ASA 8.X: Esempio di routing del traffico VPN SSL tramite il gateway predefinito tunneled

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Convenzioni
Premesse
Configurazione
Esempio di rete
Configurazione ASA con ASDM 6.1(5)
Verifica
Risoluzione dei problemi
Informazioni correlate

Introduzione

In questo documento viene descritto come configurare Adaptive Security Appliance (ASA) in modo che instradi il traffico VPN SSL attraverso il gateway predefinito tunneled (TDG). Quando si crea una route predefinita con l'opzione tunneled, tutto il traffico di un tunnel che termina sull'ASA e che non può essere instradato utilizzando route apprese o statiche viene inviato a questa route. Per il traffico che emerge da un tunnel, questo percorso ignora qualsiasi altro percorso predefinito configurato o appreso.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- ASA in esecuzione sulla versione 8.x
- Cisco SSL VPN Client (SVC) 1.x**Nota:** scaricare il pacchetto SSL VPN Client (sslclient-win*.pkg) da Cisco Software Download (solo utenti registrati). Copiare lo SVC sulla memoria flash dell'appliance ASA. Per stabilire la connessione VPN SSL con l'appliance ASA, l'SVC deve essere scaricato sui computer degli utenti remoti.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Cisco serie 5500 ASA con software versione 8.x
- Cisco SSL VPN Client versione per Windows 1.1.4.179
- PC con Windows 2000 Professional o Windows XP
- Cisco Adaptive Security Device Manager (ASDM) versione 6.1(5)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

SSL VPN Client (SVC) è una tecnologia di tunneling VPN che offre agli utenti remoti i vantaggi di un client VPN IPSec senza la necessità per gli amministratori di rete di installare e configurare client VPN IPSec in computer remoti. SVC utilizza la crittografia SSL già presente nel computer remoto, nonché l'accesso e l'autenticazione WebVPN di Security Appliance.

Nello scenario corrente, un client VPN SSL si connette alle risorse interne dietro l'ASA tramite il tunnel VPN SSL. Split-tunnel non abilitato. Quando il client VPN SSL è connesso all'ASA, tutti i dati vengono tunneling. Oltre ad accedere alle risorse interne, il criterio principale è instradare il traffico tunneling attraverso il DTG (Default Tunneled Gateway).

Èpossibile definire un percorso predefinito separato per il traffico tunneling insieme al percorso predefinito standard. Il traffico non crittografato ricevuto dall'ASA, per il quale non esiste una route statica o appresa, viene instradato attraverso il percorso predefinito standard. Il traffico crittografato ricevuto dall'ASA, per il quale non vi è una route statica o appresa, verrà passato al DTG definito tramite la route predefinita del tunnel.

Per definire una route predefinita con tunneling, utilizzare questo comando:

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

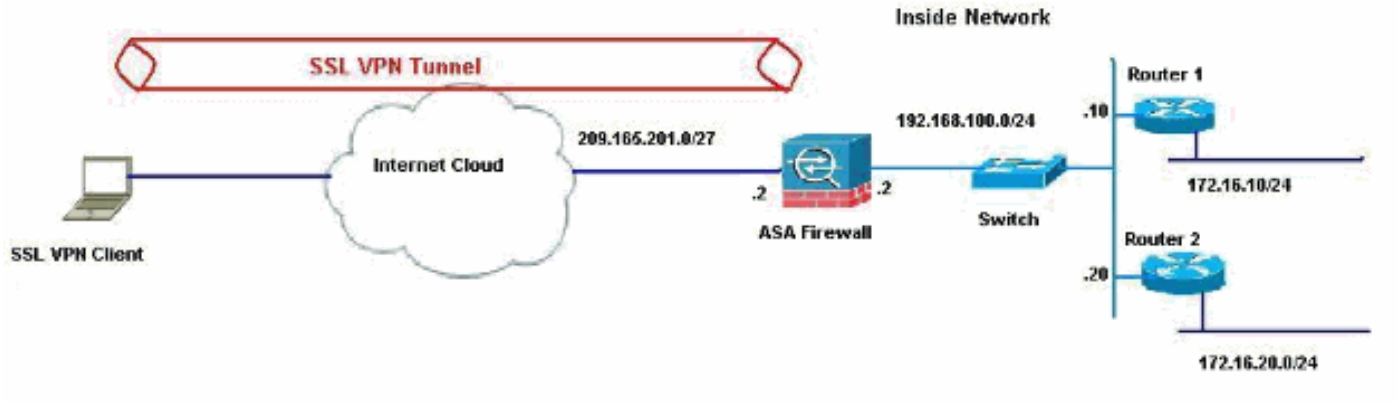
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nell'esempio, il client VPN SSL accede alla rete interna dell'ASA tramite il tunnel. Anche il traffico destinato a destinazioni diverse dalla rete interna viene tunneling, in quanto non è configurato uno split-tunnel, e viene instradato attraverso il TDG (192.168.100.20).

Dopo aver instradato i pacchetti al TDG, che in questo caso è il router 2, esegue la conversione degli indirizzi per instradare i pacchetti verso Internet. Per ulteriori informazioni su come configurare un router come gateway Internet, consultare il documento sulla configurazione di un router Cisco dietro un modem via cavo non Cisco.

Configurazione ASA con ASDM 6.1(5)

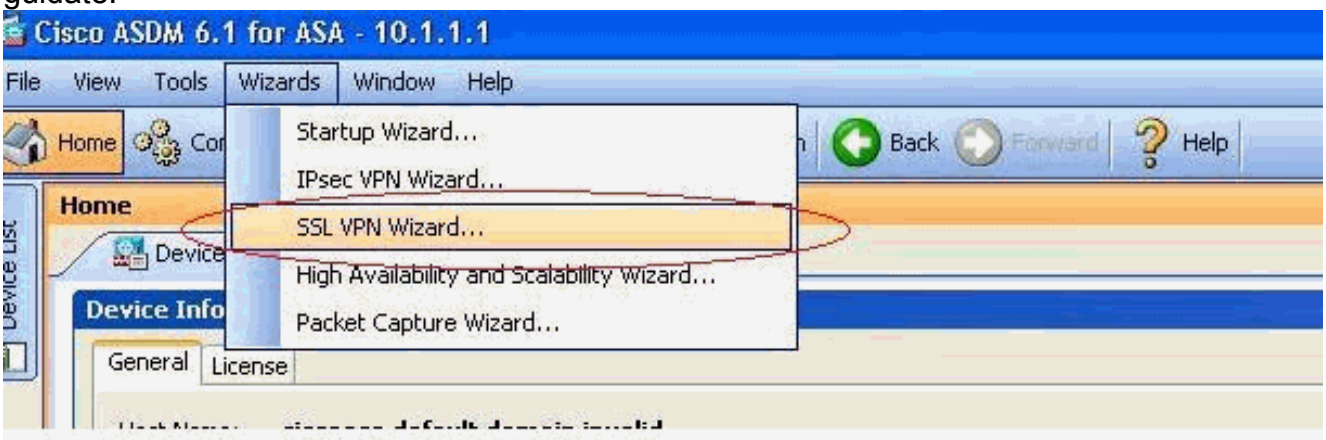
In questo documento si presume che le configurazioni di base, ad esempio la configurazione dell'interfaccia, siano complete e funzionino correttamente.

Nota: per informazioni su come consentire all'ASA di essere configurata dall'ASDM, consultare il documento sull'autorizzazione dell'accesso HTTPS per ASDM.

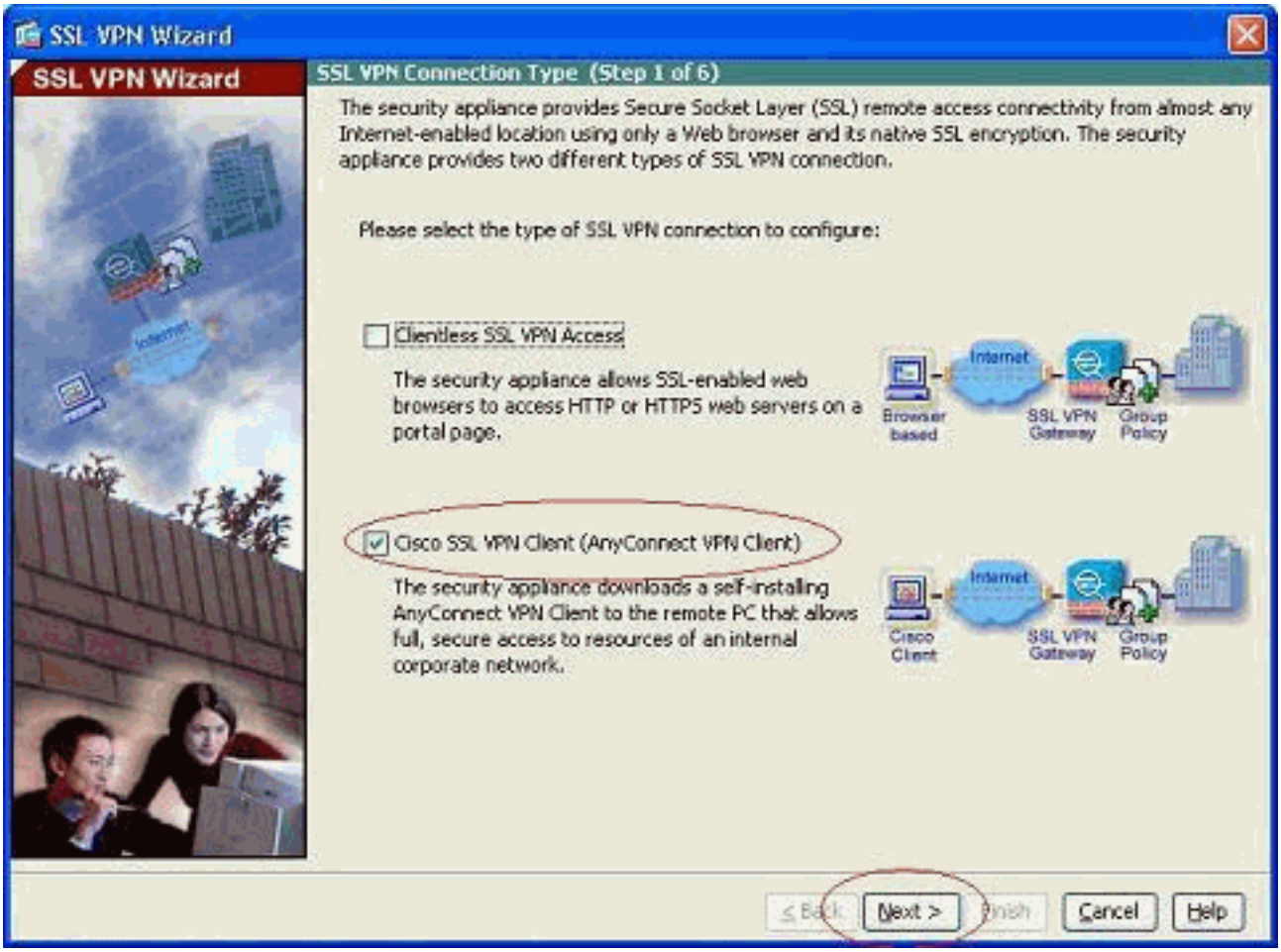
Nota: WebVPN e ASDM non possono essere abilitati sulla stessa interfaccia ASA a meno che non si modifichino i numeri di porta. Per ulteriori informazioni, fare riferimento a ASDM e WebVPN abilitati sulla stessa interfaccia dell'ASA.

Completare questa procedura per configurare la VPN SSL utilizzando la Creazione guidata VPN SSL.

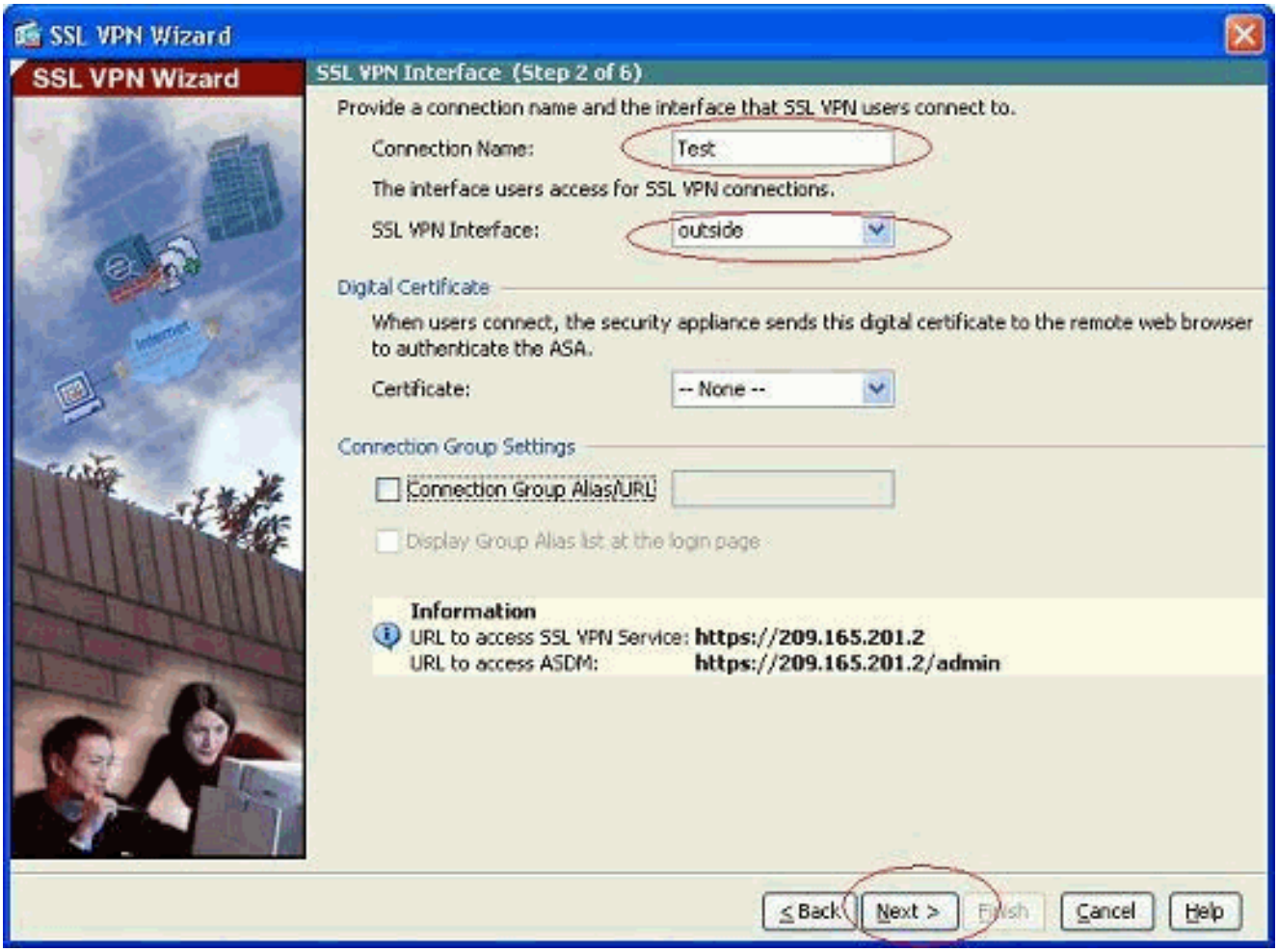
1. Scegliere **Creazione guidata VPN SSL** dal menu Procedure guidate.



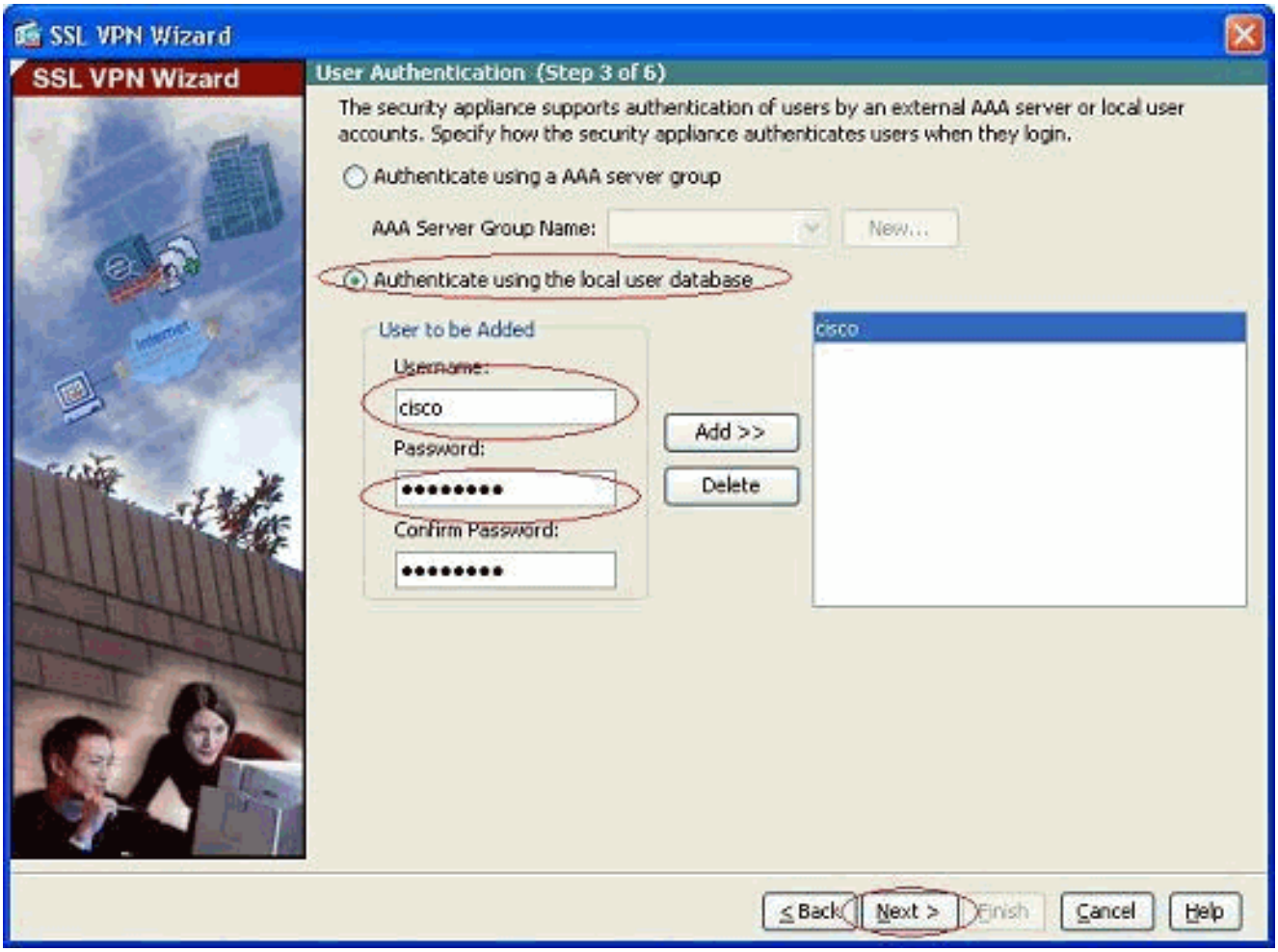
2. Selezionare la casella di controllo **Cisco SSL VPN Client** e fare clic su **Avanti**.



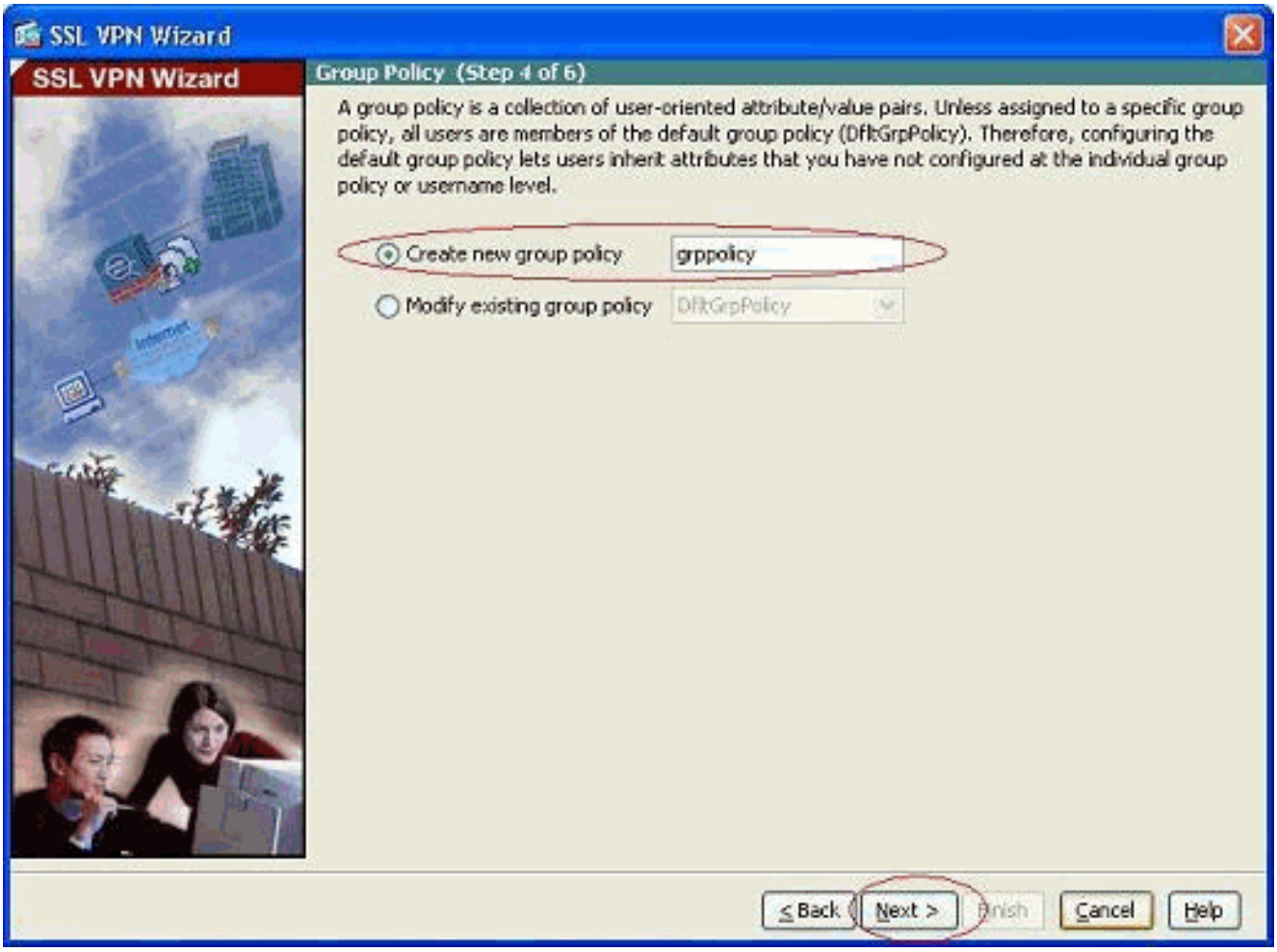
3. Immettere un nome per la connessione nel campo Nome connessione, quindi scegliere l'interfaccia utilizzata dall'utente per accedere alla VPN SSL dall'elenco a discesa Interfaccia VPN
   SSL.



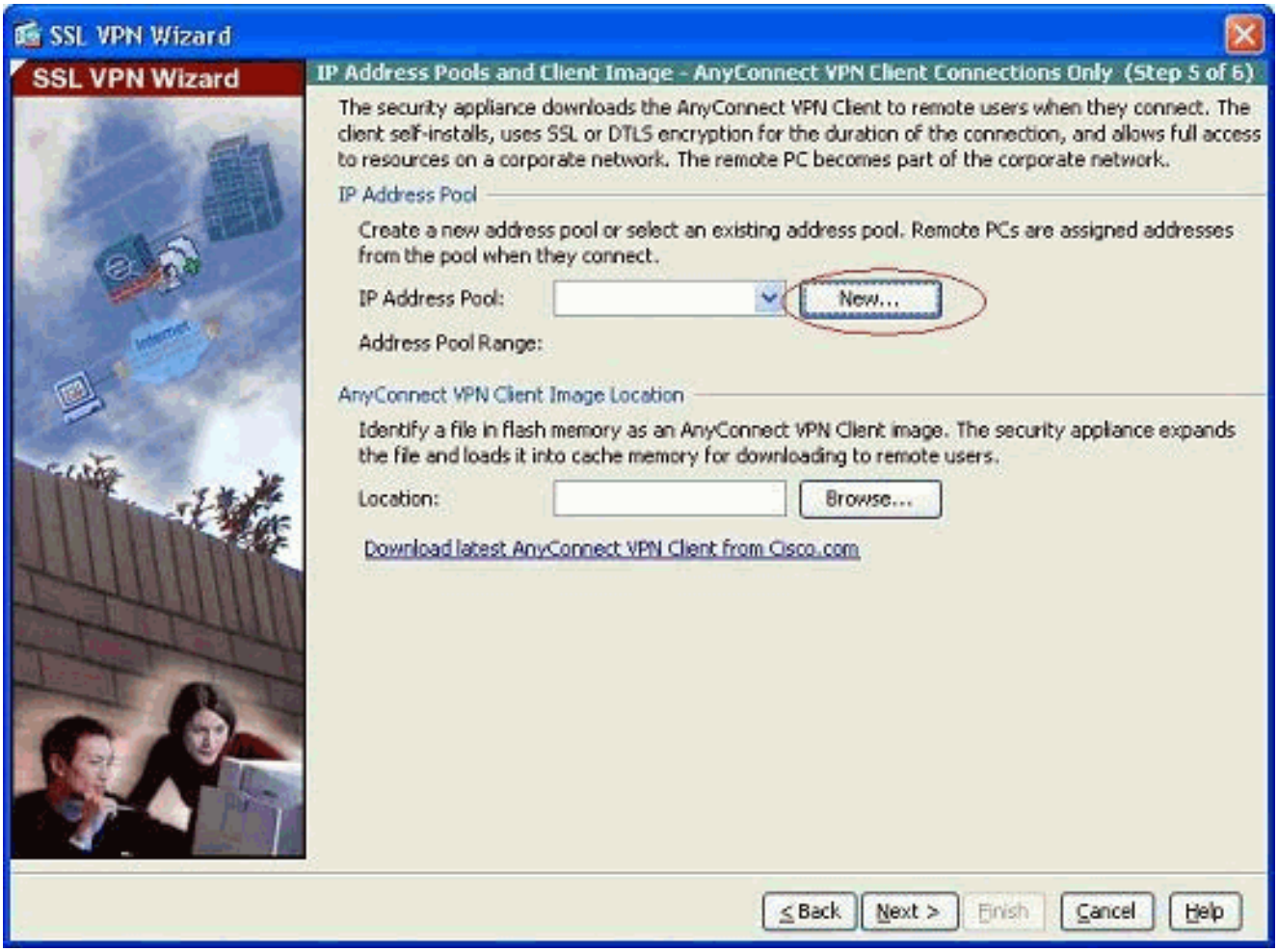
4. Fare clic su **Next** (Avanti).
5. Scegliere una modalità di autenticazione e fare clic su **Avanti**. In questo esempio viene utilizzata l'autenticazione
   locale.



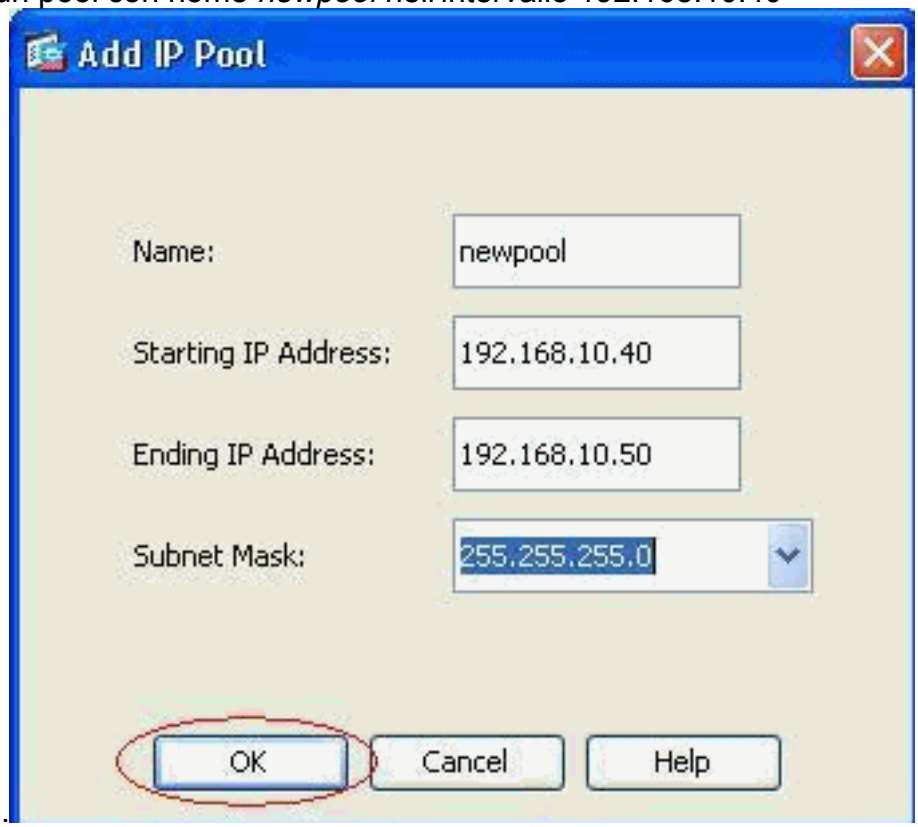
6. Creare un nuovo criterio di gruppo diverso da quello predefinito esistente.



7. Crea un nuovo pool di indirizzi che verrà assegnato ai PC client VPN SSL dopo la connessione.

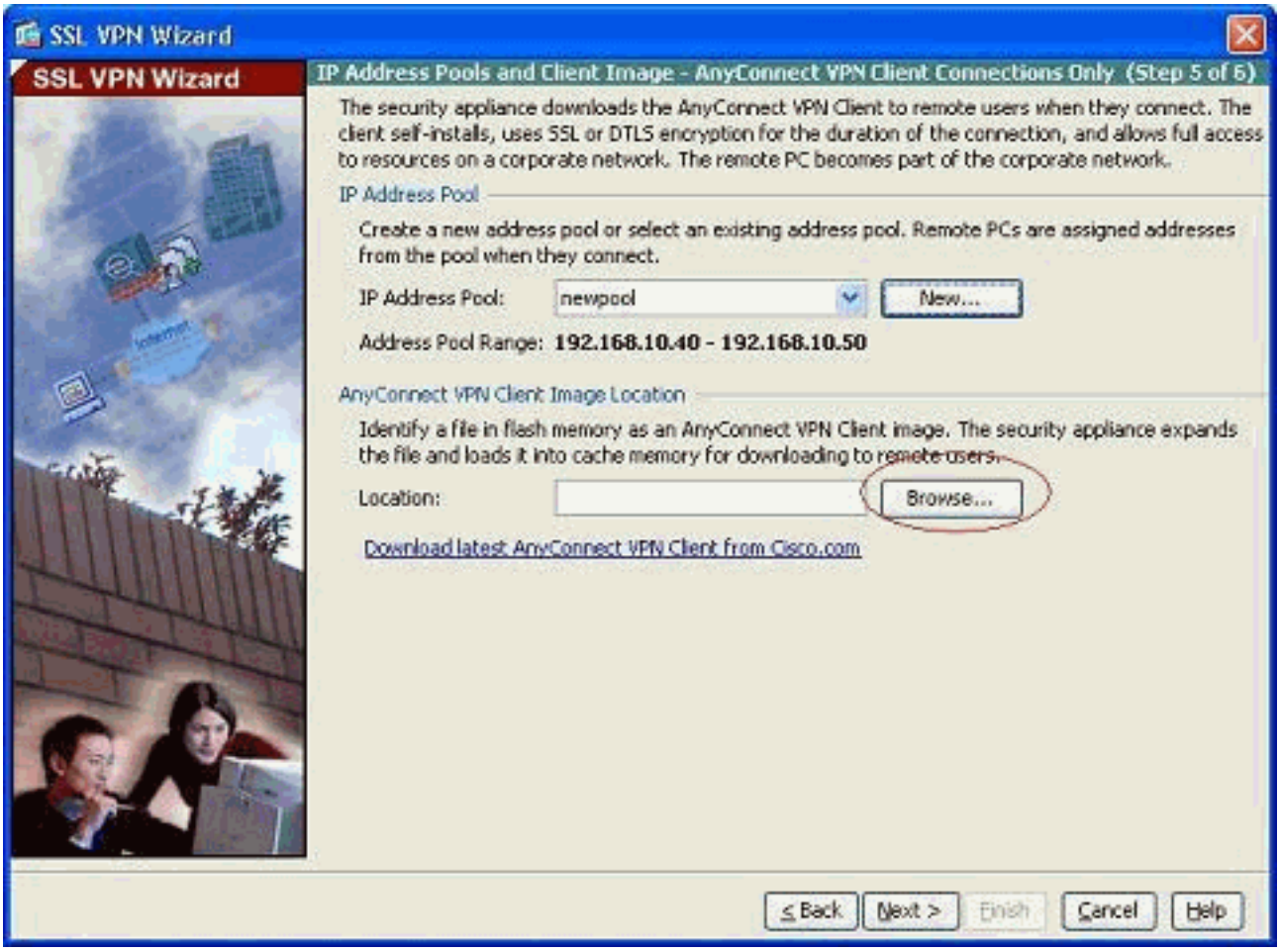


Èstato creato un pool con nome *newpool* nell'intervallo 192.168.10.40-192.168.10.50.



8. Fare clic su **Browse** per scegliere e caricare l'immagine VPN Client SSL nella memoria flash dell'appliance

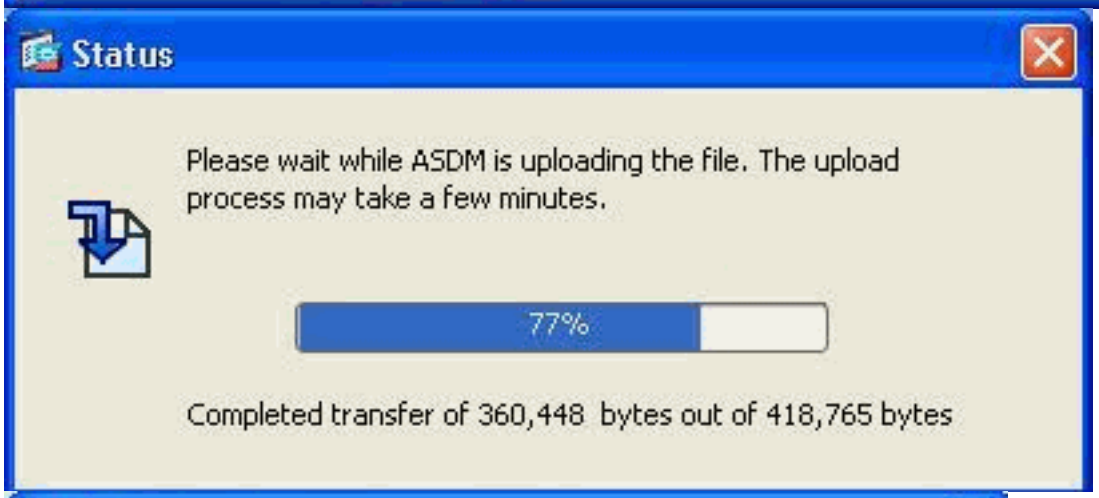
ASA.



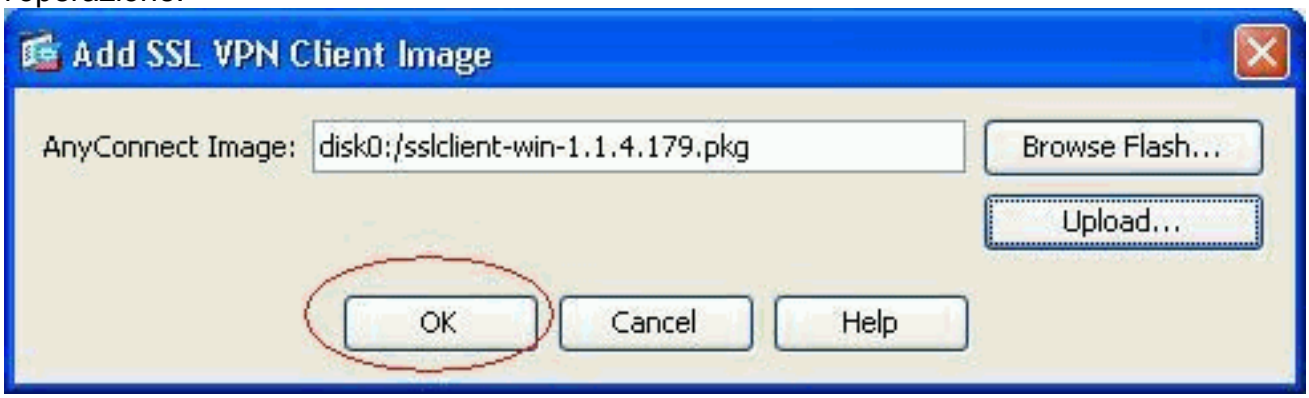
9. Fare clic su **Upload** per impostare il percorso del file dalla directory locale del computer.

10. Fare clic su **Sfoglia file locali** per selezionare la directory in cui si trova il file sslclient.pkg.

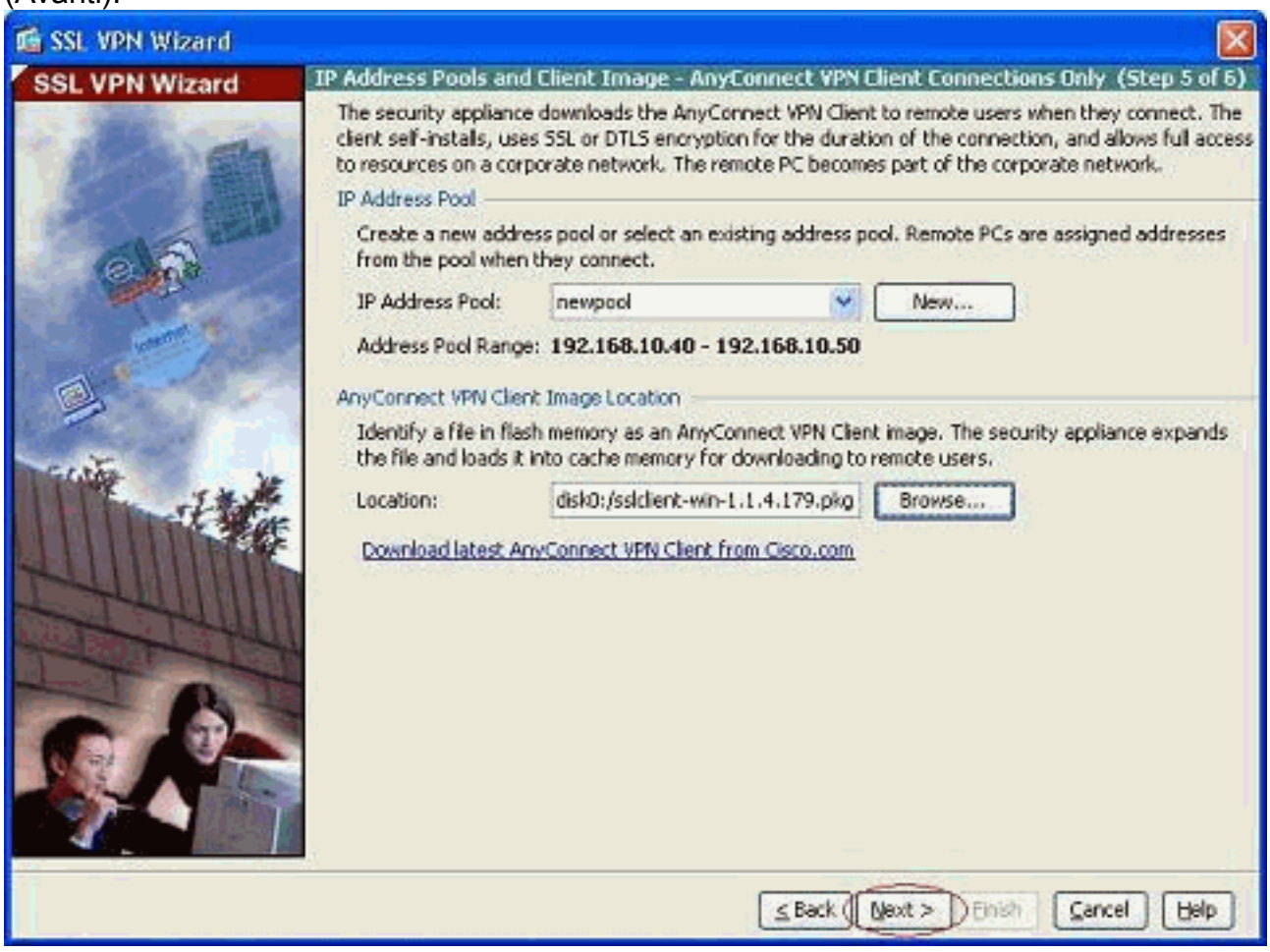
11. Per caricare il file selezionato nella memoria flash dell'ASA, fare clic su **Upload File**.



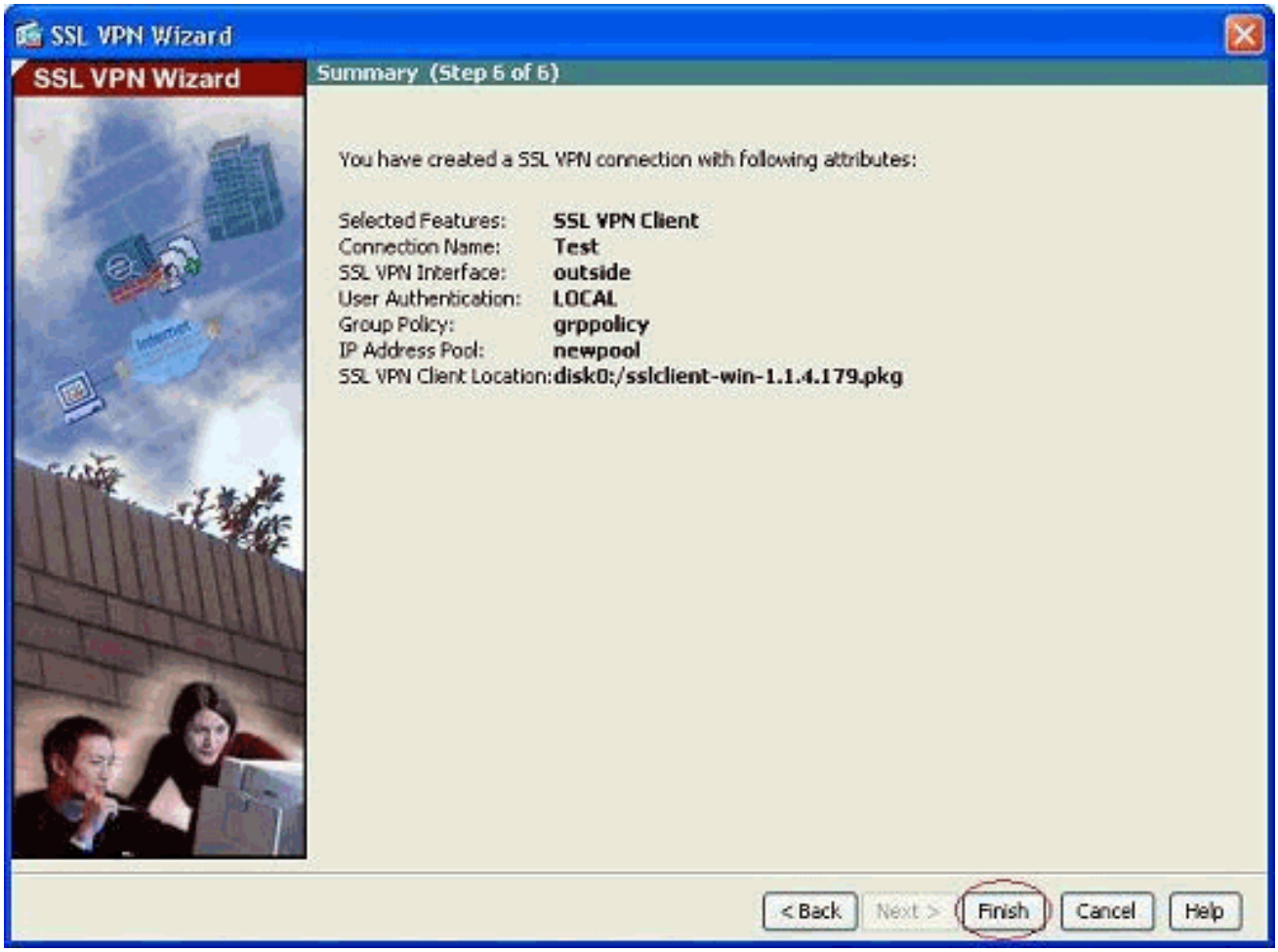
12. Una volta caricato il file sulla memoria flash dell'ASA, fare clic su **OK** per completare l'operazione.



13. Ora mostra l'ultimo file anyconnect pkg caricato sulla memoria flash dell'ASA. Fare clic su **Next**
(Avanti).



14. Viene visualizzato il riepilogo della configurazione del client VPN SSL. Fare clic su **Fine** per completare la procedura
guidata.



La configurazione mostrata in ASDM si riferisce principalmente alla configurazione guidata del client VPN SSL.

Dalla CLI, è possibile osservare alcune configurazioni aggiuntive. La configurazione CLI completa è mostrata di seguito e sono stati evidenziati alcuni comandi importanti.

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#
```

Verifica

I comandi forniti in questa sezione possono essere usati per verificare questa configurazione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **show webvpn svc**: visualizza le immagini SVC memorizzate nella memoria flash ASA.
- **show VPN-sessiondb svc**: visualizza le informazioni sulle connessioni SSL correnti.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Cisco serie 5500 Adaptive Security Appliance Support
- Esempio di configurazione di PIX/ASA e VPN Client per VPN Internet pubblica su Memory Stick
- Esempio di configurazione di SSL VPN Client (SVC) su ASA con ASDM
- Documentazione e supporto tecnico – Cisco Systems