PIX/ASA 7.x ASDM: Einschränkung des Netzwerkzugriffs von VPN-Benutzern mit Remote-Zugriff

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration mit dem Cisco Adaptive Security Device Manager (ASDM), um festzulegen, auf welche internen Netzwerke Remote-Access-VPN-Benutzer hinter der PIX Security Appliance oder der Adaptive Security Appliance (ASA) zugreifen können. Sie können Remotezugriff-VPN-Benutzer auf die Bereiche des Netzwerks beschränken, auf die sie zugreifen möchten, wenn Sie:

1. Erstellen Sie Zugriffslisten.
2. Ordnen Sie sie Gruppenrichtlinien zu.
3. Ordnen Sie diese Gruppenrichtlinien Tunnelgruppen zu.

Unter Konfigurieren des Cisco VPN 3000 Concentrator für Blockierung mit Filtern und RADIUS-Filterzuweisung finden Sie weitere Informationen zu dem Szenario, in dem der VPN Concentrator den Zugriff von VPN-Benutzern blockiert.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Das PIX kann mithilfe des ASDM konfiguriert werden.**Hinweis:** Informationen zur Konfiguration des PIX durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.
- Sie haben mindestens eine zweifelsfrei funktionierende VPN-Konfiguration für den Remote-Zugriff eingerichtet.**Hinweis:** Wenn Sie über keine dieser Konfigurationen verfügen, finden Sie im ASA-as-a-Remote-VPN-Server unter Verwendung des ASDM-Konfigurationsbeispiels weitere Informationen zum Konfigurieren einer guten VPN-Konfiguration für den Remote-Zugriff.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Secure PIX Security Appliance der Serie 500, Version 7.1(1)**Hinweis:** Die Sicherheitslösungen PIX 501 und 506E unterstützen Version 7.x nicht.
- Cisco Adaptive Security Device Manager Version 5.1(1)**Hinweis:** Das ASDM ist nur in PIX oder ASA 7.x verfügbar.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

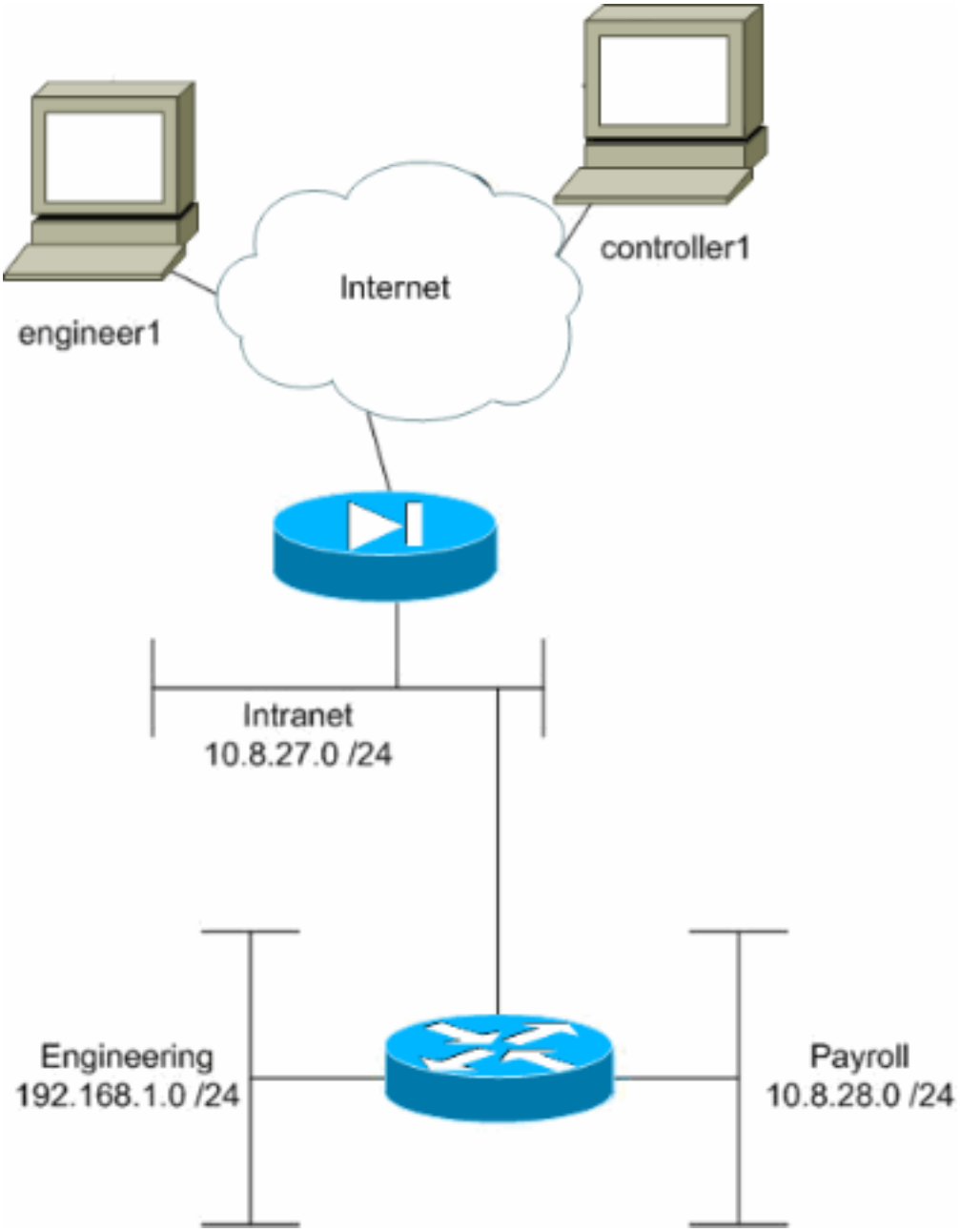
Zugehörige Produkte

Diese Konfiguration kann auch mit den folgenden Hardware- und Softwareversionen verwendet werden:

- Cisco Adaptive Security Appliance der Serie ASA 5500, Version 7.1(1)

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



In diesem Konfigurationsbeispiel ist ein kleines Unternehmensnetzwerk mit drei Subnetzen vorgesehen. Dieses Diagramm zeigt die Topologie. Die drei Subnetze sind Intranet, Engineering und Payroll. Ziel dieses Konfigurationsbeispiels ist es, dem Gehaltsabrechnungspersonal den Remote-Zugriff auf die Subnetze für Intranet und Payroll zu ermöglichen und diesen den Zugriff auf das Engineering-Subnetz zu verwehren. Außerdem sollten die Techniker remote auf die Subnetze Intranet und Engineering, nicht aber auf das Payroll-Subnetz zugreifen können. Der Payroll-Benutzer in diesem Beispiel ist "controller1". Der technische Benutzer in diesem Beispiel ist "engineering1".

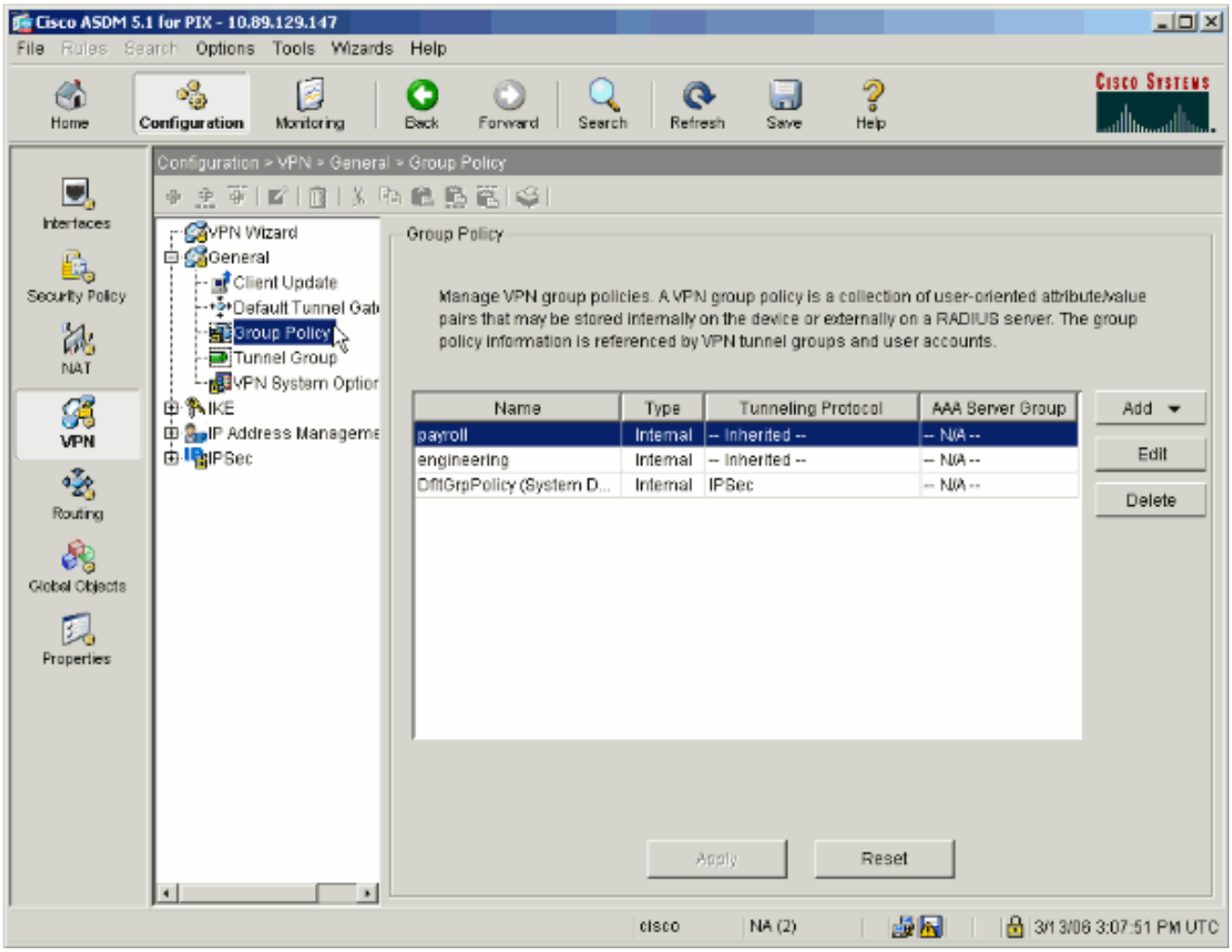
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

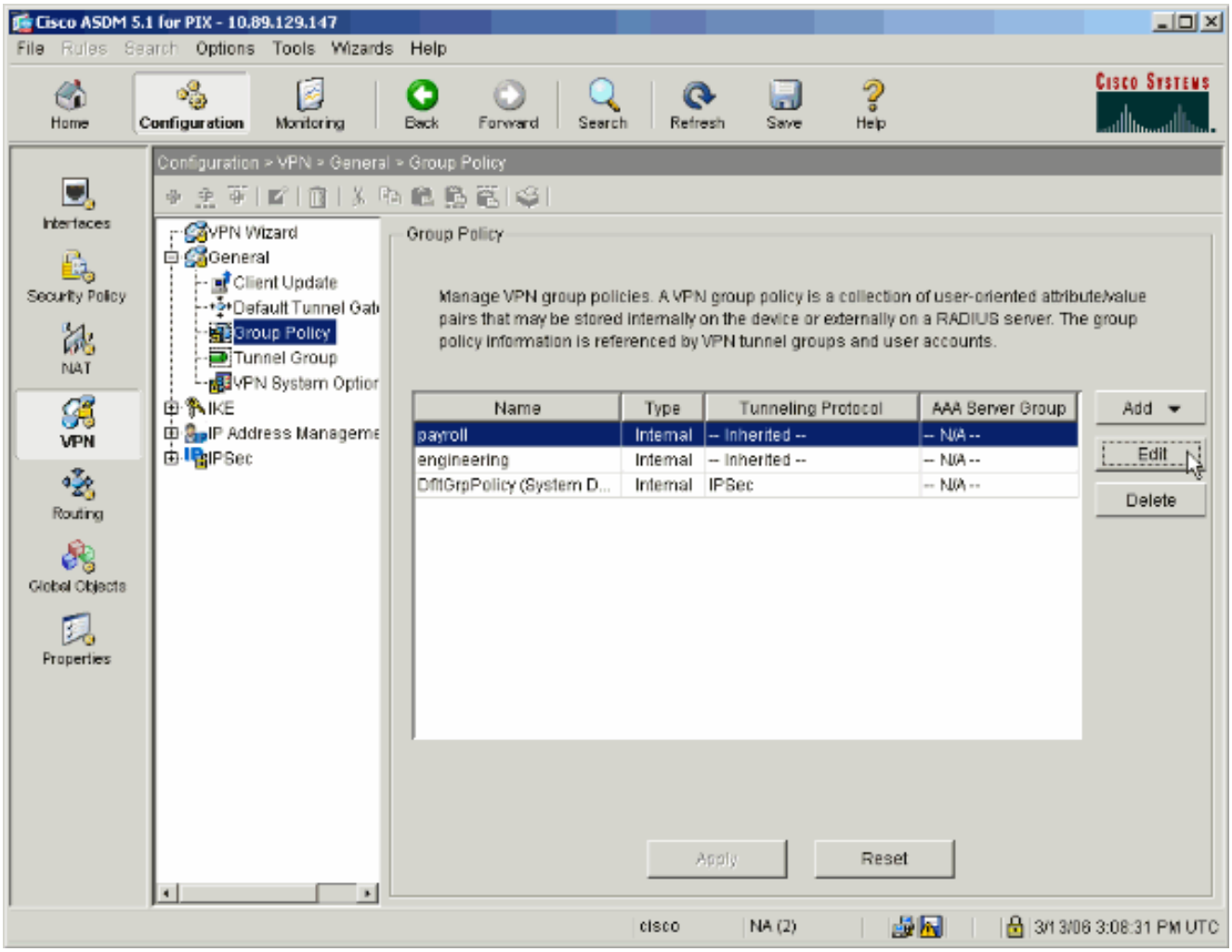
Konfiguration des Zugriffs über ASDM

Gehen Sie wie folgt vor, um die PIX Security Appliance mithilfe von ASDM zu konfigurieren:

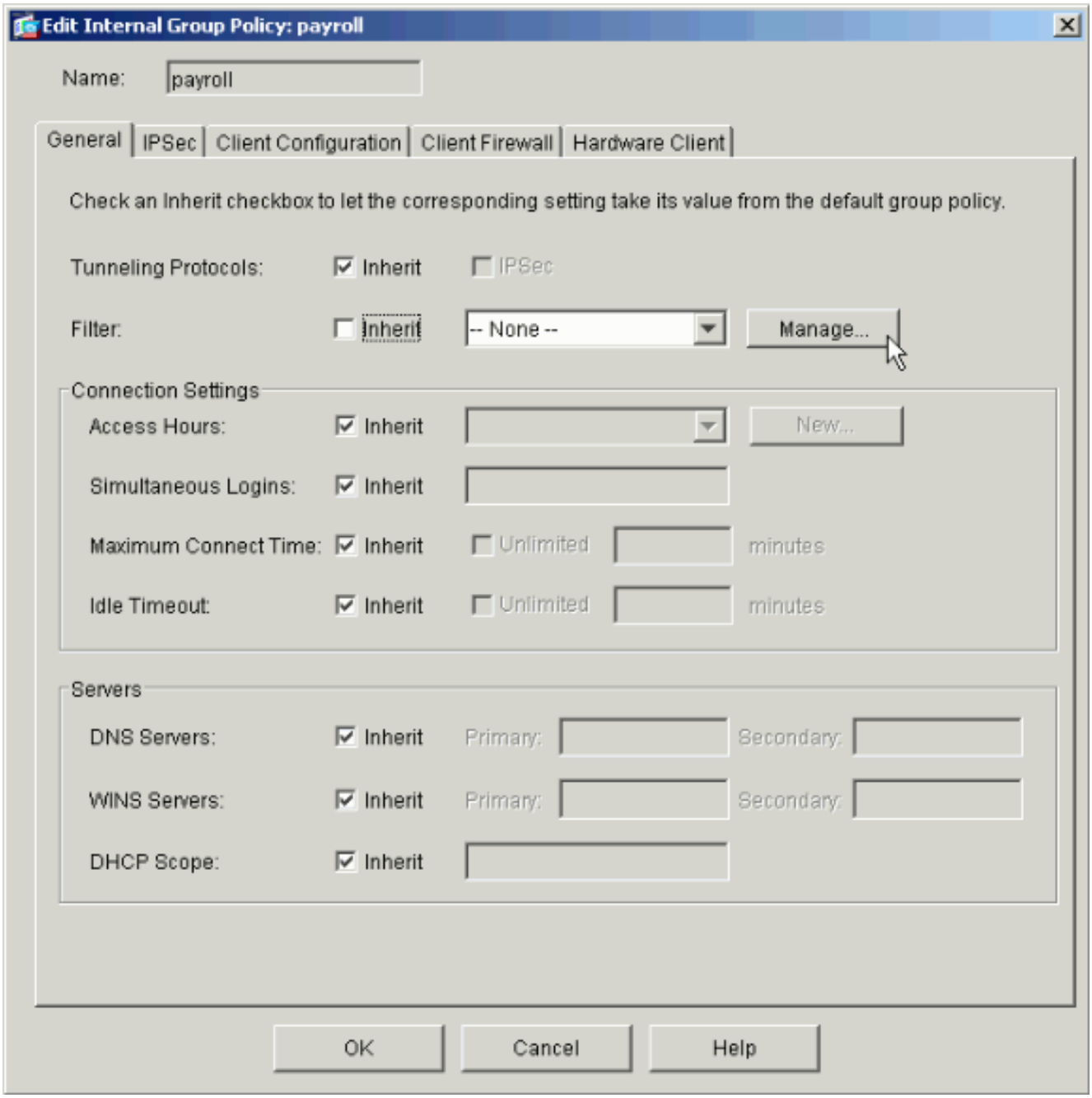
1. Wählen Sie **Konfiguration > VPN > Allgemein > Gruppenrichtlinie aus**.



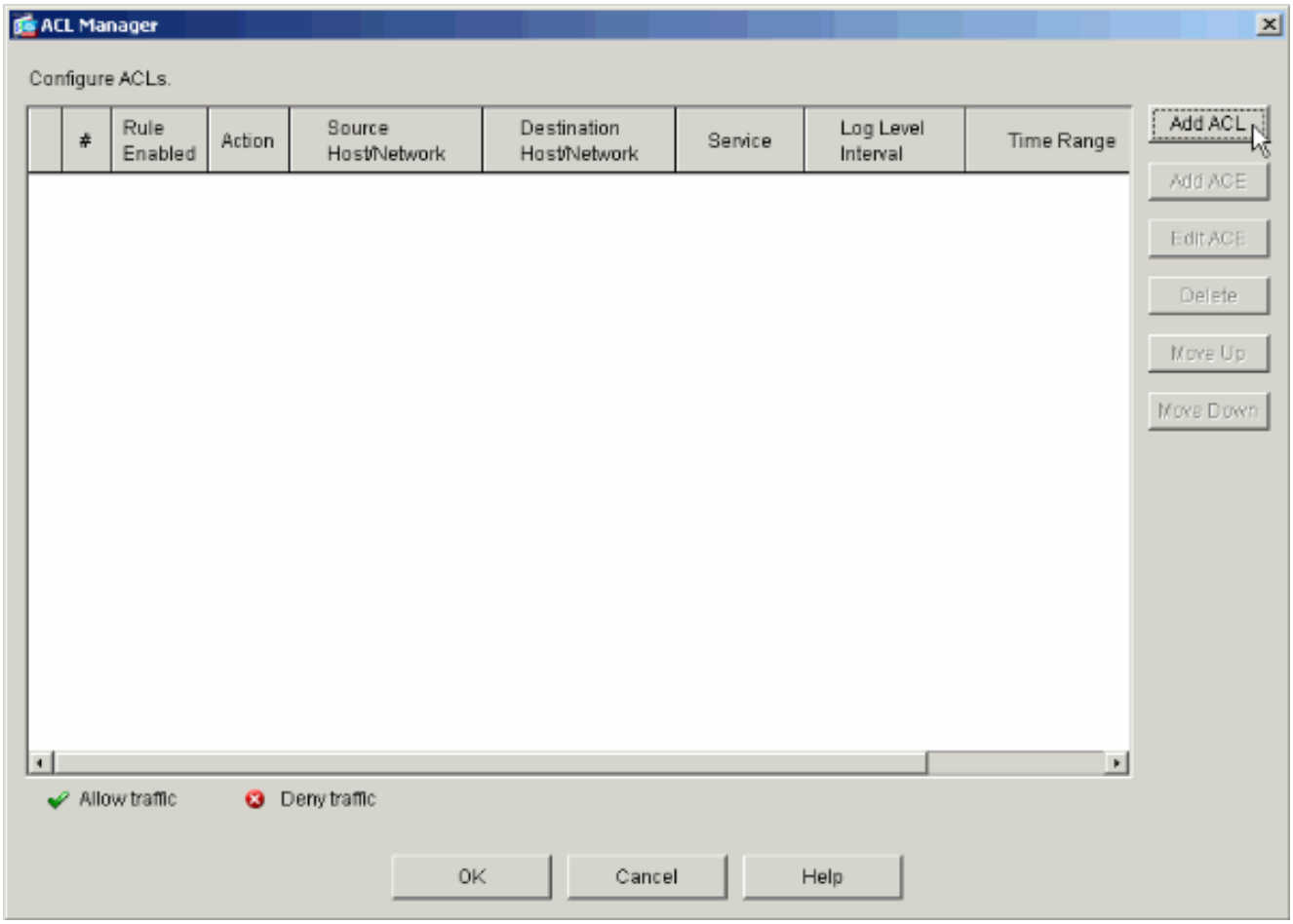
2. Basierend auf den Schritten, die zur Konfiguration von Tunnelgruppen auf dem PIX unternommen wurden, existieren möglicherweise bereits Gruppenrichtlinien für die Tunnelgruppen, deren Benutzer Sie beschränken möchten. Wenn bereits eine geeignete Gruppenrichtlinie vorhanden ist, wählen Sie diese aus, und klicken Sie auf **Bearbeiten**. Andernfalls klicken Sie auf **Hinzufügen** und wählen **Interne Gruppenrichtlinie aus...**.



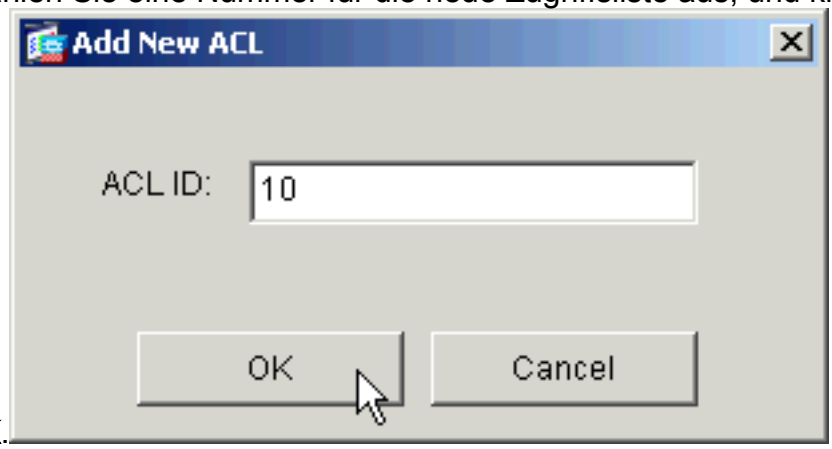
3. Geben Sie ggf. den Namen der Gruppenrichtlinie am oberen Rand des sich öffnenden Fensters ein, oder ändern Sie diesen.
4. Deaktivieren Sie auf der Registerkarte Allgemein das Kontrollkästchen **Erben** neben Filter, und klicken Sie dann auf **Verwalten**.



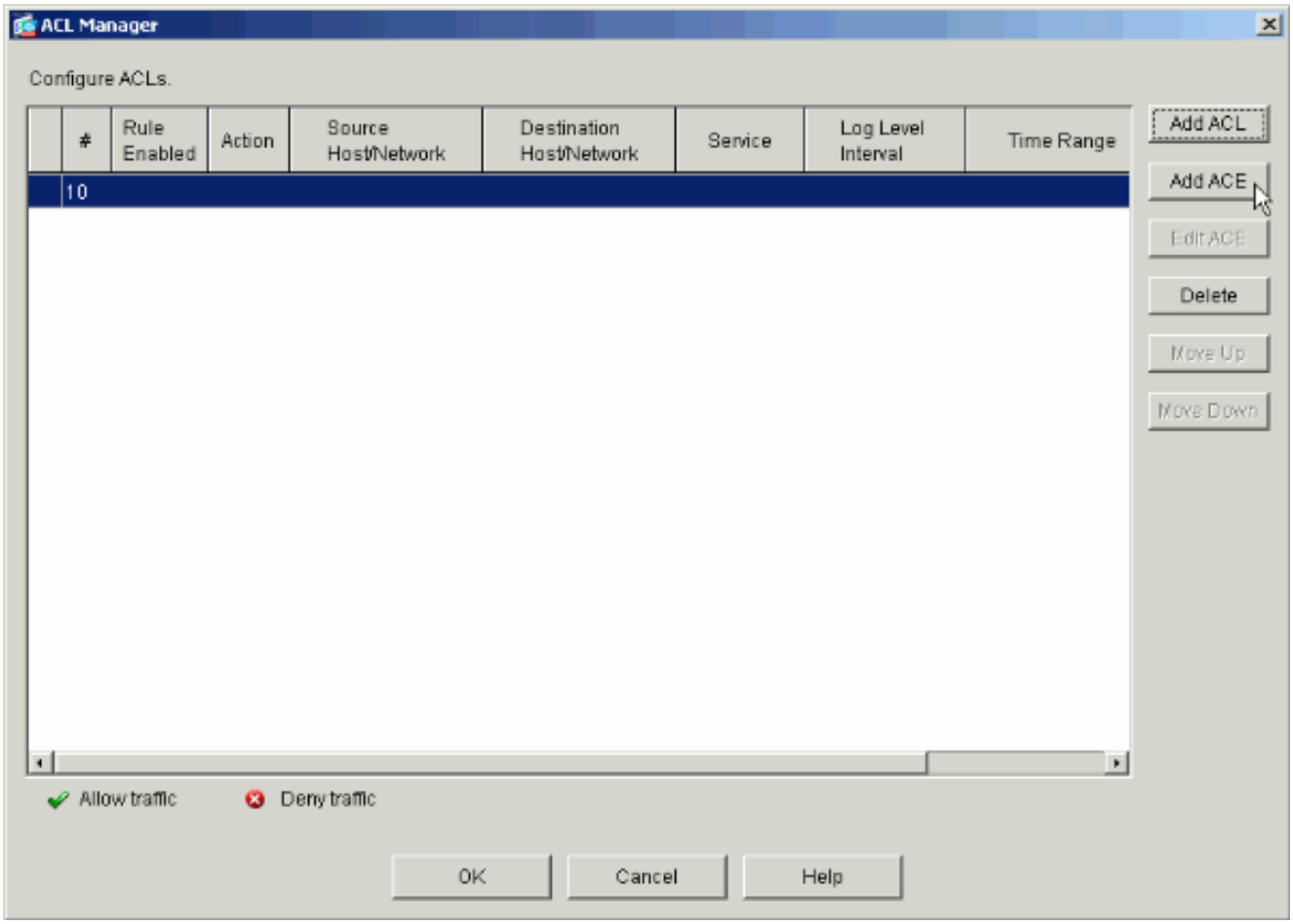
5. Klicken Sie auf **ACL hinzufügen**, um im daraufhin angezeigten Fenster ACL Manager eine neue Zugriffsliste zu
erstellen.



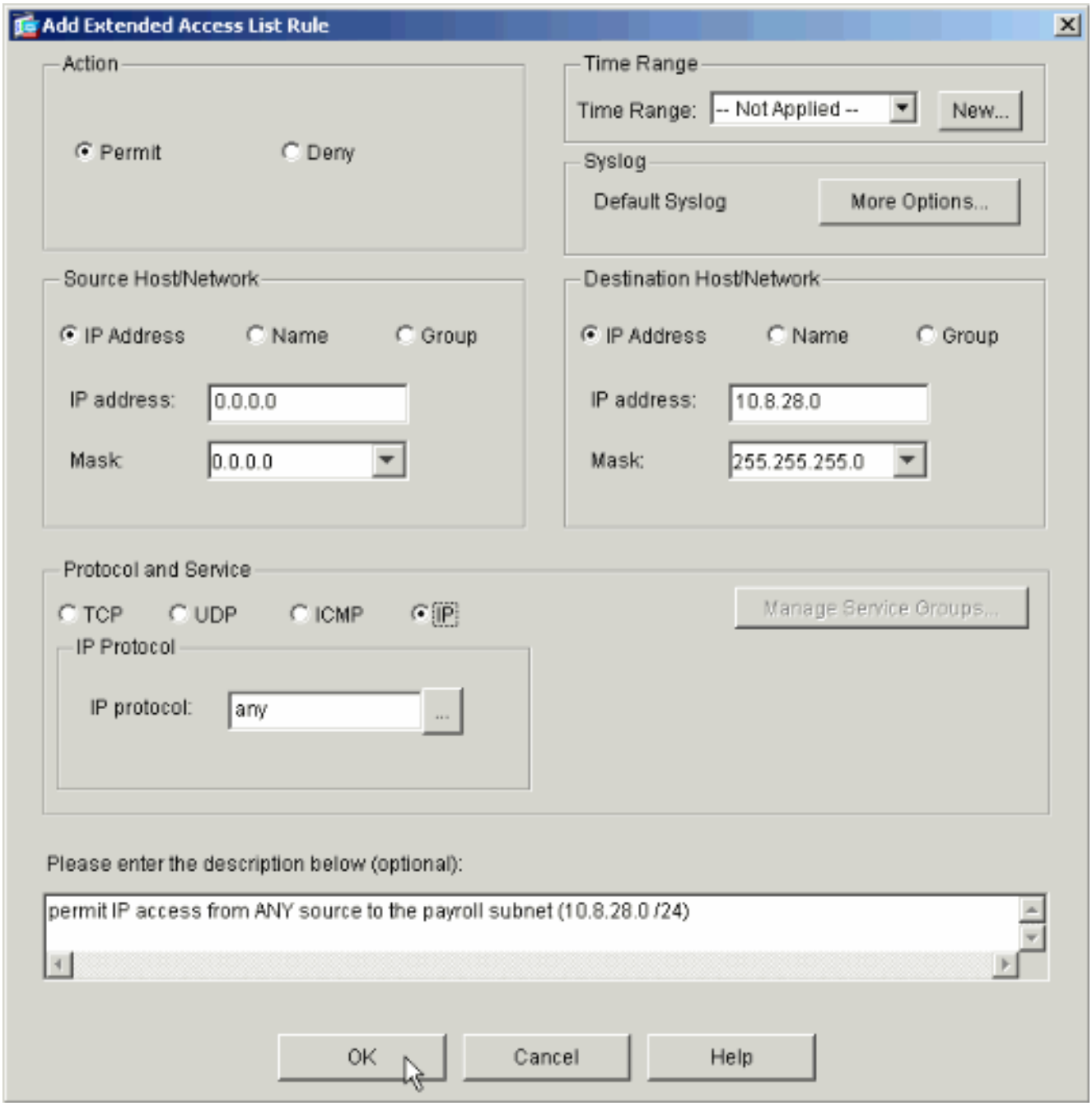
6. Wählen Sie eine Nummer für die neue Zugriffsliste aus, und klicken Sie auf **OK**.



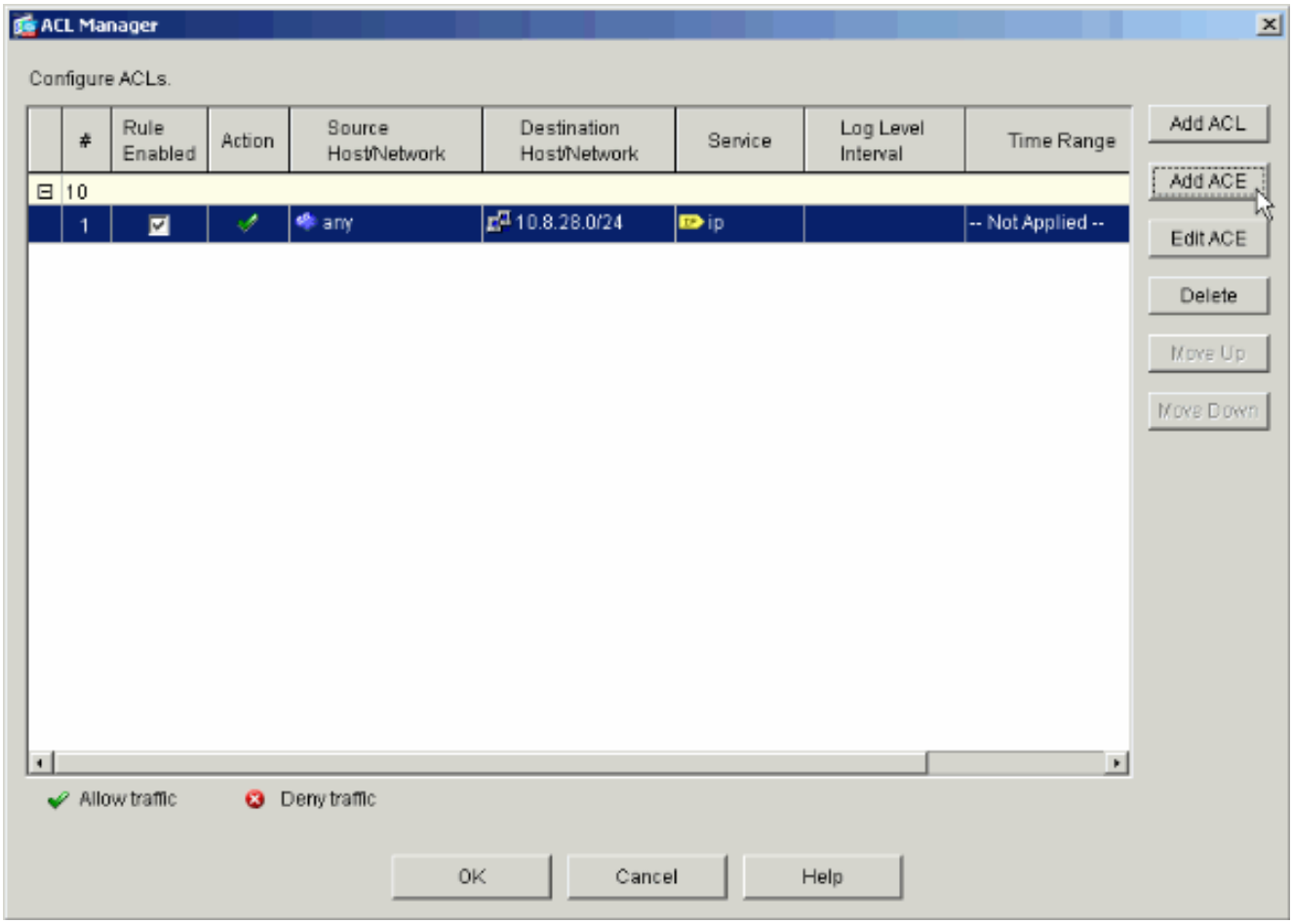
7. Wenn Ihre neue ACL links ausgewählt ist, klicken Sie auf **Add ACE (ACE hinzufügen)**, um der Liste einen neuen Zugriffssteuerungseintrag hinzuzufügen.



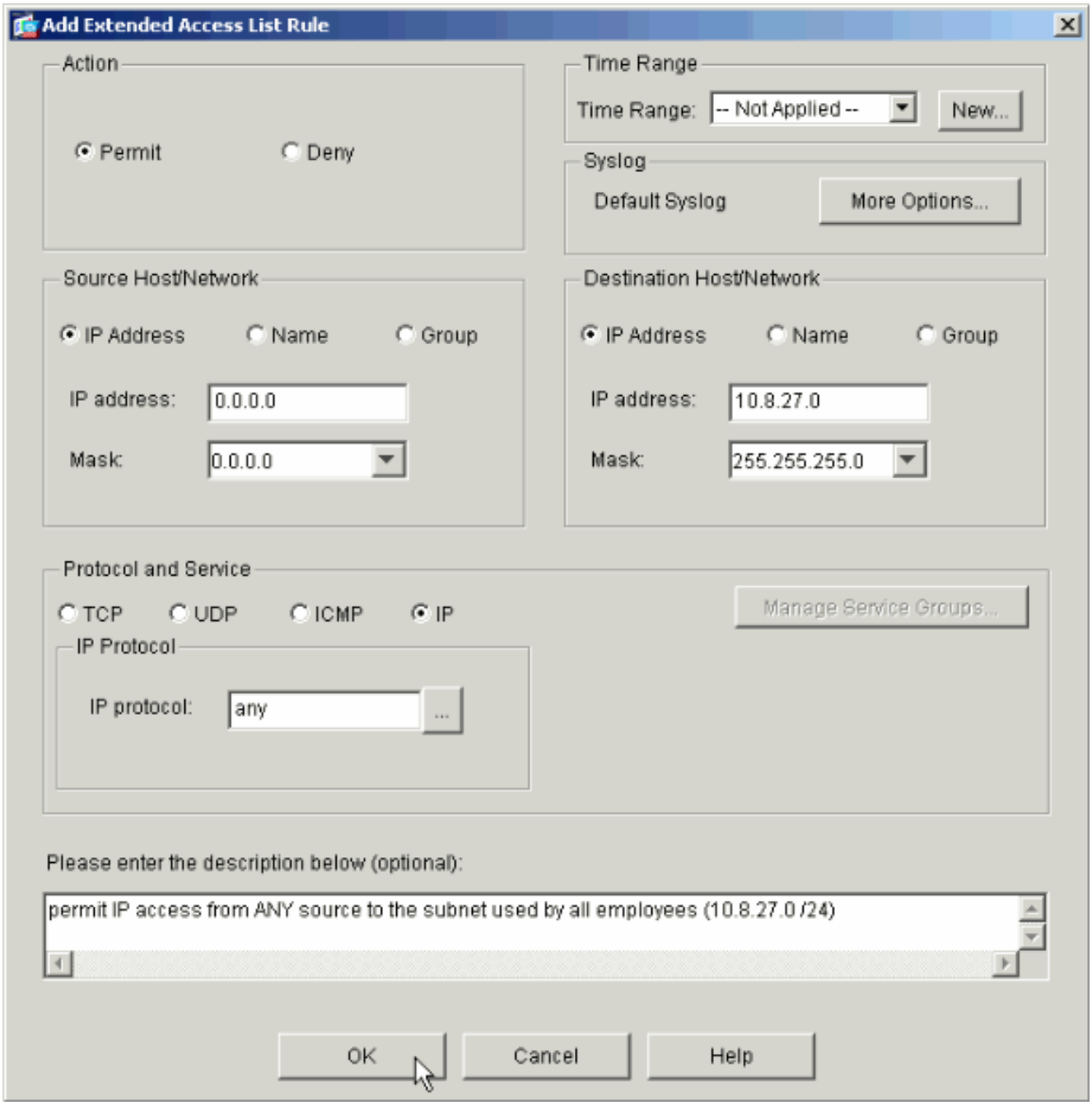
8. Definieren Sie den hinzuzufügenden Zugriffssteuerungseintrag (ACE).In diesem Beispiel erlaubt der erste ACE in ACL 10 den IP-Zugriff auf das Payroll-Subnetz von einer beliebigen Quelle.**Hinweis:** Standardmäßig wählt ASDM nur TCP als Protokoll aus. Sie müssen IP auswählen, wenn Sie den Benutzern vollständigen IP-Zugriff erlauben oder verweigern möchten. Klicken Sie abschließend auf
OK.



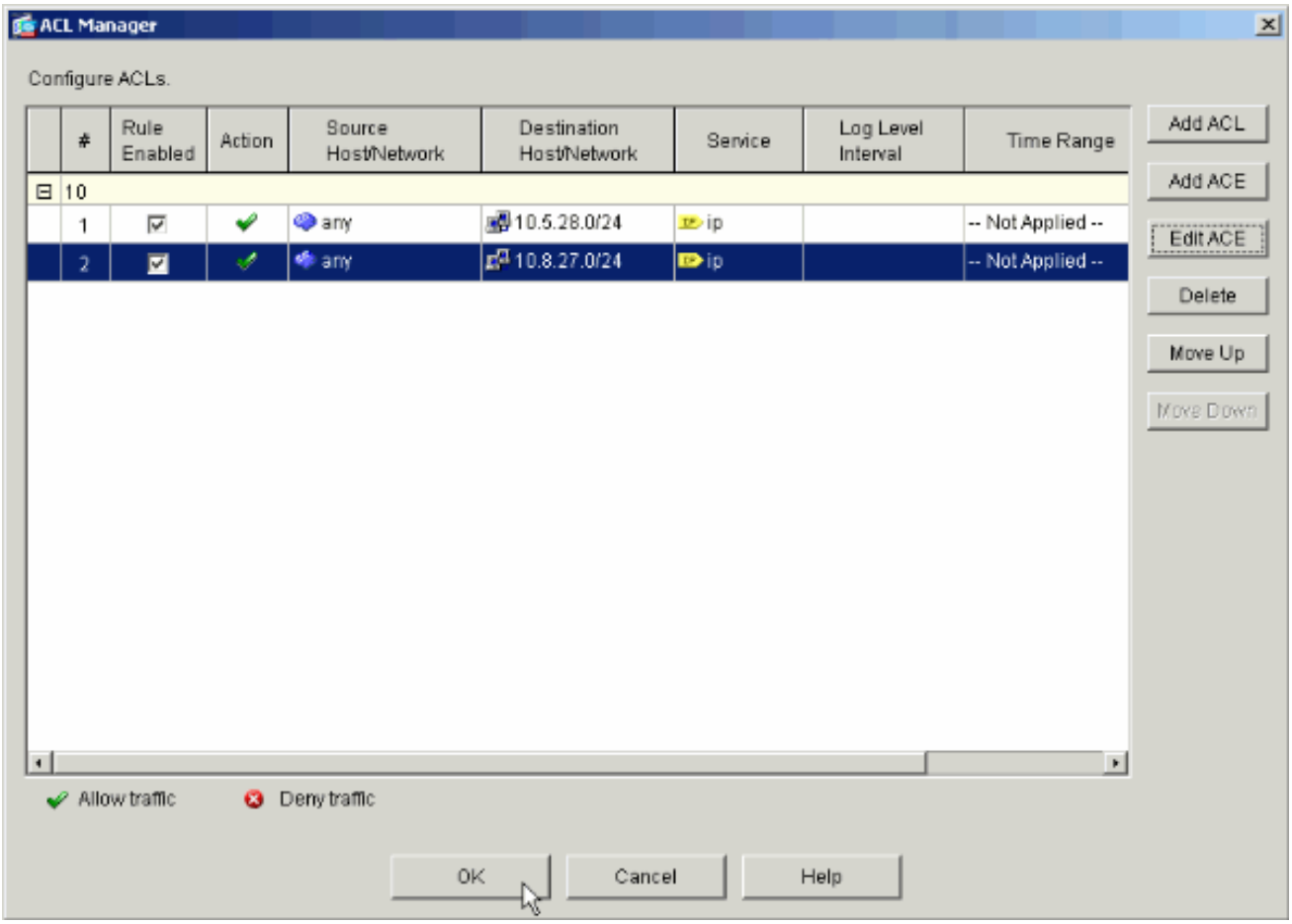
9. Der gerade hinzugefügte ACE wird nun in der Liste angezeigt. Wählen Sie erneut **ACE hinzufügen**, um weitere Zeilen zur Zugriffsliste hinzuzufügen.



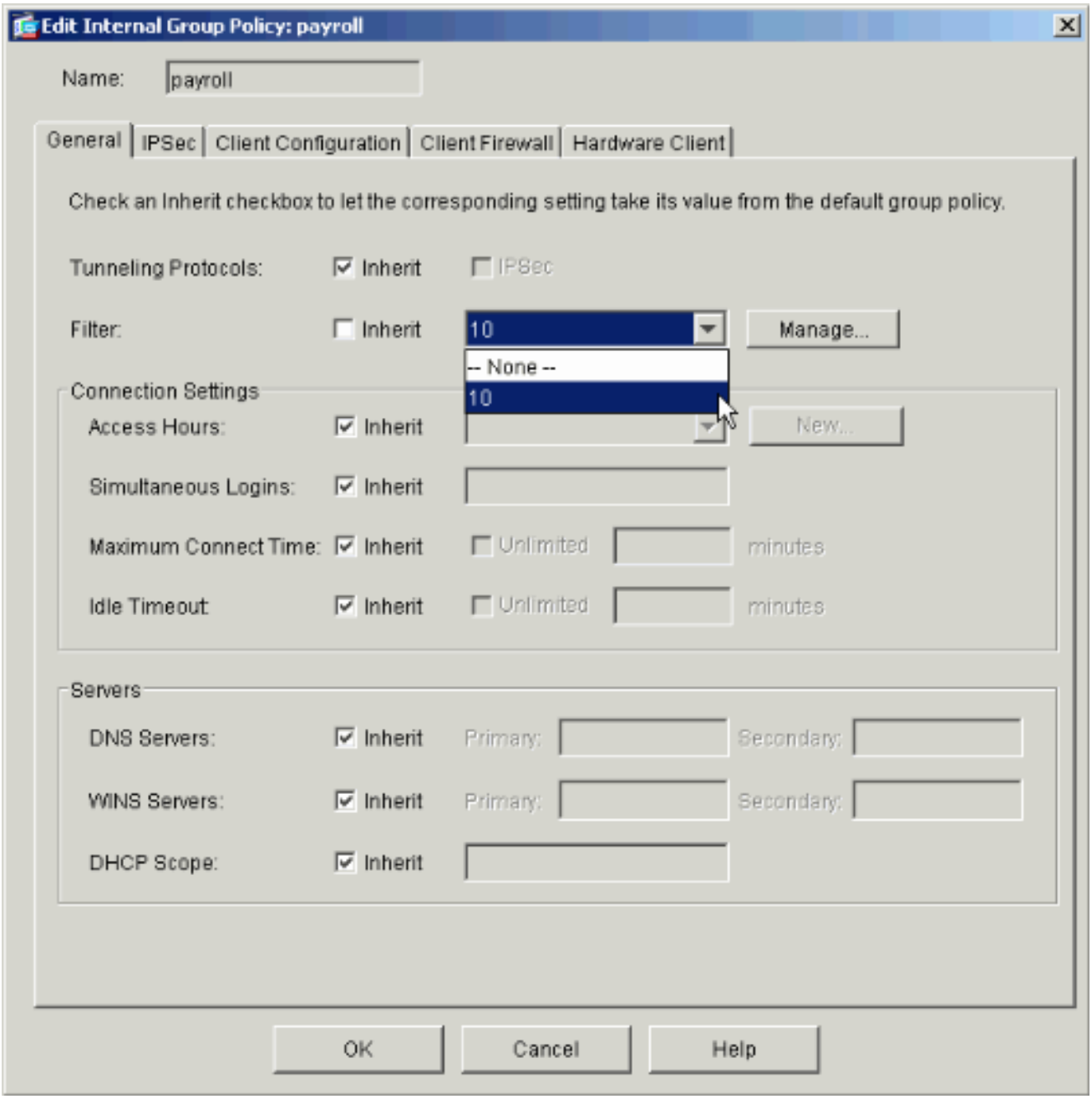
In diesem Beispiel wird ACL 10 ein zweiter ACE hinzugefügt, um den Zugriff auf das Intranet-Subnetz zu
ermöglichen.



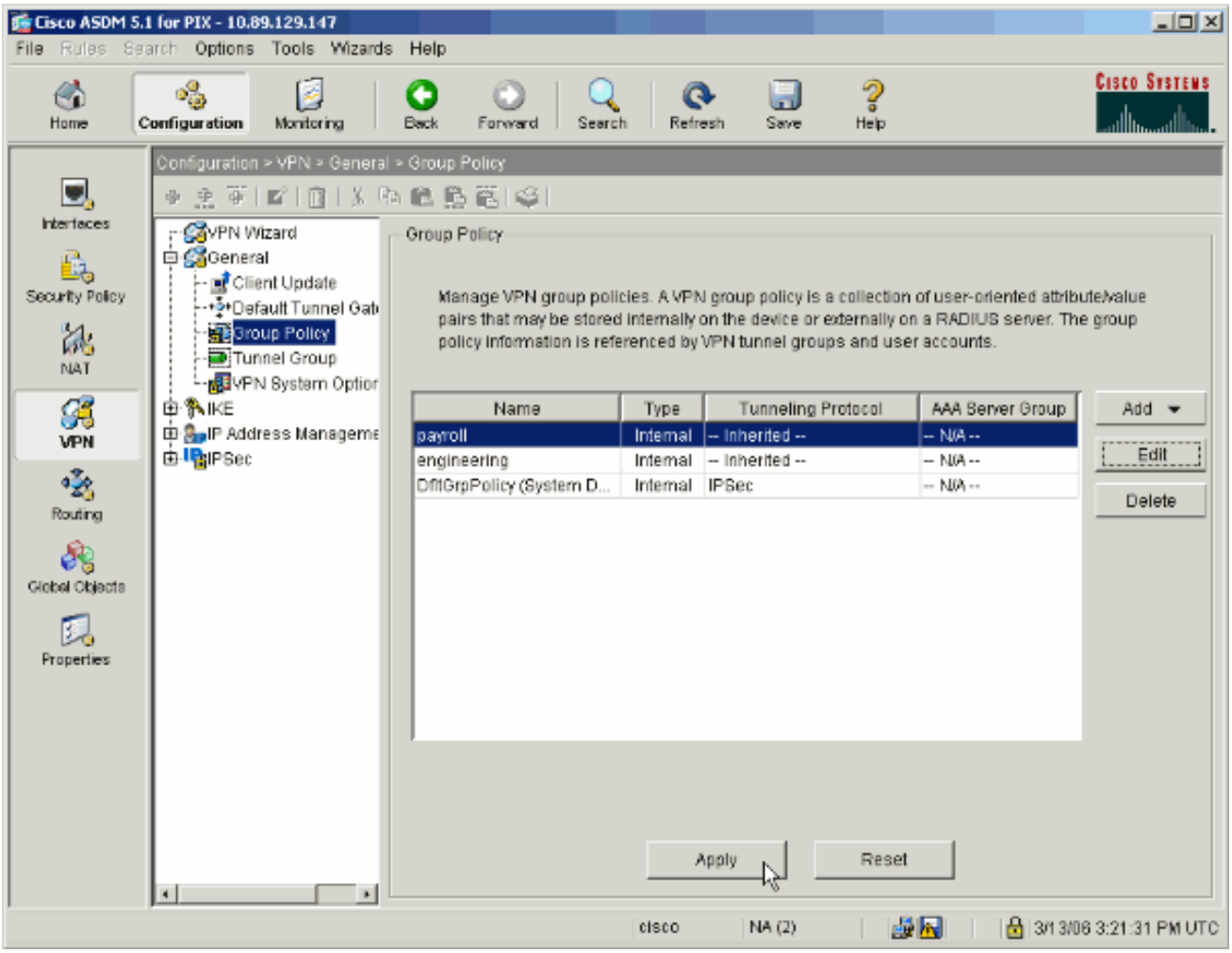
10. Klicken Sie nach dem Hinzufügen von ACEs auf **OK**.



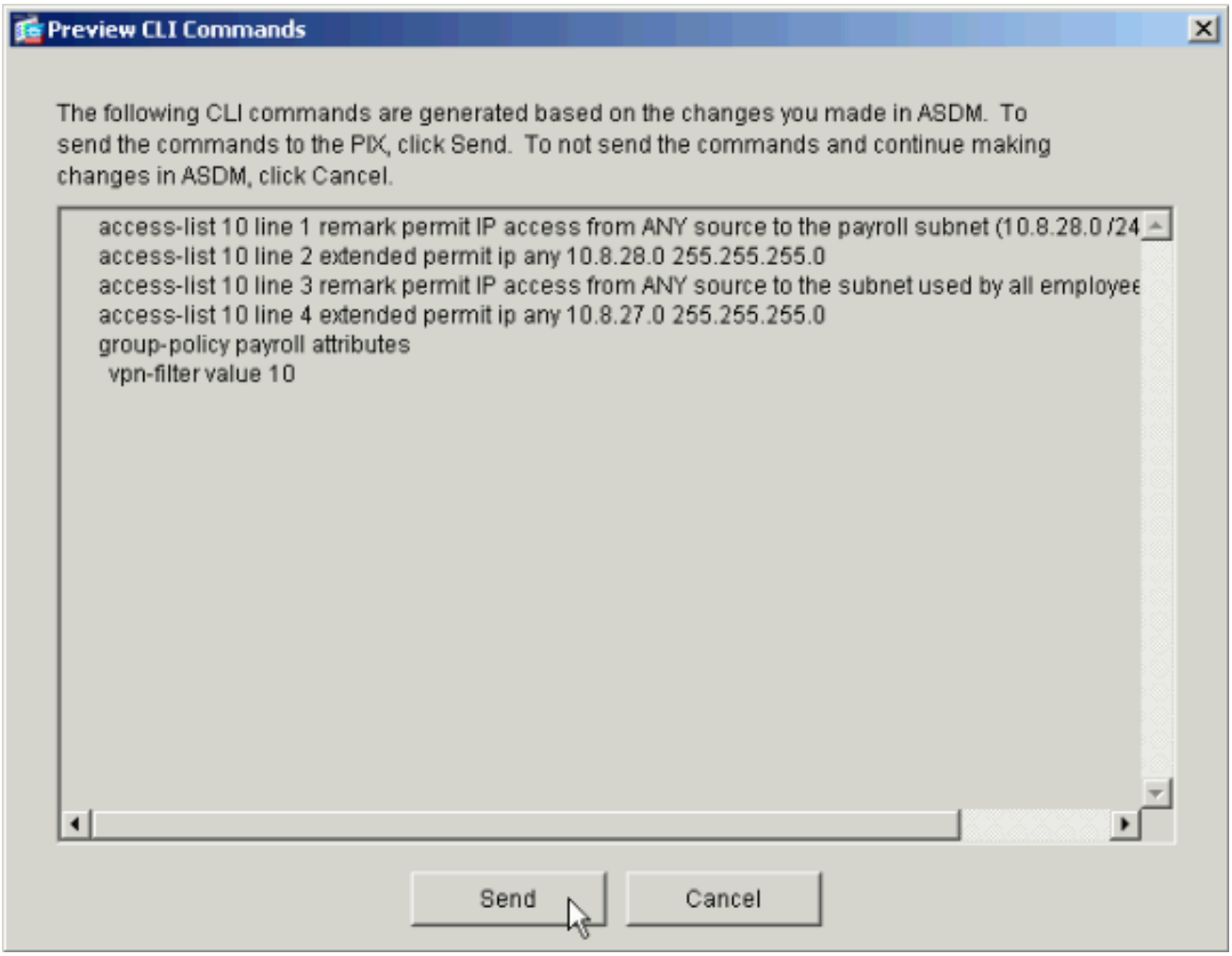
11. Wählen Sie die in den letzten Schritten definierte und ausgefüllte ACL aus, um als Filter für Ihre Gruppenrichtlinie zu dienen. Klicken Sie abschließend auf **OK**.



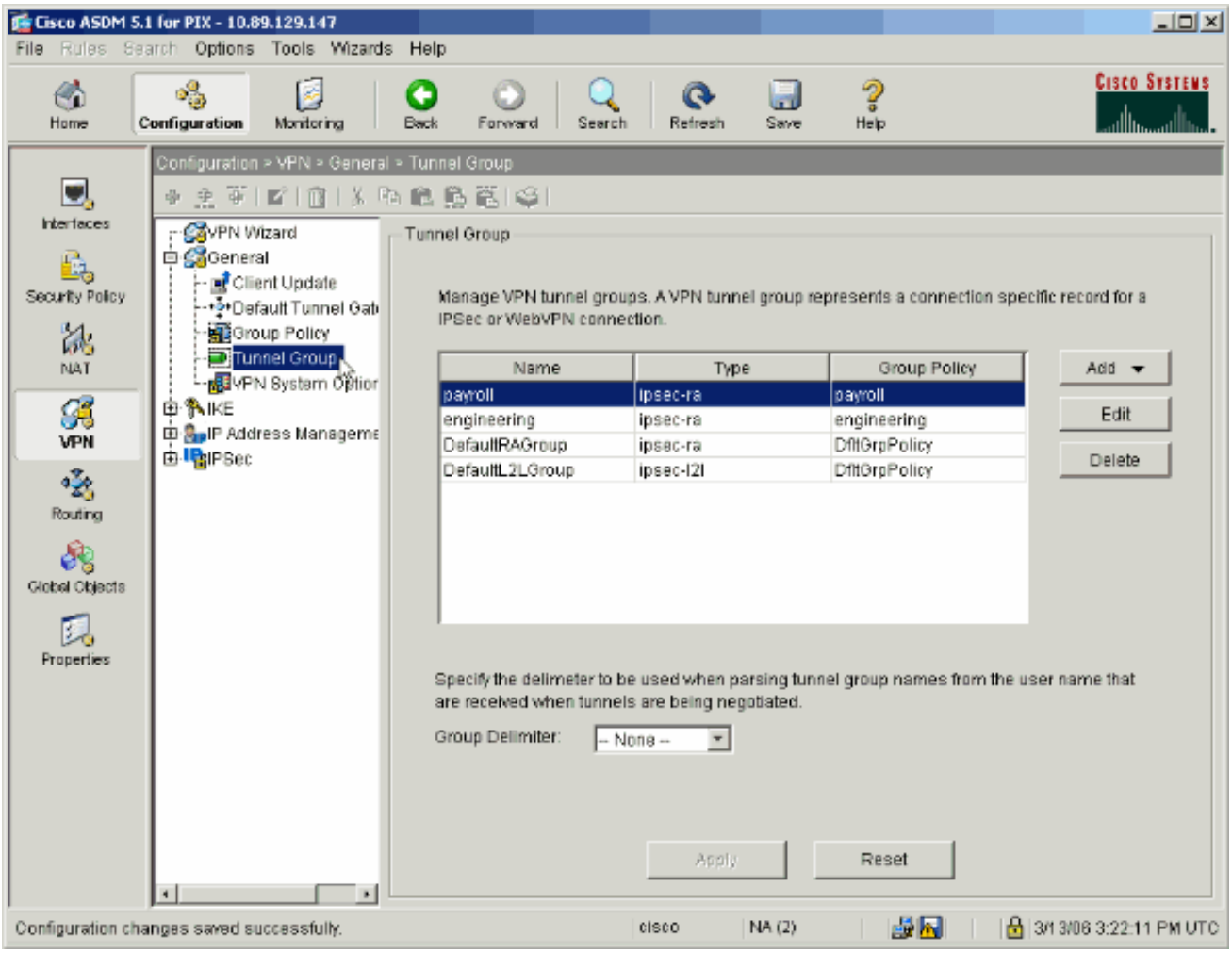
12. Klicken Sie auf **Apply**, um die Änderungen an PIX zu senden.



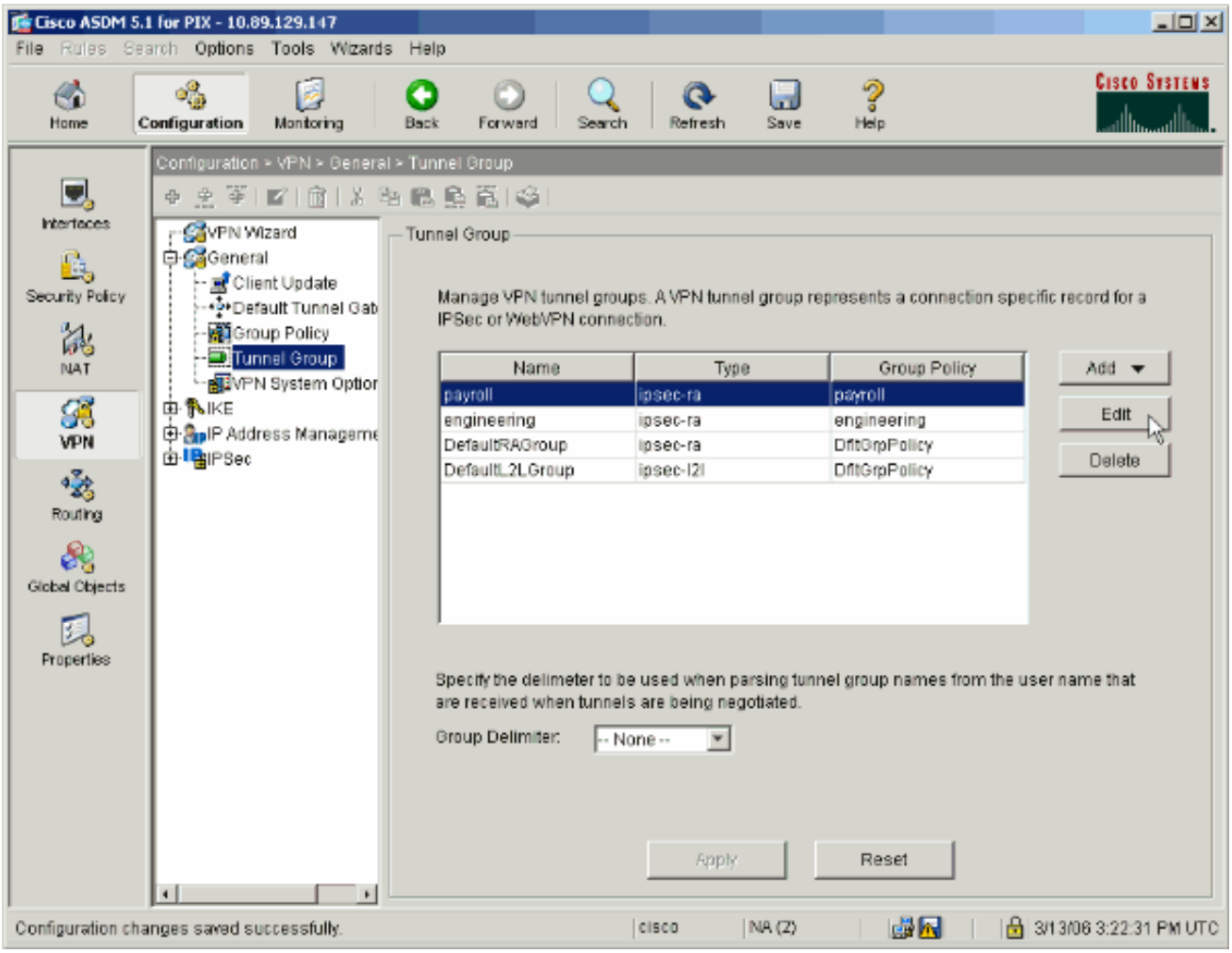
13. Wenn Sie dies unter **Optionen > Voreinstellungen** konfiguriert haben, zeigt der ASDM im Voraus die Befehle an, die er an den PIX senden möchte. Klicken Sie auf **Senden**.



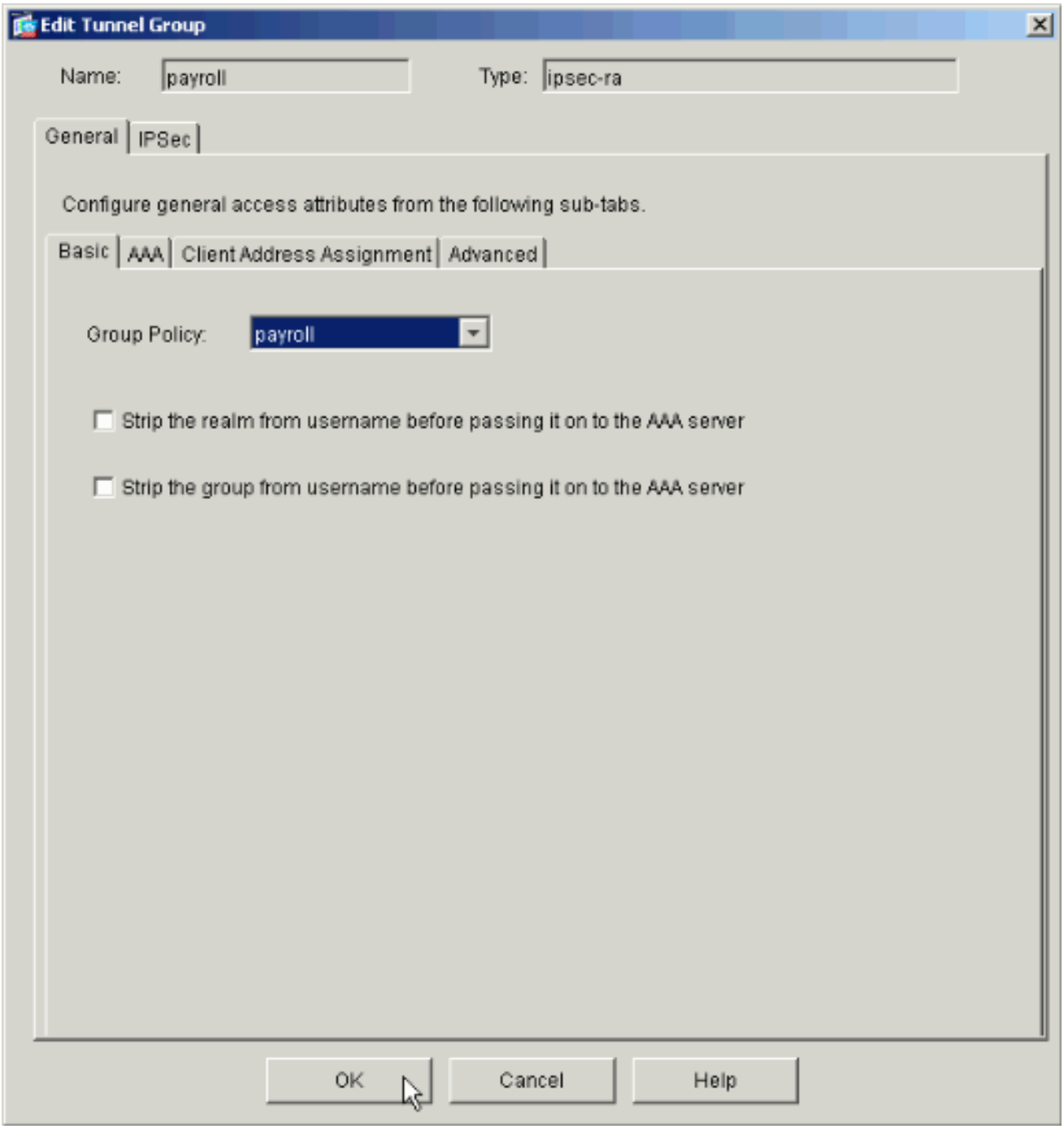
14. Wenden Sie die soeben erstellte oder geänderte Gruppenrichtlinie auf die richtige Tunnelgruppe an. Klicken Sie im linken Rahmen auf **Tunnelgruppe**.



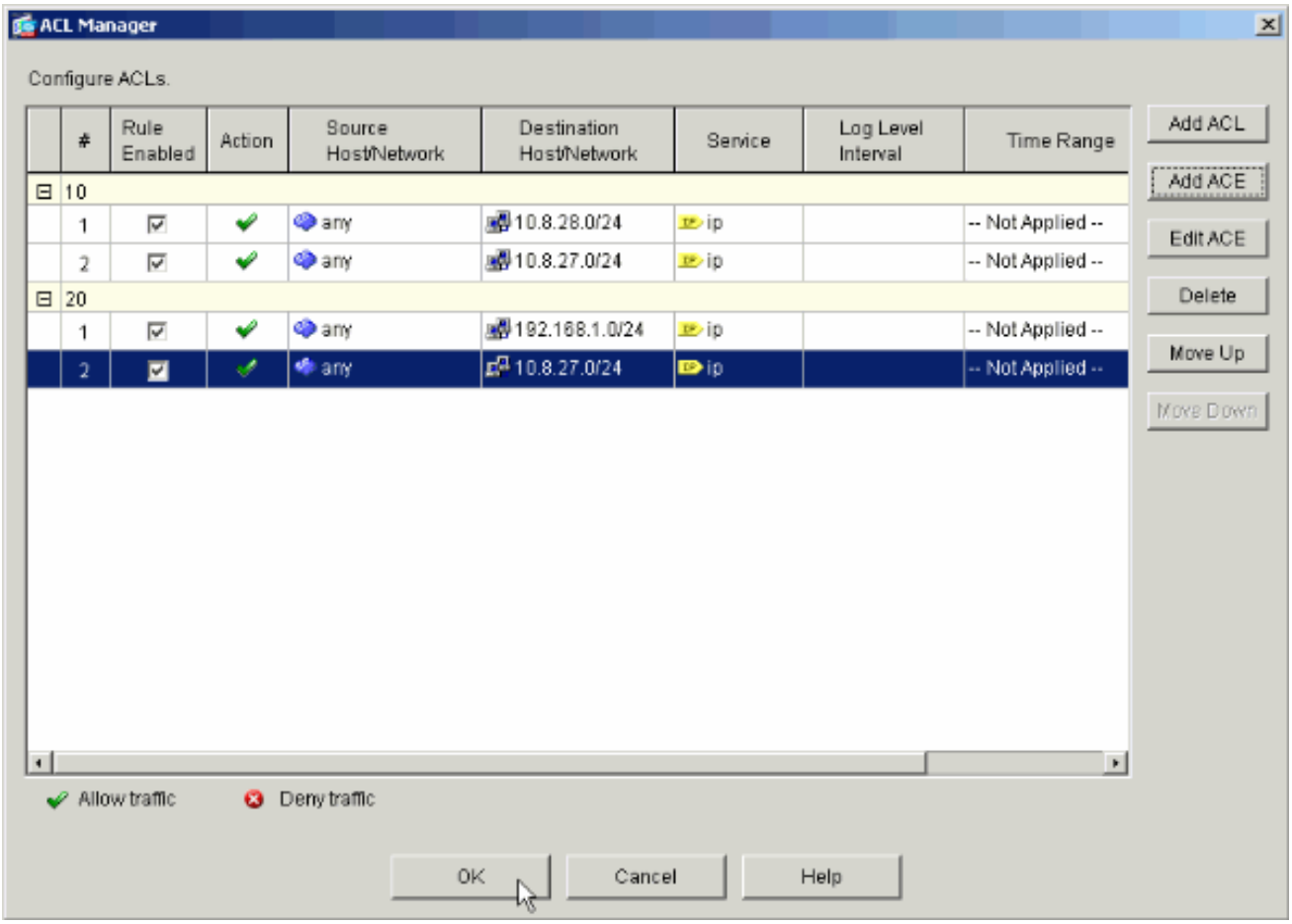
15. Wählen Sie die Tunnelgruppe aus, auf die Sie die Gruppenrichtlinie anwenden möchten, und klicken Sie auf **Bearbeiten**.



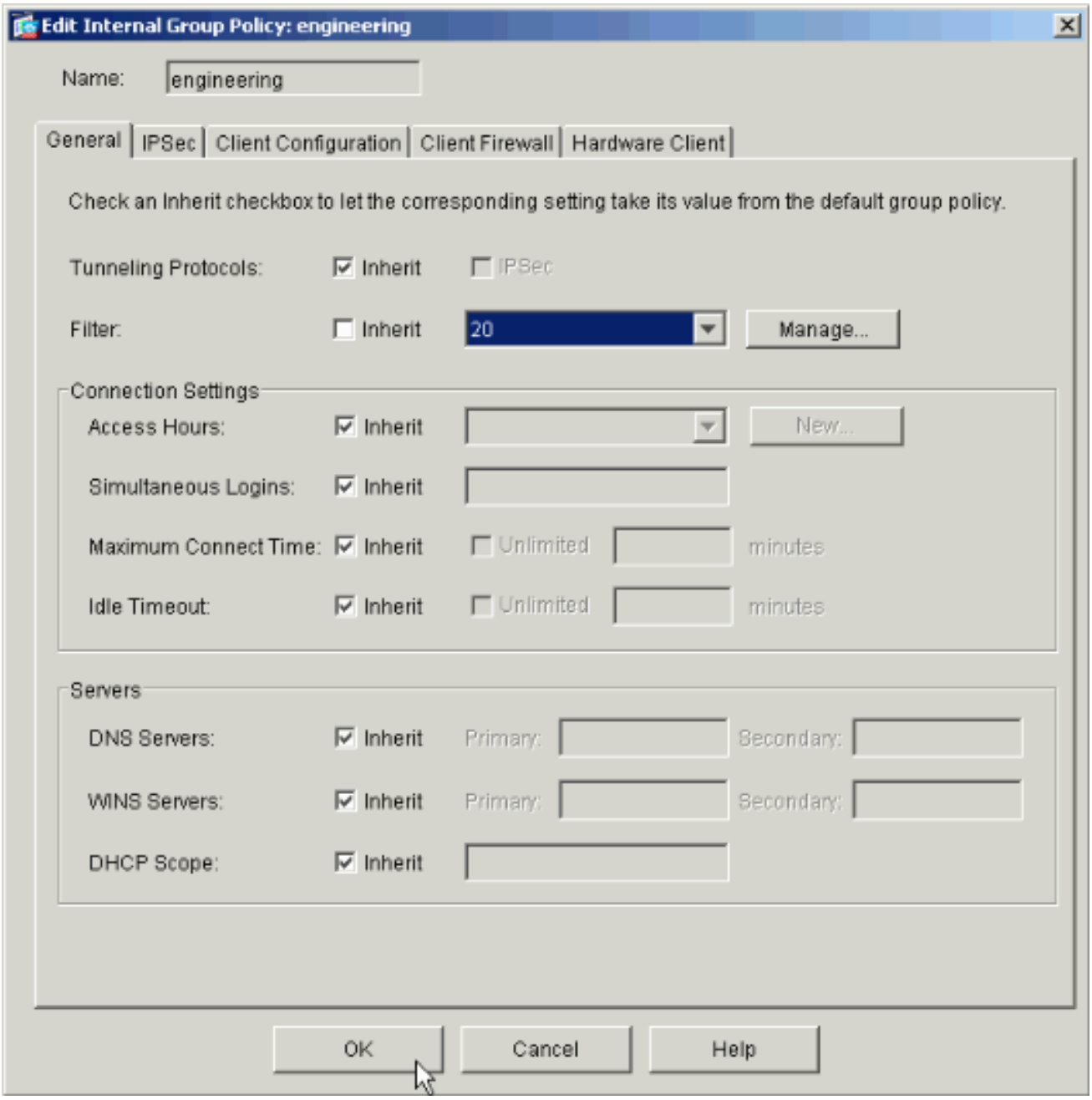
16. Wenn Ihre Gruppenrichtlinie automatisch erstellt wurde (siehe Schritt 2), überprüfen Sie, ob die soeben konfigurierte Gruppenrichtlinie im Dropdown-Feld ausgewählt ist. Wenn Ihre Gruppenrichtlinie nicht automatisch konfiguriert wurde, wählen Sie sie aus dem Dropdown-Feld aus. Klicken Sie abschließend auf
OK.



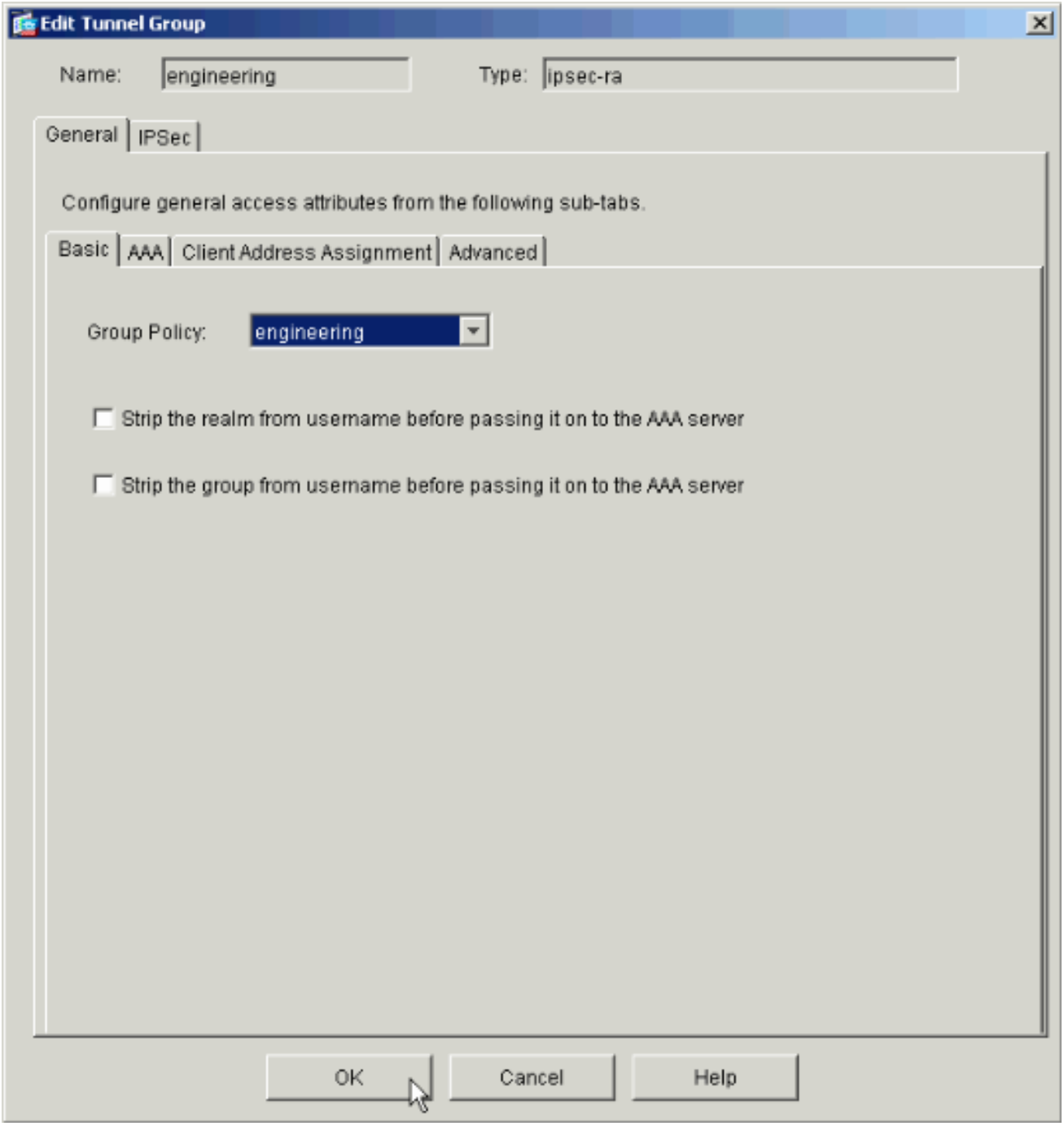
17. Klicken Sie auf **Übernehmen** und, wenn Sie dazu aufgefordert werden, auf **Senden**, um die Änderung zur PIX-Konfiguration hinzuzufügen.Wenn die Gruppenrichtlinie bereits ausgewählt wurde, erhalten Sie möglicherweise die Meldung "Es wurden keine Änderungen vorgenommen." Klicken Sie auf **OK**.
18. Wiederholen Sie die Schritte 2 bis 17 für alle zusätzlichen Tunnelgruppen, denen Sie Einschränkungen hinzufügen möchten.In diesem Konfigurationsbeispiel muss auch der Zugang der Techniker eingeschränkt werden. Obwohl das Verfahren identisch ist, gibt es einige Fenster, in denen Unterschiede erkennbar sind:Neue Zugriffsliste
20



Wählen Sie **Zugriffsliste 20** als Filter in der Richtlinie der Technikergruppe aus.



Überprüfen Sie, ob die Richtlinien der Engineering Group für die Engineering Tunnel Group festgelegt
sind.



Zugriff über CLI konfigurieren

Gehen Sie wie folgt vor, um die Sicherheits-Appliance mithilfe der CLI zu konfigurieren:

Hinweis: Einige der Befehle in dieser Ausgabe werden aus räumlichen Gründen auf eine zweite Zeile herabgesetzt.

1. Erstellen Sie zwei verschiedene Zugriffskontrolllisten (15 und 20), die auf Benutzer angewendet werden, wenn diese eine Verbindung zum VPN für den Remote-Zugriff herstellen. Diese Zugriffsliste wird später in der Konfiguration aufgerufen.

```
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. Erstellen Sie zwei verschiedene VPN-Adresspools. Erstellen Sie eine Gehaltsabrechnung und eine für die Remote-Benutzer Engineering.

```
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. Erstellen Sie Richtlinien für die Gehaltsabrechnung, die nur für sie gelten, wenn sie eine Verbindung herstellen.

```
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. Dieser Schritt ist mit Schritt 3 identisch, mit Ausnahme der Engineering-Gruppe.

```
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. Erstellen Sie lokale Benutzer, und weisen Sie diesen Benutzern die soeben erstellten Attribute zu, um den Zugriff auf Ressourcen zu beschränken.

```
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. Erstellen Sie Tunnelgruppen, die Verbindungsrichtlinien für die Payroll-Benutzer enthalten.

```
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. Erstellen Sie Tunnelgruppen, die Verbindungsrichtlinien für die Engineering-Benutzer enthalten.

```
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
```

Nach Eingabe der Konfiguration wird dieser hervorgehobene Bereich in Ihrer Konfiguration angezeigt:

Gerätename 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
```

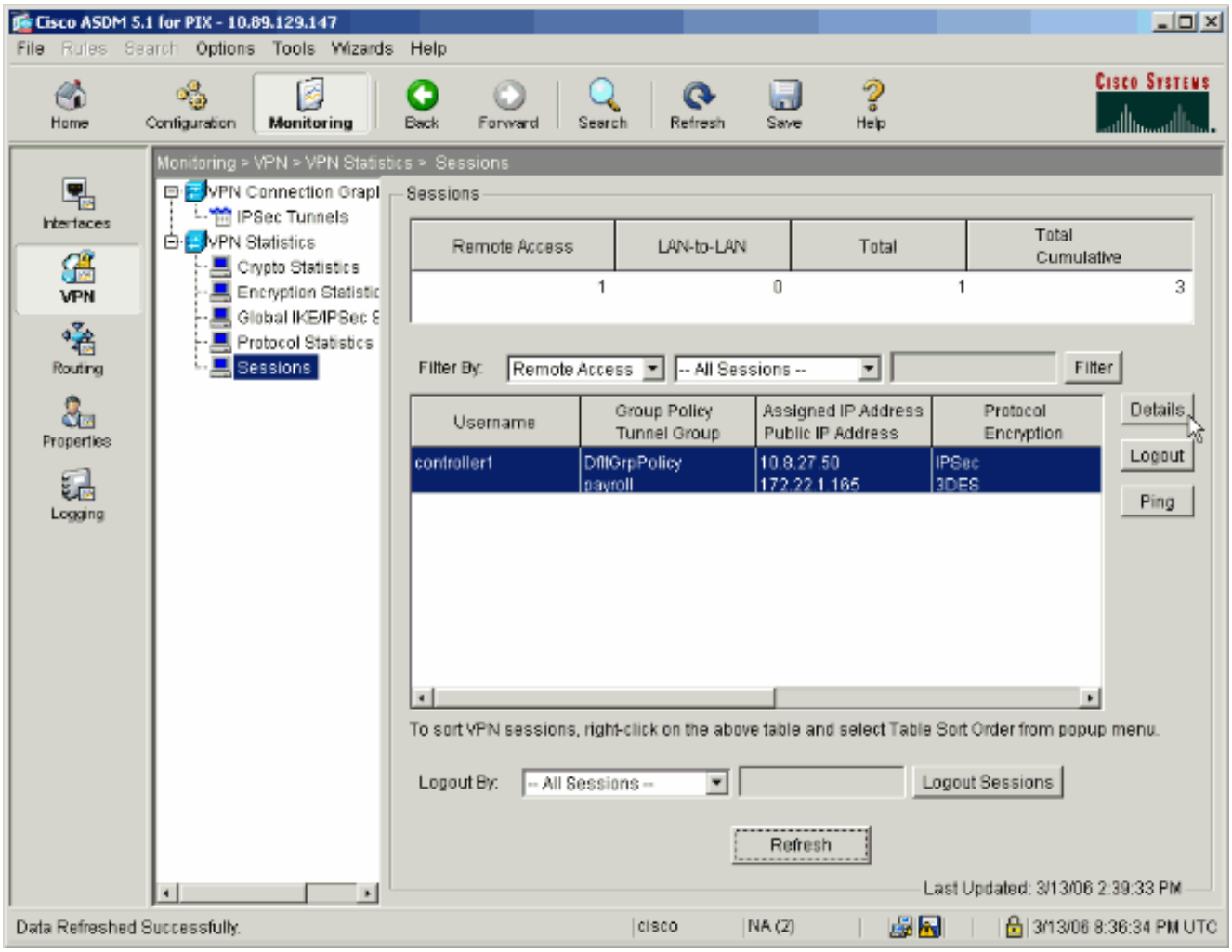
```
no asdm history enable
arp timeout 14400
global (Intranet) 1 interface
nat (Inside) 0 access-list Inside_nat0_outbound
nat (Inside) 1 192.168.1.0 255.255.255.0
nat (Inside) 1 10.8.27.0 255.255.255.0
nat (Inside) 1 10.8.28.0 255.255.255.0
route Intranet 0.0.0.0 0.0.0.0 10.8.27.2
timeout xlate 3:00:00
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)#
```

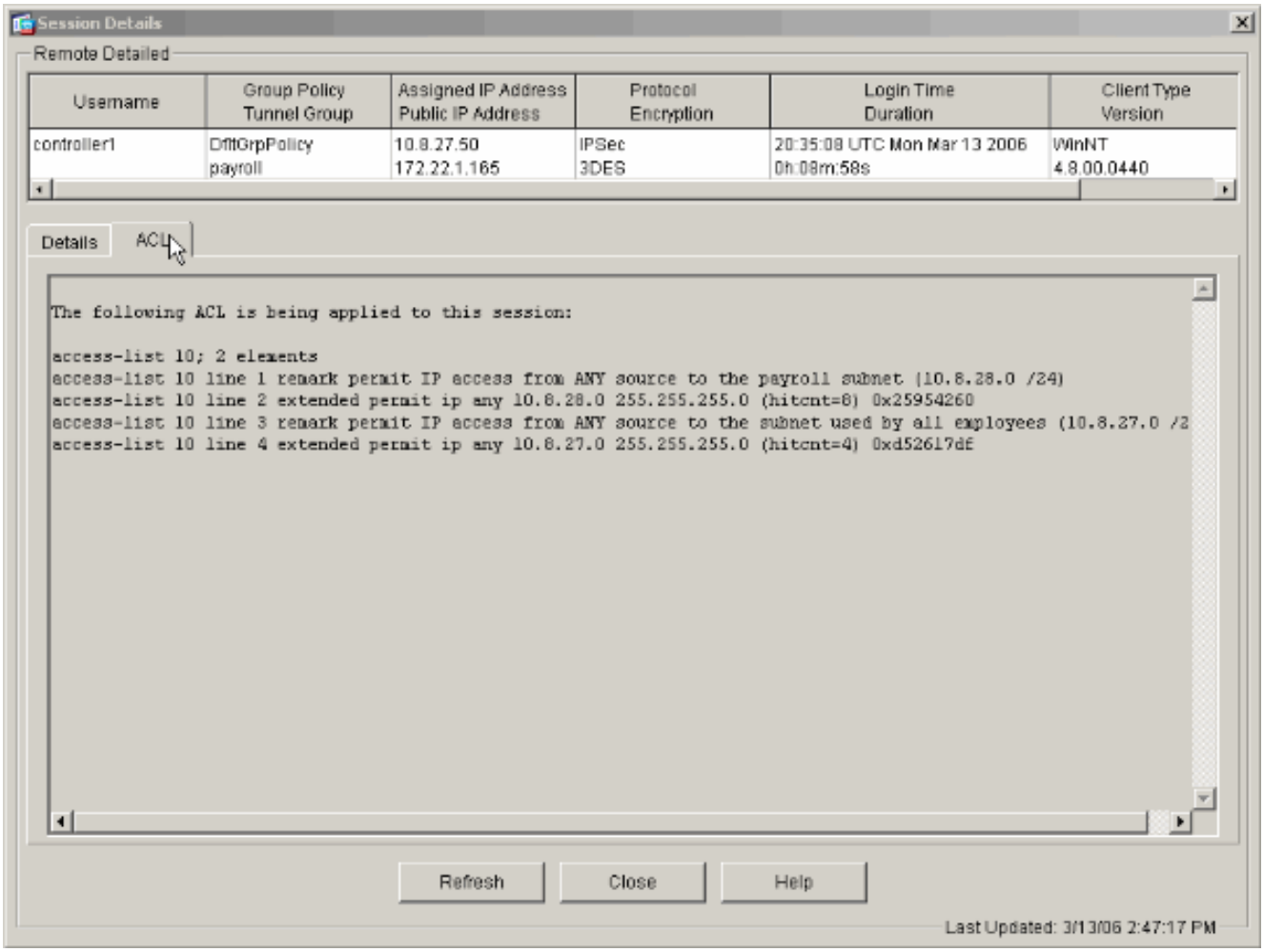
Überprüfen

Überprüfen Sie Ihre Konfiguration mithilfe der Überwachungsfunktionen des ASDM:

1. Wählen Sie **Monitoring > VPN > VPN Statistics > Sessions aus**.Sie sehen die aktiven VPN-Sitzungen auf dem PIX. Wählen Sie die Sitzung aus, die Sie interessieren, und klicken Sie auf
   Details.



2. Wählen Sie die Registerkarte ACL aus.Die Zugriffskontrolllisten reflektieren den Datenverkehr, der den Tunnel vom Client zu den zulässigen Netzwerken durchläuft.



Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Cisco Adaptive Security Appliances ASA der Serie ASA 5500 als Remote-VPN-Server mit ASDM - Konfigurationsbeispiel
- Konfigurationsbeispiele für Sicherheitsgeräte der Cisco PIX 500-Serie und technische Hinweise
- Konfigurationsbeispiele für Cisco Adaptive Security Appliances der Serie ASA 5500 und technische Hinweise
- Konfigurationsbeispiele für Cisco VPN-Clients und technische Hinweise
- Technischer Support und Dokumentation - Cisco Systems