ASA 8.x: Konfigurationsbeispiel für das Routing von SSL-VPN-Datenverkehr durch das Tunneled Standard-Gateway

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Adaptive Security Appliance (ASA) so konfiguriert wird, dass der SSL VPN-Datenverkehr über das getunnelte Standard-Gateway (TDG) weitergeleitet wird. Wenn Sie eine Standardroute mit der Option getunnelt erstellen, wird der gesamte Datenverkehr eines auf der ASA terminierenden Tunnels, der nicht über erlernte oder statische Routen weitergeleitet werden kann, an diese Route gesendet. Bei einem Tunnel aufkommenden Datenverkehr überschreibt diese Route alle anderen konfigurierten oder abgefragten Standardrouten.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- ASA mit Version 8.x
- Cisco SSL VPN Client (SVC) 1.x**Hinweis:** Laden Sie das SSL VPN Client-Paket (sslclient-win*.pkg) vom Cisco Software Download (nur registrierte Kunden) herunter. Kopieren Sie den SVC in den Flash-Speicher der ASA. Der SVC muss auf die Computer der Remote-Benutzer heruntergeladen werden, um die SSL VPN-Verbindung mit der ASA herzustellen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ASA der Serie 5500 mit Softwareversion 8.x
- Cisco SSL VPN Client-Version für Windows 1.1.4.179
- PC, auf dem Windows 2000 Professional oder Windows XP ausgeführt wird
- Cisco Adaptive Security Device Manager (ASDM) Version 6.1(5)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Der SSL VPN Client (SVC) ist eine VPN-Tunneling-Technologie, die Remote-Benutzern die Vorteile eines IPSec VPN-Clients bietet, ohne dass Netzwerkadministratoren IPSec VPN-Clients auf Remote-Computern installieren und konfigurieren müssen. Der SVC verwendet die SSL-Verschlüsselung, die bereits auf dem Remote-Computer vorhanden ist, sowie die WebVPN-Anmeldung und -Authentifizierung der Security Appliance.

Im aktuellen Szenario ist ein SSL VPN-Client vorhanden, der über den SSL VPN-Tunnel mit den internen Ressourcen hinter der ASA verbunden ist. Der Split-Tunnel ist nicht aktiviert. Wenn der SSL VPN-Client mit der ASA verbunden ist, werden alle Daten getunnelt. Neben dem Zugriff auf die internen Ressourcen besteht das Hauptkriterium darin, diesen getunnelten Verkehr über das Default Tunneled Gateway (DTG) zu leiten.

Sie können zusammen mit der Standardroute eine separate Standardroute für getunnelten Datenverkehr definieren. Der von der ASA empfangene unverschlüsselte Datenverkehr, für den es keine statische oder abgefragte Route gibt, wird über die Standardroute weitergeleitet. Der von der ASA empfangene verschlüsselte Datenverkehr, für den es keine statische oder abgefragte Route gibt, wird über die getunnelte Standardroute an die DTG weitergeleitet.

Verwenden Sie den folgenden Befehl, um eine getunnelte Standardroute zu definieren:

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

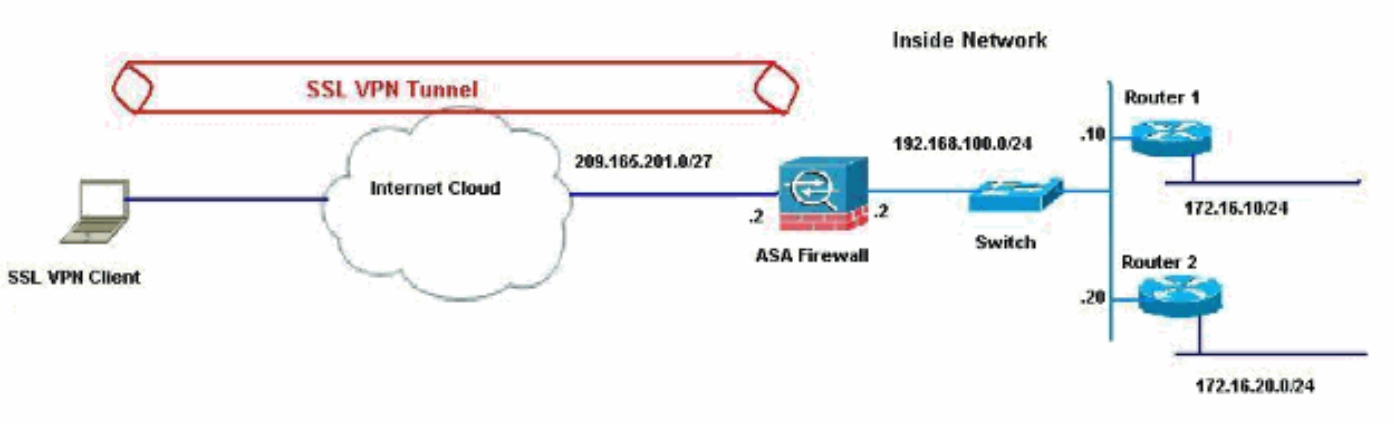
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



In diesem Beispiel greift der SSL VPN-Client über den Tunnel auf das interne Netzwerk der ASA zu. Der Datenverkehr für andere Ziele als das interne Netzwerk wird ebenfalls getunnelt, da kein Split-Tunnel konfiguriert ist, und wird über das TDG (192.168.100.20) geleitet.

Nachdem die Pakete an das TDG geroutet wurden, das in diesem Fall Router 2 ist, führt es die Adressumwandlung durch, um diese Pakete über das Internet weiterzuleiten. Weitere Informationen zum Konfigurieren eines Routers als Internet-Gateway finden Sie unter Konfigurieren eines Cisco Routers hinter einem nicht von Cisco stammenden Kabelmodem.

ASA-Konfiguration mit ASDM 6.1(5)

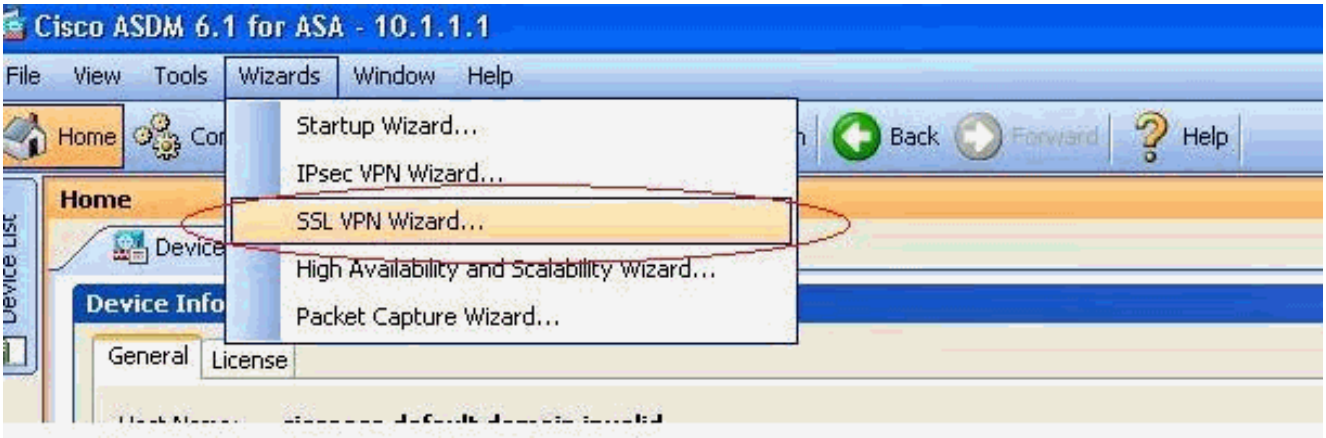
In diesem Dokument wird davon ausgegangen, dass die grundlegenden Konfigurationen, z. B. die Schnittstellenkonfiguration, vollständig sind und ordnungsgemäß funktionieren.

Hinweis: Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

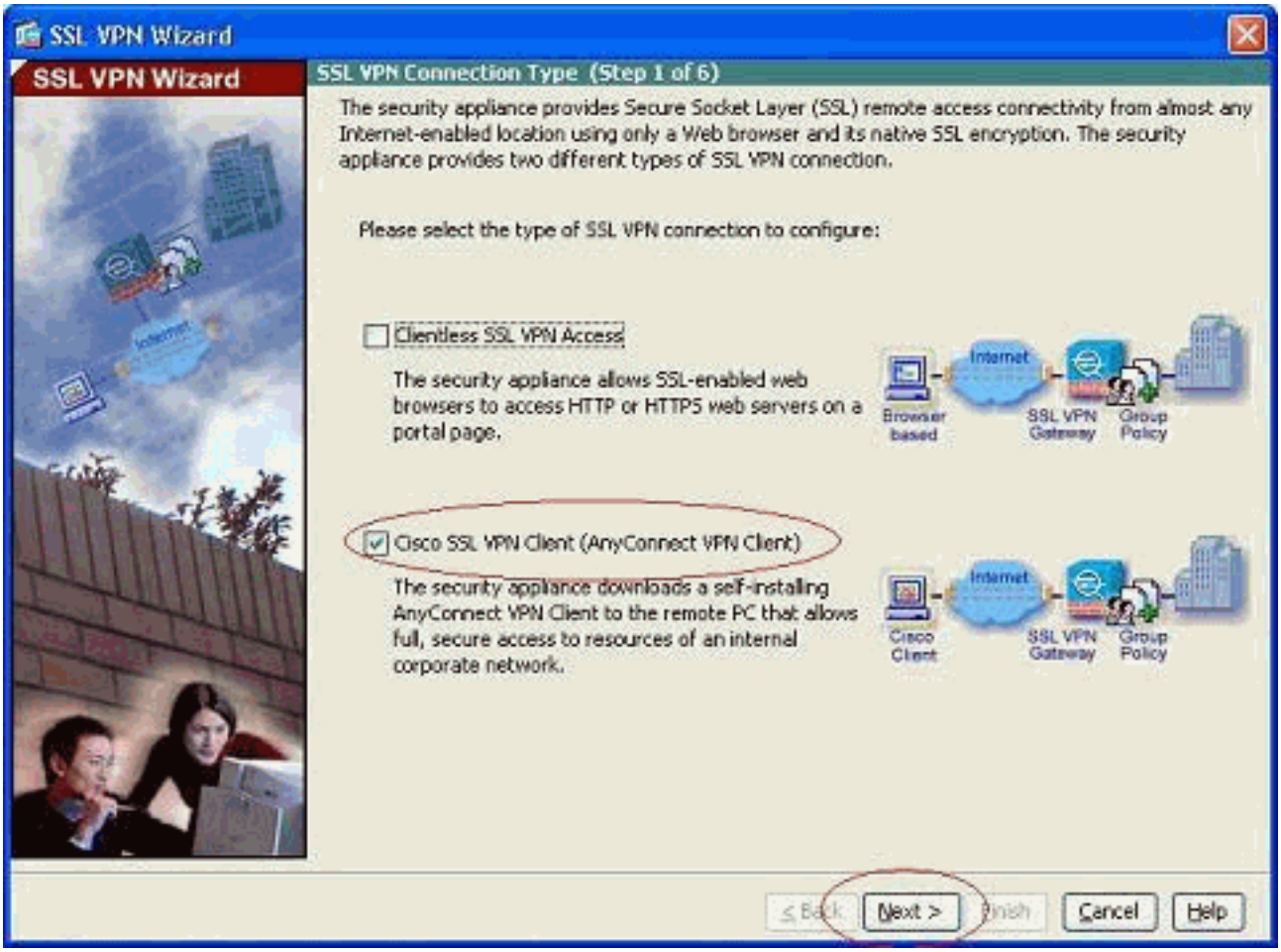
Hinweis: WebVPN und ASDM können nicht auf derselben ASA-Schnittstelle aktiviert werden, es sei denn, Sie ändern die Portnummern. Weitere Informationen finden Sie unter ASDM und WebVPN Enabled auf derselben ASA-Schnittstelle.

Führen Sie diese Schritte aus, um das SSL VPN mithilfe des SSL VPN-Assistenten zu konfigurieren.

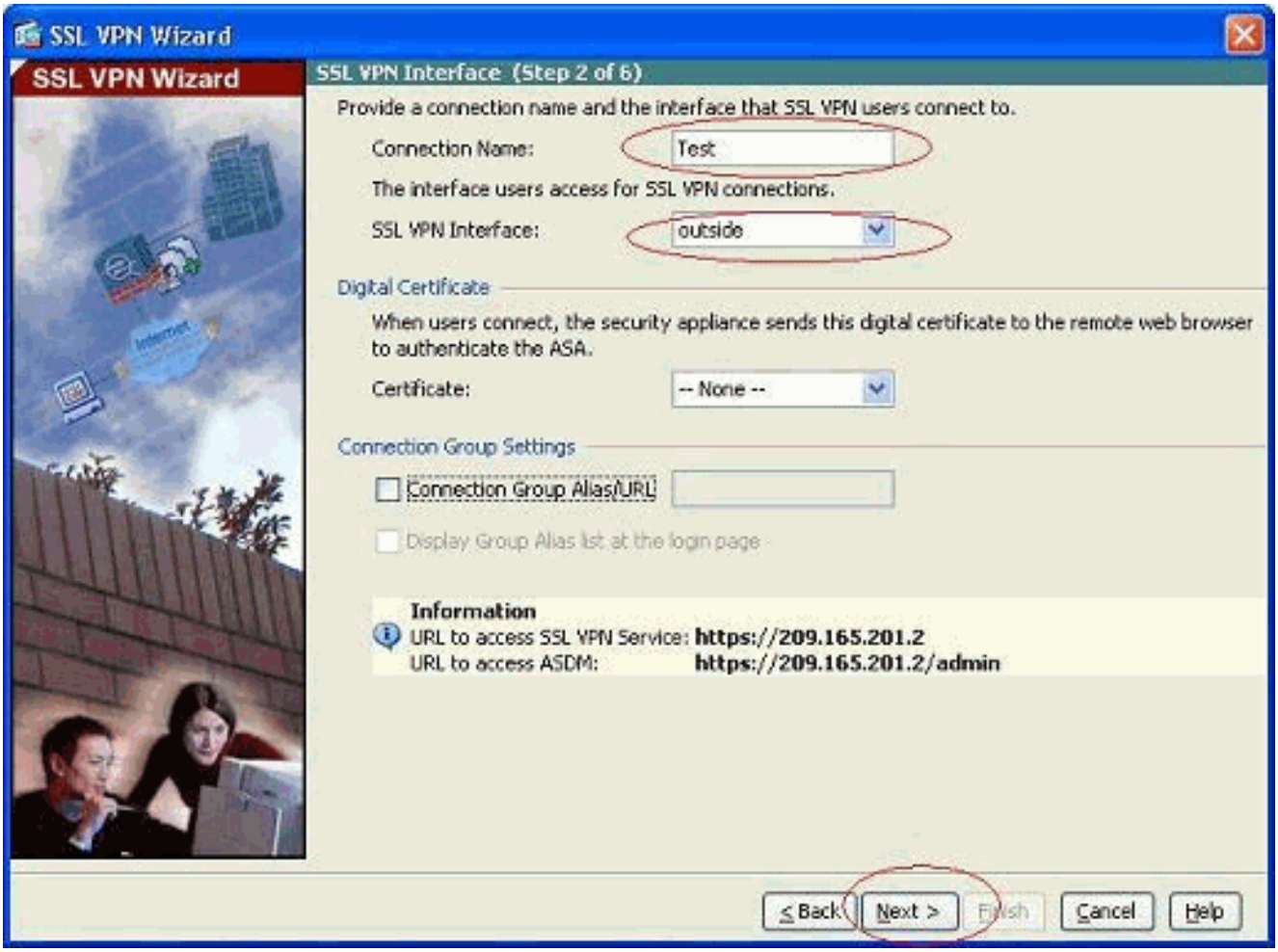
1. Wählen Sie im Menü Assistenten die Option **SSL VPN Wizard** aus.



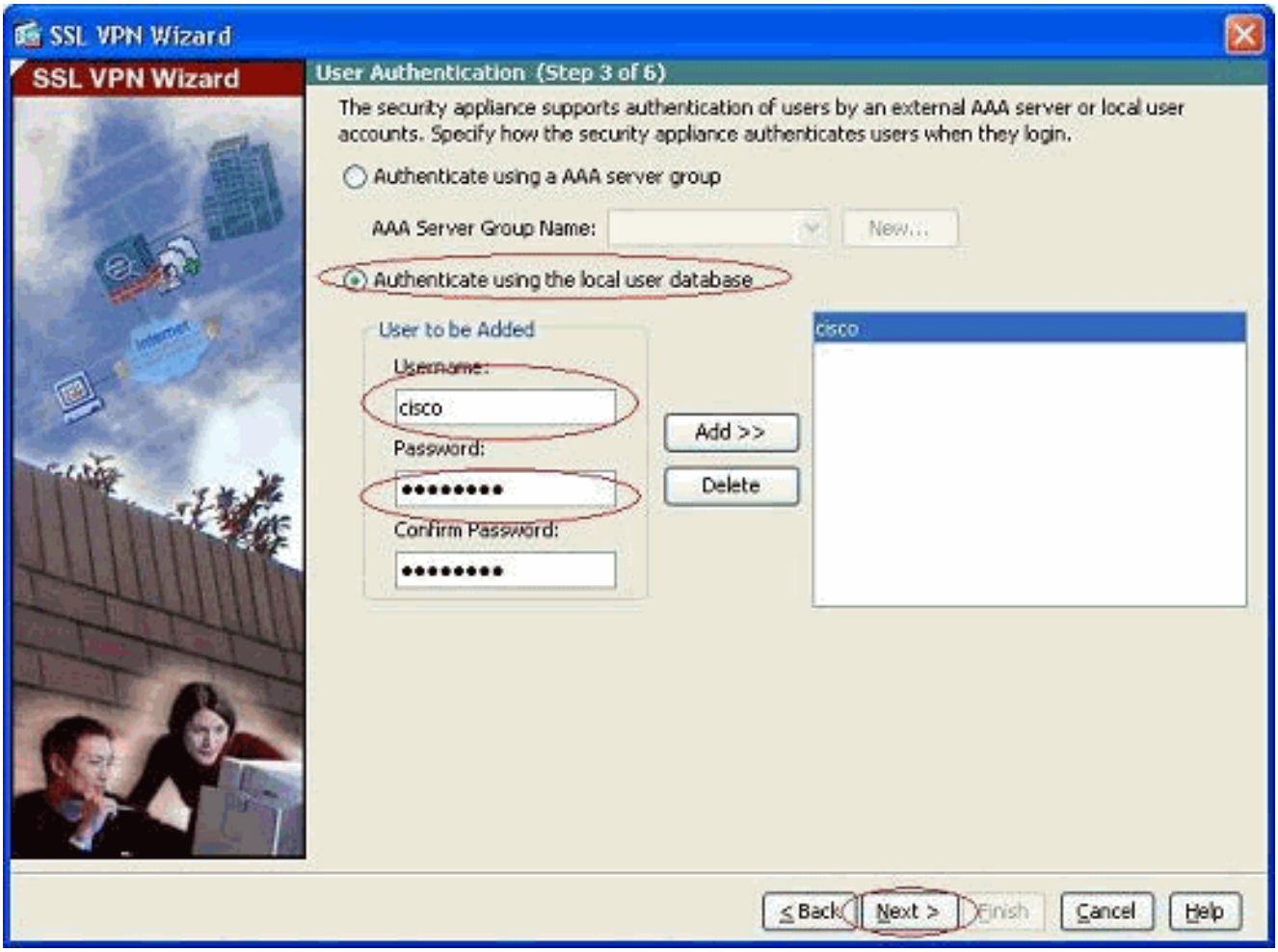
2. Aktivieren Sie das Kontrollkästchen **Cisco SSL VPN Client**, und klicken Sie auf **Weiter**.



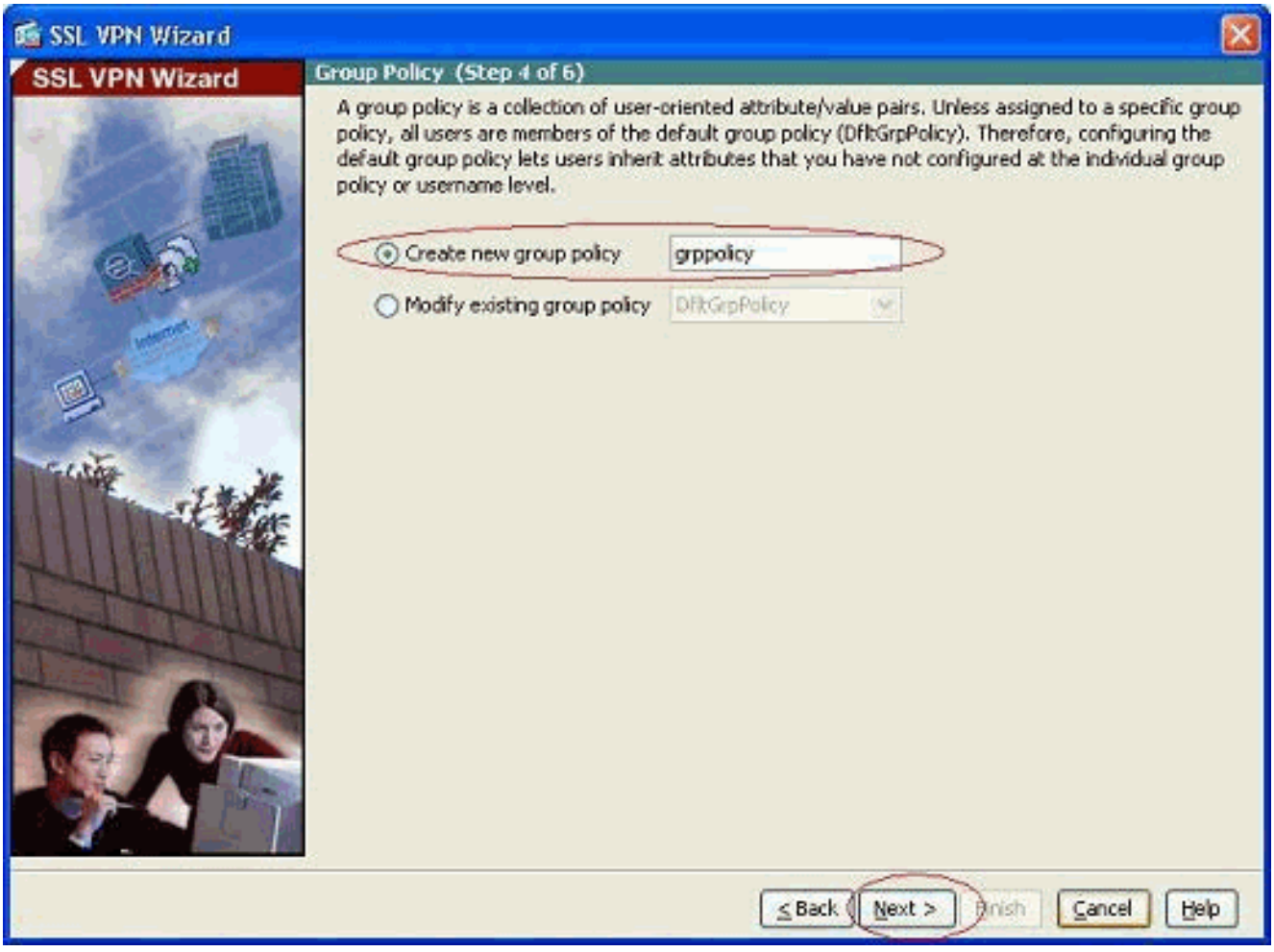
3. Geben Sie im Feld Connection Name (Verbindungsname) einen Namen für die Verbindung ein, und wählen Sie dann die Schnittstelle aus, die der Benutzer verwendet, um über die Dropdown-Liste SSL VPN Interface (SSL VPN-Schnittstelle) auf das SSL VPN zuzugreifen.



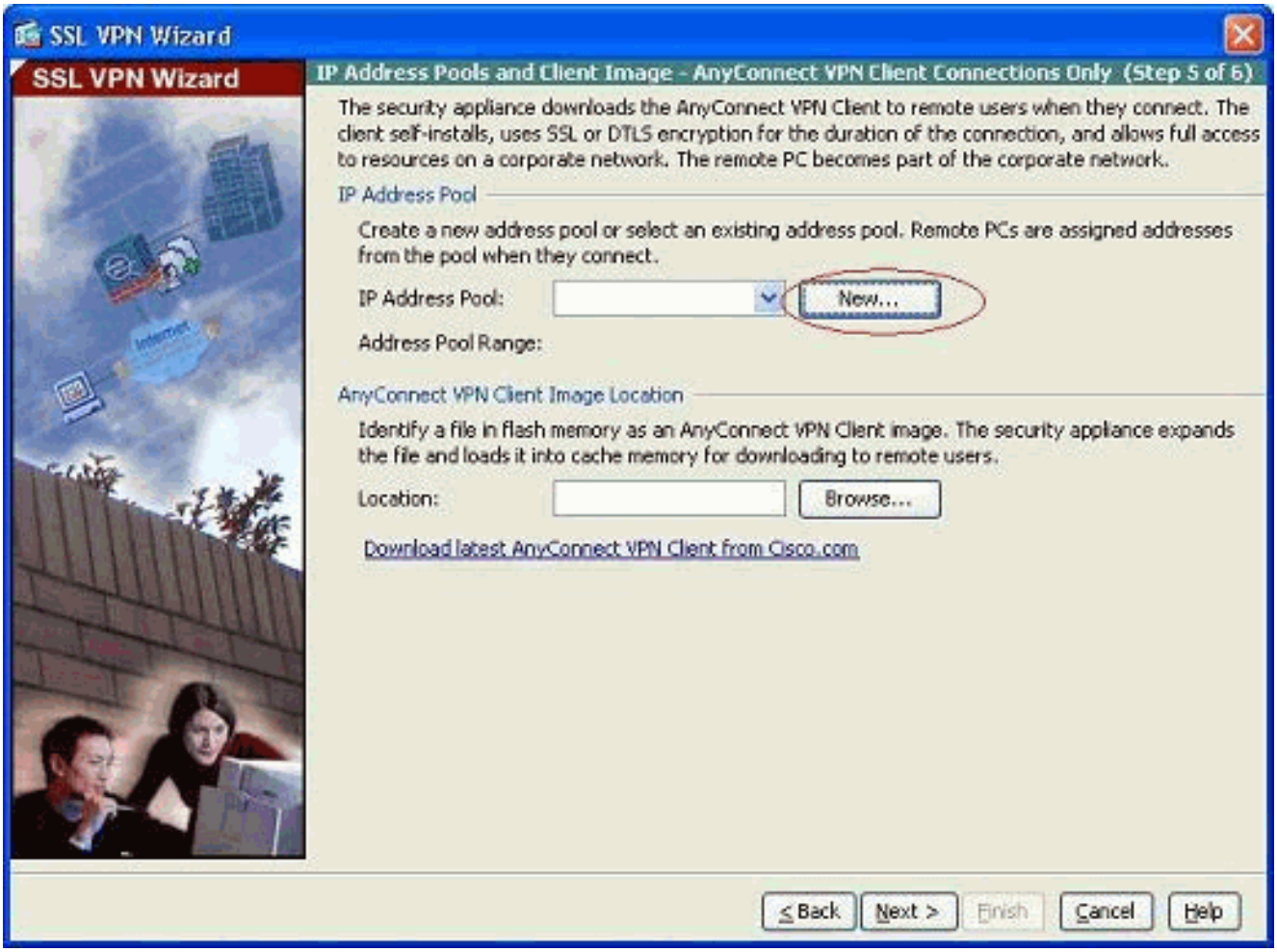
4. Klicken Sie auf **Weiter**.
5. Wählen Sie einen Authentifizierungsmodus aus, und klicken Sie auf **Weiter**. (In diesem Beispiel wird die lokale Authentifizierung verwendet.)



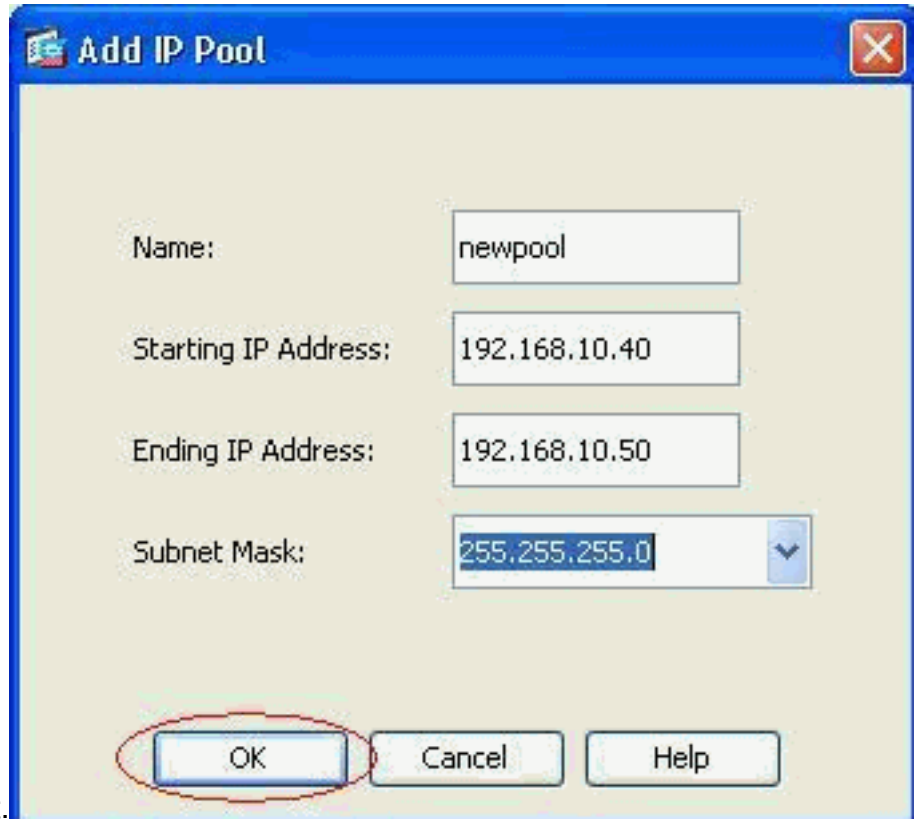
6. Erstellen Sie eine neue Gruppenrichtlinie, die nicht die vorhandene Standardgruppenrichtlinie ist.



7. Erstellen Sie einen neuen Adresspool, der den SSL VPN-Client-PCs zugewiesen wird, sobald sie verbunden
werden.



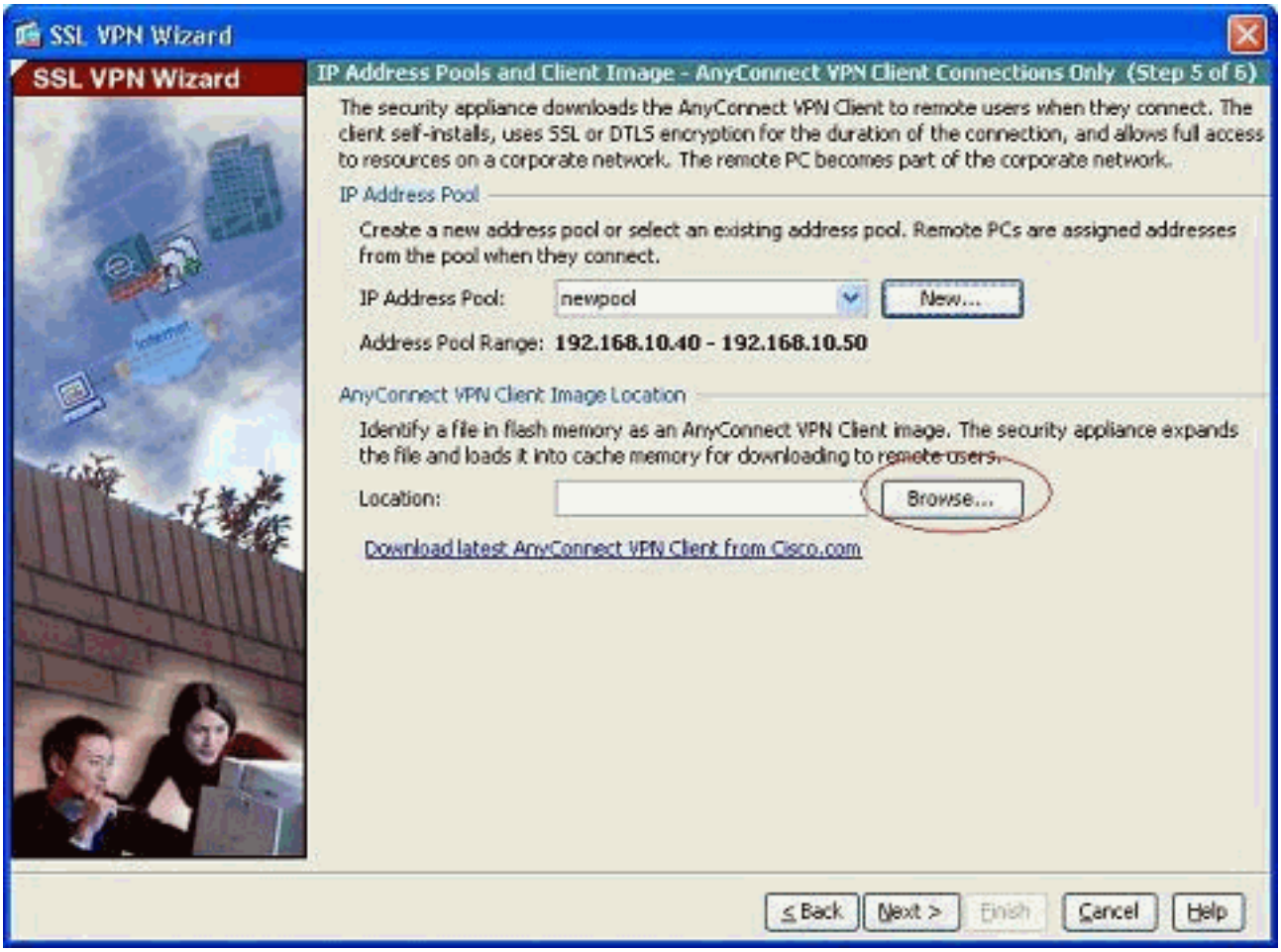
Ein Pool des Bereichs 192.168.10.40-192.168.10.50 wurde mit dem Namen *newpool*



erstellt.

8. Klicken Sie auf **Durchsuchen**, um das SSL VPN Client-Image auszuwählen und in den Flash-

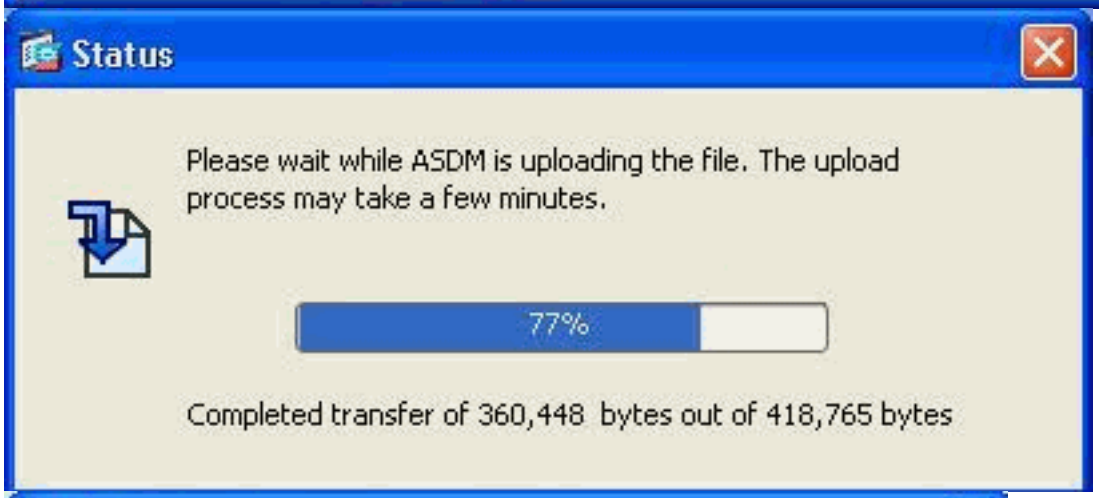
Speicher der ASA
hochzuladen.



9. Klicken Sie auf **Upload**, um den Dateipfad aus dem lokalen Verzeichnis des Computers festzulegen.

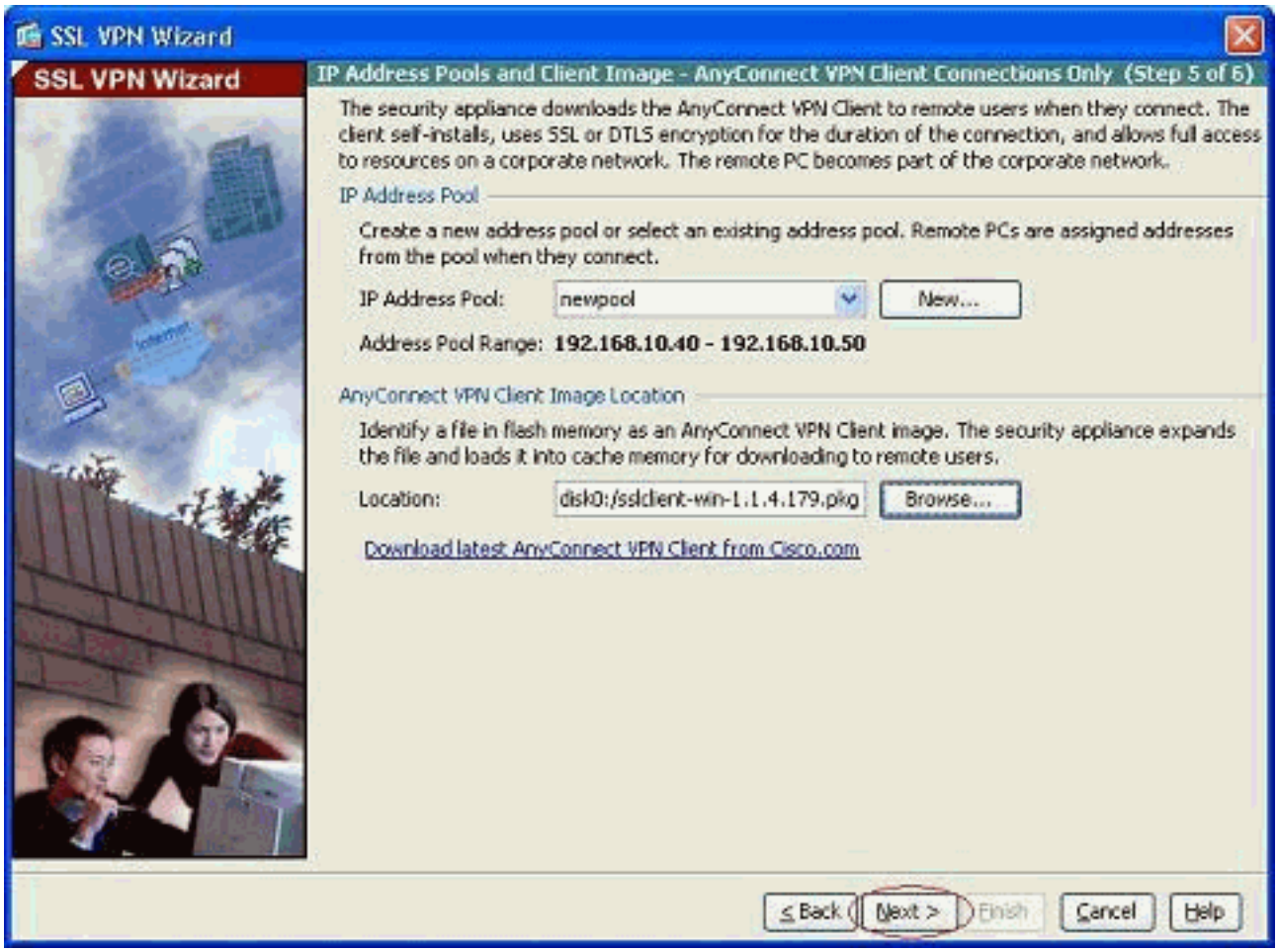
10. Klicken Sie auf **Lokale Dateien durchsuchen**, um das Verzeichnis auszuwählen, in dem die Datei sslclient.pkg vorhanden
ist.

11. Klicken Sie auf **Datei hochladen**, um die ausgewählte Datei in den Flash-Speicher der ASA hochzuladen.

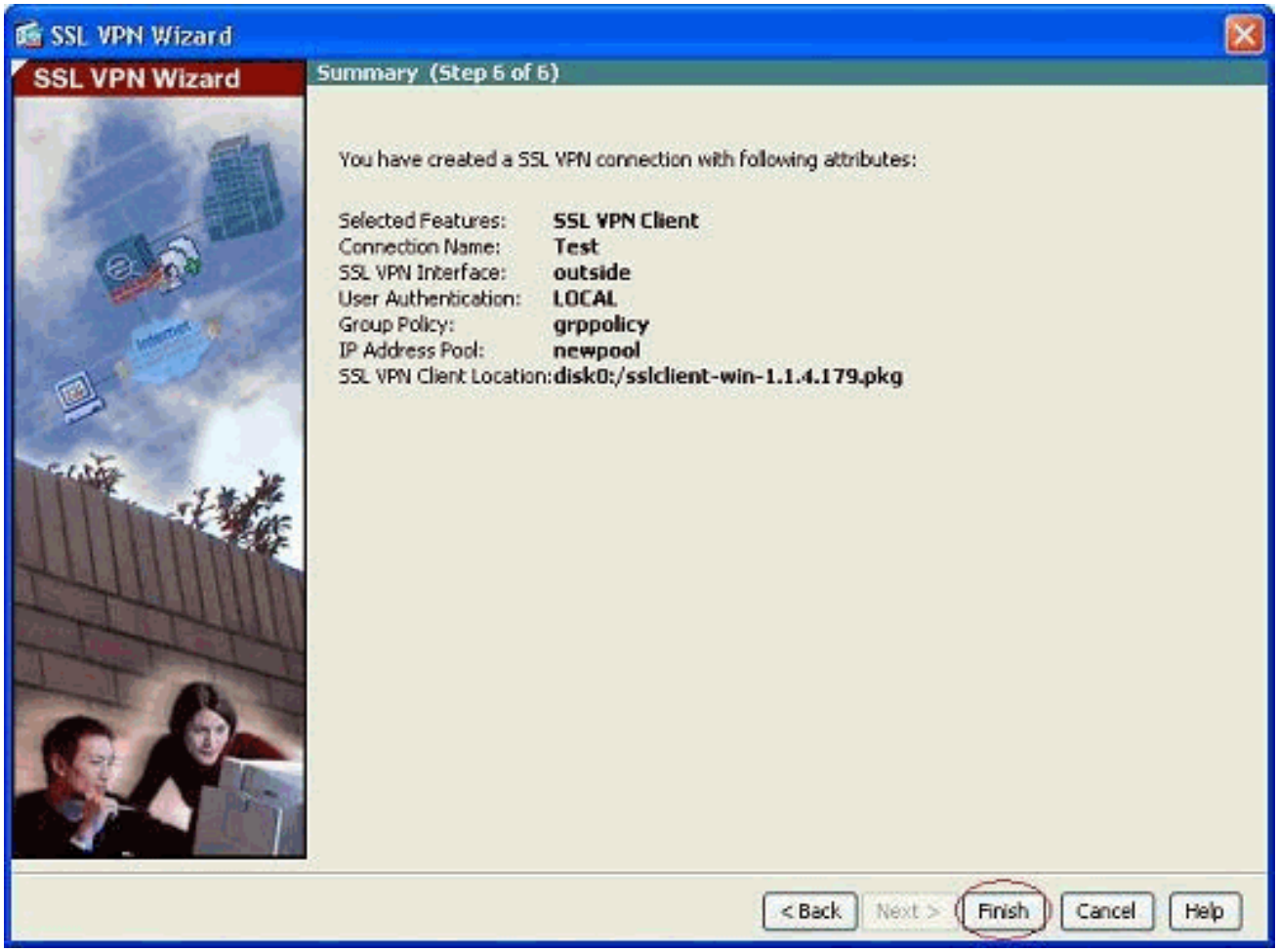


12. Wenn die Datei im Flash-Speicher der ASA hochgeladen wurde, klicken Sie auf **OK**, um diese Aufgabe abzuschließen.

13. Jetzt wird die neueste anyconnect pkg-Datei angezeigt, die auf den Flash-Speicher der ASA hochgeladen wurde. Klicken Sie auf **Weiter**.



14. Die Zusammenfassung der SSL VPN-Client-Konfiguration wird angezeigt. Klicken Sie auf **Fertig stellen**, um den Assistenten abzuschließen.



Die Konfiguration in ASDM bezieht sich hauptsächlich auf die Konfiguration des SSL VPN-Client-Assistenten.

In der CLI können Sie einige zusätzliche Konfigurationen beobachten. Nachfolgend wird die vollständige CLI-Konfiguration dargestellt, und wichtige Befehle wurden hervorgehoben.

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#
```

Überprüfen

Die in diesem Abschnitt angegebenen Befehle können verwendet werden, um diese Konfiguration zu überprüfen.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show webvpn svc**: Zeigt die im ASA-Flash-Speicher gespeicherten SVC-Images an.
- **show VPN-sessiondb svc**: Zeigt Informationen über die aktuellen SSL-Verbindungen an.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Unterstützung für Cisco Adaptive Security Appliances der Serie 5500
- Beispiel für eine Stick-Konfiguration: PIX/ASA und VPN-Client für Public Internet VPN
- SSL VPN Client (SVC) auf ASA mit ASDM - Konfigurationsbeispiel
- Technischer Support und Dokumentation - Cisco Systems