ASDM 및 NTLMv1 컨피그레이션을 사용하는 ASA with WebVPN 및 Single Sign-on 예

목차

소개

이 문서에서는 NTLMv1(NT LAN Manager version 1)을 실행하는 Windows Active Directory에 대한 추가 로그인 검증이 필요한 서버에 WebVPN 사용자 로그인 자격 증명 및 보조 인증을 자동으로 전달하도록 Cisco ASA(Adaptive Security Appliance)를 구성하는 방법에 대해 설명합니다. 이 기능을 SSO(Single-Sign-On)라고 합니다. 특정 WebVPN 그룹에 대해 구성된 링크를 이 사용자 인증 정보를 전달할 수 있는 기능을 제공하므로 여러 인증 프롬프트가 제거됩니다.이 기능은 전역 또는 사용자 구성 레벨에서도 사용할 수 있습니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 대상 VPN 사용자에 대한 NTLMv1 및 Windows 권한이 구성되어 있는지 확인합니다.Windows 도메인 액세스 권한에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 7.1(1)
- Cisco ASDM(Adaptive Security Device Manager) 5.1(2)
- Microsoft IIS(인터넷 정보 서비스)

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.

구성

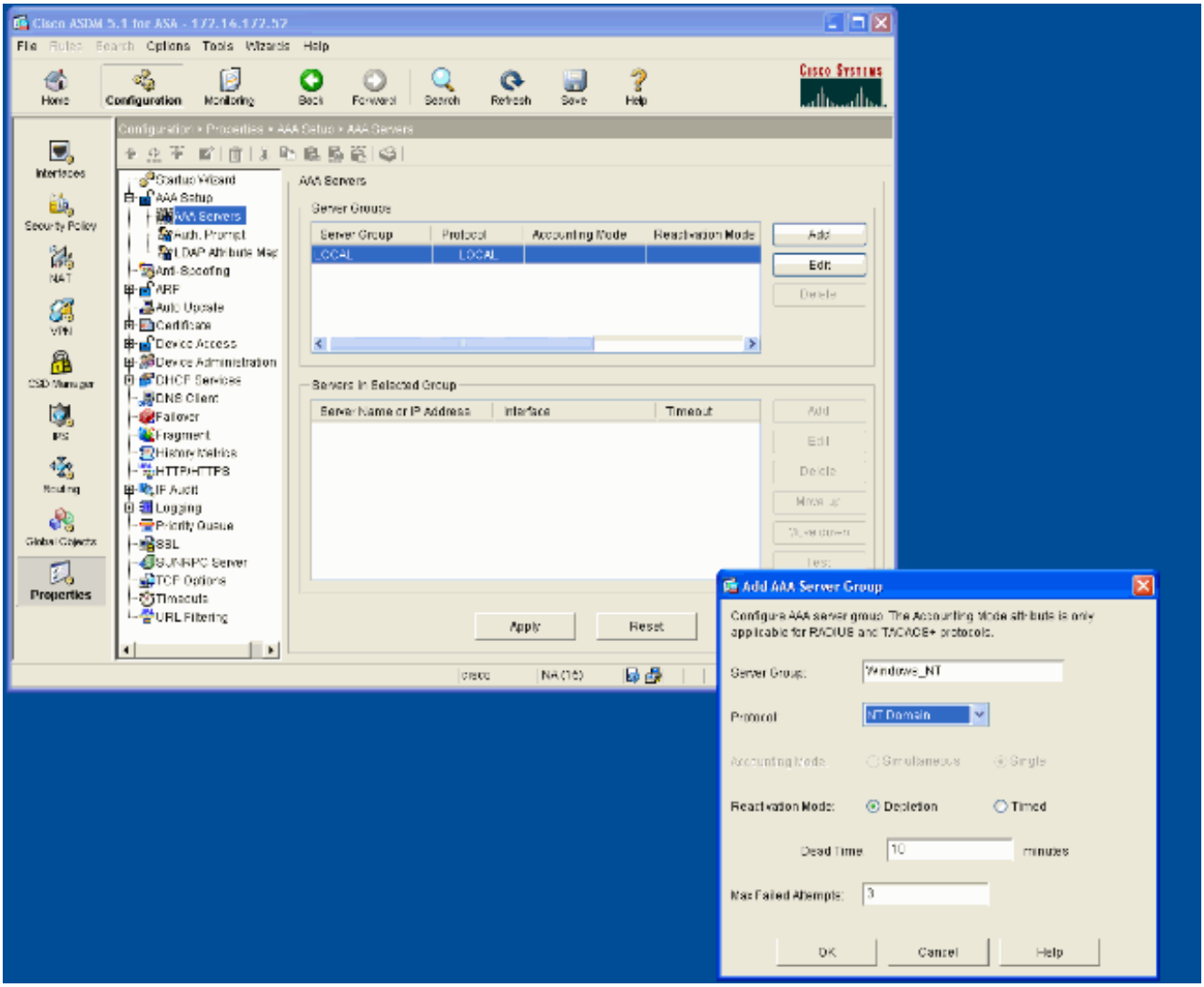
이 섹션에서는 ASA를 SSO가 포함된 WebVPN 서버로 구성하는 정보를 제공합니다.

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

Windows 도메인 인증을 위한 AAA 서버 추가

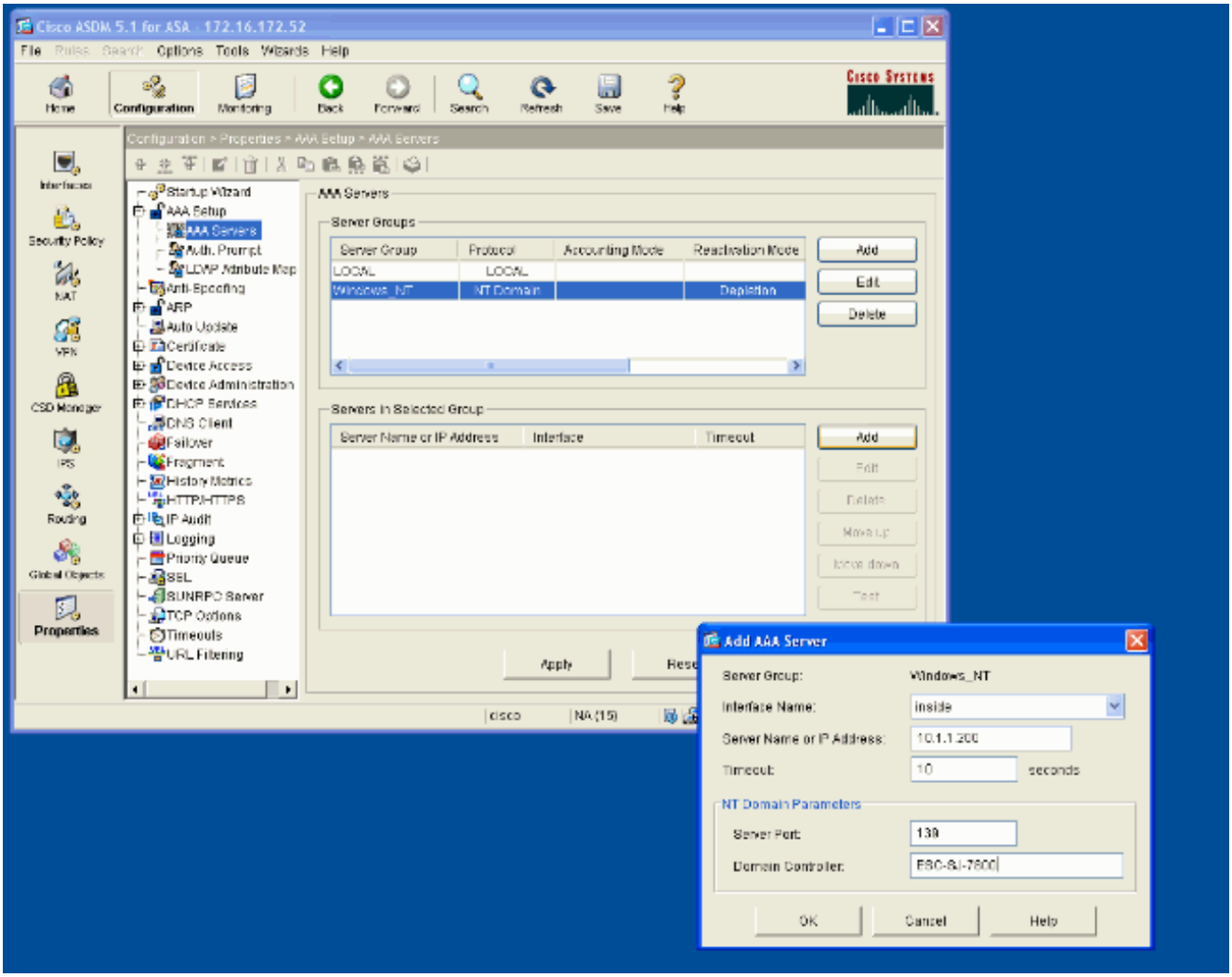
인증에 도메인 컨트롤러를 사용하도록 ASA를 구성하려면 다음 단계를 완료합니다.

1. Configuration **> Properties > AAA Setup > AAA Servers를 선택하고 Add를 클릭합니다** .Windows_NT와 같은 서버 그룹의 이름을 제공하고 **NT 도메인**을 프로토콜로 선택합니다 .



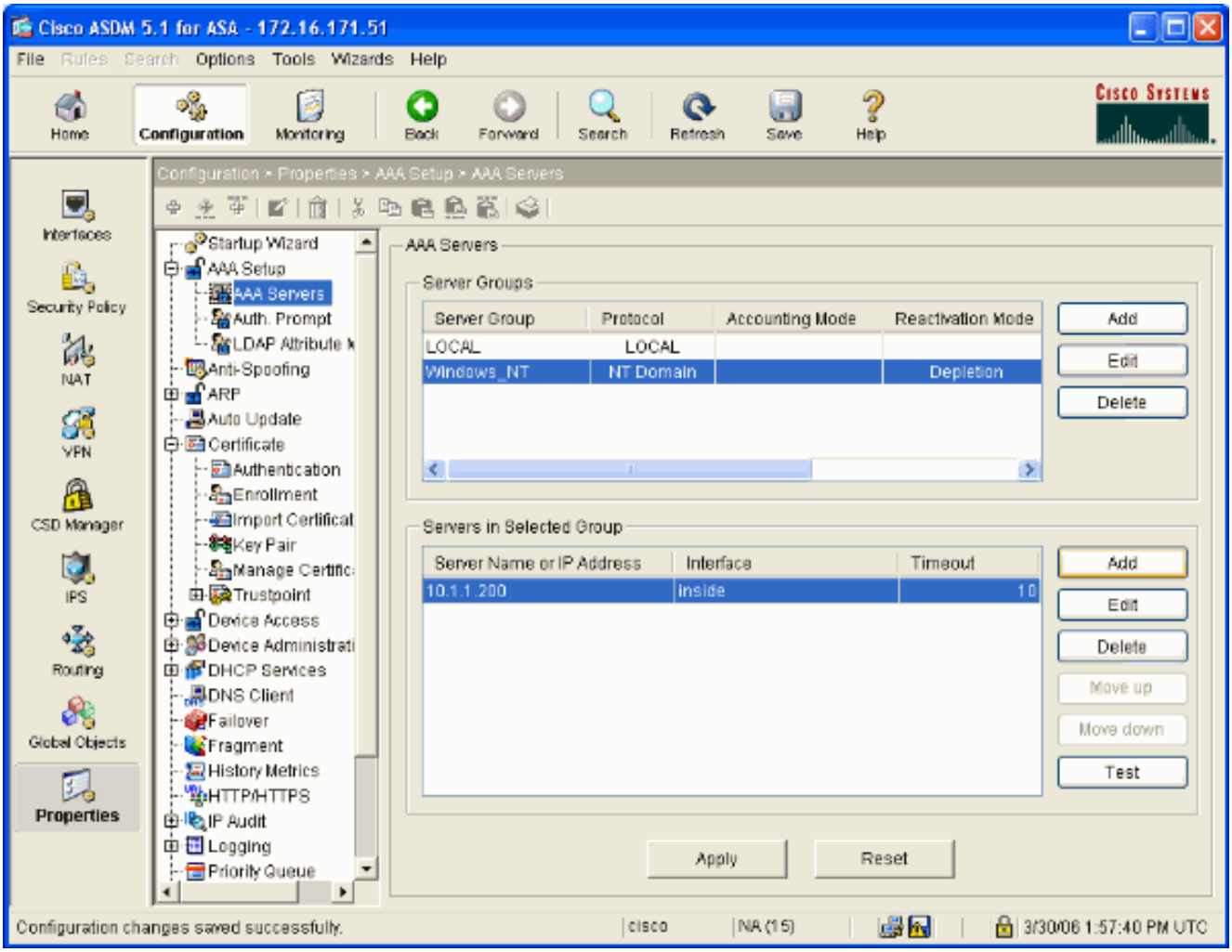
2. Windows 서버를 추가합니다.새로 생성된 그룹을 선택하고 Add(추가)를 **클릭합니다**.서버가 있는 인터페이스를 선택하고 IP 주소 및 도메인 컨트롤러 이름을 입력합니다.도메인 컨트롤러 이름이 모든 대문자로 입력되었는지 확인합니다.완료되면 **OK**(확인)를 클릭합니다

.



이 창에는 완료된 AAA 컨피그레이션이 표시됩니다

.



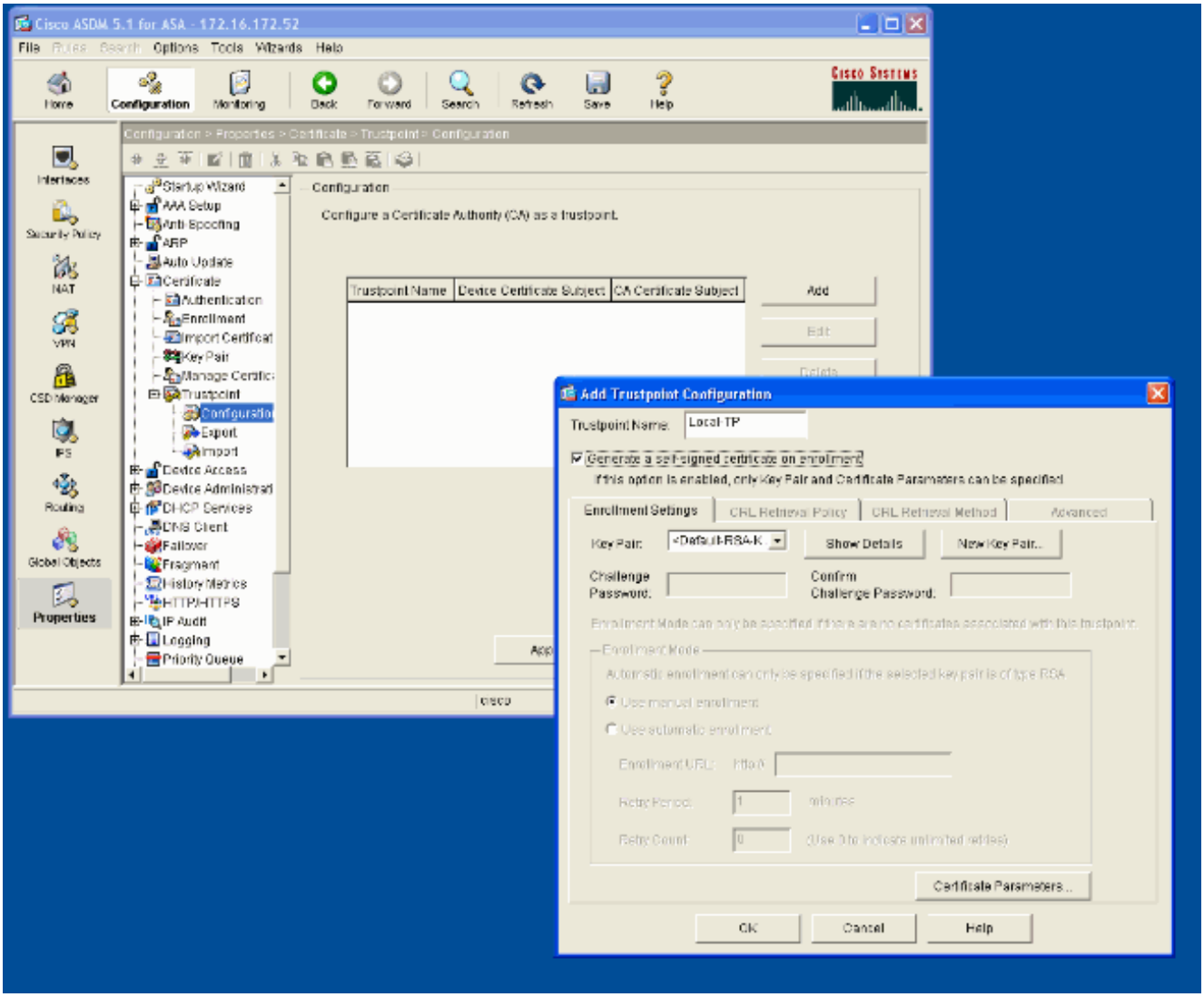
자체 서명 인증서 생성

자체 서명 인증서를 사용하도록 ASA를 구성하려면 다음 단계를 완료합니다.

참고: 이 예에서는 자체 서명된 인증서가 단순하게 사용됩니다.외부 CA에 등록하는 것과 같은 다른 인증서 등록 옵션에 대해서는 인증서 구성을 참조하십시오.

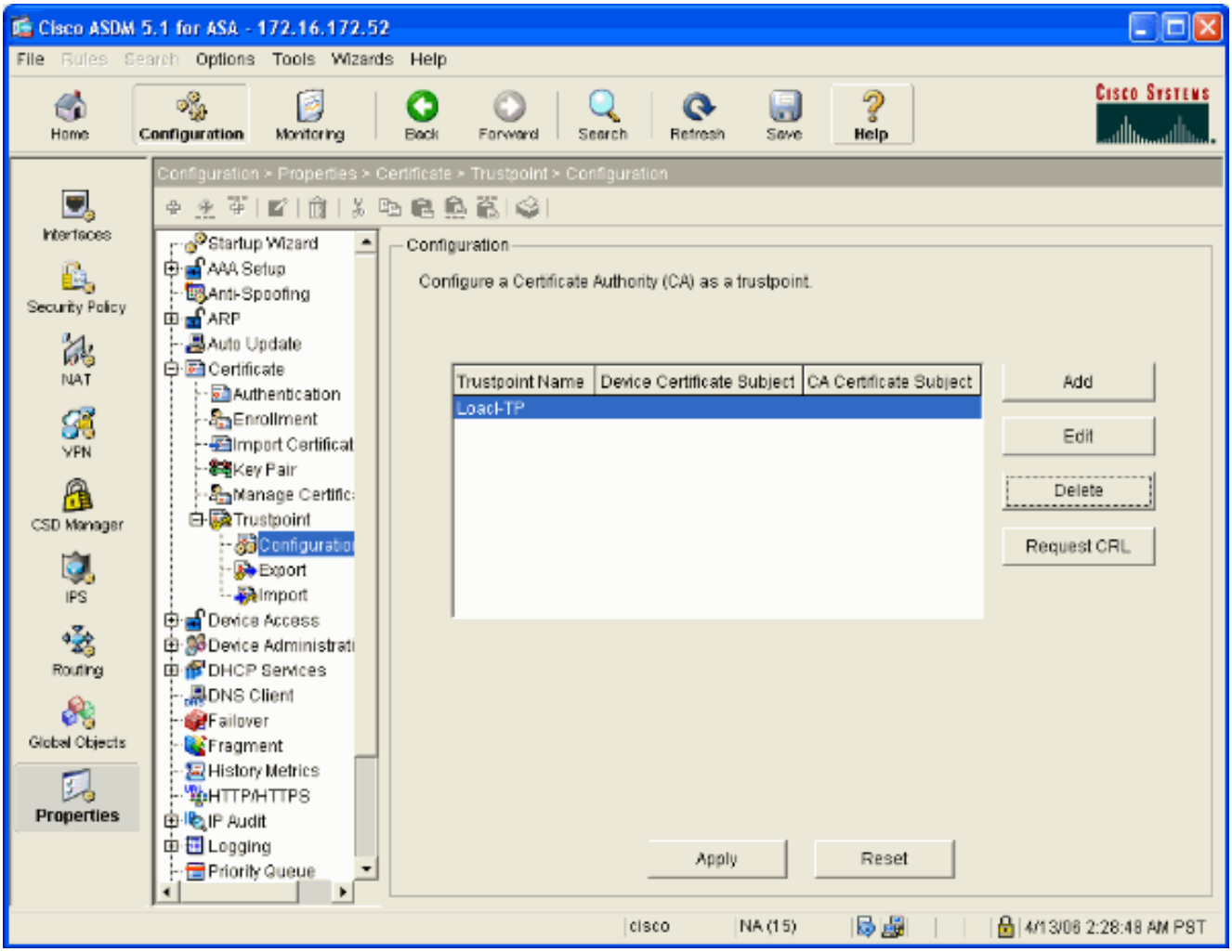
1. Configuration **> Properties > Certificate > Trustpoint > Configuration을 선택하고 Add를 클릭합니다**.
2. 표시되는 창에 Local-TP와 같은 신뢰 지점 이름을 입력하고 **Generate a self-signed certificate on enrollment를** 선택합니다.다른 옵션은 기본 설정으로 남겨둘 수 있습니다.완료되면 **OK**(확인)를 클릭합니다

.



이 창에는 완료된 신뢰 지점 컨피그레이션이 표시됩니다

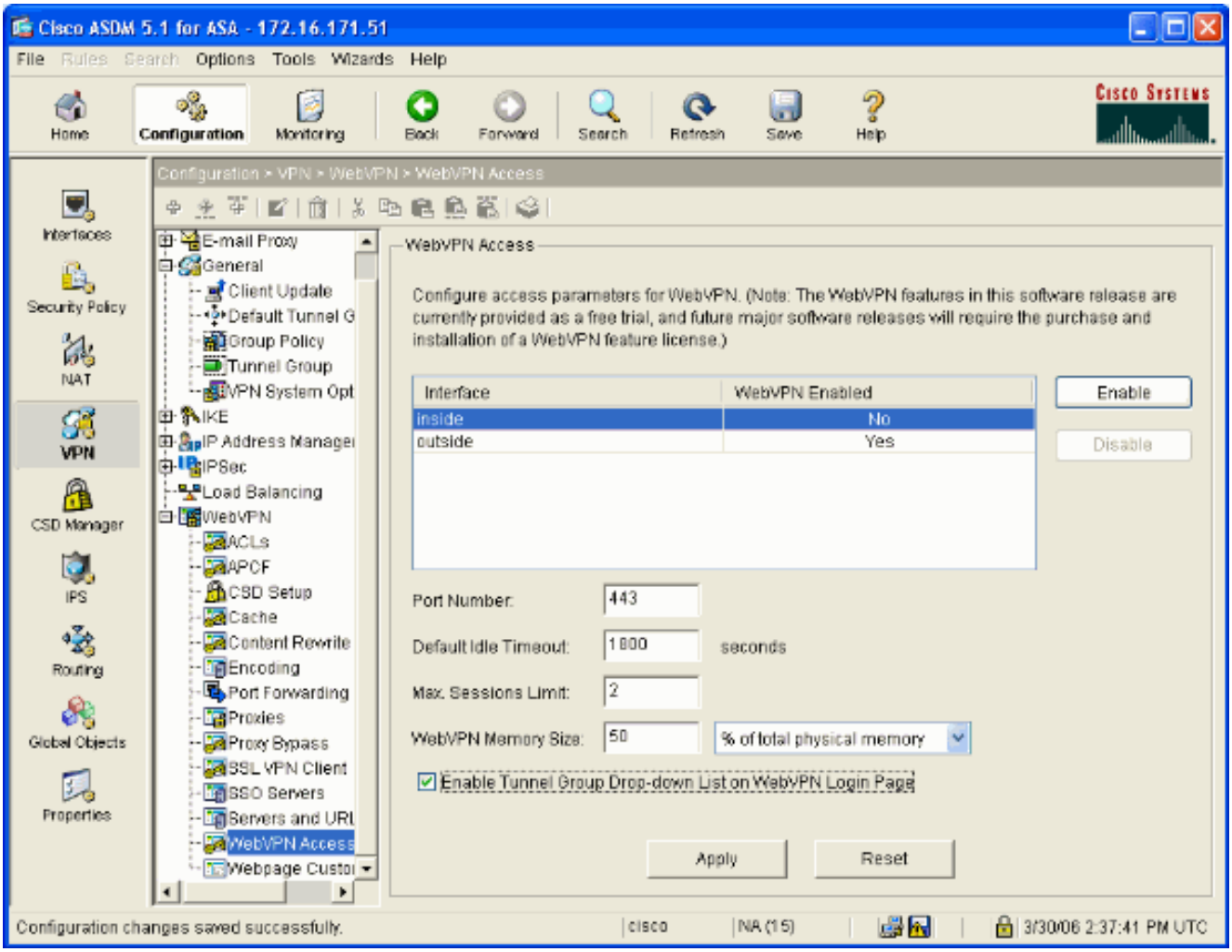
.



외부 인터페이스에서 WebVPN 활성화

네트워크 외부의 사용자가 WebVPN을 사용하여 연결할 수 있도록 하려면 다음 단계를 완료하십시오.

1. Configuration **> VPN > WebVPN > WebVPN Access를 선택합니다**.
2. 원하는 인터페이스를 선택하고 **Enable**(활성화)을 클릭한 다음 WebVPN **Login Page(WebVPN 로그인 페이지)에서 Enable Tunnel Group Drop-down List(터널 그룹 드롭다운 목록 활성화)를 선택합니다.참고:** 동일한 인터페이스가 WebVPN 및 ASDM 액세스에 사용되는 경우 포트 80에서 새 포트(예: 8080)로 ASDM 액세스에 대한 기본 포트를 변경해야 합니다.이는 Configuration(컨피그레이션) **> Properties(속성) > Device Access(디바이스 액세스) > HTTPS/ASDM에서 수행됩니다.참고:** 사용자가 https://**<ip_address>**가 아닌 **http://<ip_address>**로 이동하는 경우 사용자를 포트 443으로 자동으로 리디렉션할 수 있습니다.Configuration **> Properties > HTTP/HTTPS**를 선택하고 원하는 인터페이스를 선택한 다음 **Edit**를 클릭하고 Redirect HTTP to HTTPS(**HTTP를 HTTPS로 리디렉션)를 선택합니다**
.

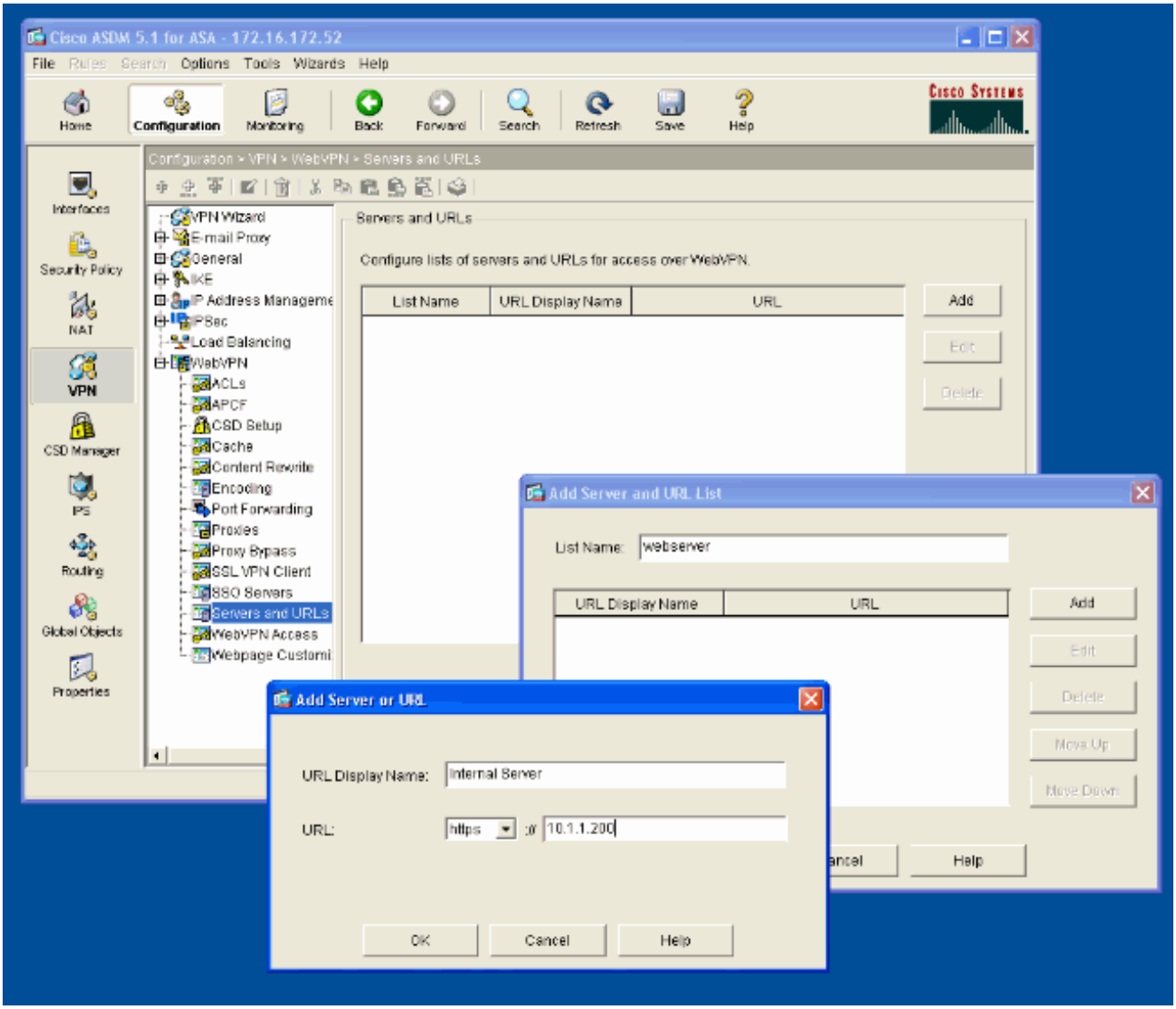


내부 서버의 URL 목록 구성

WebVPN 사용자에게 액세스 권한을 부여할 서버가 포함된 목록을 생성하려면 다음 단계를 완료합니다.

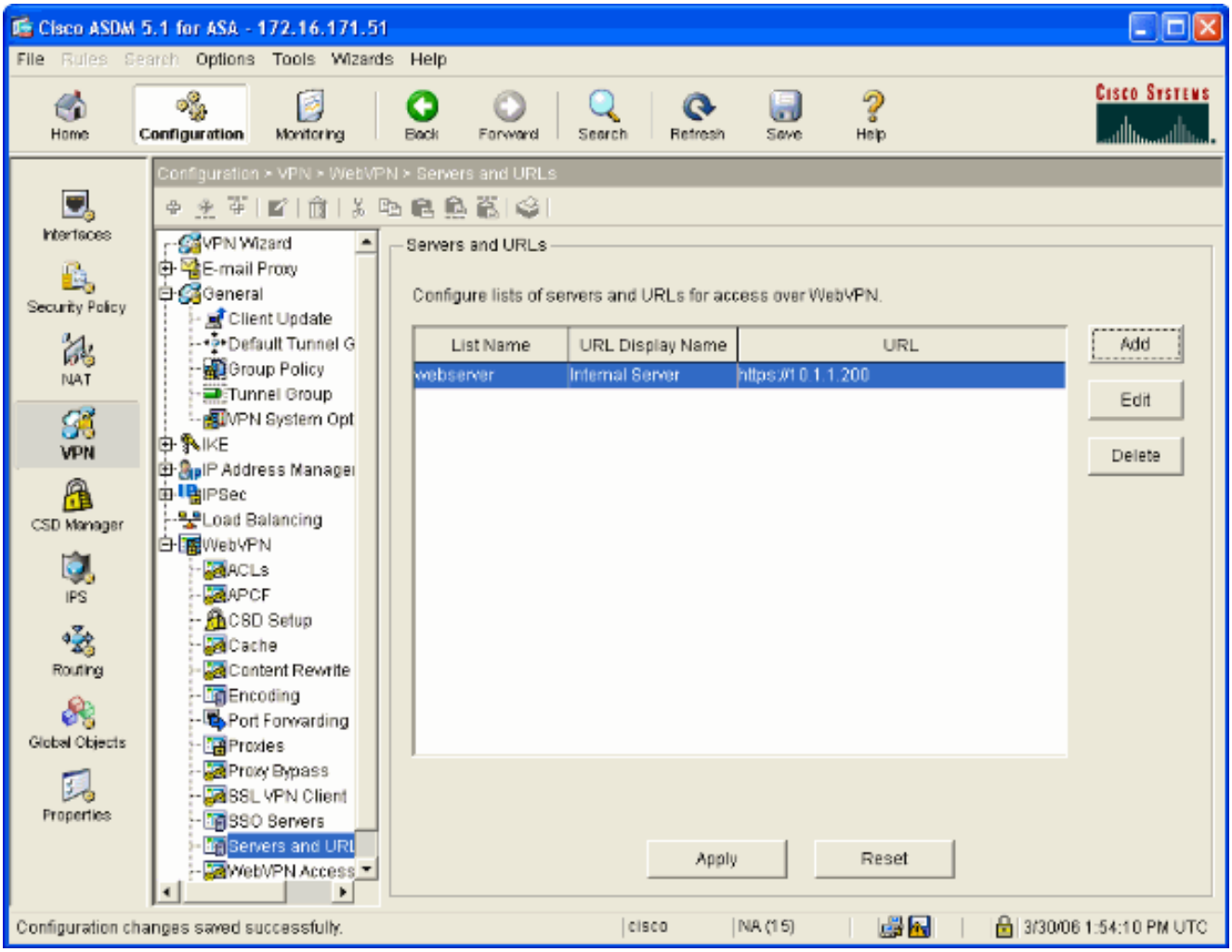
1. Configuration(**구성) > VPN > WebVPN > Servers and URLs(서버 및 URL)를 선택하고 Add(추가)를 클릭합니다**.
2. URL 목록의 이름을 입력합니다.이 이름은 최종 사용자에게 표시되지 않습니다.Add(**추가)를 클릭합니다**.
3. 사용자에게 표시할 URL 표시 이름을 입력합니다.서버의 URL 정보를 입력합니다.이는 일반적으로 서버에 액세스하는 방법이어야 합니다

   .



4. **확인**, **확인**, 적용을 **클릭합니다**

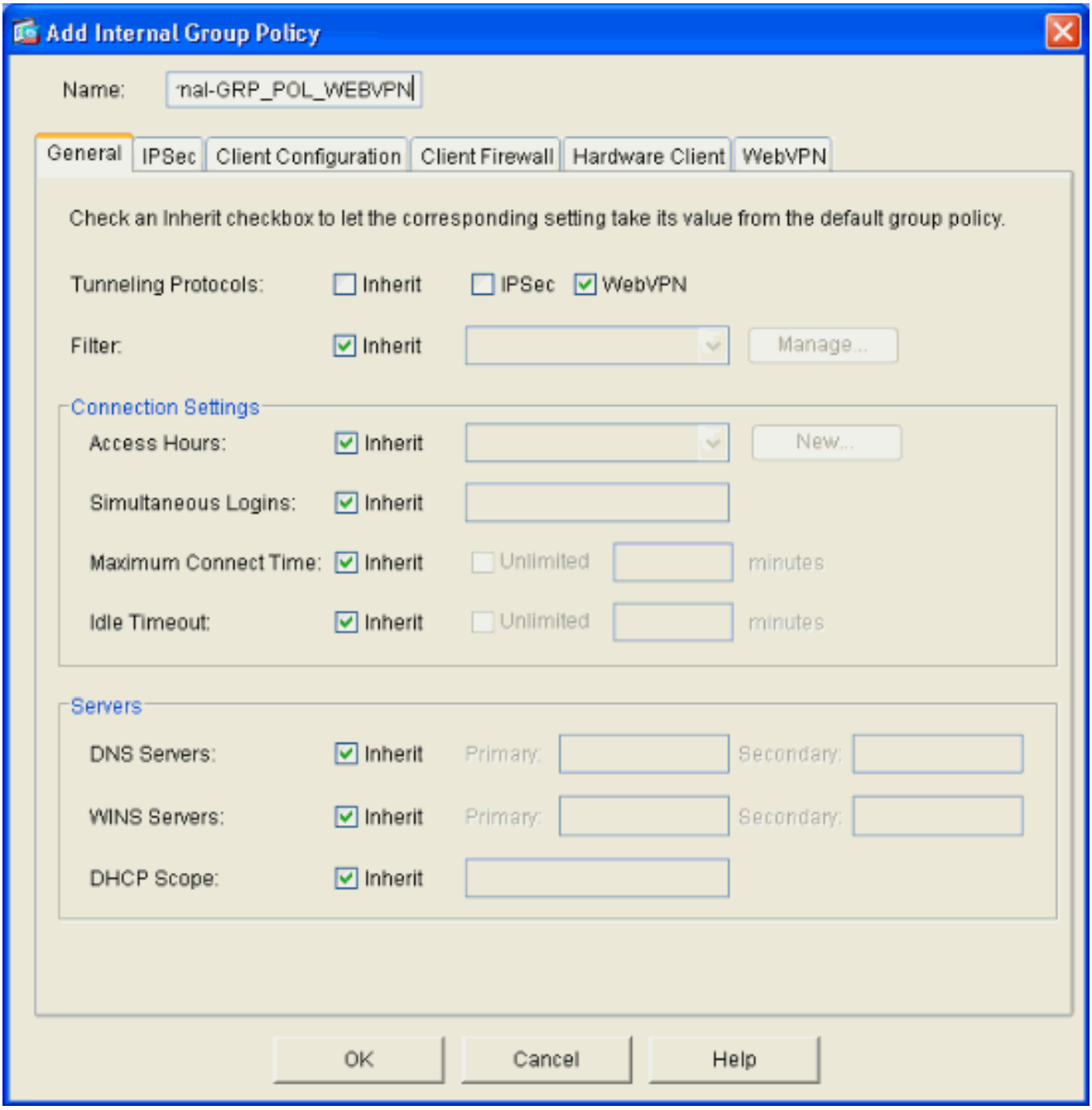
.



내부 그룹 정책 구성

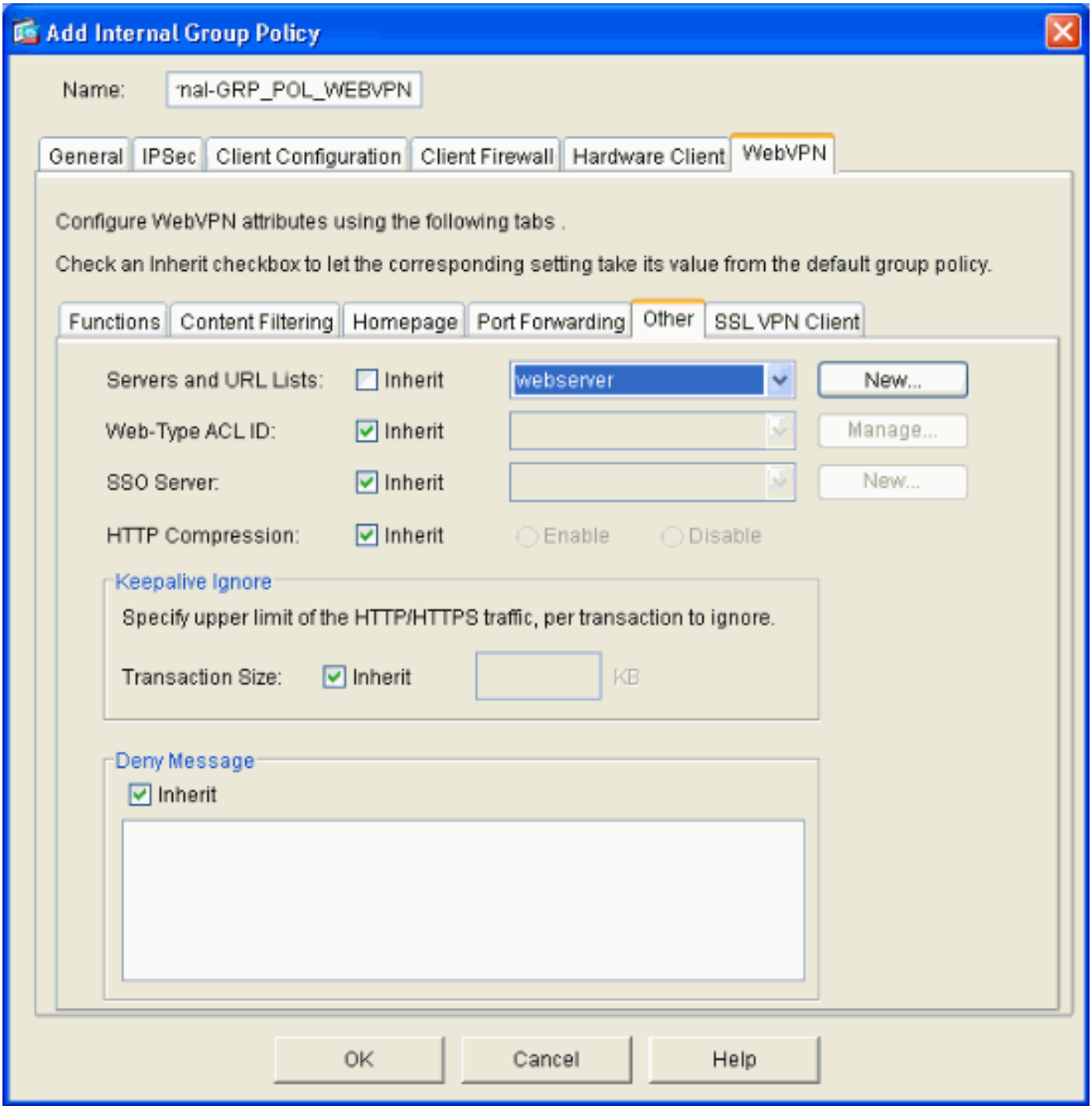
WebVPN 사용자에 대한 그룹 정책을 구성하려면 다음 단계를 완료합니다.

1. Configuration(**컨피그레이션) > VPN > General(일반) > Group Policy(그룹 정책)를** 선택하고 **Add(추가)**를 클릭한 다음 Internal **Group Policy(내부 그룹 정책)를 선택합니다**.
2. General(일반) 탭에서 Internal-Group_POL_WEBVPN과 같은 정책 이름을 지정합니다.그런 다음 Tunneling **Protocols** 옆에 있는 Inherit(상속)를 선택 취소하고 WebVPN을 **선택합니다**
.



3. WebVPN 탭에서 **기타** 하위 탭을 선택합니다.Inherit 옆에 있는 Servers and URL Lists(서버 및 URL 목록)를 선택 취소하고 드롭다운 목록에서 구성한 URL List(URL 목록)를 선택합니다.완료되면 **OK**(확인)를 클릭합니다

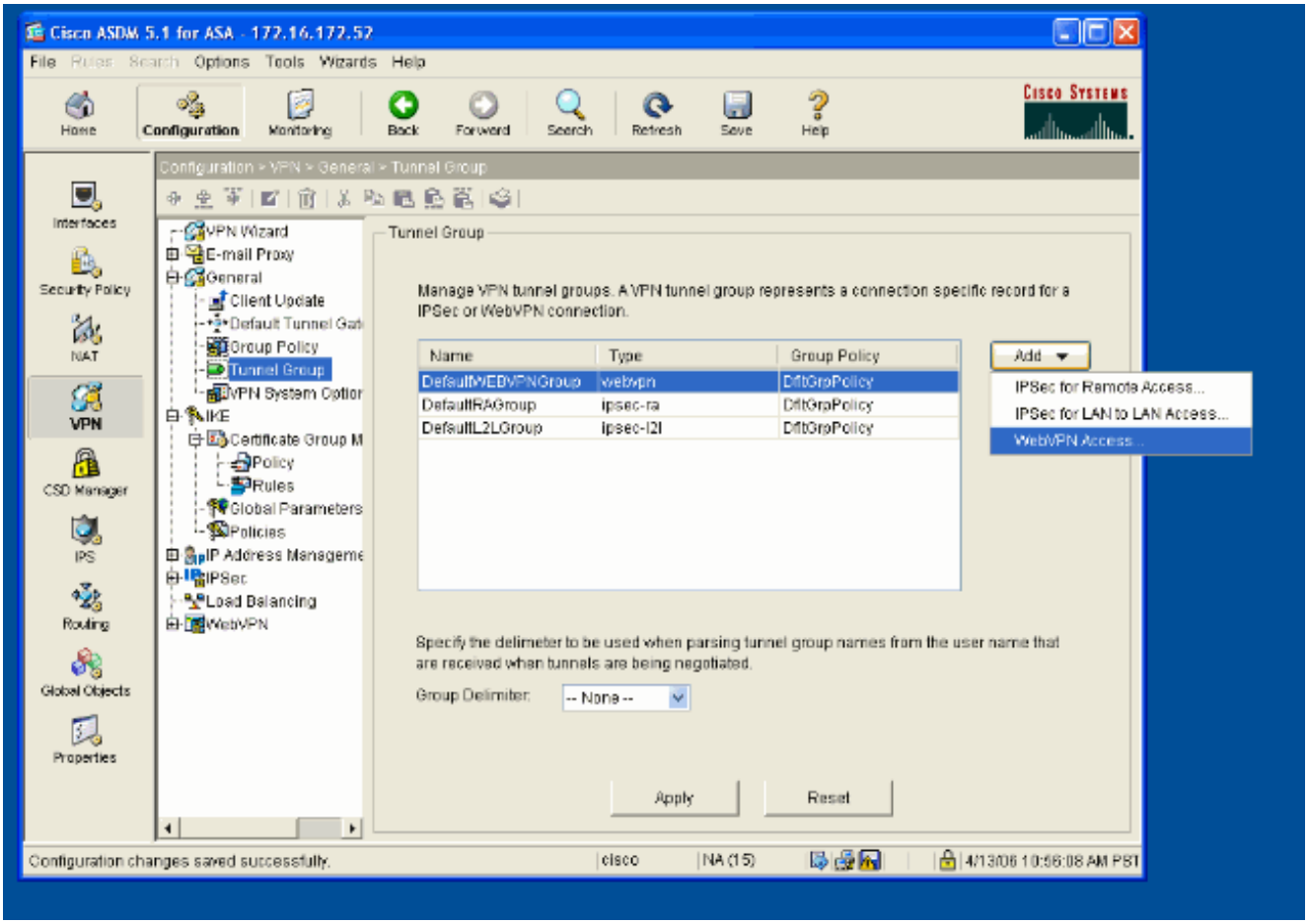
.



터널 그룹 구성

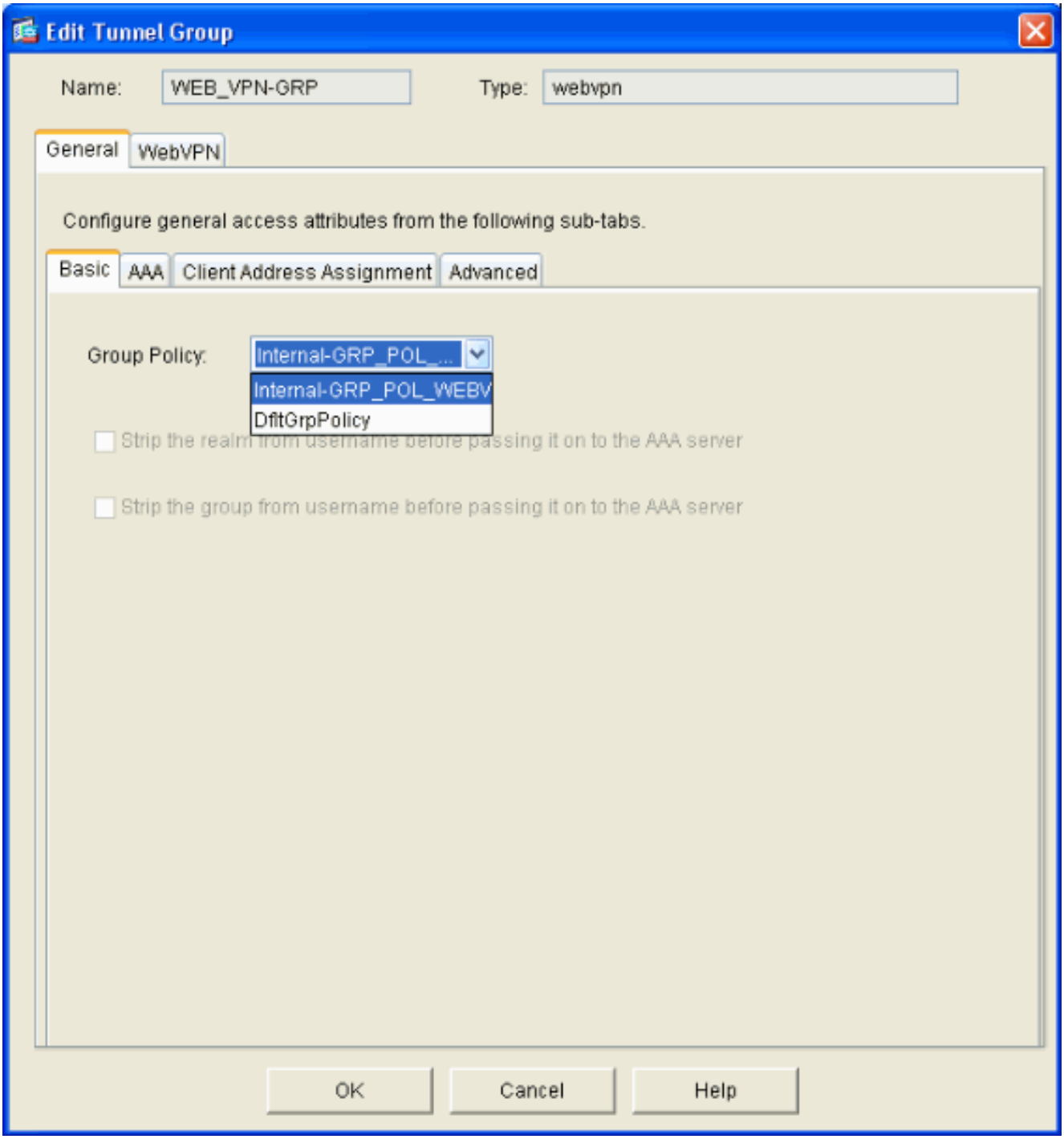
WebVPN 사용자를 위한 터널 그룹을 구성하려면 다음 단계를 완료합니다.

1. Configuration(**구성) > VPN > General(일반) > Tunnel Group(터널 그룹)**을 선택하고 **Add(추가)**를 클릭하고 **WebVPN Access..(WebVPN 액세스..)**를 선택합니다
.



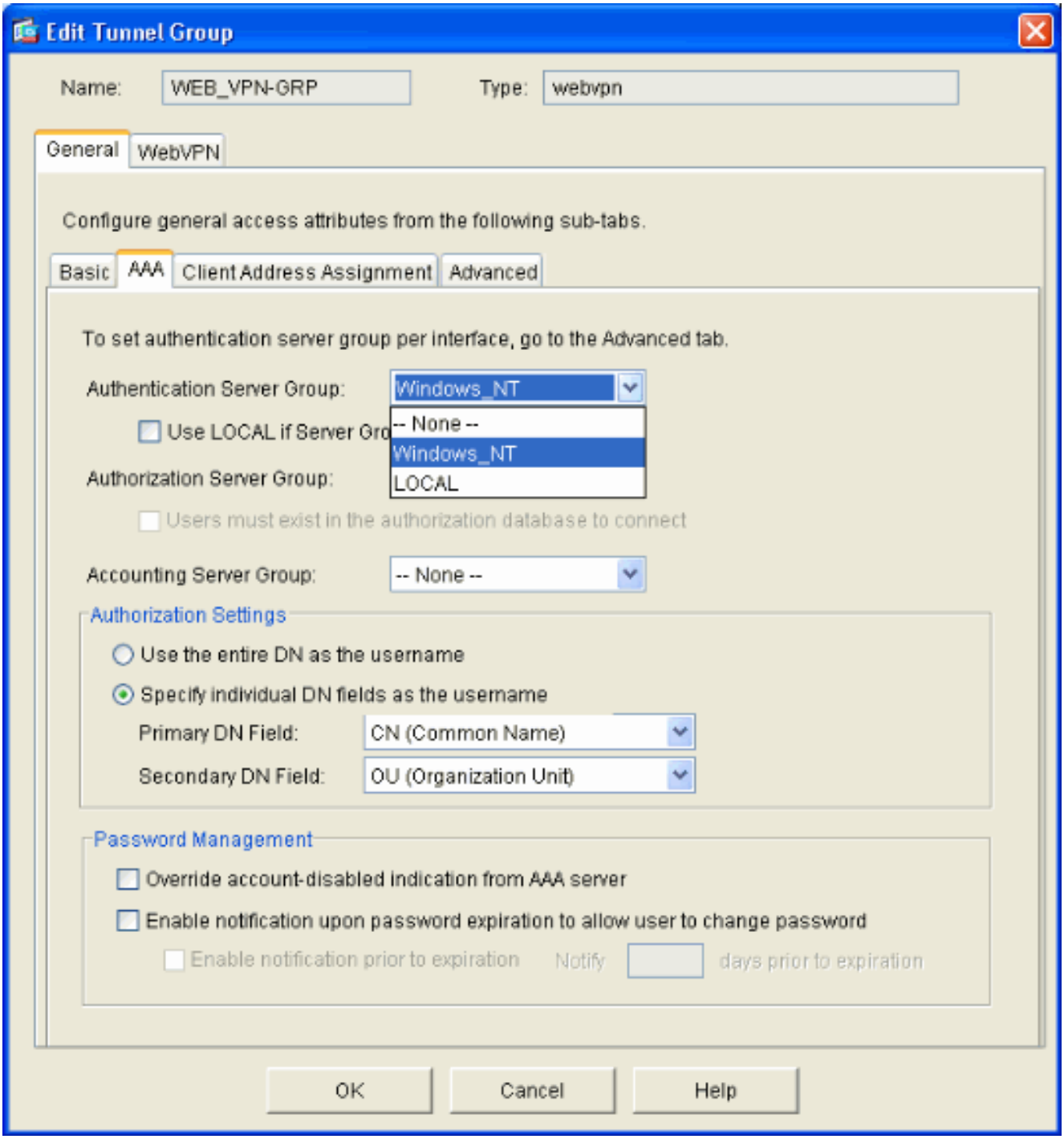
2. WEB_VPN-GRP와 같은 터널 그룹의 이름을 입력합니다.Basic(기본) 탭에서 생성한 그룹 정책을 선택하고 그룹 Type(유형)이 webvpn인지 **확인합니다**

.



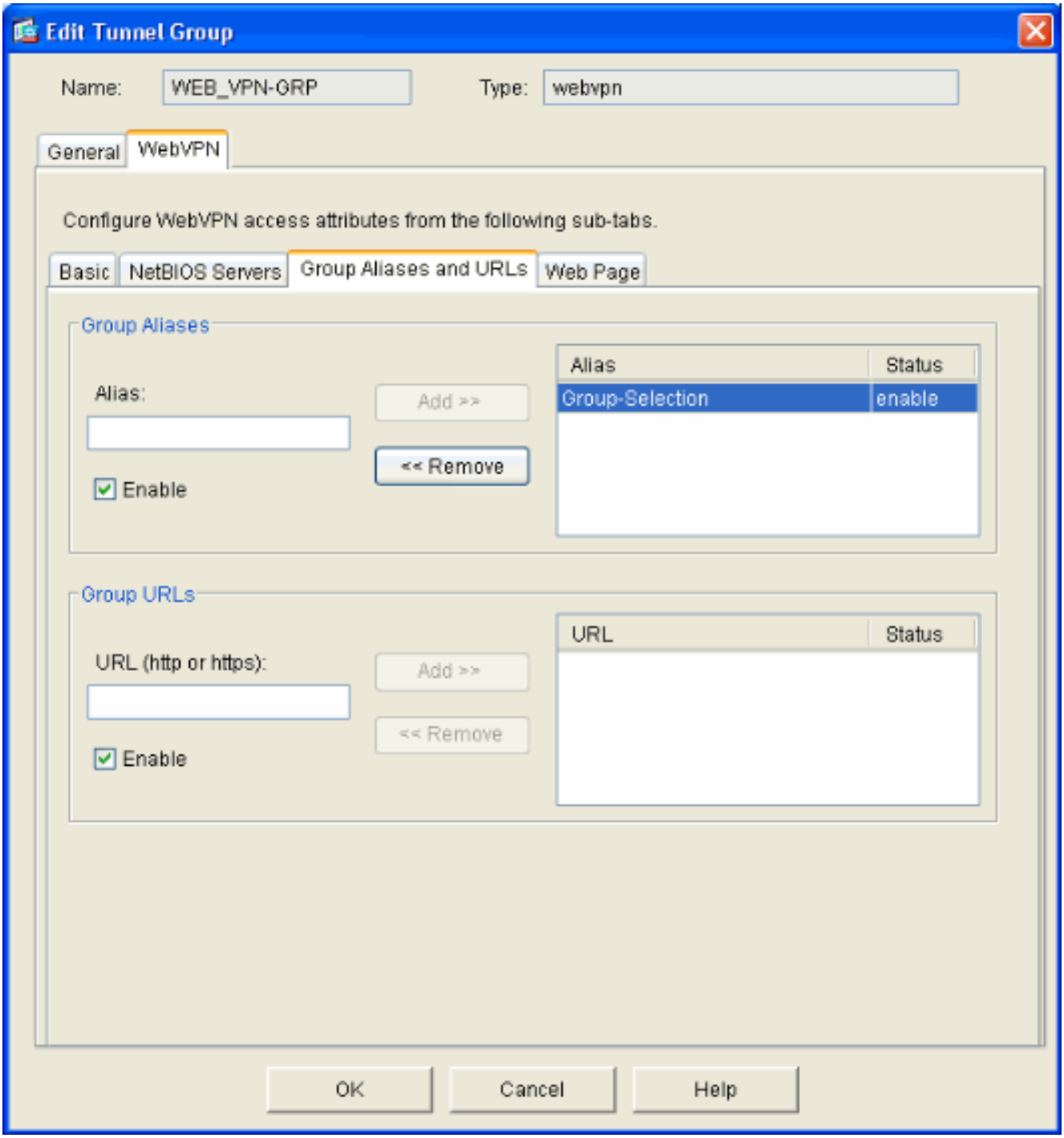
3. AAA 탭으로 이동합니다.Authentication Server Group(인증 서버 그룹)의 경우 도메인 컨트롤러와의 NTLMv1 인증을 활성화하기 위해 구성한 그룹을 선택합니다.**선택 사항:**Use **LOCAL if Server Group Fails(서버 그룹**이 구성된 AAA 그룹이 실패할 경우 LOCAL 사용자 데이터베이스 사용을 활성화하려면 LOCAL 사용)을 선택합니다.나중에 문제를 해결하는 데 도움이 될 수 있습니다

.



4. WebVPN 탭으로 이동한 다음 **Group Aliases and URLs** 하위 탭**으로** 이동합니다.
5. Group Aliases(그룹 별칭) 아래에 별칭을 입력하고 Add(추가)를 **클릭합니다**.이 별칭은 로그인 시 WebVPN 사용자에게 표시되는 드롭다운 목록에 나타납니다

.



6. OK(**확인**)를 클릭한 다음 Apply(적용)를 **클릭합니다**.

서버의 자동 로그온 구성

명령줄로 전환하여 내부 서버에 대해 SSO를 활성화합니다.

참고: 이 단계는 ASDM에서 완료할 수 없으며 명령줄을 사용하여 수행해야 합니다.자세한 내용은 명령줄 인터페이스 액세스를 참조하십시오.

auto-**signon** 명령을 사용하여 사용자에게 액세스 권한을 부여할 네트워크 리소스(예: 서버)를 지정합니다.여기에 단일 서버 IP 주소가 구성되어 있지만 **10.1.1.0 /24**와 같은 네트워크 범위를 지정할 수도 있습니다.자세한 내용은 auto-signon 명령을 참조하십시오.

```
ASA>enable
ASA#configure terminal
```

```
ASA(config)#webvpn
ASA(config-webpvn)#auto-signon allow ip 10.1.1.200 255.255.255.255 auth-type ntlm
ASA(config-webvpn)#quit
ASA(config)#exit
ASA#write memory
```

이 예제 출력에서는 **auto-signon** 명령이 WebVPN에 대해 전역으로 구성됩니다.이 명령은 WebVPN 그룹 컨피그레이션 모드 또는 WebVPN 사용자 이름 컨피그레이션 모드에서도 사용할 수 있습니다 .WebVPN 그룹 컨피그레이션 모드에서 이 명령을 사용하면 특정 그룹으로 제한됩니다.마찬가지로 WebVPN 사용자 이름 컨피그레이션 모드에서 이 명령을 사용하면 개별 사용자로 제한됩니다.자세한 내용은 auto-signon 명령을 참조하십시오.

최종 ASA 컨피그레이션

이 문서에서는 다음 구성을 사용합니다.

ASA 버전 7.1(1)

```
ASA# show running-config
: Saved
:
ASA Version 7.1(1)
!
terminal width 200
hostname ASA
domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.171.51 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
```

```
 domain-name cisco.com
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image disk0:/asdm512.bin
no asdm history enable
arp timeout 14400
route outside 0.0.0.0 0.0.0.0 172.16.171.1 1
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
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

!--- AAA server configuration aaa-server Windows_NT
protocol nt aaa-server Windows_NT host 10.1.1.200 nt-
auth-domain-controller ESC-SJ-7800 !--- Internal group
policy configuration group-policy Internal-
GRP_POL_WEBVPN internal group-policy Internal-
GRP_POL_WEBVPN attributes vpn-tunnel-protocol webvpn
webvpn url-list value webserver username cisco password
Q/odgwmtmVIw4Dcm encrypted privilege 15 aaa
authentication http console LOCAL aaa authentication ssh
console LOCAL aaa authentication enable console LOCAL
http server enable 8181 http 0.0.0.0 0.0.0.0 outside no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart !--- Trustpoint/certificate configuration
crypto ca trustpoint Local-TP enrollment self crl
configure crypto ca certificate chain Local-TP
certificate 31 308201b0 30820119 a0030201 02020131
300d0609 2a864886 f70d0101 04050030 1e311c30 1a06092a
864886f7 0d010902 160d4153 412e6369 73636f2e 636f6d30
1e170d30 36303333 30313334 3930345a 170d3136 30333237
31333439 30345a30 1e311c30 1a06092a 864886f7 0d010902
160d4153 412e6369 73636f2e 636f6d30 819f300d 06092a86
4886f70d 01010105 0003818d 00308189 02818100 e47a29cd
56becf8d 99d6d919 47892f5a 1b8fc5c0 c7d01ea6 58f3bec4
a60b2025 03748d5b 1226b434 561e5507 5b45f30e 9d65a03f
30add0b5 81f6801a 766c9404 9cabcbde 44b221f9 b6d6dc18
496fe5bb 4983927f adabfb17 68b4d22c cddfa6c3 d8802efc
ec3af7c7 749f0aa2 3ea2c7e3 776d6d1d 6ce5f748 e4cda3b7
4f007d4f 02030100 01300d06 092a8648 86f70d01 01040500
03818100 c6f87c61 534bb544 59746bdb 4e01680f 06a88a15
e3ed8929 19c6c522 05ec273d 3e37f540 f433fb38 7f75928e
1b1b6300 940b8dff 69eac16b af551d7f 286bc79c e6944e21
49bf15f3 c4ec82d8 8811b6de 775b0c57 e60a2700 fd6acc16
a77abee6 34cb0cad 81dfaf5a f544258d cc74fe2d 4c298076
294f843a edda3a0a 6e7f5b3c quit !--- Tunnel group
configuration tunnel-group WEB_VPN-GRP type webvpn
tunnel-group WEB_VPN-GRP general-attributes
authentication-server-group Windows_NT default-group-
policy Internal-GRP_POL_WEBVPN tunnel-group WEB_VPN-GRP
webvpn-attributes group-alias Group-Selection enable
telnet timeout 5 ssh timeout 5 console timeout 0 !
class-map inspection_default match default-inspection-
traffic ! ! policy-map global_policy class
inspection_default inspect dns maximum-length 512
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 Configuration webvpn enable outside url-list
webserver "Internal Server" https://10.1.1.200 1 tunnel-
group-list enable auto-signon allow ip 10.1.1.200
255.255.255.255 auth-type ntlm
Cryptochecksum:c80ac5f6232df50fc1ecc915512c3cd6
: end
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

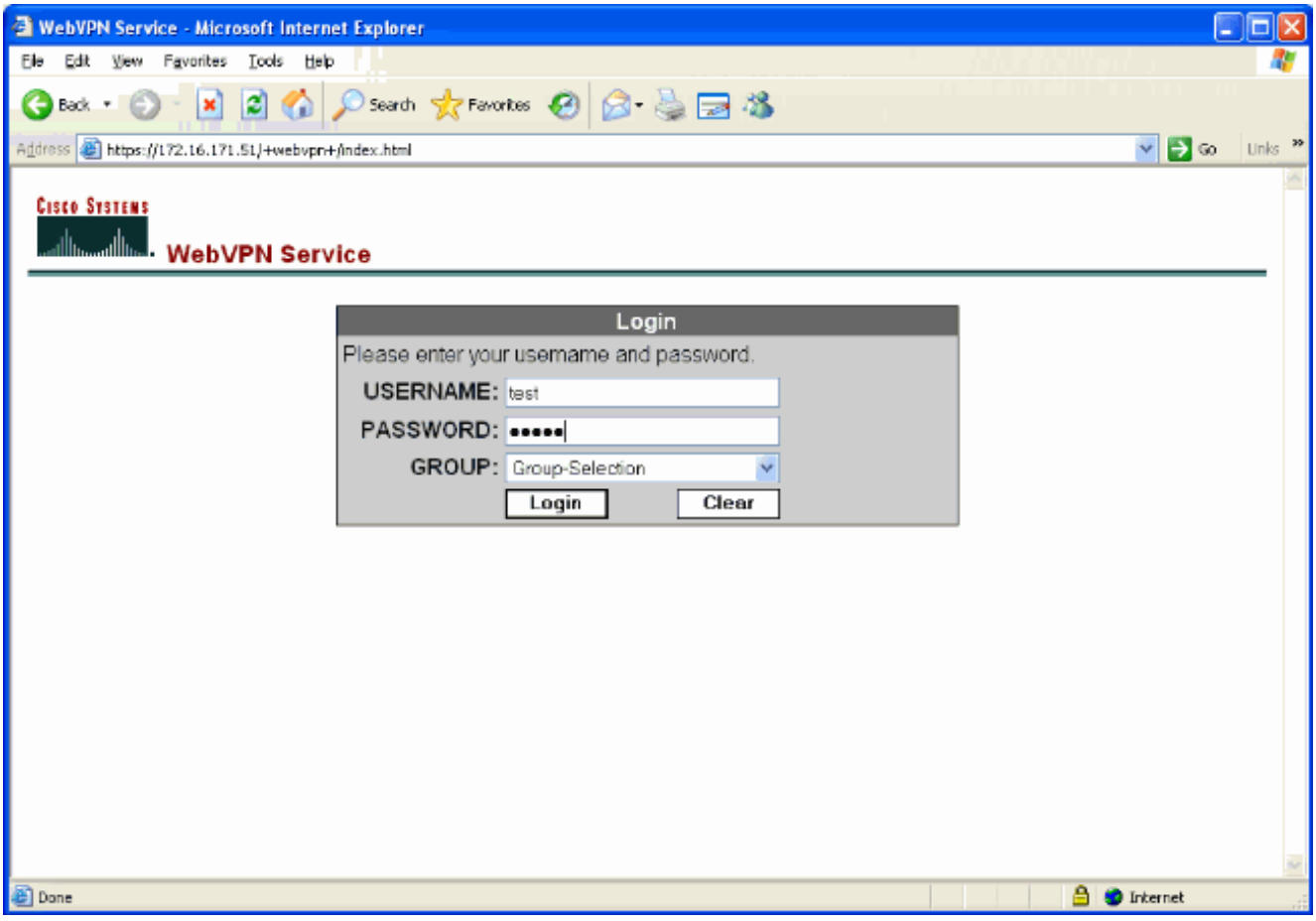
Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

WebVPN 로그인 테스트

사용자로 로그인하여 구성을 테스트합니다.

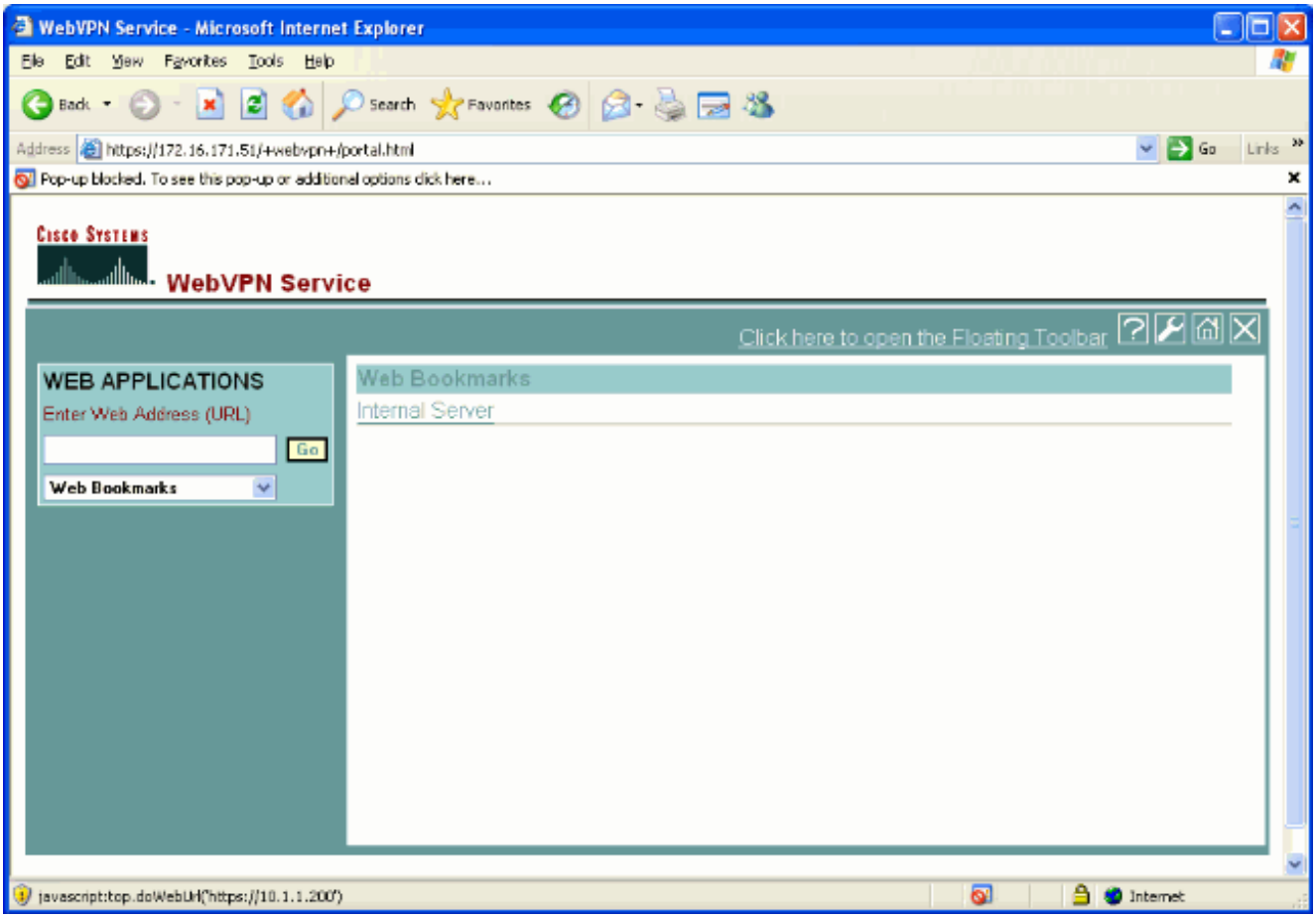
1. NT 도메인의 사용자 정보를 사용하여 ASA에 로그인을 시도합니다.Configure a Tunnel Group(터널 그룹 구성)에서 5단계에서 구성된 그룹 별칭을 선택합니다

.



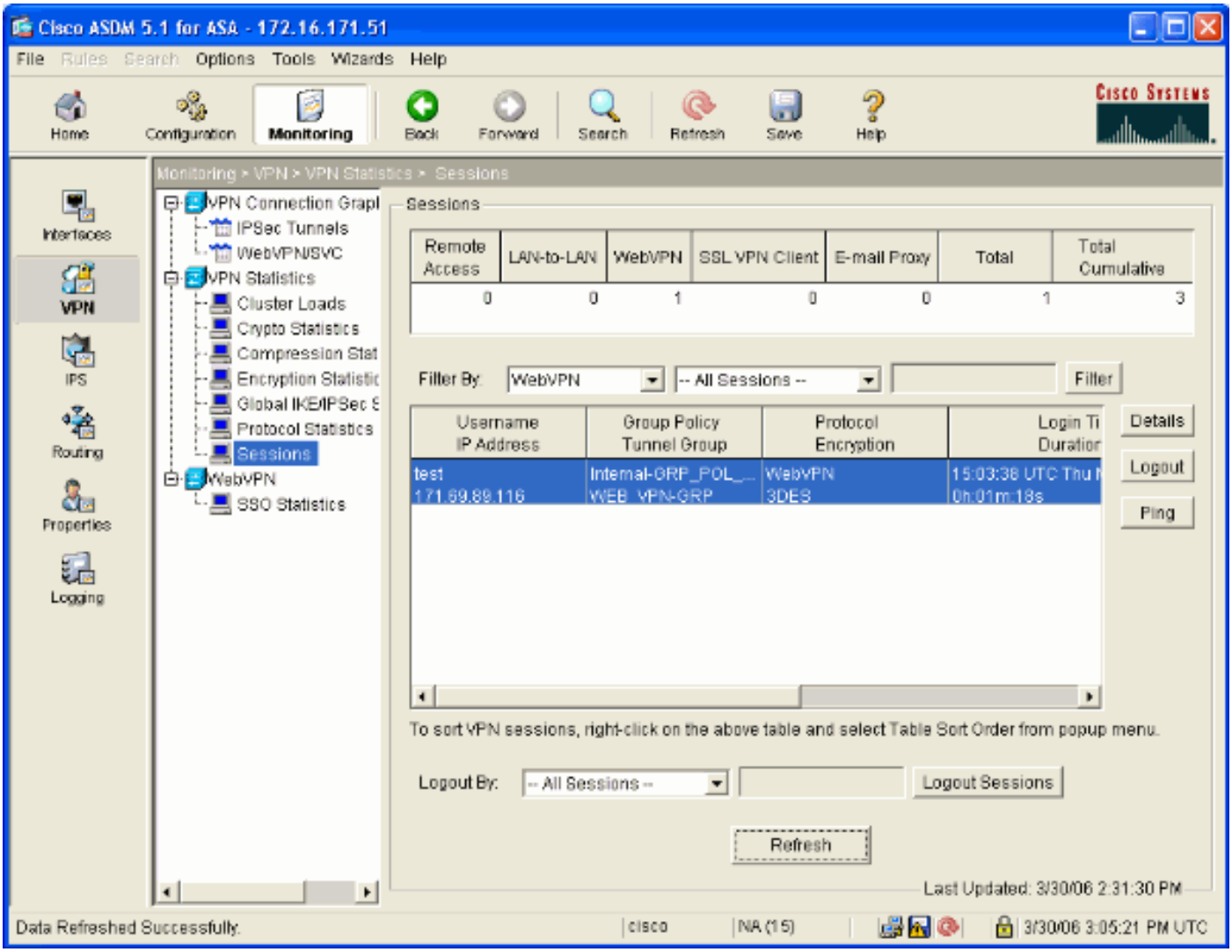
2. 내부 서버에 구성된 링크를 찾습니다. 확인하려면 링크를 클릭합니다

.



세션 모니터링

Monitoring(**모니터링**) > **VPN** > **VPN Statistics(VPN 통계)** > **Sessions(세션)**를 선택하고 이 문서에 구성된 그룹에 속한 WebVPN 세션을 찾습니다.



WebVPN 세션 디버그

이 출력은 성공한 WebVPN 세션의 샘플 디버그입니다.

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

```
ASA#debug webvpn 255
INFO: debug webvpn enabled at level 255
ASA#
ASA# webvpn_portal.c:ewaFormServe_webvpn_login[1570]
webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:webvpn_auth[286]
WebVPN: no cookie present!!
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:http_webvpn_pre_authentication[1782]
!--- Begin AAA WebVPN: calling AAA with ewsContext (78986968) and nh (78960800)! WebVPN: started
user authentication...
webvpn_auth.c:webvpn_aaa_callback[3422]
WebVPN: AAA status = (ACCEPT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_auth.c:http_webvpn_post_authentication[1095]
WebVPN: user: (test) authenticated.
!--- End AAA webvpn_auth.c:http_webvpn_auth_accept[2093]
webvpn_session.c:http_webvpn_create_session[159] webvpn_session.c:http_webvpn_find_session[136]
WebVPN session created!
```

```
webvpn_session.c:http_webvpn_find_session[136]
webvpn_db.c:webvpn_get_server_db_first[161]
webvpn_db.c:webvpn_get_server_db_next[202]
traversing list: (webserver)
webvpn_portal.c:ewaFormServe_webvpn_cookie[1421]
webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated.
webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated.
!--- Output supressed webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

- WebVPN 로그인 페이지에 Group(그룹) 드롭다운 상자가 없는 경우 Enable WebVPN on the Outside Interface(외부 인터페이스에서 WebVPN 활성화) 및 Configure a Tunnel Group(터널 그룹 구성)의 5단계에서 2단계를 완료했는지 확인합니다.이러한 단계가 완료되지 않고 드롭다운이 없는 경우, 인증은 Default Group(기본 그룹)에 속하며 실패할 수 있습니다.
- ASDM 또는 ASA의 사용자에게 액세스 권한을 할당할 수는 없지만 도메인 컨트롤러에서 Microsoft Windows 액세스 권한을 가진 사용자를 제한할 수 있습니다.사용자가 인증하는 웹 페이지에 필요한 NT 그룹 권한을 추가합니다.사용자가 그룹의 권한으로 WebVPN에 로그인하면 지정된 페이지에 대한 액세스가 부여되거나 거부됩니다.ASA는 도메인 컨트롤러를 대신하여 프록시 인증 호스트로만 작동하며, 여기에 있는 모든 통신은 NTLMv1입니다.
- Sharepoint Server는 양식 기반 인증을 지원하지 않으므로 WebVPN을 통해 Sharepoint에 대한 SSO를 구성할 수 없습니다.따라서 여기에 게시물 또는 포스트 플러그인 프로시저가 있는 책갈피는 적용되지 않습니다.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliance
- 기술 지원 및 문서 – Cisco Systems