

L2TP sobre IPsec entre o Windows 2000/XP PC e PIX/ASA 7.2 usando exemplo de configuração de chave pré-compartilhada

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Conventions](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração de cliente L2TP/IPsec do Windows](#)

[Servidor L2TP na configuração PIX](#)

[L2TP usando a configuração ASDM](#)

[Microsoft Windows 2003 Server com configuração IAS](#)

[Autenticação estendida para L2TP sobre IPsec usando o Active Directory](#)

[Verificar](#)

[Troubleshoot](#)

[Comandos para Troubleshooting](#)

[Exemplo de saída de depuração](#)

[Solucionar problemas usando o ASDM](#)

[Problema: Desconexões frequentes](#)

[Solucionar problemas do Windows Vista](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar o L2TP (Layer 2 Tunneling Protocol) 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 com o Microsoft Windows 2003 Internet Authentication Service (IAS) RADIUS Server para autenticação de usuário. Consulte [Microsoft - Checklist: Configurando o IAS para acesso discado e VPN](#) para obter mais informações sobre o IAS.

O principal benefício de configurar L2TP com IPsec em um cenário de acesso remoto é que os usuários remotos podem acessar uma VPN em uma rede IP pública sem um gateway ou uma

linha dedicada. Isso permite acesso remoto de praticamente qualquer lugar com POTS. Um benefício adicional é que o único requisito de cliente para acesso VPN é o uso do Windows 2000 com o Microsoft DUN (Dial-Up Networking). Nenhum software cliente adicional, como o software Cisco VPN Client, é necessário.

Este documento também descreve como usar o Cisco Adaptive Security Device Manager (ASDM) para configurar o PIX 500 Series Security Appliance para L2TP sobre IPsec.

Observação: o [L2TP \(Layer 2 Tunneling Protocol\) sobre IPsec](#) é compatível com o Cisco Secure PIX Firewall Software Release 6.x e posterior.

Para configurar L2TP sobre IPsec entre o PIX 6.x e o Windows 2000, consulte [Configurando L2TP sobre IPsec entre o PIX Firewall e o Windows 2000 PC usando certificados](#).

Para configurar L2TP sobre IPsec de clientes remotos Microsoft Windows 2000 e XP para um site corporativo usando um método criptografado, consulte [Configurando L2TP sobre IPsec de um cliente Windows 2000 ou XP para um Cisco VPN 3000 Series Concentrator usando chaves pré-compartilhadas](#).

Prerequisites

Requirements

Antes do estabelecimento do túnel seguro, a conectividade IP precisa existir entre os pares.

Certifique-se de que a porta UDP 1701 não esteja bloqueada em nenhum lugar ao longo do caminho da conexão.

Use somente o grupo de túnel padrão e a política de grupo padrão no Cisco PIX/ASA. As políticas e grupos definidos pelo usuário não funcionam.

Observação: o Security Appliance não estabelece um túnel L2TP/IPsec com o Windows 2000 se o Cisco VPN Client 3.x ou o Cisco VPN 3000 Client 2.5 estiver instalado. Desative o serviço Cisco VPN para o Cisco VPN Client 3.x ou o serviço ANetIKE para o Cisco VPN 3000 Client 2.5 do painel Serviços no Windows 2000. Para fazer isso, escolha **Iniciar > Programas > Ferramentas Administrativas > Serviços**, reinicie o Serviço do Agente de Política IPsec no painel Serviços e reinicialize a máquina.

Componentes Utilizados

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

- PIX Security Appliance 515E com software versão 7.2(1) ou posterior
- Adaptive Security Device Manager 5.2(1) ou posterior
- Microsoft Windows 2000 Server
- Microsoft Windows XP Professional com SP2
- Windows 2003 Server com IAS

Observação: se você atualizar o PIX 6.3 para a versão 7.x, certifique-se de ter instalado o SP2 no Windows XP (cliente L2TP).

Observação: as informações no documento também são válidas para o dispositivo de segurança ASA.

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.

Produtos Relacionados

Essa configuração também pode ser usada com o Cisco ASA 5500 Series Security Appliance 7.2(1) ou posterior.

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

Informações de Apoio

Conclua estes passos para configurar L2TP sobre IPsec.

1. Configure o modo de transporte IPsec para habilitar o IPsec com L2TP. O cliente L2TP/IPsec do Windows 2000 usa o modo de transporte IPsec — somente o payload IP é criptografado e os cabeçalhos IP originais permanecem intactos. As vantagens desse modo são que ele adiciona apenas alguns bytes a cada pacote e permite que os dispositivos na rede pública vejam a origem e o destino finais do pacote. Portanto, para que os clientes L2TP/IPsec do Windows 2000 se conectem ao Security Appliance, você deve configurar o modo de transporte IPsec para uma transformação (consulte a etapa 2 na [configuração do ASDM](#)). Com esse recurso (transporte), você pode ativar o processamento especial (por exemplo, QoS) na rede intermediária com base nas informações no cabeçalho IP. No entanto, o cabeçalho da Camada 4 é criptografado, o que limita o exame do pacote. Infelizmente, a transmissão do cabeçalho IP em texto claro, o modo de transporte permite que um invasor realize alguma análise de tráfego.
2. Configure L2TP com um grupo de rede de discagem privada virtual (VPDN).

A configuração de L2TP com IPsec suporta certificados que usam as chaves pré-compartilhadas ou métodos de assinatura RSA, e o uso de mapas de criptografia dinâmicos (em vez de estáticos). A chave pré-compartilhada é usada como uma autenticação para estabelecer o túnel L2TP sobre IPsec.

Configurar

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

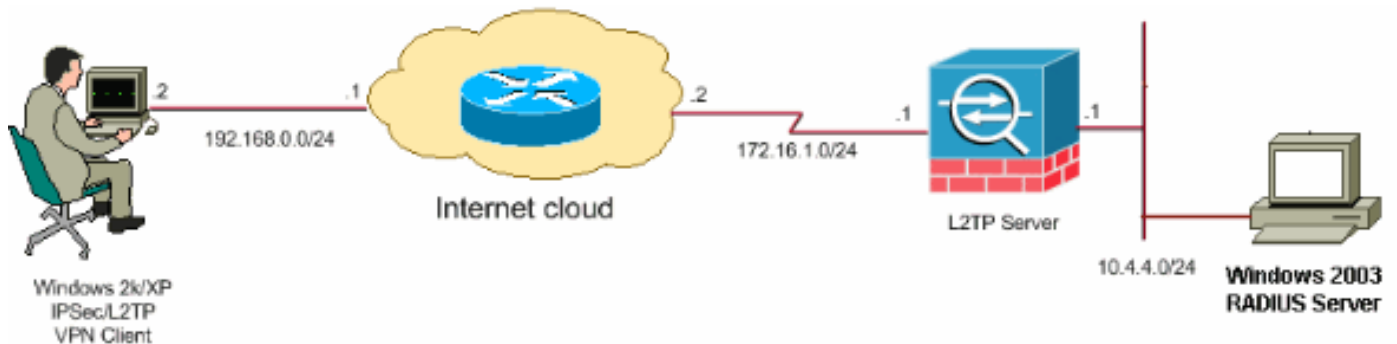
Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Observação: os esquemas de endereçamento IP usados nesta configuração não são legalmente

roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- [Configuração de cliente L2TP/IPsec do Windows](#)
- [Servidor L2TP na configuração PIX](#)
- [L2TP usando a configuração ASDM](#)
- [Microsoft Windows 2003 Server com configuração IAS](#)

Configuração de cliente L2TP/IPsec do Windows

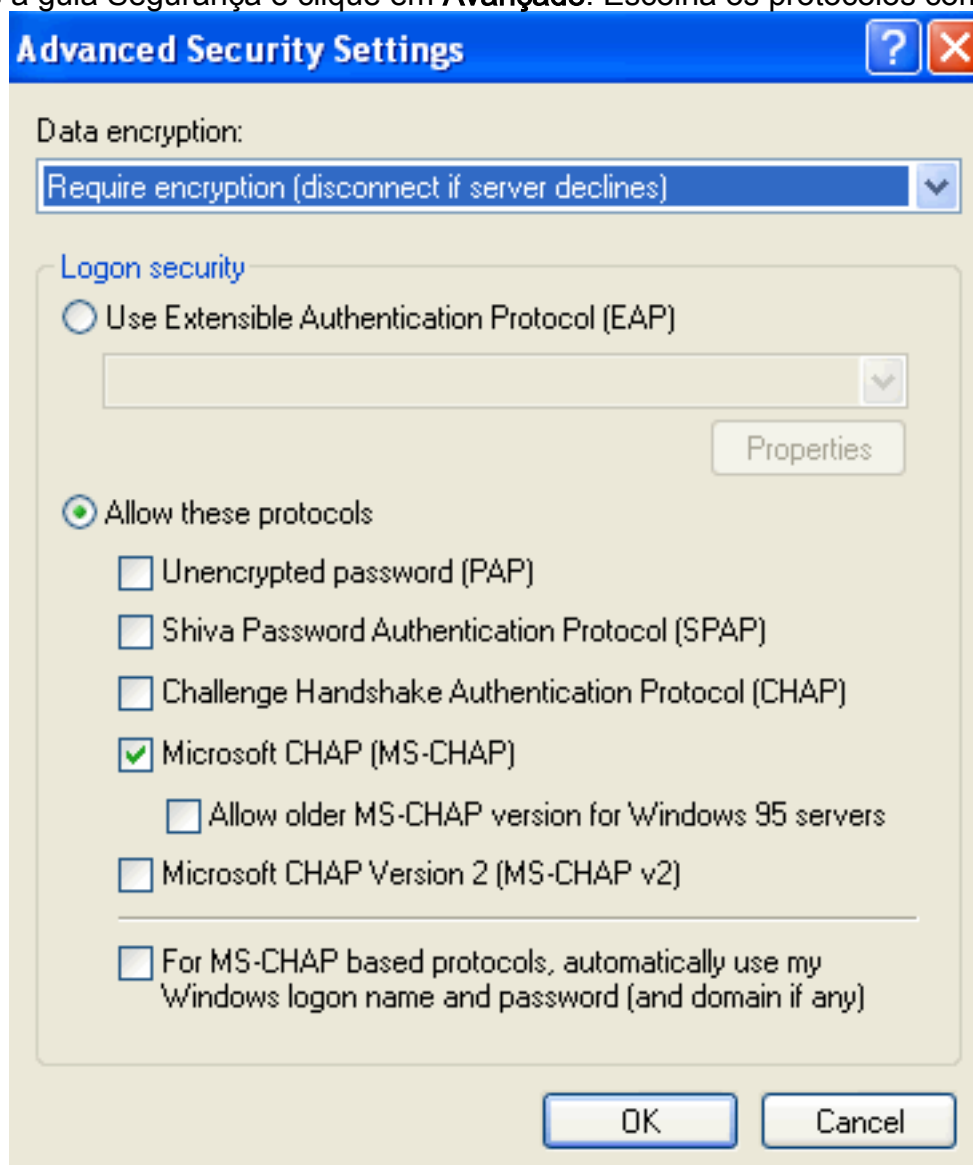
Conclua estes passos para configurar L2TP sobre IPsec no Windows 2000. Para o Windows XP, ignore as etapas 1 e 2 e inicie a partir da etapa 3:

1. Adicione este valor de registro à sua máquina Windows 2000:
`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters`
2. Adicionar este valor de registro a esta chave:
Value Name: ProhibitIpSec
Data Type: REG_DWORD
Value: 1

Observação: em alguns casos (Windows XP Sp2), a adição desta chave (**Valor: 1**) parece quebrar a conexão, pois faz com que a caixa do XP negocie apenas L2TP em vez de L2TP com conexão IPsec. É obrigatório adicionar uma política IPsec em conjunto com essa chave do registro. Se você receber um erro 800 quando tentar estabelecer uma conexão, remova a chave (Valor: 1) para que a conexão funcione. **Observação:** você deve reiniciar o computador Windows 2000/2003 ou XP para que as alterações entrem em vigor. Por padrão, o cliente Windows tenta usar o IPsec com uma Autoridade de Certificação (CA). A configuração desta chave do Registro impede que isso ocorra. Agora você pode configurar uma política IPsec na estação do Windows para corresponder aos parâmetros desejados no PIX/ASA. Consulte [Como configurar uma conexão L2TP/IPSec usando a autenticação de chave pré-compartilhada \(Q240262\)](#) para obter uma configuração passo a passo da política do

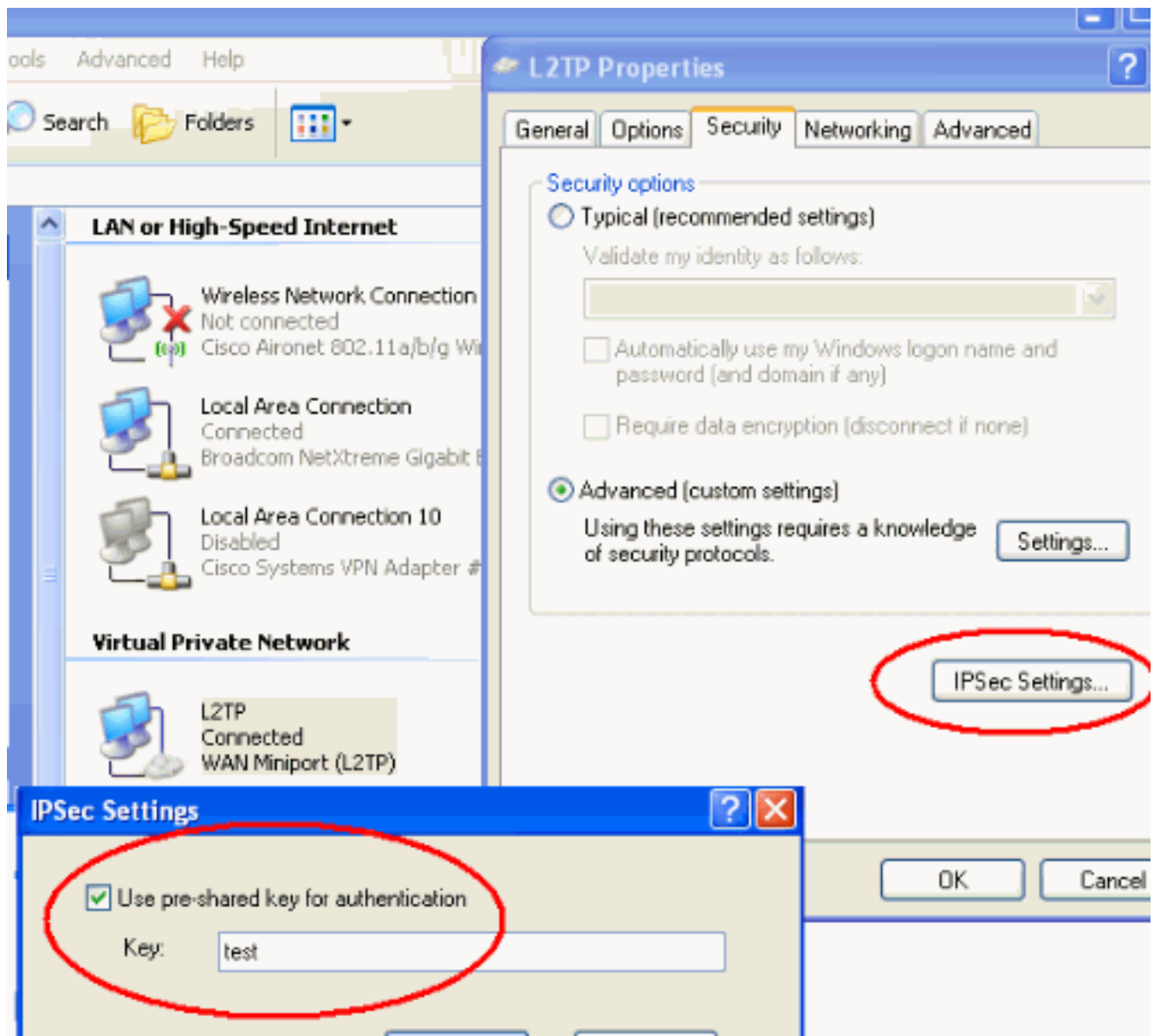
Windows IPsec. Consulte [Configurar uma Chave Pré-Compartilhada para Uso com Conexões do Protocolo de Tunelamento de Camada 2 no Windows XP \(Q281555\)](#) para obter mais informações.

3. Crie sua conexão.
4. Em Conexões dial-up e de rede, clique com o botão direito do mouse na conexão e escolha **Propriedades**. Vá até a guia Segurança e clique em **Avançado**. Escolha os protocolos como



esta imagem mostra.

5. **Note:** Esta etapa se aplica somente ao Windows XP. Clique em **Configurações de IPsec**, marque **Usar chave pré-compartilhada para autenticação** e digite a chave pré-compartilhada para definir a chave pré-compartilhada. Neste exemplo, o teste é usado como a chave pré-compartilhada.



Servidor L2TP na configuração PIX

PIX 7.2

```
pixfirewall#show run

PIX Version 7.2(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Configures the outside and inside interfaces.
interface Ethernet0 nameif outside security-level 0 ip
address 172.16.1.1 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.4.4.1
255.255.255.0 ! passwd 2KFQnbNIdI.2KYOU encrypted ftp
mode passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list nonat extended permit
ip 10.4.4.0 255.255.255.0 10.4.5.0 255.255.255.0
nat (inside) 0 access-list nonat

pager lines 24
```

```

logging console debugging
mtu outside 1500
mtu inside 1500

!--- Creates a pool of addresses from which IP addresses
are assigned !--- dynamically to the remote VPN Clients.
ip local pool clientVPNpool 10.4.5.10-10.4.5.20 mask
255.255.255.0

no failover
asdm image flash:/asdm-521.bin
no asdm history enable
arp timeout 14400

!--- The global and nat command enable !--- the Port
Address Translation (PAT) using an outside interface IP
!--- address for all outgoing traffic.

global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0

route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute

!--- Create the AAA server group "vpn" and specify its
protocol as RADIUS. !--- Specify the IAS server as a
member of the "vpn" group and provide its !--- location
and key. aaa-server vpn protocol radius
aaa-server vpn host 10.4.4.2
key radiuskey

!--- Identifies the group policy as internal. group-
policy DefaultRAGroup internal
!--- Instructs the security appliance to send DNS and !-
-- WINS server IP addresses to the client. group-policy
DefaultRAGroup attributes
wins-server value 10.4.4.99
dns-server value 10.4.4.99
!--- Configures L2TP over IPsec as a valid VPN tunneling
protocol for a group. vpn-tunnel-protocol IPSec l2tp-
ipsec
default-domain value cisco.com
!--- Configure usernames and passwords on the device !--
- in addition to using AAA. !--- If the user is an L2TP
client that uses Microsoft CHAP version 1 or !---
version 2, and the security appliance is configured !---
to authenticate against the local !--- database, you
must include the mschap keyword. !--- For example,
username

username test password DLaUiAX3178qgoB5c7iVNw== nt-

```

encrypted

vpn-tunnel-protocol l2tp-ipsec

http server enable

http 0.0.0.0 0.0.0.0 inside

no snmp-server location

no snmp-server contact

snmp-server enable traps snmp authentication linkup

linkdown coldstart

!--- Identifies the IPsec encryption and hash algorithms

*!--- to be used by the transform set. **crypto ipsec***

transform-set TRANS_ESP_3DES_MD5 esp-3des esp-md5-hmac

!--- Since the Windows 2000 L2TP/IPsec client uses IPsec

transport mode, !--- set the mode to transport. !--- The

*default is tunnel mode. **crypto ipsec transform-set***

TRANS_ESP_3DES_MD5 mode transport

!--- Specifies the transform sets to use in a dynamic

*crypto map entry. **crypto dynamic-map outside_dyn_map 20***

set transform-set TRANS_ESP_3DES_MD5

!--- Requires a given crypto map entry to refer to a

*pre-existing !--- dynamic crypto map. **crypto map***

outside_map 20 ipsec-isakmp dynamic outside_dyn_map

!--- Applies a previously defined crypto map set to an

*outside interface. **crypto map outside_map interface***

outside

crypto isakmp enable outside

crypto isakmp nat-traversal 20

*!--- Specifies the IKE Phase I policy parameters. **crypto***

isakmp policy 10

authentication pre-share

encryption 3des

hash md5

group 2

lifetime 86400

*!--- Creates a tunnel group with the **tunnel-group***

command, and specifies the local !--- address pool name

used to allocate the IP address to the client. !---

Associate the AAA server group (VPN) with the tunnel

group.

tunnel-group DefaultRAGroup general-attributes

address-pool clientVPNpool

authentication-server-group vpn

!--- Link the name of the group policy to the default

tunnel !--- group from tunnel group general-attributes

*mode. **default-group-policy DefaultRAGroup***

*!--- Use the **tunnel-group ipsec-attributes** command !---*

in order to enter the ipsec-attribute configuration


```
mode. !--- Set the pre-shared key. !--- This key should
be the same as the key configured on the Windows
machine.
```

```
tunnel-group DefaultRAGroup ipsec-attributes
pre-shared-key *
```

```
!--- Configures the PPP authentication protocol with the
authentication type !--- command from tunnel group ppp-
attributes mode.
```

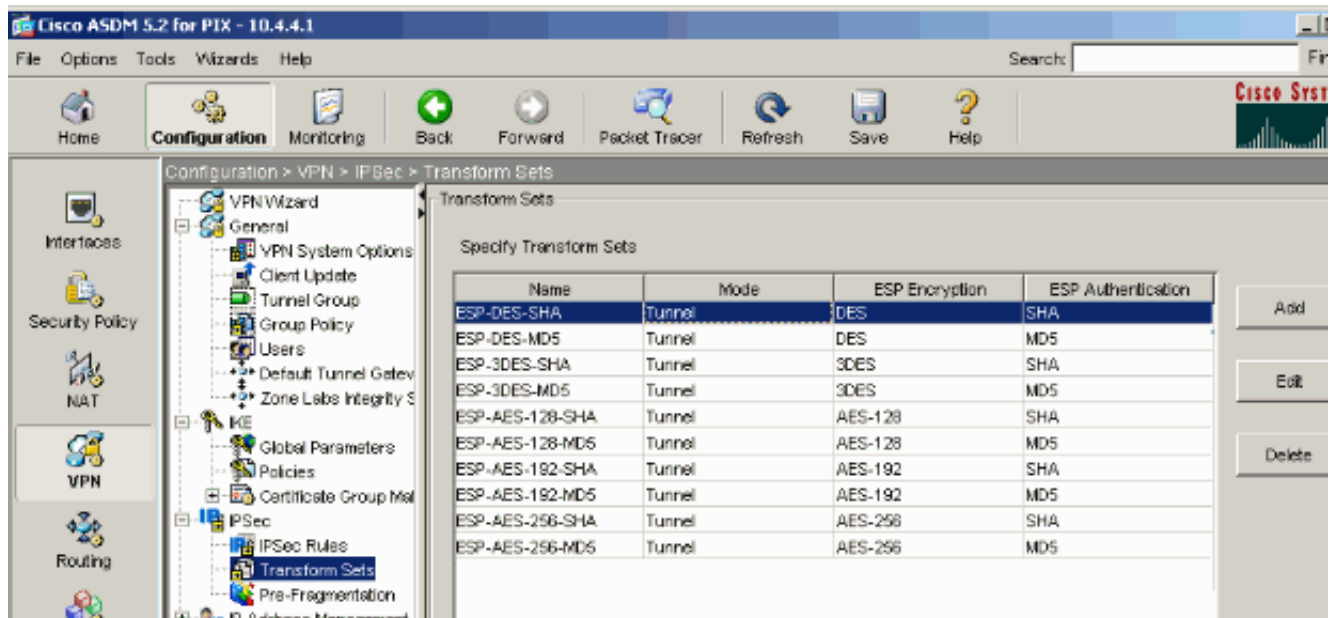
```
tunnel-group DefaultRAGroup ppp-attributes
no authentication chap
authentication ms-chap-v2
```

```
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:ele0730fa260244caa2e2784f632accd
: end
```

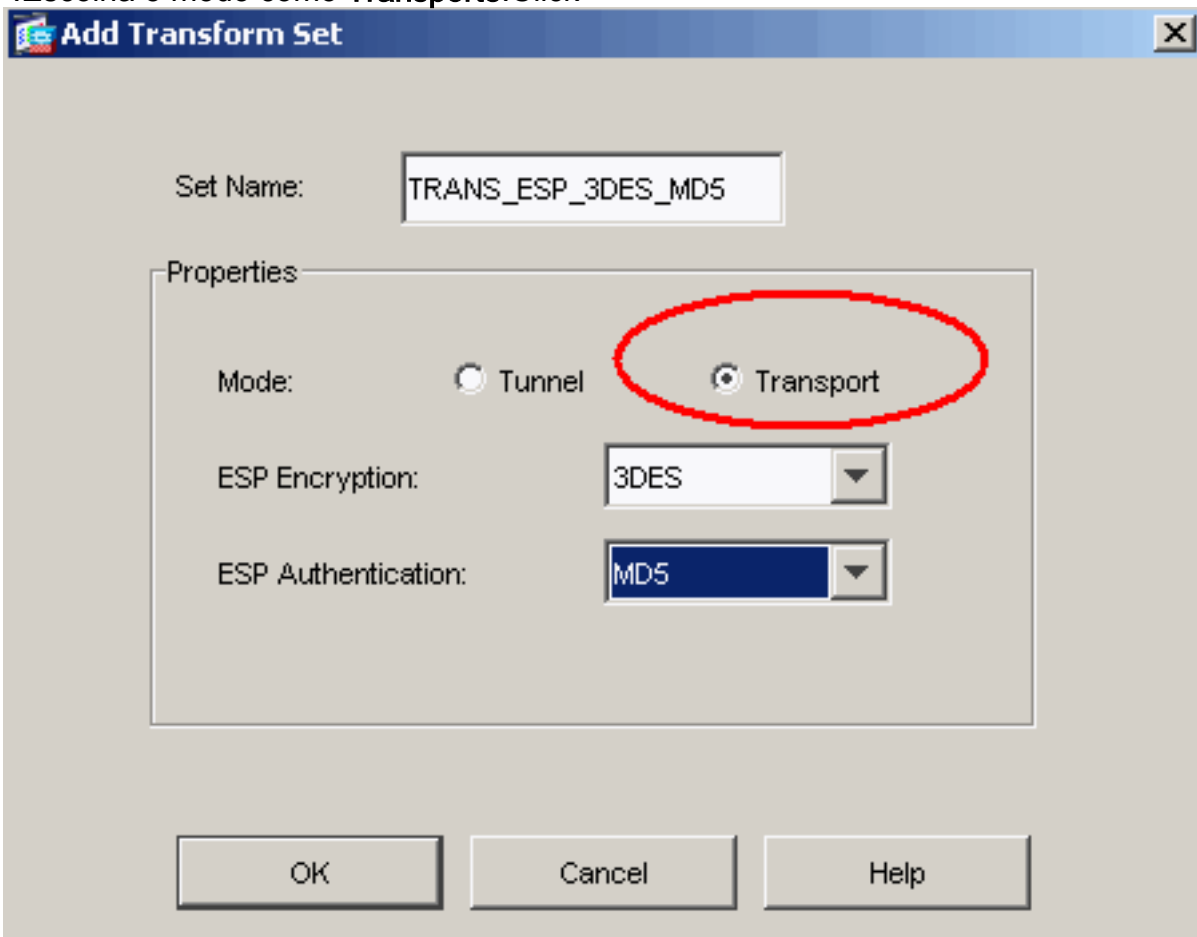
[L2TP usando a configuração ASDM](#)

Conclua estes passos para configurar o Security Appliance para aceitar conexões L2TP sobre IPsec:

1. Adicione um conjunto de transformação IPsec e especifique IPsec para usar o modo de transporte em vez do modo de túnel. Para fazer isso, escolha **Configuration > VPN > IPsec > Transform Sets** e clique em **Add**. O painel Conjuntos de transformação é exibido.

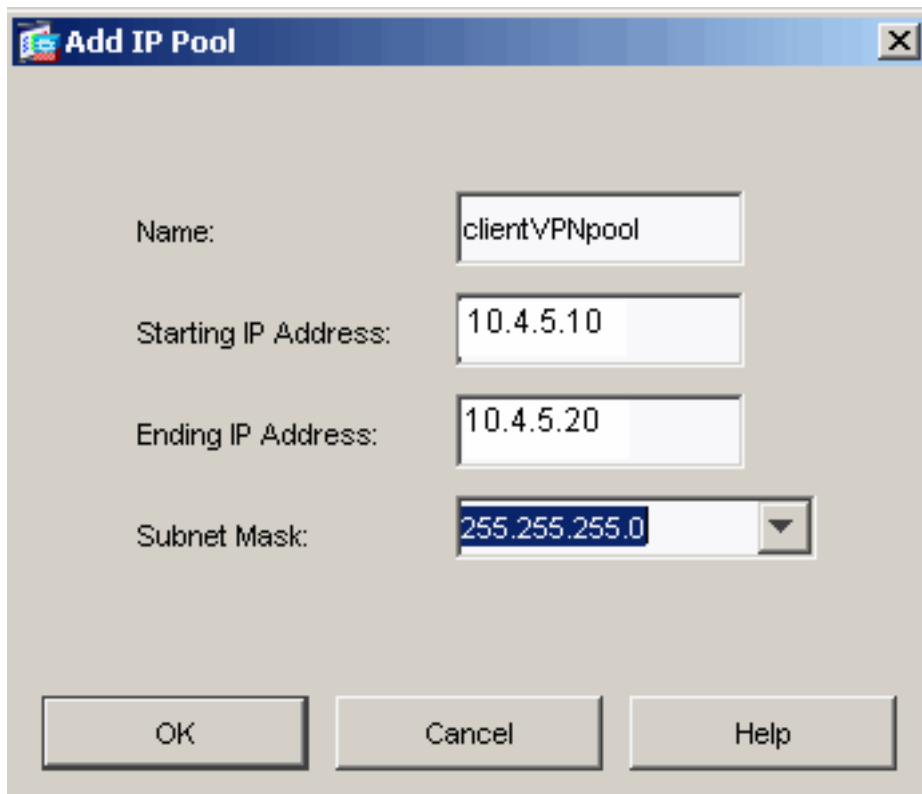


2. Conclua estes passos para adicionar um conjunto de transformação: Insira um nome para o conjunto de transformações. Escolha os métodos de criptografia ESP e autenticação ESP. Escolha o modo como **Transporte**. Click



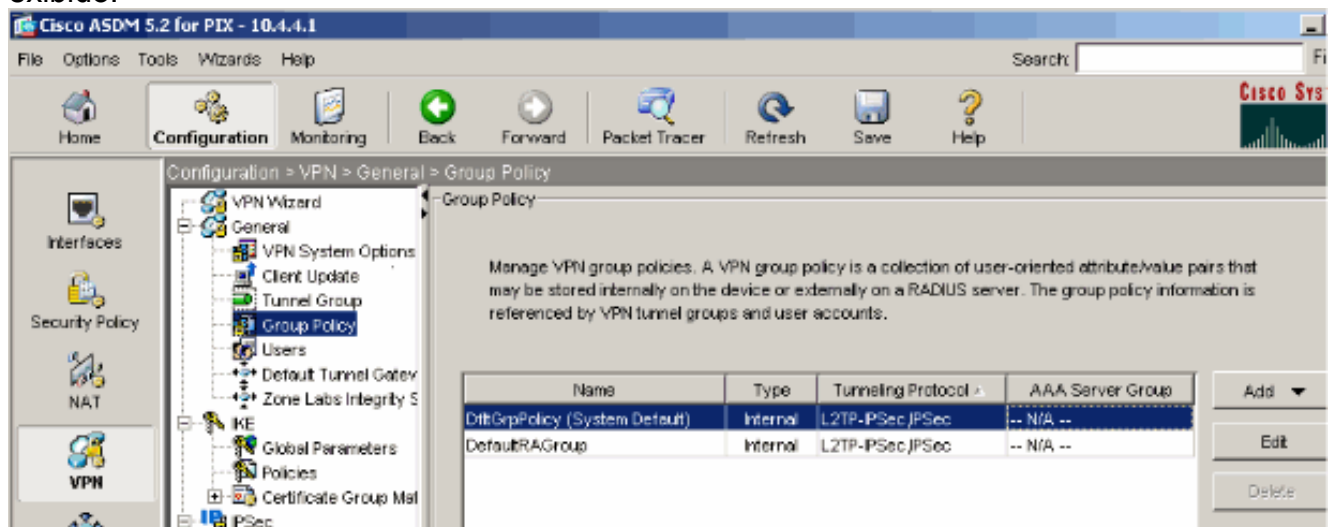
OK.

3. Conclua estas etapas para configurar um método de atribuição de endereço. Este exemplo usa pools de endereços IP. Escolha **Configuration > VPN > IP Address Management > IP Pools**. Clique em Add. A caixa de diálogo Add IP Pool é exibida. Digite o nome do novo pool de endereços IP. Insira os endereços IP inicial e final. Digite a máscara de sub-rede e clique

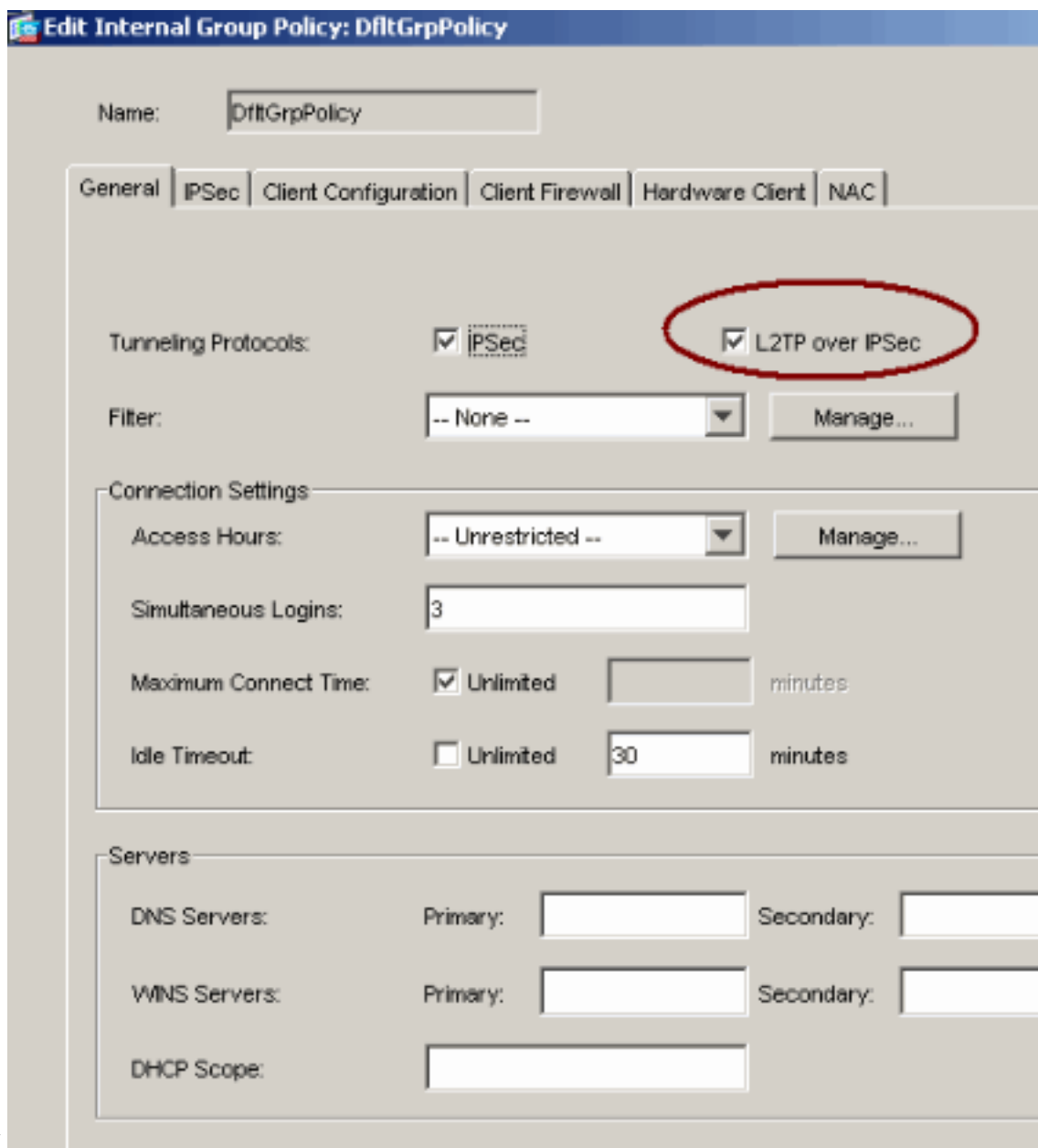


em OK.

- Escolha **Configuration > VPN > General > Group Policy** para configurar L2TP sobre IPsec como um protocolo de tunelamento VPN válido para a política de grupo. O painel Diretiva de grupo é exibido.

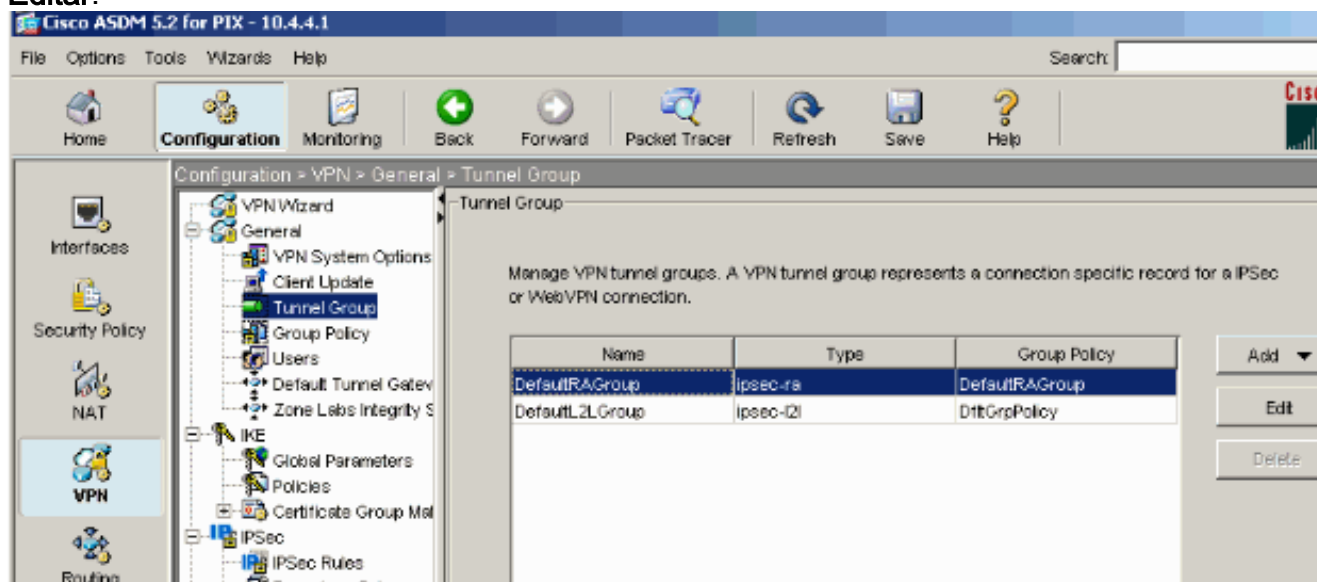


- Selecione uma política de grupo (DiffGrpPolicy) e clique em **Editar**. A caixa de diálogo Editar política de grupo é exibida. Marque **L2TP sobre IPsec** para habilitar o protocolo para a política de grupo e clique em



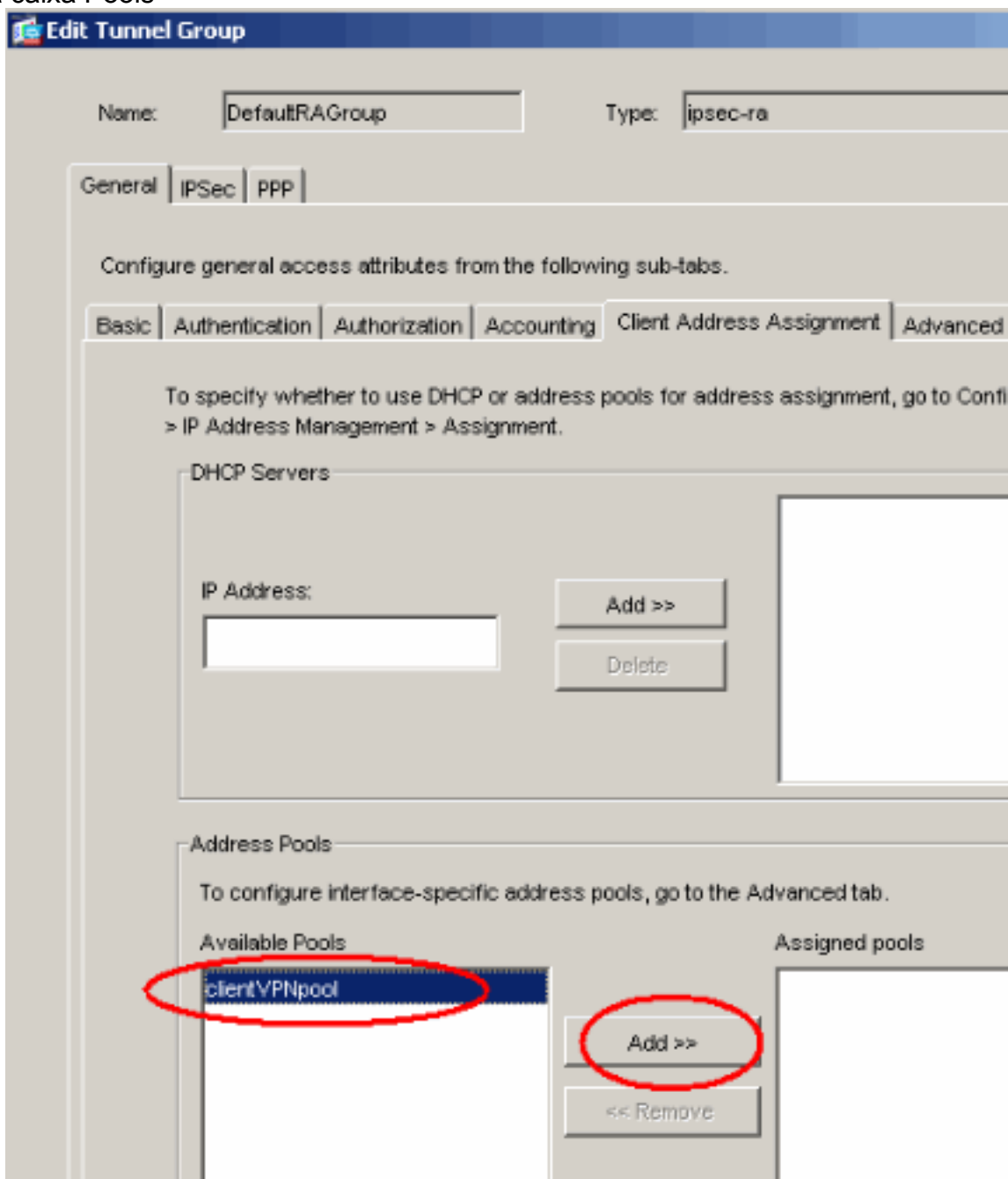
OK.

- Conclua estes passos para atribuir o pool de endereços IP a um grupo de túneis: Escolha **Configuration > VPN > General > Tunnel Group**. Depois que o painel Grupo de Túneis for exibido, selecione um grupo de túnel (DefaultRAGroup) na tabela. Clique em **Editar**.



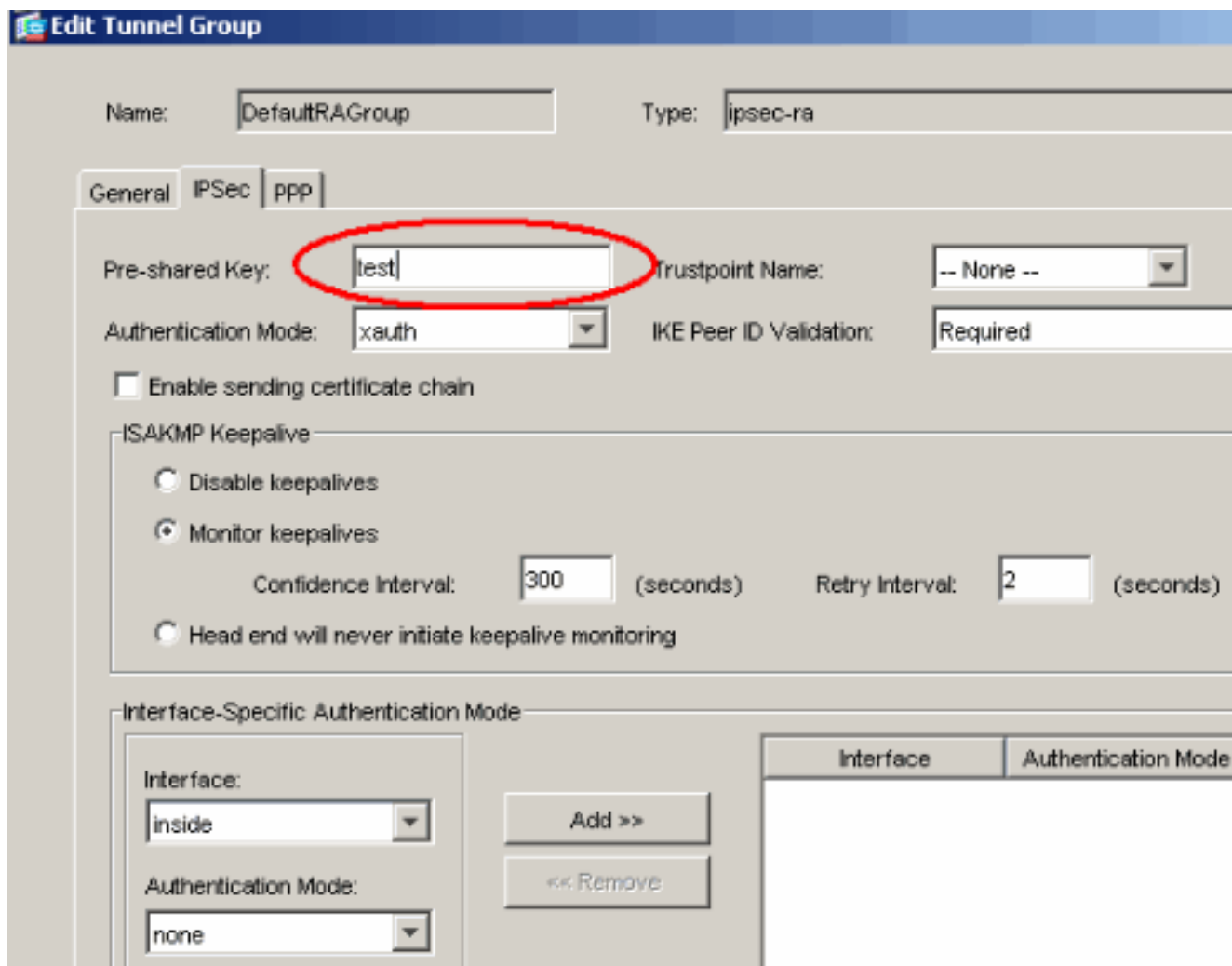
- Conclua estes passos quando a janela Editar grupo de túnel for exibida: Na guia Geral,

acesse a guia Atribuição de endereço do cliente. Na área Pools de endereços, escolha um pool de endereços para atribuir ao grupo de túneis. Clique em Add. O pool de endereços é exibido na caixa Pools

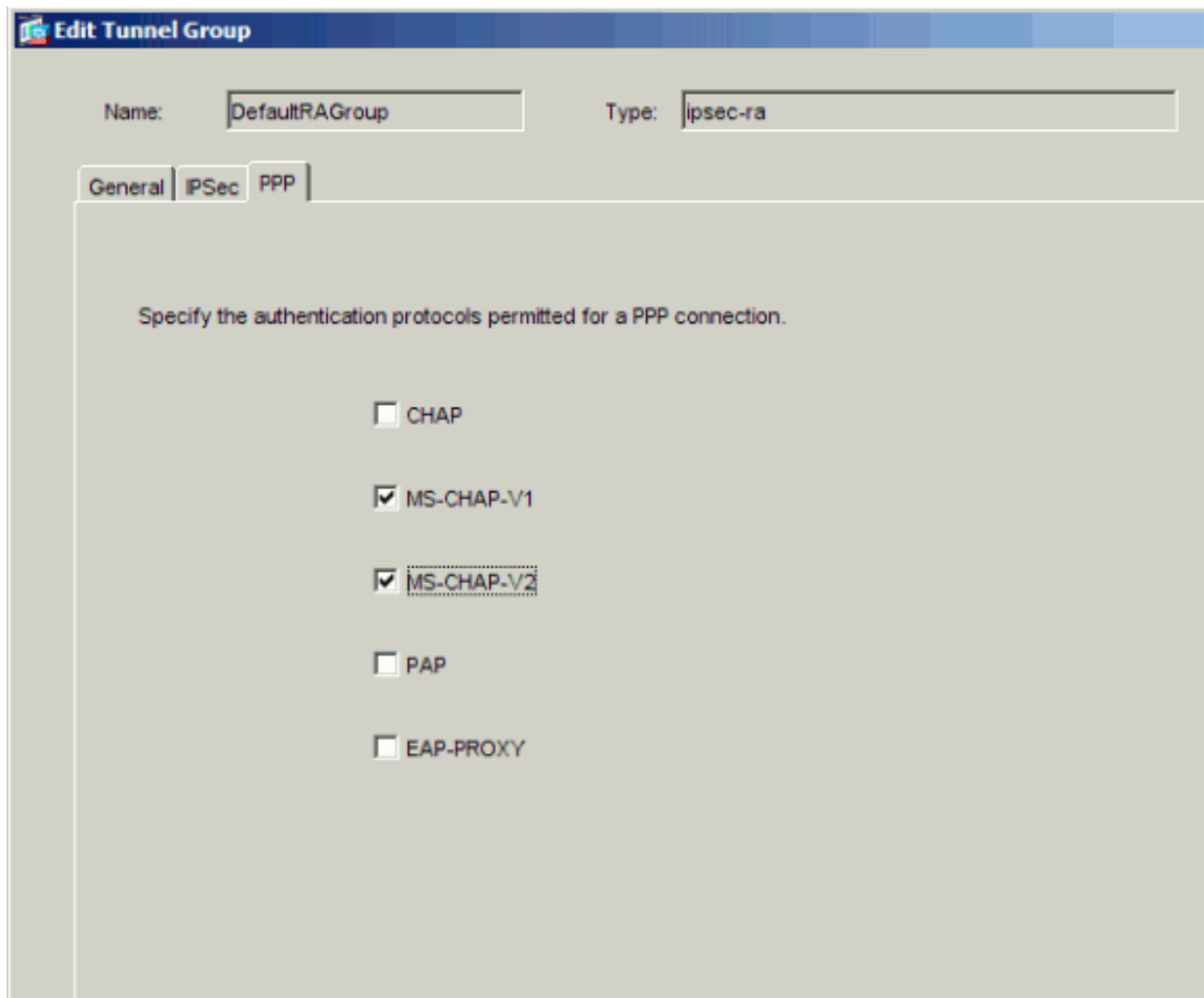


atribuídos.

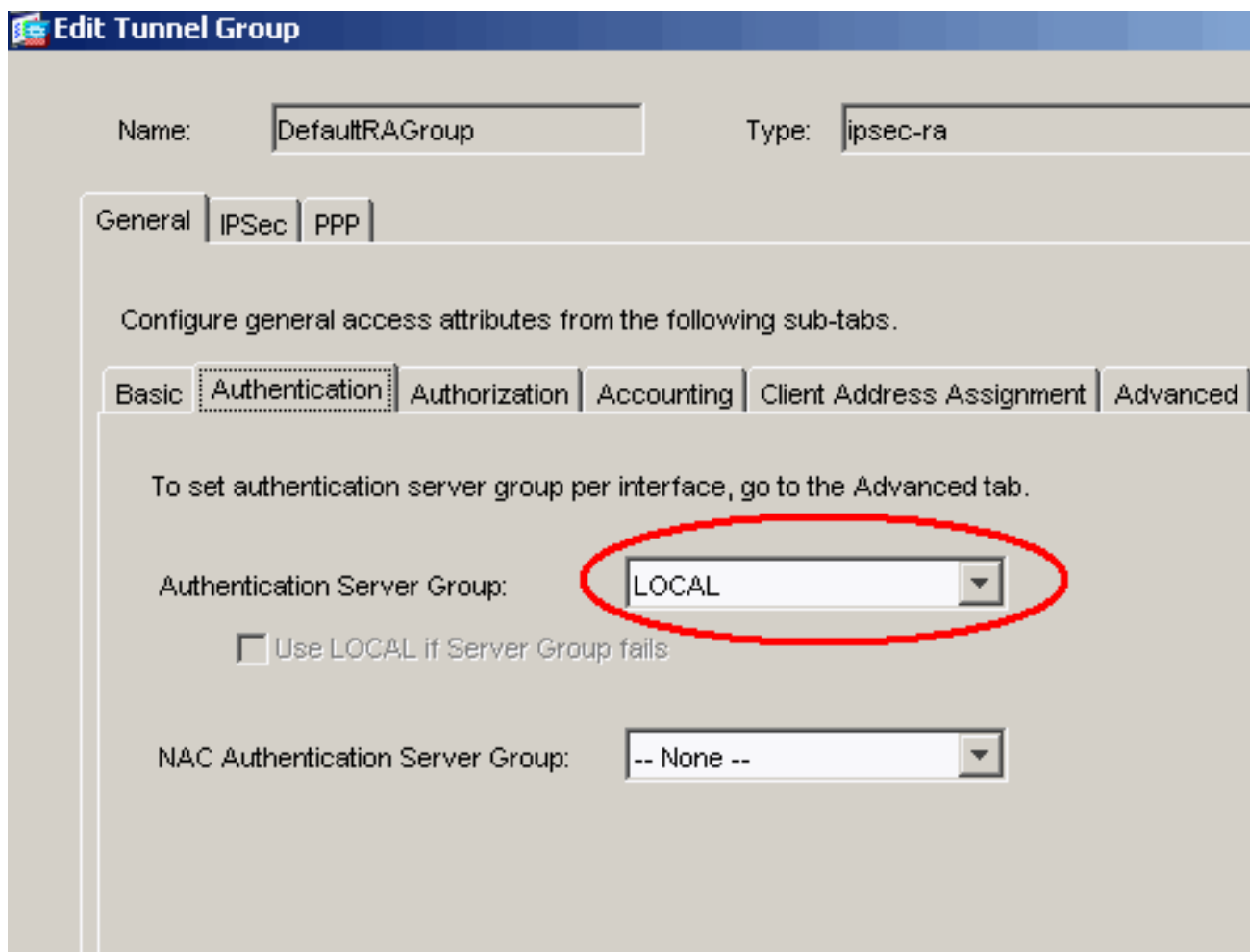
8. Para definir a chave pré-compartilhada, vá até a guia IPSec, insira sua **chave pré-compartilhada** e clique em **OK**.



9. O L2TP sobre IPsec usa protocolos de autenticação PPP. Especifique os protocolos permitidos para conexões PPP na guia PPP do grupo de túneis. Selecione o protocolo **MS-CHAP-V1** para autenticação.



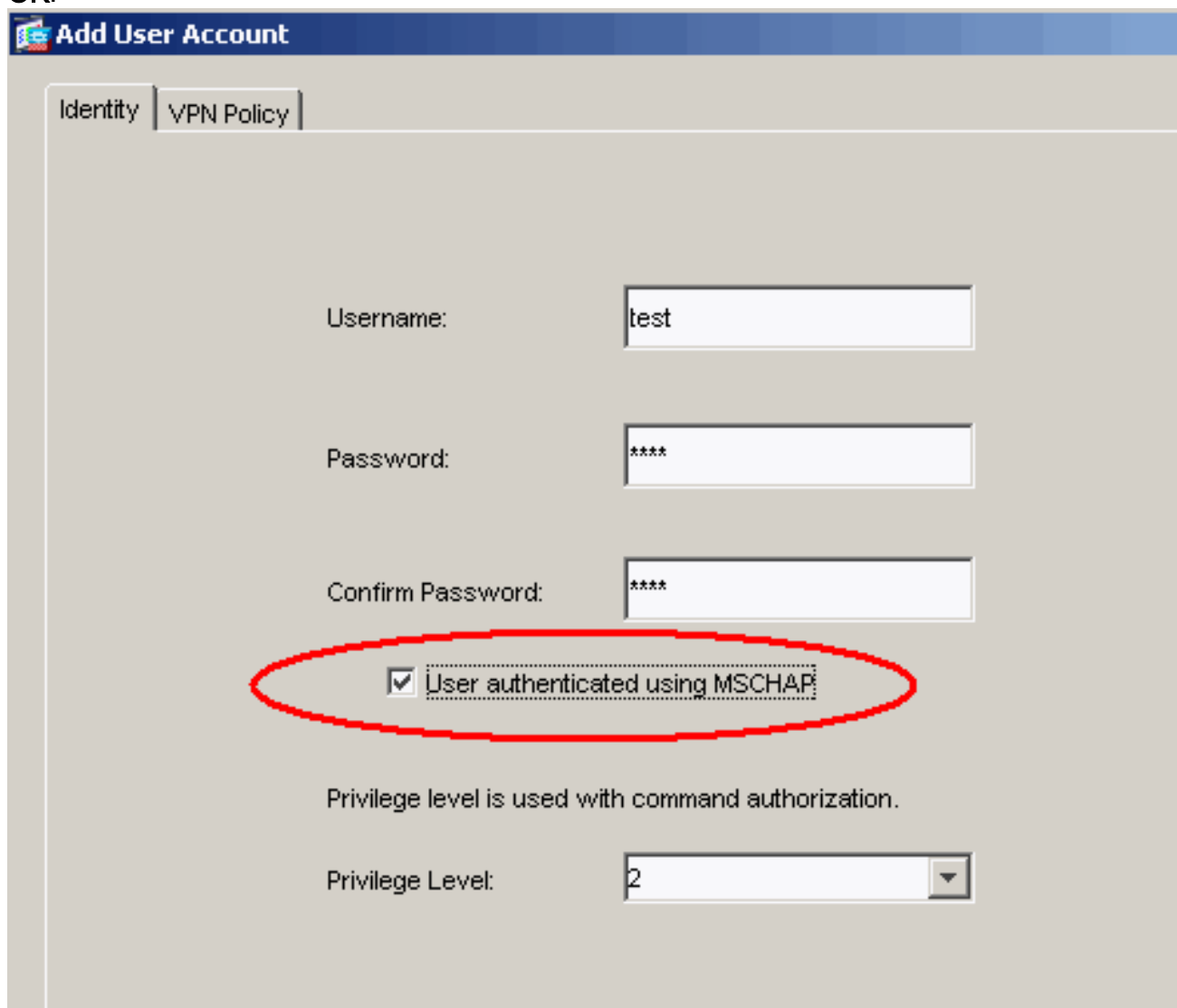
10. Especifique um método para autenticar usuários que tentam conexões L2TP sobre IPsec. Você pode configurar o Security Appliance para usar um servidor de autenticação ou seu próprio banco de dados local. Para fazer isso, acesse a guia Authentication (Autenticação) do grupo tunnel. Por padrão, o Security Appliance usa seu banco de dados local. A lista suspensa Grupo de servidores de autenticação exibe LOCAL. Para usar um servidor de autenticação, selecione um na lista. **Observação:** o Security Appliance oferece suporte somente às autenticações PPP PAP e Microsoft CHAP versões 1 e 2 no banco de dados local. O EAP e o CHAP são executados por servidores de autenticação de proxy. Portanto, se um usuário remoto pertencer a um grupo de túneis configurado com EAP ou CHAP e o Security Appliance estiver configurado para usar o banco de dados local, esse usuário não poderá se conectar.



Observação: escolha **Configuration > VPN > General > Tunnel Group** para voltar à configuração do grupo de túneis para que você possa vincular a política de grupo ao grupo de túneis e ativar Tunnel Group Switching (opcional). Quando o painel Grupo de Túneis for exibido, escolha o grupo de túneis e clique em **Editar**. **Observação:** o Tunnel Group Switching permite que o Security Appliance associe diferentes usuários que estabelecem conexões L2TP sobre IPsec a diferentes grupos de túneis. Como cada grupo de túneis tem seu próprio grupo de servidores AAA e pools de endereços IP, os usuários podem ser autenticados através de métodos específicos para seu grupo de túneis. Com esse recurso, em vez de enviar apenas um nome de usuário, o usuário envia um nome de usuário e um nome de grupo no formato `username@group_name`, onde "@" representa um delimitador que você pode configurar, e o nome do grupo é o nome de um grupo de túneis configurado no Security Appliance. **Observação:** a Túnel Group Switching é habilitada pelo processamento do Strip Group, que permite que o Security Appliance selecione o grupo de túneis para conexões de usuário obtendo o nome do grupo do nome de usuário apresentado pelo VPN Client. O Security Appliance envia somente a parte do usuário do nome de usuário para autorização e autenticação. Caso contrário (se desabilitado), o Security Appliance enviará o nome de usuário inteiro, incluindo o território. Para habilitar a Túnel Group Switching, marque **Strip the realm from username antes de passá-lo para o servidor AAA** e marque **Strip the group from username antes de passá-lo para o servidor AAA**. Em seguida, clique em "OK".

11. Conclua estes passos para criar um usuário no banco de dados local: Escolha **Configuration > Properties > Device Administration > User Accounts**. Clique em Add. Se o usuário for um cliente L2TP que usa o Microsoft CHAP versão 1 ou 2, e o Security Appliance estiver configurado para autenticação no banco de dados local, você deverá

verificar **Autenticado pelo Usuário usando o MSCHAP** para habilitar o MSCHAP. Clique em OK.



Add User Account

Identity | VPN Policy

Username: test

Password: ****

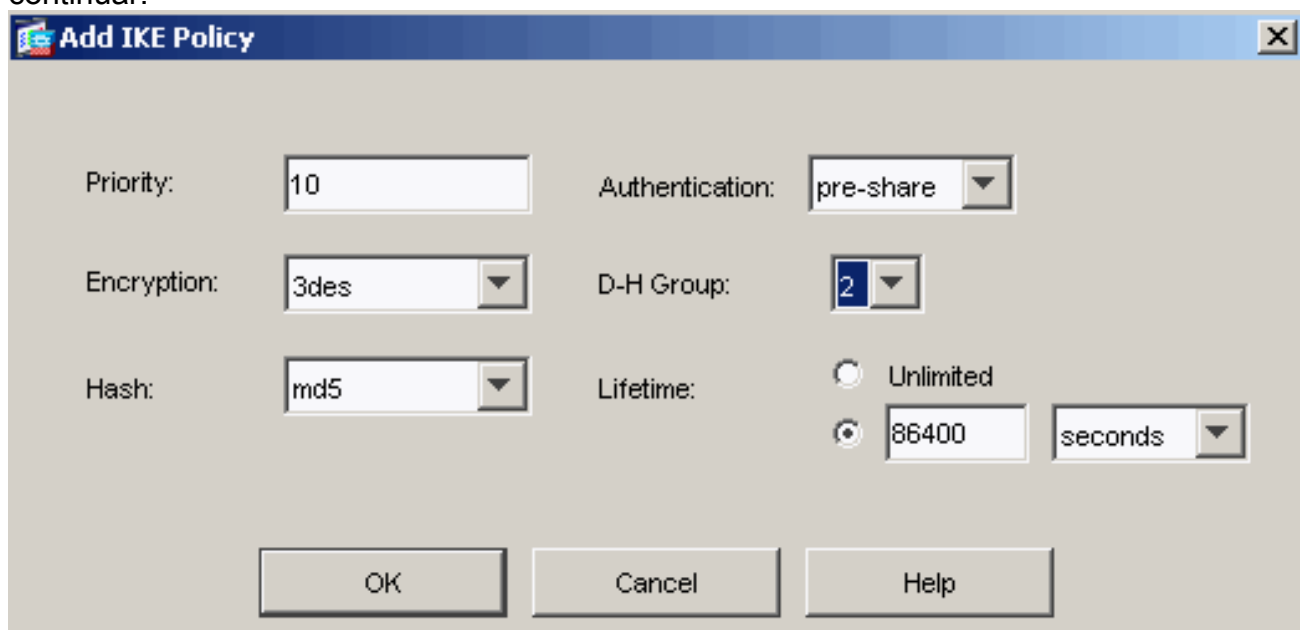
Confirm Password: ****

User authenticated using MSCHAP

Privilege level is used with command authorization.

Privilege Level: 2

12. Escolha **Configuration > VPN > IKE > Policies** e clique em **Add** para criar uma política IKE para a Fase I. Clique em OK para continuar.



Add IKE Policy

Priority: 10 Authentication: pre-share

Encryption: 3des D-H Group: 2

Hash: md5 Lifetime: Unlimited 86400 seconds

OK Cancel Help

13. (Opcional) Se você espera que vários clientes L2TP atrás de um dispositivo NAT tentem

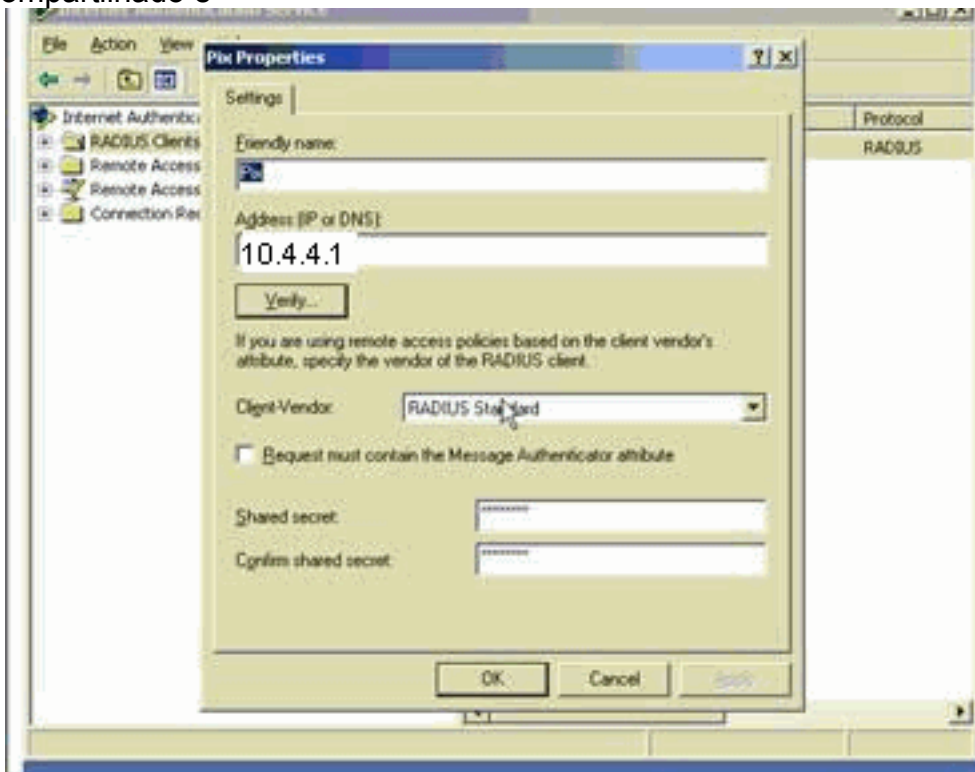
conexões L2TP sobre IPsec com o Security Appliance, você deve ativar a passagem de NAT para que os pacotes ESP possam passar por um ou mais dispositivos NAT. Conclua estes passos para fazer isso: Escolha **Configuration > VPN > IKE > Global Parameters**. Verifique se **ISAKMP** está habilitado em uma interface. Marque **Ativar IPsec sobre NAT-T**. Clique **OK**.

[Microsoft Windows 2003 Server com configuração IAS](#)

Conclua estes passos para configurar o servidor Microsoft Windows 2003 com IAS.

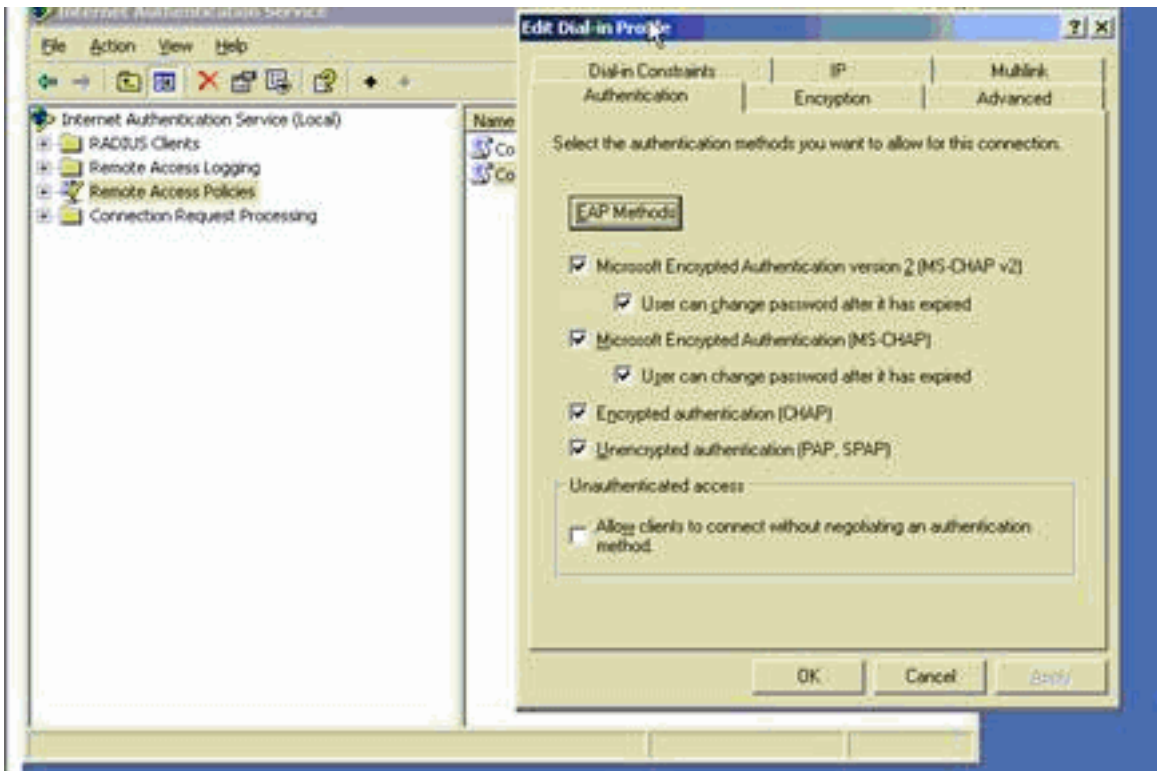
Observação: estas etapas presumem que o IAS já está instalado na máquina local. Caso contrário, adicione-o através do **Painel de controle > Adicionar ou remover programas**.

1. Escolha **Administrative Tools > Internet Authentication Service** e clique com o botão direito do mouse em **RADIUS Client** para adicionar um novo cliente RADIUS. Depois de digitar as informações do cliente, clique em **OK**. Este exemplo mostra um cliente chamado "Pix" com um endereço IP de 10.4.4.1. Client-Vendor está definido como **RADIUS Standard**, e o segredo compartilhado é



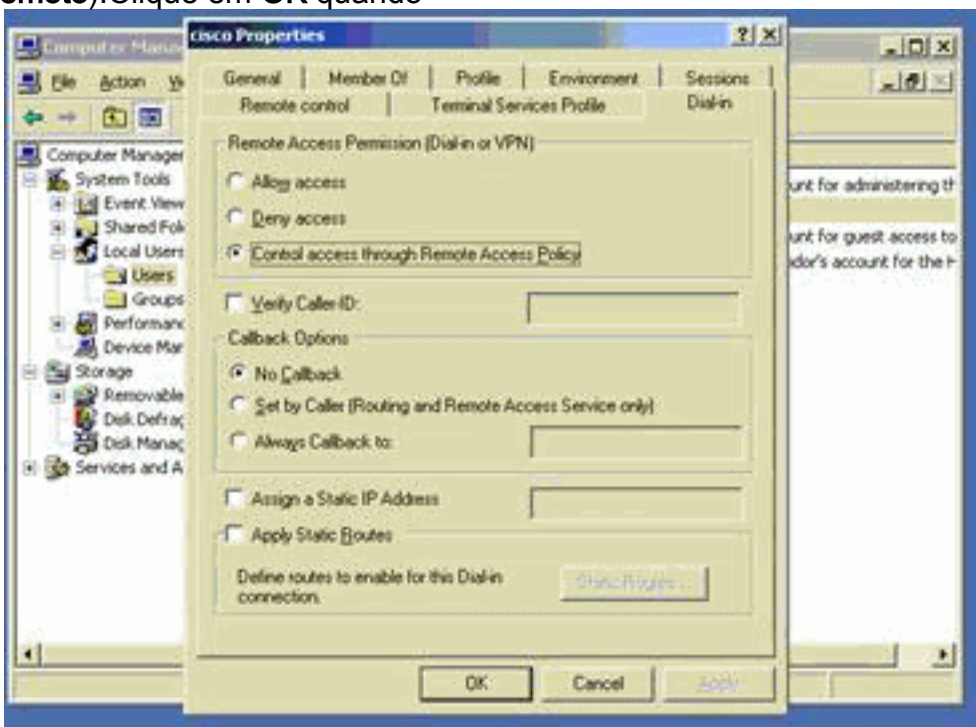
radiuskey.

2. Escolha **Políticas de acesso remoto**, clique com o botão direito do mouse em **Conexões a outros servidores de acesso** e selecione **Propriedades**.
3. Verifique se a opção **Grant Remote Access Permissions** está selecionada.
4. Clique em **Editar perfil** e verifique estas configurações: Na guia **Autenticação**, marque **Autenticação não criptografada (PAP, SPAP)**. Na guia **Encryption (Criptografia)**, verifique se a opção **No Encryption (Sem criptografia)** está selecionada. Clique em **OK** quando



terminar.

5. Escolha **Administrative Tools > Computer Management > System Tools > Local Users and Groups**, clique com o botão direito do mouse em **Users** e selecione **New Users** para adicionar um usuário à conta do computador local.
6. Adicione um usuário com a senha da Cisco **password1** e verifique estas informações de perfil: Na guia Geral, certifique-se de que a opção **Senha nunca expirada** esteja selecionada, em vez da opção Usuário deve alterar a senha. Na guia Discar, selecione a opção **Permitir acesso** (ou deixe a configuração padrão de **acesso de controle por meio da Diretiva de acesso remoto**). Clique em **OK** quando



terminar.

[Autenticação estendida para L2TP sobre IPSec usando o Active Directory](#)

Use esta configuração no ASA para permitir que a autenticação da conexão L2tp ocorra a partir do Active Directory:

```
ciscoasa(config-tunnel-general)# tunnel-group DefaultRAGroup
ppp-attributes
ciscoasa(config-ppp)# authentication pap
```

Além disso, no cliente L2tp, vá para **Advanced Security Settings (Custom)** e escolha somente a opção **Unencrypted password (PAP)**.

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **show crypto ipsec sa** — Mostra todas as associações de segurança (SAs) IKE atuais em um peer.

```
pixfirewall#show crypto ipsec sa
interface: outside
  Crypto map tag: outside_dyn_map, seq num: 20, local addr: 172.16.1.1

  access-list 105 permit ip host 172.16.1.1 host 192.168.0.2
  local ident (addr/mask/prot/port): (172.16.1.1/255.255.255.255/17/0)
  remote ident (addr/mask/prot/port): (192.168.0.2/255.255.255.255/17/1701)
  current_peer: 192.168.0.2, username: test
  dynamic allocated peer ip: 10.4.5.15

#pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 23
#pkts decaps: 93, #pkts decrypt: 93, #pkts verify: 93
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 23, #pkts comp failed: 0, #pkts decomp failed: 0
#post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1, remote crypto endpt.: 192.168.0.2

path mtu 1500, ipsec overhead 58, media mtu 1500
current outbound spi: C16F05B8

inbound esp sas:
  spi: 0xEC06344D (3959829581)
  transform: esp-3des esp-md5-hmac
  in use settings ={RA, Transport, }
  slot: 0, conn_id: 3, crypto-map: outside_dyn_map
  sa timing: remaining key lifetime (sec): 3335
  IV size: 8 bytes
  replay detection support: Y

outbound esp sas:
  spi: 0xC16F05B8 (3245278648)
  transform: esp-3des esp-md5-hmac
  in use settings ={RA, Transport, }
  slot: 0, conn_id: 3, crypto-map: outside_dyn_map
  sa timing: remaining key lifetime (sec): 3335
  IV size: 8 bytes
  replay detection support: Y
```

- **show crypto isakmp sa** — Mostra todas as SAs IKE atuais em um peer.

```
pixfirewall#show crypto isakmp sa
```

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

```
1 IKE Peer: 192.168.0.2
Type      : user          Role      : responder
Rekey     : no           State     : MM_ACTIVE
```

- **show vpn-sessiondb** —Inclui filtros de protocolo que você pode usar para exibir informações detalhadas sobre conexões L2TP sobre IPsec. O comando completo do modo de configuração global é **show vpn-sessiondb detailed remote filter protocol l2tpoveripsec**. Este exemplo mostra os detalhes de uma única conexão L2TP sobre IPsec:

```
pixfirewall#show vpn-sessiondb detail remote filter protocol l2tpoveripsec
```

```
Session Type: Remote Detailed
```

```
Username      : test
Index         : 1
Assigned IP   : 10.4.5.15      Public IP    : 192.168.0.2
Protocol      : L2TPOverIPSec Encryption   : 3DES
Hashing       : MD5
Bytes Tx      : 1336          Bytes Rx     : 14605
Client Type   :              Client Ver     :
Group Policy  : DefaultRAGroup
Tunnel Group  : DefaultRAGroup
Login Time    : 18:06:08 UTC Fri Jan 1 1993
Duration      : 0h:04m:25s
Filter Name   :
NAC Result    : N/A
Posture Token :
```

```
IKE Sessions: 1
IPSec Sessions: 1
L2TPOverIPSec Sessions: 1
```

```
IKE:
```

```
Session ID    : 1
UDP Src Port  : 500          UDP Dst Port : 500
IKE Neg Mode  : Main        Auth Mode     : preSharedKeys
Encryption    : 3DES       Hashing       : MD5
Rekey Int (T): 28800 Seconds Rekey Left(T): 28536 Seconds
D/H Group     : 2
```

```
IPSec:
```

```
Session ID    : 2
Local Addr    : 172.16.1.1/255.255.255.255/17/1701
Remote Addr   : 192.168.0.2/255.255.255.255/17/1701
Encryption    : 3DES       Hashing       : MD5
Encapsulation: Transport
Rekey Int (T): 3600 Seconds Rekey Left(T): 3333 Seconds
Idle Time Out: 30 Minutes  Idle TO Left  : 30 Minutes
Bytes Tx      : 1336       Bytes Rx      : 14922
Pkts Tx       : 25        Pkts Rx      : 156
```

```
L2TPOverIPSec:
```

```
Session ID    : 3
Username      : test
Assigned IP   : 10.4.5.15
Encryption    : none       Auth Mode     : msCHAPV1
```

Idle Time Out: 30 Minutes
Bytes Tx : 378
Pkts Tx : 16

Idle TO Left : 30 Minutes
Bytes Rx : 13431
Pkts Rx : 146

Troubleshoot

Esta seção fornece informações para solucionar problemas de configuração. Exemplo de saída de depuração também é mostrado.

Comandos para Troubleshooting

Determinados comandos são suportados pela [Output Interpreter Tool](#) (somente clientes [registrados](#)), que permite exibir uma análise da saída do comando **show**.

Observação: consulte [Informações Importantes sobre Comandos de Depuração](#) e [Solução de Problemas de Segurança de IP - Entendendo e Usando Comandos de Depuração](#) antes de usar comandos de depuração.

- **debug crypto ipsec 7** — Exibe as negociações de IPsec da Fase 2.
- **debug crypto isakmp 7** — Exibe as negociações ISAKMP da Fase 1.

Exemplo de saída de depuração

Firewall de PIX

```
PIX#debug crypto isakmp 7
pixfirewall# Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Mess
age (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR
(13) + NONE (0) total length : 256
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Oakley proposal is acceptable
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received Fragmentation VID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing VID payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Received NAT-Traversal ver 02 V
ID
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing IKE SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, IKE SA Proposal # 1, Transform
# 2 acceptable Matches global IKE entry # 2
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ISAKMP SA payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Fragmentation VID
+ extended capabilities payload
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 104
Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + NONE (0) total length : 184
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ke payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing ISA_KE payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, processing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing ke payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing nonce payload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing Cisco Unity VID pa
yload
Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing xauth V6 VID paylo
```

ad

Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send IOS VID

Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001)

Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, constructing VID payload

Jan 02 18:26:44 [IKEv1 DEBUG]: IP = 192.168.0.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group DefaultRAGroup

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generating keys for Responder...

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 256

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + NONE (0) total length : 60

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing ID payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing hash payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computing hash for ISAKMP

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection landed on tunnel_group DefaultRAGroup

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Freeing previously allocated memory for authorization-dn-attributes

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing ID payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing hash payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computing hash for ISAKMP

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing dpd vid payload

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 80

!--- Phase 1 completed successfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, **PHASE 1 COMPLETED**

ETED

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alive type for this connection: None

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Keep-alives configured on but peer does not support keep-alives (type = None)

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Starting P1 rekey timer: 21600 seconds.

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1b84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 164

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing hash payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing SA payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing nonce payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing ID payload

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received remote Proxy Host data in ID Payload: Address 192.168.0.2, Protocol 17, Port 1701

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing ID payload

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received local Proxy Host data in ID Payload: Address 172.16.1.1, Protocol 17, Port 1701

!--- PIX identifies the L2TP/IPsec session. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, **L2TP/IPSec session detected.**

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, QM IsRekeyed old sa not found by addr

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE Remote Peer configured for crypto map: outside_dyn_map

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing IPsec SA payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IPsec SA Proposal # 1, Transform # 1 acceptable Matches global IPsec SA entry # 20

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE: requesting SPI!

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got SPI from key engine: SPI = 0xce9f6e19

!--- Constructs Quick mode in Phase 2. Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, **oakley**

constructing quick mode

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing blank hash payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing IPsec SA payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing IPsec nonce payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing proxy ID

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Transmitting Proxy Id:

Remote host: 192.168.0.2 Protocol 17 Port 1701

Local host: 172.16.1.1 Protocol 17 Port 1701

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constructing qm hash payload

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=elb84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 144

Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=elb84b0) with payloads : HDR + HASH (8) + NONE (0) total length : 48

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, processing hash payload

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, loading all IPSEC SAs

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generating Quick Mode Key!

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generating Quick Mode Key!

Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Security negotiation complete for User () Responder, Inbound SPI = 0xce9f6e19, Outbound SPI = 0xd08f711b

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IKE got a KEY_ADD msg for SA: SPI = 0xd08f711b

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Pitcher: received KEY_UPDATE, spi 0xce9f6e19

Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Starting P2 rekey timer: 3059 seconds.

!--- Phase 2 completes successfully. Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, PHASE 2 COMPLETED (msgid=0elb84b0) Jan 02 18:26:44 [IKEv1]: IKEQM_Active() Add L2TP classification rules: ip <192.168.0.2> mask <0xFFFFFFFF> port <1701> PIX#**debug crypto ipsec 7**

pixfirewall# IPSEC: Deleted inbound decrypt rule, SPI 0x71933D09

Rule ID: 0x028D78D8

IPSEC: Deleted inbound permit rule, SPI 0x71933D09

Rule ID: 0x02831838
IPSEC: Deleted inbound tunnel flow rule, SPI 0x71933D09
Rule ID: 0x029134D8
IPSEC: Deleted inbound VPN context, SPI 0x71933D09
VPN handle: 0x0048B284
IPSEC: Deleted outbound encrypt rule, SPI 0xAF4DA5FA
Rule ID: 0x028DAC90
IPSEC: Deleted outbound permit rule, SPI 0xAF4DA5FA
Rule ID: 0x02912AF8
IPSEC: Deleted outbound VPN context, SPI 0xAF4DA5FA
VPN handle: 0x0048468C
IPSEC: New embryonic SA created @ 0x01BFCF80,
SCB: 0x01C262D0,
Direction: inbound
SPI : 0x45C3306F
Session ID: 0x0000000C
VPIF num : 0x00000001
Tunnel type: ra
Protocol : esp
Lifetime : 240 seconds
IPSEC: New embryonic SA created @ 0x0283A3A8,
SCB: 0x028D1B38,
Direction: outbound
SPI : 0x370E8DD1
Session ID: 0x0000000C
VPIF num : 0x00000001
Tunnel type: ra
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0x370E8DD1
IPSEC: Creating outbound VPN context, SPI 0x370E8DD1
Flags: 0x00000205
SA : 0x0283A3A8
SPI : 0x370E8DD1
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x028D1B38
Channel: 0x01693F08
IPSEC: Completed outbound VPN context, SPI 0x370E8DD1
VPN handle: 0x0048C164
IPSEC: New outbound encrypt rule, SPI 0x370E8DD1
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.0.2
Dst mask: 255.255.255.255
Src ports
Upper: 1701
Lower: 1701
Op : equal
Dst ports
Upper: 1701
Lower: 1701
Op : equal
Protocol: 17
Use protocol: true
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x370E8DD1
Rule ID: 0x02826540
IPSEC: New outbound permit rule, SPI 0x370E8DD1
Src addr: 172.16.1.1
Src mask: 255.255.255.255
Dst addr: 192.168.0.2

Dst mask: 255.255.255.255
Src ports
 Upper: 0
 Lower: 0
 Op : ignore
Dst ports
 Upper: 0
 Lower: 0
 Op : ignore
Protocol: 50
Use protocol: true
SPI: 0x370E8DD1
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x370E8DD1
 Rule ID: 0x028D78D8
IPSEC: Completed host IBSA update, SPI 0x45C3306F
IPSEC: Creating inbound VPN context, SPI 0x45C3306F
 Flags: 0x00000206
 SA : 0x01BF8CF80
 SPI : 0x45C3306F
 MTU : 0 bytes
 VCID : 0x00000000
 Peer : 0x0048C164
 SCB : 0x01C262D0
 Channel: 0x01693F08
IPSEC: Completed inbound VPN context, SPI 0x45C3306F
 VPN handle: 0x0049107C
IPSEC: Updating outbound VPN context 0x0048C164, SPI 0x370E8DD1
 Flags: 0x00000205
 SA : 0x0283A3A8
 SPI : 0x370E8DD1
 MTU : 1500 bytes
 VCID : 0x00000000
 Peer : 0x0049107C
 SCB : 0x028D1B38
 Channel: 0x01693F08
IPSEC: Completed outbound VPN context, SPI 0x370E8DD1
 VPN handle: 0x0048C164
IPSEC: Completed outbound inner rule, SPI 0x370E8DD1
 Rule ID: 0x02826540
IPSEC: Completed outbound outer SPD rule, SPI 0x370E8DD1
 Rule ID: 0x028D78D8
IPSEC: New inbound tunnel flow rule, SPI 0x45C3306F
 Src addr: 192.168.0.2
 Src mask: 255.255.255.255
 Dst addr: 172.16.1.1
 Dst mask: 255.255.255.255
 Src ports
 Upper: 1701
 Lower: 1701
 Op : equal
 Dst ports
 Upper: 1701
 Lower: 1701
 Op : equal
 Protocol: 17
 Use protocol: true
 SPI: 0x00000000
 Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x45C3306F
 Rule ID: 0x02831838
IPSEC: New inbound decrypt rule, SPI 0x45C3306F
 Src addr: 192.168.0.2
 Src mask: 255.255.255.255

```
Dst addr: 172.16.1.1
Dst mask: 255.255.255.255
Src ports
  Upper: 0
  Lower: 0
  Op   : ignore
Dst ports
  Upper: 0
  Lower: 0
  Op   : ignore
Protocol: 50
Use protocol: true
SPI: 0x45C3306F
Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x45C3306F
  Rule ID: 0x028DAC90
IPSEC: New inbound permit rule, SPI 0x45C3306F
  Src addr: 192.168.0.2
  Src mask: 255.255.255.255
  Dst addr: 172.16.1.1
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op   : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op   : ignore
  Protocol: 50
  Use protocol: true
  SPI: 0x45C3306F
  Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x45C3306F
  Rule ID: 0x02912E50
```

[Solucionar problemas usando o ASDM](#)

Você pode usar o ASDM para ativar o registro e exibir os registros.

1. Escolha **Configuration > Properties > Logging > Logging Setup**, selecione **Enable Logging** e clique em **Apply** para ativar o registro.
2. Escolha **Monitoring > Logging > Log Buffer > On Logging Level**, selecione **Logging Buffer** e clique em **View** para exibir os logs.

[Problema: Desconexões frequentes](#)

Tempo limite de ociosidade/sessão

Se o timeout de ociosidade for definido como 30 minutos (padrão), significa que ele descarta o túnel depois que nenhum tráfego passa por ele por 30 minutos. O cliente VPN é desconectado após 30 minutos, independentemente da configuração do timeout de ociosidade, e encontra a mensagem de erro `PEER_DELETE-IKE_DELETE_UNSPECIFIED`.

Configure idle timeout e session timeout como none para fazer com que o túnel esteja sempre ativo e nunca seja descartado.

Insira o comando `vpn-idle-timeout` no modo de configuração de política de grupo ou no modo de

configuração de nome de usuário para configurar o período de timeout do usuário.

```
hostname(config)#group-policy DfltGrpPolicy attributes  
hostname(config-group-policy)#vpn-idle-timeout none
```

Configure o tempo máximo para as conexões de VPN com o comando `vpn-session-timeout` no modo de configuração de política de grupo ou no modo de configuração de nome de usuário:

```
hostname(config)#group-policy DfltGrpPolicy attributes  
hostname(config-group-policy)#vpn-session-timeout none
```

[Solucionar problemas do Windows Vista](#)

Usuário simultâneo

O Windows Vista L2TP/IPsec introduziu algumas alterações na arquitetura que proibiam mais de um usuário simultâneo de estar conectado a um PIX/ASA headend. Esse comportamento não ocorre no Windows 2K/XP. A Cisco implementou uma solução alternativa para essa alteração a partir da versão 7.2(3) e posterior.

O PC Vista não consegue se conectar

Se o computador com Windows Vista não puder conectar o servidor L2TP, verifique se você configurou SOMENTE `mschap-v2` sob os atributos `ppp` no `DefaultRAGroup`.

[Informações Relacionadas](#)

- [Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto](#)
- [Cisco PIX 500 Series Security Appliances](#)
- [Dispositivos de segurança adaptáveis Cisco ASA 5500 Series](#)
- [Suporte ao produto do software Cisco PIX Firewall](#)
- [Referências do comando Cisco Secure PIX Firewall](#)
- [Página de suporte RADIUS](#)
- [Página de Suporte de Negociação IPsec/Protocolos IKE](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [L2TP \(Layer Two Tunnel Protocol\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)