ASA 8.X: 터널링된 기본 게이트웨이 구성을 통해 SSL VPN 트래픽 라우팅 예

목차

소개

이 문서에서는 터널링된 기본 게이트웨이(TDG)를 통해 SSL VPN 트래픽을 라우팅하도록 ASA(Adaptive Security Appliance)를 구성하는 방법에 대해 설명합니다. tunneled 옵션을 사용하여 기본 경로를 생성하면 학습된 경로 또는 고정 경로를 사용하여 라우팅할 수 없는 ASA에서 종료되는 터널의 모든 트래픽이 이 경로로 전송됩니다. 터널에서 발생하는 트래픽의 경우 이 경로는 다른 구성 또는 학습된 기본 경로를 재정의합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 버전 8.x에서 실행되는 ASA
- Cisco SSL VPN Client(SVC) 1.x**참고:** Cisco 소프트웨어 다운로드(등록된 고객만 해당)에서 SSL VPN 클라이언트 패키지(sslclient-win*.pkg)를 다운로드합니다. ASA의 플래시 메모리에 SVC를 복사합니다. ASA와의 SSL VPN 연결을 설정하려면 SVC를 원격 사용자 컴퓨터로 다운로드해야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 8.x를 실행하는 Cisco 5500 Series ASA
- Windows 1.1.4.179용 Cisco SSL VPN Client 버전
- Windows 2000 Professional 또는 Windows XP를 실행하는 PC
- Cisco ASDM(Adaptive Security Device Manager) 버전 6.1(5)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

SVC(SSL VPN Client)는 원격 사용자에게 IPSec VPN 클라이언트를 설치 및 구성할 필요 없이 IPSec VPN 클라이언트의 이점을 제공하는 VPN 터널링 기술입니다. SVC는 원격 컴퓨터에 이미 있는 SSL 암호화와 보안 어플라이언스의 WebVPN 로그인 및 인증을 사용합니다.

현재 시나리오에서는 SSL VPN 터널을 통해 ASA 뒤의 내부 리소스에 연결하는 SSL VPN 클라이언트가 있습니다. 스플릿 터널이 활성화되지 않았습니다. SSL VPN 클라이언트가 ASA에 연결되면 모든 데이터가 터널링됩니다. 내부 리소스에 액세스하는 것 외에도, 주요 기준은 이 터널링된 트래픽을 DTG(Default Tunneled Gateway)를 통해 라우팅하는 것입니다.

표준 기본 경로와 함께 터널링된 트래픽에 대해 별도의 기본 경로를 정의할 수 있습니다. 고정 경로 또는 학습된 경로가 없는 ASA에서 수신한 암호화되지 않은 트래픽은 표준 기본 경로를 통해 라우팅됩니다. 고정 경로 또는 학습 경로가 없는 ASA에서 수신한 암호화된 트래픽은 터널링된 기본 경로를 통해 정의된 DTG로 전달됩니다.

터널링된 기본 경로를 정의하려면 다음 명령을 사용합니다.

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

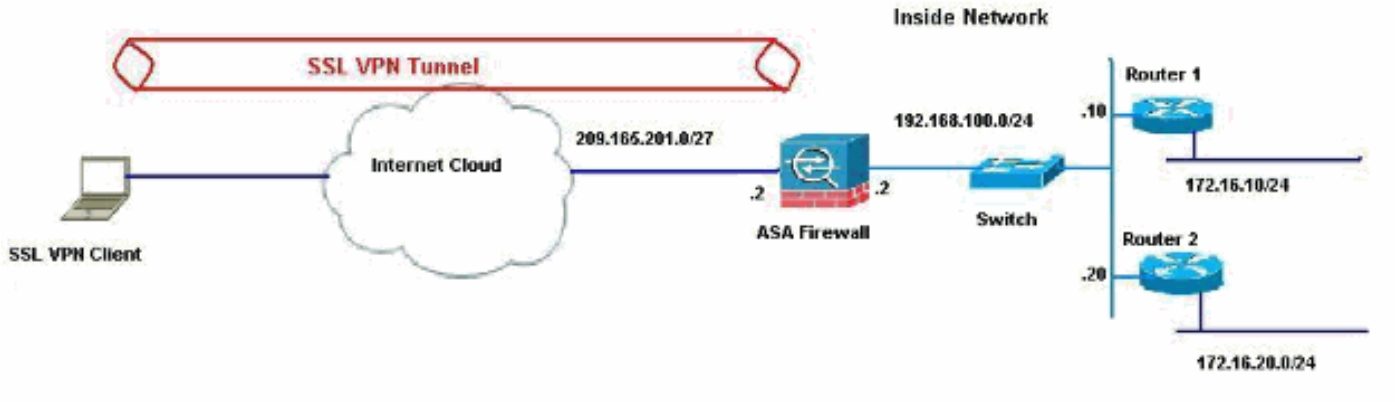
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



이 예에서 SSL VPN 클라이언트는 터널을 통해 ASA의 내부 네트워크에 액세스합니다. 내부 네트워크 이외의 목적지를 위한 트래픽도 터널링됩니다. 스플릿 터널이 구성되지 않고 TDG(192.168.100.20)을 통해 라우팅되기 때문입니다.

패킷이 라우터 2인 TDG로 라우팅되면 주소 변환을 수행하여 해당 패킷을 인터넷에 미리 라우팅합니다. 라우터를 인터넷 게이트웨이로 구성하는 방법에 대한 자세한 내용은 Cisco 이외의 케이블 모뎀 뒤에 Cisco 라우터를 구성하는 방법을 참조하십시오.

ASDM 6.1(5)을 사용하는 ASA 컨피그레이션

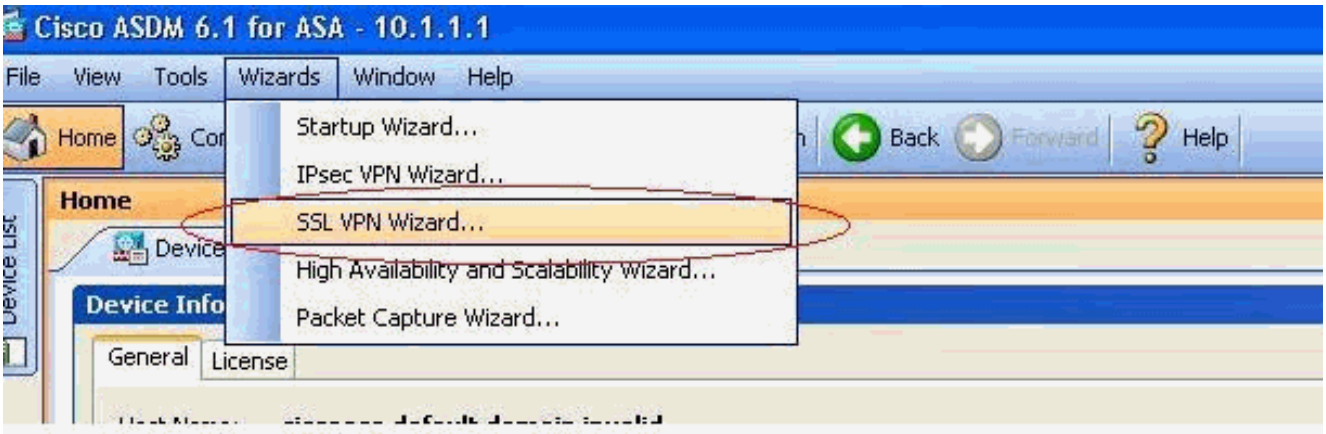
이 문서에서는 인터페이스 컨피그레이션과 같은 기본 컨피그레이션이 완료되었으며 제대로 작동한다고 가정합니다.

참고: ASDM에서 ASA를 구성하는 방법에 대한 자세한 내용은 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.

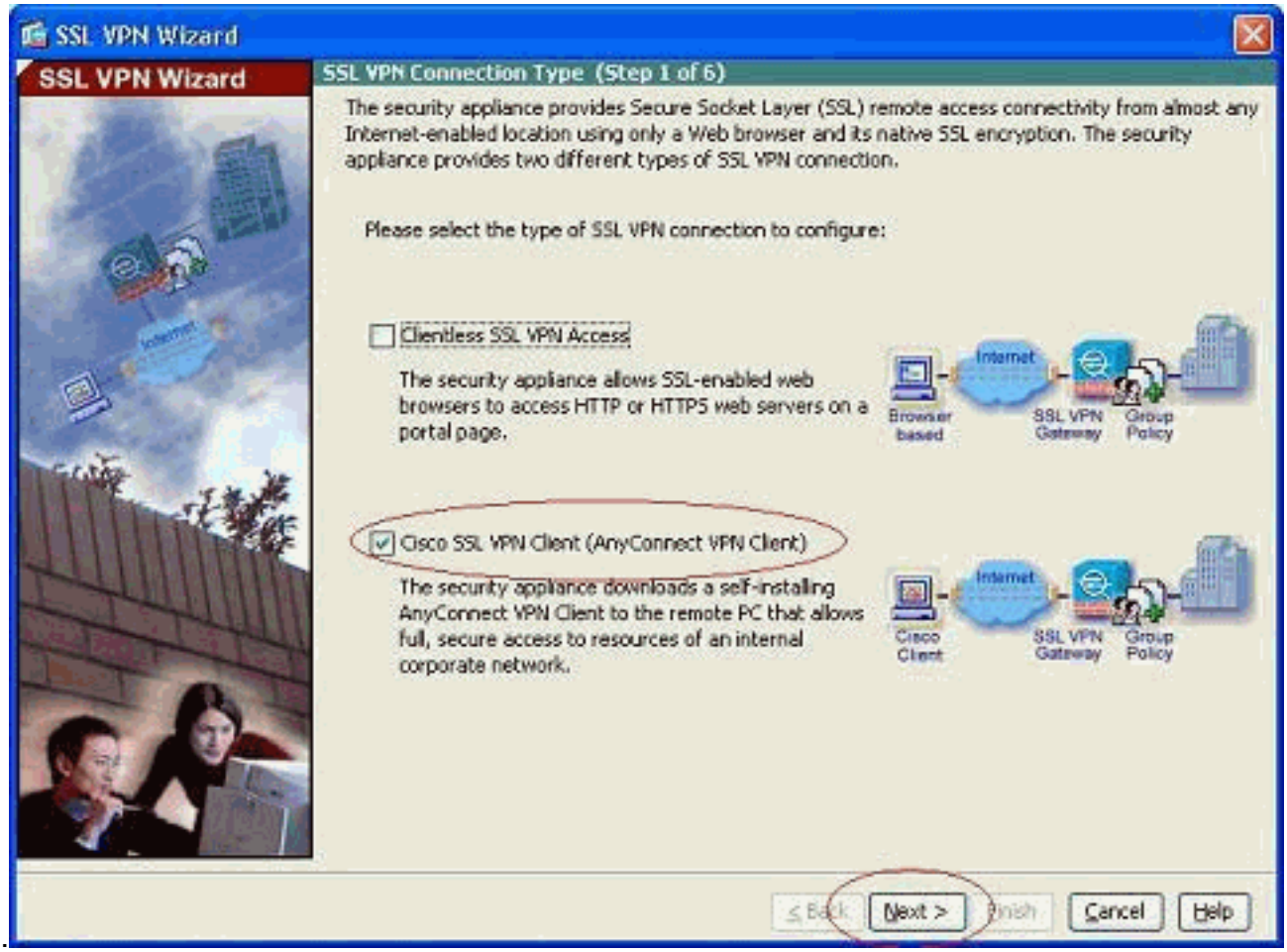
참고: 포트 번호를 변경하지 않으면 동일한 ASA 인터페이스에서 WebVPN 및 ASDM을 활성화할 수 없습니다. 자세한 내용은 ASA의 동일한 인터페이스에서 ASDM 및 WebVPN 활성화를 참조하십시오.

SSL VPN 마법사를 사용하여 SSL VPN을 구성하려면 다음 단계를 완료합니다.

1. Wizards(마법사) 메뉴에서 **SSL VPN Wizard(SSL VPN 마법사)**를 선택합니다



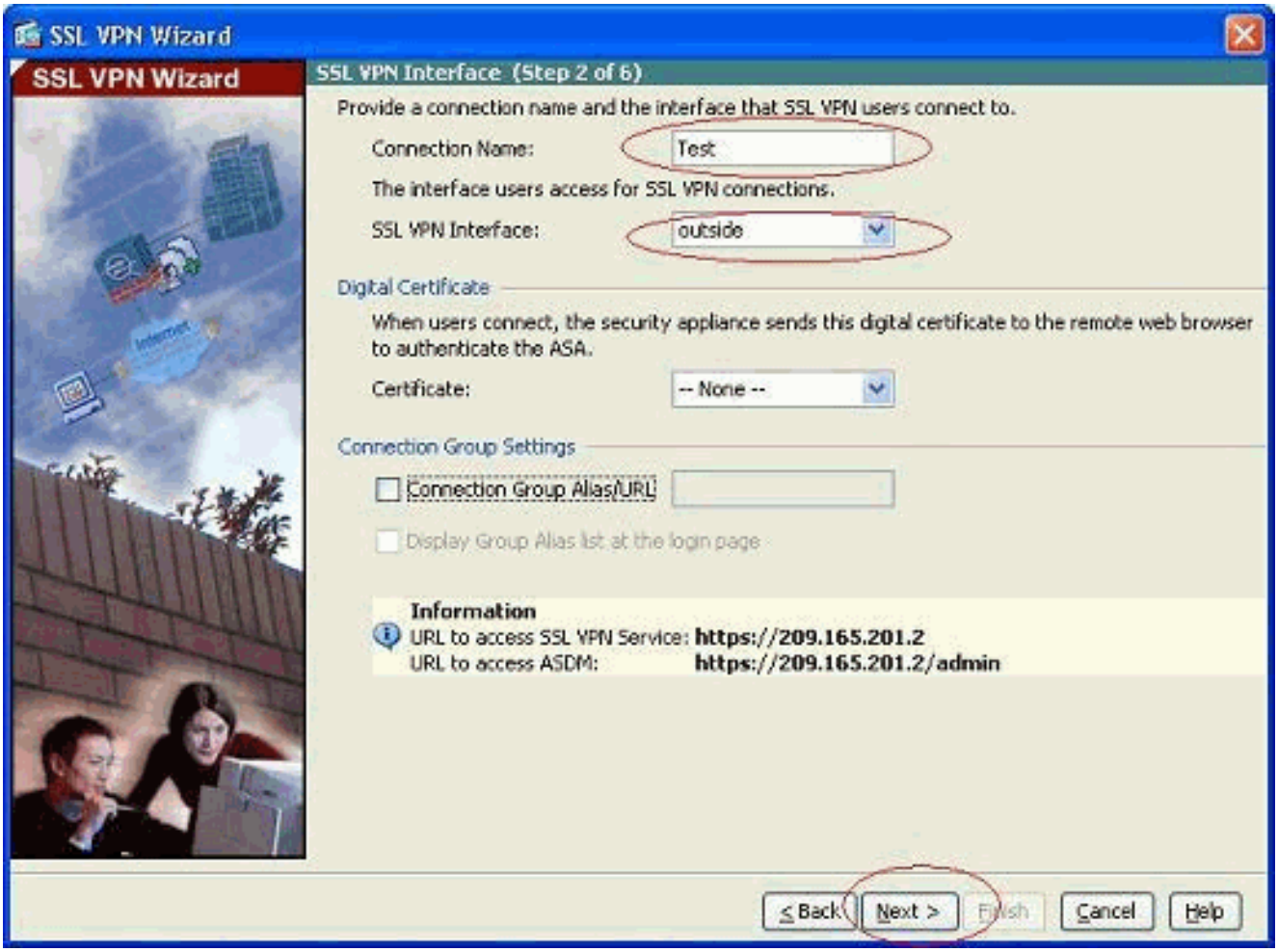
2. **Cisco SSL VPN Client(Cisco SSL VPN 클라이언트)** 확인란을 클릭하고 **Next(다음)**를 클릭합니다



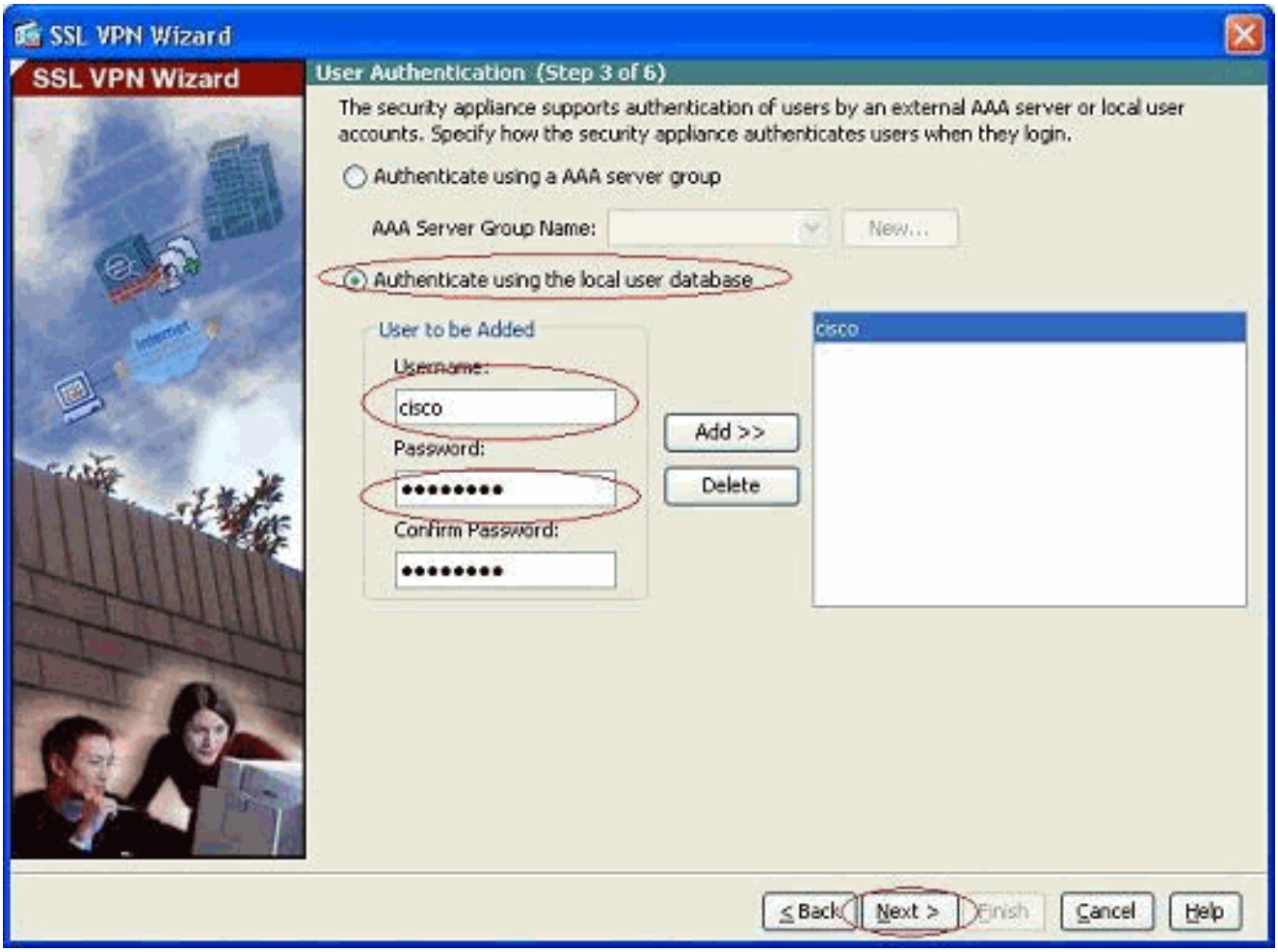
.

3. Connection Name(연결 이름) 필드에 연결 이름을 입력한 다음 SSL VPN Interface(SSL VPN 인터페이스) 드롭다운 목록에서 사용자가 SSL VPN에 액세스하는 데 사용할 인터페이스를 선택합니다

.

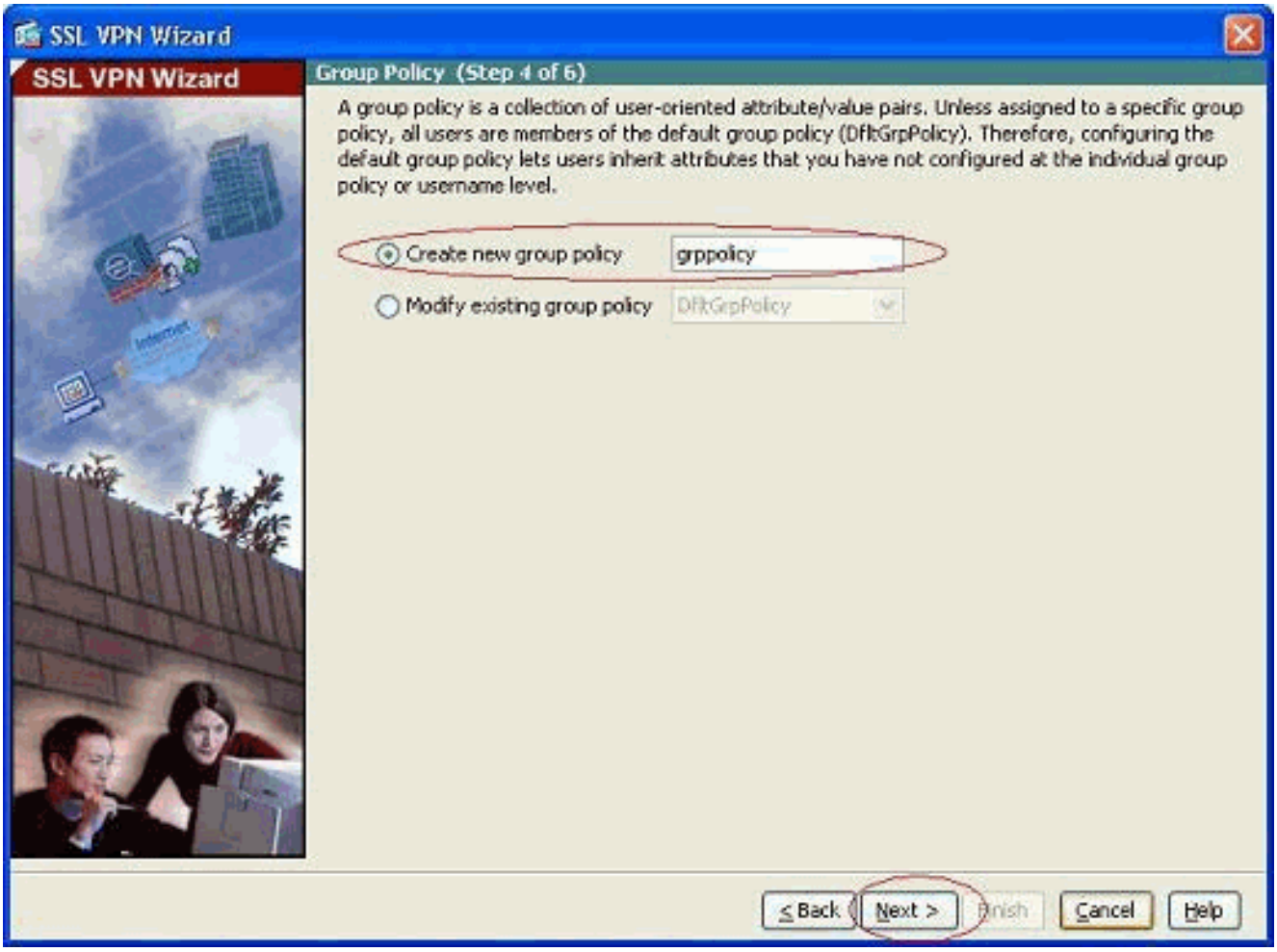


4. Next(**다음**)**를 클릭합니다**.
5. 인증 모드를 선택하고 Next(**다음**)를 클릭합니다. (이 예에서는 로컬 인증을 사용합니다 .)



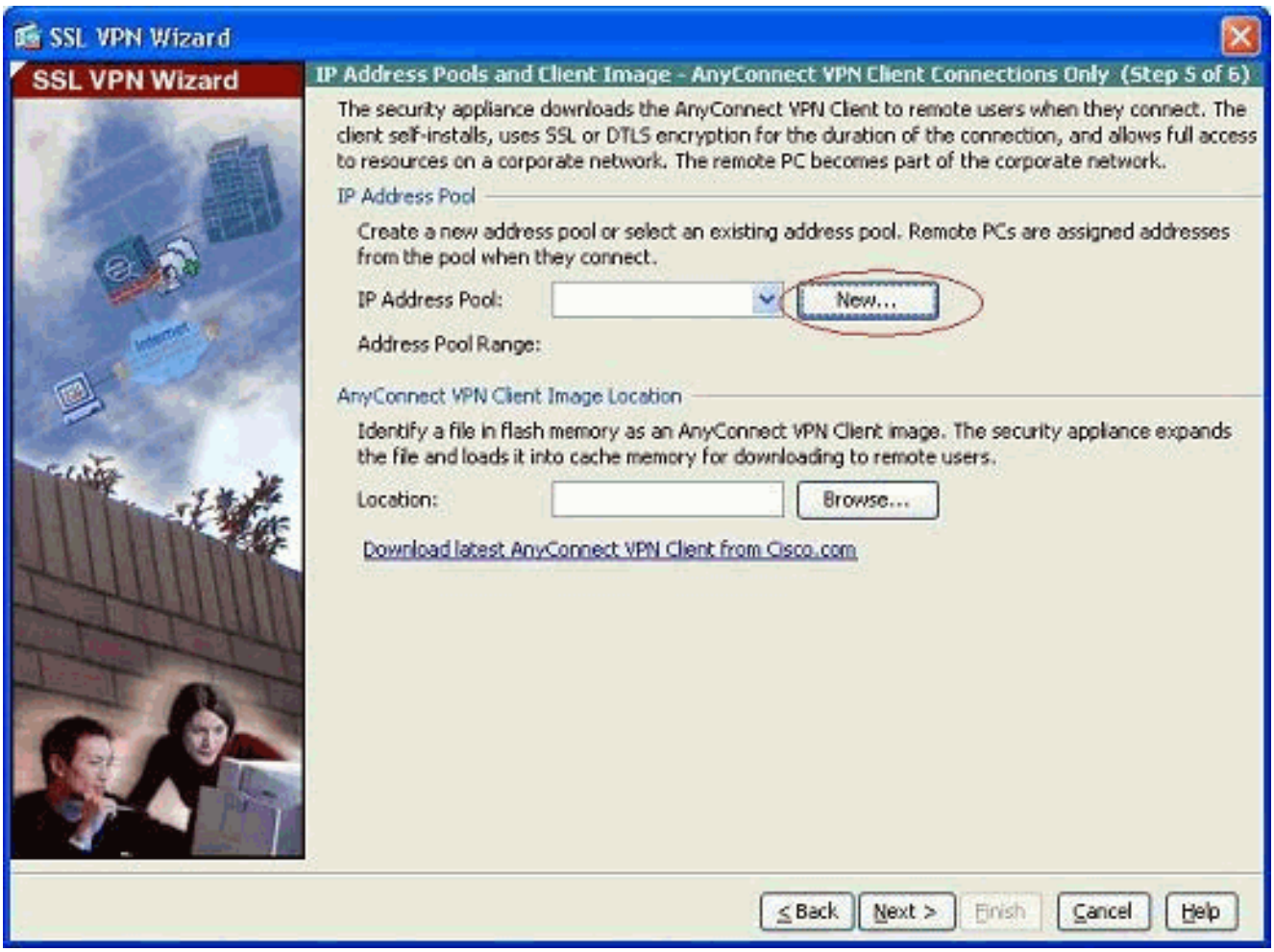
6. 기존 기본 그룹 정책 이외의 새 그룹 정책을 생성합니다

.

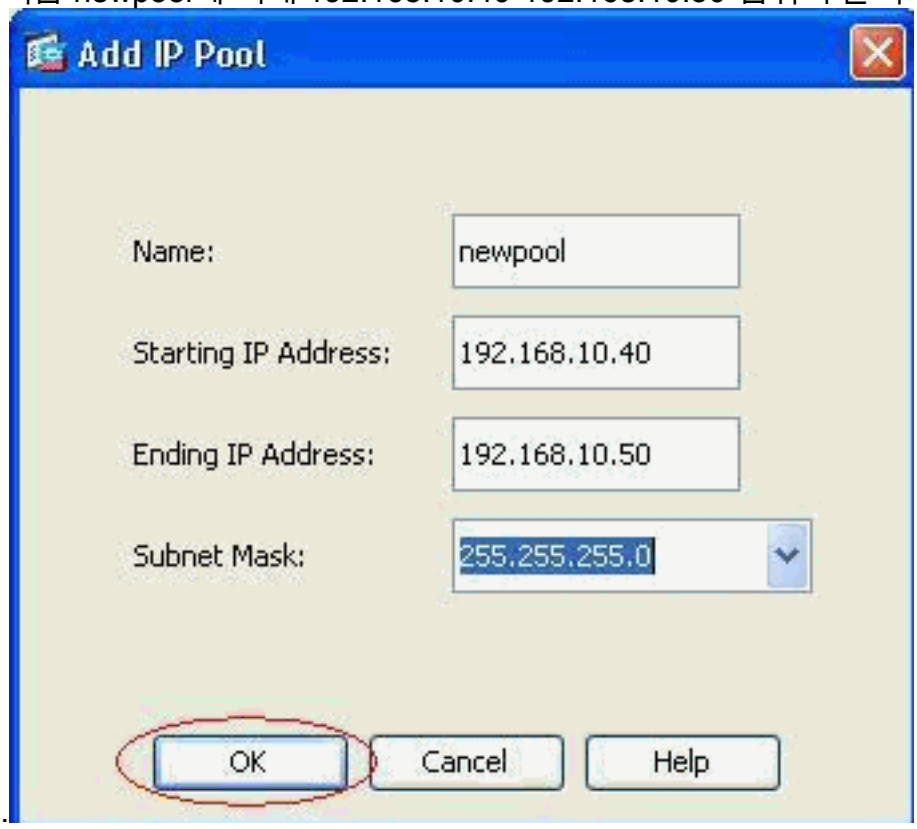


7. SSL VPN 클라이언트 PC가 연결되면 SSL VPN 클라이언트 PC에 할당할 새 주소 풀을 생성합니다

.



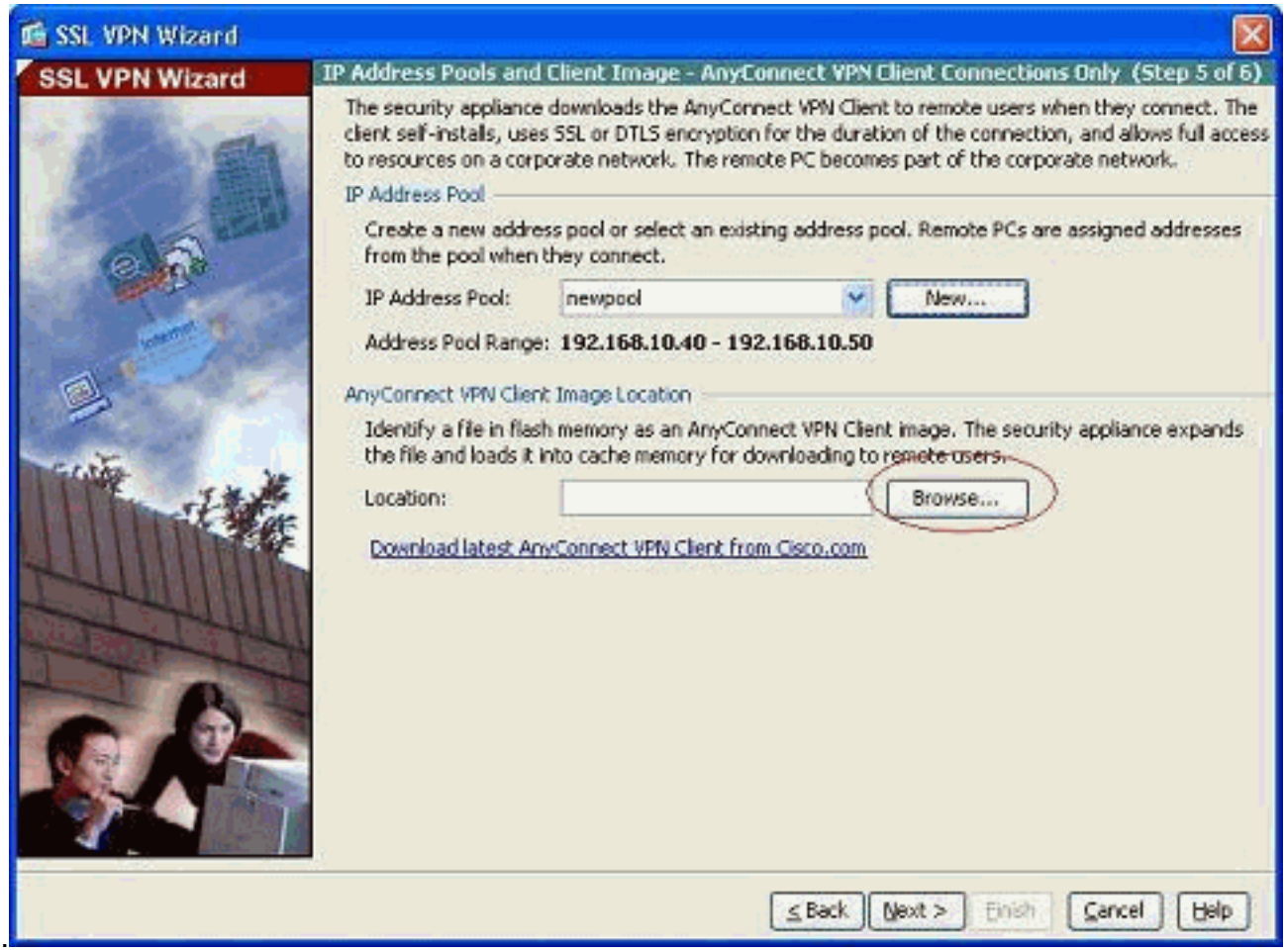
이름 newpool에 의해 192.168.10.40-192.168.10.50 범위의 풀이 *생성되었습니다*



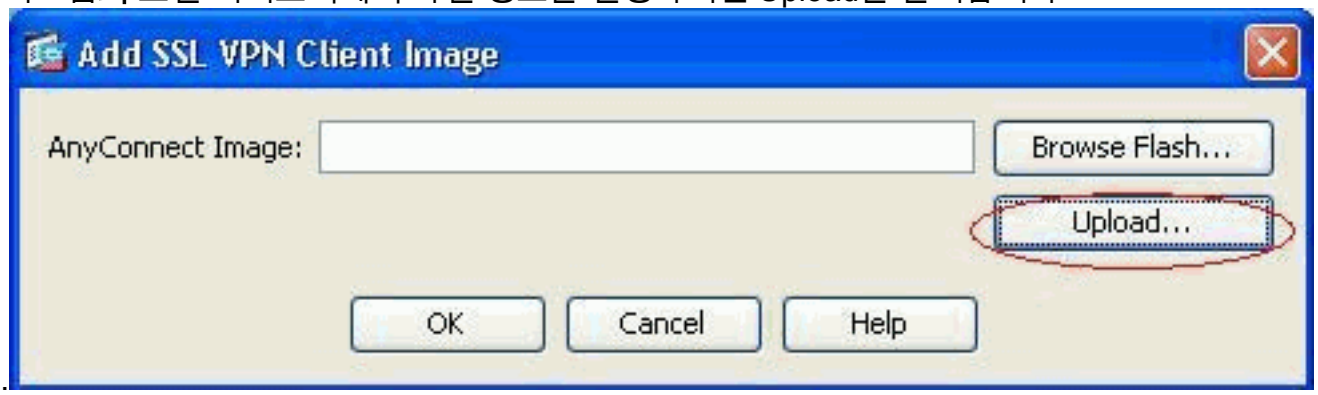
.

8. SSL VPN 클라이언트 이미지를 선택하고 ASA의 플래시 메모리에 업로드하려면 **Browse**를 클

릭합니다

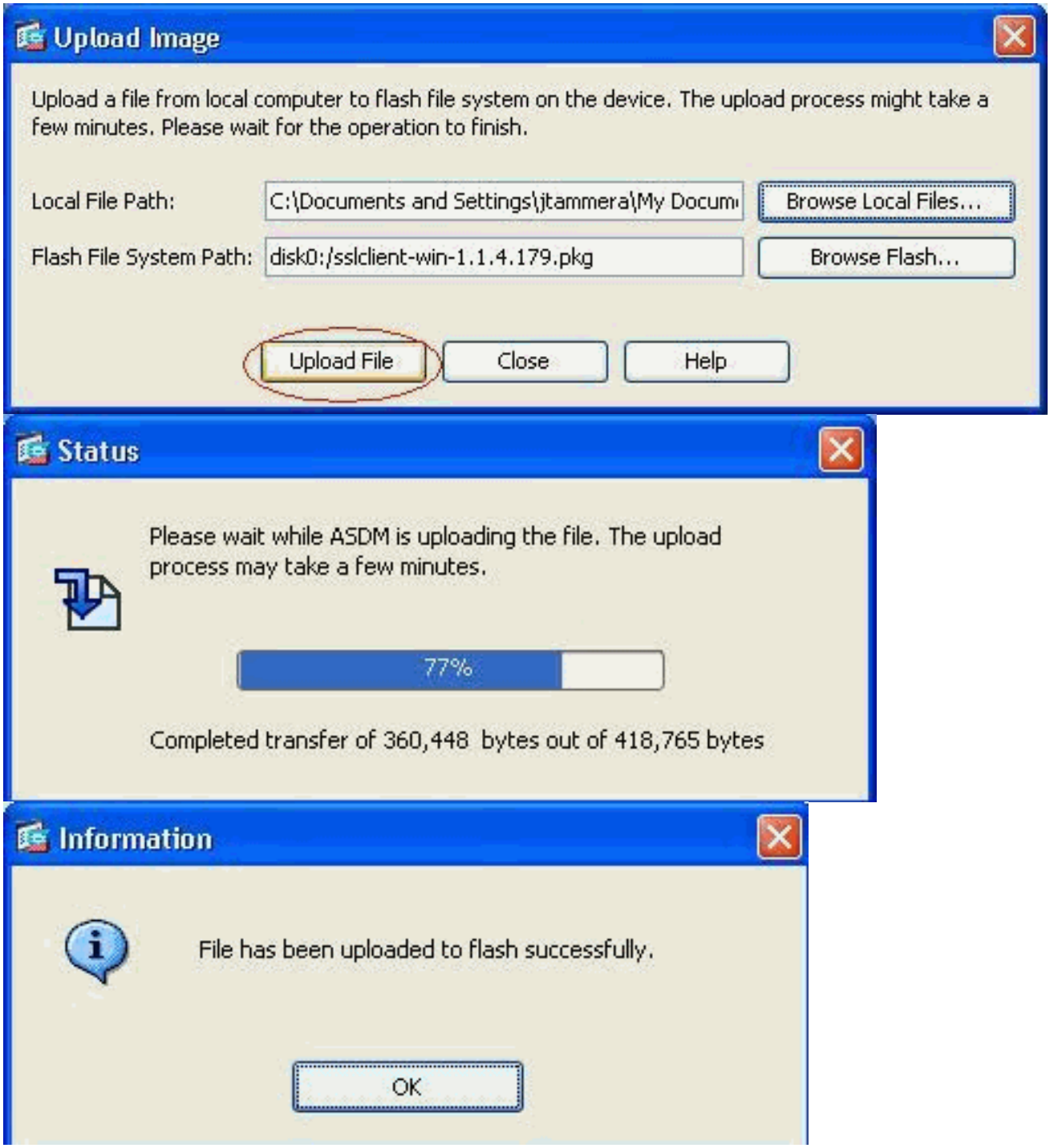


9. 시스템의 로컬 디렉토리에서 파일 경로를 설정하려면 Upload를 클릭합니다

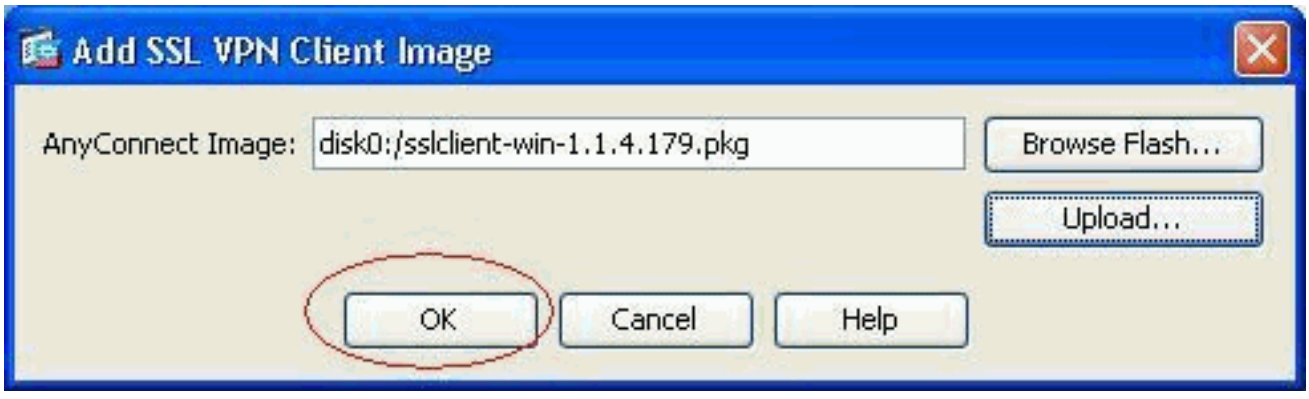


10. sslclient.pkg 파일이 있는 디렉토리를 선택하려면 Browse Local Files를 클릭합니다

11. 선택한 파일을 ASA 플래시에 업로드하려면 **Upload File**을 클릭합니다

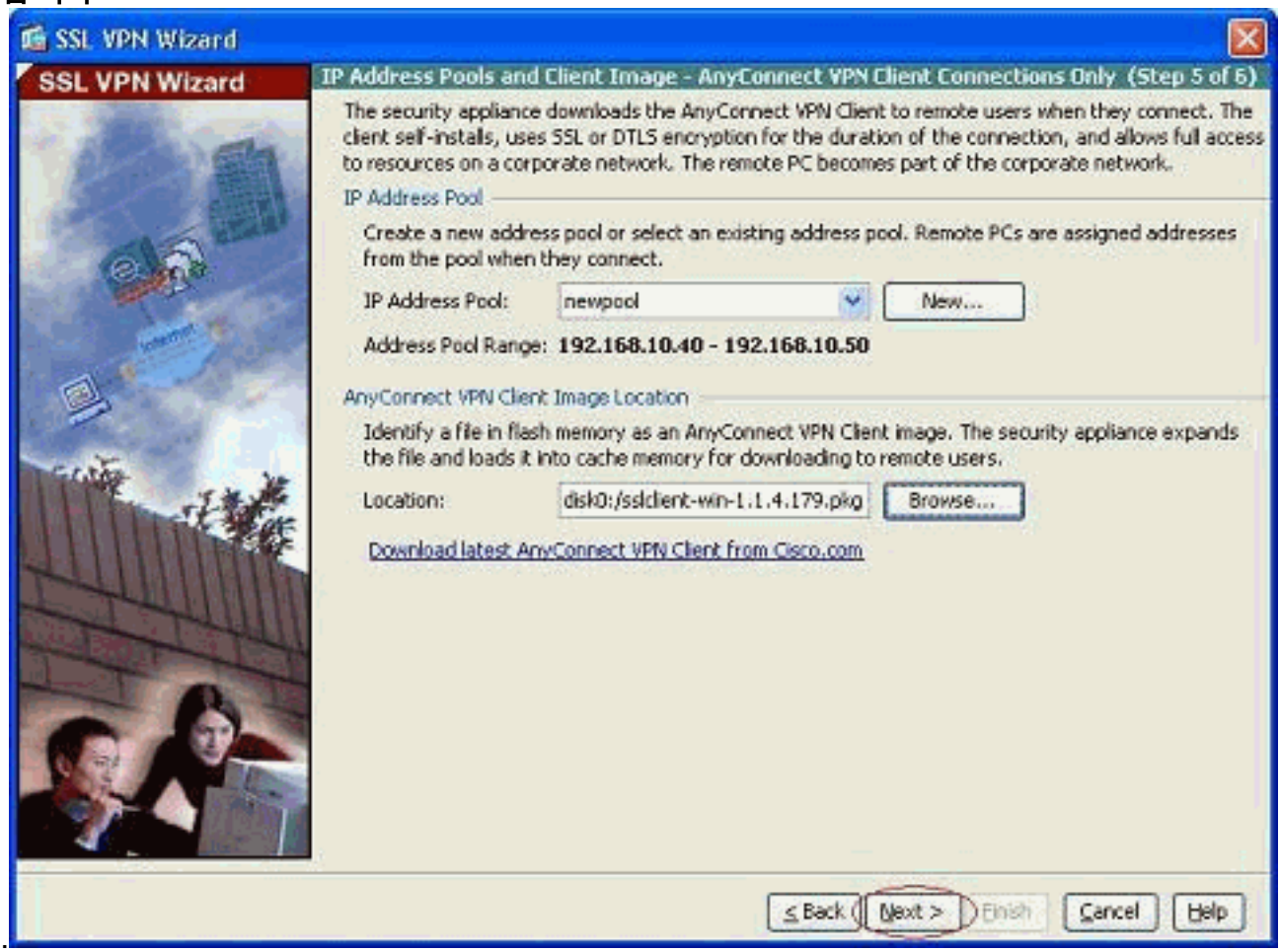


12. 파일이 ASA의 플래시에 업로드되면 **OK**를 클릭하여 해당 작업을 완료합니다



13. 이제 ASA의 플래시에 업로드된 최신 anyconnect pkg 파일이 표시됩니다. Next(**다음)를 클릭**

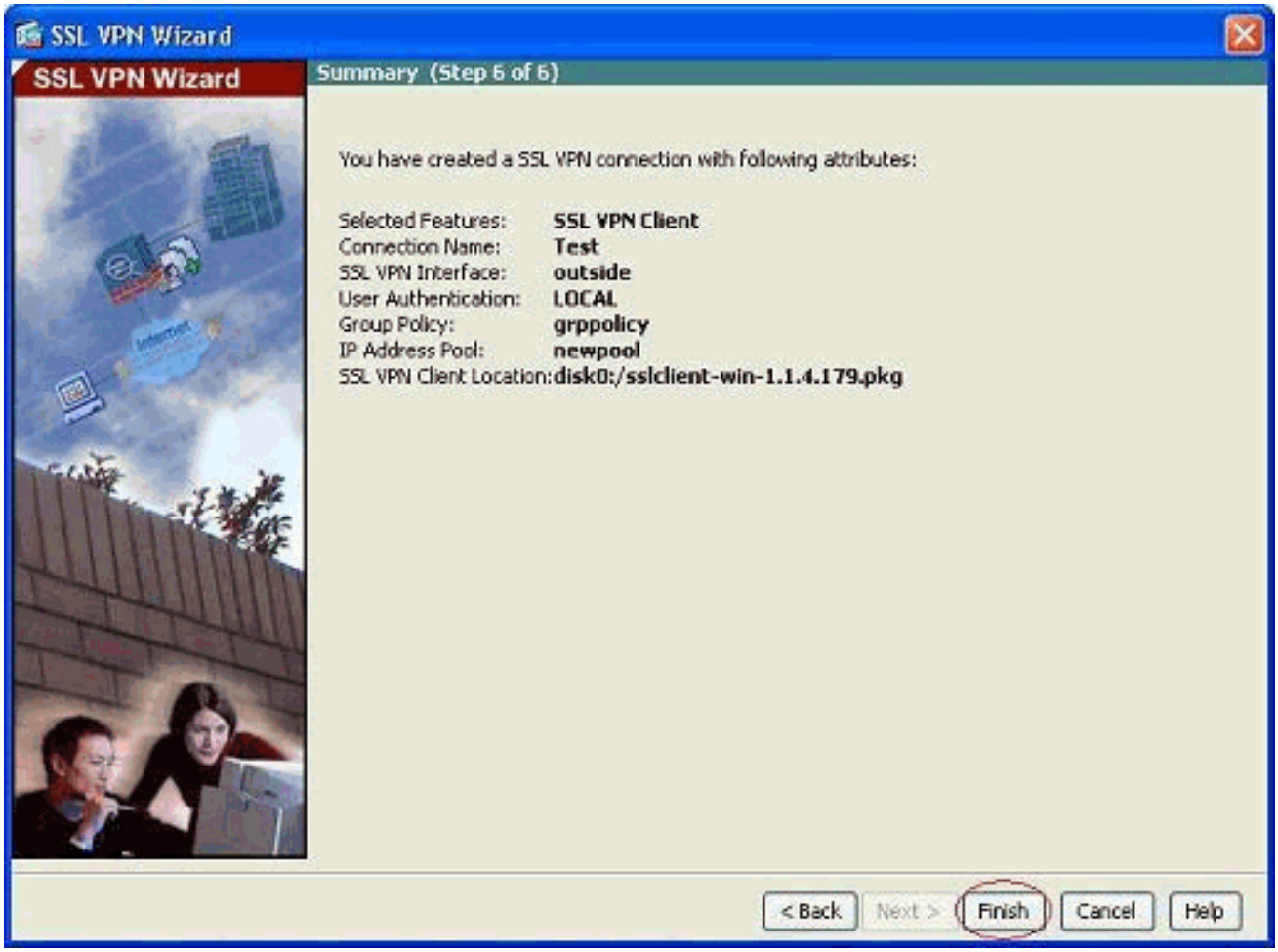
합니다



.

14. SSL VPN 클라이언트 컨피그레이션의 요약이 표시됩니다. **마침**을 클릭하여 마법사를 완료합니다

.



ASDM에 표시된 컨피그레이션은 주로 SSL VPN 클라이언트 마법사 컨피그레이션과 관련이 있습니다.

CLI에서 몇 가지 추가 컨피그레이션을 관찰할 수 있습니다. 전체 CLI 컨피그레이션이 아래에 표시되고 중요한 명령이 강조 표시됩니다.

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#
```

다음을 확인합니다.

이 섹션에 제공된 명령을 사용하여 이 컨피그레이션을 확인할 수 있습니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show webvpn svc** - ASA 플래시 메모리에 저장된 SVC 이미지를 표시합니다.
- **show VPN-sessiondb svc** - 현재 SSL 연결에 대한 정보를 표시합니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco 5500 Series Adaptive Security Appliance 지원
- 스틱 컨피그레이션의 공용 인터넷 VPN용 PIX/ASA 및 VPN 클라이언트 예
- ASA의 SVC(SSL VPN Client) with ASDM 컨피그레이션 예
- 기술 지원 및 문서 – Cisco Systems