Migración dura de DMVPN a FlexVPN en los mismos dispositivos

Contenido

Introducción

Este documento proporciona información sobre cómo migrar de una red DMVPN existente a FlexVPN en los mismos dispositivos.

Las configuraciones de ambos marcos coexistirán en los dispositivos.

En este documento sólo se muestra el escenario más común: DMVPN con clave previamente compartida para la autenticación y EIGRP como protocolo de ruteo.

Este documento muestra la migración a BGP (protocolo de ruteo recomendado) y EIGRP menos deseable.

Prerequisites

Requirements

Este documento asume que el lector conoce conceptos básicos de DMVPN y FlexVPN.

Componentes Utilizados

Tenga en cuenta que no todo el software y hardware admite IKEv2. Consulte Cisco Feature Navigator para obtener más información. Idealmente, las versiones de software que se utilizarán son:

- ISR - 15.2(4)M1 o posterior
- ASR1k - versión 3.6.2 15.2(2)S2 o posterior

Entre las ventajas de la plataforma y el software más nuevos está la posibilidad de utilizar la criptografía de última generación, por ejemplo, AES GCM para el cifrado en IPsec. Esto se analiza en RFC 4106.

AES GCM permite alcanzar una velocidad de cifrado mucho más rápida en algunos equipos.

Para ver las recomendaciones de Cisco sobre el uso y la migración a la criptografía de última generación, consulte:

http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Procedimiento de migración

Actualmente, la forma recomendada de migrar de DMVPN a FlexVPN es que los dos marcos no funcionen al mismo tiempo.

Esta limitación se eliminará debido a las nuevas funciones de migración que se introducirán en la versión ASR 3.10, supervisadas en varias solicitudes de mejora en el lado de Cisco, incluido CSCuc08066. Esas funciones deberían estar disponibles a finales de junio de 2013.

Una migración en la que ambos marcos de trabajo coexisten y funcionan al mismo tiempo en los mismos dispositivos se denominará migración de software, lo que indica un impacto mínimo y una conmutación por fallas sin problemas de un marco a otro.

Una migración en la que la configuración de ambos marcos coexiste, pero no funciona al mismo tiempo, se denomina migración de hardware. Esto indica que un switchover de un marco a otro significa una falta de comunicación sobre VPN, aunque sea mínima.

Migración dura en los mismos dispositivos

En este documento se analiza la migración de una red DMVPN existente a una nueva red FlexVPN en los mismos dispositivos.

Esta migración requiere que ambos marcos de trabajo no funcionen al mismo tiempo en los dispositivos, lo que requiere esencialmente que la funcionalidad de DMVPN esté desactivada en todos los aspectos antes de habilitar FlexVPN.

Hasta que la nueva función de migración esté disponible, la forma de realizar migraciones con los mismos dispositivos es:

1. Verifique la conectividad a través de DMVPN.
2. Agregue la configuración de FlexVPN y cierre las interfaces de túnel y plantilla virtual que pertenecen a la nueva configuración.
3. (Durante una ventana de mantenimiento) Cierre todas las interfaces de túnel DMVPN en todos los radios y concentradores antes de pasar al paso 4.
4. Desconecte las interfaces de túnel FlexVPN.
5. Verifique la conectividad radial con el hub.
6. Verifique la conectividad spoke a spoke.
7. *Si la verificación de los puntos 5 ó 6 no volvió correctamente a DMVPN cerrando la interfaz FlexVPN y descerrando las interfaces DMVPN.*
8. *Verifique el radio con la comunicación del hub.*
9. *Verifique la comunicación radial.*

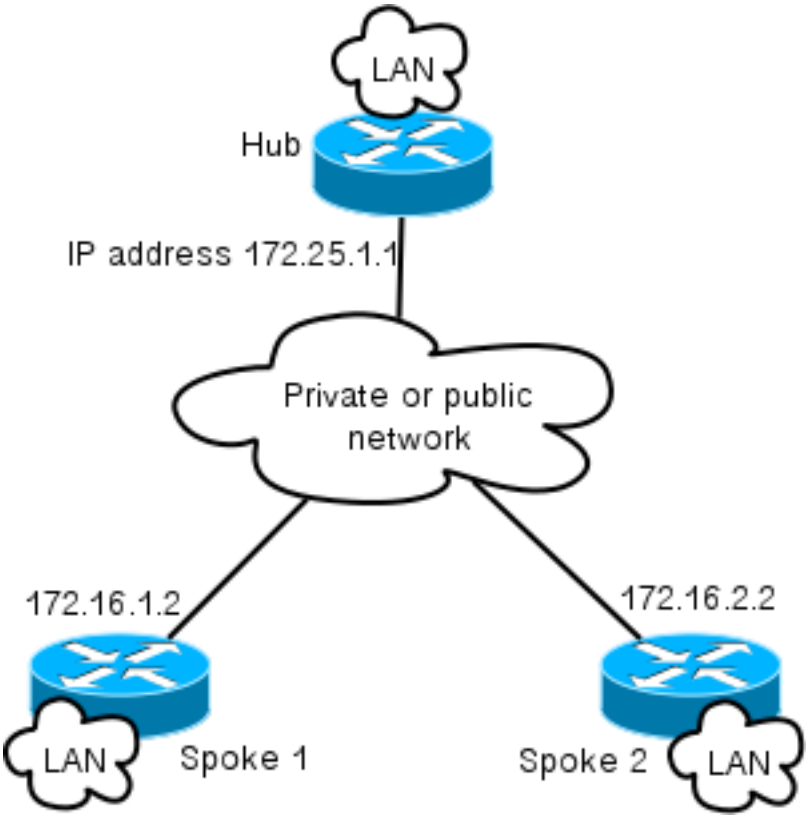
Enfoque personalizado

Si, debido a las complejidades de su red o de routing, es posible que el enfoque no sea la mejor idea para usted, inicie una conversación con su representante de Cisco antes de migrar. La mejor persona para hablar de un proceso de migración personalizado es su ingeniero de sistemas o ingeniero de servicios avanzados.

Topología de red

Topología de red de transporte

Este diagrama muestra una topología de conexiones típica de los hosts en Internet. En este documento, la dirección IP del hub de loopback0 (172.25.1.1) se utiliza para finalizar la sesión IPsec.

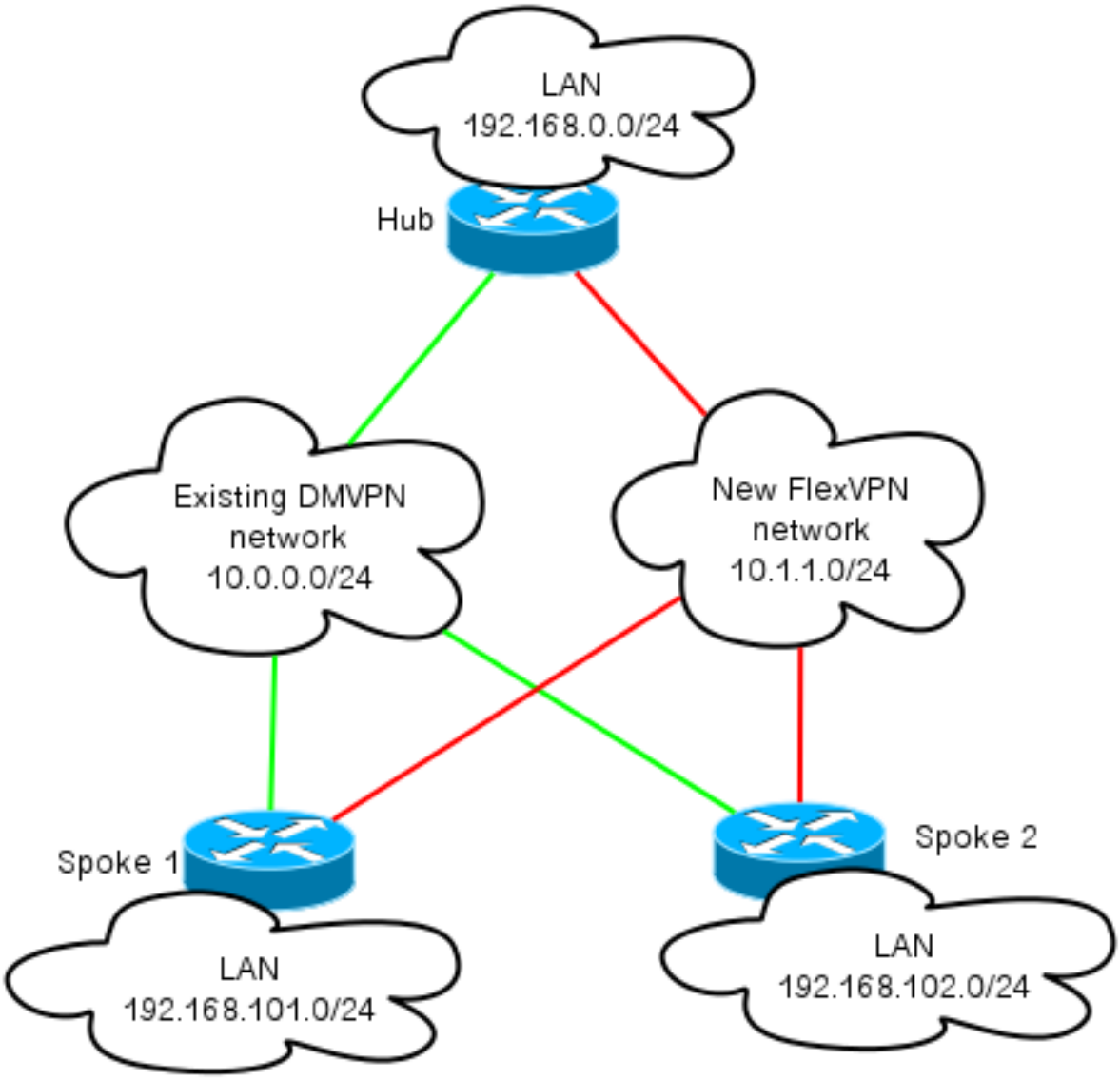


Topología de red superpuesta

Este diagrama de topología muestra dos nubes separadas usadas para superposición: Conexiones DMVPN (conexiones verdes) y FlexVPN.

Los prefijos de red de área local se muestran para los lados correspondientes.

La subred 10.1.1.0/24 no representa una subred real en términos de direccionamiento de la interfaz, sino más bien una parte del espacio IP dedicado a la nube FlexVPN. Más adelante, en la sección Configuración de FlexVPN, se analiza el motivo subyacente.



Configuración

Configuración de DMVPN

Esta sección contiene la configuración básica del hub y spoke de DMVPN.

La clave previamente compartida (PSK) se utiliza para la autenticación IKEv1.

Una vez que se ha establecido IPsec, el registro NHRP se realiza de spoke a hub, de modo que el hub pueda aprender el direccionamiento NBMA de los spokes dinámicamente.

Cuando NHRP realiza el registro en spoke y hub, la adyacencia de ruteo puede establecer y las rutas intercambiadas. En este ejemplo, EIGRP se utiliza como protocolo de ruteo básico para la red superpuesta.

Configuración de DMVPN de radio

Este es un ejemplo básico de configuración de DMVPN con autenticación de clave previamente compartida y EIGRP como protocolo de ruteo.

```
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 de hub DMVPN

En la configuración del hub, el túnel se origina en loopback0 con una dirección IP de 172.25.1.1.

El resto es la implementación estándar del hub DMVPN con EIGRP como protocolo de ruteo.

```
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 FlexVPN

FlexVPN se basa en las mismas tecnologías fundamentales:

- : A diferencia del valor predeterminado en DMVPN, se utiliza IKEv2 en lugar de IKEv1 para negociar SAs IPsec. IKEv2 ofrece mejoras con respecto a IKEv1, empezando por la resistencia y terminando con cuántos mensajes se necesitan para establecer un canal de datos protegido.
- GRE: A diferencia de DMVPN, se utilizan interfaces punto a punto estáticas y dinámicas, y no sólo en interfaces GRE multipunto estáticas. Esta configuración permite mayor flexibilidad, especialmente para el comportamiento por radio/por hub.
- NHRP: En FlexVPN, NHRP se utiliza principalmente para establecer la comunicación spoke a spoke. Los radios no se registran en el hub.
- Ruteo: Debido a que los radios no realizan el registro NHRP al hub, debe confiar en otros mecanismos para asegurarse de que el hub y los radios puedan comunicarse bidireccionalmente. Al igual que DMVPN, se pueden utilizar protocolos de routing dinámicos. Sin embargo, FlexVPN le permite utilizar IPsec para introducir información de ruteo. El valor predeterminado es introducir como ruta /32 para la dirección IP en el otro lado del túnel, lo que permitirá la comunicación directa de spoke a hub.

En la migración dura de DMVPN a FlexVPN, las dos tramas no funcionan al mismo tiempo en los mismos dispositivos. Sin embargo, se recomienda mantenerlos separados.

Separarlos en varios niveles:

- NHRP: utilice un ID de red NHRP diferente (recomendado).
- Routing: utilice procesos de routing independientes (recomendado).
- VRF: la separación VRF puede permitir una mayor flexibilidad, pero no se tratará aquí (opcional).

Configuración de Spoke FlexVPN

Una de las diferencias en la configuración radial en FlexVPN en comparación con DMVPN, es que tiene potencialmente dos interfaces.

Hay un túnel necesario para la comunicación radio a hub y un túnel opcional para los túneles spoke a spoke. Si decide no tener spoke dinámico para tunelización spoke y prefiere que todo pase a través del dispositivo hub, puede quitar la interfaz de plantilla virtual y quitar el switching de acceso directo NHRP de la interfaz de túnel.

También observará que la interfaz de túnel estático tiene una dirección IP recibida en función de la negociación. Esto permite que el hub proporcione IP de la interfaz de túnel para spoke dinámicamente sin necesidad de crear direccionamiento estático en la nube 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
 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
```

Cisco recomienda utilizar AES GCM en hardware que lo admita.

```
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 172.25.1.1
 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
```

PKI es la forma recomendada de realizar una autenticación a gran escala en IKEv2.

Sin embargo, todavía puede utilizar una clave previamente compartida siempre y cuando esté al tanto de sus limitaciones.

A continuación se muestra un ejemplo de configuración que utiliza "cisco" como 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
```

Configuración de FlexVPN Hub

Normalmente, un hub sólo terminará los túneles dinámicos spoke-to-hub. Esta es la razón por la

que en la configuración del hub no encontrará una interfaz de túnel estática para FlexVPN, en su lugar se utiliza una interfaz de plantilla virtual. Esto creará una interfaz de acceso virtual para cada conexión.

Tenga en cuenta que en el lado del eje de conexión debe señalar las direcciones del grupo que se asignarán a los radios.

Las direcciones de este conjunto se agregarán más adelante en la tabla de ruteo como rutas /32 para cada radio.

```
aaa new-model
aaa authorization network default local
aaa session-id common
crypto ikev2 authorization policy default
 pool FlexSpokes
crypto ikev2 profile Flex_IKEv2
 match identity remote fqdn domain 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
```

Cisco recomienda utilizar AES GCM en hardware que lo admita.

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

Tenga en cuenta que en la siguiente configuración se ha comentado la operación de AES GCM.

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
interface Loopback0
 description DMVPN termination
 ip address 172.25.1.1 255.255.255.255
interface Loopback100
 ip address 10.1.1.1 255.255.255.255
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback100
 ip nhrp network-id 2
 ip nhrp redirect
 shutdown
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

Con la autenticación en IKEv2, el mismo principio se aplica en el hub que en el spoke.

Para obtener escalabilidad y flexibilidad, utilice certificados. Sin embargo, puede reutilizar la misma configuración para PSK que en spoke.

Nota: IKEv2 ofrece flexibilidad en términos de autenticación. Un lado puede autenticarse usando PSK mientras que el otro RSA-SIG.

Migración del tráfico

Migración a BGP como protocolo de ruteo superpuesto [recomendado]

BGP es un protocolo de ruteo basado en unicast exchange. Debido a sus características, ha sido el mejor protocolo de ampliación en redes DMVPN.

En este ejemplo, se utiliza iBGP.

Configuración de Spoke BGP

La migración de radio consta de dos partes. Habilitación de BGP como ruteo dinámico.

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

Después de que aparezca el vecino BGP (consulte la configuración de BGP del hub en esta sección de migración) y se detecten nuevos prefijos sobre BGP, puede cambiar el tráfico desde la nube DMVPN existente a la nueva nube FlexVPN.

Configuración de Hub BGP

En el hub para evitar mantener la configuración de vecindad para cada spoke por separado, se configuran receptores dinámicos.

En esta configuración, BGP no iniciará nuevas conexiones, pero aceptará la conexión del conjunto de direcciones IP proporcionado. En este caso, dicho grupo es 10.1.1.0/24, que es todas las direcciones en la nueva nube FlexVPN.

```
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
```

Migración del tráfico a FlexVPN

Como se mencionó anteriormente, la migración debe realizarse mediante el cierre de la funcionalidad de DMVPN y la activación de FlexVPN.

Este procedimiento garantiza un impacto mínimo.

1. En todos los radios:
   ```
   interface tunnel 0
      shut
   ```
2. En Hub:
   ```
   interface tunnel 0
     shut
   ```
   En este momento, asegúrese de que no haya sesiones IKEv1 establecidas a este hub desde los radios.Esto se puede verificar verificando el resultado del comando **show crypto isakmp sa** y monitoreando los mensajes syslog generados por la sesión de registro crypto.Una vez

que se haya confirmado, podrá continuar con la activación de FlexVPN.

3. Continuación en el hub:

```
interface Virtual-template 1
 no shut
```

4. Sobre los radios:

```
interface tunnel 1
   no shut
```

Pasos de verificación

estabilidad IPsec

La mejor manera de evaluar la estabilidad de IPSec es monitoreando sylogs con este comando de configuración habilitado:

```
crypto logging session
```

Si ve que las sesiones sube y baja, esto puede indicar un problema en el nivel IKEv2/FlexVPN que debe corregirse antes de que pueda comenzar la migración.

información de BGP rellenada

Si IPsec es estable, asegúrese de que la tabla BGP se llene con entradas de radios (en el hub) y resumen del hub (en radios).

En el caso de BGP, esto se puede ver realizando lo siguiente:

```
show bgp
! or
show bgp ipv4 unicast
! or
show ip bgp summary
```

Ejemplo de información correcta desde el hub:

```
Hub#show bgp
BGP router identifier 172.25.1.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.101 4 65001 83 82 13 0 0 01:10:46 1
*10.1.1.102 4 65001 7 7 13 0 0 00:00:44 1
```

Puede ver que el hub ha aprendido que 1 prefijo de cada uno de los radios y ambos radios son dinámicos (marcados con un asterisco (*)).

Ejemplo de información similar de spoke:

```
Spoke1#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 11 11 6 0 0 00:03:43 1
```

Spoke ha recibido un prefijo del hub. En caso de esta configuración, este prefijo debe ser el resumen anunciado en el hub.

Migración a nuevos túneles mediante EIGRP

EIGRP es una opción popular en las redes DMVPN debido a su implementación relativamente sencilla y su rápida convergencia.

Sin embargo, se ampliará peor que el BGP y no ofrece muchos de los mecanismos avanzados que el BGP puede utilizar directamente desde el primer momento.

En esta sección se describe una de las formas de pasar a FlexVPN mediante un nuevo proceso EIGRP.

Configuración de spoke actualizada

En este ejemplo, se agrega un nuevo AS con un proceso EIGRP separado.

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
 network 192.168.101.0
 passive-interface default
 no passive-interface Tunnel1
```

Nota: Debe evitar establecer la adyacencia del protocolo de ruteo sobre los túneles spoke a los túneles spoke, por lo tanto, sólo debe hacer que la interfaz del túnel1 (spoke to hub) no sea pasiva.

Configuración del hub actualizada

De forma similar en el hub, DMVPN debe seguir siendo la forma preferida de intercambiar tráfico. Sin embargo, FlexVPN ya debería anunciar y aprender los mismos prefijos.

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
```

Hay dos maneras de proporcionar un resumen hacia el spoke.

- Redistribución de una ruta estática que apunta a null0 (opción preferida).
  ```
  ip route 192.168.0.0 255.255.0.0 null 0
  ip access-list standard EIGRP_SUMMARY
   permit 192.168.0.0 0.0.255.255
  router eigrp 200
   distribute-list EIGRP_SUMMARY out Virtual-Template1
   redistribute static metric 1500 10 10 1 1500
  ```
  Esta opción permite tener control sobre el resumen y la redistribución sin tocar la configuración VT del hub.
- O bien, puede configurar una dirección de resumen de estilo DMVPN en una plantilla virtual. Esta configuración no se recomienda debido al procesamiento interno y la replicación de dicho resumen en cada acceso virtual. Se muestra aquí como referencia:
  ```
  interface Virtual-Template1 type tunnel
  ```

```
ip summary-address eigrp 200 172.16.1.0 255.255.255.0
ip summary-address eigrp 200 192.168.0.0 255.255.0.0
delay 2000
```

Migración del tráfico a FlexVPN

La migración debe realizarse mediante el cierre de la funcionalidad de DMVPN y la activación de FlexVPN.

El siguiente procedimiento garantiza un impacto mínimo.

1. En todos los radios:
   ```
   interface tunnel 0
      shut
   ```
2. En Hub:
   ```
   interface tunnel 0
     shut
   ```
   En este momento, asegúrese de que no haya sesiones IKEv1 establecidas a este hub desde los radios.Esto se puede verificar verificando el resultado del comando **show crypto isakmp sa** y monitoreando los mensajes syslog generados por la sesión de registro crypto.Una vez que se haya confirmado, podrá continuar con la activación de FlexVPN.
3. Continuación en el hub:
   ```
   interface Virtual-template 1
    no shut
   ```
4. En todos los radios:
   ```
   interface tunnel 1
      no shut
   ```

Pasos de verificación

estabilidad IPsec

Como en el caso de BGP, debe evaluar si IPSec es estable. La mejor manera de hacerlo es monitoreando sylogs con este comando de configuración habilitado:

```
crypto logging session
```

Si ve que las sesiones sube y baja, esto puede indicar un problema en el nivel IKEv2/FlexVPN que debe corregirse antes de que pueda comenzar la migración.

información EIGRP en la tabla de topología

Asegúrese de que su tabla de topología EIGRP se rellene con entradas LAN radiales en el hub y resumen en radios. Esto se puede verificar ejecutando este comando en los concentradores y los radios.

```
show ip eigrp topology
```

Ejemplo de salida adecuada de spoke:

```
Spoke1#sh 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
(...omitted as output related to DMVPN cloud ...)
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)


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 (26114560/1709056), Tunnel1


P 10.1.1.107/32, 1 successors, FD is 26112000
 via Connected, Tunnel1
```

Se dará cuenta de que spoke conoce su subred LAN (en cursiva) y los resúmenes para ellos (en **negrita**).

Ejemplo de salida adecuada del hub.

```
Hub#sh ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(172.25.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
(...omitted, related to DMVPN...)
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.1.1)
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, Loopback100


P 192.168.101.0/24, 1 successors, FD is 1561600 via 10.1.1.107 (1561600/281600), Virtual-Access1
P 192.168.0.0/16, 1 successors, FD is 1709056
 via Rstatic (1709056/0)

P 10.1.1.107/32, 1 successors, FD is 1709056
 via Rstatic (1709056/0)


P 10.1.1.106/32, 1 successors, FD is 1709056
 via Rstatic (1709056/0)


P 0.0.0.0/0, 1 successors, FD is 1709056
 via Rstatic (1709056/0)

P 192.168.102.0/24, 1 successors, FD is 1561600 via 10.1.1.106 (1561600/281600), Virtual-Access2
```

Observará que el hub conoce las subredes LAN de los radios (en cursiva), el prefijo de resumen que anuncia (en **negrita**) y la dirección IP asignada de cada radio mediante negociación.

Consideraciones adicionales

Radios existentes a túneles radiales

Debido a que cerrar la interfaz de túnel DMVPN hace que se quiten las entradas NHRP, se desactivarán los túneles de radio a radio existentes.

Eliminación de entradas NHRP

Como se mencionó anteriormente, un hub FlexVPN no se basará en el proceso de registro NHRP de spoke para saber cómo enrutar el tráfico de vuelta. Sin embargo, los túneles spoke dinámicos dependen de las entradas NHRP.

En DMVPN, donde la compensación de NHRP en el hub podría haber generado problemas de conectividad de corta duración.

En FlexVPN, la eliminación de NHRP en radios hará que la sesión IPsec de FlexVPN, relacionada con los túneles radiales, se deslice. Al borrar NHRP, ningún hub tendrá efecto en la sesión FlexVPN.

Esto se debe al hecho de que en FlexVPN, de forma predeterminada:

- Los radios no se registran en los concentradores.
- Los hubs funcionan solamente como redirector NHRP y no instalan las entradas NHRP.
- Las entradas de acceso directo NHRP se instalan en radios para los túneles de radio a radio y son dinámicas.

Advertencias conocidas

El tráfico de radio a radio puede verse afectado por CSCub07382.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems