Ejemplo de Configuración de FlexVPN Spoke in Redundant Hub Design with FlexVPN Client Block

Contenido

Introducción

Este documento describe cómo configurar un spoke en una red FlexVPN con el uso del bloque de configuración del cliente FlexVPN en un escenario donde hay varios hubs disponibles.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- FlexVPN
- Protocolos de routing de Cisco

Componentes Utilizados

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

- Router de servicios integrados (ISR) de la serie G2 de Cisco
- Cisco IOS® versión 15.2M

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.

Antecedentes

Por motivos de redundancia, un spoke puede necesitar conectarse a varios hubs. La redundancia en el lado del radio permite un funcionamiento continuo sin un único punto de falla en el lado del hub.

Los dos diseños de hub redundantes FlexVPN más comunes que utilizan la configuración spoke son:

- **Enfoque de nube dual**, donde un spoke tiene dos túneles separados activos a ambos hubs en todo momento.
- **Enfoque de failover**, donde un spoke tiene un túnel activo con un hub en cualquier momento dado.

Ambos enfoques tienen un conjunto único de ventajas y desventajas.

Enfoque	Pros	Cons
Nube doble	• Recuperación más rápida en caso de fallo, basada en los temporizadores del protocolo de ruteo • Más posibilidades de distribuir el tráfico entre los concentradores, ya que las conexiones a ambos concentradores están activas	• Spoke mantiene la sesión en ambos concentradores al mismo tiempo, lo que consume recursos en ambos concentradores
Failover	• Configuración sencilla: integrada en FlexVPN • No confía en el protocolo de ruteo en una falla	• Tiempo de recuperación más lento basa en la detección de puntos inactivos (DP (opcionalmente) en el seguimiento de objetos • Todo el tráfico se ve obligado a desplazarse a un hub cada vez

Este documento describe el segundo enfoque.

Configurar

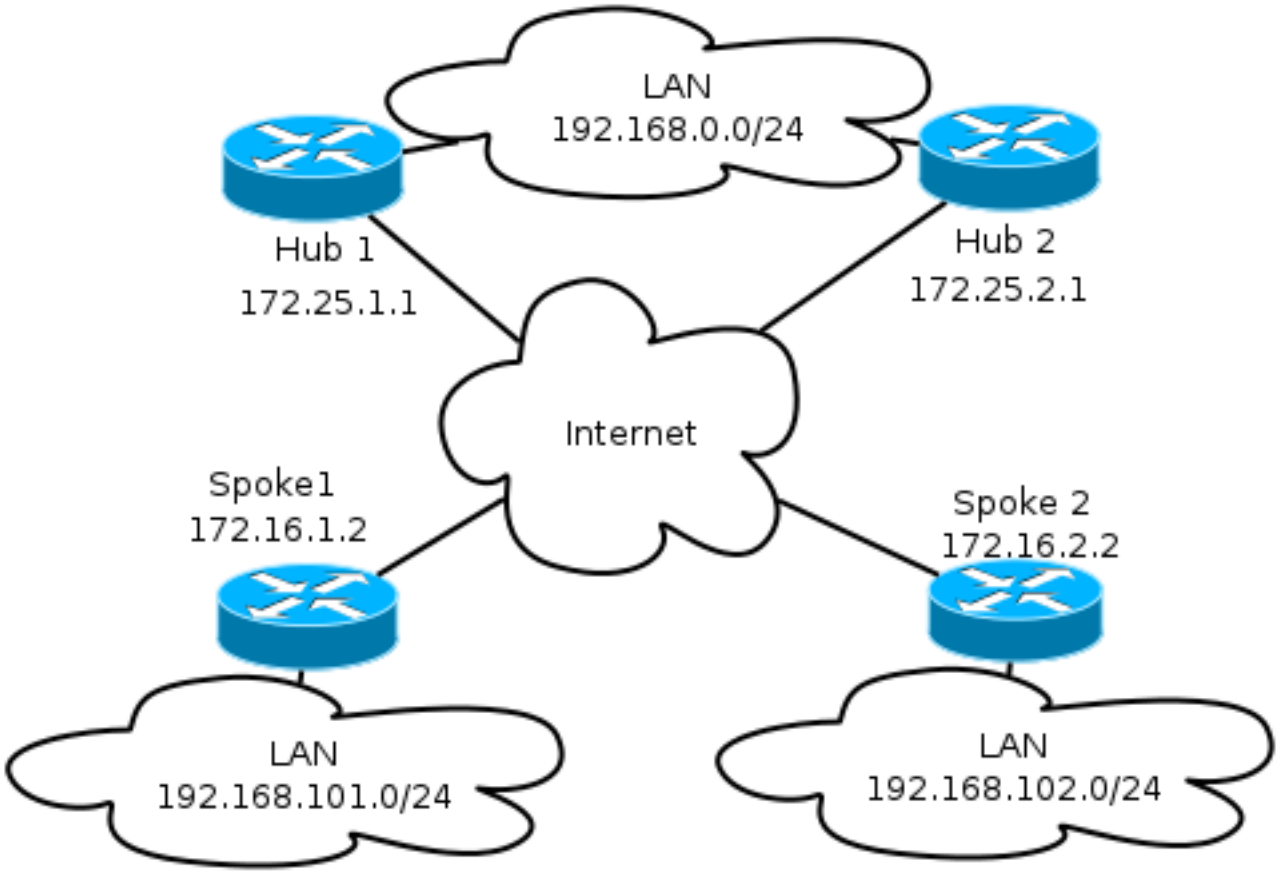
> **Nota:** Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagramas de la Red

Estos diagramas muestran los diagramas de topología de transporte y superposición.

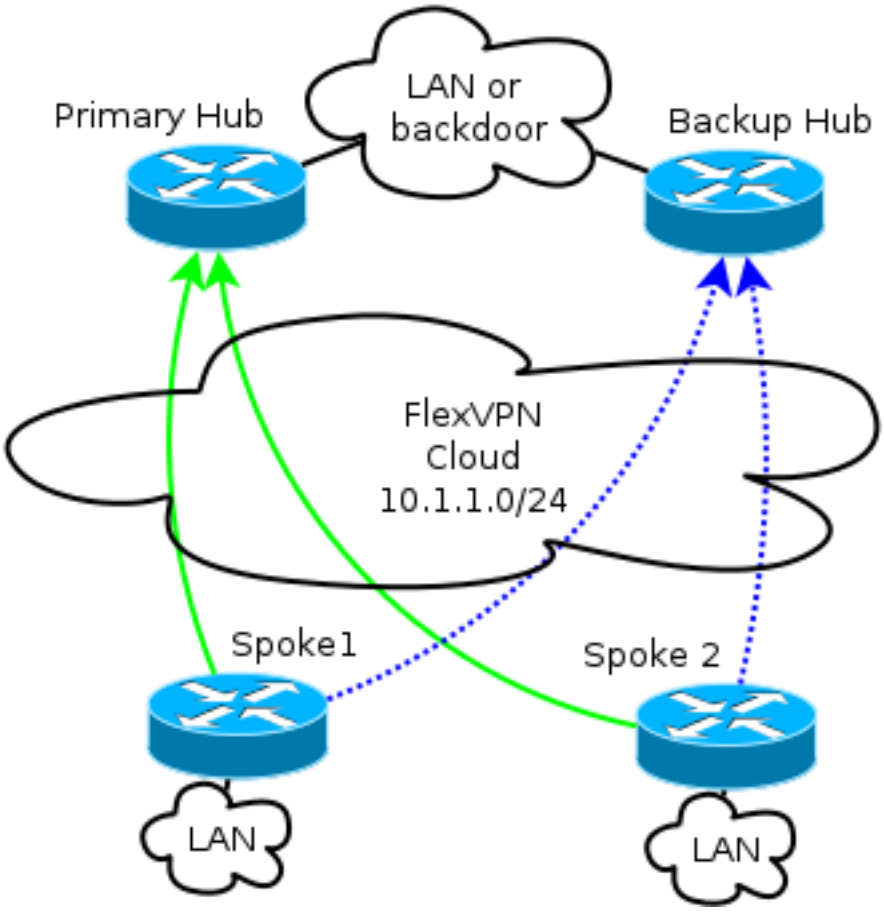
Red de transporte

Este diagrama ilustra la red de transporte básica que se suele utilizar en las redes FlexVPN.



Red superpuesta

Este diagrama ilustra la red superpuesta con conectividad lógica que muestra cómo debería funcionar la conmutación por fallas. Durante el funcionamiento normal, Spoke 1 y Spoke 2 mantienen una relación con un solo hub.



Nota: En el diagrama, las líneas verdes sólidas muestran la conexión y dirección de las sesiones principales de Intercambio de claves de Internet versión 2 (IKEv2)/Flex, y las líneas azules punteadas indican la conexión de respaldo en caso de que falle la sesión de Intercambio de claves de Internet (IKE) al hub principal.

El direccionamiento **/24** representa el conjunto de direcciones asignadas para esta nube, y no el direccionamiento de la interfaz real. Esto se debe a que el concentrador FlexVPN suele asignar una dirección IP dinámica a la interfaz spoke y depende de rutas insertadas dinámicamente a través de comandos de ruta en el bloque de autorización FlexVPN.

Configuración básica de Spoke and Hub

La configuración básica del hub y del spoke se basa en los documentos de migración de la VPN dinámica multipunto (DMVPN) a FlexVPN. Esta configuración se describe en la Migración de FlexVPN: Paso difícil del artículo DMVPN a FlexVPN en los mismos dispositivos.

Ajuste de configuración de radios

Configuración de Spoke - Bloque de configuración del cliente

El bloque de configuración del cliente debe ampliar la configuración de spoke.

En la configuración básica, se especifican varios peers. El par con la preferencia más alta (el

número más bajo) se considera antes que los demás.

```
crypto ikev2 client flexvpn Flex_Client
peer 1 172.25.1.1
peer 2 172.25.2.1
client connect Tunnel1
```

La configuración del túnel debe cambiar para permitir que el destino del túnel se elija dinámicamente, según el bloque de configuración del cliente FlexVPN.

```
interface Tunnel1
 tunnel destination dynamic
```

Es fundamental recordar que el bloque de configuración del cliente FlexVPN está vinculado a una interfaz y no al IKEv2 o al perfil de seguridad de protocolo de Internet (IPsec).

El bloque de configuración del cliente proporciona varias opciones para ajustar el tiempo de conmutación por fallas y las operaciones, que incluyen el uso de objetos de seguimiento, respaldo de marcado y funciones de grupos de respaldo.

Con la configuración básica, el spoke se basa en los DPD para detectar si un spoke no responde, y desencadena un cambio una vez que el par se declara muerto. La opción de utilizar DPD no es rápida, debido a cómo funcionan los DPD. Un administrador puede querer mejorar la configuración con el seguimiento de objetos o mejoras similares.

Para obtener más información, refiérase al capítulo **Configuración de FlexVPN Client** de la guía de configuración de Cisco IOS, que está enlazada en la sección **Información Relacionada** al final de este documento.

Configuración de radio completa - Referencia

```
crypto logging session

crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco

crypto ikev2 profile Flex_IKEv2
 match identity remote address 0.0.0.0
 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

crypto ikev2 client flexvpn Flex_Client
 peer 1 172.25.1.1
 peer 2 172.25.2.1
 client connect Tunnel1

crypto ipsec transform-set IKEv2 esp-gcm
 mode transport
```

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

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 2000
 tunnel source Ethernet0/0
 tunnel destination dynamic
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
```

Configuración del hub

Aunque la mayoría de la configuración del hub sigue siendo la misma, se deben abordar varios aspectos. La mayoría de ellas se refieren a una situación en la que uno o más radios están conectados a un hub, mientras que otros permanecen en relación con otro hub.

Direcciones de radio

Dado que los radios obtienen direcciones IP de los concentradores, normalmente se desea que los concentradores asignen direcciones de diferentes subredes o de una parte diferente de una subred.

Por ejemplo:

Hub1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.175
```

Hub2

```
ip local pool FlexSpokes 10.1.1.176 10.1.1.254
```

Esto evita la creación de superposiciones, incluso si las direcciones no se enrutan fuera de la nube FlexVPN, lo que podría afectar a la resolución de problemas.

Dirección superpuesta del hub

Ambos hubs pueden conservar la misma dirección IP en una interfaz de plantilla virtual; sin embargo, esto puede afectar a la resolución de problemas en algunos casos. Esta opción de diseño facilita la implementación y la planificación, ya que el spoke sólo debe tener una dirección de peer para el protocolo de gateway fronterizo (BGP).

En algunos casos, puede que no se desee o no se necesite.

Ruteo

Es necesario que los concentradores intercambien información sobre los radios que están conectados.

Los concentradores deben poder intercambiar las rutas específicas de los dispositivos que han conectado y, aun así, proporcionar un resumen a los radios.

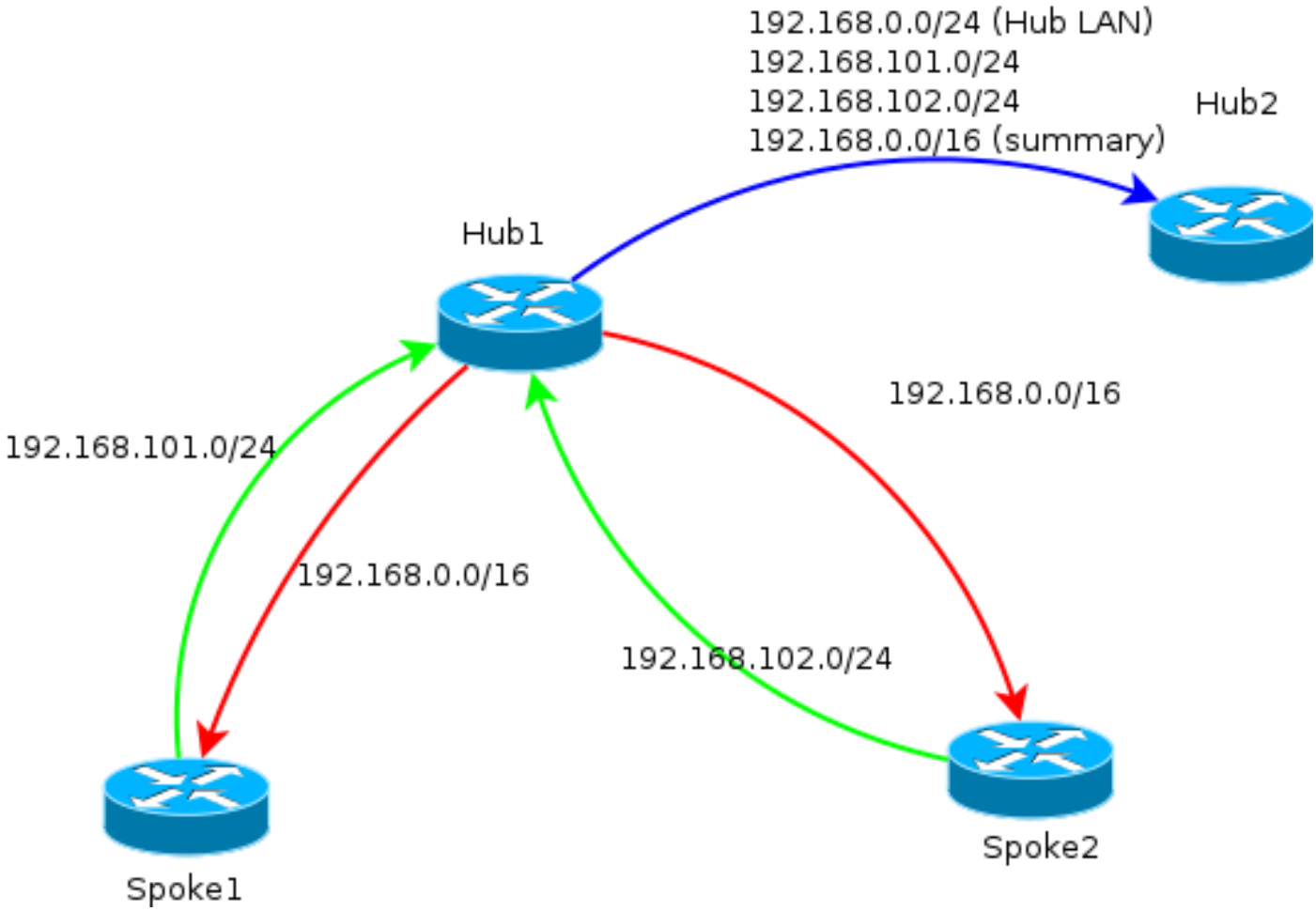
Dado que Cisco recomienda utilizar iBGP con FlexVPN y DMVPN, sólo se muestra ese protocolo de ruteo.

```
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
neighbor 192.168.0.2 remote-as 65001
neighbor 192.168.0.2 route-reflector-client
neighbor 192.168.0.2 next-hop-self all
neighbor 192.168.0.2 unsuppress-map ALL

access-list 1 permit any

route-map ALL permit 10
match ip address 1
```

Esta configuración permite:

- Receptor dinámico de direcciones asignadas a radios
- Red de publicidad de 192.168.0.0/24
- Ruta de resumen de publicidad de 192.168.0.0/16 a todos los radios. La configuración aggregate-address crea una ruta estática para ese prefijo a través de la interfaz null0, que es una ruta de descarte que se utiliza para evitar loops de ruteo.
- Reenvío de prefijos específicos al otro hub
- Cliente de reflector de ruta para asegurarse de que los concentradores intercambian la información aprendida de los radios entre sí

Este diagrama representa el intercambio de prefijos en BGP en esta configuración, desde la perspectiva de uno de los hubs.



Nota: En este diagrama, la línea verde representa la información proporcionada por los radios al hub, la línea roja representa la información proporcionada por cada hub a los radios (sólo un resumen) y la línea azul representa los prefijos intercambiados entre ejes.

Uso de resúmenes de red

Es posible que los resúmenes no sean aplicables o no se deseen en algunos escenarios. Tenga cuidado al designar la IP de destino en los prefijos, porque iBGP no invalida el salto siguiente de forma predeterminada.

Se recomiendan resúmenes en redes que cambian con frecuencia. Por ejemplo, las conexiones inestables a Internet podrían requerir resúmenes para: evite la eliminación y adición de prefijos, limite el número de actualizaciones y permita que la mayoría de las configuraciones escalen correctamente.

Túneles de Spoke a Spoke

En el escenario y la configuración mencionados en la sección anterior, los radios en diferentes concentradores no pueden establecer túneles directos de radio a radio. El tráfico entre radios conectadas a diferentes concentradores fluye a través de los dispositivos centrales.

Hay una solución alternativa fácil para esto. Sin embargo, requiere que el protocolo de resolución de salto siguiente (NHRP) con el mismo ID de red esté habilitado entre los concentradores. Esto

se puede lograr, por ejemplo, si se crea un túnel de encapsulación de routing genérico (GRE) punto a punto entre ejes de conexión. A continuación, no se requiere IPSec.

Verificación

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.

El comando **show crypto ikev2 sa** le informa dónde está conectado actualmente el spoke.

El comando **show crypto ikev2 client flexvpn** permite que un administrador comprenda el estado actual de la operación del cliente FlexVPN.

```
Spoke2# show crypto ikev2 client flexvpn

Profile : Flex_Client
Current state:ACTIVE
Peer : 172.25.1.1
Source : Ethernet0/0
ivrf : IP DEFAULT
fvrf : IP DEFAULT
Backup group: Default
Tunnel interface : Tunnel1
Assigned IP address: 10.1.1.111
```

Un failover exitoso con la configuración **show logging** registra este resultado en el dispositivo spoke:

```
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is DOWN.  Peer 172.25.1.1:500
Id: 172.25.1.1
%FLEXVPN-6-FLEXVPN_CONNECTION_DOWN: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.1.1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.  Peer 172.25.2.1:500
Id: 172.25.2.1
%FLEXVPN-6-FLEXVPN_CONNECTION_UP: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.2.1 Assigned_Tunnel_v4_addr = 10.1.1.177
```

En este resultado, el spoke se desconecta del **hub 172.25.1.1**, el bloque de configuración del cliente Flex_Client detecta una falla y fuerza una conexión a **172.25.2.1** donde se activa un túnel, y a un spoke se le asigna una IP de **10.1.177**.

Troubleshoot

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.

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

Estos son los comandos debug relevantes:

- **debug crypto ikev2**
- **debug radius**

Información Relacionada

- Guía de Configuración de FlexVPN e Internet Key Exchange Versión 2, Cisco IOS Release 15 M&T
- Soporte Técnico y Documentación - Cisco Systems