PIX/ASA 7.x и более поздние: Пример конфигурации подключения нескольких внутренних сетей к Интернету

Содержание

Введение

В этом документе приводится пример конфигурации для Устройства защиты PIX/ASA версии 7.x и выше с несколькими внутренними сетями, которые соединяются с Интернетом (или внешней сетью). Настройка выполняется в интерфейсе командной строки (CLI) или диспетчере устройств адаптивной защиты (ASDM) 5.x и выше.

См. Устанавливают и Подключение Устранения неполадок через Cisco Security Appliance для получения информации о том, как установить и устранить неполадки подключения через PIX/ASA.

См. Использование nat, глобального, статичного, conduit, и команды access-list и Перенаправление порта (Передача) на PIX для получения информации об общих командах PIX.

Примечание: Некоторые опции в других версиях ASDM могут казаться отличающимися от опций в ASDM 5.1. Дополнительные сведения см. в документации по ASDM.

Предварительные условия

Требования

При добавлении более одной внутренней сети, которые находятся за брандмауэром PIX, необходимо помнить следующее:

- PIX не поддерживает вторичную адресацию.
- За PIX необходимо использовать маршрутизатор, который будет обеспечивать маршрутизацию между имеющейся сетью и вновь добавляемой сетью.
- Шлюзом по умолчанию для всех узлов должен быть внутренний маршрутизатор.
- На внутреннем маршрутизаторе добавьте маршрут по умолчанию, который указывает на PIX.
- Удалите кэш протокола разрешения адресов (ARP) на внутреннем маршрутизаторе.

Устройству необходимо разрешить настройку посредством ASDM, как описано в разделе Разрешение доступа по HTTPS для ASDM.

Используемые компоненты

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

- PIX Security Appliance 515E с ПО версии 7.1
- ASDM 5.1
- Маршрутизаторы Cisco с программным обеспечением Cisco IOS® Release 12.3(7)T

Примечание: Этот документ повторно сертифицировался с версией программного обеспечения 8.x PIX/ASA и Cisco IOS Software Release 12.4.

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 с версией 7.x Устройства безопасности Cisco ASA и позже.

Условные обозначения

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

Настройка

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

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных

пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

Общие сведения

В этом сценарии существует три внутренних сети (10.1.1.0/24, 10.2.1.0/24 и 10.3.1.0/24), чтобы быть связанными с Интернетом (или Внешняя сеть) через PIX. Внутренние сети связаны с внутренним интерфейсом PIX. Интернет-соединение через маршрутизатор, который связан с внешним интерфейсом PIX. PIX Имеет IP-адрес 172.16.1.1/24.

Статические маршруты используются для маршрутизации пакетов от внутренних сетей до Интернета и наоборот. Вместо того, чтобы использовать статические маршруты, можно также использовать протокол динамической маршрутизации, такой как Протокол RIP или Протокол OSPF.

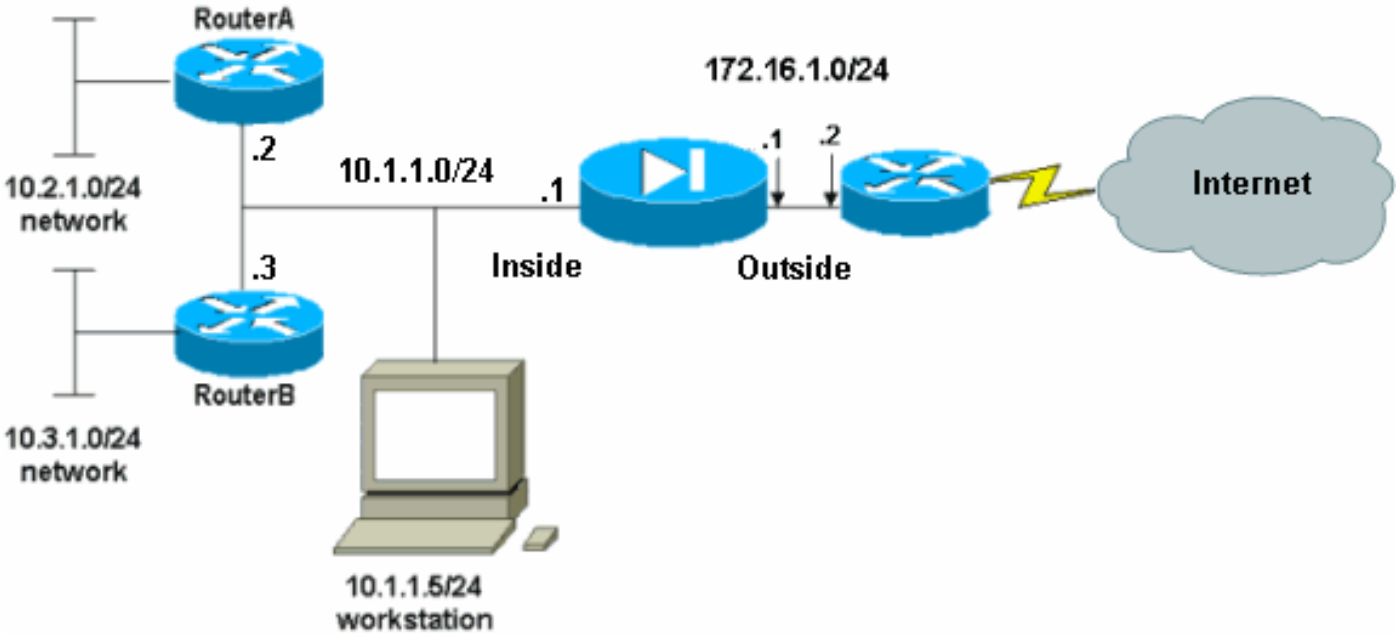
Внутренние хосты связываются с Интернетом путем перевода внутренних сетей на PIX с помощью динамического NAT (пул IP-адресов - 172.16.1.5 к 172.16.1.10). Если пул IP-адресов будет исчерпан, то PIX будет PAT (использующий IP-адрес 172.16.1.4) внутренние хосты для достижения Интернета.

См. PIX/ASA 7.x NAT и Операторы PAT для получения дополнительной информации о NAT/PAT.

Примечание: Если статическое NAT использование внешний IP (global_IP) адрес для перевода, то это могло бы вызвать трансляцию. По этой причине вместо IP-адреса в статическом преобразовании следует указывать ключевое слово interface.

Схема сети

В настоящем документе используется следующая схема сети:



Шлюз по умолчанию для узлов сети 10.1.1.0 указывает на маршрутизатор RouterA. В маршрутизаторе RouterB добавлен маршрут по умолчанию, который указывает на RouterA. У маршрутизатора A имеется маршрут по умолчанию, который указывает на блок расширения параллельного интерфейса (PIX) внутри интерфейса.

Конфигурации

Эти конфигурации используются в данном документе:

- Конфигурация RouterA
- Конфигурация маршрутизатора B
- Конфигурация PIX Security Appliance 7.1Конфигурация PIX с помощью ASDMНастройка PIX Security Appliance посредством интерфейса командной строки

Конфигурация RouterA

```
RouterA#show running-config Building configuration...
Current configuration : 1151 bytes ! version 12.4
service config service timestamps debug uptime service
timestamps log uptime no service password-encryption !
hostname RouterA ! interface Ethernet2/0 ip address
10.2.1.1 255.255.255.0 half-duplex ! interface
Ethernet2/1 ip address 10.1.1.2 255.255.255.0 half-
duplex ! ip classless ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3 ! ! line con 0
line aux 0 line vty 0 4 ! end RouterA#
```

Конфигурация маршрутизатора B

```
RouterB#show running-config Building configuration...
Current configuration : 1132 bytes ! version 12.4
service config service timestamps debug datetime msec
service timestamps log datetime msec no service
password-encryption ! hostname RouterB ! interface
FastEthernet0/0 ip address 10.1.1.3 255.255.255.0 speed
auto ! interface Ethernet1/0 ip address 10.3.1.1
255.255.255.0 half-duplex ! ip classless ip route
0.0.0.0 0.0.0.0 10.1.1.2 ! control-plane ! ! line con 0
line aux 0 line vty 0 4 ! end RouterB#
```

Если для настройки PIX Security Appliance необходимо использовать ASDM, но начальная загрузка устройства не произведена, выполните следующие действия:

1. Войдите в консоль PIX.
2. Из очищенной конфигурации используйте интерактивные запросы, позволяющие включить ASDM для управления PIX с рабочей станции 10.1.1.5.

Конфигурация PIX Security Appliance 7.1

```
Pre-configure Firewall now through interactive prompts
[yes]? yes
Firewall Mode [Routed]:
Enable password [<use current password>]: cisco
Allow password recovery [yes]?
Clock (UTC):
  Year [2005]:
  Month [Mar]:
  Day [15]:
  Time [05:40:35]: 14:45:00
```

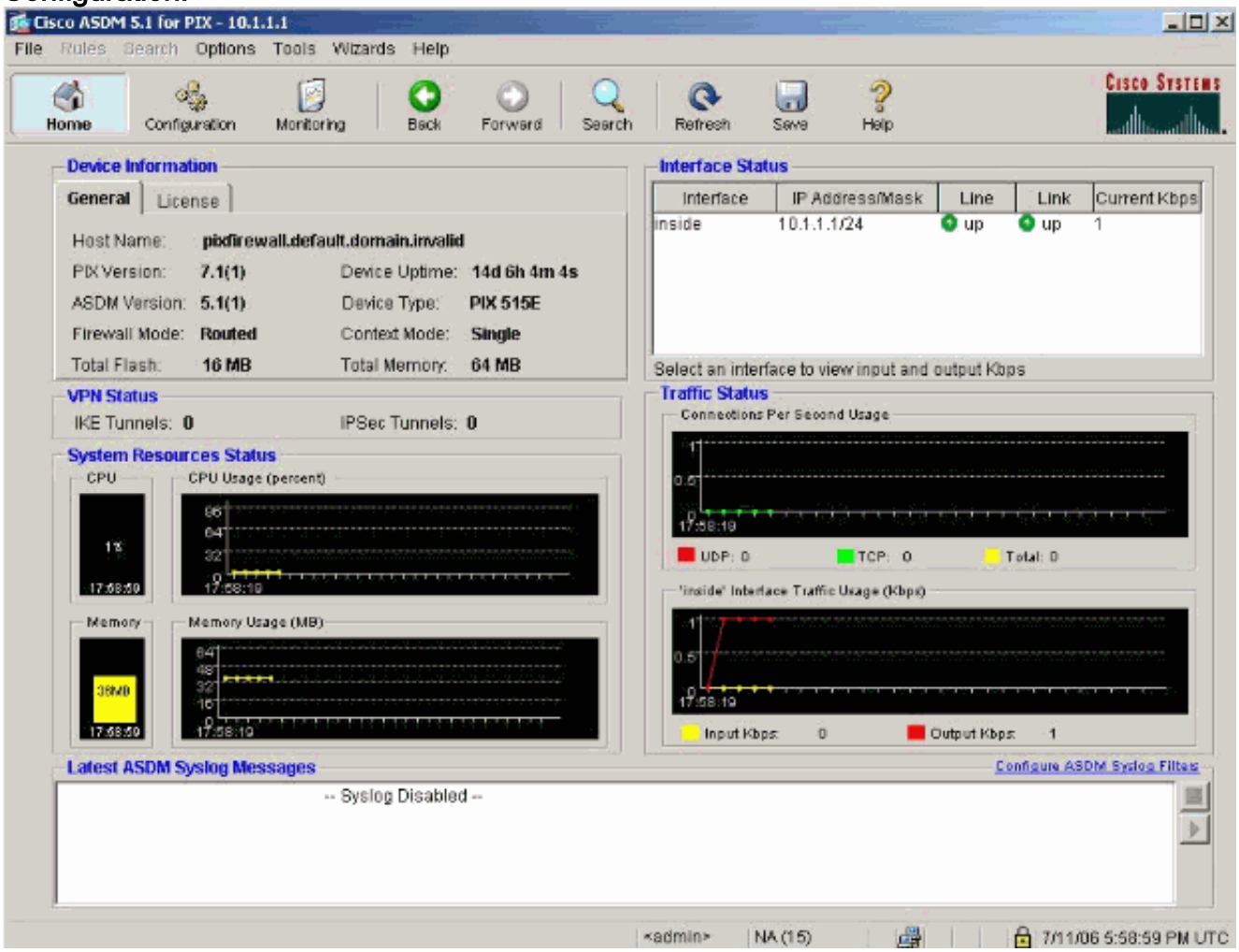
```
Inside IP address: 10.1.1.1
Inside network mask: 255.255.255.0
Host name: OZ-PIX
Domain name: cisco.com
IP address of host running Device Manager: 10.1.1.5

The following configuration will be used:
         Enable password: cisco
         Allow password recovery: yes
         Clock (UTC): 14:45:00 Mar 15 2005
         Firewall Mode: Routed
         Inside IP address: 10.1.1.1
         Inside network mask: 255.255.255.0
         Host name: OZ-PIX
         Domain name: cisco.com
         IP address of host running Device Manager:
10.1.1.5

Use this configuration and write to flash? yes
         INFO: Security level for "inside" set to 100 by
default.
         Cryptochecksum: a0bff9bb aa3d815f c9fd269a
3f67fef5

965 bytes copied in 0.880 secs
         INFO: converting 'fixup protocol dns maximum-
length 512' to MPF commands
         INFO: converting 'fixup protocol ftp 21' to MPF
commands
         INFO: converting 'fixup protocol h323_h225
1720' to MPF commands
         INFO: converting 'fixup protocol h323_ras 1718-
1719' to MPF commands
         INFO: converting 'fixup protocol netbios 137-
138' to MPF commands
         INFO: converting 'fixup protocol rsh 514' to
MPF commands
         INFO: converting 'fixup protocol rtsp 554' to
MPF commands
         INFO: converting 'fixup protocol sip 5060' to
MPF commands
         INFO: converting 'fixup protocol skinny 2000'
to MPF commands
         INFO: converting 'fixup protocol smtp 25' to
MPF commands
         INFO: converting 'fixup protocol sqlnet 1521'
to MPF commands
         INFO: converting 'fixup protocol sunrpc_udp
111' to MPF commands
         INFO: converting 'fixup protocol tftp 69' to
MPF commands
         INFO: converting 'fixup protocol sip udp 5060'
to MPF commands
         INFO: converting 'fixup protocol xdmcp 177' to
MPF commands

Type help or '?' for a list of available commands.
         OZ-PIX>
```

Конфигурация PIX с помощью ASDM

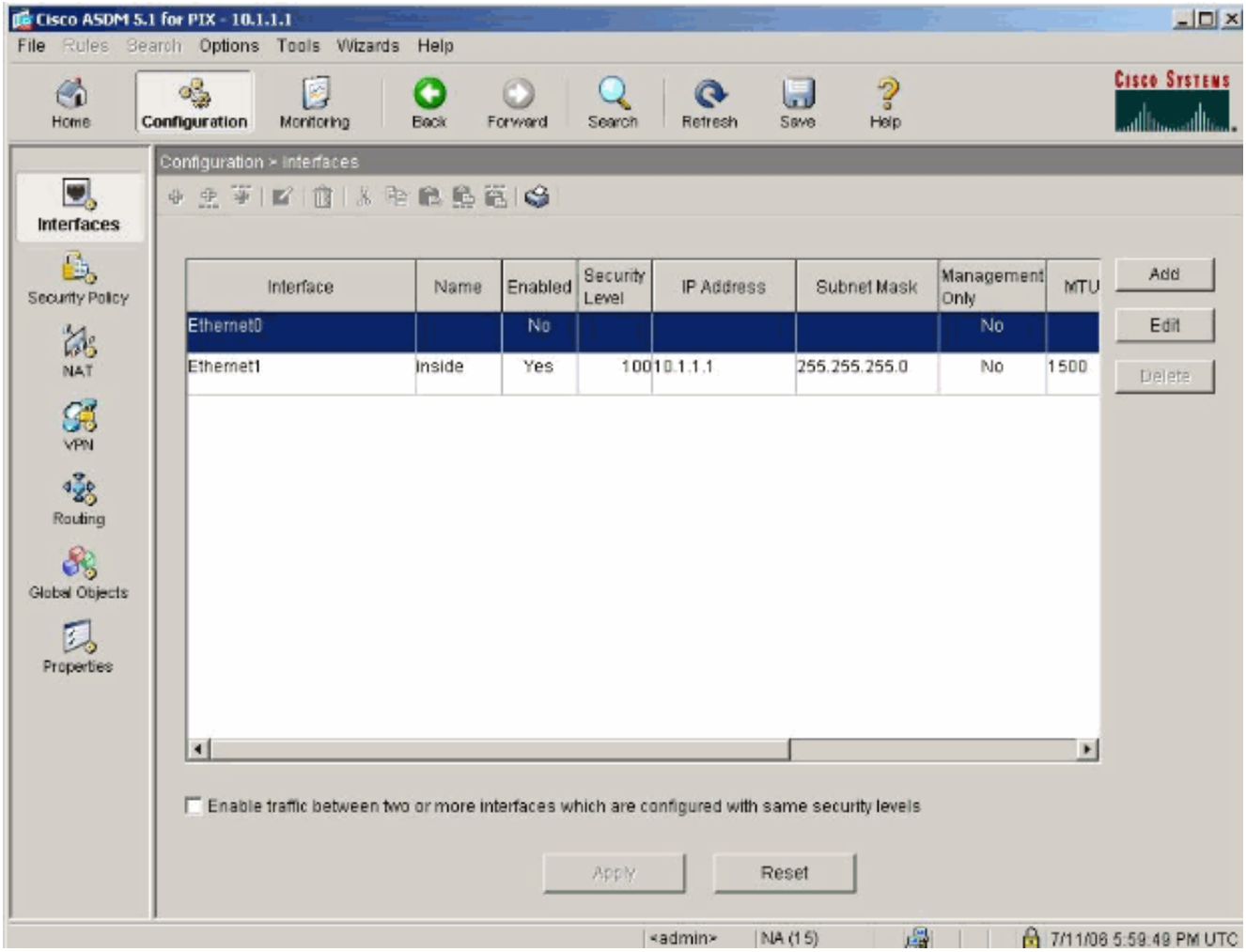
Для настройки при помощи графического интерфейса пользователя ASDM выполните

следующие действия:

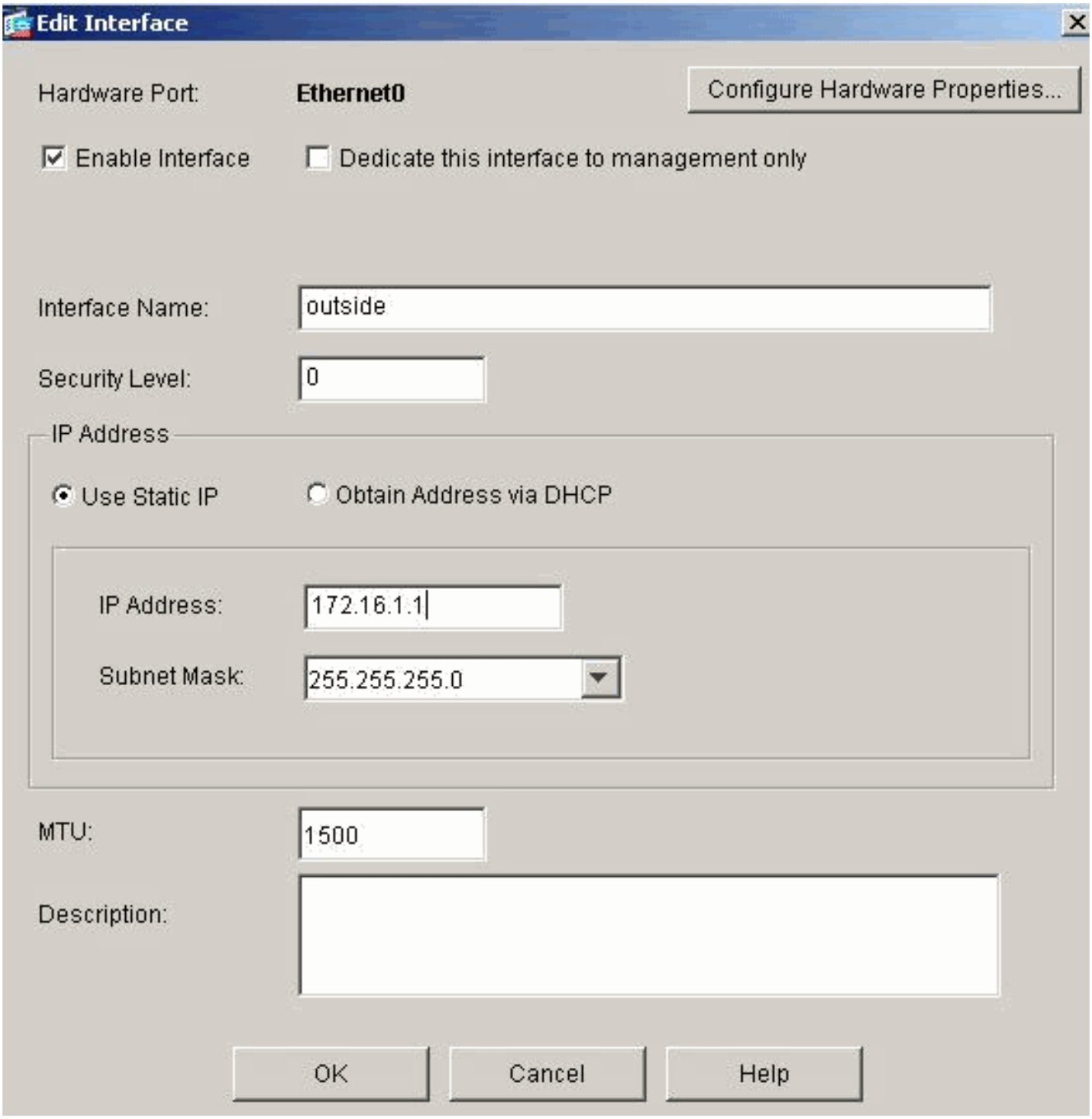
1. На рабочей станции 10.1.1.5 откройте веб-браузер, чтобы воспользоваться ADSM (в данном примере https://10.1.1.1).
2. **В запросах сертификата нажмите Yes.**
3. Войдите с настроенным ранее паролем режима включения.
4. Если это первый запуск ASDM на ПК, будет выдан запрос на использование ASDM Launcher или использование ASDM в качестве Java-приложения. В данном примере выбирается и устанавливается ASDM Launcher.
5. **Перейдите на страницу Home ASDM и нажмите кнопку Configuration.**



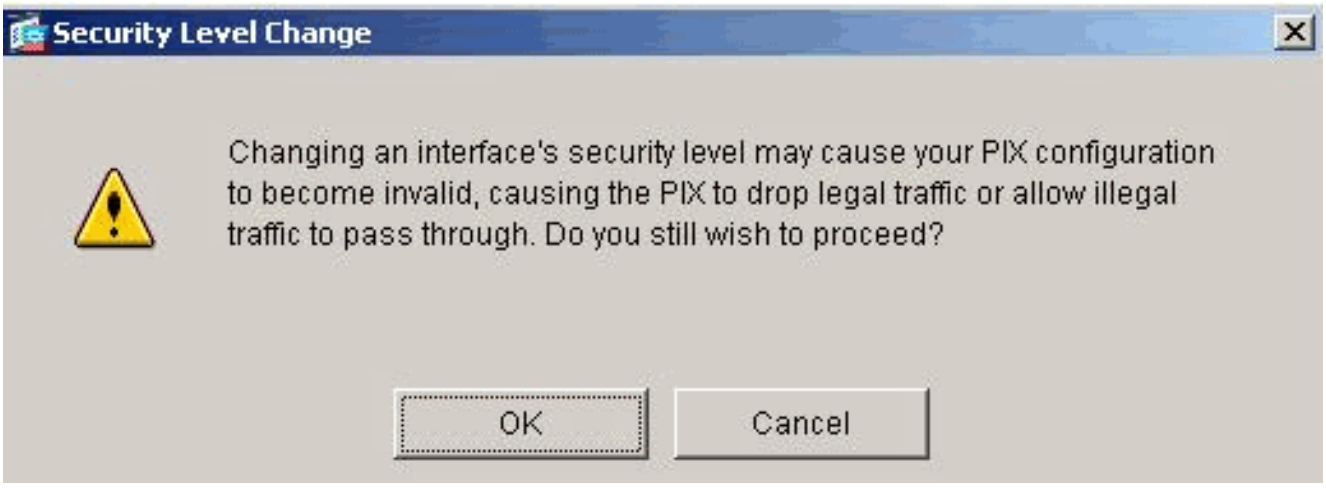
6. **Чтобы настроить внешний интерфейс, выберите Interface > Edit.**



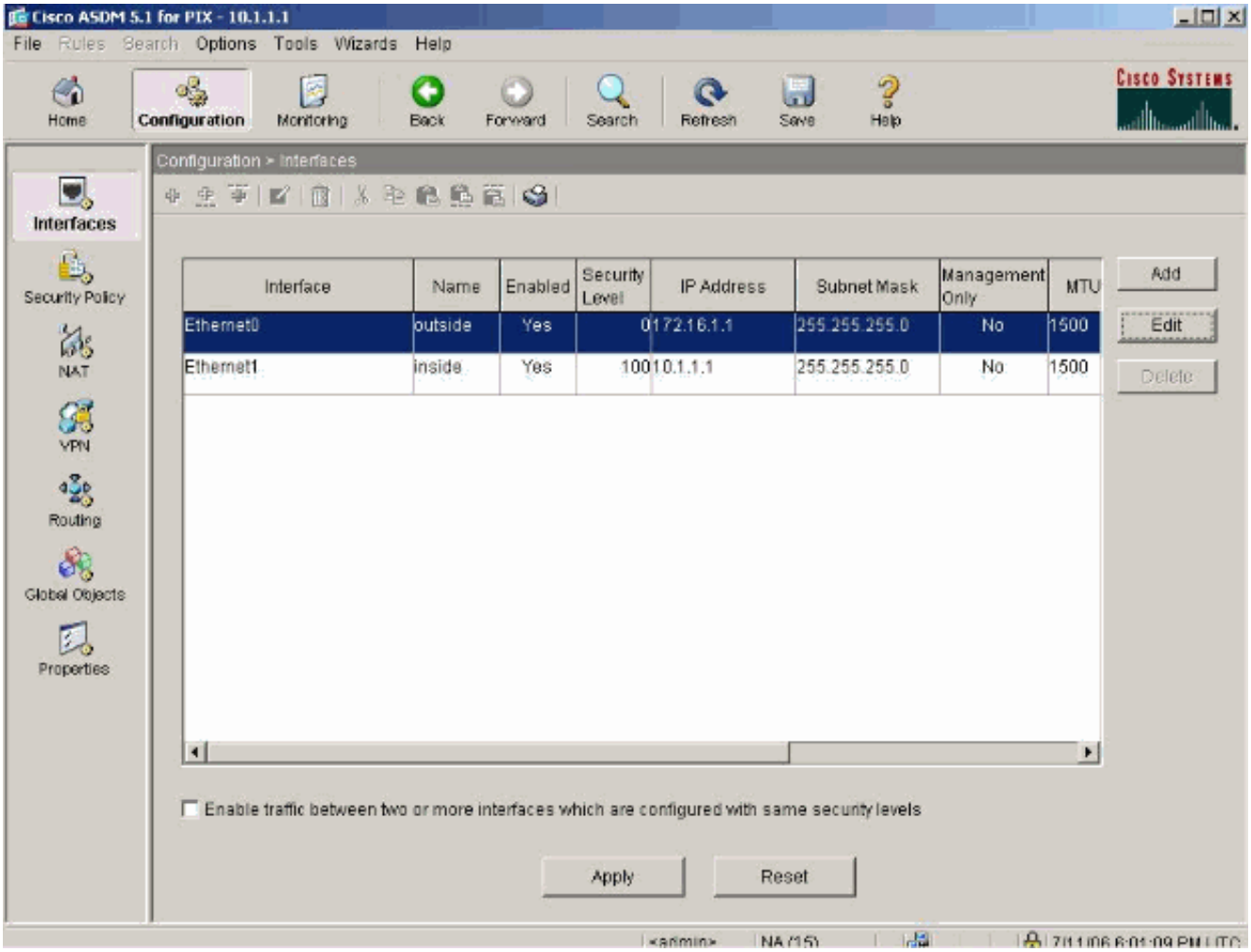
7. Введите все данные интерфейса и после завершения нажмите кнопку OK.



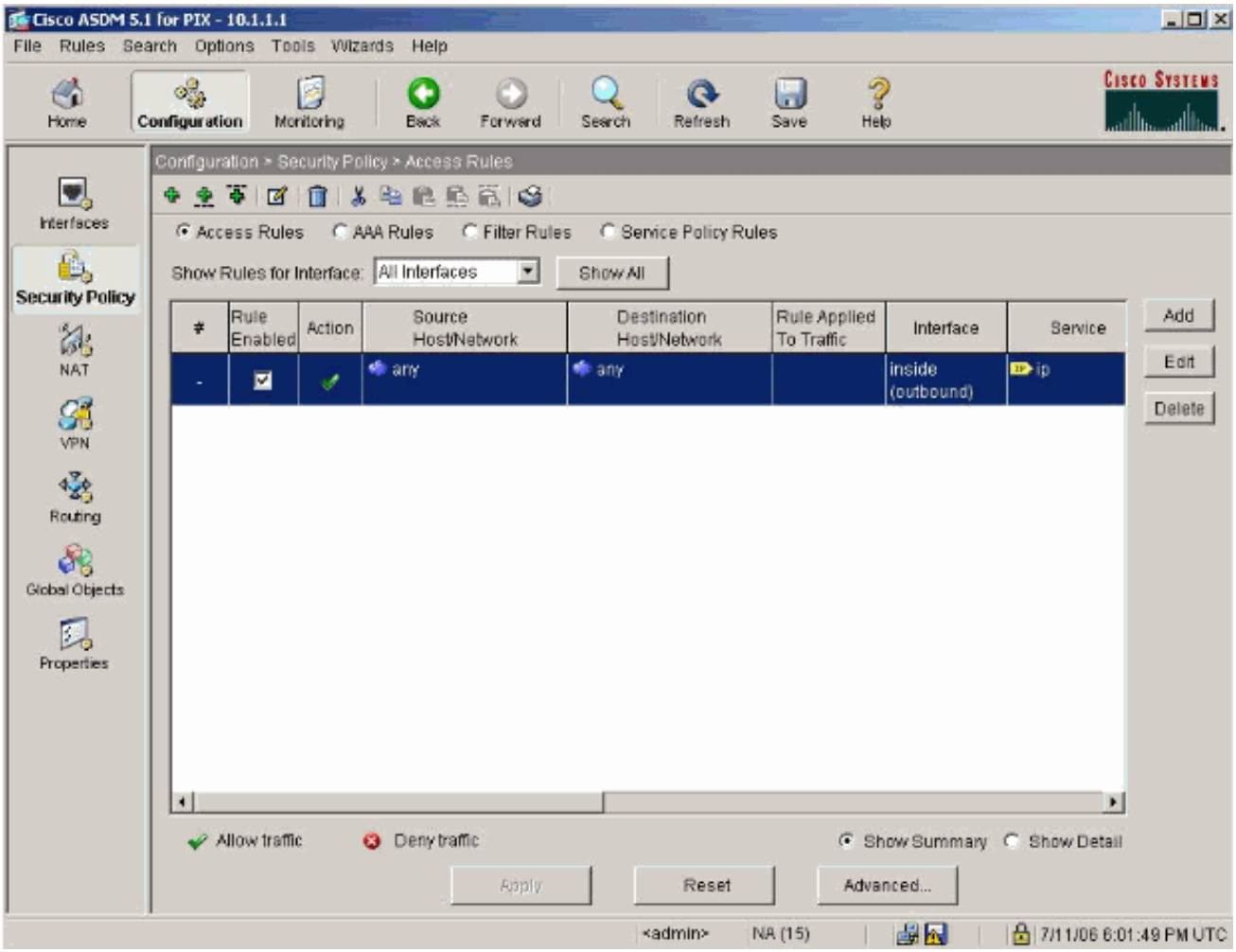
8. **В диалоговом окне Security Level Change нажмите кнопку OK.**



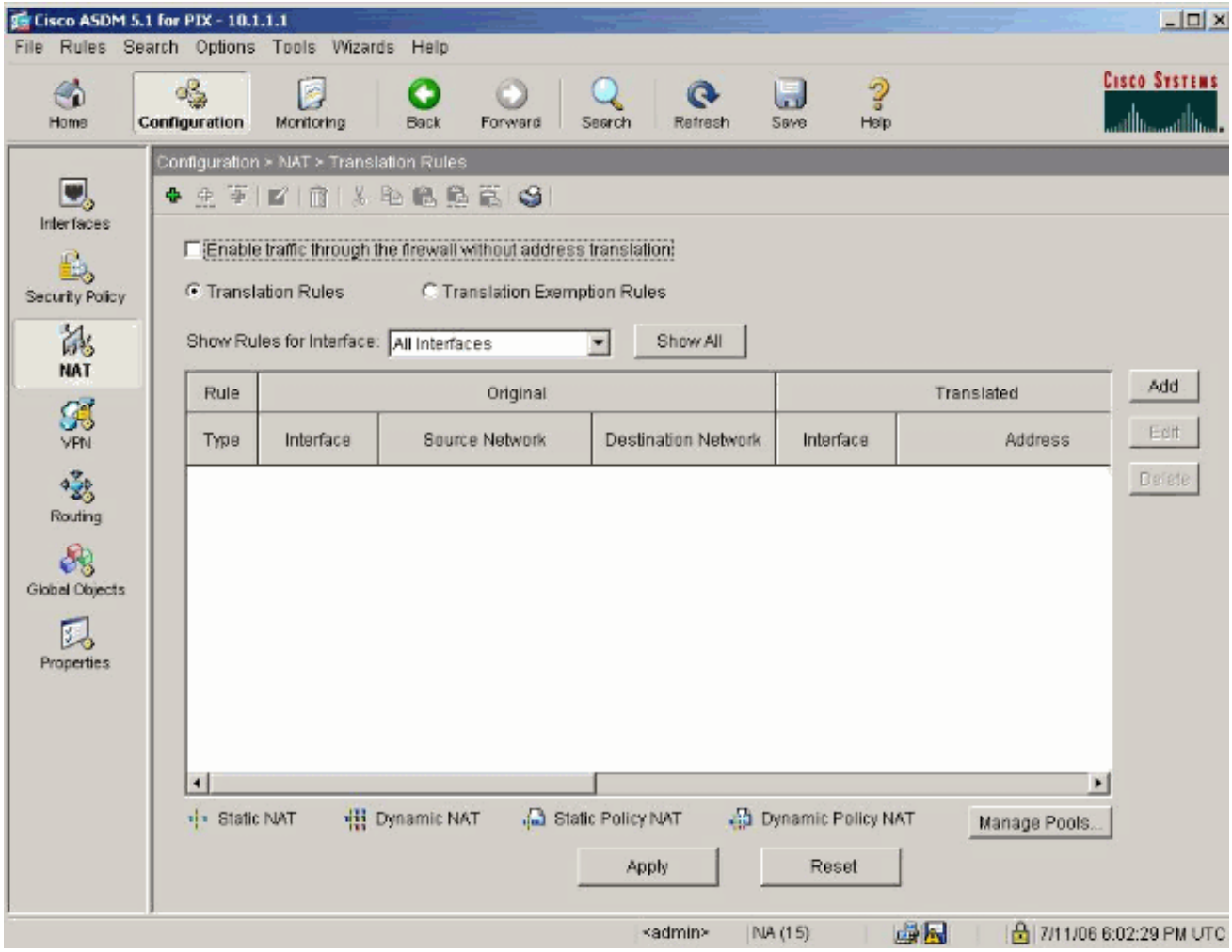
9. **Чтобы сохранить конфигурацию интерфейса, нажмите кнопку Apply.** При этом конфигурация загружается в PIX.



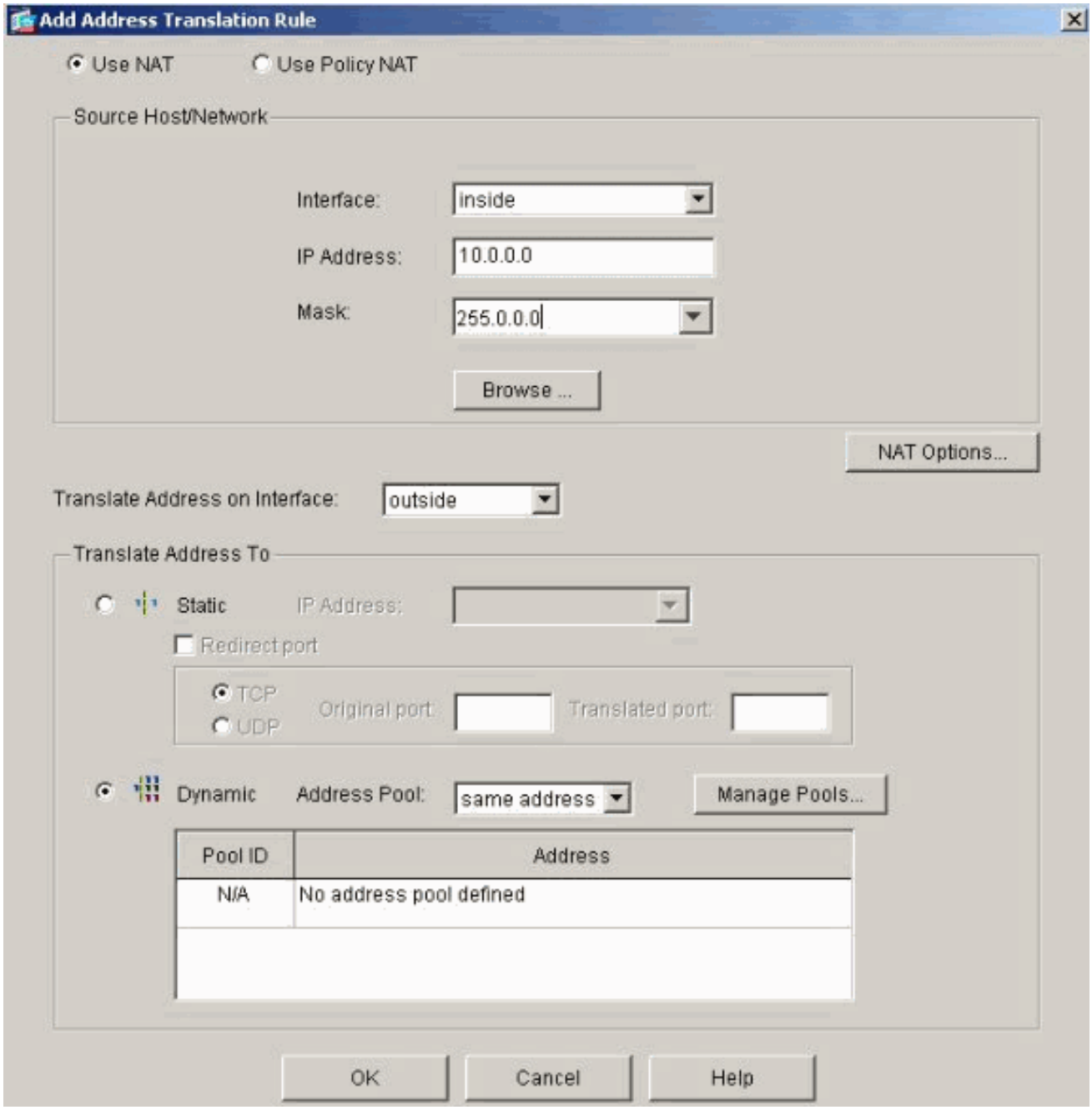
10. **Во вкладке Features выберите Security Policy, чтобы просмотреть используемое правило политики безопасности.** В данном примере используется внутреннее правило по
умолчанию.



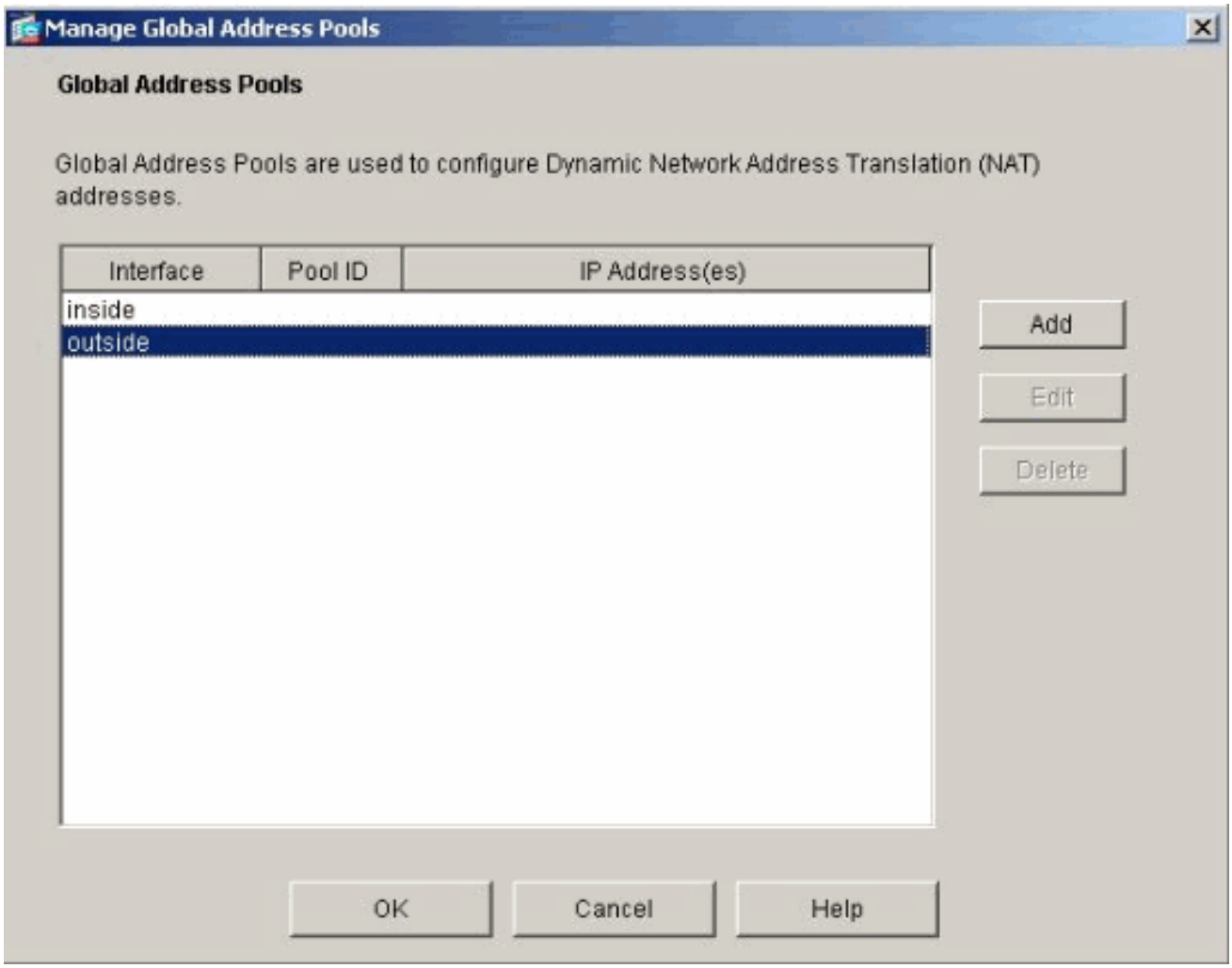
11. В данном примере используется NAT. Анчек **Разрешать трафик через межсетевой экран без** флажка **переадресации** и **нажмите Add** для настройки правила NAT.



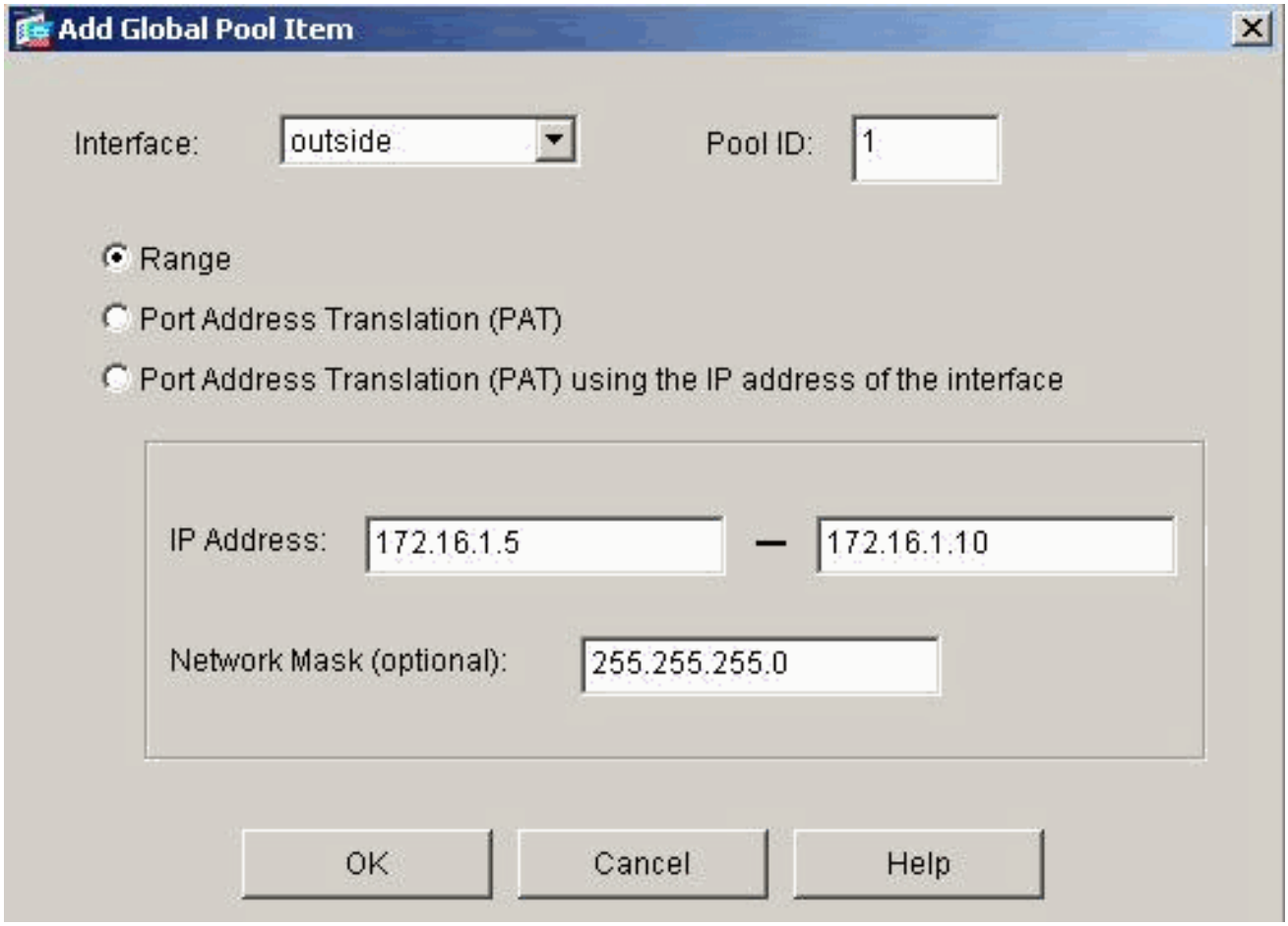
12. Настройте исходную сеть. В данном примере в качестве IP-адреса используется 10.0.0.0, а в качестве маски используется 255.0.0.0.**Чтобы задать пул адресов NAT, щелкните Manage Pools (Управление пулами).**



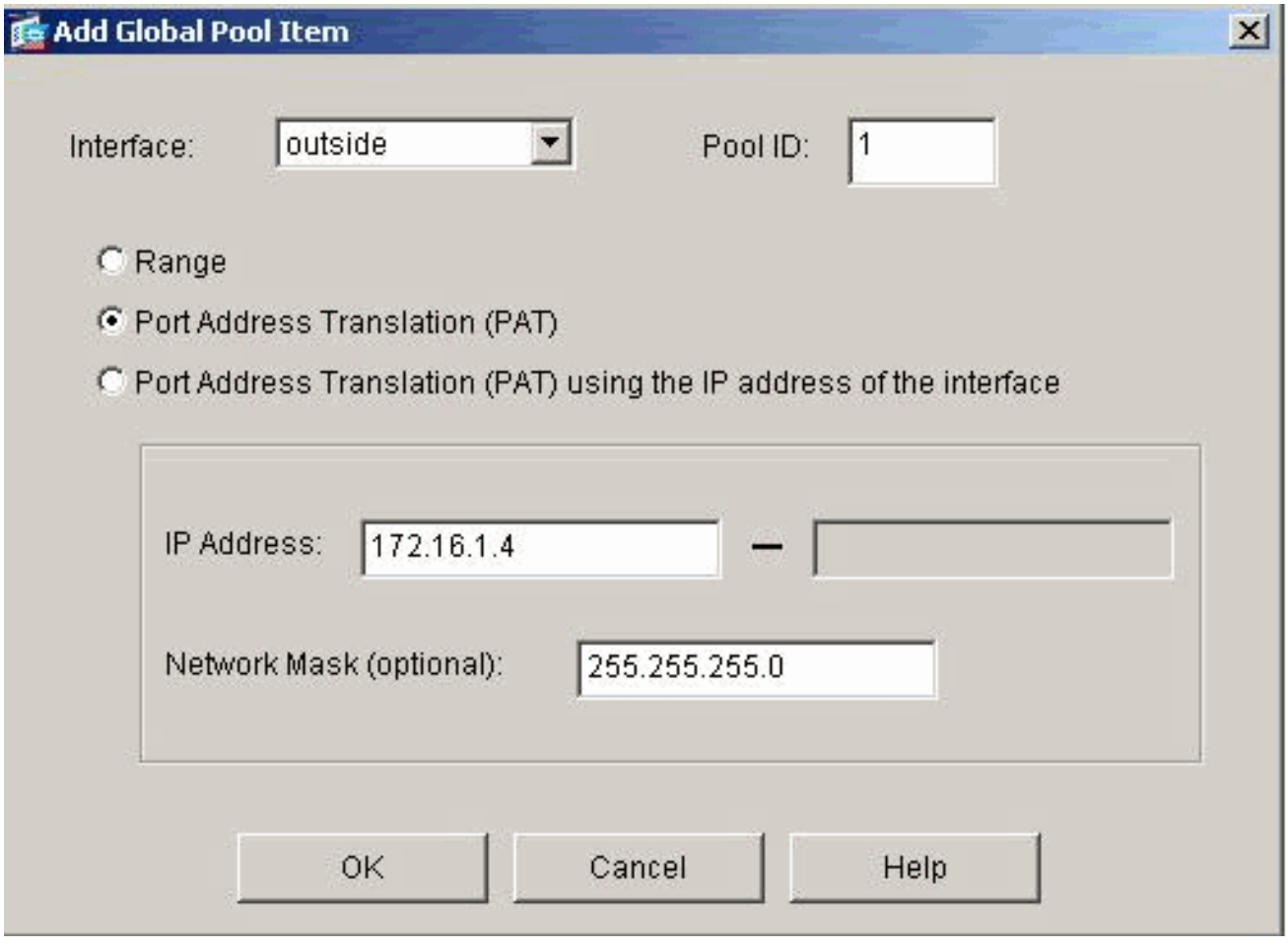
13. **Выберите outside интерфейс и нажмите Add.**



14. В данном примере настраиваются пулы адресов Range и PAT. **Настройте диапазон пула адресов NAT и нажмите кнопку OK.**

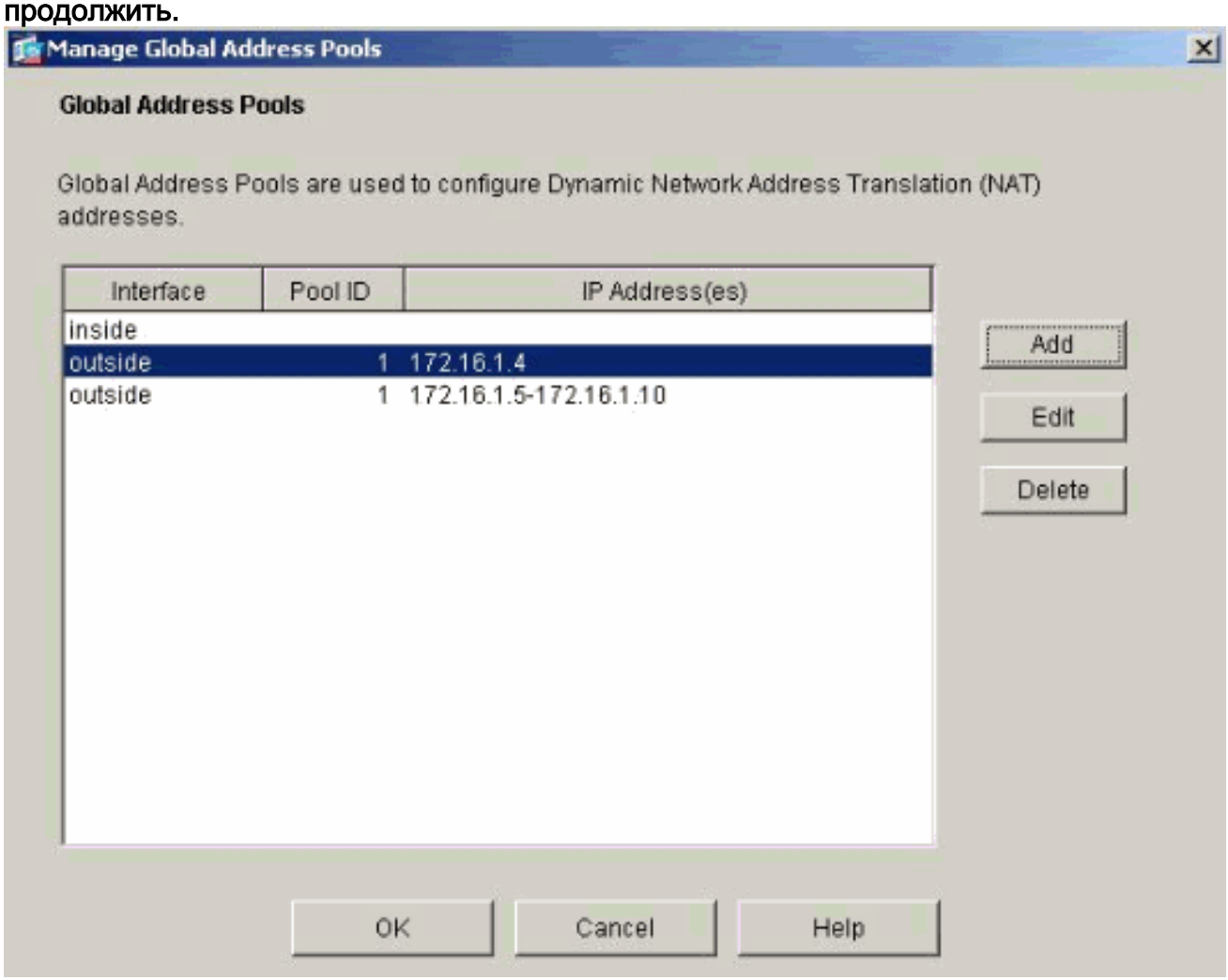


15. Чтобы настроить адрес PAT, выберите внешний интерфейс шага 13. **Нажмите кнопку ОК**

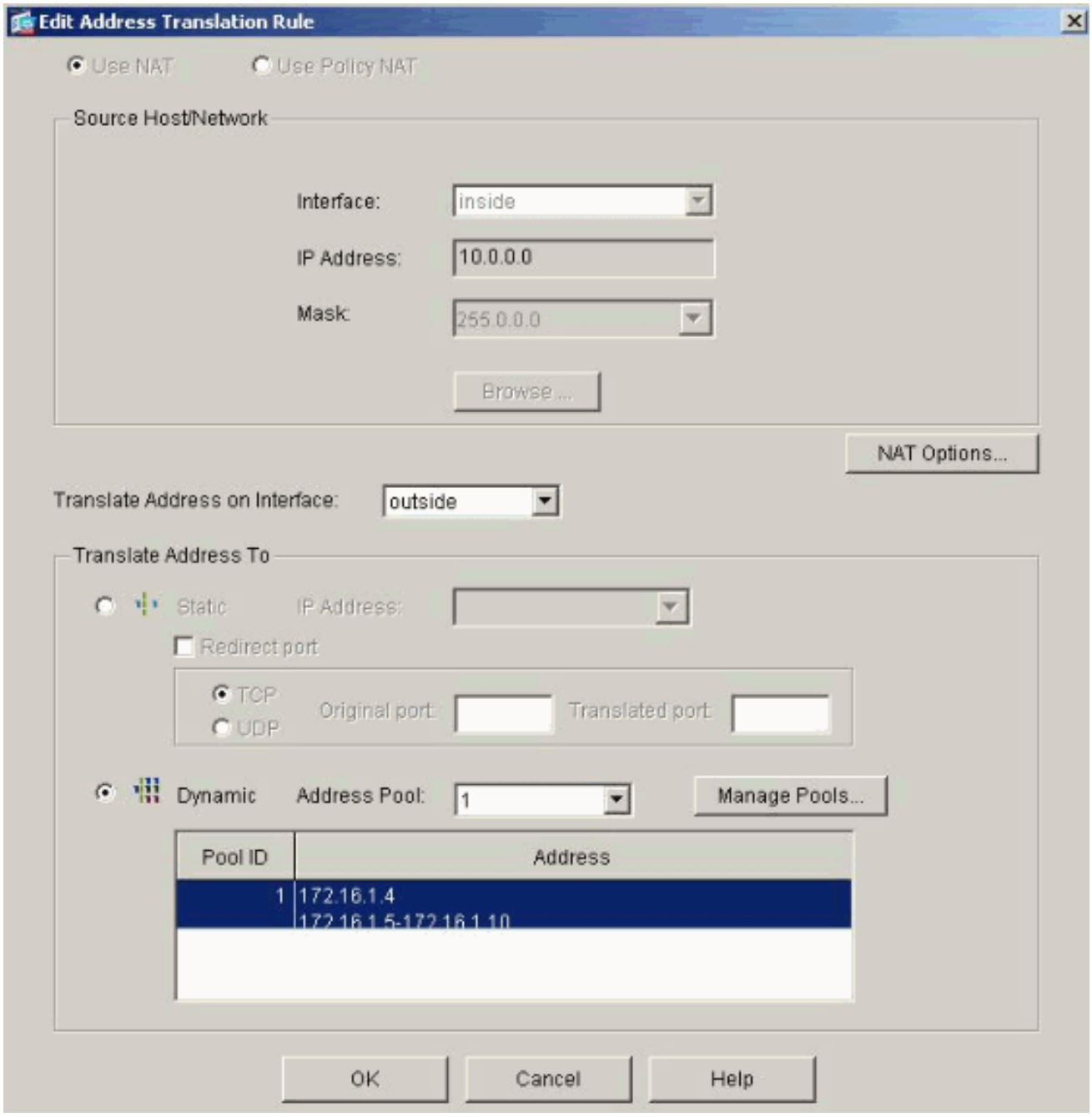


Нажмите OK, чтобы

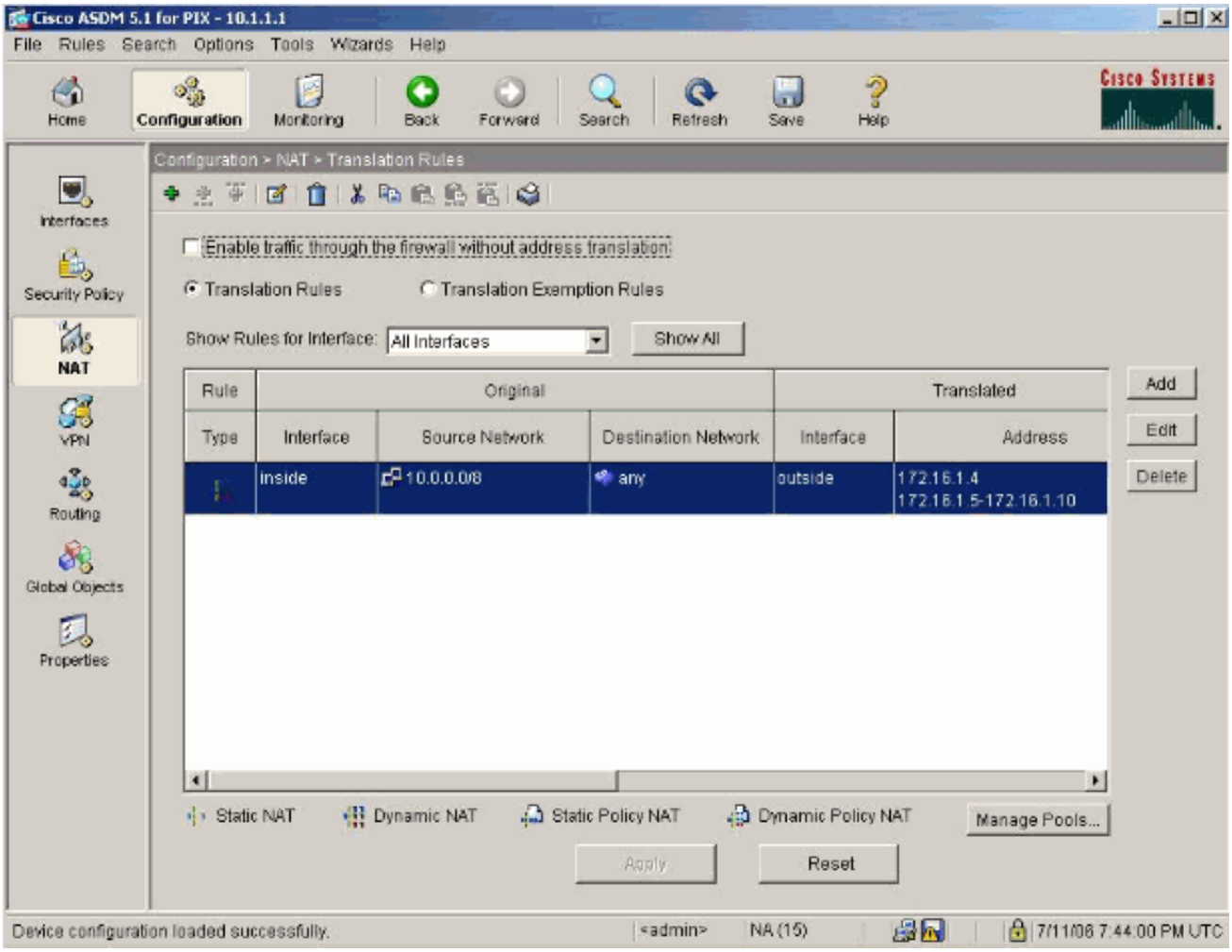
продолжить.



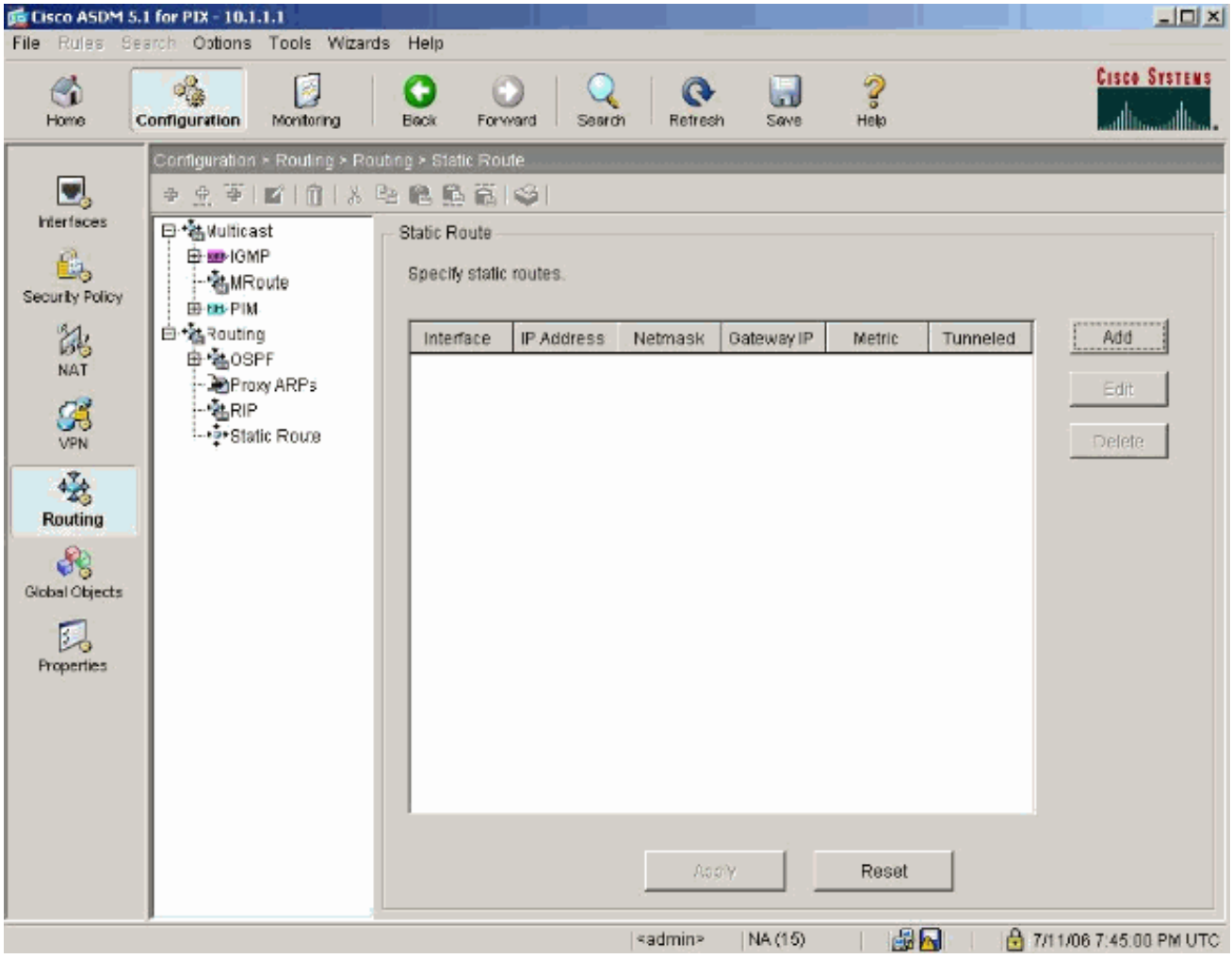
16. В окне Edit Address Translation Rule выберите идентификатор пула Pool ID, который будет использоваться настроенной сетью-источником. **Нажмите кнопку ОК.**



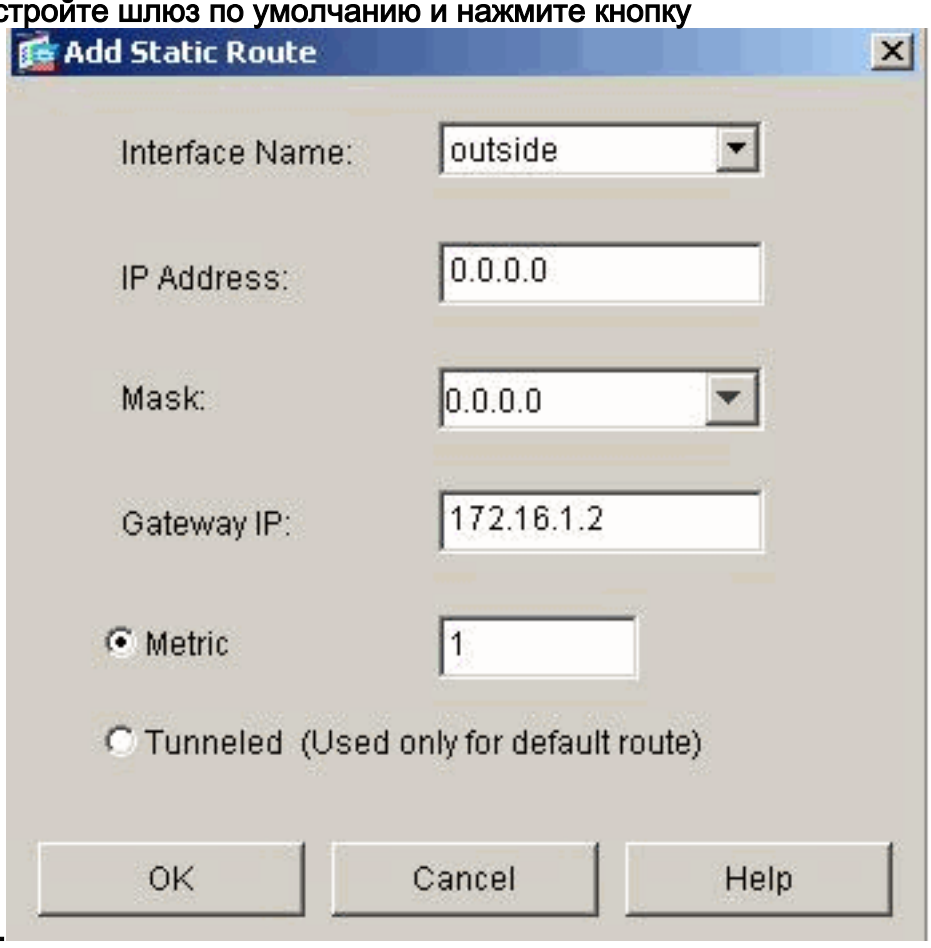
17. Чтобы загрузить настроенное правило NAT в PIX, нажмите кнопку Apply.



18. В данном примере используются статические маршруты. **Нажмите кнопку Routing, выберите Static Route и нажмите кнопку Add.**

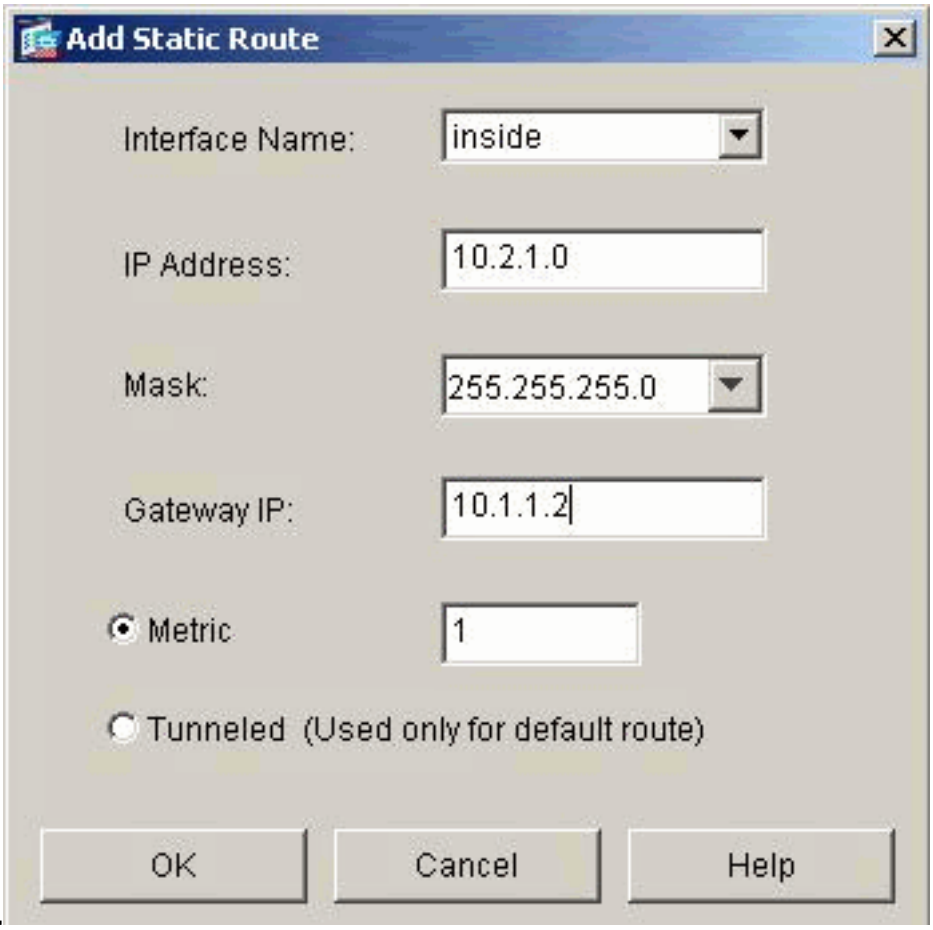


19. Настройте шлюз по умолчанию и нажмите кнопку



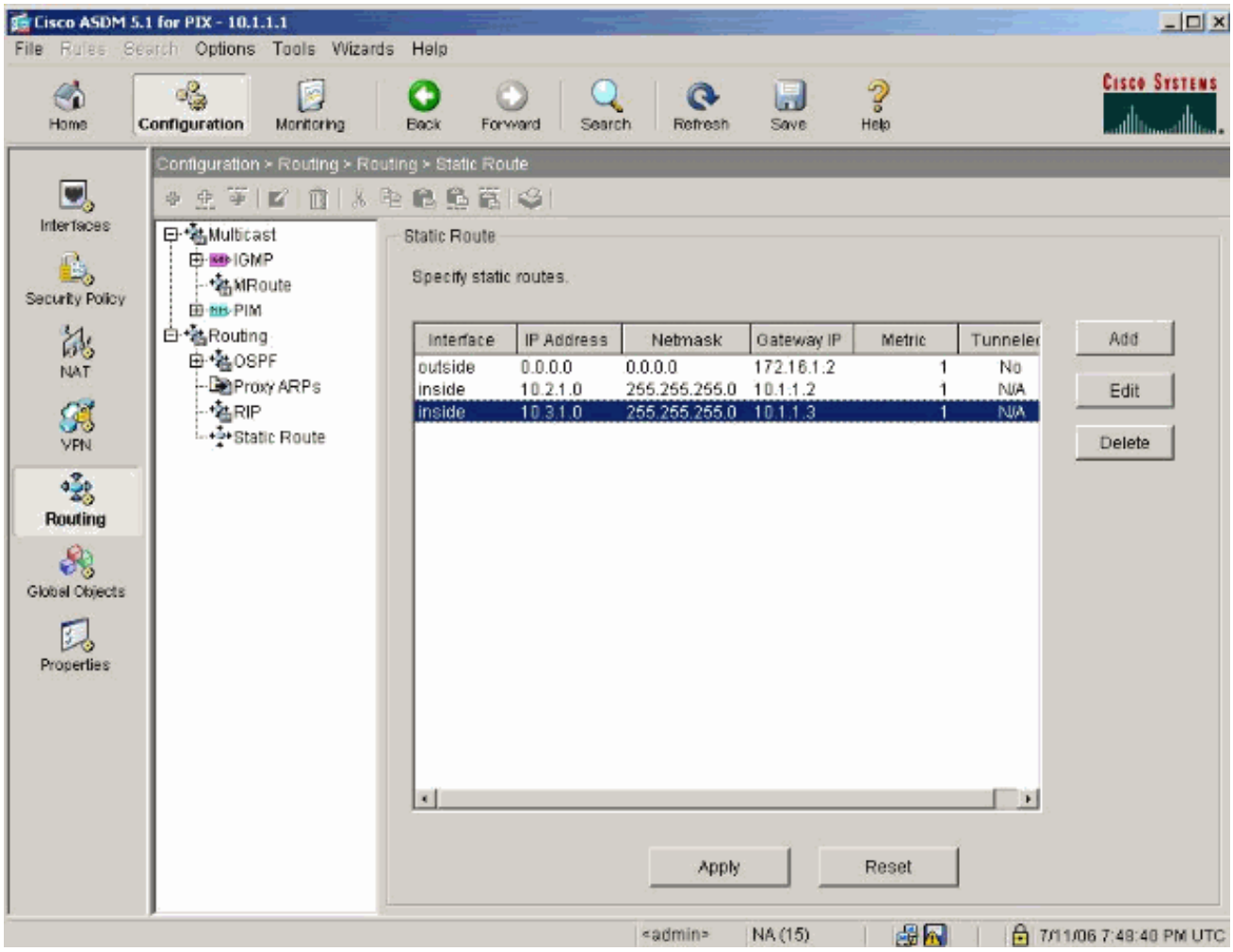
OK.

20. Нажмите кнопку Add и добавьте маршруты к внутренним



сетям.

21. Подтвердите правильность настройки маршрутов и щелкните Apply.



Конфигурация PIX с помощью CLI

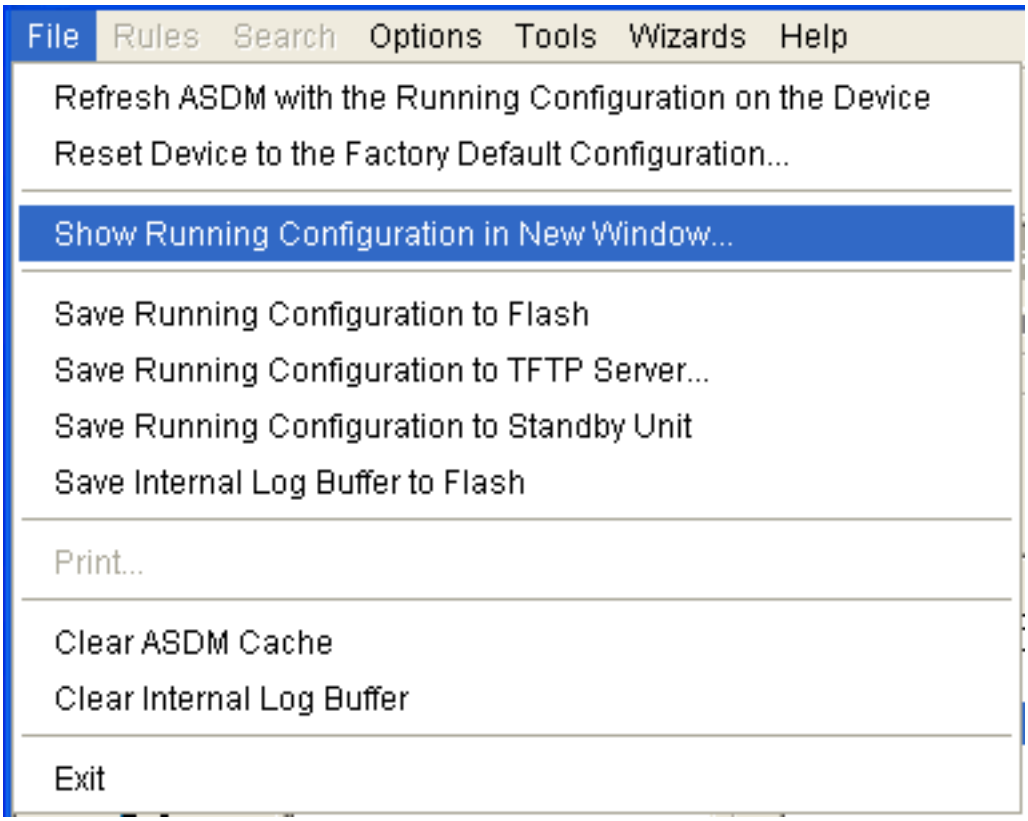
Настройка при помощи графического интерфейса пользователя ASDM завершена.

Данную конфигурацию можно просмотреть при помощи интерфейса командной строки:

Интерфейс командной строки PIX Security Appliance
pixfirewall(config)#**write terminal** PIX Version 7.0(0)102 names ! **interface Ethernet0 nameif outside security-level 0 ip address 172.16.1.1 255.255.255.0** ! **interface Ethernet1 nameif inside security-level 100 ip address 10.1.1.1 255.255.255.0** *!--- Assign name and IP address to the interfaces* enable password 2KFQnbNIdI.2KYOU encrypted passwd 2KFQnbNIdI.2KYOU encrypted asdm image flash:/asdmfile.50073 no asdm history enable arp timeout 14400 **nat-control** *!--- Enforce a strict NAT for all the traffic through the Security appliance* **global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0** *!--- Define a pool of global addresses 172.16.1.5 to 172.16.1.10 with !--- NAT ID 1 to be used for NAT* **global (outside) 1 172.16.1.4 netmask 255.255.255.0** *!--- Define a single IP address 172.16.1.4 with NAT ID 1 to be used for PAT* **nat (inside) 1 10.0.0.0 255.0.0.0** *!--- Define the inside networks with same NAT ID 1 used in the global command for NAT* **route inside 10.3.1.0 255.255.255.0 10.1.1.3 1 route inside 10.2.1.0 255.255.255.0 10.1.1.2 1** *!--- Configure static routes for routing the packets towards the internal network* **route outside 0.0.0.0 0.0.0.0 172.16.1.2 1** *!---*

```
Configure static route for routing the packets towards
the Internet (or External network) 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 !--- Enable the HTTP server on PIX for ASDM
access http 10.1.1.5 255.255.255.255 inside !--- Enable
HTTP access from host 10.1.1.5 to configure PIX using
ASDM (GUI) ! !--- Output suppressed ! !
Cryptochecksum:a0bff9bbaa3d815fc9fd269a3f67fef5 : end
```

Выберите **File> Show Running Configuration in New Window** для просмотра конфигурации интерфейса командой строки в ASDM.



Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Команды для устранения неполадок

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

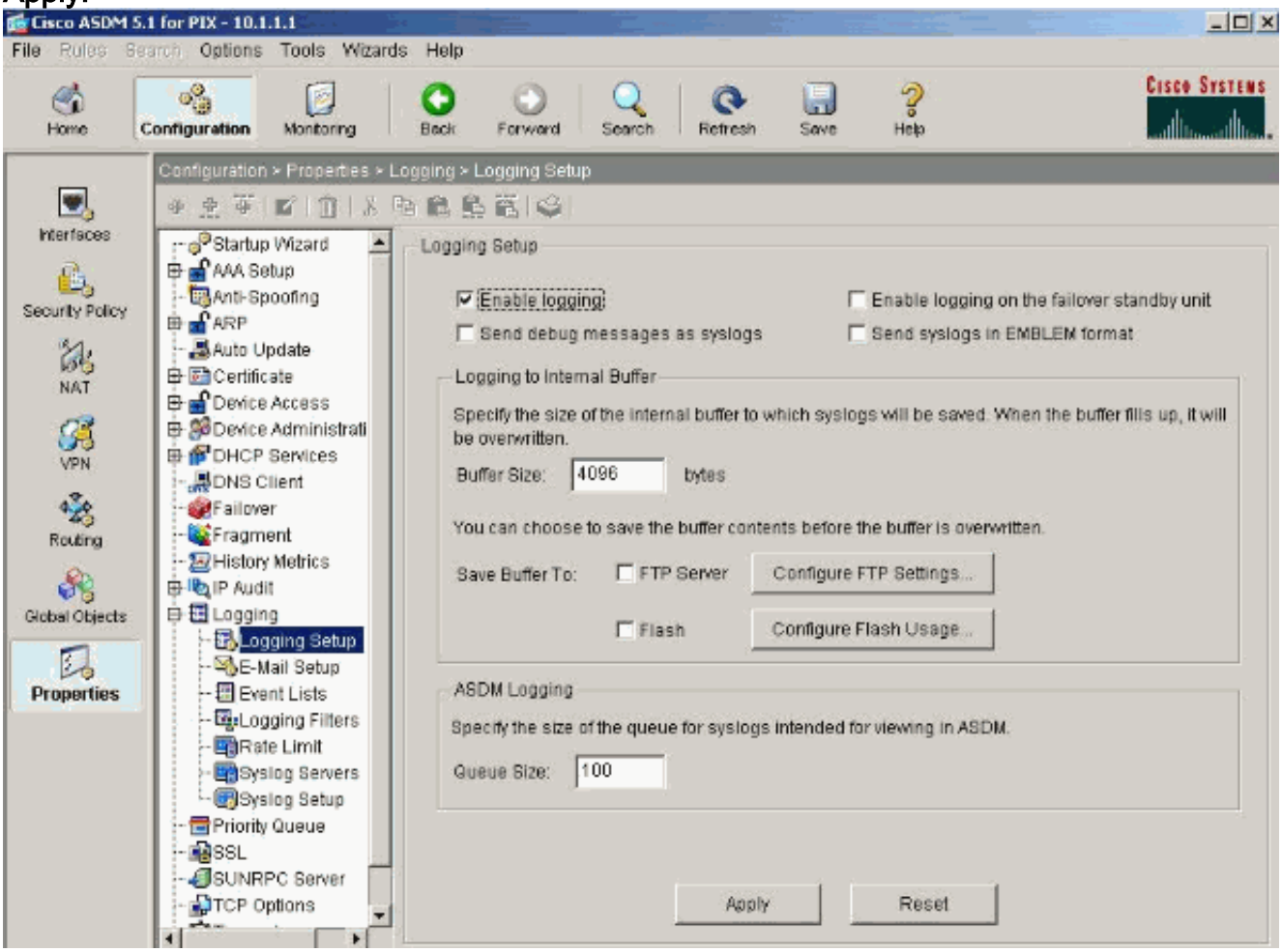
Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- **debug icmp trace— данная команда показывает, достигают ли устройства PIX запросы ICMP, отправляемые хостами. Для выполнения этой отладки добавьте команду access-list, чтобы разрешить ICMP в вашей конфигурации.**
- **регистрация перед отладкой** — Показывает соединения, которые установлены и запрещены хостам, которые проходят PIX. **Информация хранится в буфере журнала PIX. Его можно просмотреть при помощи команды show log.**

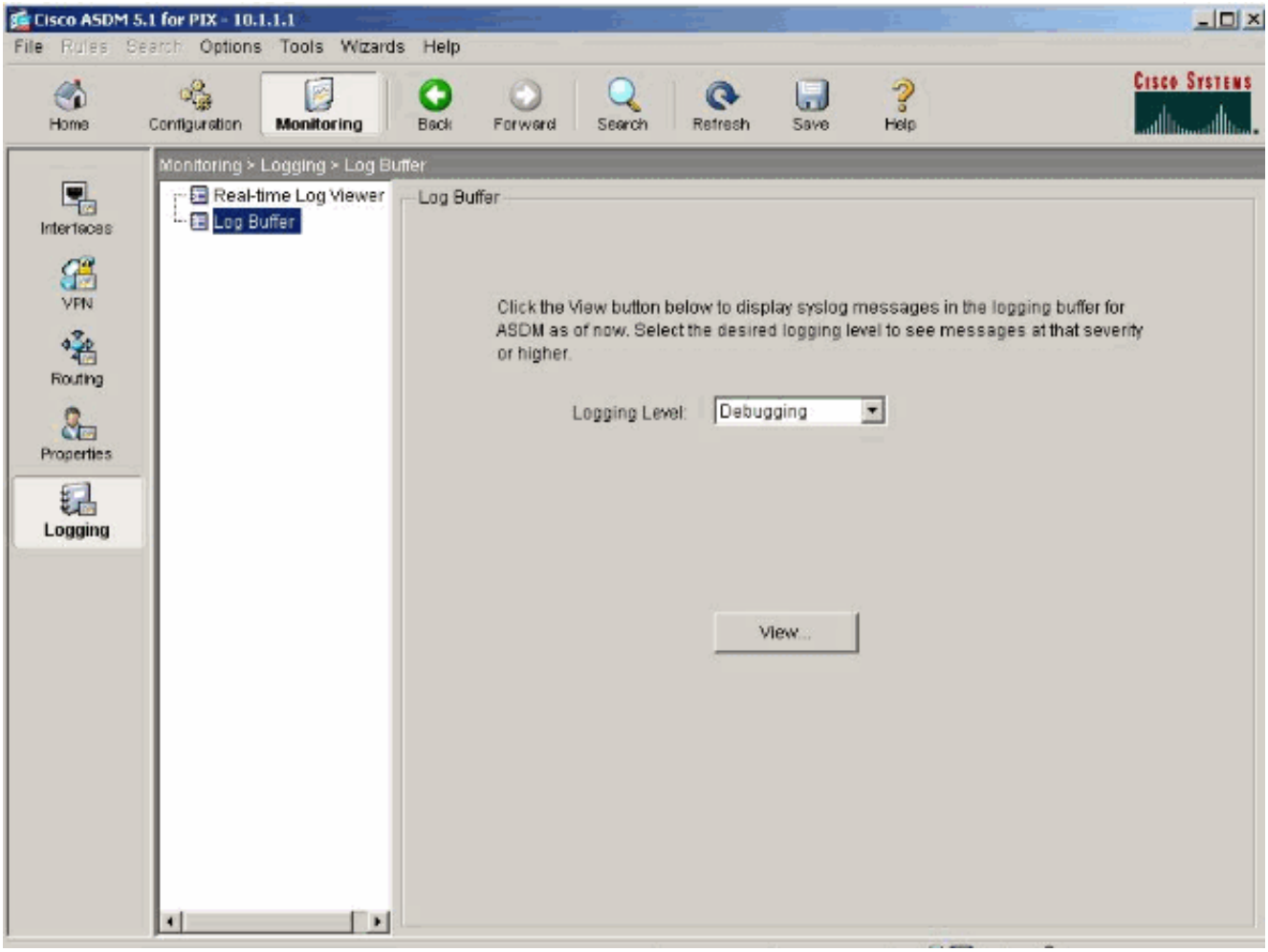
Процедура устранения неполадок

ASDM можно использовать для включения регистрации, а также для просмотра журналов:

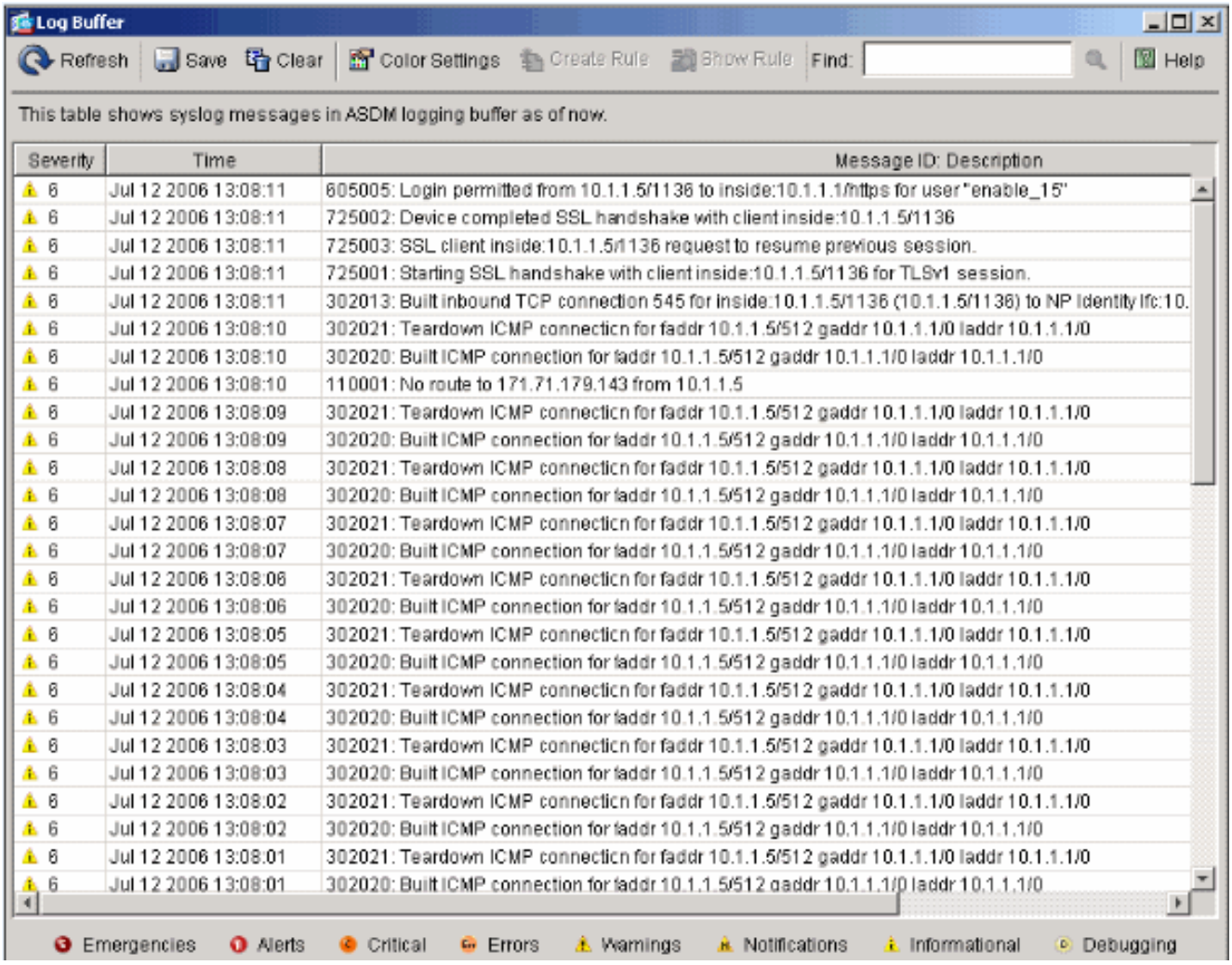
1. **Выберите Configuration > Properties > Logging > Logging Setup, установите флажок Enable logging (включить регистрацию) и нажмите Apply.**



2. Выберите **Monitoring> Logging> Log Buffer> Logging Level** и выберите **Logging Buffer** из выпадающего списка. **Нажмите кнопку View.**



3. Пример буфера журнала:



Неспособный обратиться к веб-сайтам по имени

В определенных сценариях не могут обратиться внутренние сети, интернет-веб-сайты при помощи названия (работает с IP-адресом) в web-браузере. Эта проблема распространена и обычно происходит, если сервер DNS не определен, особенно в случаях, где PIX/ASA является сервером DHCP. Кроме того, это может произойти в случаях, если PIX/ASA неспособен выдвинуть сервер DNS или если сервер DNS не достижим.

Дополнительные сведения

- Cisco PIX 500 Series Security Appliances
- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Диспетчер адаптивных устройств защиты Cisco (Cisco Adaptive Security Device Manager)
- Поиск и устранение неисправностей и предупреждения Cisco Adaptive Security Device Manager (ASDM)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация