Migración de FlexVPN: Movimiento duro del DMVPN a FlexVPN en un diverso concentrador

Contenido

Introducción

Este documento proporciona la información sobre cómo emigrar de una red del Dynamic Multipoint VPN (DMVPN) que exista actualmente a FlexVPN en diversos dispositivos del concentrador. Los configuations para ambos marcos coexisten en los dispositivos. En este documento, solamente la mayoría del escenario frecuente se muestra - DMVPN con el uso de la clave del preshared para la autenticación y del Enhanced Interior Gateway Routing Protocol (EIGRP) como el Routing Protocol. En este documento, la migración al Border Gateway Protocol (BGP), que es el Routing Protocol recomendado, y el EIGRP menos-deseable se demuestra.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento básico de estos temas:

- DMVPN
- FlexVPN

Componentes Utilizados

> Nota: 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 más información.

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

- Versión 15.2(4)M1 posterior del router del servicio integrado de Cisco (ISR)
- Versión 3.6.2 15.2(2)S2 de las 1000 Series del router de los servicios de la agregación de Cisco (ASR1K) o más nuevo

Uno las ventajas de una más nuevos plataforma y software es la capacidad de utilizar la criptografía de la última generación, tal como Advanced Encryption Standard (AES) Galois/modo contrario (GCM) para el cifrado en la seguridad de protocolos en Internet (IPSec), como se debate en la Solicitud de comentarios (RFC) 4106. El AES GCM permite que usted alcance una velocidad mucho más rápida del cifrado en un poco de hardware. Para ver las Recomendaciones de Cisco en el uso de y la migración a la criptografía de la última generación, refiera al artículo del cifrado de la última generación.

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.

Procedimiento de migración

Actualmente, el método recomendado a emigrar del DMVPN a FlexVPN está para que los dos marcos no actúen al mismo tiempo. Esta limitación se programa para deber quitado a las nuevas características de la migración ser introducido en la versión ASR 3.10, seguida conforme a los pedidos de mejora del multilple en el lado de Cisco, que incluyen el Id. de bug Cisco CSCuc08066. Esas características deben ser a finales de junio 2013 disponibles.

Una migración donde ambos marcos coexisten y actúan al mismo tiempo en los mismos dispositivos se refiere como **migración suave**, que indica el efecto mínimo y la Conmutación por falla lisa a partir de un marco a otro. Una migración donde coexisten las configuraciones para ambos marcos, pero no actúa al mismo tiempo se refiere como **migración dura**. Esto indica que un intercambio a partir de un marco a otro significa una falta de comunicación sobre el VPN, incluso si es mínimo.

Migración dura entre dos diverso Hubs

En este documento, la migración del concentrador DMVPN que se utiliza actualmente a un nuevo concentrador de FlexVPN se discute. Esta migración permite la intercomunicación entre el spokes emigrada ya a FlexVPN, y las que todavía se ejecutan en el DMVPN y se pueden realizar en fases múltiples, en cada hablaron por separado.

A condición de que la información de ruteo se puebla correctamente, la comunicación entre el spokes emigrado y nonmigrated debe seguir siendo posible. Sin embargo, el tiempo de espera adicional puede ser observado porque está emigrado y el spokes nonmigrated no construye los túneles del spoke al spoke entre uno a. Al mismo tiempo, el spokes emigrado debe poder establecer los túneles directos del spoke al spoke entre ellos mismos. Lo mismo se aplica al spokes nonmigrated.

Hasta que esta nueva característica de la migración esté disponible, complete estos pasos para realizar las migraciones con un diverso concentrador del DMVPN y de FlexVPN:

1. Verifique la Conectividad sobre el DMVPN.
2. Agregue la configuración de FlexVPN, y apague el túnel que pertenece a la nueva configuración.
3. (Durante una ventana de mantenimiento) en cada spoke, uno por uno, apague el túnel DMVPN.
4. En el mismo spoke que en el paso 3, unshut las interfaces del túnel de FlexVPN.
5. Verifique la Conectividad del spoke a hub.
6. Verifique la Conectividad del spoke al spoke dentro de FlexVPN.
7. Verifique la Conectividad del spoke al spoke con el DMVPN de FlexVPN.
8. Relance los pasos 3 a 7 para cada habló por separado.
9. Si usted encuentra cualesquiera problemas con las verificaciones descritas en los pasos 5, 6, o 7, apague la interfaz de FlexVPN, y el unshut las interfaces DMVPN para invertir al DMVPN.
10. Verifique la comunicación del spoke a hub sobre el DMVPN con copia de seguridad.
11. Verifique la comunicación del spoke al spoke sobre el DMVPN con copia de seguridad.

Acercamiento de encargo

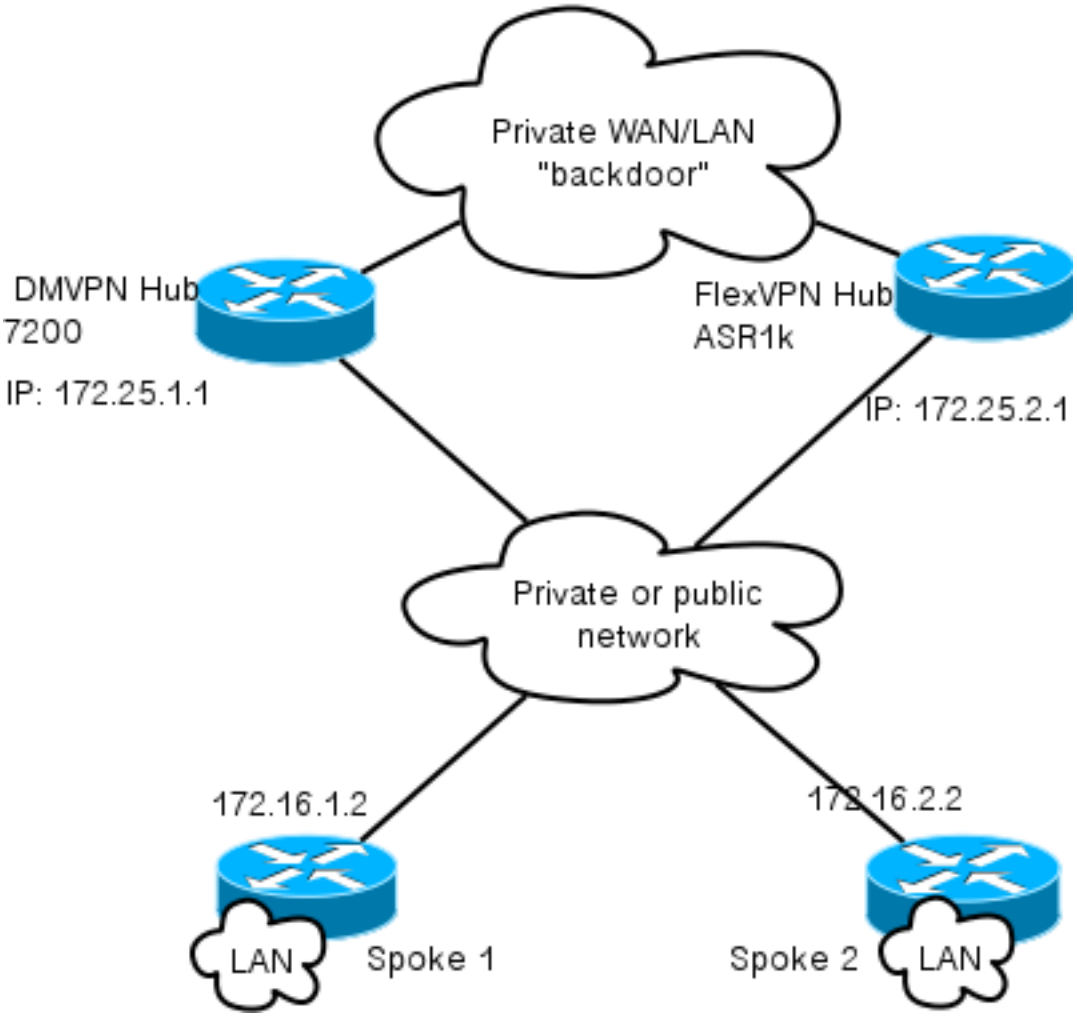
Si el acercamiento anterior no pudo ser la mejor solución para usted debido a sus complejidades

de la red o de la encaminamiento, comience una discusión con su representante de Cisco antes de que usted emigre. La mejor persona con quien discutir un proceso de migración de encargo es su ingeniero en sistemas o ingeniero del Advanced Services.

Topología de red

Topología de red de transporte

Este diagrama muestra la topología de la conexión típica de los host en Internet. La dirección IP del concentrador del **loopback0** (**172.25.1.1**) se utiliza para terminar el DMVPN sesión IPSec. La dirección IP en el nuevo concentrador (**172.25.2.1**) se utiliza para FlexVPN.

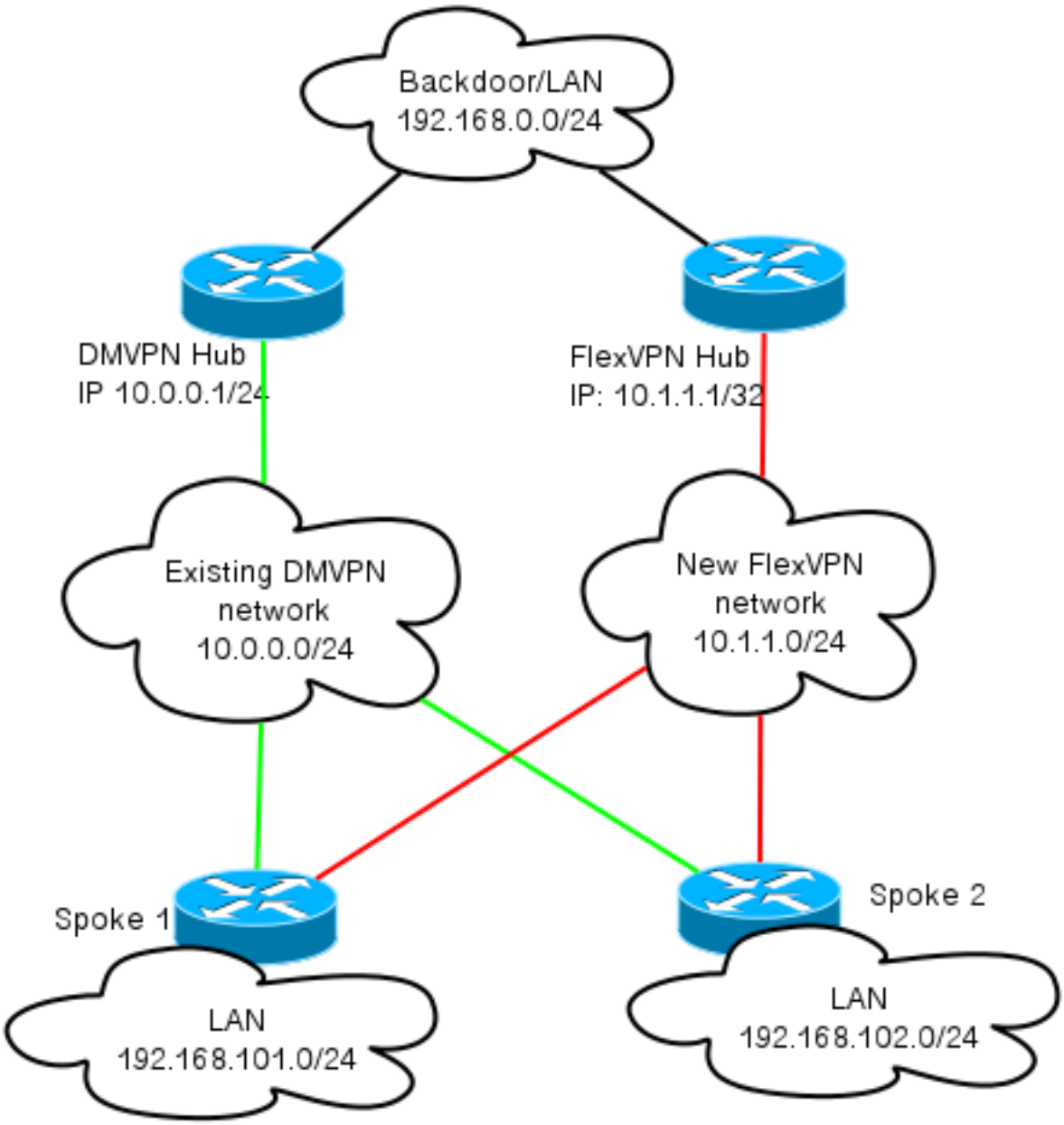


Note el link entre el dos Hubs. Este link es crucial para permitir la Conectividad entre el FlexVPN y las nubes DMVPN durante la migración. Permite el spokes emigrado ya a FlexVPN para comunicar con las redes DMVPN y vice versa.

Topología de red del recubrimiento

Este Diagrama de topología muestra dos nubes separadas usadas para el recubrimiento: DMVPN (conexiones verdes) y FlexVPN (conexiones rojas). Los prefijos LAN se muestran para los sitios correspondientes. La subred **10.1.1.0/24** no representa una subred real en términos de interfaz

que dirige, sino representa un pedazo del espacio IP dedicado a la nube de FlexVPN. El fundamento detrás de esto se discute más adelante en la **sección de configuración de FlexVPN**.



Configuración

Esta sección describe el DMVPN y las configuraciones de FlexVPN.

Configuración DMVPN

Esta sección describe la configuración básica para el hub and spoke DMVPN.

La clave previamente compartida (PSK) se utiliza para la autenticación IKEv1. Una vez que se establece el IPSec, el registro del Next Hop Resolution Protocol (NHRP) del spoke a hub se realiza de modo que el concentrador pueda aprender el acceso múltiple sin broadcast de los rayos (NBMA) que dirige dinámicamente.

Cuando el NHRP realiza el registro en el spoke y el concentrador, rutear el adjacancy puede

establecer, y las rutas pueden ser intercambiadas. En este ejemplo, el EIGRP se utiliza como Routing Protocol básico para la red de recubrimiento.

Configuración del spoke DMVPN

Aquí usted puede encontrar una configuración del ejemplo básico del DMVPN con la autenticación del PSK y del EIGRP como el Routing Protocol.

```
crypto isakmp policy 10
 encr aes
 authentication pre-share

crypto isakmp key cisco address 0.0.0.0

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

interface Tunnel0

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 protection ipsec profile DMVPN_IKEv1

router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.102.0
passive-interface default
no passive-interface Tunnel0
```

Configuración del concentrador DMVPN

En la Configuración del hub, el túnel es originado del **loopback0** con un IP Address de **172.25.1.1**. El resto es un despliegue estándar de un concentrador DMVPN con el EIGRP como el Routing Protocol.

```
crypto isakmp policy 10
encr aes
authentication pre-share
```

```
crypto isakmp key cisco 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

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 protection ipsec profile DMVPN_IKEv1

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
```

Configuración de FlexVPN

FlexVPN se basa en estas mismas Tecnologías fundamentales:

- **IPSec**: A diferencia del valor por defecto en el DMVPN, IKEv2 se utiliza en vez de IKEv1 para negociar las asociaciones de seguridad IPSec (SA). IKEv2 ofrece las mejoras sobre IKEv1, tal como elasticidad y el número de mensajes que sean necesarios para establecer un canal de datos protegidos.

- **GRE**: A diferencia del DMVPN, se utilizan las interfaces Point-to-Point estáticas y dinámicas, y no sólo una interfaz estática del multpoint GRE. Esta configuración permite la flexibilidad agregada, especialmente para el por-spoke/el comportamiento del por-concentrador.

- **NHRP**: En FlexVPN, el NHRP se utiliza sobre todo para establecer la comunicación del spoke al spoke. El spokes no se registra al concentrador.

- **El rutear**: Porque el spokes no realiza el registro NHRP al concentrador, usted debe confiar en otros mecanismos para aseegurarse el concentrador y el spokes puede comunicar bidireccional. Simliar al DMVPN, los Dynamic Routing Protocol puede ser utilizado. Sin embargo, FlexVPN permite que usted utilice el IPSec para introducir la información de ruteo. El valor por defecto es introducir como ruta de **/32** para la dirección IP en el otro lado del túnel, que permite la comunicación directa del spoke a hub.

En una migración dura del DMVPN a FlexVPN, los dos framemworks no trabajan al mismo tiempo en los mismos dispositivos. Sin embargo, se recomienda para mantenerlos separados.

Sepárelos en varios niveles:

- NHRP - Utilice una diversa red NHRP ID (recomendada).
- El rutear - Utilice los procesos de ruteo separados (recomendados).
- Ruteo virtual y expedición (VRF) - La separación VRF permite la flexibilidad agregada pero no se discute aquí (opcional).

Configuración de FlexVPN del spoke

Una de las diferencias en la configuración radial en FlexVPN con respecto al DMVPN es que usted potencialmente tiene dos interfaces. Hay un túnel requerido para la comunicación del spoke a hub y un túnel opcional para los túneles del spoke al spoke. Si usted elige no tener Tunelización dinámico del spoke al spoke y preferiría que todo pasa a través del dispositivo del concentrador, usted puede quitar la interfaz de plantilla virtual, y quita la transferencia del acceso directo NHRP de la interfaz del túnel.

Note que la interfaz del túnel estática recibe una dirección IP basada en la negociación. Esto permite que el concentrador proporcione la dirección IP de la interfaz del túnel al spoke dinámicamente sin la necesidad de crear la dirección estática en la nube de FlexVPN.

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 profile Flex_IKEv2
match identity remote fqdn domain cisco.com
local identity fqdn spoke.cisco.com
authentication remote rsa-sig
authentication local rsa-sig
aaa authorization group cert list default default
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

> Nota: Por abandono, la identidad local se fija para utilizar la dirección IP. La declaración de coincidencia correspondiente en el par debe hacer juego tan basado en el direccionamiento también. Si el requisito es hacer juego basado en el Nombre distintivo (DN) en el certifcate, después la coincidencia se debe hacer con el uso de una correspondencia del certificado.

Cisco recomienda que usted utiliza AES GCM con el hardware que lo soporta.

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

crypto ipsec profile default
set ikev2-profile Flex_IKEv2
! set transform-set IKEv2

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

```
interface Virtual-Template1 type tunnel
ip unnumbered Tunnel1
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 Public Key Infrastructure (PKI) es el método recomendado para realizar la autenticación del gran escala en IKEv2. Sin embargo, usted puede todavía utilizar el PSK mientras usted sea consciente de sus limitaciones.

Aquí está un ejemplo de configuración que utiliza **Cisco** como el PSK.

```
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
```

Configuración del hub de FlexVPN

Típicamente, un concentrador termina solamente los túneles dinámicos del spoke a hub. Esta es la razón por la cual usted no encuentra una interfaz del túnel estática para FlexVPN en la Configuración del hub. En lugar, se utiliza una interfaz de plantilla virtual.

> Nota: En el lado del eje de conexión, usted debe indicar a las direcciones del agrupamiento que se asignarán al spokes.

Los direccionamientos de este pool se agregan más adelante en la tabla de ruteo como rutas de **/32** para cada spoke.

```
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
```

Cisco recomienda que usted utiliza AES GCM con el hardware que lo soporta.

```
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
```

Nota: En esta configuración, la operación AES GCM se ha comentado hacia fuera.

```
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
```

Con la autenticación en IKEv2, el mismo principio se aplica en el concentrador como en el spoke. Para el scalability y la flexibilidad, utilice los Certificados. Sin embargo, usted puede reutilizar la misma configuración para el PSK como en el spoke.

Nota: IKEv2 ofrece la flexibilidad en términos de autenticación. Un lado puede autenticar con el PSK mientras que el otro lado utiliza la firma del Rivest-Shamir-Adleman (RSA-SIG).

Si el requisito es utilizar las claves del preshared para la autenticación, después los cambios de configuración son similares a ésos descritos para el router radial aquí.

Conexión BGP del Inter-concentrador

Aseegurese que el Hubs sabe dónde se localizan los prefijos específicos. Esto llega a ser cada vez más importante porque algún spokes fue emigrado a FlexVPN mientras que algún otro spokes permanece en el DMVPN.

Aquí está la conexión BGP del inter-concentrador basada en la Configuración del hub DMVPN:

```
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
```

Migración del tráfico

Emigre al BGP como el [Recommended] del Routing Protocol del recubrimiento

El BGP es un Routing Protocol que se basa en el intercambio del unicast. Debido a sus características, es el mejor protocolo del escalamiento de las redes DMVPN.

En este ejemplo, se utiliza el Internal BGP (iBGP).

Configuración BGP del spoke

La migración del spoke consiste en dos porciones. Primero, permiso BGP como Dynamic Routing:

```
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
```

Después de que suba el vecino BGP (véase la siguiente sección) y los nuevos prefijos sobre el BGP son doctos, usted puede balancear el tráfico de la nube actual DMVPN a una nueva nube de FlexVPN.

Configuración BGP del concentrador

Concentrador de FlexVPN - Configuración BGP completa

En el concentrador, para evitar guardar la configuración de la vecindad para cada habló por separado, configura a los módulos de escucha dinámicos. En esta configuración, el BGP no inicia las nuevas conexiones, sino valida las conexiones del pool proporcionado de los IP Addresses. En este caso, el pool dicho es **10.1.1.0/24**, que es todos los direccionamientos en la nueva nube de FlexVPN.

Dos puntas a observar:

- El concentrador de FlexVPN hace publicidad de los prefijos específicos al concentrador DMVPN; así la correspondencia de los unsupress se está utilizando.

- Haga publicidad de la subred de FlexVPN de **10.1.1.0/24 a la** tabla de ruteo, o aseegurese que el concentrador DMVPN ve el concentrador de FlexVPN como el salto siguiente.

Este documento muestra el último enfoque.

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

Concentrador DMVPN - BGP lleno y configuración EIGRP

La configuración en el concentrador DMVPN es básica, porque recibe solamente los prefijos específicos del concentrador de FlexVPN y hace publicidad de los prefijos que aprende del EIGRP.

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

Emigre el tráfico a BGP/FlexVPN

Según lo discutido antes, usted debe apagar las funciones DMVPN y traer FlexVPN para arriba para realizar la migración.

Este procedimiento garantiza el efecto mínimo:

1. En cada spoke, ingrese por separado esto:

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

En este momento, aseegurese allí no son ninguna sesión IKEv1 establecida a este spoke. Esto puede ser verificada si usted marca la salida de los mensajes de Syslog del **comando show crypto isakmp sa** y del monitor generados por el **comando session crypto del registro**. Una vez que se confirma esto, usted puede proceder a traer para arriba FlexVPN.

2. En el mismo spoke, ingrese esto:

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

Pasos de verificación

Estabilidad del IPSec

La mejor manera de evaluar la estabilidad del IPSec es monitorear los sylogs con el comando enabled **crypto de la configuración de la sesión del registro**. Si usted ve las sesiones que van hacia arriba y hacia abajo, ésta puede indicar un problema en el nivel IKEv2/FlexVPN que debe ser corregido antes de que la migración pueda comenzar.

Información sobre BGP poblada

Si el IPSec es estable, aseegurese que la tabla BGP está poblada con las entradas del spokes (en el concentrador) y el resumen del concentrador (en el spokes). En el caso del BGP, esto se

puede ver con estos comandos:

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

Aquí está un ejemplo de la información correcta del concentrador de FlexVPN:

```
BGP router identifier 172.25.2.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.100 4 65001 112 123 16 0 0 01:35:58 1
192.168.0.1 4 65001 97 99 16 0 0 01:24:12 4
```

La salida muestra que el concentrador ha aprendido un prefijo de cada uno del spokes, y ambo spokes es dinámico y marcado con una muestra del asterisco (*). También muestra que un total de cuatro prefijos de la conexión del inter-concentrador están recibidos.

Aquí está un ejemplo de la información similar del spoke:

```
show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
```

El spoke ha recibido dos prefijos del concentrador. En el caso de esta configuración, un prefijo debe ser el resumen de divulgación en el concentrador de FlexVPN. La otra es red DMVPN 10.0.0.0/24 redistribuida en el spoke DMVPN en el BGP.

Emigre a los nuevos túneles con el EIGRP

El EIGRP es una opción popular en las redes DMVPN debido a su despliegue y convergencia rápida relativamente simples. Sin embargo, escala peor que el BGP, y no ofrece muchos mecanismos avanzados que se puedan utilizar por el cuadro recto de los BGP. La siguiente sección describe una de las maneras de moverse a FlexVPN con un nuevo proceso EIGRP.

Configuración radial actualizada

Un nuevo sistema se agrega con un proceso EIGRP separado:

```
show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
```

Nota: Es el mejor no establecer la adyacencia del Routing Protocol sobre los túneles del spoke al spoke. Por lo tanto, solamente haga la interfaz de **tunnel1** (spoke a hub) no pasiva.

Configuración del hub actualizada de FlexVPN

Semejantemente, para el concentrador de FlexVPN, prepare el Routing Protocol en el appopriate COMO, correspondiendo con uno configurado en el spokes.

```
show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
```

Hay dos métodos que se utilizan para proporcionar la parte posterior del resumen hacia el spoke.

- Redistribuya una Static ruta que señale al **null0** (opción preferida).

  ```
  show ip bgp summary
  BGP router identifier 192.168.101.1, local AS number 65001
  (...omitted...)

  Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
  10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
  ```

  Esta opción permite el control sobre el resumen y la redistribución sin las modificaciones a la configuración de la tecnología de la virtualización del concentrador (VT). Esto es importante, porque la configuración VT del concentrador no puede ser modificada si hay acceso virtual activo asociado a él.

- Configure a una dirección de resumen del DMVPN-estilo en una plantilla virtual.

  Esta configuración *no se recomienda*, debido al procesamiento interno y la replicación del resumen dicho a cada acceso virtual. Se muestra aquí para la referencia.

  ```
  interface Virtual-Template1 type tunnel
   ip summary-address eigrp 200 192.168.0.0 255.255.0.0
  ```

  Otro aspecto a explicar es el intercambio de ruteo del inter-concentrador. Esto puede ser hecha si usted redistribuye los casos del EIGRP al iBGP.

Concentrador DMVPN - Configuración BGP actualizada

La configuración sigue siendo básica. Usted debe redistribuir los prefijos específicos del EIGRP al BGP:

```
interface Virtual-Template1 type tunnel
```

```
 ip summary-address eigrp 200 192.168.0.0 255.255.0.0
```

Concentrador de FlexVPN - Configuración BGP actualizada

Similar al concentrador DMVPN, en FlexVPN, usted debe redistribuir los prefijos de los nuevos procesos EIGRP al BGP:

```
interface Virtual-Template1 type tunnel
 ip summary-address eigrp 200 192.168.0.0 255.255.0.0
```

Emigre el tráfico a FlexVPN

Usted debe apagar las funciones DMVPN y traer FlexVPN para arriba en cada spoke, uno a la vez, para realizar la migración. Este procedimiento garantiza el impacto mínimo:

1. En cada spoke, ingrese por separado esto:
   ```
   interface Virtual-Template1 type tunnel
    ip summary-address eigrp 200 192.168.0.0 255.255.0.0
   ```
   En este momento, aseegurese allí no son ninguna sesión IKEv1 establecida en este spoke. Esto puede ser verificada si usted marca la salida de los mensajes de Syslog del **comando show crypto isakmp sa** y del monitor generados por el **comando session crypto del registro**. Una vez que se confirma esto, usted puede proceder a traer para arriba FlexVPN.
2. En el mismo spoke, ingrese esto:
   ```
   interface Virtual-Template1 type tunnel
    ip summary-address eigrp 200 192.168.0.0 255.255.0.0
   ```

Pasos de verificación

Estabilidad del IPSec

Como en el caso del BGP, usted debe evaluar si el IPSec es estable. La mejor manera de hacer tan es monitorear los sylogs con el comando enabled **crypto de la configuración de la sesión del registro**. Si usted ve las sesiones ir hacia arriba y hacia abajo, esto puede indicar un problema en el nivel IKEv2/FlexVPN que debe ser corregido antes de que la migración pueda comenzar.

Información EIGRP en la tabla de topología

Aseegurese que su tabla de topología EIGRP está poblada con las entradas del spoke LAN en el concentrador y el resumen en el spokes. Esto puede ser verificada si usted ingresa este comando en los concentradores y los spoke:

```
show ip eigrp [AS_NUMBER] topology
```

Aquí está un ejemplo de salida del spoke:

```
Spoke1#show ip eigrp 200 topology
EIGRP-IPv4 Topology Table for AS(200)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 26112000
via Rstatic (26112000/0)
```

```
via 10.1.1.1 (26240000/128256), Tunnel1

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 26114560
via 10.1.1.1 (26114560/2562560), Tunnel1

P 10.1.1.100/32, 1 successors, FD is 26112000
via Connected, Tunnel1

P 10.1.1.0/24, 1 successors, FD is 26114560
via 10.1.1.1 (26114560/2562560), Tunnel1
```

La salida muestra que el spoke sabe sobre su subred LAN (en el *itálico*) y los resúmenes para ésos (en **intrépido**).

Aquí está un ejemplo de salida del concentrador:

```
hub2# show ip eigrp 200 topology
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.2.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 128256
via Connected, Loopback200

P 192.168.101.0/24, 1 successors, FD is 26905600
via 10.1.1.100 (26905600/281600), Virtual-Access1

P 192.168.0.0/16, 1 successors, FD is 2562560
via Rstatic (2562560/0)

P 10.1.1.0/24, 1 successors, FD is 2562560
via Rstatic (2562560/0)
```

La salida muestra que el concentrador sabe sobre las subredes LAN de los rayos (en el *itálico*), el prefijo sumario que hace publicidad (en **intrépido**), y el IP Address asignado de cada rayo vía la negociación.

Consideraciones adicionales

Túneles del spoke al spoke que existen ya

Porque un apagar de la interfaz del túnel DMVPN hace las entradas NHRP ser quitado, los túneles del spoke al spoke que existen ya serán rasgados abajo.

Borre las entradas NHRP

Un concentrador de FlexVPN no confía en el proceso de inscripción NHRP del spoke para saber rutear la parte posterior del tráfico. Sin embargo, los túneles dinámicos del spoke al spoke confían en las entradas NHRP.

En el DMVPN, si el NHRP en el concentrador se borra, puede dar lugar a los problemas de conectividad efímeros. En FlexVPN, el NHRP que borra en el spokes causará el FlexVPN sesión

IPSec, relacionado con los túneles del spoke al spoke, para ser derribado. Borrar el NHRP en el concentrador no tiene ningún efecto sobre la sesión de FlexVPN.

Esto es porque, en FlexVPN por abandono:

- El spokes no se registra al Hubs.
- El Hubs funciona solamente como redirectors NHRP, y no instala las entradas NHRP.
- Las entradas del acceso directo NHRP están instaladas en el spokes para los túneles del spoke al spoke y son dinámicas.

Advertencias conocidas

El tráfico del spoke al spoke se pudo afectar por el Id. de bug Cisco CSCub07382.

Información Relacionada

- DMVPN al ejemplo de configuración suave de la migración de FlexVPN
- Soporte Técnico y Documentación - Cisco Systems