Почему нельзя просматривать Интернет при использовании туннеля GRE?

Содержание

Введение

Иногда при прохождении трафика через туннель общей инкапсуляции для маршрутизации (GRE) можно успешно использовать команду **ping** и Telnet, но нельзя загружать Интернет-страницы или пересылать файлы при помощи протокола передачи файлов (FTP). Данный документ содержит описание стандартной причины этой проблемы, а также методов ее обхода.

Предварительные условия

Требования

Для понимания данного документа требуется общее знание протокола GRE. Дополнительные сведения о GRE доступны в следующих документах:

- Настраиваемая инкапсуляция маршрутизации
- Раздел Настройка GRE-туннеля статьи Бизнес-сценарии межузловых и внешних виртуальных частных сетей

Используемые компоненты

Данный документ не ограничен отдельными версиями программного и аппаратного обеспечения.

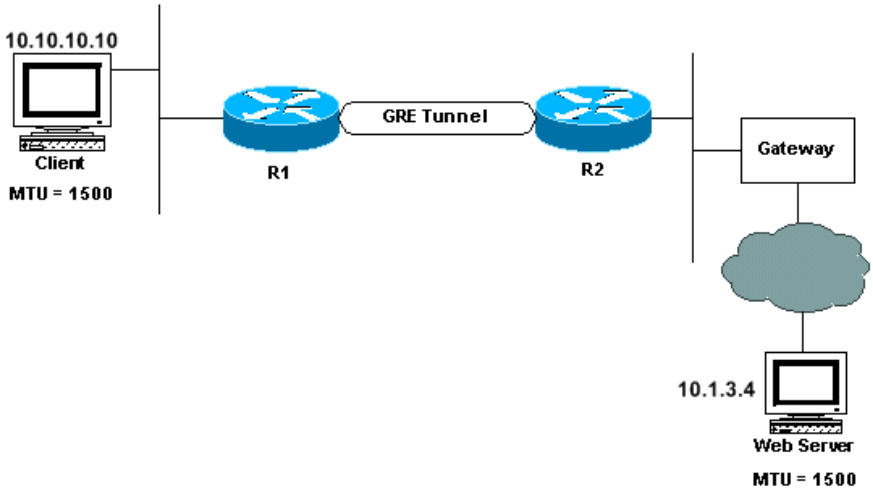
Для поиска дополнительной информации о командах в данном документе используйте средство Command Lookup (только для зарегистрированных клиентов).

Условные обозначения

Дополнительные сведения об условных обозначениях см. в разделе Технические советы Cisco. Условные обозначения.

Фрагментация пакетов и сообщения ICMP

В данном документе в качестве примера используется следующая схема сети:



На диаграмме, представленной выше, показано, как устанавливается сеанс TCP с веб-сервером, когда клиент хочет получить доступ к странице в Интернет. Во время этого процесса клиент и веб-сервер обмениваются значениями MSS (максимальный размер сегмента), которые задают ограничения на размер принимаемых TCP-сегментов. Получив значение MSS, каждое устройство вычисляет допустимый размер отправляемого сегмента. Такой размер называется максимальным размером сегмента для отправки (SMSS); он равен меньшему из значений MSS. Дополнительные сведения о максимальном размере сегмента TCP см. в документе RFC 879 .

Предположим, что веб-сервер в предыдущем примере определяет размер отправляемых пакетов в 1500 байт. Следовательно, сервер отсылает клиенту пакет длиной 1500 байт и в IP-заголовке задает необходимость включения бита "не фрагментировать" (DF). Когда пакет поступает на R2, маршрутизатор пытается инкапсулировать его в туннельный пакет. При использовании туннельного интерфейса GRE максимальный размер передаваемого блока данных (MTU) на 24 байта меньше, чем IP MTU реального исходящего интерфейса. Для исходящего интерфейса Ethernet максимальный размер передаваемого блока данных IP на туннельном интерфейсе будет составлять 1500 минус 24, что составляет 1476 байт.

R2 осуществляет попытку отправки IP-пакета в 1500 байт на 1476-байтный IP MTU интерфейс. Поскольку это невозможно, R2 необходимо фрагментировать пакет, создав один пакет размером 1476 байт (IP-заголовок и данные) и один пакет размером 44 байта (24 байта данных и новый IP-заголовок размером 20 байт). R2 затем осуществляет инкапсуляцию GRE двух пакетов для получения пакетов 1500 и 68 байт, соответственно. Эти пакеты теперь можно отправить через реальный исходящий интерфейс, MTU IP которого составляет 1500 байт.

Однако помните, что пакет, полученный R2, имеет набор битов DF. Следовательно, R2 не может фрагментировать пакеты; вместо этого он должен подать команду веб-серверу для сокращения размеров пакетов. Для этого он отсылает пакет протокола управляющих сообщений Интернета (ICMP) тип 3 код 4 (Назначение недоступно; необходима фрагментация и набор DF). В этом сообщении ICMP содержатся правильный MTU для использования веб-сервером, который должен получить это сообщение и соответствующим образом изменить размер пакета.

Примечание. Прежде чем выполнять какие-либо команды **отладки** , ознакомьтесь с документом Важные сведения о командах отладки.

Для просмотра сообщений ICMP, переданных системой R2, выполните команду **debug ip icmp**:

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

Заблокированные сообщения ICMP

Блокировка сообщений ICMP на пути к веб-серверу - это типичная проблема. Когда это происходит, пакет ICMP не достигает веб-сервера, что препятствует передаче данных между клиентом и сервером.

Решения

Ниже приводятся 4 способа устранения этой проблемы.

- Определите, в каком месте пути заблокировано сообщение ICMP и можно ли его разблокировать.
- Установите значение MTU на сетевом интерфейсе клиента равным 1476 байт, принуждая SMSS быть меньше, чтобы пакеты не фрагментировались при достижении R2. Однако, если вы изменяете MTU для клиента, следует также изменить MTU для всех устройств, работающих в сети вместе с клиентом. В сегменте Ethernet может присутствовать большое количество этих устройств.
- Используйте прокси-сервер (или еще лучше Web cache engine) между R2 и маршрутизатором шлюза и позвольте прокси-серверу посылать запрос ко всем Интернет-страницам.
- Если туннель GRE проходит по соединениям, для которых значение MTU может превышать1500 байт плюс заголовок туннеля, решением является увеличение значения MTU до 1524 байт (1500 плюс 24 байта для служебных данных GRE) для всех интерфейсов и соединений между конечными маршрутизаторами GRE.

Дальнейшие решения

Если приведенные выше параметры недопустимы, можно использовать следующие параметры.

- Используйте политику маршрутизации для очистки и установки DF-бита в IP-пакете данных (доступном в Cisco IOS® версии 12.1(6) и выше).

```
interface ethernet0
...
 ip policy route-map clear-df

!--- Эта команда используется для идентификации карты маршрутов,

!--- применяемой для маршрутизации на основе политик на интерфейсе.

!--- Используйте команду ip policy route-map

!--- в режиме настройки интерфейса.

route-map clear-df permit 10
match ip address 101
 set ip df 0

!--- Эта команда используется для изменения

!--- значения бита "не фрагментировать" (DF) в IP-заголовке.

!--- Используйте эту команду в режиме настройки карты маршрутизации.

access-list 101 permit tcp 10.1.3.0 0.0.0.255 any
```

  Это позволит пакетам данных IP фрагментироваться перед инкапсуляцией GRE. Принимающий конечный хост должен затем повторно собрать IP-пакеты данных, что не является сложной задачей.

- Измените значение параметра TCP MSS для пакетов SYN, которые проходят сквозь маршрутизатор (доступен в IOS версии 12.2(4)T и выше). Это позволит сделать значение параметра MSS в пакете TCP SYN меньше, чем значение в команде **ip tcp adjust-mss *value***, что в данном случае составляет 1436 (MTU минус размер заголовков IP, TCP и GRE). После этого конечные хосты отправляют пакеты TCP/IP размером менее указанного значения.

```
interface tunnel0
...
 ip tcp adjust-mss 1436
```

```
!--- Эта команда используется для изменения значения максимального размера сегмента (MSS)

!--- пакетов TCP SYN, передаваемых через маршрутизатор.

!--- Максимальный размер сегмента находится в диапазоне от 500 до 1460.
```

- Последний параметр – увеличение IP MTU на туннельном интерфейсе до 1500 (доступно в IOS 12.0 и выше). Однако увеличение туннеля IP MTU приводит к фрагментации туннельных пакетов, поскольку DF-бит исходного пакета не копируется в заголовок туннельного пакета. В этом сценарии перед тем, как удалить заголовок GRE и переслать внутренний пакет, маршрутизатор на другом конце туннеля GRE должен повторно собрать туннельный пакет GRE. Повторная сборка IP-пакета выполняется в режиме обычной коммутации и использует память. Следовательно, этот параметр может значительно уменьшить проброс пакетов через GRE-туннель.

```
interface tunnel0
  ...
ip mtu 1500

!--- Эта команда используется для задания максимального размера передаваемого

!--- блока данных (MTU) IP-пакетов, отправляемых на интерфейс. Минимальный размер,

!--- который можно задать, равен 128 байтам; максимальный размер зависит от среды интерфейса.
```

В заключение необходимо упомянуть, что наиболее частой причиной невозможности просмотра Интернет-страниц через туннель GRE становится упомянутая выше проблема фрагментации. Решение заключается в разрешении пакетов ICMP или использование любого из приведенных выше решений.

Дополнительные сведения

- **IP-фрагментация и PMTUD**
- **Выбор подходящего VPN-решения.**
- **Страница поддержки GRE**
- **Примеры настройки GRE**
- **Страница поддержки IP-маршрутизации**
- **Техническая поддержка Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/92057/56.shtml