ASA/PIX：带有用于 VPN 客户端流量的入站 NAT 的远程 VPN 服务器（带有 CLI 和 ASDM）配置示例

目录

简介

本文档介绍了如何使用自适应安全设备管理器 (ASDM) 或 CLI 将 Cisco 5500 系列自适应安全设备 (ASA) 配置为充当远程 VPN 服务器，以及如何将 NAT 配置为入站 VPN 客户端流量。ASDM 通过一个直观且易于使用的基于 Web 的管理界面提供一流的安全管理和监控。完成 Cisco ASA 配置后，可以使用 Cisco VPN 客户端对其进行验证。

先决条件

要求

本文档假设 ASA 处于完全运行状态，并配置为允许 Cisco ASDM 或 CLI 进行配置更改。此外，也假设要对 ASA 进行配置，使之适用于出站 NAT。有关如何配置出站 NAT 的详细信息，请参阅允许内部主机使用 PAT 访问外部网络。

注意： 请参阅允许对 ASDM 进行 HTTPS 访问或 PIX/ASA 7.x：内部和外部接口上的 SSH 配置示例以允许通过 ASDM 或Secure Shell (SSH) 远程对设备进行配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco可适应安全工具软件版本7.x和以上
- 自适应安全设备管理器版本 5.x 及更高版本
- Cisco VPN 客户端 4.x 及更高版本

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

此配置也可用于 Cisco PIX 安全设备版本 7.x 及更高版本。

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

远程访问配置提供对 Cisco VPN 客户端（如移动用户）的安全远程访问。远程访问 VPN 使远程用户可以安全地访问集中的网络资源。Cisco VPN 客户端遵守 IPSec 协议并专门设计为可与安全设备配合使用。但是，安全设备可以与许多协议兼容客户端建立 IPSec 连接。有关 IPSec 的详细信息，请参阅 ASA 配置指南。

组和用户是 VPN 安全管理和安全设备配置中的核心概念。它们指定确定用户访问和使用 VPN 的属性。组是被视为单个实体的用户集合。用户从组策略获得他们的属性。隧道组标识特定连接的组策略。如果没有为用户分配特定组策略，则应用连接的默认组策略。

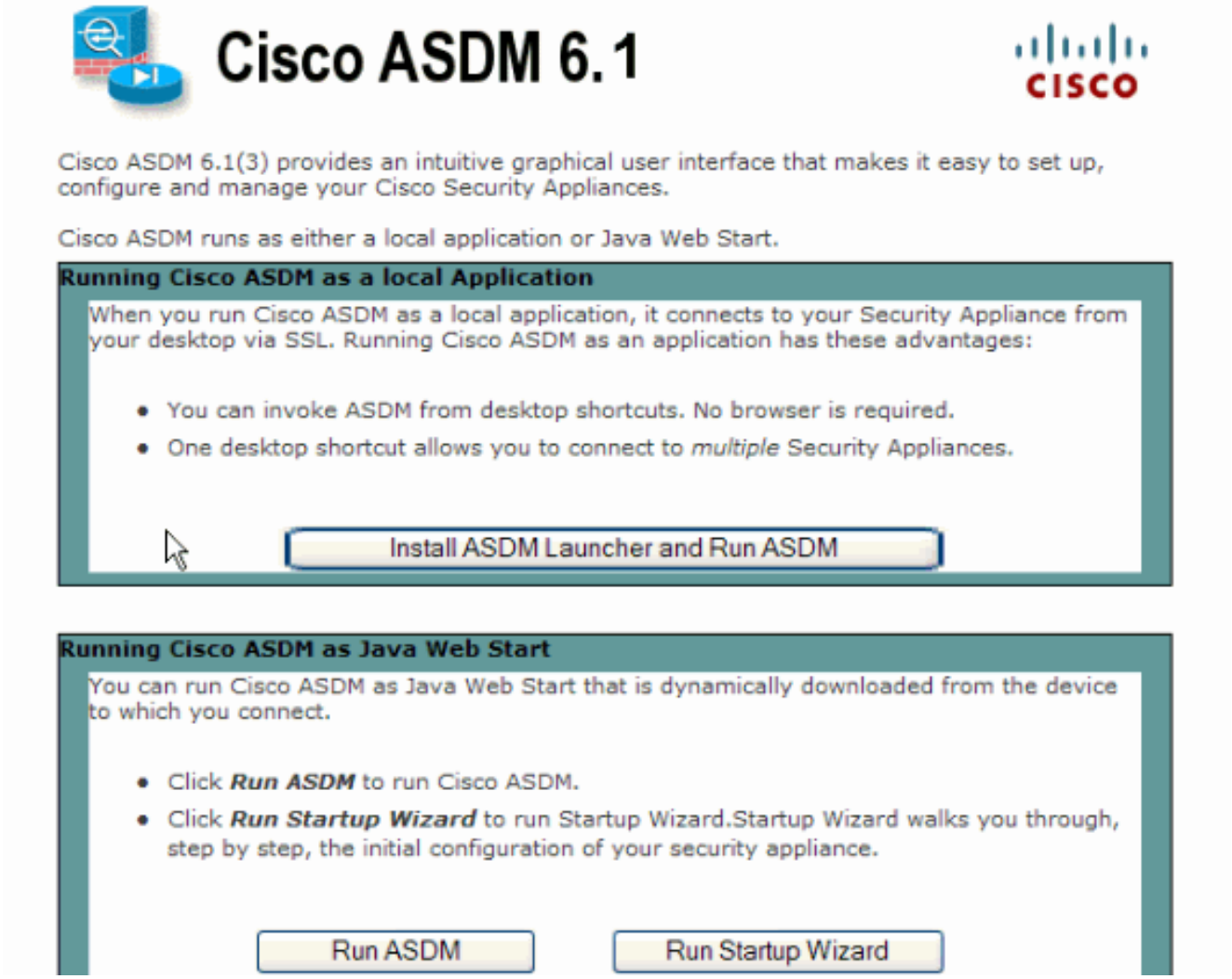
隧道组由确定隧道连接策略的一组记录构成。这些记录标识用于对隧道用户进行身份验证的服务器，以及向其发送连接信息的记帐服务器（如果有）。它们还标识连接的默认组策略，并且它们包含协议特定的连接参数。隧道组包括与隧道自身创建相关的少量属性。隧道组包括指向定义面向用户的属性的组策略的一个指针。

配置

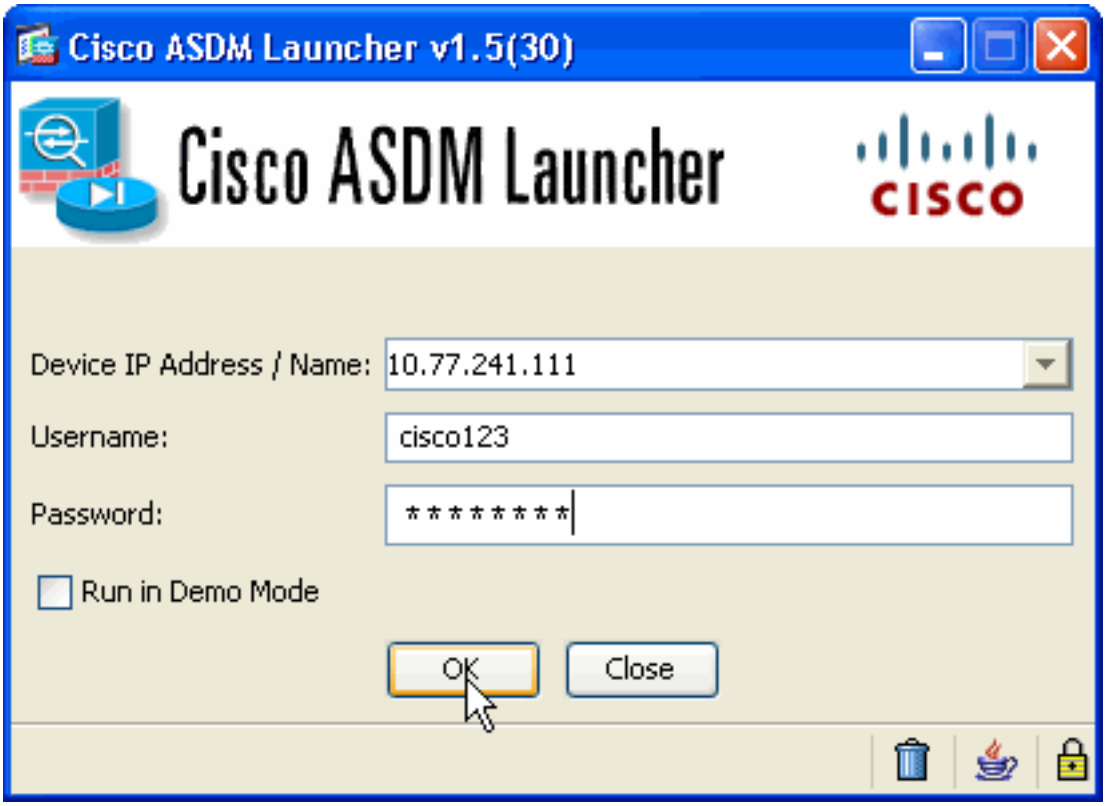
使用 ASDM 将 ASA/PIX 配置为远程 VPN 服务器

要使用 ASDM 将 Cisco ASA 配置为远程 VPN Server，请完成以下步骤：

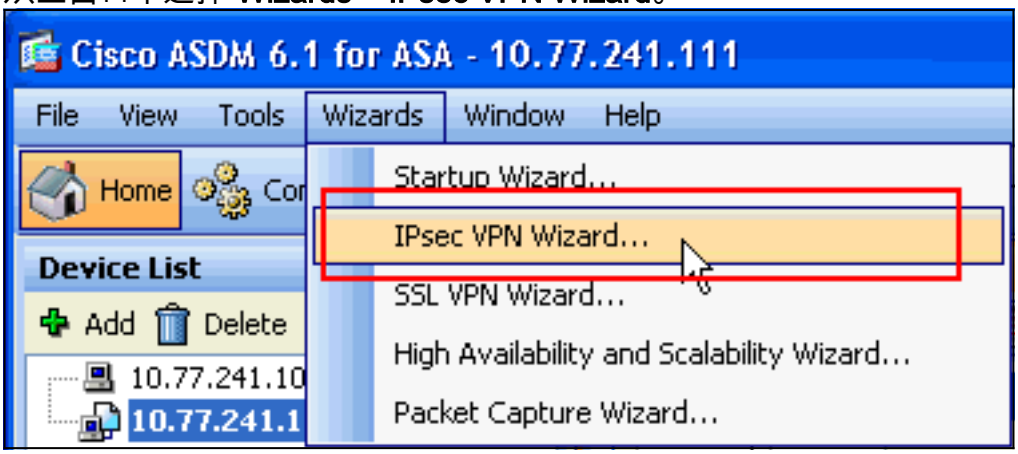
1. 打开浏览器并输入 **https://<为访问 ASDM 而配置的 ASA 接口的 IP 地址>**，以访问 ASA 上的 ASDM。确保核准浏览器提供的有关 SSL 证书真实性的任何警告。默认的用户名和口令均为空。ASA 显示此窗口以允许下载 ASDM 应用程序。此示例将应用程序加载到本地计算机，但不在 Java 小程序中运行。



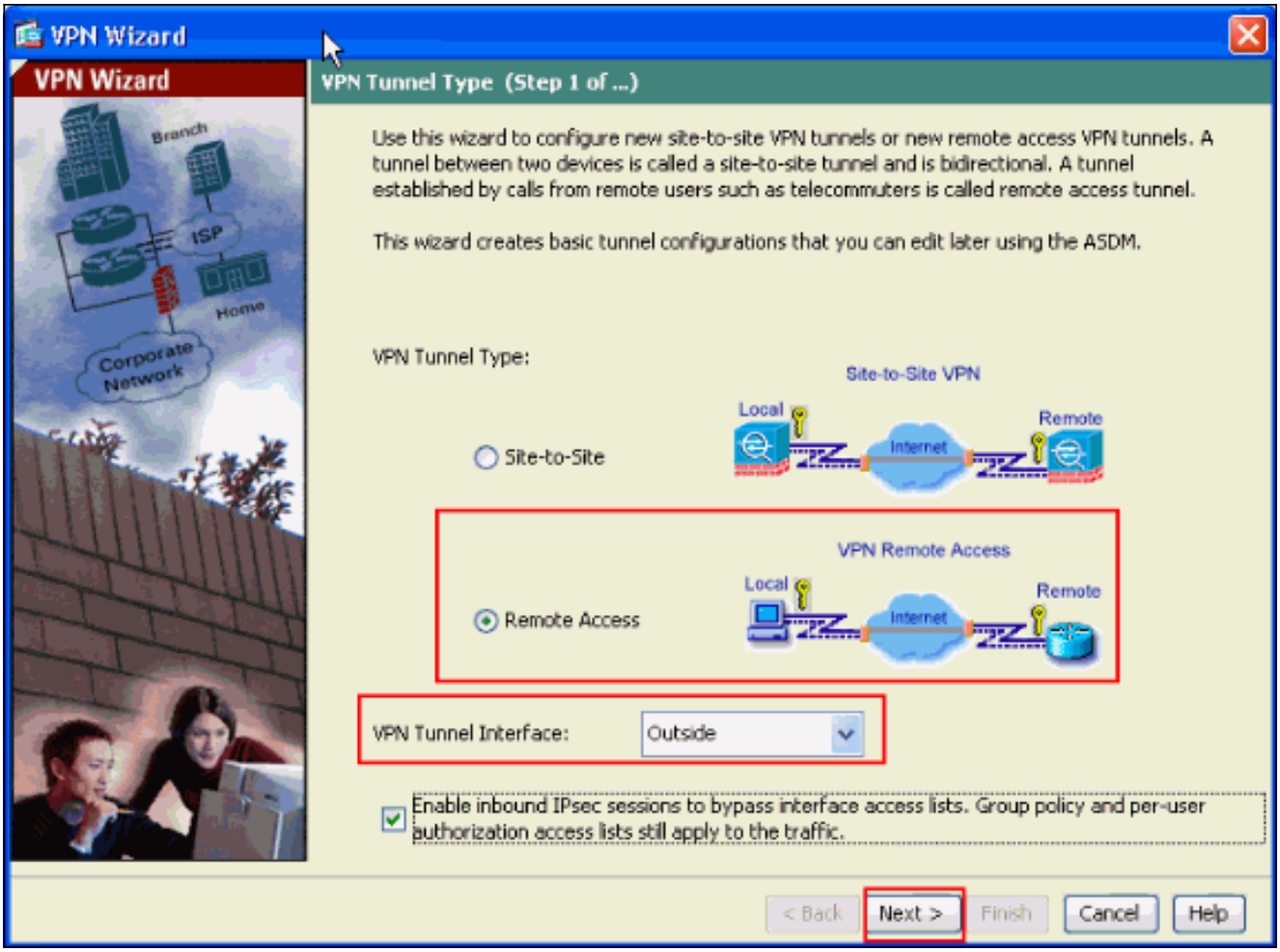
2. 单击 **Download ASDM Launcher and Start ASDM** 以下载 ASDM 应用程序的安装程序。
3. 下载 ASDM 启动程序之后，完成提示所指示的步骤，以便安装该软件并运行 Cisco ASDM 启动程序。
4. 输入使用 **http -** 命令配置的接口的 IP 地址，以及用户名和口令（如果已指定）。此示例使用 **cisco123** 作为用户名，使用 **cisco123** 作为口令。



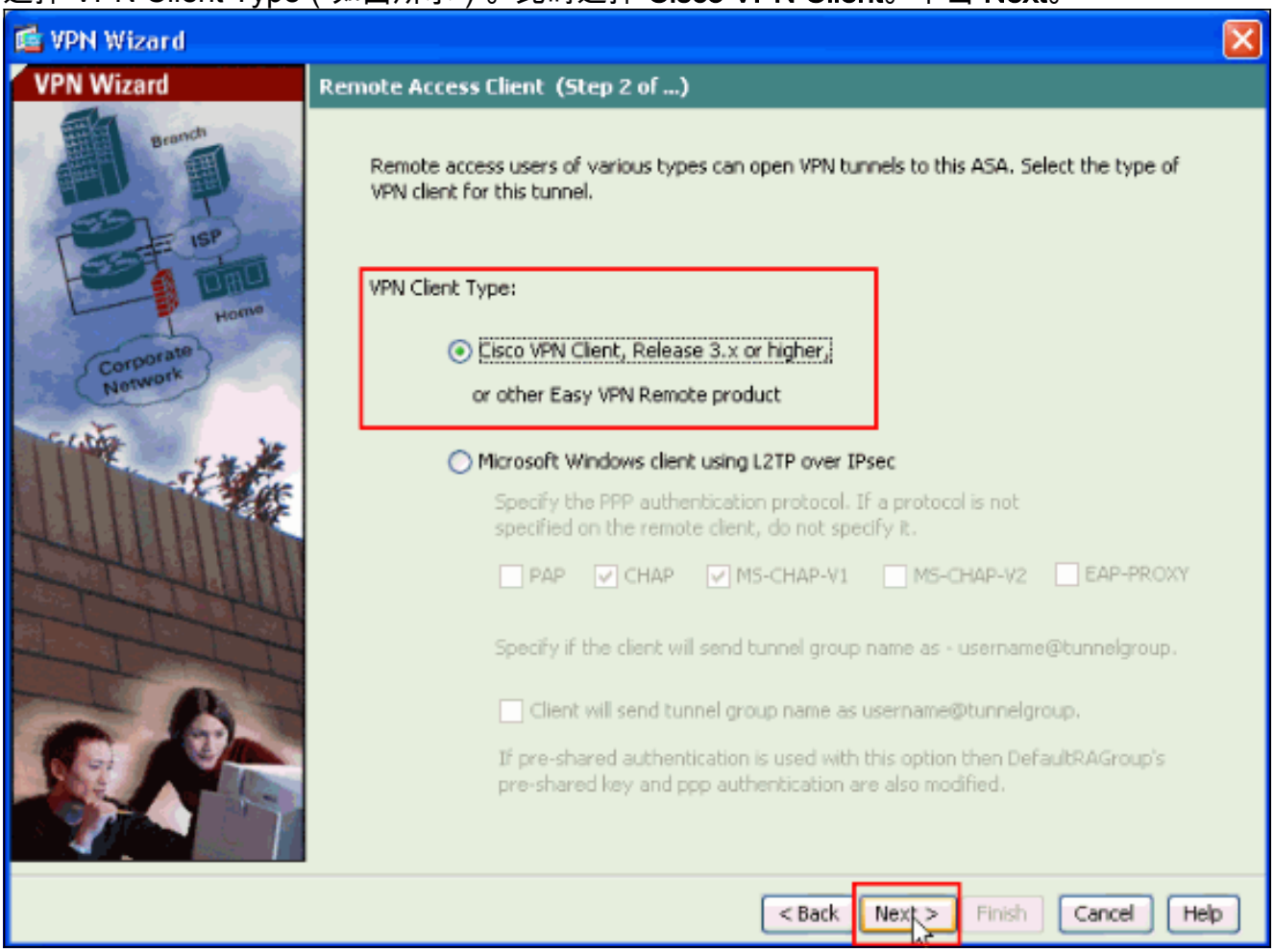
5. 从主窗口中选择 **Wizards > IPsec VPN Wizard**。



6. 选择 **Remote Access VPN** 隧道类型，并确保根据需要设置了 VPN Tunnel Interface，然后单击 **Next**（如图所示）。

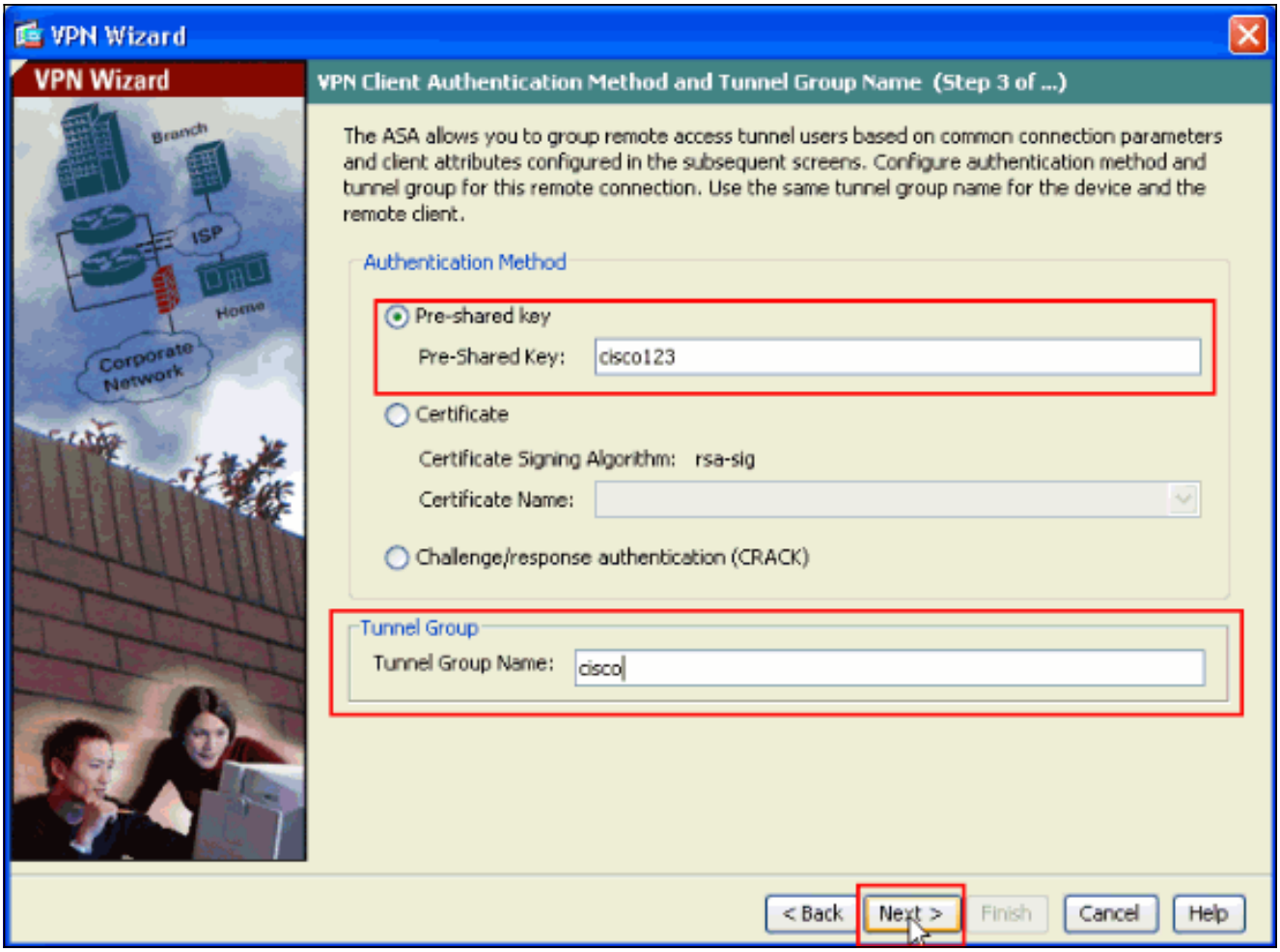


7. 选择 VPN Client Type（如图所示）。此时选择 **Cisco VPN Client**。单击 **Next**。

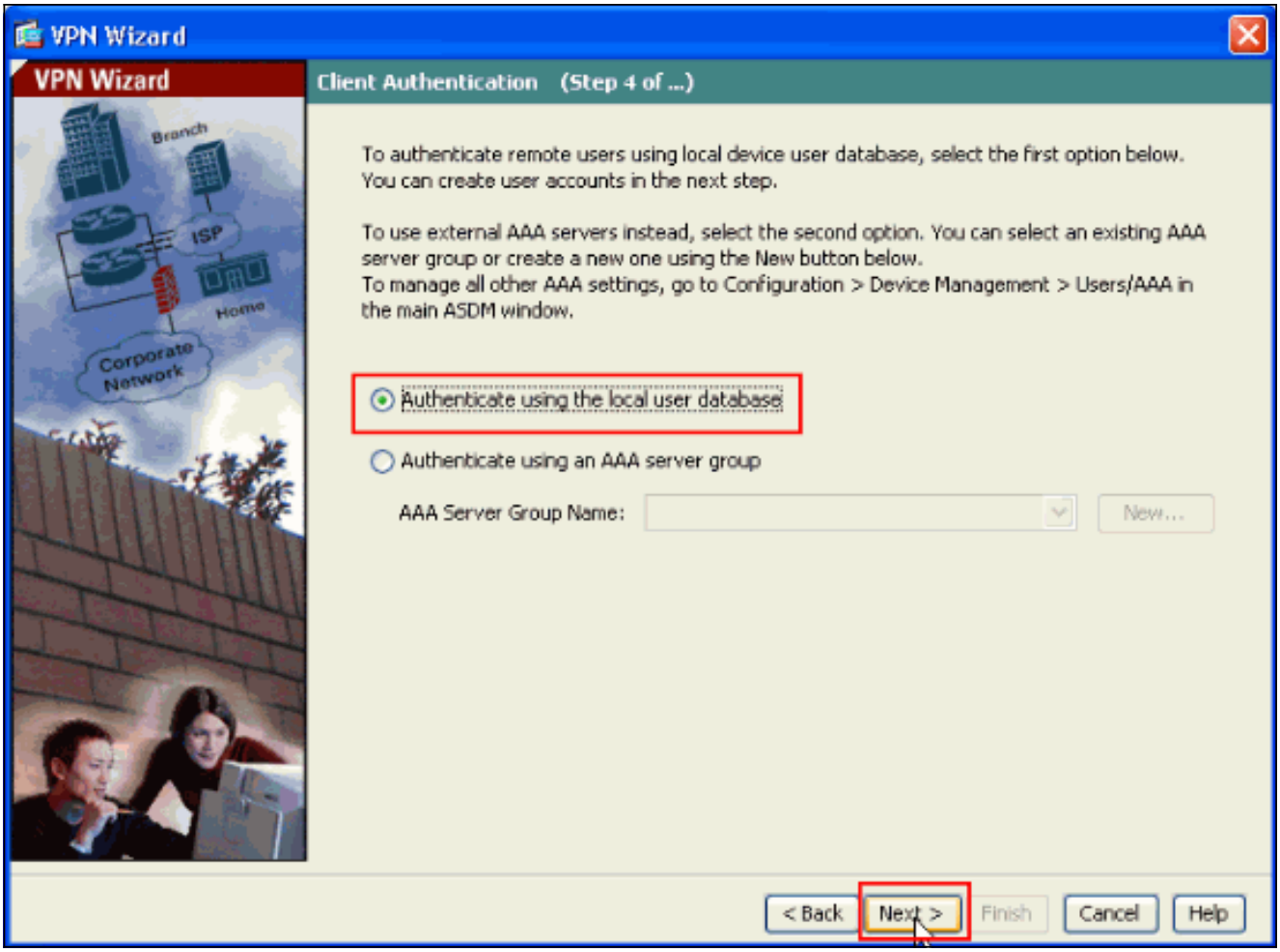


8. 为**Tunnel Group Name**输入名称。输入要使用的身份验证信息，在本示例中是预共享密钥。本

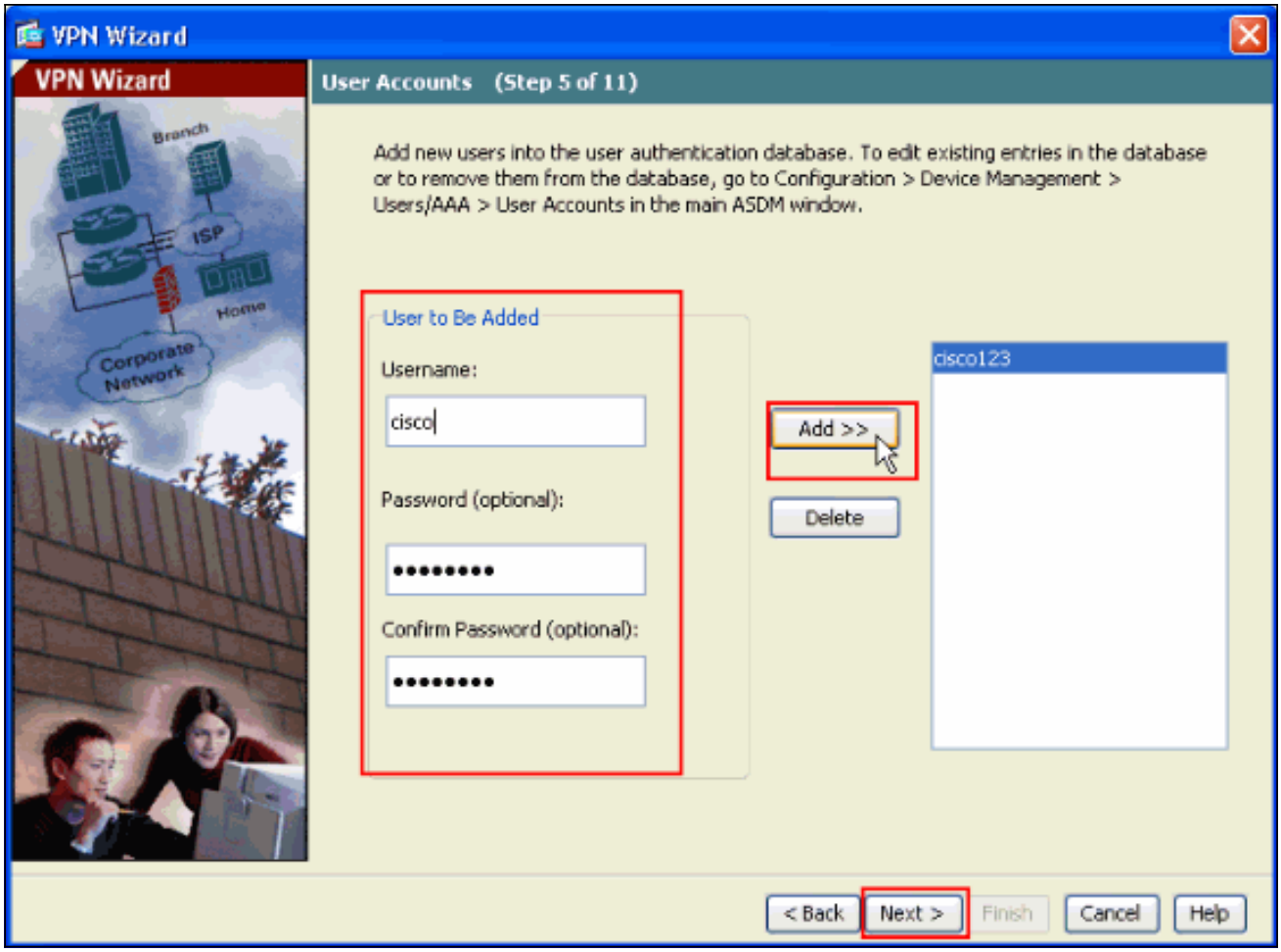
示例中使用的预共享密钥是 **cisco123**。此示例中使用的 Tunnel Group Name 为 **cisco**。单击 **Next**。



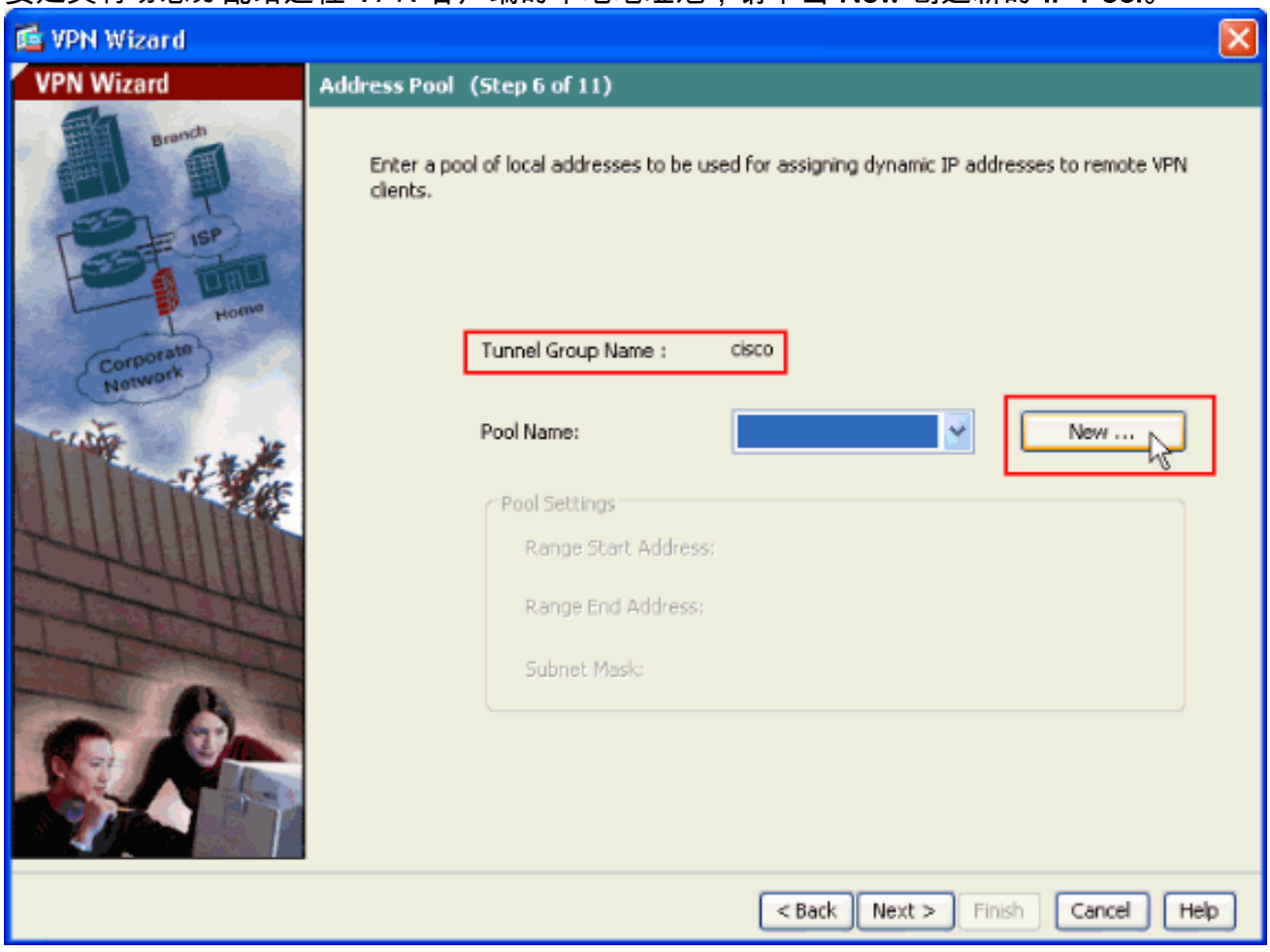
9. 选择是希望使用本地用户数据库对远程用户进行身份验证，还是希望使用外部 AAA 服务器组对远程用户进行身份验证。**注意：** 您将在步骤 10 中将用户添加到本地用户数据库中。**注意：** 有关如何通过 ASDM 配置外部 AAA 服务器组的信息，请参阅 [PIX/ASA 7.x 的通过 ASDM 为 VPN 用户配置身份验证和授权服务器组的配置示例]。



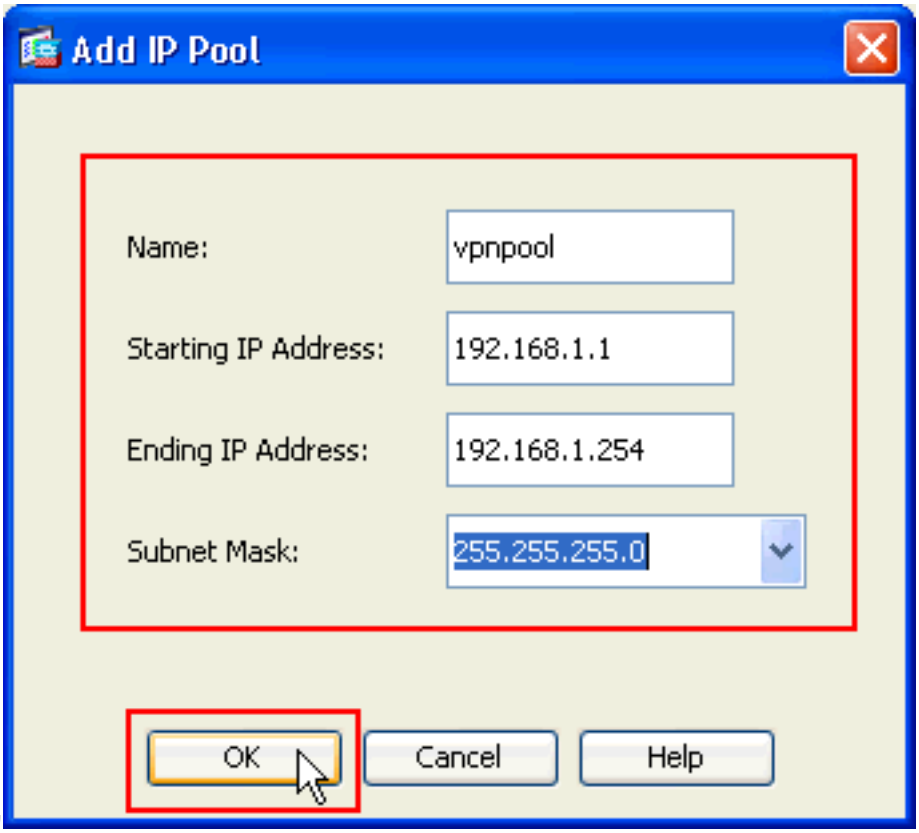
10. 提供 **Username** 和可选的 **Password** ，然后单击 **Add** 将新用户添加到用户认证数据库中。单击 **Next**。**注意**： 请不要从此窗口中删除现有用户。在 ASDM 主窗口中选择 **Configuration > Device Management > Users/AAA > User Accounts**，以编辑数据库中的现有条目或将其从数据库中删除。



11. 要定义将动态分配给远程 VPN 客户端的本地地址池，请单击 **New** 创建新的 **IP Pool**。

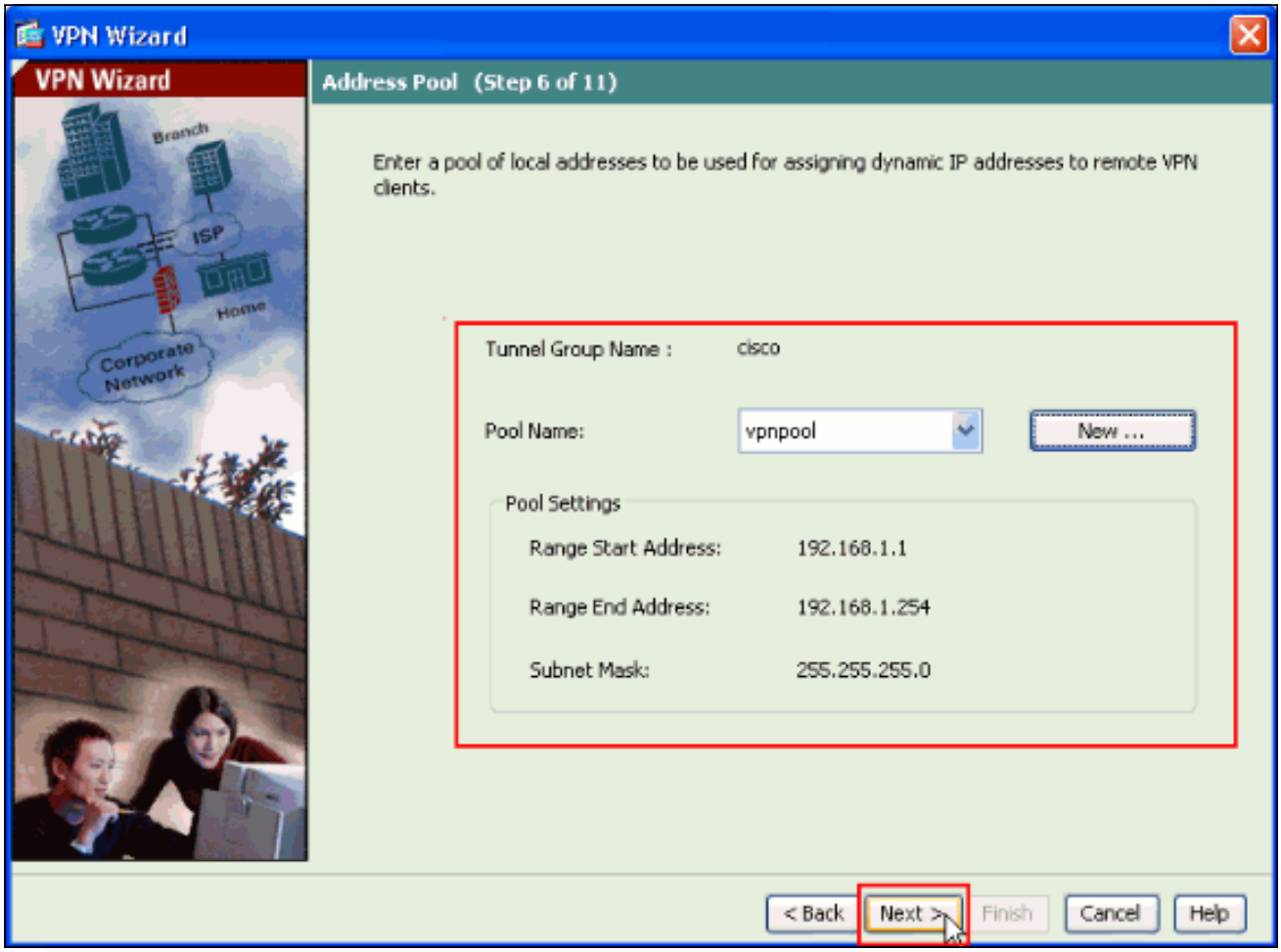


12. 在名为 **Add IP Pool** 的新窗口中，请提供以下信息，然后单击 **OK**。**IP 池的名称起始 IP 地址**

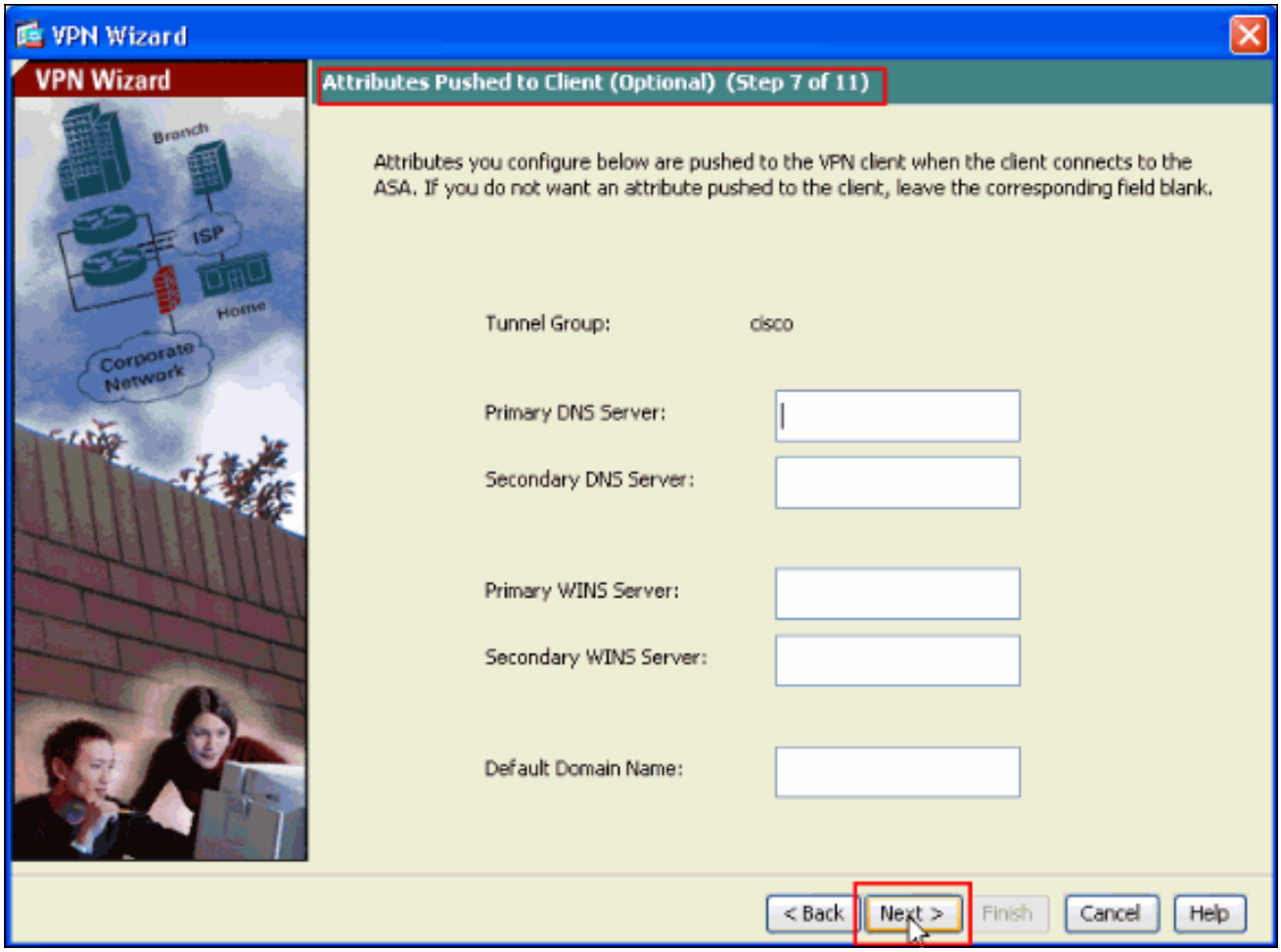


终止 IP 地址子网掩码

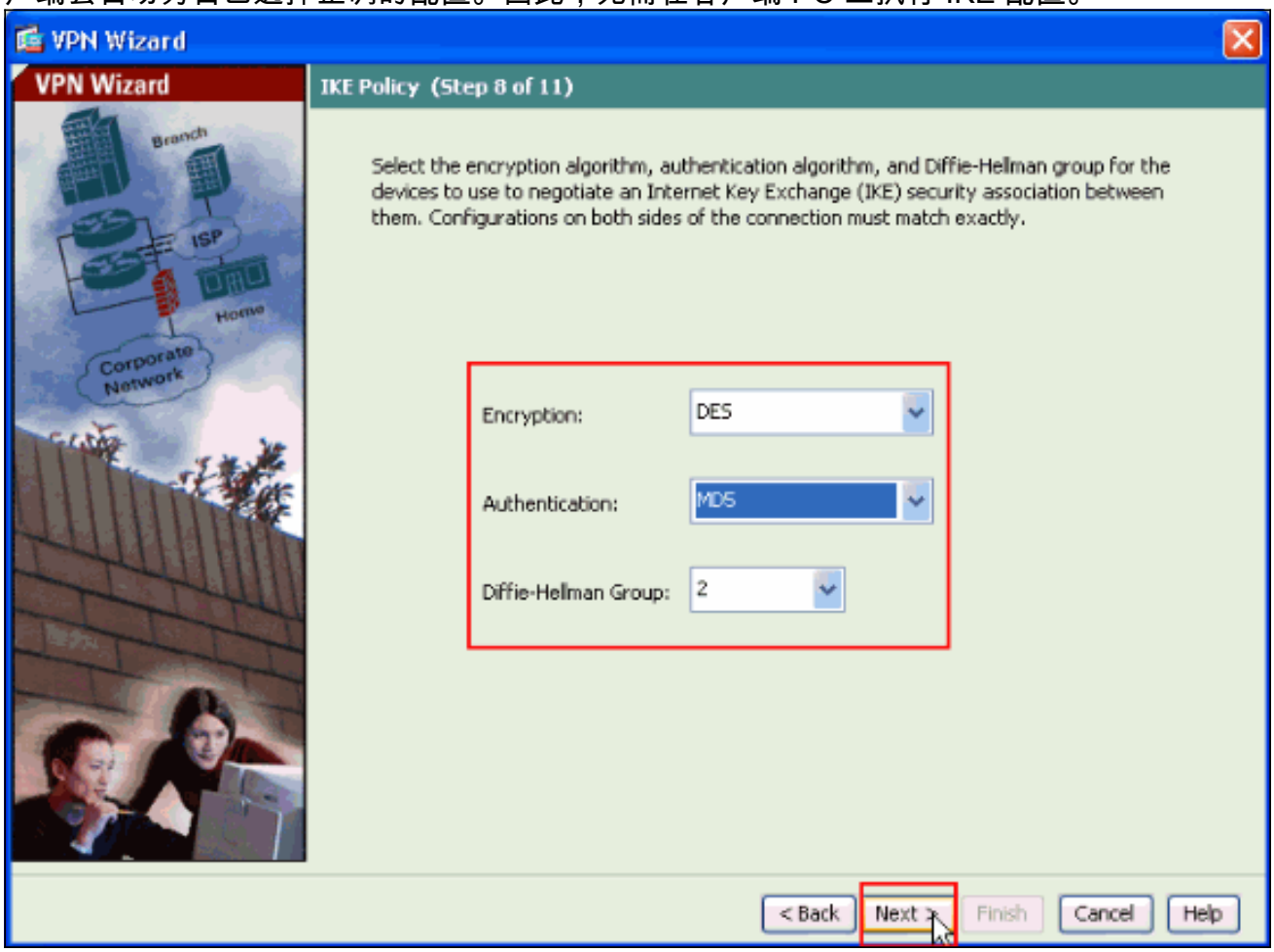
13. 定义在远程 VPN 客户端建立连接时将动态分配给这些客户端的本地地址池后，请单击 **Next**。



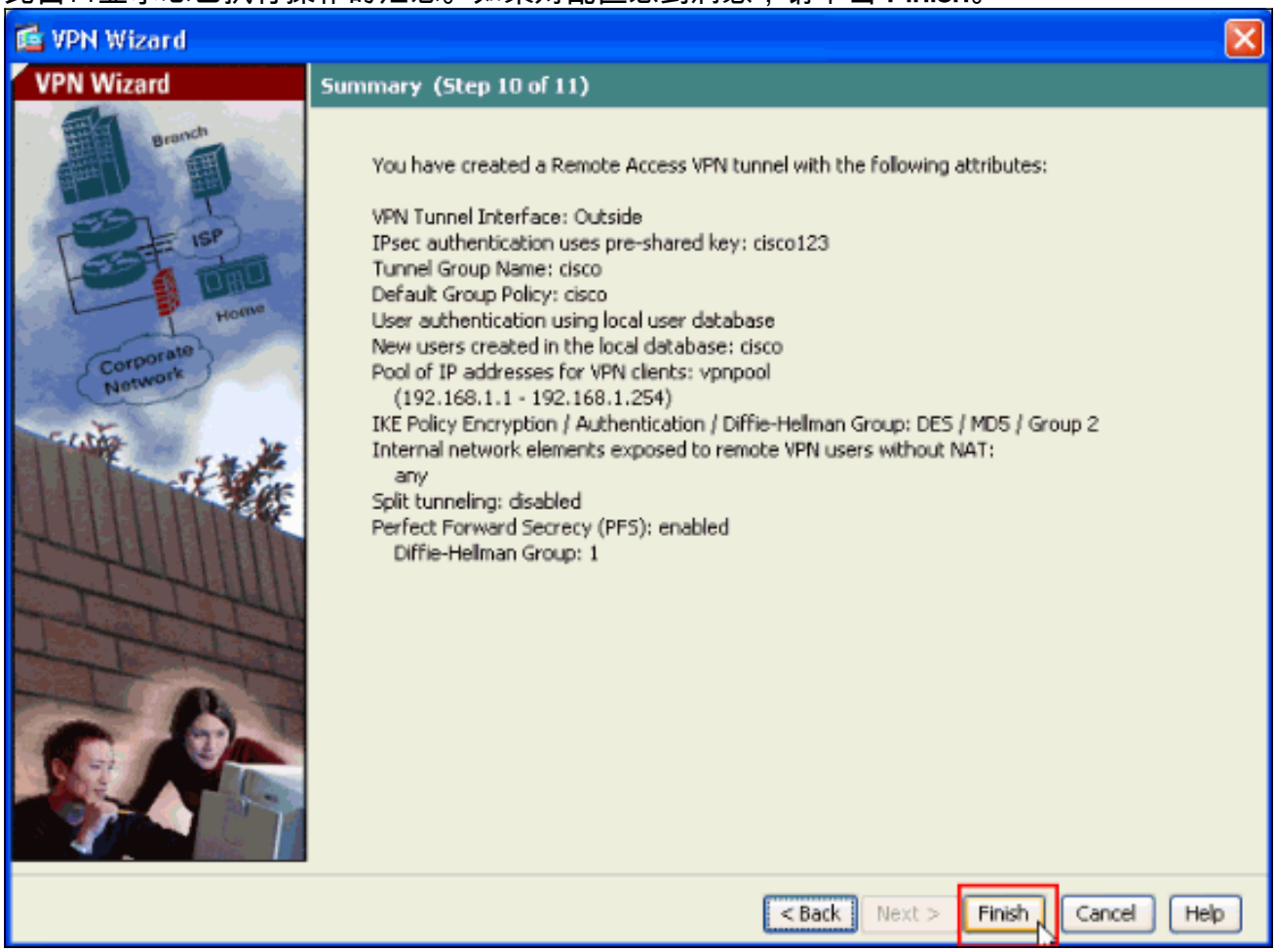
14. ***可选：***指定 DNS 和 WINS 服务器信息以及将被推送到远程 VPN 客户端的默认域名。



15. 为 IKE 指定参数，也称为 IKE 第 1 阶段。隧道两端的配置必须完全一致。但 Cisco VPN 客户端会自动为自己选择正确的配置。因此，无需在客户端 PC 上执行 IKE 配置。



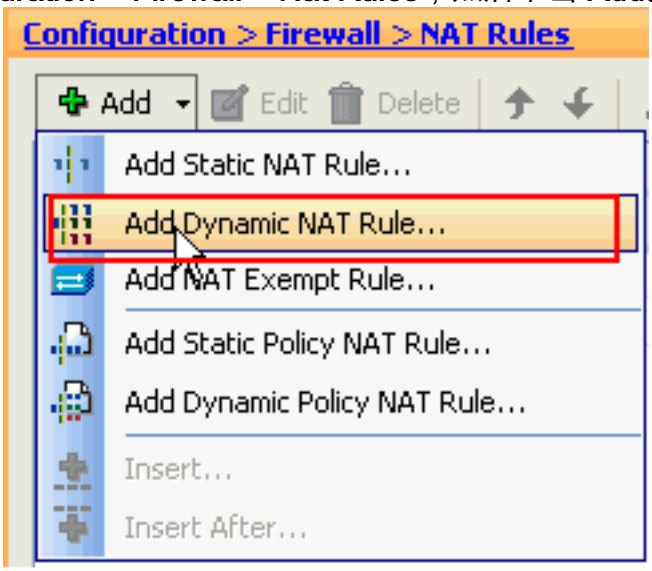
16. 此窗口显示您已执行操作的汇总。如果对配置感到满意，请单击 **Finish**。



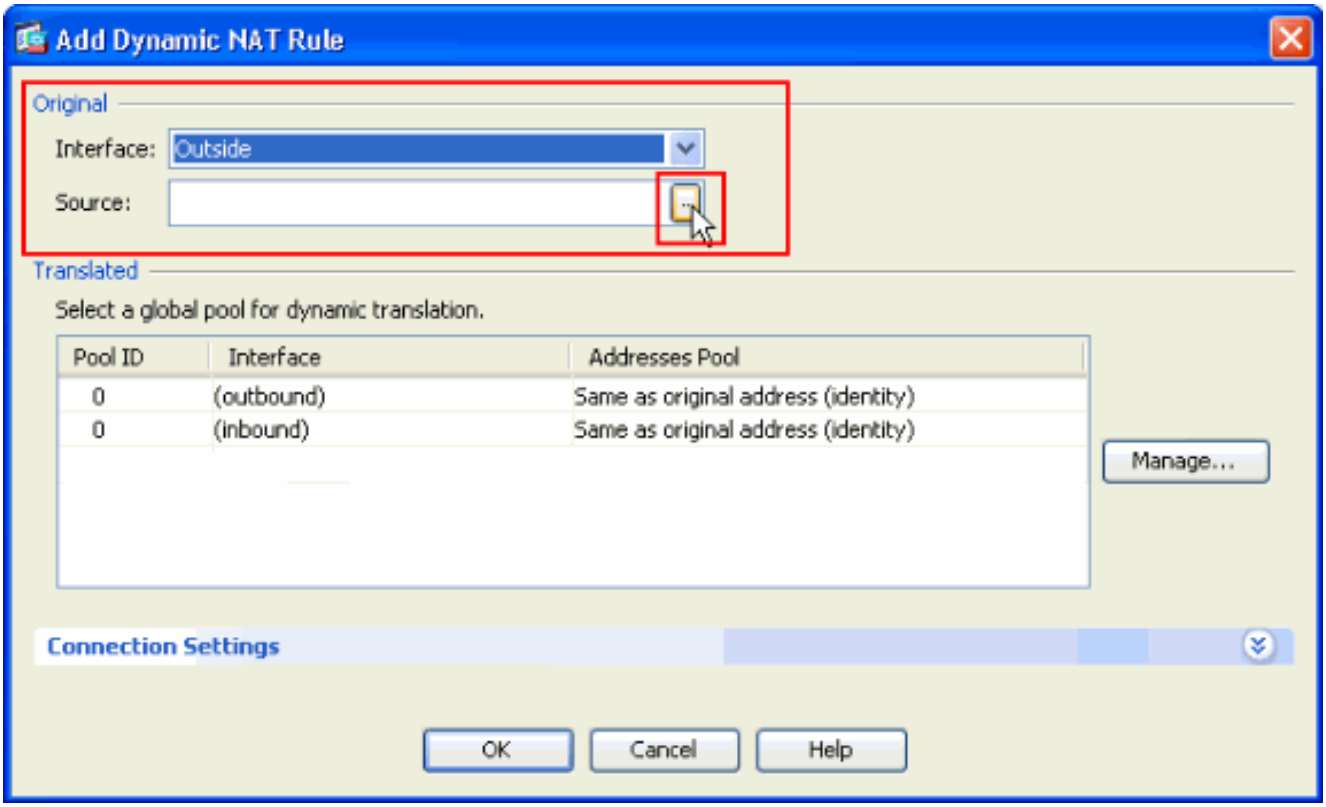
使用 ASDM 配置从 ASA/PIX 到 NAT 的入站 VPN 客户端流量

要使用 ASDM 配置从 Cisco ASA 到 NAT 的入站 VPN 客户端流量，请完成以下步骤：

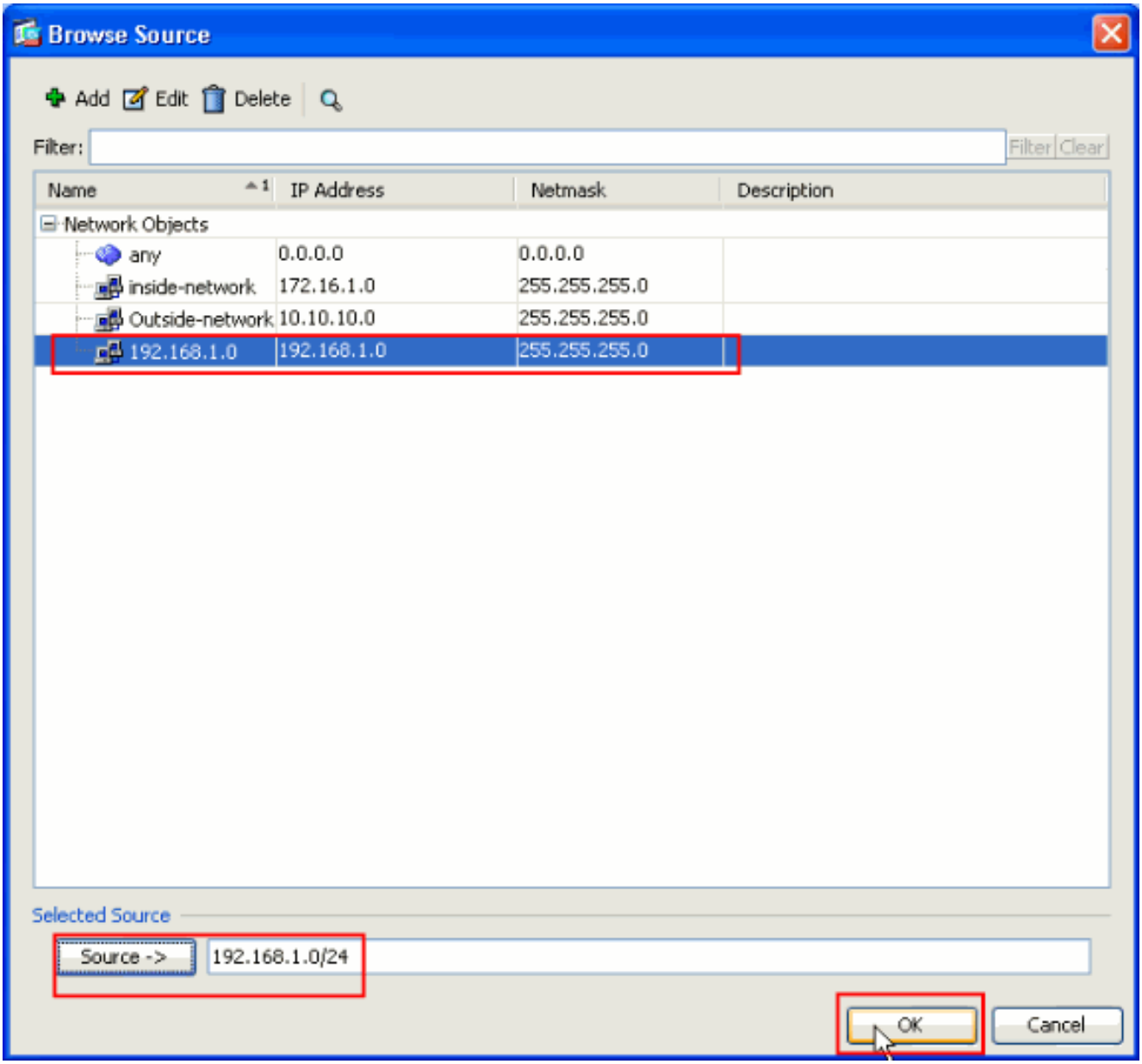
1. 选择 **Configuration > Firewall > Nat Rules**，然后单击 **Add**。在下拉列表中选择 **Add Dynamic NAT Rule**。



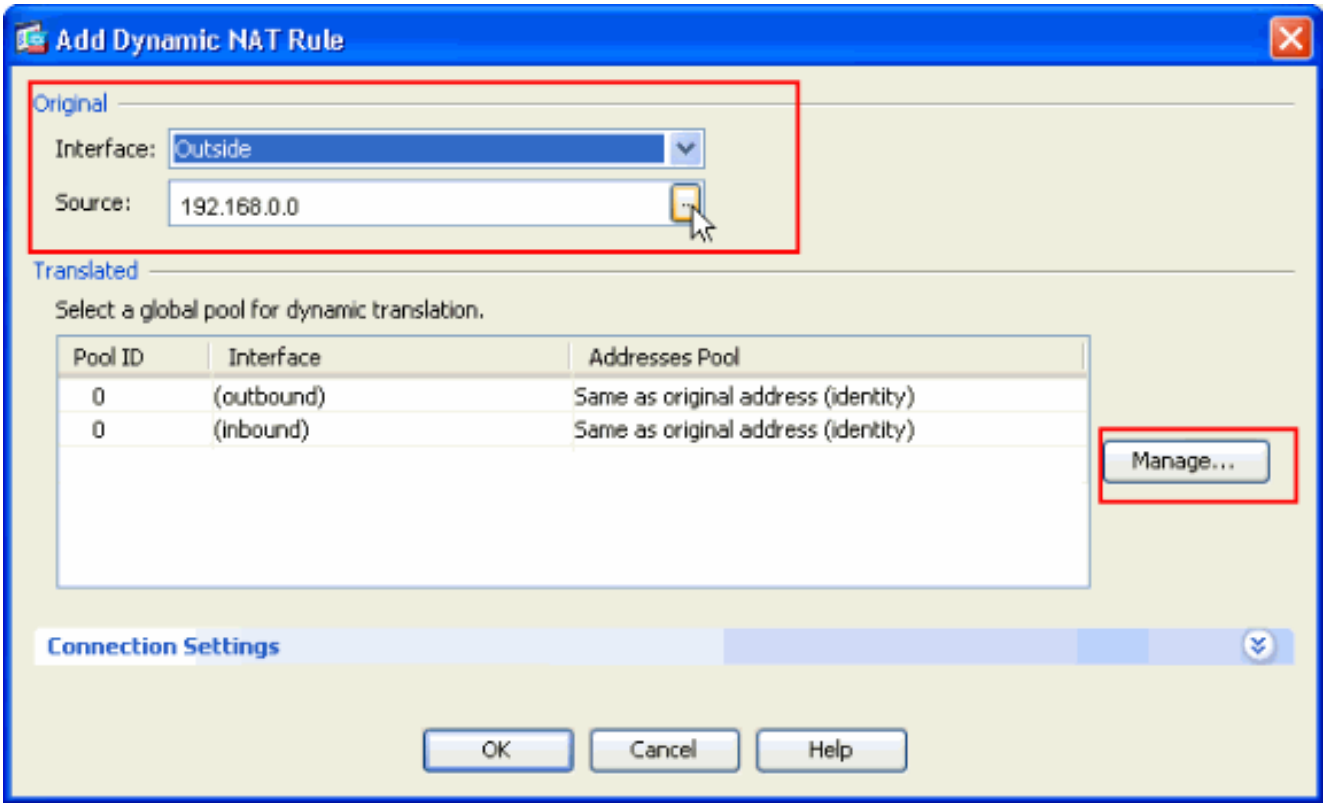
2. 在 **Add Dynamic NAT Rule** 窗口中，选择 **Outside** 作为 Interface，然后单击 **Source** 框旁边的浏览按钮。



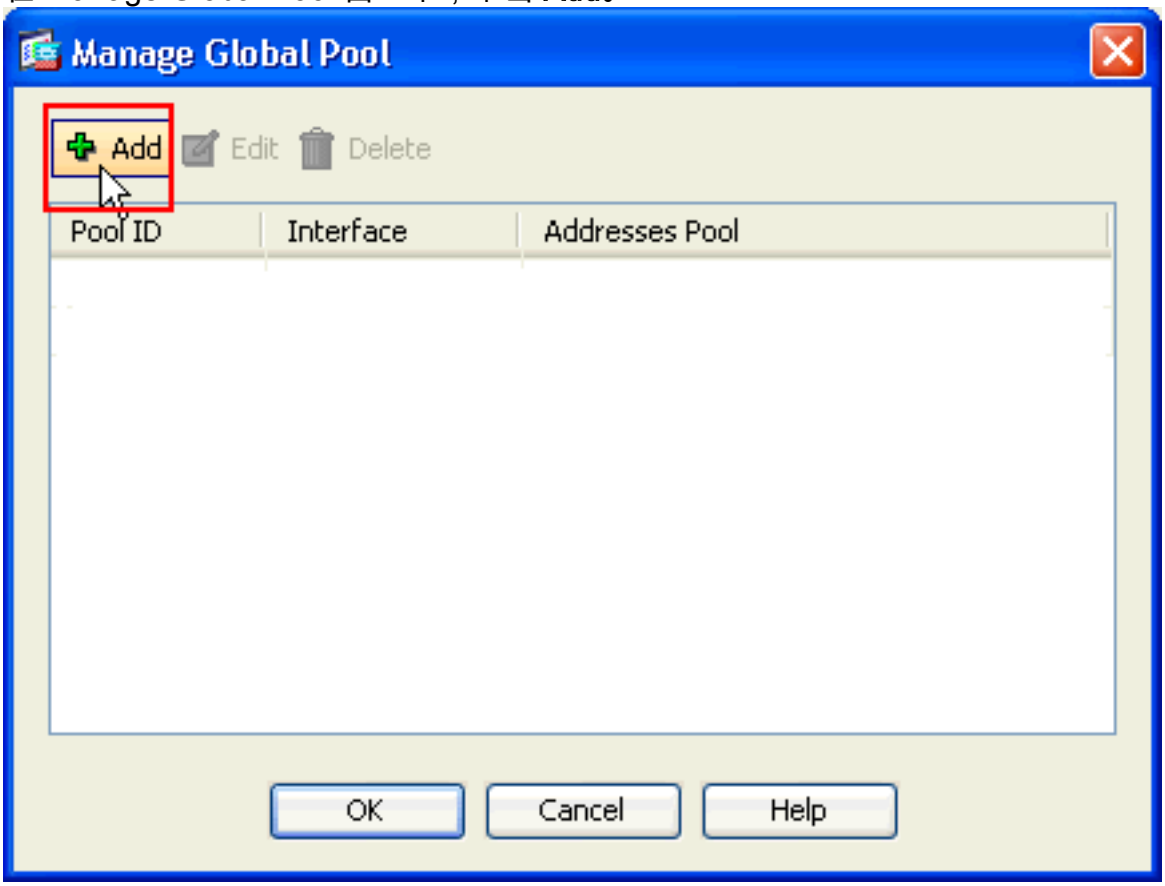
3. 在 Browse Source 窗口中，选择正确的网络对象，同时选择 Selected Source 部分下的 **source**，然后单击 **OK**。此处选择的网络对象 (Network Object) 为 192.168.1.0。


Browse Source
Add
Edit
Delete
Filter:
Filter
Clear
Name
IP Address
Netmask
Description
Network Objects
any
0.0.0.0
0.0.0.0
inside-network
172.16.1.0
255.255.255.0
Outside-network
10.10.10.0
255.255.255.0
192.168.1.0
192.168.1.0
255.255.255.0
Selected Source
Source ->
192.168.1.0/24
OK
Cancel

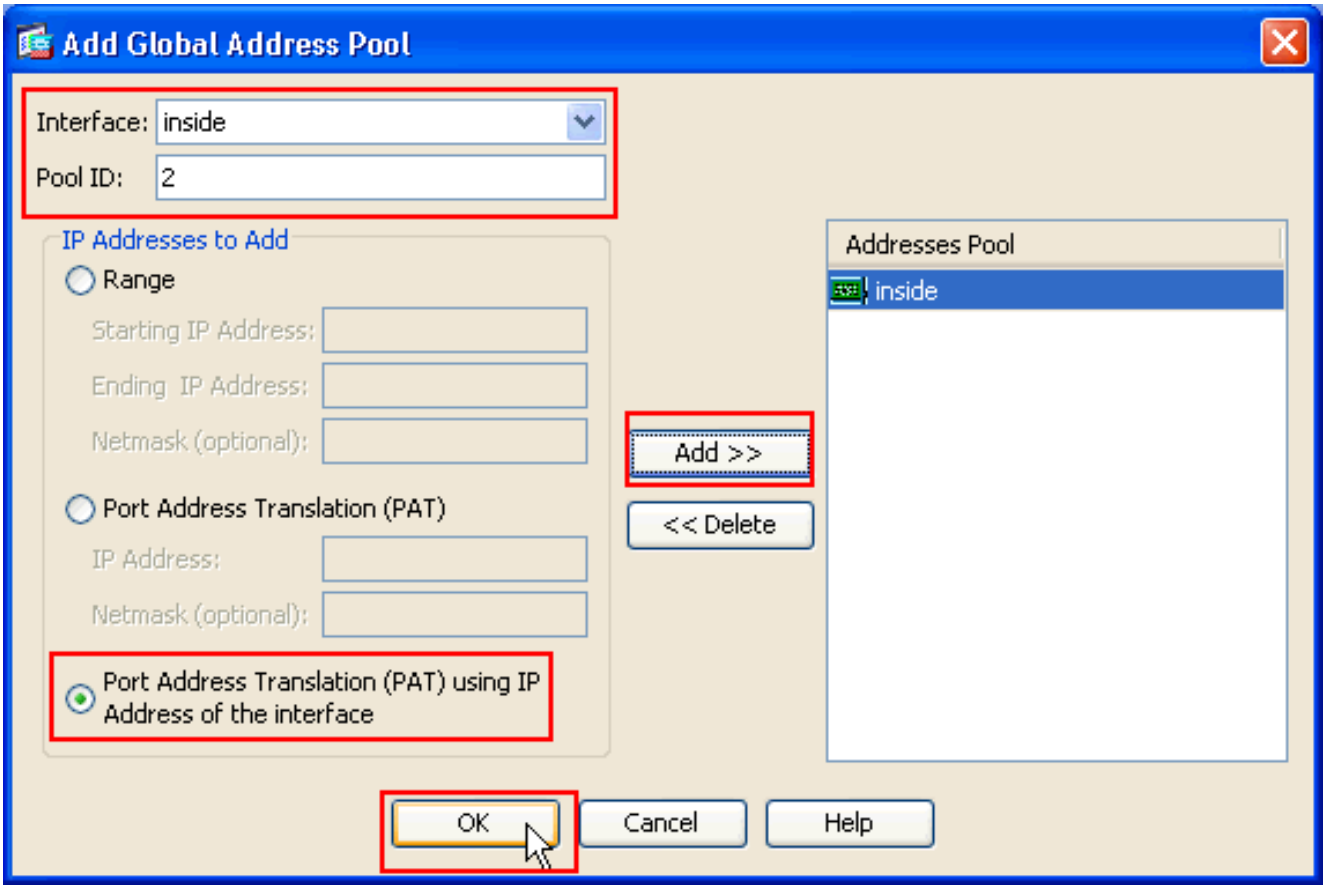
4. 单击 **Manage**。



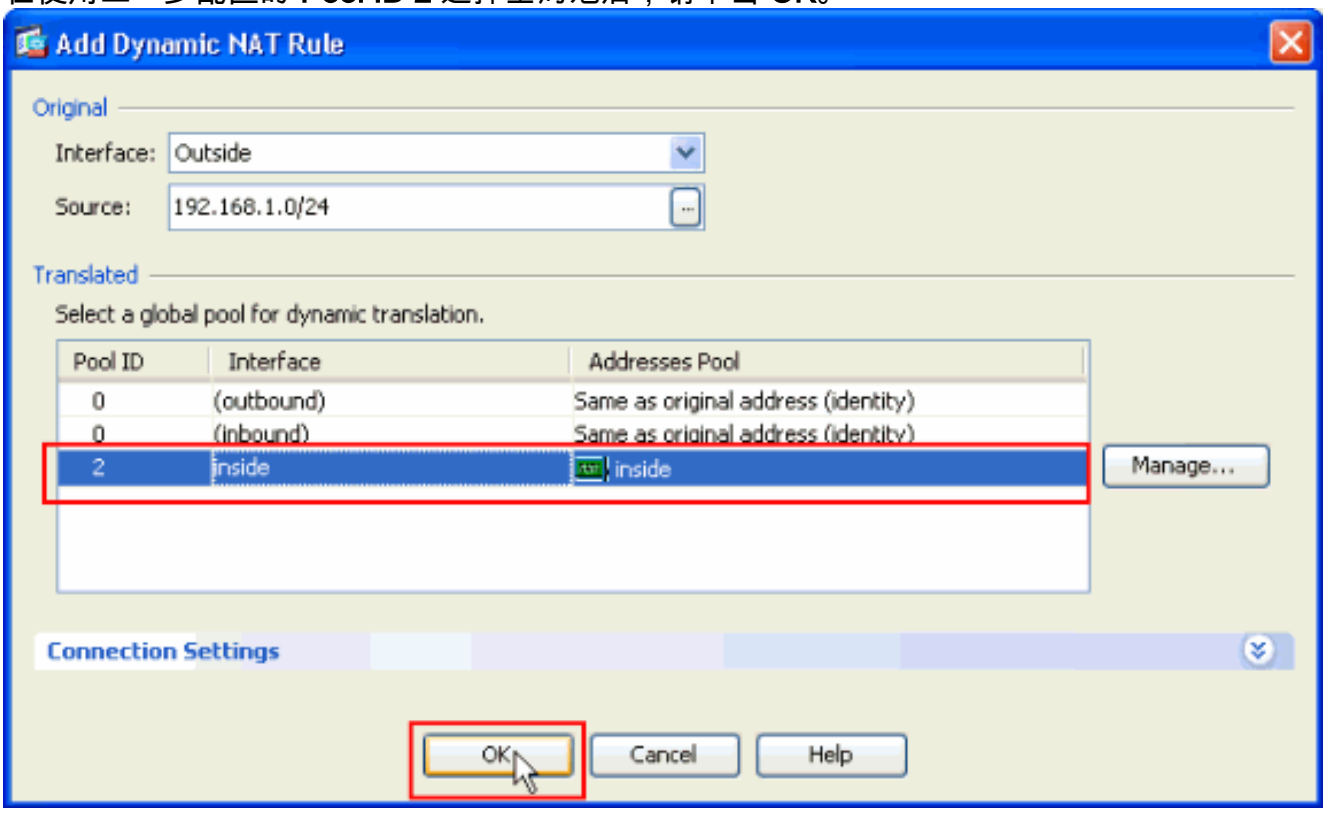
5. 在 Manage Global Pool 窗口中，单击 **Add**。



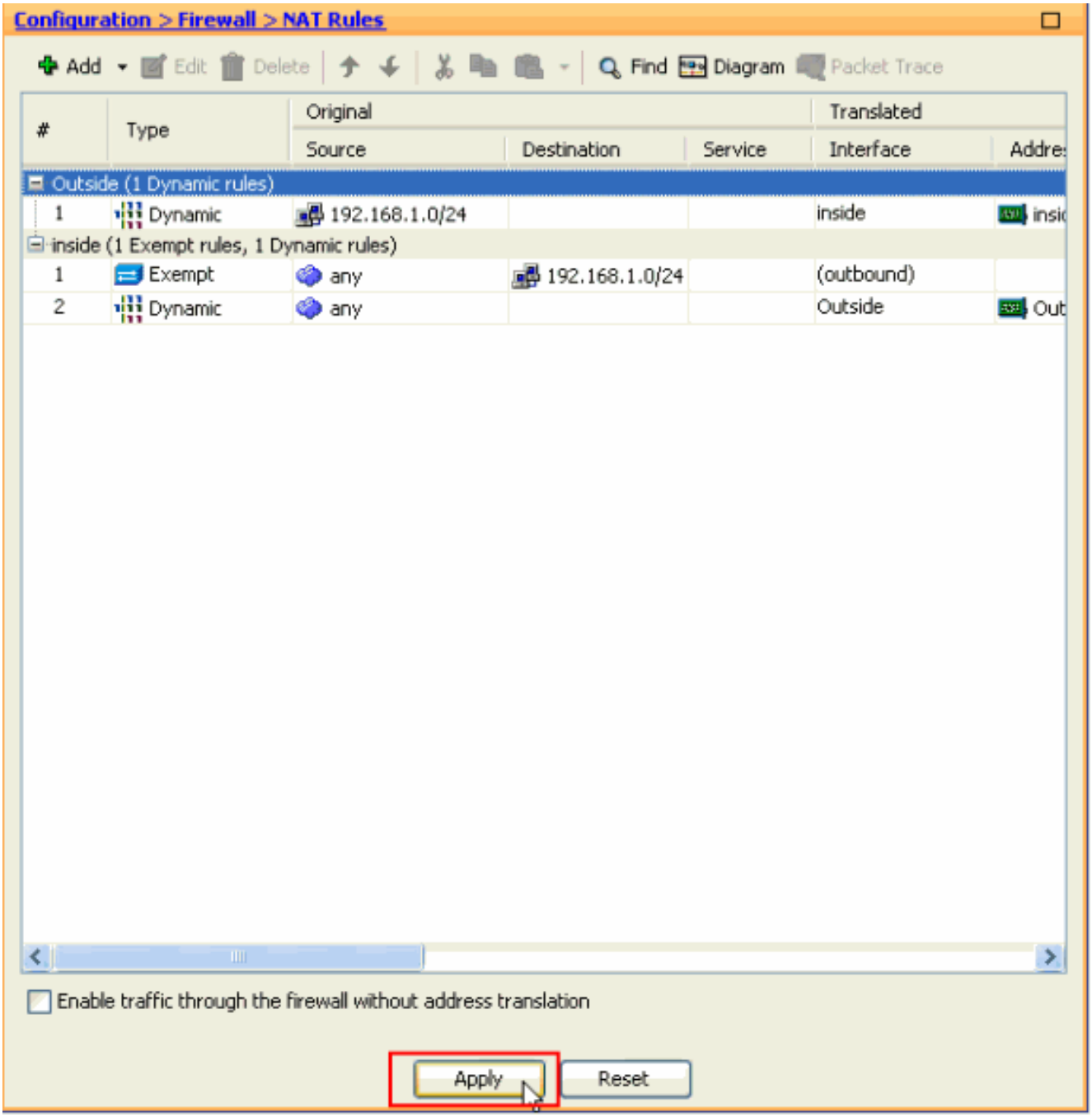
6. 在 Add Global Address Pool 窗口中，选择 **Inside** 作为 Interface，选择 **2** 作为 **Pool ID**。此外，请确保选中 **PAT using IP Address of the interface** 旁边的单选按钮。单击 **Add>>**，然后单击 **OK**。



7. 在使用上一步配置的 **Pool ID 2** 选择全局池后，请单击 **OK**。



8. 现在请单击 **Apply**，以便将配置应用到 ASA。配置到此结束。



使用 CLI 将 ASA/PIX 配置为远程 VPN 服务器并使之适用于入站 NAT

在 ASA 设备上运行配置

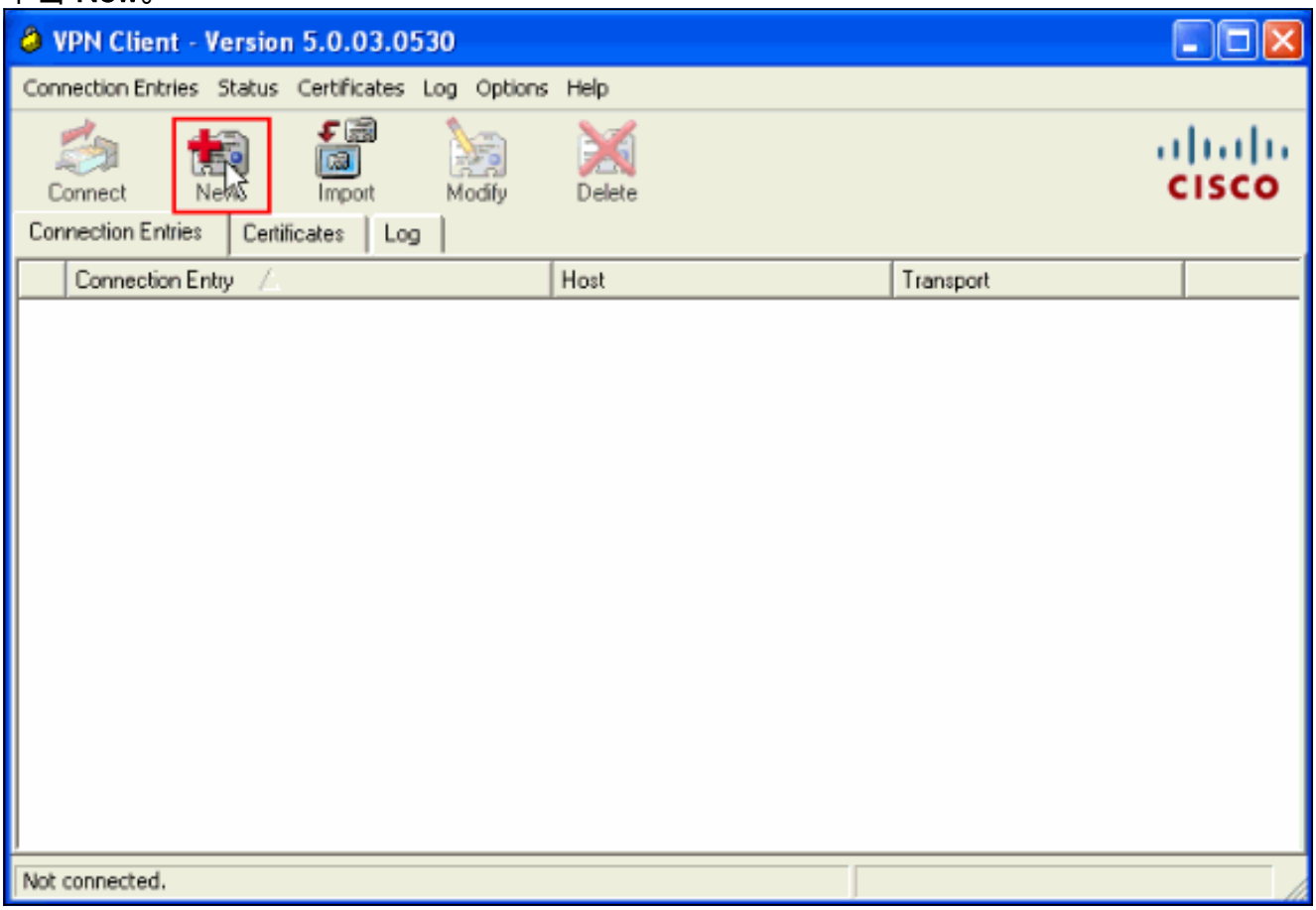
```
ciscoasa#show running-config : Saved ASA Version 8.0(3)
! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0/0 nameif Outside
security-level 0 ip address 10.10.10.2 255.255.255.0 !
interface Ethernet0/1 nameif inside security-level 100
ip address 172.16.1.2 255.255.255.0 ! ! passwd
2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa803-
k8.bin ftp mode passive access-list inside_nat0_outbound
extended permit ip any 192.168.1.0 255.255.255 0 pager
lines 24 logging enable mtu Outside 1500 mtu inside 1500
ip local pool vpnpool 192.168.1.1-192.168.1.254 mask
255.255.255.0 no failover icmp unreachable rate-limit 1
burst-size 1 asdm image disk0:/asdm-615.bin asdm history
enable arp timeout 14400 nat-control global (Outside) 1
interface global (inside) 2 interface nat (Outside) 2
192.168.1.0 255.255.255.0 outside nat (inside) 0 access-
```

```
list inside_nat0_outbound nat (inside) 1 0.0.0.0 0.0.0.0
route Outside 0.0.0.0 0.0.0.0 10.10.10.3 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
dynamic-access-policy-record DfltAccessPolicy http
server enable no snmp-server location no snmp-server
contact !--- Configuration for IPsec policies. !---
Enables the crypto transform configuration mode, !---
where you can specify the transform sets that are used
!--- during an IPsec negotiation. crypto ipsec
transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto
ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
pfs group1 crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP
65535 set transform-set ESP-DES-SH ESP-DES-MD5 crypto
map Outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP crypto map Outside_map
interface Outside crypto isakmp enable Outside !---
Configuration for IKE policies. !--- Enables the IKE
policy configuration (config-isakmp) !--- command mode,
where you can specify the parameters that !--- are used
during an IKE negotiation. Encryption and !--- Policy
details are hidden as the default values are chosen.
crypto isakmp policy 10 authentication pre-share
encryption des hash sha group 2 lifetime 86400 crypto
isakmp policy 30 authentication pre-share encryption des
hash md5 group 2 lifetime 86400 telnet timeout 5 ssh
timeout 60 console timeout 0 management-access inside
threat-detection basic-threat threat-detection
statistics access-list group-policy cisco internal
group-policy cisco attributes vpn-tunnel-protocol IPSec
!--- Specifies the username and password with their !---
respective privilege levels username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15 username cisco
password ffIRPGpDSOJh9YLq encrypted privilege 0 username
cisco attributes vpn-group-policy cisco tunnel-group
cisco type remote-access tunnel-group cisco general-
attributes address-pool vpnpool default-group-policy
cisco !--- Specifies the pre-shared key "cisco123" which
must !--- be identical at both peers. This is a global
!--- configuration mode command. tunnel-group cisco
ipsec-attributes pre-shared-key * ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns migrated_dns_map_1
parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
migrated_dns_map_1 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:f2ad6f9d5bf23810a26f5cb464e1fdf3 : end
ciscoasa#
```

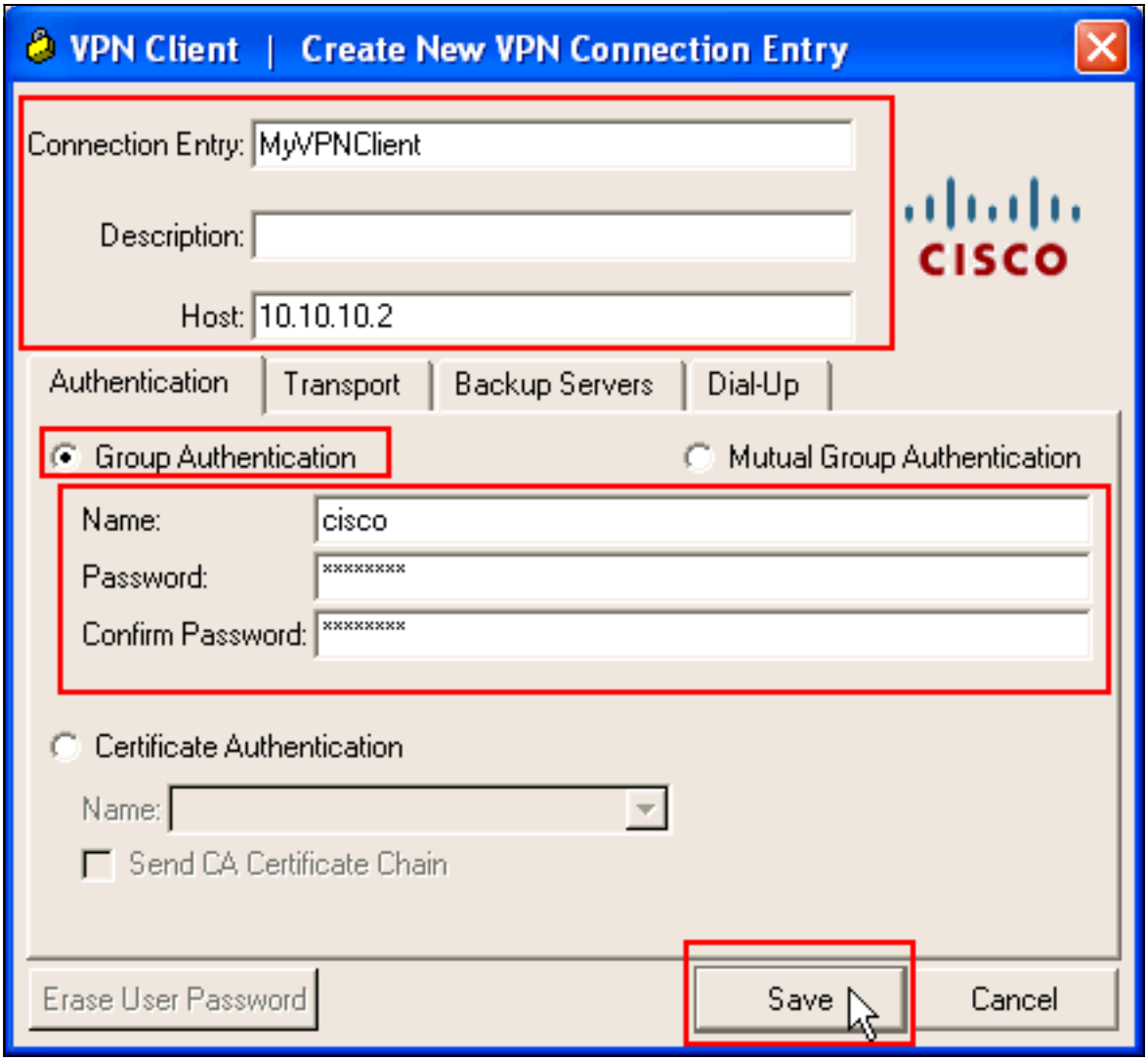
验证

尝试通过 Cisco VPN 客户端连接到 Cisco ASA，以便验证是否已成功配置 ASA。

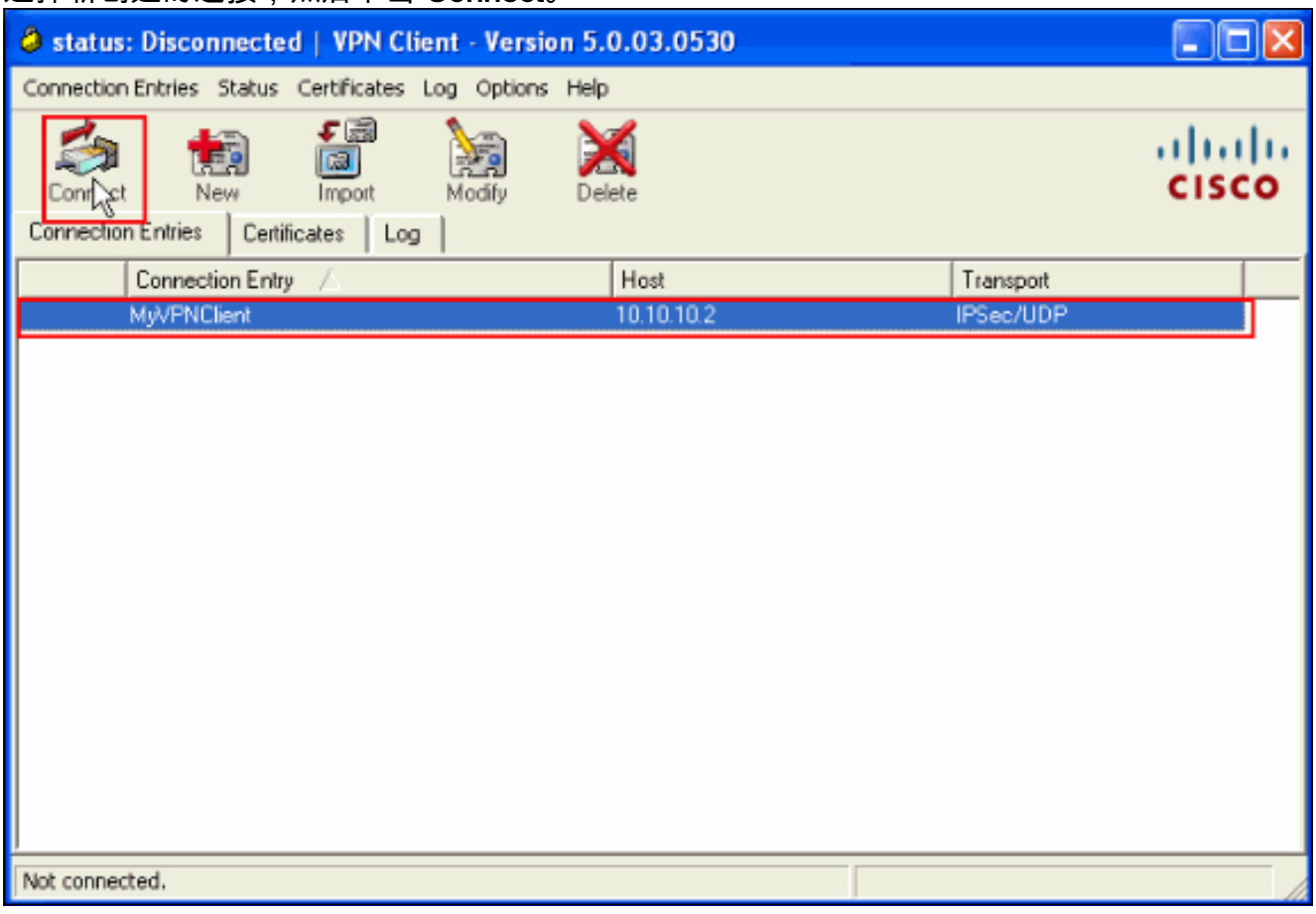
1. 单击 **New**。



2. 填写新连接的详细信息。Host 字段必须包含以前配置的 Cisco ASA 的 IP 地址或主机名。组身份验证 (Group Authentication) 信息必须与**步骤 4** 中使用的组身份验证信息对应。完成后，请单击 **Save**。

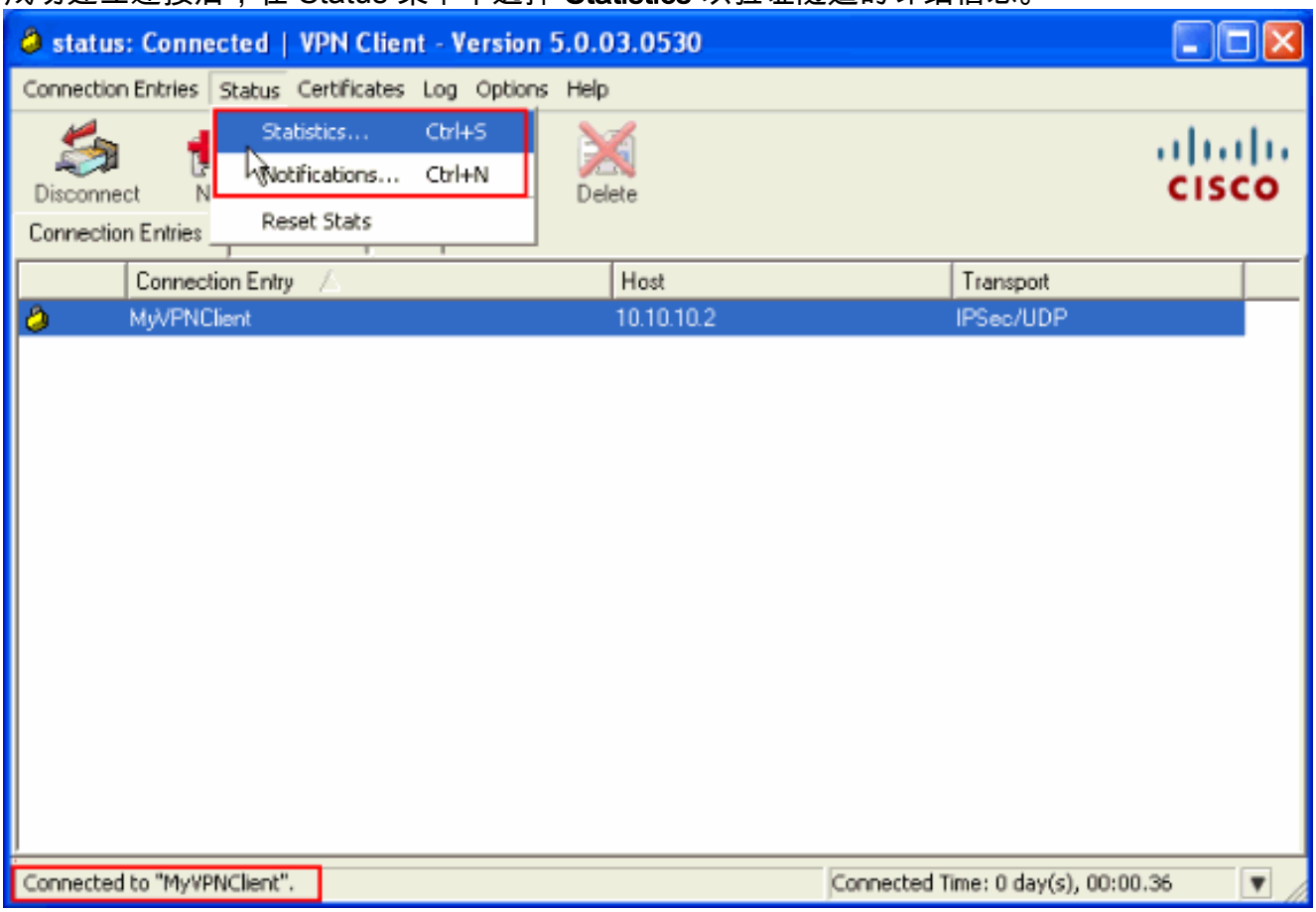


3. 选择新创建的连接，然后单击 **Connect**。

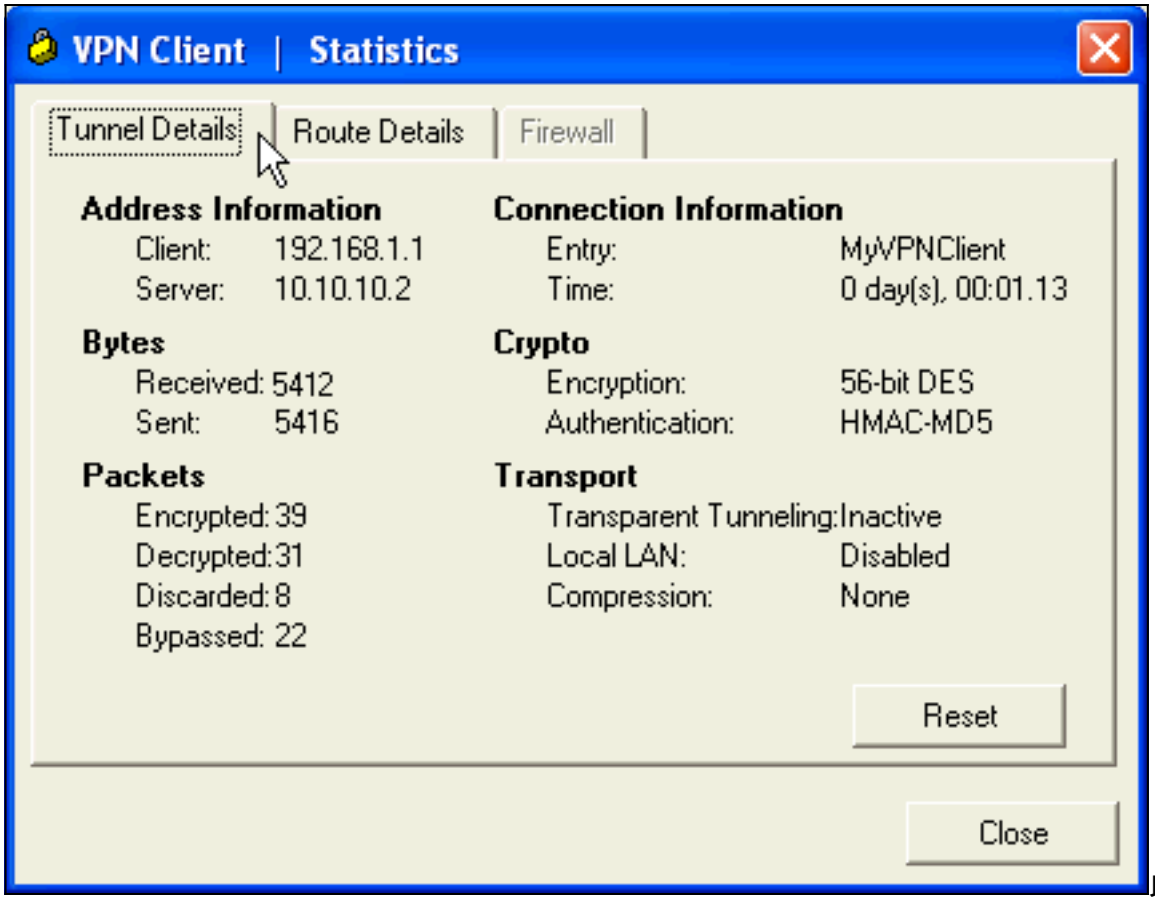


4. 输入用于扩展身份验证的用户名和口令。此信息必须与**步骤 5 和步骤 6** 中指定的信息一致。

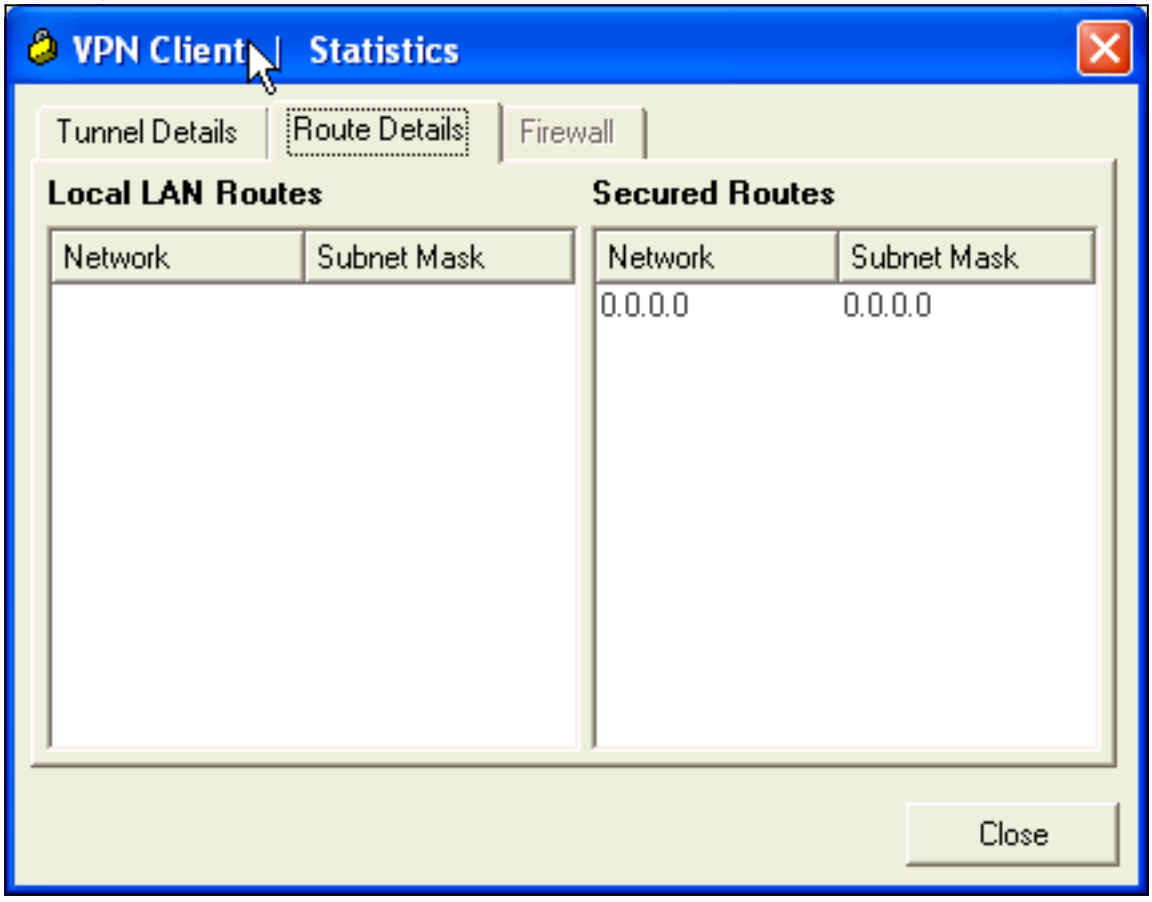
5. 成功建立连接后，在 Status 菜单中选择 **Statistics** 以验证隧道的详细信息。



此窗口显示数据流和加密信息



：此窗口显示分割隧道信息



：

ASA/PIX 安全设备 - show 命令

- **show crypto isakmp sa** - 显示对等体上的所有当前 IKE SA。`ASA#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: 10.10.10.1 Type : user Role : responder Rekey : no State : AM_ACTIVE
```

- **show crypto ipsec sa** — 显示对等体上的所有当前 IPsec SA。
```
ASA#show crypto ipsec sa
interface: Outside Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr:
10.10 .10.2 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident
(addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0) current_peer: 10.10.10.1, username:
cisco123 dynamic allocated peer ip: 192.168.1.1 #pkts encaps: 20, #pkts encrypt: 20, #pkts
digest: 20 #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-
frag successes: 0, #pre-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.: 10.10.10.2, remote crypto endpt.: 10.10.10.1 path mtu 1500, ipsec overhead 58, media
mtu 1500 current outbound spi: F49F954C inbound esp sas: spi: 0x3C10F9DD (1007745501)
transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id:
24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255
IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xF49F954C (4104099148)
transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id:
24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255
IV size: 8 bytes replay detection support: Y
```

-
```
ciscoasa(config)#debug icmp trace !--- Inbound Nat Translation is shown below for Outside to
Inside ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1 ICMP
echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3 2 !--- Inbound
Nat Translation is shown below for Inside to Outside ICMP echo reply untranslating
inside:172.16.1.2/1 to Outside:192.168.1.1/768 ICMP echo request from Outside:192.168.1.1 to
inside:172.16.1.3 ID=768 seq=8192 len=32 ICMP echo request translating
Outside:192.168.1.1/768 to inside:172.16.1.2/1 ICMP echo reply from inside:172.16.1.3 to
Outside:172.16.1.2 ID=1 seq=8192 len=3 2 ICMP echo reply untranslating inside:172.16.1.2/1
to Outside:192.168.1.1/768 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448
len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32 ICMP echo
request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32 ICMP echo reply from
172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32 ICMP echo request from 192.168.1.1 to
172.16.1.2 ID=768 seq=8960 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768
seq=8960 len=32
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

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。

有关站点到站点 VPN 故障排除的详细信息，请参阅最常见的 L2L 和远程访问 IPsec VPN 故障排除解决方案。

相关信息

- Cisco ASA 5500 系列自适应安全设备
- Cisco 自适应安全设备管理器
- Cisco ASA 5500 系列自适应安全设备故障排除和警报
- 技术支持和文档 - Cisco Systems