Pourquoi ne puis-je pas surfer sur Internet lorsque j'utilise un tunnel GRE ?

Contenu

Introduction

Parfois quand le trafic passe par un tunnel d'encapsulation de routage générique (GRE), vous pouvez utiliser avec succès la **commande ping** et le Telnet, mais vous ne pouvez pas télécharger des pages Web ou des fichiers de transfert en utilisant le Protocole de transfert de fichiers (FTP). Ce document explique une raison courante à ce problème et offre plusieurs solutions de contournement.

Conditions préalables

Conditions requises

Ce document requiert une compréhension de base de GRE. Consultez ces documents pour en savoir plus sur GRE :

- Encapsulation de routage générique
- La section Configurer un tunnel GRE dans Scénarios d'entreprise de VPN de site à site et extranet

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

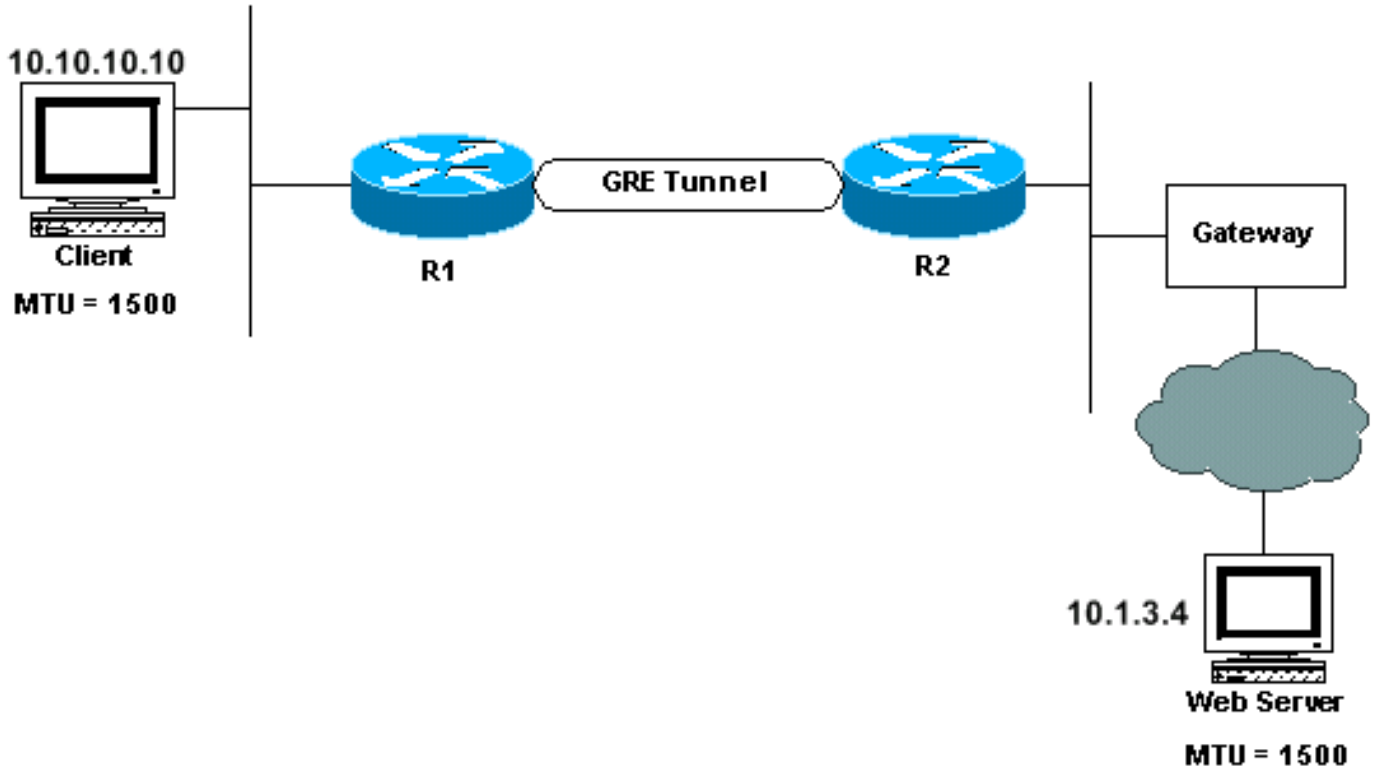
Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Fragmentation des paquets et messages ICMP

Ce document utilise ce schéma de réseau comme exemple :



Dans le schéma ci-dessus, quand le client veut accéder à une page sur Internet, il établit une session TCP avec le serveur Web. Pendant ce processus, le client et le serveur Web annoncent leur taille maximale de segment (MSS), en s'indiquant qu'ils peuvent accepter des segments TCP jusqu'à cette taille. Lors de la réception de l'option MSS, chaque périphérique calcule la taille du segment qui peut être envoyé. Ceci est appelé la taille maximum de segment d'envoi (SMSS), qui est égale à la plus petite des deux MSS. Pour plus d'informations sur la taille maximale de segment de TCP, consultez RFC 879 .

Pour les besoins de l'argumentation, disons que le serveur Web dans l'exemple ci-dessus détermine qu'il peut envoyer des paquets jusqu'à 1 500 octets de longueur. Il envoie donc un paquet de 1 500 octets au client et, dans l'en-tête IP, il définit le bit sur « don't fragment » (DF). Quand le paquet arrive au R2, le routeur essaie de l'encapsuler dans le paquet de tunnel. Dans le cas de l'interface de tunnel GRE, l'unité de transmission maximale d'IP (MTU) est de 24 octets de moins que la MTU d'IP de la vraie interface sortante. Pour une interface sortante Ethernet , cela signifie que la MTU de l'IP sur l'interface du tunnel serait de 1 500 moins 24, ou 1 476 octets.

R2 essaye d'envoyer des paquets IP de 1 500 octets dans une interface MTU d'IP de 1 476 octets. Puisque ce n'est pas possible, R2 doit fragmenter le paquet, créant un paquet de 1 476 octets (données et en-tête IP) et un paquet de 44 octets (24 octets de données et une nouvelle en-tête IP de 20 octets). R2 GRE encapsule alors chacun des deux paquets pour obtenir des

paquets de 1 500 et 68 octets, respectivement. Ces paquets peuvent maintenant être envoyés à la vraie interface de sortie, qui a une MTU d'IP de 1 500 octets.

Cependant, souvenez-vous que le bit du paquet reçu par R2 est défini sur DF. Par conséquent, R2 ne peut pas fragmenter le paquet et, à la place, il doit demander au serveur Web d'envoyer de plus petits paquets. Il fait ceci en envoyant un paquet Internet Control Message Protocol (ICMP) type 3 code 4 (destination inaccessible ; fragmentation nécessaire et DF défini). Ce message ICMP contient la MTU correcte à utiliser par le serveur Web, qui devrait recevoir ce message et régler la taille de paquet en conséquence.

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Vous pouvez afficher les messages ICMP envoyés par R2 en activant la commande **debug ip icmp** :

```
ICMP: dst (10.10.10.10) frag. needed and DF set unreachable sent to 10.1.3.4
```

Messages ICMP bloqués

Un problème courant se pose quand des messages ICMP sont bloqués le long du chemin vers le serveur Web. Quand ceci se produit, le paquet ICMP n'atteint jamais le serveur Web, empêchant de ce fait le passage des données entre le client et le serveur.

Solutions

Une des quatre solutions suivantes devrait résoudre le problème :

- Découvrez où le message ICMP est bloqué le long du chemin et regardez si vous pouvez faire en sorte de l'autoriser.
- Définissez la MTU sur l'interface réseau du client à 1 476 octets, obligeant le SMSS à être plus petit, ainsi les paquets ne devront pas être fragmentés quand ils atteignent R2. Cependant, si vous modifiez la MTU pour le client, vous devrez également modifier la MTU pour tous les périphériques qui partagent le réseau avec ce client. Sur un segment Ethernet, cela peut concerner un grand nombre de périphériques.
- Utilisez un serveur proxy (ou, encore mieux, un moteur de cache Web) entre R2 et le routeur de passerelle, et laissez le serveur de proxy demander toutes les pages Web.
- Si le tunnel GRE s'exécute sur des liaisons dont le MTU peut être supérieure à 1 500 octets plus l'en-tête de tunnel, alors une autre solution est d'augmenter la MTU à 1 524 (1500 plus 24 pour la surcharge GRE) sur toutes les interfaces et liaisons entre les routeurs de point d'extrémité de GRE.

Autres solutions

Si les options ci-dessus ne sont pas réalisables, les options suivantes peuvent alors être utiles :

- Utilisez la politique de routage pour effacer et définir le bit DF dans le paquet IP de données (disponible dans le logiciel Cisco IOS® Versions 12.1(6) et ultérieures).

```
interface ethernet0
 ...
 ip policy route-map clear-df !--- This command is used to identify a route map !--- to use
for policy routing on an interface, !--- use the ip policy route-map command in !---
```

```
interface configuration mode. route-map clear-df permit 10 match ip address 101 set ip df 0
!--- This command is used to change the Don't Fragment (DF) !--- bit value in the IP header,
use this command !--- in route-map configuration mode. access-list 101 permit tcp 10.1.3.0
0.0.0.255 any
```
Ceci permettra la fragmentation du paquet de données IP avant l'encapsulation GRE. L'hôte d'extrémité réceptrice doit alors rassembler les paquets IP de données. Ce n'est habituellement pas un problème.

- Modifiez la valeur de l'option MSS de TCP sur les paquets SYN qui passent par le routeur (disponible dans IOS Versions 12.2(4)T et ultérieures). Ceci réduit la valeur de l'option MSS dans le paquet SYN de TCP de sorte qu'elle est inférieure à la valeur dans la commande **ip tcp adjust-mss value** , à savoir dans ce cas 1 436 octets (MTU sans la taille des en-têtes d'IP, de TCP et de GRE). Les hôtes d'extrémité envoient maintenant des paquets TCP/IP dont la taille ne dépasse pas cette valeur.
```
interface tunnel0
 ...
 ip tcp adjust-mss 1436 !--- This command is used to adjust the maximum segment size (MSS)
!--- value of TCP SYN packets going through the router. !--- The maximum segment size is in
the range from 500 to 1460.
```
- Une dernière possibilité consiste à augmenter la MTU d'IP sur l'interface du tunnel à 1 500 (disponible dans IOS Versions 12.0 et ultérieures). Cependant, l'augmentation de la MTU de l'IP entraîne la fragmentation des paquets parce que le bit DF du paquet original n'est pas copié vers l'en-tête de paquet de tunnel. Dans ce scénario, le routeur sur l'autre extrémité du tunnel GRE doit rassembler le paquet de tunnel GRE avant de pouvoir supprimer l'en-tête GRE et transférer le paquet interne. Le réassemblage de paquet IP est fait dans le mode de commutation de processus et utilise la mémoire. Par conséquent, cette option peut de manière significative réduire le débit de paquets par le tunnel GRE.
```
interface tunnel0
   ...
ip mtu 1500 !--- This command is used to set the maximum transmission unit (MTU) !--- size
of IP packets sent on an interface. The minimum size !--- you can configure is 128 bytes;
the maximum depends on the interface medium.
```

En conclusion, le problème de fragmentation mentionné ci-dessus est la plupart du temps la raison pour laquelle il est impossible de naviguer sur Internet à travers un tunnel GRE. La solution consiste à autoriser les paquets ICMP ou à contourner le problème d'ICMP grâce à l'une des solutions ci-dessus.

Informations connexes

- Résoudre les problèmes de fragmentation IP, MTU, MSS et PMTUD avec GRE et IPSEC
- Quelle solution VPN est la bonne pour vous ?
- Pages d'assistance GRE
- Exemples de configuration GRE
- Page de support pour le routage IP
- Support technique - Cisco Systems