PIX 6.x: PPTP con el ejemplo de configuración de la autenticación de RADIUS

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Configurar
Diagrama de la red
Extremidades de la configuración para el firewall PIX
Configure la característica PPTP en el cliente PC
Windows 98
Windows 2000
Windows NT
Configure el PIX
Configuración de PIX - Autenticación local con encripción
Configuración de Autenticación PIX - RADIUS con encripción
3.0 del Cisco Secure ACS for Windows de la configuración
Autenticación de RADIUS con encripción
Verificación
Comandos show PIX (Post autenticación)
Verificación de PC de cliente
Troubleshooting
Comandos para resolución de problemas
Apertura de sesión del permiso PPP PC del cliente
Temas adicionales de Microsoft
Ejemplo de resultado del comando debug
Qué Puede Salir Mal
Información Relacionada

Introducción

Point-to-Point Tunneling Protocol (PPTP) es un protocolo de tunelización de Capa 2 que permite a un cliente remoto utilizar una red IP pública para comunicarse de forma segura con los servidores de una red corporativa privada. PPTP se conecta por túneles al IP. El PPTP se describe en RFC2637 . El soporte de PPTP en el Firewall PIX se agregó en la versión 5.1 del Software PIX. La documentación sobre PIX proporciona más información sobre PPTP y su uso con el PIX. En este documento se describe cómo configurar PIX para utilizar PPTP con autenticación local,

TACACS+ y RADIUS. Este documento también proporciona consejos y ejemplos que puede utilizar como ayuda para resolver problemas comunes.

Este documento muestra cómo configurar las conexiones PPTP al PIX. Para configurar un PIX o un ASA para permitir el PPTP *a través del* dispositivo de seguridad, refiera a las conexiones de permiso PPTP/L2TP con el PIX.

Refiera al Cisco Secure PIX Firewall 6.x y al servidor de RADIUS 3.5 para Windows con el Microsoft Windows 2000 y la autenticación de RADIUS de 2003 IAS para configurar el firewall PIX y al cliente VPN para el uso con el Windows 2000 y 2003 del Cliente Cisco VPN del Internet Authentication Service (IAS).

Refiera a configurar el concentrador VPN 3000 y el PPTP con la autenticación de RADIUS del Cisco Secure ACS for Windows para configurar el PPTP en un concentrador VPN 3000 con el Cisco Secure ACS for Windows para la autenticación de RADIUS.

Refiera a configurar la autenticación PPTP del router del Cisco Secure ACS for Windows para configurar una conexión de PC al router, que entonces proporciona la autenticación de usuario al Cisco Secure Access Control System (ACS) 3.2 para el Servidor Windows, antes de que usted permita al usuario en la red.

Nota: En los términos PPTP, por el RFC, el PPTP Network Server (PNS) es el servidor (en este caso, el PIX, o el callee) y el PPTP Access Concentrator (PAC) es el cliente (el PC, o el llamador).

Nota: El Túnel dividido no se soporta en el PIX para los clientes PPTP.

Nota: El PIX 6.x necesita el v1.0 MS-CHAP para que el PPTP trabaje. Windows Vista no soporta el v1.0 MS-CHAP. El PPTP en PIX 6.x no trabajará tan para Windows Vista. El PPTP no se soporta en la versión de PIX 7.x y posterior.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el Software Release 6.3(3) del Cisco Secure PIX Firewall.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

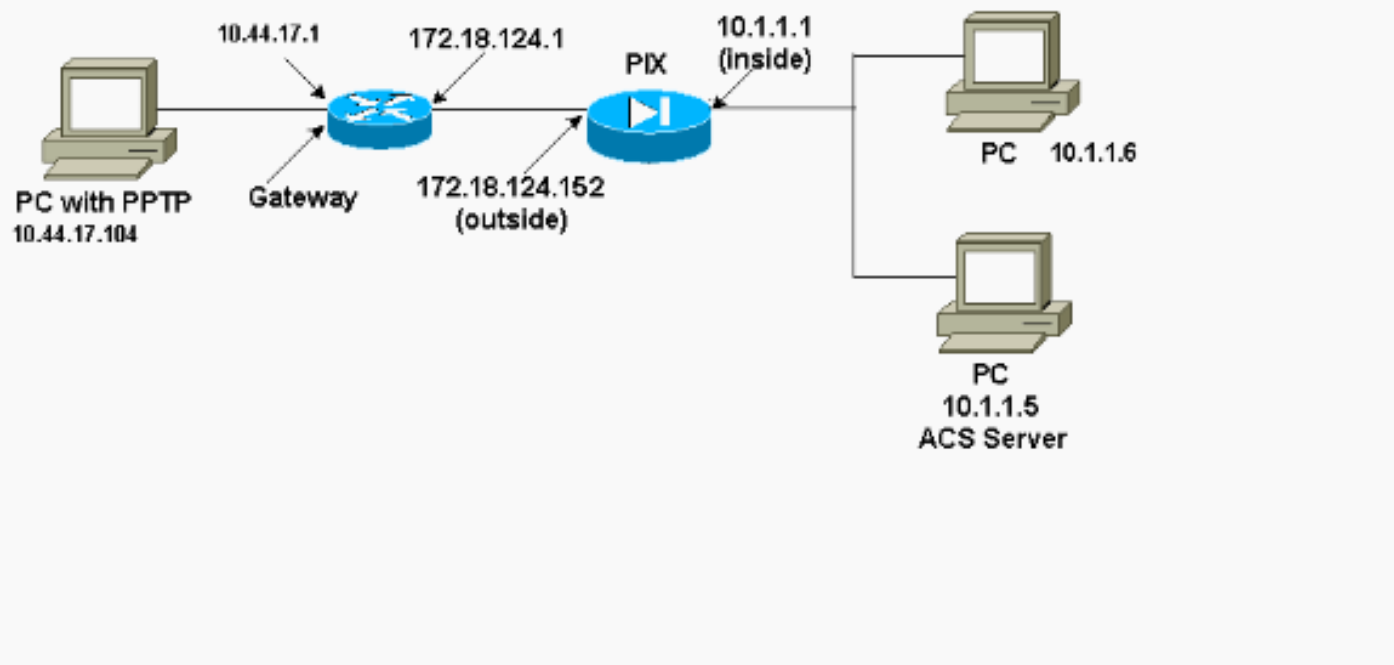
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

Este documento utiliza esta configuración de red:



Extremidades de la configuración para el firewall PIX

Tipo de autenticación - CHAP, PAP, MS-CHAP

El PIX configurado para los tres métodos de autentificación (GRIETA, PAP, MS-CHAP) al mismo tiempo proporciona la mejor ocasión de conectar no importa cómo se configura el PC. Esto es una buena idea para los propósitos de Troubleshooting.

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

Microsoft Point-to-Point Encryption (MPPE)

Utilice esta sintaxis de los comandos para configurar la encripción MPPE en el firewall PIX.

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

En este comando, **requerido** es una palabra clave optativa. Debe configurarse el MS-CHAP.

Configure la característica PPTP en el cliente PC

Nota: La información disponible aquí en relacionado a la configuración del software Microsoft no viene con ninguna garantía o soporte para el software Microsoft. El soporte para el software Microsoft es disponible desde Microsoft y en el sitio Web de soporte técnico de Microsoft .

Windows 98

Siga los siguientes pasos para instalar la característica PPTP en Windows 98.

1. Seleccione Start (Inicio) > Settings (Configuraciones) > Control Panel (Panel de control) > Add New Hardware (Agregar nuevo hardware). Haga clic en Next (Siguiente).
2. Haga clic en Select from List (Seleccionar de la lista) y elija Network Adapter (Adaptador de red). Haga clic en Next (Siguiente).
3. Elija Microsoft en el panel izquierdo y Microsoft VPN Adapter en el derecho.

Siga los siguientes pasos para configurar la característica PPTP.

1. Seleccione Start (Inicio) > Programs (Programas) > Accessories (Accesorios) > Communications (Comunicaciones) > Dial Up Networking (Interconexión de redes de marcación manual).
2. Haga clic el **Make New Connection**. Para **Select un dispositivo**, conecta con el **adaptador VPN de Microsoft**. La dirección IP del servidor VPN es el punto final del túnel PIX.
3. La autenticación predeterminada de Windows 98 utiliza la encripción de contraseña (GRIETA o MS-CHAP). Para cambiar el PC también para permitir el PAP, seleccione el **Properties (Propiedades) > Server Types (Tipos de servidor)**. Anule la selección de Require encrypted password. Puede configurar un cifrado de datos (MPPE o no) en esta área.

Windows 2000

Siga los siguientes pasos para configurar la característica PPTP en el Windows 2000.

1. Seleccione el **Start (Inicio) > Programs (Programas) > Accessories (Accesorios) > Communications (Comunicaciones) > Network and Dialup Connections (Conexiones de red y de marcado manual)**.
2. Haga clic en Make new connection (Establecer una conexión nueva) y luego en Next (Siguiente).
3. Seleccione Connect to a private network through the Internet and Dial a connection prior (Conectarse a una red privada a través de Internet y Marcar una conexión antes)[No seleccione esta opción si tiene una LAN]. Haga clic en Next (Siguiente).
4. Ingrese el nombre del host o la dirección IP de punto final del túnel (PIX/router).
5. Si necesita cambiar el tipo de contraseña, seleccione Properties (Propiedades)> Security for the connection (Seguridad para la conexión)> Advanced (Avanzada). El valor predeterminado es MS-CHAP y MS-CHAP v2 (no CHAP o PAP). Puede configurar un cifrado de datos (MPPE o no) en esta área.

Windows NT

Refiera a instalar, a configurar, y a usar el PPTP con los clientes Microsoft y los servidores para configurar a los clientes de NT para el PPTP.

Configure el PIX

Configuración de PIX - Autenticación local sin encripción

```
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
```

Configuración de PIX - Autenticación local con encripción

Si usted agrega este comando a la configuración PIX - la configuración de la autenticación local, del no encryption, el PC y el PIX no autonegocian el cifrado 40-bit o ninguno (basado en las configuraciones PC).

vpdn group 1 ppp encryption mppe auto

Si el PIX tiene la característica 3DES habilitada, el **comando show version** visualiza este mensaje.

- Versiones 6.3 y posterior:`VPN-3DES-AES: Enabled`
- Versiones 6.2 y anterior:`VPN-3DES: Enabled`

La encriptación en 128 bits también es posible. Sin embargo, si uno de estos mensajes se visualiza, después el PIX no se habilita para el cifrado del 128-bit.

- Versiones 6.3 y posterior:`Warning: VPN-3DES-AES license is required for 128 bits MPPE encryption`
- Versiones 6.2 y anterior:`Warning: VPN-3DES license is required for 128 bits MPPE encryption`

El sintaxis para el comando mppe se muestra aquí.

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

La PC y el PIX se deben configurar para autenticación de MS-CHAP junto con MPPE.

Configuración de PIX - Autenticación TACACS+/RADIUS sin encripción

```
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]
```

Configuración de Autenticación PIX - RADIUS con encripción

Si se utiliza el RADIUS, y si el servidor de RADIUS (atributo específico del proveedor 26, Microsoft como vendedor) soporta la codificación MPPE, la encripción MPPE puede ser agregada. La autenticación TACACS+ no funciona con el encripción debido a que los servidores TACACS+ no pueden devolver claves MPPE espaciales. El Cisco Secure ACS for Windows 2.5 y posterior RADIUS soporta el MPPE (todos los servidores de RADIUS no soportan el MPPE).

Con la suposición que los trabajos de la autenticación de RADIUS sin el cifrado, agregan el cifrado incluyendo este comando en la configuración previa:

vpdn group 1 ppp encryption mppe auto

El PC y el PIX no autonegocia el cifrado 40-bit o ninguno (basado en las configuraciones PC).

Si el PIX tiene la característica 3DES habilitada, el **comando show version** visualiza este mensaje.

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

La encriptación en 128 bits también es posible. Sin embargo, si se visualiza este mensaje, el PIX no se habilita para el cifrado del 128-bit.

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

El sintaxis para el comando mppe se muestra en esta salida.

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

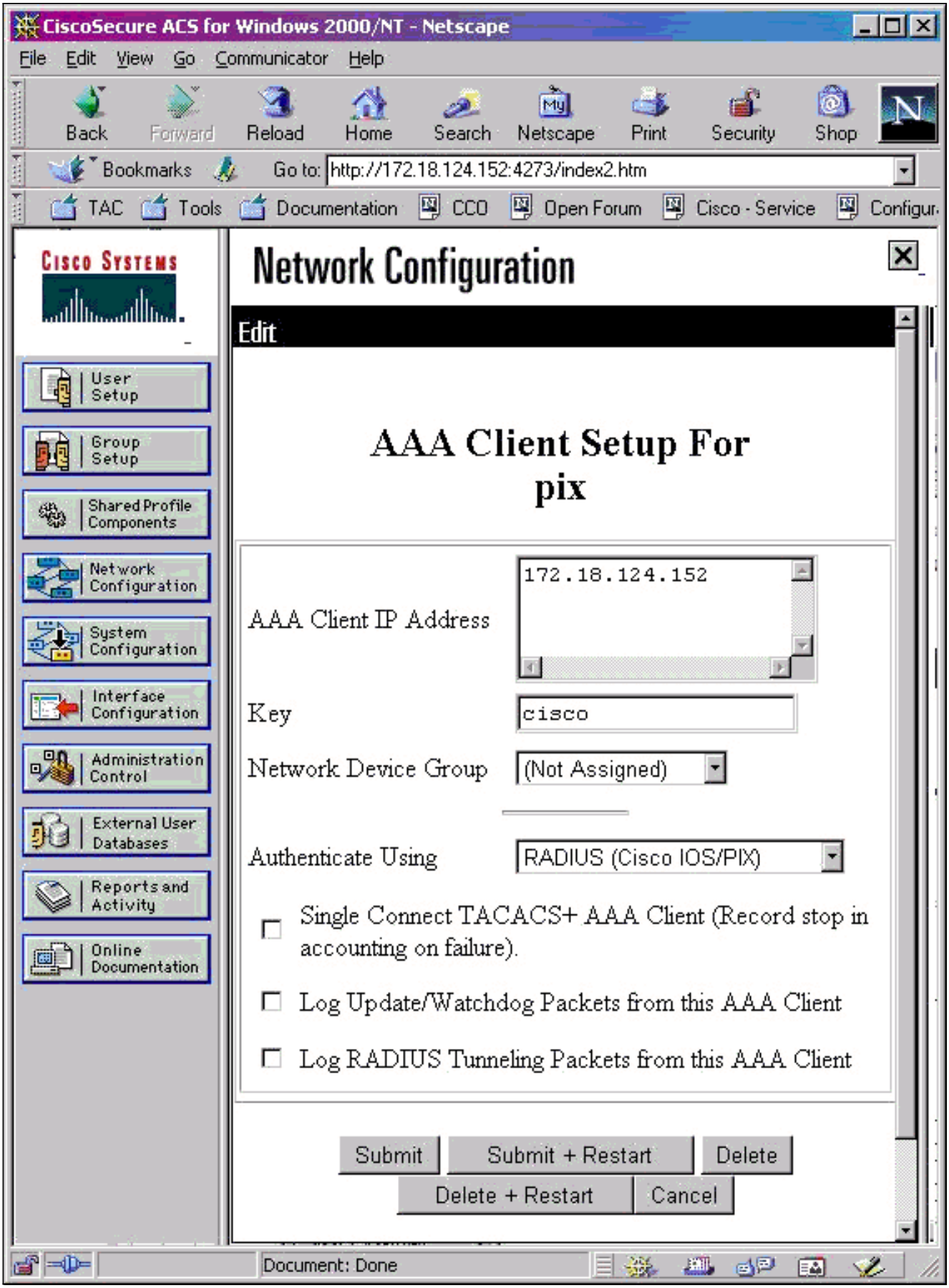
La PC y el PIX se deben configurar para autenticación de MS-CHAP junto con MPPE.

3.0 del Cisco Secure ACS for Windows de la configuración

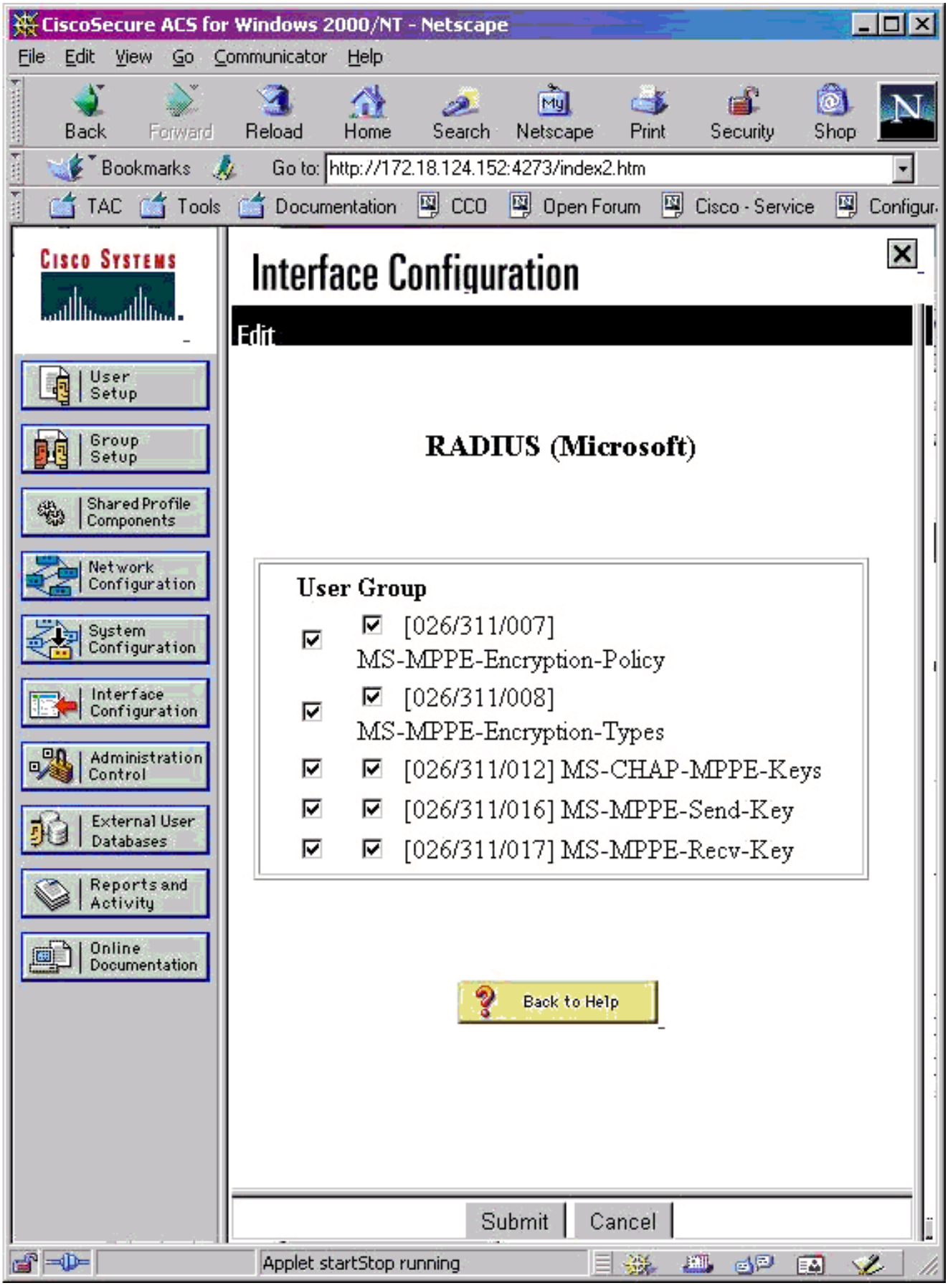
Autenticación de RADIUS con encripción

Utilice estos pasos para configurar el 3.0 del Cisco Secure ACS for Windows. Los pasos de la misma configuración se aplican a los ACS versión 3.1 y 3.2.

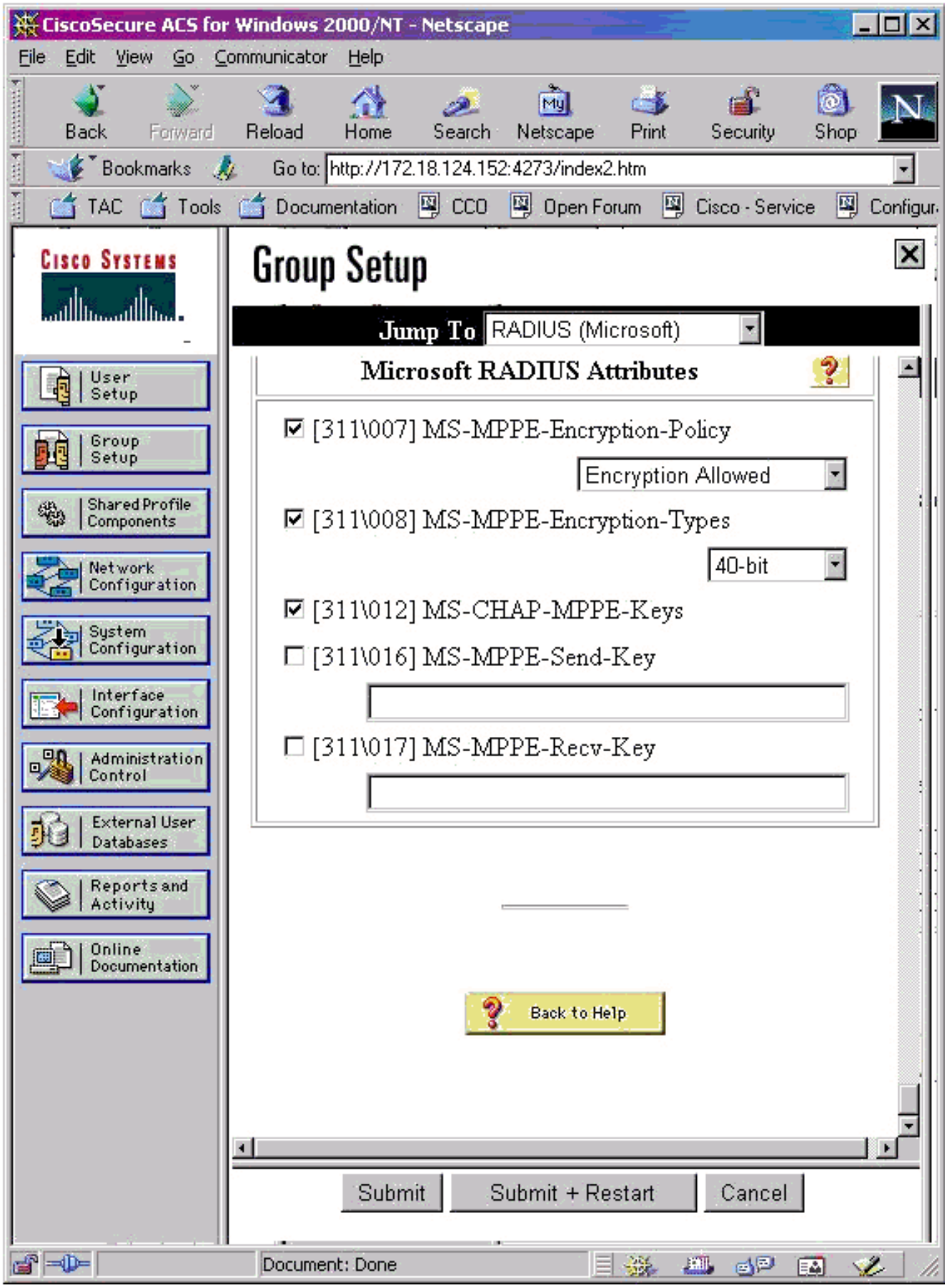
1. Agregue el PIX al Secure ACS de Cisco para la configuración de redes del servidor Windows e identifique el tipo de diccionario como RADIUS (IOS/PIX de Cisco).



2. **La configuración de la** interfaz abierta **> el RADIUS (Microsoft)** y marcan los atributos MPPE para hacer que aparecen en la interfaz de grupo.



3. Agregue a un usuario. En el grupo de usuario, agregue el [RADIUS (Microsoft)] MPPE atributos. Usted debe habilitar estos atributos para el cifrado y es opcional cuando el PIX no se configura para el
cifrado.



Verificación

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

Comandos show PIX (Post autenticación)

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Las listas de **comando show vpdn** hacen un túnel y información de la sesión.

```
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
```

Verificación de PC de cliente

En una ventana de MS-DOS, o de la ventana del funcionamiento, **ipconfig /all del** tipo. La porción del adaptador PPP muestra esta salida.

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

Usted puede también hacer clic los **detalles** para ver la información en la conexión PPTP.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

- Debe haber Conectividad para el Generic Routing Encapsulation (GRE) y el TCP 1723 del PC al punto final del túnel PIX. Si hay cualquier ocasión que esto es bloqueada por un Firewall o una lista de acceso, mueva el PC más cercano al PIX.
- Windows 98 y el Windows 2000 PPTP son los más fáciles de configurar. Si es dudoso, intente con PCs y sistemas operativos. Después de una conexión satisfactoria, haga clic los **detalles** en el mostrar información PC para sobre la conexión. Por ejemplo, si usted utiliza el PAP, GRIETA, IP, cifrado, y así sucesivamente.
- Si usted se prepone utilizar el RADIUS y/o el TACACS+, intente configurar (nombre de usuario y contraseña en el PIX) la autenticación local primero. Si esto no trabaja, la autenticidad con un servidor RADIUS o TACACS+ no trabaja.
- Inicialmente, aseegurese los ajustes de seguridad en el PC permitir tantos diversos tipos de autenticación como posible (PAP, GRIETA, MS-CHAP) y desmarcar el cuadro para la **encripción de datos Require** (haga le opcionales ambos en el PIX y el PC).
- Dado que el tipo de autenticación se negocia, configure PIX con la mayor cantidad de posibilidades. Por ejemplo, si el PC se configura para solamente el MS-CHAP y el router para

solamente el PAP, nunca hay cualquier acuerdo.
- Si el PIX actúa como servidor PPTP para dos ubicaciones diferentes y cada ubicación tiene su propio servidor de RADIUS en el interior, usando un solo PIX para ambas ubicaciones mantenidas por su propio servidor de RADIUS no se soporta.
- Algunos servidores RADIUS no admiten MPPE. Si un servidor de RADIUS no soporta la codificación MPPE, la autenticación de RADIUS trabaja, pero la encripción MPPE no trabaja.
- Con Windows 98 o posterior, cuando use PAP o CHAP, el nombre de usuario enviado al PIX es idéntico al que es ingresado en la conexión de red Dial-Up (DUN). Pero cuando usted utiliza el MS-CHAP, el Domain Name se puede añadir al final del fichero al frente del nombre de usuario, por ejemplo:Nombre de usuario ingresado en el DUN - “Cisco”Conjunto de dominios en el cuadro de Windows 98 - “DOMINIO”Nombre de usuario MS-CHAP enviado al PIX - “DOMINIO \ Cisco”Nombre de usuario en el PIX - “Cisco”Resultado - Nombre de usuario inválido/contraseñaÉsta es una sección del registro PPP de Windows 98 PC que muestre el comportamiento.
```
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.
```
Si usted utiliza Windows 98 y MS-CHAP al PIX, además del tener el nombre de usuario sin dominio, usted puede agregar el “DOMINIO \ el nombre de usuario” al PIX:

vpdn username cisco password cisco vpdn username DOMAIN\cisco password cisco **Nota:** Si usted realiza la autenticación remota en un servidor de AAA, lo mismo se aplica.

Comandos para resolución de problemas

La información sobre la secuencia de secuencia esperada de eventos PPTP se encuentra en el RFC 2637 PPTP . En el PIX, los eventos importantes en una buena secuencia PPTP muestran:

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

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Comandos de depuración PIX

- debug ppp io — Muestra la información de paquete para la interfaz virtual PPTP PPP.
- debug ppp error — Muestra los errores de protocolo y las estadísticas de error relacionadas con la negociación y operación de conexiones PPP.
- debug vpdn error — Muestra errores que evitan que se establezca un túnel PPP o errores que provocan que un túnel establecido se cierre.
- debug vpdn packet - Muestra errores L2TP y eventos que son una parte del establecimiento normal de túneles o apagado para las VPDN.
- debug vpdn events — Muestra mensajes relativos a eventos que forman parte del establecimiento o cierre normal del túnel PPP.

- debug ppp uauth - Muestra los mensajes de depuración de autenticación de usuario de AAA de la interfaz virtual de PPTP PPP.

Comandos PIX clear

Este comando se debe publicar en el modo de configuración.

- **túnel del clear vpdn [todo |** [id tunnel_id - Elimina uno o más túneles PPTP de la configuración.

Precaución: No publique el **comando clear vpdn**. Esto limpia todos los comandos vpdn.

Apertura de sesión del permiso PPP PC del cliente

Complete estas instrucciones para girar el debugging de PPP para diversos Windows y sistemas operativos Microsoft.

Windows 95

Siga los siguientes pasos para habilitar el PPP que abre una sesión una máquina de Windows 95.

1. En la opción de red en el panel de control, haga doble clic el **adaptador de dial up de Microsoft** en las listas de componentes de red instalados.
2. Haga clic en la ficha Advanced (Opciones avanzadas). En la lista de propiedades, haga clic la opción nombrada el **expediente un archivo del registro**, y en la lista de valor, tecleo **sí**. Luego haga clic en OK (Aceptar).
3. Cierre y reinicie la computadora para que se aplique esta opción. El registro se guarda en un archivo denominado ppplog.txt.

Windows 98

Siga los siguientes pasos para habilitar el PPP que abre una sesión una máquina de Windows 98.

1. En el **dial-up networking**, el solo-tecleo un icono de conexión, y entonces selecciona el **File (Archivo) > Properties (Propiedades)**.
2. Haga clic en la ficha Tipo de servidor.
3. Seleccione la opción denominada Record a log file (Inscriba un archivo de registro) para esta conexión. El archivo del registro está situado en C:\Windows\ppplog.txt

Windows 2000

Para habilitar el PPP que abre una sesión una máquina del Windows 2000, ir a la página de soporte y a la búsqueda de Microsoft para el “permiso PPP que abre una sesión Windows.”

Windows NT

Siga los siguientes pasos para habilitar el PPP que abre una sesión un sistema de NT.

1. Localice el sistema de teclado **\ el CurrentControlSet \ los servicios \ RasMan \ PPP** y cambie

el **registro** a partir de la 0 a **1.** Esto crea un archivo llamado PPP.Login el directorio del <winnt root>\SYSTEM32\RAS.

2. Para hacer el debug de una sesión PPP, un primer registro del permiso y después iniciar la conexión PPP. Cuando la conexión falla o se interrumpe, examine PPP.LOG para determinar qué sucedió.

Para más información, refiera a la página de soporte y a la búsqueda de Microsoft para “habilitar el Windows NT de apertura de sesión PPP.”

Temas adicionales de Microsoft

Varios Problemas relacionados con Microsoft a considerar al resolver problemas el PPTP se enumeran aquí. La información detallada se encuentra disponible en la Base de datos de conocimiento de Microsoft en los links proporcionados.

- Cómo Mantener las Conexiones RAS Activas después de Cerrar una SesiónLas conexiones de Windows Remote Access Service (RAS) se desconectan automáticamente cuando cierra una sesión de un cliente RAS. Puede permanecer conectado si activa la clave de registro de KeepRasConnections en el cliente RAS.
- No se Alerta al Usuario cuando se Inicia Sesión con las Credenciales Guardadas en CachéSi usted abre una sesión a un dominio de una estación de trabajo basada en Windows o el servidor miembro y el controlador de dominio no pueden ser localizados, usted no recibe un mensaje de error que indique este problema. En su lugar, se abre una sesión en el equipo local con las credenciales guardadas en caché.
- Cómo Escribir un Archivo LMHOSTS para la Validación de Dominio y Otros Problemas de Resolución de NombreSi usted experimenta los problemas de la resolución de nombre en su red TCP/IP, usted necesita utilizar los archivos de Lmhosts para resolver los nombres de NETBIOS. Usted debe seguir un procedimiento específico para crear un archivo de Lmhosts para utilizar en la resolución de nombre y la validación del dominio.

Ejemplo de resultado del comando debug

PIX debug - Autenticación local

Esta salida de los debugs muestra los eventos importantes en los *itálicos*.

```
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
009c00011a2b3c4d0001000001000000000000010000... Tnl 42 PPTP: CC I SCCRQ Tnl 42 PPTP: protocol
version 0x100 Tnl 42 PPTP: framing caps 0x1 Tnl 42 PPTP: bearer caps 0x1 Tnl 42 PPTP: max
channels 0 Tnl 42 PPTP: firmware rev 0x0 Tnl 42 PPTP: hostname "local" Tnl 42 PPTP: vendor "9x"
Tnl 42 PPTP: SCCRQ-ok -> state change wt-sccrq to estabd SCCRP = Start-Control-Connection-Reply
- message code bytes 9 & 10 = 0002 Tnl 42 PPTP: CC O SCCRP PPTP: cc snddata, socket fd=1,
len=156, data: 009c00011a2b3c4d0002000001000100000000030000... PPTP: cc waiting for input, max
soc FD = 1 PPTP: soc select returns rd mask = 0x2 PPTP: cc rcvdata, socket FD=1, new_conn: 0
PPTP: cc rcv 168 bytes of data OCRQ = Outgoing-Call-Request - message code bytes 9 & 10 = 0007
```

Tnl 42 PPTP: CC I 00a800011a2b3c4d000700000000000000000dac00000... Tnl 42 PPTP: CC I OCRQ Tnl 42 PPTP: call id 0x0 Tnl 42 PPTP: serial num 0 Tnl 42 PPTP: min bps 56000:0xdac0 Tnl 42 PPTP: max bps 64000:0xfa00 Tnl 42 PPTP: bearer type 3 Tnl 42 PPTP: framing type 3 Tnl 42 PPTP: recv win size 16 Tnl 42 PPTP: ppd 0 Tnl 42 PPTP: phone num Len 0 Tnl 42 PPTP: phone num "" Tnl/Cl 42/42 PPTP: l2x store session: tunnel id 42, session id 42, hash_ix=42 PPP virtual access open, ifc = 0 Tnl/Cl 42/42 PPTP: vacc-ok -> state change wt-vacc to estabd *OCRP = Outgoing-Call-Reply - message code bytes 9 & 10 = 0008* Tnl/Cl 42/42 PPTP: CC O OCRP PPTP: cc snddata, socket FD=1, Len=32, data: 002000011a2b3c4d00080000002a00000100000000fa... *!--- Debug following this last event is flow of packets.* PPTP: cc waiting for input, max soc FD = 1 outside PPTP: Recvd xGRE pak from 99.99.99.5, Len 39, seq 1 PPP rcvd, ifc = 0, pppdev: 1, Len: 27, data: ff03c021010100170206000a00000506001137210702... PPP xmit, ifc = 0, Len: 23 data: ff03c021010100130305c22380050609894ab407020802 Interface outside - PPTP xGRE: Out paket, PPP Len 23 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 39, seq 1, ack 1, data: 3081880b00170000000000100000001ff03c0210101... PPP xmit, ifc = 0, Len: 17 data: ff03c0210401000d0206000a00000d0306 Interface outside - PPTP xGRE: Out paket, PPP Len 17 outside PPTP: Sending xGRE pak to 99.99.99.5, Len 33, seq 2, ack 1, data: 3081880b00110000000000020000001ff03c0210401... 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: 3081880b00120000000000030000000 3ff03c0210202... 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: 3081880b00240000000000070000000 5802104010022... 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: 3081880b00060000000000000800000000680fd01010004 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: 3081880b00060000000000000a0000000980fd02020004 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: 3081880b00060000000000000b0000000a80fd06030004 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: ff0380210402001c810600000000820600000000 8306... 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 - Autenticación de RADIUS

Esta salida de los debugs muestra los eventos importantes en los *itálicos*.

```
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: 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: 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 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: 3081880b00124000000000003000000002ff03c0210201... 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 001800011a2b3c4d000f000000900000000000000000... 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: 3081880b000c400000000070000000780fd0101000a... PPP xmit, ifc = 0, Len: 14 data: ff0380fd0304000a120601000020 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 8, ack 7, data: 3081880b000c400000000080000000780fd0304000a... outside PPTP: Recvd xGRE pak from 10.44.17.104, Len 48, seq 8 PPP rcvd, ifc = 0, pppdev: 1, Len: 38, data: ff038021010500220306000000008106000000008206... PPP xmit, ifc = 0, Len: 14 data: ff0380210101000a0306ac127c98 Interface outside - PPTP xGRE: Out paket, PPP Len 12 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 28, seq 9, ack 8, data:

3081880b000c40000000000900000000880210101000a... PPP xmit, ifc = 0, Len: 32 data:
ff0380210405001c810600000000820600000000008306.. . Interface outside - PPTP xGRE: Out paket, PPP
Len 30 outside PPTP: Sending xGRE pak to 10.44.17.104, Len 46, seq 10, ack 8, data:
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...
```

Qué Puede Salir Mal

Túnel simultáneo PPTP

Usted no puede conectar más de 127 conexiones con PIX 6.x, y este mensaje de error aparece:

%PIX-3-213001: El socket io de la daemon del control PPTP valida el error, el errno= 5

Solución:

Hay una limitación del hardware de las sesiones concurrentes 128 en PIX 6.x. Si usted resta uno para el socket que escucha PPTP, las conexiones del número máximo is127.

El PIX y la PC no pueden negociar la autenticación

Los Protocolos de autenticación PC se fijan para unos que el PIX no puede hacer (protocolo de autenticación de contraseña Shiva (SPAP) y Microsoft CHAP versión 2 (MS-CHAP v.2) en vez de la versión 1). El PC y el PIX no pueden estar de acuerdo con la autenticación. El PC visualiza este

mensaje:

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

El PIX y la PC no pueden negociar el encripción

El PC se fija para **cifrado solamente** y borran al **comando vpdn group 1 ppp encrypt mppe 40 required del** PIX. El PC y el PIX no pueden estar de acuerdo con el cifrado y el PC visualiza este mensaje:

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

El PIX y la PC no pueden negociar el encripción

El PIX se fija para el **vpdn group 1 ppp encrypt mppe 40 required** y el PC para el no encryption permitido. Esto no produce ninguna mensajes en el PC, pero las desconexiones de la sesión y el PIX debug muestra esta salida:

```
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 del PIX MPPE RADIUS

El PIX se fija para el **vpdn group 1 ppp encrypt mppe 40 required** y el PC para el cifrado permitido con la autenticación a un servidor de RADIUS no vuelve la clave MPPE. El PC muestra este mensaje:

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

Las demostraciones del PIX debug:

```
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
```

El PC muestra este mensaje:

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

Información Relacionada

- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Soluciones a los Problemas más frecuentes de IPSec VPN L2L y de Acceso Remoto
- Página de soporte de PPTP
- RFC 2637: Protocolo de Tunelización punto a Punto (PPTP)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico - Cisco Systems