Keepalives do túnel GRE

Índice

[Introdução](#)
[Túneis GRE](#)
[Como os keepalives de túnel trabalham](#)
[Keepalives do túnel GRE](#)
[Manutenções de atividade de GRE e Unicast Reverse Path Forwarding](#)
[IPsec e manutenções de atividade de GRE](#)
[Túneis GRE com IPsec](#)
[Problemas com Keepalives quando você combinar o IPsec e o GRE](#)
[Cenário 1](#)
[Cenário 2](#)
[Cenário 3](#)
[Solução](#)
[Informações Relacionadas](#)

Introdução

Este documento explica o que o Keepalives do Generic Routing Encapsulation (GRE) é e como trabalha.

> Nota: As manutenções de atividade de GRE não são apoiadas junto com a proteção do túnel de IPsec em qualquer circunstância. Este documento discute esta edição.

Túneis GRE

Um túnel GRE é uma interface lógica em um roteador Cisco que forneça uma maneira de encapsular pacotes de passageiro dentro de um protocolo de transporte. É uma arquitetura projetada proporcionar os serviços a fim executar um esquema do encapsulamento de Point-to-Point.

Os túneis GRE são projetados ser completamente apátridas. Isto significa que cada ponto final de túnel não mantém nenhuma informação sobre o estado ou Disponibilidade do ponto final de túnel remoto. Uma consequência desta é que o roteador local do ponto final de túnel não tem a capacidade para derrubar o protocolo de linha da interface do túnel GRE se a extremidade remota do túnel é inacessível. A capacidade para marcar uma relação como quando a extremidade remota do link não está disponível é usada para baixo a fim remover todas as rotas (especificamente rotas estáticas) na tabela de roteamento que usarem essa relação como a interface externa. Especificamente, se o protocolo de linha para uma relação é mudado a para baixo, a seguir algumas rotas estáticas que indicarem que a relação está removida da tabela de roteamento. Isto permite a instalação de uma rota estática (de flutuação) alternativa ou o Policy Based Routing (PBR) a fim selecionar um salto seguinte ou uma relação alternativa.

Normalmente, uma interface do túnel GRE vem acima assim que estiver configurada e ficar acima

enquanto há um endereço ou uma relação válida de origem de túnel que estejam acima. O endereço IP de destino de túnel deve igualmente ser roteável. Isto é verdadeiro mesmo se o outro lado do túnel não foi configurado. Isto significa que uma rota estática ou um encaminhamento PBR de pacotes através da interface do túnel GRE permanecem de fato mesmo que os pacotes de túnel GRE não alcancem a outra extremidade do túnel.

Antes que as manutenções de atividade de GRE estiveram executadas, houve somente umas maneiras de não determinar edições locais no roteador e nenhuma maneira determinar problemas na rede de intervenção. Por exemplo, a caixa em que os pacotes tunelado de GRE são enviados com sucesso, mas é perdida antes que alcancem a outra extremidade do túnel. Tais encenações causariam os pacotes de dados que atravessam o túnel GRE ser “preto furado”, mesmo que uma rota alternativa que se use PBR ou uma Rota estática flutuante através de uma outra relação possa estar disponível. O Keepalives na interface do túnel GRE está usado a fim resolver da mesma forma esta edição enquanto o Keepalives é usado em interfaces física.

Como os keepalives de túnel trabalham

O mecanismo keepalive do túnel GRE é similar às manutenções de atividade de PPP que dá a capacidade para que um lado origine e receba pacotes keepalive a e de um roteador remoto mesmo se o roteador remoto não apoia manutenções de atividade de GRE. Desde que o GRE é um mecanismo de tunelamento do pacote para escavar um túnel o IP dentro do IP, um pacote do túnel IP GRE pode ser construído dentro de um outro pacote do túnel IP GRE. Para manutenções de atividade de GRE, os prebuilds do remetente o pacote da resposta de keepalive dentro do pacote de requisição do keepalive original de modo que as necessidades da extremidade remota somente de fazer o desencapsulamento GRE padrão do cabeçalho IP exterior GRE e de reverter então o pacote GRE interno IP ao remetente. Estes pacotes ilustram os conceitos de Tunelamento IP onde o GRE é o protocolo de encapsulamento e o IP é o protocolo de transporte. O protocolo de passageiro é igualmente IP (embora pode ser um outro protocolo como o DECNet, as Trocas de Pacote Entre Redes IPX (IPX), ou o APPLETALK).

Pacote normal:

Cabeçalho IP	Cabeçalho de TCP	Telnet

Pacote em túnel:

Cabeçalho IP	GRE	GRE	Cabeçalho IP	Cabeçalho de TCP	Telnet

- O IP é o protocolo de transporte.
- O GRE é o protocolo de encapsulamento.
- O IP é o protocolo de passageiro.

Aqui está um exemplo de um pacote keepalive que origine do roteador A e é destinado para o roteador B. A resposta de keepalive que o roteador B retorna ao roteador A é já dentro do cabeçalho IP interno. Os decapsulates do roteador B simplesmente o pacote keepalive e enviam-lhe para trás para fora a interface física (S2). Processa o pacote do GRE keepalive apenas como todo o outro pacote de dados IP GRE.

Manutenções de atividade de GRE:

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

Este mecanismo faz com que a resposta de keepalive envie para fora a interface física um pouco do que a interface de túnel. Isto significa que o pacote de resposta do GRE keepalive não está afetado por nenhuns **recursos de emissor na** interface de túnel, tal como do “a proteção túnel…”, o QoS, o roteamento virtual e a transmissão (VRF), e assim por diante.

> Nota: Se um Access Control List de entrada (ACL) na interface do túnel GRE é configurado, a seguir o pacote keepalive do túnel GRE que o dispositivo oposto envia deve ser permitido. Se não, o túnel GRE do dispositivo oposto estará para baixo. (`<tunnel-destination> do host do <tunnel-source> do host do gre da licença do <number> da lista de acesso`)

Um outro atributo do Keepalives do túnel GRE é que os temporizadores de keepalive em cada lado são independentes e não têm que combinar, similar às manutenções de atividade de PPP.

> Dica: O problema com a configuração do Keepalives somente em um lado do túnel é que somente o roteador que tem o Keepalives configurado marca sua interface de túnel como para baixo se o temporizador de keepalive expira. A interface do túnel GRE no outro lado, onde o Keepalives não é configurado, permanece acima mesmo se o outro lado do túnel está para baixo. O túnel pode assentar bem em um buraco negro para os pacotes dirigidos no túnel do lado que não teve o Keepalives configurado.

> Dica: Em uma grande rede do túnel GRE do Hub-and-Spoke, pôde ser apropriado configurar somente manutenções de atividade de GRE no lado de raio e não no lado de hub. Isto é porque é frequentemente mais importante para falou para descobrir que o hub é inacessível e comuta consequentemente a um caminho backup (Dial backup por exemplo).

Keepalives do túnel GRE

Com Cisco IOS ® Software libere 12.2(8)T, ele é possível para configurar o Keepalives em uma interface do túnel GRE ponto a ponto. Com esta mudança, a interface de túnel fechou dinamicamente se o Keepalives falha por um determinado período de tempo.

Para obter mais informações sobre de como outras formas de keepalive funcionam, refira a vista geral dos mecanismos keepalive no Cisco IOS.

> Nota: O Keepalives do túnel GRE é apoiado somente em túneis GRE pontos a ponto. Os keepalives de túnel são configuráveis em túneis multipontos GRE (mGRE) mas não têm nenhum efeito.

> Nota: Geralmente, os keepalives de túnel não trabalharão quando os VRF estão usados na interface de túnel e o fVRF (do “vrf túnel… ") e iVRF (“o vrf IP que envia…” na interface de túnel) não combine. Isto é crítico no ponto final de túnel que “reflete” o keepalive de volta ao solicitador. Quando o pedido do keepalive é recebido está recebido no fVRF e no descapsulado. Isto revela a resposta pré-fabricado do keepalive, que então as necessidades de ser enviado de volta ao remetente, MAS essa transmissão são no contexto do iVRF na interface de túnel. Consequentemente, se o iVRF e o fVRF não combinam então o pacote

de resposta do keepalive não é enviado de volta ao remetente. Isto é verdadeiro mesmo se você substitui o iVRF e/ou o fVRF com o “global”.

Esta saída mostra os comandos que você se usa a fim configurar o 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.
```

A fim compreender melhor como os trabalhos do mecanismo do keepalive de túnel, consideram estes exemplo de topologia de túnel e configuração:

Roteador 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.
```

roteador 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.
```

Nesta encenação, o roteador A executa estas etapas:

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

   a fonte é ajustada como o local o destino de túnel, que é 192.168.1.2o destino é ajustado como o origem de túnel local, que é 192.168.1.1

   e um cabeçalho de GRE é adicionado com um tipo de protocolo (PT) de 0

   O pacote gerou pelo roteador A mas não enviado:

2. Envia esse pacote fora de sua interface de túnel, que conduz ao encapsulamento do pacote com o cabeçalho IP exterior onde:

   a fonte é ajustada como o local o origem de túnel, que é 192.168.1.1o destino é ajustado como o destino de túnel local, que é 192.168.1.2

   e um cabeçalho de GRE é adicionado com PT = IP.

   O pacote enviou do roteador A ao roteador B:

3. Incrementa o contador do keepalive de túnel por um.

4. Com a suposição que há uma maneira de alcançar o ponto final de túnel da ponta oposta e o protocolo de linha do túnel não é abaixo de devido a outras razões, o pacote chega no roteador B. É combinado contra o tunnel0, transforma-se o descapsulado, e é enviado então ao IP de destino que é o endereço IP de Um ou Mais Servidores Cisco ICM NT do origem de túnel no roteador A.

   Enviado do roteador B ao roteador A:

5. Em cima da chegada no roteador A, o pacote transforma-se descapsulado e a verificação dos resultados PT em 0. Isto significa que este é um pacote keepalive. O contador do keepalive de túnel é restaurado então a 0 e o pacote é rejeitado.

Se o roteador B é inacessível, o roteador A continua a construir e enviar pacotes keepalive assim como o tráfego normal. Se o Keepalives não volta, o protocolo de linha do túnel fica acima enquanto o contador do keepalive de túnel é menos do que o número de novas tentativas, que é neste caso quatro. Se essa circunstância não é verdadeira, a seguir a próxima vez que o roteador A tenta enviar um keepalive ao roteador B, o protocolo de linha está derrubado.

Nota: No estado up/down, o túnel não envia nem processa nenhum tráfego de dados. Contudo, continua a enviar pacotes keepalive. Na recepção de uma resposta de keepalive, com a implicação que o ponto final de túnel é outra vez alcançável, o contador do keepalive de túnel é restaurado a 0, e o protocolo de linha no túnel vem acima.

A fim ver o Keepalives na ação, permita **debugam o túnel** e **debugam o keepalive de túnel**.

A amostra debuga 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
```

Manutenções de atividade de GRE e Unicast Reverse Path Forwarding

O unicast RPF (Unicast Reverse Path Forwarding) é uns recursos de segurança que as ajudas detectem e o tráfego IP falsificado da gota com uma validação do endereço de origem de pacote contra a tabela de roteamento. Quando o unicast RPF estiver executado no modo restrito (o **IP verifica a fonte do unicast alcançável-através do RX**), o pacote deve ser recebido na relação que o roteador usaria a fim enviar o pacote de informação de retorno. Se o modo restrito ou o unicast fraco RPF do modo são permitidos na interface de túnel do roteador que recebe os pacotes do GRE keepalive, a seguir os pacotes do Keepalives serão deixados cair pelo RPF após o decapsulation do túnel desde que a rota ao endereço de origem do pacote (endereço de origem de túnel do roteador próprio) não é através da interface de túnel. As quedas de pacote de informação RPF podem ser observadas no **tráfego da mostra IP** output como segue:

```
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
```

Em consequência, o iniciador dos keepalives de túnel derrubará o túnel devido aos pacotes de informação de retorno faltados do Keepalives. Assim o unicast RPF não deve ser configurado no modo restrito ou fraco para que o Keepalives do túnel GRE trabalhe. Para obter mais informações sobre do unicast RPF, refira compreendendo o Unicast Reverse Path Forwarding.

IPsec e manutenções de atividade de GRE

Túneis GRE com IPsec

Os túneis GRE são combinados às vezes com o IPsec porque o IPsec não apoia pacotes do Protocolo IP multicast. Devido a isto, os protocolos de roteamento dinâmico não podem ser executado com sucesso sobre uma rede do IPSec VPN. Desde que os túneis GRE apoiam o Protocolo IP multicast, um protocolo de roteamento dinâmico pode ser executado sobre um túnel GRE. Os pacotes do unicast IP GRE que o resultado pode ser cifrado pelo IPsec.

Há duas maneiras diferentes que o IPsec pode cifrar pacotes GRE:

- Uma maneira é com o uso de um **crypto map**. Quando um crypto map é usado, está aplicado à interface física de partida para os pacotes de túnel GRE. Neste caso, a sequência das etapas é como segue:

O pacote criptografado alcança a interface física.O pacote é decifrado e enviado à interface de túnel.O pacote é descapsulado e enviado então ao destino IP no texto claro.

- A outra maneira é usar a **proteção do túnel**. Quando a **proteção do túnel** é usada, está configurada na interface do túnel GRE. **O comando tunnel protection** tornou-se disponível no Cisco IOS Software Release 12.2(13)T. Neste caso, a sequência das etapas é como segue:

  O pacote criptografado alcança a interface física.O pacote é enviado à interface de túnel.O pacote é decifrado e descapsulado e enviado então ao destino IP no texto claro.

Ambos os métodos especificam que a criptografia IPSec está executada após a adição do encapsulamento de GRE. Há duas diferenças chave entre quando você usa um crypto map e quando você usa a proteção do túnel:

- O crypto map do IPsec está amarrado à interface física e verificado enquanto os pacotes são enviados para fora a interface física.

  O túnel GRE tem já o GRE encapsulou o pacote por este ponto.
- A proteção do túnel amarra a funcionalidade de criptografia ao túnel GRE e está verificada depois que o pacote é GRE encapsulado mas antes que o pacote esteja entregado à interface física.

Problemas com Keepalives quando você combinar o IPsec e o GRE

Dado as duas maneiras de adicionar a criptografia aos túneis GRE, há três maneiras distintas de estabelecer um túnel GRE cifrado:

1. Espreita A tem a proteção do túnel configurada na interface de túnel quando o par B tiver o crypto map configurado na interface física.
2. Espreita A tem o crypto map configurado na interface física quando o par B tiver a proteção do túnel configurada na interface de túnel.
3. Ambos os pares têm a proteção do túnel configurada na interface de túnel.

A configuração descrita nas encenações 1 e 2 é feita frequentemente em um projeto de hub-and-spoke. A proteção do túnel é configurada no roteador de hub a fim reduzir o tamanho da configuração e um mapa estático de criptografia é usado em cada spoke.

Considere cada um destas encenações com as manutenções de atividade de GRE permitidas no par B(spoke) e onde o modo de túnel é usado para a criptografia.

Cenário 1

Ajuste:

- Espreita uma proteção do túnel dos usos.
- O par B usa crypto map.
- O Keepalives é permitido no par B.
- A criptografia IPSec é feita no modo de túnel.

Nesta encenação, desde que as manutenções de atividade de GRE são configuradas no par B,

os eventos da sequência quando um keepalive é gerado são como segue:

1. O par B gerencie um pacote keepalive que seja GRE encapsulado e enviado então à relação phyiscal onde é cifrado e enviado sobre ao destino de túnel, o par A.

   O pacote enviou do par B para espreitar A:

2. No par A, o GRE keepalive é recebido decifrou:

   descapsulado:

   O pacote de resposta interno do GRE keepalive é distribuído então com base em seu endereço de destino que é o par B. Isso significa no par A, o pacote é distribuído imediatamente para trás para fora a interface física a espreitar B. Desde que os usos do par A escavam um túnel a proteção na **interface de túnel**, o pacote keepalive não é cifrado.

   Consequentemente, o pacote enviou do par A para espreitar B:

   Nota: O keepalive não é cifrado.

3. O par B recebe agora uma resposta do GRE keepalive que não seja cifrada em sua interface física, mas devido ao crypto map configurado na interface física, espera um pacote criptografado e deixa-o cair assim.

Consequentemente, mesmo que o par A responda aos keepailves e ao roteador de origem, o par B recebe as respostas, nunca processa-as e muda-o eventualmente o protocolo de linha da interface de túnel ao estado inativo.

Resultado:

O Keepalives permitido no par B faz com que o estado de túnel no par B mude a up/down.

Cenário 2

Ajuste:

- Espreitam os crypto map dos usos.
- Os usos do par B escavam um túnel a proteção.
- O Keepalives é permitido no par B.
- A criptografia IPSec é feita no modo de túnel.

Nesta encenação, desde que as manutenções de atividade de GRE onfigured no par B, os eventos da sequência quando um keepalive é gerado são como segue:

1. O par B gerencie um pacote keepalive que seja GRE encapsulado e cifrado então pela proteção do túnel na interface de túnel e enviado então à interface física.

   O pacote enviou do par B para espreitar A:

2. No par A, o GRE keepalive é recebido decifrou:

   descapsulado:

   O pacote de resposta interno do GRE keepalive é distribuído então com base em seu endereço de destino que é o par B. Isso significa no par A, o pacote é distribuído imediatamente para trás para fora a interface física a espreitar B. Desde que o par A usa crypto map na **interface física**, cifrará primeiramente este pacote antes que ele para a frente ele sobre.

   Consequentemente, o pacote enviou do par A para espreitar B:

   Nota: A resposta de keepalive é cifrada.

3. O par B recebe agora uma resposta cifrada do GRE keepalive cujo o destino seja enviado à interface de túnel onde é decifrado:

   Desde que o tipo de Protocal é ajustado a 0, o par B sabe que esta é uma resposta de keepalive e a processa como tal.

Resultado:

O Keepalives permitido no par B determina com sucesso o que o estado de túnel deve ser baseado na Disponibilidade do destino de túnel.

Cenário 3

Ajuste:

- Proteção do túnel do uso de ambos os pares.
- O Keepalives é permitido no par B.
- A criptografia IPSec é feita no modo de túnel.

Esta encenação é similar à encenação 1 naquela quando o par A recebe o keepalive cifrado, ele decifra e decapsulates ele. Contudo, quando a resposta é enviada para trás para fora, não é cifrada desde que os usos do par A escavam um túnel a proteção na **interface de túnel**. Assim, o

par B deixa cair a resposta de keepalive unencrypted e não a processa.

Resultado:

O Keepalives permitido no par B faz com que o estado de túnel no par B mude a up/down.

Solução

Em tais situações onde os pacotes GRE devem ser cifrados, há três soluções possíveis:

1. **Use um crypto map no par A, escave um túnel a proteção no par B, e permita o Keepalives no par B.**

   Desde que o este tipo de configuração é usado na maior parte em instalações do Hub-and-Spoke e porque em tais instalações é mais importante para falou para estar ciente da alcançabilidade do hub, a solução é usar um mapa cripto dinâmico no hub (par A) e proteção do túnel no spoke (par B) e para permitir manutenções de atividade de GRE no spoke. Esta maneira, embora a interface do túnel GRE no hub permaneçam acima, o vizinho de roteamento e as rotas através do túnel é perdida e a rota alternativa pode ser estabelecida. No spoke, o fato de que a interface de túnel foi para baixo pode provocá-la para trazer acima uma interface do discador e um retorno de chamada ao hub (ou a um outro roteador no hub), a seguir estabelece uma nova conexão.

2. **Use algo a não ser manutenções de atividade de GRE a fim determinar a alcançabilidade de peer**.

   Se ambo o Roteadores é configurado com proteção do túnel, a seguir os keeaplives do túnel GRE não podem ser usados em um ou outro sentido. Neste caso, a única opção é usar o protocolo de roteamento ou o outro mecanismo, tal como o Service Assurance Agent, a fim descobrir se o par é alcançável ou não.

3. **Use crypto map no par A e no par B.**

   Se ambo o Roteadores é configurado com crypto map, os keepalives de túnel podem obter completamente nos ambos sentidos e as interfaces do túnel GRE podem fechar no um ou outro ou em ambos sentidos e provocar uma conexão de backup a ser feita. Esta é a maioria de opção flexível.

Informações Relacionadas

- RFC 1701, Generic Router Encapsulation (GRE)
- RFC 2890, chave e Ramais do número de sequência ao GRE
- Keepalive do túnel de encapsulamento de roteamento genérico (GRE)
- Fragmentação de IP e PMTUD
- Vista geral dos mecanismos keepalive no Cisco IOS
- Suporte Técnico - Cisco Systems