PIX/ASA 7.x ASDM:限制遠端訪問VPN使用者的網路訪問

目錄

簡介

本文檔提供了使用思科自適應安全裝置管理器(ASDM)的示例配置，用於限制在PIX安全裝置或自適應安全裝置(ASA)之後哪些內部網路遠端訪問VPN使用者可以訪問。 在以下情況下，您可以將遠端訪問VPN使用者限制在希望其訪問的網路區域：

1. 建立訪問清單。
2. 將它們與組策略關聯。
3. 將這些組策略與隧道組關聯。

請參閱配置Cisco VPN 3000集中器以使用過濾器和RADIUS過濾器分配進行阻止，以瞭解有關VPN集中器阻止VPN使用者訪問的方案的詳細資訊。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 可以使用ASDM配置PIX。**注意：**請參閱允許ASDM的HTTPS訪問，以便允許ASDM配置PIX。
- 您至少有一個已知正常的遠端訪問VPN配置。**附註：** 如果您沒有任何此類配置，請參閱使用ASDM作為遠端VPN伺服器的ASA配置示例，瞭解有關如何配置一個好的遠端訪問VPN配置的資訊。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco安全PIX 500系列安全裝置版本7.1(1)**附註：** PIX 501和506E安全裝置不支援7.x版。
- 思科調適型安全裝置管理員版本5.1(1)**附註：** ASDM僅在PIX或ASA 7.x中可用。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

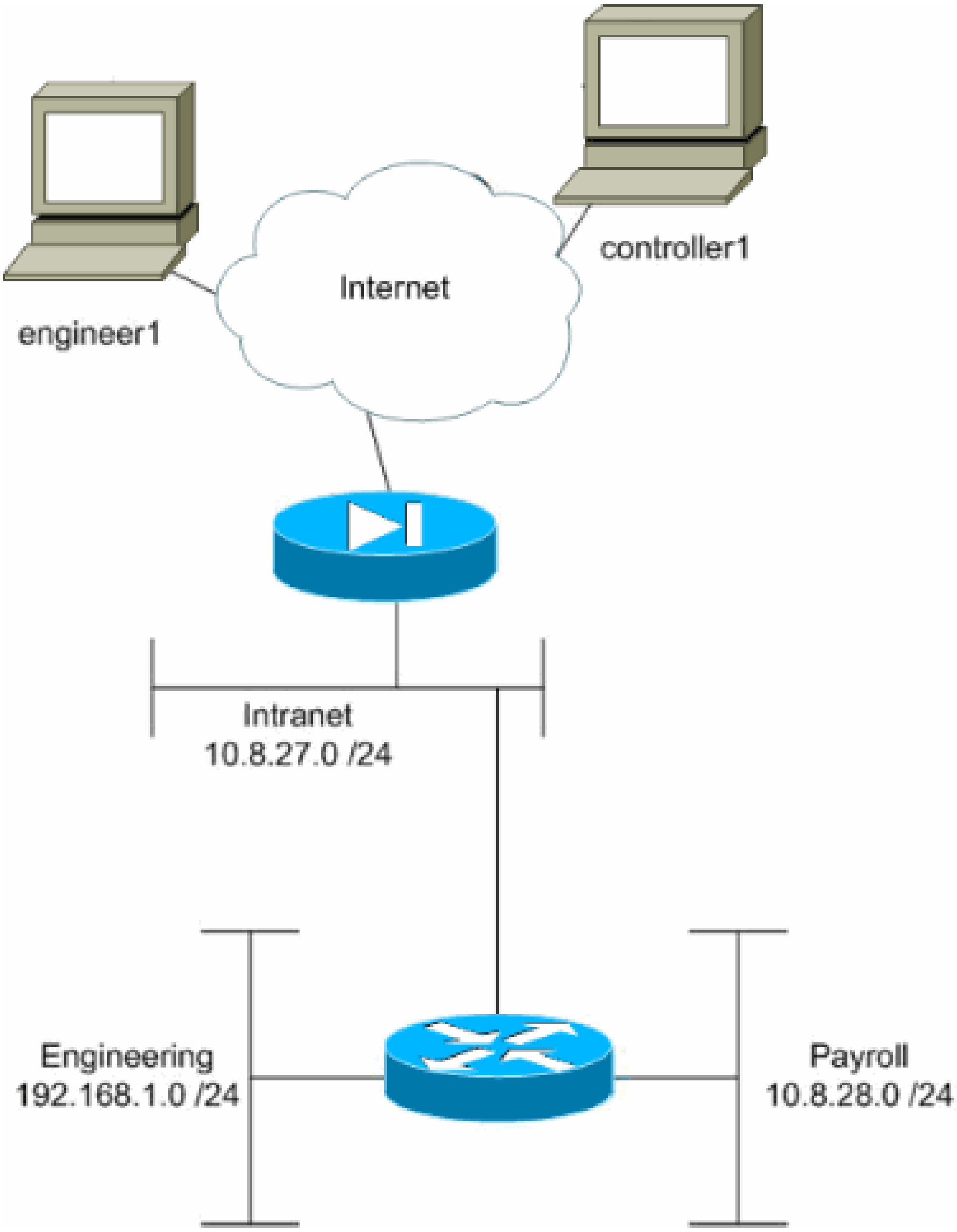
相關產品

此配置還可以用於以下硬體和軟體版本：

- Cisco ASA 5500系列調適型安全裝置版本7.1(1)

網路圖表

本檔案會使用以下網路設定：



在此配置示例中，假設一個小型公司網路包含三個子網。此圖說明拓撲。這三個子網是Intranet、Engineering和Payroll。此配置示例的目標是允許工資單人員遠端訪問Intranet和Payroll子網，並防止他們訪問Engineering子網。此外，工程師應能夠遠端訪問Intranet和Engineering子網，但不能訪問Payroll子網。本示例中的工資單使用者是「controller1」。 本示例中的工程使用者是「engineer1」。

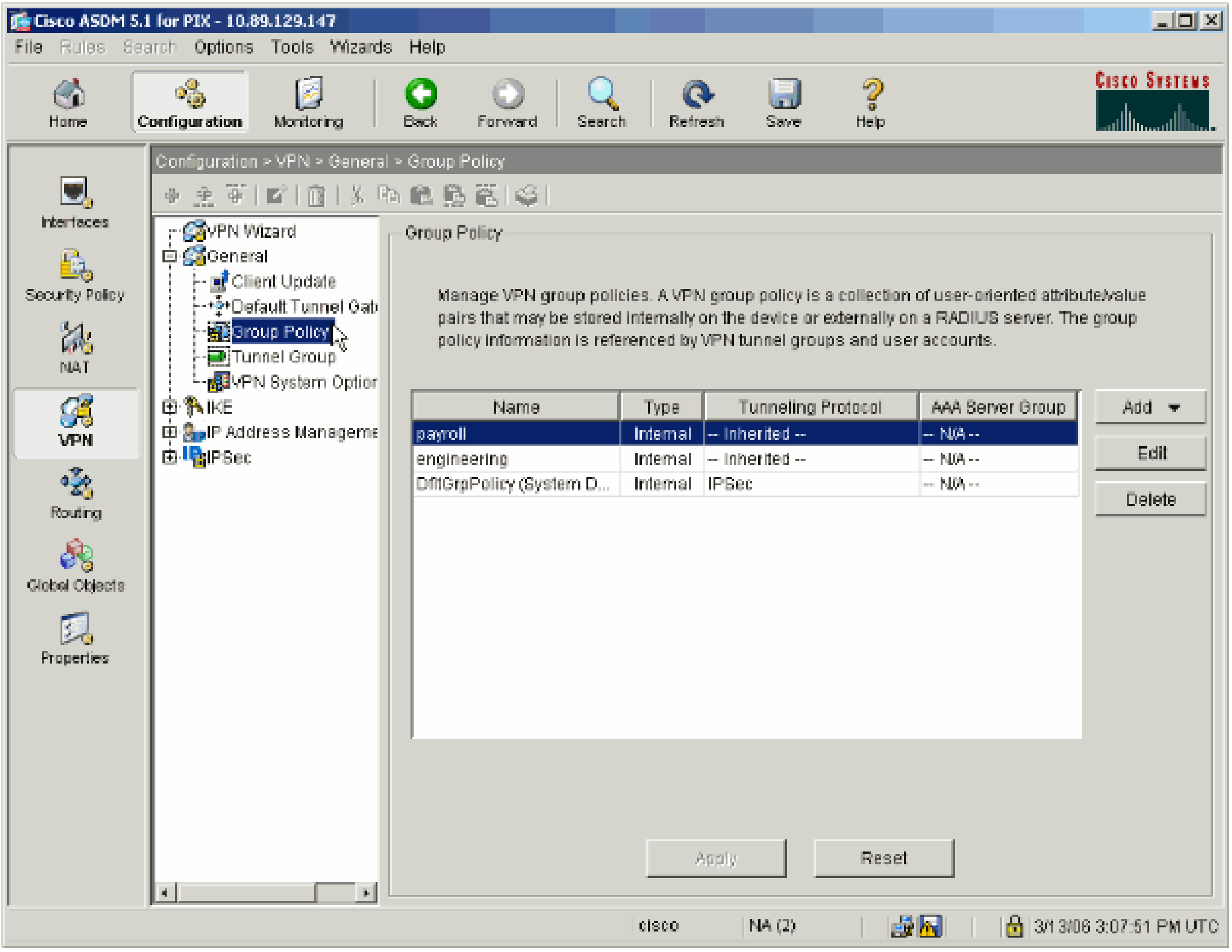
慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

通過ASDM配置訪問

完成以下步驟，使用ASDM配置PIX安全裝置：

1. 選擇**Configuration > VPN > General > Group Policy**。



Configuration > VPN > General > Group Policy

Group Policy

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally on the device or externally on a RADIUS server. The group policy information is referenced by VPN tunnel groups and user accounts.

Name	Type	Tunneling Protocol	AAA Server Group
payroll	Internal	-- Inherited --	-- N/A --
engineering	Internal	-- Inherited --	-- N/A --
DfltGrpPolicy (System D...	Internal	IPSec	-- N/A --

Add ▾

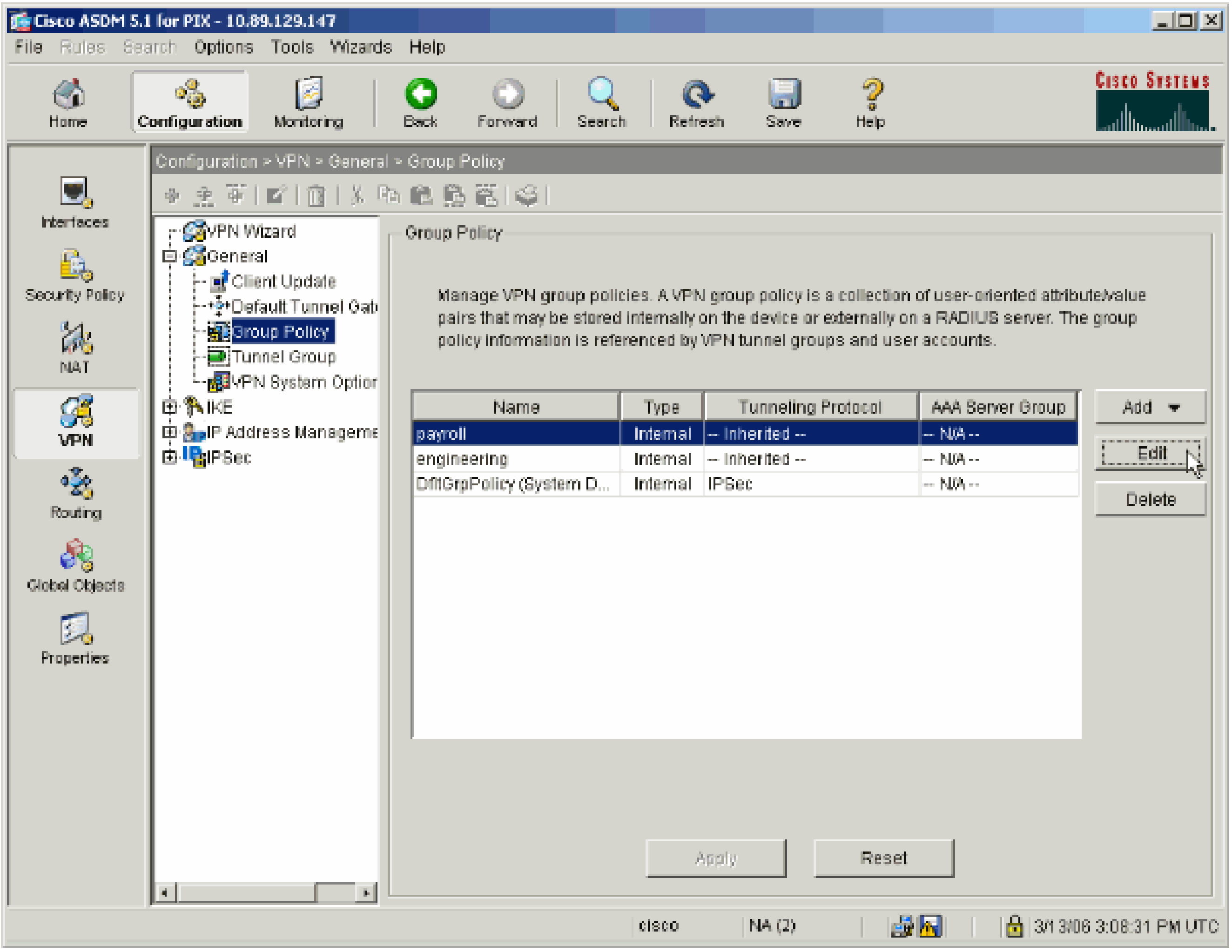
Edit

Delete

Apply

Reset

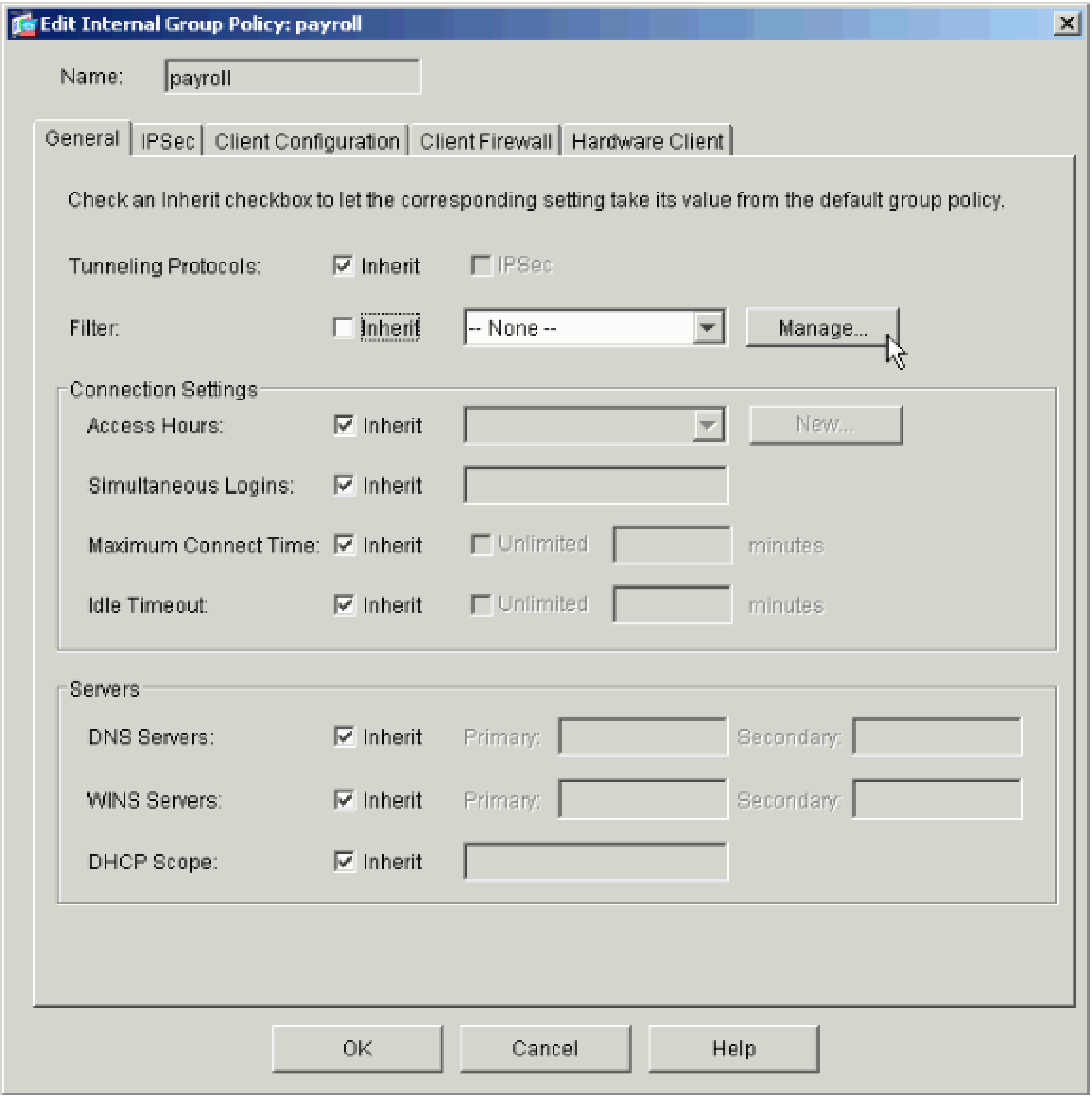
2. 根據在PIX上配置隧道組的步驟，對於要限制其使用者的隧道組，可能已存在組策略。如果已經存在合適的組策略，請選擇它，然後按一下**編輯**。否則，請按一下**Add**並選擇**Internal Group Policy...**.



Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally on the device or externally on a RADIUS server. The group policy information is referenced by VPN tunnel groups and user accounts.

Name	Type	Tunneling Protocol	AAA Server Group
payroll	Internal	-- Inherited --	-- N/A --
engineering	Internal	-- Inherited --	-- N/A --
DfltGrpPolicy (System D...	Internal	IPSec	-- N/A --

3. 如有必要，在開啟的視窗頂部輸入或更改組策略的名稱。
4. 在「General（常規）」頁籤上，取消選中「Filter（過濾器）」旁邊的「**Inherit**」框，然後按一下「**Manage**」。



Edit Internal Group Policy: payroll

Name: payroll

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

Tunneling Protocols: ☑ Inherit □ IPSec

Filter: □ Inherit -- None -- Manage...

Connection Settings

Access Hours: ☑ Inherit New...

Simultaneous Logins: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ Unlimited minutes

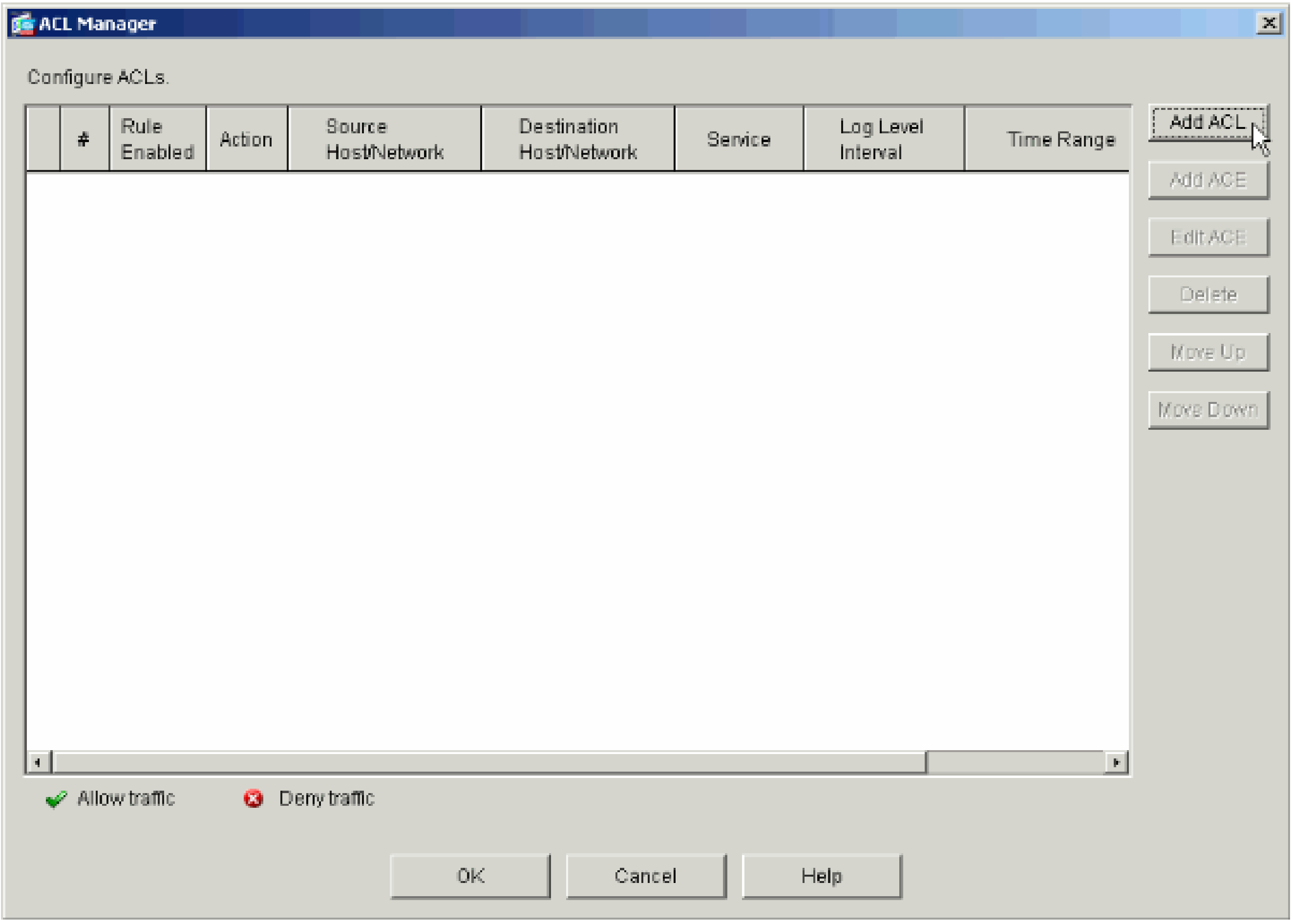
Servers

DNS Servers: ☑ Inherit Primary: Secondary:

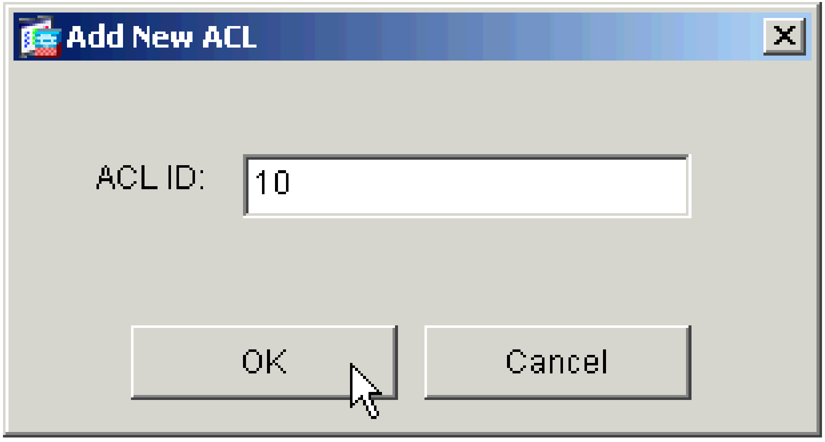
WINS Servers: ☑ Inherit Primary: Secondary:

DHCP Scope: ☑ Inherit

5. 在出現的ACL Manager視窗中，按一下**Add ACL**以建立新的訪問清單。

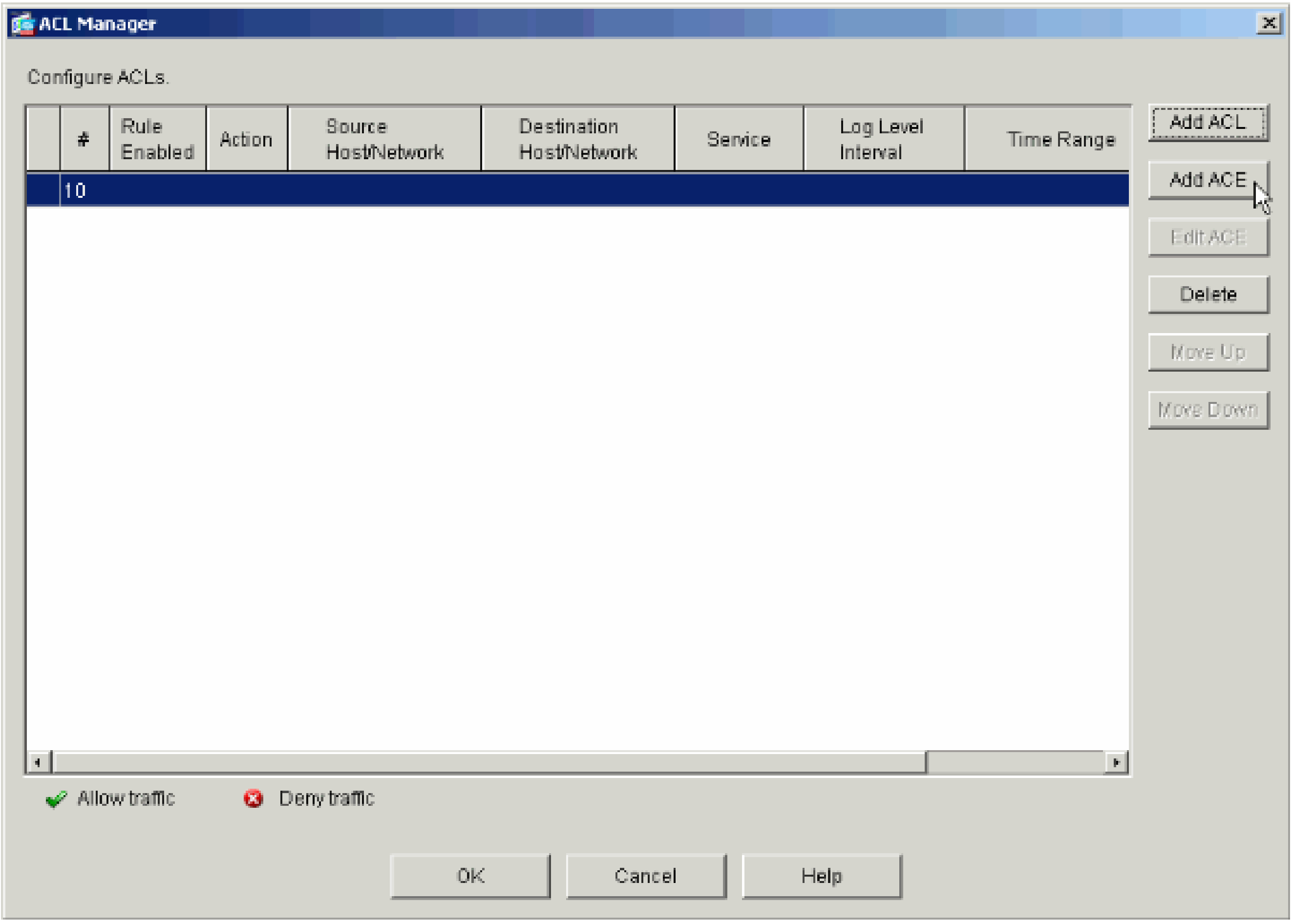


6. 為新訪問清單選擇一個數字，然後按一下**OK**。



ACL ID: 10

7. 在左側選擇新ACL的情況下，按一下**Add ACE**將新的訪問控制項新增到清單中。

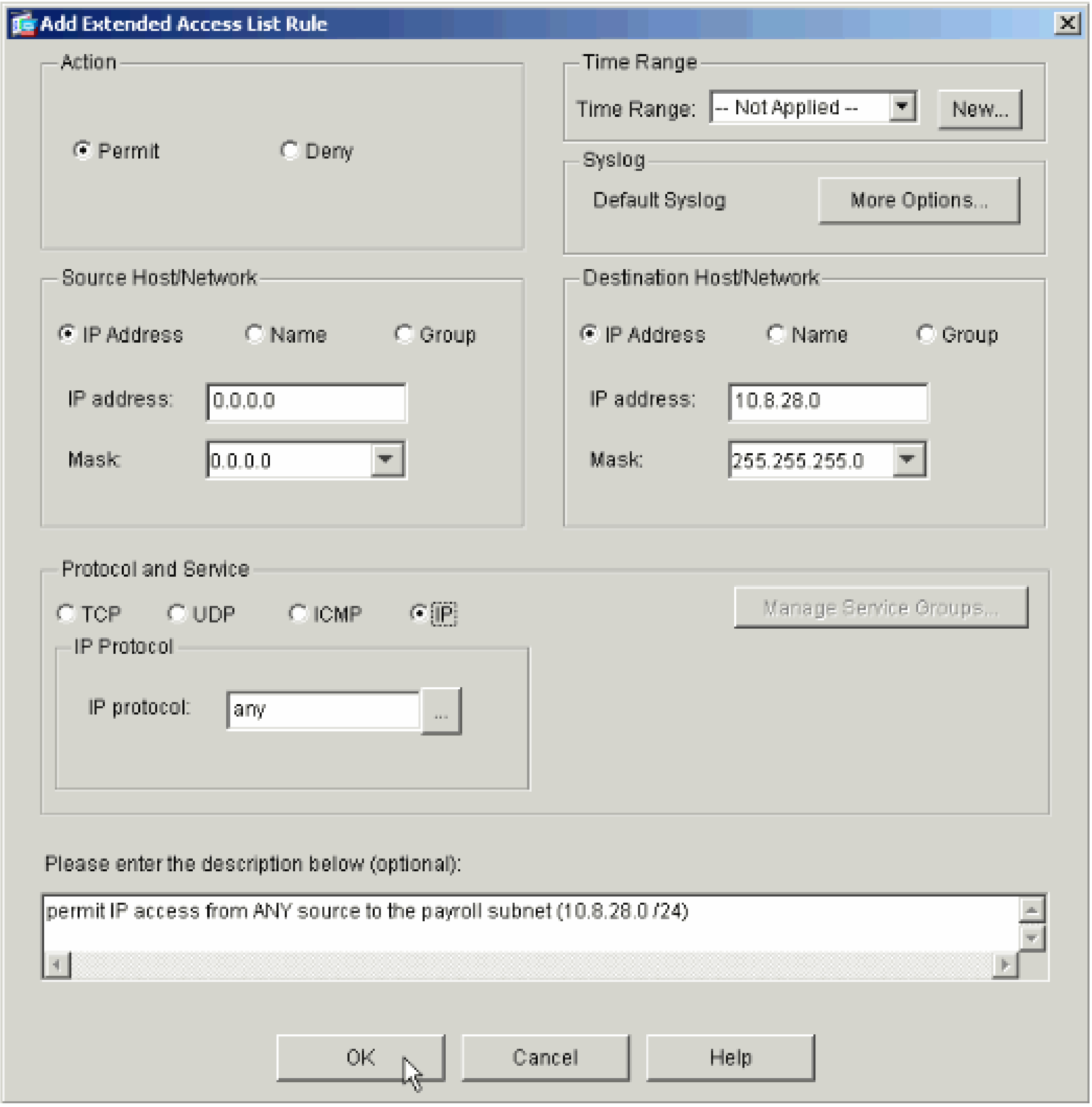


ACL Manager

Configure ACLs.

	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range
	10							

8. 定義要新增的訪問控制條目(ACE)。在本例中，ACL 10中的第一個ACE允許從任何源對Payroll子網進行IP訪問。**注意：**預設情況下，ASDM僅選擇TCP作為協定。如果要允許或拒絕使用者完全IP訪問，則必須選擇IP。完成後按一下**OK**。



Add Extended Access List Rule

Action

● Permit ○ Deny

Time Range

Time Range: -- Not Applied --

Syslog

Default Syslog

Source Host/Network

● IP Address ○ Name ○ Group

IP address: 0.0.0.0

Mask: 0.0.0.0

Destination Host/Network

● IP Address ○ Name ○ Group

IP address: 10.8.28.0

Mask: 255.255.255.0

Protocol and Service

○ TCP ○ UDP ○ ICMP ● IP

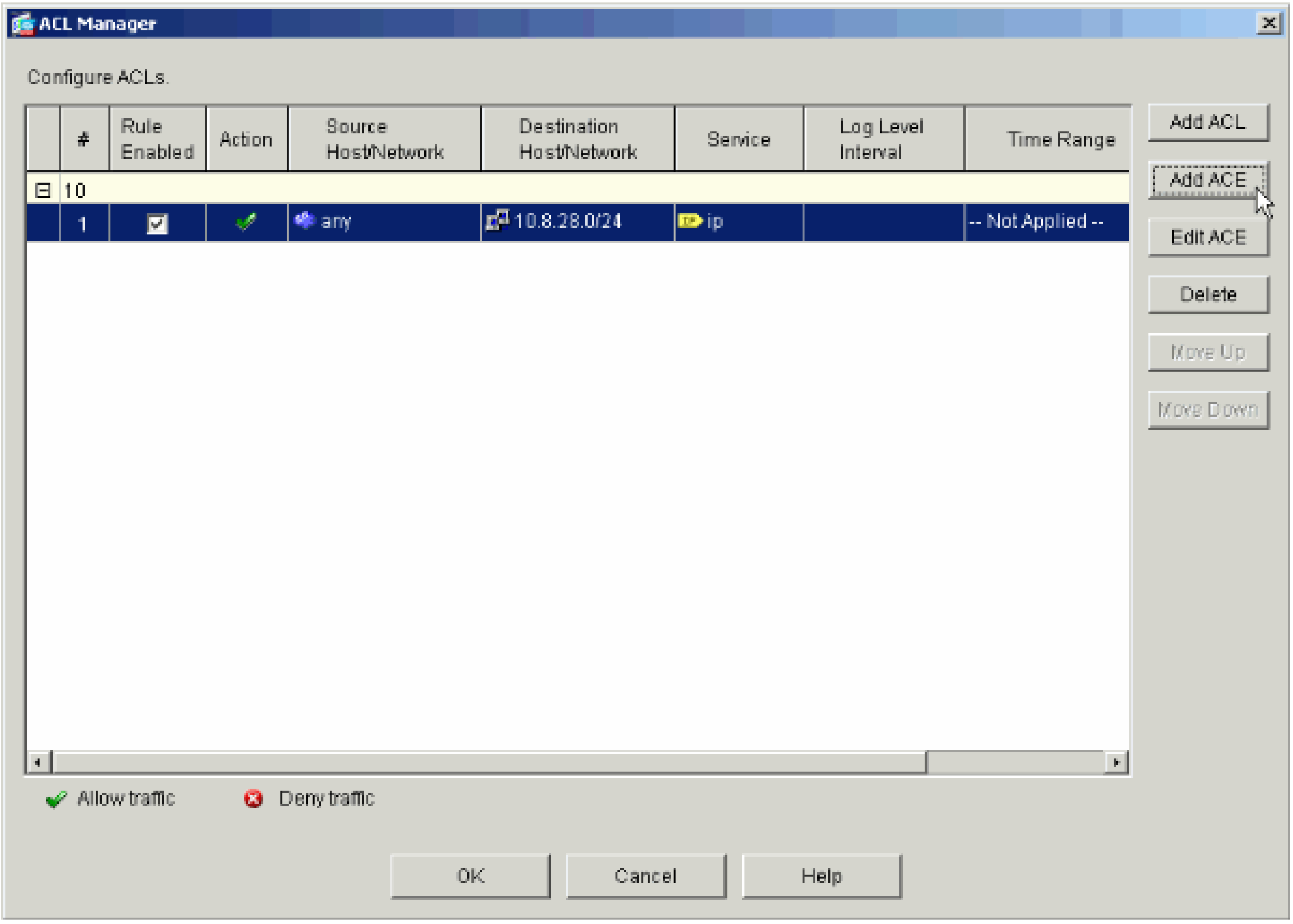
IP Protocol

IP protocol: any

Please enter the description below (optional):

permit IP access from ANY source to the payroll subnet (10.8.28.0 /24)

9. 您剛剛新增的ACE現在出現在清單中。再次選擇**Add ACE**以將任何附加行新增到訪問清單。

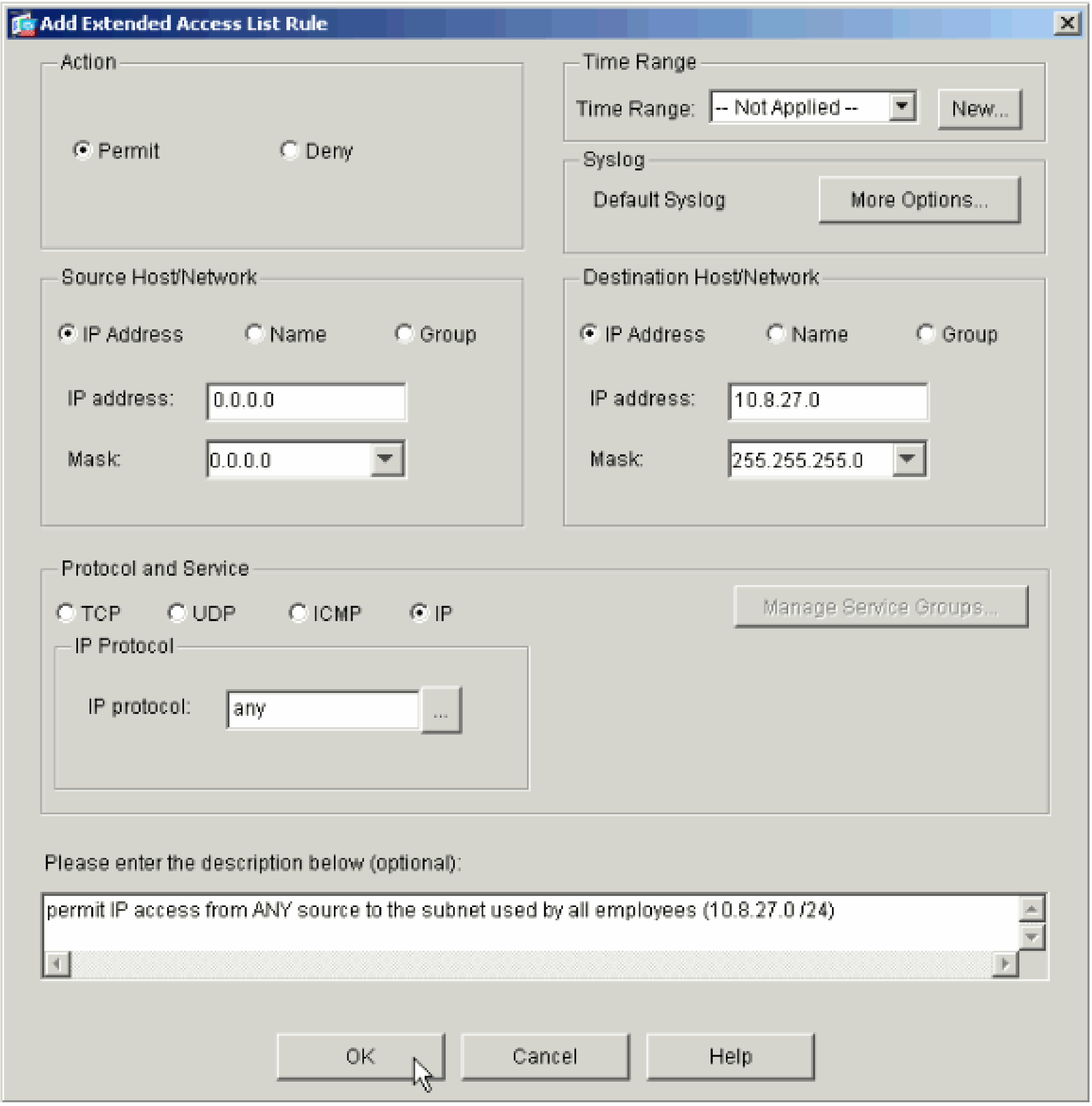


Configure ACLs.

	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range
⊟	10							
	1	☑	✓	any	10.8.28.0/24	ip		-- Not Applied --

✓ Allow traffic ✗ Deny traffic

在本示例中，將第二個ACE新增到ACL 10中，以便允許訪問Intranet子網。



Add Extended Access List Rule

Action: ● Permit ○ Deny

Time Range: -- Not Applied --

Syslog: Default Syslog

Source Host/Network: ● IP Address ○ Name ○ Group

IP address: 0.0.0.0

Mask: 0.0.0.0

Destination Host/Network: ● IP Address ○ Name ○ Group

IP address: 10.8.27.0

Mask: 255.255.255.0

Protocol and Service: ○ TCP ○ UDP ○ ICMP ● IP

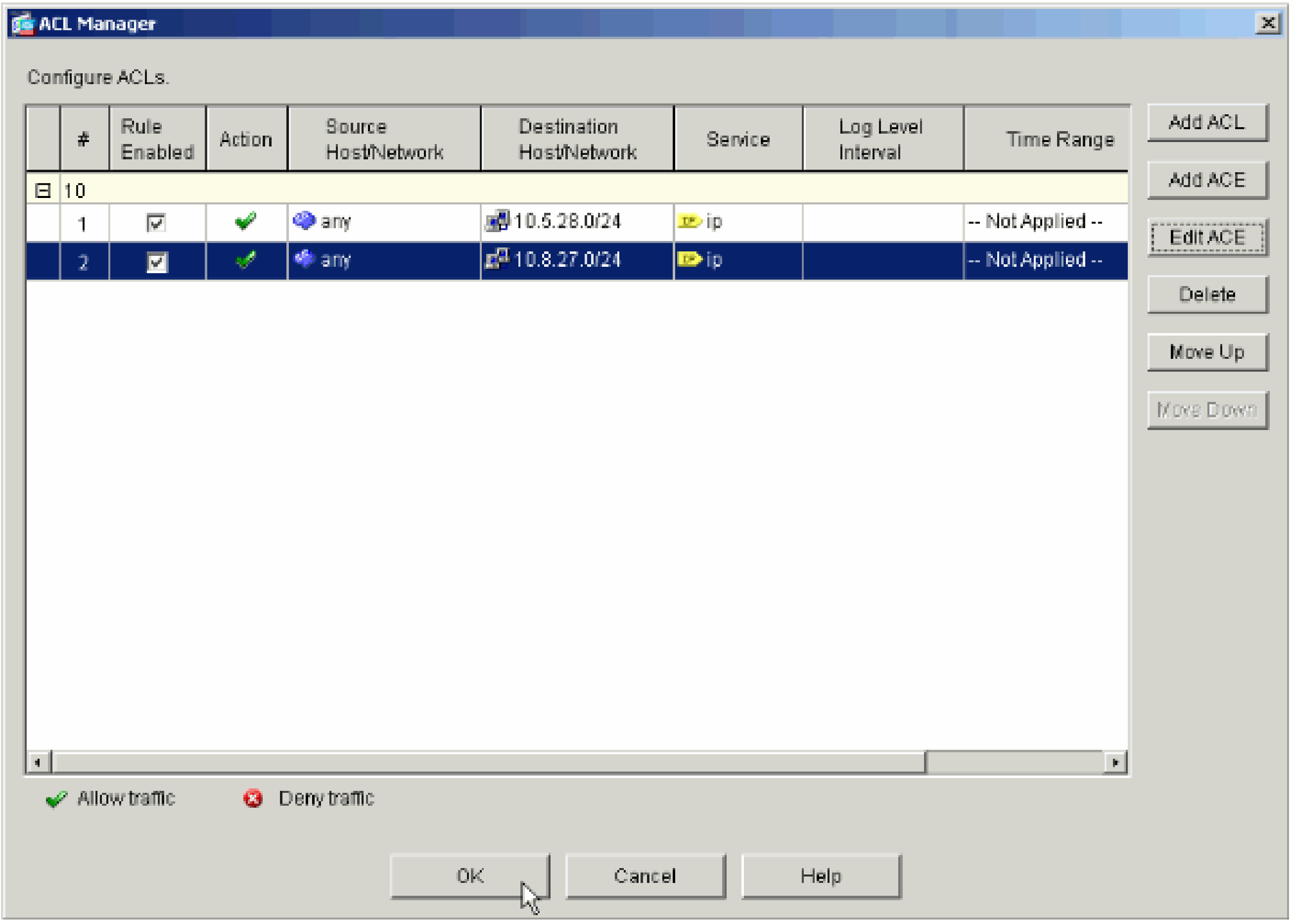
IP Protocol

IP protocol: any

Please enter the description below (optional):

permit IP access from ANY source to the subnet used by all employees (10.8.27.0 /24)

10. 新增ACE後，按一下**OK**。

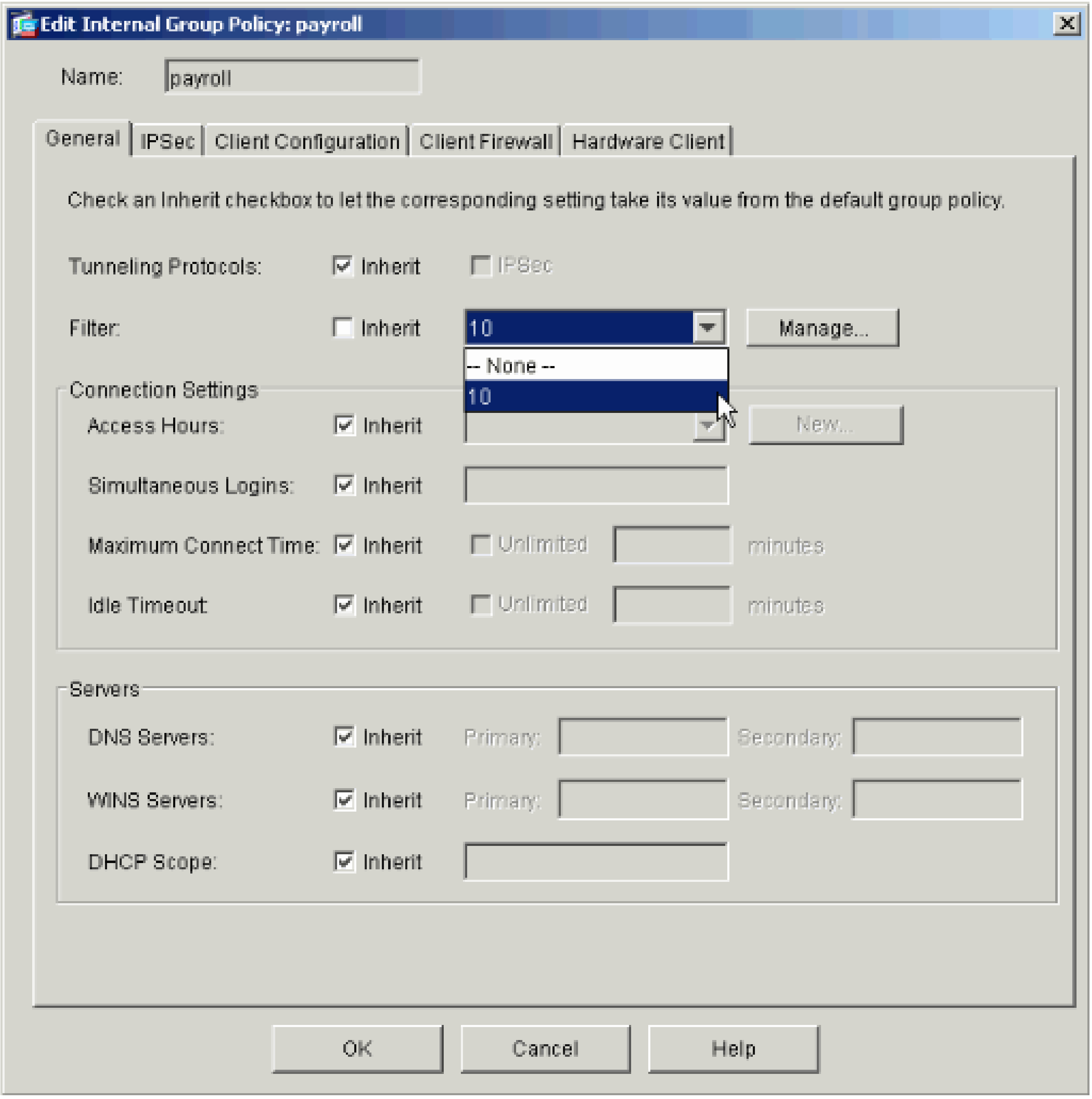


Configure ACLs.

	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range
⊟	10							
	1	☑	✓	any	10.5.28.0/24	ip		-- Not Applied --
	2	☑	✓	any	10.8.27.0/24	ip		-- Not Applied --

✓ Allow traffic ✖ Deny traffic

11. 選擇在最後步驟中定義並填充的ACL作為組策略的過濾器。完成後按一下**OK**。



Edit Internal Group Policy: payroll

Name: payroll

General | IPSec | Client Configuration | Client Firewall | Hardware Client

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

Tunneling Protocols: ☑ Inherit □ IPSec

Filter: □ Inherit 10 Manage...

-- None --

10

Connection Settings

Access Hours: ☑ Inherit New...

Simultaneous Logins: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ Unlimited minutes

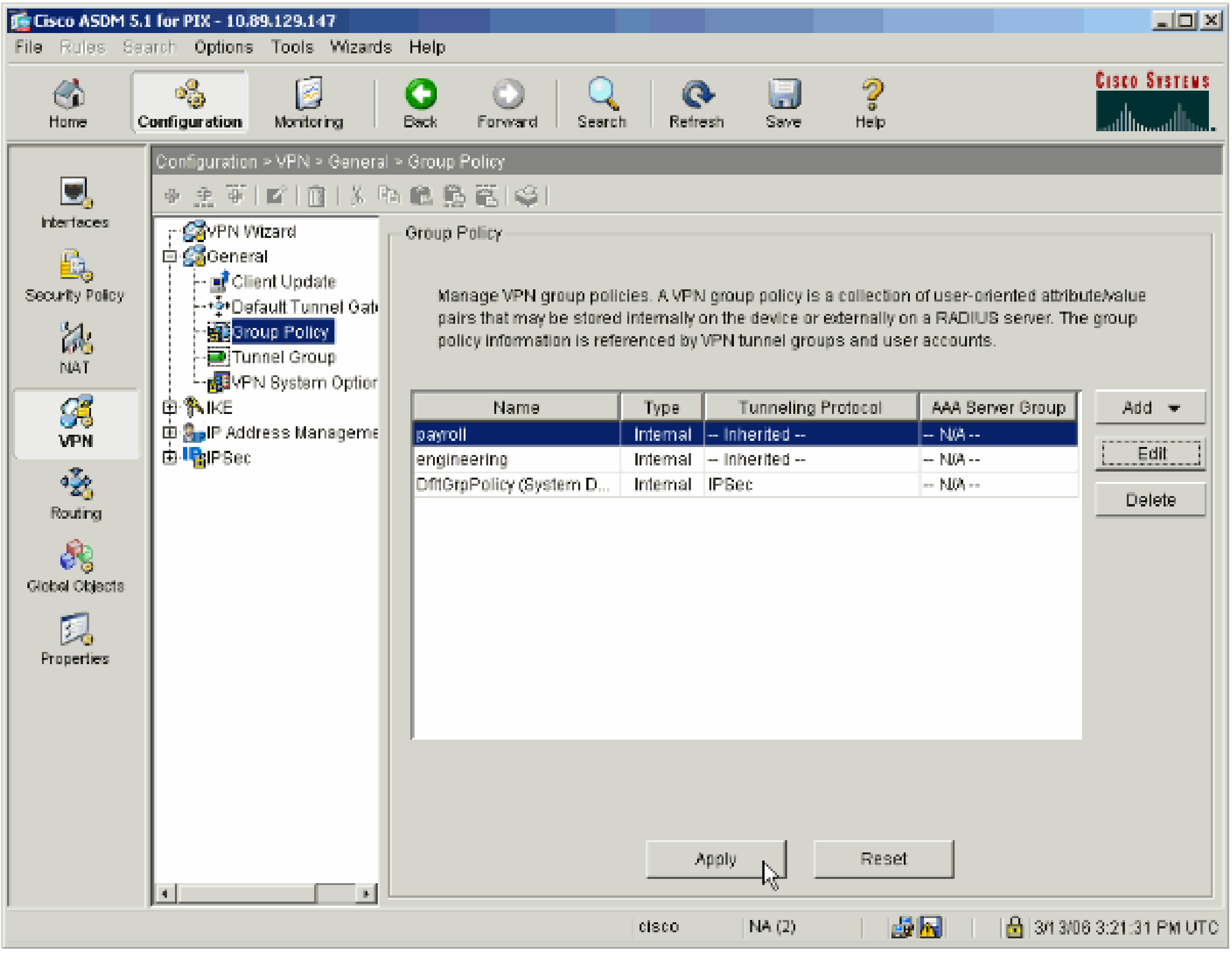
Servers

DNS Servers: ☑ Inherit Primary: Secondary:

WINS Servers: ☑ Inherit Primary: Secondary:

DHCP Scope: ☑ Inherit

12. 按一下**Apply**將更改傳送到PIX。



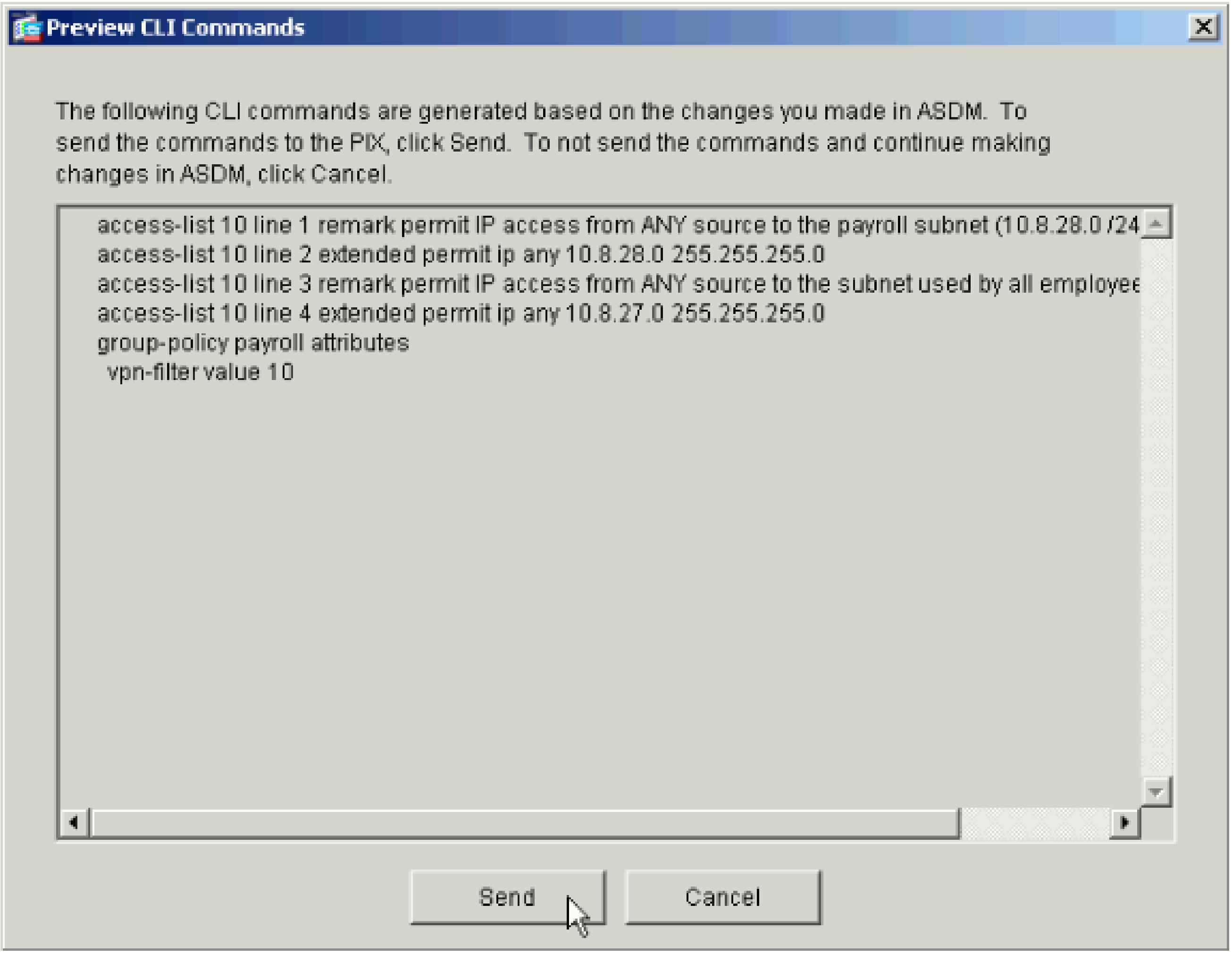
Configuration > VPN > General > Group Policy

Group Policy

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored internally on the device or externally on a RADIUS server. The group policy information is referenced by VPN tunnel groups and user accounts.

Name	Type	Tunneling Protocol	AAA Server Group
payroll	Internal	-- Inherited --	-- N/A --
engineering	Internal	-- Inherited --	-- N/A --
DfltGrpPolicy (System D...	Internal	IPSec	-- N/A --

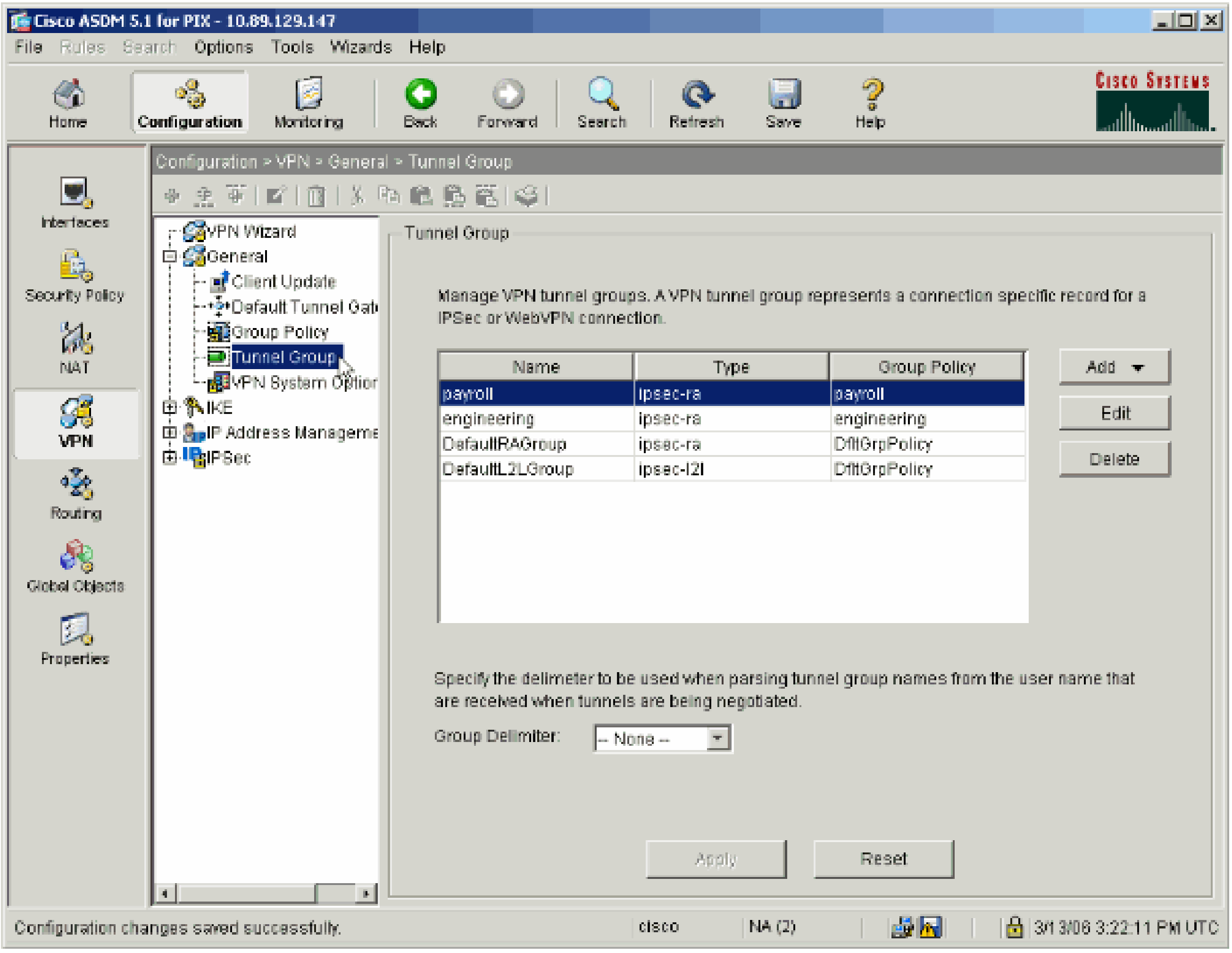
13. 如果在**選項>首選項**下配置了該命令，ASDM會預覽要傳送到PIX的命令。按一下「**Send**」。



The following CLI commands are generated based on the changes you made in ASDM. To send the commands to the PIX, click Send. To not send the commands and continue making changes in ASDM, click Cancel.

```
access-list 10 line 1 remark permit IP access from ANY source to the payroll subnet (10.8.28.0 /24
access-list 10 line 2 extended permit ip any 10.8.28.0 255.255.255.0
access-list 10 line 3 remark permit IP access from ANY source to the subnet used by all employee
access-list 10 line 4 extended permit ip any 10.8.27.0 255.255.255.0
group-policy payroll attributes
 vpn-filter value 10
```

14. 將剛建立或修改的組策略應用到正確的隧道組。按一下左框架中的**Tunnel Group**。



Tunnel Group

Manage VPN tunnel groups. A VPN tunnel group represents a connection specific record for a IPSec or WebVPN connection.

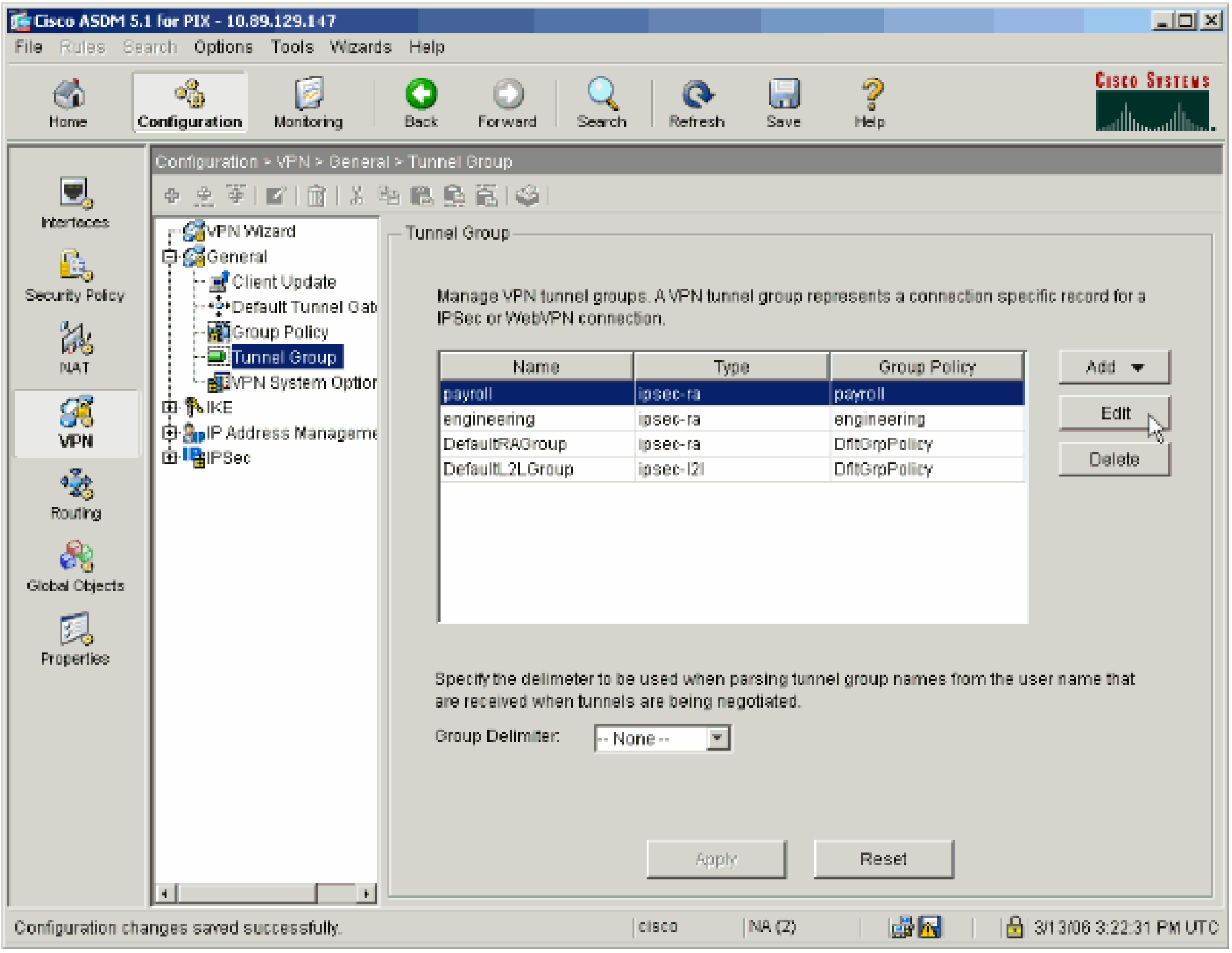
Name	Type	Group Policy
payroll	ipsec-ra	payroll
engineering	ipsec-ra	engineering
DefaultRAGroup	ipsec-ra	DfltGrpPolicy
DefaultL2LGroup	ipsec-l2l	DfltGrpPolicy

Specify the delimeter to be used when parsing tunnel group names from the user name that are received when tunnels are being negotiated.

Group Delimiter: -- None --

Configuration changes saved successfully. cisco NA (2) 3/13/06 3:22:11 PM UTC

15. 選擇要應用組策略的隧道組，然後按一下**Edit**。


Cisco ASDM 5.1 for PIX - 10.89.129.147
File Rules Search Options Tools Wizards Help
Home Configuration Monitoring Back Forward Search Refresh Save Help
Interfaces Security Policy NAT VPN Routing Global Objects Properties
Configuration > VPN > General > Tunnel Group
VPN Wizard
General
Client Update
Default Tunnel Gat
Group Policy
Tunnel Group
VPN System Optior
IKE
IP Address Manageme
IPSec
Add
Edit
Delete
Apply
Reset

Tunnel Group

Manage VPN tunnel groups. A VPN tunnel group represents a connection specific record for a IPSec or WebVPN connection.

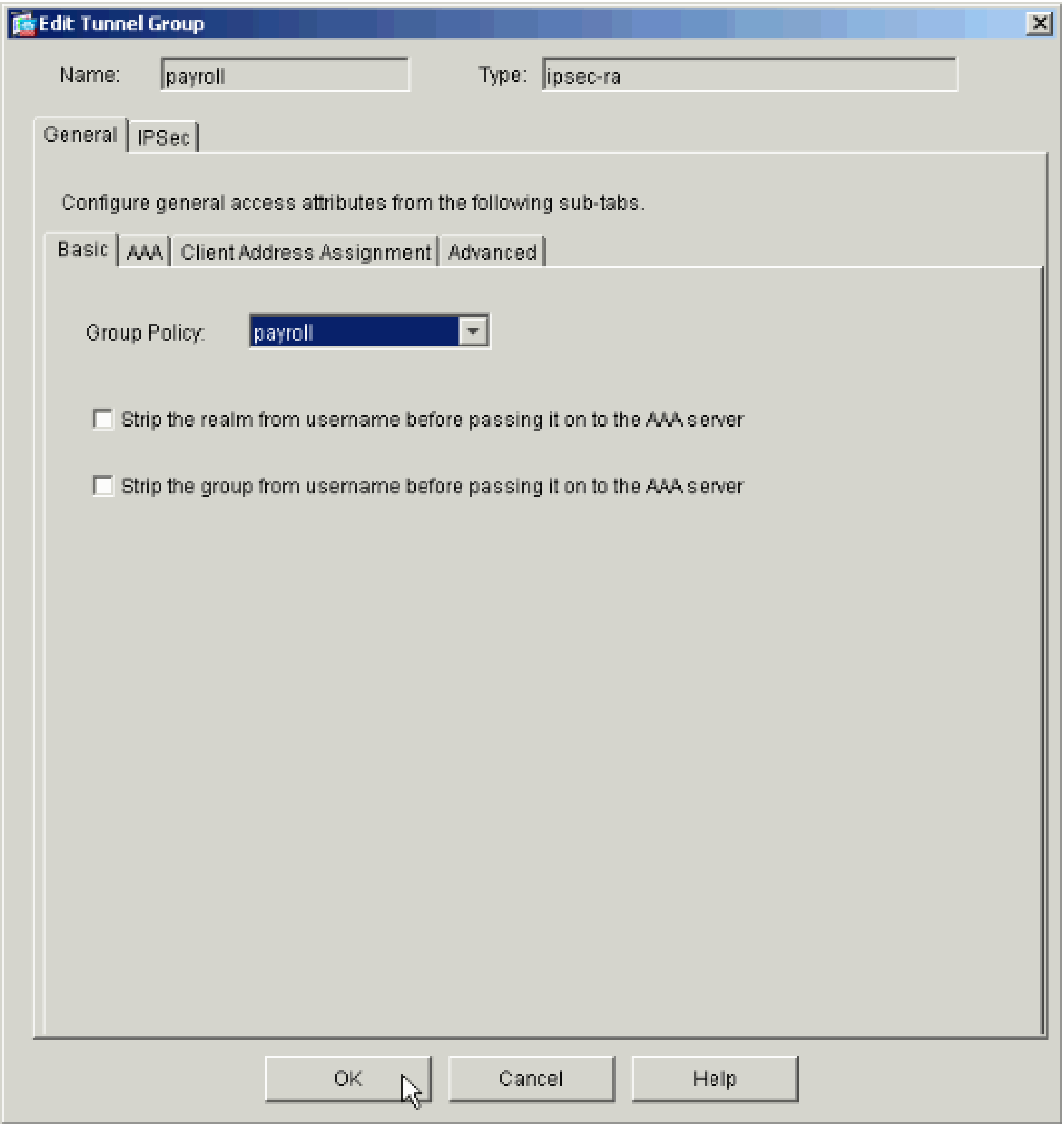
Name	Type	Group Policy
payroll	ipsec-ra	payroll
engineering	ipsec-ra	engineering
DefaultRAGroup	ipsec-ra	DfltGrpPolicy
DefaultL2LGroup	ipsec-l2l	DfltGrpPolicy

Specify the delimeter to be used when parsing tunnel group names from the user name that are received when tunnels are being negotiated.

Group Delimiter: -- None --

Configuration changes saved successfully. cisco NA (2) 3/13/06 3:22:31 PM UTC

16. 如果您的組策略是自動建立的（請參閱步驟2），請確認在下拉框中選擇了剛配置的組策略。如果未自動配置組策略，請從下拉框中選擇它。完成後按一下**OK**。



Name: payroll

Type: ipsec-ra

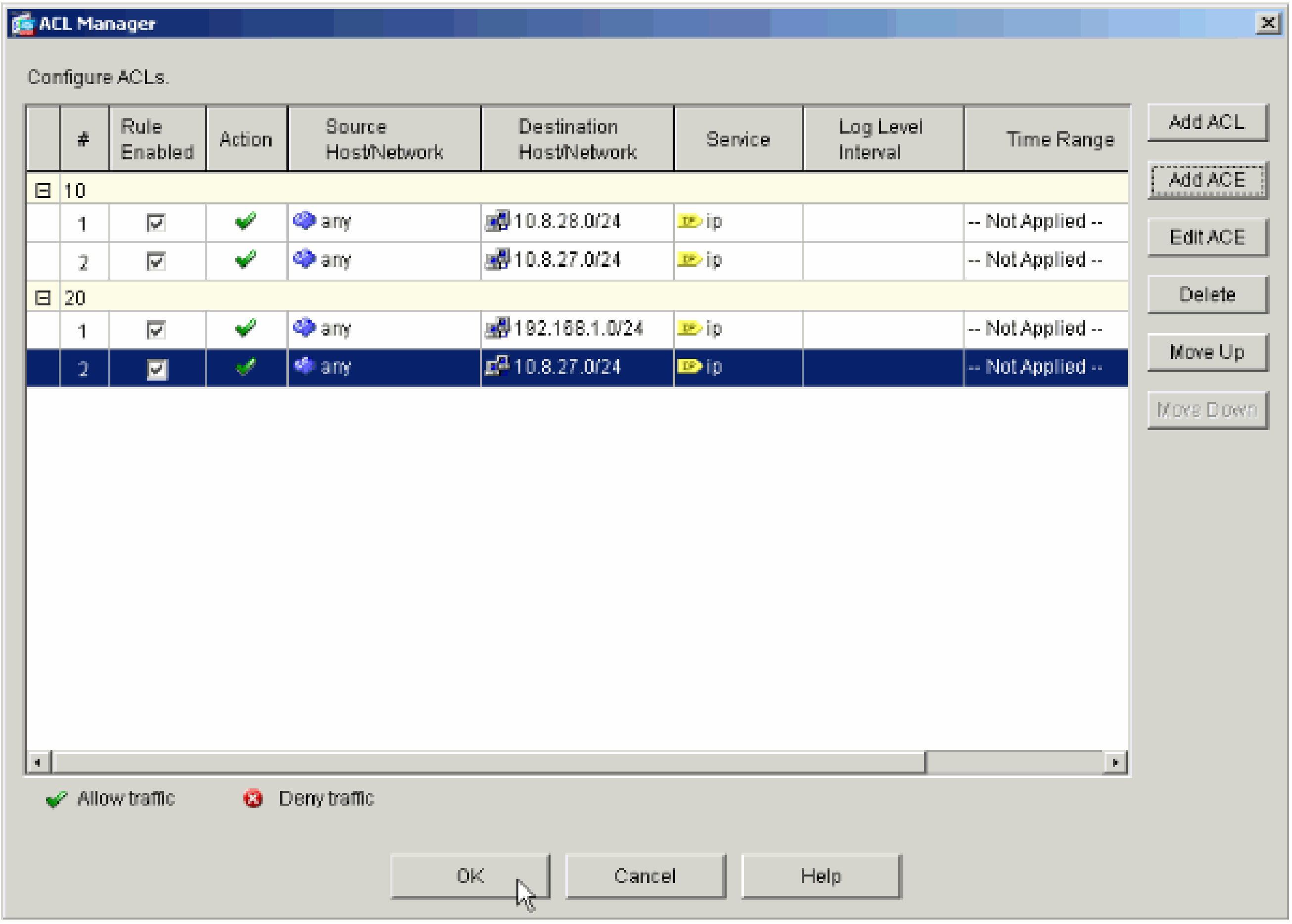
Configure general access attributes from the following sub-tabs.

Group Policy: payroll

□ Strip the realm from username before passing it on to the AAA server

□ Strip the group from username before passing it on to the AAA server

17. 按一下**Apply**，如果出現提示，請按一下**Send**將更改新增到PIX配置。如果已選擇組策略，您可能會收到一則消息「未進行任何更改」。 按一下「**OK**」（確定）。
18. 對於要新增限制的任何其他隧道組，重複步驟2到17。在此配置示例中，還必須限制工程師的訪問。雖然程式相同，但也有幾個視窗存在顯著差異：新存取清單

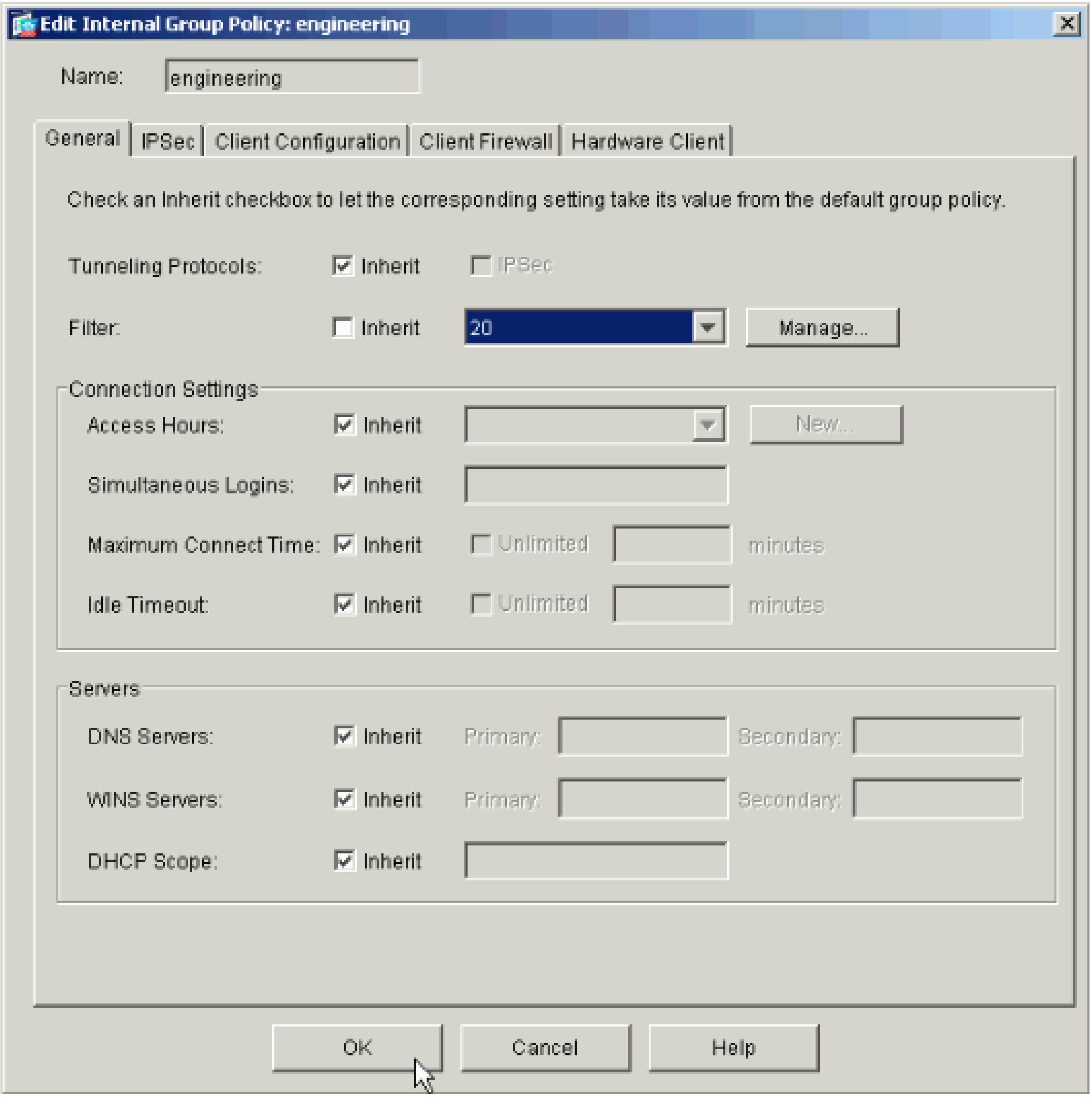


Configure ACLs.

	#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Service	Log Level Interval	Time Range
⊟	10							
	1	☑	✓	any	10.8.28.0/24	ip		-- Not Applied --
	2	☑	✓	any	10.8.27.0/24	ip		-- Not Applied --
⊟	20							
	1	☑	✓	any	192.168.1.0/24	ip		-- Not Applied --
	2	☑	✓	any	10.8.27.0/24	ip		-- Not Applied --

✓ Allow traffic ✖ Deny traffic

選擇**Access List 20**作為Engineering Group Policy中的篩選器。



Edit Internal Group Policy: engineering

Name: engineering

General | IPSec | Client Configuration | Client Firewall | Hardware Client

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

Tunneling Protocols: ☑ Inherit □ IPSec

Filter: □ Inherit 20 Manage...

Connection Settings

Access Hours: ☑ Inherit New...

Simultaneous Logins: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ Unlimited minutes

Servers

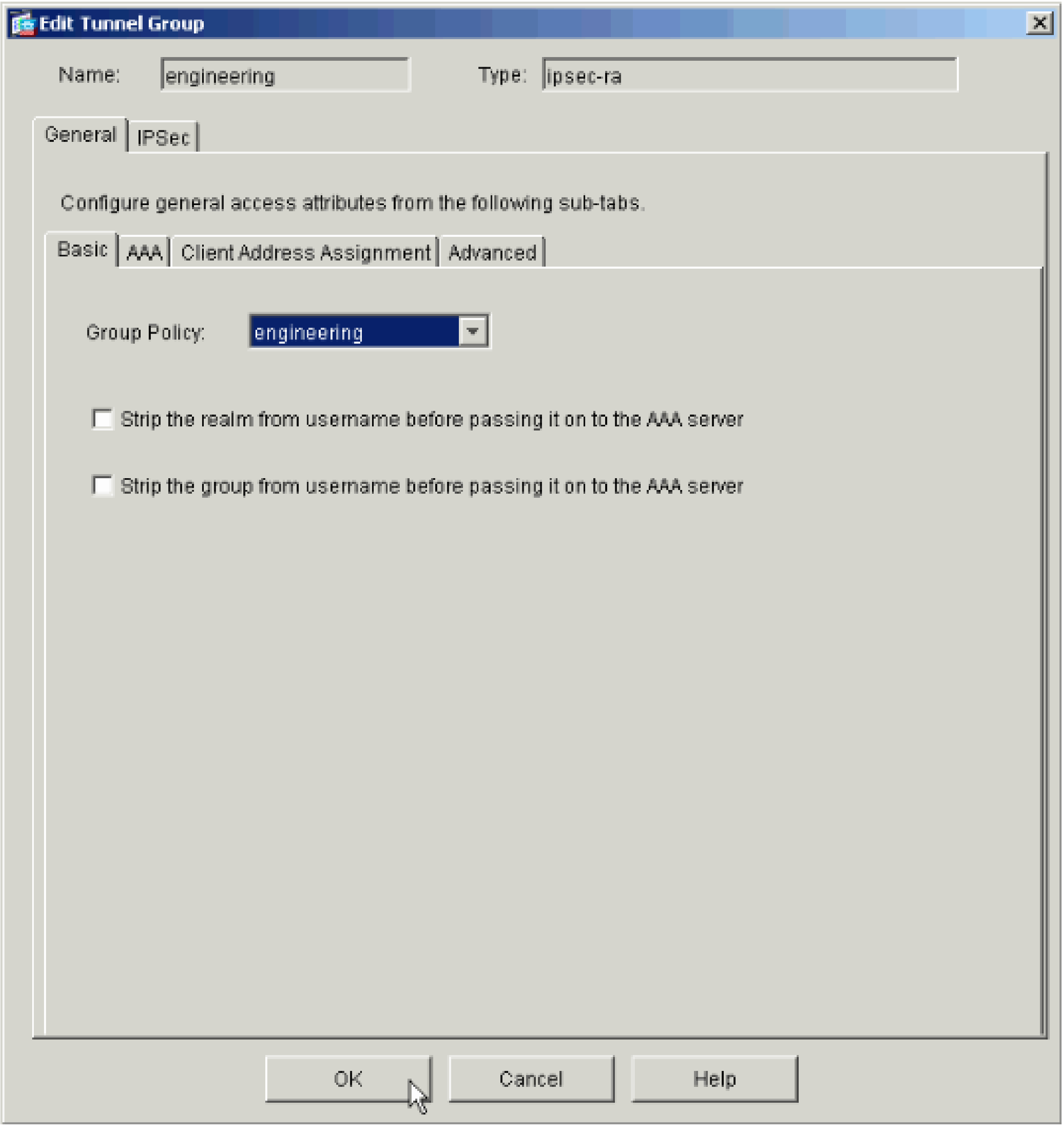
DNS Servers: ☑ Inherit Primary: Secondary:

WINS Servers: ☑ Inherit Primary: Secondary:

DHCP Scope: ☑ Inherit

OK Cancel Help

驗證是否已為工程隧道組設定工程組策略。



Name: engineering

Type: ipsec-ra

Edit Tunnel Group
General
IPSec
Configure general access attributes from the following sub-tabs.
Basic
AAA
Client Address Assignment
Advanced

Group Policy: engineering

□ Strip the realm from username before passing it on to the AAA server

□ Strip the group from username before passing it on to the AAA server

通過CLI配置訪問

完成以下步驟，使用CLI配置安全裝置：

注意：由於空間原因，此輸出中顯示的某些命令會下降到第二行。

1. 建立兩個不同的訪問控制清單（15和20），在使用者連線到遠端訪問VPN時應用這些清單。稍後將在配置中呼叫此訪問清單。
   ```
   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. 建立兩個不同的VPN地址池。為Payroll和Engineering遠端使用者分別建立一個。

```
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. 為工資單建立僅在連線時應用的策略。

```
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. 此步驟與步驟3相同，只是適用於Engineering組。

```
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. 建立本地使用者並將您剛剛建立的屬性分配給這些使用者，以限制其對資源的訪問。

```
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. 建立包含工資單使用者的連線策略的隧道組。

```
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. 建立包含Engineering使用者的連線策略的隧道組。

```
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
```

輸入配置後，可以在配置中看到此突出顯示的區域：

裝置名稱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
```

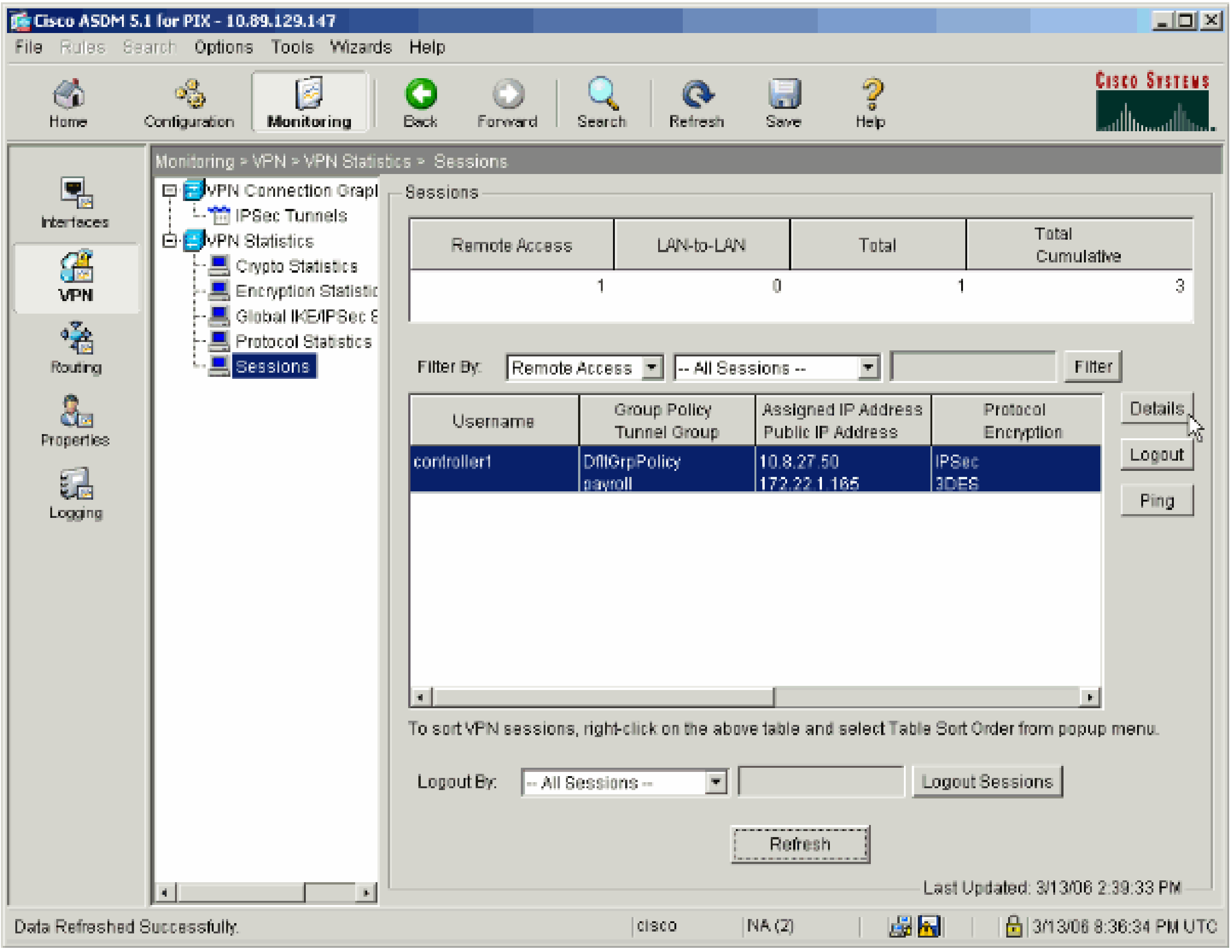
```
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
group-policy Payroll internal
group-policy Payroll attributes
 dns-server value 10.8.27.10
 vpn-filter 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)#
```

驗證

使用ASDM的監控功能驗證您的配置：

1. 選擇**Monitoring > VPN > VPN Statistics > Sessions**。您會看到PIX上的活動VPN會話。選擇您感興趣的會話並按一下**Details**。



Monitoring > VPN > VPN Statistics > Sessions

Sessions

Remote Access	LAN-to-LAN	Total	Total Cumulative
1	0	1	3

Filter By: Remote Access | -- All Sessions --

Username	Group Policy Tunnel Group	Assigned IP Address Public IP Address	Protocol Encryption
controller1	DfltGrpPolicy payroll	10.8.27.50 172.22.1.165	IPSec 3DES

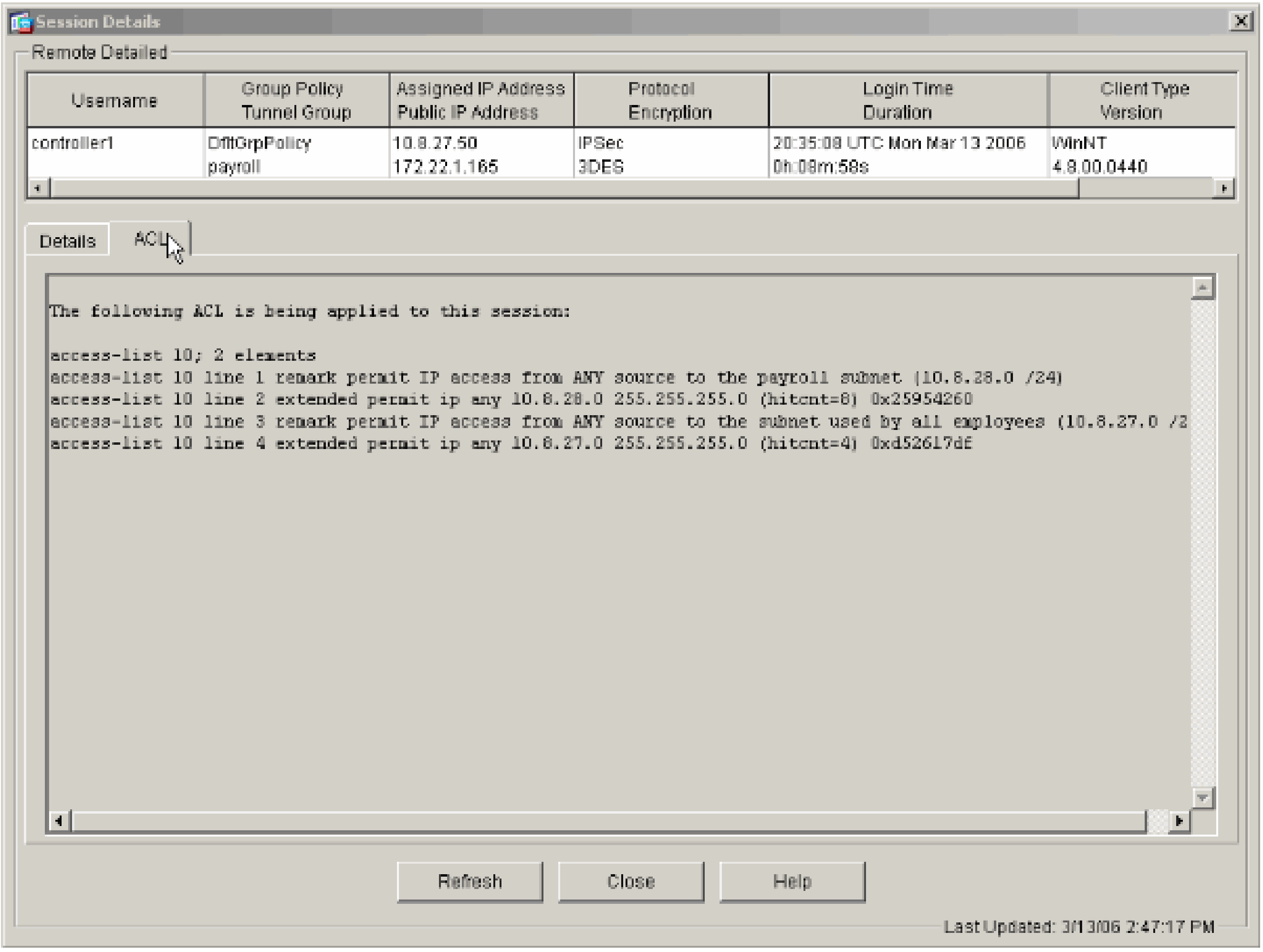
To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions --

Last Updated: 3/13/06 2:39:33 PM

Data Refreshed Successfully. | cisco | NA (2) | 3/13/06 8:36:34 PM UTC

2. 選擇ACL頁籤。ACL `hitcnts`會反映從使用者端流經通道到允許網路的流量。



Username	Group Policy Tunnel Group	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Client Type Version
controller1	DfltGrpPolicy payroll	10.8.27.50 172.22.1.165	IPSec 3DES	20:35:08 UTC Mon Mar 13 2006 0h:08m:58s	WinNT 4.8.00.0440

```
The following ACL is being applied to this session:

access-list 10; 2 elements
access-list 10 line 1 remark permit IP access from ANY source to the payroll subnet (10.8.28.0 /24)
access-list 10 line 2 extended permit ip any 10.8.28.0 255.255.255.0 (hitcnt=8) 0x25954260
access-list 10 line 3 remark permit IP access from ANY source to the subnet used by all employees (10.8.27.0 /2
access-list 10 line 4 extended permit ip any 10.8.27.0 255.255.255.0 (hitcnt=4) 0xd52617df
```

Last Updated: 3/13/06 2:47:17 PM

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 使用ASDM將Cisco ASA 5500系列自適應安全裝置ASA用作遠端VPN伺服器配置示例
- Cisco PIX 500系列安全裝置配置示例和技術說明
- Cisco ASA 5500系列自適應安全裝置配置示例和技術說明
- Cisco VPN客戶端配置示例和技術說明
- 技術支援與文件 - Cisco Systems