PIX/ASA 7.x ASDM: De netwerktoegang van VPN-gebruikers die toegang hebben tot Remote Access beperken

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie met behulp van Cisco Adaptieve Security Devices Manager (ASDM) voor het beperken van wat interne netwerken voor VPN-gebruikers die toegang hebben tot externe netwerken achter de PIX security applicatie of adaptieve security applicatie (ASA). U kunt de externe toegang tot VPN-gebruikers beperken tot alleen de gebieden van het netwerk waartoe u toegang wilt hebben wanneer u:

1. Toegangslijsten maken.
2. Associeer ze met groepsbeleid.
3. Associeer dat groepsbeleid met tunnelgroepen.

Raadpleeg de Cisco VPN 3000 Concentrator configureren voor blokkering met filters en RADIUS-filtertoewijzing om meer te weten te komen over het scenario waarin de VPN-Concentrator de toegang van VPN-gebruikers blokkeert.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- De PIX kan worden ingesteld met behulp van de ASDM.**Opmerking:** Raadpleeg HTTPS-

toegang voor ASDM om de PIX te kunnen configureren door de ASDM.
- U hebt ten minste één bekende goede VPN-configuratie voor toegang op afstand.**Opmerking:** Als u geen van dergelijke configuraties hebt, raadpleegt u ASA als een Remote VPN-server met behulp van het ASDM Configuration Voorbeeld voor informatie over de configuratie van een goede externe VPN-configuratie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure PIX 500 Series security applicatie versie 7.1(1)**Opmerking:** De PIX 501 en 506E security applicaties ondersteunen versie 7.x niet.
- Cisco Adaptieve Security Adapter Manager versie 5.1(1)**Opmerking:** ASDM is alleen beschikbaar in PIX of ASA 7.x.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

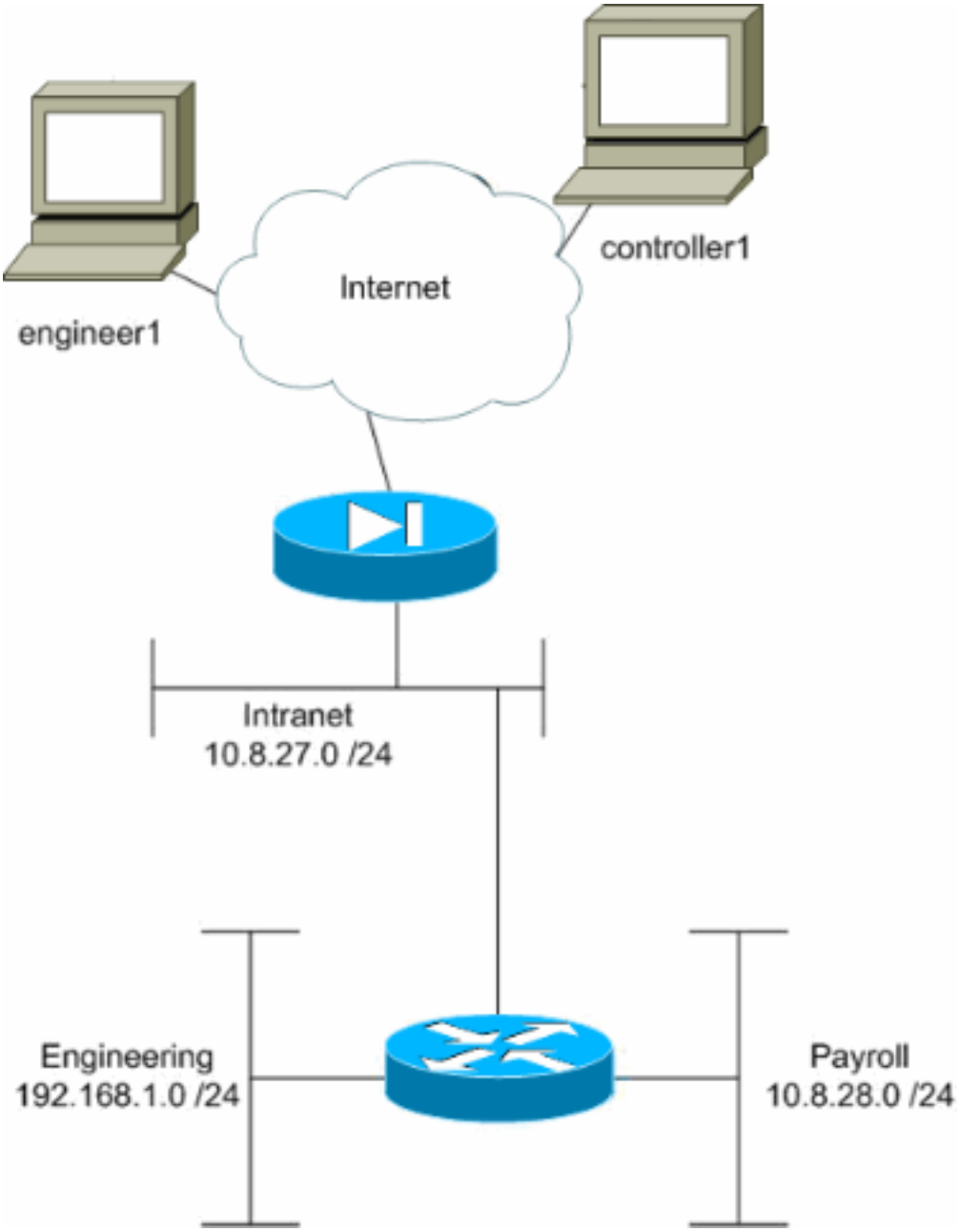
Verwante producten

Deze configuratie kan ook worden gebruikt in combinatie met deze hardware- en softwareversies:

- Cisco ASA 5500 Series adaptieve security applicatie, versie 7.1(1)

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



In dit configuratievoorbeeld is een klein bedrijfsnetwerk met drie subnetten verondersteld. Dit diagram illustreert de topologie. De drie subnetten zijn Intranet, Engineering en Payroll. Het doel van dit configuratievoorbeeld is om salarissen personeel op afstand toegang tot het Intranet en Loonsubnetwerk toe te staan en hen te verhinderen om toegang te krijgen tot het subnet van de Bouwnijverheid. Ook zouden de ingenieurs in staat moeten zijn om op afstand toegang te hebben tot het Intranet en de technische subnetten, maar niet tot het Subnet van de Betaling. De loonwerker in dit voorbeeld is "controller1". De technische gebruiker in dit voorbeeld is "ingenieur1".

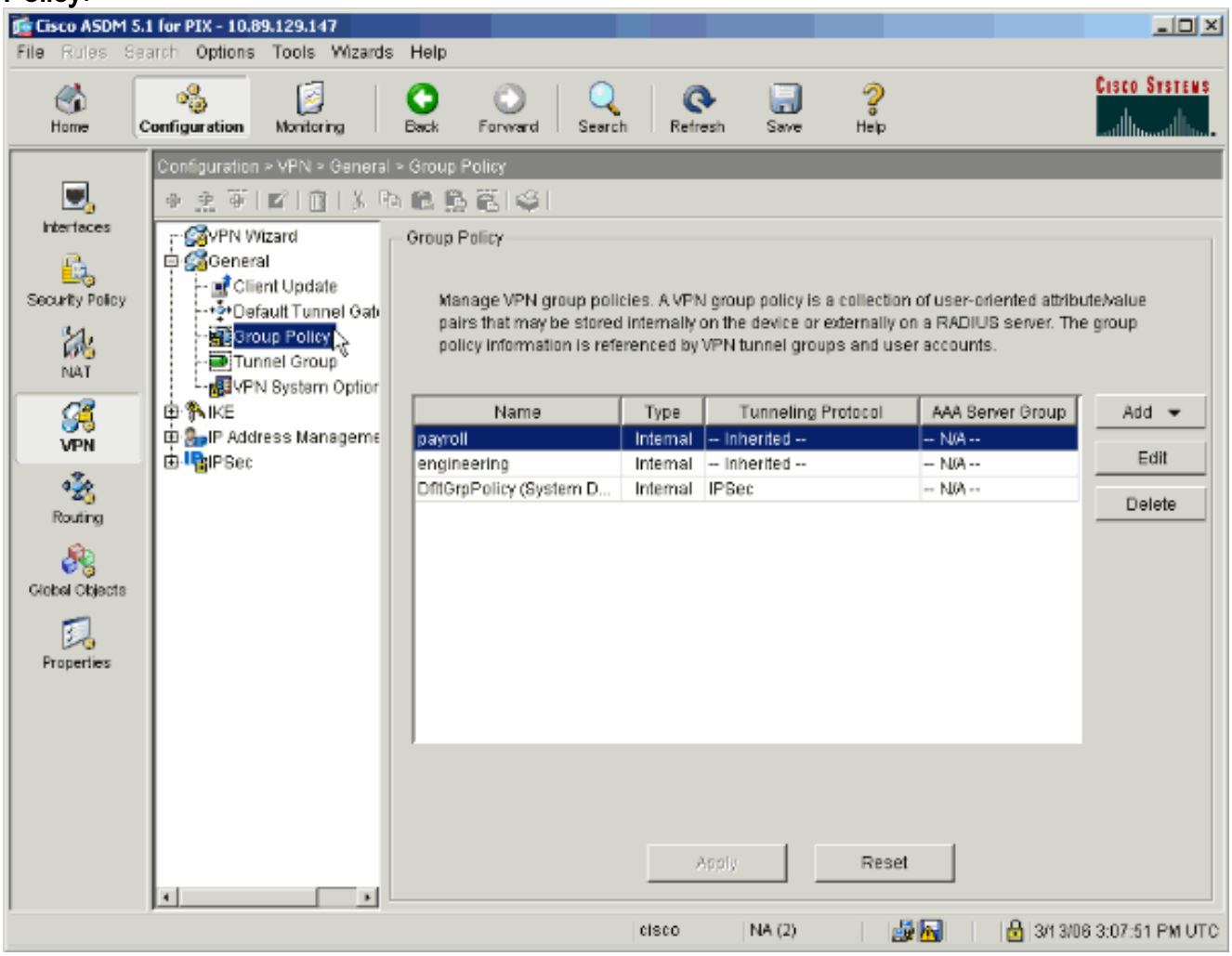
Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

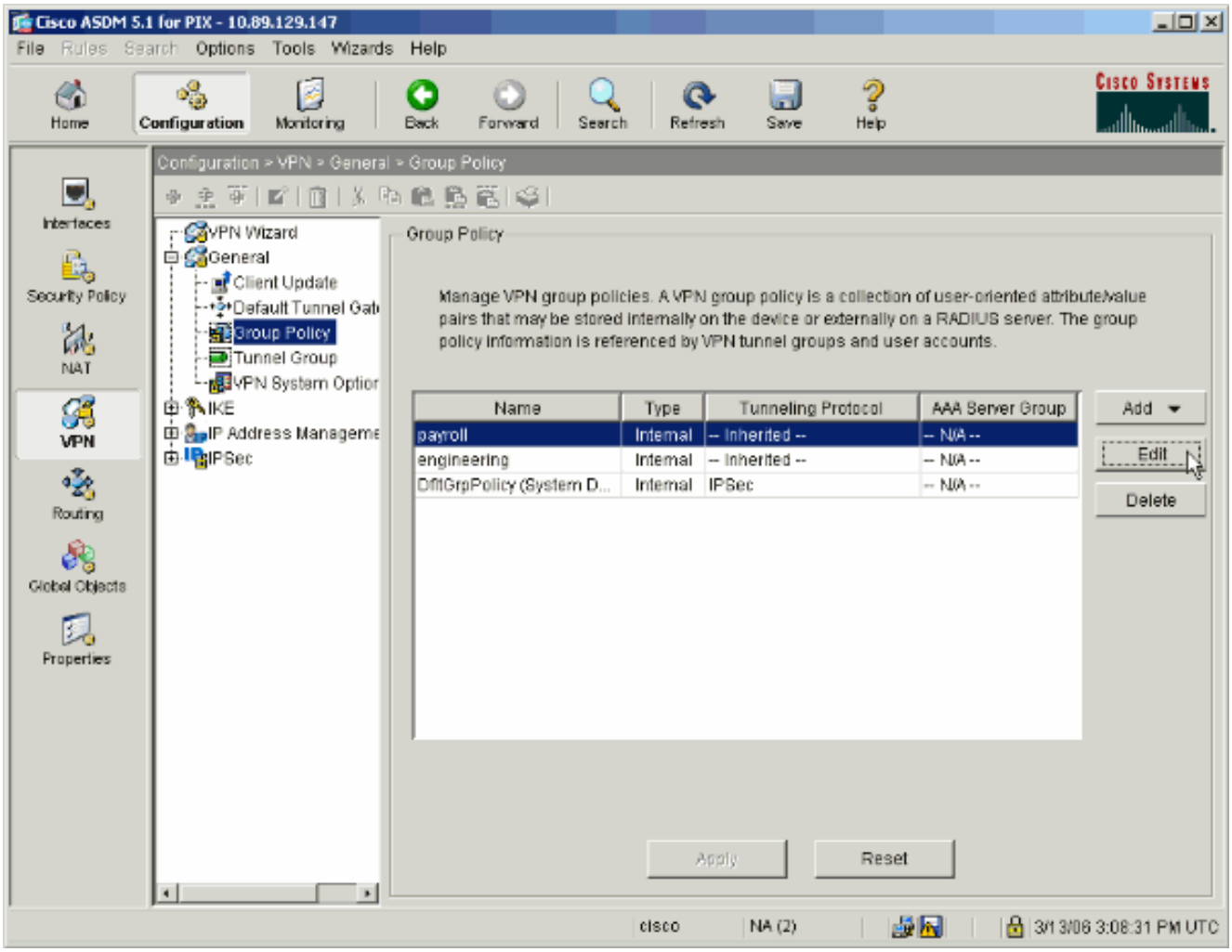
Toegang configureren via ASDM

Volg deze stappen om de PIX security applicatie te configureren met ASDM:

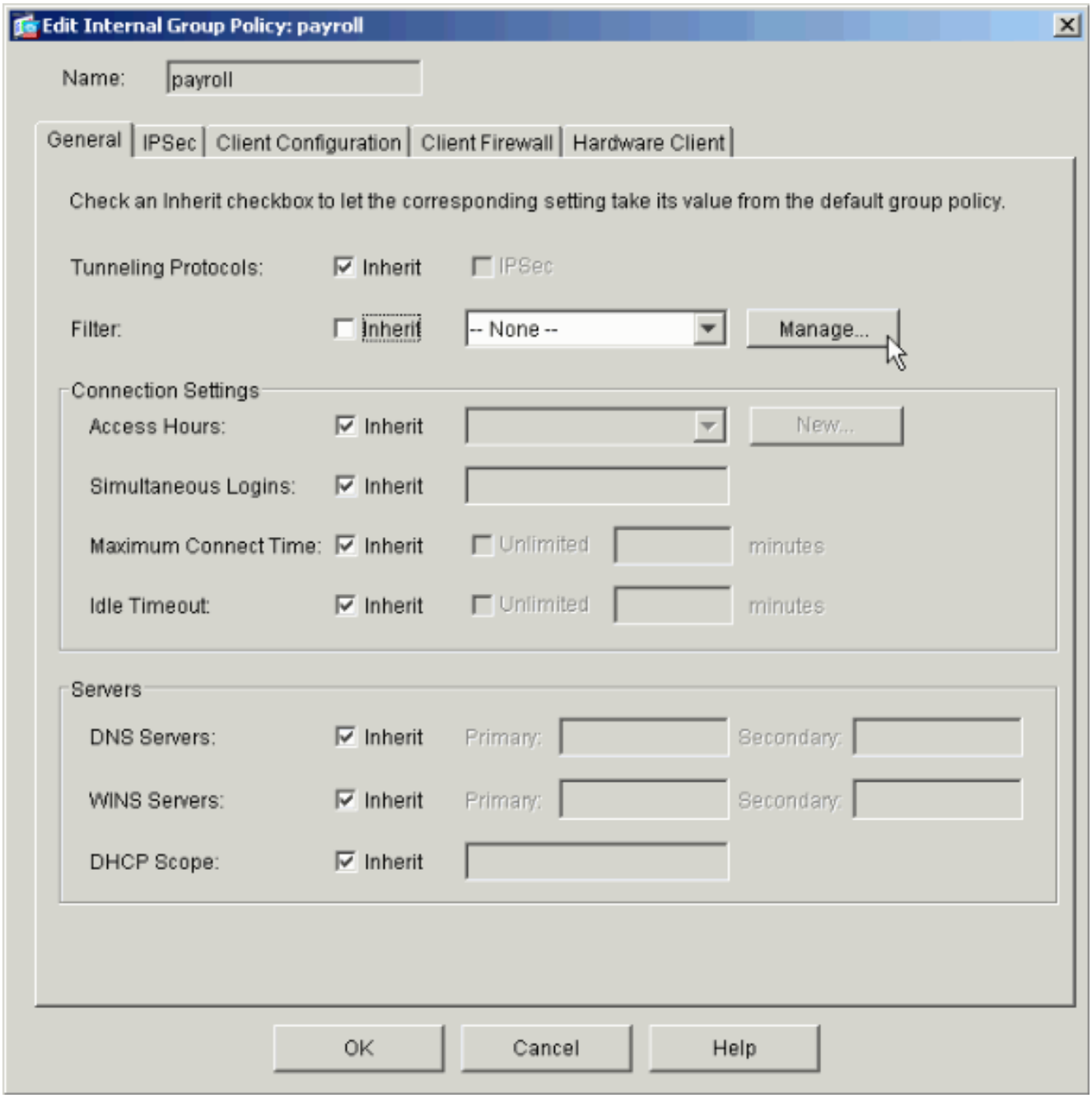
1. Selecteer **Configuration > VPN > General > Group Policy**.



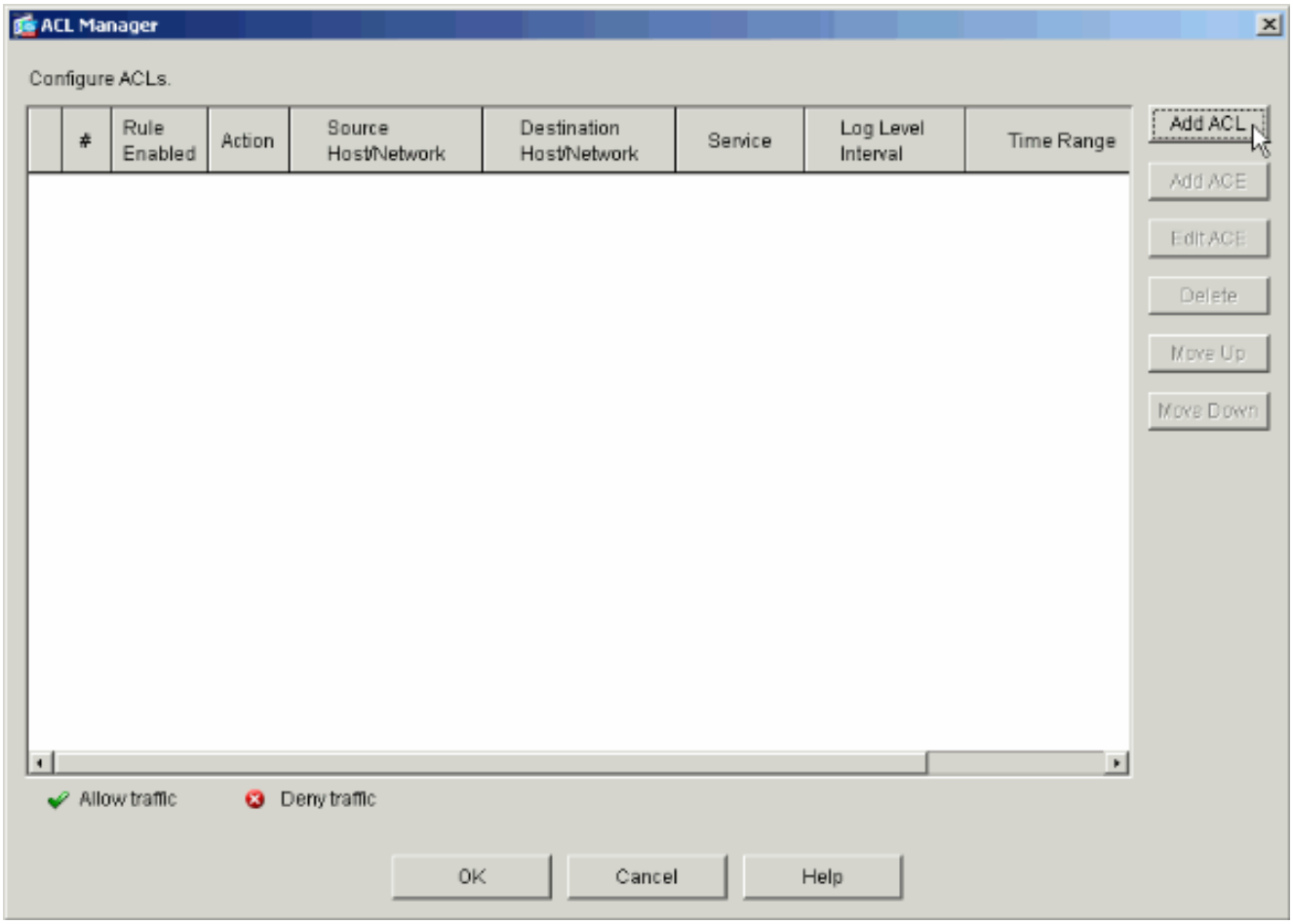
2. Op basis van welke stappen zijn ondernomen om tunnelgroepen op de PIX te configureren bestaat groepsbeleid al voor tunnelgroepen waarvan u de gebruikers wilt beperken. Als er al een geschikt groepsbeleid bestaat, kiest u het programma en klikt u op **Bewerken**. Klik anders op **Toevoegen** en kies **intern groepsbeleid...**.



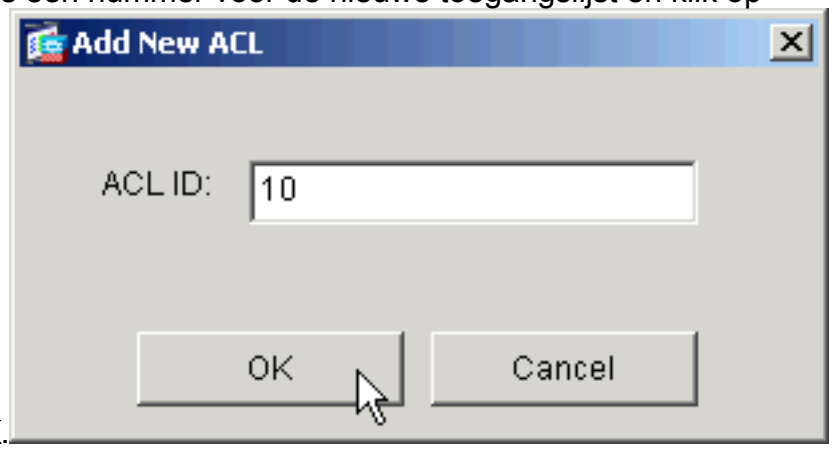
3. Indien nodig voert u de naam van het groepsbeleid in of wijzigt u dit boven in het venster dat nu wordt geopend.
4. Schakel op het tabblad Algemeen het vakje Inherit naast Filter uit en klik vervolgens op **Bewerken**.



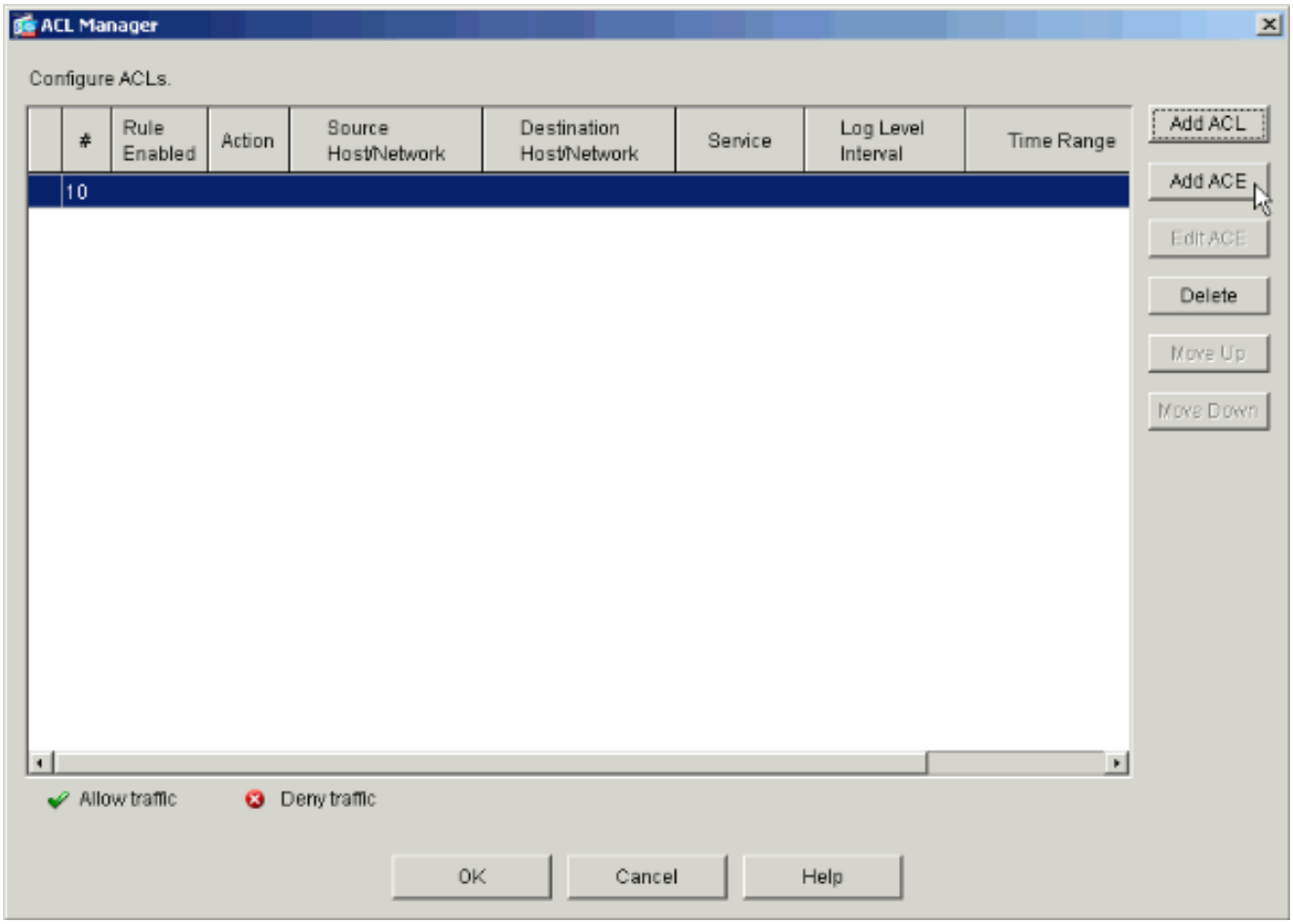
5. Klik op **Add ACL** om een nieuwe toegangslijst in het venster van ACL Manager te maken dat verschijnt.



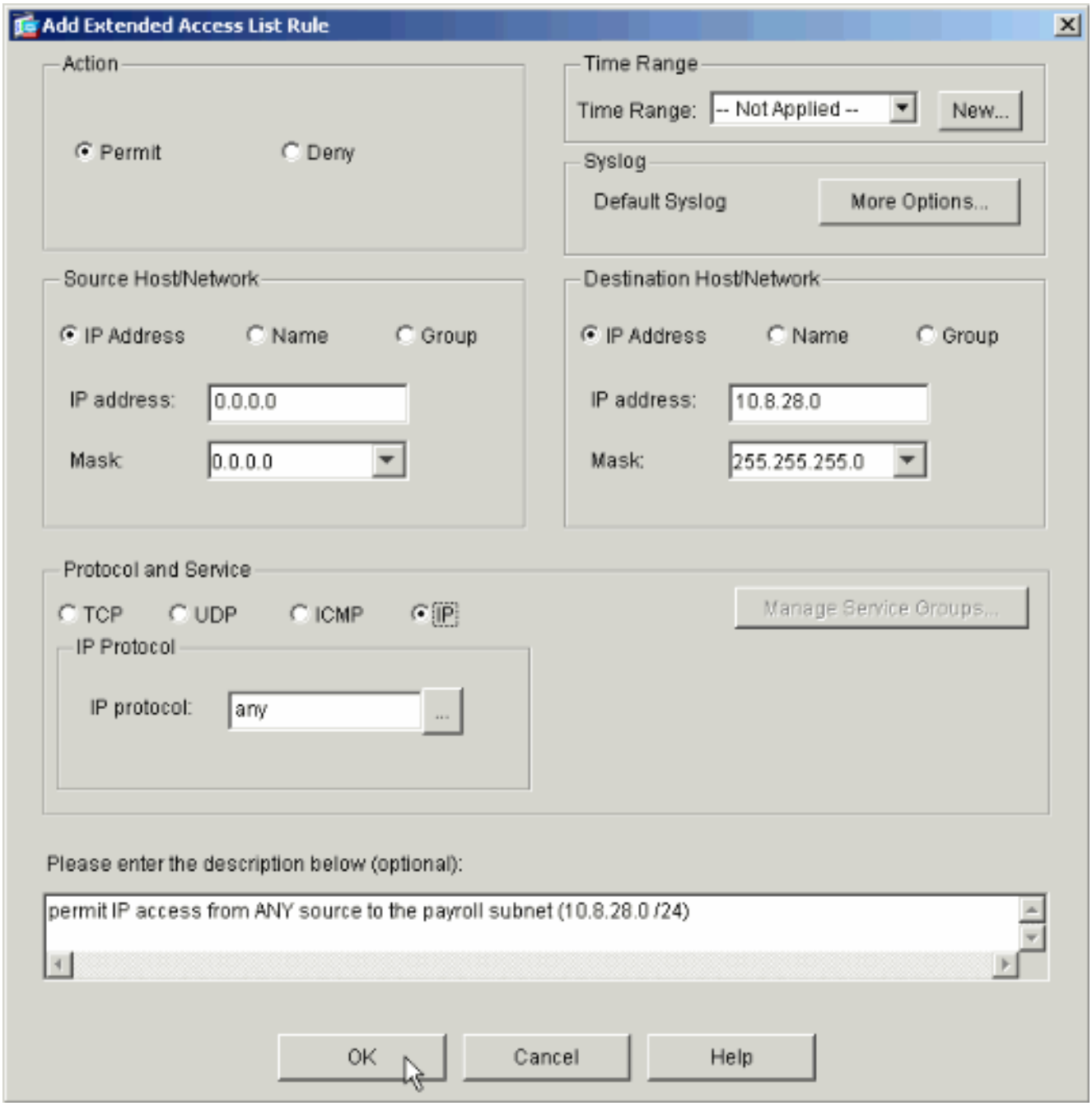
6. Kies een nummer voor de nieuwe toegangslijst en klik op **OK**.



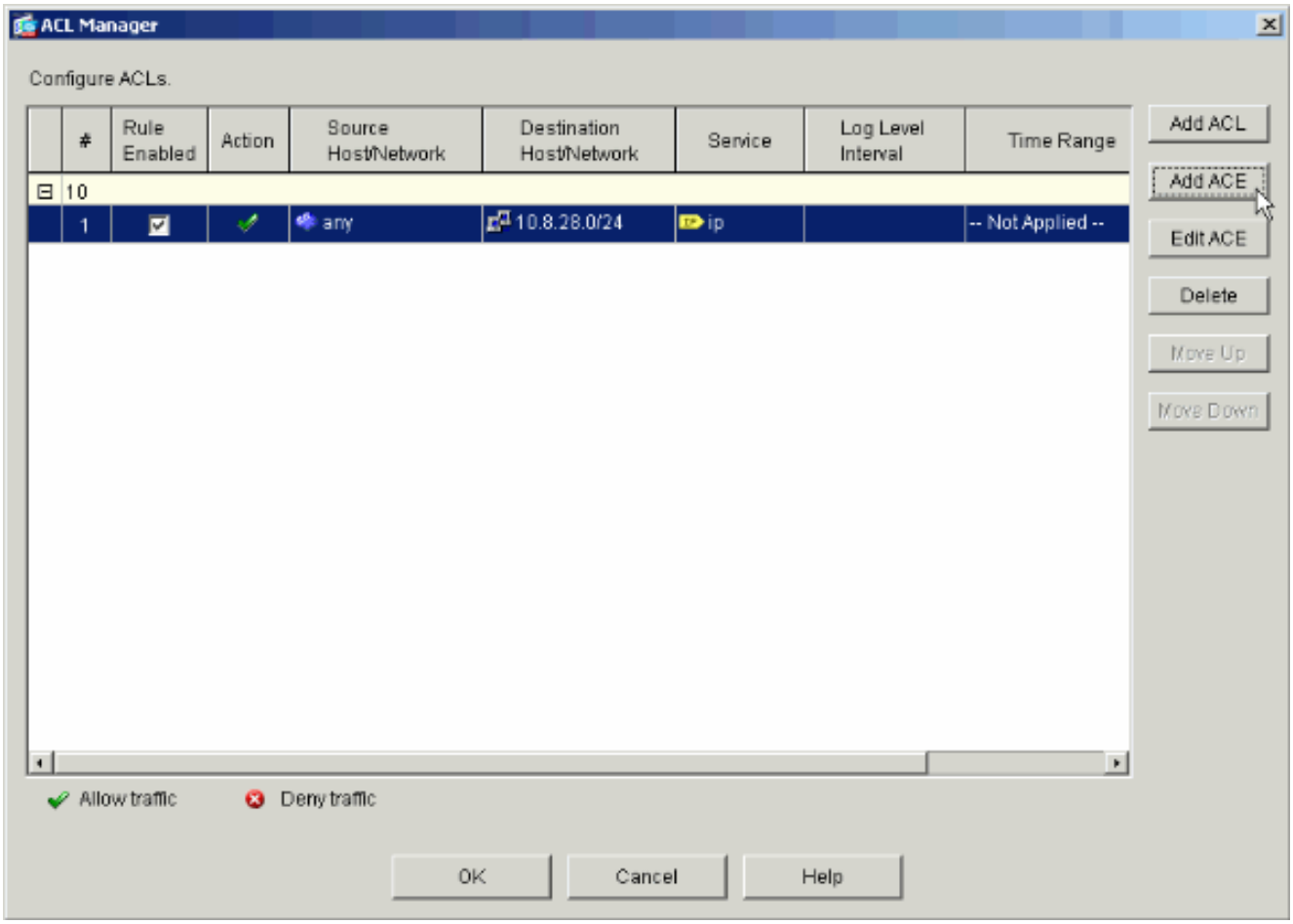
7. Als uw nieuwe ACL links is geselecteerd, klikt u op **ACE toevoegen** om een nieuwe toegangscontrole aan de lijst toe te voegen.



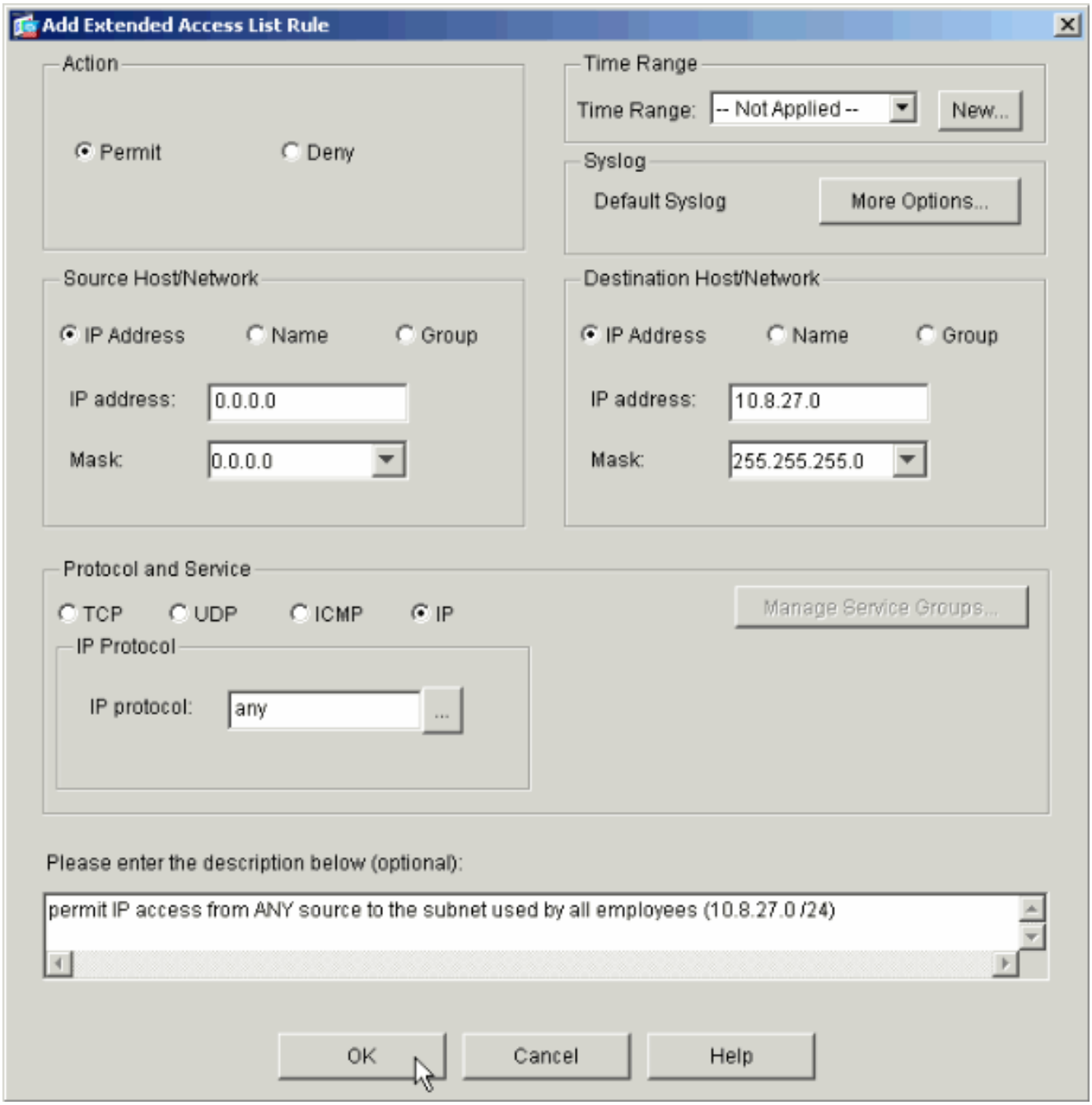
8. Defineer de toegangscontrole ingang (ACE) die u wilt toevoegen.In dit voorbeeld, het eerste ACE in ACL 10 staat IP toegang tot het Subnet van de Loon van elke bron toe.**Opmerking:** standaard selecteert ASDM alleen TCP als protocol. U moet IP kiezen als u gebruikers volledige IP-toegang wilt toestaan of weigeren. Klik op **OK** wanneer u klaar bent.



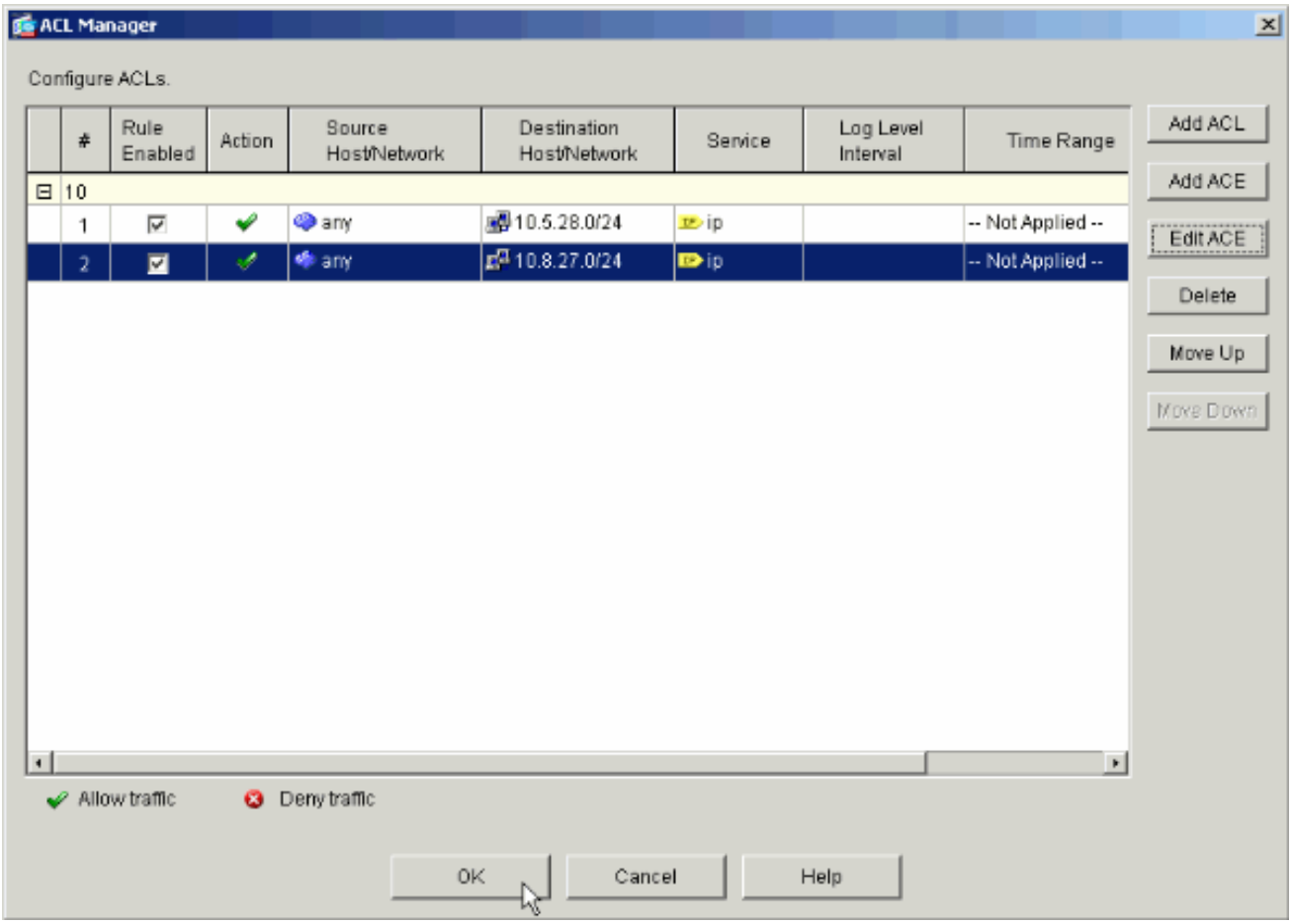
9. Het ACE dat u zojuist hebt toegevoegd, verschijnt nu in de lijst. Kies nogmaals **ACE toevoegen** om extra lijnen aan de toegangslijst toe te voegen.



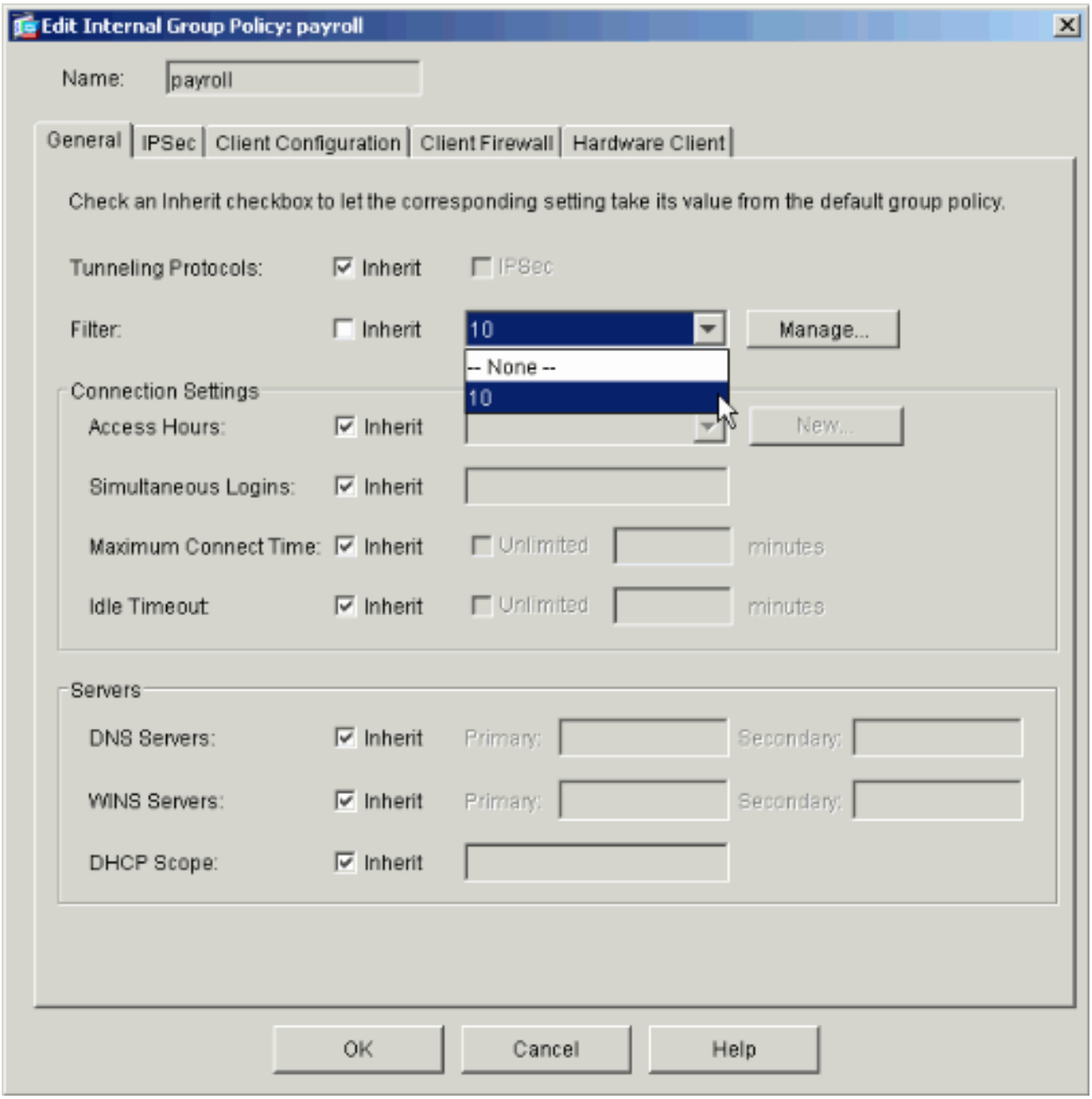
In dit voorbeeld, wordt een tweede ACE aan ACL 10 toegevoegd om toegang tot Intranet toe te
staan.



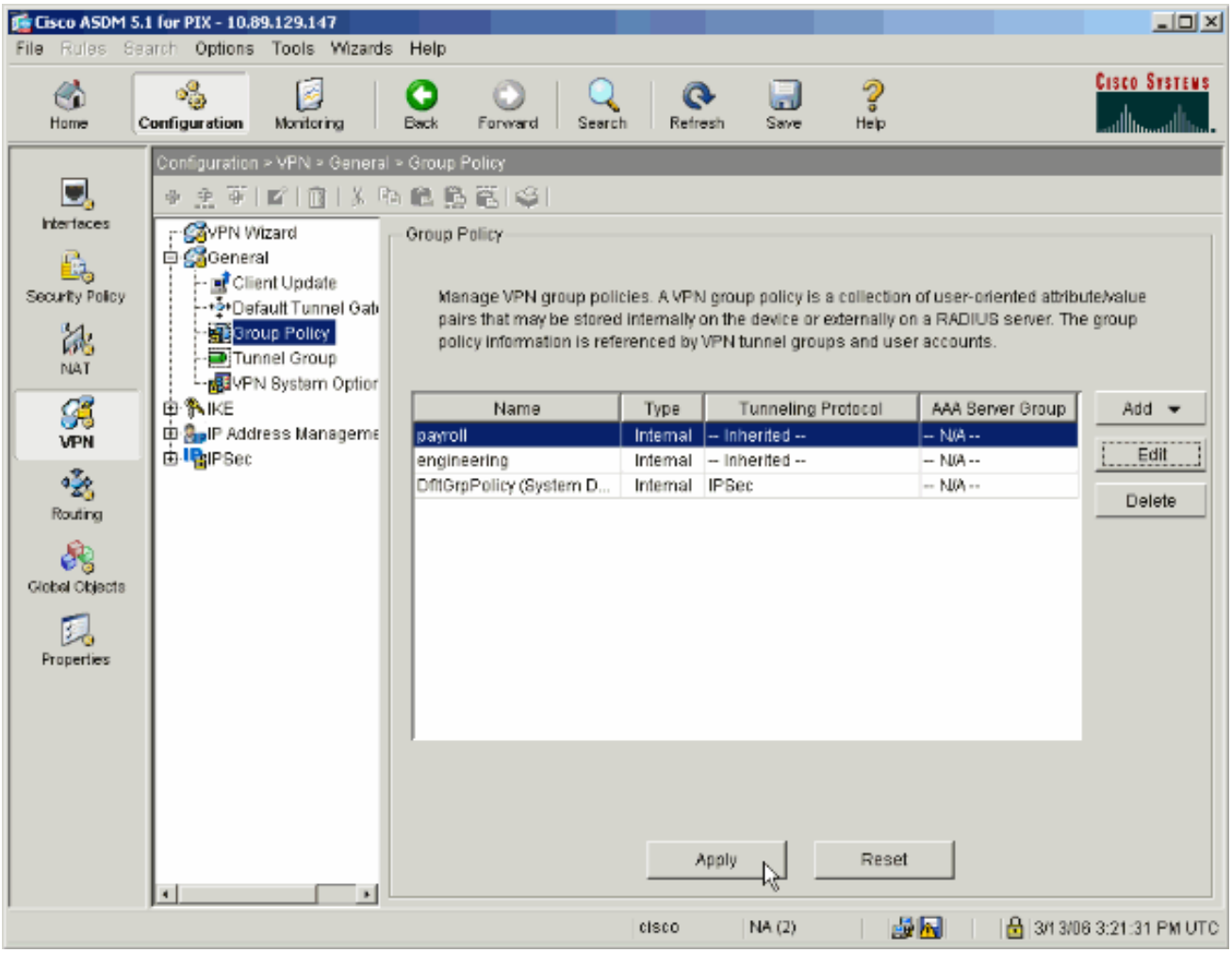
10. Klik op **OK** zodra u klaar bent met het toevoegen van ACE's.



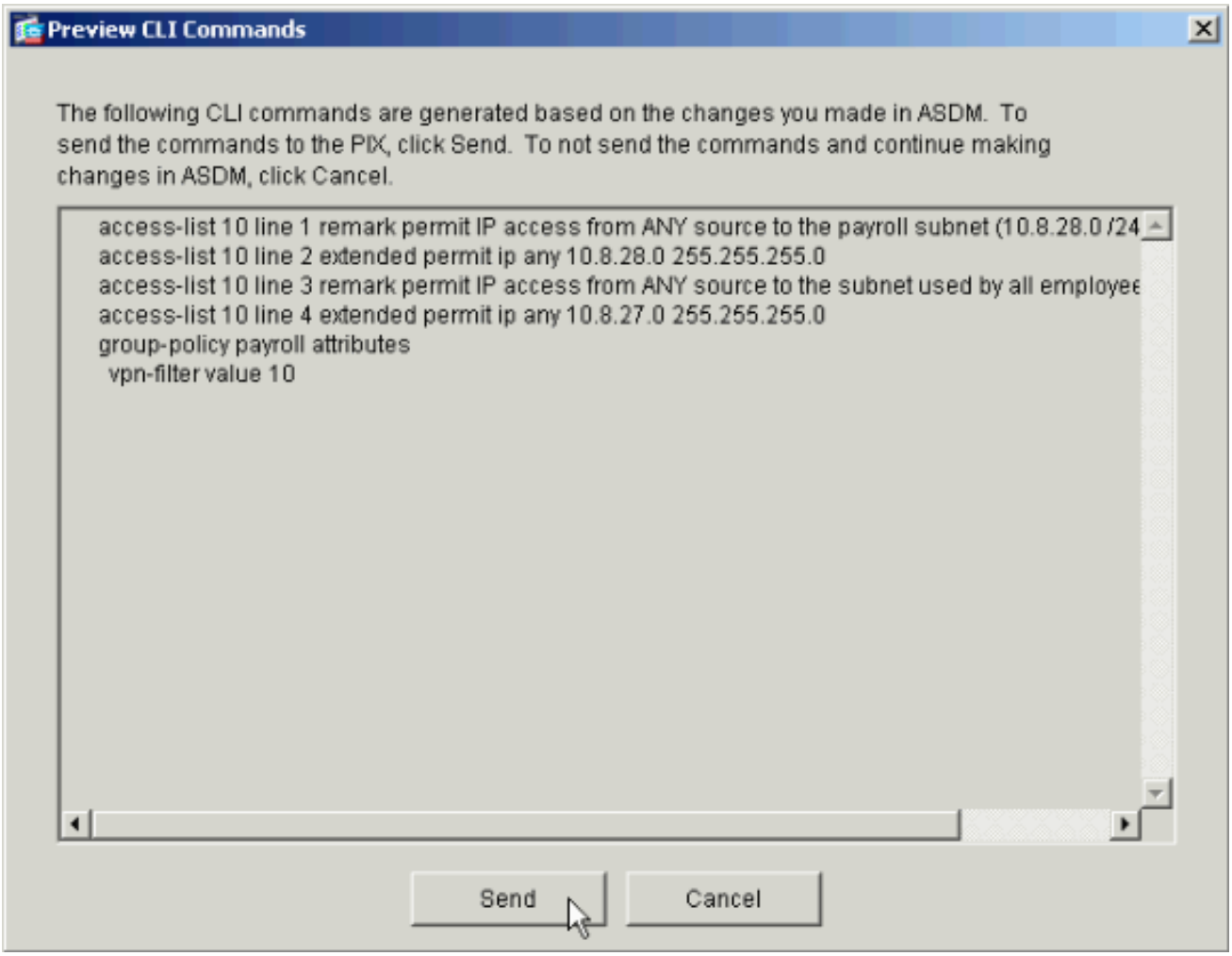
11. Selecteer ACL die u in de laatste stappen hebt gedefinieerd en ingevuld om het filter voor uw groepsbeleid te zijn. Klik op **OK** wanneer u klaar bent.



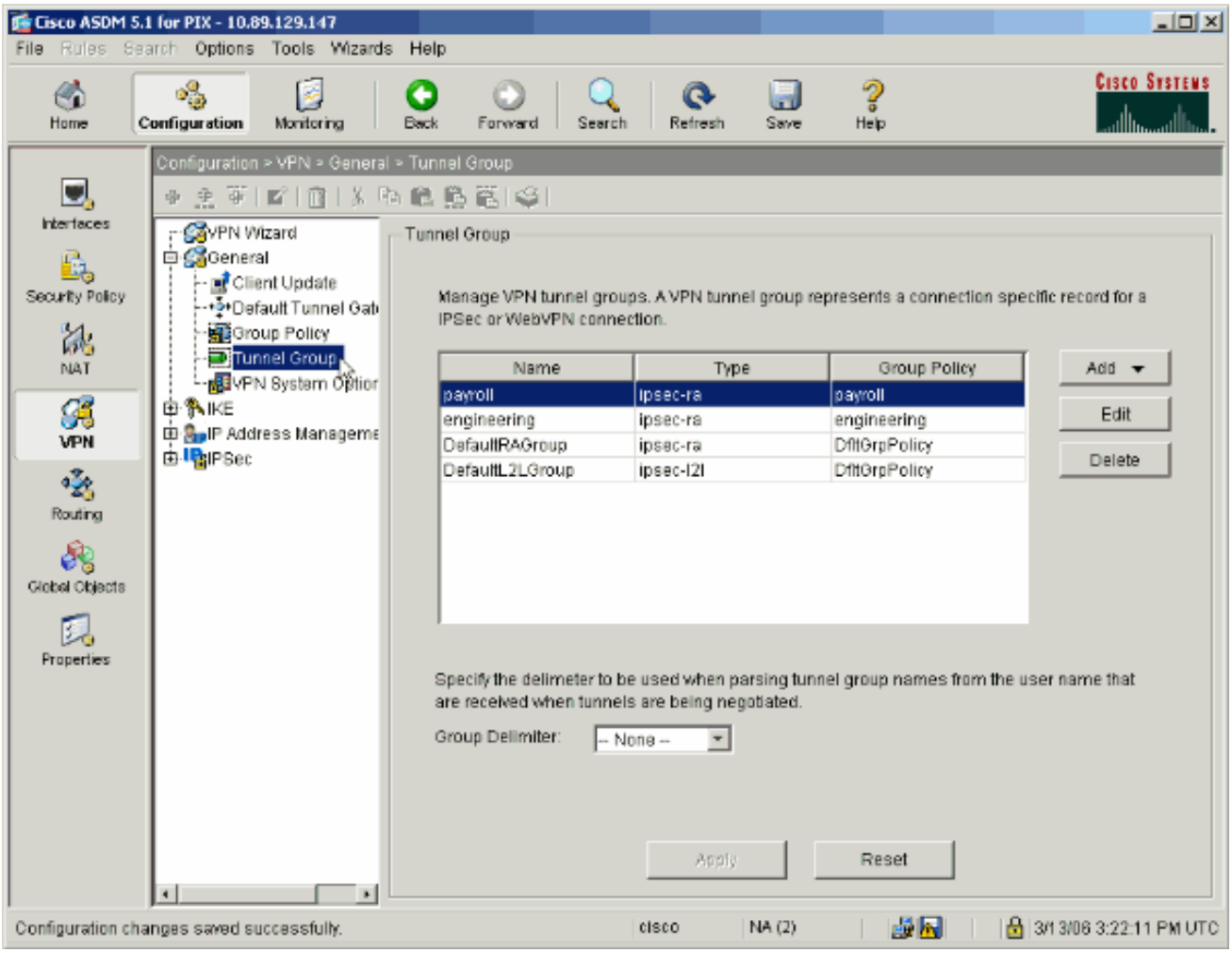
12. Klik op **Toepassen** om de wijzigingen in de PIX te verzenden.



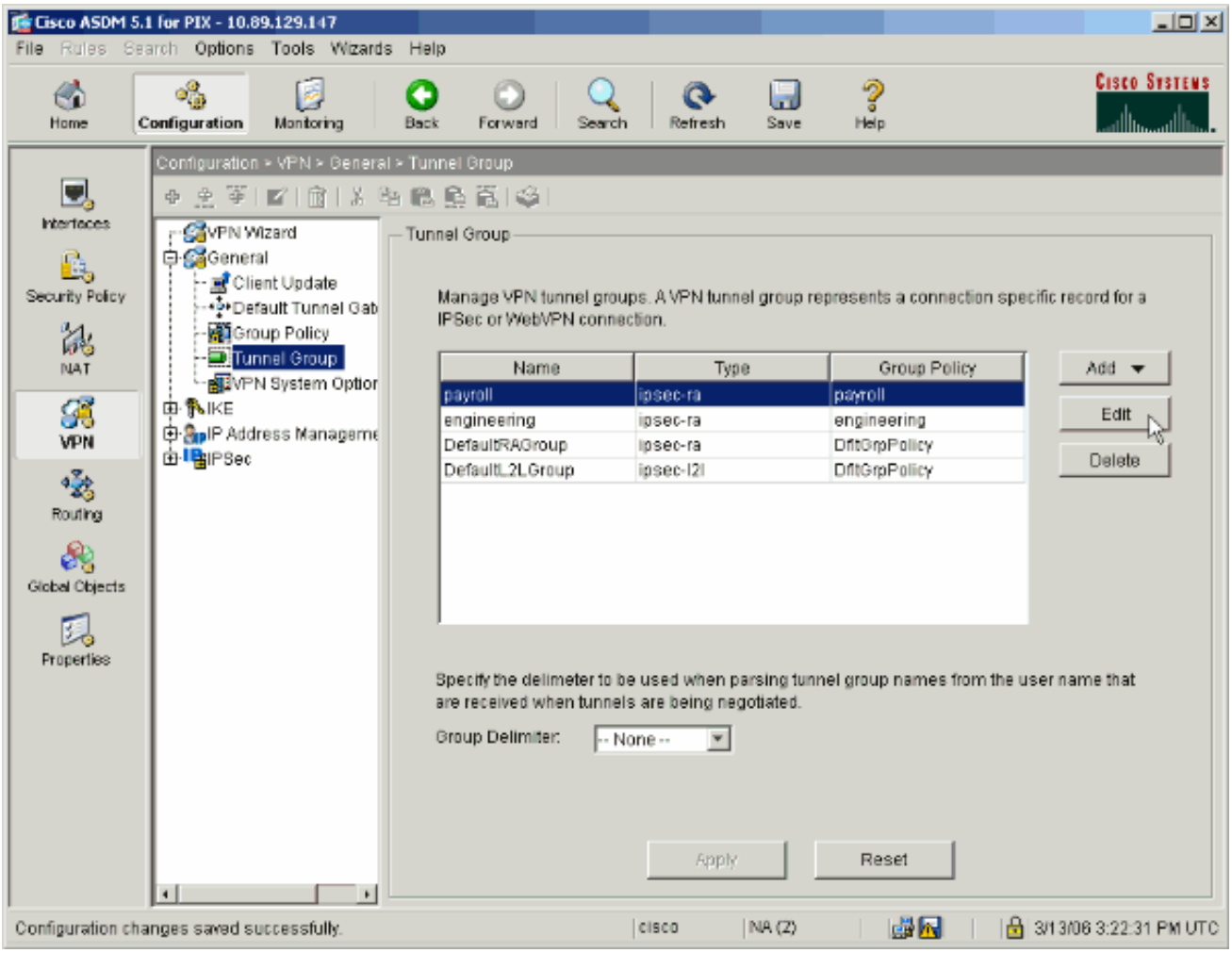
13. Als u dit onder **Opties > Voorkeuren** hebt ingesteld, wordt de opdracht in de ASDM gepresteerd dat deze naar de PIX wordt verzonden. Klik op **Verzenden**.



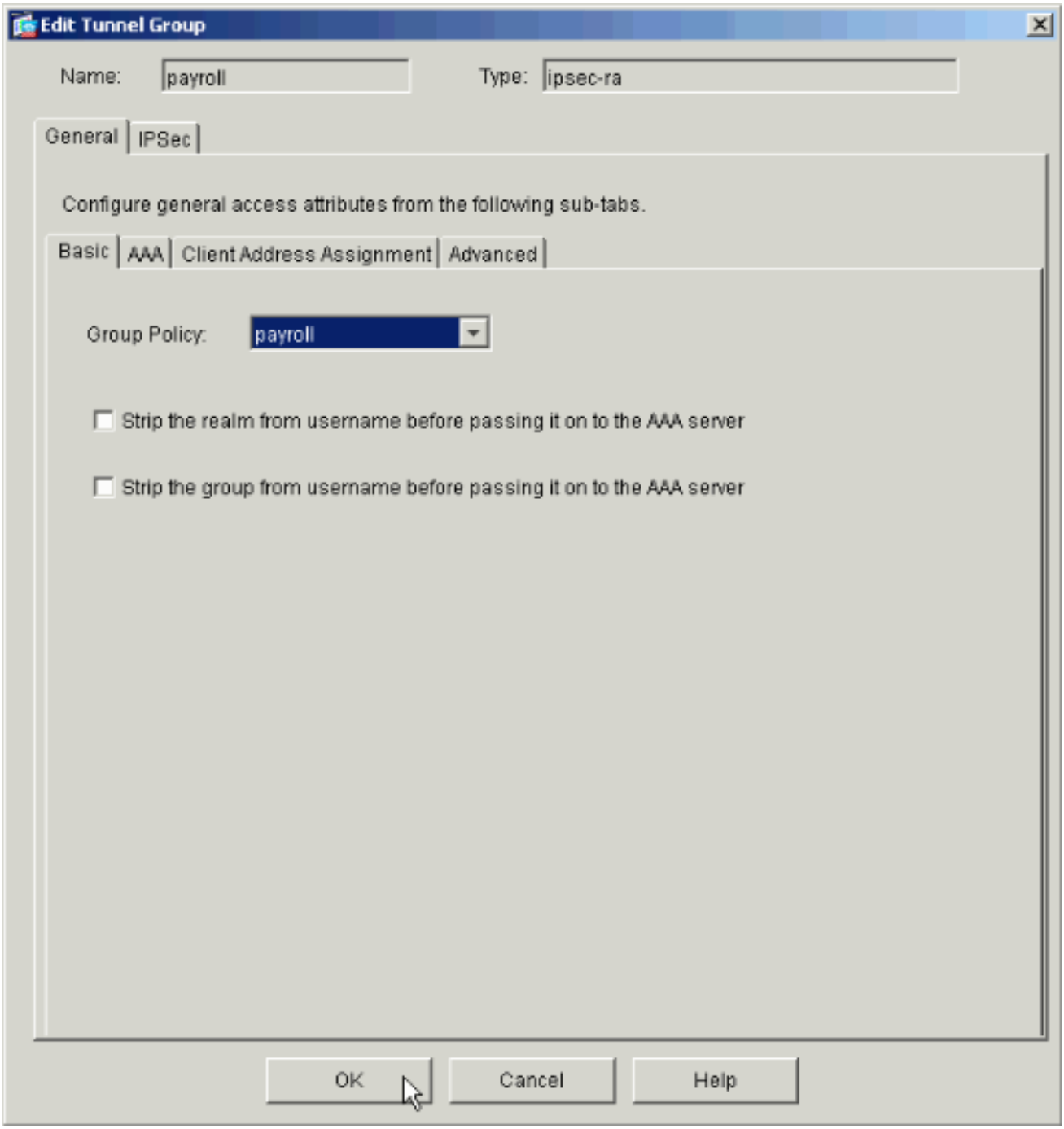
14. Pas het beleid van de Groep toe dat net tot de juiste tunnelgroep werd gemaakt of aangepast. Klik op **Tunnelgroep** in het linker kader.



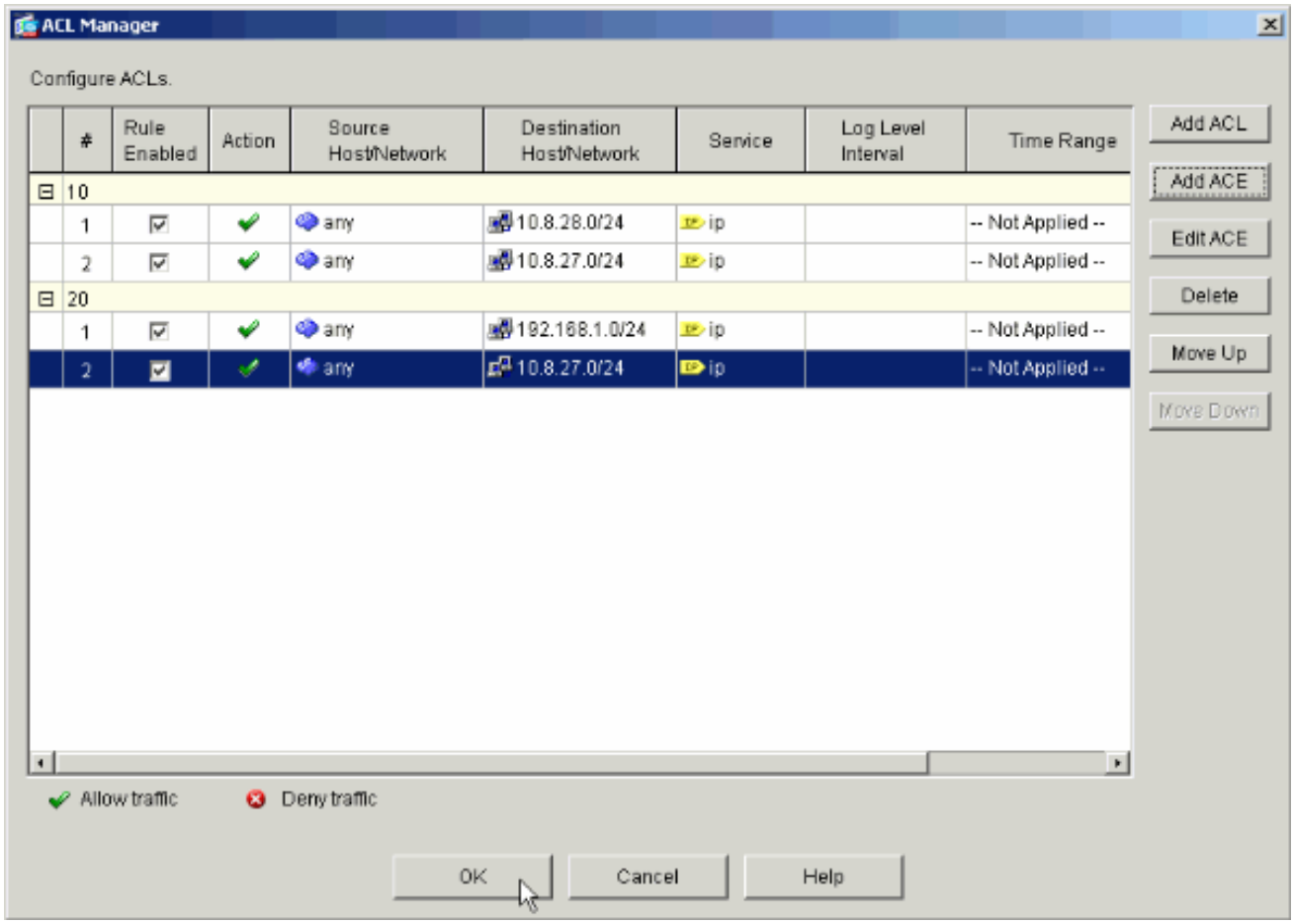
15. Kies de tunnelgroep waarop u het groepsbeleid wilt toepassen en klik op **Bewerken**.



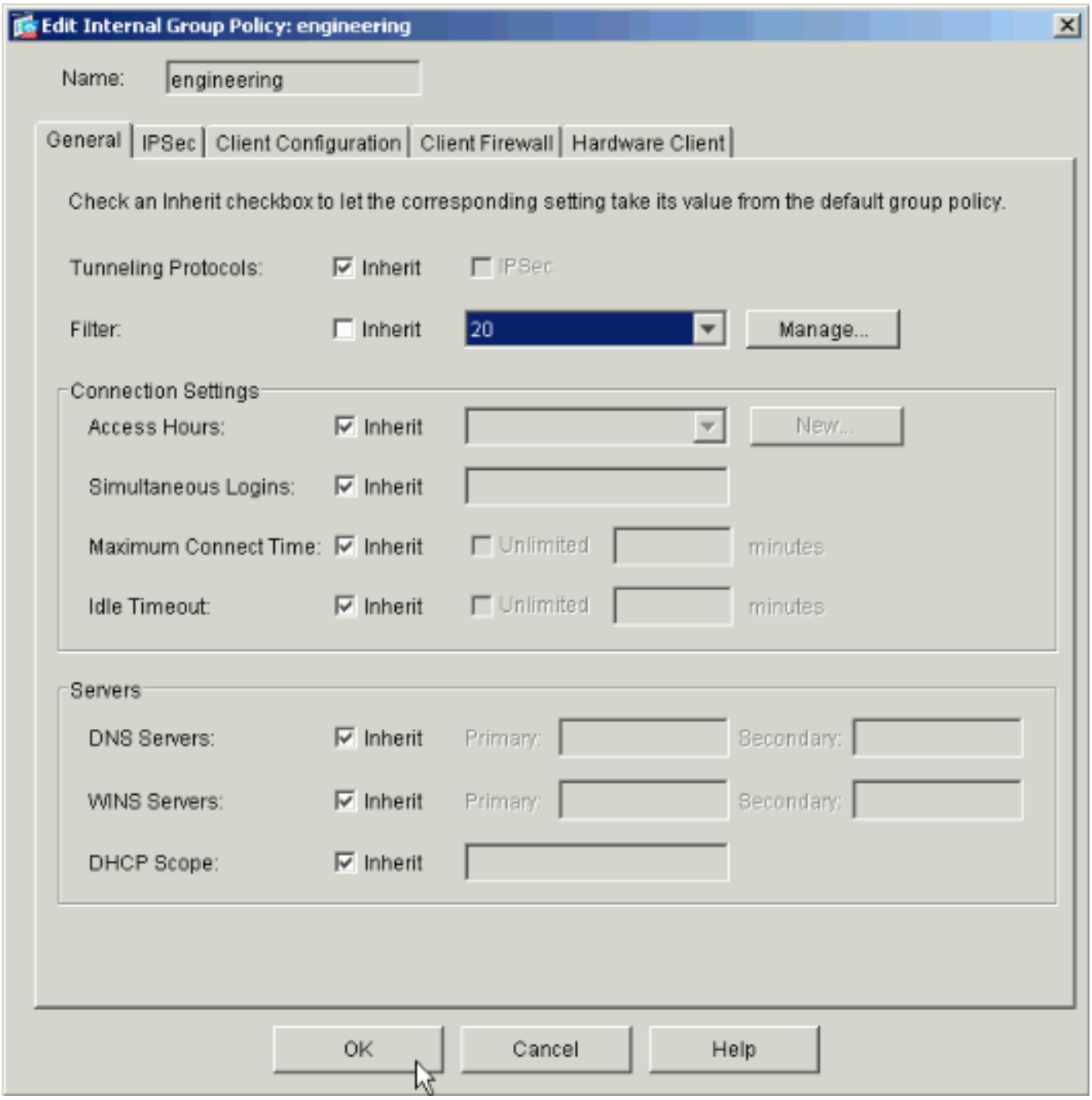
16. Als uw groepsbeleid automatisch is gemaakt (zie stap 2), controleer of het groepsbeleid dat u zojuist hebt ingesteld, in het vervolgkeuzevenster is geselecteerd. Als uw groepsbeleid niet automatisch is ingesteld, selecteert u dit in het uitrolvak. Klik op **OK** wanneer u klaar bent.



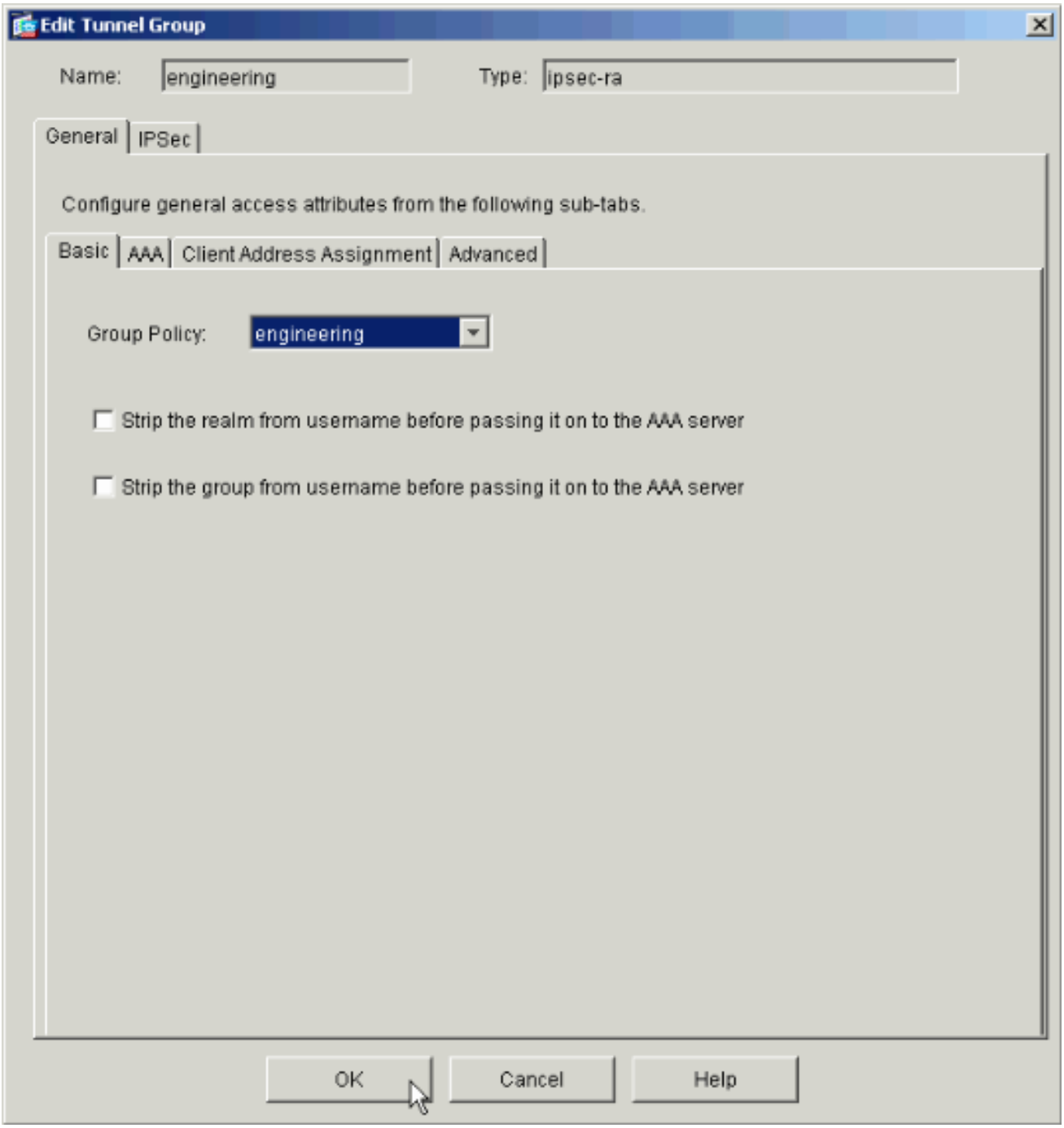
17. Klik op **Toepassen** en klik, indien dit wordt gevraagd, op **Verzend** om de verandering in de PIX-configuratie toe te voegen.Als het groepsbeleid al was geselecteerd, ontvangt u een bericht dat luidt: "Er zijn geen wijzigingen aangebracht". Klik op **OK**.
18. Herhaal stap 2 tot en met 17 voor alle extra tunnelgroepen waaraan u beperkingen wilt toevoegen.In dit configuratievoorbeeld is het ook noodzakelijk de toegang van de ingenieurs te beperken. Hoewel de procedure hetzelfde is, zijn er hier een paar etappes waar grote verschillen bestaan:Nieuwe toegangslijst



Kies **toegangslijst 20** als een filter in het beleid van de technische groep.



Controleer dat het beleid van de Engineering Group voor de Engineering Tunnel Group is ingesteld.



Toegang via CLI configureren

Volg deze stappen om het security apparaat te configureren met behulp van de CLI:

Opmerking: Sommige opdrachten in deze uitvoer worden vanwege ruimtelijke redenen naar een tweede regel teruggebracht.

1. Maak twee verschillende toegangscontrolelijsten (15 en 20) die op gebruikers worden toegepast terwijl ze verbinding maken met de externe VPN-toegang. Deze toegangslijst wordt later in de configuratie ingeschakeld.

```
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. Maak twee verschillende VPN-adrespools. Maak er een voor Payroll en één voor de technische externe gebruikers.

```
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. Creëer beleid voor loonlijst dat alleen op hen van toepassing is wanneer ze zich verbinden.

```
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. Deze stap is hetzelfde als stap 3, behalve voor de technische groep.

```
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. Maak lokale gebruikers en wijs de eigenschappen toe die u net aan die gebruikers hebt

gemaakt om hun toegang tot middelen te beperken.

```
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. Maak tunnelgroepen die verbindingsbeleid bevatten voor de gebruikers van de loonlijst.

```
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. Maak tunnelgroepen die verbindingsbeleid bevatten voor de gebruikers van de Engineering.

```
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
```

Nadat u de configuratie hebt ingevoerd, kunt u dit gemarkeerde gebied in uw configuratie zien:

Apparaatnaam 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
```

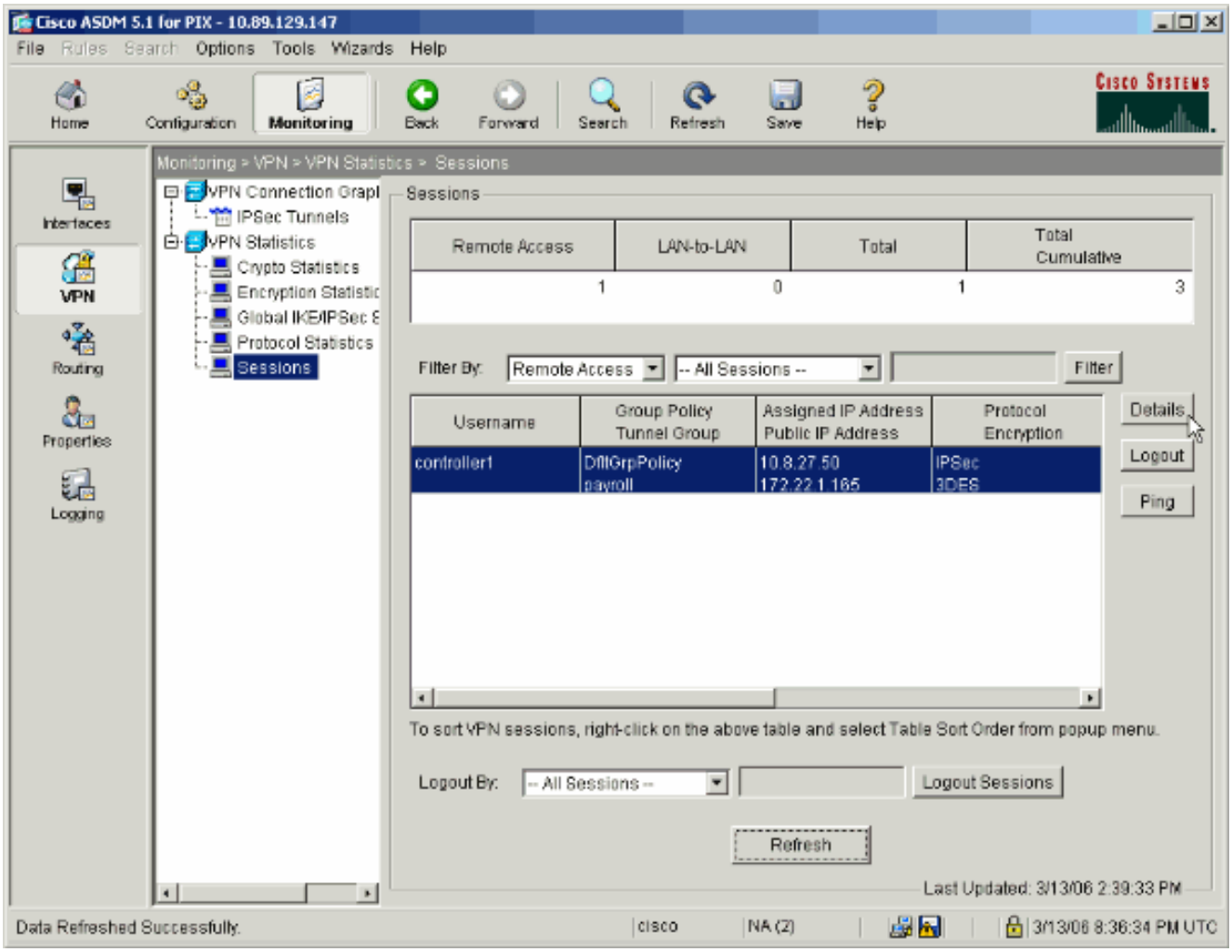
```
nat (Inside) 1 192.168.1.0 255.255.255.0
nat (Inside) 1 10.8.27.0 255.255.255.0
nat (Inside) 1 10.8.28.0 255.255.255.0
route Intranet 0.0.0.0 0.0.0.0 10.8.27.2
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 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)#
```

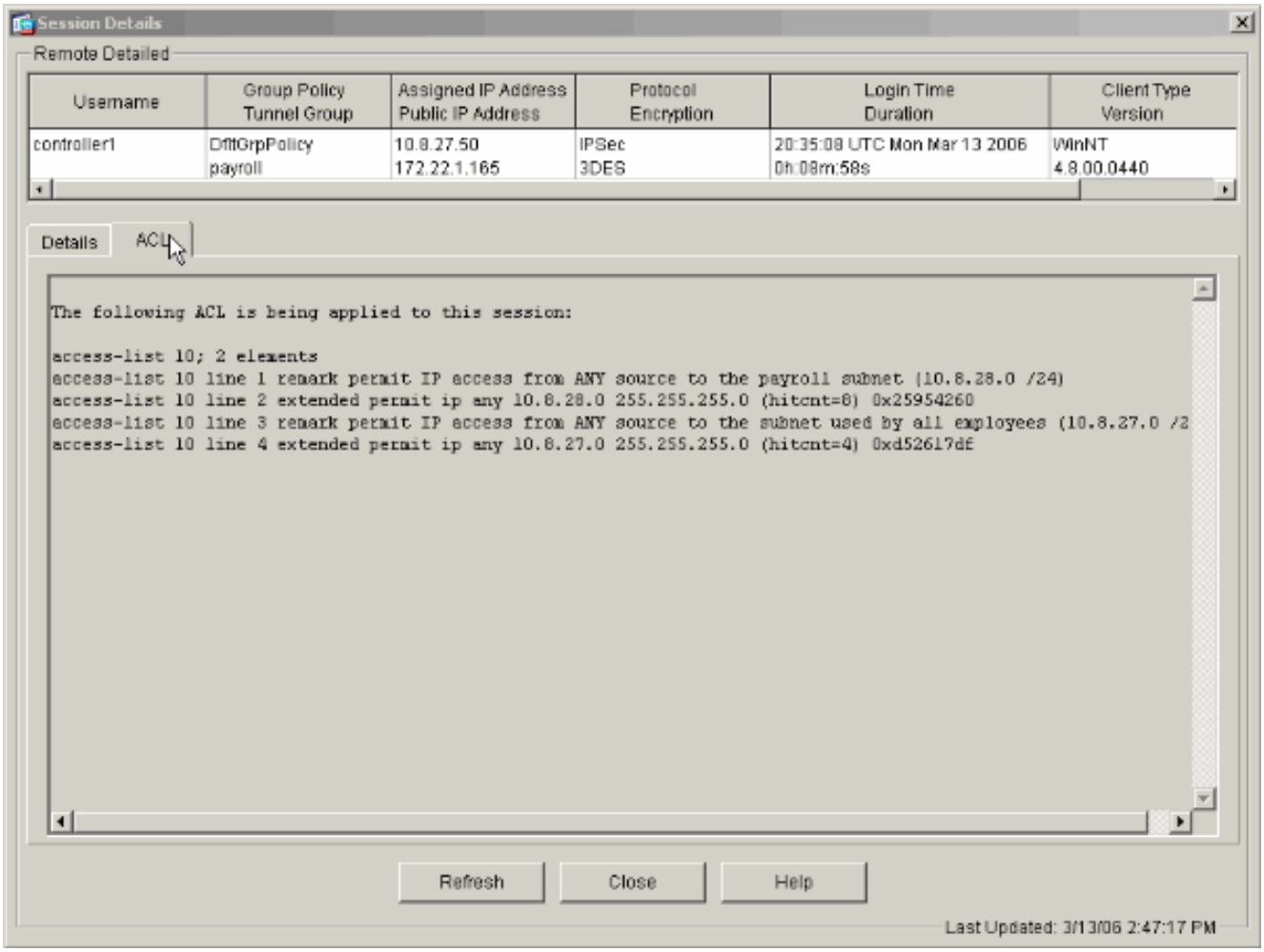
Verifiëren

Gebruik de bewakingsfuncties van ASDM om uw configuratie te controleren:

1. Selecteer **Monitoring > VPN > VPN Statistieken > Sessies**.U ziet de actieve VPN sessies op de PIX. Selecteer de sessie waarin u geïnteresseerd bent en klik op **Details**.



2. Selecteer het tabblad ACL.De ACL-signalering `geeft` verkeer weer dat door de tunnel stroomt van de client naar het (de) toegestane netwerk(en).



Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Cisco ASA 5500 Series adaptieve security applicaties ASA als externe VPN-server met ASDM-configuratievoorbeeld
- Cisco PIX 500 Series security applicaties en configuratie voorbeelden van TechNotes
- Cisco ASA 5500 Series adaptieve security applicaties en configuratie voorbeelden van TechNotes
- Cisco VPN-clientconfiguratie - voorbeelden en TechNotes
- Technische ondersteuning en documentatie – Cisco Systems