PIX/ASA 7.x ASDM: Limita l'accesso alla rete degli utenti VPN di Accesso remoto

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio con Cisco Adaptive Security Device Manager (ASDM) per limitare le reti interne a cui gli utenti VPN ad accesso remoto possono accedere dietro PIX Security Appliance o Adaptive Security Appliance (ASA). È possibile limitare gli utenti VPN ad accesso remoto solo alle aree della rete a cui si desidera che accedano quando:

1. Creare elenchi degli accessi.
2. Associarli ai criteri di gruppo.
3. Associare i criteri di gruppo ai gruppi di tunnel.

Per ulteriori informazioni sullo scenario in cui VPN Concentrator blocca l'accesso degli utenti VPN, consultare il documento sulla configurazione di Cisco VPN 3000 Concentrator per il blocco con filtri e l'assegnazione di filtri RADIUS.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Il PIX può essere configurato usando l'ASDM.**Nota:** per consentire la configurazione del PIX da parte di ASDM, consultare il documento sulla concessione dell'accesso HTTPS per ASDM.
- Èdisponibile almeno una configurazione VPN di accesso remoto valida.**Nota:** Se non si

dispone di una configurazione di questo tipo, fare riferimento all'ASA come server VPN remoto usando l'esempio di configurazione ASDM per informazioni su come configurare una VPN di accesso remoto valida.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure PIX serie 500 Security Appliance versione 7.1(1)**Nota:** Le appliance di sicurezza PIX 501 e 506E non supportano la versione 7.x.
- Cisco Adaptive Security Device Manager versione 5.1(1)**Nota:** ASDM è disponibile solo in PIX o ASA 7.x.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

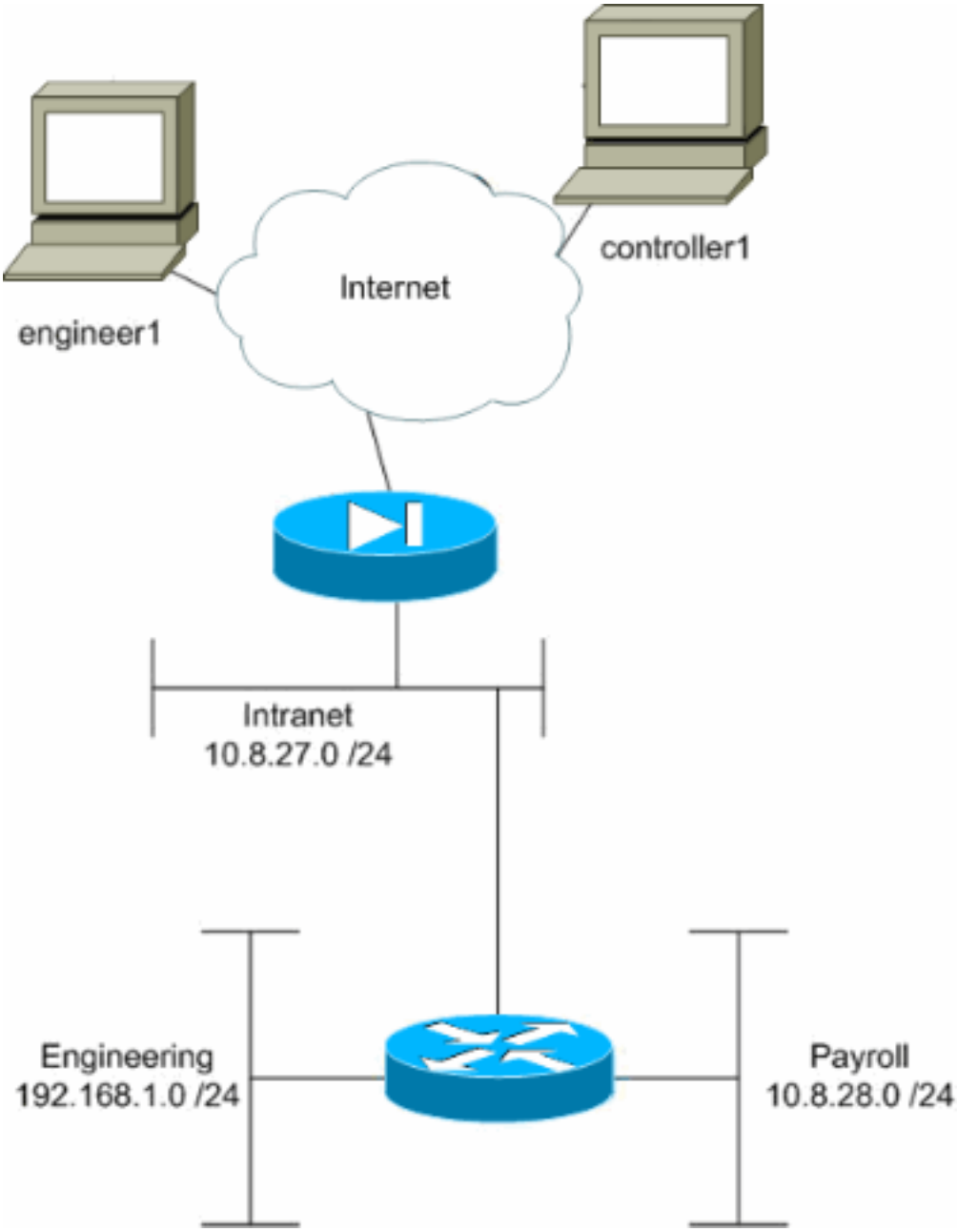
Prodotti correlati

Questa configurazione può essere utilizzata anche con le seguenti versioni hardware e software:

- Cisco ASA serie 5500 Adaptive Security Appliance versione 7.1(1)

Esempio di rete

Nel documento viene usata questa impostazione di rete:



In questo esempio di configurazione, è prevista una piccola rete aziendale con tre subnet. Il diagramma mostra la topologia. Le tre subnet sono Intranet, Engineering e Payroll. L'obiettivo di questo esempio di configurazione è consentire al personale del ciclo paghe l'accesso remoto alle subnet Intranet e Ciclo paghe e impedire l'accesso alla subnet Engineering. Inoltre, i tecnici devono essere in grado di accedere in remoto alle subnet Intranet e Engineering, ma non alla subnet Payroll. L'utente del ciclo paghe in questo esempio è "controller1". L'utente che utilizza questo esempio è "engineer1".

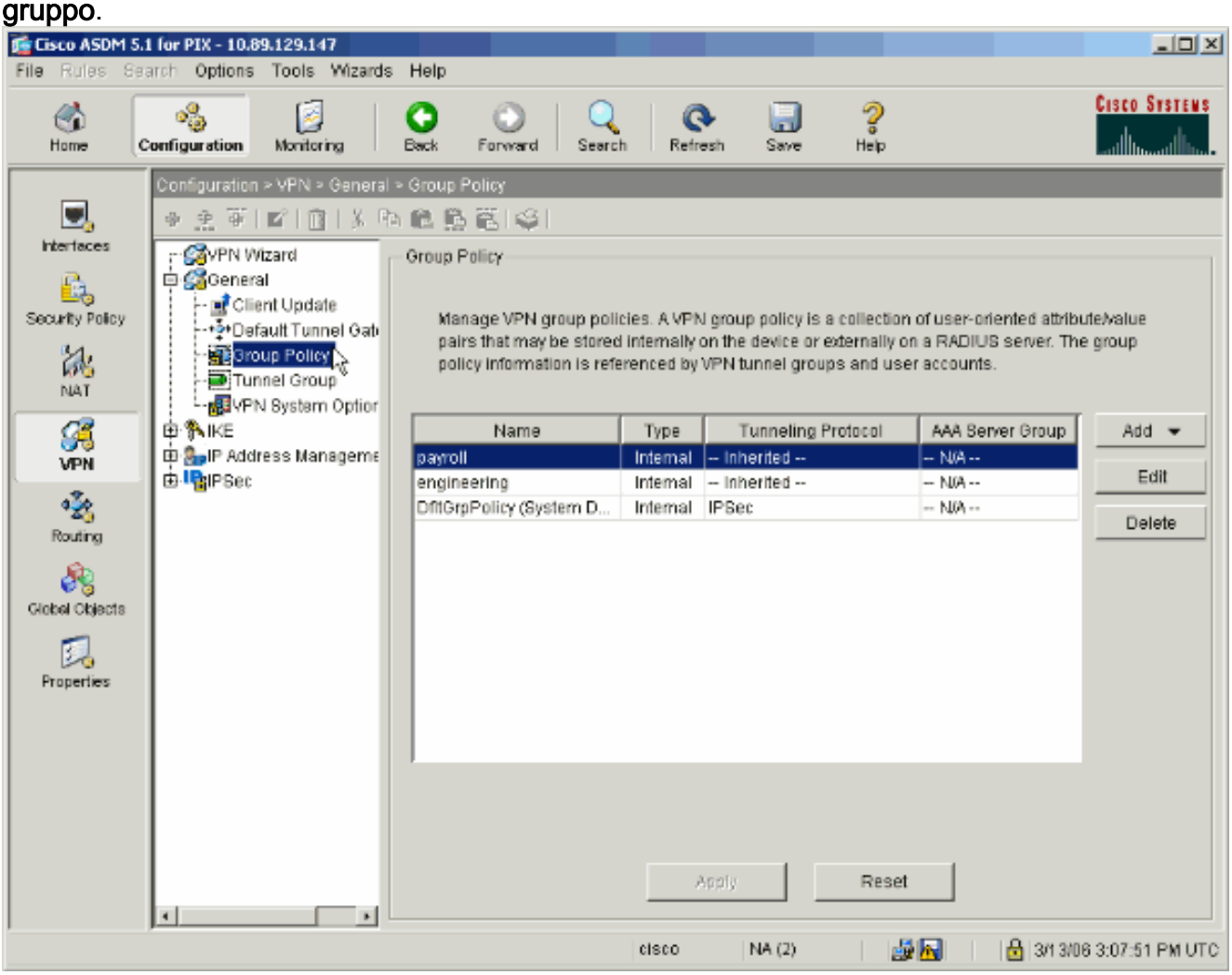
Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

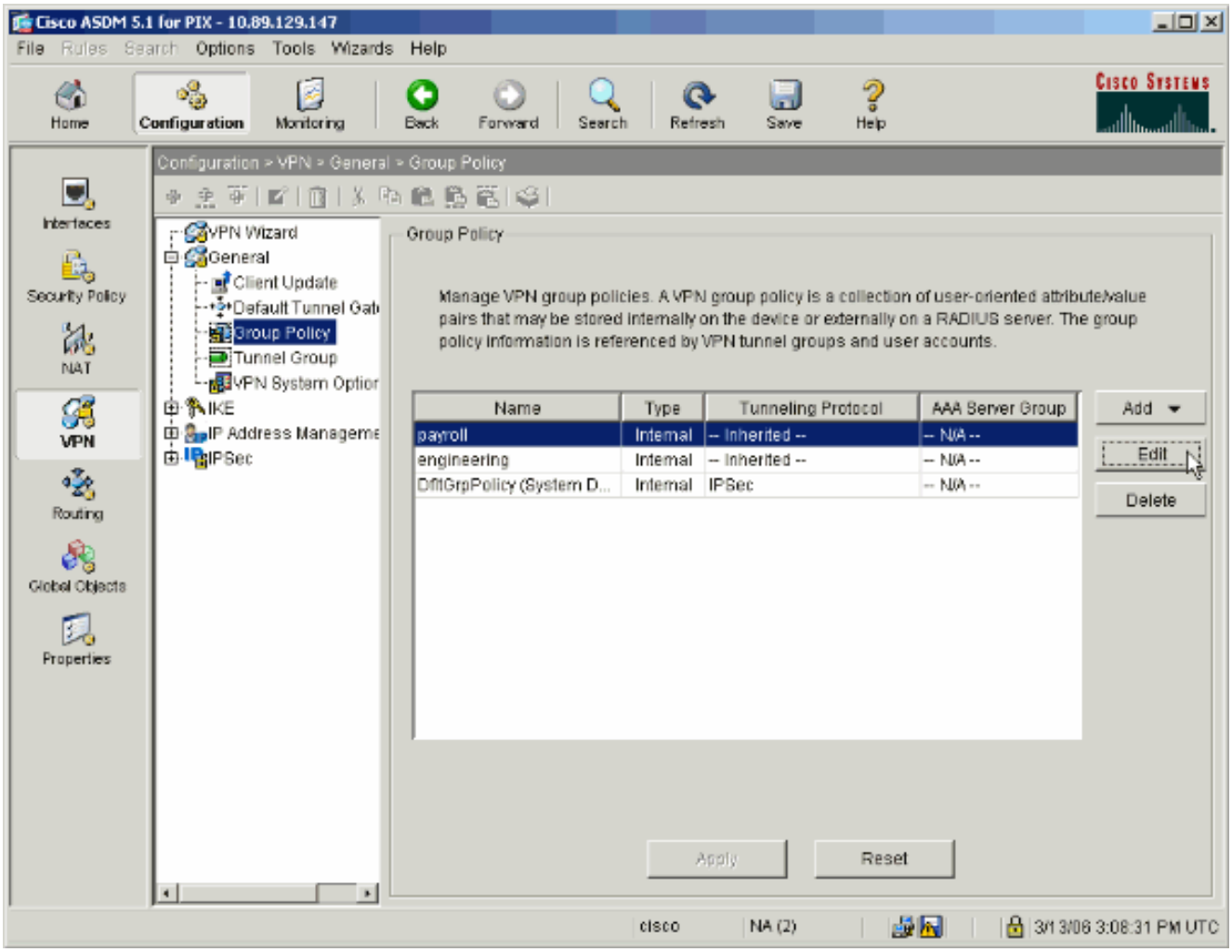
Configurazione dell'accesso tramite ASDM

Completare la procedura seguente per configurare l'appliance di sicurezza PIX utilizzando ASDM:

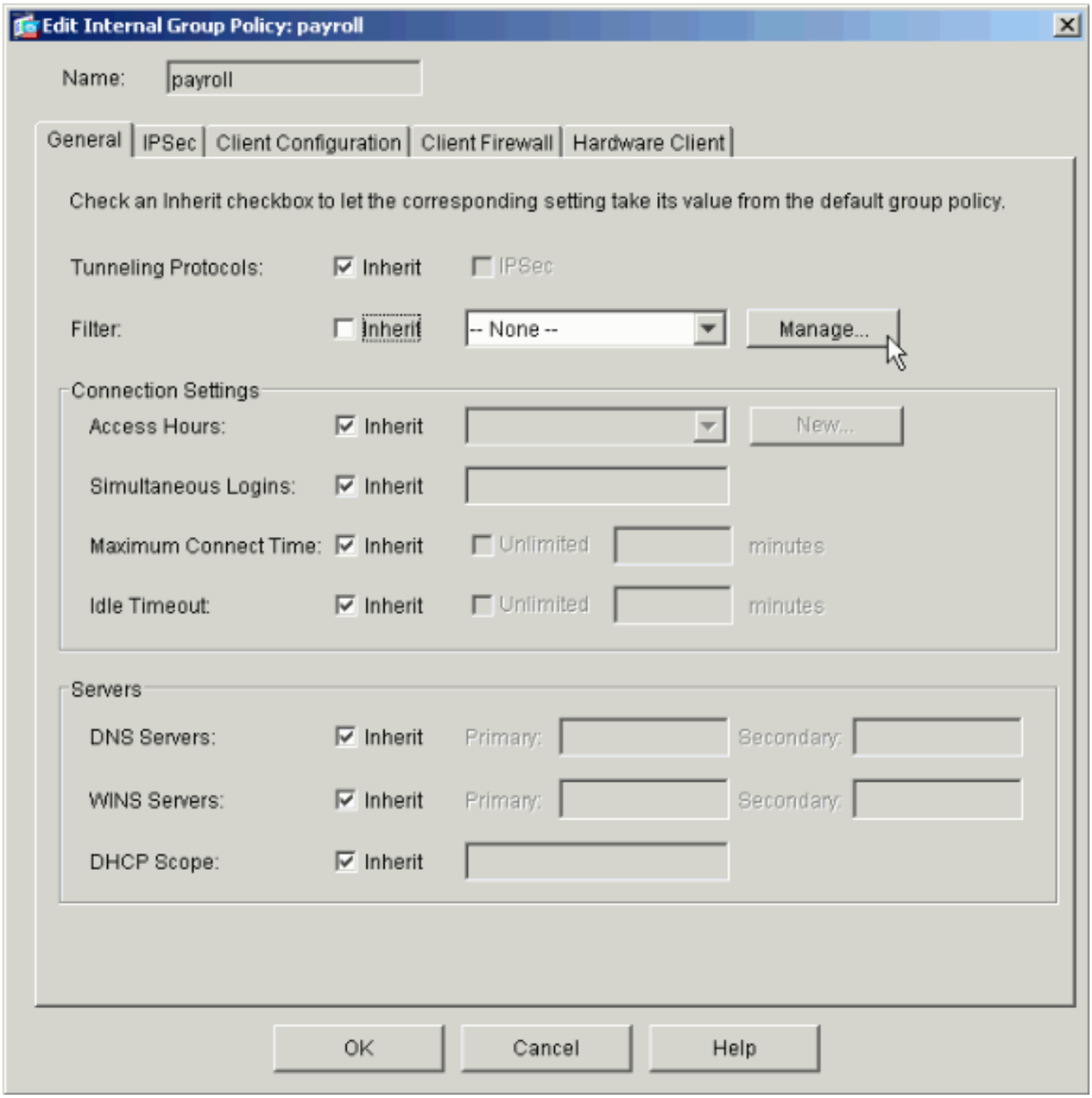
1. Selezionare **Configurazione > VPN > Generale > Criteri di gruppo**.



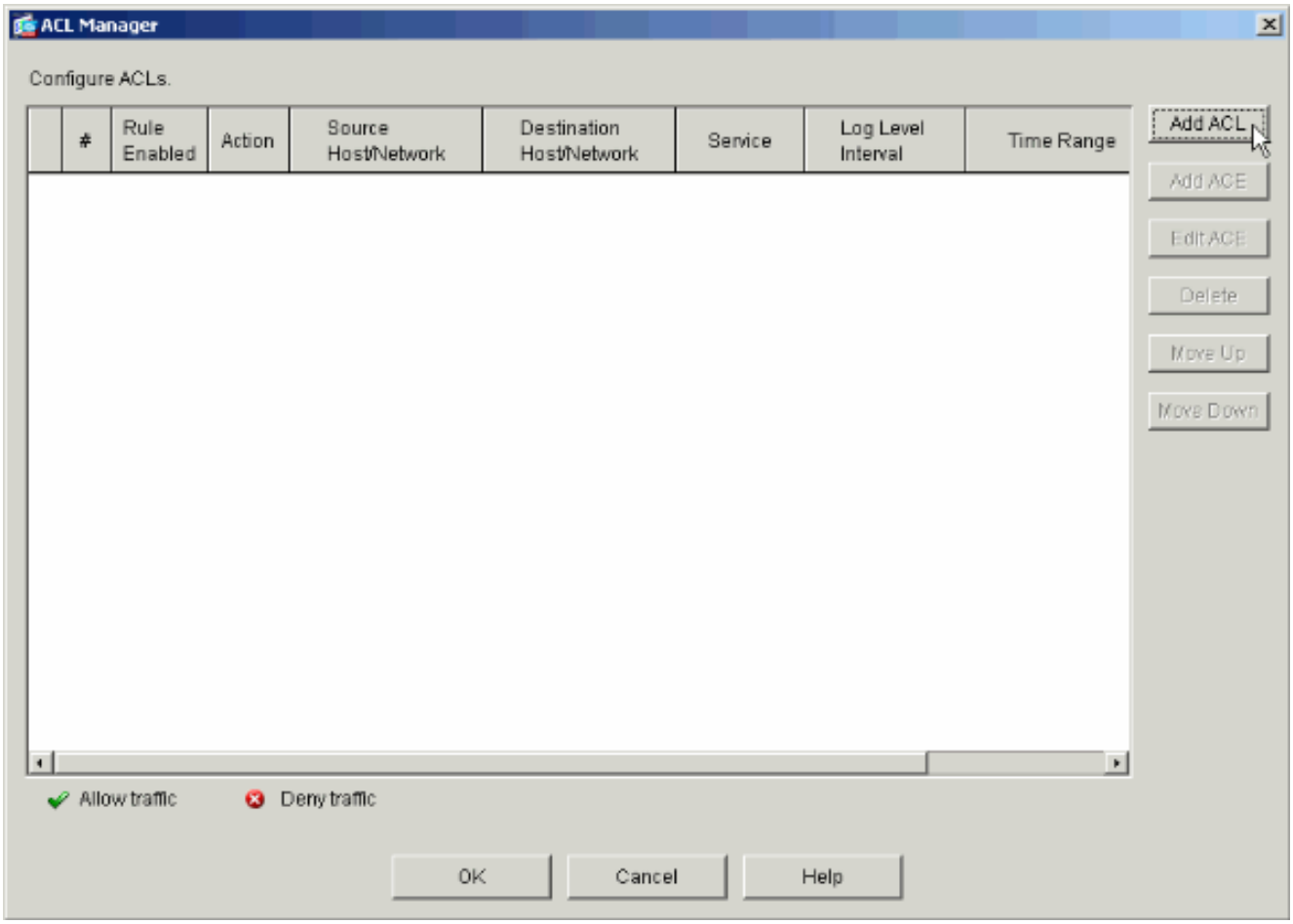
2. In base alla procedura eseguita per configurare i gruppi di tunnel sul PIX, è possibile che esistano già Criteri di gruppo per i gruppi di tunnel di cui si desidera limitare gli utenti. Se esiste già un criterio di gruppo appropriato, selezionarlo e fare clic su **Modifica**. In caso contrario, fare clic su **Aggiungi** e scegliere **Criteri di gruppo interni...**.



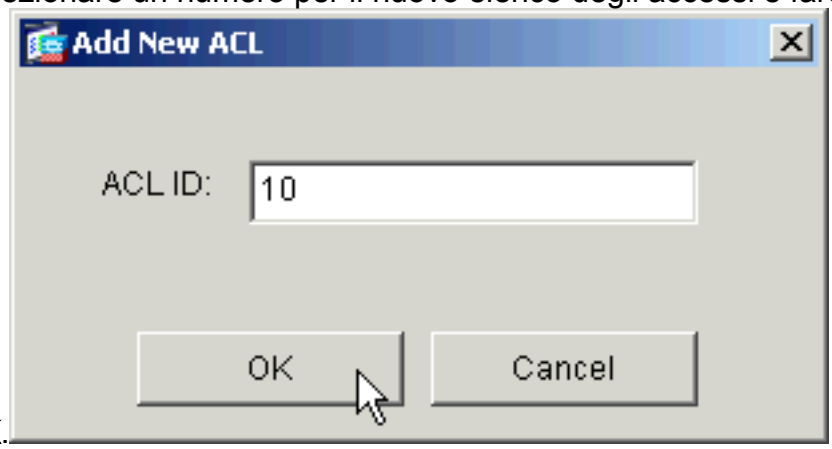
3. Se necessario, immettere o modificare il nome dei Criteri di gruppo nella parte superiore della finestra visualizzata.
4. Nella scheda Generale deselezionare la casella **Eredita** accanto a Filtro e quindi fare clic su **Gestisci**.



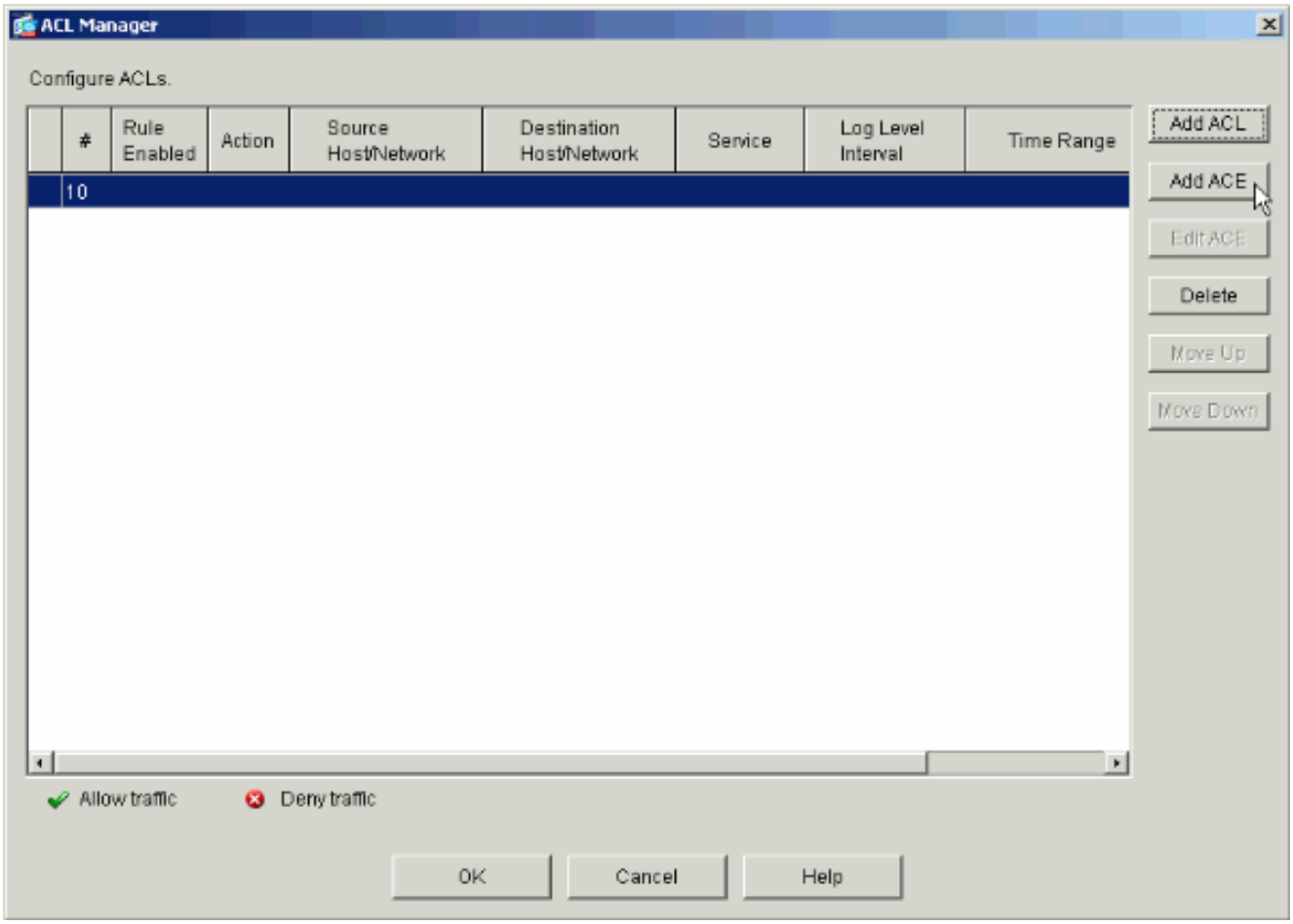
5. Fare clic su **Add ACL** per creare un nuovo elenco degli accessi nella finestra ACL Manager visualizzata.



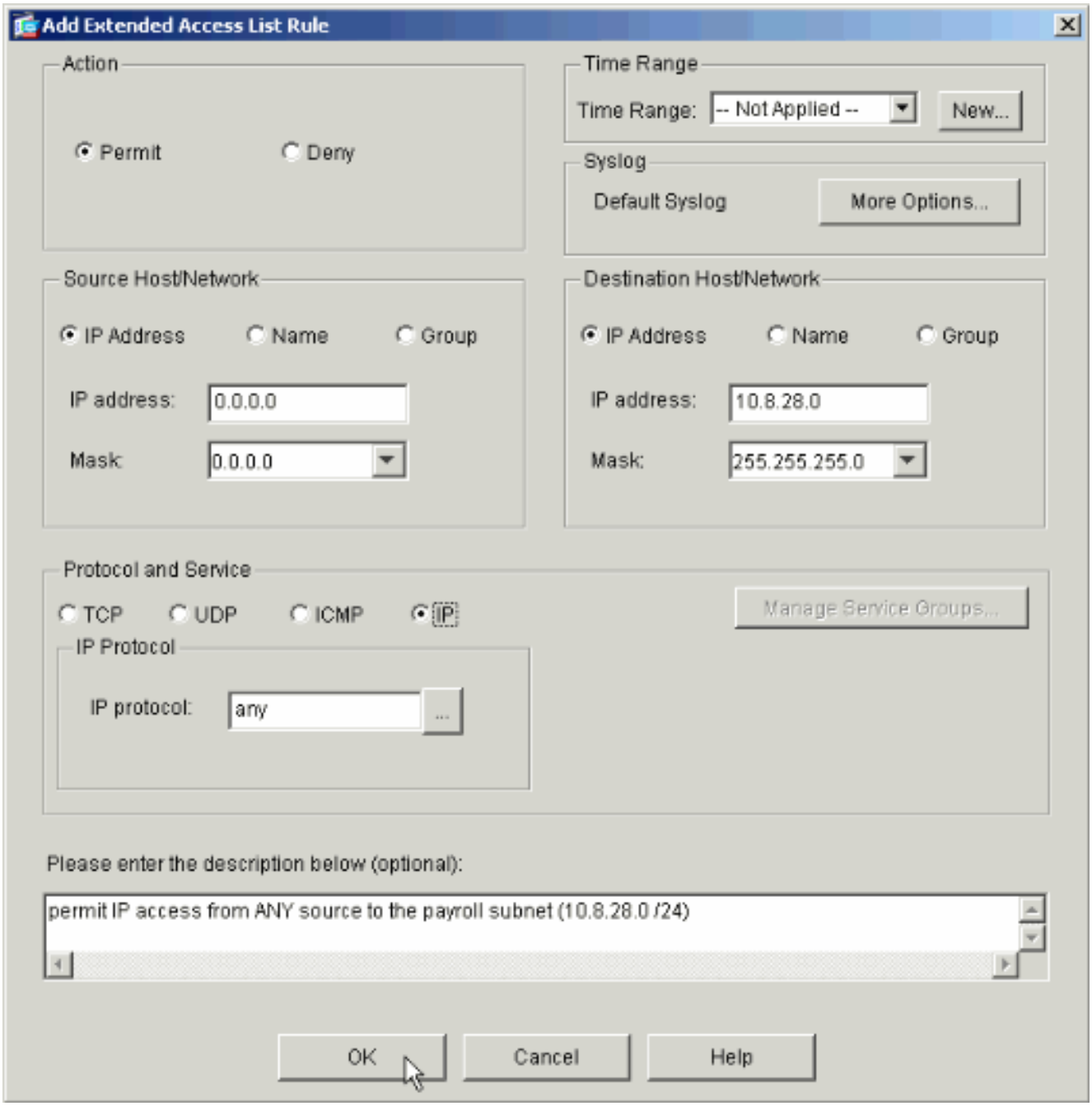
6. Selezionare un numero per il nuovo elenco degli accessi e fare clic su **OK**.



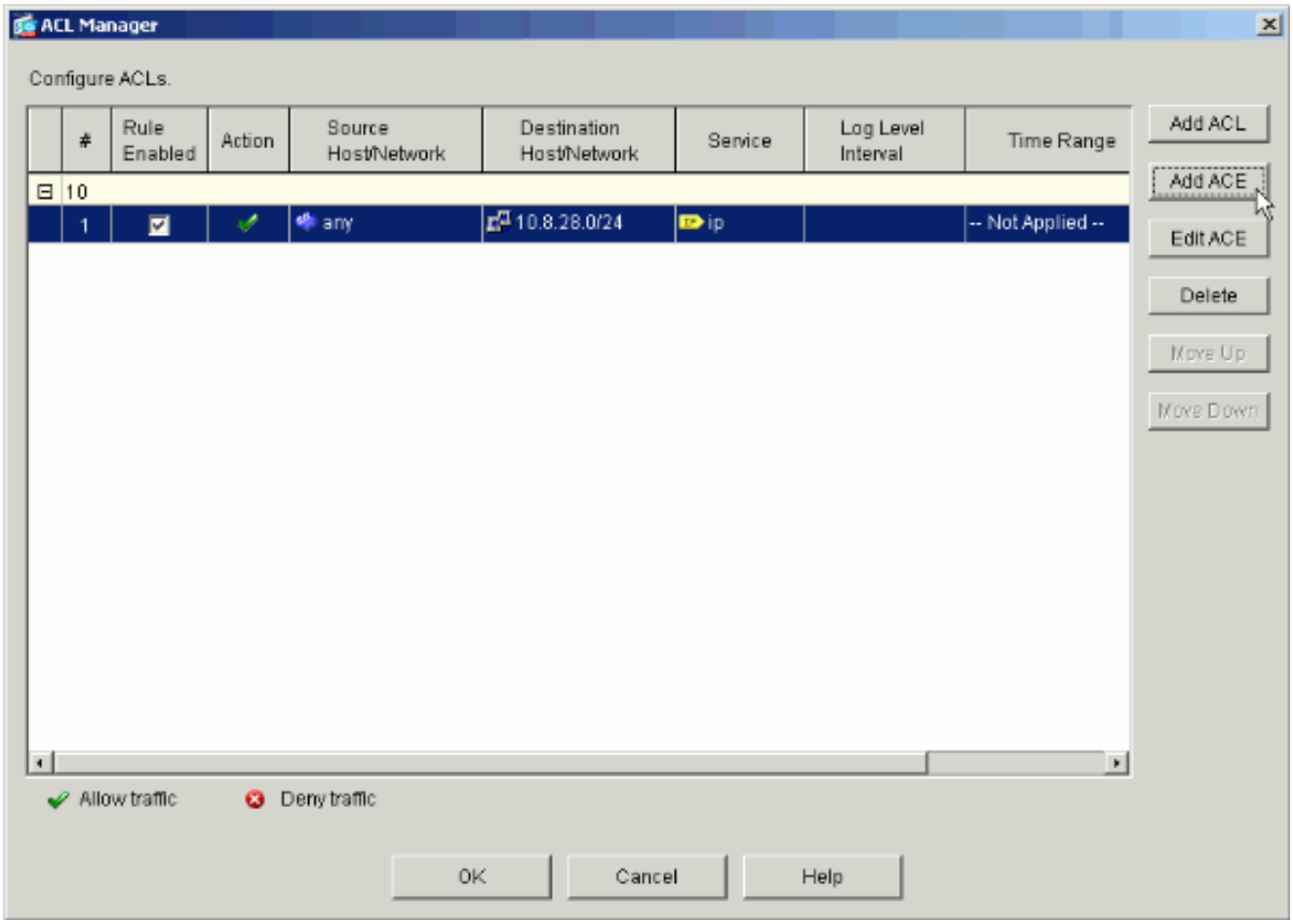
7. Con il nuovo ACL selezionato a sinistra, fare clic su **Add ACE** (Aggiungi voce di controllo di accesso) per aggiungere una nuova voce di controllo di accesso all'elenco.



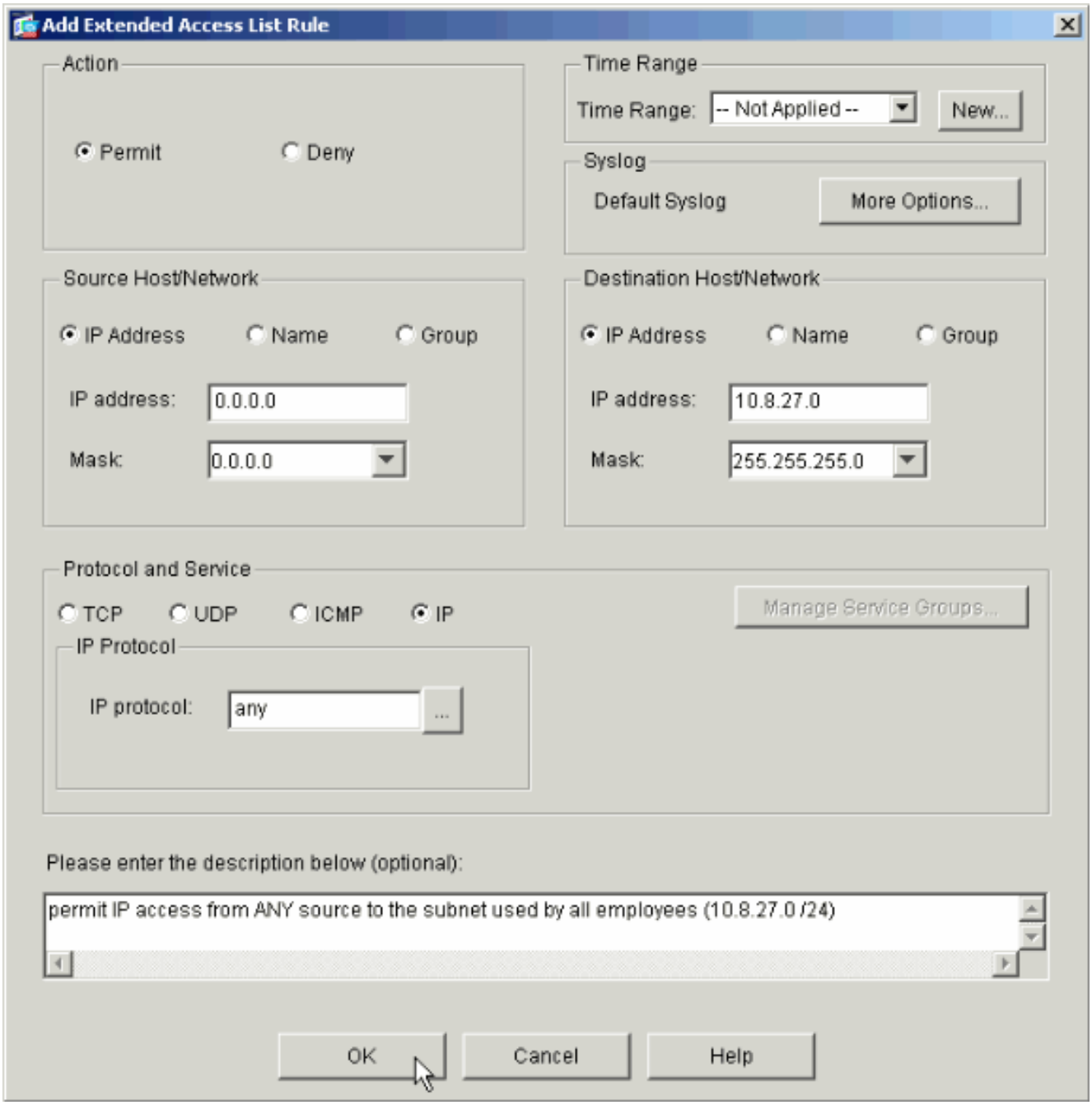
8. Definire la voce di controllo di accesso (ACE, Access Control Entry) che si desidera aggiungere.Nell'esempio, la prima voce ACE nell'ACL 10 consente l'accesso IP alla subnet del ciclo paghe da qualsiasi origine.**Nota:** per impostazione predefinita, ASDM seleziona solo il protocollo TCP. È necessario scegliere IP se si desidera consentire o negare agli utenti l'accesso IP completo. Al termine, fare clic su
OK.



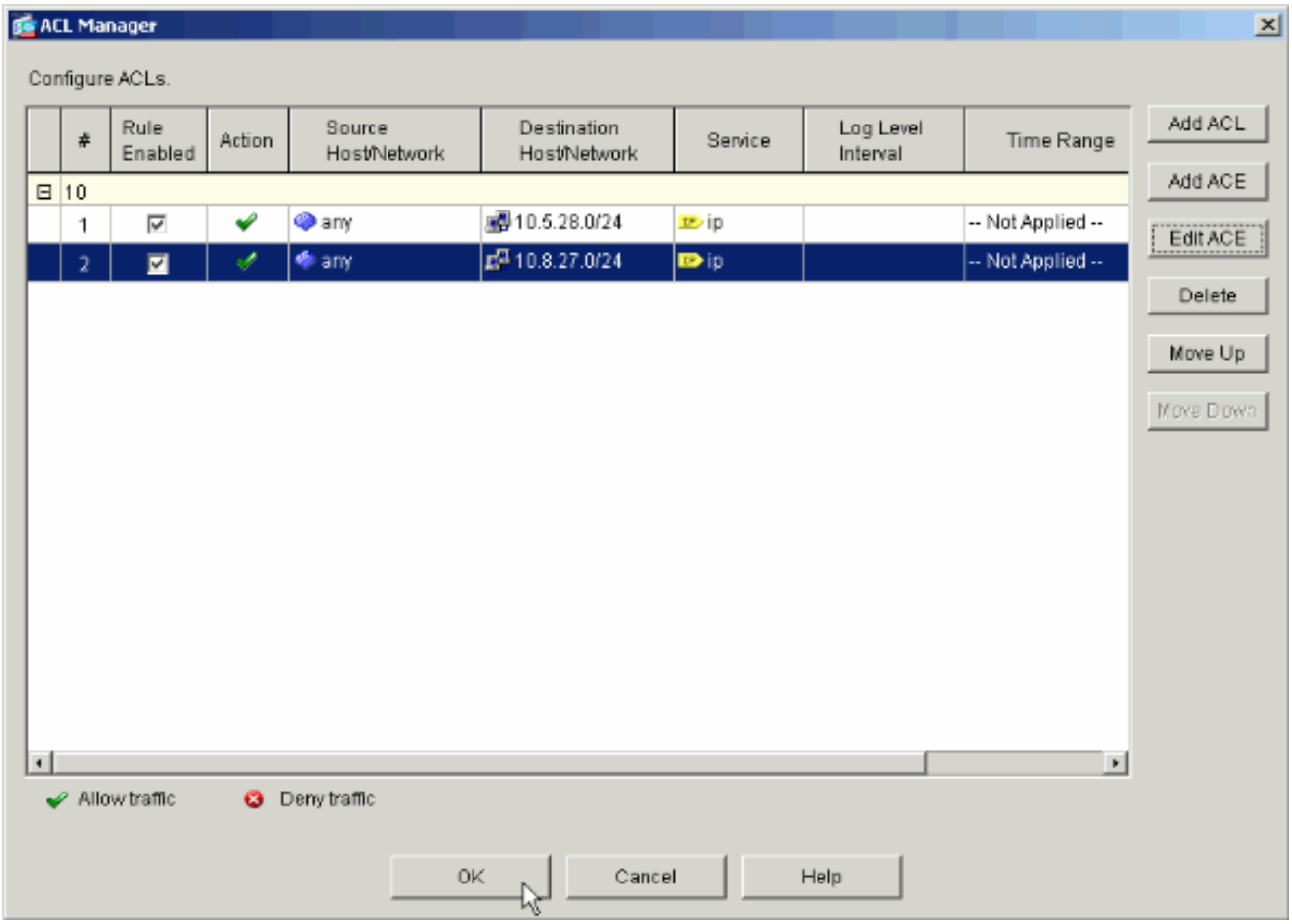
9. La voce di controllo di accesso appena aggiunta verrà visualizzata nell'elenco. Scegliere nuovamente **Aggiungi voce ACE** per aggiungere altre righe all'elenco degli accessi.



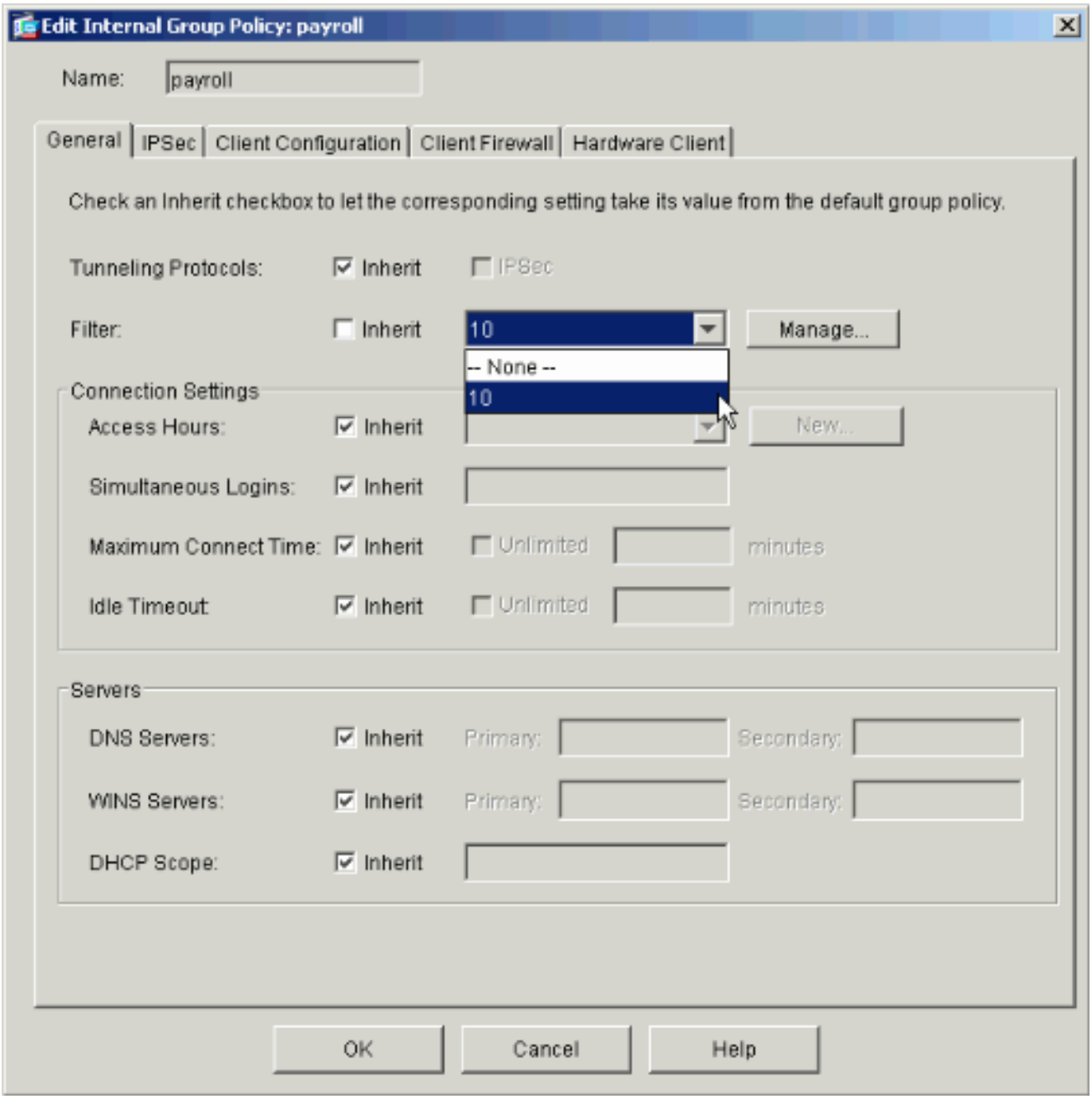
Nell'esempio, una seconda voce ACE viene aggiunta all'ACL 10 per consentire l'accesso alla subnet
Intranet.



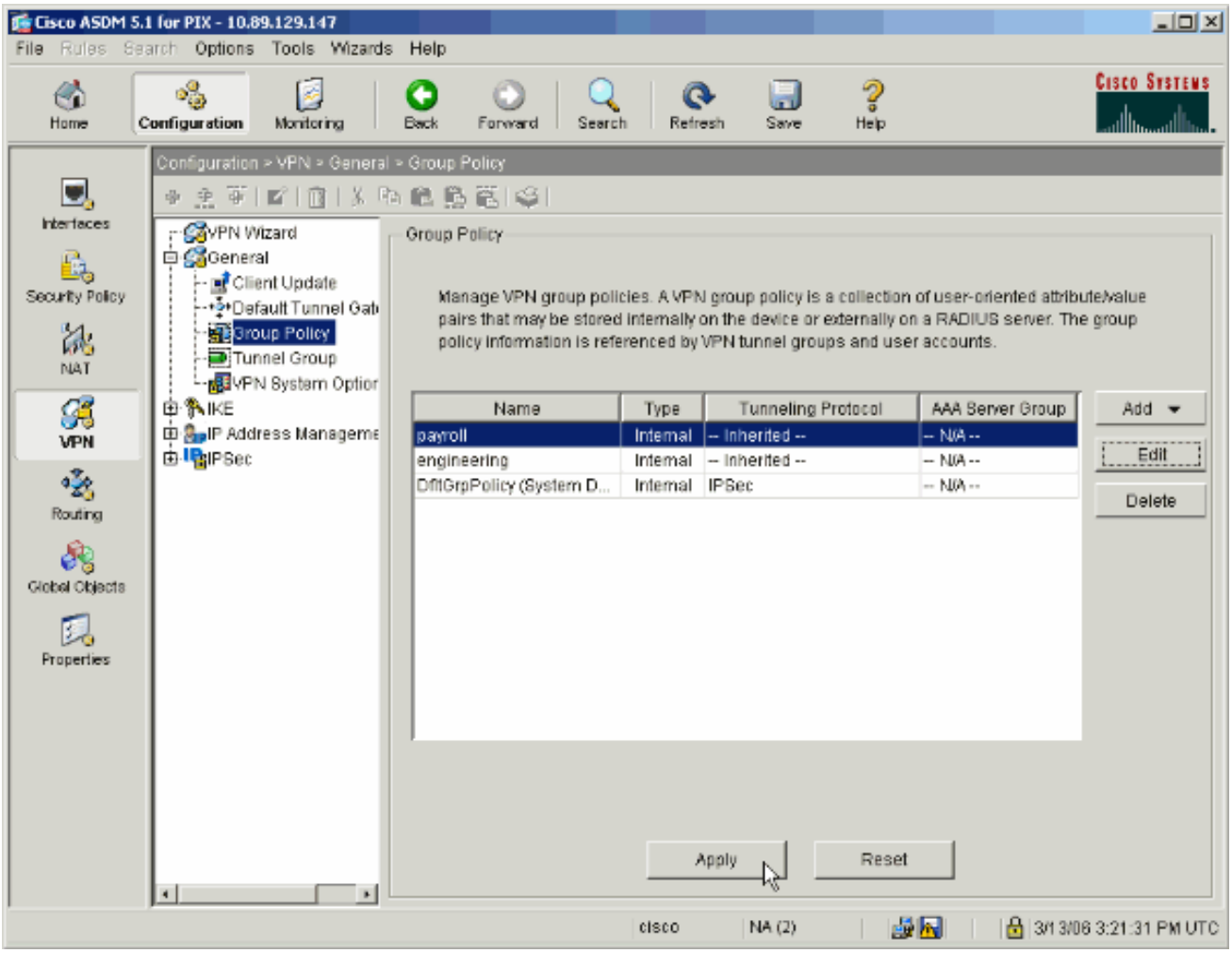
10. Dopo aver aggiunto le voci ACE, fare clic su **OK**.



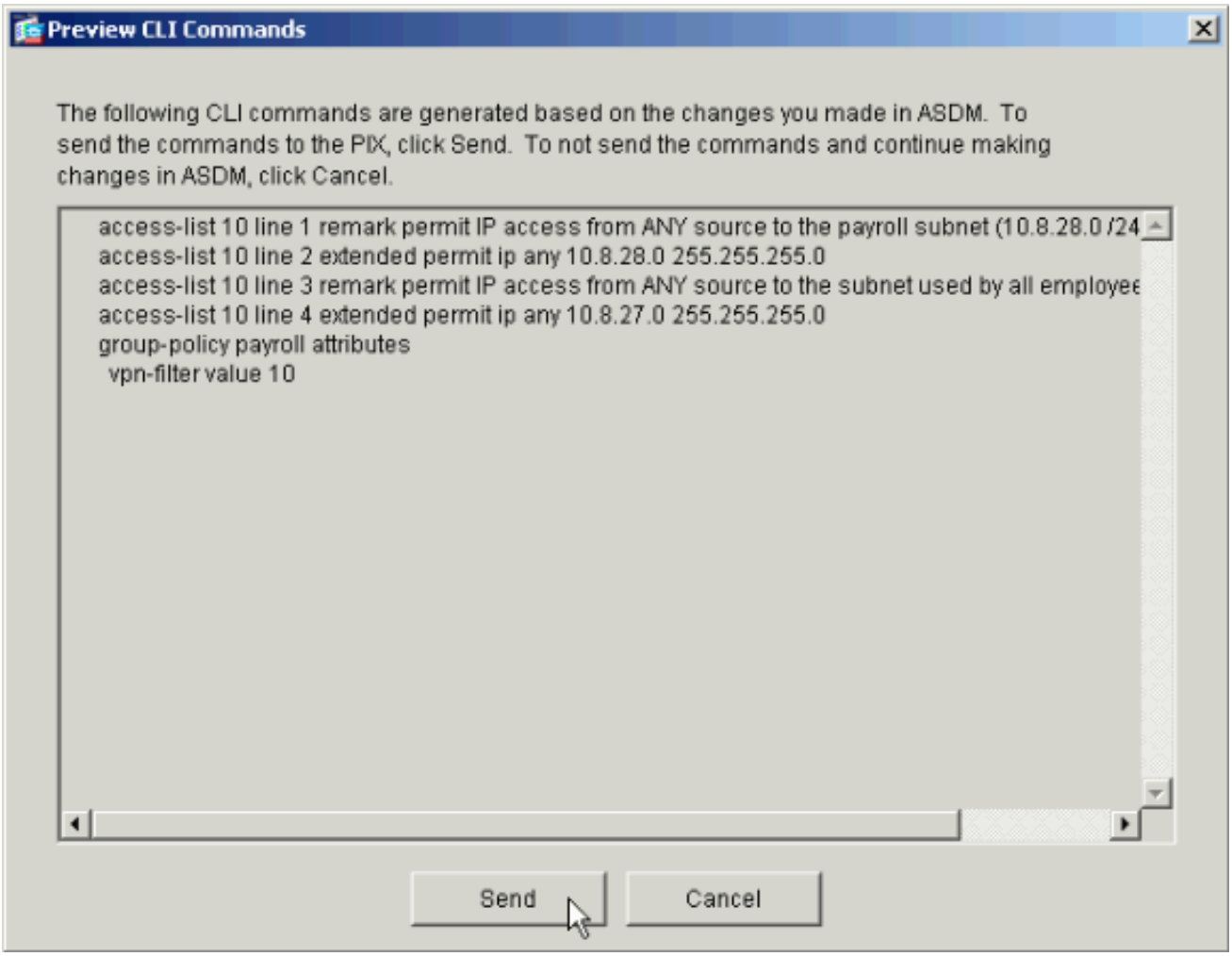
11. Selezionare l'ACL definito e compilato negli ultimi passaggi da utilizzare come filtro per Criteri di gruppo. Al termine, fare clic su
OK.



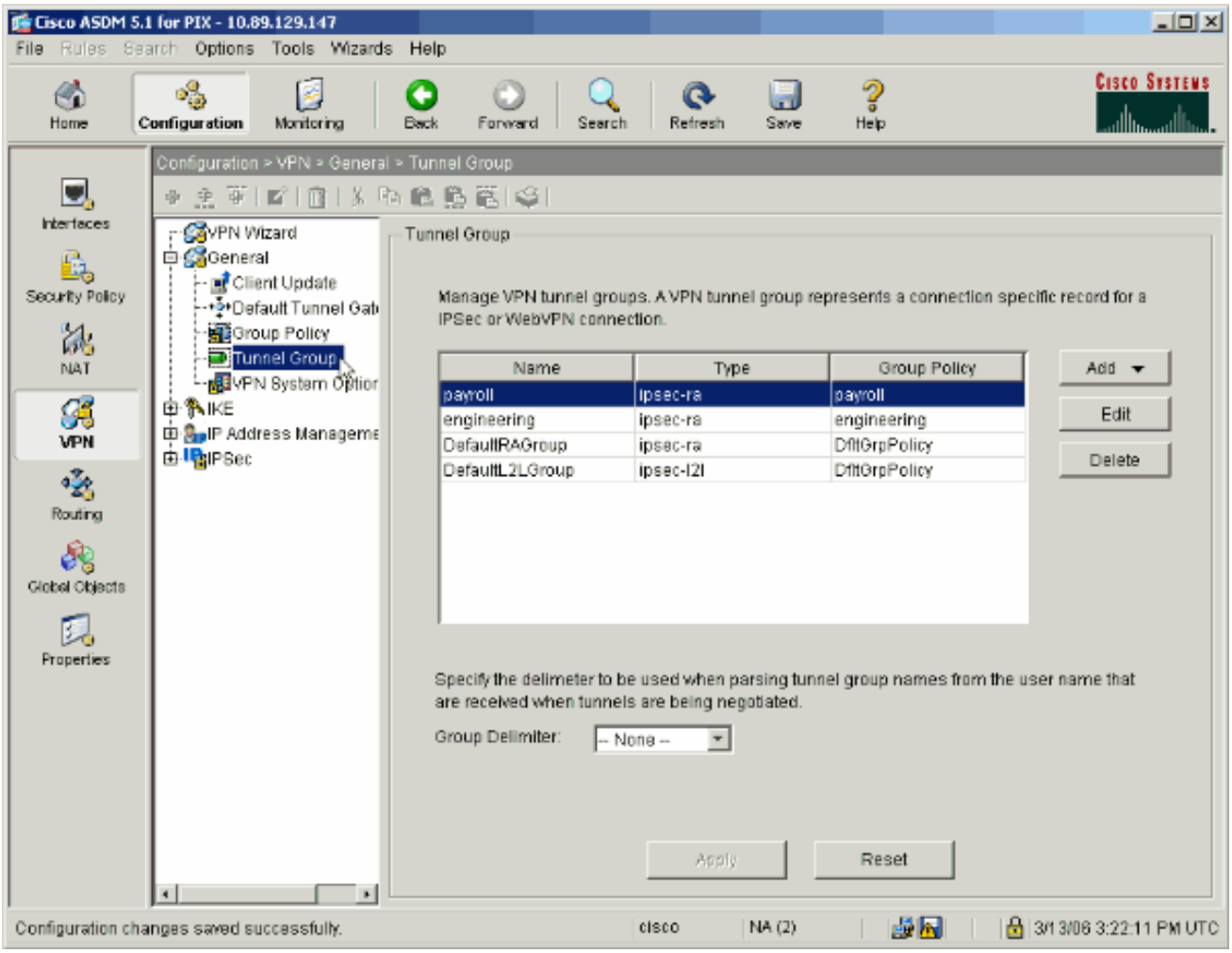
12. Fare clic su **Applica** per inviare le modifiche al PIX.



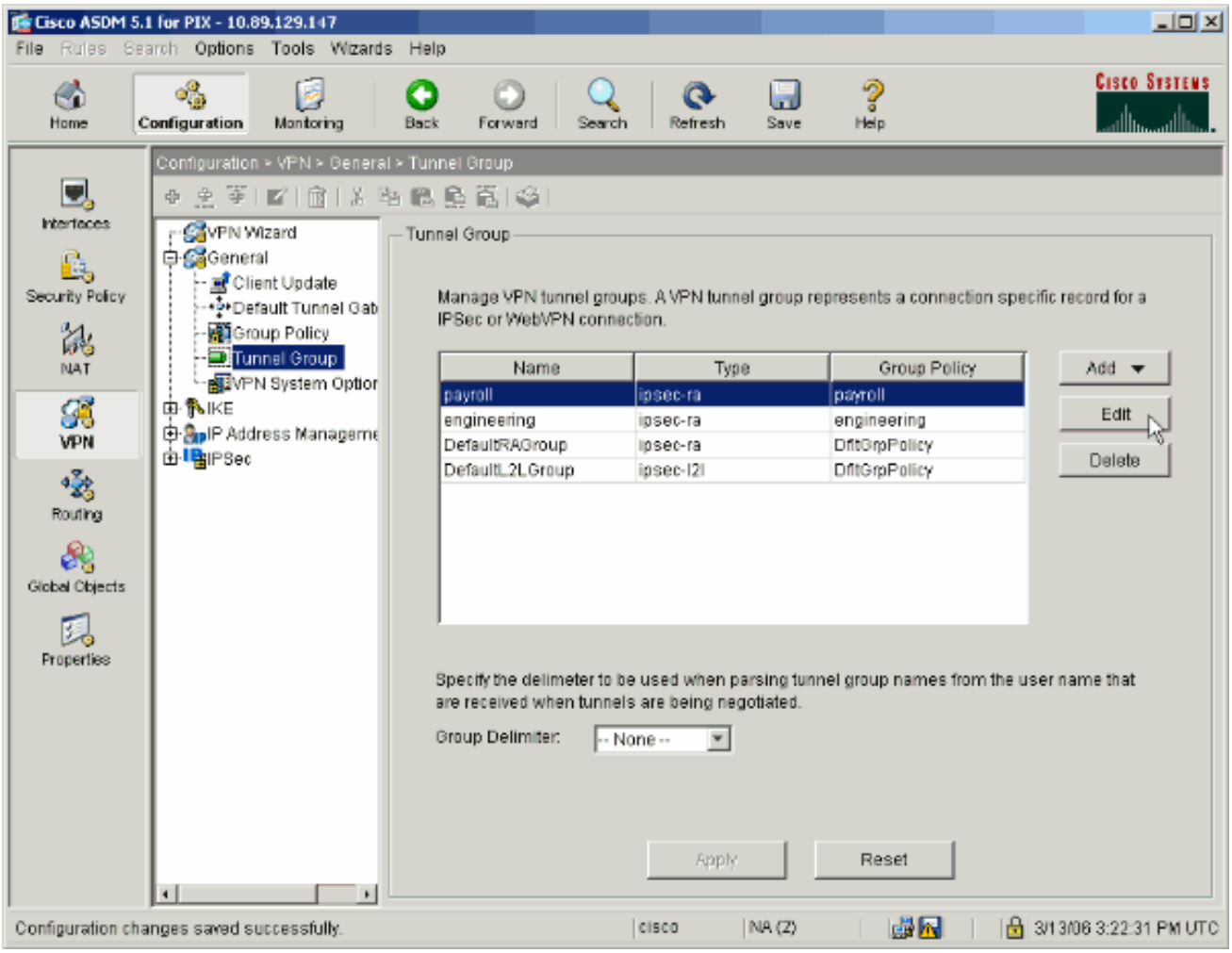
13. Se è stata configurata per eseguire questa operazione in **Opzioni > Preferenze**, ASDM visualizza in anteprima i comandi che sta per inviare al PIX. Fare clic su **Invia**.



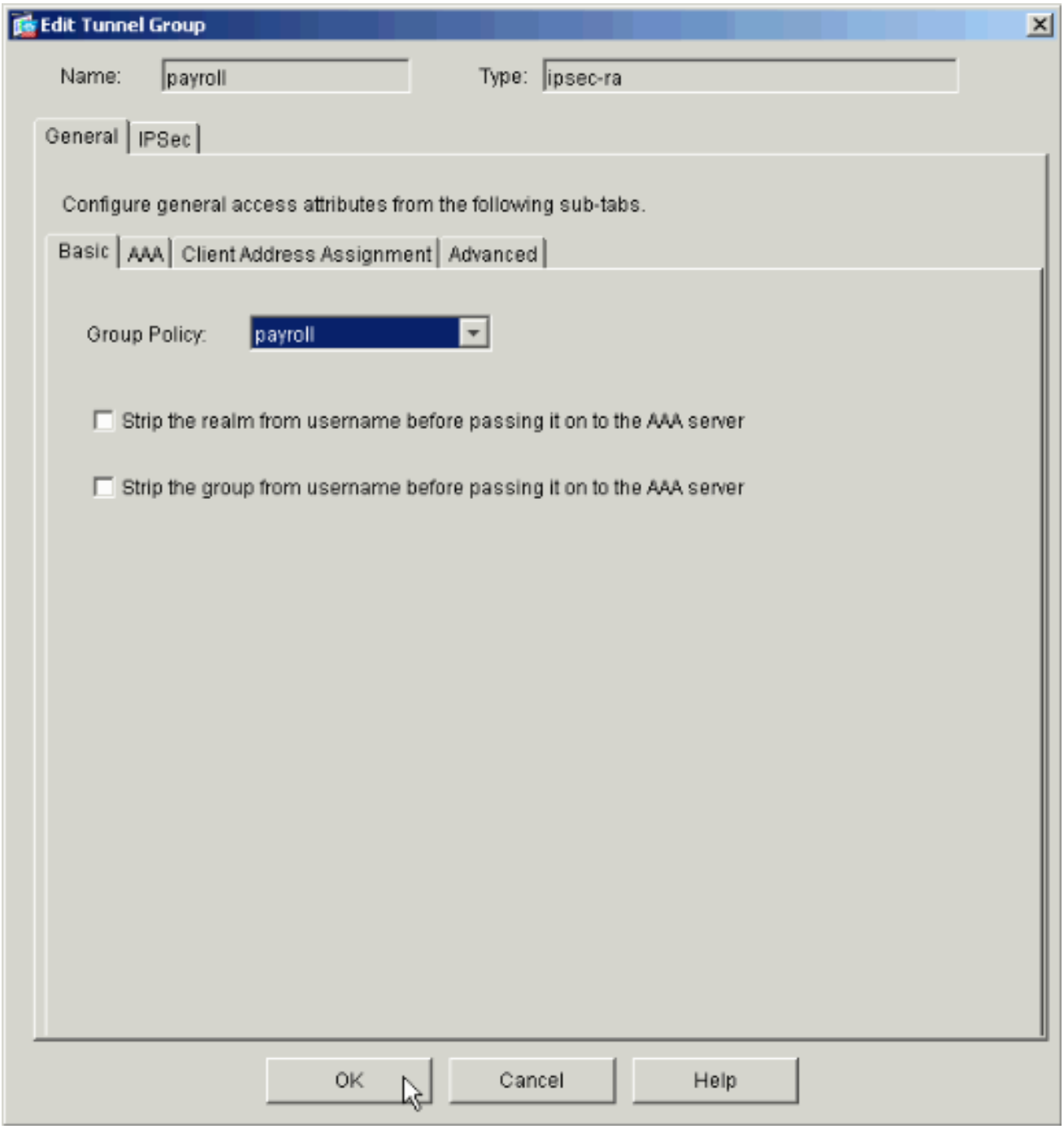
14. Applicare i Criteri di gruppo appena creati o modificati al gruppo di tunnel corretto. Fare clic su **Tunnel Group** nel frame di sinistra.



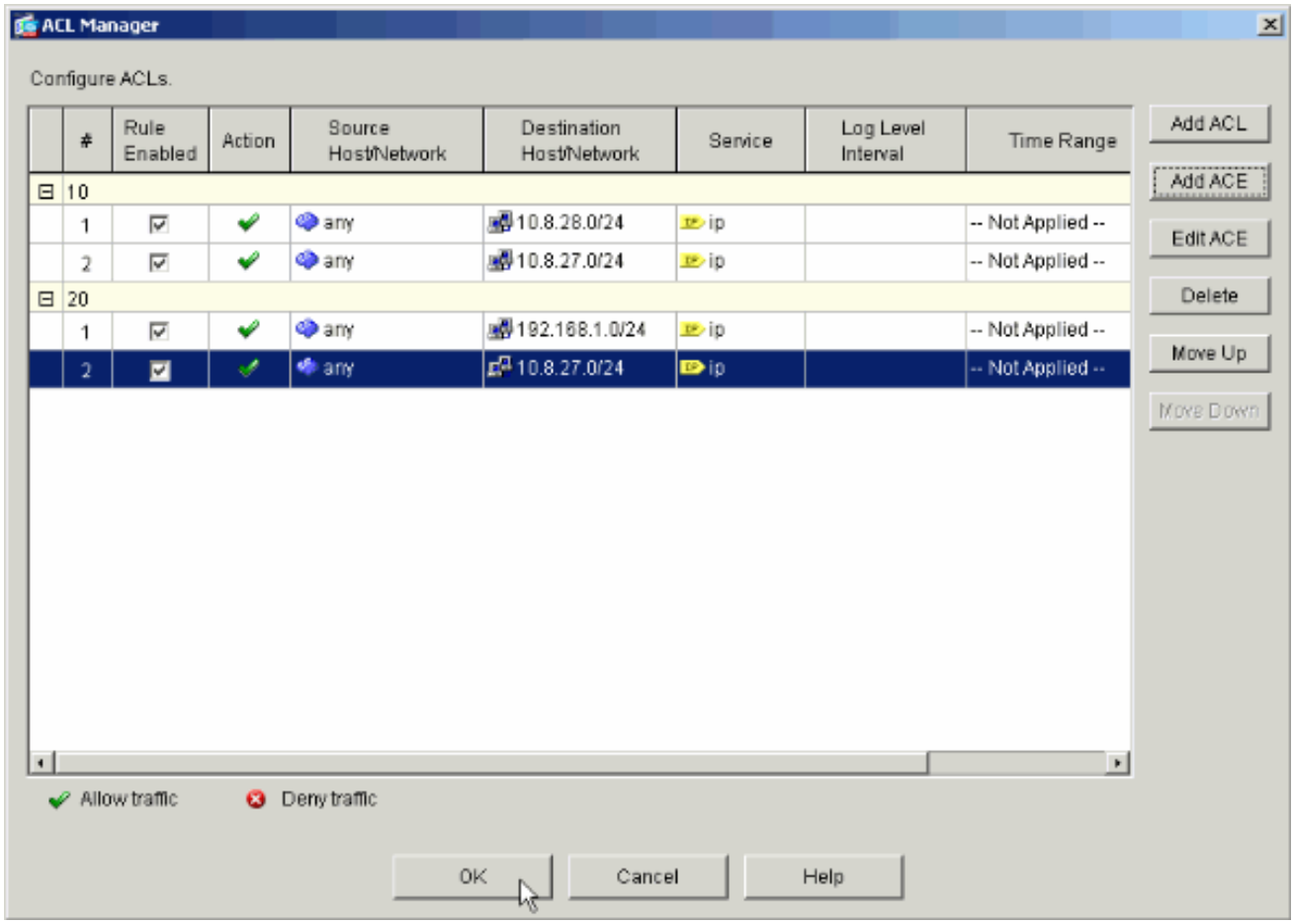
15. Selezionare il gruppo di tunnel a cui si desidera applicare i Criteri di gruppo e fare clic su **Modifica**.



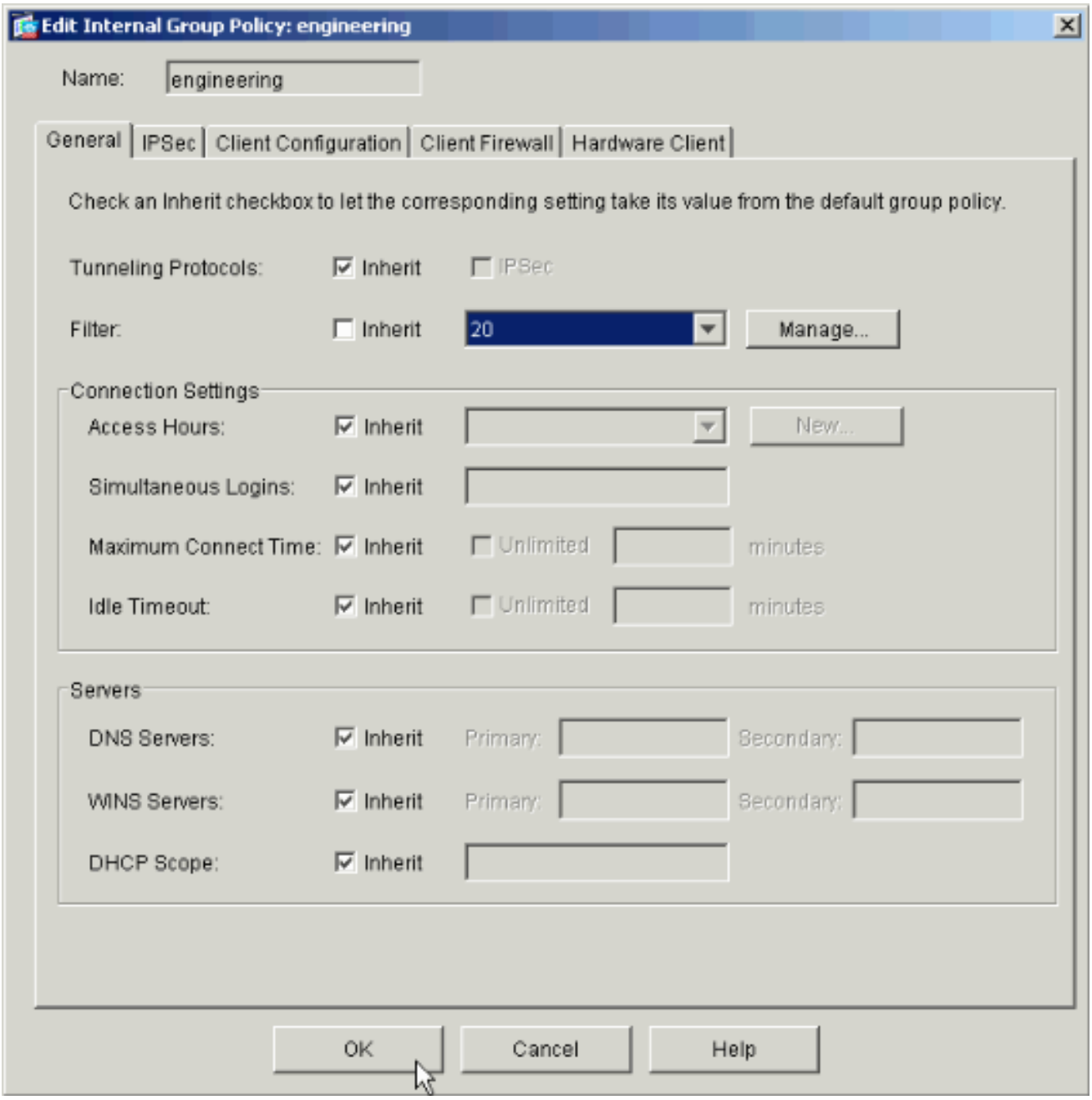
16. Se i Criteri di gruppo sono stati creati automaticamente (vedere il passaggio 2), verificare che i Criteri di gruppo appena configurati siano selezionati nella casella a discesa. Se i Criteri di gruppo non sono stati configurati automaticamente, selezionarli dall'elenco a discesa. Al termine, fare clic su
OK.



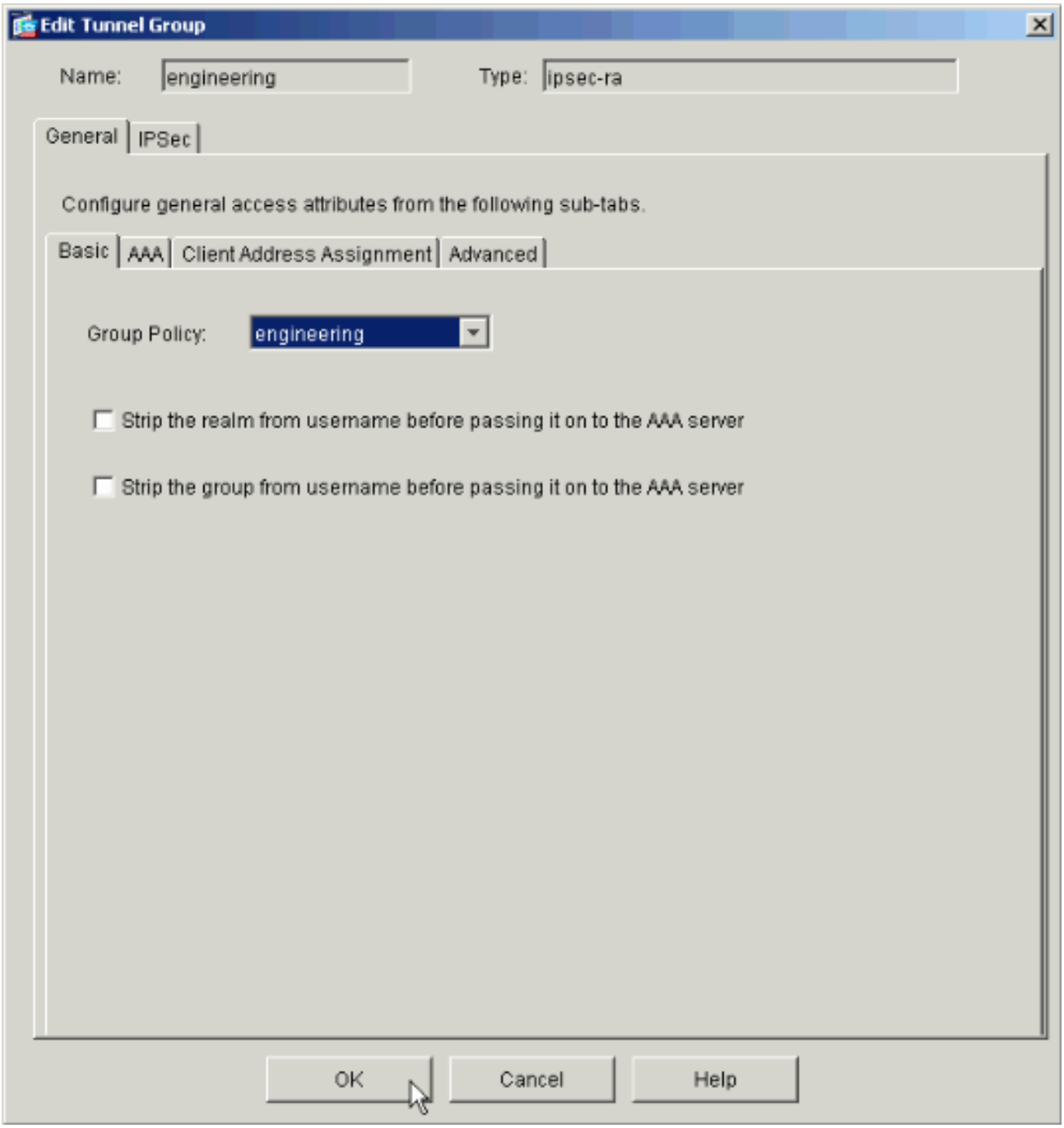
17. Fare clic su **Apply** (Applica), quindi, se richiesto, su **Send** per aggiungere la modifica alla configurazione PIX.Se i Criteri di gruppo sono già stati selezionati, è possibile che venga visualizzato il messaggio "Non sono state apportate modifiche". Fare clic su **OK**.
18. Ripetere i passaggi da 2 a 17 per ogni gruppo di tunnel aggiuntivo a cui si desidera aggiungere restrizioni.In questo esempio di configurazione, è anche necessario limitare l'accesso dei tecnici. Mentre la procedura è la stessa, queste sono alcune finestre in cui le differenze sono notevoli:Nuovo elenco accessi



Scegliere **Elenco accessi 20** come filtro in Criteri di gruppo di Engineering.



Verificare che i Criteri di gruppo di progettazione siano impostati per il gruppo di tunnel di progettazione.



Configurazione dell'accesso tramite CLI

Completare la procedura seguente per configurare l'appliance di sicurezza tramite la CLI:

Nota: alcuni dei comandi mostrati in questo output sono riportati su una seconda riga per motivi di spazio.

1. Creare due diversi elenchi di controllo di accesso (15 e 20) da applicare agli utenti durante la connessione alla VPN di accesso remoto. L'elenco degli accessi verrà richiamato più avanti nella configurazione.

```
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. Creare due pool di indirizzi VPN diversi. Crearne uno per il ciclo paghe e uno per gli utenti remoti del reparto tecnico.

```
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. Creare criteri per il ciclo paghe che si applicano solo a loro quando si connettono.

```
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. Questo passo è uguale al passo 3, con la differenza che è per il gruppo Engineering.

```
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. Creare utenti locali e assegnare gli attributi appena creati a tali utenti per limitarne l'accesso

alle risorse.

```
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. Creare gruppi di tunnel contenenti criteri di connessione per gli utenti del ciclo paghe.

```
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. Creare gruppi di tunnel contenenti criteri di connessione per gli utenti del reparto tecnico.

```
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
```

Dopo aver immesso la configurazione, è possibile visualizzare questa area evidenziata nella configurazione:

Nome dispositivo 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
```

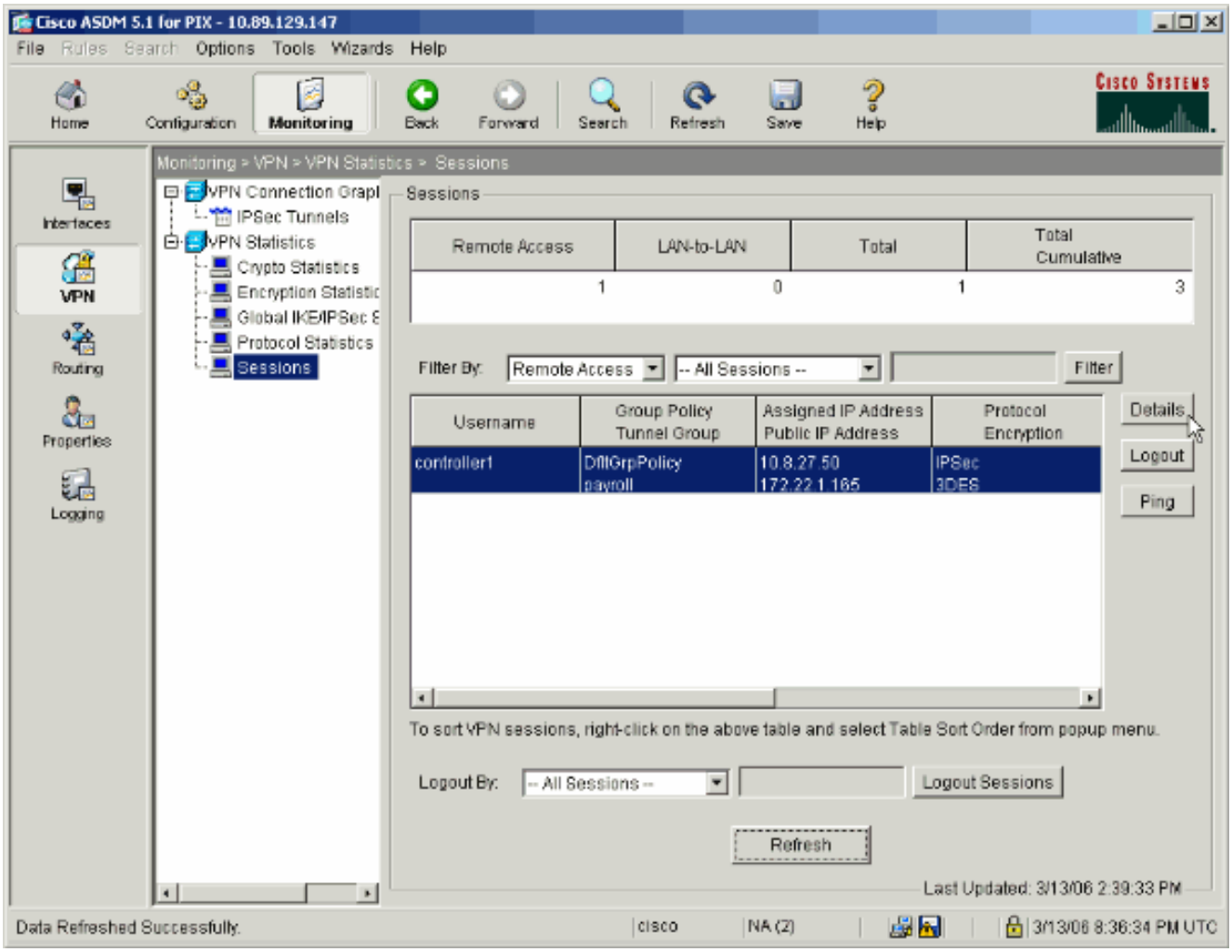
```
nat (Inside) 0 access-list Inside_nat0_outbound
nat (Inside) 1 192.168.1.0 255.255.255.0
nat (Inside) 1 10.8.27.0 255.255.255.0
nat (Inside) 1 10.8.28.0 255.255.255.0
route Intranet 0.0.0.0 0.0.0.0 10.8.27.2
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout 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)#
```

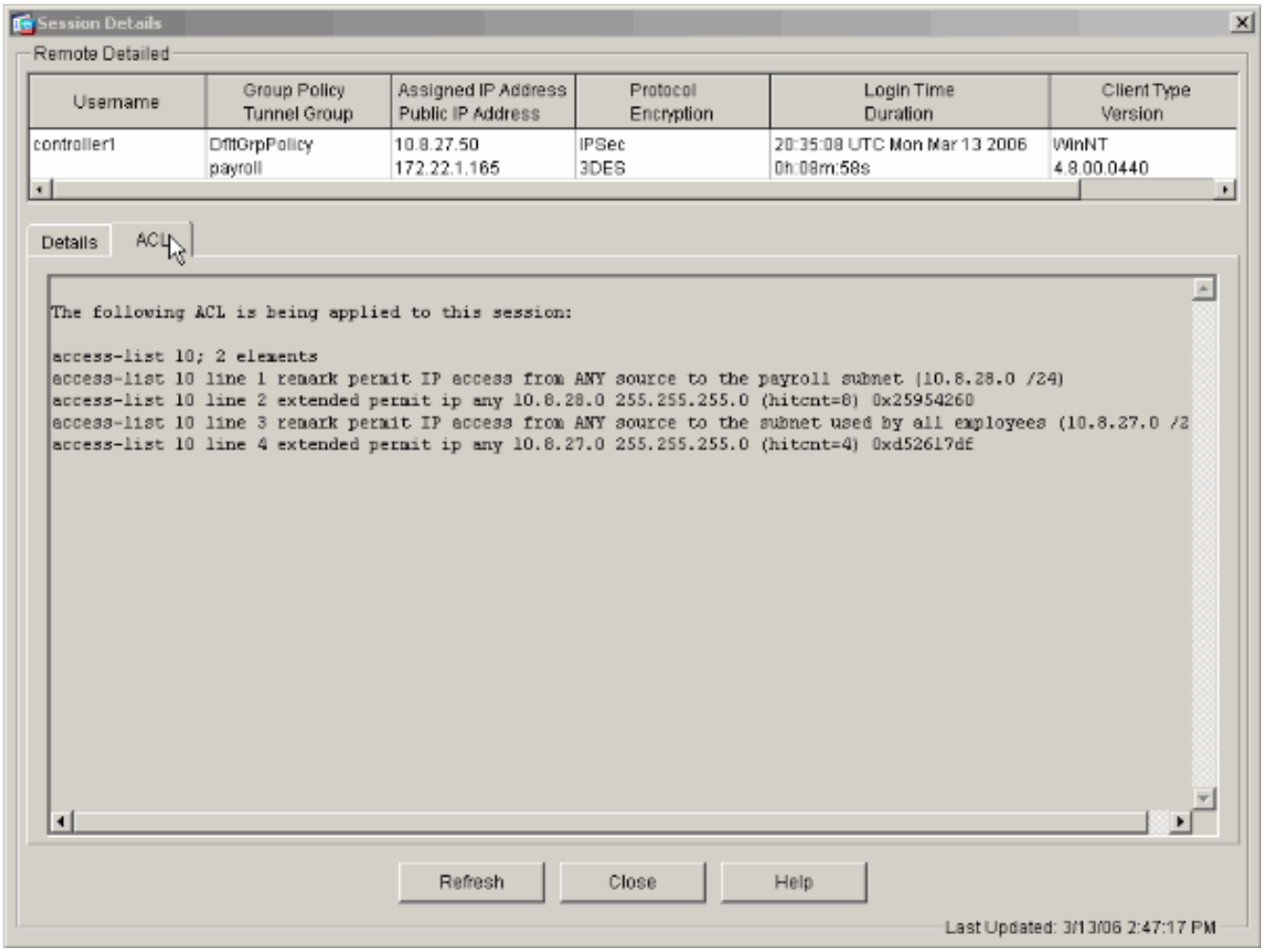
Verifica

Utilizzare le funzionalità di monitoraggio di ASDM per verificare la configurazione:

1. Selezionare **Monitoraggio > VPN > Statistiche VPN > Sessioni**.Si vedono le sessioni VPN attive sul PIX. Selezionare la sessione desiderata e fare clic su **Dettagli**.



2. Selezionare la scheda ACL.Gli `accessi` riflettono il traffico che attraversa il tunnel tra il client e le reti
consentite.



Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance ASA come server VPN remoto con esempio di configurazione ASDM
- Esempi di configurazione di appliance di sicurezza Cisco PIX serie 500 e note tecniche
- Esempi di configurazione di appliance Cisco ASA serie 5500 Adaptive Security e note tecniche
- Esempi di configurazione di Cisco VPN Client e note tecniche
- Documentazione e supporto tecnico – Cisco Systems