>在Windows 2000 /XP PC和PIX/ASA 7.2之间的IPSec上的L2TP使用预共享密钥的配置示例

目录

简介

本文档介绍如何将预共享密钥和 Microsoft Windows 2003 Internet 身份验证服务 (IAS) RADIUS 服务器结合使用以进行用户身份验证，从而配置从远程 Microsoft Windows 2000/2003 和 XP 客户端到 PIX 安全设备企业机构的第二层隧道协议 (L2TP) over IP Security (IPsec)。请参阅 Microsoft - 清单：配置 IAS 进行拨号和 VPN 访问，以了解有关 IAS 的更多信息。

在远程访问方案中使用 IPsec 配置 L2TP 的主要优点是，远程用户可以通过公用 IP 网络访问 VPN，而无需网关或专用线路。这样，实际上便可以从具有 POTS 的任何地方进行远程访问。其他优点是，VPN 访问的唯一客户端要求是组合使用 Windows 2000 与 Microsoft 拨号网络 (DUN)。不需要任何附加客户端软件（如 Cisco VPN Client 软件）。

本文档还介绍了如何使用 Cisco 自适应安全设备管理器 (ASDM) 对 PIX 500 系列安全设备配置

L2TP over IPsec。

注意： Cisco Secure PIX 防火墙软件版本 6.x 及更高版本支持第二层隧道协议 (L2TP) over IPsec。

要在 PIX 6.x 和 Windows 2000 之间配置 L2TP Over IPsec，请参阅使用证书在 PIX 防火墙与 Windows 2000 PC 之间配置 L2TP Over IPsec。

要使用加密方法配置从远程 Microsoft Windows 2000 和 XP 客户端到企业站点的 L2TP over IPsec，请参阅使用预共享密钥配置从 Windows 2000 或 XP 客户端到 Cisco VPN 3000 系列集中器的 L2TP over IPsec。

先决条件

要求

在建立安全隧道之前，对等体之间需要存在 IP 连接。

确保 UDP 端口 1701 在沿连接路径的任何地方都不受阻止。

请在 Cisco PIX/ASA 上仅使用默认隧道组和默认组策略。用户定义的策略和组不工作。

注意： 如果已安装 Cisco VPN Client 3.x 或 Cisco VPN 3000 Client 2.5，则安全设备与 Windows 2000 之间不会建立 L2TP/IPsec 隧道。从 Windows 2000 中的“服务”面板中，禁用 Cisco VPN Client 3.x 的 Cisco VPN 服务，或 Cisco VPN 3000 Client 2.5 的 ANetIKE 服务。为此，请选择**开始 > 程序 > 管理工具 > 服务**，从“服务”面板中，重新启动 IPsec Policy Agent 服务，然后重新启动计算机。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 软件版本为 7.2(1) 或更高版本的 PIX 安全设备 515E
- 自适应安全设备管理器 5.2(1) 或更高版本
- Microsoft Windows 2000 Server
- Microsoft Windows XP Professional SP2
- 具有 IAS 的 Windows 2003 Server

注意： 如果将 PIX 6.3 升级到版本 7.x，请确保已在 Windows XP（L2TP 客户端）中安装了 SP2。

注意： 本文档中的信息对 ASA 安全设备同样有效。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置也可与 Cisco ASA 5500 系列安全设备 7.2(1) 一起使用。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

完成以下步骤以配置 L2TP over IPsec。

1. 配置 IPsec 传输模式以便启用具有 L2TP 的 IPsec。Windows 2000 L2TP/IPsec 客户端使用 IPsec 传输模式 - 仅加密 IP 有效负载，并保留原始 IP 报头的完整性。此模式的优点是它仅向每个数据包添加少量的字节，并允许公用网络上的设备查看数据包的最终源和目标。因此，要使 Windows 2000 L2TP/IPsec 客户端连接到安全设备，必须配置转换的 IPsec 传输模式（请参阅 ASDM 配置中的步骤 2）。通过此功能（传输），您可以基于 IP 报头中的信息对媒介网络执行特殊处理（例如，QoS）。然而，第 4 层报头已被加密，用于限制对数据包的检查。遗憾的是，IP 报头是以明文传输的，传输模式允许攻击者执行一些流量分析。
2. 使用虚拟专用拨号网络 (VPDN) 组配置 L2TP。

配置具有 IPsec 的 L2TP 支持使用预共享密钥或 RSA 签名方法的证书，且支持使用动态（与静态相对）加密映射。使用预共享密钥作为身份验证来建立 L2TP over IPsec 隧道。

配置

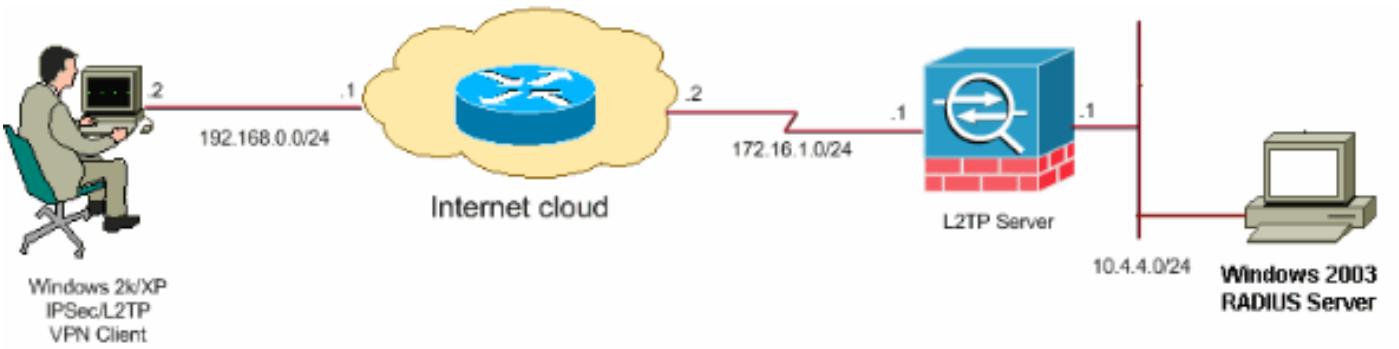
本部分提供有关如何配置本文档所述功能的信息。

注意： 有关本文档所用命令的详细信息，请使用命令查找工具（仅限注册用户）。

注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

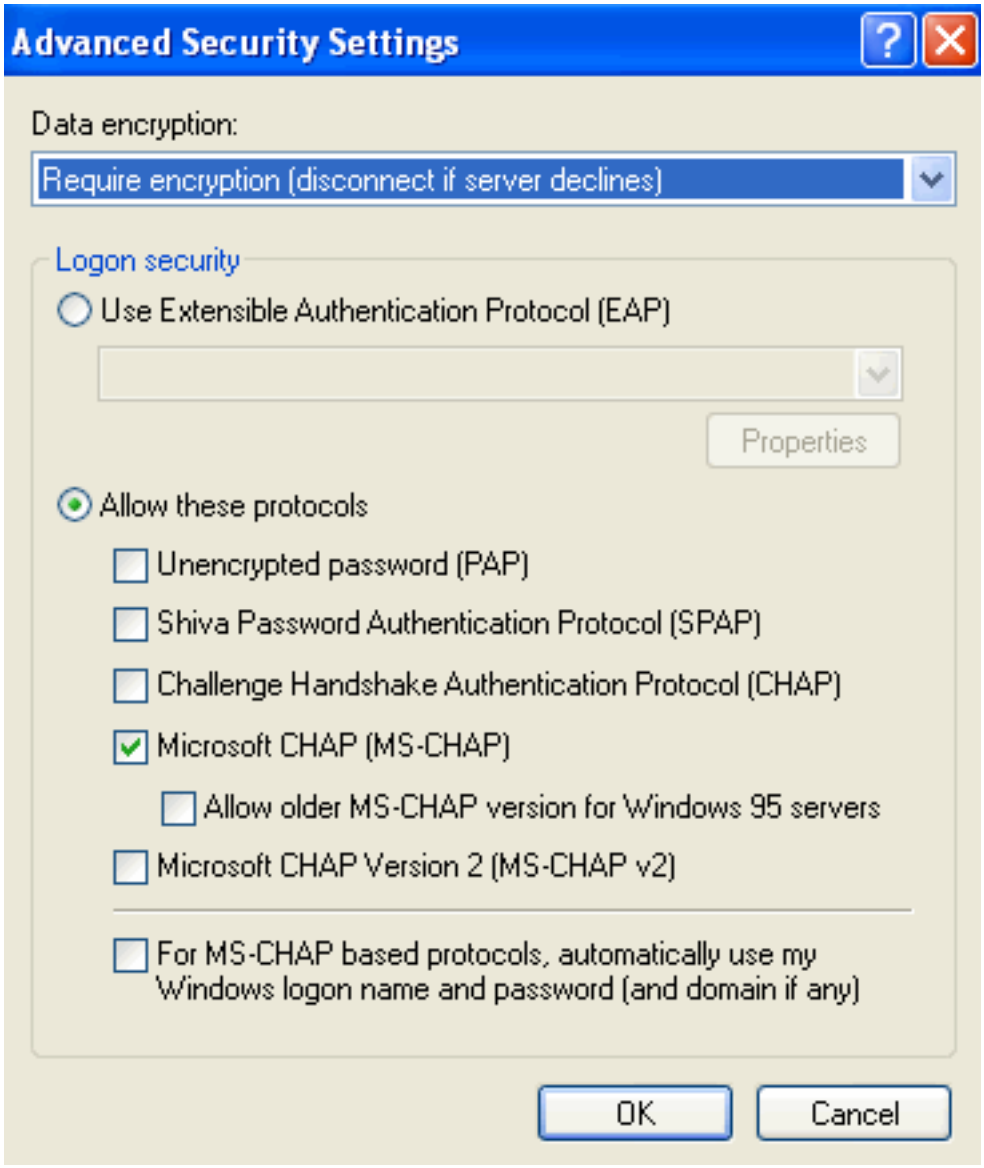
- Windows L2TP/IPsec 客户端配置
- PIX 中的 L2TP 服务器配置
- 使用 ASDM 的 L2TP 配置

- 具有 IAS 的 Microsoft Windows 2003 Server 配置

Windows L2TP/IPsec 客户端配置

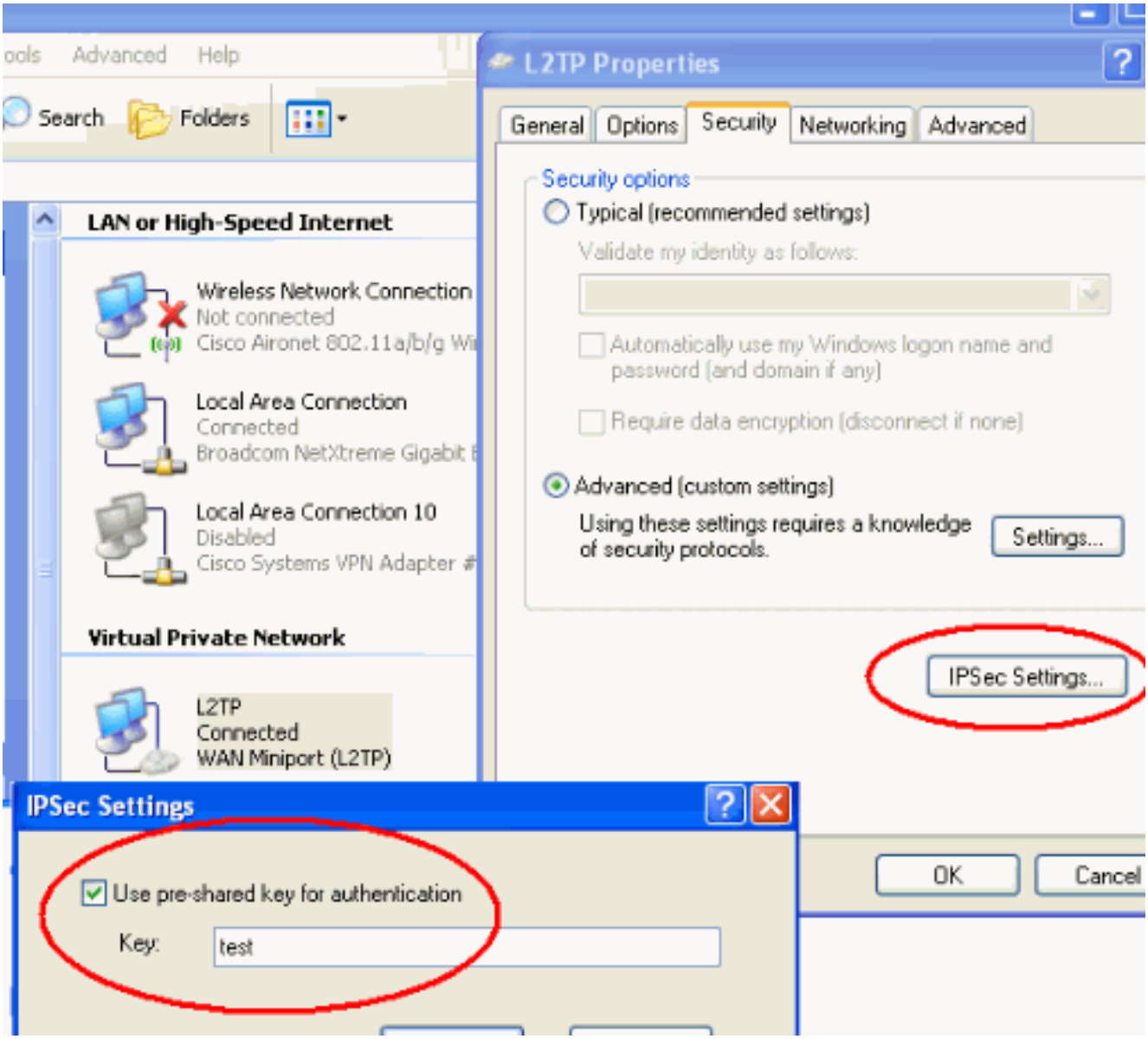
完成以下步骤以在 Windows 2000 上配置 L2TP over IPsec。对于 Windows XP，请跳过步骤 1 和步骤 2，从步骤 3 开始：

1. 将以下注册表值添加到 Windows 2000 计算机
   ：HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
2. 将以下注册表值添加到此项：Value Name: ProhibitIpSec
   Data Type: REG_DWORD
   Value: 1**注意：** 在某些情况下 (Windows XP SP2)，添加此项 **(值：1)** 似乎会中断连接，因为它会使 XP 机箱仅协商 L2TP 而不是协商 L2TP 与 IPsec 连接。强制添加 IPsec 策略与该注册表项。如果在尝试建立连接时收到 error 800，请删除项（值：1）以使连接得以进行。**注意：** 必须重新启动 Windows 2000/2003 或 XP 计算机才能使更改生效。默认情况下，Windows 客户端尝试在证书颁发机构 (CA) 中使用 IPsec。配置此注册表项可防止出现此情况。现在您可以在 Windows 工作站上配置 IPsec 策略以匹配在 PIX/ASA 上所需的参数。有关 Windows IPsec 策略的逐步配置，请参阅如何使用预共享密钥身份验证配置 L2TP/IPSec 连接 (Q240262)。有关详细信息，请参阅在 Windows XP 中配置用于第二层隧道协议 (L2TP) 连接的预共享密钥 (Q281555)\。
3. 创建连接。
4. 在“网络和拨号连接”下，右键单击“连接”并选择**属性**。转到“安全”选项卡并单击**高级**。按照此图



的显示选择协议。

5. **注意：**此步骤仅适用于 Windows XP。单击 **IPSec 设置**，选中“使用预共享的密钥进行身份验证”并键入预共享密钥以设置预共享密钥。在本示例中，使用 test 作为预共享密钥。



PIX 中的 L2TP 服务器配置

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**

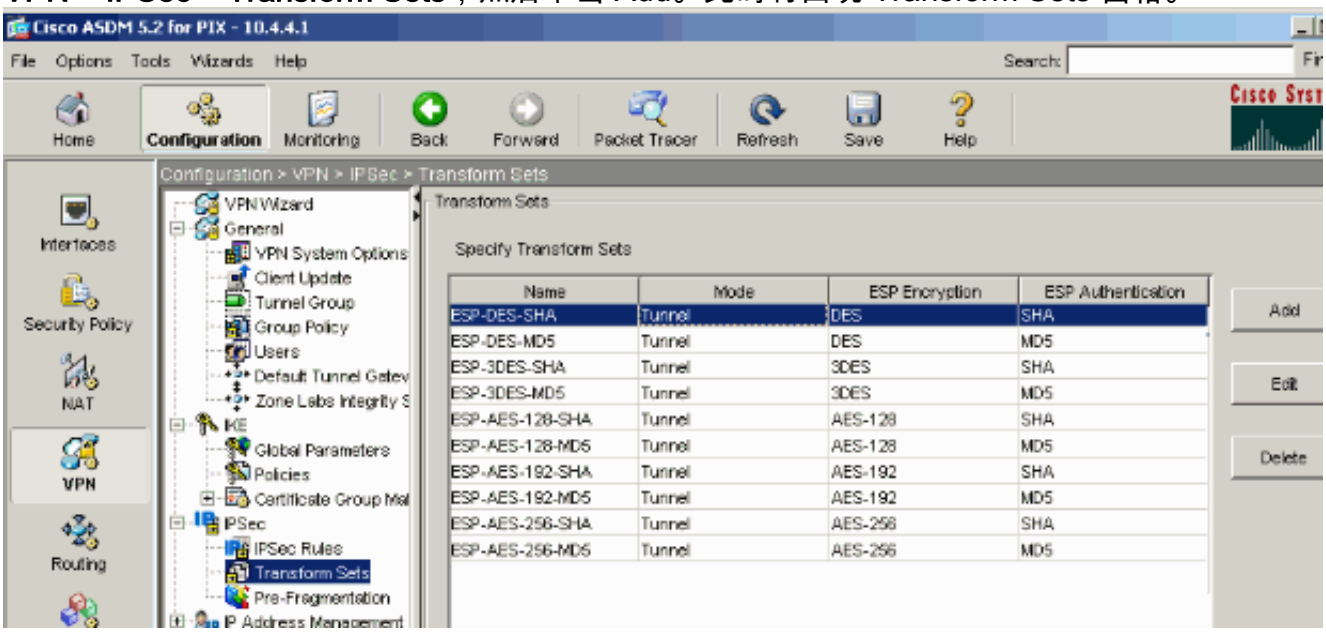
```
(inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0
172.16.1.2 1 timeout xlate 3:00:00 timeout conn 1:00:00
half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00
sip-invite 0:03:00 sip-disconnect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

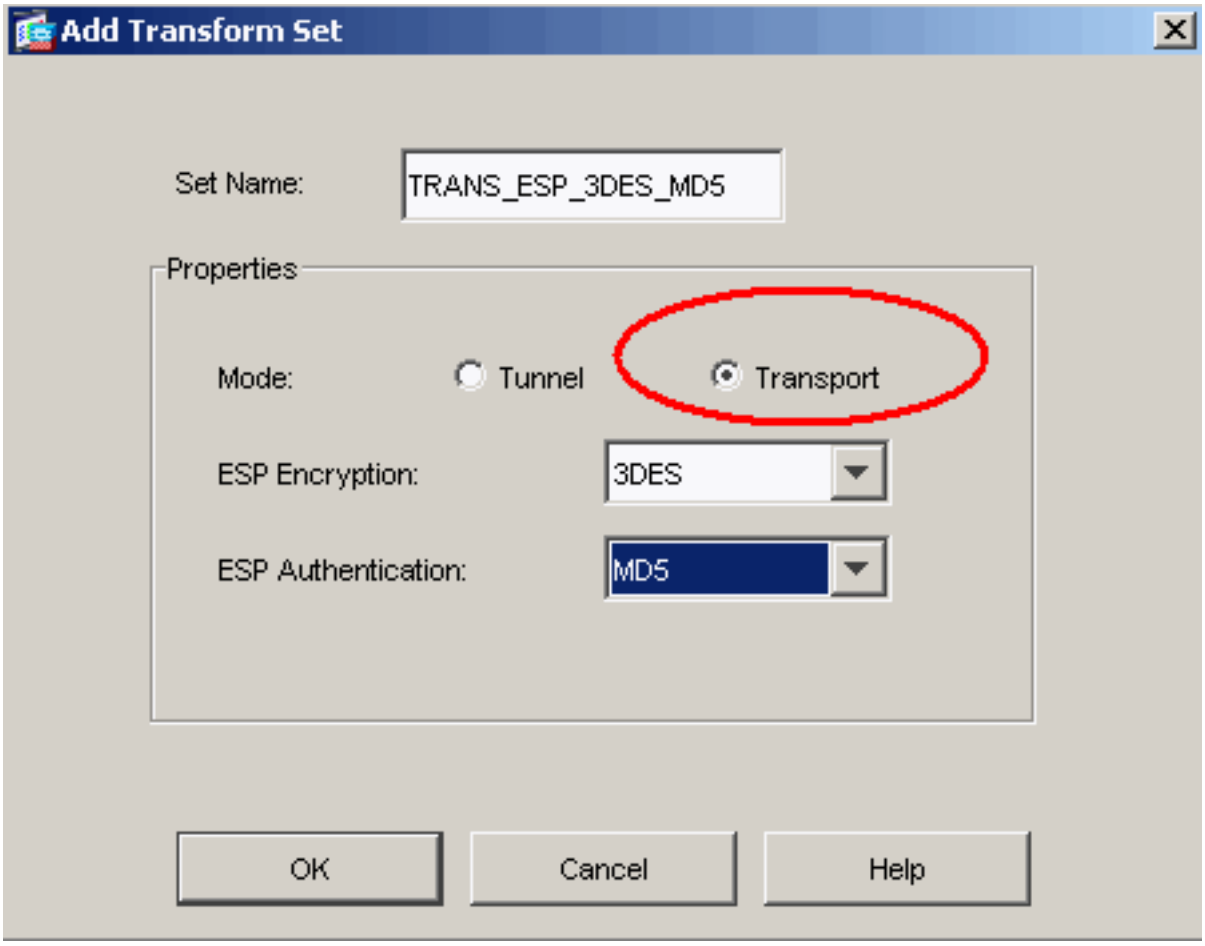
使用 ASDM 的 L2TP 配置

完成以下步骤以将安全设备配置为接受 L2TP over IPsec 连接：

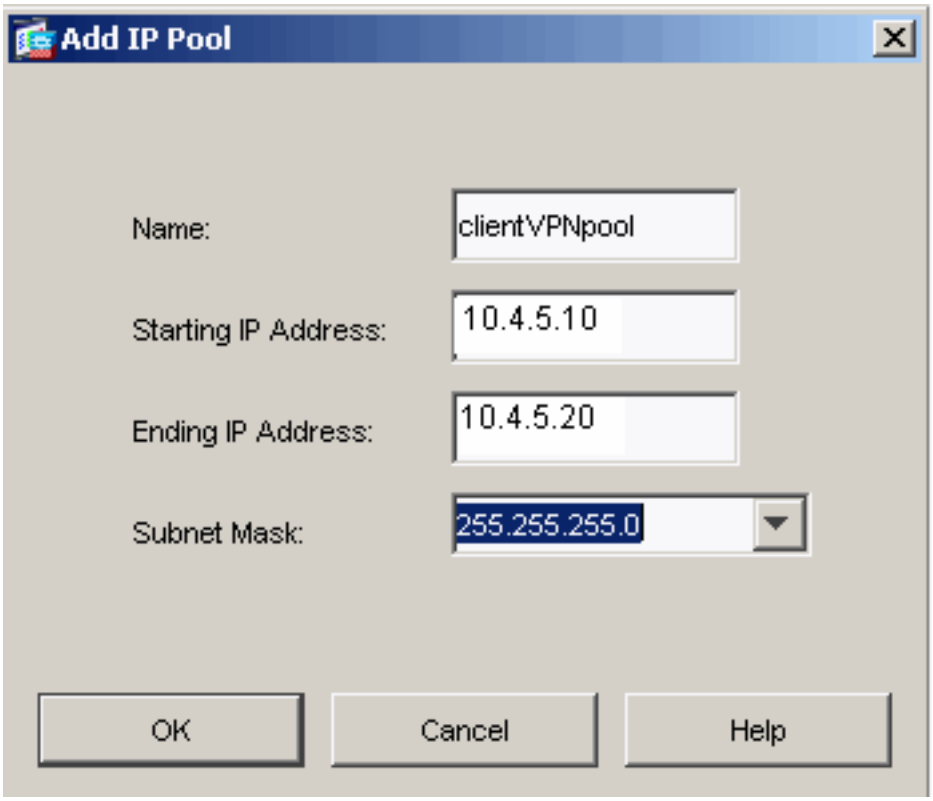
1. 添加 IPsec 转换集并指定 IPsec 使用传输模式而不是隧道模式。为此，请选择 **Configuration > VPN > IPSec > Transform Sets**，然后单击 Add。此时将出现 Transform Sets 窗格。



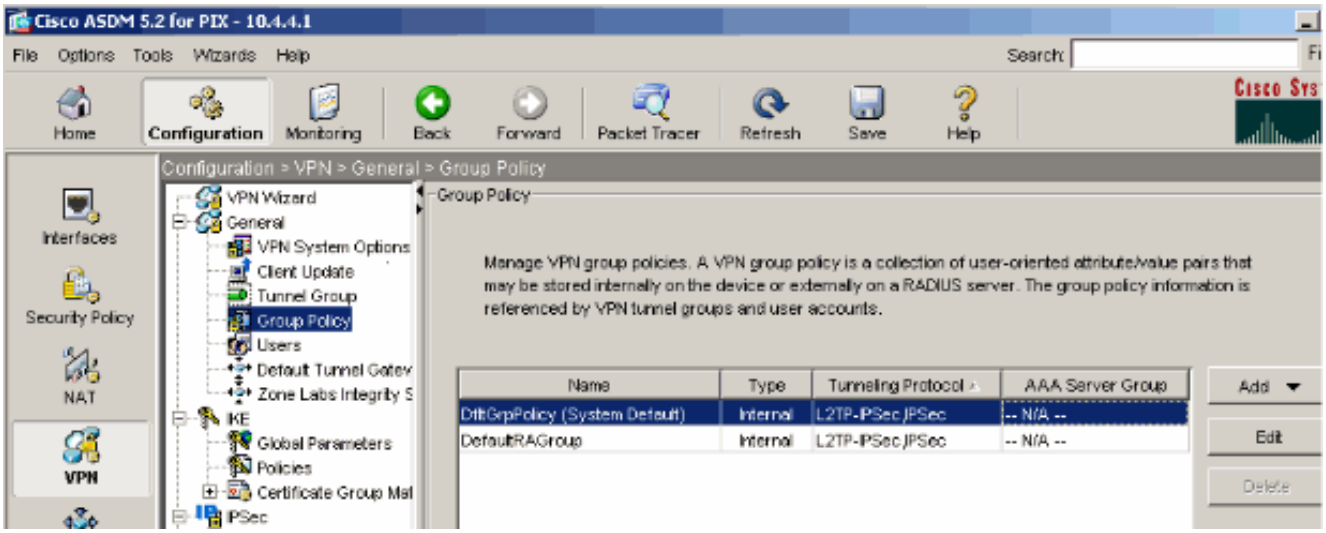
2. 完成以下步骤以添加转换集：为转换集输入一个名称。选择 ESP Encryption 和 ESP Authentication 方法。选择 **Transport** 模式。单击 **Ok**。



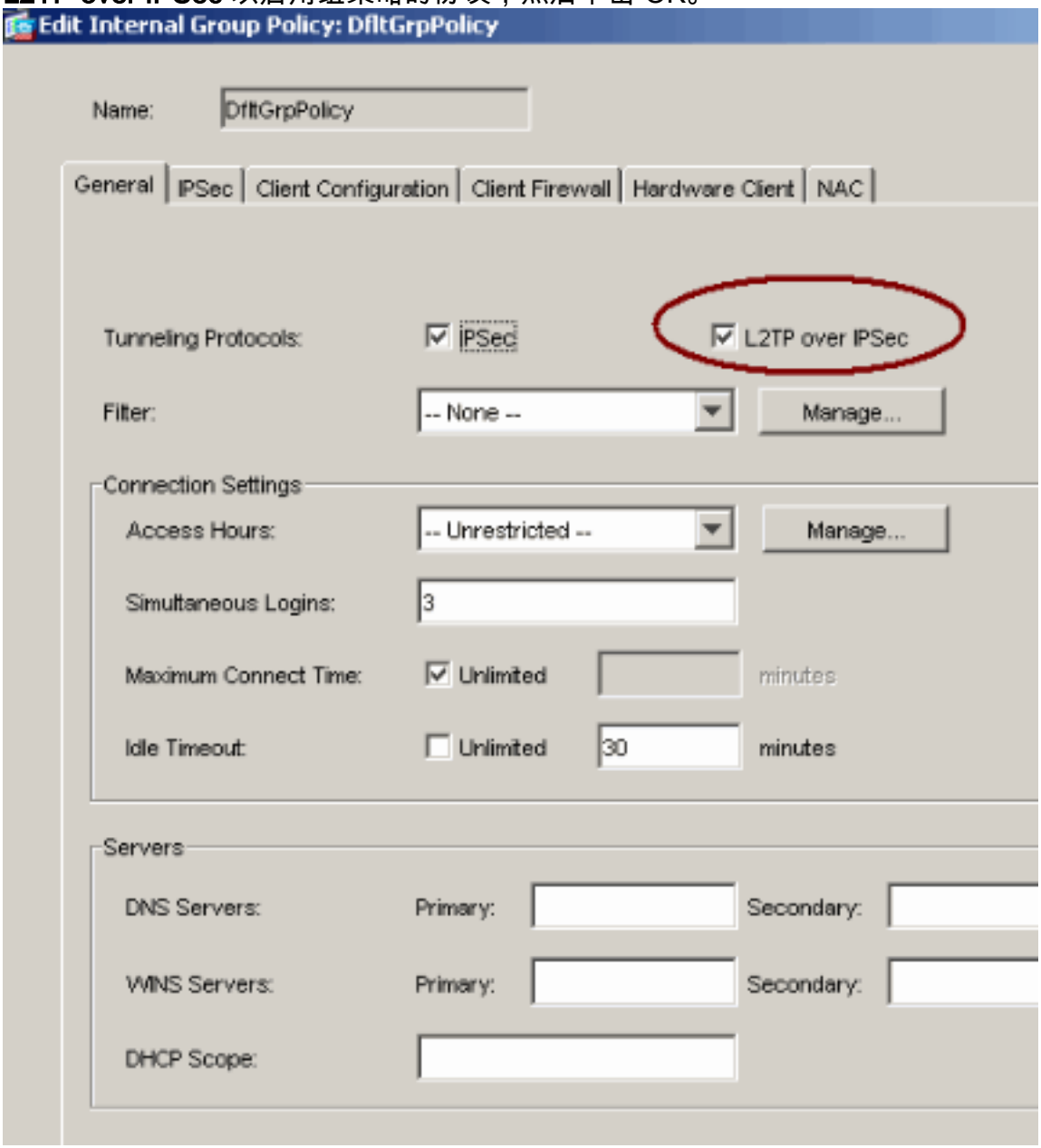
3. 完成以下步骤以配置地址分配方法。此示例使用 IP 地址池。选择 **Configuration> VPN > IP Address Management > IP Pools**。单击 **Add**。此时将出现 Add IP Pool 对话框。输入新 IP 地址池的名称。输入起始和结束 IP 地址。输入子网掩码并单击 **OK**。



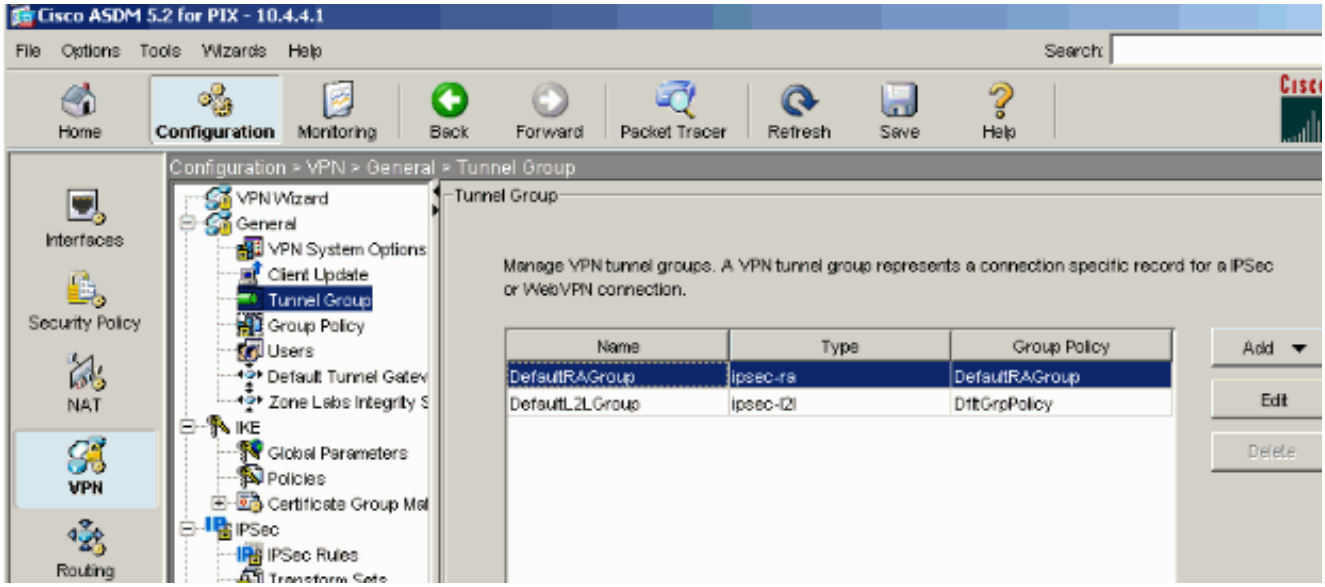
4. 选择 **Configuration > VPN > General > Group Policy** 以将 L2TP over IPsec 配置为组策略的有效 VPN 隧道协议。此时将出现 Group Policy 窗格。



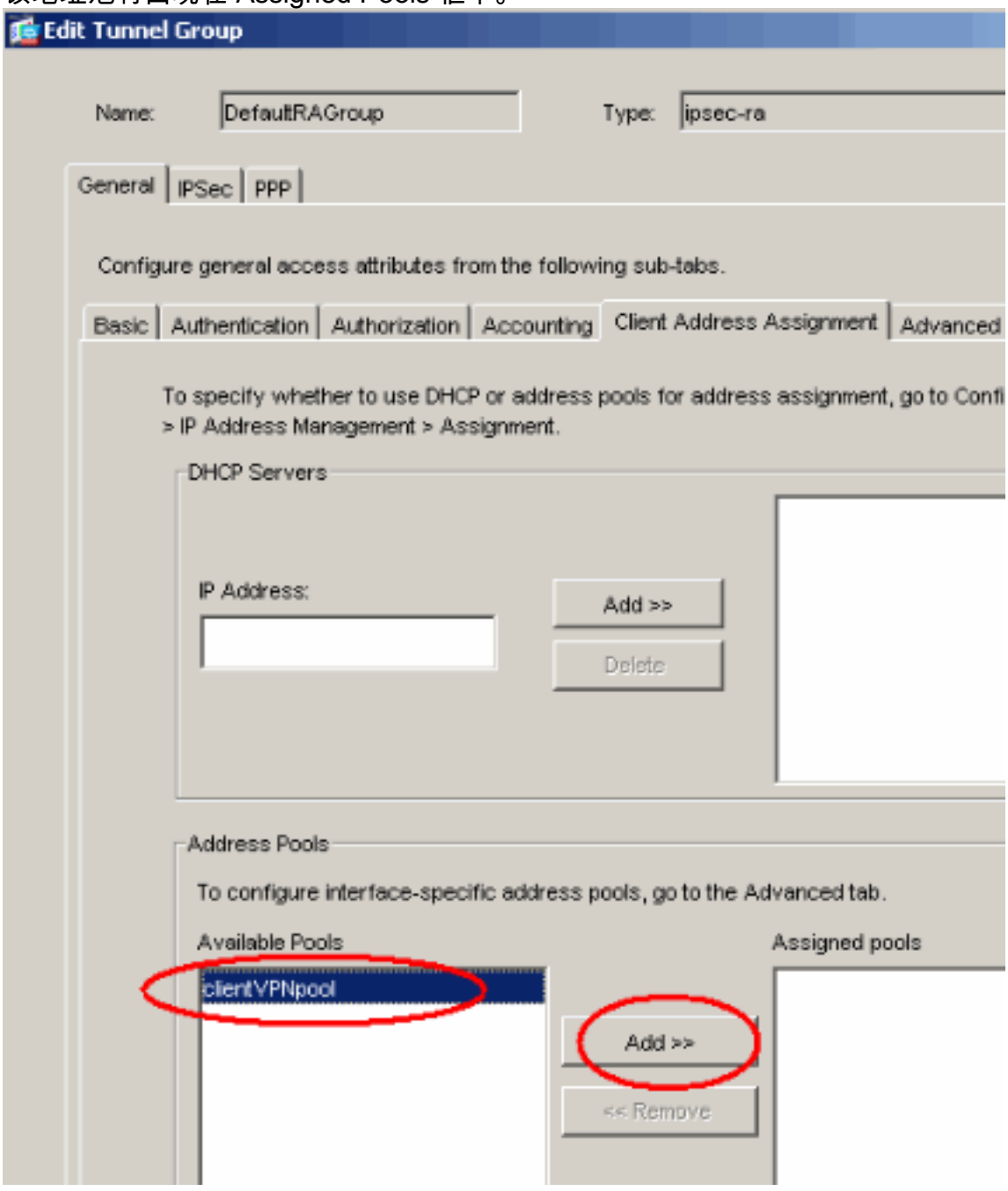
5. 选择一个组策略 (DiffGrpPolicy) 并单击 **Edit**。此时将出现 Edit Group Policy 对话框。选中 **L2TP over IPSec** 以启用组策略的协议，然后单击 OK。



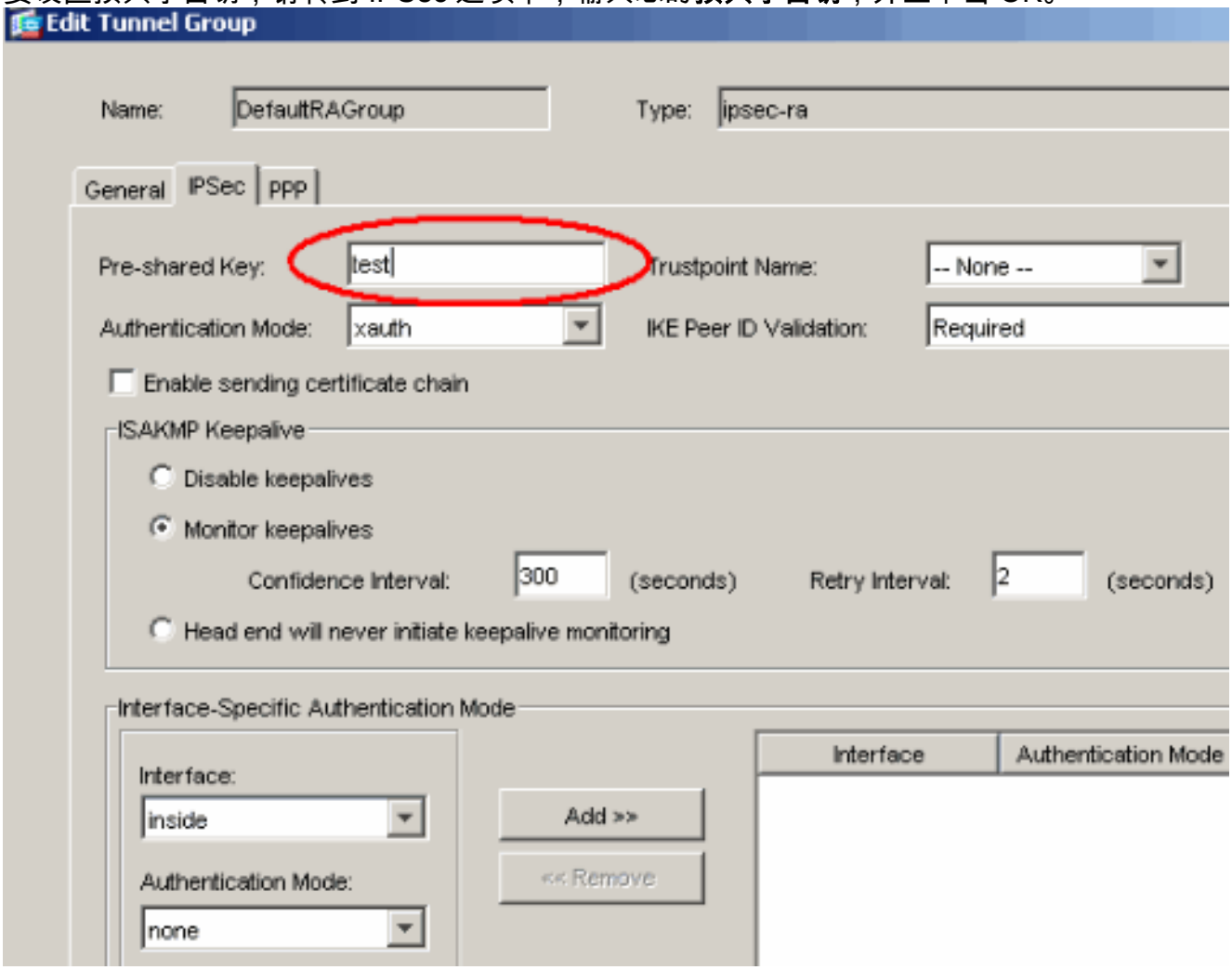
6. 完成以下步骤以将 IP 地址池分配到隧道组：选择 **Configuration > VPN > General > Tunnel Group**。出现 Tunnel Group 窗格后，在表中选择一个隧道组 (DefaultRAGroup)。单击 **Edit**。



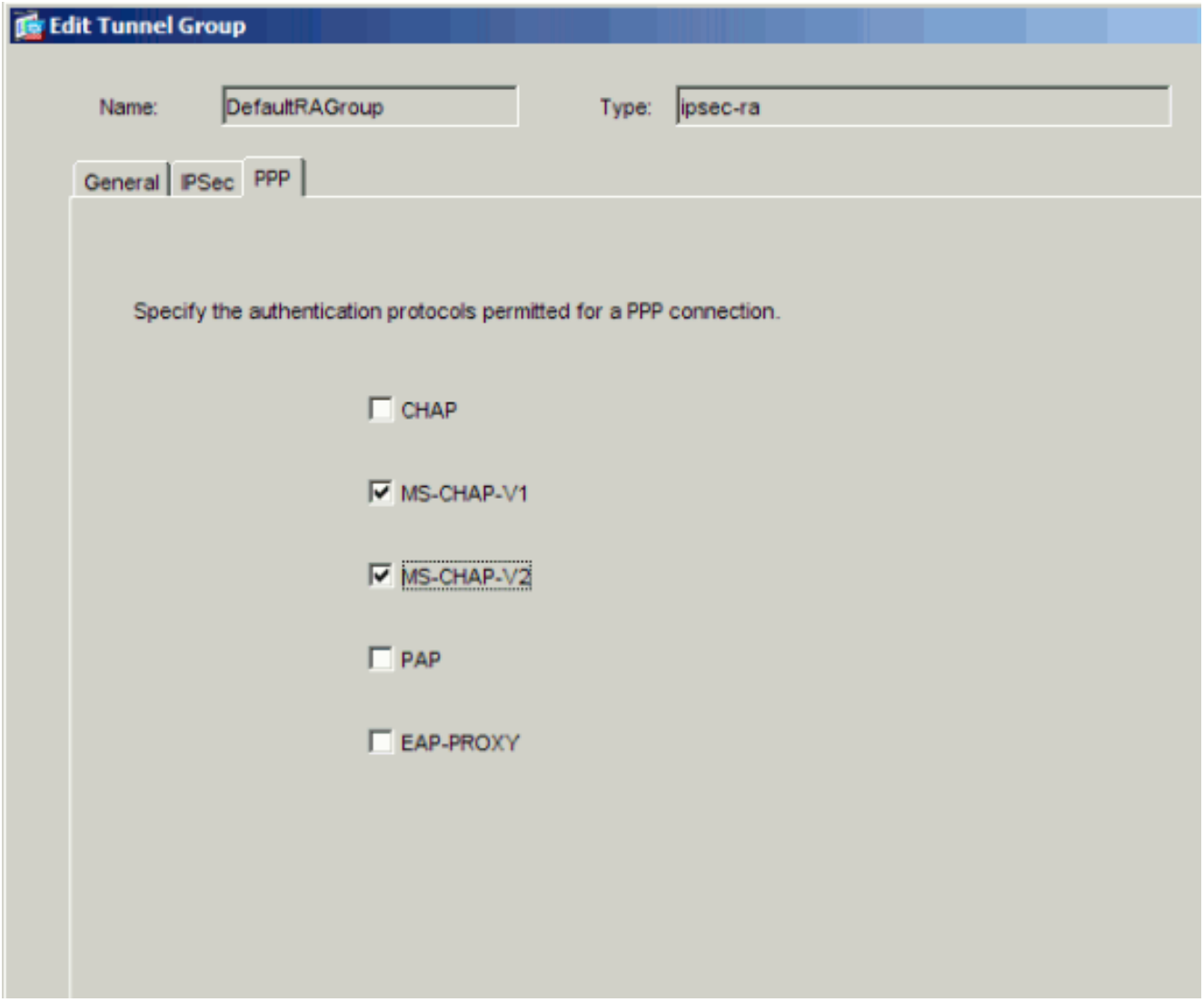
7. 出现 Edit Tunnel Group 窗口时，完成以下步骤：在 General 选项卡中，转到 Client Address Assignment 选项卡。在 Address Pools 区域中，选择要分配给隧道组的地址池。单击 **Add**。该地址池将出现在 Assigned Pools 框中。



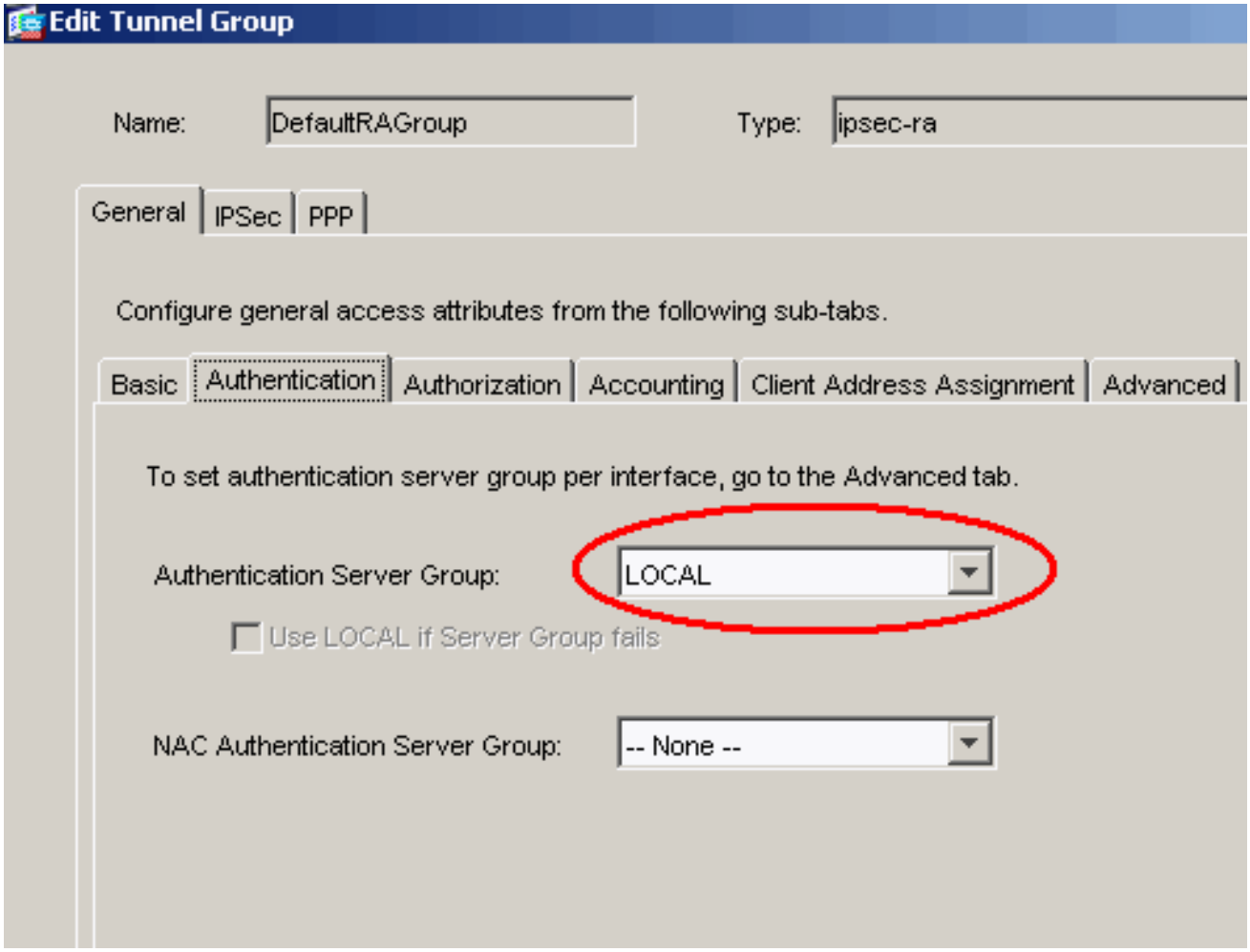
8. 要设置预共享密钥，请转到 IPSec 选项卡，输入您的**预共享密钥**，并且单击 OK。



9. L2TP over IPsec 使用 PPP 身份验证协议。指定隧道组的 PPP 选项卡上的 PPP 连接允许的协议。选择 **MS-CHAP-V1** 协议进行身份验证。

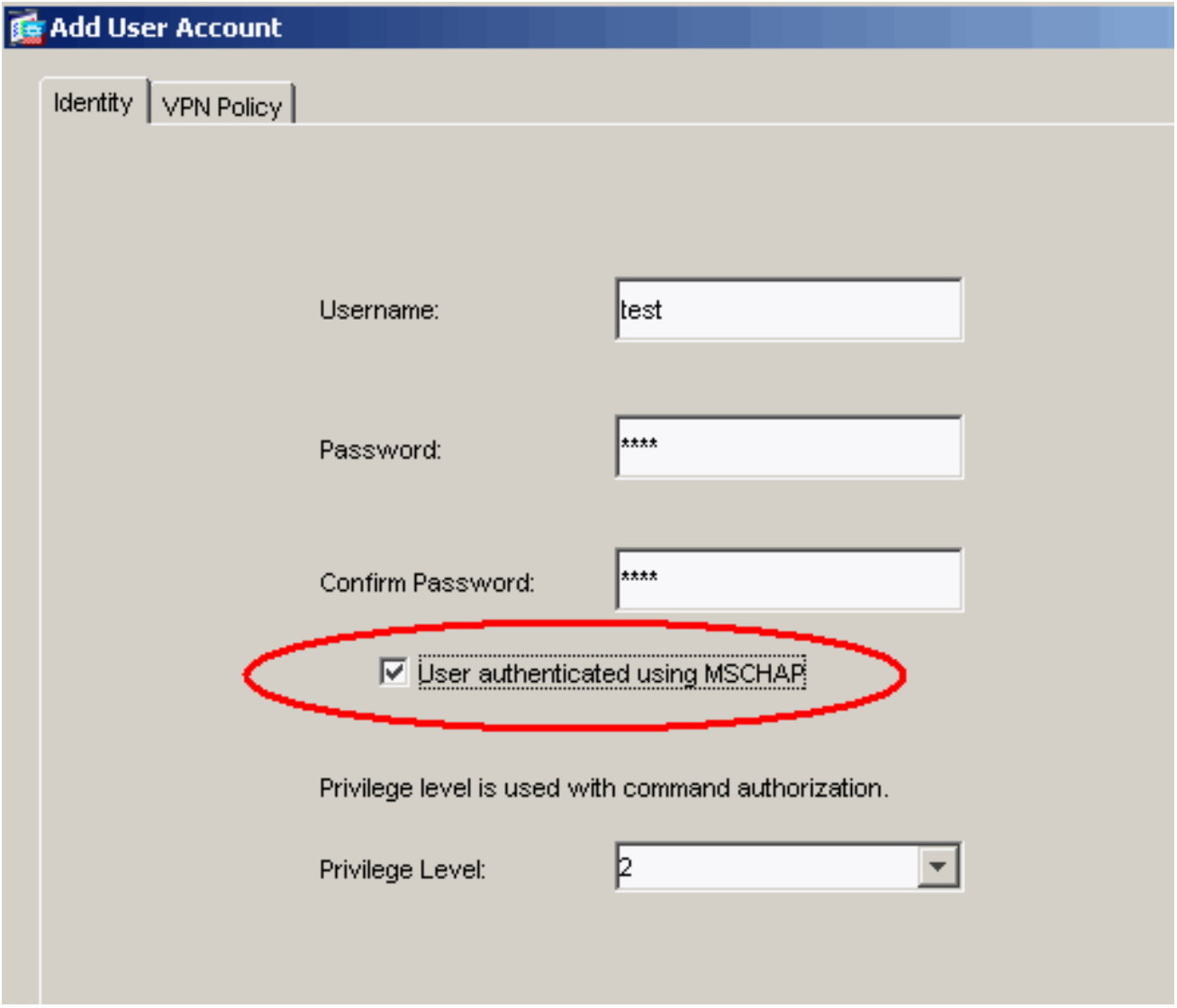


10. 指定用于对尝试进行 L2TP over IPsec 连接的用户进行身份验证的方法。可以将安全设备配置为使用身份验证服务器或其自己的本地数据库。为此，请转到隧道组的 Authentication 选项卡。默认情况下，安全设备使用其本地数据库。Authentication Server Group 下拉列表显示 LOCAL。要使用身份验证服务器，请从列表中选择一项。**注意：** 安全设备仅支持本地数据库上的 PPP 身份验证 PAP 和 Microsoft CHAP 版本 1 和 2。EAP 和 CHAP 由代理身份验证服务器执行。因此，如果远程用户属于配置为使用 EAP 或 CHAP 的隧道组，且安全设备配置为使用本地数据库，则用户无法连接。

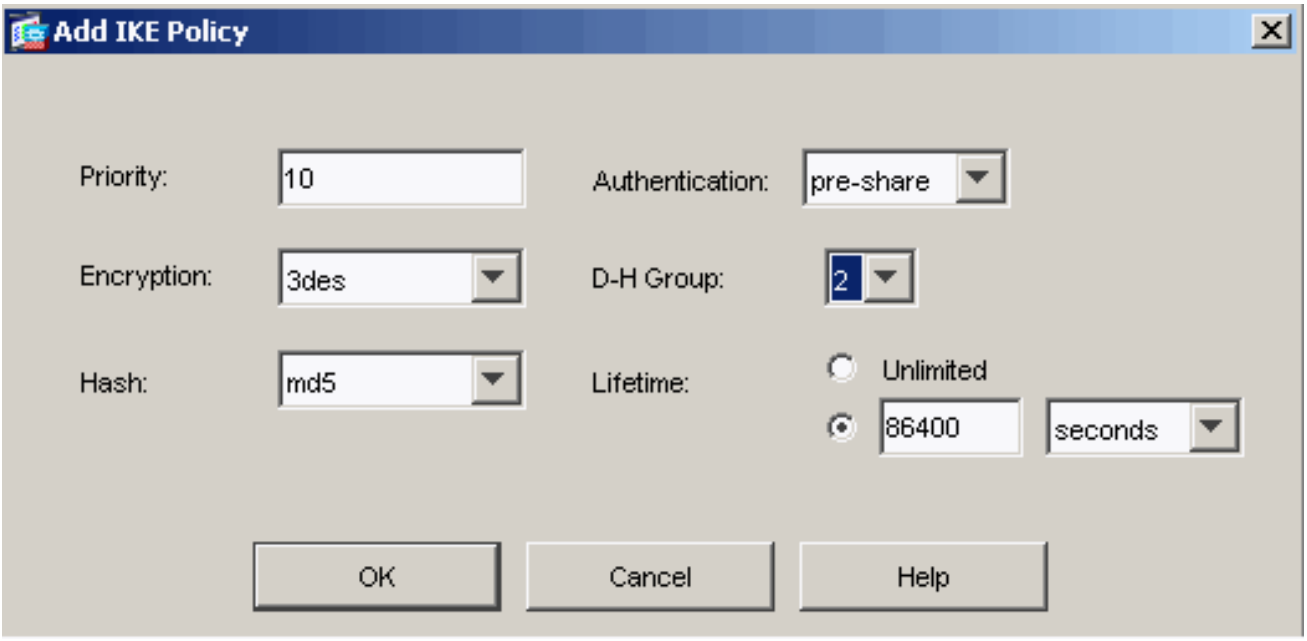


注意： 选择 **Configuration > VPN > General > Tunnel Group** 以返回隧道组配置，这样您可以将组策略链接到隧道组并启用隧道组交换（可选）。出现 Tunnel Group 窗格时，请选择隧道组并单击 **Edit**。**注意：** 通过隧道组交换，安全设备可以将建立 L2TP over IPsec 连接的不同用户与不同的隧道组相关联。由于每个隧道组都具有其自己的 AAA 服务器组和 IP 地址池，因此可以通过特定于用户的隧道组的方法对用户进行身份验证。使用此功能，而不是仅发送用户名，用户可以采用 username@group_name 格式发送用户名和组名，其中，“@”表示可以配置的分隔符，且组名是在安全设备上配置的隧道组的名称。**注意：** 隧道组交换通过条带组处理启用，后者可使安全设备通过从 VPN Client 提供的用户名获取组名来选择用户连接的隧道组。安全设备然后仅发送用户名的用户部分进行授权和身份验证。否则（如果禁用），安全设备将发送整个用户名，包括领域。要启用隧道组交换，请选中 **Strip the realm from username before passing it on to the AAA server**，并选中 Strip the group from username before passing it on to the AAA server。然后单击 **OK**。

11. 完成以下步骤以在本地数据库中创建用户：选择 **Configuration > Properties > Device Administration > User Accounts**。单击 **Add**。如果用户是使用 Microsoft CHAP 版本 1 或 2 的 L2TP 客户端，且安全设备配置为对照本地数据库进行身份验证，则必须选中 **User Authenticated using MSCHAP** 才能启用 MSCHAP。单击 **Ok**。



12. 选择 **Configuration > VPN > IKE > Policies** 并单击 Add，以便为阶段 I 创建 IKE 策略。单击 OK 以继续。



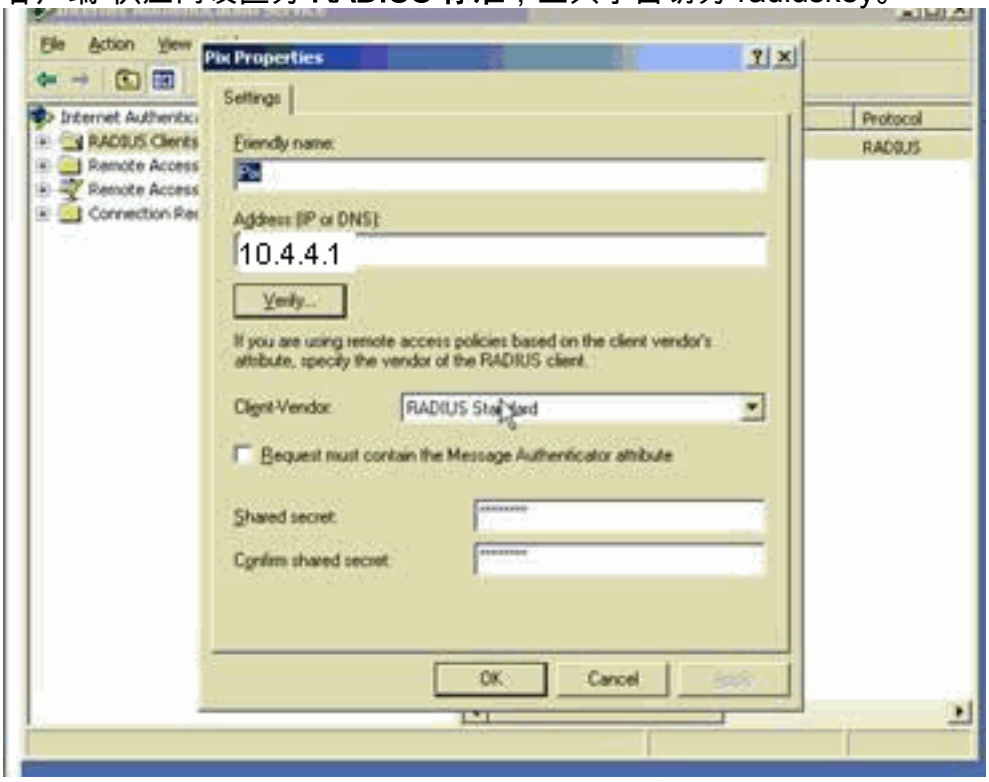
13. （可选）如果希望 NAT 设备后的多个 L2TP 客户端尝试建立到安全设备的 L2TP over IPsec 连接，则必须启用 NAT 穿透以便 ESP 数据包可以通过一个或多个 NAT 设备。要执行上述操作，请完成以下步骤：选择 **Configuration > VPN > IKE > Global Parameters**。确保在接口上启用 **ISAKMP**。选中 **Enable IPSec over NAT-T**。单击 **Ok**。

具有 IAS 的 Microsoft Windows 2003 Server 配置

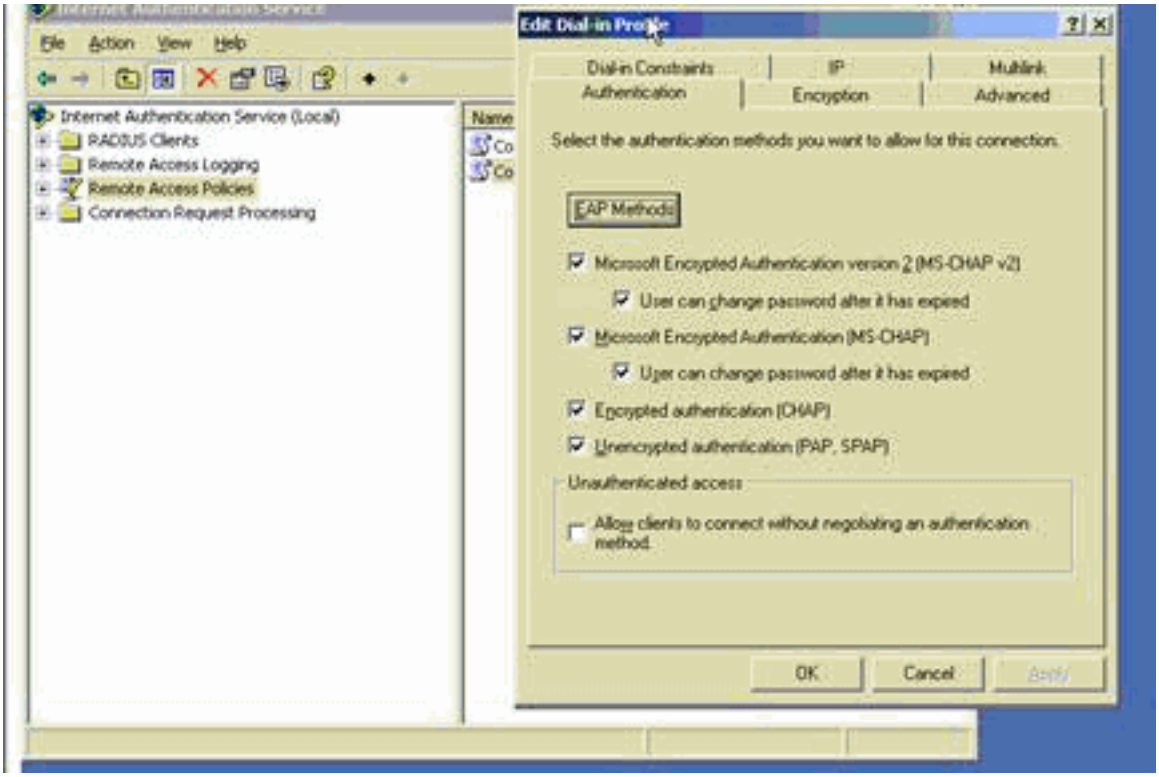
完成以下步骤以配置具有 IAS 的 Microsoft Windows 2003 Server。

注意： 这些步骤假设本地计算机上已安装 IAS。如果未安装，请通过**控制面板 > 添加/删除程序**进行添加。

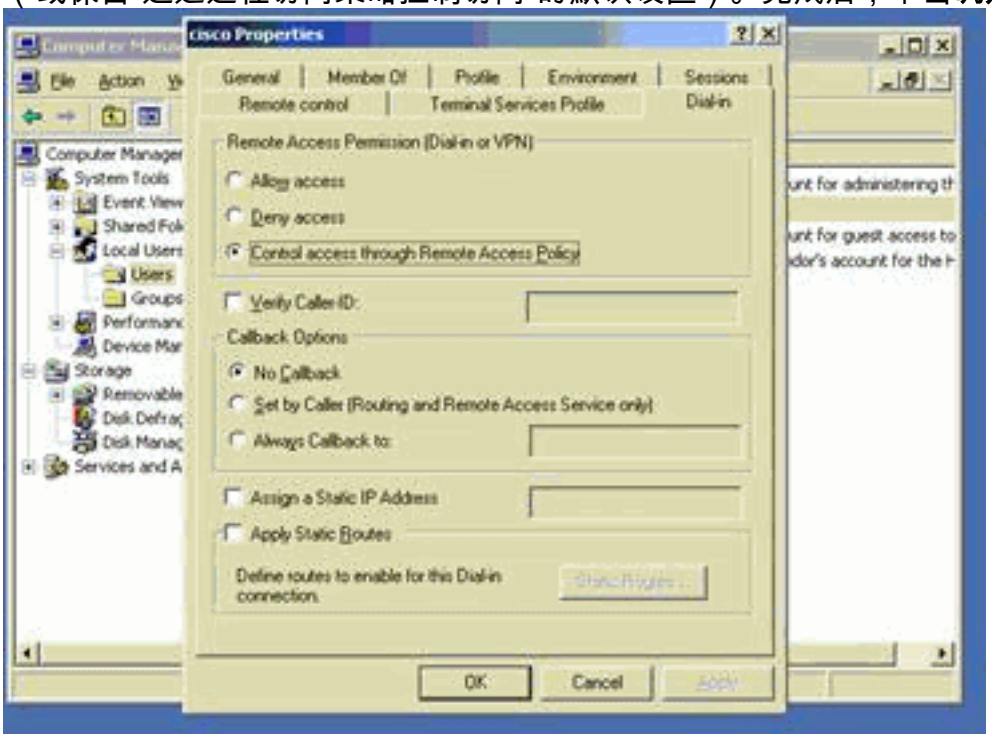
1. 选择**管理工具> Internet 验证服务**并右键单击 RADIUS 客户端，以添加新的 RADIUS 客户端。键入客户端信息后，单击**确定**。本示例显示一个名为“Pix”的客户端，其 IP 地址为 10.4.4.1。客户端-供应商设置为 **RADIUS 标准**，且共享密钥为 radiuskey。



2. 选择**远程访问策略**，右键单击“到其他访问服务器的连接”，然后选择“属性”。
3. 确保选中**授予远程访问权限**选项。
4. 单击**编辑配置文件**并选中以下设置：在“身份验证”选项卡上，选中**未加密的身份验证 (PAP，SPAP)**。在“加密”选项卡上，确保选中**不加密**选项。完成后，单击**确定**。



5. 选择**管理工具 > 计算机管理 > 系统工具 > 本地用户和组**，右键单击“用户”并选择“新用户”，以向本地计算机帐户中添加用户。
6. 使用 Cisco 口令 **password1** 添加用户，并检查此配置文件信息：在“常规”选项卡上，确保选中**口令永不过期**选项而不是“用户必须更改口令”选项。在“拨入”选项卡上，选中**允许访问**选项（或保留“通过远程访问策略控制访问”的默认设置）。完成后，单击**确定**。



IPSec上的L2TP的扩展认证使用活动目录

请使用在ASA的此配置为了允许验证L2TP连接从活动目录发生：

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

并且，在L2TP客户端，请去**高级安全设置(自定义)**并且选择**未加密的密码的(PAP)**仅选项。

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

- **show crypto ipsec sa** - 显示对等体上的所有当前 IKE 安全关联 (SA)。`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** - 显示对等体上的所有当前 IKE SA。`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** - 包含可用来查看有关 L2TP over IPsec 连接的详细信息的协议过滤器。全局配置模式下的完整命令是 **show vpn-sessoindb detailed remote filter protocol l2tpOverIpsec**。本示例显示单个 L2TP over IPsec 连接的详细信息：`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`

故障排除

本部分提供的信息可用于对配置进行故障排除。此外本部分还提供了 debug 输出示例。

故障排除命令

Certain commands are supported by the 命令输出解释程序工具（仅限注册用户）支持某些命令，使用此工具可以查看对 show 命令输出的分析。

注意： 使用 **debug** 命令之前，请参阅有关 debug 命令的重要信息和 IP 安全故障排除 - 了解和使用 debug 命令。

- **debug crypto ipsec 7** - 显示第 2 阶段的 IPsec 协商。
- **debug crypto isakmp 7** - 显示第 1 阶段的 ISAKMP 协商。

调试输出示例

PIX 防火墙

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
```

使用 ASDM 进行故障排除

您可以使用 ASDM 启用日志记录和查看日志。

1. 选择 **Configuration > Properties > Logging > Logging Setup**，选择 Enable Logging 并且单击 Apply 以启用日志记录。
2. 选择 **Monitoring > Logging > Log Buffer > On Logging Level**，选择 Logging Buffer，并单击 View 以查看日志。

问题：频繁断开连接

空闲/会话超时

如果空闲超时设置为 30 分钟（默认值），则意味着如果超过 30 分钟没有流量通过隧道，则将丢弃该隧道。VPN Client 将在 30 分钟后断开连接，而不管空闲超时的设置如何，并且将出现 PEER_DELETE-IKE_DELETE_UNSPECIFIED 错误消息。

将 **idle timeout** 和 session timeout 配置为 none，以便使隧道始终保持活动状态，这样将不再会丢弃隧道。

在组策略配置模式下或用户名配置模式下输入 **vpn-idle-timeout** 命令，以配置用户超时时长：

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

请在组策略配置模式下或用户名配置模式下，使用 vpn-session-timeout 命令为 VPN 连接配置最大时长。

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

对 Windows Vista 进行故障排除

并发用户

Windows Vista L2TP/IPsec 引入了一些体系结构更改，禁止多个并发用户连接到前端 PIX/ASA。此行为在 Windows 2K/XP 中不会出现。自版本 7.2(3) 和更高版本以来，Cisco 已实现了此更改的解

决方法。

Vista PC 无法连接

如果 Windows Vista 计算机无法连接 L2TP 服务器，则请验证在 DefaultRAGroup 上的 PPP 属性下仅配置了 mschap-v2。

相关信息

- 最常用的 L2L 和远程访问 IPSec VPN 故障排除解决方案
- Cisco PIX 500 系列安全设备
- Cisco ASA 5500 系列自适应安全设备
- 思科PIX防火墙软件产品支持
- Cisco Secure PIX 防火墙命令参考
- RADIUS 支持页
- IPsec 协商/IKE 协议支持页
- 请求注解 (RFC)
- 第二层隧道协议 (L2TP)
- 技术支持和文档 - Cisco Systems