Ejemplo de Configuración de la Migración de Soft DMVPN a FlexVPN

Contenido

Introducción

Este documento describe cómo realizar una migración *de software* donde tanto la VPN dinámica multipunto (DMVPN) como FlexVPN funcionan en un dispositivo simultáneamente sin necesidad de una solución alternativa y proporciona un ejemplo de configuración.

> **Nota:** Este documento se extiende sobre los conceptos descritos en la Migración de FlexVPN: Cambio difícil de DMVPN a FlexVPN en los mismos dispositivos y Migración de FlexVPN: Cambio difícil de DMVPN a FlexVPN en artículos de Cisco de un centro diferente. Ambos documentos describen migraciones *duras*, que causan alguna interrupción en el tráfico durante la migración. Las limitaciones en estos artículos se deben a una deficiencia

en el software Cisco IOS® que ahora se rectifica.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- DMVPN
- FlexVPN

Componentes Utilizados

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

- Router de servicios integrados (ISR) de Cisco versión 15.3(3)M o posterior
- Cisco 1000 Series Aggregated Service Router (ASR1K) Versiones 3.10 o posteriores

Nota: No todo el software y el hardware admiten el intercambio de claves de Internet versión 2 (IKEv2). Consulte Cisco Feature Navigator para obtener más información.

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

Una de las ventajas de la plataforma y el software Cisco IOS más nuevos es la capacidad de utilizar la criptografía de última generación. Un ejemplo es el uso del estándar de cifrado avanzado (AES) en el modo Galois/Counter (GCM) para el cifrado en IPsec, como se describe en RFC 4106. AES GCM permite velocidades de cifrado mucho más rápidas en algunos equipos.

Nota: Para obtener información adicional sobre el uso y la migración a la criptografía de última generación, refiérase al artículo Cifrado de última generación de Cisco.

Configurar

Este ejemplo de configuración se centra en una migración de una configuración de la Fase 3 de DMVPN a una FlexVPN, porque ambos diseños funcionan de forma similar.

	Fase 2 de DMVPN	Fase 3 de DMVPN	FlexVPN
Transporte	GRE sobre IPsec	GRE sobre IPsec	GRE sobre IPs VTI

Uso de NHRP	Registro y resolución	Registro y resolución	Resolución
Siguiente salto desde Spoke	Otros radios o concentrador	Resumen del hub	Resumen del h
Switching de acceso directo NHRP	No	Yes	Sí (opcional)
Redirección NHRP	No	Yes	Yes
IKE e IPsec	IPsec opcional, IKEv1 típico	IPsec opcional, IKEv1 típico	IPsec, IKEv2

Diagramas de la Red

Esta sección proporciona diagramas de red de transporte y superposición.

Diagrama de red de transporte

La red de transporte utilizada en este ejemplo incluye un único hub con dos radios conectados. Todos los dispositivos están conectados a través de una red que simula Internet.

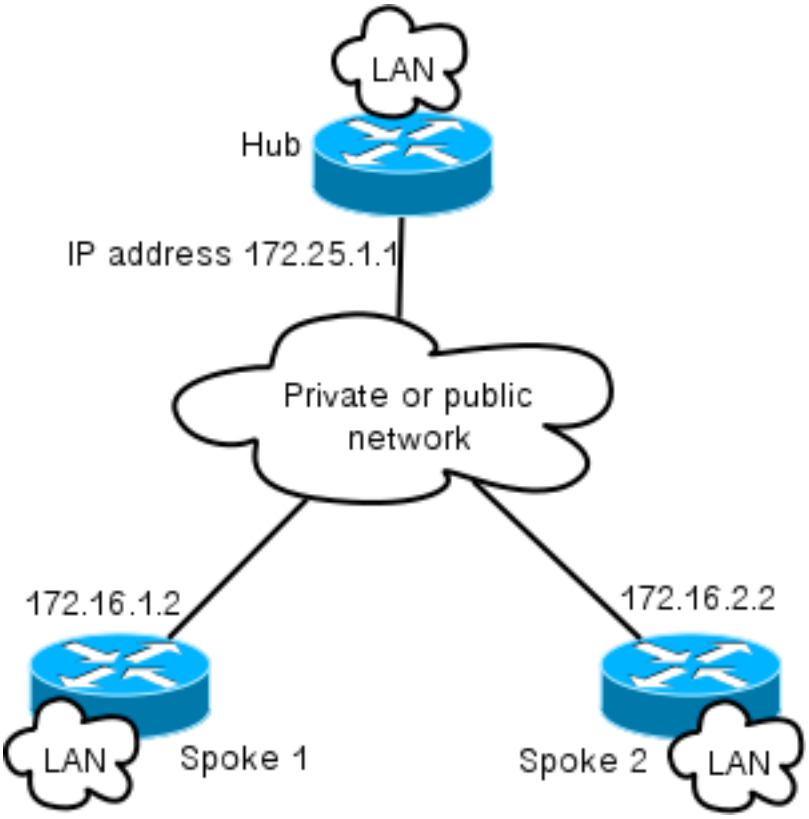
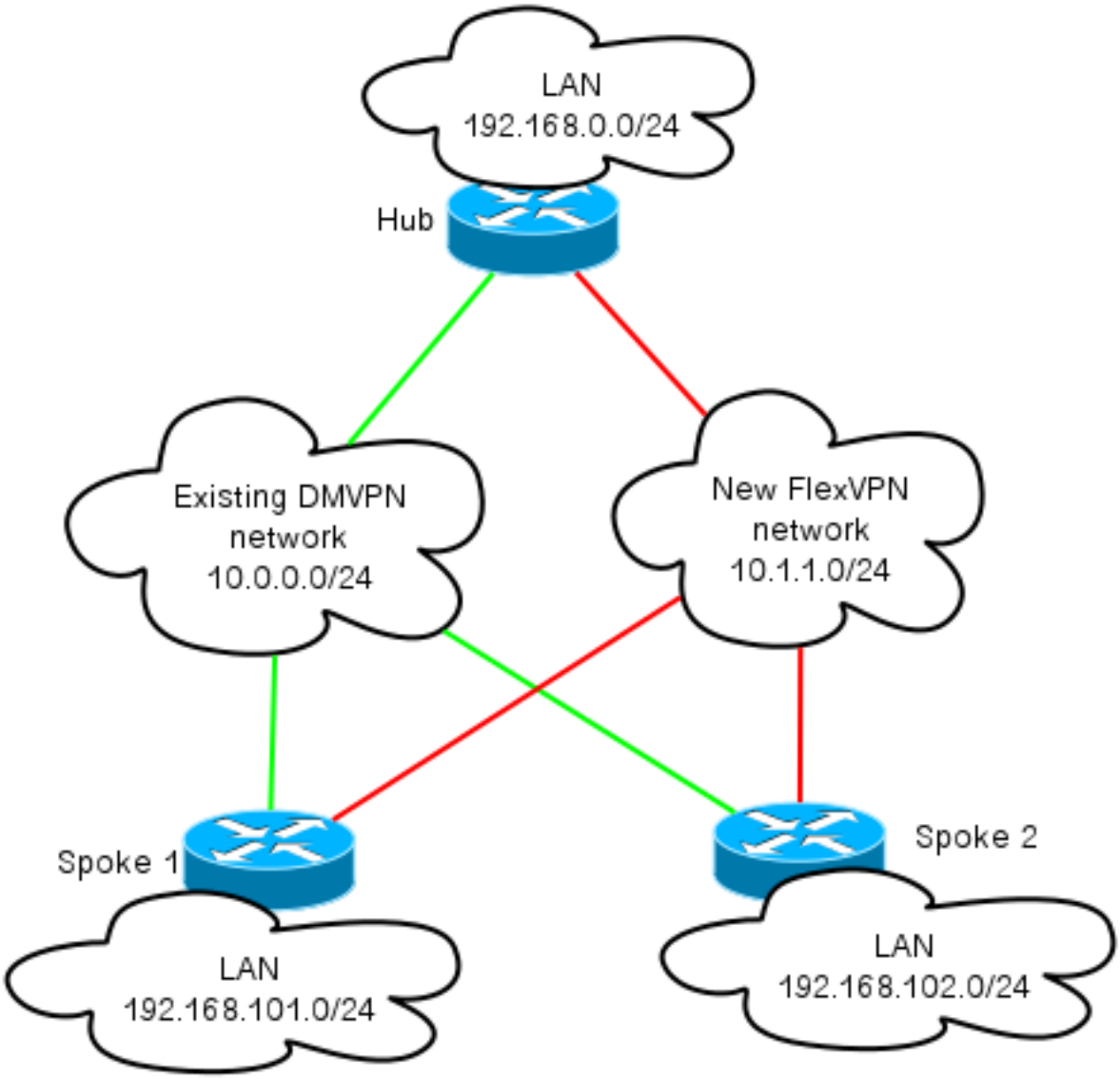


Diagrama de red superpuesta

La red superpuesta utilizada en este ejemplo incluye un único hub con dos radios conectados. Recuerde que tanto DMVPN como FlexVPN están activos simultáneamente, pero utilizan diferentes espacios de direcciones IP.



Configuraciones

Esta configuración migra la implementación más popular de la Fase 3 de DMVPN a través del protocolo de routing de gateway interior mejorado (EIGRP) a FlexVPN con protocolo de gateway fronterizo (BGP). Cisco recomienda el uso de BGP con FlexVPN, ya que permite que las implementaciones se amplíen mejor.

> **Nota:** El hub finaliza las sesiones IKEv1 (DMVPN) e IKEv2 (FlexVPN) en la misma dirección IP. Esto sólo es posible con las versiones recientes de Cisco IOS.

Configuración de Spoke

Se trata de una configuración muy básica, con dos excepciones notables que permiten la interoperabilidad de IKEv1 e IKEv2, así como dos marcos que utilizan Generic Routing Encapsulation (GRE) sobre IPsec para el transporte con el fin de coexistir.

> **Nota:** Los cambios relevantes en la configuración de IKEv2 y de la Asociación de seguridad de Internet (ISAKMP) se resaltan en negrita.

```
crypto keyring DMVPN_IKEv1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco

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 isakmp policy 10
encr aes
authentication pre-share

crypto isakmp keepalive 30 5

crypto isakmp profile DMVPN_IKEv1
keyring DMVPN_IKEv1
match identity address 0.0.0.0

crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
mode transport

crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1
set isakmp-profile DMVPN_IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel0
 desciption DMVPN tunnel
ip address 10.0.0.101 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map 10.0.0.1 172.25.1.1
ip nhrp map multicast 172.25.1.1
ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp nhs 10.0.0.1
ip nhrp shortcut
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel mode gre multipoint
 tunnel key 0
tunnel protection ipsec profile DMVPN_IKEv1 isakmp-profile DMVPN_IKEv1

interface Tunnel1
description FlexVPN spoke-to-hub 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
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
 tunnel protection ipsec profile default ikev2-profile Flex_IKEv2


interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
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 protection ipsec profile default ikev2-profile Flex_IKEv2
```

Cisco IOS Release 15.3 le permite unir los perfiles IKEv2 e ISAKMP en una configuración *de protección de túnel*. Junto con algunos cambios internos en el código, esto permite que IKEv1 e IKEv2 funcionen en el mismo dispositivo simultáneamente.

Debido a la forma en que Cisco IOS selecciona los perfiles (IKEv1 o IKEv2) en las versiones anteriores a 15.3, se derivaron algunas advertencias, como situaciones en las que se inicia IKEv1 a IKEv2 a través del par. La separación de IKE se basa ahora en el nivel de perfil, no en el nivel de interfaz, que se logra a través de la nueva CLI.

Otra actualización en la nueva versión de Cisco IOS es la adición de la *clave de túnel*. Esto es necesario porque tanto DMVPN como FlexVPN utilizan la misma interfaz de origen y la misma dirección IP de destino. Con esto en su lugar, no hay manera de que el túnel GRE sepa qué interfaz de túnel se utiliza para desencapsular el tráfico. La clave de túnel le permite diferenciar **tunnel0** y **tunnel1** con la adición de una sobrecarga pequeña (4 bytes). Se puede configurar una clave diferente en ambas interfaces, pero normalmente sólo necesita diferenciar un túnel.

> **Nota:** La opción de protección de túnel compartido no es necesaria cuando DMVPN y FlexVPN comparten la misma interfaz.

Por lo tanto, la configuración del protocolo de ruteo spoke es básica. EIGRP y BGP funcionan por separado. EIGRP se anuncia solamente a través de la interfaz de túnel para evitar el peering sobre los túneles de spoke a spoke, lo que limita la escalabilidad. BGP mantiene una relación solamente con el router hub (**10.1.1.1**) para anunciar la red local (**192.168.101.0/24**).

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.101.0
passive-interface default
no passive-interface Tunnel0

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

Configuración del hub

Debe realizar cambios similares en la configuración del eje de conexión como los descritos en la sección **Configuración de radio**.

Nota: Los cambios relevantes en la configuración ISAKMP e IKEV2 se resaltan en negrita.

```
crypto ikev2 authorization policy default
pool FlexSpokes
route set interface

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 isakmp policy 10
encr aes
authentication pre-share

crypto isakmp key cisco address 0.0.0.0


crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel0
ip address 10.0.0.1 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map multicast dynamic
 ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp server-only
ip nhrp redirect
 ip summary-address eigrp 100 192.168.0.0 255.255.0.0
ip tcp adjust-mss 1360
tunnel source Loopback0
tunnel mode gre multipoint
 tunnel key 0
 tunnel protection ipsec profile DMVPN_IKEv1

interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip mtu 1400
 ip nhrp network-id 2
ip tcp adjust-mss 1360
 tunnel protection ipsec profile default
```

En el lado del hub, el enlace entre el perfil IKE y el perfil IPsec ocurre en el nivel del perfil, a diferencia de la configuración spoke, donde esto se completa a través del comando **tunnel protection**. Ambos enfoques son métodos viables para completar este enlace.

Es importante tener en cuenta que las ID de red del protocolo de resolución de salto siguiente (NHRP) son diferentes para DMVPN y FlexVPN en la nube. En la mayoría de los casos, no es deseable cuando NHRP crea un dominio único sobre ambos marcos.

La clave de túnel diferencia los túneles DMVPN y FlexVPN en el nivel GRE para alcanzar el mismo objetivo mencionado en la sección **Configuración de radio**.

La configuración de ruteo en el hub es bastante básica. El dispositivo hub mantiene dos relaciones con cualquier spoke dado, una que utiliza EIGRP y otra que utiliza BGP. La configuración BGP utiliza el rango de escucha para evitar una configuración larga por radio.

Las direcciones de resumen se introducen dos veces. La configuración EIGRP envía un resumen con el uso de la configuración **tunnel0** (IP summary-address EIGRP 100), y el BGP introduce un resumen con el uso de aggregate-address. Los resúmenes son necesarios para asegurarse de que se produzca la redirección NHRP y para simplificar las actualizaciones de ruteo. Puede enviar una redirección NHRP (al igual que una redirección de protocolo de mensajes de control de Internet (ICMP)) que indica si existe un mejor salto para un destino determinado, lo que permite establecer un túnel de radio a radio. Estos resúmenes también se utilizan para minimizar la cantidad de actualizaciones de ruteo que se envían entre el hub y cada spoke, lo que permite que las configuraciones se escalen mejor.

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel0

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
```

Verificación

La verificación para este ejemplo de configuración se divide en varias secciones.

Comprobaciones previas a la migración

Dado que tanto DMVPN/EIGRP como FlexVPN/BGP funcionan simultáneamente, debe verificar que el spoke mantiene una relación sobre IPsec con IKEv1 e IKEv2, y que los prefijos apropiados se aprenden a través de EIGRP y BGP.

En este ejemplo, **Spoke1** muestra que se mantienen dos sesiones con el router hub; uno utiliza IKEv1/**Tunnel0** y uno utiliza IKEv2/**Tunnel1**.

Nota: Se mantienen dos asociaciones de seguridad IPsec (una entrante y otra saliente) para cada uno de los túneles.

```
Spoke1#show cry sess
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
 IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

Cuando verifica los protocolos de ruteo, debe verificar que se ha formado una vecindad y que se han aprendido los prefijos correctos. Esto se verifica primero con el EIGRP. Verifique que el hub esté visible como vecino y que la dirección 192.168.0.0/16 (el resumen) se obtenga del hub:

```
Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.0.0.1 Tu0 10 00:04:02 7 1398 0 13

Spoke1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 192.168.101.0/24, 1 successors, FD is 281600
via Connected, Ethernet1/0
P 192.168.0.0/16, 1 successors, FD is 26880000
via 10.0.0.1 (26880000/256), Tunnel0
P 10.0.0.0/24, 1 successors, FD is 26880000
via Connected, Tunnel0
```

Luego, verifique el BGP:

```
Spoke1#show bgp summary
(...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 13 11 3 0 0 00:06:56 1
Spoke1#show bgp
BGP table version is 3, 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
r>i 192.168.0.0/16 10.1.1.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
```

El resultado muestra que la dirección IP FlexVPN del hub (10.1.1.1) es un vecino a través del cual el spoke recibe un prefijo (192.168.0.0/16). Además, el BGP informa al administrador de que se ha producido una falla en la Base de información de routing (RIB) para el prefijo 192.168.0.0/16. Esta falla ocurre porque hay una mejor ruta para ese prefijo que ya existe en la tabla de ruteo. EIGRP origina esta ruta y puede confirmarse si verifica la tabla de ruteo.

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
 Known via "eigrp 100", distance 90, metric 26880000, type internal
Redistributing via eigrp 100
Last update from 10.0.0.1 on Tunnel0, 00:10:07 ago
Routing Descriptor Blocks:
* 10.0.0.1, from 10.0.0.1, 00:10:07 ago, via Tunnel0
Route metric is 26880000, traffic share count is 1
Total delay is 50000 microseconds, minimum bandwidth is 100 Kbit
Reliability 255/255, minimum MTU 1400 bytes
Loading 1/255, Hops 1
```

Migración

La sección anterior verificó que los protocolos IPsec y de ruteo se configuran y funcionan como se esperaba. Una de las formas más sencillas de migrar de DMVPN a FlexVPN en el mismo dispositivo es cambiar la distancia administrativa (AD). En este ejemplo, el BGP interno (iBGP) tiene un AD de 200, y el EIGRP tiene un AD de 90.

Para que el tráfico fluya correctamente a través de FlexVPN, el BGP debe tener un mejor AD. En este ejemplo, el EIGRP AD se cambia a 230 y 240 para las rutas internas y externas, respectivamente. Esto hace que el BGP AD (de 200) sea más preferible para el prefijo 192.168.0.0/16.

Otro método que se utiliza para lograr esto es para disminuir el BGP AD. Sin embargo, el protocolo que se ejecuta después de la migración tiene valores no predeterminados, lo que puede afectar a otras partes de la implementación.

En este ejemplo, se utiliza el comando debug ip routing para verificar la operación en el spoke.

> **Nota:** Si la información de esta sección se utiliza en una red de producción, evite el uso de los comandos debug y confíe en los comandos show enumerados en la siguiente sección. Además, el proceso EIGRP radial debe restablecer la adyacencia con el hub.

```
Spoke1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Spoke1(config)#router eigrp 100
Spoke1(config-router)# distance eigrp 230 240
Spoke1(config-router)#^Z
Spoke1#
*Oct 9 12:12:34.207: %SYS-5-CONFIG_I: Configured from console by console
```

```
*Oct 9 12:12:43.648: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is down: route configuration changed

*Oct 9 12:12:43.648: RT: delete route to 192.168.0.0 via 10.0.0.1,
 eigrp metric [90/26880000]
*Oct 9 12:12:43.648: RT: no routes to 192.168.0.0, delayed flush
*Oct 9 12:12:43.648: RT: delete network route to 192.168.0.0/16
*Oct 9 12:12:43.650: RT: updating bgp 192.168.0.0/16 (0x0) :
via 10.1.1.1

*Oct 9 12:12:43.650: RT: add 192.168.0.0/16 via 10.1.1.1, bgp metric [200/0]
Spoke1#
*Oct 9 12:12:45.750: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is up: new adjacency
```

Hay tres acciones importantes que deben tenerse en cuenta en este resultado:

- El spoke observa que el AD cambió y deshabilita la adyacencia.
- En la tabla de ruteo, se retira el prefijo EIGRP y se introduce el BGP.
- La adyacencia al hub a través del EIGRP vuelve a estar en línea.

Cuando cambia el AD en un dispositivo, sólo afecta el trayecto del dispositivo a las otras redes; no afecta al modo en que otros routers realizan el ruteo. Por ejemplo, después de aumentar la distancia EIGRP en **Spoke1** (y utiliza FlexVPN en la nube para enrutar el tráfico), el hub mantiene los AD configurados (predeterminados). Esto significa que utiliza DMVPN para rutear el tráfico nuevamente a **Spoke1**.

En algunos escenarios, esto puede causar problemas, como cuando los firewalls esperan tráfico de retorno en la misma interfaz. Por lo tanto, debe cambiar el AD en todos los radios antes de cambiarlo en el hub. FlexVPN migra completamente el tráfico solo una vez que se ha completado.

Migración de EIGRP a EIGRP

En este documento no se analiza en profundidad una migración de DMVPN a FlexVPN que ejecuta solamente EIGRP; sin embargo, se menciona aquí para más detalles.

Es posible agregar DMVPN y EIGRP a la misma instancia de routing del sistema autónomo EIGRP (AS). Con esto en su lugar, la adyacencia de ruteo se establece sobre ambos tipos de nubes. Esto puede hacer que se produzca un balanceo de carga, lo que normalmente no se recomienda.

Para asegurarse de que se elige FlexVPN o DMVPN, un administrador puede asignar diferentes valores de **retraso** por interfaz. Sin embargo, es importante recordar que no es posible realizar cambios en las interfaces de plantilla virtual mientras que las interfaces de acceso virtual correspondientes están presentes.

Comprobaciones posteriores a la migración

De manera similar al proceso utilizado en la sección **Verificaciones previas a la migración**, se debe verificar el IPSec y el protocolo de ruteo.

Primero, verifique el IPSec:

```
Spoke1#show crypto session
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

Como antes, se ven dos sesiones, ambas con dos SA IPSec activas.

En el spoke, la ruta agregada (192.168.0.0/16) apunta desde el hub y se aprende sobre el BGP.

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.1 00:14:07 ago
Routing Descriptor Blocks:
* 10.1.1.1, from 10.1.1.1, 00:14:07 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none
```

De manera similar, la LAN de radio que está prefijada en el hub debe ser conocida a través del EIGRP. En este ejemplo, la subred LAN Spoke2 está marcada:

```
Hub#show ip route 192.168.102.0 255.255.255.0
Routing entry for 192.168.102.0/24
 Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.106 00:04:35 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:04:35 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none

Hub#show ip cef 192.168.102.100
192.168.102.0/24
nexthop 10.1.1.106 Virtual-Access2
```

En el resultado, la trayectoria de reenvío se actualiza correctamente y se señala desde una interfaz de acceso virtual.

Consideraciones adicionales

Esta sección describe algunas áreas adicionales de importancia que son relevantes para este ejemplo de configuración.

Túneles de radio a radio existentes

Con una migración de EIGRP a BGP, los túneles de spoke a spoke no se ven afectados, porque el switching de acceso directo todavía está en funcionamiento. El switching de acceso directo en el spoke inserta una ruta NHRP más específica con un AD de 250.

Aquí hay un ejemplo de tal ruta:

```
Spoke1#show ip route 192.168.102.100
Routing entry for 192.168.102.0/24
Known via "nhrp", distance 250, metric 1
Last update from 10.1.1.106 on Virtual-Access1, 00:00:42 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:00:42 ago, via Virtual-Access1
Route metric is 1, traffic share count is 1
```

Comunicación entre radios migradas y no migradas

Si un spoke que ya se encuentra en un FlexVPN/BGP desea comunicarse con un dispositivo para el que el proceso de migración no ha comenzado, el tráfico siempre fluye a través del hub.

Este es el proceso que ocurre:

1. El spoke realiza una búsqueda de ruta para el destino, que apunta a través de una ruta de resumen anunciada por el hub.
2. El paquete se envía hacia el hub.
3. El hub recibe el paquete y realiza una búsqueda de ruta para el destino, que señala desde otra interfaz que forma parte de un dominio NHRP diferente.

   Nota: El ID de red NHRP en la configuración del hub anterior es diferente tanto para FlexVPN como para DMVPN.

Incluso si los ID de red NHRP están unificados, puede ocurrir un problema cuando el spoke migrado enruta objetos a través de la red FlexVPN. Esto incluye la directiva utilizada para configurar la conmutación de acceso directo. El spoke no migrado intenta ejecutar objetos a través de la red DMVPN, con un objetivo específico para realizar el switching de acceso directo.

Troubleshoot

En esta sección se describen las dos categorías que se utilizan habitualmente para solucionar la migración.

Problemas con los Intentos de Establecer Túneles

Complete estos pasos si falla la negociación IKE:

1. Verifique el estado actual con estos comandos:

show crypto isakmp sa - Este comando revela la cantidad, el origen y el destino de una sesión IKEv1.**show crypto ipsec sa** - Este comando revela la actividad de las SAs IPsec.**Nota:** A diferencia de IKEv1, en este resultado el valor Diffie-Hellman (DH) Diffie-Secrecy Perfect Forward Secrecy (PFS) Group aparece como **PFS (Y/N): N, grupo DH: ninguno** durante la primera negociación del túnel; sin embargo, después de que se produce una nueva clave, aparecen los valores correctos. Esto no es un error, aunque el comportamiento se describe en CSCug67056. La diferencia entre IKEv1 e IKEv2 es que en este último, las SAs secundarias se crean como parte del intercambio **AUTH**. El grupo DH configurado bajo el mapa criptográfico se utiliza solamente durante una nueva clave. Por esta razón, verá **PFS (Y/N): N, grupo DH: ninguno hasta la primera llave.** Con IKEv1, verá un comportamiento diferente porque la creación de SA secundaria ocurre durante el modo rápido, y el mensaje **CREATE_CHILD_SA** contiene disposiciones para la transferencia de la carga útil de intercambio de claves que especifica los parámetros DH para derivar un nuevo secreto compartido.**show crypto ikev2 sa** - Este comando proporciona resultados similares a ISAKMP pero es específico de IKEv2.**show crypto session** - Este comando proporciona el resultado de resumen de las sesiones criptográficas en este dispositivo.**show crypto socket** - Este comando muestra el estado de los crypto-sockets.**show crypto map** - Este comando muestra la asignación de perfiles IKE e IPsec a las interfaces.**show ip nhrp** - Este comando proporciona la información NHRP del dispositivo. Esto es útil para spoke-to-spoke en las configuraciones de FlexVPN y para los enlaces de spoke-to-spoke y spoke-to-hub en las configuraciones de DMVPN.

2. Utilice estos comandos para depurar el establecimiento del túnel:

   debug crypto ikev2debug crypto isakmpdebug crypto ipsecdebug crypto kmi

Problemas con la Propagación de Rutas

Estos son algunos comandos útiles que puede utilizar para resolver problemas de EIGRP y topología:

- **show bgp summary** - Utilice este comando para verificar los vecinos conectados y sus estados.
- **show ip eigrp neighbor** - Utilice este comando para mostrar los vecinos que están conectados a través de EIGRP.
- **show bgp** - Utilice este comando para verificar los prefijos aprendidos sobre el BGP.
- **show ip eigrp topology** - Utilice este comando para mostrar los prefijos aprendidos a través de EIGRP.

Es importante saber que un prefijo aprendido es diferente de un prefijo que está instalado en la tabla de ruteo. Para obtener más información sobre esto, refiérase al artículo Selección de ruta en routers Cisco de Cisco o al Libro de Cisco Press sobre TCP/IP de enrutamiento.

Advertencias conocidas

Existe una limitación que coincide con el manejo del túnel GRE en el ASR1K. Esto se rastrea bajo el ID de bug de Cisco CSCue00443. En este momento, la limitación tiene una corrección programada en Cisco IOS XE Software Release 3.12.

Controle este error si desea una notificación una vez que la corrección esté disponible.