PIX 6.x: Пример конфигурации PPTP с проверкой подлинности RADIUS

Содержание

Введение

Point-to-Point Tunneling Protocol (PPTP) - это протокол туннелирования уровня 2, который разрешает удаленному клиенту использовать публичную IP-сеть для безопасной связи с серверами в частной корпоративной сети. PPTP является туннелем для IP. PPTP описывается в RFC 2637 . Поддержка PPTP в брандмауэре PIX была добавлена в программном обеспечении PIX, релизе 5.1. В документации PIX дается больше сведений о PPTP и его использовании с PIX. Этот документ описывает настройку PIX для

использования PPTP с локальной аутентификацией, TACACS+ и RADIUS. В документе также даны приемы и примеры, которые могут помочь при разрешении часто возникающих проблем.

Этот документ также показывает, как настраивать соединения PPTP к PIX. Для настройки PIX или ASA для разрешения PPTP *через* устройство безопасности, обратитесь к Разрешению Соединений PPTP/L2TP Через PIX.

Чтобы настроить брандмауэр PIX и клиент VPN для использования с сервером IAS RADIUS для Windows 2000 и 2003, обратитесь к "Cisco Secure PIX Firewall 6.x и Cisco VPN Client 3.5 for Windows с сервером аутентификации Microsoft Windows 2000 и 2003 IAS RADIUS".

См. Настройку VPN 3000 Concentrator и PPTP с Cisco Secure ACS для Аутентификации Windows RADIUS для настройки PPTP на VPN 3000 Concentrator с Cisco Secure ACS для Windows для Проверки подлинности RADIUS.

См. Cisco Secure ACS Настройки для Аутентификации PPTP маршрутизатора Windows для устанавливания Подключения ПК к маршрутизатору, который тогда предоставляет проверку подлинности пользователя системе управления доступом Cisco Secure Access Control System (ACS) 3.2 для Windows Server, прежде чем вы позволите пользователю в сеть.

Примечание: В сроках PPTP, на RFC, PPTP Network Server (PNS) является сервером (в этом случае, PIX или вызываемый), и Концентратор доступа PPTP (PAC) является клиентом (ПК или абонент).

Примечание: Раздельное туннелирование не поддерживается на PIX для клиентов PPTP.

Примечание: PIX 6.x нужен v1.0 MS-CHAP для PPTP для работы. Windows Vista не поддерживает v1.0 MS-CHAP. Таким образом, PPTP на PIX 6.x не будет работать для Windows Vista. PPTP не поддерживается в Версии PIX 7.x и позже.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Выпуске ПО межсетевого экрана Cisco Secure PIX 6.3 (3).

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.

Условные обозначения

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

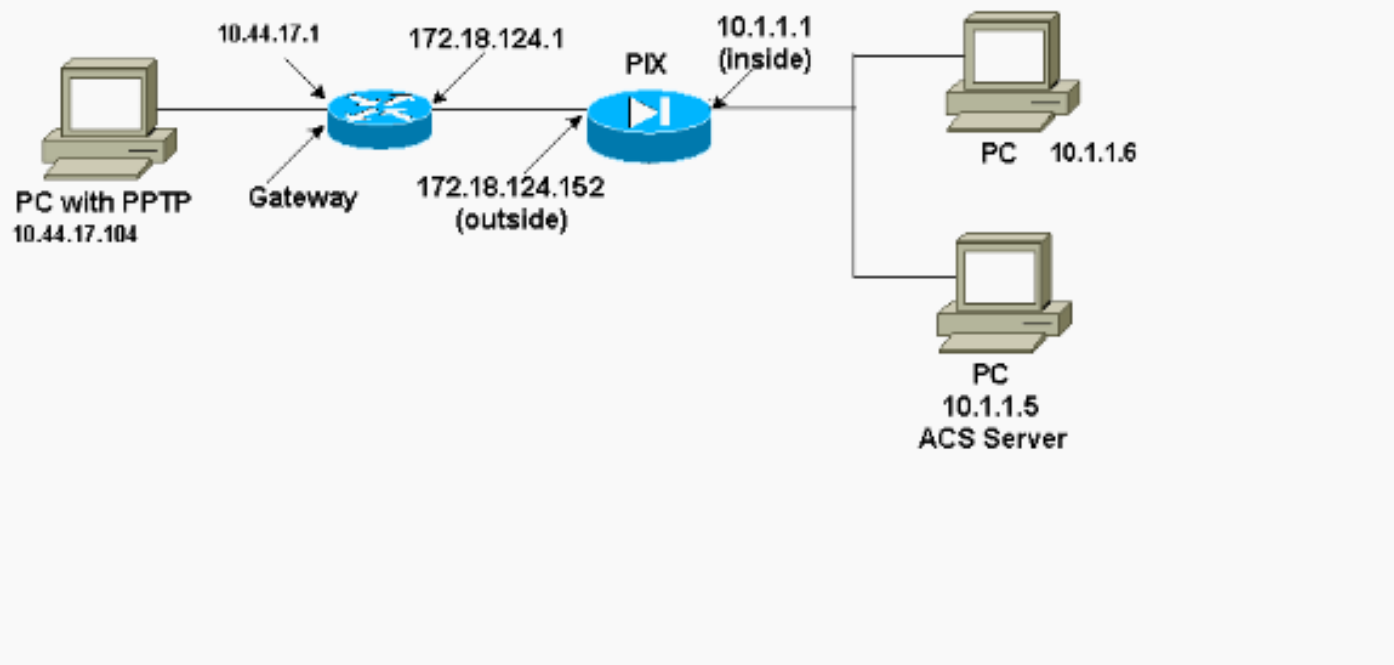
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети.



Советы конфигурации для межсетевого экрана PIX

Тип аутентификации - CHAP, PAP, MS-CHAP

PIX, настроенный одновременно для всех трех методов аутентификации (CHAP, PAP, MS-CHAP), дает наибольшие шансы для установления соединения, вне зависимости от того, как настроен ПК. Это хорошая идея для устранения неисправностей.

```
vpdn group 1 ppp authentication chap vpdn group 1 ppp authentication mschap vpdn group 1 ppp authentication pap
```

Средства шифрования Microsoft точка-точка (MPPE)

Используйте этот синтаксис команды для настройки шифрования MPPE на Межсетевом экране PIX.

```
vpdn group 1 ppp encryption mppe 40|128|auto [required]
```

В этой команде required является опциональным ключевым словом. Должен быть настроен MS-CHAP.

Настройка функции PPTP на клиентских ПК

Примечание: Доступная информация здесь на связанном с конфигурацией программного обеспечения компании Microsoft не идет ни с какой гарантией или поддержкой программного обеспечения компании Microsoft. Поддержка программного обеспечения Microsoft предоставляется Microsoft на веб-сайте поддержки Microsoft .

Windows 98

Выполните эти действия для установки функции PPTP на Windows 98.

1. **Выберите "Пуск > Параметры > Панель управления > Установить новое оборудование". Нажмите кнопку Next.**
2. **Щелкните "Select from List" и выберите "Network Adapter". Нажмите кнопку Next.**
3. **В панели слева выберите Microsoft, а справа - Microsoft VPN Adapter.**

Чтобы настроить функцию PPTP, выполните следующие шаги.

1. **Выберите "Пуск > Программы > Стандартные > Связь > Удаленный доступ к сети".**
2. **Нажмите на Make new connection. В пункте Select a device выберите Microsoft VPN Adapter.** IP-адрес VPN-сервера является конечной точкой туннеля с межсетевым экраном PIX.
3. Аутентификация по умолчанию Windows 98 использует шифрование пароля (CHAP или MS-CHAP). Для изменения ПК, чтобы также позволить PAP, выберите **Properties> Server Type**. **Снимите флажок Require encrypted password (Требовать зашифрованный пароль).** В этой области можно настроить шифрование данных (с использованием MPPE или без MPPE).

Windows 2000

Выполните эти действия для настройки функции PPTP на Windows 2000.

1. Выберите **Start> Programs> Accessories> Communications> Network и Подключения удаленного доступа**.
2. **Нажмите кнопку Make new connection, затем нажмите кнопку Next.**
3. **Выберите параметры Connect to a private network through the Internet и Dial a connection prior (не нужно для LAN). Нажмите кнопку Next.**
4. Введите имя узла или IP-адрес конечной точки туннеля (PIX/маршрутизатор).
5. **Если требуется изменить тип пароля, выберите Properties > Security for the connection > Advanced.** По умолчанию используется MS-CHAP и MS-CHAP v2 (а не CHAP или PAP). В этой области можно настроить шифрование данных (с использованием MPPE или без MPPE).

Windows NT

См. Установку, Настройку и Использование PPTP с клиентами Microsoft и Серверами для устанавливания клиентов NT для PPTP.

Настройка PIX

Конфигурация PIX – локальная аутентификация, без шифрования

```
PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list 101 permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0 pager lines 24 logging on no
logging timestamp no logging standby no logging console
no logging monitor logging trap debugging no logging
history logging facility 20 logging queue 512 interface
ethernet0 10baset interface ethernet1 10baset interface
ethernet2 10baset mtu outside 1500 mtu inside 1500 mtu
pix/intf2 1500 ip address outside 172.18.124.152
255.255.255.0 ip address inside 10.1.1.1 255.255.255.0
ip address pix/intf2 127.0.0.1 255.255.255.255 ip local
pool pptp-pool 192.168.1.1-192.168.1.50 no failover
failover timeout 0:00:00 failover ip address outside
0.0.0.0 failover ip address inside 0.0.0.0 failover ip
address pix/intf2 0.0.0.0 arp timeout 14400 global
(outside) 1 172.18.124.201-172.18.124.202 nat (inside) 0
access-list 101 nat (inside) 1 10.1.1.0 255.255.255.0 0
0 conduit permit icmp any any route outside 0.0.0.0
0.0.0.0 172.18.124.1 1 timeout xlate 3:00:00 conn
1:00:00 half-closed 0:10:00 udp 0:02:00 timeout rpc
0:10:00 h323 0:05:00 timeout uauth 0:05:00 absolute aaa-
server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps floodguard enable sysopt connection permit-
pptp isakmp identity hostname telnet timeout 5 vpdn
group 1 accept dialin pptp vpdn group 1 ppp
authentication pap vpdn group 1 ppp authentication chap
vpdn group 1 ppp authentication mschap vpdn group 1
client configuration address local pptp-pool vpdn group
1 client authentication local vpdn username cisco
password cisco vpdn enable outside terminal width 80
Cryptochecksum:a72d9f71d1a31332307fcd348e02410d : end
```

Конфигурация PIX – Локальная проверка с шифрованием

Если вы добавляете эту команду к Конфигурации PIX - Локальная проверка подлинности, Никакая Настройка шифрования, ПК и автосогласование PIX 40-разрядное шифрование или ни один (на основе Настроек ПК).

```
vpdn group 1 ppp encryption mppe auto
```

Если у PIX включена функция 3DES, команда show version выводит следующее сообщение.

- Версия 6.3 и более поздние:`VPN-3DES-AES: Enabled`
- Версия 6.2 и более ранние:`VPN-3DES: Enabled`

Можно также использовать 128-битное шифрование. Однако если отображается одно из следующих сообщений, 128-битное шифрование в PIX невозможно.

- Версия 6.3 и более поздние:`Warning: VPN-3DES-AES license is required for 128 bits MPPE encryption`
- Версия 6.2 и более ранние:`Warning: VPN-3DES license is required for 128 bits MPPE encryption`

Далее приводится синтаксис для команды MPPE.

`vpdn group ppp encryption mppe 40|128|auto [required]`

ПК и PIX должны быть настроены на выполнение проверки подлинности MS-CHAP совместно с MPPE.

Конфигурация PIX - TACACS+/RADIUS аутентификация без шифрования

```
PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname PIX
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
access-list 101 permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0 pager lines 24 logging on
logging timestamp no logging standby logging console
debugging no logging monitor logging buffered debugging
logging trap debugging no logging history logging
facility 20 logging queue 512 interface ethernet0
10baset interface ethernet1 10baset interface ethernet2
10baset mtu outside 1500 mtu inside 1500 mtu pix/intf2
1500 ip address outside 172.18.124.152 255.255.255.0 ip
address inside 10.1.1.1 255.255.255.0 ip address
pix/intf2 127.0.0.1 255.255.255.255 ip local pool pptp-
pool 192.168.1.1-192.168.1.50 no failover failover
timeout 0:00:00 failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0 failover ip address
pix/intf2 0.0.0.0 arp timeout 14400 global (outside) 1
172.18.124.201-172.18.124.202 nat (inside) 0 access-list
101 nat (inside) 1 10.1.1.0 255.255.255.0 0 0 conduit
permit icmp any any route outside 0.0.0.0 0.0.0.0
172.18.124.1 1 timeout xlate 3:00:00 conn 1:00:00 half-
closed 0:10:00 udp 0:02:00 timeout rpc 0:10:00 h323
0:05:00 timeout uauth 0:05:00 absolute aaa-server
TACACS+ protocol tacacs+ aaa-server RADIUS protocol
radius !--- Use either RADIUS or TACACS+ in this
statement. aaa-server AuthInbound protocol radius |
tacacs+ aaa-server AuthInbound (outside) host
```

```
172.18.124.99 cisco timeout 5 no snmp-server location no
snmp-server contact snmp-server community public no
snmp-server enable traps floodguard enable sysopt
connection permit-pptp isakmp identity address telnet
10.1.1.5 255.255.255.255 inside telnet 10.1.1.5
255.255.255.255 pix/intf2 telnet timeout 5 vpdn group 1
accept dialin pptp vpdn group 1 ppp authentication pap
vpdn group 1 ppp authentication chap vpdn group 1 ppp
authentication mschap vpdn group 1 client configuration
address local pptp-pool vpdn group 1 client
authentication aaa AuthInbound vpdn enable outside
terminal width 80
Cryptochecksum:96e9c93cb0a6ad6f53581dd7b61ac763 : end
[OK]
```

Конфигурация PIX - аутентификация RADIUS с шифрованием

Если сервер RADIUS (определяемые производителем характеристика 26, Microsoft как поставщик) кодирование MPPE поддержек, шифрование MPPE может быть добавлено, если RADIUS используется, и. Аутентификация TACACS+ не поддерживает шифрование, потому что серверы TACACS+ не способны возвращать специальные ключи MPPE. Cisco Secure ACS для Windows 2.5 и более поздние RADIUS не поддерживают MPPE (все серверы RADIUS не поддерживают MPPE).

С допущением, что аутентификация RADIUS работает без шифрования, добавьте шифрование, включив следующую команду в предыдущую конфигурацию:

vpdn group 1 ppp encryption mppe auto

ПК и PIX производят автосогласование шифрования (40-битное или нет) на основании настроек ПК.

Если у PIX включена функция 3DES, команда show version выводит следующее сообщение.

```
VPN-3DES: Enabled
```

Можно также использовать 128-битное шифрование. Однако если отображается следующее сообщение, 128-битное шифрование в PIX невозможно.

```
Warning: VPN-3DES license is required
for 128 bits MPPE encryption
```

Далее приводится синтаксис для команды MPPE.

vpdn group ppp encryption mppe 40|128|auto [required]

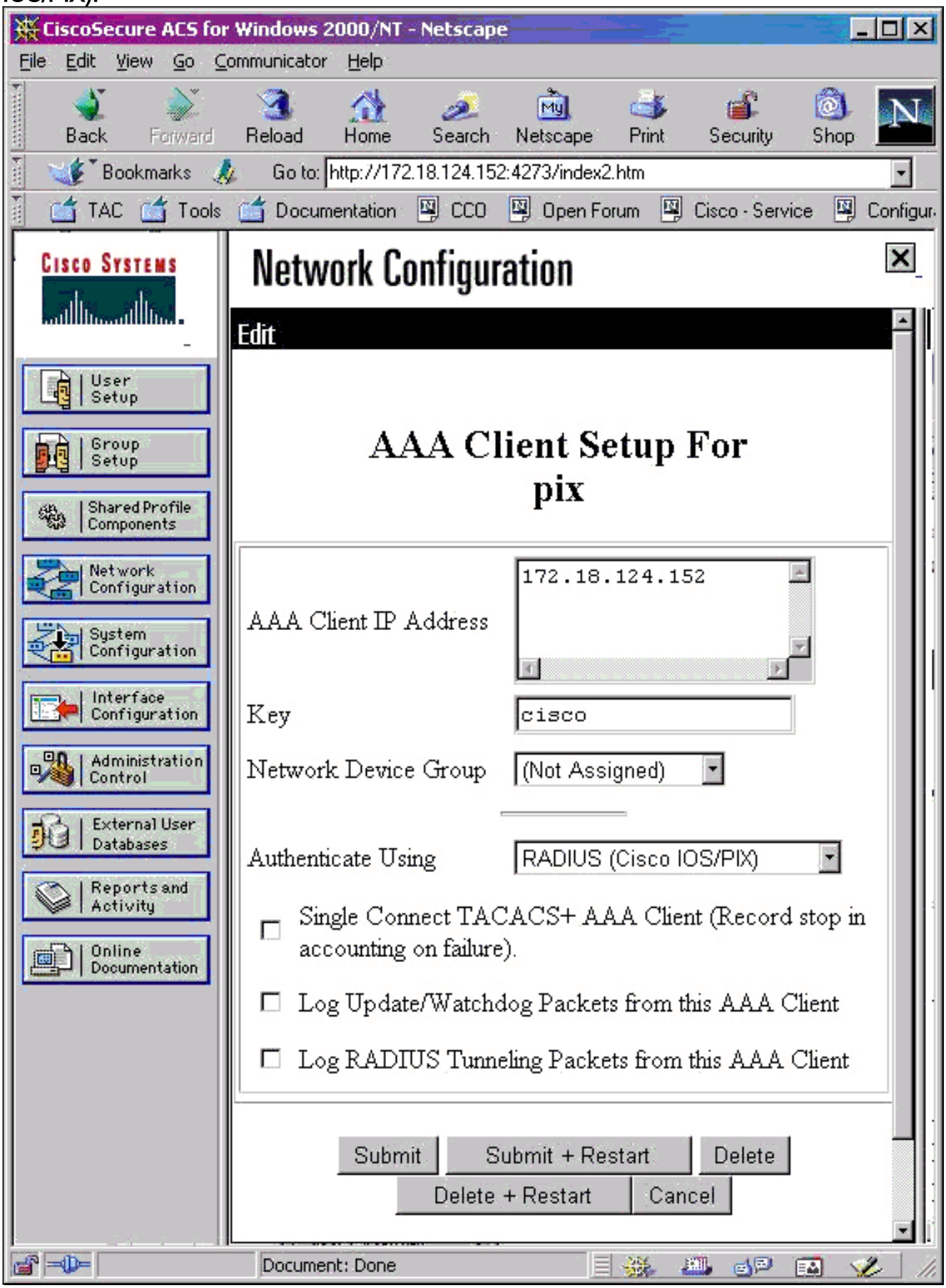
ПК и PIX должны быть настроены на выполнение проверки подлинности MS-CHAP совместно с MPPE.

Настройте Cisco Secure ACS для Windows 3.0

Аутентификация RADIUS с шифрованием

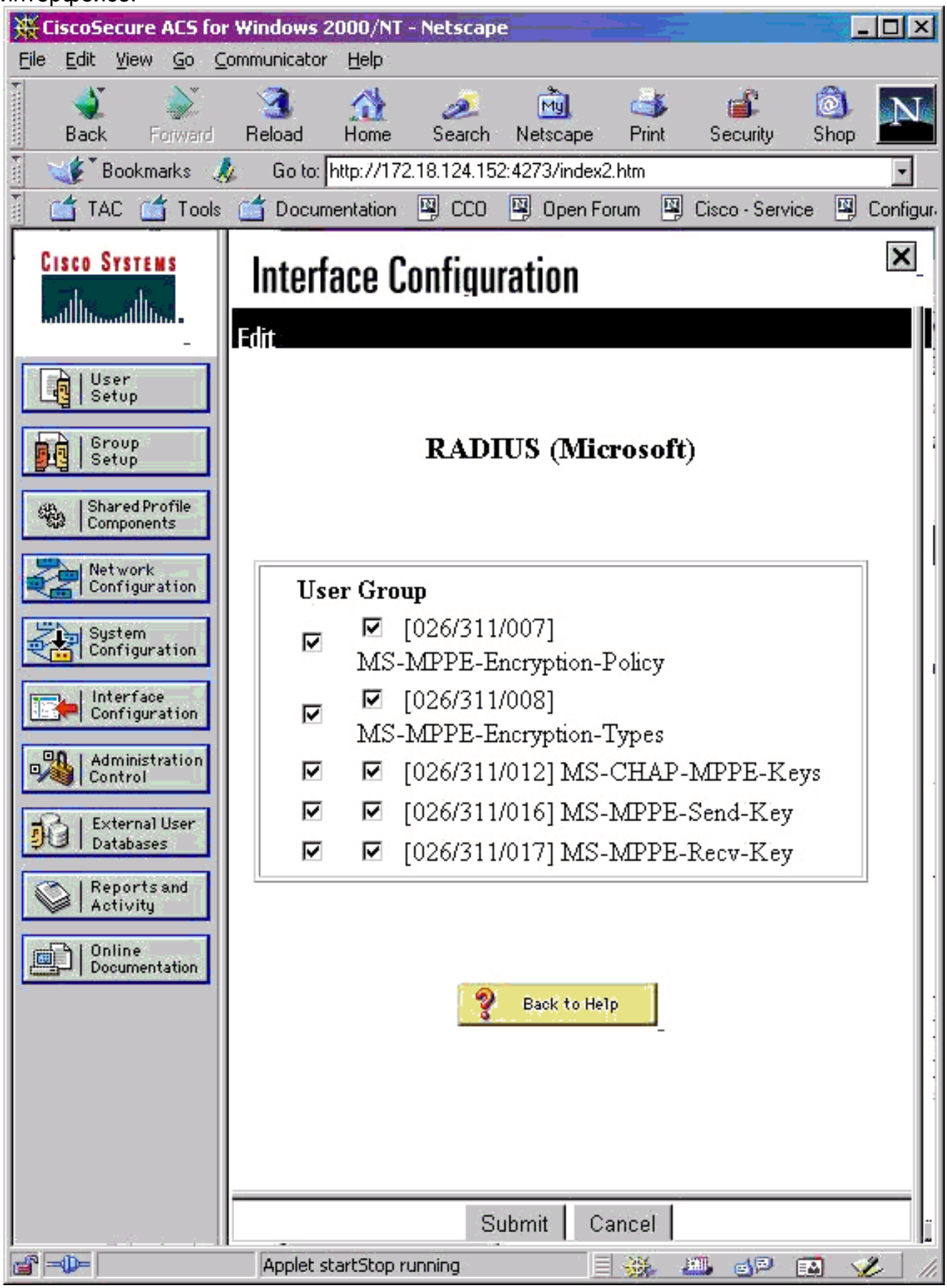
Следуйте этим шагам для настройки Cisco Secure ACS для Windows версии 3,0. Те же самые этапы настройки применимы для ACS версий 3.1 и 3.2.

1. **Добавьте PIX к Cisco Secure ACS для сетевой конфигурации сервера Windows и укажите тип словаря RADIUS (Cisco IOS/PIX).**

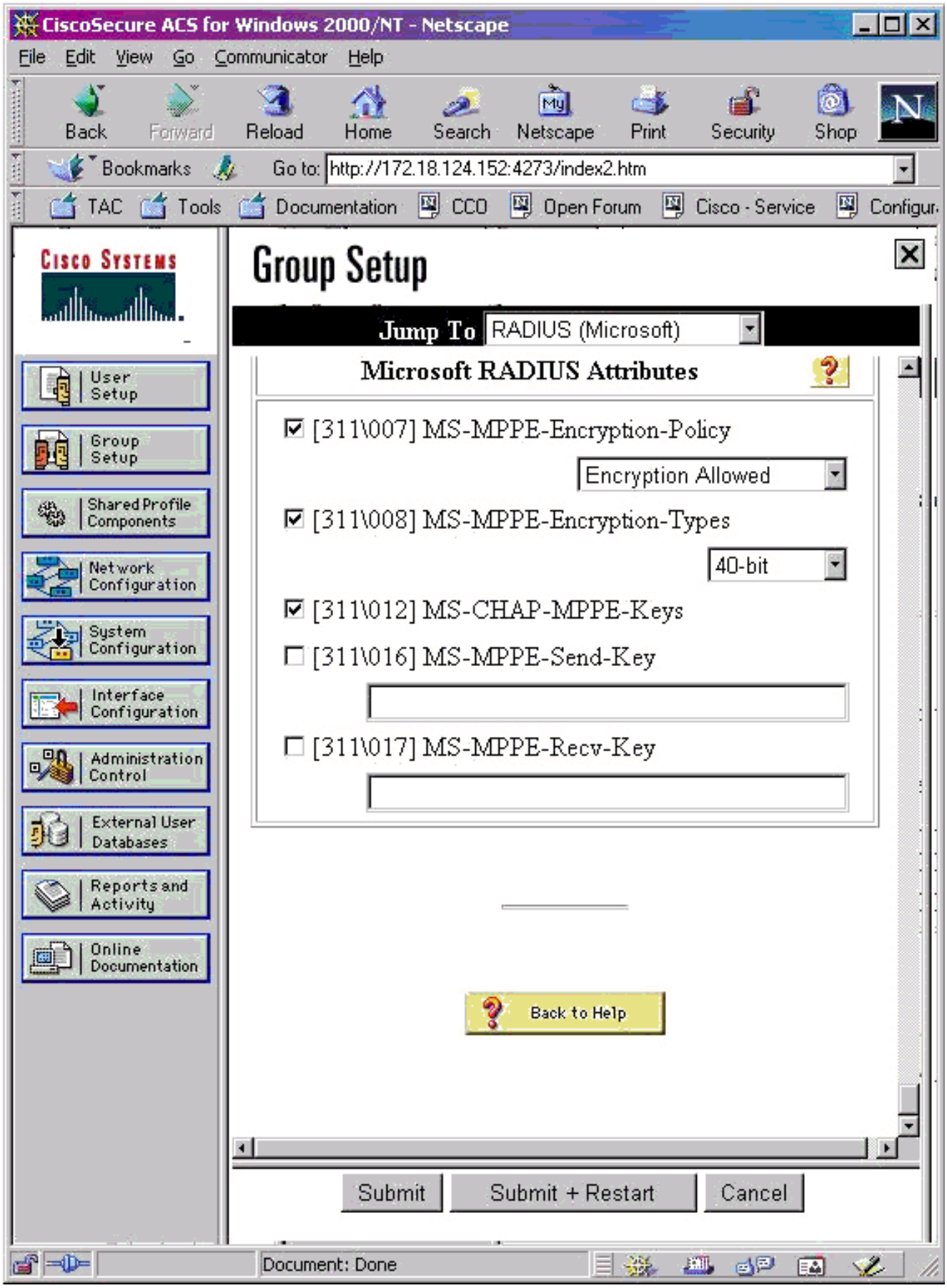


2. **Конфигурация Открытого интерфейса> RADIUS (Microsoft)** и проверка Атрибуты MPPE, чтобы заставить их появиться в групповом

интерфейсе.



3. Добавьте пользователя. В группе пользователя добавьте атрибуты MPPE [RADIUS (Microsoft)]. Для шифрования следует включить эти атрибуты, но они являются необязательными, когда PIX не настроен для шифрования.



Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Команды show в PIX (после аутентификации)

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

Команда show vpdn выводит информацию о туннелях и сеансах.

```
PIX#show vpdn PPTP Tunnel and Session Information (Total tunnels=1 sessions=1) Tunnel id 13,
remote id is 13, 1 active sessions Tunnel state is estabd, time since event change 24 secs
remote Internet Address 10.44.17.104, port 1723 Local Internet Address 172.18.124.152, port 1723
12 packets sent, 35 received, 394 bytes sent, 3469 received Call id 13 is up on tunnel id 13
Remote Internet Address is 10.44.17.104 Session username is cisco, state is estabd Time since
event change 24 secs, interface outside Remote call id is 32768 PPP interface id is 1 12 packets
sent, 35 received, 394 bytes sent, 3469 received Seq 13, Ack 34, Ack_Rcvd 12, peer RWS 64 0 out
of order packets
```

Проверка компьютера пользователя

В окне MS-DOS, или из окна Run, **ipconfig** типа **/ все**. Эти данные выводит часть адаптера PPP.

```
PPP adapter pptp:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : WAN (PPP/SLIP) Interface
        Physical Address. . . . . . . . . : 00-53-45-00-00-00
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . :
```

Можно также нажать Details для просмотра сведений в соединении PPTP.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

- Для общей инкапсуляции маршрутов (GRE) и TCP 1723 должно существовать соединение из ПК в конечную точку туннеля PIX. Есть если вероятность, что оно заблокировано брандмауэром или списком доступа, передвиньте ПК ближе к PIX.
- Наиболее легко установить PPTP в Windows 98 и Windows 2000. При возникновении сомнений попытайтесь повторить операцию на разных компьютерах и операционных системах. **После установления соединения нажмите на Details на ПК для отображения информации о соединении.** Например, данных о том, используете ли вы PAP, CHAP, IP, шифрование и т.д.
- Если вы намерены использовать RADIUS и/или TACACS+, сначала попытайтесь настроить локальную аутентификацию (имя пользователя и пароль на PIX). Если она не работает, не будет работать и аутентификация сервером RADIUS или TACACS+.
- **Сначала убедитесь, что настройки Security на ПК разрешают максимально возможное число типов аутентификации (PAP, CHAP, MS-CHAP) и снимите флажок Require data encryption (сделайте этот параметр опциональным как для PIX, так и для ПК).**
- Поскольку тип проверки подлинности согласован, настройте PIX с максимальным

числом возможностей. Например, если ПК настроен только для MS-CHAP, а маршрутизатор только для PAP, они никогда не будут работать вместе.
- Если PIX действует как сервер PPTP для двух разных расположений, и каждое расположение имеет собственный сервер RADIUS, использование единого PIX для обоих расположений, обслуживаемых их собственными серверами RADIUS, не поддерживается.
- Некоторые серверы RADIUS не поддерживают MPPE. Если сервер RADIUS не поддерживает манипуляции MPPE, аутентификация RADIUS будет работать, а шифрование MPPE - нет.
- В операционной системе Windows 98 или более поздней версии при использовании аутентификации PAP или CHAP имя пользователя, отправляемое на PIX, совпадает с тем, которое было введено в настройках модемного подключения. Однако при использовании MS-CHAP имя домена может быть добавлено к имени пользователя, в его начало, например:Имя пользователя, введенное в DUN, — "cisco"Домен, установленный на коробке Windows 98 - "DOMAIN"Имя пользователя MS-CHAP, передаваемое PIX - "DOMAIN\cisco"Имя пользователя на PIX - "Cisco"Результат - недопустимое имя пользователя / парольЭто - раздел журнала PPP от ПК Windows 98, который показывает поведение.
```
02-01-2001 08:32:06.78 - Data 0038: 49 53 4c 41 42 5c 63 69
| DOMAIN\ci
02-01-2001 08:32:06.78 - Data 0040: 73 63 6f 00 00 00 00 00 | sco.....
|
|
02-01-2001 08:32:06.80 - Data 0000: c2 23 04 01 00 1a 41 75 | .#...^ZAu
02-01-2001 08:32:06.80 - Data 0008: 74 68 65 6e 74 69 63 61 | thentica
02-01-2001 08:32:06.80 - Data 0010: 74 69 6f 6e 20 66 61 69 | tion fai
02-01-2001 08:32:06.80 - Data 0018: 6c 65 64 2e 00 00 00 00 | led.....
02-01-2001 08:32:06.80 - CHAP : Login failed: username, password,
   or domain was incorrect
```
При использовании Windows 98 и MS-CHAP к PIX кроме имени пользователя без домена вы можете добавить PIX "DOMAIN\username":
```
vpdn username cisco password cisco vpdn username DOMAIN\cisco password cisco
```
Примечание: При выполнении удаленной аутентификации на AAA-сервере то же применяется.

Команды для устранения неполадок

Сведения об ожидаемой последовательности событий PPTP даны в RFC 2637 для PPTP . В PIX важные события в хорошей последовательности PPTP показывают:

```
SCCRQ (Start-Control-Connection-Request)
SCCRP (Start-Control-Connection-Reply)
OCRQ (Outgoing-Call-Request)
OCRP (Outgoing-Call-Reply)
```
Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Команды отладки PIX

- **debug ppp io - вывод сведений о пакетах для виртуального интерфейса PPTP PPP.**
- **debug ppp error – отображает ошибки протокола и статистику ошибок, связанных с согласованием и функционированием PPP-соединения.**
- **debug vpdn error– показывает ошибки, не позволяющие установить туннель или**

вызывающие закрытие установленного туннеля.
- debug vpdn packet – отображает ошибки и события L2TP, которые сопровождают нормальную установку туннеля или завершение VPDN.
- debug vpdn events– выводит сообщения о событиях, свидетельствующих о нормальном ходе установления или закрытия туннеля PPP.
- debug ppp uauth - показывает сообщения отладки аутентификации пользователей AAA виртуального интерфейса PPTP PPP.

Команды clear PIX

Эта команда должна быть выполнена в режиме конфигурации.

- **clear vpdn tunnel [все |** *[идентификатор tunnel_id]***]** — Удаляет один или несколько туннелей PPTP из конфигурации.

Внимание. : *Не* выполняйте команду **clear vpdn**. *Удаляет все команды vpdn.*

Включение регистрации PPP на клиенте

Следуйте данным инструкциям для включения отладки PPP в различных операционных системах Windows и Microsoft.

Windows 95

Выполните эти действия для включения Регистрации PPP на машине Windows 95/98.

1. **В меню Network на панели управления нажмите два раза на Microsoft Dial-Up Adapter в списке установленных компонентов сети.**
2. **Щелкните вкладку Advanced ("Дополнительно"). В списке Property нажмите на параметр Record A Log File, а в списке Value - на Yes. Затем нажмите кнопку OK.**
3. Чтобы данный параметр вступил в силу, выключите и перезагрузите компьютер. Журнал сохранен в файл ppplog.txt.

Windows 98

Выполните эти действия для включения Регистрации PPP на машине Windows 98.

1. В **Удаленном доступе к сети**, одиночный щелчок значок подключения, и затем выбирают **File> Properties**.
2. Откройте вкладку Server Types.
3. **Выберите параметр "Record a log file" для этого соединения.** Файл журнала находится в C:\Windows\ppplog.txt

Windows 2000

Для включения Регистрации PPP на машине Windows 2000 перейдите к Microsoft Support Page, и поиск "Включают Регистрацию PPP в Windows".

Windows NT

Выполните эти действия для включения Регистрации PPP в системе NT.

1. **Найдите ключ SYSTEM\CurrentControlSet\Services\RasMan\PPP и измените Logging с 0 на 1.** Это создает файл, призвал PPP.LOG <root winnt> \SYSTEM32\RAS каталог.
2. Чтобы провести отладку сеанса PPP, сначала включите регистрацию и затем инициируйте соединение PPP. Если во время соединения произошла ошибка или оно прервалось, сведения об этом можно посмотреть в PPP.LOG.

Подробнее см. "Справка и поддержка Microsoft" , документ "Включение регистрации PPP в Windows NT" ("Enabling PPP Logging in Windows NT")."

Дополнительные ошибки Microsoft

Несколько Проблем с программным обеспечением от Microsoft для рассмотрения при устранении проблем PPTP перечислены здесь. Подробнее см. Базу знаний Майкрософт и приведенные ниже ссылки.

- Как поддержать RAS - подключения активными после того, чтобы выходить из системыСоединения службы удаленного доступа Windows (RAS) автоматически разрываются при отключении клиента RAS. Можно оставаться подключенным, включив в клиенте RAS ключ реестра KeepRasConnections.
- Пользователь не предупрежден при входе с кэшированными учетными даннымиЕсли вы входите в систему домена от Рабочей станции под управлением Windows или рядового сервера, и контроллер домена не может быть расположен, вы не получаете сообщение об ошибках, которое указывает на эту проблему. Вместо этого происходит регистрация на локальном компьютере с использованием кэшированных учетных данных.
- Как записать файл LMHOSTS для проверки данных домена и других проблем разрешения именПри испытании проблем разрешения имен в сети TCP/IP необходимо использовать файлы Lmhosts для решения Имен NETBIOS. Следуйте специальной процедуре для создания файла Lmhosts, который используется в разрешении имен и проверке данных домена.

Пример результата отладки

Отладка PIX - локальная проверка подлинности

Эти выходные данные отладки показывают важные события *курсивом*.

```
PPTP: new peer fd is 1

Tnl 42 PPTP: Tunnel created; peer initiated PPTP:
   created tunnel, id = 42

PPTP: cc rcvdata, socket fd=1, new_conn: 1
PPTP: cc rcv 156 bytes of data

SCCRQ = Start-Control-Connection-Request - message code bytes 9 & 10 = 0001 Tnl 42 PPTP: CC I
009c00011a2b3c4d0001000001000000000000010000... Tnl 42 PPTP: CC I SCCRQ Tnl 42 PPTP: protocol
version 0x100 Tnl 42 PPTP: framing caps 0x1 Tnl 42 PPTP: bearer caps 0x1 Tnl 42 PPTP: max
channels 0 Tnl 42 PPTP: firmware rev 0x0 Tnl 42 PPTP: hostname "local" Tnl 42 PPTP: vendor "9x"
Tnl 42 PPTP: SCCRQ-ok -> state change wt-sccrq to estabd SCCRP = Start-Control-Connection-Reply
- message code bytes 9 & 10 = 0002 Tnl 42 PPTP: CC O SCCRP PPTP: cc snddata, socket fd=1,
len=156, data: 009c00011a2b3c4d0002000001000100000000030000... PPTP: cc waiting for input, max
```

soc FD = 1 PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0 PPTP: cc rcv 168 bytes of data *OCRQ = Outgoing-Call-Request - message code bytes 9 & 10 = 0007* Tnl 42 PPTP: CC I 00a800011a2b3c4d000700000000000000000dac00000... Tnl 42 PPTP: CC I OCRQ Tnl 42 PPTP: call id 0x0 Tnl 42 PPTP: serial num 0 Tnl 42 PPTP: min bps 56000:0xdac0 Tnl 42 PPTP: max bps 64000:0xfa00 Tnl 42 PPTP: bearer type 3 Tnl 42 PPTP: framing type 3 Tnl 42 PPTP: recv win size 16 Tnl 42 PPTP: ppd 0 Tnl 42 PPTP: phone num Len 0 Tnl 42 PPTP: phone num "" Tnl/Cl 42/42 PPTP: l2x store session: tunnel id 42, session id 42, hash_ix=42 PPP virtual access open, ifc = 0 Tnl/Cl 42/42 PPTP: vacc-ok -> state change wt-vacc to estabd *OCRP = Outgoing-Call-Reply - message code bytes 9 & 10 = 0008* Tnl/Cl 42/42 PPTP: CC O OCRP PPTP: cc snddata, socket FD=1, Len=32, data: 002000011a2b3c4d00080000002a00000100000000fa... *!--- Debug following this last event is flow of packets.* PPTP: cc waiting for input, max soc FD = 1 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 39, seq 1 PPP rcvd, ifc = 0, pppdev: 1, Len: 27, data: ff03c021010100170206000a00000506001137210702... PPP xmit, ifc = 0, Len: 23 data: ff03c021010100130305c22380050609894ab407020802 Interface outside - PPTP xGRE: Out paket, PPP Len 23 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 39, seq 1, ack 1, data: 3081880b00170000000000010000000 1ff03c0210101... PPP xmit, ifc = 0, Len: 17 data: ff03c0210401000d0206000a00000d0306 Interface outside - PPTP xGRE: Out paket, PPP Len 17 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 33, seq 2, ack 1, data: 3081880b00110000000000002000000001ff03c0210401... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 39, seq 2, ack 1 PPP rcvd, ifc = 0, pppdev: 1, Len: 23, data: ff03c021020100130305c22380050609894ab407020802 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 34, seq 3, ack 2 PPP rcvd, ifc = 0, pppdev: 1, Len: 18, data: ff03c0210102000e05060011372107020802 PPP xmit, ifc = 0, Len: 18 data: ff03c0210202000e05060011372107020802 Interface outside - PPTP xGRE: Out paket, PPP Len 18 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 34, seq 3, ack 3, data: 3081880b00120000000000003000000003ff03c0210202... PPP xmit, ifc = 0, Len: 17 data: ff03c2230101000d08d36602863630eca8 Interface outside - PPTP xGRE: Out paket, PPP Len 15 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 31, seq 4, ack 3, data: 3081880b000f0000000000400000003c2230101000d... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 76, seq 4, ack 4 PPP rcvd, ifc = 0, pppdev: 1, Len: 62, data: ff03c2230201003a31d4d0a397a064668bb00d954a85... PPP xmit, ifc = 0, Len: 8 data: ff03c22303010004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 22, seq 5, ack 4, data: 3081880b00060000000000000500000004c22303010004 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 58, seq 5, ack 5 PPP rcvd, ifc = 0, pppdev: 1, Len: 44, data: ff038021010100280206002d0f010306000000008106... PPP xmit, ifc = 0, Len: 14 data: ff0380210101000a030663636302 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 28, seq 6, ack 5, data: 3081880b000c0000000000060000000580210101000a... PPP xmit, ifc = 0, Len: 38 data: ff038021040100220206002d0f018106000000008206... Interface outside - PPTP xGRE: Out paket, PPP Len 36 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 52, seq 7, ack 5, data: 3081880b00240000000000007000000005802104010022... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 29, seq 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 19, data: ff0380fd0101000f120601000011105000104 PPP xmit, ifc = 0, Len: 8 data: ff0380fd01010004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 22, seq 8, ack 6, data: 3081880b00060000000000000800000000680fd01010004 PPP xmit, ifc = 0, Len: 19 data: ff0380fd0401000f120601000011105000104 Interface outside - PPTP xGRE: Out paket, PPP Len 17 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 33, seq 9, ack 6, data: 3081880b00110000000000009000000000680fd0401000f... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 28, seq 7, ack 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210201000a030663636302 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 22, seq 8, ack 8 PPP rcvd, ifc = 0, pppdev: 1, Len: 8, data: ff0380fd02010004 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 22, seq 9, ack 9 PPP rcvd, ifc = 0, pppdev: 1, Len: 8, data: ff0380fd01020004 PPP xmit, ifc = 0, Len: 8 data: ff0380fd02020004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 22, seq 10, ack 9, data: 3081880b00060000000000000a0000000980fd02020004 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 22, seq 10, ack 10 PPP rcvd, ifc = 0, pppdev: 1, Len: 8, data: ff0380fd05030004 PPP xmit, ifc = 0, Len: 8 data: ff0380fd06030004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 22, seq 11, ack 10, data: 3081880b00060000000000000b0000000a80fd06030004 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 48, seq 11 PPP rcvd, ifc = 0, pppdev: 1, Len: 38, data: ff038021010200220306000000008106000000008206... PPP xmit, ifc = 0, Len: 32 data: ff0380210402001c810600000000820600000000 8306... Interface outside - PPTP xGRE: Out paket, PPP Len 30 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 46, seq 12, ack 11, data: 3081880b001e00000000000c0000000b80210402001c... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 28, seq 12, ack 12 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210103000a030600000000

```
PPP xmit, ifc = 0, Len: 14 data: ff0380210303000a0306ac100101 Interface outside - PPTP xGRE: Out
paket, PPP Len 12 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 28, seq 13, ack 12, data:
3081880b000c00000000000d0000000c80210303000a... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 28, seq 13, ack 13 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210104000a0306ac100101
PPP xmit, ifc = 0, Len: 14 data: ff0380210204000a0306ac100101 Interface outside - PPTP xGRE: Out
paket, PPP Len 12 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 28, seq 14, ack 13, data:
3081880b000c00000000000e0000000d80210204000a... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 41, seq 14 PPP rcvd, ifc = 0, pppdev: 1, Len: 32, data:
ff0300214500001cc80000008001e5ccac100101e000... PPP IP Pkt:
4500001cc80000008001e5ccac100101e00000020a00... 603104: PPTP Tunnel created, tunnel_id is 42,
remote_peer_ip is 99.99.99.5 ppp_virtual_interface_id is 1, client_dynamic_ip is 172.16.1.1
username is john, MPPE_key_strength is None outside PPTP: Recvd xGRE pak from 99.99.99.5, Len
109, seq 15 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060ca0000008011176bac100101ac10... PPP IP Pkt:
45000060ca0000008011176bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 16 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060cb0000008011166bac100101ac10... PPP IP Pkt:
45000060cb0000008011166bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 17 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060cc0000008011156bac100101ac10... PPP IP Pkt:
45000060cc0000008011156bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 18 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060d00000008011116bac100101ac10... PPP IP Pkt:
45000060d00000008011116bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 19 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060d200000080110f6bac100101ac10... PPP IP Pkt:
45000060d200000080110f6bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 20 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060d300000080110e6bac100101ac10... PPP IP Pkt:
45000060d300000080110e6bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 41, seq 21 PPP rcvd, ifc = 0, pppdev: 1, Len: 32, data:
ff0300214500001cd60000008001d7ccac100101e000... PPP IP Pkt:
4500001cd60000008001d7ccac100101e00000020a00... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 22 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060d80000008011096bac100101ac10... PPP IP Pkt:
45000060d80000008011096bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 23 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060da0000008011076bac100101ac10... PPP IP Pkt:
45000060da0000008011076bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 24 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060db0000008011066bac100101ac10... PPP IP Pkt:
45000060db0000008011066bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 25 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060de0000008011036bac100101ac10... PPP IP Pkt:
45000060de0000008011036bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 26 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060e00000008011016bac100101ac10... PPP IP Pkt:
45000060e00000008011016bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 27 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060e10000008011006bac100101ac10... PPP IP Pkt:
45000060e10000008011006bac100101ac10ffff0089... inside:172.16.255.255/137 outside PPTP: Recvd
xGRE pak from 99.99.99.5, Len 41, seq 28 PPP rcvd, ifc = 0, pppdev: 1, Len: 32, data:
ff0300214500001ce40000008001c9ccac100101e000... PPP IP Pkt:
4500001ce40000008001c9ccac100101e00000020a00...
```

Отладка PIX - проверка подлинности RADIUS

Эти выходные данные отладки показывают важные события *курсивом*.

```
PIX#terminal monitor PIX# 106011: Deny inbound (No xlate) icmp src outside:172.17.194.164 dst
outside:172.18.124.201 (type 8, code 0) 106011: Deny inbound (No xlate) icmp src
outside:172.17.194.164 DST outside:172.18.124.201 (type 8, code 0) PIX# PPTP: soc select returns
rd mask = 0x1 PPTP: new peer FD is 1 Tnl 9 PPTP: Tunnel created; peer initiatedPPTP: created
```

tunnel, id = 9 PPTP: cc rcvdata, socket FD=1, new_conn: 1 PPTP: cc rcv 156 bytes of data *SCCRQ = Start-Control-Connection-Request - message code bytes 9 & 10 = 0001* Tnl 9 PPTP: CC I 009c00011a2b3c4d000100000100000000000010000... Tnl 9 PPTP: CC I SCCRQ Tnl 9 PPTP: protocol version 0x100 Tnl 9 PPTP: framing caps 0x1 Tnl 9 PPTP: bearer caps 0x1 Tnl 9 PPTP: max channels 0 Tnl 9 PPTP: firmware rev 0x870 Tnl 9 PPTP: hostname "" Tnl 9 PPTP: vendor "Microsoft Windows NT" Tnl 9 PPTP: SCCRQ-ok -> state change wt-sccrq to estabd *SCCRP = Start-Control-Connection-Reply - message code bytes 9 & 10 = 0002* Tnl 9 PPTP: CC O SCCRP PPTP: cc snddata, socket FD=1, Len=156, data: 009c00011a2b3c4d000200000100010000000000030000... PPTP: cc waiting for input, max soc FD = 1 PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0 PPTP: cc rcv 168 bytes of data *OCRQ = Outgoing-Call-Request - message code bytes 9 & 10 = 0007* Tnl 9 PPTP: CC I 00a800011a2b3c4d000700004000e4f50000012c05f5... Tnl 9 PPTP: CC I OCRQ Tnl 9 PPTP: call id 0x4000 Tnl 9 PPTP: serial num 58613 Tnl 9 PPTP: min bps 300:0x12c Tnl 9 PPTP: max BPS 100000000:0x5f5e100 Tnl 9 PPTP: bearer type 3 Tnl 9 PPTP: framing type 3 Tnl 9 PPTP: recv win size 64 Tnl 9 PPTP: ppd 0 Tnl 9 PPTP: phone num Len 0 Tnl 9 PPTP: phone num "" Tnl/Cl 9/9 PPTP: l2x store session: tunnel id 9, session id 9, hash_ix=9 PPP virtual access open, ifc = 0 Tnl/CL 9/9 PPTP: vacc-ok -> state change wt-vacc to estabd *OCRP = Outgoing-Call-Reply - message code bytes 9 & 10 = 0008* Tnl/CL 9/9 PPTP: CC O OCRP PPTP: cc snddata, socket FD=1, Len=32, data: 002000011a2b3c4d000800000009400001000000000fa... PPTP: cc waiting for input, max soc FD = 1 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 60, seq 0 PPP rcvd, ifc = 0, pppdev: 1, Len: 48, data: ff03c0210100002c0506447e217e070208020d030611... PPP xmit, ifc = 0, Len: 23 data: ff03c021010100130305c2238005065a899b2307020802 Interface outside - PPTP xGRE: Out paket, PPP Len 23 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 39, seq 1, ack 0, data: 3081880b00174000000000010000000ff03c0210101... PPP xmit, ifc = 0, Len: 38 data: ff03c021040000220d03061104064e131701beb613cb.. . Interface outside - PPTP xGRE: Out paket, PPP Len 38 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 54, seq 2, ack 0, data: 3081880b00264000000000002000000000ff03c0210400... PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0 PPTP: cc rcv 24 bytes of data Tnl 9 PPTP: CC I 001800011a2b3c4d000f0000000900000fffffffffffff... Tnl/CL 9/9 PPTP: CC I SLI PPTP: cc waiting for input, max soc FD = 1 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 39, seq 1, ack 1 PPP rcvd, ifc = 0, pppdev: 1, Len: 23, data: ff03c021020100130305c2238005065a899b2307020802 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 34, seq 2, ack 2 PPP rcvd, ifc = 0, pppdev: 1, Len: 18, data: ff03c0210101000e0506447e217e07020802 PPP xmit, ifc = 0, Len: 18 data: ff03c0210201000e0506447e217e07020802 Interface outside - PPTP xGRE: Out paket, PPP Len 18 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 34, seq 3, ack 2, data: 3081880b00124000000000003000000002ff03c0210201... PPP xmit, ifc = 0, Len: 17 data: ff03c2230101000d08f3686cc47e37ce67 Interface outside - PPTP xGRE: Out paket, PPP Len 15 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 31, seq 4, ack 2, data: 3081880b000f4000000000400000002c2230101000d... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 36, seq 3, ack 3 PPP rcvd, ifc = 0, pppdev: 1, Len: 22, data: ff03c0210c020012447e217e4d5352415356352e3030 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 45, seq 4 PPP rcvd, ifc = 0, pppdev: 1, Len: 35, data: ff03c0210c03001f447e217e4d535241532d312d4349... PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0 PPTP: cc rcv 24 bytes of data Tnl 9 PPTP: CC I 001800011a2b3c4d000f0000000900000000000000000... Tnl/CL 9/9 PPTP: CC I SLI PPTP: cc waiting for input, max soc FD = 1 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 76, seq 5, ack 4 PPP rcvd, ifc = 0, pppdev: 1, Len: 62, data: ff03c2230201003a3100000000000000000000000000000... uauth_mschap_send_req: pppdev=1, ulen=4, user=john 6031 uauth_mschap_proc_reply: pppdev = 1, status = 1 PPP xmit, ifc = 0, Len: 8 data: ff03c22303010004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 22, seq 5, ack 5, data: 3081880b000640000000000500000005c22303010004 CHAP peer authentication succeeded for john outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 72, seq 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 62, data: ff03c2230201003a3100000000000000000000000000000... PPP xmit, ifc = 0, Len: 8 data: ff03c22303010004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 22, seq 6, ack 6, data: 3081880b000640000000000600000006c22303010004 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 7, ack 5 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380fd0104000a120601000001 PPP xmit, ifc = 0, Len: 14 data: ff0380fd0101000a120601000020 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 7, ack 7, data: 3081880b000c400000000070000000780fd0101000a... PPP xmit, ifc = 0, Len: 14 data: ff0380fd0304000a120601000020 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 8, ack 7, data: 3081880b000c400000000080000000780fd0304000a... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 48, seq 8 PPP rcvd, ifc = 0, pppdev: 1, Len: 38, data: ff038021010500220306000000008106000000008206... PPP xmit, ifc = 0, Len: 14 data:

ff0380210101000a0306ac127c98 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 9, ack 8, data: 3081880b000c40000000000900000080210101000a... PPP xmit, ifc = 0, Len: 32 data: ff0380210405001c810600000000820600000000008306.. . Interface outside - PPTP xGRE: Out paket, PPP Len 30 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 46, seq 10, ack 8, data: 3081880b001e40000000000a000000080210405001c... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 9, ack 7 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380fd0201000a120601000020 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 10, ack 8 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380fd0106000a120601000020 PPP xmit, ifc = 0, Len: 14 data: ff0380fd0206000a120601000020 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 11, ack 10, data: 3081880b000c40000000000b0000000a80fd0206000a... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 11, ack 9 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210201000a0306ac127c98 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 12, ack 10 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210107000a030600000000 PPP xmit, ifc = 0, Len: 14 data: ff0380210307000a0306c0a80101 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 12, ack 12, data: 3081880b000c40000000000c0000000c80210307000a... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 24, seq 13 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210108000a030600000000 PPP xmit, ifc = 0, Len: 14 data: ff0380210308000a0306c0a80101 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 13, ack 13, data: 3081880b000c40000000000d0000000d80210308000a... 0 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 14, ack 13 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210109000a0306c0a80101 PPP xmit, ifc = 0, Len: 14 data: ff0380210209000a0306c0a80101 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 14, ack 14, data: 3081880b000c40000000000e0000000e80210209000a... 2: PPP virtual interface 1 - user: john aaa authentication started 603103: PPP virtual interface 1 - user: john aaa authentication succeed 109011: Authen Session Start: user 'joh outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 117, seq 15, ack 14 PPP rcvd, ifc = 0, pppdev: 1, Len: 104, data: ff0300fd9000bccf59b71755d9af7330dae3bbc94d28... PPP Encr/Comp Pkt: 9000bccf59b71755d9af7330dae3bbc94d28e431d057... PPP IP Pkt: 4500006002bb000080117629c0a80101ffffffff0089... n', sid 3 603104: PPTP Tunnel created, tunnel_id is 9, remote_peer_ip is 10.44.17.104 ppp_virtual_interface_id is 1, client_dynamic_ip is 192.168.1.1 username is john, MPPE_key_strength is 40 bits outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 113, seq 16 PPP rcvd, ifc = 0, pppdev: 1, Len: 104, data: ff0300fd9001f8348351ef9024639ed113b43adfeb44... PPP Encr/Comp Pkt: 9001f8348351ef9024639ed113b43adfeb4489af5ab3... PPP IP Pkt: 4500006002bd000080117627c0a80101ffffffff0089... ide outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 113, seq 17 PPP rcvd, ifc = 0, pppdev: 1, Len: 104, data: ff0300fd9002cc73cd65941744a1cf30318cc4b4b783... PPP Encr/Comp Pkt: 9002cc73cd65941744a1cf30318cc4b4b783e825698a... PPP IP Pkt: 4500006002bf000080117625c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 18 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd9003aaa545eaeeda0f82b5999e2fa9ba3245... PPP Encr/Comp Pkt: 9003aaa545eaeeda0f82b5999e2fa9ba324585a1bc8d... PPP IP Pkt: 4500006002c1000080117623c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 19 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd90045b35d080900ab4581e64706180e3540e... PPP Encr/Comp Pkt: 90045b35d080900ab4581e64706180e3540ee15d664a... PPP IP Pkt: 4500006002c3000080117621c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 20 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd90052878b256edbd17b42f2cb672ba80b40a... PPP Encr/Comp Pkt: 90052878b256edbd17b42f2cb672ba80b40a79760cef... PPP IP Pkt: 4500006002c500008011761fc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 21 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd900632359a2c07e79106c5e282e3892e60de... PPP Encr/Comp Pkt: 900632359a2c07e79106c5e282e3892e60ded6c6d4d1... PPP IP Pkt: 4500006002c700008011761dc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 22 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd90070ca6ea48b2ad26987d52a4e109ca68b6... PPP Encr/Comp Pkt: 90070ca6ea48b2ad26987d52a4e109ca68b6758569d3... PPP IP Pkt: 4500006002c900008011761bc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 23 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd90085aba60edf57e50eea4d523596cb9d690... PPP Encr/Comp Pkt:

```
90085aba60edf57e50eea4d523596cb9d69057715894... PPP IP Pkt:
4500006002cb000080117619c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 24 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd90094b73b6c962272b60d32f135b5f29f2a5... PPP Encr/Comp Pkt:
90094b73b6c962272b60d32f135b5f29f2a58bacd050... PPP IP Pkt:
4500006002cc000080117618c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 345, seq 25 PPP rcvd, ifc = 0, pppdev: 1, len: 336, data:
ff0300fd900a86307ed9537df5389ea09223d62c20fd... PPP Encr/Comp Pkt:
900a86307ed9537df5389ea09223d62c20fd9e34072f... PPP IP Pkt:
4500014802cf00008011752dc0a80101ffffffff0044... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 26 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900b45303a5fe7b2dc3f62db739b4bb1b802... PPP Encr/Comp Pkt:
900b45303a5fe7b2dc3f62db739b4bb1b80253278fad... PPP IP Pkt:
4500006002d1000080117613c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 27 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900ceb5aaaecc832df3c12bc6c519c25b4db... PPP Encr/Comp Pkt:
900ceb5aaaecc832df3c12bc6c519c25b4dba569d10... PPP IP Pkt:
4500006002d2000080117612c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 28 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900dbdaaf071c2bd1c92c1f56085813d1a77... PPP Encr/Comp Pkt:
900dbdaaf071c2bd1c92c1f56085813d1a778cc61c29... PPP IP Pkt:
4500006002d500008011760fc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 29 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900e97de47036d95a0721ef6b28479b8efde... PPP Encr/Comp Pkt:
900e97de47036d95a0721ef6b28479b8efde8e16b398... PPP IP Pkt:
4500006002d600008011760ec0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 30 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900f75bf4c8cbcf11464bf52bd7f6155c7d6... PPP Encr/Comp Pkt:
900f75bf4c8cbcf11464bf52bd7f6155c7d62ea2ca5e... PPP IP Pkt:
4500006002d900008011760bc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 31 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd9010f221e7ba169702765529e4ffa368dba5... PPP Encr/Comp Pkt:
9010f221e7ba169702765529e4ffa368dba5610921ae... PPP IP Pkt:
4500006002da00008011760ac0a80101ffffffff0089... from (192.168.1.1) to 255.255.255.255 on
interface outside outside PPTP: Recvd xGRE pak from 10.44.17.104, len 231, seq 32 PPP rcvd, ifc
= 0, pppdev: 1, len: 222, data: ff0300fd9011c23a03921c1e10ccc38847cb8056fa93... PPP Encr/Comp
Pkt: 9011c23a03921c1e10ccc38847cb8056fa9387018912... PPP IP Pkt:
450000d602dd000080117591c0a80101ffffffff008a... side outside PPTP: Recvd xGRE pak from
10.44.17.104, len 345, seq 33 PPP rcvd, ifc = 0, pppdev: 1, len: 336, data:
ff0300fd90127d7213f35cd1d82d8988e28e0930ecc1... PPP Encr/Comp Pkt:
90127d7213f35cd1d82d8988e28e0930ecc104a993f... PPP IP Pkt:
4500014802df00008011751dc0a80101ffffffff0044...
```

Возможные проблемы

Одновременный туннель PPTP

Вы неспособны подключить больше чем 127 соединений с PIX 6.x, и это сообщение об ошибках появляется:

%PIX-3-213001: io сокета демона контроля за PPTP принимают ошибку, errno = 5

Решение:

Существует аппаратное ограничение 128 параллельных сеансов в PIX 6. x. Если вы вычитаете один для PPTP, слушая сокет, максимальное число is127 соединения.

Брандмауэр PIX и компьютер не могут согласовать аутентификацию

Протоколы аутентификации ПК установлены для, которые PIX неспособен сделать (Протокол проверки пароля Shiva (SPAP) и Версия 2 Microsoft CHAP (MS-CHAP v.2) вместо версии 1). ПК и PIX не могут договориться об аутентификации. ПК выдает следующее сообщение:

```
Disconnected - Error 732: Your computer and the remote computer
    could not agree on PPP control protocols
```

PIX и ПК не может согласовать шифрование

ПК установлен для **Зашифрованного только**, и **vpdn group 1 ppp encrypt mppe 40 required** команда удалена из PIX. ПК и PIX не могут договориться о шифровании, и ПК выдает следующее сообщение:

```
Error 742 : The remote computer does not support the required
    data encryption type.
```

PIX и ПК не может согласовать шифрование

PIX установлен для **vpdn group 1 ppp encrypt mppe 40 required** и ПК ни для какого позволенного шифрования. В этом случае на ПК не появляется никаких сообщений, однако сеанс прерывается, и отладка PIX выдает следующие выходные данные:

```
PPTP: Call id 8, no session id protocol: 21,
    reason: mppe required but not active, tunnel terminated
603104: PPTP Tunnel created, tunnel_id is 8,
    remote_peer_ip is 10.44.17.104
ppp_virtual_interface_id is 1, client_dynamic_ip is 192.168.1.1
username is cisco, MPPE_key_strength is None
603105: PPTP Tunnel deleted, tunnel_id = 8,
    remote_peer_ip = 10.44.17.104
```

Проблема PIX MPPE RADIUS

PIX установлен для **vpdn group 1 ppp encrypt mppe 40 required**, и ПК для шифрования, позволенного с аутентификацией серверу RADIUS, не возвращает ключ MPPE. ПК выдает следующее сообщение:

```
Error 691: Access was denied because the username
    and/or password was invalid on the domain.
```

Отладка PIX показывает:

```
2: PPP virtual interface 1 -
   user: cisco  aaa authentication started
603103: PPP virtual interface 1 -
   user: cisco  aaa authentication failed
403110: PPP virtual interface 1,
   user: cisco missing MPPE key from aaa server
603104: PPTP Tunnel created,
   tunnel_id is 15,
   remote_peer_ip is 10.44.17.104
   ppp_virtual_interface_id is 1,
   client_dynamic_ip is 0.0.0.0
   username is Unknown,
   MPPE_key_strength is None
603105: PPTP Tunnel deleted,
   tunnel_id = 15,
   remote_peer_ip = 10.44.17.104
```

ПК выдает следующее сообщение:

```
Error 691: Access was denied because the username
    and/or password was invalid on the domain.
```

Дополнительные сведения

- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Устранение наиболее распространенных проблем удаленных VPN-подключений и VPN-туннелей LAN — LAN на базе протокола IPSec
- Страница поддержки PPTP
- RFC 2637: Протокол PPTP
- Запросы комментариев (RFC)
- Техническая поддержка - Cisco Systems