

PIX 6.x : 使用 Radius 身份验证的 PPTP 配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[PIX 防火墙的配置提示](#)

[在客户端 PC 上配置 PPTP 功能](#)

[Windows 98](#)

[Windows 2000](#)

[Windows NT](#)

[配置 PIX](#)

[PIX 配置- 本地验证 \(带加密\)](#)

[PIX 配置- RADIUS 验证 \(带加密\)](#)

[配置 Cisco Secure ACS for Windows 3.0](#)

[RADIUS 验证 \(带加密\)](#)

[验证](#)

[PIX \(身份验证后\) show 命令](#)

[客户端 PC 验证](#)

[故障排除](#)

[故障排除命令](#)

[在客户端 PC 上启用 PPP 日志记录](#)

[其他 Microsoft 问题](#)

[调试输出示例](#)

[可能出现的错误](#)

[相关信息](#)

简介

点对点隧道协议 (PPTP) 是第二层隧道协议，它使远程客户端可以使用公共 IP 网络与专用公司网络中的服务器安全地进行通信。PPTP 以隧道方式传输 IP 数据流。[RFC 2637 中介绍了 PPTP。](#) PIX 软件版本 5.1 中增加了 PIX 防火墙上的 PPTP 支持。PIX [文档](#) 提供了有关 PPTP 及其与 PIX 的使用的详细信息。本文档说明如何配置 PIX 以将 PPTP 与本地、TACACS+ 和 RADIUS 身份验证配合使用。本文档还提供了可用来帮助您排除常见问题的提示和示例。

本文档显示如何配置到 *PIX* 的 *PPTP* 连接。要配置 *PIX* 或 *ASA* 以允许 *PPTP* 通过安全设备，请参阅[允许通过 *PIX* 的 *PPTP/L2TP* 连接](#)。

请参阅[Cisco Secure *PIX* 防火墙 6.x 和适用于 Windows 的 Cisco VPN 客户端 3.5 与 Microsoft Windows 2000 和 2003 IAS RADIUS 身份验证以配置 *PIX* 防火墙和 VPN 客户端以与 Windows 2000 和 2003 Internet 身份验证服务 \(IAS\) RADIUS 服务器一起使用](#)。

请参阅[配置使用 Cisco Secure ACS for Windows RADIUS 身份验证的 VPN 3000 集中器和 *PPTP* 以在使用 Cisco Secure ACS for Windows 进行 RADIUS 身份验证的 VPN 3000 集中器上配置 *PPTP*](#)。

请参阅[配置 Cisco Secure ACS for Windows 路由器 *PPTP* 身份验证以设置到路由器的 PC 连接](#)，该路由器会先提供对用于 Windows 的 Cisco 安全访问控制系统 (ACS) 3.2 服务器的用户身份验证，然后再允许该用户进入网络。

注意：在 *PPTP* 术语中，根据 RFC，*PPTP* 网络服务器 (PNS) 是服务器（在本例中为 *PIX* 或被叫方），而 *PPTP* 接入集中器 (PAC) 是客户端（PC 或主叫方）。

注意：*PIX* 上不支持 *PPTP* 客户端的拆分隧道。

注意：*PIX* 6.x 需要 MS-CHAP v1.0，以便 *PPTP* 能够工作。Windows Vista 不支持 MS-CHAP v1.0。因此 *PIX* 6.x 上的 *PPTP* 对 Windows Vista 不起作用。*PIX* 版本 7.x 及更高版本不支持 *PPTP*。

[先决条件](#)

[要求](#)

本文档没有任何特定的要求。

[使用的组件](#)

本文档中的信息基于 Cisco Secure *PIX* 防火墙软件版本 6.3(3)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

[规则](#)

有关文档约定的更多信息，请参考[Cisco 技术提示约定](#)。

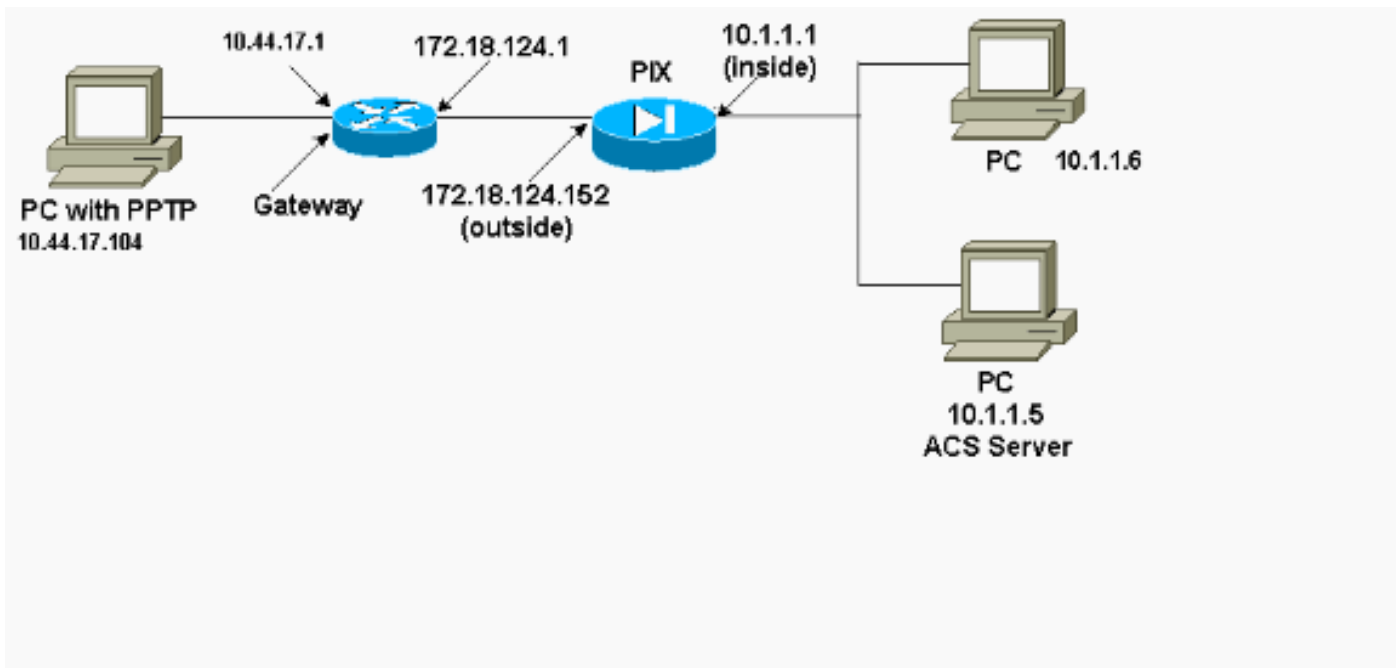
[配置](#)

本部分提供有关如何配置本文档所述功能的信息。

注意：使用[命令查找工具](#)（仅限注册客户）可获取有关本节中使用的命令的详细信息。

[网络图](#)

本文档使用此网络设置。



[PIX 防火墙的配置提示](#)

[身份验证类型 - CHAP、PAP 和 MS-CHAP](#)

无论 PC 的配置方式如何，同时配置了所有三种身份验证方法（CHAP、PAP 和 MS-CHAP）的 PIX 都可提供最好的连接机会。这是进行故障排除的好办法。

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

[Microsoft 点对点加密 \(MPPE\)](#)

使用此命令语法可在 PIX 防火墙上配置 MPPE 加密。

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

在此命令中，**required** 是可选关键字。必须配置 MS-CHAP。

[在客户端 PC 上配置 PPTP 功能](#)

注意：此处提供的有关 Microsoft 软件配置的信息不附带任何 Microsoft 软件保修或支持。Microsoft 软件支持由 Microsoft 提供，可从 [Microsoft 支持网站](#) 获得。

[Windows 98](#)

要在 Windows 98 上安装 PPTP 功能，请执行以下步骤。

1. 选择开始 > 设置 > 控制面板 > 添加新硬件。单击 Next。
2. 单击 **Select from List** 并选择 **Network Adapter**。单击 Next。
3. 在左侧面板中选择 **Microsoft**，在右侧面板中选择 **Microsoft VPN Adapter**。

要配置 PPTP 功能，请执行以下步骤。

1. 选择开始 > 程序 > 附件 > 通讯 > 拨号网络。
2. 单击 **新建连接**。对于 **选择设备**，使用 **Microsoft VPN 适配器** 连接。VPN 服务器 IP 地址是 PIX 隧道端点。
3. Windows 98 默认身份验证使用口令加密 (CHAP 或 MS-CHAP)。要将 PC 更改为也允许 PAP，请选择 **属性 > 服务器类型**。取消选中 **Require encrypted password**。可在该区域配置数据加密 (MPPE 或没有 MPPE)。

Windows 2000

要在 Windows 2000 上配置 PPTP 功能，请执行以下步骤。

1. 选择开始 > 程序 > 附件 > 通讯 > 网络和拨号连接。
2. 单击 **新建连接**，然后单击“下一步”。
3. 选择 **通过 Internet 连接到专用网络**和“**先进行拨号连接**” (如果有 LAN，请勿选择该项)。单击 **Next**。
4. 输入隧道端点 (PIX/路由器) 的主机名或 IP 地址。
5. 如果要更改口令类型，请选择 **Properties > Security for the connection > Advanced**。默认值是 MS-CHAP 和 MS-CHAP v2 (不是 CHAP 或 PAP)。可在该区域配置数据加密 (MPPE 或没有 MPPE)。

Windows NT

请参阅[通过 Microsoft 客户端和服务端安装、配置和使用 PPTP 以设置用于 PPTP 的 NT 客户端。](#)

配置 PIX

PIX 配置 - 本地身份验证 (不加密)

```
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

```

[PIX 配置- 本地验证 \(带加密\)](#)

如果将此命令添加到“PIX 配置 - 本地身份验证 (不加密)”配置，则 PC 和 PIX 会自动协商 40 位加密或不加密 (基于 PC 设置)。

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

如果 PIX 上已启用 3DES 功能，则 `show version` 命令会显示此消息。

- 版本 6.3 及更高版本：

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

- 版本 6.2 及更低版本：

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

也可使用 128 位加密。但是，如果显示以下消息之一，则表示 PIX 不支持 128 位加密。

- 版本 6.3 及更高版本：

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

- 版本 6.2 及更低版本：

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

MPPE 命令的语法如下所示。

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

必须将 PC 和 PIX 配置为将 MS-CHAP 身份验证和 MPPE 一起使用。

PIX 配置 - TACACS+/RADIUS 身份验证 (不带加密)

```
PIX Version 6.3(3)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pix/intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUGlTp0edmkr 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]

```

[PIX 配置- RADIUS 验证 \(带加密\)](#)

如果使用 RADIUS，并且如果 RADIUS 服务器（供应商特定属性 26，Microsoft 作为供应商）支持 MPPE 密钥设置，则可以添加 MPPE 加密。TACACS+ 身份验证不能与加密配合使用，因为 TACACS+ 服务器无法返回特殊 MPPE 密钥。Cisco Secure ACS for Windows 2.5 及更高版本的 RADIUS 不支持 MPPE（并非所有 RADIUS 服务器都支持 MPPE）。

假设 RADIUS 身份验证在不加密的情况下工作，则可通过在前面的配置中包括以下命令来添加加密：

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

PC 和 PIX 自动协商 40 位加密或不加密（基于 PC 设置）。

如果 PIX 上已启用 3DES 功能，则 **show version** 命令会显示此消息。

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

也可使用 128 位加密。但是，如果显示以下消息，则表示 PIX 不支持 128 位加密。

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

MPPE 命令的语法显示在此输出中。

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

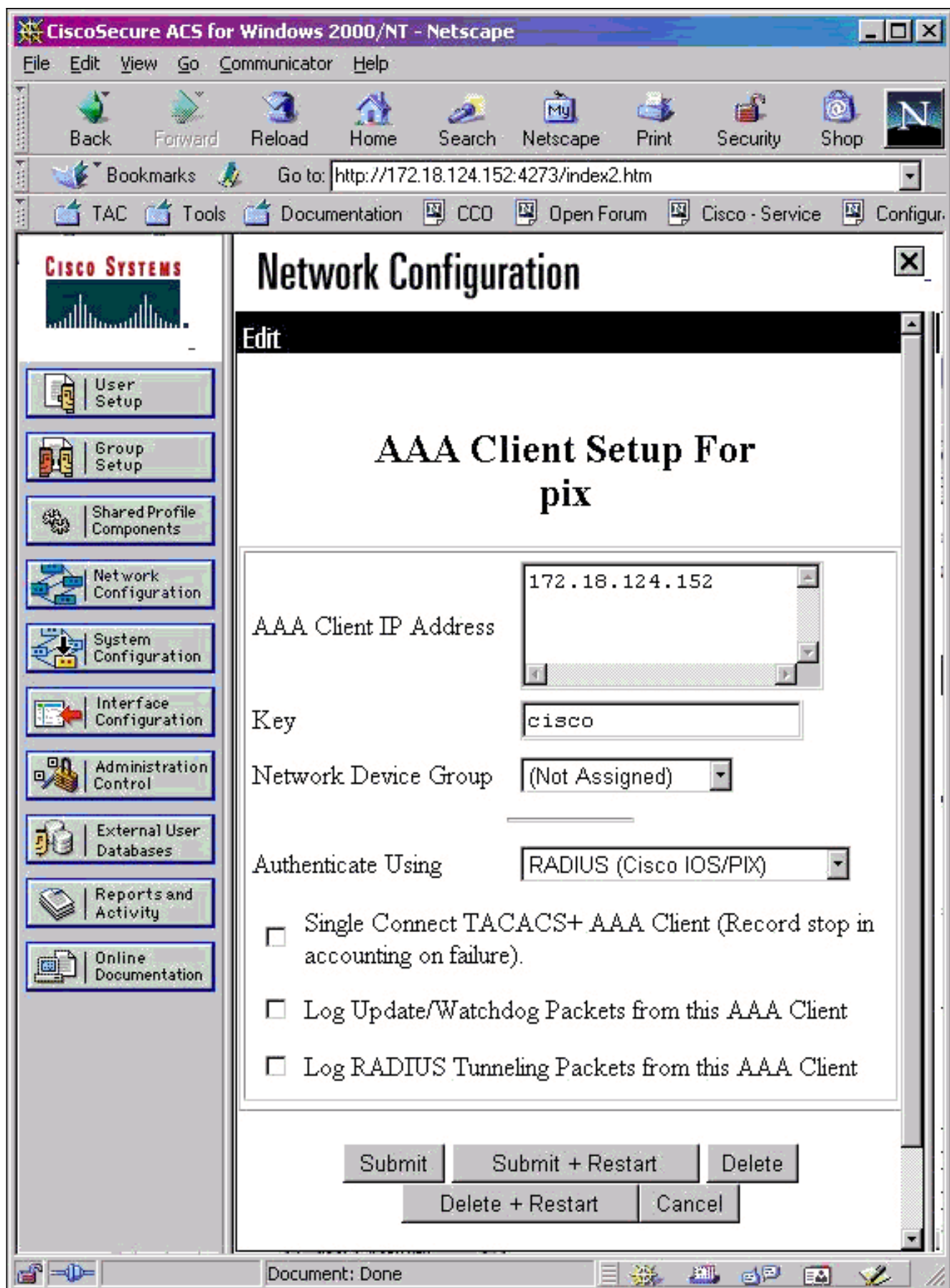
必须将 PC 和 PIX 配置为将 MS-CHAP 身份验证和 MPPE 一起使用。

[配置 Cisco Secure ACS for Windows 3.0](#)

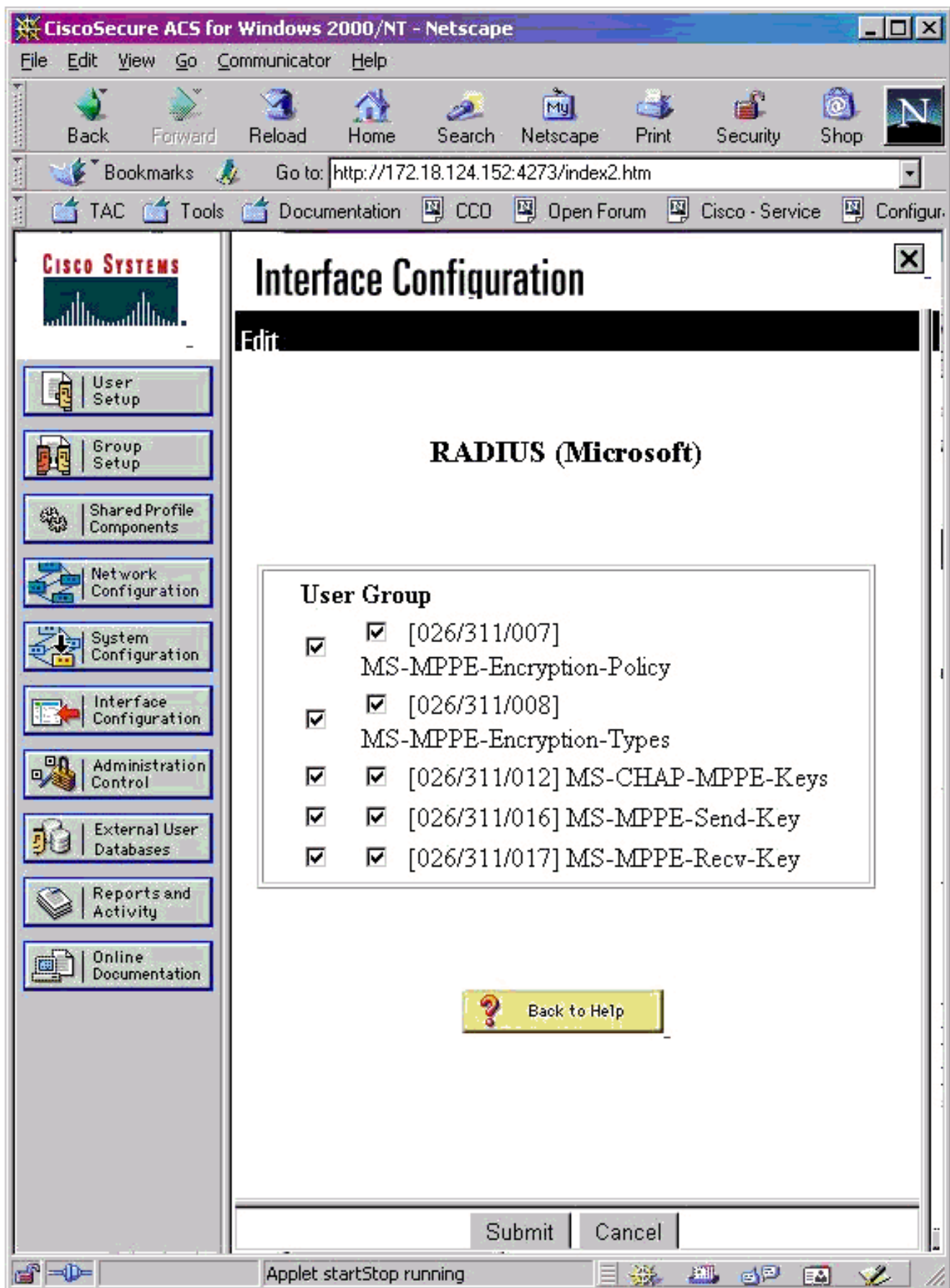
[RADIUS 验证（带加密）](#)

使用这些步骤配置 Cisco Secure ACS for Windows 3.0。相同的配置步骤适用于 ACS 版本 3.1 和 3.2。

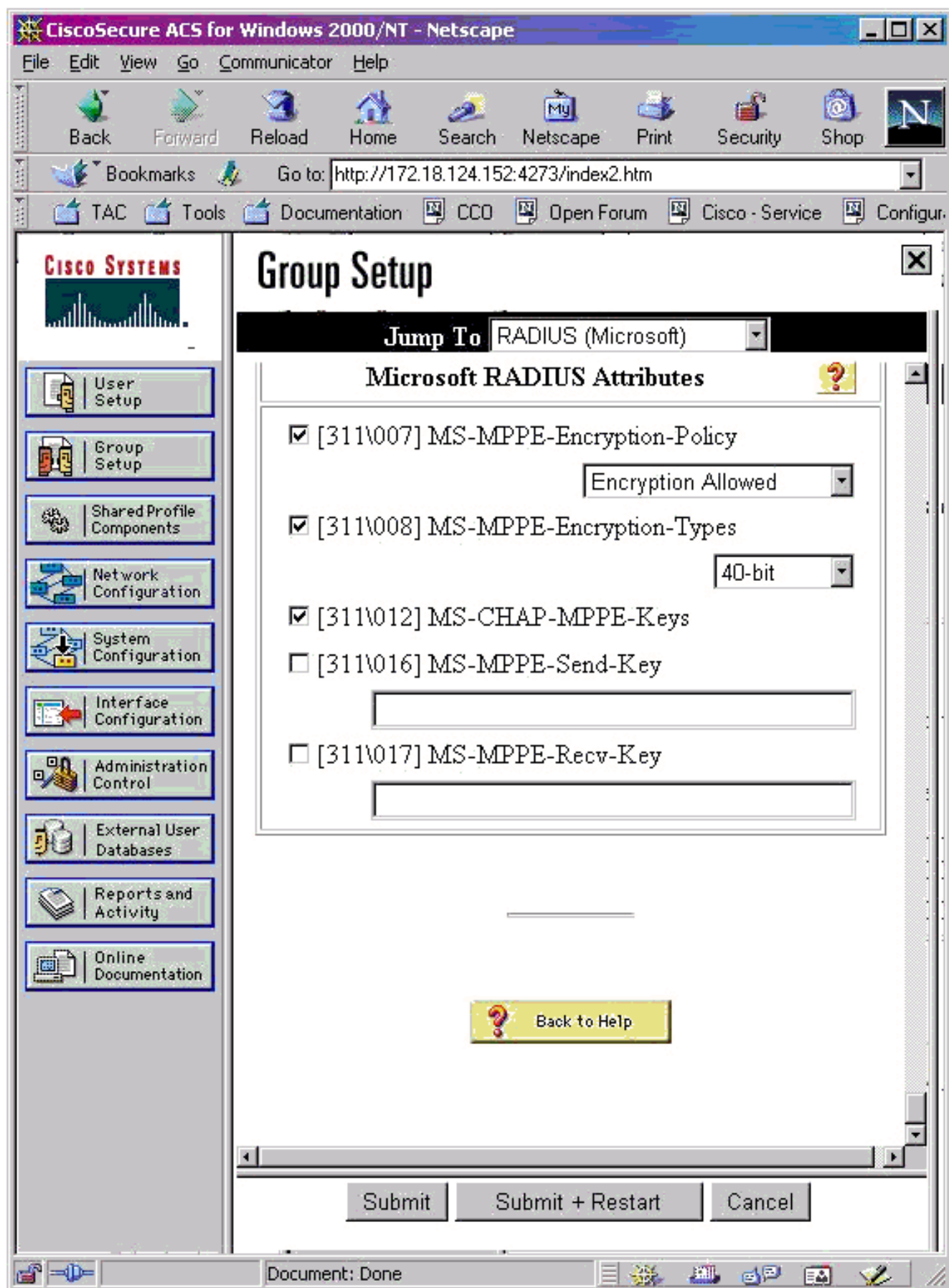
1. 将 PIX 添加到 Cisco Secure ACS for Windows 服务器网络配置并将字典类型标识为 RADIUS (Cisco IOS/PIX)。



2. 打开 Interface Configuration > RADIUS (Microsoft) 并选中 MPPE 属性以使它们出现在组接口中。



3. 添加用户。在用户组中，添加MPPE [RADIUS(Microsoft)]属性。您必须启用这些属性才能使用加密，当 PIX 未配置为使用加密时，这是可选的。



验证

本部分提供的信息可帮助您确认您的配置是否可正常运行。

[PIX \(身份验证后 \) show 命令](#)

[命令输出解释程序 \(仅限注册用户 \) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

show vpdn 命令可列出隧道和会话信息。

```
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
```

[客户端 PC 验证](#)

在 MS-DOS 窗口中，或在“运行”窗口中，键入 **ipconfig /all**。PPP 适配器部分显示以下输出。

```
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 . . . . . :
```

也可以单击 **Details** 以查看 PPTP 连接中的信息。

[故障排除](#)

本部分提供的信息可用于对配置进行故障排除。

- 必须存在从 PC 到 PIX 隧道端点的通用路由封装 (GRE) 和 TCP 1723 的连接。如果此连接有可能被防火墙或访问列表禁止，请将 PC 向 PIX 靠近。
- Windows 98 和 Windows 2000 PPTP 是最容易设置的。如果拿不准，请尝试多个 PC 和操作系统。连接成功后，单击 PC 上的 **Details** 以显示有关连接的信息。例如，显示您是否使用 PAP、CHAP、IP、加密等。
- 如果计划使用 RADIUS 和/或 TACACS+，请首先尝试设置本地 (PIX 上的用户名和口令) 身份验证。如果这不起作用，则表示使用 RADIUS 或 TACACS+ 服务器进行身份验证不起作用。

- 最初，请确保 PC 上的安全设置允许尽可能多的不同身份验证类型 (PAP、CHAP 和 MS-CHAP) 并取消选中 **Require data encryption** 的复选框 (使它在 PIX 和 PC 上都可选)。
- 由于身份验证类型是协商确定的，因此请将 PIX 配置为具有最大可能数量的身份验证类型。例如，如果 PC 配置为仅使用 MS-CHAP，而路由器配置为仅使用 PAP，则永远达不成任何协议。
- 如果 PIX 充当两个不同位置的 PPTP 服务器，并且每个位置内部都有其自己的 RADIUS 服务器，则不支持对由其各自的 RADIUS 服务器提供服务的两个位置使用单个 PIX。
- 有些 RADIUS 服务器不支持 MPPE。如果 RADIUS 服务器不支持 MPPE 密钥设置，则 RADIUS 身份验证可以起作用，但 MPPE 加密不起作用。
- 对于 Windows 98 或更高版本，当您使用 PAP 或 CHAP 时，发送到 PIX 的用户名与您在拨号网络 (DUN) 连接中输入的内容相同。但当您使用 MS-CHAP 时，可以在用户名前面附加域名，例如：在 DUN 中输入的用户名 -“cisco”在 Windows 98 框中设置的域 -“DOMAIN”发送到 PIX 的 MS-CHAP 用户名 -“DOMAIN\cisco”PIX 上的用户名 -“cisco”结果 - 无效的用户名/口令这是 Windows 98 PC 的 PPP 日志中显示此行为的一个部分。

```
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.
```

如果对 PIX 使用 Windows 98 和 MS-CHAP，则除了具有非域用户名外，还可以将“DOMAIN\用户名”添加到 PIX：

```
vpdn username cisco password cisco
vpdn username DOMAIN\cisco password cisco
```

注：如果在 AAA 服务器上执行远程身份验证，则同样适用。

故障排除命令

有关 PPTP 事件的预期序列的序列信息，可在 PPTP [RFC 2637 中找到](#)。在 PIX 上，正常 PPTP 序列中的重大事件显示：

```
SCCRQ (Start-Control-Connection-Request)
SCCRP (Start-Control-Connection-Reply)
OCRQ (Outgoing-Call-Request)
OCRP (Outgoing-Call-Reply)
```

注意：在使用 debug 命令之前，请参阅有关 Debug 命令的重要信息。

PIX debug 命令

- debug ppp io—显示 PPTP PPP 虚拟接口的数据包信息。
- debug ppp error - 显示与 PPP 连接协商和操作关联的协议错误和错误统计数据。
- debug vpdn error - 显示导致无法建立 PPP 隧道的错误或导致已建立的隧道关闭的错误。
- debug vpdn packet - 显示作为 VPDN 的正常隧道建立或关闭一部分的 L2TP 错误和事件。
- debug vpdn events - 显示正常 PPP 隧道建立或关闭过程中的事件的相关消息。
- debug ppp uauth—显示 PPTP PPP 虚拟接口 AAA 用户身份验证调试消息。

[PIX clear 命令](#)

此命令必须在配置模式下发出。

- **clear vpdn tunnel [all | [id tunnel_id]]** — 从配置中删除一个或多个PPTP隧道。

注意：不发出clear vpdn命令。这将清除所有 vpdn 命令。

[在客户端 PC 上启用 PPP 日志记录](#)

要为各种 Windows 和 Microsoft 操作系统启用 PPP 日志记录，请按照以下说明完成操作。

[Windows 95](#)

要在 Windows 95 计算机上启用 PPP 日志记录，请执行以下步骤。

1. 在“控制面板”中的“网络”选项中，双击已安装网络组件列表中的 **Microsoft 拨号适配器**。
2. 单击 **Advanced 选项卡**。在“属性”列表中，单击名为 **记录日志文件**的选项，并在“值”列表中，单击“是”。然后单击 **OK**。
3. 关闭并重新启动计算机以使此选项生效。日志将保存在名为 ppplog.txt 的文件中。

[Windows 98](#)

要在 Windows 98 计算机上启用 PPP 日志记录，请执行以下步骤。

1. 在**拨号网络**中，单击连接图标，然后选择“文件”>“属性”。
2. 单击“服务器类型”选项卡。
3. 选择名为**为此连接记录一个日志文件**的选项。该日志文件位于 C:\Windows\ppplog.txt

[Windows 2000](#)

要在 Windows 2000 计算机上启用 PPP 日志记录，请转到 [Microsoft 支持页 并搜索“在 Windows 中启用 PPP 日志记录”](#)。

[Windows NT](#)

要在 NT 系统上启用 PPP 日志记录，请执行以下步骤。

1. 找到密钥SYSTEM\CurrentControlSet\Services\RasMan\PPP，并将Logging从0更改为1。这将在<winnt root>\SYSTEM32\RAS directory中创建一个名为PPP.LOG的文件。
2. 要调试 PPP 会话，请先启用日志记录，然后启动 PPP 连接。当连接失败或退出时，可检查 PPP.LOG 以了解发生的情况。

有关详细信息，请参阅 [Microsoft 支持页 并搜索“在 Windows NT 中启用 PPP 日志记录”](#)。

[其他 Microsoft 问题](#)

下面列出了排除 PPTP 故障时要考虑的几个 Microsoft 相关问题。通过下面提供的链接，可以从 Microsoft 知识库获得详细信息。

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: 3081880b000f00000000000400000003c2230101000d... 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: 3081880b00060000000000500000004c22303010004 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: 3081880b000c000000000060000000580210101000a... 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: 3081880b00240000000000700000005802104010022... outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 29, seq 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 19, data: ff0380fd0101000f1206010000011105000104 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: 3081880b0006000000000080000000680fd01010004 PPP xmit, ifc = 0, Len: 19 data: ff0380fd0401000f1206010000011105000104 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: 3081880b0011000000000090000000680fd0401000f... 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: 3081880b00060000000000a0000000980fd02020004 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: 3081880b00060000000000b0000000a80fd06030004 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: ff0380210402001c8106000000008206000000008306... 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: 3081880b001e0000000000c0000000b80210402001c... 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: 3081880b000c0000000000d0000000c80210303000a... 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: 3081880b000c0000000000e0000000d80210204000a... 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...
```

PIX 调试 - RADIUS 身份验证

此调试输出以斜体显示重大事件。

```
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
009c00011a2b3c4d0001000001000000000000010000... 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: 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 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: 002000011a2b3c4d00080000000940000100000000fa... 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: 3081880b001740000000000100000000ff03c0210101... 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: 3081880b002640000000000200000000ff03c0210400... 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 001800011a2b3c4d000f000000090000fffffffff... 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: 3081880b001240000000000300000002ff03c0210201... 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: 3081880b000f40000000000400000002c2230101000d... 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 001800011a2b3c4d000f000000090000000000000000... 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: ff03c2230201003a31000000000000000000000000... 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: ff03c2230201003a31000000000000000000000000... 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: 3081880b000c400000000090000000880210101000a... PPP xmit, ifc = 0, Len: 32 data: ff0380210405001c81060000000820600000008306.. . 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: 3081880b001e4000000000a0000000880210405001c... 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: 3081880b000c4000000000b0000000a80fd0206000a... 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:
3081880b000c4000000000c0000000c80210307000a... 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:
3081880b000c4000000000d0000000d80210308000a... 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: 3081880b000c4000000000e0000000e80210209000a... 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:
ff0300fd90045b35d080900ab4581e64706180e3540ee15d664a... 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...
```

[可能出现的错误](#)

[同时 PPTP 隧道](#)

您与 PIX 6.x 之间不能建立 127 个以上的连接，将显示以下错误消息：

```
%PIX-3-213001:PPTP control daemon socket io accept error, errno = 5
```

解决方案：

PIX 6.x 中有 128 个并发会话的硬件限制。如果减去一个用于 PPTP 监听套接字的连接，则最大连接数为 127。

[PIX 和 PC 无法协商身份验证](#)

PC 身份验证协议设置为 PIX 无法执行的协议（Shiva 口令身份验证协议 (SPAP) 和 Microsoft CHAP 版本 2 (MS-CHAP v.2) 而不是版本 1）。PC 和 PIX 无法就身份验证达成协议。PC 显示以下消息：

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

[PIX 和 PC 无法协商加密](#)

PC 设置为 **Encrypted only** 并且 **vpdn group 1 ppp encrypt mppe 40 required** 命令已从 PIX 中删除。PC 和 PIX 无法就加密达成协议，PC 显示以下消息：

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

[PIX 和 PC 无法协商加密](#)

PIX 设置为 **vpdn group 1 ppp encrypt mppe 40 required** 并且 PC 设置为不允许任何加密。这不会在 PC 上生成任何消息，但会话会断开连接并且 PIX debug 显示以下输出：

```
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
```

[PIX MPPE RADIUS 问题](#)

PIX 设置为 **vpdn group 1 ppp encrypt mppe 40 required** 并且 PC 设置为“**encryption allowed with authentication to a RADIUS server does not return the MPPE key**”。PC 显示以下消息：

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

PIX debug 显示：

```
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
```

PC 显示以下消息：

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

[相关信息](#)

- [Cisco PIX 防火墙软件](#)
- [Cisco Secure PIX 防火墙命令参考](#)
- [安全产品 Field Notices \(包括 PIX\)](#)
- [最常见的L2L和远程访问IPSec VPN故障排除解决方案](#)

- [PPTP 支持页](#)
- [RFC 2637 : 点对点隧道协议 \(PPTP\)](#)
- [请求注解 \(RFC\)](#)
- [技术支持 - Cisco Systems](#)