ASA with ASDM 컨피그레이션 예시 ASA의 씬 클라이언트 SSL VPN(WebVPN)

목차

소개

씬 클라이언트 SSL VPN 기술을 사용하면 Telnet(23), SSH(22), POP3(110), IMAP4(143) 및 SMTP(25)와 같은 정적 포트가 있는 일부 애플리케이션에 대해 보안 액세스를 허용합니다. 씬 클라이언트 SSL VPN을 사용자 기반 애플리케이션, 정책 기반 애플리케이션 또는 둘 다로 사용할 수 있습니다.즉, 사용자별로 액세스를 구성하거나 하나 이상의 사용자를 추가하는 그룹 정책을 생성할 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 브라우징에 대한 액세스를 제공합니다.OWA(Outlook Web Access)는 HTTP 액세스의 예입니다.클라이언트리스 SSL VPN에 대한 자세한 내용은 ASA 컨피그레이션 예의 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.보안 액세스의 예로는 POP3(Post Office Protocol), SMTP(Simple Mail Transfer Protocol), IMAP(Internet Message Access Protocol), SSH(Secure Shell) 및 텔넷이 있습니다.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.**참고:** UDP(User Datagram Protocol)는 지원되지 않습니다.
- **SSL VPN Client(Tunnel Mode)(SSL VPN 클라이언트(터널 모드))** - 소규모 클라이언트를 원격 워크스테이션에 다운로드하고 내부 기업 네트워크의 리소스에 대한 완전한 보안 액세스를 허용합니다.원격 워크스테이션에 SSL VPN 클라이언트(SVC)를 영구적으로 다운로드하거나 보안 세션이 닫히면 클라이언트를 제거할 수 있습니다.SSL VPN 클라이언트에 대한 자세한 내용은 ASA with ASDM Configuration Example(ASA with ASDM Configuration Example)의 SSL VPN Client(SVC)를 참조하십시오.

이 문서에서는 ASA(Adaptive Security Appliance)의 씬 클라이언트 SSL VPN에 대한 간단한 컨피그레이션을 보여 줍니다. 컨피그레이션을 사용하면 사용자가 ASA 내부에 있는 라우터에 안전하게 텔넷할 수 있습니다.이 문서의 컨피그레이션은 ASA 버전 7.x 이상에서 지원됩니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 원격 클라이언트 스테이션에 대한 다음 요구 사항을 충족해야 합니다.

- SSL 지원 웹 브라우저
- SUN Java JRE 버전 1.4 이상
- 쿠키 사용
- 팝업 차단 사용 안 함
- 로컬 관리 권한(필수는 아니지만 강력하게 제안)

참고: 최신 버전의 SUN Java JRE는 Java 웹 사이트에서 무료로 다운로드할 수 있습니다 .

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

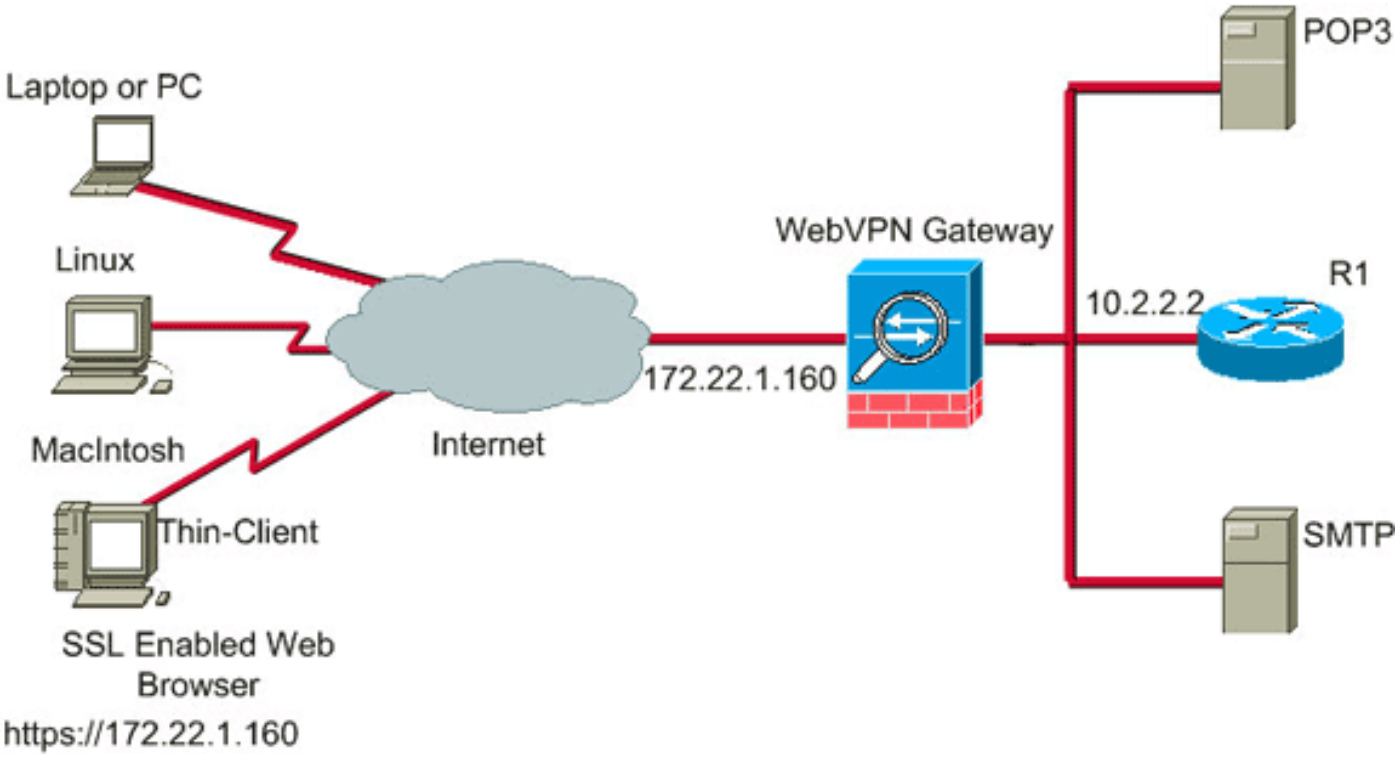
- Cisco Adaptive Security Appliance 5510 시리즈
- Cisco ASDM(Adaptive Security Device Manager) 5.2(1)**참고:** ASDM에서 ASA를 구성할 수 있도록 허용하려면 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.
- Cisco Adaptive Security Appliance Software 버전 7.2(1)
- Microsoft Windows XP Professional(SP 2) 원격 클라이언트

이 문서의 정보는 랩 환경에서 개발되었습니다.이 문서에 사용된 모든 장치가 기본 구성으로 재설정되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.이 구성에 사용된 모든 IP 주소는 랩 환경의 RFC 1918 주소에서 선택되었습니다.이러한 IP 주소는 인터넷에서 라우팅할 수 없으며 테스트 용도로만 사용됩니다.

네트워크 다이어그램

이 문서에서는 이 섹션에 설명된 네트워크 구성을 사용합니다.

원격 클라이언트가 ASA로 세션을 시작하면 클라이언트는 작은 Java 애플릿을 워크스테이션으로 다운로드합니다.클라이언트에는 사전 구성된 리소스 목록이 표시됩니다.



표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

배경 정보

세션을 시작하려면 원격 클라이언트가 ASA의 외부 인터페이스에 대한 SSL 브라우저를 엽니다.세션이 설정되면 사용자는 ASA에 구성된 매개변수를 사용하여 텔넷 또는 애플리케이션 액세스를 호출할 수 있습니다.ASA는 보안 연결을 프록시하고 사용자가 디바이스에 액세스할 수 있도록 합니다.

참고: ASA가 법적 세션의 구성 요소를 이미 알고 있으므로 인바운드 액세스 목록은 이러한 연결에 필요하지 않습니다.

ASDM을 사용한 씬 클라이언트 SSL VPN 구성

ASA에서 씬 클라이언트 SSL VPN을 구성하려면 다음 단계를 완료하십시오.

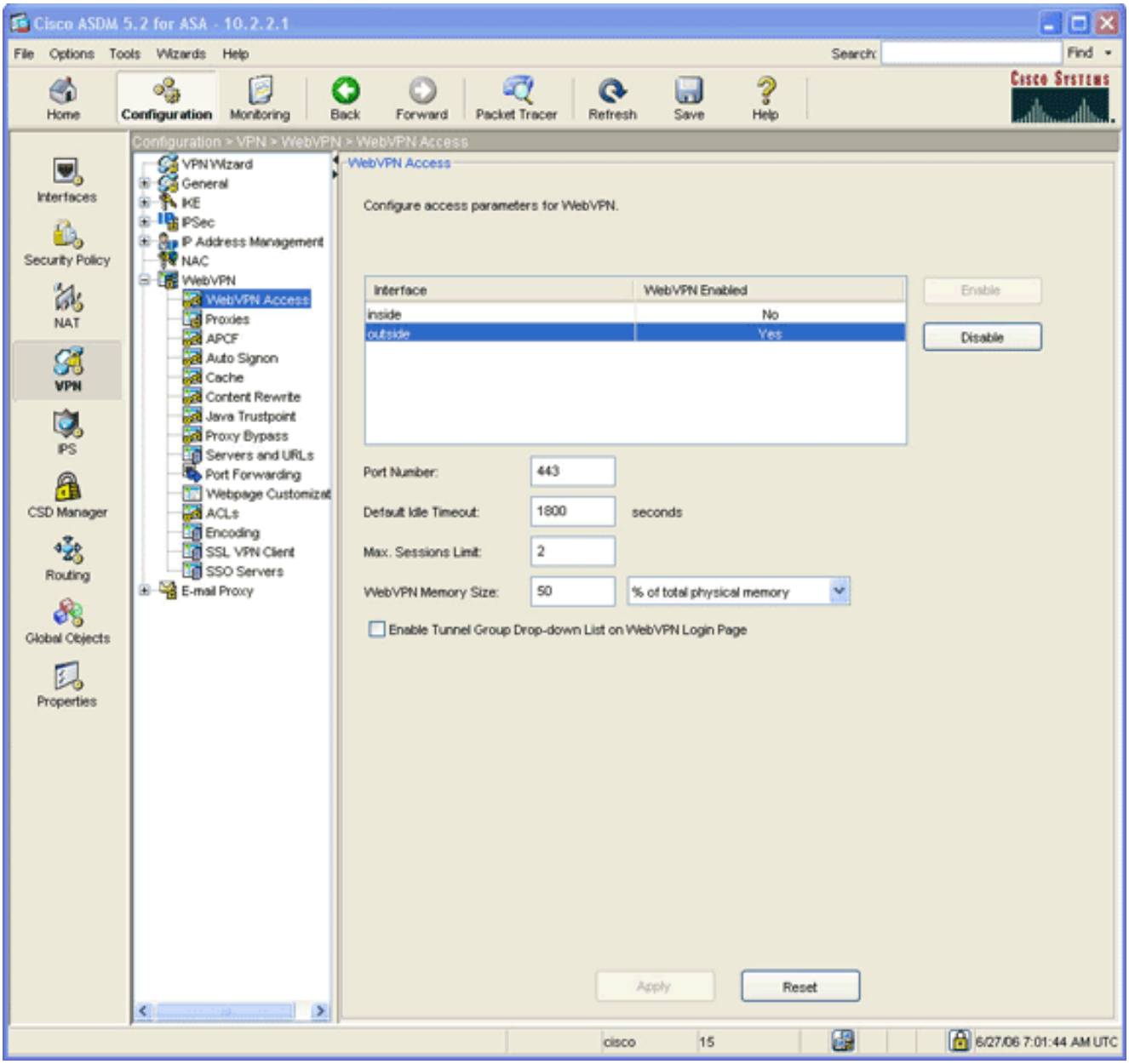
1. ASA에서 WebVPN 활성화
2. 포트 전달 특성 구성
3. 그룹 정책을 생성하고 포트 전달 목록(2단계에서 생성)에 연결
4. 터널 그룹을 생성하고 그룹 정책에 연결(3단계에서 생성)
5. 사용자를 생성하고 그룹 정책에 해당 사용자 추가(3단계에서 생성)

1단계. ASA에서 WebVPN을 활성화합니다.

ASA에서 WebVPN을 활성화하려면 다음 단계를 완료하십시오.

1. ASDM 애플리케이션 내에서 Configuration(컨피그레이션)을 클릭한 다음 **VPN**을 클릭합니다.
2. WebVPN을 확장하고 WebVPN **Access를 선택합니다**

.



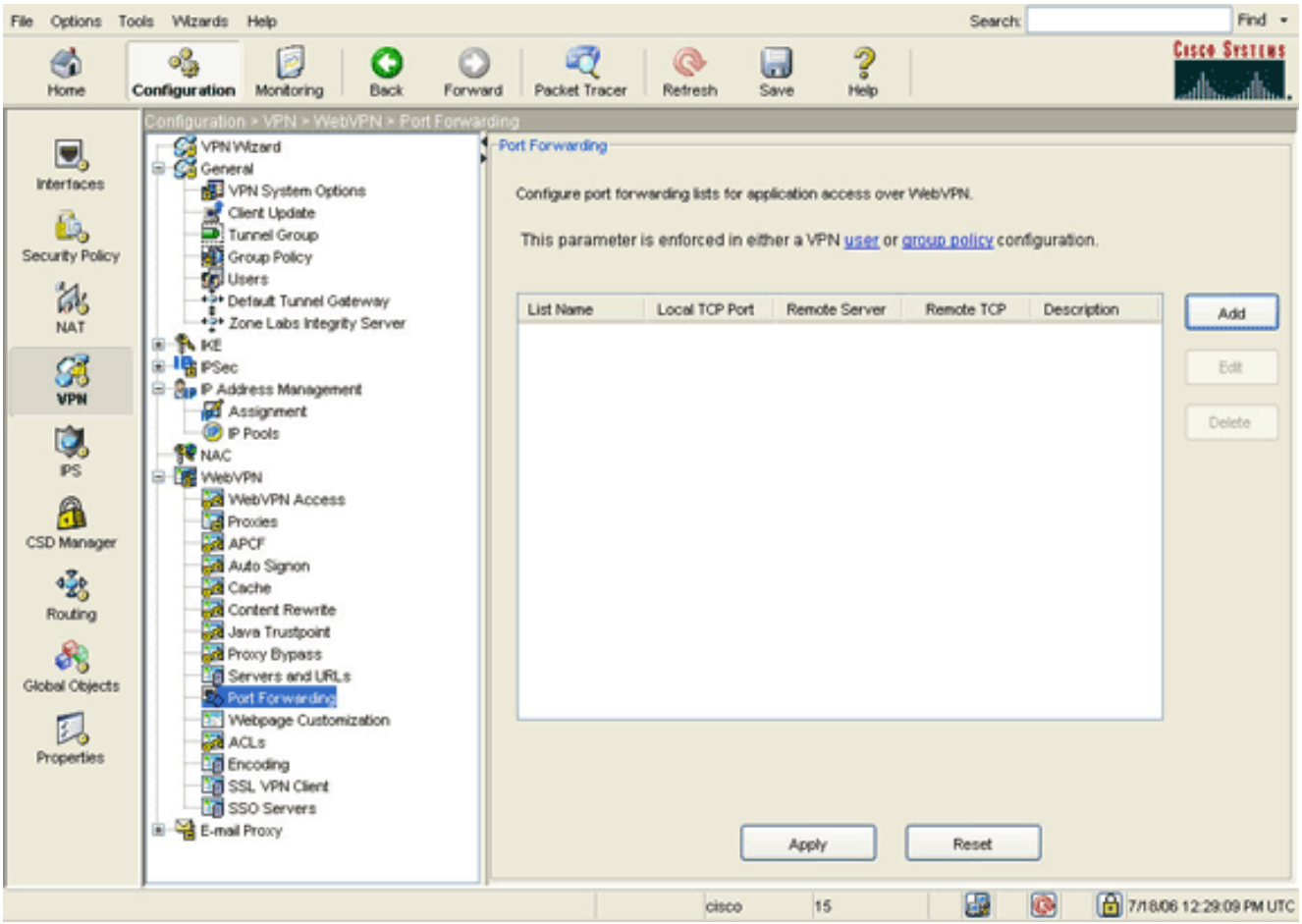
3. 인터페이스를 강조 표시하고 Enable을 **클릭합니다**.
4. Apply(**적용**)를 클릭하고 **Save(저장)**를 클릭한 다음 **Yes(예)**를 클릭하여 변경 사항을 적용합니다.

2단계. 포트 전달 특성 구성

포트 전달 특성을 구성하려면 다음 단계를 완료하십시오.

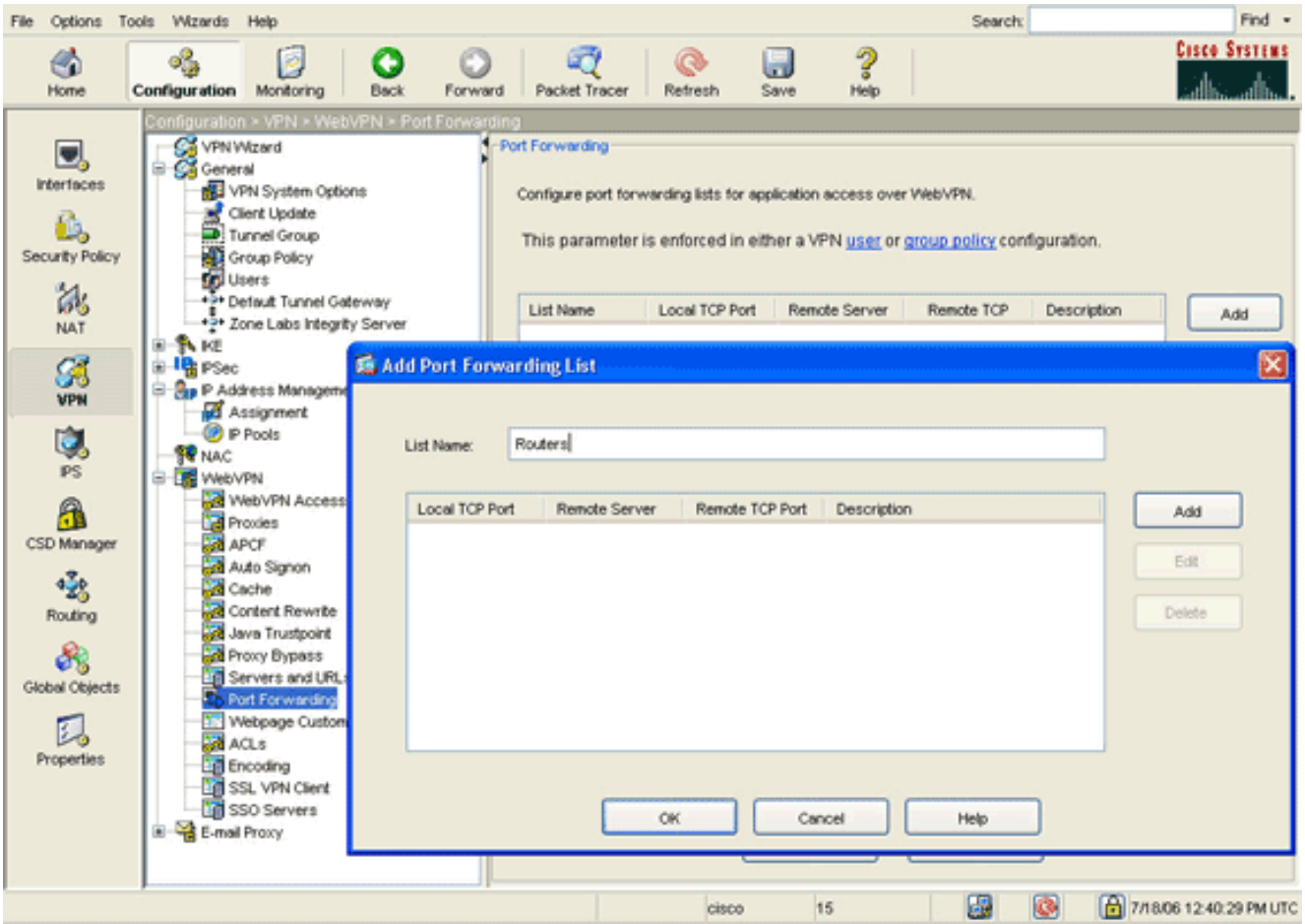
1. WebVPN을 확장하고 Port **Forwarding을** 선택합니다

.



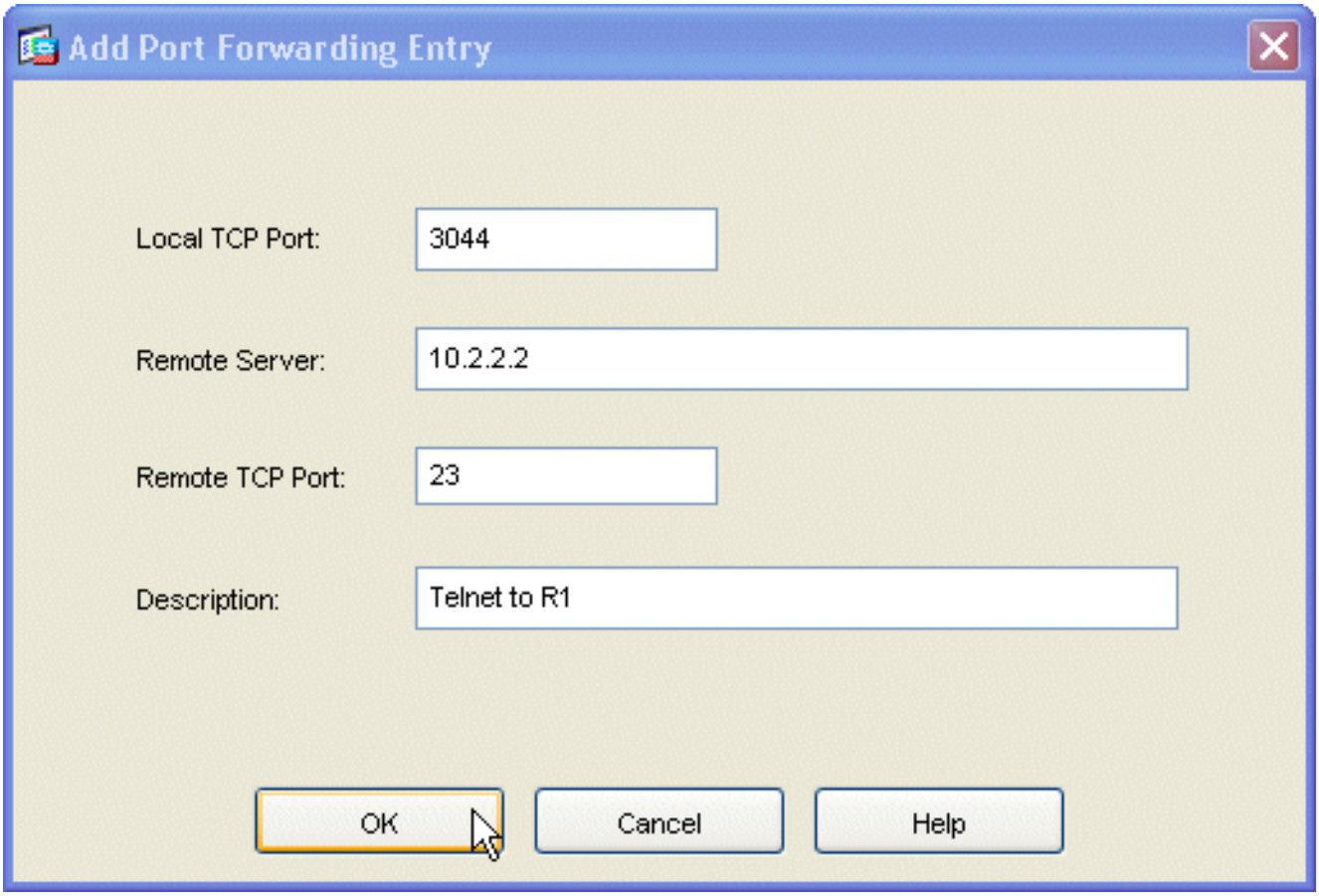
2. **Add** 버튼을 클릭합니다

.



3. Add Port Forwarding List(포트 전달 목록 추가) 대화 상자에서 목록 이름을 입력하고 Add(추가)를 **클릭합니다**.Add Port Forwarding Entry 대화 상자가 나타납니다

.

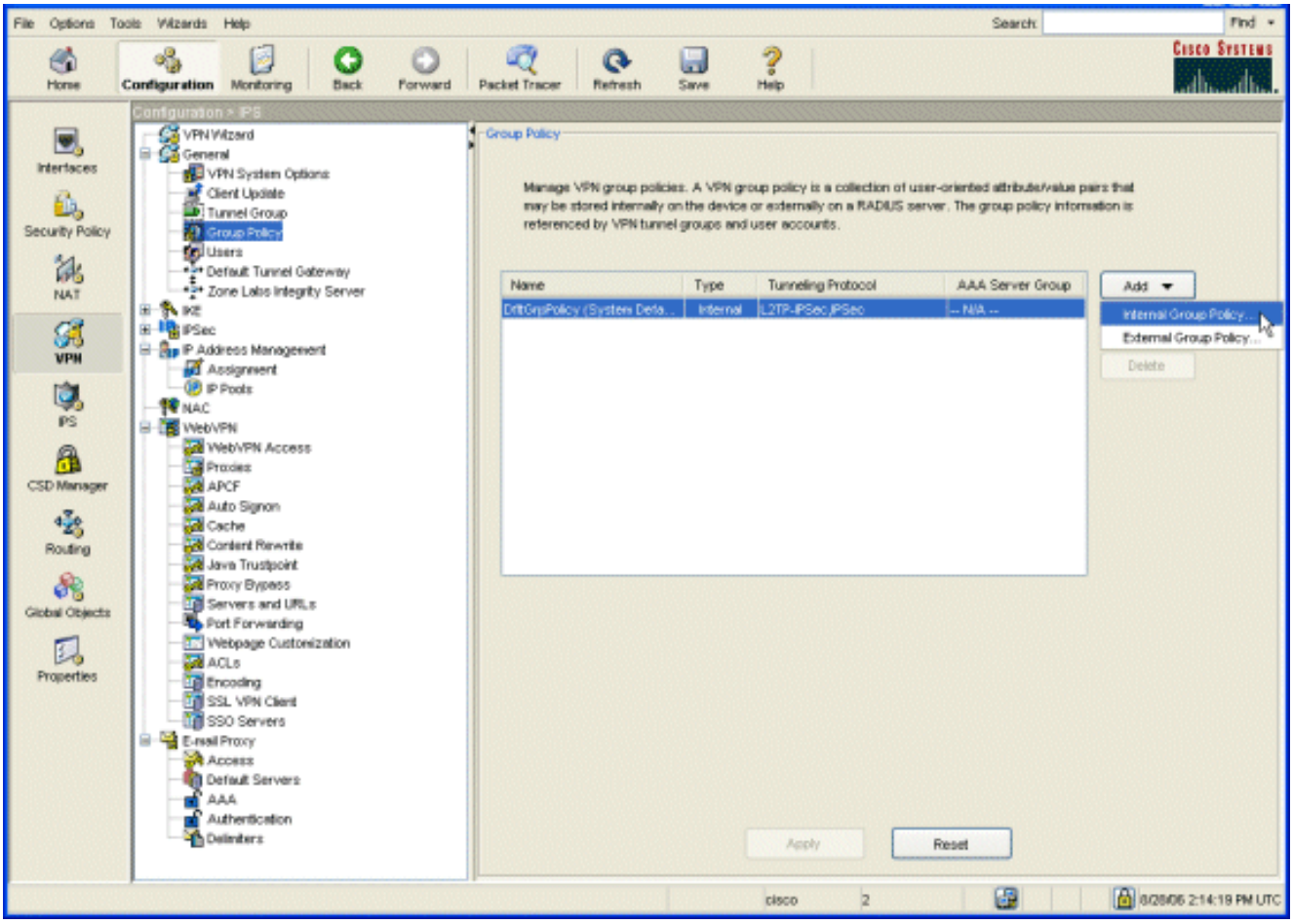


4. Add Port Forwarding Entry(포트 전달 항목 추가) 대화 상자에서 다음 옵션을 입력합니다 .Local TCP Port 필드에 포트 번호를 입력하거나 기본값을 적용합니다.입력하는 값은 1024~65535의 숫자일 수 있습니다.Remote Server(원격 서버) 필드에 IP 주소를 입력합니다 .이 예에서는 라우터의 주소를 사용합니다.Remote TCP Port 필드에 포트 번호를 입력합니다 .이 예에서는 포트 23을 사용합니다.Description 필드에 설명을 입력하고 **확인**을 클릭합니다.
5. OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**.
6. Save(**저장**)를 클릭한 다음 **Yes(예)**를 클릭하여 변경 사항을 적용합니다.

3단계. 그룹 정책을 생성하고 포트 전달 목록에 연결

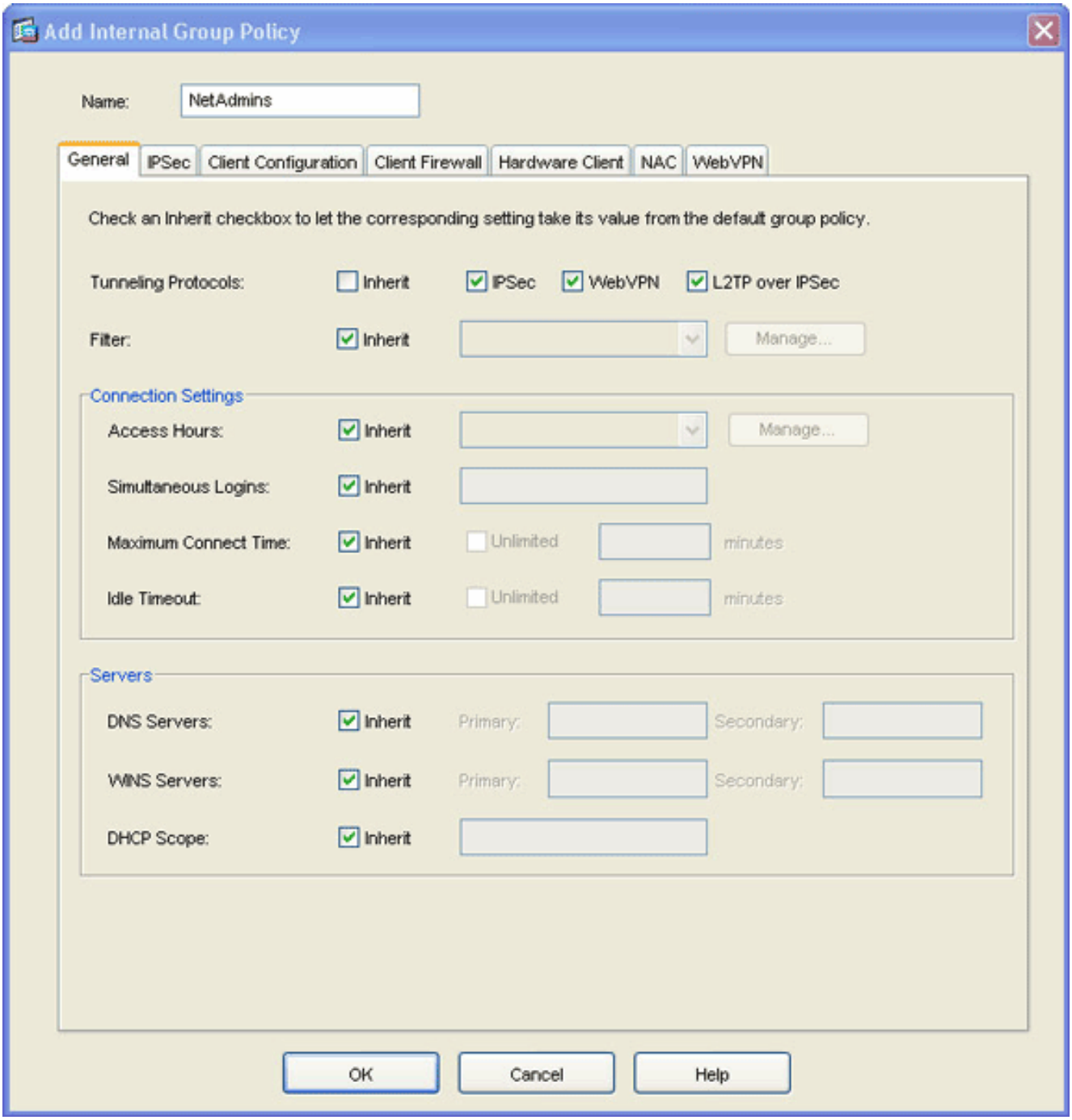
그룹 정책을 생성하고 포트 전달 목록에 연결하려면 다음 단계를 완료합니다.

1. General(**일반**)을 확장하고 **Group Policy(그룹 정책)를** 선택합니다
.



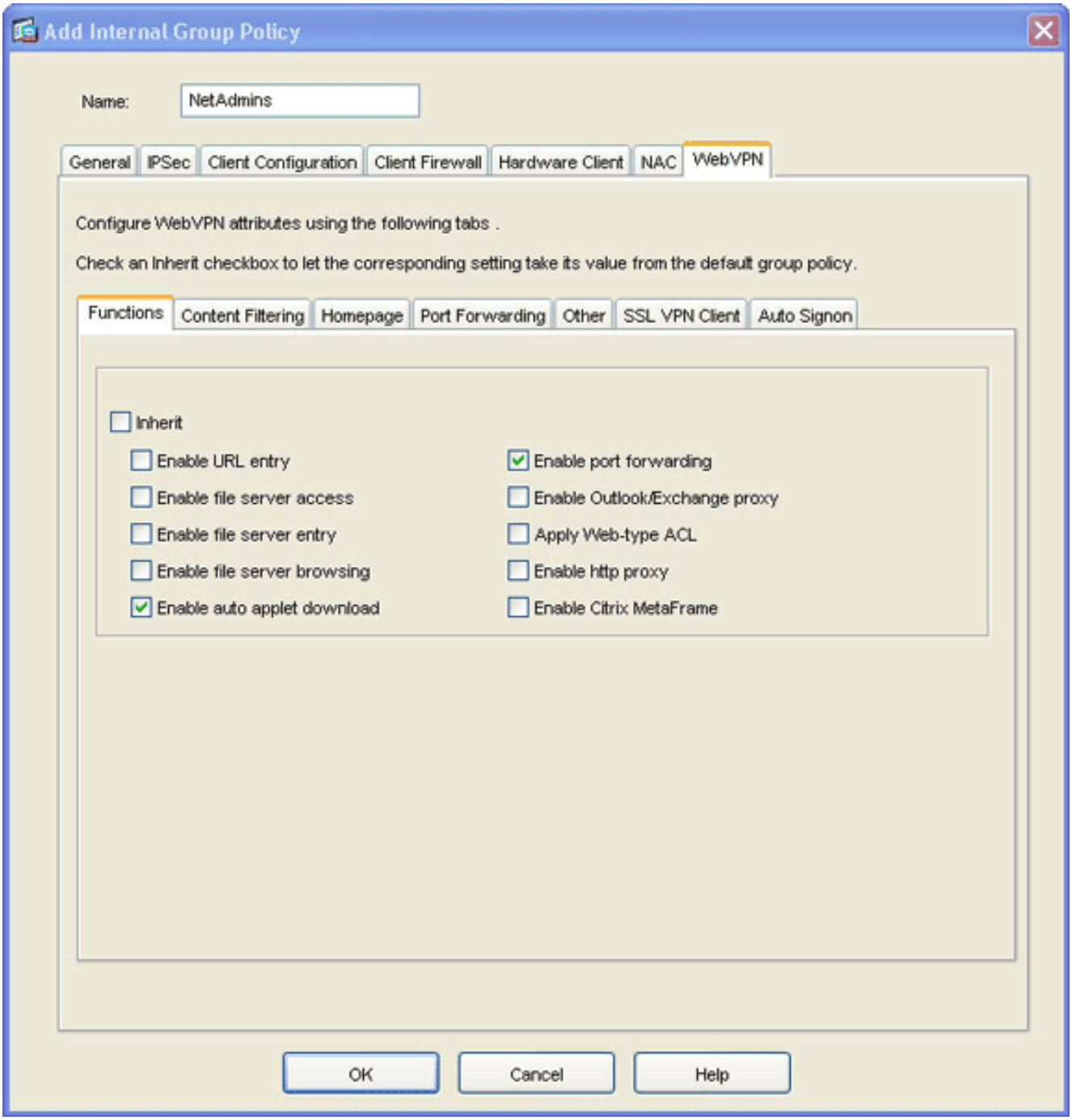
2. Add(**추가**)를 클릭하고 **Internal Group Policy(내부 그룹 정책)**를 선택합니다.Add Internal Group Policy 대화 상자가 나타납니다

.

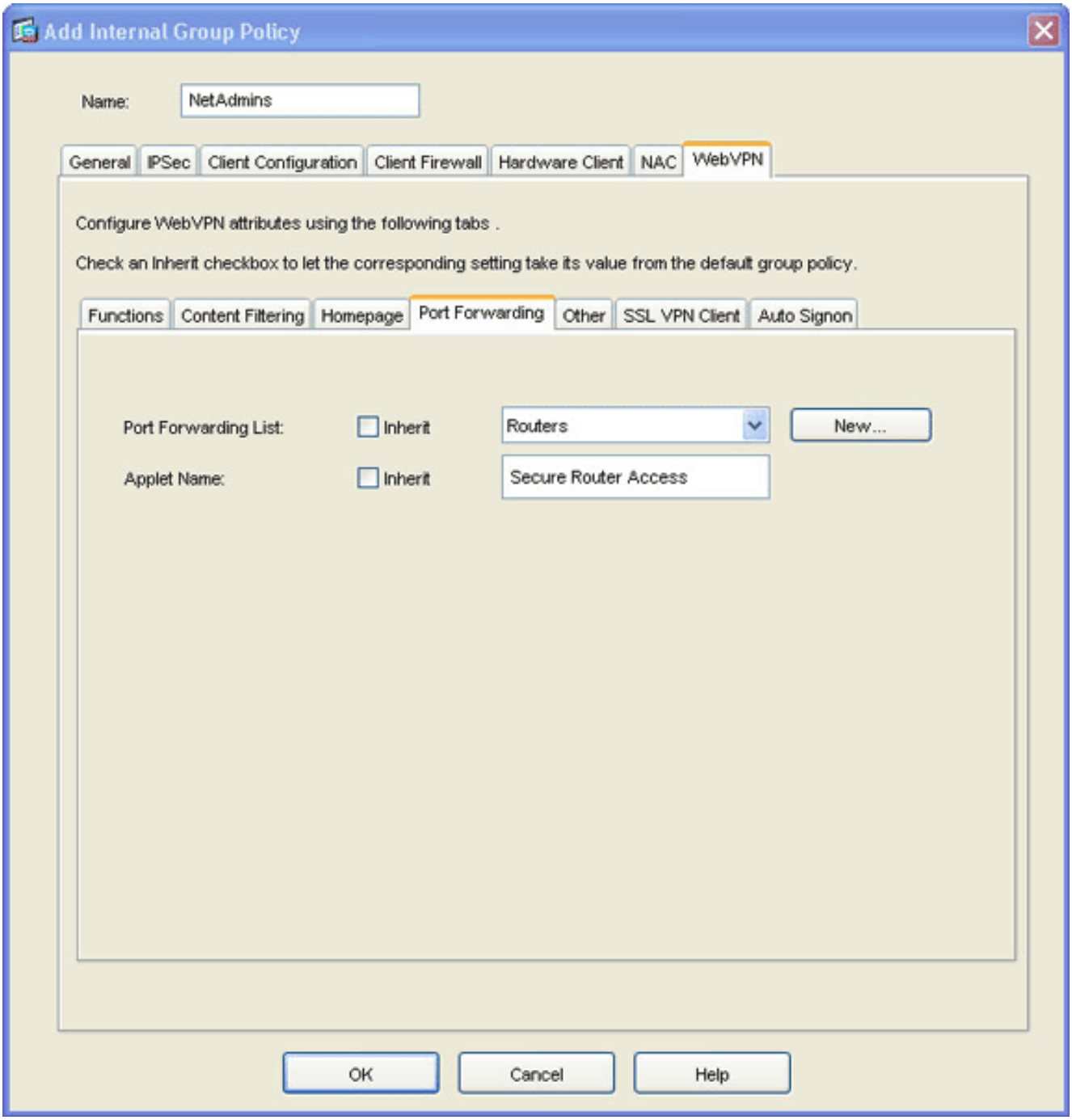


3. 이름을 입력하거나 기본 그룹 정책 이름을 적용합니다.
4. Tunneling Protocols Inherit(터널링 프로토콜 **상속**) 확인란의 선택을 취소하고 WebVPN **확인란을** 선택합니다.
5. 대화 상자 맨 위에 있는 **WebVPN** 탭을 클릭한 다음 **Functions** 탭을 클릭합니다.
6. Inherit(**상속**) 확인란의 선택을 취소하고 다음 이미지에 표시된 대로 **Enable auto applet download** and **Enable port forwarding** 확인란을 선택합니다

.



7. 또한 WebVPN 탭에서 **Port Forwarding**(포트 전달) 탭을 클릭하고 Port Forwarding List Inherit(포트 전달 목록 상속) 확인란의 선택을 취소합니다
.



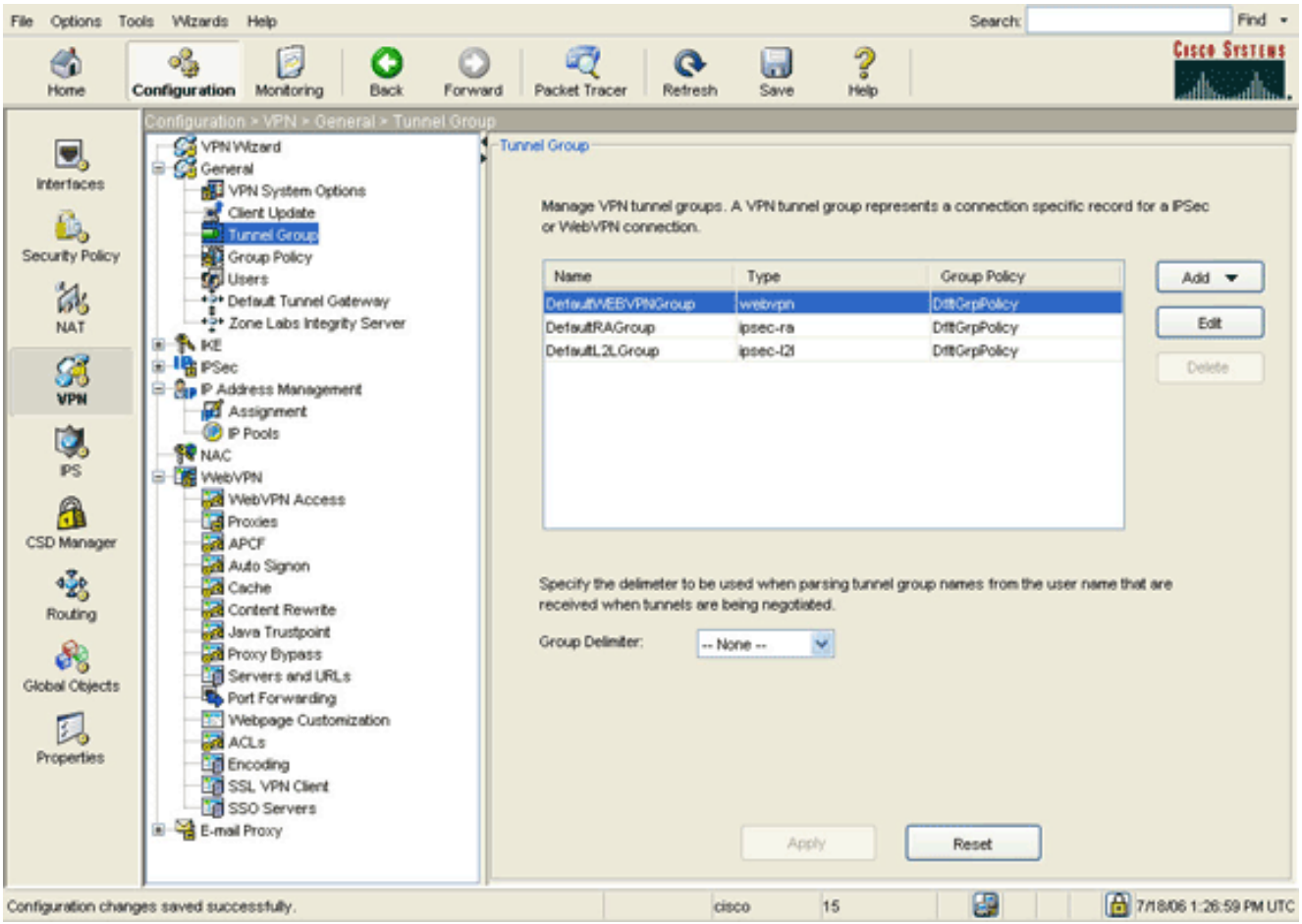
8. **Port Forwarding List** 드롭다운 화살표를 클릭하고 2단계에서 생성한 포트 전달 목록을 선택합니다.
9. Applet Name Inherit(애플릿 이름 **상속**) 확인란의 선택을 취소하고 텍스트 필드에서 이름을 변경합니다.클라이언트는 연결 시 애플릿 이름을 표시합니다.
10. OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**.
11. Save(**저장**)를 클릭한 다음 **Yes(예)**를 클릭하여 변경 사항을 적용합니다.

4단계. 터널 그룹을 생성하고 그룹 정책에 연결

기본 DefaultWebVPNGroup 터널 그룹을 편집하거나 새 터널 그룹을 생성할 수 있습니다.

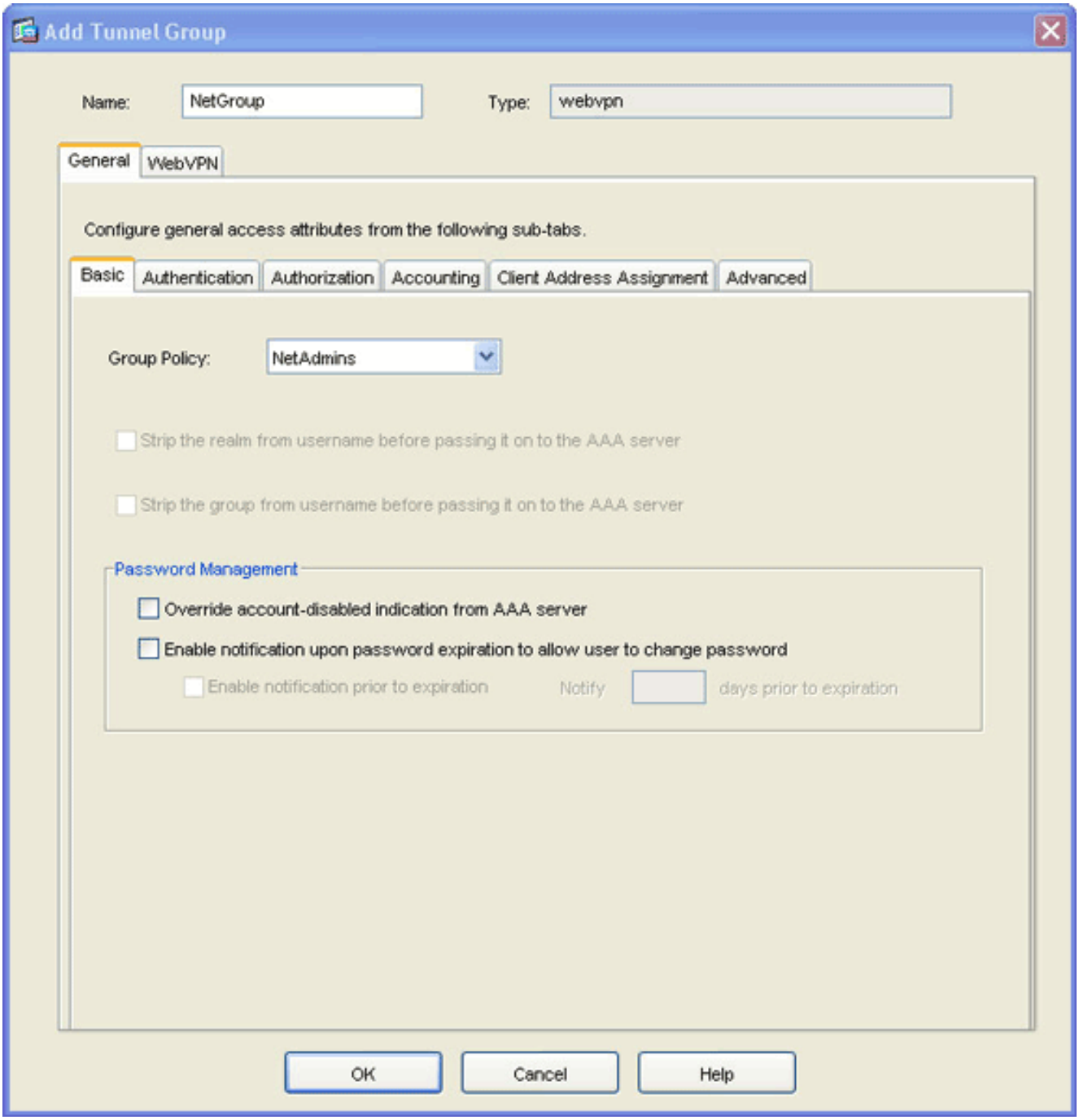
새 터널 그룹을 생성하려면 다음 단계를 완료하십시오.

1. General(**일반**)을 확장하고 **Tunnel Group(터널 그룹)을** 선택합니다
.



2. Add(**추가**)를 클릭하고 WebVPN **Access(WebVPN 액세스)를** 선택합니다.Add Tunnel Group 대화 상자가 나타납니다

.

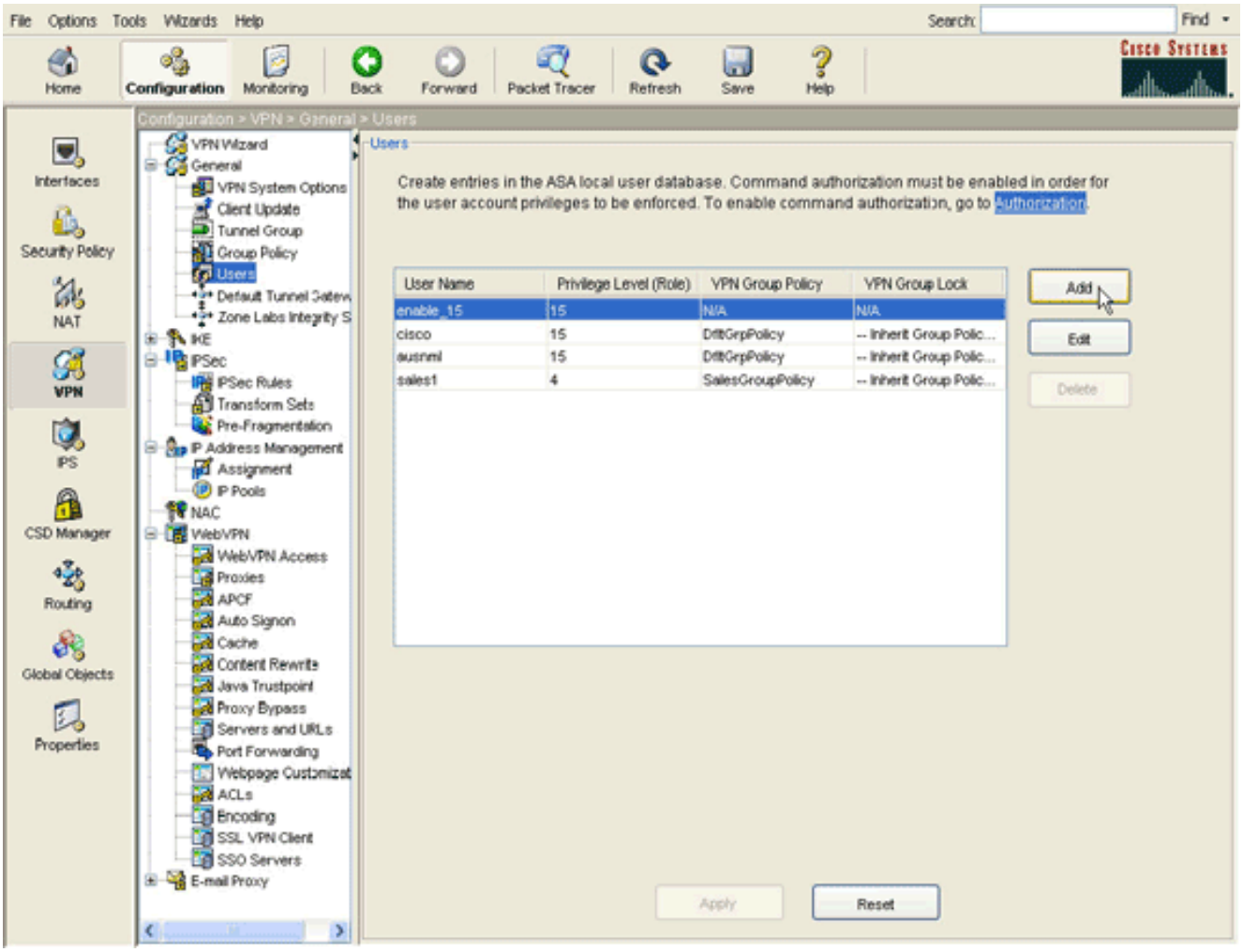


3. 이름 필드에 이름을 입력합니다.
4. **그룹 정책** 드롭다운 화살표를 클릭하고 3단계에서 생성한 그룹 정책을 선택합니다.
5. OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**.
6. Save(**저장**)를 클릭한 다음 **Yes(예)**를 클릭하여 변경 사항을 적용합니다.이제 터널 그룹, 그룹 정책 및 포트 전달 특성이 연결됩니다.

5단계. 사용자를 생성하고 그룹 정책에 해당 사용자를 추가합니다.

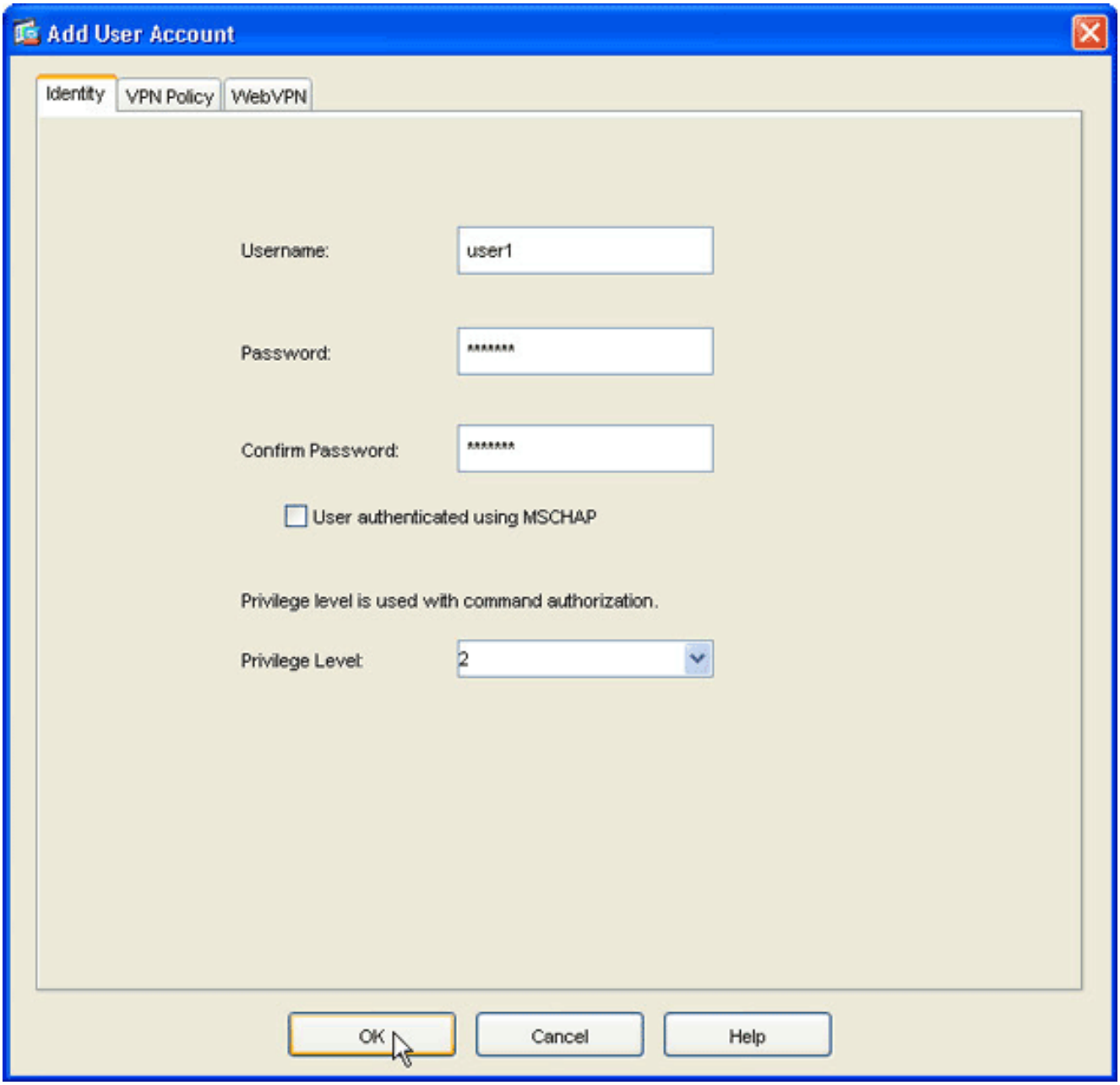
사용자를 생성하고 그룹 정책에 해당 사용자를 추가하려면 다음 단계를 완료합니다.

1. **일반**을 확장하고 **사용자**를 **선택합니다**
.

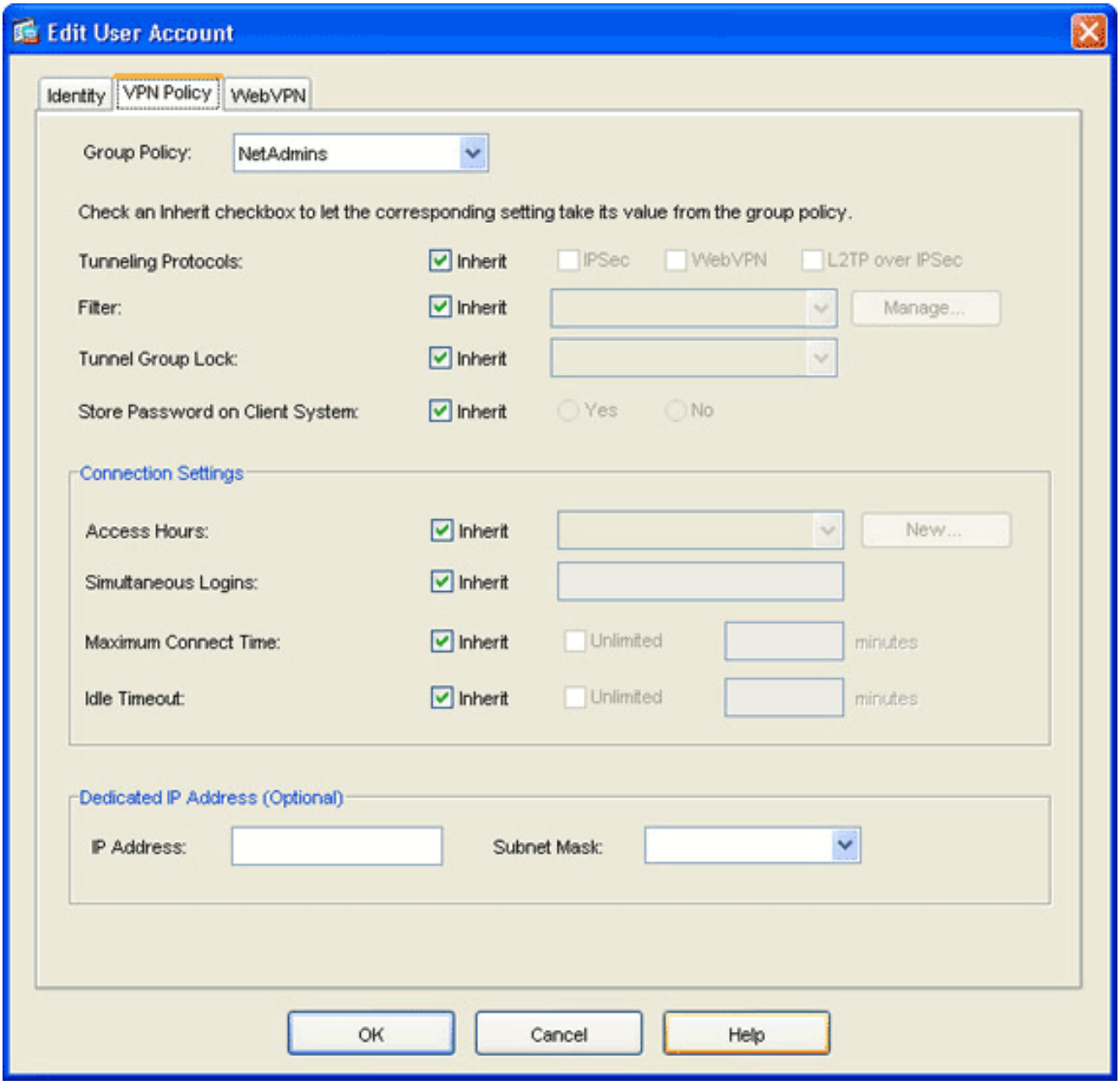


2. **Add** 버튼을 클릭합니다.Add User Account 대화 상자가 나타납니다

.



3. 사용자 이름, 비밀번호 및 권한 정보의 값을 입력한 다음 **VPN Policy** 탭을 클릭합니다
.



4. **그룹 정책** 드롭다운 화살표를 클릭하고 3단계에서 생성한 그룹 정책을 선택합니다.이 사용자는 선택한 그룹 정책의 WebVPN 특성 및 정책을 상속받습니다.
5. OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**.
6. Save(**저장**)를 클릭한 다음 **Yes(예**)를 클릭하여 변경 사항을 적용합니다.

CLI를 사용한 씬 클라이언트 SSL VPN 구성

ASA
ASA Version 7.2(1) ! hostname ciscoasa domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif inside security-level 100 ip address 10.1.1.1 255.255.255.0

```
!--- Output truncated  port-forward portforward 3044
10.2.2.2 telnet Telnet to R1
!--- Configure the set of applications that WebVPN
users !--- can access over forwarded TCP ports group-
policy NetAdmins internal
!--- Create a new group policy for enabling WebVPN
access group-policy NetAdmins attributes
 vpn-tunnel-protocol IPSec l2tp-ipsec webvpn
!--- Configure group policy attributes webvpn
  functions port-forward auto-download
!--- Configure group policies for WebVPN   port-forward
value portforward
!--- Configure port-forward to enable WebVPN
application access !--- for the new group policy  port-
forward-name value Secure Router Access
!--- Configure the display name that identifies TCP
port !--- forwarding to end users username user1
password tJsDL6po9m1UFs.h encrypted
username user1 attributes
 vpn-group-policy NetAdmins
!--- Create and add User(s) to the new group policy
http server enable http 0.0.0.0 0.0.0.0 DMZ no snmp-
server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart tunnel-group NetGroup type webvpn
tunnel-group NetGroup general-attributes
 default-group-policy NetAdmins
!--- Create a new tunnel group and link it to the group
policy telnet timeout 5 ssh timeout 5 console timeout 0
! 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 webvpn
 enable outside
!--- Enable Web VPN on Outside interface port-forward
portforward 3044 10.2.2.2 telnet Telnet to R1 prompt
hostname context
```

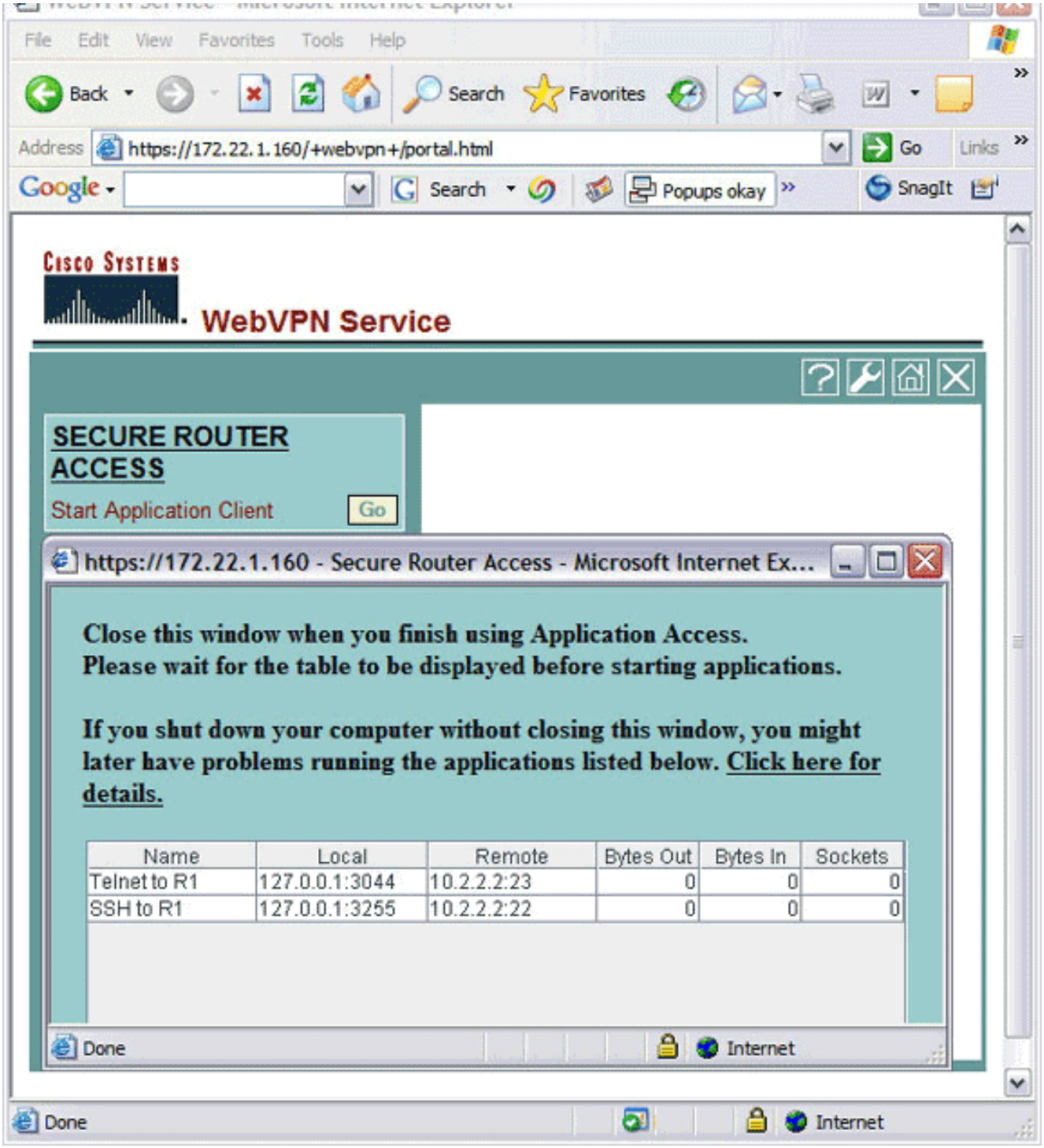
다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

절차

이 절차에서는 컨피그레이션의 유효성을 확인하는 방법과 컨피그레이션을 테스트하는 방법을 설명합니다.

1. 클라이언트 워크스테이션에서 https:// ***outside_ASA_IP Address를 입력합니다.***여기서 *outside_ASA_IPAddress*는 ASA의 SSL URL입니다.디지털 인증서가 수락되고 사용자가 인증되면 WebVPN Service 웹 페이지가 나타납니다
   .



애플리케이션에 액세스하는 데 필요한 주소 및 포트 정보가 로컬 열에 나타납니다.현재 응용 프로그램이 호출되지 않았으므로 Bytes Out(바이트 출력) 및 Bytes In(바이트 입력) 열에 활동이 표시되지 않습니다.

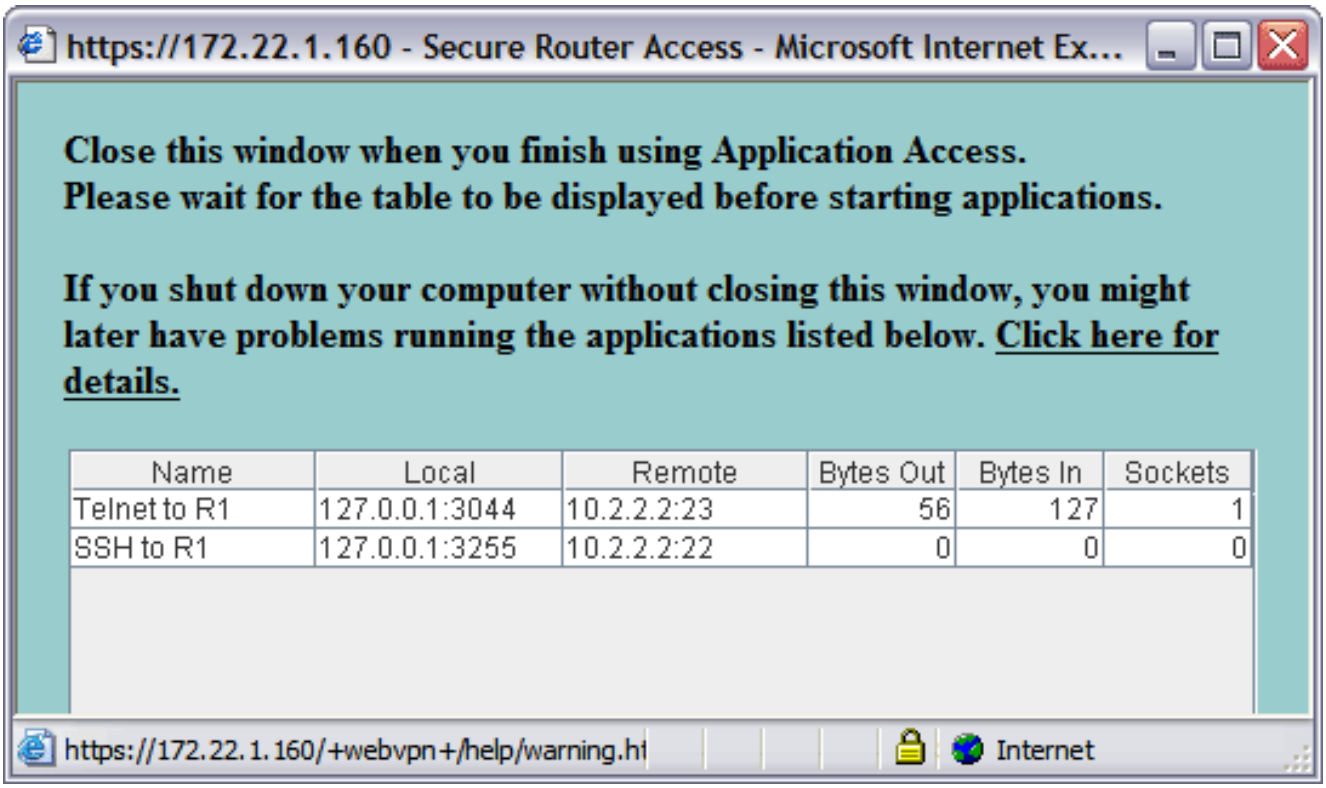
2. 텔넷 세션을 시작하려면 DOS 프롬프트 또는 기타 텔넷 애플리케이션을 사용합니다.
3. 명령 프롬프트에서 telnet **127.0.0.1 3044를 입력합니다.참고:** 이 명령은 이 문서의 WebVPN 서비스 웹 페이지 이미지에 표시된 로컬 포트에 액세스하는 방법의 예를 제공합니다.*명령에는 콜론(:)이 포함되어 있지 않습니다.* 이 문서에 설명된 대로 명령을 입력합니다.ASA는 보안 세션을 통해 명령을 수신하며 정보의 맵을 저장하므로 ASA는 매핑된 디바이스에 대한 보안 텔넷 세션을 열 수 있음을 즉시 알고 있습니다

.

사용자 이름과 비밀번호를 입력하면 디바이스에 대한 액세스가 완료됩니다.

4. 디바이스에 대한 액세스를 확인하려면 다음 이미지에 표시된 대로 Bytes Out and Bytes In 열을 확인합니다

.



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.

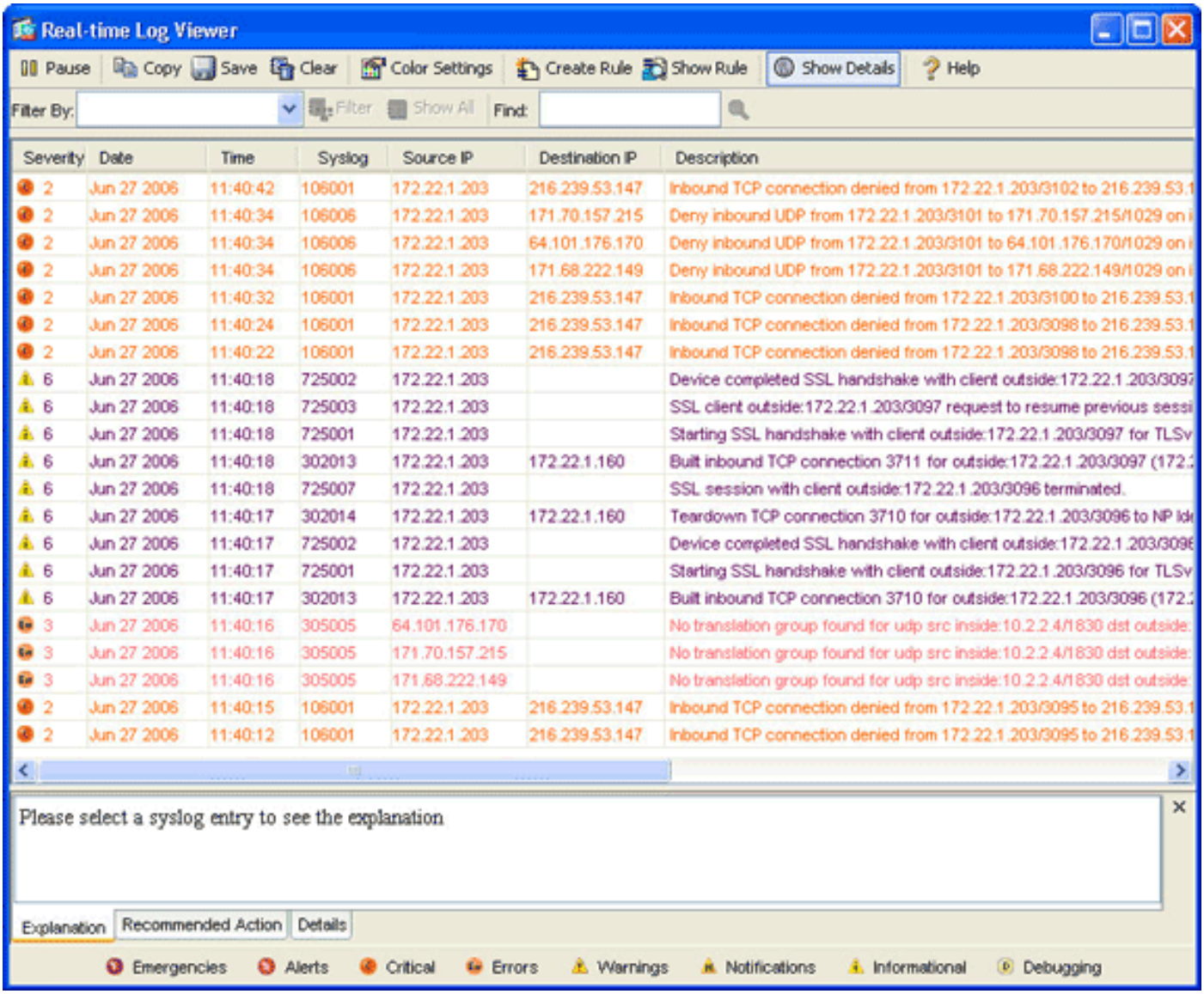
참고: Output Interpreter Tool(등록된 고객만 해당)(OIT)은 특정 **show** 명령을 **지원합니다**.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

SSL 핸드셰이크 프로세스가 완료되었습니까?

ASA에 연결한 후 실시간 로그에 SSL 핸드셰이크의 완료가 표시되는지 확인합니다.

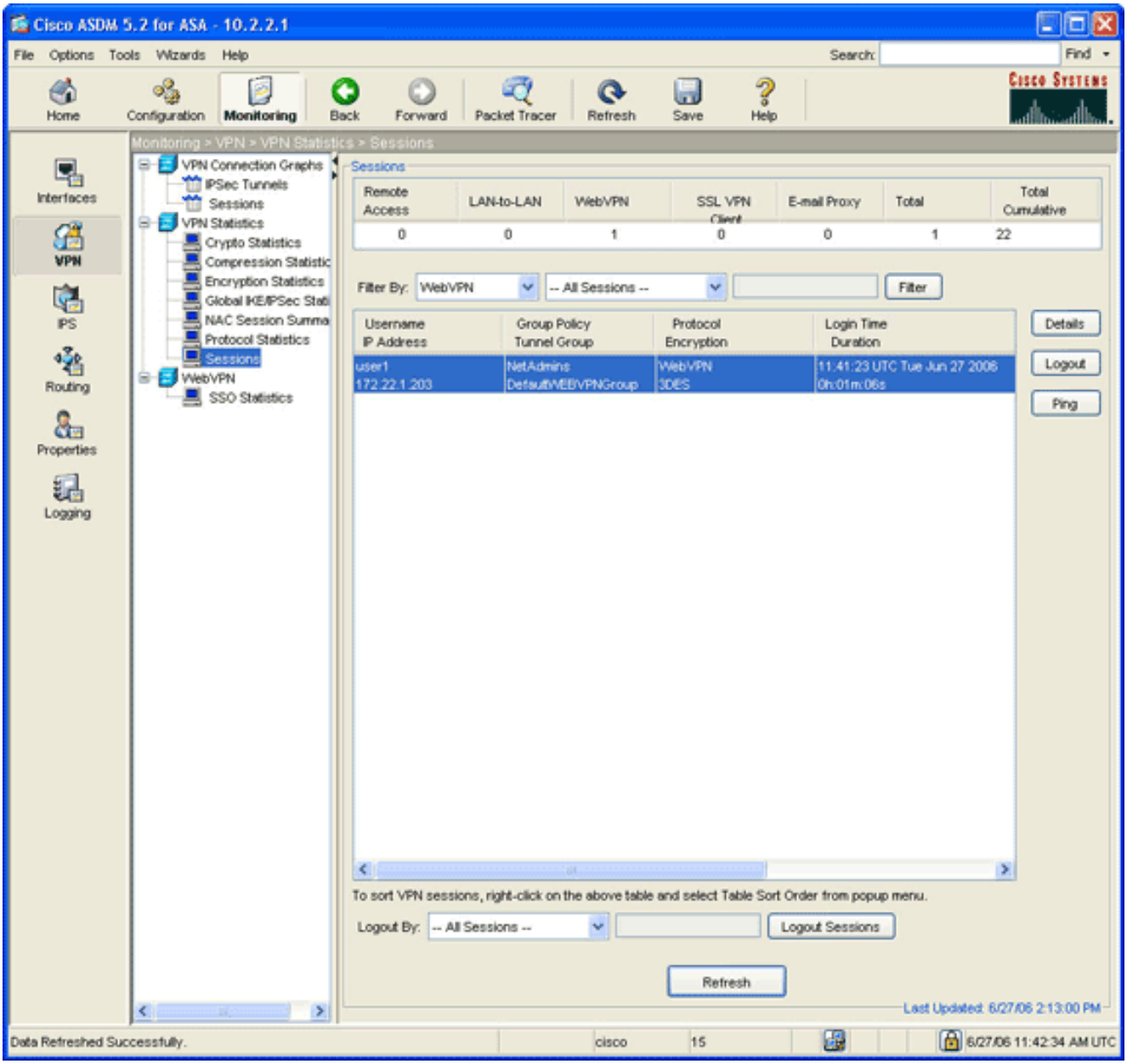


SSL VPN Thin-Client가 작동합니까?

SSL VPN Thin-Client가 작동하는지 확인하려면 다음 단계를 수행하십시오.

1. Monitoring(**모니터링**)을 클릭한 다음 **VPN**을 클릭합니다.
2. **VPN Statistics(VPN 통계)**를 확장하고 **Sessions(세션)**를 클릭합니다.SSL VPN Thin-Client 세션이 세션 목록에 나타나야 합니다.다음 이미지에 표시된 대로 WebVPN을 기준으로 필터링해야 합니다

.



명령

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

- ASA 컨피그레이션의 클라이언트리스 SSL VPN(WebVPN) 예
- ASA의 SVC(SSL VPN Client) with ASDM 컨피그레이션 예
- Cisco ASA 5500 Series Adaptive Security Appliance
- ASDM 및 NTLMv1 컨피그레이션을 사용하는 ASA with WebVPN 및 Single Sign-on 예
- 기술 지원 및 문서 – Cisco Systems