Ejemplo de Configuración de FlexVPN Spoke in Redundant Hub Design with a Dual Cloud Approach

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.

Configurar

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.

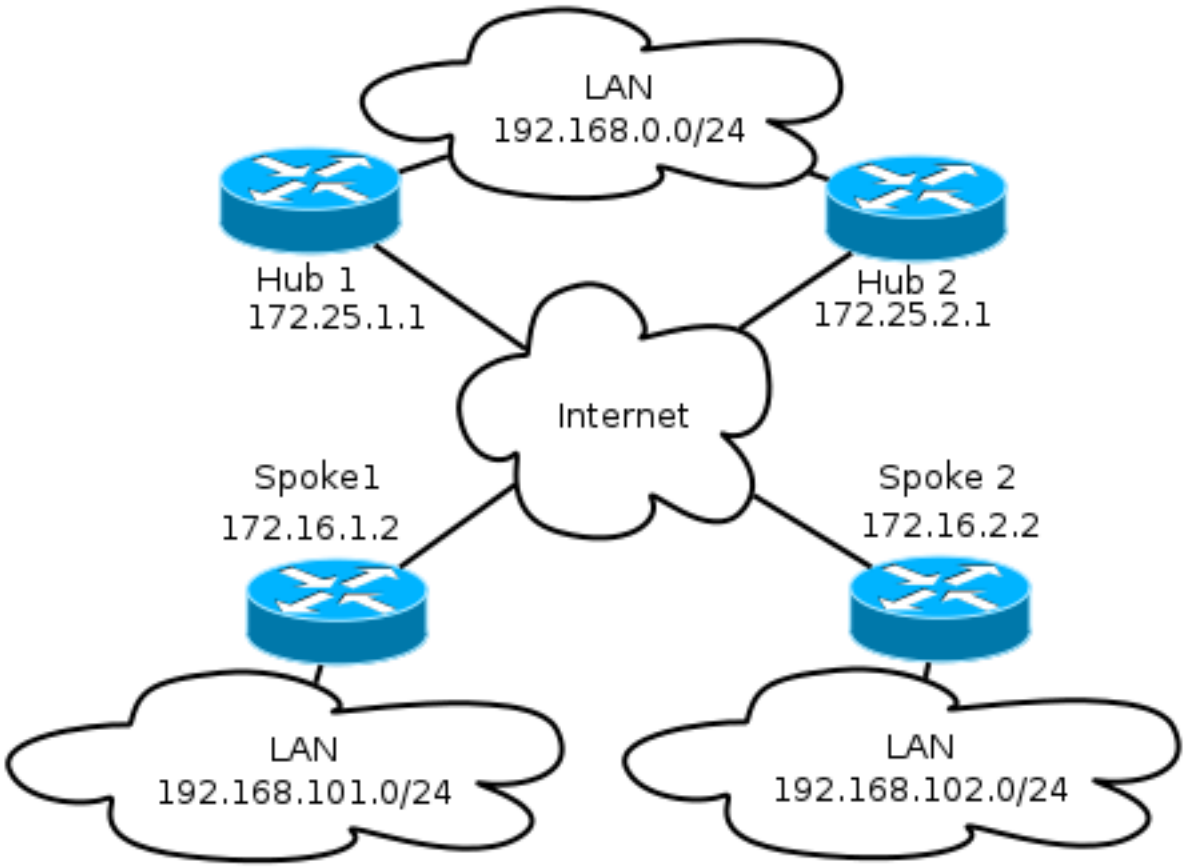
Enfoque	Pros	Cons
Nube doble	• Recuperación más rápida durante la falla, basada en los temporizadores del protocolo de ruteo • Más posibilidades de distribuir el tráfico entre los concentradores, ya que la conexión a ambos concentradores está activa	• Spoke mantiene la sesión en ambos concentradores al mismo tiempo, lo que consume recursos en ambos concentrad
Failover	• Configuración sencilla: integrada en FlexVPN • No confía en el protocolo de ruteo en una falla	• Tiempo de recuperación más lento basad en la detección de puntos inactivos (DPD (opcionalmente) en el seguimiento de objetos • Todo el tráfico se ve obligado a desplaza a un hub cada vez.

Este documento describe el primer enfoque. El enfoque de esta configuración es similar a la configuración de nube dual de VPN multipunto dinámica (DMVPN). La configuración básica de hub y spoke se basa en los documentos de migración de DMVPN a FlexVPN. Consulte Migración de FlexVPN: Artículo Transferencia difícil de DMVPN a FlexVPN en Mismos Dispositivos para una descripción de esta configuración.

Diagrama de la red

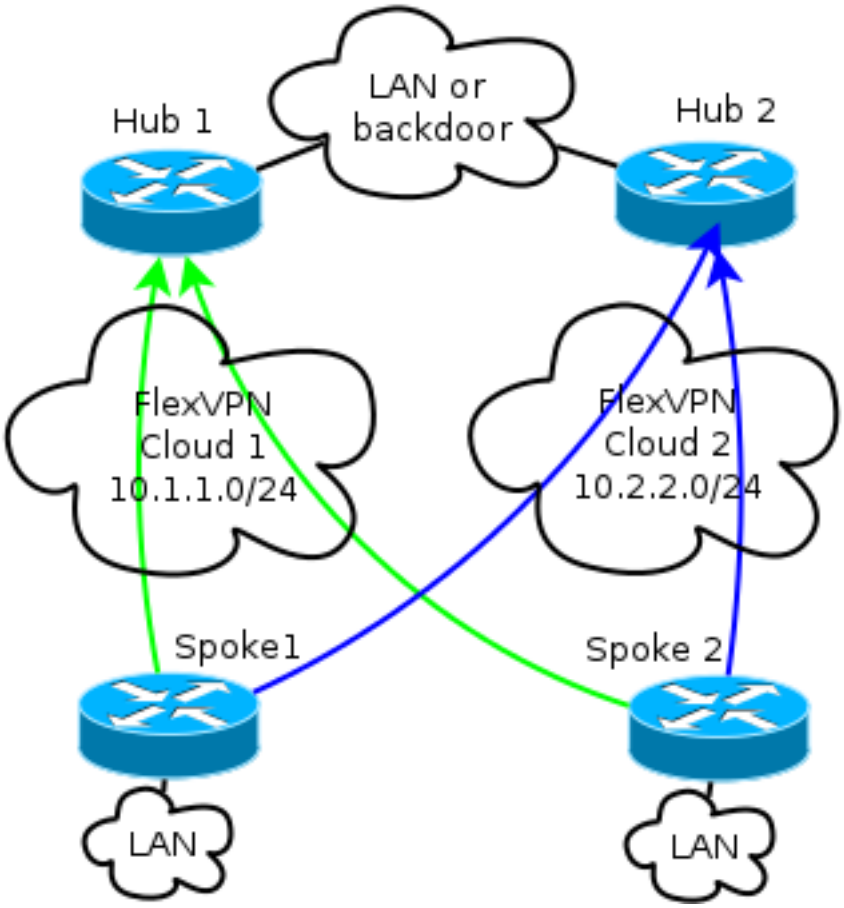
Red de transporte

Este diagrama ilustra la red de transporte básica que se utiliza habitualmente en las redes FlexVPN.



Red superpuesta

El 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 ambos hubs. En caso de falla, el protocolo de ruteo cambia de un hub a otro.



Nota: En el diagrama, las líneas verdes muestran la conexión y la dirección de las sesiones de intercambio de claves de Internet versión 2 (IKEv2)/Flex al Hub 1, y las líneas azules indican la conexión al Hub 2.

Ambos concentradores conservan direcciones IP separadas en nubes superpuestas. El direccionamiento **/24** representa el conjunto de direcciones asignadas para esta nube, 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.

Configuraciones de Spoke

Configuración de la interfaz de túnel de radio

La configuración típica utilizada en este ejemplo es simplemente dos interfaces de túnel con dos direcciones de destino separadas.

```
interface Tunnel1
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
tunnel source Ethernet0/0
```

```
tunnel destination 172.25.1.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default

interface Tunnel2
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
tunnel source Ethernet0/0
tunnel destination 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

Para permitir que los túneles de radio a radio se formen correctamente, se necesita una plantilla virtual (VT).

```
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
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

El spoke utiliza una interfaz sin numerar que indica la interfaz LAN en el routing y reenvío virtuales (VRF), que es global en este caso. Sin embargo, podría ser mejor hacer referencia a una interfaz de loopback. Esto se debe a que las interfaces de loopback permanecen en línea bajo casi todas las condiciones.

Configuración del protocolo de gateway fronterizo de radio (BGP)

Dado que Cisco recomienda iBGP como el protocolo de ruteo que se utilizará en la red superpuesta, este documento menciona solamente esta configuración.

> **Nota:** Los radios deben conservar la disponibilidad BGP a ambos hubs.

```
router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
neighbor 10.1.1.1 fall-over
neighbor 10.2.2.1 remote-as 65001
neighbor 10.2.2.1 fall-over
```

FlexVPN en esta configuración no tiene un concepto de hub primario o secundario. El administrador decide si el protocolo de ruteo prefiere un hub a otro o, en algunos casos, realiza el balanceo de carga.

Consideraciones sobre la convergencia y la conmutación por fallo

Para minimizar el tiempo que tarda un spoke en detectar una falla, utilice estos dos métodos típicos.

- Acorte los temporizadores BGP. El tiempo de espera predeterminado causa la conmutación por fallas.
- Configure la caída de BGP, que se analiza en este artículo, Soporte BGP para la Desactivación de Sesión de Peering Rápido.
- No utilice la detección de reenvío bidireccional (BFD) porque no se recomienda en la mayoría de las implementaciones de FlexVPN.

Túneles de Spoke a Spoke y Failover

Los túneles de radio a radio utilizan switching de acceso directo de protocolo de resolución de salto siguiente (NHRP). Cisco IOS indica que esos accesos directos son rutas NHRP, por ejemplo:

```
Spoke1#show ip route nhrp
(...)

192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks
H 192.168.102.0/24 [250/1] via 10.2.2.105, 00:00:21, Virtual-Access1
```

Esas rutas no caducan cuando caduca la conexión BGP; en su lugar, se retienen para el tiempo de espera de NHRP, que es de dos horas de forma predeterminada. Esto significa que los túneles de radio a radio activos permanecen en funcionamiento incluso en caso de fallo.

Configuraciones del hub

Conjuntos locales

Como se explica en la sección **Diagrama de red**, ambos hubs conservan el direccionamiento IP separado.

Hub1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

Hub2

```
ip local pool FlexSpokes 10.2.2.100 10.2.2.254
```

Configuración de Hub BGP

La configuración de Hub BGP sigue siendo similar a los ejemplos anteriores.

Esta salida viene del Hub 1 con una dirección IP LAN de **192.168.0.1**.

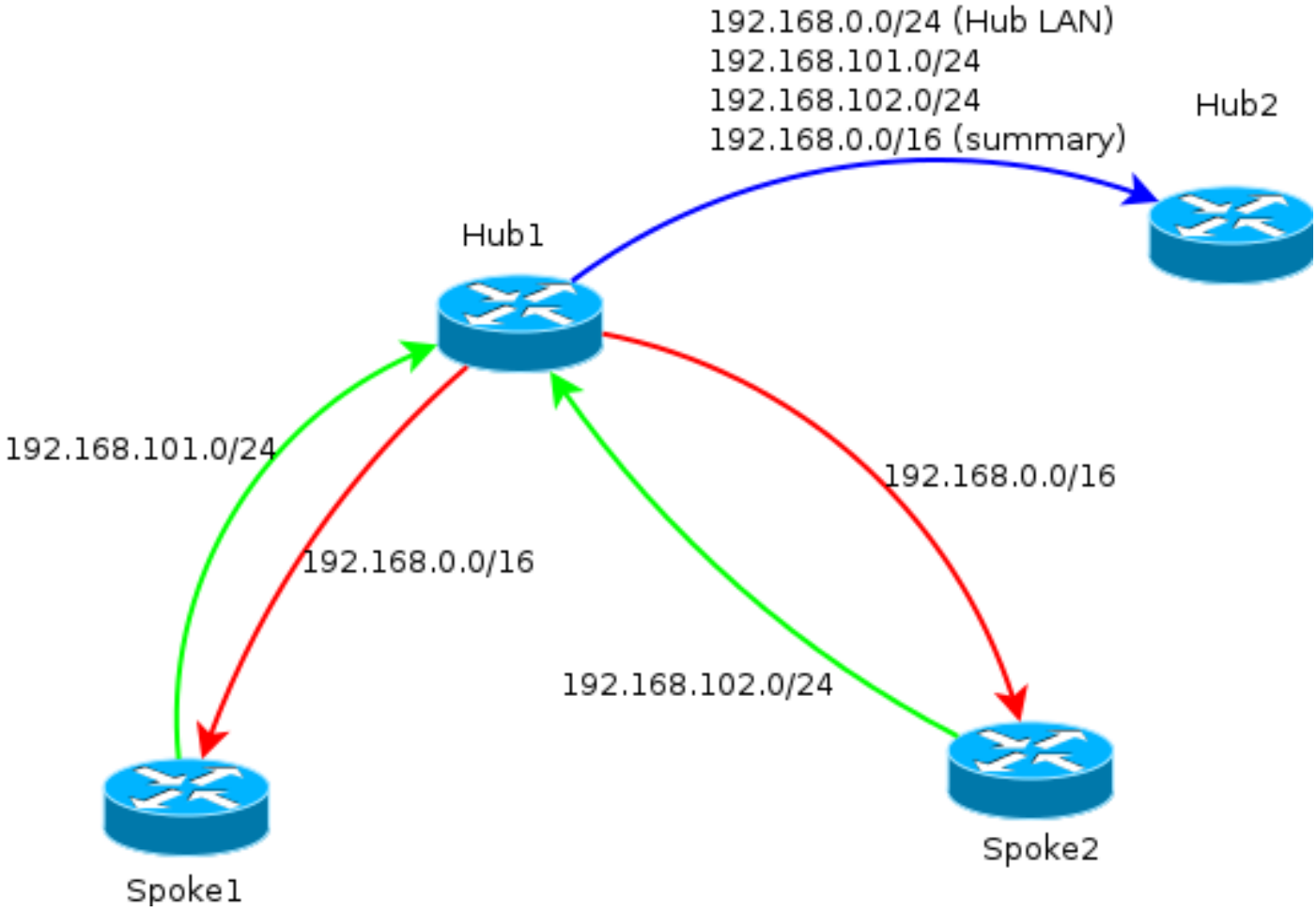
```
router bgp 65001
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
aggregate-address 192.168.0.0 255.255.0.0 summary-only
neighbor Spokes peer-group
```

```
neighbor Spokes remote-as 65001
neighbor Spokes fall-over
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

route-map ALL permit 10
match ip address 1

ip access-list standard 1
permit any
```

En esencia, esto es lo que se hace:

- El conjunto de direcciones FlexVPN local está en el rango de escucha BGP.
- La red local es 192.168.0.0/24.
- Un resumen sólo se anuncia a los radios. La configuración de dirección de agregación 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.
- Todos los prefijos específicos se anuncian al otro hub. Puesto que también es una conexión iBGP, requiere una configuración de reflector de ruta.

Este diagrama representa el intercambio de prefijos BGP entre radios y concentradores en una nube FlexVPN.



Nota: En el 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.

Verificación

Dado que cada spoke conserva la asociación con ambos hubs, se ven dos sesiones IKEv2 con el comando **show crypto ikev2 sa**.

```
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
3 172.16.1.2/500 172.16.2.2/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3147 sec

Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.2/500 172.25.2.1/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3256 sec
```

Para ver la información del protocolo de ruteo, ingrese estos comandos:

```
show bgp ipv4 unicast

show bgp summary
```

En los spokes, debe ver que el prefijo de resumen se recibe de los hubs y que las conexiones a ambos hubs están activas.

```
Spoke1#show bgp ipv4 unicast
BGP table version is 4, local router ID is 192.168.101.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*>i 192.168.0.0/16 10.1.1.1 0 100 0 i
* i 10.2.2.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
Spoke1#show bgp summa
Spoke1#show bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
BGP table version is 4, main routing table version 4
2 network entries using 296 bytes of memory
3 path entries using 192 bytes of memory
3/2 BGP path/bestpath attribute entries using 408 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 896 total bytes of memory
BGP activity 2/0 prefixes, 3/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 7 7 4 0 0 00:00:17 1
10.2.2.1 4 65001 75 72 4 0 0 01:02:24 1
```

Troubleshoot

Hay dos bloques principales para resolver problemas:

- Intercambio de claves de Internet (IKE)
- Seguridad de protocolo de Internet (IPsec)

Estos son los comandos show relevantes:

```
show crypto ipsec sa

show crypto ikev2 sa
```

Estos son los comandos debug relevantes:

```
debug crypto ikev2 [internal|packet]

debug crypto ipsec

debug vtemplate event
```

Este es el protocolo de ruteo relevante:

```
show bgp ipv4 unicast (or show ip bgp)

show bgp summary
```