

GRE 터널을 사용할 때 인터넷을 탐색할 수 없는 이유는 무엇입니까?

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[패킷 조각화 및 ICMP 메시지](#)

[차단된 ICMP 메시지](#)

[솔루션](#)

[추가 솔루션](#)

[관련 정보](#)

소개

트래픽이 GRE(Generic Routing Encapsulation) 터널을 통과할 때 ping 명령과 텔넷을 성공적으로 사용할 수 있지만 FTP(File Transfer Protocol)를 사용하여 인터넷 페이지 또는 전송 파일을 다운로드할 수는 없습니다. 이 문서에서는 이 문제의 일반적인 이유를 설명하고 몇 가지 해결 방법을 제공합니다.

사전 요구 사항

요구 사항

이 문서에는 GRE에 대한 기본적인 이해가 필요합니다. GRE에 대한 자세한 내용은 다음 문서를 참조하십시오.

- [일반 라우팅 캡슐화](#)
- [Site-to-Site 및 엑스트라넷 VPN 비즈니스 시나리오의 Configuring a GRE Tunnel\(GRE 터널 구성\) 섹션](#)

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

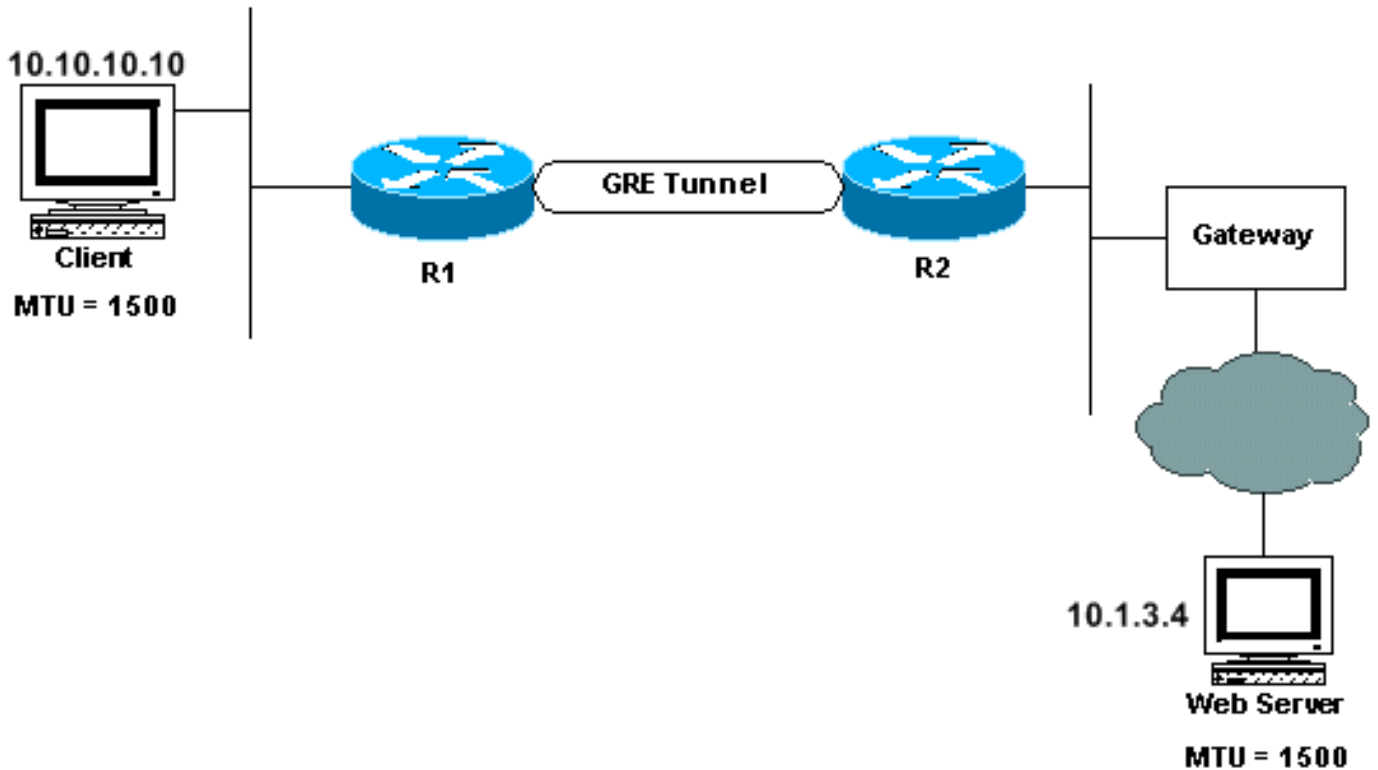
명령 조회 [도구](#)([등록된](#) 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 정보를 찾습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

패킷 조각화 및 ICMP 메시지

이 문서에서는 이 네트워크 다이어그램을 예로 사용합니다.



위의 다이어그램에서 클라이언트가 인터넷의 페이지에 액세스하려는 경우 웹 서버와의 TCP 세션을 설정합니다. 이 프로세스 중에 클라이언트와 웹 서버는 최대 세그먼트 크기(MSS)를 발표하고, 이는 서로 이 크기까지 TCP 세그먼트를 수락할 수 있음을 나타냅니다. MSS 옵션을 수신하면 각 디바이스는 전송할 수 있는 세그먼트의 크기를 계산합니다. 이를 SMSS(Send Max Segment Size)라고 하며, 두 MSS 중 작은 값과 같습니다. TCP 최대 세그먼트 크기에 대한 자세한 내용은 [RFC 879](#)를 참조하십시오.

인수를 위해 위의 예에서 웹 서버가 최대 1500바이트의 패킷을 전송할 수 있다고 결정한다고 가정해 보겠습니다. 따라서 클라이언트로 1500바이트 패킷을 전송하고, IP 헤더에서 "DF(Don't Fragment)" 비트를 설정합니다. 패킷이 R2에 도착하면 라우터는 터널 패킷에 패킷을 캡슐화합니다. GRE 터널 인터페이스의 경우 IP MTU(Maximum Transmission Unit)가 실제 발신 인터페이스의 IP MTU보다 24바이트 작습니다. 터널 인터페이스의 IP MTU를 의미하는 인터넷 발신 인터페이스의 경우 1500에서 24 또는 1476바이트가 됩니다.

R2는 1500바이트 IP 패킷을 1476바이트 IP MTU 인터페이스로 전송하려고 합니다. 이는 불가능하므로 R2는 1476바이트(데이터 및 IP 헤더)의 패킷 1개와 44바이트(24바이트 데이터 및 20바이트의 새 IP 헤더)의 패킷을 생성하여 패킷을 프래그먼트화해야 합니다. R2, GRE는 이러한 패킷을 모두 캡슐화하여 각각 1500 및 68바이트 패킷을 가져옵니다. 이제 이러한 패킷은 1500바이트 IP MTU가 있는 실제 아웃바운드 인터페이스로 전송될 수 있습니다.

그러나 R2에서 수신한 패킷에는 DF 비트가 설정되어 있습니다. 따라서 R2는 패킷을 프래그먼트화할 수 없으며 대신 웹 서버에 더 작은 패킷을 전송하도록 지시해야 합니다. ICMP(Internet Control Message Protocol) 유형 3 코드 4 패킷(Destination Unreachable; 필요한 프래그먼트화 및 DF 세트). 이 ICMP 메시지는 웹 서버에서 사용할 올바른 MTU가 포함되어 있습니다. 이 MTU는 이 메시

지를 받고 그에 따라 패킷 크기를 조정해야 합니다.

참고: debug 명령을 사용하기 전에 [디버그 명령에 대한 중요 정보](#)를 참조하십시오.

debug ip icmp 명령을 활성화하여 R2에서 보낸 ICMP 메시지를 볼 수 있습니다.

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

차단된 ICMP 메시지

웹 서버 경로를 따라 ICMP 메시지가 차단될 때 일반적인 문제가 발생합니다. 이 경우 ICMP 패킷은 웹 서버에 도달하지 않으므로 클라이언트와 서버 간에 데이터가 전달되지 않습니다.

솔루션

이 네 가지 솔루션 중 하나는 문제를 해결해야 합니다.

- 경로를 따라 ICMP 메시지가 차단된 위치를 확인하고 허용되는 메시지를 받을 수 있는지 확인합니다.
- 클라이언트 네트워크 인터페이스의 MTU를 1476바이트로 설정하여 MSS가 더 작도록 하여 R2에 도달할 때 패킷이 프래그먼트화될 필요가 없습니다. 그러나 클라이언트에 대해 MTU를 변경하는 경우 이 클라이언트와 네트워크를 공유하는 모든 장치에 대해서도 MTU를 변경해야 합니다. 이더넷 세그먼트에서 이는 많은 수의 장치일 수 있습니다.
- R2와 게이트웨이 라우터 간에 프록시 서버(또는 더 나은 웹 캐시 엔진)를 사용하고 프록시 서버가 모든 인터넷 페이지를 요청하도록 합니다.
- GRE 터널이 MTU가 1500바이트보다 크고 터널 헤더가 추가될 수 있는 링크를 통해 실행되는 경우 다른 솔루션은 GRE 엔드포인트 라우터 간의 모든 인터페이스와 링크에서 MTU를 1524(GRE 오버헤드의 경우 1500 + 24)로 늘리는 것입니다.

추가 솔루션

위 옵션을 사용할 수 없는 경우 다음 옵션이 유용할 수 있습니다.

- 정책 라우팅을 사용하여 데이터 IP 패킷에서 DF 비트를 지우고 설정합니다(Cisco IOS® Software 릴리스 12.1(6) 이상에서 사용 가능).

```
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
```

이렇게 하면 데이터 IP 패킷이 GRE로 캡슐화되기 전에 프래그먼트화될 수 있습니다. 그런 다음 수신 엔드 호스트가 데이터 IP 패킷을 다시 어셈블해야 합니다. 이것은 보통 문제가 아닙니다.

- 라우터를 통과하는 SYN 패킷의 TCP MSS 옵션 값을 변경합니다(IOS 12.2(4)T 이상에서 사용 가능). 이렇게 하면 TCP SYN 패킷의 MSS 옵션 값이 줄어들어 ip tcp adjust-mss value 명령의 값보다 작아야 합니다(이 경우 1436(MTU - IP, TCP 및 GRE 헤더 크기 제외). 이제 엔드 호스트

가 이 값보다 크지 않은 TCP/IP 패킷을 전송합니다.

```
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.
```

- 마지막 옵션은 터널 인터페이스의 IP MTU를 1500으로 늘리는 것입니다(IOS 12.0 이상에서 사용 가능). 그러나 터널 IP MTU를 늘리면 원래 패킷의 DF 비트가 터널 패킷 헤더에 복사되지 않기 때문에 터널 패킷이 조각화됩니다. 이 시나리오에서는 GRE 터널의 반대쪽 끝에 있는 라우터가 GRE 헤더를 제거하고 내부 패킷을 전달하려면 먼저 GRE 터널 패킷을 재조합해야 합니다. IP 패킷 리어셈블리는 프로세스 스위치 모드에서 수행되며 메모리를 사용합니다. 따라서 이 옵션은 GRE 터널을 통해 패킷 처리량을 크게 줄일 수 있습니다.

```
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.
```

결론적으로, 위에서 언급한 프래그먼트화 문제 때문에 GRE 터널을 통해 인터넷을 탐색할 수 없는 가장 일반적인 원인은 바로 GRE 터널 때문입니다. 해결책은 ICMP 패킷을 허용하거나 위의 솔루션 중 하나에서 ICMP 문제를 해결하는 것입니다.

관련 정보

- [GRE 및 IPSEC의 IP 프래그먼트화, MTU, MSS 및 PMTUD 문제 해결](#)
- [귀사에 적합한 VPN 솔루션은 무엇입니까?](#)
- [GRE 지원 페이지](#)
- [GRE 컨피그레이션 예](#)
- [IP 라우팅 지원 페이지](#)
- [Technical Support - Cisco Systems](#)