ASA 8.X:通过隧道默认网关路由SSL VPN流量配置示例

目录

简介

本文档介绍如何配置自适应安全设备(ASA)，以通过隧道默认网关(TDG)路由SSL VPN流量。 当您使用tunneled选项创建默认路由时，来自隧道的所有流量都将发送到此路由，该隧道终止于ASA上，无法使用已获知或静态路由进行路由。对于从隧道涌出的流量，此路由会覆盖任何其他已配置或已获取的默认路由。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 在8.x版上运行的ASA
- 思科SSL VPN客户端(SVC)1.x**注意**：从思科软件下载（仅限注册客户）下载SSL VPN客户端软件包(sslclient-win*.pkg)。 将 SVC 复制到 ASA 上的闪存中。SVC需要下载到远程用户计算机，以便与ASA建立SSL VPN连接。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本8.x的Cisco 5500系列ASA

- 适用于 Windows 1.1.4.179 的 Cisco SSL VPN Client 版本
- 运行 Windows 2000 Professional 或 Windows XP 的 PC
- Cisco 自适应安全设备管理器 (ASDM) 版本 6.1(5)

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。

背景信息

SSL VPN 客户端 (SVC) 是一种 VPN 隧道技术，这种技术让远程用户可以利用 IPsec VPN 客户端的优势，而无需网络管理员在远程计算机上安装和配置 IPsec VPN 客户端。SVC 使用远程计算机上已经具有的 SSL 加密以及安全设备的 WebVPN 登录和身份验证。

在当前场景中，有一个SSL VPN客户端通过SSL VPN隧道连接到ASA后面的内部资源。拆分隧道未启用。当SSL VPN客户端连接到ASA时，所有数据都将通过隧道传输。除了访问内部资源外，主要标准是通过默认隧道网关(DTG)路由此隧道流量。

您可以为隧道流量定义单独的默认路由以及标准默认路由。ASA接收的未加密流量（没有静态或已获取路由）通过标准默认路由路由路由。ASA收到的加密流量（没有静态或已获知的路由）将通过隧道默认路由传递到定义的DTG。

要定义隧道默认路由，请使用以下命令：

```
route <if_name> 0.0.0.0 0.0.0.0 <gateway_ip> tunneled
```

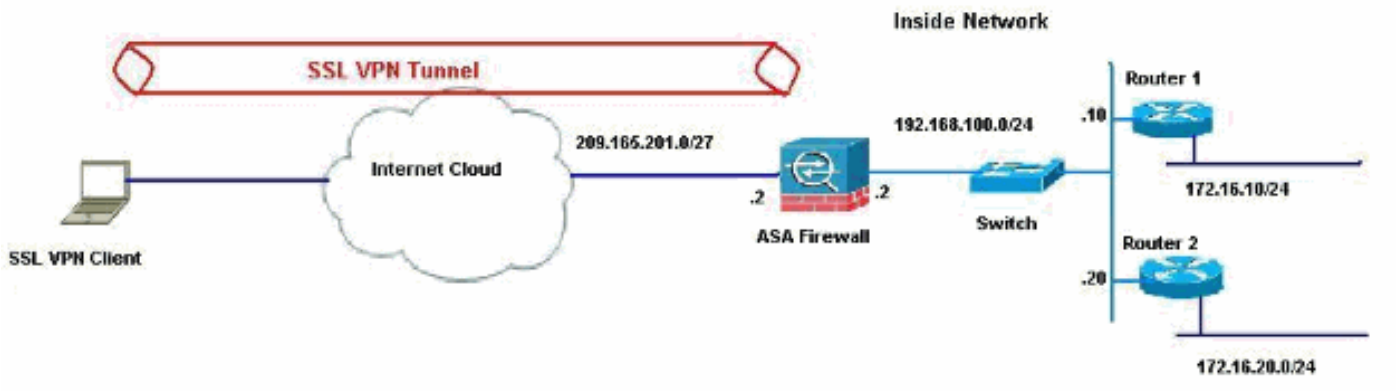
配置

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：



在本示例中，SSL VPN客户端通过隧道访问ASA的内部网络。为内部网络以外的目的地传输的流量也通过隧道传输，因为没有配置拆分隧道，并通过TDG(192.168.100.20)进行路由。

在将数据包路由到TDG（在本例中为路由器2）后，它执行地址转换以将这些数据包提前路由到Internet。有关将路由器配置为互联网网关的详细信息，请参阅如何在非思科电缆调制解调器后配置思科路由器。

使用 ASDM 6.1(5) 配置 ASA

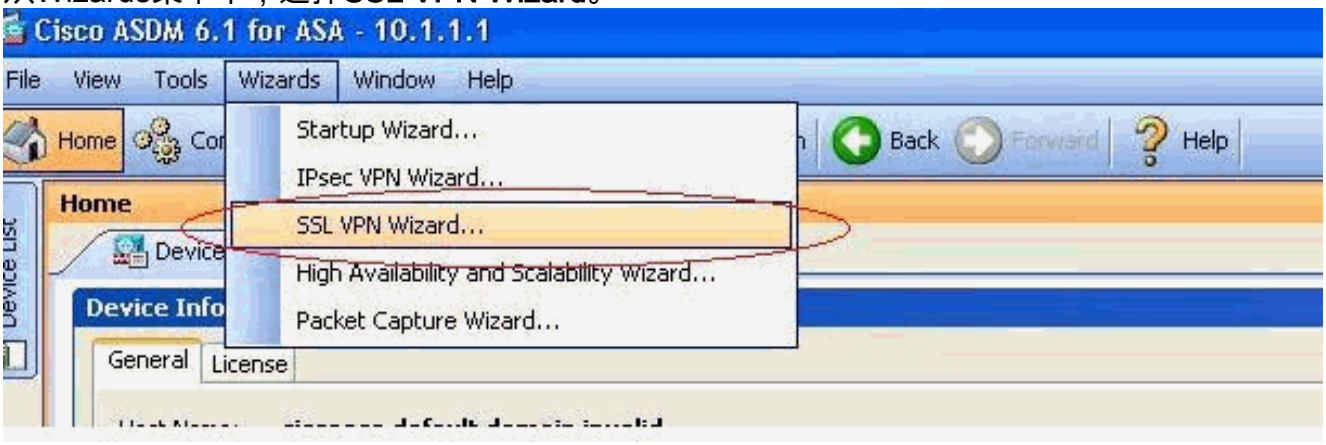
本文档假设基本配置（如接口配置）已完成且工作正常。

注意：有关如何允许ASDM配置ASA的信息，请参阅允许ASDM访问HTTPS。

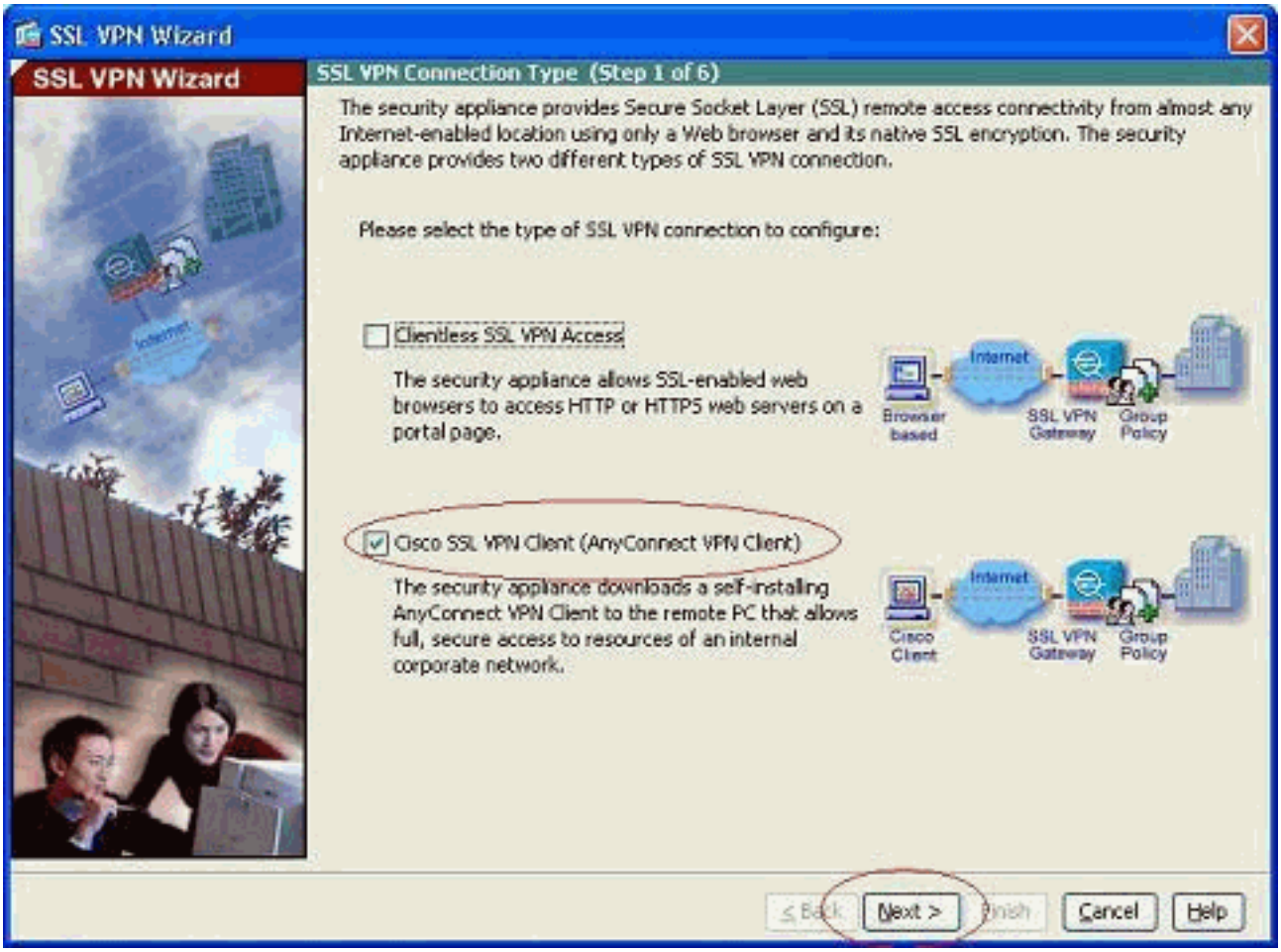
注意：除非更改端口号，否则无法在同一ASA接口上启用WebVPN和ASDM。有关详细信息，请参阅在相同 ASA 接口上同时启用 Webvpn 和 ASDM。

要使用SSL VPN向导配置SSL VPN，请完成以下步骤。

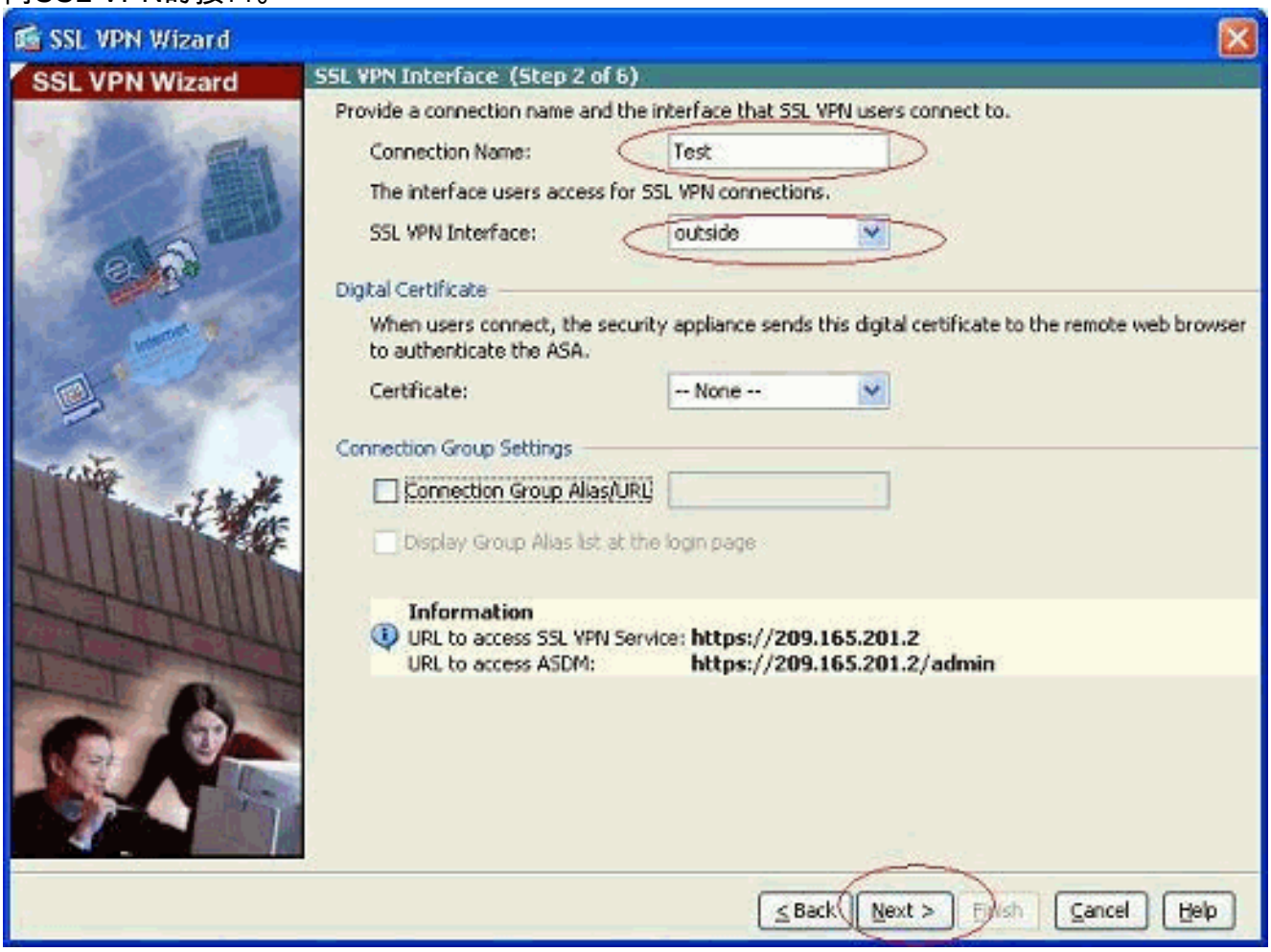
1. 从Wizards菜单中，选择**SSL VPN Wizard**。



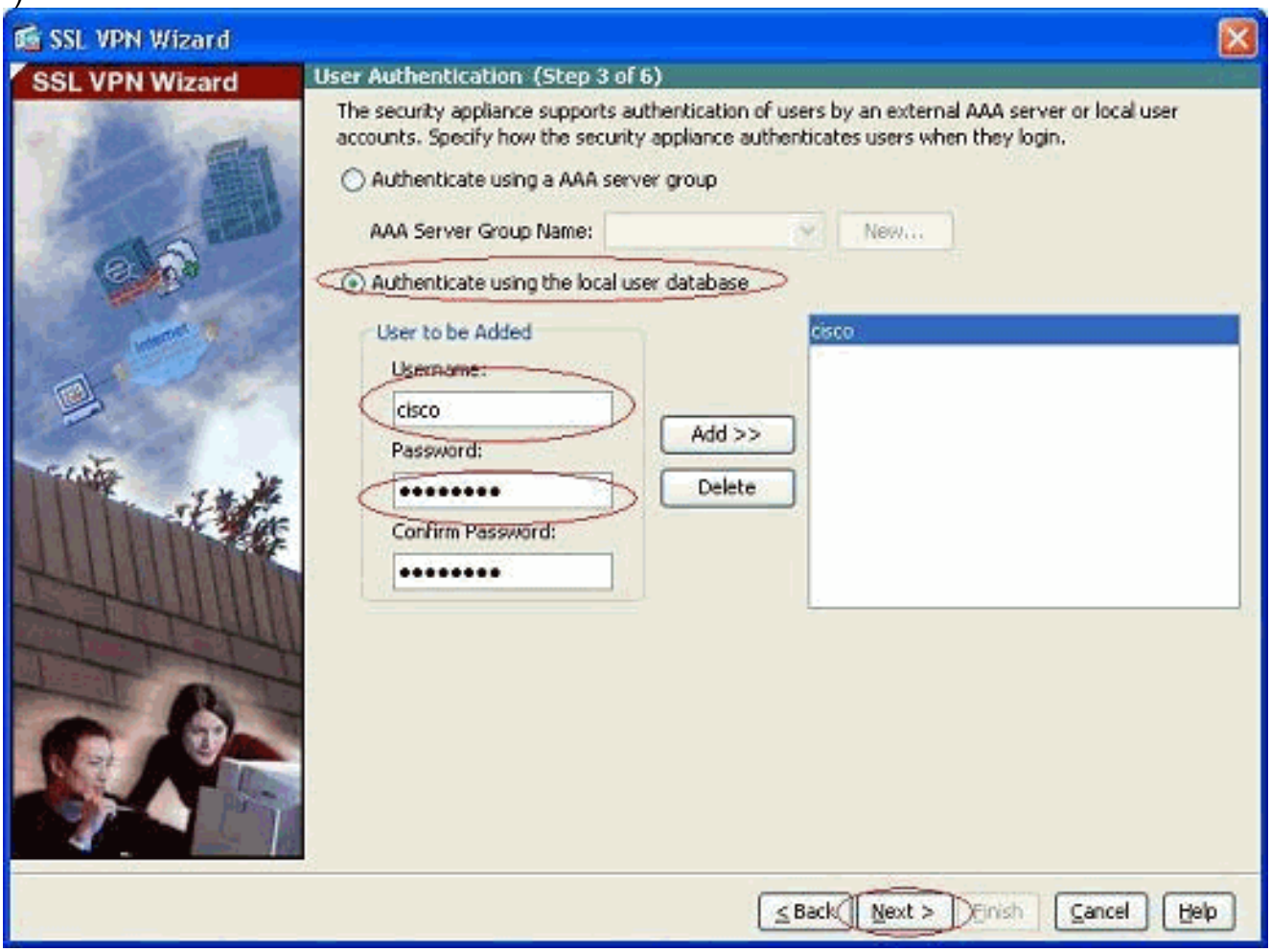
2. 单击“**Cisco SSL VPN Client(Cisco SSL VPN Client)**”复选框，然后单击“**Next(下一步)**”。



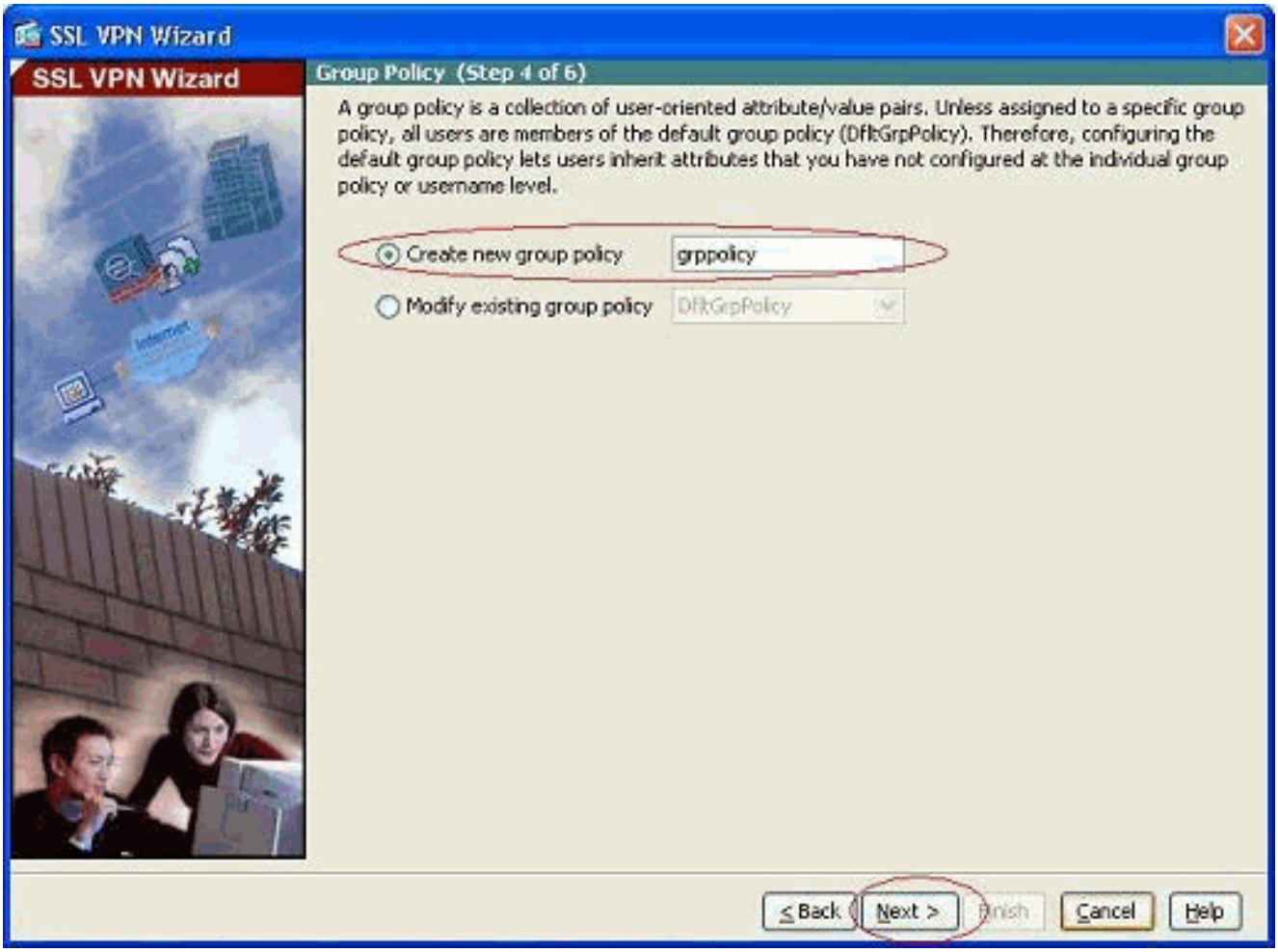
3. 在Connection Name字段中输入连接的名称，然后从SSL VPN接口下拉列表中选择用户用于访问SSL VPN的接口。



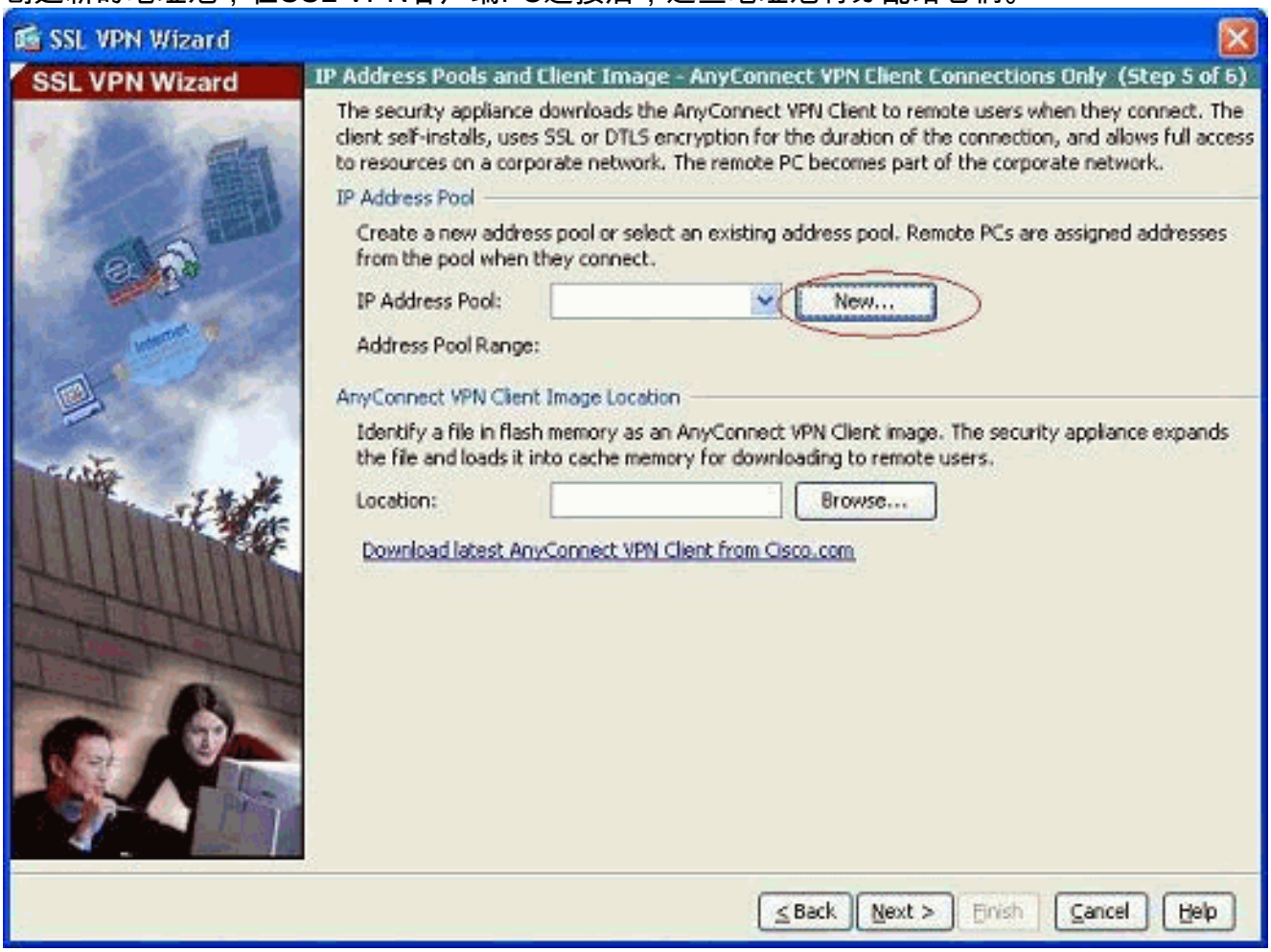
4. 单击 **Next**。
5. 选择身份验证模式，然后单击**Next**。（本示例使用本地身份验证。
   ）



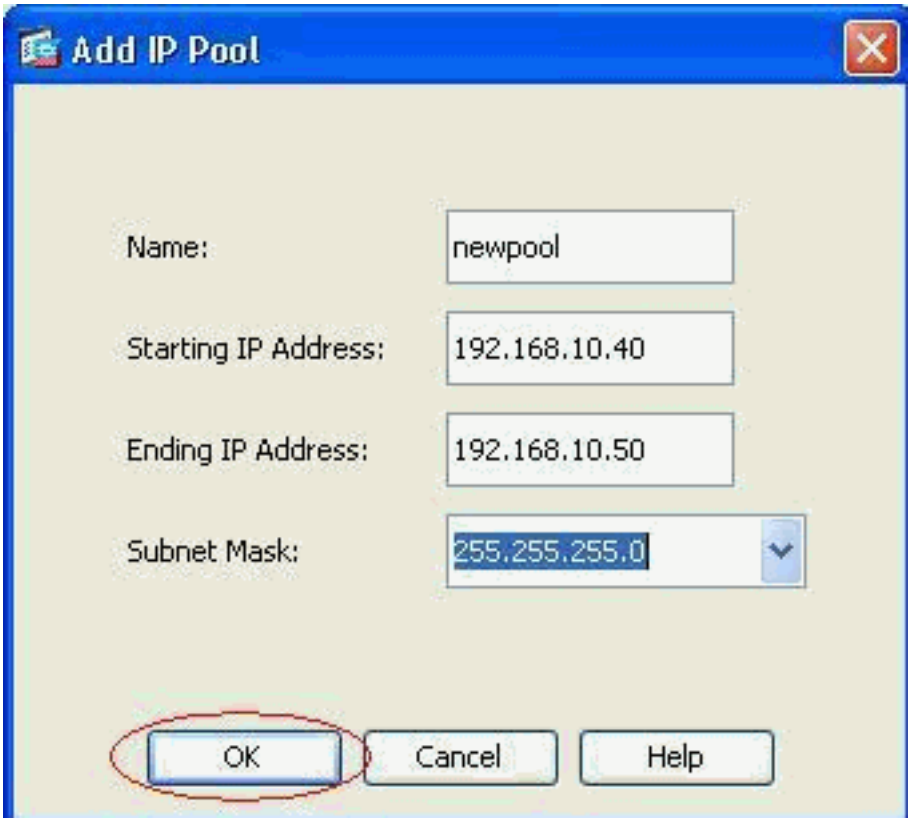
6. 创建除现有默认组策略之外的新组策略。



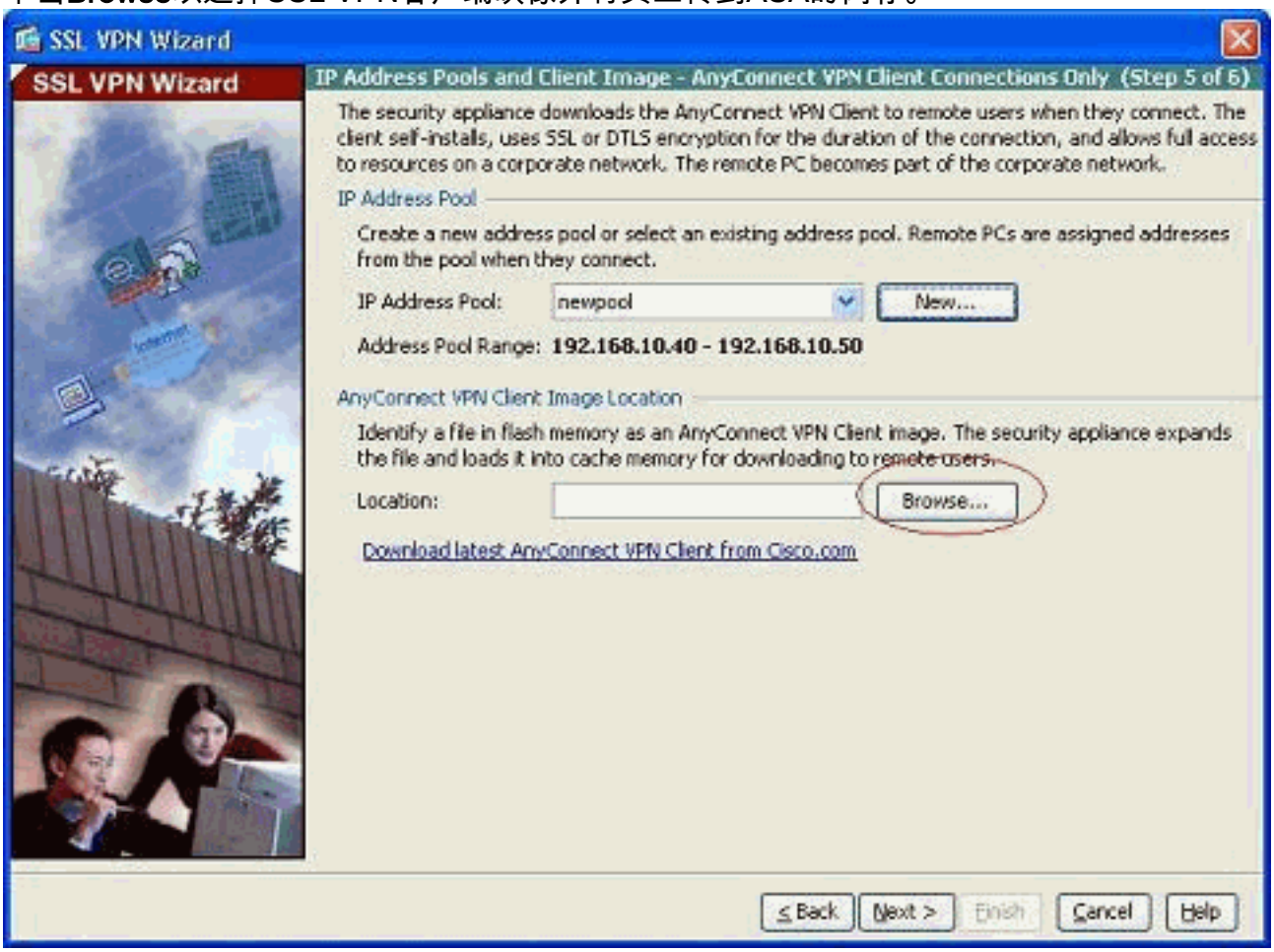
7. 创建新的地址池，在SSL VPN客户端PC连接后，这些地址池将分配给它们。



名称newpool已创建范围为192.168.10.40-192.168.10.50的池。

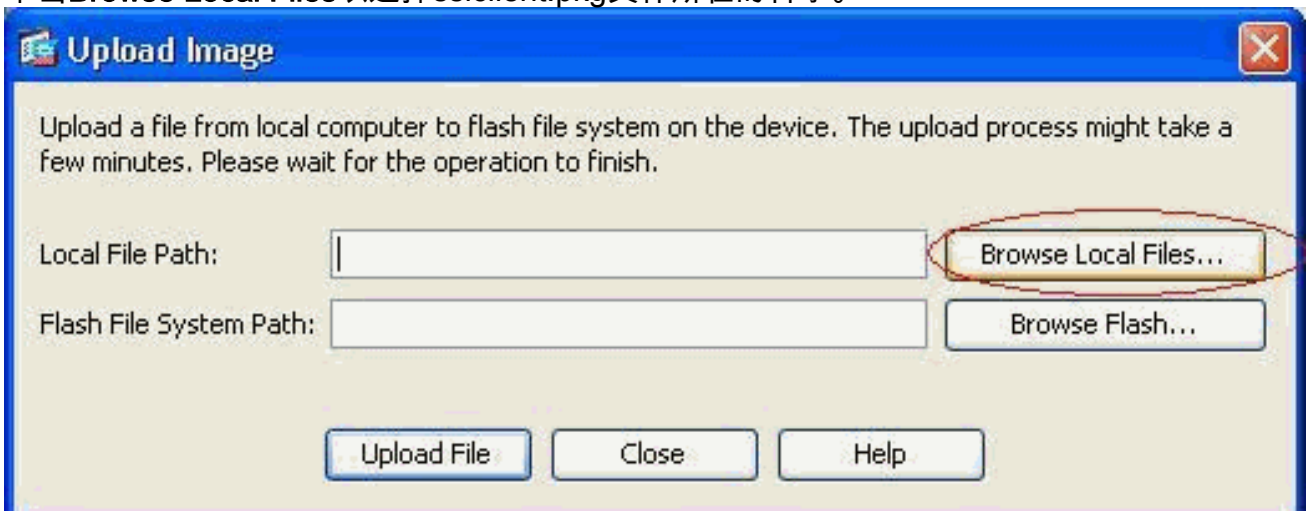


8. 单击**Browse**以选择SSL VPN客户端映像并将其上传到ASA的闪存。

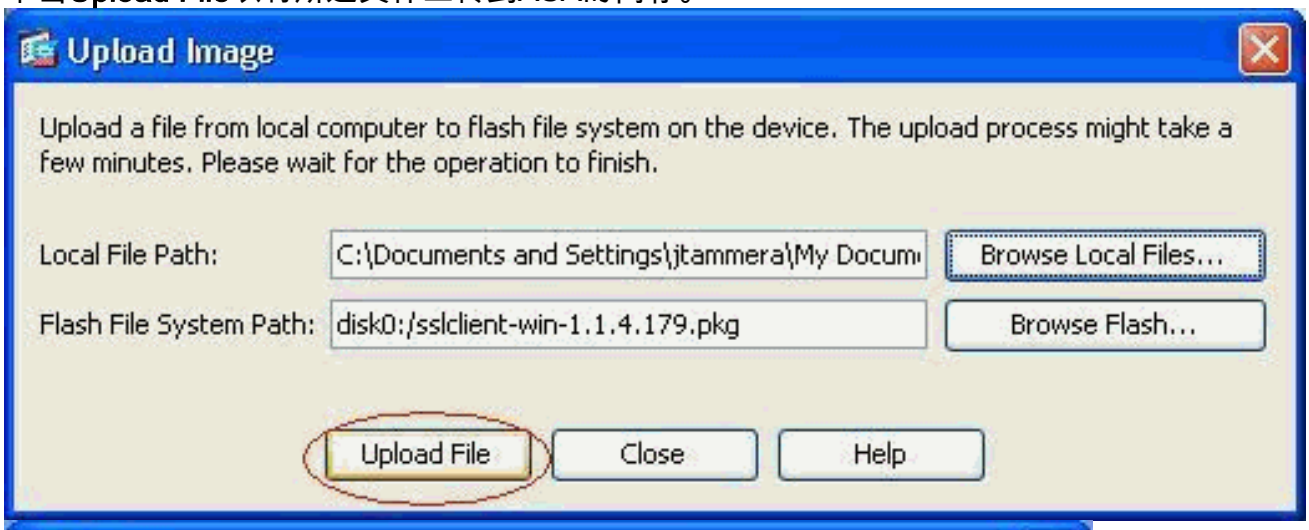


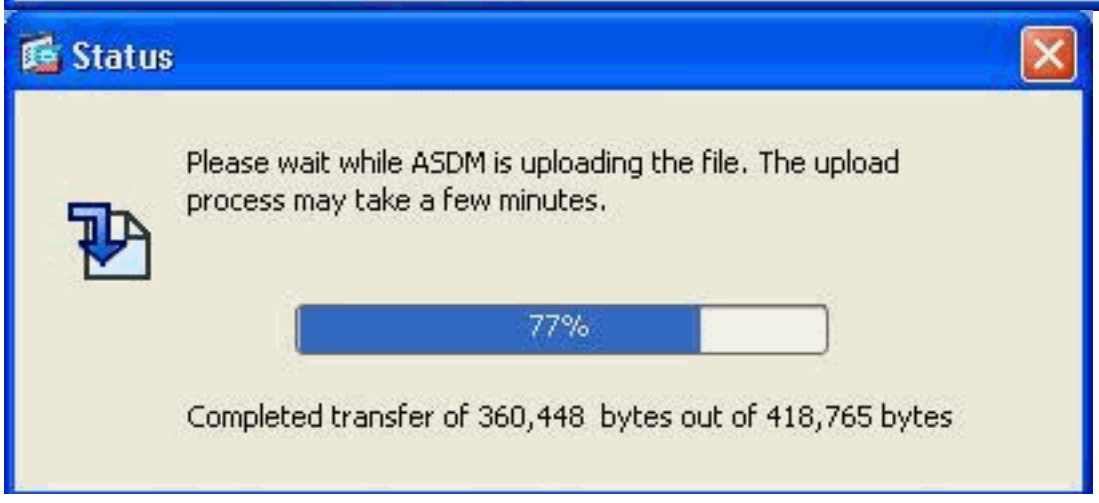
9. 单击**Upload**以设置计算机本地目录的文件路径。

10. 单击**Browse Local Files**以选择sslclient.pkg文件所在的目录。

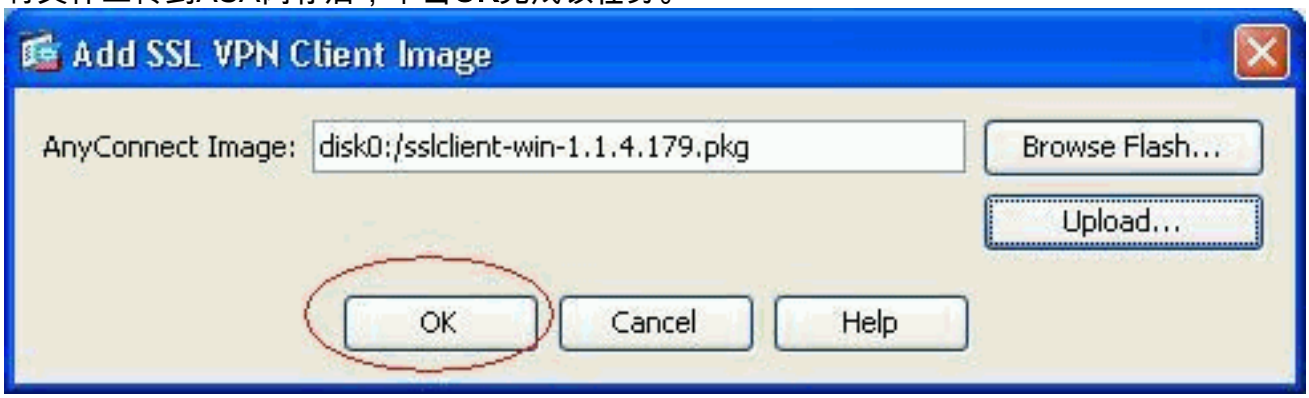


11. 单击**Upload File**以将所选文件上传到ASA的闪存。

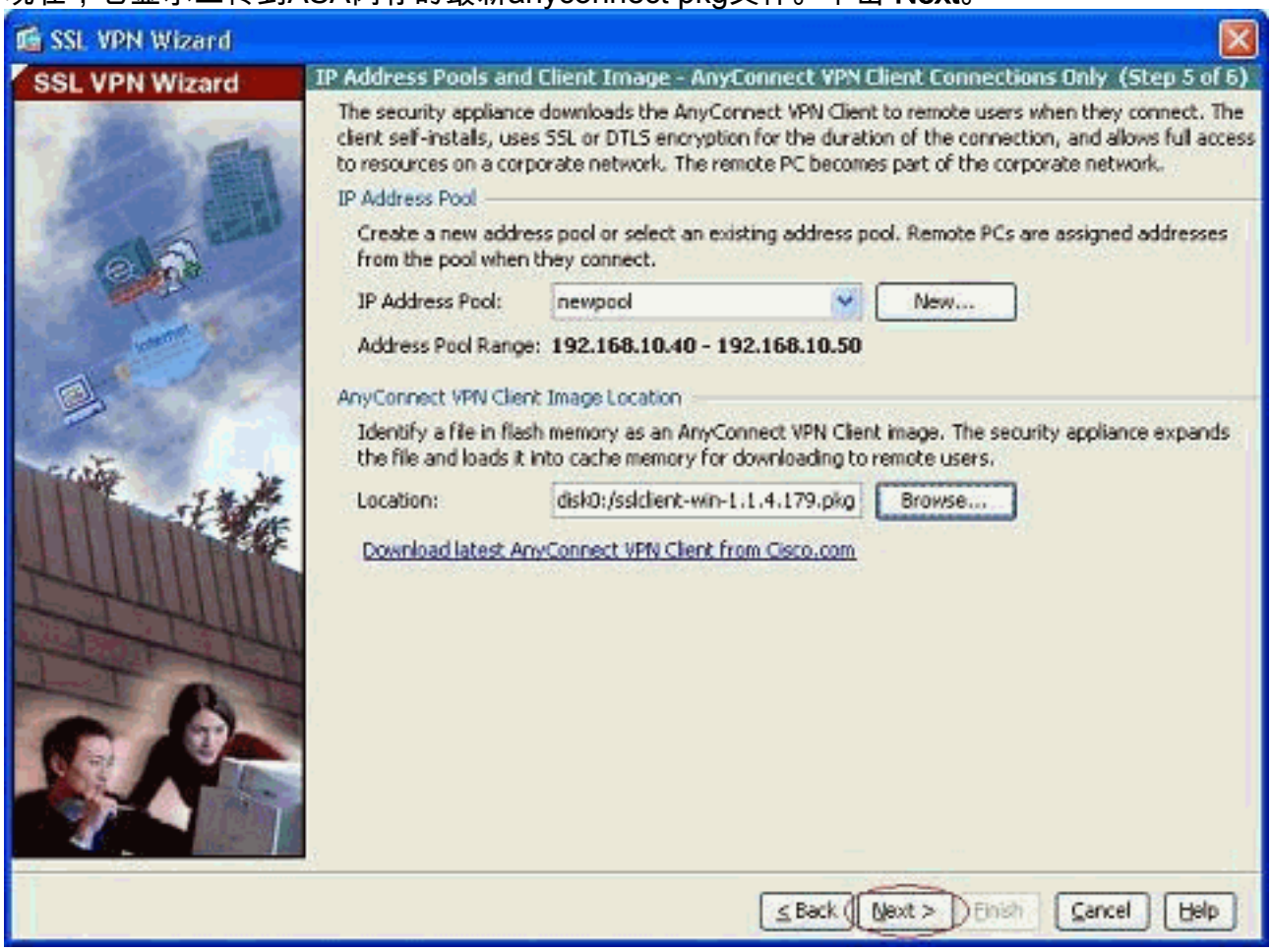




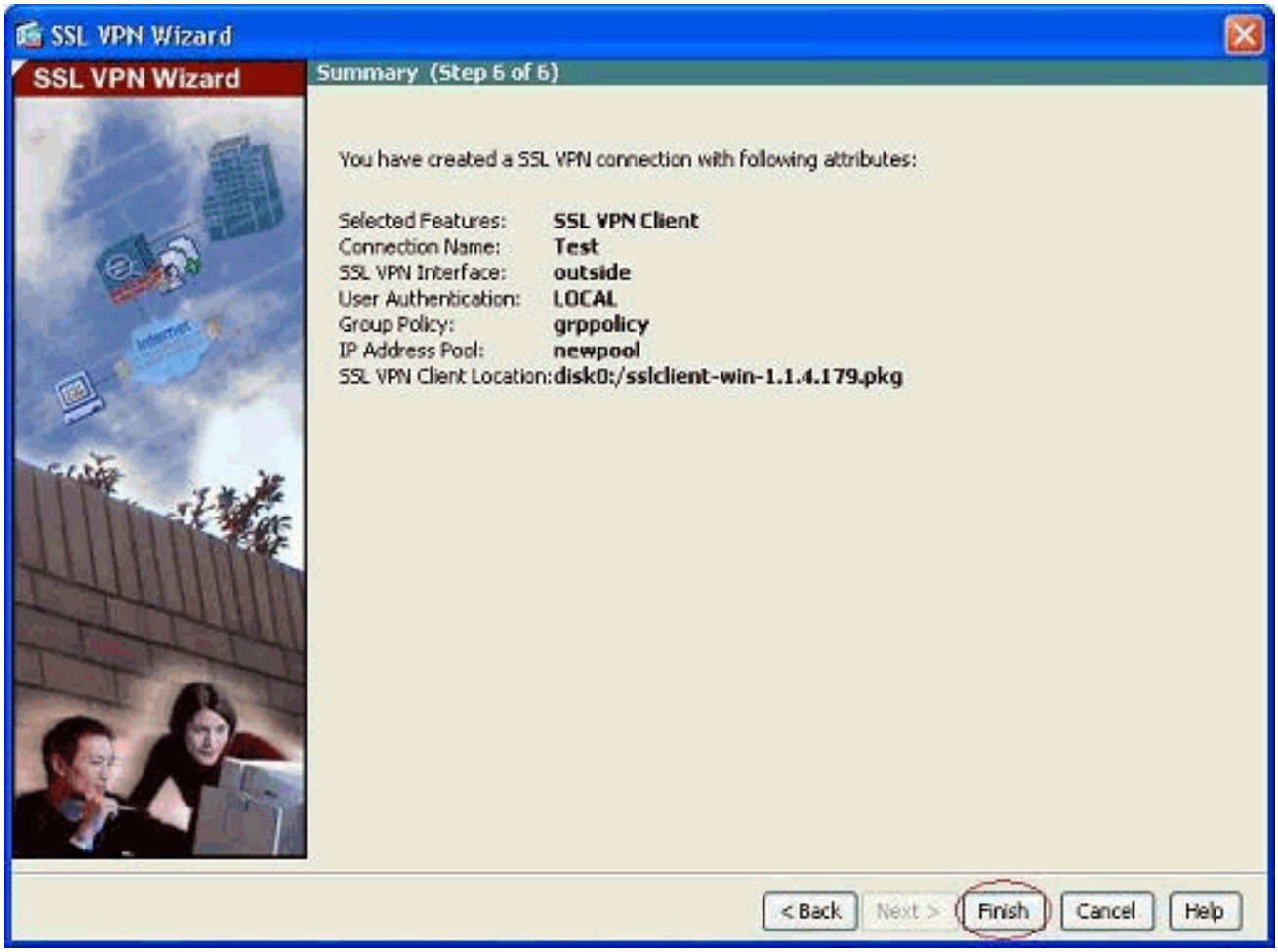
12. 将文件上传到ASA闪存后，单击**OK**完成该任务。



13. 现在，它显示上传到ASA闪存的最新anyconnect pkg文件。单击 **Next**。



14. SSL VPN客户端配置摘要如图所示。单击**Finish**完成向导。



ASDM中显示的配置主要涉及SSL VPN客户端向导配置。

在CLI中，您可以观察一些其他配置。完整的CLI配置如下所示，重要命令已突出显示。

ciscoasa

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(4)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.224
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.100.2 255.255.255.0
!
interface Ethernet0/2
 nameif manage
 security-level 0
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/3
 shutdown
```

```
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list nonat extended permit ip 192.168.100.0
255.255.255.0 192.168.10.0 255.255.255.0
access-list nonat extended permit ip 192.168.10.0
255.255.255.0 192.168.100.0 255.255.255.0
!--- ACL to define the traffic to be exempted from NAT.
no pager logging enable logging asdm informational mtu
outside 1500 mtu inside 1500 mtu manage 1500 !---
Creating IP address block to be assigned for the VPN
clients ip local pool newpool 192.168.10.40-
192.168.10.50 mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-615.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
!--- The traffic permitted in "nonat" ACL is exempted
from NAT. nat (inside) 1 192.168.100.0 255.255.255.0
route outside 0.0.0.0 0.0.0.0 209.165.201.1 1
!--- Default route is configured through "inside"
interface for normal traffic. route inside 0.0.0.0
0.0.0.0 192.168.100.20 tunneled
!--- Tunneled Default route is configured through
"inside" interface for encrypted traffic ! 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
!--- Configuring the ASA as HTTP server. http 10.1.1.0
255.255.255.0 manage
!--- Configuring the network to be allowed for ASDM
access. ! !--- Output is suppressed ! 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 ! !--- Output suppressed !
webvpn
 enable outside
!--- Enable WebVPN on the outside interface svc image
disk0:/sslclient-win-1.1.4.179.pkg 1
!--- Assign the AnyConnect SSL VPN Client image to be
used svc enable
!--- Enable the ASA to download SVC images to remote
computers group-policy grppolicy internal
!--- Create an internal group policy "grppolicy" group-
policy grppolicy attributes
 VPN-tunnel-protocol svc
!--- Specify SSL as a permitted VPN tunneling protocol !
username cisco password ffIRPGpDSOJh9YLq encrypted
privilege 15
!--- Create a user account "cisco" tunnel-group Test
type remote-access
!--- Create a tunnel group "Test" with type as remote
access tunnel-group Test general-attributes
 address-pool newpool
!--- Associate the address pool vpnpool created default-
group-policy grppolicy
!--- Associate the group policy "clientgroup" created
prompt hostname context
Cryptochecksum:1b247197c8ff70ee4432c13fb037854e : end
ciscoasa#
```

验证

本节中提供的命令可用于检验此配置。

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 webvpn svc** — 显示存储在ASA闪存中的SVC映像。
- **show vpn-sessiondb svc — 显示有关当前 SSL 连接的信息。**

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 思科5500系列自适应安全设备支持
- 单臂路由器上用于公共 Internet 的 PIX/ASA 和 VPN 客户端配置示例
- 在 ASA 上用 ASDM 配置 SSL VPN Client (SVC) 的示例
- 技术支持和文档 - Cisco Systems