¿Por qué no puedo navegar por Internet cuando utilizo un túnel GRE?

Contenido

Introducción

A veces, cuando el tráfico atraviesa un encapsulado de ruteo genérico (GRE), puede utilizar con éxito el comando ping y realizar una conexión Telnet, pero no puede descargar páginas de Internet o transferir archivos utilizando el protocolo de transferencia de archivos (FTP). Este documento explica un motivo frecuente para este problema y ofrece varias soluciones alternativas.

prerrequisitos

Requisitos

Este documento requiere una comprensión básica de GRE. Refiera a estos documentos para aprender más sobre el GRE:

- Generic Routing Encapsulation
- Configurar una sección del túnel GRE del sitio a localizar y de los escenarios de negocio VPN extranet

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

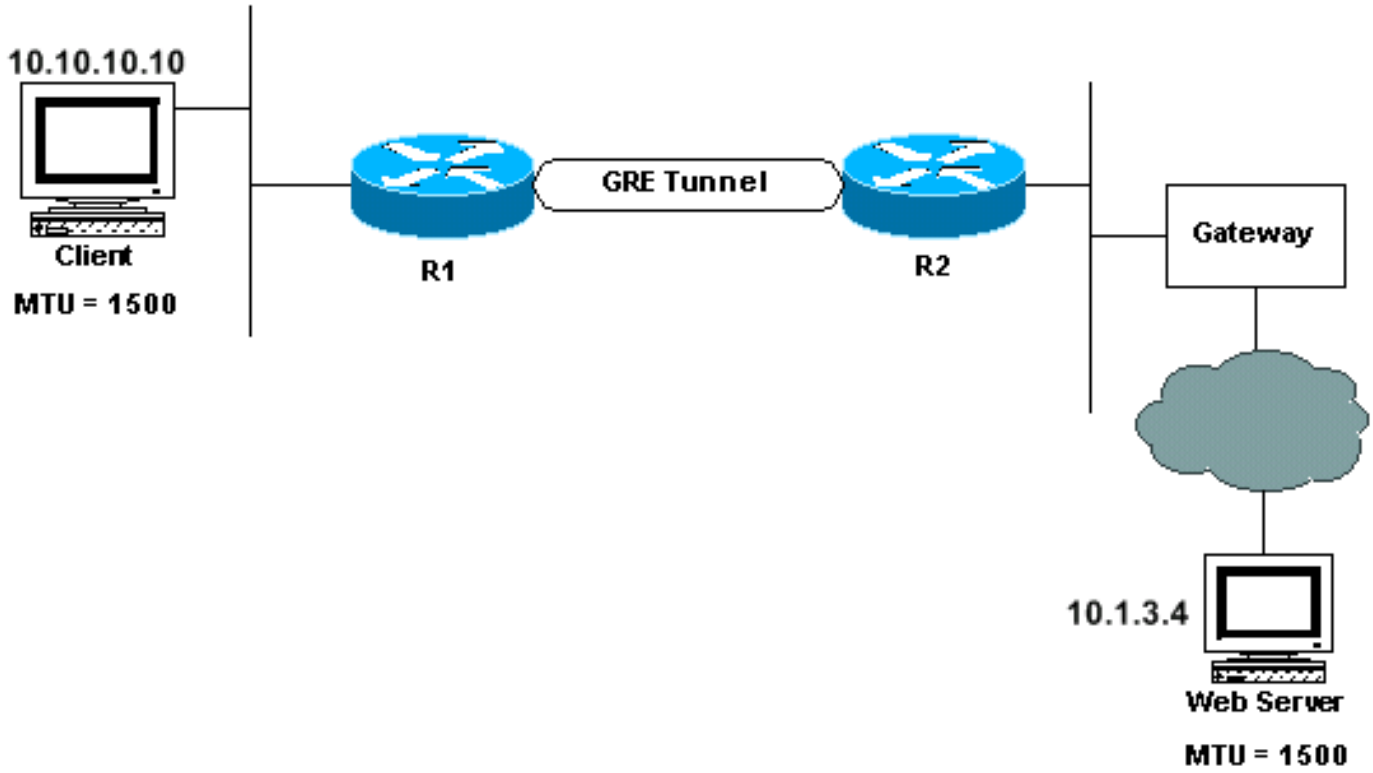
Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Fragmentación de paquetes y mensajes ICMP

Este documento utiliza este diagrama de la red como un ejemplo:



En el diagrama precedente, cuando el cliente desea acceder a una página en Internet, establece una sesión TCP con el servidor Web. Durante este proceso, el cliente y el servidor Web anuncian el tamaño de segmento máximo (MSS), y así se indican el uno al otro que pueden aceptar segmentos TCP hasta este tamaño. Luego de recibir la opción MSS, cada dispositivo calcula el tamaño del segmento que se puede enviar. Esto se llama –Envío del tamaño máximo de segmento (SMSS) y es igual al más chico de los dos MSS. Si desea obtener más información sobre el tamaño máximo de segmento de TCP, consulte RFC 879.

Por el argumento, digamos al servidor Web en el ejemplo anterior determina que puede enviar los paquetes hasta 1500 bytes en la longitud. Por lo tanto envía un paquete de bytes 1500 al cliente, y, en el encabezado IP, fija el bit del “Don't Fragment” (DF). Cuando un paquete ingresa al router R2, el router intenta encapsularlo al paquete de túnel. En el caso de la interfaz de túnel GRE, la unidad máxima de transmisión IP (MTU) es 24 bytes menos que el IP MTU de la interfaz saliente real. Para una interfaz saliente de los Ethernetes que significa el IP MTU en la interfaz del túnel sería 1500 menos 24, o 1476 bytes.

R2 intenta enviar un paquete IP de 1500 bytes dentro de una interfaz MTU IP de 1476 bytes. Dado que esto no es posible, R2 debe fragmentar el paquete, creando un paquete de 1476 bytes (datos y encabezado IP) y un paquete de 44 bytes (24 bytes de datos y un nuevo encabezado IP de 20 bytes). El r2 entonces GRE encapsula ambos paquetes para conseguir 1500 y 68 paquetes

de bytes, respectivamente. Estos paquetes ahora pueden enviarse a la interfaz de salida real, la cual tiene una MTU IP de 1500 bytes.

Sin embargo, recuerde que el paquete recibido por R2 tiene configurado el bit DF. Por lo tanto, R2 no puede fragmentar el paquete y, en su lugar, necesita instruir al servidor Web para que envíe paquetes más pequeños. Hace esto enviando un paquete del código 4 del tipo 3 del Internet Control Message Protocol (ICMP) (destino inalcanzable; Fragmentación necesaria y DF para fijar). Este mensaje ICMP contiene el MTU correcto que se utilizará por el servidor Web, que debe recibir este mensaje y ajusta el tamaño de paquetes por consiguiente.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Usted puede ver los mensajes ICMP enviados por el r2 habilitando el **comando debug ip icmp**:

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

Mensajes ICMP bloqueados

Un problema común ocurre cuando los mensajes ICMP se bloquean a lo largo de la trayectoria al servidor Web. Cuando sucede esto, los paquetes icmp nunca alcanzan al servidor Web, de tal modo evitando que los datos pasen entre el cliente y servidor.

Soluciones

Una de estas cuatro soluciones debe solucionar el problema:

- Averigüe adónde durante el camino, se bloquea el mensaje ICPM y vea si puede autorizarlo.
- Fije el MTU en la interfaz de la red del cliente a 1476 bytes, forzando el SMSS para ser más pequeño, así que los paquetes no tendrán que ser hechos fragmentos cuando alcanzan el r2. Sin embargo, si cambia la MTU para el Cliente, también debería cambiar la MTU para todos los dispositivos que comparten la red con este Cliente. En un segmento Ethernet, éste podía ser un gran número de dispositivos.
- Utilice un proxy server (o, incluso mejor, un motor de memoria caché de Web) entre el r2 y el router de gateway, y deje la petición del proxy server todas las páginas de Internet.
- Si el túnel GRE se ejecuta sobre links que pueden tener una MTU de más de 1500 bytes más el encabezado del túnel, entonces otra solución es aumentar la MTU a 1524 (1500 más 24 para el overhead de GRE) en todas las interfaces y links entre los routers de puntos extremos de GRE.

Soluciones adicionales

Si las opciones antedichas no son posibles entonces estas opciones pueden ser útiles:

- Utilice el Policy Routing para borrar y para fijar el DF mordido en el paquete del IP de los datos (disponible en el Software Release 12.1(6) y Posterior de Cisco IOS®).
```
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
```

Esto permitirá que el paquete del IP de los datos sea hecho fragmentos antes de que sea GRE encapsulado. Luego, el host final de recepción debe reensamblar los paquetes IP de datos. Esto no suele ser un problema.

- Cambie el valor de opción MSS TCP en los paquetes SYN que transversal a través del router (disponible en IOS 12.2(4)T y más alto). Esto reduce el valor de opción MSS en paquete TCP Syn de modo que sea más pequeño que el valor en el **comando ip tcp adjust-mss value**, en este caso los 1436 (MTU menos el tamaño del IP, del TCP, y de los encabezados GRE). Los host extremos ahora envían los paquetes TCP/IP no más grandes que este valor.

```
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.
```

- Una última opción es aumentar el IP MTU en la interfaz del túnel a 1500 (disponible en IOS 12.0 y posterior). Sin embargo, el aumento del IP MTU del túnel hace los paquetes del túnel ser hecho fragmentos porque el bit DF del paquete original no se copia a la encabezado de paquete del túnel. En este escenario, el router en el otro extremo del túnel GRE debe volver a ensamblar el paquete del túnel GRE antes de que pueda quitar el encabezado GRE y reenviar el paquete interno. El reensamblado de paquetes de IP se realiza en modo de switch de proceso y utiliza memoria. Por lo tanto, esta opción puede reducir en gran medida la producción de paquetes a través del túnel 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 resumen, la causa más frecuente por la que no se puede navegar por Internet sobre un túnel GRE se debe al problema de fragmentación ya mencionado. La solución es admitir los paquetes ICMP o resolver el problema ICMP con cualquiera de las soluciones alternativas previamente mencionadas.

Información Relacionada

- Resolución fragmentación de IP, problemas MTU, MSS, y PMTUD con el GRE y el IPSEC
- ¿Qué solución VPN es la adecuada para usted?
- Páginas de soporte de GRE
- Ejemplos de configuración de GRE
- Página de Soporte de IP Routing
- Soporte Técnico - Cisco Systems