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

Índice

Introdução

Este documento descreve como configurar o protocolo Layer 2 Tunneling Protocol (L2TP) sobre a Segurança IP (IPsec) de Microsoft Windows remoto 2000/2003 e dos clientes XP a um escritório corporativo da ferramenta de segurança PIX usando chaves pré-compartilhada com o servidor Radius do Internet Authentication Service de Microsoft Windows 2003 (IAS) para a autenticação de usuário. Refira a Lista de Verificação do Microsoft: Configurando IAS para o tratamento por imagens e o VPN alcance para mais informações sobre de IAS.

As vantagens principal de configurar o L2TP com IPsec em uma encenação do Acesso remoto são que os usuários remotos podem alcançar um VPN sobre uma rede IP pública sem um

gateway ou uma linha dedicada. Isto permite o Acesso remoto de virtualmente todo o lugar com POTENCIÔMETROS. Um benefício adicional é que a única exigência do cliente para o acesso VPN é o uso do Windows 2000 com rede de comunicação dial-up de Microsoft (DUN). Nenhum software do cliente adicional, tal como o software Cisco VPN Client, é exigido.

Este documento igualmente descreve como usar o Cisco Adaptive Security Device Manager (ASDM) a fim configurar a ferramenta de segurança da série PIX 500 para o L2TP sobre o IPsec.

Nota: O protocolo de tunelamento de camada 2 (L2TP) em IPSec é apoiado no Software Release 6.x e Mais Recente do firewall PIX segura Cisco.

A fim configurar o L2TP sobre o IPsec entre o PIX 6.x e Windows 2000, refira configurar o L2TP sobre o IPsec entre o PIX Firewall e o Windows 2000 PC usando Certificados.

A fim configurar o L2TP sobre o IPsec do Microsoft Windows 2000 remoto e os clientes XP a uma site corporativo usando um método cifrado, refira configurar o L2TP sobre o IPsec de um Windows 2000 ou do cliente XP a um concentrador da Cisco VPN 3000 Series usando chaves pré-compartilhada.

Pré-requisitos

Requisitos

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

Certifique-se de que a porta 1701 UDP não está obstruída em qualquer lugar ao longo do trajeto da conexão.

Use a política somente do padrão do grupo de túneis e do grupo padrão em Cisco PIX/ASA. As políticas e os grupos definidos pelo utilizador não trabalham.

Nota: A ferramenta de segurança não estabelece um túnel L2TP/IPsec com Windows 2000 se o Cisco VPN Client 3.x ou o Cisco VPN 3000 Client 2.5 são instalados. Desabilite o serviço de Cisco VPN para o Cisco VPN Client 3.x, ou o serviço de ANetIKE para o Cisco VPN 3000 Client 2.5 do painel dos serviços no Windows 2000. A fim fazer isto escolha o **iniciar > programas > ferramentas administrativas > serviços**, reinicie o serviço do agente da política de IPsec do painel dos serviços, e recarregue a máquina.

Componentes Utilizados

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

- Ferramenta de segurança 515E PIX com versão de software 7.2(1) ou mais atrasado
- Security Device Manager 5.2(1) ou mais atrasado adaptável
- Microsoft Windows 2000 Server
- Profissional do Microsoft Windows XP com SP2
- Server de Windows 2003 com IAS

Nota: Se você promove o PIX 6.3 à versão 7.x, certifique-se de que você instalou o SP2 em Windows XP (cliente L2TP).

Nota: A informação no documento é igualmente válida para a ferramenta de segurança ASA.

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

Produtos Relacionados

Esta configuração pode igualmente ser usada com a ferramenta de segurança do 5500 Series de Cisco ASA 7.2(1) ou o mais atrasado.

Convenções

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

Informações de Apoio

Termine estas etapas a fim configurar o L2TP sobre o IPsec.

1. Configurar o modo transporte de IPpsec a fim permitir o IPsec com L2TP.O cliente do Windows 2000 L2TP/IPsec usa o modo transporte de IPpsec — Somente a virulência IP é cifrada, e os cabeçalhos de IP original são deixados intactos. As vantagens deste modo são que adiciona somente alguns bytes a cada pacote e permite que os dispositivos na rede pública ver o origem final e o destino do pacote. Consequentemente, para que os clientes do Windows 2000 L2TP/IPsec conectem à ferramenta de segurança, você deve configurar o modo transporte de IPpsec para uma transformação (veja etapa 2 na configuração ASDM). Com esta capacidade (transporte), você pode permitir o special que processa (por exemplo, QoS) na rede intermediária baseada na informação no cabeçalho IP. Contudo, o encabeçamento da camada 4 é cifrado, que limita o exame do pacote. Infelizmente, a transmissão do cabeçalho IP no texto claro, modo de transporte permite que um atacante execute alguma análise de tráfego.
2. Configurar o L2TP com um grupo do Virtual Private Dial-up Network (VPDN).

A configuração do L2TP com Certificados dos suportes de IPSec que usam as chaves pré-compartilhada ou os métodos de assinatura de RSA, e o uso (ao contrário da estática) de crypto map dinâmicos. A chave pré-compartilhada é usada como uma autenticação para estabelecer o L2TP sobre o túnel de IPsec.

Configurar

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

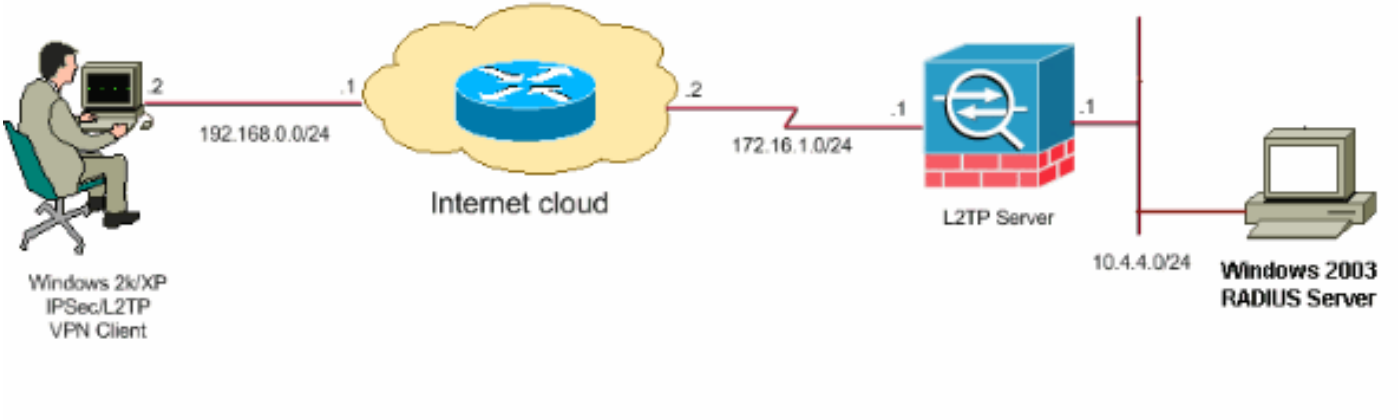
Nota: Use a ferramenta Command Lookup Tool (apenas para clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Nota: 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:

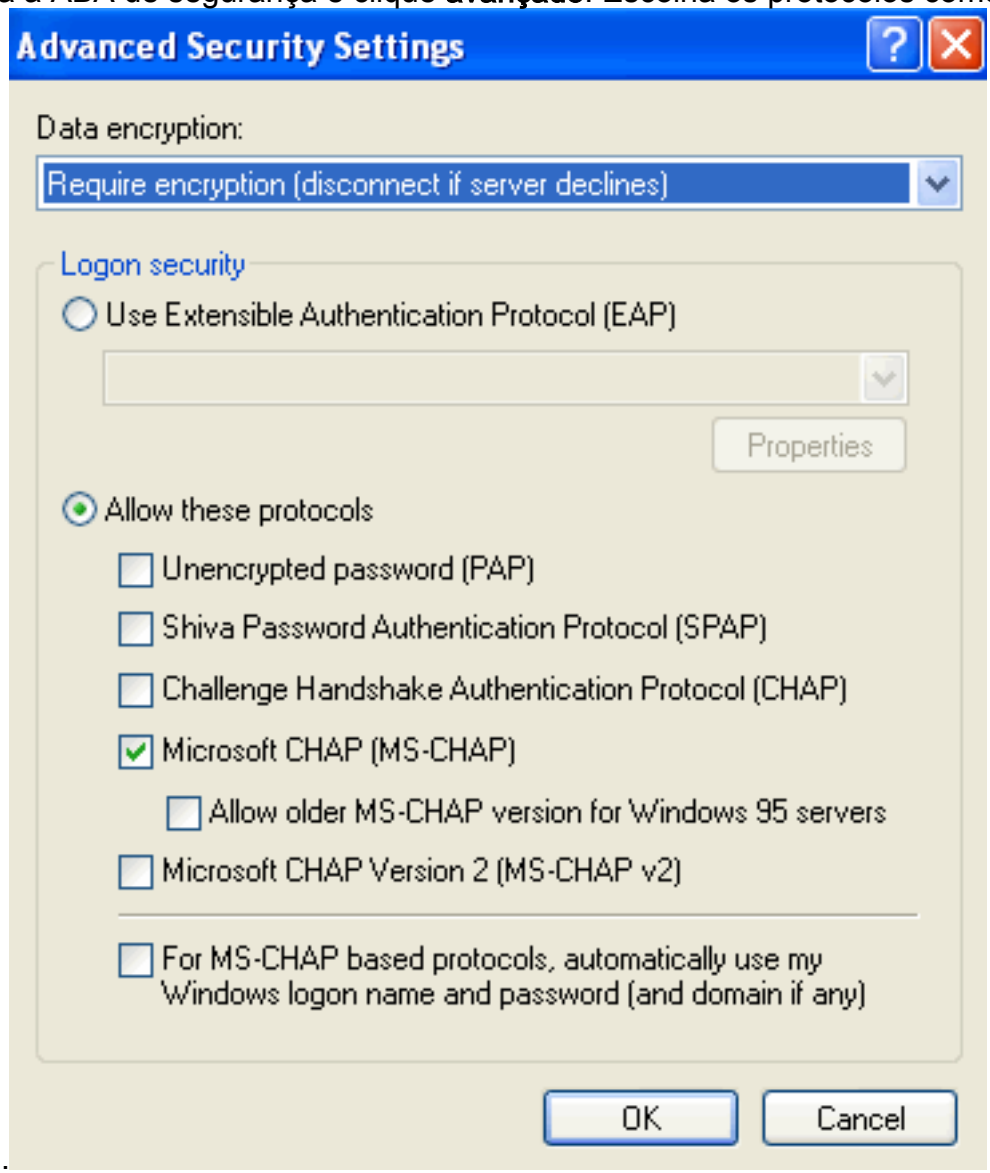
- Configuração de cliente de Windows L2TP/IPsec
- Server L2TP na configuração de PIX
- L2TP usando a configuração ASDM
- Server de Microsoft Windows 2003 com configuração de IAS

Configuração de cliente de Windows L2TP/IPsec

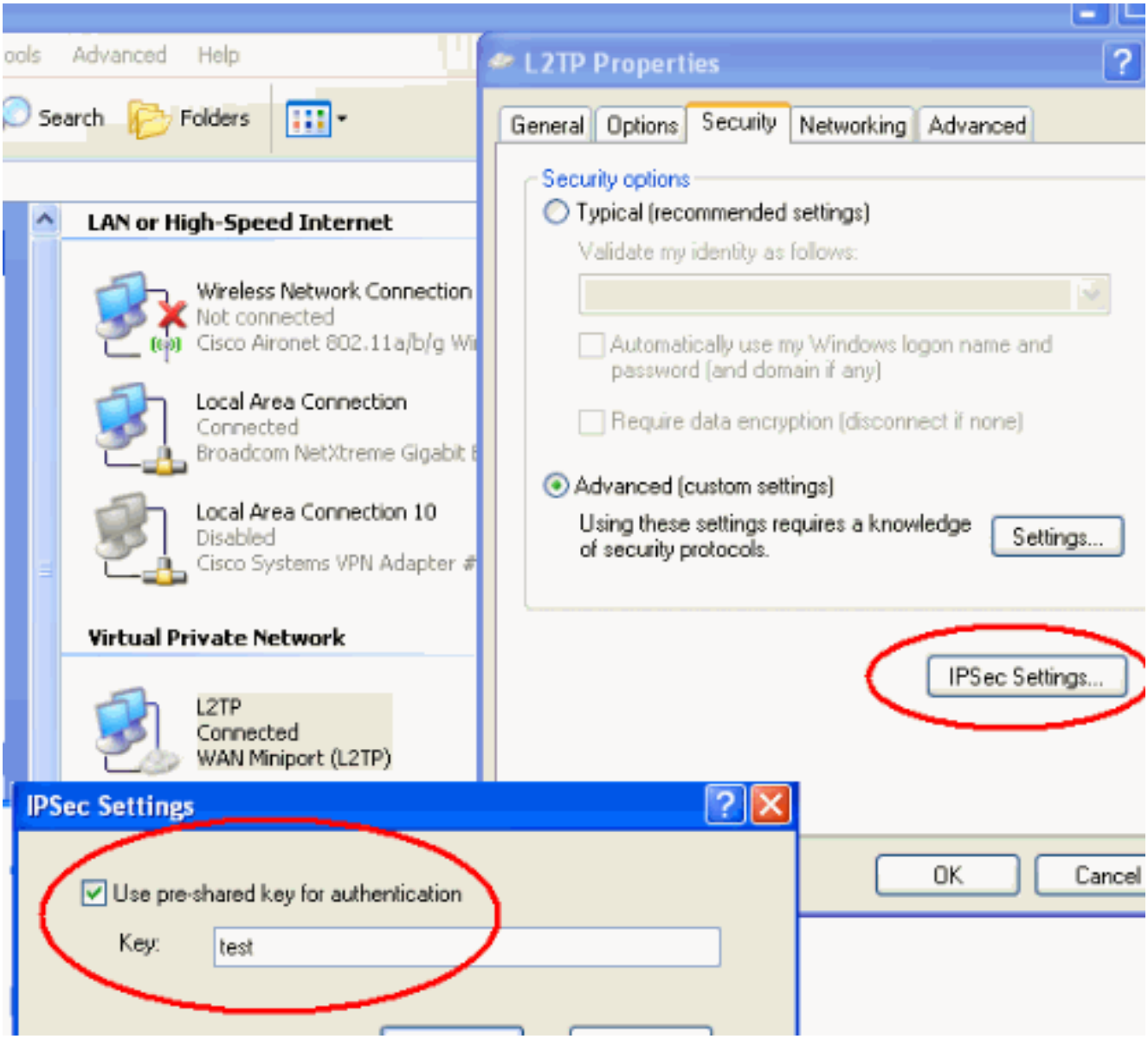
Termine estas etapas a fim configurar o L2TP sobre o IPsec no Windows 2000. Para Windows XP salte etapas 1 e 2 e parta-as de etapa 3:

1. Adicionar este valor de registro a sua máquina do 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`**Nota:** Em alguns casos (Windows XP Sp2), a adição desta chave **(valor: 1)** parece quebrar a conexão como faz a caixa XP negociar somente um pouco o L2TP do que um L2TP com a conexão IPSec. É imperativo adicionar uma política de IPsec conjuntamente com essa chave de registro. Se você recebe um `erro 800` quando você tenta estabelecer uma conexão, remova a chave (valor: 1) a fim conseguir a conexão trabalhar.**Nota:** Você deve reiniciar Windows 2000/2003 ou a máquina XP para que as mudanças tomem o efeito. À revelia o cliente do Windows tenta usar o IPsec com um Certificate Authority (CA). A configuração desta chave de registro impede que esta ocorra. Agora você pode configurar uma política de IPsec na estação de Windows para combinar os parâmetros que você quer no PIX/ASA. Refira como configurar uma conexão do L2TP/IPSec usando a autenticação da chave pré-compartilhada (Q240262) para uma configuração passo a passo da política de IPsec de Windows.Consulte para configurar uma chave Preshared para o uso com conexões do protocolo Layer 2 Tunneling Protocol em Windows XP (Q281555)\ para mais informação.

3. Crie sua conexão.
4. Sob a rede e as conexões dial-up, clicar com o botão direito na conexão e escolha **propriedades**.Vá à ABA de segurança e clique **avançado**. Escolha os protocolos como esta imagem mostra.



5. **Nota:** Esta etapa é aplicável somente para Windows XP.Clique **ajustes do IPsec**, verifique a **chave pré-compartilhada do uso para ver se há a autenticação** e datilografe dentro a chave pré-compartilhada a fim ajustar a chave pré-compartilhada.Neste exemplo, o teste é usado como a chave pré-
compartilhada.



Server L2TP na configuração de 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**

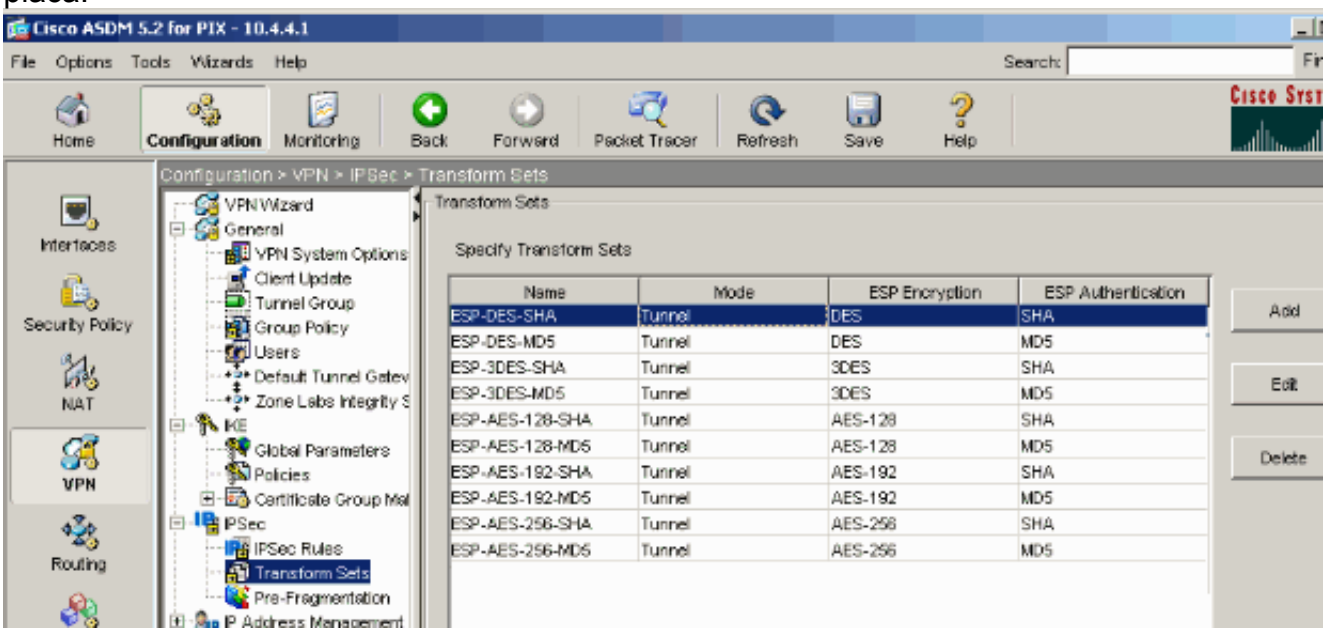
```
(inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0
172.16.1.2 1 timeout xlate 3:00:00 timeout conn 1:00:00
half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00
sip-invite 0:03:00 sip-disconnect 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>
password <password> mschap. username test password
DLaUiAX3l78qgoB5c7iVNw== 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:e1e0730fa260244caa2e2784f632accd : end
```

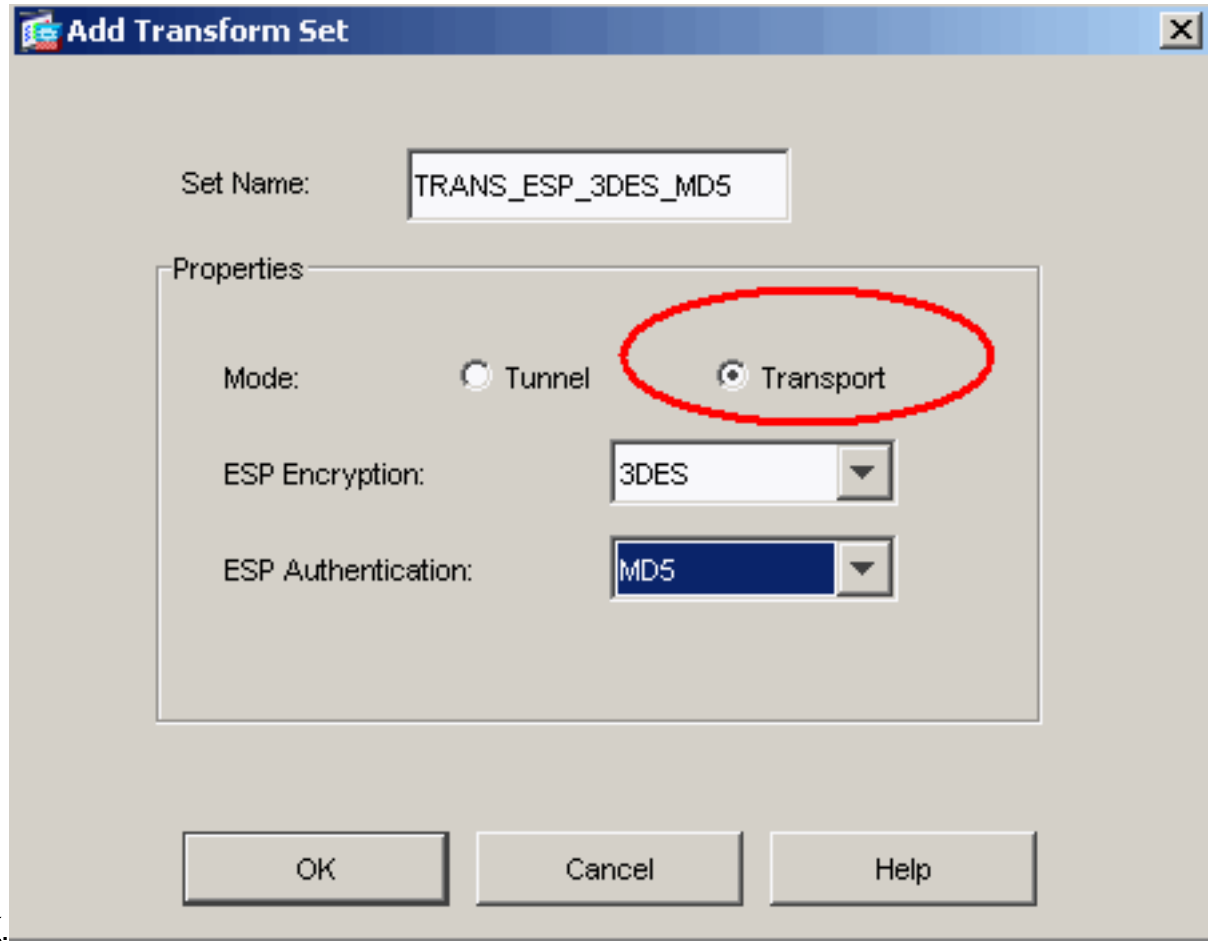
L2TP usando a configuração ASDM

Termine estas etapas a fim configurar a ferramenta de segurança para aceitar o L2TP sobre conexões IPSec:

1. Adicionar um IPsec transformam o grupo e especificam o IPsec para usar o modo de transporte um pouco do que o modo de túnel. A fim fazer isto, para escolher a **configuração > o VPN > o IPsec > transforma grupos** e o clique **adiciona**. A transformação ajusta indicadores da
placa.

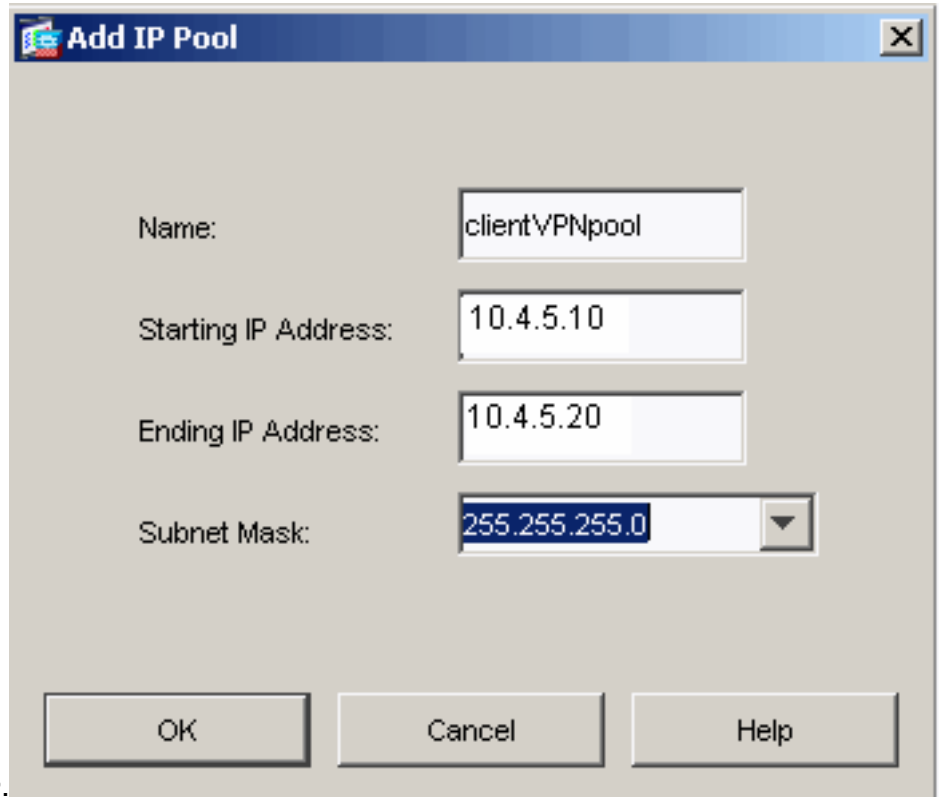


2. Termine estas etapas a fim adicionar uma transformação ajustada:Dê entrada com um nome para o grupo da transformação.Escolha os métodos da criptografia e de autenticação ESP ESP.Escolha o modo como o **transporte**.Clique em



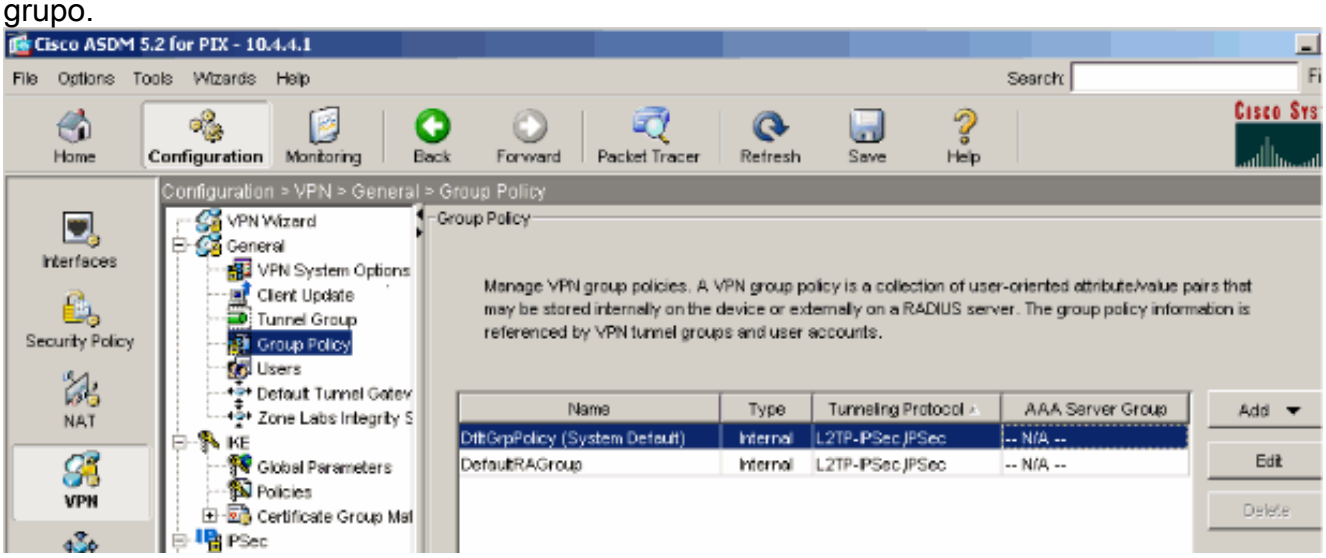
OK.

3. Termine estas etapas a fim configurar um método da atribuição de endereço. Este exemplo usa associações do endereço IP de Um ou Mais Servidores Cisco ICM NT.Escolha a **configuração > o VPN > o gerenciamento de endereços IP > as associações IP**.Clique em Add. A caixa de diálogo do IP pool adicionar aparece.Dê entrada com o nome do pool novo do endereço IP de Um ou Mais Servidores Cisco ICM NT.Incorpore os endereços IP de Um ou Mais Servidores Cisco ICM NT começando e de término.Incorpore a máscara de sub-rede e clique a

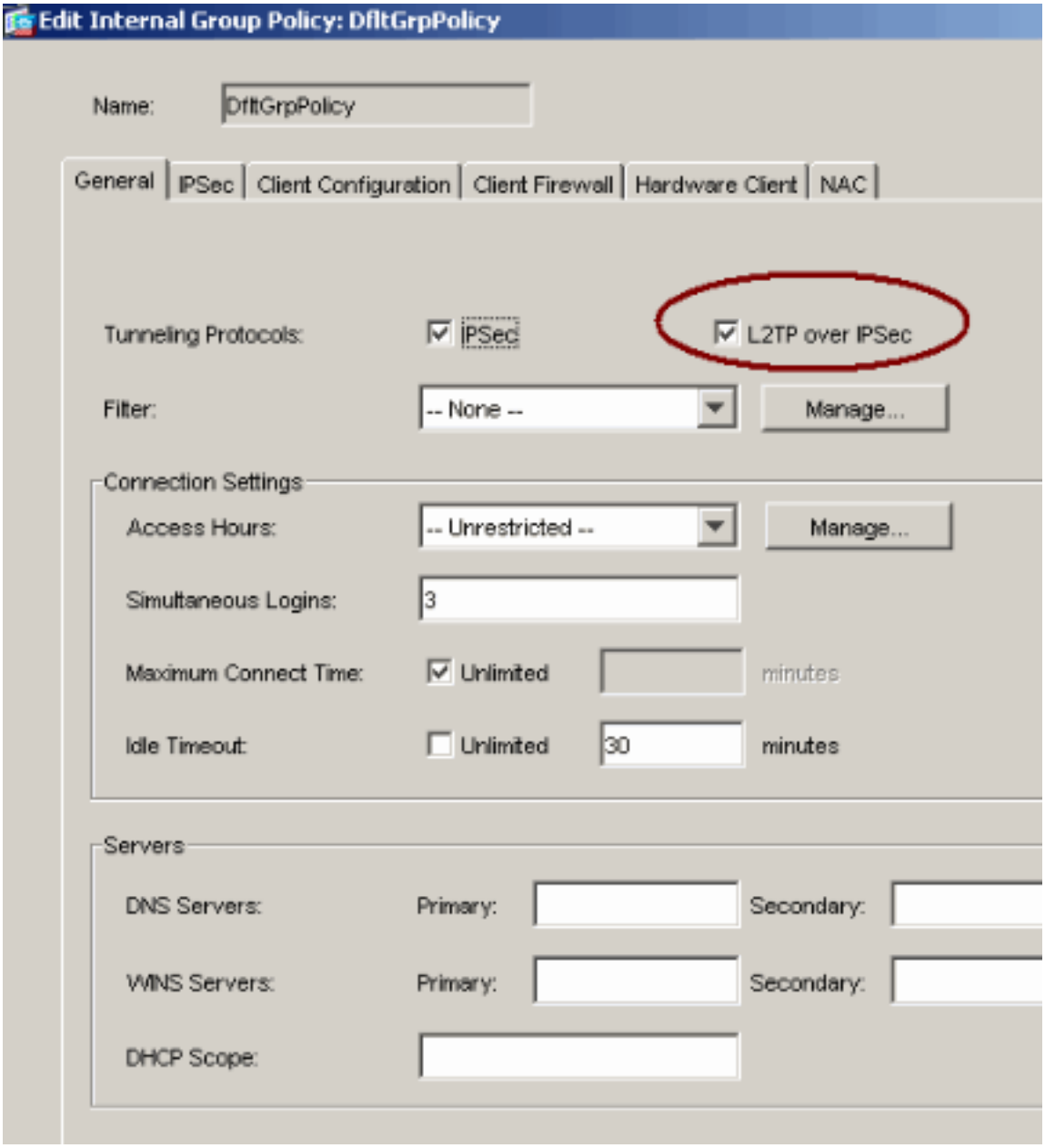


APROVAÇÃO.

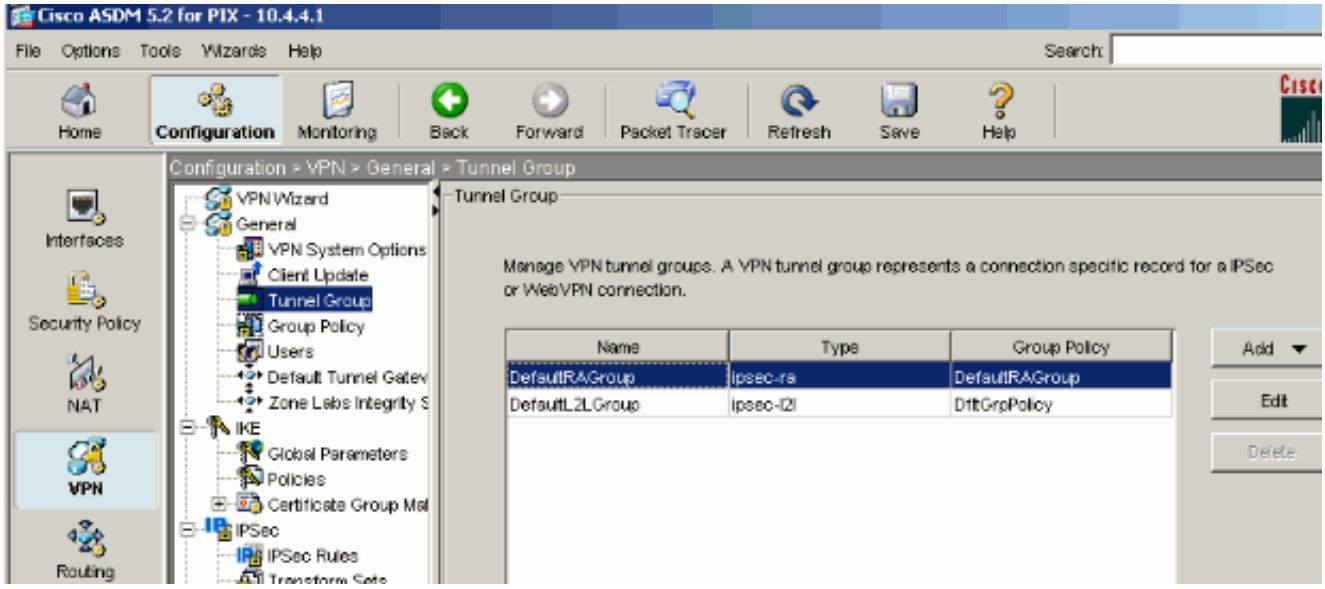
4. Escolha a **configuração > o VPN > a política do general > do grupo** a fim configurar o L2TP sobre o IPsec como um protocolo de tunelamento válido VPN para a política do grupo. Os indicadores da placa da política do grupo.



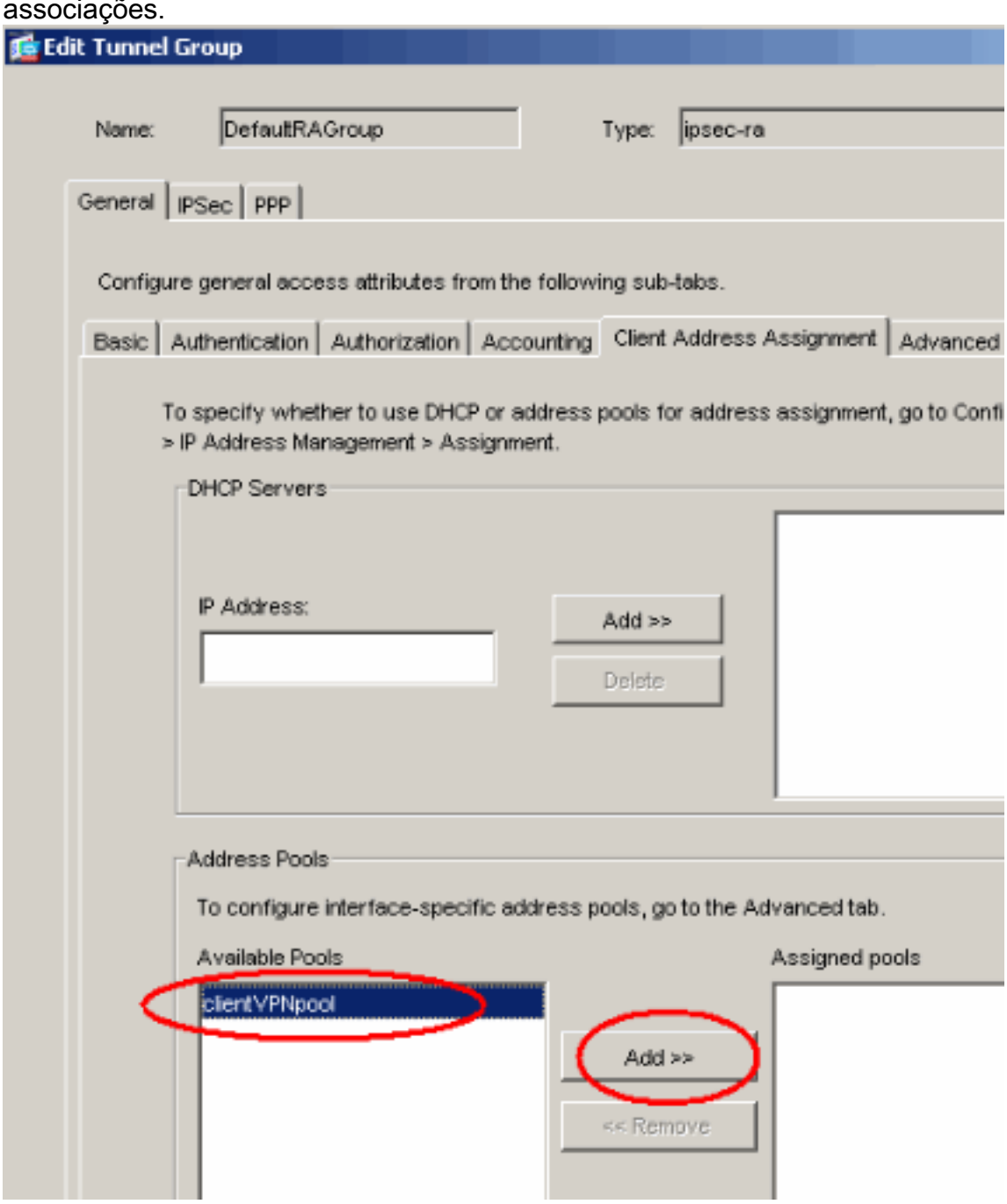
5. Selecione uma política do grupo (DiffGrpPolicy) e o clique **edita**.Os indicadores do diálogo da política do grupo da edição. Verifique o **L2TP sobre o IPsec** a fim permitir o protocolo para a política do grupo e clicar então a **APROVAÇÃO**.



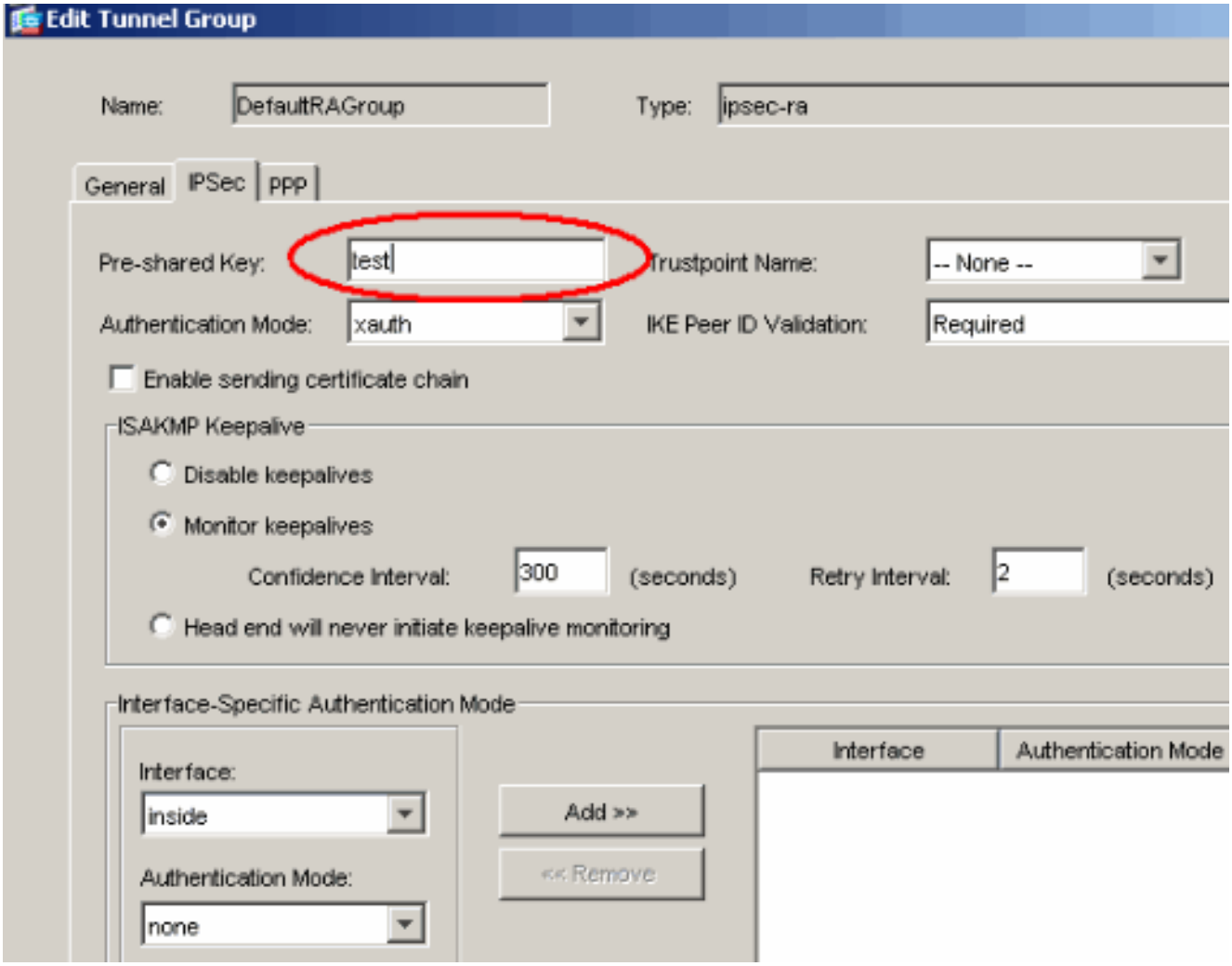
6. Termine estas etapas a fim atribuir o pool do endereço IP de Um ou Mais Servidores Cisco ICM NT a um grupo de túneis:Escolha a **configuração > o VPN > o general > o grupo de túneis**.Depois que a placa do grupo de túneis aparece, selecione um grupo de túneis (DefaultRAGroup) na tabela.O clique **edita**.



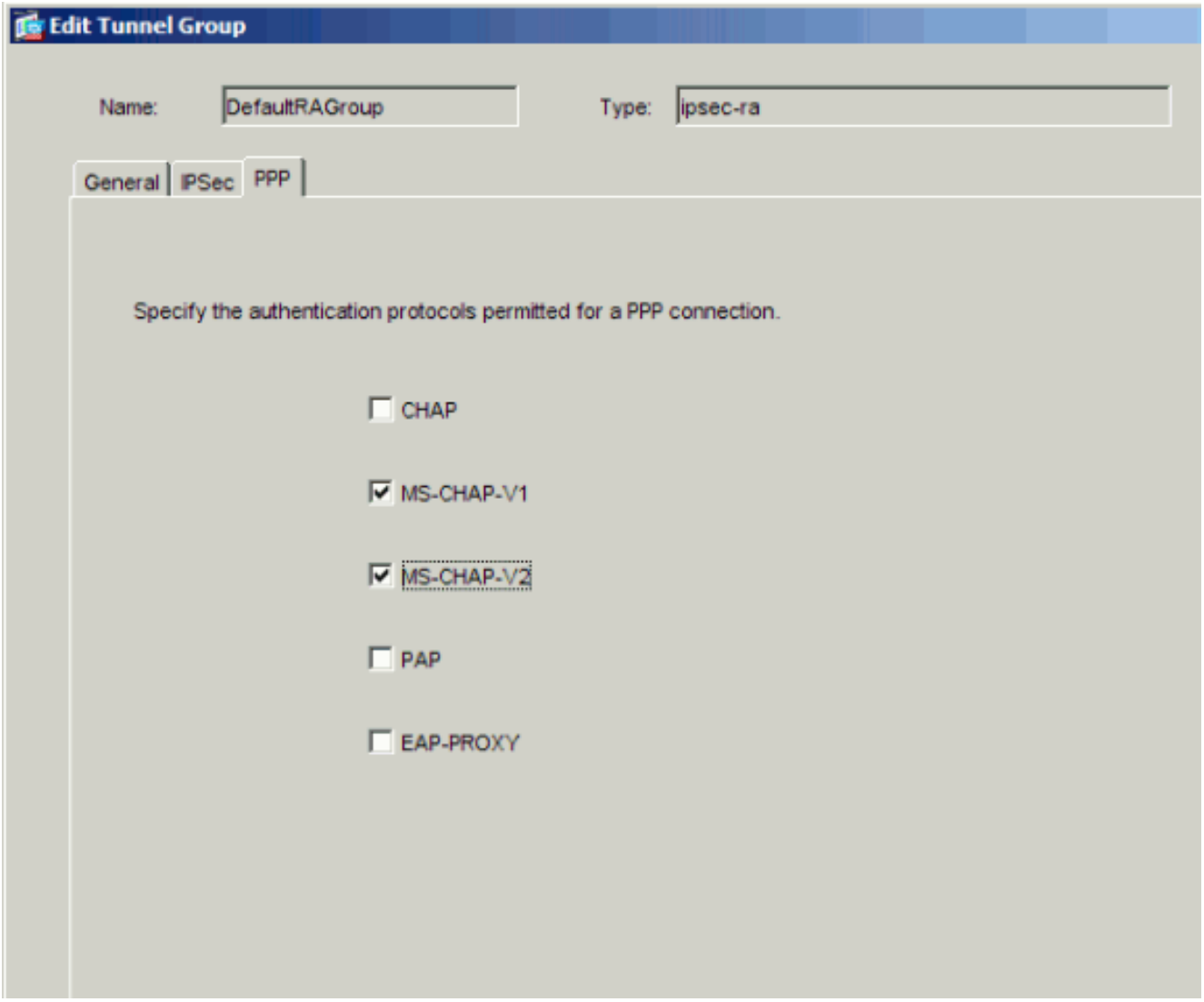
7. Termine estas etapas quando o indicador de grupo de túneis da edição aparece:Do tab geral, vá à aba da atribuição de endereço de cliente.Na área de conjuntos de endereços, escolha um conjunto de endereços atribuir ao grupo de túneis.Clique em Add. O conjunto de endereços aparece na caixa atribuída das associações.



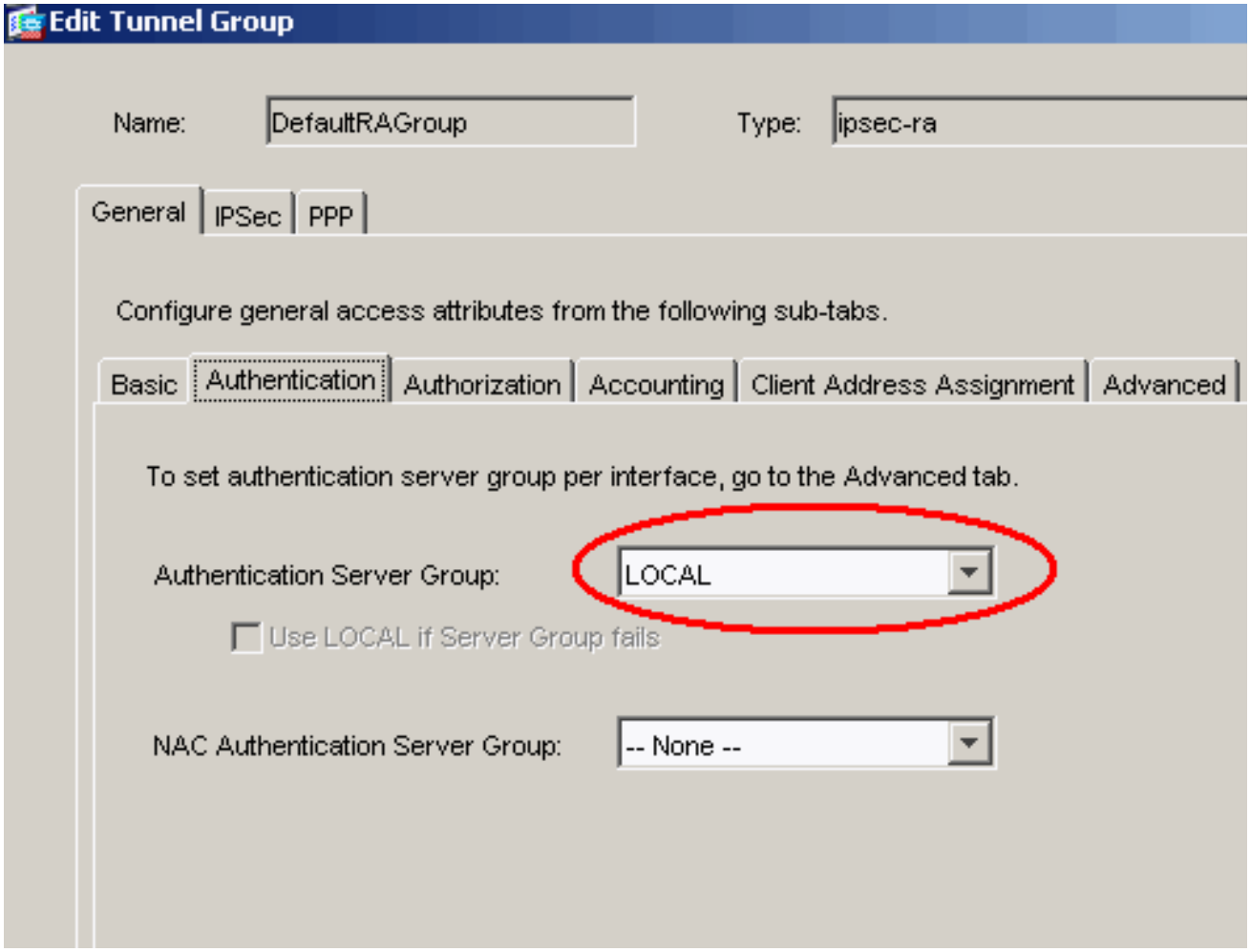
8. A fim ajustar a chave pré-compartilhada, vá à aba do IPsec, incorpore sua **chave pré-compartilhada**, e clique a **APROVAÇÃO**.



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



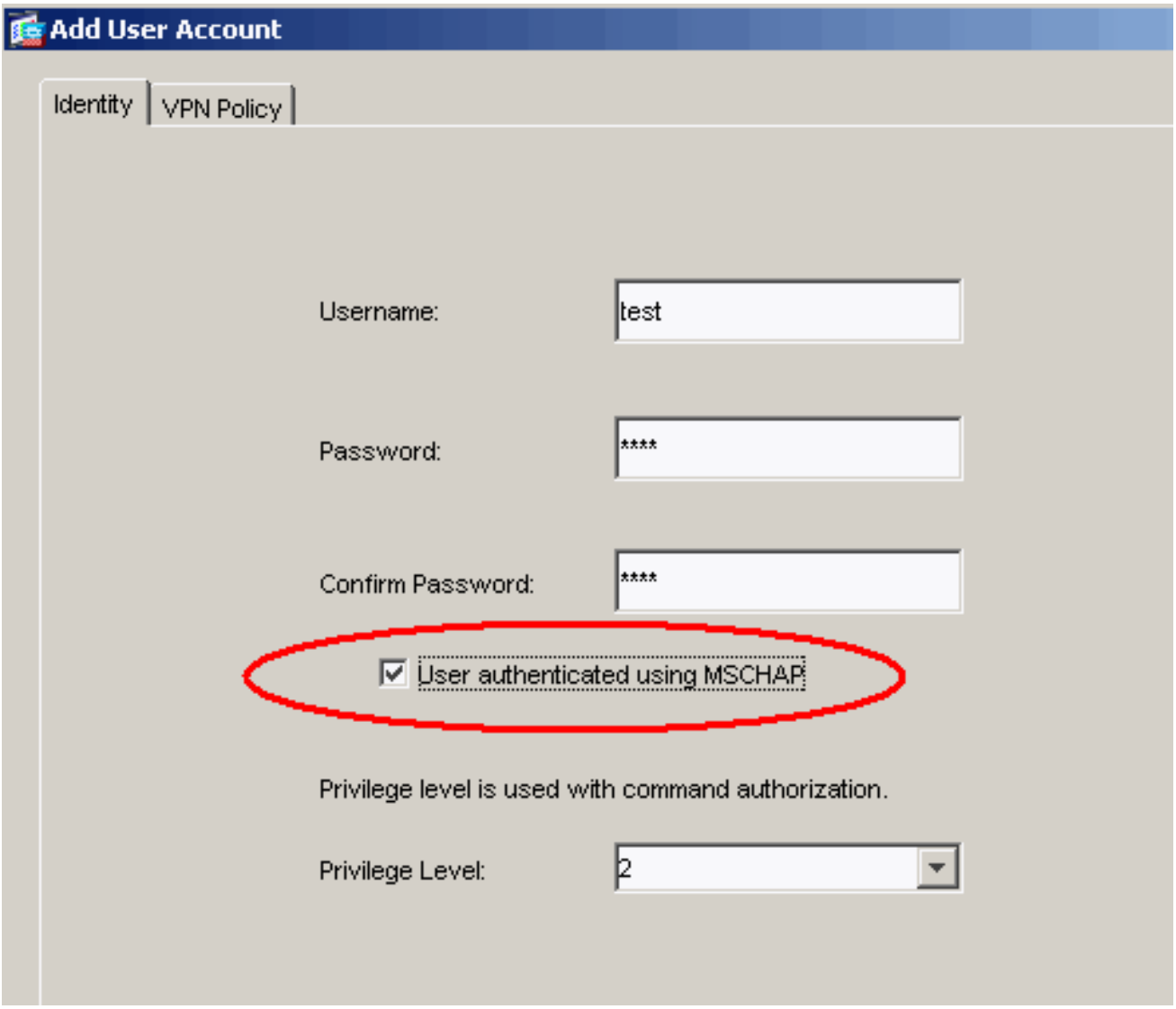
10. Especifique um método para autenticar os usuários que tentam o L2TP sobre conexões IPSec.Você pode configurar a ferramenta de segurança para usar um Authentication Server ou seu próprio base de dados local. A fim fazer isto, vá à aba da autenticação do grupo de túneis. À revelia, a ferramenta de segurança usa seu base de dados local. Os indicadores da lista de drop-down do grupo de Authentication Server LOCAIS. A fim usar um Authentication Server, selecione um da lista.**Nota:** A ferramenta de segurança apoia somente as versões 1 e 2 das autenticações de PPP PAP e do Microsoft CHAP no base de dados local. O EAP e a RACHADURA são executados por server da autenticação de proxy. Consequentemente, se um usuário remoto pertence a um grupo de túneis configurado com EAP ou RACHADURA, e a ferramenta de segurança é configurado para usar o base de dados local, que o usuário não pode
conectar.



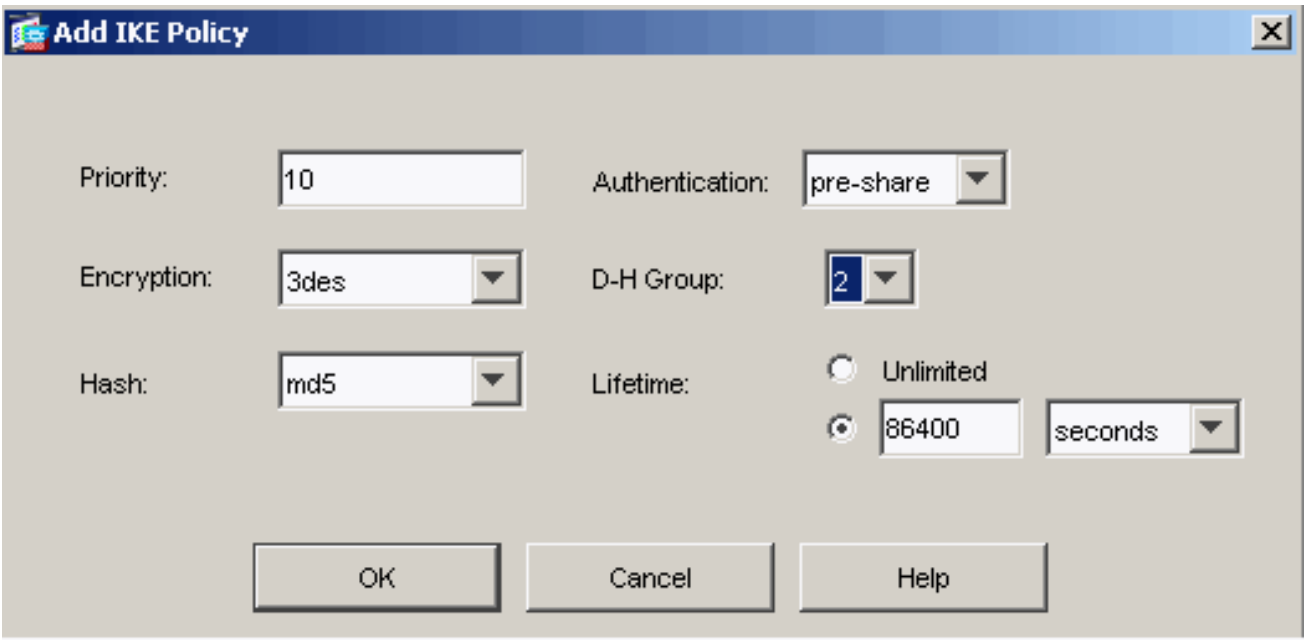
Nota: Escolha a **configuração > o VPN > o general > o grupo de túneis** a fim ir para trás à configuração do grupo de túneis de modo que você possa ligar a política do grupo ao grupo de túneis e permitir o interruptor do grupo de túneis (opcional). Quando a placa do grupo de túneis aparece, escolha o grupo de túneis e o clique **edita**.**Nota:** O interruptor do grupo de túneis permite a ferramenta de segurança de associar os usuários diferentes que estabelecem o L2TP sobre conexões IPSec com grupos de túneis diferentes. Desde que cada grupo de túneis tem suas próprias associações do Grupo de servidores AAA e do endereço IP de Um ou Mais Servidores Cisco ICM NT, os usuários podem ser autenticados com os métodos específicos a seu grupo de túneis. Com esta característica, em vez de enviar apenas um username, o usuário envia um username e um nome do grupo no formato username@group_name, onde “@” representa um delimitador que você possa configurar, e o nome do grupo é o nome de um grupo de túneis que seja configurado na ferramenta de segurança.**Nota:** O interruptor do grupo de túneis é permitido pelo grupo da tira que processa, que permite a ferramenta de segurança de selecionar o grupo de túneis para conexões do usuário obtendo o nome do grupo do username apresentado pelo cliente VPN. A ferramenta de segurança envia então somente ao usuário parte do username para a autorização e a autenticação. Se não (se deficiente), a ferramenta de segurança envia o username inteiro, incluindo o reino. A fim permitir o interruptor do grupo de túneis, verificar a **tira o reino do username antes de passá-lo sobre ao servidor AAA**, e verificar a **tira o grupo do username antes de passá-lo sobre ao servidor AAA**. Em seguida, clique em “OK”.

11. Termine estas etapas a fim criar um usuário no base de dados local:Escolha **>Properties da configuração > administração > contas de usuário do dispositivo**.Clique em Add.Se o usuário é um cliente L2TP que use a versão 1 ou 2 do Microsoft CHAP, e a ferramenta de segurança é configurado para autenticar contra o base de dados local, você deve verificar

o **usuário autenticado usando o MSCHAP** a fim permitir o MSCHAP.Clique em **OK**.



12. Escolha a **configuração > o VPN > o IKE > as políticas** e o clique **adiciona** a fim criar uma política de IKE para a fase I. Clique **APROVAÇÃO** para continuar.



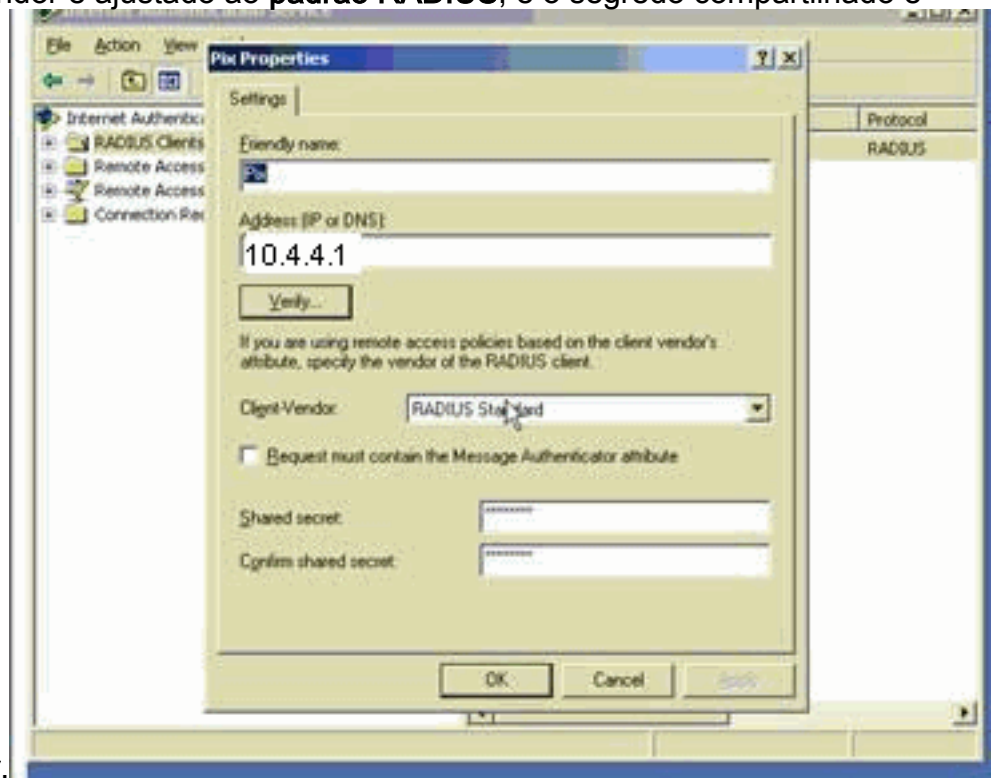
13. (Opcional) se você espera clientes múltiplos L2TP atrás de um dispositivo NAT tentar o

L2TP sobre conexões IPSec à ferramenta de segurança, você deve permitir o traversal NAT de modo que os pacotes ESP possam passar através de uns ou vários dispositivos NAT. Termine estas etapas a fim fazer isto:Escolha a **configuração > o VPN > o IKE > os parâmetros globais**.Assegure-se de que o **ISAKMP** esteja permitido em uma relação.A verificação **permite o IPsec sobre o NAT-T**.Clique em **OK**.

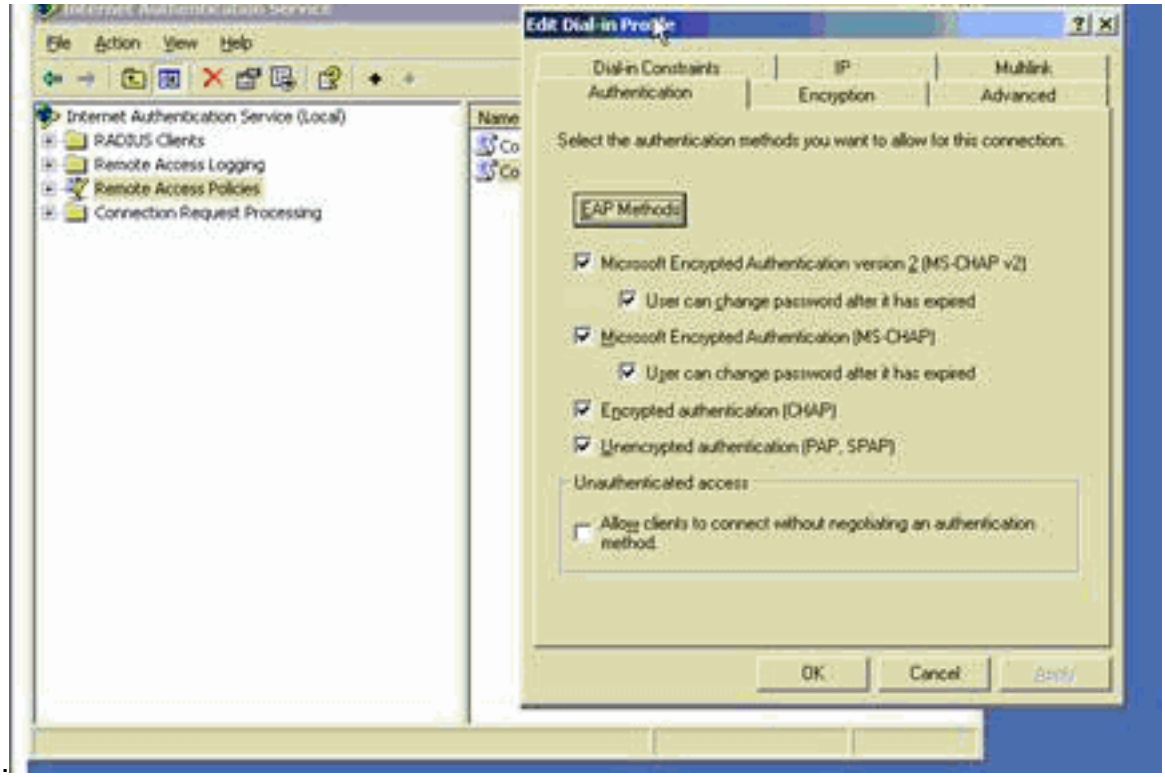
Server de Microsoft Windows 2003 com configuração de IAS

Termine estas etapas a fim configurar o server de Microsoft Windows 2003 com IAS.

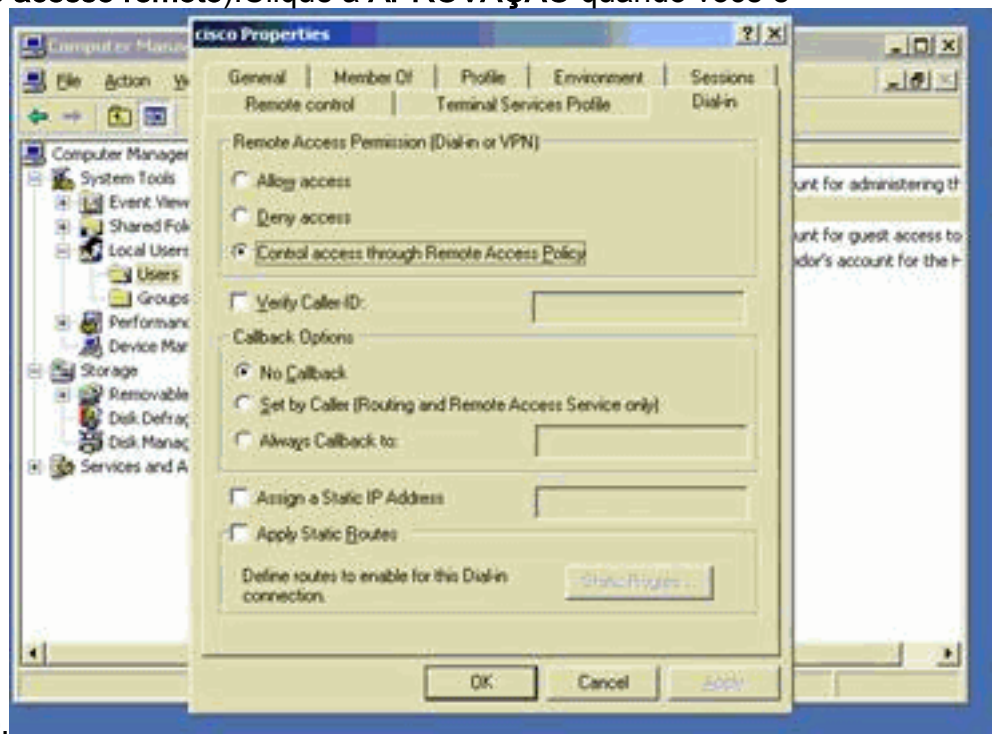
Nota: Estas etapas supõem que IAS está instalado já na máquina local. Se não, adicionar isto com o **> Add do Control Panel/remova os programas**.

1. Escolha o **Ferramentas Administrativas > Serviço de Autenticação de Internet** e clicar com o botão direito no **cliente RADIUS** a fim adicionar um cliente RADIUS novo. Depois que você datilografa a informação cliente, clique a **APROVAÇÃO**.Este exemplo mostra um cliente nomeado “Pix” com um endereço IP de Um ou Mais Servidores Cisco ICM NT de 10.4.4.1. Client-Vendor é ajustado ao **padrão RADIUS**, e o segredo compartilhado é **radiuskey**. 

2. Escolha **políticas de acesso remoto**, clicar com o botão direito em **conexões a outros servidores de acesso**, e selecione **propriedades**.
3. Assegure-se de que a opção para **permissões de acesso remoto de Grant** esteja selecionada.
4. O clique **edita o perfil** e verifica estes ajustes:Na aba da autenticação, verifique a **autenticação não criptografada (PAP, SPAP)**.Na aba da criptografia, assegure-se de que a opção para o **no encryption** esteja selecionada.Clique a **APROVAÇÃO** quando você é

terminado. 

5. Escolha o **Ferramentas Administrativas > Gerenciamento de Computador > Ferramentas de Sistema > Usuários e Grupos Locais**, clicar com o botão direito em **usuários** e em **novos usuários** seletos a fim adicionar um usuário na conta do computador local.
6. Adicionar um usuário com senha Cisco **password1** e verifique esta informação do perfil:No tab geral, assegure-se de que a opção de senha **Expired** esteja selecionada **nunca** em vez da opção para o usuário deva mudar a senha.No guia de discagem de entrada, selecione a opção para o **acesso Allow** (ou deixe a configuração padrão do **acesso do controle com a política de acesso remoto**).Clique a **APROVAÇÃO** quando você é

terminado. 

Autenticação extendida para o L2TP sobre o IPsec usando o diretório ativo

Use esta configuração no ASA a fim permitir que a autenticação para que a conexão L2tp ocorra do diretório ativo:

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

Também, no cliente L2tp, vá aos **ajustes da segurança avançada (costume)** e escolha somente a opção para a **senha não criptografada (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.

- **mostre IPsec cripto sa** — Mostra todas as associações de segurança atuais IKE (SA) em um par.`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`
- **mostre isakmp cripto sa** — Mostra todo o IKE atual SA em um par.`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`
- **mostra VPN-sessiondb** — Inclui os filtros de protocolo que você pode usar a fim ver a informação detalhada sobre o L2TP sobre conexões IPSec. O comando cheio do modo de configuração global é o **protocolo remoto detalhado VPN-sessoindb l2tpOverIpsec do filtro da mostra**.Este exemplo mostra os detalhes de um único L2TP sobre a conexão 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 Idle TO Left : 30 Minutes Bytes Tx : 378 Bytes Rx : 13431 Pkts Tx : 16 Pkts Rx : 146`

Troubleshooting

Esta seção fornece a informação para pesquisar defeitos sua configuração. O exemplo de debug é mostrado igualmente.

Comandos para Troubleshooting

Determinados comandos são apoiados pela ferramenta Output Interpreter (clientes registrados somente), que permite que você ver uma análise do emissor de comando de execução.

Nota: Refira a informação importante em comandos Debug e em Troubleshooting de Segurança IP - compreendendo e usando comandos debug antes que você use **comandos debug**.

- **IPsec 7 do debug crypto** — Indica as negociações de IPSEC de fase 2.
- **isakmp 7 do debug crypto** — Indica as negociações de ISAKMP de fase 1.

Exemplo de debug

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 V endor 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 Def aultRAGroup Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP
= 192.168.0.2, Generat ing 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, process ing ID payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP =
192.168.0.2, process ing hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP
= 192.168.0.2, Computi ng hash for ISAKMP Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, Connection
landed on tunnel_group Def aultRAGroup Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP =
192.168.0.2, Freeing previ ously allocated memory for authorization-dn-attributes Jan 02
18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting ID payload Jan
02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting hash payload
Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Computi ng hash for
```

ISAKMP Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting 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 succesfully.* Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, **PHASE 1 COMPL 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 do es not support keep-alives (type = None) Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Startin g P1 rekey timer: 21600 seconds. Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1 b84b0) 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, process ing hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing ID payload Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received remo te 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, process ing ID payload Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Received loca l 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 se ssion 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 Pe er configured for crypto map: outside_dyn_map Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing IPSec SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, IPSec S A 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: requesti ng 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 constucting quick mode** Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting blank hash payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting IPSec SA payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting IPSec nonce payload Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, constru cting proxy ID Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Transmi tting 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, constru cting qm hash payload Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE SENDING Message (msgid=e1b 84b0) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + N ONE (0) total length : 144 Jan 02 18:26:44 [IKEv1]: IP = 192.168.0.2, IKE_DECODE RECEIVED Message (msgid=e1 b84b0) with payloads : HDR + HASH (8) + NONE (0) total length : 48 Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, process ing 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, Generat ing Quick Mode Key! Jan 02 18:26:44 [IKEv1 DEBUG]: Group = DefaultRAGroup, IP = 192.168.0.2, Generat ing Quick Mode Key! Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, Security nego tiation 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, Startin g P2 rekey timer: 3059 seconds. *!--- Phase 2 completes succesfully.* Jan 02 18:26:44 [IKEv1]: Group = DefaultRAGroup, IP = 192.168.0.2, PHASE 2 COMPL ETED (msgid=0e1b84b0) Jan 02 18:26:44 [IKEv1]: IKEQM_Active() Add L2TP classification rules: ip <192.1 68.0.2> 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 : 0x01BFCF80 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
```

Pesquise defeitos usando o ASDM

Você pode usar o ASDM a fim permitir o registro e ver os logs.

1. Escolha a **configuração > as propriedades > instalação de registro > de registro**, seleta **permita o registro** e o clique **aplica-se** a fim permitir o registro.
2. Escolha a **monitoração > registrando > buffer de registro > no nível de registro**, no **logging buffer** seleto, e na **opinião do** clique a fim ver os logs.

Problema: Frequente disconexões

Quietude/timeout de sessão

Se o idle timeout está ajustado a 30 minutos (padrão), significa que deixa cair o túnel depois que o sem tráfego passa através dele por 30 minutos. O cliente VPN obtém desligado após 30 minutos apesar do ajuste do idle timeout e encontra o 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
```

Pesquise defeitos Windows Vista

Usuário simultâneo

Windows Vista L2TP/IPsec introduziu algumas mudanças arquitetural que proibiram mais de um usuário simultâneo da conexão a uma extremidade principal PIX/ASA. Este comportamento não ocorre em Windows 2K/XP. Cisco executou uma ação alternativa para esta mudança até à data da liberação 7.2(3) e maior.

Vista PC não capaz de conectar

Se o computador de Windows Vista não pode conectar o server L2TP, a seguir verifique que você configurou SOMENTE mschap-v2 sob os PPP-atributos no DefaultRAGroup.

Informações Relacionadas

- Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto
- Cisco PIX 500 Series Security Appliances
- Cisco ASA 5500 Series Adaptive Security Appliances
- Sustentação do produto do Software do firewall Cisco PIX
- Referências do comando Cisco Secure PIX Firewall
- Página de suporte RADIUS
- Página de Suporte de Negociação IPSec/Protocolos IKE
- Solicitações de Comentários (RFCs)
- Layer Two Tunnel Protocol (L2TP)
- Suporte Técnico e Documentação - Cisco Systems