Keepalives de tunnel GRE

Contenu

Introduction

Ce document explique ce qu'est le Keepalives d'Encapsulation de routage générique (GRE) et comment ils fonctionnent.

> Remarque: Le Keepalives GRE n'est pas pris en charge ainsi que le tunnel protection d'IPsec en toutes circonstances. Ce document traite de ce problème.

Tunnels GRE

Un tunnel GRE est une interface logique sur un routeur Cisco qui fournit une méthode d'encapsulation de paquets passagers au sein d'un protocole de transport. C'est une architecture conçue pour fournir les services afin d'implémenter un schéma point par point d'encapsulation.

Les tunnels GRE sont conçus pour être totalement sans état. Ceci signifie que chaque périphérique du tunnel ne garde aucune information sur l'état ou Disponibilité du périphérique du tunnel distant. Une conséquence de ceci est que le routeur local de périphérique du tunnel n'a pas la capacité de réduire la ligne protocole de l'interface de tunnel GRE si l'extrémité distante du tunnel est inaccessible. La capacité à marquer une interface comme désactivée quand l'extrémité distante de la liaison n'est pas disponible est utilisée afin de supprimer toutes les routes (spécifiquement les routes statiques) dans la table de routage qui utilisent cette interface comme interface de sortie. Spécifiquement, si le protocole de ligne pour une interface est modifié comme étant désactivé, toutes les routes statiques qui pointent vers cette interface sont supprimées de la table de routage. Ceci tient compte pour l'installation d'une artère statique (de flottement) alternative ou du Routage à base de règles (PBR) afin de sélectionner un prochain-saut ou une interface alternatif.

Normalement, une interface de tunnel GRE est activée dès qu'elle est configurée et elle le reste

tant qu'il y a une adresse source de tunnel valide ou une interface activée. L'adresse IP de destination du tunnel doit également être routable. Ceci est vrai même si l'autre côté du tunnel n'a pas été configuré. Cela signifie qu'une route statique ou le transfert PBR des paquets par l'intermédiaire de l'interface de tunnel GRE demeure effectif même si les paquets de tunnel GRE n'atteignent pas l'autre extrémité du tunnel.

Avant que le Keepalives GRE ait été mis en application, il y avait seulement des manières de déterminer les questions locales sur le routeur et aucun chemin de déterminer des problèmes dans le réseau intervenant. Par exemple, la caisse en laquelle le GRE a percé un tunnel des paquets sont avec succès expédiées, mais sont perdues avant qu'ils atteignent l'autre extrémité du tunnel. De tels scénarios entraîneraient les paquets de données qui passent par le tunnel GRE pour être « noir troué », quoiqu'une autre route qui l'utilise PBR ou une Route statique flottante par l'intermédiaire d'une autre interface pourrait être disponible. Les keepalives sur l'interface de tunnel GRE servent à résoudre ce problème de la même manière que les keepalives sont utilisés sur des interfaces physiques.

Fonctionnement des keepalives de tunnel

Le mécanisme de keepalive de tunnel GRE est semblable au Keepalives de PPP parce qu'il donne la capacité pour qu'un côté lance et de reçoit des paquets keepalive à et d'un routeur distant même si le routeur distant ne prend en charge pas le Keepalives GRE. Puisque GRE est un mécanisme de transmission tunnel de paquet pour la transmission tunnel IP à l'intérieur d'IP, un paquet de tunnel IP GRE peut être construit à l'intérieur d'un autre paquet de tunnel IP GRE. Pour le Keepalives GRE, les prebuilds d'expéditeur le paquet de réponse de keepalive à l'intérieur du paquet de demandes d'origine de keepalive de sorte que les besoins d'extrémité distante seulement de faire le décapsulage standard GRE de l'en-tête IP externe GRE et puis de retourner le paquet intérieur IP GRE à l'expéditeur. Ces paquets illustrent les concepts de transmission tunnel IP dans lesquels GRE est le protocole d'encapsulation et IP est le protocole de transport. Le protocole passager est également IP (bien que ce peut être un autre protocole comme le DECNet, l'Internetwork Packet Exchange (IPX), ou l'AppleTalk).

Paquet normal :

En-tête IP	En-tête de TCP	Telnet

Paquet percé un tunnel :

En-tête IP	GRE	GRE	En-tête IP	En-tête de TCP	Telnet

- IP est le protocole de transport.
- GRE est le protocole d'encapsulation.
- IP est le protocole passager.

Être un exemple d'un paquet keepalive qui provient du routeur A et voici est destiné au routeur B. La réponse de keepalive renvoyée par Routeur B à Routeur A est déjà à l'intérieur de l'en-tête IP interne. Routeur B désencapsule simplement le paquet keepalive et le renvoie par le biais de l'interface physique (S2). Il traite le paquet keepalive GRE comme n'importe quel autre paquet de données IP GRE.

Keepalives GRE :

En-tête IP GRE		GRE	En-tête IP		GRE
Source A	Destination B	PT=IP	Source B	Destination A	PT=0

Ce mécanisme fait en sorte que la réponse keepalive transfère l'interface physique plutôt que l'interface du tunnel. Ceci signifie que le paquet de réponse de keepalive GRE n'est affecté par aucune caractéristique de **sortie** sur l'interface de tunnel, telle que le « tunnel protection… », QoS, Virtual Routing and Forwarding (VRF), et ainsi de suite.

> Remarque: Si une liste de contrôle d'accès d'arrivée (ACL) sur l'interface de tunnel GRE est configurée, alors on doit permettre le paquet keepalive de tunnel GRE que le périphérique opposé envoie. Sinon, le tunnel GRE du périphérique opposé sera désactivé. (access-list <numéro> permit gre host <source_tunnel> host <destination_tunnel>)

Un autre attribut de Keepalives de tunnel GRE est que les temporisateurs de keepalive de chaque côté sont indépendants et ne doivent pas apparier, semblable au Keepalives de PPP.

> **Conseil** : Le problème lié à la configuration des keepalives d'un seul côté du tunnel est que seul le routeur pour lequel les keepalives sont configurés marque son interface de tunnel comme désactivée si le minuteur de keepalive expire. L'interface de tunnel GRE à l'autre extrémité, où les keepalives ne sont pas configurés, demeure active même si l'autre extrémité du tunnel est désactivée. Le tunnel peut devenir un trou noir pour les paquets dirigés dans le tunnel depuis l'extrémité où les keepalives n'ont pas été configurés.

> **Conseil** : Dans un grand réseau de tunnel GRE en étoile, il peut être préférable de configurer seulement les keepalives GRE du côté des rayons et non du côté du concentrateur. En effet, il est souvent plus important que le rayon détecte que le concentrateur est inaccessible et puisse basculer vers un chemin de secours (enregistrement d'appel, par exemple).

Keepalives de tunnel GRE

Avec le logiciel Cisco IOS® version 12.2(8)T, il est possible de configurer des keepalives sur une interface de tunnel GRE point à point. Avec cette modification, l'interface du tunnel s'arrête de manière dynamique si les keepalives échouent pendant une certaine durée.

Pour plus d'informations sur la façon dont d'autres formes de Keepalives fonctionnent, référez-vous à l'aperçu des mécanismes de keepalive sur le Cisco IOS.

> Remarque: les keepalives de tunnel GRE sont seulement pris en charge sur les tunnels GRE point à point. Les keepalives de tunnel sont configurables sur les tunnels multipoints GRE (mGRE) mais n'ont aucun effet.

> Remarque: Généralement le Keepalives de tunnel ne fonctionnera pas quand des vrf sont utilisés sur l'interface de tunnel et le fVRF (« tunnel vrf… ") et iVRF (« l'ip vrf forwarding… » sur l'interface de tunnel) n'appariez pas. C'est essentiel sur le périphérique du tunnel que « reflète » la keepalive de nouveau au demandeur. Quand la demande de keepalive est reçue elle est reçue dans le fVRF et désencapsulée. Ceci indique la réponse pré-faite de keepalive, qui puis les besoins d'être expédié de nouveau à l'expéditeur, MAIS cet expédition est dans le cadre de l'iVRF sur l'interface de tunnel. Par conséquent, si l'iVRF et

le fVRF ne s'assortissent pas alors le paquet de réponse de keepalive n'est pas expédié de nouveau à l'expéditeur. C'est vrai même si vous remplacez l'iVRF et/ou le fVRF par « global ».

Cette sortie montre les commandes que vous utilisez afin de configurer des keepalives sur des tunnels 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.
```

Afin de comprendre mieux comment les travaux de mécanisme de keepalive de tunnel, considèrent ces topologie et configuration de tunnel d'exemple :

routeur 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
```

routeur 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
```

Dans ce scénario, le routeur A exécute ces étapes :

1. Construit l'en-tête IP intérieure toutes les cinq secondes où :

la source est placée comme gens du pays la destination de tunnel, qui est 192.168.1.2la destination est placée comme source du tunnel locale, qui est 192.168.1.1

et une en-tête GRE est ajoutée avec un type de Protocol (pinte) de 0

Le paquet a généré par le routeur A mais non envoyé :

2. Envoie ce paquet hors de son interface de tunnel, qui a comme conséquence l'encapsulation du paquet avec l'en-tête IP externe où :

   la source est placée comme gens du pays la source du tunnel, qui est 192.168.1.1la destination est placée comme destination locale de tunnel, qui est 192.168.1.2

   et une en-tête GRE est ajoutée avec pinte = IP.

   Le paquet a envoyé du routeur A au routeur B :

3. Incrémente la keepalive de tunnel contre- par une.

4. En supposant qu'il y a une façon d'atteindre le point de terminaison du tunnel lointain et que le protocole de ligne de tunnel n'est pas désactivé pour d'autres raisons, le paquet parvient au Routeur B. Il est alors apparié contre le tunnel 0, devient désencapsulé, et est expédié à l'IP de destination qui est l'adresse IP de source du tunnel sur le routeur A.

   Envoyé du routeur B au routeur A :

5. Sur l'arrivée sur le routeur A, le paquet devient désencapsulé et le contrôle des résultats pinte dans 0. Cela signifie qu'il s'agit d'un paquet keepalive. Le compteur de keepalives de tunnel est alors réinitialisé à 0 et le paquet est ignoré.

Si le routeur B est inaccessible, le routeur A continue à construire et envoyer les paquets keepalive aussi bien que le trafic normal. Si le Keepalives ne revient pas, la ligne protocole de tunnel reste tant que le compteur de keepalive de tunnel est moins que le nombre de relances, qui est dans ce cas quatre. Si cette condition n'est pas remplie, la prochaine fois que Routeur A tente d'envoyer un keepalive à Routeur B, le protocole de ligne est désactivé.

> Remarque: À l'état actif/inactif, le tunnel ne transfère ou ne traite aucun trafic de données. Cependant, il continue à envoyer des paquets keepalives. Sur la réception d'une réponse de keepalive, avec l'implication que le périphérique du tunnel est de nouveau accessible, le compteur de keepalive de tunnel est remis à l'état initial à 0, et la ligne protocole sur le tunnel est soulevée.

Afin de voir le Keepalives dans l'action, l'enable **mettent au point le tunnel** et **mettent au point la keepalive de tunnel**.

L'échantillon met au point du routeur 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 et Unicast Reverse Path Forwarding GRE

Unicast RPF (Unicast Reverse Path Forwarding) est une fonctionnalité de sécurité que les aides détectent et le trafic IP charrié par baisse avec une validation de l'adresse source de paquet contre la table de routage. Quand Unicast RPF est exécuté en mode strict (**rx d'ip verify unicast source reachable-via**), le paquet doit être reçu sur l'interface que le routeur avait l'habitude afin d'expédier le paquet de retour. Si le mode strict ou le mode lâche Unicast RPF est activé sur l'interface de tunnel du routeur qui reçoit les paquets keepalive GRE, alors les paquets de Keepalives seront lâchés par RPF après décapsulage de tunnel puisque l'artère à l'adresse source du paquet (la propre adresse de source du tunnel du routeur) n'est pas par l'interface de tunnel. On peut observer des pertes de paquets RPF dans le **show ip traffic** sorti comme suit :

```
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
```

En conséquence, le demandeur du Keepalives de tunnel réduira au tunnel dû au Keepalives manqué les paquets de retour. Ainsi Unicast RPF ne doit pas être configuré en mode strict ou lâche pour que le Keepalives de tunnel GRE fonctionne. Pour plus d'informations sur Unicast RPF, référez-vous compréhension derrière l'Unicast Reverse Path Forwarding.

IPsec et Keepalives GRE

Tunnels GRE avec IPsec

Des tunnels GRE sont parfois combinés avec IPsec parce qu'IPsec ne prend en charge pas des paquets de Protocole IP Multicast. Pour cette raison, les protocoles de routage dynamique ne peuvent pas fonctionner avec succès au-dessus d'un réseau VPN d'IPsec. Puisque les tunnels GRE prennent en charge Multicast IP, un protocole de routage dynamique peut être exécuté sur un tunnel GRE. Les paquets d'unicast sur IP GRE que le résultat peut être chiffré par IPsec.

Il y a deux manières différentes qu'IPsec peut chiffrer des paquets GRE :

- Une manière est avec l'utilisation d'un **crypto map**. Quand un crypto map est utilisé, il est appliqué à l'interface physique sortante pour les paquets de tunnel GRE. Dans ce cas, l'ordre des étapes est comme suit :

  Le paquet chiffré atteint l'interface physique.Le paquet est déchiffré et expédié à l'interface de tunnel.Le paquet est désencapsulé et puis expédié à la destination IP en texte clair.

- L'autre manière est d'utiliser le **tunnel protection**. Quand la **protection de tunnel** est utilisée, elle est configurée sur l'interface de tunnel GRE. La commande **tunnel protection** est devenue disponible dans le logiciel Cisco IOS version 12.2(13)T. Dans ce cas, l'ordre des étapes est

comme suit :

Le paquet chiffré atteint l'interface physique.Le paquet est expédié à l'interface de tunnel.Le paquet est déchiffré et désencapsulé et puis expédié à la destination IP en texte clair.

Les deux méthodes spécifient que le cryptage d'IPsec est exécuté après l'ajout de l'encapsulation GRE. Il y a deux différences principales entre quand vous utilisez un crypto map et quand vous utilisez le tunnel protection :

- Le crypto map d'IPsec est attaché à l'interface physique et est vérifié pendant que des paquets sont expédiés l'interface physique.

  àce stade, le tunnel GRE a déjà effectué une encapsulation GRE du paquet.
- La protection de tunnel lie la fonctionnalité de chiffrement au tunnel GRE et est vérifiée après l'encapsulation GRE du paquet mais avant que le paquet soit remis à l'interface physique.

Problèmes avec le Keepalives quand vous combinez IPsec et GRE

Etant donné les deux manières d'ajouter le cryptage aux tunnels GRE, il y a trois manières distinctes d'installer un tunnel chiffré GRE :

1. Scrutent A a le tunnel protection configuré sur l'interface de tunnel tandis que le pair B a le crypto map configuré sur l'interface physique.
2. Scrutent A a le crypto map configuré sur l'interface physique tandis que le pair B a le tunnel protection configuré sur l'interface de tunnel.
3. Les deux pairs ont le tunnel protection configuré sur l'interface de tunnel.

La configuration décrite dans les scénarios 1 et 2 sont souvent faites dans une conception d'en étoile. La protection de tunnel est configurée sur le routeur concentrateur afin de réduire la taille de la configuration et une carte de chiffrement statique est utilisée sur chaque rayon.

Considérez chacun de ces scénarios avec le Keepalives GRE activé sur le pair B(spoke) et où le tunnel mode est utilisé pour le cryptage.

Scénario 1

Établissement :

- Scrutent un tunnel protection d'utilisations.
- Le pair B utilise des crypto map.
- Le Keepalives est activé sur le pair B.
- Le cryptage d'IPsec est fait dans le tunnel mode.

Dans ce scénario, puisque le Keepalives GRE est configuré sur le pair B, les événements d'ordre quand une keepalive est générée sont comme suit :

1. Le pair B génère un paquet keepalive qui est GRE encapsulé et alors expédié à l'interface phyiscal où il est chiffré et envoyé en fonction à la destination de tunnel, le pair R.

   Le paquet a envoyé du pair B pour scruter A :

2. Au pair A, la keepalive GRE est reçue a déchiffré :

   désencapsulé :

   Alors le paquet intérieur de réponse de keepalive GRE est conduit a basé sur son adresse de destination qui est le pair B. Cela signifie sur le pair A, le paquet est immédiatement conduit soutiennent l'interface physique à scruter B. Puisque le pair A utilise le tunnel protection sur l'**interface de tunnel**, le paquet keepalive n'est pas chiffré.

   Par conséquent, le paquet a envoyé du pair A pour scruter B :

   Remarque: La keepalive n'est pas chiffrée.

3. Le pair B reçoit maintenant une réponse de keepalive GRE qui n'est pas chiffrée sur son interface physique, mais en raison du crypto map configuré sur l'interface physique, elle attend un paquet chiffré et le relâche ainsi.

Par conséquent, quoique le pair A réponde aux keepailves et au routeur d'origine, le pair B reçoit les réponses, il ne les traitent jamais et changent par la suite la ligne protocole de l'interface de tunnel à l'état d'indisponibilité.

Résultat :

Le Keepalives activé sur le pair B fait changer l'état du tunnel sur le pair B à haut/bas.

Scénario 2

Établissement :

- Scrutent les crypto map d'utilisations.
- Le pair B utilise le tunnel protection.
- Le Keepalives est activé sur le pair B.
- Le cryptage d'IPsec est fait dans le tunnel mode.

Dans ce scénario, puisque le Keepalives GRE onfigured sur le pair B, les événements d'ordre quand une keepalive est générée sont comme suit :

1. Le pair B génère un paquet keepalive qui est GRE encapsulé et alors chiffré par le tunnel protection sur l'interface de tunnel et alors expédié à l'interface physique.

   Le paquet a envoyé du pair B pour scruter A :

2. Au pair A, la keepalive GRE est reçue a déchiffré :

   désencapsulé :

   Alors le paquet intérieur de réponse de keepalive GRE est conduit a basé sur son adresse de destination qui est le pair B. Cela signifie sur le pair A, le paquet est immédiatement conduit soutiennent l'interface physique à scruter B. Puisque le pair A utilise des crypto map sur l'**interface physique**, elle chiffrera d'abord ce paquet avant qu'il en avant il en fonction.

   Par conséquent, le paquet a envoyé du pair A pour scruter B :

   Remarque: La réponse de keepalive est chiffrée.

3. Le pair B reçoit maintenant une réponse chiffrée de keepalive GRE dont la destination est expédiée à l'interface de tunnel où elle est déchiffrée :

   Puisque le type de Protocal est placé à 0, le pair B sait que c'est une réponse de keepalive et la traite en soi.

Résultat :

Le Keepalives activé sur le pair B détermine avec succès ce que l'état du tunnel devrait être basé sur la Disponibilité de la destination de tunnel.

Scénario 3

Établissement :

- Tunnel protection d'utilisation de les deux pairs.
- Le Keepalives est activé sur le pair B.
- Le cryptage d'IPsec est fait dans le tunnel mode.

Ce scénario est semblable au scénario 1 dans cela quand le pair A reçoit la keepalive chiffrée, il le déchiffre et désencapsule. Cependant, quand la réponse est expédiée soutiennent, il n'est pas chiffré puisque le pair A utilise le tunnel protection sur l'**interface de tunnel**. Ainsi, le pair B relâche la réponse décryptée de keepalive et ne la traite pas.

Résultat :

Le Keepalives activé sur le pair B fait changer l'état du tunnel sur le pair B à haut/bas.

Contournement

Dans de telles situations où les paquets GRE doivent être chiffrés, il y a trois solutions possibles :

1. **Utilisez un crypto map sur le pair A, le tunnel protection sur le pair B, et le Keepalives d'enable sur le pair B.**

   Puisque ce type de configuration est en grande partie utilisé dans des installations d'en étoile et parce que dans de telles installations il est plus important pour a parlé pour se rendre compte de l'accessibilité du hub, la solution est d'utiliser une crypto-carte dynamique sur le hub (pair A) et tunnel protection sur le rai (pair B) et Keepalives d'enable GRE sur le rai. De cette façon, bien que l'interface de tunnel GRE sur le hub demeure, le voisin de routage et les artères par le tunnel sont perdues et l'autre route peut être établie. Sur le rayon, le fait que l'interface du tunnel a été désactivée peut provoquer l'appel d'une interface de numérotation et un rappel au concentrateur (ou à un routeur différent au concentrateur), puis l'établissement d'une nouvelle connexion.

2. **Employez quelque chose autre que le Keepalives GRE afin de déterminer l'accessibilité de pair**.

   Si les deux Routeurs sont configurés avec le tunnel protection, alors des keeaplives de tunnel GRE ne peuvent pas être utilisés dans l'un ou l'autre de direction. Dans ce cas, la seule option est d'employer le protocole de routage ou tout autre mécanisme, tel que le Service Assurance Agent (SAA), afin de la découvrir si le pair est accessible ou pas.

3. **Utilisez les crypto map sur le pair A et le pair B.**

   Si les les deux les Routeurs sont configurés avec des crypto map, le Keepalives de tunnel peut obtenir dans les deux directions et les interfaces de tunnel GRE peuvent s'arrêter dans le l'un ou l'autre ou des directions et déclencher une connexion de sauvegarde à faire. Il s'agit de l'option la plus flexible.

Informations connexes

- RFC 1701, Generic Router Encapsulation (GRE)
- RFC 2890, Extensions de clé et de numéro de séquence à GRE
- Keepalive de tunnel GRE (Generic Routing Encapsulation)
- Fragmentation IP et PMTUD
- Aperçu des mécanismes de keepalive sur le Cisco IOS
- Support technique - Cisco Systems