PIX 6.x: PPTP mit Konfigurationsbeispiel für RADIUS-Authentifizierung

Inhalt

Einführung

Point-to-Point Tunneling Protocol (PPTP) ist ein Layer-2-Tunneling-Protokoll, das einem Remote-Client die Verwendung eines öffentlichen IP-Netzwerks ermöglicht, um sicher mit Servern in einem privaten Unternehmensnetzwerk zu kommunizieren. PPTP tunnelt die IP. PPTP wird in RFC 2637 beschrieben. PPTP-Unterstützung für die PIX-Firewall wurde in Version 5.1 der PIX-Software hinzugefügt. Die PIX-Dokumentation enthält weitere Informationen über PPTP und dessen Verwendung mit dem PIX. In diesem Dokument wird beschrieben, wie PIX für die Verwendung

von PPTP mit lokaler, TACACS+- und RADIUS-Authentifizierung konfiguriert wird. Dieses Dokument enthält auch Tipps und Beispiele, die Sie bei der Behebung gängiger Probleme verwenden können.

Dieses Dokument zeigt, wie PPTP-Verbindungen *zum* PIX konfiguriert werden. Informationen zum Konfigurieren eines PIX oder einer ASA, um PPTP *über* die Sicherheits-Appliance zuzulassen, finden Sie unter Zulassen von PPTP/L2TP-Verbindungen über das PIX.

Informationen zur Konfiguration der PIX-Firewall und des VPN-Clients für Windows mit Microsoft Windows 2000 und 2003 IAS RADIUS-Authentifizierung zur Verwendung mit dem RADIUS-Server Windows 2000 und 2003 finden Sie unter Cisco Secure PIX Firewall 6.x und Cisco VPN Client 3.5.

Informationen zur Konfiguration von PPTP auf einem VPN 3000-Konzentrator mit Cisco Secure ACS für Windows RADIUS-Authentifizierung finden Sie unter Konfigurieren des VPN 3000-Concentrators mit Cisco Secure ACS für Windows für die RADIUS-Authentifizierung.

Unter Konfigurieren von Cisco Secure ACS für die PPTP-Authentifizierung des Windows-Routers finden Sie Informationen zum Einrichten einer PC-Verbindung mit dem Router. Diese Verbindung ermöglicht dann die Benutzerauthentifizierung des Cisco Secure Access Control System (ACS) 3.2 für Windows-Server, bevor Sie den Benutzer in das Netzwerk zulassen.

Hinweis: In PPTP-Hinsicht ist der PPTP-Netzwerkserver (PNS) laut RFC der Server (in diesem Fall der PIX oder der Angerufene), und der PPTP-Zugriffs-Konzentrator (PAC) ist der Client (der PC oder der Anrufer).

Hinweis: Split-Tunneling wird auf PIX für PPTP-Clients nicht unterstützt.

Hinweis: Für PIX 6.x ist MS-CHAP v1.0 erforderlich, damit PPTP funktioniert. Windows Vista unterstützt MS-CHAP v1.0 nicht. PPTP auf PIX 6.x funktioniert also nicht für Windows Vista. PPTP wird in PIX, Version 7.x und höher, nicht unterstützt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Secure PIX Firewall Software, Version 6.3(3).

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

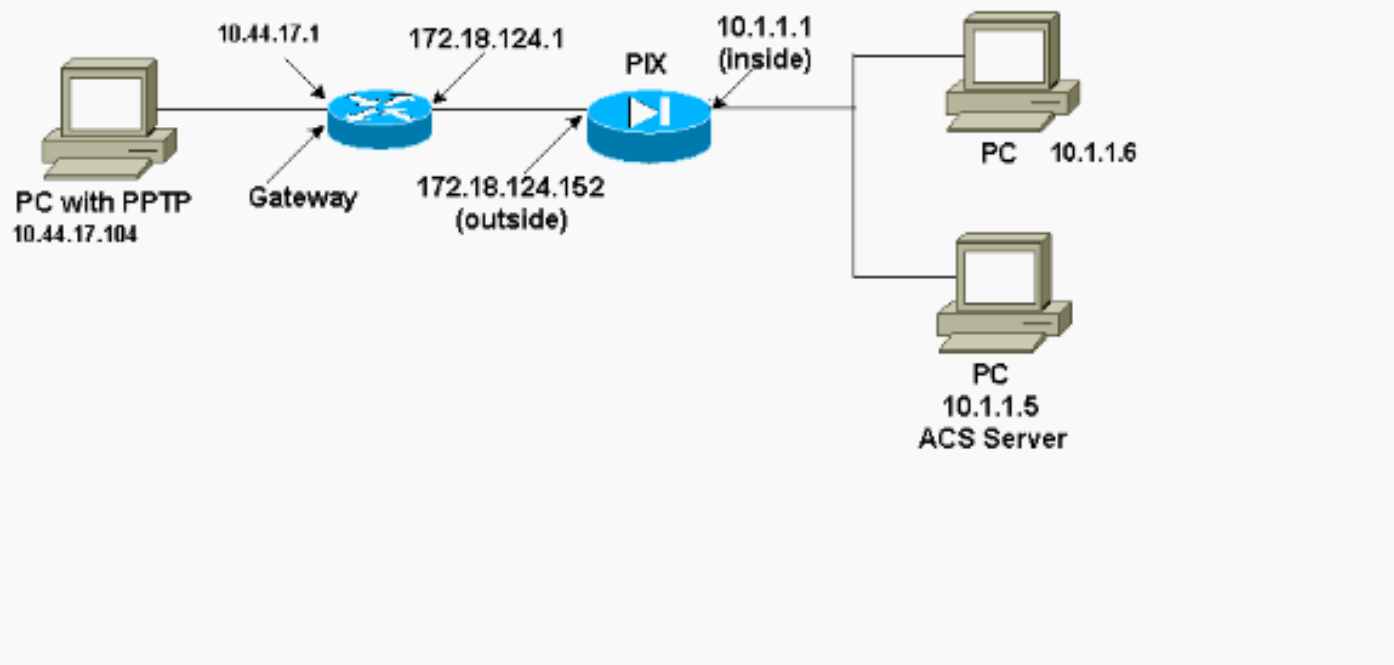
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird diese Netzwerkeinrichtung verwendet.



Konfigurationstipps für die PIX-Firewall

Authentifizierungstyp - CHAP, PAP, MS-CHAP

Das PIX, das für alle drei Authentifizierungsmethoden (CHAP, PAP, MS-CHAP) gleichzeitig konfiguriert ist, bietet die beste Möglichkeit, eine Verbindung herzustellen, unabhängig davon, wie der PC konfiguriert ist. Dies ist eine gute Idee für die Fehlerbehebung.

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

Microsoft Point-to-Point Encryption (MPPE)

Verwenden Sie diese Befehlssyntax, um die MPPE-Verschlüsselung auf der PIX-Firewall zu konfigurieren.

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

In diesem Befehl ist ein optionales Schlüsselwort **erforderlich**. MS-CHAP muss konfiguriert werden.

Konfigurieren der PPTP-Funktion auf Client-PCs

Hinweis: Die hier verfügbaren Informationen zur Microsoft-Softwarekonfiguration enthalten keine Garantie oder Unterstützung für Microsoft-Software. Der Support für Microsoft-Software ist von Microsoft und auf der Microsoft-Support-Website verfügbar.

Windows 98

Befolgen Sie diese Schritte, um die PPTP-Funktion unter Windows 98 zu installieren.

1. Wählen Sie **Start > Einstellungen > Systemsteuerung > Neue Hardware hinzufügen aus**. Klicken Sie auf **Weiter**.
2. Klicken Sie auf **Aus Liste auswählen** und wählen Sie **Netzwerkadapter aus**. Klicken Sie auf **Weiter**.
3. Wählen Sie **Microsoft** im linken Bereich und **Microsoft VPN Adapter** im rechten Bereich aus.

Befolgen Sie diese Schritte, um die PPTP-Funktion zu konfigurieren.

1. Wählen Sie **Start > Programme > Zubehör > Kommunikation > DFÜ-Netzwerk aus**.
2. Klicken Sie auf **Neue Verbindung herstellen**. Um **ein Gerät auszuwählen**, stellen Sie eine Verbindung mit dem **Microsoft VPN-Adapter her**. Die IP-Adresse des VPN-Servers ist der PIX-Tunnel-Endpunkt.
3. Die Windows 98-Standardauthentifizierung verwendet Kennwortverschlüsselung (CHAP oder MS-CHAP). Um den PC so zu ändern, dass er auch PAP zulässt, wählen Sie **Eigenschaften > Servertypen aus**. Deaktivieren Sie **Verschlüsseltes Kennwort erforderlich**. In diesem Bereich können Sie die Datenverschlüsselung (MPPE oder kein MPPE) konfigurieren.

Windows 2000

Führen Sie diese Schritte aus, um die PPTP-Funktion unter Windows 2000 zu konfigurieren.

1. Wählen Sie **Start > Programme > Zubehör > Kommunikation > Netzwerk- und DFÜ-Verbindungen aus**.
2. Klicken Sie auf **Neue Verbindung herstellen** und dann auf **Weiter**.
3. Wählen Sie **Verbinden mit einem privaten Netzwerk über das Internet** und **Wählen Sie eine Verbindung vorher** (oder nicht, wenn LAN). Klicken Sie auf **Weiter**.
4. Geben Sie den Hostnamen oder die IP-Adresse des Tunnelendpunkts (PIX/Router) ein.
5. Wenn Sie den Kennworttyp ändern müssen, wählen Sie **Eigenschaften > Sicherheit für die Verbindung > Erweitert aus**. Der Standardwert ist MS-CHAP und MS-CHAP v2 (nicht CHAP oder PAP). In diesem Bereich können Sie die Datenverschlüsselung (MPPE oder kein MPPE) konfigurieren.

Windows NT

Informationen zum Einrichten von NT-Clients für PPTP finden Sie unter Installieren, Konfigurieren und Verwenden von PPTP mit Microsoft-Clients und -Servern .

Konfigurieren des PIX

PIX-Konfiguration - Lokale Authentifizierung, keine Verschlüsselung

```
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-Konfiguration - Lokale Authentifizierung mit Verschlüsselung

Wenn Sie diesen Befehl zur PIX-Konfiguration - Lokale Authentifizierung, Konfiguration ohne Verschlüsselung hinzufügen, verhandeln der PC und PIX automatisch eine 40-Bit-Verschlüsselung oder keine Verschlüsselung (basierend auf PC-Einstellungen).

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

Wenn die 3DES-Funktion auf dem PIX aktiviert ist, wird diese Meldung über den Befehl **show version** angezeigt.

- Versionen 6.3 und höher:
  `VPN-3DES-AES: Enabled`
- Versionen 6.2 und frühere Versionen:
  `VPN-3DES: Enabled`

Eine 128-Bit-Verschlüsselung ist ebenfalls möglich. Wenn jedoch eine dieser Meldungen angezeigt wird, ist PIX nicht für die 128-Bit-Verschlüsselung aktiviert.

- Versionen 6.3 und höher:
  ```
  Warning: VPN-3DES-AES license is required
  for 128 bits MPPE encryption
  ```
- Versionen 6.2 und frühere Versionen:
  ```
  Warning: VPN-3DES license is required
  for 128 bits MPPE encryption
  ```

Die Syntax für den MPPE-Befehl wird hier angezeigt.

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

PC und PIX müssen für die MS-CHAP-Authentifizierung in Verbindung mit MPPE konfiguriert werden.

PIX-Konfiguration - TACACS+/RADIUS-Authentifizierung ohne Verschlüsselung

```
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-Konfiguration - RADIUS-Authentifizierung mit Verschlüsselung

Wenn RADIUS verwendet wird und der RADIUS-Server (anbieterspezifisches Attribut 26, Microsoft als Anbieter) MPPE-Keying unterstützt, kann die MPPE-Verschlüsselung hinzugefügt werden. Die TACACS+-Authentifizierung funktioniert nicht mit der Verschlüsselung, da TACACS+-Server keine speziellen MPPE-Schlüssel zurückgeben können. Cisco Secure ACS für Windows 2.5 und höher RADIUS unterstützt MPPE (alle RADIUS-Server unterstützen MPPE nicht).

Unter der Annahme, dass die RADIUS-Authentifizierung ohne Verschlüsselung funktioniert, fügen Sie die Verschlüsselung hinzu, indem Sie diesen Befehl in die vorherige Konfiguration einfügen:

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

PC und PIX verhandeln entweder eine 40-Bit-Verschlüsselung oder keine Verschlüsselung (basierend auf den PC-Einstellungen).

Wenn die 3DES-Funktion auf dem PIX aktiviert ist, wird diese Meldung über den Befehl **show version** angezeigt.

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

Eine 128-Bit-Verschlüsselung ist ebenfalls möglich. Wenn diese Meldung angezeigt wird, ist PIX jedoch nicht für die 128-Bit-Verschlüsselung aktiviert.

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

Die Syntax für den MPPE-Befehl wird in dieser Ausgabe angezeigt.

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

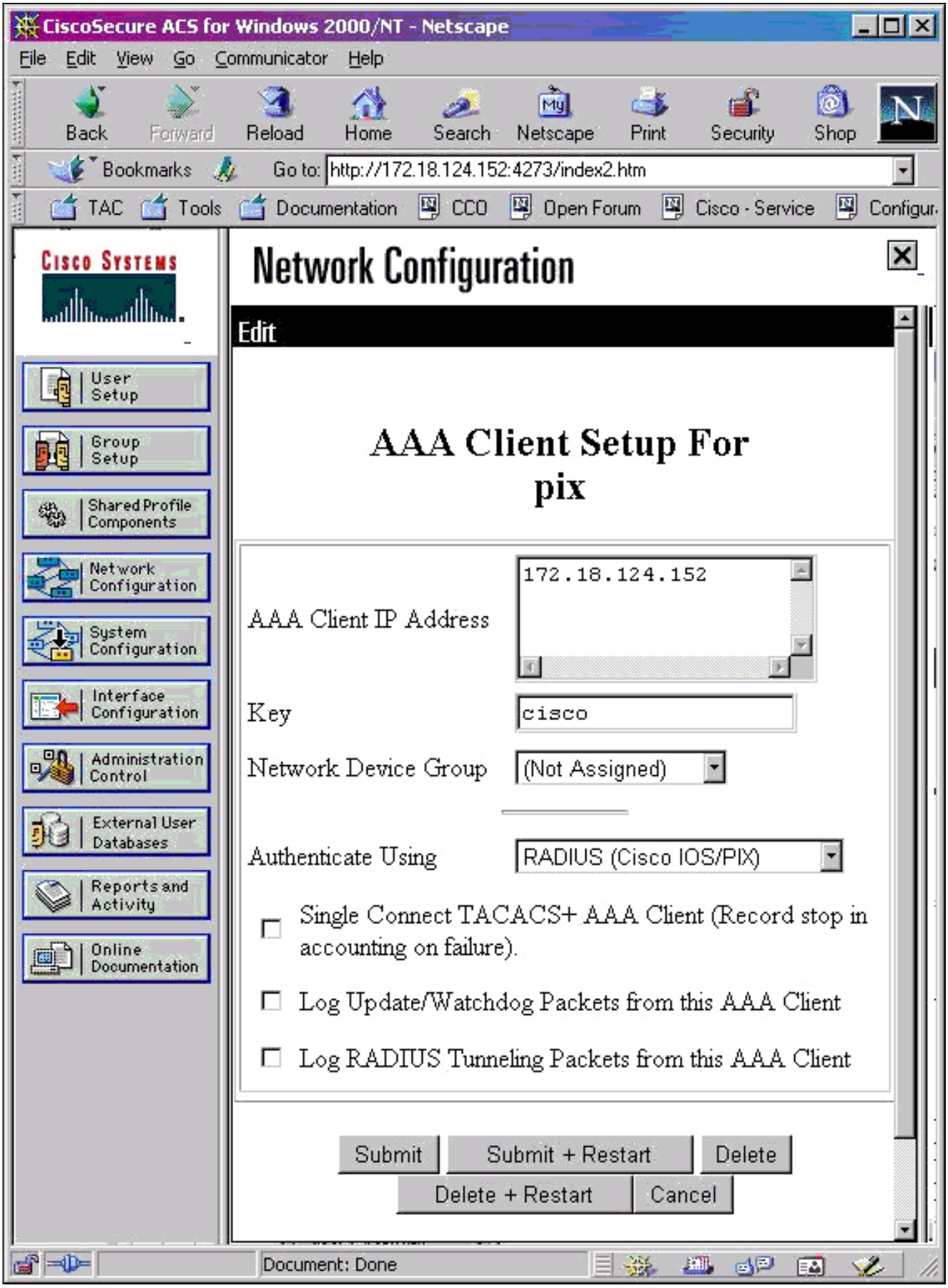
PC und PIX müssen für die MS-CHAP-Authentifizierung in Verbindung mit MPPE konfiguriert werden.

Konfigurieren von Cisco Secure ACS für Windows 3.0

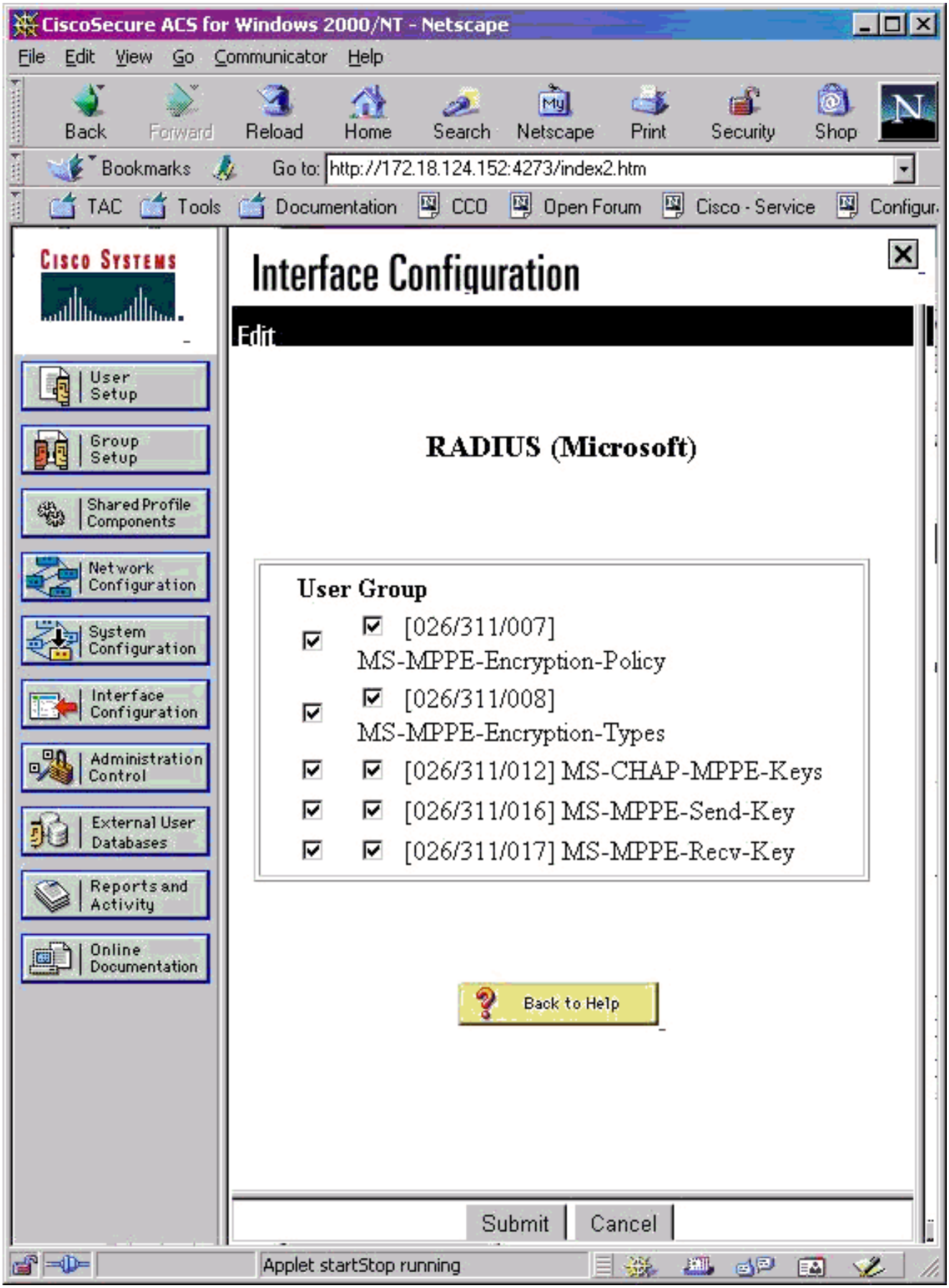
RADIUS-Authentifizierung mit Verschlüsselung

Führen Sie diese Schritte aus, um Cisco Secure ACS für Windows 3.0 zu konfigurieren. Die gleichen Konfigurationsschritte gelten für ACS 3.1 und 3.2.

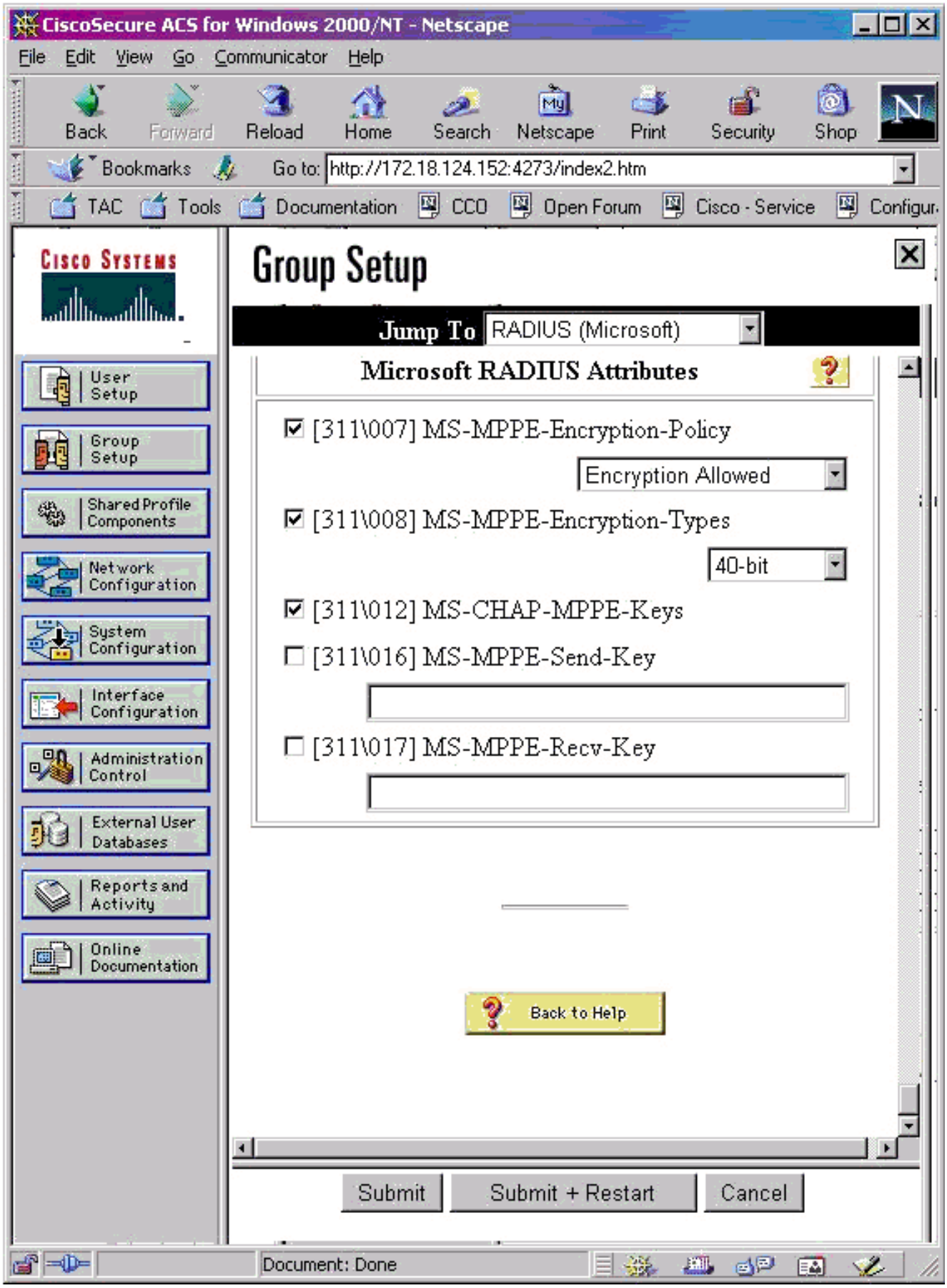
1. Fügen Sie das PIX zur Cisco Secure ACS for Windows Server **Network Configuration hinzu**, und identifizieren Sie den Wörterbuchtyp als **RADIUS (Cisco IOS/PIX)**.



2. Öffnen Sie **Interface Configuration > RADIUS (Microsoft)**, und überprüfen Sie die MPPE-Attribute, um sie in der Gruppenschnittstelle anzuzeigen.



3. Fügen Sie einen Benutzer hinzu. Fügen Sie in der Benutzergruppe die MPPE [RADIUS (Microsoft)]-Attribute hinzu. Sie müssen diese Attribute für die Verschlüsselung aktivieren. Sie ist optional, wenn das PIX nicht für die Verschlüsselung konfiguriert ist.



Überprüfen

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

PIX-Befehle (nach der Authentifizierung) anzeigen

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Der Befehl **show vpdn** listet Tunnel- und Sitzungsinformationen auf.

```
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
```

Client-PC-Verifizierung

Geben Sie in einem MS-DOS-Fenster oder im Fenster Ausführen **ipconfig /all ein**. Der PPP-Adapterteil zeigt diese Ausgabe an.

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

Sie können auch auf **Details** klicken, um Informationen in der PPTP-Verbindung anzuzeigen.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

- Es müssen Verbindungen für die Generic Routing Encapsulation (GRE) und TCP 1723 vom PC zum PIX-Tunnel-Endpunkt vorhanden sein. Wenn die Möglichkeit besteht, dass dies durch eine Firewall oder eine Zugriffsliste blockiert wird, stellen Sie den PC näher an den PIX.
- PPTP für Windows 98 und Windows 2000 ist am einfachsten einzurichten. Versuchen Sie im Zweifelsfall mehrere PCs und Betriebssysteme. Klicken Sie nach erfolgreicher Verbindung auf **Details** auf dem PC, um Informationen zur Verbindung anzuzeigen. Ob Sie beispielsweise

PAP, CHAP, IP, Verschlüsselung usw. verwenden.

- Wenn Sie RADIUS und/oder TACACS+ verwenden möchten, versuchen Sie zunächst, die lokale Authentifizierung (Benutzername und Kennwort) für die PIX-Authentifizierung einzurichten. Wenn dies nicht funktioniert, funktioniert die Authentifizierung mit einem RADIUS- oder TACACS+-Server nicht.
- Stellen Sie zunächst sicher, dass die Sicherheitseinstellungen auf dem PC so viele verschiedene Authentifizierungstypen wie möglich zulassen (PAP, CHAP, MS-CHAP) und deaktivieren Sie das Kontrollkästchen **Datenverschlüsselung** anfordern (aktivieren Sie diese Option sowohl auf dem PIX als auch auf dem PC).
- Da der Authentifizierungstyp ausgehandelt wird, konfigurieren Sie den PIX mit der maximalen Anzahl von Möglichkeiten. Wenn der PC beispielsweise nur für MS-CHAP und der Router nur für PAP konfiguriert ist, gibt es keine Vereinbarung.
- Wenn das PIX für zwei verschiedene Standorte als PPTP-Server fungiert und jeder Standort einen eigenen RADIUS-Server im Inneren hat, wird die Verwendung eines einzigen PIX für beide Standorte, die vom eigenen RADIUS-Server bedient werden, nicht unterstützt.
- Einige RADIUS-Server unterstützen MPPE nicht. Wenn ein RADIUS-Server MPPE-Keying nicht unterstützt, funktioniert die RADIUS-Authentifizierung, aber die MPPE-Verschlüsselung funktioniert nicht.
- Bei Windows 98 oder höher, wenn Sie PAP oder CHAP verwenden, ist der an den PIX gesendete Benutzername identisch mit dem, was in der DFÜ-Netzwerkverbindung (DUN) eingegeben wird. Wenn Sie jedoch MS-CHAP verwenden, kann der Domänenname an die Vorderseite des Benutzernamens angehängt werden, z. B.:Benutzername in DUN eingegeben - "cisco"Domain Set on Windows 98 box - "DOMAIN"MS-CHAP-Benutzername wird an PIX gesendet - "DOMAIN\cisco"Benutzername auf PIX - "cisco"Ergebnis: Ungültiger Benutzername/ungültiges KennwortDies ist ein Abschnitt des PPP-Protokolls von einem Windows 98-PC, der das Verhalten anzeigt.

```
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.
```

Wenn Sie Windows 98 und MS-CHAP auf dem PIX verwenden, können Sie neben dem Nicht-Domänen-Benutzernamen auch "DOMÄNE\Benutzername" zu PIX hinzufügen:

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

Hinweis: Wenn Sie eine Remote-Authentifizierung auf einem AAA-Server durchführen, gilt dasselbe.

Befehle zur Fehlerbehebung

Informationen zur Sequenz der erwarteten Sequenz von PPTP-Ereignissen finden Sie im PPTP RFC 2637 . Auf dem PIX zeigen bedeutende Ereignisse in einer guten PPTP-Sequenz Folgendes an:

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

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

PIX-Debug-Befehle

- **debug ppp io**: Zeigt die Paketinformationen für die virtuelle PPTP PPP-Schnittstelle an.
- **debug ppp error** (**ppp-Fehler debug**): Zeigt Protokollfehler und Fehlerstatistiken an, die mit der PPP-Verbindungsverhandlung und -Operation verknüpft sind.
- **debug vpdn error** (**vpdn-Fehler debug**): Zeigt Fehler an, die das Herstellen eines PPP-Tunnels verhindern, oder Fehler, die das Schließen eines etablierten Tunnels verursachen.
- **debug vpdn paket**: Zeigt L2TP-Fehler und -Ereignisse an, die Teil der normalen Tunneleinrichtung oder des normalen Tunnelabschaltens für VPDNs sind.
- **debug vpdn events**: Zeigt Meldungen über Ereignisse an, die Teil der normalen PPP-Tunneleinrichtung oder des normalen Herunterfahrens sind.
- **debug ppp uauth**: Zeigt die Debug-Meldungen zur AAA-Benutzerauthentifizierung für die virtuelle PPTP PPP-Schnittstelle an.

PIX Clear Commands

Dieser Befehl muss im Konfigurationsmodus ausgegeben werden.

- **clear vpdn tunnel [alle | *[id tunnel_id]*]** - Entfernt einen oder mehrere PPTP-Tunnel aus der Konfiguration.

Vorsicht: Stellen Sie *nicht* den Befehl **clear vpdn aus**. Dadurch werden *alle* vpdn-Befehle gelöscht.

Aktivieren der PPP-Protokollierung auf dem Client-PC

Führen Sie diese Anweisungen aus, um PPP-Debugging für verschiedene Windows- und Microsoft-Betriebssysteme zu aktivieren.

Windows 95

Führen Sie diese Schritte aus, um die PPP-Protokollierung auf einem Windows 95-Computer zu aktivieren.

1. Doppelklicken Sie in der Systemsteuerung unter der Option Netzwerk auf **Microsoft Dial-Up Adapter** in der Liste der installierten Netzwerkkomponenten.
2. Klicken Sie auf die Registerkarte **Erweitert**. Klicken Sie in der Liste Eigenschaften auf die Option **Protokolldatei aufzeichnen**, und klicken Sie in der Liste Wert auf **Ja**. Klicken Sie anschließend auf **OK**.
3. Fahren Sie den Computer herunter, und starten Sie ihn neu, damit diese Option wirksam wird. Das Protokoll wird in einer Datei mit dem Namen ppplog.txt gespeichert.

Windows 98

Führen Sie diese Schritte aus, um die PPP-Protokollierung auf einem Windows 98-Computer zu aktivieren.

1. Klicken Sie unter **DFÜ-Netzwerke** einmal auf ein Verbindungssymbol, und wählen Sie dann **Datei > Eigenschaften aus**.
2. Klicken Sie auf die Registerkarte Servertypen.
3. Wählen Sie die Option **Protokolldatei für diese Verbindung aufzeichnen aus**. Die Protokolldatei finden Sie unter C:\Windows\ppplog.txt.

Windows 2000

Um die PPP-Protokollierung auf einem Windows 2000-Computer zu aktivieren, rufen Sie die Microsoft-Support-Seite auf, und suchen Sie nach "Enable PPP Logging in Windows" (PPP-Anmeldung unter Windows aktivieren).

Windows NT

Befolgen Sie diese Schritte, um die PPP-Anmeldung auf einem NT-System zu aktivieren.

1. Suchen Sie den Schlüssel **SYSTEM\CurrentControlSet\Services\RasMan\PPP** , und ändern Sie die **Protokollierung** von 0 in **1**. Dadurch wird im <winnt root>\SYSTEM32\RAS directory eine Datei mit dem Namen PPP.LOG erstellt.
2. Um eine PPP-Sitzung zu debuggen, aktivieren Sie zunächst die Protokollierung, und initiieren Sie anschließend die PPP-Verbindung. Wenn die Verbindung fehlschlägt oder beendet wird, überprüfen Sie PPP.LOG, um zu sehen, was passiert ist.

Weitere Informationen finden Sie auf der Microsoft-Support-Seite , und suchen Sie nach "Aktivieren der PPP-Protokollierung in Windows NT".

Weitere Microsoft-Probleme

Hier sind einige Microsoft-bezogene Probleme aufgeführt, die bei der Fehlerbehebung für PPTP berücksichtigt werden sollten. Ausführliche Informationen finden Sie in der Microsoft Knowledge Base unter den angegebenen Links.

- So halten Sie RAS-Verbindungen nach der Abmeldung aktivRAS-Verbindungen (Windows Remote Access Service) werden automatisch getrennt, wenn Sie sich von einem RAS-Client abmelden. Sie können die Verbindung beibehalten, indem Sie den Registrierungsschlüssel KeepRasConnections auf dem RAS-Client aktivieren.
- Der Benutzer wird nicht benachrichtigt, wenn er sich mit zwischengespeicherten Anmeldeinformationen anmeldet.Wenn Sie sich von einer Windows-basierten Workstation oder einem Mitgliedserver in eine Domäne anmelden und der Domänencontroller nicht gefunden werden kann, erhalten Sie keine Fehlermeldung, die auf dieses Problem hinweist. Stattdessen sind Sie mit zwischengespeicherten Anmeldeinformationen am lokalen Computer angemeldet.
- Schreiben einer LMHOSTS-Datei für Probleme mit der Domänenvalidierung und anderen NamensauflösungWenn Probleme mit der Namensauflösung in Ihrem TCP/IP-Netzwerk auftreten, müssen Sie Lmhosts-Dateien verwenden, um NetBIOS-Namen aufzulösen. Sie müssen eine bestimmte Prozedur befolgen, um eine Lmhosts-Datei zu erstellen, die in der

Namensauflösung und Domänenvalidierung verwendet werden soll.

Beispielausgabe für Debugging

PIX Debug - Lokale Authentifizierung

Diese Debugausgabe zeigt wichtige Ereignisse in *Kursivschrift*.

```
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: 009c00011a2b3c4d000200000100010000000000030000... PPTP: cc waiting for input, max
soc FD = 1 PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0
PPTP: cc rcv 168 bytes of data OCRQ = Outgoing-Call-Request - message code bytes 9 & 10 = 0007
Tnl 42 PPTP: CC I 00a800011a2b3c4d000700000000000000000dac00000... Tnl 42 PPTP: CC I OCRQ Tnl 42
PPTP: call id 0x0 Tnl 42 PPTP: serial num 0 Tnl 42 PPTP: min bps 56000:0xdac0 Tnl 42 PPTP: max
bps 64000:0xfa00 Tnl 42 PPTP: bearer type 3 Tnl 42 PPTP: framing type 3 Tnl 42 PPTP: recv win
size 16 Tnl 42 PPTP: ppd 0 Tnl 42 PPTP: phone num Len 0 Tnl 42 PPTP: phone num "" Tnl/Cl 42/42
PPTP: l2x store session: tunnel id 42, session id 42, hash_ix=42 PPP virtual access open, ifc =
0 Tnl/Cl 42/42 PPTP: vacc-ok -> state change wt-vacc to estabd OCRP = Outgoing-Call-Reply -
message code bytes 9 & 10 = 0008 Tnl/Cl 42/42 PPTP: CC O OCRP PPTP: cc snddata, socket FD=1,
Len=32, data: 002000011a2b3c4d00080000002a00000100000000fa... !--- Debug following this last
event is flow of packets. PPTP: cc waiting for input, max soc FD = 1 outside PPTP: Recvd xGRE
pak from 99.99.99.5, Len 39, seq 1 PPP rcvd, ifc = 0, pppdev: 1, Len: 27, data:
ff03c021010100170206000a00000506001137210702... PPP xmit, ifc = 0, Len: 23 data:
ff03c021010100130305c22380050609894ab407020802 Interface outside - PPTP xGRE: Out paket, PPP Len
23 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 39, seq 1, ack 1, data:
3081880b00170000000000010000000 1ff03c0210101... PPP xmit, ifc = 0, Len: 17 data:
ff03c0210401000d0206000a00000d0306 Interface outside - PPTP xGRE: Out paket, PPP Len 17 outside
PPTP: Sending xGRE pak to 99.99.99.5, Len 33, seq 2, ack 1, data:
3081880b00110000000000002000000001ff03c0210401... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 39, seq 2, ack 1 PPP rcvd, ifc = 0, pppdev: 1, Len: 23, data:
ff03c021020100130305c22380050609894ab407020802 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len
34, seq 3, ack 2 PPP rcvd, ifc = 0, pppdev: 1, Len: 18, data:
ff03c0210102000e05060011372107020802 PPP xmit, ifc = 0, Len: 18 data:
ff03c0210202000e05060011372107020802 Interface outside - PPTP xGRE: Out paket, PPP Len 18
outside PPTP: Sending xGRE pak to 99.99.99.5, Len 34, seq 3, ack 3, data:
3081880b00120000000000003000000003ff03c0210202... PPP xmit, ifc = 0, Len: 17 data:
ff03c2230101000d08d36602863630eca8 Interface outside - PPTP xGRE: Out paket, PPP Len 15 outside
PPTP: Sending xGRE pak to 99.99.99.5, Len 31, seq 4, ack 3, data:
3081880b000f0000000000400000003c2230101000d... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 76, seq 4, ack 4 PPP rcvd, ifc = 0, pppdev: 1, Len: 62, data:
ff03c2230201003a31d4d0a397a064668bb00d954a85... PPP xmit, ifc = 0, Len: 8 data: ff03c22303010004
Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to
99.99.99.5, Len 22, seq 5, ack 4, data: 3081880b00060000000000000500000004c22303010004 outside
PPTP: Recvd xGRE pak from 99.99.99.5, Len 58, seq 5, ack 5 PPP rcvd, ifc = 0, pppdev: 1, Len:
44, data: ff038021010100280206002d0f010306000000008106... PPP xmit, ifc = 0, Len: 14 data:
ff0380210101000a030663636302 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP:
Sending xGRE pak to 99.99.99.5, Len 28, seq 6, ack 5, data:
```

3081880b000c000000000060000000580210101000a... PPP xmit, ifc = 0, Len: 38 data:
ff038021040100220206002d0f018106000000008206... Interface outside - PPTP xGRE: Out paket, PPP
Len 36 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 52, seq 7, ack 5, data:
3081880b00240000000000070000005802104010022... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 29, seq 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 19, data:
ff0380fd0101000f1206010000011105000104 PPP xmit, ifc = 0, Len: 8 data: ff0380fd01010004
Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to
99.99.99.5, Len 22, seq 8, ack 6, data: 3081880b000600000000000080000000680fd01010004 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:
3081880b00110000000000090000000680fd0401000f... 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:
ff0300214500001cc80000008001e5ccac100101e000... PPP IP Pkt:
4500001cc80000008001e5ccac100101e00000020a00... 603104: PPTP Tunnel created, tunnel_id is 42,
remote_peer_ip is 99.99.99.5 ppp_virtual_interface_id is 1, client_dynamic_ip is 172.16.1.1
username is john, MPPE_key_strength is None outside PPTP: Recvd xGRE pak from 99.99.99.5, Len
109, seq 15 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060ca0000008011176bac100101ac10... PPP IP Pkt:
45000060ca0000008011176bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 16 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060cb0000008011166bac100101ac10... PPP IP Pkt:
45000060cb0000008011166bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 17 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060cc0000008011156bac100101ac10... PPP IP Pkt:
45000060cc0000008011156bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 18 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060d00000008011116bac100101ac10... PPP IP Pkt:
45000060d00000008011116bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 19 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060d200000080110f6bac100101ac10... PPP IP Pkt:
45000060d200000080110f6bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 20 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060d300000080110e6bac100101ac10... PPP IP Pkt:
45000060d300000080110e6bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 41, seq 21 PPP rcvd, ifc = 0, pppdev: 1, Len: 32, data:
ff0300214500001cd60000008001d7ccac100101e000... PPP IP Pkt:
4500001cd60000008001d7ccac100101e00000020a00... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 22 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060d80000008011096bac100101ac10... PPP IP Pkt:
45000060d80000008011096bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 23 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:

```
ff03002145000060da0000008011076bac100101ac10... PPP IP Pkt:
45000060da0000008011076bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 24 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060db0000008011066bac100101ac10... PPP IP Pkt:
45000060db0000008011066bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 25 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060de0000008011036bac100101ac10... PPP IP Pkt:
45000060de0000008011036bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 26 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060e00000008011016bac100101ac10... PPP IP Pkt:
45000060e00000008011016bac100101ac10ffff0089... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 109, seq 27 PPP rcvd, ifc = 0, pppdev: 1, Len: 100, data:
ff03002145000060e10000008011006bac100101ac10... PPP IP Pkt:
45000060e10000008011006bac100101ac10ffff0089... inside:172.16.255.255/137 outside PPTP: Recvd
xGRE pak from 99.99.99.5, Len 41, seq 28 PPP rcvd, ifc = 0, pppdev: 1, Len: 32, data:
ff0300214500001ce40000008001c9ccac100101e000... PPP IP Pkt:
4500001ce40000008001c9ccac100101e00000020a00...
```

PIX Debug - RADIUS-Authentifizierung

Diese Debugausgabe zeigt wichtige Ereignisse in *Kursivschrift*.

```
PIX#terminal monitor
PIX# 106011: Deny inbound (No xlate) icmp src
   outside:172.17.194.164 dst
   outside:172.18.124.201 (type 8, code 0)
106011: Deny inbound (No xlate) icmp src
   outside:172.17.194.164 DST
   outside:172.18.124.201 (type 8, code 0)

PIX#
PPTP: soc select returns rd mask = 0x1
PPTP: new peer FD is 1

Tnl 9 PPTP: Tunnel created; peer initiatedPPTP:
   created tunnel, id = 9

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

SCCRQ = Start-Control-Connection-Request - message code bytes 9 & 10 = 0001 Tnl 9 PPTP: CC I
009c00011a2b3c4d000100000100000000000010000... Tnl 9 PPTP: CC I SCCRQ Tnl 9 PPTP: protocol
version 0x100 Tnl 9 PPTP: framing caps 0x1 Tnl 9 PPTP: bearer caps 0x1 Tnl 9 PPTP: max channels
0 Tnl 9 PPTP: firmware rev 0x870 Tnl 9 PPTP: hostname "" Tnl 9 PPTP: vendor "Microsoft Windows
NT" Tnl 9 PPTP: SCCRQ-ok -> state change wt-sccrq to estabd SCCRP = Start-Control-Connection-
Reply - message code bytes 9 & 10 = 0002 Tnl 9 PPTP: CC O SCCRP PPTP: cc snddata, socket FD=1,
Len=156, data: 009c00011a2b3c4d000200000100010000000000030000... PPTP: cc waiting for input, max
soc FD = 1 PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0
PPTP: cc rcv 168 bytes of data OCRQ = Outgoing-Call-Request - message code bytes 9 & 10 = 0007
Tnl 9 PPTP: CC I 00a800011a2b3c4d000700004000e4f50000012c05f5... Tnl 9 PPTP: CC I OCRQ Tnl 9
PPTP: call id 0x4000 Tnl 9 PPTP: serial num 58613 Tnl 9 PPTP: min bps 300:0x12c Tnl 9 PPTP: max
BPS 100000000:0x5f5e100 Tnl 9 PPTP: bearer type 3 Tnl 9 PPTP: framing type 3 Tnl 9 PPTP: recv
win size 64 Tnl 9 PPTP: ppd 0 Tnl 9 PPTP: phone num Len 0 Tnl 9 PPTP: phone num "" Tnl/Cl 9/9
PPTP: l2x store session: tunnel id 9, session id 9, hash_ix=9 PPP virtual access open, ifc = 0
Tnl/CL 9/9 PPTP: vacc-ok -> state change wt-vacc to estabd OCRP = Outgoing-Call-Reply - message
code bytes 9 & 10 = 0008 Tnl/CL 9/9 PPTP: CC O OCRP PPTP: cc snddata, socket FD=1, Len=32, data:
002000011a2b3c4d000800000009400001000000000fa... PPTP: cc waiting for input, max soc FD = 1
outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 60, seq 0 PPP rcvd, ifc = 0, pppdev: 1, Len:
48, data: ff03c0210100002c0506447e217e070208020d030611... PPP xmit, ifc = 0, Len: 23 data:
ff03c021010100130305c2238005065a899b2307020802 Interface outside - PPTP xGRE: Out paket, PPP Len
23 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 39, seq 1, ack 0, data:
3081880b0017400000000001000000000ff03c0210101... 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: 3081880b0026400000000002000000000ff03c0210400... 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 001800011a2b3c4d000f000000090000fffffffffffff... 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: 3081880b0012400000000003000000002ff03c0210201... PPP xmit, ifc = 0, Len: 17 data: ff03c2230101000d08f3686cc47e37ce67 Interface outside - PPTP xGRE: Out paket, PPP Len 15 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 31, seq 4, ack 2, data: 3081880b000f4000000000400000002c2230101000d... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 36, seq 3, ack 3 PPP rcvd, ifc = 0, pppdev: 1, Len: 22, data: ff03c0210c020012447e217e4d5352415356352e3030 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 45, seq 4 PPP rcvd, ifc = 0, pppdev: 1, Len: 35, data: ff03c0210c03001f447e217e4d535241532d312d4349... PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0 PPTP: cc rcv 24 bytes of data Tnl 9 PPTP: CC I 001800011a2b3c4d000f000000090000000000000000... Tnl/CL 9/9 PPTP: CC I SLI PPTP: cc waiting for input, max soc FD = 1 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 76, seq 5, ack 4 PPP rcvd, ifc = 0, pppdev: 1, Len: 62, data: 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: 3081880b000640000000000500000005c22303010004 CHAP peer authentication succeeded for john outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 72, seq 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 62, data: 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: 3081880b000640000000000600000006c22303010004 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 7, ack 5 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380fd0104000a120601000001 PPP xmit, ifc = 0, Len: 14 data: ff0380fd0101000a120601000020 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 7, ack 7, data: 3081880b000c4000000000070000000780fd0101000a... 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: 3081880b000c4000000000080000000780fd0304000a... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 48, seq 8 PPP rcvd, ifc = 0, pppdev: 1, Len: 38, data: ff038021010500220306000000008106000000008206... PPP xmit, ifc = 0, Len: 14 data: ff0380210101000a0306ac127c98 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 9, ack 8, data: 3081880b000c4000000000090000000880210101000a... PPP xmit, ifc = 0, Len: 32 data: ff0380210405001c8106000000008206000000008306.. . 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: 3081880b001e40000000000a0000000880210405001c... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 9, ack 7 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380fd0201000a120601000020 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 10, ack 8 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380fd0106000a120601000020 PPP xmit, ifc = 0, Len: 14 data: ff0380fd0206000a120601000020 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 11, ack 10, data: 3081880b000c40000000000b0000000a80fd0206000a... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 11, ack 9 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210201000a0306ac127c98 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 12, ack 10 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210107000a030600000000 PPP xmit, ifc = 0, Len: 14 data: ff0380210307000a0306c0a80101 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 12, ack 12, data: 3081880b000c40000000000c0000000c80210307000a... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 24, seq 13 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380210108000a030600000000 PPP xmit, ifc = 0, Len: 14 data: ff0380210308000a0306c0a80101 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 13, ack 13, data: 3081880b000c40000000000d0000000d80210308000a... 0 outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 14, ack 13 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data:

ff0380210109000a0306c0a80101 PPP xmit, ifc = 0, Len: 14 data: ff0380210209000a0306c0a80101 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 14, ack 14, data: 3081880b000c40000000000e0000000e80210209000a... 2: PPP virtual interface 1 - user: john aaa authentication started 603103: PPP virtual interface 1 - user: john aaa authentication succeed 109011: Authen Session Start: user 'joh outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 117, seq 15, ack 14 PPP rcvd, ifc = 0, pppdev: 1, Len: 104, data: ff0300fd9000bccf59b71755d9af7330dae3bbc94d28... PPP Encr/Comp Pkt: 9000bccf59b71755d9af7330dae3bbc94d28e431d057... PPP IP Pkt: 4500006002bb000080117629c0a80101ffffffff0089... n', sid 3 603104: PPTP Tunnel created, tunnel_id is 9, remote_peer_ip is 10.44.17.104 ppp_virtual_interface_id is 1, client_dynamic_ip is 192.168.1.1 username is john, MPPE_key_strength is 40 bits outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 113, seq 16 PPP rcvd, ifc = 0, pppdev: 1, Len: 104, data: ff0300fd9001f8348351ef9024639ed113b43adfeb44... PPP Encr/Comp Pkt: 9001f8348351ef9024639ed113b43adfeb4489af5ab3... PPP IP Pkt: 4500006002bd000080117627c0a80101ffffffff0089... ide outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 113, seq 17 PPP rcvd, ifc = 0, pppdev: 1, Len: 104, data: ff0300fd9002cc73cd65941744a1cf30318cc4b4b783... PPP Encr/Comp Pkt: 9002cc73cd65941744a1cf30318cc4b4b783e825698a... PPP IP Pkt: 4500006002bf000080117625c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 18 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd9003aaa545eaeeda0f82b5999e2fa9ba3245... PPP Encr/Comp Pkt: 9003aaa545eaeeda0f82b5999e2fa9ba324585a1bc8d... PPP IP Pkt: 4500006002c1000080117623c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 19 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd90045b35d080900ab4581e64706180e3540e... PPP Encr/Comp Pkt: 90045b35d080900ab4581e64706180e3540ee15d664a... PPP IP Pkt: 4500006002c3000080117621c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 20 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd90052878b256edbd17b42f2cb672ba80b40a... PPP Encr/Comp Pkt: 90052878b256edbd17b42f2cb672ba80b40a79760cef... PPP IP Pkt: 4500006002c500008011761fc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 21 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd900632359a2c07e79106c5e282e3892e60de... PPP Encr/Comp Pkt: 900632359a2c07e79106c5e282e3892e60ded6c6d4d1... PPP IP Pkt: 4500006002c700008011761dc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 22 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd90070ca6ea48b2ad26987d52a4e109ca68b6... PPP Encr/Comp Pkt: 90070ca6ea48b2ad26987d52a4e109ca68b6758569d3... PPP IP Pkt: 4500006002c900008011761bc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 23 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd90085aba60edf57e50eea4d523596cb9d690... PPP Encr/Comp Pkt: 90085aba60edf57e50eea4d523596cb9d69057715894... PPP IP Pkt: 4500006002cb000080117619c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 24 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd90094b73b6c962272b60d32f135b5f29f2a5... PPP Encr/Comp Pkt: 90094b73b6c962272b60d32f135b5f29f2a58bacd050... PPP IP Pkt: 4500006002cc000080117618c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 345, seq 25 PPP rcvd, ifc = 0, pppdev: 1, len: 336, data: ff0300fd900a86307ed9537df5389ea09223d62c20fd... PPP Encr/Comp Pkt: 900a86307ed9537df5389ea09223d62c20fd9e34072f... PPP IP Pkt: 4500014802cf00008011752dc0a80101ffffffff0044... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 26 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd900b45303a5fe7b2dc3f62db739b4bb1b802... PPP Encr/Comp Pkt: 900b45303a5fe7b2dc3f62db739b4bb1b80253278fad... PPP IP Pkt: 4500006002d1000080117613c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 27 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd900ceb5aaaecc832df3c12bc6c519c25b4db... PPP Encr/Comp Pkt: 900ceb5aaaecc832df3c12bc6c519c25b4dba569d10... PPP IP Pkt: 4500006002d2000080117612c0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 28 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data: ff0300fd900dbdaaf071c2bd1c92c1f56085813d1a77... PPP Encr/Comp Pkt: 900dbdaaf071c2bd1c92c1f56085813d1a778cc61c29... PPP IP Pkt: 4500006002d500008011760fc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104, len 113, seq 29 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:

```
ff0300fd900e97de47036d95a0721ef6b28479b8efde... PPP Encr/Comp Pkt:
900e97de47036d95a0721ef6b28479b8efde8e16b398... PPP IP Pkt:
4500006002d600008011760ec0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 30 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd900f75bf4c8cbcf11464bf52bd7f6155c7d6... PPP Encr/Comp Pkt:
900f75bf4c8cbcf11464bf52bd7f6155c7d62ea2ca5e... PPP IP Pkt:
4500006002d900008011760bc0a80101ffffffff0089... outside PPTP: Recvd xGRE pak from 10.44.17.104,
len 113, seq 31 PPP rcvd, ifc = 0, pppdev: 1, len: 104, data:
ff0300fd9010f221e7ba169702765529e4ffa368dba5... PPP Encr/Comp Pkt:
9010f221e7ba169702765529e4ffa368dba5610921ae... PPP IP Pkt:
4500006002da00008011760ac0a80101ffffffff0089... from (192.168.1.1) to 255.255.255.255 on
interface outside outside PPTP: Recvd xGRE pak from 10.44.17.104, len 231, seq 32 PPP rcvd, ifc
= 0, pppdev: 1, len: 222, data: ff0300fd9011c23a03921c1e10ccc38847cb8056fa93... PPP Encr/Comp
Pkt: 9011c23a03921c1e10ccc38847cb8056fa9387018912... PPP IP Pkt:
450000d602dd000080117591c0a80101ffffffff008a... side outside PPTP: Recvd xGRE pak from
10.44.17.104, len 345, seq 33 PPP rcvd, ifc = 0, pppdev: 1, len: 336, data:
ff0300fd90127d7213f35cd1d82d8988e28e0930ecc1... PPP Encr/Comp Pkt:
90127d7213f35cd1d82d8988e28e0930ecc104a993f... PPP IP Pkt:
4500014802df00008011751dc0a80101ffffffff0044...
```

Was kann schief gehen?

Simultaner PPTP-Tunnel

Sie können nicht mehr als 127 Verbindungen mit PIX 6.x verbinden, und diese Fehlermeldung wird angezeigt:

%PIX-3-213001: PPTP-Steuerungs-Daemon Socket io Accept-Fehler, errno = 5

Lösung:

In PIX 6.x ist die Anzahl der gleichzeitigen Sitzungen auf 128 begrenzt. Wenn Sie einen für den PPTP Listening-Socket subtrahieren, ist die maximale Anzahl 127 Verbindungen.

PIX und PC können Authentifizierung nicht verhandeln

Die PC-Authentifizierungsprotokolle sind für solche Protokolle festgelegt, die das PIX nicht ausführen kann (Shiva Password Authentication Protocol (SPAP) und Microsoft CHAP Version 2 (MS-CHAP v.2) anstelle von Version 1). Der PC und PIX können sich nicht auf die Authentifizierung einigen. Der PC zeigt folgende Meldung an:

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

PIX und PC können Verschlüsselung nicht aushandeln

Der PC ist auf **Nur verschlüsselt** eingestellt, und der Befehl **vpdn group 1 ppp encrypt mppe 40** wird aus dem PIX gelöscht. Der PC und PIX können sich nicht auf die Verschlüsselung einigen, und der PC zeigt folgende Meldung an:

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

PIX und PC können Verschlüsselung nicht aushandeln

Der PIX ist für die **vPdn-Gruppe 1 ppp verschlüsselt mppe 40 erforderlich**, und der PC für die nicht zulässige Verschlüsselung. Dies erzeugt keine Nachrichten auf dem PC, aber die Sitzung wird unterbrochen, und das PIX-Debuggen zeigt diese Ausgabe an:

```
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-Problem

Der PIX ist für die **erforderliche VPN-Verschlüsselungsmethode 40** der **VPN-Gruppe 1** festgelegt, und der PC für die Verschlüsselung, die mit Authentifizierung zulässig ist, gibt den MPPE-Schlüssel nicht an einen RADIUS-Server zurück. Der PC zeigt folgende Meldung an:

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

Das PIX-Debuggen zeigt Folgendes:

```
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
```

Der PC zeigt folgende Meldung an:

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

Zugehörige Informationen

- Cisco PIX Firewall-Software
- Cisco Secure PIX Firewall - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Häufigste L2L- und Remote Access IPSec VPN-Lösungen zur Fehlerbehebung
- PPTP-Support-Seite
- RFC 2637: Point-to-Point Tunneling Protocol (PPTP)
- Anforderungen für Kommentare (RFCs)

- Technischer Support - Cisco Systems