Comprensión de Keepalives de Túnel GRE

Contenido

Introducción

Este documento describe qué son las señales de mantenimiento de Generic Routing Encapsulation (GRE) y cómo funcionan.

Túneles GRE

Un túnel GRE es una interfaz lógica en un router de Cisco que proporciona una manera de encapsular los paquetes de pasajeros dentro de un protocolo de transporte. Se trata de una arquitectura diseñada para proporcionar los servicios con el fin de implementar un esquema de encapsulación punto a punto.

Los túneles GRE están diseñados para ser completamente independientes del estado. Esto significa que cada extremo del túnel no conserva ninguna información sobre el estado o la disponibilidad del extremo del túnel remoto. Una consecuencia de esto es que el router de punto final del túnel local no tiene la capacidad de desactivar el protocolo de línea de la interfaz del túnel GRE si el extremo remoto del túnel es inalcanzable. La capacidad de marcar una interfaz como inactiva cuando el extremo remoto del link no está disponible se utiliza para quitar cualquier ruta (específicamente rutas estáticas) en la tabla de ruteo que utiliza esa interfaz como interfaz saliente. Específicamente, si el protocolo de línea para una interfaz se cambia a down, las rutas estáticas que señalan esa interfaz se eliminan de la tabla de ruteo. Esto permite la instalación de una ruta estática alternativa (flotante) o de Policy Based Routing (PBR) para seleccionar un salto o interfaz siguiente alternativos.

Normalmente, una interfaz de túnel GRE aparece tan pronto como se configura y permanece activa mientras haya una dirección o interfaz de origen de túnel válida que esté activa. La dirección IP de destino del túnel también debe ser enrutable. Esto es así incluso si el otro lado del túnel no se ha configurado. Esto significa que una ruta estática o reenvío PBR de paquetes a través de la interfaz de túnel GRE permanece activa aunque los paquetes de túnel GRE no

alcancen el otro extremo del túnel.

Antes de que se implementaran las señales de mantenimiento GRE, solo había formas de determinar los problemas locales en el router y no había forma de determinar los problemas en la red interviniente. Por ejemplo, el caso en el que los paquetes tunelados GRE se reenvían correctamente, pero se pierden antes de llegar al otro extremo del túnel. Tales escenarios causarían que los paquetes de datos que pasan a través del túnel GRE sean "agujeros negros", aunque haya disponible una ruta alternativa que utilice PBR o una ruta estática flotante a través de otra interfaz. Los keepalives en la interfaz de túnel GRE se utilizan para resolver este problema de la misma manera que los keepalives se utilizan en las interfaces físicas.

> **Nota**: los keepalives GRE no se soportan junto con la protección de túnel IPsec bajo ninguna circunstancia. Este documento trata este problema.

Cómo Funcionan los Keepalives del Túnel

El mecanismo de keepalive del túnel GRE es similar a los keepalives PPP en cuanto que brinda a un lado la capacidad de originar y recibir paquetes keepalive hacia y desde un router remoto incluso si el router remoto no soporta keepalives GRE. Dado que GRE es un mecanismo de tunelización de paquetes para tunelizar IP dentro de IP, se puede construir un paquete de túnel IP GRE dentro de otro paquete de túnel IP GRE. Para las señales de mantenimiento GRE, el remitente preconstruye el paquete de respuesta de señal de mantenimiento dentro del paquete de solicitud de señal de mantenimiento original de modo que el extremo remoto solo necesita realizar una desencapsulación GRE estándar del encabezado IP GRE externo y luego revertir el paquete GRE IP interno al remitente. Estos paquetes ilustran los conceptos de tunelización IP donde GRE es el protocolo de encapsulación e IP es el protocolo de transporte. El protocolo pasajero también es IP (aunque puede ser otro protocolo como Decnet, Intercambio de paquetes entre redes (IPX) o Appletalk).

Paquete normal:

Encabezado IP	Encabezado TCP	TELNET

Paquete tunelizado:

Encabezado IP de	GRE	Encabezado IP	Encabezado TCP	TELNET

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

Este es un ejemplo de un paquete de señal de mantenimiento que se origina desde el Router A y está destinado al Router B. La respuesta de señal de mantenimiento que el router B devuelve al router A ya está dentro del encabezado IP interno. El router B simplemente desencapsula el paquete de señal de mantenimiento y lo envía de vuelta a la interfaz física (S2). Procesa el paquete de señal de mantenimiento GRE como cualquier otro paquete de datos IP GRE.

Keepalives de GRE:

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

Este mecanismo hace que la respuesta de keepalive reenvíe fuera de la interfaz física en lugar de la interfaz de túnel. Esto significa que el paquete de respuesta de keepalive GRE no se ve afectado por ninguna función de salida en la interfaz de túnel, como 'protección de túnel ...', QoS, Virtual Routing and Forwarding (VRF), etc.

> **Nota**: si se configura una lista de control de acceso (ACL) entrante en la interfaz de túnel GRE, se debe permitir el paquete de señal de mantenimiento del túnel GRE que envía el dispositivo opuesto. Si no es así, el túnel GRE del dispositivo opuesto se desactiva. (**access-list** <number> **permit gre host** <tunnel-source> **host** <tunnel-destination>)

Otro atributo de los keepalives del túnel GRE es que los temporizadores de keepalive en cada lado son independientes y no tienen que coincidir, de manera similar a los keepalives PPP.

> **Sugerencia**: El problema con la configuración de señales de mantenimiento solamente en un lado del túnel es que solamente el router que tiene señales de mantenimiento configuradas marca su interfaz de túnel como inactiva si el temporizador de señal de mantenimiento caduca. La interfaz de túnel GRE del otro lado, donde no se configuran señales de mantenimiento, permanece activa incluso si el otro lado del túnel está inactivo. El túnel puede convertirse en un agujero negro para los paquetes dirigidos al túnel desde el lado que no tenía keepalives configurados.

> **Sugerencia**: en una red de túnel GRE de hub y radio grande, puede ser apropiado configurar solamente señales de mantenimiento GRE en el lado del spoke y no en el lado del hub. Esto se debe a que, a menudo, es más importante que el spoke detecte que el hub es inalcanzable y, por lo tanto, cambie a una ruta de respaldo (Respaldo de marcado, por ejemplo).

Keepalives de túnel GRE

Con Cisco IOS® Software Release 12.2(8)T, es posible configurar señales de mantenimiento en una interfaz de túnel GRE punto a punto. Con este cambio, la interfaz de túnel se apaga dinámicamente si las señales de mantenimiento fallan durante un cierto período de tiempo.

Para obtener más información sobre cómo funcionan otras formas de señales de mantenimiento, consulte Descripción General de los Mecanismos de Keepalive en Cisco IOS.

> **Nota**: los keepalives de túnel GRE sólo se soportan en túneles GRE punto a punto. Las señales de mantenimiento del túnel se pueden configurar en túneles GRE multipunto (mGRE), pero no tienen ningún efecto.

> **Nota**: En general, los keepalives de túnel no pueden funcionar cuando se utilizan VRF en la interfaz de túnel y el fVRF (‘tunnel vrf ...’) e iVRF (‘ip vrf forwarding ...’ en la interfaz de túnel) no coinciden. Esto es crítico en el punto final del túnel que "refleja" la señal de mantenimiento de vuelta al solicitante. Cuando se recibe la solicitud de keepalive, se recibe en fVRF y se desencapsula. Esto revela la respuesta de señal de mantenimiento

predefinida, que luego debe ser reenviada de vuelta al remitente, PERO ese reenvío está en el contexto del iVRF en la interfaz de túnel. Por lo tanto, si el iVRF y el fVRF no coinciden, el paquete de respuesta de keepalive no se reenvía al remitente. Esto es así incluso si reemplaza iVRF y/o fVRF por "global".

Este resultado muestra los comandos que se utilizan para configurar señales de mantenimiento en 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 funciona el mecanismo de señal de mantenimiento de túnel, considere este ejemplo de topología y configuración de túnel:

Router A

```
interface loopback 0
ip address 192.168.1.1 255.255.255.255
interface tunnel 0
ip address 10.10.10.1 255.255.255.252
tunnel source loopback0
tunnel destination 192.168.1.2
keepalive 5 4
```

Router B

```
interface loopback 0
ip address 192.168.1.2 255.255.255.255
interface tunnel 0
ip address 10.10.10.2 255.255.255.252
tunnel source loopback0
tunnel destination 192.168.1.1
```

```
keepalive 5 4
```

En este escenario, el Router A realiza estos pasos:

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

   el origen se establece como el destino local del túnel, que es 192.168.1.2el destino se establece como el origen del túnel local, que es 192.168.1.1

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

   Paquete generado por el router A pero no enviado:

2. Envía ese paquete fuera de su interfaz de túnel, lo que resulta en la encapsulación del paquete con el encabezado IP externo donde:

   el origen se establece como el origen local del túnel, que es 192.168.1.1el destino se establece como el destino del túnel local, que es 192.168.1.2

   y se agrega un encabezado GRE con PT = IP.

   Paquete enviado desde el Router A al Router B:

3. Incrementa el contador de señales de mantenimiento de túnel en uno.

4. Suponiendo que existe una manera de alcanzar el extremo final del túnel y que el protocolo de línea de túnel no está inactivo debido a otras razones, el paquete llega al Router B. Luego se compara con el Túnel 0, se desencapsula y se reenvía a la IP de destino que es la dirección IP de origen del túnel en el Router A.

   Enviado desde el Router B al Router A:

5. Al llegar al Router A, el paquete se desencapsula y la verificación del PT da como resultado 0. Esto significa que se trata de un paquete de señal de mantenimiento. El contador de señales de mantenimiento del túnel se restablece a 0 y el paquete se descarta.

Si el Router B es inalcanzable, el Router A continúa construyendo y enviando paquetes keepalive, así como el tráfico normal. Si los keepalives no regresan, el protocolo de línea de túnel permanece activo mientras el contador de keepalive del túnel sea menor que el número de reintentos, que en este caso es cuatro. Si esa condición no es verdadera, entonces la próxima vez que el Router A intente enviar una señal de mantenimiento al Router B, el protocolo de línea se desactiva.

> **Nota**: En el estado activo/inactivo, el túnel no reenvía ni procesa ningún tráfico de datos. Sin embargo, continúa enviando paquetes keepalive. En la recepción de una respuesta de señal de mantenimiento, con la implicación de que el extremo del túnel es nuevamente alcanzable, el contador de señal de mantenimiento del túnel se reinicia a 0 y el protocolo de línea en el túnel aparece.

Para ver keepalives en acción, habilite **debug tunnel** y **debug tunnel keepalive**.

Depuraciones de ejemplo 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
```

Keepalives de GRE y Unicast Reverse Path Forwarding

Unicast RPF (Unicast Reverse Path Forwarding) es una función de seguridad que ayuda a detectar y descartar tráfico IP falsificado con una validación de la dirección de origen del paquete frente a la tabla de ruteo. Cuando Unicast RPF se ejecuta en modo estricto (**ip verify unicast source reachable-via rx), el paquete se debe recibir en la interfaz que el router utilizaría para reenviar el paquete de retorno.** Si se habilita el modo estricto o el modo flexible Unicast RPF en la interfaz de túnel del router que recibe los paquetes keepalive GRE, RPF descarta los paquetes keepalives después de la desencapsulación del túnel ya que la ruta a la dirección de origen del paquete (dirección de origen de túnel propio del router) no pasa por la interfaz de túnel. Las caídas de paquetes RPF se pueden observar en la salida de **show ip traffic** de la siguiente manera:

```
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 resultado, el iniciador de los keepalives del túnel hace caer el túnel debido a paquetes de retorno de keepalives perdidos. Por lo tanto, RPF unidifusión no debe configurarse en modo estricto o flexible para que funcionen las señales de mantenimiento del túnel GRE. Para obtener más información sobre Unicast RPF, consulte Comprensión de Unicast Reverse Path Forwarding.

Keepalives de IPSec y GRE

Túneles GRE con IPsec

Los túneles GRE a veces se combinan con IPSec porque IPSec no admite paquetes de multidifusión IP. Debido a esto, los protocolos de ruteo dinámico no pueden ejecutarse con éxito a través de una red VPN IPsec. Dado que los túneles GRE admiten multidifusión IP, se puede ejecutar un protocolo de routing dinámico a través de un túnel GRE. Los paquetes de unidifusión IP GRE resultantes se pueden cifrar mediante IPSec.

IPSec puede cifrar paquetes GRE de dos maneras:

- Una forma es con el uso de un mapa criptográfico. Cuando se utiliza un mapa criptográfico, se aplica a las interfaces físicas salientes para los paquetes de túnel GRE. En este caso, la secuencia de pasos es la siguiente:

El paquete cifrado alcanza la interfaz física.El paquete se descifra y se reenvía a la interfaz de túnel.El paquete se desencapsula y luego se reenvía al destino IP en texto no cifrado.

- La otra forma es utilizar la protección de túnel. Cuando se utiliza la protección de túnel, se configura en la interfaz de túnel GRE. El comando tunnel protection pasó a estar disponible en Cisco IOS Software Release 12.2(13)T. En este caso, la secuencia de pasos es la siguiente:

  El paquete cifrado alcanza la interfaz física.El paquete se reenvía a la interfaz de túnel.El paquete se descifra y desencapsula y luego se reenvía al destino IP en texto no cifrado.

Ambos métodos especifican que el cifrado IPsec se realiza después de la adición de la encapsulación GRE. Existen dos diferencias clave entre el uso de un mapa criptográfico y la protección de túnel:

- El mapa criptográfico IPSec está vinculado a la interfaz física y se comprueba a medida que los paquetes se reenvían fuera de la interfaz física.

  El túnel GRE ya ha encapsulado el paquete en este punto.
- La protección del túnel vincula la funcionalidad de cifrado con el túnel GRE y se comprueba después de que el paquete esté encapsulado en GRE, pero antes de que el paquete se entregue a la interfaz física.

Problemas con Keepalives al Combinar IPsec y GRE

Dadas las dos formas de agregar cifrado a los túneles GRE, existen tres formas distintas de configurar un túnel GRE cifrado:

1. El Peer A tiene la protección de túnel configurada en la interfaz de túnel, mientras que el Peer B tiene el mapa criptográfico configurado en la interfaz física.
2. El Peer A tiene un mapa criptográfico configurado en la interfaz física, mientras que el Peer B tiene la protección de túnel configurada en la interfaz de túnel.
3. Ambos Peers tienen la protección de túnel configurada en la interfaz de túnel.

La configuración descrita en los escenarios 1 y 2 se realiza a menudo en un diseño radial. La protección del túnel se configura en el router hub para reducir el tamaño de la configuración y se utiliza un mapa criptográfico estático en cada radio.

Considere cada uno de estos escenarios con señales de mantenimiento GRE habilitadas en el Peer B (spoke) y donde el modo de túnel se utiliza para el cifrado.

Escenario 1

Configuración:

- El Peer A utiliza la Protección de Túnel.
- El Peer B utiliza Crypto Maps.
- Las señales de mantenimiento están habilitadas en el Peer B.
- El cifrado IPSec se realiza en modo túnel.

En este escenario, dado que las señales de mantenimiento GRE se configuran en el Peer B, los eventos de secuencia cuando se genera una señal de mantenimiento son los siguientes:

1. El Peer B genera un paquete de señal de mantenimiento que es GRE encapsulado y luego reenviado a la interfaz física donde se cifra y se envía al destino del túnel, Peer A.

   Paquete enviado desde el Peer B al Peer A:

2. En el Peer A, la señal de mantenimiento GRE se recibe descifrada:

   desencapsulado:

   Luego, el paquete de respuesta de señal de mantenimiento GRE interno se enruta en función de su dirección de destino, que es el Peer B. Esto significa que en el Peer A, el paquete se rutea inmediatamente de regreso fuera de la interfaz física al Peer B. Dado que el Peer A utiliza protección de túnel en la interfaz de túnel, el paquete de señal de mantenimiento no está cifrado.

   Por lo tanto, el paquete enviado del Peer A al Peer B:

   Nota: El keepalive no está cifrado.

3. El par B ahora recibe una respuesta de keepalive GRE que no está encriptada en su interfaz física, pero debido al mapa criptográfico configurado en la interfaz física, espera un paquete encriptado y por lo tanto lo descarta.

Por lo tanto, aunque el Peer A responda a los kepailves y el Peer B del router reciba las respuestas, nunca las procesa y finalmente cambia el protocolo de línea de la interfaz de túnel al estado inactivo.

Resultado:

Los keepalives habilitados en el Peer B hacen que el estado del túnel en el Peer B cambie a up/down.

Escenario 2

Configuración:

- El Peer A utiliza Crypto Maps.
- El Peer B utiliza la Protección de Túnel.
- Las señales de mantenimiento están habilitadas en el Peer B.

- El cifrado IPSec se realiza en modo túnel.

En este escenario, dado que las señales de mantenimiento GRE se configuran en el Peer B, los eventos de secuencia cuando se genera una señal de mantenimiento son los siguientes:

1. El par B genera un paquete de señal de mantenimiento que es GRE encapsulado y luego cifrado por la protección del túnel en la interfaz del túnel y luego reenviado a la interfaz física.

   Paquete enviado desde el Peer B al Peer A:

2. En el Peer A, la señal de mantenimiento GRE se recibe descifrada:

   desencapsulado:

   Luego, el paquete de respuesta de señal de mantenimiento GRE interno se enruta en función de su dirección de destino, que es el Peer B. Esto significa que en el Peer A, el paquete se enruta inmediatamente de regreso fuera de la interfaz física al Peer B. Dado que el Peer A utiliza mapas criptográficos en la interfaz física, primero cifra este paquete antes de reenviarlo.

   Por lo tanto, el paquete enviado del Peer A al Peer B:

   Nota: La respuesta de keepalive está cifrada.

3. El par B ahora recibe una respuesta de señal de mantenimiento GRE cifrada cuyo destino se reenvía a la interfaz de túnel donde se descifra:

   Dado que el Tipo de Protocolo se establece en 0, el Peer B sabe que se trata de una respuesta de keepalive y la procesa como tal.

Resultado:

Las señales de mantenimiento habilitadas en el Peer B determinan correctamente cuál puede ser el estado del túnel en función de la disponibilidad del destino del túnel.

Escenario 3

Configuración:

- Ambos pares utilizan protección de túnel.

- Las señales de mantenimiento están habilitadas en el Peer B.
- El cifrado IPSec se realiza en modo túnel.

Este escenario es similar al Escenario 1 en que cuando el Peer A recibe el keepalive cifrado, lo descifra y desencapsula. Sin embargo, cuando la respuesta se reenvía hacia fuera, no se cifra ya que el Peer A utiliza protección de túnel en la interfaz de túnel. Por lo tanto, el Peer B descarta la respuesta de keepalive no encriptada y no la procesa.

Resultado:

Los keepalives habilitados en el Peer B hacen que el estado del túnel en el Peer B cambie a up/down.

Solución Aternativa

En tales situaciones donde los paquetes GRE deben ser cifrados, hay tres soluciones posibles:

1. Utilice un mapa criptográfico en el Peer A, la protección del túnel en el Peer B y habilite los keepalives en el Peer B.

   Dado que este tipo de configuración se utiliza principalmente en configuraciones de hub y spoke y dado que en tales configuraciones es más importante que el spoke conozca la disponibilidad de los hubs, la solución consiste en utilizar un mapa criptográfico dinámico en el hub (Peer A) y la protección de túnel en el spoke (Peer B) y habilitar señales de mantenimiento GRE en el spoke. De esta manera, aunque la interfaz de túnel GRE en el hub permanece activa, el vecino de ruteo y las rutas a través del túnel se pierden y se puede establecer la ruta alternativa. En el spoke, el hecho de que la interfaz de túnel se haya caído puede hacer que active una interfaz de marcador y llame nuevamente al hub (u otro router en el hub), luego establezca una nueva conexión.

2. Utilice señales de mantenimiento que no sean GRE para determinar la disponibilidad de pares.

   Si ambos routers están configurados con protección de túnel, las keeplives del túnel GRE no se pueden utilizar en ninguna dirección. En este caso, la única opción es utilizar el protocolo de ruteo u otro mecanismo, como el Agente de garantía de servicio, para descubrir si el par es alcanzable o no.

3. Utilice mapas criptográficos en Peer A y Peer B.

   Si ambos routers se configuran con mapas criptográficos, las señales de mantenimiento del túnel pueden atravesar en ambas direcciones y las interfaces de túnel GRE pueden apagarse en una o ambas direcciones y activar una conexión de respaldo. Esta es la opción más flexible.

Información Relacionada

- RFC 1701, encapsulación de router genérico (GRE)
- RFC 2890, extensiones de clave y número de secuencia a GRE
- keepalive de túnel de encapsulación de routing genérico (GRE)
- Fragmentación de IP y PMTUD
- Descripción General de los Mecanismos Keepalive en Cisco IOS
- Soporte Técnico - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).