PIX 6.x:使用Radius驗證的PPTP組態範例

目錄

簡介

點對點通道通訊協定(PPTP)是第2層通道通訊協定，允許遠端使用者端使用公用IP網路，以便與私人企業網路中的伺服器安全通訊。PPTP通過IP隧道。RFC 2637 中詳述PPTP。PIX軟體版本5.1中新增了PIX防火牆上的PPTP支援。PIX文檔提供了有關PPTP及其與PIX一起使用的詳細資訊。本文檔介紹如何配置PIX以將PPTP與本地、TACACS+和RADIUS身份驗證配合使用。本文還提供可用於幫助您解決常見問題的提示和示例。

本文檔介紹如何配置與PIX*的*PPTP連線。要配置PIX或ASA以允許PPTP *通過安全裝置*，請參閱允許PPTP/L2TP連線通過PIX。

請參閱[Cisco Secure PIX Firewall 6.x和Cisco VPN Client 3.5 for Windows with Microsoft Windows 2000 and 2003 IAS RADIUS Authentication](#)，以配置PIX防火牆和VPN Client以與Windows 2000和2003 Internet Authentication Service(IAS)RADIUS伺服器一起使用。

請參閱[使用適用於Windows RADIUS身份驗證的Cisco Secure ACS配置VPN 3000集中器和PPTP](#)，以在具有Cisco Secure ACS for Windows的VPN 3000集中器上配置PPTP以進行RADIUS身份驗證。

在允許使用者進入網路之前，請參閱[配置Cisco Secure ACS for Windows路由器PPTP身份驗證](#)，以設定與路由器的PC連線，該連線然後向Cisco Secure Access Control System(ACS)3.2 for Windows伺服器提供使用者身份驗證。

注意：在PPTP術語中，根據RFC，PPTP網路伺服器(PNS)是伺服器（在本例中為PIX或被叫），PPTP訪問集中器(PAC)是客戶端（PC或呼叫者）。

注意：PIX不支援PPTP客戶端的拆分隧道。

註：PIX 6.x需要MS-CHAP v1.0才能使PPTP正常工作。Windows Vista不支援MS-CHAP v1.0。因此PIX 6.x上的PPTP在Windows Vista下無法運行。PIX版本7.x及更高版本不支援PPTP。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco Secure PIX防火牆軟體版本6.3(3)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。
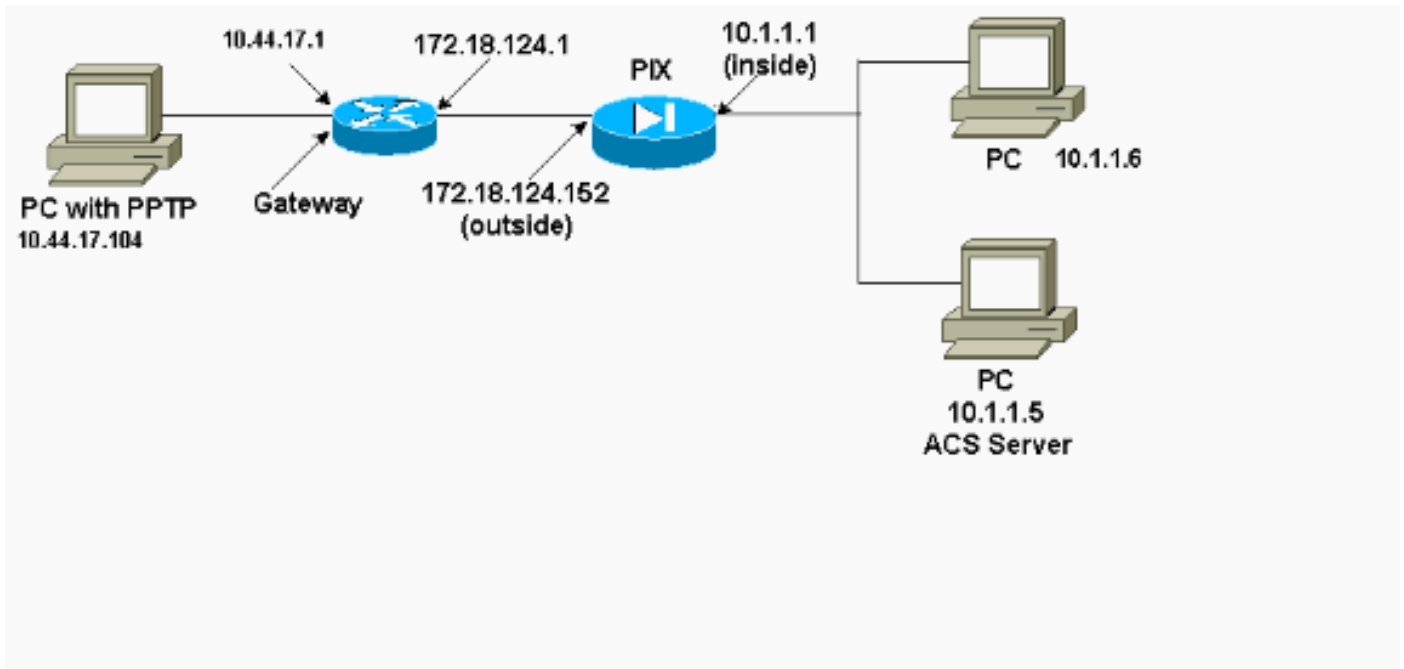
慣例

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。](#)

設定

本節提供用於設定本文件中所述功能的資訊。

註：使用[Command Lookup Tool](#)(僅[供](#)已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用此網路設定。

PIX防火牆配置提示

身份驗證型別 — CHAP、PAP、MS-CHAP

同時為所有三種身份驗證方法(CHAP、PAP、MS-CHAP)配置的PIX提供了最佳連線機會，無論PC是如何配置的。這是進行故障排除的好主意。

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

Microsoft點對點加密(MPPE)

使用以下命令語法在PIX防火牆上配置MPPE加密。

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

在此命令中，required是可選關鍵字。必須配置MS-CHAP。

在客戶端PC上配置PPTP功能

注意：此處提供的有關Microsoft軟體配置的資訊不附帶對Microsoft軟體的任何保修或支援。Microsoft和Microsoft支援網站提供對Microsoft軟體的支援 。

Windows 98

按照以下步驟在Windows 98上安裝PPTP功能。

1. 選擇**開始>設定>控制面板>新增新硬體**。按「**Next**」（下一步）。
2. 按一下**Select from List**，然後選擇**Network Adapter**。按「**Next**」（下一步）。
3. 在左側面板中選擇**Microsoft**，在右側面板中選擇**Microsoft VPN Adapter**。

請依照以下步驟操作，設定PPTP功能。

1. 選擇**Start > Programs > Accessories > Communications > Dial Up Networking**。
2. 按一下**Make new connection**。對於**選擇裝置**，請使用**Microsoft VPN介面卡連線**。VPN伺服器IP地址是PIX隧道端點。
3. Windows 98預設身份驗證使用密碼加密（CHAP或MS-CHAP）。 若要將PC更改為也允許PAP，請選擇**Properties > Server types**。取消選中**Require encrypted password**。您可以在此區域配置資料加密（MPPE或無MPPE）。

Windows 2000

按照以下步驟在Windows 2000上配置PPTP功能。

1. 選擇**Start > Programs > Accessories > Communications > Network & Dialup connections**。
2. 按一下**Make new connection**，然後按一下**Next**。
3. 選擇**Connect to a private network through the Internet**和**Dial a connection previous**（如果是LAN，則不選）。 按「**Next**」（下一步）。
4. 輸入隧道終端（PIX/路由器）的主機名或IP地址。
5. 如果需要更改密碼型別，請為連線選擇**Properties > Security > Advanced**。預設值為MS-CHAP和MS-CHAP v2（不是CHAP或PAP）。 您可以在此區域配置資料加密（MPPE或無MPPE）。

Windows NT

請參閱安裝、配置和使用PPTP與Microsoft客戶端和伺服器 ，為PPTP設定NT客戶端。

配置PIX

PIX配置 — 本地身份驗證，無加密

```
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 — 使用加密的本地身份驗證

如果將此命令新增到PIX配置 — 本地身份驗證、無加密配置，則PC和PIX自動協商40位加密或不協商（基於PC設定）。

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

如果PIX啟用了3DES功能，**show version**命令將顯示此消息。

- 6.3及更高版本：
  ```
  VPN-3DES-AES: Enabled
  ```
- 6.2及更低版本：
  ```
  VPN-3DES: Enabled
  ```

128位加密也是可能的。但是，如果顯示其中一條消息，則不會啟用PIX進行128位加密。

- 6.3及更高版本：
  ```
  Warning: VPN-3DES-AES license is required
  for 128 bits MPPE encryption
  ```
- 6.2及更低版本：
  ```
  Warning: VPN-3DES license is required
  for 128 bits MPPE encryption
  ```

MPPE命令的語法如下所示。

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

PC和PIX必須與MPPE一起配置用於MS-CHAP身份驗證。

PIX配置 — 無加密的TACACS+/RADIUS身份驗證

```
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]
```

PIX配置 — 使用加密的RADIUS身份驗證

如果使用RADIUS，且如果RADIUS伺服器（供應商特定屬性26,Microsoft作為供應商）支援MPPE金鑰，則可以新增MPPE加密。TACACS+驗證無法使用加密功能，因為TACACS+伺服器無法傳回特殊的MPPE金鑰。適用於Windows 2.5及更高版本的Cisco Secure ACS RADIUS不支援MPPE（所有RADIUS伺服器都不支援MPPE）。

假定RADIUS驗證可以在不加密的情況下工作，請通過在先前的設定中包含以下命令來新增加密：

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

PC和PIX自動協商40位加密或不加密（基於PC設定）。

如果PIX啟用了3DES功能，**show version**命令將顯示此消息。

```
VPN-3DES: Enabled
```
128位加密也是可能的。但是，如果顯示此消息，則不會為128位加密啟用PIX。

```
Warning: VPN-3DES license is required
for 128 bits MPPE encryption
```
MPPE命令的語法顯示在此輸出中。

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

PC和PIX必須與MPPE一起配置用於MS-CHAP身份驗證。

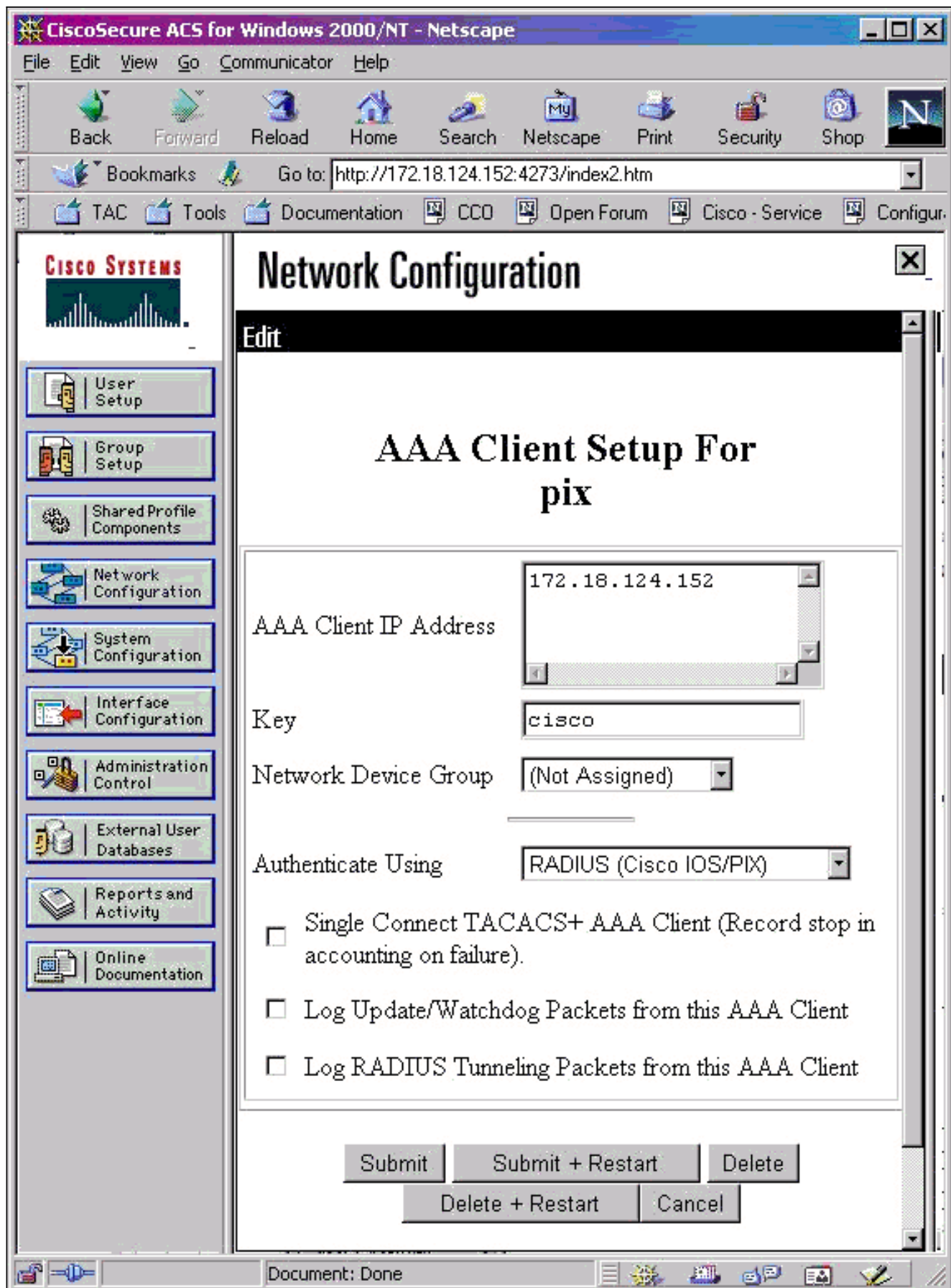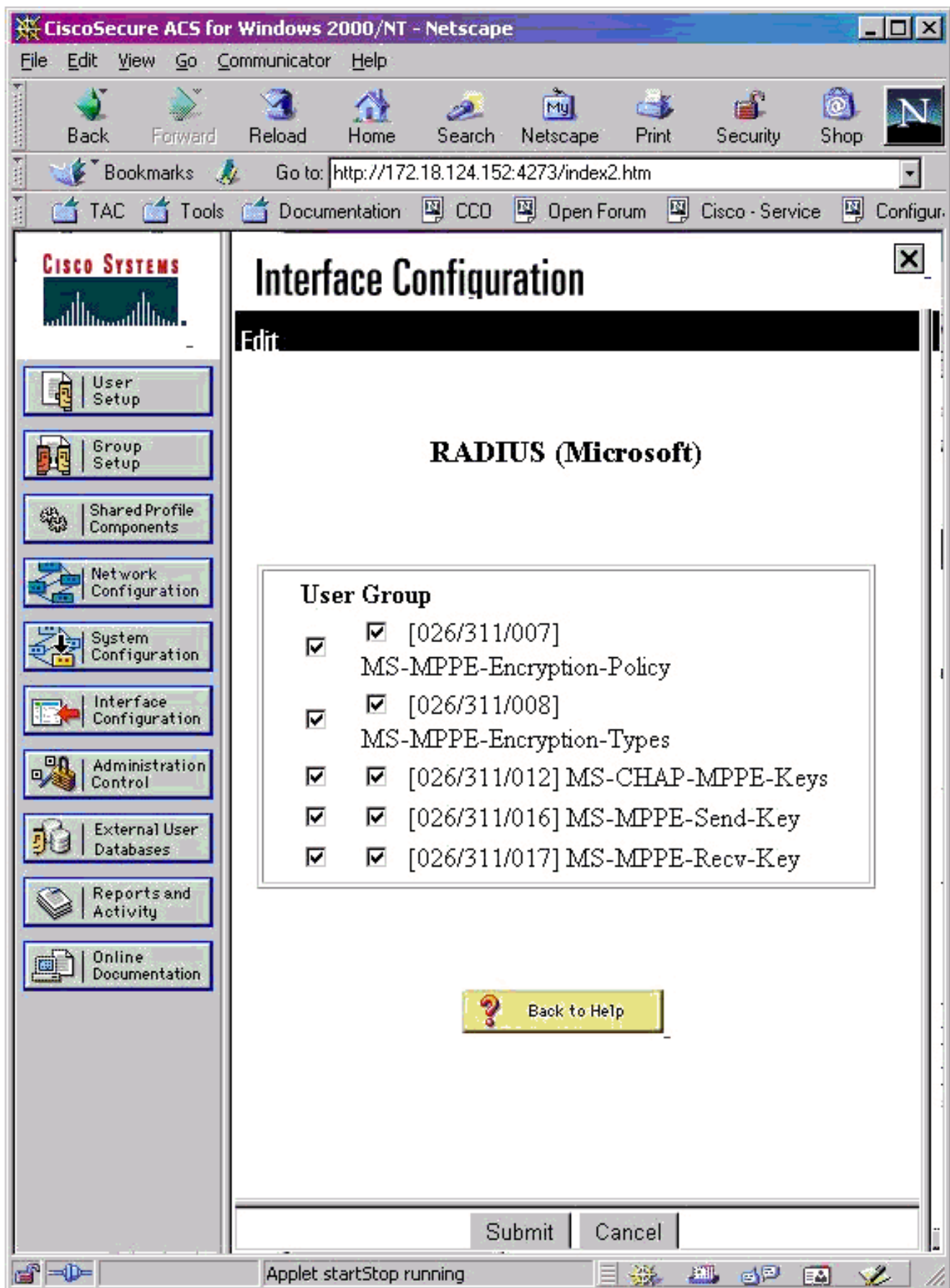# 配置適用於Windows 3.0的Cisco Secure ACS

使用加密的RADIUS驗證

使用以下步驟配置適用於Windows 3.0的Cisco Secure ACS。同樣的配置步驟適用於ACS 3.1和3.2版。

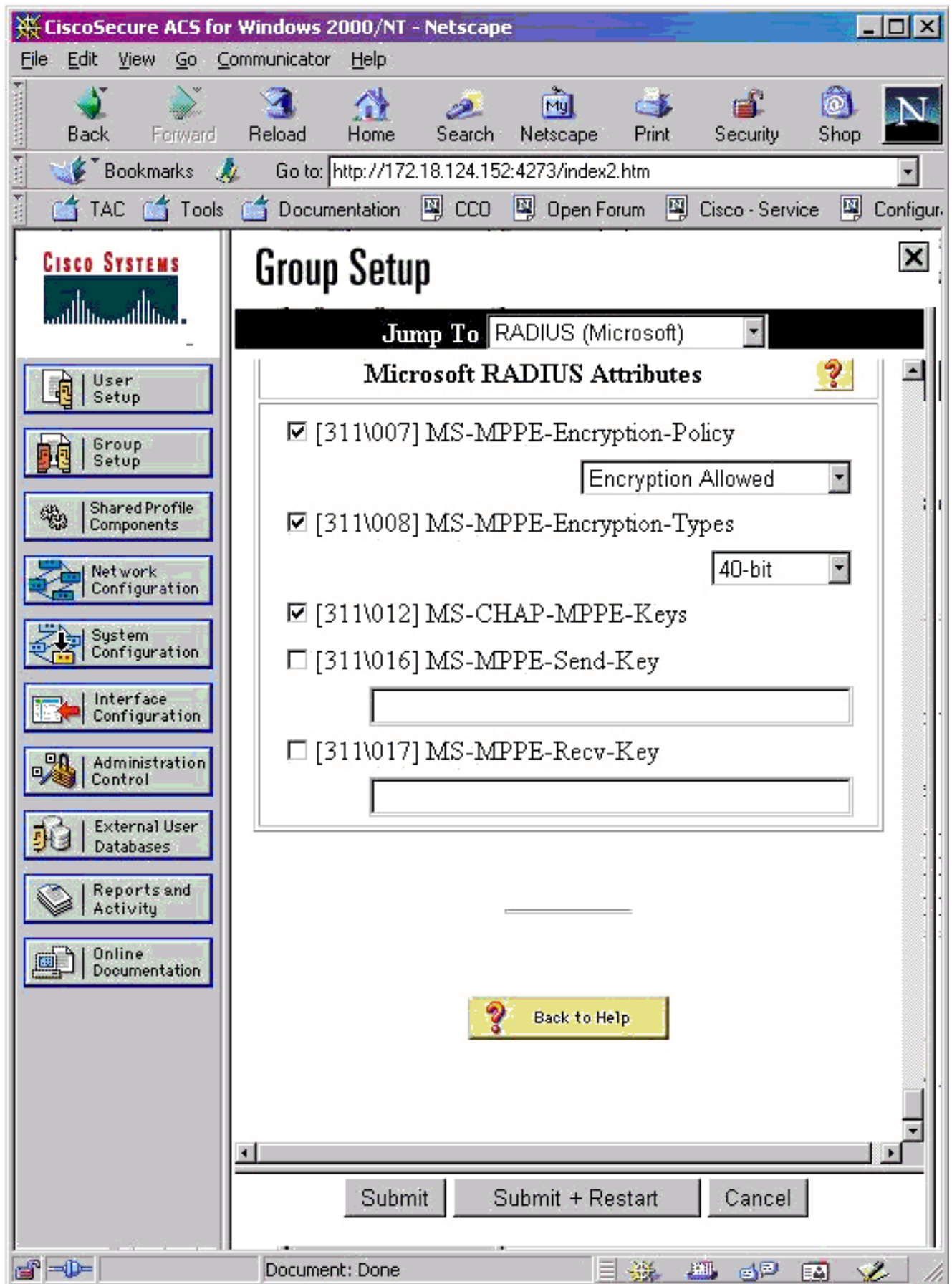1. 將PIX新增到Cisco Secure ACS for Windows server **Network Configuration**，並將字典型別標識為RADIUS(Cisco IOS/PIX)。

2. 開啟Interface Configuration > RADIUS(Microsoft)，然後檢查MPPE屬性，使其顯示在組介面中。

3. 新增使用者。在使用者組中，新增MPPE [RADIUS(Microsoft)]屬性。您必須啟用這些屬性進行加密，並且在PIX未配置為加密時它是可選的。

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

PIX（身份驗證後）show命令

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

show vpdn命令會列出通道和作業階段資訊。

```
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
```

客戶端PC驗證

在MS-DOS視窗中，或者從Run（運行）視窗中，鍵入ipconfig /all。PPP介面卡部分顯示此輸出。

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

也可以按一下Details以檢視PPTP連線中的資訊。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

- 必須存在從PC到PIX隧道端點的通用路由封裝(GRE)和TCP 1723連線。如果存在被防火牆或訪問清單阻止的可能性，請將PC移動到PIX附近。
- Windows 98和Windows 2000 PPTP最容易設定。如有疑問，請嘗試多台PC和作業系統。連線成功後，按一下PC上的Details以顯示有關連線的資訊。例如，您是否使用PAP、CHAP、IP、加密等。
- 如果您打算使用RADIUS和/或TACACS+，請嘗試首先設定本地（PIX上的使用者名稱和密碼）身份驗證。如果無法正常工作，則使用RADIUS或TACACS+伺服器進行身份驗證無效。

- 最初，確保PC上的安全設定允許儘可能多的不同身份驗證型別(PAP、CHAP、MS-CHAP)，並取消選中**Require data encryption**框（使其在PIX和PC上均可選）。
- 由於身份驗證型別是協商的，因此請配置PIX的最大可能數量。例如，如果PC僅配置為MS-CHAP，而路由器僅配置為PAP，則從來不會有任何協定。
- 如果PIX充當兩個不同位置的PPTP伺服器，並且每個位置在內部都有自己的RADIUS伺服器，則不支援對由其自己的RADIUS伺服器服務的兩個位置使用單個PIX。
- 某些RADIUS伺服器不支援MPPE。如果RADIUS伺服器不支援MPPE金鑰，RADIUS驗證會執行，但MPPE加密無法執行。
- 在Windows 98或更高版本中，當您使用PAP或CHAP時，傳送到PIX的使用者名稱與在撥號網路(DUN)連線中輸入的相同。但是使用MS-CHAP時，域名可以附加到使用者名稱的前面，例如：在DUN中輸入的使用者名稱 — "cisco"在Windows 98上設定的域 — 「域」傳送到PIX的MS-CHAP使用者名稱 — "DOMAIN\cisco"PIX上的使用者名稱 — "cisco"結果 — 無效的使用者名稱/密碼這是來自Windows 98 PC的PPP日誌中的一個部分，其中顯示了此行為。

```
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.
```

如果您在PIX中使用Windows 98和MS-CHAP，除了具有非域使用者名稱之外，還可以將「DOMAIN\username」新增到PIX：

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

注意：如果在AAA伺服器上執行遠端身份驗證，則同樣適用。

疑難排解指令

有關PPTP事件預期序列的資訊，請參閱PPTP RFC 2637 。在PIX上，良好的PPTP序列中的重要事件顯示：

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

附註：使用 debug 指令之前，請先參閱有關 Debug 指令的重要資訊。

PIX debug命令

- **debug ppp io** — 顯示PPTP PPP虛擬介面的資料包資訊。
- **debug ppp error** — 顯示與PPP連線協商和操作相關的協定錯誤和錯誤統計資訊。
- **debug vpdn error** — 顯示阻止PPP隧道建立的錯誤或導致已建立的隧道關閉的錯誤。
- **debug vpdn packet** — 顯示L2TP錯誤和事件，這些錯誤和事件是VPDN正常隧道建立或關閉的一部分。
- **debug vpdn events** — 顯示有關屬於正常PPP隧道建立或關閉部分的事件的消息。
- **debug ppp uauth** — 顯示PPTP PPP虛擬介面AAA使用者身份驗證調試消息。

必須在配置模式下發出此命令。

- clear vpdn tunnel [all | *[id tunnel_id]*] — 從配置中刪除一個或多個PPTP隧道。

注意：請*不要*發出**clear vpdn命令**。這會消*除*所有vpdn命令。

在客戶端PC上啟用PPP日誌記錄

完成以下說明以便為各種Windows和Microsoft作業系統啟用PPP調試。

Windows 95

要在Windows 95電腦上啟用PPP日誌記錄，請執行以下步驟。

1. 在「控制面板」中的「網路」選項中，按兩下已安裝網路元件清單中的**Microsoft撥號介面卡**。
2. 按一下**Advanced**頁籤。在「屬性」清單中，按一下名為**記錄日誌檔案**的選項，在「值」清單中，按一下**是**。然後按一下**OK**。
3. 關閉並重新啟動電腦以使此選項生效。日誌儲存在名為ppplog.txt的檔案中。

Windows 98

要在Windows 98電腦上啟用PPP日誌記錄，請執行以下步驟。

1. 在**撥號網路**中，按一下連線圖示，然後選擇**檔案>屬性**。
2. 按一下「伺服器型別」頁籤。
3. 選擇名為**記錄此連線的日誌檔案的選項**。日誌檔案位於C:\Windows\ppplog.txt

Windows 2000

要在Windows 2000電腦上啟用PPP日誌記錄，請轉到Microsoft支援頁面 ，並搜尋「在Windows中啟用PPP日誌記錄」。

Windows NT

按照以下步驟在NT系統上啟用PPP日誌記錄。

1. 找到金鑰SYSTEM\CurrentControlSet\Services\RasMan\PPP，將**Logging**從0更改為**1**。這樣會在<winnt root>\SYSTEM32\RAS目錄下建立一個名為PPP.LOG的檔案。
2. 要調試PPP會話，請先啟用日誌記錄，然後啟動PPP連線。當連線失敗或退出時，檢查PPP.LOG以檢視發生的情況。

有關詳細資訊，請參閱Microsoft支援頁面 ，並搜尋「在Windows NT中啟用PPP日誌記錄」。

其他Microsoft問題

此處列出了排除PPTP故障時要考慮的幾個與Microsoft相關的問題。有關詳細資訊，請訪問Microsoft知識庫提供的連結。

- [如何在註銷後保持RAS連線處於活動狀態](#)從RAS客戶端註銷時，Windows遠端訪問服務(RAS)連線將自動斷開。通過在RAS客戶端上啟用KeepRasConnections登錄檔項，可以保持連線。
- [使用快取憑據登入時不會提示使用者](#)如果您從基於Windows的工作站或成員伺服器登入到域，但找不到域控制器，則不會收到指示此問題的錯誤消息。而是使用快取的憑據登入到本地電腦。
- [如何針對域驗證和其他名稱解析問題編寫LMHOSTS檔案](#)如果您在TCP/IP網路上遇到名稱解析問題，則需要使用Lmhosts檔案來解析NetBIOS名稱。您必須按照特定的過程建立一個Lmhosts檔案，以用於名稱解析和域驗證。

調試輸出示例

PIX調試 — 本地身份驗證

此調試輸出以斜體顯示重要事件。

```
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: 009c00011a2b3c4d00020000010001000000000030000... 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: ff03c0210101001702060000a00005060011372107020702... PPP xmit, ifc = 0, Len: 23 data: ff03c0210101001303055c22380050609894ab407020802 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: 3081880b001700000000000100000001ff03c0210101... 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: ff03c0210201001303055c22380050609894ab407020802 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:
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: ff03802101010028020600240f010306000000008106... 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:
3081880b000c00000000000600000005802101010000a... 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:
3081880b002400000000000700000005802104010022... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 29, seq 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 19, data:
ff0380fd0101000f12060100000011105000104 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: 3081880b00060000000000080000000680fd01010004 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:
3081880b001100000000000900000006800fd0401000f... 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:
ff0380210102002203060000000081060000000008206... 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:
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:
ff03002145000060d2000000800110f6bac100101ac10... 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調試 — RADIUS身份驗證

此調試輸出以斜體顯示重要事件。

```
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:
3081880b00174000000000000100000000ff03c0210101... 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:
3081880b00264000000000000200000000ff03c0210400... 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 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:
3081880b00124000000000000300000002ff03c0210201... 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:
3081880b000f4000000000000400000002c2230101000d... 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
001800011a2b3c4d000f00000009000000000000000000... 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: 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 10.44.17.104, Len 22, seq 5, ack 5, data:
3081880b00064000000000000500000005c22303010004 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: ff03c2230201003a3100000000000000000000000000... 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: 3081880b00064000000000000600000006c22303010004
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:
3081880b000c4000000000000700000007 80fd0101000a... 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:
3081880b000c40000000000008000000078 0fd0304000a... outside PPTP: Recvd xGRE pak from 10.44.17.104,
Len 48, seq 8 PPP rcvd, ifc = 0, pppdev: 1, Len: 38, data:
ff03802101050022030600000000810600000000008206... 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:
3081880b000c40000000000009000000088 02101 01000a... 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:
3081880b001e40000000000a00000008802104 05001c... 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:
3081880b000c40000000000b0000000a8 0fd0206000a... 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:
4500014802cf000080117652dc0a80101ffffffff0044... 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...
```

可能出錯的地方

同時PPTP通道

您無法通過PIX 6.x連線超過127個連線，並且出現以下錯誤消息：

%PIX-3-213001:PPTP控制守護進程套接字io接受錯誤，錯誤號= 5

解決方案：

在PIX 6.x中，硬體限製為128個併發會話。如果為PPTP偵聽套接字減去一個，則最大連線數為
127。

PIX和PC無法協商身份驗證

PC身份驗證協定為PIX無法執行的協定設定(Shiva密碼身份驗證協定(SPAP)和Microsoft CHAP版本
2(MS-CHAP v.2)而不是版本1)。 PC和PIX無法就身份驗證達成一致。PC將顯示以下消息：

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

PIX和PC無法協商加密

PC設定為**Encrypted only**，並且**vpdn group 1 ppp encrypt mppe 40 required**命令從PIX中刪除。
PC和PIX無法就加密達成一致，PC將顯示以下消息：

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

PIX和PC無法協商加密

PIX設定為**vpdn group 1 ppp encrypt mppe 40 required**，而PC設定為不允許加密。這不會在PC上產生任何消息，但會話會斷開，PIX調試將顯示以下輸出：

```
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問題

PIX設定為**vpdn group 1 ppp encrypt mppe 40 required**,PC用於通過向RADIUS伺服器進行身份驗證的加密不會返回MPPE金鑰。PC顯示以下消息：

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

PIX調試顯示：

```
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顯示以下消息：

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

相關資訊

- Cisco PIX防火牆軟體
- Cisco Secure PIX防火牆命令參考
- 安全產品現場通知（包括PIX）
- 最常見的L2L和遠端訪問IPSec VPN故障排除解決方案

- [PPTP支援頁面](#)
- [RFC 2637:點對點通道通訊協定(PPTP)](#)
- [要求建議 (RFC)](#)
- [技術支援 - Cisco Systems](#)