

# PIX/ASA 7.x ASDM : リモートアクセスVPNユーザのネットワークアクセスの制限

## 内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[ネットワーク図](#)

[表記法](#)

[ASDM を使用したアクセス設定](#)

[CLI を使用したアクセス設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## はじめに

このドキュメントでは、Cisco Adaptive Security Device Manager ( ASDM ) を使用して、PIX セキュリティ アプライアンスまたは適応型セキュリティ アプライアンス ( ASA ) の内側にアクセスできる内部ネットワークのリモート アクセス VPN ユーザを制限するための設定例を紹介します。次の場合にユーザにアクセスさせるネットワークのエリアだけにリモート アクセス VPN ユーザを制限できます。

1. アクセス リストを作成します。
2. グループ ポリシーと関連付けます。
3. それらのグループ ポリシーをトンネル グループと関連付けます。

VPN コンセントレータで VPN ユーザのアクセスをブロックする方法は、『[フィルタおよび RADIUS フィルタの割り当てでブロックするための Cisco VPN 3000 コンセントレータの設定](#)』を参照してください。

## 前提条件

### 要件

この設定を行う前に、次の要件が満たされていることを確認します。

- ASDM を使って PIX を設定できること

注：PIXをASDMで設定できるようにするには、『[ASDMでのHTTPSアクセスの許可](#)』を参照してください。

- 問題のない既知のリモート アクセス VPN が少なくとも 1 つ設定されていること

注：設定されていない場合は、『[ASDMを使用したリモートVPNサーバとしてのASAの設定例](#)』で、1つの適切なリモートアクセスVPN設定を設定する方法を参照してください。

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン 7.1(1) が稼働している Cisco Secure PIX 500 シリーズ セキュリティ アプライアンス

注：PIX 501および506Eセキュリティアプライアンスでは、バージョン7.xはサポートされていません。

- Cisco Adaptive Security Device Manager バージョン 5.1(1)

注：ASDMはPIXまたはASA 7.xでのみ使用できます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

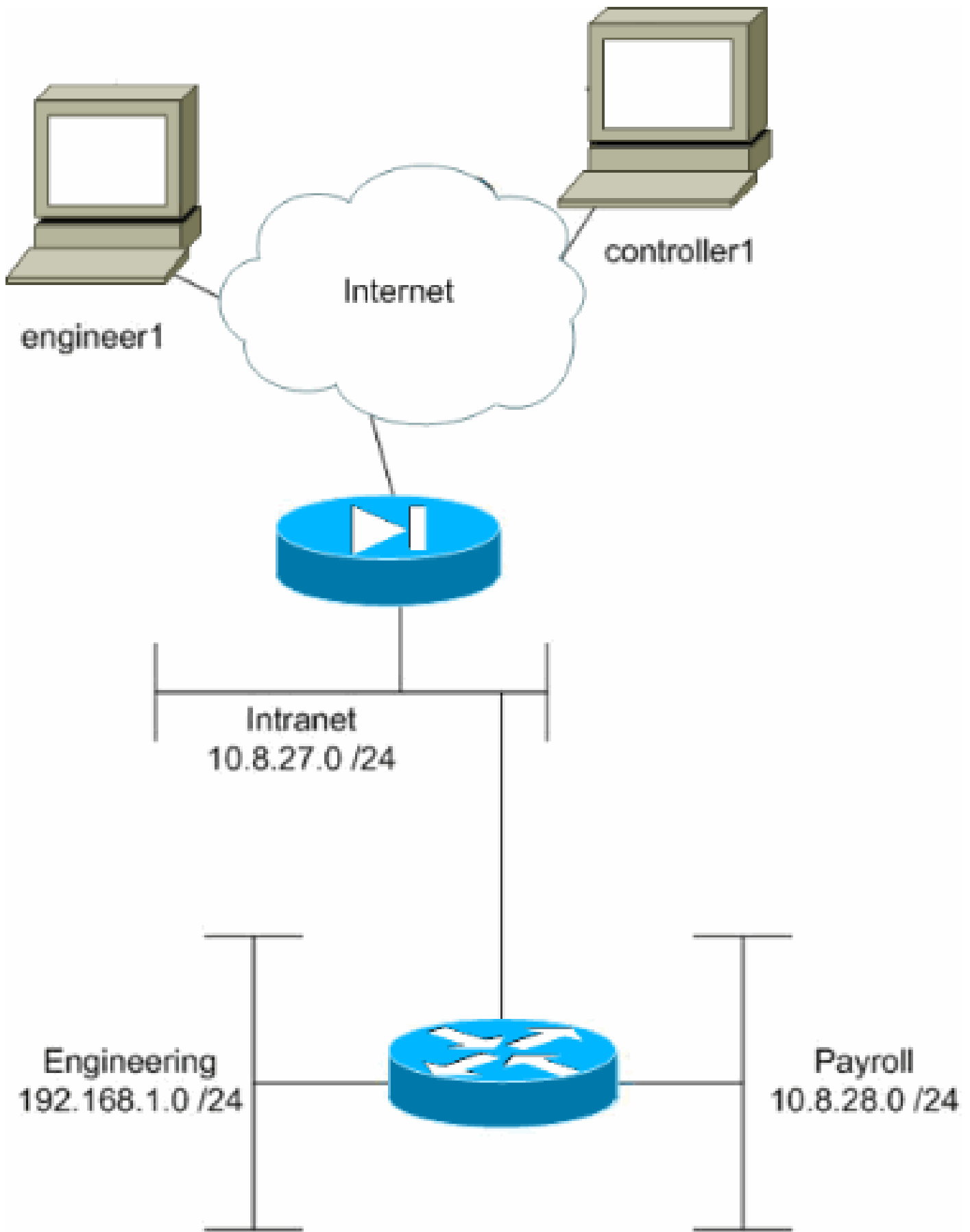
## 関連製品

この設定は、次のバージョンのハードウェアとソフトウェアにも使用できます。

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス バージョン 7.1(1)

## ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



この設定例では、3つのサブネットで構成された小企業のネットワークを取り上げます。次の図は、トポロジを示しています。3つのサブネットは、イントラネット、技術部、経理部です。この設定例の目的は、経理部の担当者がイントラネットと経理部サブネットにリモートアクセスで

きるように許可し、技術部サブネットへのアクセスを防止することです。同様に、エンジニアはイントラネットと技術部サブネットにリモート アクセスできるようにする一方で、経理部サブネットにはアクセスできないように設定します。この設定例の経理部ユーザは「controller1」で、技術部ユーザは「engineer1」です。

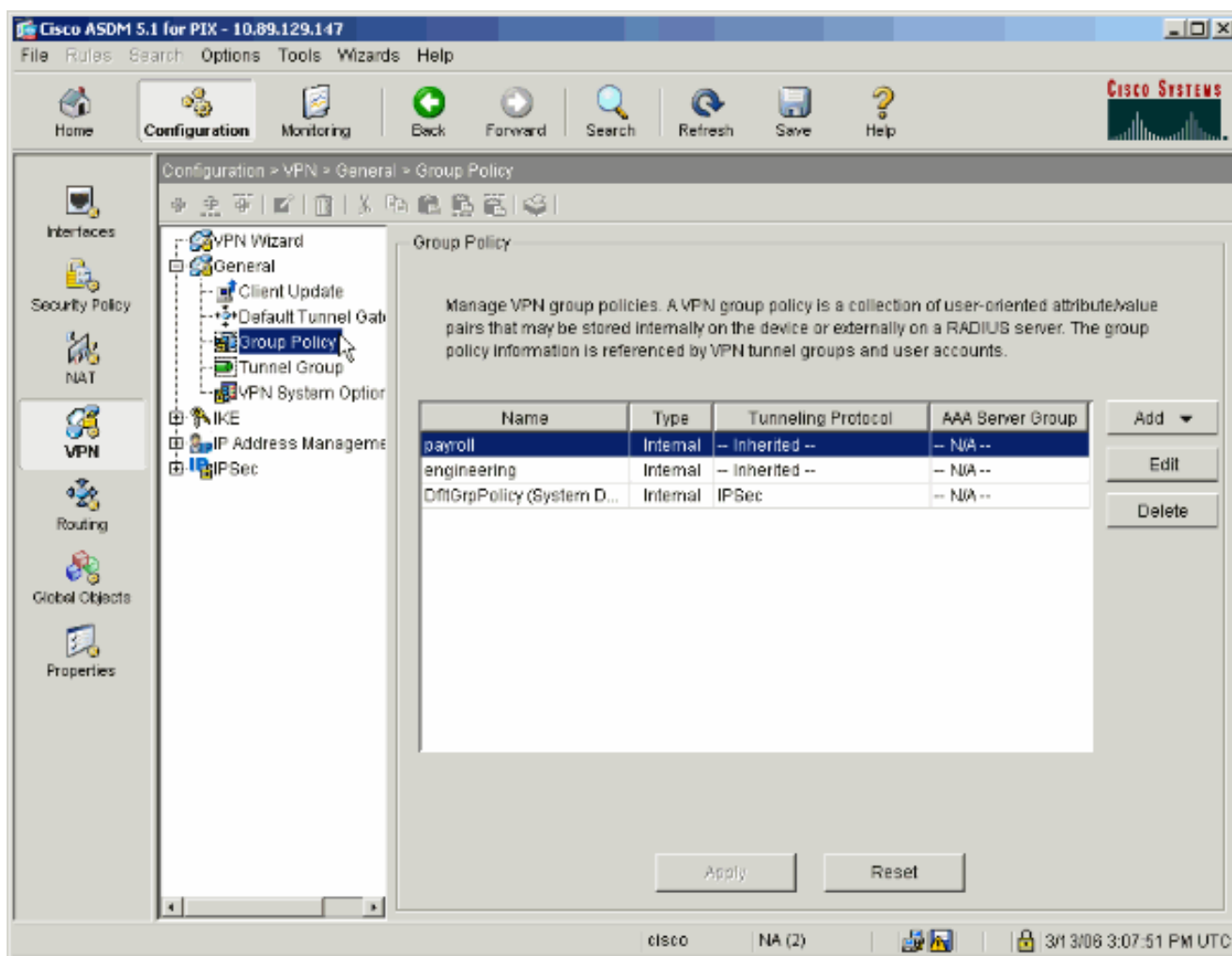
## 表記法

ドキュメント表記の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

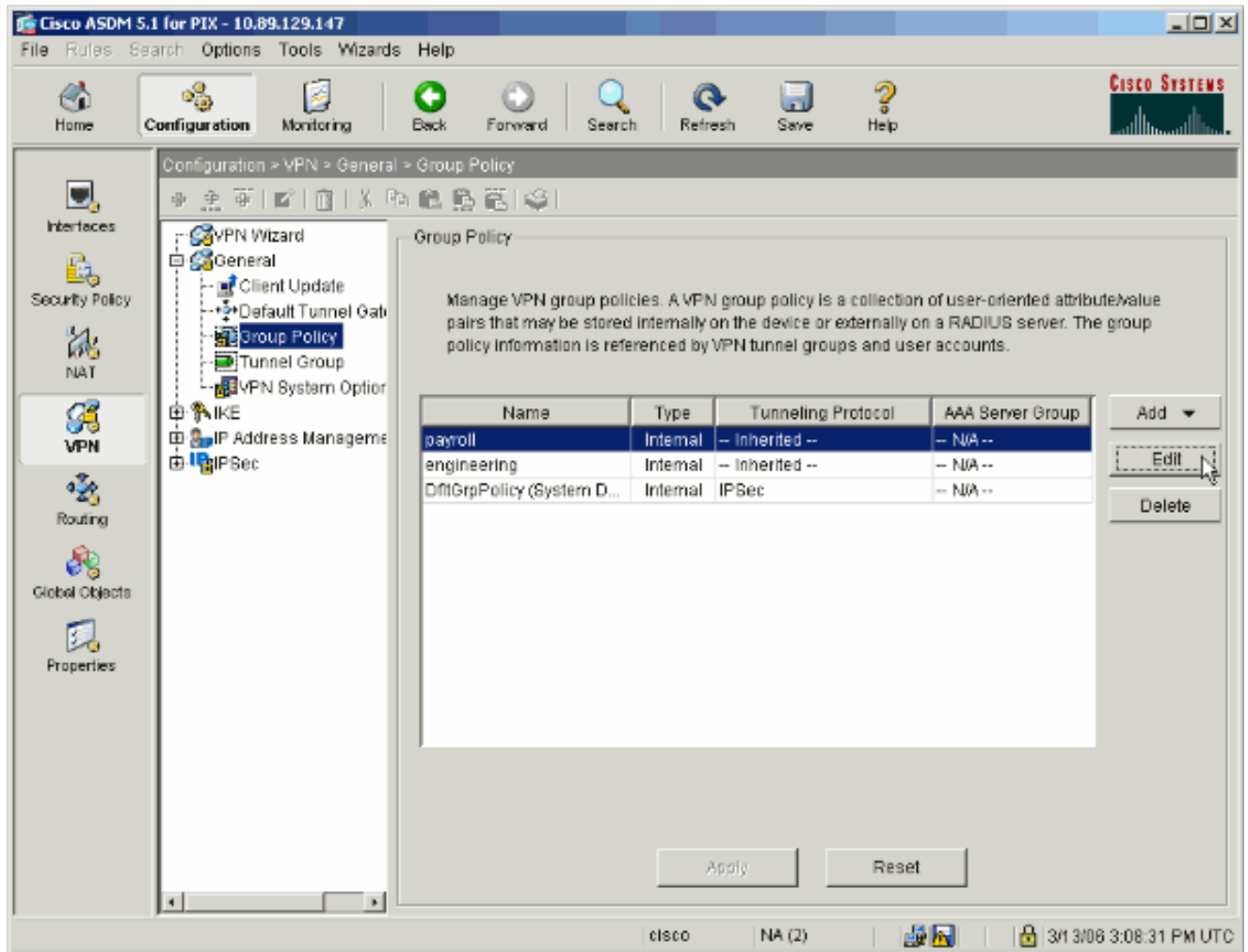
## ASDM を使用したアクセス設定

ASDM を使用して PIX セキュリティ アプライアンスを設定するには、次の手順を実行します。

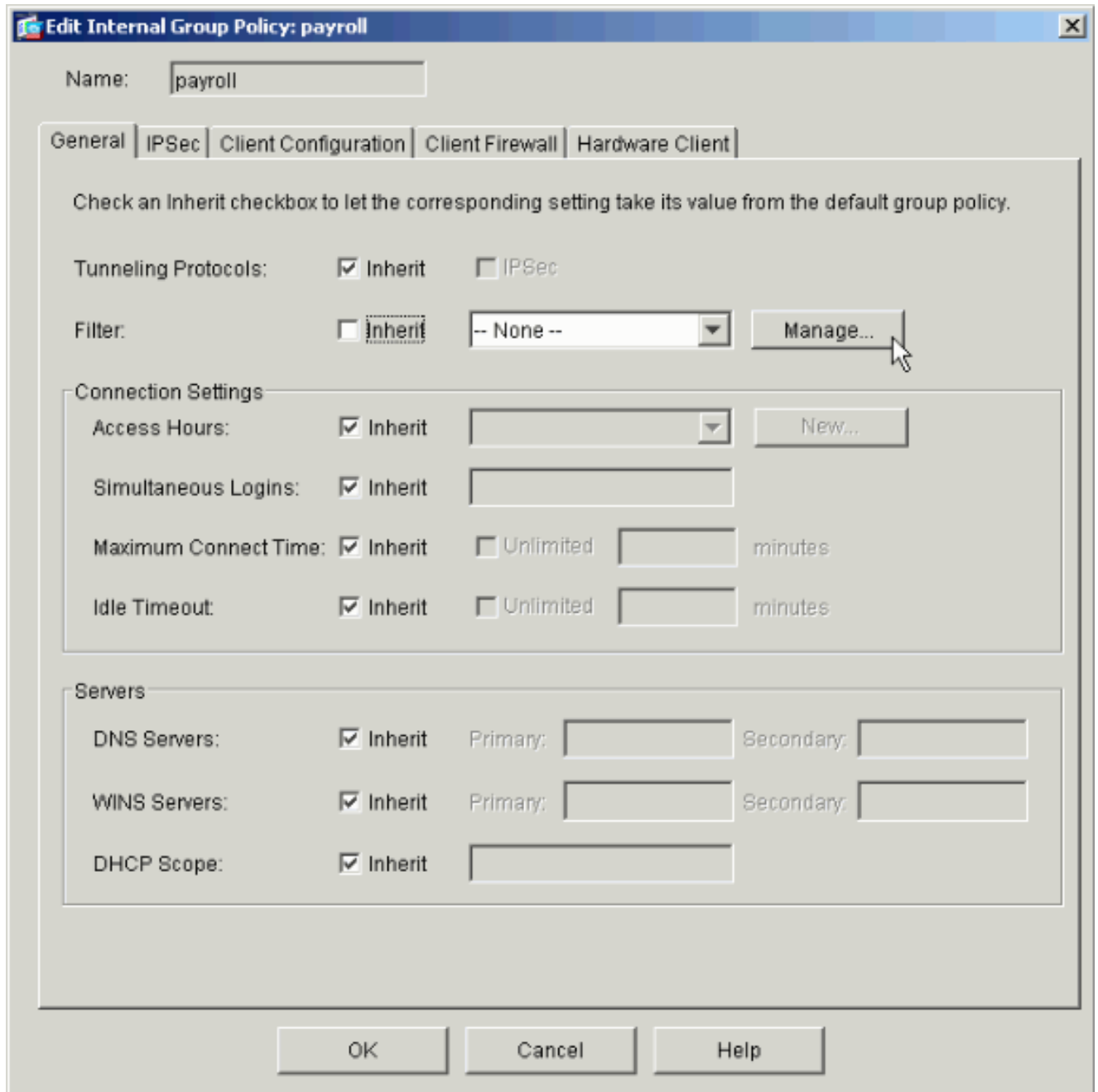
1. [Configuration] > [VPN] > [General] > [Group Policy] の順に選択します。



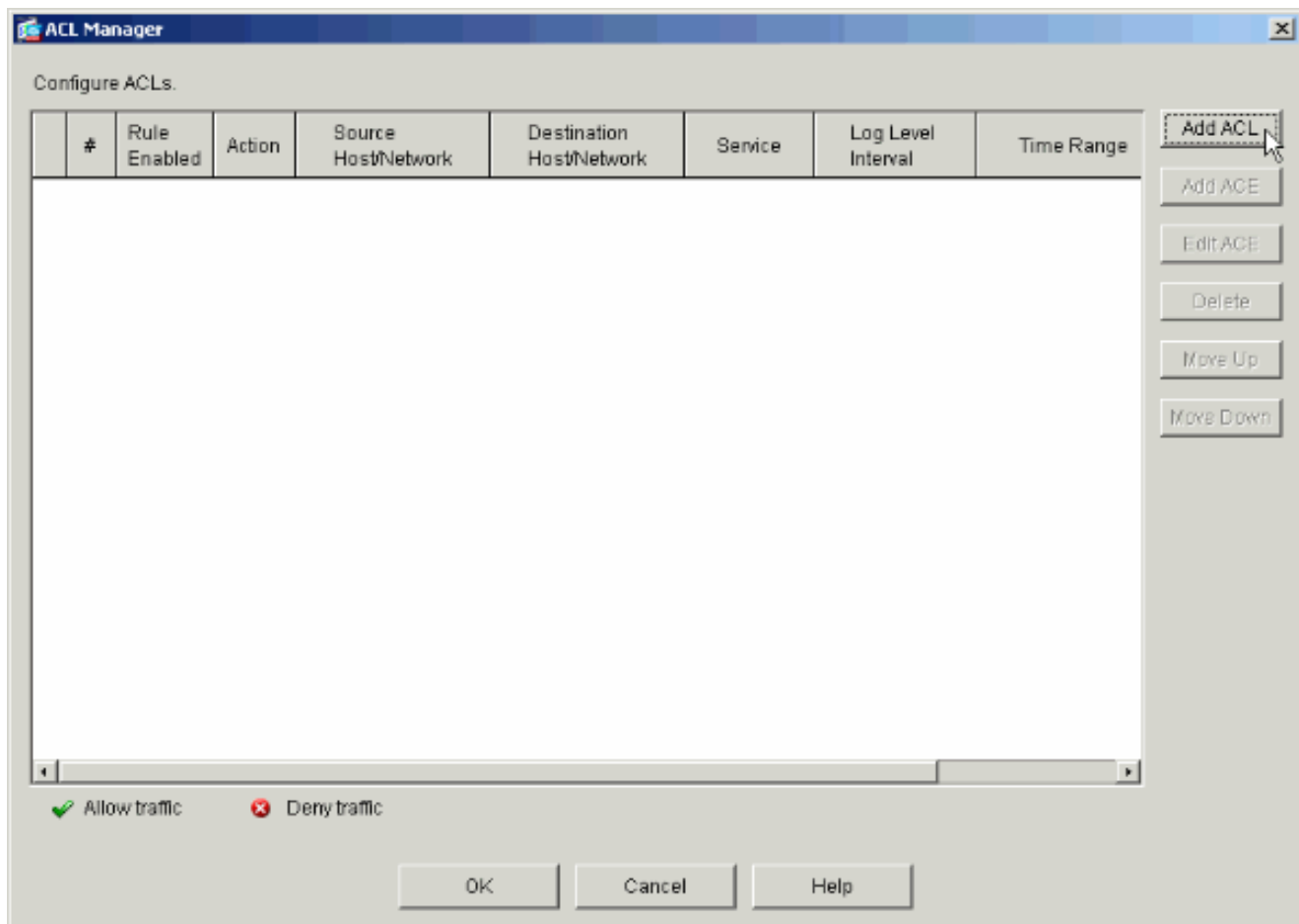
2. PIX でトンネルグループを設定した際の手順によっては、制限したいユーザが属するトンネルグループのグループポリシーがすでに存在している場合があります。適切なグループポリシーがすでに存在する場合は、[Edit] をクリックします。それ以外の場合は、[Add] をクリックして、[Internal Group Policy] を選択します。



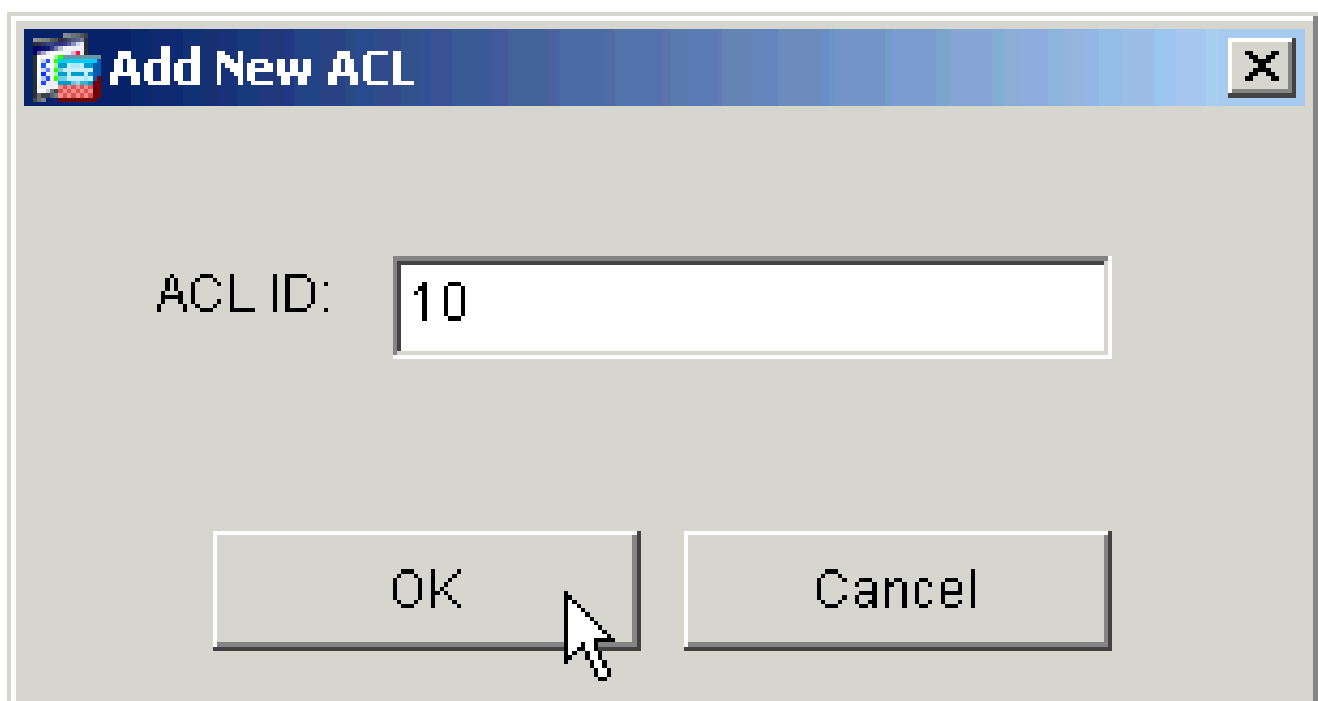
- 必要に応じて、開いたウィンドウの上部にあるグループポリシー名を入力または変更します。
- [General] タブで、[Filter] の横にある [Inherit] ボックスをオフにしたら、[Manage] をクリックします。



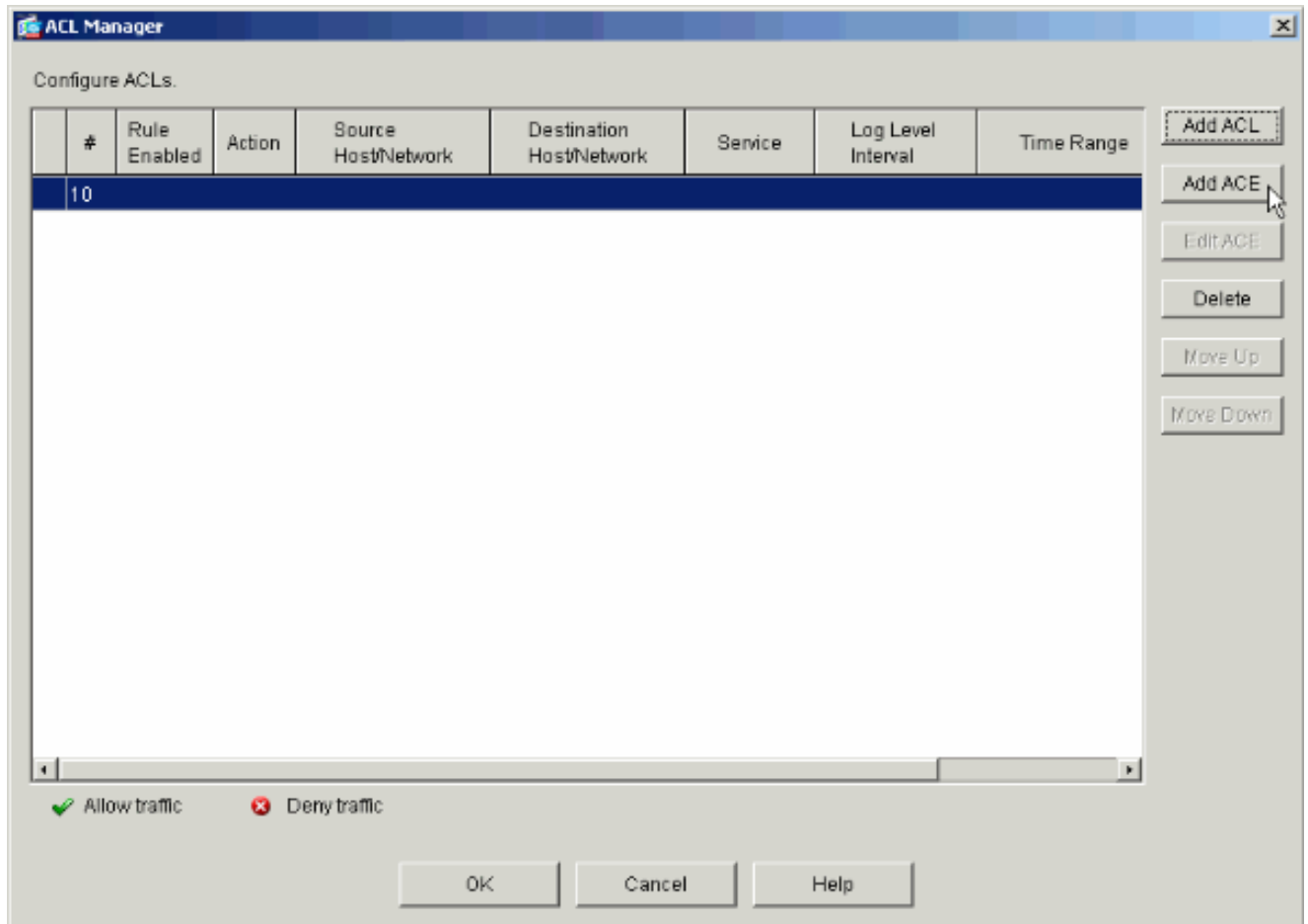
5. [Add ACL] をクリックして、表示された [ACL Manager] ウィンドウでアクセス リストを新規作成します。



6. 新しいアクセス リストの番号を入力し、[OK] をクリックします。



7. 左側で新しい ACL を選択したら、[Add ACE] をクリックしてリストに新しいアクセス コントロール エントリを作成します。



## 8. 追加するアクセスコントロール エントリ ( ACE ) を定義します。

この例では、ACL 10 の最初の ACE で経理部サブネットにアクセスできる IP アドレスを無制限に設定します。

注：デフォルトでは、ASDMはプロトコルとしてTCPのみを選択します。すべての IP からのフルアクセスを許可または拒否するか選択します。完了したら、[OK] をクリックします。



**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

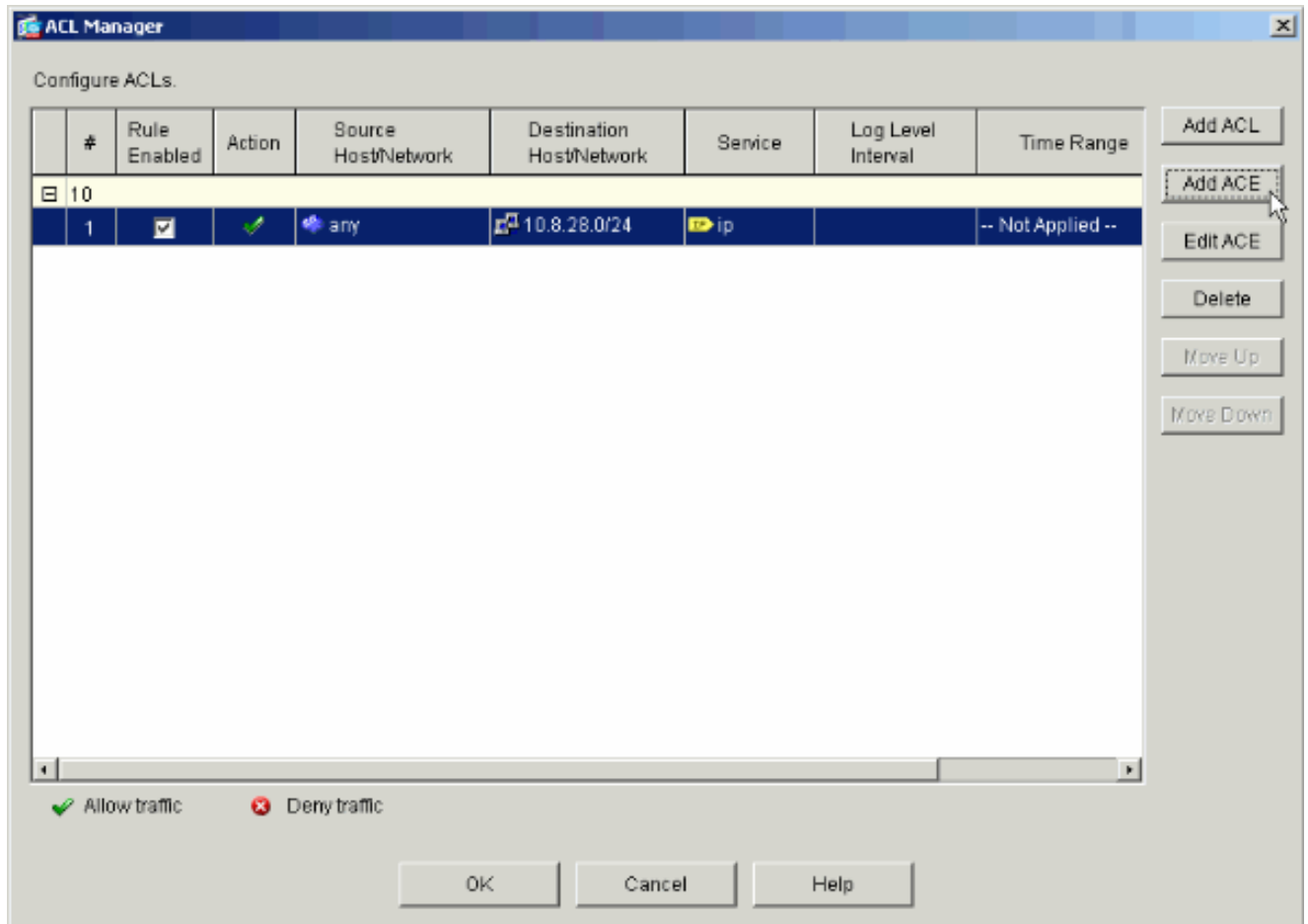
**IP Protocol**

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. 追加した ACE がリスト内に表示されます。再び [Add ACE] を選択し、アクセス リストに必要なだけ行を追加します。



この例では、イントラネット サブネットへのアクセスを許可するための ACL 10 を ACE に追加しています。

**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: 10.8.27.0

Mask: 255.255.255.0

**Protocol and Service**

TCP  UDP  ICMP  IP

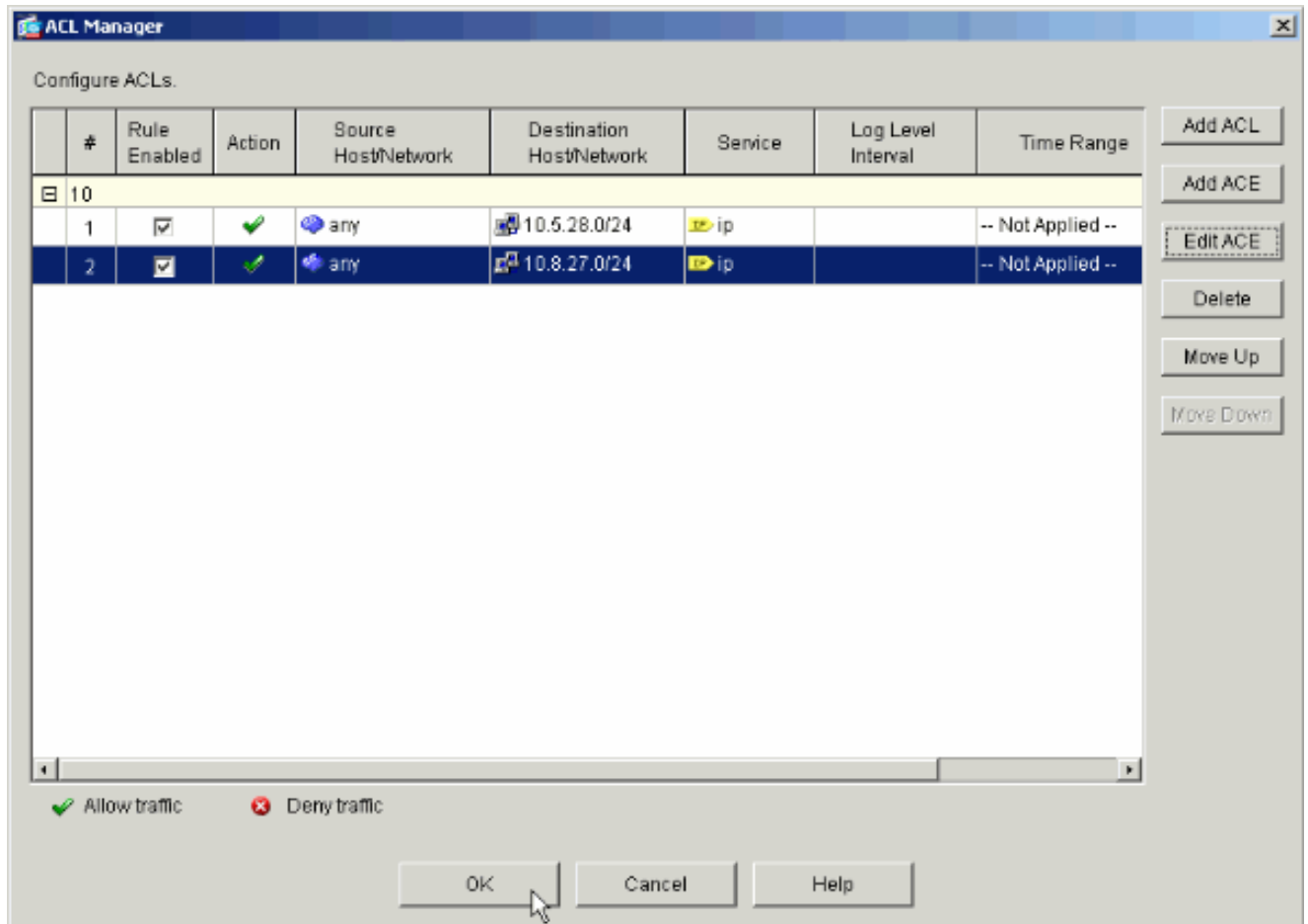
**IP Protocol**

IP protocol: any

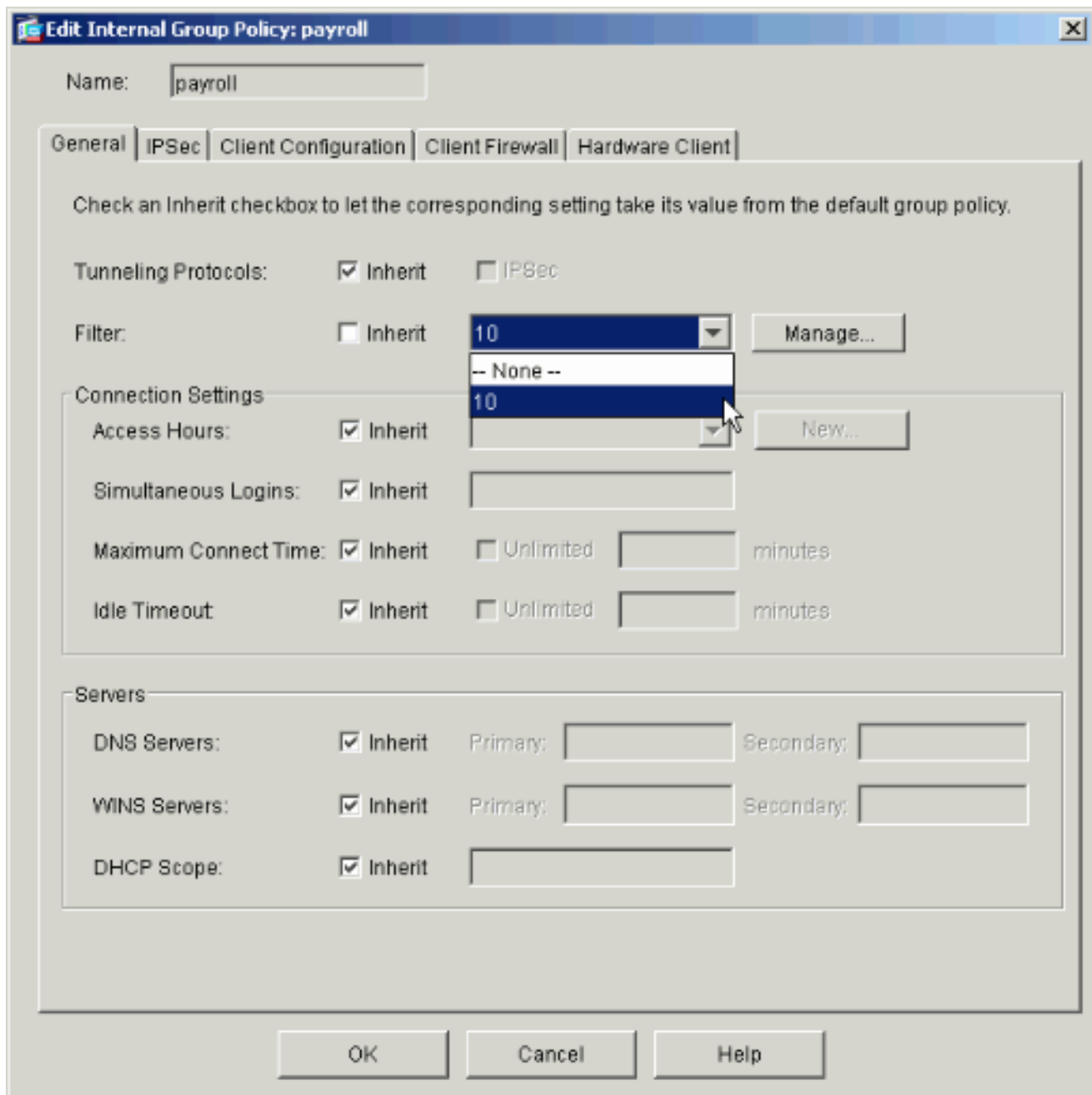
Please enter the description below (optional):

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

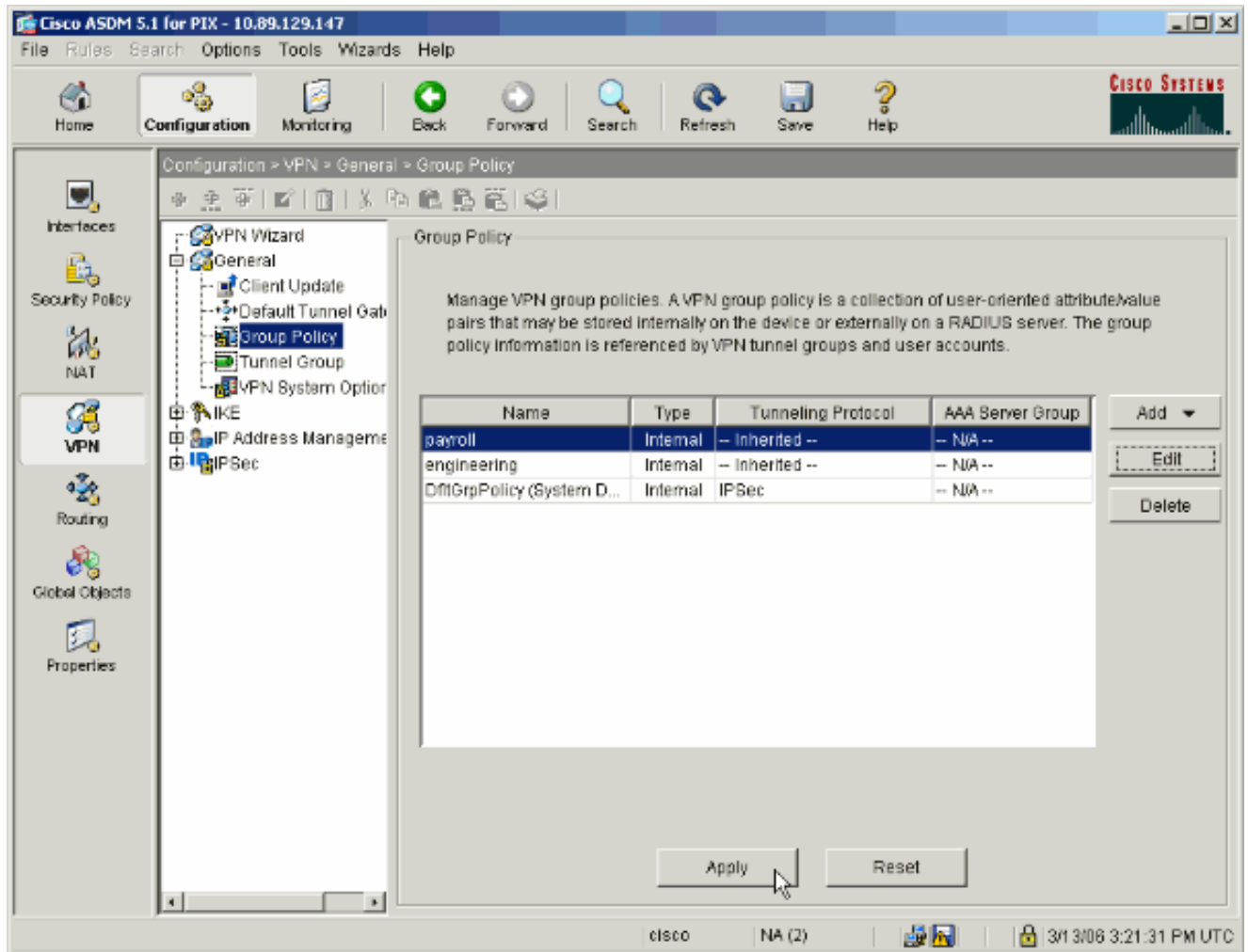
10. ACE の追加が完了したら、[OK] をクリックします。



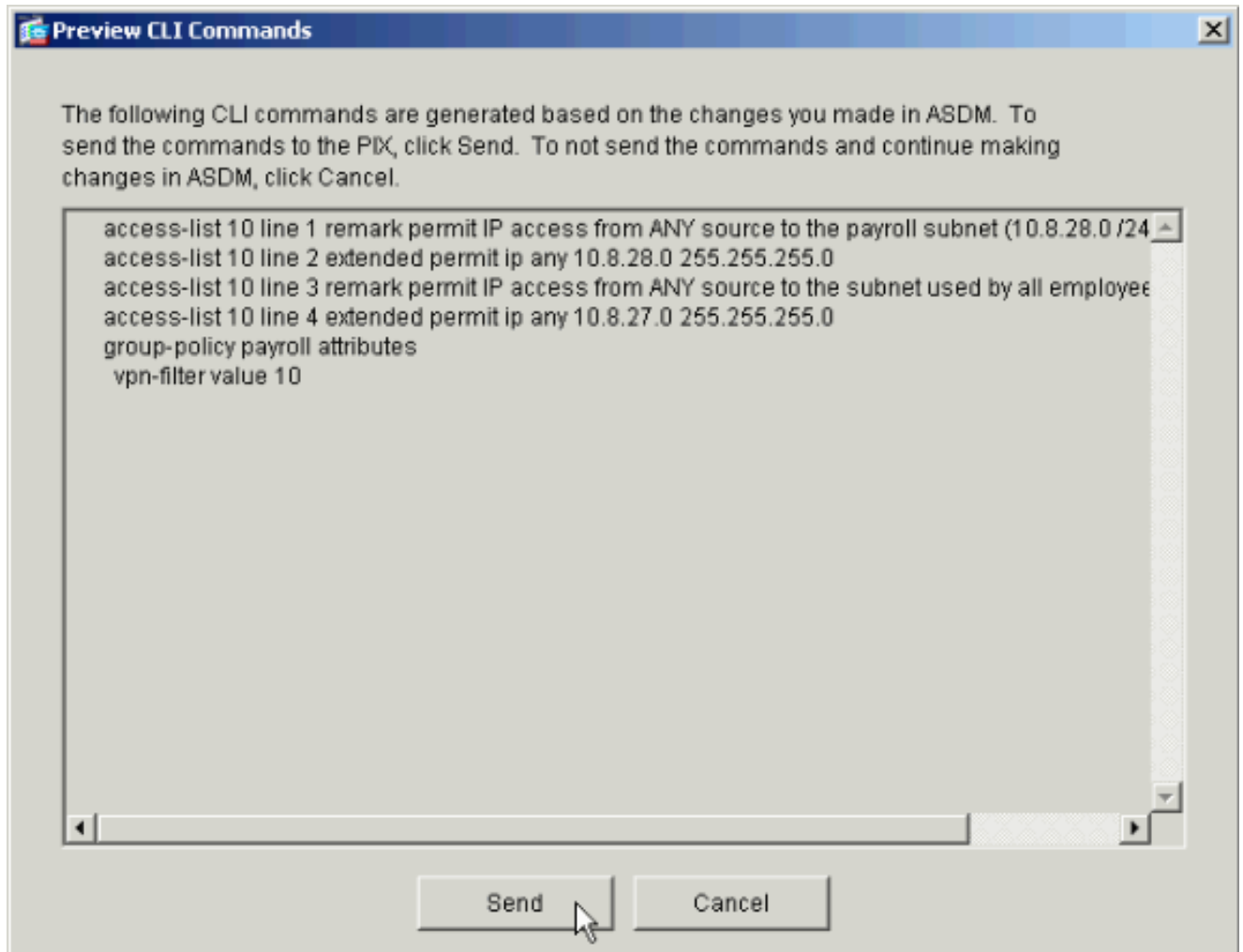
11. グループ ポリシーのフィルタとして、前の手順で定義および入力した ACL を選択します。完了したら、[OK] をクリックします。



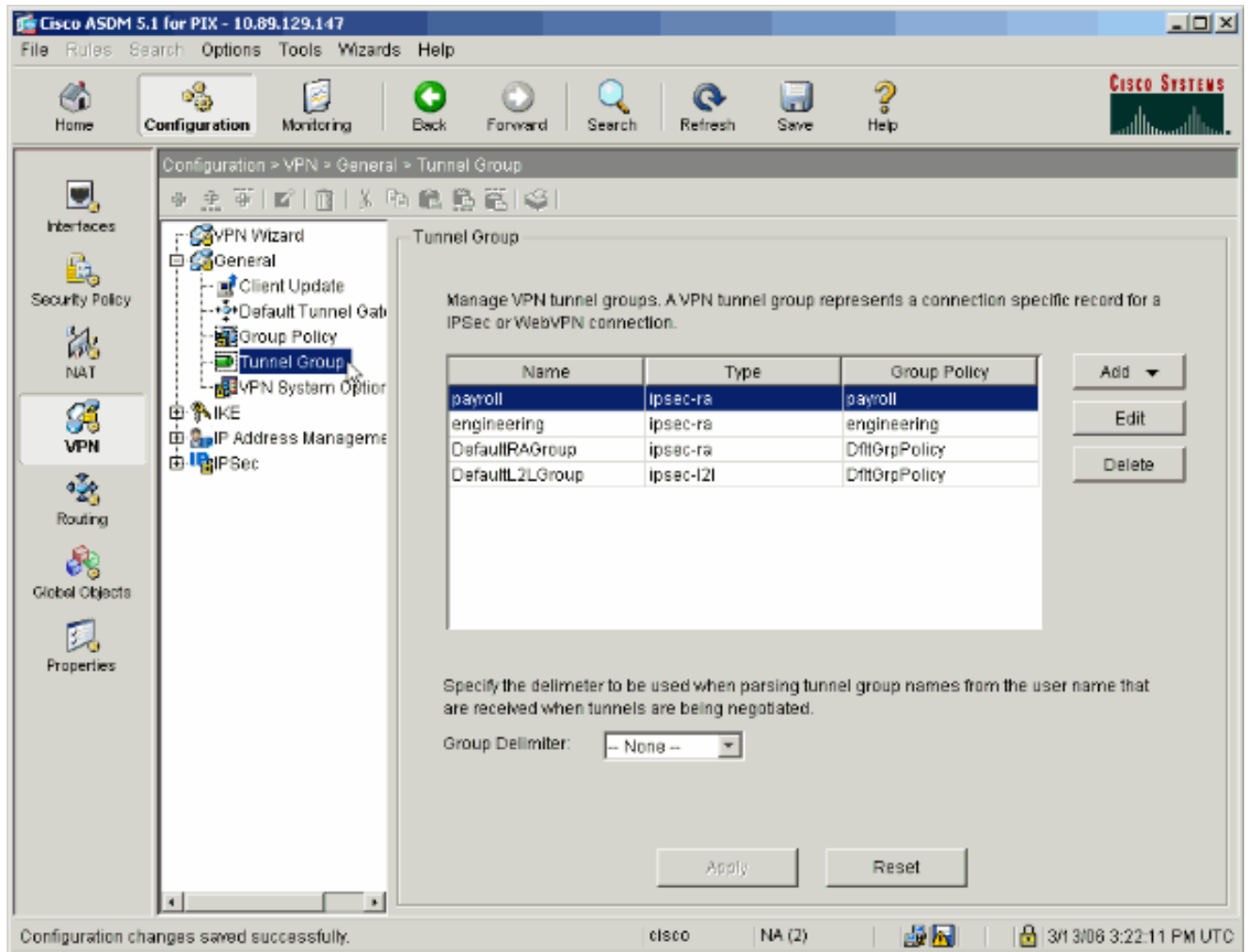
12. [Apply] をクリックすると、変更が PIX に送信されます。



13. [Options] > [Preferences] で設定している場合、PIX へ送信されるコマンドが ASDM に表示されます。[Send] をクリックします。

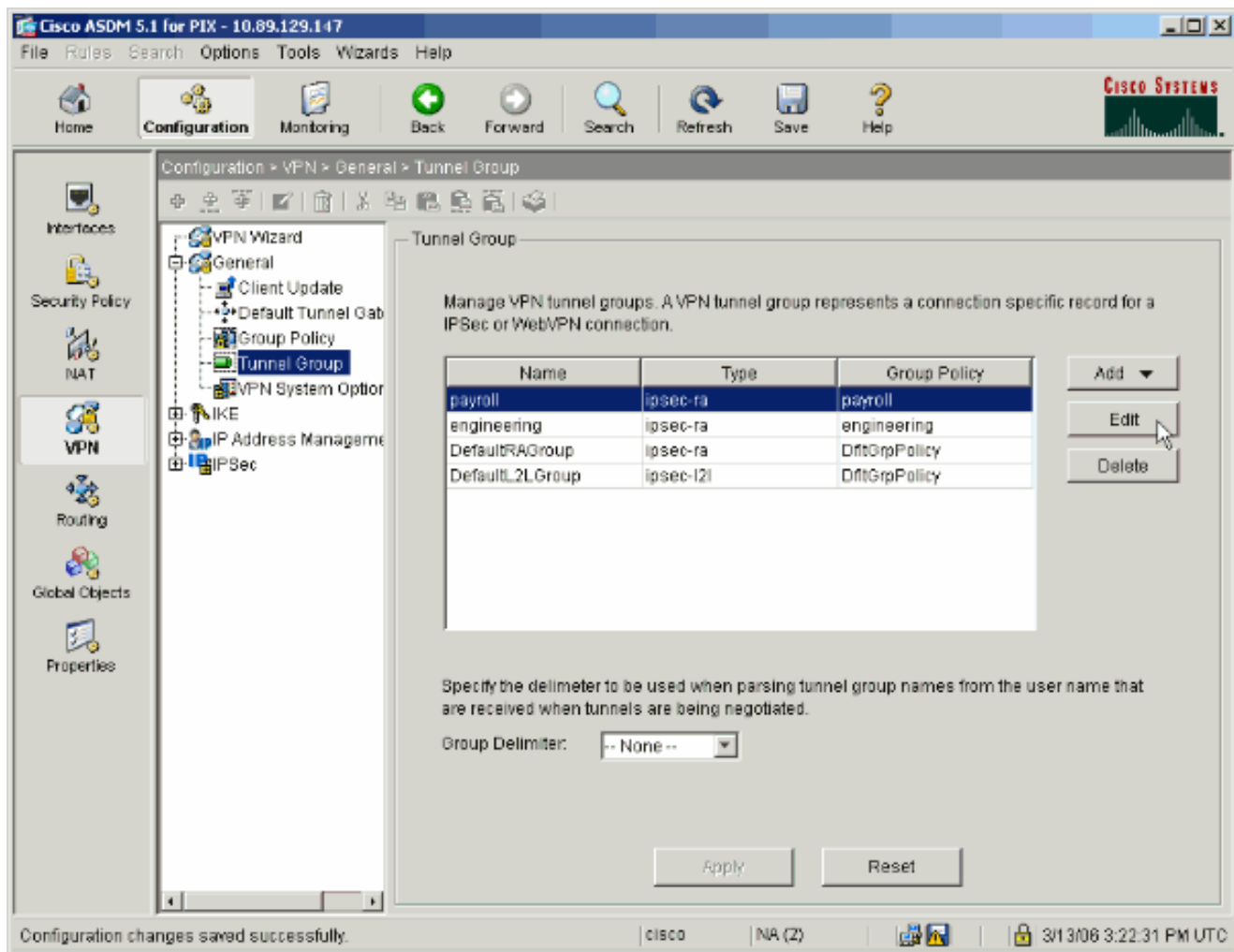


14. 作成または変更したグループ ポリシーを適切なトンネル グループに適用します。左側のフレームで [Tunnel Group] をクリックします。

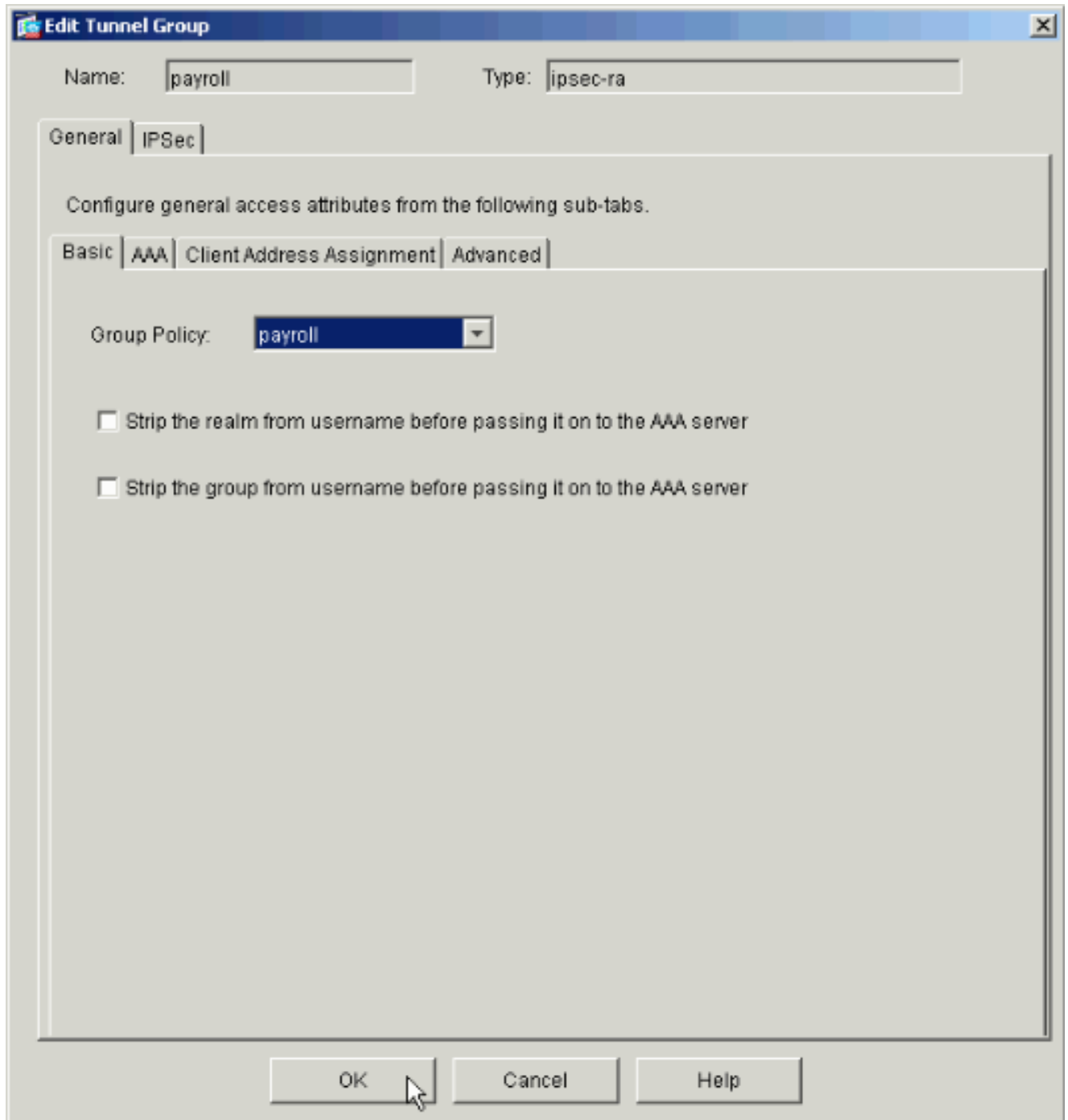


15. グループ ポリシーを適用するトンネル グループを選択したら、[Edit] をクリックします。





16. グループ ポリシーが自動作成された場合（手順 2 を参照）、設定したばかりのグループ ポリシーがドロップダウン ボックスで選択できるか確認します。グループ ポリシーが自動作成されなかった場合は、ドロップダウン ボックスから選択します。完了したら、[OK] をクリックします。



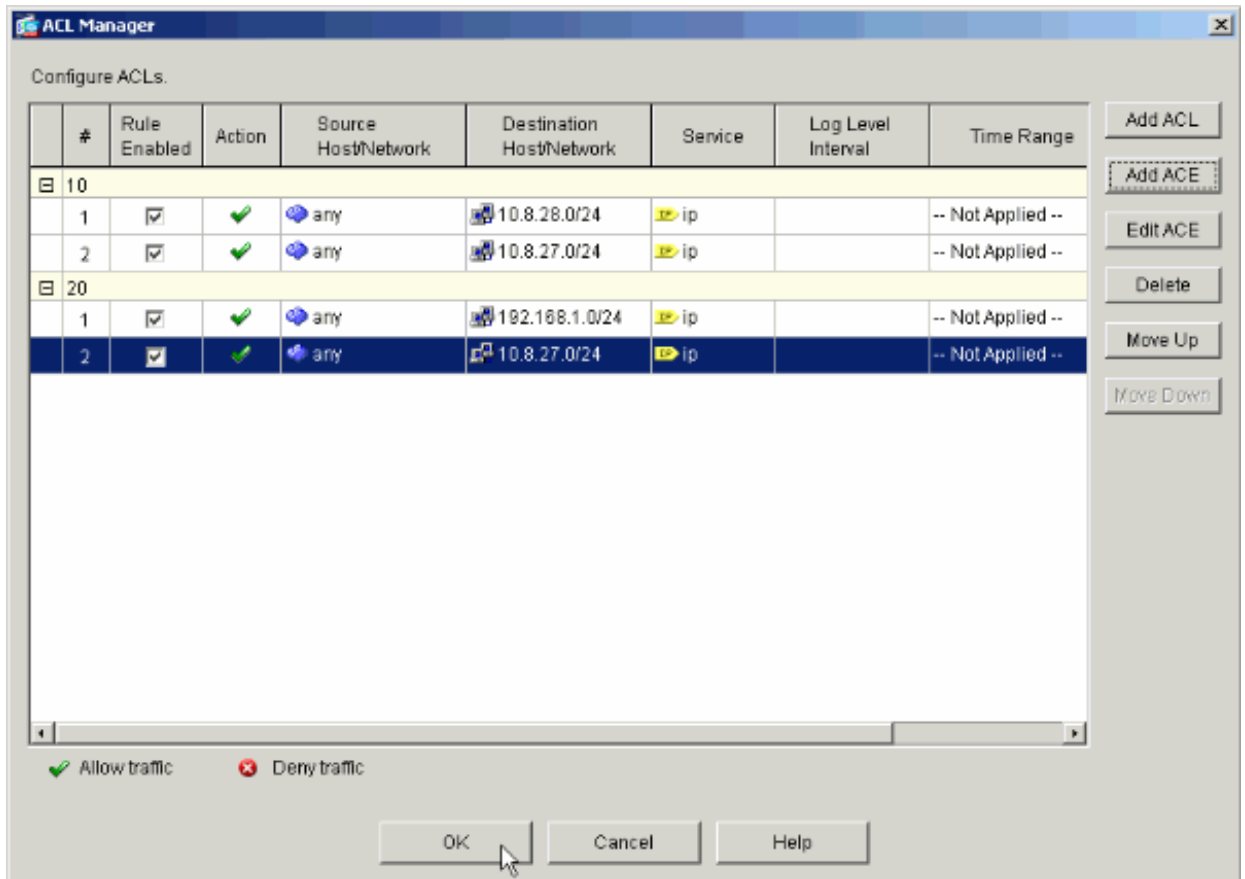
17. [Apply] をクリックし、プロンプトが表示されたら [Send] をクリックして、PIX 設定に変更を追加します。

すでにグループ ポリシーが選択されている場合は、「No changes were made」というメッセージが表示されます。[OK] をクリックします。

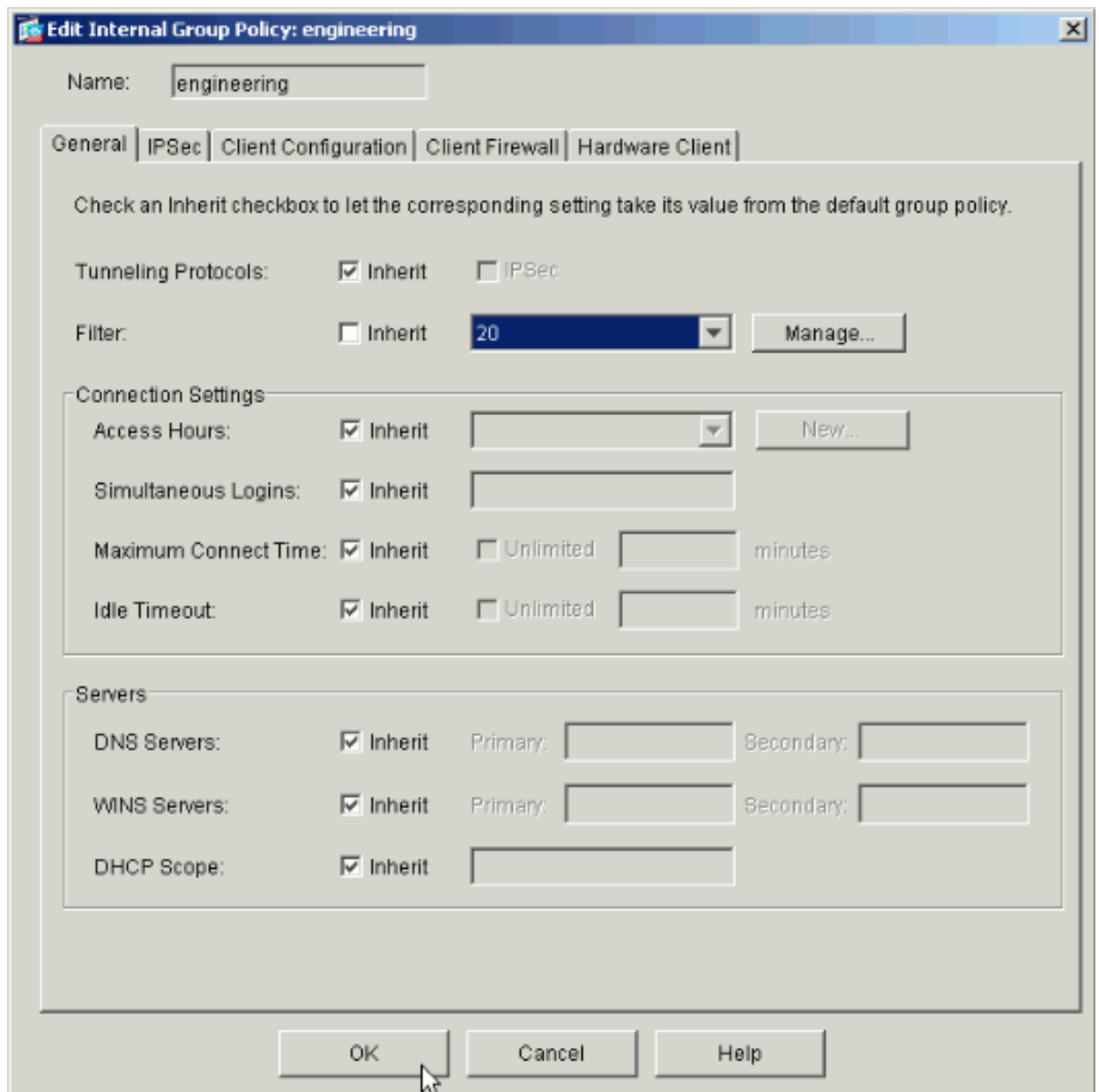
18. 制限を追加したいトンネルグループがある場合は、手順 2 ~ 17 を繰り返します。

この設定例では、エンジニアのアクセス制限を設定する必要があります。手順は同じですが、目立った違いがあるウィンドウをいくつか紹介します。

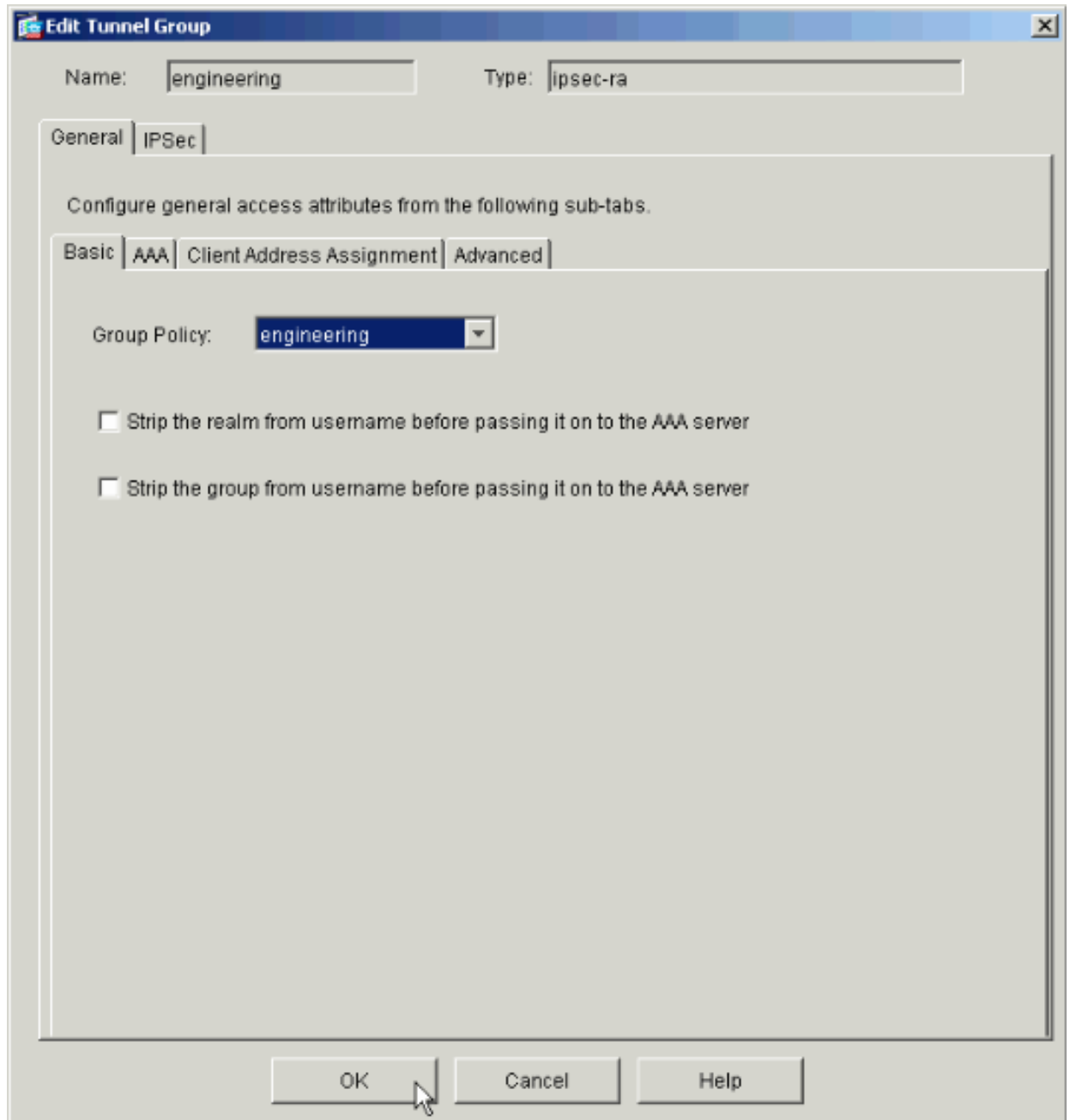
- 新しい ACL 20



- 技術部のグループ ポリシーのフィルタとしてアクセス リスト 20 を選択します。



- 技術部のグループ ポリシーが技術部のトンネル グループに設定されたことを確認します。



## CLI を使用したアクセス設定

CLI を使用してセキュリティ アプライアンスを設定するには、次の手順を実行します。

注：この出力に示すコマンドの中には、スペースの関係上2行にわたって表記されているものがあります。

1. ユーザがリモート アクセス VPN で接続する際に適用される、2つの異なるアクセス コントロール リスト ( 15 および 20 ) を作成します。このアクセス リストは設定の最後で呼び出されます。

```
<#root>
```

```
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
```

- 異なる VPN アドレス プールを 2 つ作成します。1 つは経理部のリモート ユーザ用、もう 1 つは技術部のリモート ユーザ用です。

```
<#root>
```

```
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. 経理部のユーザが接続した場合にのみ適用されるポリシーを作成します。

```
<#root>
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. この手順は、技術部グループ向けであること以外は手順3と同じです。

```
<#root>
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.*

- ローカル ユーザを作成し、リソースへのアクセス制限を適用するユーザに対して属性を割り当てます。

```
<#root>
```

```
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. 経理部ユーザの接続ポリシーを含むトンネルグループを作成します。

```
<#root>
```

```
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. 技術部ユーザの接続ポリシーを含むトンネルグループを作成します。

```
<#root>
```

```
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
```

設定の入力が完了すると、太字部分のような設定になります。

#### デバイス名 1

```
<#root>  
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 6XmYwQ009tiYnUDN 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)#
```

## 確認

ASDM のモニタリング機能を使用して設定を確認します。

1. [Monitoring] > [VPN] > [VPN Statistics] > [Sessions] の順に選択します。

PIX にはアクティブな VPN セッションが表示されます。気になるセッションを選択して [Details] をクリックします。

The screenshot shows the Cisco ASDM 5.1 for PIX - 10.89.129.147 interface. The navigation pane on the left shows the path: Monitoring > VPN > VPN Statistics > Sessions. The main content area displays the following summary table:

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

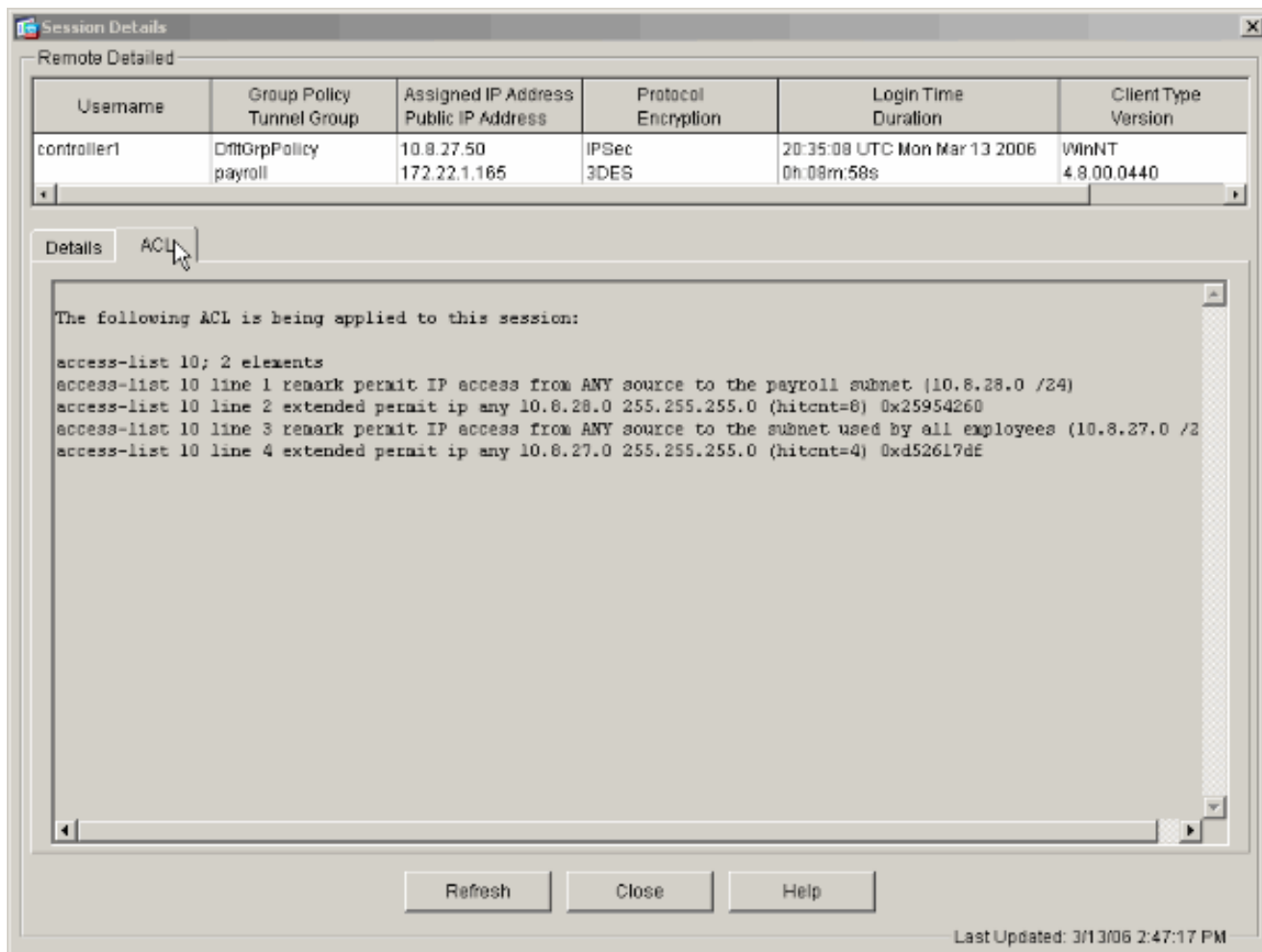
Below the summary table, there is a filter section: Filter By: Remote Access, -- All Sessions --, and a Filter button. The main table lists active sessions:

Username	Group Policy Tunnel Group	Assigned IP Address Public IP Address	Protocol Encryption	Details	Logout	Ping
controller1	DfltGrpPolicy payroll	10.8.27.50 172.22.1.185	IPSec 3DES			

At the bottom of the page, there is a Logout By: -- All Sessions --, Logout Sessions button, and a Refresh button. The status bar at the bottom indicates: Data Refreshed Successfully. | cisco | NA (2) | 3/13/06 8:36:34 PM UTC.

2. [ACL] タブを選択します。

ACL の hitcnts は、クライアントから許可されたネットワークへ流れるトラフィックを表しています。



The screenshot shows a 'Session Details' window with a table of session information and a detailed view of the ACL configuration.

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

Details | **ACL**

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
```

Refresh Close Help

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

## トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- [Cisco ASA 5500 適応型セキュリティ アプライアンス：拡張認証を備えたリモート VPN サーバとしての PIX/ASA の CLI と ASDM を使用した設定例](#)
- [Cisco PIX 500 シリーズ セキュリティ アプライアンス製品の設定例とテクニカル ノート](#)
- [Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス製品の設定例とテクニカル ノート](#)
- [Cisco VPN クライアントの設定例とテクニカル ノート](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。