VPN IPSec de multipunto dinámico (Uso de NHRP/GRE multipunto para escalar a VPN IPSec)

Contenido

Introducción

Este documento explica el Ipsec VPN de multipunto dinámico (DMVPN) y porqué una compañía podría querer diseñar o migrar su red para usar esta nueva solución de IPsec VPN en Cisco IOS® Software.

Antecedentes

Es posible que las empresas necesiten interconectar muchos sitios a un sitio principal y quizá también entre sí a través de Internet, a la vez que cifran el tráfico para protegerlo. Por ejemplo, es probable que un grupo de tiendas minoristas que necesitan conectarse con la oficina central de la compañía por cuestiones de inventario y órdenes, también necesite conectarse con otras tiendas de la compañía para verificar la disponibilidad de los productos. En el pasado, la única forma de efectuar la conexión fue mediante una red de capa 2, como por ejemplo: ISDN o Fram Relay para interconectar todo. Configurar y pagar por estos links de cableado directo de tráfico IP interno puede ser lento y costoso. Si todos los sitios (incluso el sitio principal) ya cuentan con acceso a Internet relativamente económico, este acceso puede usarse asimismo para la comunicación interna por IP entre las tiendas y oficinas principales a través de túneles IPsec con el objeto de asegurar la privacidad y la integridad de los datos.

A fin de que las compañías creen extensas redes IPsec que interconecten sus sitios por Internet, debe ser posible ampliar la red IPsec. IPsec encripta el tráfico entre dos puntos finales (pares) y los dos puntos finales realizan el encripción utilizando un “secreto” compartido. Como el secreto es compartido sólo entre estos dos puntos finales, las redes cifradas son intrínsecamente una colección de links punto a punto. Debido a esto, esencialmente, IPsec es una red de túneles punto a punto. El método más factible para escalar una gran red punto a punto es organizarla dentro de una red hub y spoke o de una red de interconexión completa (parcial). En casi todas las redes, la mayoría del tráfico IP se realiza entre los spokes y el hub y sólo una pequeña parte entre los spokes, por lo que el diseño hub y spoke es a menudo la mejor opción. Este diseño también es compatible con las anteriores redes Frame Relay ya que era extremadamente costoso pagar por los links entre todos los sitios en estas redes.

Al usar Internet como la interconexión entre el concentrador y el spokes, el spokes también tiene acceso directo el uno al otro sin el coste adicional, pero ha sido muy difícil, si no imposible, configurar y/o manejar una red de interconexión (parcial) completa. A veces se prefieren las redes de interconexión completas o parciales ya que puede haber un ahorro de costos si el tráfico de radio a radio se transmite de manera directa en lugar de a través del concentrador. El tráfico del spoke al spoke que atraviesa a los recursos del concentrador de las aplicaciones del concentrador y puede incurrir en los retardos adicionales, especialmente al usar la encripción de IPSec, puesto que el concentrador necesitará desencriptar los paquetes entrantes del spokes de envío y después encriptar nuevamente el tráfico para enviarlo al spoke de recepción. Otro ejemplo en el que el tráfico directo de radio a radio podría resultar útil es el caso en el que dos radios están en la misma ciudad y el eje de conexión se encuentra en otra parte del país.

Mientras que las redes radiales del IPSec fueron desplegadas y crecieron de tamaño, llegó a ser más deseable hacer que ruteen los paquetes del IP tan dinámicamente como sea posible. En las más viejas redes radiales del Frame Relay esto fue lograda ejecutando un Dynamic Routing Protocol como el OSPF o el EIGRP sobre los links de Frame Relay. Esto fue útil para anunciar de forma dinámica el alcance de las redes spoke y también para admitir la redundancia en la red de IP Routing. Si la red perdió un router hub, puede tomar el mando un router hub de respaldo en forma automática para retener la conectividad de la red con redes spoke.

Hay un problema fundamental con los túneles IPsec y los Dynamic Routing Protocol. Los Dynamic Routing Protocol confían en usar el Multicast IP o los paquetes de broadcast, pero el IPSec no soporta el Multicast que cifra o los paquetes de broadcast. El método actual para la resolución de este problema es usar los túneles de encapsulación de ruteo genérica (GRE) junto con el encripción IPSec.

Los túneles GRE soportan el transporte del Multicast IP y de los paquetes de broadcast al otro extremo del túnel GRE. El paquete de túnel GRE es un paquete de unidifusión IP, de manera que el paquete GRE puede ser encripción mediante IPsec. En esta situación, GRE realiza el trabajo de tunelización e IPsec realiza la parte de encripción del soporte para la red VPN. Cuando se configuran los túneles GRE, los IP Addresses para los puntos finales del túnel (**origen de túnel…**, el **destino del túnel…**) se debe saber por el otro punto final y debe ser el routable sobre Internet. Esto significa que el concentrador y todos los routeres radiales en esta red deben tener IP Addresses estáticos del NON-soldado.

Para las pequeñas conexiones del sitio a Internet, es típico para que el IP Address externo de un rayo cambie cada vez que conecta con Internet porque su Proveedor de servicios de Internet (ISP) proporciona dinámicamente a la dirección de interfaz externa (vía el Protocolo de configuración dinámica de host (DHCP)) cada vez que el spoke viene en la línea (Asymmetric Digital Subscriber Line (ADSL) y los servicios de cable). Esta asignación dinámica de la “dirección externa” del router permite que el ISP suscriba excesivamente el uso de sus espacios de dirección de Internet, ya que no todos los usuarios se conectarán al mismo tiempo. Puede ser mucho más caro abonarle al proveedor para que le asigne una dirección estática al router spoke. La ejecución de un protocolo de ruteo dinámico sobre una VPN IPsec exige el uso de túneles GRE, pero se pierde la opción de tener radios con direcciones de IP asignadas dinámicamente en las interfaces físicas exteriores.

Las restricciones antedichas y algunos otras se resumen en las cuatro puntas siguientes:

- El IPSec utiliza un Access Control List (ACL) para definir qué datos deben ser cifrados. Por esto, cada vez que se agrega una nueva (sub)red detrás del router radial o el concentrador, el cliente debe cambiar la ACL en los routers radiales o el concentrador. Si el SP administra el router, el cliente debe notificar al SP a fin de obtener el cambio de la ACL IPsec para que el nuevo tráfico sea encripción.
- Con las redes radiales grandes, el tamaño de la configuración en el router de eje de conexión puede llegar a ser muy grande, hasta el punto de esté inutilizable. Por ejemplo, un router de eje de conexión necesitaría hasta 3900 líneas de configuración para soportar 300 routers de radio. Esto es lo suficientemente grande como para que resulte difícil mostrar la configuración y encontrar la sección de la configuración que es pertinente al problema actual que se trata de depurar. Además, esta configuración de tamaño podría ser demasiado extensa para adaptarse a la NVRAM y necesitaría ser almacenada en la memoria flash.
- GRE + IPsec debe conocer la dirección del par de punto final. Las direcciones IP de los radios se conectan directamente a Internet a través de su propio ISP y, con frecuencia, están configuradas de manera que sus direcciones de interfaces externas no sean fijas. Las direcciones IP pueden cambiar cada vez que el sitio se conecta (a través de DHCP).
- Si la necesidad del spokes de hablar directamente con uno a sobre el IPSec VPN, entonces la red radial debe convertirse en una interconexión total. Puesto que no se sabe ya qué spokes necesitará hablar directamente con uno a, se requiere una interconexión total, aunque cada spoke puede no necesitar hablar directamente con cada otro spoke. También, no es posible configurar el IPSec en un pequeño router radial de modo que tenga conectividad directa con el resto de los routeres radiales en la red; así los routeres radiales pueden necesitar ser más routeres potentes.

La solución para DMVPN

La solución DMVPN utiliza Multipunto GRE (mGRE) y Protocolo de resolución de salto siguiente (NHRP), junto con IPsec y otras mejoras nuevas, para resolver gradualmente los problemas mencionados con anterioridad.

Iniciación automática de encripción de IPsec

Cuando no usando la solución DMVPN, el túnel de encripción IPSec no se inicia hasta que haya el tráfico de datos que requiere el uso de este túnel IPsec. Puede tardar 1 a 10 segundos para completar el lanzamiento del túnel IPsec y el tráfico de datos se cae durante este tiempo. Al usar el GRE con el IPSec, la configuración del túnel GRE incluye ya al par del túnel GRE (el **destino del túnel…**) direccionamiento, que también es el direccionamiento del peer IPSec. Ambas direcciones están preconfiguradas.

Si usted utiliza el Tunnel Endpoint Discovery (TED) y las correspondencias cifradas dinámicas en el router de eje de conexión, después usted puede evitar tener que preconfigurar los direccionamientos del peer IPSec en el concentrador, pero una sonda y una respuesta de TED necesita ser enviada y ser recibida antes de que la negociación ISAKMP pueda comenzar. Esto no debería ser necesario, ya que al usar GRE las direcciones de los pares de origen y destino se conocen de antemano. Están ya sea en la configuración o resueltos con NHRP (para túneles multipunto GRE).

Con la solución DMVPN, el IPSec se acciona inmediatamente para los túneles GRE de punto a punto y de múltiples puntos. Además, no es necesario configurar ninguna ACL de encripción ya que éstas surgirán automáticamente a partir de las direcciones de origen y destino del túnel GRE. Los siguientes comandos se utilizan para definir los parámetros de encripción de IPsec. Observe que no se requieren comandos set peer... ni match address... ya que esta dirección se deriva directamente del túnel GRE asociado o correspondencias NHRP.

```
crypto ipsec profile <profile-name> set transform-set <transform-name>
```

El siguiente comando asocia una interfaz del túnel con el perfil de ipsec.

```
interface tunnel<number> ... tunnel protection ipsec profile <profile-name>
```

Creación del túnel dinámico para los links del “spoke a hub”

No se configura ningún GRE o información de IPSec sobre un spoke en el router de eje de conexión en la red DMVPN. El túnel GRE del router radial se configura (vía los comandos NHRP) con la información sobre el router de eje de conexión. Cuando se inicia el router radial, éste inicia el túnel IPSec con el router de eje de conexión de manera automática como se describió anteriormente. Luego utiliza NHRP para informar al concentrador del router de cada dirección IP física actual. Esto es útil por tres motivos:

- Si la dirección IP de la interfaz física del router spoke se asignó en forma dinámica (como sucede, por ejemplo, con ADSL o cablemódem), el router hub no puede configurarse con esta información ya que cada vez que el router spoke se recargue obtendrá una nueva dirección IP de la interfaz física.
- Se acorta y simplifica la configuración del router hub ya que no necesita ninguna información GRE o IPSec acerca de los routers de par. Toda esta información se aprende dinámicamente vía el NHRP.
- Cuando agrega un nuevo router radial a la red DMVPN, no necesita cambiar la configuración

en el eje de conexión ni en los routers radiales actuales. Configuran al nuevo router radial con información del hub, y cuando empieza para arriba, se registra dinámicamente con el router de eje de conexión. El Dynamic Routing Protocol propaga la información de ruteo para este habló al concentrador. El concentrador distribuye esta nueva información a los otros spokes. También propaga la información de ruteo del otro spokes a este spoke.

Creación del túnel dinámico para el tráfico del “spoke al spoke”

Como se dijo antes, actualmente en una red de interconexión, todos los túneles IPsec punto a punto (o IPsec+GRE) deben ser configurados en todos los routers, aún cuando algunos o la mayoría de esos túneles no estén siendo ejecutados o no se los necesite todo el tiempo. Con la solución DMVPN, un router es el concentrador, y configuran al resto de Routers (spokes) con los túneles al concentrador. Los túneles de radio a eje de conexión están activos continuamente, y los radios no necesitan configurarse para túneles directos a ninguno de los otros radios. En lugar, cuando un spoke quiere transmitir un paquete a otro spoke (tal como la subred detrás de otro spoke), utiliza el NHRP para determinar dinámicamente el direccionamiento de destino requerido del spoke de la blanco. El router hub actúa como un servidor NHRP y administra este pedido para el spoke fuente. Luego, los dos spokes crean de forma dinámica un túnel IPSec entre ellos (a través de la interfaz mGRE única) y la información se puede transferir directamente. Este túnel dinámico radio a radio será automáticamente desmontado luego de un período de inactividad (configurable).

Soporte de protocolos de ruteo dinámico

La solución DMVPN se basa en los túneles GRE que soportan los paquetes del Multicast/del IP de broadcast del Tunelización, así que la solución DMVPN también soporta los Dynamic Routing Protocol que se ejecutan sobre los túneles IPsec+mGRE. Anteriormente, NHRP necesitaba que el usuario configure de manera explícita la correspondencia de difusión/multidifusión para que las direcciones IP de destino del túnel admitan la tunelización GRE de paquetes IP de multidifusión y de difusión. Por ejemplo, en el concentrador usted necesitaría la línea de configuración del **<spoke-n-addr> del Multicast de la correspondencia del nhrp del IP** para cada spoke. Con la solución DMVPN, las direcciones radiales no se conocen con anticipación, por lo tanto esta configuración no es posible. En lugar, el NHRP se puede configurar para agregar automáticamente cada habló a la lista del destino multidifusión en el concentrador con el **comando ip nhrp map multicast dynamic**. Con este comando, cuando los routeres radiales registran su mapeo NHRP del unicast con el servidor NHRP (concentrador), el NHRP también creará un broadcast/un mapeo multidifusión para este spoke. Esto elimina la necesidad de conocer de antemano las direcciones del spoke.

Fast Switching de Cisco Express Forwarding para mGRE

Actualmente, el tráfico en una interfaz mGRE utiliza el modo de switch de proceso, y su rendimiento es pobre. La solución DMVPN agrega la conmutación de Cisco Express Forwarding para el tráfico mGRE, lo cual resulta en un rendimiento superior. No hay comandos de configuración necesarios para activar esta función. Si el Cisco Express Forwarding Switching se permite en la interfaz de túnel GRE y las interfaces físicas salientes/entrantes, después los paquetes de túnel GRE de múltiples puntos serán expresos de Cisco Expedición-conmutados.

Uso de ruteo dinámico en VPN protegidas IPsec

Esta sección describe el estado actual (solución pre-DMVPN). El IPSec se implementa en los routeres Cisco vía un conjunto de comandos que definen el cifrado y entonces un **comando crypto map <map-name>** aplicados en la interfaz externa del router. Debido a este diseño y el hecho de que no haya actualmente un estándar para usar el IPSec para cifrar el Multicast IP/los paquetes de broadcast, los paquetes del IP Routing Protocol no se pueden “remitir” a través del túnel IPsec y ninguna cambios de ruteo no se pueden propagar dinámicamente al otro lado del túnel IPsec.

Nota: Todos los Dynamic Routing Protocol excepto el BGP utilizan el broadcast o los paquetes del IP de multidifusión. Los túneles GRE se usan en combinación con IPsec para resolver este problema.

Los túneles GRE se implementan en los routeres Cisco usando una interfaz del túnel virtual (**tunnel<#> de la interfaz**). El protocolo de la tunelización GRE se diseña para manejar el Multicast IP/los paquetes de broadcast así que un Dynamic Routing Protocol se puede “funcionar con encima” un túnel GRE. Los paquetes de túnel GRE son paquetes de unidifusión IP que encapsulan el paquete de multdifusión/unidifusión IP original. Puede usar IPsec para cifrar el paquete de túnel GRE. También puede ejecutar IPsec en modo de transporte y ahorrar 20 bytes, ya que GRE ya ha encapsulado el paquete de datos original y no necesita que IPsec encapsule el paquete IP GRE en otro encabezado de IP.

Cuando se ejecuta IPsec en modo de transporte, hay una restricción que consiste en que las direcciones de origen y destino de IP del paquete que van a cifrarse deben coincidir con las direcciones del par IPsec (el mismo router). En este caso, esto sólo significa que el punto final del túnel GRE y la dirección IPsec del par deben ser las mismas. Esto no es un problema, ya que los mismos routers son puntos finales del túnel tanto de IPsec como de GRE. Combinando los túneles GRE con la encripción de IPSec, usted puede utilizar un protocolo del Dynamic IP Routing para poner al día las tablas de ruteo en los ambos extremos del túnel encriptado. Las entradas de tabla de IP Routing para las redes que eran doctas a través del túnel encriptado tendrán el otro extremo del túnel (dirección IP de la interfaz de túnel GRE) como el salto siguiente IP. Así, si las redes cambian a cada lado del túnel, después el otro lado aprenderá dinámicamente del cambio y la Conectividad continuará sin ningunos cambios de configuración en el Routers.

Configuración base

La siguiente es una configuración estándar punto a punto IPsec+GRE. Luego de esto, existe una serie de ejemplos de configuración en los que paso a paso se agregan características específicas de la solución DMVPN para mostrar las diferentes capacidades de DMVPN. Cada ejemplo utiliza al anterior para mostrar cómo utilizar la solución para DMVPN en diseños de red cada vez más complejos. Esta sucesión de ejemplos puede usarse como una plantilla para migrar una VPN IPsec+GRE actual a una DMVPN. Usted puede parar “la migración” en cualquier momento si ese ejemplo de la configuración determinada hace juego sus requisitos de diseño de red.

Hub and spoke del IPsec+GRE (n = 1,2,3,…)

Router del eje de conexión
version 12.3 ! hostname Hub ! crypto isakmp policy 1 authentication pre-share crypto isakmp key cisco47 address 0.0.0.0 ! crypto ipsec transform-set trans2 esp-des esp-md5-hmac

```
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0 crypto map
vpnmap1 10 ipsec-isakmp set peer 172.16.1.1 set
transform-set trans2 match address 101 crypto map
vpnmap1 20 ipsec-isakmp set peer 172.16.2.1 set
transform-set trans2 match address 102 . . . crypto map
vpnmap1 <10*n> ipsec-isakmp set peer 172.16.<n>.1 set
transform-set trans2 match address <n+100> ! interface
Tunnel1 bandwidth 1000 ip address 10.0.0.1
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.16.1.1 ! interface
Tunnel2 bandwidth 1000 ip address 10.0.0.5
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.16.2.1 ! . . . !
interface Tunnel<n> bandwidth 1000 ip address
10.0.0.<4n-3> 255.255.255.252 ip mtu 1400 delay 1000
tunnel source Ethernet0 tunnel destination 172.16.<n>.1
! interface Ethernet0 ip address 172.17.0.1
255.255.255.0 crypto map vpnmap1 ! interface Ethernet1
ip address 192.168.0.1 255.255.255.0 ! router eigrp 1
network 10.0.0.0 0.0.0.255 network 192.168.0.0 0.0.0.255
no auto-summary ! access-list 101 permit gre host
172.17.0.1 host 172.16.1.1 access-list 102 permit gre
host 172.17.0.1 host 172.16.2.1 ... access-list <n+100>
permit gre host 172.17.0.1 host 172.16.<n>.1
```

Router Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1 authentication pre-share crypto
isakmp key cisco47 address 0.0.0.0 ! crypto ipsec
transform-set trans2 esp-des esp-md5-hmac mode transport
! crypto map vpnmap1 local-address Ethernet0 crypto map
vpnmap1 10 ipsec-isakmp set peer 172.17.0.1 set
transform-set trans2 match address 101 ! interface
Tunnel0 bandwidth 1000 ip address 10.0.0.2
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 ! interface
Ethernet0 ip address 172.16.1.1 255.255.255.252 crypto
map vpnmap1 ! interface Ethernet1 ip address 192.168.1.1
255.255.255.0 ! router eigrp 1 network 10.0.0.0
0.0.0.255 network 192.168.1.0 0.0.0.255 no auto-summary
! access-list 101 permit gre host 172.16.1.1 host
172.17.0.1
```

Router Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0 crypto map
vpnmap1 10 ipsec-isakmp set peer 172.17.0.1 set
transform-set trans2 match address 101 ! interface
Tunnel0 bandwidth 1000 ip address 10.0.0.6
```

```
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 ! interface
Ethernet0 ip address 172.16.2.1 255.255.255.252 crypto
map vpnmap1 ! interface Ethernet1 ip address 192.168.2.1
255.255.255.0 ! router eigrp 1 network 10.0.0.0
0.0.0.255 network 192.168.2.0 0.0.0.255 no auto-summary
! access-list 101 permit gre host 172.16.2.1 host
172.17.0.1
```

Router del Spoke<n>

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
mode transport ! crypto map vpnmap1 local-address
Ethernet0 crypto map vpnmap1 10 ipsec-isakmp set peer
172.17.0.1 set transform-set trans2 match address 101 !
interface Tunnel0 bandwidth 1000 ip address 10.0.0.<4n-
2> 255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 ! interface
Ethernet0 ip address 172.16.<n>.1 255.255.255.252 crypto
map vpnmap1 ! interface Ethernet1 ip address
192.168.<n>.1 255.255.255.0 ! router eigrp 1 network
10.0.0.0 0.0.0.255 network 192.168.<n>.0 0.0.0.255 no
auto-summary ! access-list 101 permit gre host
172.16.<n>.1 host 172.17.0.1
```

En la configuración antedicha, los ACL se utilizan para definir qué tráfico será cifrado. En los routers concentradores y los radiales, esta ACL solamente debe coincidir con los paquetes IP del túnel GRE. No importa cómo las redes cambian en cualquier extremo, los paquetes del túnel IP GRE no cambiarán, así que este ACL no necesita cambiar.

Nota: Al usar las versiones del Cisco IOS Software antes de 12.2(13)T, usted debe aplicar el comando configuration del **vpnmap1 de la correspondencia de criptografía a las** interfaces de túnel GRE (Tunnel<x>) y a la interfaz física (ethernet0). Con un IOS de Cisco versión 12.2(13)T y superior, sólo se usa el comando de configuración crypto map vpnmap1 en la interfaz física (Ethernet0).

Ejemplos de tablas de ruteo en los routers radiales y de eje de conexión

Tabla de ruteo sobre router de eje de conexión

```
172.17.0.0/24 is subnetted, 1 subnets
 C       172.17.0.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 C       10.0.0.0 is directly connected, Tunnel1
 C       10.0.0.4 is directly connected, Tunnel2
 ...
 C       10.0.0.<4n-4> is directly connected, Tunnel<n>
 C    192.168.0.0/24 is directly connected, Ethernet1
 D    192.168.1.0/24 [90/2841600] via 10.0.0.2,
18:28:19, Tunnel1
 D    192.168.2.0/24 [90/2841600] via 10.0.0.6, 2d05h,
Tunnel2
 ...
 D    192.168.<n>.0/24 [90/2841600] via 10.0.0.<4n-2>,
```

```
2d05h, Tunnel<n>
```

Tabla de ruteo en el router Radio1

```
172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.1.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 C       10.0.0.0 is directly connected, Tunnel1
 D       10.0.0.4 [90/2841600] via 10.0.0.1, 23:00:58,
Tunnel0
 ...
 D      10.0.0.<4n-4> [90/2841600] via 10.0.0.1,
23:00:58, Tunnel0
 D    192.168.0.0/24 [90/2841600] via 10.0.0.1,
23:00:58, Tunnel0
 C    192.168.1.0/24 is directly connected, Loopback0
 D    192.168.2.0/24 [90/3097600] via 10.0.0.1,
23:00:58, Tunnel0
 ...
 D    192.168.<n>.0/24 [90/3097600] via 10.0.0.1,
23:00:58, Tunnel0
```

Tabla de ruteo en el router del Spoke<n>

```
172.16.0.0/24 is subnetted, 1 subnets
 C       172.16.<n>.0 is directly connected, Ethernet0
      10.0.0.0/30 is subnetted, <n> subnets
 D       10.0.0.0 [90/2841600] via 10.0.0.1, 22:01:21,
Tunnel0
 D       10.0.0.4 [90/2841600] via 10.0.0.1, 22:01:21,
Tunnel0
 ...
 C        10.0.0.<4n-4> is directly connected, Tunnel0
 D    192.168.0.0/24 [90/2841600] via 10.0.0.1,
22:01:21, Tunnel0
 D    192.168.1.0/24 [90/3097600] via 10.0.0.1,
22:01:21, Tunnel0
 D    192.168.2.0/24 [90/3097600] via 10.0.0.1,
22:01:21, Tunnel0
 ...
 C    192.168.<n>.0/24 is directly connected, Ethernet0
```

Ésta es la configuración básica, y es utilizada como un punto de partida para la comparación con las configuraciones más complejas posibles utilizando la solución DMVPN. El primer cambio reducirá el tamaño de la configuración en el router de eje de conexión. Esto no es importante si la cantidad de routers radiales es poca, pero es crítico cuando hay más de 50 ó 100.

Reducción del tamaño de la configuración del hub/router

En el siguiente ejemplo, la configuración se modifica mínimamente en el router de eje de conexión de varias interfaces de túnel punto a punto GRE a una única interfaz de túnel multipunto GRE. Este es un primer paso en la solución DMVPN.

Hay un bloque único de las líneas de configuración en el router de eje de conexión para definir las características de la correspondencia de criptografía para cada router radial. Esta parte de la configuración define la ACL criptográfica y la interfaz de túnel GRE para ese router spoke. Estas características son sobre todo lo mismo para todo el spokes, a excepción de los IP Addresses (**fije el par…**, el **destino del túnel…**).

Mirando la configuración antedicha en el router de eje de conexión, usted ve que hay por lo menos 13 líneas de configuración por el router radial; cuatro para la correspondencia de

criptografía, uno para el ACL crypto, y ocho para la interfaz de túnel GRE. El número total de líneas de configuraciones, en caso de que haya 300 routers radiales, es equivalente a 3900 líneas. Usted también necesita 300 (/30) subred para dirigir cada link del túnel. Una configuración de este tamaño es muy dura de manejar y aún más difícil al resolver problemas la red VPN. Para reducir este valor, puede utilizar mapas de criptografía dinámicos, lo que reduciría el valor anterior en 1200 línea y dejaría 2700 líneas en una red de 300 radios.

Nota: Al utilizar mapas de criptografía dinámicos, el túnel de encripción IPsec debe ser iniciado mediante el router radial. Usted puede también utilizar el **<interface> innumerable del IP** para reducir el número de subredes necesarias para los túneles GRE, pero esto puede hacer resolver problemas un más adelante más difícil.

Con la solución DMBPN, puede configurar una sola interfaz de túnel GRE multipunto y un solo perfil IPSec en el router de eje de conexión para manejar todos los routers radiales. Esto permite que el tamaño de la configuración en el router de eje de conexión permanezca constante irrespectivamente de la cantidad de routers de eje de conexión que se agreguen a la red VPN.

La solución DMVPN presenta a los comandos new siguientes:

```
crypto ipsec profile <name> <ipsec parameters> tunnel protection ipsec profile <name> ip nhrp map multicast dynamic
```

Utilizan al **comando crypto ipsec profile <name>** como una correspondencia cifrada dinámica, y se diseña específicamente para las interfaces del túnel. Este comando se usa para definir los parámetros para el encripción de IPsec en los túneles VPN de spoke a hub y de spoke a spoke. El único parámetro que se requiere bajo perfil es el conjunto de la transformación. El direccionamiento del peer IPSec y la cláusula del **direccionamiento de la coincidencia…** para proxy IPsec se derivan automáticamente de los mapeos NHRP para el túnel GRE.

Configuran bajo interfaz de túnel GRE y se utilizan al **comando tunnel protection ipsec profile <name>** para asociar la interfaz de túnel GRE con el perfil de ipsec. Además, el **comando tunnel protection ipsec profile <name>** puede también ser utilizado con un túnel GRE de punto a punto. En este caso derivará el par IPsec e información proxy desde la configuración de ... origen de túnel y ... destino de túnel. Esto simplifica la configuración ya que el par IPsec y las ACL criptográficas ya no se necesitan.

Nota: El comando tunnel protection… especifica que la encripción de IPSec será hecha después de que la encapsulación GRE se haya agregado al paquete.

Estos primeros dos comandos new son similares a configurar una correspondencia de criptografía y a asignar la correspondencia de criptografía a una interfaz usando el **comando crypto map <name>**. La gran diferencia es que, con los nuevos comandos, no es necesario especificar la dirección de par IPsec o una ACL para hacer coincidir los paquetes que se van a cifrar. Estos parámetros se determinan de forma automática desde los mapeos NHRP para la interfaz del túnel mGRE.

Nota: Al usar el **comando tunnel protection…** en la interfaz del túnel, no configuran a un **comando crypto map…** en la interfaz saliente física.

El comando new más reciente, **Multicast de la correspondencia del nhrp del IP dinámico**, permite que el NHRP agregue automáticamente a los routeres radiales a los mapeos NHRP del Multicast cuando estos routeres radiales inician el túnel del mGRE+IPsec y registran sus mapeos NHRP del unicast. Esto es necesario permitir a los Dynamic Routing Protocol para trabajar sobre los túneles

del mGRE+IPsec entre el concentrador y el spokes. Si este comando no estuviera disponible, después el router de eje de conexión necesitaría tener una línea de configuración separada para un mapeo multidifusión a cada spoke.

Nota: Con esta configuración, los routers radiales deben iniciar la conexión de túnel mGRE+IPsec, ya que el router hub no está configurado con información sobre los radios. No obstante, éste no es un problema porque con DMVPN el túnel mGRE+IPsec se inicia automáticamente cuando se inicia el router radial, y se mantiene siempre activo.

Nota: El siguiente ejemplo muestra las interfaces de túnel GRE punto a punto en los routers de radio y líneas de configuración NHRP incorporadas a los routers de radio y eje de conexión para soportar el túnel mGRE en el router de eje de conexión. Los cambios de configuración son los siguientes.

Router del eje de conexión (anterior)

```
crypto map vpnmap1 10 IPsec-isakmp set peer 172.16.1.1
set transform-set trans2 match address 101 crypto map
vpnmap1 20 IPsec-isakmp set peer 172.16.2.1 set
transform-set trans2 match address 102 . . . crypto map
vpnmap1 <10n> IPsec-isakmp set peer 172.16.<n>.1 set
transform-set trans2 match address <n+100> ! interface
Tunnel1 bandwidth 1000 ip address 10.0.0.1
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.16.1.1 ! interface
Tunnel2 bandwidth 1000 ip address 10.0.0.5
255.255.255.252 ip mtu 1400 delay 1000 tunnel source
Ethernet0 tunnel destination 172.16.2.1 ! . . . !
interface Tunnel<n> bandwidth 1000 ip address
10.0.0.<4n-1> 255.255.255.252 ip mtu 1400 delay 1000
tunnel source Ethernet0 tunnel destination 172.16.<n>.1
! interface Ethernet0 ip address 172.17.0.1
255.255.255.0 crypto map vpnmap1 ! access-list 101
permit gre host 172.17.0.1 host 172.16.1.1 access-list
102 permit gre host 172.17.0.1 host 172.16.2.1 . . .
access-list <n+100> permit gre host 172.17.0.1 host
172.16.<n>.1
```

Router de eje de conexión (nuevo)

```
crypto ipsec profile vpnprof set transform-set trans2 !
interface Tunnel0 bandwidth 1000 ip address 10.0.0.1
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map multicast dynamic ip nhrp network-id 100000 ip
nhrp holdtime 600 no ip split-horizon eigrp 1 delay 1000
tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address 172.17.0.1
255.255.255.0
```

Router del Spoke<n> (viejo)

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<4n-2> 255.255.255.252 ip mtu 1400
delay 1000 tunnel source Ethernet0 tunnel destination
```

```
172.17.0.1 ! interface Ethernet0 ip address 172.16.<n>.1
255.255.255.252 crypto map vpnmap1 ! . . . ! access-list
101 permit gre host 172.16.<n>.1 host 172.17.0.1 !
```

Router del Spoke<n> (nuevo)

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<n+1> 255.255.255.0 ip mtu 1400 ip
nhrp authentication test ip nhrp map 10.0.0.1 172.17.0.1
ip nhrp network-id 100000 ip nhrp holdtime 300 ip nhrp
nhs 10.0.0.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.1 tunnel key 100000 ! interface
Ethernet0 ip address 172.16.<n>.1 255.255.255.252 crypto
map vpnmap1 ! . . . ! access-list 101 permit gre host
172.16.<n>.1 host 172.17.0.1 !
```

En los routeres radiales, la máscara de subred ha cambiado, y los comandos NHRP se han agregado bajo interfaz del túnel. Los comandos NHRP son necesarios puesto que el router de eje de conexión ahora está utilizando el NHRP para asociar la dirección IP de la interfaz del túnel del spoke a la dirección IP de la interfaz física del spoke.

ip address 10.0.0.<n+1> 255.255.255.0 ip mtu 1400 ip nhrp authentication test ip nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000 ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 ... tunnel key 100000

La subred ahora está /24 en lugar de /30, entonces todos los nodos están en la misma subred en lugar de estar en subredes distintas. Los radios aún envían tráfico de radio a radio a través del hub, ya que utilizan una interfaz de túnel punto a punto GRE. Utilizan a los **comandos ip nhrp authentication…, ip nhrp network-id… y tunnel key…** de asociar los paquetes del túnel y los paquetes nhrp a la interfaz de túnel GRE y a la red NHRP de múltiples puntos correctas cuando los reciben en el concentrador. **La correspondencia del nhrp del IP…** y los comandos de los **nhs del nhrp del IP**… son utilizados por el NHRP en hablaron para hacer publicidad del mapeo NHRP del spokes (10.0.0.<n+1> --> 172.16.<n>.1) al concentrador. El direccionamiento 10.0.0.<n+1> se extrae del **comando ip address…** en la interfaz del túnel y el direccionamiento 172.16.<n>.1 se extrae del **comando tunnel destination…** en la interfaz del túnel.

En un caso donde hay 300 routeres radiales, este cambio reduciría el número de líneas de configuración en el concentrador a partir de 3900 líneas a 16 líneas (una reducción de 3884 líneas). La configuración en cada router radial aumentaría en 6 líneas.

Soporte de direcciones dinámicas en radios

En un router de Cisco, cada par IPsec debe ser configurado con la dirección IP del otro par IPsec antes de que el túnel IPsec pueda aparecer. Esto ocasiona un problema si el router spoke tiene una dirección dinámica en su interfaz física, lo cual es común en los routers conectados mediante links de DSL o cable.

TED permite que un par IPSec busque a otro par IPSec por medio del envío de un paquete de Protocolos de administración de claves y asociaciones de seguridad de Internet (ISAKMP) a la dirección IP de destino del paquete de datos originales que debían cifrarse. Se supone que este paquete atravesará la red interviniente por el mismo trayecto que el que recorre por el paquete del

túnel IPsec. Este paquete será cogido por el peer IPSec del otro extremo, que responderá al primer par. Los dos routers entonces negociarán asociaciones de seguridad (SA) IPsec e ISAKMP y encenderán el túnel IPsec. Esto sólo funcionará si los paquetes de datos a cifrar tienen direcciones IP enrutables.

La TED puede utilizarse en combinación con los túneles GRE con la configuración de la sección anterior. Se ha probado esto y los trabajos, aunque había un bug en las versiones anteriores del Cisco IOS Software donde TED forzó todo el tráfico IP entre los dos peeres IPSec a ser cifrado, no apenas los paquetes de túnel GRE. La solución DMVPN proporciona esta y otras capacidades adicionales sin que el host tenga que utilizar direcciones de IP enrutables y sin tener que enviar paquetes de prueba y respuesta. Con una pequeña modificación, la configuración de la última sección puede utilizarse para el soporte de routers radiales con direcciones IP dinámicas en sus interfaces físicas externas.

Router de eje de conexión (sin cambios)

```
crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
```

Router del Spoke<n> (viejo)

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  match address 101
 !
 ...
 !
 access-list 101 permit gre host 172.16.<n>.1 host
172.17.0.1
```

Router del Spoke<n> (nuevo)

```
crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set transform-set trans2
  set security-association level per-host match address
101 ! ... ! access-list 101 permit gre any host
172.17.0.1
```

La funcionalidad utilizada en la nueva configuración spoke funciona de la siguiente manera.

- Cuando aparece la interfaz de túnel GRE, comenzará a enviar paquetes de registro NHRP al router concentrador. Estos paquetes de inscripción NHRP accionarán el IPSec que se

iniciará. En el router radial, configuran al par del conjunto <peer-address> y a los **comandos match ip access-list <ACL>**. El ACL especifica el GRE como el protocolo, ninguno para la fuente, y la dirección IP del concentrador para el destino.**Nota:** Es importante observar que ninguno se está utilizando como la fuente en el ACL, y éste debe ser el caso puesto que la dirección IP del router radial es dinámica y, por lo tanto, no sabida antes de que la interfaz física sea activa. Puede usarse una subred de IP para la fuente en ACL si la dirección spoke de la interfaz dinámica estará restringida a una dirección dentro de esa subred.

- Utilizan al **comando set security-association level per-host** de modo que el IP de origen en el spokes proxy IPsec sea apenas el direccionamiento actual de la interfaz física del spokes (/32), bastante que el “ningunos” del ACL. Si el “ningunos” del ACL fueran utilizados como la fuente en proxy IPsec, impedirían a cualquier otro router radial también de configurar un túnel del IPsec+GRE con este concentrador. Esto se debe a que la IPsec proxy resultante en el hub sería equivalente para permitir gre host 172.17.0.1 any. Esto significaría que a todos los paquetes de túnel GRE destinados a cualquier spoke se los cifraría y enviaría al primer spoke que estableció un túnel con el concentrador, ya que su proxy IPsec hace coincidir paquetes GRE para cada spoke.
- Una vez establecido el túnel IPsec, un paquete de registro NHRP va desde el router spoke hasta el Servidor de salto siguiente (NHS) configurado. El NHS es el router hub de esta red hub-and-spoke. El paquete de registro NHRP proporciona la información para el router de eje de conexión que permite crear una correspondencia NHRP para este router radial. Con esta correspondencia, el router de eje de conexión puede reenviar paquetes de datos IP de unidifusión a este router de radio por el túnel mGRE+IPsec. También, el concentrador agrega al router radial a su lista del mapeo multidifusión NHRP. El eje de conexión comienza a enviar paquetes de Dynamic IP Routing Multicast a la radio (en caso de que el Dynamic Routing Protocol esté configurado). El spoke entonces sentirá bien a un vecino del Routing Protocol del concentrador, e intercambiarán las actualizaciones de ruteo.

Hub y spoke IPsec + mGRE

Router del eje de conexión

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map multicast dynamic ip
nhrp network-id 100000 ip nhrp holdtime 600 no ip split-
horizon eigrp 1 delay 1000 tunnel source Ethernet0
tunnel mode gre multipoint tunnel key 100000 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
ip address 172.17.0.1 255.255.255.0 ! interface
Ethernet1 ip address 192.168.0.1 255.255.255.0 ! router
eigrp 1 network 10.0.0.0 0.0.0.255 network 192.168.0.0
```

```
0.0.0.255 no auto-summary !
```

En la configuración del eje de conexión anterior, observe que las direcciones IP de los routers radiales no están configuradas. La interfaz física externa del spoke y la asignación a la dirección IP de la interfaz del túnel spoke son aprendidas en forma dinámica por el hub a través del NHRP. Esto permite que la dirección IP externa de la interfaz física del rayo sea asignada dinámicamente.

Router Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set security-association level per-host set transform-
set trans2 match address 101 ! interface Tunnel0
bandwidth 1000 ip address 10.0.0.2 255.255.255.0 ip mtu
1400 ip nhrp authentication test ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp network-id 100000 ip nhrp holdtime
300 ip nhrp nhs 10.0.0.1 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 tunnel key
100000 ! interface Ethernet0 ip address dhcp hostname
Spoke1 crypto map vpnmap1 ! interface Ethernet1 ip
address 192.168.1.1 255.255.255.0 ! router eigrp 1
network 10.0.0.0 0.0.0.255 network 192.168.1.0 0.0.0.255
no auto-summary ! access-list 101 permit gre 172.16.1.0
0.0.0.255 host 172.17.0.1
```

Router Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto map vpnmap1 local-address Ethernet0
 crypto map vpnmap1 10 IPsec-isakmp
  set peer 172.17.0.1
  set security-association level per-host set transform-
set trans2 match address 101 ! interface Tunnel0
bandwidth 1000 ip address 10.0.0.3 255.255.255.0 ip mtu
1400 ip nhrp authentication test ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp network-id 100000 ip nhrp holdtime
300 ip nhrp nhs 10.0.0.1 delay 1000 tunnel source
Ethernet0 tunnel destination 172.17.0.1 tunnel key
100000 ! interface Ethernet0 ip address dhcp hostname
Spoke2 crypto map vpnmap1 ! interface Ethernet1 ip
address 192.168.2.1 255.255.255.0 ! router eigrp 1
```

```
network 10.0.0.0 0.0.0.255 network 192.168.1.0 0.0.0.255
no auto-summary ! access-list 101 permit gre 172.16.2.0
0.0.0.255 host 172.17.0.1
```

Lo más importante que debe tener en cuenta acerca de la configuración de spoke es lo siguiente:

- La dirección IP de la interfaz física externa (ethernet0) es dinámica por DHCP.**ip address dhcp hostname Spoke2**
- El ACL crypto (101) especifica una subred como la fuente para proxy IPsec.**access-list 101 permit gre 172.16.2.0 0.0.0.255 host 172.17.0.1**
- El siguiente comando en el mapa de encripción de IPsec especifica que la asociación de seguridad se hará por host.**set security-association level per-host**
- Todos los túneles forman parte de la misma subred, dado que todos ellos se encuentran conectados a través de la misma interfaz GRE multipunto en el router hub.**ip address 10.0.0.2 255.255.255.0**

La combinación de estos tres comandos hace innecesaria la configuración de la dirección IP de la interfaz física externa para el spoke's. Proxy IPsec se utiliza que sea bastante entonces basado en la subred basado en el host.

La configuración en los routers radiales tiene la dirección IP del router de eje de conexión configurada ya que necesita iniciar el túnel IPsec+GRE. Note la similitud entre las configuraciones Spoke 1 y Spoke 2. No sólo son estos dos similares, pero todas las configuraciones del router radial serán similares. En la mayoría de los casos, todos los del spokes IP Address únicos de la necesidad simplemente en sus interfaces, y el resto de sus configuraciones serán lo mismo. Esto hace posible una rápida configuración e instrumentación de varios routers spoke.

Los datos NHRP tienen el siguiente aspecto en el eje de conexión y radio.

Router del eje de conexión

```
Hub#show ip nhrp 10.0.0.2/32 via 10.0.0.2, Tunnel0
created 01:25:18, expire 00:03:51 Type: dynamic, Flags:
authoritative unique registered NBMA address: 172.16.1.4
10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:06:02,
expire 00:04:03 Type: dynamic, Flags: authoritative
unique registered NBMA address: 172.16.2.10 ...
10.0.0.<n>/32 via 10.0.0.<n>, Tunnel0 created 00:06:00,
expire 00:04:25 Type: dynamic, Flags: authoritative
unique registered NBMA address: 172.16.<n>.41
```

Router Spoke1

```
Spoke1#sho ip nhrp 10.0.0.1/32 via 10.0.0.1, Tunnel0
created 4d08h, never expire Type: static, Flags:
authoritative NBMA address: 172.17.0.1
```

Configuración multipunto dinámica de eje de conexión y radio

La configuración en los routers radiales arriba no se basa en funciones de la solución DMVPN, de manera que estos routers radiales pueden ejecutar las versiones del software Cisco IOS anteriores a la 12.2 (13)T. La configuración del router hub depende de las funciones DMVPN, por lo que debe ejecutar la versión 12.2(13)T u otra posterior del IOS de Cisco. Esto no le prohibe una cierta flexibilidad en decidir cuando usted necesita actualizar a sus routeres radiales que se desplieguen ya. Si los routers radiales también están ejecutando Cisco IOS 12.2(13)T o posterior, puede simplificar la configuración radial como se indica a continuación.

Router del Spoke<n> (antes del Cisco IOS 12.2(13)t)

```
crypto map vpnmap1 10 IPsec-isakmp set peer 172.17.0.1
set security-association level per-host set transform-
set trans2 match address 101 ! interface Tunnel0
bandwidth 1000 ip address 10.0.0.<n+1> 255.255.255.0 ip
mtu 1400 ip nhrp authentication test ip nhrp map
10.0.0.1 172.17.0.1 ip nhrp network-id 100000 ip nhrp
holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000 tunnel
source Ethernet0 tunnel destination 172.17.0.1 tunnel
key 100000 ! interface Ethernet0 ip address dhcp
hostname Spoke<n> crypto map vpnmap1 ! . . . ! access-
list 101 permit gre any host 172.17.0.1
```

Router del Spoke<n> (después del Cisco IOS 12.2(13)t)

```
crypto ipsec profile vpnprof set transform-set trans2 !
interface Tunnel0 bandwidth 1000 ip address 10.0.0.<n+1>
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000
ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000
tunnel source Ethernet0 tunnel destination 172.17.0.1
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke<n> !
```

Tenga en cuenta que hicimos lo siguiente:

1. Eliminamos el comando crypto map vpnmap1 10 ipsec-isakmp y lo reemplazamos por crypto ipsec profile vpnprof.
2. Quitó el **comando crypto map vpnmap1 de las** interfaces del ethernet0 y ponen el **comando tunnel protection ipsec profile vpnprof** en la interfaz del tunnel0.
3. Eliminó la ACL de criptografía, access-list 101 permit gre any host 172.17.0.1.

En este caso las direcciones y proxies pares de IPsec se derivan automáticamente de la configuración del túnel de origen … y del túnel de destino. Los pares y los proxys son como sigue (como se ve en la salida del **comando show crypto ipsec sa**):

```
...
local ident (addr/mask/prot/port):    (172.16.1.24/255.255.255.255/47/0)
remote ident (addr/mask/prot/port):   (172.17.0.1/255.255.255.255/47/0)
...
local crypto endpt.: 172.17.1.24, remote crypto endpt.:172.17.0.1
...
```

En resumen, las siguientes configuraciones totales incluyen todos los cambios realizados en este punto desde la configuración base (eje de conexión y radio IPsec+GRE).

Router del eje de conexión

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
```

```
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  no ip split-horizon eigrp 1
  delay 1000
  tunnel source Ethernet0
  tunnel mode gre multipoint
  tunnel key 100000
  tunnel protection ipsec profile vpnprof
 !
 interface Ethernet0
  ip address 172.17.0.1 255.255.255.0
 !
 interface Ethernet1
  ip address 192.168.0.1 255.255.255.0
 !
 router eigrp 1
  network 10.0.0.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
  no auto-summary
 !
```

No hay cambios en la configuración del eje de conexión.

Router Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof set transform-set trans2 !
interface Tunnel0 bandwidth 1000 ip address 10.0.0.2
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000
ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000
tunnel source Ethernet0 tunnel destination 172.17.0.1
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke2 ! interface Ethernet1 ip address 192.168.1.1
255.255.255.0 ! router eigrp 1 network 10.0.0.0
0.0.0.255 network 192.168.1.0 0.0.0.255 no auto-summary
!
```

Router Spoke2

```
version 12.3
 !
 hostname Spoke2
```

```
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof set transform-set trans2 !
interface Tunnel0 bandwidth 1000 ip address 10.0.0.3
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000
ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000
tunnel source Ethernet0 tunnel destination 172.17.0.1
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke2 ! interface Ethernet1 ip address 192.168.2.1
255.255.255.0 ! router eigrp 1 network 10.0.0.0
0.0.0.255 network 192.168.2.0 0.0.0.255 no auto-summary
!
```

Red privada virtual multipunto dinámica con IPsec

Los conceptos y la configuración de esta sección muestran las capacidades completas de DMVPN. El NHRP proporciona la capacidad para que los routeres radiales aprendan dinámicamente el direccionamiento exterior de la interfaz física de los otros routeres radiales en la red VPN. Esto significa que el router spoke tendrá suficiente información para construir dinámicamente un túnel IPsec+mGRE directamente hacia otro router spoke. Esto es muy beneficioso ya que, si este tráfico de datos de radio a radio fuera enviado a través del router concentrador debería ser encripción/desencripción, aumentando al doble el retraso y la carga en el router concentrador. Para utilizar esta función, los routers radiales deben estar conmutados de interfaces de túnel GRE punto a punto (p-pGRE) a GRE multipunto (mGRE). También deben aprender las redes o subredes disponibles detrás de los otros radiales con un salto siguiente de IP de la dirección IP del túnel del otro router radial. Los routeres radiales aprenden estas redes (sub) vía el protocolo del Dynamic IP Routing que se ejecuta sobre el túnel IPsec+mGRE con el concentrador.

El Dynamic IP Routing Protocol que se ejecuta en el router hub puede configurarse para reflejar a todos los spokes las rutas que aprendió un spoke fuera de la misma interfaz pero la IP de próximo salto en estas rutas será generalmente el router hub, no el router spoke del que aprendió esta ruta el hub.

Nota: El protocolo de ruteo dinámico se ejecuta sólo en los links de red radial pero no en los links de red radial dinámica.

Los protocolos de ruteo dinámico (RIP, OSPF y EIGRP) deben configurarse en un router hub para promocionar las rutas de regreso fuera de la interfaz de túnel mGRE. Además, deben configurarse para establecer el próximo salto de IP al router spoke de origen para aquellas rutas que se conocen por un spoke cuando la ruta se promociona a otros spokes.

A continuación se presentan los requisitos para las configuraciones de los protocolos de ruteo.

RIP

Usted necesita dar vuelta al horizonte apagado partido en la interfaz de túnel MGRE en el

concentrador, si no el RIP no hará publicidad de las rutas aprendidas vía la interfaz del mGRE se retira que lo mismo interconecta.

no ip split-horizon
No se necesitan otros cambios. El RIP utilizará automáticamente el Next-Hop original IP en las rutas de que hace publicidad se retira la misma interfaz donde aprendió estas rutas.

EIGRP

Debe apagar el horizonte dividido en la interfaz del túnel mGRE del hub, de lo contrario EIGRP no publicitará las rutas aprendidas a través de la interfaz mGRE de regreso a través de esa misma interfaz.

no ip split-horizon eigrp <as>
De manera predeterminada, EIGRP establecerá el next-hop de IP como router hub para las rutas que anuncia, aunque anuncie dichas rutas hacia la misma interfaz de la cual las obtuvo. Por consiguiente, en este caso necesita el siguiente comando de configuración para indicar a EIGRP que utilice el salto siguiente de IP original al anunciar estas rutas.

no ip next-hop-self eigrp <as>
Nota: El comando no ip next-hop-self eigrp <as> será el comenzar disponible en el Cisco IOS Release 12.3(2). Para las versiones del IOS de Cisco entre 12.2(13)T y 12.3(2) debe hacer lo siguiente:

- Si no se desean túneles dinámicos de spoke a spoke, no necesita el comando a continuación.
- Si se quieren los túneles dinámicos del spoke al spoke, después usted debe utilizar el process switching en la interfaz del túnel en los routeres radiales.
- De lo contrario, necesitará usar un protocolo de ruteo diferente sobre la DMVPN.

OSPF

Debido a que OSPF es un protocolo de ruteo de estado de link, no hay problemas de horizonte dividido. Normalmente para las interfaces multipunto debe configurar el tipo de red OSPF para que sea punto-a-multipunto, pero esto haría que el OSPF agregue rutas de host a la tabla de ruteo en los routers spoke. Estas rutas de los hosts harían que los paquetes destinados a las redes detrás de otros routers spoke sean reenviados a través del hub y no reenviados directamente al otro spoke. Para solucionar este problema, configure el tipo de red OSPF para difusión mediante el comando.

ip ospf network broadcast
Usted también necesita aseegurarse que el router de eje de conexión sea el router designado (DR) para la red IPsec+mGRE. Esto se realiza haciendo que la configuración de la prioridad OSPF sea mayor a 1 en el hub y a 0 en los spokes.

- Hub **prioridad 2 OSPF del IP**
- Spoke: **prioridad 0 OSPF del IP**

Hub simple para red DMVPN

Router del eje de conexión

```
version 12.3
 !
 hostname Hub
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
  ip nhrp holdtime 600
  ip ospf network broadcast ip ospf priority 2 delay
1000 tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address 172.17.0.1
255.255.255.0 ! interface Ethernet1 ip address
192.168.0.1 255.255.255.0 ! router ospf 1 network
10.0.0.0 0.0.0.255 area 0 network 192.168.0.0 0.0.0.255
area 0 !
```

El único cambio en la configuración del concentrador es que el OSPF es el protocolo de ruteo en lugar del EIGRP. Note que fijan al tipo de red OSPF para transmitir y la prioridad se fija a 2. que fijan el tipo de red OSPF para transmitir hará el OSPF instalar las rutas para las redes detrás del Routers del spokes con una dirección del salto siguiente IP como el direccionamiento del túnel GRE para ese router radial.

Router Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.2 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp network-id 100000 ip nhrp holdtime
300 ip nhrp nhs 10.0.0.1 ip ospf network broadcast ip
```

```
ospf priority 0 delay 1000 tunnel source Ethernet0
tunnel mode gre multipoint tunnel key 100000 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
ip address dhcp hostname Spoke1 ! interface Ethernet1 ip
address 192.168.1.1 255.255.255.0 ! router ospf 1
network 10.0.0.0 0.0.0.255 area 0 network 192.168.1.0
0.0.0.255 area 0 !
```

La configuración de los routers spoke es ahora muy similar a la configuración del hub. Las diferencias son como sigue:

- La prioridad OSPF se establece en 0. No se puede permitir que los routers radiales se conviertan en DR para la red de acceso múltiple sin difusión (NBMA) mGRE. Sólo el router hub tiene conexiones estáticas directas a todos los routers spoke. El DR debe tener acceso a todos los miembros de la red NBMA.
- Hay correspondencias NHRP unidifusión y multidifusión configuradas para el router de eje de conexión.
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1 172.17.0.1 En la configuración anterior, no se necesitaba el comando ip nhrp map multicast porque el túnel GRE era de punto a punto. En ese caso, los paquetes de multidifusión serán encapsulados automáticamente a través del túnel al solo destino posible. Este comando ahora se necesita porque el túnel GRE del spokes ha cambiado a de múltiples puntos y hay más entonces un destino posible.
- Cuando el router radial aparece, debe iniciar la conexión de túnel con el núcleo central, debido a que el router del núcleo central no está configurado con ninguna información referida a los routers radiales y los routers radiales pueden tener direcciones IP asignadas dinámicamente. Los routers radiales también están configurados con el eje de conexión como su NHS NHRP.`ip nhrp nhs 10.0.0.1`Mediante el comando anterior, el router spoke le envía, en intervalos regulares, paquetes de registro NHRP al router del concetrador a través del túnel mGRE+IPsec. Estos paquetes de registro proporcionan la información de correspondencia NHRP radial que necesita el router de eje de conexión para tunelizar los paquetes a los routers radiales.

Router Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.3 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
```

```
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  ip ospf network broadcast ip ospf priority 0 delay
1000 tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke1 ! interface Ethernet1 ip address 192.168.3.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 0 network 192.168.2.0 0.0.0.255 area 0 !
```

Router del Spoke<n>

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.<n+1> 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  ip ospf network broadcast ip ospf priority 0 delay
1000 tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke<n> ! interface Ethernet1 ip address 192.168.<n>.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 0 network 192.168.<n>.0 0.0.0.255 area 0 !
```

Observe que las configuraciones de todos los routers radiales son muy similares. Las únicas diferencias son los IP Addresses en las interfaces locales. Esto ayuda al desplegar a un gran número de routeres radiales. Todos los routers radiales pueden configurarse del mismo modo y sólo es necesario agregar las direcciones de interfaz IP locales.

En este momento, heche una ojeada las tablas de ruteo y las tablas del mapeo NHRP en el concentrador, Spoke1, y Routers del Spoke2 para ver las Condiciones iniciales (enseguida después que sube el Spoke1 y Routers del Spoke2) y las condiciones después de que el Spoke1 y el Spoke2 hayan establecido un link dinámico entre ellas.

Condiciones iniciales

Información del router de eje de conexión

```
Hub#show ip route 172.17.0.0/24 is subnetted, 1 subnets
C 172.17.0.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 C 192.168.0.0/24 is directly
```

```
connected, Ethernet1 O 192.168.1.0/24 [110/2] via
10.0.0.2, 00:19:53, Tunnel0 O 192.168.2.0/24 [110/2] via
10.0.0.3, 00:19:53, Tunnel0 Hub#show ip nhrp 10.0.0.2/32
via 10.0.0.2, Tunnel0 created 00:57:27, expire 00:04:13
Type: dynamic, Flags: authoritative unique registered
NBMA address: 172.16.1.24 10.0.0.3/32 via 10.0.0.3,
Tunnel0 created 07:11:25, expire 00:04:33 Type: dynamic,
Flags: authoritative unique registered NBMA address:
172.16.2.75 Hub#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 204
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 205
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 2628
Tunnel0 10.0.0.1 set HMAC_MD5 0 402 2629 Tunnel0
10.0.0.1 set HMAC_MD5 357 0 2630 Tunnel0 10.0.0.1 set
HMAC_MD5 0 427 2631 Tunnel0 10.0.0.1 set HMAC_MD5 308 0
```

Información del router Spoke1

```
Spoke1#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.1.24 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 O 192.168.0.0/24 [110/2] via
10.0.0.1, 00:31:46, Tunnel0 C 192.168.1.0/24 is directly
connected, Ethernet1 O 192.168.2.0/24 [110/2] via
10.0.0.3, 00:31:46, Tunnel0 Spoke1#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 01:42:00,
never expire Type: static, Flags: authoritative used
NBMA address: 172.17.0.1 Spoke1#show crypto engine
connection active ID Interface IP-Address State
Algorithm Encrypt Decrypt 2 Ethernet0 172.16.1.24 set
HMAC_SHA+DES_56_CB 0 0 2064 Tunnel0 10.0.0.2 set
HMAC_MD5 0 244 2065 Tunnel0 10.0.0.2 set HMAC_MD5 276 0
```

Información del router Spoke 2

```
Spoke2#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.2.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 O 192.168.0.0/24 [110/2] via
10.0.0.1, 00:38:52, Tunnel0 O 192.168.1.0/24 [110/2] via
10.0.0.2, 00:38:52, Tunnel0 C 192.168.2.0/24 is directly
connected, Ethernet1 Spoke2#show ip nhrp 10.0.0.1/32 via
10.0.0.1, Tunnel0 created 01:32:10, never expire Type:
static, Flags: authoritative used NBMA address:
172.17.0.1 Spoke2#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
17 Ethernet0 172.16.2.75 set HMAC_SHA+DES_56_CB 0 0 2070
Tunnel0 10.0.0.3 set HMAC_MD5 0 279 2071 Tunnel0
10.0.0.3 set HMAC_MD5 316 0
```

En este punto hacemos un ping desde la dirección 192.168.1.2 a la dirección 192.168.2.3. Estas direcciones son para host detrás de los routers Spoke1 y Spoke2 respectivamente. La Secuencia de eventos siguiente ocurre para construir el túnel directo del mGRE+IPsec del spoke al spoke.

1. El router Spoke1 recibe el paquete ping con el destino 192.168.2.3. Mira para arriba este destino en la tabla de ruteo y encuentra que necesita remitir a este paquete hacia fuera la interfaz del tunnel0 al nexthop IP, 10.0.0.3.
2. El router Radio1 verifica la tabla de correspondencia NHRP para el destino 10.0.0.3 y encuentra que no hay entrada. El router del Spoke1 crea un paquete de pedidos de la resolución NHRP y lo envía a su NHS (el router de eje de conexión).
3. El router Hub verifica la tabla de mapeo NHRP para el destino 10.0.0.3 y encuentra que corresponde a la dirección 172.16.2.75. El router concentrador crea un paquete de

respuesta con resolución NHRP y lo envía al router Spoke1.

4. El router del Spoke1 recibe la contestación de la resolución NHRP, y ingresa 10.0.0.3 — >172.16.2.75 que asocia en su tabla del mapeo NHRP. Cuando se agrega la correlación de NHRP se activa el IPSec para que inicie un túnel IPsec con el par 172.16.2.75.
5. El router del Spoke1 inicia el ISAKMP con 172.16.2.75 y negocia el ISAKMP y el SA de IPSec. Proxy IPsec se deriva del **comando tunnel source <address> del** tunnel0 y del mapeo NHRP.
   local ident (addr/mask/prot/port): (172.16.1.24/255.255.255.255/47/0) remote ident (addr/mask/prot/port): (172.16.2.75/255.255.255.255/47/0)
6. Una vez que el túnel IPsec ha acabado la construcción, todos los otros paquetes de datos a la subred 192.168.2.0/24 se envían directamente al Spoke2.
7. Después de que un paquete destinado a 192.168.2.3 se haya remitido al host, este host enviará un paquete de devolución a 192.168.1.2. Cuando el router Spoke2 recibe este paquete destinado a 192.168.1.2, buscará este destino en la tabla de ruteo y encontrará que necesita reenviar este paquete hacia afuera por la interfaz Tunnel0 al próximo salto de IP, 10.0.0.2.
8. El router Spoke2 verifica la tabla de mapeo NHRP correspondiente al destino 10.0.0.2 y detecta que no hay una entrada. El router del Spoke2 crea un paquete de pedidos de la resolución NHRP y lo envía a su NHS (el router de eje de conexión).
9. El router de eje de conexión marca su tabla del mapeo NHRP para el destino 10.0.0.2 y encuentra que asocia al direccionamiento 172.16.1.24. El router concentrador crea un paquete de respuesta con resolución NHRP y lo envía al router Spoke2.
10. El router del Spoke2 recibe la contestación de la resolución NHRP, y ingresa 10.0.0.2 — > 172.16.1.24 que asocia en su tabla del mapeo NHRP. El agregado del mapeo NHRP hace que IPsec inicie un túnel IPsec con el par 172.16.1.24, pero como ya existe un túnel IP con el par 172.16.1.24, no se necesita hacer nada más.
11. El Spoke1 y el Spoke2 pueden ahora remitir los paquetes directamente el uno al otro. Cuando no se ha utilizado el mapeo NHRP para reenviar paquetes para la retención del tiempo, aquélla se borrará. La eliminación de la entrada de mapeo NHRP hará que IPsec elimine las SA de IPsec para este link directo.

Condiciones luego de la creación de un link dinámico entre Spoke1 y Spoke2

Información del router Spoke1

```
Spoke1#show ip nhrp 10.0.0.1/32 via 10.0.0.1, Tunnel0
created 02:34:16, never expire Type: static, Flags:
authoritative used NBMA address: 172.17.0.1 10.0.0.3/32
via 10.0.0.3, Tunnel0 created 00:00:05, expire 00:03:35
Type: dynamic, Flags: router unique used NBMA address:
172.16.2.75 Spoke1#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
2 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB 0 0 3
Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB 0 0 2064
Tunnel0 10.0.0.2 set HMAC_MD5 0 375 2065 Tunnel0
10.0.0.2 set HMAC_MD5 426 0 2066 Tunnel0 10.0.0.2 set
HMAC_MD5 0 20 2067 Tunnel0 10.0.0.2 set HMAC_MD5 19 0
```

Información del router Spoke 2

```
Spoke2#show ip nhrp 10.0.0.1/32 via 10.0.0.1, Tunnel0
created 02:18:25, never expire Type: static, Flags:
authoritative used NBMA address: 172.17.0.1 10.0.0.2/32
via 10.0.0.2, Tunnel0 created 00:00:24, expire 00:04:35
Type: dynamic, Flags: router unique used NBMA address:
```

```
172.16.1.24 Spoke2#show crypto engine connection active
ID Interface IP-Address State Algorithm Encrypt Decrypt
17 Ethernet0 172.16.2.75 set HMAC_SHA+DES_56_CB 0 0 18
Ethernet0 172.16.2.75 set HMAC_SHA+DES_56_CB 0 0 2070
Tunnel0 10.0.0.3 set HMAC_MD5 0 407 2071 Tunnel0
10.0.0.3 set HMAC_MD5 460 0 2072 Tunnel0 10.0.0.3 set
HMAC_MD5 0 19 2073 Tunnel0 10.0.0.3 set HMAC_MD5 20 0
```

A partir de la salida anterior, puede ver que el Radio 1 y el Radio 2 han recibido asignaciones NHRP para cada uno del router de eje de conexión, y han construido y utilizado un túnel mGRE+Ipsec. Las correspondencias NHRP caducarán transcurridos cinco minutos (el valor actual de retención de tiempo NHRP = 300 segundos). Si los mapeos NHRP se utilizan dentro de última hora antes de expirar, después una petición y una contestación de la resolución NHRP serán enviadas para restaurar la entrada antes de que se borre. De lo contrario, se eliminará el mapeo NHRP y eso hará que IPSec borre los IPSec SA.

IPSec VPN multipunto dinámico con ejes de conexión dobles

Con algunas líneas de configuración adicionales a los routeres radiales usted puede configurar a los routeres de eje de conexión duales (o múltiplo), para la Redundancia. Hay dos maneras de configurar el Hub dual DMVPN.

- Una sola red DMVPN con cada spoke usando una sola interfaz de túnel GRE de múltiples puntos y señalar a dos diverso Hubs como su Next Hop Server (NHS).Los routers hub sólo tendrán una única interfaz de túnel GRE multipunto.
- Redes duales DMVPN con cada una de las radios con dos interfaces de túnel GRE (punto a punto o multipunto) y cada túnel GRE conectado a un router de eje de conexión diferente.Una vez más los routeres de eje de conexión tendrán solamente una sola interfaz de túnel GRE de múltiples puntos.

Los siguientes ejemplos mirarán que configuran estos dos diversos escenarios para el Hub dual DMVPN. En ambos casos, las diferencias destacadas están relacionadas con la configuración del hub simple para DMVPN.

Eje de conexión dual – Diseño DMPVN simple

El hub doble con una sola disposición de DMVPN es fácilmente configurable, pero no le permite ejercer tanto control sobre el ruteo a través de la DMVPN como el hub doble con doble disposición de DMVPN. La idea en este caso es tener un solo DMVPN “nube” con todo el Hubs (dos en este caso) y todo el spokes conectado con esta subred única (“nube”). Los mapeos estáticos NHRP desde los spokes a los hubs definen los links estáticos IPsec+mGRE sobre los cuáles se ejecutarán los protocolos de ruteo dinámico. El protocolo de ruteo dinámico no se ejecutará en los links dinámicos IPsec+mGRE entre spokes. Puesto que los routeres radiales son vecinos de ruteo con los routeres de eje de conexión sobre la misma interfaz de túnel MGRE, usted no puede utilizar el link ni interconecta las diferencias (como métrico, cueste, retrase, o ancho de banda) para modificar la métrica del Dynamic Routing Protocol para preferir un concentrador sobre el otro concentrador cuando ella es ambas para arriba. Si se necesita esta preferencia, se deben usar las técnicas inherentes a la configuración del protocolo de ruteo. Por este motivo, sería mejor que utilice EIGRP o RIP en lugar de OSPF para el protocolo de ruteo dinámico.

Nota: La cuestión anterior constituye un problema sólo si los routers hubs son ubicados en forma

conjunta. Cuando no están ubicados de manera conjunta, el ruteo dinámico probablemente elija el router de hub apropiado, incluso si la red de destino puede alcanzarse a través de cualquier router hub.

Eje de conexión dual – Diseño DMPVN simple

Router del eje de conexión

```
version 12.3
 !
 hostname Hub1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000 ip address 10.0.0.1 255.255.255.0 ip
mtu 1400 ip nhrp authentication test ip nhrp map
multicast dynamic ip nhrp network-id 100000 ip nhrp
holdtime 600 ip ospf network broadcast ip ospf priority
2 delay 1000 tunnel source Ethernet0 tunnel mode gre
multipoint tunnel key 100000 tunnel protection ipsec
profile vpnprof ! interface Ethernet0 ip address
172.17.0.1 255.255.255.0 ! interface Ethernet1 ip
address 192.168.0.1 255.255.255.0 ! router ospf 1
network 10.0.0.0 0.0.0.255 area 1 network 192.168.0.0
0.0.0.255 area 0 !
```

Router del Hub2

```
version 12.3
 !
 hostname Hub2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 900 ip address 10.0.0.2 255.255.255.0 ip mtu
1400 ip nhrp authentication test ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp map multicast 172.17.0.1 ip nhrp map
multicast dynamic ip nhrp network-id 100000 ip nhrp
holdtime 600 ip nhrp nhs 10.0.0.1 ip ospf network
broadcast ip ospf priority 1 delay 1000 tunnel source
Ethernet0 tunnel mode gre multipoint tunnel key 100000
tunnel protection ipsec profile vpnprof ! interface
Ethernet0 ip address 172.17.0.5 255.255.255.0 !
interface Ethernet1 ip address 192.168.0.2 255.255.255.0
! router ospf 1 network 10.0.0.0 0.0.0.255 area 1
network 192.168.0.0 0.0.0.255 area 0 !
```

El único cambio en la configuración del Hub1 es cambiar el OSPF para utilizar dos áreas. El área 0 se utiliza para la red detrás de los dos ejes de conexión y el área 1 se utiliza para la red DMVPN y las redes detrás de los routers radiales. OSPF podría utilizar una sola área, pero aquí se utilizaron dos áreas para demostrar la configuración para varias áreas OSPF.

La configuración para Hub2 es básicamente la misma que para Hub1 con los correspondientes cambios de dirección IP. La una diferencia principal es que el Hub2 es también un spoke (o cliente) del Hub1, haciendo Hub1 el hub primario y el Hub2 hub secundario. Se hace esto de modo que el Hub2 sea un vecino OSPF con el Hub1 sobre el túnel del mGRE. Como el Hub1 es el OSPF DR, debe tener una conexión directa con los demás routers OSPF por la interfaz mGRE (red NBMA). Sin el link directo entre el Hub1 y el Hub2, el Hub2 no participaría en el OSPF Routing cuando el Hub1 está también para arriba. Cuando Hub1 no funcione, Hub2 será el OSPF DR para DMVPN (red NBMA). Cuando viene el Hub1 salvaguardia, asumirá el control el ser el OSPF DR para el DMVPN.

Los routers detrás del Hub1 y el Hub2 utilizarán el Hub1 para enviar paquetes a las redes spoke porque el ancho de banda para la interfaz de túnel GRE se encuentra configurado para 1000 Kb/seg contra los 900 Kb/seg del Hub2. En contraste, los routers spoke enviarán paquetes para las redes detrás de los routers hub a ambos Hub1 y Hub2, dado que existe una sola interfaz de túnel mGRE en cada router spoke y habrá dos rutas con costos equivalentes. Si se utiliza el equilibrio de carga por paquete, esto puede causar paquetes defectuosos.

Router Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp map multicast 172.17.0.5 ip nhrp map
10.0.0.2 172.17.0.5 ip nhrp network-id 100000 ip nhrp
holdtime 300 ip nhrp nhs 10.0.0.1 ip nhrp nhs 10.0.0.2
ip ospf network broadcast ip ospf priority 0 delay 1000
tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke1 ! interface Ethernet1 ip address 192.168.1.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 1 network 192.168.1.0 0.0.0.255 area 1 !
```

Las diferencias en la configuración de los routers radiales son las siguientes:

- En la nueva configuración, la red radial está configurada con correspondencias NHRP

estáticas para Hub2, y Hub2 es agregado como un servidor del salto siguiente.Original:
ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1 172.17.0.1 ip nhrp nhs 10.0.0.1
Nuevo:
ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1 172.17.0.1 ip nhrp map multicast 172.17.0.5 ip nhrp map 10.0.0.2 172.17.0.5 ip nhrp nhs 10.0.0.1 ip nhrp nhs 10.0.0.2

- Las áreas OSPF en los routers radiales se han cambiado al área 1.

Recuerde que al definir el mapeo NHR P estático y NHS en un router spoke para un concentrador, usted ejecutará el protocolo de ruteo dinámico a través de este túnel. Esto define al ruteo hub y spoke o a la red vecina. Tome en cuenta que el Hub2 es un hub para todos los radios y también es un radio para el Hub1. Esto facilita el diseño, la configuración y la modificación de redes radiales multicapa cuando se utiliza la solución DMVPN.

Router Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.12 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp map multicast 172.17.0.5 ip nhrp map
10.0.0.2 172.17.0.5 ip nhrp network-id 100000 ip nhrp
holdtime 300 ip nhrp nhs 10.0.0.1 ip nhrp nhs 10.0.0.2
ip ospf network broadcast ip ospf priority 0 delay 1000
tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke1 ! interface Ethernet1 ip address 192.168.2.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 0 network 192.168.2.0 0.0.0.255 area 0 !
```

Router del Spoke<n>

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0
  bandwidth 1000
```

```
  ip address 10.0.0.<n+10> 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map multicast 172.17.0.1 ip nhrp map 10.0.0.1
172.17.0.1 ip nhrp map multicast 172.17.0.5 ip nhrp map
10.0.0.2 172.17.0.5 ip nhrp network-id 100000 ip nhrp
holdtime 300 ip nhrp nhs 10.0.0.1 ip nhrp nhs 10.0.0.2
ip ospf network broadcast ip ospf priority 0 delay 1000
tunnel source Ethernet0 tunnel mode gre multipoint
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Ethernet0 ip address dhcp hostname
Spoke<x> ! interface Ethernet1 ip address 192.168.<n>.1
255.255.255.0 ! router ospf 1 network 10.0.0.0 0.0.0.255
area 0 network 192.168.<n>.0 0.0.0.255 area 0 !
```

En este momento, usted puede hechar una ojeada las tablas de ruteo, las tablas del mapeo NHRP, y las conexiones del IPSec en el Routers del Hub1, del Hub2, del Spoke1, y del Spoke2 para ver las Condiciones iniciales (enseguida después del Routers del Spoke1 y del Spoke2 suba).

Cambios y condiciones iniciales

Información del router Hub1

```
Hub1#show ip route 172.17.0.0/24 is subnetted, 1 subnets
C 172.17.0.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 C 192.168.0.0/24 is directly
connected, Ethernet1 O 192.168.1.0/24 [110/2] via
10.0.0.11, 00:02:17, Tunnel0 O 192.168.2.0/24 [110/2]
via 10.0.0.12, 00:02:17, Tunnel0 Hub1#show ip nhrp
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 1w3d, expire
00:03:15 Type: dynamic, Flags: authoritative unique
registered NBMA address: 172.17.0.5 10.0.0.11/32 via
10.0.0.11, Tunnel0 created 1w3d, expire 00:03:49 Type:
dynamic, Flags: authoritative unique registered NBMA
address: 172.16.1.24 10.0.0.12/32 via 10.0.0.12, Tunnel0
created 1w3d, expire 00:04:06 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.2.75 Hub1#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 4
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 5
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 6
Ethernet0 172.17.0.1 set HMAC_SHA+DES_56_CB 0 0 3532
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 232 3533
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 212 0 3534
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 18 3535
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 17 0 3536
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 7 3537 Tunnel0
10.0.0.1 set HMAC_MD5+DES_56_CB 7 0
```

Información del router Hub2

```
Hub2#show ip route 172.17.0.0/24 is subnetted, 1 subnets
C 172.17.0.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 C 192.168.0.0/24 is directly
connected, Ethernet1 O 192.168.1.0/24 [110/2] via
10.0.0.11, 00:29:15, Tunnel0 O 192.168.2.0/24 [110/2]
via 10.0.0.12, 00:29:15, Tunnel0 Hub2#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 1w3d, never
expire Type: static, Flags: authoritative used NBMA
address: 172.17.0.1 10.0.0.11/32 via 10.0.0.11, Tunnel0
```

```
created 1w3d, expire 00:03:15 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.1.24 10.0.0.12/32 via 10.0.0.12, Tunnel0 created
00:46:17, expire 00:03:51 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.2.75 Hub2#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 4
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 5
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 6
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 3520
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 0 351 3521
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 326 0 3522
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 0 311 3523
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 339 0 3524
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 0 25 3525
Tunnel0 10.0.0.2 set HMAC_MD5+DES_56_CB 22 0
```

Información del router Spoke1

```
Spoke1#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.1.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 O IA 192.168.0.0/24 [110/11]
via 10.0.0.1, 00:39:31, Tunnel0 [110/11] via 10.0.0.2,
00:39:31, Tunnel0 C 192.168.1.0/24 is directly
connected, Ethernet1 O 192.168.2.0/24 [110/2] via
10.0.0.12, 00:37:58, Tunnel0 Spoke1#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 00:56:40,
never expire Type: static, Flags: authoritative used
NBMA address: 172.17.0.1 10.0.0.2/32 via 10.0.0.2,
Tunnel0 created 00:56:40, never expire Type: static,
Flags: authoritative used NBMA address: 172.17.0.5
Spoke1#show crypto engine connection active ID Interface
IP-Address State Algorithm Encrypt Decrypt 1 Ethernet0
172.16.1.24 set HMAC_SHA+DES_56_CB 0 0 2 Ethernet0
172.16.1.24 set HMAC_SHA+DES_56_CB 0 0 2010 Tunnel0
10.0.0.11 set HMAC_MD5+DES_56_CB 0 171 2011 Tunnel0
10.0.0.11 set HMAC_MD5+DES_56_CB 185 0 2012 Tunnel0
10.0.0.11 set HMAC_MD5+DES_56_CB 0 12 2013 Tunnel0
10.0.0.11 set HMAC_MD5+DES_56_CB 13 0
```

Información del router Spoke 2

```
Spoke2#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.2.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 O IA 192.168.0.0/24 [110/11]
via 10.0.0.1, 00:57:56, Tunnel0 [110/11] via 10.0.0.2,
00:57:56, Tunnel0 O 192.168.1.0/24 [110/2] via
10.0.0.11, 00:56:14, Tunnel0 C 192.168.2.0/24 is
directly connected, Ethernet1 Spoke2#show ip nhrp
10.0.0.1/32 via 10.0.0.1, Tunnel0 created 5w6d, never
expire Type: static, Flags: authoritative used NBMA
address: 172.17.0.1 10.0.0.2/32 via 10.0.0.2, Tunnel0
created 6w6d, never expire Type: static, Flags:
authoritative used NBMA address: 172.17.0.5 Spoke2#show
crypto engine connection active ID Interface IP-Address
State Algorithm Encrypt Decrypt 2 Ethernet0 172.16.2.75
set HMAC_SHA+DES_56_CB 0 0 3 Ethernet0 172.16.2.75 set
HMAC_SHA+DES_56_CB 0 0 3712 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 0 302 3713 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 331 0 3716 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 0 216 3717 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 236 0
```

Se deben considerar varios temas interesantes con respecto a las tablas de ruteo en Hub1, Hub2, Spoke1 y Spoke2:

- Ambos routers de eje de conexión tienen rutas de costo equivalentes a las redes detrás de los routers radiales.Hub1:`O 192.168.1.0/24 [110/2] via 10.0.0.11, 00:02:17, Tunnel0`
  `O 192.168.2.0/24 [110/2] via 10.0.0.12, 00:02:17, Tunnel0`Hub2:`O 192.168.1.0/24 [110/2] via 10.0.0.11, 00:29:15, Tunnel0`
  `O 192.168.2.0/24 [110/2] via 10.0.0.12, 00:29:15, Tunnel0`Esto significa que Hub1 y Hub2 promocionarán el mismo costo para las redes detrás de los routers spoke hacia los routers en las redes detrás de los routers hub. Por ejemplo, la tabla de ruteo en un router, R2, que está conectado directamente a la LAN 192.168.0.0/24, sería de la siguiente manera:R2:`O IA 192.168.1.0/24 [110/12] via 192.168.0.1, 00:00:26, Ethernet1/0/3`
  `[110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/3O`
  `O IA 192.168.2.0/24 [110/12] via 192.168.0.1, 00:00:27, Ethernet1/0/3`
  `[110/12] via 192.168.0.2, 00:00:27, Ethernet1/0/3`
- Los routers radiales tienen rutas de costo equivalente por medio de ambos routers hub a la red debajo de los routers hub.Spoke1:`O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:39:31, Tunnel0`
  `[110/11] via 10.0.0.2, 00:39:31, Tunnel0`Spoke2`O IA 192.168.0.0/24 [110/11] via 10.0.0.1, 00:57:56, Tunnel0`
  `[110/11] via 10.0.0.2, 00:57:56, Tunnel0`Si los routers spoke realizan un equilibrio de carga por paquete, entonces usted podría obtener paquetes fuera de servicio.

Para evitar hacer un ruteo asimétrico o equilibrio de carga por paquete entre los links de los dos ejes de conexión, debe configurar el protocolo de ruteo con preferencia de un trayecto de radio a eje de conexión en ambas direcciones. Si quiere que el Hub1 sea el principal y el Hub 2 el de respaldo, puede configurar el costo de OSPF en las interfaces del túnel del hub para que sean diferentes.

Hub1:

```
interface tunnel0
...
ip ospf cost 10
...
```

Hub2:

```
interface tunnel0
...
ip ospf cost 20
...
```

Ahora la rutas se ven de la siguiente manera:

Hub1:

```
O     192.168.1.0/24 [110/11] via 10.0.0.11, 00:00:28, Tunnel0
O     192.168.2.0/24 [110/11] via 10.0.0.12, 00:00:28, Tunnel0
```

Hub2:

```
O     192.168.1.0/24 [110/21] via 10.0.0.11, 00:00:52, Tunnel0
O     192.168.2.0/24 [110/21] via 10.0.0.12, 00:00:52, Tunnel0
```

R2:

```
O     IA 192.168.1.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
O     IA 192.168.2.0/24 [110/31] via 192.168.0.1, 00:01:06, Ethernet1/0/3
```

Los dos routers hub ahora presentan diferentes costos en las rutas para las redes detrás de los routers spoke. Esto significa que el Hub1 será preferido para el tráfico de reenvío a los routeres radiales, como puede ser visto en el r2 del router. Esto tomará el cuidado del problema del Asymmetric Routing descrito en el primer punto negro arriba.

El ruteo asimétrico en la otra dirección, tal como se describió arriba en la segunda viñeta, aún permanece allá. Cuando se utiliza OSPF como protocolo de ruteo dinámico, puede resolverse el problema por medio de una solución alternativa: mediante el uso del comando distance... en el router ospf 1 en las spokes para preferir rutas adquiridas a través del Hub 1 en vez de las rutas adquiridas a través del Hub 2.

Spoke1:

```
router ospf 1
 distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

Spoke2

```
router ospf 1
 distance 111 10.0.0.2 0.0.0.0 1
access-list 1 permit any
```

Ahora la rutas se ven de la siguiente manera:

Spoke1:

```
O     192.168.0.0/24 [110/11] via 10.0.0.1, 00:00:06, Tunnel0
```

Spoke2

```
O     192.168.1.0/24 [110/11] via 10.0.0.1, 00:00:10, Tunnel0
```

La configuración del ruteo anterior brindará protección contra el ruteo asimétrico y, al mismo tiempo, admitirá las fallas a Hub2 si Hub1 deja de funcionar. Significa que cuando los dos ejes de conexión están activos, sólo se utiliza el Hub1. Si desea usar ambos ejes de conexión equilibrando los radios en los ejes de conexión, con protección contra fallas y sin ruteo asimétrico, entonces la configuración de ruteo puede ser compleja, especialmente si se usa OSPF. Por este motivo, la siguiente configuración de eje de conexión dual con DMVPN dual puede ser una mejor opción.

‘Hub dual – Esquema DMPVN dual’

El hub dual con un diseño dual DMVPN es apenas más difícil de configurar, pero le brinda un mejor control del ruteo a través de DMVPN. La idea es tener dos DMVPN separado “nubes”. Cada eje de conexión (dos en este caso) está conectado a una subred DMVPN (“nube”) y los radios están conectados a ambas subredes (“nubes”). Dado que los routers spoke son vecinos de ruteo de ambos routers hub en las dos interfaces de túnel GRE, puede usar diferencias en la configuración de la interfaz (como ancho de banda, costo y retraso) para modificar las métricas del protocolo de ruteo dinámico de modo que prefiera un hub sobre el otro hub cuando ambos estén activos.

Nota: El problema anterior, por lo general, sólo es relevante si los routers hub son ubicados de forma conjunta. Cuando no están ubicados de manera conjunta, el ruteo dinámico probablemente elija el router de hub apropiado, incluso si la red de destino puede alcanzarse a través de cualquier router hub.

Puede usar las interfaces de túnel p-pGRE o mGRE en los routers radiales. El múltiplo p-pGRE interconecta en un router radial puede utilizar la misma dirección IP del **origen de túnel…**, pero las interfaces múltiples del mGRE en un router radial deben tener una dirección IP de la **fuente del** túnel único**…**. Esto es porque cuando se inicia IPsec, el primer paquete es un paquete ISAKMP que necesita asociarse con uno de los túneles mGRE. El paquete ISAKMP sólo tiene la dirección IP de destino (dirección de entidad par IPsec remoto) con la que realiza esta asociación. Esta dirección se compara con la dirección … de origen de túnel, pero dado que ambos túneles poseen la misma dirección … de origen de túnel, la primera interfaz de túnel mGRE siempre coincide. Quiere decir que los paquetes de datos entrantes de multidifusión pueden estar asociados con la interfaz mGRE equivocada, lo que rompe el protocolo de ruteo dinámico.

Los paquetes GRE en sí mismos no tienen este problema, ya que tienen el valor ... de clave de túnel para diferenciar las dos interfaces mGRE. Comenzando en los Cisco IOS Software Releases 12.3(5) y 12.3(7)T, un parámetro adicional fue introducido para superar esta limitación: **protección del túnel….compartido**. La palabra clave **compartida** indica que las interfaces del mGRE del mutiple utilizarán la encripción de IPSec con la misma dirección IP de origen. Si usted tiene una versión anterior usted puede utilizar p-pGRE los túneles en este Hub dual con el Diseño DMVPN dual. En el caso del túnel p-pGRE, tanto las direcciones IP de origen del túnel... como las de destino del túnel... Pueden utilizarse para la correspondencia. Por este ejemplo p-pGRE hace un túnel será utilizado en este Hub dual con el Diseño DMVPN dual y no utilizar al calificador **compartido**.

'Hub dual – Esquema DMPVN dual'

Los siguientes cambios resaltados están relacionados con las configuraciones dinámicas multipunto de red radial, ilustradas anteriormente en este documento.

Router Hub1

```
version 12.3
 !
 hostname Hub1 ! crypto isakmp policy 1 authentication
pre-share crypto isakmp key cisco47 address 0.0.0.0
0.0.0.0 ! crypto ipsec transform-set trans2 esp-des esp-
md5-hmac mode transport ! crypto ipsec profile vpnprof
set transform-set trans2 ! interface Tunnel0 bandwidth
1000 ip address 10.0.0.1 255.255.255.0 ip mtu 1400 ip
nhrp authentication test ip nhrp map multicast dynamic
ip nhrp network-id 100000 ip nhrp holdtime 600 no ip
split-horizon eigrp 1 delay 1000 tunnel source Ethernet0
tunnel mode gre multipoint tunnel key 100000 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
ip address 172.17.0.1 255.255.255.252 ! interface
Ethernet1 ip address 192.168.0.1 255.255.255.0 ! router
eigrp 1 network 10.0.0.0 0.0.0.255 network 192.168.0.0
0.0.0.255 no auto-summary !
```

Router del Hub2

```
version 12.3
 !
 hostname Hub2 ! crypto isakmp policy 1 authentication
pre-share crypto isakmp key cisco47 address 0.0.0.0
0.0.0.0 ! crypto ipsec transform-set trans2 esp-des esp-
md5-hmac mode transport ! crypto ipsec profile vpnprof
set transform-set trans2 ! interface Tunnel0 bandwidth
1000 ip address 10.0.1.1 255.255.255.0 ip mtu 1400 ip
nhrp authentication test ip nhrp map multicast dynamic
ip nhrp network-id 100001 ip nhrp holdtime 600 no ip
split-horizon eigrp 1 delay 1000 tunnel source Ethernet0
tunnel mode gre multipoint tunnel key 100001 tunnel
```

```
protection ipsec profile vpnprof ! interface Ethernet0
ip address 172.17.0.5 255.255.255.252 ! interface
Ethernet1 ip address 192.168.0.2 255.255.255.0 ! router
eigrp 1 network 10.0.1.0 0.0.0.255 network 192.168.0.0
0.0.0.255 no auto-summary !
```

En este caso, las configuraciones del Hub1 y del Hub2 son similares. La diferencia principal es que cada uno es el concentrador de un diverso DMVPN. Cada DMVPN utiliza un diferente:

- Subred IP (10.0.0.0/24, 10.0.0.1/24)
- Id de la red NHRP (100000, 100001)
- Clave de túnel (100000, 100001)

El protocolo de ruteo dinámico ha sido conmutado de OSPF a EIGRP, porque es más fácil configurar y administrar una red NBMA usando EIGRP, como se describe más adelante en este documento.

Router Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0 bandwidth 1000 ip address 10.0.0.11
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000
ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000
tunnel source Ethernet0 tunnel destination 172.17.0.1
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Tunnel1 bandwidth 1000 ip address
10.0.1.11 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.1.1 172.17.0.5 ip
nhrp network-id 100001 ip nhrp holdtime 300 ip nhrp nhs
10.0.1.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.5 tunnel key 100001 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
ip address dhcp hostname Spoke1 ! interface Ethernet1 ip
address 192.168.1.1 255.255.255.0 ! router eigrp 1
network 10.0.0.0 0.0.0.255 network 10.0.1.0 0.0.0.255
network 192.168.1.0 0.0.0.255 no auto-summary !
```

Cada uno de los routers spoke está configurado con dos interfaces de túnel p-pGRE, una en cada uno de los dos DMVPN. Los valores dirección ip ..., id de red nhrp ip ..., clave de túnel ... y destino de túnel ... se emplean para diferenciar los dos túneles. El protocolo de ruteo dinámico, EIGRP, se ejecuta sobre subredes de túnel p-pGRE y se utiliza para seleccionar una interfaz p-pGRE (DMVPN) sobre la otra.

Router Spoke2

```
version 12.3
 !
```

```
 hostname Spoke2
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0 bandwidth 1000 ip address 10.0.0.12
255.255.255.0 ip mtu 1400 ip nhrp authentication test ip
nhrp map 10.0.0.1 172.17.0.1 ip nhrp network-id 100000
ip nhrp holdtime 300 ip nhrp nhs 10.0.0.1 delay 1000
tunnel source Ethernet0 tunnel destination 172.17.0.1
tunnel key 100000 tunnel protection ipsec profile
vpnprof ! interface Tunnel1 bandwidth 1000 ip address
10.0.1.12 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.1.1 172.17.0.5 ip
nhrp network-id 100001 ip nhrp holdtime 300 ip nhrp nhs
10.0.1.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.5 tunnel key 100001 tunnel
protection ipsec profile vpnprof ! interface Ethernet0
ip address dhcp hostname Spoke2 ! interface Ethernet1 ip
address 192.168.2.1 255.255.255.0 ! router eigrp 1
network 10.0.0.0 0.0.0.255 network 10.0.1.0 0.0.0.255
network 192.168.2.0 0.0.0.255 no auto-summary !
```

Router del Spoke<n>

```
version 12.3
 !
 hostname Spoke<n>
 !
 crypto isakmp policy 1
  authentication pre-share
 crypto isakmp key cisco47 address 0.0.0.0 0.0.0.0
 !
 crypto ipsec transform-set trans2 esp-des esp-md5-hmac
  mode transport
 !
 crypto ipsec profile vpnprof
  set transform-set trans2
 !
 interface Tunnel0 bandwidth 1000 ip address
10.0.0.<n+10> 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.0.1 172.17.0.1 ip
nhrp network-id 100000 ip nhrp holdtime 300 ip nhrp nhs
10.0.0.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.1 tunnel key 100000 tunnel
protection ipsec profile vpnprof ! interface Tunnel1
bandwidth 1000 ip address 10.0.1.<n+10> 255.255.255.0 ip
mtu 1400 ip nhrp authentication test ip nhrp map
10.0.1.1 172.17.0.5 ip nhrp network-id 100001 ip nhrp
holdtime 300 ip nhrp nhs 10.0.1.1 delay 1000 tunnel
source Ethernet0 tunnel destination 172.17.0.5 tunnel
key 100001 tunnel protection ipsec profile vpnprof !
interface Ethernet0 ip address dhcp hostname Spoke<x> !
interface Ethernet1 ip address 192.168.<n>.1
255.255.255.0 ! router eigrp 1 network 10.0.0.0
0.0.0.255 network 10.0.1.0 0.0.0.255 network
192.168.<n>.0 0.0.0.255 no auto-summary !
```

En este momento, hechemos una ojeada las tablas de ruteo, las tablas del mapeo NHRP, y las conexiones del IPSec en el Routers del Hub1, del Hub2, del Spoke1 y del Spoke2 para ver las Condiciones iniciales (enseguida después del Routers del Spoke1 y del Spoke2 suba).

Cambios y condiciones iniciales

Información del router Hub1

```
Hub1#show ip route 172.17.0.0/30 is subnetted, 1 subnets
C 172.17.0.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets C 10.0.0.0 is
directly connected, Tunnel0 D 10.0.1.0 [90/2611200] via
192.168.0.2, 00:00:46, Ethernet1 C 192.168.0.0/24 is
directly connected, Ethernet1 D 192.168.1.0/24
[90/2841600] via 10.0.0.11, 00:00:59, Tunnel0 D
192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:00:34,
Tunnel0 Hub1#show ip nhrp 10.0.0.12/32 via 10.0.0.12,
Tunnel0 created 23:48:32, expire 00:03:50 Type: dynamic,
Flags: authoritative unique registered NBMA address:
172.16.2.75 10.0.0.11/32 via 10.0.0.11, Tunnel0 created
23:16:46, expire 00:04:45 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.1.24 Hub1#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 15
Ethernet0 172.17.63.18 set HMAC_SHA+DES_56_CB 0 0 16
Ethernet0 10.0.0.1 set HMAC_SHA+DES_56_CB 0 0 2038
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 759 2039
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 726 0 2040
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 0 37 2041
Tunnel0 10.0.0.1 set HMAC_MD5+DES_56_CB 36 0
```

Información del router Hub2

```
Hub2#show ip route 172.17.0.0/30 is subnetted, 1 subnets
C 172.17.0.4 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets D 10.0.0.0
[90/2611200] via 192.168.0.1, 00:12:22, Ethernet1 C
10.0.1.0 is directly connected, Tunnel0 C 192.168.0.0/24
is directly connected, Ethernet1 D 192.168.1.0/24
[90/2841600] via 10.0.1.11, 00:13:24, Tunnel0 D
192.168.2.0/24 [90/2841600] via 10.0.1.12, 00:12:11,
Tunnel0 Hub2#show ip nhrp 10.0.1.12/32 via 10.0.1.12,
Tunnel3 created 06:03:24, expire 00:04:39 Type: dynamic,
Flags: authoritative unique registered NBMA address:
172.16.2.75 10.0.1.11/32 via 10.0.1.11, Tunnel3 created
23:06:47, expire 00:04:54 Type: dynamic, Flags:
authoritative unique registered NBMA address:
172.16.1.24 Hub2#show crypto engine connection active ID
Interface IP-Address State Algorithm Encrypt Decrypt 4
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 6
Ethernet0 171.17.0.5 set HMAC_SHA+DES_56_CB 0 0 2098
Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 0 722 2099
Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 690 0 2100
Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 0 268 2101
Tunnel0 10.0.1.1 set HMAC_MD5+DES_56_CB 254 0
```

Información del router Spoke1

```
Spoke1#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.1.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 1 subnets C 10.0.0.0 is
directly connected, Tunnel0 C 10.0.1.0 is directly
connected, Tunnel1 D 192.168.0.0/24 [90/2841600] via
10.0.1.1, 00:26:30, Tunnel1 [90/2841600] via 10.0.0.1,
```

```
00:26:30, Tunnel0 C 192.168.1.0/24 is directly
connected, Ethernet1 D 192.168.2.0/24 [90/3097600] via
10.0.1.1, 00:26:29, Tunnel1 [90/3097600] via 10.0.0.1,
00:26:29, Tunnel0 Spoke1#show ip nhrp 10.0.0.1/32 via
10.0.0.1, Tunnel0 created 23:25:46, never expire Type:
static, Flags: authoritative NBMA address: 172.17.0.1
10.0.1.1/32 via 10.0.1.1, Tunnel1 created 23:24:40,
never expire Type: static, Flags: authoritative NBMA
address: 172.17.0.5 Spoke1#show crypto engine connection
active ID Interface IP-Address State Algorithm Encrypt
Decrypt 16 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB
0 0 18 Ethernet0 172.16.1.24 set HMAC_SHA+DES_56_CB 0 0
2118 Tunnel0 10.0.0.11 set HMAC_MD5+DES_56_CB 0 181 2119
Tunnel0 10.0.0.11 set HMAC_MD5+DES_56_CB 186 0 2120
Tunnel1 10.0.1.11 set HMAC_MD5+DES_56_CB 0 105 2121
Tunnel1 10.0.1.11 set HMAC_MD5+DES_56_CB 110 0
```

Información del router Spoke 2

```
Spoke2#show ip route 172.16.0.0/24 is subnetted, 1
subnets C 172.16.2.0 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets C 10.0.0.0 is
directly connected, Tunnel0 C 10.0.1.0 is directly
connected, Tunnel1 D 192.168.0.0/24 [90/2841600] via
10.0.1.1, 00:38:04, Tunnel1 [90/2841600] via 10.0.0.1,
00:38:04, Tunnel0 D 192.168.1.0/24 [90/3097600] via
10.0.1.1, 00:38:02, Tunnel1 [90/3097600] via 10.0.0.1,
00:38:02, Tunnel0 C 192.168.2.0/24 is directly
connected, Ethernet1 Spoke2#show ip nhrp 10.0.0.1/32 via
10.0.0.1, Tunnel0 created 1d02h, never expire Type:
static, Flags: authoritative used NBMA address:
172.17.0.1 10.0.1.1/32 via 10.0.1.1, Tunnel1 created
1d02h, never expire Type: static, Flags: authoritative
used NBMA address: 172.17.0.5 Spoke2#show crypto engine
connection active ID Interface IP-Address State
Algorithm Encrypt Decrypt 8 Ethernet0 172.16.2.75 set
HMAC_SHA+DES_56_CB 0 0 9 Ethernet0 172.16.2.75 set
HMAC_SHA+DES_56_CB 0 0 2036 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 0 585 2037 Tunnel0 10.0.0.12 set
HMAC_MD5+DES_56_CB 614 0 2038 Tunnel1 10.0.1.12 set
HMAC_MD5+DES_56_CB 0 408 2039 Tunnel1 10.0.1.12 set
HMAC_MD5+DES_56_CB 424 0
```

De nuevo, hay varios puntos interesantes que deben tenerse en cuenta acerca de las tablas de ruteo en el Hub1, Hub2, Spoke1 y Spoke2:

- Ambos routers de eje de conexión tienen rutas de costo equivalentes a las redes detrás de los routers radiales.Hub1:`D 192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:00:59, Tunnel0`
  `D 192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:00:34, Tunnel0`Hub2:`D 192.168.1.0/24 [90/2841600] via 10.0.1.11, 00:13:24, Tunnel0`
  `D 192.168.2.0/24 [90/2841600] via 10.0.1.12, 00:12:11, Tunnel0`Esto significa que Hub1 y Hub2 promocionarán el mismo costo para las redes detrás de los routers spoke hacia los routers en las redes detrás de los routers hub. Por ejemplo, la tabla de ruteo en un router, R2, que está conectado directamente a la LAN 192.168.0.0/24, sería de la siguiente manera:R2:
```
D 192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:51:51, Ethernet1/0/3
                              [90/2867200] via 192.168.0.2, 00:51:51, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:52:43, Ethernet1/0/3
                    [90/2867200] via 192.168.0.1, 00:52:43, Ethernet1/0/3
```
- Los routers radiales tienen rutas de costo equivalente por medio de ambos routers hub a la red debajo de los routers hub.Spoke1:`D 192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:26:30, Tunnel1`

```
                            [90/3097600] via 10.0.0.1, 00:26:30, Tunnel0Spoke2D
    192.168.0.0/24 [90/3097600] via 10.0.1.1, 00:38:04, Tunnel1
                            [90/3097600] via 10.0.0.1, 00:38:04, Tunnel0
```

Si los routeres radiales están haciendo el equilibrio de carga por paquete, después usted podría conseguir los paquetes defectuosos.

Para evitar hacer un ruteo asimétrico o equilibrio de carga por paquete entre los links de los dos ejes de conexión, debe configurar el protocolo de ruteo con preferencia de un trayecto de radio a eje de conexión en ambas direcciones. Si usted quisiera que el Hub1 fuera el primario y Hub2 a ser el respaldo, después usted puede fijar el retardo en las interfaces del túnel del concentrador para ser diferente.

Hub1:

```
interface tunnel0
...
delay 1000
...
```

Hub2:

```
interface tunnel0
...
delay 1050
...
```

Nota: En este ejemplo, se agregaron 50 al retraso en la interfaz del túnel en el Hub2 ya que es menor al retraso en la interfaz Ethernet1 entre los dos hubs (100). Al hacer esto, el Eje de conexión 2 aún reenviará paquetes directamente a los routers radiales, pero anunciará una ruta menos deseable que el Eje de conexión 1 a los routers detrás del Eje de conexión 1 y el Eje de conexión 2. Si el retardo fuera aumentado en más de 100, después el Hub2 remitiría los paquetes para los routeres radiales con el Hub1 vía la interfaz del Ethernet1, aunque el Routers detrás del Hub1 y del Hub2 sin embargo preferiría correctamente Hub-1 para enviar los paquetes a los routeres radiales.

Ahora la rutas se ven de la siguiente manera:

Hub1:

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:01:11, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.0.0.12, 00:01:11, Tunnel0
```

Hub2:

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:00:04, Tunnel0
D    192.168.2.0/24 [90/2854400] via 10.0.1.12, 00:00:04, Tunnel0
```

R2:

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.1, 00:02:18, Ethernet1/0/3
```

Los dos routers de eje de conexión tienen diferentes costos para los routers de la red detrás de los routers radiales; por lo tanto, en este caso, Hub1 será el preferido para reenviar el tráfico a los routers radiales, como se puede observar en R2. Esto toma el cuidado del problema descrito en el primer punto negro arriba.

El problema descrito en el segundo punto mencionado aún existe pero, como usted cuenta con dos interfaces de túnel, puede fijar el retardo ... en las interfaces de túnel separadamente para cambiar la métrica EIGRP para las rutas aprendidas desde Hub1 versus Hub 2.

Spoke1:

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

Spoke2

```
interface tunnel0
  delay 1000
interface tunnel1
  delay 1050
```

Ahora la rutas se ven de la siguiente manera:

Spoke1:

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:15:44, Tunnel0
D    192.168.2.0/24 [90/3097600] via 10.0.0.1, 00:15:44, Tunnel0
```

Spoke2

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:13:54, Tunnel0
D    192.168.1.0/24 [90/3097600] via 10.0.0.1, 00:13:54, Tunnel0
```

La configuración del ruteo anterior brindará protección contra el ruteo asimétrico y, al mismo tiempo, admitirá las fallas a Hub2 si Hub1 deja de funcionar. Significa que cuando los dos ejes de conexión están activos, sólo se utiliza el Hub1.

Si usted quiere utilizar ambo Hubs equilibrando el spokes a través del Hubs, con la protección contra fallas y ningún Asymmetric Routing, después la configuración de ruteo es más compleja, pero usted puede hacerla al usar el EIGRP. Para lograr esto, fije el **retardo…** en las interfaces del túnel de los routeres de eje de conexión de nuevo a ser igual y después utilice el **comando offset-list <acl> out <offset> <interface>** en los routeres radiales de aumentar el EIGRP métrico para las rutas hizo publicidad hacia fuera de las interfaces de túnel GRE al hub de backup. El retraso desigual ... entre las interfaces Tunnel0 y Tunnel1 del spoke aún se usa, por lo que el router spoke preferirá su router hub primario. Los cambios en los routers spoke son los siguientes.

Router Spoke1

```
version 12.3
 !
 hostname Spoke1
 !
 ...
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.11 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1000 tunnel source Ethernet0 tunnel destination
172.17.0.1 tunnel key 100000 tunnel protection ipsec
profile vpnprof ! interface Tunnel1 bandwidth 1000 ip
address 10.0.1.11 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.1.1 172.17.0.5 ip
nhrp network-id 100001 ip nhrp holdtime 300 ip nhrp nhs
10.0.1.1 delay 1500 tunnel source Ethernet0 tunnel
```

```
destination 172.17.0.5 tunnel key 100001 tunnel
protection ipsec profile vpnprof ! ... ! router eigrp 1
offset-list 1 out 12800 Tunnel1 network 10.0.0.0
0.0.0.255 network 10.0.1.0 0.0.0.255 network 192.168.1.0
distribute-list 1 out no auto-summary ! access-list 1
permit 192.168.1.0 !
```

Router Spoke2

```
version 12.3
 !
 hostname Spoke2
 !
 ...
 !
 interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.12 255.255.255.0
  ip mtu 1400
  ip nhrp authentication test
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp network-id 100000
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.0.1
  delay 1500 tunnel source Ethernet0 tunnel destination
172.17.0.1 tunnel key 100000 tunnel protection ipsec
profile vpnprof ! interface Tunnel1 bandwidth 1000 ip
address 10.0.1.12 255.255.255.0 ip mtu 1400 ip nhrp
authentication test ip nhrp map 10.0.1.1 172.17.0.5 ip
nhrp network-id 100001 ip nhrp holdtime 300 ip nhrp nhs
10.0.1.1 delay 1000 tunnel source Ethernet0 tunnel
destination 172.17.0.5 tunnel key 100001 tunnel
protection ipsec profile vpnprof ! ... ! router eigrp 1
offset-list 1 out 12800 Tunnel1 network 10.0.0.0
0.0.0.255 network 10.0.1.0 0.0.0.255 network 192.168.2.0
distribute-list 1 out no auto-summary ! access-list 1
permit 192.168.2.0 !
```

Nota: El valor de desplazamiento de 12800 (50*256) fue agregado al EIGRP métrico porque es más pequeño de 25600 (100*256). Este valor (25600) es lo que se le agrega a la métrica EIGRP para rutas aprendidas entre los routers hub. Usando 12800 en el **comando offset-list**, el router del hub de backup remitirá los paquetes directamente a los routeres radiales, bastante que remitiendo estos paquetes vía los Ethernetes para pasar a través del router del hub primario para eso spokes. La métrica en las rutas notificadas por los routers de eje de conexión será aún de tal manera que el router de eje de conexión principal correcto la preferirá. Recuerde que la mitad de los radios tienen al Eje 1 como su router principal y la otra mitad al Eje 2 como su router principal.

Nota: Si el valor de desplazamiento se incrementó en más de 25600 (100*256), los concentradores retransmitirán paquetes por la mitad de los routers radiales a través del otro concentrador, por medio de la interfaz Ethernet1, aun cuando los routers que están detrás de los concentradores preferirían el concentrador correcto para el envío de paquetes a los routers radiales.

Nota: También se agregó el comando distribute-list 1 out ya que es posible que las rutas aprendidas desde un router hub a través de una interfaz de túnel en un spoke, se anuncien al otro hub a través del otro túnel. El comando distribute-list... asegura que el router radial sólo puede anunciar sus propias reglas.

Nota: Si usted prefiere controlar los anuncios de la encaminamiento en los routeres de eje de conexión bastante que en los routeres radiales, después los **comandos offset-list <acl1> in**

<value> <interface> y distribute-list <acl2> in pueden ser configurados en los routeres de eje de conexión en vez en del spokes. <acl2> la lista de acceso enumeraría las rutas de detrás todo el spokes y <acl1> la lista de acceso enumeraría solamente las rutas de detrás el spokes donde está ser otro router de eje de conexión el hub primario.

Con estos cambios las rutas parecen el siguiente:

Hub1:

```
D    192.168.1.0/24 [90/2841600] via 10.0.0.11, 00:12:11, Tunnel2
D    192.168.2.0/24 [90/2854400] via 10.0.0.12, 00:13:24, Tunnel2
```

Hub2:

```
D    192.168.1.0/24 [90/2854400] via 10.0.1.11, 00:09:58, Tunnel0
D    192.168.2.0/24 [90/2841600] via 10.10.1.12, 00:11:11, Tunnel0
```

R2:

```
D    192.168.1.0/24 [90/2867200] via 192.168.0.1, 00:13:13, Ethernet1/0/3
D    192.168.2.0/24 [90/2867200] via 192.168.0.2, 00:14:25, Ethernet1/0/3
```

Spoke1:

```
D    192.168.0.0/24 [90/2841600] via 10.0.0.1, 00:16:12, Tunnel0
```

Spoke2

```
D    192.168.0.0/24 [90/2841600] via 10.0.1.1, 00:18:54, Tunnel1
```

Conclusión

La solución DMVPN proporciona las funciones siguientes para escalar mejor las redes grandes y pequeñas del IPSec VPN.

- El DMVPN permite un mejor escalamiento en la interconexión total o en el IPSec VPN de la Interconexión parcial.Es especialmente útil cuando el tráfico del spoke al spoke es esporádico (por ejemplo, cada spoke no está enviando constantemente los datos a cada otro spoke). Permite cualquier habló para enviar los datos directamente a cualquier otro spoke, al igual que hay conectividad IP directa entre el spokes.
- Nodos del IPSec de los soportes DMVPN con los direccionamientos dinámicamente asignados (tales como cable, ISDN, y DSL).Esto se aplica tanto a hub y spoke como a redes de interconexión. Es posible que DMVPN requiera el link eje de conexión a radio para estar activo constantemente.
- DMVPN simplifica la incorporación de nodos VPN.Cuando agregue un nuevo router radial, sólo tiene que configurar el router radial y conectarlo a la red (aunque, es posible que necesite agregar la información de la autorización ISAKMP para la nueva radio en el eje de conexión). El concentrador aprenderá dinámicamente sobre el nuevo spoke y el Dynamic Routing Protocol propagará la encaminamiento al concentrador y al resto del spokes.
- El DMVPN reduce el tamaño de la configuración necesaria en todo el Routers en el VPN.Este también es el caso para las redes VPN GRE+IPsec hub y spoke solamente.
- DMVPN utiliza GRE y, por lo tanto, admite el tráfico de ruteo dinámico y de multidifusión de IP en la VPN.Esto significa que un Dynamic Routing Protocol puede ser utilizado, y el “Hubs redundante” se puede soportar por el protocolo. También se admiten las aplicaciones de multidifusión.

- DMVPN admite la tunelización dividida en los radios.

Información Relacionada

- Dynamic Multipoint VPN (DMVPN)
- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems