PIX/ASA 7.x ASDM: Restringir o acesso à rede de usuários de VPN de acesso remoto

Contents

Introdução

Este documento fornece uma configuração de exemplo usando o Cisco Adaptive Security Device Manager (ASDM) para restringir quais redes internas os usuários do acesso remoto VPN podem acessar por trás do Mecanismo de Segurança PIX ou do Adaptive Security Appliance (ASA). É possível limitar os usuários do acesso remoto VPN apenas às áreas da rede que deseja que elas acessem quando você:

1. Crie listas de acesso.
2. Associá-los a políticas de grupo.
3. Associe essas políticas de grupo a grupos de túnel.

Consulte Configuring the Cisco VPN 3000 Concentrator for Blocking with Filters and RADIUS Filter Assignment para saber mais sobre o cenário em que o VPN Concentrator bloqueia o acesso de usuários VPN.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- O PIX pode ser configurado usando o ASDM.

Observação: consulte Permitindo o Acesso HTTPS para o ASDM para permitir que o PIX seja configurado pelo ASDM.

- Você tem pelo menos uma configuração de VPN de acesso remoto em boas condições em vigor.

  Observação: Se você não tiver nenhuma dessas configurações, consulte ASA como um Servidor VPN Remoto usando o Exemplo de Configuração do ASDM para obter informações sobre como configurar uma boa configuração de VPN de acesso remoto.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure PIX 500 Series Security Appliance versão 7.1(1)

  Observação: os PIX 501 e 506E Security Appliances não suportam a versão 7.x.

- Cisco Adaptive Security Device Manager versão 5.1(1)

  Observação: O ASDM está disponível apenas no PIX ou no ASA 7.x.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

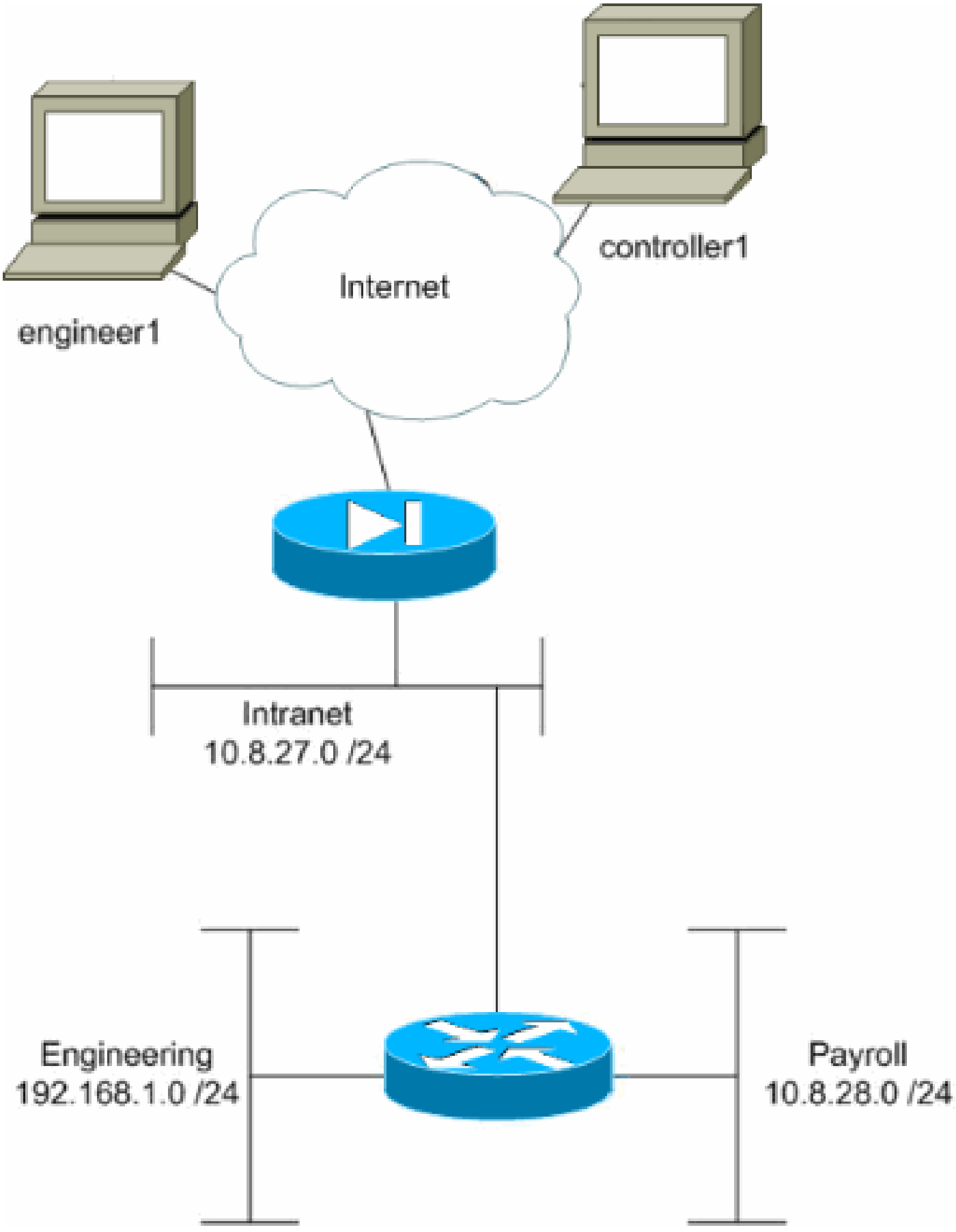
Produtos Relacionados

Esta configuração também pode ser utilizada com estas versões de hardware e software:

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

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Neste exemplo de configuração, supõe-se uma rede corporativa pequena com três sub-redes. Este diagrama ilustra a topologia. As três sub-redes são Intranet, Engenharia e Folha de Pagamento. O objetivo deste exemplo de configuração é permitir que o pessoal da folha de

pagamento acesse remotamente as sub-redes Intranet e Folha de Pagamento e impedi-los de acessar a sub-rede Engenharia. Além disso, os engenheiros devem ser capazes de acessar remotamente as sub-redes Intranet e Engenharia, mas não a sub-rede Folha de pagamento. O usuário da folha de pagamento neste exemplo é "controller1". O usuário de engenharia neste exemplo é "engenheiro1".

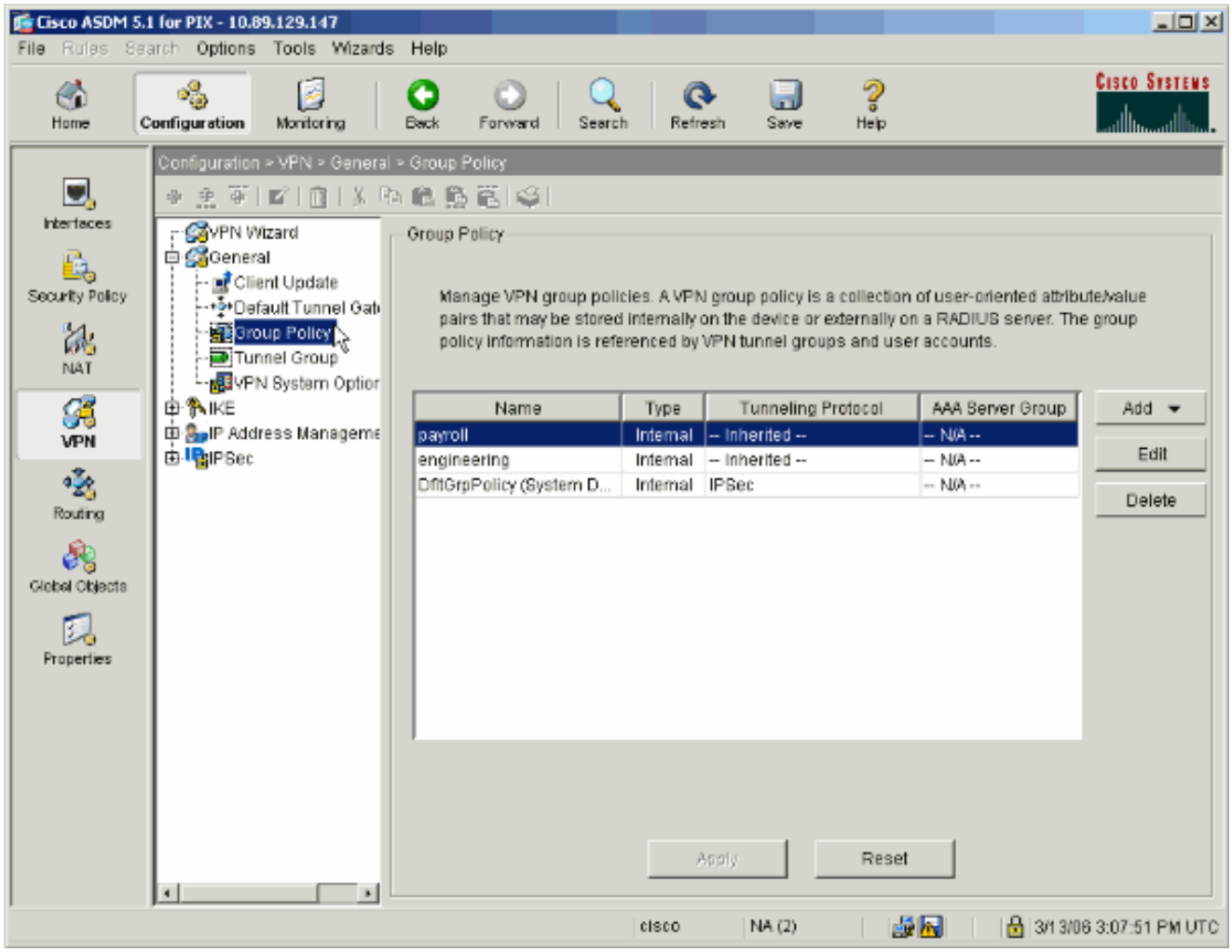
Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

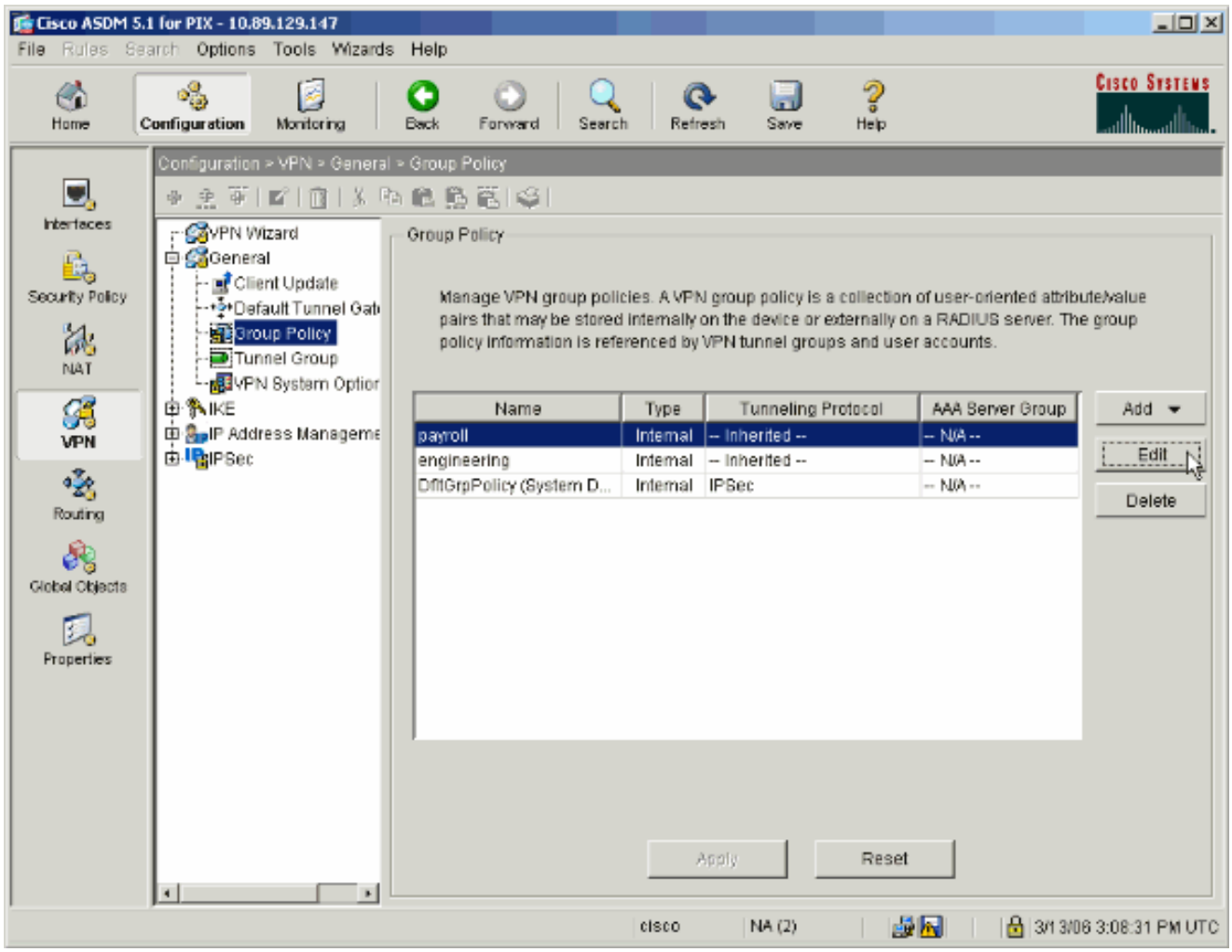
Configurar Acesso via ASDM

Conclua estas etapas para configurar o PIX Security Appliance usando o ASDM:

1. Selecione Configuration > VPN > General > Group Policy.

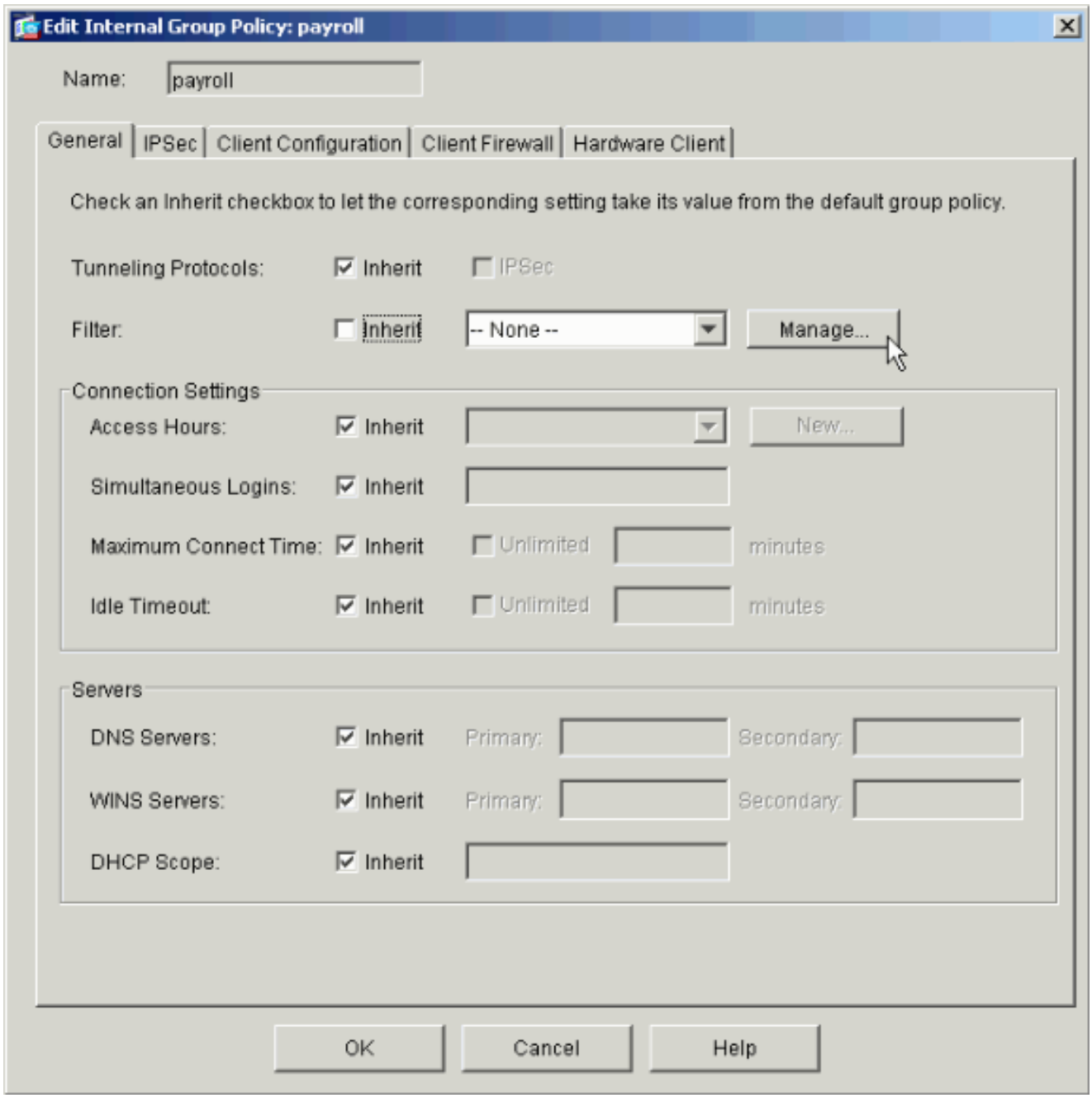


2. Com base em quais etapas foram executadas para configurar grupos de túneis no PIX, as Políticas de Grupo podem já existir para os grupos de túneis cujos usuários você deseja restringir. Se já existir uma Diretiva de Grupo adequada, escolha-a e clique em Editar. Caso contrário, clique em Add e escolha Internal Group Policy....

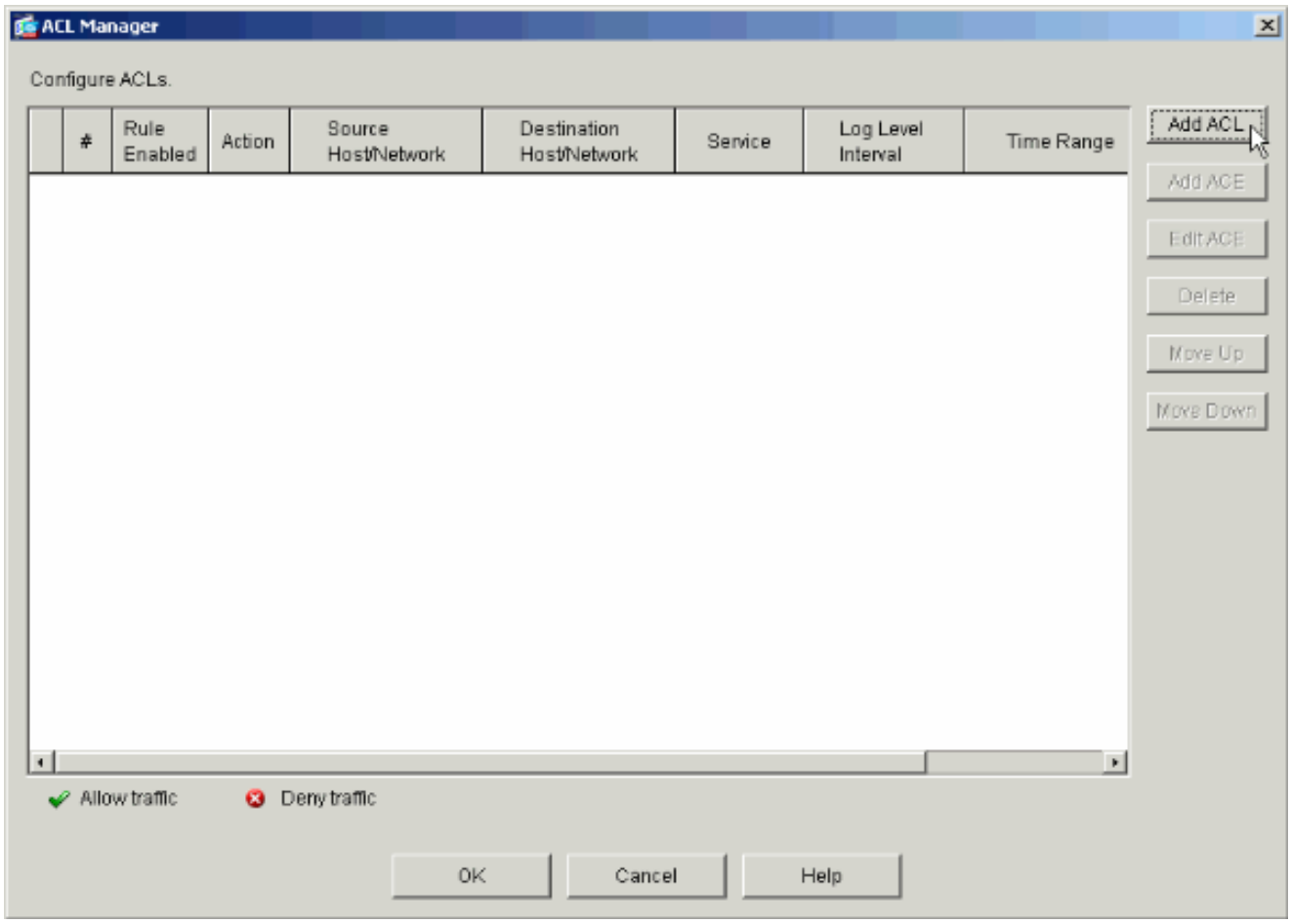


3. Se necessário, insira ou altere o nome da Diretiva de Grupo na parte superior da janela que será aberta.

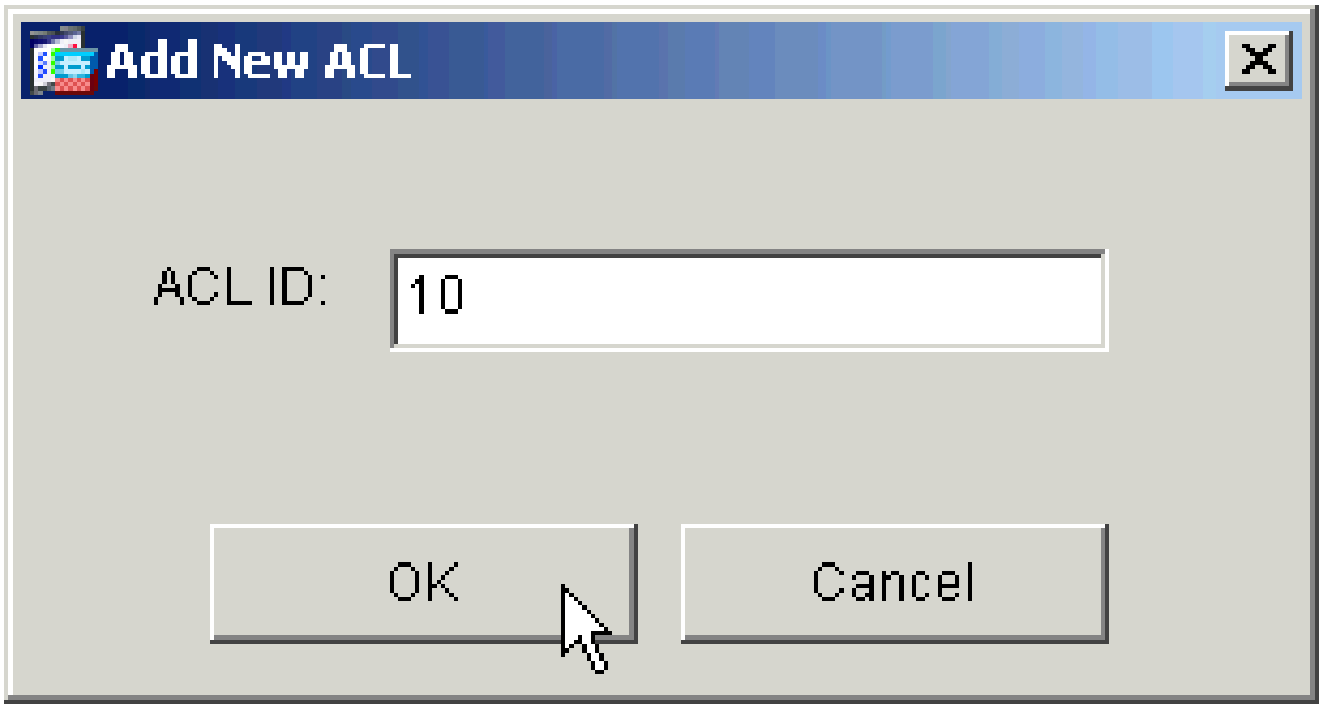
4. Na guia Geral, desmarque a caixa Herdar ao lado de Filtro e clique em Gerenciar.



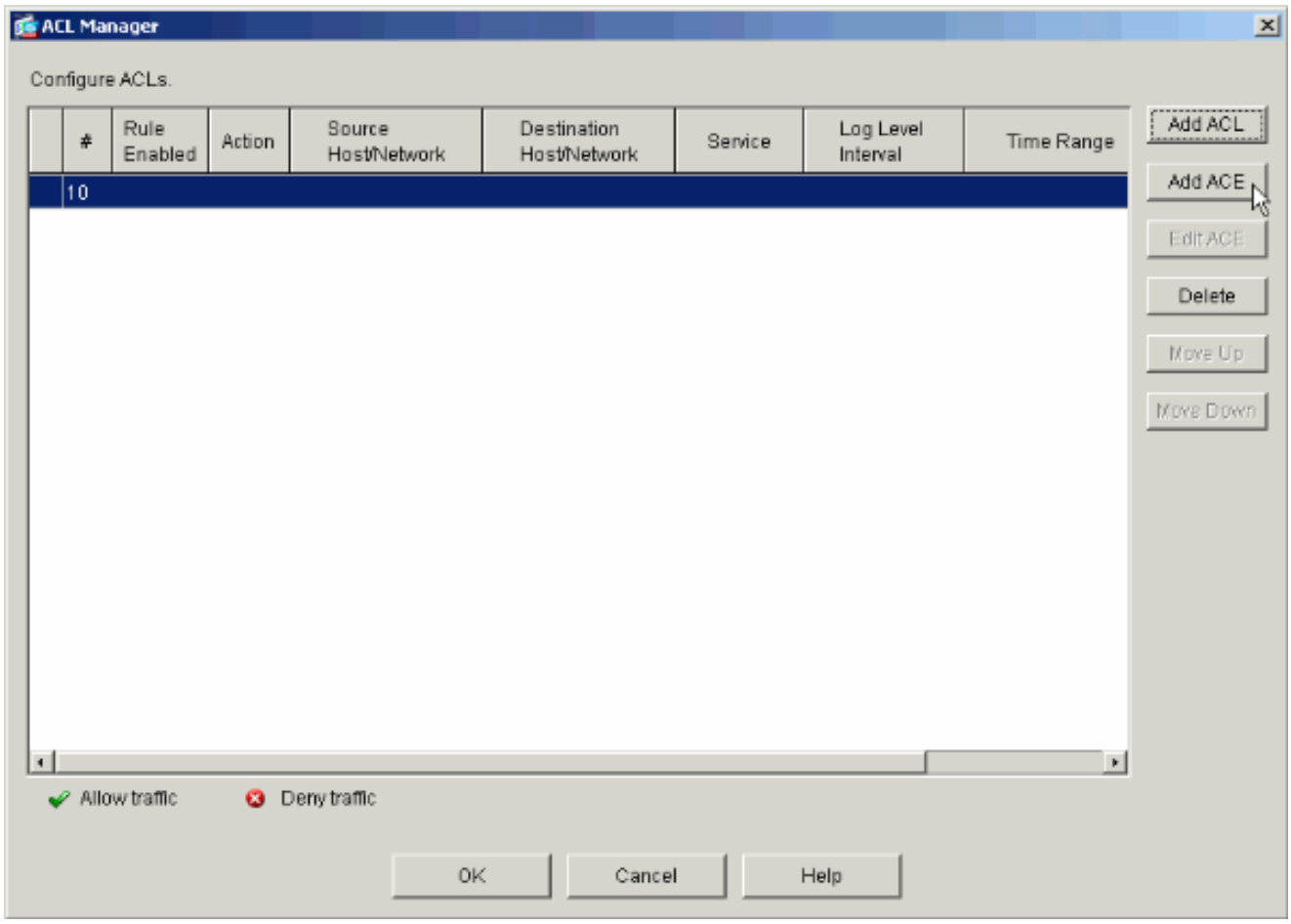
5. Clique em Add ACL para criar uma nova lista de acesso na janela do ACL Manager exibida.



6. Escolha um número para a nova lista de acesso e clique em OK.



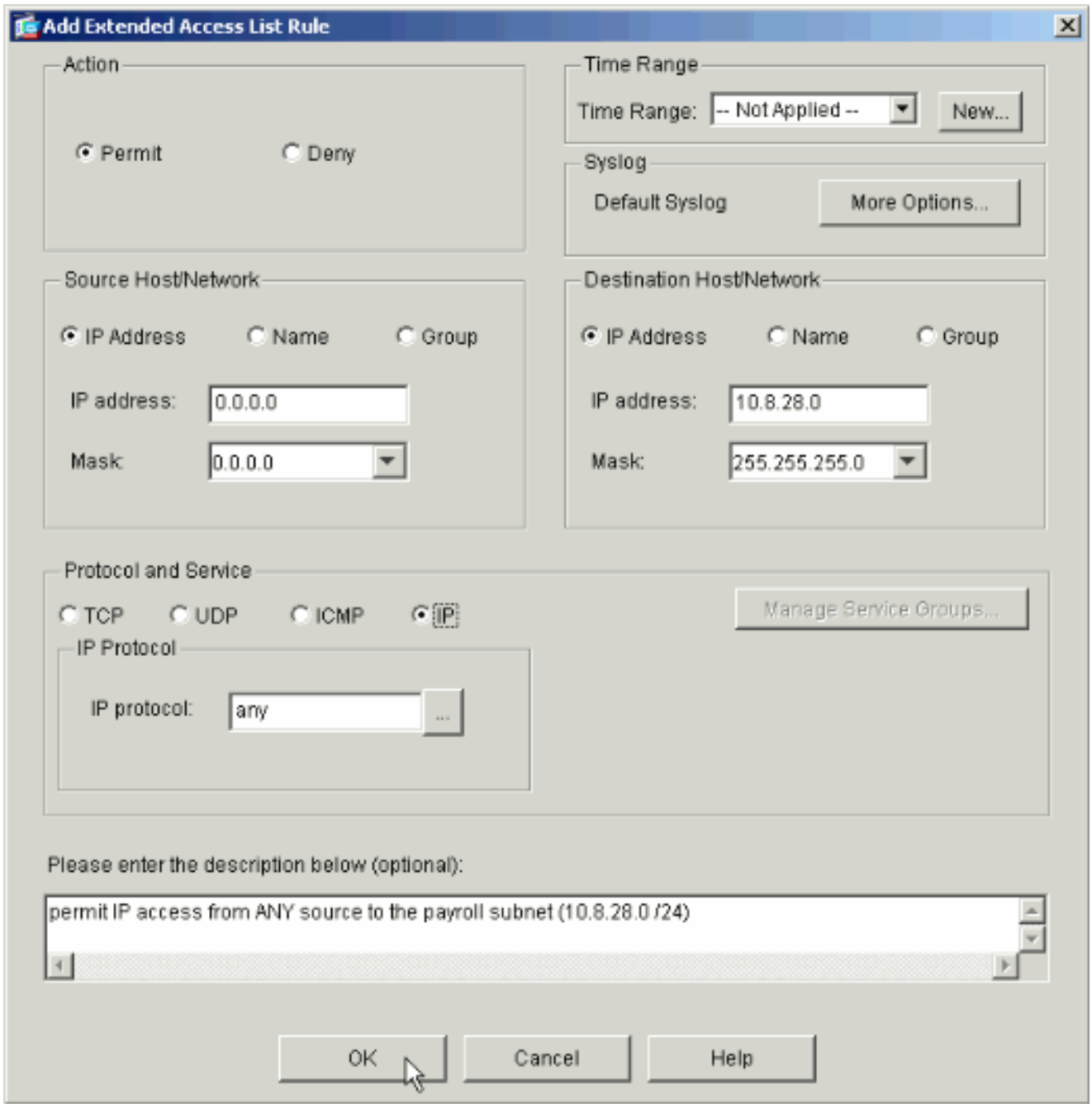
7. Com a nova ACL selecionada à esquerda, clique em Adicionar ACE para adicionar uma nova entrada de controle de acesso à lista.



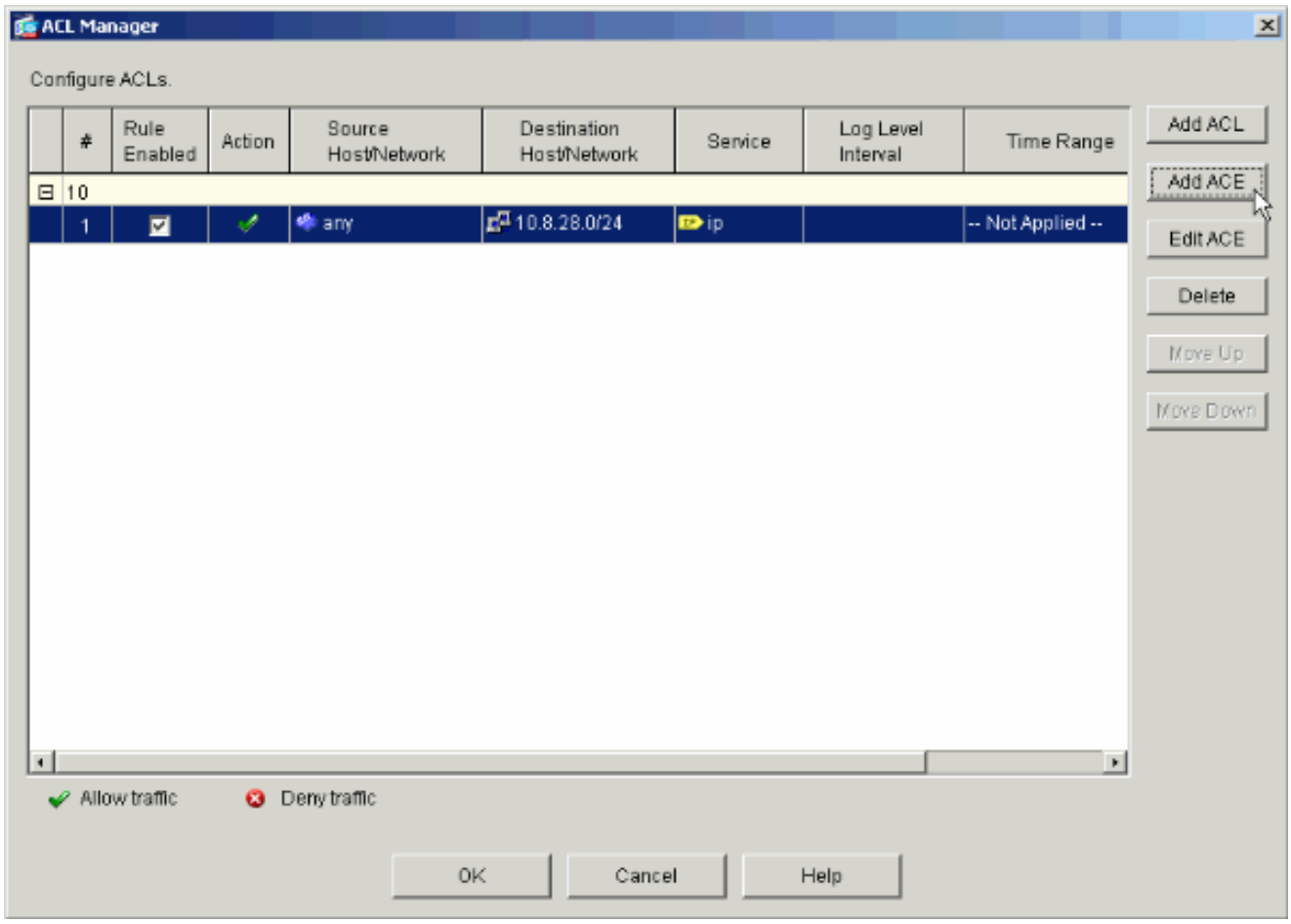
8. Defina a entrada de controle de acesso (ACE) que deseja adicionar.

   Neste exemplo, a primeira ACE na ACL 10 permite acesso IP à sub-rede de folha de pagamento de qualquer origem.

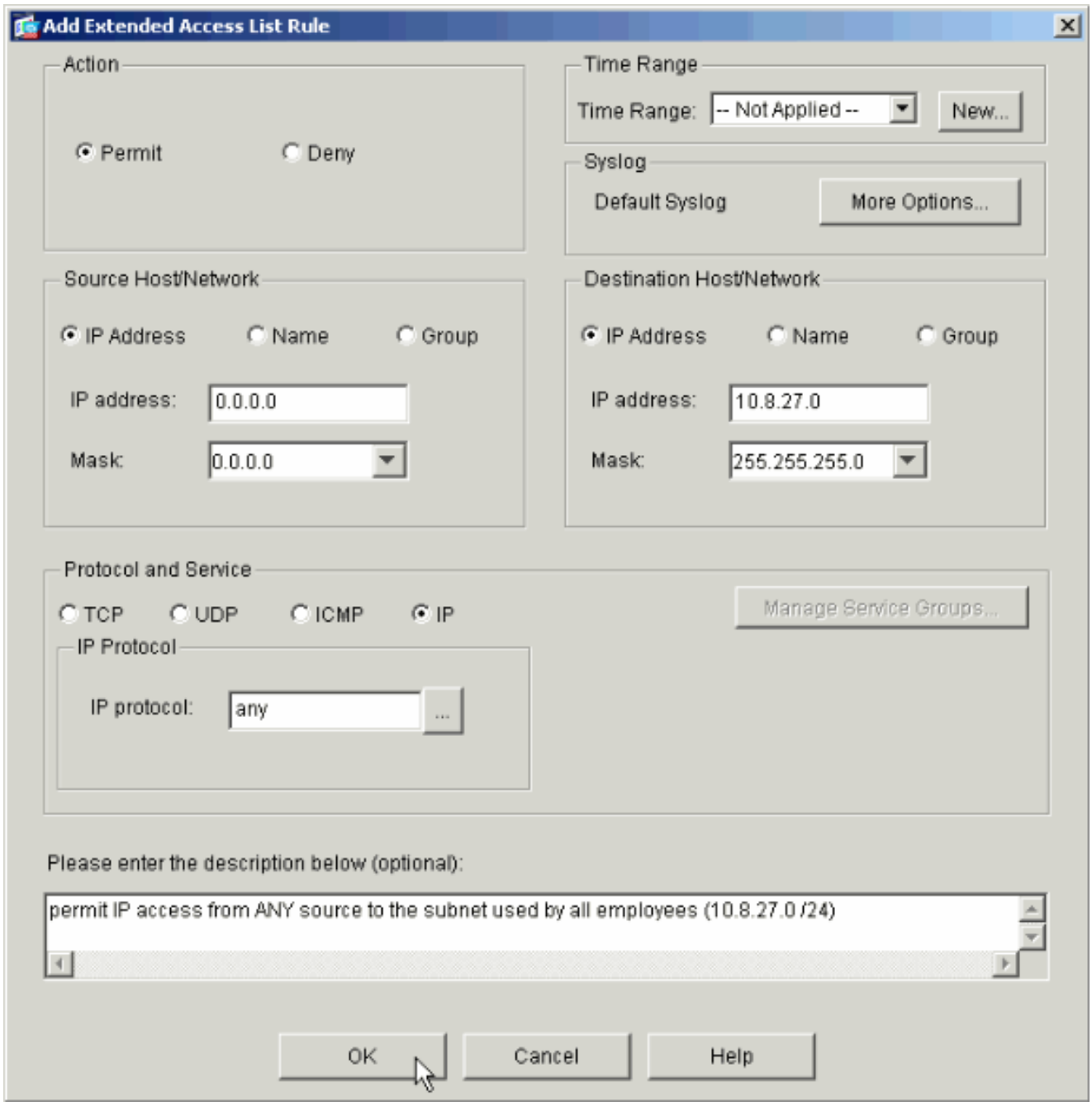
   Observação: Por padrão, o ASDM seleciona somente o TCP como o protocolo. Você deve escolher IP se quiser permitir ou negar aos usuários acesso IP completo. Clique em OK quando terminar.



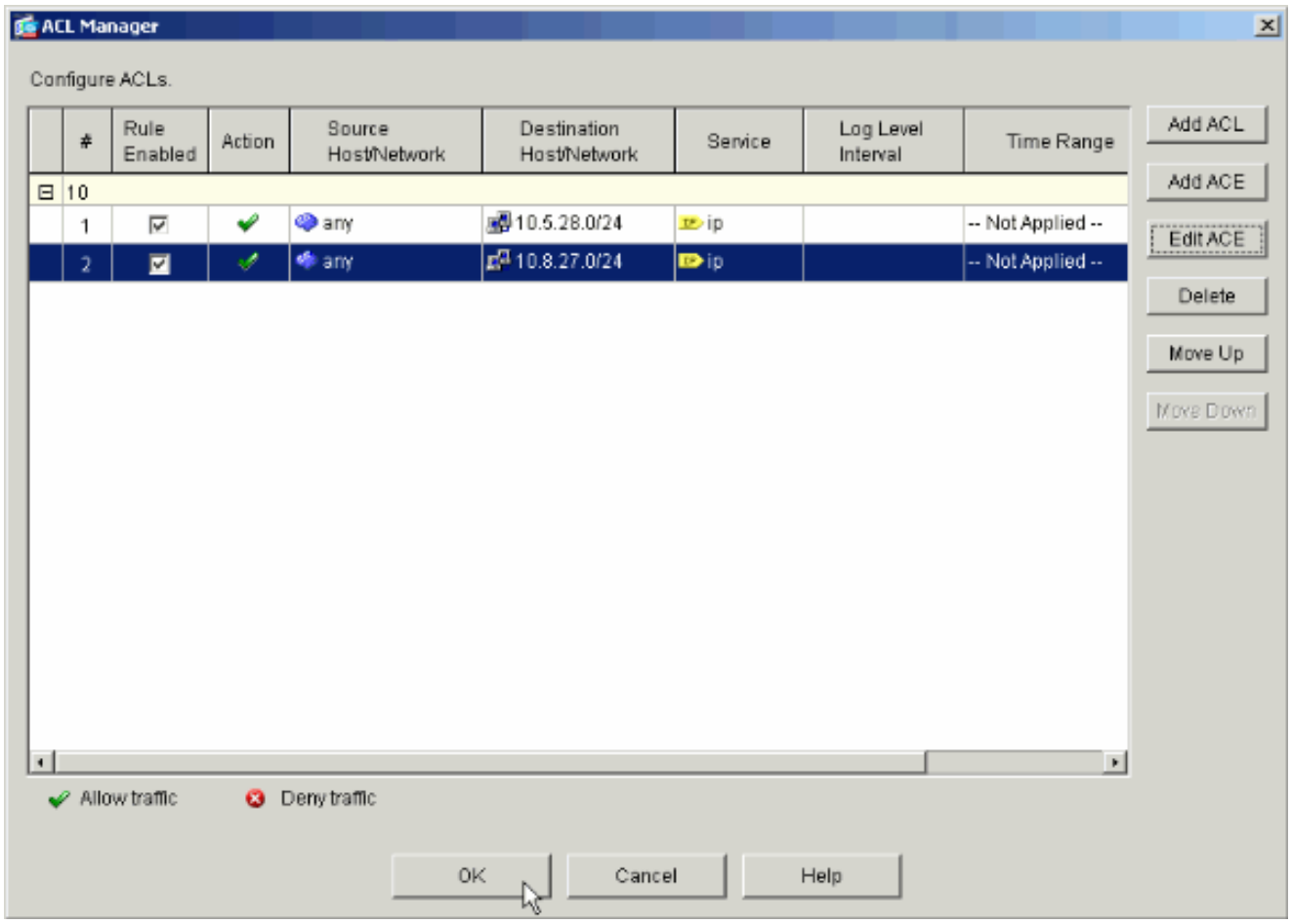
9. O ACE que você acabou de adicionar agora aparece na lista. Escolha Adicionar ACE novamente para adicionar mais linhas à lista de acesso.



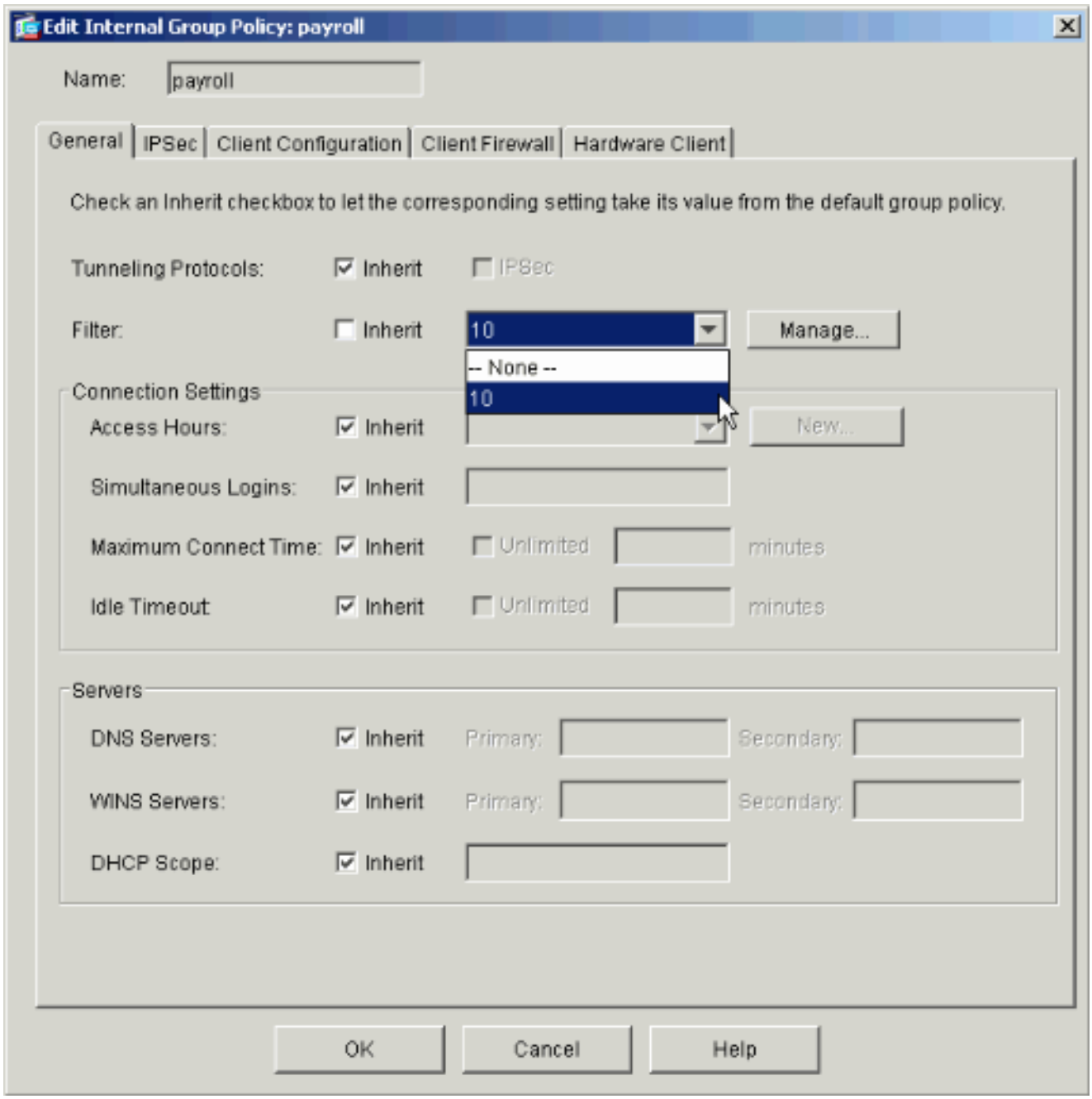
Neste exemplo, uma segunda ACE é adicionada à ACL 10 para permitir o acesso à sub-rede da Intranet.



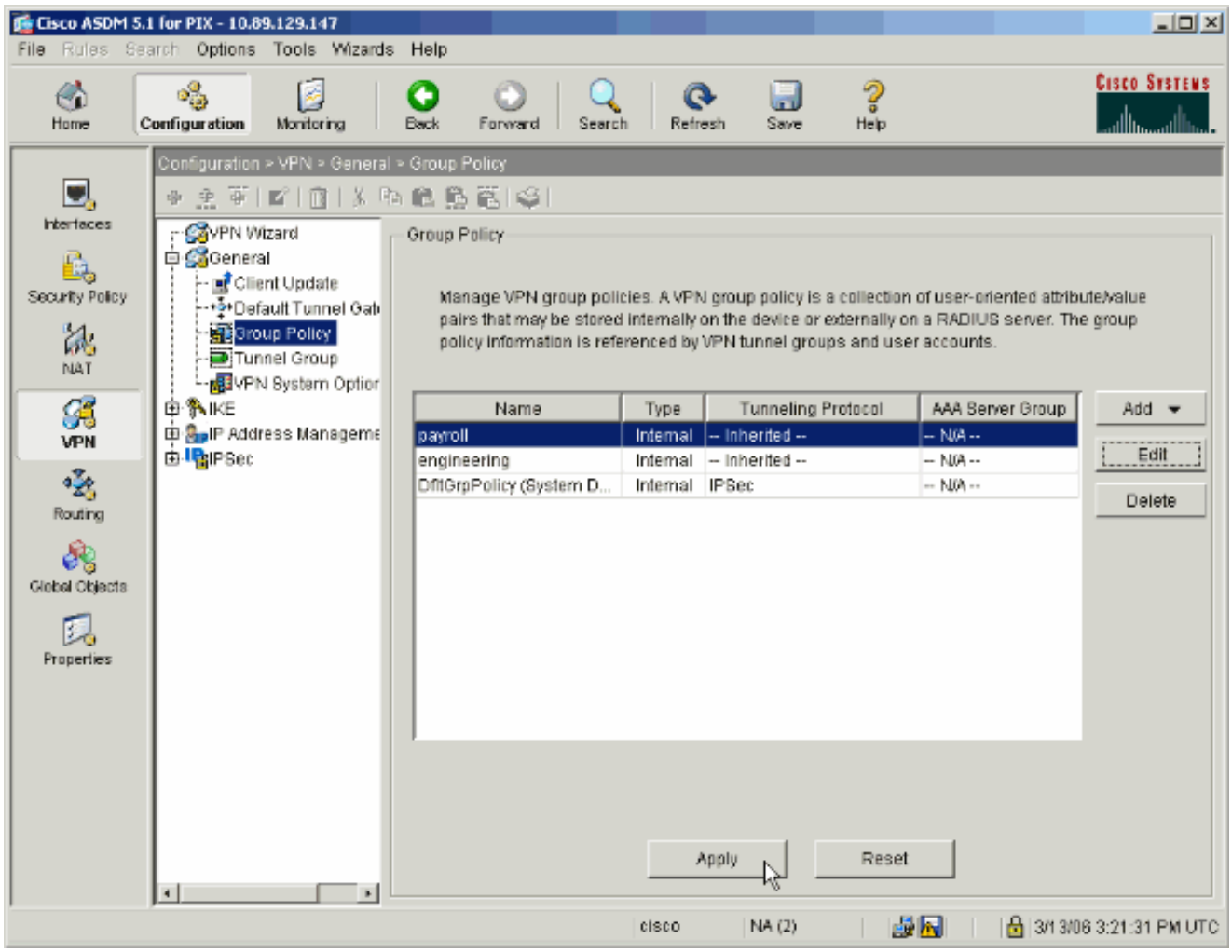
10. Clique em OK quando terminar de adicionar ACEs.



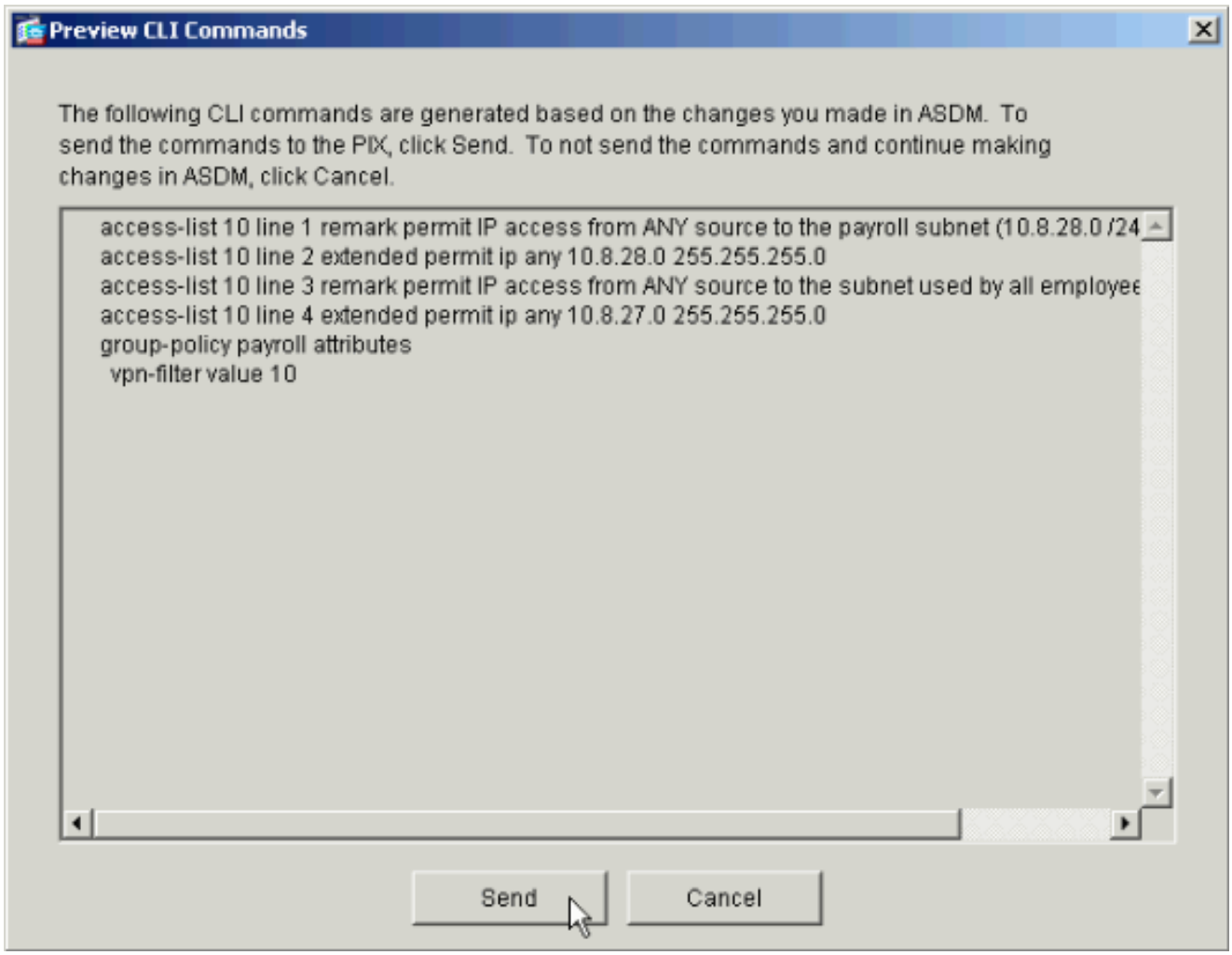
11. Selecione a ACL que você definiu e preencheu nas últimas etapas para ser o filtro da sua Política de grupo. Clique em OK quando terminar.



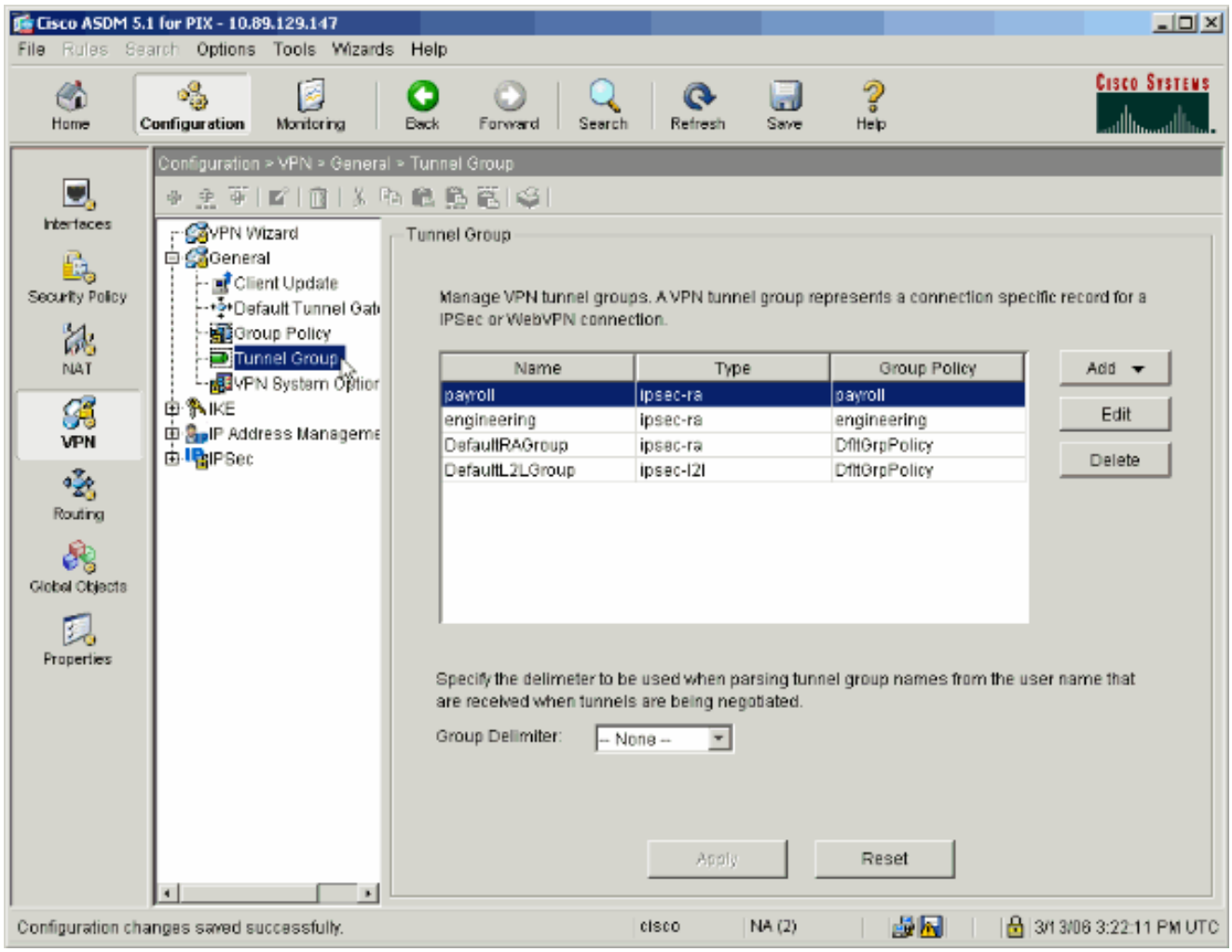
12. Clique em Apply para enviar as alterações ao PIX.



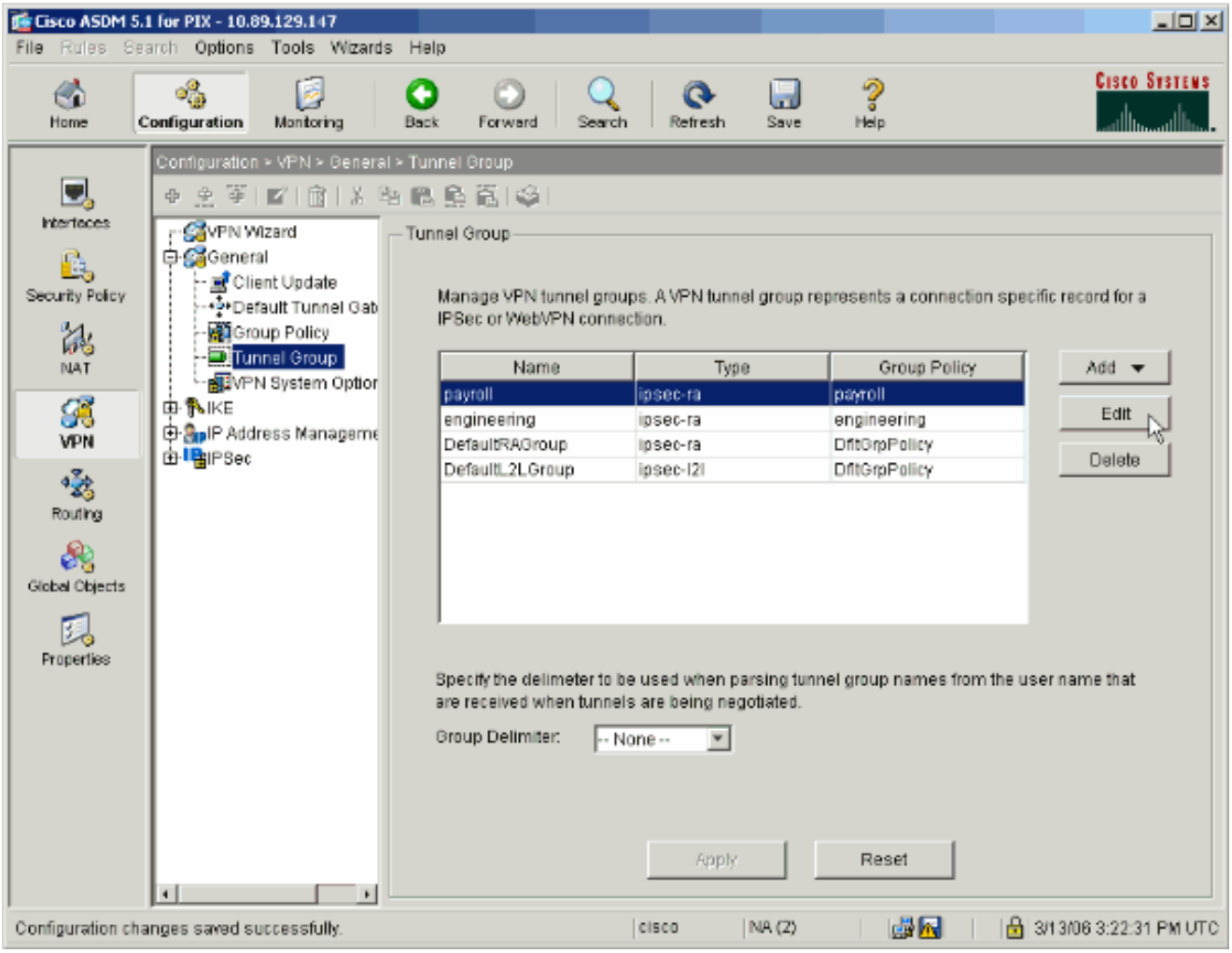
13. Se estiver configurado para fazer isso em Options > Preferences, o ASDM visualizará os comandos que está prestes a enviar para o PIX. Clique em Enviar.



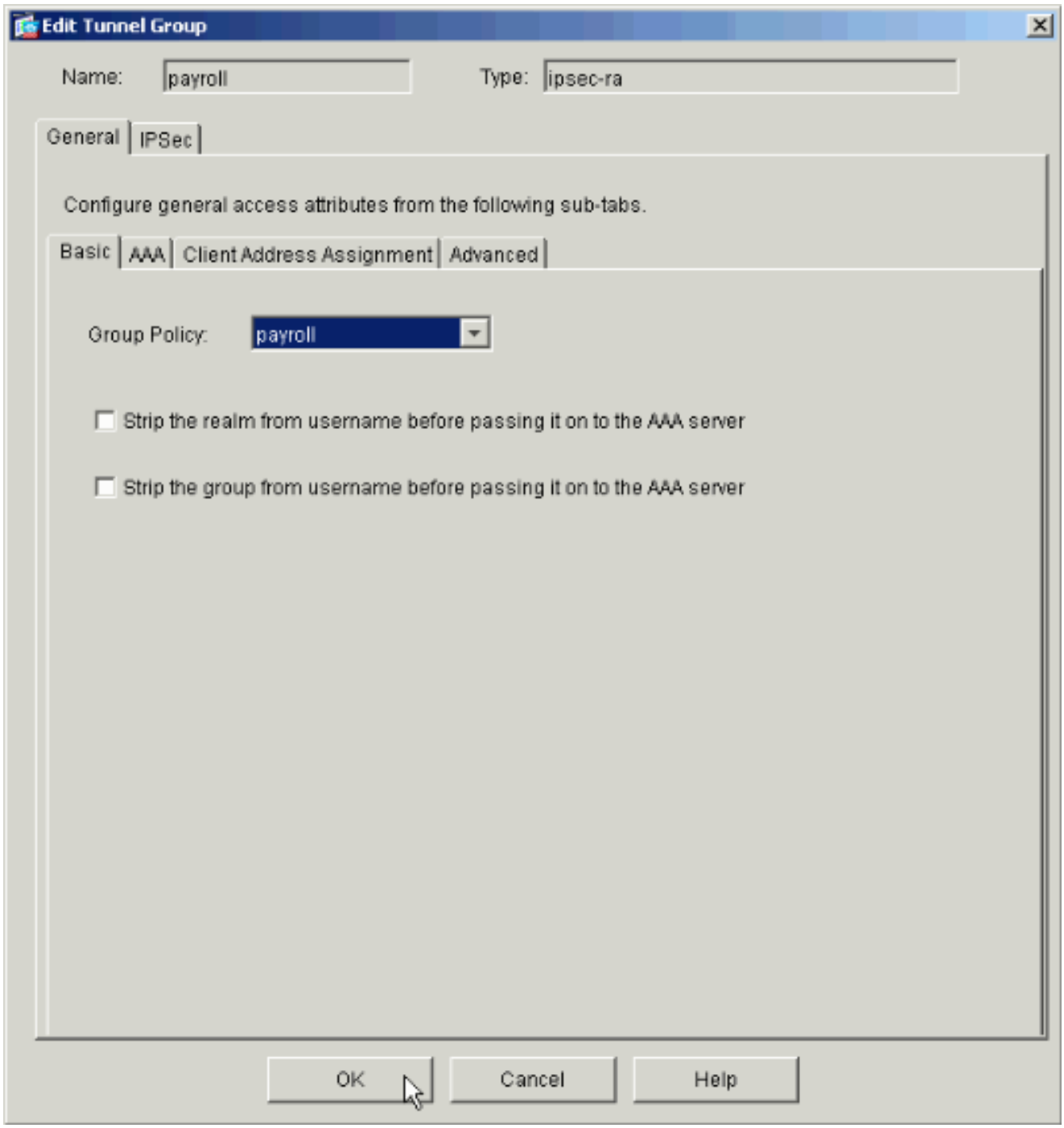
14. Aplique a Diretiva de Grupo que acabou de ser criada ou modificada ao grupo de túneis correto. Clique em Tunnel Group no quadro esquerdo.



15. Escolha o grupo de túneis ao qual deseja aplicar a diretiva de grupo e clique em Edit.



16. Se a Diretiva de Grupo foi criada automaticamente (consulte a etapa 2), verifique se a Diretiva de Grupo que você acabou de configurar está selecionada na caixa suspensa. Se sua Diretiva de Grupo não foi configurada automaticamente, selecione-a na caixa suspensa. Clique em OK quando terminar.



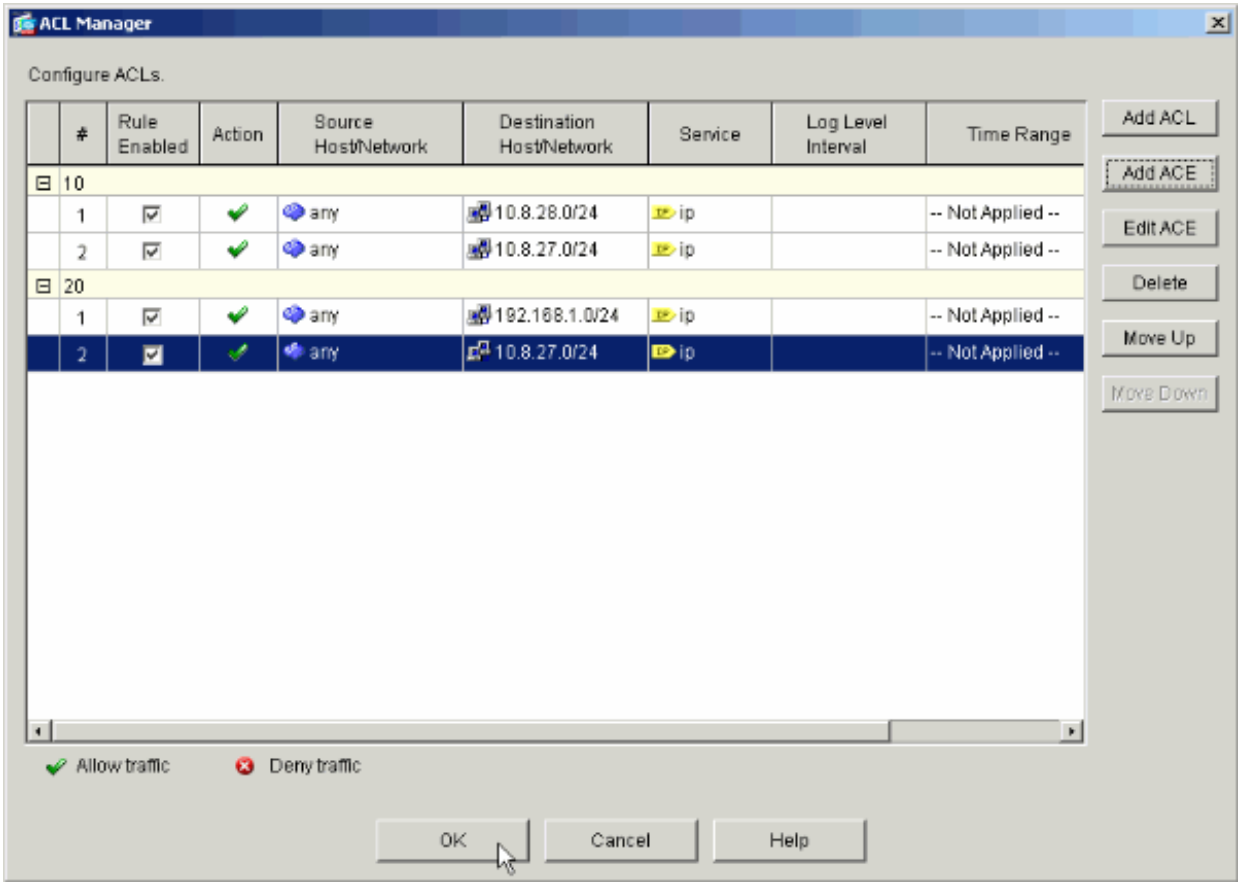
17. Clique em Apply e, se solicitado, clique em Send para adicionar a alteração à configuração do PIX.

    Se a Diretiva de Grupo já tiver sido selecionada, você poderá receber uma mensagem informando "Nenhuma alteração foi feita". Click OK.

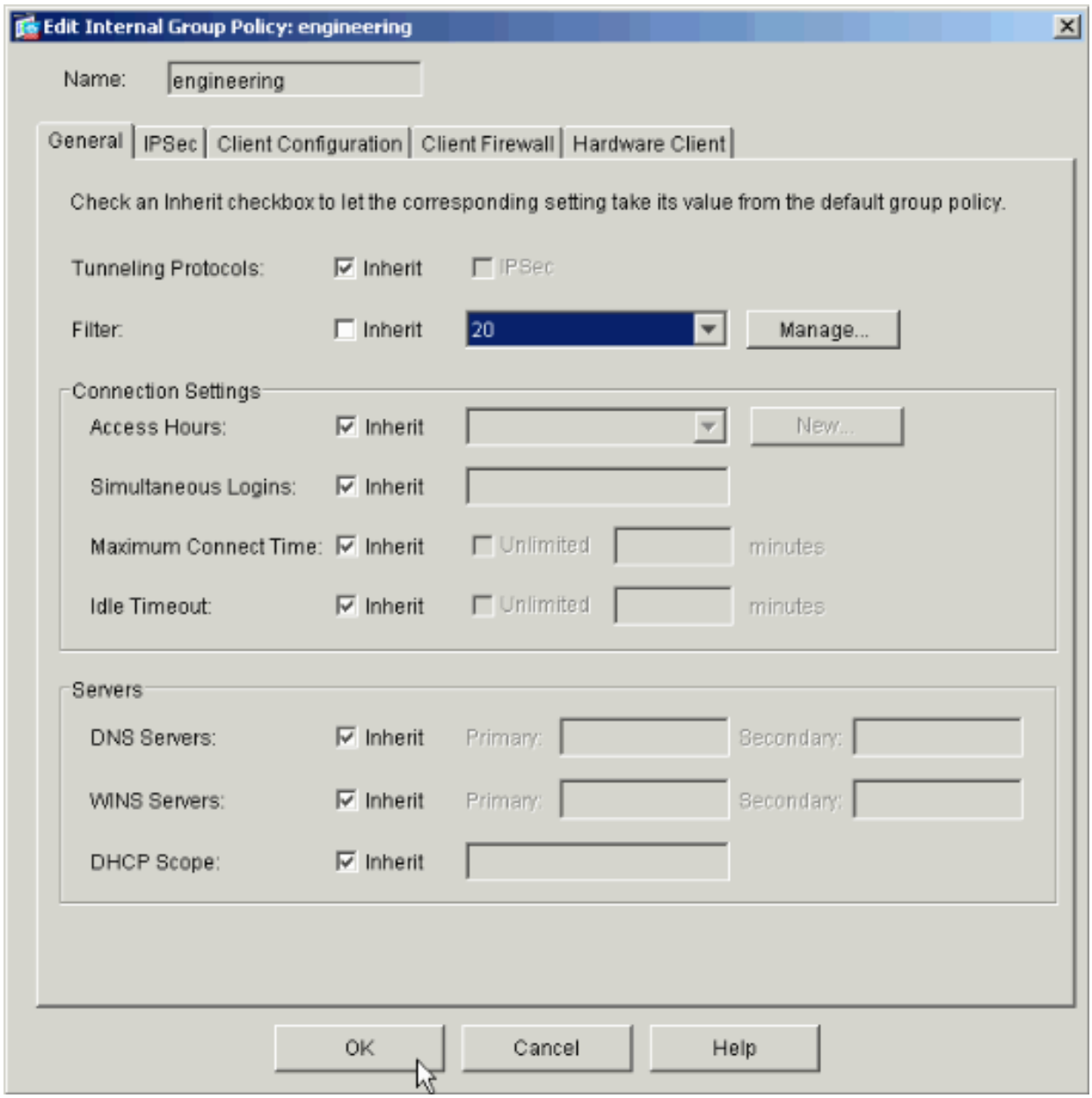
18. Repita as etapas de 2 a 17 para todos os grupos de túnel adicionais aos quais você deseja adicionar restrições.

    Neste exemplo de configuração, também é necessário restringir o acesso dos engenheiros. Embora o procedimento seja o mesmo, estas são algumas janelas nas quais as diferenças são notáveis:

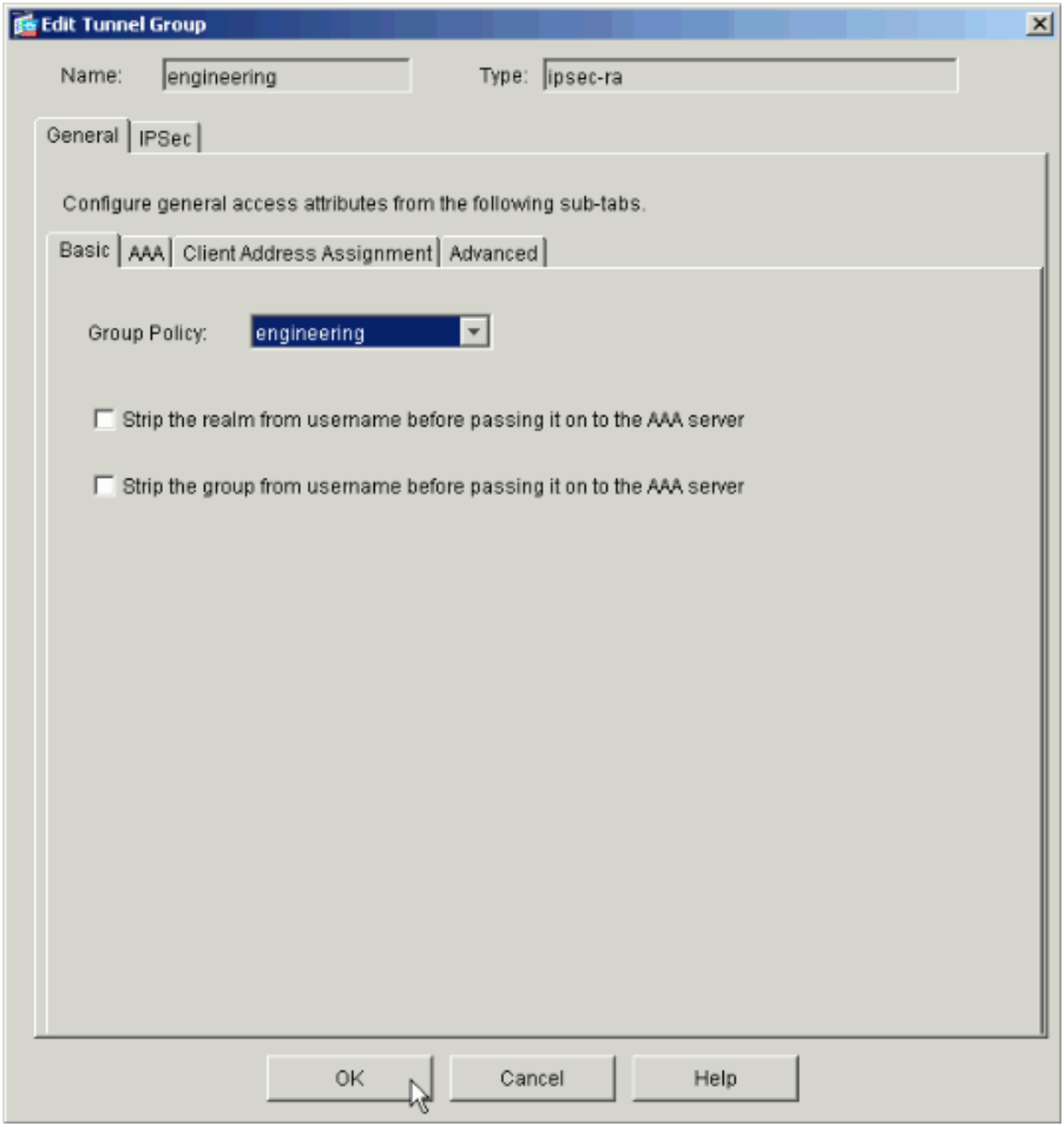
    - Nova lista de acesso 20



- Escolha Access List 20 como um filtro na Engineering Group Policy.



- Verifique se a diretiva de grupo de engenharia está definida para o grupo de túnel de engenharia.



Configurar o acesso via CLI

Conclua estas etapas para configurar o Security Appliance usando a CLI:

Observação: alguns dos comandos mostrados nesta saída são trazidos para uma segunda linha devido a razões espaciais.

1. Crie duas listas de controle de acesso diferentes (15 e 20) que são aplicadas aos usuários quando eles se conectam à VPN de acesso remoto. Essa lista de acesso é chamada posteriormente na configuração.

```
<#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
```

2. Crie dois pools de endereços VPN diferentes. Crie um para Folha de Pagamento e um para os usuários remotos do Engineering.

```
<#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. Crie políticas para Folha de Pagamento que se apliquem somente a elas quando se conectarem.

<#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. Esta etapa é igual à etapa 3, exceto que é para o grupo Engenharia.

<#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.
```

5. Crie usuários locais e designe os atributos recém-criados a esses usuários para restringir seu acesso aos recursos.

```
<#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. Crie grupos de túnel que contenham políticas de conexão para os usuários do Payroll.

```
<#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. Crie grupos de túneis que contenham políticas de conexão para os usuários do Engineering.

```
<#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
```

Depois que a configuração for inserida, você poderá ver esta área destacada em sua configuração:

Nome do dispositivo 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 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
```

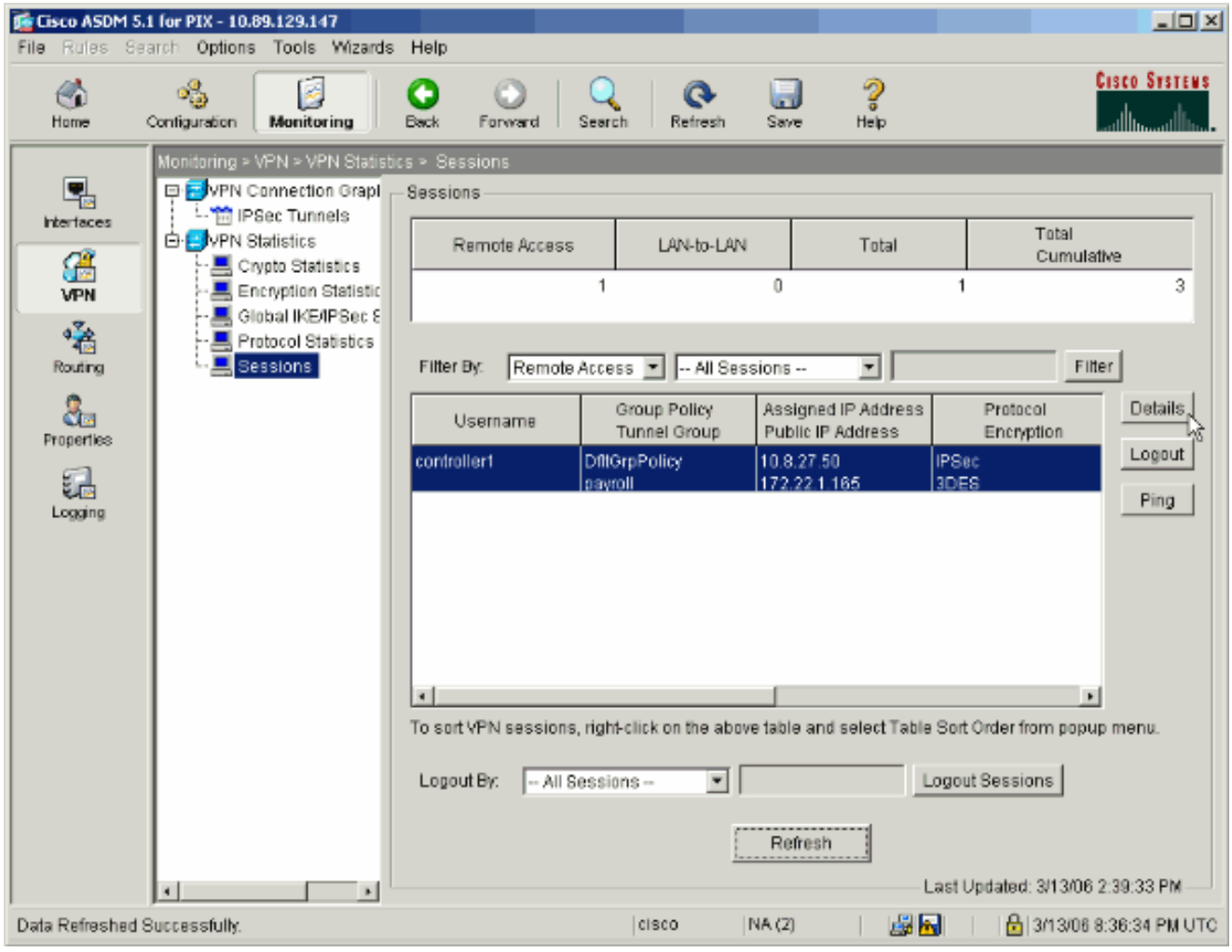
```
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:0e579c85004dcfb4071cb561514a392b
: end
ASA-AIP-CLI(config)#
```

Verificar

Use os recursos de monitoramento do ASDM para verificar sua configuração:

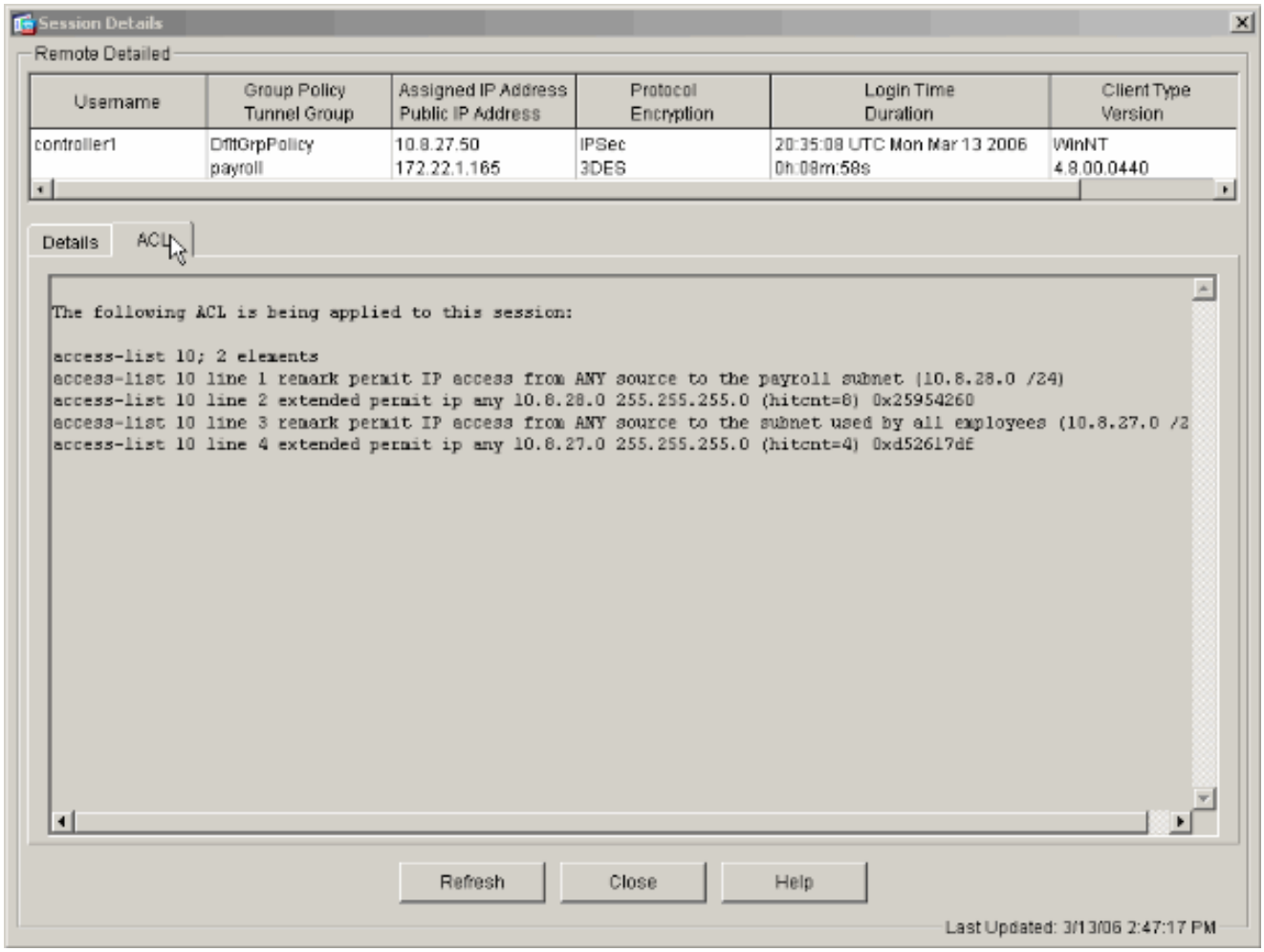
1. Selecione Monitoring > VPN > VPN Statistics > Sessions.

   Você vê as sessões de VPN ativas no PIX. Selecione a sessão na qual está interessado e clique em Details.



2. Selecione a guia ACL.

   O `hitcnts da` ACL reflete o tráfego que flui pelo túnel do cliente para a(s) rede(s) permitida(s).



Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Exemplo de Configuração do Cisco ASA 5500 Series Adaptive Security Appliances ASA como um Servidor VPN Remoto Usando o ASDM
- Exemplos de Configuração e Notas Técnicas dos Dispositivos de Segurança Cisco PIX 500 Series
- Exemplos de configuração e notas técnicas dos dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Exemplos de configuração e notas técnicas do Cisco VPN Client
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.