Entender as manutenções de atividades de túnel GRE

Contents

Introduction

Este documento descreve o que são manutenções de atividades de Encapsulamento de Roteamento Genérico (GRE - Generic Routing Encapsulation) e como funcionam.

Túneis GRE

Um túnel GRE é uma interface lógica em um roteador Cisco que fornece uma maneira de encapsular pacotes de passageiros dentro de um protocolo de transporte. É uma arquitetura projetada para fornecer os serviços a fim de implementar um esquema de encapsulamento ponto-a-ponto.

Os túneis GRE são projetados para serem completamente stateless. Isso significa que cada endpoint de túnel não mantém nenhuma informação sobre o estado ou a disponibilidade do endpoint de túnel remoto. Uma consequência disso é que o roteador de ponto final de túnel local não tem a capacidade de desativar o protocolo de linha da interface de túnel GRE se a extremidade remota do túnel estiver inalcançável. A capacidade de marcar uma interface como inativa quando a extremidade remota do link não está disponível é usada para remover quaisquer rotas (especificamente rotas estáticas) na tabela de roteamento que usa essa interface como a interface de saída. Especificamente, se o protocolo de linha de uma interface for alterado para inativo, todas as rotas estáticas que apontam essa interface serão removidas da tabela de roteamento. Isso permite a instalação de uma rota estática alternativa (flutuante) ou de Roteamento Baseado em Políticas (PBR - Policy Based Routing) para selecionar um próximo salto alternativo ou uma interface.

Normalmente, uma interface de túnel GRE é ativada assim que é configurada e permanece ativa enquanto houver um endereço origem de túnel válido ou uma interface que esteja ativa. O

endereço IP destino do túnel também deve ser roteável. Isso é verdadeiro mesmo que o outro lado do túnel não tenha sido configurado. Isso significa que uma rota estática ou encaminhamento PBR de pacotes através da interface de túnel GRE permanece em vigor mesmo que os pacotes de túnel GRE não atinjam a outra extremidade do túnel.

Antes da implementação das manutenções de atividades de GRE, havia apenas maneiras de determinar problemas locais no roteador e nenhuma maneira de determinar problemas na rede interveniente. Por exemplo, o caso em que os pacotes em túnel GRE são encaminhados com êxito, mas são perdidos antes de alcançarem a outra extremidade do túnel. Tais cenários fariam com que os pacotes de dados que passam pelo túnel GRE fossem "black holed", mesmo que uma rota alternativa que usa PBR ou uma rota estática flutuante através de outra interface estivesse disponível. Os keepalives na interface do túnel GRE são usados para resolver esse problema da mesma forma que os keepalives são usados nas interfaces físicas.

> **Observação**: os keepalives de GRE não são suportados junto com a proteção de túnel IPsec em nenhuma circunstância. Este documento discute essa questão.

Como funcionam as manutenções de atividades de túnel

O mecanismo de keepalive de túnel GRE é semelhante aos keepalives PPP, pois dá a capacidade para que um lado origine e receba pacotes de keepalive de e para um roteador remoto, mesmo que o roteador remoto não suporte keepalives GRE. Como o GRE é um mecanismo de tunelamento de pacotes para tunelamento de IP dentro do IP, um pacote de túnel IP do GRE pode ser criado dentro de outro pacote de túnel IP do GRE. Para keepalives de GRE, o remetente pré-compila o pacote de resposta de keepalive dentro do pacote de solicitação de keepalive original, de modo que a extremidade remota só precise fazer o desencapsulamento de GRE padrão do cabeçalho IP de GRE externo e reverter o pacote de GRE IP interno para o remetente. Esses pacotes ilustram os conceitos de tunelamento IP, em que GRE é o protocolo de encapsulamento e IP é o protocolo de transporte. O protocolo passageiro também é IP (embora possa ser outro protocolo como Decnet, Internetwork Packet Exchange (IPX) ou Appletalk).

Pacote normal:

Cabeçalho IP	Cabeçalho TCP	Telnet

Pacote em túnel:

Cabeçalho IP	GRE	GRE	Cabeçalho IP	Cabeçalho TCP	Telnet

- IP é o protocolo de transporte.
- GRE é o protocolo de encapsulamento.
- IP é o protocolo de passageiros.

Este é um exemplo de um pacote keepalive que se origina do Roteador A e é destinado ao Roteador B. A resposta de keepalive que o Roteador B retorna ao Roteador A já está dentro do Cabeçalho IP Interno. O roteador B simplesmente desencapsula o pacote keepalive e o envia de volta para a interface física (S2). Ele processa o pacote de keepalive GRE como qualquer outro pacote de dados IP GRE.

Keepalives de GRE:

Cabeçalho IP GRE		GRE	Cabeçalho IP		GRE
Origem A	Destino B	PT=IP	Origem B	Destino A	PT=0

Esse mecanismo faz com que a resposta de keepalive encaminhe a interface física em vez da interface de túnel. Isso significa que o pacote de resposta keepalive do GRE não é afetado por nenhum recurso de saída na interface de túnel, como 'tunnel protection ...', QoS, Virtual Routing and Forwarding (VRF) e assim por diante.

> **Observação**: se uma ACL (Access Control List, lista de controle de acesso) de entrada na interface de túnel GRE estiver configurada, o pacote keepalive de túnel GRE enviado pelo dispositivo oposto deverá ser permitido. Caso contrário, o túnel GRE do dispositivo oposto será desativado. (**access-list** <number> **permit gre host** <tunnel-source> **host** <tunnel-destination>)

Outro atributo de keepalives de túnel GRE é que os temporizadores de keepalive em cada lado são independentes e não têm que coincidir, semelhante aos keepalives PPP.

> **Dica**: o problema com a configuração de keepalives somente em um lado do túnel é que somente o roteador que tem keepalives configurados marca sua interface de túnel como inativa se o temporizador keepalive expirar. A interface de túnel GRE no outro lado, onde keepalives não são configurados, permanece ativa mesmo se o outro lado do túnel estiver inativo. O túnel pode se tornar um buraco negro para pacotes direcionados para o túnel a partir do lado que não tinha keepalives configurados.

> **Dica**: em uma grande rede de túnel GRE hub-and-spoke, pode ser apropriado configurar apenas keepalives GRE no lado do spoke e não no lado do hub. Isso ocorre porque, muitas vezes, é mais importante que o spoke descubra que o hub está inacessível e, portanto, alterne para um caminho de backup (Backup de discagem, por exemplo).

Keepalives de túnel GRE

Com o Cisco IOS® Software Release 12.2(8)T, é possível configurar keepalives em uma interface de túnel GRE ponto a ponto. Com essa alteração, a interface do túnel é desativada dinamicamente se os keepalives falharem por um determinado período.

Para obter mais informações sobre como outras formas de keepalives funcionam, consulte Visão Geral dos Mecanismos de Keepalive no Cisco IOS.

> **Observação**: as manutenções de atividades de túnel GRE são suportadas apenas em túneis GRE ponto a ponto. Os keepalives de túnel são configuráveis em túneis GRE multiponto (mGRE), mas não têm efeito.

> **Observação**: em geral, os keepalives de túnel não podem funcionar quando os VRFs são usados na interface de túnel e o fVRF (‘tunnel vrf ...") e iVRF (‘ip vrf forwarding ...na interface do túnel) não correspondem. Isso é crítico no ponto final do túnel que "reflete" a manutenção de atividade de volta para o solicitante. Quando a solicitação de keepalive é

recebida, ela é recebida no fVRF e desencapsulada. Isso revela a resposta de keepalive pré-feita, que precisa ser encaminhada de volta ao remetente, MAS esse encaminhamento está no contexto do iVRF na interface do túnel. Portanto, se o iVRF e o fVRF não corresponderem, o pacote de resposta keepalive não será encaminhado de volta ao remetente. Isso é verdade mesmo se você substituir o iVRF e/ou o fVRF por "global".

Esta saída mostra os comandos que você usa para configurar keepalives em túneis 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 melhor como o mecanismo de keepalive do túnel funciona, considere este exemplo de topologia e configuração 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
```

Neste cenário, o Roteador A executa estas etapas:

1. Constrói o cabeçalho IP interno a cada cinco segundos onde:

   a origem é definida como o destino local do túnel, que é 192.168.1.2o destino é definido como a origem do túnel local, que é 192.168.1.1

   e um cabeçalho GRE é adicionado com um Tipo de Protocolo (PT) de 0

   Pacote gerado pelo Roteador A mas não enviado:

2. Envia esse pacote para fora de sua interface de túnel, o que resulta no encapsulamento do pacote com o cabeçalho IP externo, onde:

   a origem é definida como a origem local do túnel, que é 192.168.1.1o destino é definido como o destino do túnel local, que é 192.168.1.2

   e um cabeçalho GRE é adicionado com PT = IP.

   Pacote enviado do Roteador A para o Roteador B:

3. Incrementa o contador keepalive do túnel em um.

4. Supondo que haja uma maneira de alcançar o ponto final do túnel e que o protocolo de linha do túnel não esteja inativo devido a outros motivos, o pacote chega ao Roteador B. Em seguida, ele é comparado ao túnel 0, torna-se desencapsulado e é encaminhado ao IP destino, que é o endereço IP origem do túnel no roteador A.

   Enviado do roteador B para o roteador A:

5. Na chegada ao Roteador A, o pacote é desencapsulado e a verificação do PT resulta em 0. Isso significa que esse é um pacote keepalive. O contador de keepalive do túnel é redefinido para 0 e o pacote é descartado.

Se o Roteador B estiver inacessível, o Roteador A continuará a construir e enviar pacotes de keepalive, bem como tráfego normal. Se os keepalives não voltarem, o protocolo de linha de túnel permanecerá ativo, contanto que o contador de keepalive do túnel seja menor que o número de novas tentativas, que, neste caso, é quatro. Se essa condição não for verdadeira, na próxima vez que o Roteador A tentar enviar um keepalive para o Roteador B, o protocolo de linha será desativado.

> **Observação**: no estado ativo/inativo, o túnel não encaminha nem processa nenhum tráfego de dados. No entanto, ele continua a enviar pacotes de keepalive. Na recepção de uma resposta de keepalive, com a implicação de que o ponto final do túnel está novamente acessível, o contador de keepalive do túnel é redefinido para 0 e o protocolo de linha no túnel é ativado.

Para ver keepalives em ação, habilite **debug tunnel** e **debug tunnel keepalive**.

Exemplo de depurações do roteador 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 e Encaminhamento de caminho reverso unicast

O Unicast RPF (Unicast Reverse Path Forwarding) é um recurso de segurança que ajuda a detectar e descartar tráfego IP falsificado com uma validação do endereço origem do pacote na tabela de roteamento. Quando o RPF unicast é executado no modo estrito (**ip verify unicast source reachable-via rx), o pacote deve ser recebido na interface que o roteador usaria para encaminhar o pacote de retorno.** Se o modo estrito ou o modo solto RPF unicast estiver habilitado na interface de túnel do roteador que recebe os pacotes keepalive do GRE, os pacotes keepalives serão descartados pelo RPF após o desencapsulamento do túnel, já que a rota para o endereço de origem do pacote (endereço de origem do próprio roteador) não é através da interface de túnel. As quedas de pacotes RPF podem ser observadas na saída do **show ip traffic** da seguinte maneira:

```
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, o iniciador dos keepalives do túnel derruba o túnel devido aos pacotes de retorno de keepalives perdidos. Assim, o RPF unicast não deve ser configurado no modo estrito ou solto para que as manutenções de atividade do túnel GRE funcionem. Para obter mais informações sobre o Unicast RPF, consulte Entendendo o Unicast Reverse Path Forwarding.

Keepalives de IPsec e GRE

Túneis GRE com IPsec

Túneis GRE às vezes são combinados com IPsec porque o IPsec não suporta pacotes multicast IP. Por isso, os protocolos de roteamento dinâmico não podem ser executados com êxito em uma rede VPN IPsec. Como os túneis GRE suportam multicast IP, um protocolo de roteamento dinâmico pode ser executado em um túnel GRE. Os pacotes IP unicast GRE que resultam podem ser criptografados pelo IPsec.

Há duas maneiras diferentes de o IPsec criptografar pacotes GRE:

- Uma maneira é com o uso de um mapa de criptografia. Quando um mapa de criptografia é usado, ele é aplicado às interfaces físicas de saída para os pacotes de túnel GRE. Nesse caso, a sequência de etapas é a seguinte:

O pacote criptografado alcança a interface física.O pacote é descriptografado e encaminhado para a interface de túnel.O pacote é desencapsulado e encaminhado ao destino IP em texto claro.

- A outra maneira é usar a proteção de túnel. Quando a proteção de túnel é usada, ela é configurada na interface de túnel GRE. O comando tunnel protection tornou-se disponível no Cisco IOS Software Release 12.2(13)T. Nesse caso, a sequência de etapas é a seguinte:

  O pacote criptografado alcança a interface física.O pacote é encaminhado para a interface túnel.O pacote é descriptografado e desencapsulado e, em seguida, encaminhado ao destino IP em texto claro.

Ambos os métodos especificam que a criptografia IPsec seja executada após a adição do encapsulamento GRE. Há duas diferenças-chave entre quando você usa um mapa de criptografia e quando você usa a proteção de túnel:

- O mapa de criptografia IPsec está ligado à interface física e é verificado à medida que os pacotes são encaminhados para fora da interface física.

  O túnel GRE já encapsulou o pacote por este ponto.
- A proteção de túnel vincula a funcionalidade de criptografia ao túnel GRE e é verificada depois que o pacote é encapsulado, mas antes de ser entregue à interface física.

Problemas com manutenções de atividade ao combinar IPsec e GRE

Dadas as duas maneiras de adicionar criptografia aos túneis GRE, há três maneiras distintas de configurar um túnel GRE criptografado:

1. O peer A tem a proteção de túnel configurada na interface de túnel, enquanto o peer B tem o mapa de criptografia configurado na interface física.
2. O peer A tem o mapa de criptografia configurado na interface física, enquanto o peer B tem a proteção de túnel configurada na interface de túnel.
3. Ambos os Peers têm a proteção de túnel configurada na interface de túnel.

A configuração descrita nos cenários 1 e 2 é frequentemente feita em um design hub-and-spoke. A proteção de túnel é configurada no roteador de hub para reduzir o tamanho da configuração e um mapa de criptografia estático é usado em cada spoke.

Considere cada um desses cenários com keepalives GRE ativados no Peer B(spoke) e onde o modo de túnel é usado para criptografia.

Cenário 1

Configuração:

- O peer A usa a proteção de túnel.
- O Peer B usa mapas de criptografia.
- Keepalives são ativados no Peer B.

- A criptografia IPsec é feita no modo de túnel.

Neste cenário, como os keepalives de GRE são configurados no Peer B, os eventos de sequência quando um keepalive é gerado são os seguintes:

1. O peer B gera um pacote keepalive encapsulado em GRE e, em seguida, encaminha-o para a interface física, onde é criptografado e enviado para o destino do túnel, o peer A.

   Pacote enviado do Peer B para o Peer A:

2. No Peer A, o keepalive do GRE é recebido descriptografado:

   desencapsulado:

   Em seguida, o pacote interno de resposta de keepalive do GRE é roteado com base no endereço destino, que é o Peer B. Isso significa que no Peer A, o pacote é imediatamente roteado de volta para a interface física para o Peer B. Como o Peer A usa a proteção de túnel na interface de túnel, o pacote keepalive não é criptografado.

   Portanto, o pacote enviado do Peer A para o Peer B:

   Observação: o keepalive não é criptografado.

3. O Peer B agora recebe uma resposta de keepalive de GRE que não é criptografada em sua interface física, mas devido ao mapa de criptografia configurado na interface física, ele espera um pacote criptografado e, portanto, o descarta.

Portanto, mesmo que o Peer A responda aos keepilves e o Peer B do roteador receba as respostas, ele nunca as processará e, eventualmente, alterará o protocolo de linha da interface do túnel para o estado inativo.

Resultado:

Os keepalives ativados no Peer B fazem com que o estado do túnel no Peer B mude para up/down.

Cenário 2

Configuração:

- O Peer A usa mapas de criptografia.
- O peer B usa a proteção de túnel.
- Keepalives são ativados no Peer B.

- A criptografia IPsec é feita no modo de túnel.

Neste cenário, como os keepalives de GRE são configurados no Peer B, os eventos de sequência quando um keepalive é gerado são os seguintes:

1. O peer B gera um pacote keepalive encapsulado em GRE e depois criptografado pela proteção de túnel na interface de túnel e, em seguida, encaminhado à interface física.

   Pacote enviado do Peer B para o Peer A:

2. No Peer A, o keepalive do GRE é recebido descriptografado:

   desencapsulado:

   Em seguida, o pacote interno de resposta de keepalive do GRE é roteado com base no endereço destino, que é o Peer B. Isso significa que no Peer A, o pacote é imediatamente roteado de volta para a interface física para o Peer B. Como o Peer A usa mapas de criptografia na interface física, primeiro criptografa esse pacote antes de encaminhá-lo.

   Portanto, o pacote enviado do Peer A para o Peer B:

   Observação: a resposta do keepalive é criptografada.

3. O peer B agora recebe uma resposta de keepalive de GRE criptografado cujo destino é encaminhado para a interface de túnel onde é descriptografado:

   Como o Tipo de protocolo está definido como 0, o Peer B sabe que essa é uma resposta de keepalive e a processa como tal.

Resultado:

Os keepalives ativados no Peer B determinam com sucesso o estado do túnel com base na disponibilidade do destino do túnel.

Cenário 3

Configuração:

- Ambos os correspondentes usam a proteção de túnel.
- Keepalives são ativados no Peer B.
- A criptografia IPsec é feita no modo de túnel.

Esse cenário é semelhante ao Cenário 1, pois quando o Peer A recebe a manutenção de atividade criptografada, ele a descriptografa e a desencapsula. No entanto, quando a resposta é encaminhada de volta, ela não é criptografada, pois o peer A usa a proteção de túnel na interface do túnel. Assim, o Peer B descarta a resposta de keepalive não criptografada e não a processa.

Resultado:

Os keepalives ativados no Peer B fazem com que o estado do túnel no Peer B mude para up/down.

Solução

Em situações em que os pacotes GRE devem ser criptografados, há três soluções possíveis:

1. Use um mapa de criptografia no Peer A, proteja o túnel no Peer B e habilite keepalives no Peer B.

   Como esse tipo de configuração é usado principalmente em configurações hub-and-spoke e, como nessas configurações, é mais importante que o spoke esteja ciente da alcançabilidade dos hubs, a solução é usar um mapa de criptografia dinâmico no hub (Peer A) e a proteção de túnel no spoke (Peer B) e ativar keepalives GRE no spoke. Dessa forma, embora a interface do túnel GRE no hub permaneça ativa, o vizinho de roteamento e as rotas pelo túnel são perdidos e a rota alternativa pode ser estabelecida. No spoke, o fato de a interface do túnel ter sido desativada pode acioná-la para ativar uma interface do discador e retornar a chamada para o hub (ou outro roteador no hub), e então estabelecer uma nova conexão.

2. Use algo diferente de keepalives de GRE para determinar a acessibilidade do peer.

   Se ambos os roteadores forem configurados com proteção de túnel, os keeaplives de túnel GRE não poderão ser usados em nenhuma direção. Nesse caso, a única opção é usar o protocolo de roteamento ou outro mecanismo, como o Agente de Garantia de Serviço, para descobrir se o peer está acessível ou não.

3. Use mapas de criptografia nos Peers A e B.

   Se ambos os roteadores forem configurados com mapas de criptografia, os keepalives do túnel podem passar em ambas as direções e as interfaces do túnel GRE podem ser desligadas em uma ou ambas as direções e acionar uma conexão de backup a ser feita. Essa é a opção mais flexível.

Informações Relacionadas

- RFC 1701, Encapsulamento de roteador genérico (GRE)
- RFC 2890, extensões de números de sequência e chave para GRE
- Manutenção de atividade do túnel do Generic Routing Encapsulation (GRE)
- Fragmentação de IP e PMTUD

- Visão geral dos mecanismos de manutenção de atividade no Cisco IOS
- Suporte Técnico - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.