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

Contents

Introduction

Este documento fornece instruções sobre como configurar o software Cisco IOS® e clientes Windows 2000 para o Protocolo de Túnel de Camada 2 (L2TP - Layer 2 Tunnel Protocol) usando o Internet Authentication Server (IAS - Internet Authentication Server) da Microsoft.

Consulte Exemplo de Configuração de Chave Pré-compartilhada L2TP sobre IPsec entre o Windows 2000/XP PC e PIX/ASA 7.2 Usando Exemplo de Configuração de Chave Pré-compartilhada para obter mais informações sobre como configurar o L2TP sobre IP Security (IPSec) de clientes remotos do Microsoft Windows 2000/2003 e XP para um escritório corporativo do PIX Security Appliance usando chaves pré-compartilhadas 2003 IAS RADIUS Server para autenticação de usuário.

Consulte Configurando L2TP sobre IPSec de um cliente Windows 2000 ou XP para um Cisco

VPN 3000 Series Concentrator usando chaves pré-compartilhadas para obter mais informações sobre como configurar L2TP sobre IPSec de clientes remotos do Microsoft Windows 2000 e XP para um site corporativo usando um método criptografado.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Componente opcional do Microsoft IAS instalado em um servidor avançado do Microsoft 2000 com Active Directory
- Um Cisco Router 3600
- Software Cisco IOS versão c3640-io3s56i-mz.121-5.T

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.

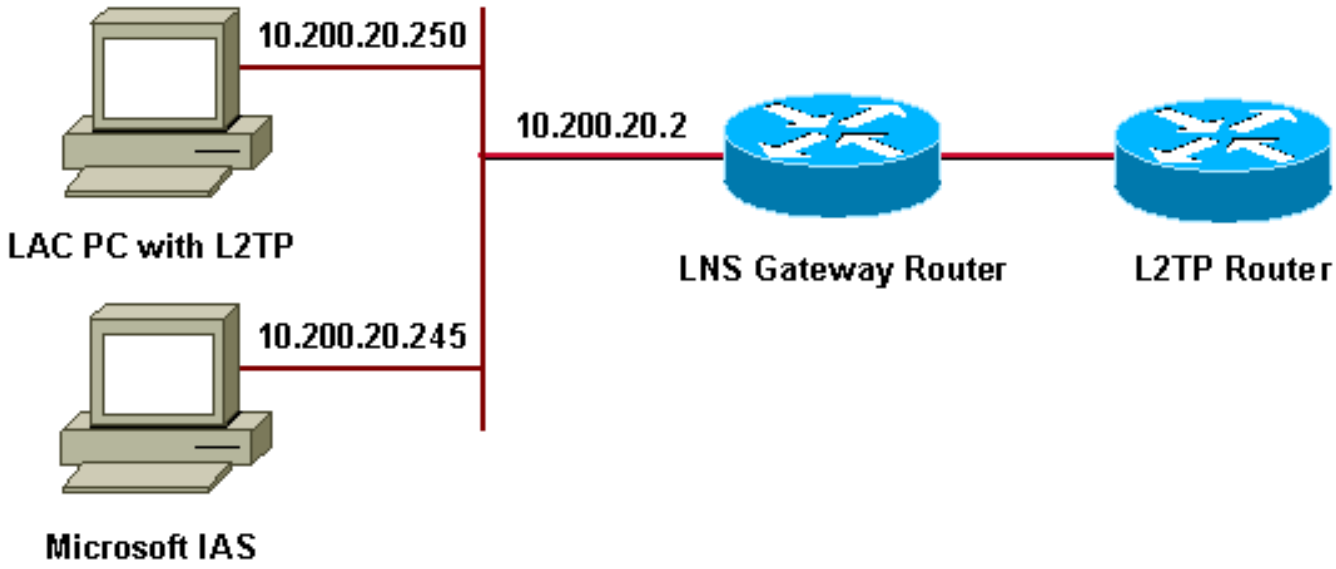
Configurar

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 neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Este documento usa estes pools de 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. Para instalar o Microsoft IAS, faça login como administrador e conclua estas etapas:

1. Em **Network Services**, verifique se todas as caixas de seleção estão desmarcadas.
2. Marque a caixa de seleção **Internet Authentication Server (IAS)** e clique em **OK**.
3. No Windows Components wizard, clique em Next. Se solicitado, insira o CD do Windows 2000.
4. Quando os arquivos necessários tiverem sido copiados, clique em **Concluir** e feche todas as janelas. 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 **Friendly Name Box**, digite o endereço IP do servidor de acesso à rede (NAS).
3. Clique em **Usar este IP**.
4. Na lista suspensa **Client-Vendor**, certifique-se de que **RADIUS Standard** esteja selecionado.
5. Nas caixas **Shared Secret** e **Confirm Shared Secret**, digite a senha e clique em **Finish**.
6. Na árvore do console, clique com o botão direito do mouse em **Internet Authentication Service** e clique em **Start**.
7. Feche a console.

Configurando usuários em IAS

Ao contrário do CiscoSecure, o banco de dados de usuários do Windows 2000 Remote Authentication Dial-In User Server (RADIUS) está estreitamente vinculado ao banco de dados de usuários do Windows.

- Se o Ative Diretory estiver instalado no servidor Windows 2000, crie os novos usuários de discagem a partir de **Usuários e Computadores do Ative Diretory**.
- Se o Ative Diretory não estiver instalado, você poderá usar **Usuários e Grupos Locais** em **Ferramentas Administrativas** para criar novos usuários.

Configuração de Usuários de Diretório Ativo

Conclua estes passos para configurar usuários com o Ative Diretory:

1. Na console **Active Directory Users and Computers, expanda seu domínio.**
2. Clique com o botão direito do mouse na **rolagem Usuários** para selecionar **Novo usuário**.
3. Crie um novo usuário chamado tac.
4. Digite sua senha nas caixas de diálogo **Senha** e **Confirmar senha**.
5. Desmarque a opção **User Must Change Password at Next Logon e clique em Next.**
6. Abra a caixa **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

Conclua estes passos para configurar usuários se o Ative Diretory não estiver instalado:

1. Em **Administrative Tools**, clique em **Computer Management**.
2. Expanda a console do **Computer Management e clique em Local Users and Groups.**
3. Clique com o botão direito do mouse em **Users Scroll** para selecionar **New User**.
4. Digite uma senha nas caixas de diálogo **Senha** e **Confirmar senha**.
5. Desmarque a opção **User Must Change Password at Next Logon e clique em Next.**
6. Abra a caixa **Propriedades** do novo 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.

Aplicando uma política de acesso remoto ao usuário Windows

Conclua estes passos para aplicar uma política de acesso remoto:

1. Em **Administrative Tools**, abra o console **Internet Authentication Server** e clique em **Remote Access Policies**.
2. Clique no botão **Adicionar** em **Especificar as condições para corresponder** e adicionar **tipo de serviço**. Escolha o tipo disponível como **Framed**. Adicione-o aos tipos selecionados e pressione **OK**.
3. Clique no botão **Add, em Specify the Conditions to Match, e adicione Framed Protocol.** Escolha o tipo disponível como **PPP**. Adicione-o aos tipos selecionados e pressione **OK**.
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 adicione-o aos tipos selecionados. Pressione **OK**.
5. Em **Permitir acesso se a Permissão de discagem estiver Habilitada**, selecione **Conceder**

permissão de acesso remoto.
6. Feche a console.

Configurando o cliente Windows 2000 para L2TP

Conclua estes passos para configurar o cliente Windows 2000 para L2TP:

1. No **menu Iniciar**, escolha **Configurações** e siga um destes caminhos:**Painel de controle > Conexões de rede e dial-up***OU***Conexões de rede e dial-up > Criar nova conexão**
2. Use o Assistente para criar uma conexão chamada **L2TP**. Essa conexão conecta a uma rede privada através da Internet. Você também precisa especificar o endereço IP ou o nome do gateway do túnel L2TP.
3. A nova conexão aparece na janela **Network and Dial-up Connections no Control Panel.** Aqui, clique no botão direito do mouse para editar as propriedades.
4. Na guia **Networking**, verifique se **Type Of Server I Am Calling** está definido como L2TP.
5. Se você planeja alocar um endereço interno dinâmico para esse cliente a partir do gateway, por meio de um pool local ou DHCP, selecione **TCP/IP protocol**. Verifique se o cliente está configurado para obter um endereço IP automaticamente. Você também pode emitir informações de DNS automaticamente.O botão **Avançado** permite definir informações estáticas de WINS e DNS.A guia **Options** permite desativar o IPSec ou atribuir uma política diferente à conexão.Na guia **Segurança**, você pode definir os parâmetros de autenticação do usuário, como PAP, CHAP ou MS-CHAP ou login de domínio do Windows.
6. Quando a conexão estiver configurada, você poderá clicar duas vezes nela para iniciar a tela de login e, em seguida, **conectar**.

Desabilitando o IPSec para o Windows 2000 Client

1. Edite as propriedades da conexão dial-up L2TP que acabou de criar. Clique com o botão direito do mouse na nova conexão **L2TP** para obter a janela **Propriedades L2TP**.
2. Na guia **Networking**, clique em **Propriedades de Internet Protocol (TCP/IP)**. Clique duas vezes na guia **Avançado**. Vá para a guia **Options**, clique em **IP security properties** e, se **Não usar IPSEC** estiver selecionado, verifique-o duas vezes.

Observação: os clientes do Microsoft Windows 2000 têm um acesso remoto padrão e serviços do Agente de política que, por padrão, criam uma política para o tráfego L2TP. Essa política padrão não permite tráfego L2TP sem IPSec e criptografia. Você pode desabilitar o comportamento padrão da Microsoft editando o Editor do Registro do cliente da Microsoft. O procedimento para editar o registro do Windows e desativar a política padrão de IPSec para tráfego L2TP é fornecido nesta seção. Consulte a documentação da Microsoft para editar o Registro do Windows.

Use o Editor do Registro (Regedt32.exe) para adicionar a nova entrada do Registro para desabilitar o IPSec. Consulte a documentação da Microsoft ou o tópico de ajuda da Microsoft para Regedt32.exe para obter mais informações.

Você deve adicionar o valor do registro ProhibitIpSec a cada computador de ponto de extremidade baseado no Windows 2000 de uma conexão L2TP ou IPSec para impedir que o filtro automático para o tráfego L2TP e IPSec seja criado. Quando o valor do registro ProhibitIpSec é definido como um, o computador baseado no Windows 2000 não cria o filtro automático que utiliza a autenticação CA. Em vez disso, verifica se há uma política IPSec local ou do Ative Diretory. Para adicionar o valor do registro ProhibitIpSec ao computador baseado no Windows

2000, use Regedt32.exe para localizar 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
```

Observação: você deve reiniciar o computador baseado no Windows 2000 para que as alterações entrem em vigor. Consulte estes artigos da Microsoft para obter mais detalhes:

- Q258261 - Desabilitando a política IPSEC usada com L2TP
- Q240262- How to Configure a L2TP/IPSec Connection Using a Pre-shared Key (Como configurar uma conexão L2TP/IPSec usando uma chave pré-compartilhada)

Configuração do Cisco IOS para L2TP

Essas configurações descrevem os comandos necessários para L2TP sem IPSec. Quando essa configuração básica estiver funcionando, você também poderá 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/Cl 8663/44 L2TP: Session FS enabled
*Mar 12 23:10:54.356: Tnl/Cl 8663/44 L2TP: Session state
change from idle to wait-connect *Mar 12 23:10:54.356:
Tnl/Cl 8663/44 L2TP: New session created *Mar 12
23:10:54.356: Tnl/Cl 8663/44 L2TP: O ICRP to RSHANMUG-
W2K1.cisco.com 5/1 *Mar 12 23:10:54.544: Tnl/Cl 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=1v1O1~11a1W11151\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=1v1O1~11a1W11151\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 CONFREJ
[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=1v1O1~11a1W11151\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=1v1O1~11a1W11151\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     UserIP AddressLocal NumberRemote Number<->
Vi1     tac172.16.10.1--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
C172.16.10.0/24 is directly connected, Loopback0
C172.16.10.1/32 is directly connected, Virtual-Access1
10.0.0.0/24 is subnetted, 1 subnets
C10.200.20.0 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

Adicione o comando **ppp encrypt mppe 40** em **interface virtual-template 1**. Verifique se 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:   (0x10D0AC0000000A)
*Mar 12 23:27:38.984: Vi1 LCP: O CONFREJ [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:   (0x10D0AC0000000A)
*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=1v1O1~11a1W11151\1V1M1#11Z1`1k1}111
*Mar 12 23:27:39.316: Vi1 MS-CHAP: O 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: O 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 CONFREJ [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=1v1O1~11a1W11151\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 (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Se as coisas não funcionarem, a **depuração** mínima 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 os pacotes PPP transmitidos durante a inicialização do PPP, onde as opções do PPP são negociadas.
- **debug ppp authentication** —Exibe mensagens do protocolo de autenticação, que inclui trocas de pacotes CHAP (Challenge Authentication Protocol Protocolo de Autenticação de Desafio) e PAP (Password Authentication Protocol Protocolo de Autenticação de Senha).
- **debug radius — Exibe informações de debug detalhadas associadas ao RADIUS.**

Se a autenticação funcionar, mas houver problemas com a criptografia Microsoft Point-to-Point Encryption (MPPE), use um destes comandos:

- **debug ppp mppe packet** — Exibe todo o tráfego MPPE de entrada 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** — Exibe mensagens sobre os cabeçalhos e o status do protocolo de Encaminhamento de Nível 2 (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 um 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.
- **show vpdn** — Exibe informações sobre o túnel de protocolo L2F ativo e identificadores de

mensagem em uma Virtual Private Dialup Network (VPDN).

Você também pode usar o **comando show vpdn ?** para ver outros comandos vpdn-specific **show**.

Encapuslamento dividido

Suponha que o roteador do gateway seja um roteador do ISP (Provedor de serviços de Internet). Quando o túnel PPTP (Point-to-Point Tunneling Protocol) é ativado no PC, a rota PPTP é instalada com uma métrica maior do que o padrão anterior, então perdemos a conectividade com a Internet. Para corrigir isso, modifique o roteamento da Microsoft para excluir o padrão e reinstalar a rota padrão (isso é necessário sabendo o endereço IP que o cliente PPTP recebeu; para o exemplo atual, 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
```

Troubleshoot

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

Problema 1: IPSec não desativado

Sintoma

O usuário do PC vê esta mensagem:

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

Solução

Vá para a seção **Propriedades** da janela **Conexão Privada Virtual** e clique na guia **Segurança**. Desative a opção **Require Data Encryption**.

Problema 2: Erro 789

Sintoma

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

Os serviços do Agente de Política e Acesso Remoto da Microsoft criam uma política que é usada para o tráfego L2TP porque o L2TP não fornece criptografia. Isso se aplica ao Microsoft Windows 2000 Advanced Server, Microsoft Windows 2000 Server e Microsoft Windows 2000 Professional.

Solução

Use o Editor do Registro (Regedt32.exe) para adicionar a nova entrada do Registro para desabilitar o IPSec. Consulte a documentação da Microsoft ou o tópico de ajuda da Microsoft para Regedt32.exe.

Você deve adicionar o valor do registro ProhibitIpSec a cada computador de ponto de extremidade baseado no Windows 2000 de uma conexão L2TP ou IPSec para impedir que o filtro automático para o tráfego L2TP e IPSec seja criado. Quando o valor do registro ProhibitIpSec é definido como um, o computador baseado no Windows 2000 não cria o filtro automático que utiliza a autenticação CA. Em vez disso, verifica se há uma política IPSec local ou do Ative Diretory. Para adicionar o valor do registro ProhibitIpSec ao computador baseado no Windows 2000, use Regedt32.exe para localizar 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
```

Observação: você deve reiniciar o computador baseado no Windows 2000 para que as alterações entrem em vigor.

Problema 3: Problema com autenticação de túnel

Os usuários são autenticados no NAS ou LNS antes do túnel ser estabelecido. Isso não é necessário para túneis iniciados pelo cliente, como L2TP, de um cliente Microsoft.

O usuário do 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
ICRQ ns 3 nr 2
```

Informações Relacionadas

- L2TP (Layer Two Tunneling Protocol)
- Exemplo de configuração de L2TP sobre IPsec entre o concentrador Windows 2000 e VPN 3000 usando 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