# PIX/ASA 7.x и IOS: Фрагментация VPN

## Содержание



## Введение

Этот документ излагает алгоритм действий для устранения проблем, связанных с фрагментацией пакетов. Примером проблемы с фрагментацией является ситуация, в которой сетевой ресурс откликается на команды ping, но при этом недоступен для подключения из определенного приложения, например, клиента электронной почты или базы данных.

## Предварительные условия

### Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Подключение между узлами VPN

### Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям

программного обеспечения и оборудования.

### Схема сети

В настоящем документе используется следующая схема сети:

### Родственные продукты

Эта конфигурация может также использоваться со следующими версиями программного/аппаратного обеспечения:

- Маршрутизаторы IOS
- Устройства безопасности PIX/ASA

### Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

## Общие сведения

Поддержка IP максимальная длина 65,536 байтов для пакета IP, но большинство протоколов уровня канала связи поддерживает намного меньшую длину, названную максимальным размером передаваемого блока данных (MTU). На основе поддерживаемого MTU может быть необходимо разбить (фрагмент) пакет IP для передачи его через определенный тип носителя уровня канала передачи данных. Назначение тогда должно повторно собрать фрагменты назад в исходный, завершенный пакет IP.

При использовании VPN для защиты данных между двумя узлами VPN, дополнительные издержки добавлены к исходным данным, которые могут потребовать, чтобы произошла фрагментация. Эти поля списка таблицы, которые потенциально должны быть добавлены к защищенным данным для поддержки VPN-подключения. Обратите внимание на то, что множественные протоколы могут быть необходимыми, который увеличивает размер оригинального пакета. Например, при использовании IP - безопасного соединения DMVPN L2L между двумя маршрутизаторами Cisco где вы внедрили Туннель GRE, вам нужны эти дополнительные издержки: ESP, GRE и внешний IP - заголовок. Если у вас есть соединение клиентского программного обеспечения IPSec со Шлюзом VPN, когда трафик проходит устройство адреса, вам нужны эти дополнительные издержки для Трансляции сетевых адресов - прохождение (NAT-T), а также внешний IP - заголовок для соединения туннельного режима.

### Проблемы с фрагментацией

Когда источник передает пакет назначению, он размещает значение в поле флагов управления IP - заголовков, которое влияет на фрагментацию пакета промежуточными устройствами. Флаг управления три бита длиной, но только первые два используются на фрагментации. Если второй бит установлен в 0, пакету позволяют быть фрагментированным; если это установлено в 1, пакету не позволяют быть фрагментированным. *Второй бит называют битом don't fragment (DF)*. Третий бит задает, когда фрагментация происходит, является ли этот фрагментированный пакет последним

фрагментом (набор к 0), или если существует больше фрагментов (набор к 1), которые составляют пакет.

Существует четыре области, которые могут создать проблемы, когда требуется фрагментация:

- Дополнительные издержки в циклах ЦПУ и памяти требуются двумя устройствами, которые выполняют фрагментацию и повторную сборку.
- Если один фрагмент отброшен на пути к назначению, пакет не может быть повторно собран, и целый пакет должен быть фрагментирован и передан снова. Это создает дополнительные проблемы с пропускной способностью, особенно в ситуациях, где рассматриваемый трафик с ограниченной скоростью, и источник передает трафик выше допустимого предела.
- Фильтрация пакетов и самонастраивающиеся межсетевые экраны могут испытать затруднения при обработке фрагментов. Когда фрагментация происходит, первый фрагмент содержит внешний IP - заголовок, внутренний заголовок, такой как TCP, UDP, ESP и другие и часть информационного наполнения. Последующие фрагменты оригинального пакета заключают внешний IP - заголовок и продолжение информационного наполнения. Проблема с этим процессом состоит в том, что определенные межсетевые экраны должны видеть информацию о внутреннем заголовке в каждом пакете для принятия интеллектуальных решений фильтрации; если та информация отсутствует, они непреднамеренно могут отбросить все фрагменты, за исключением первого.
- *Источник IP-заголовка пакета может установить для третьего управляющего бита значение don't fragment, означающее, что если промежуточное устройство получает пакет и должно разбить его на фрагменты, то оно не может выполнить данное действие.* Вместо этого промежуточное устройство отбрасывает пакет.

# Основная задача

## Обнаружение фрагментации

Большинство сетей использует Ethernet со значением MTU по умолчанию 1,500 байтов, которое, как правило, используется для пакетов IP. Чтобы узнать, происходит ли фрагментация или необходима, но не может быть сделана (бит DF установлен), сначала переведите свой сеанс VPN в рабочее состояние. Затем можно использовать любую из этих четырех процедур для обнаружения фрагментации.

1. Пропингуйте устройство, расположенное в другом конце. Это находится под предположением, что прозванивание позволено через туннель. Если это успешно, попытайтесь обратиться к приложению через то же устройство; например, если сервер Microsoft E-mail или Удаленного рабочего стола через туннель, открытый Outlook и попытку загрузить вашу Электронную почту или попробовать к Удаленному рабочему столу к серверу. Если это не работает, и у вас есть корректное разрешение имен, существует хороший шанс, что фрагментация является проблемой.
2. От Windows устройство используют это: **C:\> ping -f -l packet_size_in_bytes destination_IP_address.Параметр -f используется, чтобы указывать, что пакет не предназначен для фрагментации. Параметр -l используется, чтобы указывать длину**

**пакета. Сначала используйте размер пакета, равный 1500. Например, отправьте запрос "ICMP-эхо" -f -l 1500 192.168.100.** Если фрагментация требуется, но не может быть выполнена, вы получаете сообщение, такое как это: *Packets need to be fragmented but DF set.*

3. **В маршрутизаторах Cisco введите команду debug ip icmp и используйте команду extended ping.** *Если придет сообщение ICMP:dst (x.x.x.x) fragmentation needed and DF set, unreachable sent to y.y.y.y, где x.x.x.x – это устройство назначения, а y.y.y.y – это ваш маршрутизатор, промежуточное устройство сообщит о необходимости фрагментации, но так как в эхо-запросе установлен бит DF, промежуточное устройство не может разбить его и направить для следующего перехода.* В этом случае постепенно уменьшайте максимальный размер передаваемого блока данных эхо-запросов, пока вы не находите тот, который работает.
4. На Cisco Security Устройства используйте фильтр перехвата.CiscoASA (config) #`access-list outside_test permit tcp any host 172.22.1.1 eq 80`**Примечание:** *Если оставить источник в качестве any, это позволит администратору проводить мониторинг преобразования сетевых адресов (NAT).*CiscoASA (config) #`access-list outside_test permit tcp host 172.22.1.1 eq 80 any`**Примечание:** При инвертировании сведений об источнике и назначении они позволяют ответному трафику быть перехваченным.`ciscoasa(config)# capture outside_interface access-list outside_test interface outside`**Пользователю необходимо начать новый сеанс связи с приложением X. После выполнения пользователем данного действия, администратору ASA необходимо применить команду show capture outside_interface.**

## Решения проблем Framentation

Существуют другие способы, которыми можно решить проблемы с фрагментацией. Они обсуждены в этом разделе.

### Способ 1: Статический параметр MTU

Статический Параметр MTU может решить проблемы с фрагментацией.

1. **Изменение MTU на маршрутизаторе:**Обратите внимание на то, что при ручной установке MTU на устройстве он говорит устройство, которое действует как Шлюз VPN к полученным пакетам фрагмента, прежде чем он защитит и передаст им через туннель. Это предпочтительно для наличия маршрутизатора, защищают трафик и затем фрагментируют его, но устройство фрагментирует его.**% Warning:** При изменении максимального размера передаваемого блока данных на каком-либо интерфейсе устройства он заставляет все туннели, завершенные на том интерфейсе быть разъединенными и восстановленными.**В маршрутизаторах Cisco используйте команду ip mtu для настройки размера MTU на интерфейсе, где подключается VPN:**`router (config)# interface type [slot_#/] port_# router (config-if)# ip mtu MTU_size_in_bytes`
2. **Изменение MTU на ASA/PIX:В устройствах ASA/PIX используйте команду mtu, чтобы настроить размер MTU в режиме глобальной конфигурации.** *По умолчанию MTU равен 1500. Например, если в устройстве защиты имеется интерфейс с именем Outside (где подключается VPN), и вам необходимо (в соответствии с оценками в разделе Обнаружение фрагментации) назначить фрагменту длину, равную 1380, используйте*

*следующую команду:*`security appliance (config)# mtu Outside 1380`

## Способ 2: Maximum Segment Size TCP

Maximum Segment Size TCP может решить проблемы с фрагментацией.

**Примечание:** Эта функция только работает с TCP; другие Протоколы "IP" должны использовать другое решение решить проблемы Фрагментации ip. Даже при установке ip mtu на маршрутизаторе он не влияет на то, о чем с двумя окончаниями хосты выполняют согласование в трехэтапном установлении связи TCP с TCP MSS.

1. **Изменение MSS на маршрутизаторе:**Фрагментация происходит при Трафике TCP, потому что Трафик TCP обычно используется для переноса больших количеств данных. TCP поддерживает функцию, названную Maximum Segment Size (MSS) TCP, который позволяет этим двум устройствам выполнять согласование о подходящем размере для Трафика TCP. Значение MSS настроено статически на каждом устройстве и представляет размер буфера для использования для ожидаемого пакета. Когда два устройства устанавливают TCP - подключения, они сравнивают локальное значение MSS с локальным значением MTU в трехэтапном установлении связи; какой бы ни ниже, передается удаленному узлу. Два узла тогда используют ниже двух обмененных значений. Для настройки этой функции сделайте это:**В маршрутизаторах Cisco используйте команду tcp adjust-mss на интерфейсе, где подключается VPN.**`router (config)# interface type [slot_#/] port_# router (config-if)# ip tcp adjust-mss MSS_Size_in_bytes`
2. **Изменение MSS на ASA/PIX:Чтобы убедиться, что максимальное значение сегмента TCP не превышает установленного значения, и данное значение не меньше указанного размера, используйте команду sysopt connection в режиме глобальной конфигурации. Чтобы восстановить настройку по умолчанию, используйте аргумент no данной команды.** Значение максимума по умолчанию составляет 1380 байтов. Минимальная возможность отключена по умолчанию (набор к 0).Для изменения предела MSS максимума по умолчанию сделайте это:`security appliance (config)# sysopt connection tcp-mss MSS_size_in_bytes` **Примечание:** Если вы заставляете максимальный размер быть больше, чем 1380, пакеты могут стать фрагментированными, зависящими от максимального размера передаваемого блока данных (который является 1500 по умолчанию). Большие числа фрагментов могут повлиять на производительность устройства безопасности, когда это использует Функцию защиты Frag. При установке минимального размера он препятствует тому, чтобы сервер TCP передал много маленьких пакетов данных TCP клиенту и повлиял на производительность сервера и сети.Для изменения минимального предела MSS сделайте это:`security appliance (config)# sysopt connection tcp-mss minimum MSS_size_in_bytes`устройство безопасности (config) # `sysopt connection tcp-mss minimum MSS_size_in_bytes`**Примечание:** См. Конфигурацию MPF для Разрешения Пакетов, которые Превышают раздел MSS документа PIX/ASA 7. X Проблем: Превышенный MSS - Клиенты HTTP не Могут Перейти к Некоторым веб-сайтам для получения дополнительной информации, чтобы позволить превышенным пакетам MSS другой метод.

## Метод 3: обнаружение MTU-маршрута (PMTUD)

PMTUD может решить проблемы с фрагментацией.

Основная проблема с TCP MSS - то, что администратор должен знать что значение настроить на вашем маршрутизаторе для предотвращения возникновения фрагментации. Это может быть проблемой, если несколько путей существуют между вами и удаленным местоположением VPN, или, когда вы делаете свой начальный запрос, вы находите, что второе - или третий меньший MTU, вместо самого маленького, основывается на решении о маршрутизации, используемом в вашем начальном запросе. С PMTUD можно определить значение MTU для пакетов IP, которое избегает фрагментации. Если сообщения ICMP заблокированы маршрутизатором, MTU путь сломан, и от пакетов с Набором битов DF сбрасывают. **Используйте команду set ip df, чтобы удалить значение DF бита и разрешить фрагментацию и отправку пакета.** Фрагментация может замедлить скорость пересылки пакетов в сети, но списки доступа могут использоваться для ограничения количества пакетов, на которых очищен бит DF.

1. Три проблемы могут заставить PMTUD не функционировать:Промежуточный маршрутизатор может отбросить пакет и не ответить сообщением ICMP. Это не очень распространено в Интернете, но может быть распространено в сети, где маршрутизаторы настроены для не отвечания сообщениями о недоступности ICMP.Промежуточный маршрутизатор может ответить сообщением о недоступности ICMP, но на потоке return межсетевой экран блокирует это сообщение. Это - большее обычное явление.Сообщение о недоступности ICMP делает свой путь назад к источнику, но источник игнорирует сообщение фрагментации. Это является самым редким из трех проблем.При испытании первой проблемы вы могли бы или очистить бит DF в IP - заголовке, что источник, размещенный там или вручную, отрегулировал размер TCP MSS. Для очистки бита DF промежуточный маршрутизатор должен изменить значение от 1 до 0. Обычно это сделано маршрутизатором в вашей сети, прежде чем пакет оставит сеть. Это - простая конфигурация кода, которая делает это на Маршрутизаторе на основе IOS:`Router (config) # **access-list** *ACL_#* **permit tcp any any** Router (config) # **route-map** *route_map_name* **permit** *seq#* Router (config-route-map) # **match ip address** *ACL_#* Router (config-route-map) # **set ip df** *0* Router (config-route-map) # **exit** Router (config) # **interface** *type [slot#/]port #* Router (config-if) # **ip policy router-map** *route_map_name*`
2. **PMTUD и туннели GRE**По умолчанию маршрутизатор не выполняет PMTUD на Пакетах многопротокольного туннеля GRE, которые это генерирует само. Чтобы включить PMTUD на Туннельных интерфейсах GRE и иметь маршрутизатор, участвуют в настраивающем процессе MTU для источника/целевых устройств для трафика, который пересекает туннель, используйте эту конфигурацию:Маршрутизатор (config) # `interface tunnel` tunnel_#Маршрутизатор (config-if) # `tunnel path-mtu-discovery`**С помощью команды tunnel path-mtu-discovery активизируется PMTUD для интерфейса туннеля GRE маршрутизатора.** Дополнительный параметр таймера возраста задает количество минут, после которых туннельный интерфейс перезагружает обнаруженный размер максимального значения размера блока данных минус 24 байта для заголовка GRE. *Если указать infinite для таймера, он не будет использоваться.* Параметр mtu min задает минимальный номер байтов, который включает значение MTU.
3. **PIX/ASA 7.x - Clear Don't Fragment (DF) или обработка больших файлов или пакетов.**Вы все еще неспособны должным образом обратиться к Интернету, большим файлам или приложениям через туннель, потому что это дает это сообщение об ошибках максимального размера передаваемого блока данных:
   **`PMTU-D packet 1440 bytes greater than effective mtu 1434, dest_addr=10.70.25.1,`**

`src_addr=10.10.97.55, prot=TCP` Для решения этого, убедиться очистить бит DF от внешнего интерфейса устройства. **Задайте конфигурацию политике DF-бита для пакетов IPSec с помощью команды crypto ipsec df-bit в режиме глобальной настройки.** `pix(config)# crypto ipsec df-bit clear-df outside` Бит DF с функцией Туннелей IPSec позволяет вам задать, может ли устройство безопасности очиститься, установить, или копировать `Don't Fragment (DF)` укусил от инкапсулированного заголовка. Бит DF в рамках IP - заголовка определяет, позволяют ли устройству фрагментировать пакет.**Используйте команду crypto ipsec df-bit в режиме глобальной конфигурации, чтобы настроить устройство защиты для указания DF-бита в инкапсулированном заголовке.**При инкапсуляции Трафика IPSec туннельного режима используйте значение `clear-df` для бита DF. Эта установка позволяет устройству передать пакеты больше, чем доступный максимальный размер передаваемого блока данных. Если вы не знаете доступный максимальный размер передаваемого блока данных, также эта установка является соответствующей.

**Примечание: Если проблемы фрагментации остаются, и происходит отбрасывание пакетов, дополнительно можно установить размер MTU вручную с помощью команды ip mtu tunnel interface.** В этом случае маршрутизатор фрагментирует пакет, прежде чем это защитит его. Эта команда может использоваться в сочетании с PMTUD и/или TCP MSS.

# Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

# Устранение неполадок

## Ошибка шифрования VPN

Предположите, что Туннель IPSec установил между маршрутизатором и PIX. Если вы видите сообщения ошибки шифрования, что пакеты отброшены, выполняют эти шаги для решения вопроса:

1. Выполните отслеживание средств прослушивания от клиента к стороне сервера для обнаружения, который является лучшим MTU для использования.Можно также использовать эхо - тест (ping test):
   `ping -l 1400 192.168.1.1 -f` 192.168.1.1 IP-адрес удаленной машины.
2. Продолжите уменьшать значение 1400 на 20, пока не будет ответ.**Примечание:** Волшебное значение, которое работает в большинстве экземпляров, является 1300.
3. После того, как соответствующий Maximum Segment Size достигнут, отрегулируйте его соответственно для устройств в использовании:На межсетевом экране PIX:
   `sysopt connection tcpmss 1300` На маршрутизаторе:
   `ip tcp adjust-mss 1300`

## RDP и проблемы Citrix

**Проблема:**

Можно пропинговать между сетями VPN, но Протокол удаленного рабочего стола (RDP) и соединения Citrix не могут быть установлены через туннель.

**Решение:**

Проблемой может быть максимальный размер передаваемого блока данных на ПК позади PIX/ASA. Установите максимальный размер передаваемого блока данных как 1300 для клиентского компьютера и попытайтесь установить соединение Citrix через VPN-туннель.

## Дополнительные сведения

- "Устранение проблем с фрагментацией IP, значениями MTU, MSS, и PMTUD для GRE и IPSEC"
- Проблема PIX/ASA 7.0: Превышено допустимое значение MSS — HTTP-клиенты не могут просматривать определенные веб-узлы
- Устранение наиболее распространенных проблем удаленных VPN-подключений и VPN-туннелей LAN — LAN на базе протокола IPSec
- Почему нельзя просматривать интернет при использовании туннеля GRE
- Cisco Systems – техническая поддержка и документация