Warum kann ich nicht im Internet surfen, wenn ich einen GRE-Tunnel verwende?

Inhalt

Einführung

Wenn der Datenverkehr einen GRE-Tunnel (Generic Routing Encapsulation) durchläuft, können Sie manchmal den **Ping-**Befehl und Telnet erfolgreich verwenden, jedoch keine Internetseiten herunterladen oder Dateien über File Transfer Protocol (FTP) übertragen. Dieses Dokument erläutert einen häufigen Grund für dieses Problem und bietet eine Reihe von Problemumgehungen.

Voraussetzungen

Anforderungen

Dieses Dokument erfordert ein grundlegendes Verständnis der GRE. Weitere Informationen zu GRE finden Sie in diesen Dokumenten:

- Allgemeine Routing-Kapselung
- Der Abschnitt Konfiguration eines GRE-Tunnels in Site-to-Site- und Extranet-VPN-Geschäftsszenarien

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

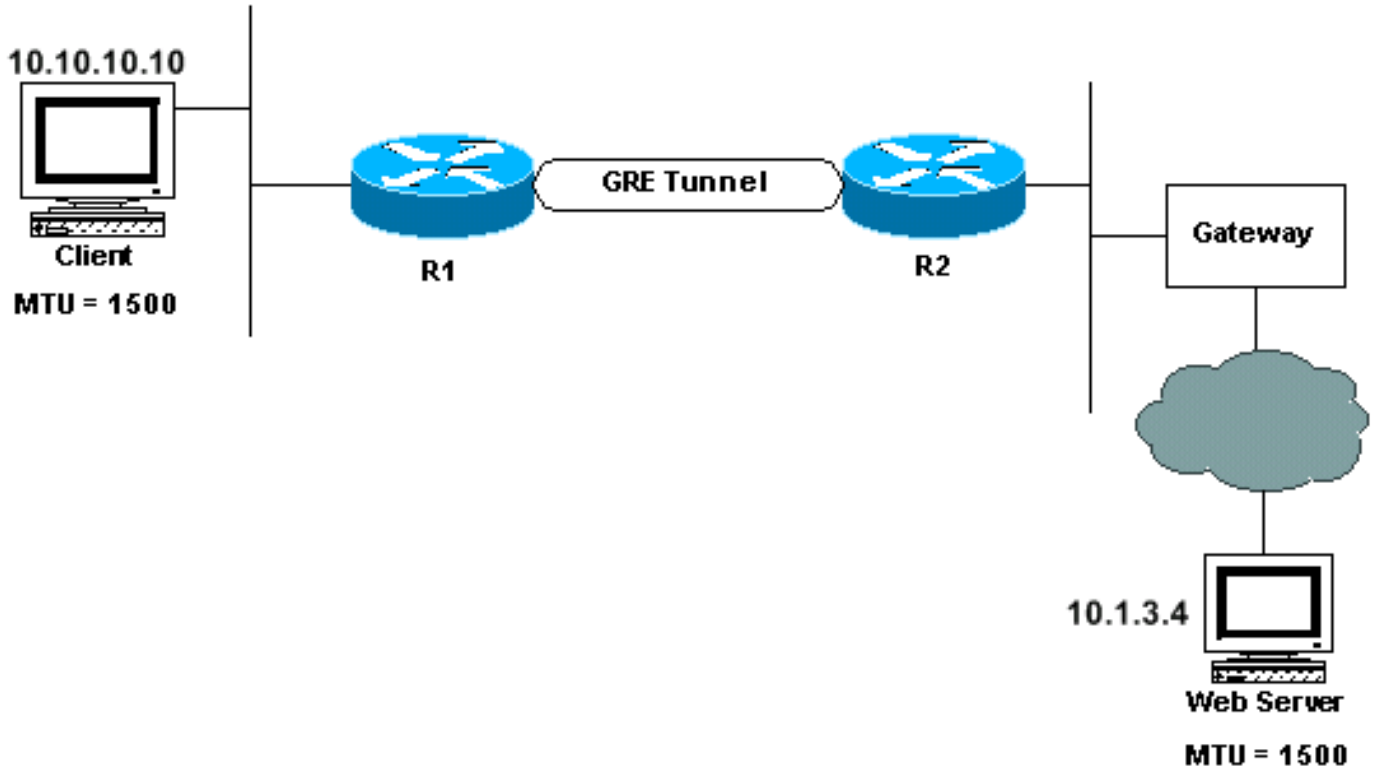
Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Paketfragmentierung und ICMP-Nachrichten

In diesem Dokument wird dieses Netzwerkdiagramm als Beispiel verwendet:



Wenn der Client im obigen Diagramm auf eine Seite im Internet zugreifen möchte, richtet er eine TCP-Sitzung mit dem Webserver ein. Während dieses Vorgangs geben der Client und der Webserver ihre maximale Segmentgröße (MSS) bekannt und geben gegenseitig an, dass sie TCP-Segmente bis zu dieser Größe akzeptieren können. Beim Empfang der MSS-Option berechnet jedes Gerät die Größe des Segments, das gesendet werden kann. Dies wird als Send Max Segment Size (SMSS) bezeichnet und entspricht dem kleineren der beiden MSSs. Weitere Informationen zur maximalen TCP-Segmentgröße finden Sie unter RFC 879 .

Angenommen, der Webserver im obigen Beispiel bestimmt, dass er Pakete mit einer Länge von bis zu 1.500 Byte senden kann. Es sendet daher ein 1500-Byte-Paket an den Client und legt im IP-Header das DF-Bit (don't fragment) fest. Wenn das Paket bei R2 ankommt, versucht der Router, es in das Tunnelpaket zu kapseln. Bei der GRE-Tunnelschnittstelle ist die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) für die IP 24 Byte kleiner als die IP-MTU der tatsächlichen ausgehenden Schnittstelle. Für eine ausgehende Ethernet-Schnittstelle bedeutet dies, dass die IP-MTU auf der Tunnelschnittstelle 1500 minus 24 oder 1476 Byte beträgt.

R2 versucht, ein 1500-Byte-IP-Paket an eine 1476-Byte-IP-MTU-Schnittstelle zu senden. Da dies nicht möglich ist, muss R2 das Paket fragmentieren und ein Paket von 1476 Byte (Daten- und IP-Header) und ein Paket von 44 Byte (24 Byte Daten und ein neuer IP-Header von 20 Byte) erstellen. R2 kapselt dann beide Pakete, um Pakete mit 1500 bzw. 68 Byte zu erhalten. Diese

Pakete können nun über die tatsächliche ausgehende Schnittstelle mit einer IP-MTU von 1500 Byte gesendet werden.

Denken Sie jedoch daran, dass das von R2 empfangene Paket über das DF-Bit verfügt. Daher kann R2 das Paket nicht fragmentieren, sondern muss den Webserver anweisen, kleinere Pakete zu senden. Dazu sendet er ein ICMP-Paket (Internet Control Message Protocol) vom Typ 3, Code 4 (Ziel nicht erreichbar). Fragmentierung erforderlich und DF festgelegt). Diese ICMP-Nachricht enthält die vom Webserver zu verwendende MTU, die diese Nachricht empfangen und die Paketgröße entsprechend anpassen sollte.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die wichtigen Informationen zu Debug-Befehlen.

Sie können die von R2 gesendeten ICMP-Meldungen anzeigen, indem Sie den Befehl **debug ip icmp** aktivieren:

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

Gesperrte ICMP-Nachrichten

Ein häufiges Problem tritt auf, wenn ICMP-Meldungen entlang des Pfads zum Webserver blockiert werden. In diesem Fall erreicht das ICMP-Paket nie den Webserver, wodurch das Übergeben von Daten zwischen Client und Server verhindert wird.

Lösungen

Eine dieser vier Lösungen sollte das Problem lösen:

- Finden Sie heraus, wo auf dem Pfad die ICMP-Nachricht blockiert ist, und sehen Sie, ob Sie sie zulassen können.
- Legen Sie die MTU auf der Netzwerkschnittstelle des Clients auf 1476 Byte fest, wodurch der SMSS kleiner werden muss, sodass Pakete nicht fragmentiert werden müssen, wenn sie R2 erreichen. Wenn Sie jedoch die MTU für den Client ändern, sollten Sie auch die MTU für alle Geräte ändern, die das Netzwerk mit diesem Client gemeinsam nutzen. In einem Ethernet-Segment kann dies eine große Anzahl von Geräten sein.
- Verwenden Sie einen Proxyserver (oder, besser noch, eine Web-Cache-Engine) zwischen R2 und dem Gateway-Router, und lassen Sie den Proxy-Server alle Internetseiten anfordern.
- Wenn der GRE-Tunnel über Verbindungen ausgeführt wird, die eine MTU von mehr als 1.500 Byte plus dem Tunnel-Header aufweisen können, besteht eine andere Lösung darin, die MTU auf 1.524 (1.500 plus 24 für den GRE-Overhead) an allen Schnittstellen und Verbindungen zwischen den GRE-Endpunkt-Routern zu erhöhen.

Weitere Lösungen

Wenn die oben genannten Optionen nicht praktikabel sind, können diese Optionen nützlich sein:

- Verwenden Sie Policy-Routing, um das DF-Bit im Daten-IP-Paket zu löschen und festzulegen (verfügbar in Cisco IOS® Software Release 12.1(6) und höher).
```
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
```

Dadurch kann das Daten-IP-Paket fragmentiert werden, bevor es GRE-gekapselt wird. Der empfangende End-Host muss dann die Daten-IP-Pakete neu zusammenstellen. Das ist normalerweise kein Problem.

- Ändern Sie den Wert der TCP-MSS-Option für SYN-Pakete, die den Router durchlaufen (verfügbar in IOS 12.2(4)T und höher). Dadurch wird der Wert der MSS-Option im TCP-SYN-Paket reduziert, sodass er kleiner ist als der Wert im Befehl **ip tcp adjust-mss**, in diesem Fall 1436 (MTU abzüglich der Größe der IP-, TCP- und GRE-Header). Die End-Hosts senden nun TCP/IP-Pakete, die nicht größer als dieser Wert sind.

```
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.
```

- Eine letzte Option besteht darin, die IP-MTU auf der Tunnelschnittstelle auf 1500 zu erhöhen (verfügbar ab IOS 12.0). Durch die Erhöhung der Tunnel-IP-MTU werden die Tunnelpakete fragmentiert, da das DF-Bit des ursprünglichen Pakets nicht in den Tunnel-Paket-Header kopiert wird. In diesem Szenario muss der Router am anderen Ende des GRE-Tunnels das GRE-Tunnelpaket neu zusammenbauen, bevor er den GRE-Header entfernen und das innere Paket weiterleiten kann. Die IP-Paketreassemblierung erfolgt im Prozess-Switch-Modus und verwendet Speicher. Daher kann diese Option den Paketdurchsatz durch den GRE-Tunnel erheblich reduzieren.

```
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.
```

Zusammenfassend lässt sich feststellen, dass die häufigste Ursache dafür, dass nicht über einen GRE-Tunnel im Internet surfen kann, in der oben genannten Fragmentierungsproblematik liegt. Die Lösung besteht darin, die ICMP-Pakete zuzulassen oder das ICMP-Problem mit einer der oben genannten Lösungen zu umgehen.

Zugehörige Informationen

- Lösung von Problemen mit IP-Fragmentierung, MTU, MSS und PMTUD mit GRE und IPSEC
- Welche VPN-Lösung ist die richtige für Sie?
- GRE-Support-Seiten
- GRE-Konfigurationsbeispiele
- Support-Seite für IP-Routing
- Technischer Support - Cisco Systems