PIX/ASA (Версия 7.x и Позже) VPN-туннель IPSec с Примером конфигурации Трансляции сетевых адресов

Содержание

Введение

Этот пример конфигурации демонстрирует туннель IPSec VPN через межсетевой экран, который выполняет преобразование сетевых адресов (NAT). **Эта конфигурация не будет работать с преобразованием адресов портов (PAT), если используются выпуски программного обеспечения Cisco IOS®, предшествующие 12.2(13)T.** Этот вид настройки можно использовать для туннелирования IP-трафика. Его нельзя использовать для шифрования трафика, который не идет через брандмауэр, такой как IPX или для обновлений маршрутов. Для этого вида настройки подходит туннелирование общей инкапсуляции маршрутов (GRE). В этом примере маршрутизаторы Cisco 2621 и 3660 являются конечными точками туннеля IPSec, соединяющими две частные сети с кондуитами или списками управления доступом (ACL) на PIX между ними для обеспечения трафика IPSec.

Примечание: NAT является трансляцией адресов один к одному, чтобы не быть перепутанным с PAT, который является многими (в межсетевом экране)-to-one трансляция. Дополнительные сведения о работе и настройке NAT см. в статье Проверка работы NAT и основные способы поиска и устранения неисправностей NAT или Принципы работы NAT.

Примечание: IPSec с PAT может работать неправильно, поскольку внешнее оконечное устройство туннеля не может управлять несколькими туннелями с одного IP-адреса. Свяжитесь со своим поставщиком для выяснения, работают ли оконечные устройства туннеля с PAT. Кроме того, в версиях ПО Cisco IOS начиная с Release 12.2(13)T для PAT также можно использовать функцию прозрачности NAT. Дополнительные сведения см. в статье Прозрачность NAT IPSec. Подробнее о данных функциях в версиях ПО Cisco IOS начиная с Release 12.2(13)T см. в статье Поддержка ESP IPSec через NAT.

Примечание: Перед созданием обращения в TAC также обратитесь к документу Ответы на вопросы по NAT, где есть ответы на многие общие вопросы.

См. Настройку Туннель IPSec через Межсетевой экран с NAT для получения дополнительной информации о том, как настроить Туннель IPSec через межсетевой экран с NAT на Версии PIX 6.x и ранее.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Программное обеспечение Cisco IOS Release 12.0.7.T (до, но не включая, версии ПО Cisco IOS Release 12.2(13)T)Информацию о более новых версиях см. в документе Прозрачность NAT IPSec.
- Маршрутизатор Cisco 2621
- Маршрутизатор Cisco 3660
- Устройство защиты Cisco PIX серии 500, которое выполняется 7.x и выше.

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.

Условные обозначения

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

Родственные продукты

Этот документ может также использоваться с Устройством адаптивной защиты (ASA) серии 5500 Cisco с версией программного обеспечения 7.x и позже.

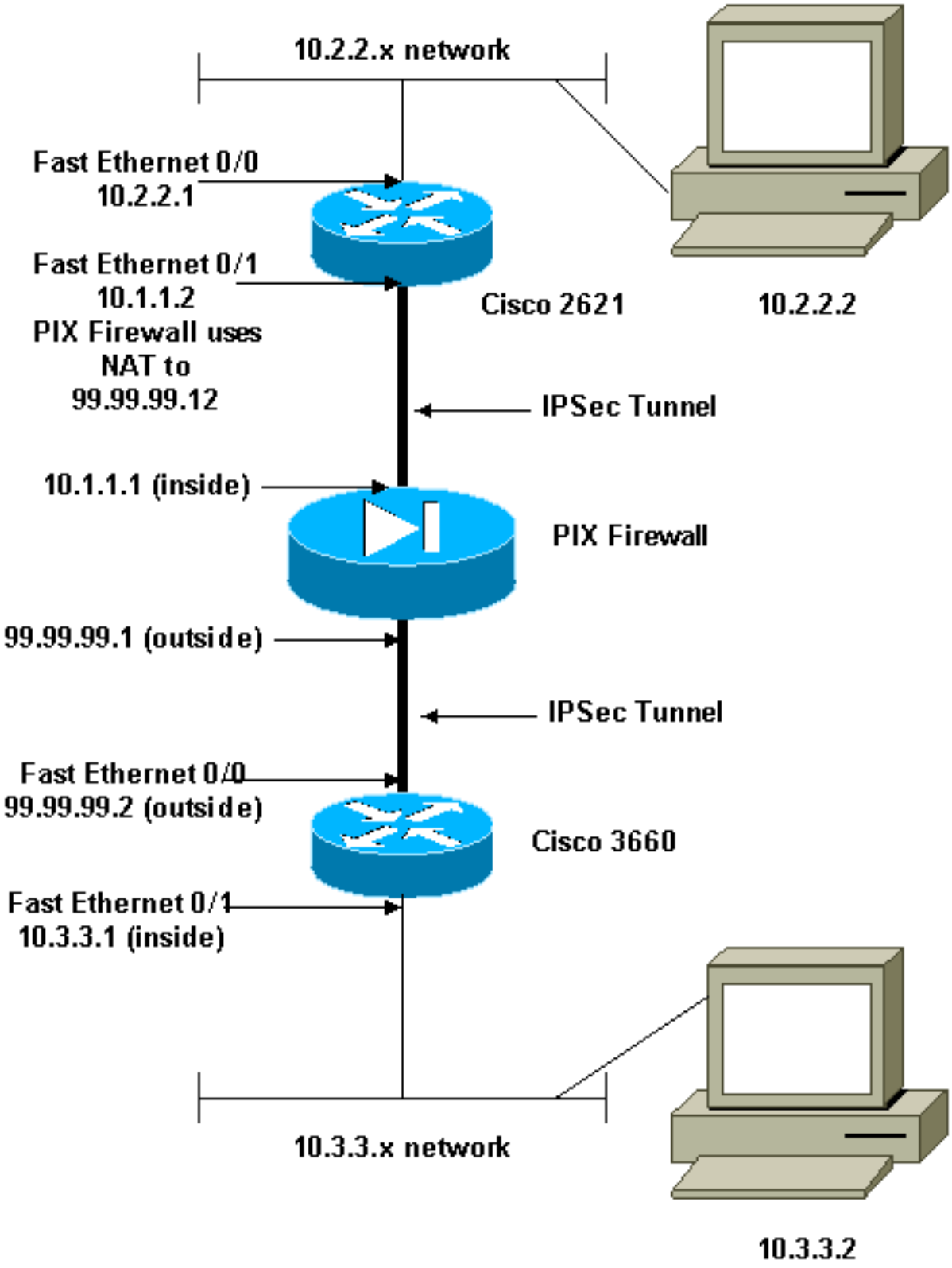
Настройка

В данном разделе приводятся сведения о настройке функций, описанных в этом документе.

Примечание: Для обнаружения дополнительных сведений об использовании этого документа команд используйте Средство поиска команд Command Lookup Tool (только зарегистрированные клиенты).

Схема сети

В настоящем документе используется следующая схема сети:



Конфигурации

Эти конфигурации используются в данном документе:

- Конфигурация Cisco 2621
- Конфигурация Cisco 3660
- Устройство безопасности PIX и конфигурация списка доступаМенеджер устройств дополнительной безопасности GUI (ASDM) конфигурацияКонфигурация интерфейса командной строки (CLI)
- Устройство безопасности PIX и MPF (модульная система политик) конфигурация

Cisco 2621

```
Current configuration:
 !
 version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-2621
 !
 ip subnet-zero
 !
 ip audit notify log
 ip audit po max-events 100
 isdn voice-call-failure 0
 cns event-service server
 !
!--- The IKE policy. crypto isakmp policy 10 hash md5
authentication pre-share crypto isakmp key cisco123
address 99.99.99.2 ! crypto ipsec transform-set myset
esp-des esp-md5-hmac ! crypto map mymap local-address
FastEthernet0/1 !--- IPsec policy. crypto map mymap 10
ipsec-isakmp set peer 99.99.99.2 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101 ! controller T1 1/0 ! interface FastEthernet0/0 ip
address 10.2.2.1 255.255.255.0 no ip directed-broadcast
duplex auto speed auto ! interface FastEthernet0/1 ip
address 10.1.1.2 255.255.255.0 no ip directed-broadcast
duplex auto speed auto !--- Apply to the interface.
crypto map mymap ! ip classless ip route 0.0.0.0 0.0.0.0
10.1.1.1 no ip http server !--- Include the private-
network-to-private-network traffic !--- in the
encryption process. access-list 101 permit ip 10.2.2.0
0.0.0.255 10.3.3.0 0.0.0.255 line con 0 transport input
none line aux 0 line vty 0 4 ! no scheduler allocate end
```

Cisco 3660

```
version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-3660
 !
 ip subnet-zero
 !
 cns event-service server
 !
```

```
!--- The IKE policy. crypto isakmp policy 10 hash md5
authentication pre-share crypto isakmp key cisco123
address 99.99.99.12 ! crypto ipsec transform-set myset
esp-des esp-md5-hmac ! crypto map mymap local-address
FastEthernet0/0 !--- The IPsec policy. crypto map mymap
10 ipsec-isakmp set peer 99.99.99.12 set transform-set
myset !--- Include the private-network-to-private-
network traffic !--- in the encryption process. match
address 101 ! interface FastEthernet0/0 ip address
99.99.99.2 255.255.255.0 no ip directed-broadcast ip nat
outside duplex auto speed auto !--- Apply to the
interface. crypto map mymap ! interface FastEthernet0/1
ip address 10.3.3.1 255.255.255.0 no ip directed-
broadcast ip nat inside duplex auto speed auto !
interface Ethernet3/0 no ip address no ip directed-
broadcast shutdown ! interface Serial3/0 no ip address
no ip directed-broadcast no ip mroute-cache shutdown !
interface Ethernet3/1 no ip address no ip directed-
broadcast interface Ethernet4/0 no ip address no ip
directed-broadcast shutdown ! interface TokenRing4/0 no
ip address no ip directed-broadcast shutdown ring-speed
16 ! !--- The pool from which inside hosts translate to
!--- the globally unique 99.99.99.0/24 network. ip nat
pool OUTSIDE 99.99.99.70 99.99.99.80 netmask
255.255.255.0 !--- Except the private network from the
NAT process. ip nat inside source route-map nonat pool
OUTSIDE ip classless ip route 0.0.0.0 0.0.0.0 99.99.99.1
no ip http server ! !--- Include the private-network-to-
private-network traffic !--- in the encryption process.
access-list 101 permit ip 10.3.3.0 0.0.0.255 10.2.2.0
0.0.0.255 access-list 101 deny ip 10.3.3.0 0.0.0.255 any
!--- Except the private network from the NAT process.
access-list 110 deny ip 10.3.3.0 0.0.0.255 10.2.2.0
0.0.0.255 access-list 110 permit ip 10.3.3.0 0.0.0.255
any route-map nonat permit 10 match ip address 110 !
line con 0 transport input none line aux 0 line vty 0 4
! end
```

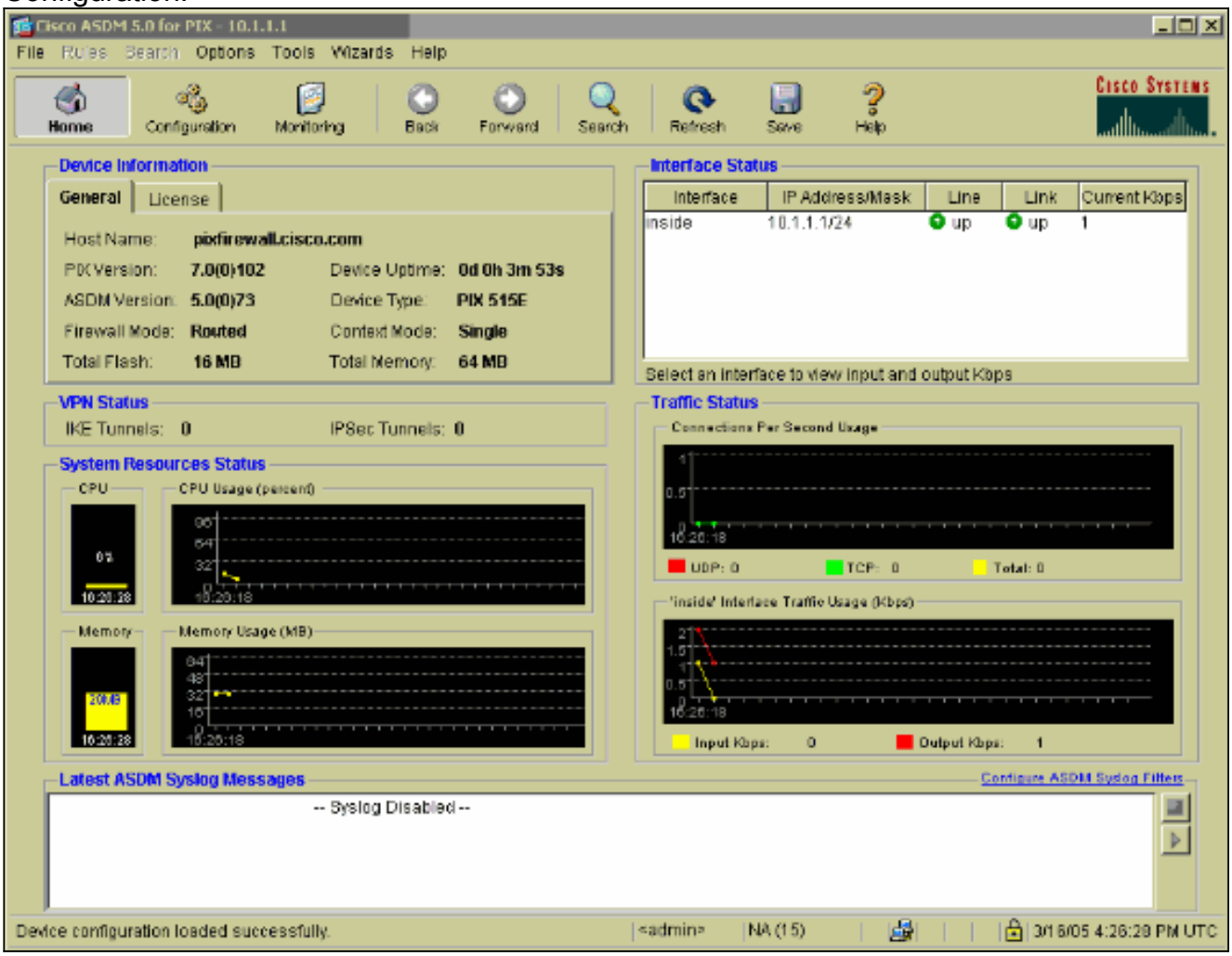
Устройство безопасности PIX и конфигурация списка доступа

Конфигурация ASDM 5.0

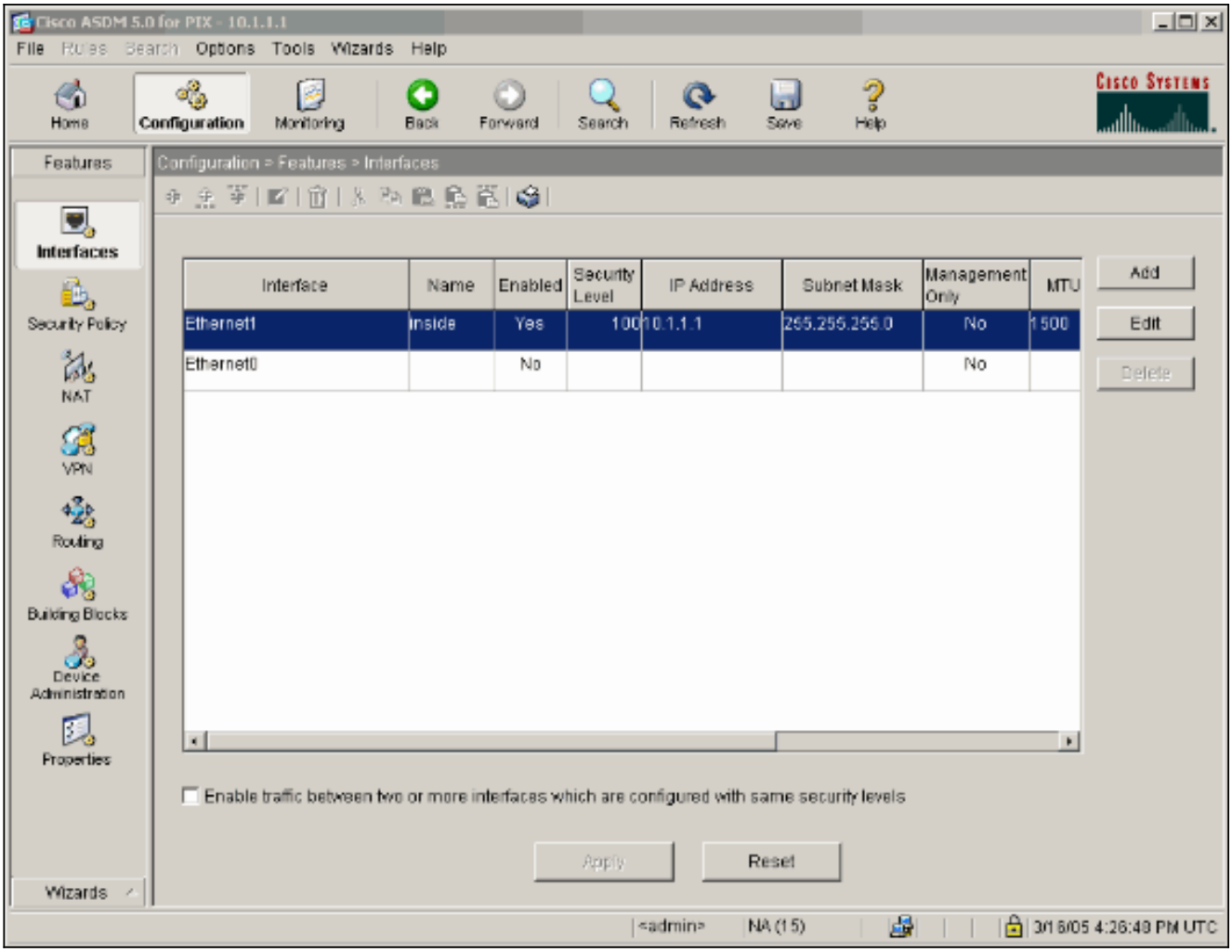
Для настройки брандмауэра PIX версии 7.0 при помощи графического интерфейса пользователя ASDM выполните следующие действия.

1. Войдите в консоль PIX. **Из очищенной конфигурации используйте интерактивные запросы, позволяющие включить графический интерфейс Advanced Security Device Manager (ASDM) для управления PIX с рабочей станции 10.1.1.3.**
2. На рабочей станции 10.1.1.3 откройте веб-браузер, чтобы воспользоваться ADSM (в данном примере https://10.1.1.1).
3. **В запросе сертификата выберите Yes и войдите с паролем режима включения, настройка которого описана в разделе Настройка начальной загрузки ASDM брандмауэра PIX.**
4. Если это первый запуск ASDM на ПК, будет выдан запрос на использование ASDM Launcher или использование ASDM в качестве Java-приложения.В данном примере выбирается и устанавливается ASDM Launcher.

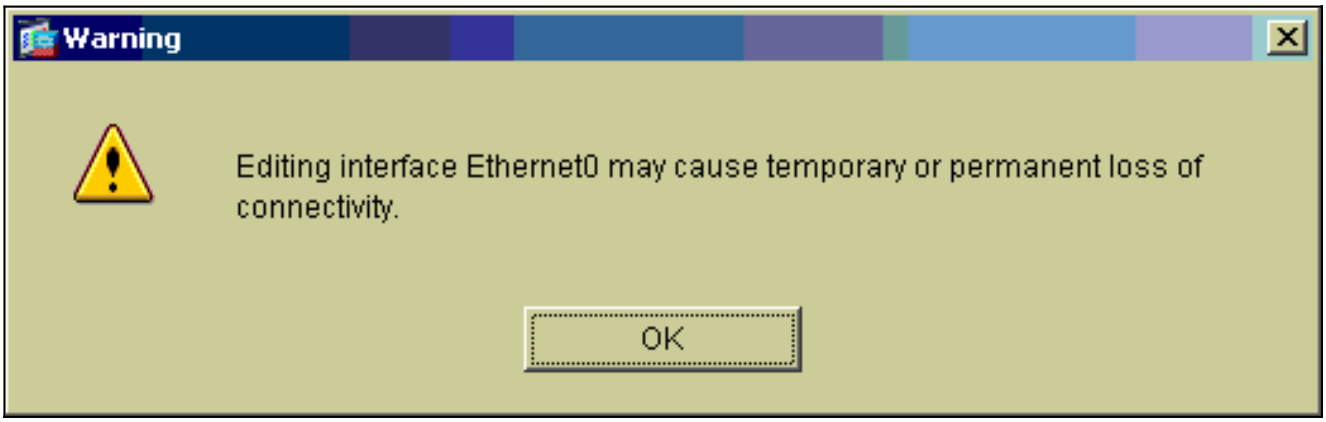
5. Перейдите на страницу Home ASDM и выберите вкладку Configuration.



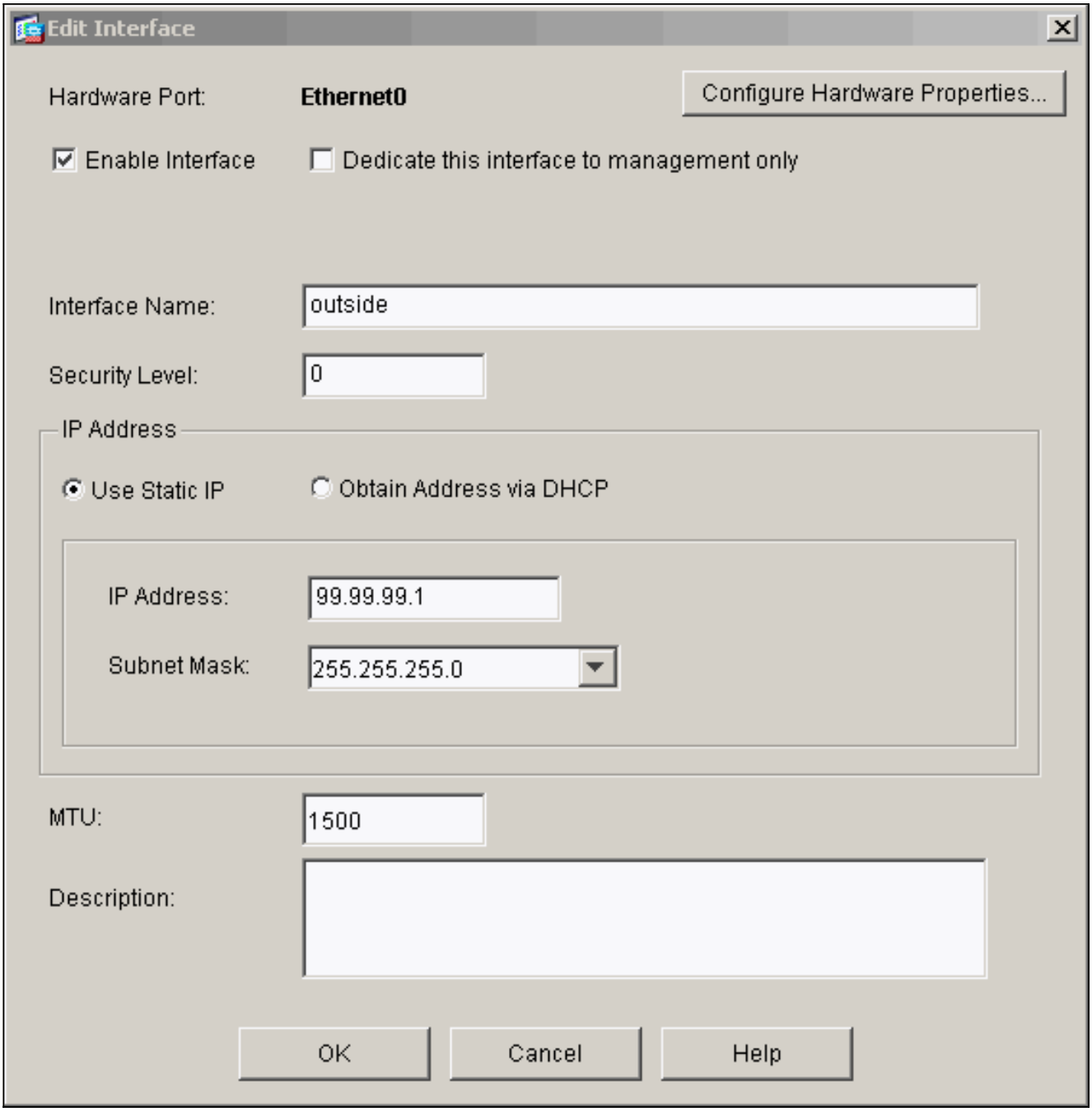
6. **Чтобы настроить внешний интерфейс, выберите интерфейс Ethernet 0 и нажмите кнопку Edit.**



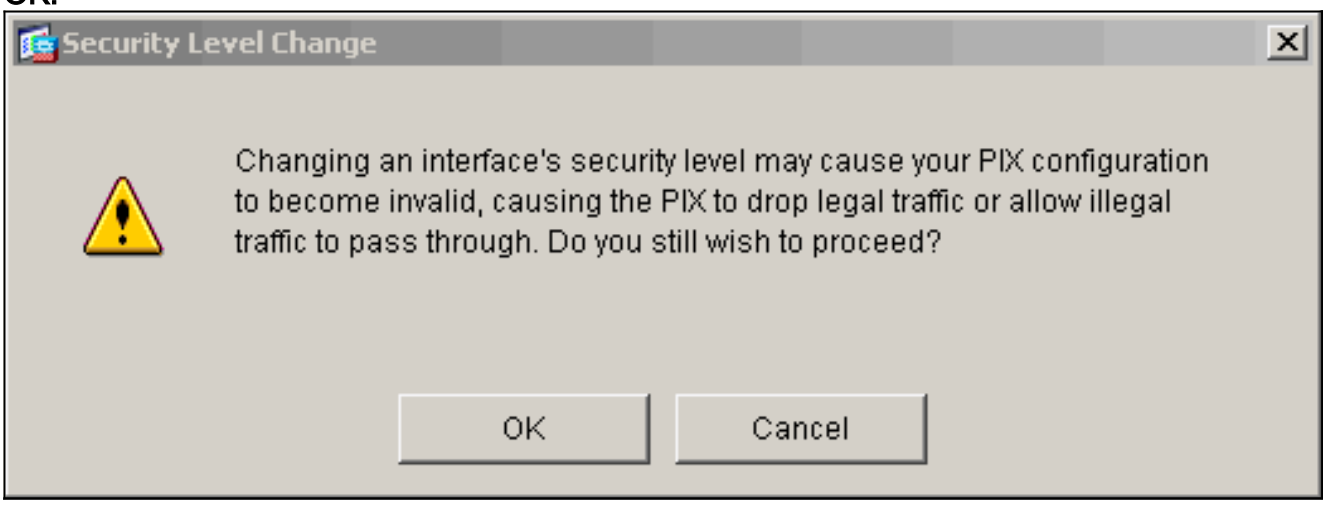
7. В запросе Editing interface нажмите кнопку OK.



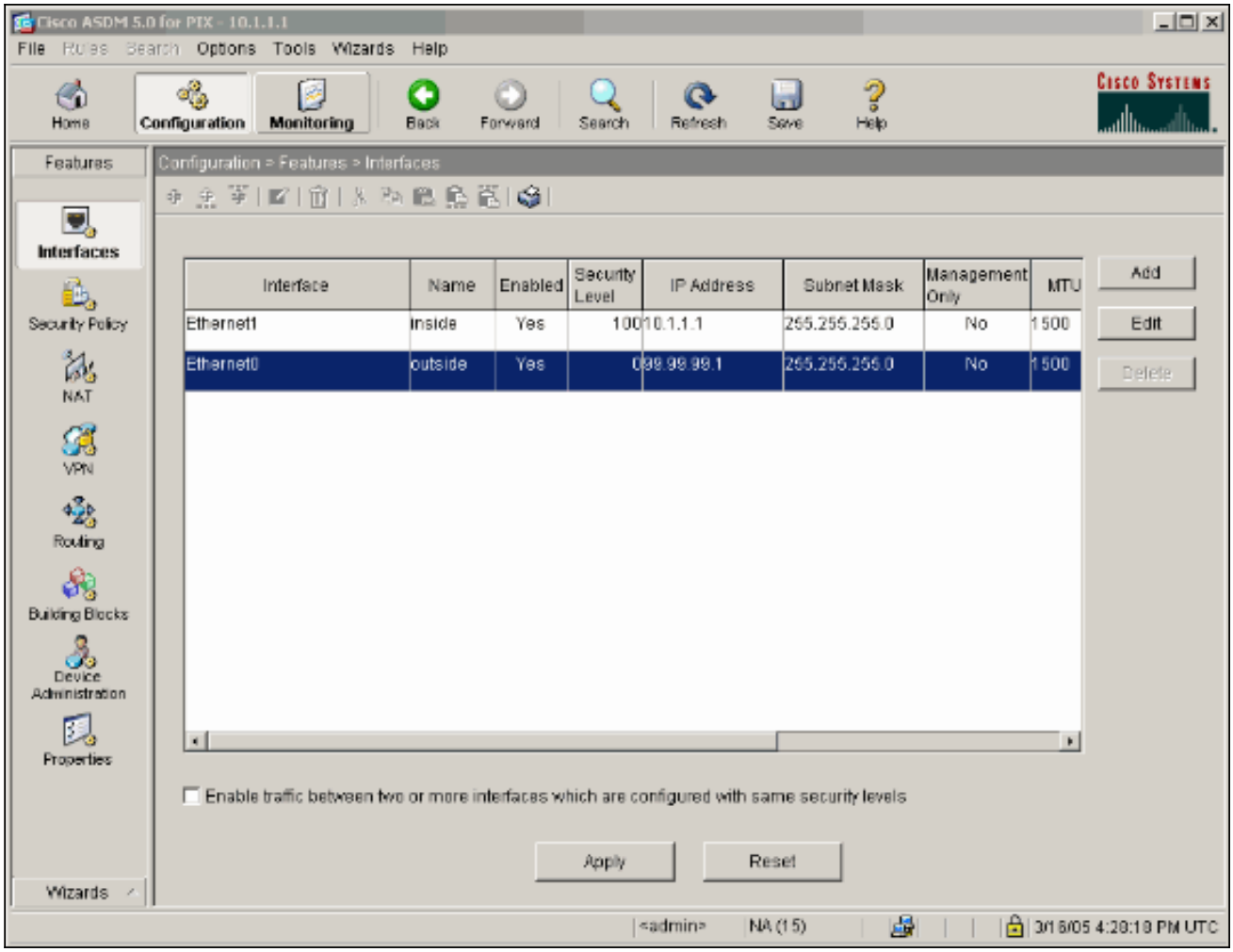
8. Введите все данные интерфейса и после завершения нажмите кнопку OK.



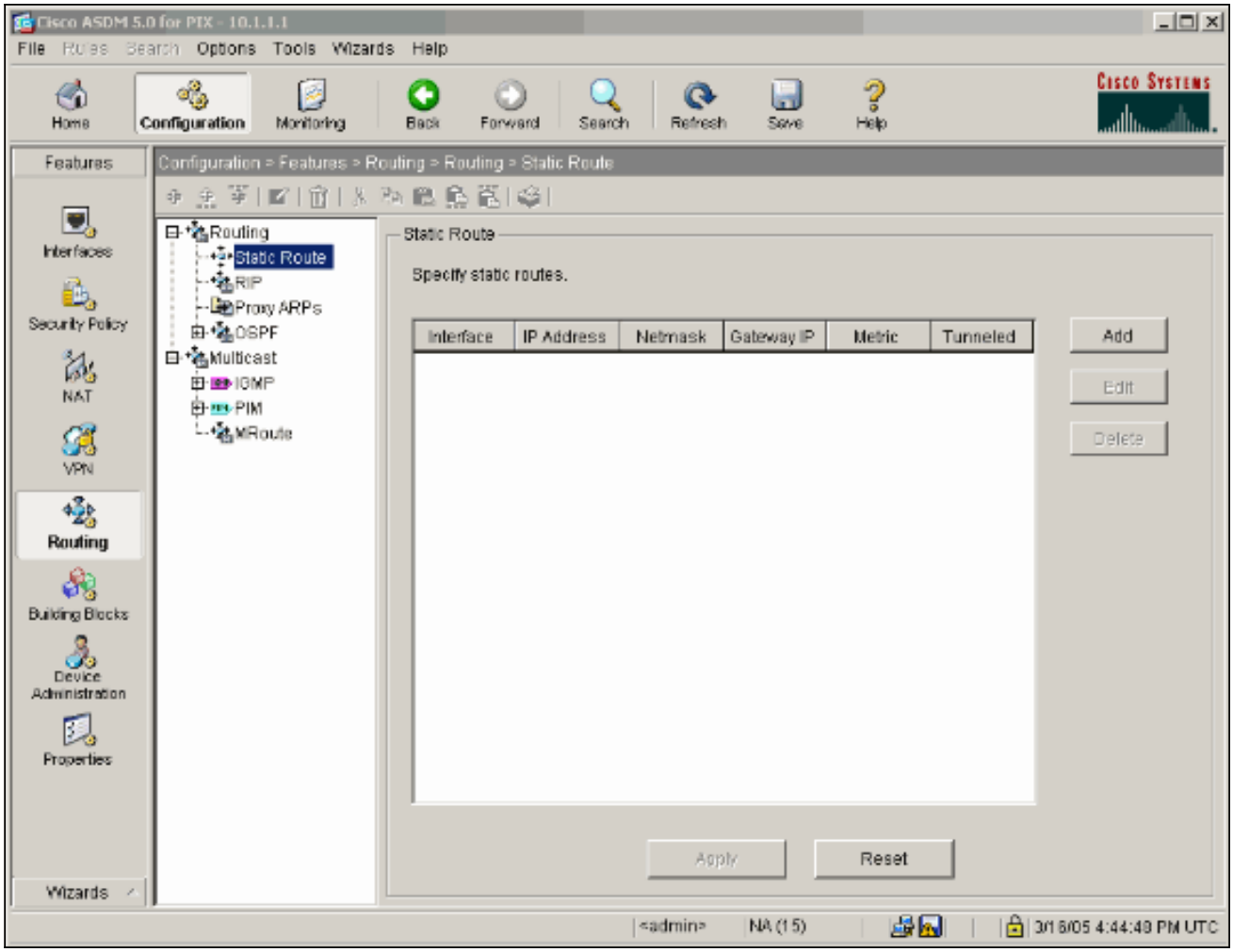
9. **В запросе Changing an Interface нажмите кнопку OK.**



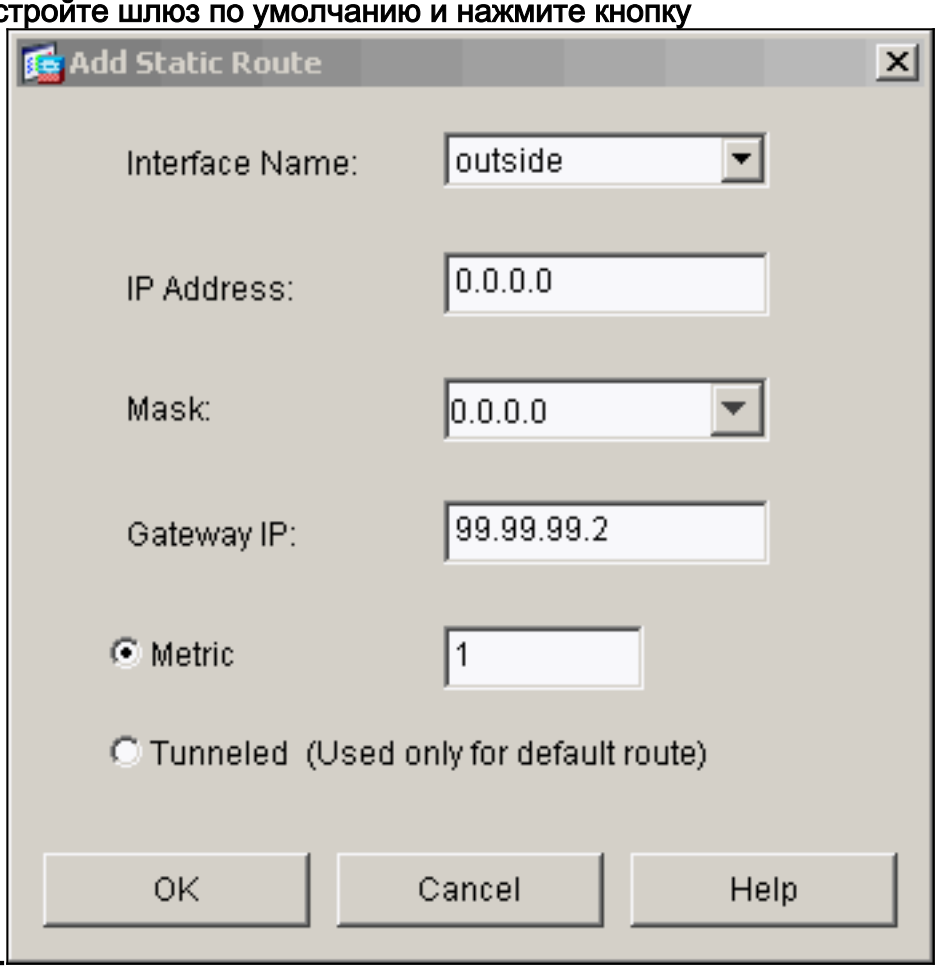
10. **Чтобы принять конфигурацию интерфейса, нажмите Apply.** При этом конфигурация загружается в PIX. В этом примере используются статические маршруты.



11. На вкладке Features нажмите кнопку Routing выберите Static Route и нажмите кнопку Add.

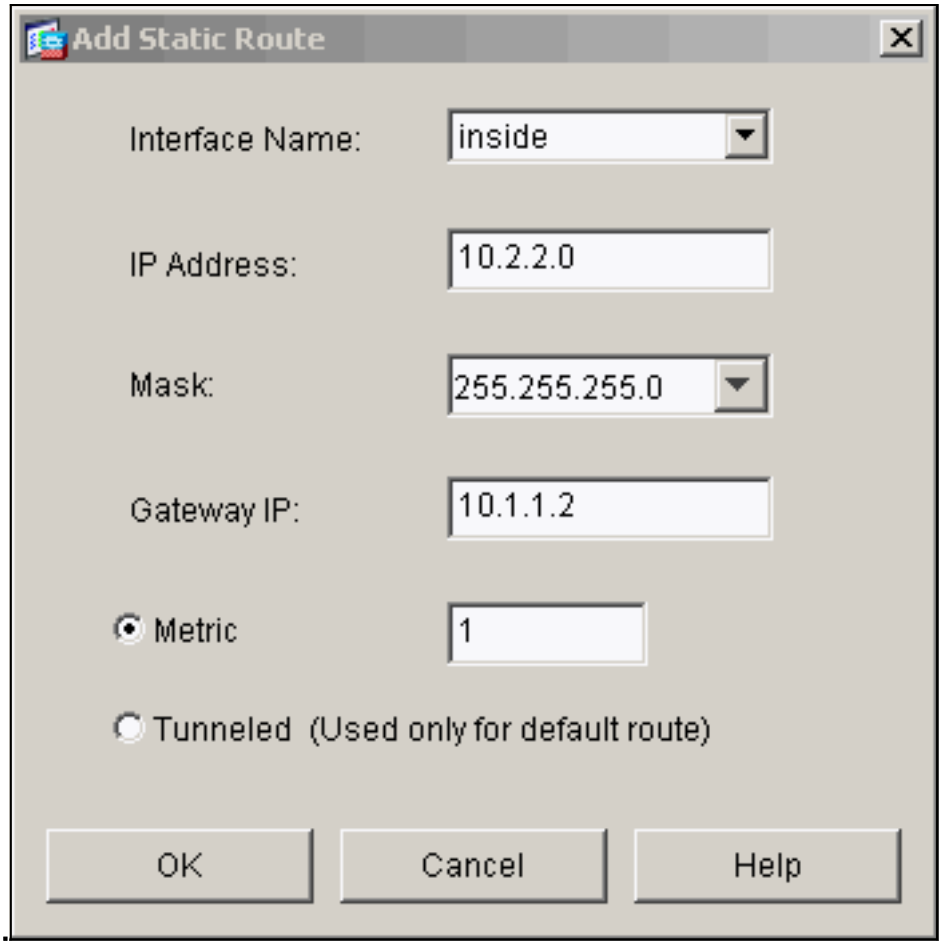


12. Настройте шлюз по умолчанию и нажмите кнопку



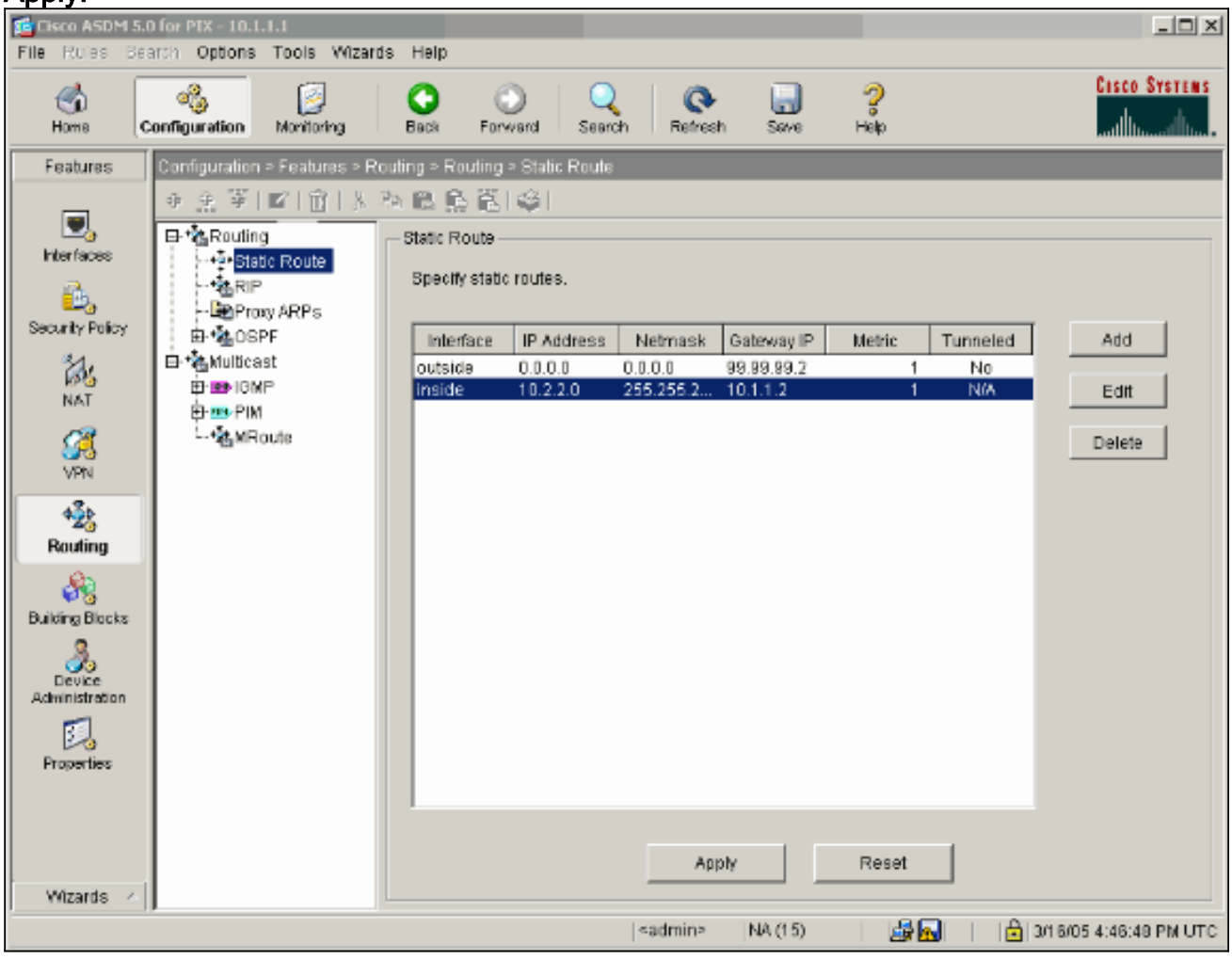
OK.

13. Нажмите кнопку Add и добавьте маршруты к внутренним

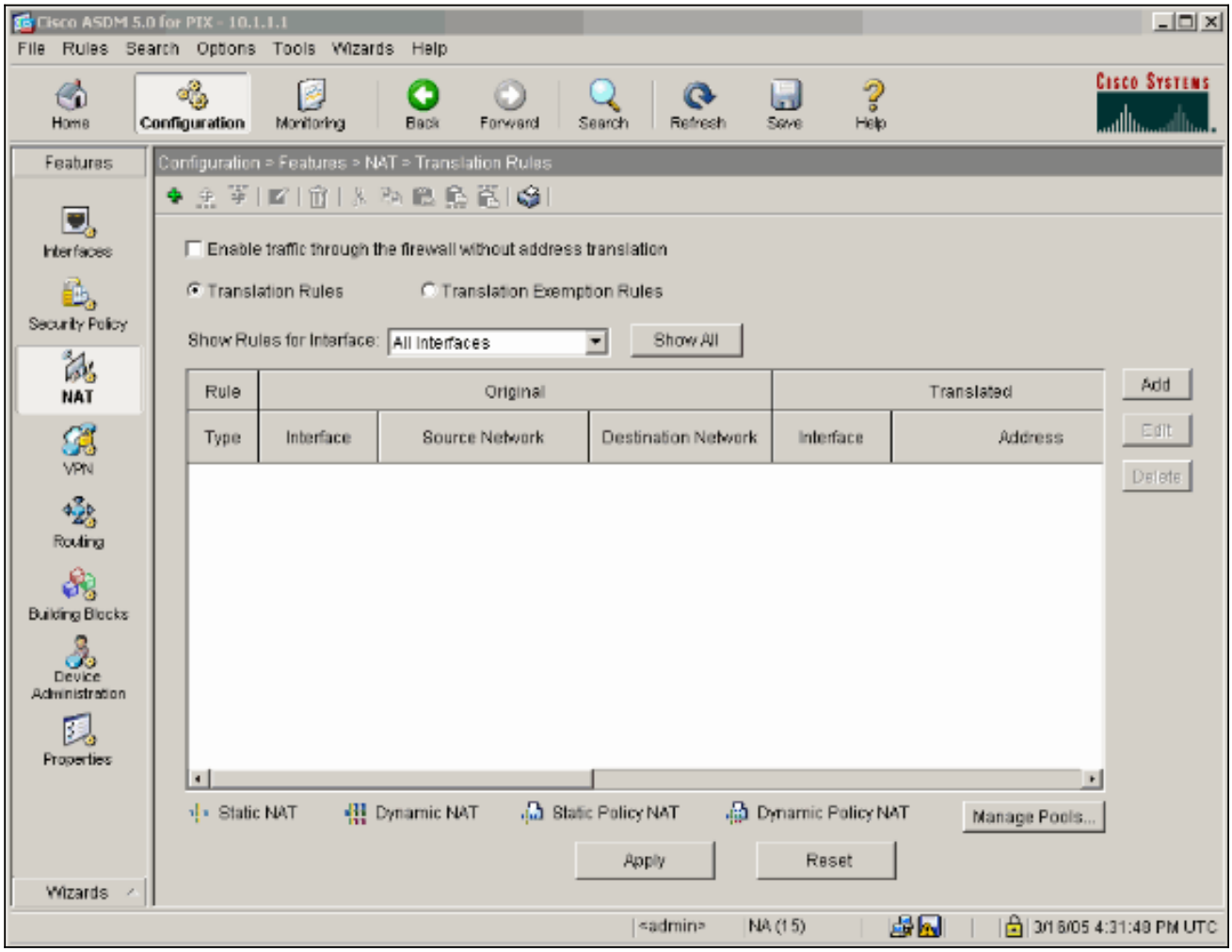


сетям.

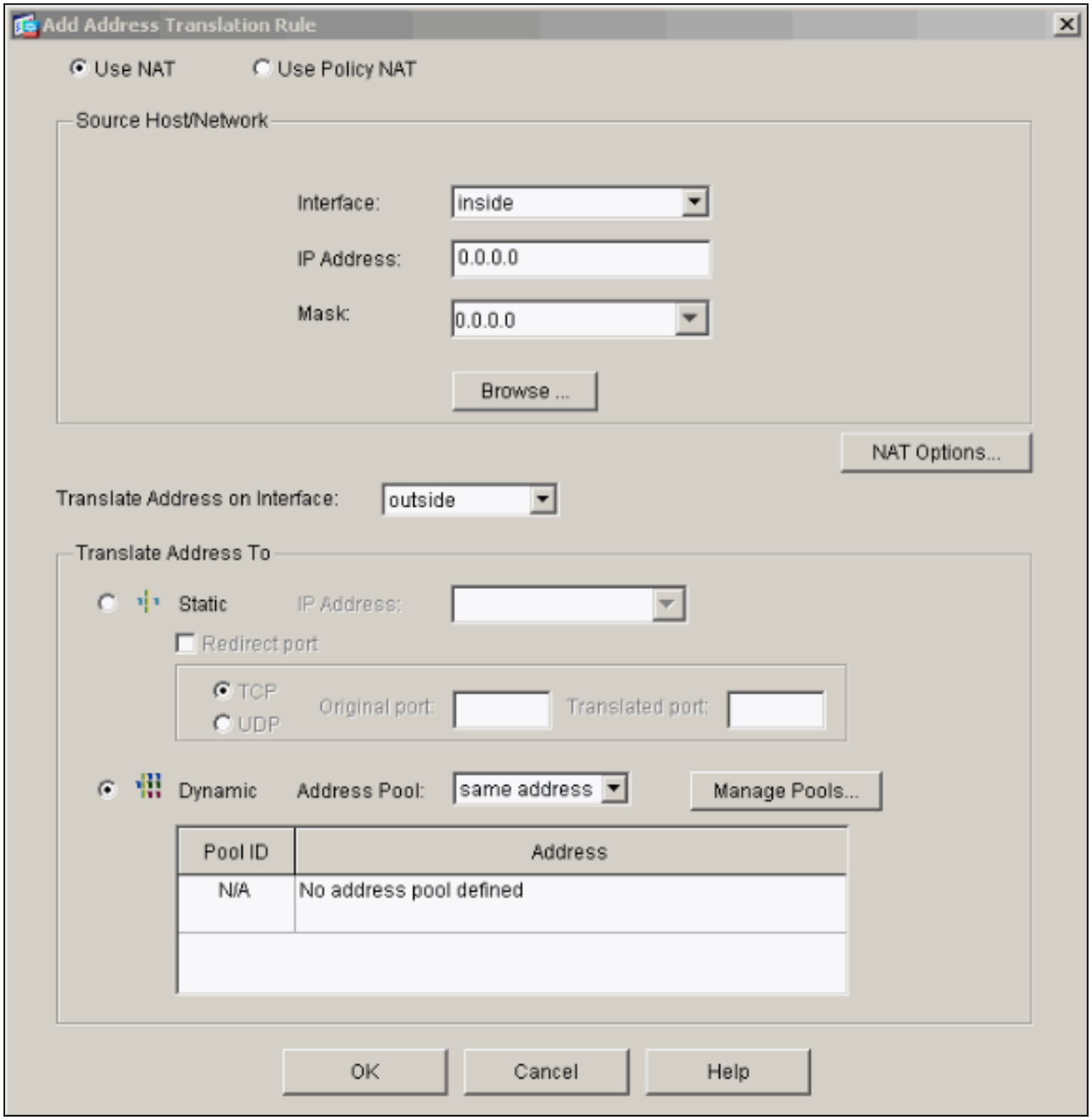
14. Подтвердите правильность настройки маршрутов и щелкните Apply.



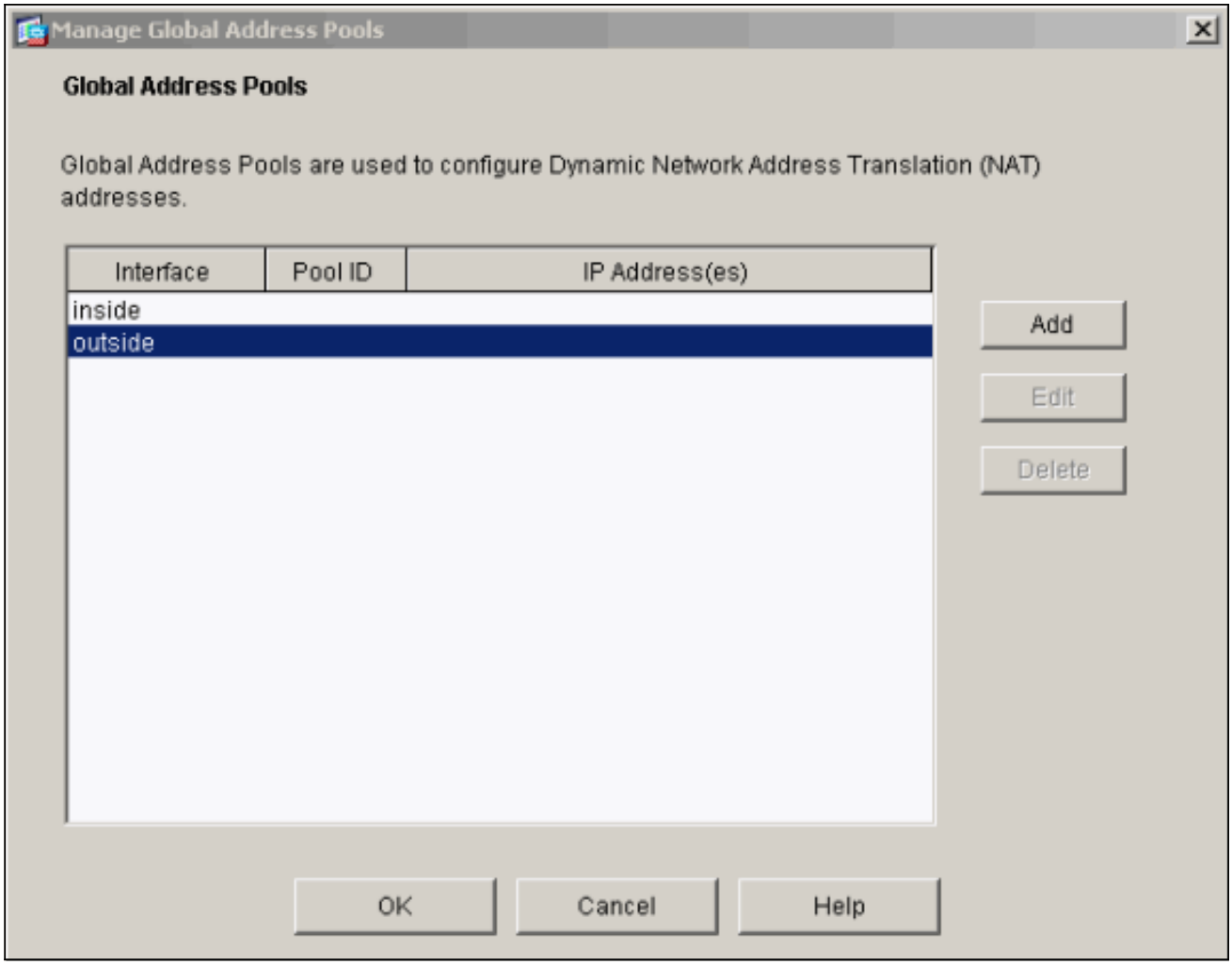
15. В данном примере используется NAT. **Чтобы настроить правило NAT, снимите флажок Enable traffic through the firewall without address translation и нажмите кнопку Add.**



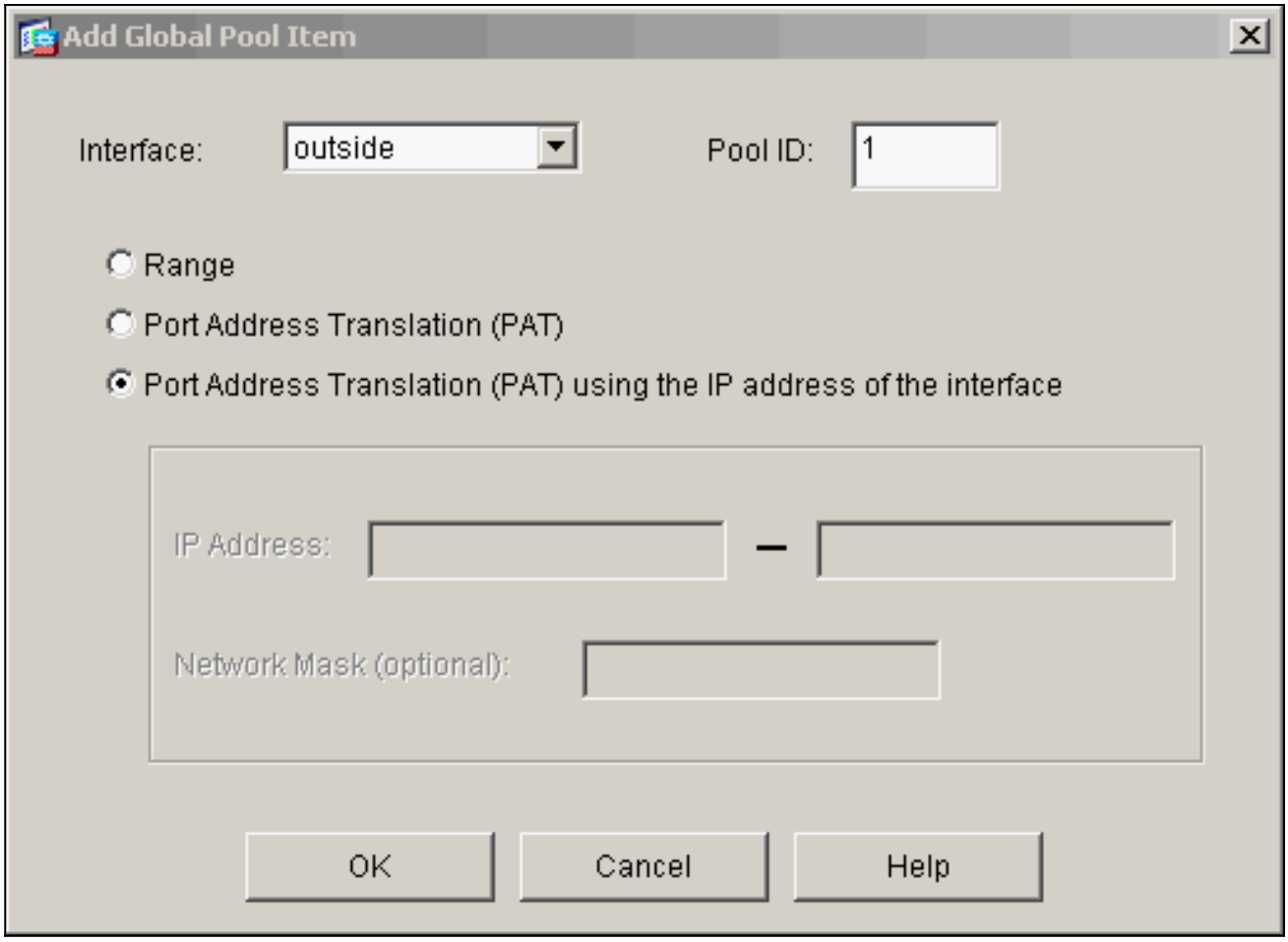
16. Настройте Source Network (сеть-источник, используется только в данном примере). **Чтобы задать PAT, нажмите кнопку Manage Pools.**



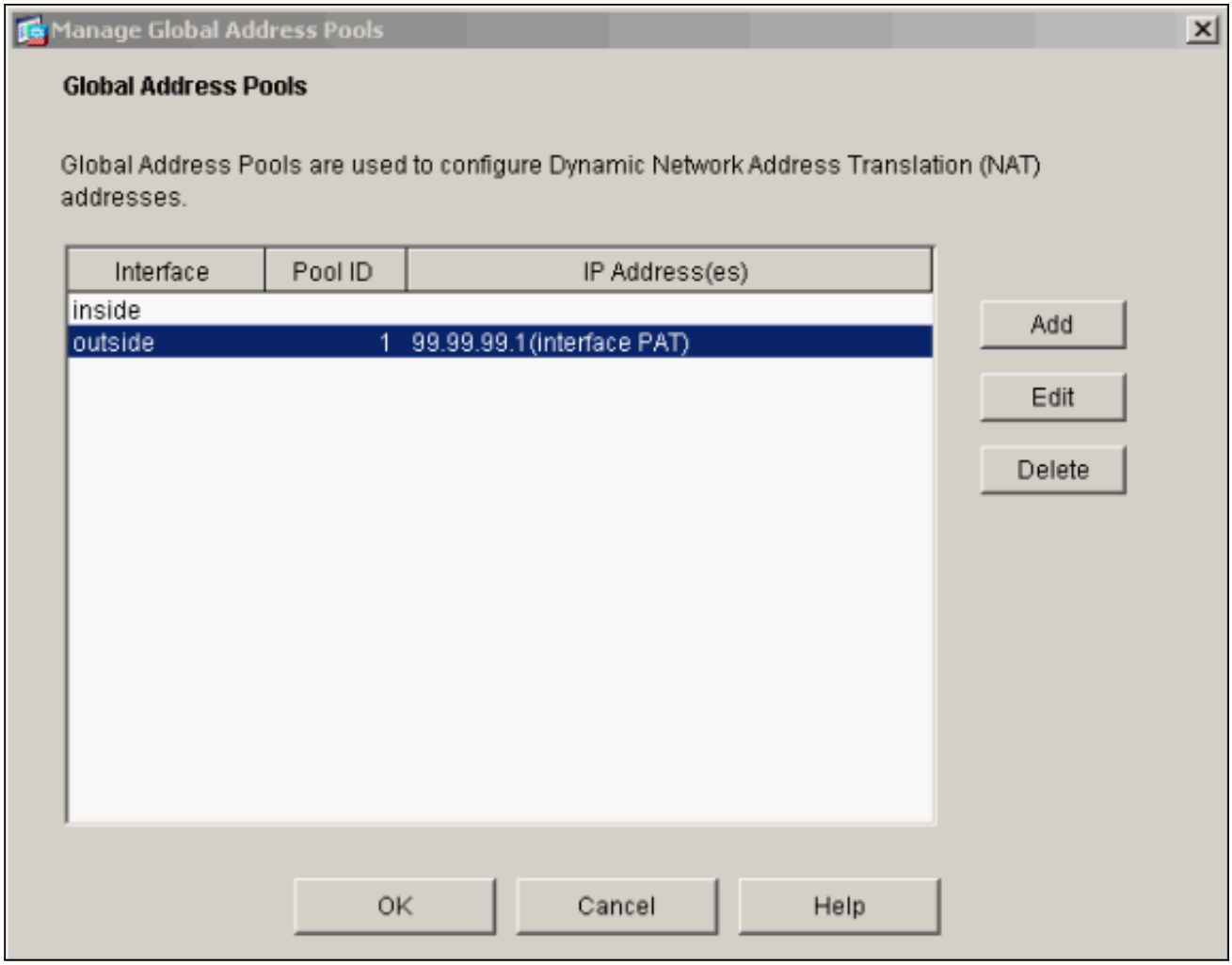
17. **Выберите outside интерфейс и нажмите Add.**



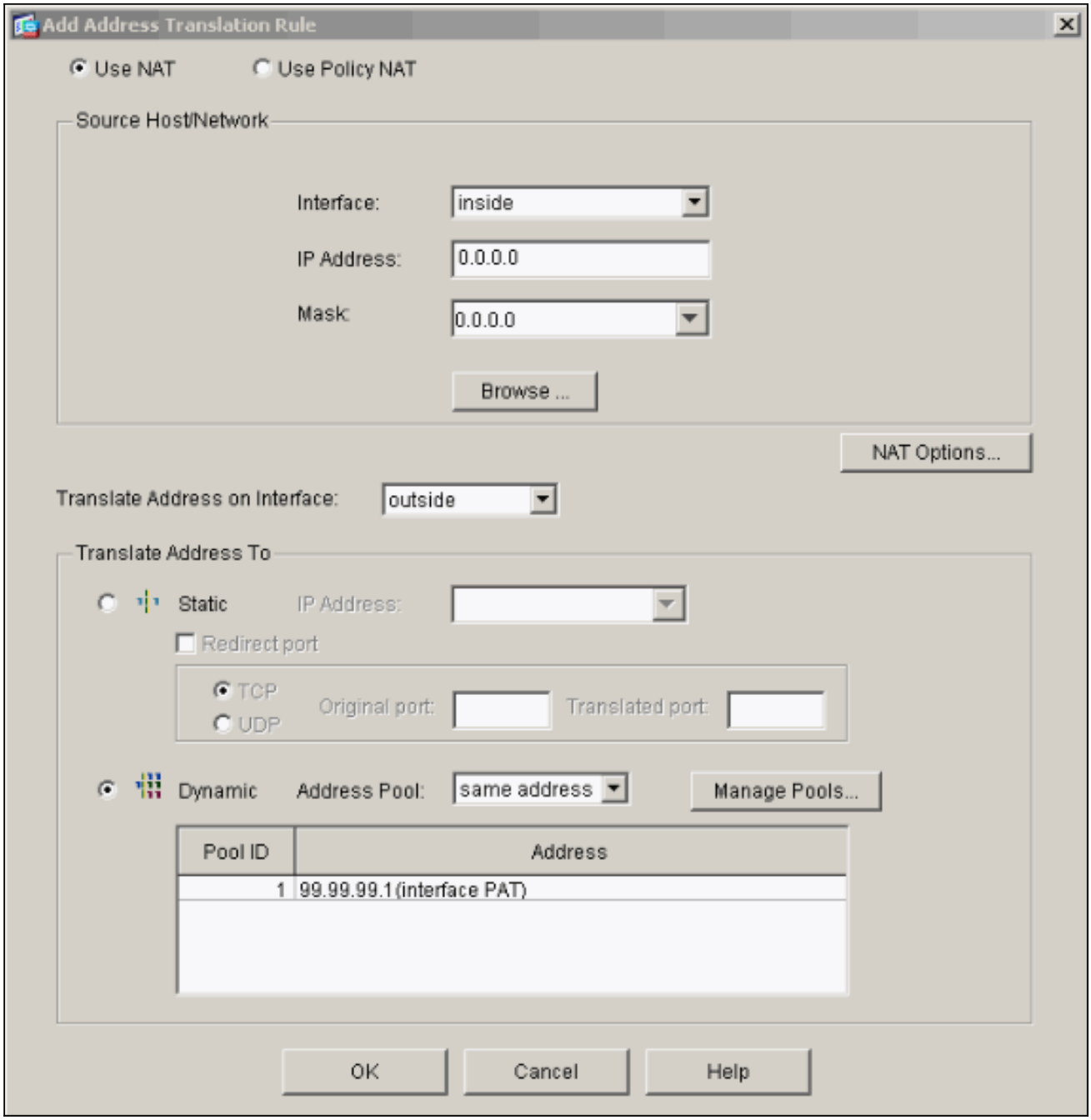
В данном примере применяется PAT, использующее IP-адрес интерфейса.



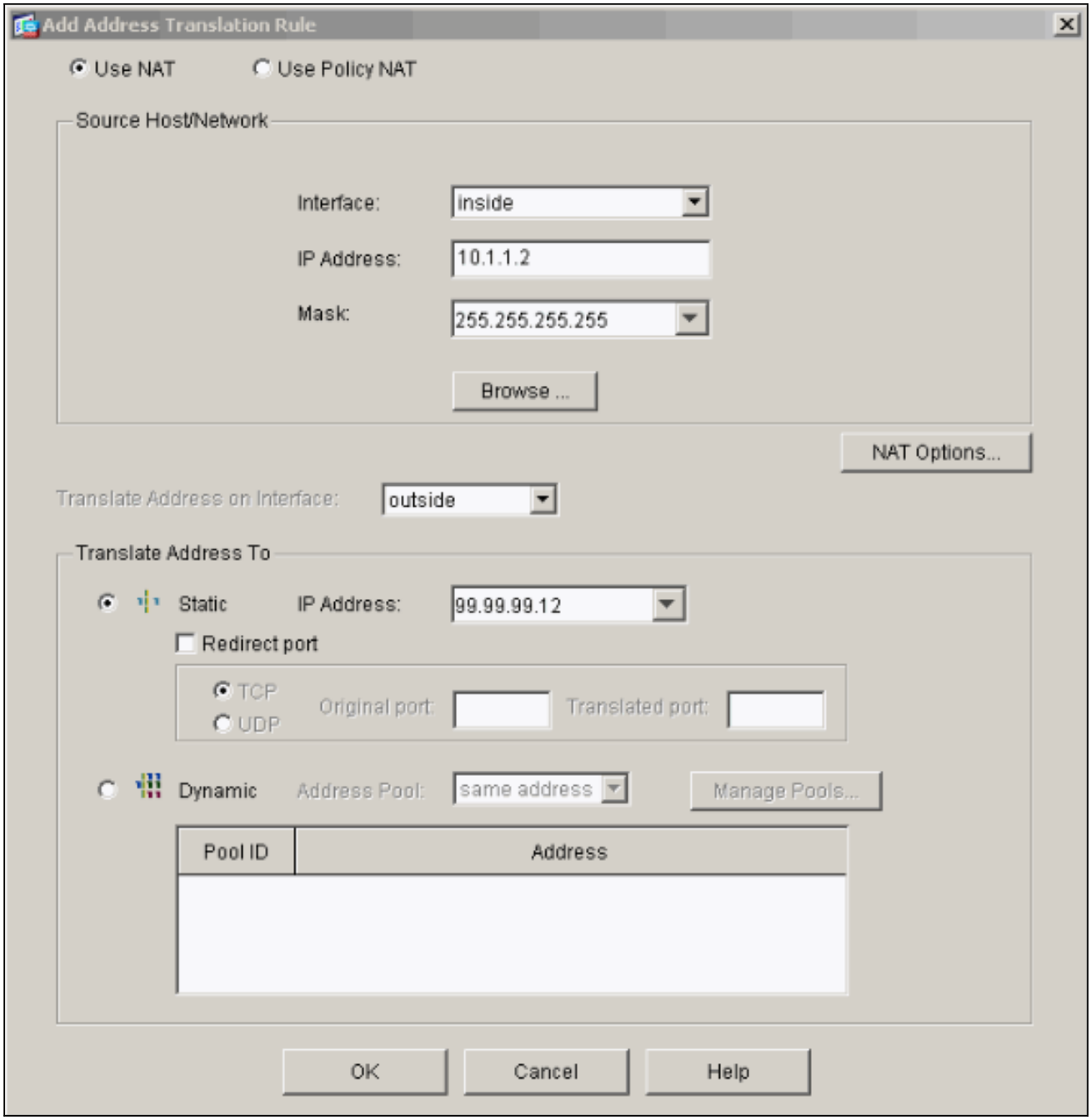
18. Настроив PAT, нажмите кнопку **OK**.



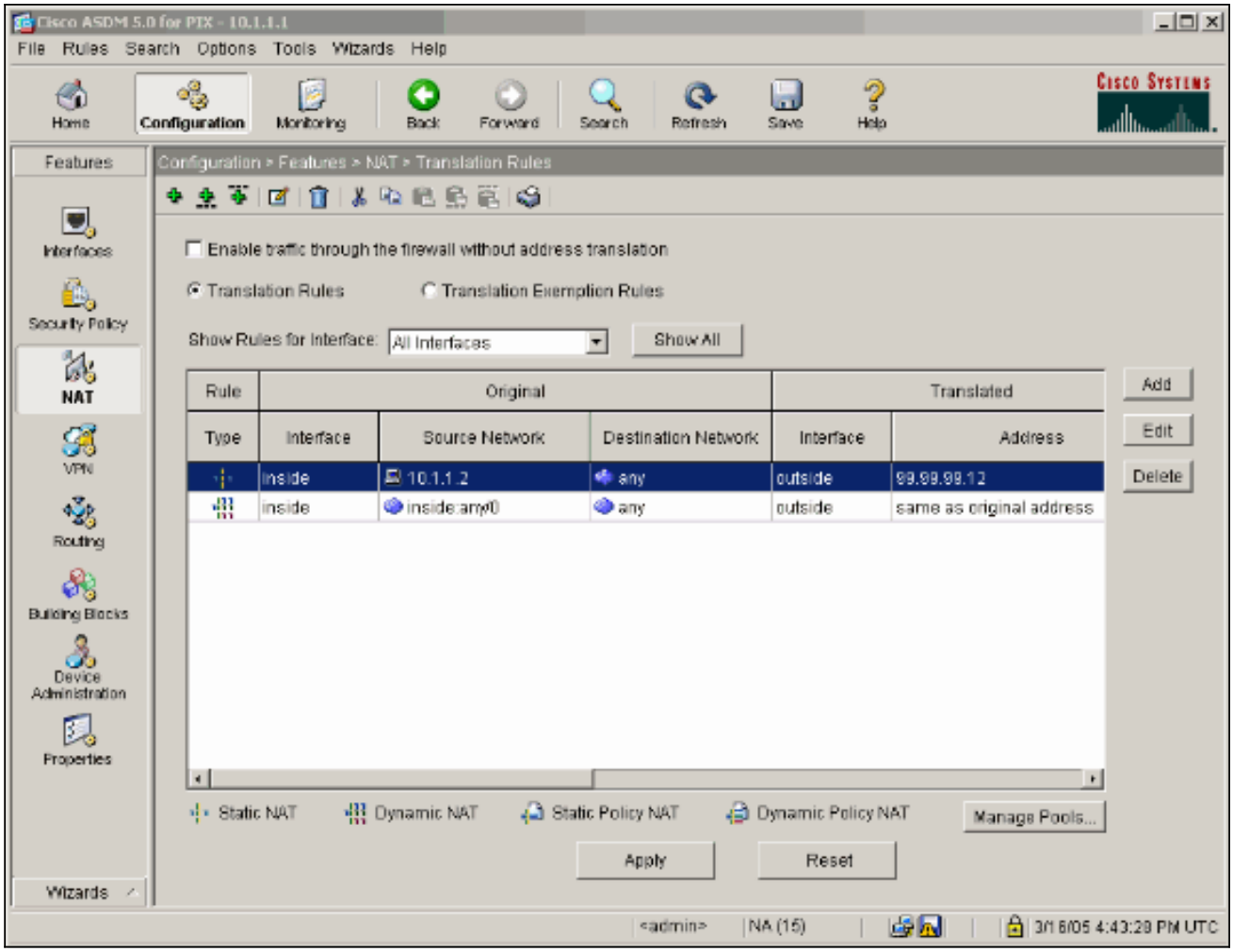
19. Для настройки статического преобразования нажмите кнопку OK.



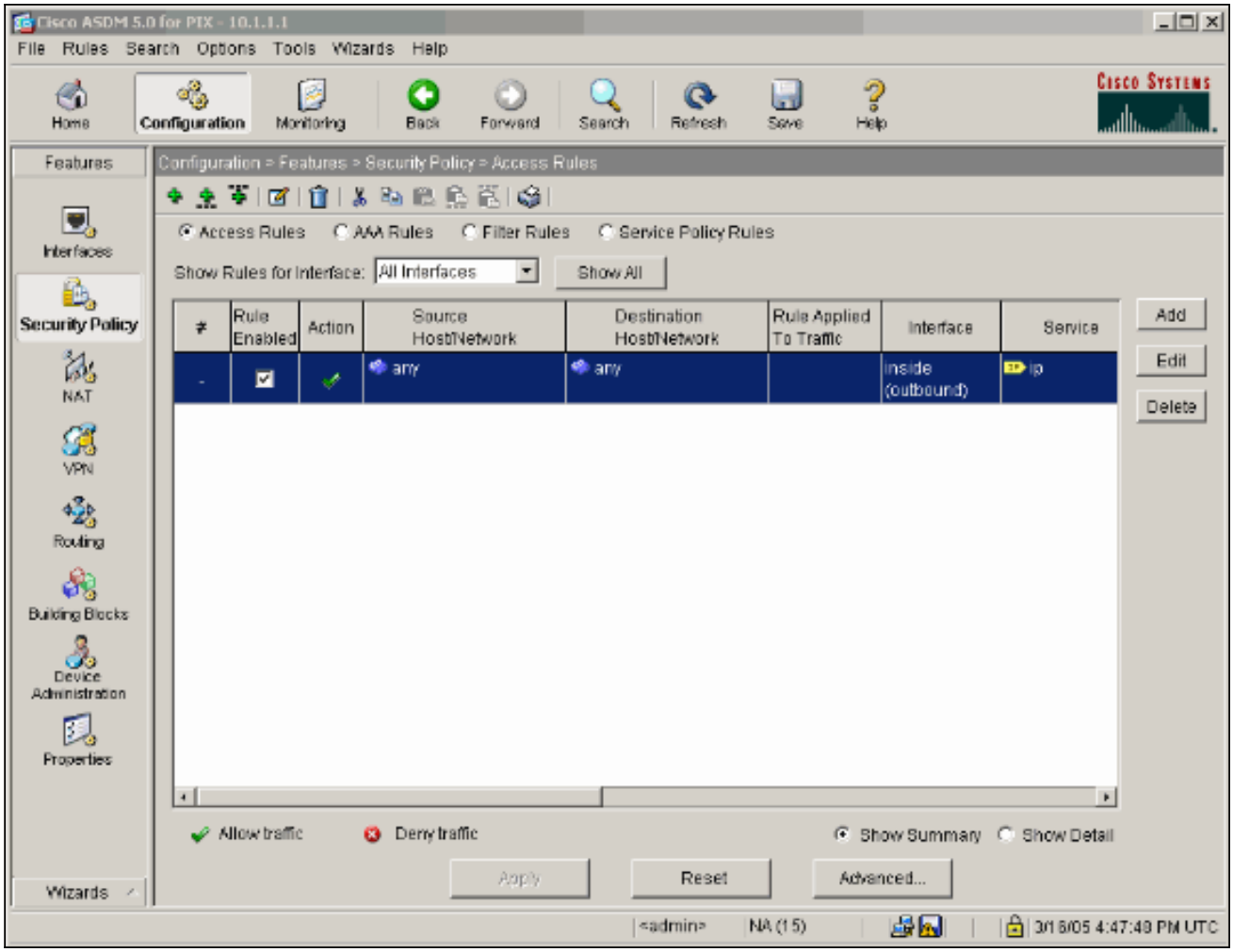
20. **В выпадающем списке интерфейсов выберите inside, введите IP-адрес 10.1.1.2, маску подсети 255.255.255.255, выберите Static, а в поле IP-адреса введите внешний адрес 99.99.99.12. Закончив все действия, нажмите кнопку OK.**



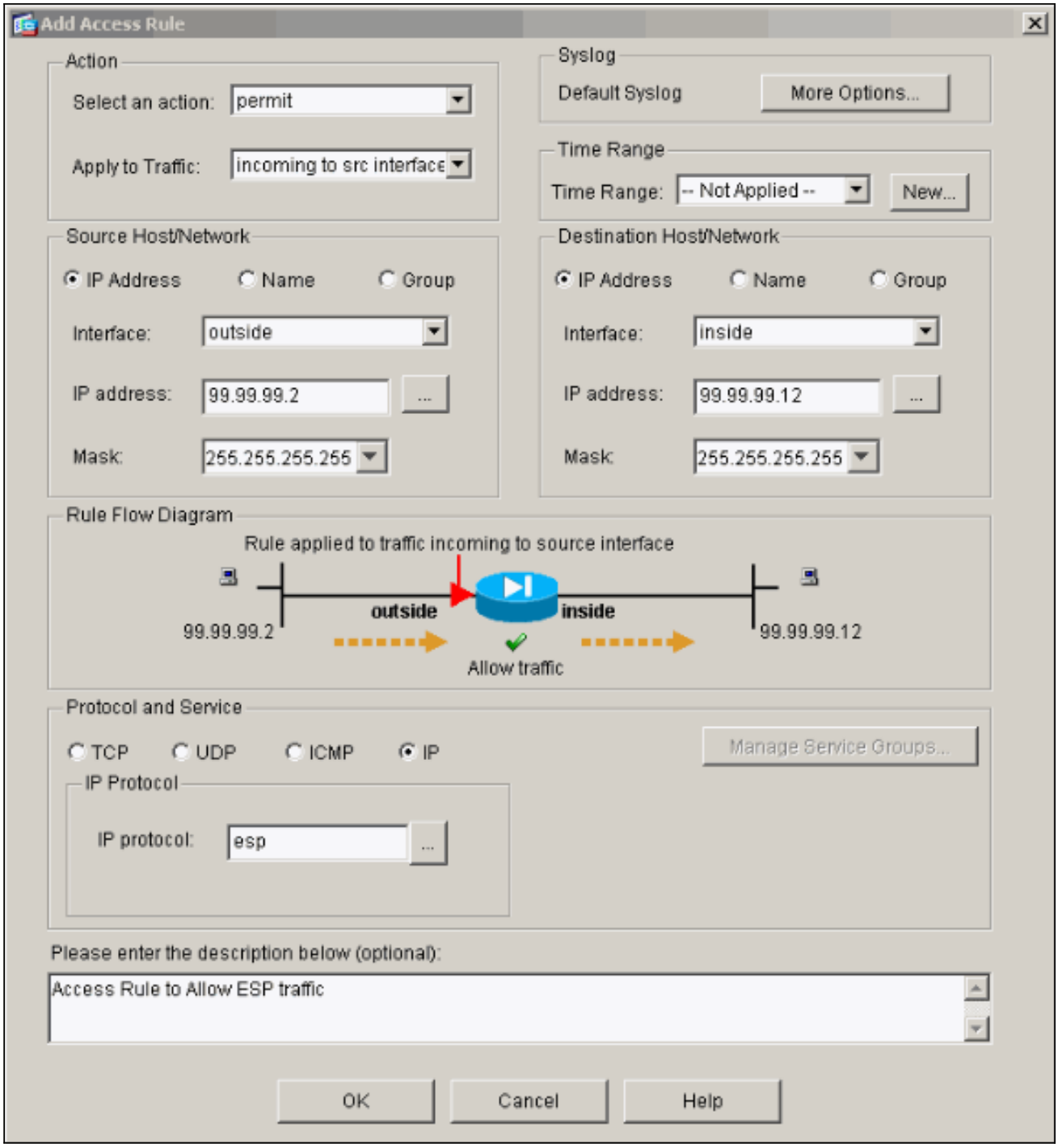
21. **Чтобы сохранить конфигурацию интерфейса, нажмите кнопку Apply.** При этом конфигурация загружается в PIX.



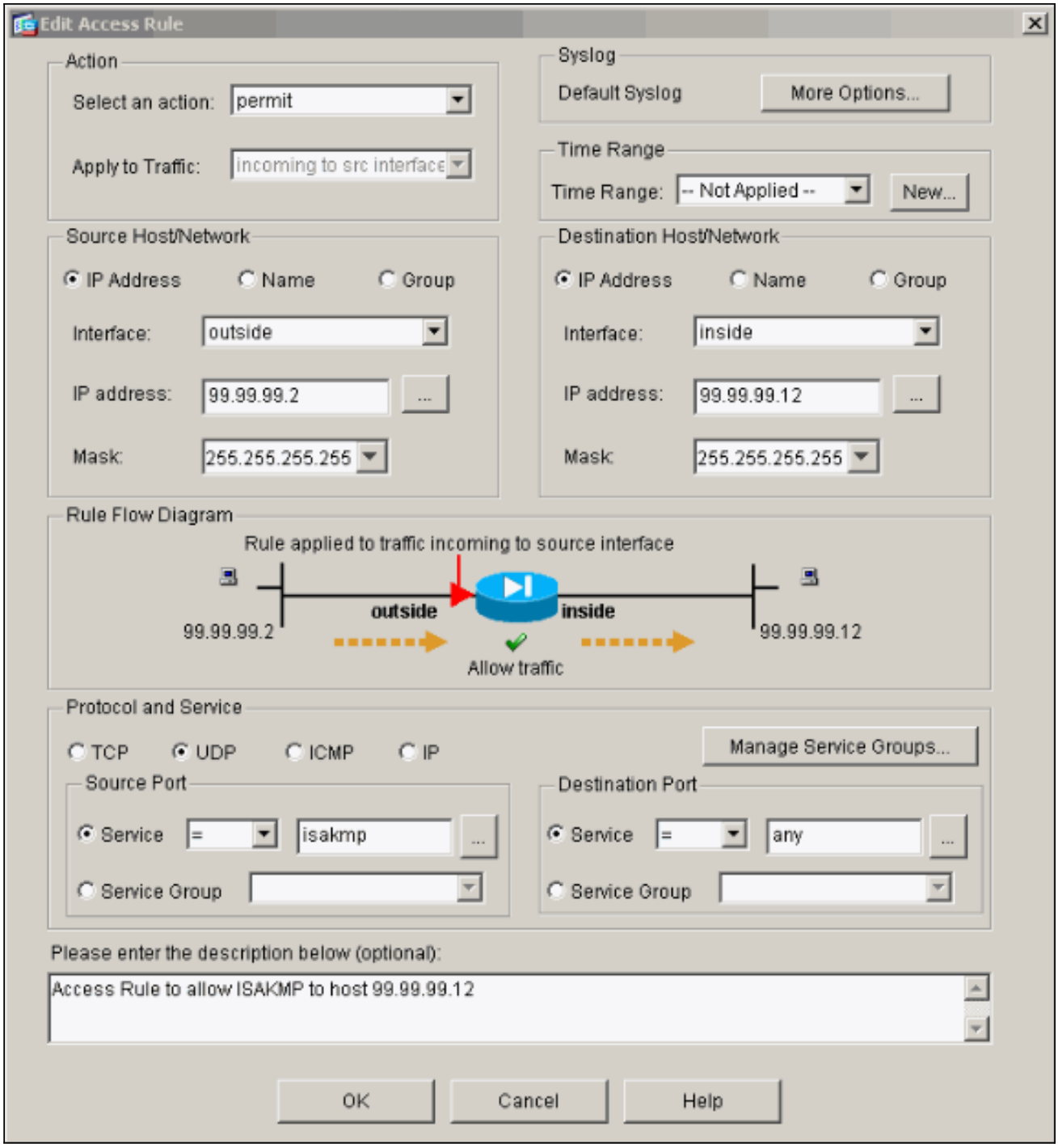
22. Во вкладке Features выберите Security Policy, чтобы настроить правило политики безопасности.



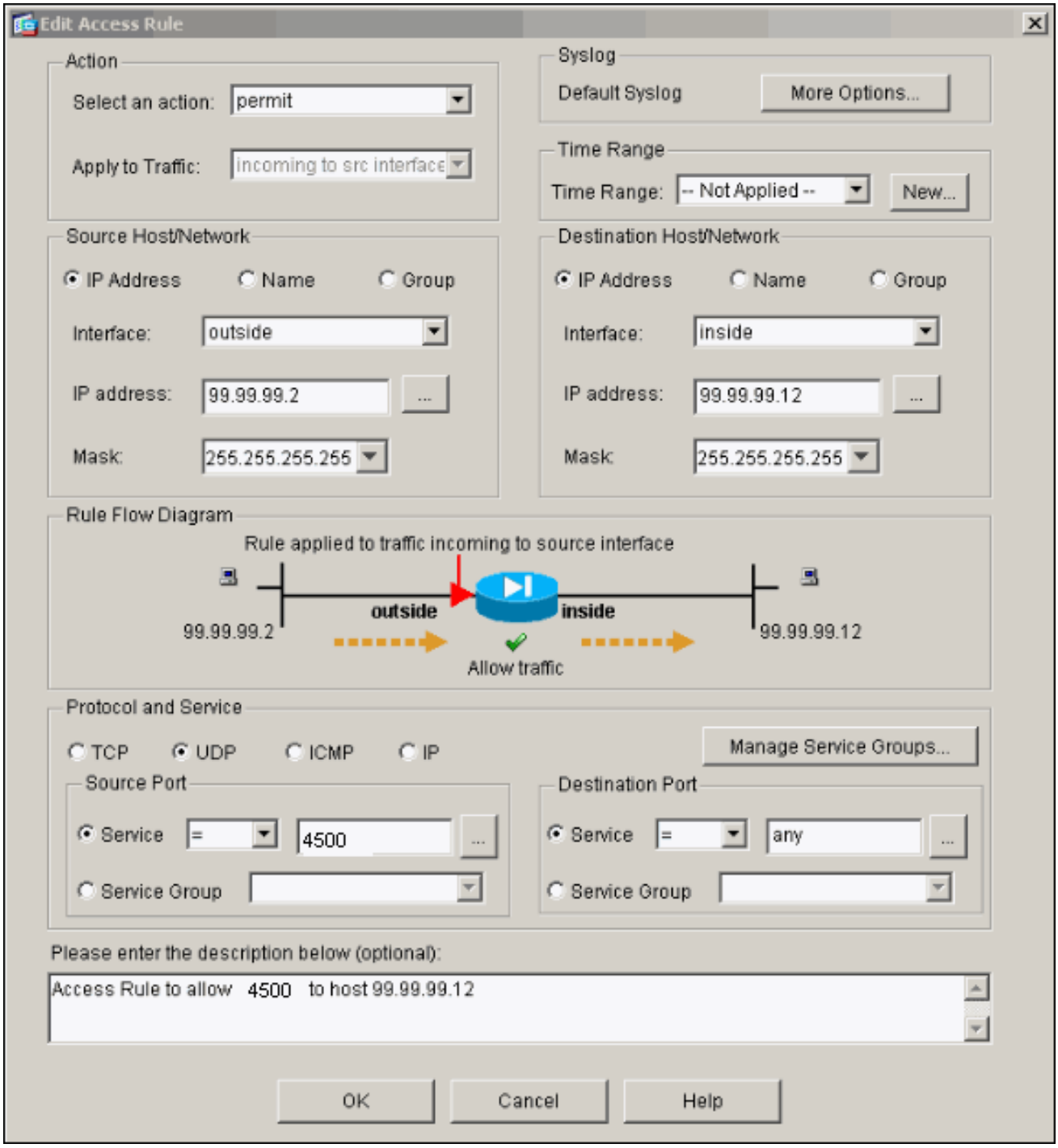
23. Чтобы разрешить трафик esp, нажмите кнопку Add. Для продолжения нажмите кнопку OK.



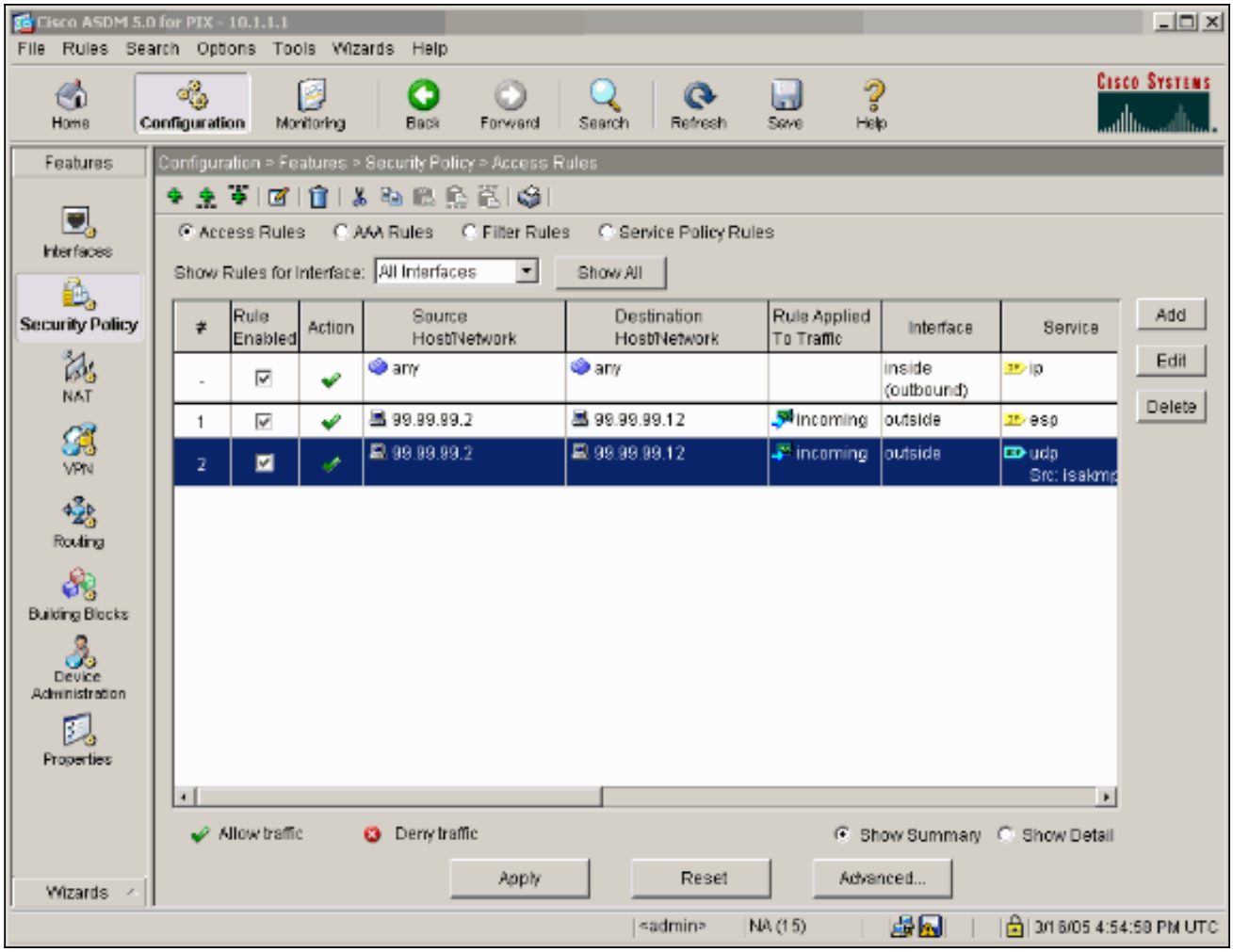
24. Чтобы разрешить трафик ISAKMP, нажмите кнопку Add. Для продолжения нажмите кнопку
OK.



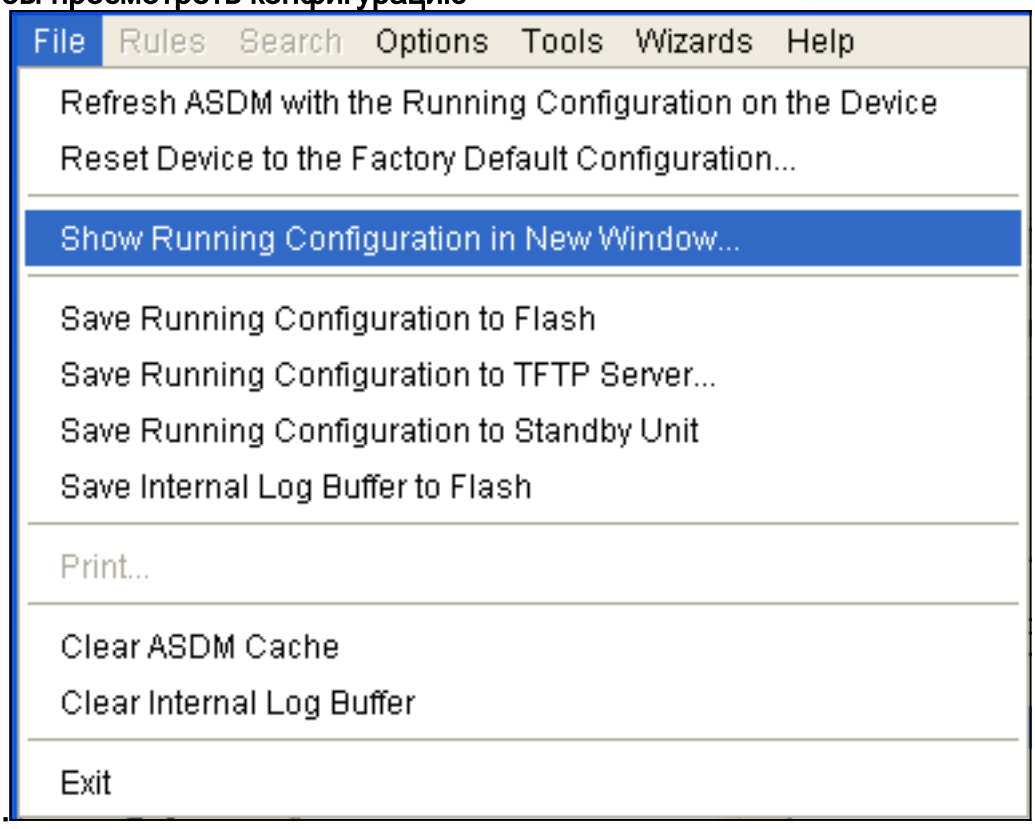
25. Чтобы разрешить трафик UDP на порт 4500 для NAT-T, нажмите кнопку Add. Для продолжения нажмите кнопку
OK.



26. **Чтобы принять конфигурацию интерфейса, нажмите Apply.** При этом конфигурация загружается в
PIX.



27. Настройка завершена.**Выберите File > Show Running Configuration in New Window, чтобы просмотреть конфигурацию CLI.**



[Конфигурация межсетевого экрана PIX]

Сетевой экран PIX

```
pixfirewall# show run : Saved : PIX Version 7.0(0)102
names ! interface Ethernet0 nameif outside security-
level 0 ip address 99.99.99.1 255.255.255.0 ! interface
Ethernet1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 ! enable password
2KFQnbNIdI.2KYOU encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pixfirewall domain-name cisco.com ftp
mode passive access-list outside_access_in remark Access
Rule to Allow ESP traffic access-list outside_access_in
extended permit esp host 99.99.99.2 host 99.99.99.12
access-list outside_access_in remark Access Rule to
allow ISAKMP to host 99.99.99.12 access-list
outside_access_in extended permit udp host 99.99.99.2 eq
isakmp host 99.99.99.12 access-list outside_access_in
remark Access Rule to allow port 4500 (NAT-T) to host
99.99.99.12 access-list outside_access_in extended
permit udp host 99.99.99.2 eq 4500 host 99.99.99.12
pager lines 24 mtu inside 1500 mtu outside 1500 no
failover monitor-interface inside monitor-interface
outside asdm image flash:/asdmfile.50073 no asdm history
enable arp timeout 14400 nat-control global (outside) 1
interface nat (inside) 0 0.0.0.0 0.0.0.0 static
(inside,outside) 99.99.99.12 10.1.1.2 netmask
255.255.255.255 access-group outside_access_in in
interface outside route inside 10.2.2.0 255.255.255.0
10.1.1.2 1 route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00 h323
0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
http server enable http 10.1.1.3 255.255.255.255 inside
no snmp-server location no snmp-server contact snmp-
server enable traps snmp telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map
asa_global_fw_policy class inspection_default inspect
dns maximum-length 512 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 asa_global_fw_policy global
Cryptochecksum:0a12956036ce4e7a97f351cde61fba7e : end
```

Устройство безопасности PIX и MPF (модульная система политик) конфигурация

Вместо списка доступа используйте **команду inspect ipsec-pass-thru** в MPF (Модульная Система политик) для передачи Трафика IPSec через Устройства безопасности PIX/ASA.

Этот контроль настроен для открытия крошечных отверстий для трафика ESP. Все потоки данных ESP разрешены, когда прямой поток существует, и нет никакого предела на максимальном числе соединений, которые могут быть позволены. AH не разрешен. Время простоя по умолчанию для потоков данных ESP набором по умолчанию к 10 минутам. Этот контроль может быть применен во всех местоположениях, что другие проверки могут быть применены, который включает командные режимы соответствия и класс. IPSec Проходит через контроль приложения, предоставляет удобный обход ESP (Протокол "IP" 50) трафик, привязанный к соединению порта 500 UDP IKE. Это избегает длинной конфигурации списка доступа для разрешения трафика ESP и также предоставляет безопасности таймаут и Max.

соединения. Используйте **class-map**, **policy-map** и **команды service-policy** для определения класса трафика, чтобы применить команду inspect к классу и применить политику к одному или более интерфейсам. Когда включено, **команда inspect IPSec-pass-thru** позволяет неограниченный трафик ESP с таймаутом 10 минут, который не конфигурируем. NAT и нетрафик NAT разрешены.

```
hostname(config)#access-list test-udp-acl extended permit udp any any eq 500
hostname(config)#class-map test-udp-class hostname(config-cmap)#match access-list test-udp-acl
hostname(config)#policy-map test-udp-policy hostname(config-pmap)#class test-udp-class
hostname(config-pmap-c)#inspect ipsec-pass-thru hostname(config)#service-policy test-udp-policy
interface outside
```

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

- **команда show crypto ipsec sa – отображает связи безопасности, соответствующие второму этапу.**
- **команда show crypto isakmp sa вЂ отображает сопоставления безопасности, соответствующие первому этапу.**
- **show crypto engine connections active – отображает зашифрованные и расшифрованные пакеты.**

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды поиска и устранения неисправностей для маршрутизатора IPsec

Примечание: Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.

- **debug crypto engine– показывает зашифрованный трафик.**
- **debug crypto ipsec – отображает согласования IPSec на Этапе 2.**
- **debug crypto isakmp** согласования Протокола ISAKMP фазы 1.

Очистка сопоставлений безопасности

- **clear crypto isakmp – удаляет связи безопасности политики обмена ключами в Интернете (IKE).**
- **clear crypto ipsec sa – удаление сопоставлений безопасности IPSec.**

Команды поиска и устранения неисправностей для PIX

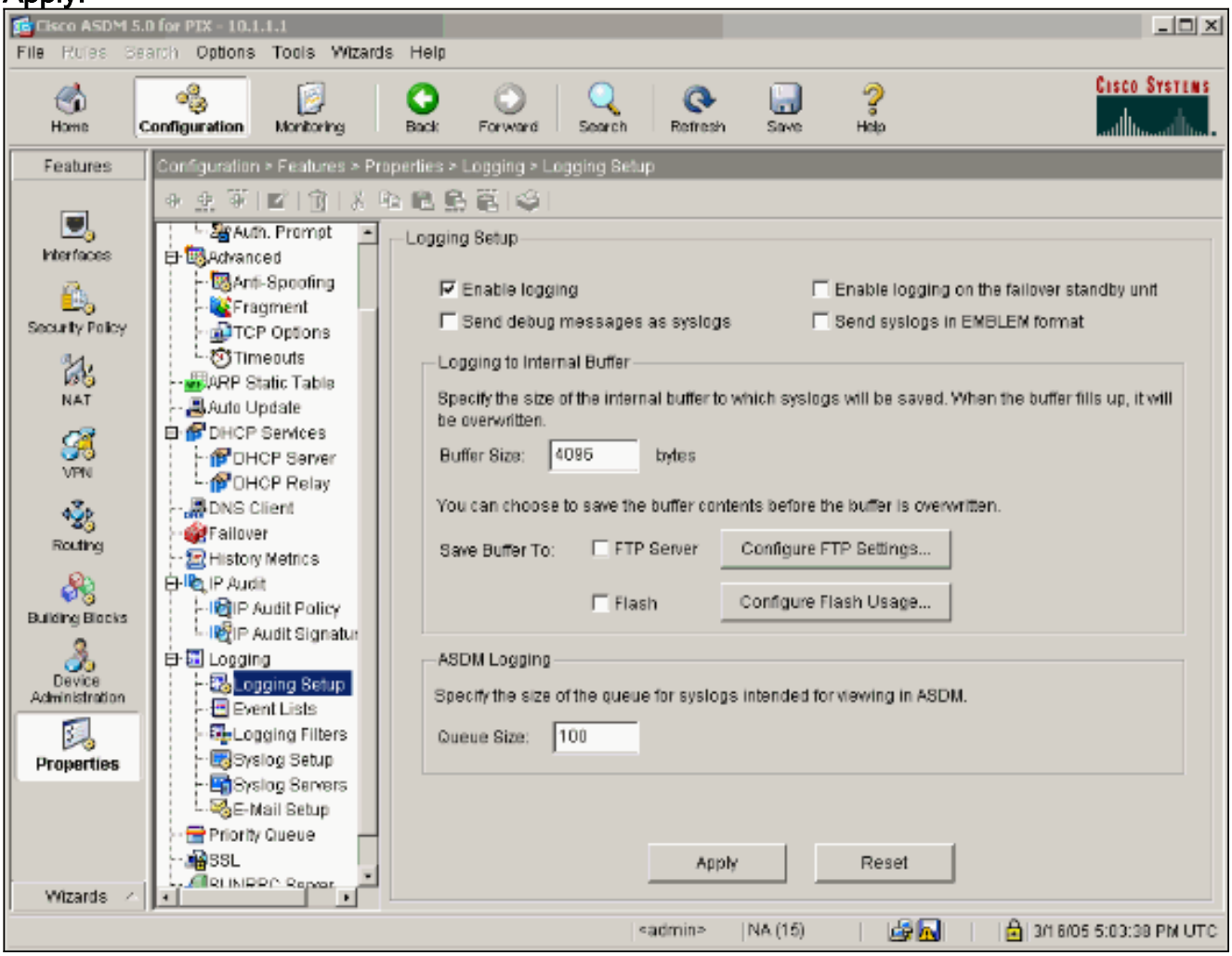
Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику

выходных данных команды show.

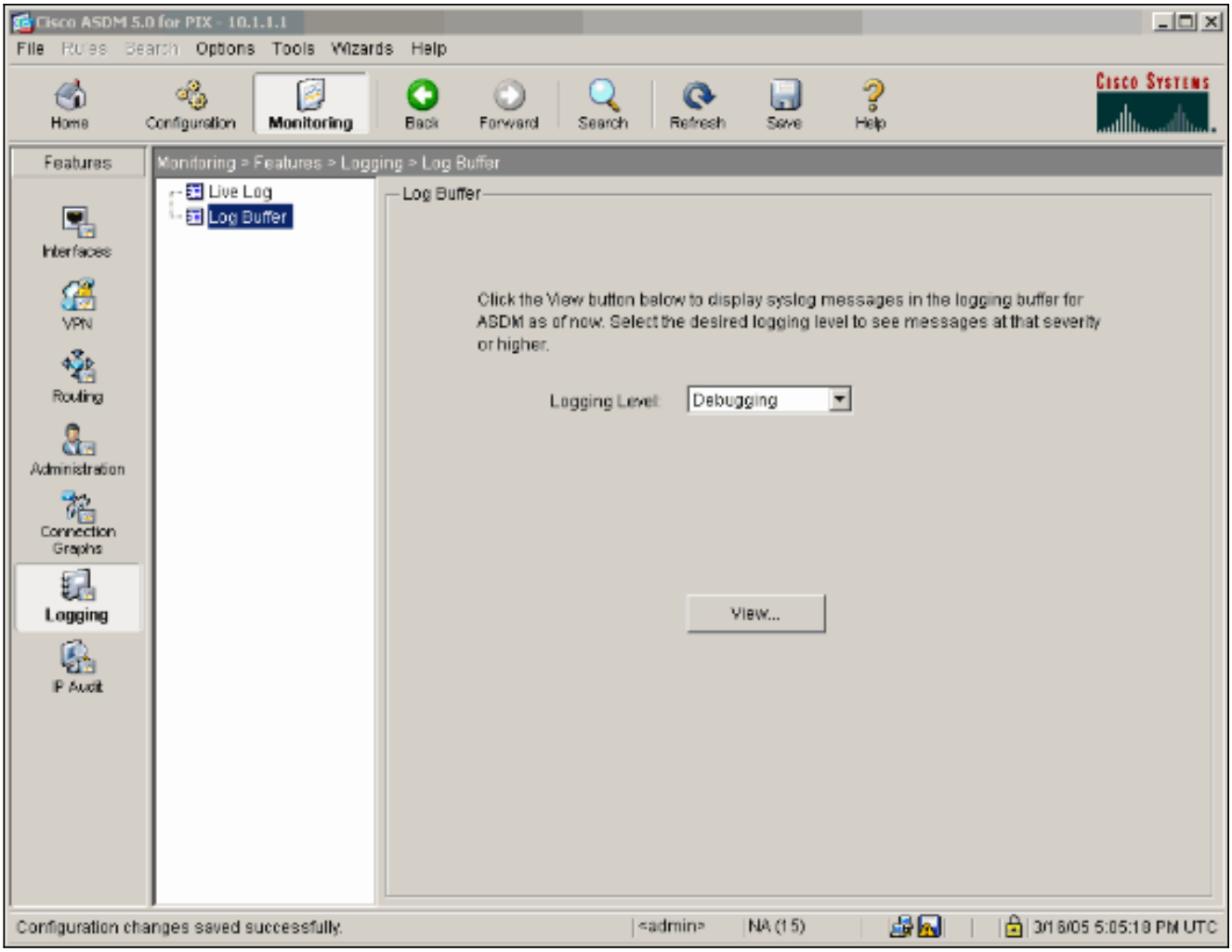
Примечание: [Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.]

- **logging buffer debugging Показывает устанавливаемые соединения с хостами и отказы в соединениях с хостами через PIX. Эти сведения хранятся в буфере журнала PIX, и выходные данные можно просмотреть при помощи команды show log.**
- Для включения регистрации, а также для просмотра журналов можно использовать ASDM.

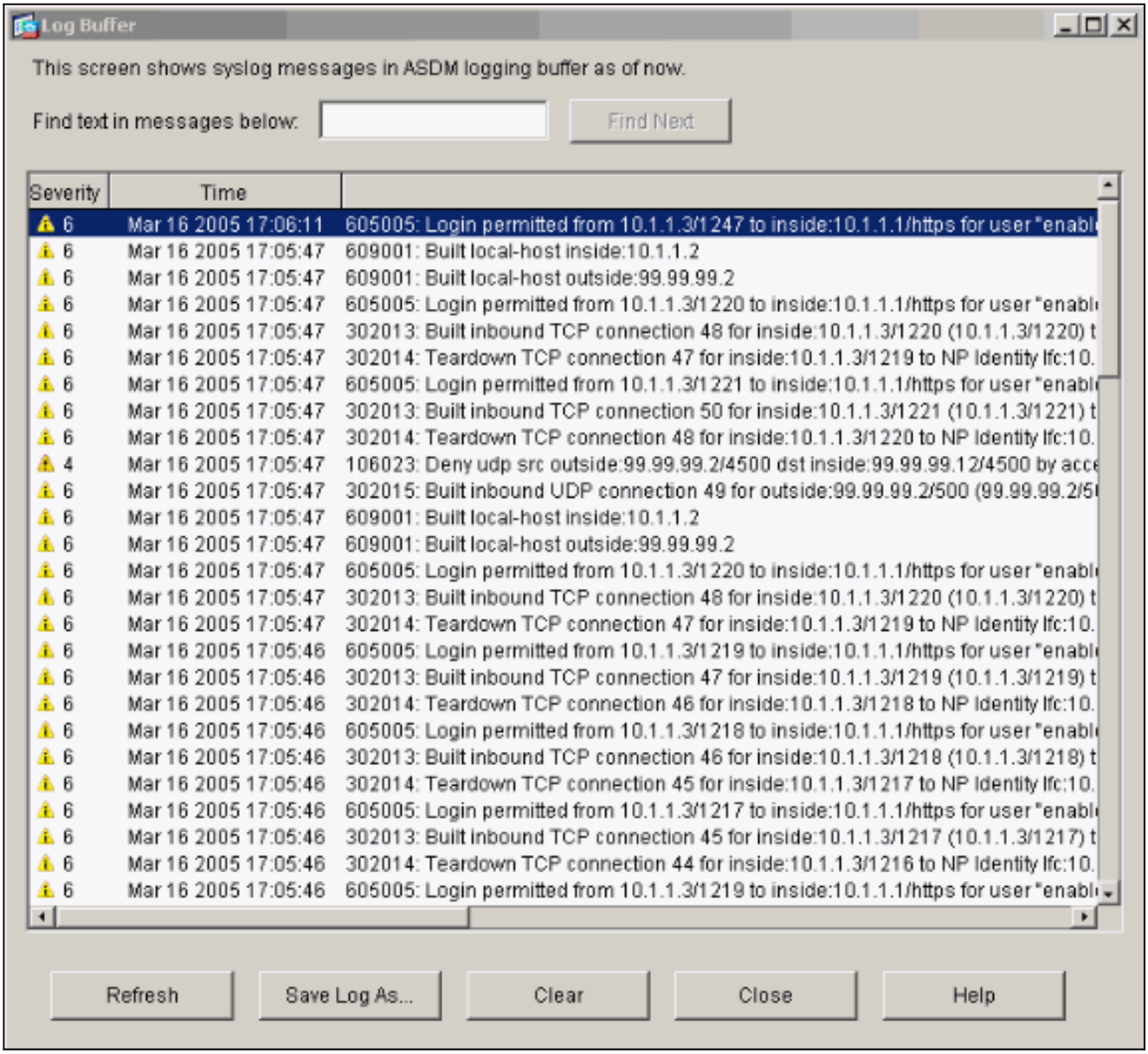
1. Выберите **Configuration> Properties> Logging> Logging Setup> Enable Logging** и затем нажмите
   Apply.



2. Выберите **Monitoring> Logging> Log Buffer> On Logging Level> Logging Buffer**, затем нажмите
   View.



Ниже приведен пример буфера журнала.



Дополнительные сведения

- Страница технической поддержки протоколов согласования IPSec и IKE
- Страница поддержки PIX
- Справочник по командам PIX
- Страница поддержки NAT
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация