Migración de FlexVPN: Movimiento duro del DMVPN a FlexVPN en los mismos dispositivos

Contenido

Introducción

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

Las configuraciones de ambos marcos coexistirán en los dispositivos.

En este documento solamente se muestra la mayoría del escenario frecuente: DMVPN usando la clave previamente compartida para la autenticación y EIGRP como Routing Protocol.

Este documento demuestra la migración a BGP (Routing Protocol recomendado) y al EIGRP menos deseable.

prerrequisitos

Requisitos

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

Componentes Utilizados

Observe que no todos los soportes de software y de hardware IKEv2. Refiera al Cisco Feature Navigator para la información. Idealmente, las versiones de software que se utilizarán son:

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

Entre las ventajas de una más nuevos plataforma y software es la posibilidad de usar la criptografía de la última generación, por ejemplo, AES GCM para el cifrado en el IPSec. Esto se discute en el RFC 4106.

El AES GCM permite alcanzar una velocidad mucho más rápida del cifrado en un poco de hardware.

Para ver las Recomendaciones de Cisco en usar y la migración a la criptografía de la última generación, refiérase:

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

Convenciones

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

Procedimiento de migración

Actualmente, la manera recomendada de emigrar del DMVPN a FlexVPN está para los dos marcos a no actuar al mismo tiempo.

Esta limitación deberá quitado a las nuevas características de la migración ser introducido en la versión ASR 3.10, seguida conforme a los pedidos de mejora múltiples bajo lado de Cisco, incluyendo CSCuc08066. Esas características deben estar disponibles a finales de junio, 2013.

Una migración donde ambos marcos coexisten y actúan al mismo tiempo en los mismos dispositivos será referida que suavemente la migración, que indica el impacto mínimo y la Conmutación por falla lisa a partir de un marco a otro.

Una migración donde coexiste la configuración de ambos marcos, pero no actúa al mismo tiempo se refiere como migración dura. Esto indica que un intercambio a partir de un marco a otro significa una falta de comunicación sobre el VPN, incluso si es mínimo.

Migración dura en los mismos dispositivos

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

Esta migración requiere que ambos marcos no actúen al mismo tiempo en los dispositivos, esencialmente requiriendo que las funciones DMVPN están inhabilitadas en todos los ámbitos antes de habilitar FlexVPN.

Hasta que la nueva característica de la migración esté disponible, la manera de realizar las migraciones usando los mismos dispositivos está a:

1. Verifique la Conectividad sobre el DMVPN.
2. Agregue la configuración de FlexVPN en el lugar y apague el túnel y las interfaces de plantilla virtual que pertenecen a la nueva configuración.
3. (Durante una ventana de mantenimiento) apague todas las interfaces del túnel DMVPN en todo el spokes y el Hubs antes de mover al paso 4.
4. Interfaces del túnel de Unshut FlexVPN.
5. Verifique habló a la Conectividad del concentrador.
6. Verifique habló a la Conectividad del spoke.
7. *Si no fue la verificación en la punta 5 o 6 correctamente invierta de nuevo al DMVPN apagando la interfaz de FlexVPN y O.N.U-cerrando las interfaces DMVPN.*
8. *Verifique habló a la comunicación del concentrador.*
9. *Verifique habló a la comunicación del spoke.*

Acercamiento de encargo

Si, debido a sus complejidades de la red o de la encaminamiento, el acercamiento no pudo ser la mejor idea para usted, comience una discusión con su representante de Cisco antes de emigrar. La mejor persona para discutir un proceso de migración de encargo es su ingeniero en sistemas o ingeniero del Advanced Services.

Topología de red

Topología de red de transporte

Este diagrama muestra una topología típica de las conexiones de los host en Internet. En este documento, la dirección IP del concentrador del loopback0 (172.25.1.1) se utiliza para terminar sesión IPSec.

Topología de red del recubrimiento

Este Diagrama de topología muestra dos nubes separadas usadas para el recubrimiento: DMVPN (conexiones verdes) y conexiones de FlexVPN.

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

La subred 10.1.1.0/24 no representa una subred real en términos de interfaz que dirige, sino bastante un pedazo del espacio IP dedicado a la nube de FlexVPN. El fundamento detrás se discute más adelante en la sección de configuración de FlexVPN.

Configuración

Configuración DMVPN

Esta sección contiene la configuración básica del hub and spoke DMVPN.

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

Una vez que se ha establecido el IPSec, el registro NHRP se realiza de habló al concentrador, de modo que el concentrador pueda aprender la dirección NBMA dinámicamente de los rayos.

Cuando el NHRP realiza el registro en el spoke y el concentrador, rutear el adjacancy puede establecer y las rutas intercambiadas. En este ejemplo, el EIGRP se utiliza como Routing Protocol básico para la red de recubrimiento.

Configuración del spoke DMVPN

Ésta es una configuración del ejemplo básico del DMVPN con la autenticación de la clave previamente compartida y del EIGRP como Routing Protocol.

```
crypto isakmp policy 10
  encr aes
  authentication pre-share
crypto isakmp key cisco address 0.0.0.0
crypto isakmp keepalive 30 5
crypto isakmp profile DMVPN_IKEv1
  keyring DMVPN_IKEv1
  match identity address 0.0.0.0
crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
  mode transport
crypto ipsec profile DMVPN_IKEv1
  set transform-set IKEv1
  set isakmp-profile DMVPN_IKEv1
interface Tunnel0
ip address 10.0.0.101 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map 10.0.0.1 172.25.1.1
 ip nhrp map multicast 172.25.1.1
 ip nhrp network-id 1
 ip nhrp holdtime 900
 ip nhrp nhs 10.0.0.1
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN_IKEv1
```

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

Configuración del concentrador DMVPN

En Configuración del hub el túnel es originado del loopback0 con un IP Address de 172.25.1.1.

El resto es despliegue estándar del concentrador DMVPN con el EIGRP como Routing Protocol.

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
crypto isakmp key cisco address 0.0.0.0
crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
 mode transport
crypto ipsec profile DMVPN_IKEv1
 set transform-set IKEv1
 interface Tunnel0
 ip address 10.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip nhrp holdtime 900
 ip nhrp server-only
 ip nhrp redirect
 ip summary-address eigrp 100 192.168.0.0 255.255.0.0
 ip tcp adjust-mss 1360
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel protection ipsec profile DMVPN_IKEv1
router eigrp 100
 network 10.0.0.0 0.0.0.255
 network 192.168.0.0 0.0.255.255
 passive-interface default
 no passive-interface Tunnel0
```

Configuración de FlexVPN

FlexVPN se basa en estas mismas Tecnologías fundamentales:

- IPSec: A diferencia del valor por defecto en el DMVPN, IKEv2 se utiliza en vez de IKEv1 para negociar el SA de IPSec. IKEv2 ofrece las mejoras sobre IKEv1, empezando por la elasticidad y la conclusión con cuántos mensajes son necesarios establecer un canal de datos protegidos.
- GRE: A diferencia del DMVPN, se utilizan las interfaces de punto a punto estáticas y dinámicas, y no sólo en el GRE de múltiples puntos estático interconecta. Esta configuración permite la flexibilidad agregada, especialmente para el por-spoke/el comportamiento del por-concentrador.
- NHRP: En FlexVPN el NHRP se utiliza sobre todo para establecer habló a la comunicación del spoke. El spokes no se registra al concentrador.
- El rutear: Porque el spokes no realiza el registro NHRP al concentrador, usted necesita confiar en otros mecanismos para aseegurarse el concentrador y el spokes puede comunicar bidireccional. Simliar al DMVPN, los Dynamic Routing Protocol puede ser utilizado. Sin

embargo, FlexVPN permite que usted utilice el IPSec para introducir la información de ruteo. El valor por defecto es introducir como ruta de /32 para la dirección IP en el otro lado del túnel, que permitirá la comunicación directa del spoke a hub.

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

Sepárelos en varios niveles:

- NHRP - Utilice diversa red NHRP ID (recomendada).
- El rutear - Utilice los procesos de ruteo separados (recomendados).
- VRF - La separación VRF puede permitir la flexibilidad agregada pero no será discutida aquí (opcional).

Configuración de FlexVPN del spoke

Una de las diferencias en configuración radial en FlexVPN con respecto al DMVPN, es que usted tiene potencialmente dos interfaces.

Hay un túnel necesario para habló a la comunicación del concentrador y el túnel opcional para habló a los túneles del spoke. Si usted elige no tener dinámico hablara al spoke que hace un túnel y bastante que todo pasa a través del dispositivo del concentrador, usted puede quitar la interfaz de plantilla virtual y quitar la transferencia del acceso directo NHRP de la interfaz del túnel.

Usted también notará que la interfaz del túnel estática tiene una dirección IP recibida basada en la negociación. Esto permite que el concentrador proporcione el IP de la interfaz del túnel habló dinámicamente sin la necesidad de crear la dirección estática en la nube de FlexVPN.

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

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

Cisco recomienda usando AES GCM en hardware que lo soporte.

```
crypto ipsec transform-set IKEv2 esp-gcm
    mode transport
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
interface Tunnel1
 ip address negotiated
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 ip tcp adjust-mss 1360
 shutdown
 tunnel source Ethernet0/0
 tunnel destination 172.25.1.1
 tunnel path-mtu-discovery
```

```
 tunnel protection ipsec profile default
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel1
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
```

El PKI es la manera recomendada de realizar la autenticación del gran escala en IKEv2.

Sin embargo, usted puede todavía utilizar la clave previamente compartida mientras usted sea consciente de ella sea limitaciones.

Aquí está un ejemplo de configuración usando “Cisco” como PSK:

```
crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco
crypto ikev2 profile Flex_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
 aaa authorization group psk list default default
```

Configuración del hub de FlexVPN

Un concentrador terminará típicamente solamente los túneles dinámicos del spoke a hub. Esta es la razón por la cual en la configuración del concentrador usted no encontrará una interfaz del túnel estática para FlexVPN, en lugar una interfaz de plantilla virtual se utiliza. Esto spawn/generará una interfaz de acceso virtual para cada conexión.

Observe que en el lado del eje de conexión usted necesita señalar a las direcciones del agrupamiento que se asignarán al spokes.

Los direccionamientos de este pool serán agregados más tarde en la tabla de ruteo como rutas de /32 para cada spoke.

```
aaa new-model
aaa authorization network default local
aaa session-id common
crypto ikev2 authorization policy default
 pool FlexSpokes
crypto ikev2 profile Flex_IKEv2
 match identity remote fqdn domain cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 aaa authorization group cert list default default
 virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

Cisco recomienda usando AES GCM en hardware que lo soporte.

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

Observe eso en la configuración debajo de la operación AES GCM se ha comentado hacia fuera.

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

Con la autenticación en IKEv2, el mismo principio se aplica en el concentrador como en el spoke.

Para el scalability y la flexibilidad, utilice los Certificados. Sin embargo, usted puede reutilizar la misma configuración para el PSK como en el spoke.

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

Migración del tráfico

Migración al BGP como [Recommended] del Routing Protocol del recubrimiento

El BGP es un Routing Protocol basado en el intercambio del unicast. Debido a él son las características que ha sido el mejor protocolo del escalamiento de las redes DMVPN.

En este ejemplo, se utiliza el iBGP.

Configuración BGP del spoke

La migración del spoke consiste en dos porciones. Habilitar el BGP como Dynamic Routing.

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

Después de que suba el vecino BGP (véase la configuración BGP del concentrador en esta sección de la migración) y los nuevos prefijos sobre el BGP son doctos, usted puede balancear el tráfico de la nube existente DMVPN a la nueva nube de FlexVPN.

Configuración BGP del concentrador

En el concentrador se configura evitar guardar la configuración de la vecindad para cada habló por separado, los módulos de escucha dinámicos.

En esta configuración el BGP no iniciará las nuevas conexiones, sino validará la conexión del pool proporcionado de los IP Addresses. En este caso el pool dicho es 10.1.1.0/24, que es todos los direccionamientos en la nueva nube de FlexVPN.

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

Tráfico de la migración a FlexVPN

Según lo mencionado antes de que la migración necesite ser hecha apagando las funciones DMVPN y trayendo FlexVPN para arriba.

Este procedimiento garantiza el impacto mínimo.

1. En todo el spokes:`interface tunnel 0`
   `shut`
2. En el concentrador:`interface tunnel 0`
   `shut`En este momento aseegurese que no hay sesiones IKEv1 establecidas a este concentrador del spokes.Esto puede ser verificada marcando la salida del **comando show crypto isakmp sa** y monitoreando los mensajes de Syslog generados por la sesión crypto del registro.Una vez que se ha confirmado esto usted puede proceder a traer para arriba FlexVPN.
3. Continuación en el concentrador:`interface Virtual-template 1`
   `no shut`
4. En el spokes:`interface tunnel 1`
   `no shut`

Pasos de verificación

Estabilidad del IPSec

La mejor manera de evaluar la estabilidad del IPSec por está monitoreando los sylogs con este comando configuration habilitado:

```
crypto logging session
```

Si usted ve las sesiones el ir hacia arriba y hacia abajo, esto puede indicar un problema en el nivel IKEv2/FlexVPN que necesita ser corregido antes de que la migración pueda comenzar.

Información sobre BGP poblada

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

En caso del BGP, esto puede ser vista realizándose:

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

Ejemplo de la información correcta del concentrador:

```
Hub#show bgp
BGP router identifier 172.25.1.1, local AS number 65001
```

```
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.101 4 65001 83 82 13 0 0 01:10:46 1 *10.1.1.102 4 65001 7 7 13 0 0 00:00:44 1
```

Usted puede ver que el concentrador ha aprendido que 1 prefijo de cada uno del spokes y ambo spokes son dinámicos (marcado con la muestra del asterisco (*)).

Ejemplo de la información similar del spoke:

```
Spoke1#show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 11 11 6 0 0 00:03:43 1
```

El spoke ha recibido un prefijo del concentrador. En caso de esta configuración, este prefijo debe ser el resumen de divulgación en el concentrador.

Migración a los nuevos túneles usando el EIGRP

El EIGRP es una opción popular en las redes DMVPN debido a ella es despliegue y convergencia rápida relativamente simples.

, Sin embargo, escalará peor que el BGP y no ofrece muchos de los mecanismos avanzados que se pueden utilizar por el cuadro recto de los BGP.

Esta siguiente sección describe una de las maneras de moverse a FlexVPN usando un nuevo proceso EIGRP.

Configuración radial actualizada

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

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

Nota: Usted debe evitar establecer la adyacencia del Routing Protocol encima habló a los túneles del spoke, así solamente hace la interfaz de tunnel1 (habló al concentrador) no pasiva.

Configuración del hub actualizada

Semejantemente en el concentrador, el DMVPN debe seguir siendo la forma más utilizada de intercambiar el tráfico encima. Sin embargo, FlexVPN debe hacer publicidad y aprender de los mismos prefijos ya.

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

Hay dos maneras de proporcionar la parte posterior del resumen hacia el spoke.

- Redistribución de una Static ruta que señala al null0 (opción preferida).`ip route 192.168.0.0 255.255.0.0 null 0`
  ```
  ip access-list standard EIGRP_SUMMARY
   permit 192.168.0.0 0.0.255.255
  router eigrp 200
  ```

```
distribute-list EIGRP_SUMMARY out Virtual-Template1
redistribute static metric 1500 10 10 1 1500
```
Esta opción permite tener el control sobre el resumen y redistribución sin la configuración VT del concentrador conmovedor.

- O, usted puede configurar a una dirección de resumen del DMVPN-estilo en la Virtual-plantilla. Esta configuración no se recomienda debido al procesamiento interno y la replicación del resumen dicho a cada acceso virtual. Se muestra aquí para la referencia:
```
interface Virtual-Template1 type tunnel
 ip summary-address eigrp 200 172.16.1.0 255.255.255.0
 ip summary-address eigrp 200 192.168.0.0 255.255.0.0 delay 2000
```

Tráfico de la migración a FlexVPN

La migración necesita ser hecha apagando las funciones DMVPN y trayendo FlexVPN para arriba.

El siguiente procedimiento garantiza el impacto mínimo.

1. En todo el spokes:
```
interface tunnel 0
 shut
```
2. En el concentrador:
```
interface tunnel 0
 shut
```
En este momento aseegurese que no hay sesiones IKEv1 establecidas a este concentrador del spokes.Esto puede ser verificada marcando la salida del **comando show crypto isakmp sa** y monitoreando los mensajes de Syslog generados por la sesión crypto del registro.Una vez que se ha confirmado esto usted puede proceder a traer para arriba FlexVPN.
3. Continuación en el concentrador:
```
interface Virtual-template 1
 no shut
```
4. En todo el spokes:
```
interface tunnel 1
 no shut
```

Pasos de verificación

Estabilidad del IPSec

Como en caso del BGP, usted necesita evaluar si el IPSec es estable. La mejor manera de hacer tan por está monitoreando los sylogs con este comando configuration habilitado:

```
crypto logging session
```
Si usted ve las sesiones el ir hacia arriba y hacia abajo, esto puede indicar un problema en el nivel IKEv2/FlexVPN que necesita ser corregido antes de que la migración pueda comenzar.

Información EIGRP en la tabla de topología

Aseegurese que usted hace su tabla de topología EIGRP poblar con las entradas del spoke LAN en el concentrador y el resumen en el spokes. Esto puede ser verificada publicando este comando en el hub and spoke.

```
show ip eigrp topology
```
Ejemplo de la salida apropiada del spoke:

```
Spoke1#sh ip eigrp topology
```

```
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
(...omitted as output related to DMVPN cloud ...)
EIGRP-IPv4 Topology Table for AS(200)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status

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


P 192.168.101.0/24, 1 successors, FD is 281600 via Connected, Ethernet1/0 P 192.168.0.0/16, 1
successors, FD is 26114560 via 10.1.1.1 (26114560/1709056), Tunnel1 P 10.1.1.107/32, 1
successors, FD is 26112000 via Connected, Tunnel1
```

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

Ejemplo de la salida apropiada del concentrador.

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

P 10.1.1.1/32, 1 successors, FD is 128256
 via Connected, Loopback100


P 192.168.101.0/24, 1 successors, FD is 1561600 via 10.1.1.107 (1561600/281600), Virtual-Access1
P 192.168.0.0/16, 1 successors, FD is 1709056 via Rstatic (1709056/0) P 10.1.1.107/32, 1
successors, FD is 1709056 via Rstatic (1709056/0) P 10.1.1.106/32, 1 successors, FD is 1709056
via Rstatic (1709056/0) P 0.0.0.0/0, 1 successors, FD is 1709056 via Rstatic (1709056/0) P
192.168.102.0/24, 1 successors, FD is 1561600 via 10.1.1.106 (1561600/281600), Virtual-Access2
```

Usted observará que el concentrador sabe sobre las subredes LAN de los rayos (en el itálico), el prefijo sumario que está haciendo publicidad (en **intrépido**) y que el IP Address asignado de cada rayo vía la negociación.

Consideraciones adicionales

La existencia habló a los túneles del spoke

Porque apagar la interfaz del túnel DMVPN hace las entradas NHRP ser quitada, la existencia habló a los túneles del spoke será rasgada abajo.

Borrar las entradas NHRP

Como se mencionó antes, un concentrador de FlexVPN no confiará en el proceso de inscripción NHRP del habló para saber rutear la parte posterior del tráfico. Sin embargo, dinámico habló a los túneles del spoke confían en las entradas NHRP.

En el DMVPN donde el NHRP que borraba en el concentrador habría podido dar lugar a los

problemas de conectividad efímeros.

En FlexVPN borrar el NHRP en el spokes causará FlexVPN sesión IPSec, relacionado con habló a los túneles del spoke, para ser derribada. En borrar el NHRP ningún concentrador tendrá un efecto sobre la sesión de FlexVPN.

Esto es debido al hecho que en FlexVPN, por abandono:

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

Advertencias conocidas

Habló al tráfico del spoke pudo ser afectado por CSCub07382.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems