

带Microsoft Windows 2000和2003 IAS RADIUS认证的 Cisco Secure PIX防火墙6.x和用 于Windows 的Cisco VPN Client 3.5

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[调试输出示例](#)

[相关信息](#)

简介

此示例配置显示了如何配置 Cisco VPN 客户端 3.5 for Windows 和 Cisco Secure PIX 防火墙，以便与 Microsoft Windows 2000 和 2003 Internet 身份验证服务 (IAS) RADIUS 服务器一起使用。请参阅 [Microsoft - 清单：为拨号和VPN访问配置IAS](#)，以了解有关IAS的详细信息。

有关 PIX/ASA 7.0 中使用 Cisco VPN 客户端 4.x 的相同方案的详细信息，请参阅[采用 Microsoft Windows 2003 IAS RADIUS 身份验证的 PIX/ASA 7.x 和 Cisco VPN 客户端 4.x for Windows 的配置示例](#)。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- Cisco Secure PIX 防火墙软件版本 6.0 支持来自 Cisco VPN 客户端 3.5 for Windows 的 VPN 连接。
- 在此示例配置中，我们假设PIX已经与相应的静态、管道或访问表一起运行。当前文档的目的不是证明这些基本概念，而是显示了从Cisco VPN客户端到PIX的连接性。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- PIX 防火墙软件版本 6.1.1 **注意**：这已在PIX软件版本6.1.1上测试，但应适用于所有6.x版本。
- 适用于 Windows 的 Cisco VPN 客户端 3.5 版
- 具有 IAS 的 Windows 2000 和 2003 服务器

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。

规则

有关文档约定的更多信息，请参考 [Cisco 技术提示约定](#)。

配置

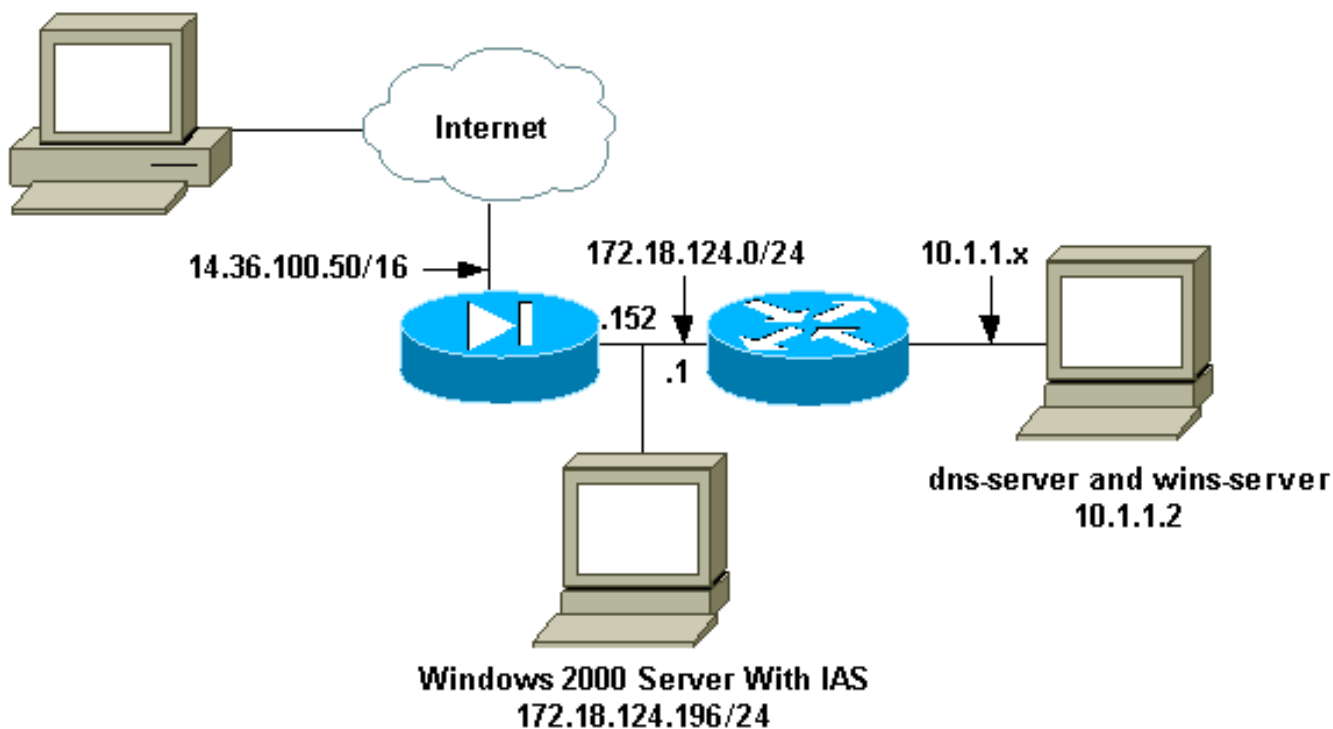
本部分提供有关如何配置本文档所述功能的信息。

注意：使用 [命令查找工具](#) (仅限注册客户) 可获取有关本节中使用的命令的详细信息。

网络图

本文档使用以下网络设置：

PC With VPN Client 3.5
14.36.100.55



配置

本文档使用以下配置。

- [PIX 防火墙](#)
- [适用于 Windows 的 Cisco VPN Client 3.5](#)
- [具有 IAS 的 Microsoft Windows 2000 服务器](#)
- [具有 IAS 的 Microsoft Windows 2003 服务器](#)

PIX 防火墙

PIX 防火墙

```

pixfirewall(config)#write terminal
Building configuration...
: Saved
:
PIX Version 6.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Issue the access-list command to avoid !--- Network
Address Translation (NAT) on the IPsec packets.

access-list 101 permit ip 10.1.1.0 255.255.255.0
10.1.2.0
255.255.255.0
pager lines 24
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 14.36.100.50 255.255.0.0
ip address inside 172.18.124.152 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool ippool 10.1.2.1-10.1.2.254
pdm history enable
arp timeout 14400
global (outside) 1 14.36.100.51
!--- Binding access list 101 to the NAT statement to
avoid !--- NAT on the IPsec packets. nat (inside) 0
access-list 101
Nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 14.36.1.1 1
route inside 10.1.1.0 255.255.255.0 172.18.124.1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout uauth 0:05:00 absolute
!--- Enable access to the RADIUS protocol.

```

```

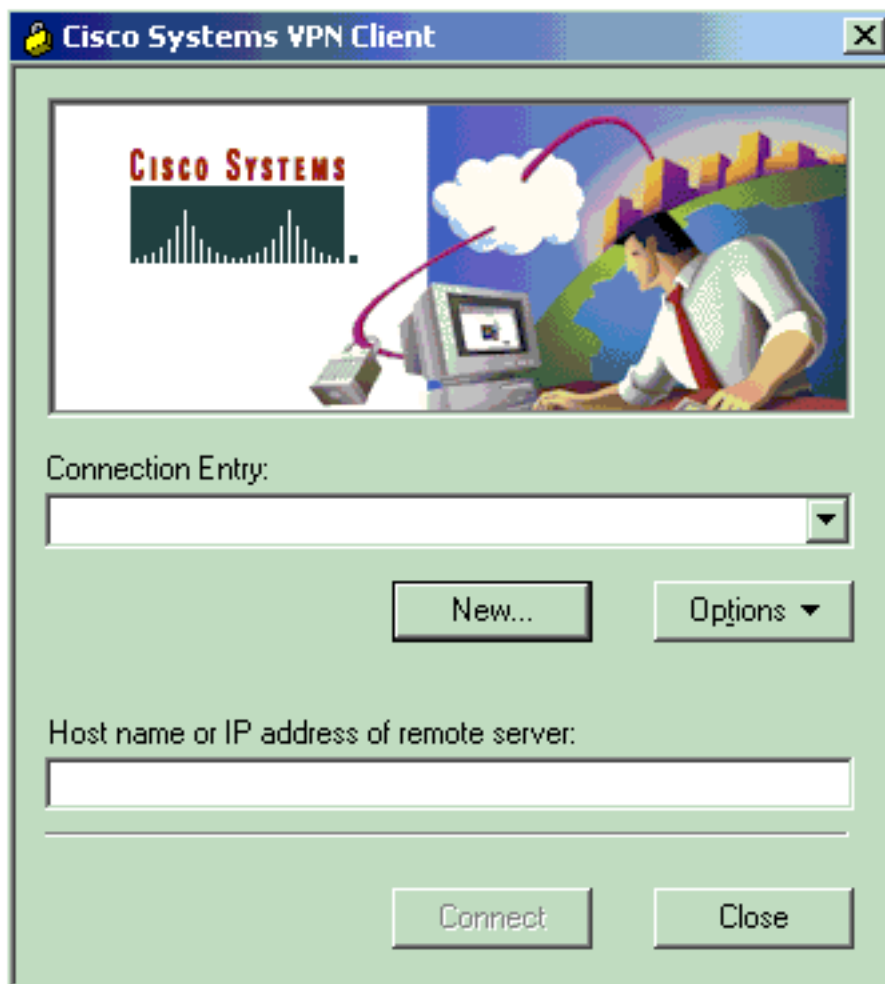
aaa-server RADIUS protocol radius
!--- Associate the partnerauth protocol to RADIUS. aaa-
server partnerauth protocol radius
aaa-server partnerauth (inside) host 172.18.124.196
cisco123
    timeout 5
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Tell PIX to implicitly permit IPsec traffic. sysopt
connection permit-ipsec
no sysopt route dnat
!--- Configure a transform set that defines how the
traffic is protected. crypto ipsec transform-set myset
esp-des esp-md5-hmac
!--- Create a dynamic crypto map and specify which !---
transform sets are allowed for this dynamic crypto map
entry. crypto dynamic-map dynmap 10 set transform-set
myset
!--- Add the dynamic crypto map set into a static crypto
map set. crypto map mymap 10 ipsec-isakmp dynamic dynmap
!--- Enable the PIX to launch the Xauth application on
the VPN Client. crypto map mymap client authentication
partnerauth
!--- Apply the crypto map to the outside interface.
crypto map mymap interface outside
!--- IKE Policy Configuration. isakmp enable outside
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- IPsec group configuration for VPN Client. vpngroup
vpn3000 address-pool ippool
vpngroup vpn3000 dns-server 10.1.1.2
vpngroup vpn3000 wins-server 10.1.1.2
vpngroup vpn3000 default-domain cisco.com
vpngroup vpn3000 idle-time 1800
vpngroup vpn3000 password *****
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:3f9e31533911b8a6bb5c0f06900c2dbc
: end
[OK]
pixfirewall(config)#

```

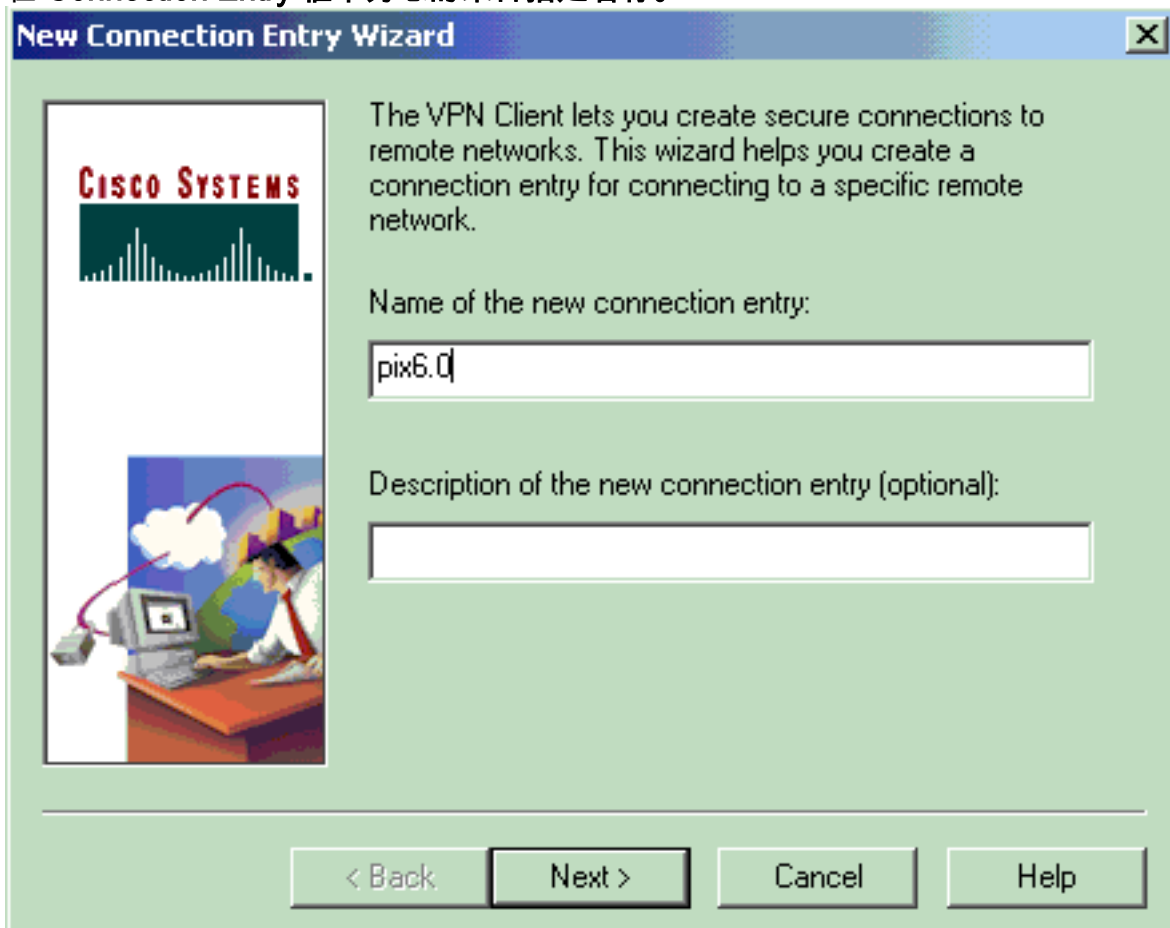
[适用于 Windows 的 Cisco VPN Client 3.5](#)

本部分说明如何配置 Cisco VPN 客户端 3.5 for Windows。

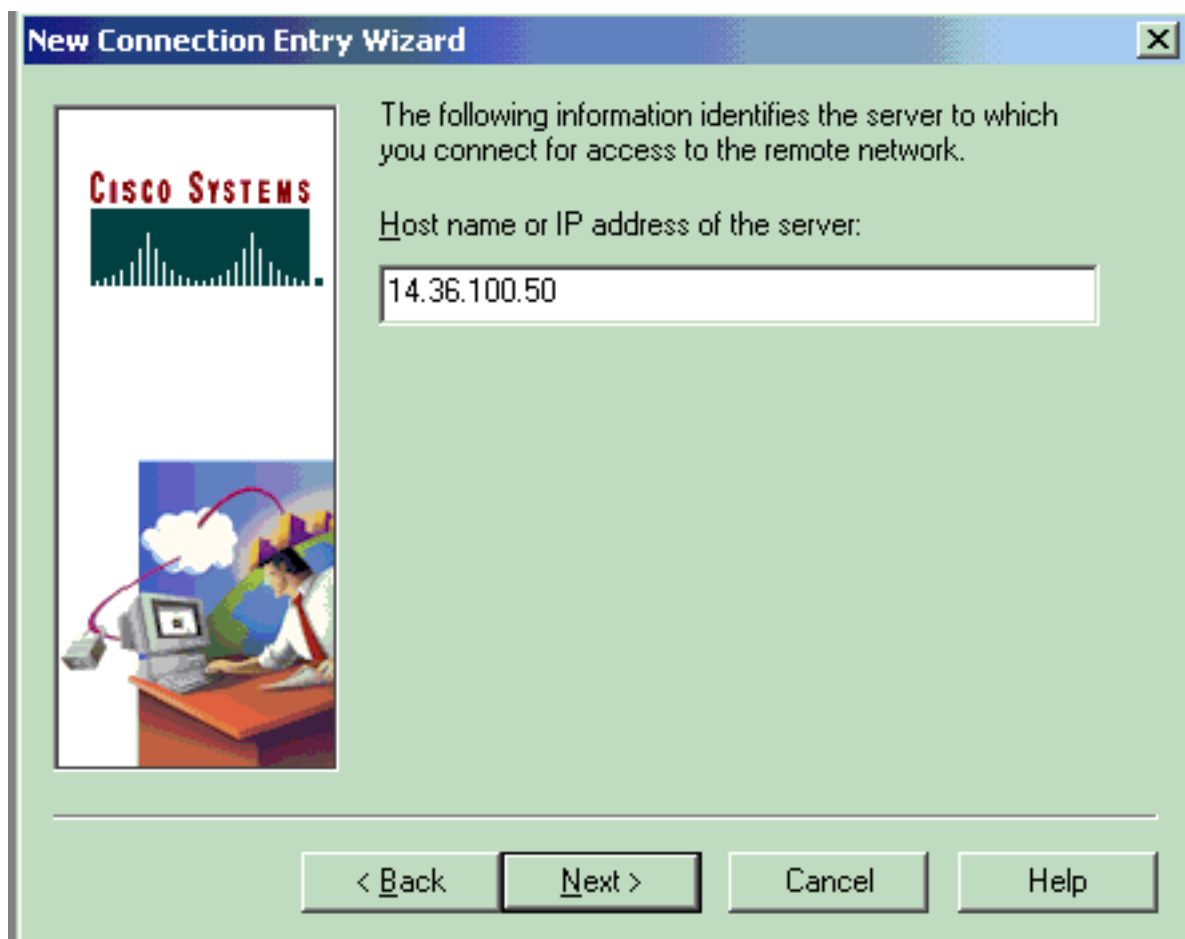
1. 启动 VPN 客户端，并单击 **New** 创建新连接。



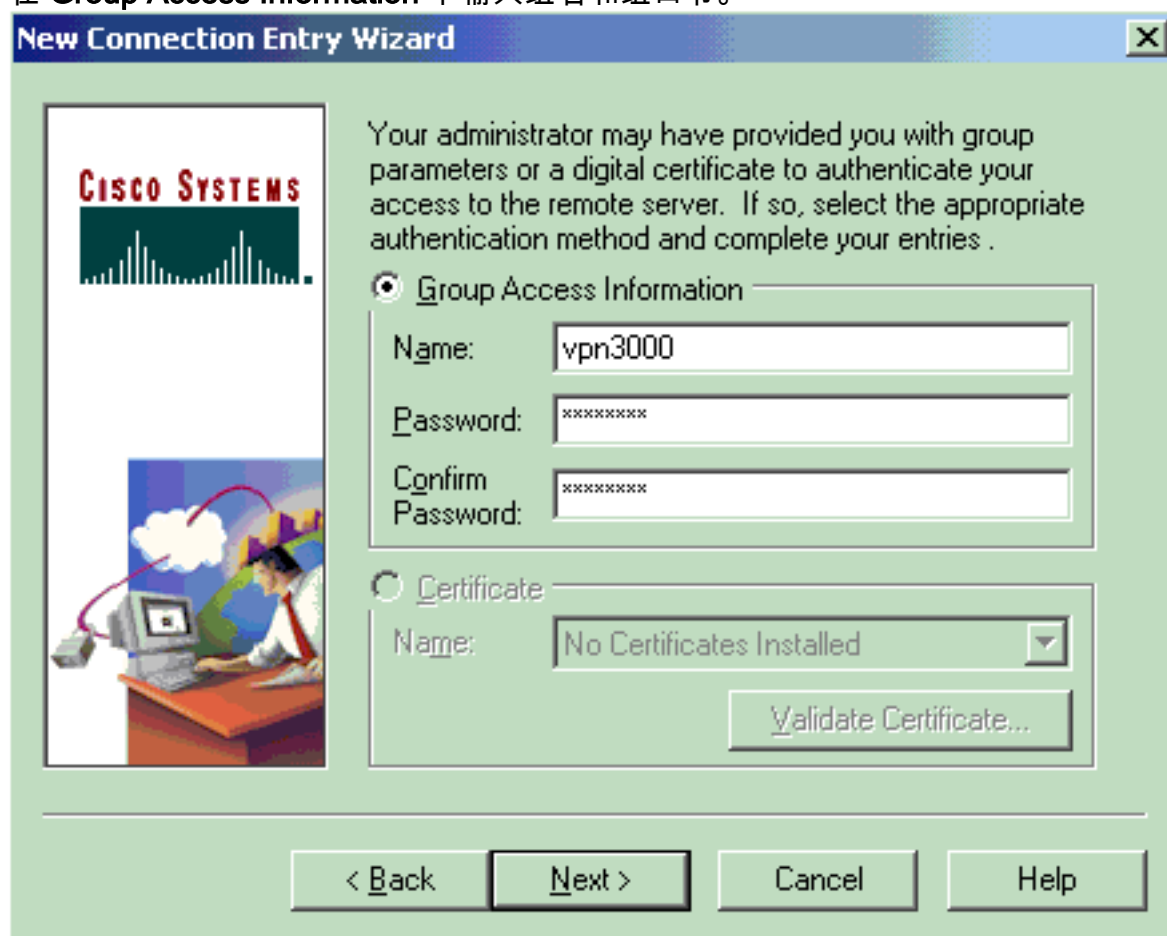
2. 在 Connection Entry 框中为您的条目指定名称。



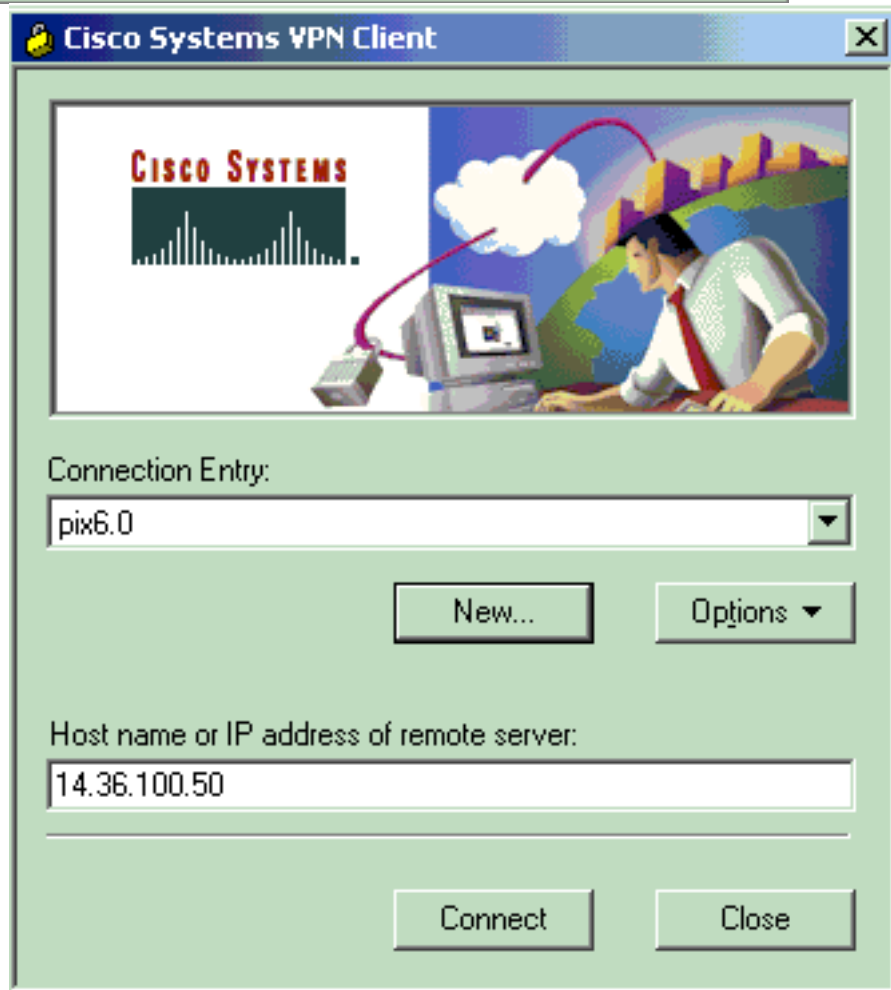
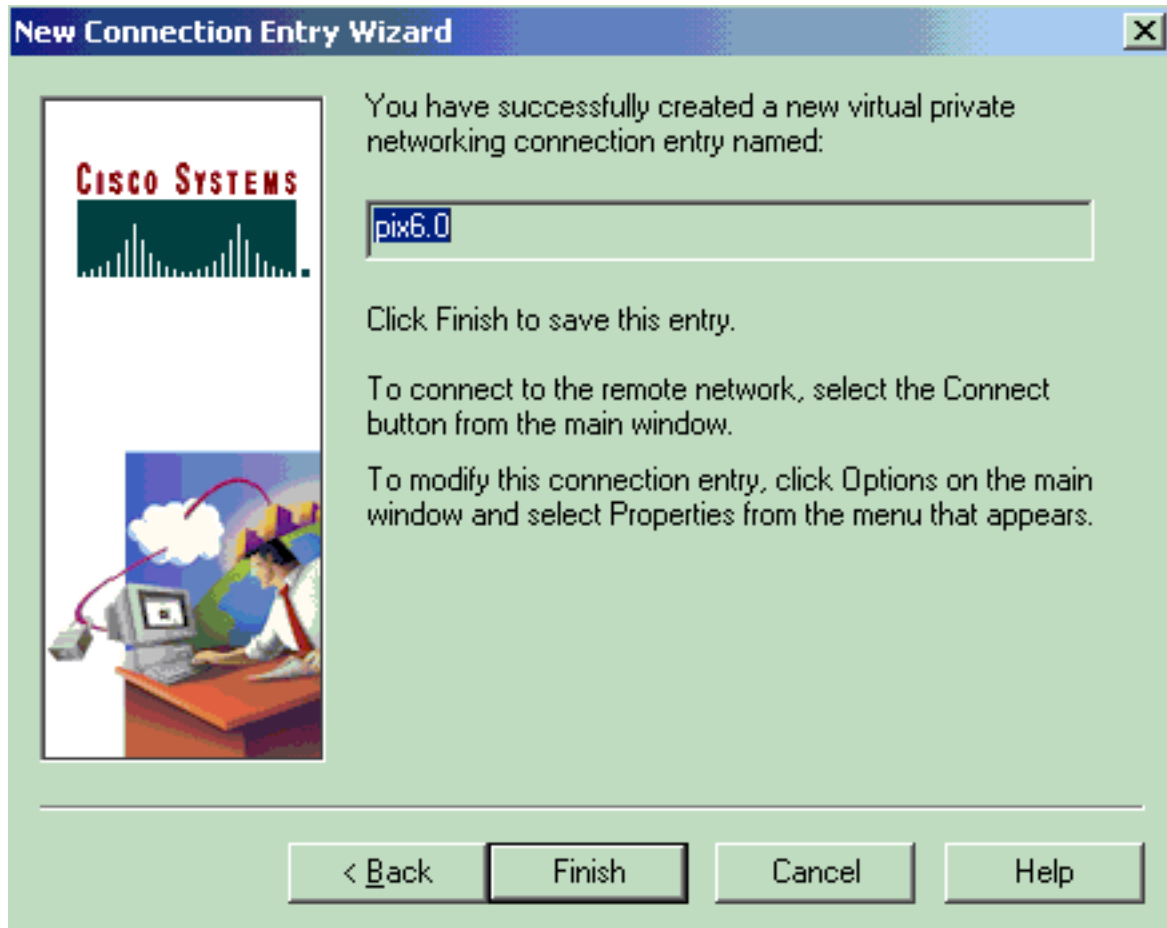
3. 输入 PIX 的公共接口的 IP 地址。



4. 在 **Group Access Information** 下输入组名和组口令。



5. 单击 **Finish** 将配置文件保存在注册表中。

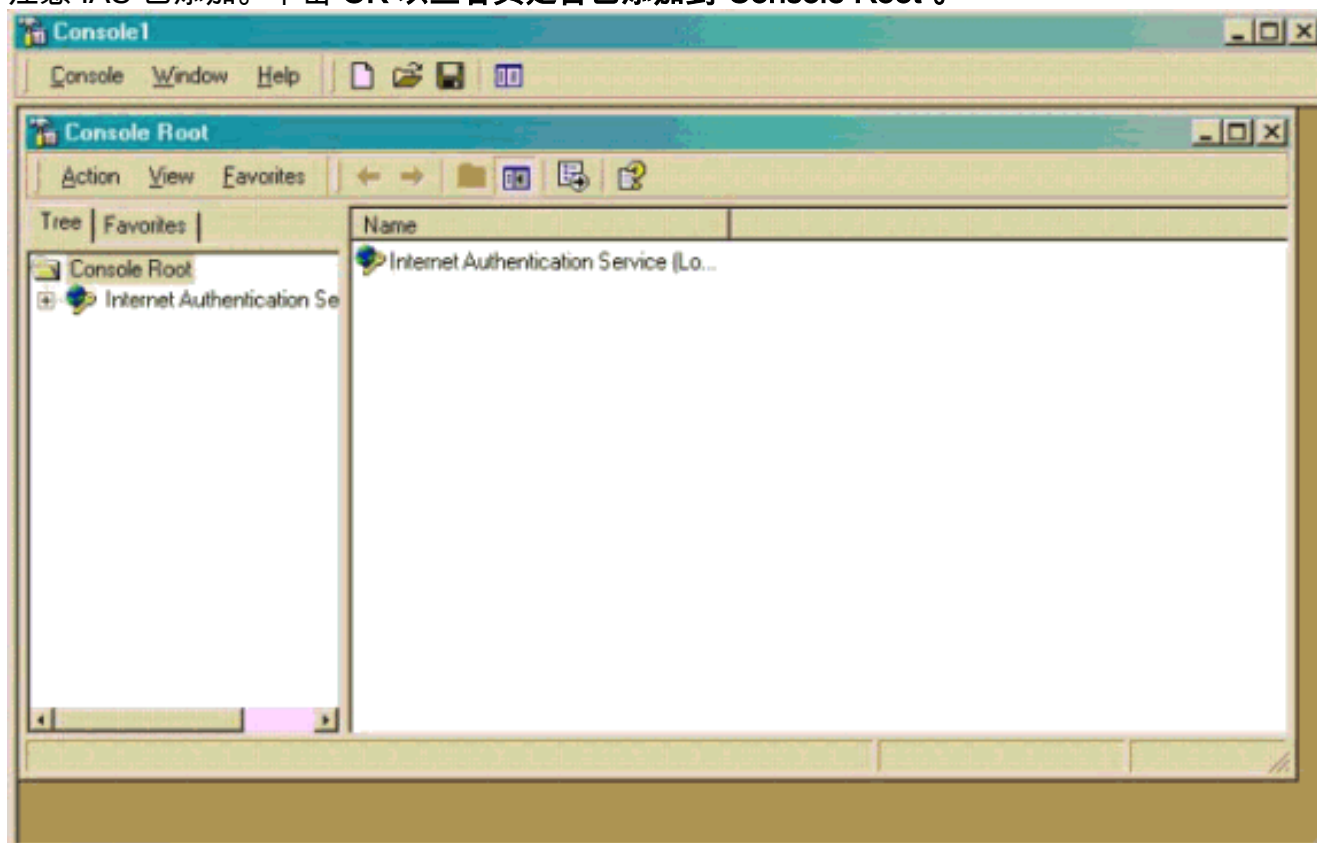


6. 单击 **Connect** 连接到 PIX。

执行以下步骤以配置具有 IAS 的 Microsoft Windows 2000 服务器。这是使用 Windows 2000 IAS 服务器进行 VPN 用户的 RADIUS 认证的非常基本的设置。如果需要更复杂的设计，请与 Microsoft 联系以获得帮助。

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

1. 启动 Microsoft 管理控制台。选择 **Start > Run** 并键入 **mmc**。然后单击 **OK**。
2. 选择控制台 > 添加删除管理单元.....将 IAS 服务添加到此控制台。
3. 单击 **Add** 以启动包含所有可用的独立管理单元的新窗口。单击 **Internet Authentication Service (IAS)** 并单击“Add”。
4. 确保选中 **Local Computer**，然后单击“Finish”。下面单击 **Close**。
5. 注意 IAS 已添加。单击 **OK** 以查看其是否已添加到“Console Root”。



6. 展开 **Internet Authentication Service**，然后右键单击“Clients”。单击 **New Client** 并输入名称。名称的选择其实并不重要；它将是此视图中显示的名称。确保选中 **RADIUS**，然后单击“Next”。
7. 用 IAS 服务器连接的 PIX 接口地址，填写客户端地址。请务必选择 RADIUS 标准，添加共享密钥，以匹配您在 PIX 上输入的命令：

```
aaa-server partnerauth (inside) host 172.18.124.196 cisco123 timeout 5
```

注意：在本例中，“cisco123”是共享密钥。

Add RADIUS Client

Client Information
Specify information regarding the client.

Client address (IP or DNS):
172.18.124.152 Verify...

Client-Vendor:
RADIUS Standard

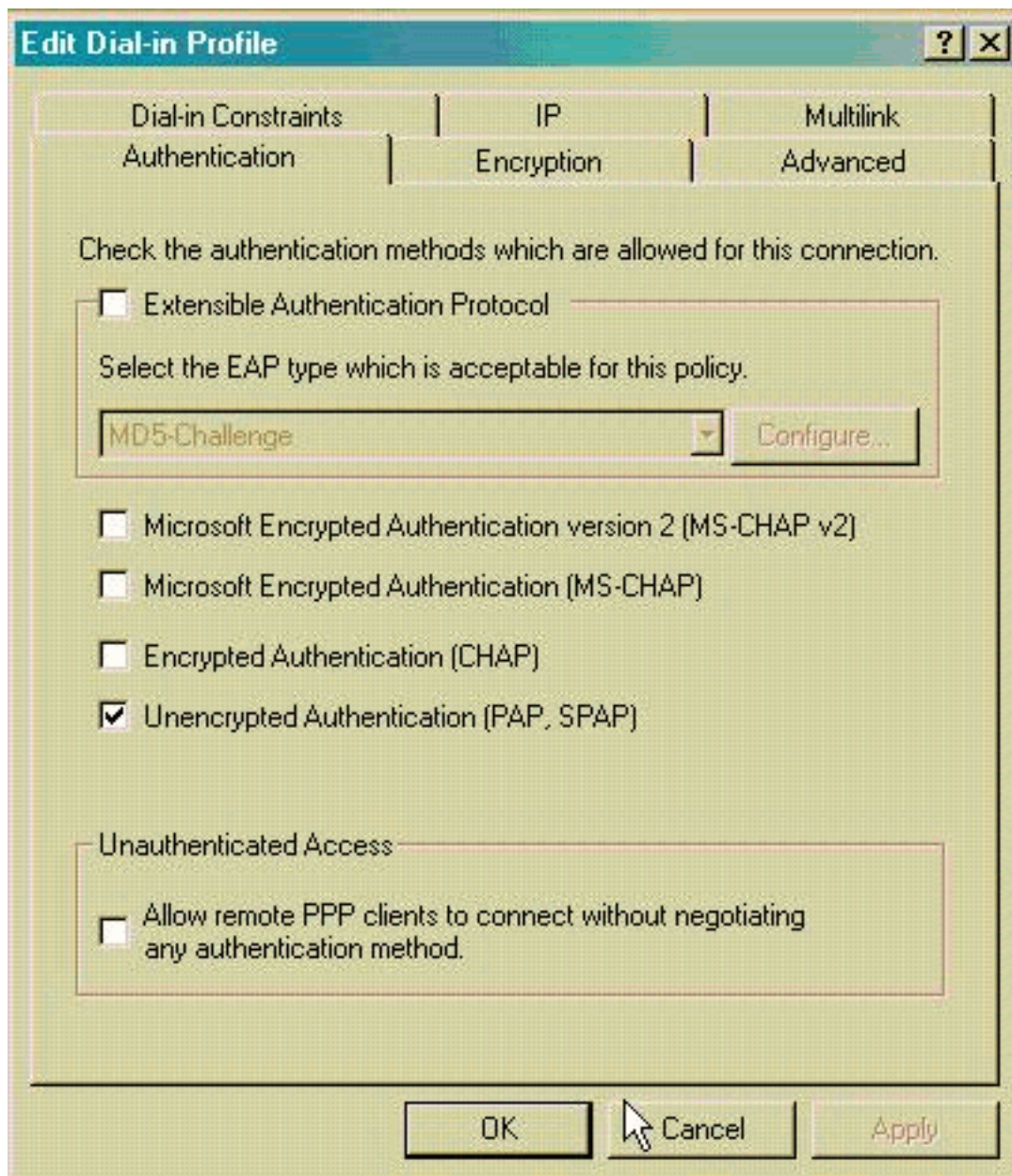
Client must always send the signature attribute in the request

Shared secret: xxxxxxxx

Confirm shared secret: xxxxxxxx

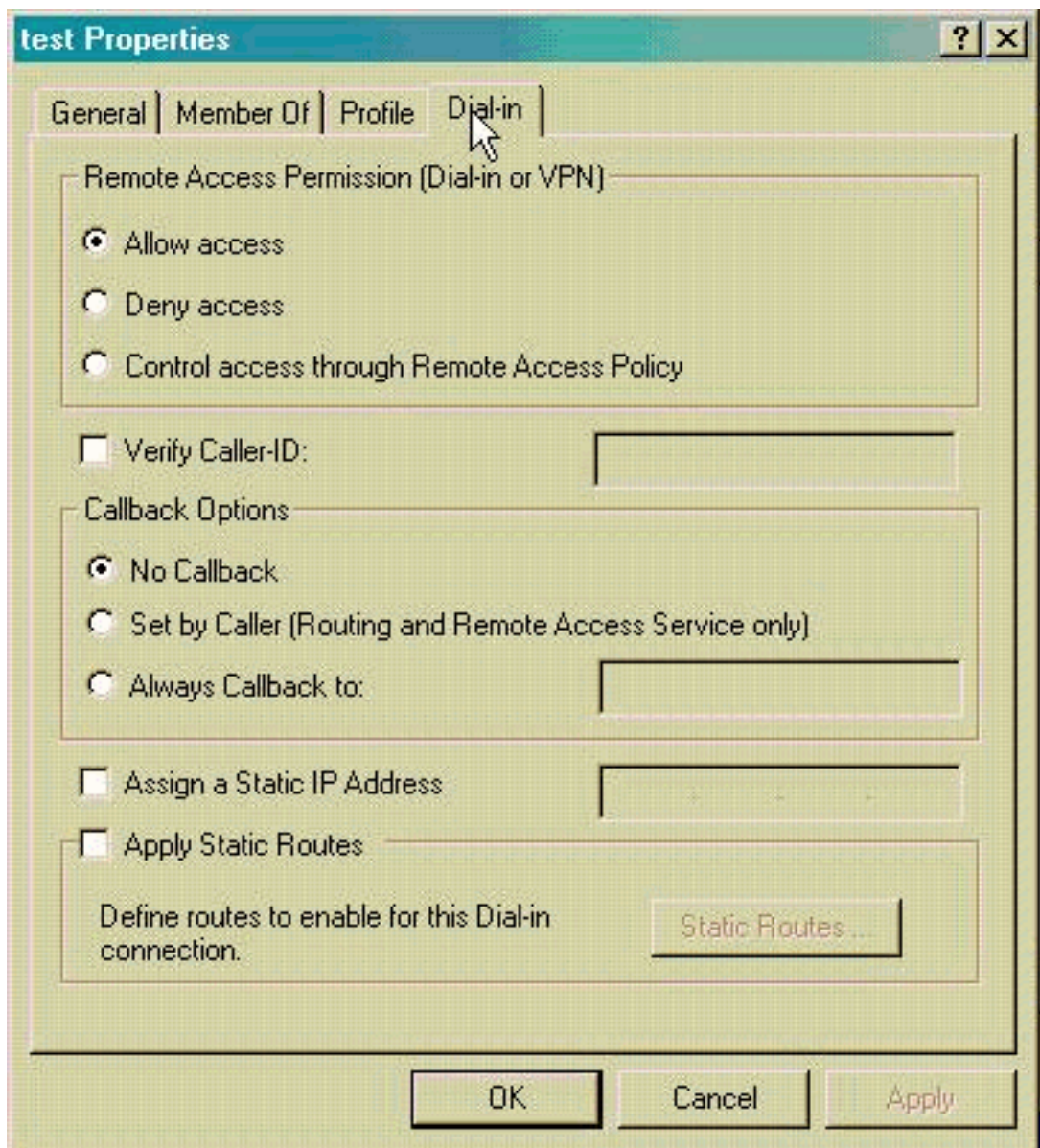
< Back Finish Cancel

8. 单击 **Finish** 返回“Console Root”。
9. 单击左窗格中的 **Remote Access Policies**，然后双击带有“Allow access if dial-in permission is enabled”标签的策略。
10. 单击 **Edit Profile** 并转到“Authentication”选项卡。在 **Authentication Methods** 下，确保仅选中“Unencrypted Authentication (PAP, SPAP)”。**注意**：VPN客户端只能使用此方法进行身份验证。



证。

11. 单击 **Apply**，然后单击“**OK**”两次。
12. 为修改用户以允许连接，请选择 **Console > Add/Remove Snap-in**。单击 **Add**，然后选择“**Local Users and Groups**”管理单元。单击 **Add**。确保选中 **Local Computer**，然后单击“**Finish**”。Click **OK**。
13. 展开 **Local User and Groups**，然后单击左窗格中的“**Users**”文件夹。在右窗格中，双击要允许其访问的用户。
14. 单击“**Dial-in**”选项卡，然后在“**Remote Access Permission (Dial-in or VPN)**”下选择 **Allow**



Access。

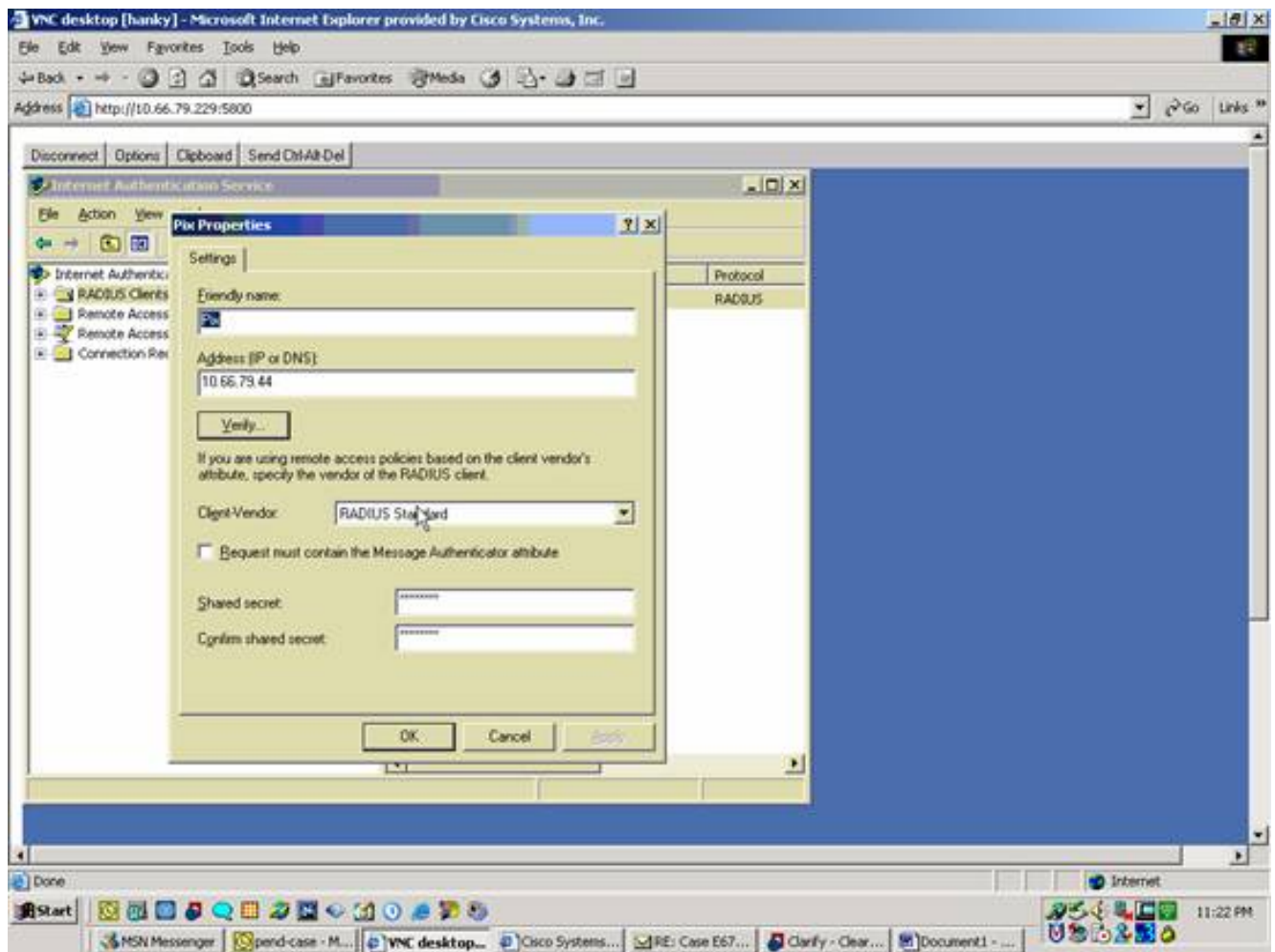
15. 单击 **Apply**，然后单击“**OK**”完成操作。如果需要，可以关闭 **Console Management** 屏幕并保存会话。
16. 您修改的用户现在应该能够使用VPN客户端3.5访问PIX。请记住，IAS服务器仅验证用户信息。组身份验证仍由 PIX 执行。

[具有 IAS 的 Microsoft Windows 2003 服务器](#)

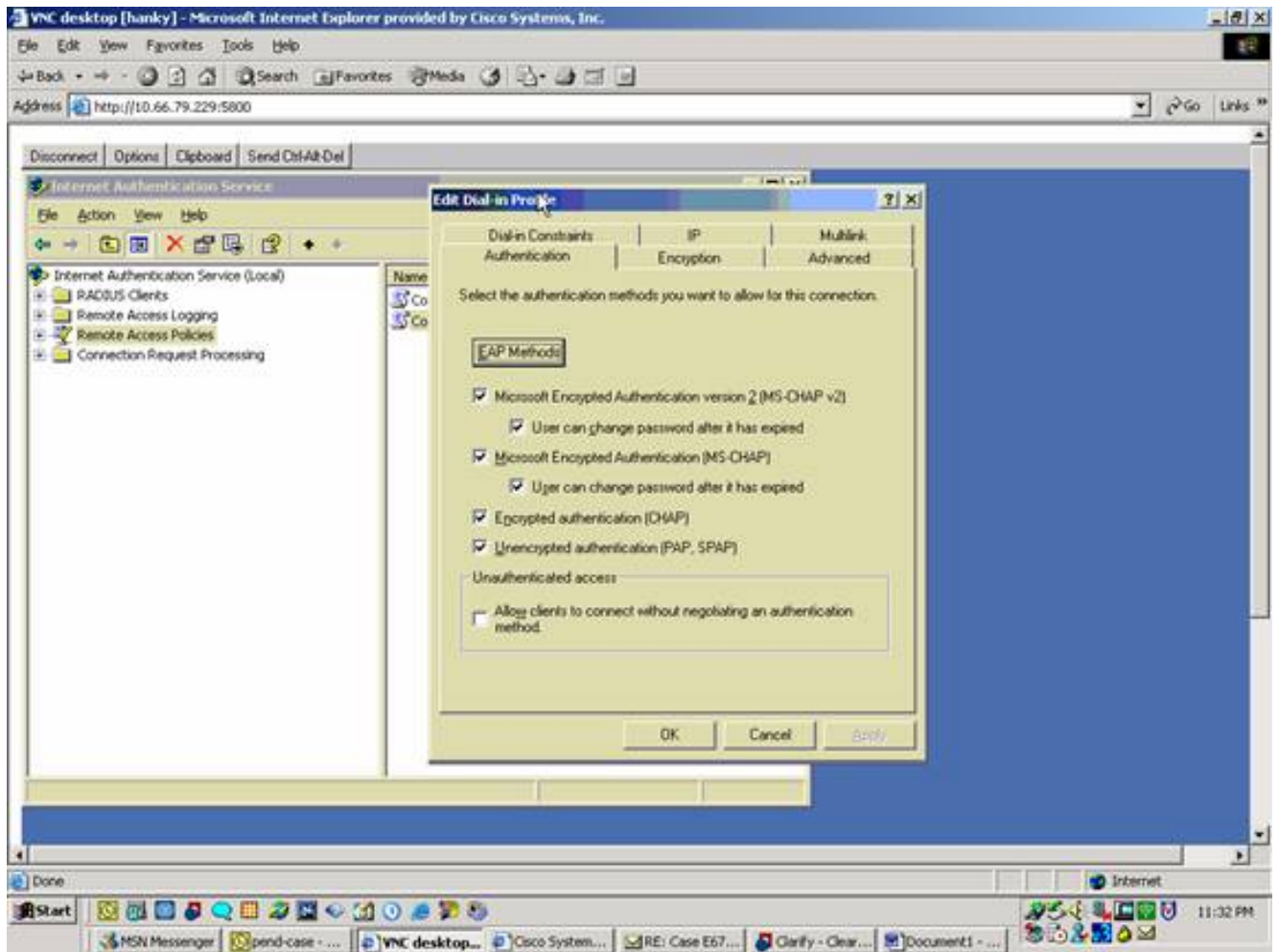
执行以下步骤以配置具有 IAS 的 Microsoft Windows 2003 服务器。

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

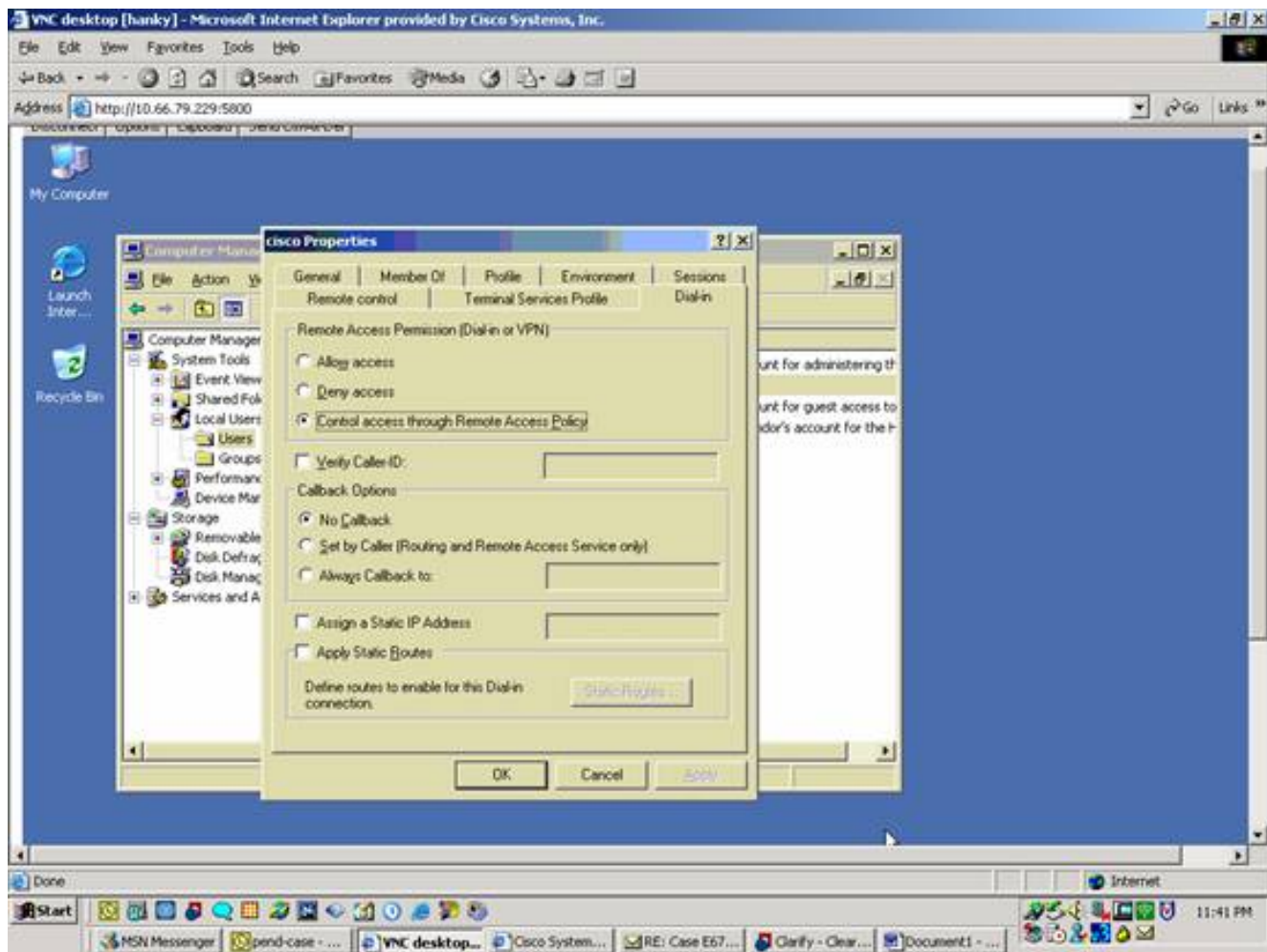
1. 选择 **Administrative Tools > Internet Authentication Service**，然后右键单击 **RADIUS Client** 以添加新的 **RADIUS 客户端**。键入客户端信息后，单击**确定**。此示例显示IP地址为 10.66.79.44的名为“Pix”的客户端。Client-Vendor设置为RADIUS Standard，共享密钥为“cisco123”。



2. 转至 **Remote Access Policies**，右键单击 **Connections to Other Access Servers**，然后选择 **Properties**。
3. 确保选中授予远程访问权限选项。
4. 单击 **Edit Profile** 并选中下列设置。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. 将一个用户添加到本地计算机帐户。为此，请选择 **Administrative Tools > Computer Management > System Tools > Local Users and Groups**。右键单击 **Users** 并选择“**New Users**”。
6. 使用 Cisco 口令“cisco123”添加用户，并检查以下配置文件信息。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。按 **Dial-in**键，选择 **Allow access** (允许访问) 选项(或通过远程访问策略，保留控制访问的默认设置)。完成后，单击 **确定**。



验证

使用本部分可确认配置能否正常运行。

[命令输出解释程序 \(仅限注册用户 \) \(OIT\) 支持某些 show 命令。](#) 使用 OIT 可查看对 show 命令输出的分析。

- show crypto isakmp sa — 显示对等体上的所有当前 IKE 安全关联 (SA)。
- show crypto ipsec sa — 显示当前安全关联所使用的设置。

故障排除

本部分提供的信息可用于对配置进行故障排除。有关其他信息，请参阅[排除 PIX 故障以便在已建立的 IPsec 隧道中传递数据流。](#)

故障排除命令

输出解释程序工具([仅限注册的客户](#))支持某些命令，它允许您查看show 命令输出的分析。

注意：在使用[debug命令之前](#)，请参阅有关debug命令的重要信息，并参阅IP安全故障排除 — 了解和[使用debug命令](#)。

- debug crypto ipsec — 查看第 2 阶段的 IPsec 协商。

- `debug crypto isakmp` — 查看第 1 阶段的 ISAKMP 协商。
- `debug crypto engine` — 查看已加密的流量。

[调试输出示例](#)

- [PIX 防火墙](#)
- [适用于 Windows 的 VPN 客户端 3.5](#)

[PIX 防火墙](#)

```

pixfirewall(config)#
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
VPN Peer: ISAKMP: Added new peer: ip:14.36.100.55 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:14.36.100.55 Ref cnt incremented to:1
    Total VPN Peers:1
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 5 against priority 10 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      extended auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 6 against priority 10 policy

```

```
ISAKMP: encryption DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: extended auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): remote peer supports dead peer detection

ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to a Unity client

ISAKMP: Created a peer node for 14.36.100.55
ISAKMP (0): ID payload
    next-payload : 10
    type          : 1
    protocol      : 17
    port          : 500
    length        : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_AG exchange
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): processing NOTIFY payload 24578 protocol 1
    spi 0, message ID = 0
ISAKMP (0): processing notify INITIAL_CONTACTIPSEC(key_engine): got
    a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas): delete all SAs shared with 14.36.100.55

ISAKMP (0): SA has been authenticated
return status is IKMP_NO_ERROR
ISAKMP/xauth: request attribute XAUTH_TYPE
ISAKMP/xauth: request attribute XAUTH_USER_NAME
ISAKMP/xauth: request attribute XAUTH_USER_PASSWORD
ISAKMP (0:0): initiating peer config to 14.36.100.55. ID = 3870616596
    (0xe6b4ec14)
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
    message ID = 84
ISAKMP: Config payload CFG_REPLY
return status is IKMP_ERR_NO_RETRANS
ISAKMP (0:0): initiating peer config to 14.36.100.55. ID = 3612718114
    (0xd755b422)
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
    message ID = 60
ISAKMP: Config payload CFG_ACK
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
ISAKMP_TRANSACTION exchange
```



```
ISAKMP (0:0): processing transaction payload from 14.36.100.55.
  message ID = 0
ISAKMP: Config payload CFG_REQUEST
ISAKMP (0:0): checking request:
ISAKMP: attribute    IP4_ADDRESS (1)
ISAKMP: attribute    IP4_NETMASK (2)
ISAKMP: attribute    IP4_DNS (3)
ISAKMP: attribute    IP4_NBNS (4)
ISAKMP: attribute    ADDRESS_EXPIRY (5)
  Unsupported Attr: 5
ISAKMP: attribute    APPLICATION_VERSION (7)
  Unsupported Attr: 7
ISAKMP: attribute    UNKNOWN (28672)
  Unsupported Attr: 28672
ISAKMP: attribute    UNKNOWN (28673)
  Unsupported Attr: 28673
ISAKMP: attribute    UNKNOWN (28674)
ISAKMP: attribute    UNKNOWN (28676)
ISAKMP: attribute    UNKNOWN (28679)
  Unsupported Attr: 28679
ISAKMP: attribute    UNKNOWN (28680)
  Unsupported Attr: 28680
ISAKMP: attribute    UNKNOWN (28677)
  Unsupported Attr: 28677
ISAKMP (0:0): responding to peer config from 14.36.100.55.
  ID = 3979868003
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 1527320241

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-MD5
ISAKMP:    encaps is 1
ISAKMP:    SA life type in seconds
ISAKMP:    SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
  IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDED proposal (1)
ISAKMP : Checking IPsec proposal 2

ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-SHA
ISAKMP:    encaps is 1
ISAKMP:    SA life type in seconds
ISAKMP:    SA life duration (VPI) of  0x0 0x20 0xc4 0x9b
  IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDED proposal (2)
ISAKMP : Checking IPsec proposal 3

ISAKMP: transform 1, ESP_3DES
ISAKMP:  attributes in transform:
ISAKMP:    authenticator is HMAC-MD5
```

ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 1) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPsec proposal 4

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans
3, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP : Checking IPsec proposal 5

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.
ISAKMP (0): bad SPI size of 2 octets!
ISAKMP : Checking IPsec proposal 6

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-SHA
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
IPSEC(validate_proposal): transform proposal (prot 3, trans
2, hmac_alg 2) not supported

ISAKMP (0): atts not acceptable. Next payload is 0
ISAKMP (0): skipping next ANDED proposal (6)
ISAKMP : Checking IPsec proposal 7

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (VPI) of 0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
proposal part #1,
(key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
dest_proxy= 14.36.100.50/255.255.255.255/0/0 (type=1),
src_proxy= 10.1.2.1/255.255.255.255/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 1527320241

ISAKMP (0): processing ID payload. message ID = 1527320241
ISAKMP (0): ID_IPV4_ADDR src 10.1.2.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 1527320241

```
ISAKMP (0): ID_IPV4_ADDR dst 14.36.100.50 prot 0 port
  0IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xf39c2217(4087095831) for SA
  from 14.36.100.55 to 14.36.100.50 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 3487980779

ISAKMP : Checking IPsec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: authenticator is HMAC-MD5
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPsec SAs
  inbound SA from 14.36.100.55 to 14.36.100.50
    (proxy 10.1.2.1 to 14.36.100.50)
  has spi 4087095831 and conn_id 1 and flags 4
  lifetime of 2147483 seconds
  outbound SA from 14.36.100.50 to 14.36.100.55
    (proxy 14.36.100.50 to 10.1.2.1)
  has spi 1929305241 and conn_id 2 and flags 4
  lifetime of 2147483 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
  dest_proxy= 14.36.100.50/0.0.0.0/0/0 (type=1),
  src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 2147483s and 0kb,
  spi= 0xf39c2217(4087095831), conn_id= 1, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 14.36.100.50, dest= 14.36.100.55,
  src_proxy= 14.36.100.50/0.0.0.0/0/0 (type=1),
  dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
  protocol= ESP, transform= esp-des esp-md5-hmac ,
  lifedur= 2147483s and 0kb,
  spi= 0x72fedc99(1929305241), conn_id= 2, keysize= 0, flags= 0x4

VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:2
  Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:3
  Total VPN Peers:1
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPsec SAs
  inbound SA from 14.36.100.55 to 14.36.100.50
    (proxy 10.1.2.1 to 0.0.0.0)
  has spi 1791135440 and conn_id 3 and flags 4
  lifetime of 2147483 seconds
  outbound SA from 14.36.100.50 to 14.36.100.55
    (proxy 0.0.0.0 to 10.1.2.1)
  has spi 173725574 and conn_id 4 and flags 4
  lifetime of 2147483 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
```

```
(key eng. msg.) dest= 14.36.100.50, src= 14.36.100.55,
dest_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
src_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 2147483s and 0kb,
spi= 0x6ac28ed0(1791135440), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 14.36.100.50, dest= 14.36.100.55,
src_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
dest_proxy= 10.1.2.1/0.0.0.0/0/0 (type=1),
protocol= ESP, transform= esp-des esp-md5-hmac ,
lifedur= 2147483s and 0kb,
spi= 0xa5ad786(173725574), conn_id= 4, keysize= 0, flags= 0x4
```

```
VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:4
Total VPN Peers:1
```

```
VPN Peer: IPSEC: Peer ip:14.36.100.55 Ref cnt incremented to:5
Total VPN Peers:1
```

```
return status is IKMP_NO_ERROR
```

```
crypto_isakmp_process_block: src 14.36.100.55, dest 14.36.100.50
```

```
ISAKMP (0): processing NOTIFY payload 36136 protocol 1
```

```
spi 0, message ID = 3443334051
```

```
ISAKMP (0): received DPD_R_U_THERE from peer 14.36.100.55
```

```
ISAKMP (0): sending NOTIFY message 36137 protocol 1
```

```
return status is IKMP_NO_ERR_NO_TRANS
```

[适用于 Windows 的 VPN 客户端 3.5](#)

```
193 19:00:56.073 01/24/02 Sev=Info/6 DIALER/0x63300002
Initiating connection.
```

```
194 19:00:56.073 01/24/02 Sev=Info/4 CM/0x63100002
Begin connection process
```

```
195 19:00:56.083 01/24/02 Sev=Info/4 CM/0x63100004
Establish secure connection using Ethernet
```

```
196 19:00:56.083 01/24/02 Sev=Info/4 CM/0x63100026
Attempt connection with server "14.36.100.50"
```

```
197 19:00:56.083 01/24/02 Sev=Info/6 IKE/0x6300003B
Attempting to establish a connection with 14.36.100.50.
```

```
198 19:00:56.124 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID)
to 14.36.100.50
```

```
199 19:00:56.774 01/24/02 Sev=Info/4 IPSEC/0x63700014
Deleted all keys
```

```
200 19:00:59.539 01/24/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50
```

```
201 19:00:59.539 01/24/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK AG (SA, VID, VID, VID, KE, ID, NON, HASH)
from 14.36.100.50
```

```
202 19:00:59.539 01/24/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100
```

```
203 19:00:59.539 01/24/02 Sev=Info/5 IKE/0x63000001
Peer is a Cisco-Unity compliant peer
```

204 19:00:59.539 01/24/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100

205 19:00:59.539 01/24/02 Sev=Info/5 IKE/0x63000001
Peer supports DPD

206 19:00:59.539 01/24/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 6D761DDC26ACECA1B0ED11FABBB860C4

207 19:00:59.569 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT)
to 14.36.100.50

208 19:00:59.569 01/24/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

209 19:00:59.569 01/24/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

210 19:00:59.569 01/24/02 Sev=Info/4 CM/0x63100015
Launch xAuth application

211 19:01:04.236 01/24/02 Sev=Info/4 CM/0x63100017
xAuth application returned

212 19:01:04.236 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

213 19:01:04.496 01/24/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

214 19:01:04.496 01/24/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

215 19:01:04.496 01/24/02 Sev=Info/4 CM/0x6310000E
Established Phase 1 SA. 1 Phase 1 SA in the system

216 19:01:04.506 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

217 19:01:04.516 01/24/02 Sev=Info/5 IKE/0x6300005D
Client sending a firewall request to concentrator

218 19:01:04.516 01/24/02 Sev=Info/5 IKE/0x6300005C
Firewall Policy: Product=Cisco Integrated Client, Capability=
(Centralized Policy Push).

219 19:01:04.516 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 14.36.100.50

220 19:01:04.586 01/24/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

221 19:01:04.586 01/24/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 14.36.100.50

222 19:01:04.586 01/24/02 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: ,
value = 10.1.2.1

223 19:01:04.586 01/24/02 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): ,
value = 10.1.1.2

224 19:01:04.586 01/24/02 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS)
: , value = 10.1.1.2

225 19:01:04.586 01/24/02 Sev=Info/5 IKE/0x6300000E
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_DEFDOMAIN: ,
value = cisco.com

226 19:01:04.586 01/24/02 Sev=Info/4 CM/0x63100019
Mode Config data received

227 19:01:04.606 01/24/02 Sev=Info/5 IKE/0x63000055
Received a key request from Driver for IP address 14.36.100.50,
GW IP = 14.36.100.50

228 19:01:04.606 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 14.36.100.50

229 19:01:04.606 01/24/02 Sev=Info/5 IKE/0x63000055
Received a key request from Driver for IP address 10.10.10.255,
GW IP = 14.36.100.50

230 19:01:04.606 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 14.36.100.50

231 19:01:04.786 01/24/02 Sev=Info/4 IPSEC/0x63700014
Deleted all keys

232 19:01:05.948 01/24/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

233 19:01:05.948 01/24/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 14.36.100.50

234 19:01:05.948 01/24/02 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

235 19:01:05.948 01/24/02 Sev=Info/5 IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

236 19:01:05.948 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 14.36.100.50

237 19:01:05.948 01/24/02 Sev=Info/5 IKE/0x63000058
Loading IPsec SA (Message ID = 0x5B090EB1 OUTBOUND SPI =
0xF39C2217 INBOUND SPI = 0x72FEDC99)

238 19:01:05.948 01/24/02 Sev=Info/5 IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0xF39C2217

239 19:01:05.948 01/24/02 Sev=Info/5 IKE/0x63000026
Loaded INBOUND ESP SPI: 0x72FEDC99

240 19:01:05.948 01/24/02 Sev=Info/4 CM/0x6310001A
One secure connection established

241 19:01:05.988 01/24/02 Sev=Info/6 DIALER/0x63300003
Connection established.

242 19:01:06.078 01/24/02 Sev=Info/6 DIALER/0x63300008
MAPI32 Information - Outlook not default mail client

243 19:01:06.118 01/24/02 Sev=Info/5 IKE/0x6300002F

Received ISAKMP packet: peer = 14.36.100.50

244 19:01:06.118 01/24/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID,
NOTIFY:STATUS_RESP_LIFETIME) from 14.36.100.50

245 19:01:06.118 01/24/02 Sev=Info/5 IKE/0x63000044
RESPONDER-LIFETIME notify has value of 28800 seconds

246 19:01:06.118 01/24/02 Sev=Info/5 IKE/0x63000045
RESPONDER-LIFETIME notify has value of 4608000 kb

247 19:01:06.118 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK QM *(HASH) to 14.36.100.50

248 19:01:06.118 01/24/02 Sev=Info/5 IKE/0x63000058
Loading IPsec SA (Message ID = 0xCFE65CEB OUTBOUND SPI =
0x6AC28ED0 INBOUND SPI = 0x0A5AD786)

249 19:01:06.118 01/24/02 Sev=Info/5 IKE/0x63000025
Loaded OUTBOUND ESP SPI: 0x6AC28ED0

250 19:01:06.118 01/24/02 Sev=Info/5 IKE/0x63000026
Loaded INBOUND ESP SPI: 0x0A5AD786

251 19:01:06.118 01/24/02 Sev=Info/4 CM/0x63100022
Additional Phase 2 SA established.

252 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

253 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0x17229cf3 into key list

254 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

255 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0x99dcfe72 into key list

256 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

257 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0xd08ec26a into key list

258 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x63700010
Created a new key structure

259 19:01:07.020 01/24/02 Sev=Info/4 IPSEC/0x6370000F
Added key with SPI=0x86d75a0a into key list

260 19:01:15.032 01/24/02 Sev=Info/6 IKE/0x6300003D
Sending DPD request to 14.36.100.50, seq# = 152233542

261 19:01:15.032 01/24/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST)
to 14.36.100.50

262 19:01:15.032 01/24/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 14.36.100.50

263 19:01:15.032 01/24/02 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:DPD_ACK)

from 14.36.100.50

264 19:01:15.032 01/24/02 Sev=Info/5 IKE/0x6300003F
Received DPD ACK from 14.36.100.50, seq# received = 152233542,
seq# expected = 152233542

[相关信息](#)

- [PIX 支持页](#)
- [PIX 命令参考](#)
- [RADIUS 支持页](#)
- [Cisco VPN 3000 系列集中器支持页](#)
- [Cisco VPN 3000 系列客户端支持页](#)
- [IPsec 协商/IKE 协议支持页](#)
- [请求注解 \(RFC\)](#)
- [技术支持 - Cisco Systems](#)