ASA/PIX：使用 CLI 和 ASDM 对 IPSec VPN 客户端进行静态 IP 寻址的配置示例

目录

简介

本文描述如何配置Cisco ASA 5500系列自适应安全设备(ASA)提供静态IP地址给VPN客户端以可适应安全设备管理器(ASDM)或CLI。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，可使用 Cisco VPN 客户端对其进行验证。

要在 Cisco VPN 客户端（适用于 Windows 的 4.x 版本）和 PIX 500 系列安全设备 7.x 之间设置远程访问 VPN 连接，请参阅使用 Windows 2003 IAS RADIUS（针对 Active Directory）进行身份验证的 PIX/ASA 7.x 和 Cisco VPN 客户端 4.x 配置示例。远程VPN客户端用户验证活动目录用Microsoft Windows 2003年互联网认证服务(IAS) RADIUS服务器。

要使用 Cisco 安全访问控制服务器（ACS 3.2 版）进行扩展身份验证 (Xauth) 以在 Cisco VPN 客户端（适用于 Windows 的 4.x 版）与 PIX 500 系列安全设备 7.x 之间设置远程访问 VPN 连接，请参阅使用 Cisco 安全 ACS 身份验证的 PIX/ASA 7.x 和 Cisco VPN 客户端 4.x 配置示例。

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。

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 自适应安全设备软件版本 7.x 及更高版本
- 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。

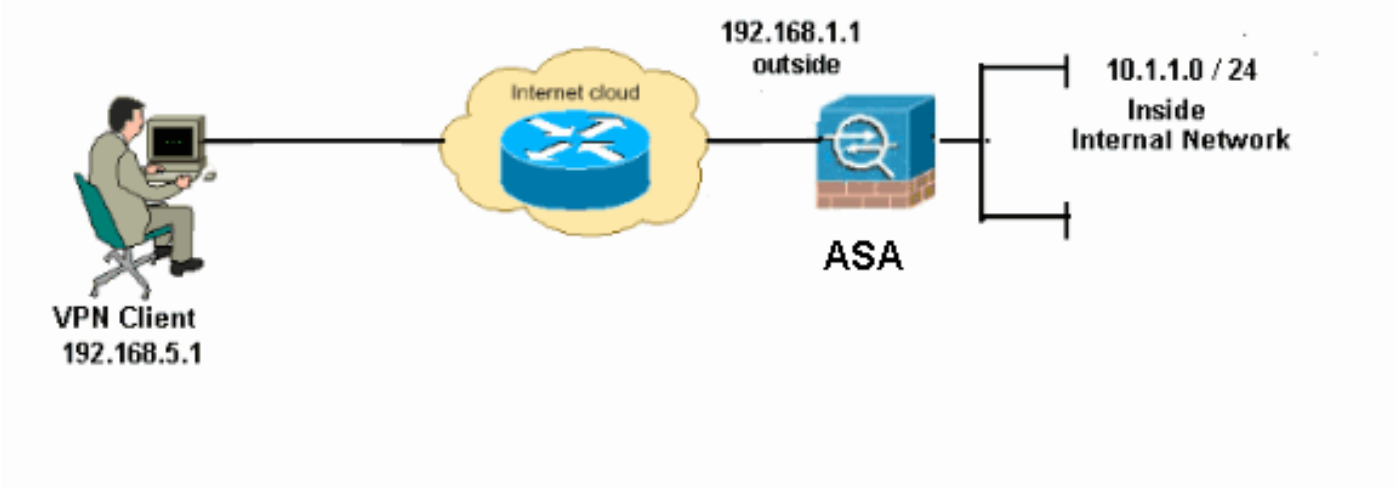
配置

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（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



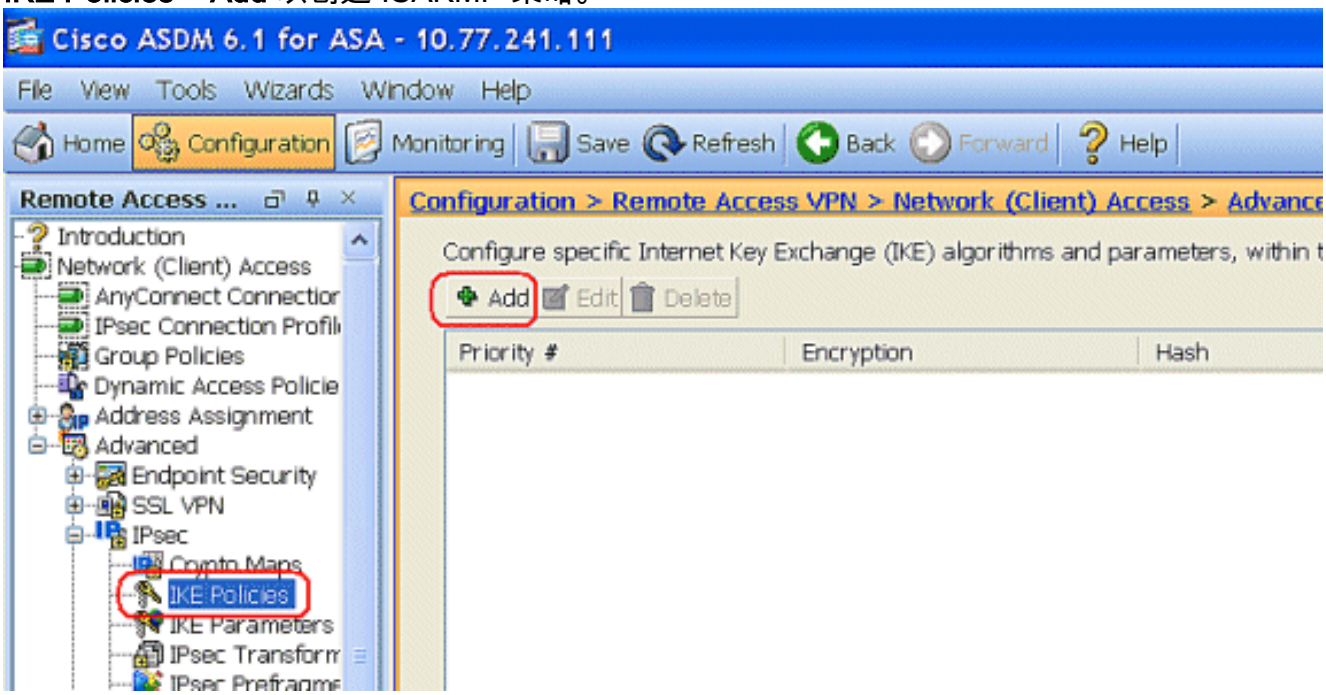
注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

配置远程访问 VPN (IPSec)

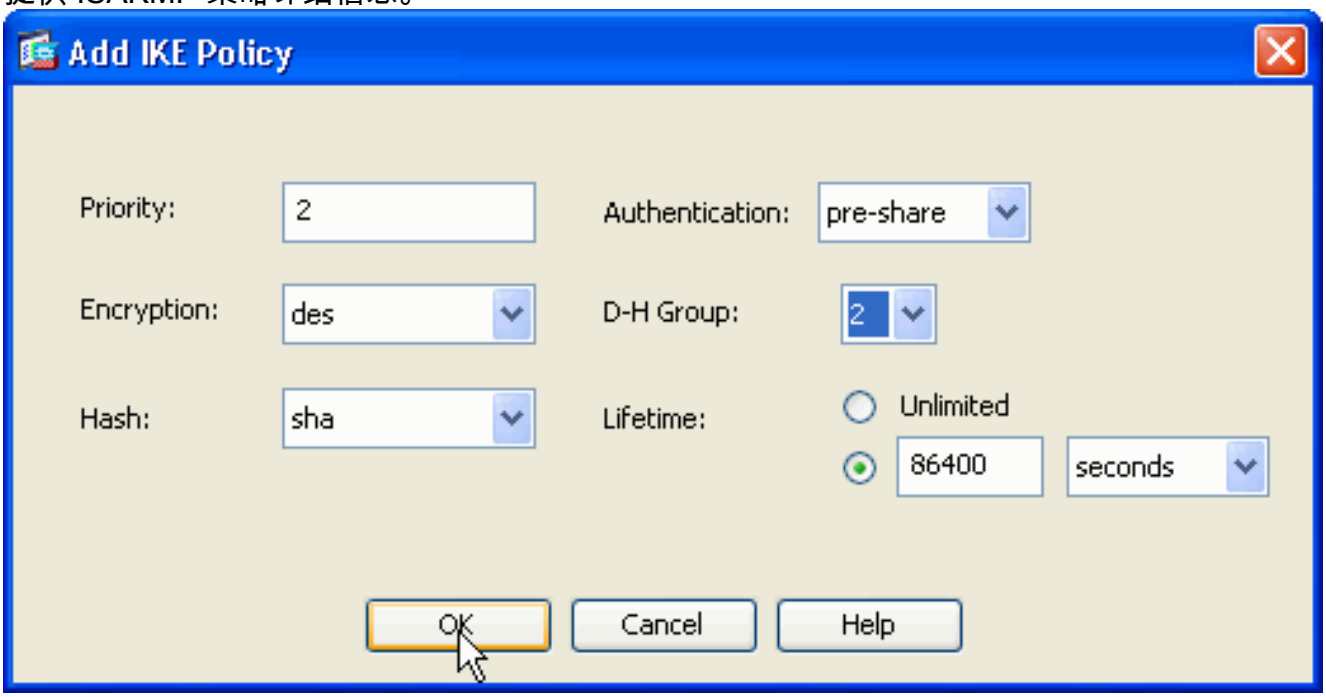
ASDM 步骤

执行下列步骤以配置远程访问 VPN：

1. 选择 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Policies > Add** 以创建 ISAKMP 策略。

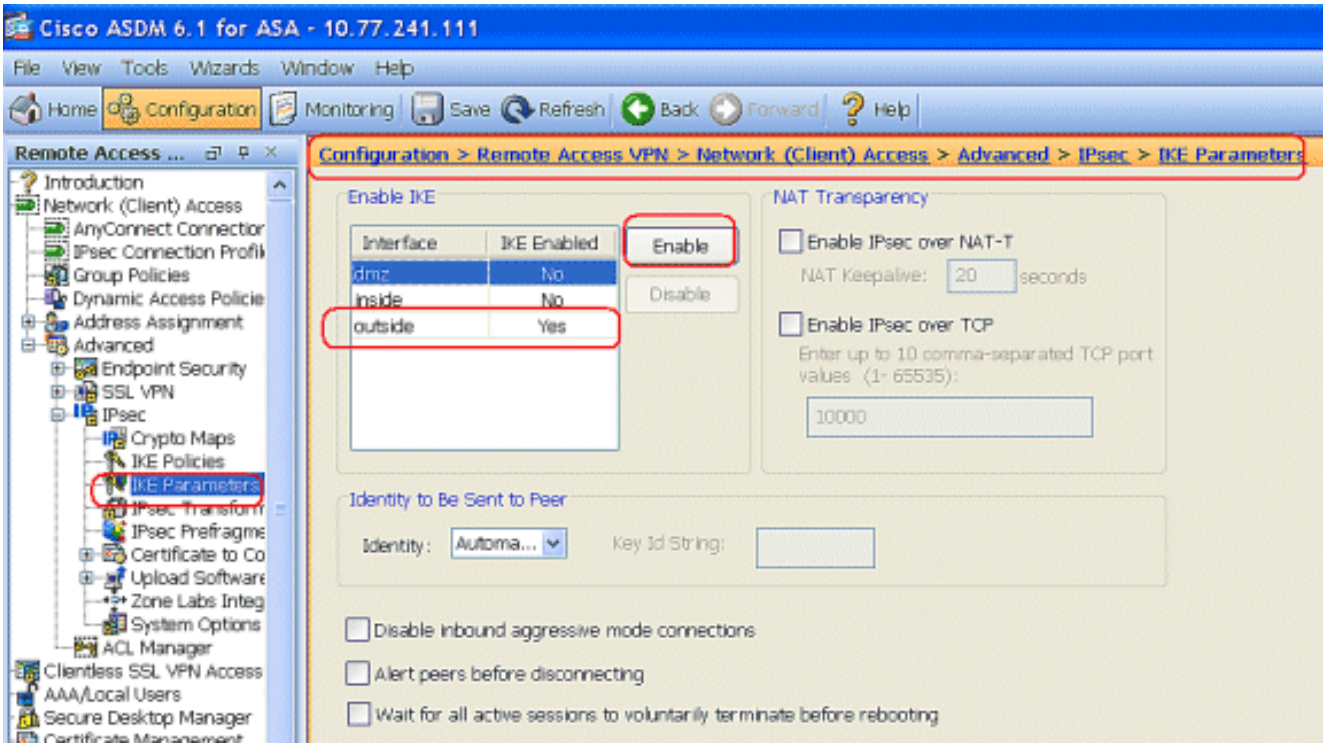


2. 提供 ISAKMP 策略详细信息。

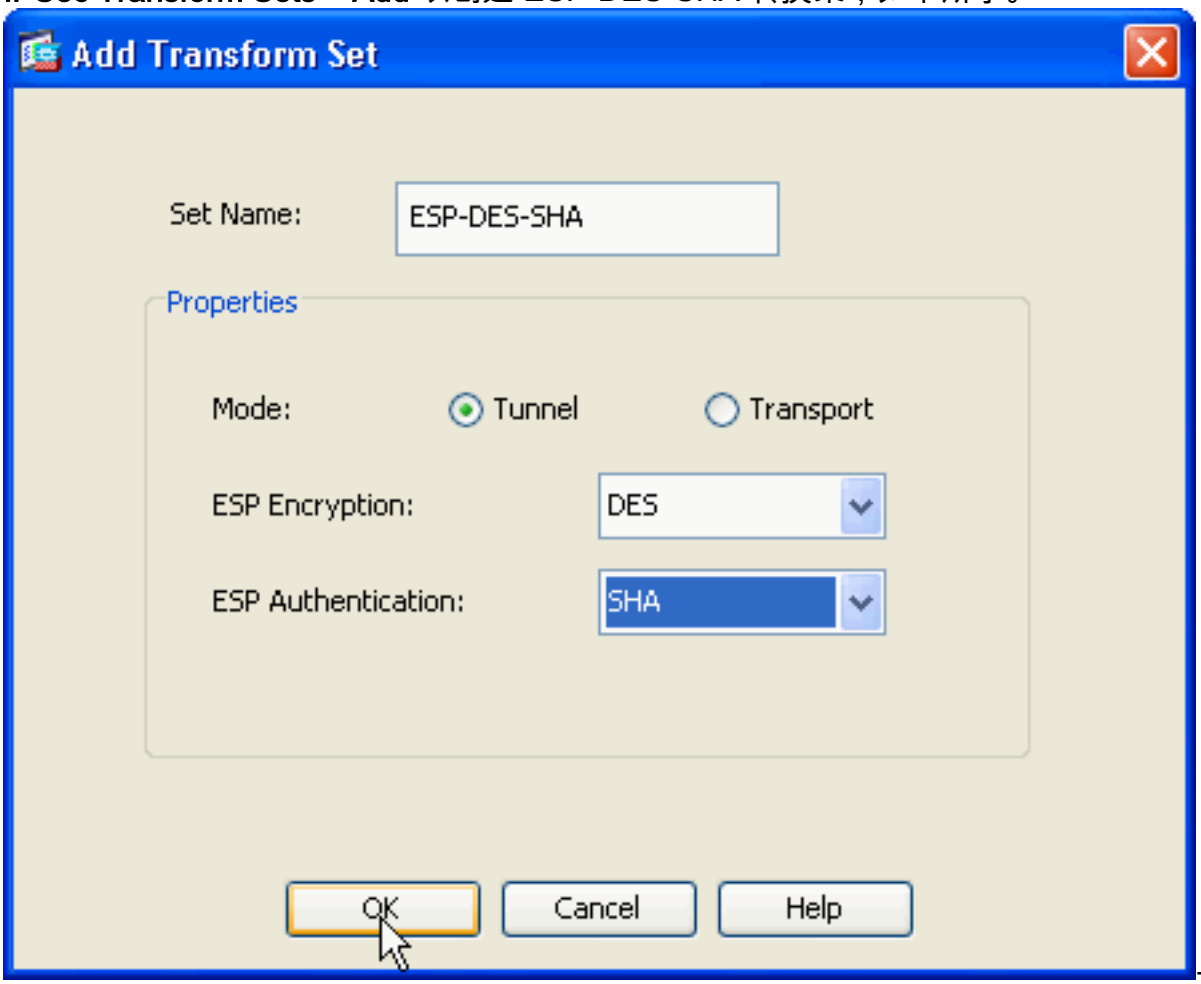


单击 **OK**，然后单击 Apply。

3. 选择 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IKE Parameters** 以启用外部接口上的 IKE。

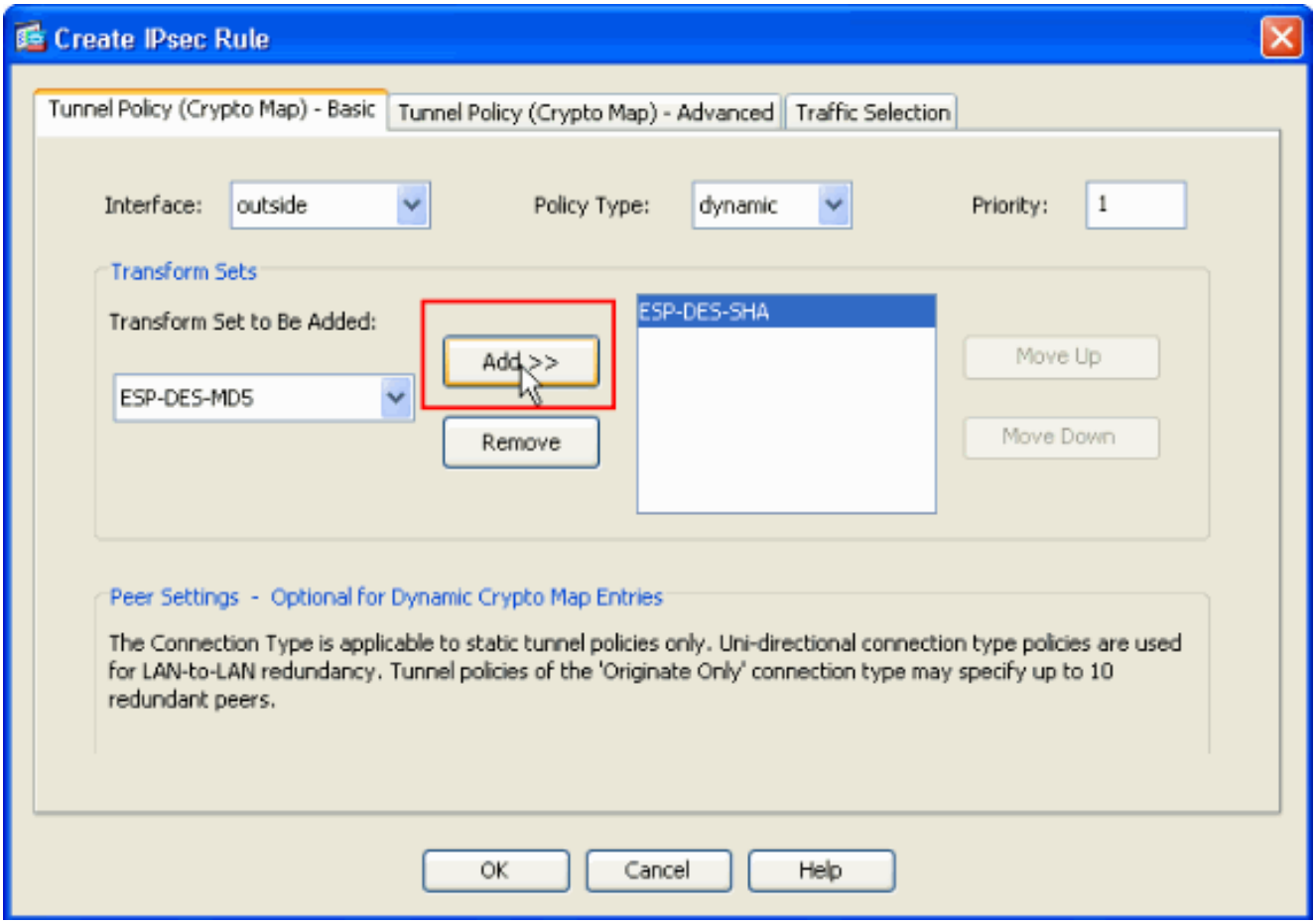


4. 选择 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > IPSec Transform Sets > Add** 以创建 ESP-DES-SHA 转换集，如下所示。



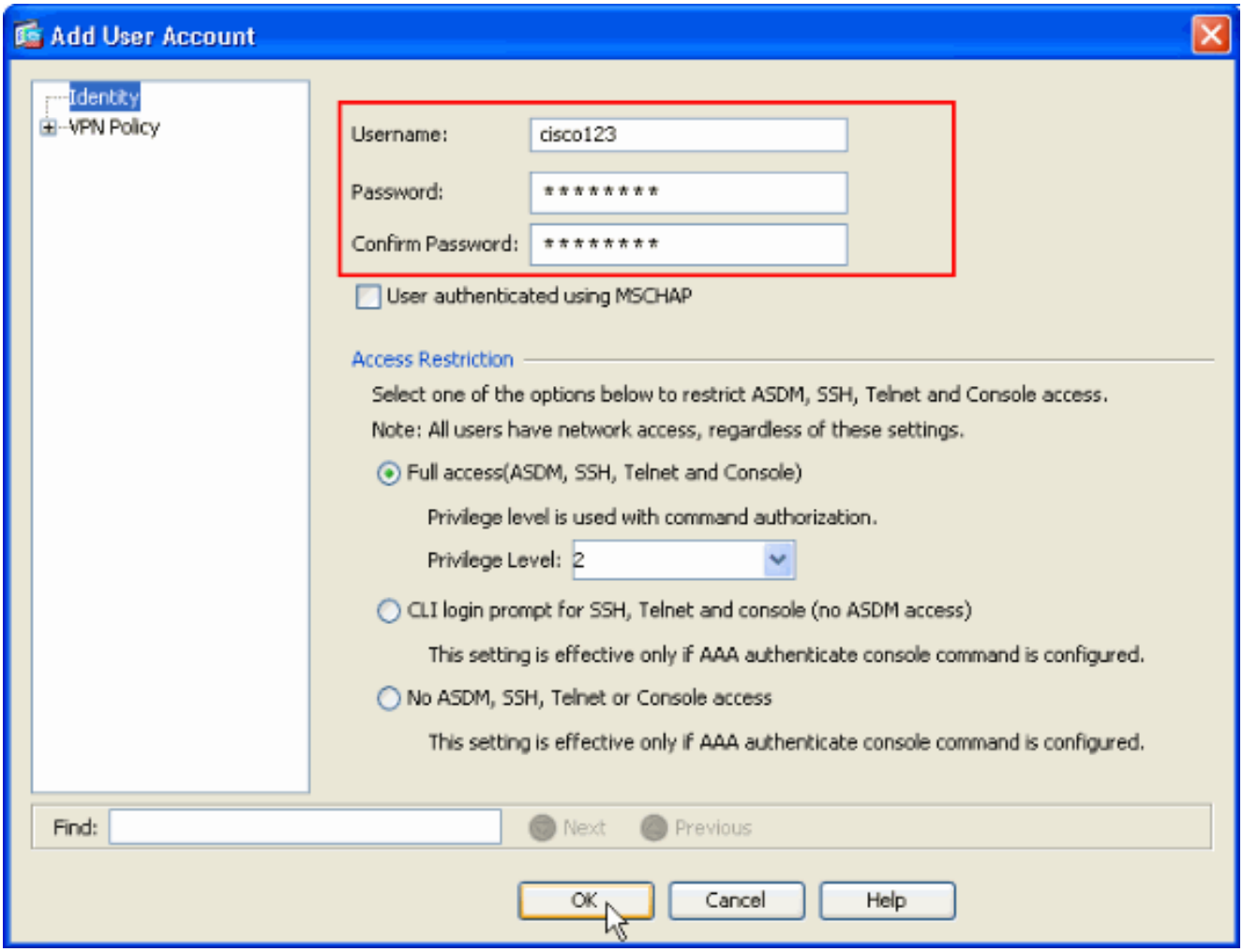
单击 **OK**，然后单击 Apply。

5. 选择 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPSec > Crypto Maps > Add** 以使用优先级为 1 的动态策略创建加密映射，如下所示。

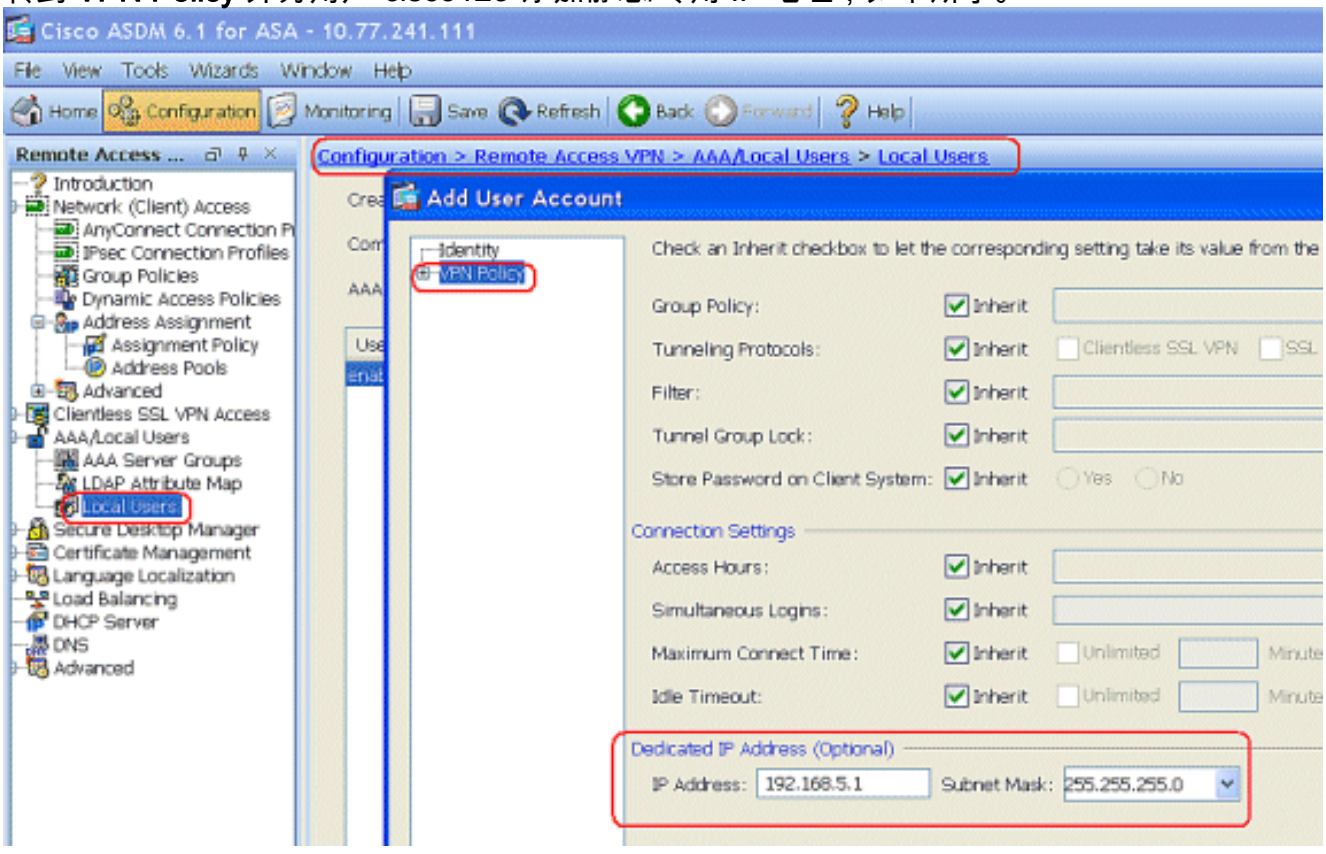


单击 **OK**，然后单击 Apply。

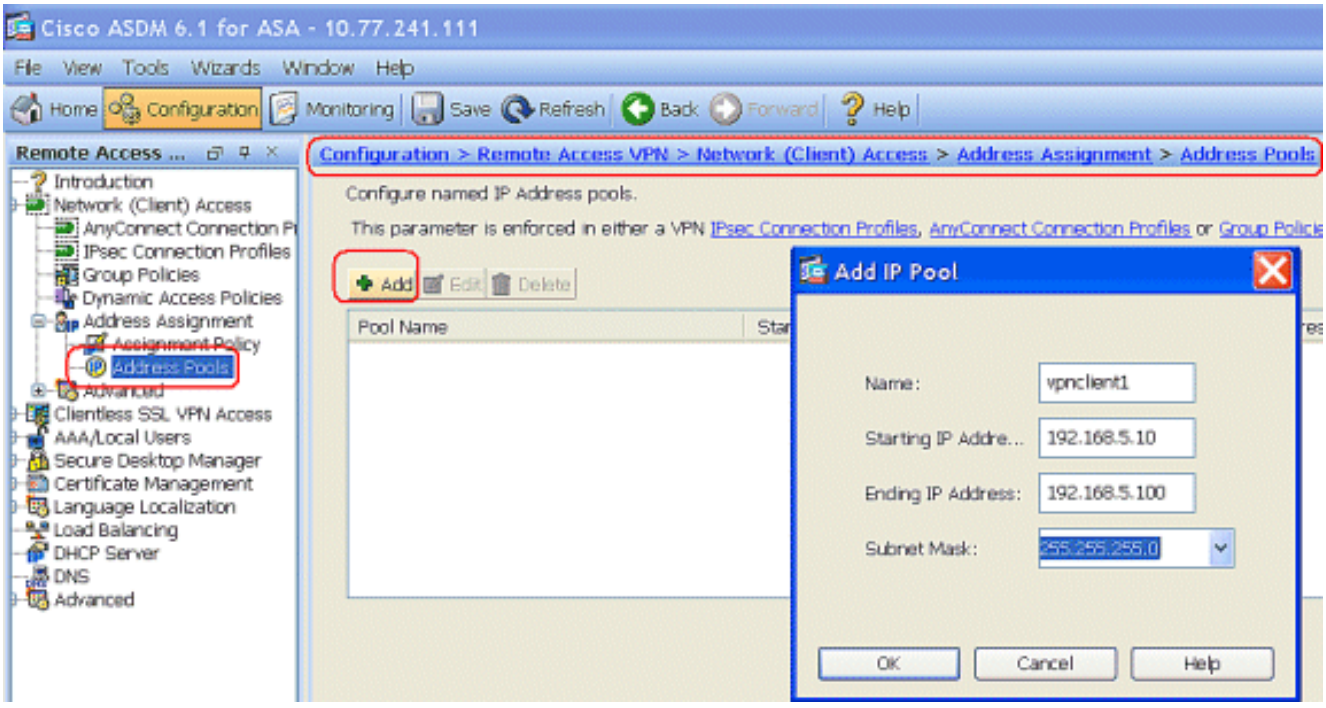
6. 选择 **Configuration > Remote Access VPN > AAA Setup > Local Users > Add** 以创建用于 VPN 客户端访问的用户帐户（例如，用户名 - cisco123，口令 - cisco123）。



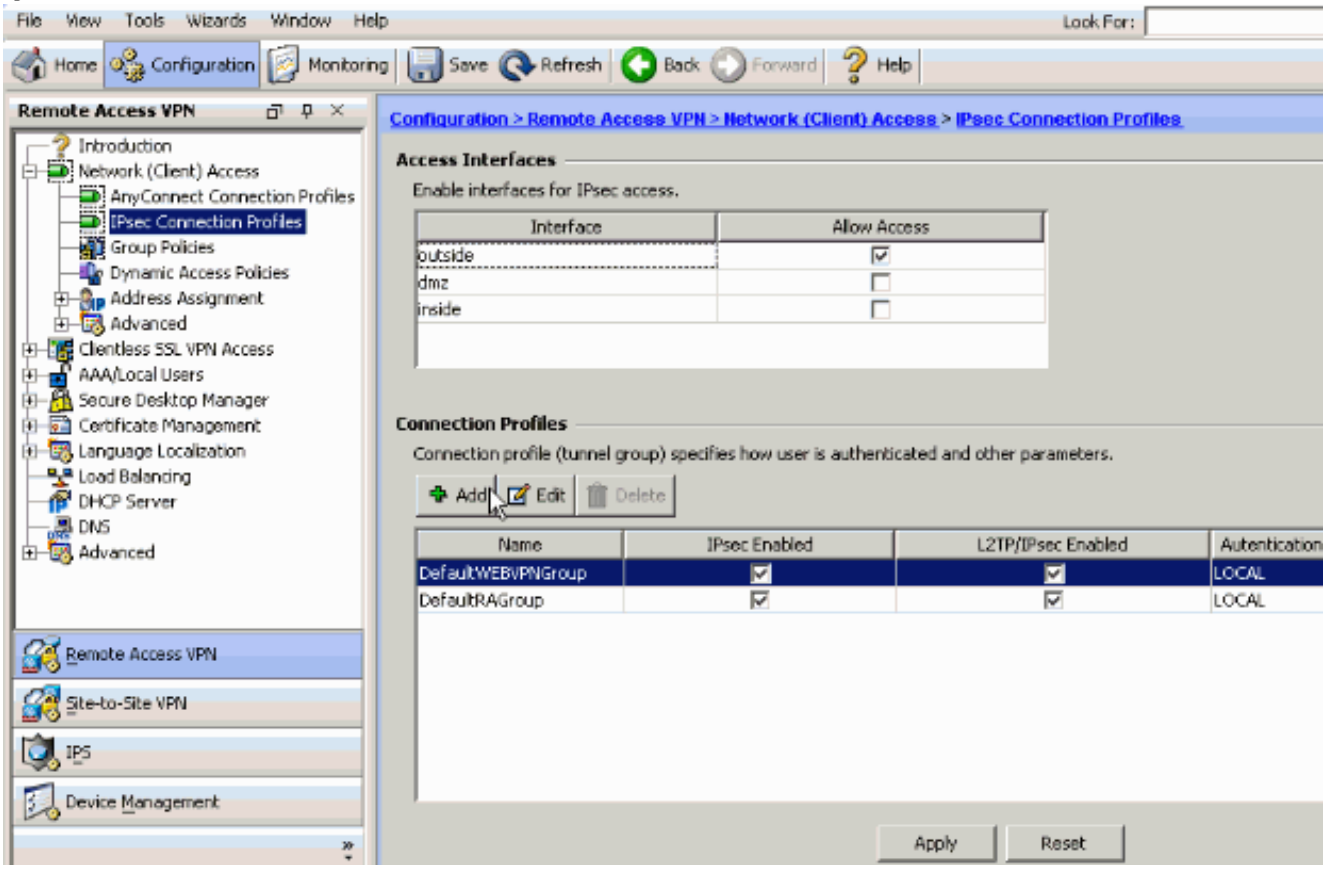
7. 转到 **VPN Policy** 并为用户“cisco123”添加静态/专用 IP 地址，如下所示。



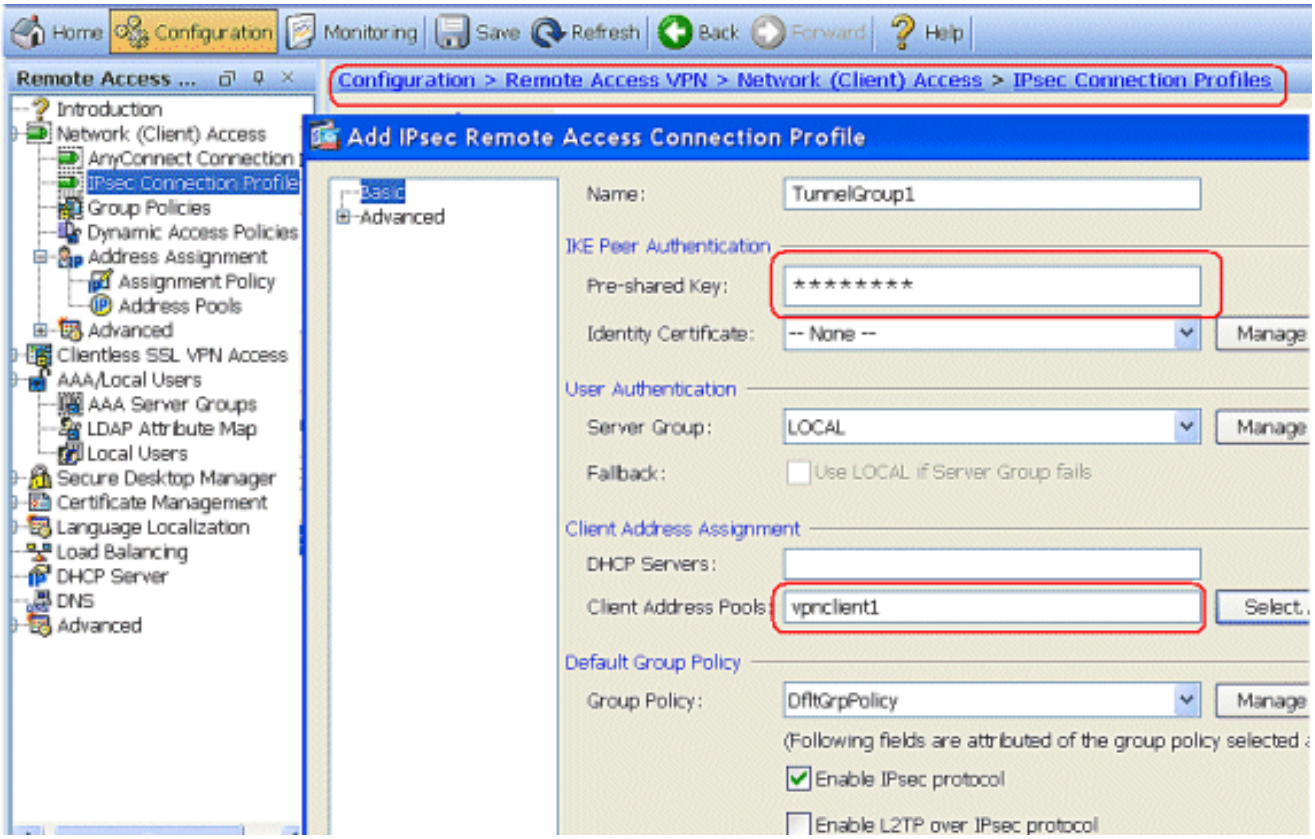
8. 选择 **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools** 并单击 Add 为 VPN 客户端用户添加 VPN 客户端。



9. 选择 **Configuration > Remote Access VPN > Network (Client) Access > IPSec Connection Profiles > Add** 以添加隧道组（例如，TunnelGroup1，Preshared key 为 cisco123），如下所示。

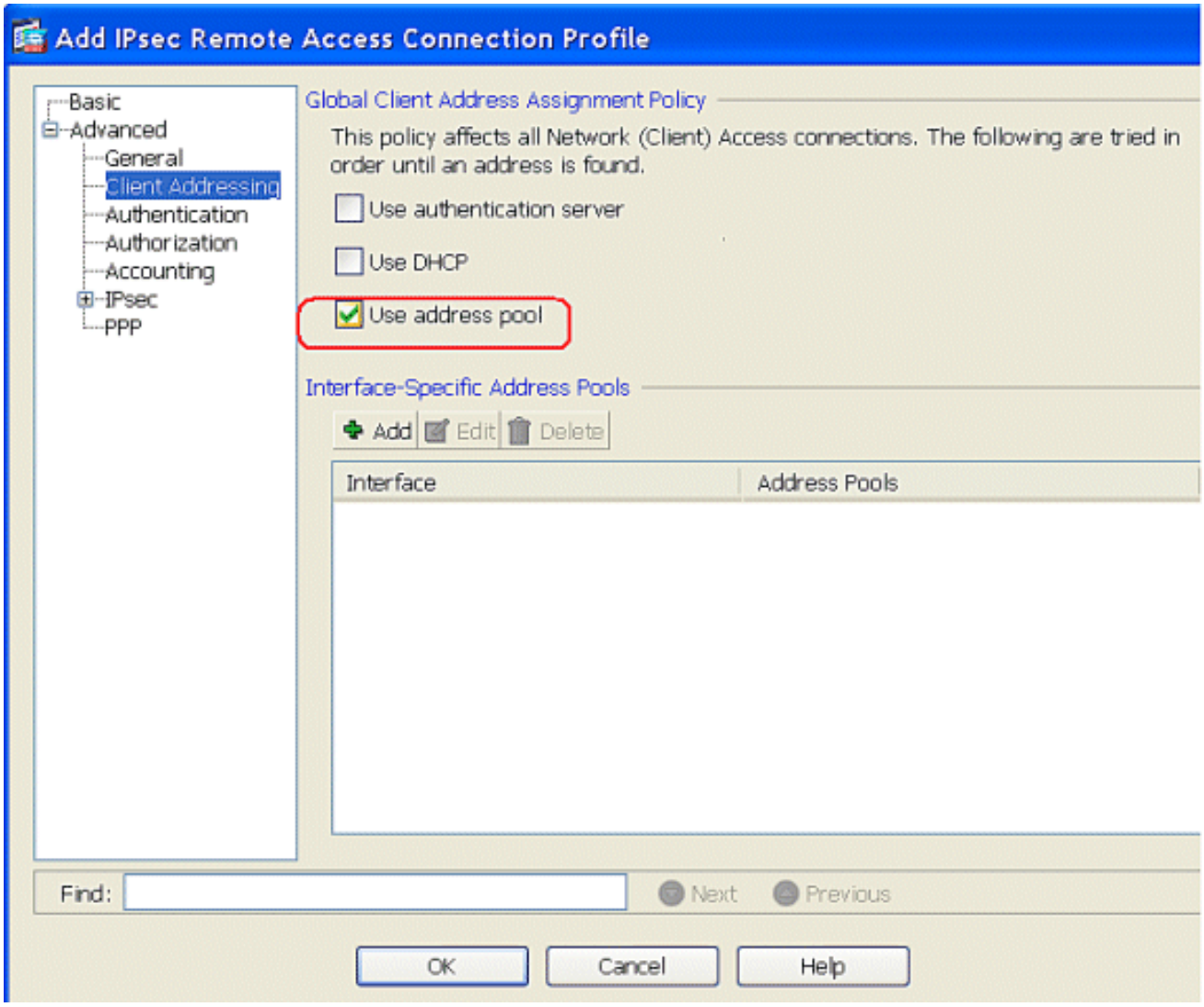


在 **Basic** 选项卡中，为 User Authentication 字段选择 LOCAL 作为 Server Group。选择 **vpnclient1** 作为 VPN 客户端用户的 Client Address Pools。



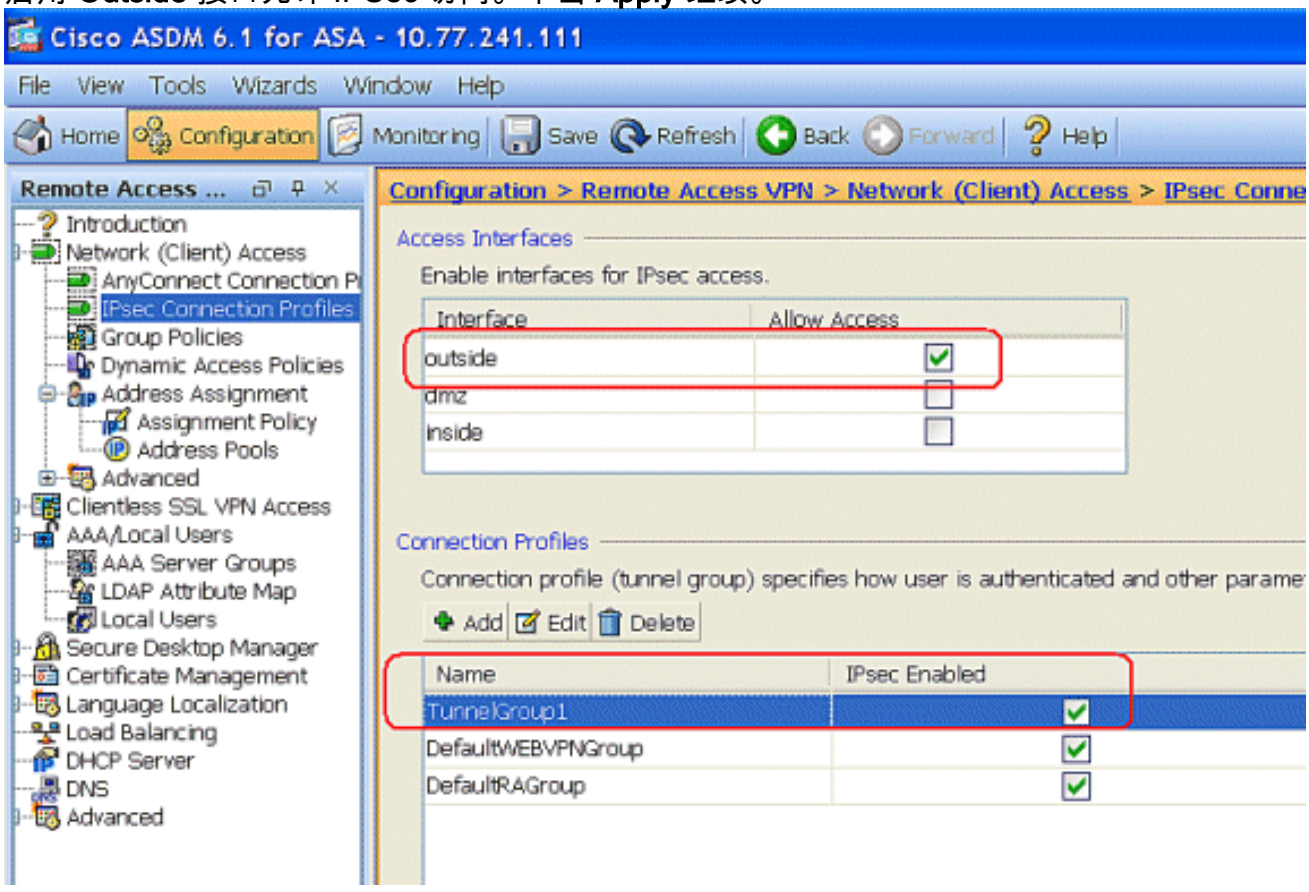
单击 **Ok**。

10. 选择 **Advanced > Client Addressing** 并选中 Use address pool 复选框，以便将 IP 地址分配至 VPN 客户端。**注意：** 确保 **Use authentication server** 和 Use DHCP 这两个复选框处于未选中状态。



单击 **Ok**。

11. 启用 **Outside** 接口允许 IPSec 访问。单击 **Apply** 继续。



使用 CLI 配置 ASA/PIX

完成以下步骤，以便通过命令行配置 DHCP 服务器向 VPN 客户端提供 IP 地址。有关所使用的每个命令的详细信息，请参阅配置远程接入 VPN 或 Cisco ASA 5500 系列自适应安全设备命令参考。

ASA 设备上的运行配置

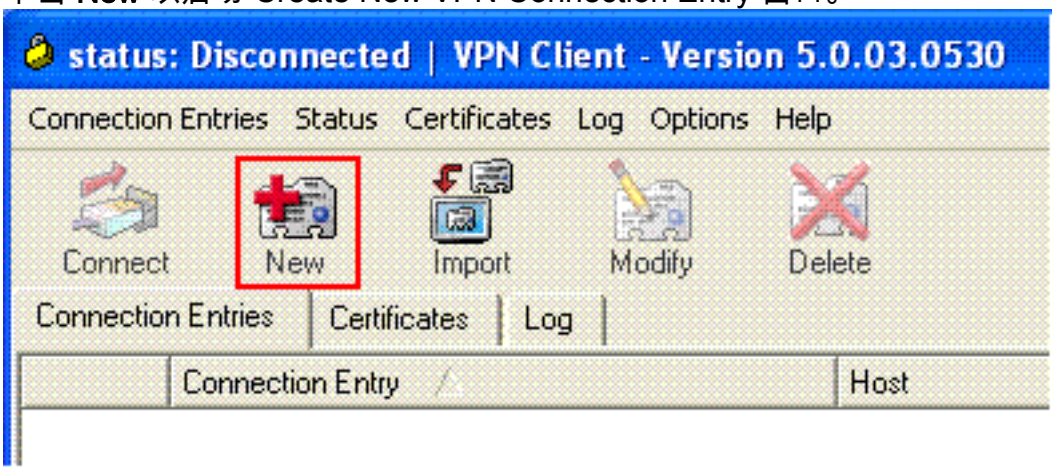
```
ASA# sh run
ASA Version 8.0(2)
!
!--- Specify the hostname for the Security Appliance.
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted
names ! !--- Configure the outside and inside
interfaces. interface Ethernet0/0 nameif inside
security-level 100 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/1 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface
Ethernet0/2 nameif DMZ security-level 50 ip address
192.168.10.2 255.255.255.0 !--- Output is suppressed.
passwd 2KFQnbNIdI.2KYOU encrypted boot system
disk0:/asa802-k8.bin ftp mode passive access-list 101
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0
255.255.255.0 pager lines 24 logging enable logging asdm
informational mtu inside 1500 mtu outside 1500 mtu dmz
1500 ip local pool vpnclient1 192.168.5.10-192.168.5.100
mask 255.255.255.0 no failover icmp unreachable rate-
limit 1 burst-size 1 !--- Specify the location of the
ASDM image for ASA to fetch the image for ASDM access.
asdm image disk0:/asdm-613.bin no asdm history enable
arp timeout 14400 global (outside) 1 192.168.1.5 nat
(inside) 0 access-list 101 nat (inside) 1 0.0.0.0
0.0.0.0 route outside 0.0.0.0 0.0.0.0 192.168.1.2 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
dynamic-access-policy-record DfltAccessPolicy 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 crypto
ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto dynamic-map outside_dyn_map 1 set transform-set
ESP-DES-SHA crypto map outside_map 1 ipsec-isakmp
dynamic outside_dyn_map !--- Specifies the interface to
be used with !--- the settings defined in this
configuration. crypto map outside_map interface outside
!--- PHASE 1 CONFIGURATION ---! !--- This configuration
uses ISAKMP policy 2. !--- The configuration commands
here define the Phase !--- 1 policy parameters that are
used. crypto isakmp enable outside crypto isakmp policy
2 authentication pre-share encryption des hash sha group
2 lifetime 86400 no crypto isakmp nat-traversal !---
Specifies that the IP address to the vpn clients are
assigned by the local and not by AAA or dhcp. The CLI
vpn-addr-assign local for VPN address assignment through
ASA is hidden in the CLI provided by show run command.
no vpn-addr-assign aaa no vpn-addr-assign dhcp telnet
timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! 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 ! group-policy DfltGrpPolicy
attributes vpn-tunnel-protocol IPSec webvpn group-policy
GroupPolicy1 internal !--- In order to identify remote
access users to the Security Appliance, !--- you can
also configure usernames and passwords on the device. !-
-- specify the IP address to assign to a particular
user, use the vpn-framed-ip-address command !--- in
username mode username cisco123 password
ffIRPGpDSOJh9YLq encrypted username cisco123 attributes
vpn-framed-ip-address 192.168.5.1 255.255.255.0 !---
Create a new tunnel group and set the connection !---
type to remote-access. tunnel-group TunnelGroup1 type
remote-access tunnel-group TunnelGroup1 general-
attributes address-pool vpnclient1 !--- Enter the pre-
shared-key to configure the authentication method.
tunnel-group TunnelGroup1 ipsec-attributes pre-shared-
key * prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end
ASA#
```

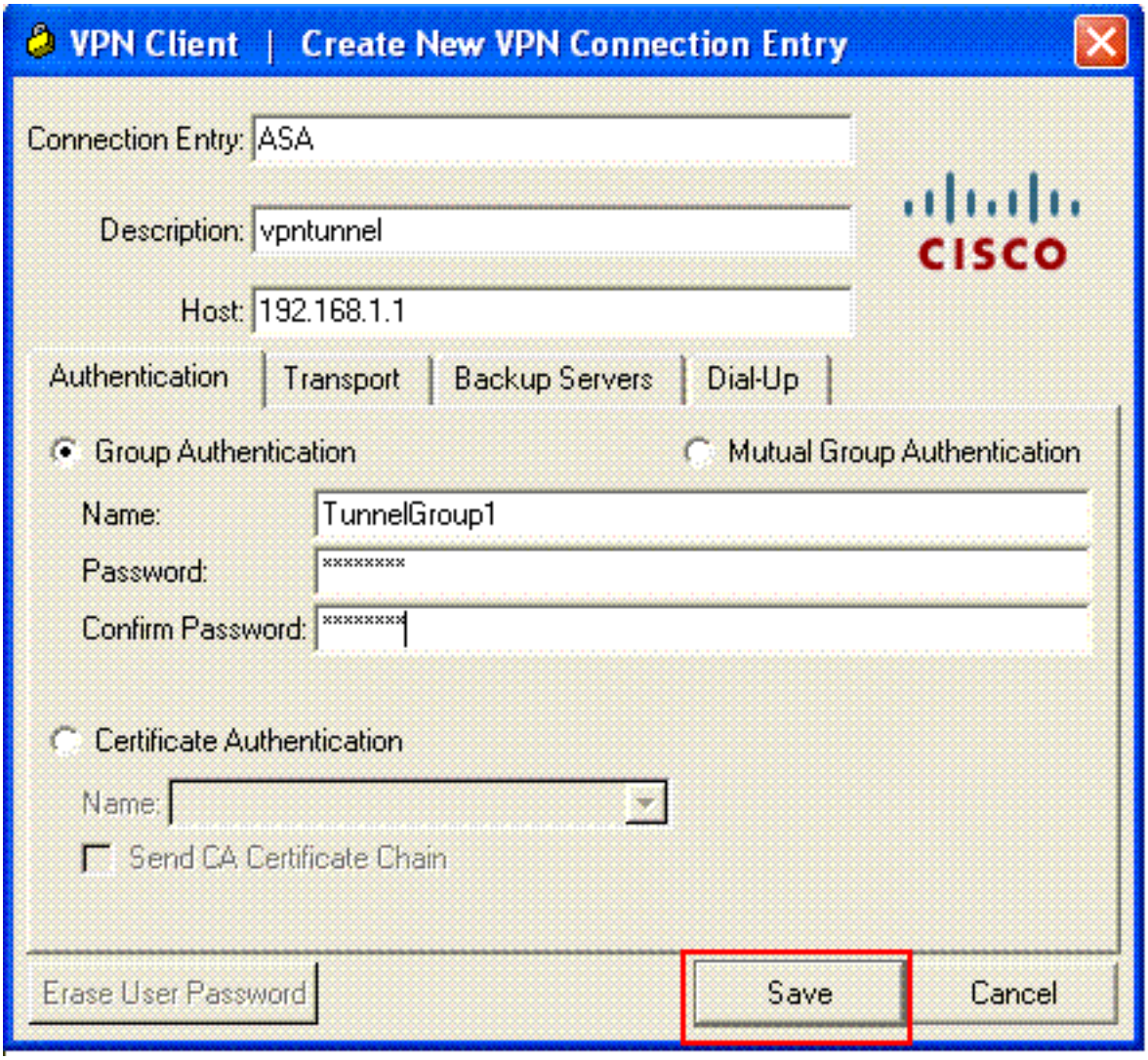
Cisco VPN 客户端配置

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

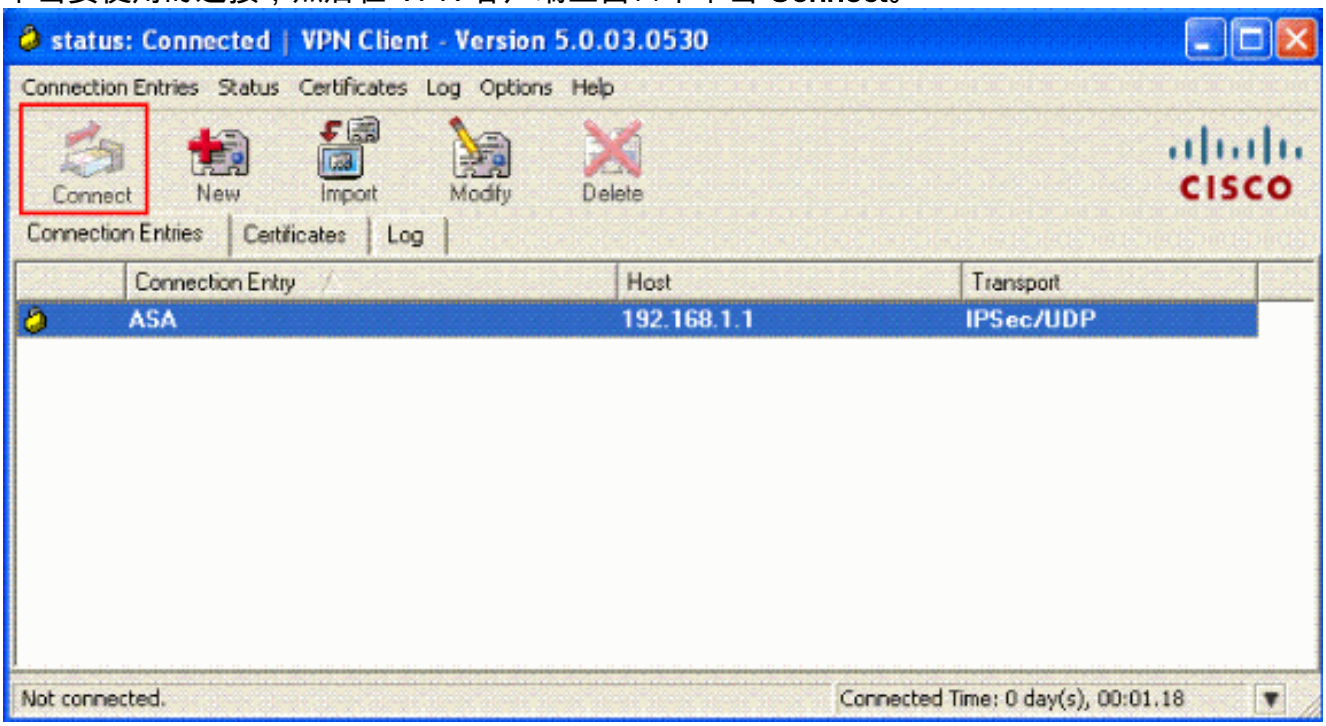
1. 选择**开始 > 程序 > Cisco Systems VPN 客户端 > VPN 客户端**。
2. 单击 **New** 以启动 Create New VPN Connection Entry 窗口。



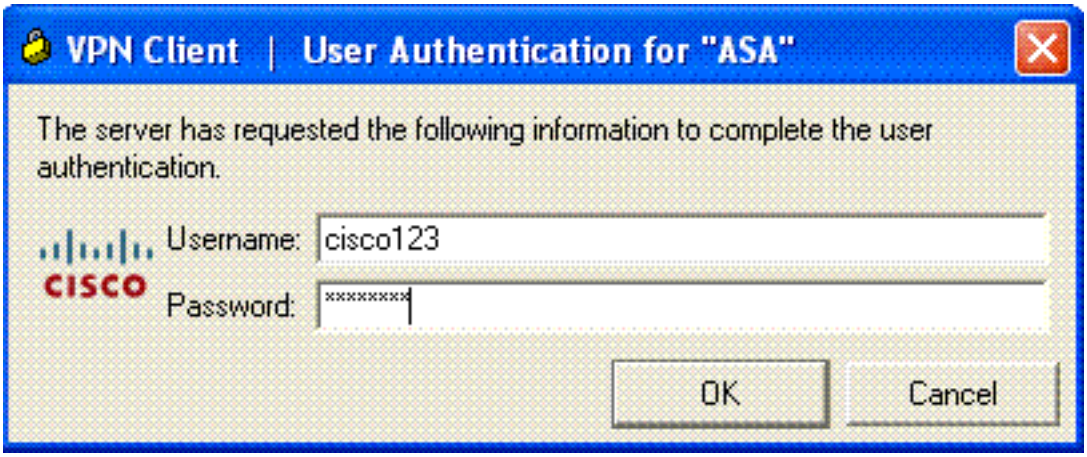
3. 填写新连接的详细信息。输入 Connection Entry 的名称与说明。在 Host 框中输入 **ASA 的外部 IP 地址**。然后按照 ASA 中的配置输入 VPN 隧道组名称 (TunnelGroup1) 和口令（预共享密钥 - cisco123）。单击 **Save**。



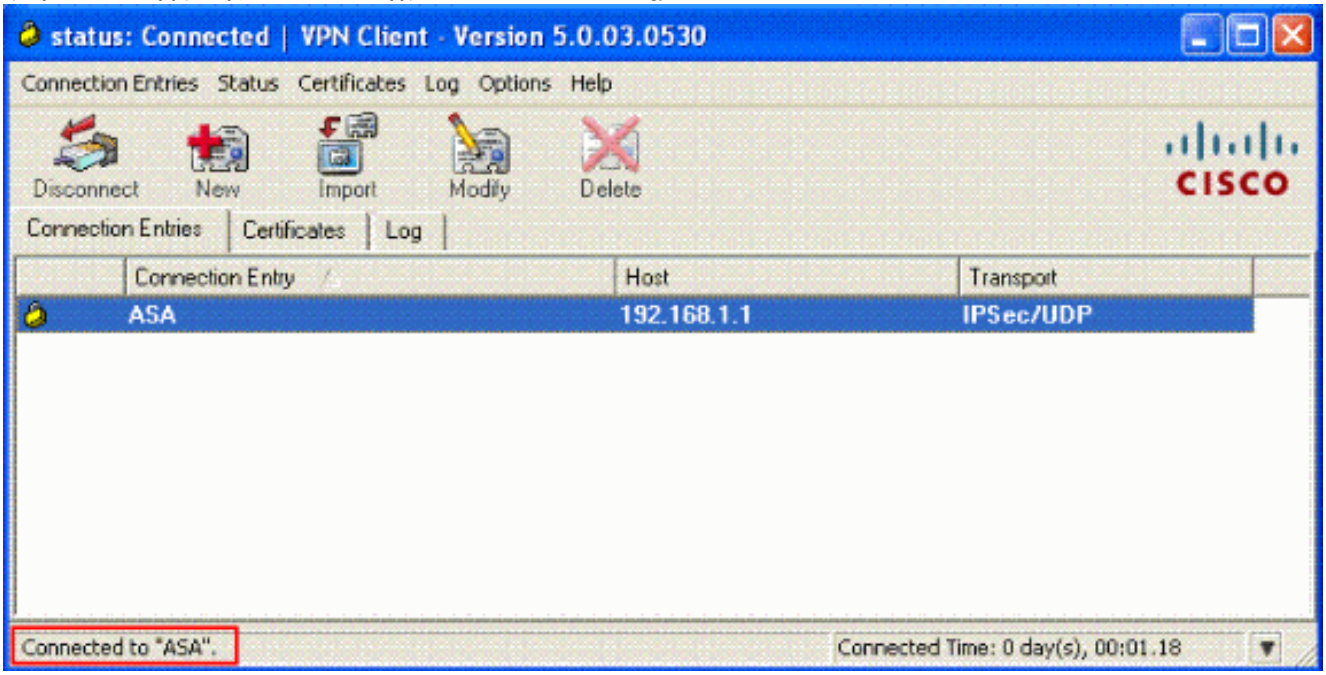
4. 单击要使用的连接，然后在 VPN 客户端主窗口中单击 **Connect**。



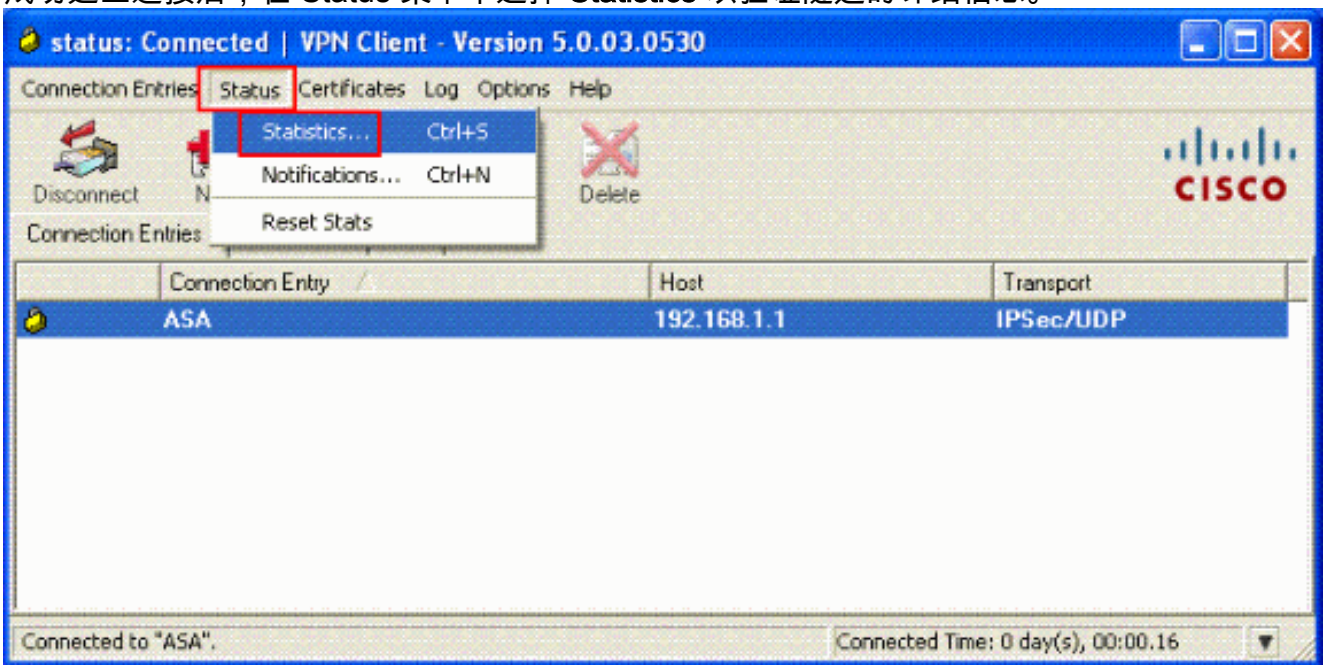
5. 出现提示时，输入 **Username:cisco123** 和 Password:**cisco123**（按照上面的 ASA 扩展验证配置进行输入），然后单击 OK 以连接到远程网络。



6. 现在 VPN 客户端将与中心站点的 ASA 建立连接。



7. 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。



验证

显示命令

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 SA 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。此外本部分还提供了 debug 输出示例。

注意： 有关远程访问 IPSec VPN 故障排除的详细信息，请参阅最常用的 L2L 和远程访问 IPSec VPN 故障排除解决方案。

清除安全关联

进行故障排除时，请务必在做出更改后清除现有的安全关联。在 PIX 的特权模式下，使用以下命令：

- **clear [crypto] ipsec sa** - 删除活动 IPsec SA。关键字 crypto 是可选的。
- **clear [crypto] isakmp sa** - 删除活动 IKE SA。关键字 crypto 是可选的。

故障排除命令

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。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **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。

相关信息

- Cisco ASA 5500 系列自适应安全设备支持页
- Cisco ASA 5500 系列自适应安全设备命令参考
- Cisco PIX 500 系列安全设备支持页
- Cisco PIX 500 系列安全设备命令参考
- Cisco 自适应安全设备管理器
- IPsec 协商/IKE 协议支持页
- Cisco VPN 客户端支持页
- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- 请求注解 (RFC)

- 技术支持和文档 - Cisco Systems