Keepalives del túnel GRE

Contenido

Introducción

Este documento explica cuáles es el Keepalives del Generic Routing Encapsulation (GRE) y cómo él trabaja.

> Nota: Las Señales de mantenimiento GRE no se soportan así como la protección del túnel IPsec bajo ninguna circunstancias. Este documento discute este problema.

Túneles GRE

Un túnel GRE es una interfaz lógica en un router Cisco los paquetes de pasajero de ese proporciona una manera de encapsular dentro de un Transport Protocol. Es una arquitectura diseñada para proporcionar los servicios para implementar un esquema de la encapsulación Point-to-Point.

Los túneles GRE se diseñan para ser totalmente apátridas. Esto significa que cada punto final del túnel no guarda ninguna información sobre el estado o la Disponibilidad del punto final del túnel remoto. Una consecuencia de esto es que el router local del punto final del túnel no tiene la capacidad de derribar el Line Protocol de la interfaz de túnel GRE si el extremo remoto del túnel es inalcanzable. La capacidad de marcar una interfaz como abajo cuando el extremo remoto del link no está disponible se utiliza para quitar cualquier ruta (específicamente Static rutas) en la tabla de ruteo que utilice esa interfaz como la interfaz de salida. Específicamente, si el Line Protocol para una interfaz se cambia a abajo, después cualquier Static rutas que señalen que la interfaz está quitada de la tabla de ruteo. Esto permite para la instalación de una Static ruta (flotante) alterna o el Routing basado en políticas (PBR) para seleccionar un Next-Hop alterno o interconectar.

Normalmente, una interfaz de túnel GRE sube tan pronto como se configure y permanece para

arriba mientras haya un direccionamiento o una interfaz válido de origen de túnel que están para arriba. El IP Address de destino del túnel debe también ser routable. Esto es verdad incluso si el otro lado del túnel no se ha configurado. Esto significa que sigue habiendo una Static ruta o un reenvío PBR de paquetes vía la interfaz de túnel GRE en efecto aunque los paquetes de túnel GRE no alcanzan el otro extremo del túnel.

Antes de que las Señales de mantenimiento GRE fueran implementadas, había solamente maneras de determinar los problemas locales en el router y ninguna manera de determinar los problemas en la red intermedia. Por ejemplo, se pierde la caja en la cual los paquetes GRE tunelizados se remiten con éxito, pero antes de que alcancen el otro extremo del túnel. Tales escenarios causarían los paquetes de datos que pasan a través del túnel GRE ser “negro agujereado”, aunque una ruta alternativa que utiliza PBR o las Rutas estáticas flotantes vía otra interfaz pudo estar disponible. El Keepalives en la interfaz de túnel GRE se utiliza para solucionar este problema de la misma forma que el Keepalives se utiliza en las interfaces físicas.

Cómo los keepalives de túnel trabajan

El mecanismo de keepalive del túnel GRE es similar a las señales de mantenimiento de PPP en que da la capacidad para que un lado origine y reciba los paquetes de keepalive a y desde un router remoto incluso si el router remoto no soporta las Señales de mantenimiento GRE. Puesto que el GRE es un mecanismo de tunelización del paquete para hacer un túnel el IP dentro del IP, un paquete del túnel IP GRE se puede construir dentro de otro paquete del túnel IP GRE. Para las Señales de mantenimiento GRE, los prebuilds del remitente el paquete de la respuesta de keepalive dentro del paquete de pedidos del keepalive original de modo que las necesidades del extremo remoto solamente de hacer la descapsulación estándar GRE del encabezado IP externo GRE y después de invertir el Paquete GRE interno IP al remitente. Estos paquetes ilustran los conceptos del Tunelización IP donde está el Encapsulation Protocol el GRE y el IP es el Transport Protocol. El protocolo pasajero es también IP (aunque puede ser otro protocolo como el DECNet, el Intercambio de paquetes entre redes (IPX), o el APPLETALK).

Paquete normal:

Encabezado IP	Encabezado TCP	Telnet

Paquete tunneled:

Encabezado IP	GRE	GRE	Encabezado IP	Encabezado TCP	Telnet

- IP es el protocolo de transporte.
- GRE es el protocolo de encapsulación.
- IP es el protocolo pasajero.

Aquí está un ejemplo de un paquete de keepalive que origine del router A y es destinado para el router B. La respuesta de keepalive que el router B vuelve al router A está ya dentro del encabezado IP interno. Los decapsulates del router B simplemente el paquete de keepalive y lo envían se retiran la interfaz física (s2). Procesa el paquete del keepalive GRE apenas como cualquier otro paquete de datos IP GRE.

Señales de mantenimiento GRE:

Encabezado IP GRE		GRE	Encabezado IP		GRE
Fuente A	Destino B	PT=IP	Fuente B	Destino A	PT=0

Este mecanismo hace la respuesta de keepalive remitir hacia fuera la interfaz física bastante que la interfaz del túnel. Esto significa que el paquete de respuesta del keepalive GRE no es afectado por ninguna **funciones de resultados** en la interfaz del túnel, tal como “protección del túnel…”, QoS, ruteo virtual y expedición (VRF), y así sucesivamente.

> Nota: Si una lista de control de acceso (ACL) entrante en la interfaz de túnel GRE se configura, después el paquete de keepalive del túnel GRE que el dispositivo opuesto envía debe ser permitido. Si no, el túnel GRE del dispositivo opuesto estará abajo. (de la `lista de acceso del <number> del permit gre host host <tunnel-source> <tunnel-destination>`)

Otro atributo del Keepalives del túnel GRE es que los temporizadores KEEPALIVE en cada lado son independientes y no tienen que hacer juego, similar a las señales de mantenimiento de PPP.

> Consejo: El problema con la configuración del Keepalives solamente en un lado del túnel es que solamente el router que hace el Keepalives configurar marca su interfaz del túnel como abajo si expira el temporizador KEEPALIVE. Sigue habiendo la interfaz de túnel GRE en el otro lado, donde el Keepalives no se configura, para arriba incluso si el otro lado del túnel está abajo. El túnel puede sentir bien a un agujero negro para los paquetes dirigidos en el túnel del lado que no tenía Keepalives configurado.

> Consejo: En una red grande del túnel GRE del hub-and-spoke, puede ser que sea apropiado configurar solamente las Señales de mantenimiento GRE en el lado radial y no en el lado del eje de conexión. Esto es porque es a menudo más importante para habló para descubrir que el concentrador es inalcanzable y por lo tanto Switch a un trayecto de backup (Respaldo de marcado por ejemplo).

Keepalives del túnel GRE

Con la versión 12.2(8)T del Cisco IOS ® Software, es posible configurar el Keepalives en una interfaz de túnel GRE de punto a punto. Con este cambio, la interfaz del túnel apaga dinámicamente si el Keepalives falla por cierto período de tiempo.

Para más información sobre cómo otras formas de Keepalives trabajan, refiera a la descripción de los mecanismos de keepalive en el Cisco IOS.

> Nota: El Keepalives del túnel GRE se soporta solamente en los túneles GRE de punto a punto. Los keepalives de túnel son configurables en los túneles de múltiples puntos GRE (mGRE) pero no tienen ningún efecto.

> Nota: Los keepalives de túnel no trabajarán generalmente cuando los VRF se utilizan en la interfaz del túnel y el fVRF (“vrf del túnel… ") y el iVRF (“IP VRF remitiendo…” en la interfaz del túnel) no haga juego. Esto es crítico en el punto final del túnel que “refleja” el keepalive de nuevo al solicitante. Cuando se recibe la petición del keepalive se recibe en el fVRF y decapsulated. Esto revela la contestación prehecha del keepalive, que entonces las necesidades de ser remitido de nuevo al remitente, PERO esa expedición son en el

contexto del iVRF en la interfaz del túnel. Por lo tanto, si el iVRF y el fVRF entonces no hacen juego el paquete de respuesta del keepalive no se remite de nuevo al remitente. Esto es verdad incluso si usted substituye el iVRF y/o el fVRF por “global”.

Esta salida muestra los comandos que usted utiliza para configurar el Keepalives en los túneles GRE.

```
Router# configure terminal
Router(config)#interface tunnel0
Router(config-if)#keepalive 5 4

!--- The syntax of this command is keepalive [seconds [retries]].



!--- Keepalives are sent every 5 seconds and 4 retries.
!--- Keepalives must be missed before the tunnel is shut down.
!--- The default values are 10 seconds for the interval and 3 retries.
```

Para entender mejor cómo los trabajos del mecanismo del keepalive de túnel, consideran esta topología de túnel ejemplo y configuración:

router A

```
Router# configure terminal
Router(config)#interface tunnel0
Router(config-if)#keepalive 5 4

!--- The syntax of this command is keepalive [seconds [retries]].



!--- Keepalives are sent every 5 seconds and 4 retries.
!--- Keepalives must be missed before the tunnel is shut down.
!--- The default values are 10 seconds for the interval and 3 retries.
```

router B

```
Router# configure terminal
Router(config)#interface tunnel0
Router(config-if)#keepalive 5 4

!--- The syntax of this command is keepalive [seconds [retries]].
```

```
!--- Keepalives are sent every 5 seconds and 4 retries.
!--- Keepalives must be missed before the tunnel is shut down.
!--- The default values are 10 seconds for the interval and 3 retries.
```

En este escenario, el router A realiza estos pasos:

1. Construye el encabezado IP interno cada cinco segundos donde:

   la fuente se fija como el local el destino del túnel, que es 192.168.1.2el destino se fija como el origen de túnel local, que es 192.168.1.1

   y un encabezado GRE se agrega con un Tipo de protocolo (PT) de 0

   El paquete generó por el router A pero no enviado:

2. Envía ese paquete de su interfaz del túnel, que da lugar a la encapsulación del paquete con el encabezado IP externo donde:

   la fuente se fija como el local el origen de túnel, que es 192.168.1.1el destino se fija como el destino del túnel local, que es 192.168.1.2

   y un encabezado GRE se agrega con PT = IP.

   El paquete envió del router A al router B:

3. Incrementa el contador del keepalive de túnel por uno.

4. Con la suposición que hay una manera de alcanzar el punto final del túnel del otro extremo y el Line Protocol del túnel no está abajo de debido a otras razones, el paquete llega en el router B. Después se corresponde con contra el tunnel0, llega a ser decapsulated, y se remite al IP de destino que es el IP Address del origen de túnel en el router A.

   Enviado del router B al router A:

5. Sobre la llegada en el router A, el paquete se convierte en decapsulated y el control de los resultados PT en 0. Esto significa que esto es un paquete de keepalive. El contador del keepalive de túnel entonces se reajusta a 0 y se desecha el paquete.

Si el router B es inalcanzable, el router A continúa construyendo y enviando los paquetes de keepalive así como el tráfico normal. Si no se vuelve el Keepalives, el Line Protocol del túnel permanece para arriba mientras el contador del keepalive de túnel sea menos que el número de recomprobaciones, que en este caso es cuatro. Si esa condición no es verdad, después la próxima vez que el router A intenta enviar un keepalive al router B, se derriba el Line Protocol.

> Nota: En el estado encendido/apagado, el túnel no remite ni procesa ningún tráfico de datos. Sin embargo, continúa enviando los paquetes de keepalive. En la recepción de una respuesta de keepalive, con la implicación que el punto final del túnel es otra vez accesible, el contador del keepalive de túnel se reajusta a 0, y el Line Protocol en el túnel sube.

Para ver el Keepalives en la acción, habilite el **túnel del debug** y **haga el debug del keepalive de túnel**.

Muestree los debugs del router A:

```
debug tunnel keepalive
Tunnel keepalive debugging is on
01:19:16.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=15
01:19:21.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=16
01:19:26.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=17
```

Señales de mantenimiento GRE y Unicast Reverse Path Forwarding

El unicast RPF (Unicast Reverse Path Forwarding) es una función de seguridad que las ayudas detectan y el tráfico IP del spoofed del descenso con una validación de la dirección de origen de paquete contra la tabla de ruteo. Cuando el unicast RPF se ejecuta en el modo estricto (el **IP verifica la fuente del unicast accesible-vía el rx**), el paquete se debe recibir en la interfaz que el router utilizaría para remitir el paquete de devolución. Si el modo estricto o el unicast flexible RPF del modo se habilita en la interfaz del túnel del router que recibe los paquetes del keepalive GRE, después los paquetes del Keepalives serán caídos por el RPF después del decapsulation del túnel puesto que la ruta a la dirección de origen del paquete (propio direccionamiento del origen de túnel del router) no está a través de la interfaz del túnel. Las caídas de paquetes RPF se pueden observar en el **tráfico del IP de la demostración** hecho salir como sigue:

```
Router#show ip traffic | section Drop
Drop: 0 encapsulation failed, 0 unresolved, 0 no adjacency
0 no route, 156 unicast RPF, 0 forced drop
0 options denied
```

Como consecuencia, el iniciador de los keepalives de túnel derribará el túnel debido a los paquetes de devolución faltados del Keepalives. El unicast RPF no se debe configurar tan en el modo estricto o flexible para que el Keepalives del túnel GRE trabaje. Para más información sobre el unicast RPF, refiera comprensión del Unicast Reverse Path Forwarding.

IPSec y Señales de mantenimiento GRE

Túneles GRE con el IPSec

Los túneles GRE se combinan a veces con el IPSec porque el IPSec no soporta los paquetes del Multicast IP. Debido a esto, los Dynamic Routing Protocol no pueden ejecutarse con éxito sobre una red del IPSec VPN. Puesto que los túneles GRE soportan el Multicast IP, un Dynamic Routing Protocol se puede funcionar con sobre un túnel GRE. Los paquetes de la unidifusión IP GRE que el resultado se puede cifrar por el IPSec.

Hay dos maneras diferentes que el IPSec puede cifrar los Paquetes GRE:

- Una manera está con el uso de una **correspondencia de criptografía**. Cuando se utiliza una correspondencia de criptografía, se aplica a la interfaz física saliente para los paquetes de túnel GRE. En este caso, la secuencia de pasos es como sigue:

El paquete encriptado alcanza la interfaz física.El paquete se desencripta y se remite a la interfaz del túnel.El paquete es decapsulated y después remitido al destino IP en el texto claro.

- La otra manera es utilizar la **protección del túnel**. Cuando se utiliza la **protección del túnel**, se configura en la interfaz de túnel GRE. **El comando tunnel protection** estaba disponible en el Cisco IOS Software Release 12.2(13)T. En este caso, la secuencia de pasos es como sigue:

  El paquete encriptado alcanza la interfaz física.El paquete se remite a la interfaz del túnel.El paquete es desencriptado y decapsulated y entonces remitido al destino IP en el texto claro.

Ambos métodos especifican que la encripción de IPSec está realizada después de la adición de la encapsulación GRE. Hay dos diferencias fundamentales entre cuando usted utiliza una correspondencia de criptografía y cuando usted utiliza la protección del túnel:

- La correspondencia de criptografía del IPSec se ata a la interfaz física y se marca mientras que los paquetes se remiten hacia fuera la interfaz física.

  El túnel GRE tiene GRE encapsuló ya el paquete por esta punta.
- La protección del túnel ata la funcionalidad de encripción al túnel GRE y se marca después de que el paquete sea GRE encapsulado pero antes de que el paquete se da a la interfaz física.

Problemas con el Keepalives cuando usted combina el IPSec y el GRE

Dado las dos maneras de agregar el cifrado a los túneles GRE, hay tres maneras distintas de configurar un túnel GRE cifrado:

1. Mira A tiene protección del túnel configurada en la interfaz del túnel mientras que el par B tiene correspondencia de criptografía configurada en la interfaz física.
2. Mira A tiene correspondencia de criptografía configurada en la interfaz física mientras que el par B tiene protección del túnel configurada en la interfaz del túnel.
3. Ambos pares tienen protección del túnel configurada en la interfaz del túnel.

La configuración descrita en los escenarios 1 y 2 se hace a menudo en a diseño de hub y spoke. La protección del túnel se configura en el router de eje de conexión para reducir el tamaño de la configuración y una correspondencia de criptografía estática se utiliza en cada spoke.

Considere cada uno de estos escenarios con las Señales de mantenimiento GRE habilitadas en el par B(spoke) y donde utilizan al modo túnel para el cifrado.

Escenario 1

Determinación:

- Mira una protección del túnel de las aplicaciones.
- El par B utiliza las correspondencias de criptografía.
- El Keepalives se habilita en el par B.

- La encripción de IPSec se hace en el modo túnel.

En este escenario, puesto que las Señales de mantenimiento GRE se configuran en el par B, los eventos de la secuencia cuando se genera un keepalive son como sigue:

1. El par B genera un paquete de keepalive que sea GRE encapsulado y después remitido a la interfaz phyiscal donde se cifra y se envía encendido al destino del túnel, el par A.

   El paquete envió del par B para mirar A:

2. En el par A, se recibe el keepalive GRE desencriptó:

   decapsulated:

   Entonces el paquete de respuesta interno del keepalive GRE se rutea sobre la base de su dirección destino que sea el par B. Eso significa en el par A, el paquete se rutea inmediatamente se retira la interfaz física a mirar B. Puesto que el par A utiliza la protección del túnel en la **interfaz del túnel**, el paquete de keepalive no se cifra.

   Por lo tanto, el paquete envió del par A para mirar B:

   Nota: El keepalive no se cifra.

3. El par B ahora recibe una respuesta del keepalive GRE que no se cifre en su interfaz física, pero debido a la correspondencia de criptografía configurada en la interfaz física, cuenta con un paquete encriptado y lo cae tan.

Por lo tanto, aunque el par A responde a los keepailves y al router de origen, el par B recibe las respuestas, nunca las procesa y cambia eventual el Line Protocol de la interfaz del túnel al estado inactivo.

Resultado:

El Keepalives habilitado en el par B hace al estado de túnel en el par B cambiar a arriba/abajo.

Escenario 2

Determinación:

- Miran las correspondencias de criptografía de las aplicaciones.
- El par B utiliza la protección del túnel.
- El Keepalives se habilita en el par B.
- La encripción de IPSec se hace en el modo túnel.

En este escenario, puesto que las Señales de mantenimiento GRE onfigured en el par B, los eventos de la secuencia cuando se genera un keepalive son como sigue:

1. El par B genera un paquete de keepalive que sea GRE encapsulado y después cifrado por la protección del túnel en la interfaz del túnel y después remitido a la interfaz física.

   El paquete envió del par B para mirar A:

2. En el par A, se recibe el keepalive GRE desencriptó:

   decapsulated:

   Entonces el paquete de respuesta interno del keepalive GRE se rutea sobre la base de su dirección destino que sea el par B. Eso significa en el par A, el paquete se rutea inmediatamente se retira la interfaz física a mirar B. Puesto que el par A utiliza las correspondencias de criptografía en la **interfaz física**, primero cifrará este paquete antes de que él adelante él encendido.

   Por lo tanto, el paquete envió del par A para mirar B:

   Nota: Se cifra la respuesta de keepalive.

3. El par B ahora recibe una respuesta cifrada del keepalive GRE cuyo destino se remita a la interfaz del túnel donde se desencripta:

   Puesto que fijan al tipo de Protocal a 0, el par B sabe que esto es una respuesta de keepalive y que la procesa como tal.

Resultado:

El Keepalives habilitado en el par B determina con éxito lo que debe ser basado el estado de túnel en la Disponibilidad del destino del túnel.

Escenario 3

Determinación:

- Protección del túnel del uso de ambos pares.
- El Keepalives se habilita en el par B.
- La encripción de IPSec se hace en el modo túnel.

Este escenario es similar al escenario 1 en eso cuando el par A recibe el keepalive cifrado, él desencripta y los decapsulates él. Sin embargo, cuando se remite la respuesta se retira, no se cifra puesto que el par A utiliza la protección del túnel en la **interfaz del túnel**. Así, el par B cae la respuesta de keepalive unencrypted y no la procesa.

Resultado:

El Keepalives habilitado en el par B hace al estado de túnel en el par B cambiar a arriba/abajo.

Solución Aternativa

En tales situaciones donde los Paquetes GRE deben ser cifrados, hay tres Soluciones posibles:

1. **Utilice una correspondencia de criptografía en el par A, haga un túnel la protección en el par B, y habilite el Keepalives en el par B.**

   Puesto que los este tipos de configuración se utilizan sobre todo en configuraciones del hub-and-spoke y porque en tales configuraciones es más importante para habló para ser consciente del accesibilidad del concentrador, la solución es utilizar una correspondencia cifrada dinámica en el concentrador (par A) y protección del túnel en el spoke (par B) y habilitar las Señales de mantenimiento GRE en el spoke. Se pierde esta manera, aunque siga habiendo la interfaz de túnel GRE en el concentrador para arriba, el vecino de ruteo y las rutas a través del túnel y la ruta alternativa puede ser establecida. En el spoke, el hecho de que fuera la interfaz del túnel abajo puede accionarla para criar una interfaz del dialer y una devolución de llamada al concentrador (o a otro router en el concentrador), después establece una nueva conexión.

2. **Utilice algo con excepción de las Señales de mantenimiento GRE para determinar el alcance del peer**.

   Si configuran a ambo Routers con la protección del túnel, después los keeaplives del túnel GRE no se pueden utilizar en cualquier dirección. En este caso, la única opción es utilizar el Routing Protocol o el otro mecanismo, tal como el Service Assurance Agent, para descubrir si el par es accesible o no.

3. **Utilice las correspondencias de criptografía en el par A y el par B.**

   Si ambo el configuran Routers con las correspondencias de criptografía, los keepalives de túnel pueden conseguir a través en las ambas direcciones y las interfaces de túnel GRE pueden apagar en cualquier o las ambas direcciones y accionar una conexión de respaldo que se hará. Ésta es la mayoría de la opción flexible.

Información Relacionada

- RFC 1701, (GRE) del Generic Router Encapsulation
- Extensiones del RFC 2890, de la clave y del número de secuencia al GRE

- Keepalive de túnel del Generic Routing Encapsulation (GRE)
- Fragmentación de IP y PMTUD
- Descripción de los mecanismos de keepalive en el Cisco IOS
- Soporte Técnico - Cisco Systems