Comprendre les keepalives de tunnel GRE

Table des matières

Introduction

Tunnels GRE

Fonctionnement des keepalives de tunnel

Keepalives de tunnel GRE

GRE Keepalive et Unicast Reverse Path Forwarding

Keepalives IPsec et GRE

- Tunnels GRE avec IPsec
- Problèmes de messages de test d'activité lorsque vous combinez IPsec et GRE
  - Scénario 1
  - Scénario 2
  - Scénario 3
- Solution de contournement

Informations connexes

Introduction

Ce document décrit ce que sont les keepalives GRE (Generic Routing Encapsulation) et comment ils fonctionnent.

Tunnels GRE

Un tunnel GRE est une interface logique sur un routeur qui fournit un moyen d'encapsuler des paquets de protocole réseau à l'intérieur d'un protocole de transport. Il s’agit d’un mécanisme qui assure le transport du trafic réseau sur un schéma d’encapsulation point à point.

Les tunnels GRE sont conçus pour être complètement sans état. Cela signifie que chaque point de terminaison du tunnel ne conserve aucune information sur l'état ou la disponibilité du point de terminaison du tunnel distant. En conséquence, le routeur du point d'extrémité du tunnel local n'a pas la capacité d'arrêter le protocole de ligne de l'interface du tunnel GRE si l'extrémité distante du tunnel est inaccessible. La possibilité de marquer une interface comme inactive lorsque l’extrémité distante de la liaison n’est pas disponible est utilisée afin de supprimer toutes les routes (en particulier les routes statiques) de la table de routage qui utilisent cette interface comme interface sortante. En particulier, si le protocole de ligne d’une interface passe à down, toutes les routes statiques qui indiquent cette interface sont supprimées de la table de routage. Cela permet l'installation d'une route statique alternative (flottante) ou d'un PBR (Policy Based Routing) afin de sélectionner un saut suivant ou une interface alternative.

Normalement, une interface de tunnel GRE apparaît dès qu'elle est configurée et reste active tant qu'il y a une adresse source de tunnel valide ou une interface source de tunnel qui est dans un état up. 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 un transfert PBR de paquets via l'interface de tunnel GRE reste en vigueur même si les paquets de tunnel GRE ne peuvent pas atteindre l'autre extrémité du tunnel.

Avant l'implémentation des keepalives GRE, il n'y avait que des moyens de désactiver une interface de tunnel en raison de problèmes locaux sur le routeur, et non en raison de problèmes dans le réseau de transport. Par exemple, le cas où les paquets en tunnel GRE sont transférés avec succès, mais sont perdus avant d'atteindre l'autre extrémité du tunnel. De tels scénarios entraîneraient la présence de « trous noirs » dans les paquets de données qui passent par le tunnel GRE, même si une autre route utilisant PBR ou une route statique flottante via une autre interface est disponible. Les keepalives sur l'interface de tunnel GRE sont utilisés afin de résoudre ce problème de la même manière que les keepalives sont utilisés sur les interfaces physiques.

Remarque : Les keepalives GRE ne sont pris en charge avec la protection de tunnel IPsec en aucune circonstance. Ce document traite de cette question.

Fonctionnement des keepalives de tunnel

Le mécanisme de keepalive de tunnel GRE est similaire aux keepalives PPP en ce qu'il permet à un côté d'émettre et de recevoir des paquets keepalive vers et depuis un routeur distant même si le routeur distant ne prend pas en charge les keepalives GRE. Puisque GRE est un mécanisme de tunneling de paquets pour le tunneling IP dans IP, un paquet de tunnel IP GRE peut être construit dans un autre paquet de tunnel IP GRE. Pour les keepalives GRE, l'expéditeur préconstruit le paquet de réponse keepalive à l'intérieur du paquet de demande de keepalive d'origine de sorte que l'extrémité distante n'ait besoin que d'effectuer une décapsulation GRE standard de l'en-tête IP GRE externe, puis de renvoyer le paquet GRE IP interne à l'expéditeur. Ces paquets illustrent les concepts de tunnellisation IP où GRE est le protocole d'encapsulation et IP le protocole de transport. Le protocole passager est également IP (bien qu'il puisse s'agir d'un autre protocole comme NHRP).

Paquet normal :

En-tête IP	En-tête TCP	Telnet

Paquet tunnelisé :

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

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

Voici un exemple de paquet keepalive qui provient du routeur A et est destiné au routeur B. La réponse de test d'activité que le routeur B renvoie au routeur A se trouve déjà dans l'en-tête IP interne. Le routeur B décapsule simplement le paquet keepalive et le renvoie à 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 entraîne le transfert de la réponse de test d'activité à l'interface physique plutôt qu'à l'interface de tunnel. Cela signifie que le paquet de réponse de keepalive GRE n'est pas affecté par les fonctionnalités de sortie sur l'interface de tunnel, telles que la « protection de tunnel ... » QoS, VRF (Virtual Routing and Forwarding), etc.

Remarque : Si une liste de contrôle d'accès (ACL) entrante sur l'interface de tunnel GRE est configurée, alors le paquet de maintien de la connexion du tunnel GRE que le périphérique opposé envoie doit être autorisé. Si ce n'est pas le cas, le tunnel GRE du périphérique opposé est désactivé. (**`access-list <number> permit gre host <tunnel-source> host <tunnel-destination>`**)

Un autre attribut des keepalives de tunnel GRE est que les minuteurs de keepalive de chaque côté sont indépendants et n'ont pas à correspondre, comme les keepalives PPP.

Conseil : Le problème avec la configuration des keepalives seulement d'un côté du tunnel est que seul le routeur qui a des keepalives configurés marque son interface de tunnel comme étant hors service si le compteur de keepalive expire. L'interface de tunnel GRE de l'autre côté, où les keepalives ne sont pas configurés, reste active même si l'autre côté du tunnel est en panne. Le tunnel peut devenir un trou noir pour les paquets dirigés dans le tunnel depuis le côté où aucun keepalive n'a été configuré.

Conseil : Dans un grand réseau de tunnels GRE hub-and-spoke, il peut être approprié de configurer uniquement des keepalives GRE du côté du rayon et non du côté du concentrateur. En effet, il est souvent plus important pour le rayon de découvrir que le concentrateur est inaccessible et donc de commuter vers un chemin de secours, par exemple, à l'aide d'une interface cellulaire de secours.

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 ce changement, l'interface du tunnel s'arrête dynamiquement si les keepalives échouent pendant un certain temps.

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

Remarque : Les keepalives de tunnel GRE sont uniquement 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 : En général, les keepalives de tunnel ne peuvent pas fonctionner quand les VRF sont utilisés sur l'interface de tunnel et que les fVRF (tunnel vrf ...) et iVRF (ip vrf forwarding ... sur l'interface de tunnel) ne correspondent pas. Ceci est essentiel sur le point d'extrémité du tunnel qui reflète le keepalive de retour au demandeur. Lorsque la demande de test d'activité est reçue, elle est reçue dans le fVRF et décapsulée. Ceci révèle la réponse keepalive pré-faite, qui doit ensuite être retransmise à l'expéditeur, MAIS que la transmission est dans le contexte de l'iVRF sur l'interface de tunnel. Par conséquent, si l'iVRF et le fVRF ne correspondent pas, le paquet de réponse keepalive n'est pas renvoyé à l'expéditeur. Cela est vrai même si vous remplacez iVRF et/ou fVRF par global.

Ce résultat montre les commandes que vous utilisez afin de configurer des keepalives sur les 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 mieux comprendre le fonctionnement du mécanisme de keepalive du tunnel, examinez cet exemple de topologie et de configuration de tunnel :



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 effectue les étapes suivantes :

- La source est définie comme la destination locale du tunnel, qui est 192.168.1.2
- La destination est définie comme source de tunnel locale, à savoir 192.168.1.1, et
- Construit l'en-tête IP interne toutes les cinq secondes où un en-tête GRE est ajouté avec un type de protocole (PT) de 0.

Paquet généré par le routeur A mais non envoyé :

En-tête IP		GRE
Source : 192.168.1.2	Destination : 192.168.1.1	PT=0

Envoie ce paquet hors de son interface de tunnel, ce qui entraîne l'encapsulation du paquet avec l'en-tête IP externe où :

- La source est définie comme la source locale du tunnel, qui est 192.168.1.1
- La destination est définie comme destination du tunnel local, à savoir 192.168.1.2, et
- Un en-tête GRE est ajouté avec PT = IP.

Paquet envoyé du routeur A au routeur B :

En-tête IP GRE		GRE	En-tête IP		GRE
Source : 192.168.1.1	Destination : 192.168.1.2	PT=IP	Source : 192.168.1.2	Destination : 192.168.1.1	PT=0

- Incrémente le compteur de keepalive du tunnel d'une unité.
- En supposant qu'il existe un moyen d'atteindre le point d'extrémité du tunnel distant et que le protocole de ligne du tunnel n'est pas désactivé pour d'autres raisons, le paquet arrive sur le routeur B. Il est ensuite mis en correspondance avec le tunnel 0, est décapsulé et transmis à l'adresse IP de destination, qui est l'adresse IP source du tunnel sur le routeur A.

Envoyé du routeur B au routeur A :

En-tête IP		GRE
Source : 192.168.1.2	Destination : 192.168.1.1	PT=0

- À l'arrivée sur le routeur A, le paquet est décapsulé et la vérification du PT donne 0. Cela signifie qu'il s'agit d'un paquet de test d'activité. Le compteur de keepalive du tunnel est alors réinitialisé à 0 et le paquet est rejeté.

Si le routeur B est inaccessible, le routeur A continue à construire et à envoyer des paquets de test d'activité ainsi que du trafic normal. Si les keepalives ne reviennent pas, le protocole de ligne de tunnel reste actif tant que le compteur de keepalive du tunnel est inférieur au nombre de nouvelles tentatives, qui dans ce cas est de quatre. Si cette condition n'est pas vraie, le protocole de ligne est désactivé la prochaine fois que le routeur A tente d'envoyer un keepalive au routeur B.

Remarque : Dans l'état up/down, le tunnel ne transfère ni ne traite aucun trafic de données. Cependant, il continue d'envoyer des paquets keepalive. À la réception d'une réponse de test d'activité, avec l'implication que le point d'extrémité du tunnel est à nouveau accessible, le compteur de test d'activité du tunnel est remis à 0 et le protocole de ligne sur le tunnel s'active.

Afin de voir les keepalive en action, activez debug tunnel et debug tunnel keepalive.

Exemples de débogages 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
```

GRE Keepalive et Unicast Reverse Path Forwarding

Unicast RPF (Unicast Reverse Path Forwarding) est une fonctionnalité de sécurité qui permet de détecter et d'abandonner le trafic IP usurpé avec une validation de l'adresse source du paquet par rapport à la table de routage. Lorsque Unicast RPF est exécuté en mode strict (ip verify unicast source reachable-via rx), le paquet doit être reçu sur l'interface que le routeur utiliserait afin de transférer 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 de test d'activité GRE, alors les paquets de test d'activité sont abandonnés par RPF après la décapsulation du tunnel puisque la route vers l'adresse source du paquet (adresse source du tunnel propre au routeur) n'est pas à travers l'interface de tunnel. Les abandons de paquets RPF peuvent être observés dans le résultat de la commande show ip traffic 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
```

Par conséquent, l'initiateur des keepalives du tunnel désactive le tunnel en raison de paquets de retour de keepalives manqués. Par conséquent, Unicast RPF ne doit pas être configuré en mode strict ou lâche pour que les keepalives de tunnel GRE fonctionnent. Pour plus d'informations sur Unicast RPF, référez-vous à Présentation du transfert de chemin inverse de monodiffusion.

Keepalives IPsec et GRE

Tunnels GRE avec IPsec

Les tunnels GRE sont parfois associés à IPsec, car IPsec ne prend pas en charge les paquets de multidiffusion IP. Pour cette raison, les protocoles de routage dynamique ne peuvent pas s'exécuter correctement sur un réseau VPN IPsec. Puisque les tunnels GRE prennent en charge la multidiffusion IP, un protocole de routage dynamique peut être exécuté sur un tunnel GRE. Les paquets de monodiffusion IP GRE qui en résultent peuvent être chiffrés par IPsec.

IPsec peut chiffrer les paquets GRE de deux manières différentes :

- Une méthode consiste à utiliser une crypto-carte. Lorsqu'une crypto-carte est utilisée, elle est appliquée aux interfaces physiques sortantes pour les paquets de tunnel GRE. Dans ce cas, la séquence d'étapes est la suivante :

    1. Le paquet chiffré atteint l’interface physique.
    2. Le paquet est décrypté et transmis à l'interface du tunnel.
    3. Le paquet est décapsulé, puis transmis à la destination IP en texte clair.

- L'autre méthode consiste à utiliser la protection du tunnel. Lorsque 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, la séquence d'étapes est la suivante :

    1. Le paquet chiffré atteint l’interface physique.
    2. Le paquet est transmis à l’interface du tunnel.
    3. Le paquet est décrypté et décapsulé, puis transmis à la destination IP en texte clair.

Les deux méthodes spécifient que le chiffrement IPsec est effectué après l'ajout de l'encapsulation GRE. Il existe deux différences clés entre l'utilisation d'une crypto-carte et l'utilisation de la protection de tunnel :

- La crypto-carte IPsec est liée à l'interface physique et est vérifiée au fur et à mesure que les

paquets sont transférés à l'interface physique. Le tunnel GRE a déjà encapsulé le paquet par ce point.
- La protection de tunnel lie la fonctionnalité de chiffrement au tunnel GRE et est vérifiée une fois que le paquet est encapsulé dans GRE, mais avant qu'il ne soit transmis à l'interface physique.

Problèmes de messages de test d'activité lorsque vous combinez IPsec et GRE

Étant donné les deux façons d'ajouter le chiffrement aux tunnels GRE, il existe trois façons distinctes de configurer un tunnel GRE chiffré :

1. La protection de tunnel est configurée sur l'interface de tunnel de l'homologue A, tandis que la crypto-carte est configurée sur l'interface physique de l'homologue B.
2. L'homologue A a une carte de chiffrement configurée sur l'interface physique tandis que l'homologue B a une protection de tunnel configurée sur l'interface de tunnel.
3. La protection du tunnel est configurée sur l'interface du tunnel des deux homologues.

La configuration décrite dans les scénarios 1 et 2 est souvent effectuée dans une conception Hub and Spoke. La protection de tunnel est configurée sur le routeur concentrateur afin de réduire la taille de la configuration et une crypto-carte statique est utilisée sur chaque rayon.

Considérez chacun de ces scénarios avec des keepalives GRE activés sur l'homologue B (rayon) et où le mode tunnel est utilisé pour le chiffrement.

Scénario 1

Configuration:

- L'homologue A utilise la protection de tunnel.
- L'homologue B utilise des crypto-cartes.
- Les messages Keepalive sont activés sur l'homologue B.
- Le chiffrement IPsec est effectué en mode tunnel.

Dans ce scénario, puisque les keepalives GRE sont configurés sur l'homologue B, les événements de séquence lorsqu'un keepalive est généré sont les suivants :

1. L'homologue B génère un paquet keepalive qui est encapsulé par GRE, puis transmis à l'interface physique où il est chiffré et envoyé à la destination du tunnel, l'homologue A.

   Paquet envoyé de l’homologue B à l’homologue A :

<table>
<tr><td>En-tête IP</td><td>En-tête ESP</td><td colspan="2">En-tête IP GRE</td><td>En-tête GRE</td><td colspan="3">En-tête IP</td><td>GRE</td><td rowspan="2">fin ESP</td></tr>
<tr><td>SourceB</td><td>DestinationA</td><td>SourceB</td><td>DestinationA</td><td>PT=IP</td><td>SourceA</td><td>DestinationB</td><td>PT=0</td></tr>
</table>

2. Au niveau de l'homologue A, le keepalive GRE est reçu déchiffré :

<table>
<tr><td colspan="3">En-tête IP GRE</td><td>GRE</td><td colspan="3">En-tête IP</td><td>GRE</td></tr>
<tr><td>SourceB</td><td>DestinationA</td><td>PT=IP</td><td>SourceA</td><td>DestinationB</td><td>PT=0</td></tr>
</table>

décapsulé :

<table>
<tr><td colspan="2">En-tête IP</td><td>GRE</td></tr>
<tr><td>SourceA</td><td>DestinationB</td><td>PT=0</td></tr>
</table>

Ensuite, le paquet de réponse keepalive GRE interne est routé en fonction de son adresse de destination qui est l'homologue B. Cela signifie que sur l'homologue A, le paquet est immédiatement routé de l'interface physique vers l'homologue B. Puisque l'homologue A utilise la protection de tunnel sur l'interface de tunnel, le paquet keepalive n'est pas chiffré.

Par conséquent, le paquet envoyé de l'homologue A à l'homologue B :

<table>
<tr><td colspan="2">En-tête IP</td><td>GRE</td></tr>
<tr><td>SourceA</td><td>DestinationB</td><td>PT=0</td></tr>
</table>

Remarque : Le keepalive n'est pas chiffré.

---

3. L'homologue B reçoit maintenant une réponse de keepalive GRE qui n'est pas chiffrée sur son interface physique, mais en raison de la crypto-carte configurée sur l'interface physique, il attend un paquet chiffré et donc l'abandonne.

Par conséquent, même si l'homologue A répond aux messages de test d'activité et que l'homologue B du routeur reçoit les réponses, il ne les traite jamais et modifie finalement le protocole de ligne de l'interface du tunnel en état down.

Résultat :

Les keepalives activés sur l'homologue B entraînent le changement de l'état du tunnel sur l'homologue B en up/down.

Scénario 2

Configuration:

- L'homologue A utilise des crypto-cartes.
- L'homologue B utilise la protection de tunnel.
- Les messages Keepalive sont activés sur l'homologue B.
- Le chiffrement IPsec est effectué en mode tunnel.

Dans ce scénario, puisque les keepalives GRE sont configurés sur l'homologue B, les événements de séquence lorsqu'un keepalive est généré sont les suivants :

1. L'homologue B génère un paquet keepalive qui est encapsulé GRE, puis chiffré par la protection de tunnel sur l'interface de tunnel, puis transféré à l'interface physique.

   Paquet envoyé de l'homologue B à l'homologue A :

<table>
<tr><td rowspan="2">En-tête IP</td><td rowspan="2">En-tête ESP</td><td rowspan="2">En-tête IP GRE</td><td rowspan="2">En-tête GRE</td><td>En-tête IP</td><td>GRE</td><td></td><td rowspan="2">fin ESP</td></tr>
<tr><td>SourceA</td><td>DestinationB</td><td>PT=0</td></tr>
<tr><td>SourceB</td><td>DestinationA</td><td>SourceB</td><td>DestinationA</td><td colspan="3">PT=IP</td></tr>
</table>

2. Au niveau de l'homologue A, le keepalive GRE est reçu déchiffré :

<table>
<tr><td colspan="2">En-tête IP GRE</td><td>GRE</td><td colspan="2">En-tête IP</td><td>GRE</td></tr>
<tr><td>SourceB</td><td>DestinationA</td><td>PT=IP</td><td>SourceA</td><td>DestinationB</td><td>PT=0</td></tr>
</table>

   décapsulé :

<table>
<tr><td colspan="2">En-tête IP</td><td>GRE</td></tr>
<tr><td>SourceA</td><td>DestinationB</td><td>PT=0</td></tr>
</table>

   Ensuite, le paquet de réponse keepalive GRE interne est routé en fonction de son adresse de destination qui est l'homologue B. Cela signifie que sur l'homologue A, le paquet est immédiatement routé de l'interface physique vers l'homologue B. Puisque l'homologue A

utilise des crypto-cartes sur l’interface physique, il chiffre d’abord ce paquet avant de le transmettre.

Par conséquent, le paquet envoyé de l'homologue A à l'homologue B :

En-tête IP		En-tête ESP	En-tête IP		GRE	fin ESP
SourceB	DestinationA		SourceA	DestinationB	PT=0	

Remarque : La réponse keepalive est chiffrée.

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

En-tête IP		GRE
SourceA	DestinationB	PT=0

Puisque le type de protocole est défini sur 0, l'homologue B sait qu'il s'agit d'une réponse de test d'activité et la traite comme telle.

Résultat :

Les keepalives activés sur l'homologue B déterminent avec succès quel état du tunnel peut être basé sur la disponibilité de la destination du tunnel.

Scénario 3

Configuration:

- Les deux homologues utilisent la protection de tunnel.
- Les messages Keepalive sont activés sur l'homologue B.
- Le chiffrement IPsec est effectué en mode tunnel.

Ce scénario est similaire au scénario 1 en ce sens que lorsque l'homologue A reçoit le keepalive chiffré, il le déchiffre et le décapsule. Cependant, lorsque la réponse est renvoyée, elle n'est pas chiffrée car l'homologue A utilise la protection de tunnel sur l'interface de tunnel. Ainsi, l'homologue B abandonne la réponse keepalive non chiffrée et ne la traite pas.

Résultat :

Les keepalives activés sur l'homologue B entraînent le changement de l'état du tunnel sur l'homologue B en up/down.

Solution de contournement

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

1. Utilisez une crypto-carte sur l'homologue A, la protection de tunnel sur l'homologue B et activez les keepalives sur l'homologue B.

   Comme ce type de configuration est principalement utilisé dans les configurations Hub-and-Spoke et que dans de telles configurations, il est plus important pour le rayon d'être conscient de l'accessibilité des concentrateurs, la solution est d'utiliser une crypto-carte dynamique sur le concentrateur (Peer A) et une protection de tunnel sur le rayon (Peer B) et d'activer les keepalives GRE sur le rayon. De cette façon, bien que l'interface de tunnel GRE sur le concentrateur reste active, le voisin de routage et les routes à travers le tunnel sont perdus et la route alternative peut être établie. Sur le rayon, le fait que l'interface du tunnel soit tombée en panne peut le déclencher pour activer une interface de numérotation et rappeler le concentrateur (ou un autre routeur au niveau du concentrateur), puis établir une nouvelle connexion.

2. Utilisez autre chose que des keepalives GRE afin de déterminer l'accessibilité des homologues.

   Si les deux routeurs sont configurés avec une protection de tunnel, les keepalives de tunnel GRE ne peuvent pas être utilisés dans les deux sens. Dans ce cas, la seule option est d'utiliser le protocole de routage ou un autre mécanisme, tel que l'agent d'assurance de service, afin de découvrir si l'homologue est accessible ou non.

3. Utilisez des crypto-cartes sur l'homologue A et l'homologue B.

   Si les deux routeurs sont configurés avec des cartes de chiffrement, les keepalives de tunnel peuvent passer dans les deux directions et les interfaces de tunnel GRE peuvent s'arrêter dans l'une ou les deux directions et déclencher une connexion de secours à établir. C'est l'option la plus flexible.

Informations connexes

- RFC 1701, encapsulation de routeur générique (GRE)
- RFC 2890, Extensions de clé et de numéro de séquence vers GRE
- Maintien en vie du tunnel GRE (Generic Routing Encapsulation)

- Fragmentation IP et PMTUD
- Présentation des mécanismes Keepalive sur Cisco IOS
- Support technique - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.