ASA 8.X: Rutear el tráfico SSL VPN con el ejemplo tunneled de la configuración del gateway predeterminado

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 usted crea una ruta predeterminado con la opción tunneled, todo el tráfico de un túnel que termina en el ASA que no se puede rutear usando docto o las Static rutas se envía a esta ruta. Para el tráfico que emerge de un túnel, esta ruta reemplaza cualquier ruta predeterminado configurada o aprendida otra.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- ASA que se ejecuta en la versión 8.x
- (SVC) 1.x del Cliente Cisco SSL VPN**Nota:** Descargue el paquete del cliente VPN SSL (sslclient-win*.package) de la descarga de software de Cisco (clientes registrados solamente). Copie SVC a memoria flash en el ASA. SVC necesita ser descargado a los ordenadores del usuario remoto 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 funcionan con la versión de software 8.x
- Versión del Cliente Cisco SSL VPN para Windows 1.1.4.179
- PC que ejecuta Windows 2000 Professional o Windows XP
- Versión 6.1(5) del Cisco Adaptive Security Device Manager (ASDM)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Antecedentes

El (SVC) del cliente VPN SSL es una tecnología de tunelización VPN que da a usuarios remotos las ventajas de un cliente del IPSec VPN sin la necesidad de los administradores de la red de instalar y de configurar a los clientes del IPSec VPN en las computadoras remotas. SVC utiliza la encripción de SSL que está ya presente en la computadora remota así como el login del WebVPN y la autenticación del dispositivo de seguridad.

En el escenario actual, hay un cliente VPN SSL que conecta con los recursos internos detrás del ASA a través del túnel SSL VPN. El túnel dividido no se habilita. Cuando el cliente VPN SSL está conectado con el ASA, todos los datos serán tunneled. Además de acceder a los recursos internos, el criterio principal es rutear este tráfico de túnel a través del gateway tunneled predeterminado (DTG).

Usted puede definir una ruta predeterminado separada para el tráfico de túnel junto con la ruta predeterminado estándar. El tráfico no encriptado recibido por el ASA, para el cual hay no estático o ruta aprendido, se rutea a través de la ruta predeterminado estándar. El tráfico encriptado recibido por el ASA, para el cual hay no estático o ruta aprendido, será pasado al DTG definido a través de la ruta predeterminado tunneled.

Para definir una ruta predeterminado tunneled, utilice este comando:

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

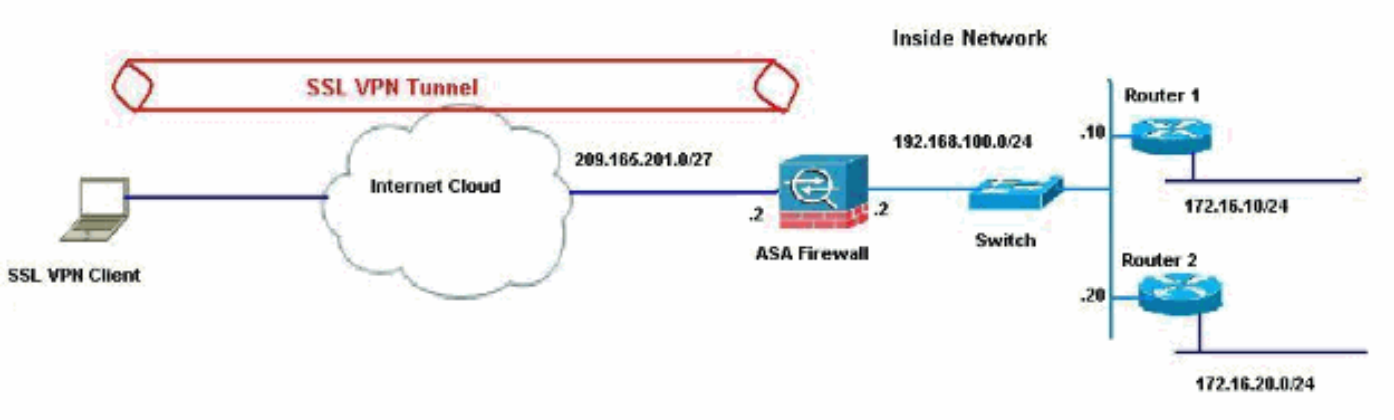
Configurar

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

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) 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, los accesos de cliente VPN SSL la red interna del ASA a través del túnel. El tráfico significado para los destinos con excepción de la red interna es también tunneled, pues no hay túnel dividido configurado, y se rutea con el TDG (192.168.100.20).

Después de que los paquetes se ruteen al TDG, que es router2 en este caso, realiza la traducción de la dirección para rutear esos paquetes a continuación a Internet. Para más información sobre configurar a un router como gateway de Internet, refiérase a cómo configurar a un router Cisco detrás de un cablemódem que no es de Cisco.

Configuración ASA usando el ASDM 6.1(5)

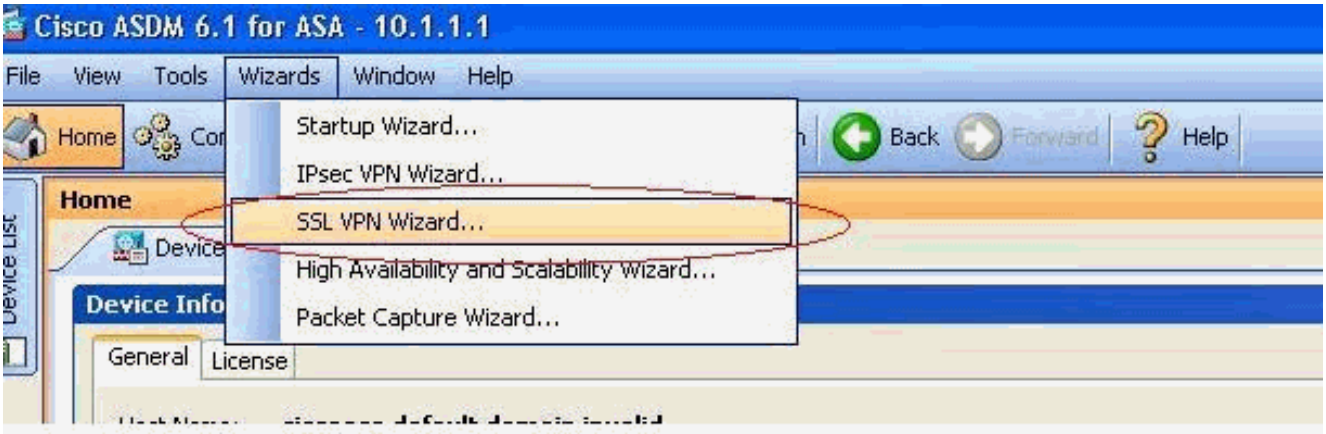
Este documento asume las configuraciones básicas, tales como configuración de la interfaz, es completo y trabajo correctamente.

Nota: Refiera a permitir el acceso HTTPS para el ASDM para la información sobre cómo permitir que el ASA sea configurado por el ASDM.

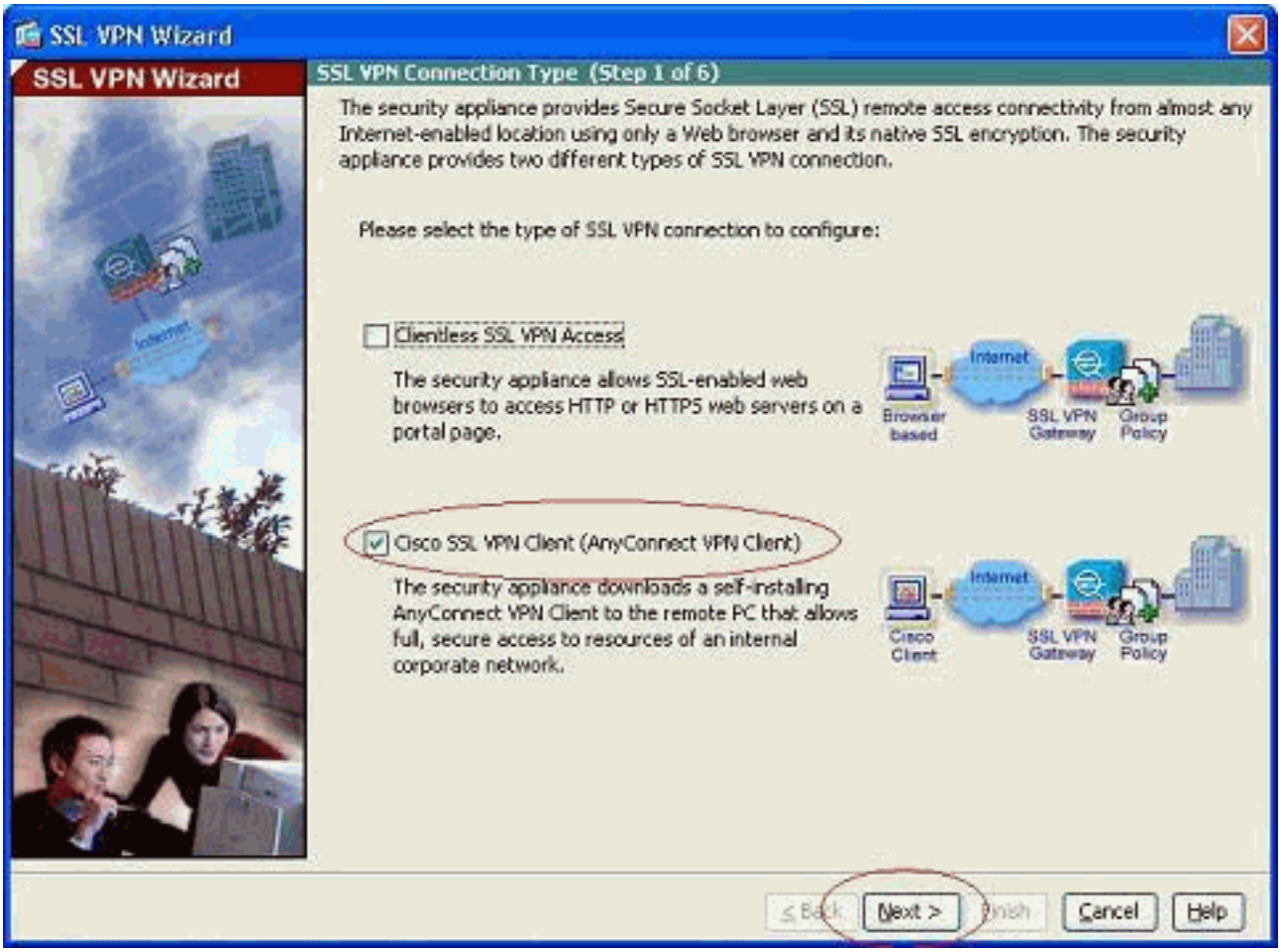
Nota: El WebVPN y el ASDM no se pueden habilitar en la misma interfaz ASA a menos que cambie los números del puerto. Consulte ASDM y WebVPN Habilitados en la Misma Interfaz de ASA para obtener más información.

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

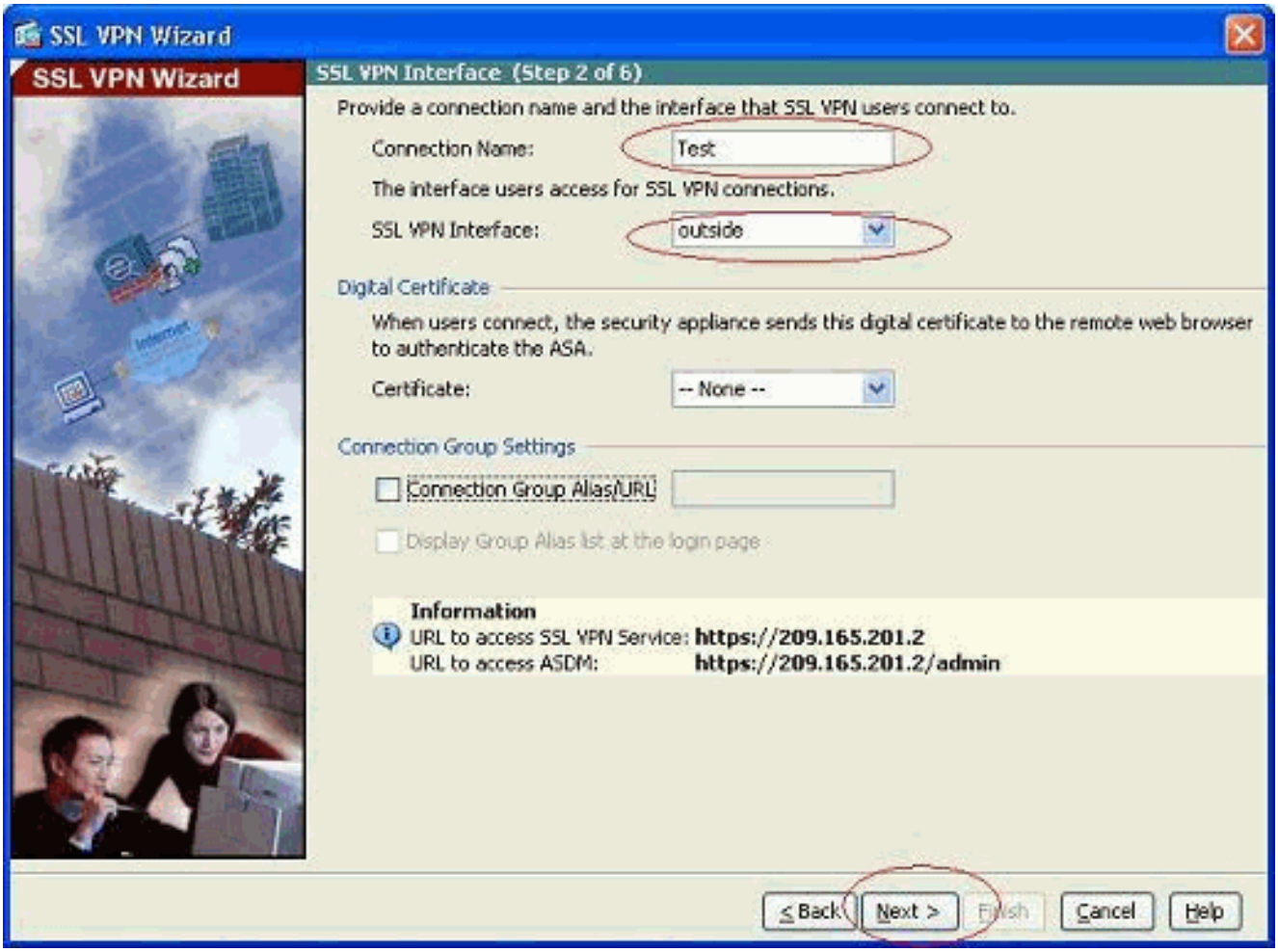
1. Del menú de los Asisitente, elija al **Asistente VPN SSL**.



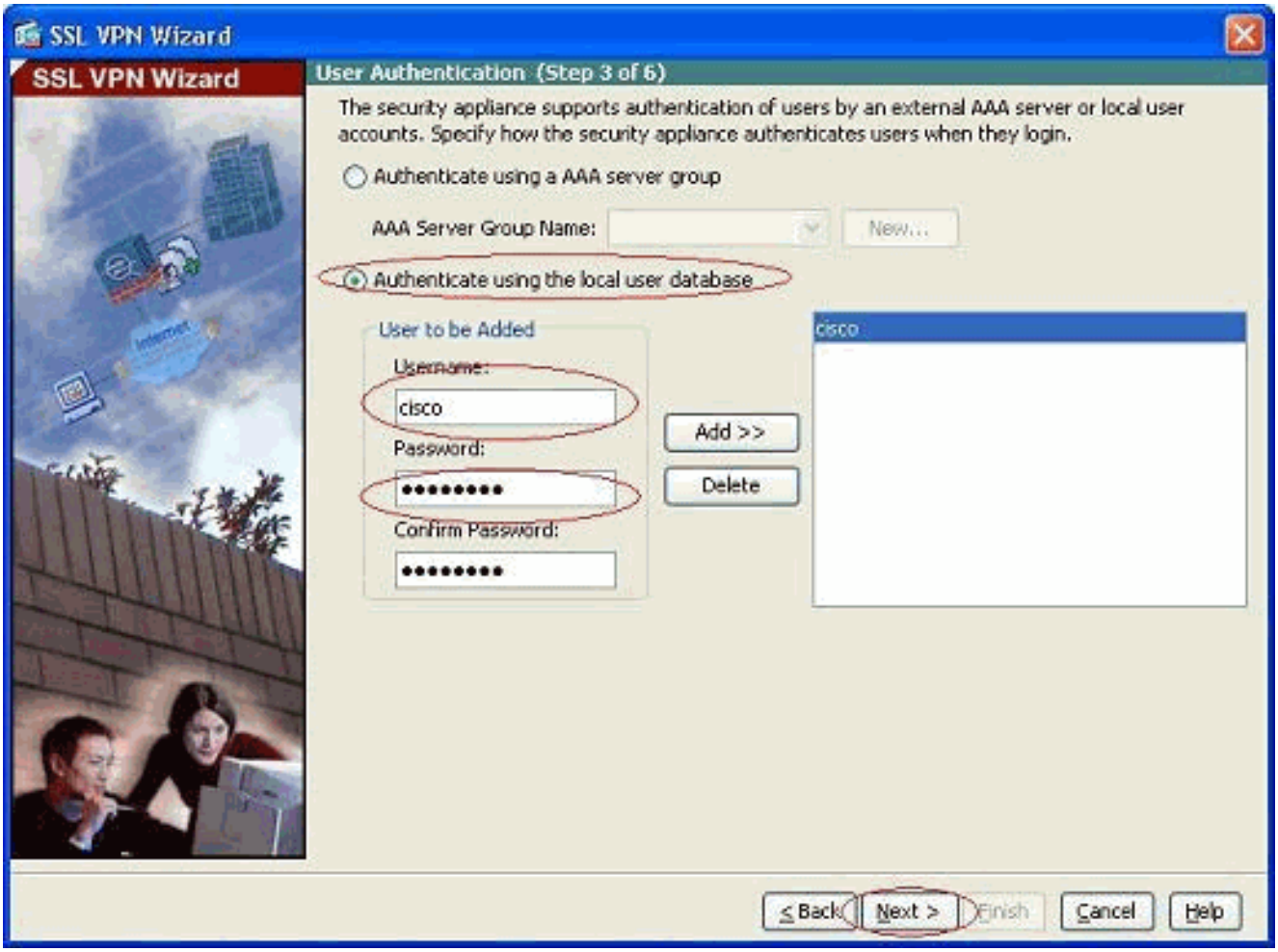
2. Haga clic la casilla de verificación del **Cliente Cisco SSL VPN**, y haga clic **después**.



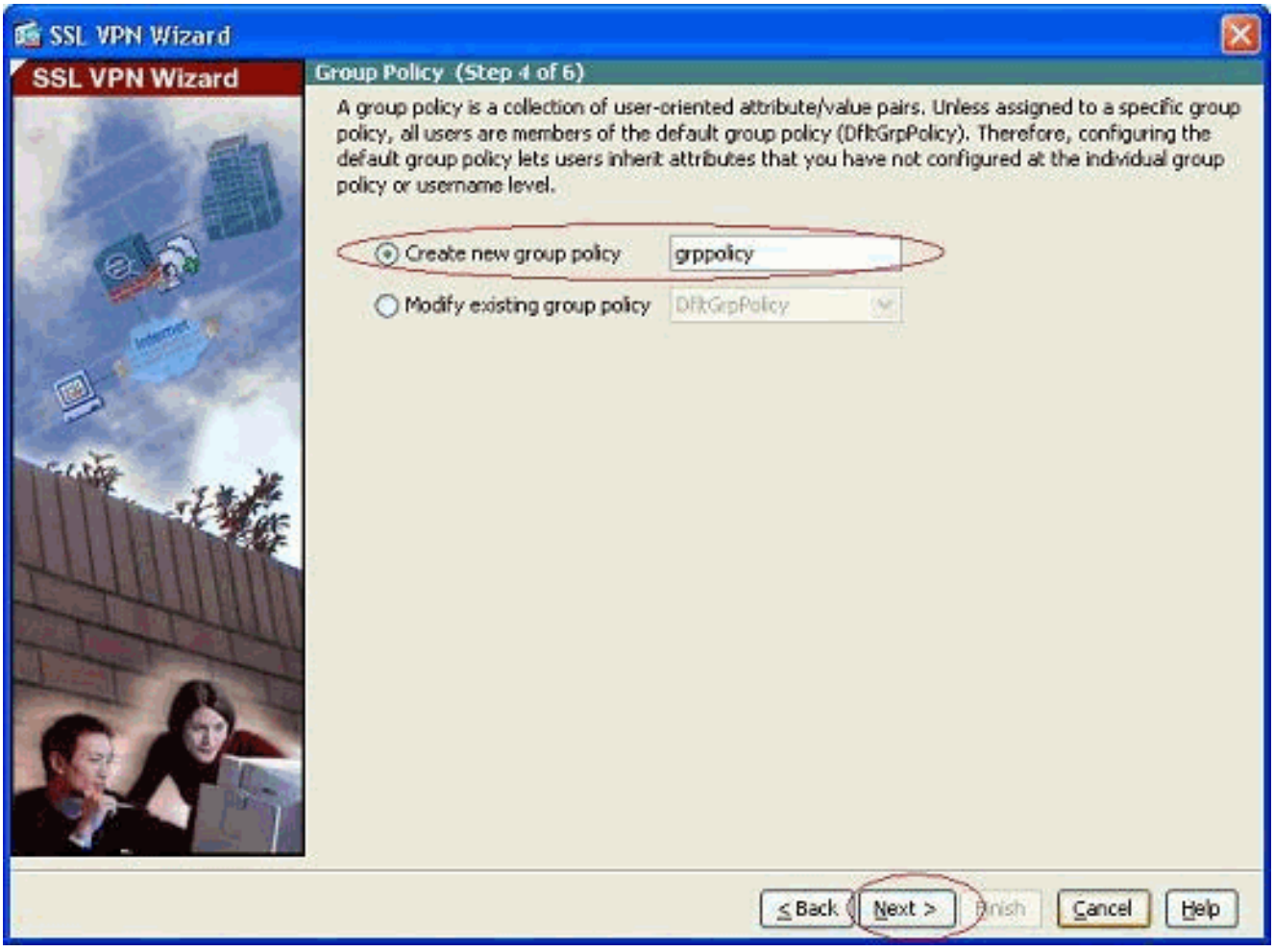
3. Ingrese un nombre para la conexión en el campo de nombre de la conexión, y después elija la interfaz que está siendo utilizada por el usuario para acceder el SSL VPN de la lista desplegable de la interfaz SSL
   VPN.



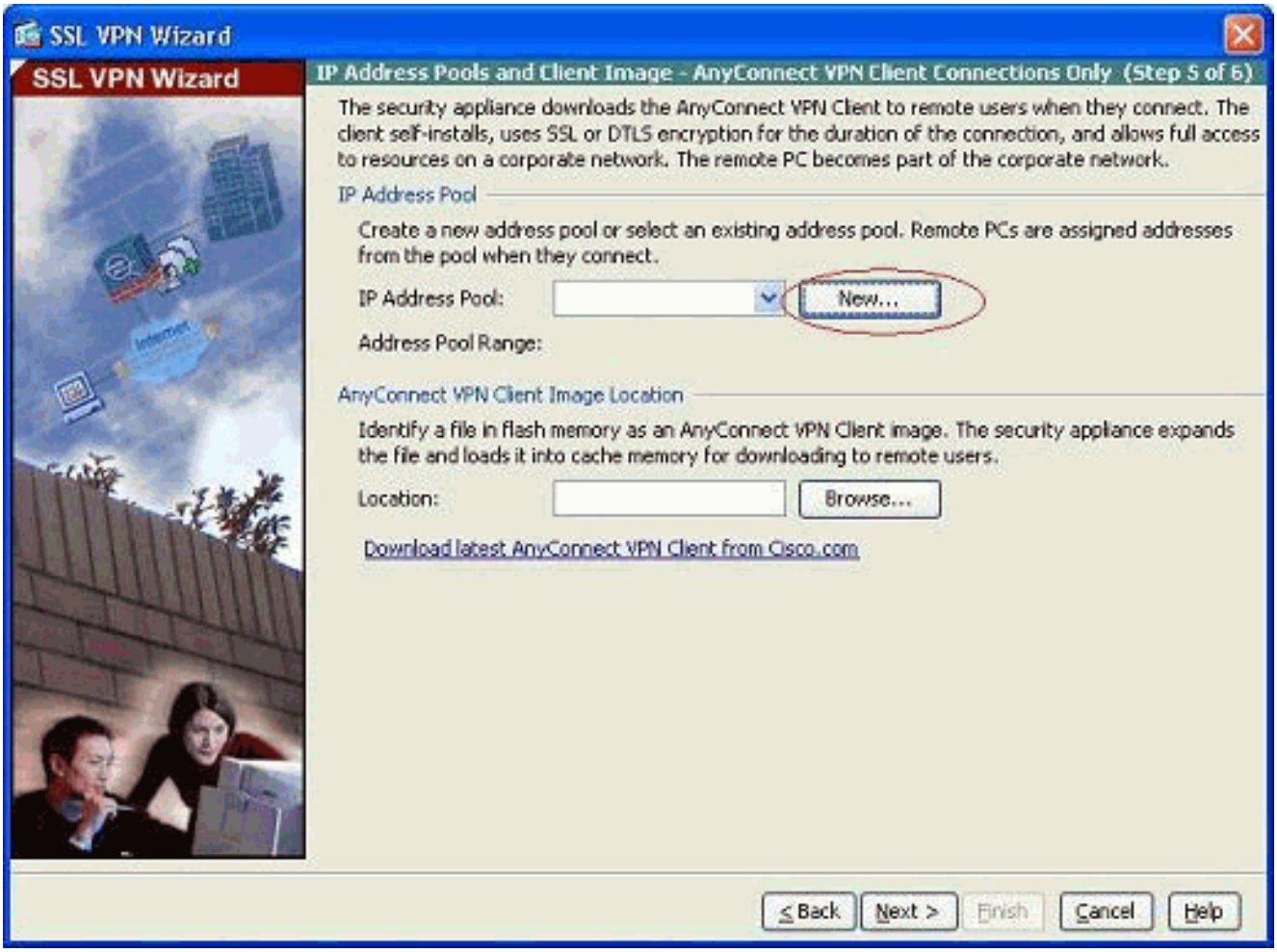
4. Haga clic en Next (Siguiente).
5. Elija a un modo de autenticación, y haga clic **después**. (Este ejemplo utiliza la autenticación local.)



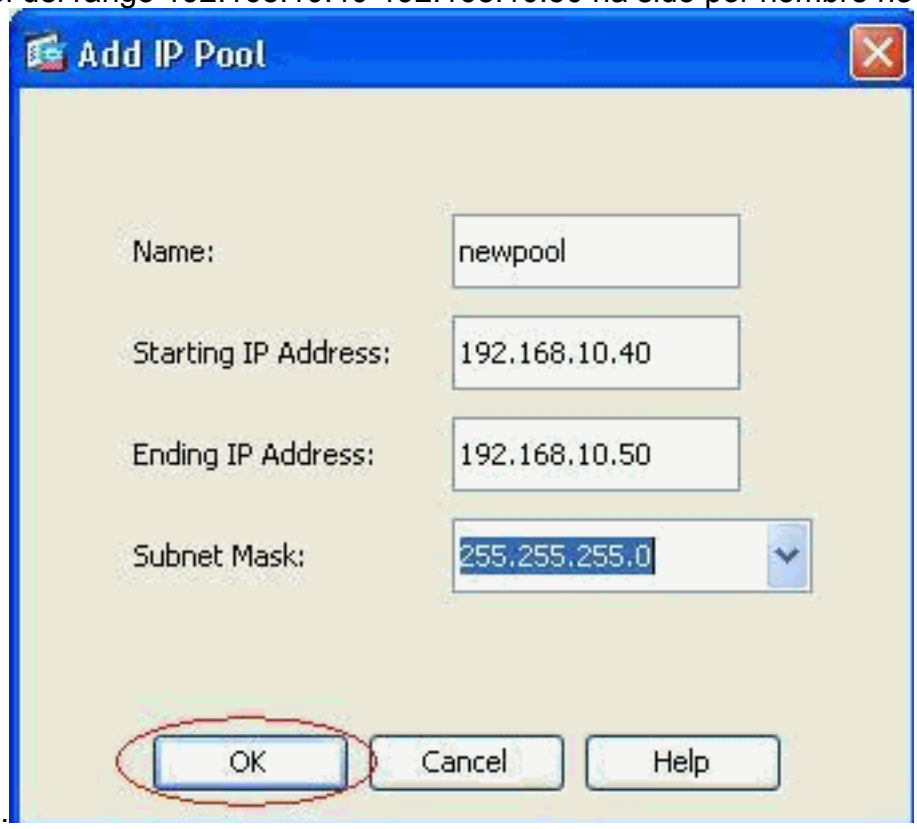
6. Crean una nueva directiva del grupo con excepción de la directiva del grupo predeterminado existente.



7. Crea a una nueva agrupación de direcciones que sea asignada al cliente VPN PC SSL que ella consigue una vez
conectada.

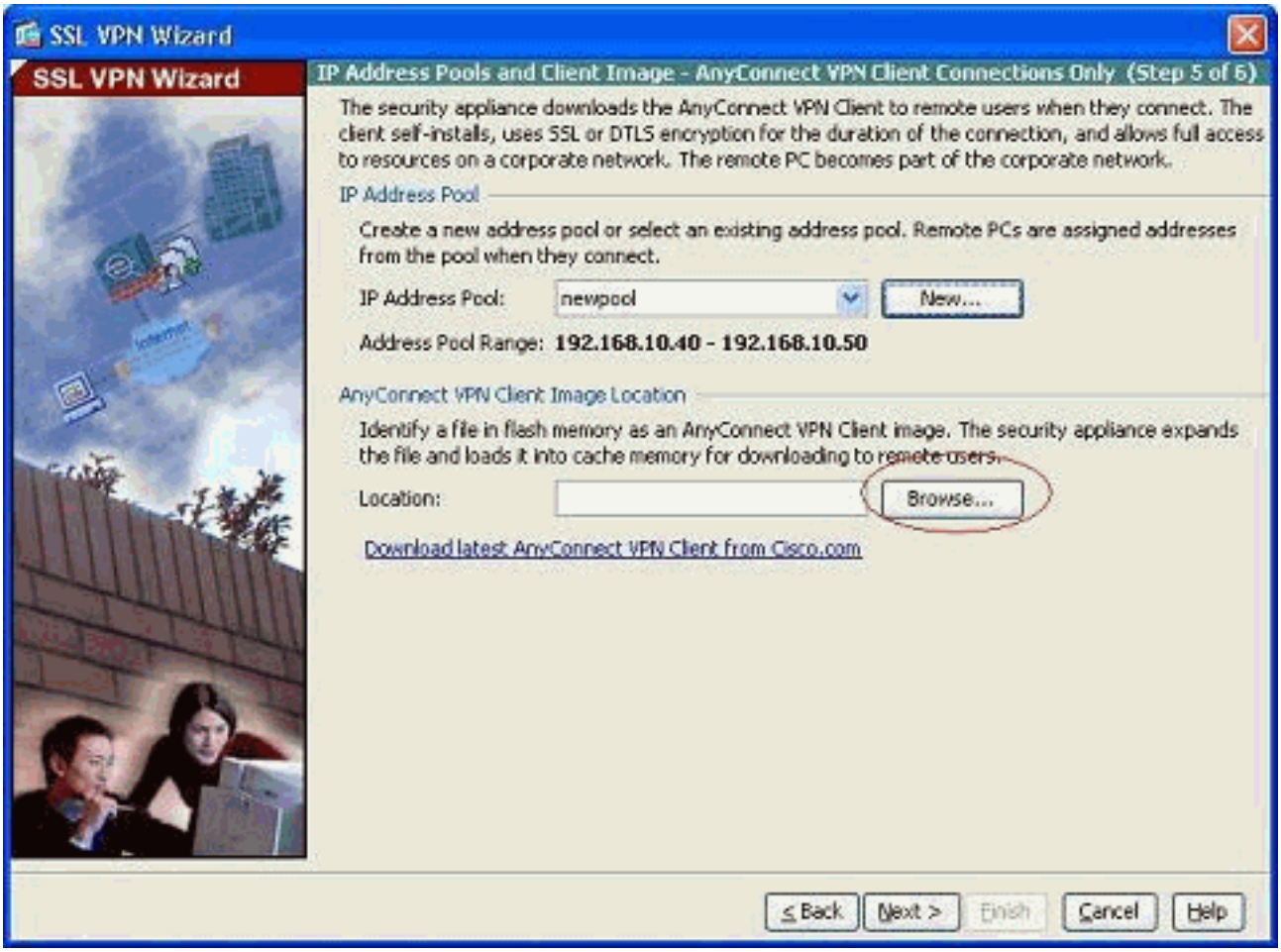


Un pool del rango 192.168.10.40-192.168.10.50 ha sido por nombre *newpool*
creado.

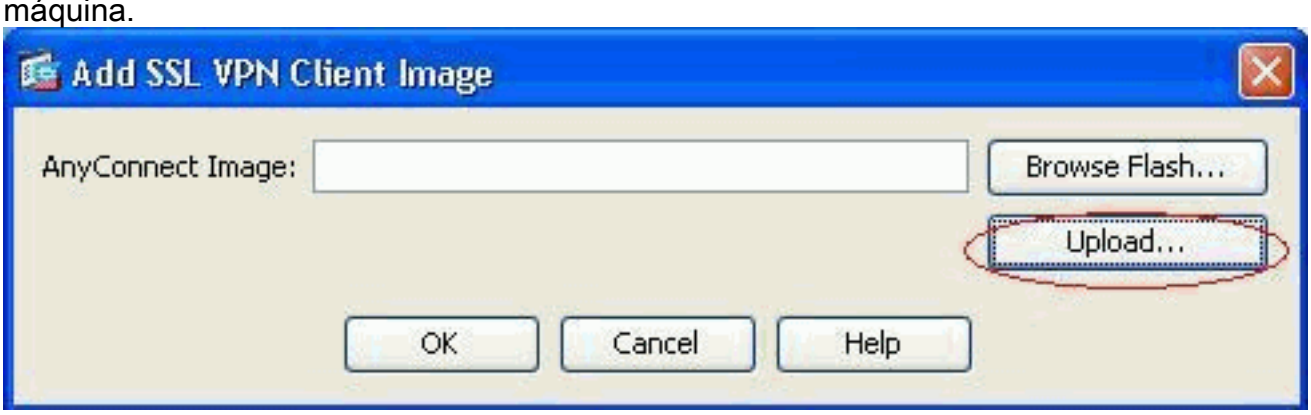


8. Haga clic **hojea** para elegir y cargar la imagen del cliente VPN SSL a memoria flash del

ASA.

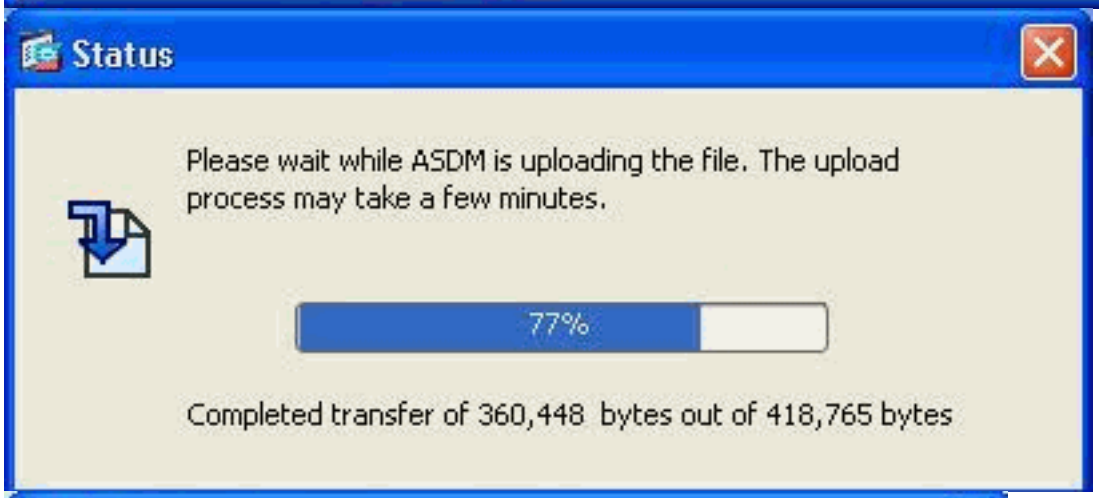


9. Haga clic la **carga** para fijar el trayecto del archivo del directorio local de la máquina.



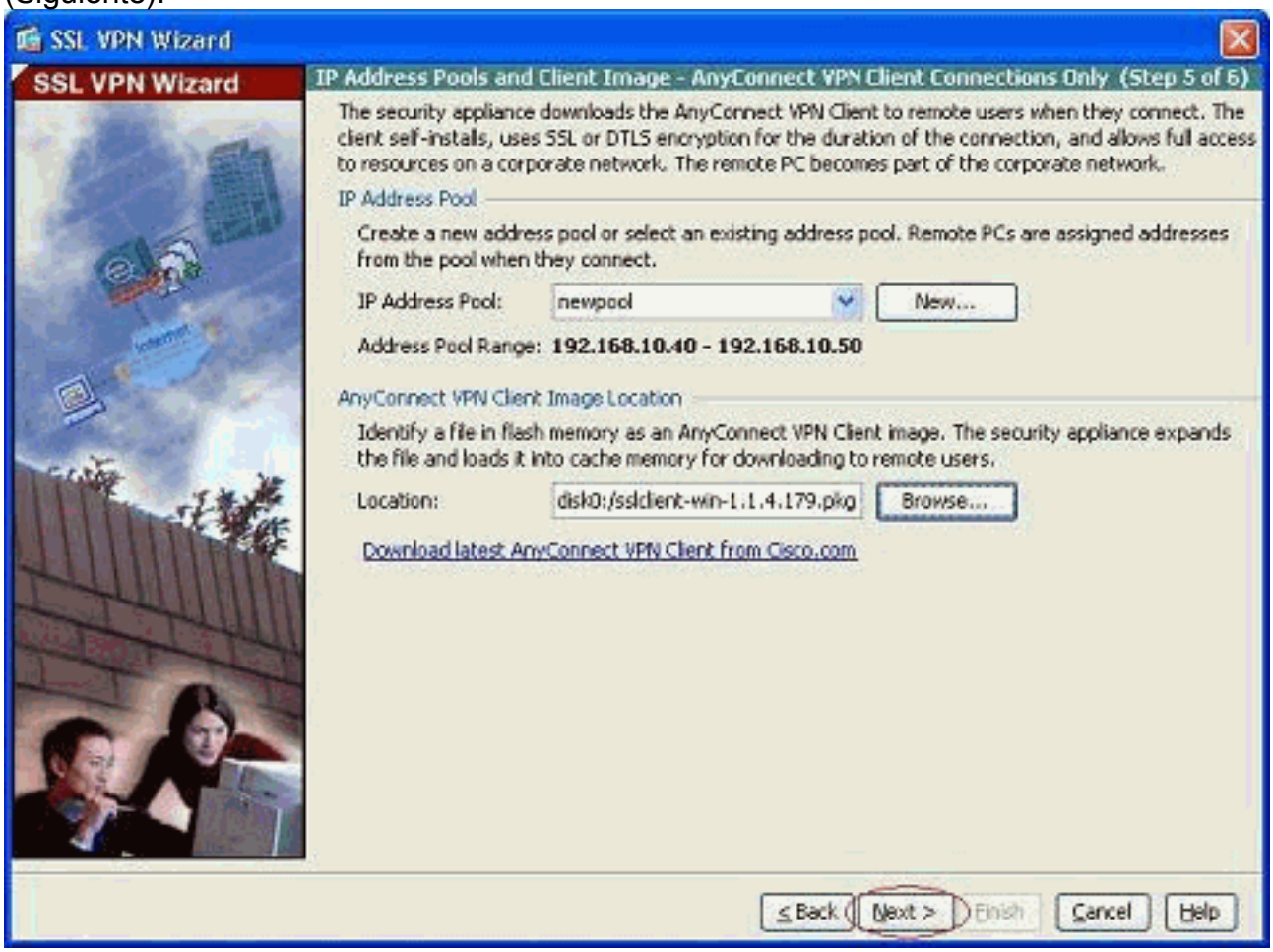
10. El tecleo **hojea los archivos locales** para seleccionar el directorio donde existe el archivo sslclient.pkg.

11. **Archivo de la carga del** tecleo para cargar el archivo seleccionado al flash del ASA.

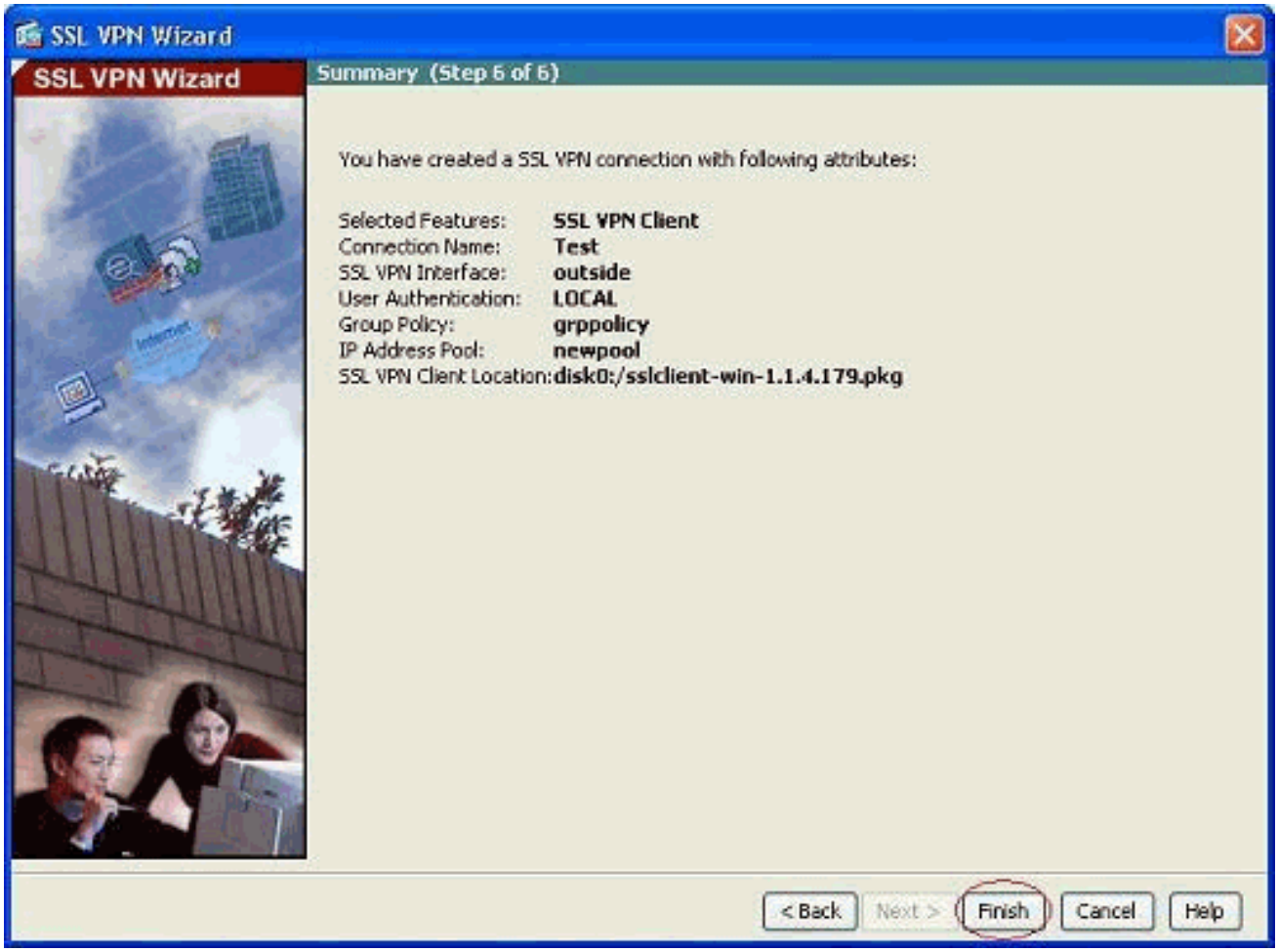


12. El archivo está cargado una vez encendido al flash del ASA, **AUTORIZACIÓN del** tecleo para completar esa
tarea.

13. Ahora muestra el último archivo de paquete del anyconnect cargado encendido al flash del ASA. Haga clic en Next
(Siguiente).



14. El resumen de la configuración de cliente VPN SSL se muestra. Clic en Finalizar para completar al
Asisitente.



La configuración mostrada en el ASDM pertenece principalmente a la configuración del asistente de cliente VPN SSL.

En el CLI, usted puede observar una cierta configuración adicional. La configuración CLI completa se muestra abajo y se han resaltado los 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.

- **muestre que el webvpn svc** — — visualiza las imágenes de SVC salvadas en memoria flash ASA.
- **show vpn-sessiondb svc: muestra la información acerca de las conexiones SSL actuales.**

Troubleshooting

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

Información Relacionada

- Soporte adaptante del dispositivo de seguridad de las Cisco 5500 Series
- PIX/ASA y cliente VPN para el Internet pública VPN en un ejemplo de configuración del palillo
- Ejemplo de Configuración de SSL VPN Client (SVC) en ASA con ASDM
- Soporte Técnico y Documentación - Cisco Systems