Migración dura de DMVPN a FlexVPN en un hub diferente

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Procedimiento de migración
Migración difícil entre dos centros diferentes
Enfoque personalizado
Topología de red
Topología de red de transporte
Topología de red superpuesta
Configuración
Configuración de DMVPN
Configuración de DMVPN de Spoke
Configuración de hub DMVPN
Configuración de FlexVPN
Configuración de Spoke FlexVPN
Configuración de FlexVPN Hub
Migración del tráfico
Migrar a BGP como Overlay Routing Protocol [recomendado]
Configuración de BGP de Spoke
Configuración de Hub BGP
Migrar el tráfico a BGP/FlexVPN
Migración a Nuevos Túneles con EIGRP
Configuración de Spoke actualizada
Configuración actualizada de FlexVPN Hub
hub DMVPN: configuración de BGP actualizada
FlexVPN Hub: configuración de BGP actualizada
Migración del tráfico a FlexVPN
Pasos de verificación
Consideraciones adicionales
Túneles de radio a radio que ya existen
Borrar entradas NHRP
Advertencias conocidas
Información Relacionada

Introducción

Este documento proporciona información sobre cómo migrar desde una red de VPN multipunto dinámica (DMVPN) que actualmente existe a FlexVPN en diferentes dispositivos hub. Las configuraciones para ambos marcos coexisten en los dispositivos. En este documento, sólo se muestra el escenario más común: DMVPN con el uso de la clave precompartida para la autenticación y el protocolo de routing de gateway interior mejorado (EIGRP) como protocolo de routing. En este documento, se muestra la migración al protocolo de gateway fronterizo (BGP), que es el protocolo de routing recomendado, y el EIGRP menos deseable.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre estos temas:

- DMVPN
- FlexVPN

Componentes Utilizados

> **Nota:** No todo el software y el hardware admite el intercambio de claves de Internet versión 2 (IKEv2). Refiérase a Cisco Feature Navigator para obtener más información.

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

- Router de servicios integrados (ISR) de Cisco versión 15.2(4)M1 o posterior
- Cisco Aggregation Services Router serie 1000 (ASR1K) 3.6.2 Versión 15.2(2)S2 o posterior

Una de las ventajas de una plataforma y un software más nuevos es la capacidad de utilizar la criptografía de última generación, como Galois/Modo de contador (GCM) estándar de cifrado avanzado (AES) para el cifrado en seguridad de protocolo de Internet (IPsec), como se explica en la solicitud de comentarios (RFC) 4106. AES GCM le 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, refiérase al artículo Encriptación de última generación.

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.

Procedimiento de migración

Actualmente, el método recomendado para migrar de DMVPN a FlexVPN es que los dos marcos de trabajo no funcionen al mismo tiempo. Esta limitación está programada para eliminarse debido

a las nuevas funciones de migración que se introducirán en la versión ASR 3.10, que se siguen en múltiples solicitudes de mejora en el lado de Cisco, que incluyen el Id. de bug de Cisco CSCuc08066. Esas funciones deberían estar disponibles a finales de junio de 2013.

Una migración en la que ambos marcos coexisten y funcionan al mismo tiempo en los mismos dispositivos se denomina **migración de software**, que indica el impacto mínimo y la conmutación por fallas sin problemas de un marco a otro. Una migración en la que las configuraciones para ambos marcos coexisten, pero no funcionan al mismo tiempo, se denomina **migración dura**. Esto indica que un switchover de un marco a otro significa una falta de comunicación sobre la VPN, aunque sea mínima.

Migración difícil entre dos centros diferentes

En este documento, se analiza la migración desde el hub DMVPN que se utiliza actualmente a un nuevo hub FlexVPN. Esta migración permite la intercomunicación entre radios migradas ya a FlexVPN y aquellas que aún se ejecutan en DMVPN y se pueden realizar en varias fases, en cada radio por separado.

Siempre que la información de ruteo se rellene correctamente, la comunicación entre los radios migrados y no migrados debe seguir siendo posible. Sin embargo, se puede observar una latencia adicional porque los radios migrados y no migrados no crean túneles de radio a radio entre sí. Al mismo tiempo, los radios migrados deben poder establecer túneles directos de radio a radio entre ellos. Lo mismo se aplica a los spokes no migrados.

Hasta que esta nueva función de migración esté disponible, complete estos pasos para realizar migraciones con un hub diferente de DMVPN y FlexVPN:

1. Verifique la conectividad a través de DMVPN.
2. Agregue la configuración FlexVPN y cierre el túnel que pertenece a la nueva configuración.
3. (Durante una ventana de mantenimiento) En cada radio, uno por uno, cierre el túnel DMVPN.
4. En el mismo spoke que en el Paso 3, descierre las interfaces de túnel FlexVPN.
5. Verifique la conectividad de spoke a hub.
6. Verifique la conectividad de radio a radio dentro de FlexVPN.
7. Verifique la conectividad de radio a radio con DMVPN desde FlexVPN.
8. Repita los pasos 3 a 7 para cada radio por separado.
9. Si encuentra algún problema con las verificaciones descritas en los pasos 5, 6 o 7, cierre la interfaz FlexVPN y descierre las interfaces DMVPN para volver a DMVPN.
10. Verifique la comunicación de spoke a hub a través de la DMVPN de respaldo.
11. Verifique la comunicación de radio a radio a través de la DMVPN de respaldo.

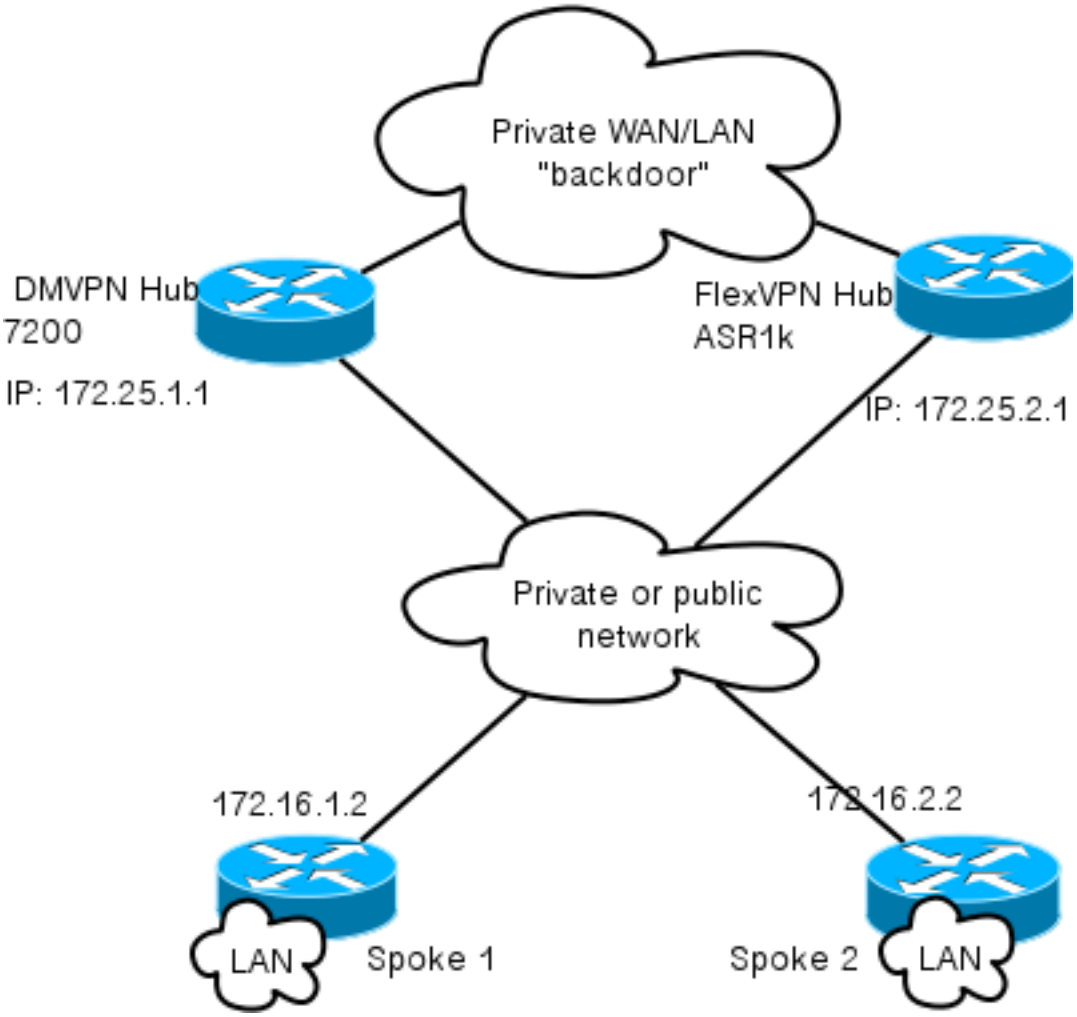
Enfoque personalizado

Si el enfoque anterior puede no ser la mejor solución para usted debido a las complejidades de su red o de routing, inicie una conversación con su representante de Cisco antes de realizar la migración. La mejor persona con la que debe 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

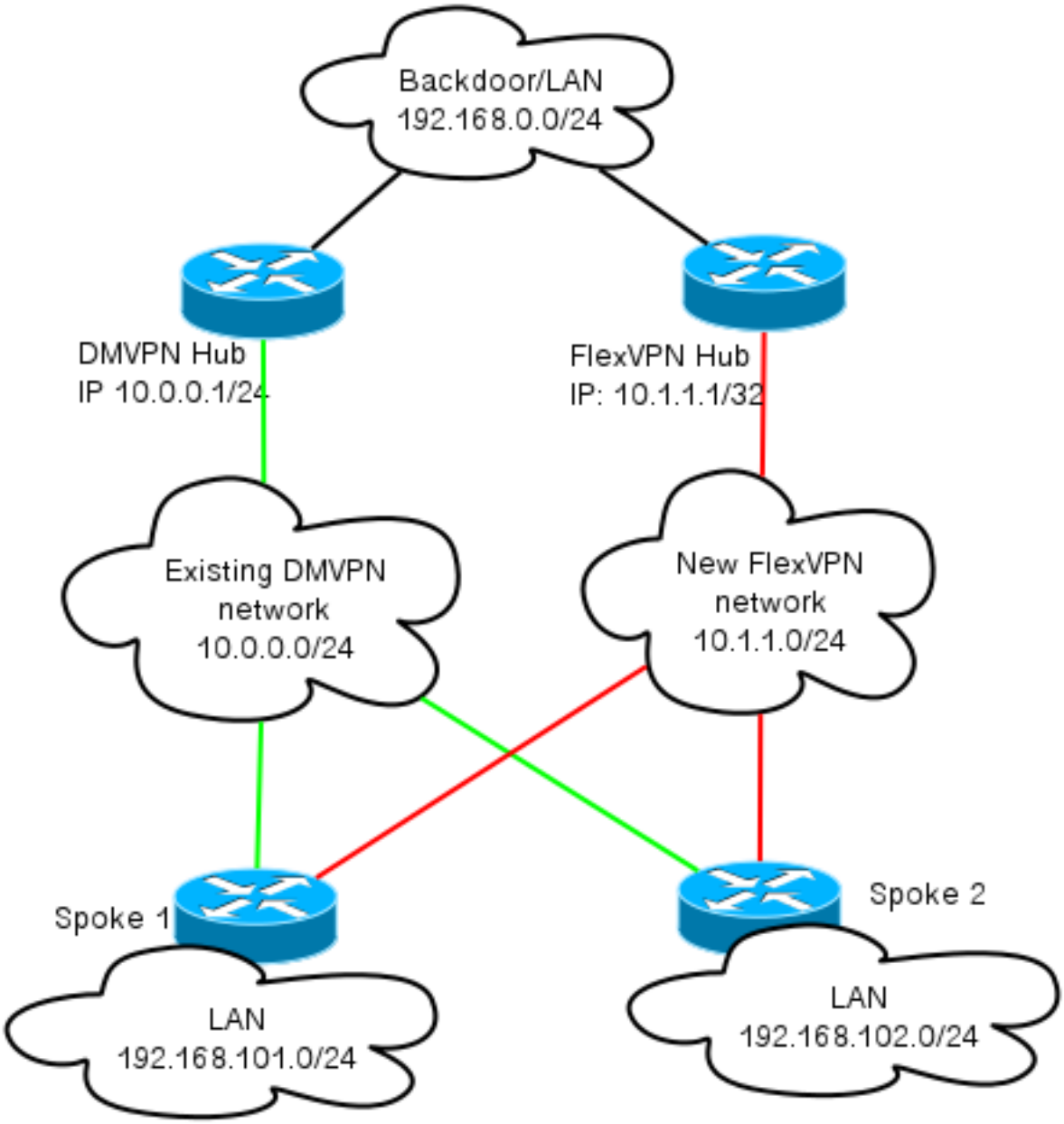
Este diagrama muestra la topología de conexión típica de los hosts en Internet. La dirección IP del hub del **loopback0** (**172.25.1.1**) se utiliza para finalizar la sesión IPSec de DMVPN. La dirección IP del nuevo hub (**172.25.2.1**) se utiliza para FlexVPN.



Observe el link entre los dos ejes de conexión. Este enlace es crucial para permitir la conectividad entre las nubes FlexVPN y DMVPN durante la migración. Permite que los radios que ya se han migrado a FlexVPN se comuniquen con las redes DMVPN y viceversa.

Topología de red superpuesta

Este diagrama de topología muestra dos nubes separadas usadas para superposición: 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 direccionamiento de interfaz, sino que representa una parte del espacio IP dedicado a la nube FlexVPN. La justificación de esto se analiza más adelante en la sección **Configuración de FlexVPN**.



Configuración

En esta sección se describen las configuraciones de DMVPN y FlexVPN.

Configuración de DMVPN

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

La clave precompartida (PSK) se utiliza para la autenticación IKEv1. Una vez establecido el IPSec, se realiza el registro del protocolo de resolución de salto siguiente (NHRP) de spoke a hub para que el hub pueda aprender dinámicamente el direccionamiento de acceso múltiple sin difusión (NBMA) de los radios.

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

Configuración de DMVPN de Spoke

Aquí puede encontrar un ejemplo básico de configuración de DMVPN con autenticación PSK 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 una implementación estándar de un 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 de 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 las asociaciones de seguridad IPsec (SA). IKEv2 ofrece mejoras con respecto a IKEv1, como la resistencia y el número de mensajes necesarios para establecer un canal de datos protegido.

- **GRE:** A diferencia de DMVPN, se utilizan interfaces punto a punto estáticas y dinámicas, y no sólo una interfaz estática multipunto GRE. Esta configuración permite mayor flexibilidad, especialmente para el comportamiento por radio/por hub.

- **NHRP**: En FlexVPN, NHRP se utiliza principalmente para establecer la comunicación de radio a radio. Los radios no se registran en el hub.

- **Ruteo:** Debido a que los radios no realizan el registro NHRP en el 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 la ruta **as/32** para la dirección IP en el otro lado del túnel, que permite la comunicación directa de spoke a hub.

En una 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).

- Virtual Routing and Forwarding (VRF): la separación de VRF permite una mayor flexibilidad, pero no se analiza aquí (opcional).

Configuración de Spoke FlexVPN

Una de las diferencias en la configuración radial en FlexVPN en comparación con DMVPN es que potencialmente tiene dos interfaces. Hay un túnel necesario para la comunicación de radio a hub y un túnel opcional para los túneles de radio a radio. Si decide no tener tunelización dinámica de spoke a spoke y prefiere que todo pase a través del dispositivo hub, puede quitar la interfaz de plantilla virtual y quitar el acceso directo de NHRP de la interfaz de túnel.

Observe que la interfaz de túnel estático recibe una dirección IP basada en la negociación. Esto permite que el hub proporcione dinámicamente la dirección IP de la interfaz de túnel al spoke 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
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:** De forma predeterminada, la identidad local se establece para utilizar la dirección IP. Por lo tanto, la sentencia de coincidencia correspondiente en el par debe coincidir también en función de la dirección. Si el requisito es coincidir según el nombre distinguido (DN) del certificado, la coincidencia debe hacerse con el uso de un mapa de certificado.

Cisco recomienda utilizar AES GCM con 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 172.25.2.1
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
```

Public Key Infrastructure (PKI) es el método recomendado para realizar la autenticación a gran escala en IKEv2. Sin embargo, puede seguir utilizando PSK siempre y cuando sea consciente 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
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

Configuración de FlexVPN Hub

Normalmente, un hub solo termina los túneles dinámicos spoke-to-hub. Esta es la razón por la que no encuentra una interfaz de túnel estática para FlexVPN en la configuración del hub. En su lugar, se utiliza una interfaz de plantilla virtual.

> **Nota:** En el lado del hub, debe indicar las direcciones del conjunto que se asignarán a los radios.

Las direcciones de este conjunto se agregan más adelante en la tabla de ruteo como **/32** rutas 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
local identity fqdn hub.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 con hardware que lo admita.

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

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

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

interface Loopback0
description DMVPN termination
ip address 172.25.2.1 255.255.255.255
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
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 el spoke.

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

Si el requisito es utilizar claves previamente compartidas para la autenticación, los cambios de configuración son similares a los descritos para el router spoke aquí.

Conexión BGP entre concentradores

Asegúrese de que los concentradores sepan dónde se encuentran los prefijos específicos. Esto cobra cada vez más importancia porque algunos radios se migraron a FlexVPN mientras que otros radios permanecen en DMVPN.

Esta es la conexión BGP entre concentradores basada en la configuración del hub DMVPN:

```
router bgp 65001
network 192.168.0.0
neighbor 192.168.0.2 remote-as 65001
```

Migración del tráfico

Migrar a BGP como Overlay Routing Protocol [recomendado]

BGP es un protocolo de ruteo que se basa en unicast exchange. Debido a sus características, es el mejor protocolo de ampliación en redes DMVPN.

En este ejemplo, se utiliza BGP interno (iBGP).

Configuración de BGP de Spoke

La migración de radio consta de dos partes. Primero, habilite 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 se active el vecino BGP (consulte la siguiente sección) y se detecten nuevos prefijos sobre BGP, puede cambiar el tráfico desde la nube DMVPN actual a una nueva nube FlexVPN.

Configuración de Hub BGP

Concentrador FlexVPN - Configuración BGP completa

En el hub, para evitar mantener la configuración de vecindad para cada spoke por separado, configure los receptores dinámicos. En esta configuración, BGP no inicia nuevas conexiones, pero acepta conexiones del conjunto de direcciones IP proporcionado. En este caso, el conjunto mencionado es 10.1.1.0/24, que es todas las direcciones en la nueva nube FlexVPN.

Dos puntos a destacar:

- El hub FlexVPN anuncia prefijos específicos al hub DMVPN; por lo tanto, se está utilizando el mapa unsupress.
- Anuncie la subred FlexVPN de 10.1.1.0/24 a la tabla de ruteo o asegúrese de que el hub DMVPN vea el hub FlexVPN como el salto siguiente.

Este documento muestra este 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
```

hub DMVPN - Configuración completa de BGP y EIGRP

La configuración en el hub DMVPN es básica, ya que solo recibe prefijos específicos del hub FlexVPN y anuncia los prefijos que aprende de EIGRP.

```
router bgp 65001
bgp log-neighbor-changes
redistribute eigrp 100
neighbor 192.168.0.2 remote-as 65001
```

Migrar el tráfico a BGP/FlexVPN

Como se ha mencionado anteriormente, debe cerrar la funcionalidad de DMVPN y activar FlexVPN para realizar la migración.

Este procedimiento garantiza un impacto mínimo:

1. En cada radio, por separado, introduzca lo siguiente:

   ```
   interface tunnel 0
    shut
   ```

   En este momento, asegúrese de que no haya sesiones IKEv1 establecidas para este spoke. Esto se puede verificar si verifica el resultado del comando **show crypto isakmp sa** y monitorea los mensajes syslog generados por el comando **crypto logging session**. Una vez que se confirme esto, puede continuar con el uso de FlexVPN.

2. En el mismo spoke, introduzca lo siguiente:

   ```
   interface tunnel 1
     no shut
   ```

Pasos de verificación

Estabilidad IPsec

La mejor manera de evaluar la estabilidad de IPSec es monitorear sylogs con el comando de configuración **crypto logging session** habilitado. Si ve sesiones que suben y bajan, esto puede indicar un problema en el nivel IKEv2/FlexVPN que se debe corregir 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 los radios (en el hub) y un resumen del hub (en los radios). En el caso de BGP, esto se puede ver con estos comandos:

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

Este es un ejemplo de información correcta del hub 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
```

El resultado muestra que el hub ha aprendido un prefijo de cada uno de los radios, y ambos radios son dinámicos y están marcados con un signo de asterisco (*). También muestra que se recibe un total de cuatro prefijos de la conexión inter-hub.

Aquí hay un ejemplo de información similar de 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 hub. En el caso de esta configuración, un prefijo debe ser el resumen anunciado en el hub FlexVPN. La otra es la red **10.0.0.0/24** DMVPN redistribuida en el radio DMVPN en BGP.

Migración a Nuevos Túneles con EIGRP

EIGRP es una opción popular en las redes DMVPN debido a su implementación relativamente sencilla y su rápida convergencia. Sin embargo, se escala peor que el BGP y no ofrece muchos mecanismos avanzados que el BGP pueda utilizar directamente desde el primer momento. En la siguiente sección se describe una de las formas de pasar a FlexVPN con un nuevo proceso EIGRP.

Configuración de Spoke actualizada

Se agrega un nuevo sistema autónomo (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:** Es mejor no establecer la adyacencia del protocolo de ruteo sobre los túneles de spoke a spoke. Por lo tanto, haga que la interfaz de **tunnel1** (spoke-to-hub) no sea pasiva.

Configuración actualizada de FlexVPN Hub

Del mismo modo, para el hub FlexVPN, prepare el protocolo de ruteo en el AS apropiado, que coincida con uno configurado en los radios.

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

Hay dos métodos que se utilizan para 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 route 10.1.1.0 255.255.255.0 null 0

  ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
  ip prefix-list EIGRP_SUMMARY_ONLY seq 10 permit 10.1.1.0/24

  route-map EIGRP_SUMMARY permit 20
  match ip address prefix-list EIGRP_SUMMARY_ONLY

  router eigrp 200
  distribute-list route-map EIGRP_SUMMARY out Virtual-Template1
  redistribute static metric 1500 10 10 1 1500 route-map EIGRP_SUMMARY
  ```

  Esta opción permite controlar el resumen y la redistribución sin modificar la configuración de la tecnología de virtualización (VT) del hub. Esto es importante, porque la configuración VT del hub no se puede modificar si hay acceso virtual activo asociado a él.

- Configure 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 200 192.168.0.0 255.255.0.0
  ```

  Otro aspecto que se debe tener en cuenta es el intercambio de ruteo entre concentradores. Esto se puede hacer si se redistribuyen las instancias de EIGRP a iBGP.

hub DMVPN: configuración de BGP actualizada

La configuración sigue siendo básica. Debe redistribuir prefijos específicos de EIGRP a BGP:

```
router bgp 65001

redistribute eigrp 100
```

```
neighbor 192.168.0.2 remote-as 65001
```

FlexVPN Hub: configuración de BGP actualizada

Al igual que el hub DMVPN, en FlexVPN, debe redistribuir los prefijos del nuevo proceso EIGRP a BGP:

```
router bgp 65001

 redistribute eigrp 200 redistribute static

 neighbor 192.168.0.1 remote-as 65001
```

Migración del tráfico a FlexVPN

Debe apagar la funcionalidad de DMVPN y activar FlexVPN en cada radio, de uno en uno, para realizar la migración. Este procedimiento garantiza un impacto mínimo:

1. En cada radio, por separado, introduzca lo siguiente:

   ```
   interface tunnel 0
    shut
   ```

   En este momento, asegúrese de que no se hayan establecido sesiones IKEv1 en este spoke. Esto se puede verificar si verifica el resultado del comando **show crypto isakmp sa** y monitorea los mensajes syslog generados por el comando **crypto logging session**. Una vez que se confirme esto, puede continuar con el uso de FlexVPN.
2. En el mismo spoke, introduzca lo siguiente:

   ```
   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 monitorear los sylogs con el comando de configuración **crypto logging session** habilitado. Si ve que las sesiones se activan y desactivan, esto puede indicar un problema en el nivel IKEv2/FlexVPN que se debe corregir antes de que pueda comenzar la migración.

Información de EIGRP en la Tabla de Topología

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

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

A continuación se muestra 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
```

El resultado muestra que el spoke conoce su subred LAN (en *cursiva*) y los resúmenes para ellos (en **negrita**).

Este es un ejemplo de salida del hub:

```
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)
```

El resultado muestra 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

Túneles de radio a radio que ya existen

Debido a que un cierre de la interfaz de túnel DMVPN hace que se eliminen las entradas NHRP, se desactivarán los túneles de radio a radio que ya existen.

Borrar entradas NHRP

Un hub FlexVPN no confía en el proceso de registro NHRP desde el spoke para saber cómo enrutar el tráfico de vuelta. Sin embargo, los túneles dinámicos de radio a radio dependen de las entradas NHRP.

En DMVPN, si se borra NHRP en el hub, puede dar lugar a problemas de conectividad de corta duración. En FlexVPN, la eliminación de NHRP en los radios hará que la sesión IPsec de FlexVPN, relacionada con los túneles de radio a radio, se desactive. La limpieza de NHRP en el hub no tiene ningún efecto en la sesión FlexVPN.

Esto se debe a que, en FlexVPN de forma predeterminada:

- Los radios no se registran en los concentradores.
- Los hubs funcionan solamente como redirectores NHRP y no instalan 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 el Id. de bug Cisco CSCub07382 .

Información Relacionada

- Ejemplo de Configuración de la Migración de Soft DMVPN a FlexVPN
- Soporte Técnico y Documentación - Cisco Systems