Разрешение соединений PPTP/L2TP через PIX/ASA/FWSM

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Теоретические сведения
Условные обозначения
PPTP с внутренним клиентом и внешним сервером
Схема сети
Команды, добавляемые к версии 6.2 и более ранним
Команды, добавляемые к версии 6.3
Команды для Добавления для Версий 7.x и 8.0 с помощью контроля
Команды для Добавления для Версий 7.x и 8.0 с помощью ACL
Конфигурация для версии 6.2 и более ранних версий
L2TP с клиентом внутри и сервер снаружи
PPTP с внешним клиентом и внутренним сервером
Схема сети
Приказывает добавить ко всем версиям
L2TP с клиентом снаружи и сервер внутри
Позвольте L2TP По IPsec Через PIX/ASA 7.x и Выше
Проверка
Устранение неполадок
Множественный Сбой Соединений PPTP/L2TP при использовании PAT
Ошибка 800 при попытке соединиться с входящей VPN PPTP
Команды "debug"
Информация, обязательная для сбора в случае обращения в центр технической поддержки
Дополнительные сведения

Введение

Этот документ обсуждает конфигурацию, требуемую на Cisco Security Appliance / FWSM, чтобы позволить Протоколу PPTP / клиент Протокола туннелирования на уровне 2 (L2TP) соединяться с сервером PPTP через Технологию NAT.

FWSM 3.1.x и более поздний PPTP поддержек проходит с PAT. Используйте проверку PPTP для добавления этой функциональности.

Примечание: Используйте одинаковую конфигурацию PIX для FWSM.

Чтобы настроить устройство безопасности для приема соединений PPTP, обратитесь к документу "Настройка брандмауэра Cisco Secure PIX для использования PPTP".

Для настройки L2TP через IP-безопасность (IPsec) от удаленного Microsoft Windows 2000/2003 и клиентов Windows XP к офису корпорации Устройства безопасности PIX/ASA, которые используют предварительные общие ключи с Интернетом Microsoft Windows 2003 года, обращаются к L2TP По IPsec Между Windows 2000/XP PC и Использованием примера конфигурации PIX/ASA 7.2 Предварительного общего ключа.

Предварительные условия

Требования

Для попытки этой конфигурации у вас должны быть рабочий сервер PPTP и клиент перед включением PIX/ASA/FWSM.

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Версии межсетевого экрана Cisco PIX 6.x и выше
- Устройство безопасности серии 5500 Cisco ASA, которое выполняет версию 7.x или выше
- FWSM, который выполняет версию 3.1.x или выше

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Теоретические сведения

PPTP описывается в RFC 2637 . Этот протокол использует соединение TCP с портом 1723 и расширение общей инкапсуляции маршрутов (GRE) [протокол 47] для передачи реальных данных (кадр PPP). Соединение TCP инициируется клиентом вслед за соединением GRE, которое инициируется сервером.

Версия 6.2 и более ранняя информация

Поскольку подключение PPTP инициируется как TCP на одном порту, и ответ является протоколом GRE, Алгоритм адаптивной безопасности (ASA) PIX не знает, что отнесены трафики. Поэтому необходимо настроить ACL так, чтобы в них был разрешен обратный трафик в PIX. PPTP через PIX с NAT (сопоставление адресов один-в-один) работает, поскольку PIX использует для хранения записей о трансляции данных порта в TCP или заголовок User Datagram Protocol (UDP). PPTP через PIX с Port Address Translation (PAT) не работает, поскольку в GRE нет концепции портов.

Информация о версии 6.3

Функция адресной привязки PPTP в версии 6.3 позволяет трафику PPTP пересекать PIX,

когда настроено для PAT. В этом процессе также производится stateful-проверка пакетов PPTP. **Команда fixup protocol pptp проверяет пакеты PPTP и динамически создает соединения и трансляции GRE, необходимые для разрешения трафика PPTP**. В частности, брандмауэр проверяет объявления версии PPTP и последовательность запросов и ответов исходящего вызова. Как определяется в RFC 2637, производится проверка только PPTP версии 1. Дальнейшая проверка в управляющем канале TCP выключается, если версия, объявленная какой-либо из сторон, оказывается не версией 1. В дополнение отслеживается последовательность запросов и ответов исходящего вызова. Подключения и трансляции создаются динамически, как это необходимо для разрешения последующего вторичного трафика данных GRE. Чтобы трафик PPTP транслировался PAT, должна быть включена функция привязки PPTP.

Информация о версии 7.x

Механизм Контроля приложения PPTP в версии 7.x работает той же формой, как **pptp протокола FIXUP** делает в версии 6.3.

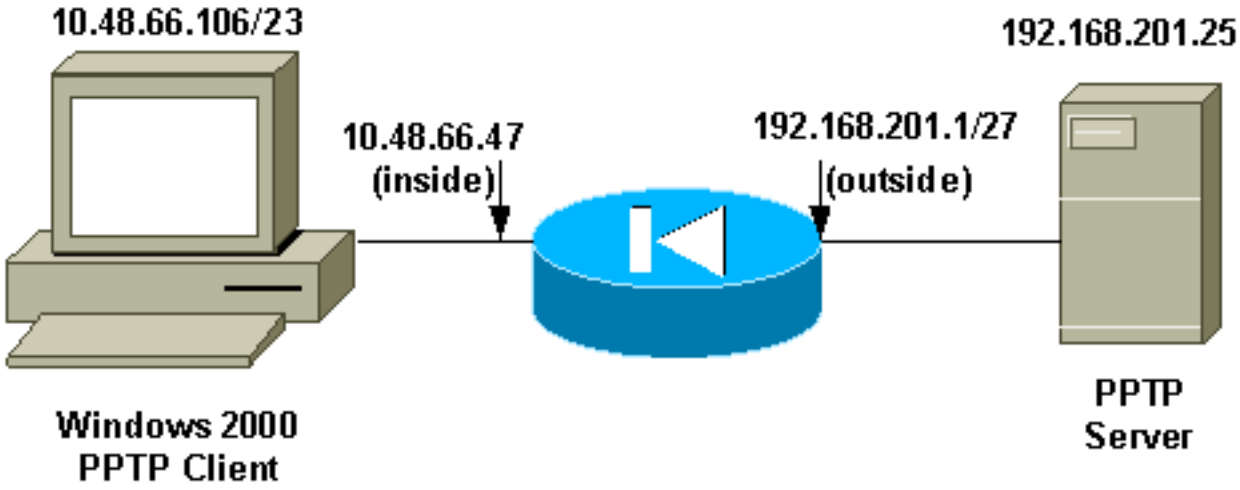
Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

PPTP с внутренним клиентом и внешним сервером

Схема сети

В настоящем документе используется следующая схема сети:



Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

Команды, добавляемые к версии 6.2 и более ранним

Выполните эти шаги, чтобы добавить команды для версии 6.2:

1. Определите статическое сопоставление для внутреннего ПК. Адрес, замеченный на внешней стороне, 192.168.201.5.`pixfirewall(config)#`**`static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0`**
2. Настройте и примените ACL для разрешения обратного трафика GRE из сервера PPTP к клиенту PPTP.`pixfirewall(config)#`**`access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5`**
3. Применение ACL.`pixfirewall(config)#`**`access-group acl-out in interface outside`**

Команды, добавляемые к версии 6.3

Выполните эти шаги к командам add для версии 6.3:

1. Включите fixup protocol pptp 1723, используя данную команду.`pixfirewall(config)#`**`fixup protocol pptp 1723`**
2. Необходимости определять статическое сопоставление нет, поскольку протокол привязки PPTP включен. Можно использовать PAT.`pixfirewall(config)#`**`nat (inside) 1 0.0.0.0 0.0.0.0 0 0`** `pixfirewall(config)#`**`global (outside) 1 interface`**

Команды для Добавления для Версий 7.x и 8.0 с помощью контроля

Выполните эти шаги к командам add для версий 7.x и 8.0 с помощью **команды inspect**:

1. Добавьте проверку PPTP в схему политик по умолчанию, используя карту классов по умолчанию.`pixfirewall(config)#`**`policy-map global_policy`** `pixfirewall(config-pmap)#`**`class inspection_default`** `pixfirewall(config-pmap-c)#`**`inspect pptp`**
2. Необходимости определять статическое сопоставление нет, поскольку PIX теперь проверяет трафик PPTP. Можно использовать PAT.`pixfirewall(config)#`**`nat (inside) 1 0.0.0.0 0.0.0.0 0 0`** `pixfirewall(config)#`**`global (outside) 1 interface`** **Или**

Команды для Добавления для Версий 7.x и 8.0 с помощью ACL

Выполните эти шаги к командам add для версий 7.x и 8.0 с помощью ACL.

1. Определите статическое сопоставление для внутреннего ПК. Адрес, замеченный на внешней стороне, 192.168.201.5.`pixfirewall(config)#`**`static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0`**
2. Настройте и примените ACL для разрешения обратного трафика GRE из сервера PPTP к клиенту PPTP.`pixfirewall(config)#`**`access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5`** `pixfirewall(config)#`**`access-list acl-out permit tcp host 192.168.201.25 host 192.168.201.5 eq 1723`**
3. Применение ACL.`pixfirewall(config)#`**`access-group acl-out in interface outside`**

Конфигурация для версии 6.2 и более ранних версий

Конфигурация PIX - клиент внутри, сервер снаружи
`pixfirewall(config)#`**`write terminal`** `Building configuration... : Saved : PIX Version 6.2(1) nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 intf2 security10 enable password Ujkil6aDv2yp6suI encrypted passwd OnTrBUG1Tp0edmkr encrypted hostname pixfirewall domain-`

```
name cisco.com fixup protocol ftp 21 fixup protocol http
80 fixup protocol h323 h225 1720 fixup protocol h323 ras
1718-1719 fixup protocol ils 389 fixup protocol rsh 514
fixup protocol rtsp 554 fixup protocol smtp 25 fixup
protocol sqlnet 1521 fixup protocol sip 5060 fixup
protocol skinny 2000 no names !--- This line allows GRE
traffic from the !--- PPTP server to the client. access-
list acl-out permit gre host 192.168.201.25 host
192.168.201.5 pager lines 24 logging on logging console
debugging logging trap debugging interface ethernet0
auto interface ethernet1 auto interface ethernet2 auto
shutdown mtu outside 1500 mtu inside 1500 mtu intf2 1500
ip address outside 209.165.201.1 255.255.255.224 ip
address inside 10.48.66.47 255.255.254.0 ip address
intf2 127.0.0.1 255.255.255.255 ip audit info action
alarm ip audit attack action alarm no failover failover
timeout 0:00:00 failover poll 15 failover ip address
outside 0.0.0.0 failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0 pdm history enable arp
timeout 14400 !--- This allows traffic from a low
security interface to !--- a high security interface.
static (inside,outside) 192.168.201.5 10.48.66.106
netmask 255.255.255.255 0 0 !--- This applies the ACL to
the outside interface. access-group acl-out in interface
outside timeout xlate 3:00:00 timeout conn 1:00:00 half-
closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
uauth 0:04:00 inactivity aaa-server TACACS+ protocol
tacacs+ aaa-server RADIUS protocol radius aaa-server
LOCAL protocol local no snmp-server location no snmp-
server contact snmp-server community public snmp-server
enable traps no floodguard enable no sysopt route dnat
telnet timeout 5 ssh timeout 5 terminal width 80
Cryptochecksum:18bdf8e21bd72ec0533795549165ecf5 : end
[OK]
```

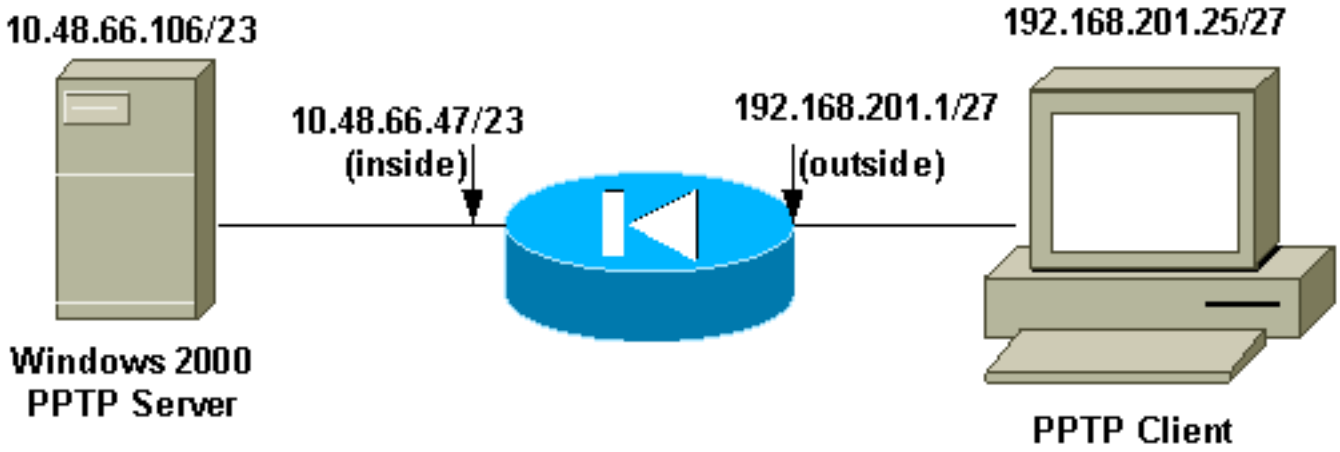
L2TP с клиентом внутри и сервер снаружи

Выполните эти шаги чтобы к командам add для версий 7.x и 8.x тот ACL использования. (Эта конфигурация принимает клиента PPTP, и IP-адреса сервера совпадают с для клиента и сервера L2TP.)

1. Определите статическое сопоставление для внутреннего ПК. Адрес, замеченный на внешней стороне, 192.168.201.5.`pixfirewall(config)#`**`static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0`**
2. Настройте и примените ACL для разрешения ответного трафика L2TP от сервера L2TP до клиента L2TP.`pixfirewall(config)#`
   `pixfirewall(config)#`**`access-list acl-out permit udp host 192.168.201.25 host 192.168.201.5 eq 1701`**
3. Применение ACL.`pixfirewall(config)#`**`access-group acl-out in interface outside`**

PPTP с внешним клиентом и внутренним сервером

Схема сети



Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

Приказывает добавить ко всем версиям

В этом примере конфигурации сервер PPTP 192.168.201.5 (статичен к 10.48.66.106 внутренней части), и клиент PPTP в 192.168.201.25.

```
access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5 access-list acl-out permit
tcp host 192.168.201.25 host 192.168.201.5 eq 1723 static (inside,outside) 192.168.201.5
10.48.66.106 netmask 255.255.255.255 0 0 access-group acl-out in interface outside
```

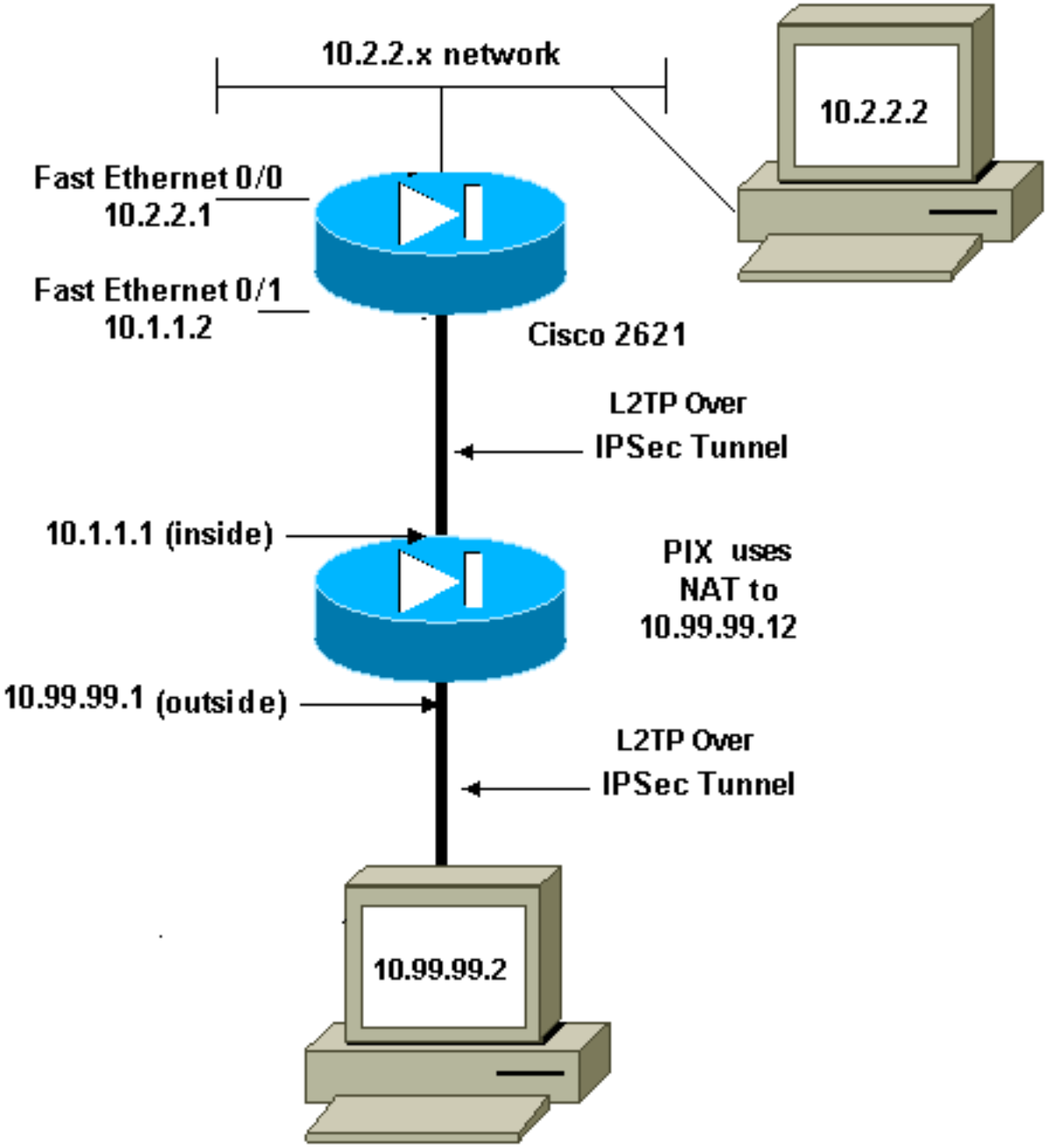
L2TP с клиентом снаружи и сервер внутри

В этом примере конфигурации сервер L2TP 192.168.201.5 (статичен к 10.48.66.106 внутренней части), и клиент L2TP в 192.168.201.25. (Эта конфигурация принимает клиента PPTP, и IP-адреса сервера совпадают с для клиента и сервера L2TP.)

```
access-list acl-out permit udp host 192.168.201.25 host 192.168.201.5 eq 1701 static
(inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0 access-group acl-out in
interface outside
```

Позвольте L2TP По IPsec Через PIX/ASA 7.x и Выше

Внешний клиент L2TP пытается установить L2TP по соединению IPSec VPN с внутренним сервером L2TP. Для разрешения L2TP по Пакетам ipsec через средний PIX/ASA необходимо позволить ESP, ISAKMP (500), NAT-T и порт 1701 L2TP устанавливать туннель. Пакеты L2TP преобразованы в PIX и переданы через VPN-туннель.




```
global (outside) 1 interface
nat (inside) 0 0.0.0.0 0.0.0.0
static (inside,outside) 10.99.99.12 10.1.1.2 netmask 255.255.255.255
access-group outside_access_in in interface outside

access-list outside_access_in remark Access Rule to Allow ESP traffic
access-list outside_access_in extended permit esp host 10.99.99.2
            host 10.99.99.12

access-list outside_access_in remark Access Rule to allow ISAKMP to
            host 10.99.99.12
access-list outside_access_in extended permit udp host 10.99.99.2 eq isakmp
            host 10.99.99.12

access-list outside_access_in remark Access Rule to allow port 4500 (NAT-T) to
            host 10.99.99.12
access-list outside_access_in extended permit udp host 10.99.99.2 eq 4500
            host 10.99.99.12

access-list outside_access_in remark Access Rule to allow port 1701 (L2TP) to
            host 10.99.99.12
```

```
access-list outside_access_in extended permit udp host 10.99.99.2 eq 1701
            host 10.99.99.12
```

Проверка

Для этой конфигурации отсутствует процедура проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Множественный Сбой Соединений PPTP/L2TP при использовании PAT

У вас может только быть одно соединение PPTP/L2TP через Устройство безопасности PIX при использовании PAT. Так происходит, потому что необходимое соединение GRE устанавливается через порт 0, а устройство безопасности PIX сопоставляет порт 0 только одному хосту. Обходной путь должен включить проверку PPTP на устройстве безопасности.

Ошибка 800 при попытке соединиться с входящей VPN PPTP

Когда вы пытаетесь соединиться с входящей VPN PPTP, это сообщение об ошибках появляется:

```
Error 800: The remote connection was not made because the attempted VPN tunnels failed. The VPN
server might be unreachable. If this connection is attempting to use an L2TP/IPsec tunnel, the
security parameters required for IPsec negotiation might not be configured properly.
```

Когда passthrough PPTP или L2TP не включен на промежуточном ASA между клиентом и устройством головной станции, эта проблема обычно происходит. Включите PPTP или passthrough L2TP и проверьте конфигурацию для решения вопроса.

Команды "debug"

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

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

В данном примере показан клиент PPTP внутри PIX, инициирующий соединение с сервером PPTP снаружи PIX, притом что не существует ACL, настроенного на разрешение трафика GRE. При записи отладочных сообщений на PIX можно видеть инициацию трафика из клиента портом 1723 TCP и отклонение обратного трафика протокола 47 GRE.

```
pixfirewall(config)#loggin on pixfirewall(config)#loggin console 7 pixfirewall(config)#302013:
Built outbound TCP connection 4 for outside: 192.168.201.25 /1723 (192.168.201.25 /1723) to
inside:10.48.66.106/4644 (192.168.201.5 /4644) 106010: Deny inbound protocol 47 src
outside:192.168.201.25 dst inside:192.168.201.5 106010: Deny inbound protocol 47 src
outside:192.168.201.25 dst inside:192.168.201.5
```

Информация, обязательная для сбора в случае обращения в центр технической поддержки

Если после выполнения описанных выше действий по устранению неполадок вам по-прежнему нужна помощь и вы планируете обращение в Центр технической поддержки Cisco, убедитесь в том, что в запрос включена следующая информация.
• Описание проблемы и соответствующие сведения о топологии • Действия по устранению проблем, выполненные перед подачей запроса на обслуживание • **Выходные данные команды show tech-support** • **Выходные данные команды show log после выполнения команды logging buffered debugging или снимки консоли, демонстрирующие проблему (при их наличии)** Приложите собранные данные к запросу на обслуживание в простом текстовом формате (.txt), не архивируя вложенный файл. Чтобы приложить информацию к запросу, можно загрузить ее Service Request Query Tool (только для зарегистрированных пользователей). При отсутствии доступа к средству Service Request Query Tool можно отправить данные электронной почтой по адресу attach@cisco.com с номером сервисного запроса в строке "Тема" отправляемого сообщения.

Дополнительные сведения

- Страница поддержки PPTP
- Пример конфигурации PIX/ASA 7.x и последующих версий, с проходом туннеля IPsec проходит через устройство защиты посредством использования списка доступа и MPF с NAT
- Настройка туннеля IPSec через межсетевой экран с NAT
- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация