SDM을 사용하여 씬 클라이언트 SSL VPN(WebVPN) Cisco IOS 구성

목차

소개

씬 클라이언트 SSL VPN 기술을 사용하여 고정 포트를 사용하는 애플리케이션에 대한 보안 액세스를 허용할 수 있습니다. 예를 들면 텔넷(23), SSH(22), POP3(110), IMAP4(143) 및 SMTP(25)가 있습니다. 씬 클라이언트는 사용자 중심, 정책 기반 또는 둘 다 될 수 있습니다. 사용자별로 액세스를 구성하거나, 하나 이상의 사용자를 포함하는 그룹 정책을 생성할 수 있습니다. SSL VPN 기술은 세 가지 기본 모드로 구성할 수 있습니다. 클라이언트리스 SSL VPN(WebVPN), 씬 클라이언트 SSL VPN(포트 전달) 및 SSL VPN 클라이언트(SVC-전체 터널 모드).

1. 클라이언트리스 SSL VPN(WebVPN):

원격 클라이언트에는 기업 LAN에서 http 또는 https 지원 웹 서버에 액세스하기 위해 SSL 지원 웹 브라우저만 필요합니다. CIFS(Common Internet File System)를 사용하여 Windows 파일을 찾아볼 수도 있습니다. http 액세스의 좋은 예는 OWA(Outlook Web Access) 클라이언트입니다.

클라이언트리스 SSL VPN에 대한 자세한 내용은 SDM 컨피그레이션 예를 사용하여 Cisco IOS의 클라이언트리스 SSL VPN(WebVPN)을 참조하십시오.

2. 씬 클라이언트 SSL VPN(포트 전달)

원격 클라이언트는 정적 포트 번호를 사용하는 TCP 애플리케이션의 안전한 액세스를 위해 작은

Java 기반 애플릿을 다운로드해야 합니다. UDP는 지원되지 않습니다. 예를 들면 POP3, SMTP, IMAP, SSH 및 텔넷에 대한 액세스가 있습니다. 로컬 시스템의 파일이 변경되었으므로 사용자에게 로컬 관리 권한이 필요합니다. 이 SSL VPN 방법은 동적 포트 할당을 사용하는 애플리케이션(예: 여러 FTP 애플리케이션)에서 작동하지 않습니다.

3. SSL VPN 클라이언트(SVC-전체 터널 모드):

SSL VPN Client는 소규모 클라이언트를 원격 워크스테이션에 다운로드하고 내부 기업 네트워크의 리소스에 대한 완전한 보안 액세스를 허용합니다. SVC는 원격 스테이션에 영구적으로 다운로드하거나 보안 세션이 종료된 후에 제거할 수 있습니다.

SSL VPN 클라이언트에 대한 자세한 내용은 SDM 구성 예를 사용하여 IOS의 SSL VPN 클라이언트(SVC)를 참조하십시오.

이 문서에서는 Cisco IOS® 라우터의 씬 클라이언트 SSL VPN에 대한 간단한 컨피그레이션을 보여줍니다. 씬 클라이언트 SSL VPN은 다음 Cisco IOS 라우터에서 실행됩니다.

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

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

Cisco IOS 라우터의 요구 사항

- SDM과 함께 로드된 나열된 라우터 및 IOS 버전 12.4(6)T 이상의 고급 이미지
- SDM과 함께 로드된 관리 스테이션Cisco는 SDM의 사전 설치된 사본을 새 라우터와 함께 제공합니다. 라우터에 SDM이 설치되어 있지 않은 경우 소프트웨어 다운로드-Cisco 보안 장치 관리자에서 소프트웨어를 가져올 수 있습니다. 서비스 계약이 있는 CCO 계정을 보유해야 합니다. 자세한 지침은 보안 장치 관리자로 라우터 구성을 참조하십시오.

클라이언트 컴퓨터의 요구 사항

- 원격 클라이언트에는 로컬 관리 권한이 있어야 합니다. 필수 사항은 아니지만, 매우 권장됩니다.
- 원격 클라이언트에는 JRE(Java Runtime Environment) 버전 1.4 이상이 있어야 합니다.
- 원격 클라이언트 브라우저: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 또는 Firefox 1.0
- 원격 클라이언트에서 쿠키 사용 및 팝업 허용

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Advanced Enterprise Software 이미지 12.4(9)T
- Cisco 3825 Integrated Services Router
- Cisco Router and Security Device Manager(SDM) 버전 2.3.1

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 지워진(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다. 이 구성에 사용되는 IP 주소는 RFC 1918 주소 공간에서 제공됩니다. 인터넷에서는 합법적이지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

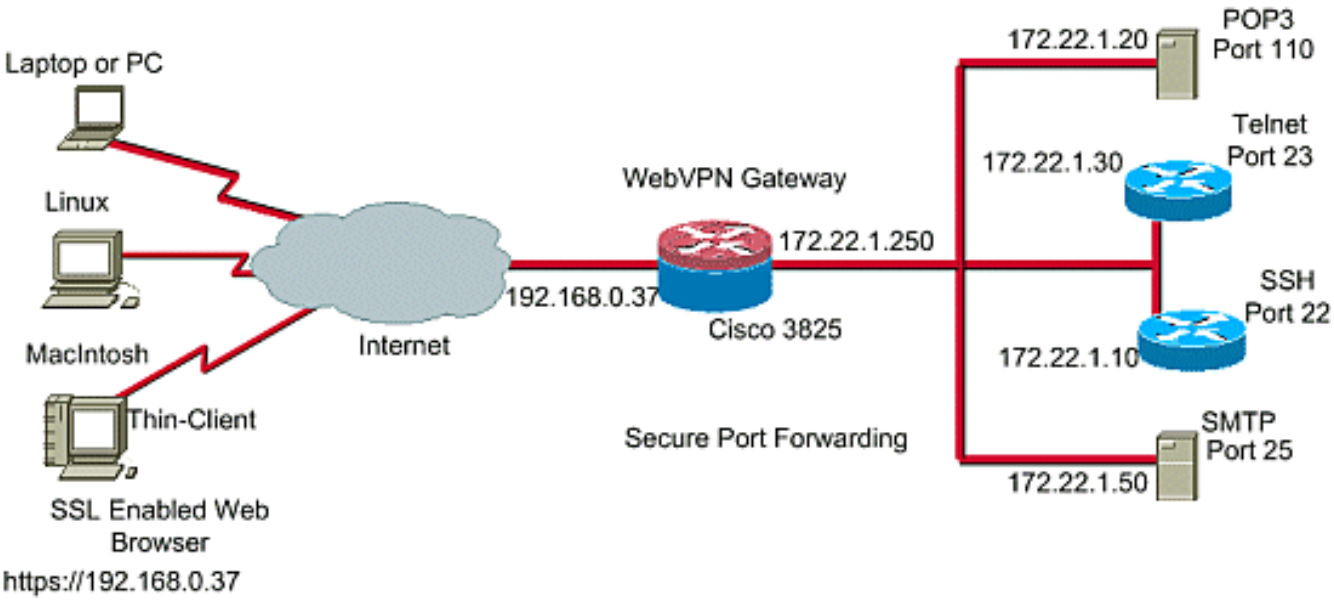
구성

작업

이 섹션에서는 이 문서에서 설명하는 기능을 구성하는 데 필요한 정보를 제공합니다.

네트워크 다이어그램

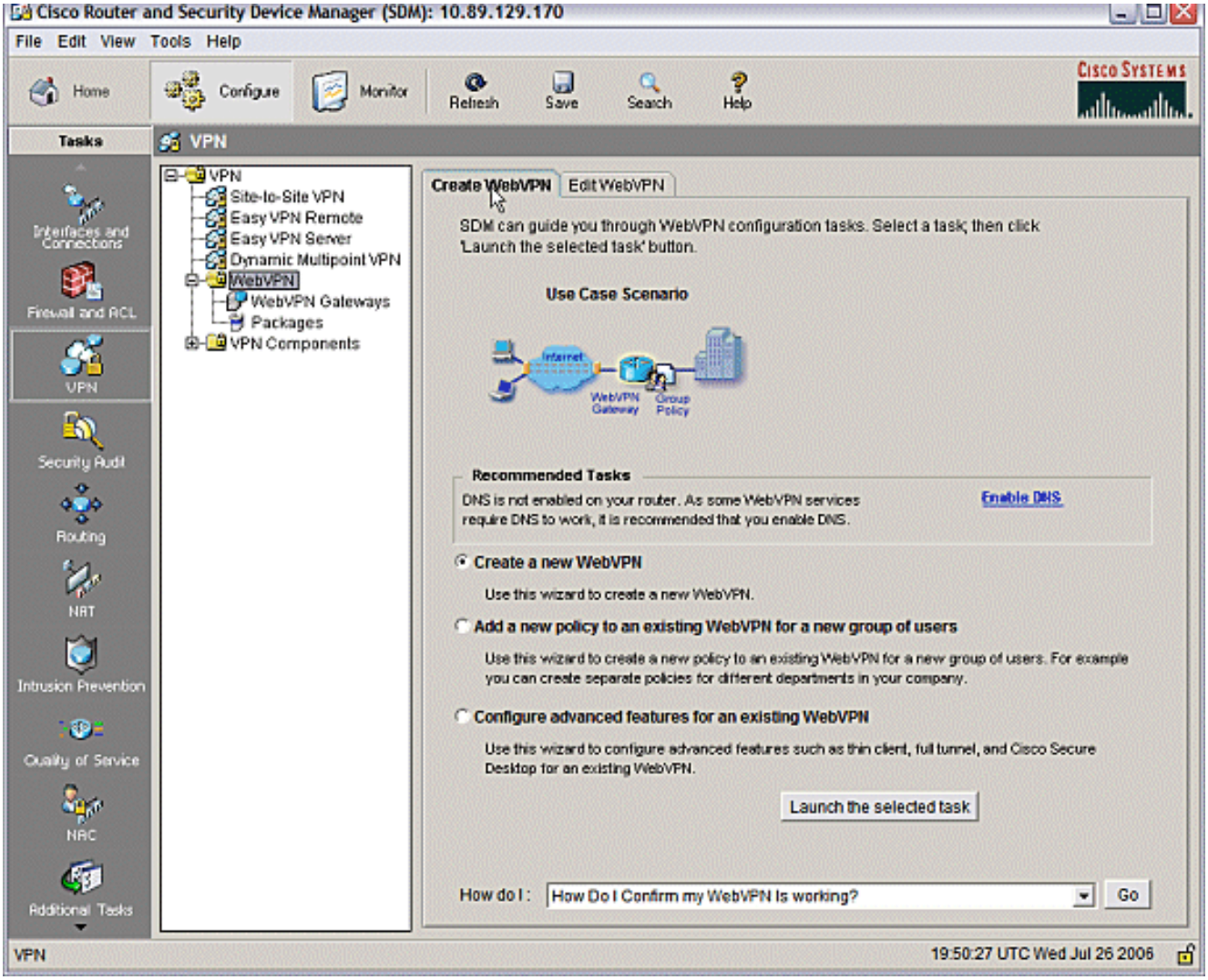
이 문서에서는 다음 네트워크 설정을 사용합니다.



씬 클라이언트 SSL VPN 구성

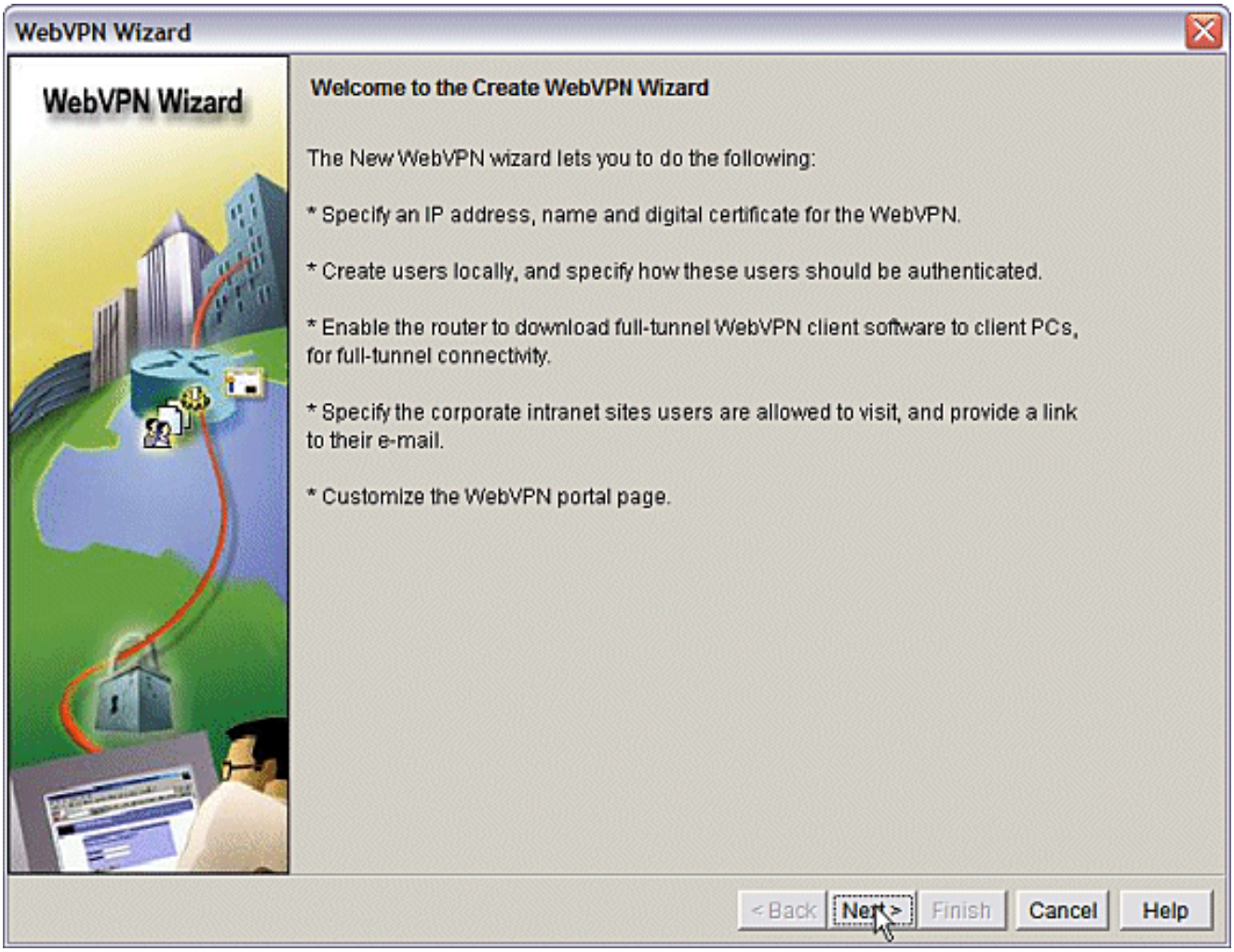
SDM(Security Device Manager) 인터페이스에 제공된 마법사를 사용하여 Cisco IOS에서 씬 클라이언트 SSL VPN을 구성하거나 CLI(Command Line Interface)에서 구성하거나 SDM 애플리케이션에서 수동으로 구성합니다. 이 예에서는 마법사를 사용합니다.

1. 구성 탭을 선택합니다.탐색 창에서 **VPN > WebVPN**을 선택합니다.Create WebVPN(**WebVPN 생성**) 탭을 클릭합니다.Create a **new WebVPN(새 WebVPN 생성)** 옆의 라디오 버튼**을 클릭합니다.선택한 작업 시작** 버튼**을** 클릭합니다
   .



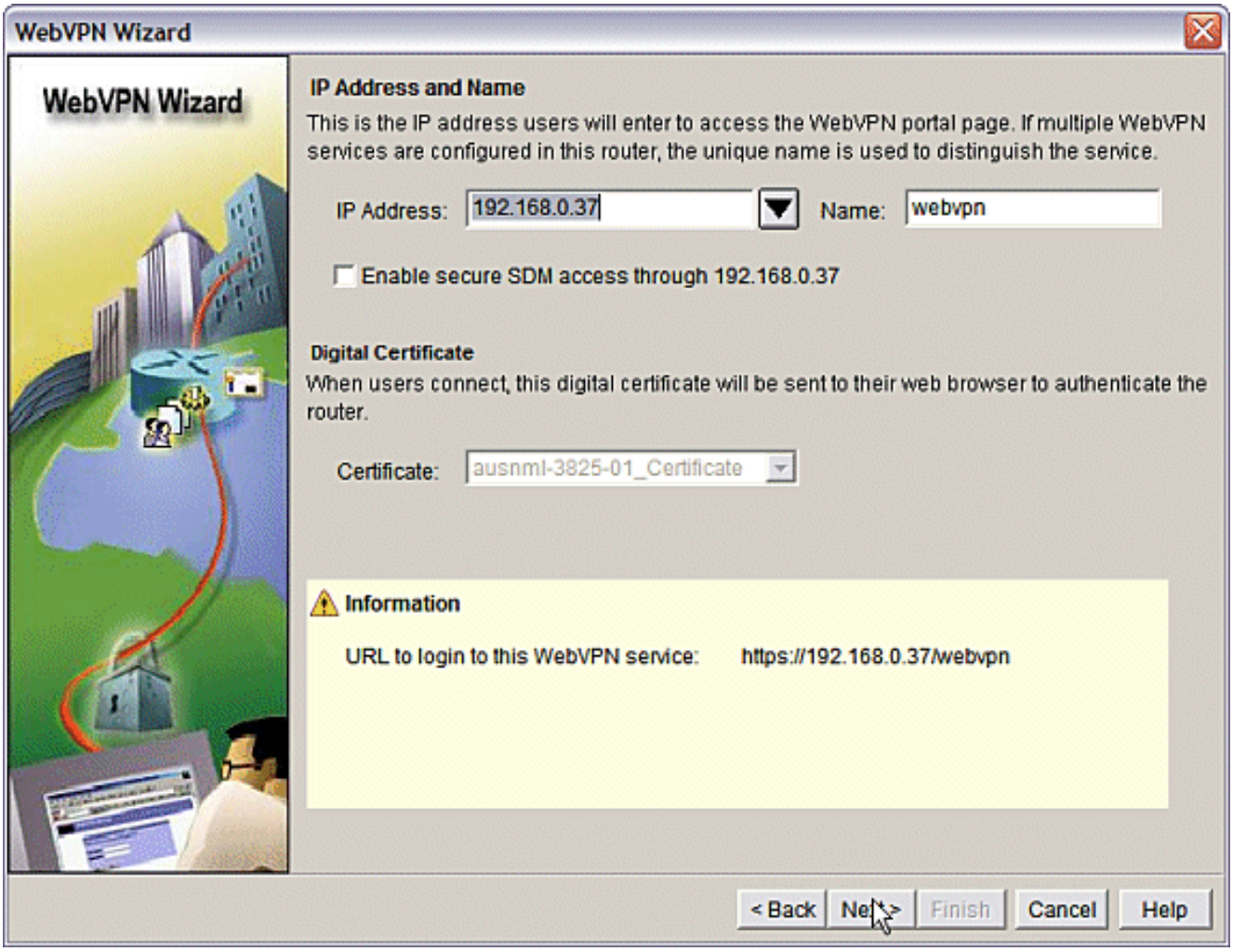
2. WebVPN 마법사가 시작됩니다. Next(**다음)를 클릭합니다**

.

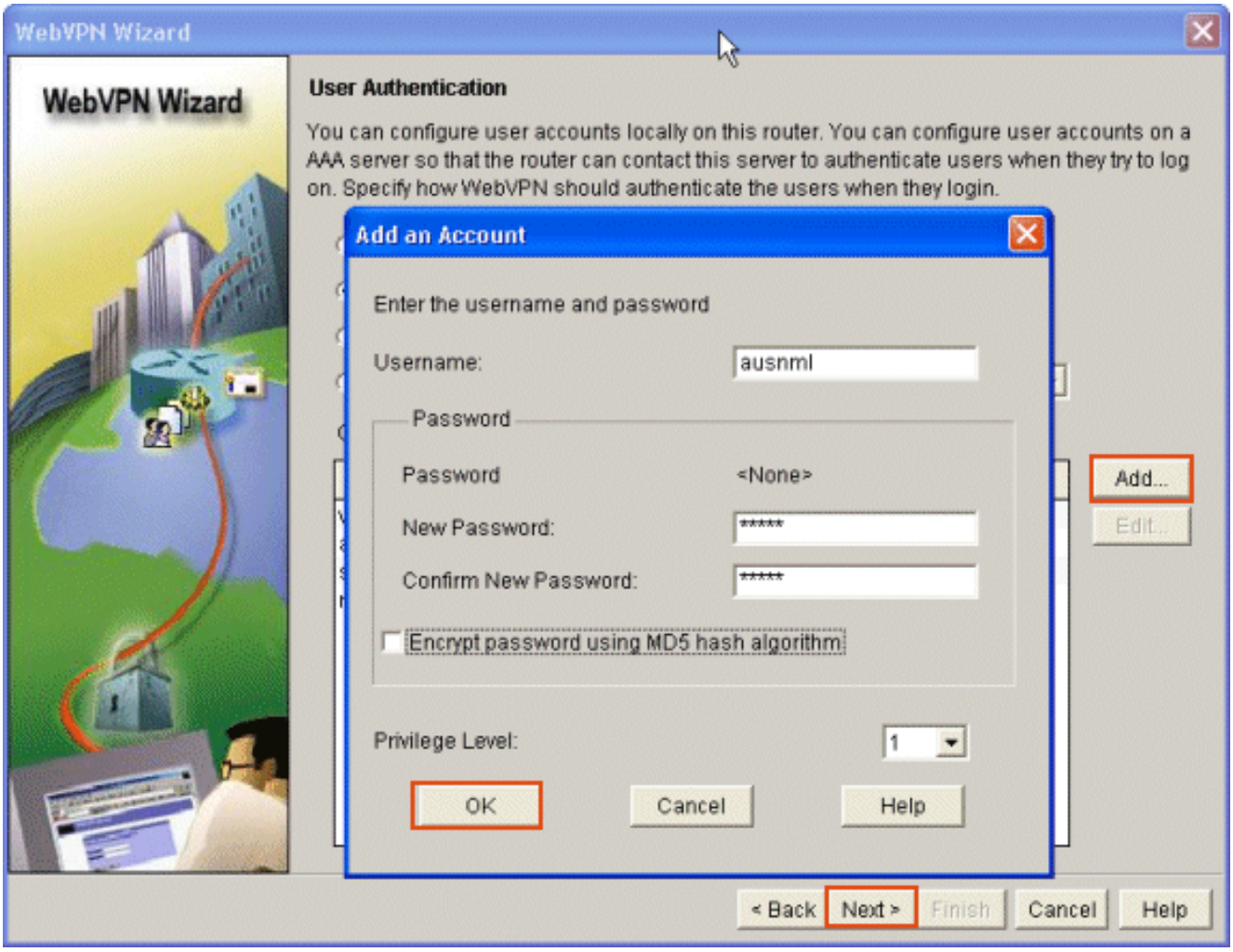


이 WebVPN 게이트웨이의 IP 주소 및 고유한 이름을 입력합니다. Next(**다음)를 클릭합니다**

.

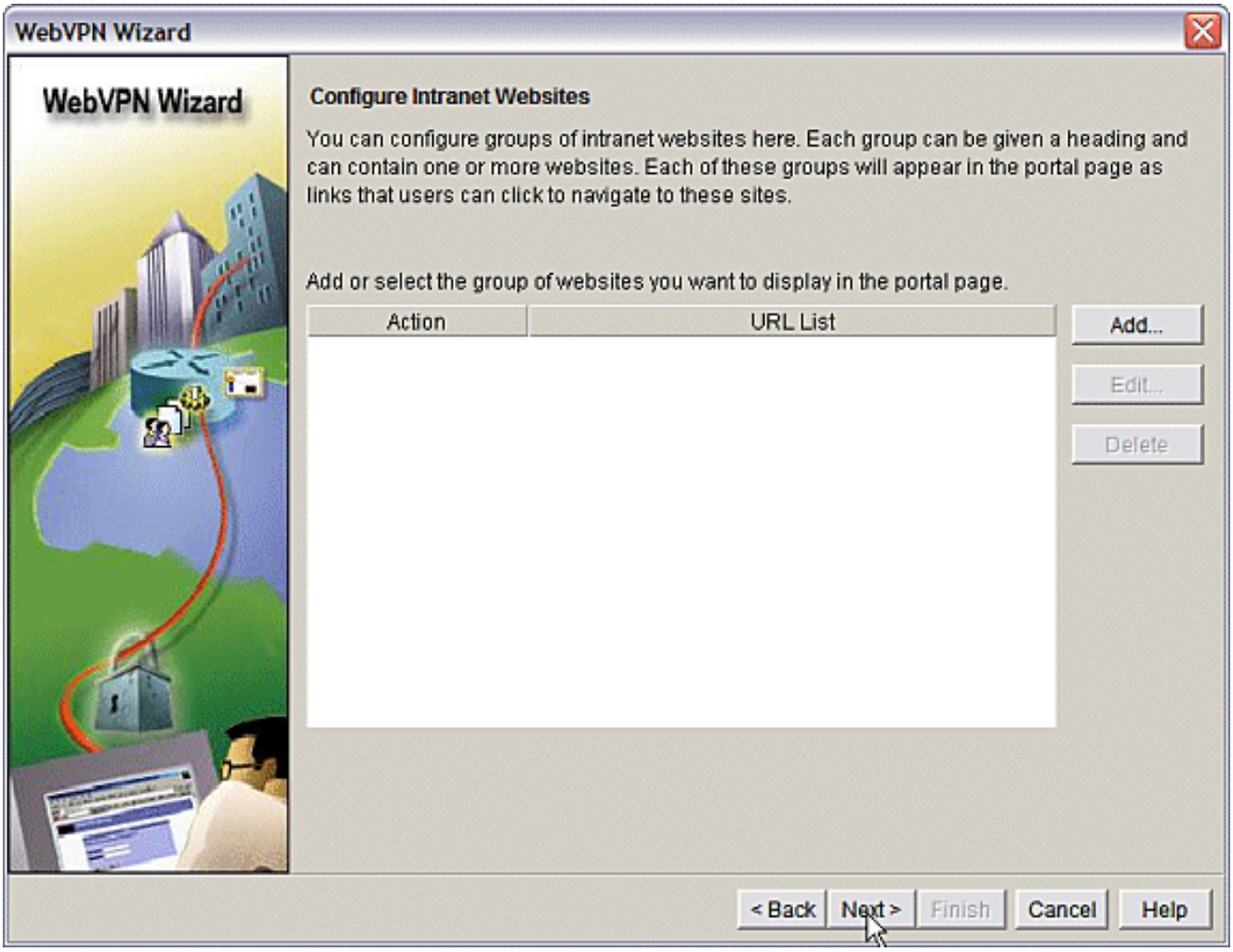


3. User Authentication(사용자 인증) 화면에서는 사용자 인증을 제공할 수 있습니다. 이 컨피그레이션에서는 라우터에서 로컬로 생성된 계정을 사용합니다. AAA(Authentication, Authorization, and Accounting) 서버를 사용할 수도 있습니다.사용자를 추가하려면 **추가**를 클릭합니다.Add an Account(계정 추가) 화면에서 사용자 정보를 입력하고 **OK**(확인)를 클릭합니다.User Authentication(사용자 인증) 화면에서 Next(다음)를 클릭합니다
.



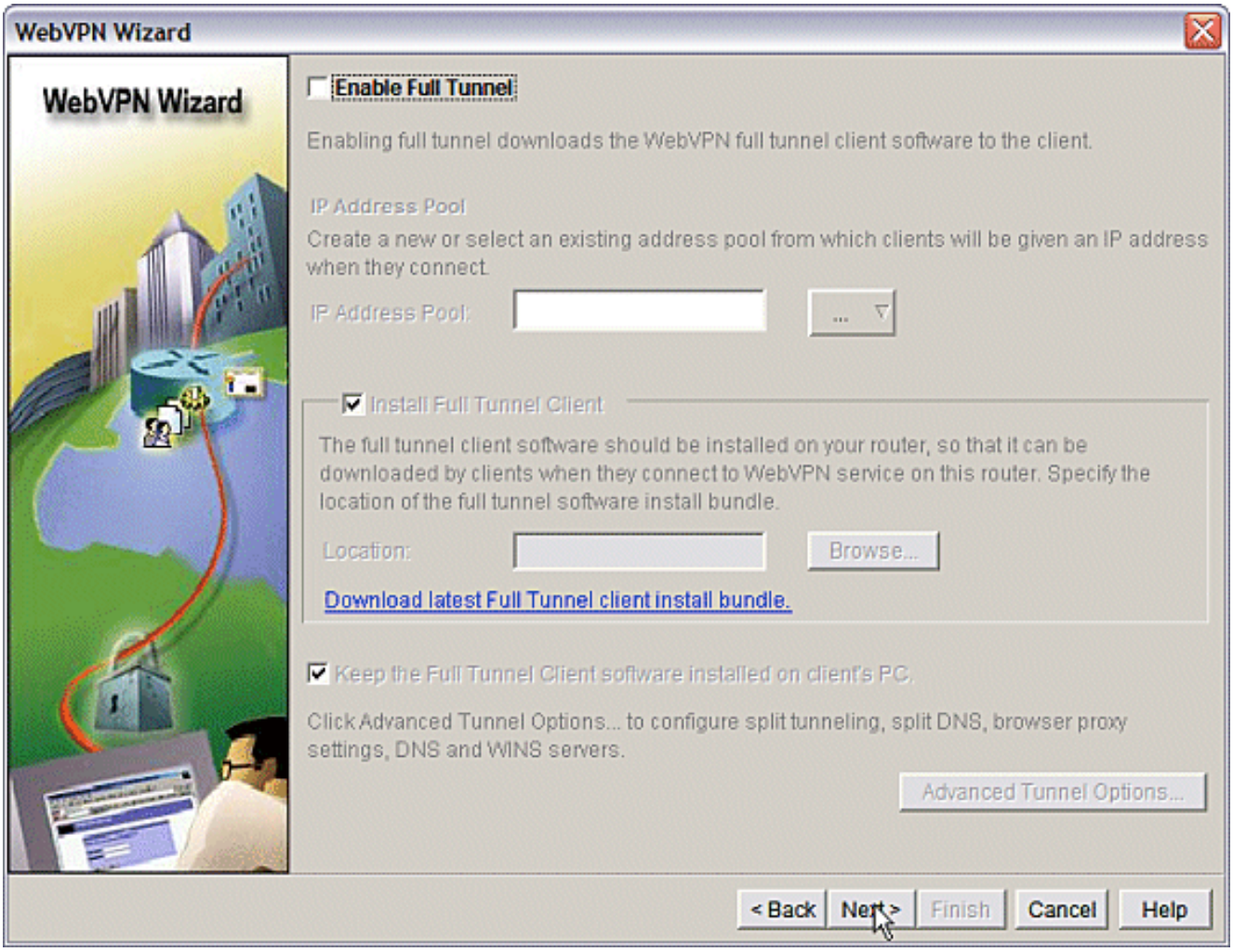
WebVPN Wizard(WebVPN 마법사) 화면에서는 인트라넷 웹 사이트의 구성을 허용하지만 이 애플리케이션 액세스에 포트 전달이 사용되므로 이 단계는 생략됩니다. 웹 사이트에 대한 액세스를 허용하려면 이 문서의 범위에 속하지 않는 클라이언트리스 또는 전체 클라이언트 SSL VPN 구성을 사용합니다

.



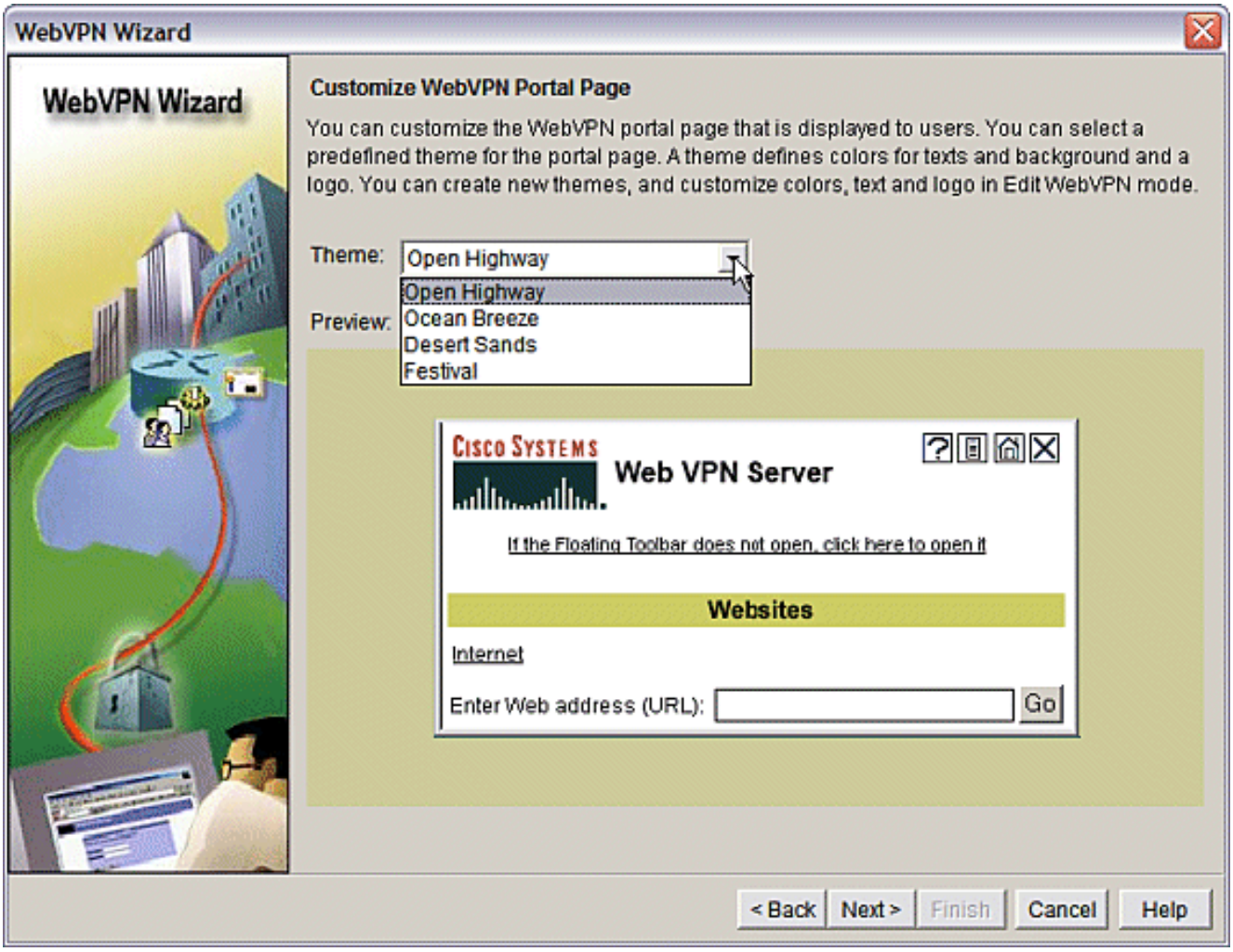
Next(**다음)를 클릭합니다**. 전체 터널 클라이언트 구성을 허용하는 화면이 표시됩니다. 이는 씬 클라이언트 SSL VPN(포트 전달)에는 적용되지 않습니다.Enable **Full Tunnel(전체 터널 활성화)을 선택 취소합니다**. Next(**다음)를 클릭합니다**

.



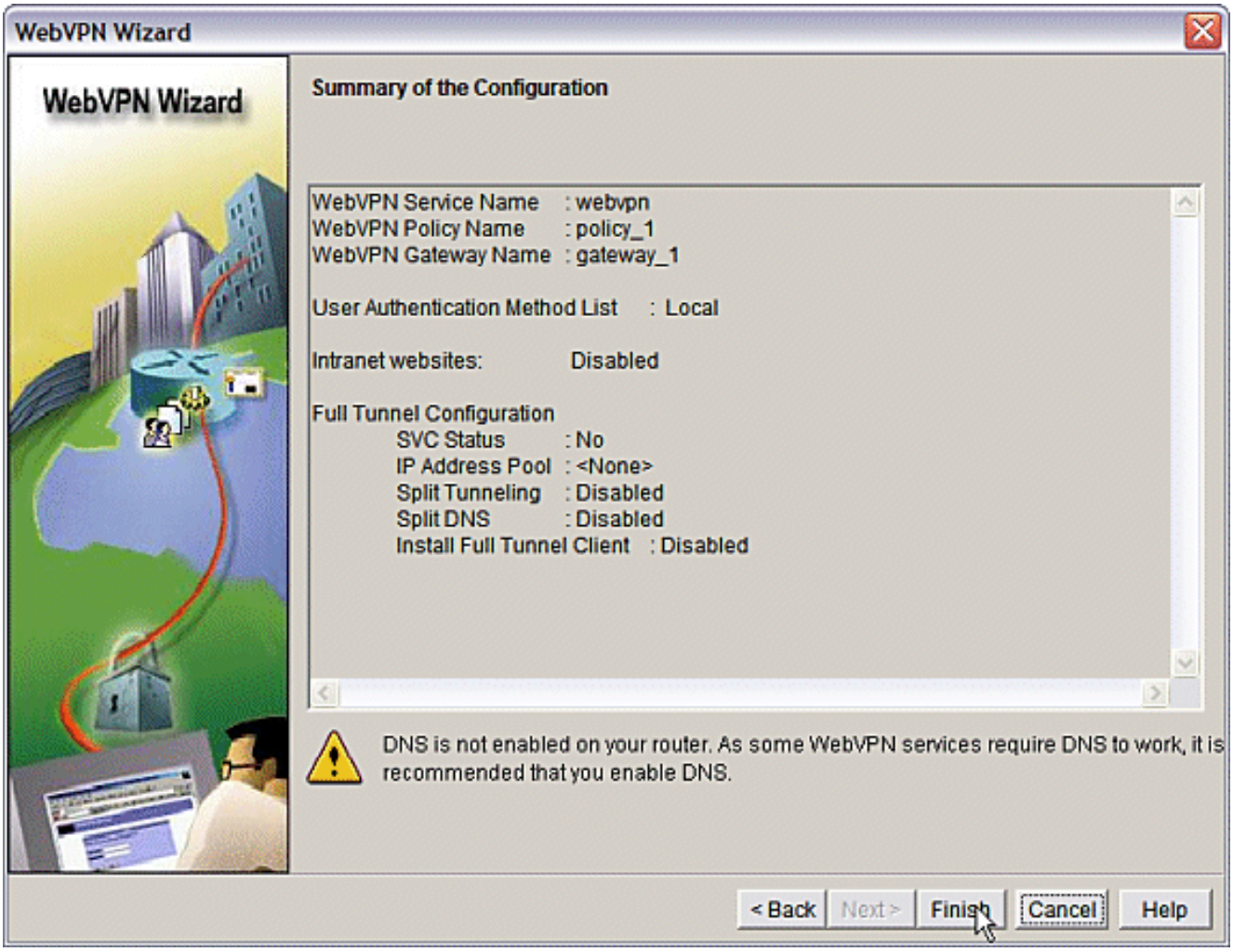
4. WebVPN 포털 페이지의 모양을 사용자 지정하거나 기본 모양을 적용합니다.Next(**다음)를 클릭합니다**

.

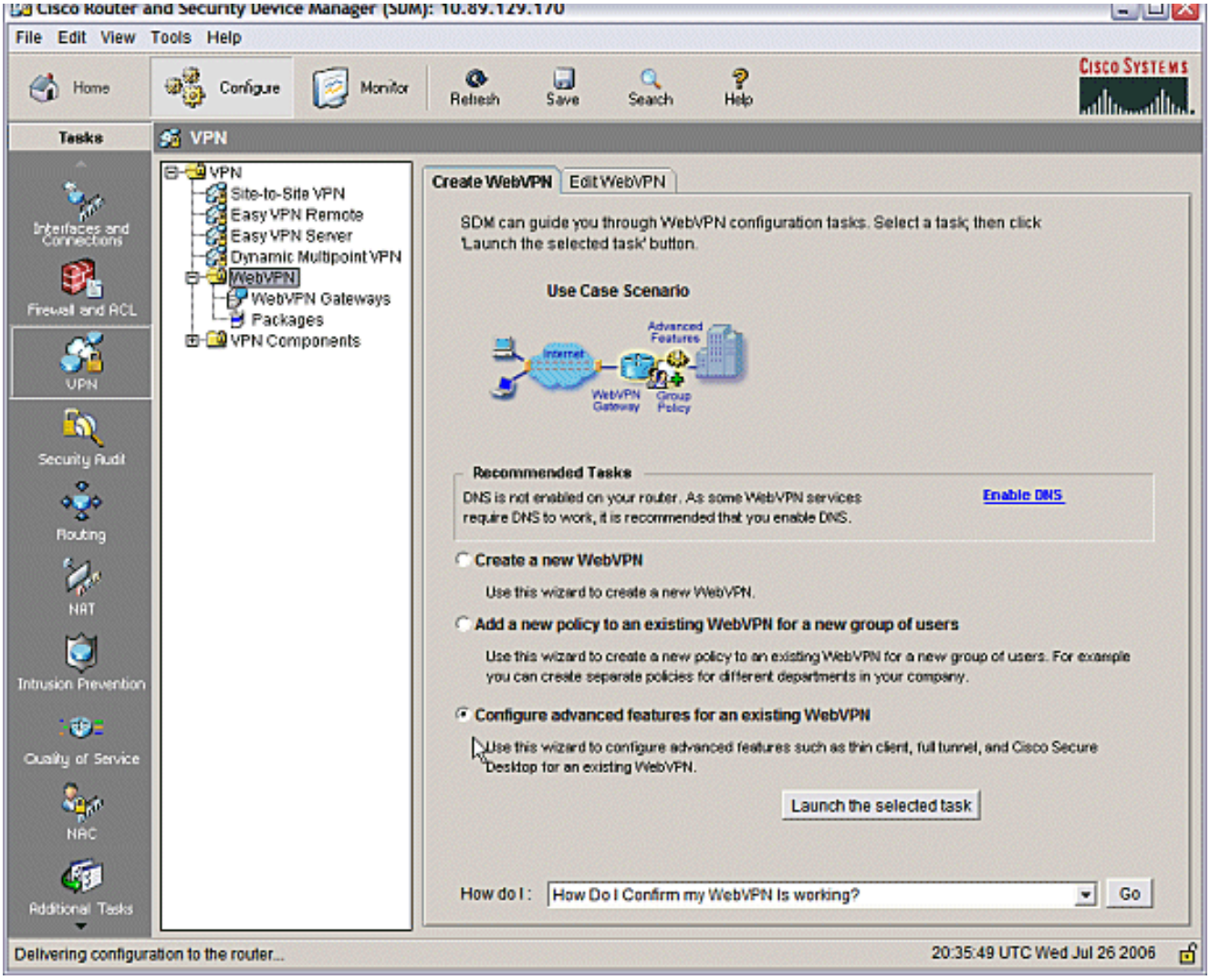


구성 요약을 미리 보고 Finish(마침) **> Save(저장)를 클릭합니다**

.

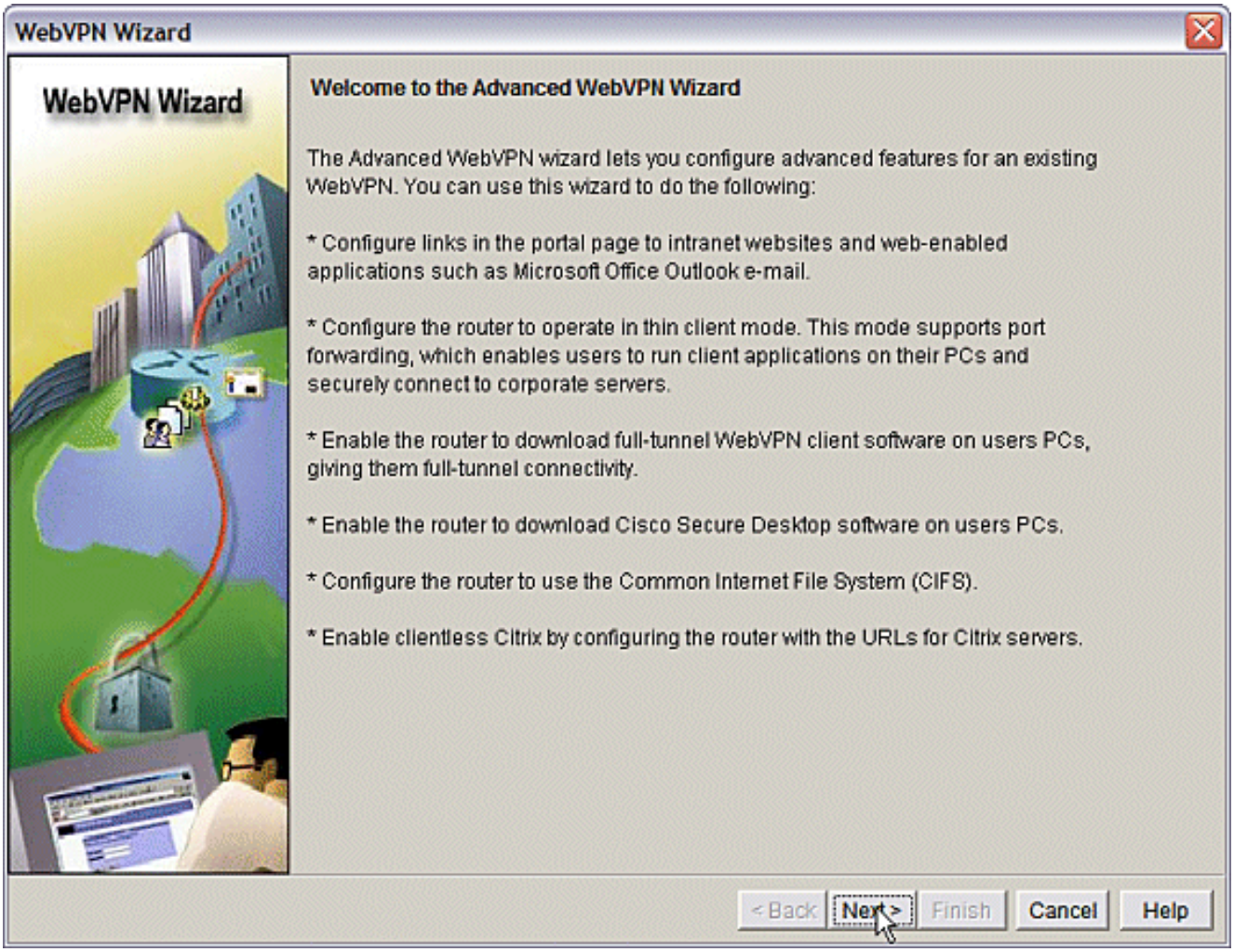


5. 연결된 그룹 정책으로 WebVPN 게이트웨이 및 WebVPN 컨텍스트를 생성했습니다. 클라이언트가 WebVPN에 연결할 때 사용할 수 있는 씬 클라이언트 포트를 구성합니다.구성을 **선택합니다**.VPN **> WebVPN을 선택합니다**.Create **WebVPN(WebVPN 생성)을 선택합니다**.**기존** WebVPN에 **대한 고급 기능 구성** 라디오 버튼을 선택하고 **선택한 작업 시작을 클릭합니다**
.



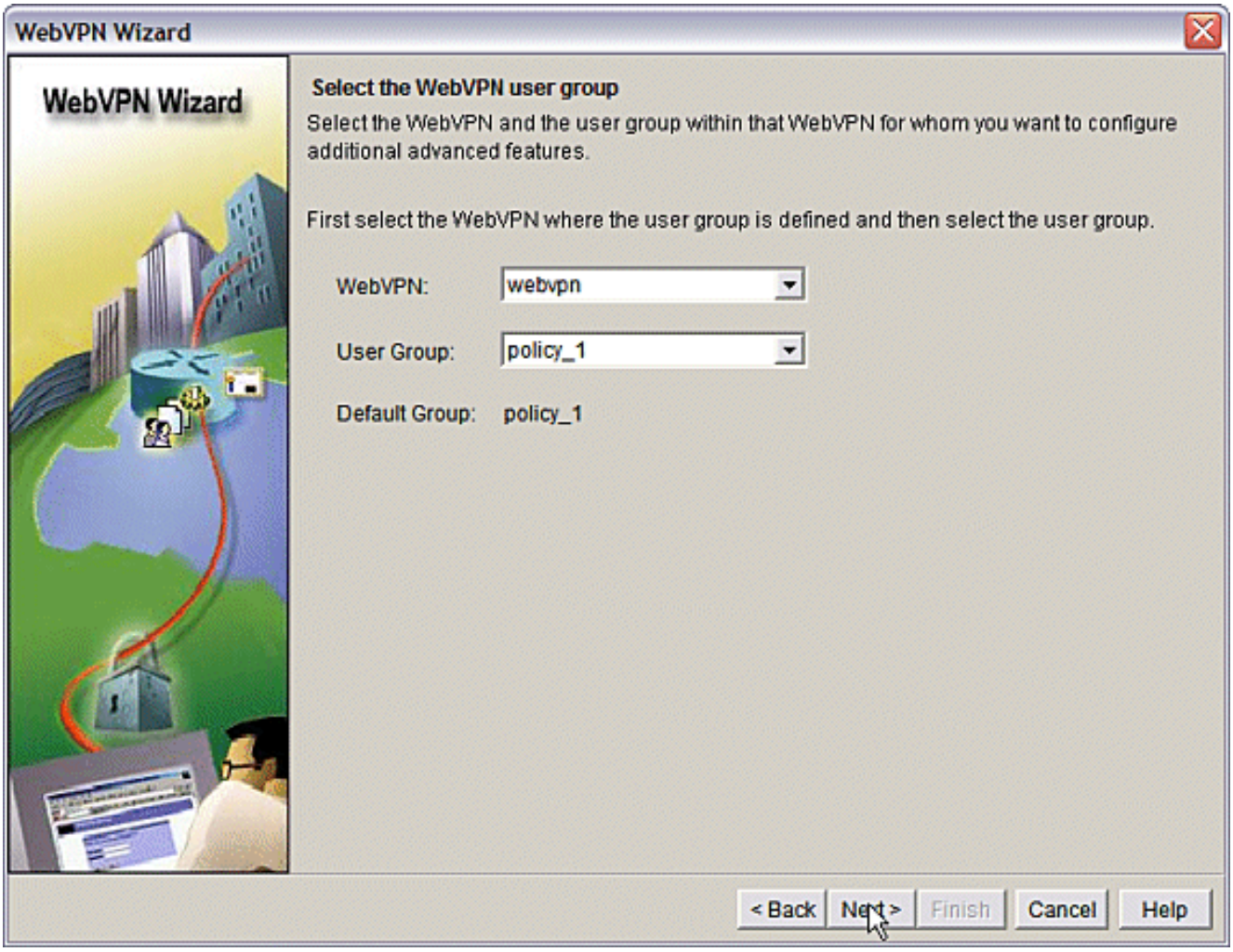
시작 화면에는 마법사의 기능이 강조 표시됩니다. Next(**다음)를 클릭합니다**

.



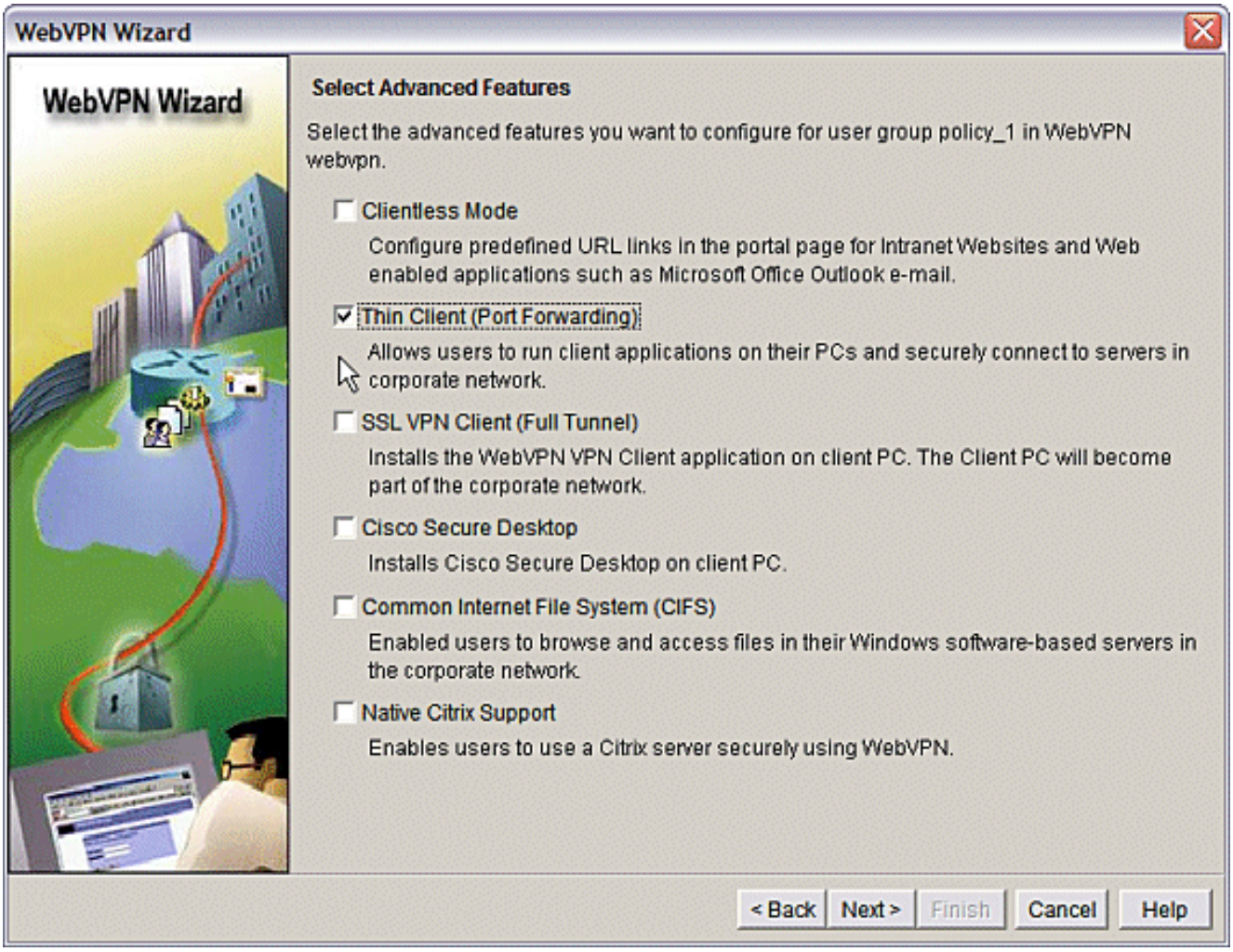
드롭다운 메뉴에서 WebVPN 컨텍스트 및 사용자 그룹을 선택합니다. Next(**다음)를 클릭합니다**

.



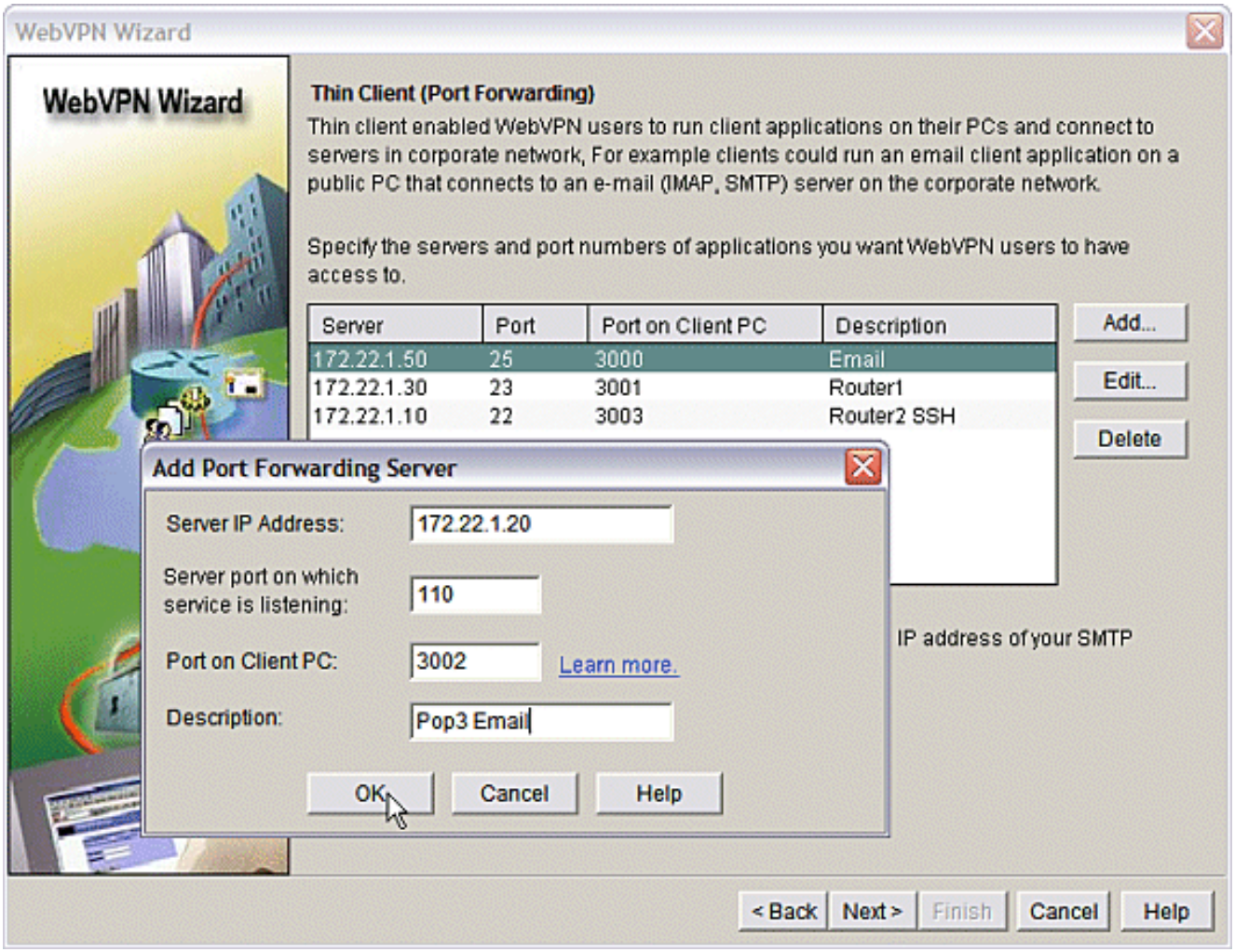
Thin **Client (Port Forwarding)**를 선택하고 **Next**를 클릭합니다

.



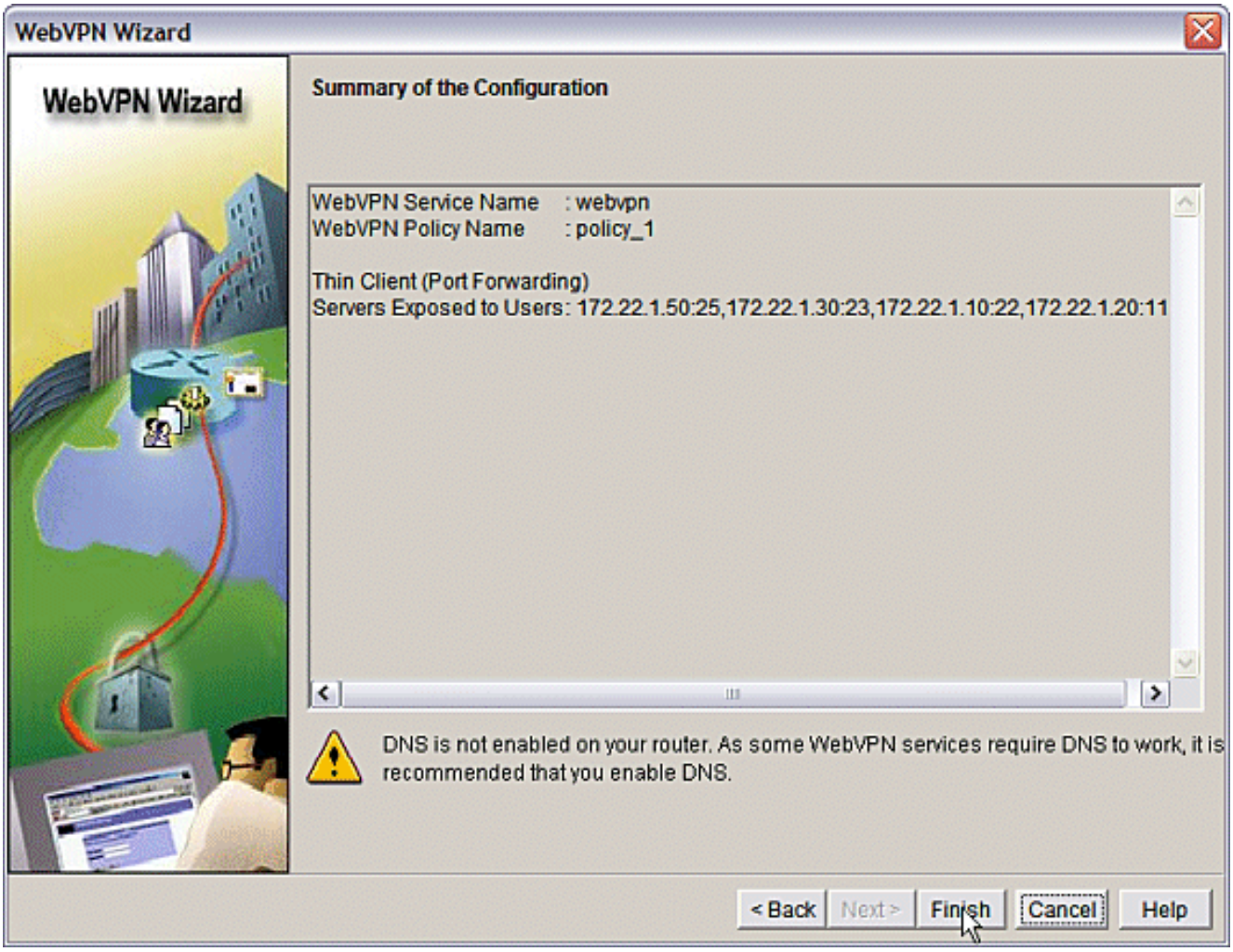
Port Forwarding(포트 전달)을 통해 사용할 리소스를 입력합니다. 서비스 포트는 고정 포트여야 하지만 마법사에서 할당한 클라이언트 PC의 기본 포트를 사용할 수 있습니다. Next(**다음**)**를 클릭합니다**

.



구성 요약을 미리 보고 Finish(마침) **> OK(확인) > Save(저장)를 클릭합니다**

.



구성

SDM 구성 결과.

ausnml-3825-01

```
Building configuration...

Current configuration : 4343 bytes
!
! Last configuration change at 15:55:38 UTC Thu Jul 27
2006 by ausnml
! NVRAM config last updated at 21:30:03 UTC Wed Jul 26
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
enable secret 5 $1$KbIu$5o8qKYAVpWvyv9rYbrJLi/
```

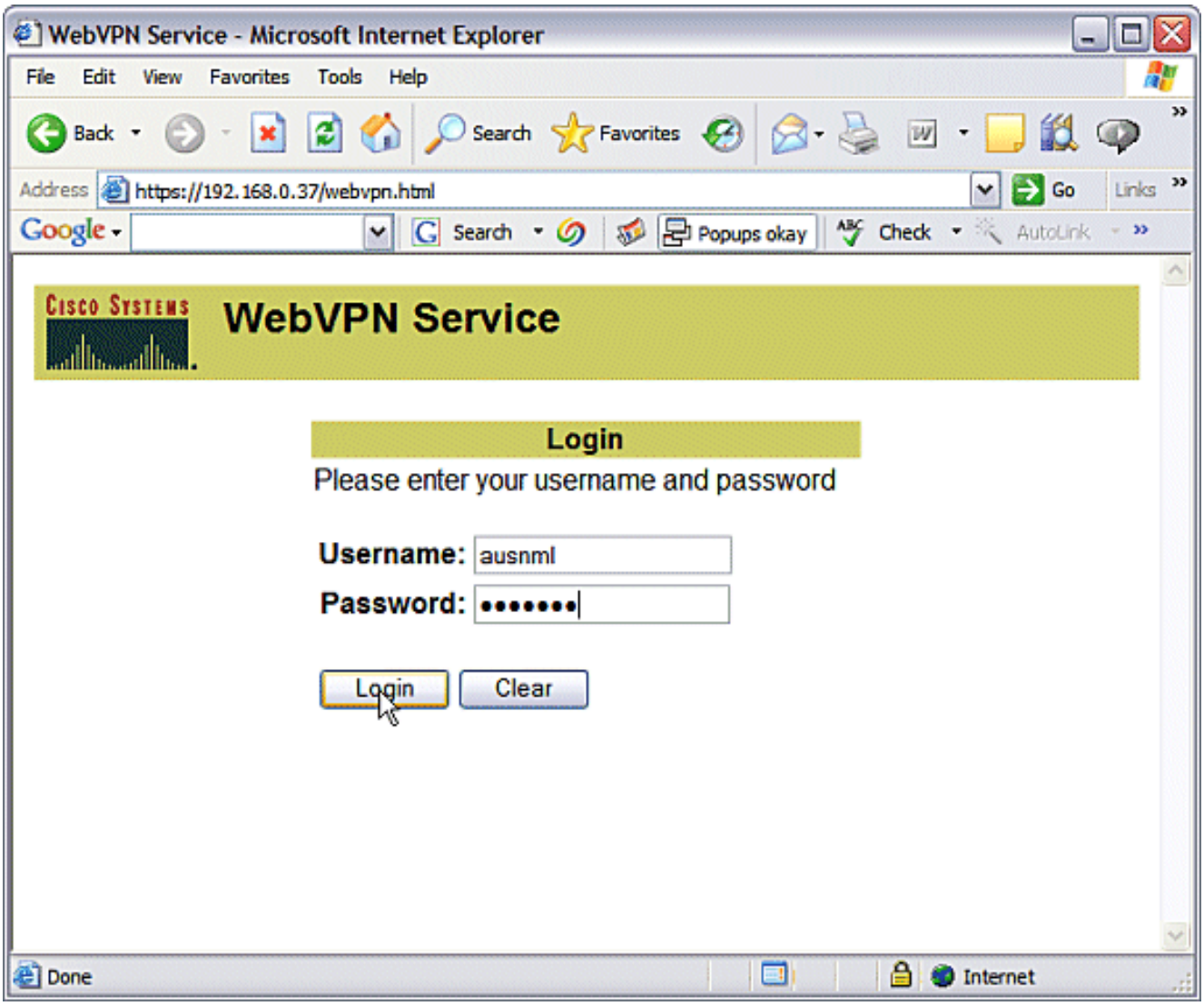
```
!
aaa new-model
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authentication login sdm_vpn_xauth_ml_2 local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
 no dspfarm
!--- Self-Signed Certificate Information crypto pki
trustpoint ausnml-3825-01_Certificate enrollment
selfsigned serial-number none ip-address none
revocation-check crl rsakeypair ausnml-3825-
01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
F70D0101 04050030 !---------------------- !--- cut for
brevity quit ! username ausnml privilege 15 password 7
15071F5A5D292421 username fallback privilege 15 password
7 08345818501A0A12 username austin privilege 15 secret 5
$1$3xFv$W0YUsKDx1adDc.cVQF2Ei0 username sales_user1
privilege 5 secret 5 $1$2/SX$ep4fsCpodeyKaRji2mJkX/
username admin0321 privilege 15 secret 5
$1$FxzG$cQUJeUpBWgZ.scSzOt8Ro1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
duplex auto speed auto media-type rj45 ! 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 exec-timeout 40 0 privilege
level 15 password 7 071A351A170A1600 transport input
telnet ssh line vty 5 15 exec-timeout 40 0 password 7
001107505D580403 transport input telnet ssh ! scheduler
allocate 20000 1000 !--- the WebVPN Gateway webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint ausnml-3825-
01_Certificate inservice !--- the WebVPN Context webvpn
context webvpn title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all !---
resources available to the thin-client port-forward
"portforward_list_1" local-port 3002 remote-server
"172.22.1.20" remote-port 110 description "Pop3 Email"
local-port 3001 remote-server "172.22.1.30" remote-port
23 description "Router1" local-port 3000 remote-server
"172.22.1.50" remote-port 25 description "Email" local-
port 3003 remote-server "172.22.1.10" remote-port 22
description "Router2 SSH" !--- the group policy policy
group policy_1 port-forward "portforward_list_1"
default-group-policy policy_1 aaa authentication list
sdm_vpn_xauth_ml_2 gateway gateway_1 domain webvpn max-
users 2 inservice ! end
```

다음을 확인합니다.

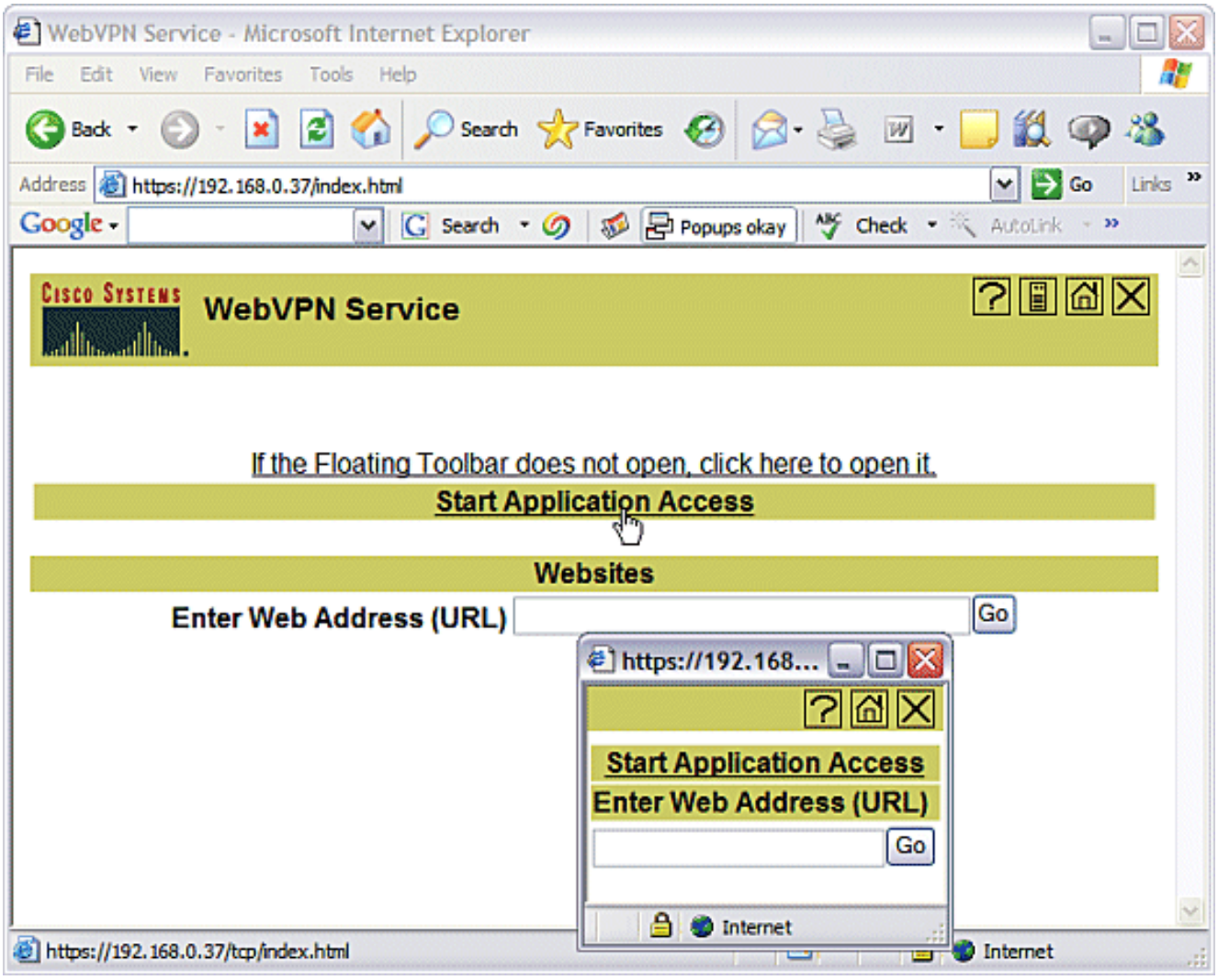
구성 확인

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

1. 클라이언트 컴퓨터를 사용하여 https://gateway_ip_address에서 WebVPN 게이트웨이에 **액세스합니다.** 고유한 WebVPN 컨텍스트를 만들 경우 WebVPN 도메인 이름을 포함해야 합니다. 예를 들어 sales라는 도메인을 생성한 경우 https://gateway_ip_address/sales을 **입력합니다**
.

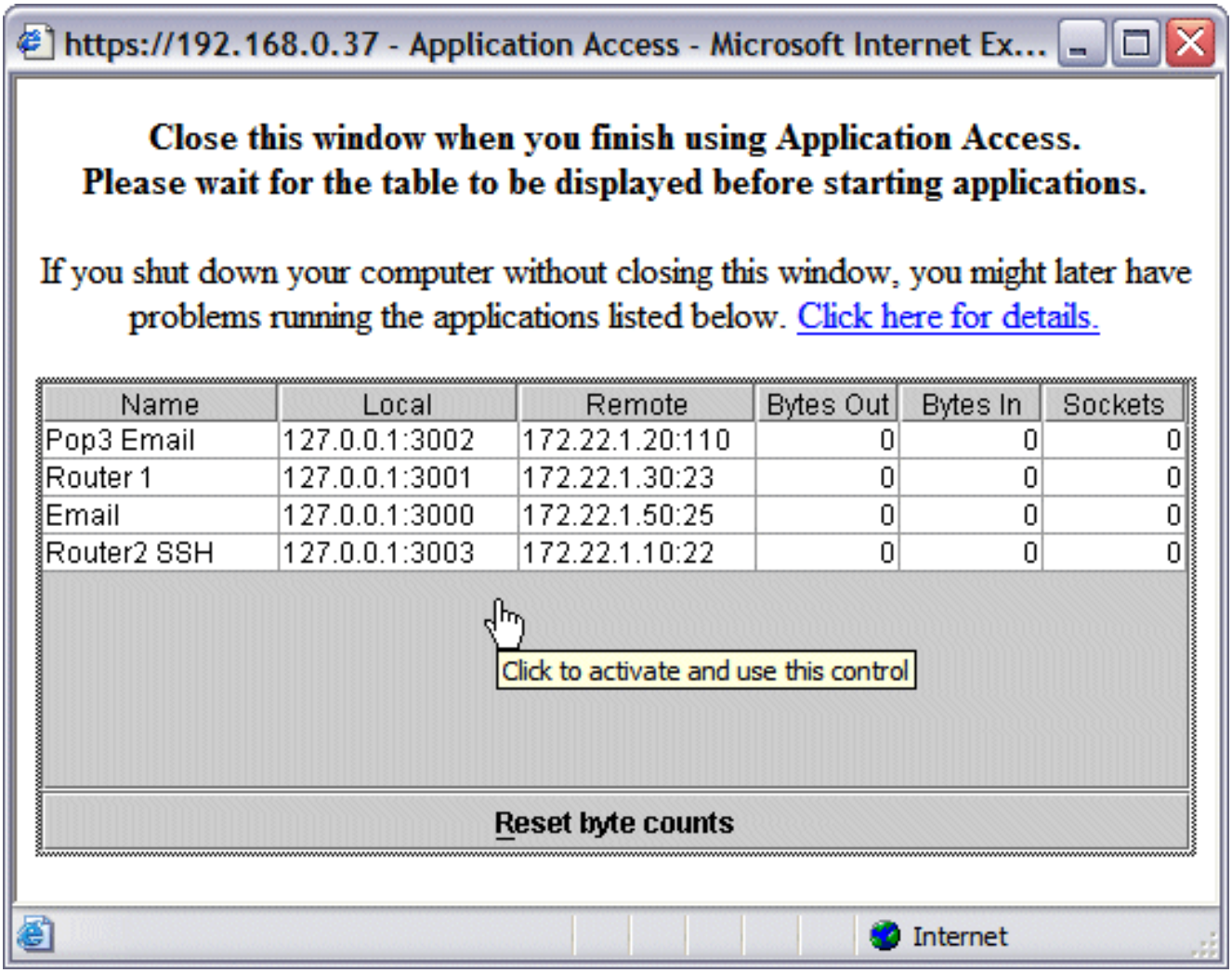


2. WebVPN 게이트웨이가 제공하는 인증서를 로그인하여 수락합니다. 애플리케이션 **액세스 시작을 클릭합니다**
.



3. 애플리케이션 액세스 화면이 표시됩니다. 로컬 포트 번호와 로컬 루프백 IP 주소를 사용하여 애플리케이션에 액세스할 수 있습니다. 예를 들어 텔넷을 통해 라우터 1에 연결하려면 **telnet 127.0.0.1 3001을 입력합니다**. 작은 Java 애플릿은 이 정보를 WebVPN 게이트웨이로 전송하고, 이 경우 세션의 두 끝을 안전한 방식으로 연결합니다. 연결에 성공하면 **바이트 출력** 및 **바이트** 열이 증가할 수 있습니다

.



명령

여러 **show** 명령이 WebVPN과 연결되어 있습니다. CLI(Command Line Interface)에서 이러한 명령을 실행하여 통계 및 기타 정보를 표시할 수 있습니다. **show 명령**의 사용을 자세히 보려면 WebVPN 구성 확인을 참조하십시오.

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

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

클라이언트 컴퓨터는 SUN Java 버전 1.4 이상에서 로드되어야 합니다. Java 소프트웨어 다운로드에서 이 소프트웨어의 복사본 받기

문제 해결에 사용되는 명령

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **show webvpn ?**—WebVPN과 관련된 **show** 명령이 많습니다. 이러한 작업은 CLI에서 수행하여 통계 및 기타 정보를 표시할 수 있습니다. **show** 명령의 사용을 자세히 보려면 WebVPN 구성 확인 을 참조하십시오.

- **debug webvpn ?**—debug 명령을 사용하면 라우터에 부정적인 영향을 미칠 수 있습니다. debug 명령의 사용을 자세히 보려면 WebVPN 디버그 명령 사용을 참조하십시오.

관련 정보

- Cisco IOS SSLVPN
- SSL VPN - WebVPN
- Cisco IOS WebVPN Q&A
- 기술 지원 및 문서 – Cisco Systems