Waarom kan ik niet door het internet bladeren wanneer ik een GRE-tunnel gebruik?

Inhoud

Inleiding

Soms wanneer het verkeer door een generieke Routing Encapsulation-tunnel (GRE) gaat, kunt u met succes de ping-opdracht en -telnet gebruiken, maar u kunt internetpagina's niet downloaden of bestanden overdragen met File Transfer Protocol (FTP). Dit document legt een gemeenschappelijke reden voor dit probleem uit en biedt verschillende tijdelijke oplossingen.

Voorwaarden

Vereisten

Dit document vereist een basisbegrip van GRE. Raadpleeg deze documenten voor meer informatie over GRE:

- Generic Routing Encapsulation
- Het configureren van een GRE-tunnelgedeelte van Site-to-Site en Extranet VPN-zakelijke scenario's

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

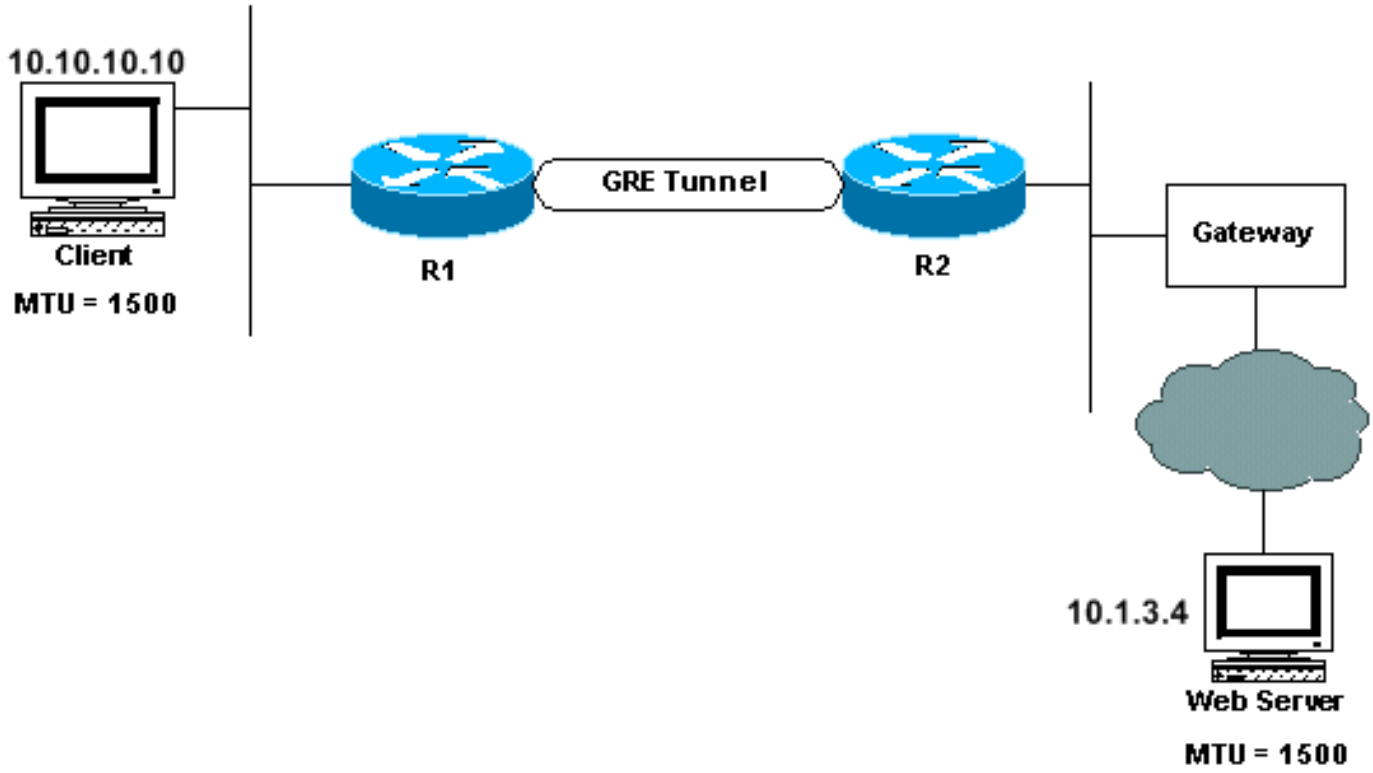
Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Packet Fragmentation- en ICMP-berichten

Dit document gebruikt dit netwerkdiagram als voorbeeld:



In het bovenstaande diagram, wanneer de client toegang wil krijgen tot een pagina op het internet, stelt het een TCP-sessie in met de webserver. Tijdens dit proces, kondigen de Cliënt en de Server van het Web hun maximum segmentgrootte (MSS) aan, wijzend op elkaar dat zij TCP segmenten tot deze grootte kunnen accepteren. Na het ontvangen van de MSS optie, berekent elk apparaat de grootte van het segment dat kan worden verstuurd. Dit wordt de Send Max Segment Size (SMSS) genoemd en het is gelijk aan de kleinere van de twee MSS. Zie RFC 879 voor meer informatie over de maximale grootte van TCP .

Terwille van de argumentatie, laten we zeggen dat de server van het Web in het bovenstaande voorbeeld bepaalt dat het pakketten tot 1500 bytes in lengte kan verzenden. Hiermee wordt een bytepakket van 1500 naar de client verzonden en in de IP-header wordt het bit "don't fragment" (DF) ingesteld. Wanneer het pakje bij R2 aankomt, probeert de router het in het tunnelpakje in te sluiten. In het geval van de GRE-tunnelinterface is de maximale IP-transmissieeenheid (MTU) 24 bytes minder dan de IP-MTU van de reële uitgaande interface. Voor een Ethernet uitgaande interface die betekent dat de IP MTU op de tunnelinterface 1500 min 24, of 1476 bytes zou zijn.

R2 probeert een IP-pakket van 1500 bytes naar een IP-interface van 1476 te verzenden. Aangezien dit niet mogelijk is, moet R2 het pakket fragmenteren, door één pakket van 1476 bytes (data en IP header) en één pakket van 44 bytes (24 bytes van gegevens en een nieuwe IP-header van 20 bytes) te maken. R2 neemt vervolgens GRE beide pakketten in om respectievelijk 1500 en 68 bytes pakketten te verkrijgen. Deze pakketten kunnen nu worden verzonden de echte uitgaande interface, die een IP-MTU van 1500 bytes heeft.

Denk er echter aan dat het pakket dat door R2 wordt ontvangen het DF-bit heeft ingesteld. Daarom kan R2 het pakket niet fragmenteren en in plaats daarvan moet het de Server van het Web opdragen om kleinere pakketten te verzenden. Dit gebeurt door een ICMP-code (Internet Control Message Protocol) van het type 3-code 4-pakket (Destination Unbereikable) te verzenden; Fragmentation NODIG en DF-instelling). Dit ICMP-bericht bevat de juiste MTU die door de Web Server moet worden gebruikt. Dit bericht moet worden ontvangen en de pakketgrootte moet worden aangepast.

OPMERKING: Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

U kunt de ICMP berichten bekijken die door R2 worden verstuurd door de **debug ip**-opdracht mogelijk te maken:

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

Vergrendelde ICMP-berichten

Een veelvoorkomend probleem doet zich voor wanneer de ICMP-berichten langs het pad naar de webserver worden geblokkeerd. Wanneer dit gebeurt, bereikt het ICMP-pakket nooit de server van het Web, waarbij de gegevens tussen client en server worden voorkomen.

Oplossingen

Eén van deze vier oplossingen moet het probleem oplossen:

- Ga na waar langs het pad het ICMP-bericht is geblokkeerd en zie of het mogelijk is.
- Stel de MTU op de netwerkinterface van de client in op 1476 bytes. U dwingt de SMSS om kleiner te worden, zodat pakketten niet gefragmenteerd hoeven te worden wanneer ze R2 bereiken. Als u echter de MTU voor de client wijzigt, moet u ook de MTU wijzigen voor alle apparaten die het netwerk met deze client delen. Op een Ethernet-segment, zou dit een groot aantal apparaten kunnen zijn.
- Gebruik een proxy-server (of, nog beter, een Web cache-motor) tussen R2 en de Gateway-router, en laat de proxy-server alle Internet pagina's opvragen.
- Als de GRE-tunnel over koppelingen loopt die een MTU van meer dan 1500 bytes plus de tunnelkop kunnen hebben, dan is een andere oplossing om de MTU op alle interfaces en verbindingen tussen de GRE-endpointrouters te verhogen tot 1524 (1500 plus 24 voor de GRE-overhead).

Verdere oplossingen

Als de bovenstaande opties niet haalbaar zijn, kunnen deze opties nuttig zijn:

- Gebruik beleidsrouting om het PDF-bit te wissen en in te stellen in het IP-pakket voor gegevens (beschikbaar in Cisco IOS® softwarerelease 12.1(6) en hoger).

```
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
```

Hierdoor kan het IP-pakket gegevens gefragmenteerd worden voordat het GRE-ingekapseld is. De ontvangende eindhost moet de IP-pakketten met gegevens vervolgens opnieuw assembleren. Dit is meestal geen probleem.

- Verandert de waarde van de optie TCP MSS op SYN-pakketten die door de router worden verzonden (beschikbaar in IOS 12.2(4)T en hoger). Dit vermindert de waarde van de optie MSS in het TCP SYN-pakket zodat het kleiner is dan de waarde in de opdracht **ip** TCP-***mss-waarde*, in dit geval 1436 (MTU minus de grootte van de IP-, TCP- en GRE-headers).** De eindhosts verzenden nu TCP/IP-pakketten die niet groter zijn dan deze waarde.

```
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.
```

- Een laatste optie is om de IP MTU op de tunnelinterface naar 1500 te verhogen (beschikbaar in IOS 12.0 en later). Door het vergroten van de tunnel IP MTU worden de tunnelpakketten echter gefragmenteerd omdat het PDF-bit van het oorspronkelijke pakket niet naar de tunnelpakketheader wordt gekopieerd. In dit scenario moet de router aan het andere uiteinde van de GRE-tunnel het GRE-tunnelpakket opnieuw assembleren voordat het de GRE-header kan verwijderen en het binnenpakket doorsturen. IP-pakkethermontage wordt uitgevoerd in proces-switch modus en gebruikt geheugen. Daarom kan deze optie de pakketdoorvoersnelheid door de GRE-tunnel aanzienlijk verminderen.

```
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.
```

Concluderend kan ik zeggen dat de meest voorkomende oorzaak van het niet kunnen doorkijken van het internet via een GRE-tunnel het gevolg is van het bovenvermelde fragmentatieprobleem. De oplossing is om de ICMP-pakketten toe te staan of rond het ICMP-probleem met een van de bovengenoemde oplossingen te werken.

Gerelateerde informatie

- Oplossen van IP-fragmentatie, MTU, MSS en PMTUD-problemen met GRE en IPSEC
- Welke VPN-oplossing is geschikt voor u?
- GRE-ondersteuningspagina's
- GRE-configuratievoorbeelden
- Ondersteuningspagina voor IP-routing
- Technische ondersteuning - Cisco-systemen