ASDM del PIX/ASA 7.x: Restrinja el acceso a la red de los usuarios del VPN de acceso remoto

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Productos Relacionados
Diagrama de la red
Convenciones
Acceso de la configuración vía el ASDM
Acceso de la configuración vía el CLI
Verificación
Troubleshooting
Información Relacionada

Introducción

Este documento proporciona una configuración de ejemplo mediante Cisco Adaptive Security Device Manager (ASDM) para restringir a lo que pueden acceder los usuarios VPN de acceso remoto de las redes internas detrás de PIX Security Appliance o Adaptive Security Appliance (ASA). Puede limitar los usuarios VPN de acceso remoto a solamente las áreas de la red a las que desea que accedan cuando:

1. Cree las Listas de acceso.
2. Asocíelas a las directivas del grupo.
3. Asocie esas directivas del grupo a los grupos de túnel.

Refiera a configurar el Cisco VPN 3000 Concentrator para bloquear con los filtros y la asignación de filtro RADIUS para aprender más sobre el escenario donde el concentrador VPN bloquea el acceso de los usuarios de VPN.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El PIX se puede configurar usando el ASDM.**Nota:** Refiera a permitir el acceso HTTPS para el ASDM para permitir que el PIX sea configurado por el ASDM.
- Usted tiene por lo menos una buena configuración sabida del VPN de acceso remoto.**Nota:**

Si usted no tiene tales configuraciones, refiera al ASA como servidor VPN remoto que usa el ejemplo de la Configuración de ASDM para la información sobre cómo configurar una buena configuración del VPN de acceso remoto.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 7.1(1) del dispositivo de seguridad de las 500 Series del Secure PIX de Cisco**Nota:** El PIX 501 y los dispositivos de seguridad 506E no soportan la versión 7.x.
- Versión 5.1(1) del Cisco Adaptive Security Device Manager**Nota:** El ASDM está solamente disponible en PIX o ASA 7.x.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

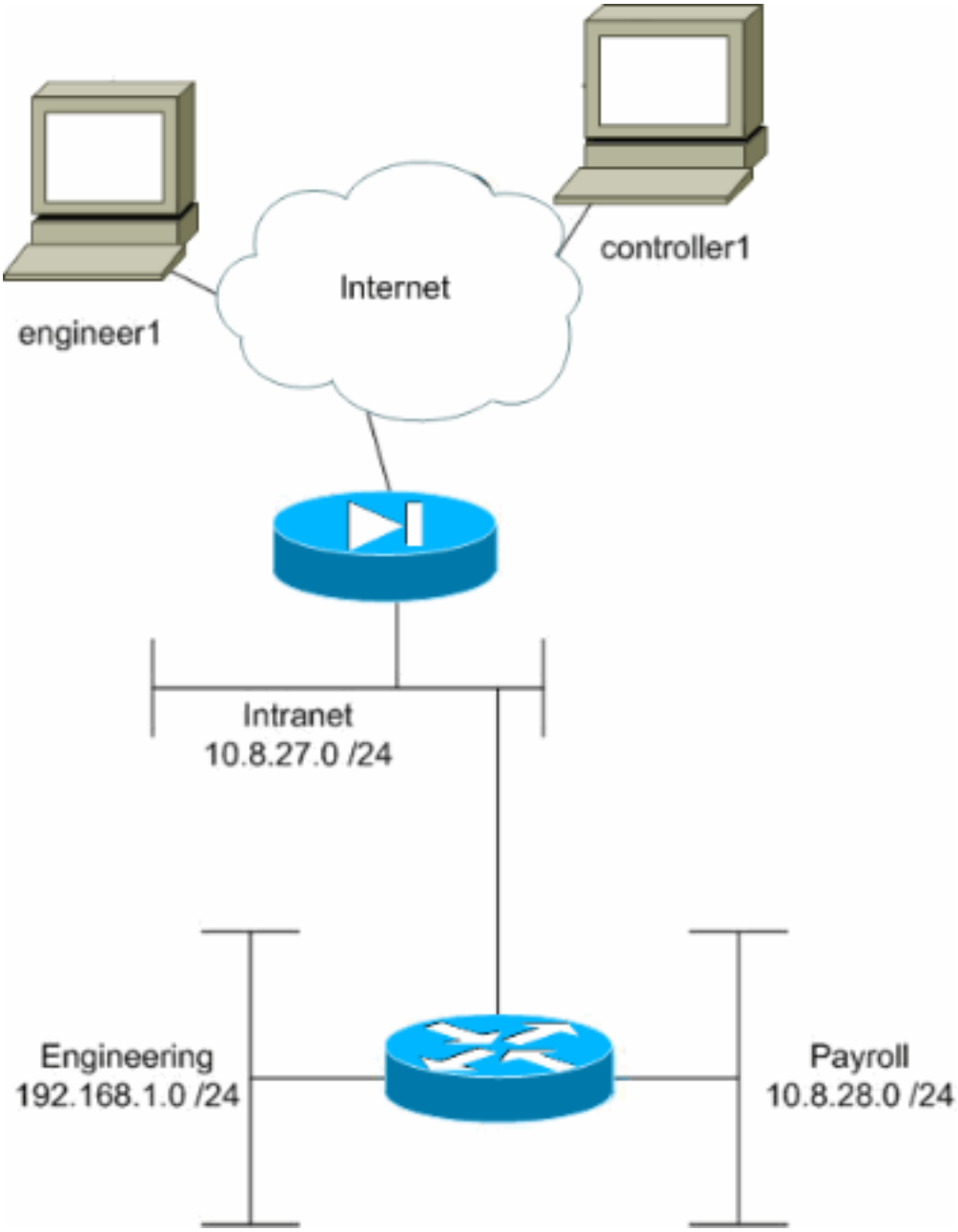
Productos Relacionados

Esta configuración también se puede utilizar con las siguientes versiones de hardware y software:

- Versión 7.1(1) adaptante del dispositivo de seguridad de las 5500 Series de Cisco ASA

Diagrama de la red

En este documento, se utiliza esta configuración de red:



En este ejemplo de configuración, una pequeña red corporativa con tres subredes es supuesta. Este diagrama ilustra la topología. Las tres subredes son Intranet, ingeniería, y nómina de pago. La meta de este ejemplo de configuración es permitir el Acceso Remoto del personal asalariado al Intranet y a las subredes de planillas de sueldos y evitar que accedan la subred de la ingeniería. También, los ingenieros deben poder acceder remotamente las subredes del Intranet y de la ingeniería, pero no la subred de planillas de sueldos. El usuario de nómina en este ejemplo es el "controller1". El usuario de la ingeniería en este ejemplo es el "engineer1".

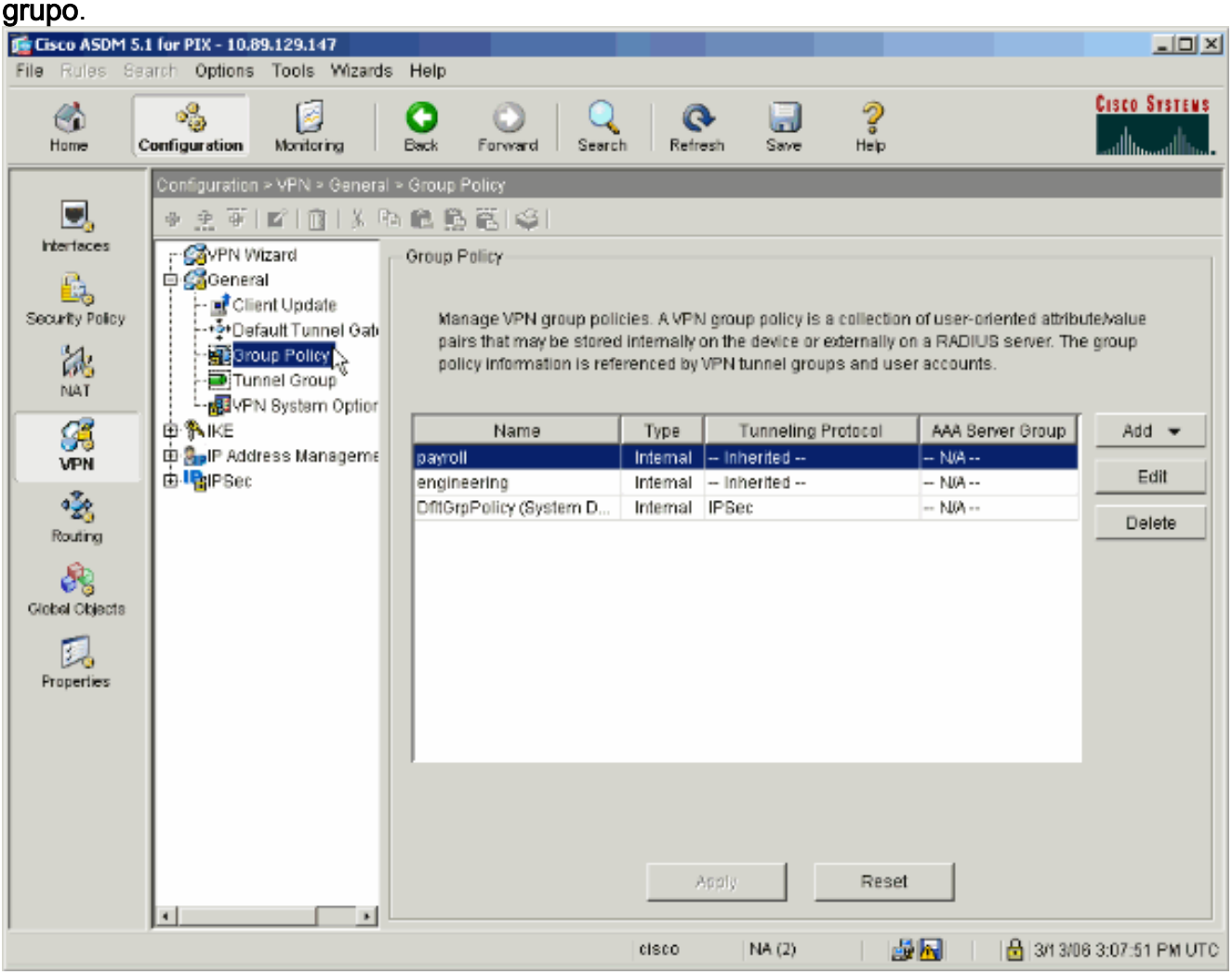
Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

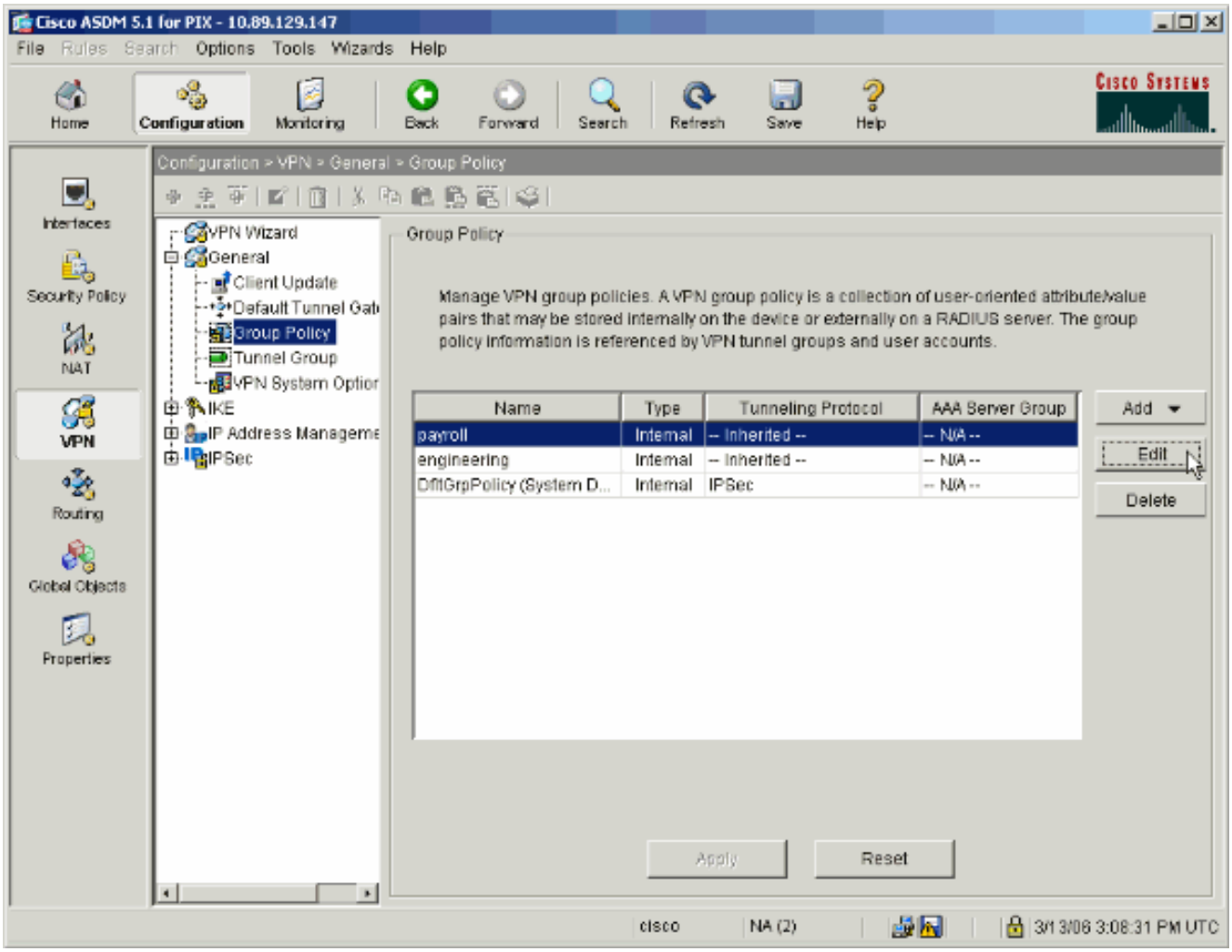
Configure el acceso vía el ASDM

Complete estos pasos para configurar el dispositivo de seguridad PIX usando el ASDM:

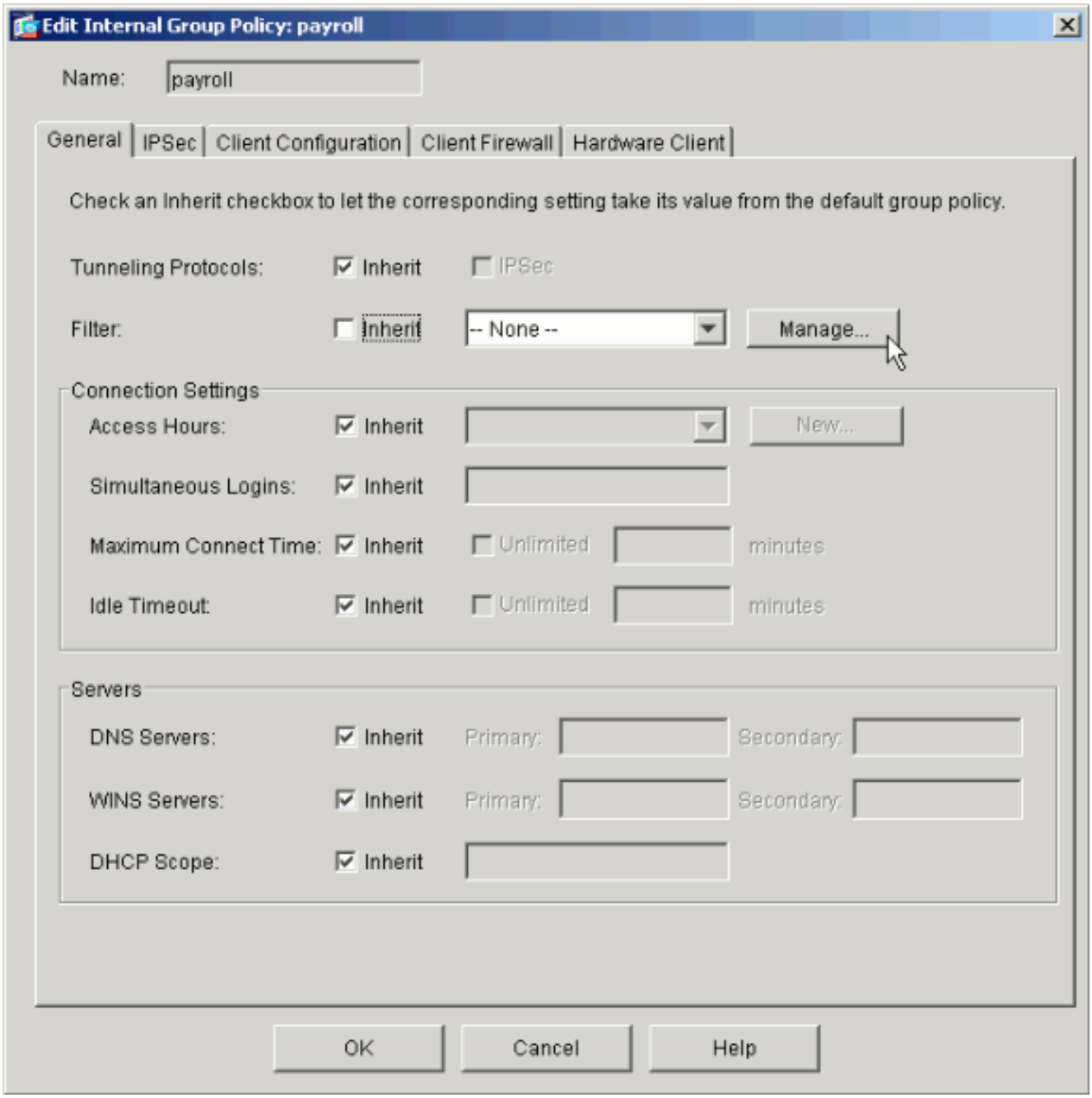
1. Seleccione la **configuración > el VPN > la directiva del general > del grupo**.



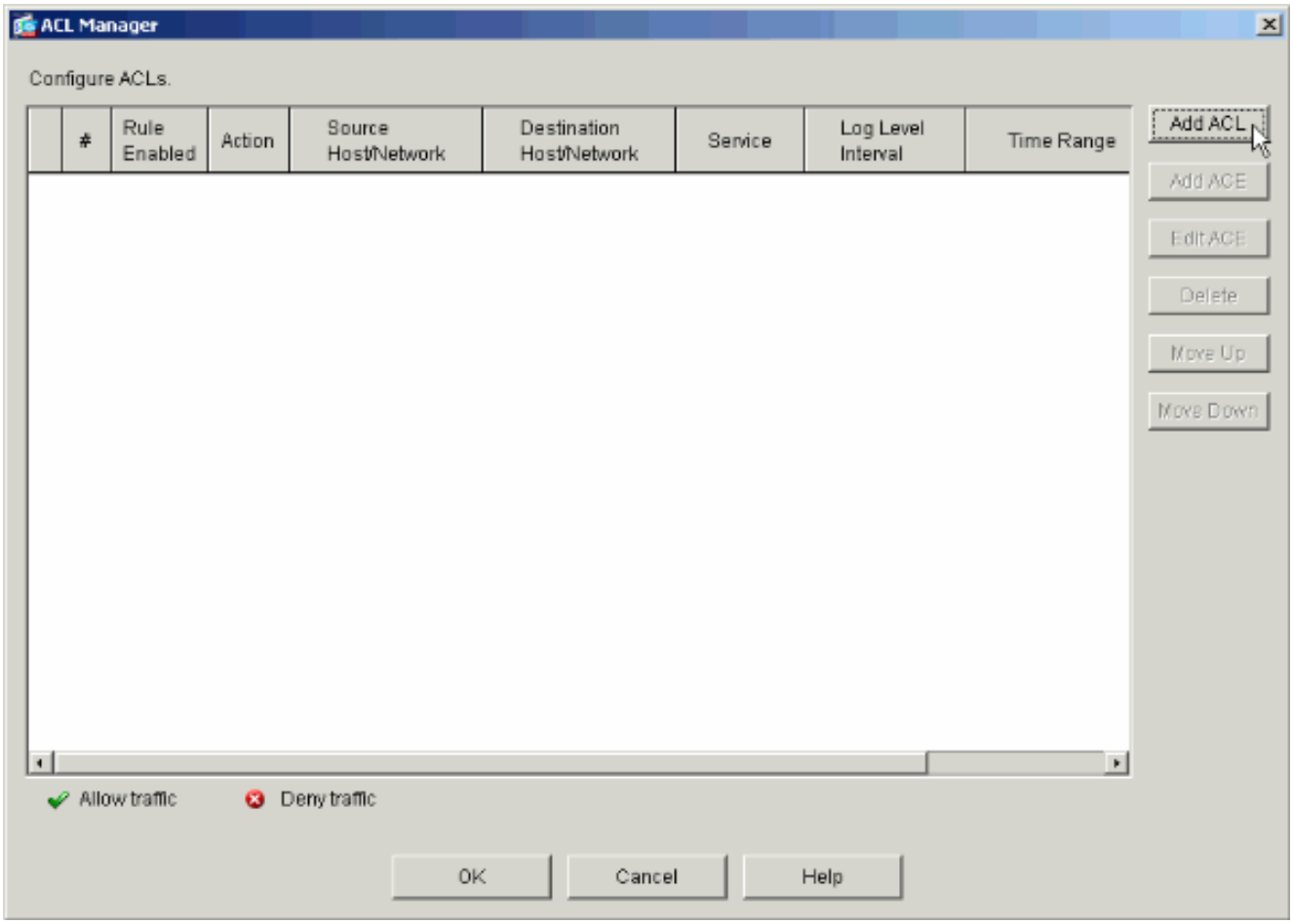
2. De acuerdo con qué medidas fueron tomadas para configurar a los grupos de túnel en el PIX, las directivas del grupo pudieron existir ya para esos grupos de túnel cuyos usuarios usted desea restringir. Si existe una política de grupo apropiada ya, elíjala y el tecleo **edita**. Si no, haga clic **agregan** y eligen el **Internal group policy (política grupal interna)….**



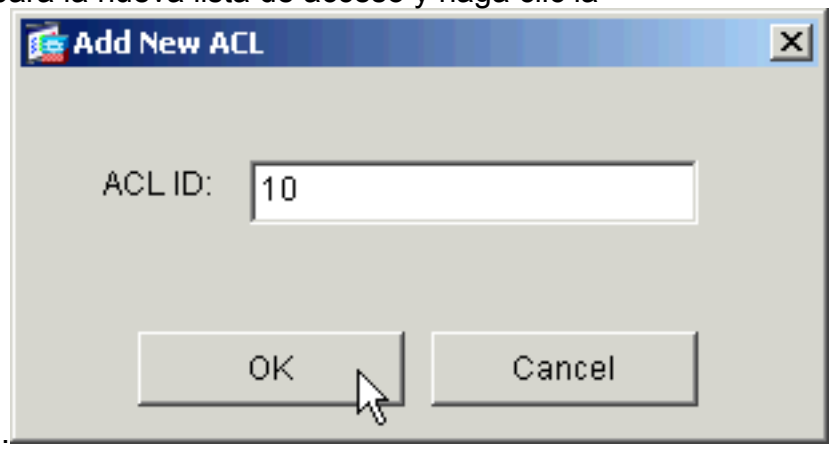
3. En caso necesario, ingresa o cambia el nombre de la directiva del grupo en la cima de la ventana que se abre.
4. En la ficha general desmarque el cuadro de la **herencia** al lado del filtro y después haga clic **manejan**.



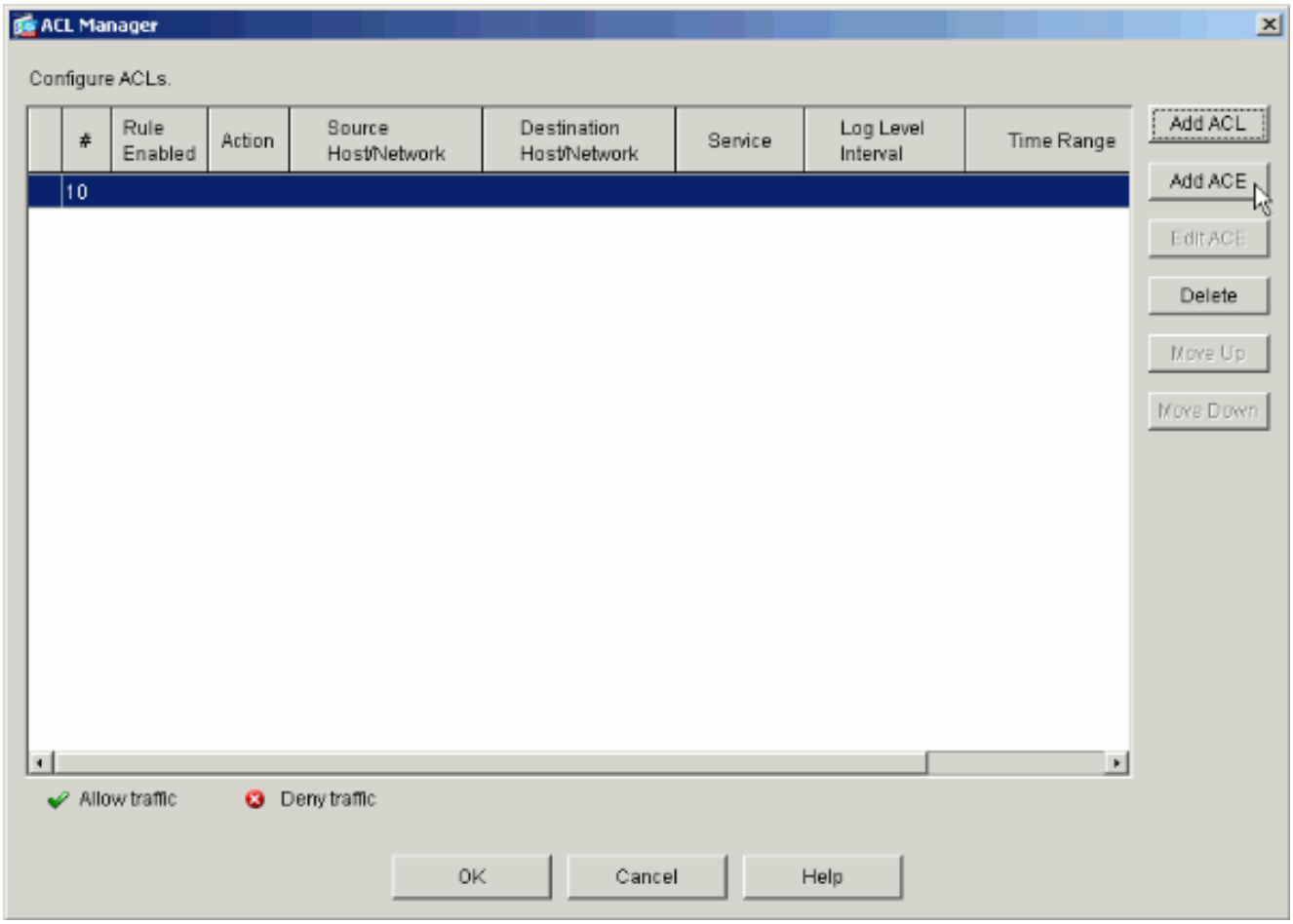
5. El tecleo **agrega el ACL** para crear una nueva lista de acceso en la ventana del ACL Manager que
aparece.



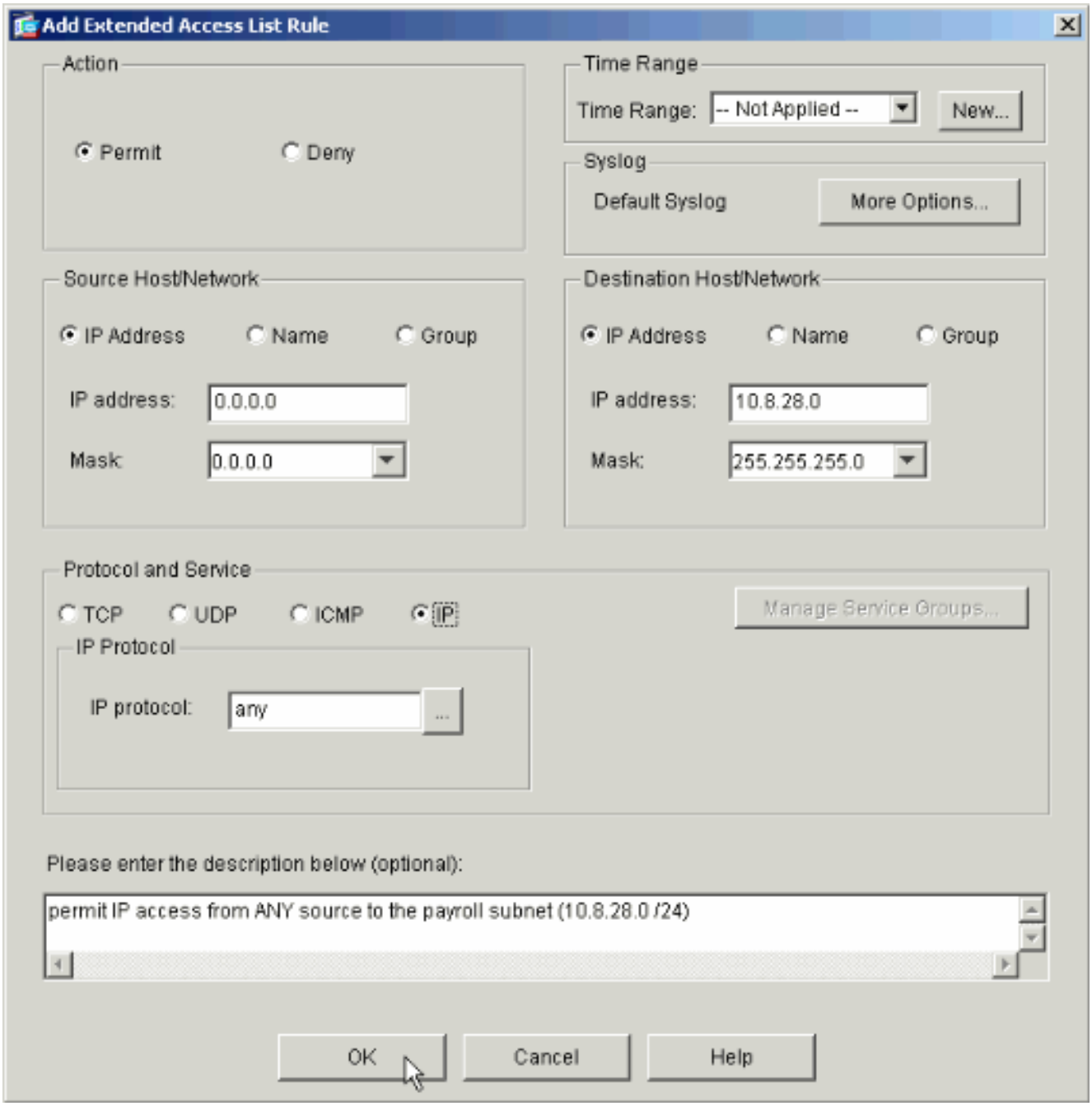
6. Elija un número para la nueva lista de acceso y haga clic la AUTORIZACIÓN.



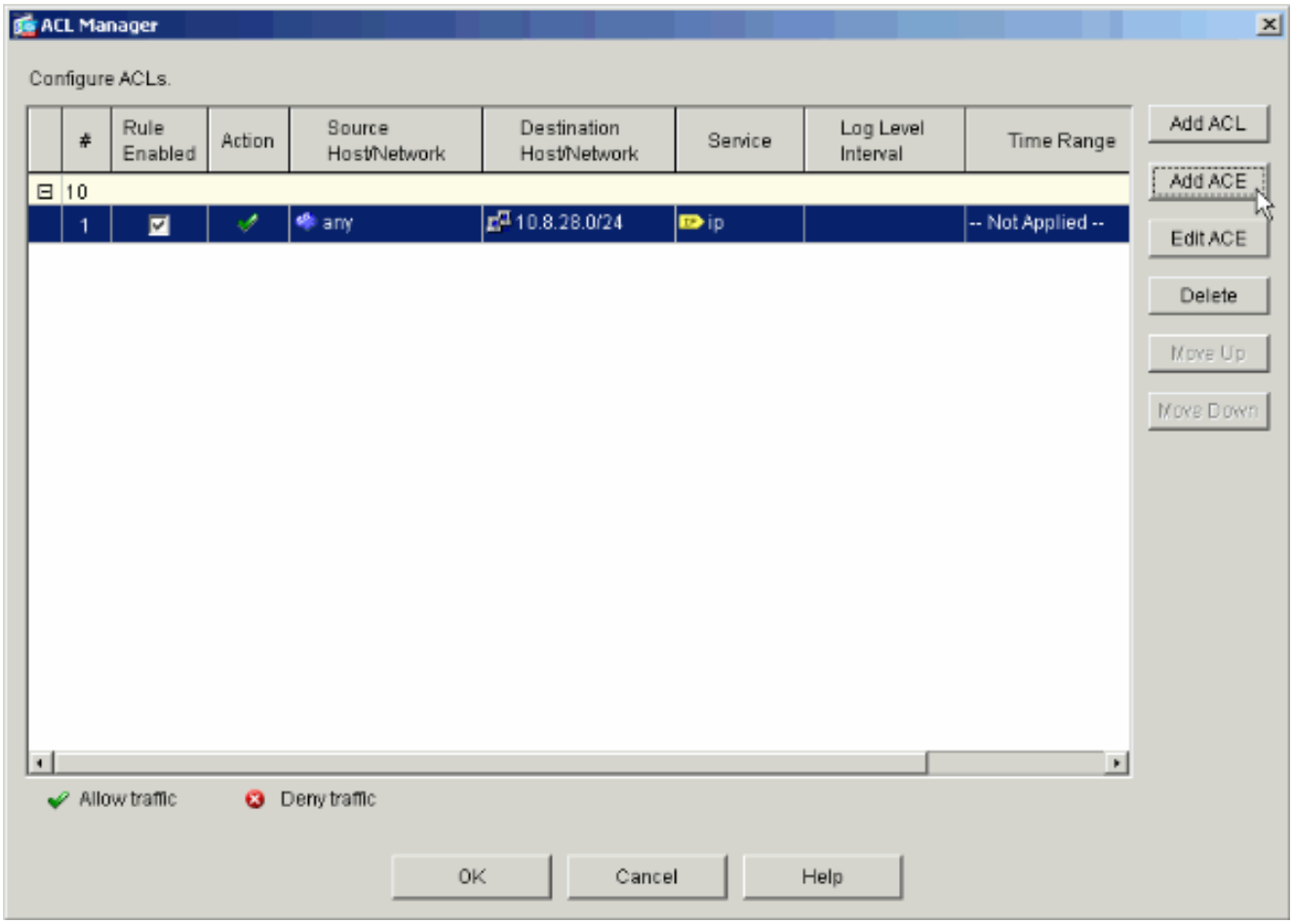
7. Con su nuevo ACL seleccionado a la izquierda, el tecleo **agrega ACE** para agregar una nueva entrada de control de acceso a la lista.



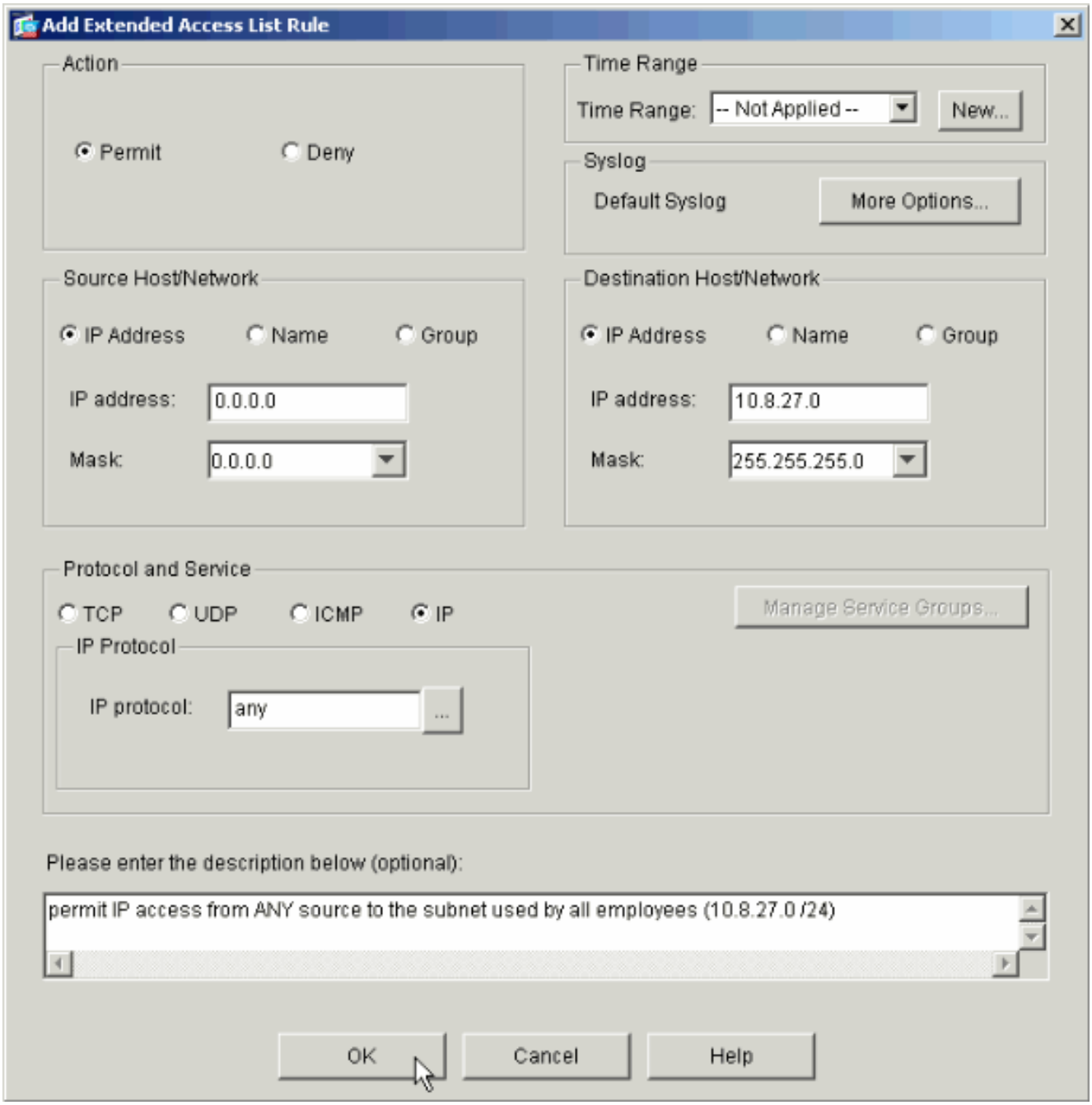
8. Defina la Entrada de control de acceso (ACE) que usted desea agregar.En este ejemplo, primer ACE en ACL 10 permite el IP Access a la subred de planillas de sueldos de cualquier fuente.**Nota:** Por abandono, el ASDM selecciona solamente el TCP como el protocolo. Usted debe elegir el IP si usted desea al IP Access completo de los usuarios del permit or deny. Haga Click en OK cuando le
acaban.



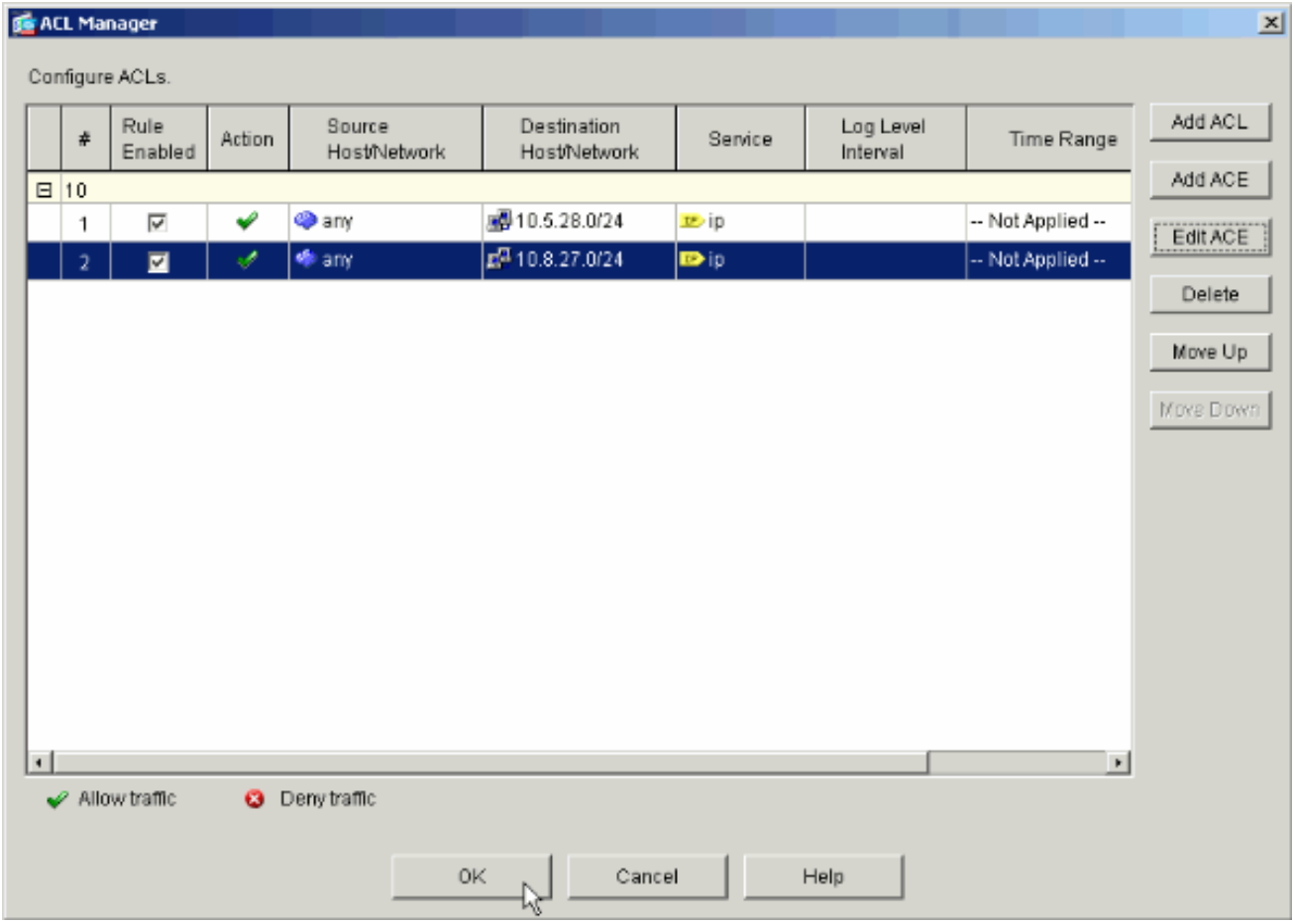
9. ACE que usted ahora acaba de agregar aparece en la lista. Elija **agregan ACE** otra vez para agregar cualquier línea adicional a la lista de acceso.



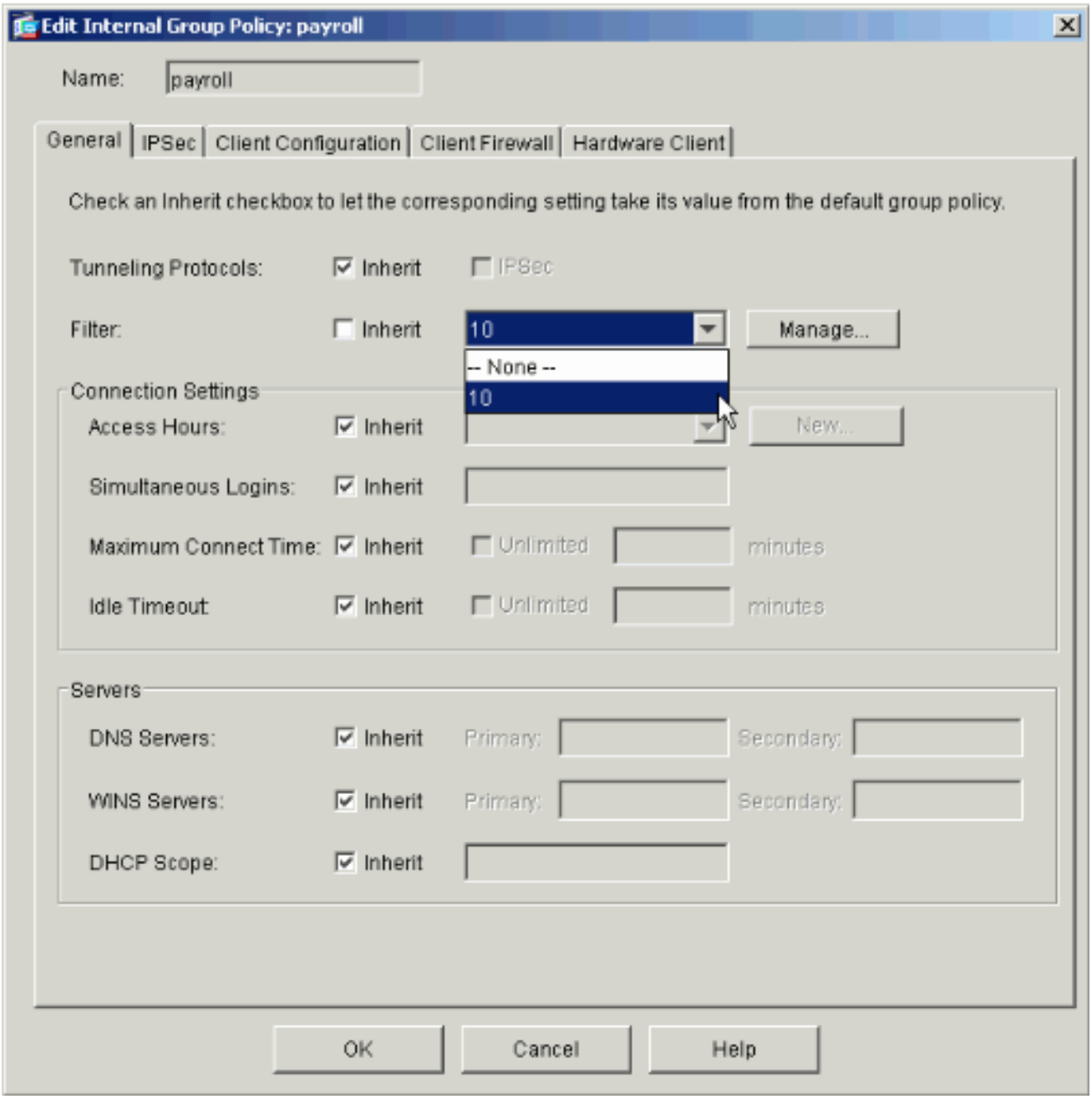
En este ejemplo, un segundo ACE se agrega a ACL 10 para permitir el acceso a la subred de
Intranet.



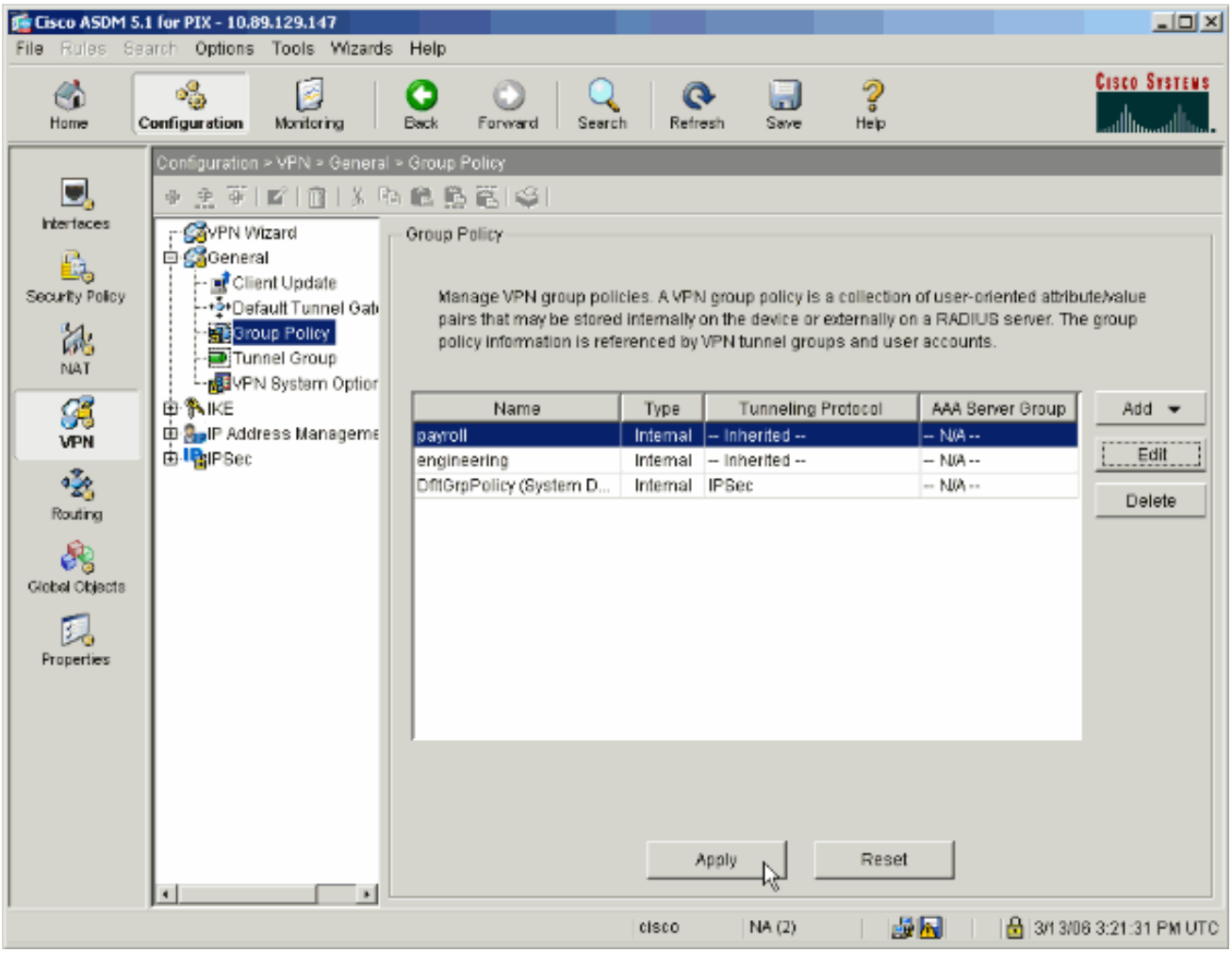
10. Haga Click en OK una vez que le hacen que agrega los ACE.



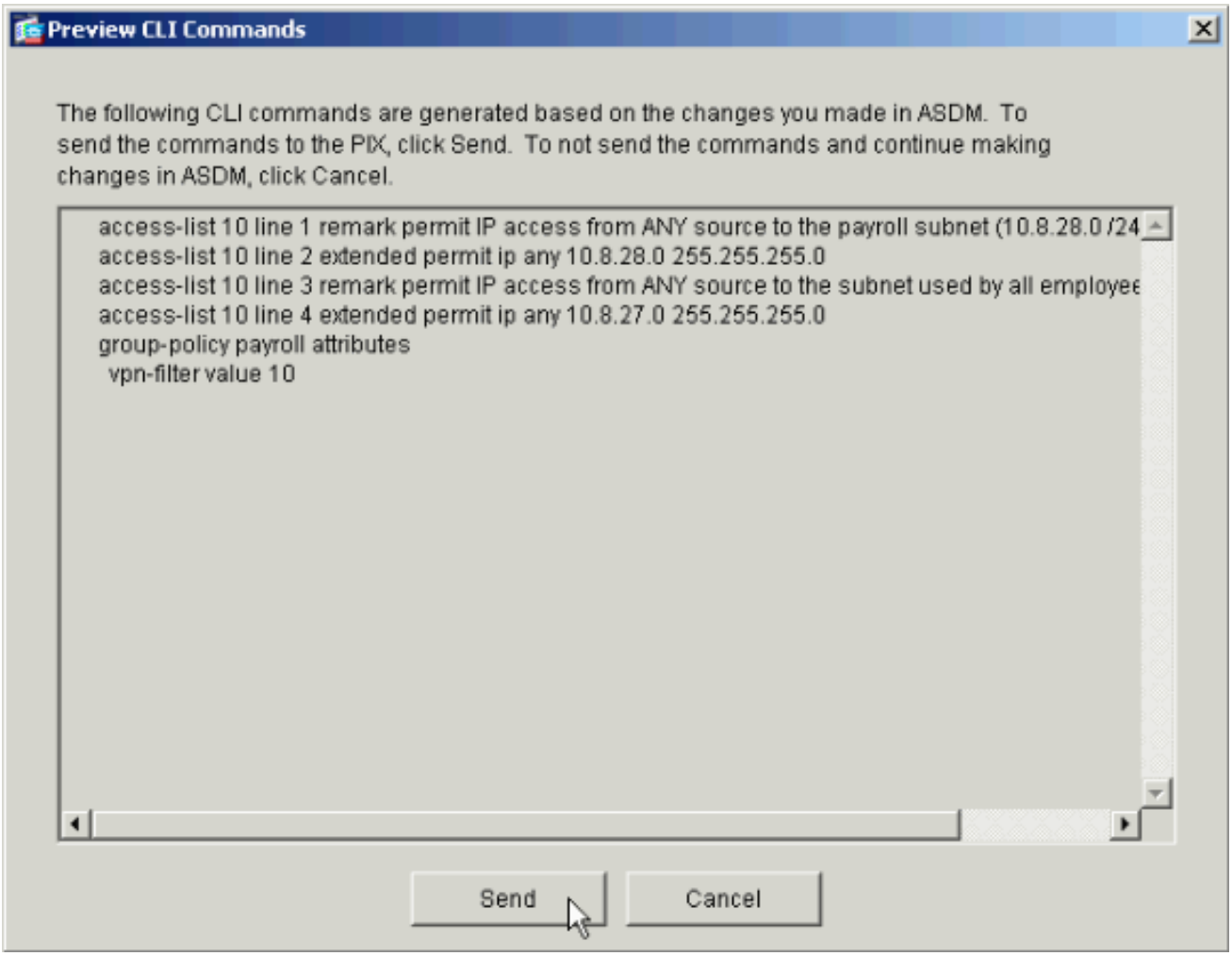
11. Seleccione el ACL que usted definió y pobló en los pasos más recientes para ser el filtro para su directiva del grupo. Haga Click en OK cuando le hacen.



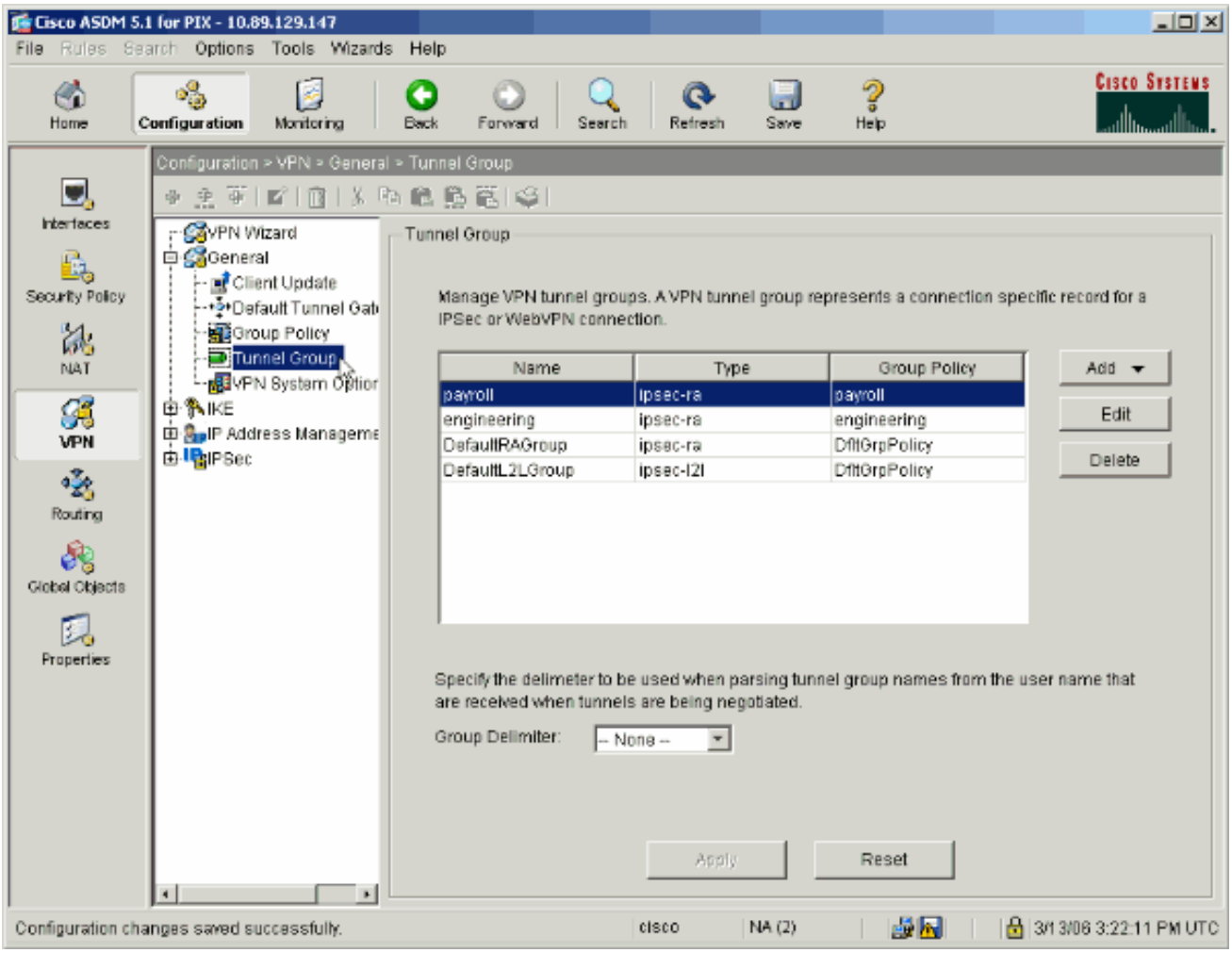
12. El tecleo **se aplica** para enviar los cambios al PIX.



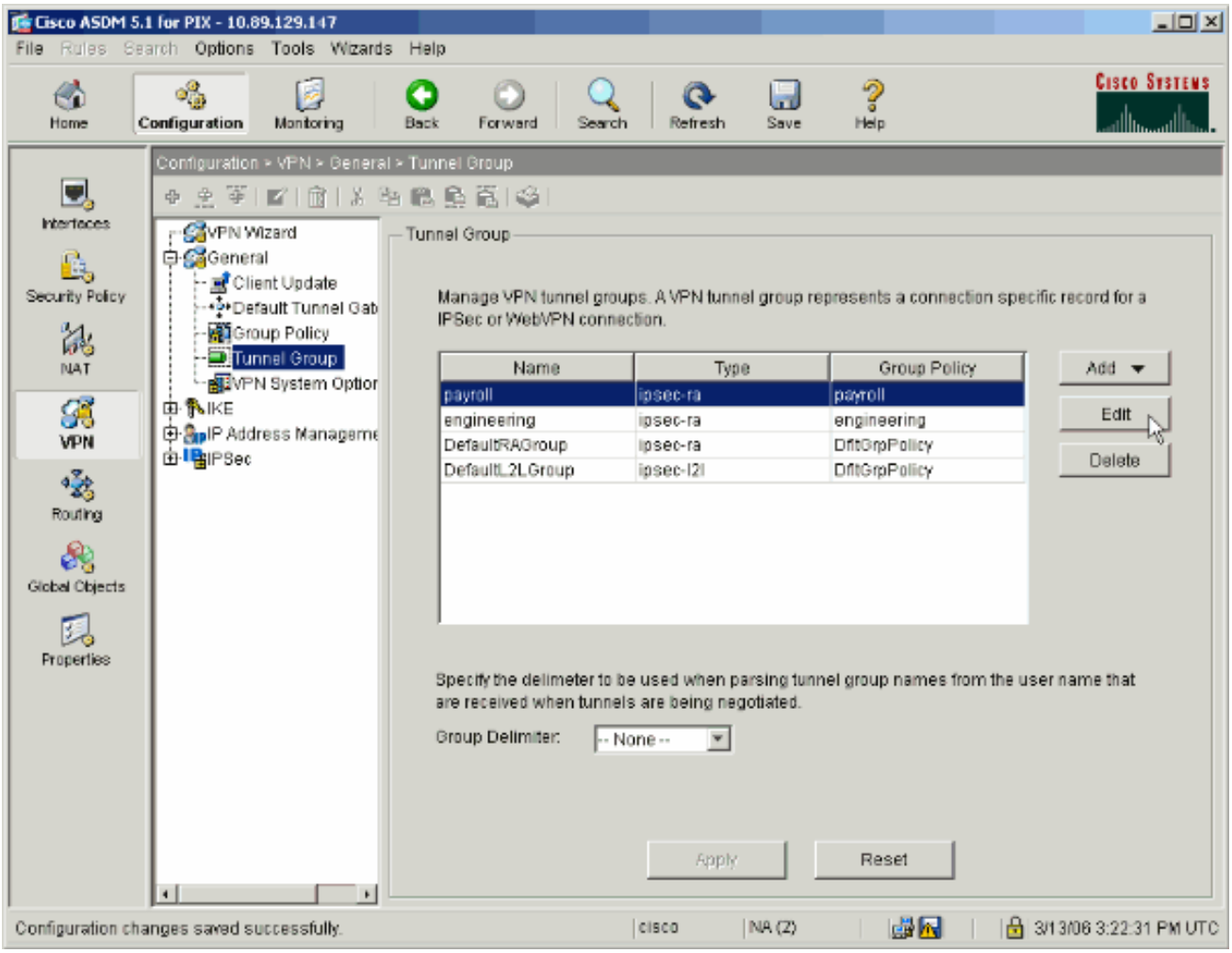
13. Si usted lo hace configurar para hacer tan bajo las **opciones > preferencias**, el ASDM ve los comandos de antemano que está a punto de enviar al PIX. El tecleo **envía**.



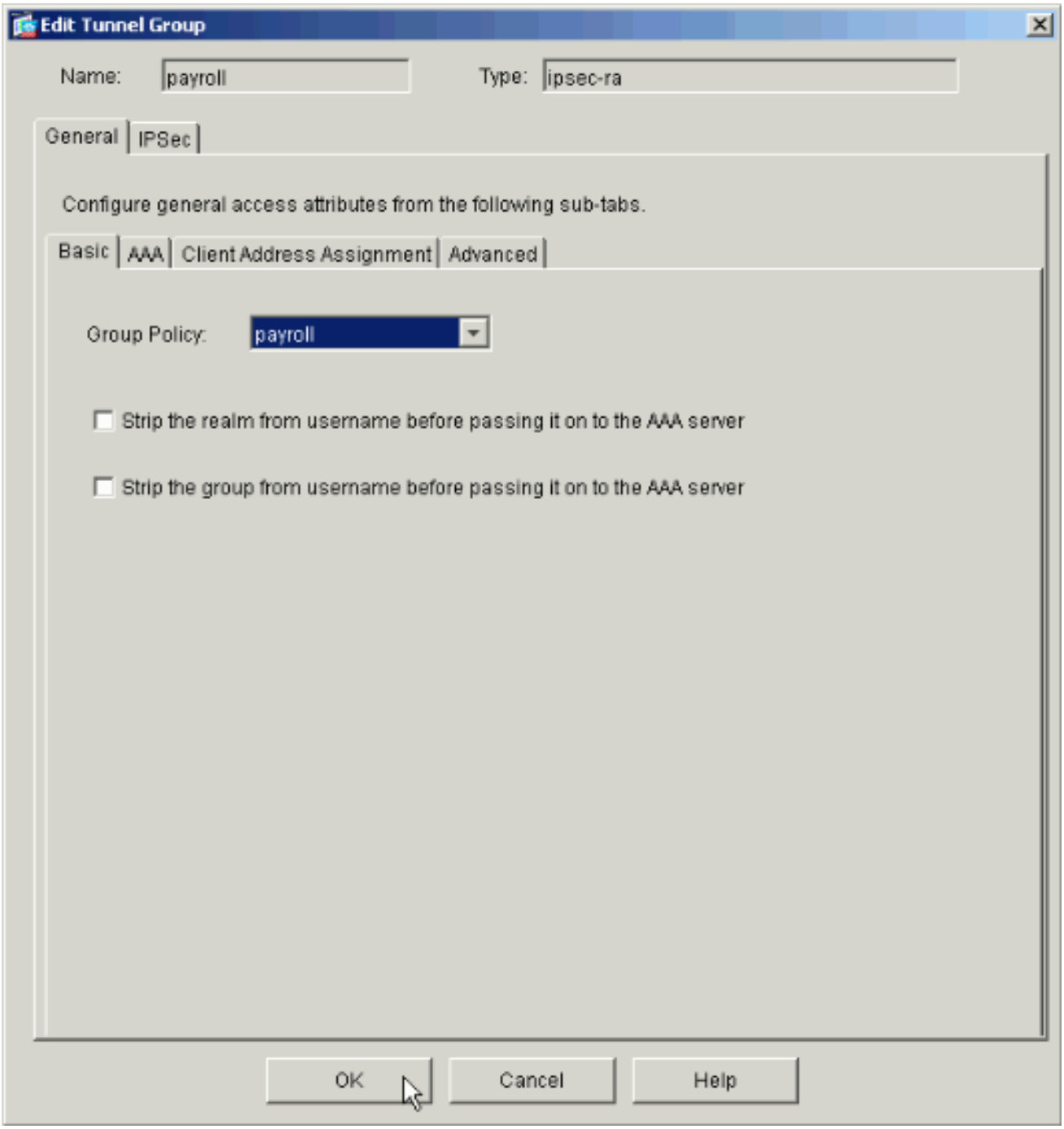
14. Aplique la directiva del grupo acaba de modificaa que fue creada o al grupo de túnel correcto. Haga clic al **grupo de túnel** en la trama izquierda.



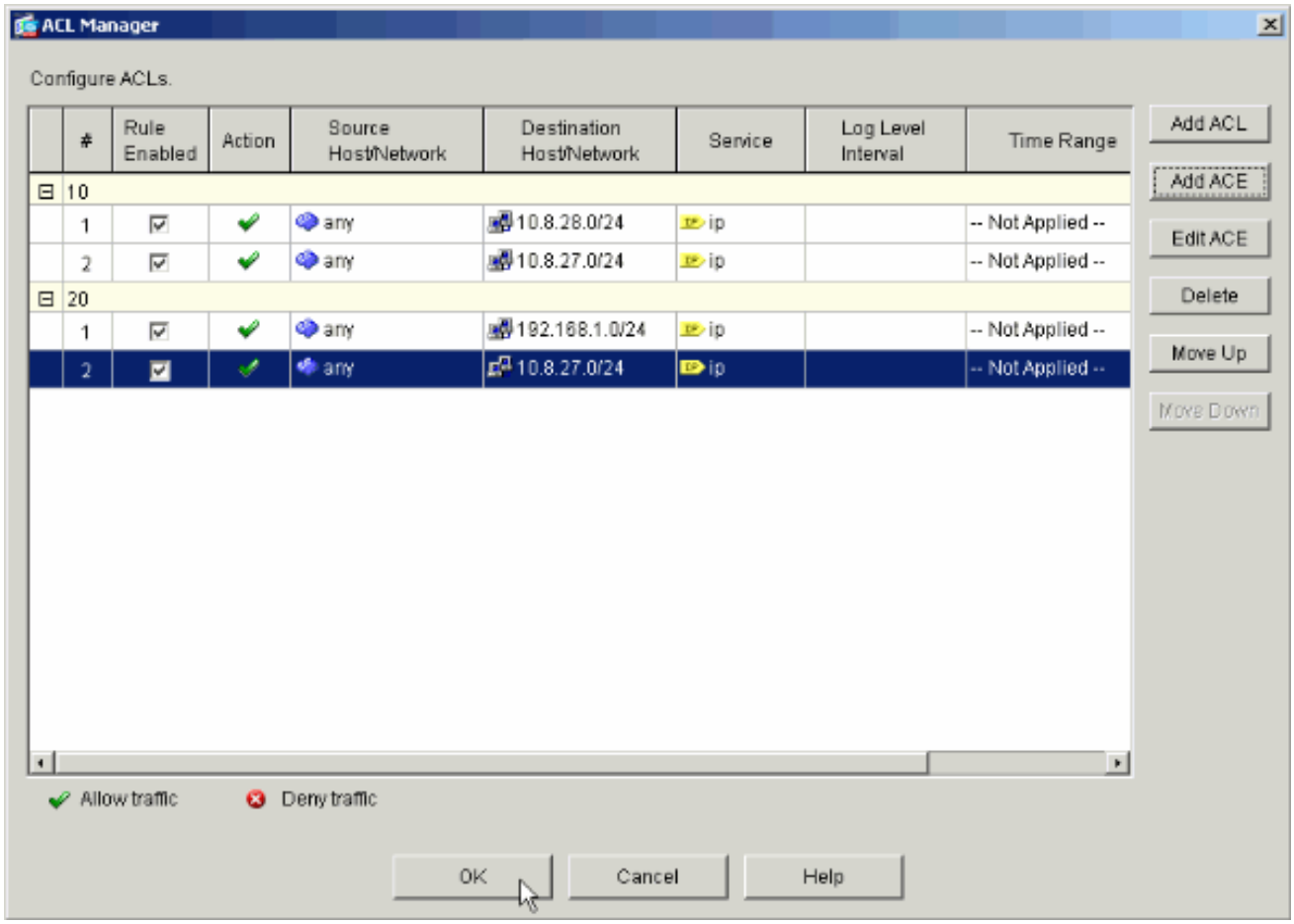
15. Elija al grupo de túnel que usted desea aplicar la directiva del grupo a y el tecleo **edita**.



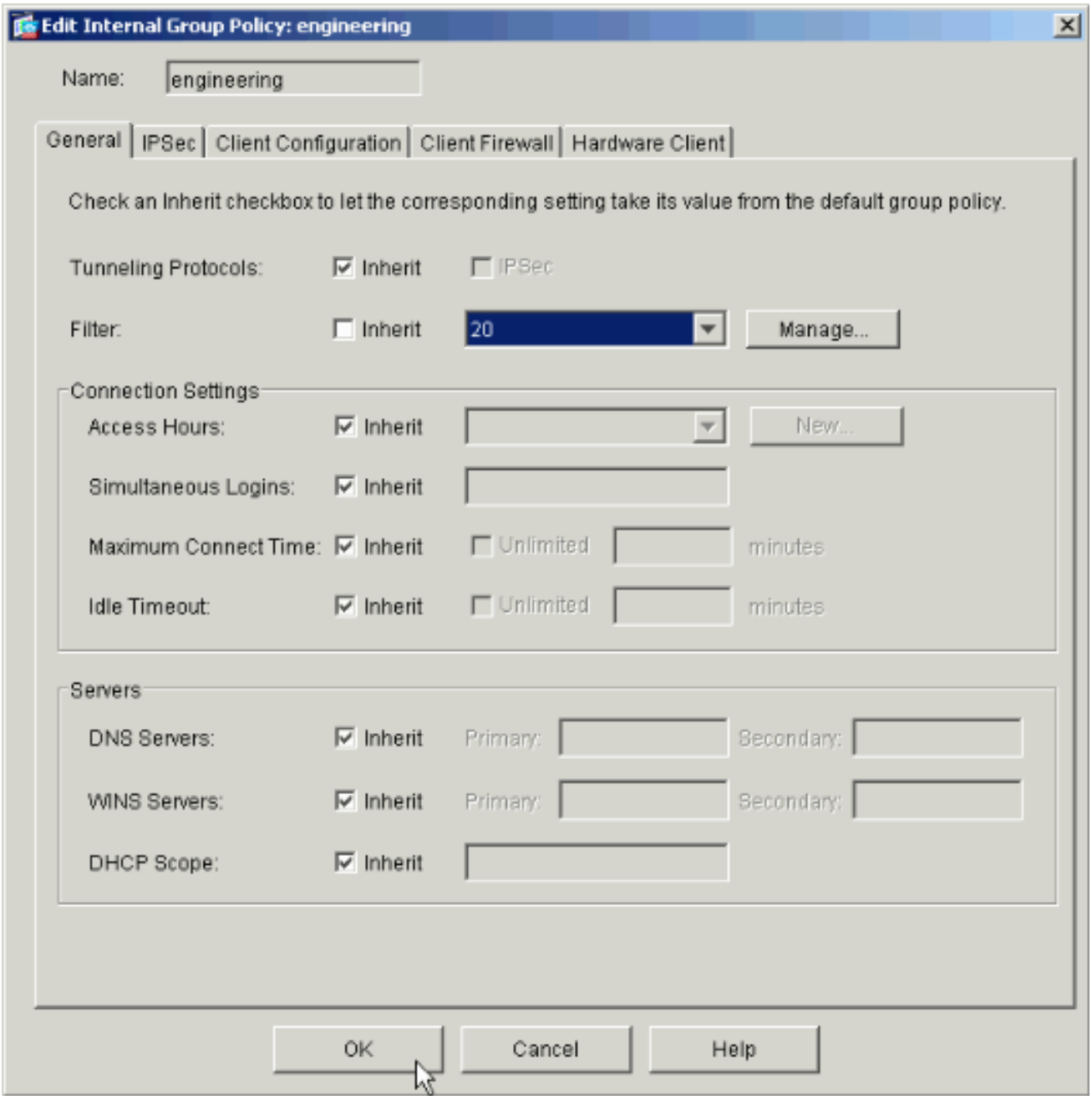
16. Si su directiva del grupo fue creada automáticamente (véase el paso 2), verifican que la directiva del grupo que usted acaba de configurar está seleccionada en la casilla desplegable. Si su directiva del grupo no fue configurada automáticamente, selecciónela de la casilla desplegable. Haga Click en OK cuando le hacen.



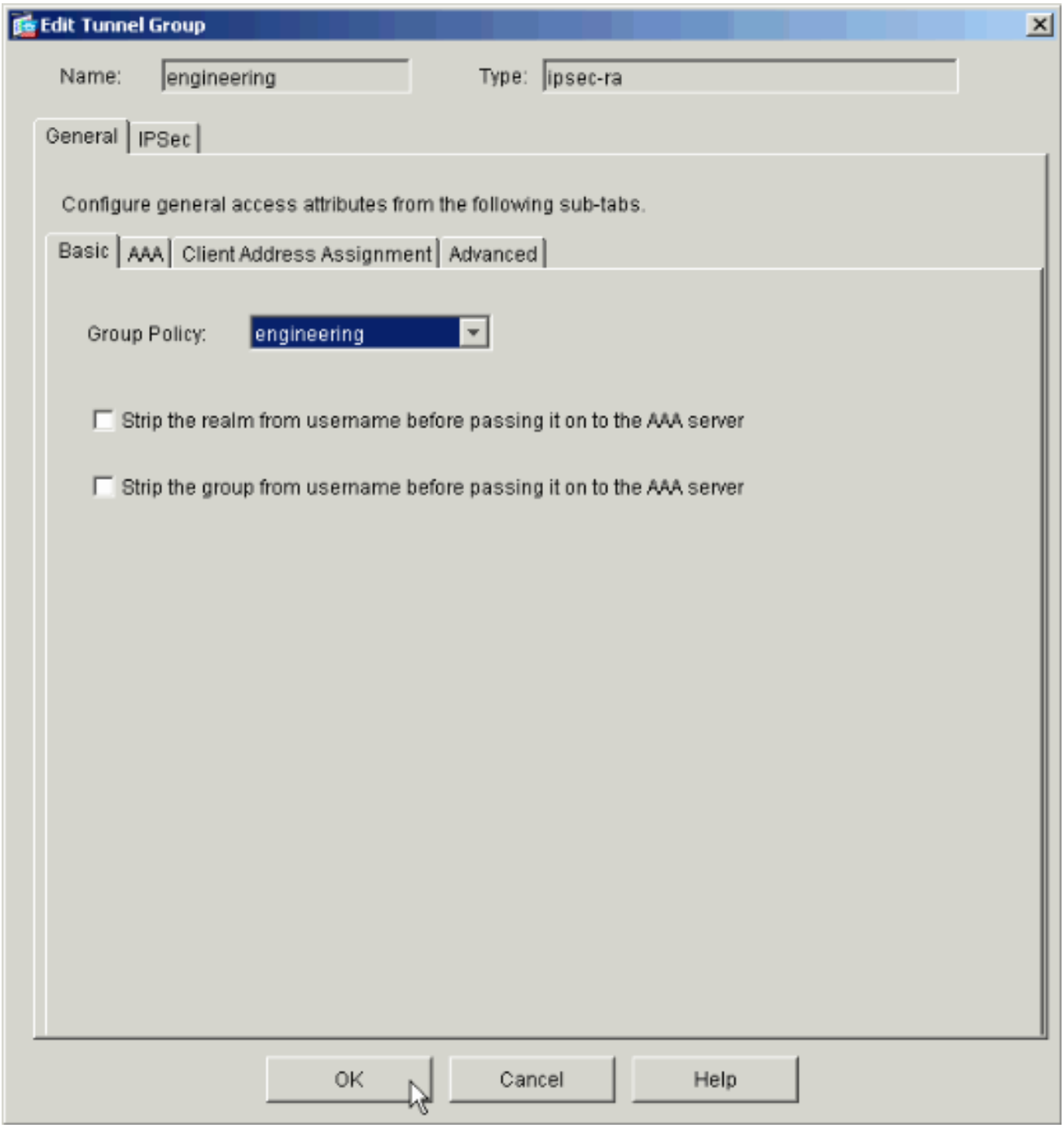
17. El tecleo **se aplica** y, si está indicado, el tecleo **envía** para agregar el cambio a la configuración PIX.Si la directiva del grupo fue seleccionada ya usted puede ser que reciba un mensaje que no dice “ningún cambio fue hecho.” Haga clic en OK.
18. Relance los pasos 2 a 17 para cualquier grupo de túnel adicional a quien usted quisiera agregar las restricciones.En este ejemplo de configuración, es también necesario restringir el acceso de los ingenieros. Mientras que el procedimiento es lo mismo, éstas son algunas ventanas en las cuales las diferencias son notables:Nueva lista de acceso



Elija la **lista de acceso 20** como filtro en la directiva del grupo de ingeniería.



Verifique que la directiva del grupo de ingeniería esté fijada para el grupo de túnel que dirige.



Configure el acceso vía el CLI

Complete estos pasos para configurar el dispositivo de seguridad usando el CLI:

Nota: Algunos de los comandos mostrados en esta salida se derriban a una segunda línea debido a las razones espaciales.

1. Cree dos diversas listas de control de acceso (15 y 20) que se apliquen a los usuarios mientras que conectan con el VPN de acceso remoto. Esta lista de acceso se invita más adelante en la configuración.`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. Cree a dos diversas agrupaciones de direcciones VPN. Cree uno para la nómina de pago y uno para los usuarios remotos de la ingeniería.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. Cree las directivas para la nómina de pago que se aplican solamente a ellas cuando conectan.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. Este paso es lo mismo que el paso 3 a menos que esté para el grupo de ingeniería.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. Cree a los usuarios locales y asigne los atributos que usted acaba de crear a esos usuarios para restringir su acceso a los recursos.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. Cree a los grupos de túnel que contienen las directivas de la conexión para los usuarios de nómina.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. Cree a los grupos de túnel que contienen las directivas de la conexión para los usuarios de la ingeniería.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**

Una vez que le configuración ingresan, usted puede ver esta área resaltada en su configuración:

Nombre del dispositivo 1
ASA-AIP-CLI(config)#**show running-config** ASA Version 7.2(2) ! hostname ASAwCSC-ASDM domain-name corp.com enable password 9jNfZuG3TC5tCVH0 encrypted names ! interface Ethernet0/0 nameif Intranet security-level 0 ip address 10.8.27.2 255.255.255.0 ! interface Ethernet0/1 nameif Engineer security-level 100 ip address 192.168.1.1 255.255.255.0 ! interface Ethernet0/2 nameif Payroll security-level 100 ip address 10.8.28.0 ! interface Ethernet0/3 no nameif no security-level no ip address ! interface Management0/0 no nameif no security-level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-group DefaultDNS domain-name corp.com access-list Inside_nat0_outbound extended permit ip any 172.10.1.0

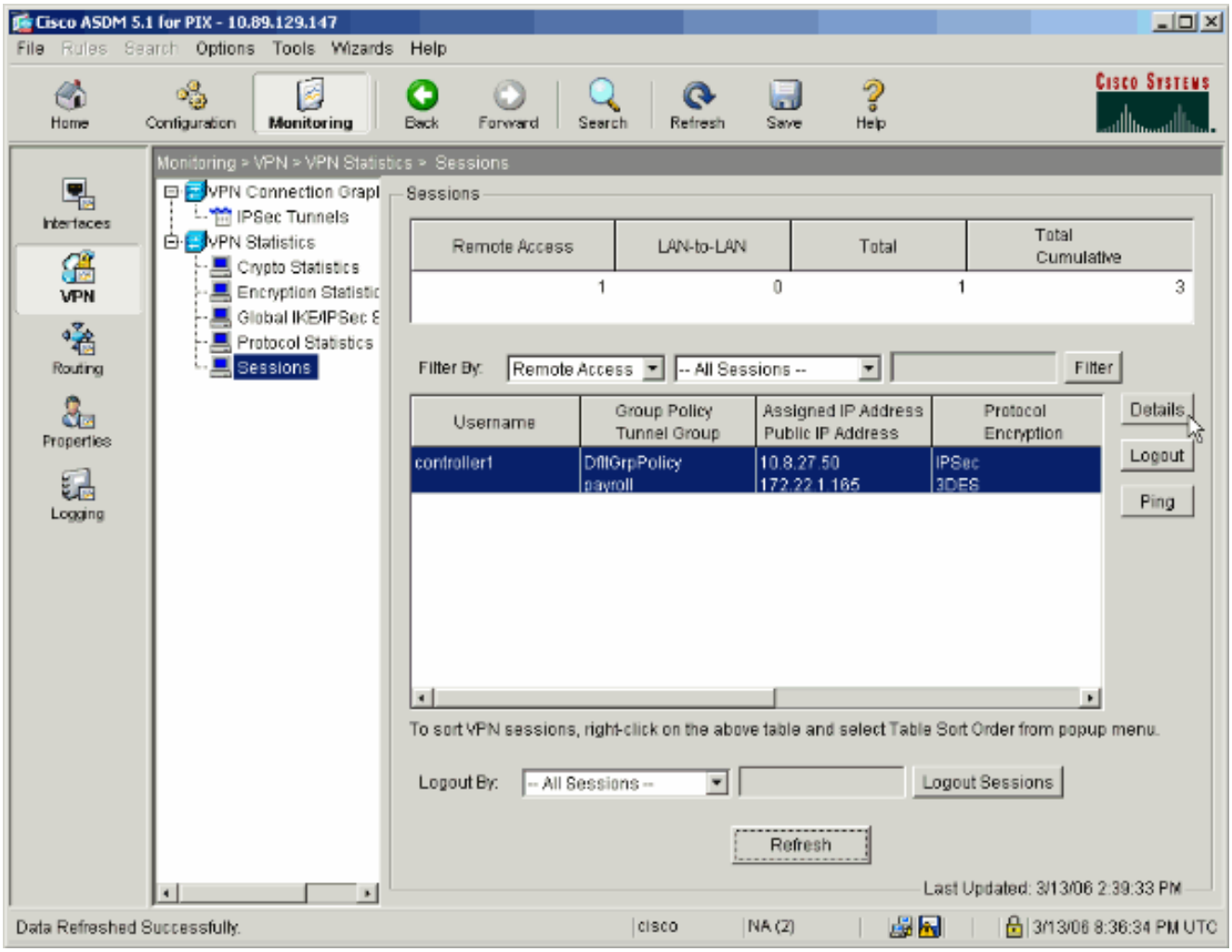
255.255.255.0 access-list Inside_nat0_outbound extended permit ip any 172.16.2.0 255.255.255.0 **access-list 15 remark permit IP access from ANY source to the Payroll subnet (10.8.28.0/24) access-list 15 extended permit ip any 10.8.28.0 255.255.255.0 access-list 15 remark Permit IP access from ANY source to the subnet used by all employees (10.8.27.0) access-list 15 extended permit ip any 10.8.27.0 255.255.255.0 access-list 20 remark Permit IP access from Any source to the Engineering subnet (192.168.1.0/24) access-list 20 extended permit ip any 192.168.1.0 255.255.255.0 access-list 20 remark Permit IP access from Any source to the subnet used by all employees (10.8.27.0/24) access-list 20 extended permit ip any 10.8.27.0 255.255.255.0** pager lines 24 mtu MAN 1500 mtu Outside 1500 mtu Inside 1500 **ip local pool Payroll-VPN 172.10.1.100-172.10.1.200 mask 255.255.255.0 ip local pool Engineer-VPN 172.16.2.1-172.16.2.199 mask 255.255.255.0** no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-522.bin no asdm history enable arp timeout 14400 global (Intranet) 1 interface nat (Inside) 0 access-list Inside_nat0_outbound nat (Inside) 1 192.168.1.0 255.255.255.0 nat (Inside) 1 10.8.27.0 255.255.255.0 nat (Inside) 1 10.8.28.0 255.255.255.0 route Intranet 0.0.0.0 0.0.0.0 10.8.27.2 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute **group-policy Payroll internal group-policy Payroll attributes dns-server value 10.8.27.10 vpn-filter value 15 vpn-tunnel-protocol IPSec default-domain value payroll.corp.com address-pools value Payroll-VPN group-policy Engineering internal group-policy Engineering attributes dns-server value 10.8.27.10 vpn-filter value 20 vpn-tunnel-protocol IPSec default-domain value Engineer.corp.com address-pools value Engineer-VPN username engineer password LCaPXI.4Xtvclaca encrypted username engineer attributes vpn-group-policy Engineering vpn-filter value 20 username marty password 6XmYwQOO9tiYnUDN encrypted privilege 0 username marty attributes vpn-group-policy Payroll vpn-filter value 15** no snmp-server location no snmp-server contact crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac crypto dynamic-map Outside_dyn_map 20 set pfs crypto dynamic-map Outside_dyn_map 20 set transform-set ESP-3DES-SHA crypto map Outside_map 65535 ipsec-isakmp dynamic Outside_dyn_map crypto map Outside_map interface Outside crypto isakmp enable Outside crypto isakmp policy 10 authentication pre-share encryption 3des hash sha group 2 lifetime 86400 **tunnel-group Payroll type ipsec-ra tunnel-group Payroll general-attributes address-pool vpnpool default-group-policy Payroll tunnel-group Payroll ipsec-attributes pre-shared-key * tunnel-group Engineering type ipsec-ra tunnel-group Engineering general-attributes address-pool Engineer-VPN default-group-policy Engineering tunnel-group Engineering ipsec-attributes pre-shared-key *** telnet timeout 5 ssh timeout 5 console timeout 0 ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns migrated_dns_map_1 parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns migrated_dns_map_1 inspect ftp inspect h323

```
h225 inspect h323 ras inspect netbios inspect rsh
inspect rtsp inspect skinny inspect esmtp inspect sqlnet
inspect sunrpc inspect tftp inspect sip inspect xdmcp !
service-policy global_policy global prompt hostname
context Cryptochecksum:0e579c85004dcfb4071cb561514a392b
: end ASA-AIP-CLI(config)#
```

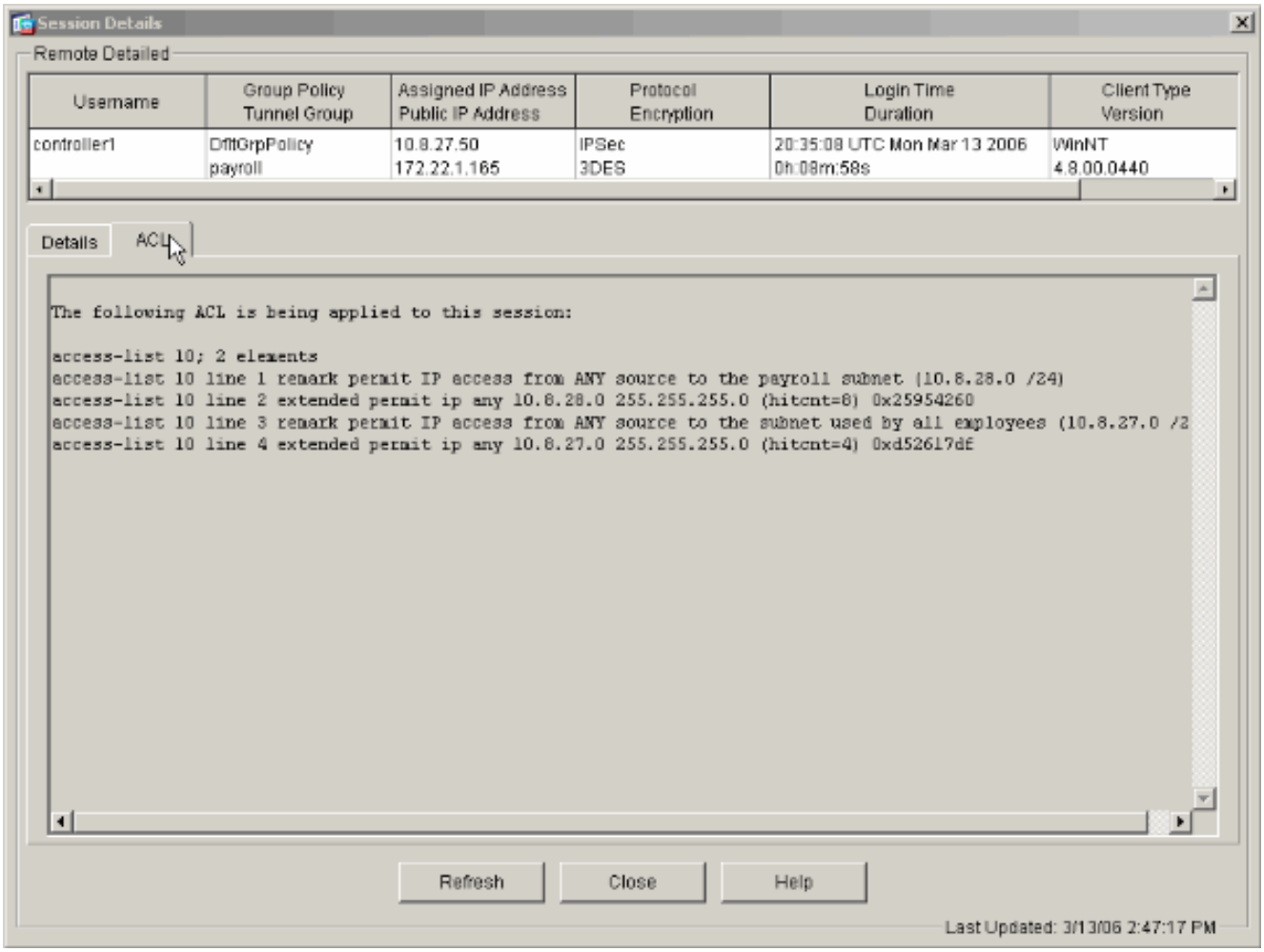
Verificación

Utilice las capacidades de monitoreo del ASDM de verificar su configuración:

1. Seleccione la **supervisión > el VPN > los VPN statistics (Estadísticas de la VPN) > las sesiones**.Usted ve a las sesiones de VPN activas en el PIX. Seleccione la sesión que usted está interesado adentro y haga clic los **detalles**.



2. Seleccione la lengueta ACL.Los ACL hitcnt reflejan el tráfico que atraviesa el túnel del cliente a las redes permitidas.



Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Dispositivos de seguridad adaptable Cisco ASA de la serie 5500 ASA como servidor VPN remoto que usa el ejemplo de la Configuración de ASDM
- Ejemplos de configuración y lista de notas técnicas del Dispositivos de seguridad Cisco PIX de la serie 500
- Ejemplos de configuración y lista de notas técnicas del Dispositivos de seguridad adaptable Cisco ASA de la serie 5500
- Ejemplos de configuración y lista de notas técnicas del Cliente Cisco VPN
- Soporte Técnico y Documentación - Cisco Systems