

Configurando clientes Cisco IOS e Windows 2000 para L2TP usando Microsoft IAS

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurando o Windows 2000 Advanced Server para Microsoft IAS](#)

[Configuração dos clientes RADIUS](#)

[Configurando usuários em IAS](#)

[Aplicando uma política de acesso remoto ao usuário Windows](#)

[Configurando o cliente Windows 2000 para L2TP](#)

[Desabilitando o IPSec para o Windows 2000 Client](#)

[Configurando o Cisco IOS para o L2TP](#)

[Para habilitar a criptografia](#)

[comandos debug e show](#)

[Divisão de túnel](#)

[Troubleshooting](#)

[Problema 1: IPSec não desativado](#)

[Problema 2: Erro 789](#)

[Problema 3: Problema com autenticação de túnel](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento fornece instruções em como configurar o software de Cisco IOS® e os clientes do Windows 2000 para o protocolo de túnel da camada 2 (L2TP) que usa o Internet Authentication Server de Microsoft (IAS).

Refira o [L2TP sobre o IPsec entre o exemplo de configuração de utilização de Windows 2000/XP PC e da chave pré-compartilhada PIX/ASA 7.2](#) para obter mais informações sobre de como configurar o L2TP sobre a Segurança IP (IPsec) de Microsoft Windows remoto 2000/2003 e dos clientes XP a um escritório corporativo da ferramenta de segurança PIX usando chaves pré-compartilhada com o servidor Radius de Microsoft Windows 2003 IAS para a autenticação de usuário.

Refira [configurar o L2TP sobre o IPsec de um Windows 2000 ou do cliente XP a um concentrador](#)

[da Cisco VPN 3000 Series usando chaves pré-compartilhada](#) para obter mais informações sobre de como configurar o L2TP sobre o IPsec do Microsoft Windows 2000 remoto e os clientes XP a uma site corporativo usando um método cifrado.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- O componente opcional do Microsoft IAS instalou em um servidor avançado de Microsoft 2000 com diretório ativo
- Um Cisco 3600 Router
- C3640-io3s56i-mz.121-5.T do Cisco IOS Software Release

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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 ferramenta [Command Lookup Tool](#) ([apenas para clientes registrados](#)) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Este documento usa estas associações IP para clientes dial-up:

- Roteador gateway: 192.168.1.2 ~ 192.168.1.254
- LNS: 172.16.10.1 ~ 172.16.10.1

Configurando o Windows 2000 Advanced Server para Microsoft IAS

Certifique-se de que o Microsoft IAS esteja instalado. A fim instalar o Microsoft IAS, entre como

um administrador e termine estas etapas:

1. Em **Network Services**, verifique se todas as caixas de seleção estão desmarcadas.
2. Verifique a caixa de verificação do **Internet Authentication Server (IAS)** e clique então a **APROVAÇÃO**.
3. No **Windows Components wizard**, clique em Next. Se solicitado, insira o CD do Windows 2000.
4. Quando os arquivos requerido foram copiados, clique o **revestimento** e feche então todos os indicadores. Não é preciso reinicializar.

Configuração dos clientes RADIUS

Conclua estes passos:

1. Em **Administrative Tools**, abra o Internet Authentication Server Console e clique em Clients.
2. Na **caixa de nome amigável**, incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor do acesso de rede (NAS).
3. Clique o **uso este IP**.
4. Na lista de drop-down de **Client-Vendor**, assegure-se de que o **padrão RADIUS** esteja selecionado.
5. No **segredo compartilhado** e confirme caixas **secretas compartilhadas**, incorpore a senha e clique então o **revestimento**.
6. Na árvore de console, clicar com o botão direito o **Internet Authentication Service**, e clique então o **começo**.
7. Feche a console.

Configurando usuários em IAS

O diferente de Cisco Secure, a base de dados de usuário do Remote Authentication Dial-In User Server do Windows 2000 (RAIO) é limitado firmemente à base de dados de usuário de Windows.

- Se o diretório ativo é instalado em seu servidor do Windows 2000, crie seus usuários dial-up novos dos **usuários e dos computadores de diretório ativo**.
- Se o diretório ativo não é instalado, você pode usar **usuários locais e grupos das ferramentas administrativas** a fim criar novos usuários.

Configuração de Usuários de Diretório Ativo

Termine estas etapas a fim configurar usuários com diretório ativo:

1. Na console **Active Directory Users and Computers**, expanda seu domínio.
2. Clicar com o botão direito o **rolo dos usuários** para selecionar o **novo usuário**.
3. Crie um novo usuário chamado **tac**.
4. Incorpore a sua senha à **senha** e confirme caixas de diálogo da senha.
5. Desmarque a opção **User Must Change Password at Next Logon** e clique em Next.
6. Abra a caixa das **propriedades do tac** do usuário. Altere para a guia **Dial-In**.
7. Em **Remote Access Permission (Dial-in or VPN)**, clique em Allow Access e depois em OK.

[Configuração de Usuários se Nenhum Diretório Ativo Estiver Instalado](#)

Termine estas etapas a fim configurar usuários se o diretório ativo não é instalado:

1. Das **ferramentas administrativas**, clique sobre a **gerência do computador**.
2. Expanda a console do **Computer Management** e clique em Local Users and Groups.
3. Clicar com o botão direito o **rolo dos usuários** para selecionar o **novo usuário**.
4. Incorpore uma senha à **senha** e **confirme caixas de diálogo da senha**.
5. Desmarque a opção **User Must Change Password at Next Logon** e clique em Next.
6. Abra a caixa das **propriedades do tac** do novo usuário. Altere para a guia **Dial-In**.
7. Em **Remote Access Permission (Dial-in or VPN)**, clique em Allow Access e depois em OK.

[Aplicando uma política de acesso remoto ao usuário Windows](#)

Termine estas etapas a fim aplicar uma política de acesso remoto:

1. Das **ferramentas administrativas**, abra o **console servidor de autenticação de Internet** e clique **políticas de acesso remoto**.
2. Clique o **botão Add Specify as circunstâncias para combinar** e adicionar o **tipo de serviço**. Escolha o tipo disponível como o **Framed**. Adicionar-lo aos tipos selecionado e pressione-o **ESTÁ BEM**.
3. Clique no botão **Add**, em Specify the Conditions to Match, e adicione Framed Protocol. Escolha o tipo disponível como o **PPP**. Adicionar-lo aos tipos selecionado e pressione-o **ESTÁ BEM**.
4. Clique no botão **Add**, em Specify the Conditions to Match, e adicione Windows-Groups para adicionar o grupo do Windows ao qual o usuário pertence. Escolha o grupo e adicionar-lo aos tipos selecionado. Pressione **OK**.
5. **Allow alcance se a permissão de discagem de entrada é propriedades habilitadas**, selecionam o **Grant remote Access permission**.
6. Feche a console.

[Configurando o cliente Windows 2000 para L2TP](#)

Termine estas etapas a fim configurar o cliente do Windows 2000 para o L2TP:

1. Desde o início o **menu**, escolhe **ajustes**, e segue então um destes trajetos:**Control Panel > rede e conexões dial-up**OU**Rede e conexões dial-up > Make New Connection**
2. Use o assistente para criar uma conexão chamada **L2TP**. Essa conexão conecta a uma rede privada através da Internet. Você igualmente precisa de especificar o endereço IP de Um ou Mais Servidores Cisco ICM NT ou o nome do gateway do túnel L2TP.
3. A nova conexão aparece na janela **Network and Dial-up Connections** no Control Panel. De aqui, clique sobre o botão direito de mouse para editar as propriedades.
4. Sob a **ABA de rede de comunicação**, certifique-se de que o **Type of Server I Am Calling** está ajustado ao L2TP.
5. Se você planeia atribuir um endereço interno dinâmico a este cliente do gateway, através de um conjunto local ou de um DHCP, selecione o **protocolo TCP/IP**. Certifique-se de que o cliente está configurado para obter automaticamente um endereço IP de Um ou Mais Servidores Cisco ICM NT. Você pode igualmente emitir a informação de DNS

automaticamente. O **botão Advanced** permite que você defina o WINS estático e a informação de DNS. A aba das **opções** permite que você desligue o IPsec, ou atribua uma política diferente à conexão. Sob a **ABA de segurança**, você pode definir os parâmetros de autenticação de usuário, tais como o PAP, a RACHADURA ou o MS-CHAP, ou o fazer login do domínio do Windows.

6. Quando a conexão é configurada, você pode fazer duplo clique nela para lançar a tela de login, a seguir **conecta**.

[Desabilitando o IPSec para o Windows 2000 Client](#)

1. Edite as propriedades da conexão dial-up L2TP que você apenas criou. Clicar com o botão direito a nova conexão **L2TP** para obter a **janela de propriedades L2TP**.
2. Sob a **ABA de rede de comunicação**, clique **propriedades do protocolo de internet (TCP/IP)**. Fazer duplo clique o **guia avançada**. Vá à aba das **opções**, clique **Ip Security Properties** e, se é selecionado **Do not use IPSEC**, verifica-a novamente.

Nota: Os clientes do Microsoft Windows 2000 têm um Acesso remoto e os serviços de agente de política do padrão que, à revelia, criam uma política para o tráfego L2TP. Esta política padrão não permite o tráfego L2TP sem IPsec e criptografia. Você pode desabilitar o comportamento padrão de Microsoft editando o editor de registro do cliente Microsoft. O procedimento para editar o registro de Windows e para desabilitar a política padrão do IPsec para o tráfego L2TP é dado nesta seção. Refira a documentação Microsoft editando o registro de Windows.

Use o editor de registro (Regedt32.exe) para adicionar a entrada de registro nova para desabilitar o IPsec. Refira a documentação ou o tópico de ajuda do Microsoft de Microsoft para Regedt32.exe para mais informação.

Você deve adicionar o valor de registro IPsec proibido a cada computador de ponto final de Windows 2000-based de um L2TP ou de uma conexão IPsec para impedir que o filtro automático para o L2TP e o tráfego de IPsec estejam criados. Quando o valor de registro IPsec proibido é ajustado a um, seu computador de Windows 2000-based não cria o filtro automático que usa a autenticação de CA. Em lugar de, verifica para ver se há um local ou uma política IPSEC de diretório ativo. A fim adicionar o valor de registro IPsec proibido a seu computador de Windows 2000-based, use Regedt32.exe para encontrar esta chave no registro:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
```

Adicionar este valor de registro a esta chave:

```
Value Name: ProhibitIpSec  
Data Type: REG_DWORD  
Value: 1
```

Nota: Você deve reiniciar seu computador de Windows 2000-based para que as mudanças tomem o efeito. Refira estes artigos Microsoft para uns detalhes mais adicionais:

- Q258261 - Política de IPsec de desabilitação usada com L2TP
- Q240262- Como configurar uma conexão do L2TP/IPsec usando uma chave pré-compartilhada

[Configurando o Cisco IOS para o L2TP](#)

Estas configurações esboçam os comandos required para o L2TP sem IPsec. Uma vez que esta configuração básica está trabalhando, você pode igualmente configurar o IPsec.

angela

```
Building configuration...
Current configuration : 1595 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname angela
!
logging rate-limit console 10 except errors
!--- Enable AAA services here. aaa new-model aaa
authentication login default group radius local aaa
authentication login console none aaa authentication ppp
default group radius local aaa authorization network
default group radius local enable password ww ! memory-
size iomem 30 ip subnet-zero ! ! no ip finger no ip
domain-lookup ip host rund 172.17.247.195 ! ip audit
notify log ip audit po max-events 100 ip address-pool
local ! ! !--- Enable VPN/VPDN services and define
groups and !--- specific variables required for the
group. vpdn enable no vpdn logging ! vpdn-group
L2TP_Windows 2000Client !--- Default L2TP VPDN group. !-
-- Allow the Router to accept incoming requests. accept-
dialin protocol L2TP virtual-template 1 no L2TP tunnel
authentication !--- Users are authenticated at the NAS
or LNS !--- before the tunnel is established. This is
not !--- required for client-initiated tunnels. ! ! call
rsvp-sync ! ! ! ! ! ! controller E1 2/0 ! ! interface
Loopback0 ip address 172.16.10.100 255.255.255.0 !
interface Ethernet0/0 ip address 10.200.20.2
255.255.255.0 half-duplex ! interface Virtual-Template1
ip unnumbered Loopback0 peer default ip address pool
default ppp authentication ms-chap ! ip local pool
default 172.16.10.1 172.16.10.10 ip classless ip route
0.0.0.0 0.0.0.0 10.200.20.1 ip route 192.168.1.0
255.255.255.0 10.200.20.250 no ip http server ! radius-
server host 10.200.20.245 auth-port 1645 acct-port 1646
radius-server retransmit 3 radius-server key cisco !
dial-peer cor custom ! ! ! ! ! line con 0 exec-timeout 0
0 login authentication console transport input none line
33 50 modem InOut line aux 0 line vty 0 4 exec-timeout 0
0 password ww ! end angela# *Mar 12 23:10:54.176: L2TP:
I SCCRQ from RSHANMUG-W2K1.cisco.com tnl 5 *Mar 12
23:10:54.176: Tnl 8663 L2TP: New tunnel created for
remote RSHANMUG-W2K1.cisco.com, address 192.168.1.56
*Mar 12 23:10:54.176: Tnl 8663 L2TP: O SCCRP to
RSHANMUG-W2K1.cisco.com tnlid 5 *Mar 12 23:10:54.180:
Tnl 8663 L2TP: Tunnel state change from idle to wait-
ctl-reply *Mar 12 23:10:54.352: Tnl 8663 L2TP: I SCCCN
from RSHANMUG-W2K1.cisco.com tnl 5 *Mar 12 23:10:54.352:
Tnl 8663 L2TP: Tunnel state change from wait-ctl-reply
to established *Mar 12 23:10:54.352: Tnl 8663 L2TP: SM
State established *Mar 12 23:10:54.356: Tnl 8663 L2TP: I
ICRQ from RSHANMUG-W2K1.cisco.com tnl 5 *Mar 12
23:10:54.356: Tnl/C1 8663/44 L2TP: Session FS enabled
*Mar 12 23:10:54.356: Tnl/C1 8663/44 L2TP: Session state
change from idle to wait-connect *Mar 12 23:10:54.356:
Tnl/C1 8663/44 L2TP: New session created *Mar 12
23:10:54.356: Tnl/C1 8663/44 L2TP: O ICRP to RSHANMUG-
W2K1.cisco.com 5/1 *Mar 12 23:10:54.544: Tnl/C1 8663/44
```

```
L2TP: I ICCN from RSHANMUG-W2K1.cisco.com tnl 5, cl 1
*Mar 12 23:10:54.544: Tnl/Cl 8663/44 L2TP: Session state
change from wait-connect to established *Mar 12
23:10:54.544: Vi1 VPDN: Virtual interface created for
*Mar 12 23:10:54.544: Vi1 PPP: Phase is DOWN, Setup [0
sess, 0 load] *Mar 12 23:10:54.544: Vi1 VPDN: Clone from
Vtemplate 1 filterPPP=0 blocking *Mar 12 23:10:54.620:
Tnl/Cl 8663/44 L2TP: Session with no hwidb *Mar 12
23:10:54.624: %LINK-3-UPDOWN: Interface Virtual-Access1,
changed state to up *Mar 12 23:10:54.624: Vi1 PPP: Using
set call direction *Mar 12 23:10:54.624: Vi1 PPP:
Treating connection as a callin *Mar 12 23:10:54.624:
Vi1 PPP: Phase is ESTABLISHING, Passive Open [0 sess, 0
load] *Mar 12 23:10:54.624: Vi1 LCP: State is Listen
*Mar 12 23:10:54.624: Vi1 VPDN: Bind interface
direction=2 *Mar 12 23:10:56.556: Vi1 LCP: I CONFREQ
[Listen] id 1 len 44 *Mar 12 23:10:56.556: Vi1 LCP:
MagicNumber 0x595E7636 (0x0506595E7636) *Mar 12
23:10:56.556: Vi1 LCP: PFC (0x0702) *Mar 12
23:10:56.556: Vi1 LCP: ACFC (0x0802) *Mar 12
23:10:56.556: Vi1 LCP: Callback 6 (0x0D0306) *Mar 12
23:10:56.556: Vi1 LCP: MRRU 1614 (0x1104064E) *Mar 12
23:10:56.556: Vi1 LCP: EndpointDisc 1 Local *Mar 12
23:10:56.556: Vi1 LCP:
(0x1317012E07E41982EB4EF790F1BF1862) *Mar 12
23:10:56.556: Vi1 LCP: (0x10D0AC00000002) *Mar 12
23:10:56.556: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds
trivially *Mar 12 23:10:56.556: Vi1 LCP: O CONFREQ
[Listen] id 1 len 15 *Mar 12 23:10:56.556: Vi1 LCP:
AuthProto MS-CHAP (0x0305C22380) *Mar 12 23:10:56.556:
Vi1 LCP: MagicNumber 0x4E1B09B8 (0x05064E1B09B8) *Mar 12
23:10:56.560: Vi1 LCP: O CONFREJ [Listen] id 1 len 34
*Mar 12 23:10:56.560: Vi1 LCP: Callback 6 (0x0D0306)
*Mar 12 23:10:56.560: Vi1 LCP: MRRU 1614 (0x1104064E)
*Mar 12 23:10:56.560: Vi1 LCP: EndpointDisc 1 Local *Mar
12 23:10:56.560: Vi1 LCP:
(0x1317012E07E41982EB4EF790F1BF1862) *Mar 12
23:10:56.560: Vi1 LCP: (0x10D0AC00000002) *Mar 12
23:10:56.700: Vi1 LCP: I CONFACK [REQsent] id 1 len 15
*Mar 12 23:10:56.700: Vi1 LCP: AuthProto MS-CHAP
(0x0305C22380) *Mar 12 23:10:56.704: Vi1 LCP:
MagicNumber 0x4E1B09B8 (0x05064E1B09B8) *Mar 12
23:10:56.704: Vi1 LCP: I CONFREQ [ACKrcvd] id 2 len 14
*Mar 12 23:10:56.704: Vi1 LCP: MagicNumber 0x595E7636
(0x0506595E7636) *Mar 12 23:10:56.704: Vi1 LCP: PFC
(0x0702) *Mar 12 23:10:56.704: Vi1 LCP: ACFC (0x0802)
*Mar 12 23:10:56.704: Vi1 LCP: O CONFACK [ACKrcvd] id 2
len 14 *Mar 12 23:10:56.708: Vi1 LCP: MagicNumber
0x595E7636 (0x0506595E7636) *Mar 12 23:10:56.708: Vi1
LCP: PFC (0x0702) *Mar 12 23:10:56.708: Vi1 LCP: ACFC
(0x0802) *Mar 12 23:10:56.708: Vi1 LCP: State is Open
*Mar 12 23:10:56.708: Vi1 PPP: Phase is AUTHENTICATING,
by this end [0 sess, 0 load] *Mar 12 23:10:56.708: Vi1
MS-CHAP: O CHALLENGE id 28 len 21 from angela *Mar 12
23:10:56.852: Vi1 LCP: I IDENTIFY [Open] id 3 len 18
magic 0x595E7636 MSRASV5.00 *Mar 12 23:10:56.872: Vi1
LCP: I IDENTIFY [Open] id 4 len 27 magic 0x595E7636
MSRAS-1- RSHANMUG-W2K1 *Mar 12 23:10:56.880: Vi1 MS-
CHAP: I RESPONSE id 28 len 57 from tac *Mar 12
23:10:56.880: AAA: parse name=Virtual-Access1 idb
type=21 tty=-1 *Mar 12 23:10:56.880: AAA: name=Virtual-
Access1 flags=0x11 type=5 shelf=0 slot=0 adapter=0
port=1 channel=0 *Mar 12 23:10:56.884: AAA/MEMORY:
create_user (0x6273D024) user='tac' ruser=''
```

```
port='Virtual-Access1' rem_addr='' authen_type=MSCHAP
service=PPP priv=1 *Mar 12 23:10:56.884:
AAA/AUTHEN/START (3634835145): port='Virtual-Access1'
list='' action=LOGIN service=PPP *Mar 12 23:10:56.884:
AAA/AUTHEN/START (3634835145): using default list *Mar
12 23:10:56.884: AAA/AUTHEN/START (3634835145):
Method=radius (radius) *Mar 12 23:10:56.884: RADIUS:
ustruct sharecount=0 *Mar 12 23:10:56.884: RADIUS:
Initial Transmit Virtual-Access1 id 173
10.200.20.245:1645, Access-Request, len 129 *Mar 12
23:10:56.884: Attribute 4 6 0AC81402 *Mar 12
23:10:56.884: Attribute 5 6 00000001 *Mar 12
23:10:56.884: Attribute 61 6 00000001 *Mar 12
23:10:56.884: Attribute 1 5 7461631A *Mar 12
23:10:56.884: Attribute 26 16 000001370B0A0053 *Mar 12
23:10:56.884: Attribute 26 58 0000013701341C01 *Mar 12
23:10:56.884: Attribute 6 6 00000002 *Mar 12
23:10:56.884: Attribute 7 6 00000001 *Mar 12
23:10:56.900: RADIUS: Received from id 173
10.200.20.245:1645, Access-Accept, len 116 *Mar 12
23:10:56.900: Attribute 7 6 00000001 *Mar 12
23:10:56.900: Attribute 6 6 00000002 *Mar 12
23:10:56.900: Attribute 25 32 502605A6 *Mar 12
23:10:56.900: Attribute 26 40 000001370C22F6D5 *Mar 12
23:10:56.900: Attribute 26 12 000001370A061C4E *Mar 12
23:10:56.900: AAA/AUTHEN (3634835145): status = PASS
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP: Authorize LCP
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP (1995716469):
Port='Virtual-Access1' list='' service=NET *Mar 12
23:10:56.900: AAA/AUTHOR/LCP: Vi1 (1995716469)
user='tac' *Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP
(1995716469): send AV service=ppp *Mar 12 23:10:56.900:
Vi1 AAA/AUTHOR/LCP (1995716469): send AV protocol=lcp
*Mar 12 23:10:56.900: Vi1 AAA/AUTHOR/LCP (1995716469):
found list default *Mar 12 23:10:56.904: Vi1
AAA/AUTHOR/LCP (1995716469): Method=radius (radius) *Mar
12 23:10:56.904: RADIUS: unrecognized Microsoft VSA type
10 *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR (1995716469):
Post authorization status = PASS_REPL *Mar 12
23:10:56.904: Vi1 AAA/AUTHOR/LCP: Processing AV
service=ppp *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/LCP:
Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:56.904: Vi1 MS-CHAP: O SUCCESS id 28
len 4 *Mar 12 23:10:56.904: Vi1 PPP: Phase is UP [0
sess, 0 load] *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/FSM:
(0): Can we start IPCP? *Mar 12 23:10:56.904: Vi1
AAA/AUTHOR/FSM (2094713042): Port='Virtual-Access1'
list='' service=NET *Mar 12 23:10:56.904:
AAA/AUTHOR/FSM: Vi1 (2094713042) user='tac' *Mar 12
23:10:56.904: Vi1 AAA/AUTHOR/FSM (2094713042): send AV
service=ppp *Mar 12 23:10:56.904: Vi1 AAA/AUTHOR/FSM
(2094713042): send AV protocol=ip *Mar 12 23:10:56.904:
Vi1 AAA/AUTHOR/FSM (2094713042): found list default *Mar
12 23:10:56.904: Vi1 AAA/AUTHOR/FSM (2094713042):
Method=radius (radius) *Mar 12 23:10:56.908: RADIUS:
unrecognized Microsoft VSA type 10 *Mar 12 23:10:56.908:
Vi1 AAA/AUTHOR (2094713042): Post authorization status =
PASS_REPL *Mar 12 23:10:56.908: Vi1 AAA/AUTHOR/FSM: We
can start IPCP *Mar 12 23:10:56.908: Vi1 IPCP: O CONFREQ
[Closed] id 1 len 10 *Mar 12 23:10:56.908: Vi1 IPCP:
Address 172.16.10.100 (0x0306AC100A64) *Mar 12
23:10:57.040: Vi1 CCP: I CONFREQ [Not negotiated] id 5
len 10 *Mar 12 23:10:57.040: Vi1 CCP: MS-PPC supported
```



```
bits 0x01000001 (0x120601000001) *Mar 12 23:10:57.040:
Vi1 LCP: O PROTREJ [Open] id 2 len 16 protocol CCP
(0x80FD0105000A120601000001) *Mar 12 23:10:57.052: Vi1
IPCP: I CONFREQ [REQsent] id 6 len 34 *Mar 12
23:10:57.052: Vi1 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 12 23:10:57.052: Vi1 IPCP: PrimaryDNS 0.0.0.0
(0x810600000000) *Mar 12 23:10:57.052: Vi1 IPCP:
PrimaryWINS 0.0.0.0 (0x820600000000) *Mar 12
23:10:57.052: Vi1 IPCP: SecondaryDNS 0.0.0.0
(0x830600000000) *Mar 12 23:10:57.052: Vi1 IPCP:
SecondaryWINS 0.0.0.0 (0x840600000000) *Mar 12
23:10:57.052: Vi1 AAA/AUTHOR/IPCP: Start. Her address
0.0.0.0, we want 0.0.0.0 *Mar 12 23:10:57.056: Vi1
AAA/AUTHOR/IPCP: Processing AV service=ppp *Mar 12
23:10:57.056: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:57.056: Vi1 AAA/AUTHOR/IPCP:
Authorization succeeded *Mar 12 23:10:57.056: Vi1
AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want
0.0.0.0 *Mar 12 23:10:57.056: Vi1 IPCP: Pool returned
172.16.10.1 *Mar 12 23:10:57.056: Vi1 IPCP: O CONFREQ
[REQsent] id 6 len 28 *Mar 12 23:10:57.056: Vi1 IPCP:
PrimaryDNS 0.0.0.0 (0x810600000000) *Mar 12
23:10:57.056: Vi1 IPCP: PrimaryWINS 0.0.0.0
(0x820600000000) *Mar 12 23:10:57.056: Vi1 IPCP:
SecondaryDNS 0.0.0.0 (0x830600000000) *Mar 12
23:10:57.056: Vi1 IPCP: SecondaryWINS 0.0.0.0
(0x840600000000) *Mar 12 23:10:57.060: Vi1 IPCP: I
CONFACK [REQsent] id 1 len 10 *Mar 12 23:10:57.060: Vi1
IPCP: Address 172.16.10.100 (0x0306AC100A64) *Mar 12
23:10:57.192: Vi1 IPCP: I CONFREQ [ACKrcvd] id 7 len 10
*Mar 12 23:10:57.192: Vi1 IPCP: Address 0.0.0.0
(0x030600000000) *Mar 12 23:10:57.192: Vi1
AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we want
172.16.10.1 *Mar 12 23:10:57.192: Vi1 AAA/AUTHOR/IPCP:
Processing AV service=ppp *Mar 12 23:10:57.192: Vi1
AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:57.192: Vi1 AAA/AUTHOR/IPCP:
Authorization succeeded *Mar 12 23:10:57.192: Vi1
AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want
172.16.10.1 *Mar 12 23:10:57.192: Vi1 IPCP: O CONFNAK
[ACKrcvd] id 7 len 10 *Mar 12 23:10:57.192: Vi1 IPCP:
Address 172.16.10.1 (0x0306AC100A01) *Mar 12
23:10:57.324: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
*Mar 12 23:10:57.324: Vi1 IPCP: Address 172.16.10.1
(0x0306AC100A01) *Mar 12 23:10:57.324: Vi1
AAA/AUTHOR/IPCP: Start. Her address 172.16.10.1, we want
172.16.10.1 *Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP
(413757991): Port='Virtual-Access1' list='' service=NET
*Mar 12 23:10:57.324: AAA/AUTHOR/IPCP: Vi1 (413757991)
user='tac' *Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP
(413757991): send AV service=ppp *Mar 12 23:10:57.324:
Vi1 AAA/AUTHOR/IPCP (413757991): send AV protocol=ip
*Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP (413757991):
send AV addr*172.16.10.1 *Mar 12 23:10:57.324: Vi1
AAA/AUTHOR/IPCP (413757991): found list default *Mar 12
23:10:57.324: Vi1 AAA/AUTHOR/IPCP (413757991):
Method=radius (radius) *Mar 12 23:10:57.324: RADIUS:
unrecognized Microsoft VSA type 10 *Mar 12 23:10:57.324:
Vi1 AAA/AUTHOR (413757991): Post authorization status =
PASS_REPL *Mar 12 23:10:57.324: Vi1 AAA/AUTHOR/IPCP:
Reject 172.16.10.1, using 172.16.10.1 *Mar 12
23:10:57.328: Vi1 AAA/AUTHOR/IPCP: Processing AV
```

```

service=ppp *Mar 12 23:10:57.328: Vi1 AAA/AUTHOR/IPCP:
Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}
111 *Mar 12 23:10:57.328: Vi1 AAA/AUTHOR/IPCP:
Processing AV addr*172.16.10.1 *Mar 12 23:10:57.328: Vi1
AAA/AUTHOR/IPCP: Authorization succeeded *Mar 12
23:10:57.328: Vi1 AAA/AUTHOR/IPCP: Done. Her address
172.16.10.1, we want 172.16.10.1 *Mar 12 23:10:57.328:
Vi1 IPCP: O CONFACK [ACKrcvd] id 8 len 10 *Mar 12
23:10:57.328: Vi1 IPCP: Address 172.16.10.1
(0x0306AC100A01) *Mar 12 23:10:57.328: Vi1 IPCP: State
is Open *Mar 12 23:10:57.332: Vi1 IPCP: Install route to
172.16.10.1 *Mar 12 23:10:57.904: %LINEPROTO-5-UPDOWN:
Line protocol on Interface Virtual-Access1, changed
state to up *Mar 12 23:11:06.324: Vi1 LCP: I ECHOREP
[Open] id 1 len 12 magic 0x595E7636 *Mar 12
23:11:06.324: Vi1 LCP: Received id 1, sent id 1, line up

```

```

angela#show vpdn L2TP Tunnel and Session Information Total tunnels 1 sessions 1 LocID RemID
Remote Name State Remote Address Port Sessions 8663 5 RSHANMUG-W2K1.c est 192.168.1.56 1701 1
LocID RemID TunID Intf Username State Last Chg Fastswitch 44 1 8663 Vi1 tac est 00:00:18 enabled
%No active L2F tunnels %No active PPTP tunnels %No active PPPoE tunnels *Mar 12 23:11:16.332:
Vi1 LCP: I ECHOREP [Open] id 2 len 12 magic 0x595E7636 *Mar 12 23:11:16.332: Vi1 LCP: Received
id 2, sent id 2, line upsh caller ip Line User IP Address Local Number Remote Number <-> Vi1 tac
172.16.10.1 - - in angela#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M -
mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA
external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external
type 2, E - EGP i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * -
candidate default, U - per-user static route, o - ODR P - periodic downloaded static route
Gateway of last resort is 10.200.20.1 to network 0.0.0.0 172.16.0.0/16 is variably subnetted, 2
subnets, 2 masks C 172.16.10.0/24 is directly connected, Loopback0 C 172.16.10.1/32 is directly
connected, Virtual-Access1 10.0.0.0/24 is subnetted, 1 subnets C 10.200.20.0 is directly
connected, Ethernet0/0 S 192.168.1.0/24 [1/0] via 10.200.20.250 S* 0.0.0.0/0 [1/0] via
10.200.20.1 *Mar 12 23:11:26.328: Vi1 LCP: I ECHOREP [Open] id 3 len 12 magic 0x595E7636 *Mar 12
23:11:26.328: Vi1 LCP: Received id 3, sent id 3, line up172.16.10.1 angela#ping 172.16.10.1 Type
escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds:
!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 156/160/168 ms

```

[Para habilitar a criptografia](#)

Adicionar o comando `ppp encrypt mppe 40` sob o virtual-molde 1. da relação certificam-se de que a criptografia está selecionada no cliente Microsoft também.

```

*Mar 12 23:27:36.608: L2TP: I SCCRQ from RSHANMUG-W2K1.cisco.com tnl 13
*Mar 12 23:27:36.608: Tnl 31311 L2TP: New tunnel created for remote
RSHANMUG-W2K1.cisco.com, address 192.168.1.56
*Mar 12 23:27:36.608: Tnl 31311 L2TP: O SCCRP to RSHANMUG-W2K1.cisco.com
tnlid 13
*Mar 12 23:27:36.612: Tnl 31311 L2TP: Tunnel state change from idle to
wait-ctl-reply
*Mar 12 23:27:36.772: Tnl 31311 L2TP: I SCCCN from RSHANMUG-W2K1.cisco.com
tnl 13
*Mar 12 23:27:36.772: Tnl 31311 L2TP: Tunnel state change from
wait-ctl-reply to established
*Mar 12 23:27:36.776: Tnl 31311 L2TP: SM State established
*Mar 12 23:27:36.780: Tnl 31311 L2TP: I ICRQ from RSHANMUG-W2K1.cisco.com
tnl 13
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: Session FS enabled
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: Session state change from idle
to wait-connect
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: New session created
*Mar 12 23:27:36.780: Tnl/Cl 31311/52 L2TP: O ICRP to
RSHANMUG-W2K1.cisco.com 13/1
*Mar 12 23:27:36.924: Tnl/Cl 31311/52 L2TP: I ICCN from

```

RSHANMUG-W2K1.cisco.com tnl 13, cl 1

```
*Mar 12 23:27:36.928: Tnl/Cl 31311/52 L2TP: Session state change from
wait-connect to established
*Mar 12 23:27:36.928: Vi1 VPDN: Virtual interface created for
*Mar 12 23:27:36.928: Vi1 PPP: Phase is DOWN, Setup [0 sess, 0 load]
*Mar 12 23:27:36.928: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
*Mar 12 23:27:36.972: Tnl/Cl 31311/52 L2TP: Session with no hwidb
*Mar 12 23:27:36.976: %LINK-3-UPDOWN: Interface Virtual-Access1, changed
state to up
*Mar 12 23:27:36.976: Vi1 PPP: Using set call direction
*Mar 12 23:27:36.976: Vi1 PPP: Treating connection as a callin
*Mar 12 23:27:36.976: Vi1 PPP: Phase is ESTABLISHING, Passive Open [0 sess,
0 load]
*Mar 12 23:27:36.976: Vi1 LCP: State is Listen
*Mar 12 23:27:36.976: Vi1 VPDN: Bind interface direction=2
*Mar 12 23:27:38.976: Vi1 LCP: TIMEout: State Listen
*Mar 12 23:27:38.976: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially
*Mar 12 23:27:38.976: Vi1 LCP: O CONFREQ [Listen] id 1 len 15
*Mar 12 23:27:38.976: Vi1 LCP: AuthProto MS-CHAP (0x0305C22380)
*Mar 12 23:27:38.976: Vi1 LCP: MagicNumber 0x4E2A5593 (0x05064E2A5593)
*Mar 12 23:27:38.984: Vi1 LCP: I CONFREQ [REQsent] id 1 len 44
*Mar 12 23:27:38.984: Vi1 LCP: MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:38.984: Vi1 LCP: PFC (0x0702)
*Mar 12 23:27:38.984: Vi1 LCP: ACFC (0x0802)
*Mar 12 23:27:38.984: Vi1 LCP: Callback 6 (0x0D0306)
*Mar 12 23:27:38.984: Vi1 LCP: MRRU 1614 (0x1104064E)
*Mar 12 23:27:38.984: Vi1 LCP: EndpointDisc 1 Local
*Mar 12 23:27:38.984: Vi1 LCP: (0x1317012E07E41982EB4EF790F1BF1862)
*Mar 12 23:27:38.984: Vi1 LCP: (0x10D0AC00000000A)
*Mar 12 23:27:38.984: Vi1 LCP: O CONFREQ [REQsent] id 1 len 34
*Mar 12 23:27:38.984: Vi1 LCP: Callback 6 (0x0D0306)
*Mar 12 23:27:38.984: Vi1 LCP: MRRU 1614 (0x1104064E)
*Mar 12 23:27:38.984: Vi1 LCP: EndpointDisc 1 Local
*Mar 12 23:27:38.988: Vi1 LCP: (0x1317012E07E41982EB4EF790F1BF1862)
*Mar 12 23:27:38.988: Vi1 LCP: (0x10D0AC00000000A)
*Mar 12 23:27:39.096: Vi1 LCP: I CONFACK [REQsent] id 1 len 15
*Mar 12 23:27:39.096: Vi1 LCP: AuthProto MS-CHAP (0x0305C22380)
*Mar 12 23:27:39.096: Vi1 LCP: MagicNumber 0x4E2A5593 (0x05064E2A5593)
*Mar 12 23:27:39.128: Vi1 LCP: I CONFREQ [ACKrcvd] id 2 len 14
*Mar 12 23:27:39.128: Vi1 LCP: MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:39.128: Vi1 LCP: PFC (0x0702)
*Mar 12 23:27:39.128: Vi1 LCP: ACFC (0x0802)
*Mar 12 23:27:39.128: Vi1 LCP: O CONFACK [ACKrcvd] id 2 len 14
*Mar 12 23:27:39.128: Vi1 LCP: MagicNumber 0x4B4817ED (0x05064B4817ED)
*Mar 12 23:27:39.128: Vi1 LCP: PFC (0x0702)
*Mar 12 23:27:39.128: Vi1 LCP: ACFC (0x0802)
*Mar 12 23:27:39.128: Vi1 LCP: State is Open
*Mar 12 23:27:39.128: Vi1 PPP: Phase is AUTHENTICATING, by this end [0
sess, 0 load]
*Mar 12 23:27:39.128: Vi1 MS-CHAP: O CHALLENGE id 32 len 21 from angela
*Mar 12 23:27:39.260: Vi1 LCP: I IDENTIFY [Open] id 3 len 18 magic
0x4B4817ED MSRASV5.00
*Mar 12 23:27:39.288: Vi1 LCP: I IDENTIFY [Open] id 4 len 27 magic
0x4B4817ED MSRAS-1- RSHANMUG-W2K1
*Mar 12 23:27:39.296: Vi1 MS-CHAP: I RESPONSE id 32 len 57 from tac
*Mar 12 23:27:39.296: AAA: parse name=Virtual-Access1 idb type=21 tty=-1
*Mar 12 23:27:39.296: AAA: name=Virtual-Access1 flags=0x11 type=5 shelf=0
slot=0 adapter=0 port=1 channel=0
*Mar 12 23:27:39.296: AAA/MEMORY: create_user (0x6273D528) user='tac'
ruser='' port='Virtual-Access1' rem_addr='' authen_type=MSCHAP service=PPP
priv=1
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): port='Virtual-Access1'
list='' action=LOGIN service=PPP
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): using default list
```

```
*Mar 12 23:27:39.296: AAA/AUTHEN/START (2410248116): Method=radius (radius)
*Mar 12 23:27:39.296: RADIUS: ustruct sharecount=0
*Mar 12 23:27:39.300: RADIUS: Initial Transmit Virtual-Access1 id 181
10.200.20.245:1645, Access-Request, len 129
*Mar 12 23:27:39.300: Attribute 4 6 0AC81402
*Mar 12 23:27:39.300: Attribute 5 6 00000001
*Mar 12 23:27:39.300: Attribute 61 6 00000001
*Mar 12 23:27:39.300: Attribute 1 5 7461631A
*Mar 12 23:27:39.300: Attribute 26 16 000001370B0AFC72
*Mar 12 23:27:39.300: Attribute 26 58 0000013701342001
*Mar 12 23:27:39.300: Attribute 6 6 00000002
*Mar 12 23:27:39.300: Attribute 7 6 00000001
*Mar 12 23:27:39.312: RADIUS: Received from id 181 10.200.20.245:1645,
Access-Accept, len 116
*Mar 12 23:27:39.312: Attribute 7 6 00000001
*Mar 12 23:27:39.312: Attribute 6 6 00000002
*Mar 12 23:27:39.312: Attribute 25 32 502E05AE
*Mar 12 23:27:39.312: Attribute 26 40 000001370C225042
*Mar 12 23:27:39.312: Attribute 26 12 000001370A06204E
*Mar 12 23:27:39.312: AAA/AUTHEN (2410248116): status = PASS
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Authorize LCP
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.316: AAA/AUTHOR/LCP: Vi1 (2365724222) user='tac'
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): send AV service=ppp
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): send AV protocol=lcp
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): found list default
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP (2365724222): Method=radius
(radius)
*Mar 12 23:27:39.316: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR (2365724222): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Processing AV service=ppp
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/LCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.316: Vi1 MS-CHAP: 0 SUCCESS id 32 len 4
*Mar 12 23:27:39.316: Vi1 PPP: Phase is UP [0 sess, 0 load]
*Mar 12 23:27:39.316: Vi1 AAA/AUTHOR/FSM: (0): Can we start IPCP?
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.320: AAA/AUTHOR/FSM: Vi1 (1499311111) user='tac'
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): send AV service=ppp
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): send AV protocol=ip
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): found list default
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (1499311111): Method=radius
(radius)
*Mar 12 23:27:39.320: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR (1499311111): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM: We can start IPCP
*Mar 12 23:27:39.320: Vi1 IPCP: 0 CONFREQ [Closed] id 1 len 10
*Mar 12 23:27:39.320: Vi1 IPCP: Address 172.16.10.100 (0x0306AC100A64)
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM: (0): Can we start CCP?
*Mar 12 23:27:39.320: Vi1 AAA/AUTHOR/FSM (327346364):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.324: AAA/AUTHOR/FSM: Vi1 (327346364) user='tac'
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): send AV service=ppp
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): send AV protocol=ccp
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): found list default
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM (327346364): Method=radius
(radius)
*Mar 12 23:27:39.324: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR (327346364): Post authorization status
= PASS_REPL
```

```
*Mar 12 23:27:39.324: Vi1 AAA/AUTHOR/FSM: We can start CCP
*Mar 12 23:27:39.324: Vi1 CCP: O CONFREQ [Closed] id 1 len 10
*Mar 12 23:27:39.324: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.460: Vi1 CCP: I CONFREQ [REQsent] id 5 len 10
*Mar 12 23:27:39.460: Vi1 CCP: MS-PPC supported bits 0x01000001
(0x120601000001)
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Check for unauthorized mandatory
AV's
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.460: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar 12 23:27:39.464: Vi1 CCP: O CONFNAK [REQsent] id 5 len 10
*Mar 12 23:27:39.464: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.472: Vi1 IPCP: I CONFREQ [REQsent] id 6 len 34
*Mar 12 23:27:39.472: Vi1 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 12 23:27:39.472: Vi1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 12 23:27:39.472: Vi1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 12 23:27:39.472: Vi1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 12 23:27:39.472: Vi1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we
want 0.0.0.0
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.472: Vi1 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we
want 0.0.0.0
*Mar 12 23:27:39.472: Vi1 IPCP: Pool returned 172.16.10.1
*Mar 12 23:27:39.476: Vi1 IPCP: O CONFREQ [REQsent] id 6 len 28
*Mar 12 23:27:39.476: Vi1 IPCP: PrimaryDNS 0.0.0.0 (0x810600000000)
*Mar 12 23:27:39.476: Vi1 IPCP: PrimaryWINS 0.0.0.0 (0x820600000000)
*Mar 12 23:27:39.476: Vi1 IPCP: SecondaryDNS 0.0.0.0 (0x830600000000)
*Mar 12 23:27:39.476: Vi1 IPCP: SecondaryWINS 0.0.0.0 (0x840600000000)
*Mar 12 23:27:39.480: Vi1 IPCP: I CONFACK [REQsent] id 1 len 10
*Mar 12 23:27:39.484: Vi1 IPCP: Address 172.16.10.100 (0x0306AC100A64)
*Mar 12 23:27:39.488: Vi1 CCP: I CONFACK [REQsent] id 1 len 10
*Mar 12 23:27:39.488: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.596: Vi1 CCP: I CONFREQ [ACKrcvd] id 7 len 10
*Mar 12 23:27:39.596: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Check for unauthorized mandatory
AV's
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Processing AV service=ppp
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.596: Vi1 AAA/AUTHOR/FSM: Succeeded
*Mar 12 23:27:39.596: Vi1 CCP: O CONFACK [ACKrcvd] id 7 len 10
*Mar 12 23:27:39.596: Vi1 CCP: MS-PPC supported bits 0x01000020
(0x120601000020)
*Mar 12 23:27:39.596: Vi1 CCP: State is Open
*Mar 12 23:27:39.600: Vi1 MPPE: Generate keys using RADIUS data
*Mar 12 23:27:39.600: Vi1 MPPE: Initialize keys
*Mar 12 23:27:39.600: Vi1 MPPE: [40 bit encryption] [stateless mode]
*Mar 12 23:27:39.620: Vi1 IPCP: I CONFREQ [ACKrcvd] id 8 len 10
*Mar 12 23:27:39.620: Vi1 IPCP: Address 0.0.0.0 (0x030600000000)
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we
want 172.16.10.1
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
```

```

*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.620: Vi1 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we
want 172.16.10.1
*Mar 12 23:27:39.624: Vi1 IPCP: O CONFNAK [ACKrcvd] id 8 len 10
*Mar 12 23:27:39.624: Vi1 IPCP: Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.756: Vi1 IPCP: I CONFREQ [ACKrcvd] id 9 len 10
*Mar 12 23:27:39.756: Vi1 IPCP: Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP: Start. Her address 172.16.10.1,
we want 172.16.10.1
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706):
Port='Virtual-Access1' list='' service=NET
*Mar 12 23:27:39.756: AAA/AUTHOR/IPCP: Vi1 (2840659706) user='tac'
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV service=ppp
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV protocol=ip
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): send AV
addr*172.16.10.1
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): found list
default
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP (2840659706): Method=radius
(radius)
*Mar 12 23:27:39.756: RADIUS: unrecognized Microsoft VSA type 10
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR (2840659706): Post authorization
status = PASS_REPL
*Mar 12 23:27:39.756: Vi1 AAA/AUTHOR/IPCP: Reject 172.16.10.1, using
172.16.10.1
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV
mschap_mppe_keys*1p1T11=1v101~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Processing AV addr*172.16.10.1
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded
*Mar 12 23:27:39.760: Vi1 AAA/AUTHOR/IPCP: Done. Her address 172.16.10.1,
we want 172.16.10.1
*Mar 12 23:27:39.760: Vi1 IPCP: O CONFACK [ACKrcvd] id 9 len 10
*Mar 12 23:27:39.760: Vi1 IPCP: Address 172.16.10.1 (0x0306AC100A01)
*Mar 12 23:27:39.760: Vi1 IPCP: State is Open
*Mar 12 23:27:39.764: Vi1 IPCP: Install route to 172.16.10.1
*Mar 12 23:27:40.316: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Virtual-Access1, changed state to up
*Mar 12 23:27:46.628: Vi1 LCP: I ECHOREP [Open] id 1 len 12 magic
0x4B4817ED
*Mar 12 23:27:46.628: Vi1 LCP: Received id 1, sent id 1, line up
*Mar 12 23:27:56.636: Vi1 LCP: I ECHOREP [Open] id 2 len 12 magic
0x4B4817ED
*Mar 12 23:27:56.636: Vi1 LCP: Received id 2, sent id 2, line upcaller ip
Line UserIP AddressLocal NumberRemote Number<->
Vi1 tac172.16.10.1--in

```

```

angela#show ppp mppe virtual-Access 1 Interface Virtual-Access1 (current connection) Software
encryption, 40 bit encryption, Stateless mode packets encrypted = 0 packets decrypted = 16 sent
CCP resets = 0 receive CCP resets = 0 next tx coherency = 0 next rx coherency = 16 tx key
changes = 0 rx key changes = 16 rx pkt dropped = 0 rx out of order pkt= 0 rx missed packets = 0
*Mar 12 23:28:06.604: Vi1 LCP: I ECHOREP [Open] id 3 len 12 magic 0x4B4817ED *Mar 12
23:28:06.604: Vi1 LCP: Received id 3, sent id 3, line up angela#ping 172.16.10.1 Type escape
sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds: !!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 188/196/204 ms angela#show ppp mppe
virtual-Access 1 Interface Virtual-Access1 (current connection) Software encryption, 40 bit
encryption, Stateless mode packets encrypted = 5 packets decrypted = 22 sent CCP resets = 0
receive CCP resets = 0 next tx coherency = 5 next rx coherency = 22 tx key changes = 5 rx key
changes = 22 rx pkt dropped = 0 rx out of order pkt= 0 rx missed packets = 0 angela#ping
172.16.10.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.10.1,
timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max =
184/200/232 ms angela#ping 172.16.10.1sh ppp mppe virtual-Access 1 Interface Virtual-Access1
(current connection) Software encryption, 40 bit encryption, Stateless mode packets encrypted =
10 packets decrypted = 28 sent CCP resets = 0 receive CCP resets = 0 next tx coherency = 10 next

```

```
rx coherency = 28 tx key changes = 10 rx key changes = 28 rx pkt dropped = 0 rx out of order
pkt= 0 rx missed packets = 0 angela#
```

comandos debug e show

Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

A [Output Interpreter Tool](#) ([apenas para clientes registrados](#)) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Se as coisas não trabalham, mínimo **debugar** inclui estes comandos:

- **debug aaa authentication** — Exibe informações sobre autenticação AAA/TACACS+
- **debug aaa authorization** — Exibe informações sobre autorização AAA/TACACS+.
- **debug ppp negotiation** - Exibe pacotes PPP transmitidos durante a inicialização de PPP, em que as opções de PPP são negociadas.
- **debugar a autenticação de PPP** — Indica mensagens do protocolo de autenticação, que inclui intercâmbios de pacotes do protocolo challenge authentication (RACHADURA) e o protocolo password authentication (o PAP) troca.
- **debug radius** — Exibe informações de debug detalhadas associadas ao RADIUS.

Se a autenticação trabalha, mas há uns problemas com criptografia da criptografia Point-to-Point microsoft (MPPE), use um destes comandos:

- **debug ppp mppe packet** - Exibe todo o tráfego MPPE de entrada e de saída.
- **debug ppp mppe event** - Exibe as principais ocorrências de MPPE.
- **debug ppp mppe detailed** — Exibe informações de MPPE detalhadas.
- **debug vpdn l2x-packets** — Mensagens dos indicadores sobre cabeçalhos de protocolo e estado do Level 2 Forwarding (L2F).
- **debug vpdn events** — Exibe mensagens sobre eventos que fazem parte do estabelecimento ou encerramento normal de túneis.
- **debug vpdn errors** - Exibe erros que impedem que um túnel seja estabelecido ou erros que fazem com que o túnel estabelecido seja fechado.
- **debug vpdn packets** — Exibe cada pacote de protocolo trocado. Essa opção pode resultar em um grande número de mensagens de depuração e normalmente deve ser usada somente em um chassi de depuração com uma única sessão ativa.
- **vpdn da mostra** — Informação dos indicadores sobre o túnel e identificadores de mensagem ativos do protocolo L2F em um Virtual Private Dialup Network (VPDN).

Você pode igualmente usar o **vpdn da mostra?** comando ver outros **comandos show VPDN**-específicos.

Divisão de túnel

Supõe que o gateway router é um roteador de provedor de serviço do Internet (ISP). Quando o túnel do Point-to-Point Tunneling Protocol (PPTP) vem acima no PC, a rota PPTP está instalada com uma métrica mais alta do que o padrão precedente, assim que nós perdemos a conectividade de Internet. A fim remediar isto, alterar o roteamento microsoft para suprimir do padrão e reinstalar a rota padrão (isto exigido conhecendo o endereço IP de Um ou Mais Servidores Cisco ICM NT o cliente de PPTP foi atribuído; para o exemplo atual, este é 172.16.10.1):

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 192.168.1.47 metric 1
route add 172.16.10.1 mask 255.255.255.0 192.168.1.47 metric 1
```

Troubleshooting

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

Problema 1: IPsec não desativado

Sintoma

O usuário de PC vê esta mensagem:

```
Error connecting to L2TP:
Error 781: The encryption attempt failed because
no valid certificate was found.
```

Solução

Vá à seção de **propriedades do** indicador da **conexão privada virtual** e clique sobre a **ABA de segurança**. Desabilite a opção da **criptografia de dados da exigência**.

Problema 2: Erro 789

Sintoma

A tentativa de conexão L2TP falha porque a camada da Segurança encontrou um erro de processamento durante negociações iniciais com o computador remoto.

Os serviços de Microsoft Remote Access and Policy Agent criam uma política que seja usada para o tráfego L2TP porque o L2TP não fornece a criptografia. Isto é aplicável para o servidor avançado do Microsoft Windows 2000, o Servidor do Microsoft Windows 2000 e o profissional do Microsoft Windows 2000.

Solução

Use o editor de registro (Regedt32.exe) para adicionar a entrada de registro nova para desabilitar o IPsec. Refira a documentação ou o tópico de ajuda do microsoft de Microsoft para Regedt32.exe.

Você deve adicionar o valor de registro IPsec proibido a cada computador de ponto final de Windows 2000-based de um L2TP ou de uma conexão IPsec para impedir que o filtro automático para o L2TP e o tráfego de IPsec estejam criados. Quando o valor de registro IPsec proibido é ajustado a um, seu computador de Windows 2000-based não cria o filtro automático que usa a autenticação de CA. Em lugar de, verifica para ver se há um local ou uma política IPSEC de diretório ativo. A fim adicionar o valor de registro IPsec proibido a seu computador de Windows 2000-based, use Regedt32.exe para encontrar esta chave no registro:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
```

Adicionar este valor de registro a esta chave:

Value Name: ProhibitIpSec

Data Type: REG_DWORD

Value: 1

Nota: Você deve reiniciar seu computador de Windows 2000-based para que as mudanças tomem o efeito.

Problema 3: Problema com autenticação de túnel

Os usuários estão autenticados no NAS ou no LNS antes que o túnel esteja estabelecido. Isto não é exigido para túneis iniciados pelo cliente como o L2TP de um cliente Microsoft.

O usuário de PC vê esta mensagem:

Connecting to 10.200.20.2..

Error 651: The modem(or other connecting device) has reported an error.

Router debugs:

```
*Mar 12 23:03:47.124: L2TP: I SCCRQ from RSHANMUG-W2K1.cisco.com tnl 1
*Mar 12 23:03:47.124: Tnl 30107 L2TP: New tunnel created for remote
RSHANMUG-W2K1.cisco.com, address 192.168.1.56
*Mar 12 23:03:47.124: Tnl 30107 L2TP: O SCCRP to RSHANMUG-W2K1.cisco.com
tnlid 1
*Mar 12 23:03:47.124: Tnl 30107 L2TP: Tunnel state change from idle to
wait-ctl-reply
*Mar 12 23:03:47.308: Tnl 30107 L2TP: I SCCCN from RSHANMUG-W2K1.cisco.com
tnl 1
*Mar 12 23:03:47.308: Tnl 30107 L2TP: Got a Challenge Response in SCCCN
from RSHANMUG-W2K1.cisco.com
*Mar 12 23:03:47.308: AAA: parse name= idb type=-1 tty=-1
*Mar 12 23:03:47.308: AAA/MEMORY: create_user (0x6273D528) user='angela'
ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): port='' list='default'
action=SENDAUTH service=PPP
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): found list default
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): Method=radius (radius)
*Mar 12 23:03:47.308: AAA/AUTHEN/SENDAUTH (4077585132): no authenstruct
hwidb
*Mar 12 23:03:47.308: AAA/AUTHEN/SENDAUTH (4077585132): Failed sendauthen
for angela
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = FAIL
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): Method=LOCAL
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): SENDAUTH no password for
angela
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = ERROR
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): no methods left to try
*Mar 12 23:03:47.308: AAA/AUTHEN (4077585132): status = ERROR
*Mar 12 23:03:47.308: AAA/AUTHEN/START (4077585132): failed to authenticate
*Mar 12 23:03:47.308: VPDN: authentication failed, couldn't find user
information for angela
*Mar 12 23:03:47.308: AAA/MEMORY: free_user (0x6273D528) user='angela'
ruser='' port='' rem_addr='' authen_type=CHAP service=PPP priv=1
*Mar 12 23:03:47.312: Tnl 30107 L2TP: O StopCCN to
RSHANMUG-W2K1.cisco.com tnlid 1
*Mar 12 23:03:47.312: Tnl 30107 L2TP: Tunnel state change from
wait-ctl-reply to shutting-down
*Mar 12 23:03:47.320: Tnl 30107 L2TP: Shutdown tunnel
*Mar 12 23:03:47.320: Tnl 30107 L2TP: Tunnel state change from
shutting-down to idle
*Mar 12 23:03:47.324: L2TP: Could not find tunnel for tnl 30107, discarding
ICRQ ns 3 nr 1
*Mar 12 23:03:47.448: L2TP: Could not find tunnel for tnl 30107, discarding
```

Informações Relacionadas

- [Protocolo layer two tunneling \(L2TP\)](#)
- [L2TP sobre o IPsec entre o Windows 2000 e o VPN 3000 concentrator usando o exemplo de configuração dos Certificados digitais](#)
- [Configurando L2TP No IPsec Entre o PIX Firewall e o PC com Windows 2000 Usando Certificados](#)
- [Protocolo de túnel camada 2](#)
- [Configurando redes privadas virtuais](#)
- [Configurando a autenticação do protocolo do túnel da camada 2 com RADIUS](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)