# PIX/ASA: Перенаправление (forwarding) порта с nat, global, static и access-list команд

## Содержание



## Введение

**Для повышения безопасности при применении устройств защиты Cisco PIX версии 7.0 важно иметь представление о движении пакетов между интерфейсами, относящимися к более и менее защищенным участкам сети. Это относится к использованию команд nat-control, nat, global, static, access-list и access-group.** В данном документе поясняются различия между этими командами, а также способы настройки перенаправления (переадресации) портов и функции преобразования внешних сетевых адресов (NAT) в ПО PIX версий 7.x посредством интерфейса командной строки и диспетчера устройств адаптивной защиты (ASDM).

**Примечание:** Некоторые опции в ASDM 5.2 и позже могут казаться другими, чем опции в ASDM 5.1. Дополнительные сведения см. в документации по ASDM.

# Предварительные условия

## Требования

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:

- ПО для устройств защиты Cisco PIX серии 500 версии 7.0 и выше
- ASDM версий 5.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.

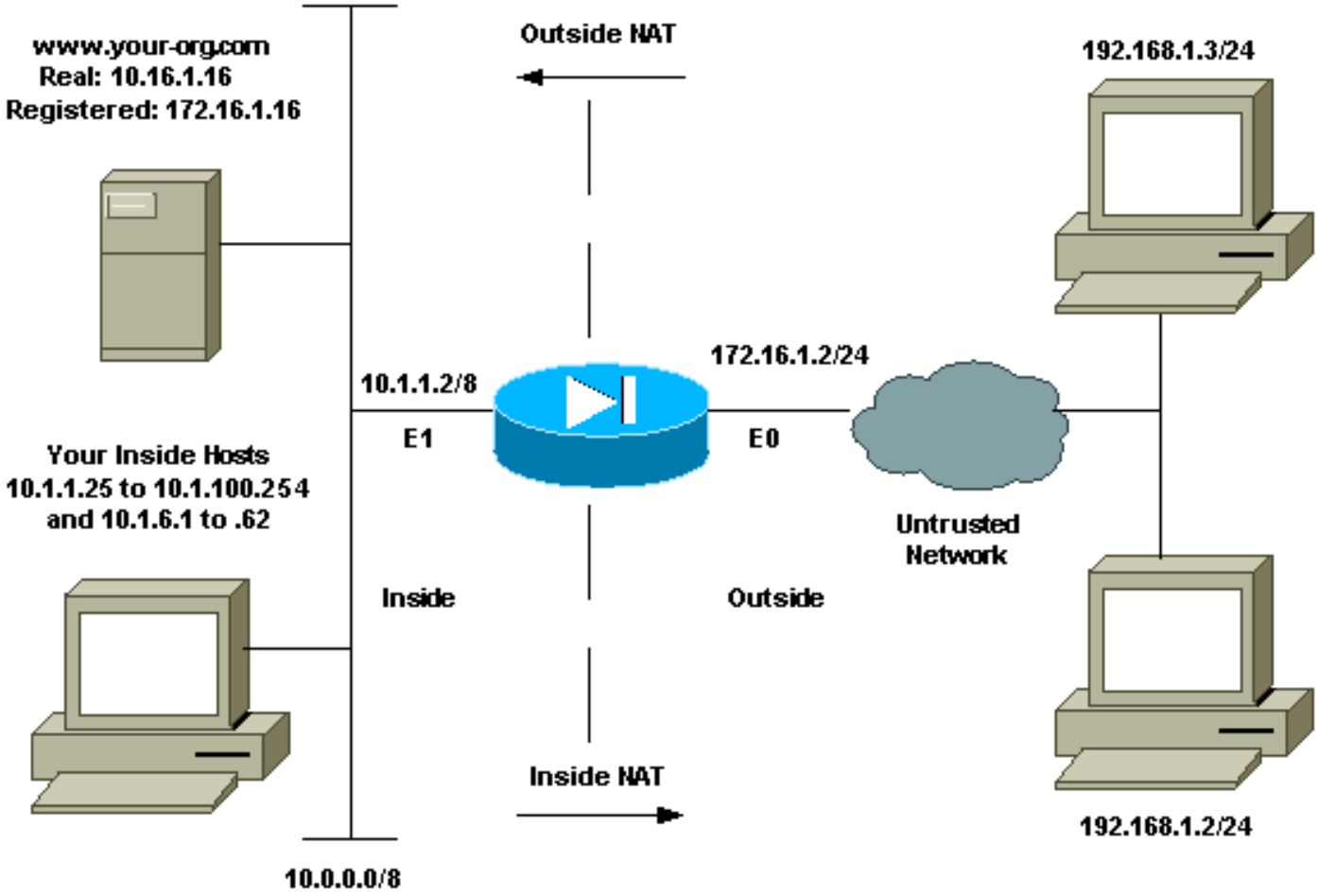
## Родственные продукты

Данную конфигурацию также можно использовать с устройством адаптивной защиты Cisco ASA версий 7.x и выше.

## Условные обозначения

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

# Схема сети




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

## Начальная конфигурация

Назначение имен интерфейсов (outside – внешний, inside – внутренний):

- **interface ethernet 0—nameif outside**
- **interface ethernet 1—nameif inside**

**Примечание:** Дополнительные сведения о командах, использованных в данном документе, см. в разделе Средство поиска команд (только для зарегистрированных клиентов).

## Разрешение исходящего доступа

Исходящий доступ – это подключения от интерфейса с высоким уровнем безопасности к интерфейсу с низким уровнем безопасности. Это понятие включает в себя исходящие соединения, соединения, направленные в DMZ (демилитаризованную зону), а также соединения, направленные от DMZ во внешнюю сеть. Также сюда относятся подключения из одной зоны DMZ к другой при условии, что интерфейс источника подключения имеет более высокий уровень безопасности, чем интерфейс назначения. Проверить это можно по настройке параметра security-level на интерфейсах PIX.

В этом примере отображается уровень безопасности и конфигурация имен интерфейсов:

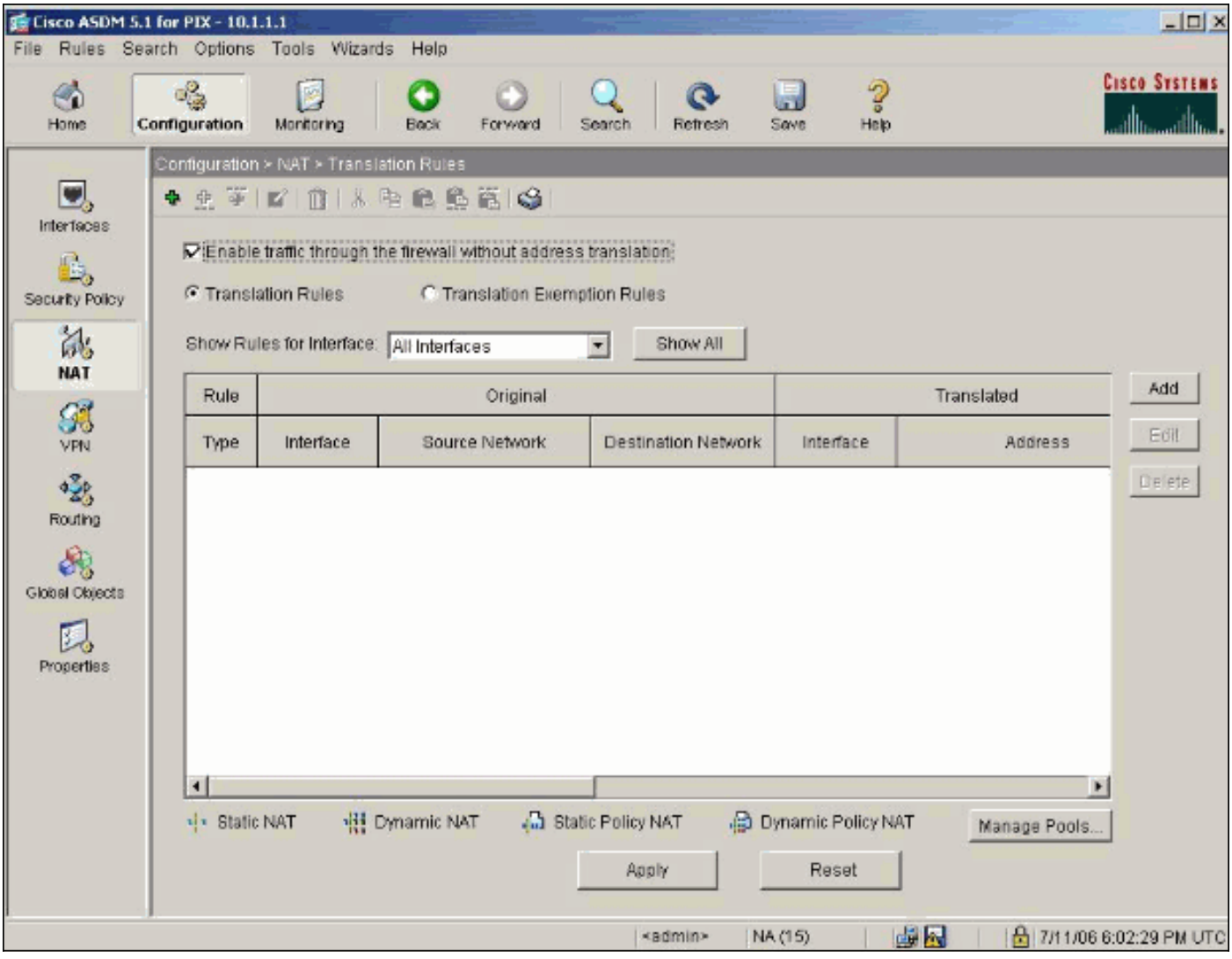
```
pix(config)#interface ethernet 0 pix(config-if)#security-level 0 pix(config-if)#nameif outside
pix(config-if)#exit
```

**В PIX 7.0 введена команда nat-control. В режиме настройки посредством команды nat-control можно указать, требуется ли NAT для обмена данными с внешней сетью.** С активированным управлением NAT для разрешения исходящего трафика необходима настройка NAT, как и в предыдущих версиях программного обеспечения PIX. **Если управление NAT отключено (no nat-control), то внутренние узлы смогут обмениваться данными с внешними сетями без настройки правила NAT.** Однако при наличии внутренних узлов, не имеющих внешних адресов, для них будет по-прежнему необходимо настраивать NAT.

**Для настройки управления NAT с использованием ASDM выберите вкладку Configuration (Конфигурация) в домашнем окне ASDM и в меню функций выберите NAT.**

**Разрешите трафик через межсетевой экран без преобразования:** Этот параметр введен в версии PIX 7.0(1). **Если установлен этот флажок, то составе конфигурации будет отсутствовать команда nat-control.** Эта команда означает, что при переходе через межсетевой экран преобразование не требуется. Обычно этот параметр проверяется только в том случае, если внутренние узлы имеют внешние IP-адреса либо если топология сети не требует преобразования адресов внутренних узлов в другие IP-адреса.

Если же внутренние узлы имеют закрытые IP-адреса, то этот флажок необходимо снять, чтобы адреса внутренних узлов могли преобразовываться во внешний IP-адрес и имелся доступ в Интернет.



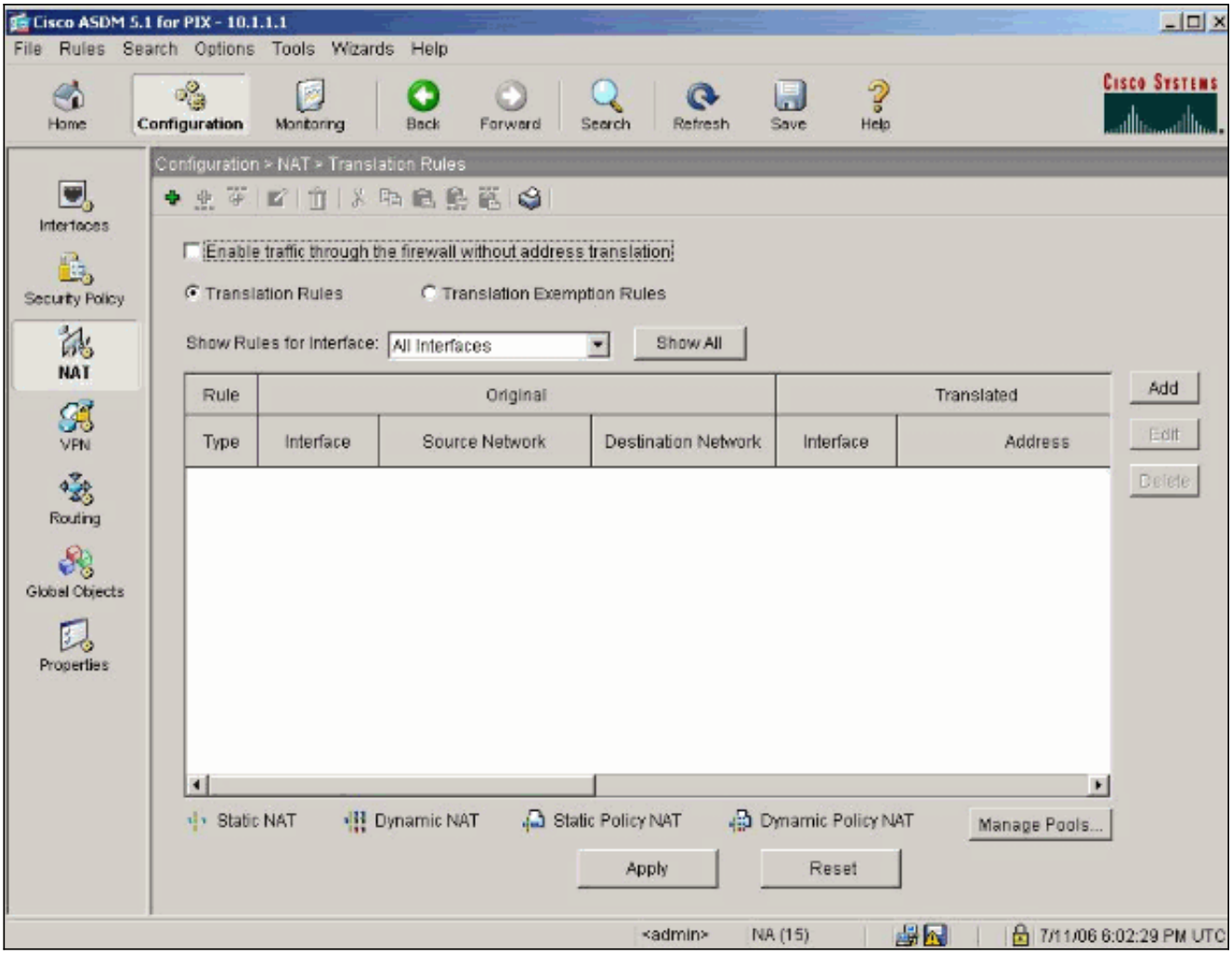
Для разрешения исходящего доступа с управлением NAT необходимо реализовать две политики. Первая – метод преобразования. **Возможно как статическое преобразование с использованием команды static, так и динамическое преобразование с использованием команд nat или global.** Это не требуется, если управление NAT отключено, а внутренние узлы имеют внешние адреса.

Второе требование для исходящего доступа (которое применяется независимо от того, включено ли управление NAT) – наличие списка управления доступом (ACL). Если существует список управления доступом, то он должен разрешать доступ с исходного узла на целевой узел с использованием определенного протокола и порта. По умолчанию нет ограничений доступа на исходящие соединения через PIX. Это означает, что если для исходного интерфейса не настроен ACL, тогда по умолчанию исходящие соединения разрешены при наличии настроенного способа преобразования.

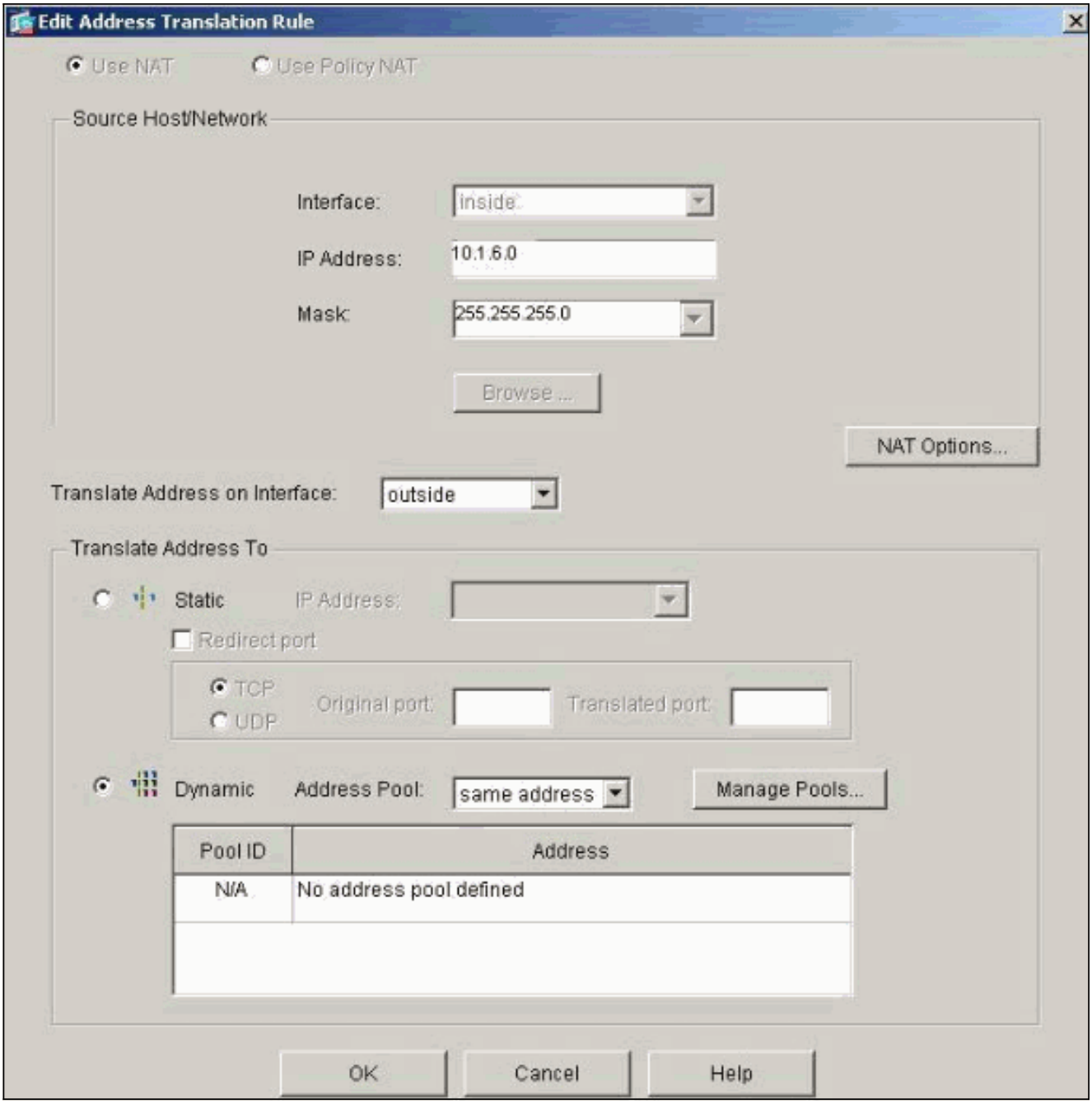
## Разрешение доступа внутренних узлов во внешние сети с использованием NAT

Эта конфигурация предоставляет всем узлам в подсети 10.1.6.0/24 доступ к внешней сети. **Для этой цели используются команды nat и global, как проиллюстрировано в данной процедуре.**

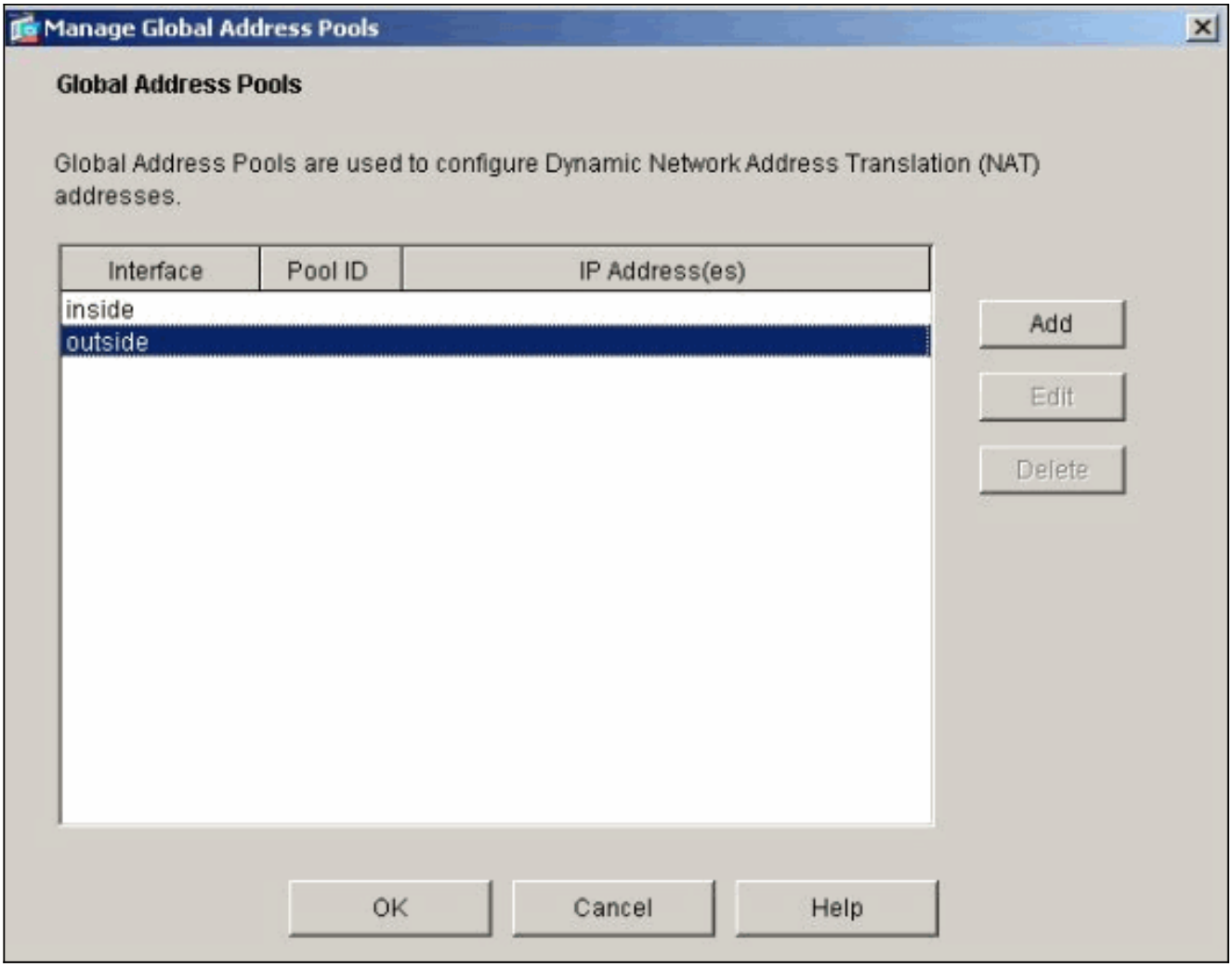
1. Определите внутреннюю группу, которая будет участвовать в преобразовании NAT.
   ```
   nat (inside) 1 10.1.6.0 255.255.255.0
   ```
2. Укажите пул адресов внешнего интерфейса, к которому преобразуются узлы, определенные в инструкции NAT.
   ```
   global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0
   ```
3. При помощи ASDM создайте пул глобальных адресов. **Выберите Configuration (Конфигурация) > Features (Функции) > NAT и снимите флажок Enable traffic through the firewall without address translation (Разрешить прохождение трафика через межсетевой экран без преобразования адресов). Затем щелкните Add (Добавить) для настройки правила**
   **NAT.**



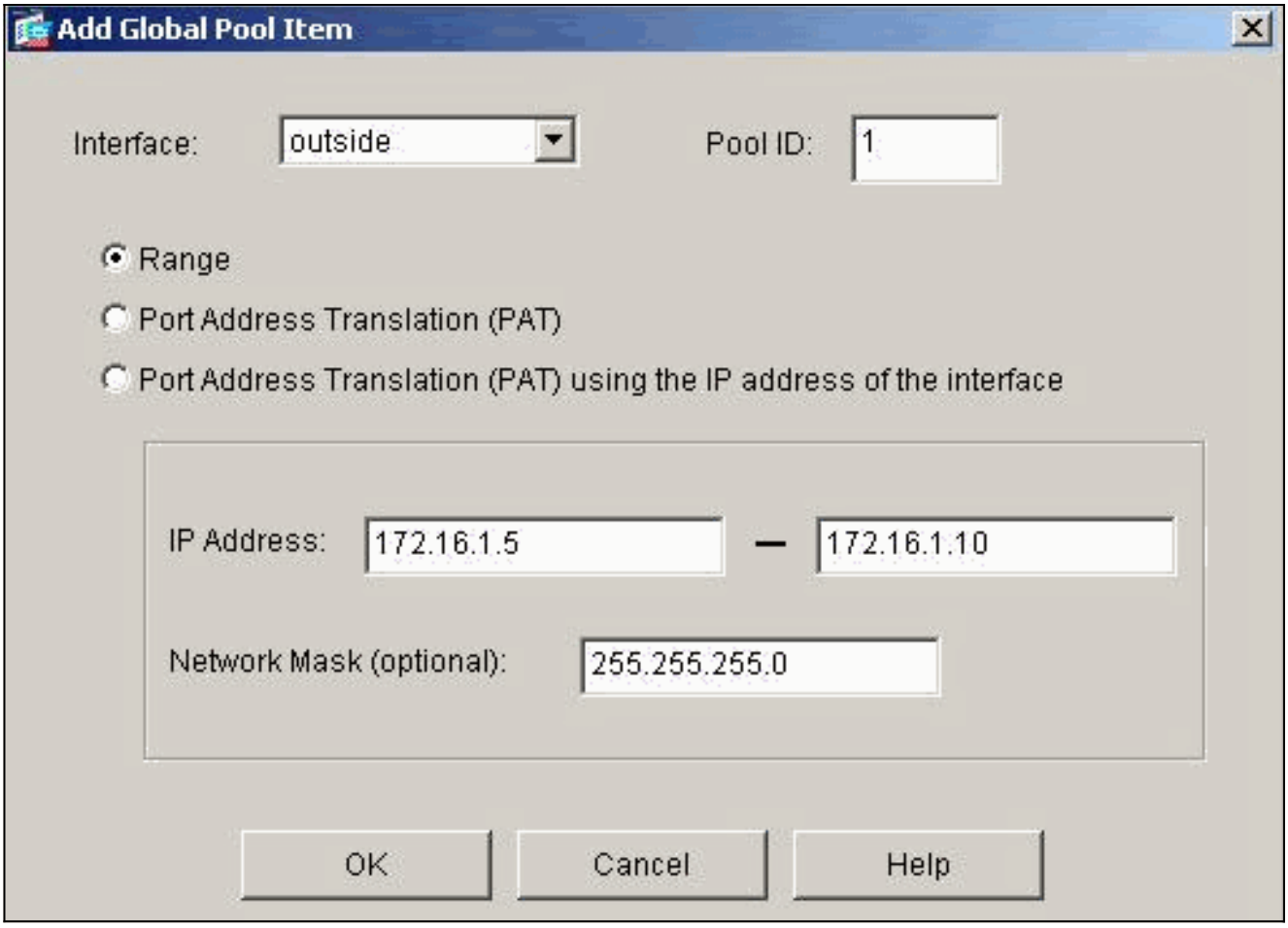

4. Чтобы задать пул адресов NAT, щелкните Manage Pools (Управление пулами).



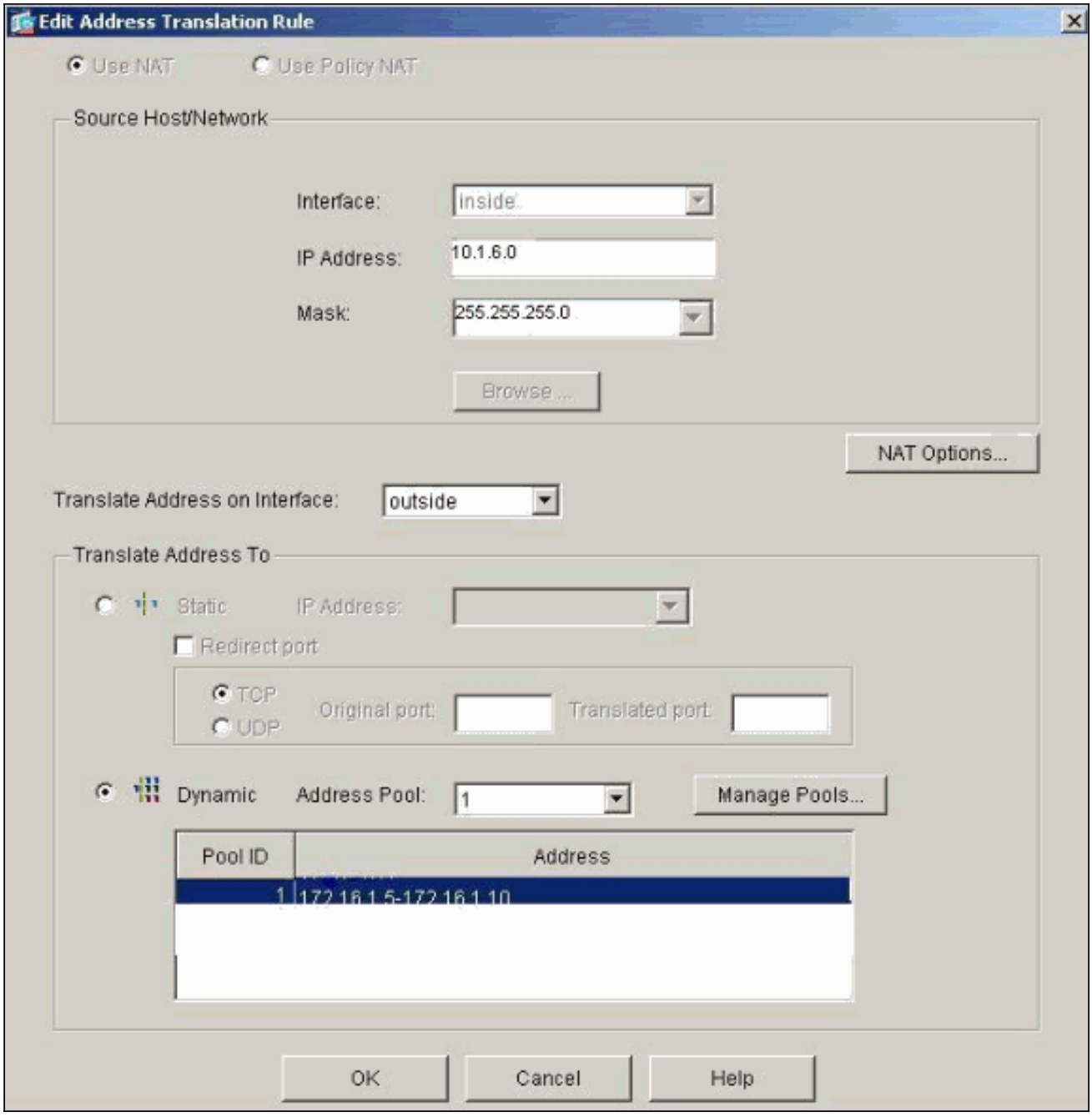

5. **Выберите Outside (Внешний) > Add (Добавить) и укажите диапазон для пула адресов.**



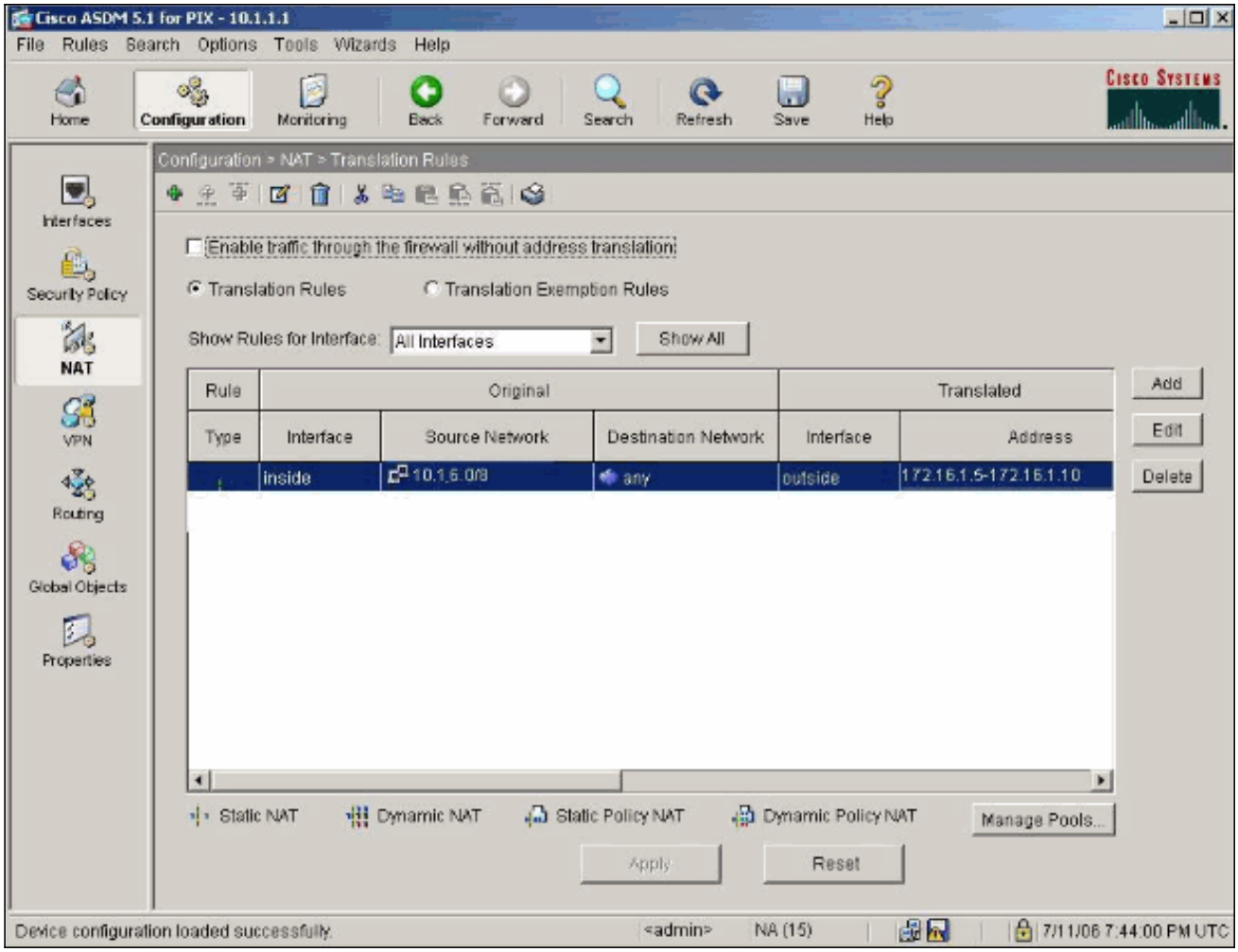

6. Введите диапазон адресов, введите идентификатор пула и щелкните OK.




7. Для создания правила трансляции выберите Configuration (Конфигурация) > Features (Функции) > NAT > Translation Rules (Правила трансляции).
8. В качестве исходного интерфейса (Source Interface) выберите Inside (Внутренний) и введите диапазон адресов, для которых следует применять NAT.
9. В поле Translate Address on Interface (Преобразование адреса на интерфейсе) выберите Outside (Внешний), затем Dynamic (Динамический) и укажите настроенный пул адресов.
10. Нажмите кнопку
    OK.




11. Преобразование будет отображено в поле Translation Rules (Правила преобразования) в разделе Configuration (Конфигурация) > Features (Функции) > NAT > Translation Rules (Правила преобразования).




Теперь узлы во внутренней сети могут иметь доступ к внешним сетям. Если внутренние узлы инициируют подключение к внешним устройствам, они транслируются к адресу из глобального пула. Адреса назначаются из глобального пула по принципу FIFO («первым прибыл, первым обслужен»), начиная с самого младшего адреса в пуле. Например, если хост 10.1.6.25 первым инициирует соединение наружу, он получает адрес 172.16.1.5. Следующий хост получает адрес 172.16.1.6 и т.д. **Это преобразование не является статическим и истекает по истечении периода бездействия, задаваемого командой timeout xlate hh:mm:ss.** Если число внутренних узлов превышает число адресов в пуле, то для преобразования адресов портов (PAT) используется последний адрес пула.

## Разрешение доступа внутренних узлов во внешние сети с использованием PAT

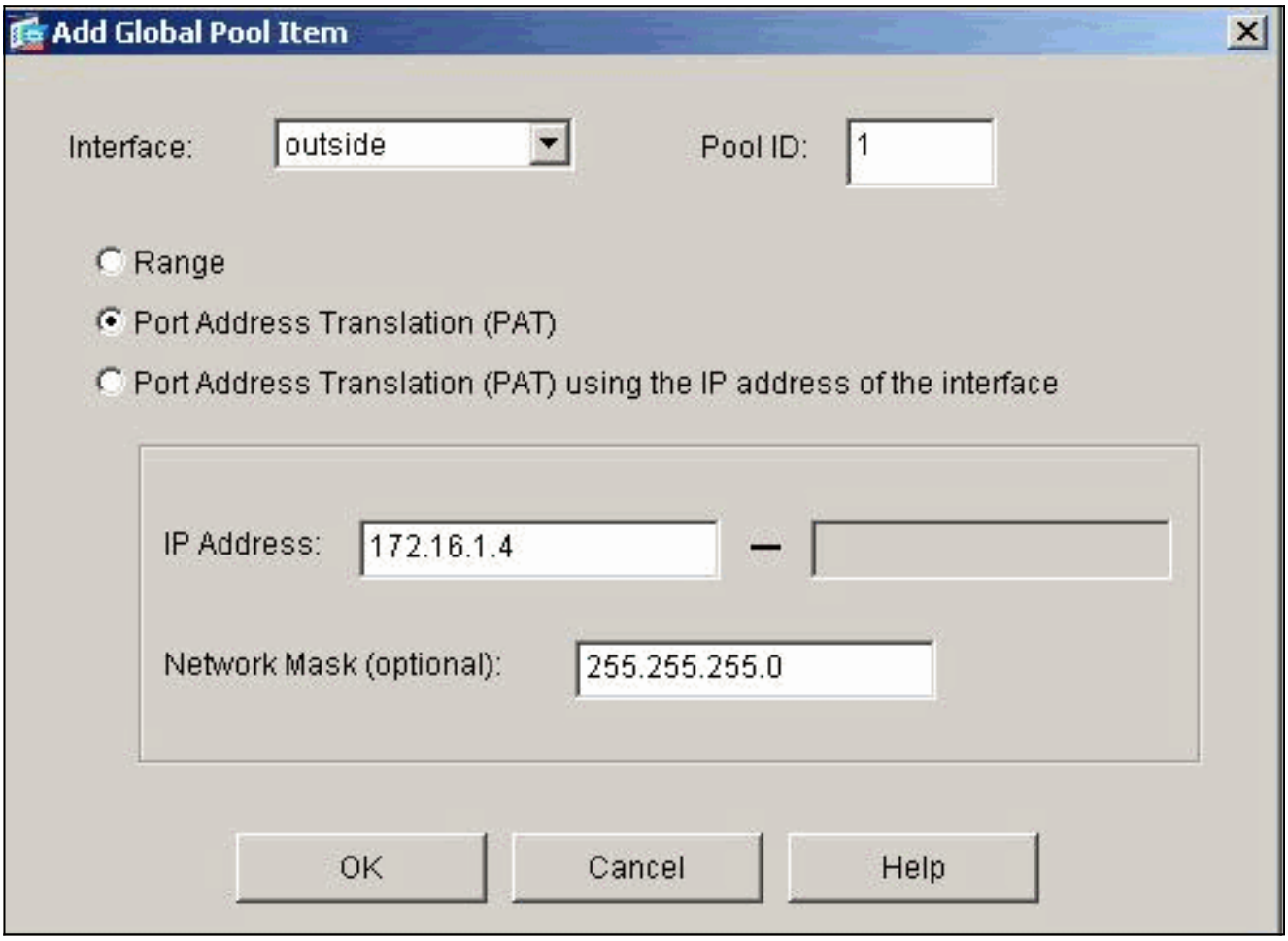
PAT следует использовать в том случае, когда преобразование адресов для внутренних узлов требуется осуществлять с одним общим внешним адресом. **Если в операторе global указан один адрес, то преобразование портов выполняется для него.** PIX позволяет преобразовывать один порт на интерфейс, и это преобразование поддерживает до 65535 активных объектов xlate на один глобальный адрес. Чтобы разрешить внутренним узлам доступ к внешним сетям с использованием PAT, выполните следующие действия.

1. Определите внутреннюю группу, которую необходимо включить для PAT («0 0» выбирает все внутренние узлы).)
   ```
   nat (inside) 1 10.1.6.0 255.255.255.0
   ```
2. Укажите глобальный адрес, который будет использоваться для PAT. В качестве него

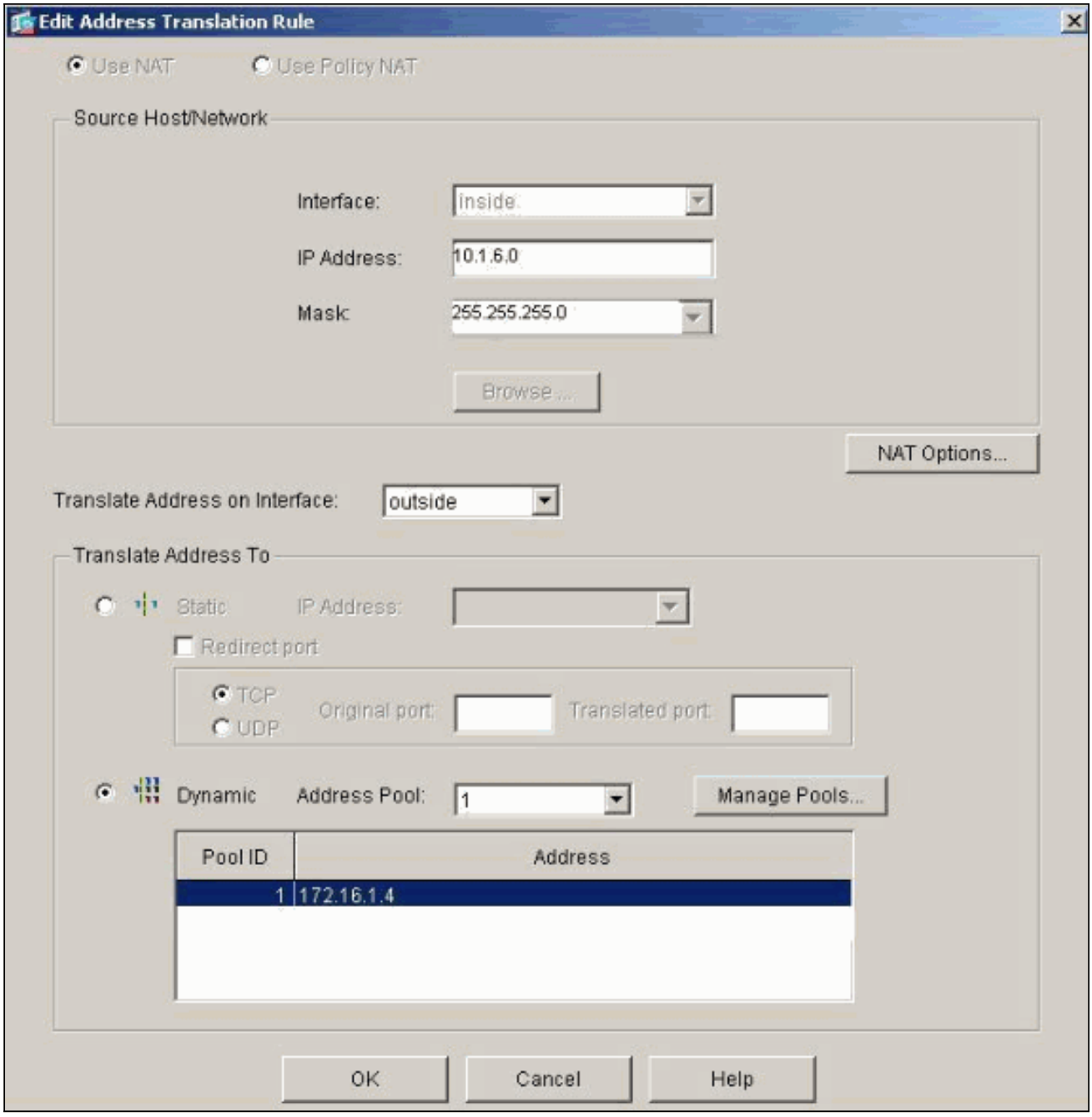
можно указать адрес интерфейса.

```
global (outside) 1 172.16.1.4 netmask 255.255.255.0
```

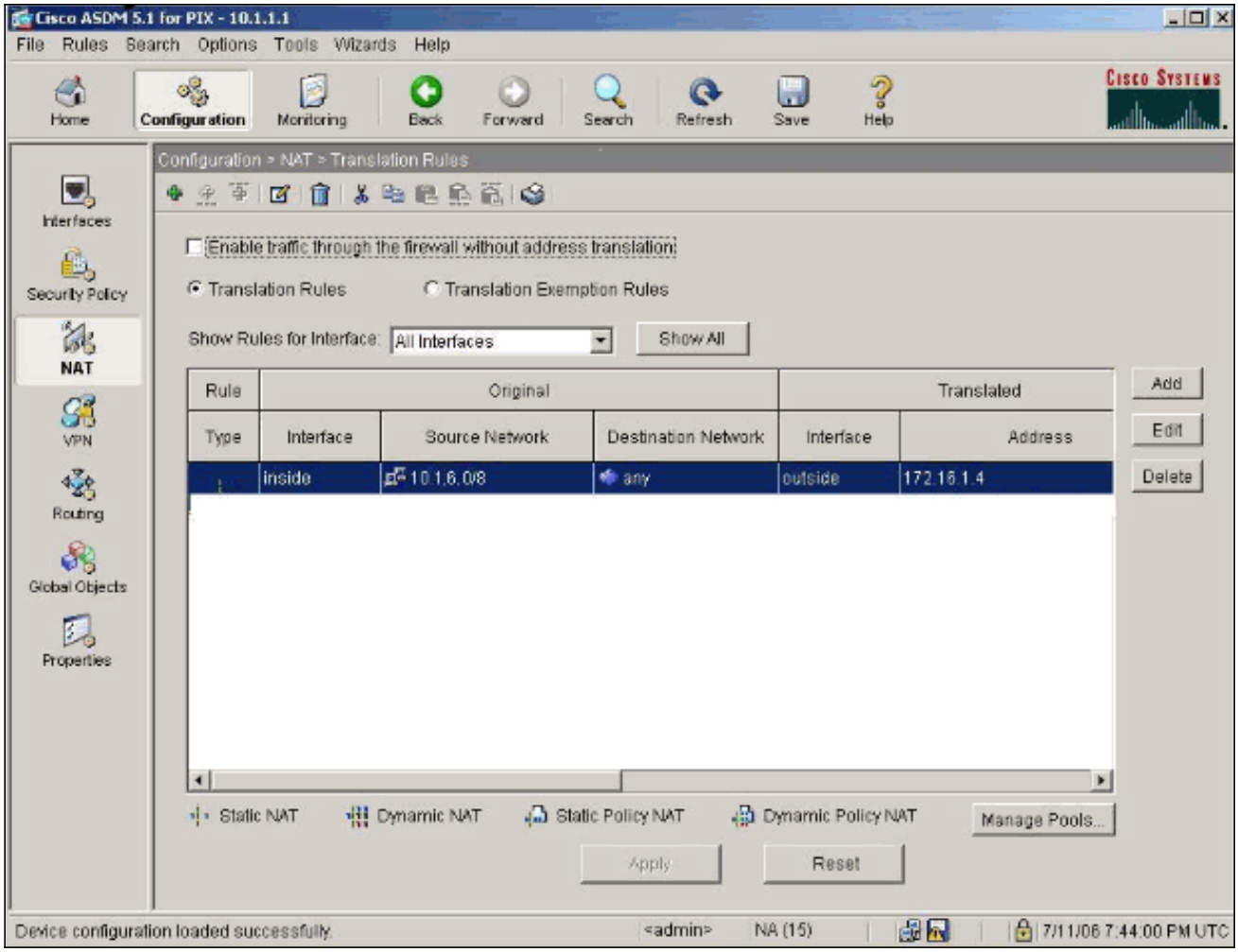
3. В ASDM выберите Configuration (Конфигурация) > Features (Функции) > NAT и снимите флажок Enable traffic through the firewall without address translation (Разрешить трафик через межсетевой экран без преобразования).
4. Затем для настройки правила NAT щелкните Add (Добавить).
5. Для настройки адреса PAT выберите Manage Pools (Управление пулами).
6. Для настройки одного адреса, используемого с преобразованием PAT, выберите Outside (Внешний) > Add (Добавить) и щелкните Port Address Translation (PAT – преобразование адресов портов).
7. Введите адрес и идентификатор пула, затем щелкните OK.




8. Для создания правила трансляции выберите Configuration (Конфигурация) > Features (Функции) > NAT > Translation Rules (Правила трансляции).
9. В качестве исходного интерфейса (Source Interface) выберите Inside (Внутренний) и введите диапазон адресов, для которых следует применять NAT.
10. В поле Translate Address on Interface (Преобразование адреса на интерфейсе) выберите Outside (Внешний), затем Dynamic (Динамический) и укажите настроенный пул адресов. Нажмите кнопку OK.




11. Преобразование будет отображено в поле Translation Rules (Правила преобразования) в разделе Configuration (Конфигурация) > Features (Функции) > NAT > Translation Rules (Правила преобразования).



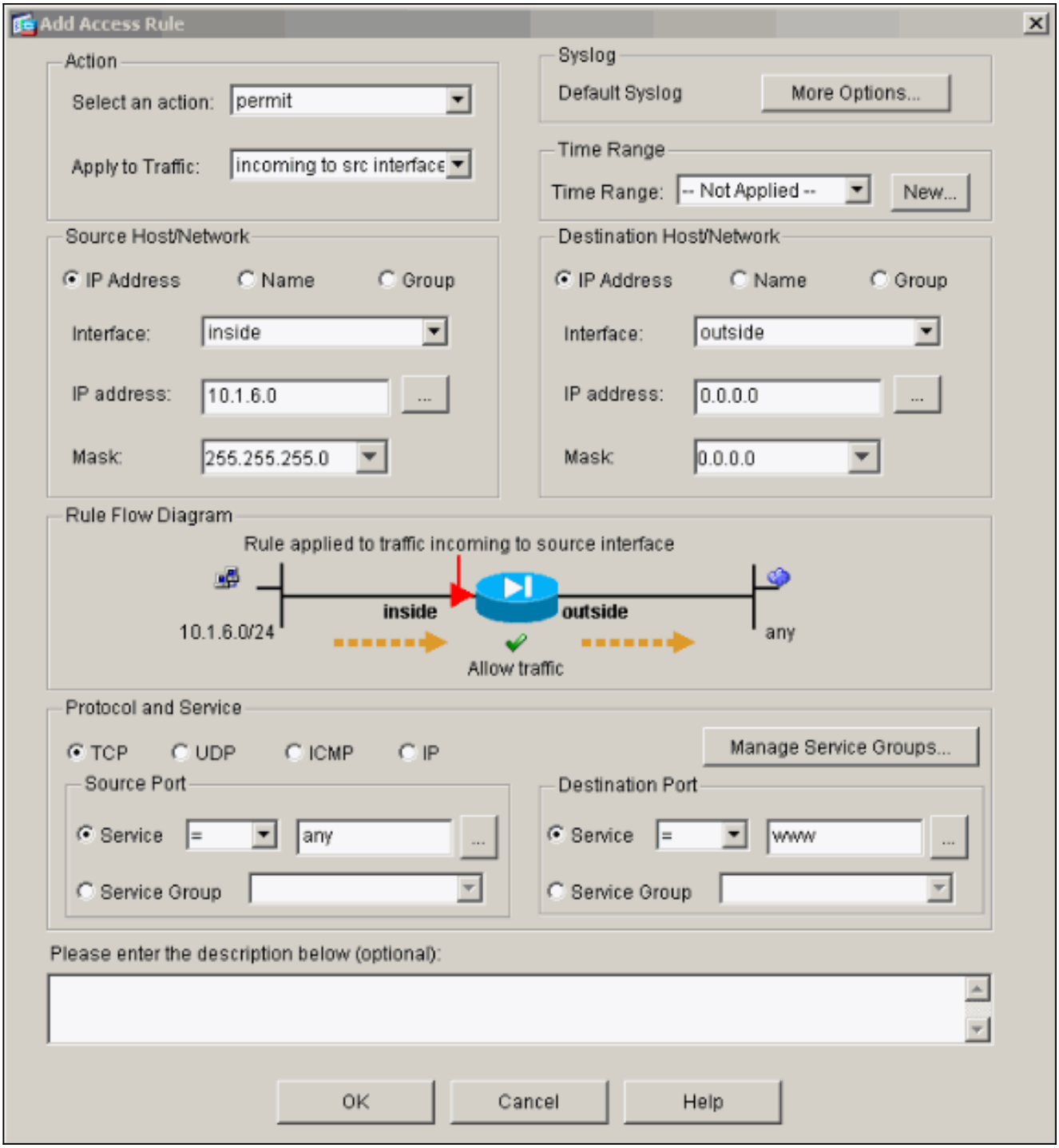

При использовании PAT необходимо помнить о следующем.

- IP-адреса, назначаемые для PAT, не могут принадлежать другому пулу глобальных адресов.
- PAT не работает с приложениями H.323, серверами кэширования имен и туннельным протоколом «точка-точка» (PPTP). PAT работает со службой имен доменов (DNS), FTP и пассивным FTP, HTTP, почтой, процедурой удаленного вызова (RPC), rshell, Telnet, фильтрацией URL-адресов и экспортным трассировщиком.
- Не используйте PAT при наличии мультимедийных приложений, работающих через межсетевой экран. Мультимедийные приложения могут конфликтовать с сопоставлениями портов PAT.
- В программном обеспечении PIX версии 4.2(2) функция PAT не работает с IP-пакетами данных, поступающими в обратном порядке. Эта проблема исправлена в версии программного обеспечения PIX 4,2(3).
- **IP-адреса в пуле глобальных адресов, заданные с помощью команды global, требуют наличия обратных записей DNS для обеспечения доступа ко всем внешним сетевым адресам через PIX.** Чтобы создать обратные сопоставления DNS, используйте запись указателя DNS (PTR) в файле сопоставления адреса и имени для каждого глобального адреса. Без записей PTR интернет-подключение может быть низкоскоростным или периодически исчезать, а FTP-запросы не будут функционировать.Например, если задан глобальный IP-адрес 192.168.1.3, а имя домена для межсетевого экрана PIX – pix.caguana.com, запись PTR будет иметь следующий вид:`3.1.1.175.in-addr.arpa. IN PTR pix3.caguana.com`
  `4.1.1.175.in-addr.arpa. IN PTR pix4.caguana.com & so on.`

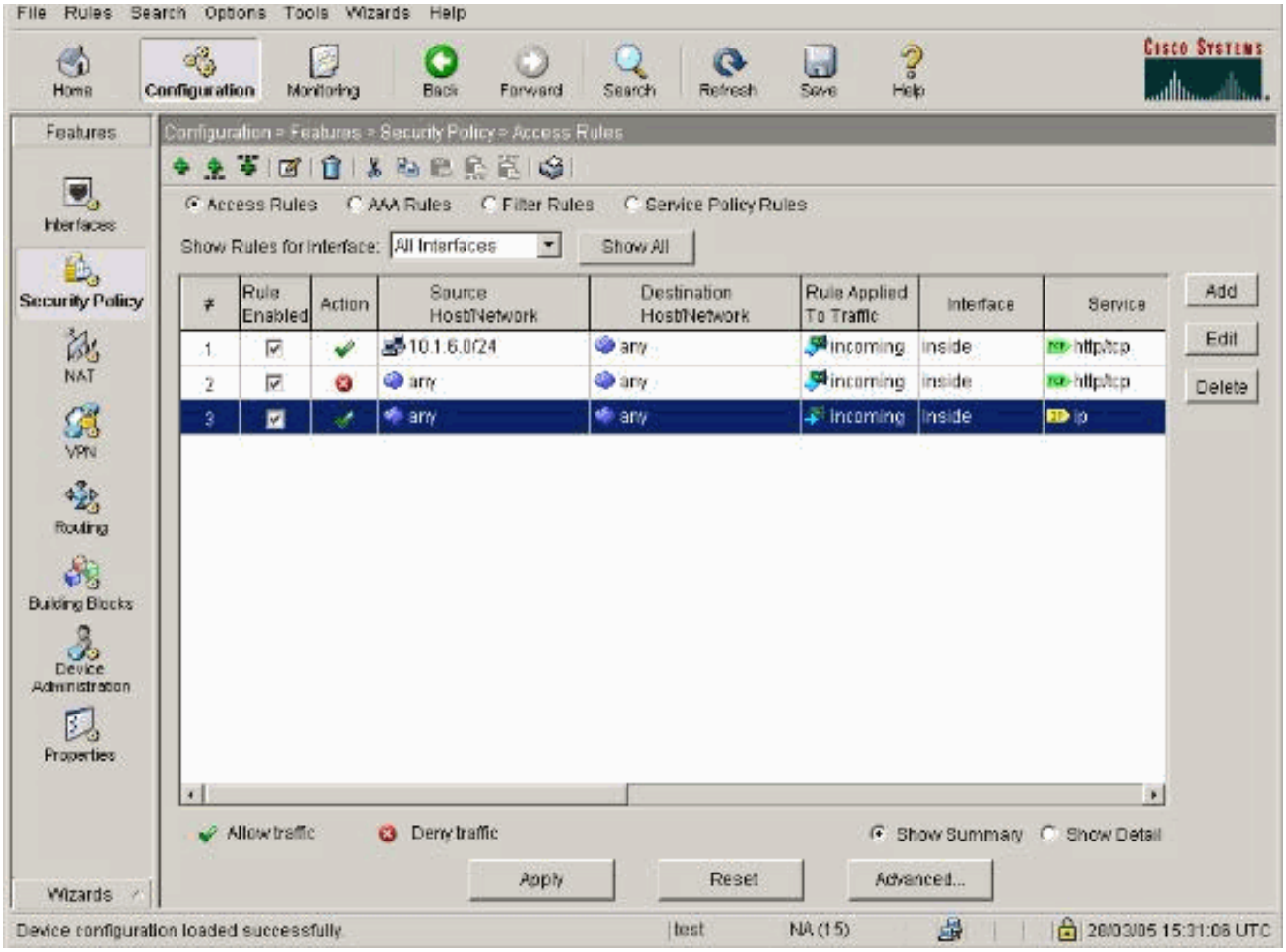
## Запрет доступа внутренних узлов во внешние сети

Если для исходного узла определен допустимый способ преобразования, а для PIX интерфейса источника не определен ACL, тогда исходящее подключение разрешено по умолчанию. Однако в некоторых случаях требуется ограничить исходящий доступ в зависимости от источника, назначения, протокола и/или порта. **Это можно осуществить, настроив список ACL командой access-list и применив его к интерфейсу PIX источника подключения командой access-group.** Списки управления доступом PIX 7.0 возможно применять как во входящем, так и в исходящем направлении. Ниже приведен пример, в котором исходящий доступ по протоколу HTTP разрешен для одной подсети, но запрещен всем другим узлам, несмотря на то что прочие виды IP-трафика разрешены для всех.

1. Определите ACL.
   ```
   access-list acl_outbound permit tcp 10.1.6.0 255.255.255.0 any eq www access-list acl_outbound deny tcp any any eq www access-list acl_outbound permit ip any any
   ```
   **Примечание:** ACL PIX отличаются от ACL на маршрутизаторах Cisco IOS®, в которых PIX не использует маску подстановочного знака как Cisco IOS. Он использует стандартную маску подсети в определении ACL. Как и в случае с маршрутизаторами Cisco IOS, в конце PIX ACL присутствует скрытый параметр "deny all".**Примечание:** Записи нового списка доступа будут добавлены до конца существующих ACE. При необходимости в определенном ACE, обработанном сначала можно использовать ключевое слово  в access-list. Это - сводка примера команды:`access-list acl_outbound line 1 extended permit tcp host 10.1.10.225 any`
2. Примените ACL к внутреннему интерфейсу.
   ```
   access-group acl_outbound in interface inside
   ```
3. **Посредством ASDM настройте первую запись списка управления доступом на шаге 1, чтобы разрешить трафик HTTP из подсети 10.1.6.0/24. Выберите Configuration (Конфигурация) > Features (Функции) > Security Policy (Политика безопасности) > Access Rules (Правила доступа).**
4. **Нажмите кнопкуAdd (Добавить), введите показанные в этом окне сведения и нажмите OK.**




5. Введя три записи списка управления доступом, выберите Configuration (Конфигурация) > Feature (Функции) > Security Policy (Политика безопасности) > Access Rules (Правила доступа).




## Разрешение доступа недоверенных узлов к узлам доверенной сети

В большинстве организаций возникает необходимость разрешения доступа недоверенным узлам в доверенную сеть. Типичный пример – внутренний веб-сервер. По умолчанию PIX запрещает подключения внешних узлов к внутренним узлам. **Чтобы разрешить такое подключение, в режиме управления NAT выполните команду static с командами access-list и access-group. Если управление NAT отключено, необходимы только команды access-list и access-group при условии, что преобразование не выполняется.**

**Для применения списков ACL к интерфейсам используйте команду access-group.** Эта команда связывает ACL с интерфейсом для проверки трафика, передаваемого в определенном направлении.

**В отличие от команд nat и global, разрешающих доступ внутренним узлам во внешнюю сеть, команда static создает двустороннее преобразование, которое при условии добавления соответствующих списков ACL или групп разрешает внутренним узлам доступ во внешнюю сеть, а внешним узлам – во внутреннюю.**

В примерах конфигурации PAT, проиллюстрированных в этом документе, внешний узел, который пытается подключиться к глобальному адресу, может использоваться тысячами внутренних узлов. **Команда static создает взаимно-однозначное сопоставление. Команда access-list определяет допустимый тип соединения с внутренним узлом, и ее необходимо использовать, когда узел с более низким уровнем безопасности подключается к узлу с более высоким уровнем безопасности. Команда access-list задается для конкретной**

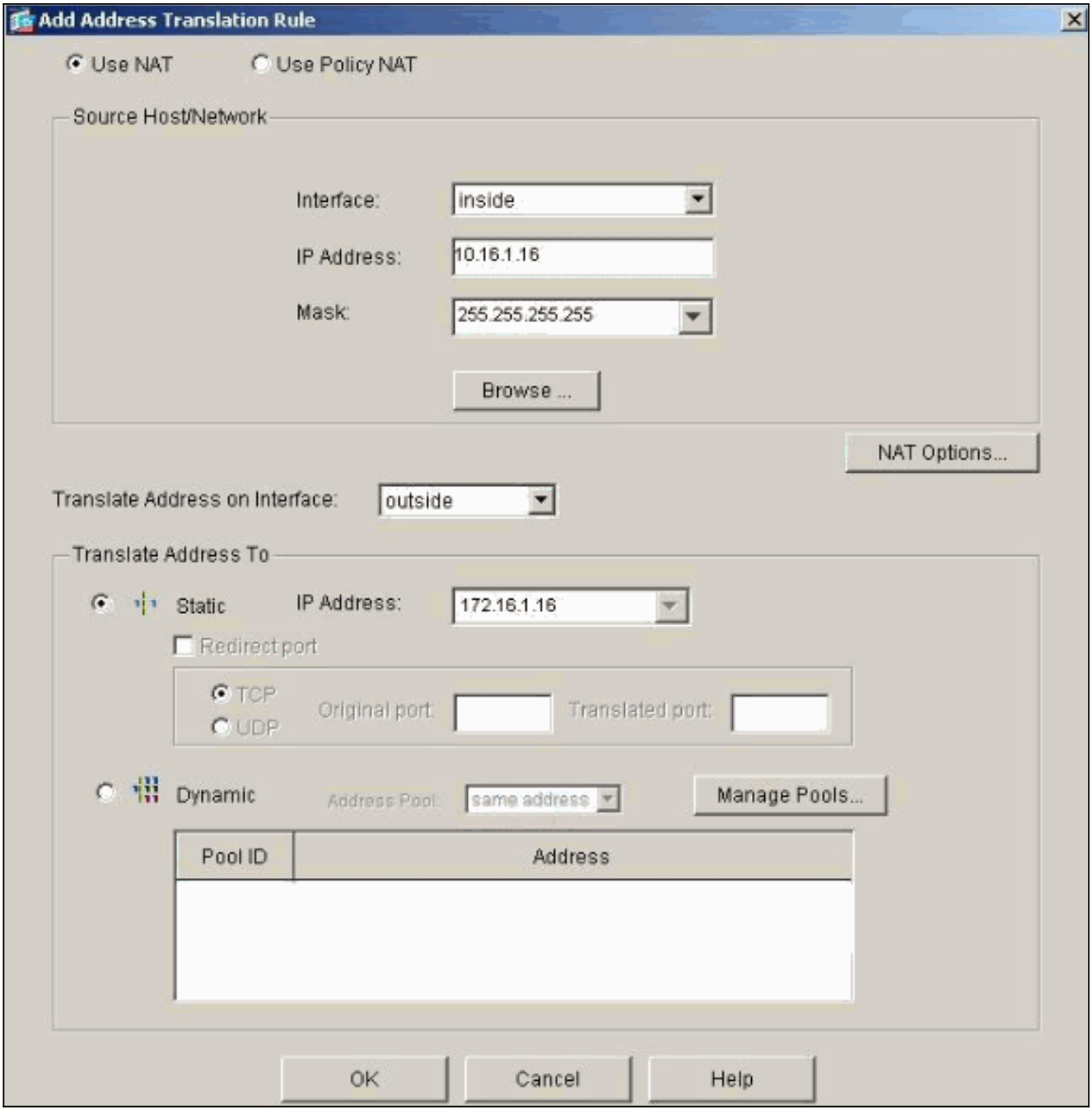
совокупности порта и протокола. Она позволяет системному администратору в зависимости от существующих задач устанавливать как весьма нестрогие, так и чрезвычайно жесткие ограничения.

Приведенная в данном документе схема сети иллюстрирует использование этих команд для задания настройки PIX, при которой все недоверенные узлы будут иметь возможность подключаться к внутреннему веб-серверу, а конкретный недоверенный узел 192.168.1.1 получит доступ к службе FTP на этом же компьютере.

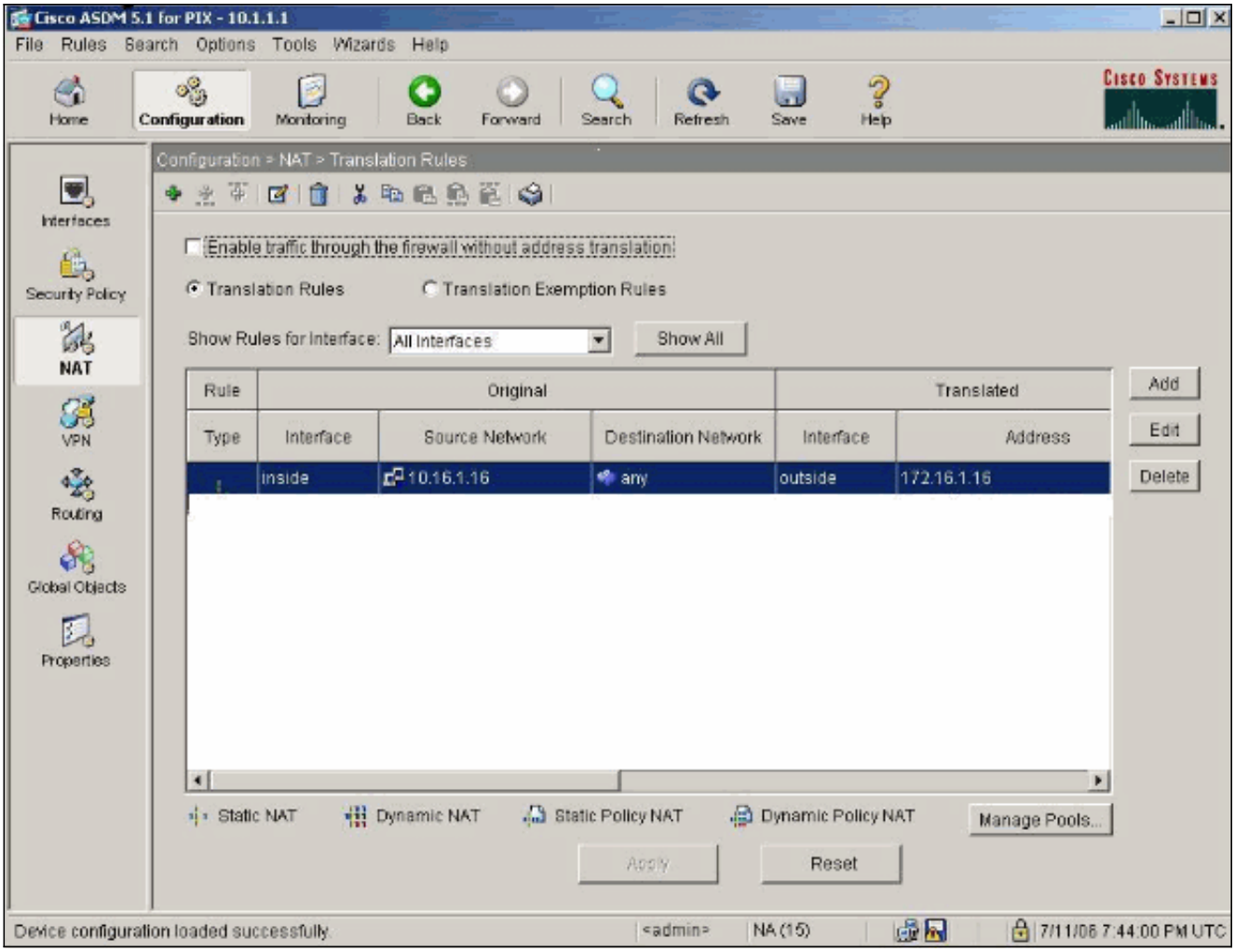
## Использование списков управления доступом (ACL) в PIX версий 7.0 и выше

Для использования ACL в программном обеспечении PIX версии 7.0 и выше выполните следующие действия.

1. Если включено управление NAT, определите статическую трансляцию адресов внутреннего веб-сервера во внешние/глобальные адреса.
   ```
   static (inside, outside) 172.16.1.16 10.16.1.16
   ```
2. Определите хосты, которые могут подключаться к веб-серверу или FTP-серверу, и соответствующие порты.
   ```
   access-list 101 permit tcp any host 172.16.1.16 eq www access-list 101 permit tcp host 192.168.1.1 host 172.16.1.16 eq ftp
   ```
3. Примените ACL к выходному интерфейсу.
   ```
   access-group 101 in interface outside
   ```
4. Чтобы создать это статическое преобразование с использованием ASDM, выберите Configuration (Конфигурация) > Features (Функции) > NAT и нажмите Add (Добавить).
5. Выберите inside в качестве исходного интерфейса и введите внутренний адрес, для которого нужно создать статическое преобразование.
6. Выберите Static (Статический) и введите в поле IP-адреса внешний адрес, который нужно преобразовать. Нажмите кнопку
   OK.




7. Преобразование будет отображено в поле Translation Rules (Правила преобразования) в разделе Configuration (Конфигурация) > Features (Функции) > NAT > Translation Rules (Правила
преобразования).




8. Для ввода записей access-list руководствуйтесь процедурой запрета доступа внутренних узлов к внешним сетям.**Примечание:** Будьте осторожны при реализации этих команд. **Команда access-list 101 permit ip any any разрешит для любого узла из недоверенной сети доступ к любому узлу в доверенной сети по протоколу IP при условии наличия действующего преобразования.**

## Отключение NAT для определенных узлов/сетей

**Если используется управление NAT, во внутренней сети имеются публичные адреса и требуется разрешить этим конкретным внутренним узлам выход во внешнюю сеть без преобразования, то можно отключить для этих узлов NAT при помощи команд nat 0 или static.**

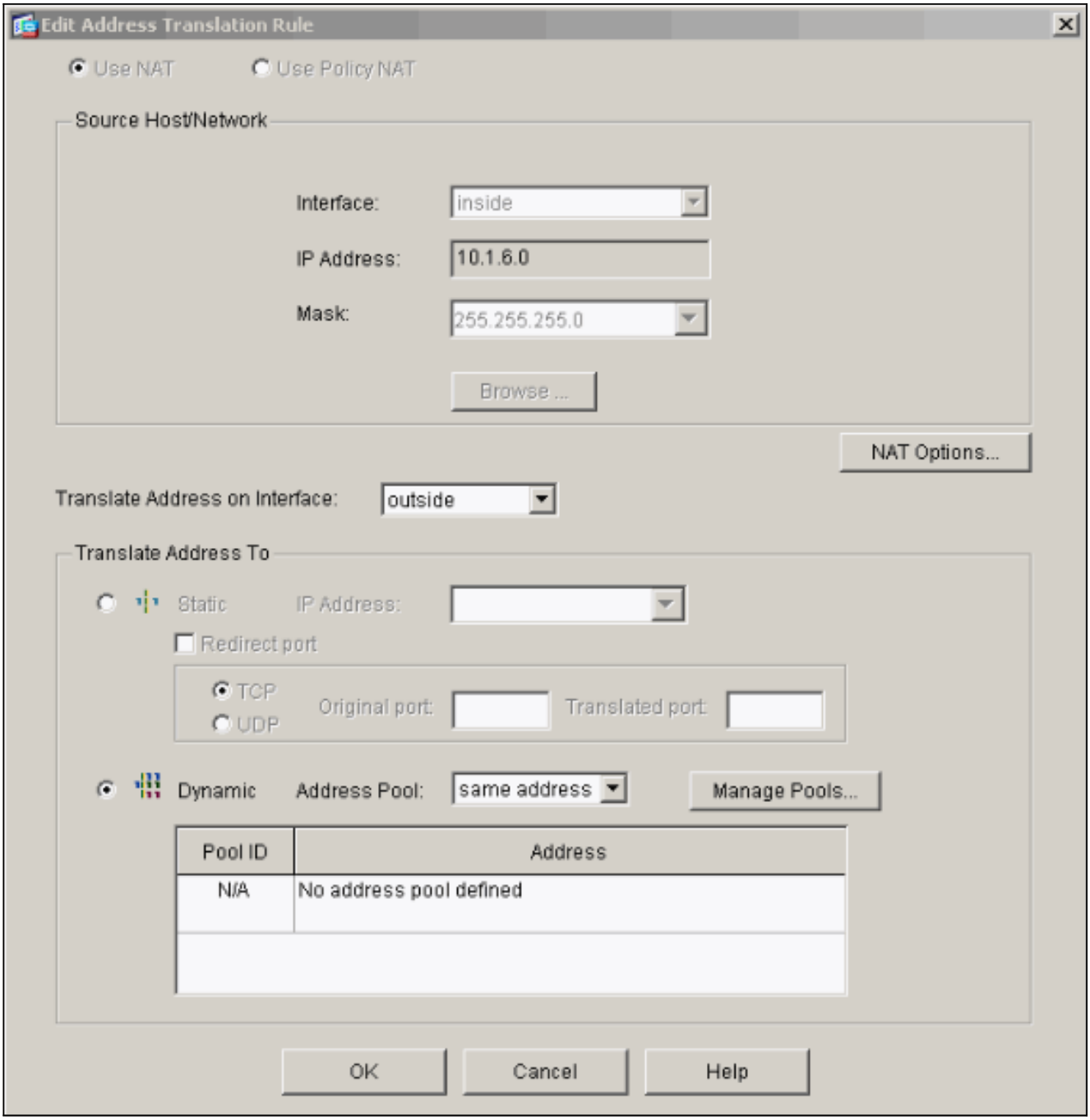
**Ниже приведен пример команды nat:**

```
nat (inside) 0 10.1.6.0 255.255.255.0
```

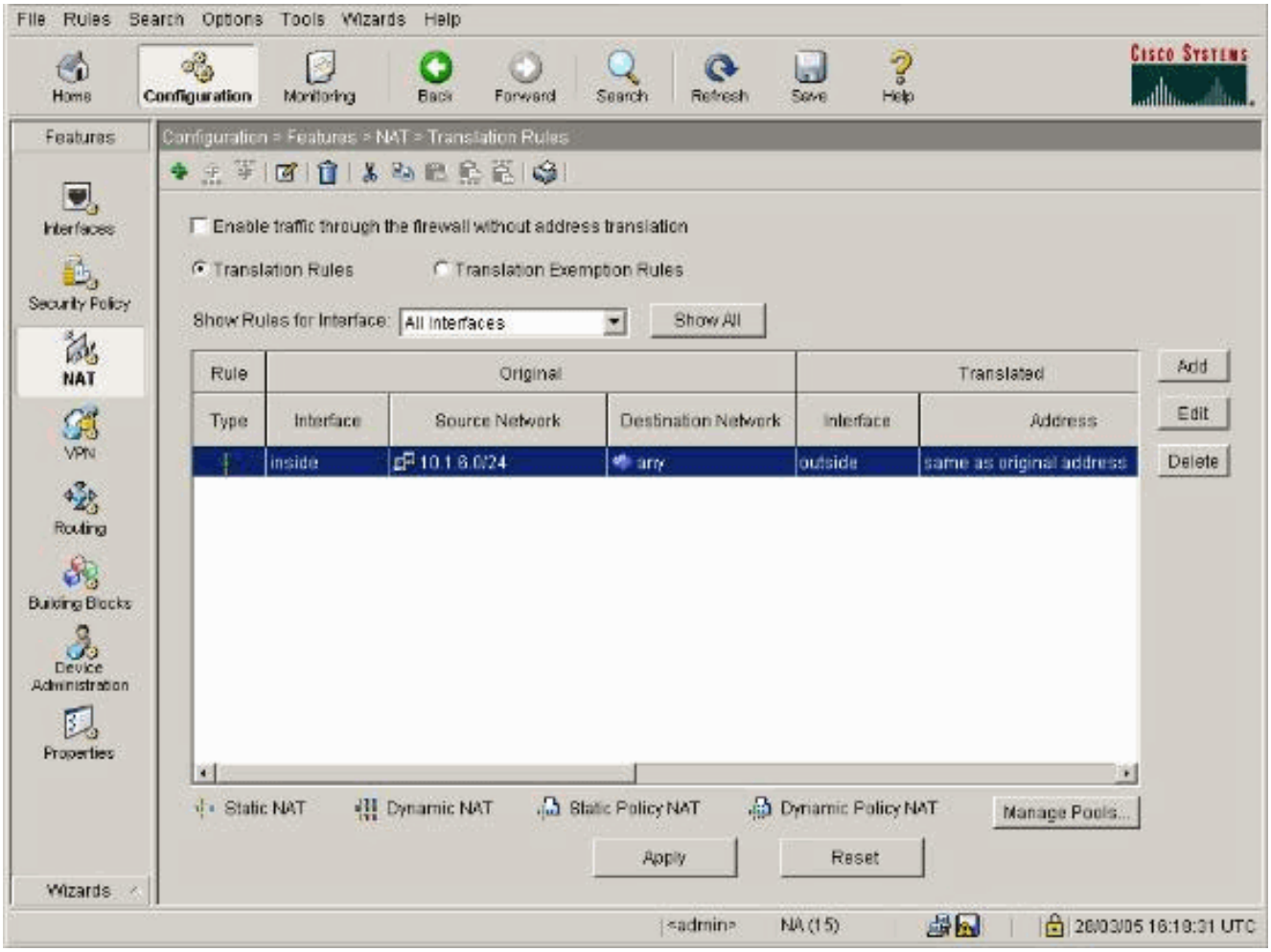
Чтобы запретить NAT для определенных узлов/сетей с использованием системы управления ASDM, выполните следующие действия.

1. **ВыберитеConfiguration (Конфигурация) > Features (Функции) > NAT и щелкните Add (Добавить).**
2. **В качестве исходного интерфейса выберите inside (внутренний), затем введите внутренний адрес/сеть для создания статического преобразования.**
3. **Укажите Dynamic (Динамический) и выберите такой же адрес для пула адресов.**

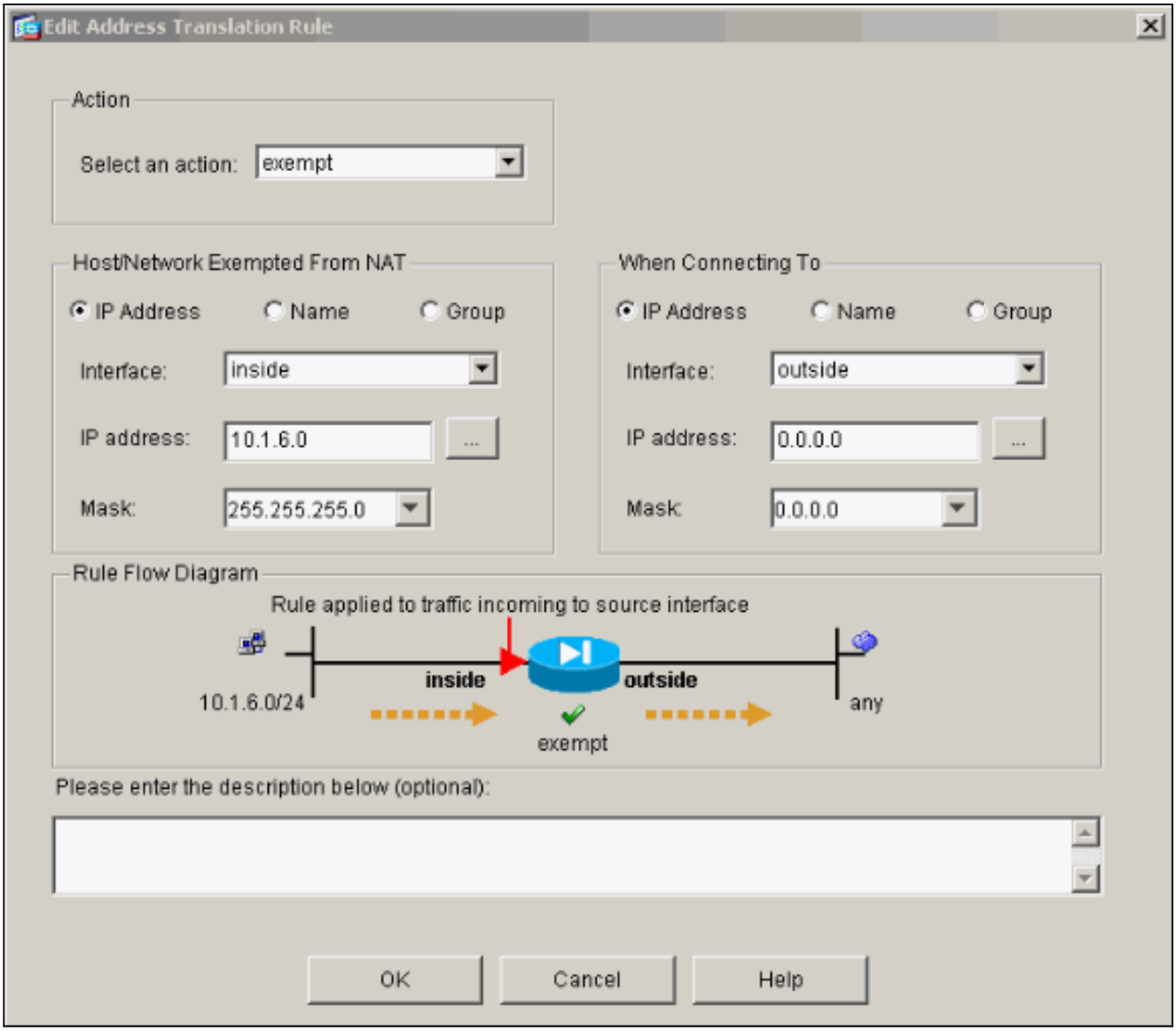
Нажмите кнопку
ОК.



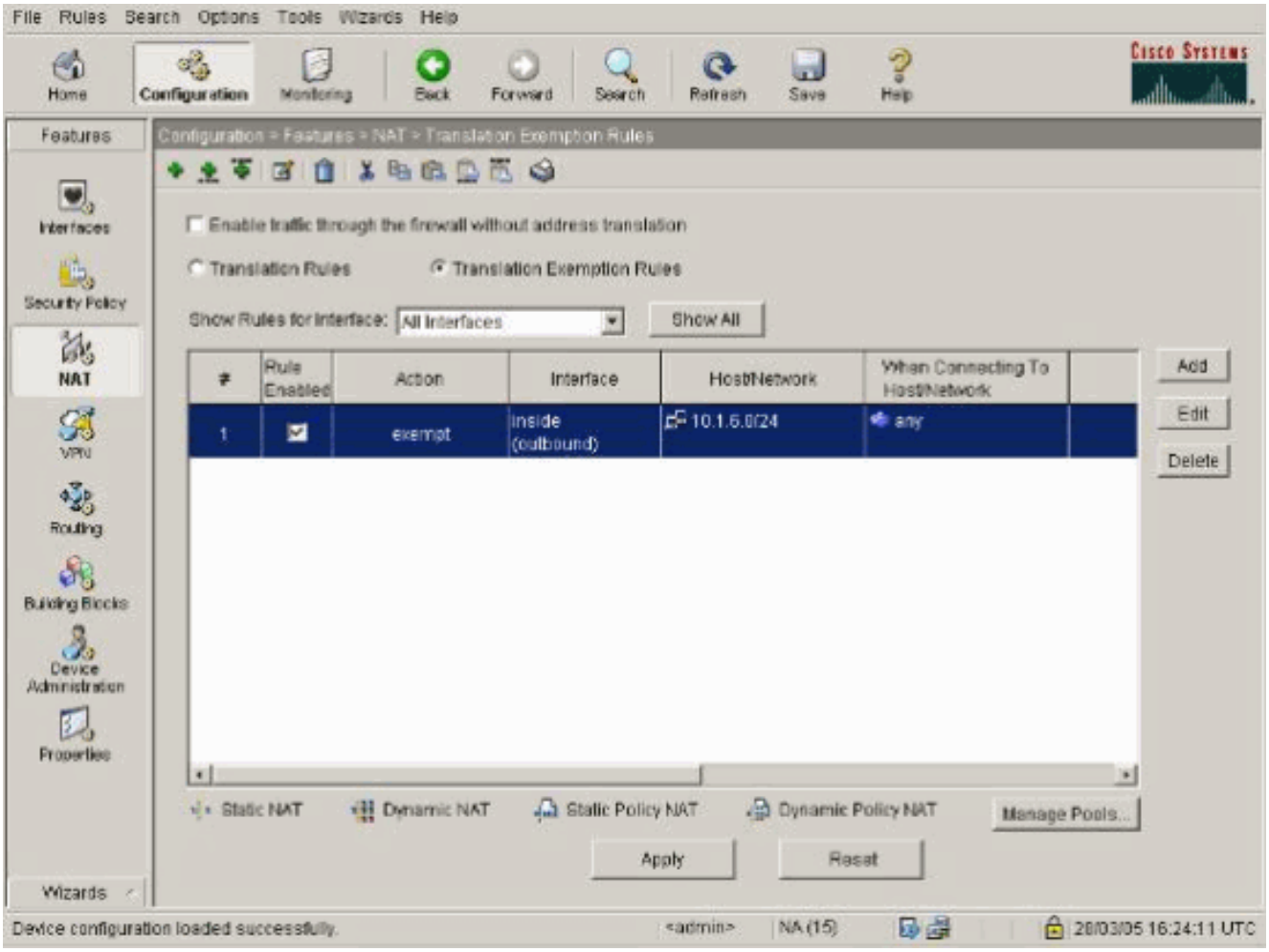

4. При выборе Configuration (Конфигурация) > Features (Функции) > NAT > Translation Rules (Правила преобразования) новое правило будет присутствовать в списке правил преобразования.



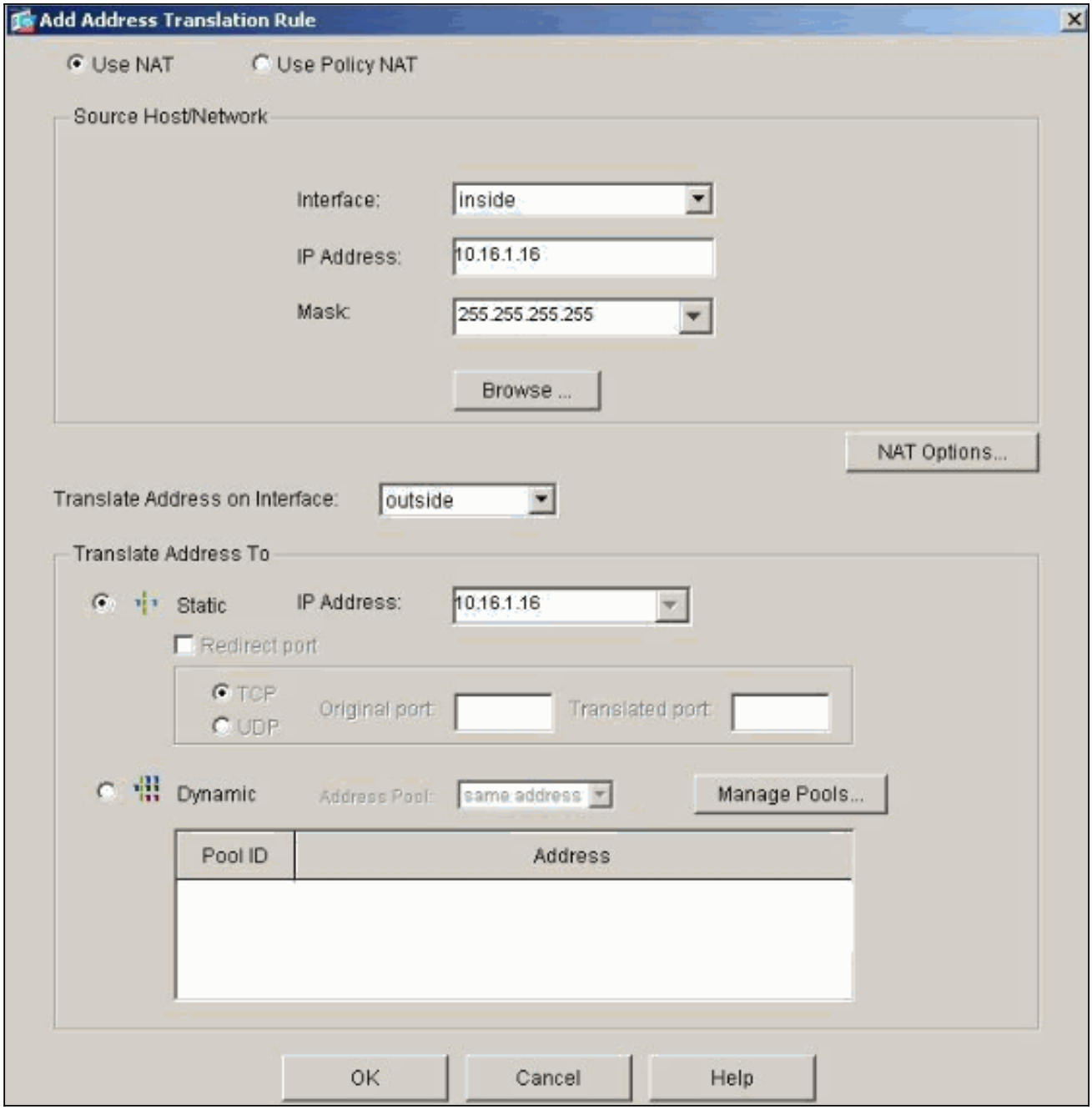

5. В случае использования списков управления доступом, позволяющих более точно регулировать трафик, не подлежащий преобразованию (на основе источника/адресата), применяйте следующие команды.
   ```
   access-list 103 permit ip 10.1.6.0 255.255.255.0 any nat (inside) 0 access-list 103
   ```
6. **В ASDM выберите Configuration (Конфигурация) > Features (Функции) > NAT > Translation Rules (Правила преобразования).**
7. **Выберите Translation Exemption Rules (Исключения из правил преобразования) и щелкните Add (Добавить).**Этот пример показывает, как исключить из преобразования трафик для любых адресатов, исходящий из подсети 10.1.6.0/24.



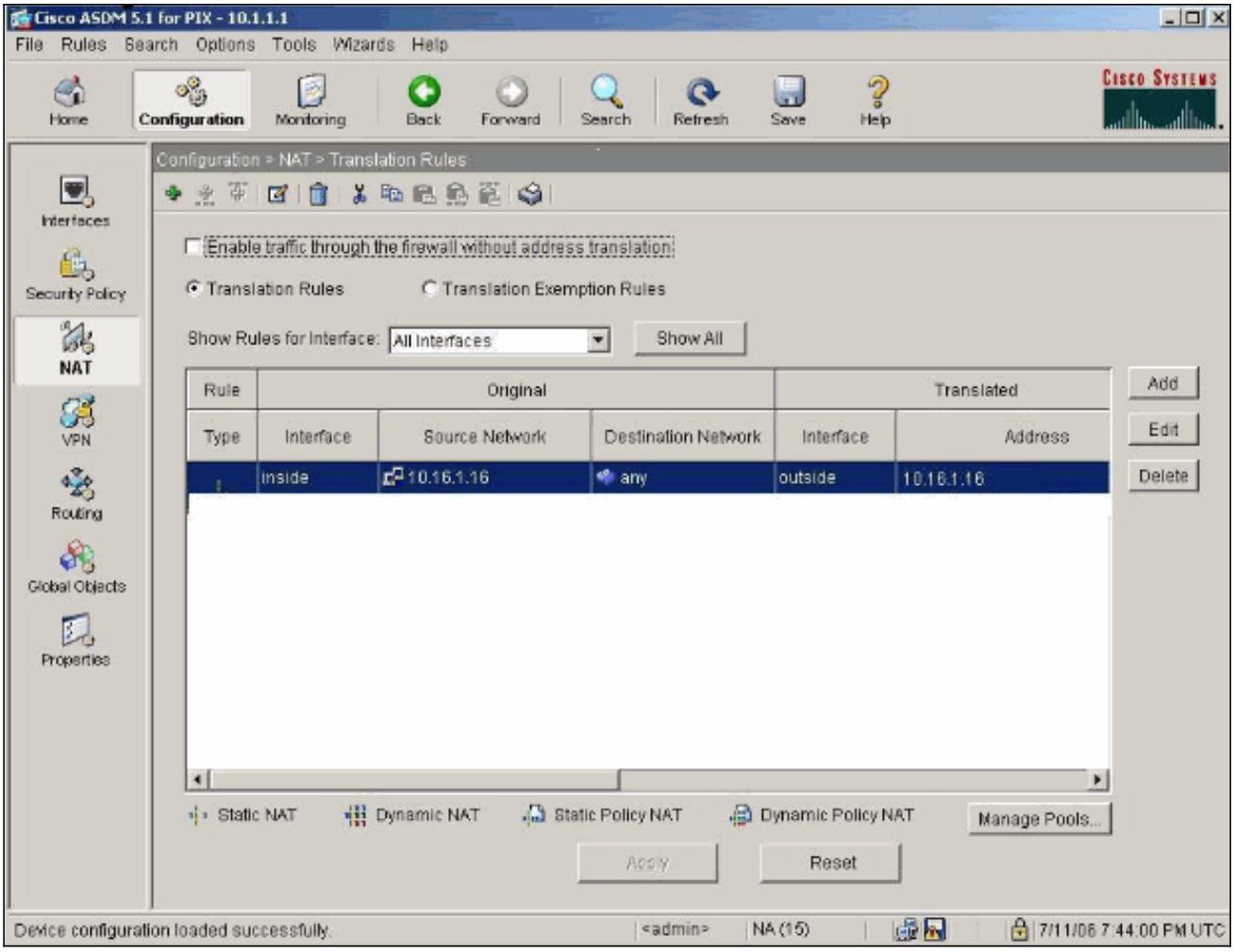

8. Для просмотра новых правил выберите Configuration (Конфигурация) > Features (Функции) > NAT > Translation Exemption Rules (Исключения из правил преобразования).




9. **Команда static для веб-сервера примет вид, показанный в этом примере.**
   ```
   static (inside, outside) 10.16.1.16 10.16.1.16
   ```
10. **В ASDM выберите Configuration (Конфигурация) > Features (Функции) > NAT > Translation Rules (Правила преобразования).**
11. **Выберите Translation Exemption Rules (Исключения из правил преобразования) и щелкните Add (Добавить). Введите сведения об адресе источника и выберите Static (Статический).** Повторите введенный адрес в поле IP Address (IP-адрес).




12. Преобразование будет отображено в поле Translation Rules (Правила преобразования) в разделе Configuration (Конфигурация) > Features (Функции) > NAT > Translation Rules (Правила преобразования).




13. В случае использования списков ACL применяйте следующие команды.
**`access-list 102 permit tcp any host 10.16.1.16 eq www access-group 102 in interface outside`** Дополнительные сведения о настройке списков ACL в ASDM см. в разделе Запрет доступа внутренних узлов к внешним сетям настоящего документа.**Обратите внимание на различие между использованием параметра nat 0 при указании сети/маски и использованием списка управления доступом с сетью/маской, разрешающего инициировать соединения только изнутри. Применение списков управления доступом с параметром nat 0 позволяет разрешить установление соединений при входящем или исходящем трафике.** Интерфейсы PIX должны находиться в разных подсетях, чтобы избежать проблем с доступностью.

## Перенаправление (переадресация) портов с использованием команд Static

В PIX 6.0 была добавлена функция перенаправления портов, чтобы разрешить внешним пользователям подключаться к конкретному IP-адресу/порту и заставить PIX перенаправить трафик соответствующему внутреннему серверу/порту. **Команда static была изменена.** Общий адрес может быть уникальным адресом, общим адресом исходящего PAT или общим с внешним интерфейсом. Эта функция доступна в PIX 7.0.

**Примечание:** Из-за ограничений длины, команды показывают на двух линиях.

**`static`** *`[(internal_if_name, external_if_name)] {global_ip|interface}local_ip [netmask mask] [max_conns [emb_limit [norandomseq]]]`* **`static`** *`[(internal_if_name, external_if_name)] {tcp|udp}`*

*{global_ip|interface} global_port local_ip local_port [netmask mask] [max_conns [emb_limit [norandomseq]]]*

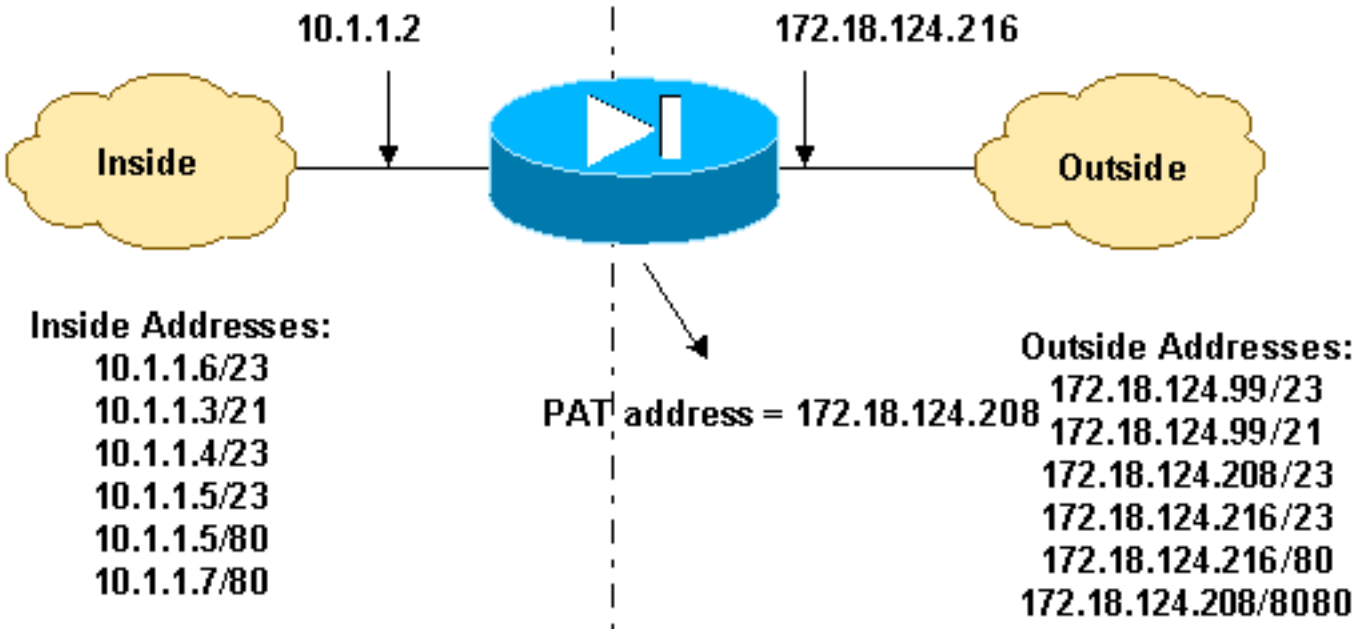
**Примечание:** Если статическое NAT использование внешний IP (global_IP) адрес для перевода, то это могло бы вызвать трансляцию. **По этой причине вместо IP-адреса в статическом преобразовании следует указывать ключевое слово interface.**

В примере сети участвуют следующие перенаправления (переадресация) портов:

- Внешние пользователи направляют запросы Telnet на уникальный IP-адрес 172.18.124.99, а PIX перенаправляет их на 10.1.1.6.
- Внешние пользователи направляют FTP-запросы на уникальный IP-адрес 172.18.124.99, затем PIX перенаправляет их на 10.1.1.3.
- Внешние пользователи прямого подключения Telnet запрашивают PAT-адрес 172.18.124.208, который PIX перенаправляет на 10.1.1.4.
- Внешние пользователи направляют на PIX запрос Telnet на внешний IP-адрес 172.18.124.216, который PIX перенаправляет на 10.1.1.5.
- Внешние пользователи направляют запросы HTTP на IP-адрес 172.18.124.216, внешний по отношению к PIX, а PIX перенаправляет эти запросы на 10.1.1.5.
- Внешние пользователи направляют запросы HTTP-порта 8080 на PAT-адрес 172.18.124.208, которые PIX перенаправляет на 10.1.1.7, порт 80.

В этом примере также блокируется доступ некоторых внутренних пользователей к внешним ресурсам с помощью списка ACL 100. Это действие является необязательным. Весь исходящий трафик разрешен при отсутствии ACL.

## Схема сети — перенаправление портов




## Частичная конфигурация PIX — перенаправление портов

Этот фрагмент конфигурации иллюстрирует использование статического перенаправления (переадресации) портов. См. схему сети с перенаправлением (переадресацией) портов.

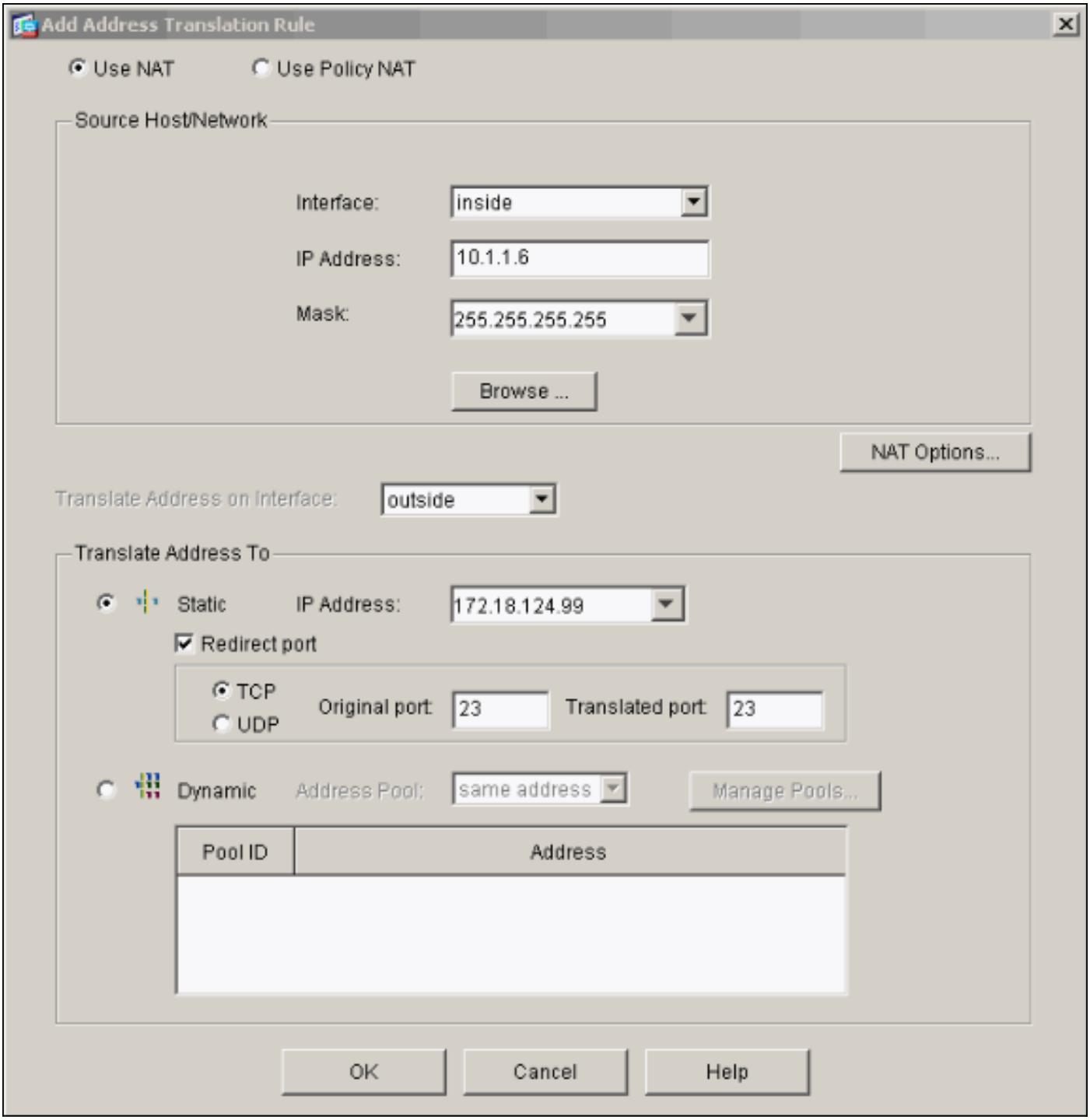
| **Фрагмент конфигурации PIX 7.x. Перенаправление (переадресация) портов** |
| --- |

```
fixup protocol ftp 21
!--- Use of an outbound ACL is optional. access-list 100
permit tcp 10.1.1.0 255.255.255.128 any eq www access-
list 100 deny tcp any any eq www access-list 100 permit
tcp 10.0.0.0 255.0.0.0 any access-list 100 permit udp
10.0.0.0 255.0.0.0 host 172.18.124.100 eq domain access-
list 101 permit tcp any host 172.18.124.99 eq telnet
access-list 101 permit tcp any host 172.18.124.99 eq ftp
access-list 101 permit tcp any host 172.18.124.208 eq
telnet access-list 101 permit tcp any host
172.18.124.216 eq telnet access-list 101 permit tcp any
host 172.18.124.216 eq www access-list 101 permit tcp
any host 172.18.124.208 eq 8080 interface Ethernet0
nameif outside security-level 0 ip address
172.18.124.216 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.1.1.2
255.255.255.0 ! global (outside) 1 172.18.124.208 nat
(inside) 1 0.0.0.0 0.0.0.0 0 0 static (inside,outside)
tcp 172.18.124.99 telnet 10.1.1.6 telnet netmask
255.255.255.255 0 0 static (inside,outside) tcp
172.18.124.99 ftp 10.1.1.3 ftp netmask 255.255.255.255 0
0 static (inside,outside) tcp 172.18.124.208 telnet
10.1.1.4 telnet netmask 255.255.255.255 0 0 static
(inside,outside) tcp interface telnet 10.1.1.5 telnet
netmask 255.255.255.255 0 0 static (inside,outside) tcp
interface www 10.1.1.5 www netmask 255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.208 8080 10.1.1.7
www netmask 255.255.255.255 0 0 !--- Use of an outbound
ACL is optional. access-group 100 in interface inside
access-group 101 in interface outside
```

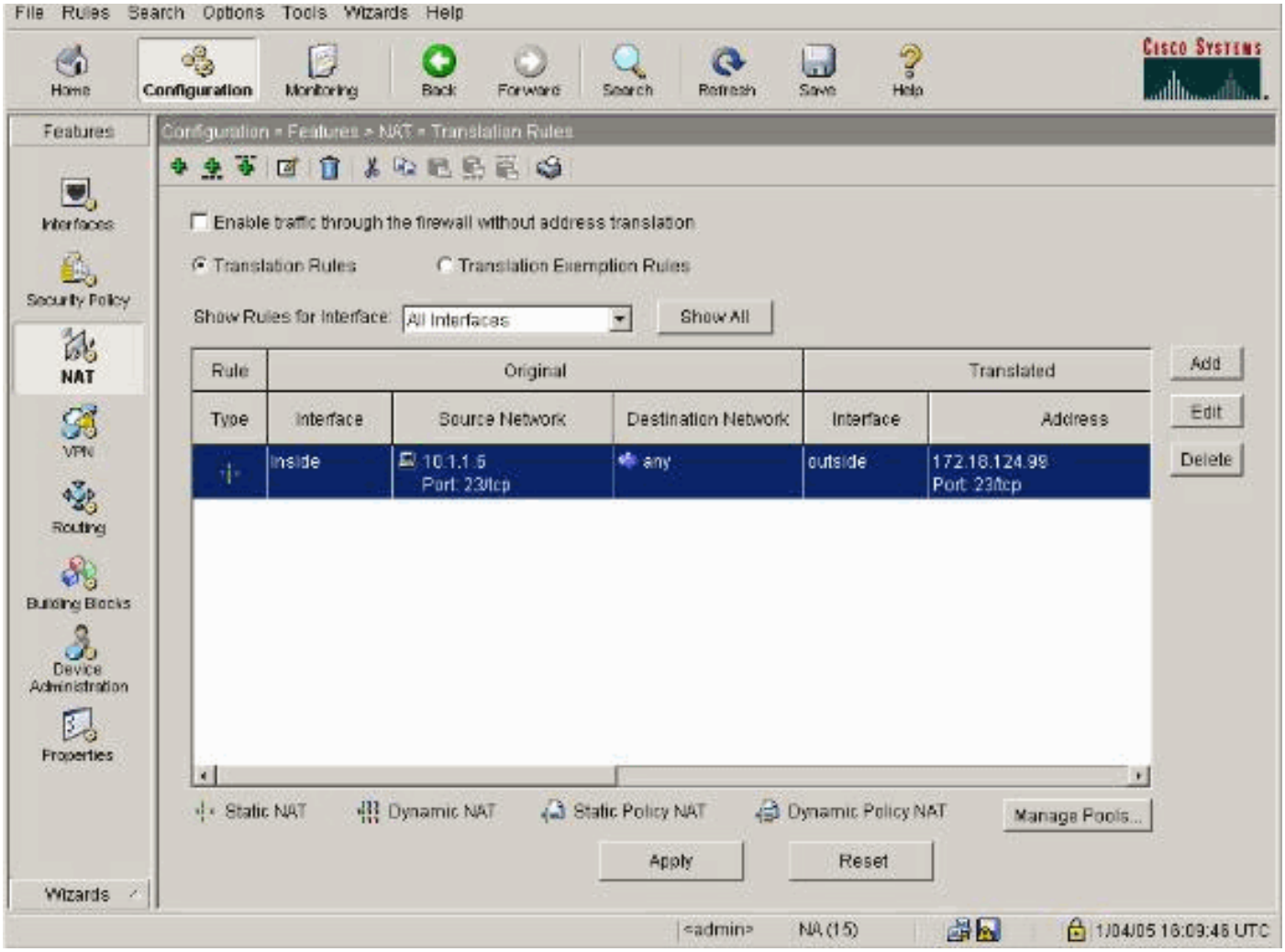
**Примечание:** Если PIX/ASA настроен с **командой sysopt noproxyarp outside**, то это не позволяет межсетевому экрану делать proxyarp и статические преобразования NAT в PIX/ASA. **Для решения этой проблемы удалите команду sysopt noproxyarp outside из конфигурации PIX/ASA и обновите записи ARP, используя необоснованный запрос ARP.** Это позволит успешно использовать статические записи NAT.

Эта процедура – пример конфигурации перенаправления (переадресации) портов, в которой внешним пользователям разрешено направлять прямые запросы Telnet на уникальный IP-адрес 172.18.124.99, которые PIX переадресует на 10.1.1.6.

1. **В ASDM выберите Configuration (Конфигурация) > Features (Функции) > NAT > Translation Rules (Правила преобразования).**
2. **Выберите Translation Exemption Rules (Исключения из правил преобразования) и щелкните Add (Добавить).**
3. В поле Source Host/Network (Исходный узел/сеть) введите параметры внутреннего IP-адреса.
4. **В поле Translate Address To (Целевой адрес преобразования) выберите Static (Статический), введите внешний IP-адрес и отметьте флажок Redirect port (Перенаправлять порт).**
5. Введите параметры состояния порта до и после преобразования (в этом примере сохраняется порт 23). **Нажмите кнопку OK.**




Преобразование будет отображено в поле Translation Rules (Правила преобразования) в разделе Configuration (Конфигурация) > Features (Функции) > NAT > Translation Rules (Правила преобразования).




## Ограничение числа TCP/UDP-сеансов с использованием команд Static

**Чтобы ограничить число сеансов TCP или UDP с внутренним сервером, размещенным в PIX/ASA, используйте команду static.**

Эта команда определяет максимальное число одновременных соединений TCP и UDP для всей подсети. **По умолчанию это значение равно 0, что означает отсутствие ограничений на число соединений (неиспользуемые соединения закрываются по истечении периода неактивности, настраиваемого командой timeout conn).**). Этот параметр не действует для внешнего преобразования NAT. Устройство адаптивной защиты отслеживает только соединения от более защищенных интерфейсов в сторону менее защищенных интерфейсов.

Ограничение числа полуоткрытых соединений позволяет защититься от DoS-атаки. Устройство безопасности руководствуется предельным числом полуоткрытых соединений для введения в действие функции перехвата TCP, которая защищает внутренние системы от разновидности DoS-атаки, состоящей в насыщении интерфейса пакетами TCP SYN. Полуоткрытое («эмбриональное») соединение – это запрос соединения, в котором не завершен необходимый протокол установления связи между источником и адресатом. Этот параметр не действует для внешнего преобразования NAT. Функция перехвата TCP применяется только к узлам или серверам с более высоким уровнем безопасности. В случае задания предельного числа полуоткрытых соединений для внешнего преобразования NAT это значение будет игнорироваться.

Пример:

```
ASA(config)#static (inside,outside) tcp 10.1.1.1 www 10.2.2.2 www tcp 500 100 !--- The maximum
number of simultaneous tcp connections the local IP !--- hosts are to allow is 500, default is 0
which means unlimited !--- connections. Idle connections are closed after the time specified !--
- by the timeout conn command !--- The maximum number of embryonic connections per host is 100.
```

**%PIX-3-201002: Too many connections on {static|xlate} global_address! econns nconns**

Это сообщение относится к соединениям. Оно появляется в журнале в случае превышения максимального числа соединений с указанным статическим адресом. Переменная econns задает максимальное число полуоткрытых соединений, а nconns – максимальное число соединений, разрешенных для команд static или xlate.

**Рекомендуется при помощи команды show static проверить предел, установленный для соединений со статическим адресом.** Этот предел настраивается.

**%ASA-3-201011: Ограничение соединения превысило 1000/1000 для входящего пакета от 10.1.26.51/2393 до 10.0.86.155/135 на интерфейсе Снаружи**

Это сообщение об ошибках происходит из-за идентификатора ошибки Cisco CSCsg52106 (только зарегистрированные клиенты). Для получения дополнительных сведений обратитесь к документации по данной ошибке.

## Список управления доступом с ограничением по времени

Сама по себе установка интервала времени не ограничивает доступ к устройству. **Команда time-range определяет только интервал времени.** Заданный интервал можно применить к правилам обработки трафика или действиям.

**Для реализации ACL с ограничением по времени задайте конкретное время суток и дни недели командой time-range. Затем при помощи команды with the access-list extended time-range привяжите временной интервал к списку управления доступом.**

Временной интервал задается для показаний системных часов устройства защиты. Однако эта функция работает наилучшим образом вместе с синхронизацией по протоколу NTP.

**После создания интервала времени и входа в режим настройки интервала можно определить его параметры командами absolute (абсолютный) и periodic (периодический). Чтобы восстановить настройки по умолчанию для ключевых слов «absolute» и «periodic» команды time-range, используйте команду default в режиме настройки интервала времени.**

**Для реализации ACL с ограничением по времени задайте конкретное время суток и дни недели командой time-range. Затем при помощи команды with the access-list extended свяжите интервал со списком управления доступом.** В следующем примере со списком управления доступом «Sales» связывается интервал «New York Minute»:

В этом примере создается интервал времени под названием «New York Minute» и происходит вход в режим настройки интервала:

```
hostname(config)#time-range New_York_Minute hostname(config-time-range)#periodic weekdays 07:00
to 19:00 hostname(config)#access-list Sales line 1 extended deny ip any any time-range
New_York_Minute hostname(config)#access-group Sales in interface inside
```

## Информация, которую необходимо собрать при обращении в службу технической поддержки

| |
|---|
| **Если после выполнения перечисленных выше действий вам по-прежнему требуется помощь Центра технической поддержки Cisco (TAC), соберите указанные ниже сведения для устранения неполадок, связанных с устройством защиты PIX.** |
| • Описание проблемы и соответствующие сведения о топологии.<br>• Меры, предпринятые для устранения проблемы перед обращением в службу поддержки.<br>• **Выходные данные команды show tech-support.**<br>• **Выходные данные команды show log после запуска команды отладки logging buffered debugging или снимки консоли, демонстрирующие проблему (при их наличии).**<br>Присоедините собранные данные к запросу в простом текстовом формате (.txt), не архивируя файл. Информацию можно приложить к запросу путем загрузки с помощью служебной программы TAC Service Request Tool (только для зарегистрированных пользователей). Если средство TAC Service Request Tool недоступно (доступ к нему предоставляется только зарегистрированным пользователям), данные можно отправить как вложение в сообщение электронной почты по адресу attach@cisco.com, указав в теме сообщения номер запроса. |

## Дополнительные сведения

- Страница поддержки устройства безопасности PIX Security Appliance
- Справочник по командам PIX
- Поиск и устранение неисправностей и предупреждения Cisco Adaptive Security Device Manager (ASDM)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация