierte en la opción ideal para redes de gran tamaño.
  - Topologías de malla completa y de malla parcial: Todos los sitios se pueden comunicar directamente sin pasar por un hub central, lo que reduce el retraso y mejora el rendimiento.

- Alta disponibilidad y redundancia:
  - Concentradores redundantes: Admite varios concentradores para realizar copias de seguridad. Si un hub falla, las sucursales pueden conectarse a otro hub, lo que garantiza una conectividad continua.

- Equilibrio de carga: Esto distribuye las conexiones VPN a través de varios dispositivos para evitar que cualquier dispositivo individual se sobrecargue, lo cual es crucial para mantener el rendimiento en grandes implementaciones.



Nota: La siguiente guía proporciona más información sobre la configuración del equilibrio de carga para la conexión de concentradores.

Configuración del equilibrador de carga IKEv2

- Autenticación y autorización escalables:
  - Integración de AAA: Funciona con servidores AAA como Cisco ISE o RADIUS para la gestión centralizada de credenciales y políticas de usuario, esencial para un uso a gran escala.
  - PKI y certificados: Admite infraestructura de clave pública (PKI) y certificados digitales para una autenticación segura, que es más escalable que el uso de clave precompartida, especialmente en entornos grandes.

Ruteo

La funcionalidad de routing de FlexVPN está diseñada para mejorar la escalabilidad y gestionar de forma eficaz varias conexiones VPN y permitir una forma dinámica de enrutar el tráfico a cada una de ellas. Los siguientes componentes y mecanismos clave que hacen que el ruteo FlexVPN sea eficiente:

- Interfaz de plantilla virtual: Se trata de una plantilla de configuración que incluye todos los parámetros necesarios para una conexión VPN, como la asignación de direcciones IP, el origen del túnel y los parámetros de IPsec. En esta interfaz se configura el`ip unnumbered`comando para tomar prestada una dirección IP, normalmente de un loopback en lugar de configurar una dirección IP específica como origen del túnel. Esto permite que cada radio utilice la misma plantilla, lo que permite que cada radio utilice su propia dirección IP de origen.

- Interfaz de acceso virtual: Se trata de interfaces creadas dinámicamente que heredan su configuración de la interfaz de plantilla virtual. Cada vez que se establece una nueva conexión VPN, se crea una nueva interfaz de acceso virtual basada en la plantilla virtual. Esto significa que cada sesión VPN tiene su propia interfaz única, lo que simplifica la gestión y la escalabilidad.

- Protocolos de enrutamiento dinámico: Funciona con protocolos de ruteo como OSPF, EIGRP y BGP sobre túneles VPN. Esto mantiene la información de ruteo actualizada automáticamente, lo cual es importante para las redes grandes y dinámicas.

- IKEv2 anuncia las rutas permitiendo que el servidor FlexVPN inserte los atributos de red al cliente, que instala estas rutas en la interfaz de túnel. El cliente también comunica sus propias redes al servidor durante el intercambio de modo de configuración, habilitando las actualizaciones de ruta en ambos extremos.

- NHRP (protocolo de resolución de próximo salto) es un protocolo de resolución de dirección dinámica que se utiliza en topologías radiales y de concentrador para asignar direcciones IP públicas a terminales VPN privados. Permite a los spokes detectar otras direcciones IP de spokes para la comunicación directa.

Política de autorización

Se puede configurar una política de autorización IKEv2 para FlexVPN para controlar diversos aspectos de la conexión VPN. Una directiva de autorización IKEv2 define la directiva de autorización local y contiene atributos locales o remotos:

- Los atributos locales, como el routing y reenvío de VPN (VRF) y la política de QoS, se aplican de forma local.
- Los atributos remotos, como las rutas, se envían al par a través del modo de configuración.
- Utilice el comando crypto ikev2 authorization policy para definir la política local.
- La política de autorización IKEv2 se remite desde el perfil IKEv2 a través del comando AAA authorization.

Esta tabla proporciona una descripción general de los parámetros clave que se pueden configurar en la directiva de autorización IKEv2.

Parámetro	Descripción
AAA	Integración con servidores AAA para validar las credenciales del usuario, autorizar el acceso y dar cuenta del uso. La política puede especificar si la validación se realiza localmente en el router o remotamente, como a través de un servidor RADIUS.
Configuración del Cliente	Envía los valores de configuración al cliente, como valores de tiempo de espera inactivo, señales de mantenimiento, asignación de servidor DNS y WINS, etc.
Configuración específica del cliente	Permite configuraciones diferentes para clientes diferentes en función de su identidad o pertenencia a grupos.
Conjunto de rutas	Esta configuración permite que cierto tráfico pase a través del túnel VPN. Esto realiza la inyección de ruta que se envía al cliente VPN tras una conexión exitosa.

FlexVPN frente a otras tecnologías

FlexVPN ofrece una serie de ventajas que lo convierten en una opción atractiva para los entornos de red modernos. Al proporcionar un marco unificado, FlexVPN simplifica la configuración y la gestión, mejora la seguridad, admite la escalabilidad, garantiza la interoperabilidad y reduce la complejidad.

	Mapa criptográfico	DMVPN	FlexVPN
Routing dinámico	No	Yes	Yes
Directo de radio a radio dinámico	No	Yes	Yes
VPN de acceso remoto	Yes	No	Yes
Transferencia de configuración	No	No	Yes
Configuración Peer-peer	No	No	Yes
QoS de peer-peer	No	Yes	Yes
Integración de servidor AAA	No	No	Yes

Diagrama de la red

FlexVPN permite la creación de túneles entre dispositivos, estableciendo la comunicación entre el concentrador y los radios. También permite la creación de túneles para la comunicación directa entre radios y la conexión de usuarios de VPN de acceso remoto, como se muestra en el diagrama.

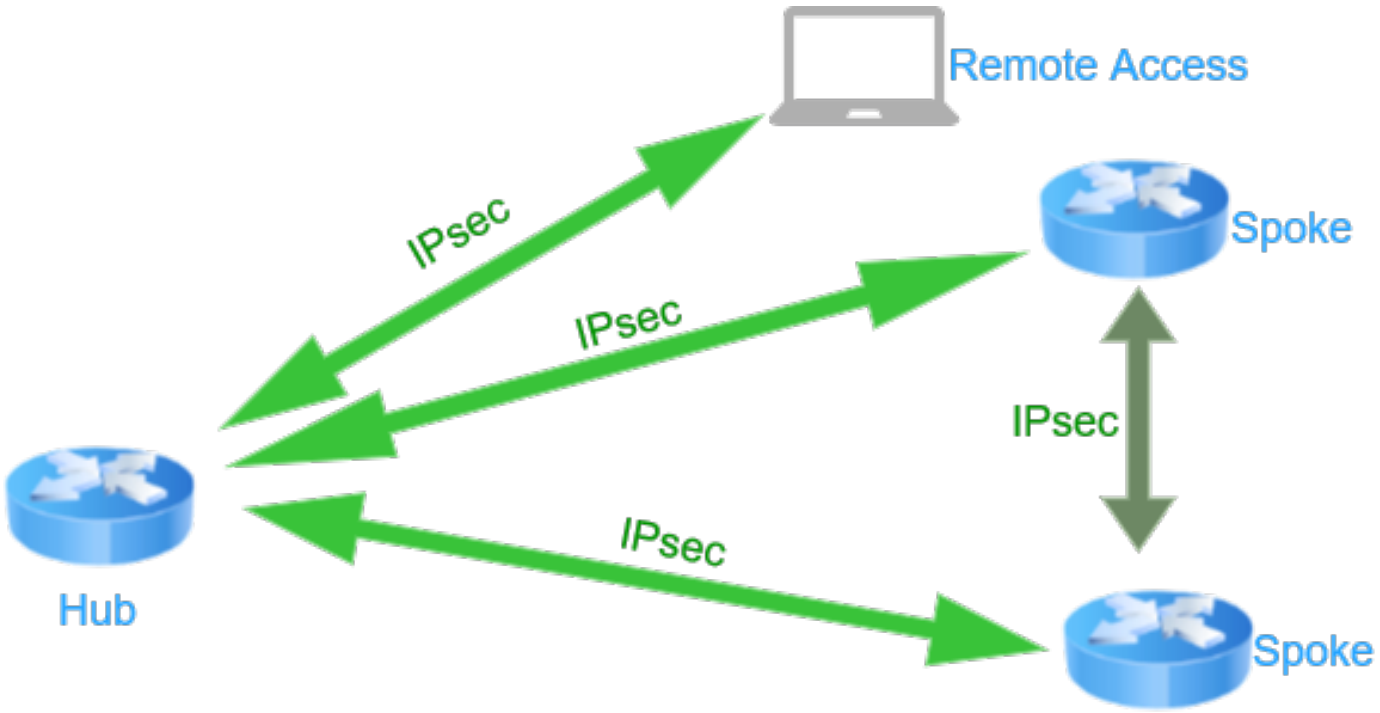
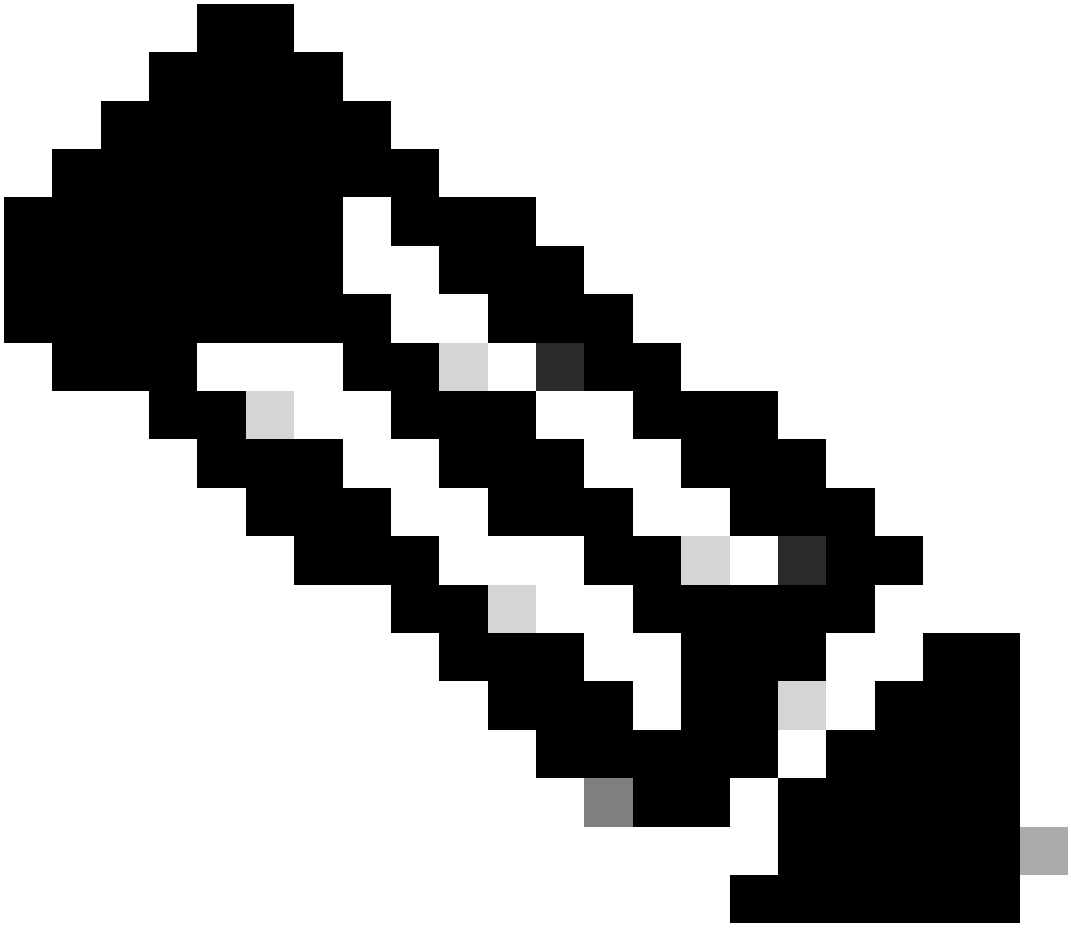


Diagrama de FlexVPN



Nota: La configuración de VPN de acceso remoto no se trata en esta guía. Para obtener más información sobre su configuración, consulte la guía:

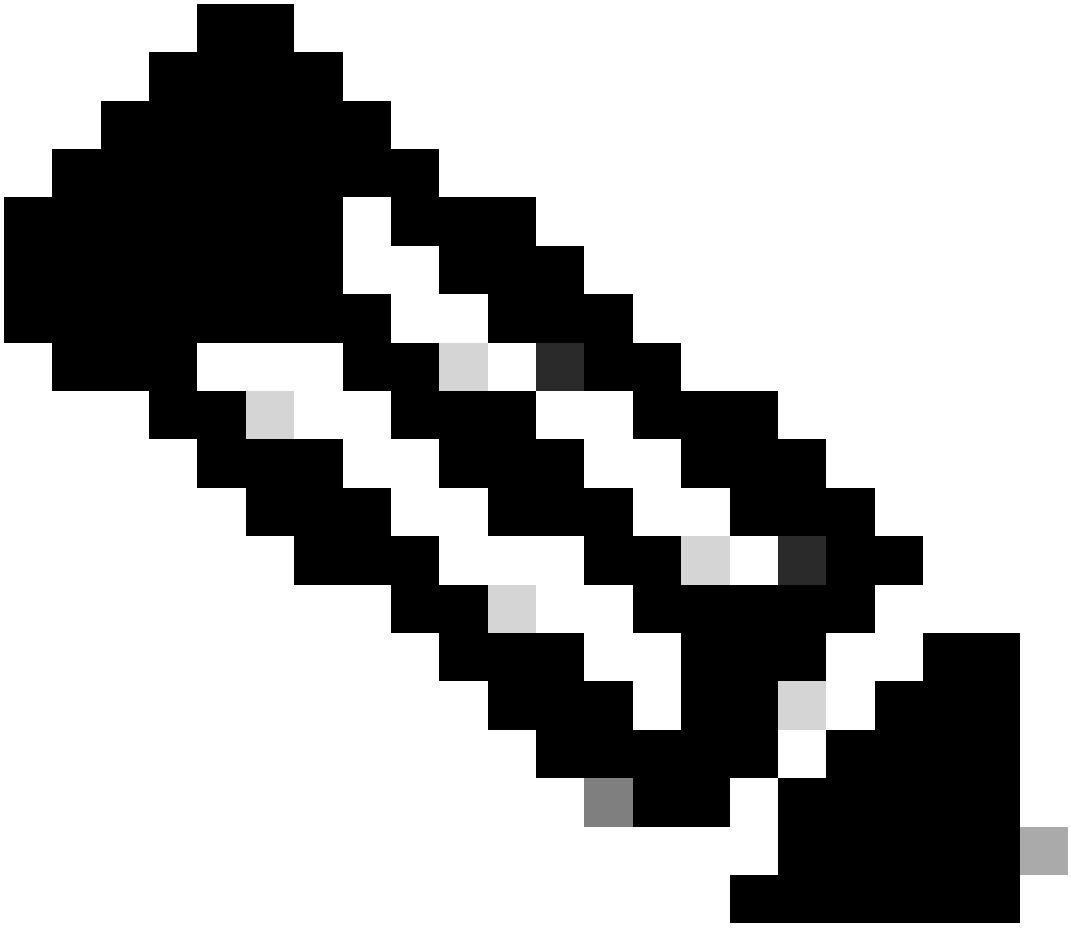
Configuración del equipo de cabecera FlexVPN para acceso remoto IKEv2 de cliente seguro (AnyConnect) mediante la base de datos de usuarios locales

Configurar

FlexVPN se caracteriza por la sencillez de su configuración. Esta simplicidad es evidente en los bloques de configuración consistentes utilizados para varios tipos de VPN. FlexVPN proporciona bloques de configuración sencillos que suelen aplicarse, con configuraciones opcionales o pasos adicionales disponibles en función de las características o requisitos específicos de la topología:

- Propuesta IKEv2: Define los algoritmos utilizados en la negociación de la asociación de seguridad (SA) IKEv2. Una vez creada, adjunte esta propuesta a una política IKEv2 para que se pueda seleccionar durante la negociación.

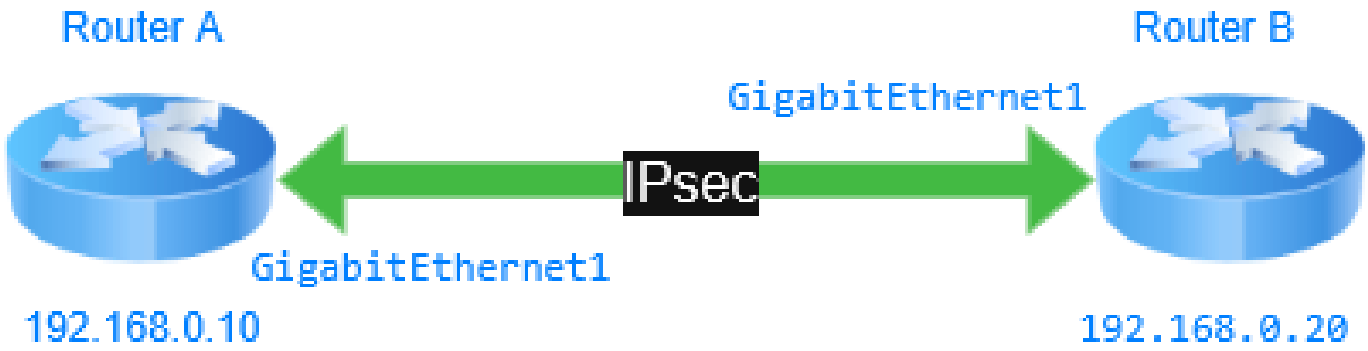
- Política IKEv2: Vincula la propuesta a una instancia de Virtual Routing and Forwarding (VRF) o a una dirección IP local. El enlace de políticas a la propuesta IKEv2.
- Anillo de claves IKEv2: Especifica claves previamente compartidas (PSK), que pueden ser asimétricas si se utilizan para la autenticación de pares.
- Punto de confianza (opcional): Configura la identidad y los atributos de la autoridad certificadora (CA) para la autenticación de pares cuando se utiliza la infraestructura de clave pública (PKI) como método de autenticación.
- Integración de AAA (opcional): FlexVPN integra servidores AAA, como Cisco ISE (Identity Services Engine) o servidores RADIUS como método de autenticación.
- Perfil IKEv2: Almacena parámetros no negociables de la SA IKE, como la dirección del par VPN y los métodos de autenticación. No hay ningún perfil IKEv2 predeterminado, por lo que debe configurar uno y asociarlo a un perfil IPsec en el iniciador. Si se utiliza la autenticación PSK, el perfil IKEv2 hace referencia al anillo de claves IKEv2. Si se utiliza la autenticación PKI o el método de autenticación AAA, se hace referencia aquí.
- Conjunto de transformación IPsec: Especifica una combinación de algoritmos aceptable para la SA IPSec.
- Perfil IPsec: Consolida la configuración de FlexVPN en un único perfil que se puede aplicar a una interfaz. Este perfil hace referencia al conjunto de transformación IPsec y al perfil IKEv2.



Nota: Los ejemplos de configuración utilizan claves previamente compartidas para proporcionar una demostración directa de la configuración y simplicidad de FlexVPN. Mientras que las claves previamente compartidas se pueden emplear para una implementación sencilla y topologías pequeñas, los métodos AAA o PKI son más adecuados para topologías más grandes.

Configuración de FlexVPN de sitio a sitio

La topología de sitio a sitio de FlexVPN está diseñada para conexiones VPN directas entre dos sitios. Cada sitio está equipado con una interfaz de túnel que establece un canal seguro a través del cual el tráfico puede fluir. La configuración explica cómo establecer una conexión VPN directa entre dos sitios, como se muestra en el diagrama.



Diagrama_de_sitio_a_sitio

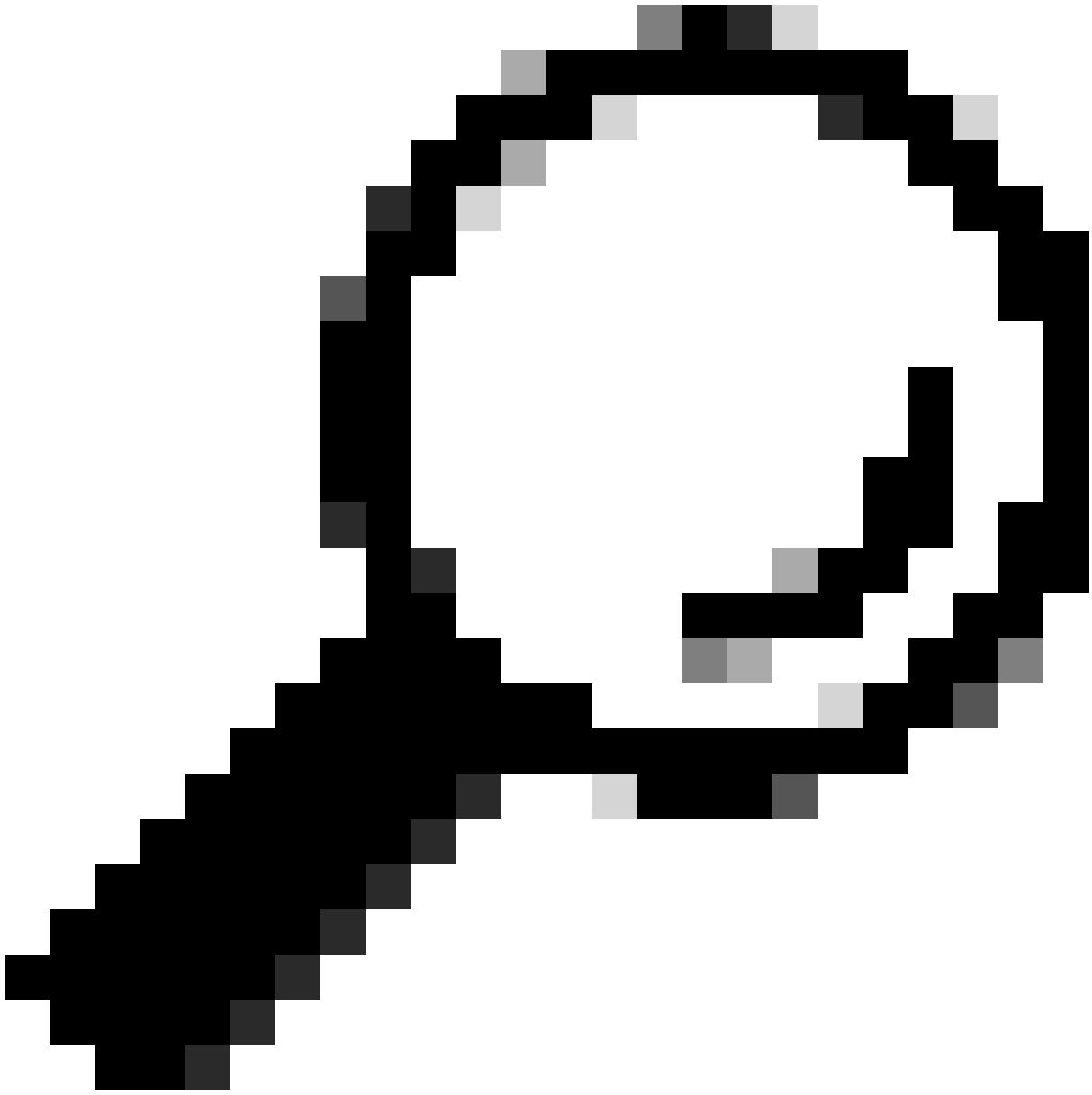
Paso 1: Configuración del router A

a. Definir propuesta y política IKEv2.

b. Configure un llavero e ingrese un nombre Pre-Shared Key que se utilice para autenticar al par.

c. Cree un IKEv2 profile y asigne el 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
!
```



Consejo: La **IKEv2 Smart Defaults** función minimiza laFlexVPNconfiguración al cubrir la mayoría de los casos prácticos. Puede personalizar **IKEv2 Smart Defaults** para casos prácticos específicos, aunque Cisco no recomienda esta práctica.

---

d. Cree un Transport Set y defina los algoritmos de cifrado y hash utilizados para proteger los datos.

e. Cree un **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 la interfaz de 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 el enrutamiento dinámico para anunciar la interfaz de túnel. Después de eso, puede anunciar otras redes que deben pasar a través del túnel.

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

Paso 2: Configuración del Router B

a. Definir propuesta y política IKEv2.

b. Configure un keyring y escriba un nombre Pre-Shared Key que se utilice para autenticar el par.

c. Cree un IKEv2 profile y asigne el 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. Cree un Transport Set y defina los algoritmos de cifrado y hash utilizados para proteger los datos.

e. Crear y IPsec profile asignar el perfil IKEv2 y el conjunto de transformación creados 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 el 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 el enrutamiento dinámico para anunciar la interfaz de túnel. Después de eso, puede anunciar otras redes que deben pasar a través del túnel.

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

Verificación

- Utilice el comando show ip interface brief para revisar el estado de la interfaz de túnel y

verificar que el túnel se encuentre en un estado 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. Utilice el comando show crypto ikev2 sa para confirmar que se ha establecido la conexión segura entre los routers.

<#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
```

- Utilice el comando show crypto ipsec sa para confirmar que el tráfico está cifrado y que pasa a través del túnel, verificando que los contadores encaps y decaps están 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:
```

- Utilice el comando show ip eigrp neighbors para confirmar que la adyacencia EIGRP se establece con el otro sitio.

```
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 de hub y radio

En la topología de hub y spoke, varios routers spoke se conectan a un router hub central. Esta configuración es óptima para escenarios donde los radios se comunican principalmente con el hub. En FlexVPN, los túneles dinámicos se pueden configurar para mejorar la eficacia de la comunicación. El hub utiliza el routing IKEv2 para distribuir rutas a los routers radiales, lo que garantiza una conectividad perfecta. Como se indica en el diagrama, la configuración explica la conexión VPN entre un hub y un spoke y cómo el hub se configura para establecer una conexión dinámica con varios spokes y es capaz de agregar más spokes.

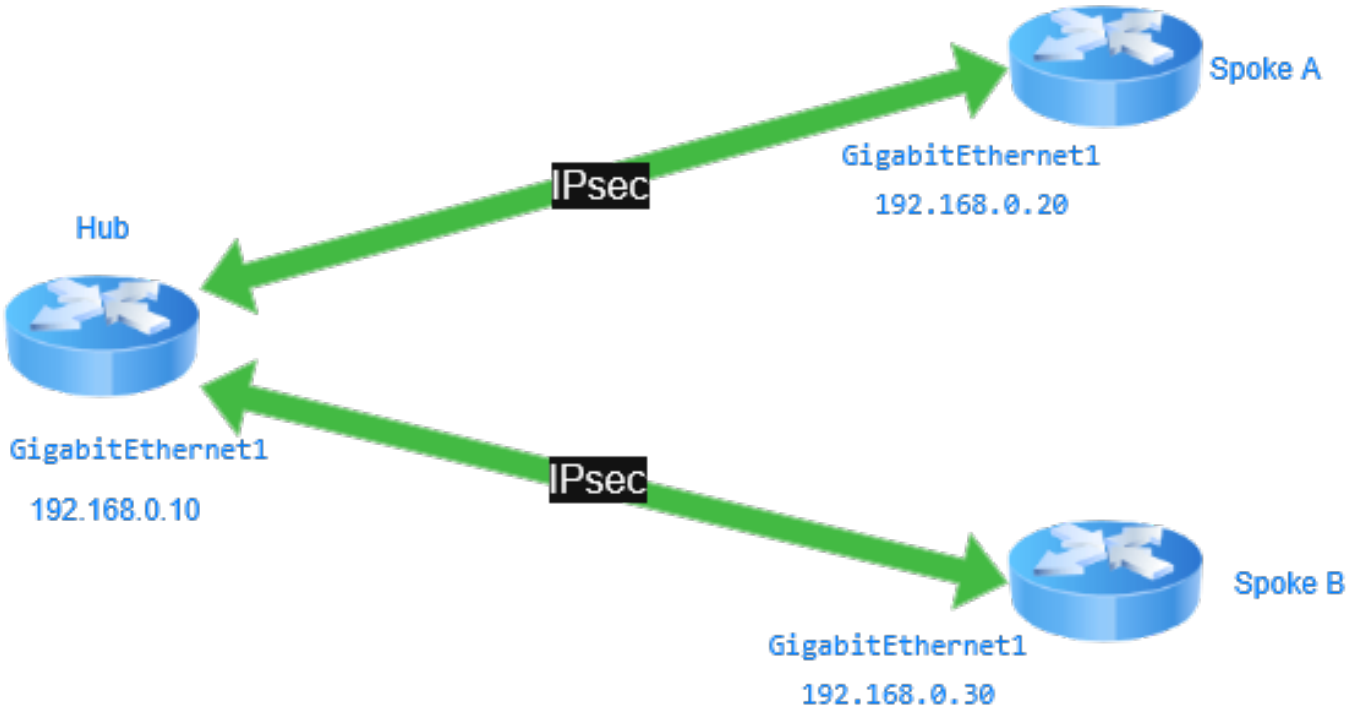


Diagrama Hub_and_Spoke_Diagram

Paso 1: Configuración del hub

a. Definir propuesta y política IKEv2.

b. Configure un keyring e ingrese un nombre Pre-Shared Key que se utilice para autenticar los radios.

```
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. Habilite los servicios AAA en el router Hub y, a continuación, defina una lista de autorización de red denominadaFlexAuthque especifique las políticas de la configuración del dispositivo local.

```
!
aaa new-model
```

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

d. Defina unIP address poolnamedFlexPool, que contiene las direcciones 10.1.1.2 a 10.1.1.254. Este pool se utiliza para asignar automáticamente una dirección IP a la interfaz de túnel de los spokes.

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

e. Defina una lista de acceso IP estándar con el nombreFlexTrafficy que permita la red 10.10.1.0/24. Esta ACL define las redes que se envían a los spokes de FlexVPN para alcanzarlas a través del túnel.

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

La lista de acceso y el conjunto de direcciones IP se mencionan en la **IKEv2 Authorization Policy**.

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

f. Cree un IKEv2 profile, asigne el grupo de autorización keyring y 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 Cree una Transport Set, defina los algoritmos de cifrado y hash utilizados para proteger los datos.

h. Cree un IPsec profile, asigne el IKEv2 profile y Transport Set creado 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 el **virtual-template 1** as **type tunnel**. Haga referencia a la interfaz como unaIP unnumbered addressy aplique el **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
!
```

Paso 2: Configuración de radio

a. Definir propuesta y política IKEv2.

b. Configure un anillo de claves e ingrese una clave previamente compartida que se utilice para autenticarse en el 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. Active los servicios AAA en el router del concentrador y, a continuación, defina una lista de autorización de red denominada **FlexAuth** que especifique las políticas de la configuración del dispositivo local. A continuación, configure la política de configuración de modo para enviar la dirección IP y las rutas a los spokes de FlexVPN.

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

d. Defina una lista de acceso IP estándar denominada **FlexTraffic** y permita que la red 10.20.2.0/24. Esta ACL define las redes compartidas por este spoke para pasar a través del túnel.

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

La lista de acceso se asigna en el **IKEv2 Authorization Policy**.

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

e. Cree un IKEv2 profile, asigne el grupo de autorización keyring y 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. Cree un conjunto de transporte y defina los algoritmos de cifrado y hash utilizados para proteger los datos.

g. Cree un perfil IPsec, asigne el perfil IKEv2 y el conjunto de transporte creados 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 la interfaz de túnel con la propiedad de dirección IP negociada, que se obtiene del conjunto que configuró en el concentrador.

```
!
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
!
```

Verificación

Utilice el comando show ip interface brief para revisar el estado del túnel, la plantilla virtual y el acceso virtual:

- En el concentrador, la plantilla virtual tiene un estado activo/inactivo que es normal. Se crea un acceso virtual para cada radio que establece una conexión con el concentrador y muestra un estado up/up.
- En el radio, la interfaz del túnel recibe una dirección IP y muestra un estado 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
```

- Utilice el comando show crypto ikev2 sa para confirmar que se ha establecido la conexión segura entre el concentrador y el radio.

<#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
```

- Utilice el comando show crypto ipsec sa para confirmar que el tráfico está cifrado y que pasa a través del túnel, verificando que los contadores encaps y decaps están 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:
```

- Utilice el comando show ip route para verificar que las rutas se han enviado a los spokes:
  - La ruta para 10.1.1.1/32 se envió a través de cargas útiles de configuración IKEv2 debido a la instrucción de interfaz de conjunto de rutas en la configuración del HUB.
  - La ruta para 10.10.1.0/24 se envió mediante cargas útiles de configuración IKEv2 debido a la instrucción FlexTraffic de la lista de acceso del conjunto de rutas en la configuración del 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
```

- Utilice el comando ping para verificar la conectividad con las 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 de radio a radio

FlexVPN en una topología de hub y radio con conectividad de radio a radio permite una comunicación VPN dinámica, escalable y segura. El hub actúa como un punto de control centralizado donde NHRP permite que los spokes consulten al hub por otras direcciones IP de spokes, lo que habilita los túneles IPsec de spoke a spoke para una comunicación eficiente y una latencia reducida.

En el hub, el **ip nhrp redirect** comando se utiliza para notificar a los spokes que es posible la comunicación directa de spoke a spoke, lo que optimiza el flujo de tráfico al omitir el hub para el tráfico del plano de datos. En los spokes, el **ip nhrp shortcut** comando les permite establecer dinámicamente túneles directos con otros spokes después de recibir la redirección del hub. El diagrama hace referencia al tráfico entre el concentrador y el radio, y a la comunicación de radio a radio.

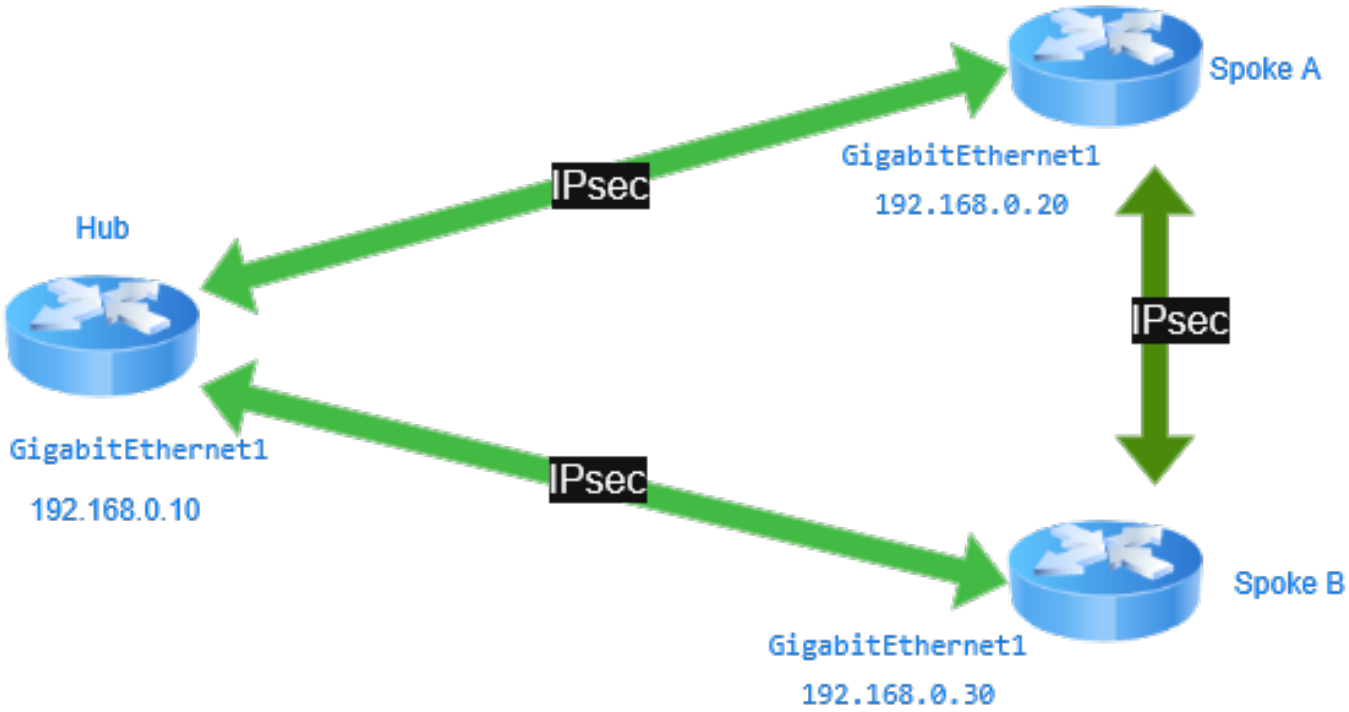


Diagrama de Spoke_to_Spoke

Paso 1: Configuración del hub

a. Definir perfiles y políticas IKEv2.

b. Configure un keyring e ingrese un nombre Pre-Shared Key que se utilice para autenticar los radios.

```
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. Habilite los servicios AAA en el router Hub, luego defina una lista de autorización de red denominada **FlexAuth** que especifique las políticas de la configuración del dispositivo local y luego configure la política de configuración de modo para enviar la dirección IP y las rutas a los spokes de FlexVPN.

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

d. Defina un nombreIP address pool **FlexPool**, que contenga las direcciones de la 10.1.1.2 a la 10.1.1.254. Este conjunto se utiliza para asignar automáticamente una dirección IP a la interfaz de túnel de los radios.

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

e. Defina una lista de acceso IP estándar denominadaFlexTrafficy que permita la red 10.0.0.0/8. Esta ACL define las redes que se envían a los spokes de FlexVPN, incluidas las redes para otros spokes conectados al Hub, de modo que los spokes sepan que esas redes se alcanzan primero a través del Hub.

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

La lista de acceso y IP address pool se asignan en la **IKEv2 Authorization Policy**.

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

f. Cree un IKEv2 profile, asigne el grupo de autorización keyring y 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 Cree un Transport Set y defina los algoritmos de cifrado y hash utilizados para proteger los datos.

h. Crear un IPsec profile, asignar el IKEv2 profile y creado Transport Set 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 el **virtual-template 1** as **type tunnel**. Haga referencia a la interfaz como un **IP unnumbered address** y aplique el **IPsec profile**.

El **ip nhrp redirect** comando se configura en la plantilla virtual para informar a los spokes que establezcan una conexión directa con otros spokes para alcanzar sus 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
!
```

Paso 2: Configuración de Spoke A

a. Definir perfiles y políticas IKEv2.

b. Configure un keyring e ingrese un nombre Pre-Shared Key que se utilice para autenticar los radios.

```
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. Active los servicios AAA en el router del concentrador y, a continuación, defina una lista de autorización de red denominada **FlexAuth** que especifique las políticas de la configuración del dispositivo local. A continuación, configure la política de configuración de modo para enviar la dirección IP y las rutas a los spokes de FlexVPN.

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

d. Defina una lista de acceso IP estándar denominada **FlexTraffic** y permita que la red 10.20.2.0/24. Esta ACL define las redes compartidas por este spoke para pasar a través del túnel.

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

La lista de acceso se asigna en el **IKEv2 Authorization Policy.**

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

e. Cree un IKEv2 profile, asigne el grupo de autorización keyring y 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. Cree un Transport Set y defina los algoritmos de cifrado y hash utilizados para proteger los datos.

g. Cree un perfil IPsec, asigne el perfil IKEv2 y el conjunto de transporte creados 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 la interfaz de túnel y la plantilla virtual. Especifique **Virtual-Template1** los dVTI que se crearán para admitir **NHRP shortcuts**. Además,tunnel0se establece como una dirección no numerada en elvirtual-template.

El **ip nhrp shortcut** comando se configura en los Spokes para permitirles establecer dinámicamente túneles directos a otros spokes basados en los mensajes de redirección NHRP del 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
!
```

Paso 3: Configuración de Spoke B

a. Definir perfiles y políticas IKEv2.

b. Configure un keyring e ingrese un nombre Pre-Shared Key que se utilice para autenticar los radios.

```
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. Habilite los servicios AAA en el router Hub, luego defina una lista de autorización de red denominada **FlexAuth** que especifique las políticas de la configuración del dispositivo local y luego configure la política de configuración de modo para enviar la dirección IP y las rutas a los spokes de FlexVPN.

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

d. Defina una lista de acceso IP estándar denominada **FlexTraffic** y permita que la red 10.30.3.0/24. Esta ACL define las redes compartidas por este spoke para pasar a través del túnel.

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

La lista de acceso se menciona en el IKEv2 Authorization Policy.

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

e. Cree un IKEv2 profile, asigne el grupo de autorización keyring y 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. Cree un Transport Set y defina los algoritmos de cifrado y hash utilizados para proteger los datos.

g. Cree un IPsec profile, asigne el IKEv2 profile y Transport Set creado 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 el tunnel interface y virtual template. Especifique **Virtual-Template1** para los dVTI que se crean para admitir NHRP shortcuts. Además,tunnel0se establece como una dirección no numerada en elvirtual-template.

El **ip nhrp shortcut** comando se configura en los Spokes para permitirles establecer dinámicamente túneles directos a otros spokes basados en los mensajes de redirección NHRP del 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
!
```

Verificación

Utilice el comando show ip interface brief para revisar el estado del túnel, la plantilla virtual y el acceso virtual. Ahora, se trata de una conexión directa de radio a radio:

- En los radios, la plantilla virtual tiene un estado activo/inactivo que es normal. Se crea un acceso virtual para la conexión en estado activo/activo.

<#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

- Utilice el comando show crypto ikev2 sa para confirmar que se ha establecido la conexión segura entre cada dispositivo.
- Utilice el comando show crypto ipsec sa para confirmar que el tráfico está cifrado y que pasa a través del túnel, verificando que los contadores encaps y decaps están aumentando.
- Utilice el comando show ip nhrp para verificar la redirección del tráfico entre los 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

Utilice el comando show ip route para verificar que las rutas se han enviado al spoke:

- Las dos rutas asociadas con la interfaz Virtual-Access1 son nuevas y están asociadas con los accesos directos NHRP.
- El carácter % indica una invalidación de salto siguiente.

<#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
```

- Utilice el comando ping para verificar la conectividad con las 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
```

Resolución de problemas

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

configuración. Utilice estos comandos para depurar el proceso de negociación de 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
```

Los debugs NHRP pueden ayudar con la resolución de problemas de las conexiones spoke a spoke.

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).