FlexVPN habló en el diseño redundante del concentrador con un ejemplo de configuración dual del acercamiento de la nube

Contenido

Introducción

Este documento describe cómo configurar un spoke en una red de FlexVPN con el uso del bloque de la configuración del cliente de FlexVPN en un escenario donde están disponibles los hub múltiple.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- FlexVPN
- Routing Protocol de Cisco

Componentes Utilizados

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

- Router del servicio integrado de las G2 Series de Cisco (ISR)
- Versión 15.2M del ® del Cisco IOS

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

Para los propósitos de la redundancia, un spoke pudo necesitar conectar con los hub múltiple. La Redundancia en el lado radial permite la operación continua sin un solo punto de falla en el lado del eje de conexión.

Los dos diseños redundantes mas comunes del concentrador de FlexVPN que utilizan la configuración radial son:

- **Acercamiento dual de la nube**, donde un spoke tiene dos túneles diferentes activos a ambo Hubs siempre.
- **Acercamiento de la Conmutación por falla**, donde un spoke tiene un túnel activo con un concentrador en cualquier punta dada a tiempo.

Ambos acercamientos tienen un conjunto único de pros - y - contra.

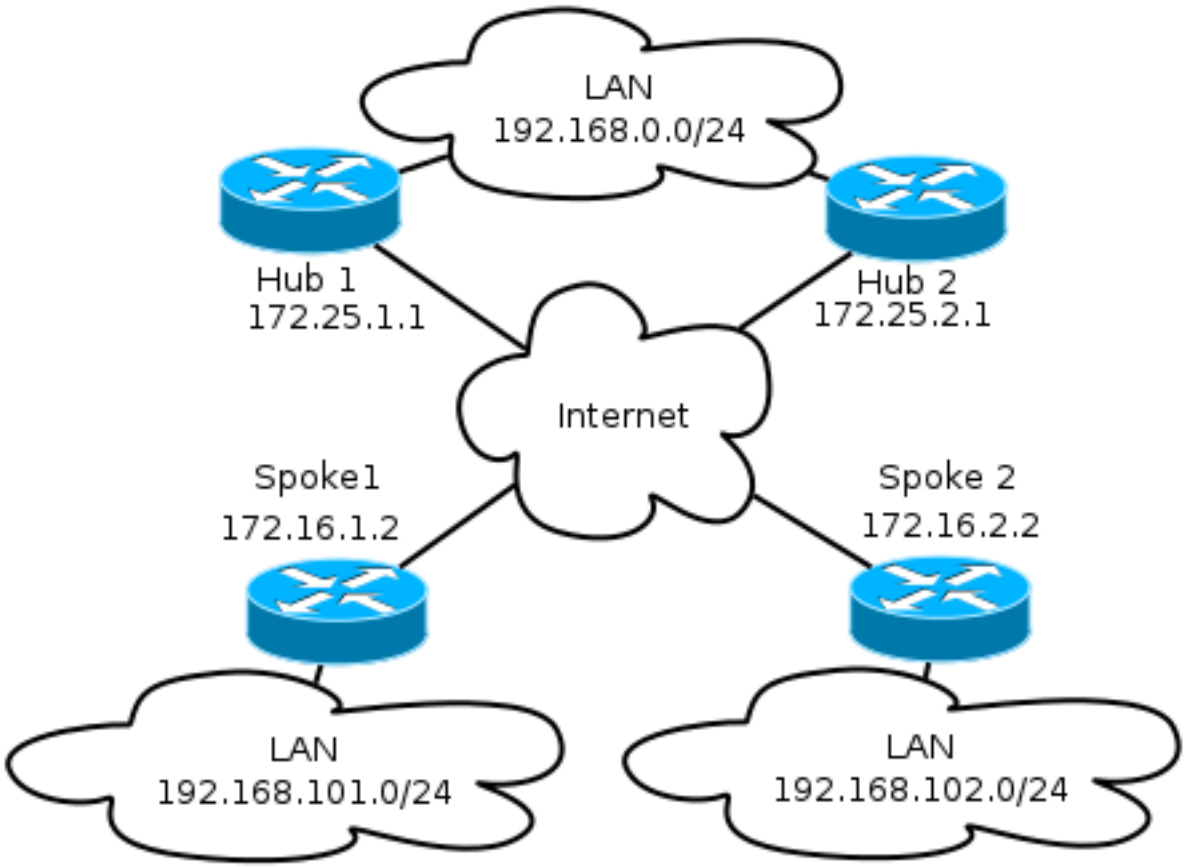
Acercamiento	Pros	Cons
Nube dual	• Una recuperación más rápida durante el error, sobre la base de los temporizadores del Routing Protocol • Más possibilties para distribuir el tráfico entre el Hubs, puesto que la conexión a ambo Hubs es activa	• El spoke mantiene la sesión a ambo H al mismo tiempo, que consume los recursos en ambo Hubs
Failover	• Configuración fácil - incorporada a FlexVPN • No confía en el Routing Protocol en un error	• Un tiempo de recuperación más lento basado en el Dead Peer Detection (D (opcionalmente) el Rastreo de objetos • Todo el tráfico se fuerza para viajar a un momento del concentrador.

Este documento describe el primer acercamiento. El acercamiento a esta configuración es similar a la configuración dual de la nube del Dynamic Multipoint VPN (DMVPN). La configuración básica del hub and spoke se basa en los documentos de la migración del DMVPN a FlexVPN. Refiera a la migración de FlexVPN: Movimiento duro del DMVPN a FlexVPN en el mismo artículo de los dispositivos para una descripción de esta configuración.

Diagrama de la red

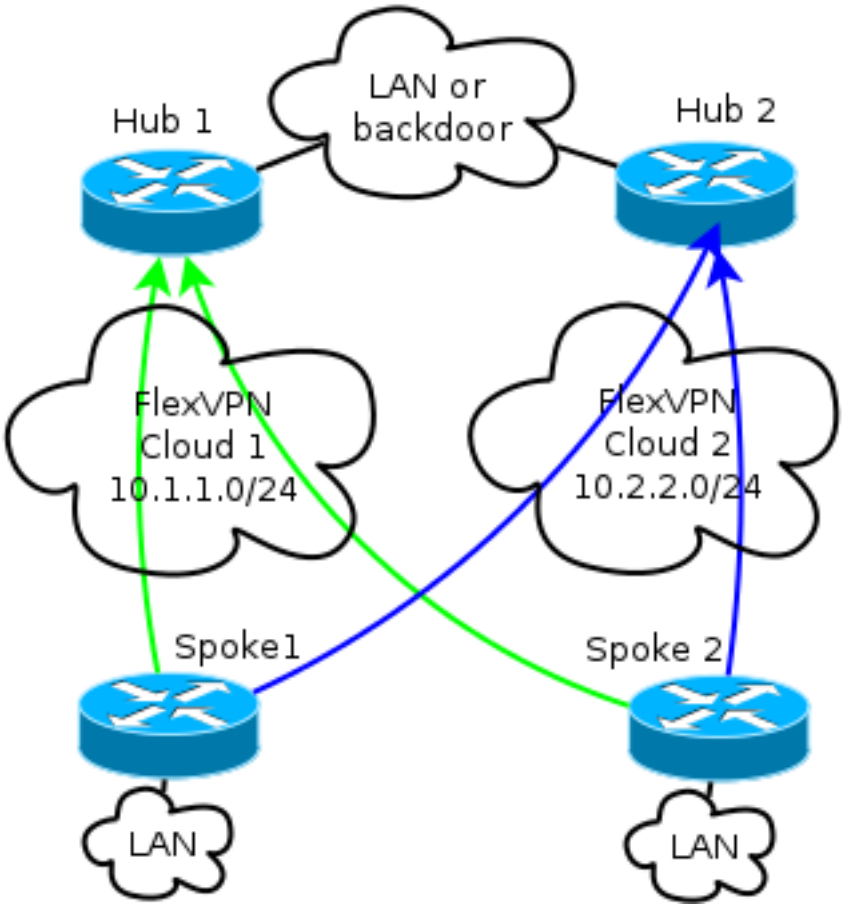
Red de transporte

Este diagrama ilustra la red de transporte básica usada típicamente en las redes de FlexVPN.



Red de recubrimiento

El diagrama ilustra la red de recubrimiento con la conectividad lógica que muestra cómo la Conmutación por falla debe trabajar. Durante el funcionamiento normal, el Spoke1 y el Spoke2 mantienen una relación con ambo Hubs. Sobre un error, el Switches del Routing Protocol a partir de un concentrador a otro.



Nota: En el diagrama, las líneas verdes muestran la conexión y la dirección del intercambio de claves de Internet versión 2 (las sesiones IKEv2)/Flex al Hub1, y las líneas azules indican la conexión al Hub2.

Ambo Hubs conserva el IP Addressing separado en las nubes del recubrimiento. La dirección de **/24** representa a la agrupación de direcciones afectada un aparato para esta nube, no la dirección real de la interfaz. Esto es porque el concentrador de FlexVPN afecta un aparato típicamente un IP Address dinámico para la interfaz del spoke, y confía en las rutas insertadas dinámicamente vía los comandos route en el bloque de la autorización de FlexVPN.

Configuraciones de Spoke

Configuración de la interfaz del túnel del spoke

La configuración típica usada en este ejemplo es simplemente dos interfaces del túnel con dos direcciones 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 del spoke al spoke formen correctamente, una plantilla virtual (VT) es necesaria.

```
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 indique la interfaz LAN en el ruteo virtual y la expedición (VRF), que es global en este caso. Sin embargo, puede ser que sea mejor referirse a un Loopback Interface. Esto es porque sigue habiendo las interfaces del loopback en línea bajo casi todas las condiciones.

Configuración del Border Gateway Protocol (BGP) del spoke

Puesto que Cisco recomienda el iBGP como el Routing Protocol que se utilizará en la red de recubrimiento, las menciones de este documento solamente esta configuración.

> Nota: El spokes debe conservar el accesibilidad BGP a ambo Hubs.

```
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
```

FlexVPN en esta configuración no tiene un primario o hub secundario un concepto. El administrador decide si el Routing Protocol prefiere un concentrador sobre otro o, en algunos escenarios, realiza el balanceo de carga.

Consideraciones de la Conmutación por falla y de la convergencia del spoke

Para minimizar el tiempo que lleva para habló para detectar el error, utiliza estos dos métodos típicos.

- Acorte los temporizadores BGP. El tiempo en espera predeterminado causa la Conmutación por falla.
- Configure el fail-over BGP, que discused en este artículo, soporte BGP para la desactivación rápida de la sesión de peer.
- No utilice la detección bidireccional de la expedición (BFD), porque no se recomienda en la mayoría de las implementaciones de FlexVPN.

Túneles y Conmutación por falla del spoke al spoke

Transferencia del acceso directo del Next Hop Resolution Protocol (NHRP) del uso de los túneles del spoke al spoke. El Cisco IOS indica que esos accesos directos son rutas NHRP, por ejemplo:

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

Esas rutas no expiran cuando expira la conexión BGP; en lugar, se sostienen para el tiempo de espera del NHRP, que es dos horas por abandono. Esto significa que los túneles activos del spoke al spoke siguen siendo en funcionamiento incluso en un error.

Configuraciones del hub

Agrupaciones locales

Como se debate en la sección del **diagrama de la red**, ambo Hubs conserva el IP Addressing separado.

Hub1

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

Hub2

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

Configuración BGP del concentrador

La configuración BGP del concentrador sigue siendo similar a los ejemplos anteriores.

Esta salida viene del Hub1 con una dirección IP LAN de **192.168.0.1**.

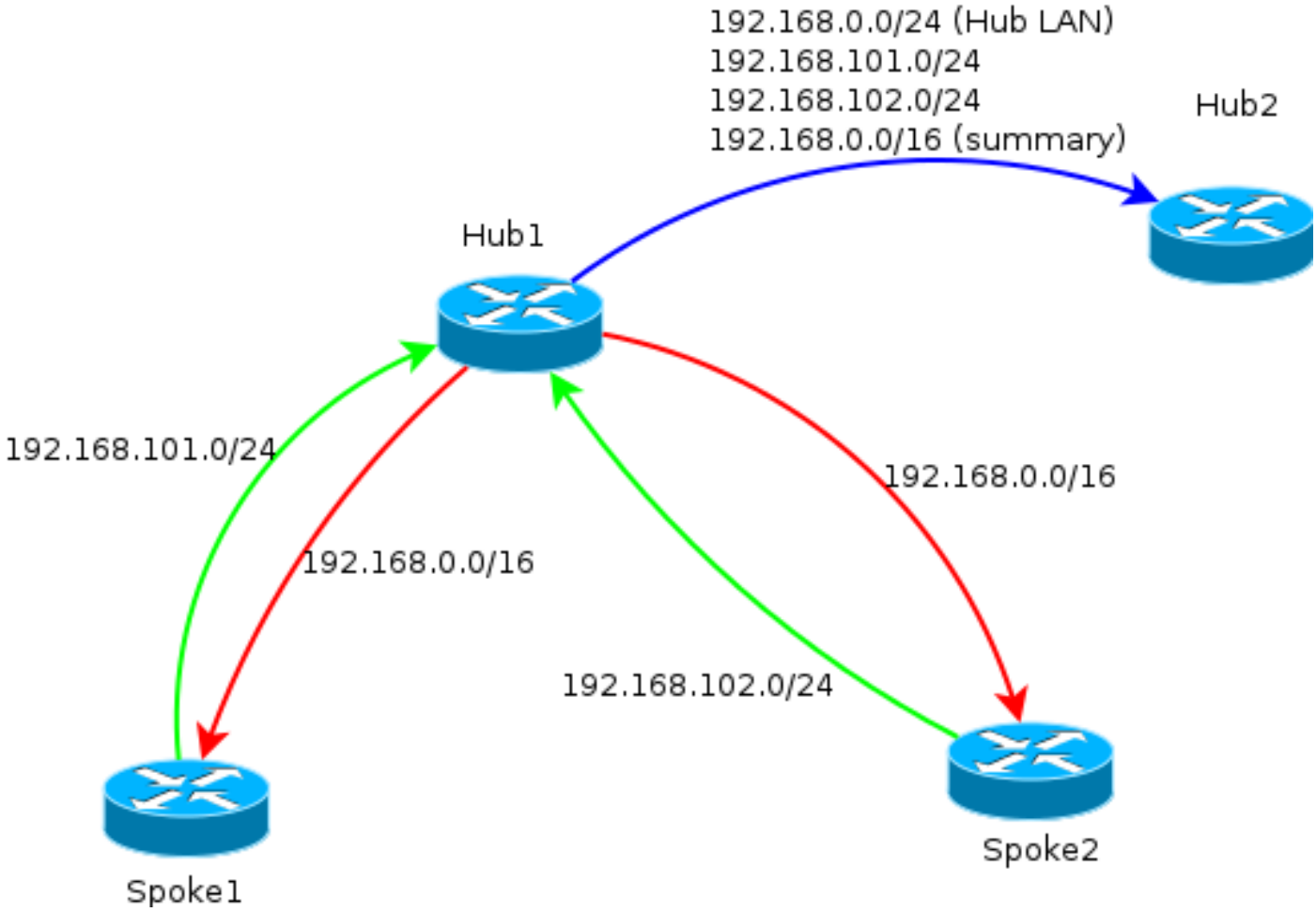
```
Spoke1#show ip route nhrp
(...)Spoke1#show ip route nhrp
(...)
```

Esencialmente, esto es se hace qué:

- La agrupación de direcciones local de FlexVPN está en el BGP escucha rango.
- La red local es 192.168.0.0/24.
- Un resumen se hace publicidad solamente al spokes. la configuración del Agregado-direccionamiento crea una Static ruta para ese prefijo vía la interfaz del null0, que es una ruta de descarte que se utiliza para evitar el rutear de los loopes.

- Todos los prefijos específicos se hacen publicidad al otro concentrador. Puesto que es también una conexión del iBGP, requiere una configuración del reflector de ruta.

Este diagrama representa el intercambio de los prefijos BGP entre el spokes y el Hubs en una nube de FlexVPN.



Nota: En el diagrama, la línea verde representa la información proporcionada por el spokes al concentrador, la línea roja representa la información proporcionada por cada concentrador al spokes (un resumen solamente), y la línea azul representa los prefijos intercambiados entre el Hubs.

Verificación

Puesto que cada spoke conserva la asociación con ambo Hubs, dos sesiones IKEv2 se consideran con el comando **crypto ikev2 sa de la demostración**.

```
Spoke1#show ip route nhrp
(...)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 secTunnel-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 Routing Protocol, ingrese estos comandos:

show bgp ipv4 unicast

show bgp summary

En el spokes, usted debe ver que el prefijo sumario está recibido del Hubs, y que las conexiones a ambo Hubs son 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 foundNetwork 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 secsNeighbor 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
```

Troubleshooting

Hay dos bloques importantes a resolver problemas:

- Internet Key Exchange (IKE)
- Seguridad de protocolos en Internet (IPSec)

Aquí están los comandos show relevantes:

show crypto ipsec sa

show crypto ikev2 sa

Aquí están los comandos relevant debug:

debug crypto ikev2 [internal|packet]

debug crypto ipsec

debug vtemplate event

Aquí está el Routing Protocol relevante:

show bgp ipv4 unicast (or show ip bgp)

show bgp summary