DMVPN al ejemplo de configuración suave de la migración de FlexVPN

Contenido

Introducción

Este documento describe cómo realizar una migración *suave* donde el Dynamic Multipoint VPN (DMVPN) y FlexVPN trabajan en un dispositivo simultáneamente sin la necesidad de una solución alternativa y proporciona un ejemplo de configuración.

> **Note**: Este documento se amplía en los conceptos descritos en la migración de FlexVPN: Movimiento duro del DMVPN a FlexVPN en los mismos dispositivos y migración de FlexVPN: Movimiento duro del DMVPN a FlexVPN en artículos de Cisco diversos de un concentrador. Ambos documentos describen las migraciones *duras*, que hacen una cierta interrupción traficar durante la migración. Las limitaciones en estos artículos son debido a

una deficiencia en el software del ® del Cisco IOS que ahora se rectifica.

Prerequisites

Requisitos

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.

- Versiones del router del servicio integrado de Cisco (ISR) el 15.3(3)M o más adelante
- El router agregado las Cisco 1000 Series del servicio (ASR1K) libera 3.10 o más adelante

Note: No todo el intercambio de claves de Internet de los soportes de software y de hardware versión 2 (IKEv2). Refiera al Cisco Feature Navigator para la información.

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.

Antecedentes

Una de las ventajas de las más nuevos plataformas de Cisco IOS y software es la capacidad de utilizar la criptografía de la última generación. Un ejemplo es el uso del Advanced Encryption Standard (AES) en Galois/el modo contrario (GCM) para el cifrado en el IPSec, como se debate en el RFC 4106. El AES GCM permite velocidades mucho más rápidas del cifrado en un poco de hardware.

Note: Para más información sobre el uso de y la migración a la criptografía de la última generación, refiera al artículo de Cisco del cifrado de la última generación.

Configurar

Este ejemplo de configuración se centra en una migración de una configuración de la fase 3 DMVPN a un FlexVPN, porque ambos diseños trabajan semejantemente.

	Fase 2 DMVPN	Fase 3 DMVPN	FlexVPN

Transporte	GRE sobre IPSec	GRE sobre IPSec	GRE sobre IPSec
Uso NHRP	Registro y resolución	Registro y resolución	Resolución
Salto siguiente del spoke	El otro spokes o concentrador	Resumen del concentrador	Resumen del concentrador
Transferencia del acceso directo NHRP	No	Yes	Sí (opcional)
Cambio de dirección NHRP	No	Yes	Yes
IKE y IPSec	IPSec opcional, IKEv1 típico	IPSec opcional, IKEv1 típico	IPSec, IKEv2

Diagramas de la Red

Esta sección proporciona los diagramas de la red del transporte y del recubrimiento.

Diagrama de red de transporte

La red de transporte usada en este ejemplo incluye a hub único con dos spokes conectados. Todos los dispositivos están conectados a través de una red que simule Internet.

Diagrama de la red del recubrimiento

La red de recubrimiento usada en este ejemplo incluye a hub único con dos spokes conectados. Recuerde que el DMVPN y FlexVPN son activos simultáneamente, solamente ellos utilizan diversos espacios de IP Address.

Configuraciones

Esta configuración emigra el despliegue más popular de la fase 3 DMVPN vía el Enhanced Interior Gateway Routing Protocol (EIGRP) a FlexVPN con el Border Gateway Protocol (BGP). Cisco recomienda el uso del BGP con FlexVPN, porque permite que las implementaciones escalen mejor.

> **Note**: El concentrador termina las sesiones IKEv1 (DMVPN) e IKEv2 (FlexVPN) sobre la misma dirección IP. Esto es posible solamente con las versiones recientes del Cisco IOS.

Configuración radial

Éste es mismo una configuración básica, con dos excepciones notables que permitan la interoperación de IKEv1 y de IKEv2, así como dos marcos que utilizan el Generic Routing Encapsulation (GRE) sobre el IPSec para el transporte para coexistir.

> **Note**: Los cambios relevantes al Internet Security Association and Key Management Protocol (ISAKMP) y la configuración IKEv2 se resaltan en intrépido.

```
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
```

El Cisco IOS Release 15.3 permite que usted ate IKEv2 y los perfiles ISAKMP juntos en una *configuración de protección del túnel*. Junto con algunos cambios internos al código, esto permite que IKEv1 e IKEv2 actúen encendido el mismo dispositivo simultáneamente.

Debido a la manera el Cisco IOS selecciona los perfiles (IKEv1 o IKEv2) en las versiones anterior de 15.3, él llevaron a algunas advertencias, tales como situaciones donde IKEv1 se inicia a IKEv2 a través del par. La separación de IKE ahora se basa en el perfil-nivel, no el interfaz-nivel, que se alcanza vía el nuevo CLI.

Otra actualización en la versión del nuevo Cisco IOS es la adición de la *clave del túnel*. Esto es necesario porque el DMVPN y FlexVPN utilizan la misma interfaz de origen y el mismo IP Address de destino. Con esto en el lugar, no hay manera para que el túnel GRE sepa qué interfaz del túnel es para tráfico usado del decapsulate. La clave del túnel permite que usted distinga el **tunnel0** y **tunnel1** con la adición de los pequeños (gastos indirectos del byte 4). Una diversa clave se puede configurar en ambas interfaces, pero usted necesita típicamente solamente distinguir un túnel.

> **Note**: La opción de protección compartida del túnel no se requiere cuando el DMVPN y FlexVPN comparten la misma interfaz.

Así, la configuración del Routing Protocol del spoke es básica. El EIGRP y el BGP trabajan por separado. El EIGRP hace publicidad solamente sobre la interfaz del túnel para evitar mirar sobre los túneles del spoke al spoke, que limita el scalability. El BGP mantiene una relación solamente con el router de eje de conexión (**10.1.1.1**) para hacer publicidad de la red local (**192.168.101.0/24**).

```
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
```

Configuración del hub

Usted debe realizar los cambios similares en la configuración del lado del eje de conexión como ésos descritos en la sección de **configuración radial**.

Note: Los cambios relevantes a la configuración ISAKMP e IKEV2 se resaltan en intrépido.

```
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


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 eje de conexión, el atascamiento entre el perfil IKE y el perfil de ipsec ocurre en el perfil-nivel, a diferencia de la configuración radial, donde esto se completa vía el **comando tunnel protection**. Ambos acercamientos son métodos viables para completar este atascamiento.

Es importante observar que los ID de la red del Next Hop Resolution Protocol (NHRP) son diferentes para el DMVPN y FlexVPN en la nube. En la mayoría de los casos, es indeseable cuando el NHRP crea un solo dominio sobre ambos marcos.

La clave del túnel distingue el DMVPN y los túneles de FlexVPN en el GRE-nivel para alcanzar la misma meta que se menciona en la sección de **configuración radial**.

La configuración de ruteo en el concentrador es bastante básica. El dispositivo del concentrador mantiene dos relaciones con spoke, que utiliza el EIGRP y dado que utilice el BGP. La

configuración BGP utiliza el escuchar-rango para evitar un muy largo, configuración del por-spoke.

Presentan a las direcciones de resumen dos veces. La configuración EIGRP envía un resumen con el uso de la configuración del **tunnel0** (EIGRP 100 del resumen-direccionamiento IP), y el BGP introduce un resumen con el uso del agregado-direccionamiento. Los resúmenes se requieren para asegurarse de que ocurra el cambio de dirección NHRP, y para simplificar las actualizaciones de ruteo. Usted puede enviar un NHRP reorienta (como un Internet Control Message Protocol (ICMP) reoriente) que indique si un mejor salto existe para un destino determinado, que permite que un túnel del spoke al spoke sea establecido. Estos resúmenes también se utilizan para minimizar la cantidad de actualizaciones de ruteo que se envíen entre el concentrador y cada spoke, que permite que las configuraciones 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.

Controles de la premigración

Puesto que DMVPN/EIGRP y FlexVPN/BGP actúan simultáneamente, usted debe verificar que el spoke mantenga una relación sobre el IPSec con IKEv1 e IKEv2, y que los prefijos apropiados son doctos sobre el EIGRP y el BGP.

En este ejemplo, el **Spoke1** muestra que dos sesiones están mantenidas con el router de eje de conexión; uno utiliza IKEv1/Tunnel0 y uno utiliza IKEv2/Tunnel1.

> **Note**: Mantienen a dos asociaciones de seguridad IPSec (SA) (uno entrante y uno 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 usted marca los Routing Protocol, usted debe verificar que una vecindad esté formada, y que los prefijos correctos son doctos. Esto primero se marca con el EIGRP. Verifique que el concentrador sea visible como vecino, y que el direccionamiento 192.168.0.0/16 (el resumen) es docto del concentrador:

```
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
```

Después, 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
```

La salida muestra que la dirección IP de FlexVPN del concentrador (10.1.1.1) es un vecino a través de quien el spoke recibe un prefijo (192.168.0.0/16). Además, el BGP informa al administrador que un error del Routing Information Base (RIB) ocurrió para el prefijo 192.168.0.0/16. Este error ocurre porque hay una mejor ruta para ese prefijo que exista ya en la

tabla de ruteo. Esta ruta es originada por el EIGRP, y puede ser confirmada si usted marca 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 el IPSec y los Routing Protocol estén configurados y trabajo como se esperaba. Una de las maneras más fáciles de emigrar del DMVPN a FlexVPN en el mismo dispositivo es cambiar la distancia administrativa (AD). En este ejemplo, el Internal BGP (iBGP) tiene un AD de 200, y el EIGRP tiene un AD de 90.

Para que el tráfico atraviese el FlexVPN correctamente, el BGP debe tener un mejor AD. En este ejemplo, el EIGRP AD se cambia a 230 y a 240 para el Routes interno y externo, respectivamente. Esto hace el BGP AD (de 200) más preferible para el prefijo 192.168.0.0/16.

Otro método que se utiliza para alcanzar esto es disminuir el BGP AD. Sin embargo, el protocolo que se ejecuta después de que la migración tenga valores no predeterminados, que pueden afectar a otras partes del despliegue.

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

> **Note**: Si la información en 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. También, el proceso EIGRP del spoke debe restablecer la adyacencia con el concentrador.

```
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
```

```
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
```

Hay tres acciones importantes a notar en esta salida:

- El spoke nota que el AD cambiado, y inhabilita la adyacencia.
- En la tabla de ruteo, el prefijo del EIGRP retied, y se introduce el BGP.
- La adyacencia al concentrador sobre el EIGRP se vuelve en línea.

Cuando usted cambia el AD en un dispositivo, afecta solamente a la trayectoria del dispositivo a las otras redes; no afecta a cómo el otro Routers realiza la encaminamiento. Por ejemplo, después de que la distancia del EIGRP se aumente en el **Spoke1** (y él utiliza FlexVPN en la nube para rutear el tráfico), el concentrador mantiene los AD (predeterminados) configurados. Esto significa que utiliza el DMVPN para rutear el tráfico de nuevo al **Spoke1**.

En ciertos escenarios, esto puede causar los problemas, por ejemplo cuando los Firewall cuentan con el tráfico de retorno en la misma interfaz. Por lo tanto, usted debe cambiar el AD en todo el spokes antes de que usted lo cambie en el concentrador. El tráfico es emigrado completamente por FlexVPN solamente una vez que éste es completo.

Migración del Eigrp-a-EIGRP

Una migración del DMVPN a FlexVPN que ejecute solamente el EIGRP no es profundizada discutido en este documento; sin embargo, se menciona aquí para lo completo.

Es posible agregar el DMVPN y el EIGRP al mismo sistema autónomo EIGRP (QUE) que rutea el caso. Con esto en el lugar, la adyacencia de la encaminamiento se establece sobre ambos tipos de nubes. Esto puede hacer el balanceo de carga ocurrir, que no se recomienda típicamente.

Para asegurarse de que FlexVPN o el DMVPN esté elegido, un administrador puede asignar diversos **valores de retraso** sobre una base del por interface. Sin embargo, es importante recordar que no hay cambios posibles en las interfaces de plantilla virtual mientras que las interfaces de acceso virtual correspondientes están presentes.

Controles de la post transferencia

Similar al proceso usado en la **premigración marca la** sección, el IPSec y el Routing Protocol debe ser verificado.

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 consideran dos sesiones, que tienen dos IPSec activo SA.

En el spoke, el total de Routes (192.168.0.0/16) señala del concentrador y es docto 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
```

Semejantemente, el spoke LAN que se prefija en el concentrador se debe saber vía el EIGRP. En este ejemplo, se marca la subred LAN del Spoke2:

```
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 la salida, el trayecto de reenvío se pone al día correctamente y señala de una interfaz de acceso virtual.

Consideraciones adicionales

Esta sección describe algunas áreas adicionales de importancia que sean relevantes a este

ejemplo de configuración.

Túneles existentes del spoke al spoke

Con una migración del EIGRP al BGP, los túneles del spoke al spoke no se afectan, porque la acceso directo-transferencia es todavía en funcionamiento. la Acceso directo-transferencia en el spoke inserta una ruta más específica NHRP con un AD de 250.

Aquí está 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 el spokes emigrado y NON-emigrado

Si un spoke que está ya en un FlexVPN/BGP quiere comunicar con un dispositivo para el cual el proceso de migración no ha comenzado, el tráfico fluye siempre sobre el concentrador.

Éste es el proceso que ocurre:

1. El spoke realiza las operaciones de búsqueda de la ruta para el destino, que señala a través de una ruta de resumen que sea hecha publicidad por el concentrador.
2. El paquete se envía hacia el concentrador.
3. El concentrador recibe el paquete y realiza las operaciones de búsqueda de la ruta para el destino, que señala de otra interfaz que sea parte de a diverso dominio NHRP.

   Note: La red NHRP ID en la Configuración del hub anterior es diferente para FlexVPN y el DMVPN.

Incluso si se unifica la red NHRP ID, un problema pudo ocurrir donde el spoke emigrado rutea los objetos sobre la red de FlexVPN. Esto incluye la directiva usada para configurar la transferencia del acceso directo. El spoke NON-emigrado intenta ejecutar los objetos sobre la red DMVPN, con una meta específica para realizar la transferencia del acceso directo.

Troubleshooting

Esta sección describe el toubleshoot típicamente usado de dos categorías para la migración.

Problemas con las tentativas de establecer los túneles

Complete estos pasos si la negociación IKE falla:

1. Verifique al estado actual con estos comandos:

muestre isakmp crypto sa - Este comando revela la cantidad, la fuente, y el destino de una sesión IKEv1.**la demostración crypto** comando **sa del IPSec** este revela la actividad del SA de IPSec.**Note**: A diferencia en de IKEv1, en este hecho salir el valor de grupo del Diffie-Hellman (DH) del Confidencialidad directa perfecta (PFS) aparece como **PFS (Y/N): N, grupo DH: ningunos** durante la primera negociación de túnel; sin embargo, después de que ocurra una reintroducción, los valores correctos aparecen. Esto no es un bug, aunque el comportamiento se describe en CSCug67056. La diferencia entre IKEv1 e IKEv2 es ésa en estos últimos, el niño que los SA se crean como parte del intercambio **AUTH**. Utilizan al grupo DH que se configura bajo correspondencia de criptografía solamente durante una reintroducción. Por este motivo, usted ve el **PFS (Y/N): N, grupo DH: ningunos** hasta los primeros reintroducen. Con IKEv1, usted ve un diverso comportamiento porque la creación niño SA ocurre durante el Quick Mode, y el mensaje **CREATE_CHILD_SA** tiene disposiciones para la transferencia del payload del intercambio de claves que especifica los parámetros DH para derivar un nuevo secreto compartido.**muestre ikev2 crypto sa** - Este comando proporciona la salida similar al ISAKMP pero es específico a IKEv2.**sesión de criptografía de la demostración** - Este comando proporciona el resumen de resultado de las sesiones criptográficas sobre este dispositivo.**muestre el socket crypto** - Este comando muestra el estatus de los crypto-socketes.**correspondencia de criptografía de la demostración** - Este comando muestra la asignación del IKE y de los perfiles de ipsec a las interfaces.**muestre el nhrp del IP** - Este comando proporciona la información NHRP del dispositivo. Esto es útil para el spoke al spoke en configuraciones de FlexVPN, y para los atascamientos del spoke al spoke y del spoke a hub en configuraciones DMVPN.
2. Utilice estos comandos para hacer el debug de al establecimiento del túnel:

   debug crypto ikev2debug crypto isakmp**debug crypto ipseckmi del debug crypto**

Problemas con la propagación de la ruta

Aquí están algunos comandos útiles que usted puede utilizar para resolver problemas el EIGRP y la topología:

- **muestre el resumen BGP** - Utilice este comando para verificar los vecinos conectados y sus estados.
- **muestre al vecino del eigrp del IP** - Utilice este comando para mostrar a los vecinos que están conectados vía el EIGRP.
- **BGP de la demostración** - Utilice este comando para verificar los prefijos aprendidos sobre el BGP.
- **muestre la topología EIGRP del IP** - Utilice este comando para mostrar los prefijos aprendidos vía el EIGRP.

Es importante saber que un prefijo docto es diferente que un prefijo que esté instalado en la tabla de ruteo. Para más información sobre esto, refiérase a la selección de Route al artículo de Cisco de los routeres Cisco, o al Cisco Press Book TCP/IP que rutea.

Advertencias conocidas

Una limitación que es paralelo a la dirección del túnel GRE existe en el ASR1K. Esto se sigue bajo el Id. de bug Cisco CSCue00443. Ahora, la limitación tiene un arreglo programado en la versión 3.12 del Software Cisco IOS XE.

Monitoree este bug si usted desea una notificación que el arreglo está una vez disponible.