PIX/ASA 7.x ASDM: Ограничение доступа в сеть пользователей VPN удаленного доступа

Содержание

Введение

В данном документе приведен пример конфигурации с использованием Cisco Adaptive Security Device Manager (ASDM) для ограничения доступа пользователей VPN внутрисетевого удаленного доступа к данным, не защищенным устройством защиты PIX или устройством адаптивной защиты (ASA). Можно ограничить удаленный доступ пользователей VPN определенными областями сети при выполнении следующих действий:

1. Создание списков доступа.
2. Связывание списков с групповыми политиками.
3. Связывание групповых политик с туннельными группами.

Чтобы получить дополнительные сведения о сценарии при блокировке концентратором VPN доступа пользователей VPN ознакомьтесь с документом Настройка концентратора Cisco VPN 3000 на блокировку с помощью фильтров и назначение фильтров RADIUS.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- PIX может быть настроен с помощью ASDM.**Примечание:** Дополнительные сведения о том, как разрешить конфигурацию PIX с помощью ASDM, см. в разделе Разрешение

HTTPS-доступа для ASDM.
- Необходимо наличие как минимум одной правильно выполненной конфигурации удаленного доступа VPN.**Примечание:** Если вы не имеете никаких подобных конфигураций, именуете ASA как Удаленный VPN-сервер с помощью Примера конфигурации ASDM для получения информации о том, как настроить одну хорошую конфигурацию VPN для удаленного доступа.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Устройство защиты Cisco Secure PIX 500 Series версии 7.1(1)**Примечание:** PIX 501 и 506E Устройства безопасности не поддерживает версию 7. x.
- Cisco Adaptive Security Device Manager версии 5.1(1)**Примечание:** ASDM только доступен в PIX или ASA 7. x.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

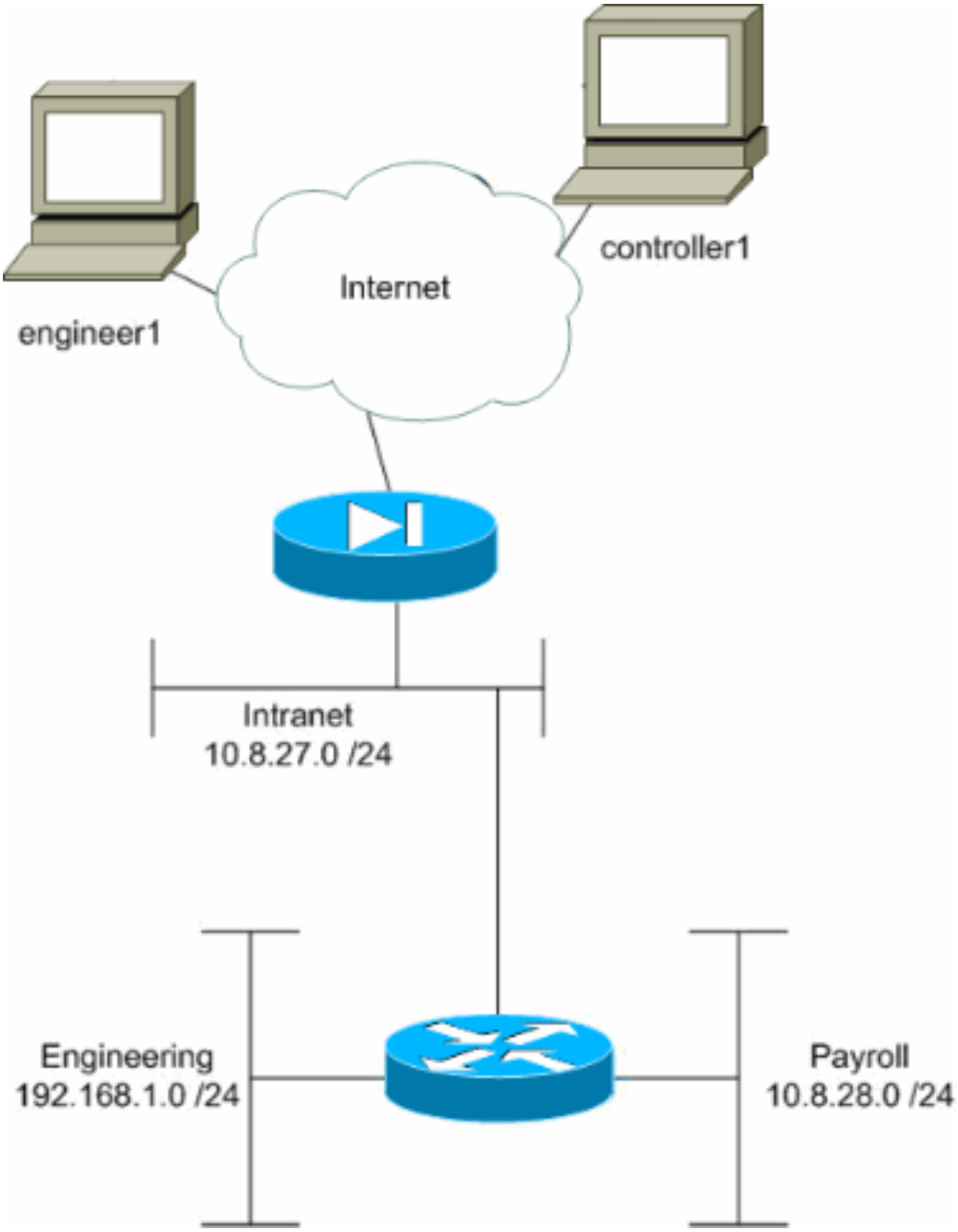
Родственные продукты

Эта конфигурация может также использоваться со следующими версиями программного/аппаратного обеспечения:

- Устройство адаптивной защиты Cisco ASA 5500 Series версии 7.1(1)

Схема сети

В настоящем документе используется следующая схема сети:



Данный пример конфигурации подразумевает наличие небольшой корпоративной сети с тремя подсетями. На схеме представлена топология. Тремя подсетями являются Intranet, Engineering и Payroll. В данном примере конфигурации преследуется цель обеспечить пользователям payroll удаленный доступ к подсетям Intranet и Payroll, а также лишить их доступа в подсеть Engineering. Инженеры должны также иметь возможность удаленного доступа в подсети Intranet и Engineering, но не в подсеть Payroll. В данном примере пользователь с ролью payroll обозначается как "controller1". Пользователь с ролью engineering обозначается как "engineer1".

Условные обозначения

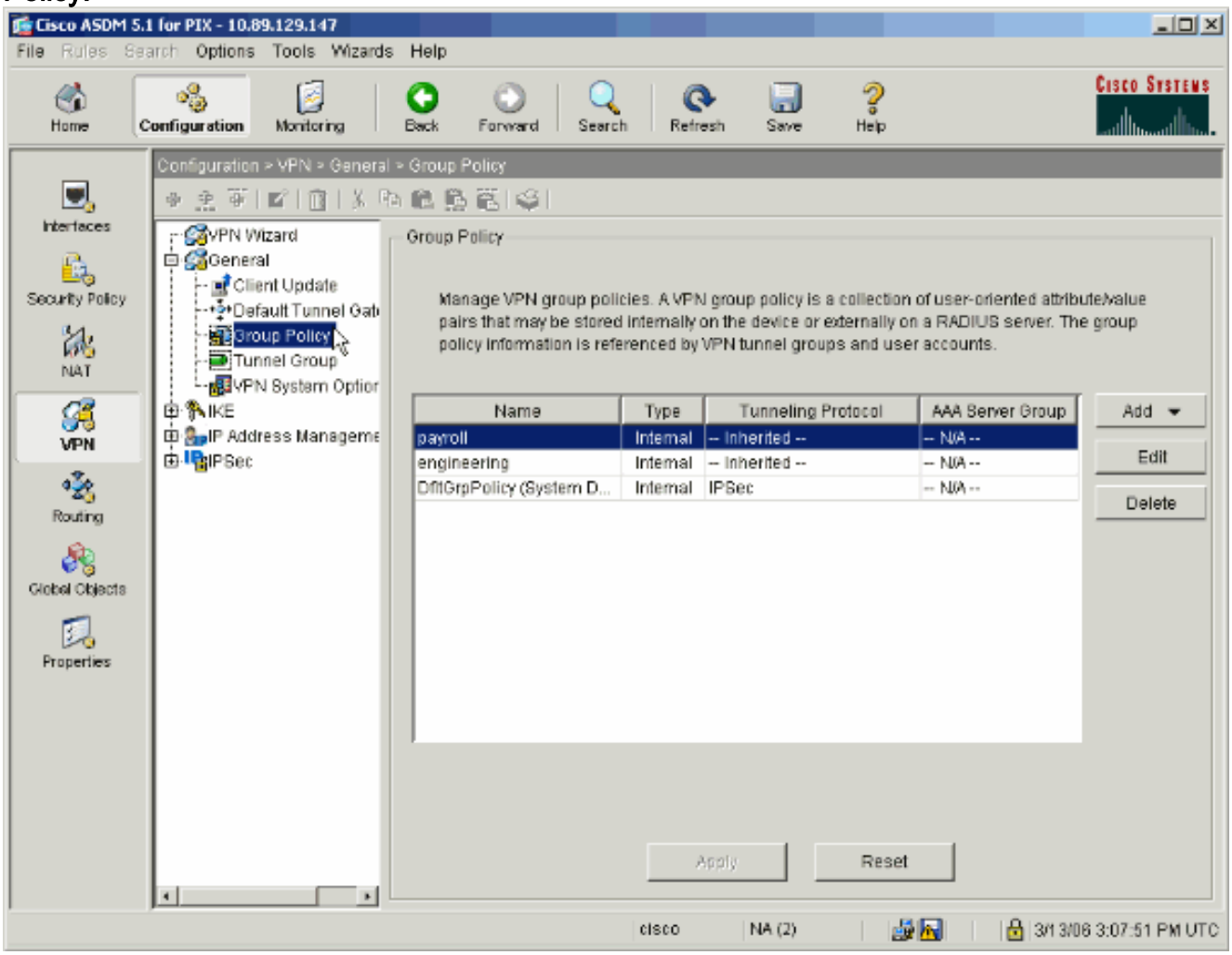
Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка доступа с помощью ASDM

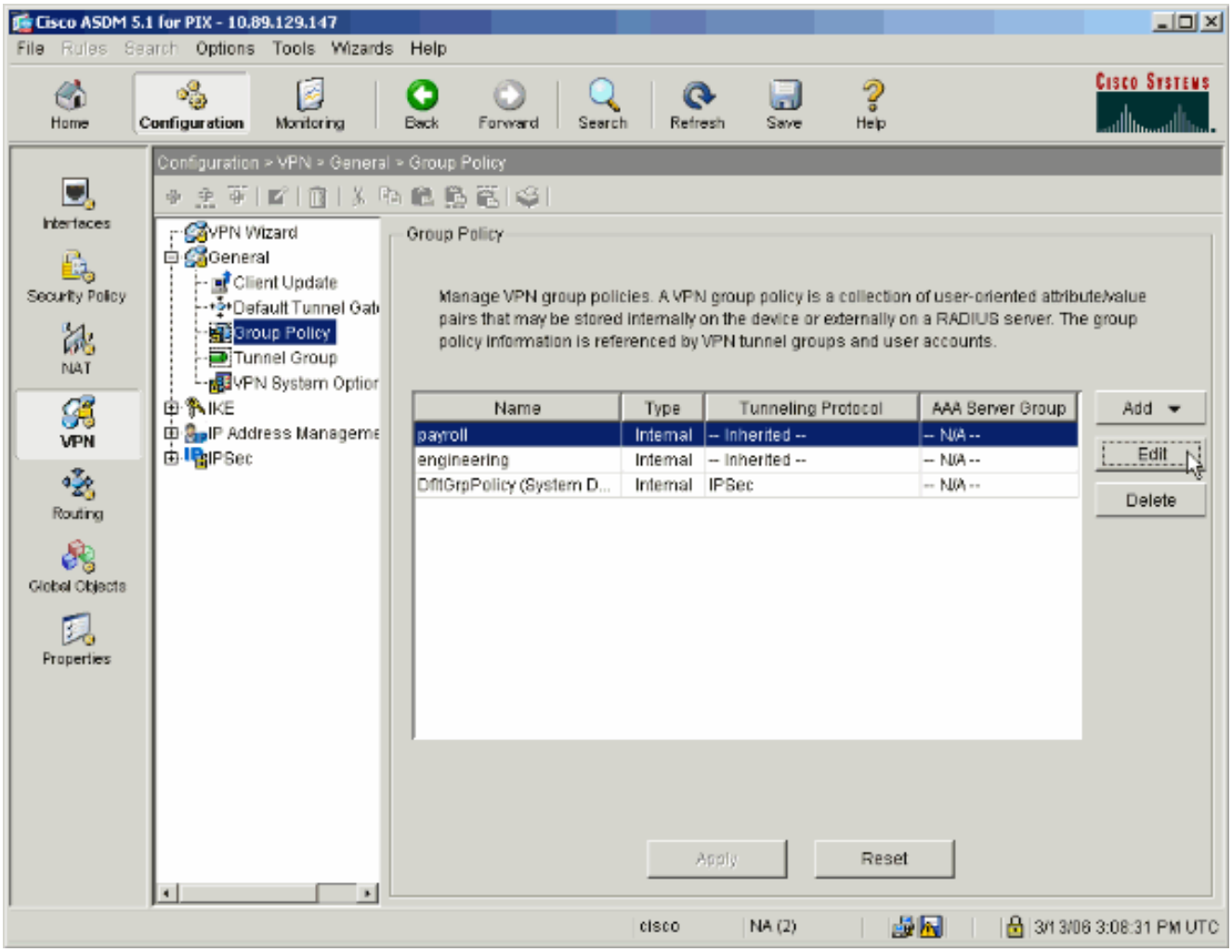
Чтобы настроить устройство защиты PIX с помощью ASDM, выполните следующие

действия:

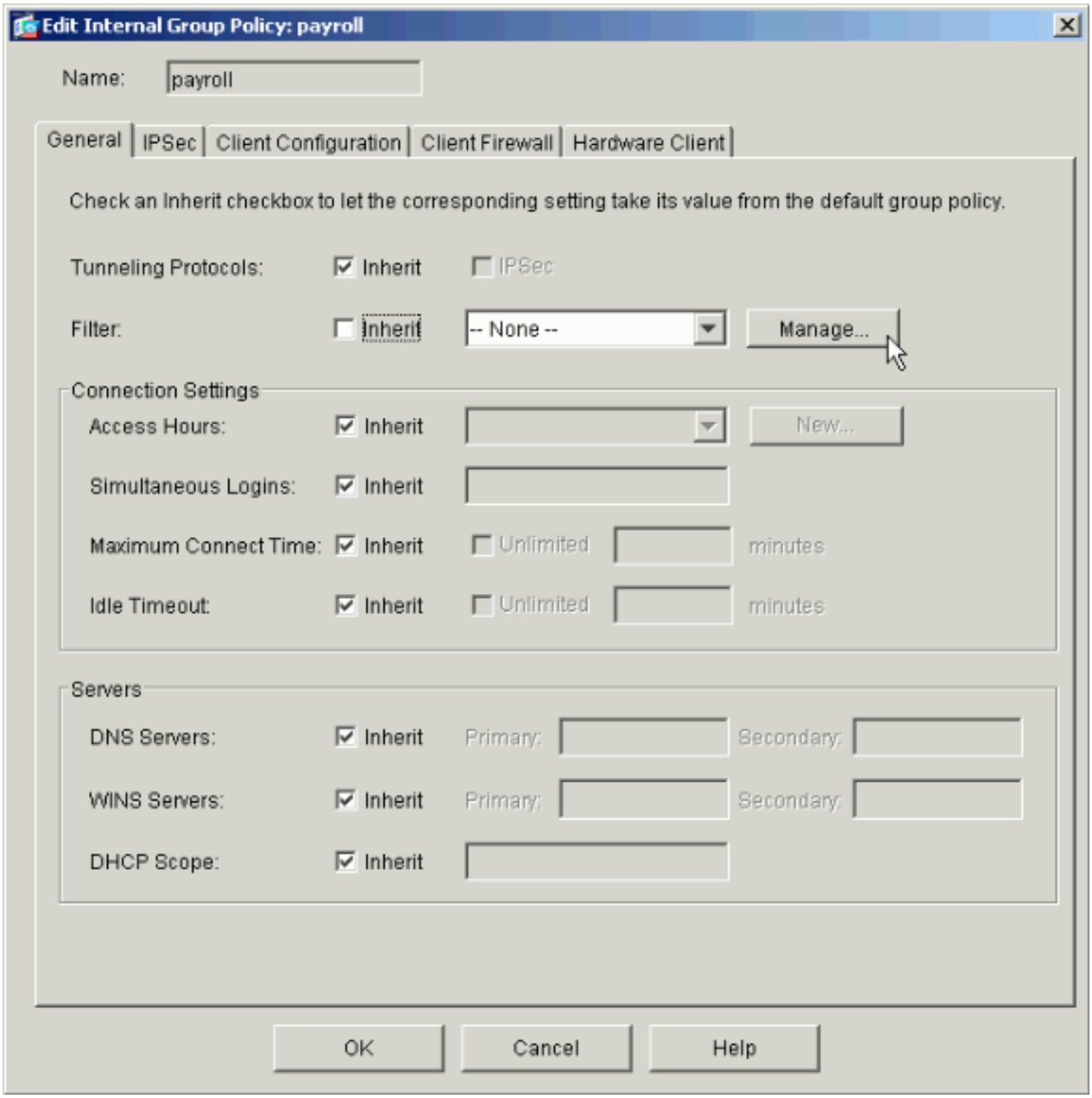
1. **Выберите Configuration > VPN > General > Group Policy.**



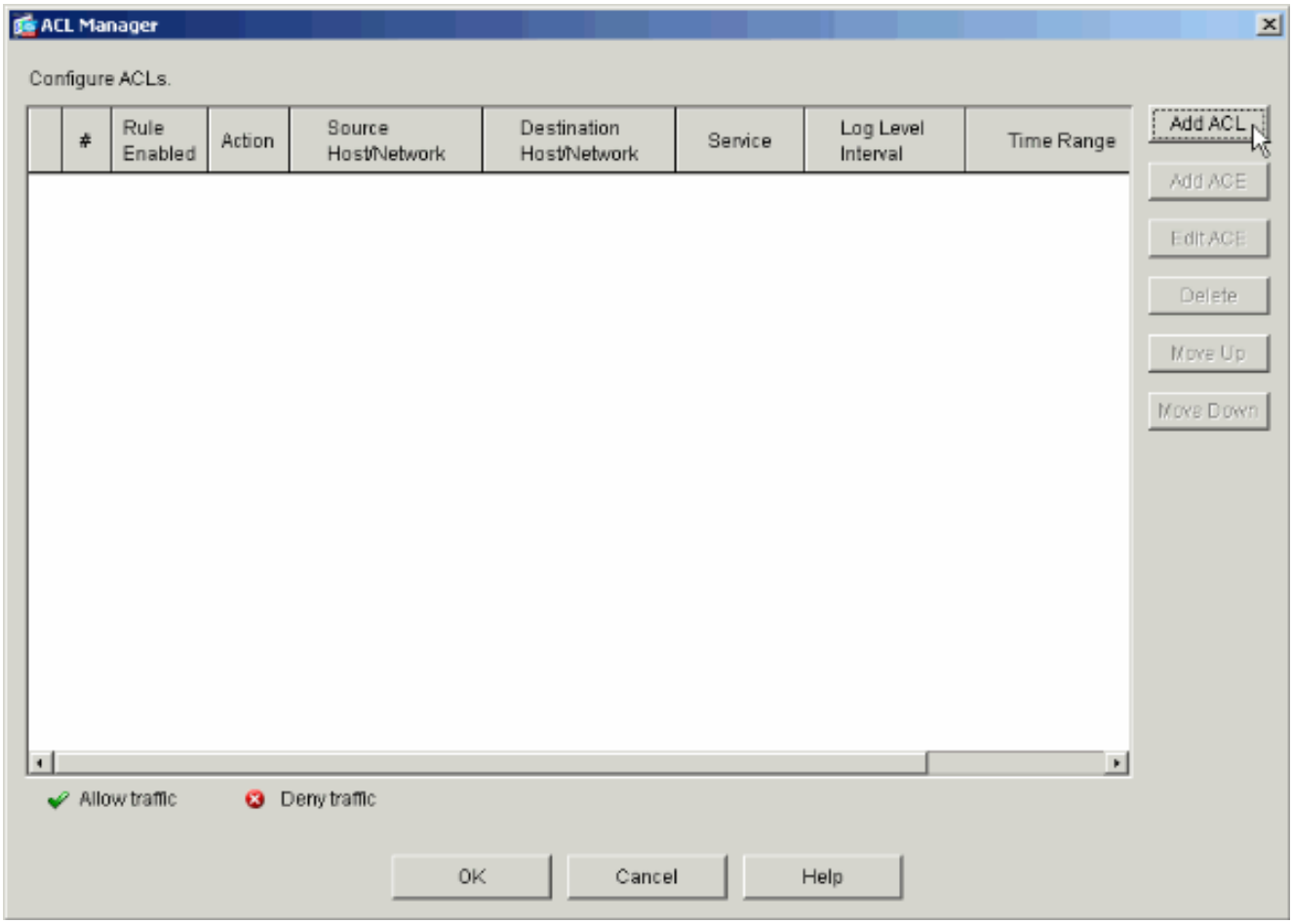
2. В зависимости от действий, выполненных для настройки туннельных групп на PIX, групповые политики могут уже существовать для туннельных групп, доступ пользователей которых необходимо ограничить. **Если подходящая групповая политика уже существует, выберите ее и нажмите Edit. В противном случае нажмите Add и выберите Internal Group Policy....**



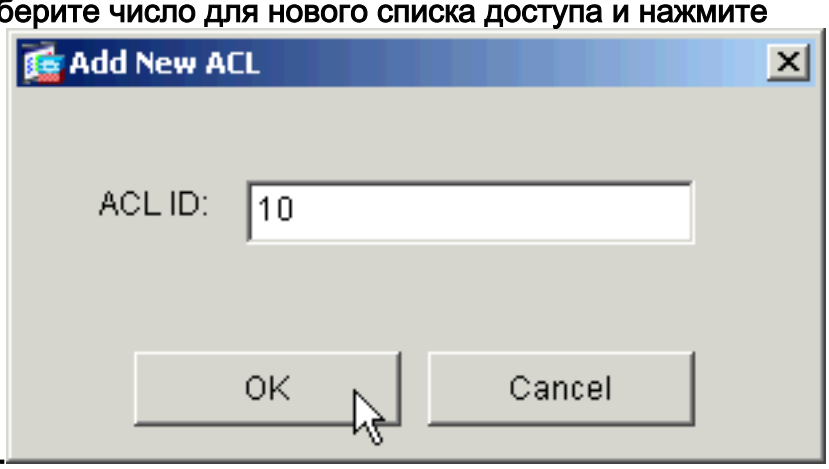
3. При необходимости введите или измените имя групповой политики в верхней части раскрывающегося окна.
4. **На вкладке Общее снимите флажок Inherit рядом с фильтром, затем нажмите Manage.**



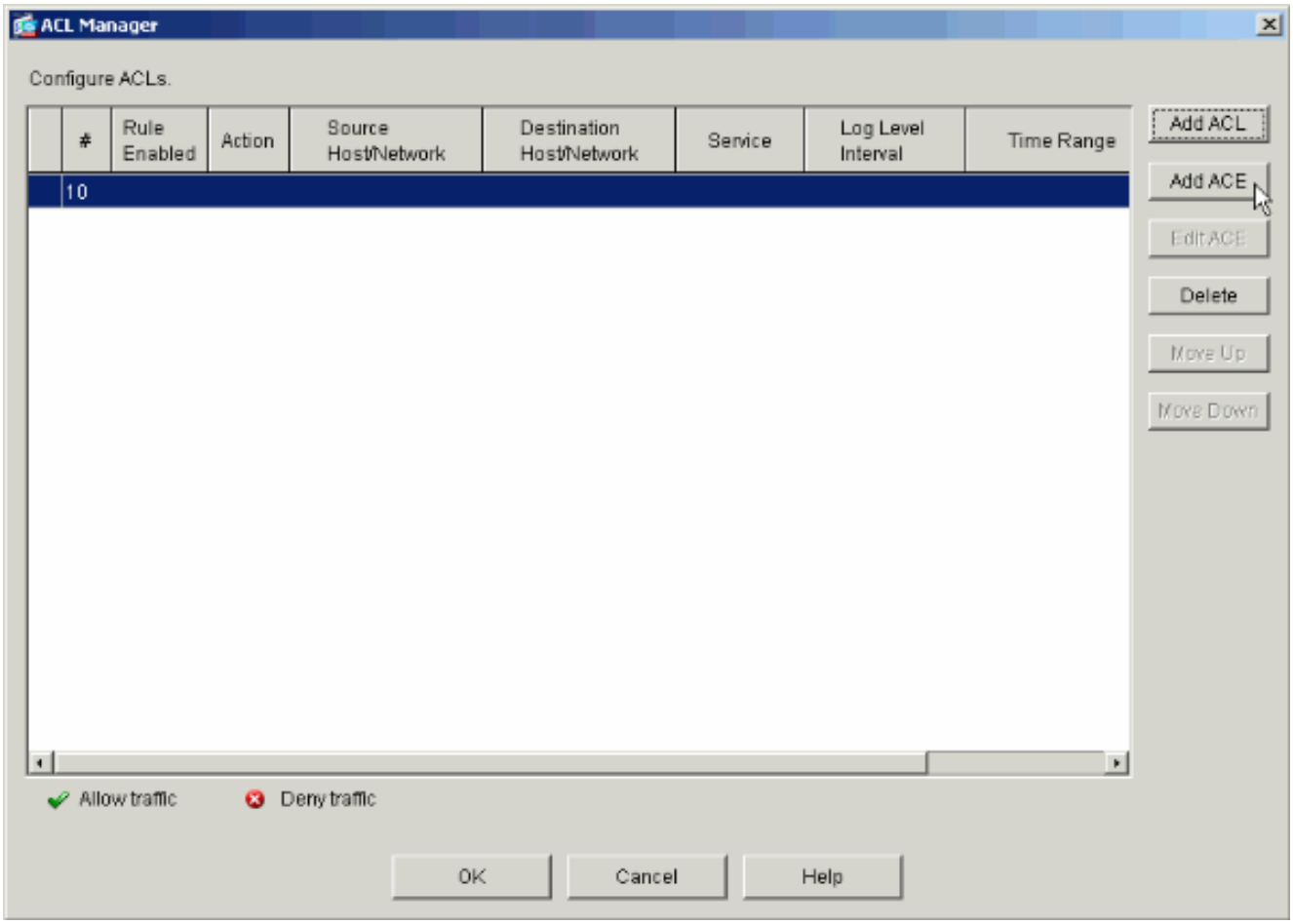
5. Нажмите Add ACL, чтобы создать новый список доступа в раскрывающемся окне диспетчера
ACL.



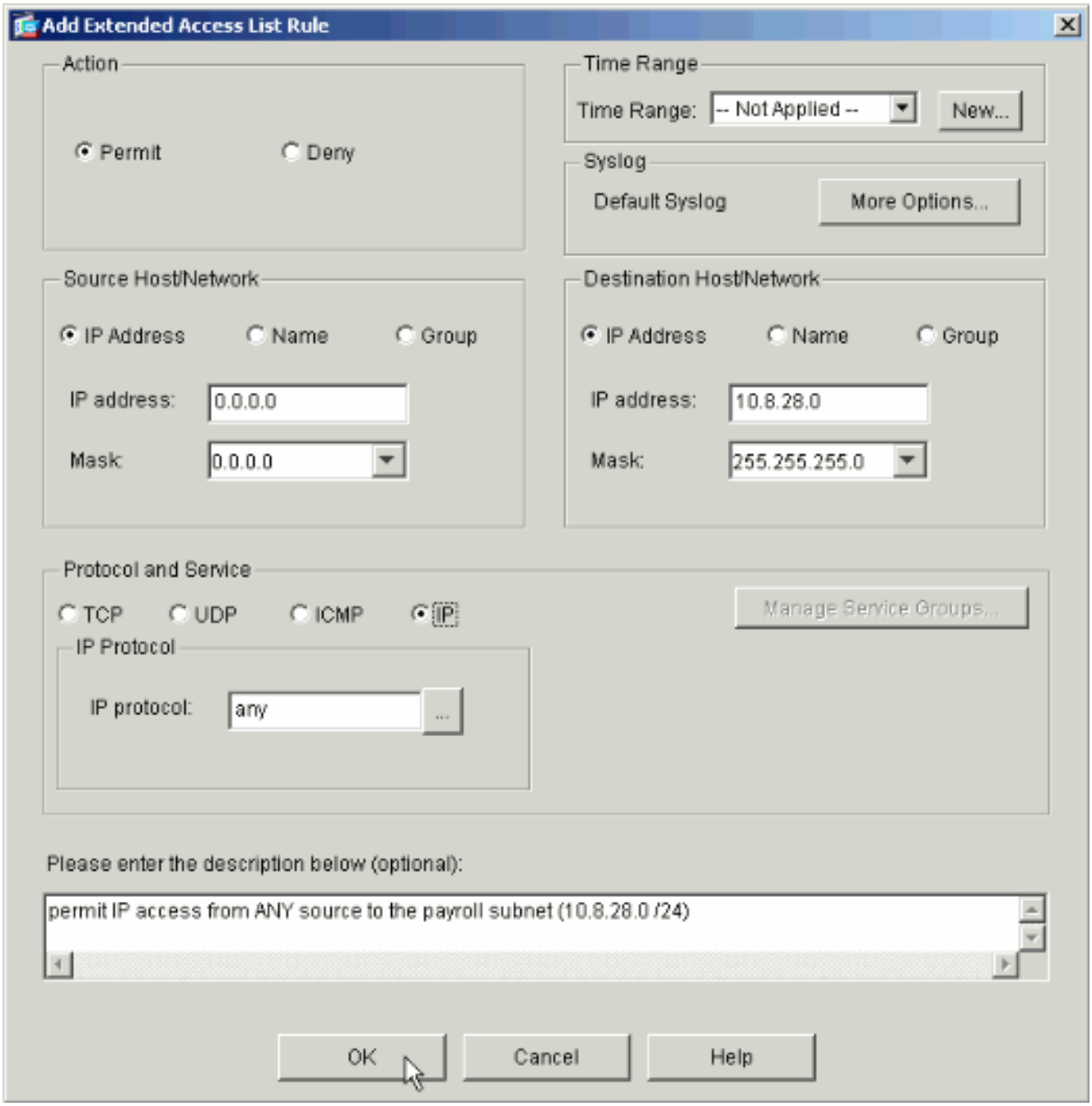
6. Выберите число для нового списка доступа и нажмите OK.



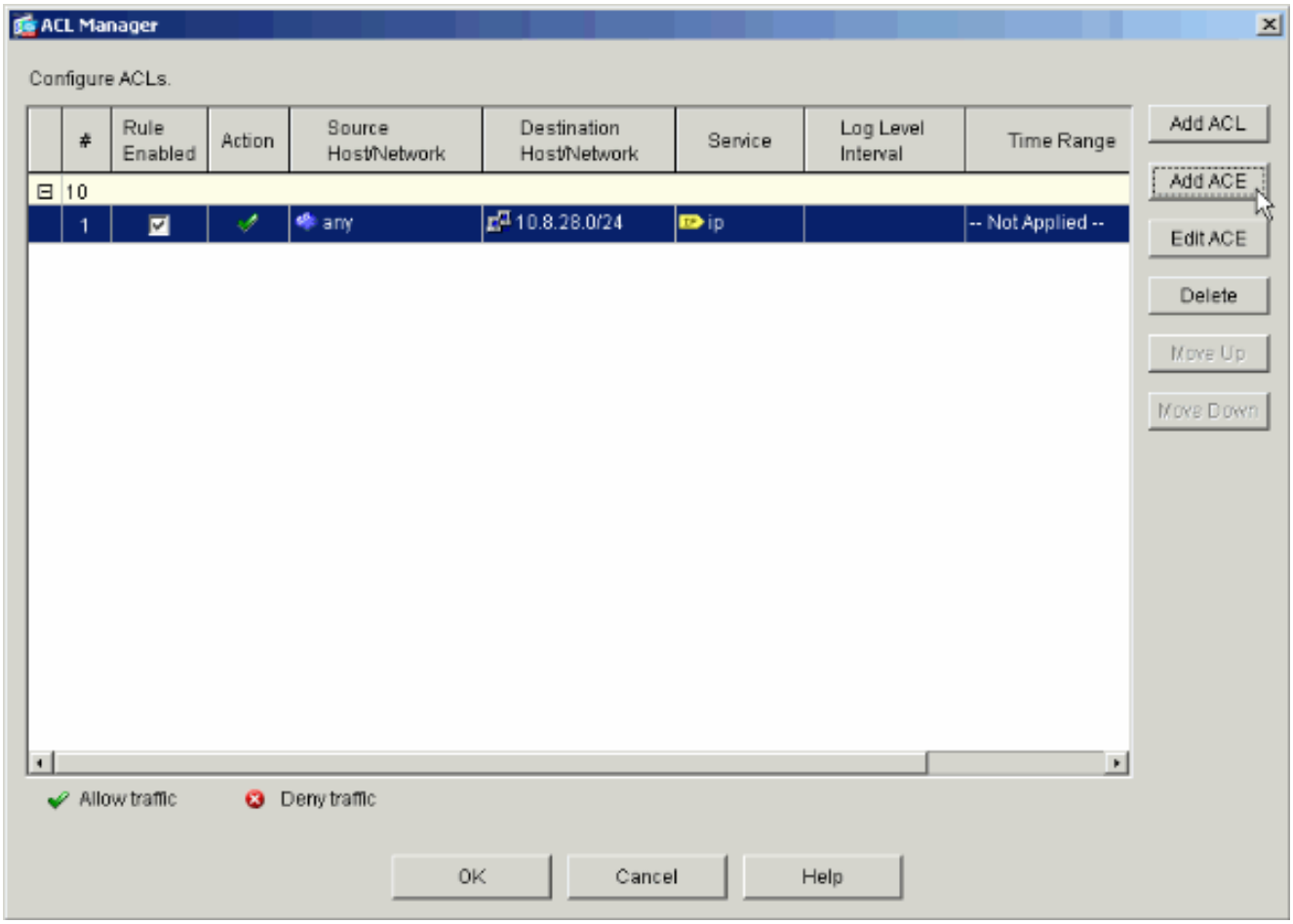
7. Выбрав ACL в левой части панели, нажмите Add ACE, чтобы добавить в список новую запись о контроле
доступа.



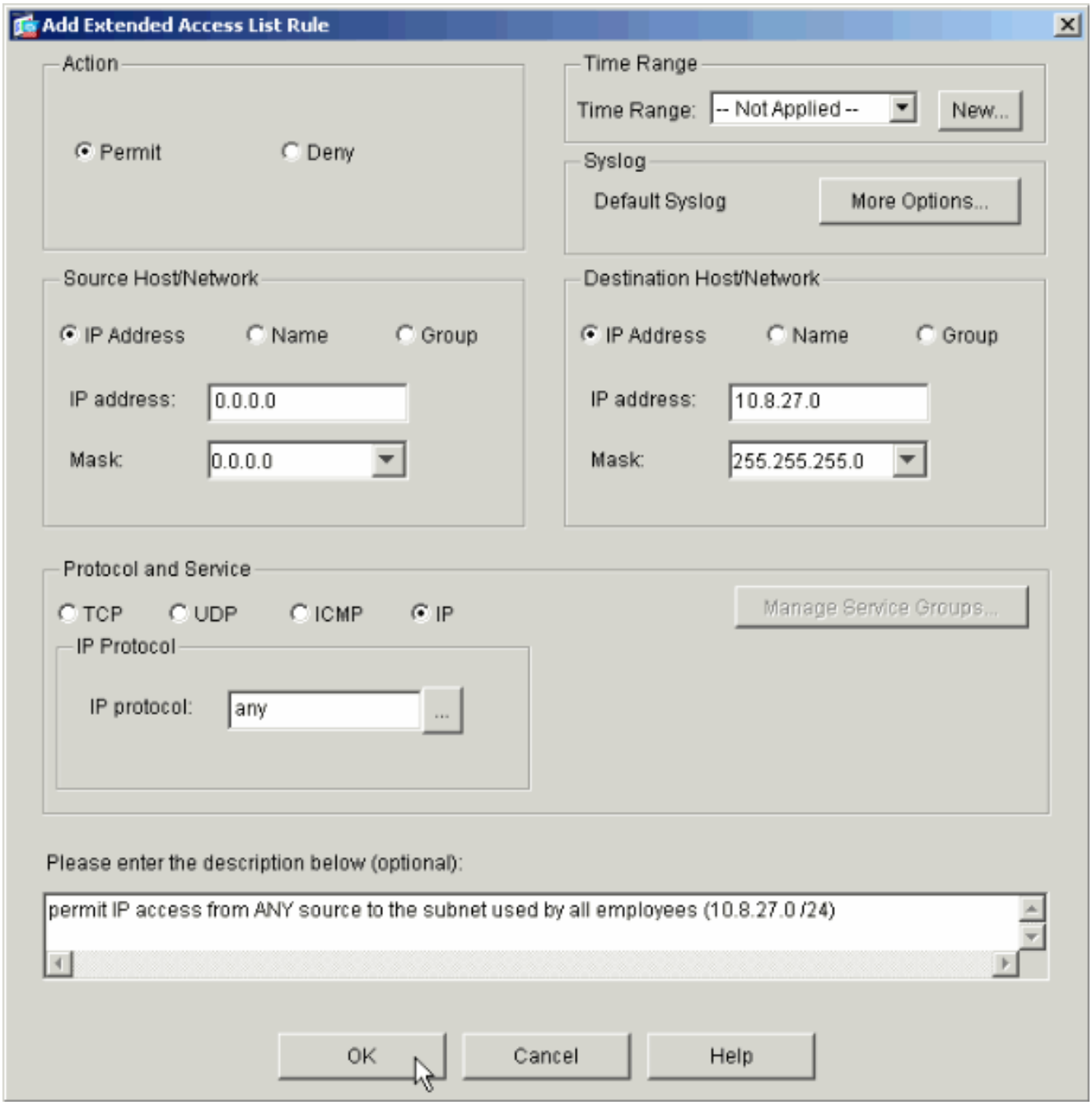
8. Определите запись контроля доступа (ACE), которую необходимо добавить.В данном примере первый ACE в ACL 10 обеспечивает IP-доступ к подсети Payroll из любого источника.**Примечание:** По умолчанию ASDM выбирает только TCP как протокол. Необходимо выбрать IP, если необходимо позволить или запретить пользователям полноценный IP-доступ. **Закончив все действия, нажмите кнопку OK.**



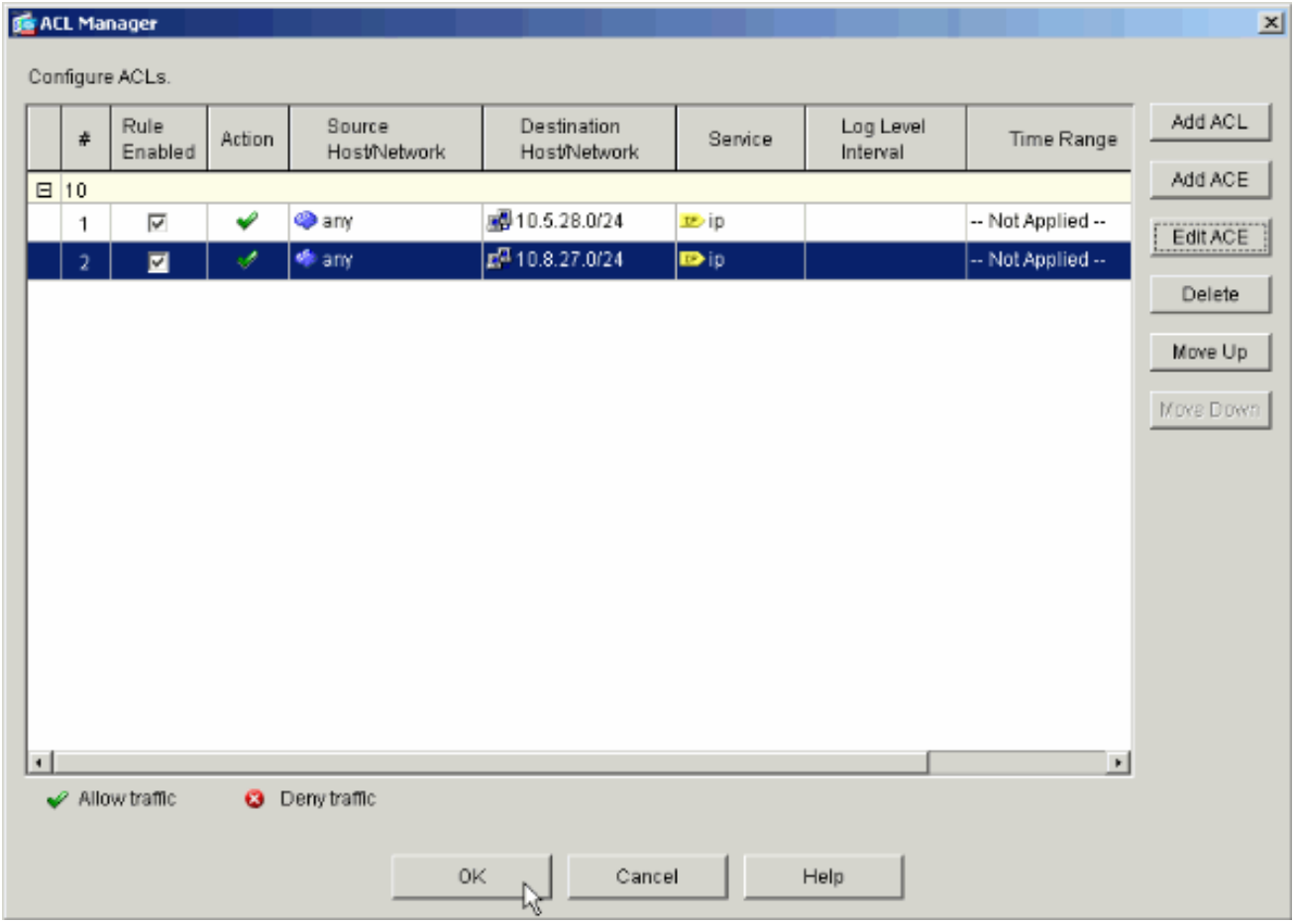
9. Только что добавленный ACE теперь отображается в списке. **Выберите Add ACE повторно, чтобы добавить строки в список доступа.**



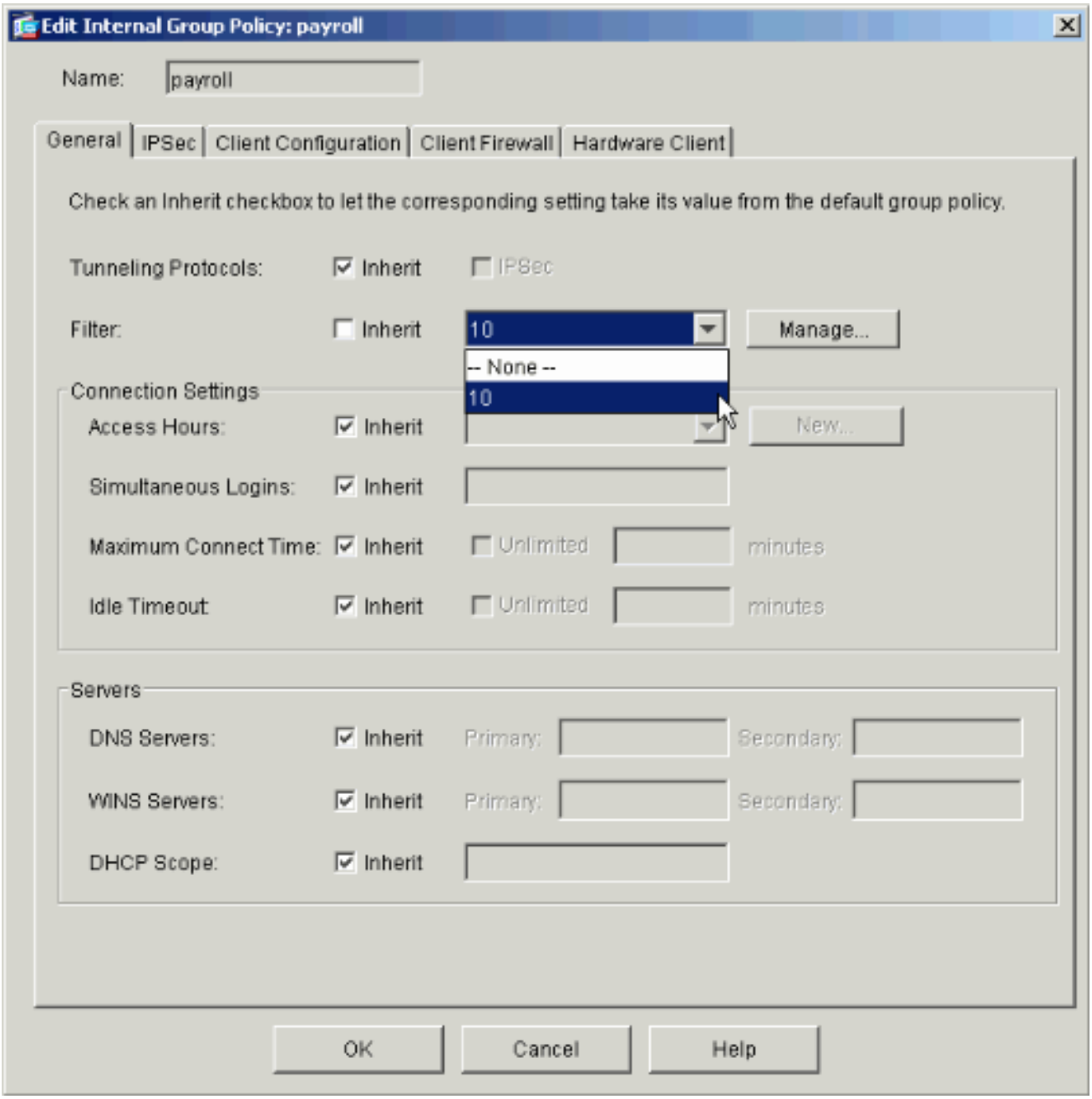
В этом примере происходит добавление второго ACE в ACL 10 с целью разрешить доступ к подсети
Intranet.



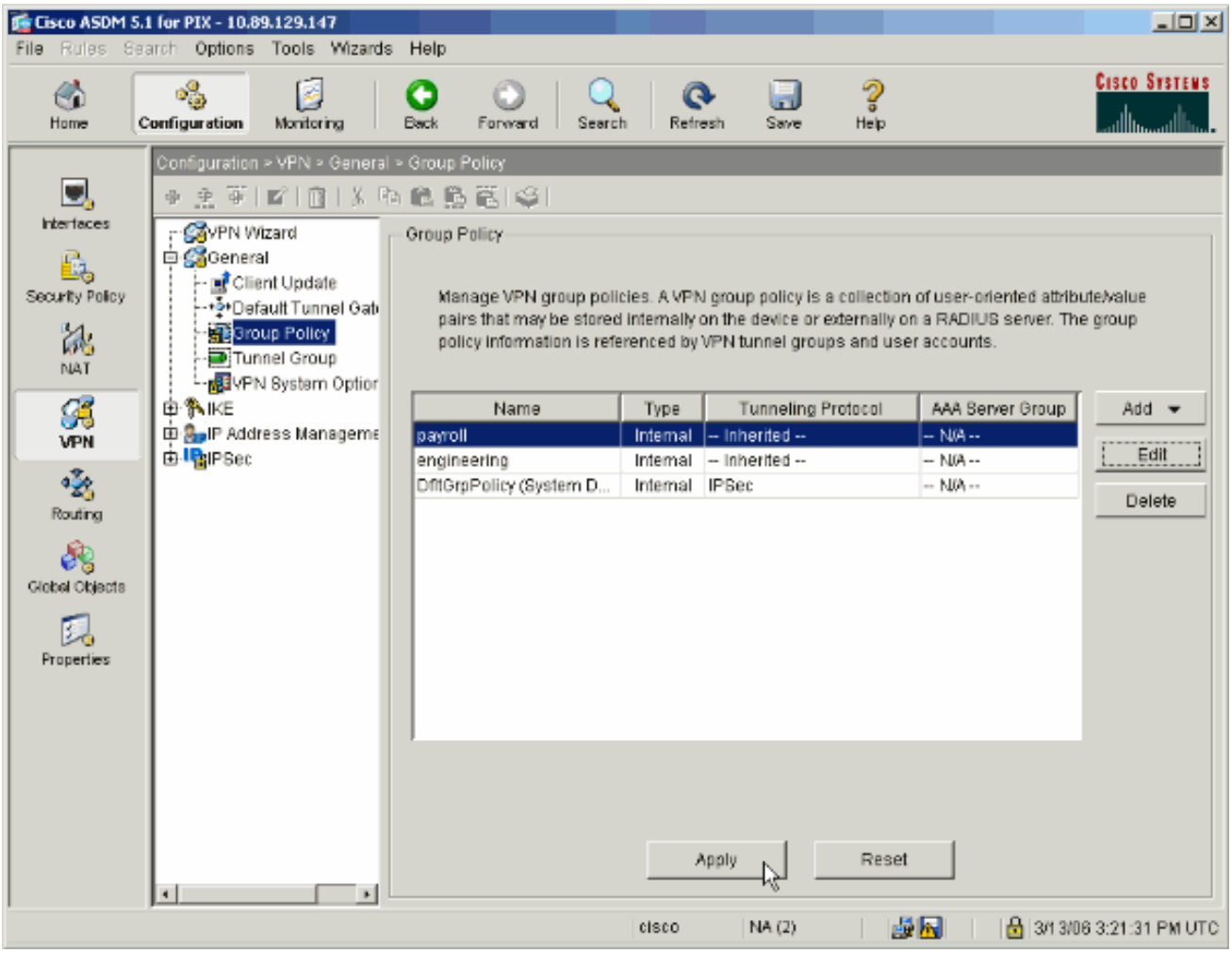
10. После добавления ACE нажмите кнопку OK.



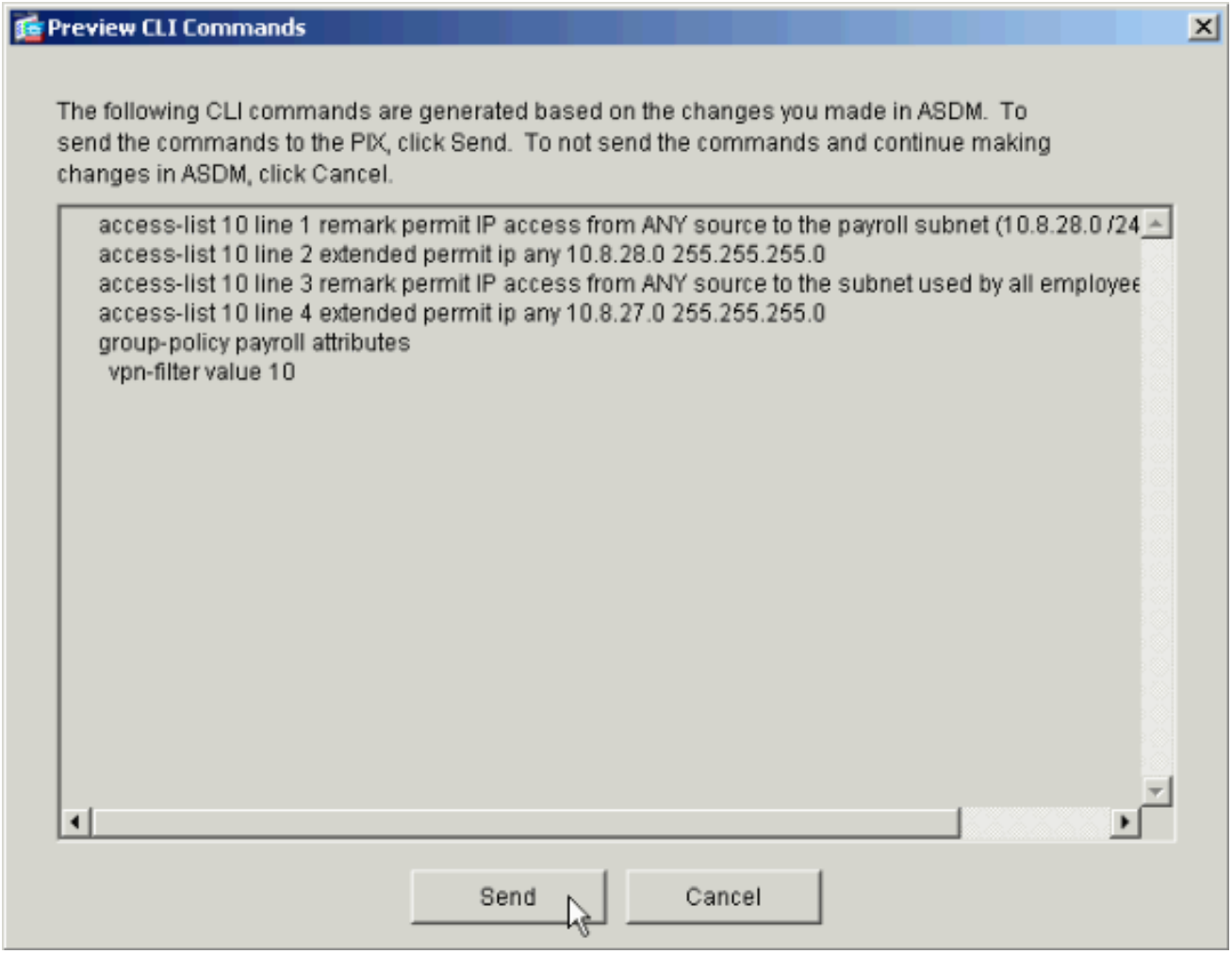
11. Выберите ACL, который был определен и заполнен во время выполнения последних действий, в качестве фильтра для групповой политики. **Закончив все действия, нажмите кнопку OK.**



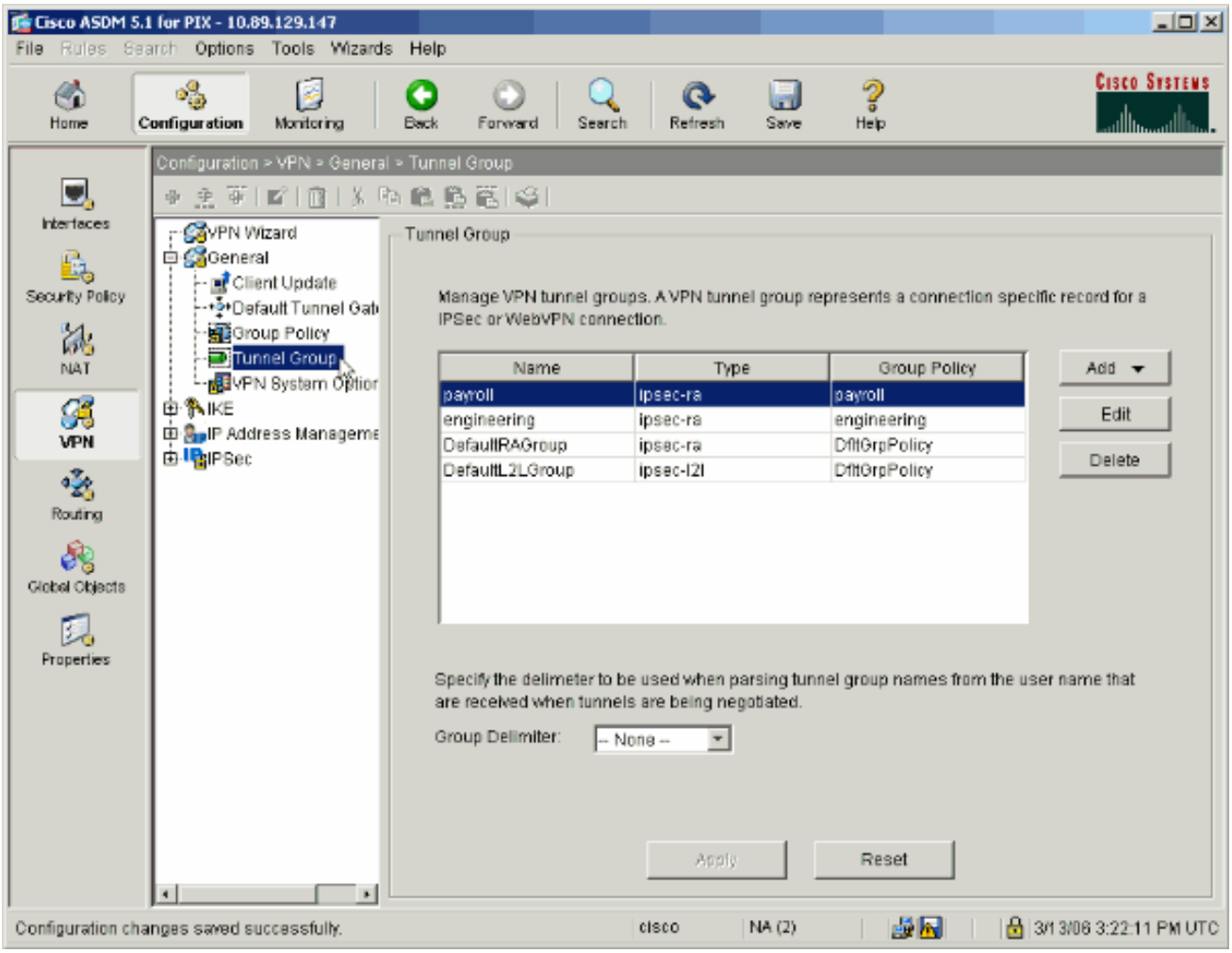
12. **Чтобы отправить изменения в PIX, нажмите кнопку Apply.**



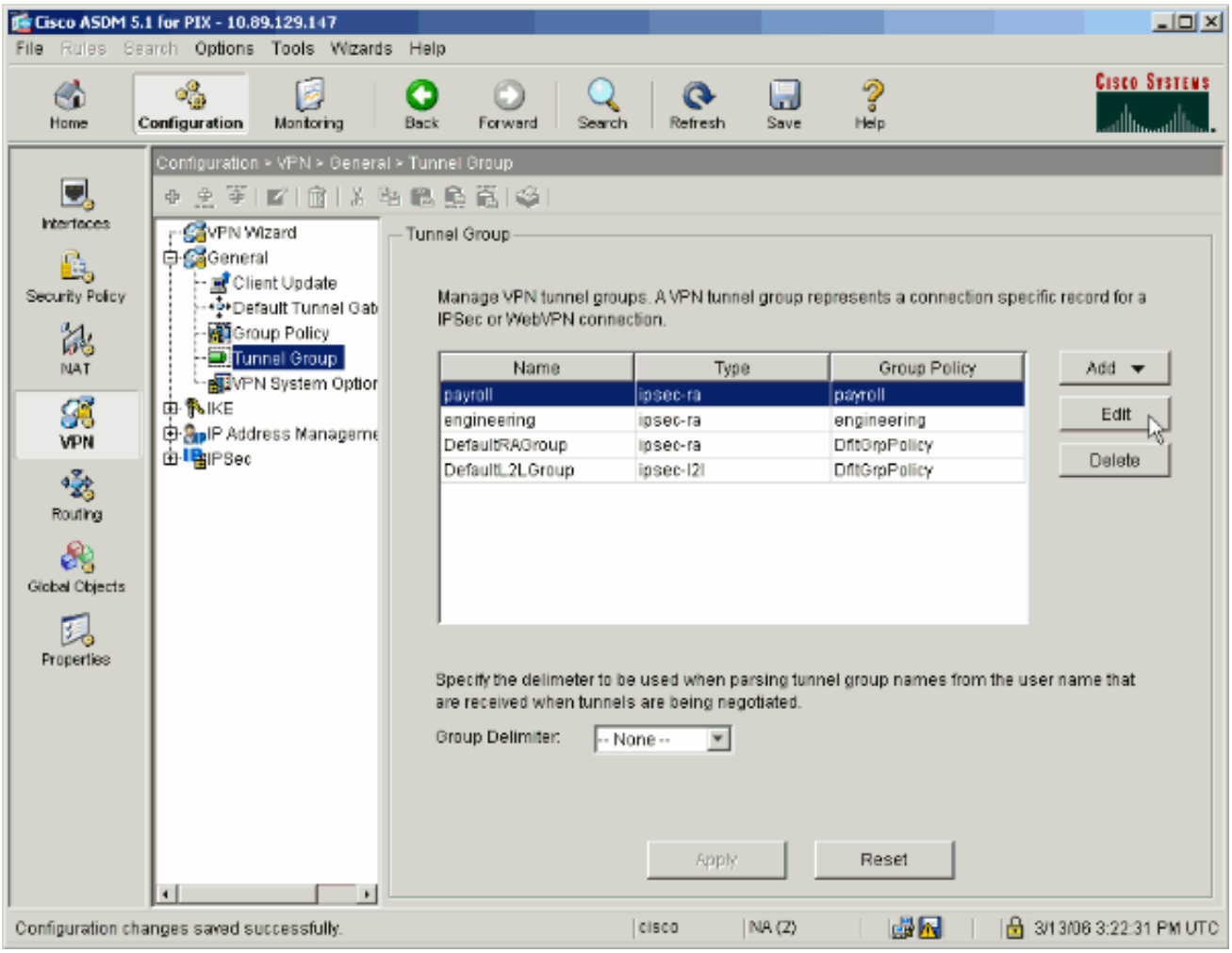
13. Если были выбраны соответствующие настройки в разделе Options > Preferences, ASDM предварительно просматривает команды перед их отправкой в PIX. Нажмите Send.



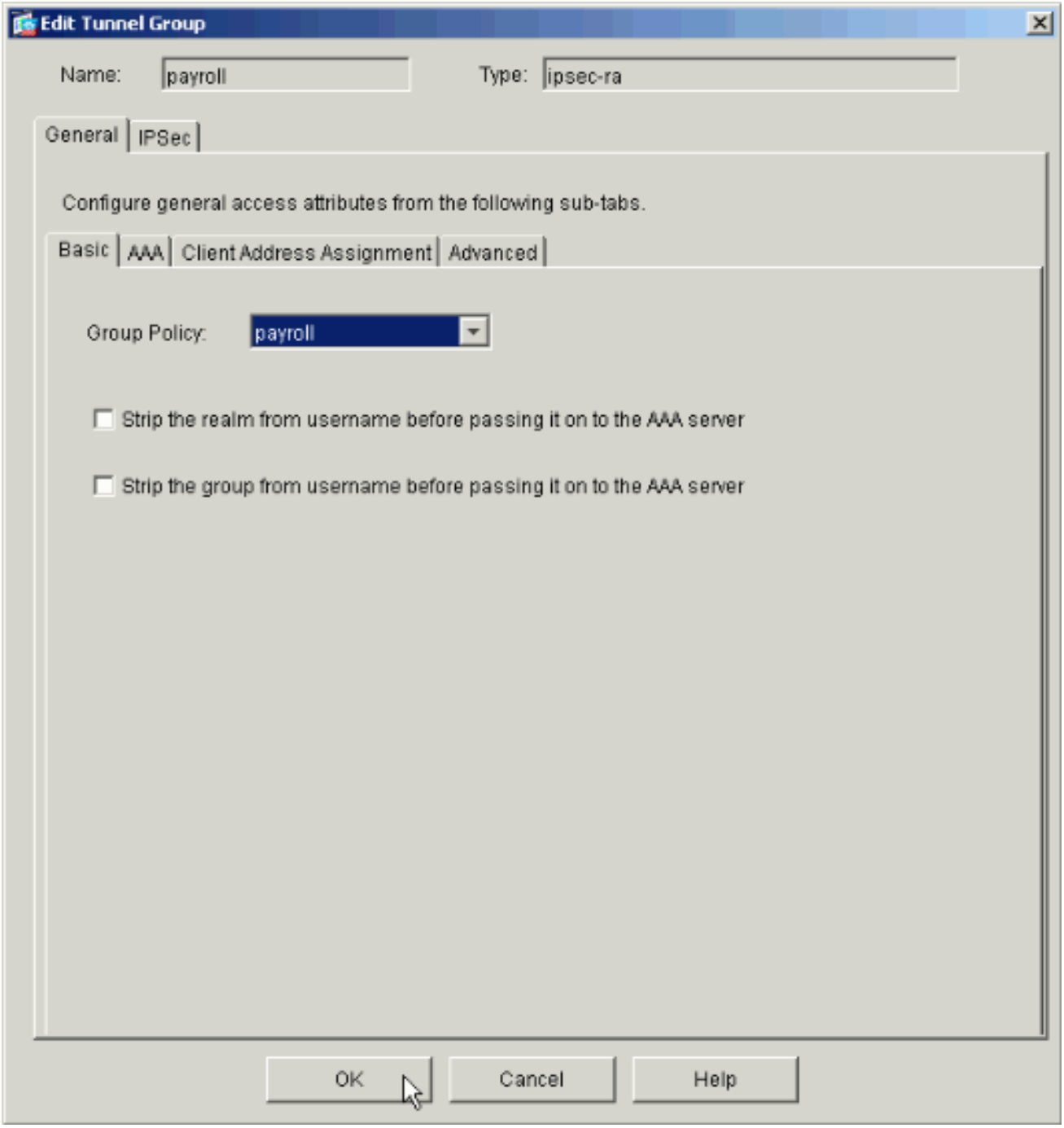
14. Примените только что созданную или измененную групповую политику к правильно выбранной туннельной группе. **Нажмите Tunnel Group в левом поле.**



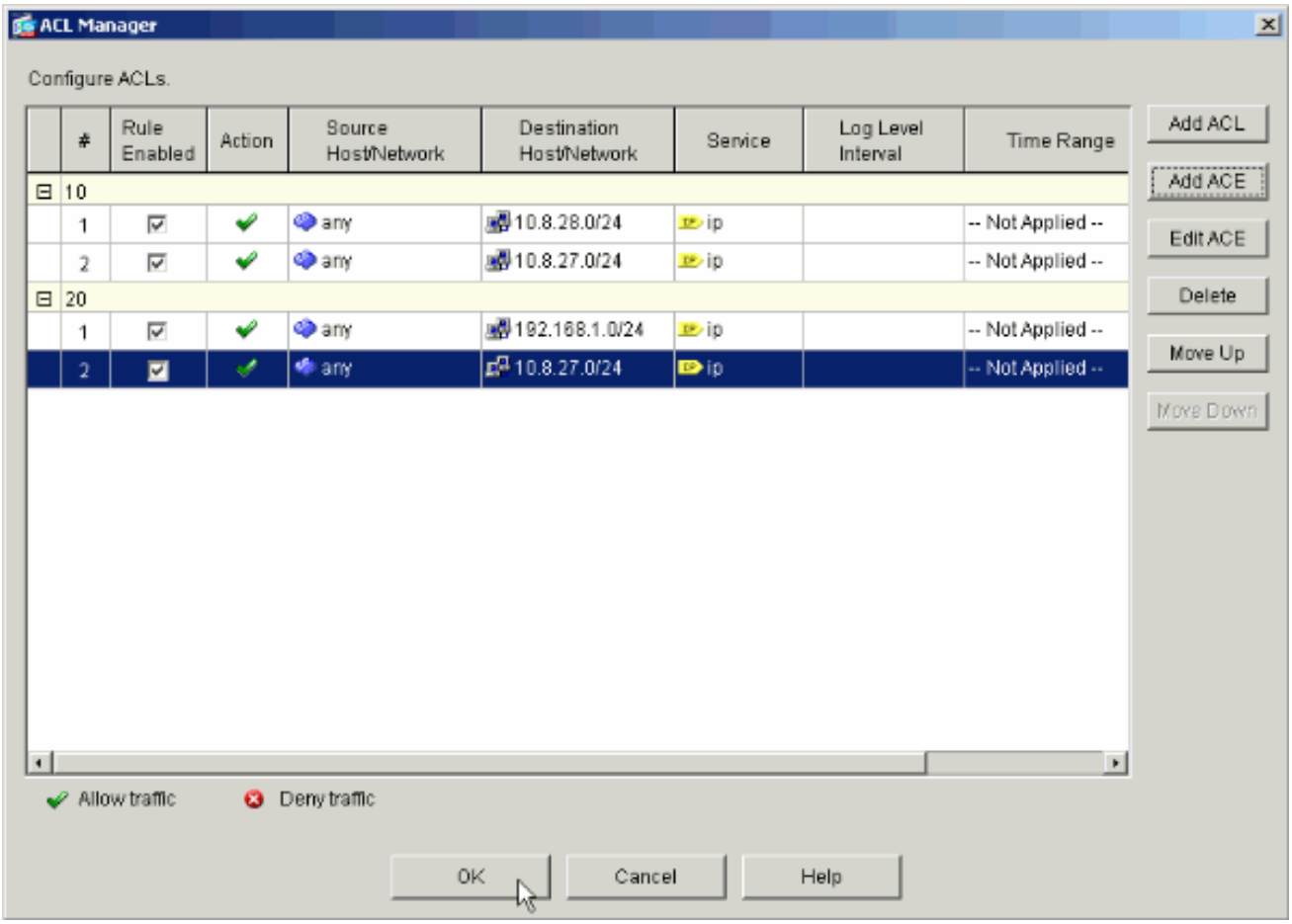
15. **Выберите туннельную группу, к которой необходимо применить групповую политику, и нажмите**
Edit.



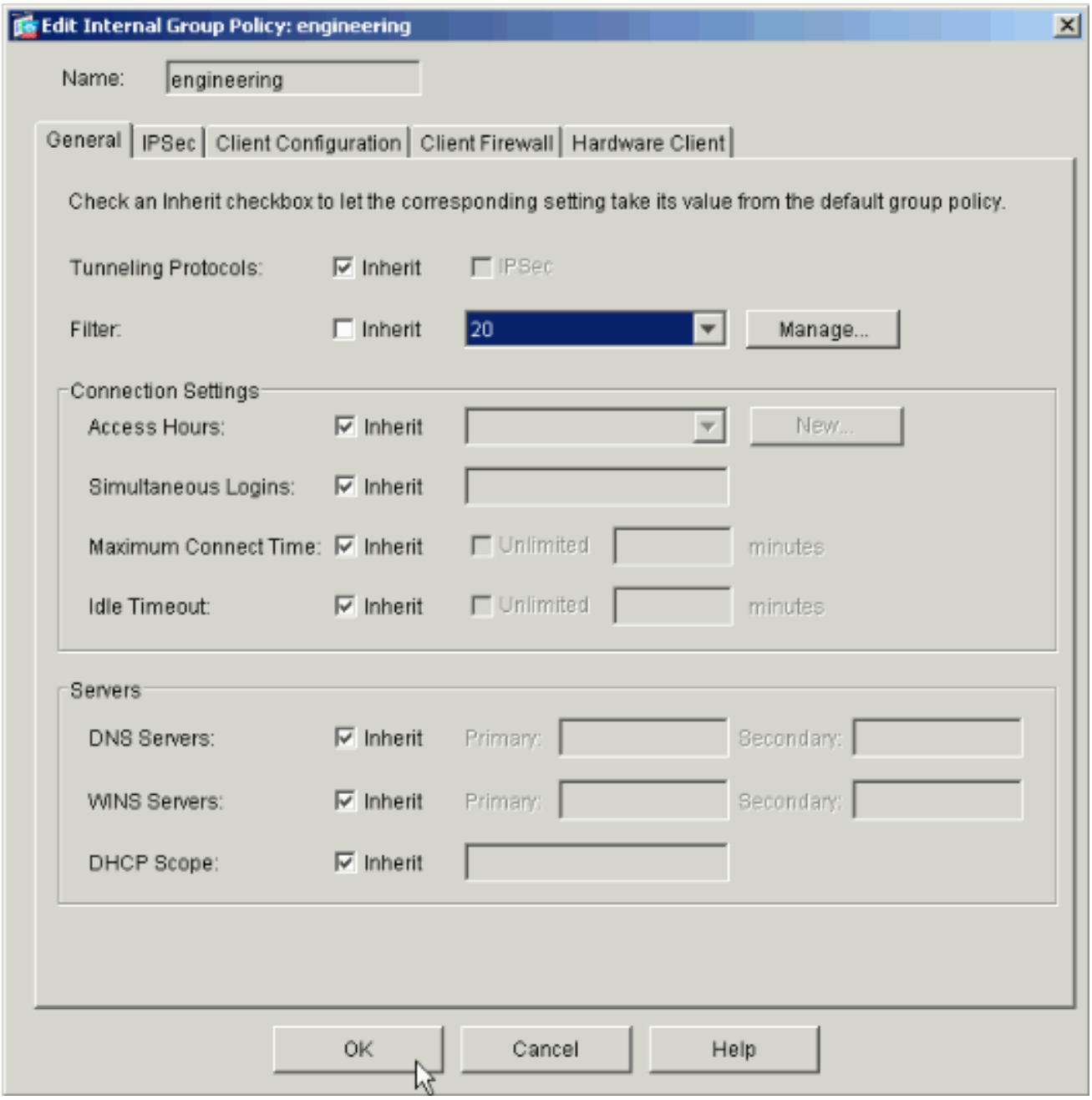
16. Если групповая политика была создана автоматически (см. действие 2), убедитесь, что только что настроенная групповая политика выбрана в раскрывающемся окне. Если групповая политика не была настроена автоматически, выберите ее в раскрывающемся окне. **Закончив все действия, нажмите кнопку OK.**



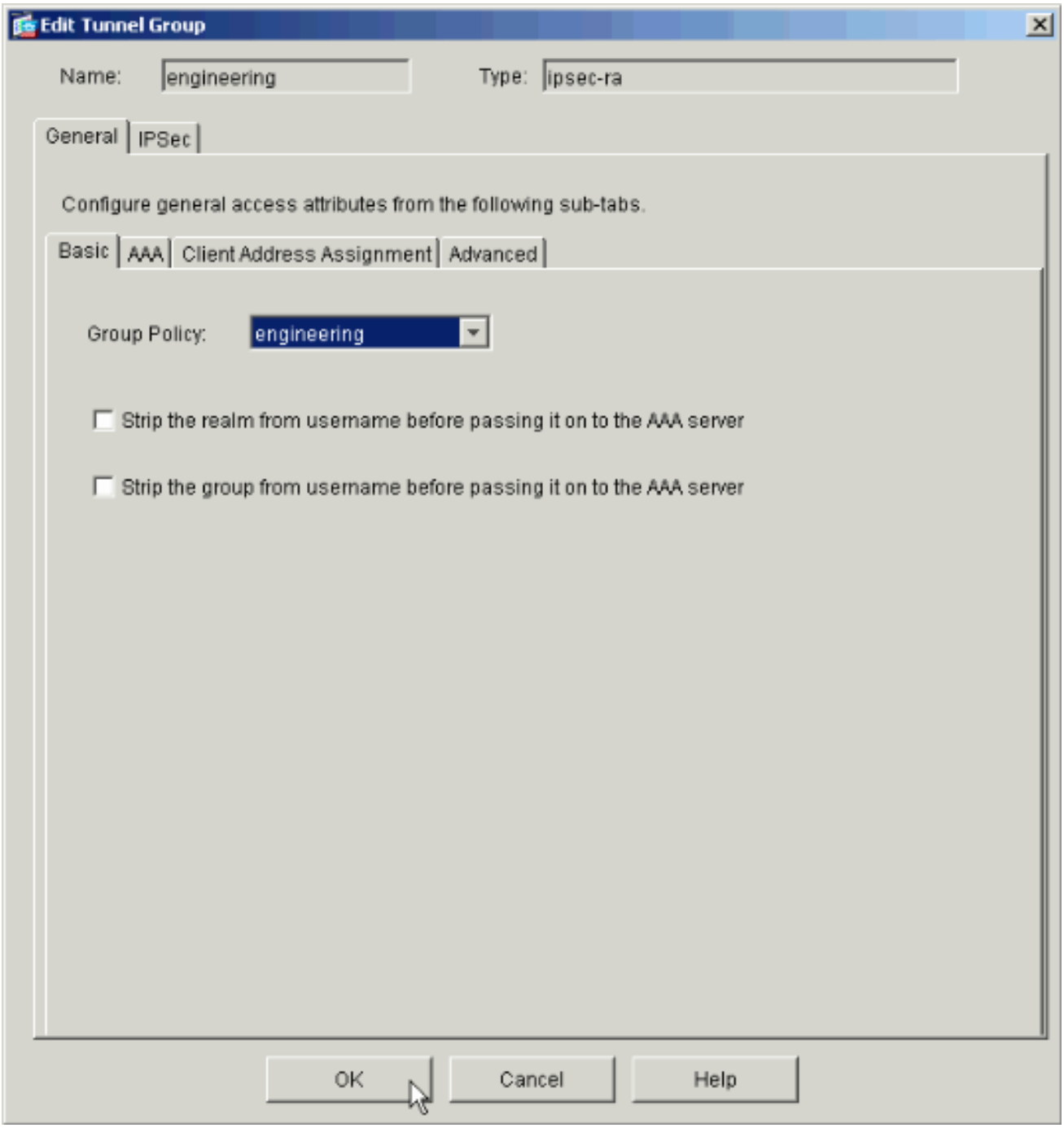
17. **Нажмите Apply, если появляется запрос, нажмите Send, чтобы добавить изменение в конфигурацию PIX.**Если групповая политика уже выбрана, отобразится сообщение "No changes were made" (изменения не внесены). **Нажмите кнопку OK.**
18. Повторите действия 2-17 для дополнительных туннельных групп, к которым необходимо добавить ограничения.В данном примере конфигурации также необходимо ограничить доступ разработчиков. Несмотря на то, что для этого необходимо выполнить тот же ряд действий, есть несколько окон, в которых присутствуют отличия:Новый список доступа



Выберите Access List 20 в качестве фильтра в политике группы Engineering.



Убедитесь, что политика группы Engineering задана для туннельной группы Engineering Tunnel
Group.



Настройка доступа с помощью CLI

Чтобы настроить устройство защиты с помощью CLI, выполните следующие действия:

Примечание: Некоторые команды, показанные в этих выходных данных, переведены в нерабочее состояние к второй линии из-за пространственных причин.

1. Создайте два разных списка контроля доступа (15 и 20), применяемые к пользователям при их подключении к VPN удаленного доступа. Этот список доступа упоминается далее в конфигурации.`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. Создайте два различных пула адресов VPN. Создайте один пул для удаленных пользователей Payroll, и один пул – для удаленных пользователей 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. Создайте политики Payroll, применяемые только при подключении.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. Это действие совпадает с действием 3, за исключением того, что оно предназначено для группы Engineering.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. Создайте локальных пользователей и назначьте только что созданные атрибуты данным пользователям, чтобы ограничить их доступ к ресурсам.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. Создайте туннельные группы, содержащие политики подключения для пользователей Payroll.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. Создайте туннельные группы, содержащие политики подключения для пользователей Engineering.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**

После ввода настроенных данных в конфигурации отобразится следующая выделенная область:

Имя устройства 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

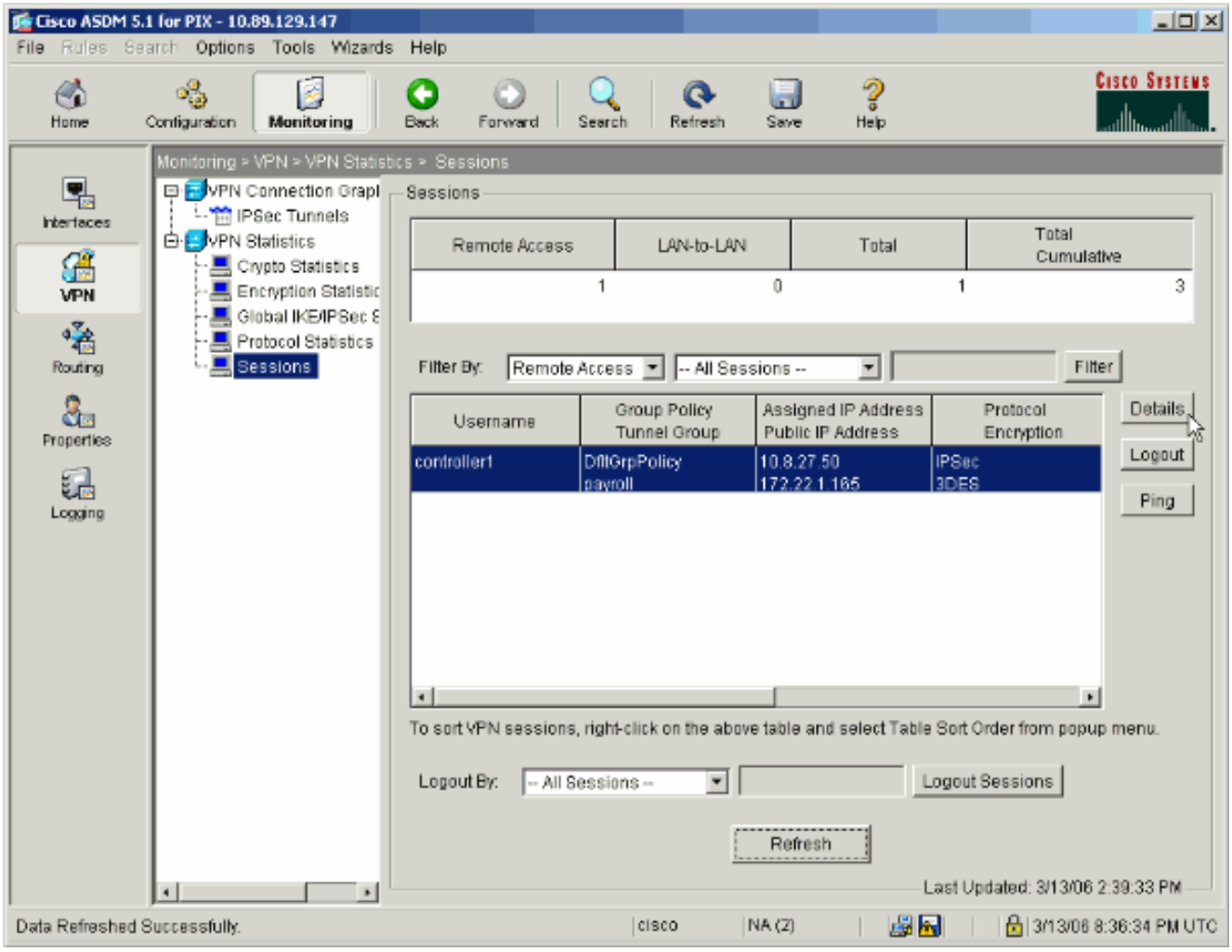
255.255.255.0 access-list Inside_nat0_outbound extended permit ip any 172.16.2.0 255.255.255.0 **access-list 15 remark permit IP access from ANY source to the Payroll subnet (10.8.28.0/24) access-list 15 extended permit ip any 10.8.28.0 255.255.255.0 access-list 15 remark Permit IP access from ANY source 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)#
```

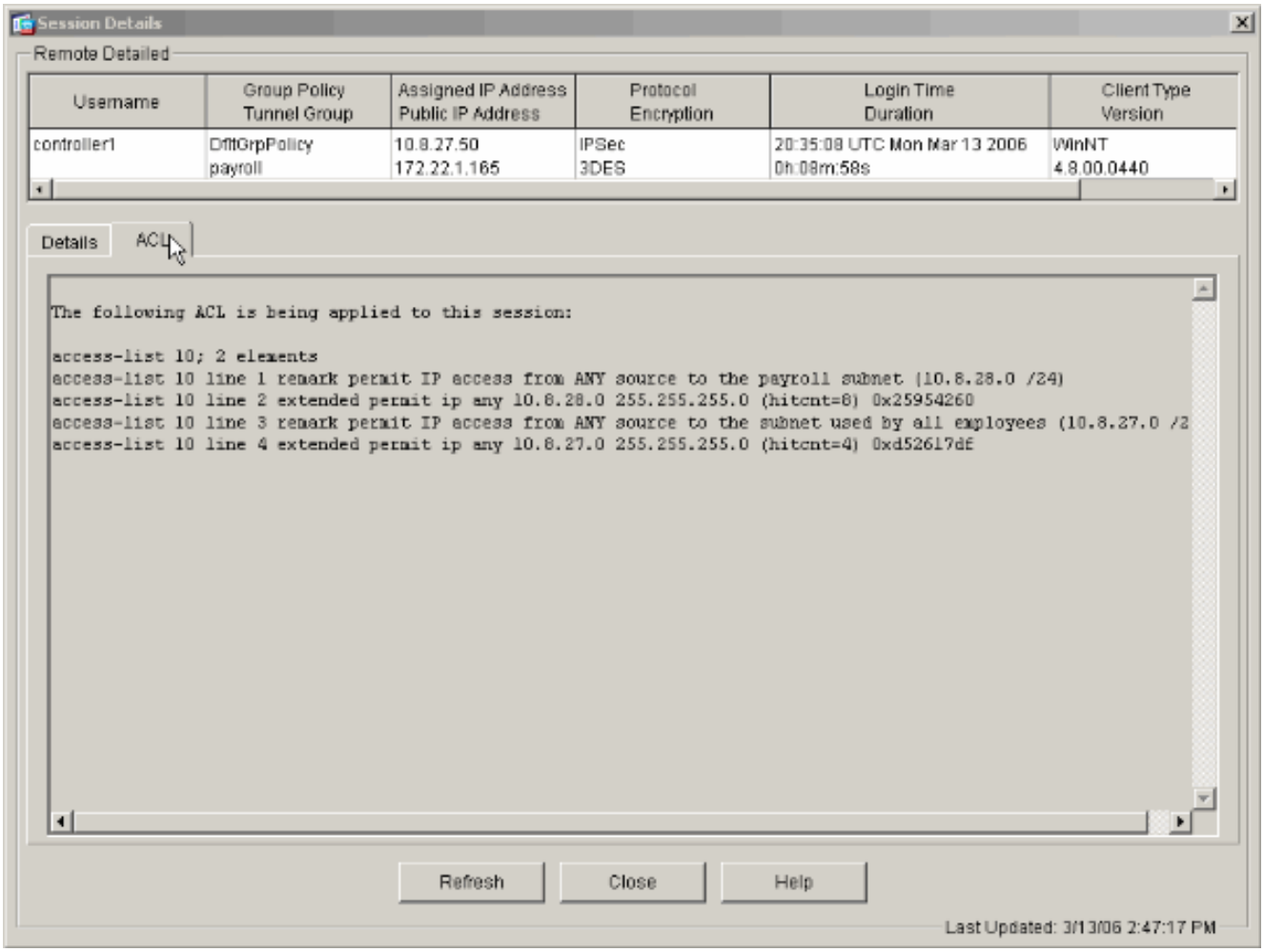
Проверка

Чтобы проверить конфигурацию, используйте функции мониторинга ASDM:

1. **Выберите Monitoring > VPN > VPN Statistics > Sessions.**В PIX отображаются активные сеансы VPN. **Выберите необходимые сеансы и нажмите Details.**



2. Выберите вкладку ACL.`ACL hitcnts` ,
.



Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Устройства адаптивной защиты Cisco ASA серии 5500 в качестве сервера удаленного VPN Server с использованием примера конфигурации ASDM
- Технические примечания и примеры конфигурации устройств защиты Cisco PIX серии 500
- Технические примечания и примеры конфигурации устройств адаптивной защиты Cisco ASA серии 5500
- Технические примечания и примеры конфигурации Cisco VPN Client
- Cisco Systems – техническая поддержка и документация