PIX/ASA 7.x ASDM:원격 액세스 VPN 사용자의 네트워크 액세스 제한

목차

소개

이 문서에서는 Cisco ASDM(Adaptive Security Device Manager)을 사용하여 내부 네트워크 원격 액세스 VPN 사용자가 PIX Security Appliance 또는 ASA(Adaptive Security Appliance) 뒤에서 액세스할 수 있는 항목을 제한하는 샘플 컨피그레이션을 제공합니다. 다음과 같은 경우 원격 액세스 VPN 사용자를 액세스하려는 네트워크 영역으로만 제한할 수 있습니다.

1. 액세스 목록을 생성합니다.
2. 그룹 정책과 연결합니다.
3. 이러한 그룹 정책을 터널 그룹과 연결합니다.

VPN Concentrator가 VPN 사용자로부터 액세스를 차단하는 시나리오에 대한 자세한 내용은 Cisco VPN 3000 Concentrator for Blocking with Filters and RADIUS Filter Assignment를 참조하십시오.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- ASDM을 사용하여 PIX를 구성할 수 있습니다.**참고:** ASDM에서 PIX를 구성하도록 허용하려면 ASDM에 대한 HTTPS 액세스 허용을 참조하십시오.
- 정상 작동이 확인된 원격 액세스 VPN 컨피그레이션이 하나 이상 있습니다.**참고:** 그러한 컨피그레이션이 없는 경우 하나의 우수한 원격 액세스 VPN 컨피그레이션을 구성하는 방법에 대한 자세한 내용은 ASDM 컨피그레이션 예를 사용하여 ASA as a Remote VPN Server를 참조하십

시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure PIX 500 Series Security Appliance 버전 7.1(1)**참고:** PIX 501 및 506E 보안 어플라이언스는 버전 7.x를 지원하지 않습니다.
- Cisco Adaptive Security Device Manager 버전 5.1(1)**참고:** ASDM은 PIX 또는 ASA 7.x에서만 사용할 수 있습니다.

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.

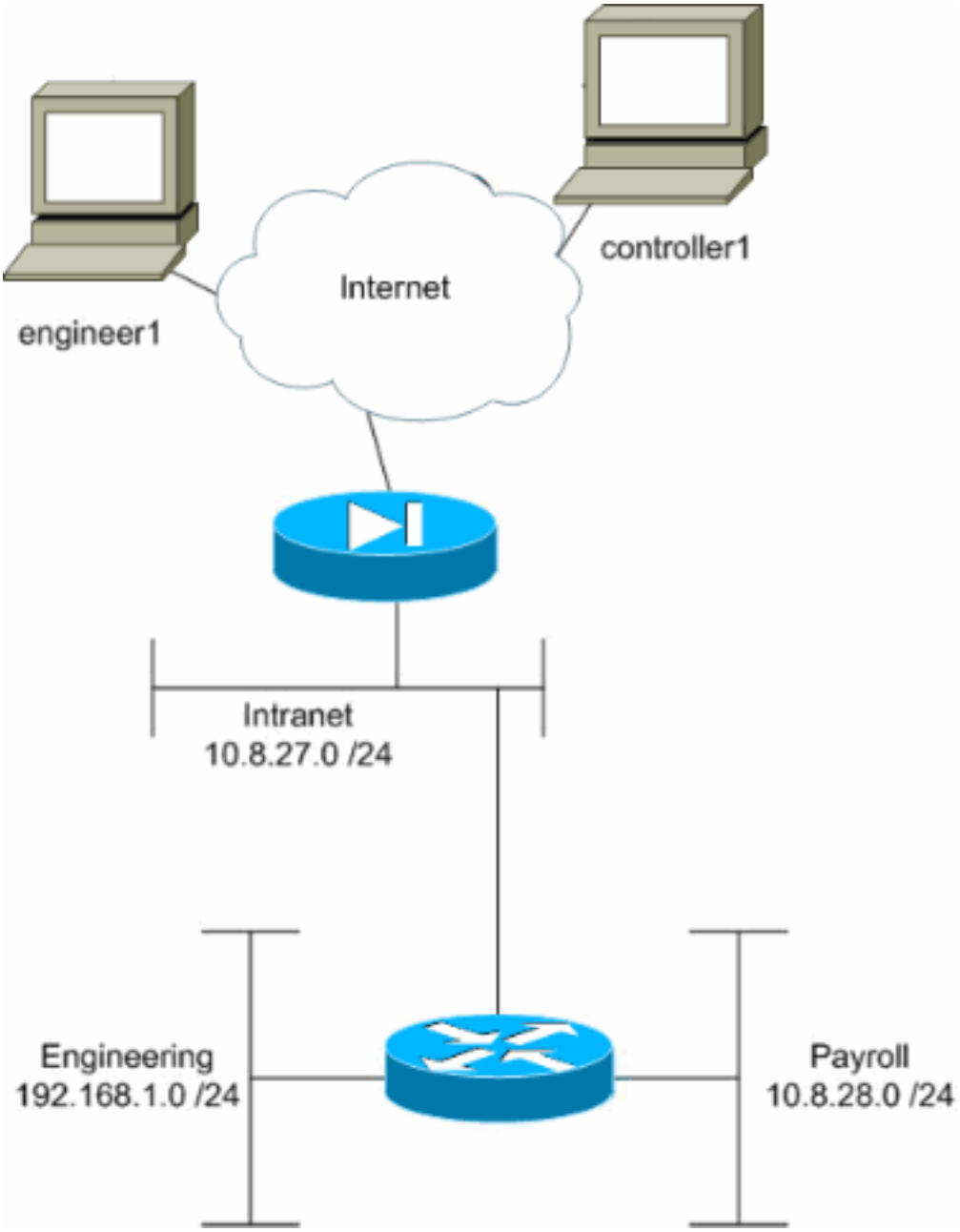
관련 제품

이 컨피그레이션은 다음 하드웨어 및 소프트웨어 버전과 함께 사용할 수도 있습니다.

- Cisco ASA 5500 Series Adaptive Security Appliance 버전 7.1(1)

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



이 컨피그레이션 예에서는 서브넷이 3개인 소규모 기업 네트워크가 필요합니다.이 다이어그램은 토폴로지를 보여줍니다.세 개의 서브넷은 인트라넷, 엔지니어링 및 Payroll입니다.이 컨피그레이션 예제의 목적은 급여 직원이 인트라넷과 급여 서브넷에 원격으로 액세스할 수 있도록 하고 이들이 엔지니어링 서브넷에 액세스하지 못하도록 하는 것입니다.또한 엔지니어는 급여 서브넷이 아닌 인트라넷 및 엔지니어링 서브넷에 원격으로 액세스할 수 있어야 합니다.이 예의 급여 사용자는 "controller1"입니다. 이 예에서 엔지니어링 사용자는 "engineer1"입니다.

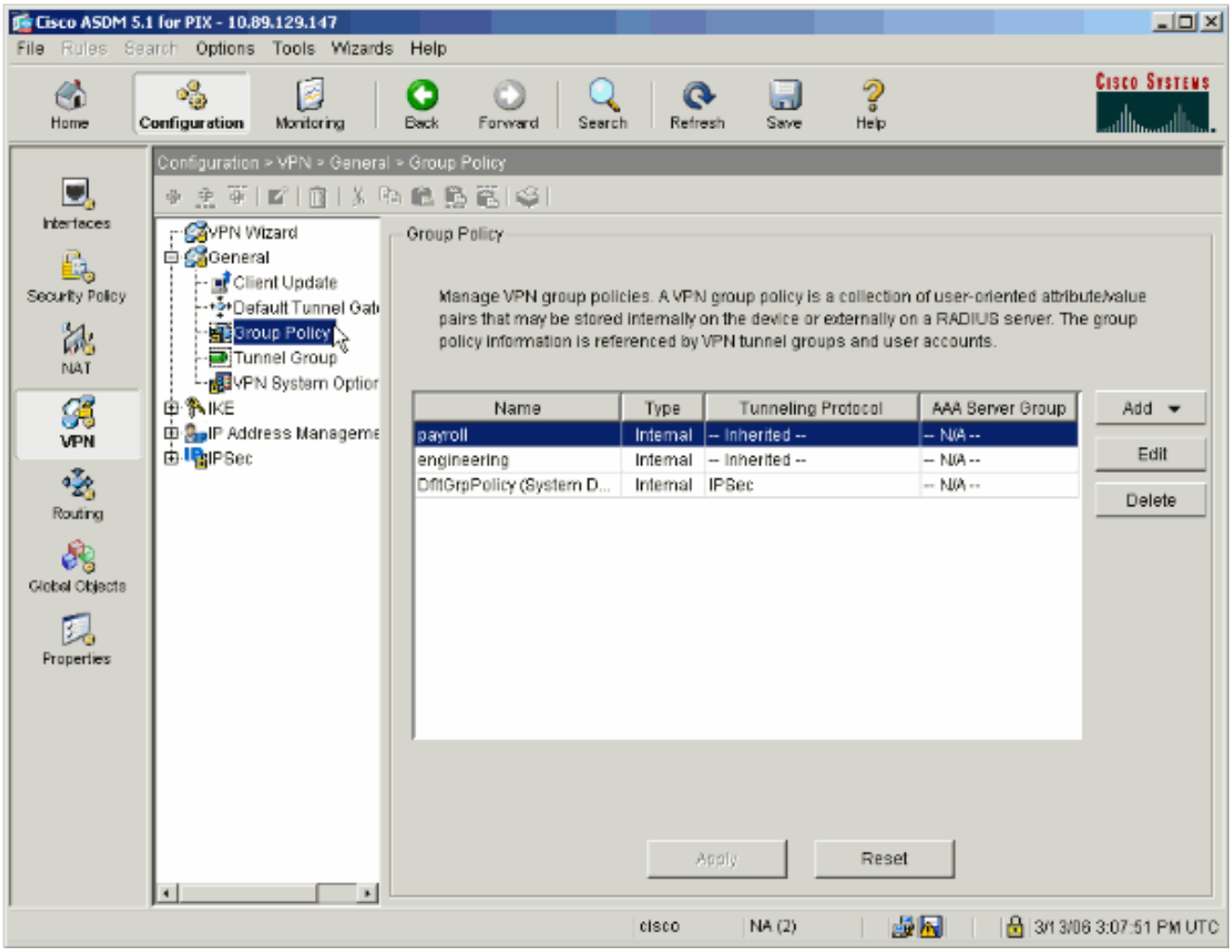
표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

ASDM을 통한 액세스 구성

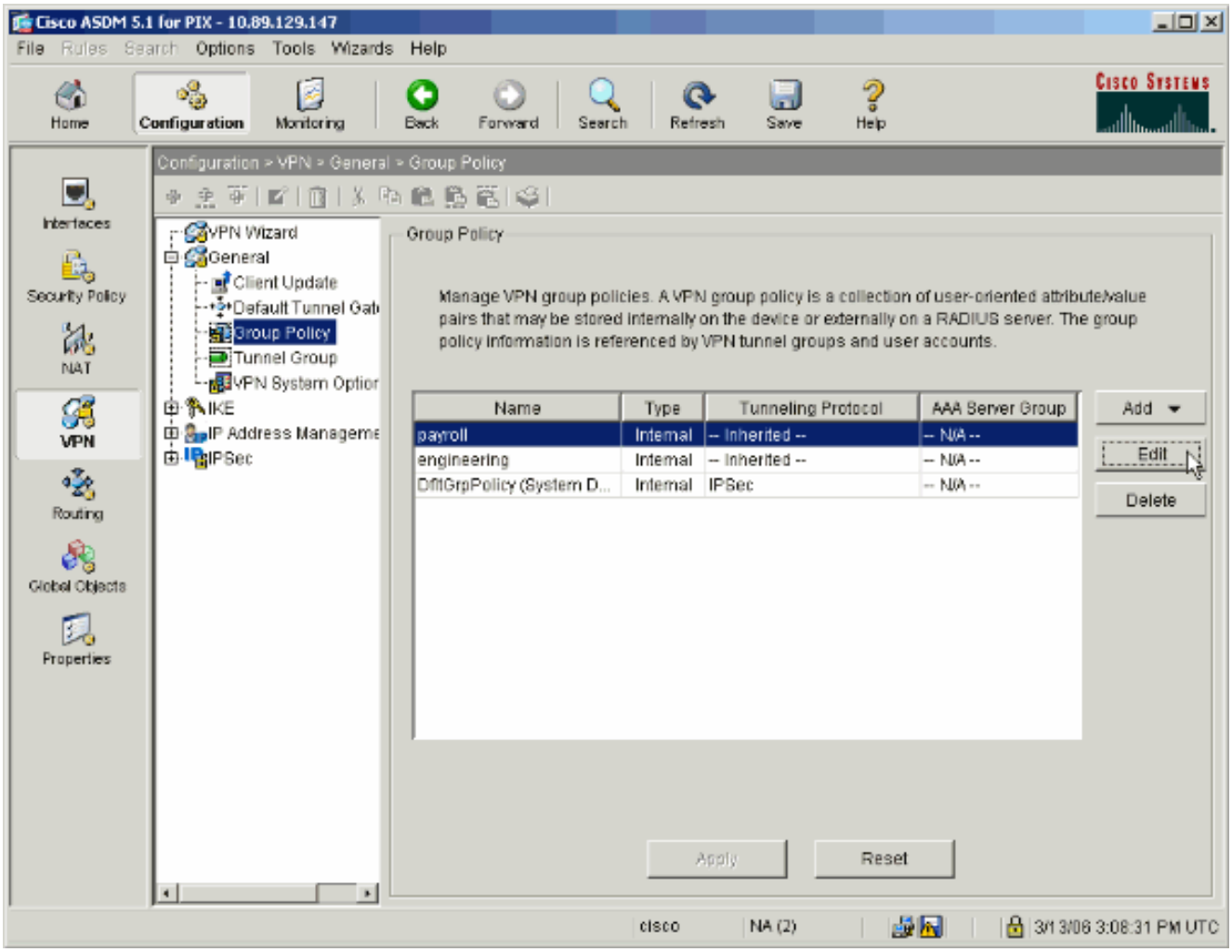
ASDM을 사용하여 PIX Security Appliance를 구성하려면 다음 단계를 완료합니다.

1. Configuration **> VPN > General > Group Policy를 선택합니다**
   .



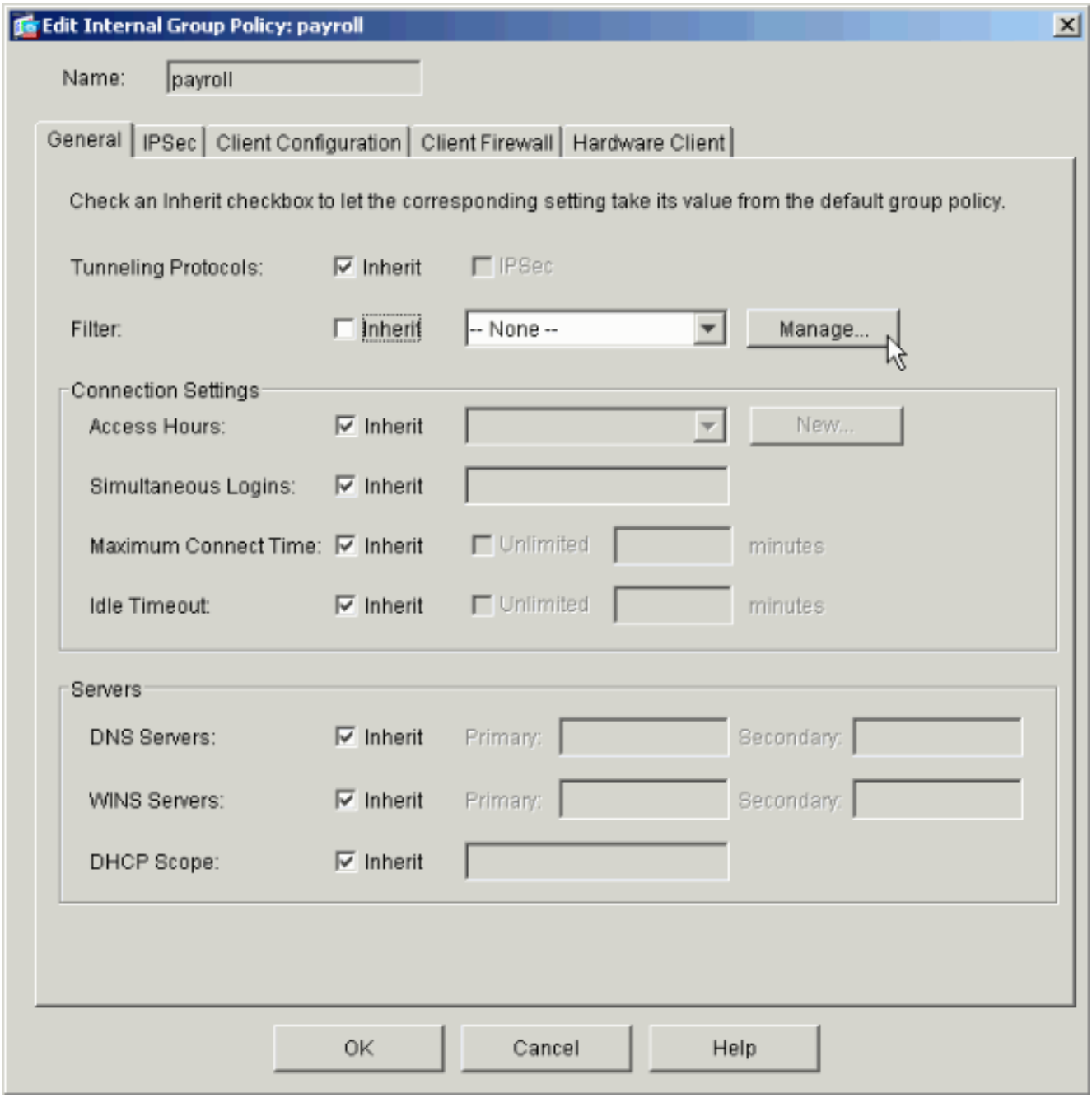
2. PIX에서 터널 그룹을 구성하기 위해 수행한 단계에 따라, 그룹 정책은 사용자가 제한하려는 터널 그룹에 대해 이미 존재할 수 있습니다.적합한 그룹 정책이 이미 있는 경우 선택한 후 **Edit**(수정)를 클릭합니다.그렇지 않으면 Add(**추가**)를 클릭하고 **Internal Group Policy(내부 그룹 정책)...를 선택합니다**

..



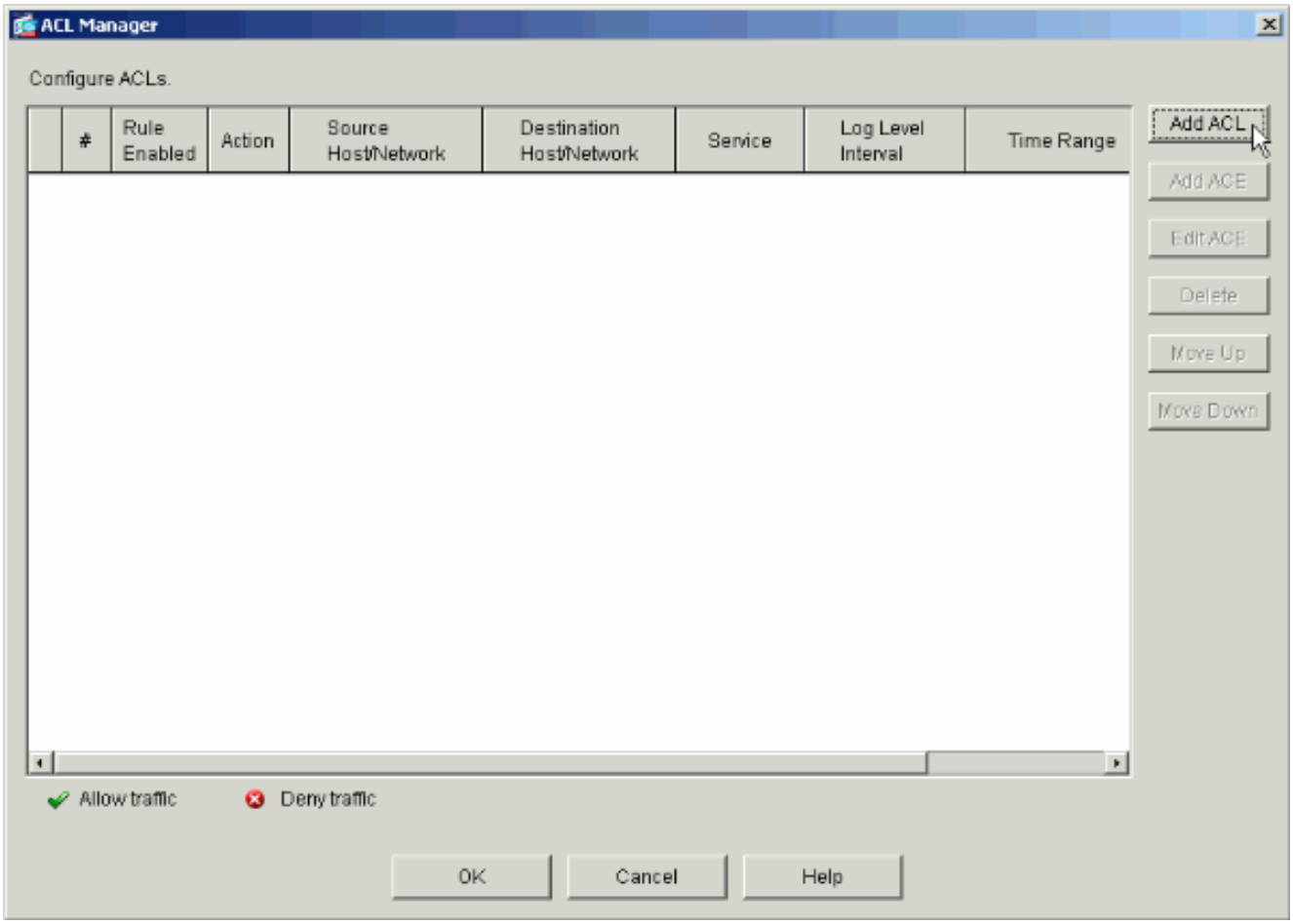
3. 필요한 경우 열려 있는 창 맨 위에 그룹 정책의 이름을 입력하거나 변경합니다.
4. General(일반) 탭에서 Filter(필터) 옆에 있는 Inherit(상속) 상자의 선택을 취소한 다음 Manage(관리)를 **클릭합니다**

.

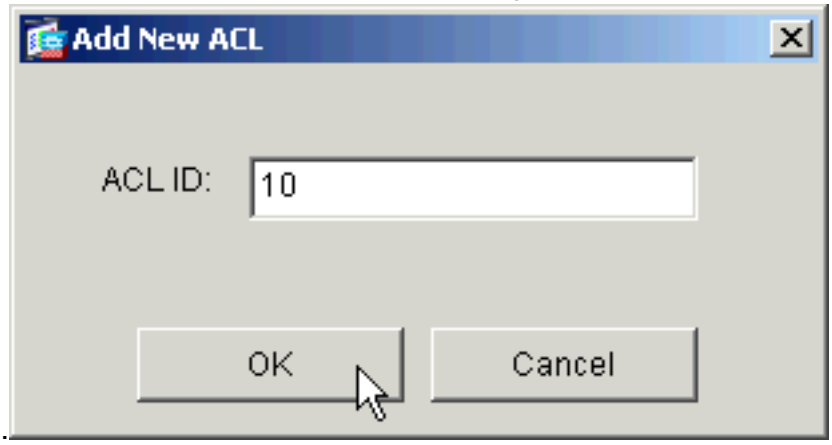


5. Add **ACL(ACL 추가)**을 클릭하여 ACL Manager(ACL 관리자) 창에 표시되는 새 액세스 목록을 생성합니다

.



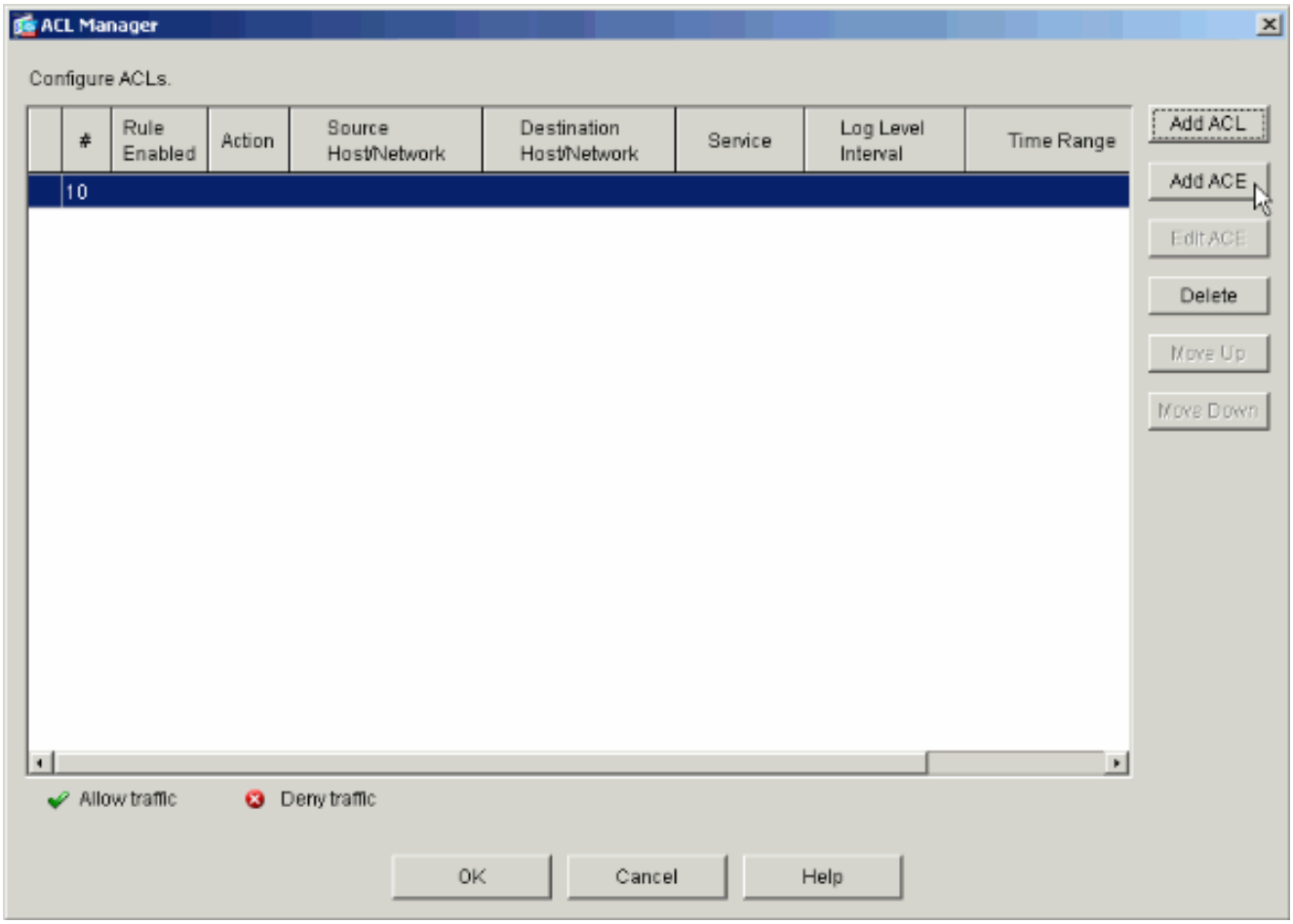
6. 새 액세스 목록의 번호를 선택하고 **확인**을 클릭합니다



.

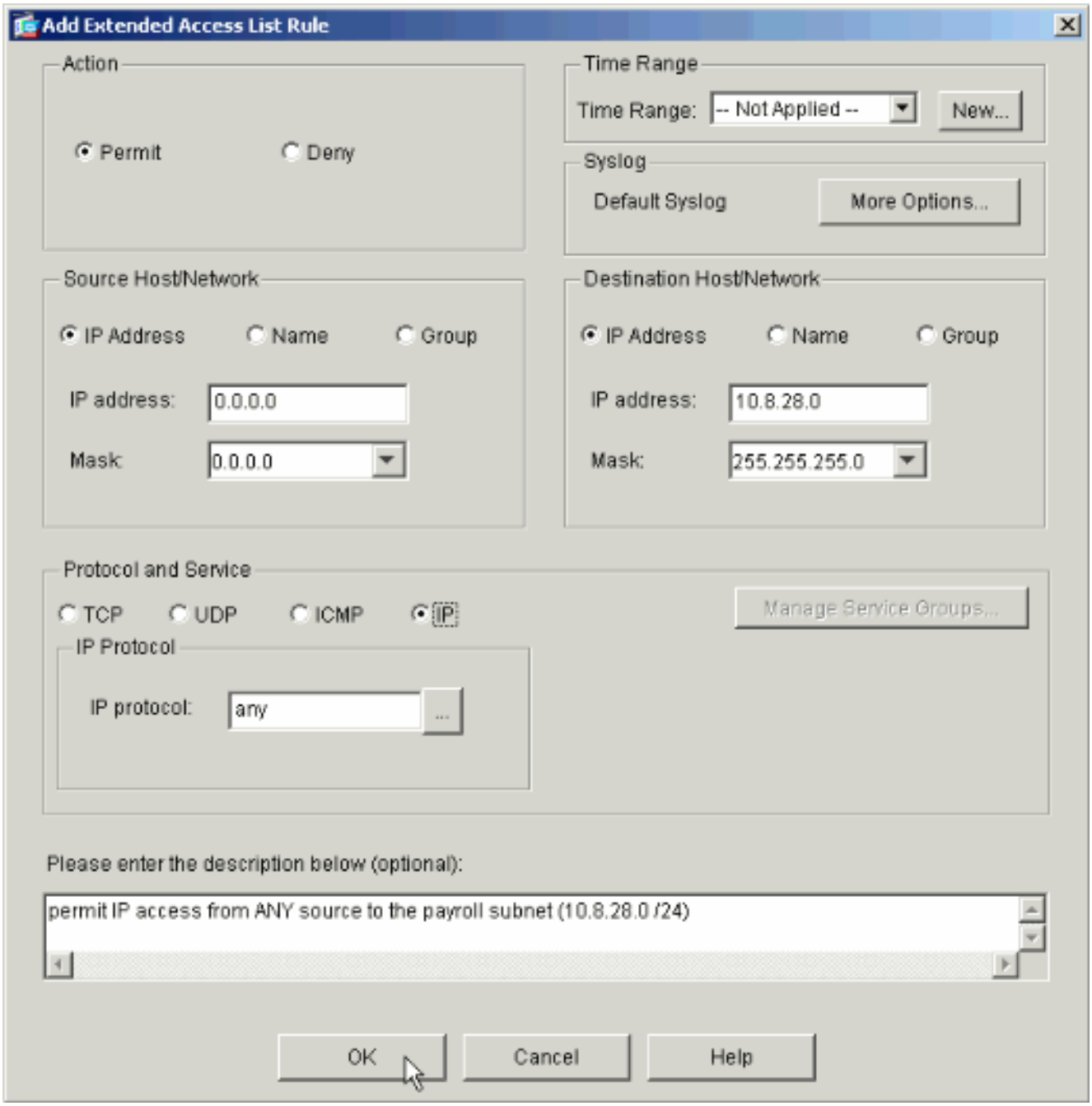
7. 왼쪽에서 새 ACL을 선택한 상태에서 **Add ACE(ACE 추가)**를 클릭하여 새 액세스 제어 항목을 목록에 추가합니다

.



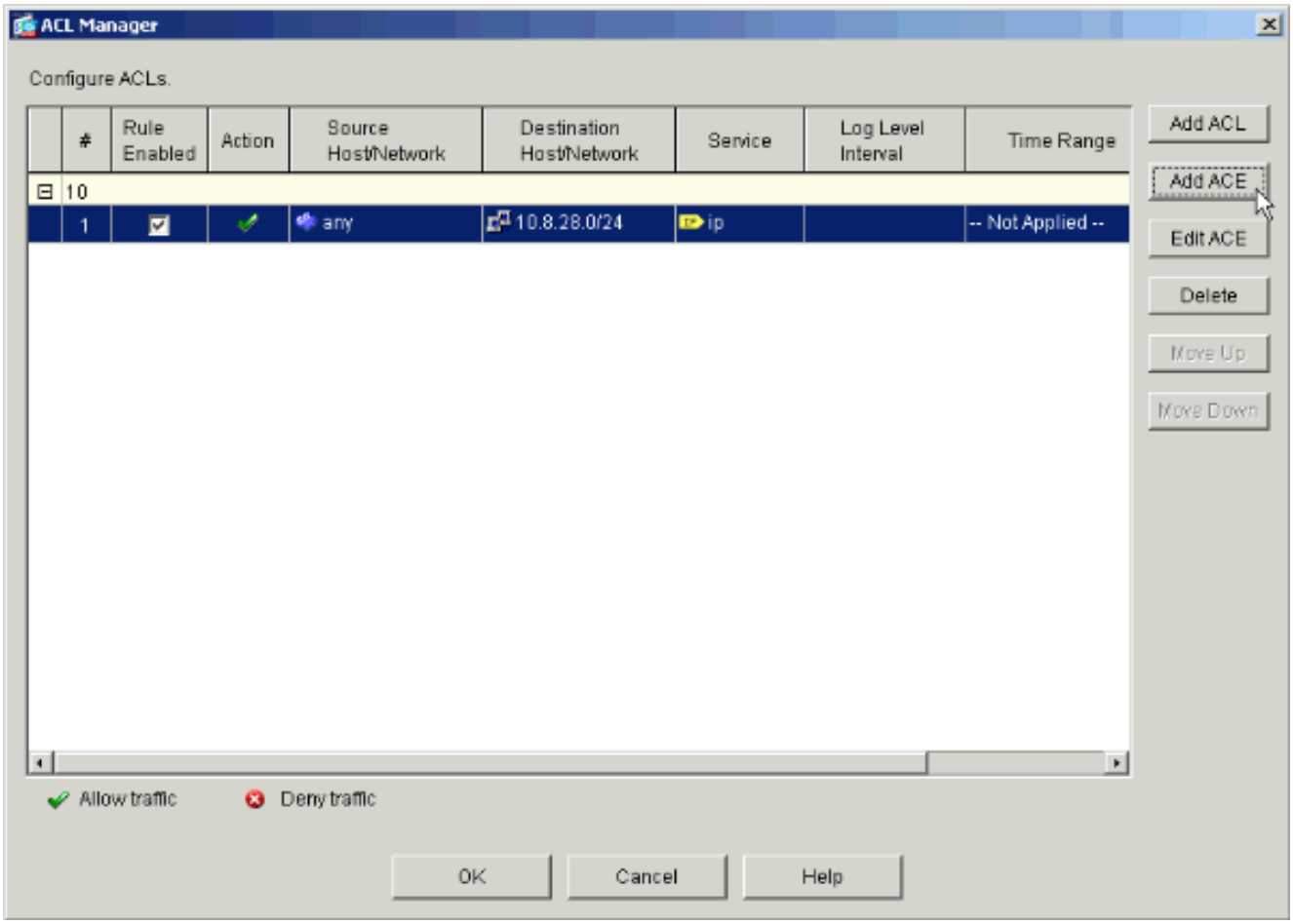
8. 추가할 ACE(액세스 제어 항목)를 정의합니다.이 예에서 ACL 10의 첫 번째 ACE는 모든 출처에서 급여 서브넷에 대한 IP 액세스를 허용합니다.**참고:** 기본적으로 ASDM은 TCP만 프로토콜로 선택합니다.사용자의 전체 IP 액세스를 허용하거나 거부하려면 IP를 선택해야 합니다.완료되면 **OK**(확인)를 클릭합니다

.



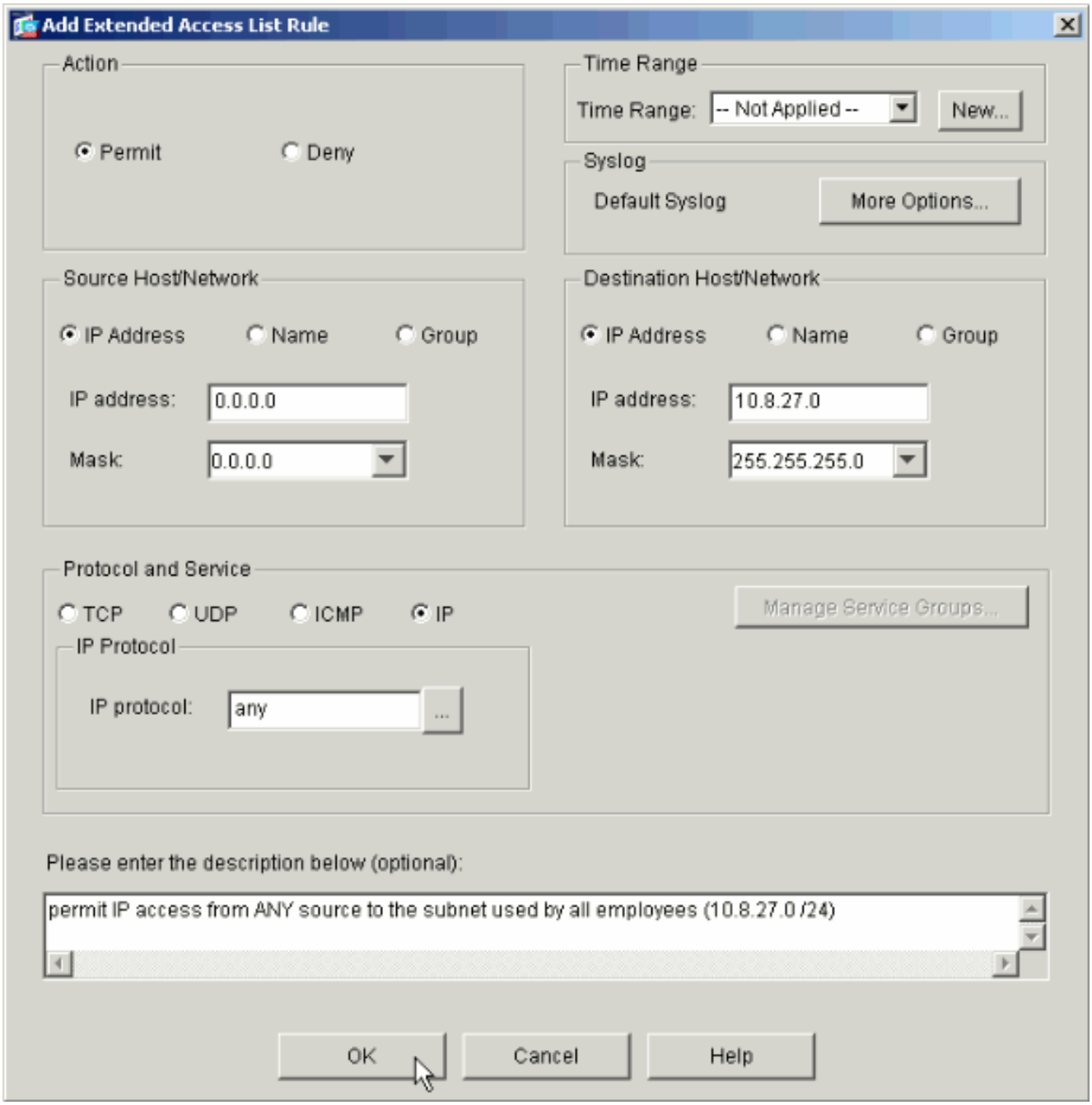
9. 방금 추가한 ACE가 목록에 나타납니다.Add **ACE(ACE 추가)**를 다시 선택하여 액세스 목록에 추가 라인을 추가합니다

.



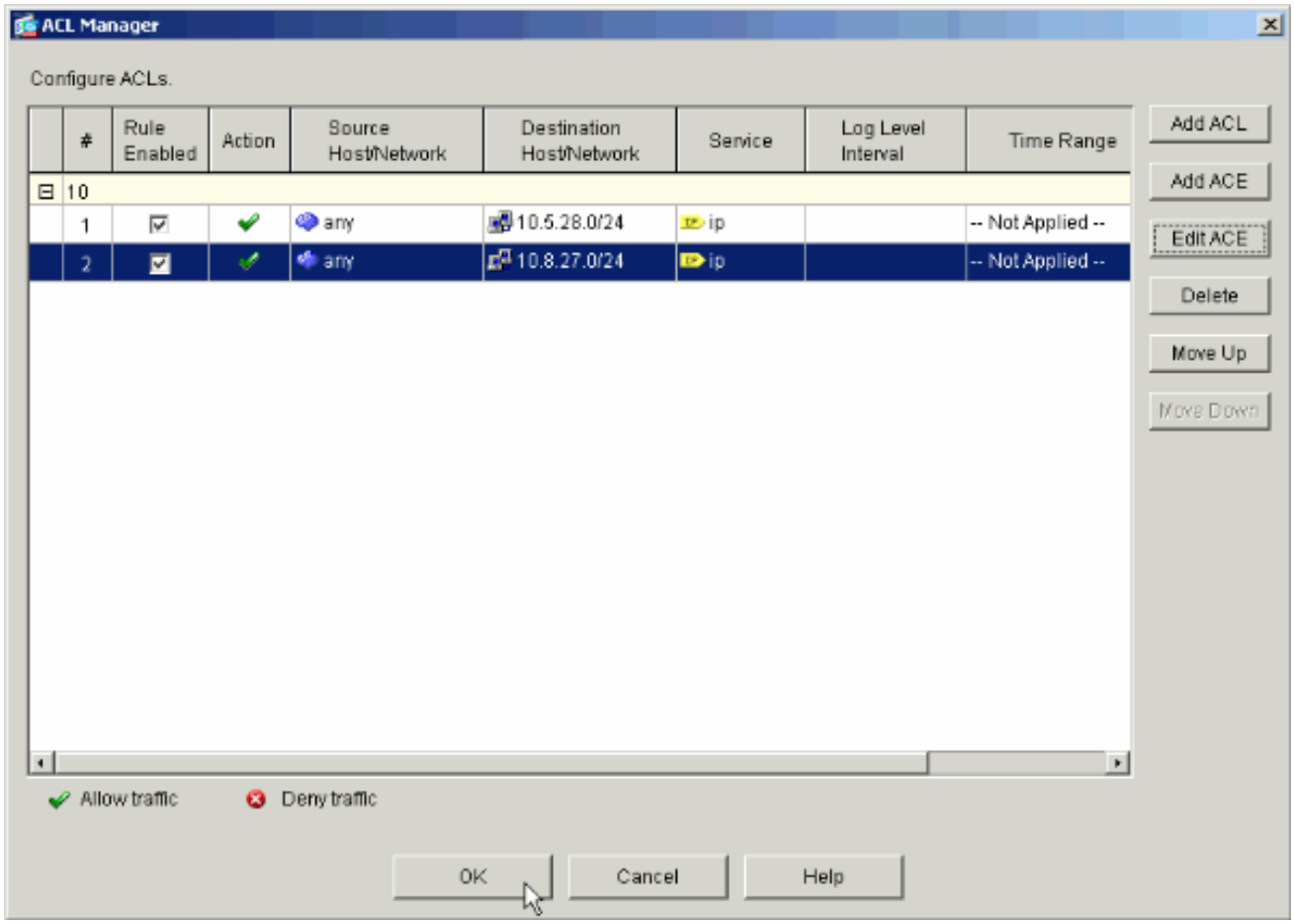
이 예에서는 인트라넷 서브넷에 대한 액세스를 허용하기 위해 두 번째 ACE가 ACL 10에 추가됩니다

.



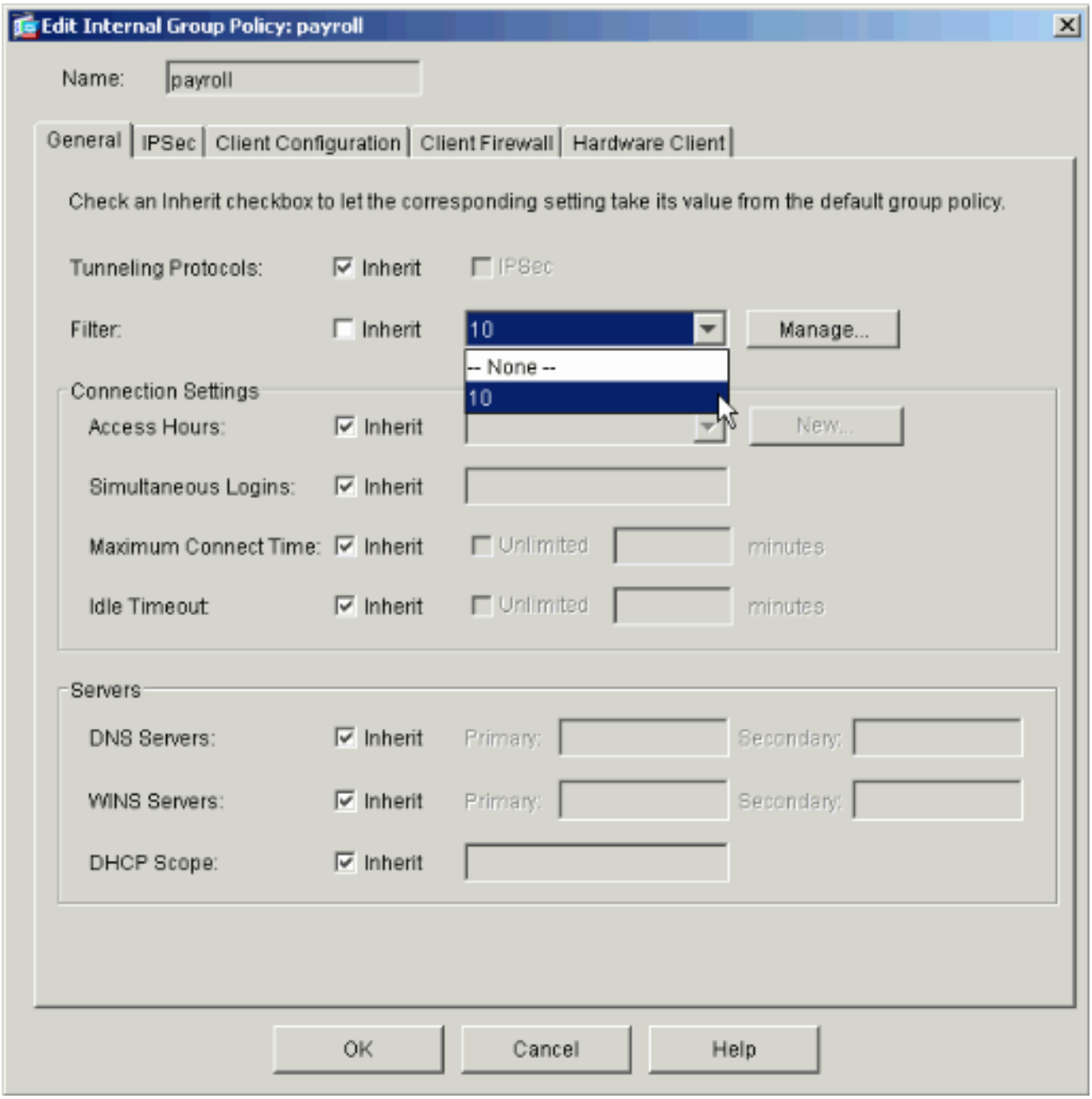
10. ACE **추가**가 완료되면 확인을 클릭합니다

.



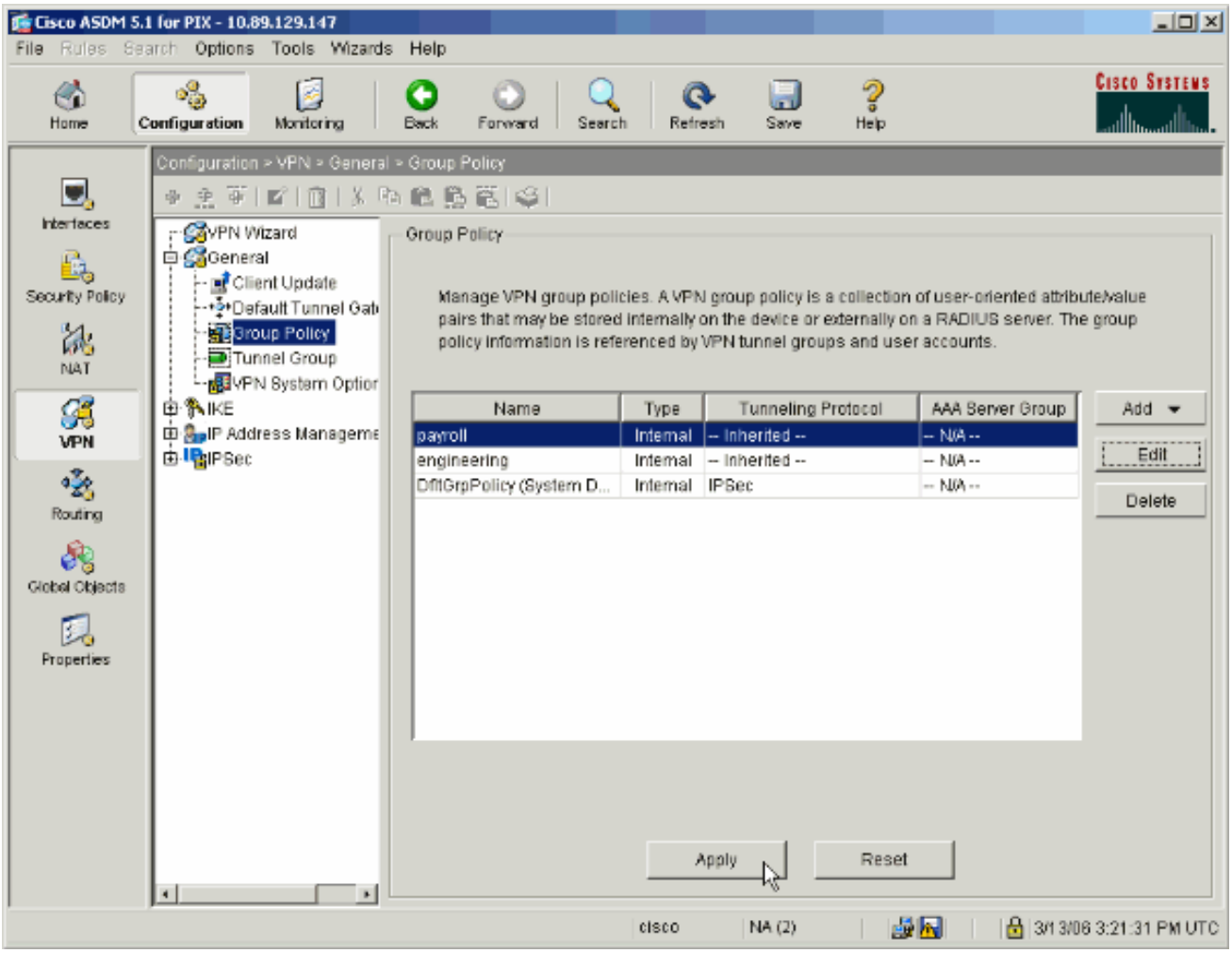
11. 그룹 정책의 필터가 되도록 마지막 단계에서 정의 및 입력 된 ACL을 선택 합니다.완료되면 **OK**(확인)를 클릭합니다

.



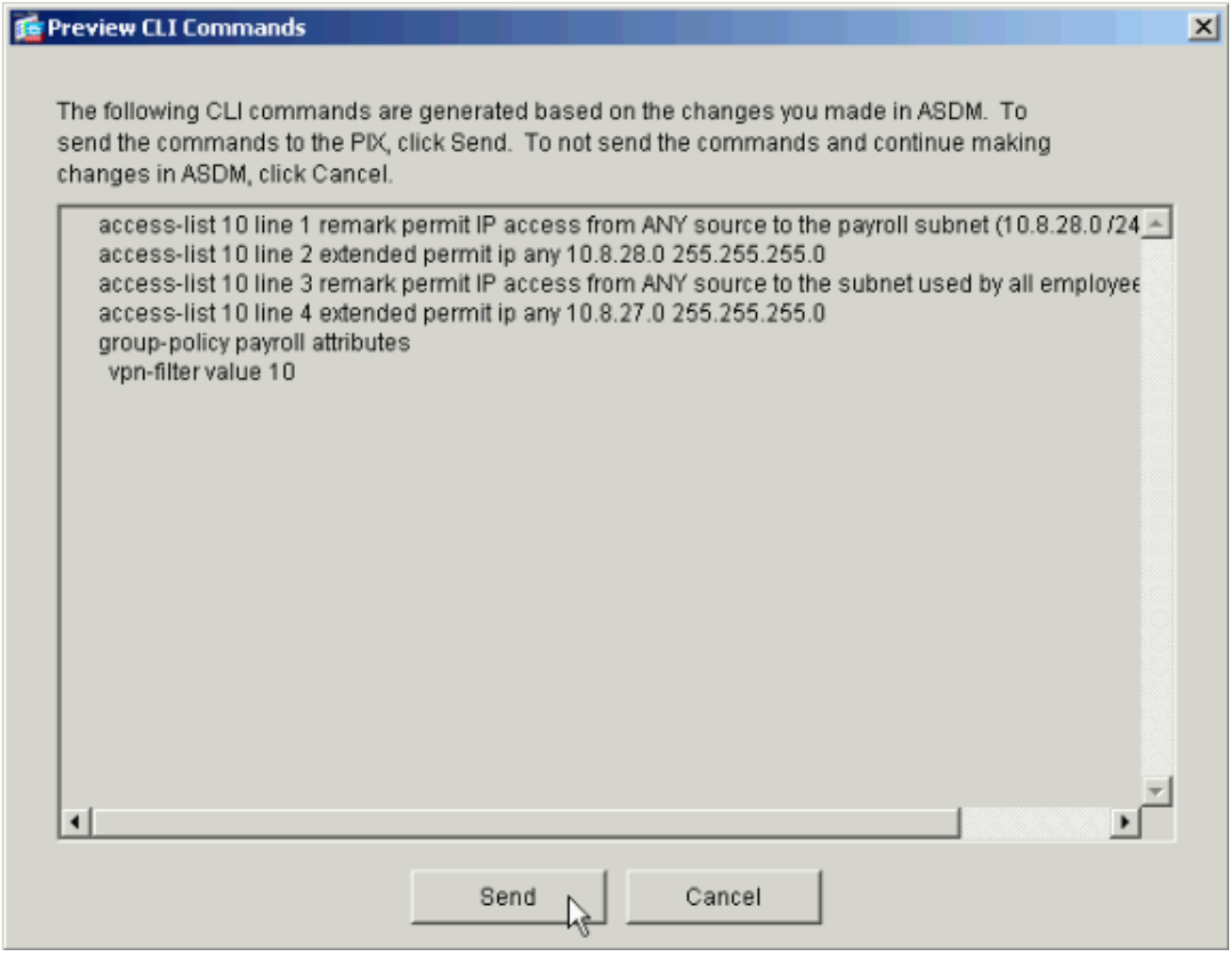
12. Apply(**적용**)를 클릭하여 변경 사항을 PIX에 전송합니다

.



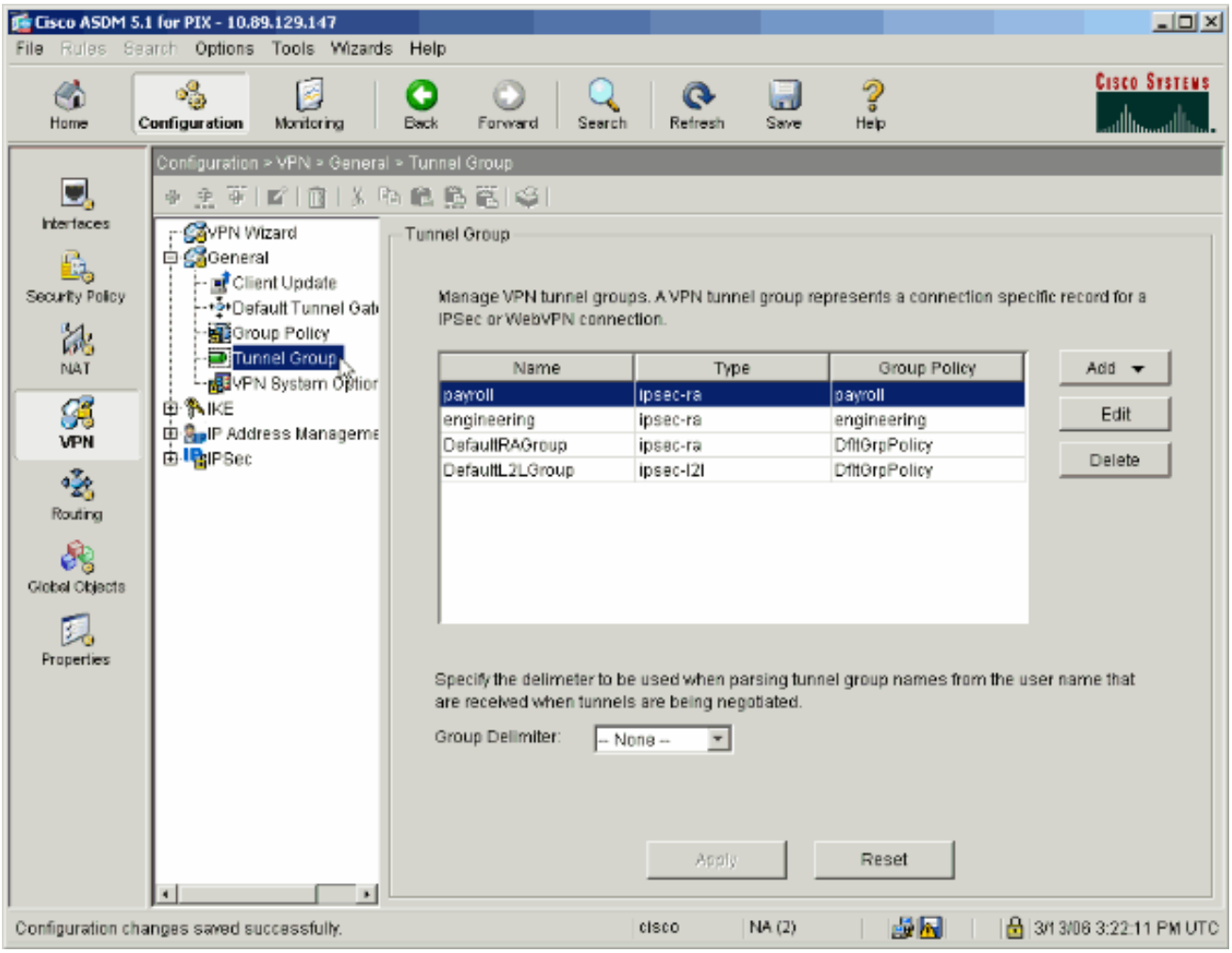
13. **Options > Preferences(옵션)**에서 **수행하도록** 구성한 경우 ASDM에서는 PIX로 전송하려는 명령을 미리 봅니다.Send를 **클릭합니다**

.



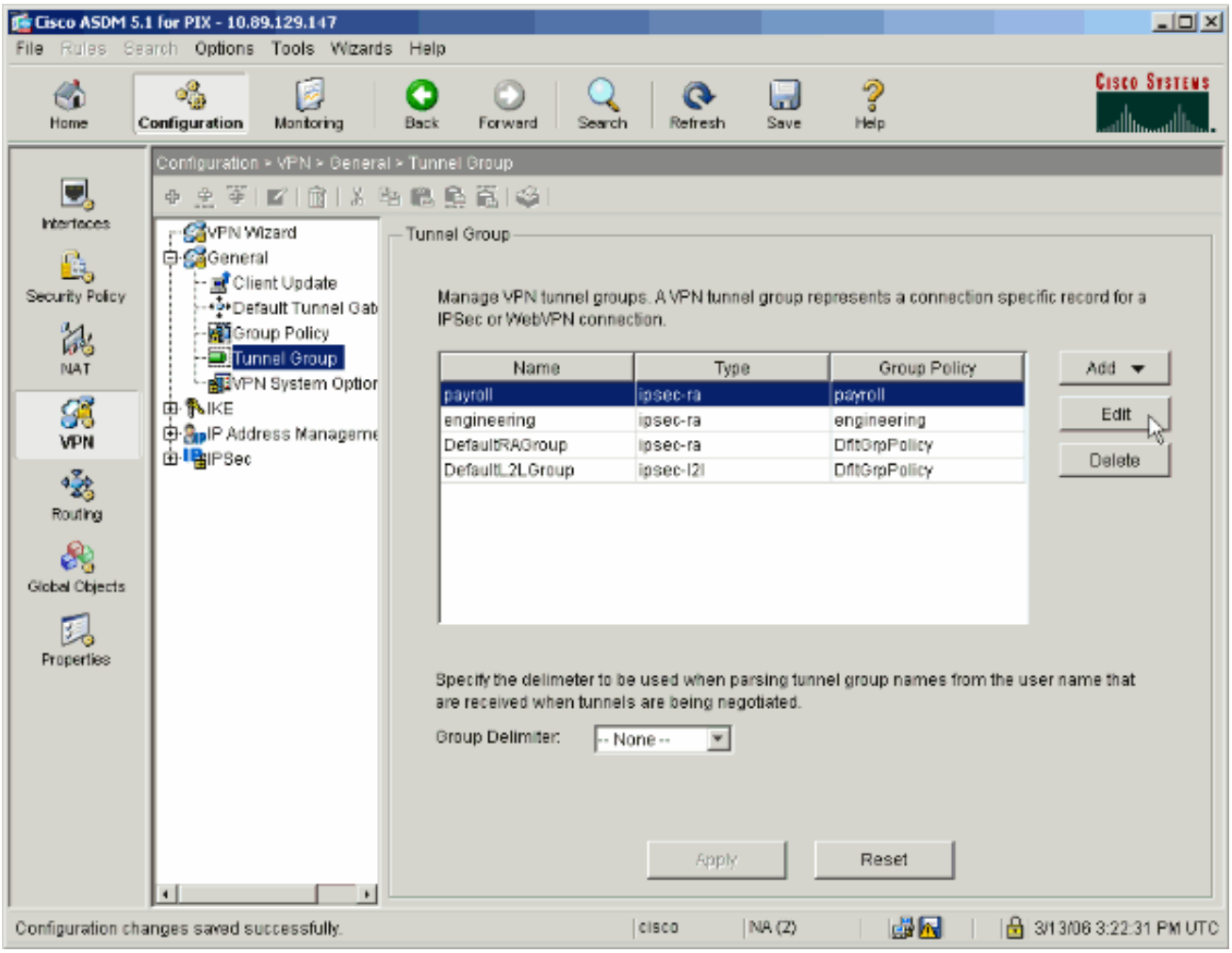
14. 방금 생성했거나 수정한 그룹 정책을 올바른 터널 그룹에 적용합니다.왼쪽 프레임에서 **Tunnel Group**을 클릭합니다

.



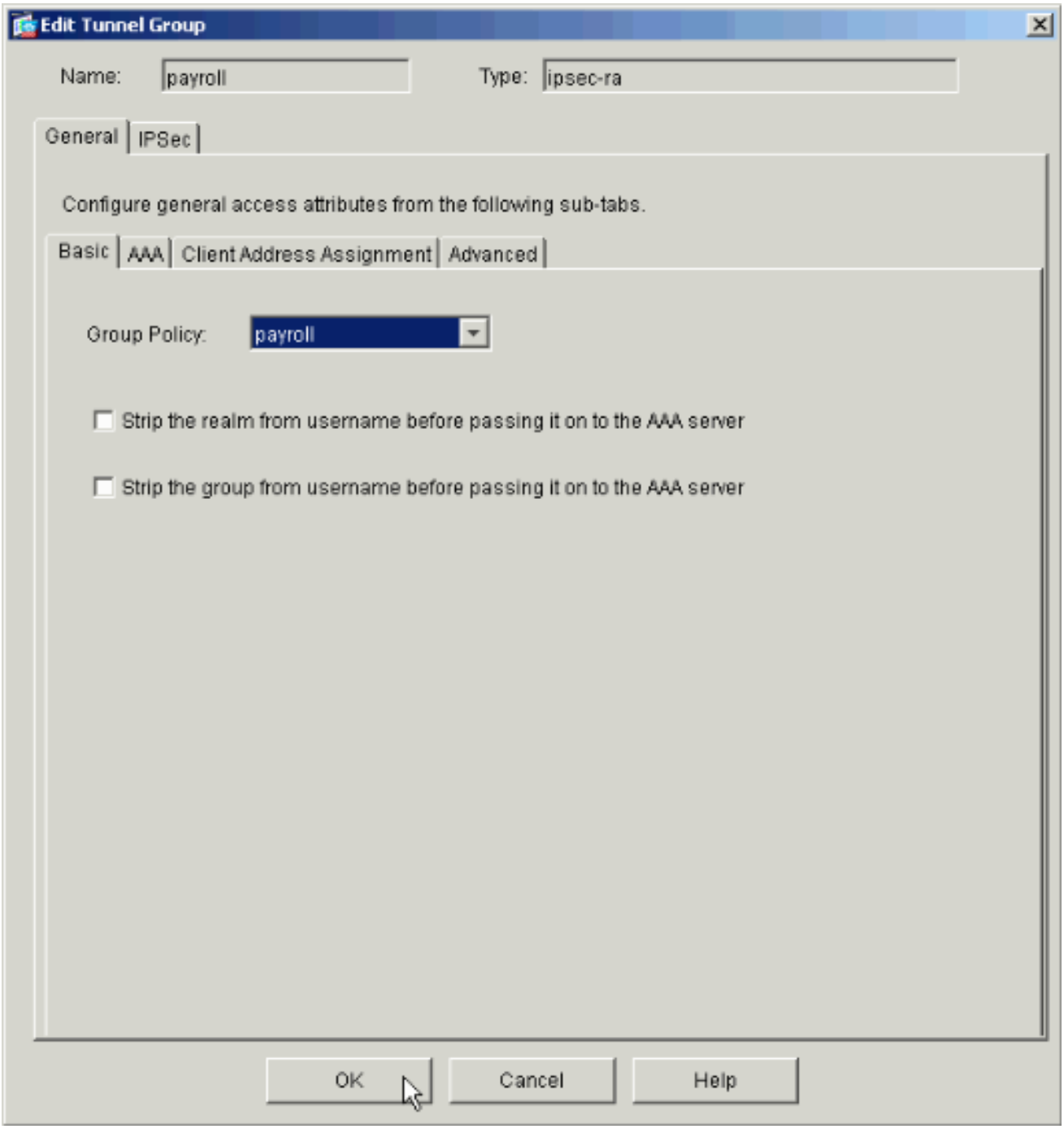
15. 그룹 정책을 적용할 터널 그룹을 선택하고 Edit를 **클릭합니다**

.

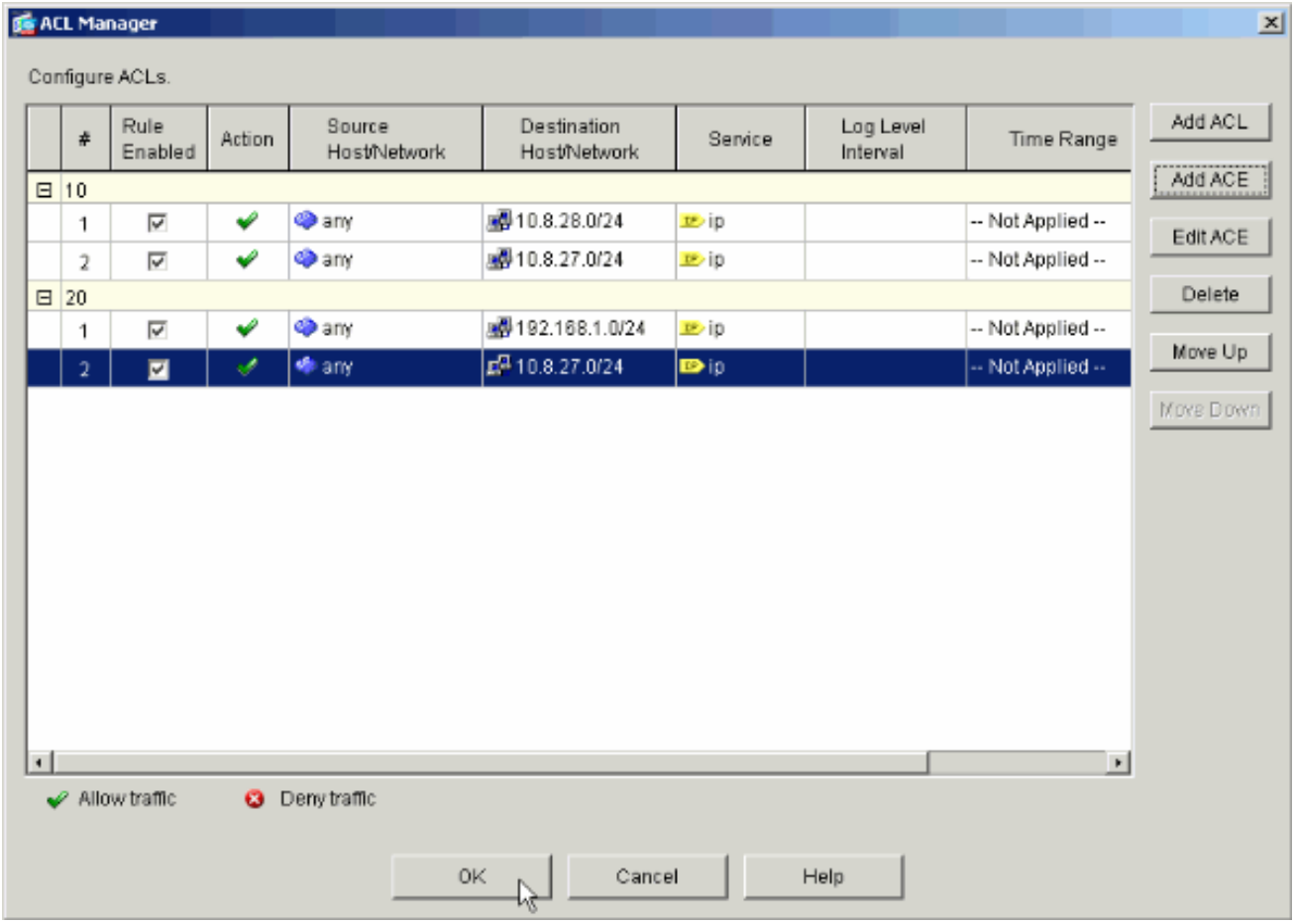


16. 그룹 정책이 자동으로 생성된 경우(2단계 참조) 드롭다운 상자에서 방금 구성한 그룹 정책이 선택되었는지 확인합니다.그룹 정책이 자동으로 구성되지 않은 경우 드롭다운 상자에서 선택합니다.완료되면 **OK**(확인)를 클릭합니다

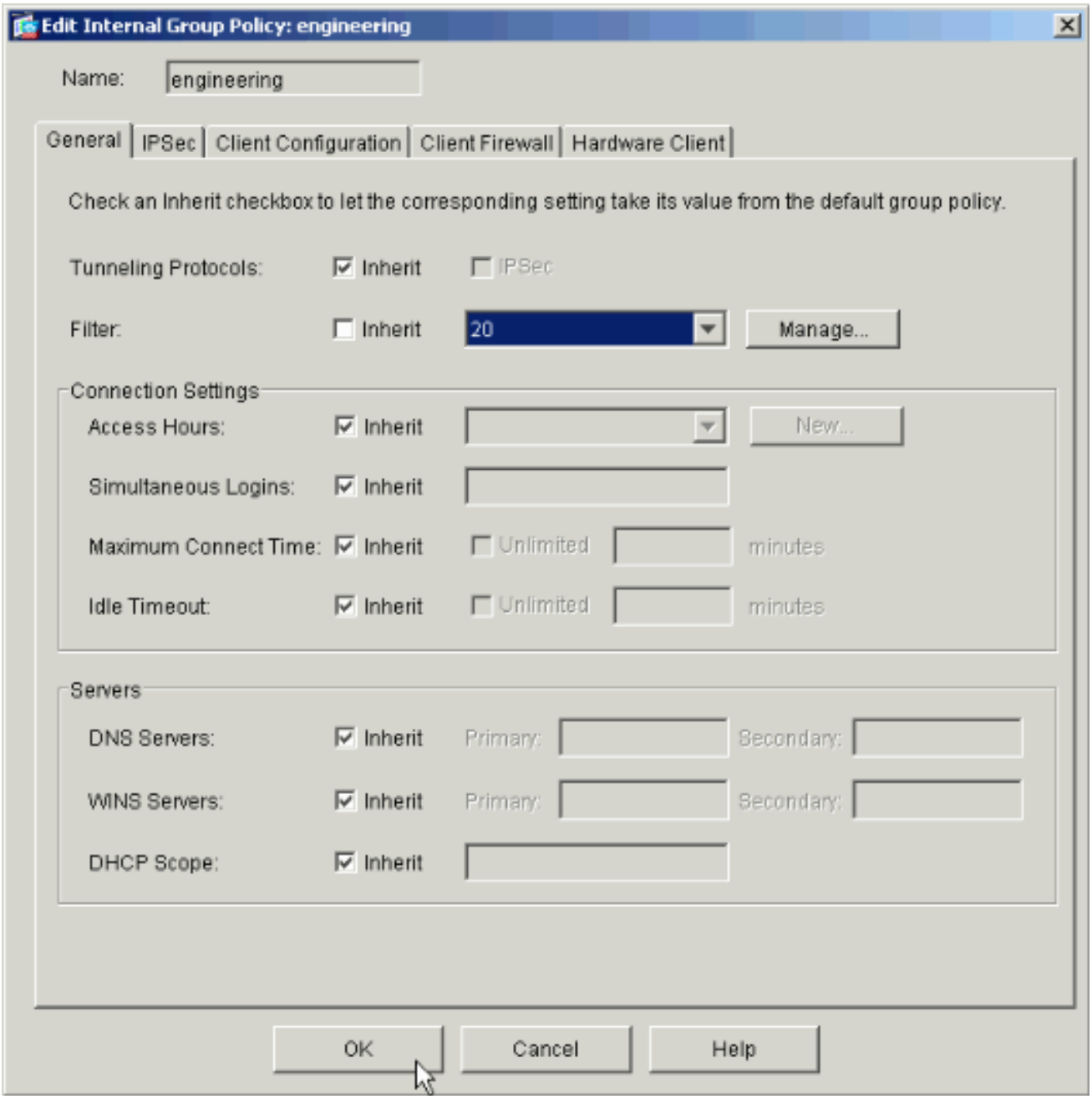
.



17. Apply(**적용**)를 클릭하고 메시지가 표시되면 Send(**보내기**)를 클릭하여 PIX 컨피그레이션에 변경 사항을 추가합니다.그룹 정책을 이미 선택한 경우 "변경 사항이 없습니다."라는 메시지가 표시될 수 있습니다. **확인**을 **클릭합니다**.
18. 제한을 추가하려는 추가 터널 그룹에 대해 2~17단계를 반복합니다.이 컨피그레이션 예에서는 엔지니어의 액세스를 제한해야 합니다.절차는 같지만 몇 가지 차이점이 눈에 띄는 부분입니다.새 액세스 목록

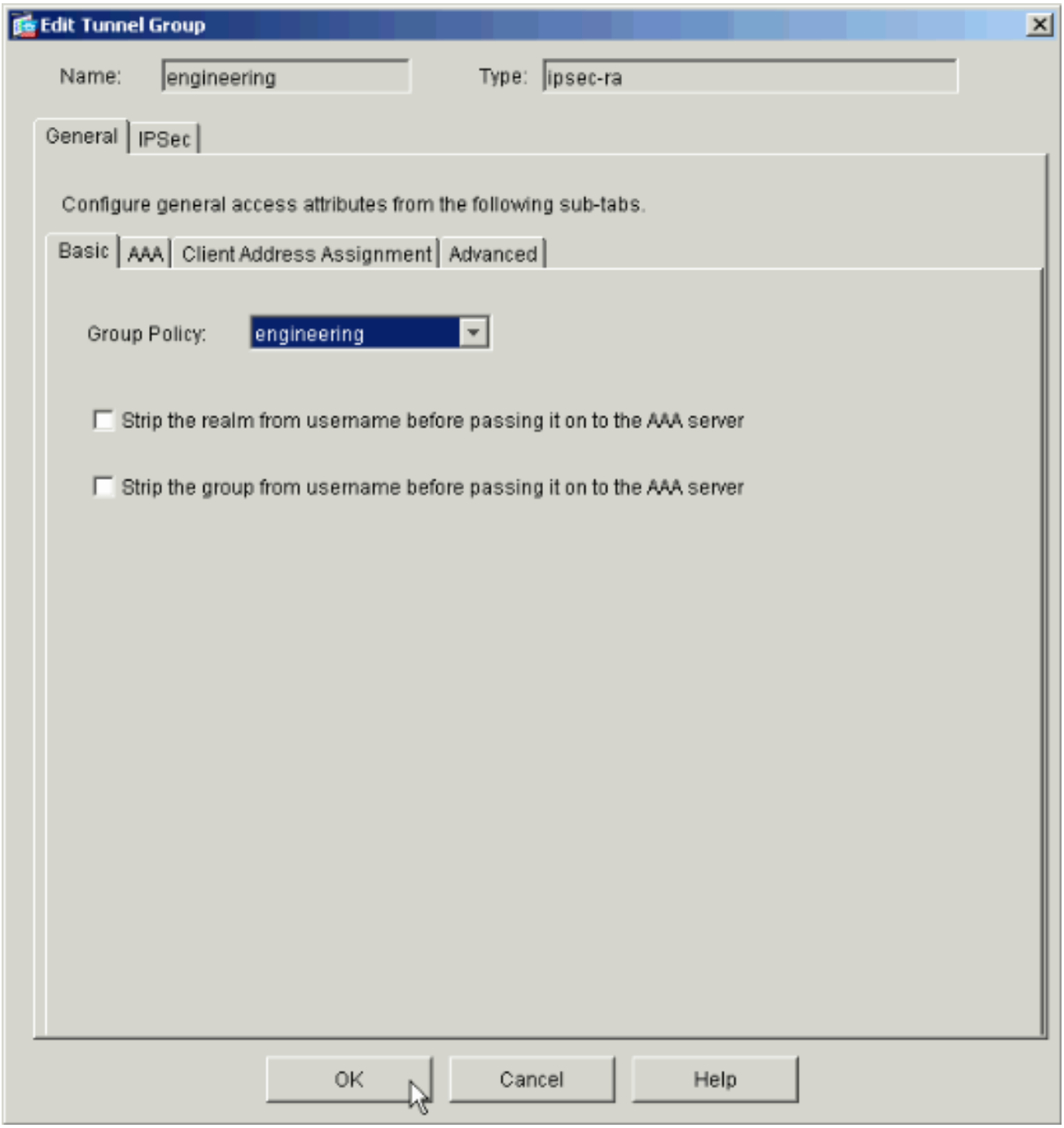


Engineering **Group Policy**(엔지니어링 그룹 정책)에서 Access List 20을 필터로 선택합니다 .



엔지니어링 그룹 정책이 엔지니어링 터널 그룹에 대해 설정되어 있는지 확인합니다

.



CLI를 통한 액세스 구성

CLI를 사용하여 보안 어플라이언스를 구성하려면 다음 단계를 완료합니다.

참고: 이 출력에 표시된 명령 중 일부는 공간 이유로 인해 두 번째 줄로 내려갑니다.

1. 원격 액세스 VPN에 연결할 때 사용자에게 적용되는 두 개의 서로 다른 액세스 제어 목록(15와 20)을 만듭니다.이 액세스 목록은 컨피그레이션의 뒷부분에서 호출됩니다.

```
ASAwCSC-CLI(config)#access-list 15 remark permit IP access from ANY
source to the payroll subnet (10.8.28.0/24)

ASAwCSC-CLI(config)#access-list 15 extended permit ip
any 10.8.28.0 255.255.255.0

ASAwCSC-CLI(config)#access-list 15 remark Permit IP access from ANY
source to the subnet used by all employees (10.8.27.0)
```

```
ASAwCSC-CLI(config)#access-list 15 extended permit ip
any 10.8.27.0 255.255.255.0

ASAwCSC-CLI(config)#access-list 20 remark Permit IP access from ANY
source to the Engineering subnet (192.168.1.0/24)

ASAwCSC-CLI(config)#access-list 20 extended permit ip
any 192.168.1.0 255.255.255.0

ASAwCSC-CLI(config)#access-list 20 remark Permit IP access from ANY
source to the subnet used by all employees (10.8.27.0/24)

ASAwCSC-CLI(config)#access-list 20 extended permit ip
any 10.8.27.0 255.255.255.0
```

2. 두 개의 서로 다른 VPN 주소 풀을 생성합니다.Payroll에 대해 하나를 생성하고 Engineering 원격 사용자에 대해 하나를 생성합니다.

```
ASAwCSC-CLI(config)#ip local pool Payroll-VPN
172.10.1.100-172.10.1.200 mask 255.255.255.0

ASAwCSC-CLI(config)#ip local pool Engineer-VPN 172.16.2.1-172.16.2.199
mask 255.255.255.0
```

3. 연결할 때만 적용되는 Payroll에 대한 정책을 생성합니다.

```
ASAwCSC-CLI(config)#group-policy Payroll internal

ASAwCSC-CLI(config)#group-policy Payroll attributes

ASAwCSC-CLI(config-group-policy)#dns-server value 10.8.27.10

ASAwCSC-CLI(config-group-policy)#vpn-filter value 15

!--- Call the ACL created in step 1 for Payroll. ASAwCSC-CLI(config-group-policy)#vpn-
tunnel-protocol IPSec

ASAwCSC-CLI(config-group-policy)#default-domain value payroll.corp.com

ASAwCSC-CLI(config-group-policy)#address-pools value Payroll-VPN

!--- Call the Payroll address space that you created in step 2.
```

4. 이 단계는 엔지니어링 그룹에 대한 것이라는 점을 제외하고 3단계와 동일합니다.

```
ASAwCSC-CLI(config)#group-policy Engineering internal

ASAwCSC-CLI(config)#group-policy Engineering attributes

ASAwCSC-CLI(config-group-policy)#dns-server value 10.8.27.10

ASAwCSC-CLI(config-group-policy)#vpn-filter value 20

!--- Call the ACL that you created in step 1 for Engineering. ASAwCSC-CLI(config-group-
policy)#vpn-tunnel-protocol IPSec

ASAwCSC-CLI(config-group-policy)#default-domain value Engineer.corp.com

ASAwCSC-CLI(config-group-policy)#address-pools value Engineer-VPN

!--- Call the Engineering address space that you created in step 2.
```

5. 로컬 사용자를 생성하고 해당 사용자에게 방금 생성한 속성을 할당하여 리소스에 대한 액세스를 제한합니다.

```
ASAwCSC-CLI(config)#username engineer password cisco123
```

```
ASAwCSC-CLI(config)#username engineer attributes

ASAwCSC-CLI(config-username)#vpn-group-policy Engineering

ASAwCSC-CLI(config-username)#vpn-filter value 20

ASAwCSC-CLI(config)#username marty password cisco456

ASAwCSC-CLI(config)#username marty attributes

ASAwCSC-CLI(config-username)#vpn-group-policy Payroll

ASAwCSC-CLI(config-username)#vpn-filter value 15
```

6. Payroll 사용자에 대한 연결 정책을 포함하는 터널 그룹을 생성합니다.

```
ASAwCSC-CLI(config)#tunnel-group Payroll type ipsec-ra

ASAwCSC-CLI(config)#tunnel-group Payroll general-attributes

ASAwCSC-CLI(config-tunnel-general)#address-pool Payroll-VPN

ASAwCSC-CLI(config-tunnel-general)#default-group-policy Payroll

ASAwCSC-CLI(config)#tunnel-group Payroll ipsec-attributes

 ASAwCSC-CLI(config-tunnel-ipsec)#pre-shared-key time1234
```

7. 엔지니어링 사용자에 대한 연결 정책을 포함하는 터널 그룹을 생성합니다.

```
ASAwCSC-CLI(config)#tunnel-group Engineering type ipsec-ra

ASAwCSC-CLI(config)#tunnel-group Engineering general-attributes

ASAwCSC-CLI(config-tunnel-general)#address-pool Engineer-VPN

ASAwCSC-CLI(config-tunnel-general)#default-group-policy Engineering

ASAwCSC-CLI(config)#tunnel-group Engineering ipsec-attributes

ASAwCSC-CLI(config-tunnel-ipsec)#pre-shared-key Engine123
```

컨피그레이션을 입력하면 컨피그레이션에서 강조 표시된 영역을 볼 수 있습니다.

장치 이름 1

```
ASA-AIP-CLI(config)#show running-config

ASA Version 7.2(2)
!
hostname ASAwCSC-ASDM
domain-name corp.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
!
interface Ethernet0/0
 nameif Intranet
 security-level 0
 ip address 10.8.27.2 255.255.255.0
!
interface Ethernet0/1
 nameif Engineer
```

```
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif Payroll
 security-level 100
 ip address 10.8.28.0
!
interface Ethernet0/3
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name corp.com
access-list Inside_nat0_outbound extended permit ip any
172.10.1.0 255.255.255.0
access-list Inside_nat0_outbound extended permit ip any
172.16.2.0 255.255.255.0
access-list 15 remark permit IP access from ANY source
to the
   Payroll subnet (10.8.28.0/24)
access-list 15 extended permit ip any 10.8.28.0
255.255.255.0
access-list 15 remark Permit IP access from ANY source
to the subnet
   used by all employees (10.8.27.0)
access-list 15 extended permit ip any 10.8.27.0
255.255.255.0
access-list 20 remark Permit IP access from Any source
to the Engineering
   subnet (192.168.1.0/24)
access-list 20 extended permit ip any 192.168.1.0
255.255.255.0
access-list 20 remark Permit IP access from Any source
to the subnet used
   by all employees (10.8.27.0/24)
access-list 20 extended permit ip any 10.8.27.0
255.255.255.0
pager lines 24
mtu MAN 1500
mtu Outside 1500
mtu Inside 1500
ip local pool Payroll-VPN 172.10.1.100-172.10.1.200 mask
255.255.255.0
ip local pool Engineer-VPN 172.16.2.1-172.16.2.199 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-522.bin
no asdm history enable
arp timeout 14400
global (Intranet) 1 interface
nat (Inside) 0 access-list Inside_nat0_outbound
nat (Inside) 1 192.168.1.0 255.255.255.0
nat (Inside) 1 10.8.27.0 255.255.255.0
nat (Inside) 1 10.8.28.0 255.255.255.0
```

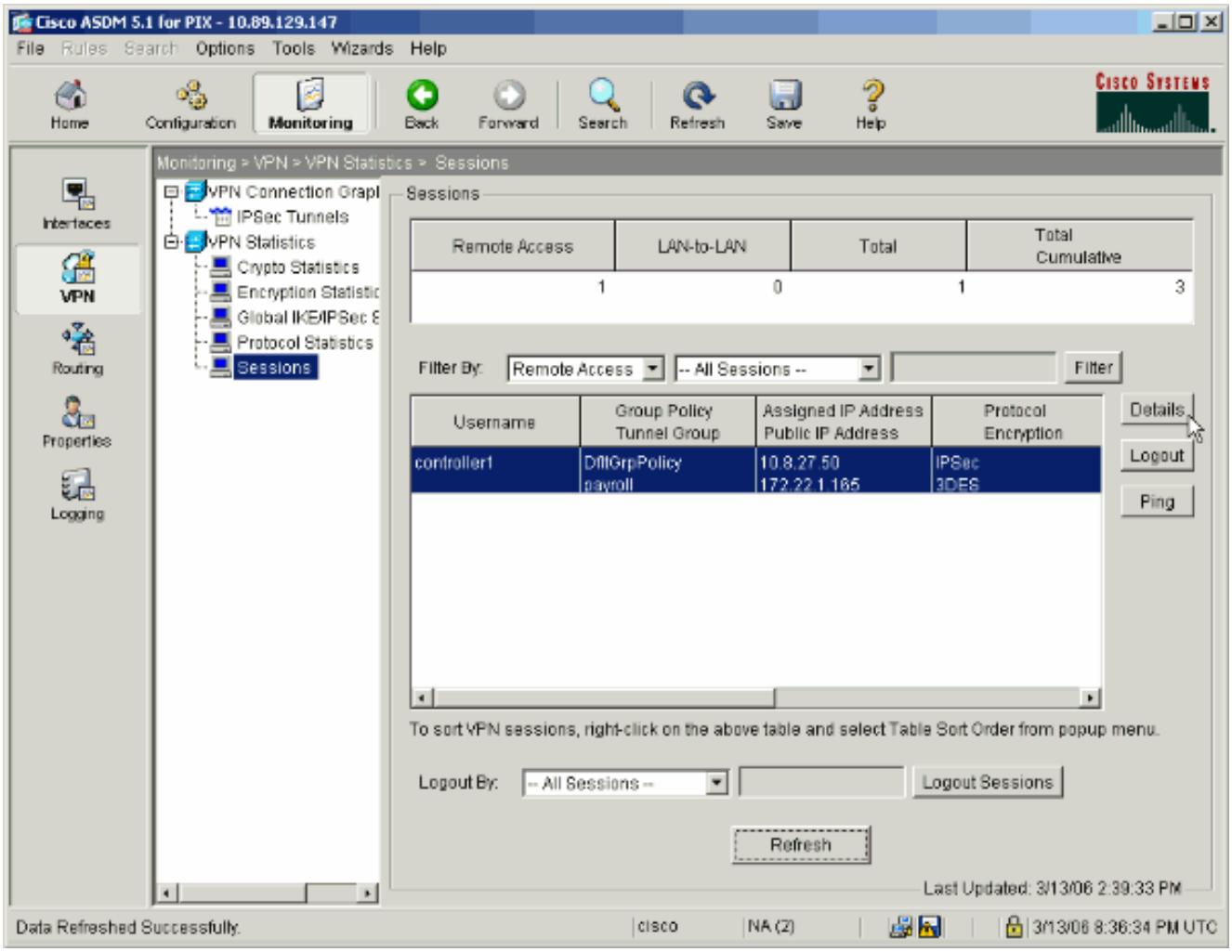
```
route Intranet 0.0.0.0 0.0.0.0 10.8.27.2
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
group-policy Payroll internal
group-policy Payroll attributes
 dns-server value 10.8.27.10
 vpn-filter value 15
 vpn-tunnel-protocol IPSec
 default-domain value payroll.corp.com
 address-pools value Payroll-VPN
group-policy Engineering internal
group-policy Engineering attributes
 dns-server value 10.8.27.10
 vpn-filter value 20
 vpn-tunnel-protocol IPSec
 default-domain value Engineer.corp.com
 address-pools value Engineer-VPN
username engineer password LCaPXI.4Xtvclaca encrypted
username engineer attributes
 vpn-group-policy Engineering
 vpn-filter value 20
username marty password 6XmYwQOO9tiYnUDN encrypted
privilege 0
username marty attributes
 vpn-group-policy Payroll
 vpn-filter value 15
no snmp-server location
no snmp-server contact
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac
crypto dynamic-map Outside_dyn_map 20 set pfs
crypto dynamic-map Outside_dyn_map 20 set transform-set
ESP-3DES-SHA
crypto map Outside_map 65535 ipsec-isakmp dynamic
Outside_dyn_map
crypto map Outside_map interface Outside
crypto isakmp enable Outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
tunnel-group Payroll type ipsec-ra
tunnel-group Payroll general-attributes
 address-pool vpnpool
 default-group-policy Payroll
tunnel-group Payroll ipsec-attributes
 pre-shared-key *
tunnel-group Engineering type ipsec-ra
tunnel-group Engineering general-attributes
 address-pool Engineer-VPN
 default-group-policy Engineering
tunnel-group Engineering ipsec-attributes
 pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
```

```
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  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
prompt hostname context
Cryptochecksum:0e579c85004dcfb4071cb561514a392b
: end
ASA-AIP-CLI(config)#
```

다음을 확인합니다.

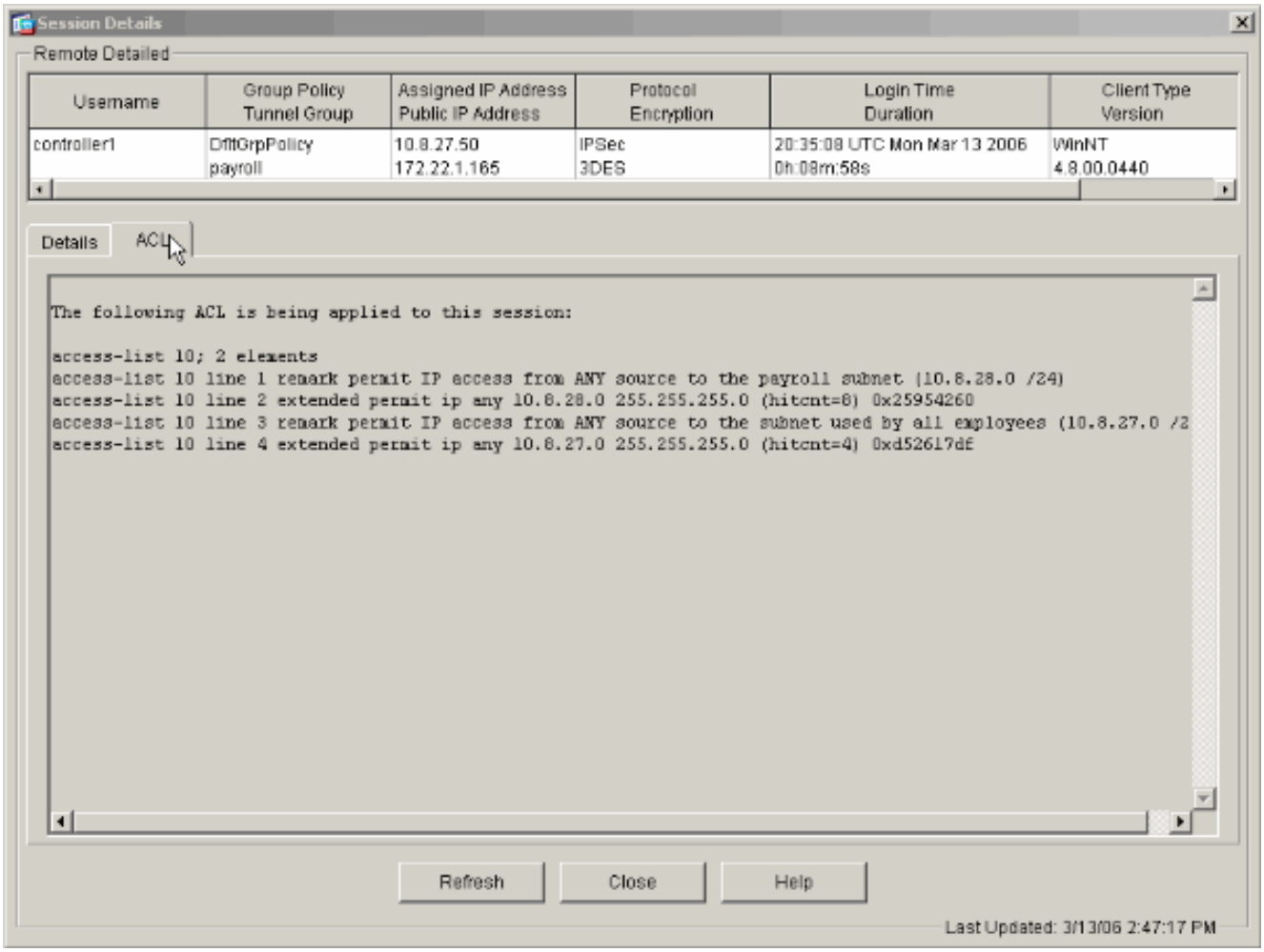
ASDM의 모니터링 기능을 사용하여 컨피그레이션을 확인합니다.

1. Monitoring **> VPN > VPN Statistics > Sessions를 선택합니다**.PIX에서 활성 VPN 세션이 표시됩니다.관심 있는 세션을 선택하고 **Details**를 클릭합니다
   .



2. ACL 탭을 선택합니다.ACL 히트는 클라이언트에서 허용된 네트워크로 터널을 통과하는 트래픽을 반영합니다

.



문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco ASA 5500 Series Adaptive Security Appliances ASA as a Remote VPN Server(ASDM 컨피그레이션 사용) 예
- Cisco PIX 500 Series Security Appliances 컨피그레이션 예 및 TechNotes
- Cisco ASA 5500 Series Adaptive Security Appliances 컨피그레이션 예 및 TechNotes
- Cisco VPN 클라이언트 컨피그레이션 예 및 기술 노트
- 기술 지원 및 문서 – Cisco Systems