PIX/ASA 7.x ASDM : limiter l'accès réseau des utilisateurs VPN d'accès à distance

Table des matières

Introduction

Ce document fournit un exemple de configuration du Cisco Adaptive Security Device Manager (ASDM) pour limiter ce à quoi les utilisateurs du VPN d'accès à distance des réseaux internes peuvent accéder derrière l'appliance de sécurité PIX ou l'appliance de sécurité adaptable (ASA). Vous pouvez limiter les utilisateurs du VPN d'accès à distance aux seules zones du réseau auxquelles vous souhaitez qu'ils puissent accéder lorsque vous :

1. Créez des listes de contrôle d'accès.
2. Associez-les aux stratégies de groupe.
3. Associez ces stratégies de groupe à des groupes de tunnels.

Référez-vous à Configuration du concentrateur Cisco VPN 3000 pour le blocage avec des filtres et l'affectation de filtre RADIUS afin d'en savoir plus sur le scénario où le concentrateur VPN bloque l'accès des utilisateurs VPN.

Conditions préalables

Exigences

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Le PIX peut être configuré en utilisant l'ASDM.

Remarque : référez-vous à Autoriser l'accès HTTPS pour ASDM afin de permettre au PIX d'être configuré par l'ASDM.

- Vous disposez d'au moins une configuration VPN d'accès à distance correcte connue.

  Remarque : si vous n'avez pas de telles configurations, référez-vous à ASA en tant que serveur VPN distant utilisant l'exemple de configuration ASDM pour plus d'informations sur la façon de configurer une configuration VPN d'accès distant correcte.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appliance de sécurité de la gamme Cisco Secure PIX 500 version 7.1(1)

  Remarque : les appliances de sécurité PIX 501 et 506E ne prennent pas en charge la version 7.x.

- Cisco Adaptive Security Device Manager version 5.1(1)

  Remarque : l'ASDM est uniquement disponible dans PIX ou ASA 7.x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

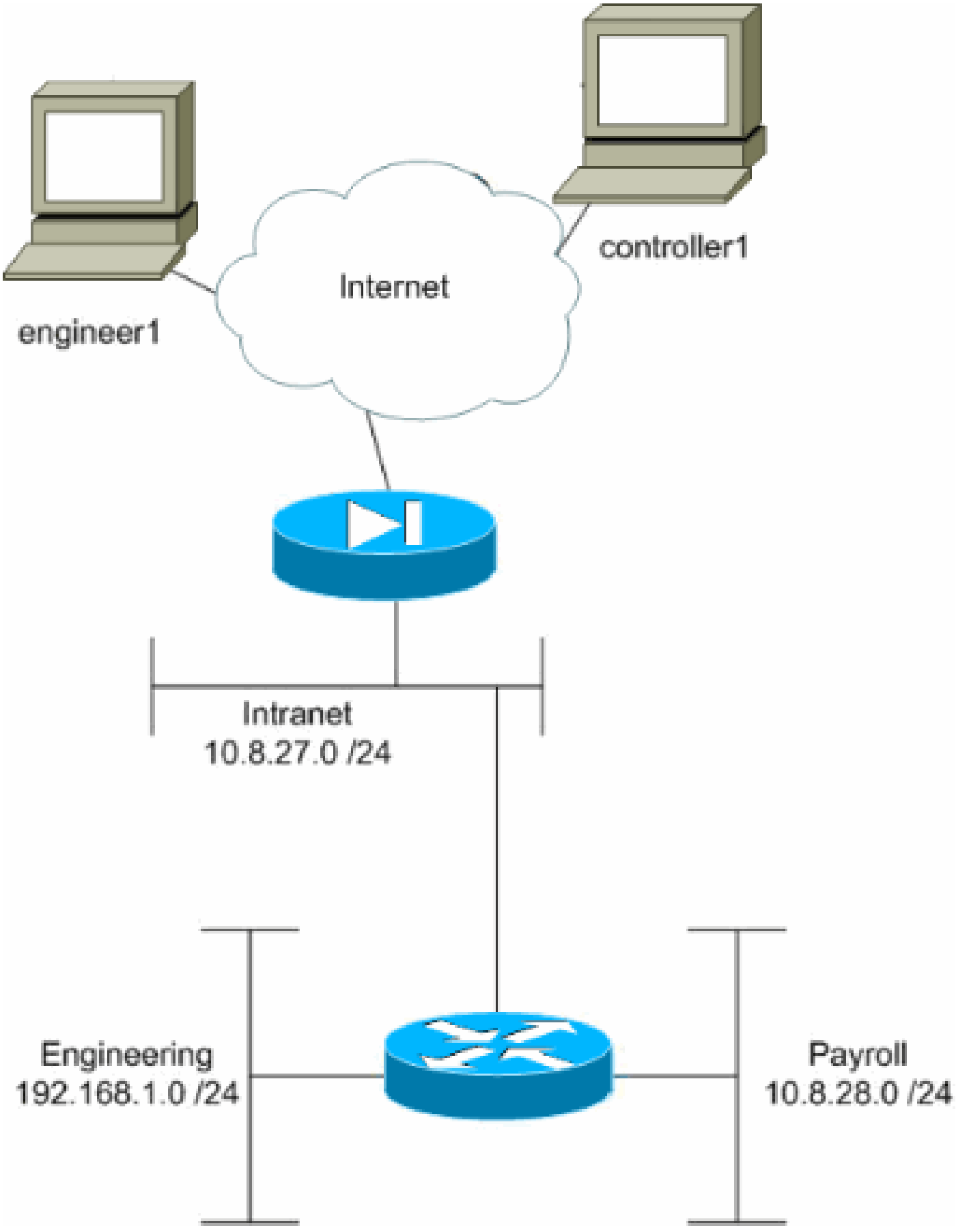
Produits connexes

Cette configuration peut également être utilisée avec les versions de matériel et de logiciel suivantes :

- Appliance de sécurité adaptatif de la gamme Cisco ASA 5500 version 7.1(1)

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Dans cet exemple de configuration, un petit réseau d'entreprise avec trois sous-réseaux est supposé. Ce schéma illustre la topologie. Les trois sous-réseaux sont Intranet, Ingénierie et Paie. L'objectif de cet exemple de configuration est d'autoriser le personnel de paie à accéder à

distance aux sous-réseaux Intranet et Payroll et de l'empêcher d'accéder au sous-réseau Ingénierie. En outre, les ingénieurs doivent pouvoir accéder à distance aux sous-réseaux Intranet et Ingénierie, mais pas au sous-réseau Paie. L'utilisateur de paie dans cet exemple est « controller1 ». L'utilisateur ingénieur dans cet exemple est "ingénieur1".

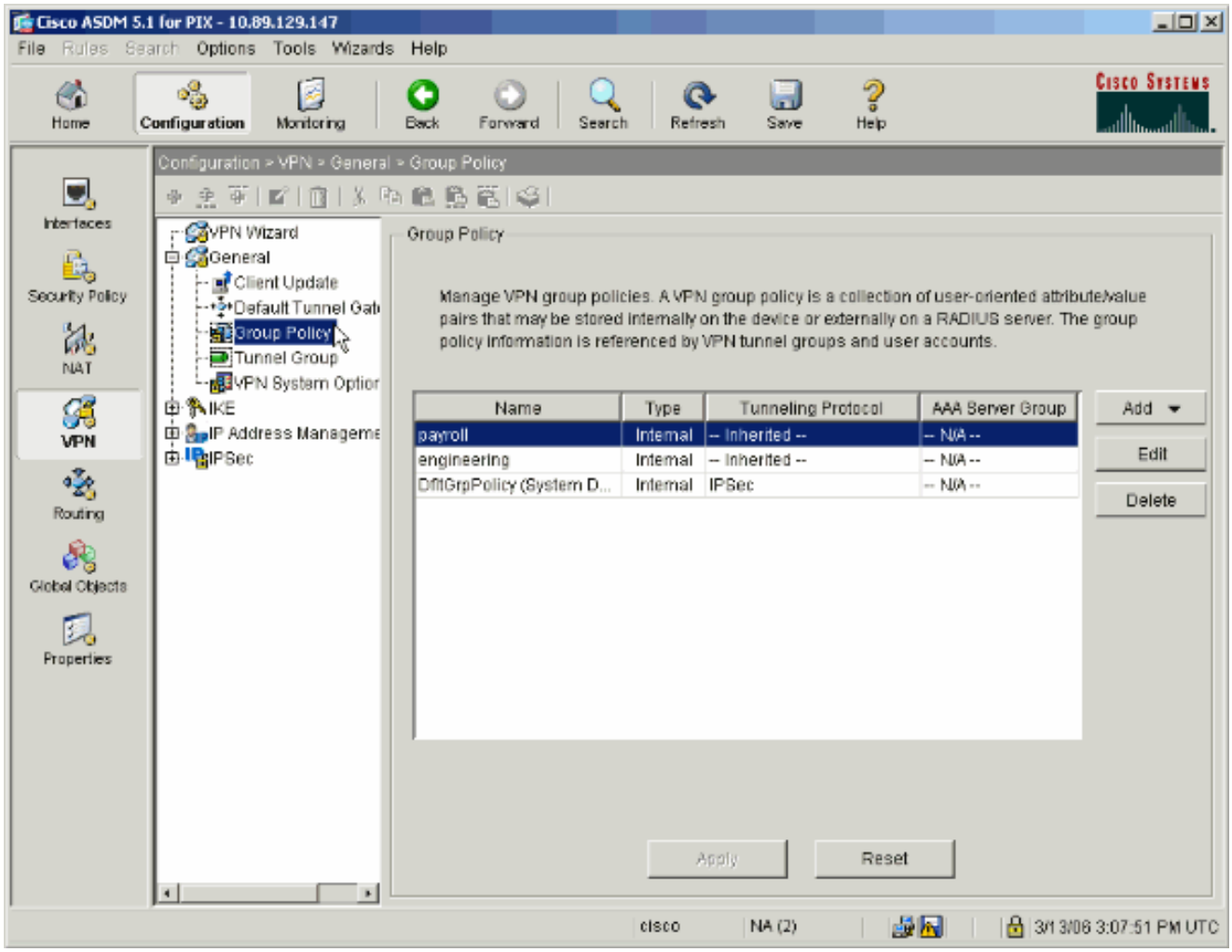
Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

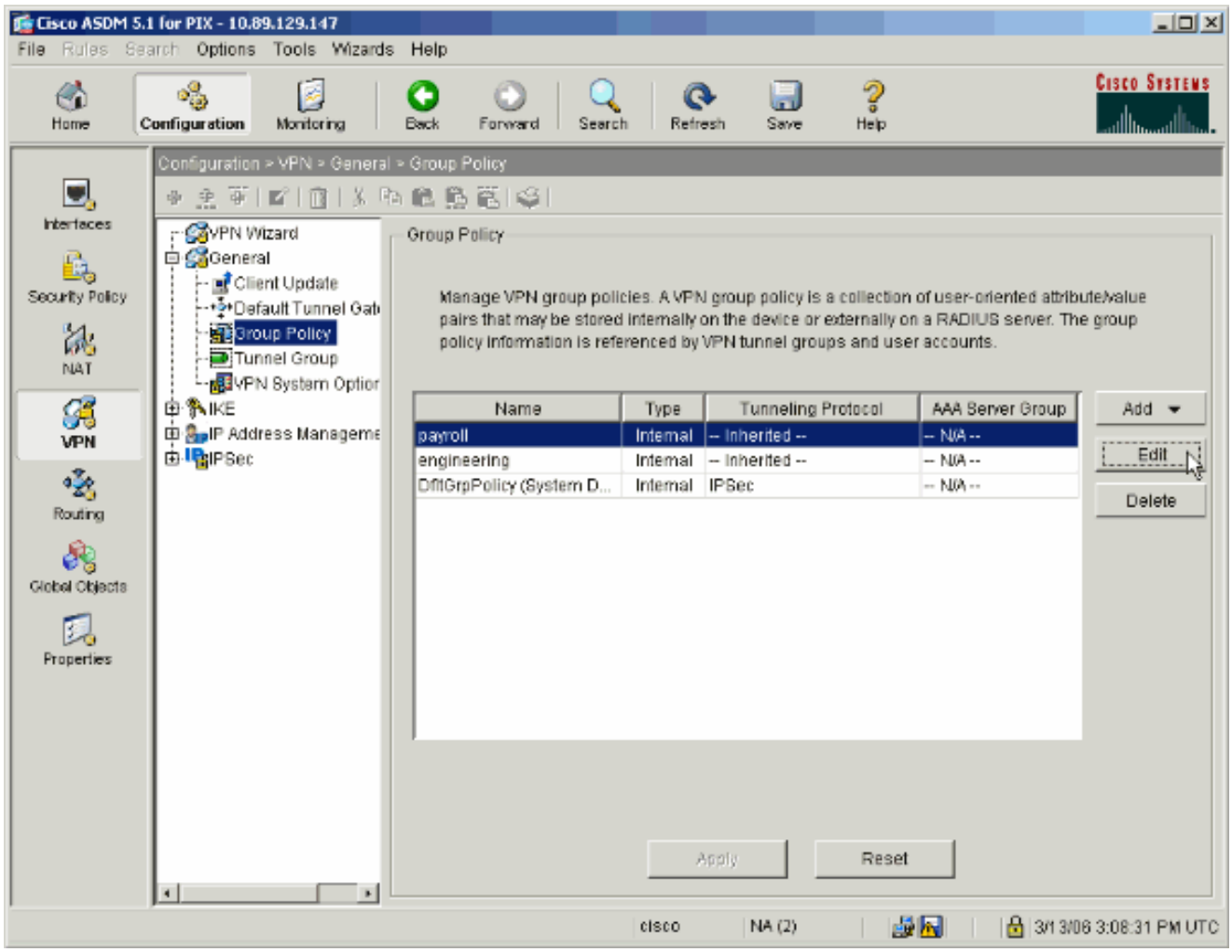
Configurer l'accès via ASDM

Complétez ces étapes pour configurer l'appliance de sécurité PIX à l'aide de l'ASDM :

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

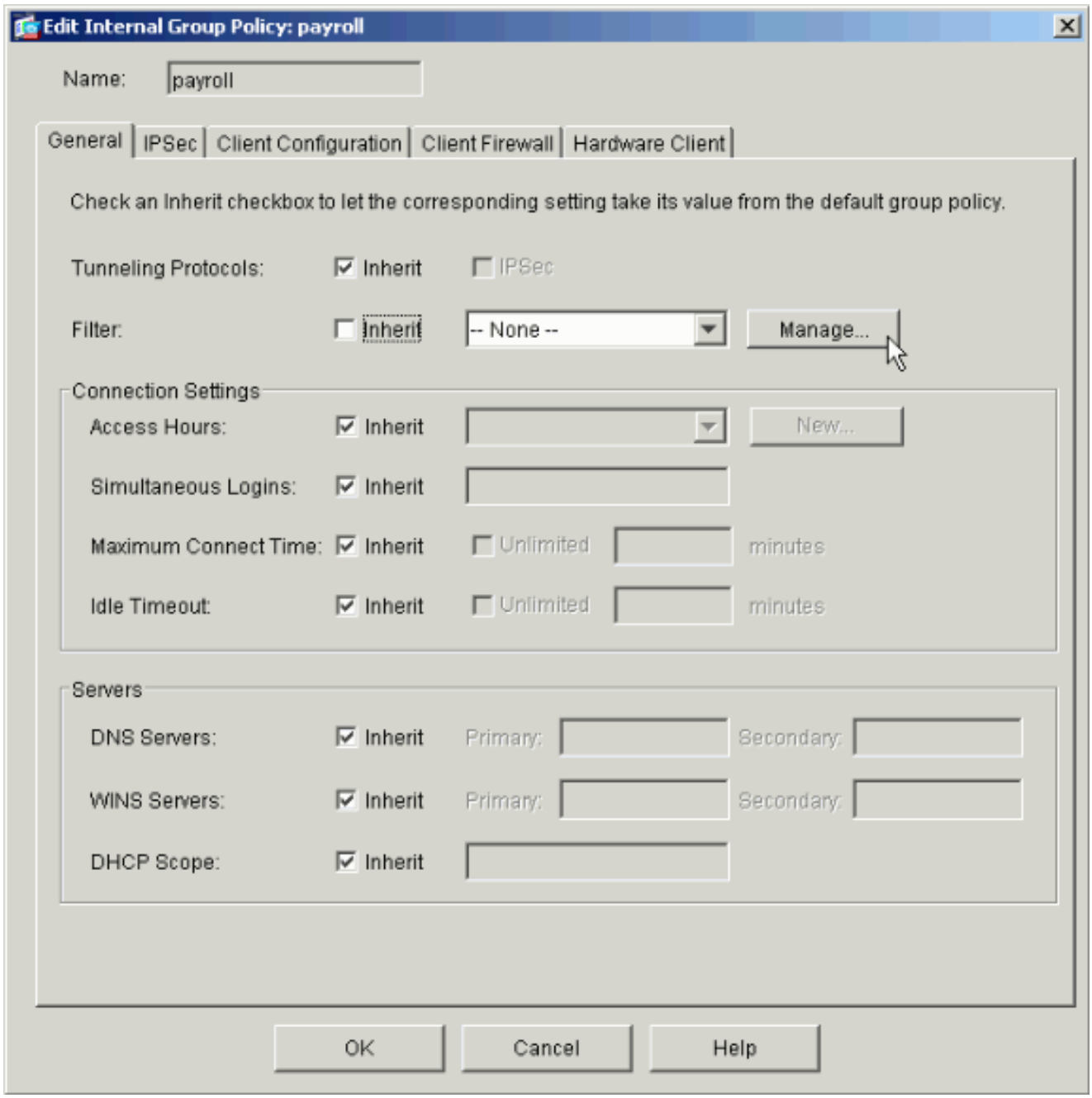


2. En fonction des étapes suivies pour configurer les groupes de tunnels sur le PIX, des stratégies de groupe peuvent déjà exister pour les groupes de tunnels dont vous souhaitez restreindre les utilisateurs. Si une stratégie de groupe appropriée existe déjà, sélectionnez-la et cliquez sur Modifier. Sinon, cliquez sur Ajouter et choisissez Stratégie de groupe interne....

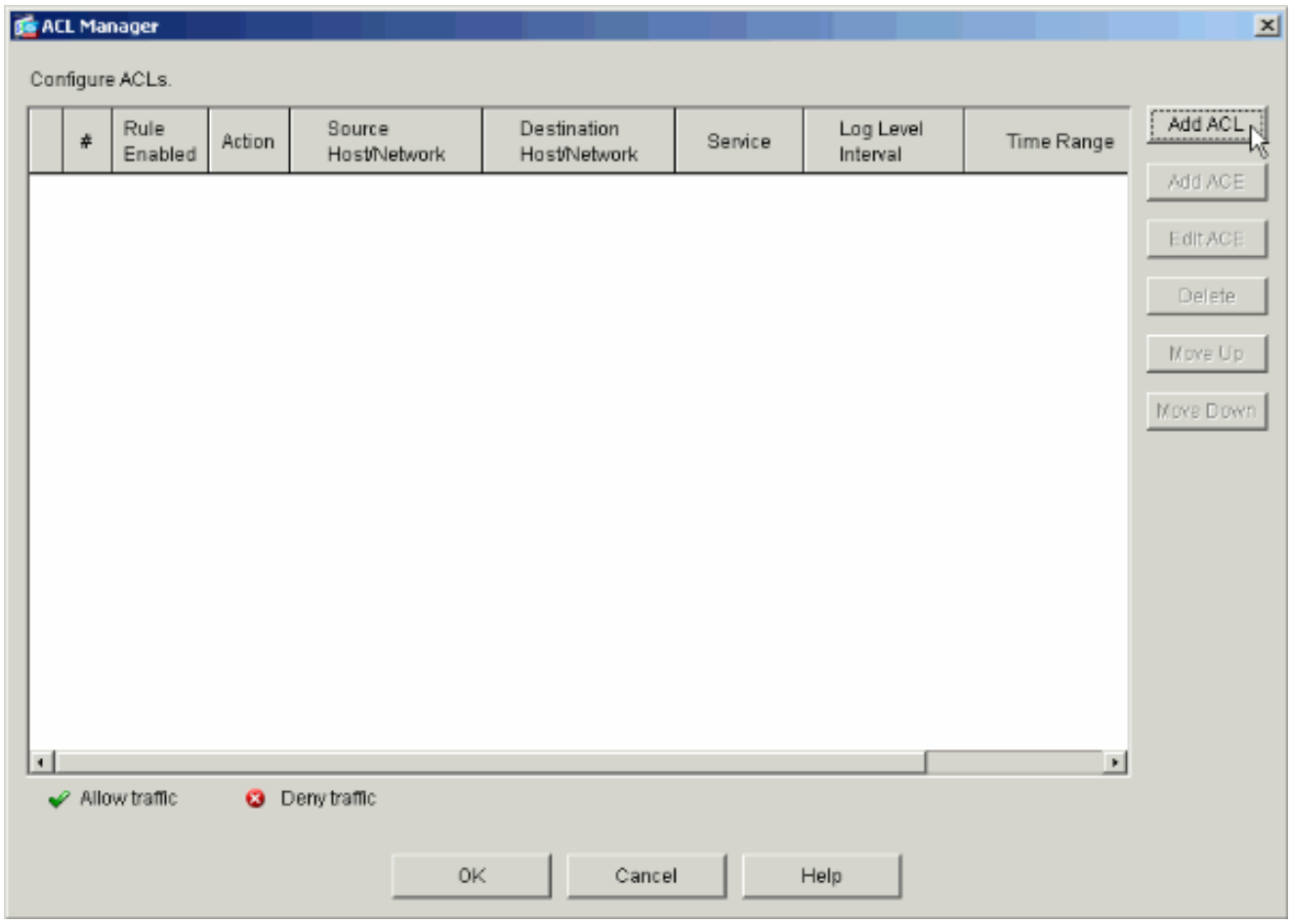


3. Si nécessaire, entrez ou modifiez le nom de la stratégie de groupe en haut de la fenêtre qui s'ouvre.

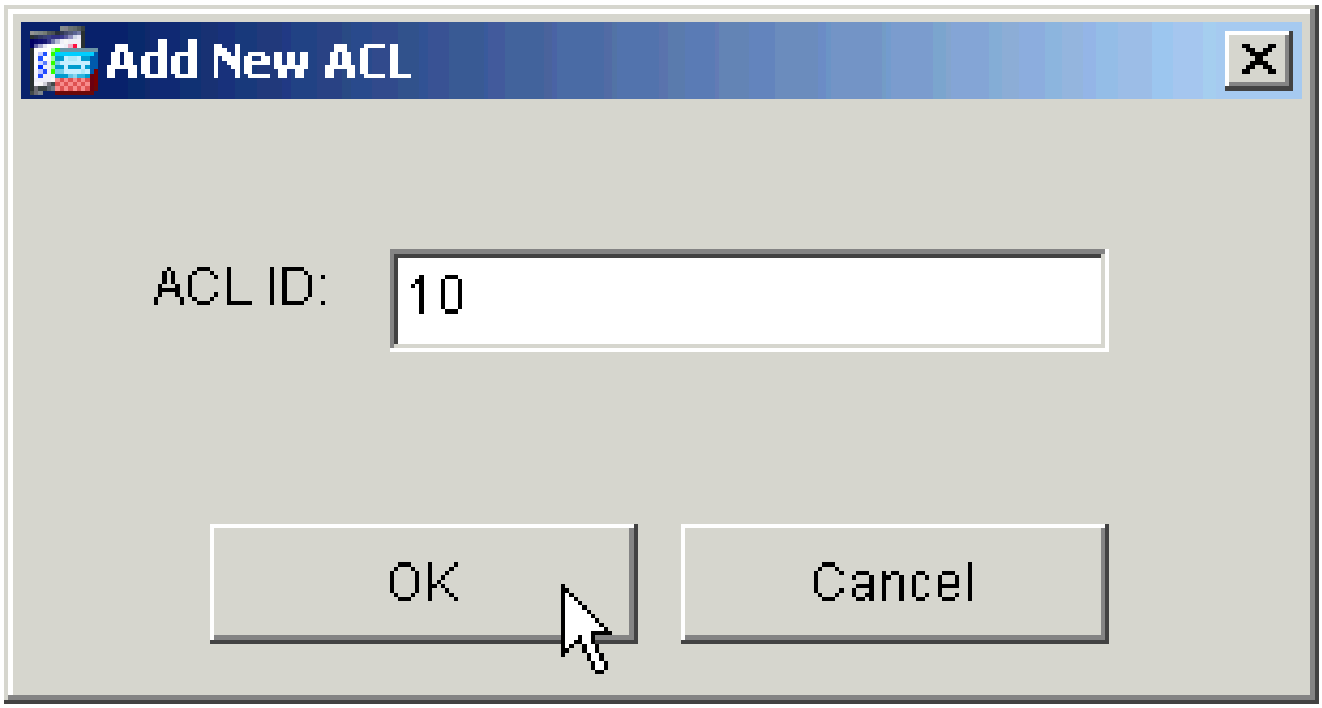
4. Dans l'onglet Général, décochez la case Hériter en regard de Filtre, puis cliquez sur Gérer.



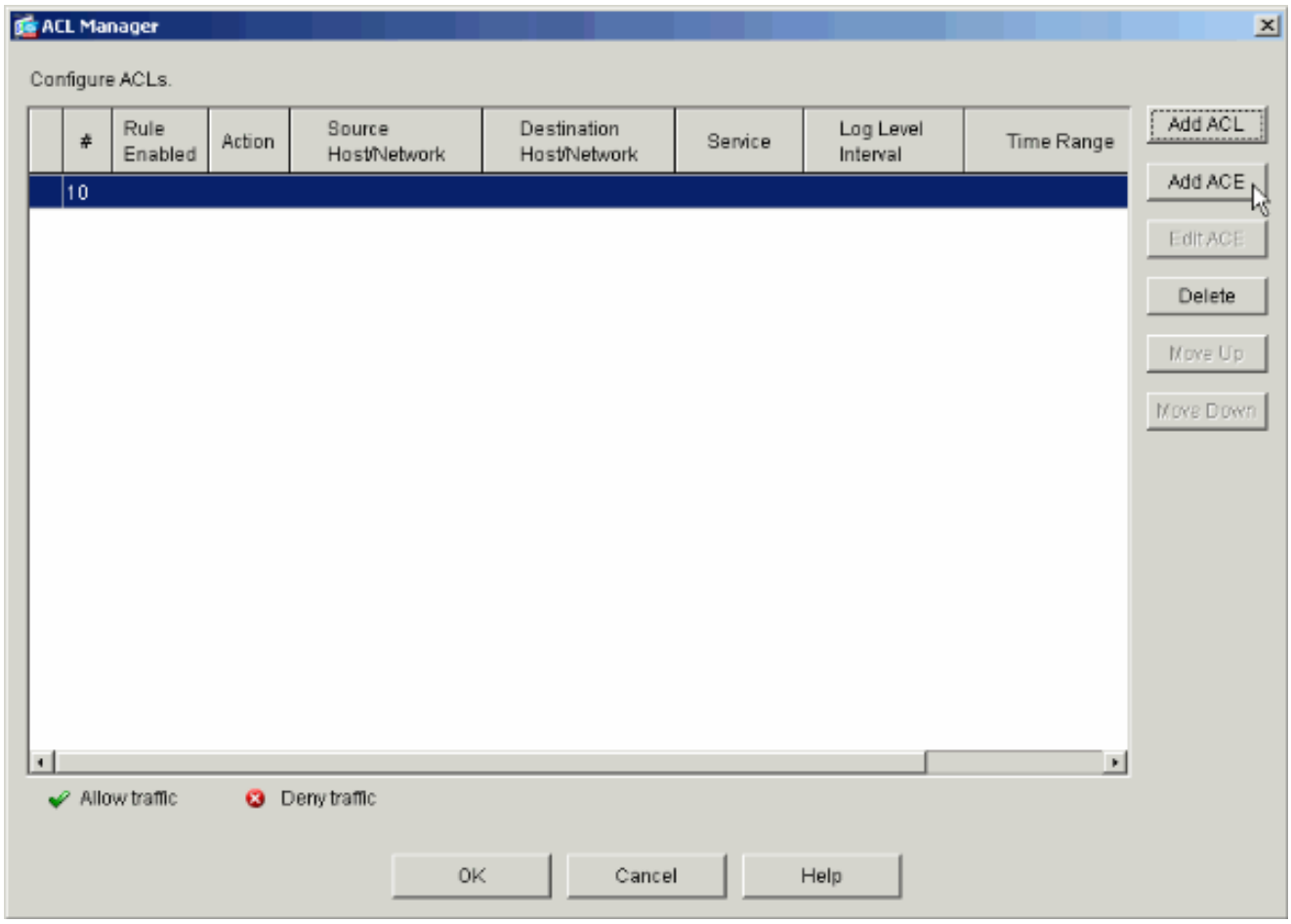
5. Cliquez sur Add ACL pour créer une nouvelle liste d'accès dans la fenêtre ACL Manager qui s'affiche.



6. Choisissez un numéro pour la nouvelle liste d'accès et cliquez sur OK.



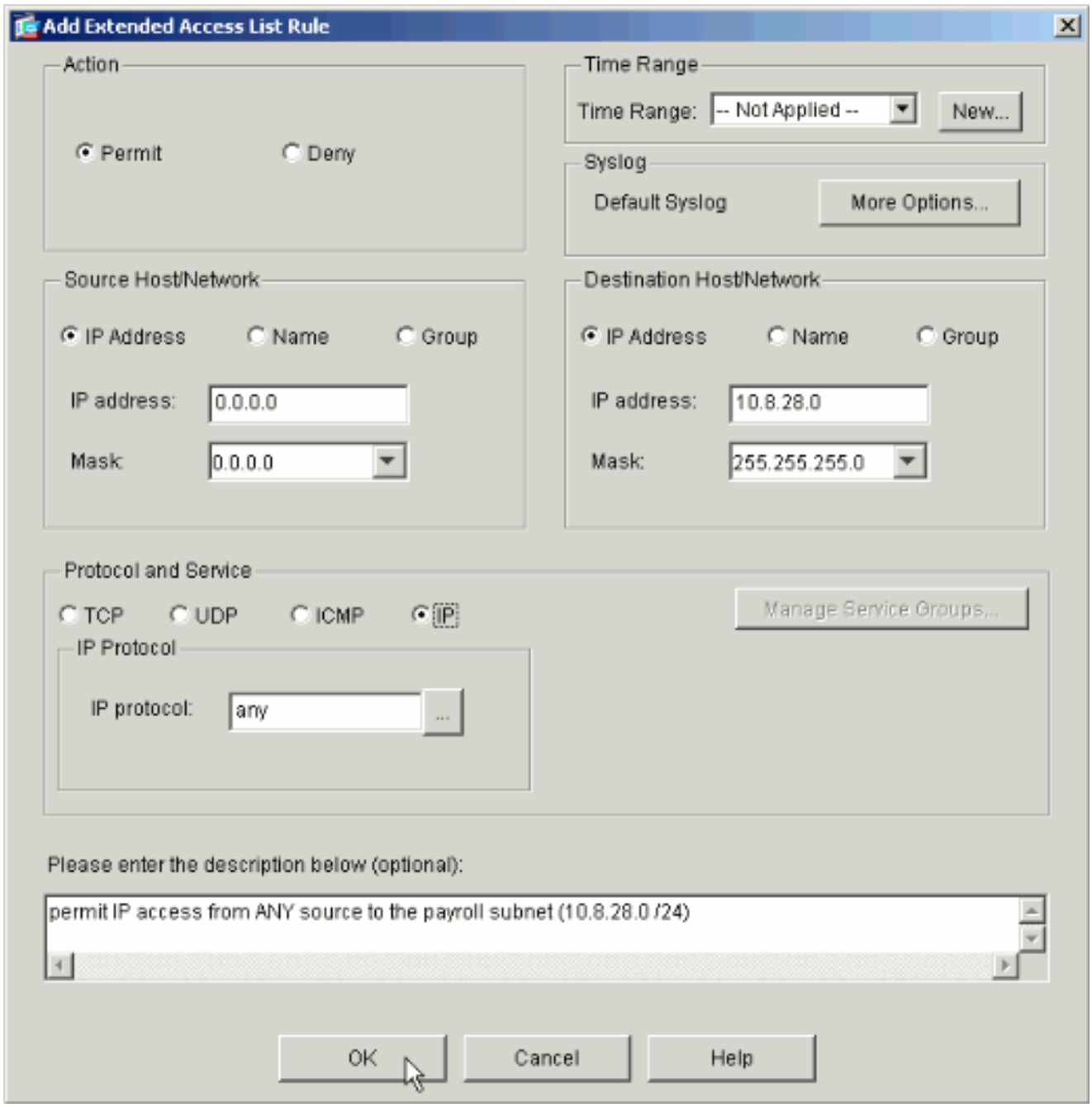
7. La nouvelle liste de contrôle d'accès étant sélectionnée à gauche, cliquez sur Add ACE pour ajouter une nouvelle entrée de contrôle d'accès à la liste.



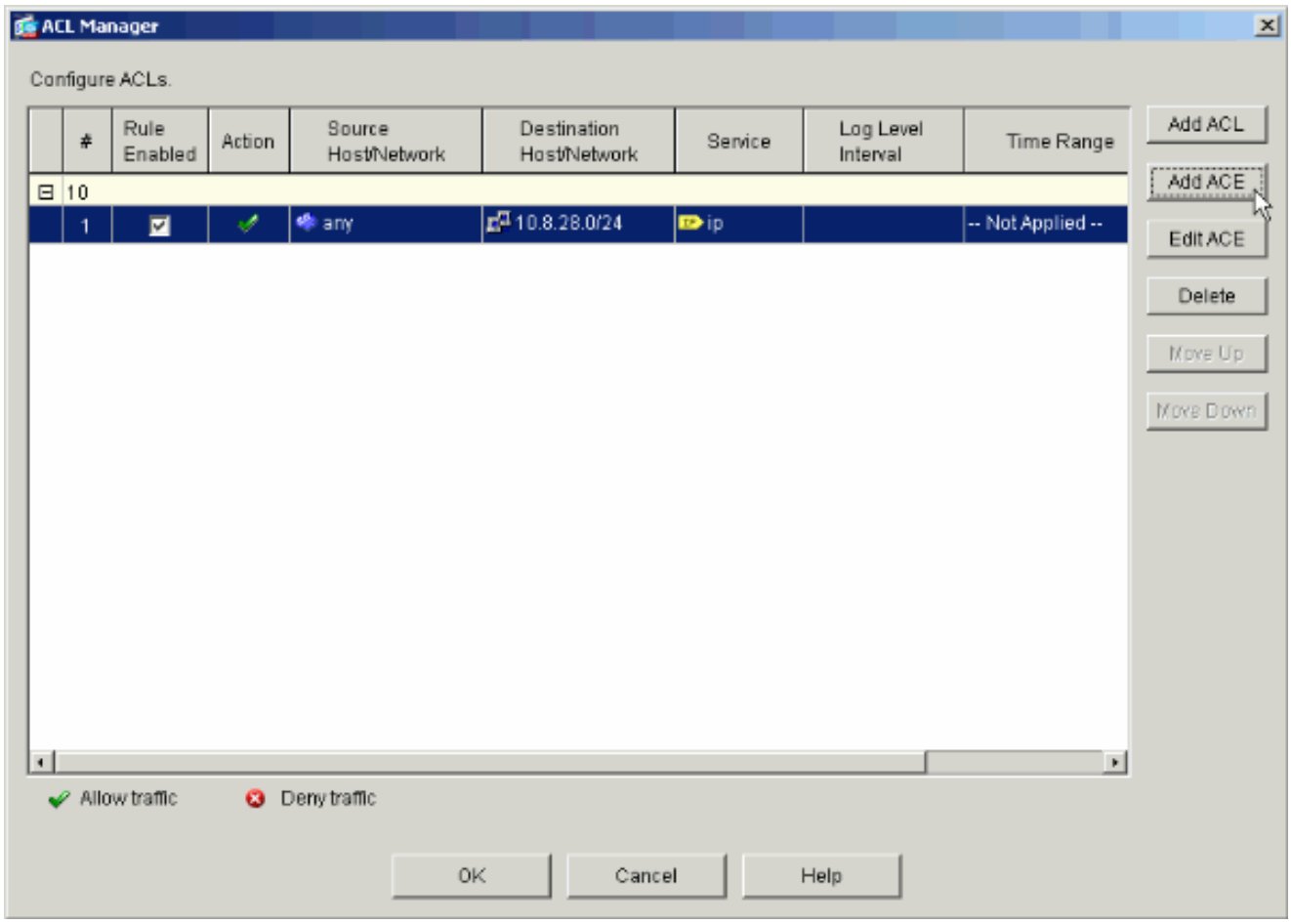
8. Définissez l'entrée de contrôle d'accès (ACE) que vous souhaitez ajouter.

   Dans cet exemple, le premier ACE de la liste de contrôle d'accès 10 autorise l'accès IP au sous-réseau Payroll à partir de n'importe quelle source.

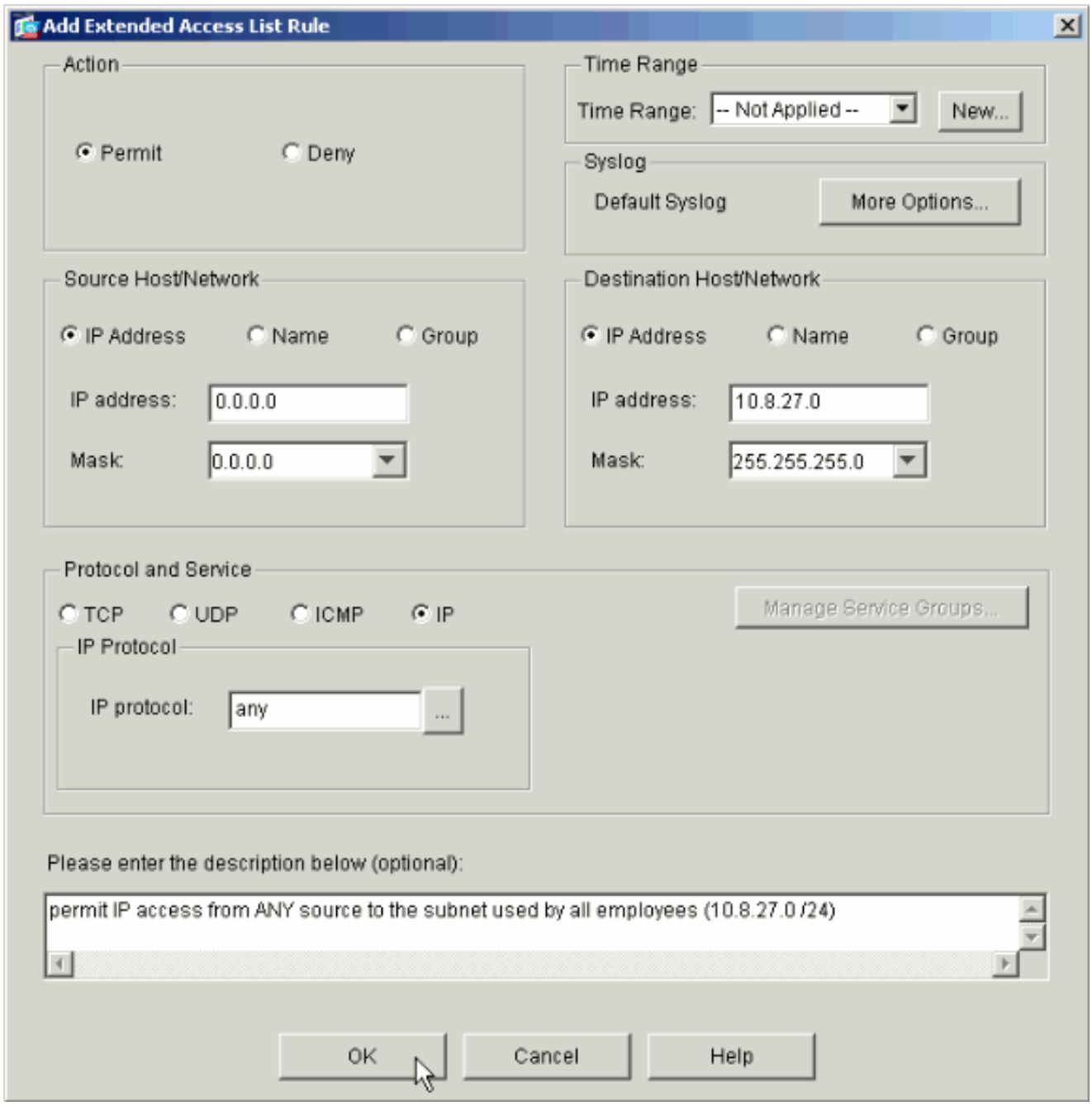
   Remarque : par défaut, ASDM sélectionne uniquement TCP comme protocole. Vous devez choisir IP si vous souhaitez autoriser ou refuser aux utilisateurs un accès IP complet. Cliquez sur OK quand vous avez terminé.



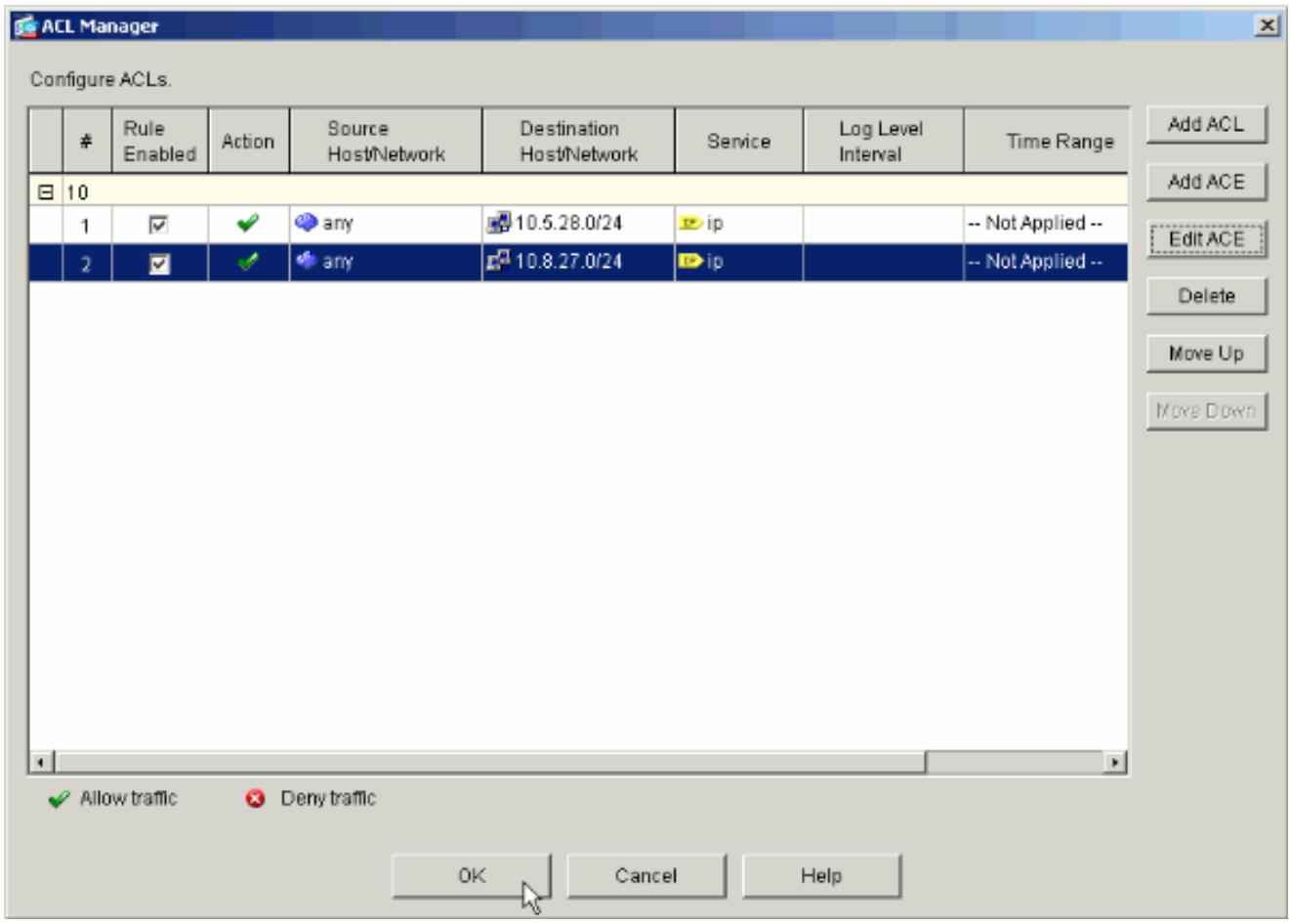
9. L'ACE que vous venez d'ajouter apparaît maintenant dans la liste. Choisissez à nouveau Add ACE pour ajouter des lignes supplémentaires à la liste d'accès.



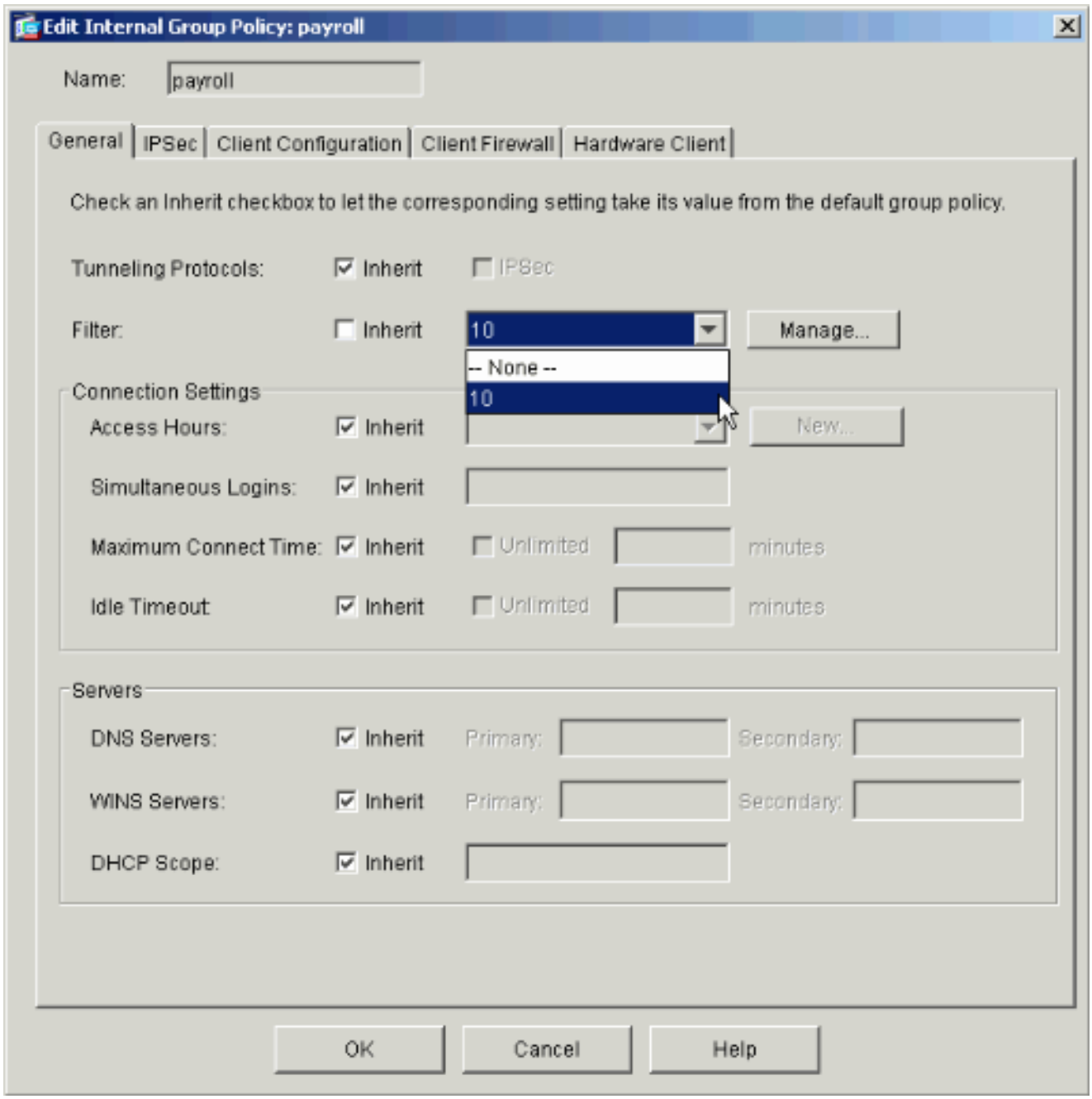
Dans cet exemple, une deuxième ACE est ajoutée à la liste de contrôle d'accès 10 afin d'autoriser l'accès au sous-réseau Intranet.



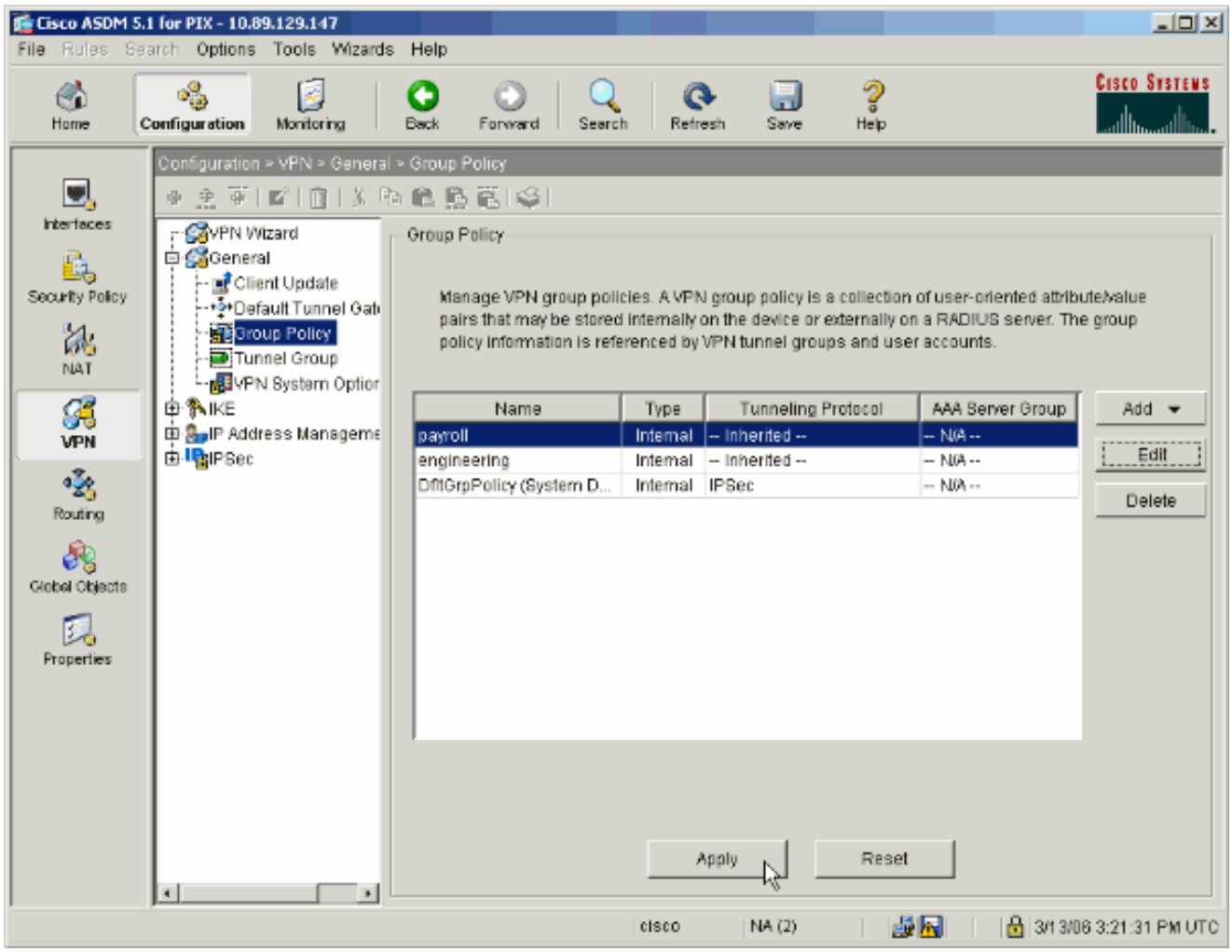
10. Cliquez sur OK une fois que vous avez terminé d'ajouter des ACE.



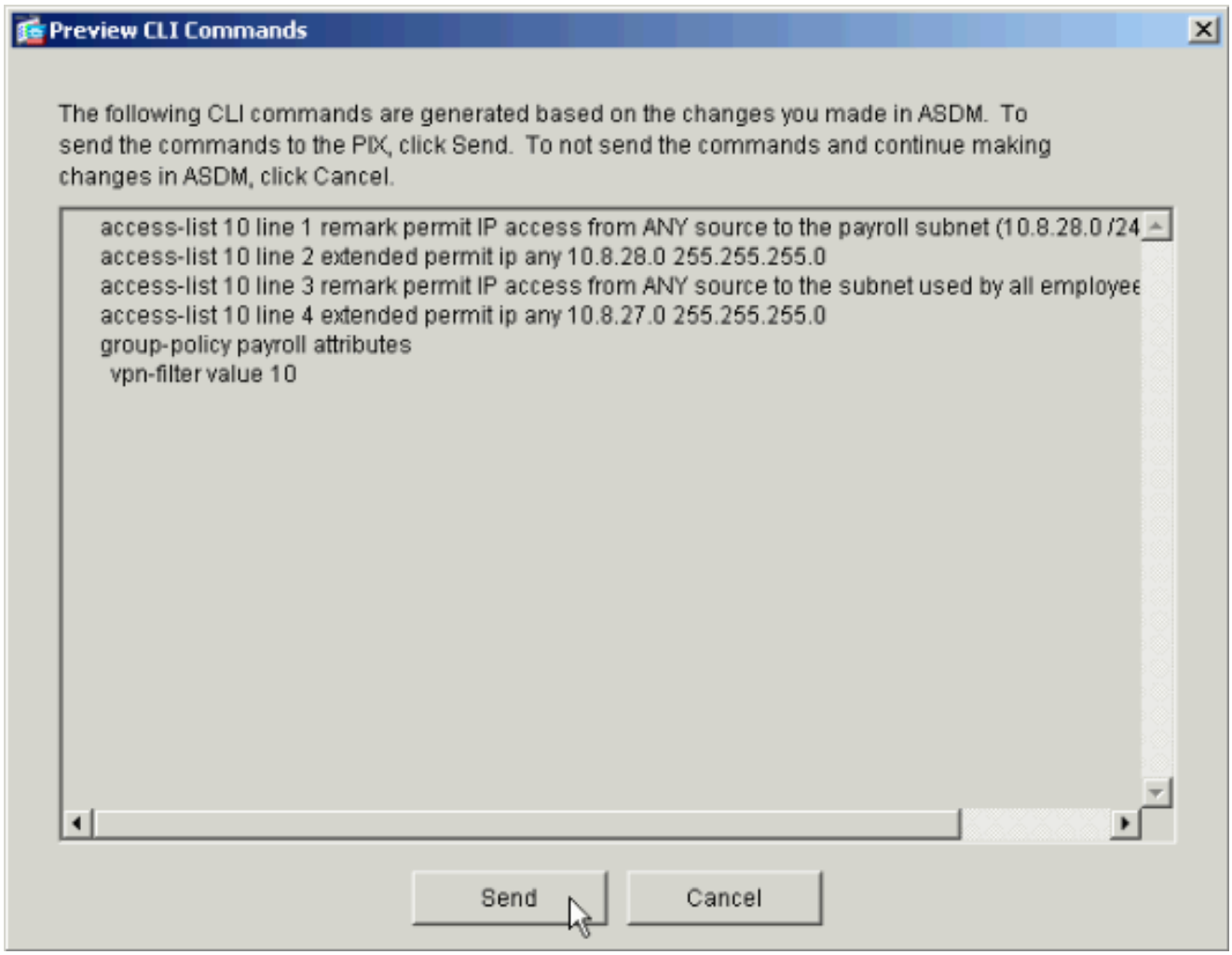
11. Sélectionnez la liste de contrôle d'accès que vous avez définie et renseignée au cours des dernières étapes comme filtre de votre stratégie de groupe. Cliquez sur OK lorsque vous avez terminé.



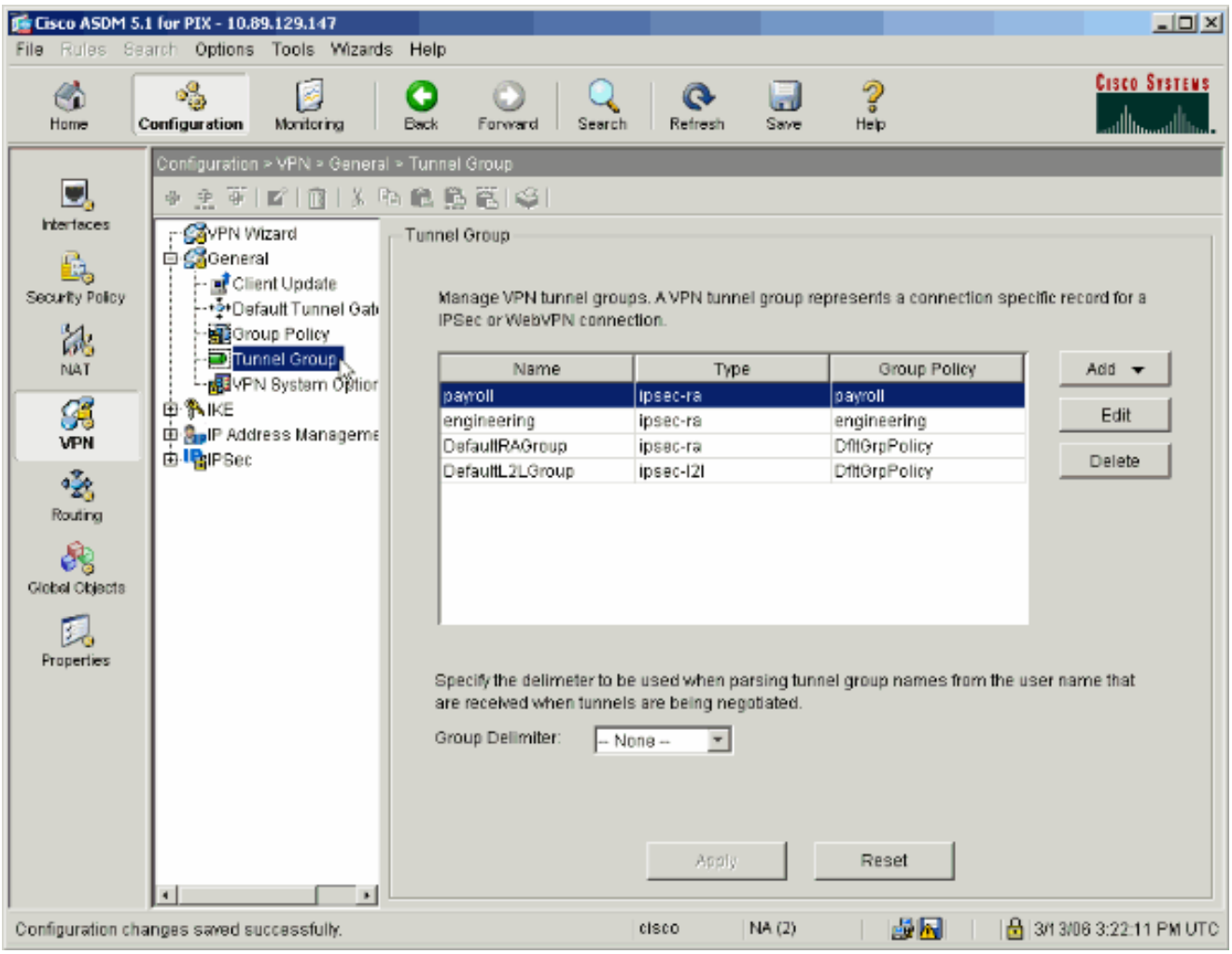
12. Cliquez sur Apply pour envoyer les modifications au PIX.



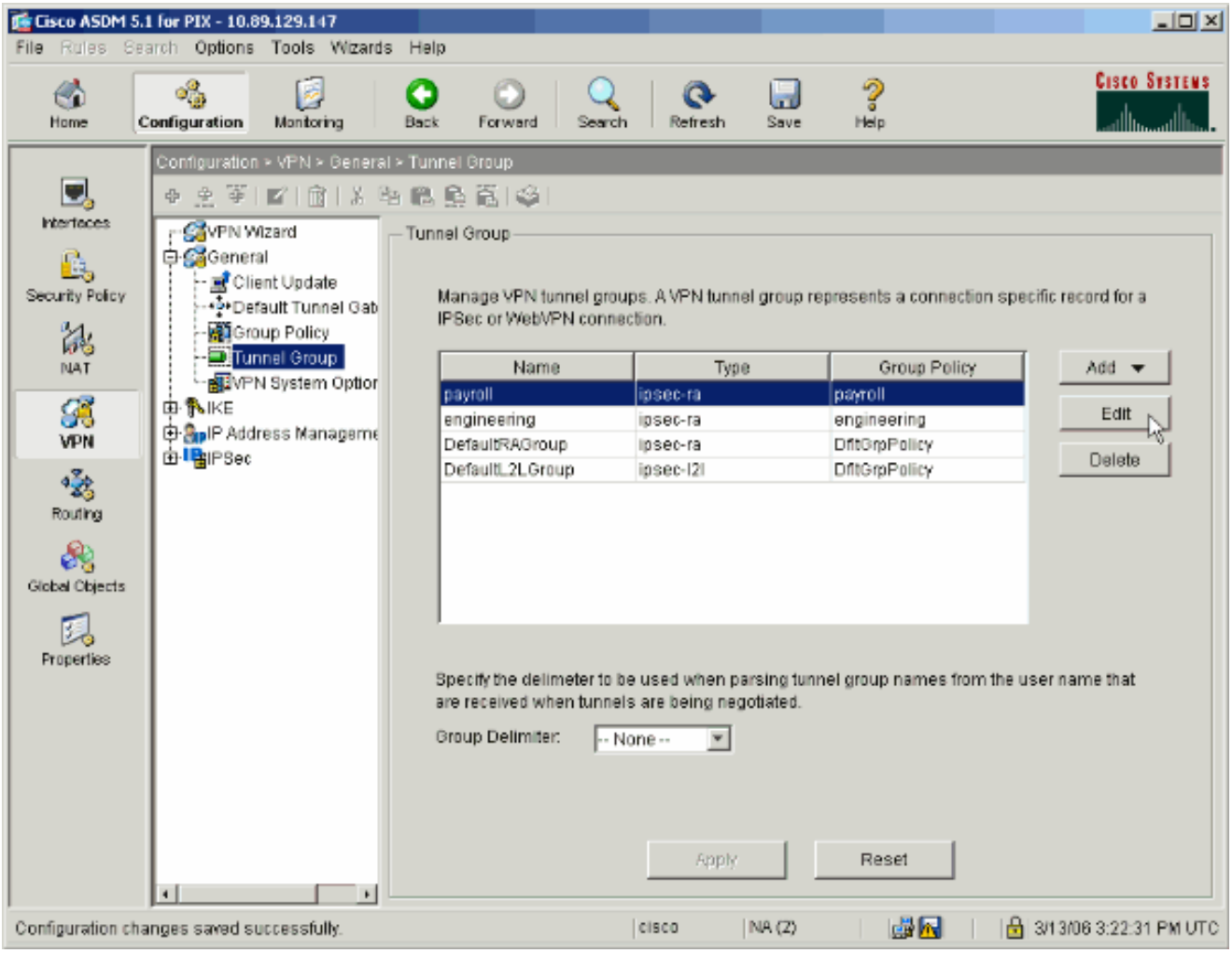
13. Si vous l'avez configuré pour le faire sous Options > Préférences, l'ASDM prévisualise les commandes qu'il est sur le point d'envoyer au PIX. Cliquez sur Envoyer.



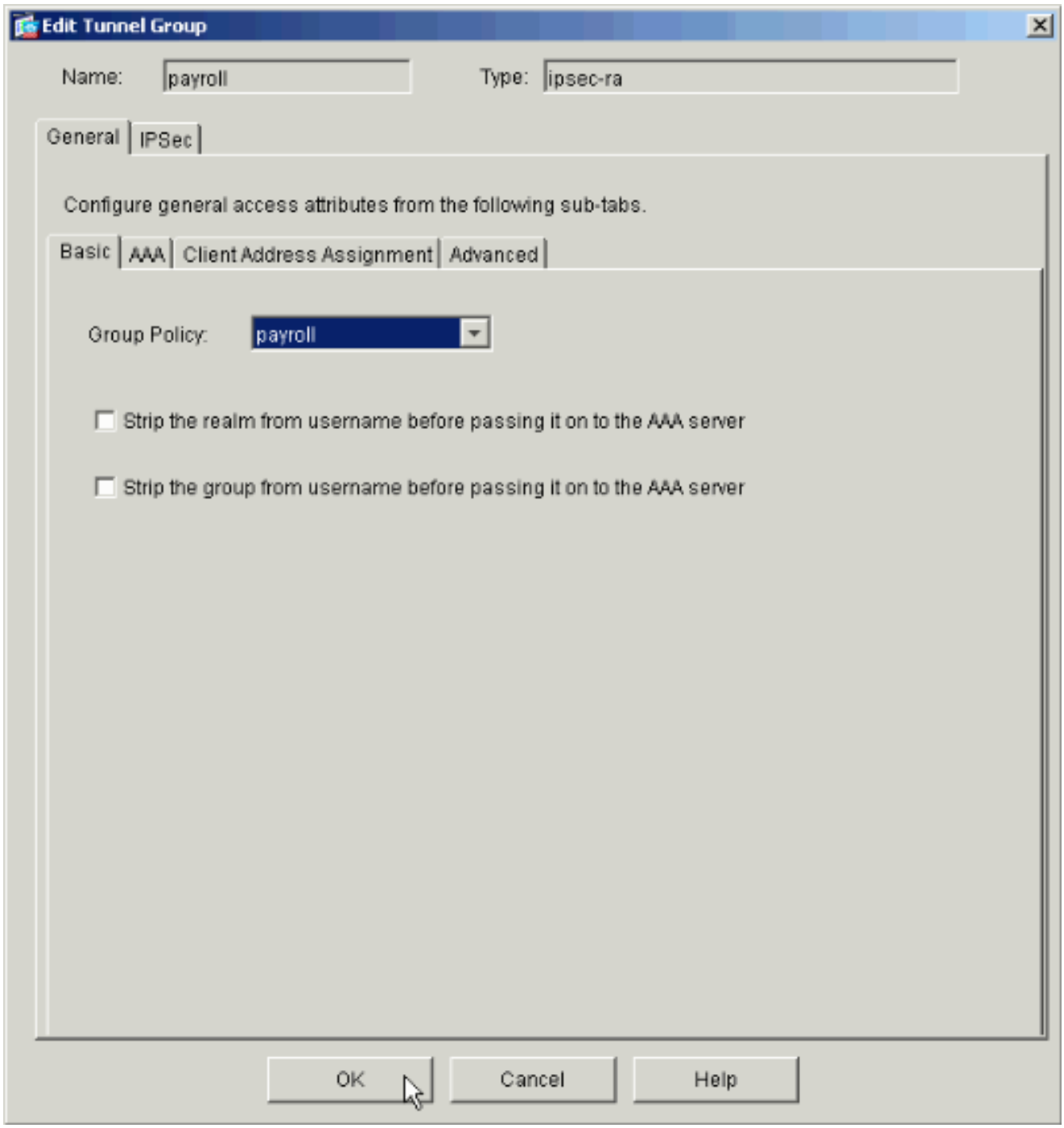
14. Appliquez la stratégie de groupe qui vient d'être créée ou modifiée au groupe de tunnels correct. Cliquez sur Tunnel Group dans le cadre de gauche.



15. Choisissez le groupe de tunnels auquel vous souhaitez appliquer la stratégie de groupe et cliquez sur Edit.



16. Si votre stratégie de groupe a été créée automatiquement (voir l'étape 2), vérifiez que la stratégie de groupe que vous venez de configurer est sélectionnée dans la liste déroulante. Si votre stratégie de groupe n'a pas été configurée automatiquement, sélectionnez-la dans la liste déroulante. Cliquez sur OK lorsque vous avez terminé.



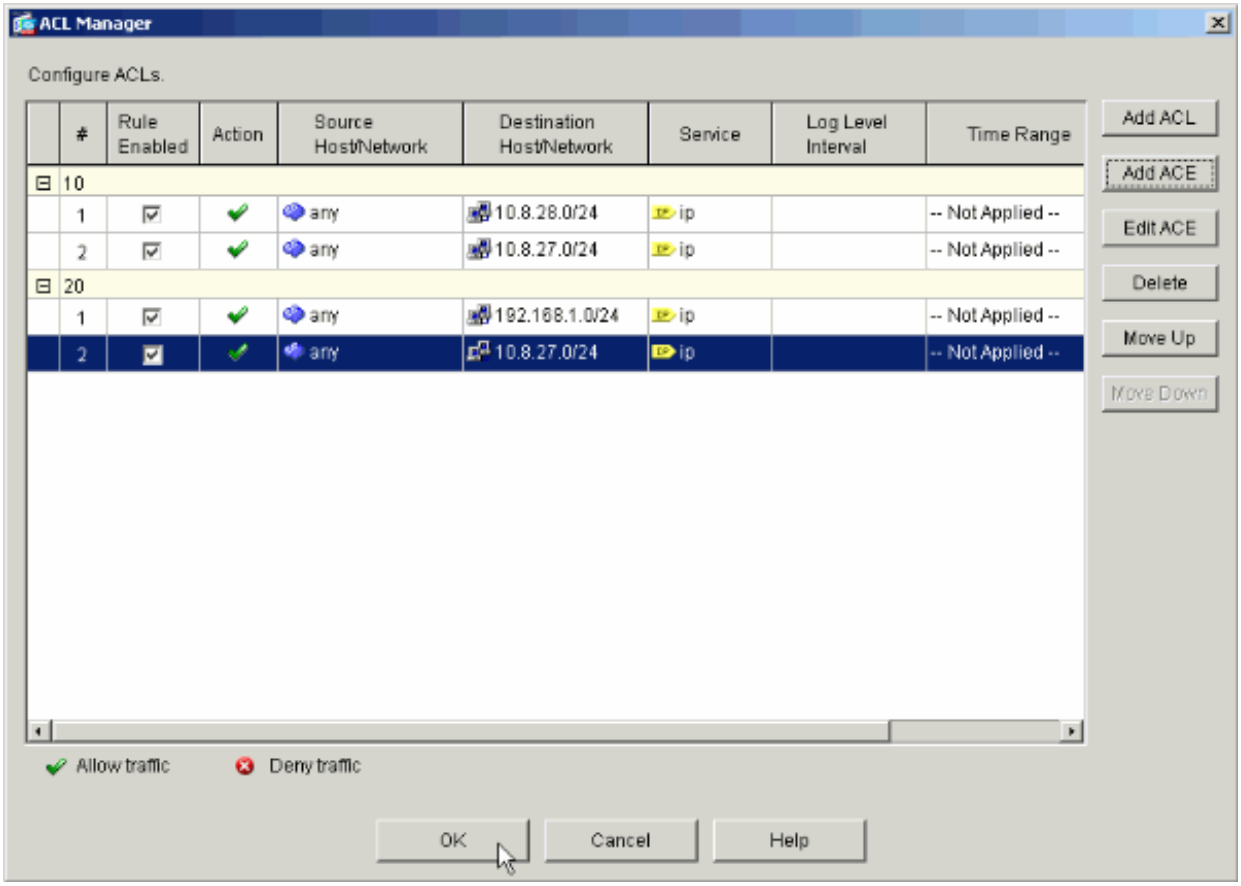
17. Cliquez sur Apply et, si vous y êtes invité, cliquez sur Send pour ajouter la modification à la configuration PIX.

    Si la stratégie de groupe a déjà été sélectionnée, vous pouvez recevoir un message indiquant « Aucune modification n'a été apportée ». Click OK.

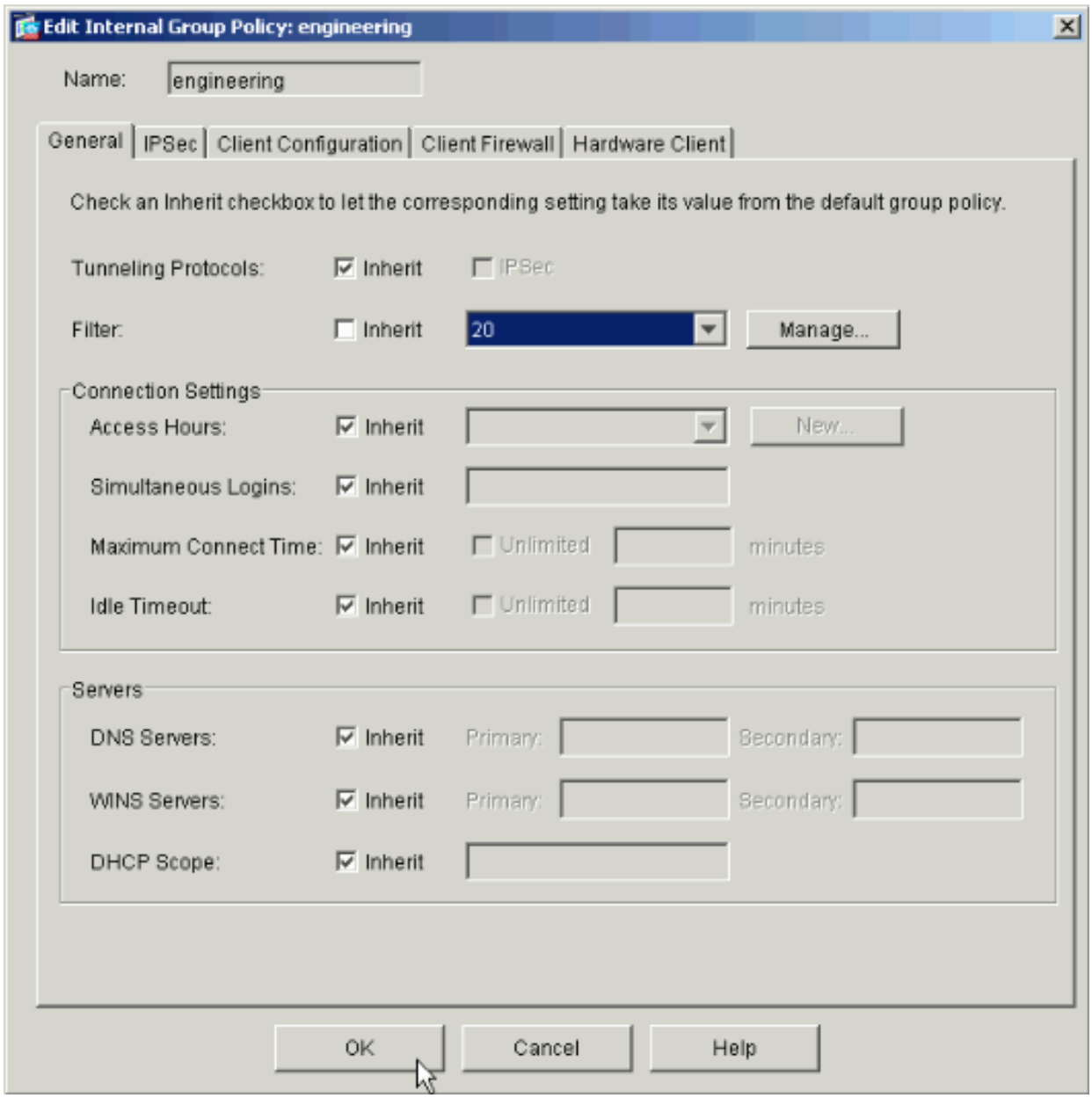
18. Répétez les étapes 2 à 17 pour tous les groupes de tunnels supplémentaires auxquels vous souhaitez ajouter des restrictions.

    Dans cet exemple de configuration, il est également nécessaire de restreindre l'accès des ingénieurs. Bien que la procédure soit la même, voici quelques fenêtres sur lesquelles les différences sont notables :

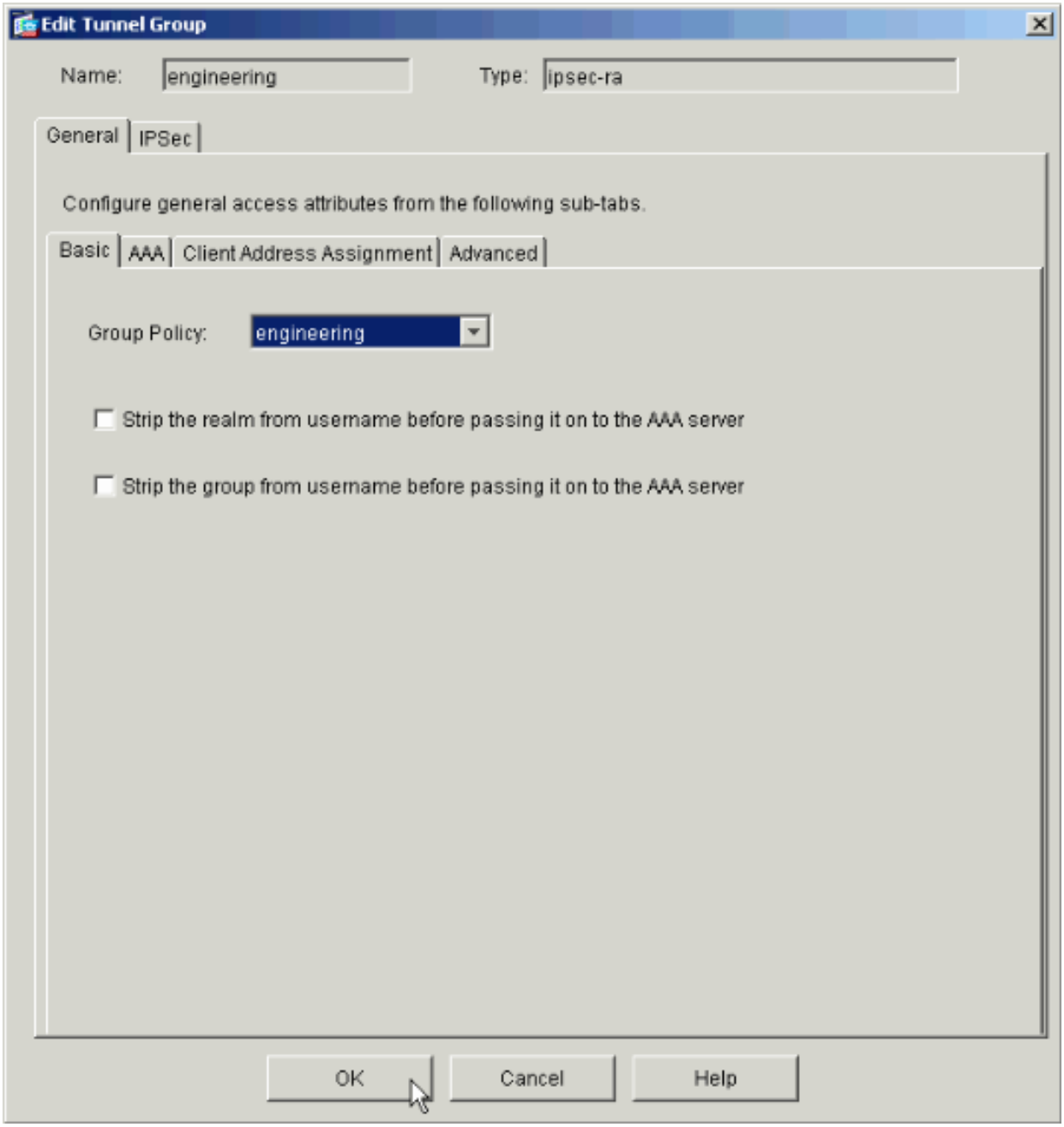
    - Nouvelle liste d'accès 20



- Sélectionnez Access List 20 comme filtre dans la politique de groupe Engineering.



- Vérifiez que la stratégie de groupe Engineering est définie pour le groupe de tunnels Engineering.



Configurer l'accès via CLI

Complétez ces étapes pour configurer l'appliance de sécurité à l'aide de l'interface CLI :

Remarque : certaines des commandes affichées dans ce résultat sont ramenées à une deuxième ligne pour des raisons spatiales.

1. Créez deux listes de contrôle d'accès différentes (15 et 20) qui sont appliquées aux utilisateurs lorsqu'ils se connectent au VPN d'accès à distance. Cette liste d’accès est appelée ultérieurement dans la configuration.

<#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. Créez deux pools d'adresses VPN différents. Créez-en un pour Payroll et un pour les utilisateurs distants 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. Créez des stratégies pour Payroll qui ne s'appliquent qu'à leur connexion.

```
<#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. Cette étape est identique à l'étape 3, sauf qu'elle concerne le groupe Ingénierie.

```
<#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. Créez des utilisateurs locaux et affectez les attributs que vous venez de créer à ces utilisateurs pour limiter leur accès aux ressources.

```
<#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. Créez des groupes de tunnels qui contiennent des stratégies de connexion pour les utilisateurs de la paie.

```
<#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. Créez des groupes de tunnels qui contiennent des stratégies de connexion pour les utilisateurs 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
```

Une fois votre configuration entrée, vous pouvez voir cette zone en surbrillance dans votre configuration :

Nom du périphérique 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
```

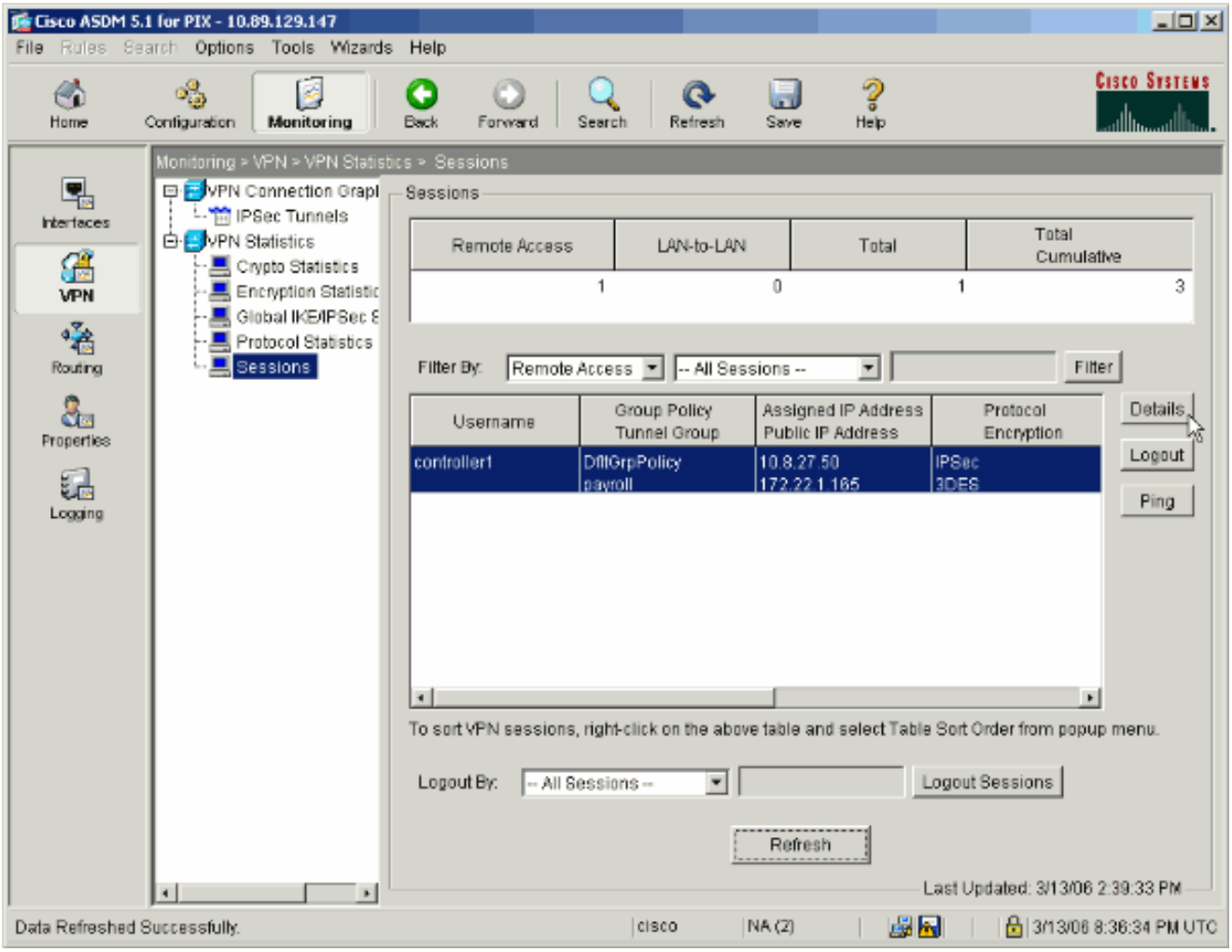
```
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:0e579c85004dcfb4071cb561514a392b
: end
ASA-AIP-CLI(config)#
```

Vérifier

Utilisez les fonctionnalités de surveillance de l'ASDM pour vérifier votre configuration :

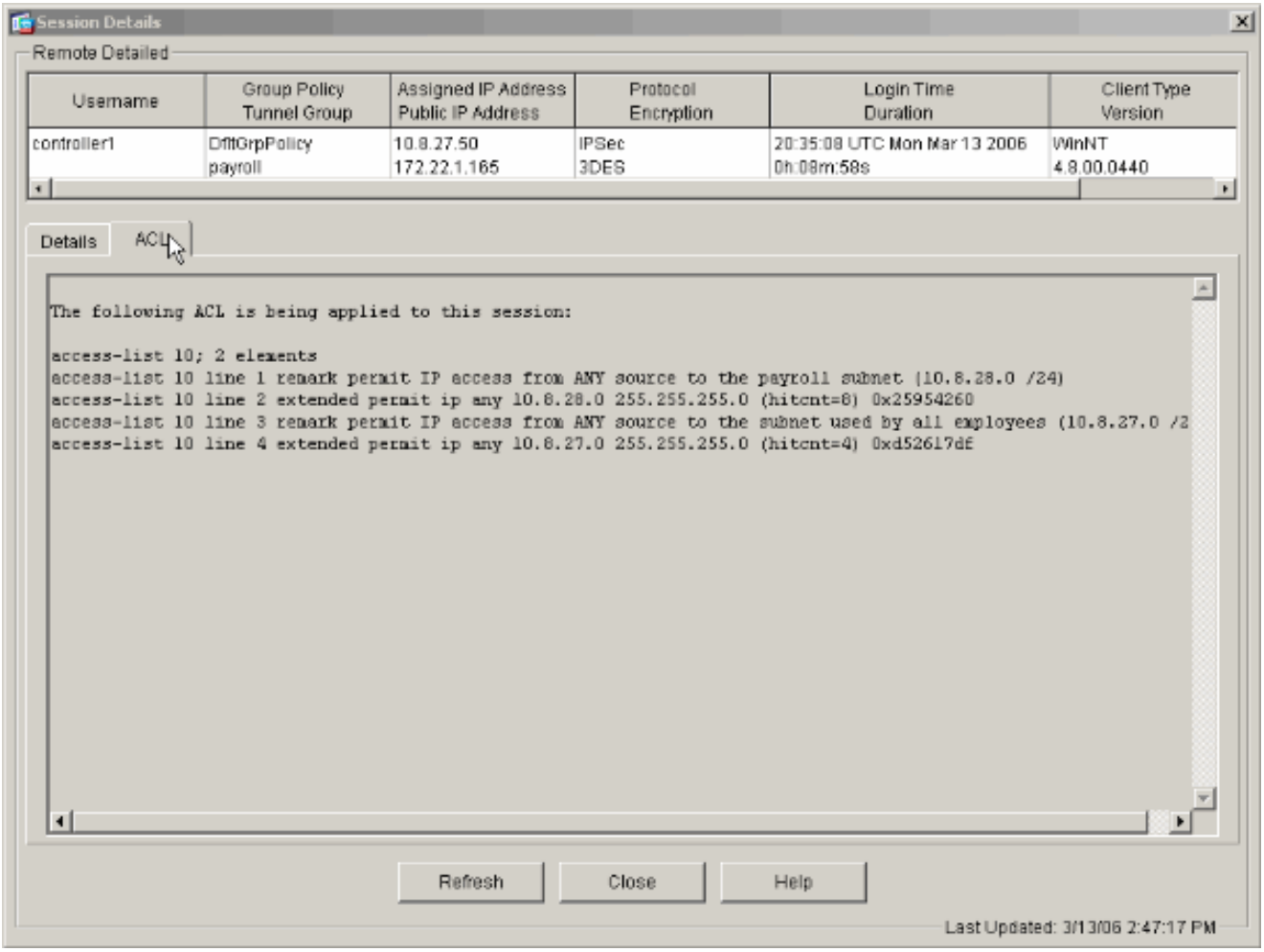
1. Sélectionnez Monitoring > VPN > VPN Statistics > Sessions.

   Vous voyez les sessions VPN actives sur le PIX. Sélectionnez la session qui vous intéresse et cliquez sur Détails.



2. Sélectionnez l'onglet ACL.

   Les `hits de` liste de contrôle d’accès reflètent le trafic qui circule dans le tunnel depuis le client vers le ou les réseaux autorisés.



Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Exemple de configuration des appareils de sécurité adaptatifs Cisco ASA 5500 ASA en tant que serveur VPN distant à l'aide de l'ASDM
- Exemples de configuration et notes techniques des appareils de sécurité de la gamme Cisco PIX 500
- Exemples de configuration et notes techniques des appareils de sécurité adaptatifs Cisco ASA 5500
- Exemples de configuration de client VPN Cisco et notes techniques
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.