SDM을 사용하여 Cisco IOS에서 클라이언트리스 SSL VPN(WebVPN) 구성

목차

소개

클라이언트리스 SSL VPN(WebVPN)을 사용하면 사용자가 SSL이 활성화된 웹 브라우저를 사용하여 어디에서나 회사 LAN의 리소스에 안전하게 액세스할 수 있습니다. 사용자는 먼저 WebVPN 게이트웨이로 인증한 다음 사용자가 미리 구성된 네트워크 리소스에 액세스할 수 있도록 합니다. WebVPN 게이트웨이는 Cisco IOS® 라우터, Cisco ASA(Adaptive Security Appliance), Cisco VPN 3000 Concentrator 및 Catalyst 6500 및 7600 라우터용 Cisco WebVPN Services Module에서 구성할 수 있습니다.

Cisco 디바이스에서 SSL(Secure Socket Layer) VPN(Virtual Private Network) 기술을 다음과 같은 세 가지 기본 모드로 구성할 수 있습니다. 클라이언트리스 SSL VPN(WebVPN), 씬 클라이언트 SSL VPN(포트 전달) 및 SSL VPN 클라이언트(SVC) 모드. 이 문서에서는 Cisco IOS 라우터에서 WebVPN의 컨피그레이션을 보여 줍니다.

참고: IP 도메인 이름 또는 라우터의 호스트 이름을 변경하지 마십시오. 이렇게 하면 자체 서명 인증

서를 재생성하고 구성된 신뢰 지점을 재정의할 수 있습니다. 자체 서명 인증서를 재생성하면 라우터가 WebVPN용으로 구성된 경우 연결 문제가 발생합니다. WebVPN은 SSL 신뢰 지점 이름을 WebVPN 게이트웨이 구성에 연결합니다. 따라서 새 자체 서명 인증서가 발급되면 새 신뢰 지점 이름이 WebVPN 컨피그레이션과 일치하지 않으며 사용자가 연결할 수 없습니다.

참고: 영구 자체 서명 인증서를 사용하는 WebVPN 라우터에서 **ip https-secure server** 명령을 실행하면 새 RSA 키가 생성되고 인증서가 무효화됩니다. SSL WebVPN을 중단시키는 새 신뢰 지점이 생성됩니다. 영구 자체 서명 인증서를 사용하는 라우터가 **ip https-secure server** 명령을 실행한 후 재부팅되면 동일한 문제가 발생합니다.

씬 클라이언트 SSL VPN에 대한 자세한 내용은 SDM과 함께 Thin-Client SSL VPN(WebVPN) IOS 구성 예를 참조하십시오.

SSL VPN 클라이언트에 대한 자세한 내용은 IOS의 SSL VPN Client(SVC) with SDM Configuration 예를 참조하십시오.

SSL VPN은 다음 Cisco 라우터 플랫폼에서 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 Software 릴리스 12.4(6)T 이상의 고급 이미지
- 소개에 나열된 Cisco 라우터 플랫폼 중 하나

사용되는 구성 요소

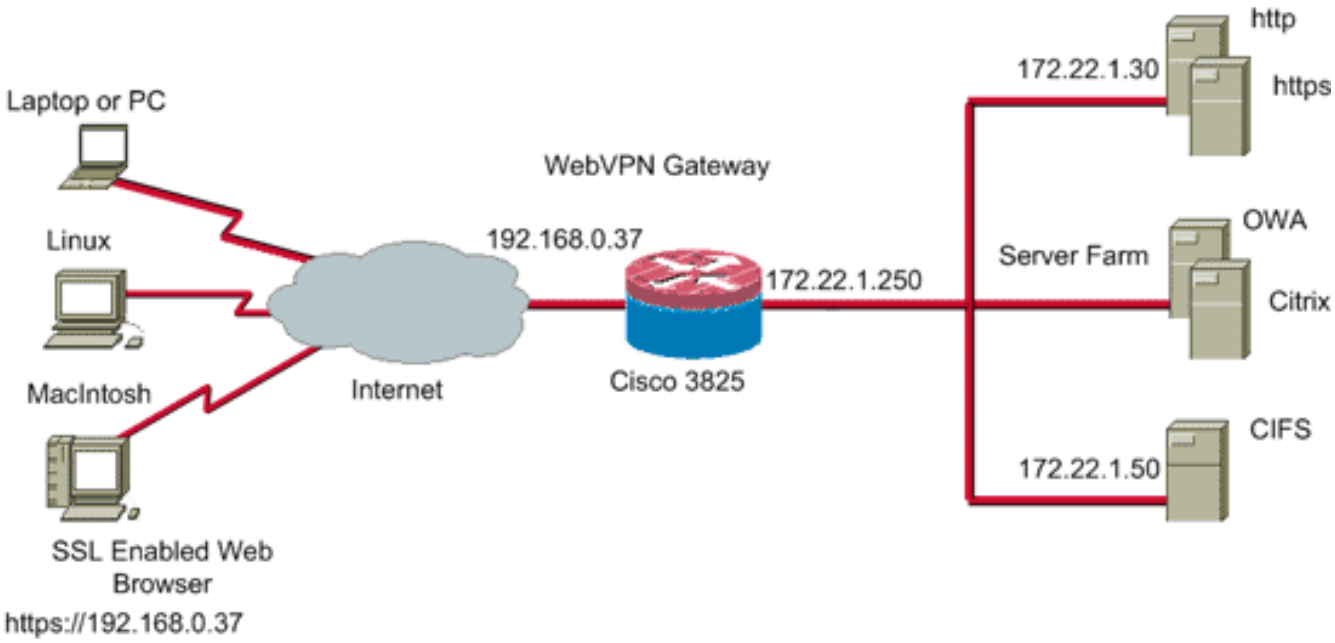
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 3825 라우터
- 고급 엔터프라이즈 소프트웨어 이미지 - Cisco IOS Software 릴리스 12.4(9)T
- Cisco 라우터 및 SDM(Security Device Manager) - 버전 2.3.1

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. 이 예제에 사용된 IP 주소는 인터넷에서 사용할 수 없는 사설 RFC 1918 주소에서 가져옵니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

사전 구성 작업

시작하기 전에 다음 작업을 완료합니다.

1. 호스트 이름 및 도메인 이름을 구성합니다.
2. SDM용 라우터를 구성합니다. Cisco는 일부 라우터에 SDM의 사전 설치된 사본을 제공합니다 .Cisco 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.
3. 라우터에 올바른 날짜, 시간 및 시간대를 구성합니다.

Cisco IOS에서 WebVPN 구성

디바이스에 둘 이상의 WebVPN 게이트웨이를 연결할 수 있습니다. 각 WebVPN 게이트웨이는 라우터에서 하나의 IP 주소에만 연결됩니다. 특정 WebVPN 게이트웨이에 대해 둘 이상의 WebVPN 컨텍스트를 생성할 수 있습니다. 개별 컨텍스트를 식별하려면 각 컨텍스트에 고유한 이름을 지정합니다. 하나의 정책 그룹은 하나의 WebVPN 컨텍스트에만 연결할 수 있습니다. 정책 그룹은 특정 WebVPN 컨텍스트에서 사용 가능한 리소스를 설명합니다.

Cisco IOS에서 WebVPN을 구성하려면 다음 단계를 완료합니다.

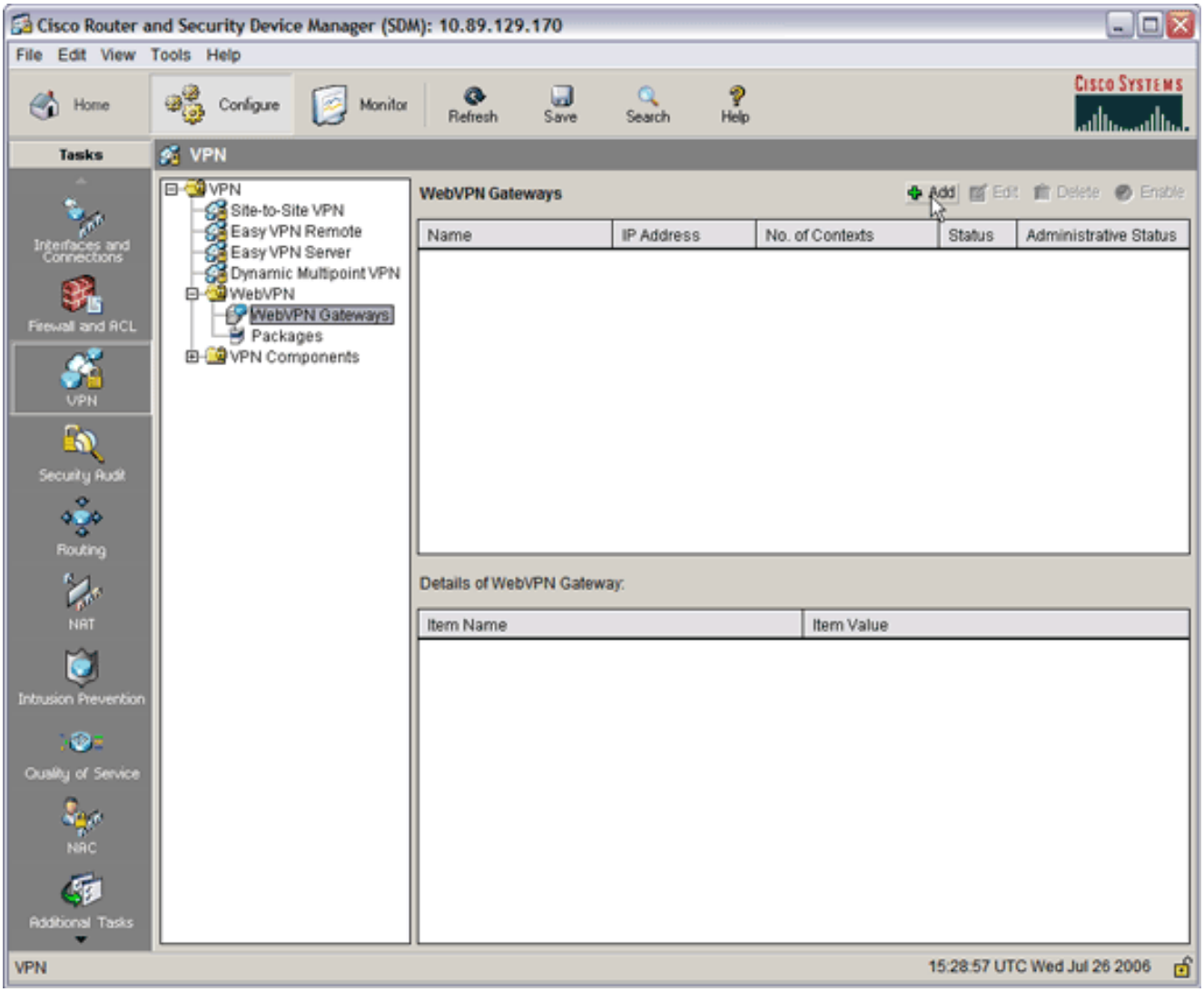
1. WebVPN 게이트웨이 구성
2. 정책 그룹에 허용되는 리소스 구성
3. WebVPN 정책 그룹 구성 및 리소스 선택
4. WebVPN 컨텍스트 구성
5. 사용자 데이터베이스 및 인증 방법 구성

1단계. WebVPN 게이트웨이 구성

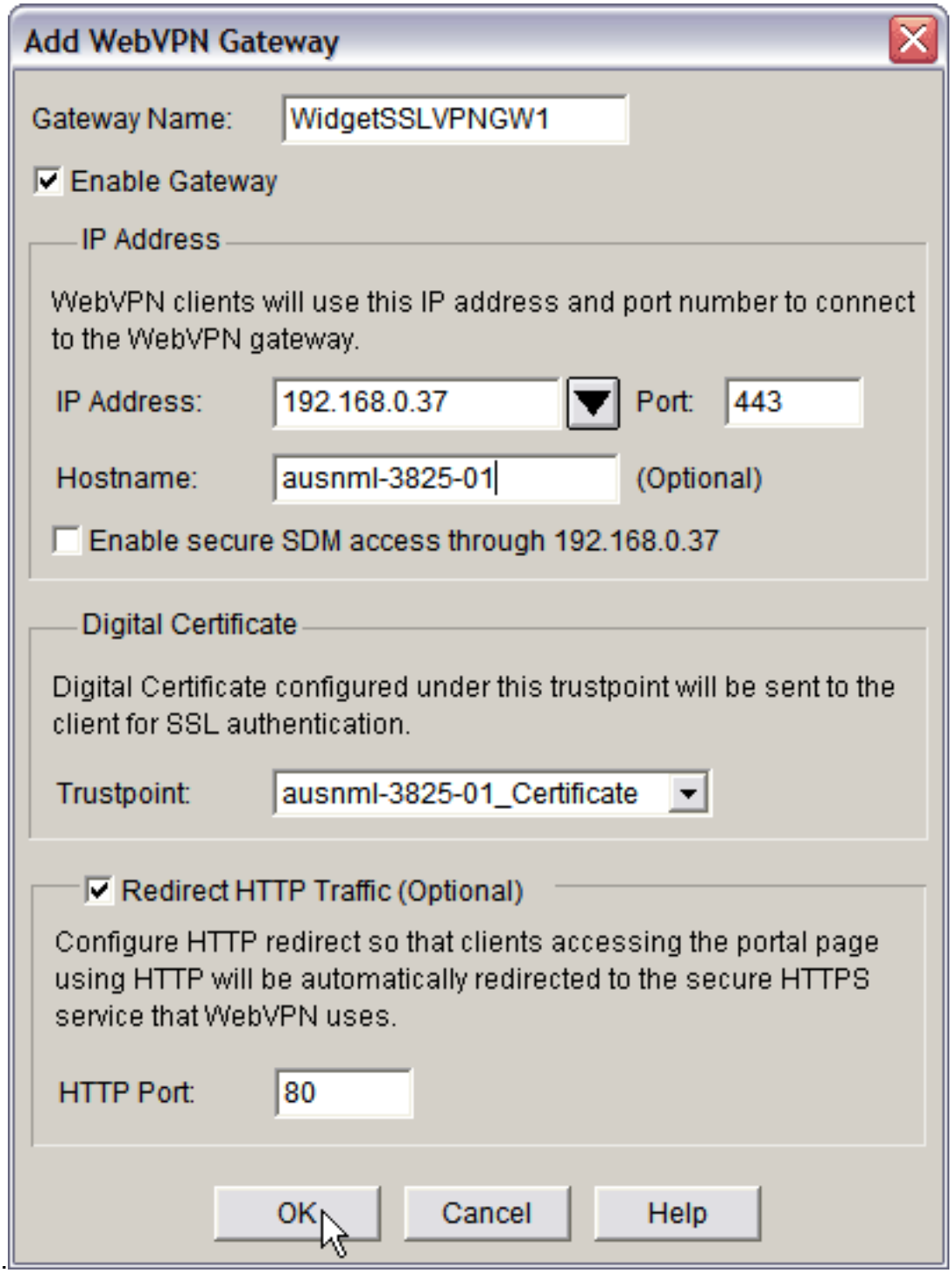
WebVPN 게이트웨이를 구성하려면 다음 단계를 완료하십시오.

1. SDM 애플리케이션 내에서 Configure(구성)**를** 클릭한 다음 **VPN**을 클릭합니다.
2. WebVPN**을** 확장하고 WebVPN **Gateway를 선택합니다**

.



3. Add(**추가)를 클릭합니다**.Add WebVPN Gateway 대화 상자가 나타납니다



4. Gateway Name(게이트웨이 이름) 및 IP Address(IP 주소) 필드에 값을 입력한 다음 Enable Gateway(게이트웨이 **활성화)** 확인란을 선택합니다.
5. Redirect **HTTP Traffic(HTTP 트래픽 리디렉션**) 확인란을 선택한 다음 **OK**(확인)를 클릭합니다 .
6. Save(**저장**)를 클릭한 다음 **Yes(예**)를 클릭하여 변경 사항을 적용합니다.

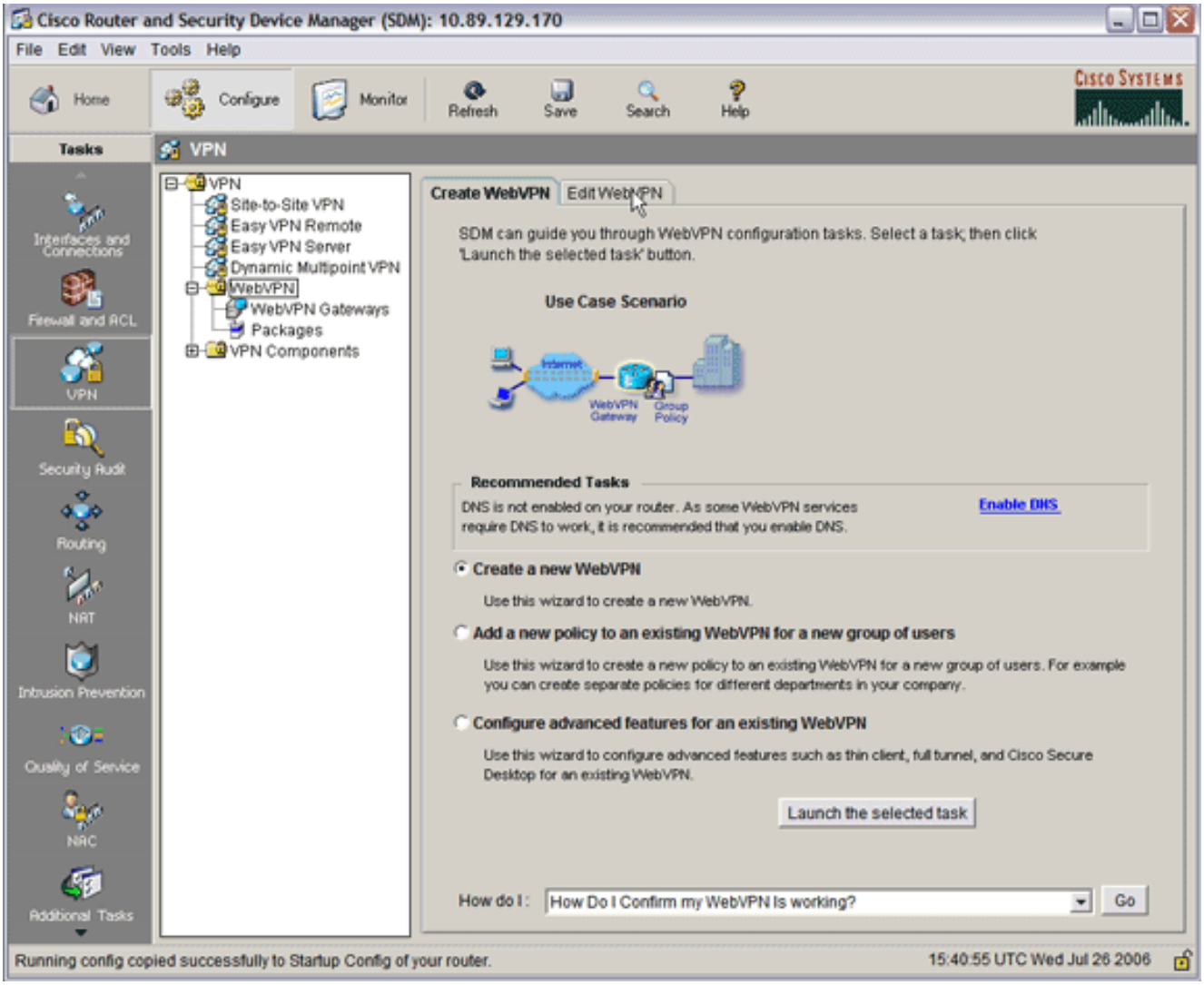
2단계. 정책 그룹에 허용되는 리소스를 구성합니다.

정책 그룹에 리소스를 더 쉽게 추가하려면 정책 그룹을 생성하기 전에 리소스를 구성할 수 있습니다.

정책 그룹에 허용되는 리소스를 구성하려면 다음 단계를 완료합니다.

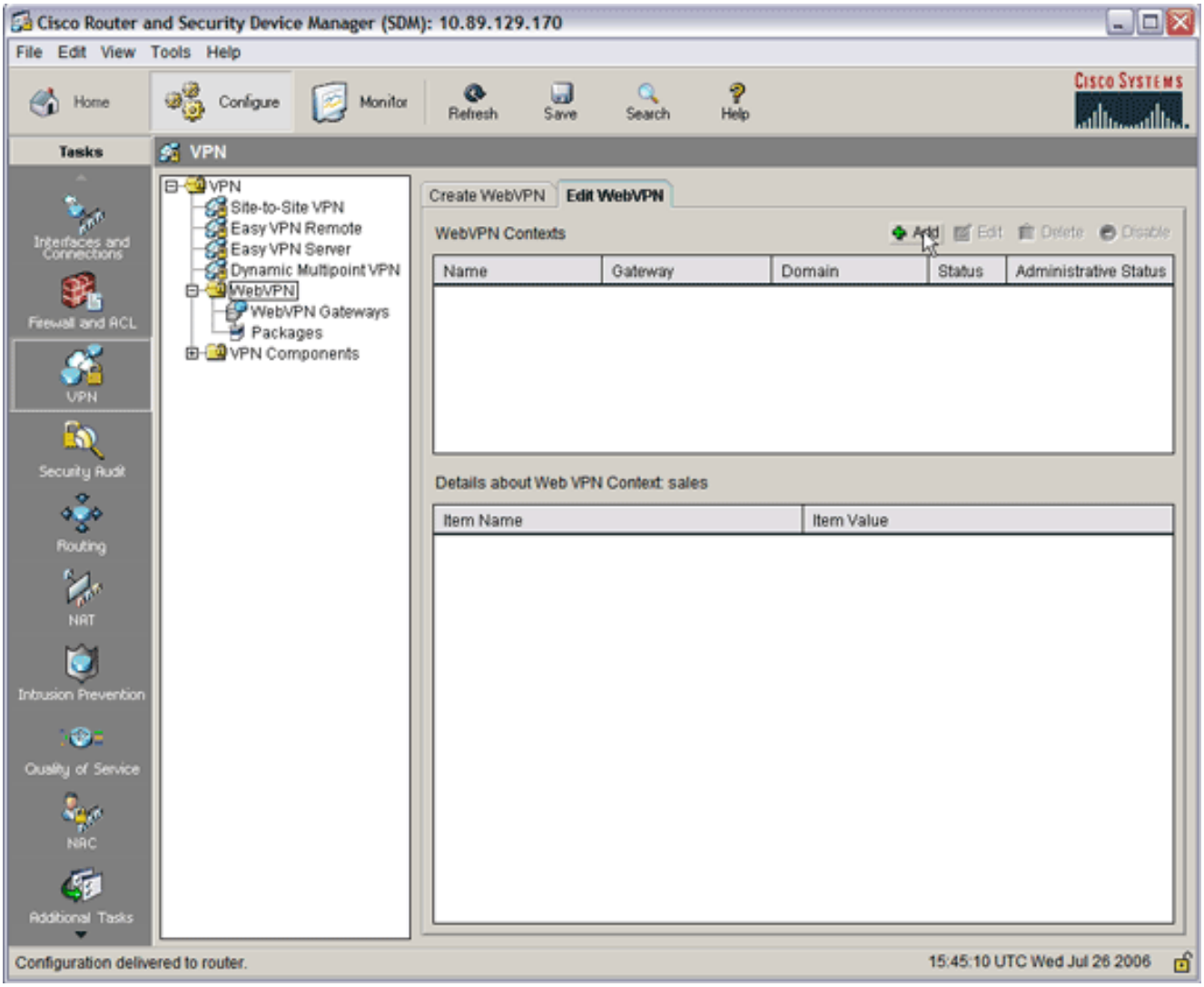
1. Configure(구성)를 클릭한 다음 **VPN**을 클릭합니다

.



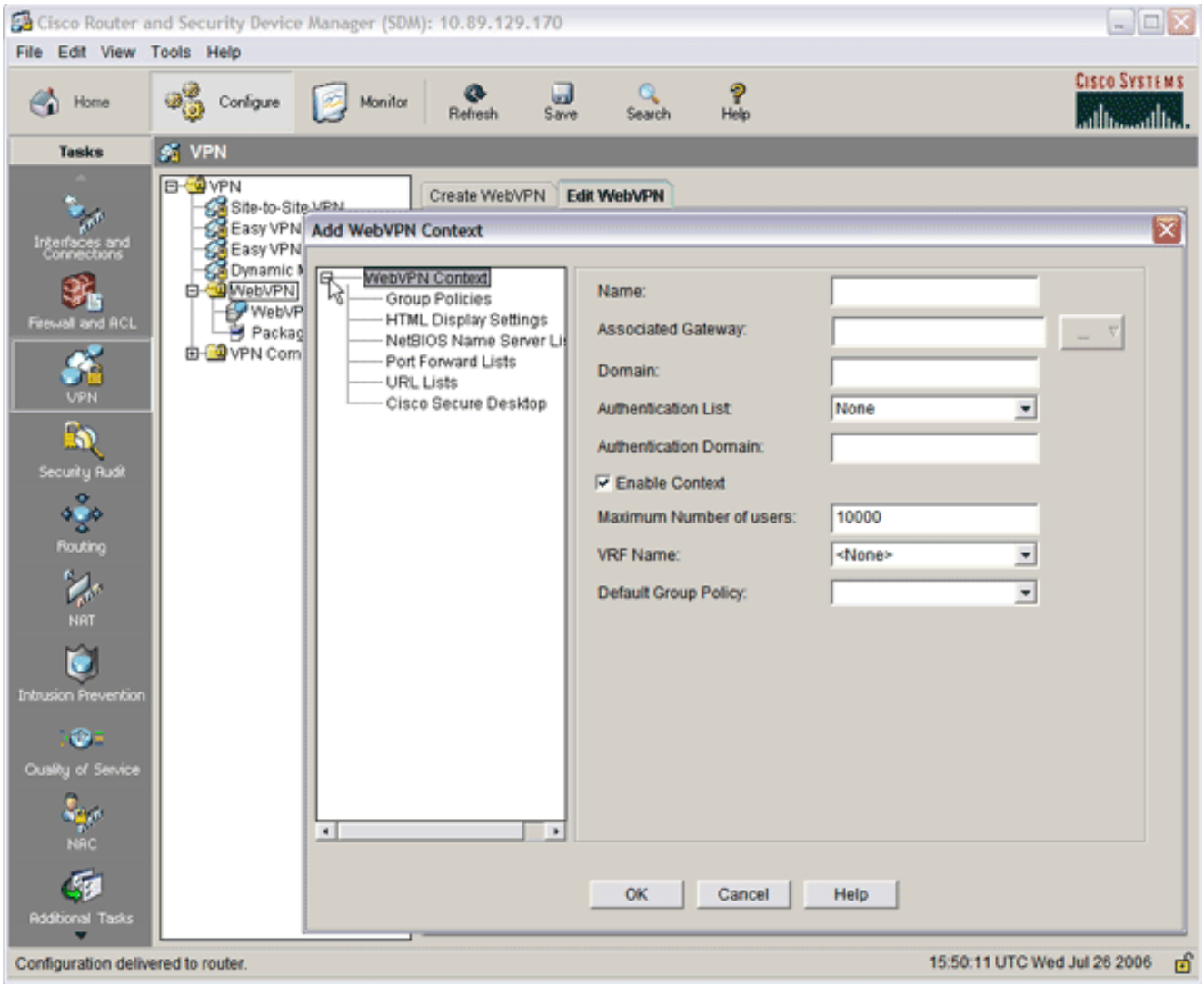
2. WebVPN**을** 선택한 다음 Edit WebVPN(WebVPN **편집)** 탭**을** 클릭합니다.**참고:** WebVPN을 사용하면 CIFS(Common Internet File System) 프로토콜 및 Citrix를 통해 HTTP, HTTPS, Windows 파일 탐색에 대한 액세스를 구성할 수 있습니다

.



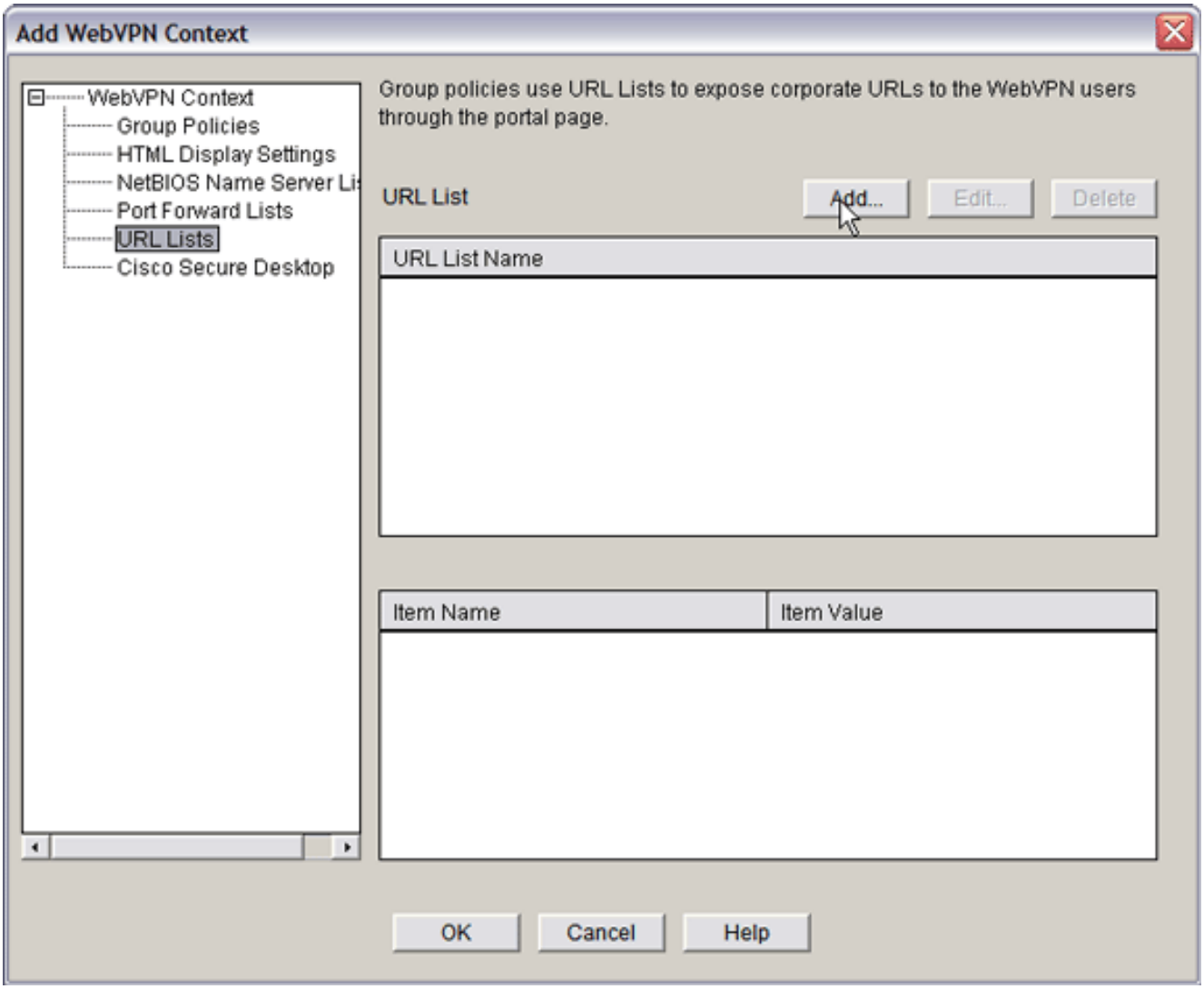
3. Add(**추가)를 클릭합니다**.Add WebVPN Context 대화 상자가 나타납니다

.

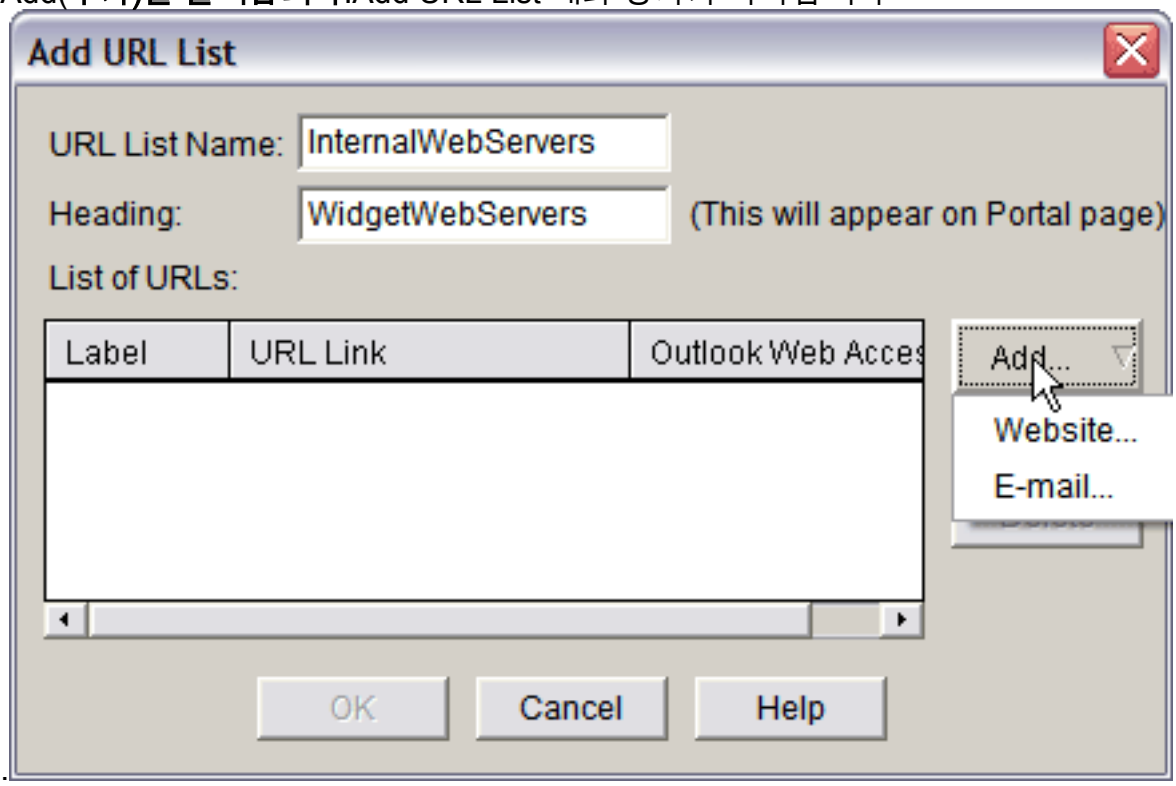


4. WebVPN **Context**를 확장하고 **URL** Lists를 **선택합니다**

.

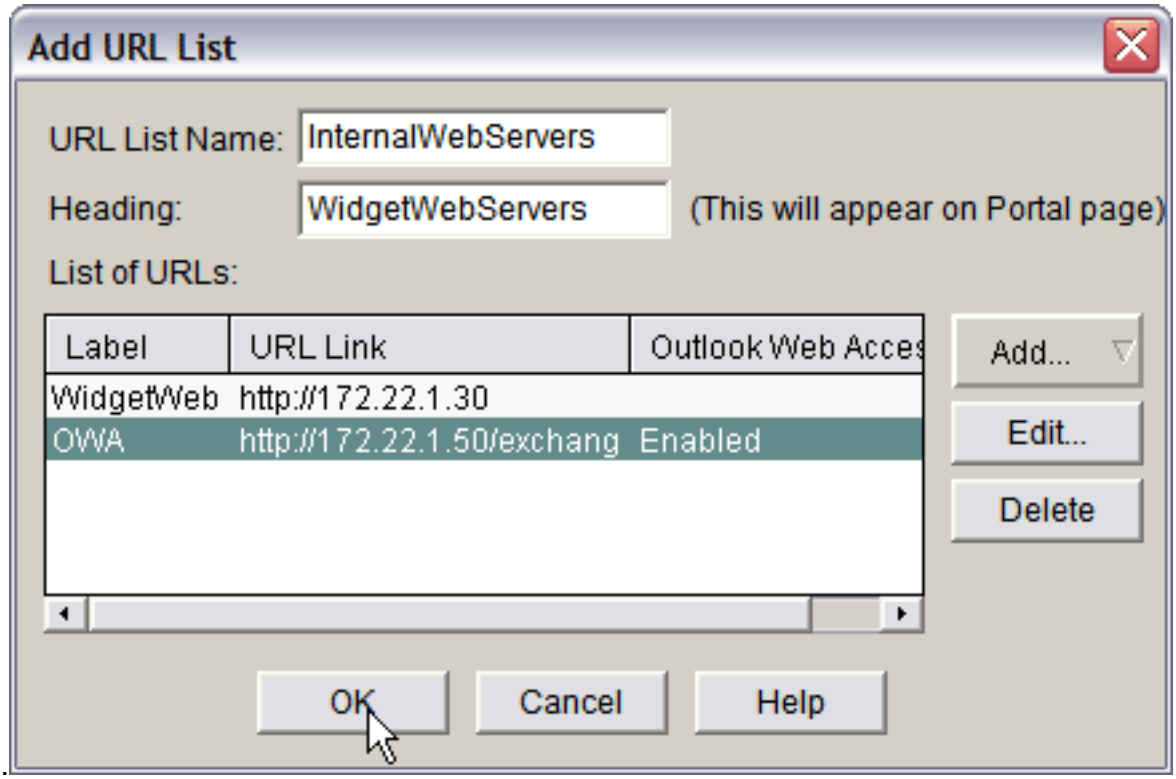


5. Add(**추가)를 클릭합니다**.Add URL List 대화 상자가 나타납니다



.

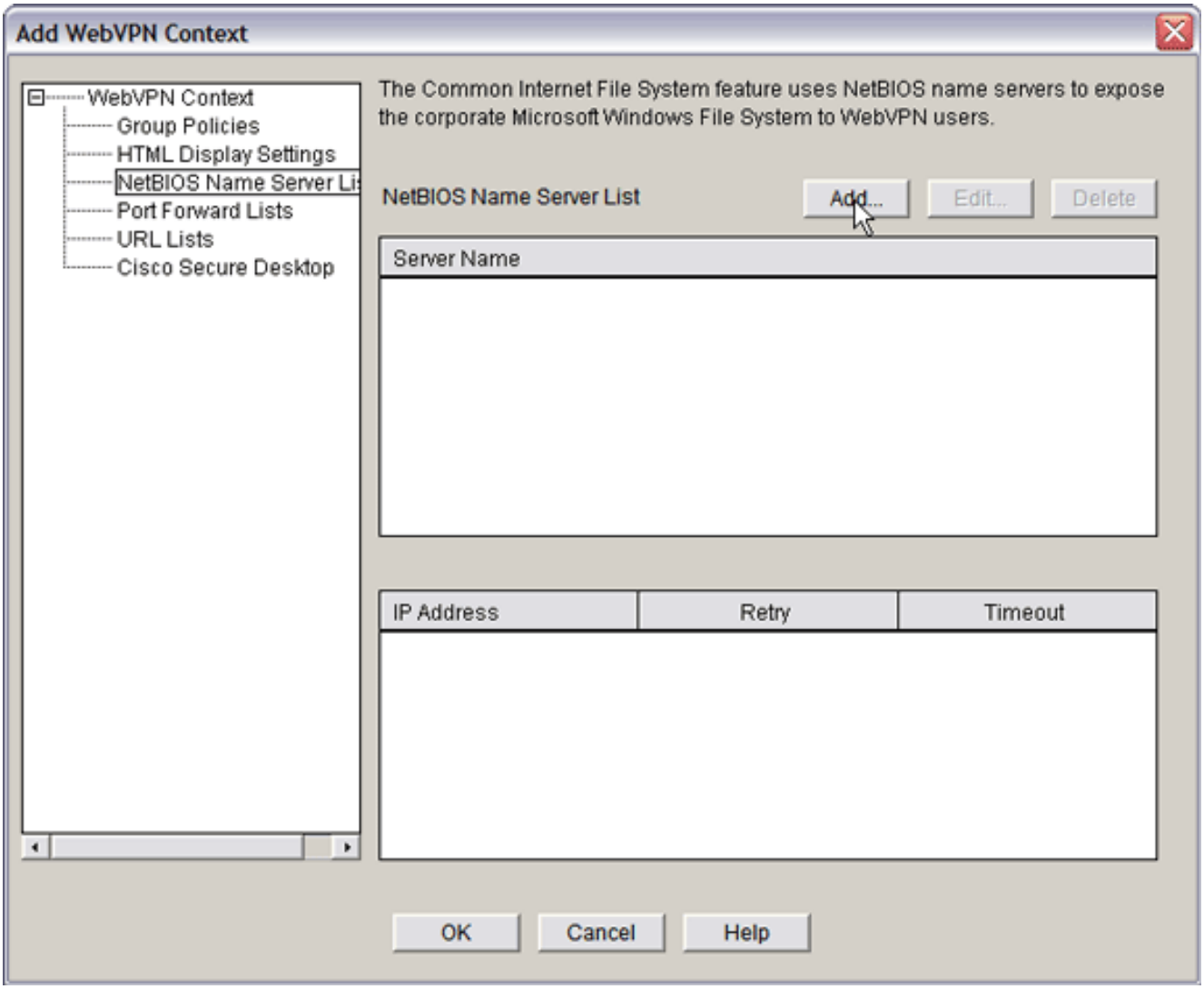
6. URL List Name 및 Heading 필드에 값을 입력합니다.
7. Add(**추가**)를 클릭하고 Website(**웹 사이트)를 선택합니다**



.이 목록에는 이 WebVPN 연결에 사용할 수 있는 모든 HTTP 및 HTTPS 웹 서버가 포함되어 있습니다.

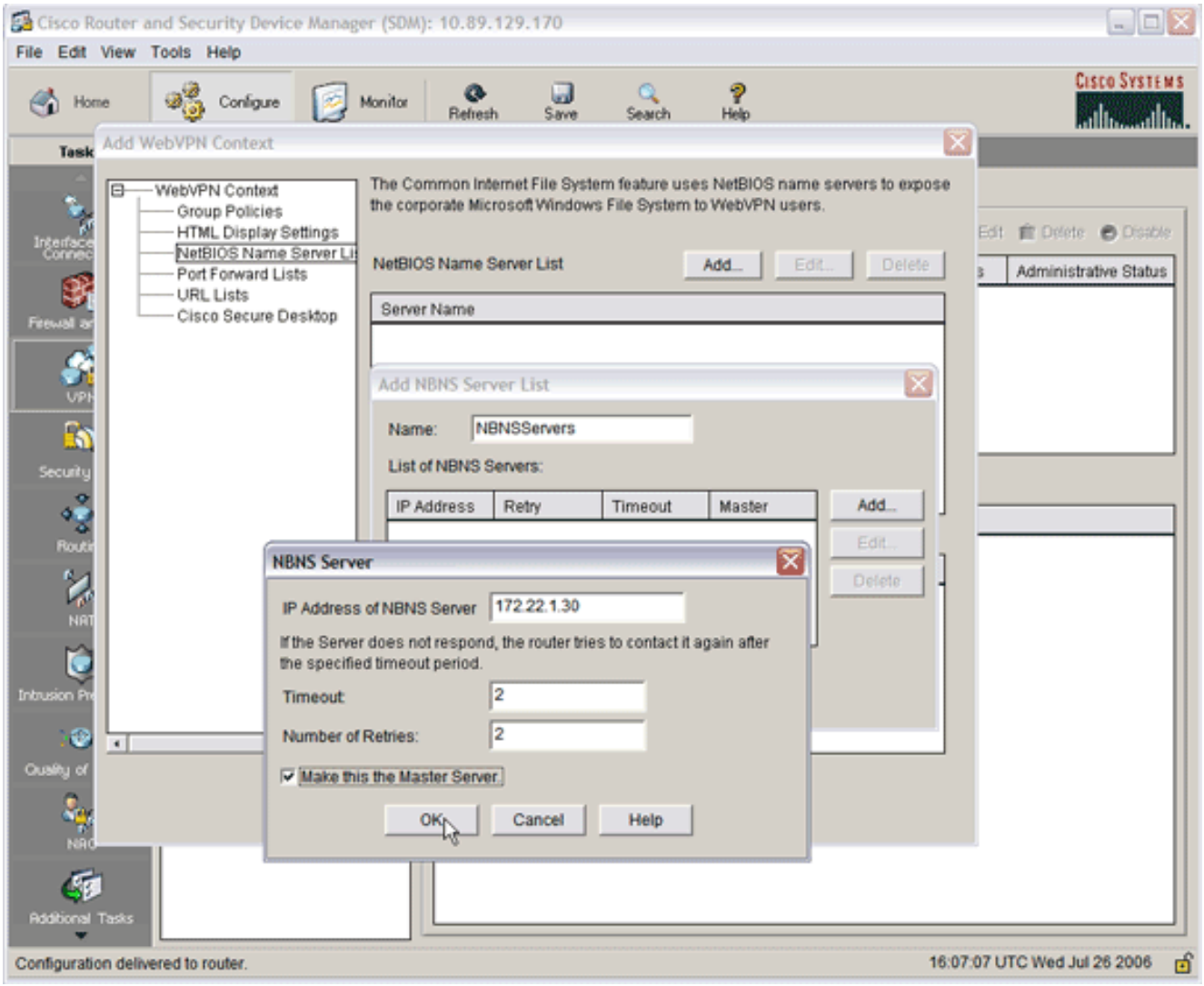
8. OWA(Outlook Web Access)에 대한 액세스를 추가하려면 **추가를** 클릭하고 **전자 메일**을 선택한 다음 원하는 필드를 모두 입력한 후 **확인**을 클릭합니다.
9. CIFS를 통한 Windows 파일 브라우징을 허용하려면 NetBIOS NBNS(Name Service) 서버를 지정하고 Windows 도메인에서 적절한 공유를 순서대로 구성할 수 있습니다.WebVPN Context 목록에서 NetBIOS **Name Server Lists를** 선택합니다

.



Add(**추가)를 클릭합니다**.Add NBNS Server List 대화 상자가 나타납니다.목록의 이름을 입력하고 Add(추가)를 **클릭합니다**.NBNS Server 대화 상자가 나타납니다

.

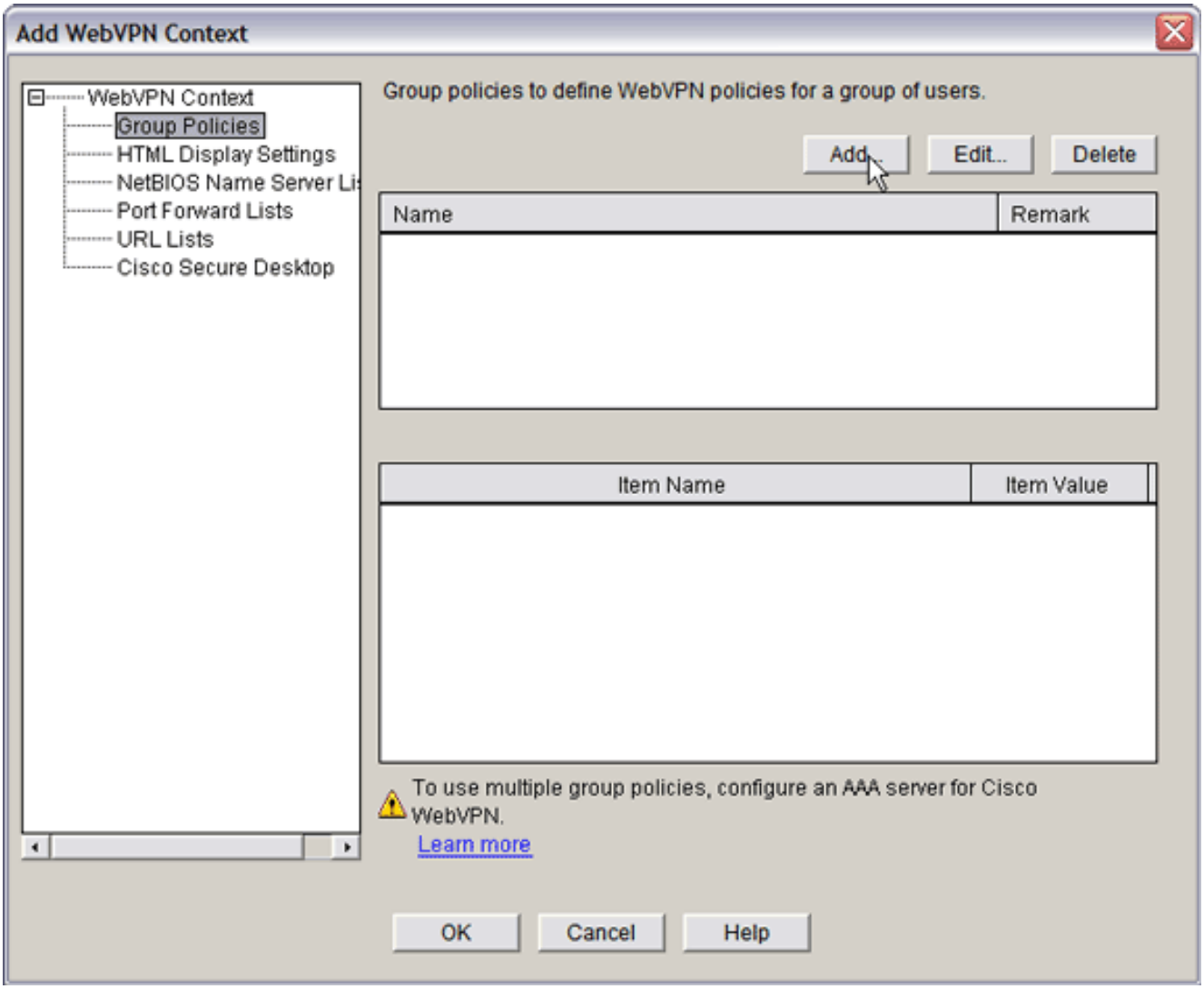


해당되는 경우 **Make This** as **Master Server** 확인란을 선택합니다.OK(**확인**)를 클릭한 다음 **OK**(확인)를 클릭합니다.

3단계. WebVPN 정책 그룹을 구성하고 리소스를 선택합니다.

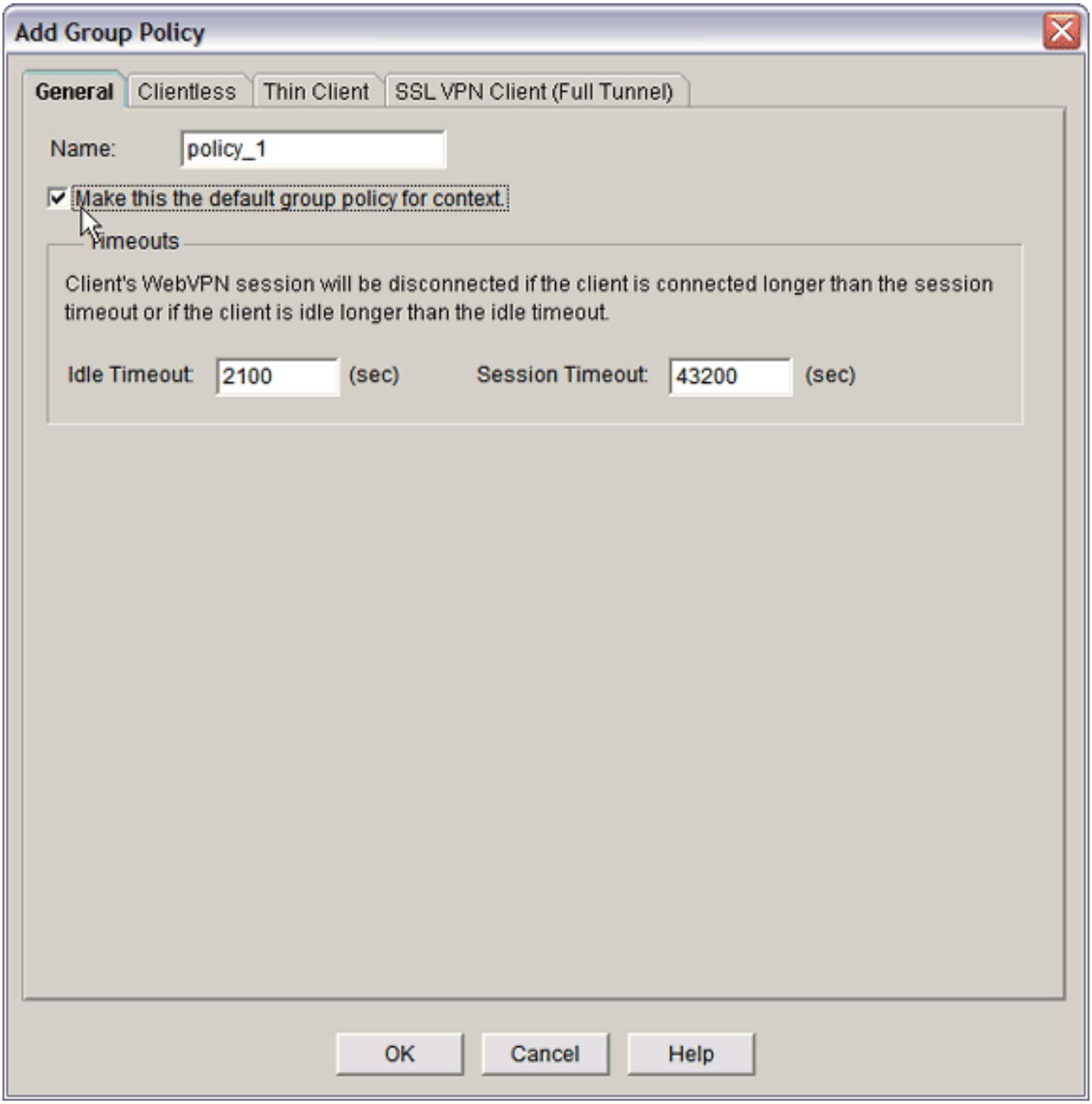
WebVPN 정책 그룹을 구성하고 리소스를 선택하려면 다음 단계를 완료하십시오.

1. Configure(구성)를 클릭한 다음 **VPN**을 클릭합니다.
2. WebVPN**을** 확장하고 WebVPN **Context를 선택합니다**
   .

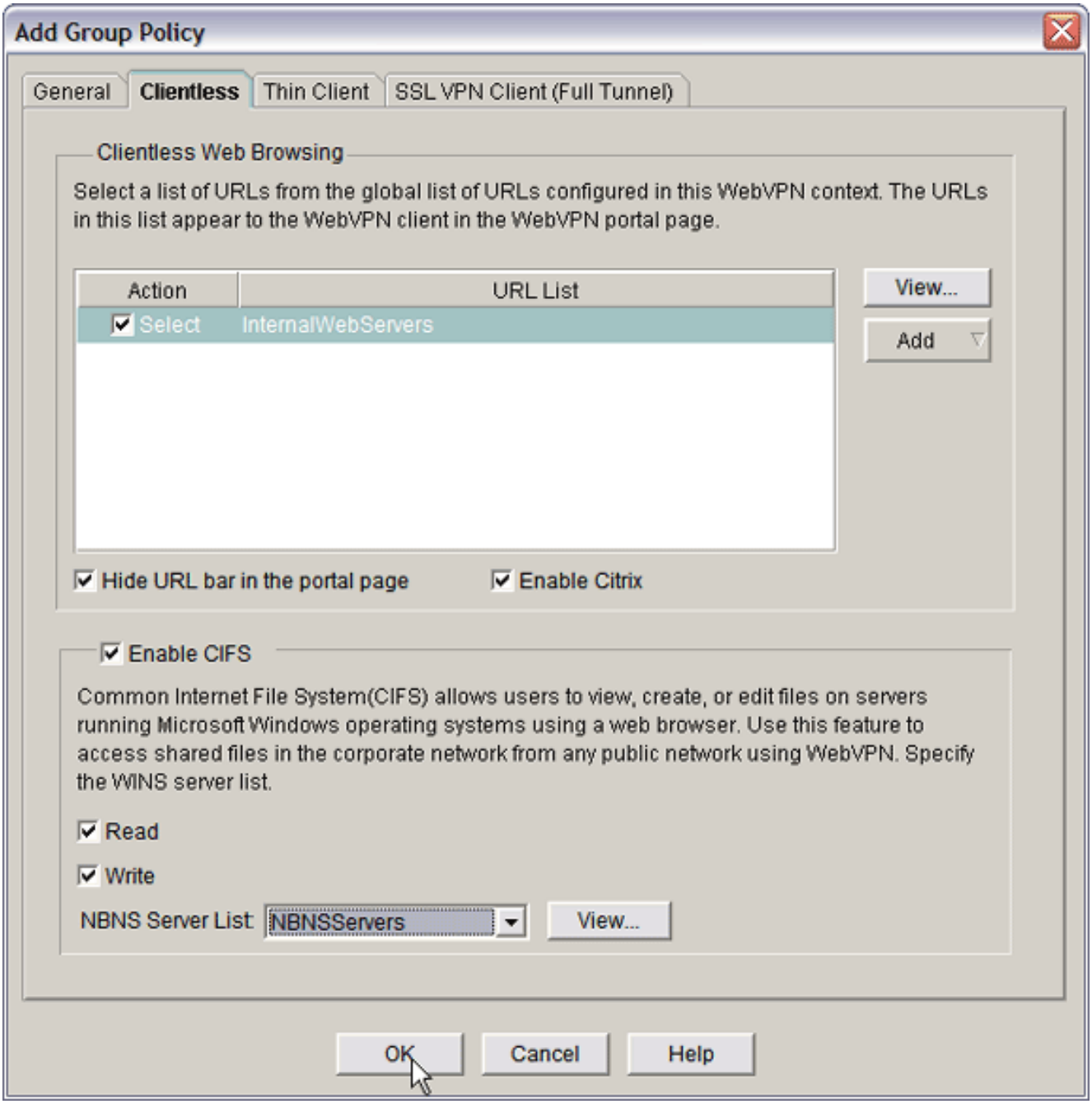


3. Group **Policies(그룹 정책)**를 선택하고 Add(**추가)**를 클릭합니다.Add Group Policy 대화 상자가 나타납니다

.



4. 새 정책의 이름을 입력하고 Make this **as default group policy for context** 확인란을 선택합니다
.
5. 대화 상자 맨 위에 있는 클라이언트리스 탭을 클릭합니다
.

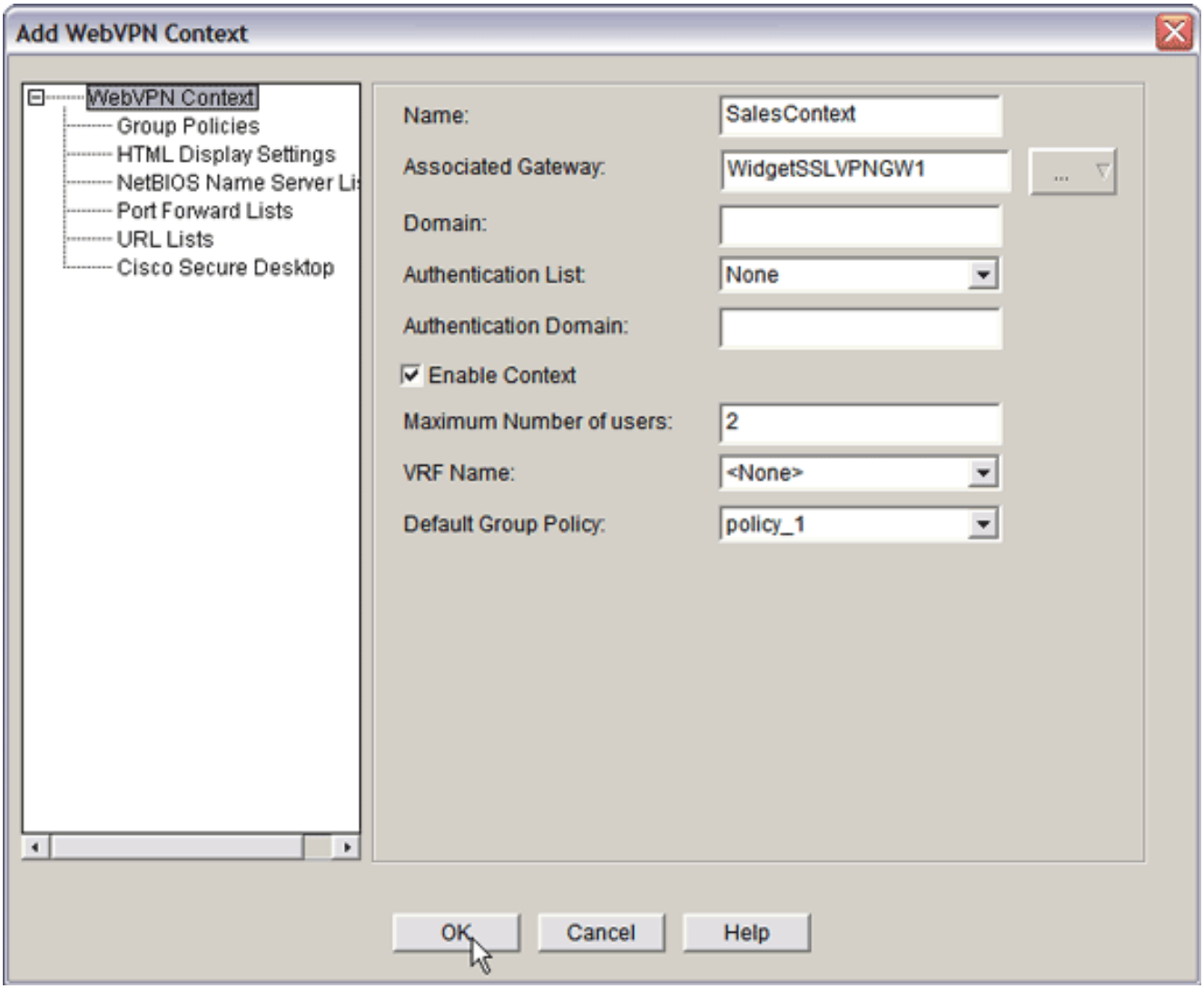


6. 원하는 URL List에 대한 Select(선택) 확인란을 선택합니다.
7. 고객이 Citrix 서버에 액세스해야 하는 Citrix 클라이언트를 사용하는 경우 Enable **Citrix** 확인란을 선택합니다.
8. Enable **CIFS**, Read 및 Write 확인란을 선택합니다.
9. NBNS **서버 목록** 드롭다운 화살표를 클릭하고 2단계에서 Windows 파일 검색을 위해 생성한 NBNS 서버 목록을 선택합니다.
10. **확인**을 **클릭합니다**.

4단계. WebVPN 컨텍스트 구성

WebVPN 게이트웨이, 그룹 정책 및 리소스를 함께 연결하려면 WebVPN 컨텍스트를 구성해야 합니다. WebVPN 컨텍스트를 구성하려면 다음 단계를 완료합니다.

1. WebVPN **Context**를 선택하고 컨텍스트의 이름을 입력합니다
   .



2. 연결된 게이트웨이 드롭다운 화살표를 클릭하고 연결된 게이트웨이를 선택합니다.
3. 둘 이상의 컨텍스트를 작성하려면 Domain 필드에 고유한 이름을 입력하여 이 컨텍스트를 식별합니다. Domain(도메인) 필드를 비워 두면 사용자는 https://을 사용하여 WebVPN에 **액세스해야 *합니다*.** 도메인 이름(예: *Sales*)을 입력한 경우 사용자는 https://IPAddress/**Sales**와 연결해야 합니다.
4. Enable **Context** 확인란을 선택합니다.
5. Maximum Number of Users 필드에 디바이스 라이센스에서 허용하는 최대 사용자 수를 입력합니다.
6. Default **Group policy(기본 그룹 정책)** 드롭다운 화살표를 클릭하고 이 컨텍스트와 연결할 그룹 정책을 선택합니다.
7. OK(**확인**)를 클릭한 다음 **OK**(확인)를 클릭합니다.

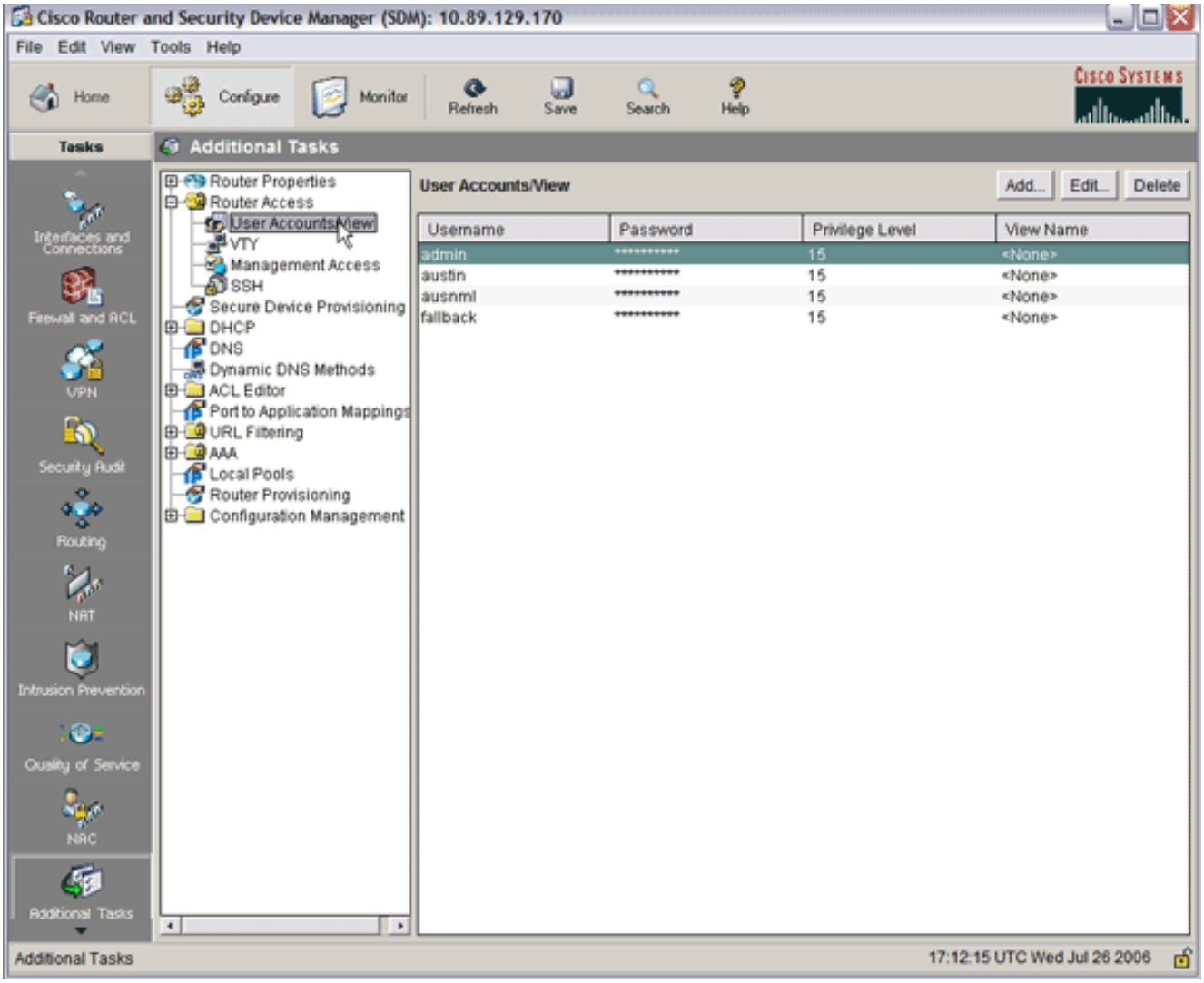
5단계. 사용자 데이터베이스 및 인증 방법 구성

클라이언트리스 SSL VPN(WebVPN) 세션을 구성하여 Radius, Cisco AAA Server 또는 로컬 데이터베이스를 인증할 수 있습니다. 이 예에서는 로컬 데이터베이스를 사용합니다.

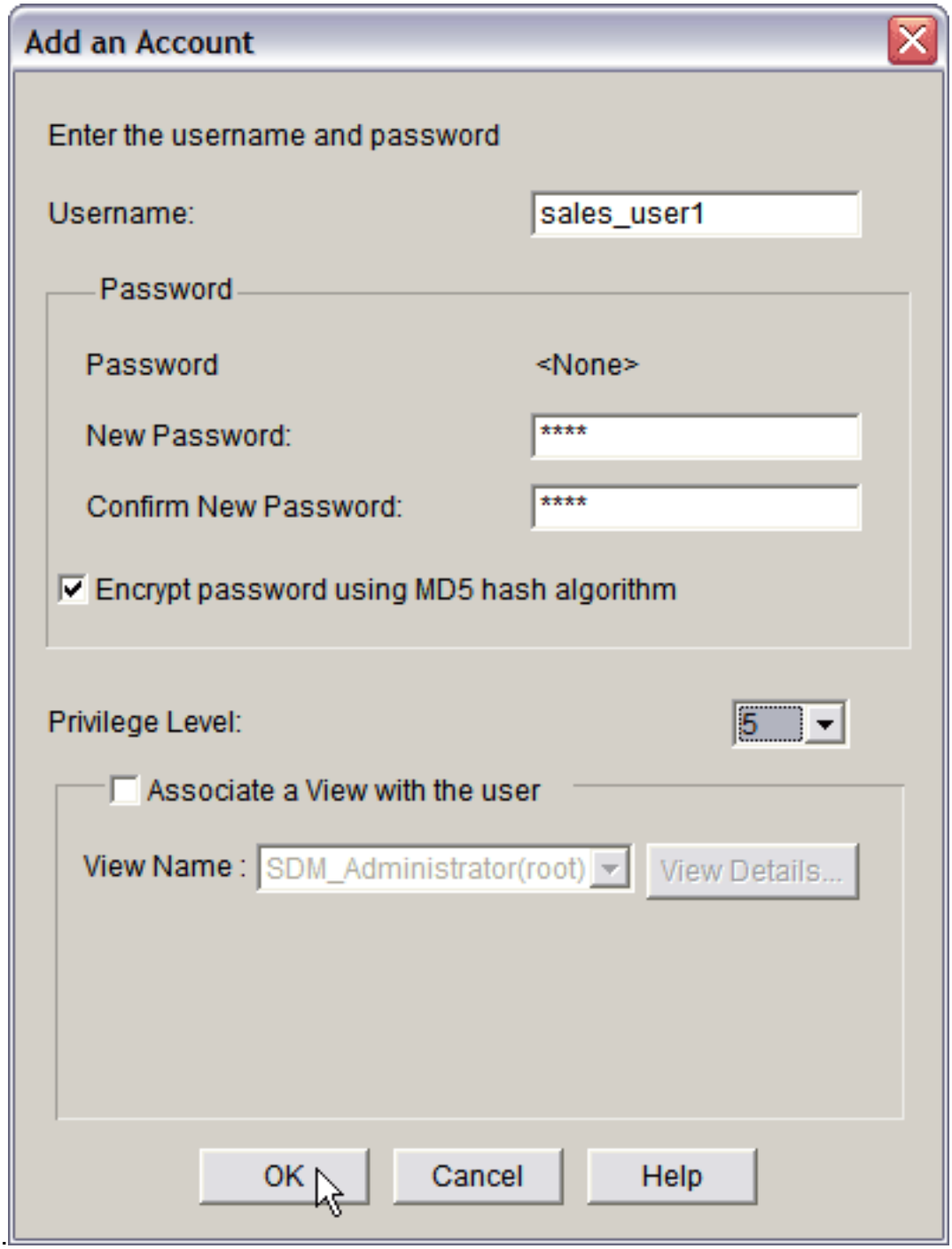
사용자 데이터베이스 및 인증 방법을 구성하려면 다음 단계를 완료합니다.

1. Configuration(컨피그레이션)을 클릭한 다음 Additional Tasks(**추가 작업)를 클릭합니다**.
2. Router **Access(라우터 액세스)**를 확장하고 User **Accounts/View(사용자 계정/보기)를 선택합니다**

.



3. **Add** 버튼을 클릭합니다.Add an Account 대화 상자가 나타납니다



4. 사용자 계정과 비밀번호를 입력합니다.
5. OK(**확인**)를 클릭한 다음 **OK**(확인)를 클릭합니다.
6. Save(**저장**)를 클릭한 다음 **Yes(예)**를 클릭하여 변경 사항을 적용합니다.

결과

ASDM은 다음과 같은 명령줄 구성을 생성합니다.

ausnml-3825-01
Building configuration... Current configuration : 4190 bytes ! ! Last configuration change at 17:22:23 UTC Wed Jul 26 2006 by ausnml

```
! NVRAM config last updated at 17:22:31 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 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 29312730 2506092A 864886F7 0D010902
16186175 736E6D6C 2D333832 352D3031 2E636973 636F2E63
6F6D301E 170D3036 30373133 32333230 34375A17 0D323030
31303130 30303030 305A3029 31273025 06092A86 4886F70D
01090216 18617573 6E6D6C2D 33383235 2D30312E 63697363
6F2E636F 6D30819F 300D0609 2A864886 F70D0101 01050003
818D0030 81890281 8100C97D 3D259BB7 3A48F877 2C83222A
A1E9E42C 5A71452F 9107900B 911C0479 4D31F42A 13E0F63B
E44753E4 0BEFDA42 FE6ED321 8EE7E811 4DEEC4E4 319C0093
C1026C0F 38D91236 6D92D931 AC3A84D4 185D220F D45A411B
09BED541 27F38EF5 1CC01D25 76D559AE D9284A74 8B52856D
BCBBF677 0F444401 D0AD542C 67BA06AC A9030203 010001A3
78307630 0F060355 1D130101 FF040530 030101FF 30230603
551D1104 1C301A82 18617573 6E6D6C2D 33383235 2D30312E
63697363 6F2E636F 6D301F06 03551D23 04183016 801403E1
5EAABA47 79F6C70C FBC61B08 90B26C2E 3D4E301D 0603551D
0E041604 1403E15E AABA4779 F6C70CFB C61B0890 B26C2E3D
4E300D06 092A8648 86F70D01 01040500 03818100 6938CEA4
2E56CDFF CF4F2A01 BCD585C7 D6B01665 595C3413 6B7A7B6C
F0A14383 4DA09C30 FB621F29 8A098FA4 F3A7F046 595F51E6
7C038112 0934A369 D44C0CF4 718A8972 2DA33C43 46E35DC6
5DCAE7E0 B0D85987 A0D116A4 600C0C60 71BB1136 486952FC
55DE6A96 1135C9D6 8C5855ED 4CD3AE55 BDA966D4 BE183920
```

```
88A8A55E quit username admin privilege 15 secret 5
$1$jm6N$2xNfhupbAinq3BQZMRzrW0 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/ ! 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 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 ! !--- WebVPN Gateway webvpn gateway
WidgetSSLVPNGW1 hostname ausnml-3825-01 ip address
192.168.0.37 port 443 http-redirect port 80 ssl
trustpoint ausnml-3825-01_Certificate inservice ! webvpn
context SalesContext ssl authenticate verify all ! !---
Identify resources for the SSL VPN session url-list
"InternalWebServers" heading "WidgetWebServers" url-text
"WidgetWeb" url-value "http://172.22.1.30" url-text
"OWA" url-value "http://172.22.1.50/exchange" ! nbns-
list NBNSServers nbns-server 172.22.1.30 ! !--- Identify
the policy which controls the resources available policy
group policy_1 url-list "InternalWebServers" nbns-list
"NBNSServers" functions file-access functions file-
browse functions file-entry hide-url-bar citrix enabled
default-group-policy policy_1 gateway WidgetSSLVPNGW1
max-users 2 inservice ! end
```

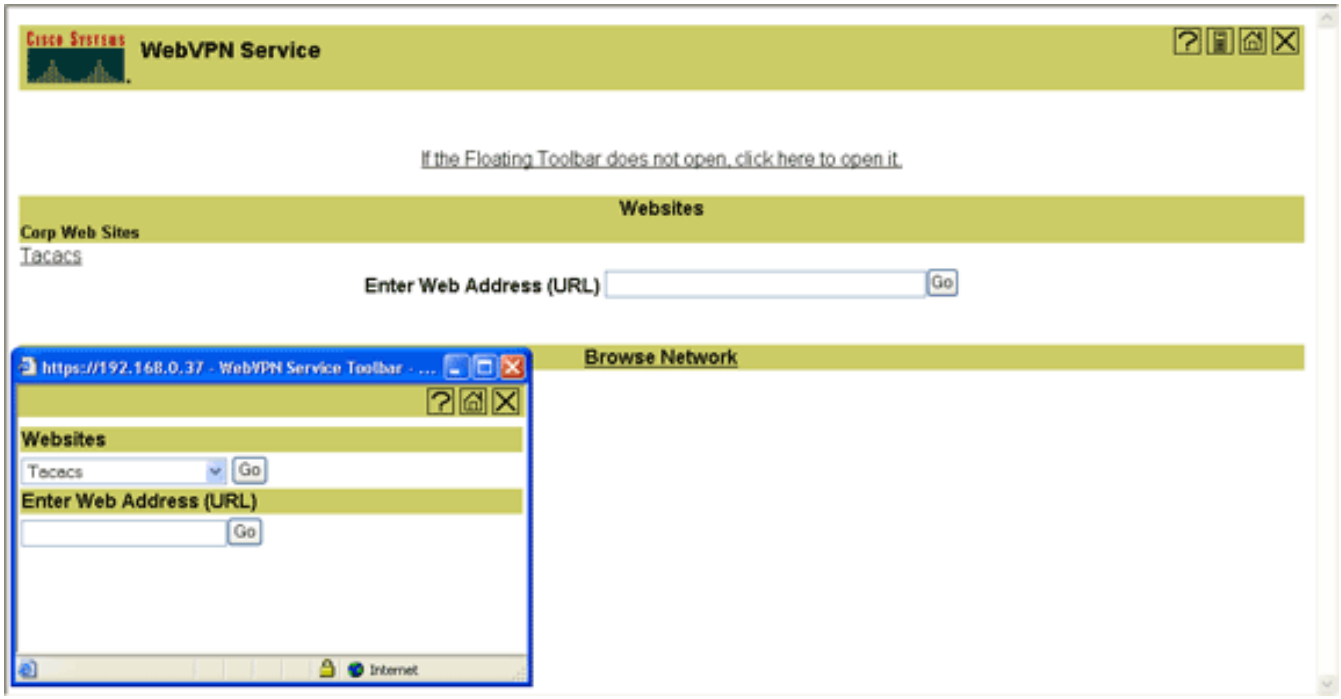
다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

절차

컨피그레이션이 제대로 작동하는지 확인하려면 다음 절차를 완료하십시오.

- 사용자와 함께 구성을 테스트합니다. SSL ***지원 웹 브라우저에 https://WebVPN_Gateway_IP_Address***를 입력합니다. 여기서 *WebVPN_Gateway_IP_Address*는 WebVPN 서비스의 IP 주소입니다. 인증서를 수락하고 사용자 이름과 암호를 입력한 후 이 이미지와 유사한 화면이 나타납니다
  .



- SSL VPN 세션을 확인합니다. SDM 애플리케이션 내에서 **Monitor**(모니터링) 버튼을 클릭한 다음 **VPN Status(VPN 상태)를 클릭합니다**. WebVPN**(All Contexts)**을 확장하고 적절한 컨텍스트를 확장한 다음 **Users**(사용자)를 **선택합니다**.
- 오류 메시지를 확인합니다. SDM 애플리케이션 내에서 **Monitor** 버튼을 클릭하고 **Logging**을 클릭한 다음 Syslog 탭**을** 클릭합니다.
- 디바이스에 대해 실행 중인 컨피그레이션을 봅니다. SDM 응용 프로그램 내에서 구성 단추**를** 클릭한 다음 추가 작업**을 클릭합니다**. Configuration **Management(컨피그레이션 관리)**를 확장하고 Config **Editor(컨피그레이션 편집기)를** 선택합니다.

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.

참고: 복사가 진행되는 동안 **Copy File to Server** 명령을 중단하거나 다른 창으로 이동하지 마십시오. 작업을 중단하면 불완전한 파일이 서버에 저장될 수 있습니다.

참고: 사용자는 WebVPN 클라이언트를 사용하여 새 파일을 업로드 및 다운로드할 수 있지만 WebVPN의 CIFS(Common Internet File System)에서 Copy File to Server 명령을 사용하여 파일을 덮어쓸 수 없습니다. 사용자가 서버의 파일을 바꾸려고 하면 이 메시지가 표시됩니다.

```
Unable to add the file
```

절차

컨피그레이션 문제를 해결하려면 다음 단계를 완료하십시오.

1. 클라이언트가 팝업 차단을 비활성화하는지 확인합니다.
2. 클라이언트가 쿠키를 사용하도록 설정했는지 확인합니다.
3. 클라이언트가 Netscape, Internet Explorer, Firefox 또는 Mozilla 웹 브라우저를 사용하는지 확인합니다.

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

- Cisco IOS SSLVPN
- Cisco IOS SSLVPN Q&A
- SDM을 사용하는 씬 클라이언트 SSL VPN(WebVPN) IOS 구성 예
- SDM 컨피그레이션이 포함된 IOS의 SSL VPN 클라이언트(SVC) 예
- 기술 지원 및 문서 – Cisco Systems