SDM 컨피그레이션이 포함된 IOS의 SSL VPN 클라이언트(SVC) 예

목차

소개

SVC(SSL VPN Client)는 기업 내부 네트워크와의 보안 통신을 위한 전체 터널을 제공합니다.사용자별로 액세스를 구성하거나, 한 명 이상의 사용자를 배치할 다른 WebVPN 컨텍스트를 생성할 수 있습니다.

SSL VPN 또는 WebVPN 기술은 다음 IOS 라우터 플랫폼에서 지원됩니다.

- 870, 1811, 1841, 2801, 2811, 2821, 2851
- 3725, 3745, 3825, 3845, 7200 및 7301

다음 모드에서 SSL VPN 기술을 구성할 수 있습니다.

- **Clientless SSL VPN(WebVPN)** - SSL 지원 웹 브라우저가 기업 LAN(Local-Area Network)의 HTTP 또는 HTTPS 웹 서버에 액세스해야 하는 원격 클라이언트를 제공합니다. 또한 클라이언트리스 SSL VPN은 CIFS(Common Internet File System) 프로토콜을 통해 Windows 파일 브라

우징에 대한 액세스를 제공합니다.OWA(Outlook Web Access)는 HTTP 액세스의 예입니다.클라이언트리스 SSL VPN에 대한 자세한 내용은 Cisco IOS with SDM Configuration 예에서 클라이언트리스 SSL VPN(WebVPN)을 참조하십시오.

- **Thin-Client SSL VPN(Port Forwarding)** - 작은 Java 기반 애플릿을 다운로드하고 고정 포트 번호를 사용하는 TCP(Transmission Control Protocol) 애플리케이션에 대한 보안 액세스를 허용하는 원격 클라이언트를 제공합니다.POP3(Point of Presence), SMTP(Simple Mail Transfer Protocol), IMAP(Internet Message Access Protocol), SSH(Secure Shell) 및 텔넷은 보안 액세스의 예입니다.로컬 시스템의 파일이 변경되므로 이 방법을 사용하려면 사용자에게 로컬 관리 권한이 있어야 합니다.이 SSL VPN 방법은 일부 FTP(File Transfer Protocol) 애플리케이션과 같은 동적 포트 할당을 사용하는 애플리케이션에서 작동하지 않습니다.씬 클라이언트 SSL VPN에 대한 자세한 내용은 SDM과 함께 씬 클라이언트 SSL VPN(WebVPN) IOS 구성 예를 참조하십시오.**참고:** UDP(User Datagram Protocol)는 지원되지 않습니다.
- **SSL VPN Client(SVC Full Tunnel Mode)**—소규모 클라이언트를 원격 워크스테이션에 다운로드하고 내부 기업 네트워크의 리소스에 대한 완전한 보안 액세스를 허용합니다.원격 워크스테이션에 SVC를 영구적으로 다운로드하거나 보안 세션이 닫히면 클라이언트를 제거할 수 있습니다.

이 문서에서는 SSL VPN 클라이언트에서 사용할 Cisco IOS 라우터의 컨피그레이션을 보여 줍니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- Microsoft Windows 2000 또는 XP
- SUN JRE 1.4 이상 또는 ActiveX 제어 브라우저가 있는 웹 브라우저
- 클라이언트에 대한 로컬 관리 권한
- Introduction(소개)에 Advanced Security 이미지(12.4(6)T 이상)가 포함된 라우터 중 하나
- Cisco SDM(Security Device Manager) 버전 2.3Cisco SDM이 라우터에 아직 로드되지 않은 경우 소프트웨어 다운로드(등록된 고객만 해당)에서 소프트웨어의 무료 사본을 얻을 수 있습니다. 서비스 계약이 있는 CCO 계정이 있어야 합니다.SDM의 설치 및 구성에 대한 자세한 내용은 Cisco 라우터 및 보안 장치 관리자를 참조하십시오.
- 라우터의 디지털 인증서영구 자체 서명 인증서 또는 외부 CA(Certificate Authority)를 사용하여 이 요구 사항을 충족할 수 있습니다.영구 자체 서명 인증서에 대한 자세한 내용은 영구 자체 서명 인증서를 참조하십시오.

사용되는 구성 요소

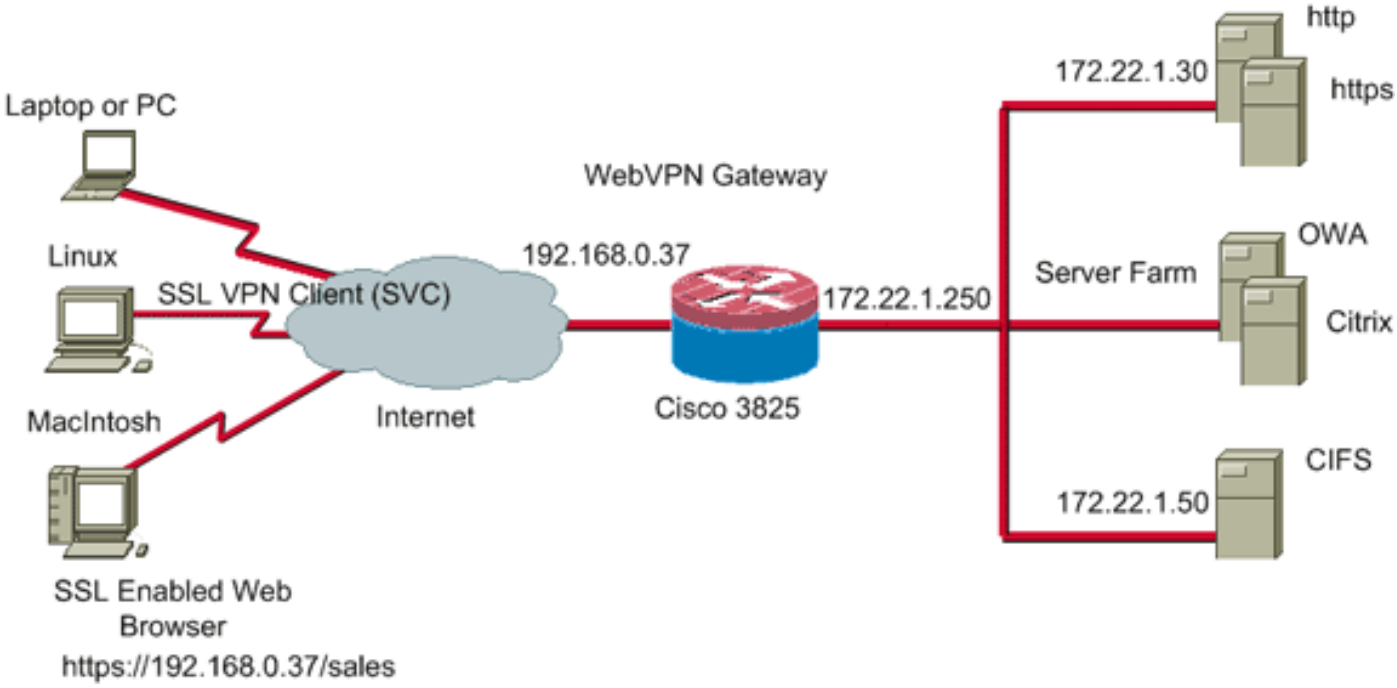
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS 라우터 3825 series with 12.4(9)T
- SDM(Security Device Manager) 버전 2.3.1

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

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



사전 구성 작업

1. SDM용 라우터를 구성합니다(선택 사항).적절한 보안 번들 라이센스가 있는 라우터에는 SDM 애플리케이션이 플래시에 로드되어 있습니다.소프트웨어를 가져오고 구성하려면 Cisco 라우터 및 SDM(Security Device Manager) 다운로드 및 설치를 참조하십시오.
2. 관리 PC에 SVC 사본을 다운로드합니다.소프트웨어 다운로드에서 SVC 패키지 파일의 복사본을 가져올 수 있습니다.Cisco SSL VPN Client(등록된 고객만 해당). 서비스 계약이 있는 유효한 CCO 계정이 있어야 합니다.
3. 올바른 날짜, 시간 및 시간대를 설정한 다음 라우터에서 디지털 인증서를 구성합니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

처음에는 SVC가 WebVPN 게이트웨이 라우터에 로드됩니다.클라이언트가 연결될 때마다 SVC의 복사본이 PC에 동적으로 다운로드됩니다.이 동작을 변경하려면 소프트웨어가 클라이언트 컴퓨터에 영구적으로 유지되도록 라우터를 구성합니다.

IOS에서 SVC 구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 데 필요한 단계를 제공합니다.이 예제 컨피그레이션에서는 SDM 마법사를 사용하여 IOS 라우터에서 SVC의 작업을 활성화합니다.

IOS 라우터에서 SVC를 구성하려면 다음 단계를 완료하십시오.

1. IOS 라우터에서 SVC 소프트웨어 설치 및 활성화

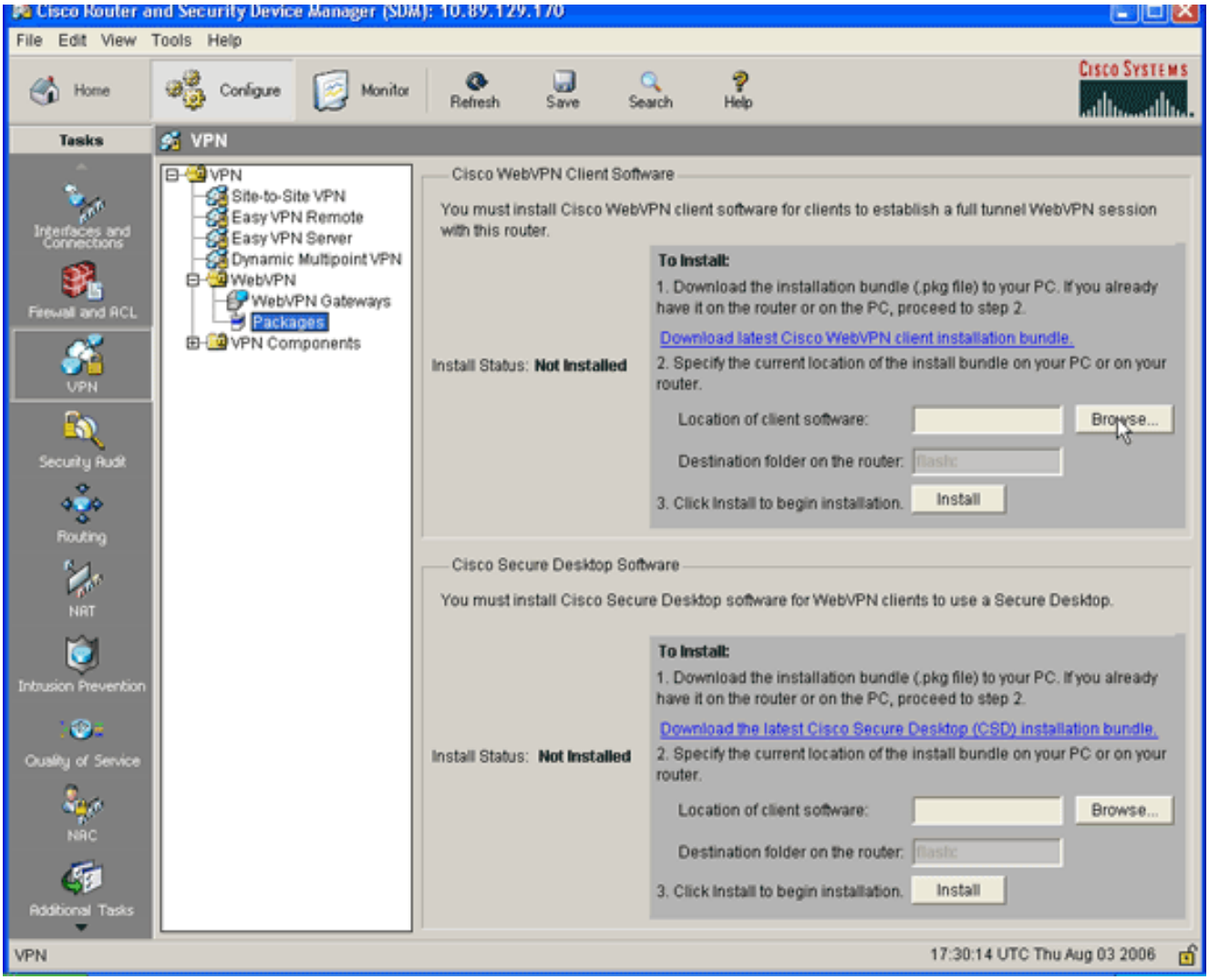
2. SDM 마법사를 사용하여 WebVPN 컨텍스트 및 WebVPN 게이트웨이 구성
3. SVC 사용자를 위한 사용자 데이터베이스 구성
4. 사용자에게 노출되도록 리소스 구성

1단계. IOS 라우터에 SVC 소프트웨어를 설치 및 활성화합니다.

IOS 라우터에 SVC 소프트웨어를 설치하고 활성화하려면 다음 단계를 완료하십시오.

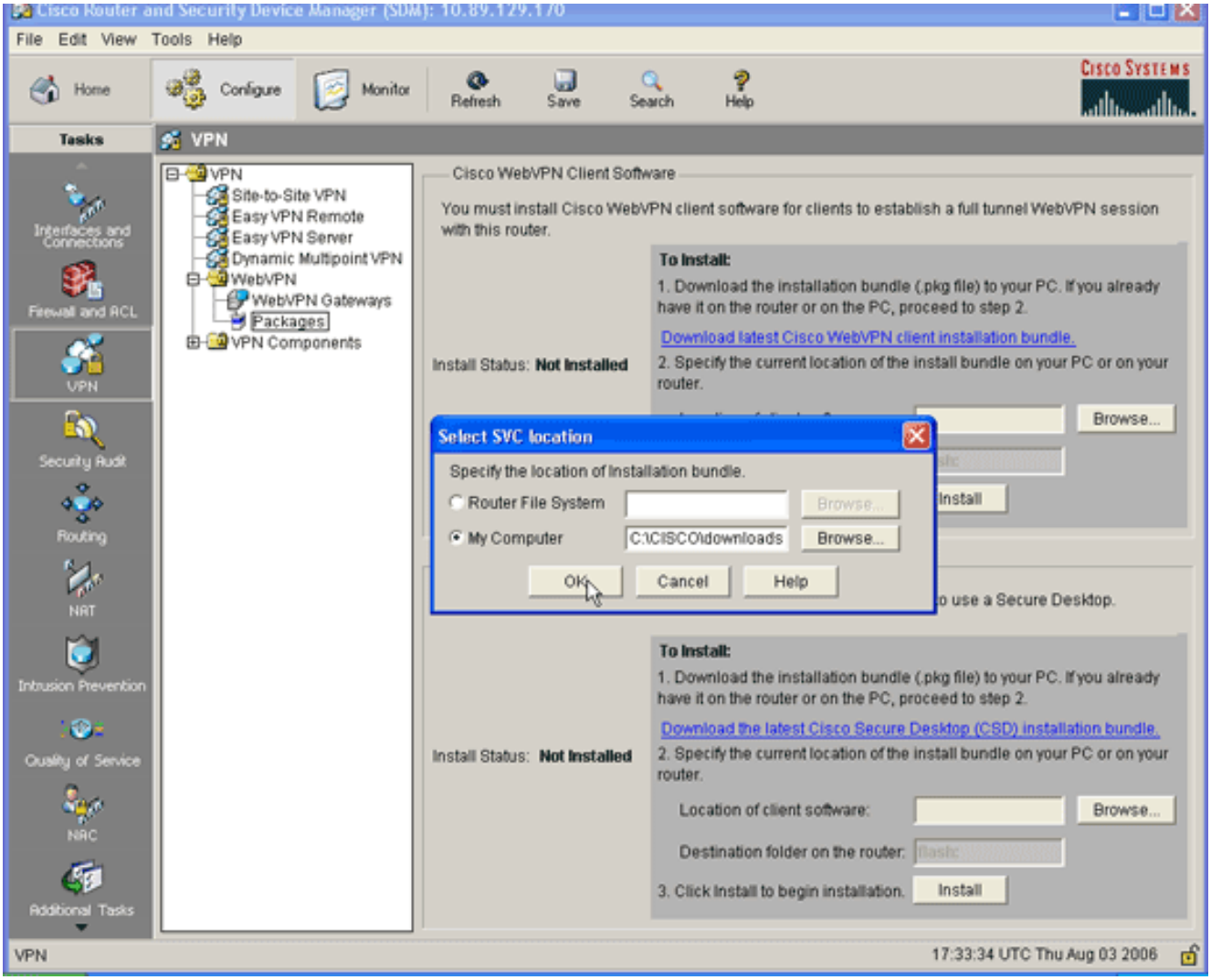
1. SDM 애플리케이션을 열고 **Configure**(구성)를 클릭한 다음 **VPN**을 클릭합니다.
2. WebVPN**을** 확장하고 Packages(패키지)를 **선택합니다**

.



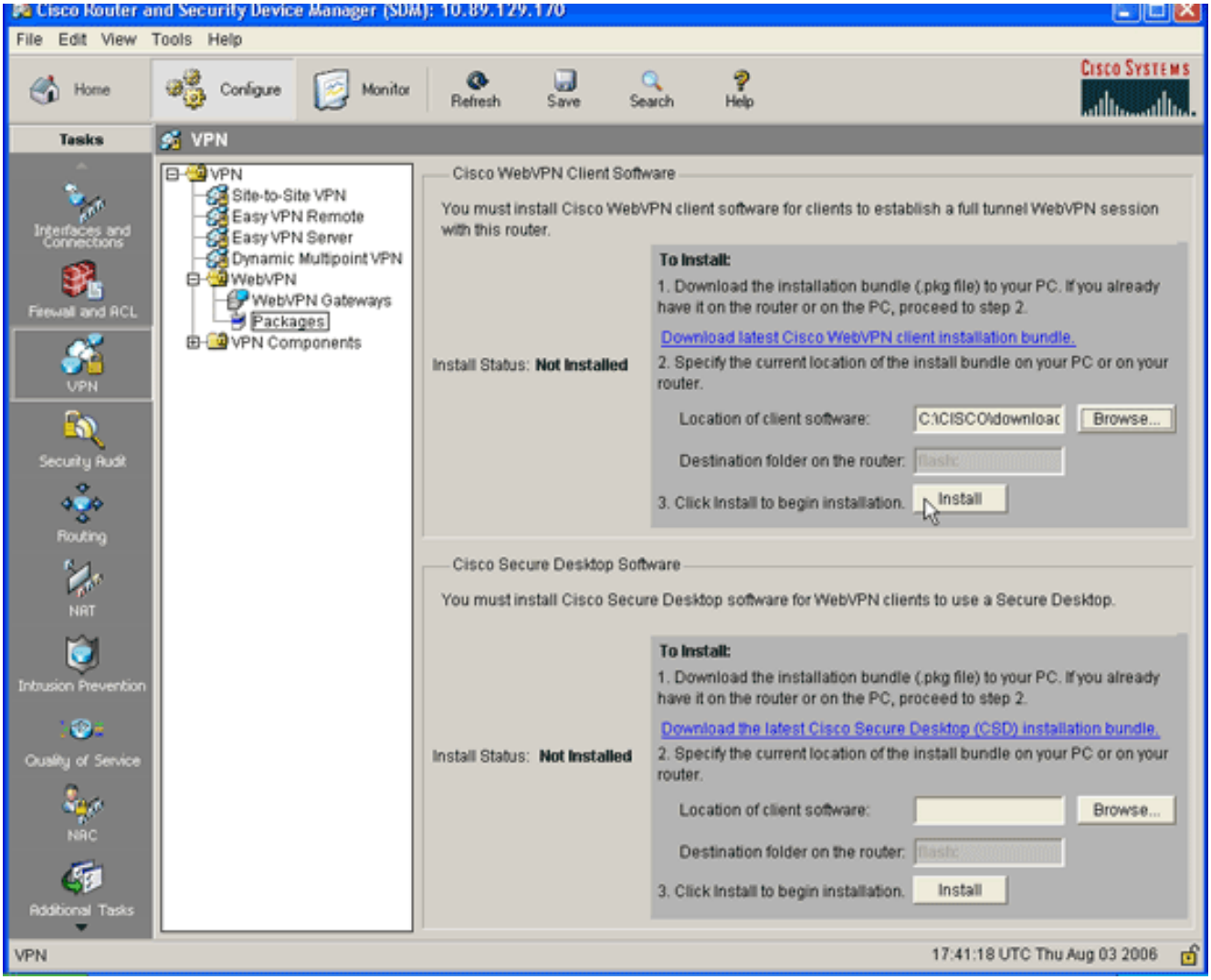
3. Cisco WebVPN Client Software(Cisco WebVPN 클라이언트 소프트웨어) 영역에서 Browse(찾아보기) 버튼을 클릭합니다.SVC 위치 선택 대화 상자가 나타납니다

.



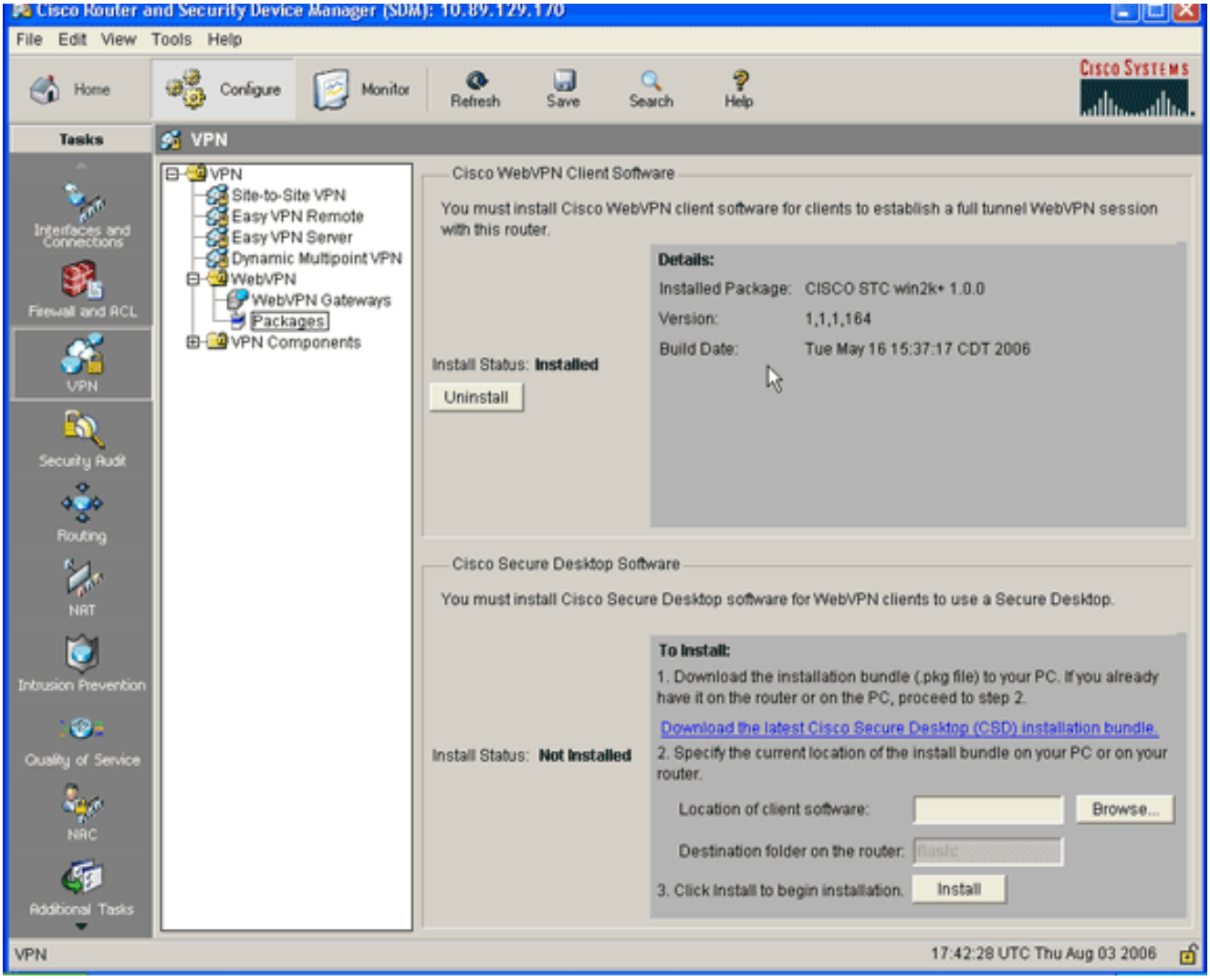
4. **내 컴퓨터** 라디오 버튼을 클릭한 다음 **찾아보기**를 클릭하여 관리 PC에서 SVC 패키지를 찾습니다.
5. **확인**을 클릭한 다음 **설치** 버튼을 클릭합니다

.



6. **예**를 클릭한 다음 **확인**을 클릭합니다.SVC 패키지를 성공적으로 설치한 경우 다음 이미지가 표시됩니다

.

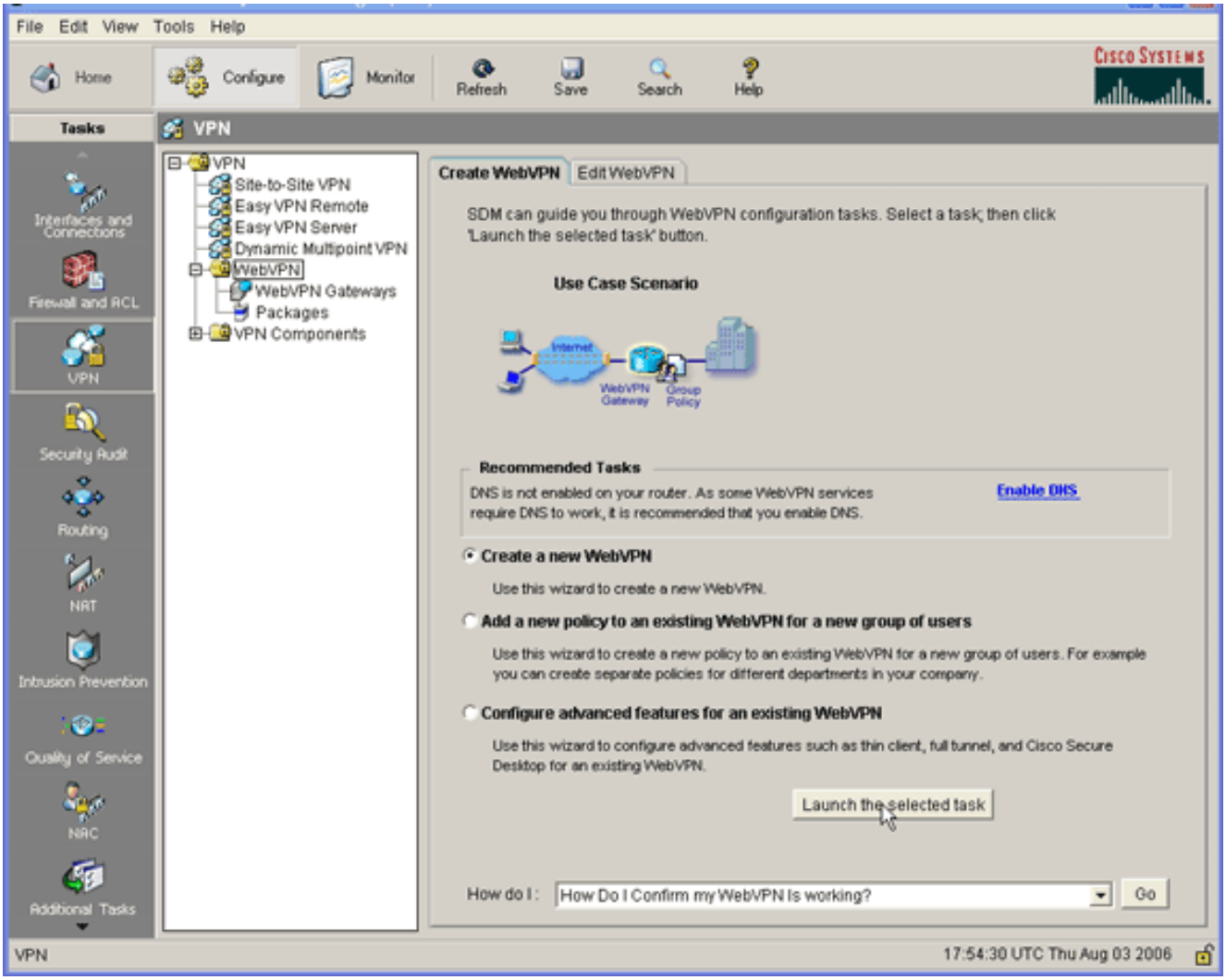


2단계. SDM 마법사를 사용하여 WebVPN 컨텍스트 및 WebVPN 게이트웨이 구성

WebVPN 컨텍스트 및 WebVPN 게이트웨이를 구성하려면 다음 단계를 완료합니다.

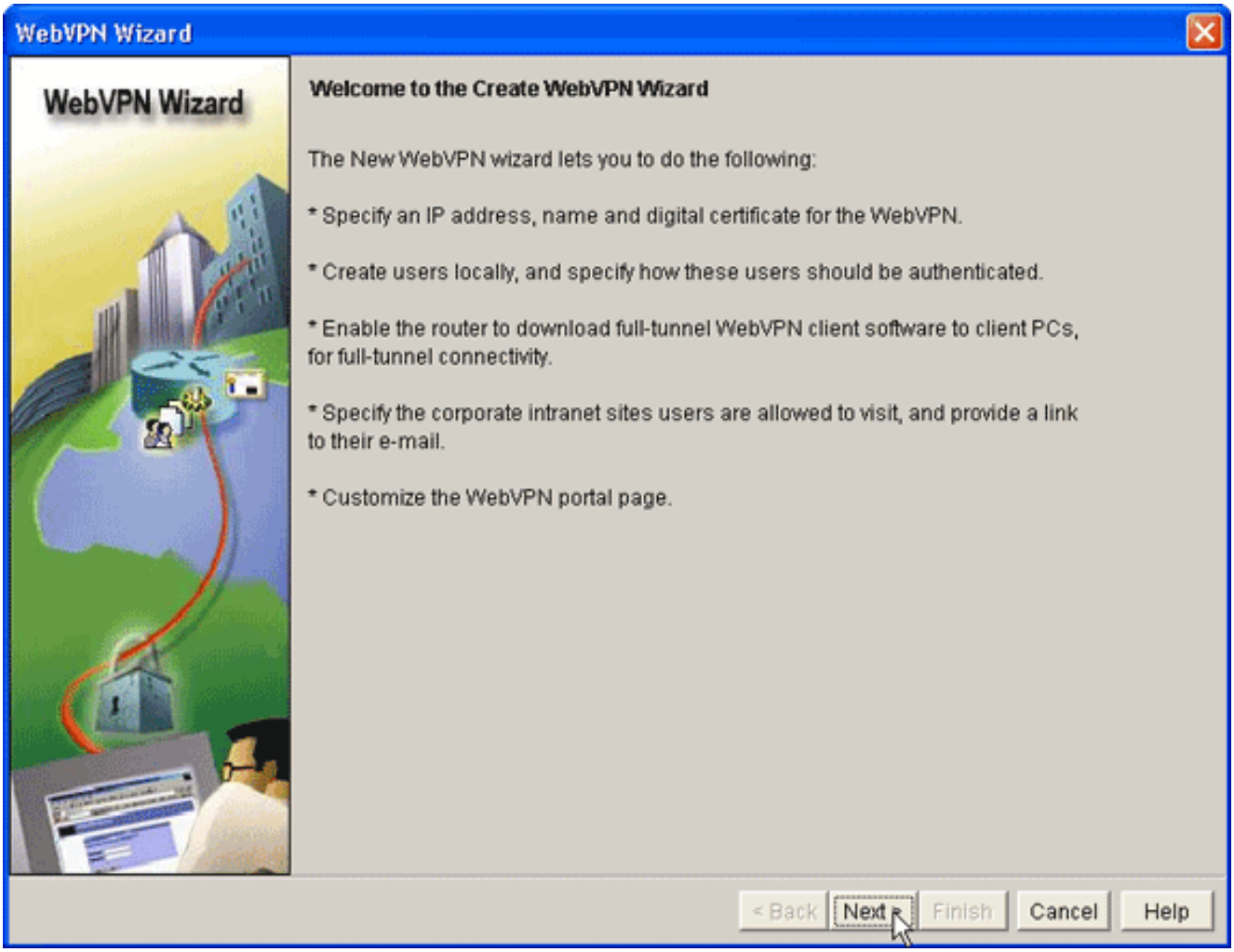
1. SVC가 라우터에 설치된 후 Configure(구성)를 **클릭한** 다음 **VPN**을 클릭합니다.
2. WebVPN**을** 클릭하고 Create **WebVPN** 탭**을** 클릭합니다

.



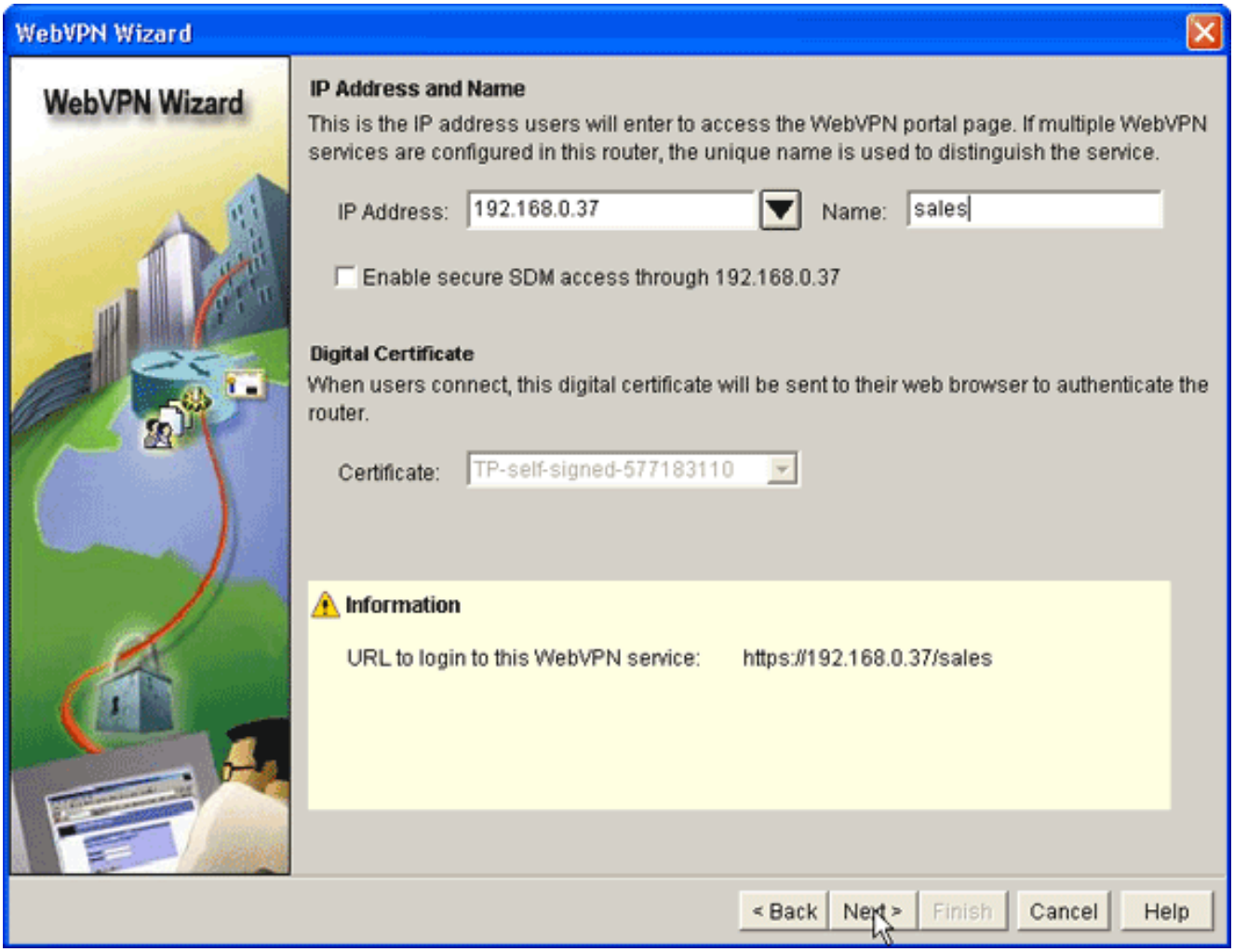
3. Create a **New WebVPN(새 WebVPN 생성)** 라디오 버튼을 선택한 다음 **Launch the selected task(선택한 작업 시작)를 클릭합니다**.WebVPN Wizard 대화 상자가 나타납니다

.



4. Next(다음)를 클릭합니다

.



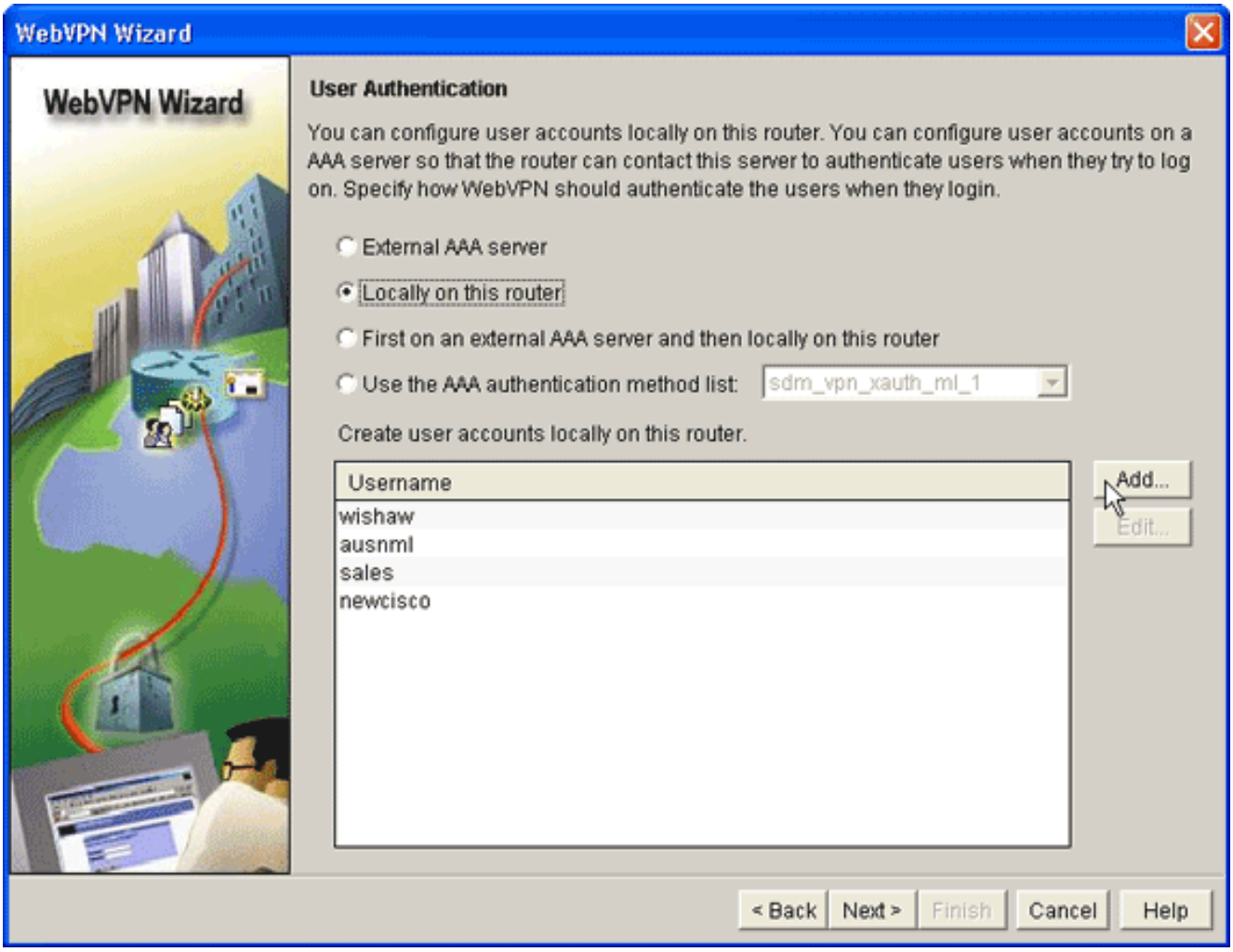
5. 새 WebVPN 게이트웨이의 IP 주소를 입력하고 이 WebVPN 컨텍스트의 고유한 이름을 입력합니다.동일한 IP 주소(WebVPN 게이트웨이)에 대해 서로 다른 WebVPN 컨텍스트를 만들 수 있지만 각 이름은 고유해야 합니다.이 예에서는 다음 IP 주소를 사용합니다 .https://192.168.0.37/sales
6. Next(**다음**)를 클릭하고 3단계로 이동합니다.

3단계. SVC 사용자를 위한 사용자 데이터베이스 구성

인증을 위해 AAA 서버, 로컬 사용자 또는 둘 모두를 사용할 수 있습니다.이 컨피그레이션 예에서는 로컬로 생성된 사용자를 인증에 사용합니다.

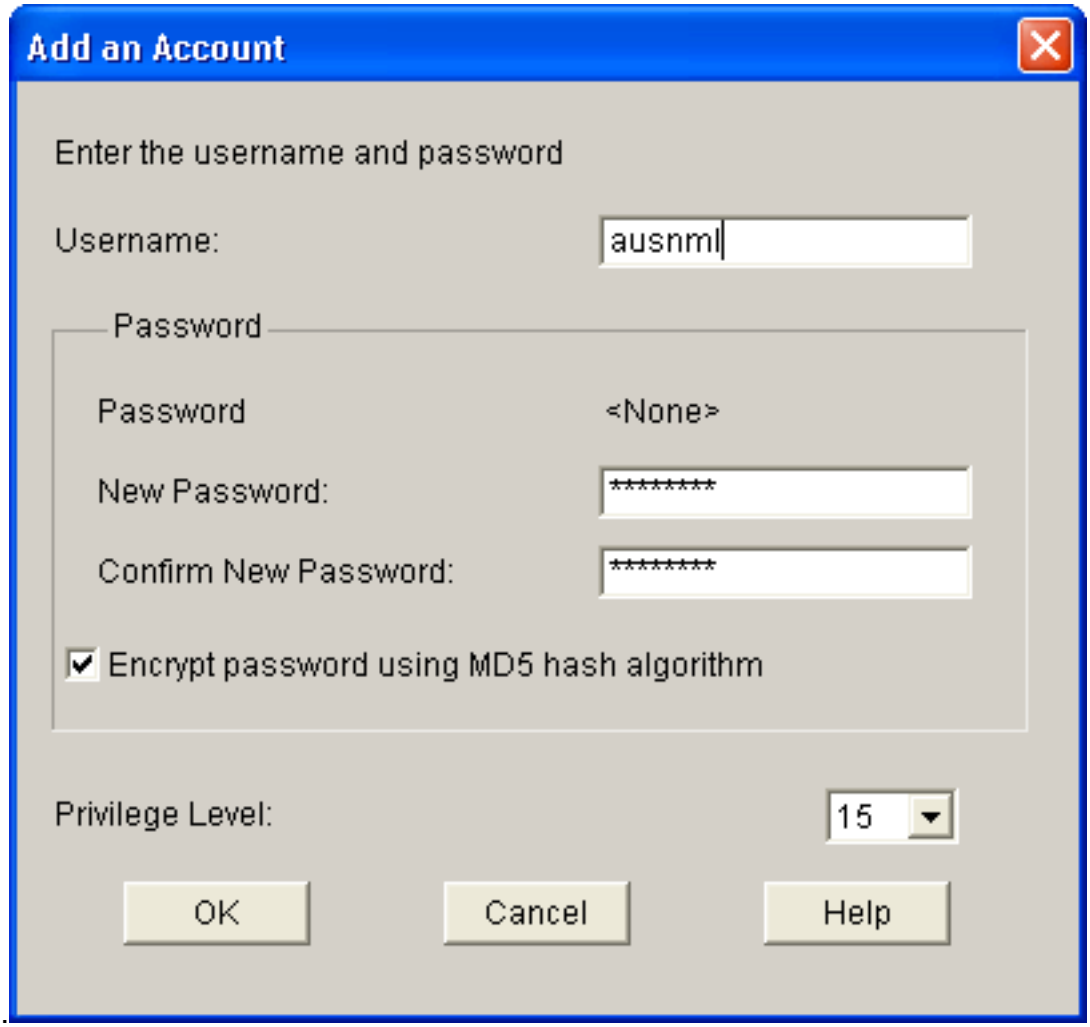
SVC 사용자를 위한 사용자 데이터베이스를 구성하려면 다음 단계를 완료하십시오.

1. 2단계를 완료한 후 WebVPN Wizard User Authentication(WebVPN 마법사 사용자 인증) 대화상자**에 있는 Locally on this router(이 라우터**에서 로컬로) 라디오 버튼을 클릭합니다 .



이 대화 상자에서는 로컬 데이터베이스에 사용자를 추가할 수 있습니다.

2. Add(**추가**)를 클릭하고 사용자 정보를 입력합니다



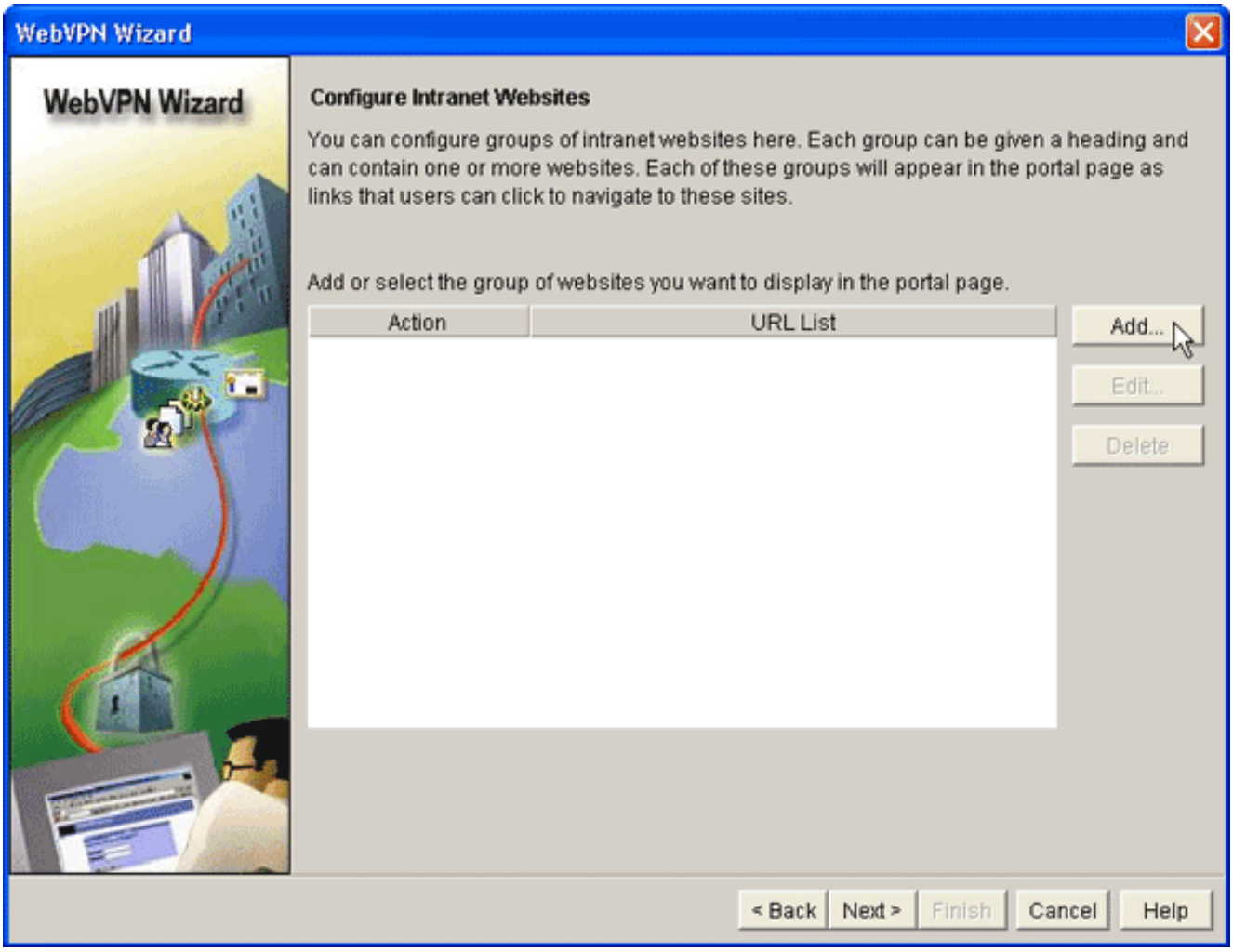
3. OK(**확인**)를 클릭하고 필요에 따라 사용자를 추가합니다.
4. 필요한 사용자를 추가한 후 **Next(다음)**를 클릭하고 4단계로 이동합니다.

4단계. 사용자에게 노출되도록 리소스를 구성합니다.

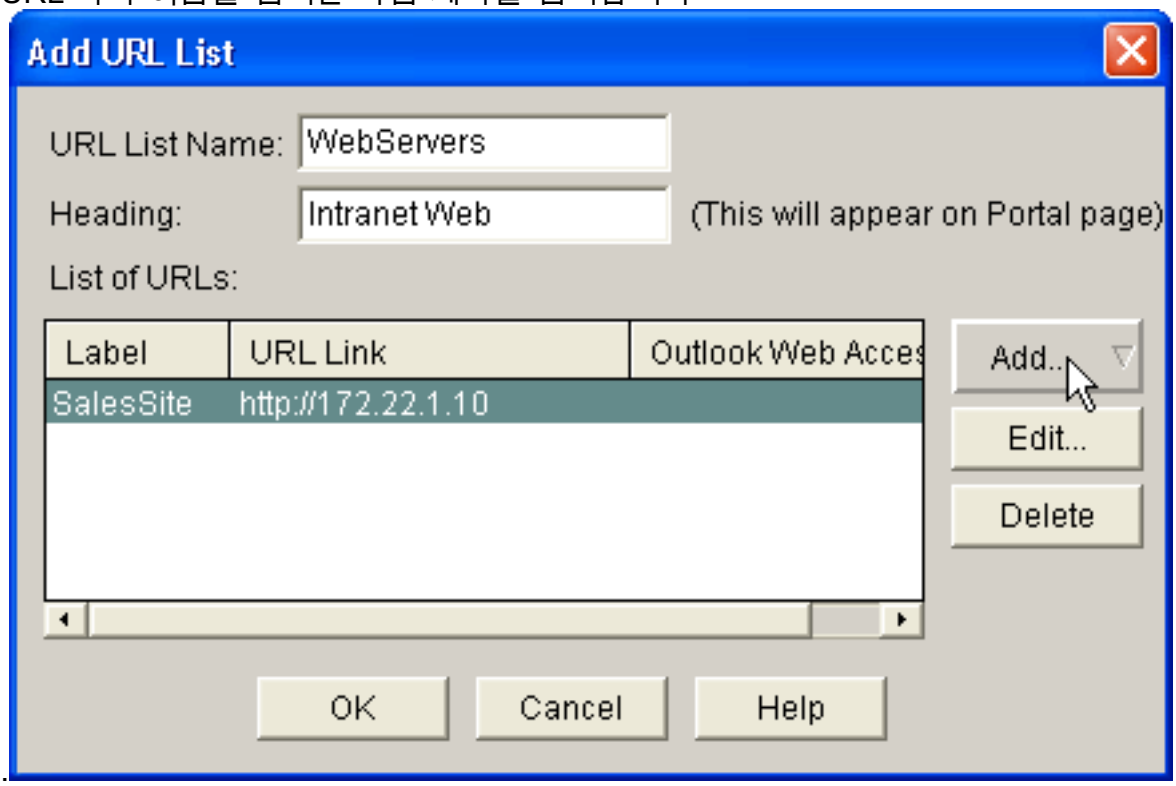
Configure Intranet Websites WebVPN Wizard(인트라넷 웹 사이트 구성 WebVPN 마법사) 대화 상자에서는 SVC 클라이언트에 노출할 인트라넷 리소스를 선택할 수 있습니다.

사용자에게 노출되도록 리소스를 구성하려면 다음 단계를 완료합니다.

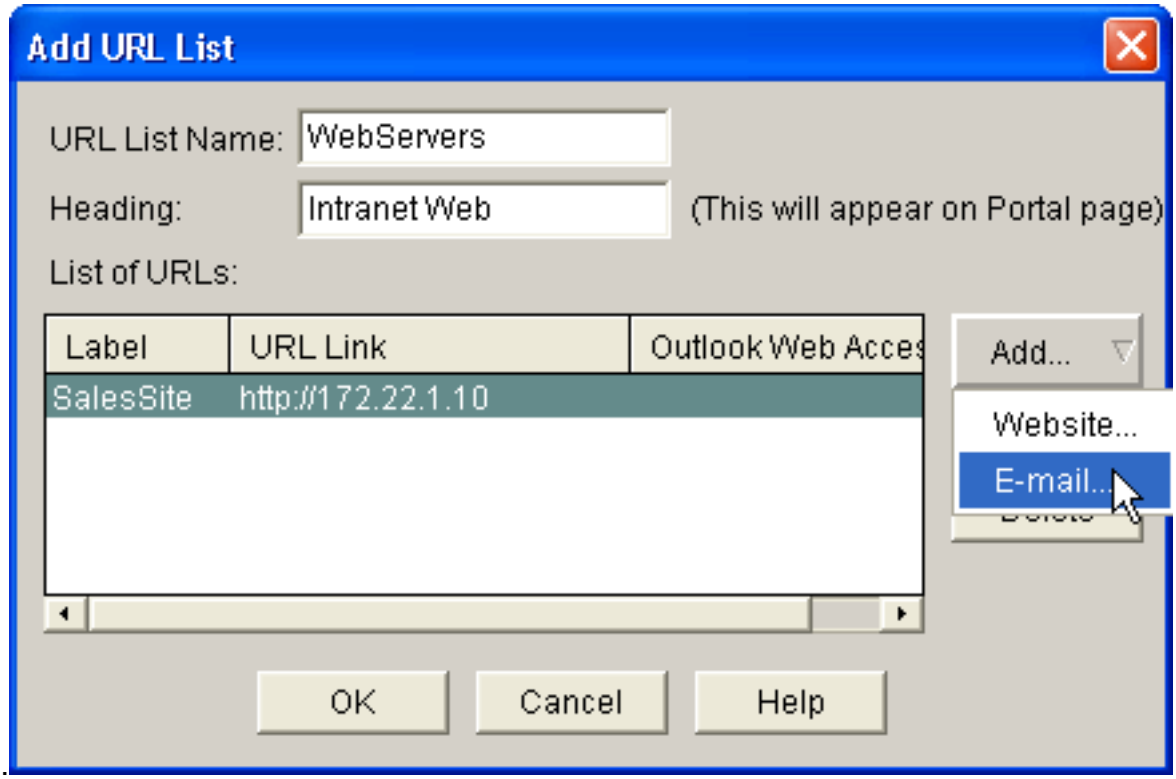
1. 3단계를 완료한 후 Configure Intranet Websites(인트라넷 웹 사이트 구성) 대화 상자에 있는 Add(**추가**) 버튼을 클릭합니다
.



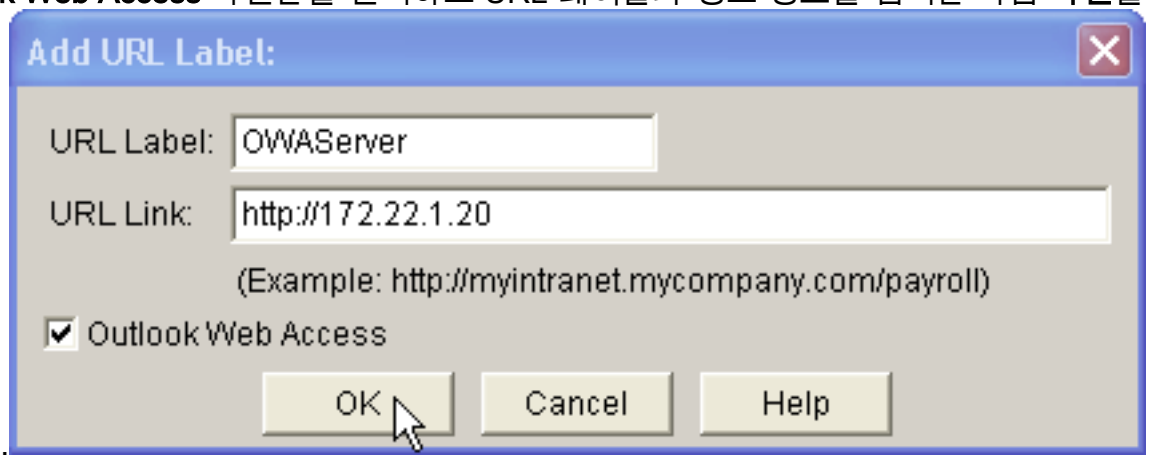
2. URL 목록 이름을 입력한 다음 제목을 입력합니다



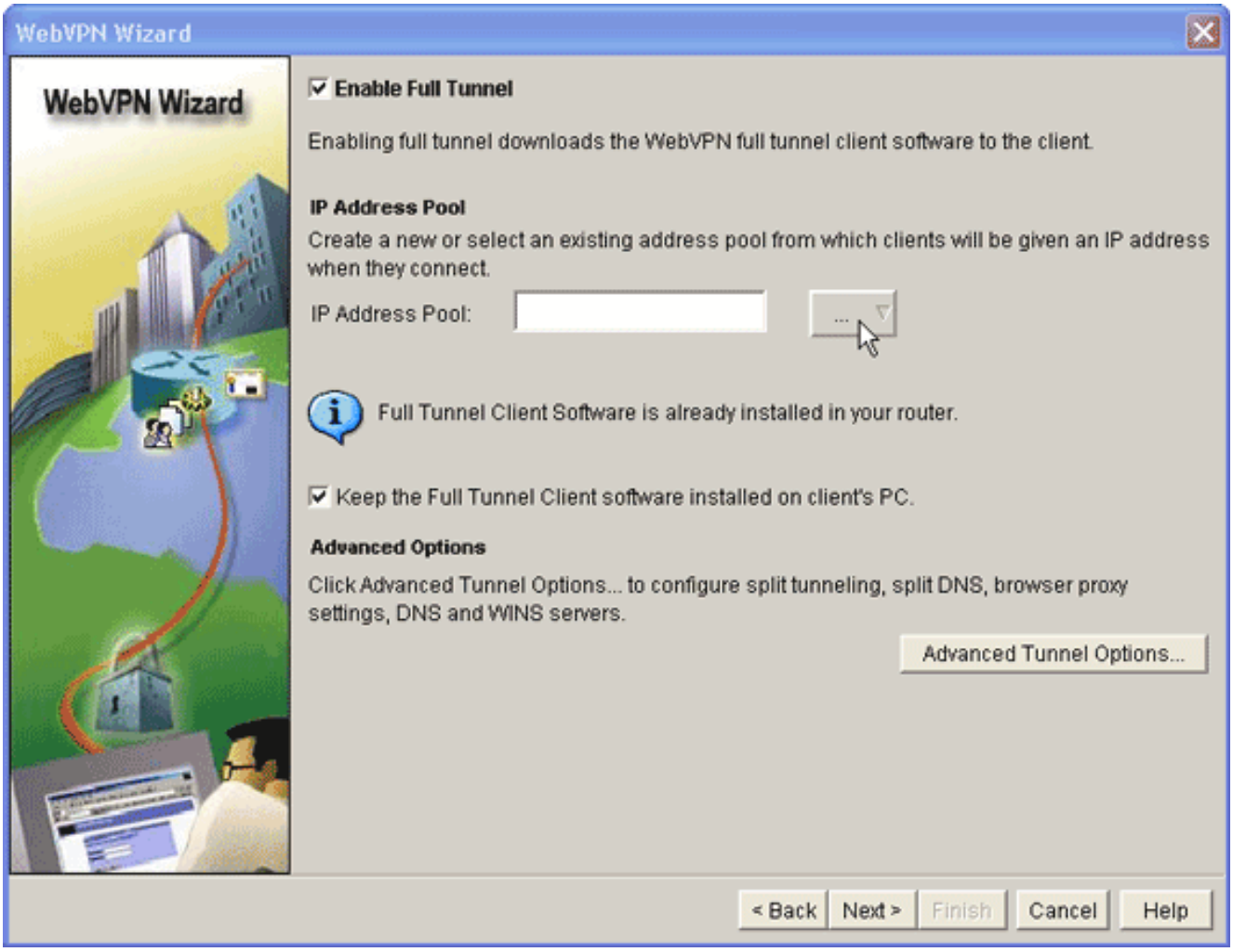
3. Add(**추가**)를 클릭하고 **Website(웹 사이트)**를 선택하여 이 클라이언트에 노출할 웹 사이트를 추가합니다.
4. URL 및 링크 정보를 입력한 다음 **OK**(확인)를 클릭합니다.
5. OWA Exchange Server에 대한 액세스를 추가하려면 **Add**(추가)를 클릭하고 **E-mail(전자 메일)을** 선택합니다



6. **Outlook Web Access** 확인란을 선택하고 URL 레이블과 링크 정보를 입력한 다음 **확인**을 클릭합니다.

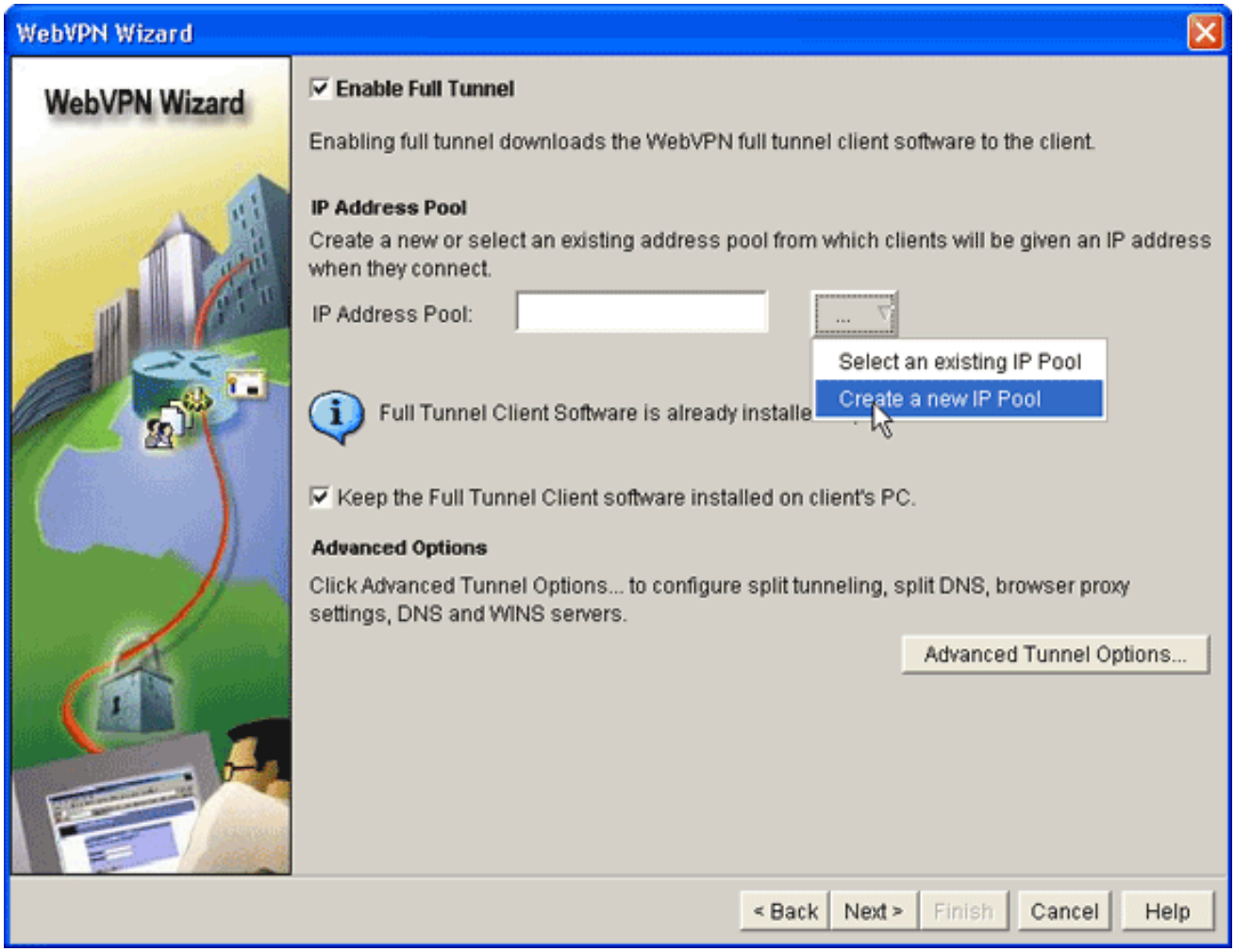


7. 원하는 리소스를 추가한 후 **확인**을 클릭한 다음 **다음**을 클릭합니다.WebVPN Wizard 전체 터널 대화 상자가 나타납니다



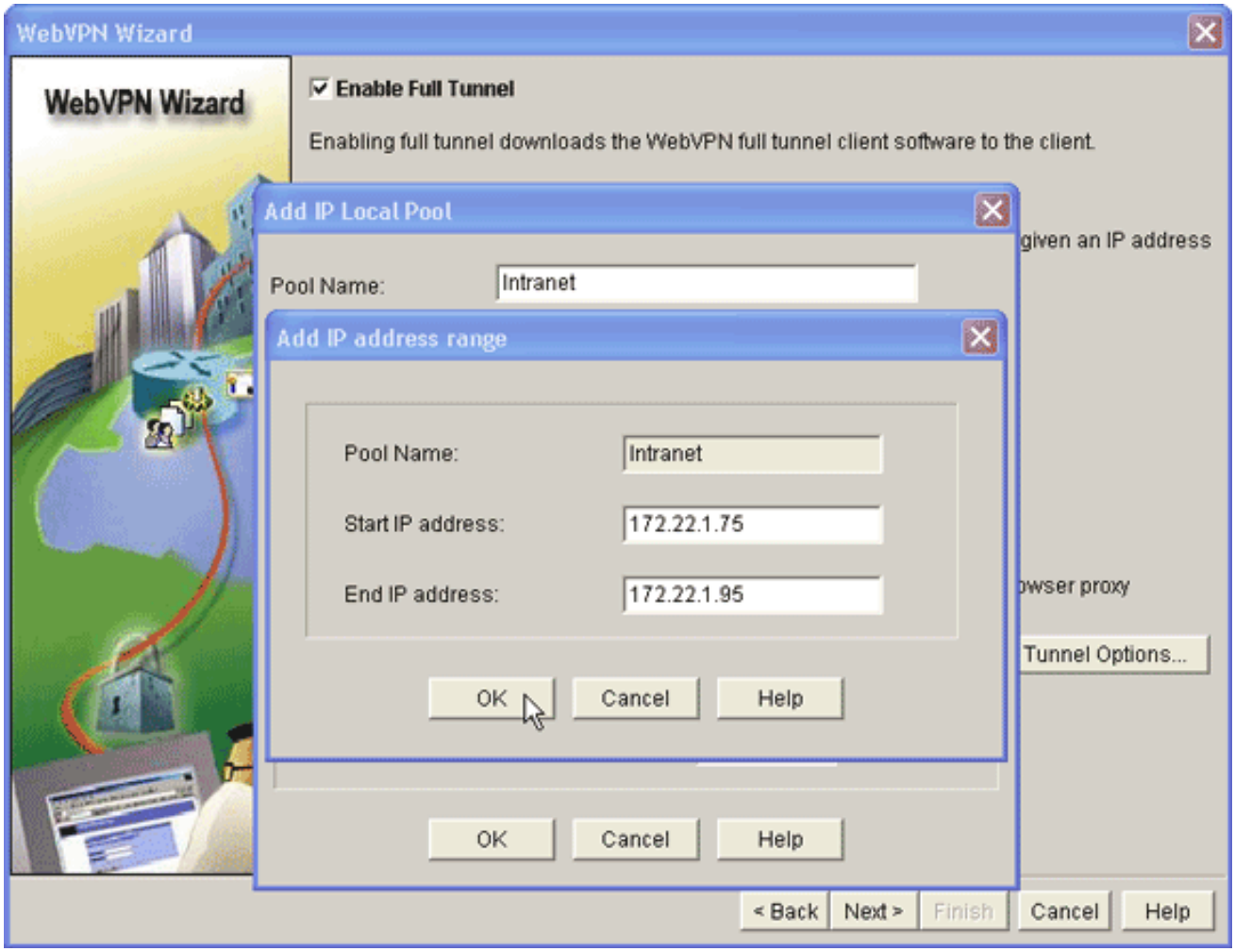
8. Enable Full **Tunnel(전체 터널 활성화**) 확인란이 선택되어 있는지 확인합니다.
9. 이 WebVPN 컨텍스트의 클라이언트가 사용할 수 있는 IP 주소 풀을 만듭니다.주소 풀은 인트라넷에서 사용 가능하며 라우팅할 수 있는 주소와 일치해야 합니다.
10. IP Address Pool(IP 주소 풀) 필드 옆에 있는 줄임표(**..**)를 클릭하고 **Create a new IP Pool(새 IP 풀 생성)을** 선택합니다

.



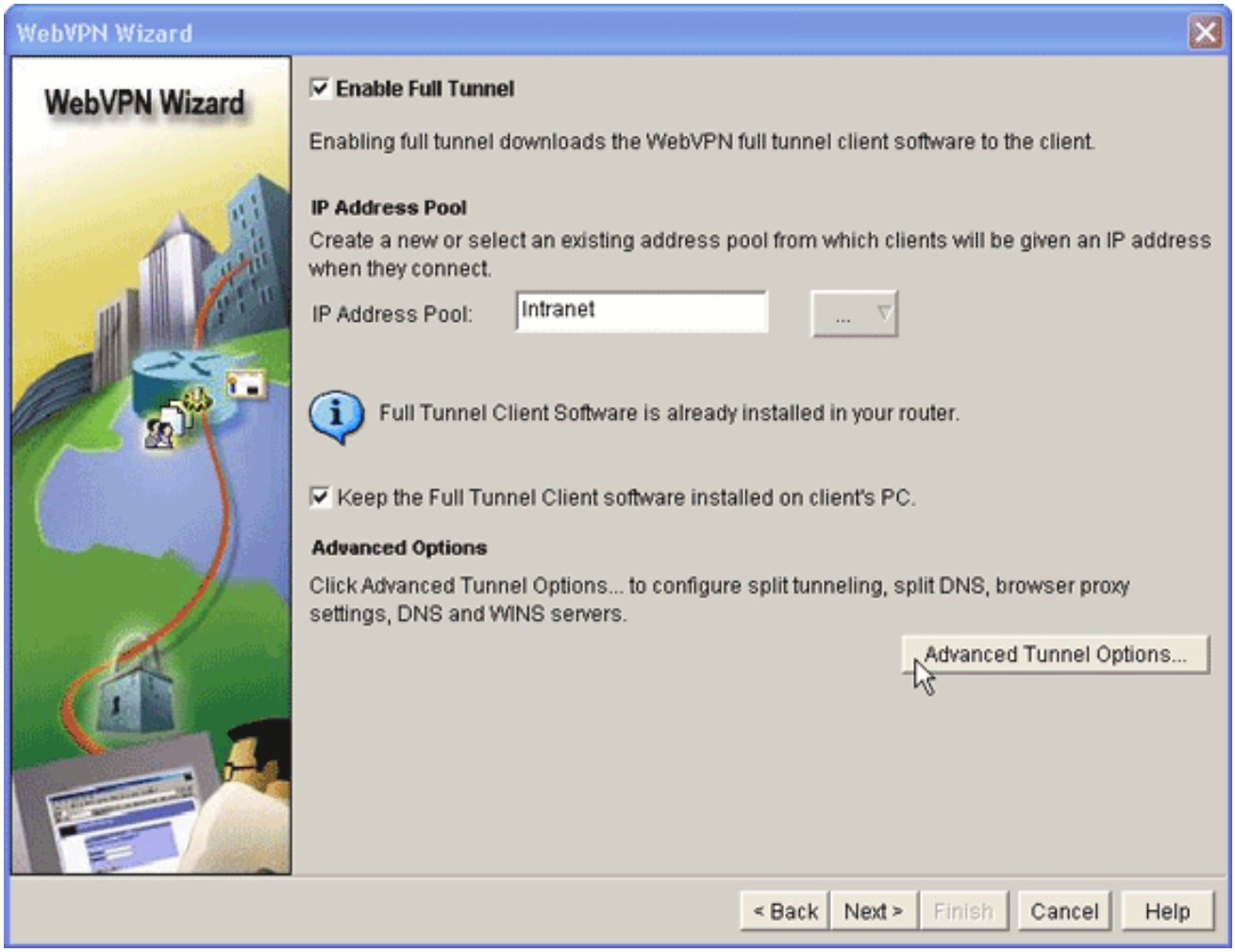
11. Add IP Local Pool(IP 로컬 풀 추가) 대화 상자에서 풀 이름을 입력하고 Add(추가)를 **클릭합니다**

.



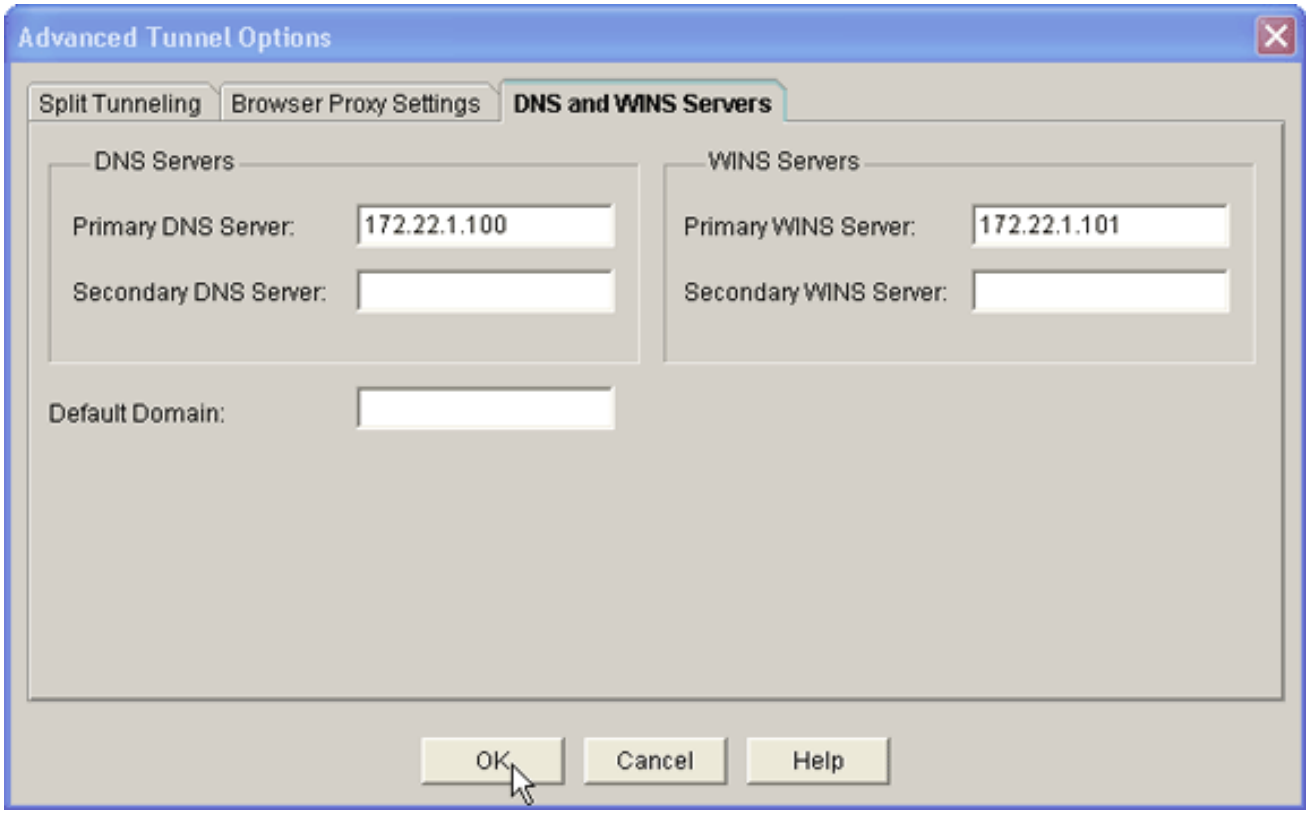
12. Add IP address range(IP 주소 범위 추가) 대화 상자에서 SVC 클라이언트의 주소 풀 범위를 입력하고 **OK**(확인)를 클릭합니다.**참고:** IP 주소 풀은 라우터에 직접 연결된 인터페이스 범위에 있어야 합니다.다른 풀 범위를 사용하려면 이 요구 사항을 충족하기 위해 새 풀과 연결된 루프백 주소를 생성할 수 있습니다.
13. **확인**을 **클릭합니다**

.



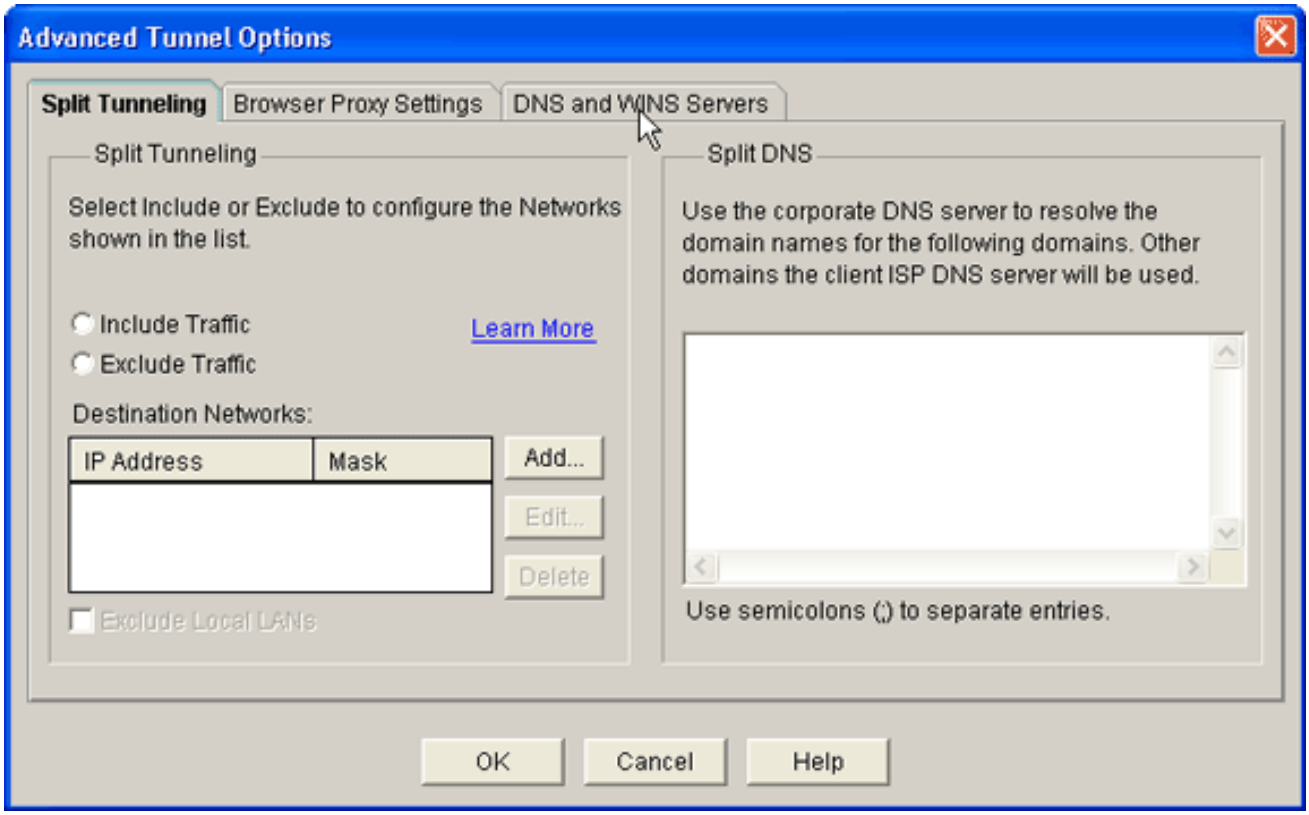
14. 원격 클라이언트가 SVC의 복사본을 영구적으로 저장하도록 하려면 **Keep the Full Tunnel Client Software installed on client's PC(클라이언트의 PC에 전체 터널 클라이언트 소프트웨어 설치 유지)** 확인란을 클릭합니다.클라이언트가 연결될 때마다 클라이언트가 SVC 소프트웨어를 다운로드하도록 하려면 이 옵션을 선택 취소합니다.
15. 스플릿 터널링, 스플릿 DNS, 브라우저 프록시 설정, DNS 및 WNS 서버와 같은 고급 터널 옵션을 구성합니다.Cisco에서는 최소 DNS 및 WINS 서버를 구성하는 것이 좋습니다.고급 터널 옵션을 구성하는 절차는 다음과 같습니다.Advanced **Tunnel Options(고급 터널 옵션)** 버튼을 클릭합니다

.

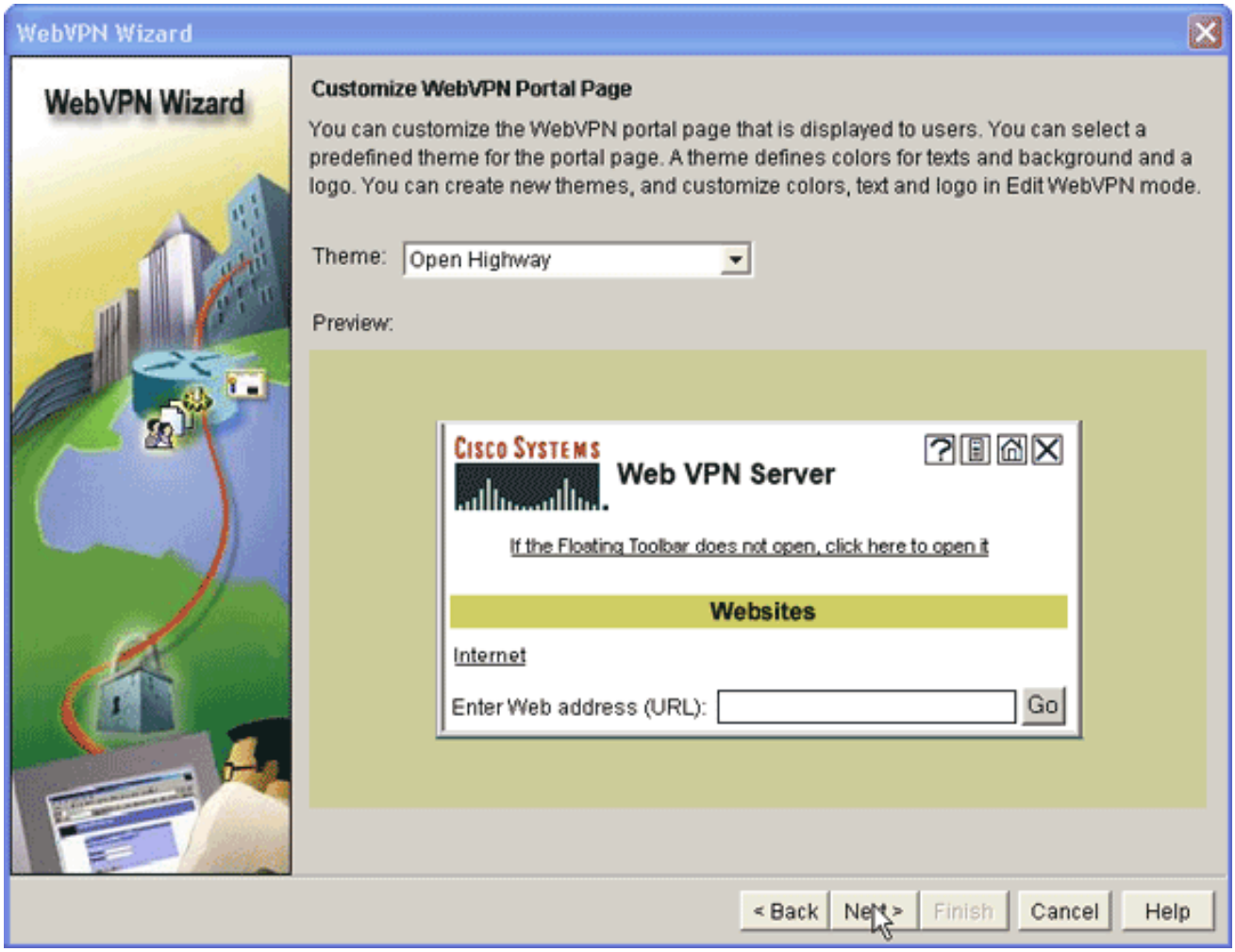


DNS and WINS Servers(DNS 및 WINS 서버) 탭을 클릭하고 DNS 및 WINS 서버의 기본 IP 주소를 입력합니다.스플릿 터널링 및 브라우저 프록시 설정을 구성하려면 **Split Tunneling** 또는 **Browser Proxy Settings** 탭을 클릭합니다

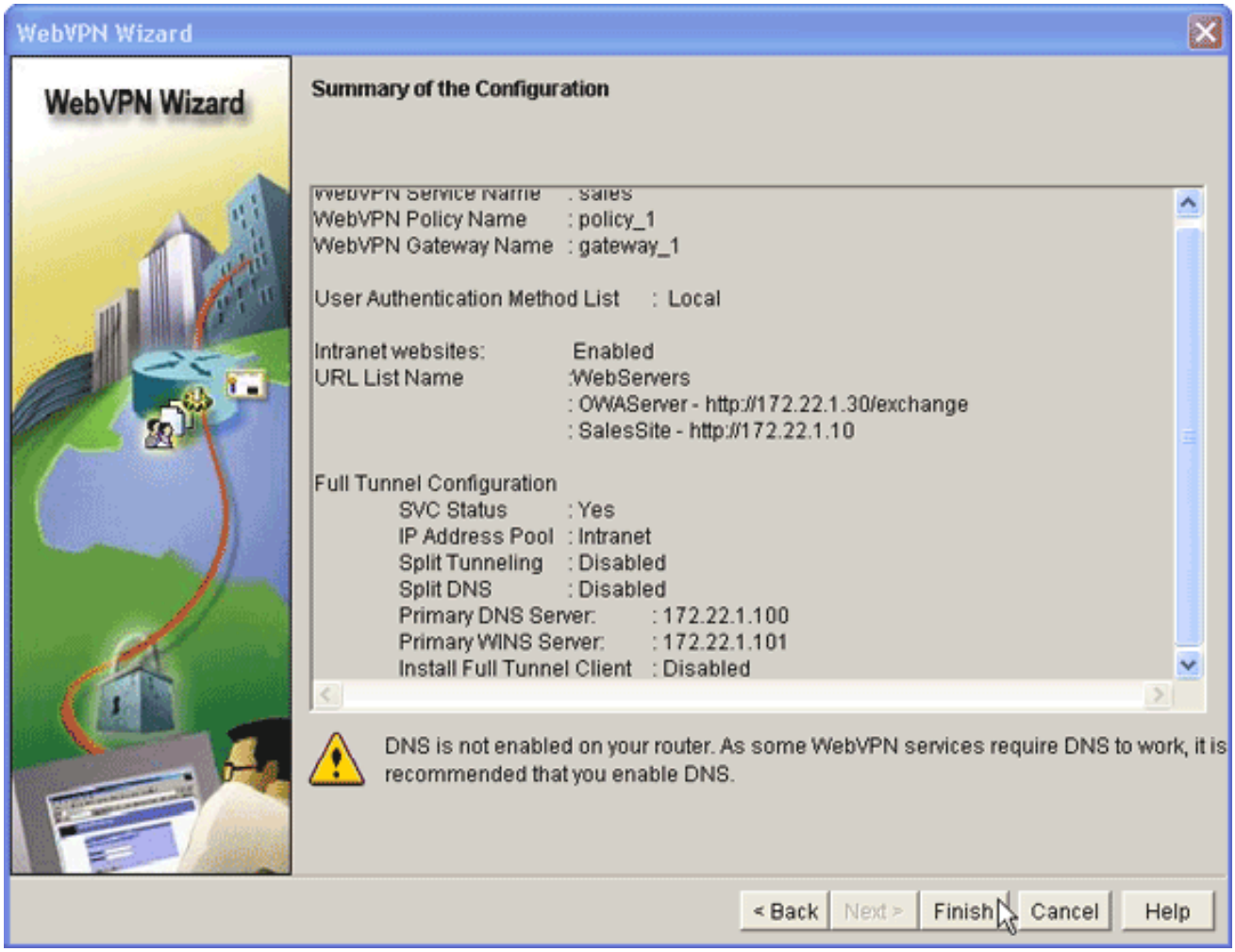
.



16. 필요한 옵션을 구성한 후 Next(**다음**)를 클릭합니다.
17. WebVPN Portal Page(WebVPN 포털 페이지)를 사용자 지정하거나 기본값을 선택합니다 .Customize WebVPN Portal Page(WebVPN 포털 사용자 지정 페이지)를 사용하면 WebVPN Portal Page(WebVPN 포털 페이지)가 고객에게 표시되는 방식을 사용자 지정할 수 있습니다 .

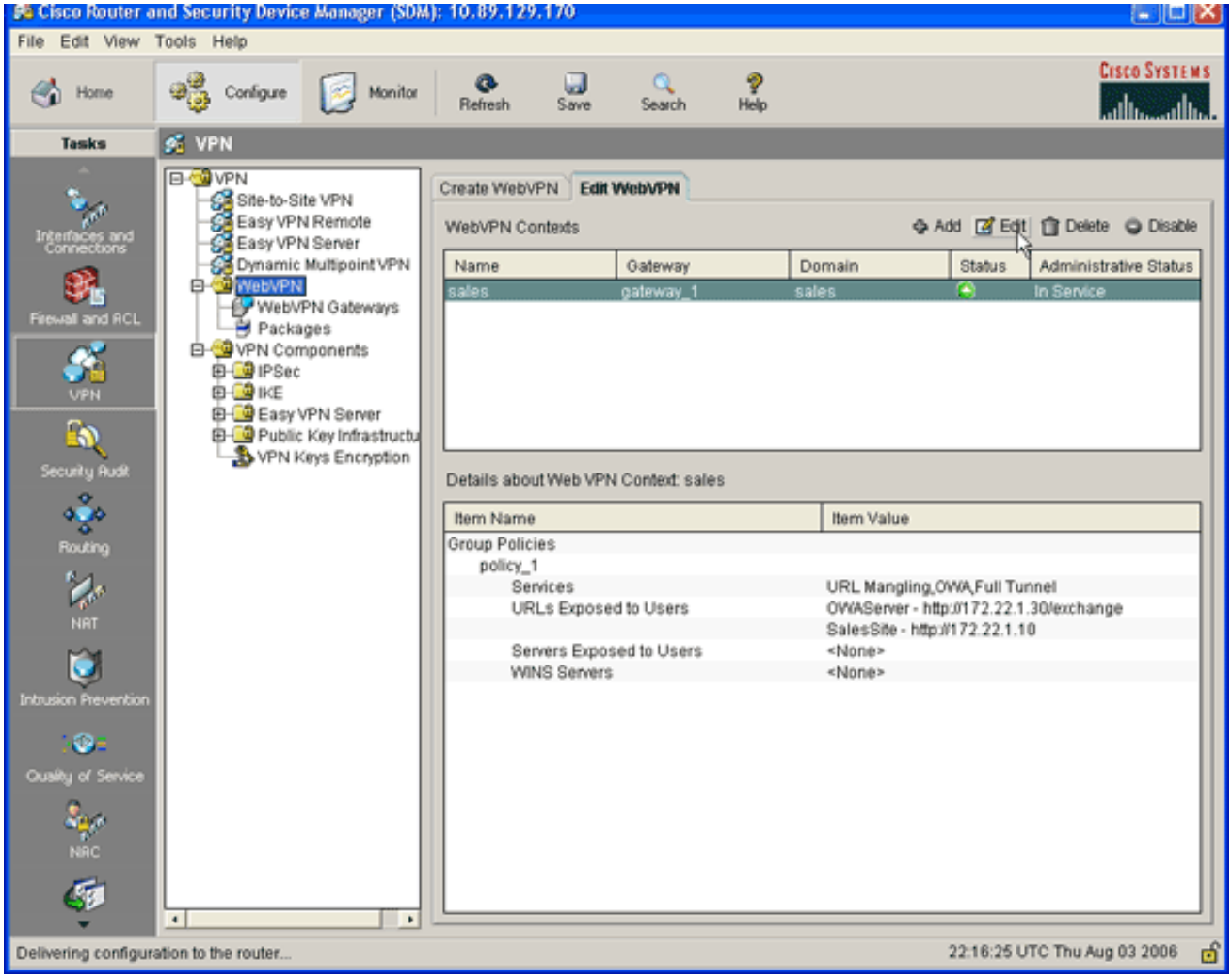


18. WebVPN Portal Page(WebVPN 포털 페이지)를 구성한 후 **Next(다음)**를 클릭하고 **Finish(마침)**를 클릭한 다음 **OK(확인)를 클릭합니다**.WebVPN 마법사가 라우터에 투어 명령을 제출합니다.
19. OK(**확인**)를 클릭하여 컨피그레이션을 저장합니다.**참고:** 오류 메시지가 표시되면 WebVPN 라이센스가 잘못되었을 수 있습니다.다음 이미지에 샘플 오류 메시지가 표시됩니다
.



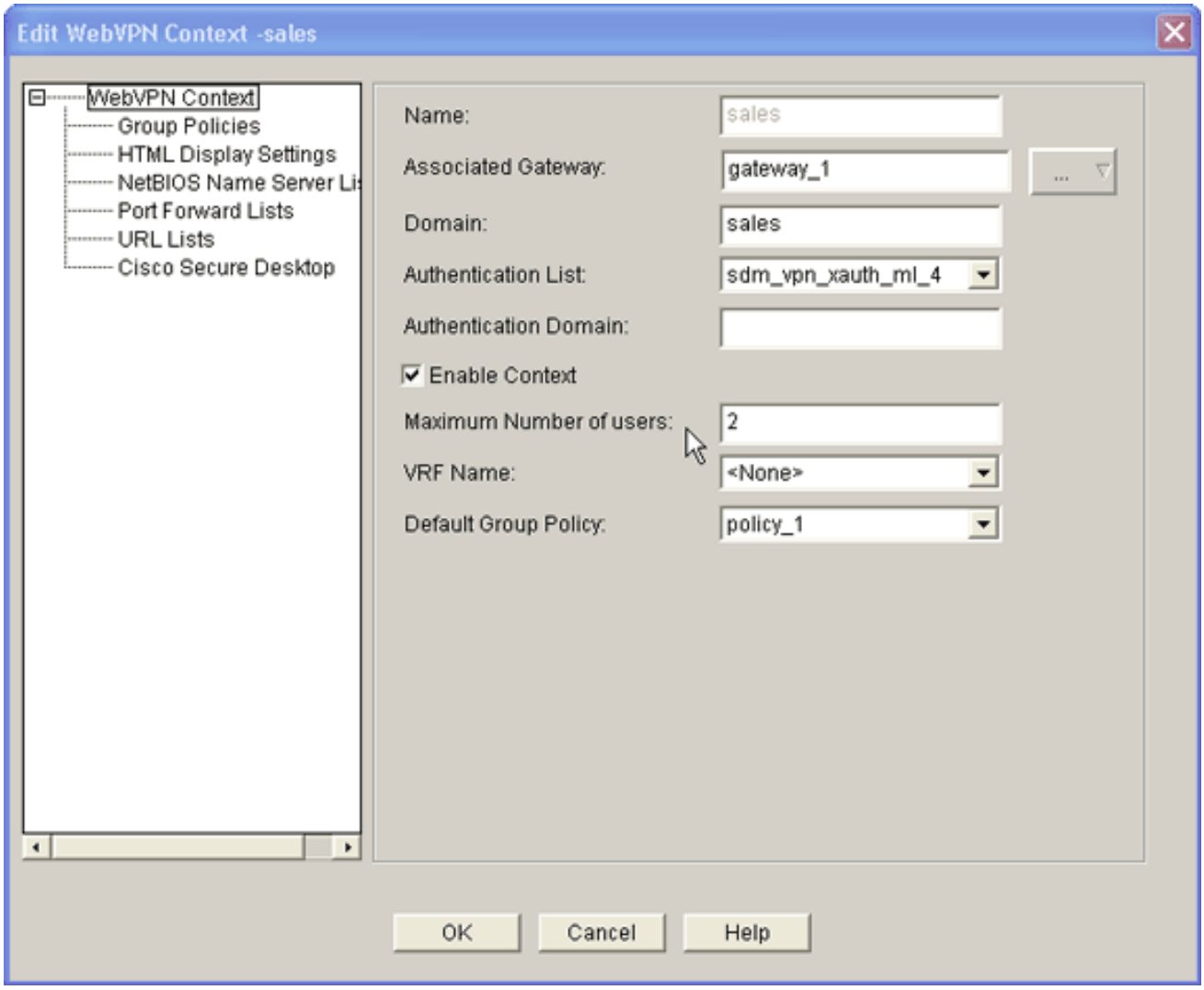
라이센스 문제를 해결하려면 다음 단계를 완료하십시오.Configure(구성)를 클릭한 다음 **VPN**을 클릭합니다.WebVPN**을** 확장하고 Edit WebVPN **탭을** 클릭합니다

.



새로 만든 컨텍스트를 강조 표시하고 **Edit** 버튼을 클릭합니다

.



Maximum Number of users(최대 사용자 수) 필드에 라이센스의 올바른 사용자 수를 입력합니다.OK(**확인**)를 클릭한 다음 **OK**(확인)를 클릭합니다.명령이 컨피그레이션 파일에 기록됩니다.Save(**저장**)를 클릭한 다음 **Yes(예)**를 클릭하여 변경 사항을 적용합니다.

결과

ASDM은 다음과 같은 명령줄 구성을 생성합니다.

ausnml-3825-01

```
ausnml-3825-01#show run
Building configuration...

Current configuration : 4393 bytes
!
! Last configuration change at 22:24:06 UTC Thu Aug 3
2006 by ausnml
! NVRAM config last updated at 22:28:54 UTC Thu Aug 3
2006 by ausnml
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ausnml-3825-01
!
```

```
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-9.T.bin
boot-end-marker
!
no logging buffered
!
aaa new-model
!
!--- Added by SDM for local aaa authentication. aaa
authentication login sdm_vpn_xauth_ml_1 local aaa
authentication login sdm_vpn_xauth_ml_2 local aaa
authentication login sdm_vpn_xauth_ml_3 local aaa
authentication login sdm_vpn_xauth_ml_4 local ! aaa
session-id common ! resource policy ! ip cef ! ip domain
name cisco.com ! voice-card 0 no dspfarm !--- Digital
certificate information. crypto pki trustpoint TP-self-
signed-577183110 enrollment selfsigned subject-name
cn=IOS-Self-Signed-Certificate-577183110 revocation-
check none rsakeypair TP-self-signed-577183110 ! crypto
pki certificate chain TP-self-signed-577183110
certificate self-signed 01 3082024E 308201B7 A0030201
02020101 300D0609 2A864886 F70D0101 04050030 30312E30
2C060355 04031325 494F532D 53656C66 2D536967 6E65642D
43657274 69666963 6174652D 35373731 38333131 30301E17
0D303630 37323731 37343434 365A170D 32303031 30313030
30303030 5A303031 2E302C06 03550403 1325494F 532D5365
6C662D53 69676E65 642D4365 72746966 69636174 652D3537
37313833 31313030 819F300D 06092A86 4886F70D 01010105
0003818D 00308189 02818100 F43F6DD9 32A264FE 4C5B0829
698265DC 6EC65B17 21661972 D363BC4C 977C3810 !--- Output
suppressed. quit username wishaw privilege 15 secret 5
$1$r4CW$SeP6ZwQEAAU68W9kbR16U. username ausnml privilege
15 password 7 044E1F505622434B username sales privilege
15 secret 5 $1$/Lc1$K.Zt41zF1jSdKZrPgNK1A. username
newcisco privilege 15 secret 5
$1$Axlm$7k5PWspXKxUpoSReHo7IQ1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
ip virtual-reassembly duplex auto speed auto media-type
rj45 no keepalive ! interface GigabitEthernet0/1 ip
address 172.22.1.151 255.255.255.0 duplex auto speed
auto media-type rj45 !--- Clients receive an address
from this pool. ip local pool Intranet 172.22.1.75
172.22.1.95 ip route 0.0.0.0 0.0.0.0 172.22.1.1 ! ip
http server ip http authentication local ip http secure-
server ip http timeout-policy idle 600 life 86400
requests 100 ! control-plane ! line con 0 stopbits 1
line aux 0 stopbits 1 line vty 0 4 ! scheduler allocate
20000 1000 !--- Identify the gateway and port. webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint TP-self-signed-577183110
inservice !--- SVC package file. webvpn install svc
flash:/webvpn/svc.pkg ! !--- WebVPN context. webvpn
context sales title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all ! !---
Resources available to this context. url-list
"WebServers" heading "Intranet Web" url-text "SalesSite"
url-value "http://172.22.1.10" url-text "OWAServer" url-
value "http://172.22.1.20/exchange" ! nbns-list NBNS-
Servers nbns-server 172.22.1.15 master !--- Group policy
for the context. policy group policy_1 url-list
"WebServers" functions svc-enabled svc address-pool
"Intranet" svc default-domain "cisco.com" svc keep-
client-installed svc dns-server primary 172.22.1.100 svc
wins-server primary 172.22.1.101 default-group-policy
```

```
policy_1 aaa authentication list sdm_vpn_xauth_ml_4
gateway gateway_1 domain sales max-users 2 inservice ! !
end
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

절차

컨피그레이션을 테스트하려면 *http://192.168.0.37/sales*을 SSL 지원 클라이언트 웹 브라우저에 입력합니다.

명령

여러 **show** 명령이 WebVPN과 연결되어 있습니다.CLI(Command Line Interface)에서 이러한 명령을 실행하여 통계 및 기타 정보를 표시할 수 있습니다.**show 명령**에 대한 자세한 내용은 WebVPN 컨피그레이션 확인을 참조하십시오.

참고: Output Interpreter Tool(등록된 고객만 해당)(OIT)은 특정 **show** 명령을 **지원합니다**.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

SSL 연결 문제

문제/장애:SSL VPN 클라이언트가 라우터에 연결할 수 없습니다.

해결책:IP 주소 풀에 IP 주소가 부족하여 이 문제가 발생할 수 있습니다.이 문제를 해결하려면 라우터의 IP 주소 풀에서 IP 주소의 수를 늘리십시오.

문제 해결 명령

여러 **clear** 명령이 WebVPN과 연결됩니다.이러한 명령에 대한 자세한 내용은 WebVPN Clear Commands 사용을 참조하십시오.

여러 **디버그** 명령이 WebVPN과 연결됩니다.이러한 명령에 대한 자세한 내용은 WebVPN 디버그 명령 사용을 참조하십시오.

참고: debug 명령을 사용하면 Cisco 디바이스에 부정적인 영향을 미칠 수 있습니다.debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

관련 정보

- Cisco IOS SSLVPN
- SSL VPN - WebVPN

- Cisco IOS의 클라이언트리스 SSL VPN(WebVPN) 및 SDM 컨피그레이션 예
- SDM을 사용하는 씬 클라이언트 SSL VPN(WebVPN) IOS 구성 예
- WebVPN 및 DMVPN 통합 구축 설명서
- 기술 지원 및 문서 – Cisco Systems