Configuring the Cisco Secure PIX Firewall to Use PPTP

Document ID: 14096

Introduction

Point−to−Point Tunneling Protocol (PPTP) is a Layer 2 tunneling protocol which allows a remote client to use a public IP network in order to communicate securely with servers at a private corporate network. PPTP tunnels the IP. PPTP is described in RFC 2637 . PPTP support on the PIX Firewall was added in PIX Software release 5.1. The PIX documentation provides more information about PPTP and its use with the PIX. This document describes how to configure the PIX to use PPTP with local, TACACS+, and RADIUS authentication. This document also provides tips and examples you can use to help you troubleshoot common problems.

This document shows how to configure PPTP connections *to* the PIX. In order to configure a PIX or ASA to permit PPTP *through* the security appliance, refer to Permitting PPTP Connections Through the PIX.

Refer to Cisco Secure PIX Firewall 6.x and Cisco VPN Client 3.5 for Windows with Microsoft Windows 2000 and 2003 IAS RADIUS Authentication in order to configure the PIX Firewall and VPN Client for use with the Windows 2000 and 2003 Internet Authentication Service (IAS) RADIUS Server.

Refer to Configuring the VPN 3000 Concentrator and PPTP with Cisco Secure ACS for Windows RADIUS Authentication to configure PPTP on a VPN 3000 Concentrator with Cisco Secure Access Control System (ACS) for Windows for RADIUS authentication.

Refer to Configuring Cisco Secure ACS for Windows Router PPTP Authentication to set up a PC connection to the router, which then provides user authentication to the Cisco Secure ACS 3.2 for Windows server, before you allow the user into the network.

Note: In PPTP terms, per the RFC, the PPTP Network Server (PNS) is the server (in this case, the PIX, or the callee) and the PPTP Access Concentrator (PAC) is the client (the PC, or the caller).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Secure PIX Firewall Software Release 6.2(1) and 6.3(3).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

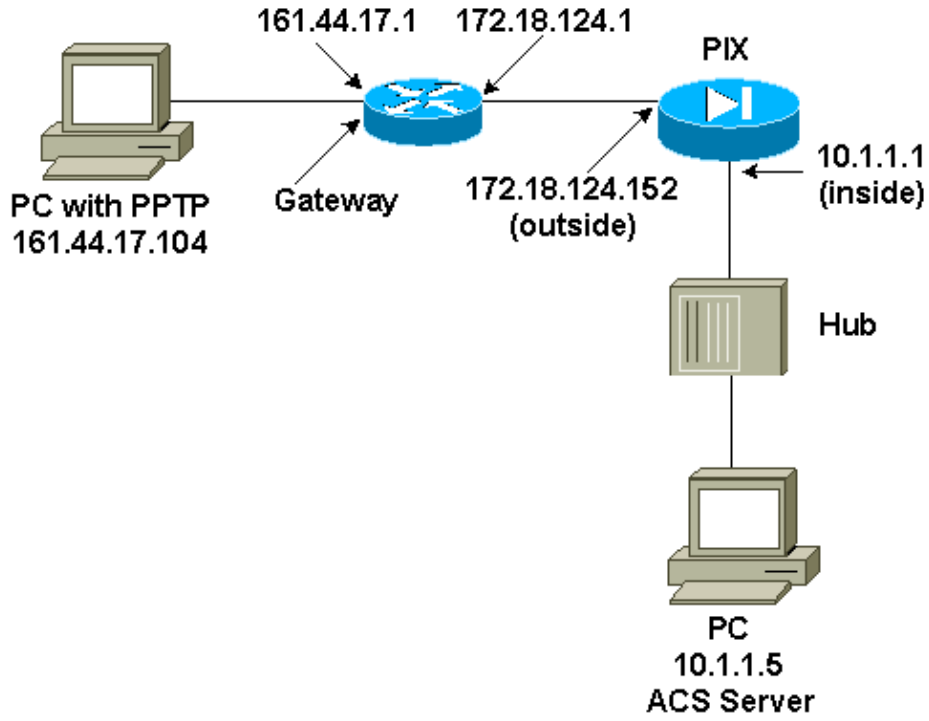
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup.



Configuration Tips for the PIX Firewall

Authentication Type − CHAP, PAP, MS−CHAP

The PIX configured for all three authentication methods (CHAP, PAP, MS−CHAP) at the same time provides the best chance to connect no matter how the PC is configured. This is a good idea for troubleshooting purposes.

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

Microsoft Point−to−Point Encryption (MPPE)

Use this command syntax in order to configure MPPE encryption on the PIX Firewall.

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

In this command, **required** is an optional keyword. MS−CHAP must be configured.

Configure the PPTP Feature on Client PCs

Note: The information available here on related to Microsoft software configuration does not come with any warranty or support for Microsoft software. Support for Microsoft software is available from Microsoft and at the Microsoft support web site .

Windows 98

Follow these steps in order to install the PPTP feature on Windows 98.

1. Select **Start > Settings > Control Panel > Add New Hardware**. Click **Next**.
2. Click **Select from List** and choose **Network Adapter**. Click **Next**.
3. Choose **Microsoft** in the left panel and **Microsoft VPN Adapter** on the right panel.

Follow these steps in order to configure the PPTP feature.

1. Select **Start > Programs > Accessories > Communications > Dial Up Networking**.
2. Click **Make new connection**. For **Select a device**, connect using **Microsoft VPN Adapter**. The VPN Server IP address is the PIX tunnel endpoint.
3. The Windows 98 default authentication uses password encryption (CHAP or MS−CHAP). In order to change the PC to also allow PAP, select **Properties > Server types**. Uncheck **Require encrypted password**. You can configure data encryption (MPPE or no MPPE) in this area.

Windows 2000

Follow these steps in order to configure the PPTP feature on Windows 2000.

1. Select **Start > Programs > Accessories > Communications > Network & Dialup connections**.
2. Click **Make new connection**, then click **Next**.
3. Select **Connect to a private network through the Internet** and **Dial a connection prior** (or not if LAN). Click **Next**.
4. Enter the hostname or IP address of tunnel endpoint (PIX/router).
5. If you need to change the password type, select **Properties > Security for the connection > Advanced**. The default is MS−CHAP and MS−CHAP v2 (not CHAP or PAP). You can configure data encryption (MPPE or no MPPE) in this area.

Windows NT

Refer to Installing, Configuring, and Using PPTP with Microsoft Clients and Servers to set up NT clients for PPTP.

Configure the PIX

PIX Configuration − Local Authentication, No Encryption

```
PIX Version 6.2(1)
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 Configuration − Local Authentication With Encryption

If you add this command to the PIX Configuration − Local Authentication, No Encryption configuration, the PC and PIX autonegotiate 40−bit encryption or none (based on PC settings).

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

If the PIX has the 3DES feature enabled, the **show version** command displays this message.

- Versions 6.3 and later:

```
VPN−3DES−AES: Enabled
```

- Versions 6.2 and earlier:

```
VPN−3DES: Enabled
```

128−bit encryption is also possible. However, if one of these messages is displayed, then the PIX is not enabled for 128−bit encryption.

- Versions 6.3 and later:

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

- Versions 6.2 and earlier:

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

The syntax for the MPPE command is shown here.

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

The PC and the PIX must be configured for MS−CHAP authentication in conjunction with MPPE.

PIX Configuration − TACACS+/RADIUS Authentication without Encryption

```
PIX Version 6.2(1)
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]
```

PIX Configuration − RADIUS Authentication With Encryption

If RADIUS is used, and if the RADIUS server (vendor−specific attribute 26, Microsoft as vendor) supports MPPE keying, MPPE encryption can be added. TACACS+ authentication does not work with encryption because TACACS+ servers are not capable of returning special MPPE keys. Cisco Secure ACS for Windows 2.5 and later RADIUS does support MPPE (all RADIUS servers do not support MPPE).

With the assumption that RADIUS authentication works without encryption, add encryption by including this command in the previous configuration:

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

The PC and PIX autonegotiates 40−bit encryption or none (based on PC settings).

If the PIX has the 3DES feature enabled, the **show version** command displays this message.

```
VPN−3DES: Enabled
```

128−bit encryption is also possible. However, if this message is displayed, the PIX is not enabled for 128−bit encryption.

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

The syntax for the MPPE command is shown in this output.

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

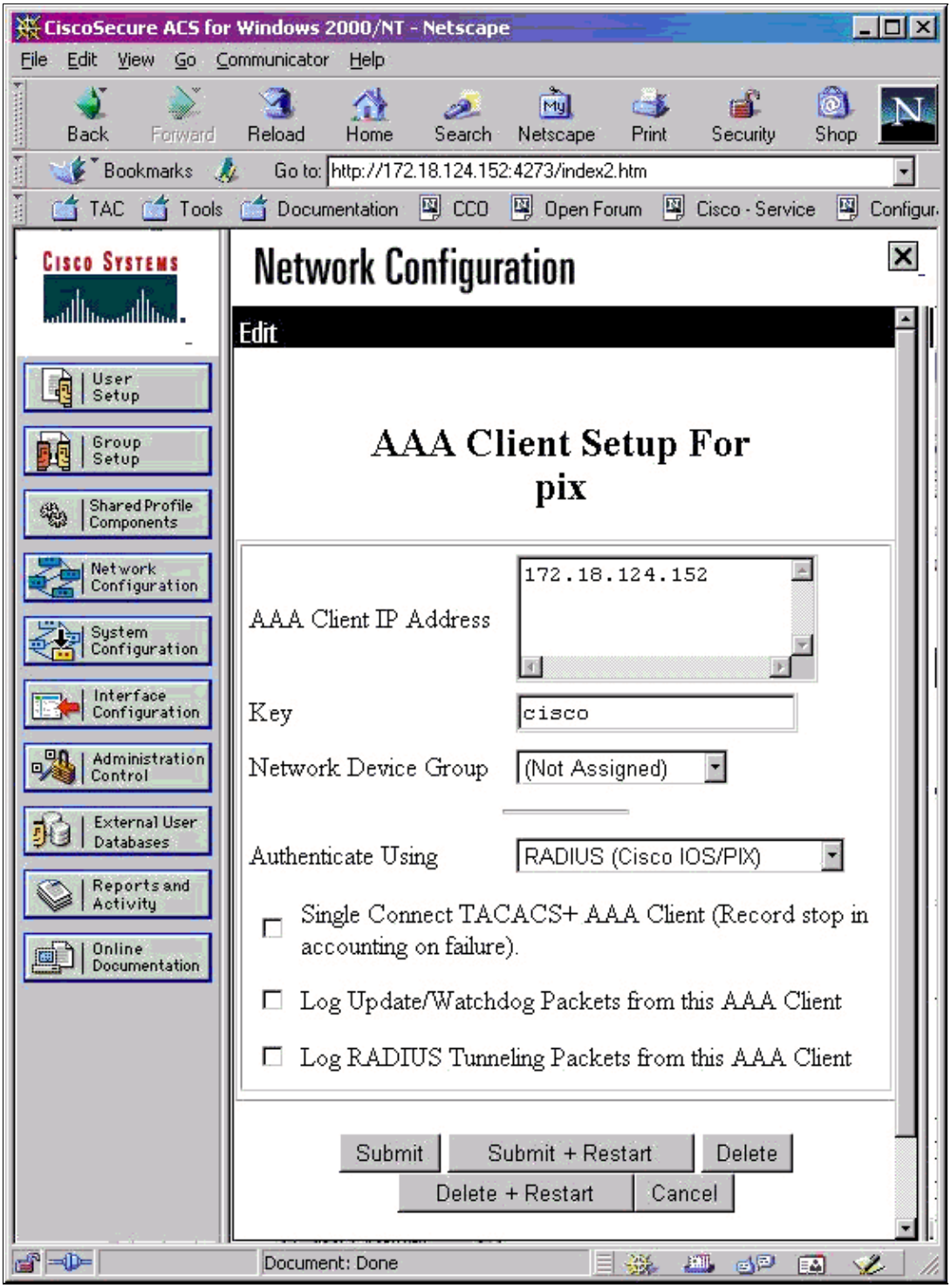
The PC and the PIX must be configured for MS−CHAP authentication in conjunction with MPPE.

Configure Cisco Secure ACS for Windows 3.0

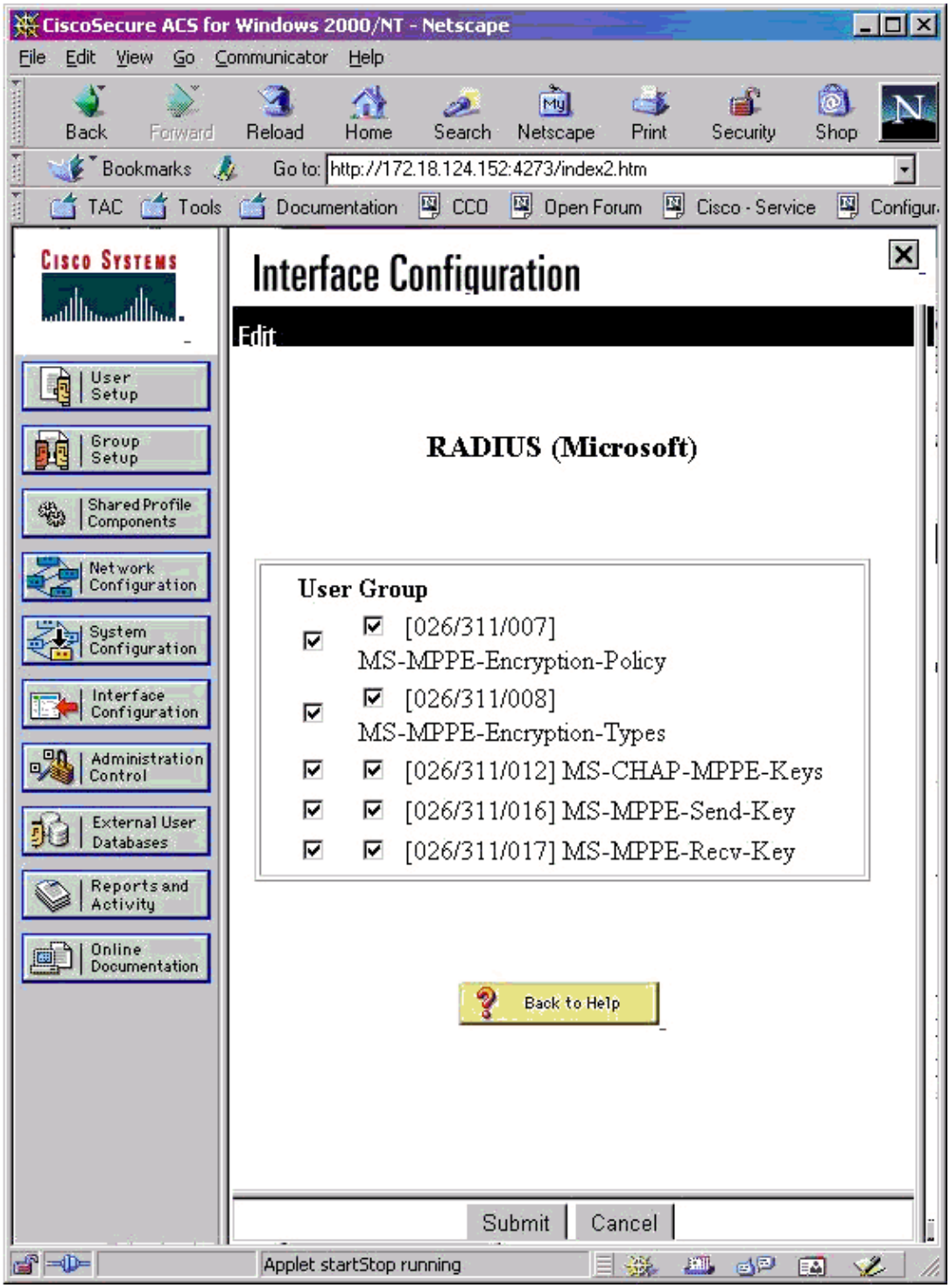
RADIUS Authentication With Encryption

Use these steps in order to configure Cisco Secure ACS for Windows 3.0. The same configuration steps apply to ACS versions 3.1 and 3.2.

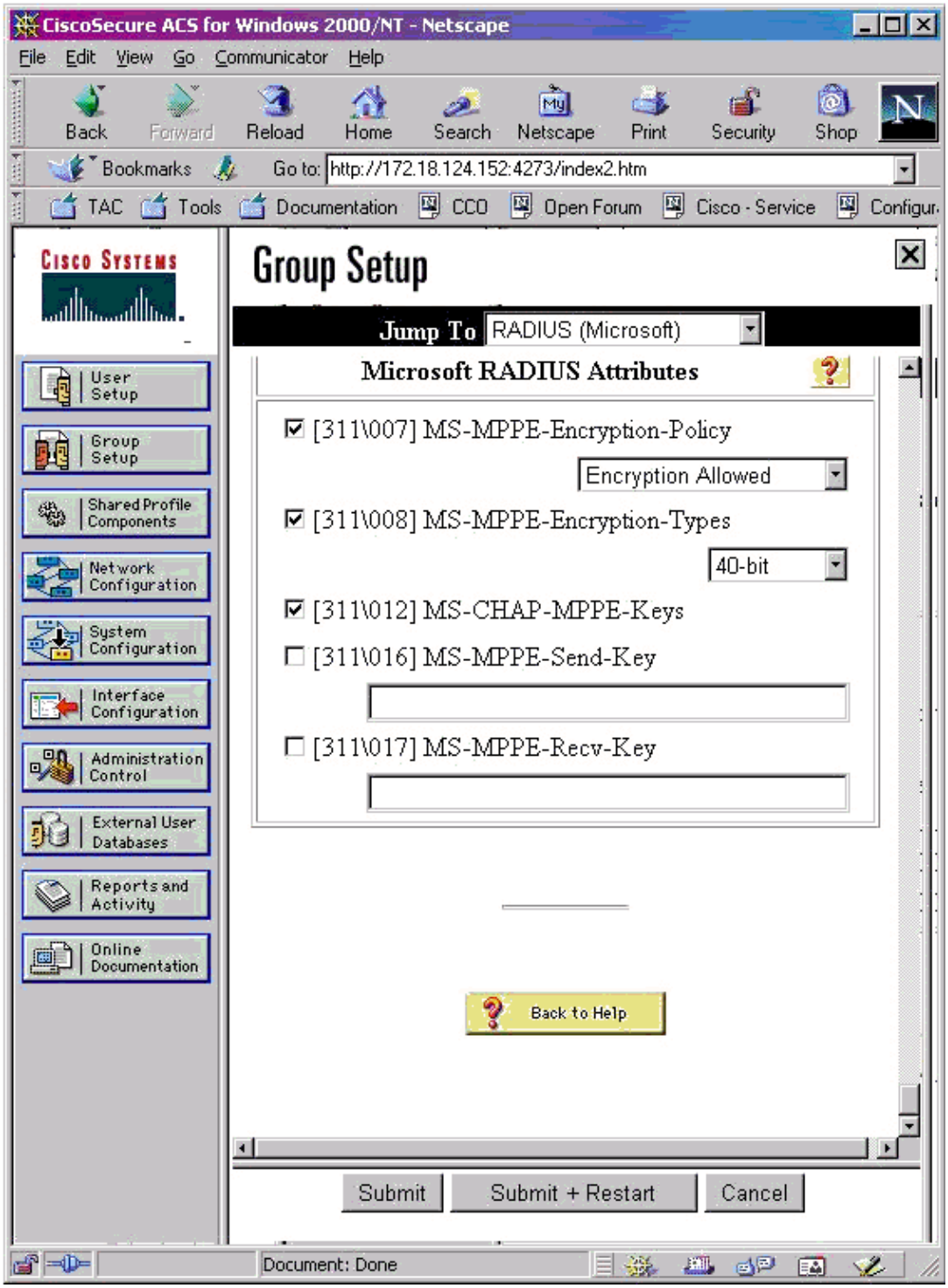
1. Add the PIX to the Cisco Secure ACS for Windows server **Network Configuration** and identify the dictionary−type as **RADIUS (Cisco IOS/PIX)**.



2. Open **Interface Configuration > RADIUS (Microsoft)** and check the MPPE attributes in order to make them appear in the group interface.



3. Add a user. In the user's group, add MPPE [RADIUS (Microsoft)] attributes. You must enable these attributes for encryption and it is optional when the PIX is not configured for encryption.



Verify

This section provides information you can use to confirm your configuration works properly.

PIX (Post Authentication) show commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

The **show vpdn** command lists tunnel and session information.

```
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 161.44.17.104, 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 161.44.17.104
  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
```

Client PC Verification

In an MS−DOS window, or from the Run window, type **ipconfig /all**. The PPP adapter portion shows this output.

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

You can also click **Details** in order to view information in the PPTP connection.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

- There must be connectivity for generic routing encapsulation (GRE) and TCP 1723 from the PC to the PIX tunnel endpoint. If there is any chance that this is blocked by a firewall or an access list, move the PC closer to the PIX.
- Windows 98 and Windows 2000 PPTP are easiest to set up. If in doubt, try multiple PCs and operating systems. After a successful connection, click **Details** on the PC in order to display information about the connection. For example, whether you use PAP, CHAP, IP, encryption, and so on.
- If you intend to use RADIUS and/or TACACS+, try to set up local (username and password on the PIX) authentication first. If this does not work, authenticating with a RADIUS or TACACS+ server does not work.
- Initially, make sure Security settings on the PC allow as many different authentication types as possible (PAP, CHAP, MS−CHAP) and uncheck the box for **Require data encryption** (make it optional both on the PIX and the PC).

- Since authentication type is negotiated, configure the PIX with the maximum number of possibilities. For example, if the PC is configured for only MS−CHAP and the router for only PAP, there is never any agreement.
- If the PIX acts as a PPTP server for two different locations and each location has its own RADIUS server on the inside, using a single PIX for both locations serviced by their own RADIUS server is not supported.
- Some RADIUS servers do not support MPPE. If a RADIUS server does not support MPPE keying, RADIUS authentication does work, but MPPE encryption does not work.
- With Windows 98 or later, when you use PAP or CHAP, the username sent to the PIX is identical to what is entered in the Dial−Up Networking (DUN) connection. But when you use MS−CHAP, the domain name can be appended to the front of the username, for example:

    - Username entered in DUN − "cisco"
    - Domain set on Windows 98 box − "DOMAIN"
    - MS−CHAP username sent to PIX − "DOMAIN\cisco"
    - Username on PIX − "cisco"
    - Result − Invalid username/password

  This is a section of the PPP log from a Windows 98 PC that shows the behavior.

```
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.
```

  If you use Windows 98 and MS−CHAP to the PIX, in addition to having the non−domain username, you can add "DOMAIN\username" to the PIX:

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

  Note: If you perform remote authentication on an AAA server, the same applies.

Troubleshooting Commands

Information on the sequence of expected sequence of PPTP events is found in the PPTP RFC 2637 . On the PIX, significant events in a good PPTP sequence show:

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

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

PIX debug Commands

- **debug ppp io** Displays the packet information for the PPTP PPP virtual interface.
- **debug ppp error** Displays protocol errors and error statistics associated with PPP connection negotiation and operation.

- **debug vpdn error** Displays errors that prevent a PPP tunnel from being established or errors that cause an established tunnel to be closed.
- **debug vpdn packet** Displays L2TP errors and events that are a part of normal tunnel establishment or shutdown for VPDNs.
- **debug vpdn events** Displays messages about events that are part of normal PPP tunnel establishment or shutdown.
- **debug ppp uauth** Displays the PPTP PPP virtual interface AAA user authentication debugging messages.

PIX clear Commands

This command must be issued in config mode.

- **clear vpdn tunnel [all | *[id tunnel_id]*]** Removes one or more PPTP tunnels from the configuration.

Caution: Do *not* issue the **clear vpdn** command. This wipes out *all* of the vpdn commands.

Enable PPP Logging on the Client PC

Complete these instructions in order to turn on PPP debugging for various Windows and Microsoft operating systems.

Windows 95

Follow these steps in order to enable PPP logging on a Windows 95 machine.

1. In the Network option in Control Panel, double−click **Microsoft Dial−Up Adapter** in the list of installed network components.
2. Click the **Advanced** tab. In the Property list, click the option named **Record A Log File**, and in the Value list, click **Yes**. Then click **OK**.
3. Shut down and restart the computer for this option to take effect. The log is saved in a file called ppplog.txt.

Windows 98

Follow these steps in order to enable PPP logging on a Windows 98 machine.

1. In **Dial−Up Networking**, single−click a connection icon, and then select **File > Properties**.
2. Click the Server Types tab.
3. Select the option named **Record a log file for this connection**. The log file is located at C:\Windows\ppplog.txt

Windows 2000

In order to enable PPP logging on a Windows 2000 machine, go to the Microsoft Support Page and search for "Enable PPP Logging in Windows."

Windows NT

Follow these steps in order to enable PPP Logging on an NT system.

1. Locate the key **SYSTEM\CurrentControlSet\Services\RasMan\PPP** and change **Logging** from 0 to **1**. This creates a file called PPP.LOG in the <winnt root>\SYSTEM32\RAS directory.
2. In order to debug a PPP session, first enable logging and then initiate the PPP connection. When the connection fails or exits, examine PPP.LOG to see what happened.

For more information, refer to the Microsoft Support Page and search for "Enabling PPP Logging in Windows NT."

Additional Microsoft Issues

Several Microsoft−related issues to consider when troubleshooting PPTP are listed here. Detailed information is available from the Microsoft Knowledge Base at the links provided.

- How to Keep RAS Connections Active After Logging Off

  Windows Remote Access Service (RAS) connections are automatically disconnected when you log off from a RAS client. You can remain connected by enabling the KeepRasConnections registry key on the RAS client.
- User Is Not Alerted When Logging On With Cached Credentials

  If you log on to a domain from a Windows−based workstation or member server and the domain controller cannot be located, you do not receive an error message that indicates this issue. Instead, you are logged on to the local computer using cached credentials.
- How to Write an LMHOSTS File for Domain Validation and Other Name Resolution Issues

  If you experience name resolution issues on your TCP/IP network, you need to use Lmhosts files in order to resolve NetBIOS names. You must follow a specific procedure in order to create an Lmhosts file to use in name resolution and domain validation.

Sample Debug Output

PIX Debug − Local Authentication

This debug output shows significant events in *italics*.

```
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 009c00011a2b3c4d000100000100000000000010000...
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: 3081880b00170000000000100000001ff03c0210101...
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: 3081880b001100000000000200000001ff03c0210401...
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: 3081880b001200000000000300000003ff03c0210202...
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: 3081880b000f000000000004000000003c2230101000d...
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: 3081880b00060000000000005000000004c22303010004
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: 3081880b000c000000000006000000580210101000a...
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: 3081880b00240000000000007000000058021040100 22...
```

```
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: 3081880b000600000000000800000000680fd01010004
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: 3081880b001100000000000900000000680fd0401000f...
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: 3081880b000600000000000a0000000980fd02020004
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: 3081880b000600000000000b0000000a80fd06030004
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: ff0380210402001c810600000000820600000000008306...

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: ff0300214500001cc800000008001e5ccac100101e000...
PPP IP Pkt: 4500001cc800000008001e5ccac100101e00000020a00...
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: ff03002145000060d000000008011116bac100101ac10...
PPP IP Pkt: 45000060d000000008011116bac100101ac10ffff0089...

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 Debug − RADIUS Authentication

This debug output shows significant events in *italics*.

```
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: 002000011a2b3c4d000800000009400001000000000fa...


PPTP: cc waiting for input, max soc FD = 1

outside PPTP: Recvd xGRE pak from 161.44.17.104,
   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 161.44.17.104, 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 161.44.17.104, Len 54,
   seq 2, ack 0,
   data: 3081880b00264000000000020000000ff03c0210400...
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 001800011a2b3c4d000f000000090000ffffffffffff...
Tnl/CL 9/9 PPTP: CC I SLI
PPTP: cc waiting for input, max soc FD = 1

outside PPTP: Recvd xGRE pak from 161.44.17.104,
   Len 39, seq 1, ack 1

PPP rcvd, ifc = 0, pppdev: 1, Len: 23,
    data: ff03c021020100130305c2238005065a899b2307020802

outside PPTP: Recvd xGRE pak from 161.44.17.104,
   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 161.44.17.104, Len 34,
   seq 3, ack 2,
   data: 3081880b00124000000000300000002ff03c0210201...
PPP xmit, ifc = 0, Len: 17
   data: ff03c2230101000d08f3686cc47e37ce67

Interface outside − PPTP xGRE: Out paket, PPP Len 15

outside PPTP: Sending xGRE pak to 161.44.17.104, Len 31,
   seq 4, ack 2,
   data: 3081880b000f400000000004000000002c2230101000d...
outside PPTP: Recvd xGRE pak from 161.44.17.104,
   Len 36, seq 3, ack 3

PPP rcvd, ifc = 0, pppdev: 1, Len: 22,
    data: ff03c0210c020012447e217e4d5352415356352e3030

outside PPTP: Recvd xGRE pak from 161.44.17.104,
   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 001800011a2b3c4d000f00000090000000000000000...
Tnl/CL 9/9 PPTP: CC I SLI
PPTP: cc waiting for input, max soc FD = 1

outside PPTP: Recvd xGRE pak from 161.44.17.104,
   Len 76, seq 5, ack 4

PPP rcvd, ifc = 0, pppdev: 1, Len: 62,
    data: ff03c2230201003a3100000000000000000000000000...

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 161.44.17.104,
   Len 22, seq 5, ack 5,
   data: 3081880b000640000000000500000005c22303010004
CHAP peer authentication succeeded for john

outside PPTP: Recvd xGRE pak from 161.44.17.104,
   Len 72, seq 6

PPP rcvd, ifc = 0, pppdev: 1, Len: 62,
    data: ff03c2230201003a3100000000000000000000000000...

PPP xmit, ifc = 0, Len: 8 data: ff03c22303010004

Interface outside − PPTP xGRE: Out paket, PPP Len 6

outside PPTP: Sending xGRE pak to 161.44.17.104, Len 22,
   seq 6, ack 6,
   data: 3081880b000640000000000600000006c22303010004
outside PPTP: Recvd xGRE pak from 161.44.17.104,
   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 161.44.17.104, Len 28,
   seq 7, ack 7,
   data: 3081880b000c400000000007000000780fd0101000a...
PPP xmit, ifc = 0, Len: 14
   data: ff0380fd0304000a120601000020

Interface outside − PPTP xGRE: Out paket, PPP Len 12


outside PPTP: Sending xGRE pak to 161.44.17.104, Len 28,
   seq 8, ack 7,
   data: 3081880b000c400000000080000000780fd0304000a...
outside PPTP: Recvd xGRE pak from 161.44.17.104,
   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 161.44.17.104, Len 28,
   seq 9, ack 8,
   data: 3081880b000c400000000090000000880210101000a...
PPP xmit, ifc = 0, Len: 32
   data: ff0380210405001c8106000000008206000000008306..
.
```

```
Interface outside − PPTP xGRE: Out paket, PPP Len 30

outside PPTP: Sending xGRE pak to 161.44.17.104,
   Len 46, seq 10, ack 8,
   data: 3081880b001e40000000000a00000080210405001c...
outside PPTP: Recvd xGRE pak from 161.44.17.104,
   Len 28, seq 9, ack 7

PPP rcvd, ifc = 0, pppdev: 1, Len: 14,
   data: ff0380fd0201000a120601000020

outside PPTP: Recvd xGRE pak from 161.44.17.104,
   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 161.44.17.104, Len 28,
   seq 11, ack 10,
   data: 3081880b000c40000000000b0000000a80fd0206000a...
outside PPTP: Recvd xGRE pak from 161.44.17.104,
   Len 28, seq 11, ack 9

PPP rcvd, ifc = 0, pppdev: 1, Len: 14,
   data: ff0380210201000a0306ac127c98

outside PPTP: Recvd xGRE pak from 161.44.17.104,
   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 161.44.17.104,
   Len 28, seq 12, ack 12,
   data: 3081880b000c40000000000c0000000c80210307000a...
outside PPTP: Recvd xGRE pak from 161.44.17.104,
   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 161.44.17.104, Len 28,
   seq 13, ack 13,
   data: 3081880b000c40000000000d0000000d80210308000a... 0
outside PPTP: Recvd xGRE pak from 161.44.17.104,
   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 161.44.17.104, 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 161.44.17.104,
   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 161.44.17.104
   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 161.44.17.104,
   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 161.44.17.104,
   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 161.44.17.104,
   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 161.44.17.104,
   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 161.44.17.104,
   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 161.44.17.104,
   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 161.44.17.104,
   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 161.44.17.104,
   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 161.44.17.104,
   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 161.44.17.104,
   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 161.44.17.104,
   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 161.44.17.104,
   len 113, seq 27

PPP rcvd, ifc = 0, pppdev: 1, len: 104,
    data: ff0300fd900ceb5aaaecc832df3c12bc6c519c25b4db...
PPP Encr/Comp Pkt: 900ceb5aaaecc832df3c12bc6c519c25b4dba569d161...
PPP IP Pkt: 4500006002d2000080117612c0a80101ffffffff0089...

outside PPTP: Recvd xGRE pak from 161.44.17.104,
   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 161.44.17.104,
   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 161.44.17.104,
   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 161.44.17.104,
   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 161.44.17.104,
   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 161.44.17.104,
   len 345, seq 33

PPP rcvd, ifc = 0, pppdev: 1, len: 336,
    data: ff0300fd90127d7213f35cd1d82d8988e28e0930ecc1...
PPP Encr/Comp Pkt: 90127d7213f35cd1d82d8988e28e0930ecc1614a993f...
PPP IP Pkt: 4500014802df00008011751dc0a80101ffffffff0044...
```

What Can Go Wrong

PIX and PC Cannot Negotiate Authentication

The PC authentication protocols are set for ones the PIX is unable to do (Shiva Password Authentication Protocol (SPAP) and Microsoft CHAP Version 2 (MS−CHAP v.2) instead of version 1). The PC and PIX are unable to agree on authentication. The PC displays this message:

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

PIX and PC Cannot Negotiate Encryption

The PC is set for **Encrypted only** and the **vpdn group 1 ppp encrypt mppe 40 required** command is deleted from the PIX. The PC and PIX are unable to agree on encryption and the PC displays this message:

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

PIX and PC Cannot Negotiate Encryption

The PIX is set for **vpdn group 1 ppp encrypt mppe 40 required** and the PC for no encryption allowed. This does not produce any messages on the PC, but the session disconnects and the PIX debug shows this output:

```
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 161.44.17.104
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 = 161.44.17.104
```

PIX MPPE RADIUS Problem

The PIX is set for **vpdn group 1 ppp encrypt mppe 40 required** and the PC for encryption allowed with authentication to a RADIUS server does not return the MPPE key. The PC shows this message:

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

The PIX debug shows:

```
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 161.44.17.104
   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 = 161.44.17.104
```

The PC shows this message:

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

NetPro Discussion Forums − Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums − Featured Conversations for Security
Security: Intrusion Detection [Systems]

Security: AAA
Security: General
Security: Firewalling

Related Information

- **Cisco PIX Firewall Software**
- **Cisco Secure PIX Firewall Command References**
- **Security Product Field Notices (including PIX)**
- **PPTP Support Page**
- **RFC 2637: Point−to−Point Tunneling Protocol (PPTP)**
- **Requests for Comments (RFCs)**
- **Technical Support − Cisco Systems**

Updated: Jul 11, 2007 Document ID: 14096