PIX 6.x: Exemplo de Configuração de PPTP com Autenticação Radius

Contents

Introduction

O Point-to-Point Tunneling Protocol (PPTP) é um protocolo de tunelamento de camada 2 que permite a um cliente remoto usar uma rede IP pública para comunicar seguramente com servidores em uma rede corporativa privada. O PPTP faz o tunelamento do IP. O PPTP é descrito no RFC 2637. O suporte ao PPTP no PIX Firewall foi adicionado no PIX Software release 5.1. A Documentação do PIX fornece mais informações sobre o PPTP e sua utilização com o PIX. Este documento descreve como configurar o PIX para utilizar o PPTP com autenticação local,

TACACS+ e RADIUS. Este documento também fornece dicas e exemplos que você pode utilizar para ajudá-lo no troubleshooting de problemas comuns.

Este documento mostra como configurar conexões PPTP *para* o PIX. Para configurar um PIX ou ASA para permitir o PPTP *através* do Security Appliance, consulte Permitindo Conexões PPTP/L2TP através do PIX.

Consulte Cisco Secure PIX Firewall 6.x e Cisco VPN Client 3.5 for Windows com a Autenticação RADIUS do IAS do Microsoft Windows 2000 e 2003 para configurar o PIX Firewall e o VPN Client para utilização com o Servidor RADIUS do Internet Authentication Service (IAS) do Windows 2000 e 2003.

Consulte Configurando o VPN 3000 Concentrator e o PPTP com a Autenticação RADIUS do Cisco Secure ACS for Windows para configurar o PPTP em um VPN 3000 Concentrator com a autenticação RADIUS do Cisco Secure ACS for Windows.

Consulte Configurando o CiscoSecure ACS para a Autenticação PPTP do Roteador Windows para configurar uma conexão de PC com o roteador, o qual fornecerá então a autenticação do usuário para o servidor Cisco Secure Access Control System (ACS) 3.2 for Windows antes que o usuário tenha permissão para utilizar a rede.

Nota:Em termos de PPTP, de acordo com a RFC, o PPTP Network Server (PNS) é o servidor (neste caso, o PIX, ou a parte chamada) e o PPTP Access Concentrator (PAC) é o cliente (o PC, ou o chamador).

Observação: o tunelamento dividido não é suportado no PIX para clientes PPTP.

Observação: o PIX 6.x precisa do MS-CHAP v1.0 para que o PPTP funcione. O Windows Vista não suporta MS-CHAP v1.0. Assim, o PPTP no PIX 6.x não funcionará no Windows Vista. O PPTP não é suportado no PIX versão 7.x ou posterior.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Secure PIX Firewall Software Release 6.3(3).

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

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

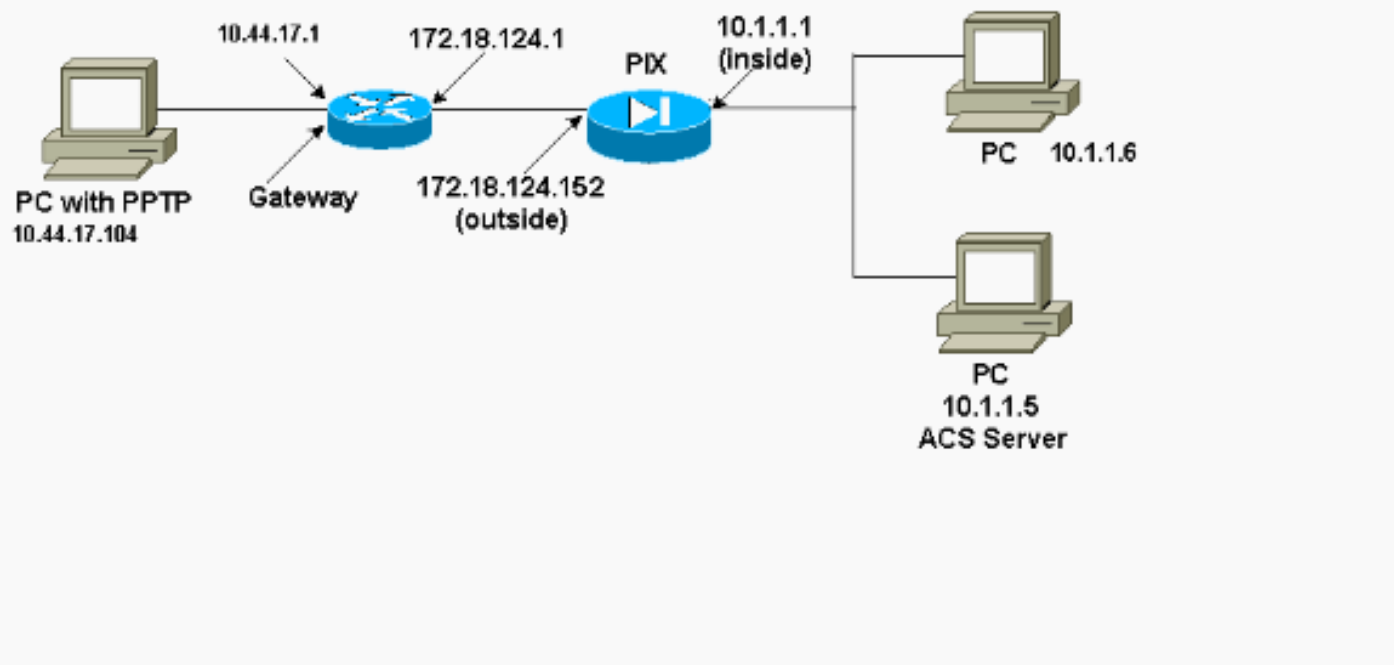
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede.



Dicas de configuração para o PIX Firewall

Tipo de Autenticação - CHAP, PAP, MS-CHAP

O PIX configurado para todos os três métodos de autenticação (CHAP, PAP, MS-CHAP) ao mesmo tempo tem a maior chance de se conectar, não importando como o PC esteja configurado. Essa é uma boa ideia para fins de solução de problemas.

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

Microsoft Point-to-Point Encryption (MPPE)

Use esta sintaxe de comando para configurar a criptografia MPPE no PIX Firewall.

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

Neste comando, **required** é uma palavra-chave opcional. O MS-CHAP deve ser configurado.

Configurar o recurso PPTP em PCs clientes

Observação: as informações disponíveis aqui sobre a configuração do software da Microsoft não vêm com nenhuma garantia ou suporte para o software da Microsoft. O suporte ao software Microsoft está disponível na Microsoft e no site de suporte da Microsoft.

Windows 98

Siga estas etapas para instalar o recurso PPTP no Windows 98.

1. Selecione Iniciar > Configurações > Painel de Controle > Adicionar novo hardware. Clique em Next.
2. Clique em Select na lista e selecione Network Adapter. Clique em Next.
3. Escolha Microsoft no painel esquerdo e Microsoft VPN Adapter no painel direito.

Siga estas etapas para configurar o recurso PPTP.

1. Selecione Iniciar > Programas > Acessórios > Comunicações > Rede dial up.
2. Clique em **Make new connection**. Em **Select a device**, conecte-se usando o **Microsoft VPN Adapter**. O endereço IP do servidor VPN é o ponto final do túnel do PIX.
3. A autenticação padrão do Windows 98 usa criptografia de senha (CHAP ou MS-CHAP). Para alterar o PC para ele também aceitar PAP, selecione **Properties > Server types**. Desmarque **Require encrypted password**. Você pode configurar a criptografia de dados (MPPE ou não MPPE) nessa área.

Windows 2000

Siga estas etapas para configurar o recurso PPTP no Windows 2000.

1. Selecione **Start > Programs > Accessories > Communications > Network & Dialup connections**.
2. Clique em Make new connection (Fazer nova conexão) e em Next (Avançar).
3. Selecione Conectar com uma rede privada por meio da Internet e Discar uma conexão antes (ou não se for uma LAN). Clique em Next.
4. Digite o nome de host ou endereço IP do ponto final do túnel (PIX/roteador)
5. Se você precisar alterar o tipo da senha, selecione Properties > Security for the connection > Advanced. O padrão é MS-CHAP e MS-CHAP v2 (não CHAP ou PAP). Você pode configurar a criptografia de dados (MPPE ou não MPPE) nessa área.

Windows NT

Consulte Instalando, Configurando e Usando o PPTP com Clientes e Servidores Microsoft para configurar clientes NT para PPTP.

Configure o PIX

Configuração de PIX - Autenticação local, sem criptografia

```
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
```

Configuração de PIX - Autenticação local com criptografia

Se você adicionar esse comando à configuração PIX - autenticação local, configuração sem criptografia, o PC e o PIX negociam automaticamente a criptografia de 40 bits ou nenhuma (com base nas configurações do PC).

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

Se o PIX estiver com o recurso 3DES habilitado, o comando **show version** exibirá esta mensagem.

- Versões 6.3 e posteriores:
  `VPN-3DES-AES: Enabled`
- Versões 6.2 e anteriores:
  `VPN-3DES: Enabled`

A criptografia de 128 bits também é possível. Entretanto, se uma destas mensagens for exibida, é porque o PIX não está habilitado para a criptografia de 128 bits.

- Versões 6.3 e posteriores:
  ```
  Warning: VPN-3DES-AES license is required
  for 128 bits MPPE encryption
  ```
- Versões 6.2 e anteriores:
  ```
  Warning: VPN-3DES license is required
  for 128 bits MPPE encryption
  ```

A sintaxe do comando MPPE é mostrada aqui.

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

O PC e o PIX devem estar configurados para autenticação MS-CHAP junto com MPPE.

Configuração de PIX - Autenticação TACACS+/RADIUS Sem Criptografia

```
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]
```

Configuração de PIX - autenticação de RADIUS com criptografia

Se o RADIUS for usado, e se o servidor RADIUS (atributo 26 específico do fornecedor, Microsoft como fornecedor) suportar chaveamento MPPE, a criptografia MPPE poderá ser adicionada. A autenticação TACACS+ não funciona com criptografia porque servidores TACACS+ não são capazes de retornar chaves MPPE especiais. O Cisco Secure ACS para Windows 2.5 e posterior RADIUS não suporta MPPE (todos os servidores RADIUS não suportam MPPE).

Com a suposição de que a autenticação RADIUS funciona sem criptografia, adicione criptografia incluindo este comando na configuração anterior:

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

O PC e o PIX negociam automaticamente a criptografia de 40 bits ou nenhuma (com base nas configurações do PC).

Se o PIX estiver com o recurso 3DES habilitado, o comando **show version** exibirá esta mensagem.

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

A criptografia de 128 bits também é possível. No entanto, se essa mensagem for exibida, o PIX não estará ativado para criptografia de 128 bits.

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

A sintaxe do comando MPPE é mostrada nesta saída.

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

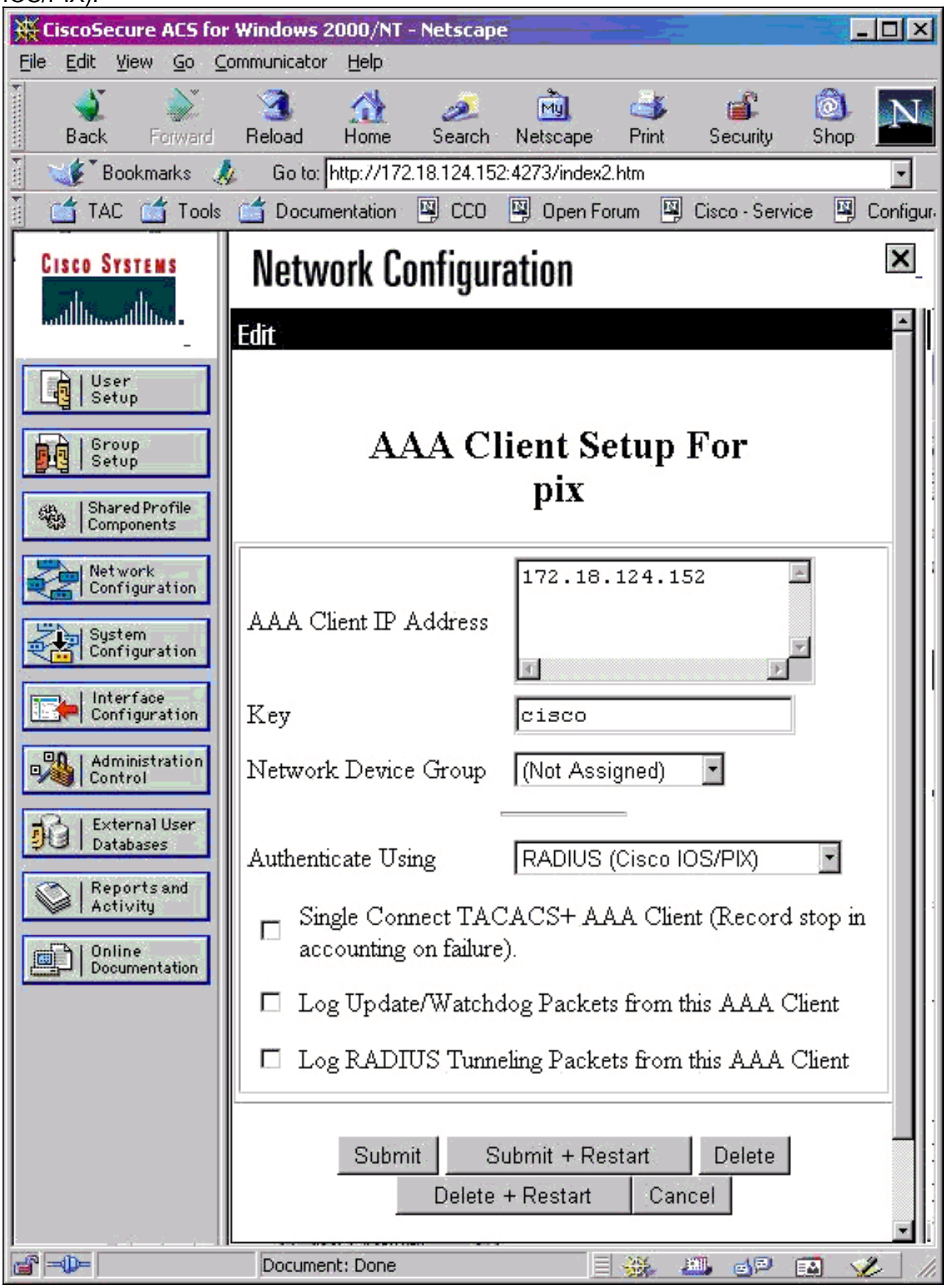
O PC e o PIX devem estar configurados para autenticação MS-CHAP junto com MPPE.

Configurar o Cisco Secure ACS para Windows 3.0

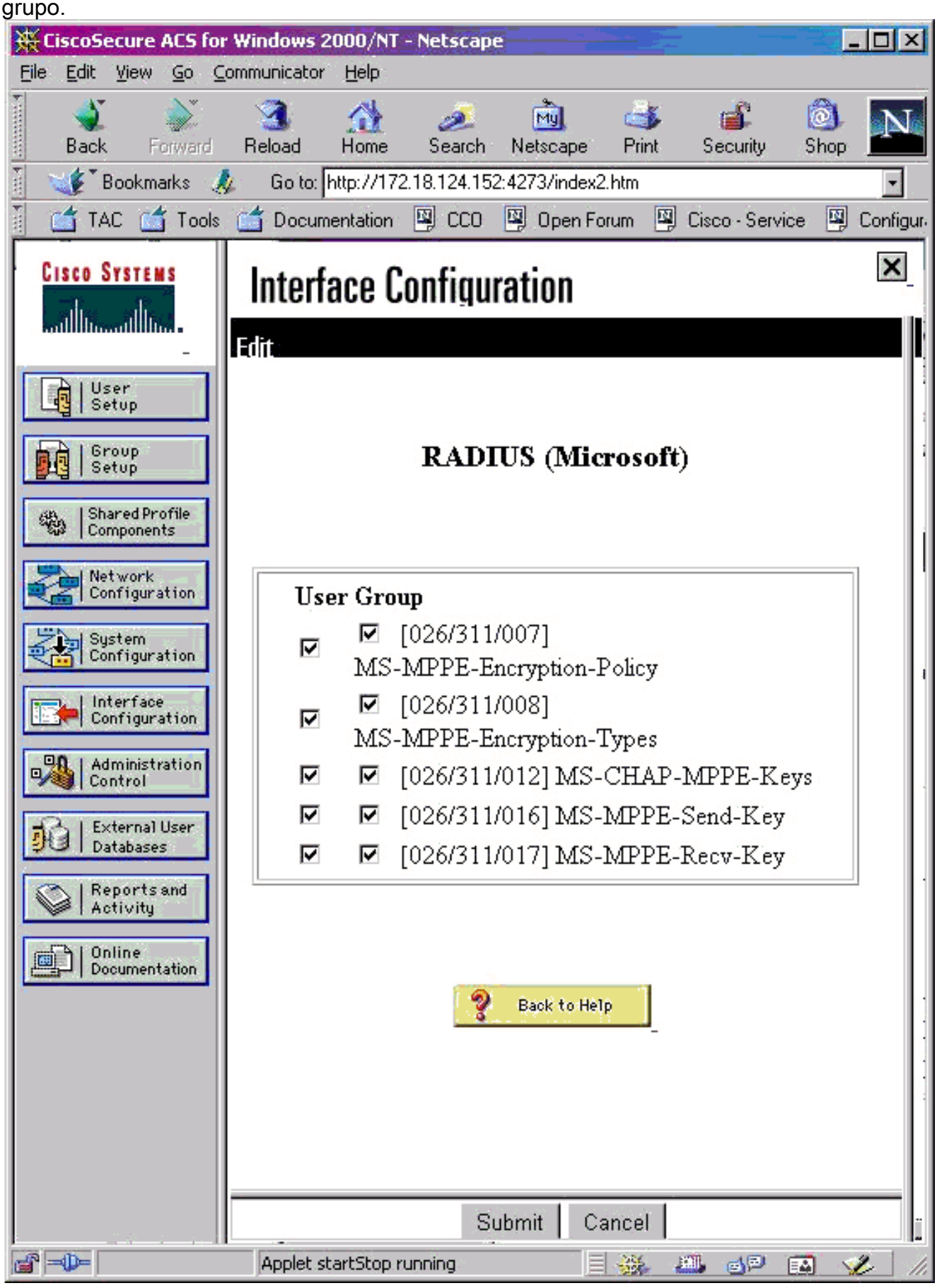
Autenticação RADIUS com criptografia

Use estas etapas para configurar o Cisco Secure ACS para Windows 3.0. As mesmas etapas de configuração se aplicam às versões 3.1 e 3.2 do ACS.

1. Adicione o PIX à configuração de rede do servidor Cisco Secure ACS para Windows e identifique o tipo de dicionário como RADIUS (Cisco IOS/PIX).

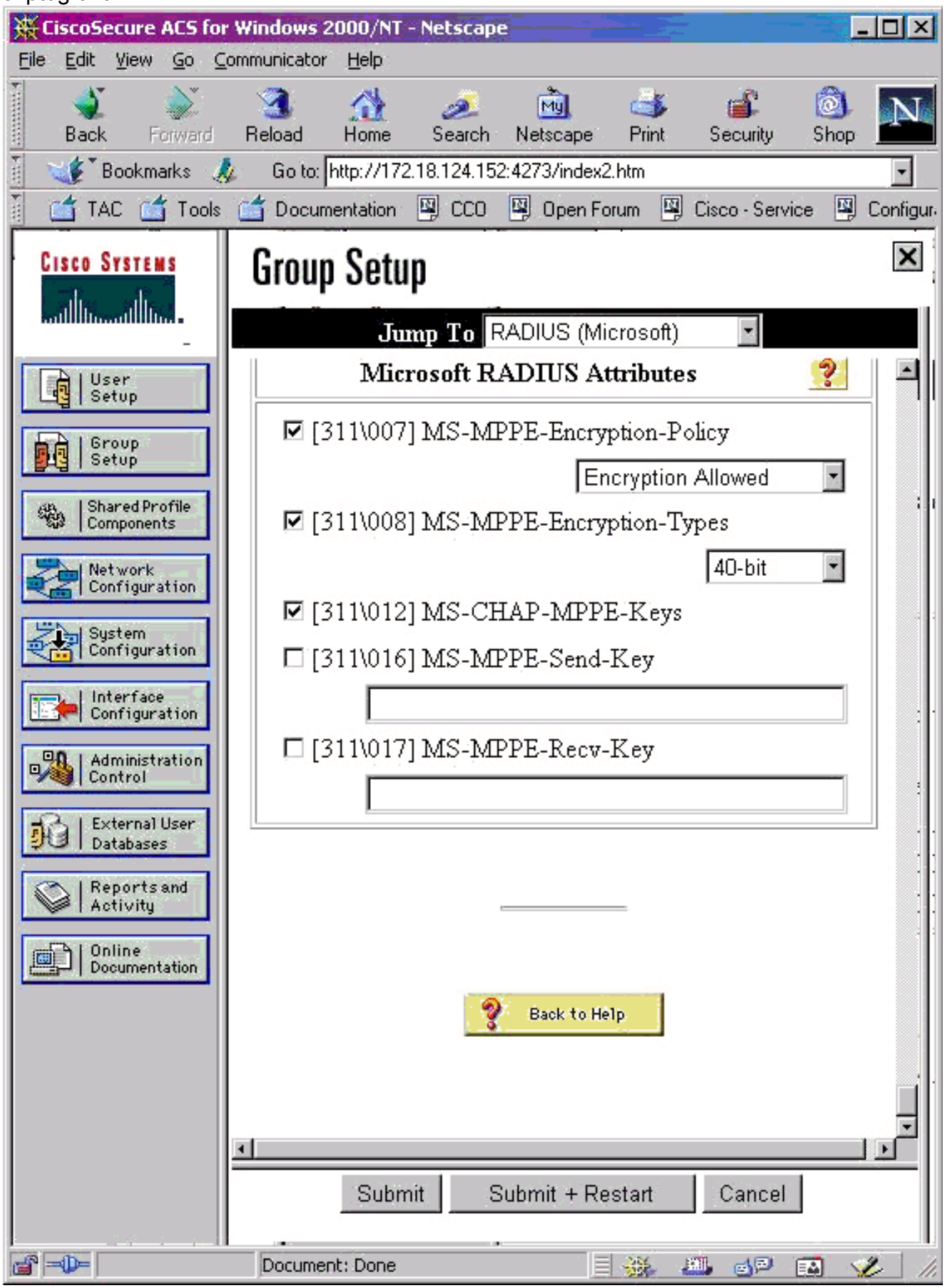


2. Abra **Interface Configuration > RADIUS (Microsoft)** e marque os atributos de MPPE para fazê-los surgir na interface de
grupo.



3. Adicionar um usuário. No grupo do usuário, adicione os atributos de MPPE [RADIUS (Microsoft)]. Você deve habilitar esses atributos para criptografia e ele é opcional quando o PIX não está configurado para

criptografia.



Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona

adequadamente.

Comandos show de PIX (pós-autenticação)

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

O comando **show vpdn** lista informações de túnel e de sessão.

```
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
```

Verificação de PC cliente

Em uma janela do MS-DOS ou na janela Run, digite**ipconfig /all**. A parte do adaptador PPP mostra essa saída.

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

Você também pode clicar em **Details** para exibir as informações da conexão PPTP.

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

- Deve haver conectividade para o Generic Routing Encapsulation (GRE) e TCP 1723 do PC para o ponto de extremidade do túnel PIX. Se houver alguma chance de isso ser bloqueado por um firewall ou uma lista de acesso, mova o PC para perto do PIX.

- O Windows 98 e o Windows 2000 PPTP são os mais fáceis de configurar. Se estiver com dúvidas, tente diversos PCs e sistemas operacionais. Após uma conexão com êxito, clique em **Details** no PC para exibir as informações sobre a conexão. Por exemplo, se você usa PAP, CHAP, IP, criptografia e assim por diante.
- Se você pretende usar RADIUS e/ou TACACS+, tente configurar primeiro a autenticação local (nome de usuário e senha no PIX). Se isso não funcionar, a autenticação com um servidor RADIUS ou TACACS+ não funcionará.
- Inicialmente, certifique-se de que as configurações de segurança no PC permitam tantos tipos de autenticação diferentes quanto possíveis (PAP, CHAP, MS-CHAP) e desmarque a caixa **Require data encryption** (torna opcional tanto no PIX quanto no PC).
- Como o tipo de autenticação é negociada, configure o PIX com o número máximo de possibilidades. Por exemplo, se o PC estiver configurado somente para MS-CHAP e o roteador somente para PAP, nunca haverá nenhum contrato.
- Se o PIX atua como um servidor PPTP para dois locais diferentes e cada local tem seu próprio servidor RADIUS no interior, não há suporte para o uso de um único PIX para ambos os locais servidos por seu próprio servidor RADIUS.
- Alguns servidores RADIUS não suportam MPPE. Se um servidor RADIUS não oferece suporte à chaveamento MPPE, a autenticação RADIUS funciona, mas a criptografia MPPE não funciona.
- Com o Windows 98 ou posterior, quando se usa PAP ou CHAP, o nome de usuário enviado ao PIX é idêntico ao que é digitado na conexão da Rede dial-up (DUN). Mas quando você usa MS-CHAP, o nome de domínio pode ser anexado à frente do nome de usuário, por exemplo:Nome de usuário inserido em DUN - "cisco"Conjunto de domínio na caixa Windows 98 - DOMAINNome de usuário MS-CHAP enviado para PIX - "DOMÍNIO\cisco"Nome de usuário no PIX - "cisco"Resultado: nome de usuário/senha inválidaEsta é uma seção do log PPP de um PC Windows 98 que mostra o 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 você usar o Windows 98 e o MS-CHAP no PIX, além de ter o nome de usuário que não é de domínio, você pode adicionar "DOMÍNIO\nome de usuário" ao PIX:

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

Observação: se você executar a autenticação remota em um servidor AAA, o mesmo se aplica.

Comandos para Troubleshooting

Informações sobre a sequência esperada de eventos PPTP estão disponíveis no PPTP RFC 2637 . No PIX, eventos significativos em uma boa sequência de PPTP mostram:

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

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Comandos debug de PIX

- **debug ppp io** — Exibe as informações do pacote para a interface virtual PPTP PPP.
- **debug ppp error — mostra erros de protocolo e estatísticas de erros associados à negociação e à operação da conexão PPP.**
- **debug vpdn error — Exibe erros que evitam que um túnel de PPP seja estabelecido ou erros que fazem com que um túnel estabelecido seja fechado.**
- **debug vpdn packet—Exibe erros e eventos L2TP que fazem parte do fechamento ou estabelecimento de túnel normal para VPDNs.**
- **debug vpdn events — Exibe mensagens sobre eventos que fazem parte do estabelecimento ou encerramento normal de túneis PPP.**
- **debug ppp uauth** — Exibe as mensagens de depuração de autenticação de usuário AAA da interface virtual PPTP PPP.

Comandos de limpeza de PIX

Esse comando deve ser emitido no modo de configuração.

- **clear vpdn tunnel [all | *[id tunnel_id]*]**—Remove um ou mais túneis PPTP da configuração.

Cuidado: *não* emita o comando **clear vpdn**. Isso apaga todos os comandos vpdn.

Ativar o registro PPP no PC cliente

Conclua estas instruções para ativar a depuração do PPP para vários sistemas operacionais Windows e Microsoft.

Windows 95

Siga estas etapas para ativar o registro PPP em uma máquina Windows 95.

1. Na opção Network no Control Panel, clique duas vezes em **Microsoft Dial-Up Adapter** na lista de componentes de rede instalados.
2. Clique na guia Advanced. Na lista Property, clique na opção **Record A Log File** e, na lista Value, clique em **Yes**. Em seguida, clique em “OK”.
3. Desligue e reinicialize o computador para que esta opção entre em vigor. O registro está salvo em um arquivo denominado ppplog.txt.

Windows 98

Siga estas etapas para ativar o registro PPP em uma máquina Windows 98.

1. Em **Dial-Up Networking**, clique uma vez em um ícone de conexão e, em seguida, selecione **File > Properties**.
2. Clique na guia Server Types.
3. Selecione a opção Record a log file (Gravar um arquivo de registro) para essa conexão. O arquivo de log está localizado em C:\Windows\ppplog.txt

Windows 2000

Para habilitar o registro PPP em um computador Windows 2000, vá para a Página de Suporte da Microsoft e pesquise por "Habilitar registro PPP no Windows".

Windows NT

Siga estas etapas para ativar o registro PPP em um sistema NT.

1. Localize a chave **SYSTEM\CurrentControlSet\Services\RasMan\PPP** e altere **Logging** de 0 para **1**. Isso criará um arquivo chamado PPP.LOG no diretório <winnt root>\SYSTEM32\RAS.
2. Para depurar uma sessão PPP, primeiro ative o registro e, em seguida, inicie a conexão PPP. Quando a conexão falha ou sai, examine o PPP.LOG para ver o que aconteceu.

Para obter mais informações, consulte a Página de Suporte da Microsoft e procure "Ativando o registro do PPP no Windows NT".

Problemas adicionais da Microsoft

Vários problemas relacionados à Microsoft a serem considerados na solução de problemas de PPTP estão listados aqui. Informações detalhadas estão disponíveis na base de conhecimento Microsoft nos links fornecidos.

- Como Manter conexões de RAS Ativas Após o Fim da SessãoAs conexões de Remote Access Service (RAS) do Windows são desconectadas automaticamente quando você faz logout de um cliente RAS. Você pode permanecer conectado habilitando a chave de registro KeepRasConnections no cliente RAS.
- O Usuário Não é Alertado ao Conectar com Credenciais no CacheSe você fizer logon em um domínio de uma estação de trabalho ou servidor membro baseado no Windows e o controlador de domínio não puder ser localizado, não receberá uma mensagem de erro indicando esse problema. Em vez disso, você será conectado ao computador local usando as credenciais em cache.
- Como Escrever um Arquivo LMHOSTS para a Validação de Domínio e Outros Problemas de Resolução de NomesSe você passar por problemas de resolução de nomes na sua rede TCP/IP, será necessário utilizar arquivos Lmhosts para resolver os nomes NetBIOS. Você deve seguir um procedimento específico para criar um arquivo Lmhosts a ser usado na resolução de nome e validação de domínio.

Exemplo de saída de depuração

Depuração de PIX - Autenticação local

Esta saída de depuração indica eventos significativos em *itálico*.

```
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...
```

Depuração de PIX - Autenticação RADIUS

Esta saída de depuração indica eventos significativos em *itálico*.

```
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:
3081880b00174000000000001000000000ff03c0210101... 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...
```

que pode dar errado

Túnel PPTP Simultâneo

Você não consegue estabelecer mais de 127 conexões com o PIX 6.x, e essa mensagem de erro é exibida:

%PIX-3-213001: PPTP control daemon socket io accept error, errno = 5

Solução:

Há um limite de hardware de 128 sessões simultâneas no PIX 6.x. Se você subtrair uma para o soquete de escuta PPTP, o número máximo será 127 conexões.

Não é possível negociar a autenticação do PIX e do PC

Os protocolos de autenticação do PC são definidos para aqueles que o PIX não pode fazer (Shiva Password Authentication Protocol (SPAP) e Microsoft CHAP Versão 2 (MS-CHAP v.2) em vez da versão 1). O PC e o PIX não podem concordar com a autenticação. O PC exibe esta mensagem:

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

PIX e PC não podem negociar a criptografia

O PC está configurado para **Encrypted only** e o comando**vpdn group 1 ppp encrypt mppe 40 required** foi excluído do PIX. O PC e o PIX não podem concordar com a criptografia e o PC exibe esta mensagem:

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

PIX e PC não podem negociar a criptografia

O PIX está configurado para **vpdn group 1 ppp encrypt mppe 40 required** e o PC para não permitir criptografia. Isso não gera nenhuma mensagem no PC, mas a sessão é desconectada e a depuração do PIX mostra esta saída:

```
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 do RADIUS MPPE PIX

O PIX está configurado para **vpdn group 1 ppp encrypt mppe 40 required** e o PC para permitir criptografia com autenticação em um servidor RADIUS não retorna a chave de MPPE. O PC mostra esta mensagem:

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

A depuração 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
```

O PC mostra esta mensagem:

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

Informações Relacionadas

- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto
- Página de suporte do PPTP
- RFC 2637: Point-to-Point Tunneling Protocol (PPTP)
- Solicitações de Comentários (RFCs)
- Suporte Técnico - Cisco Systems