ASA 8.X: Ejemplo de Configuración de Ruteo del Tráfico SSL VPN a través de la Gateway Predeterminada Tunelizada

Contenido

Introducción

Este documento describe cómo configurar Adaptive Security Appliance (ASA) para rutear el tráfico SSL VPN a través de la gateway predeterminada tunelizada (TDG). Cuando crea una ruta predeterminada con la opción tunelizada, todo el tráfico de un túnel que termina en el ASA que no se puede rutear usando rutas aprendidas o estáticas se envía a esta ruta. Para el tráfico que emerge de un túnel, esta ruta invalida cualquier otra ruta predeterminada configurada o aprendida.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- ASA que se ejecuta en la versión 8.x
- Cisco SSL VPN Client (SVC) 1.x**Nota:** Descargue el paquete SSL VPN Client (sslclient-win*.pkg) de Cisco Software Download (sólo clientes registrados) . Copie el SVC a la memoria flash en el ASA. El SVC debe descargarse en los equipos de usuario remotos para establecer la conexión VPN SSL con el ASA.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 5500 Series ASA que ejecuta la versión de software 8.x
- Cisco SSL VPN Client versión para Windows 1.1.4.179
- PC que ejecuta Windows 2000 Professional o Windows XP
- Versión 6.1(5) de Cisco Adaptive Security Device Manager (ASDM)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

SSL VPN Client (SVC) es una tecnología de tunelación VPN que ofrece a los usuarios remotos las ventajas de un cliente VPN IPSec sin necesidad de que los administradores de red instalen y configuren clientes VPN IPSec en equipos remotos. El SVC utiliza el cifrado SSL que ya está presente en el equipo remoto, así como el inicio de sesión WebVPN y la autenticación del dispositivo de seguridad.

En el escenario actual, hay un cliente SSL VPN que se conecta a los recursos internos detrás del ASA a través del túnel SSL VPN. El túnel dividido no está habilitado. Cuando el cliente SSL VPN está conectado al ASA, todos los datos serán tunelados. Además de acceder a los recursos internos, el criterio principal es enrutar este tráfico tunelizado a través de la puerta de enlace tunelizada predeterminada (DTG).

Puede definir una ruta predeterminada independiente para el tráfico tunelizado junto con la ruta predeterminada estándar. El tráfico no cifrado recibido por el ASA, para el cual no hay ruta estática o aprendida, se rutea a través de la ruta predeterminada estándar. El tráfico cifrado recibido por el ASA, para el cual no hay ruta estática o aprendida, se pasará al DTG definido a través de la ruta predeterminada tunelizada.

Para definir una ruta predeterminada tunelizada, utilice este comando:

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

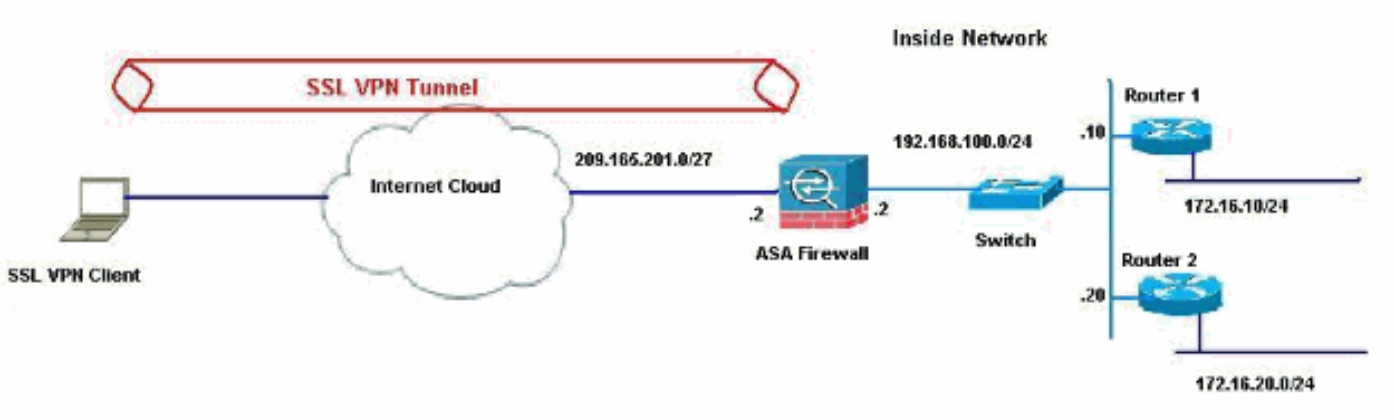
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



En este ejemplo, el SSL VPN Client accede a la red interna del ASA a través del túnel. El tráfico destinado a destinos distintos de la red interna también se tuneliza, ya que no hay túnel dividido configurado y se rutea a través del TDG (192.168.100.20).

Después de rutear los paquetes al TDG, que es el Router 2 en este caso, realiza la traducción de la dirección para rutear esos paquetes hacia Internet. Para obtener más información sobre la configuración de un router como gateway de Internet, refiérase a Cómo Configurar un Router Cisco Detrás de un Cable Módem que No es de Cisco.

Configuración de ASA con ASDM 6.1(5)

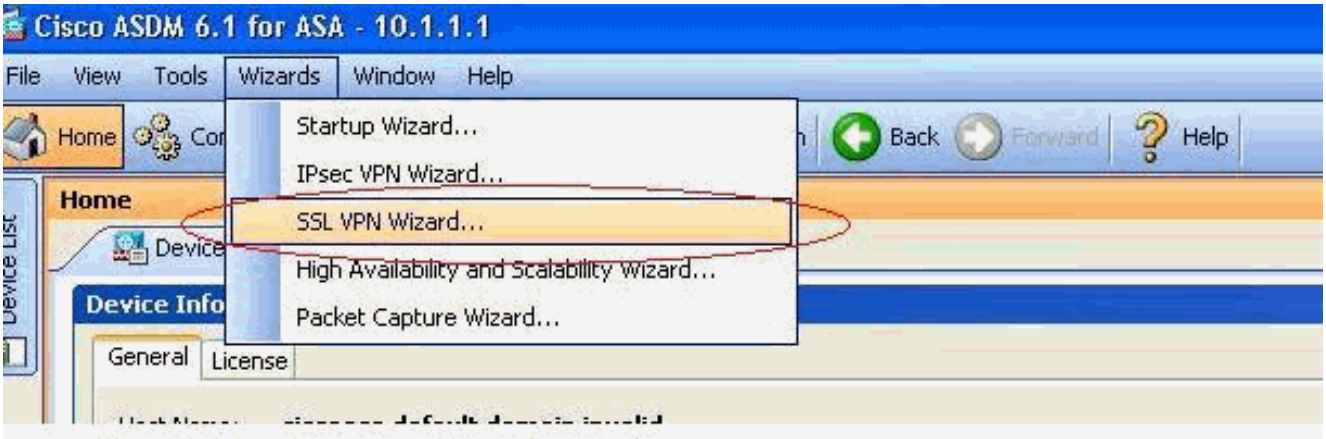
Este documento asume que las configuraciones básicas, como la configuración de la interfaz, están completas y funcionan correctamente.

Nota: Consulte Permiso de Acceso HTTPS para ASDM para obtener información sobre cómo permitir que el ASDM configure el ASA.

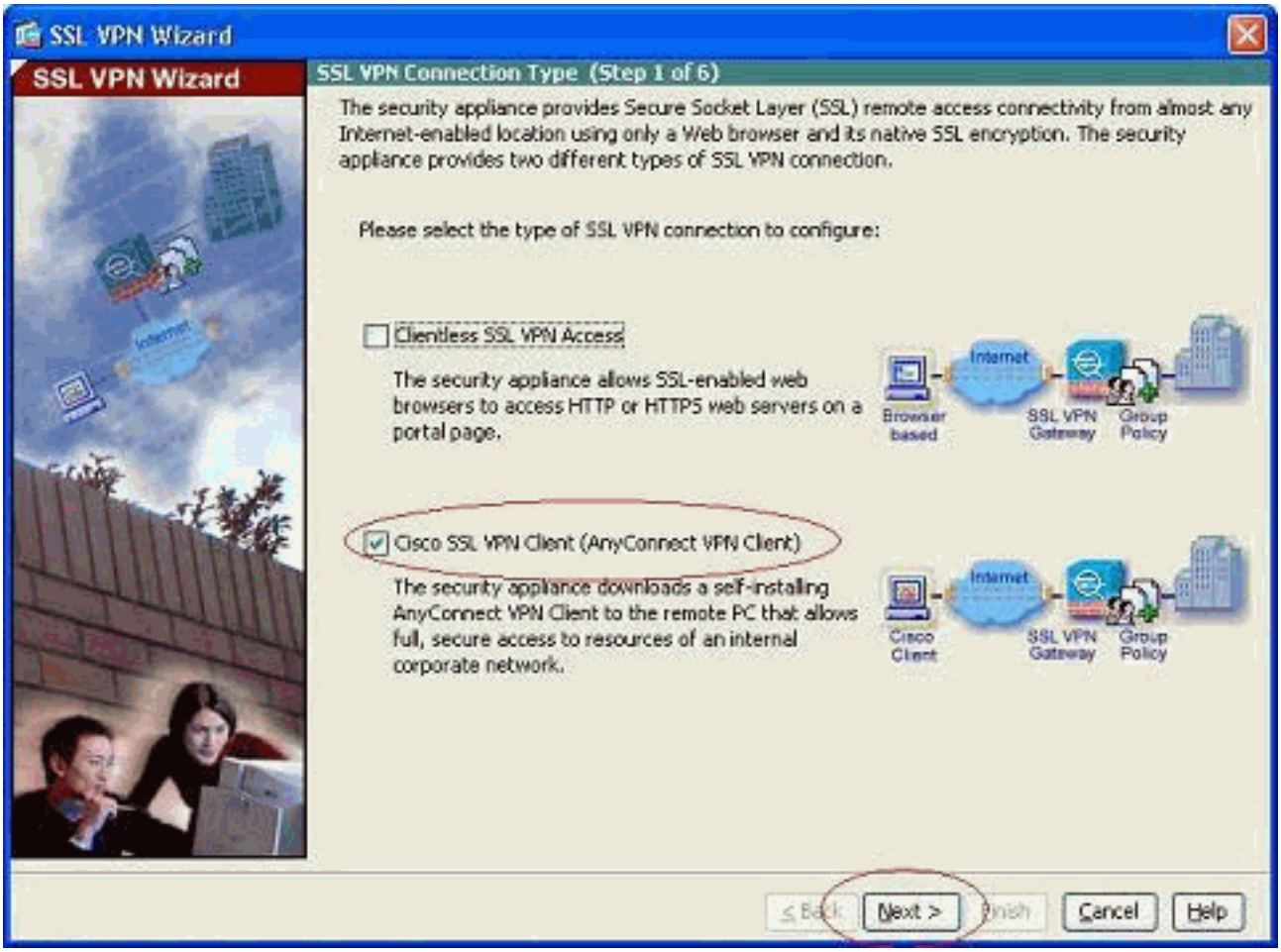
Nota: WebVPN y ASDM no se pueden habilitar en la misma interfaz ASA a menos que cambie los números de puerto. Consulte ASDM y WebVPN Habilitados en la Misma Interfaz de ASA para obtener más información.

Complete estos pasos para configurar SSL VPN mediante el Asistente SSL VPN.

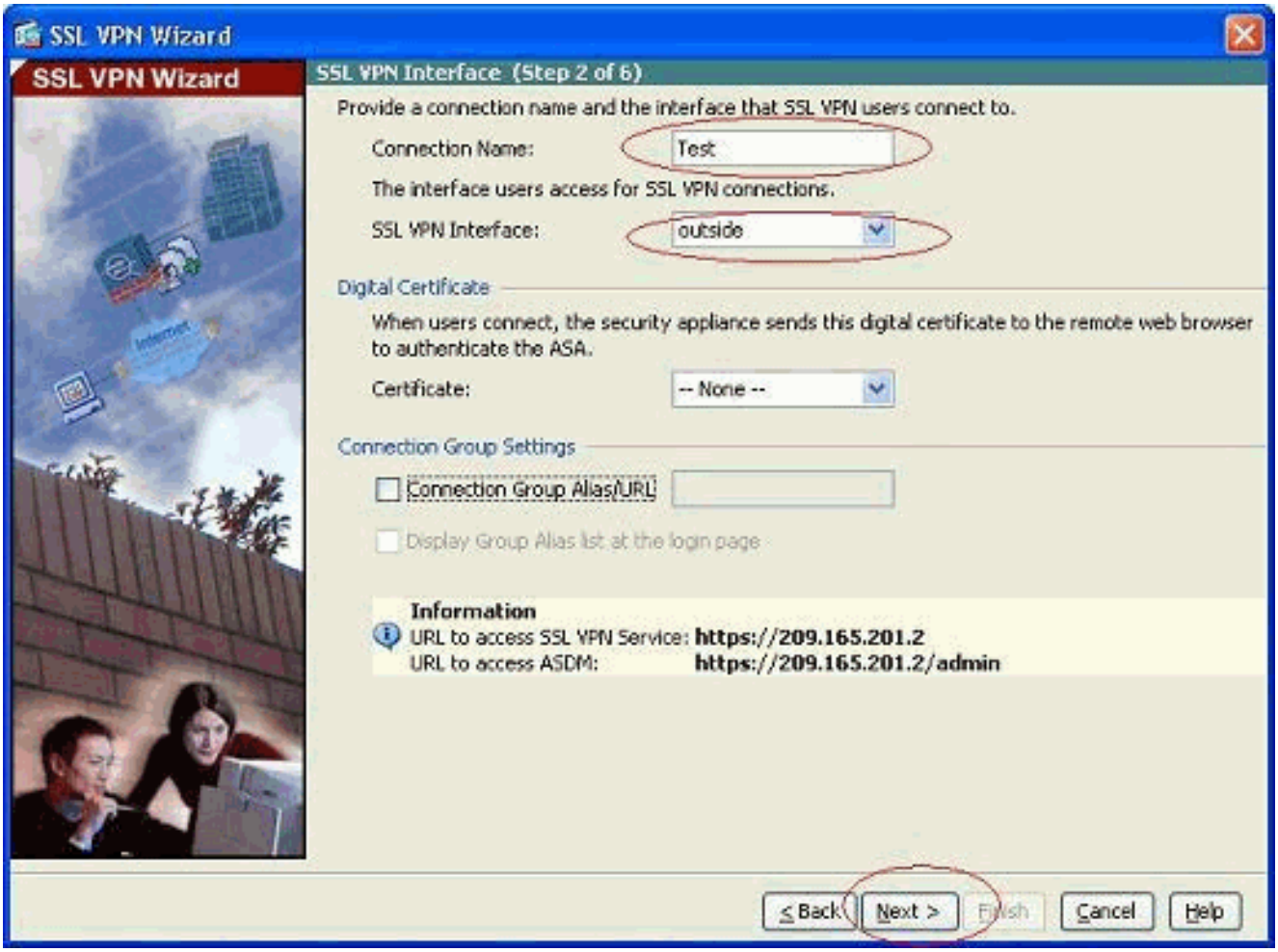
1. En el menú Asistentes, elija **Asistente SSL VPN**.



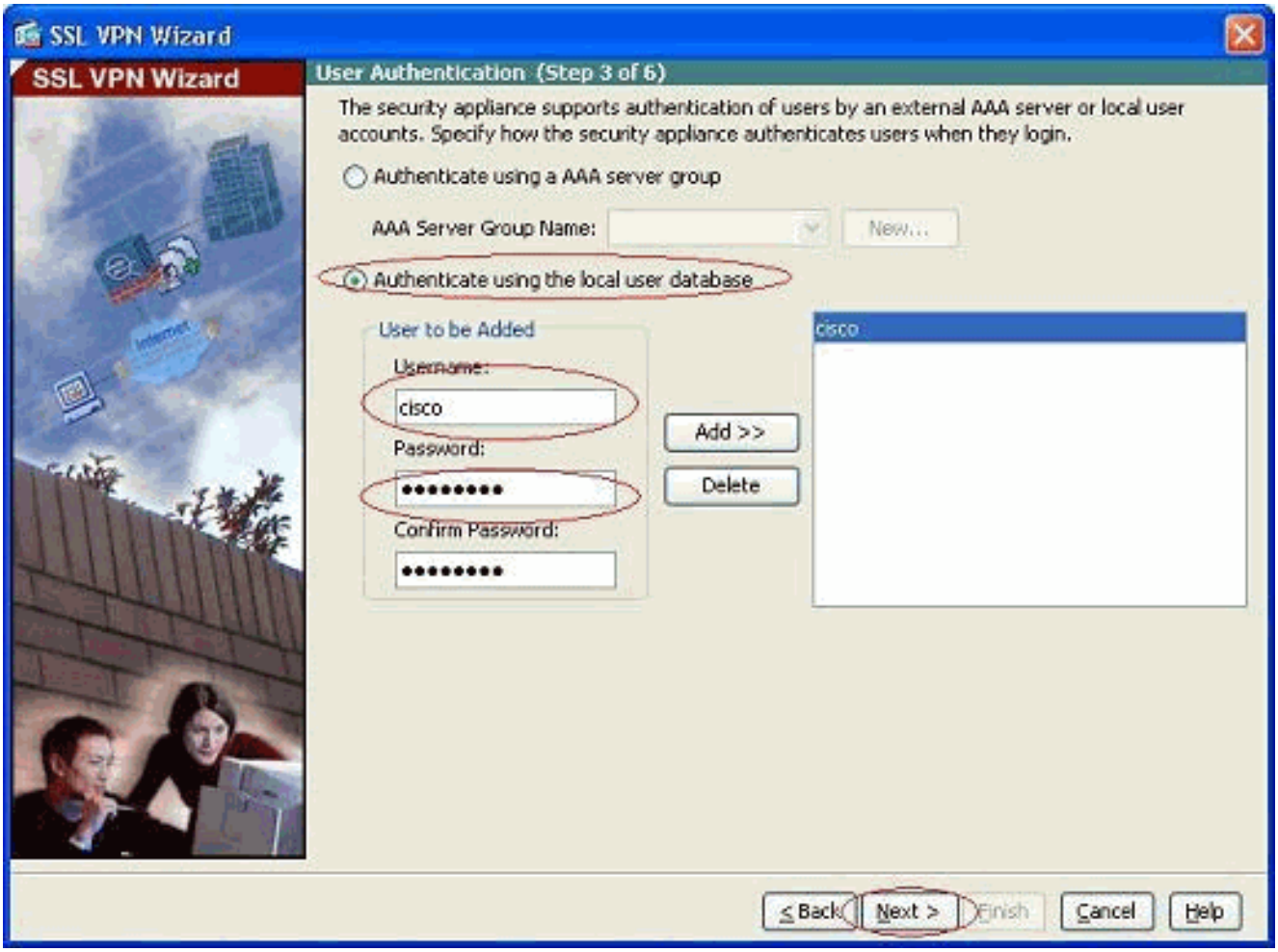
2. Haga clic en la casilla de verificación **Cisco SSL VPN Client** y haga clic en **Next**.



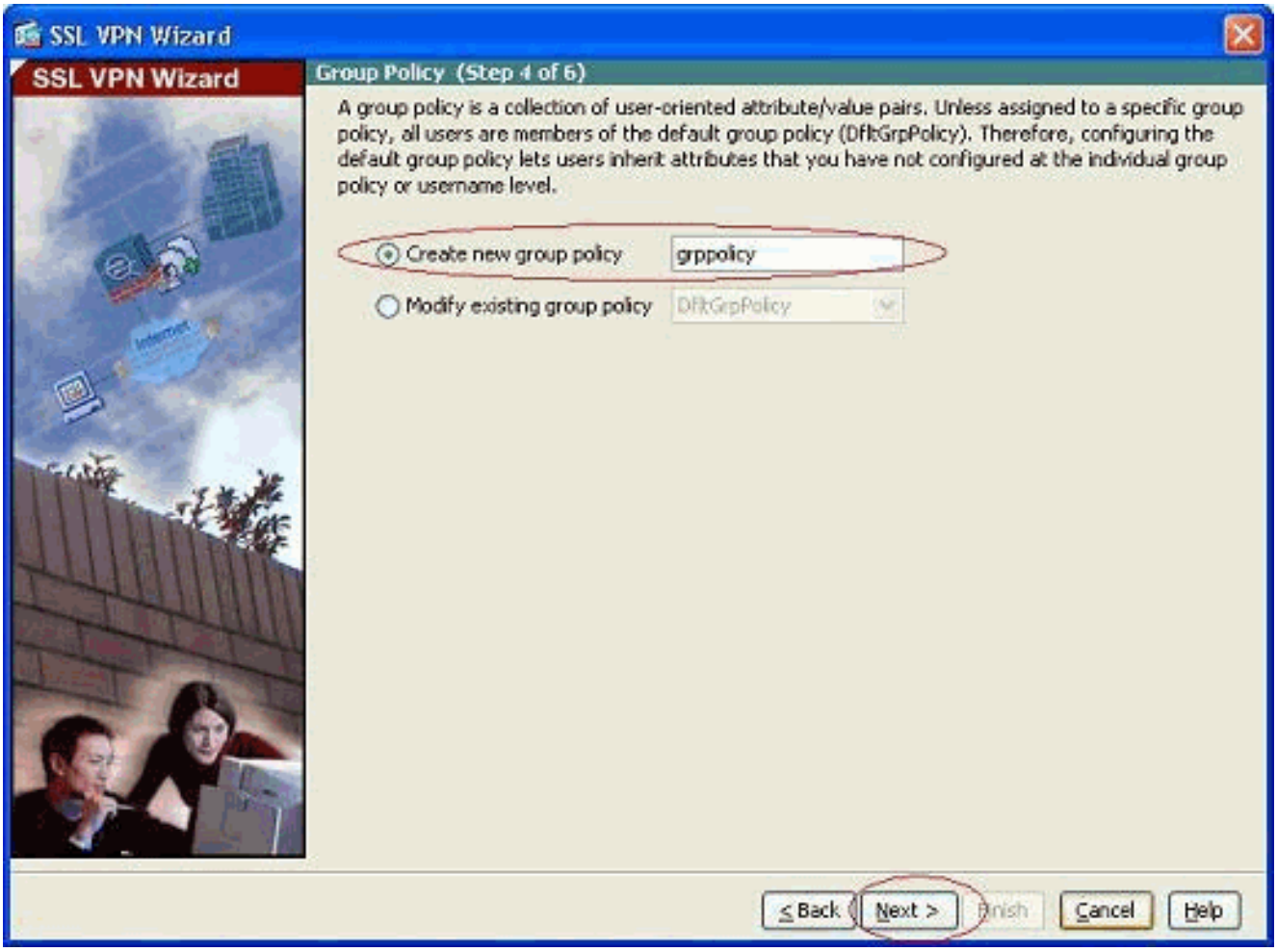
3. Introduzca un nombre para la conexión en el campo Connection Name (Nombre de la conexión) y, a continuación, elija la interfaz que está utilizando el usuario para acceder a SSL VPN en la lista desplegable SSL VPN Interface (Interfaz SSL VPN).



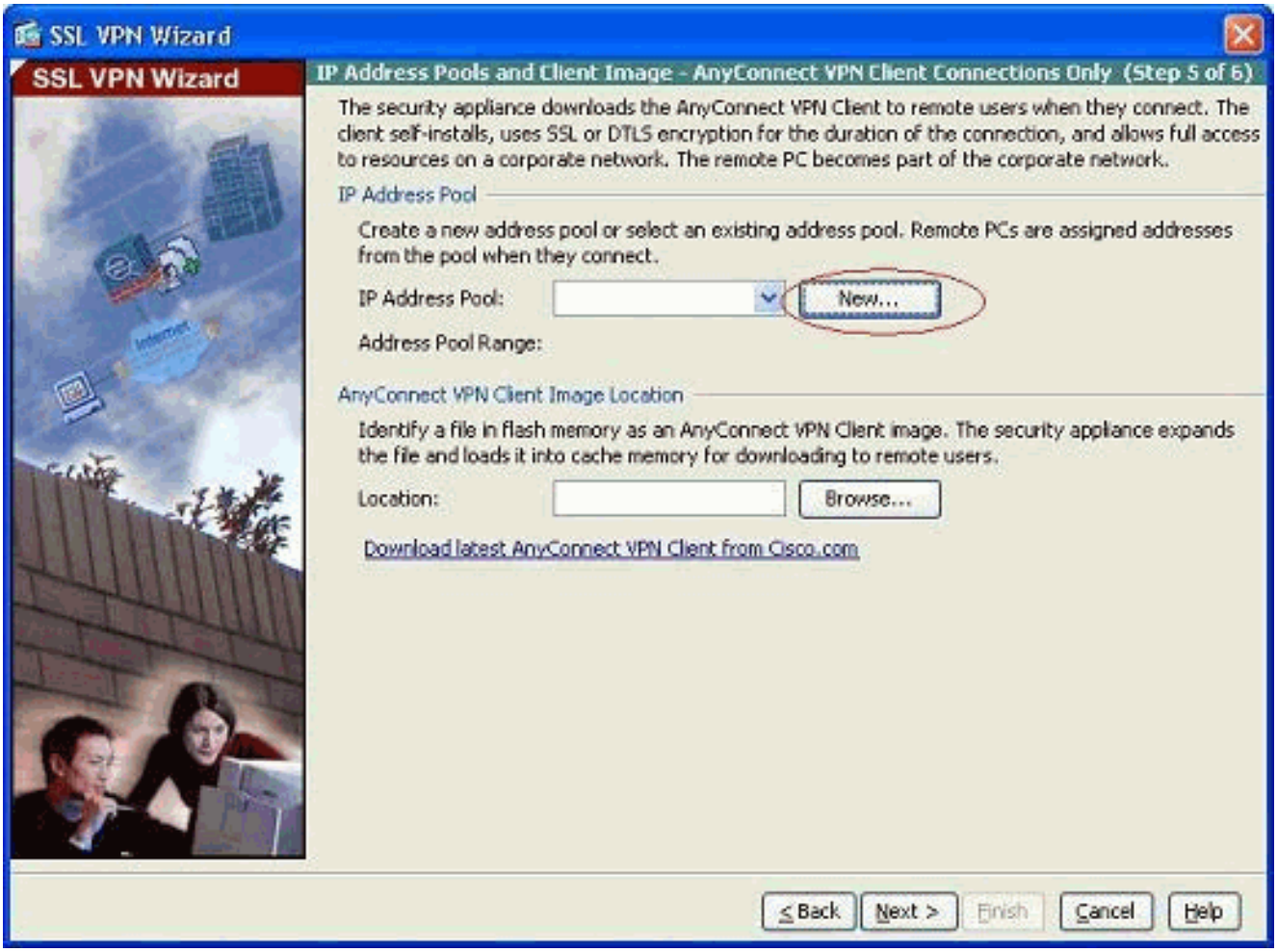
4. Haga clic en Next (Siguiente).
5. Elija un modo de autenticación y haga clic en **Next**. (Este ejemplo utiliza autenticación local.)



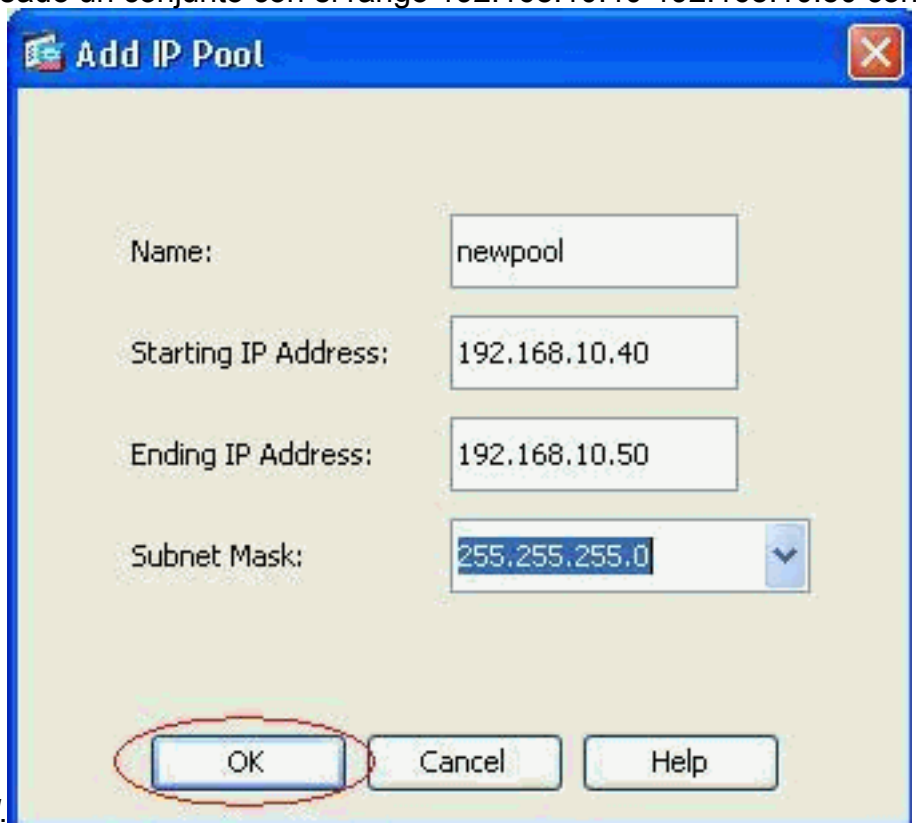
6. Cree una nueva política de grupo que no sea la política de grupo predeterminada existente.



7. Cree un nuevo conjunto de direcciones que se asignarán a los PC cliente SSL VPN una vez que se conecten.

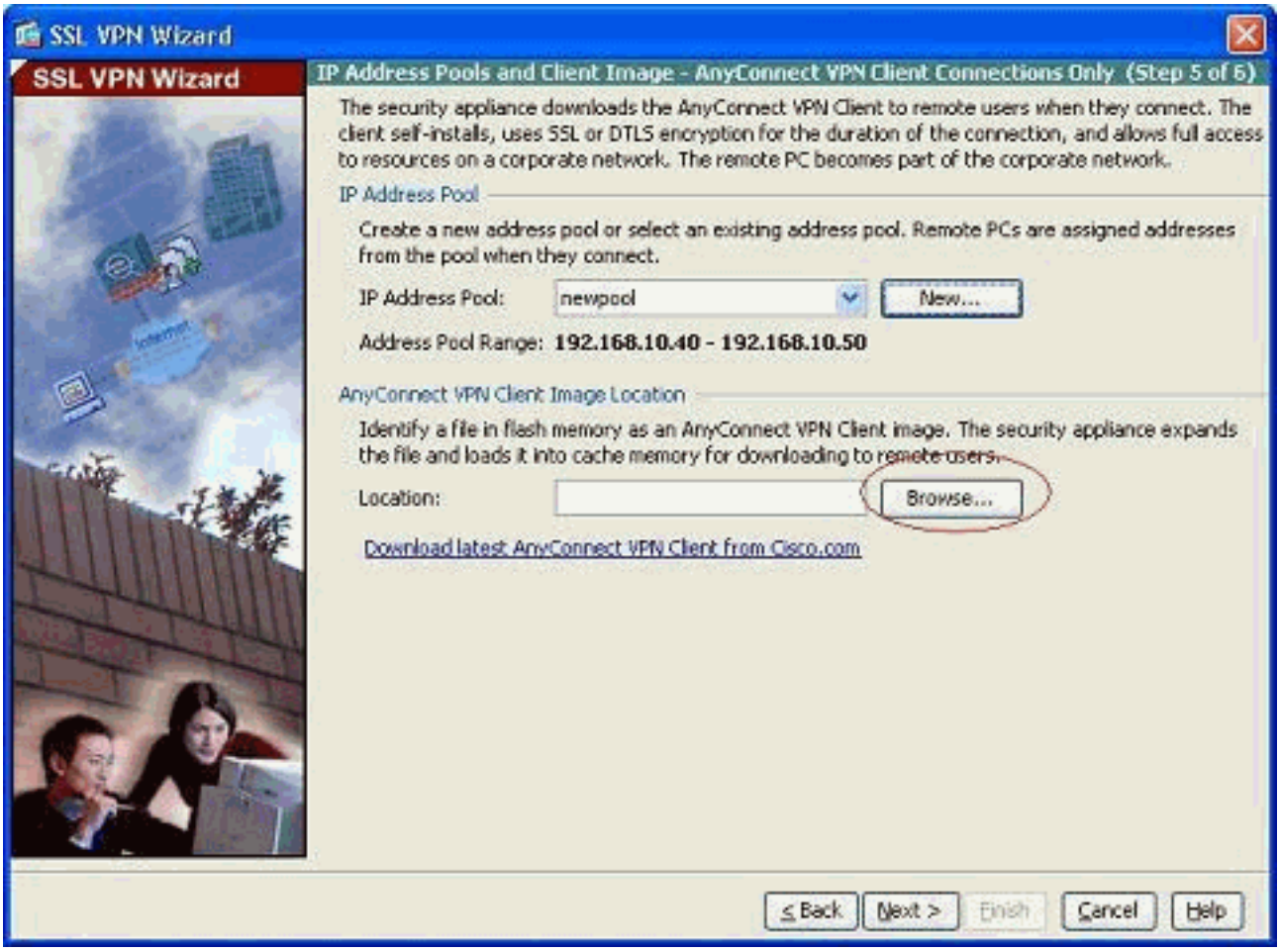


Se ha creado un conjunto con el rango 192.168.10.40-192.168.10.50 con el nombre *newpool*.

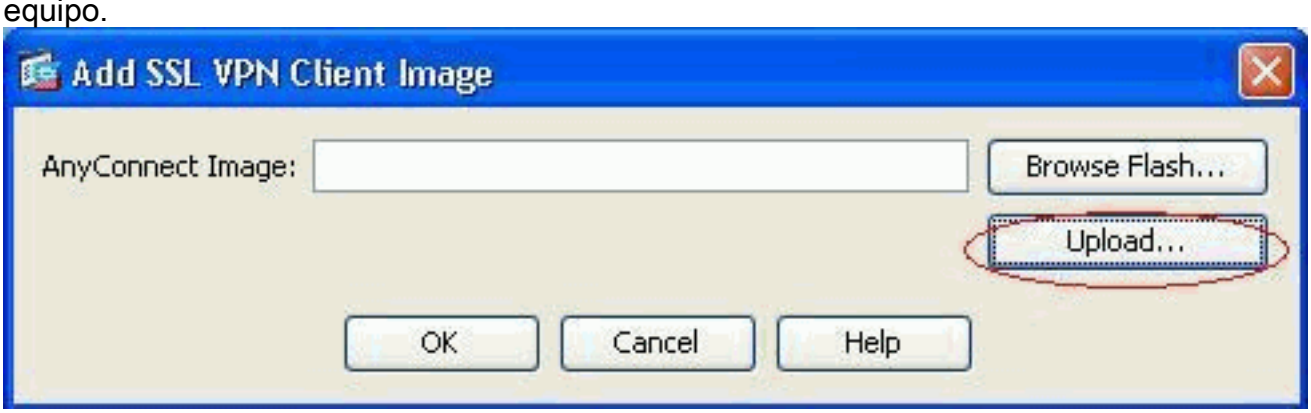


8. Haga clic en **Browse** para elegir y cargar la imagen SSL VPN Client en la memoria flash del

ASA.

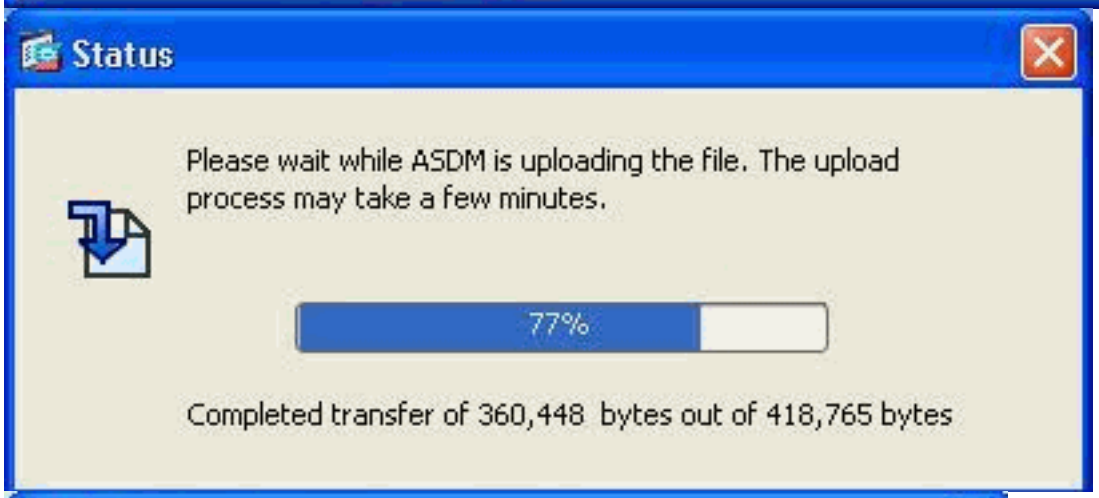


9. Haga clic en **Cargar** para establecer la ruta de acceso del archivo desde el directorio local del
equipo.



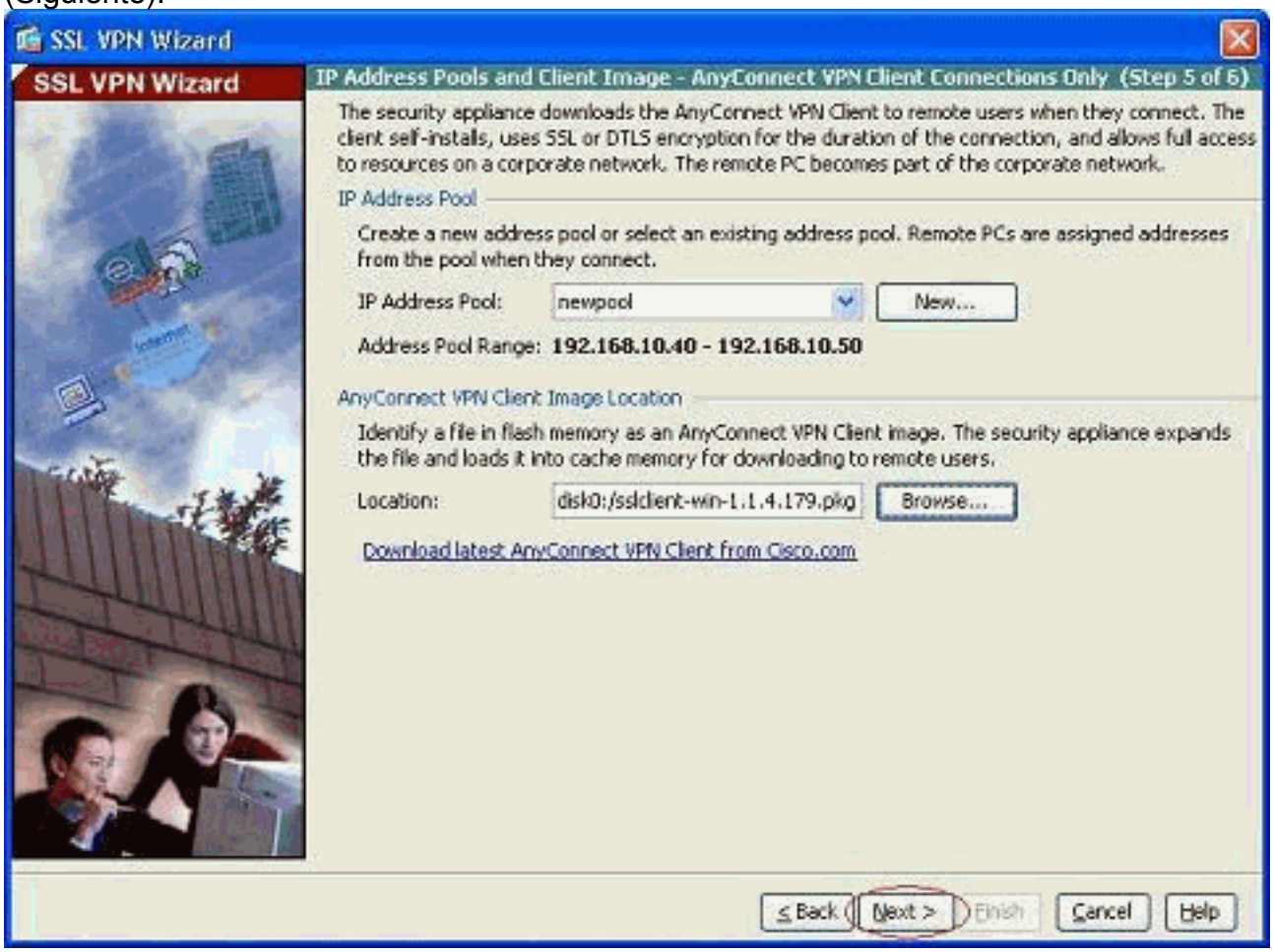
10. Haga clic en **Examinar archivos locales** para seleccionar el directorio donde existe el archivo
sslclient.pkg.

11. Haga clic en **Cargar archivo** para cargar el archivo seleccionado en la memoria flash de ASA.

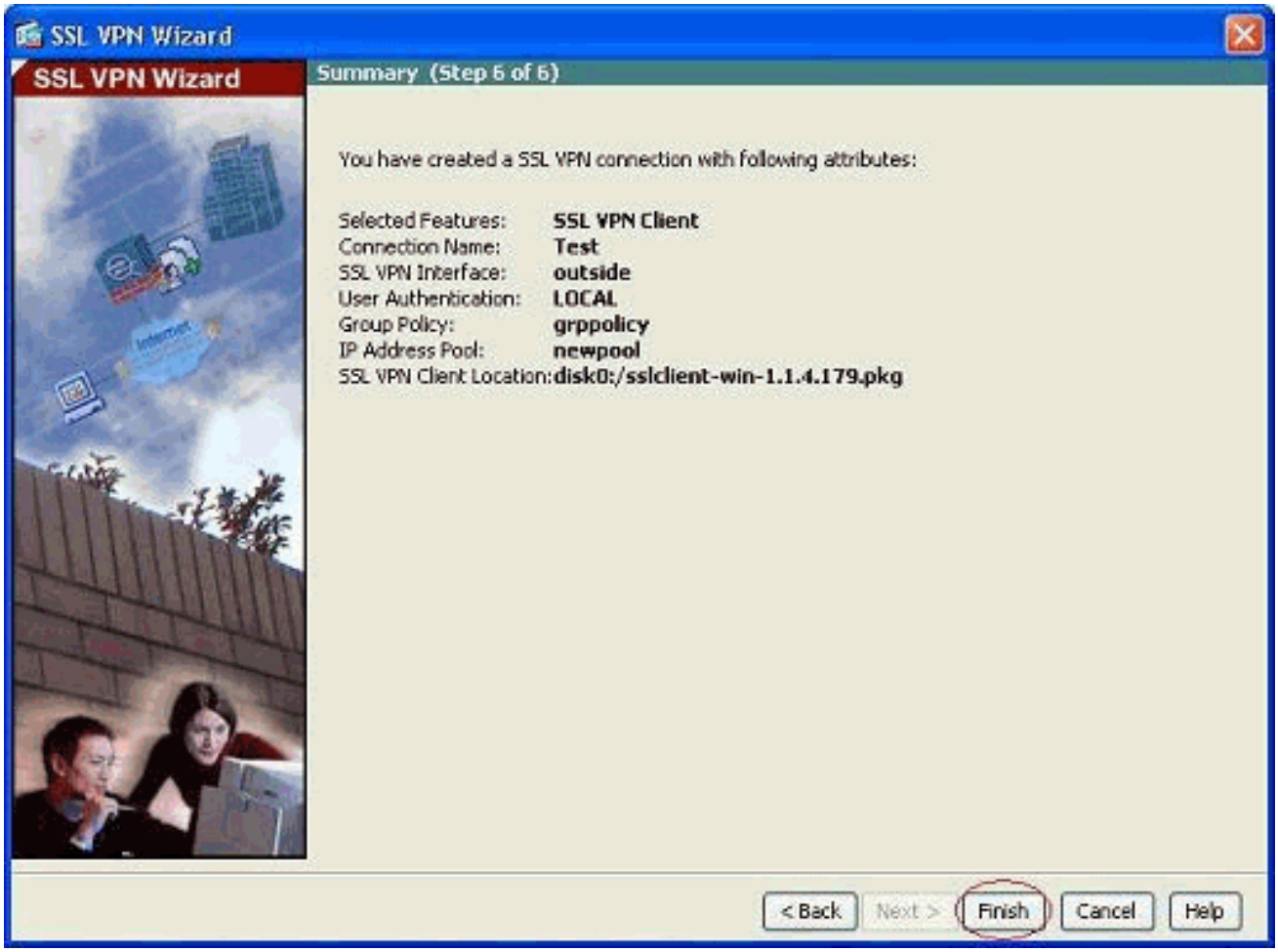


12. Una vez que el archivo se haya cargado en la memoria flash de ASA, haga clic en **Aceptar** para completar esa
tarea.

13. Ahora muestra el último archivo pkg de anyconnect cargado en la memoria flash de ASA. Haga clic en Next
(Siguiente).



14. Se muestra el resumen de la configuración del cliente SSL VPN. Haga clic en **Finalizar** para completar el
asistente.



La configuración que se muestra en ASDM se relaciona principalmente con la configuración del Asistente del cliente SSL VPN.

En la CLI, puede observar alguna configuración adicional. A continuación se muestra la configuración CLI completa y se han resaltado comandos importantes.

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#
```

Verificación

Los comandos dados en esta sección se pueden utilizar para verificar esta configuración.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **show webvpn svc**—Muestra las imágenes SVC almacenadas en la memoria flash ASA.
- **show vpn-sessiondb svc: muestra la información acerca de las conexiones SSL actuales.**

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Compatibilidad con dispositivos de seguridad adaptable de la serie 5500 de Cisco
- Ejemplo de Configuración de PIX/ASA y VPN Client for Public Internet VPN on a Stick
- Ejemplo de Configuración de SSL VPN Client (SVC) en ASA con ASDM
- Soporte Técnico y Documentación - Cisco Systems