PIX/ASA:ASDM/CLI 컨피그레이션을 통해 VPN 클라이언트 사용자를 위한 Kerberos 인증 및 LDAP 권한 부여 서버 그룹 예

목차

소개

이 문서에서는 Cisco ASDM(Adaptive Security Device Manager)을 사용하여 Cisco PIX 500 Series Security Appliance에서 Kerberos 인증 및 LDAP 권한 부여 서버 그룹을 구성하는 방법에 대해 설명합니다.이 예에서 서버 그룹은 VPN 터널 그룹의 정책에서 수신 사용자를 인증하고 권한을 부여하기 위해 사용됩니다.

사전 요구 사항

요구 사항

이 문서에서는 PIX가 완벽하게 작동하며 ASDM이 컨피그레이션을 변경할 수 있도록 구성되어 있다고 가정합니다.

참고: ASDM에서 PIX를 구성하도록 허용하려면 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco PIX Security Appliance Software 버전 7.x 이상
- Cisco ASDM 버전 5.x 이상

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.

관련 제품

이 컨피그레이션은 Cisco ASA(Adaptive Security Appliance) 버전 7.x에서도 사용할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

VPN 사용자를 다룰 때 PIX/ASA 7.x 소프트웨어에서 사용할 수 있는 모든 가능한 인증 및 권한 부여 방법이 지원되지는 않습니다.이 표에서는 VPN 사용자가 사용할 수 있는 방법을 자세히 설명합니다.

	로컬	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP
인증	예	예	예	예	예	예	아니요
Ahthorization(권한 부여)	예	예	아니요	아니요	아니요	아니요	예

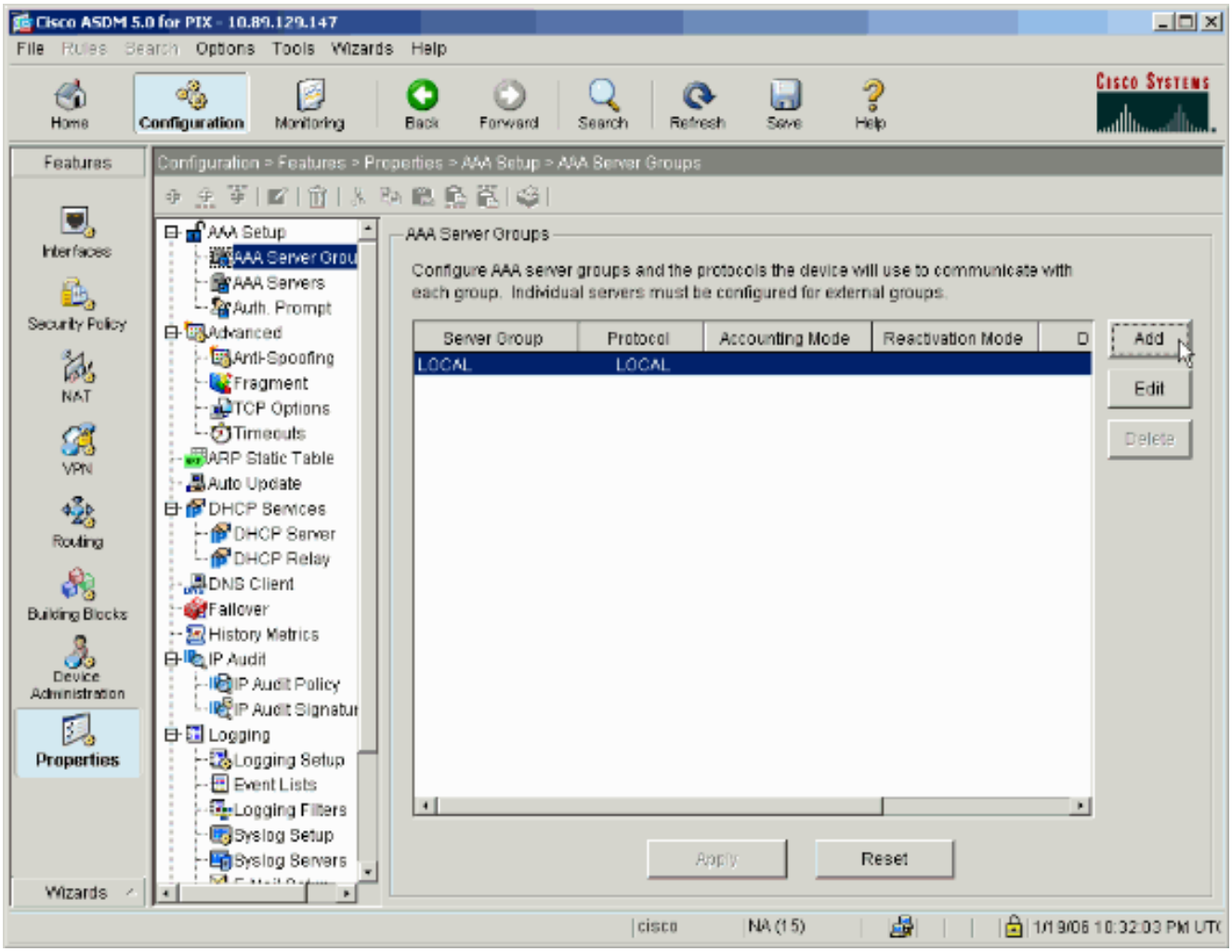
참고: Kerberos는 인증에 사용되며 LDAP는 이 예에서 VPN 사용자의 권한 부여에 사용됩니다.

ASDM을 사용하여 VPN 사용자에 대한 인증 및 권한 부여 구성

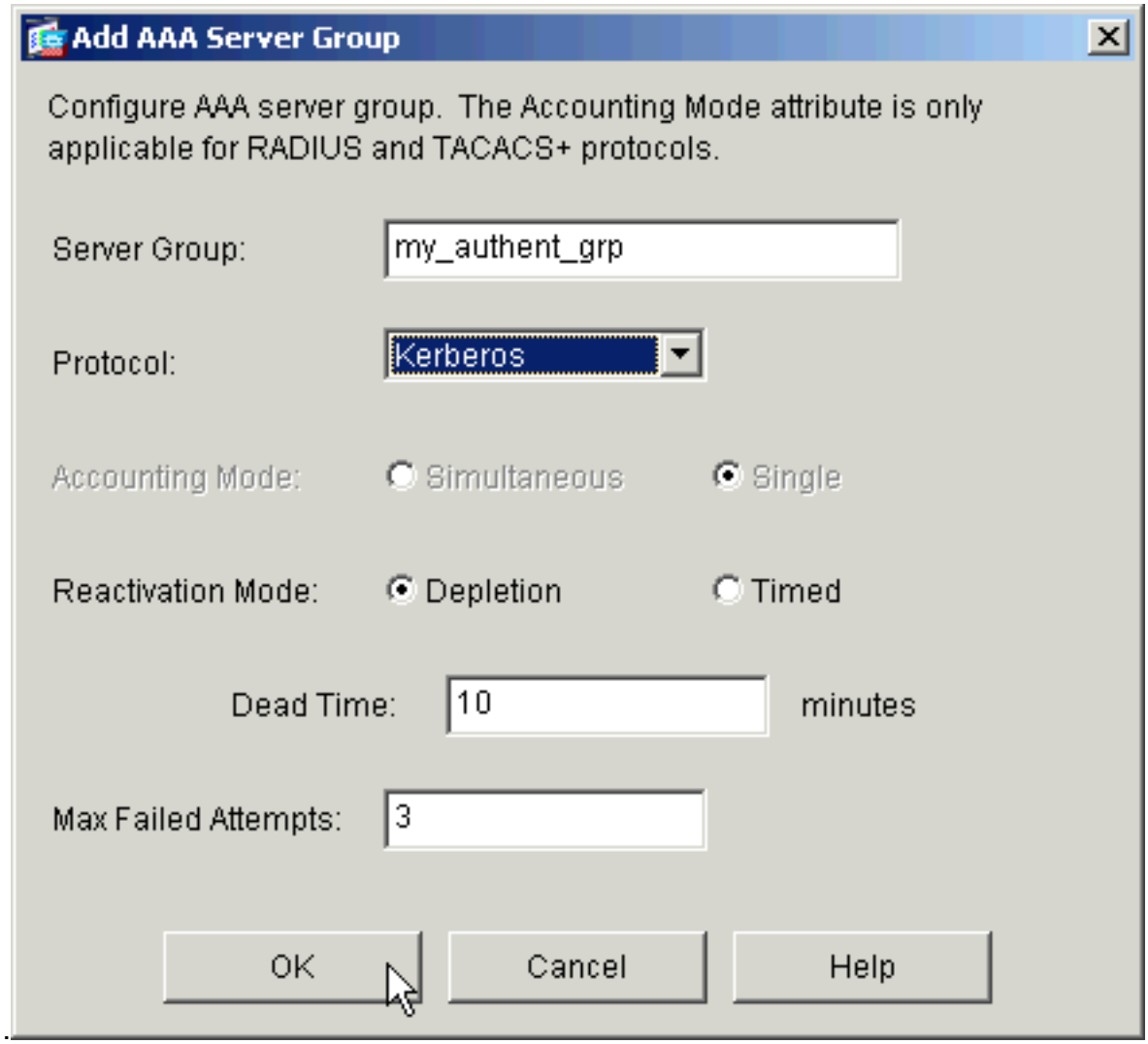
인증 및 권한 부여 서버 구성

ASDM을 통해 VPN 사용자에 대한 인증 및 권한 부여 서버 그룹을 구성하려면 다음 단계를 완료합니다.

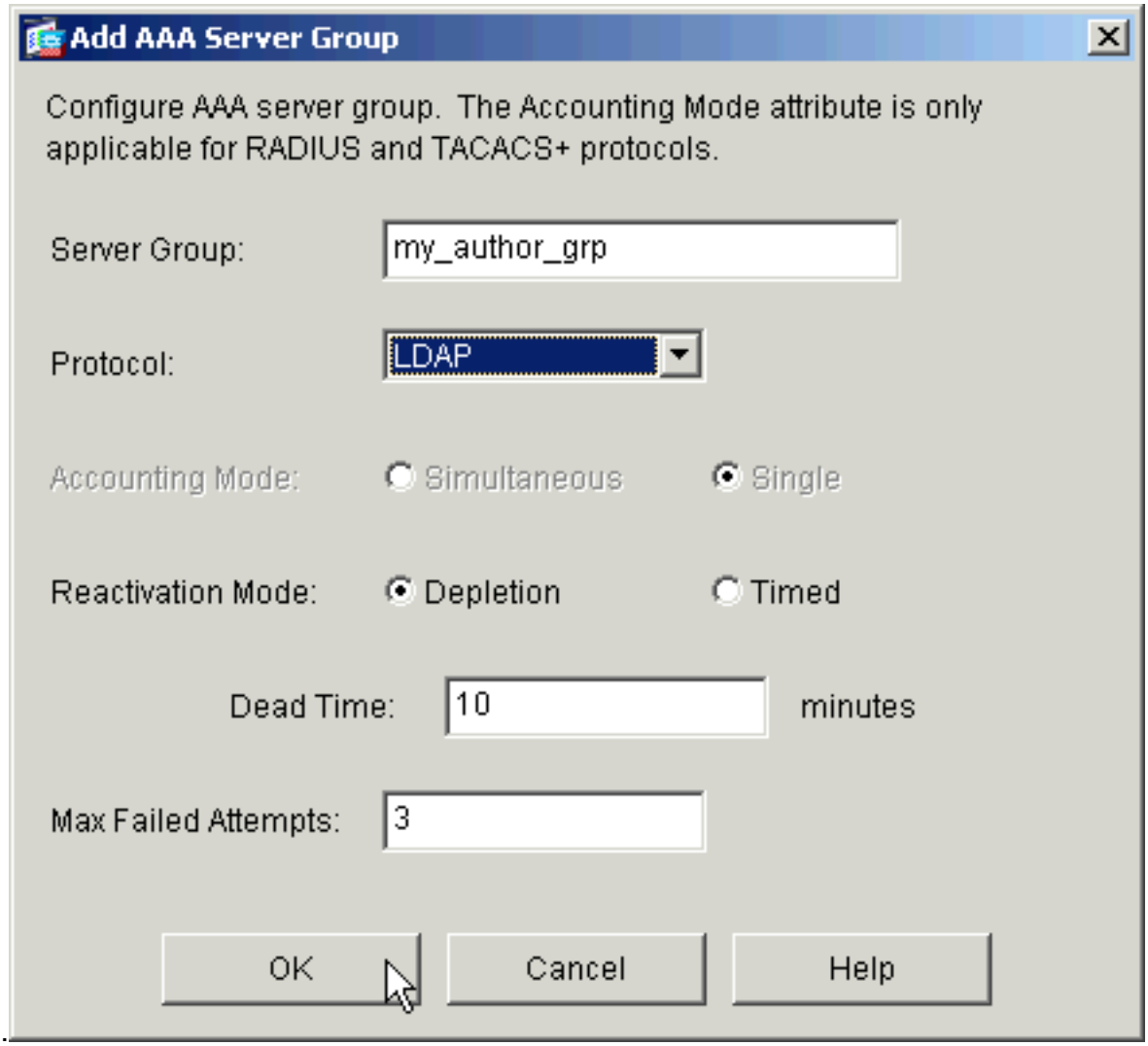
1. Configuration **> Properties > AAA Setup > AAA Server Groups를 선택하고 Add를 클릭합니다**.



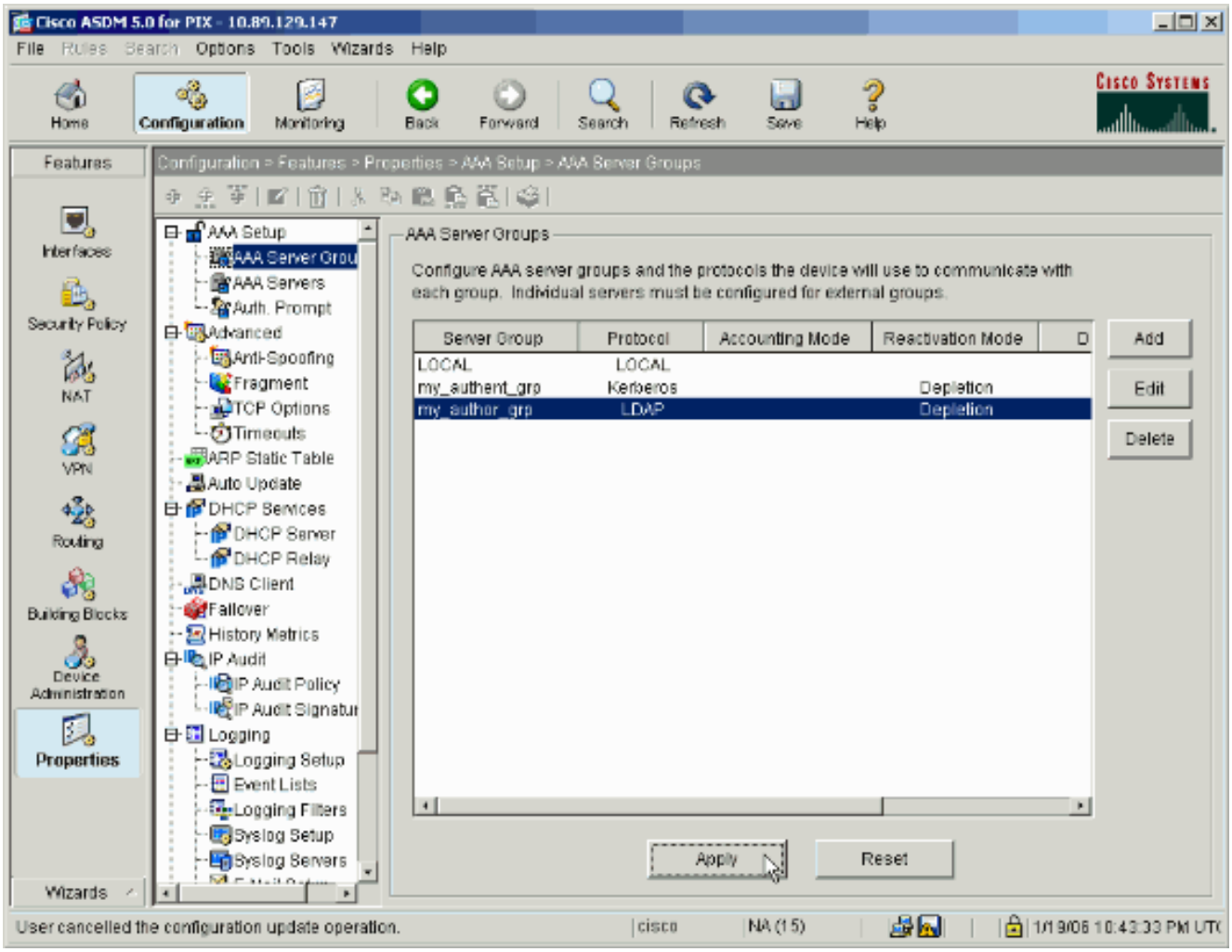
2. 새 인증 서버 그룹의 이름을 정의하고 프로토콜을 선택합니다.Accounting Mode 옵션은 RADIUS 및 TACACS+에만 적용됩니다.완료되면 **OK**(확인)를 클릭합니다



3. 새 권한 부여 서버 그룹을 만들려면 1단계와 2단계를 반복합니다



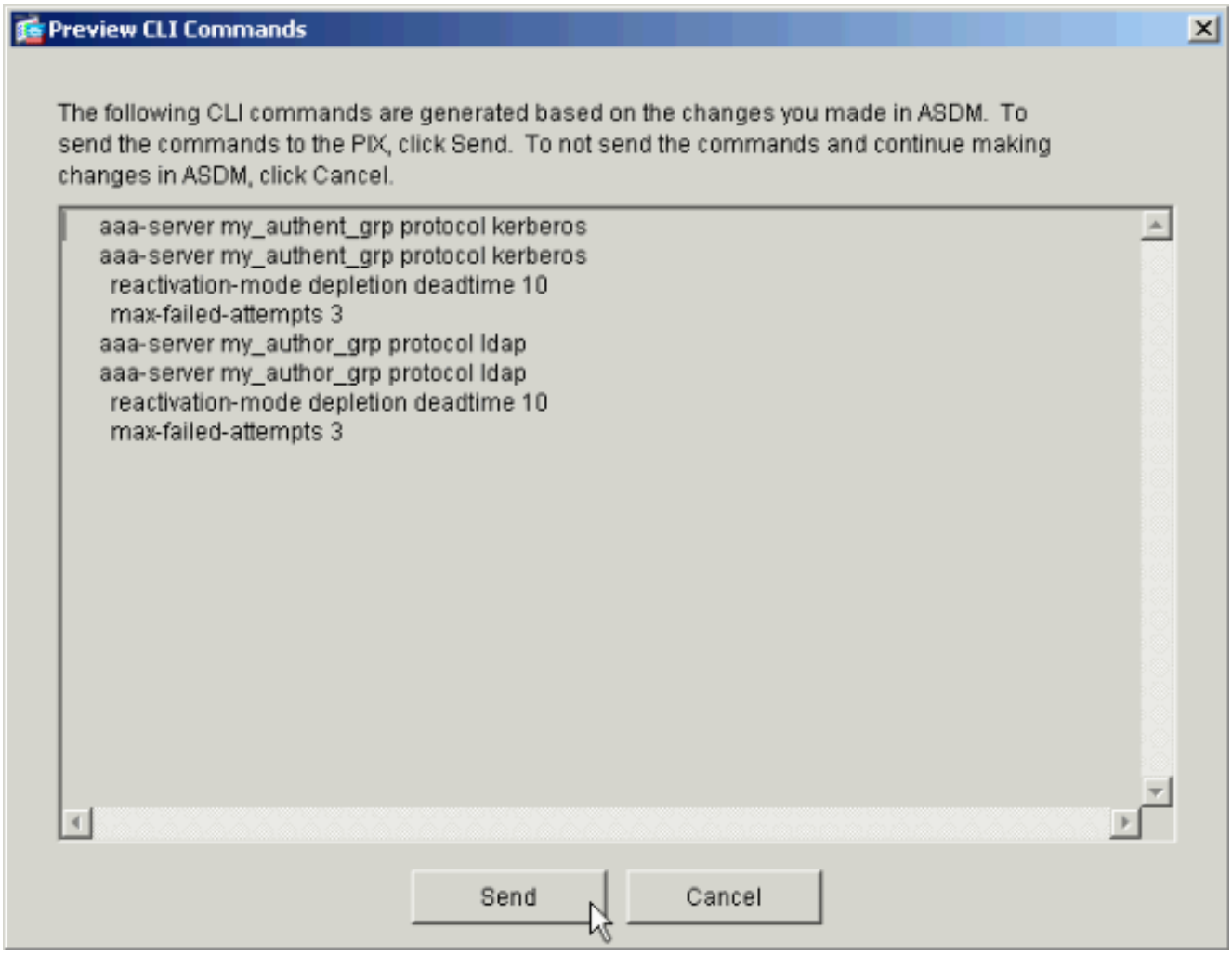
4. 변경 사항을 디바이스에 전송하려면 Apply를 클릭합니다
.



이렇게 구성한 경우 디바이스에서 실행 중인 컨피그레이션에 추가된 명령을 미리 봅니다.

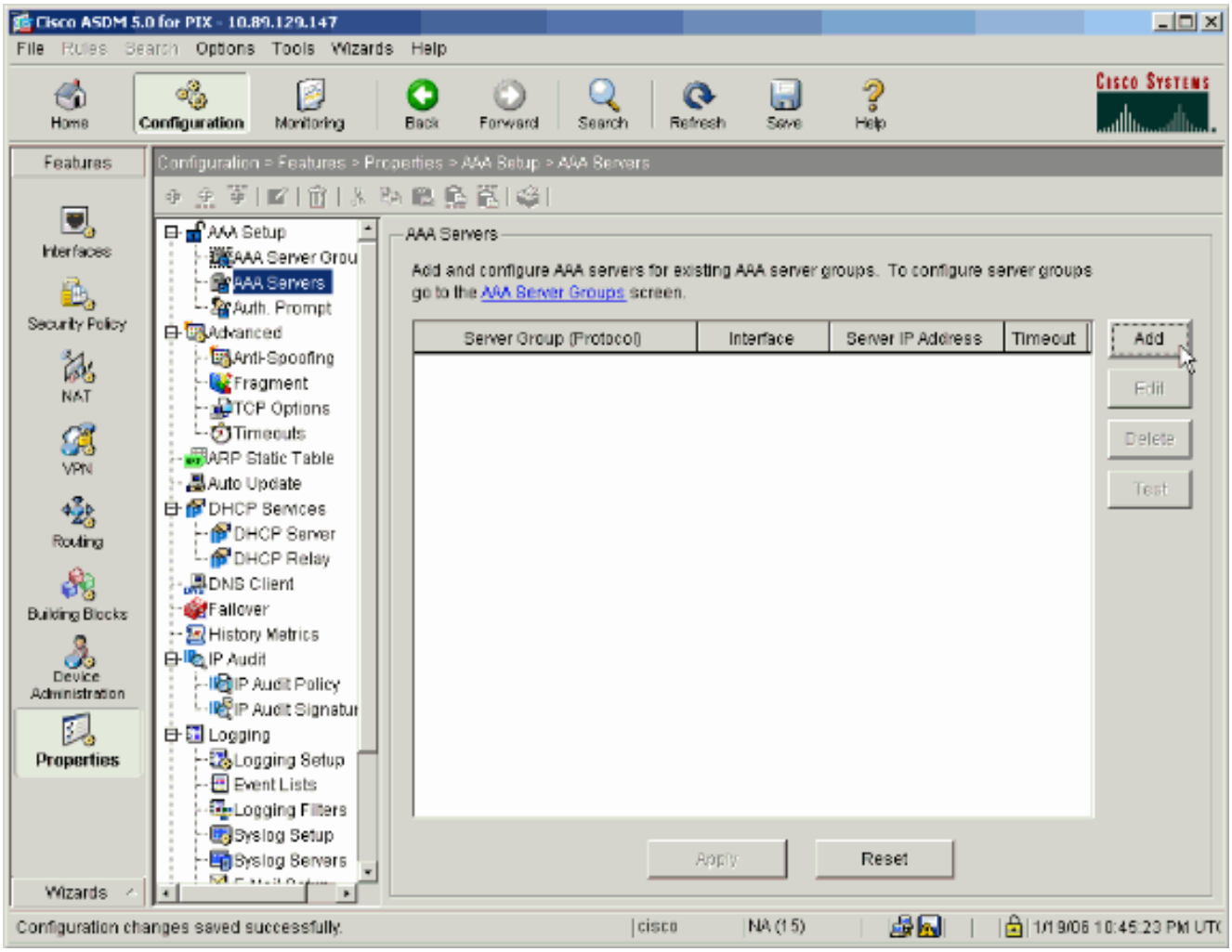
5. 디바이스로 명령을 전송하려면 Send(보내기)를 클릭합니다

.

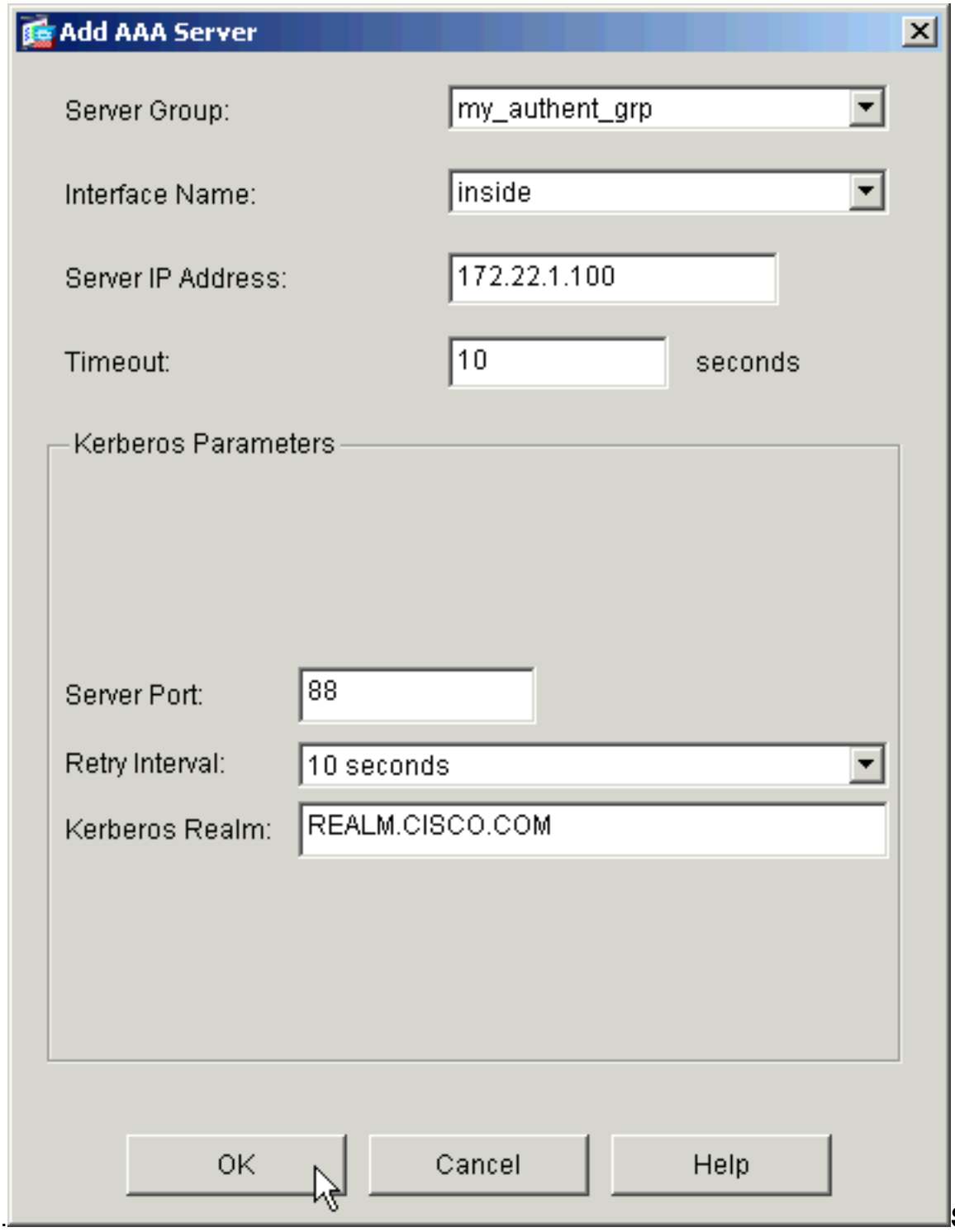


새로 생성된 서버 그룹은 이제 인증 및 권한 부여 서버로 채워져야 합니다.

6. Configuration **> Properties > AAA Setup > AAA Servers를 선택하고 Add를 클릭합니다**
.

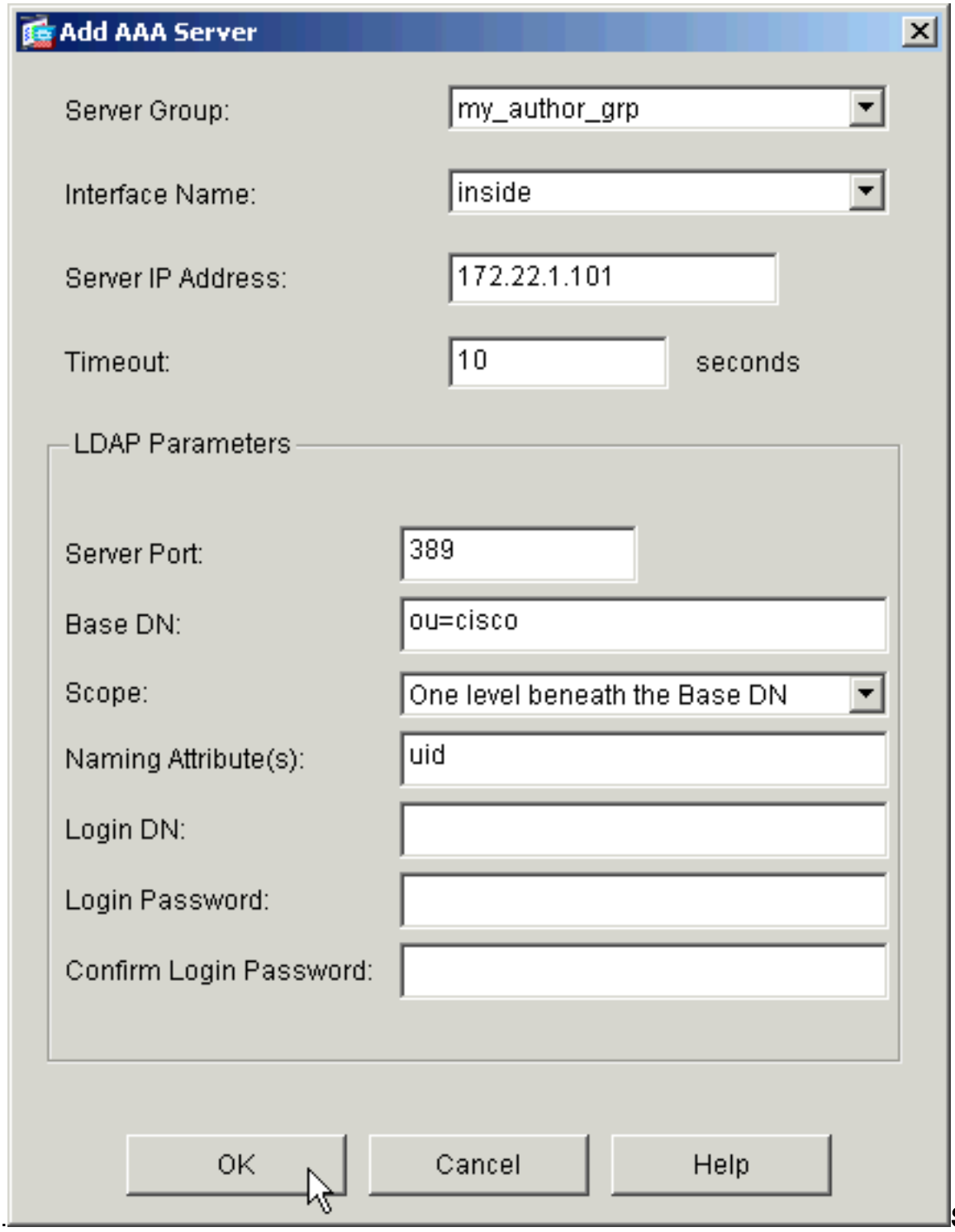


7. 인증 서버를 구성합니다.완료되면 **OK**(확인)를 클릭합니다



Server Group(서버 그룹) - 2단계에서 구성된 인증 서버 그룹을 선택합니다.**Interface Name**(인터페이스 이름) - 서버가 상주하는 인터페이스를 선택합니다.**Server IP Address(서버 IP 주소)** - 인증 서버의 IP 주소를 지정합니다.**Timeout**(시간 제한) - 서버의 응답을 기다리는 최대 시간(초)을 지정합니다.**Kerberos 매개변수:Server Port**—88은 Kerberos의 표준 포트입니다.**Retry Interval(재시도 간격)** - 원하는 재시도 간격을 선택합니다.**Kerberos 영역**—Kerberos 영역의 이름을 입력합니다.이는 대문자로 된 Windows 도메인 이름입니다.

8. 권한 부여 서버를 구성합니다.완료되면 **OK(확인)**를 클릭합니다



Server Group(서버 그룹) - 3단계에서 구성된 권한 부여 서버 그룹을 선택합니다.**Interface Name**(인터페이스 이름) - 서버가 상주하는 인터페이스를 선택합니다.**Server IP Address(서버 IP 주소)** - 권한 부여 서버의 IP 주소를 지정합니다.**Timeout**(시간 제한) - 서버의 응답을 기다리는 최대 시간(초)을 지정합니다.**LDAP 매개변수:Server Port(서버 포트)** - 389가 LDAP의 기본 포트입니다.**Base DN(기본 DN)** - 권한 부여 요청을 받으면 서버가 검색을 시작할 LDAP 계층 구조의 위치를 입력합니다.**Scope**(범위) - 권한 부여 요청을 받으면 서버가 LDAP 계층을 검색해야 하는 범위를 선택합니다.**Naming Attribute(s)**(s)(명명 특성) - LDAP 서버의 항목이 고유하게 정의되는 Relative Distinguished Name 특성을 입력합니다.공통 이름 지정 특성은 Common Name (cn) 및 User ID (uid) 입니다.**Login DN**—Microsoft Active Directory 서버를 비롯한 일부 LDAP 서버는 다른 LDAP 작업에 대한 요청을 수락하기 전에 인증된 바인딩을 통해 핸드셰이크를 설정해야 합니다.Login DN 필드는 디바이스의 인증 특성을 정의합니다. 이는 관리 권한이 있는 사용자의 인증 특성과 일치해야 합니다.예를 들어, cn=administrator입니다.익명 액세스의 경우 이 필드를 비워 둡니다.**Login Password(로그인 비밀번호)** - 로그인 DN의 비밀번호를 입력

합니다.**Confirm Login Password**(로그인 비밀번호 확인) - 로그인 DN의 비밀번호를 확인합니다.

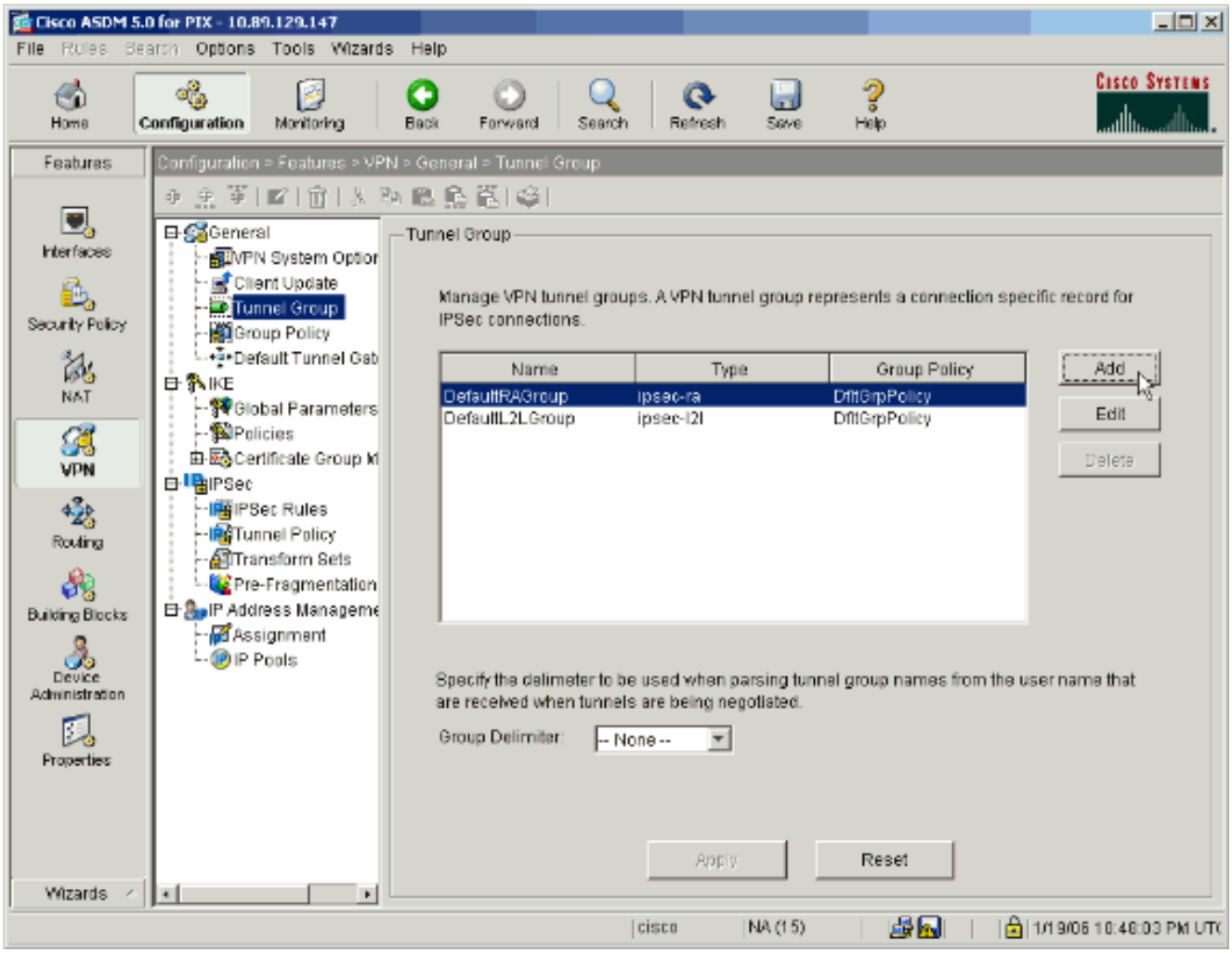
9. 모든 인증 및 권한 부여 서버가 추가된 후 디바이스에 변경 사항을 전송하려면 Apply를 클릭합니다.PIX가 이를 수행하도록 구성한 경우 PIX는 이제 실행 중인 컨피그레이션에 추가된 명령을 미리 봅니다.
10. 디바이스로 명령을 전송하려면 Send(보내기)를 클릭합니다.

인증 및 권한 부여를 위한 VPN 터널 그룹 구성

VPN 터널 그룹에 방금 구성한 서버 그룹을 추가하려면 다음 단계를 완료하십시오.

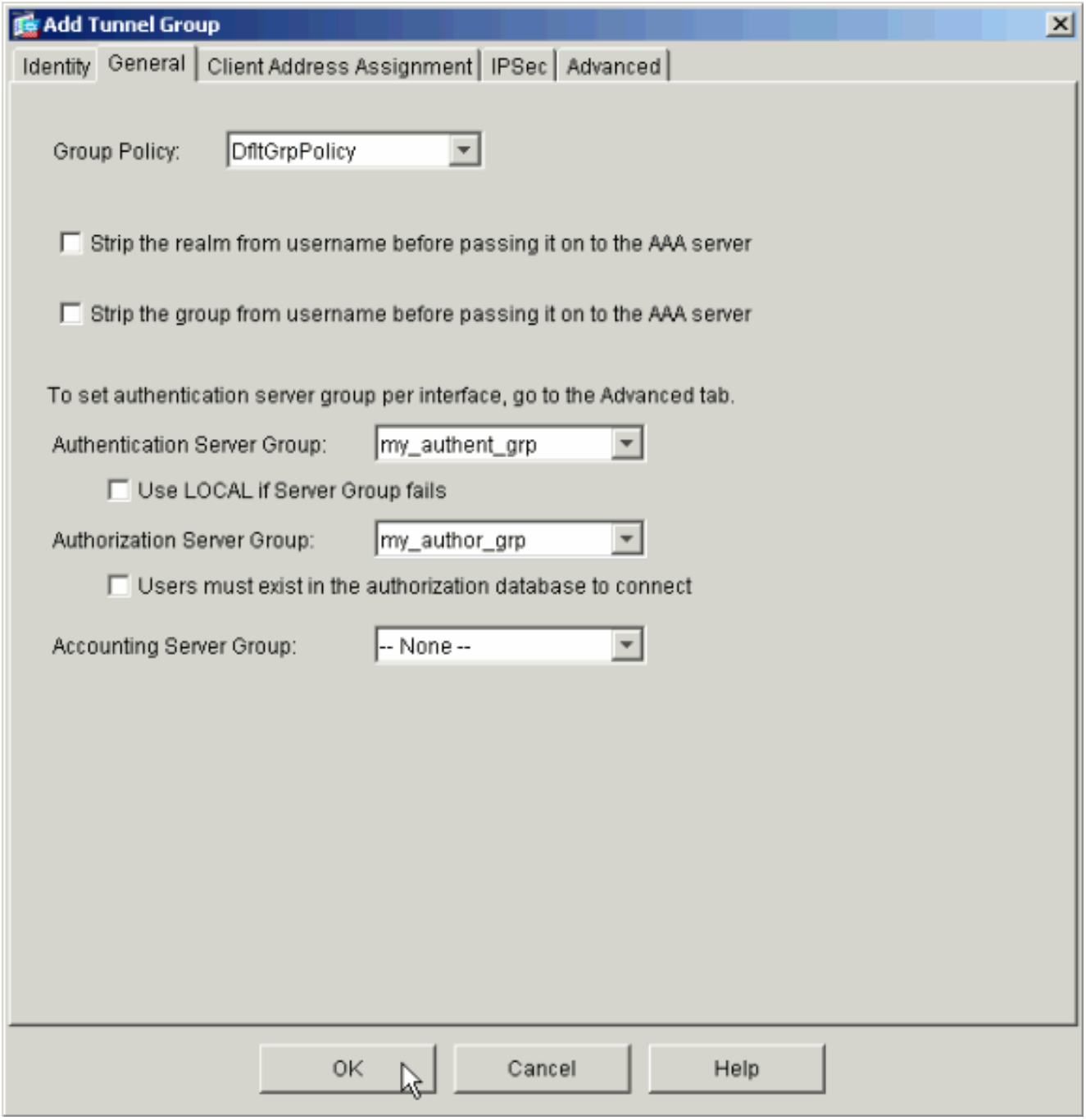
1. Configuration **> VPN > Tunnel Group**을 선택하고 **Add**를 클릭하여 새 터널 그룹을 생성하거나 기존 그룹을 수정하려면 Edit를 클릭합니다

.



2. 표시되는 창의 General(일반) 탭에서 이전에 구성된 서버 그룹을 선택합니다

.



3. *선택 사항:* 새 터널 그룹을 추가할 경우 다른 탭에서 나머지 매개변수를 구성합니다.
4. 완료되면 **OK**(확인)를 클릭합니다.
5. 터널 그룹 컨피그레이션이 완료된 후 디바이스에 변경 사항을 전송하려면 Apply를 클릭합니다.PIX가 이를 수행하도록 구성한 경우 PIX는 이제 실행 중인 컨피그레이션에 추가된 명령을 미리 봅니다.
6. 디바이스로 명령을 전송하려면 Send(보내기)를 클릭합니다.

CLI를 사용하여 VPN 사용자에 대한 인증 및 권한 부여 구성

VPN 사용자를 위한 인증 및 권한 부여 서버 그룹에 해당하는 CLI 컨피그레이션입니다.

Security Appliance CLI 컨피그레이션
pixfirewall#**show run** : Saved :

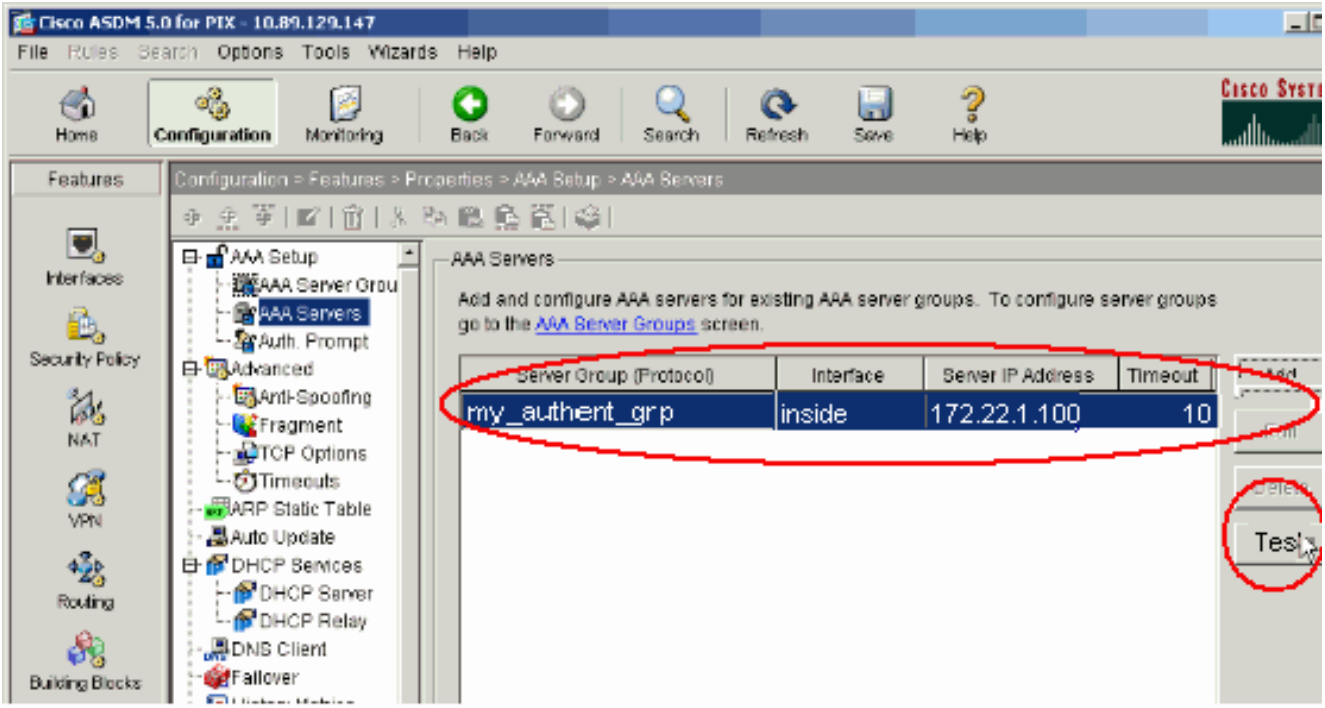
```
PIX Version 7.2(2)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 172.22.1.105 255.255.255.0
!
!--- Output is suppressed. ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive dns server-group DefaultDNS
domain-name default.domain.invalid pager lines 24 mtu
inside 1500 no failover icmp unreachable rate-limit 1
burst-size 1 asdm image flash:/asdm-522.bin !--- Output
is suppressed. aaa-server my_authent_grp protocol
kerberos
aaa-server my_authent_grp host 172.22.1.100
 kerberos-realm REALM.CISCO.COM
aaa-server my_author_grp protocol ldap
aaa-server my_author_grp host 172.22.1.101
 ldap-base-dn ou=cisco
 ldap-scope onelevel
 ldap-naming-attribute uid

http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart

tunnel-group DefaultRAGroup general-attributes
 authentication-server-group my_authent_grp
 authorization-server-group my_author_grp

!
!--- Output is suppressed.
```

다음을 확인합니다.

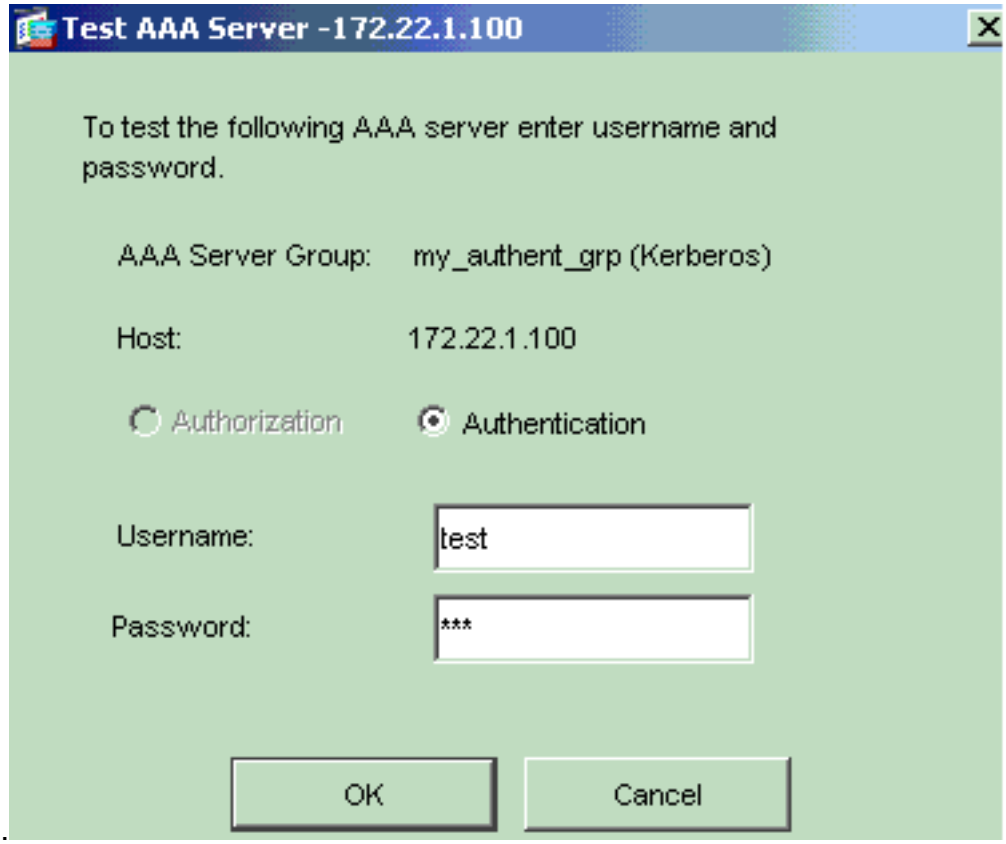
PIX/ASA와 AAA 서버 간의 사용자 인증을 확인하려면 다음 단계를 완료하십시오.

1. Configuration > **Properties > AAA Setup > AAA Servers를 선택하고** 서버 그룹 (my_authent_grp)을 선택합니다. 그런 다음 **테스트**를 클릭하여 사용자 자격 증명을 검증합니다

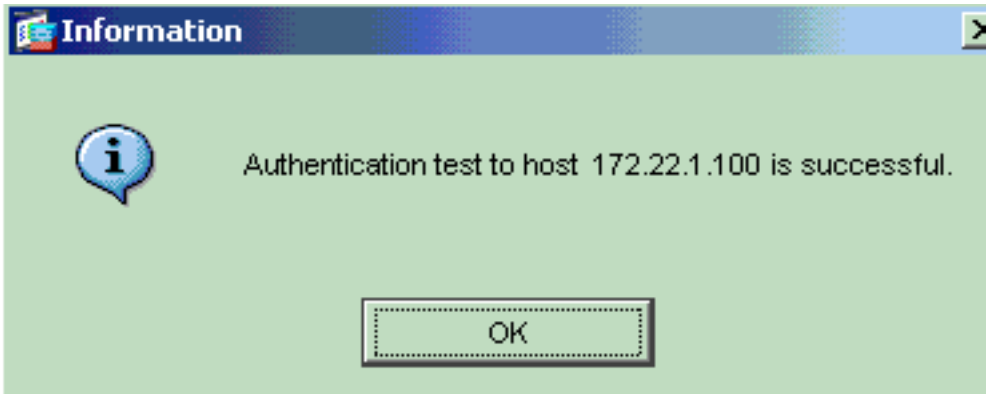
   .



2. 사용자 이름 및 비밀번호(예: 사용자 이름:테스트 및 비밀번호:테스트)를 클릭하고 **확인**을 클릭하여 유효성을 검사합니다



3. 인증이 성공했음을 확인할 수 있습니다



.

문제 해결

1. 인증 실패 원인 중 하나가 클럭 스큐(clock skew)입니다.PIX 또는 ASA 및 인증 서버의 클럭이 동기화되었는지 확인합니다.클럭 스큐(Clock Skew)로 인해 인증이 실패할 경우 다음 오류 메시지를 수신할 수 있습니다.`:- : :300 ..`또한 다음 로그 메시지가 나타납니다.`%PIX|ASA-3-113020:Kerberos : ip_address 300 ip_address` — Kerberos 서버의 IP 주소입니다.이 메시지는 보안 어플라이언스와 서버의 클럭이 5분(300초) 이상 떨어져 있기 때문에 Kerberos 서버를 통한 IPSec 또는 WebVPN 사용자에 대한 인증이 실패할 때 표시됩니다.이 경우 연결 시도가 거부됩니다.이 문제를 해결하려면 보안 어플라이언스와 Kerberos 서버의 시계를 동기화하십시오.
2. AD(Active Directory)에 대한 사전 인증을 비활성화해야 합니다. 그렇지 않으면 사용자 인증에 실패할 수 있습니다.
3. VPN 클라이언트 사용자가 Microsoft 인증서 서버에 대해 인증할 수 없습니다.다음과 같은 오류 메시지가 나타납니다." `"( 14)` 이 문제를 해결하려면 인증 서버에서 **Kerberos 사전 인증이 필요하지 않음** 확인란의 선택을 취소합니다.

관련 정보

- AAA 서버 및 로컬 데이터베이스 구성
- Cisco ASA 5500 Series Adaptive Security Appliances 제품 지원
- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- 보안 제품 필드 알림(PIX 포함)
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems