

Por que não navegar na Internet usando um túnel GRE?

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Fragmentação de pacote e mensagens ICMP](#)

[Mensagens ICMP bloqueadas](#)

[Soluções](#)

[Outras soluções](#)

[Informações Relacionadas](#)

[Introduction](#)

Às vezes, quando o tráfego passar por um túnel de Generic Routing Encapsulation (GRE), é possível usar com êxito o comando ping e o Telnet, porém será possível fazer o download de páginas de Internet ou transferir arquivos usando o File Transfer Protocol (FTP). Este documento explica um motivo comum para o problema e oferece várias soluções alternativas.

[Prerequisites](#)

[Requirements](#)

Este documento exige noções básicas de GRE. Consulte estes documentos para saber mais sobre o GRE:

- [Encapsulamento de roteamento genérico](#)
- A seção [Configurando um túnel GRE de cenários empresariais de VPN site a site e de extranet](#)

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

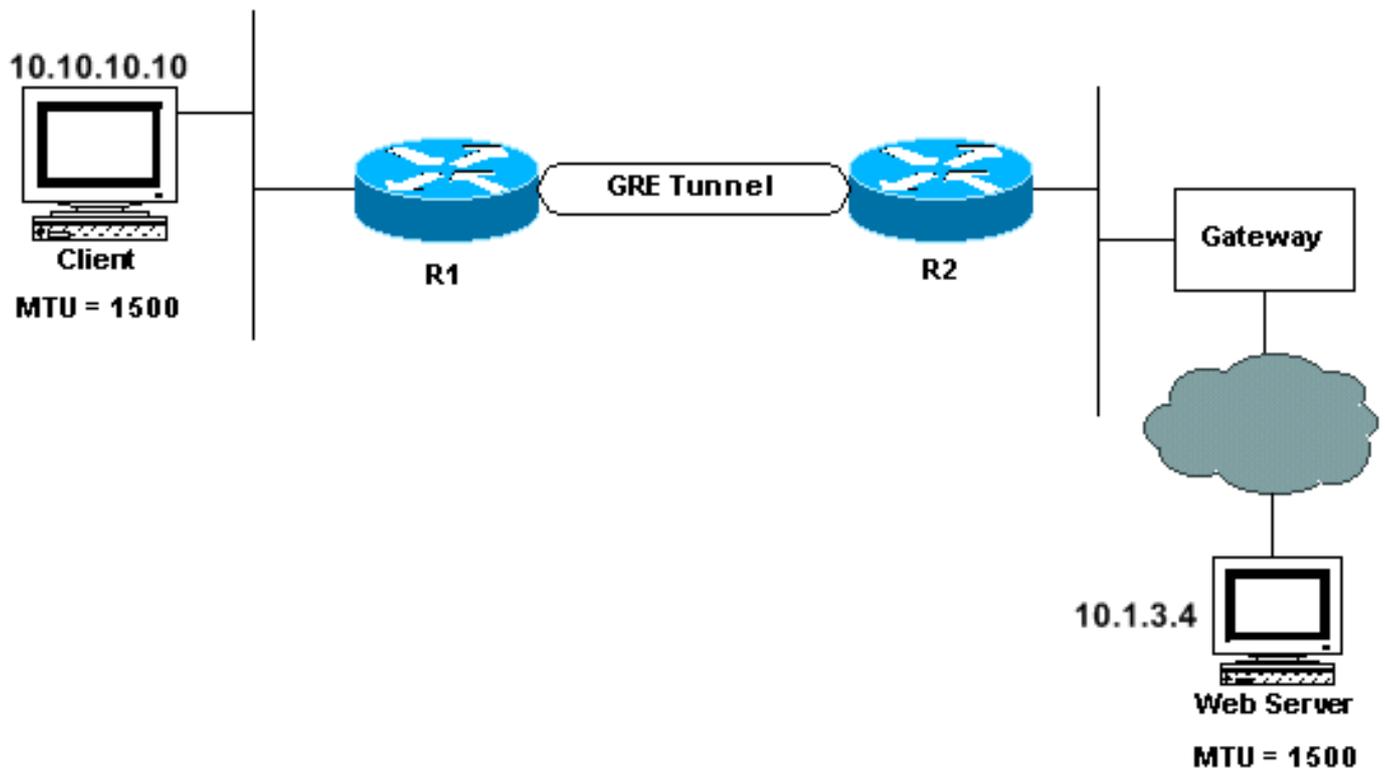
Use a ferramenta [Command Lookup Tool \(apenas para clientes registrados\)](#) para obter mais informações sobre os comandos usados neste documento.

[Conventions](#)

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.](#)

Fragmentação de pacote e mensagens ICPM

Este documento usa este diagrama de rede como exemplo:



No diagrama acima, quando o cliente quiser acessar uma página da Internet, ele estabelece uma sessão de TCP com o Servidor de Web. Durante esse processo, os Servidores Cliente e Web anunciam o tamanho máximo de segmento (MSS), indicando um ao outro que podem aceitar segmentos de TCP até esse tamanho. Após o recebimento da opção MSS, cada dispositivo calcula o tamanho do segmento que pode ser enviado. Isso se chama Send Max Segment Size (SMSS) e equivale ao menor dos dois MSSs. Para obter mais informações sobre o Tamanho máximo de segmento do TCP, consulte o RFC 879.

Por uma questão de argumento, digamos que o Servidor Web no exemplo acima determina que ele pode enviar pacotes com até 1500 bytes de comprimento. Portanto, ele envia um pacote de 1.500 bytes ao cliente e, no cabeçalho IP, define o bit "não fragmentar" (DF). Quando o pacote chega no R2, o roteador tenta encapsulá-lo no pacote de túnel. No caso da interface de túnel GRE, a MTU (Maximum Transmission Unit, unidade de transmissão máxima) de IP é 24 bytes menor que a MTU de IP da interface de saída real. Para uma interface de saída Ethernet que significa que o MTU de IP na interface de túnel seria de 1500 menos 24, ou 1476 bytes.

O R2 está tentando enviar um pacote IP de 1500 byte em uma interface MTU IP de 1476 byte. Como isto não é possível, o R2 necessita fragmentar o pacote, criando um pacote de 1476 bytes (dados e cabeçalho de IP) e um pacote de 44 bytes (24 bytes de dados e um novo cabeçalho de IP de 20 bytes). R2 então o GRE encapsula ambos os pacotes para obter pacotes de 1.500 e 68 bytes, respectivamente. Esses pacotes podem ser enviados agora para a verdadeira interface externa, que tem uma MTU de IP de 1500 bytes.

No entanto, lembre-se de que o pacote recebido pelo R2 tem o conjunto de bits DF. Portanto, o R2 não pode fragmentar o pacote e, em vez disso, precisa instruir o servidor da Web a enviar pacotes menores. Ele faz isso enviando um pacote de código 4 do ICMP (Destination Unreachable; protocolo ICMP do tipo 3); Fragmentação necessária e DF definido). Essa mensagem ICMP contém o MTU correto a ser usado pelo Servidor Web, que deve receber essa mensagem e ajustar o tamanho do pacote de acordo.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Você pode exibir as mensagens ICMP enviadas por R2 habilitando o comando **debug ip icmp**:

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

Mensagens ICMP bloqueadas

Um problema comum ocorre quando as mensagens ICMP são bloqueadas ao longo do caminho para o servidor Web. Quando isso acontece, o pacote ICMP nunca chega ao servidor Web, impedindo assim que os dados passem entre o cliente e o servidor.

Soluções

Uma destas quatro soluções deve resolver o problema:

- Descubra em que parte do caminho a mensagem de ICMP está bloqueada e veja se consegue obter permissão para ela.
- Defina o MTU na interface de rede do Cliente como 1476 bytes, forçando o SMSS a ser menor, de modo que os pacotes não precisem ser fragmentados quando chegarem a R2. No entanto, se você alterar o MTU para o cliente, você também deve alterar o MTU para todos os dispositivos que compartilham a rede com este cliente. Em um segmento Ethernet, isso pode ser um grande número de dispositivos.
- Use um servidor proxy (ou, melhor ainda, um mecanismo de cache da Web) entre R2 e o roteador Gateway e deixe que o servidor proxy solicite todas as páginas da Internet.
- Se o túnel GRE for executado em links cujo MTU possa ser maior do que 1500 bytes, além do cabeçalho do túnel, então a outra solução é aumentar o MTU para 1524 (1500 mais 24 para a carga adicional do GRE) em todas as interfaces e links entre os roteadores de ponto final de GRE.

Outras soluções

Se as opções acima não forem viáveis, essas opções poderão ser úteis:

- Use o roteamento de política para limpar e definir o bit DF no pacote IP de dados (disponível no software Cisco IOS® versão 12.1(6) e posterior).

```
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
```

Isso permitirá que o pacote IP de dados seja fragmentado antes de ser encapsulado pelo GRE. O host final receptor deve então remontar os pacotes de dados IP. Geralmente, isto não é um problema.

- Altere o valor da opção TCP MSS em pacotes SYN que atravessam o roteador (disponível no IOS 12.2(4)T e posterior). Isso reduz o valor da opção MSS no pacote TCP SYN para que seja menor que o valor no comando `ip tcp adjust-mss value`, nesse caso 1436 (MTU menos o tamanho dos cabeçalhos IP, TCP e GRE). Os hosts finais agora enviam pacotes TCP/IP não maiores que esse 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.
```

- Uma opção final é aumentar o IP MTU na interface do túnel para 1500 (disponível no IOS 12.0 e posterior). No entanto, aumentar o MTU IP do túnel faz com que os pacotes do túnel sejam fragmentados porque o bit DF do pacote original não é copiado para o cabeçalho do pacote do túnel. Neste cenário, o roteador na outra extremidade do túnel GRE deve remontar o pacote de túnel GRE antes de poder remover o cabeçalho GRE e encaminhar o pacote interno. A remontagem do pacote de IP é efetuada no modo de Process-Switch e usa memória. Portanto, essa opção pode reduzir significativamente o ritmo de transferência do pacote por meio do 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.
```

Concluindo, a causa mais comum da impossibilidade de navegar a internet por um túnel GRE é o problema de fragmentação mencionado acima. A solução é permitir pacotes ICMP ou resolver o problema ICMP com qualquer uma das soluções acima.

[Informações Relacionadas](#)

- [Resolver problemas de fragmentação de IP, MTU, MSS e PMTUD com GRE e IPSEC](#)
- [Que solução de VPN é perfeita para você?](#)
- [Páginas de suporte de GRE](#)
- [Exemplos de Configuração GRE](#)
- [Página de Suporte do IP Routing](#)
- [Suporte Técnico - Cisco Systems](#)