PIX 6.x Esempio di configurazione di PPTP con autenticazione Radius

Sommario

Introduzione

Il PPTP (Point-to-Point Tunneling Protocol) è un protocollo di tunneling di livello 2 che consente a un client remoto di utilizzare una rete IP pubblica per comunicare in modo sicuro con i server di una rete aziendale privata. Il PPTP esegue il tunneling dell'IP. Il protocollo PPTP è descritto nella RFC 2637 . Il supporto PPTP sul PIX Firewall è stato aggiunto nel software PIX versione 5.1. La documentazione PIX fornisce ulteriori informazioni su PPTP e sul suo utilizzo con PIX. In questo documento viene descritto come configurare il PIX in modo che utilizzi PPTP con l'autenticazione

locale, TACACS+ e RADIUS. In questo documento vengono inoltre forniti suggerimenti ed esempi per la risoluzione dei problemi più comuni.

In questo documento viene spiegato come configurare le connessioni PPTP *ai* PIX. Per configurare un'appliance PIX o ASA in modo che *usi* PPTP *attraverso* l'appliance di sicurezza, consultare il documento sull'autorizzazione delle connessioni PPTP/L2TP attraverso il PIX.

Per configurare il firewall PIX e il client VPN per l'utilizzo con il server RADIUS Windows 2000 e 2003, fare riferimento a Cisco Secure PIX Firewall 6.x e Cisco VPN Client 3.5 for Windows con autenticazione RADIUS IAS di Microsoft Windows 2000 e 2003.

Per configurare PPTP su un concentratore VPN 3000 con Cisco Secure ACS per Windows RADIUS Authentication, consultare il documento sulla configurazione del concentratore VPN 3000 e di PPTP con Cisco Secure ACS per Windows per l'autenticazione RADIUS.

Per configurare una connessione PC al router, consultare il documento sulla configurazione di Cisco Secure ACS per l'autenticazione PPTP del router Windows, che fornisce quindi l'autenticazione dell'utente al server Cisco Secure Access Control System (ACS) 3.2 per Windows prima di consentire l'accesso dell'utente alla rete.

Nota: in termini PPTP, in base all'RFC, il server di rete PPTP (PNS) è il server (in questo caso, il PIX o il destinatario della chiamata) e il concentratore di accesso PPTP (PAC) è il client (il PC o il chiamante).

Nota: il tunneling suddiviso non è supportato in PIX per i client PPTP.

Nota: per il corretto funzionamento del protocollo PPTP, il protocollo PIX 6.x richiede MS-CHAP v1.0. Windows Vista non supporta MS-CHAP v1.0. Pertanto PPTP su PIX 6.x non funzionerà per Windows Vista. PPTP non è supportato in PIX versione 7.x e successive.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il software Cisco Secure PIX Firewall versione 6.3(3).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

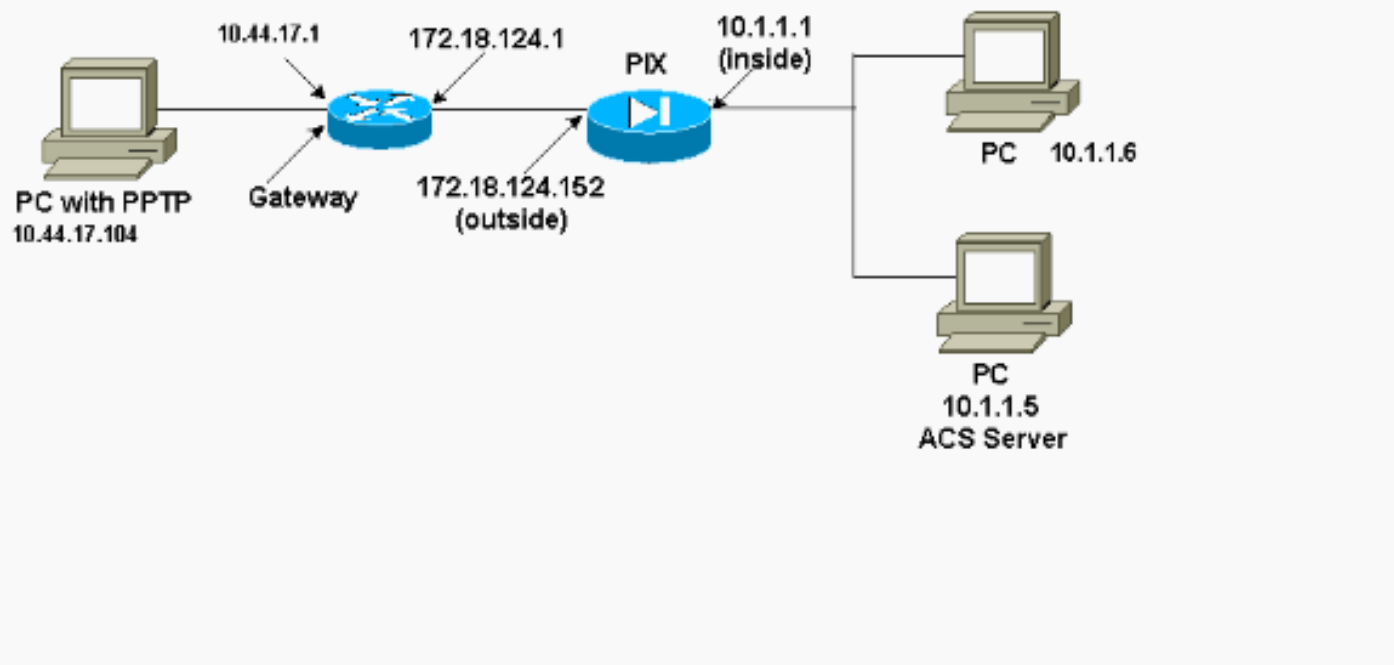
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete.



Suggerimenti per la configurazione di PIX Firewall

Tipo di autenticazione: CHAP, PAP, MS-CHAP

Il PIX configurato per tutti e tre i metodi di autenticazione (CHAP, PAP, MS-CHAP) fornisce contemporaneamente la migliore possibilità di connettersi indipendentemente dalla configurazione del PC. Questa è una buona idea per la risoluzione dei problemi.

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

Crittografia Microsoft Point-to-Point (MPPE)

Utilizzare questa sintassi del comando per configurare la crittografia MPPE sul firewall PIX.

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

In questo comando, **required** è una parola chiave facoltativa. MS-CHAP deve essere configurato.

Configurazione della funzionalità PPTP nei PC client

Nota: le informazioni disponibili qui su relative alla configurazione software Microsoft non sono incluse in alcuna garanzia o supporto per il software Microsoft. Il supporto per il software Microsoft è disponibile presso Microsoft e sul sito Web del supporto Microsoft .

Windows 98

Seguire questi passaggi per installare la funzione PPTP su Windows 98.

1. Selezionare **Start > Impostazioni > Pannello di controllo > Nuovo hardware**. Fare clic su **Next** (Avanti).
2. Fare clic su **Select from List (Seleziona dall'elenco)** e selezionare **Network Adapter**. Fare clic su **Next** (Avanti).
3. Scegliere **Microsoft** nel pannello sinistro e **Microsoft VPN Adapter** nel pannello destro.

Per configurare la funzione PPTP, attenersi alla seguente procedura.

1. Selezionare **Start > Programmi > Accessori > Comunicazioni > Accesso remoto**.
2. Fare clic su **Crea nuova connessione**. Per **Selezionare un dispositivo**, connettersi utilizzando **Microsoft VPN Adapter**. L'indirizzo IP del server VPN è l'endpoint del tunnel PIX.
3. L'autenticazione predefinita di Windows 98 utilizza la crittografia della password (CHAP o MS-CHAP). Per modificare il PC in modo da consentire anche il PAP, selezionare **Proprietà > Tipi di server**. Deselezionare **Richiedi password crittografata**. In quest'area è possibile configurare la crittografia dei dati (MPPE o MPPE assente).

Windows 2000

Per configurare la funzionalità PPTP in Windows 2000, eseguire la procedura seguente.

1. Selezionare **Start > Programmi > Accessori > Comunicazioni > Connessioni di rete e remote**.
2. Fare clic su **Crea nuova connessione**, quindi su **Avanti**.
3. Selezionare **Connetti a una rete privata tramite Internet** e **Componi una connessione prima** (o non se LAN). Fare clic su **Next** (Avanti).
4. Immettere il nome host o l'indirizzo IP dell'endpoint del tunnel (PIX/router).
5. Se è necessario modificare il tipo di password, selezionare **Proprietà > Protezione per la connessione > Avanzate**. Il valore predefinito è MS-CHAP e MS-CHAP v2 (non CHAP o PAP). In quest'area è possibile configurare la crittografia dei dati (MPPE o MPPE assente).

Windows NT

Per configurare i client NT per PPTP, consultare il documento sull'installazione, la configurazione e l'utilizzo di PPTP con client e server Microsoft.

Configurazione del PIX

Configurazione PIX - Autenticazione locale, senza crittografia

```
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
```

Configurazione PIX - Autenticazione locale con crittografia

Se si aggiunge questo comando alla configurazione PIX - Autenticazione locale, Nessuna configurazione di crittografia, il PC e PIX eseguono la negoziazione automatica della crittografia a 40 bit o nessuna (in base alle impostazioni del PC).

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

Se per il PIX la funzione 3DES è attivata, il comando **show version** visualizza questo messaggio.

- Versioni 6.3 e successive:
  `VPN-3DES-AES: Enabled`
- Versioni 6.2 e precedenti:
  `VPN-3DES: Enabled`

Èinoltre possibile eseguire la crittografia a 128 bit. Tuttavia, se viene visualizzato uno di questi messaggi, il PIX non è abilitato per la crittografia a 128 bit.

- Versioni 6.3 e successive:
  ```
  Warning: VPN-3DES-AES license is required
  for 128 bits MPPE encryption
  ```
- Versioni 6.2 e precedenti:
  ```
  Warning: VPN-3DES license is required
  for 128 bits MPPE encryption
  ```

Di seguito è riportata la sintassi del comando MPPE.

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

Il PC e il PIX devono essere configurati per l'autenticazione MS-CHAP in combinazione con MPPE.

Configurazione PIX - Autenticazione TACACS+/RADIUS senza crittografia

```
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]
```

Configurazione PIX - Autenticazione RADIUS con crittografia

Se si utilizza RADIUS e il server RADIUS (attributo specifico del fornitore 26, Microsoft come fornitore) supporta la codifica MPPE, è possibile aggiungere la crittografia MPPE. L'autenticazione TACACS+ non funziona con la crittografia perché i server TACACS+ non sono in grado di restituire chiavi MPPE speciali. Cisco Secure ACS per Windows 2.5 e versioni successive RADIUS non supporta MPPE (tutti i server RADIUS non supportano MPPE).

Supponendo che l'autenticazione RADIUS funzioni senza crittografia, aggiungere la crittografia includendo questo comando nella configurazione precedente:

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

Il PC e il PIX negoziano automaticamente la crittografia a 40 bit o nessuna crittografia (in base alle impostazioni del PC).

Se per il PIX la funzione 3DES è attivata, il comando **show version** visualizza questo messaggio.

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

Èinoltre possibile eseguire la crittografia a 128 bit. Tuttavia, se viene visualizzato questo messaggio, il PIX non è abilitato per la crittografia a 128 bit.

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

In questo output viene mostrata la sintassi del comando MPPE.

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

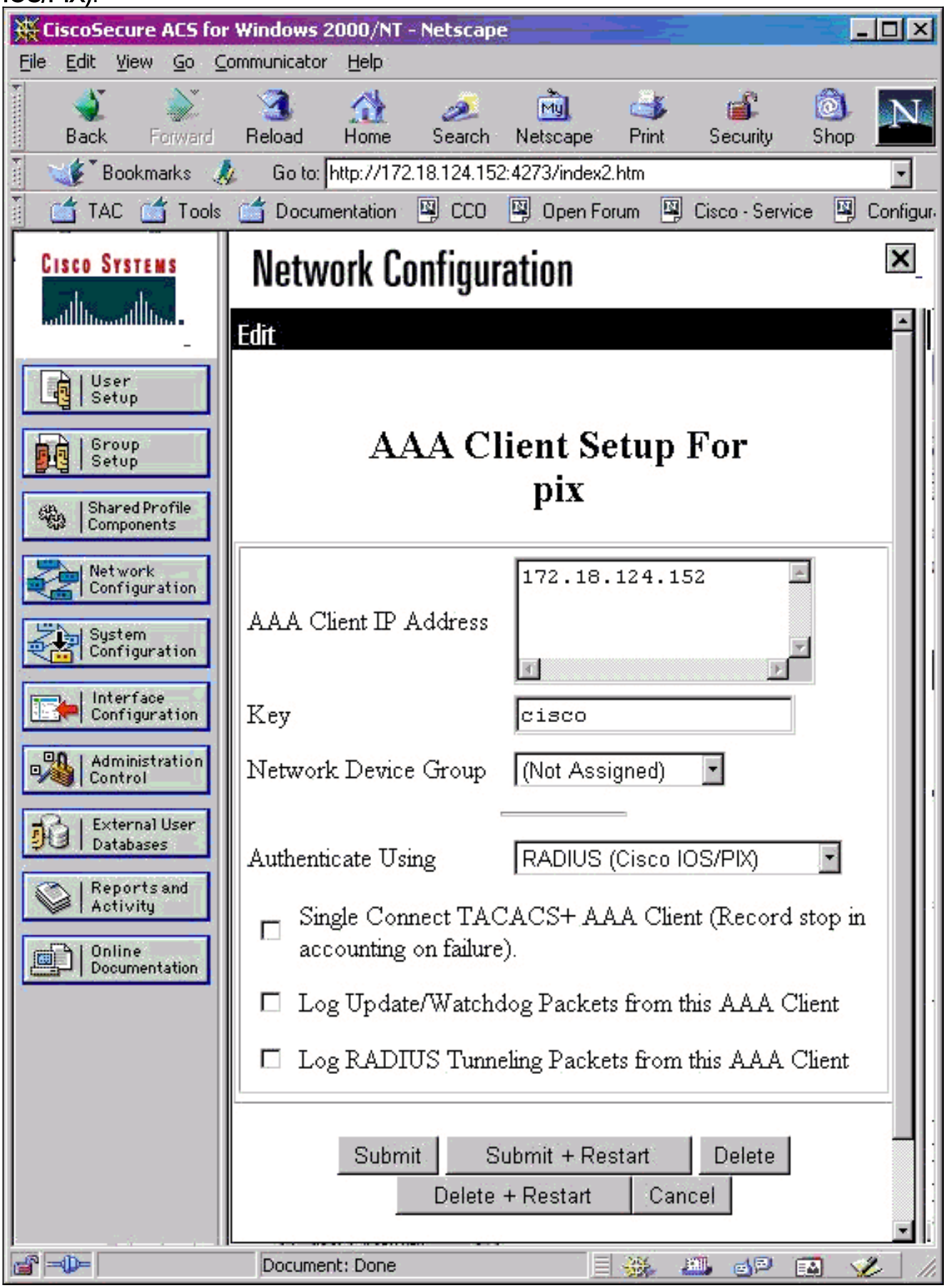
Il PC e il PIX devono essere configurati per l'autenticazione MS-CHAP in combinazione con MPPE.

Configurazione di Cisco Secure ACS per Windows 3.0

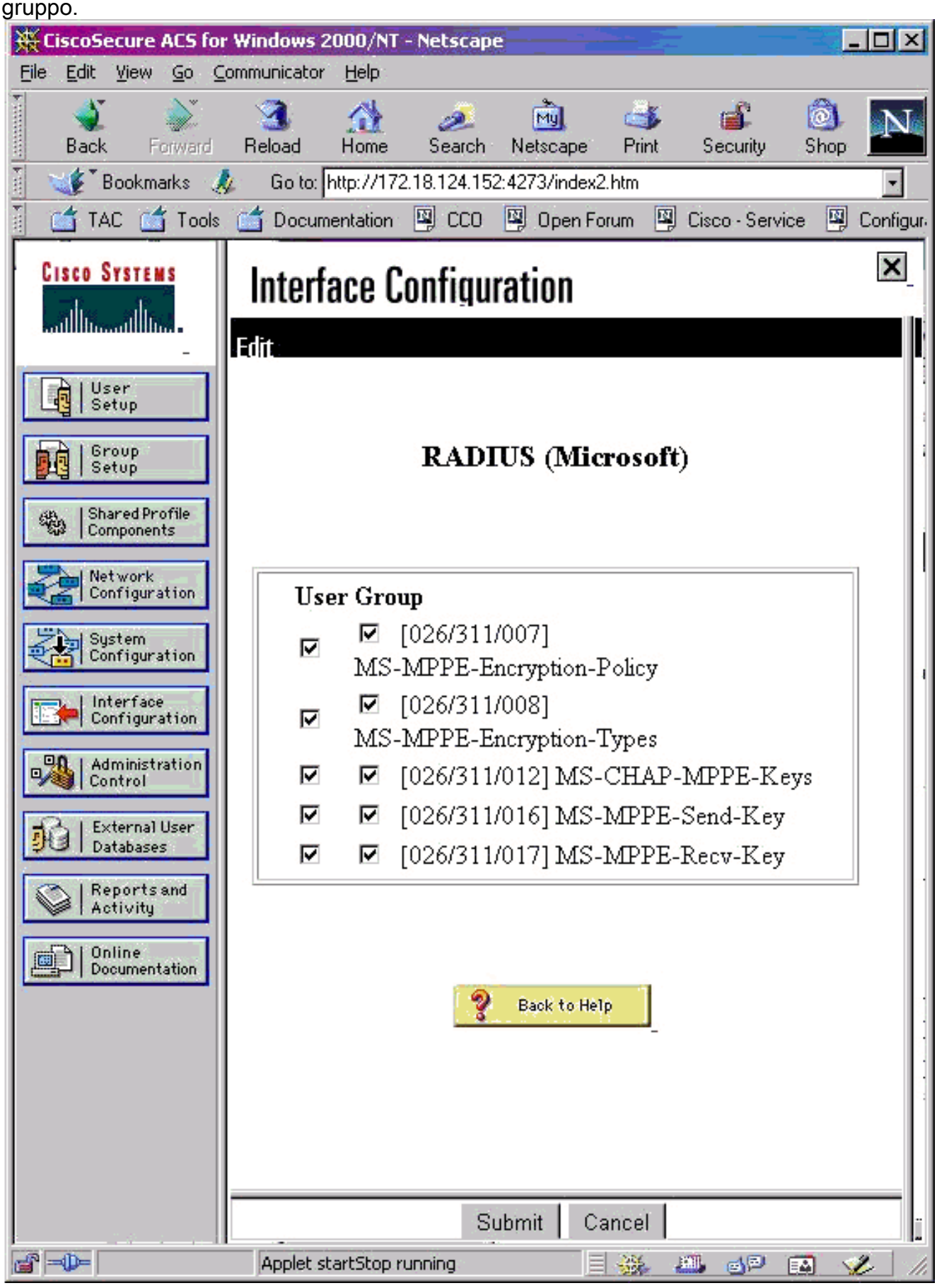
Autenticazione RADIUS con crittografia

Utilizzare questa procedura per configurare Cisco Secure ACS per Windows 3.0. La stessa procedura di configurazione si applica alle versioni 3.1 e 3.2 di ACS.

1. Aggiungere il PIX a Cisco Secure ACS for Windows server **Network Configuration** e identificare il tipo di dizionario come **RADIUS (Cisco IOS/PIX)**.

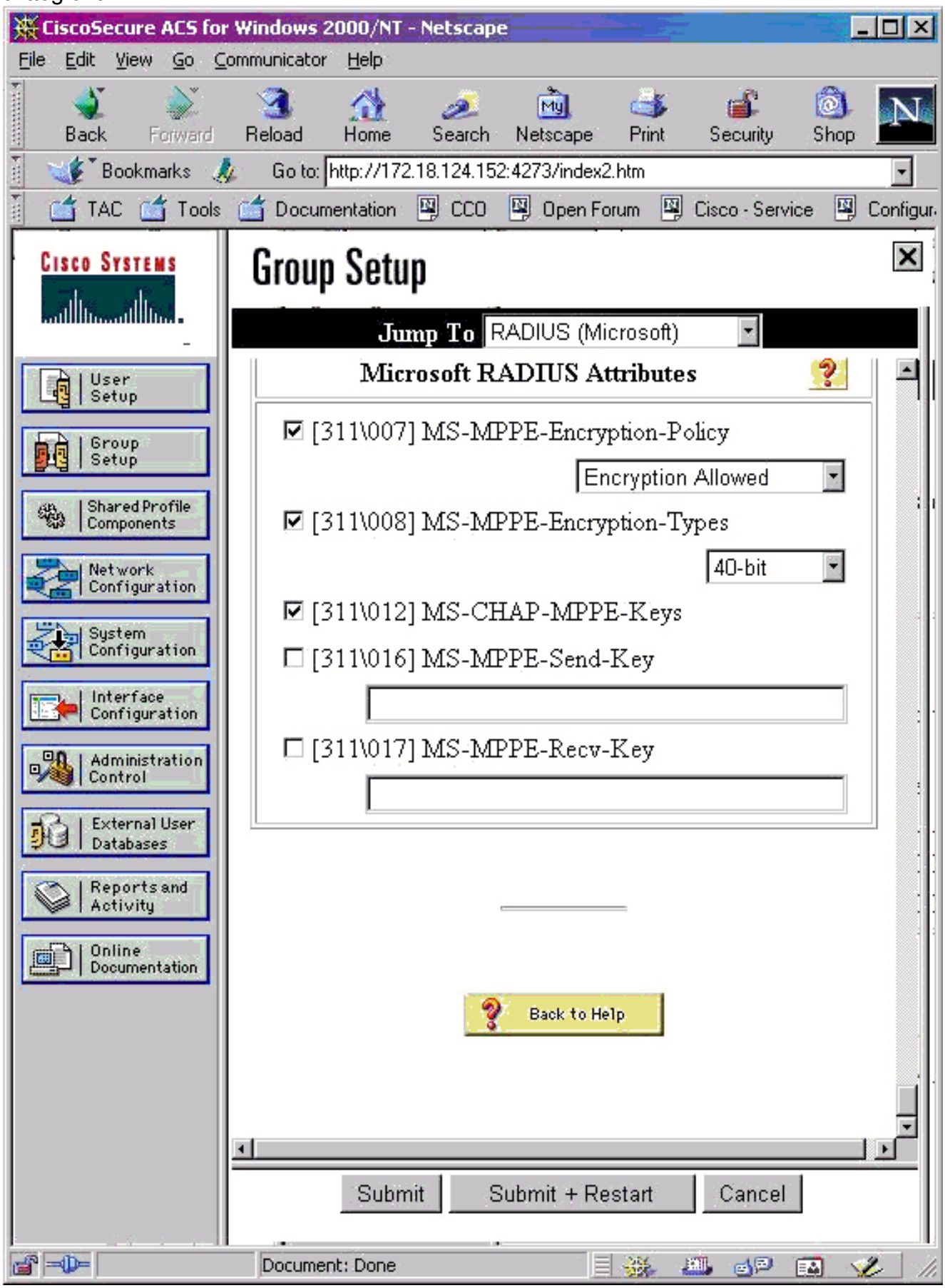


2. Aprire **Configurazione interfaccia > RADIUS (Microsoft)** e controllare gli attributi MPPE in modo che vengano visualizzati nell'interfaccia del gruppo.



3. Aggiungere un utente. Nel gruppo dell'utente aggiungere gli attributi MPPE [RADIUS (Microsoft)]. È necessario abilitare questi attributi per la crittografia ed è facoltativo quando il PIX non è configurato per la

crittografia.



Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione

funzioni correttamente.

Comandi show PIX (Post Authentication)

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Il comando **show vpdn** elenca le informazioni sul tunnel e sulla sessione.

```
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
```

Verifica PC client

In una finestra di MS-DOS o nella finestra Esegui, digitare **ipconfig /all**. L'output viene visualizzato nella sezione relativa all'adattatore PPP.

```
PPP adapter pptp:

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

Èinoltre possibile fare clic su **Dettagli** per visualizzare le informazioni nella connessione PPTP.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

- Deve essere disponibile la connettività per GRE (Generic Routing Encapsulation) e TCP 1723 dal PC all'endpoint del tunnel PIX. Se esiste la possibilità che questo sia bloccato da un firewall o da un elenco degli accessi, spostare il PC più vicino al PIX.

- Windows 98 e Windows 2000 PPTP sono i più semplici da configurare. In caso di dubbi, provare più PC e sistemi operativi. Una volta stabilita la connessione, fare clic su **Details** (Dettagli) sul PC per visualizzare le informazioni sulla connessione. Ad esempio, se si utilizza PAP, CHAP, IP, crittografia e così via.
- Se si intende utilizzare RADIUS e/o TACACS+, provare prima a configurare l'autenticazione locale (nome utente e password sul PIX). Se l'operazione non riesce, l'autenticazione con un server RADIUS o TACACS+ non funziona.
- Inizialmente, accertarsi che le impostazioni di sicurezza sul PC consentano il maggior numero possibile di tipi di autenticazione diversi (PAP, CHAP, MS-CHAP) e deselezionare la casella di controllo **Richiedi crittografia dati** (renderlo opzionale sia sul PIX che sul PC).
- Poiché il tipo di autenticazione è negoziato, configurare il PIX con il massimo numero di possibilità. Ad esempio, se il PC è configurato solo per MS-CHAP e il router solo per PAP, non vi è mai alcun accordo.
- Se il PIX funge da server PPTP per due posizioni diverse e ogni posizione dispone di un proprio server RADIUS all'interno, l'utilizzo di un singolo PIX per entrambe le posizioni servite dal proprio server RADIUS non è supportato.
- Alcuni server RADIUS non supportano MPPE. Se un server RADIUS non supporta la codifica MPPE, l'autenticazione RADIUS funziona, ma la crittografia MPPE non funziona.
- In Windows 98 o versioni successive, quando si utilizza PAP o CHAP, il nome utente inviato al PIX è identico a quello immesso nella connessione DUN (Dial-Up Networking). Tuttavia, quando si utilizza MS-CHAP, il nome di dominio può essere aggiunto alla parte anteriore del nome utente, ad esempio:Nome utente immesso in DUN - "cisco"Dominio impostato sulla confezione di Windows 98 - "DOMINIO"Nome utente MS-CHAP inviato a PIX - "DOMAIN\cisco"Nome utente su PIX - "cisco"Risultato - Nome utente/password non validiQuesta è una sezione del registro PPP da un PC con Windows 98 che mostra il comportamento.

```
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.
```

Se si utilizza Windows 98 e MS-CHAP per il PIX, oltre a disporre del nome utente non di dominio, è possibile aggiungere "DOMINIO\nomeutente" al PIX:

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

Nota: se si esegue l'autenticazione remota su un server AAA, vale la stessa cosa.

Comandi per la risoluzione dei problemi

Per informazioni sulla sequenza di eventi PPTP prevista, vedere la RFC 2637 di PPTP. Sul PIX, gli eventi significativi in una buona sequenza PPTP mostrano:

```
SCCRQ (Start-Control-Connection-Request)
SCCRP (Start-Control-Connection-Reply)
```

```
OCRQ (Outgoing-Call-Request)
OCRP (Outgoing-Call-Reply)
```

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

Comandi PIX debug

- **debug ppp io**: visualizza le informazioni sul pacchetto per l'interfaccia virtuale PPTP PPP.
- **debug ppp error**: visualizza gli errori di protocollo e le statistiche sugli errori associate alla negoziazione e al funzionamento della connessione PPP.
- **debug vpdn error**: visualizza gli errori che impediscono di stabilire un tunnel PPP o gli errori che causano la chiusura di un tunnel stabilito.
- **debug vpdn packet**: visualizza gli errori e gli eventi L2TP che fanno parte della normale procedura di impostazione del tunnel o di arresto delle VPDN.
- **debug vpdn events**: visualizza i messaggi relativi agli eventi che fanno parte della normale creazione o chiusura del tunnel PPP.
- **debug ppp auth**: visualizza i messaggi di debug dell'autenticazione utente AAA dell'interfaccia virtuale PPTP PPP.

Comandi PIX clear

Questo comando deve essere emesso in modalità config.

- **clear vpdn tunnel [all | *[id_tunnel]*]**: rimuove uno o più tunnel PPTP dalla configurazione.

Attenzione: *non* usare il comando **clear vpdn**. In questo modo vengono eliminati *tutti* i comandi vpdn.

Abilita registrazione PPP sul PC client

Completare queste istruzioni per attivare il debug PPP per diversi sistemi operativi Windows e Microsoft.

Windows 95

Per abilitare la registrazione PPP su un computer con Windows 95, procedere come segue.

1. Nell'opzione Rete del Pannello di controllo fare doppio clic su **Microsoft Dial-Up Adapter** nell'elenco dei componenti di rete installati.
2. Fare clic sulla scheda **Avanzate**. Nell'elenco Proprietà fare clic sull'opzione **Registra file registro A** e nell'elenco Valore fare clic su **Sì**. Quindi fare clic su **OK**.
3. Arrestare e riavviare il computer per rendere effettiva l'opzione. Il registro viene salvato in un file denominato ppplog.txt.

Windows 98

Per abilitare la registrazione PPP su un computer con Windows 98, procedere come segue.

1. In **Accesso remoto** fare clic sull'icona di una connessione e quindi selezionare **File >**

Proprietà.
2. Fare clic sulla scheda Tipi di server.
3. Selezionare l'opzione **Registra un file registro per questa connessione**. Il file di log si trova in C:\Windows\ppplog.txt

Windows 2000

Per abilitare la registrazione PPP su un computer Windows 2000, andare alla pagina di supporto Microsoft e cercare "Abilita registrazione PPP in Windows".

Windows NT

Per abilitare la registrazione PPP su un sistema NT, eseguire la procedura seguente.

1. Individuare la chiave **SYSTEM\CurrentControlSet\Services\RasMan\PPP** e modificare **Log** da 0 a **1**. In questo modo viene creato un file denominato PPP.LOG nella directory <winnt root>\SYSTEM32\RAS.
2. Per eseguire il debug di una sessione PPP, abilitare innanzitutto la registrazione e quindi avviare la connessione PPP. Quando la connessione si interrompe o si chiude, esaminare il file PPP.LOG per verificare l'operazione eseguita.

Per ulteriori informazioni, vedere la pagina di supporto Microsoft e cercare "Abilitazione della registrazione PPP in Windows NT".

Altri problemi relativi a Microsoft

Di seguito sono elencati diversi problemi relativi a Microsoft da considerare per la risoluzione dei problemi PPTP. Informazioni dettagliate sono disponibili nella Microsoft Knowledge Base tramite i collegamenti forniti.

- Come mantenere attive le connessioni RAS dopo la disconnessioneLe connessioni del Servizio di accesso remoto Windows (RAS) vengono disconnesse automaticamente quando si esegue la disconnessione da un client RAS. È possibile rimanere connessi abilitando la chiave del Registro di sistema KeepRasConnections nel client RAS.
- L'Utente Non Viene Avvisato Quando Accede Con Credenziali Memorizzate Nella CacheSe si accede a un dominio da una workstation basata su Windows o da un server membro e non è possibile individuare il controller di dominio, non verrà visualizzato alcun messaggio di errore per segnalare il problema. È stato invece eseguito l'accesso al computer locale utilizzando le credenziali memorizzate nella cache.
- Come scrivere un file LMHOSTS per la convalida del dominio e altri problemi di risoluzione dei nomiSe si verificano problemi di risoluzione dei nomi sulla rete TCP/IP, è necessario utilizzare i file Lmhosts per risolvere i nomi NetBIOS. Per creare un file Lmhosts da utilizzare nella risoluzione dei nomi e nella convalida del dominio, è necessario seguire una procedura specifica.

Output di esempio del comando debug

Debug PIX - Autenticazione locale

L'output del comando debug visualizza gli eventi significativi in *corsivo*.

```
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:
3081880b00170000000000010000000001ff03c0210101... 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:
3081880b00110000000000020000000001ff03c0210401... 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:
ff03c0210102000e050600011372107020802 PPP xmit, ifc = 0, Len: 18 data:
ff03c0210202000e050600011372107020802 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:
3081880b00120000000000030000000003ff03c0210202... 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: 3081880b00060000000000005000000004c22303010004 outside
PPTP: Recvd xGRE pak from 99.99.99.5, Len 58, seq 5, ack 5 PPP rcvd, ifc = 0, pppdev: 1, Len:
44, data: ff038021010100280206002d0f010306000000008106... PPP xmit, ifc = 0, Len: 14 data:
ff0380210101000a030663636302 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP:
Sending xGRE pak to 99.99.99.5, Len 28, seq 6, ack 5, data:
3081880b000c0000000000060000000580210101000a... PPP xmit, ifc = 0, Len: 38 data:
ff038021040100220206002d0f018106000000008206... Interface outside - PPTP xGRE: Out paket, PPP
Len 36 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 52, seq 7, ack 5, data:
3081880b00240000000000070000000580210401002 2... outside PPTP: Recvd xGRE pak from 99.99.99.5,
Len 29, seq 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 19, data:
ff0380fd0101000f120601000011105000104 PPP xmit, ifc = 0, Len: 8 data: ff0380fd01010004
Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE pak to
99.99.99.5, Len 22, seq 8, ack 6, data: 3081880b00060000000000080000000680fd01010004 PPP xmit,
```

ifc = 0, Len: 19 data: ff0380fd0401000f120601000011105000104 Interface outside - PPTP xGRE: Out paket, PPP Len 17 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 33, seq 9, ack 6, data: 3081880b0011000000000009000000680fd0401000f... 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...
```

Debug PIX - Autenticazione RADIUS

L'output del comando debug visualizza gli eventi significativi in *corsivo*.

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

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

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

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

SCCRQ = Start-Control-Connection-Request - message code bytes 9 & 10 = 0001 Tnl 9 PPTP: CC I
009c00011a2b3c4d000100000100000000000010000... Tnl 9 PPTP: CC I SCCRQ Tnl 9 PPTP: protocol
version 0x100 Tnl 9 PPTP: framing caps 0x1 Tnl 9 PPTP: bearer caps 0x1 Tnl 9 PPTP: max channels
0 Tnl 9 PPTP: firmware rev 0x870 Tnl 9 PPTP: hostname "" Tnl 9 PPTP: vendor "Microsoft Windows
NT" Tnl 9 PPTP: SCCRQ-ok -> state change wt-sccrq to estabd SCCRP = Start-Control-Connection-
Reply - message code bytes 9 & 10 = 0002 Tnl 9 PPTP: CC O SCCRP PPTP: cc snddata, socket FD=1,
Len=156, data: 009c00011a2b3c4d000200000100010000000000030000... PPTP: cc waiting for input, max
soc FD = 1 PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0
PPTP: cc rcv 168 bytes of data OCRQ = Outgoing-Call-Request - message code bytes 9 & 10 = 0007
Tnl 9 PPTP: CC I 00a800011a2b3c4d000700004000e4f50000012c05f5... Tnl 9 PPTP: CC I OCRQ Tnl 9
PPTP: call id 0x4000 Tnl 9 PPTP: serial num 58613 Tnl 9 PPTP: min bps 300:0x12c Tnl 9 PPTP: max
BPS 100000000:0x5f5e100 Tnl 9 PPTP: bearer type 3 Tnl 9 PPTP: framing type 3 Tnl 9 PPTP: recv
win size 64 Tnl 9 PPTP: ppd 0 Tnl 9 PPTP: phone num Len 0 Tnl 9 PPTP: phone num "" Tnl/Cl 9/9
PPTP: l2x store session: tunnel id 9, session id 9, hash_ix=9 PPP virtual access open, ifc = 0
Tnl/CL 9/9 PPTP: vacc-ok -> state change wt-vacc to estabd OCRP = Outgoing-Call-Reply - message
code bytes 9 & 10 = 0008 Tnl/CL 9/9 PPTP: CC O OCRP PPTP: cc snddata, socket FD=1, Len=32, data:
002000011a2b3c4d000800000009400001000000000fa... PPTP: cc waiting for input, max soc FD = 1
outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 60, seq 0 PPP rcvd, ifc = 0, pppdev: 1, Len:
48, data: ff03c0210100002c0506447e217e070208020d030611... PPP xmit, ifc = 0, Len: 23 data:
ff03c021010100130305c2238005065a899b2307020802 Interface outside - PPTP xGRE: Out paket, PPP Len
23 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 39, seq 1, ack 0, data:
3081880b00174000000000010000000ff03c0210101... PPP xmit, ifc = 0, Len: 38 data:
ff03c021040000220d030611040064e131701beb613cb.. . Interface outside - PPTP xGRE: Out paket, PPP
Len 38 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 54, seq 2, ack 0, data:
3081880b00264000000000002000000000ff03c0210400... PPTP: soc select returns rd mask = 0x2 PPTP: cc
rcvdata, socket FD=1, new_conn: 0 PPTP: cc rcv 24 bytes of data Tnl 9 PPTP: CC I
001800011a2b3c4d000f0000000900000ffffffffffff... 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:
3081880b0012400000000000300000002ff03c0210201... 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:
3081880b000f400000000004000000002c2230101000d... 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: ff03c2230201003a3100000000000000000000000000000...
uauth_mschap_send_req: pppdev=1, ulen=4, user=john 6031 uauth_mschap_proc_reply: pppdev = 1,
status = 1 PPP xmit, ifc = 0, Len: 8 data: ff03c22303010004 Interface outside - PPTP xGRE: Out
paket, PPP Len 6 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 22, seq 5, ack 5, data:
3081880b000640000000000500000005c22303010004 CHAP peer authentication succeeded for john outside
PPTP: Recvd xGRE pak from 10.44.17.104, Len 72, seq 6 PPP rcvd, ifc = 0, pppdev: 1, Len: 62,
data: ff03c2230201003a3100000000000000000000000000000... PPP xmit, ifc = 0, Len: 8 data:
ff03c22303010004 Interface outside - PPTP xGRE: Out paket, PPP Len 6 outside PPTP: Sending xGRE
pak to 10.44.17.104, Len 22, seq 6, ack 6, data: 3081880b000640000000000600000006c22303010004
outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 7, ack 5 PPP rcvd, ifc = 0, pppdev:
1, Len: 14, data: ff0380fd0104000a120601000001 PPP xmit, ifc = 0, Len: 14 data:
ff0380fd0101000a120601000020 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP:
Sending xGRE pak to 10.44.17.104, Len 28, seq 7, ack 7, data:
3081880b000c400000000007000000780fd0101000a... 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:
3081880b000c400000000008000000780fd0304000a... 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:
3081880b000c400000000009000000080210101000a... 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:
3081880b001e40000000000a000000080210405001c... outside PPTP: Recvd xGRE pak from 10.44.17.104,
Len 28, seq 9, ack 7 PPP rcvd, ifc = 0, pppdev: 1, Len: 14, data: ff0380fd0201000a120601000020
outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 28, seq 10, ack 8 PPP rcvd, ifc = 0, pppdev:
1, Len: 14, data: ff0380fd0106000a120601000020 PPP xmit, ifc = 0, Len: 14 data:
ff0380fd0206000a120601000020 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP:
Sending xGRE pak to 10.44.17.104, Len 28, seq 11, ack 10, data:
3081880b000c400000000000b0000000a80fd0206000a... 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:
3081880b000c400000000000c0000000c80210307000a... 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:
3081880b000c400000000000d0000000d80210308000a... 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: 3081880b000c400000000000e0000000e80210209000a... 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...
```

Problemi che possono verificarsi

Tunnel PPTP simultaneo

Non è possibile connettere più di 127 connessioni con PIX 6.x e viene visualizzato questo messaggio di errore:

%PIX-3-213001: Errore di accettazione I/O del socket del daemon di controllo PPTP, errno = 5

Soluzione:

In PIX 6.x è previsto un limite hardware di 128 sessioni simultanee. Se ne si sottrae uno per il socket di ascolto PPTP, il numero massimo è 127 connessioni.

PIX e PC non possono negoziare l'autenticazione

I protocolli di autenticazione PC sono impostati per quelli che il PIX non è in grado di eseguire (Shiva Password Authentication Protocol (SPAP) e Microsoft CHAP versione 2 (MS-CHAP v.2) anziché versione 1). Il PC e PIX non sono in grado di accordarsi sull'autenticazione. Il PC visualizza questo messaggio:

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

PIX e PC non possono negoziare la crittografia

Il PC è impostato **solo** per **Encrypted** e il comando **vpdn group 1 ppp encrypt mppe 40 required** viene eliminato dal PIX. Il PC e PIX non sono in grado di accettare la crittografia e il PC visualizza questo messaggio:

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

PIX e PC non possono negoziare la crittografia

Il PIX è impostato per il **gruppo vpdn 1 ppp, la crittografia mppe 40 è obbligatoria** e per il PC non è consentita la crittografia. Ciò non genera messaggi sul PC, ma la sessione si disconnette e il debug PIX visualizza questo output:

```
PPTP: Call id 8, no session id protocol: 21,
    reason: mppe required but not active, tunnel terminated
```

```
603104: PPTP Tunnel created, tunnel_id is 8,
    remote_peer_ip is 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
```

Problema PIX MPPE RADIUS

Il PIX è impostato per il **gruppo vpdn 1 ppp, è necessario crittografare mppe 40** e il PC per la crittografia consentito con l'autenticazione su un server RADIUS non restituisce la chiave MPPE. Il PC visualizza questo messaggio:

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

Il debug PIX mostra:

```
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
```

Il PC visualizza questo messaggio:

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

Informazioni correlate

- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- Soluzioni per la risoluzione dei problemi più comuni di VPN IPSec di L2L e ad accesso remoto
- Pagina di supporto PPTP
- RFC 2637: Protocollo PPTP (Point-to-Point Tunneling Protocol)
- RFC (Requests for Comments)
- Supporto tecnico – Cisco Systems