Настройте переадресацию портов версии ASA 9.x с NAT

Содержание

Введение

Этот документ объясняет, как настроить Перенаправление порта (Передача) и Трансляция внешнего сетевого адреса (NAT) функции в Версии программного обеспечения 9.x Устройства адаптивной защиты (ASA) с использованием CLI или Менеджера устройств адаптивной безопасности (ASDM) (ASDM).

См. Руководство по конфигурации ASDM Межсетевого экрана Серии Cisco ASA для дополнительных сведений.

Предварительные условия

Требования

См. Управляющего доступ Настройки, чтобы позволить устройству быть настроенным ASDM.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

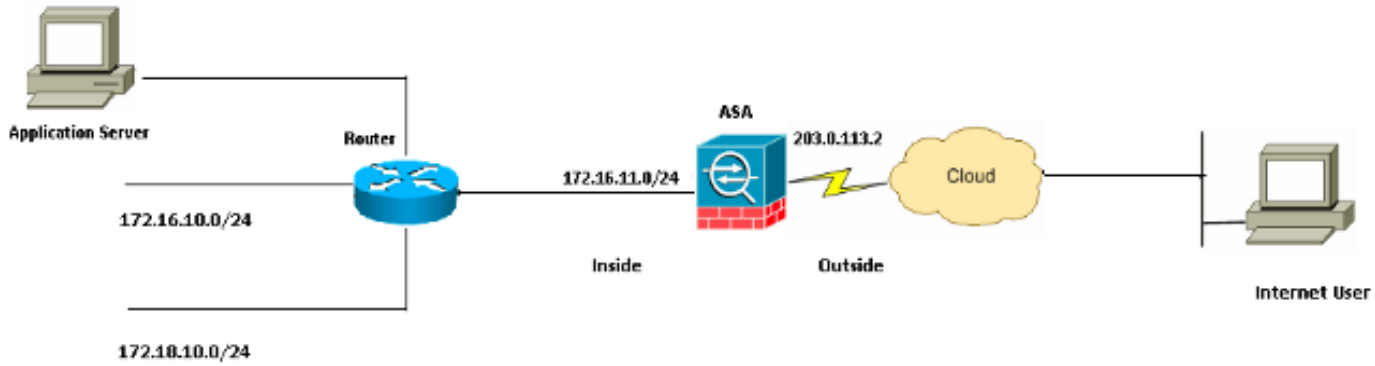
обеспечения и оборудования:

- Версия программного обеспечения 9.x Устройства безопасности Серии Cisco ASA 5525 и позже
- Версия 7.x ASDM и позже

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.

Настройка

Схема сети



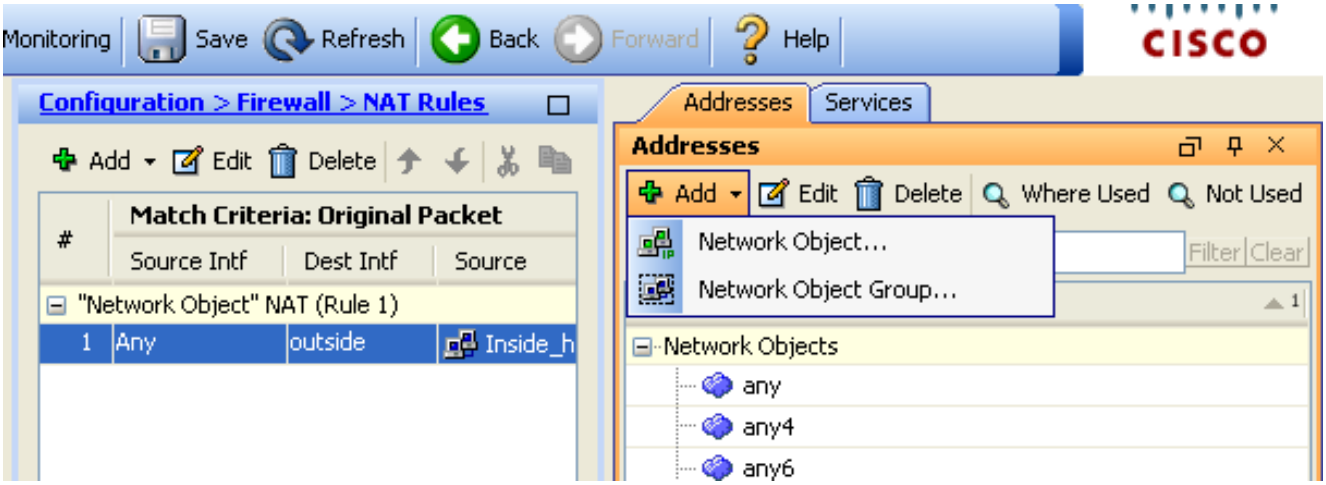
Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

Позвольте доступ для внутренних узлов внешним сетям с PAT

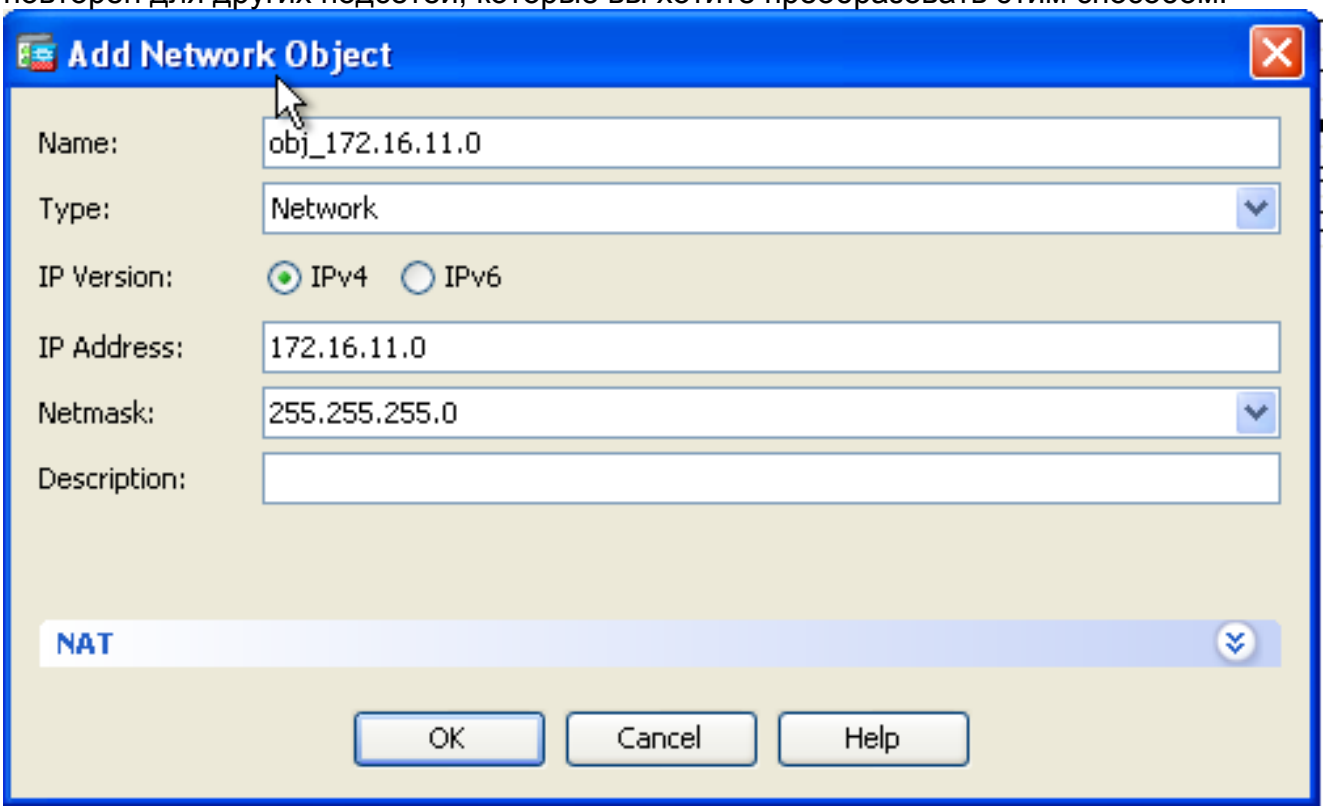
Если вы хотите, чтобы внутренние хосты совместно использовали одиночный общий адрес для трансляции, используйте Преобразование адресов портов (PAT). Одна из самых простых конфигураций PAT включает трансляцию всех внутренних хостов для сходства с IP-адресом внешнего интерфейса. Это - типичная конфигурация PAT, которая используется, когда количество маршрутизируемых IP - адресов, доступных от интернет-провайдера, ограничено только некоторыми, или возможно всего один.

Выполните эти шаги для разрешения доступа для внутренних узлов внешним сетям с PAT:

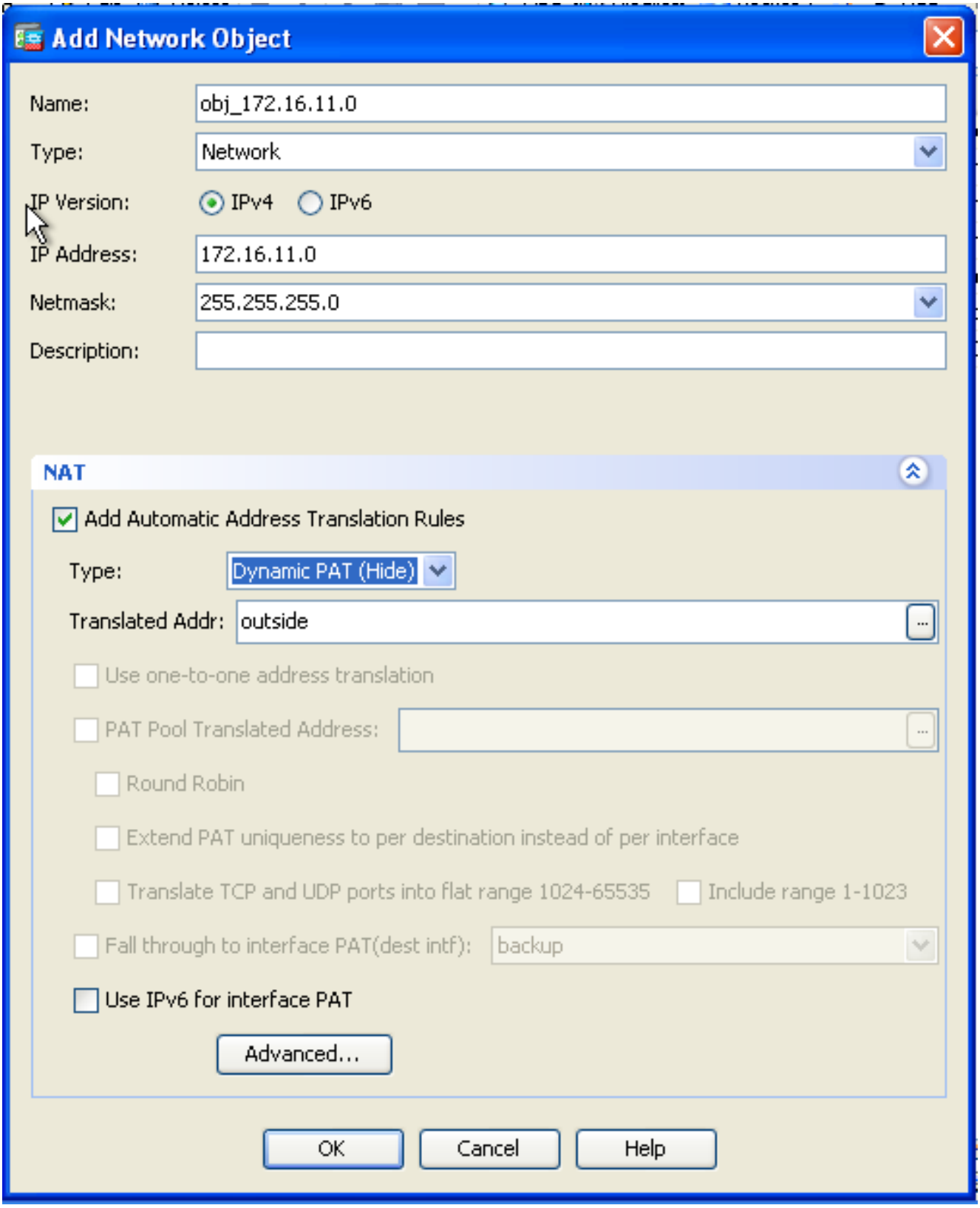
1. Выберите **Configuration> Firewall> NAT Rules**. **Нажмите Add** и затем выберите **Network Object** для настройки правила динамического преобразования сетевых адресов (NAT).



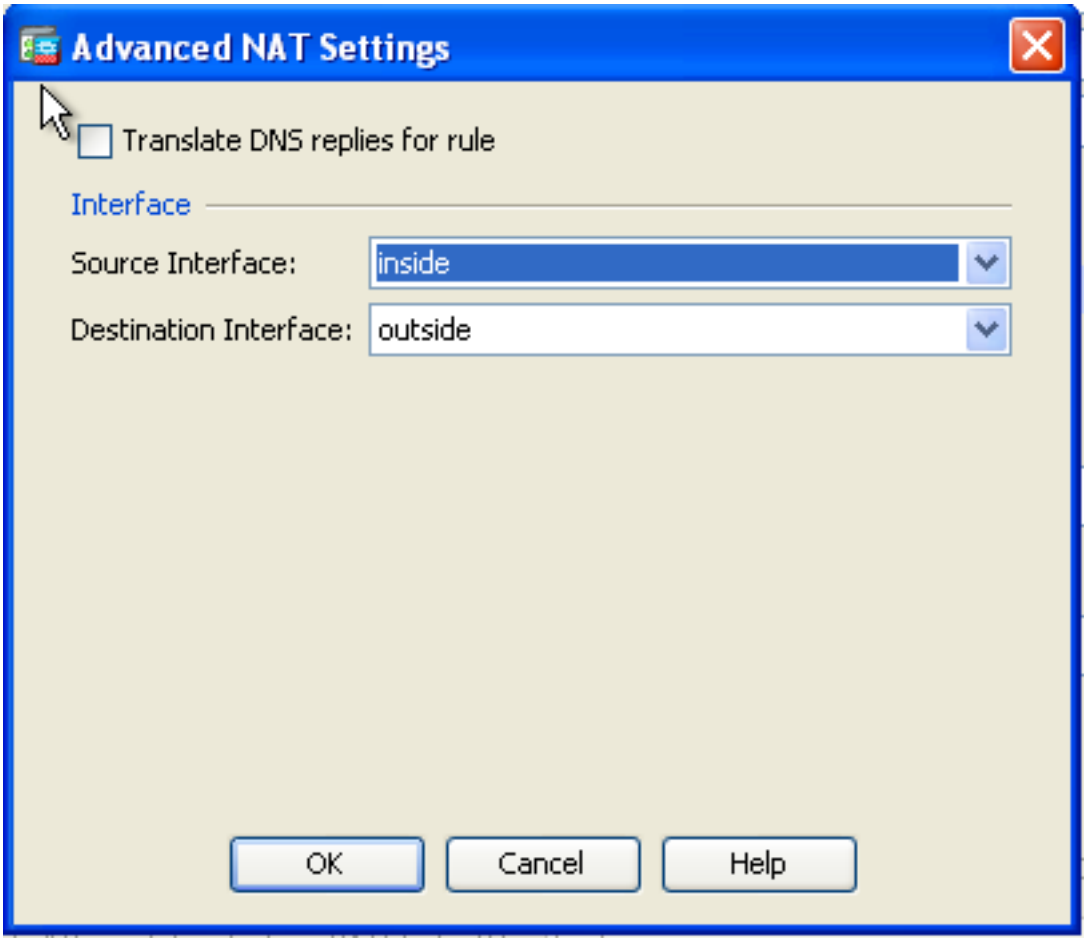
2. Настройте сеть/Хост/Диапазон, для которой требуется **Динамический PAT**. В данном примере была выбрана одна из внутренних подсетей. Этот процесс может быть повторен для других подсетей, которые вы хотите преобразовать этим способом.



3. Разверните NAT. Проверьте флажок **Add Automatic Address Translation Rules**. В выпадающем списке Типа выберите **Dynamic PAT (Hide)**. В поле **Translated Addr** выберите опцию для отражения внешнего интерфейса. **Нажмите кнопку Advanced.**



4. В выпадающих списках Исходного интерфейса и Интерфейса назначения выберите соответствующие интерфейсы. Нажмите **OK** и нажмите **Apply** для изменений для вступления в силу.



Это - эквивалентные выходные данные CLI для этой конфигурации PAT:

```
object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
nat (inside,outside) dynamic interface
```

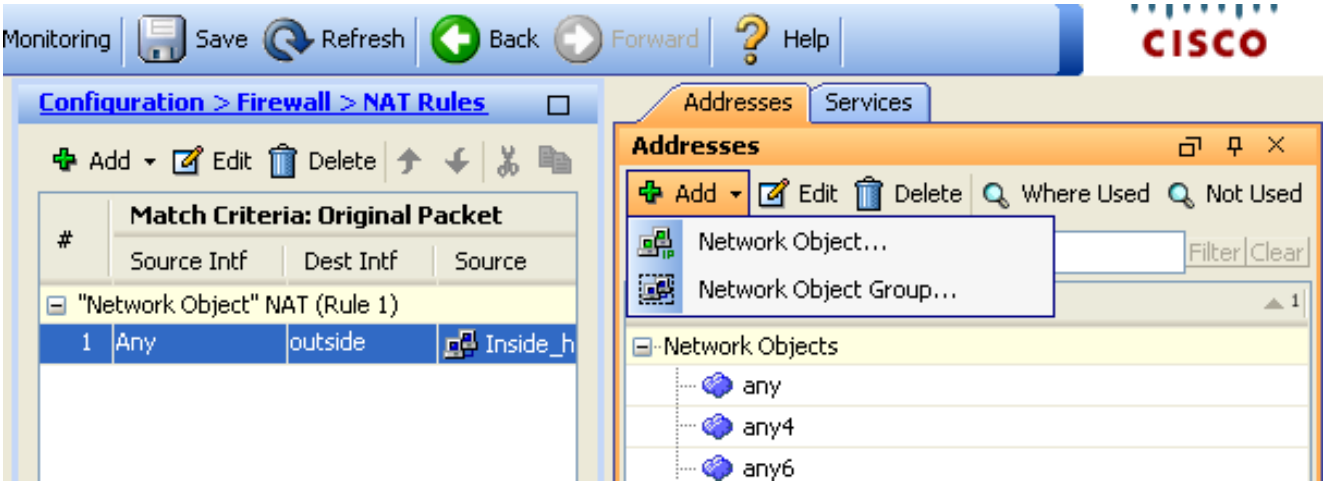
Разрешение доступа внутренних узлов во внешние сети с использованием NAT

Вы могли позволить группе внутренних хостов/сетей обращаться к внешнему миру с конфигурацией правил динамического преобразования сетевых адресов (NAT). В отличие от PAT, Динамический NAT выделяет транслированные адреса от пула адресов. В результате хост сопоставлен с его собственным преобразованным IP-адресом, и два хоста не могут совместно использовать тот же преобразованный IP-адрес.

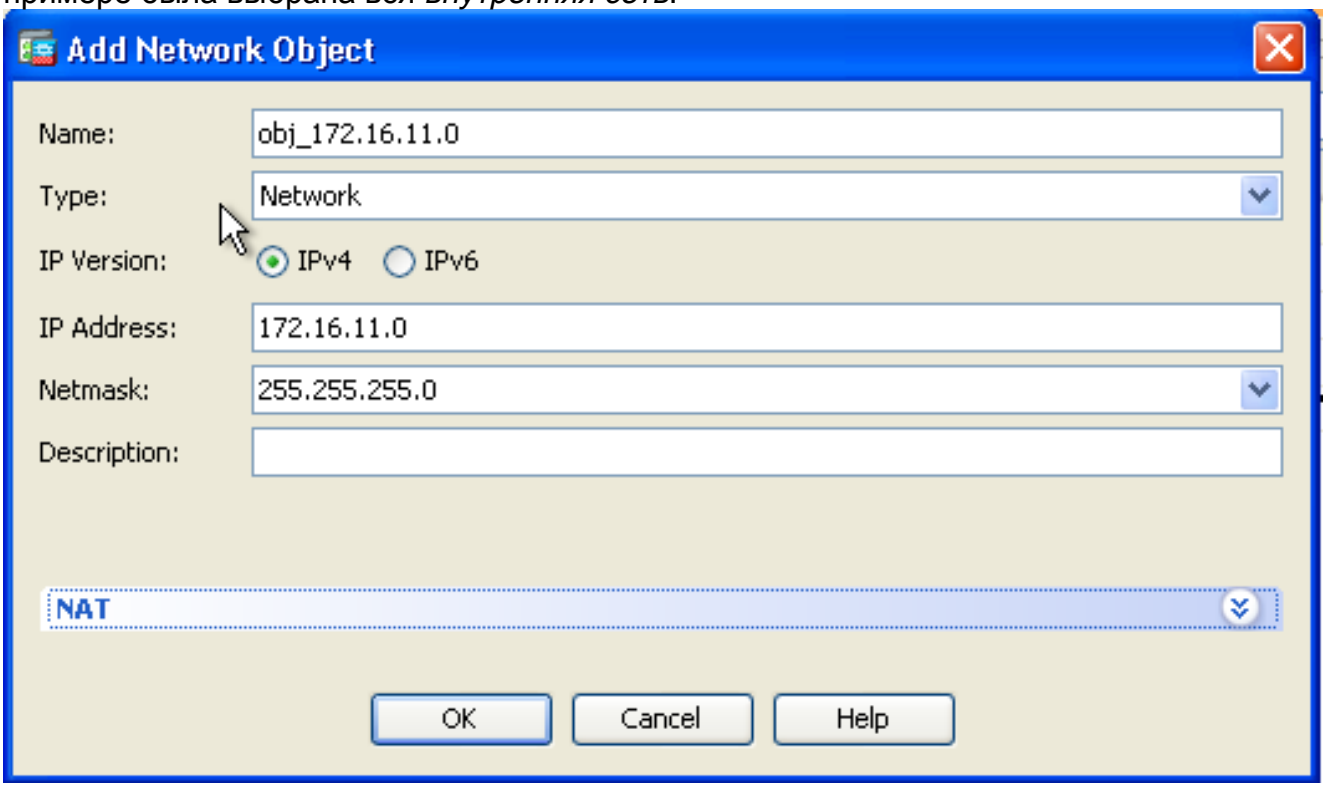
Для выполнения этого необходимо выбрать действительный адрес хостов/сетей, которым предоставят доступ, и они тогда должны быть сопоставлены с пулом преобразованных IP-адресов.

Выполните эти шаги для разрешения доступа для внутренних узлов внешним сетям с NAT:

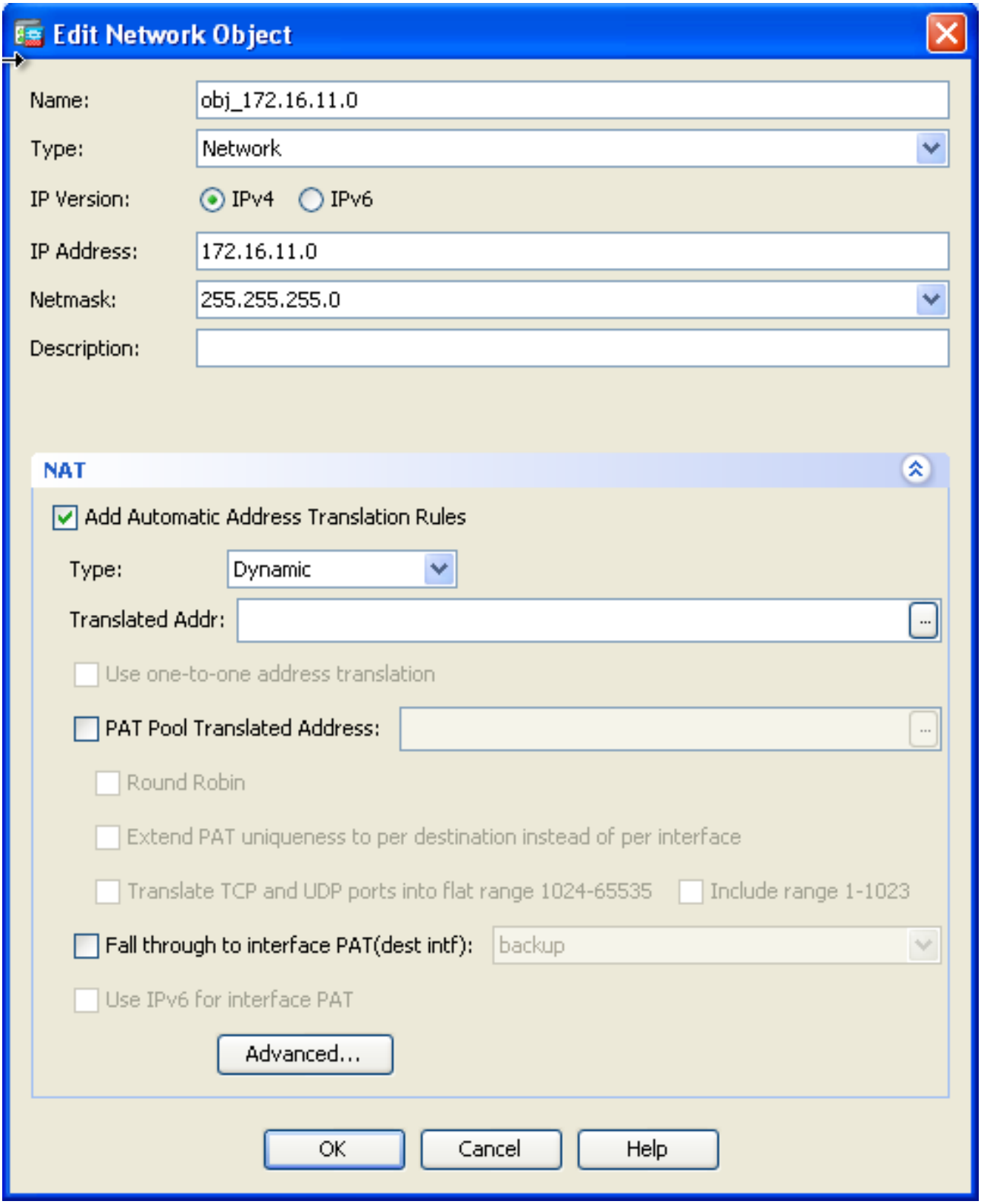
1. Выберите **Configuration> Firewall> NAT Rules**. **Нажмите Add** и затем выберите **Network Object** для настройки правила динамического преобразования сетевых адресов (NAT).



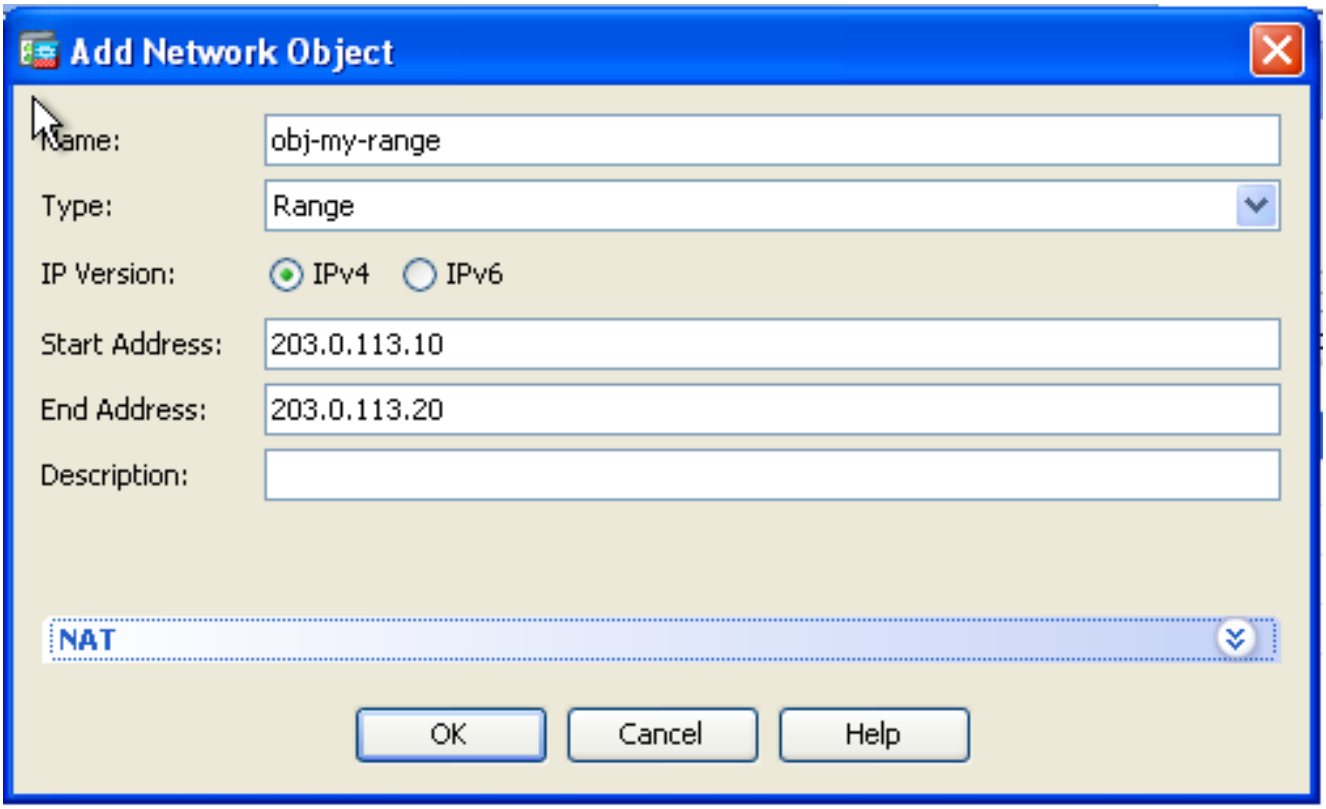
2. Настройте сеть/Хост/Диапазон, для которой требуется Динамический PAT. В данном примере была выбрана вся *внутренняя сеть*.



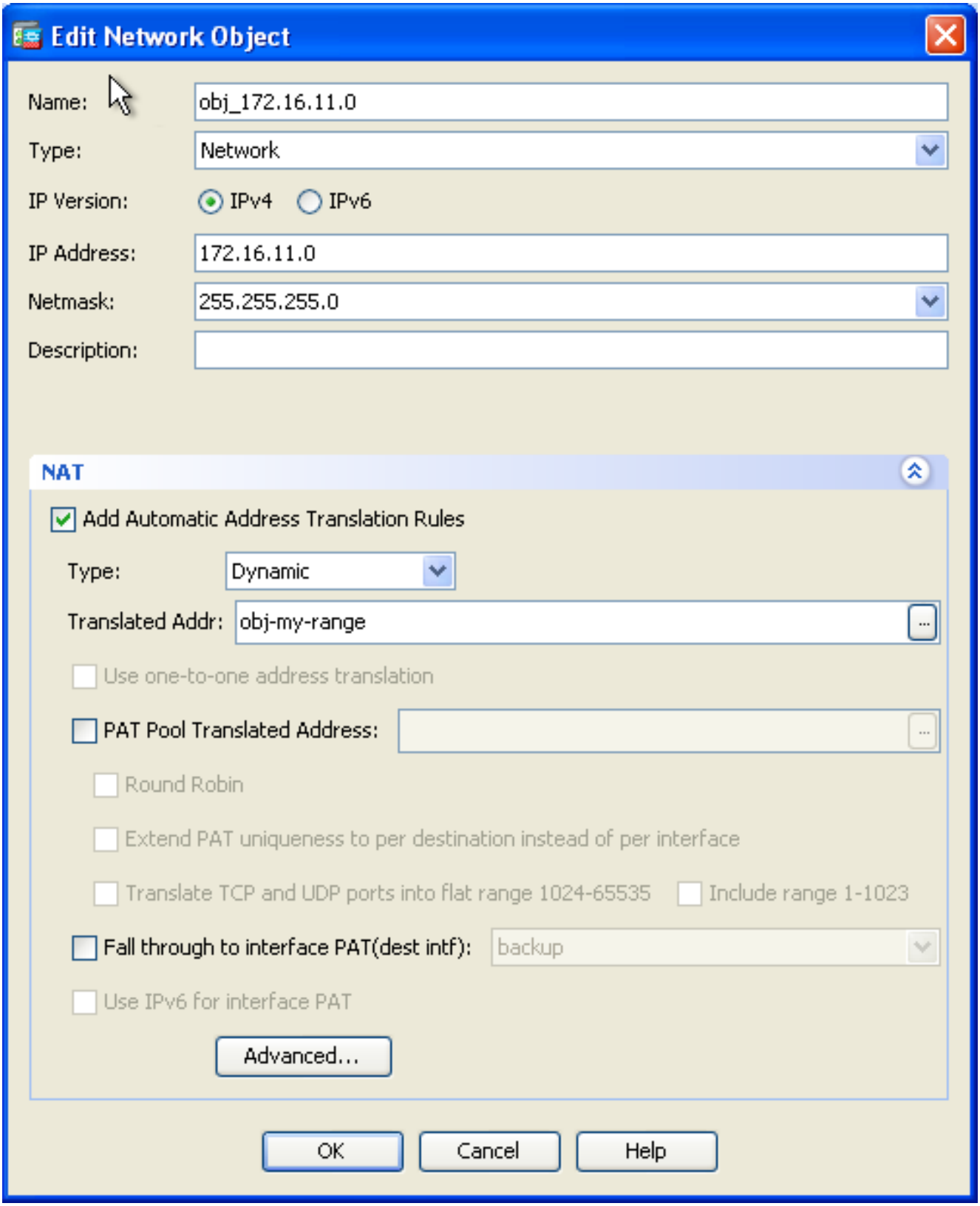
3. Разверните NAT. Проверьте флажок **Add Automatic Address Translation Rules**. В выпадающем списке Типа выберите **Dynamic**. В поле Translated Addr выберите соответствующий выбор. **Нажмите кнопку Advanced.**



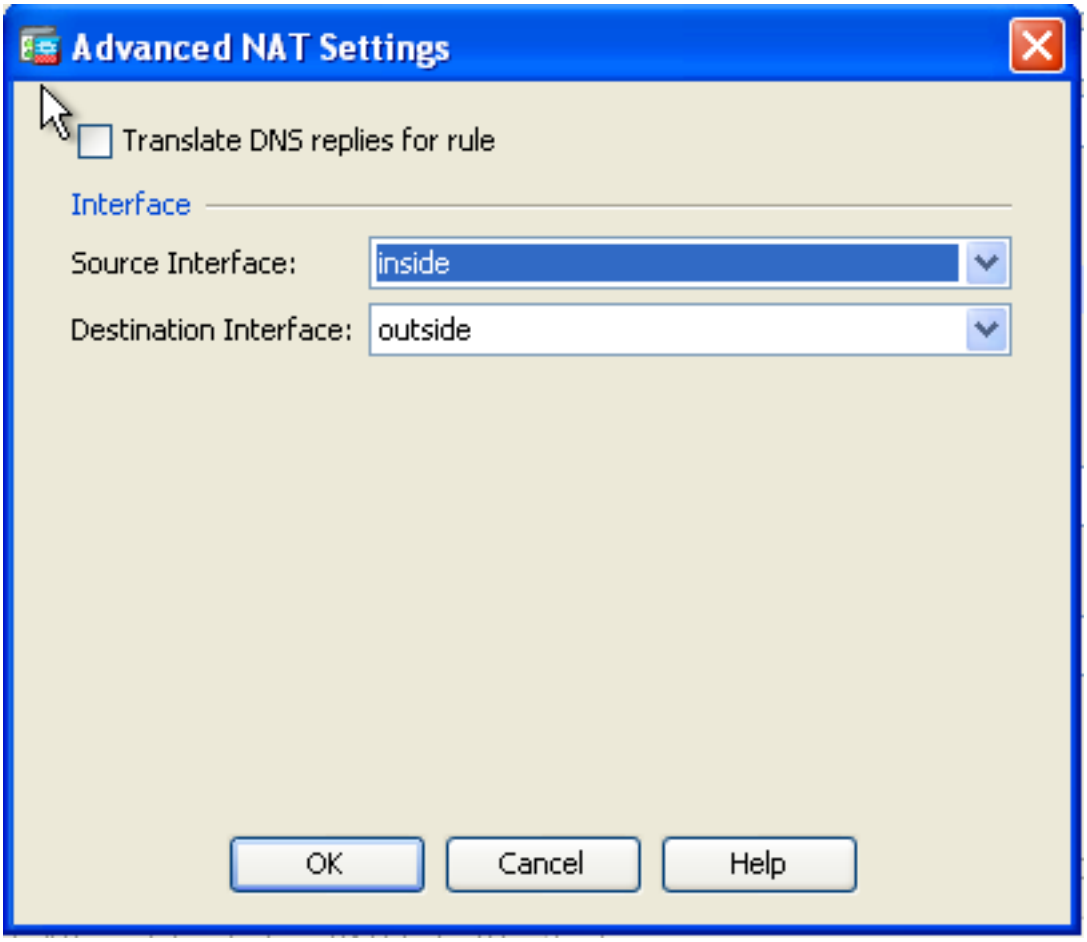
4. **Нажмите Add** для добавления сетевого объекта. В выпадающем списке Типа выберите **Range**. В полях Start Address и End Address введите начало и конечные IP-адреса PAT. **Нажмите кнопку OK.**



5. В поле Translated Addr выберите объект адреса. Нажмите **Advanced** для выбора источника и интерфейсов назначения.



6. В выпадающих списках Исходного интерфейса и Интерфейса назначения выберите соответствующие интерфейсы. Нажмите **OK** и нажмите **Apply** для изменений для вступления в силу.

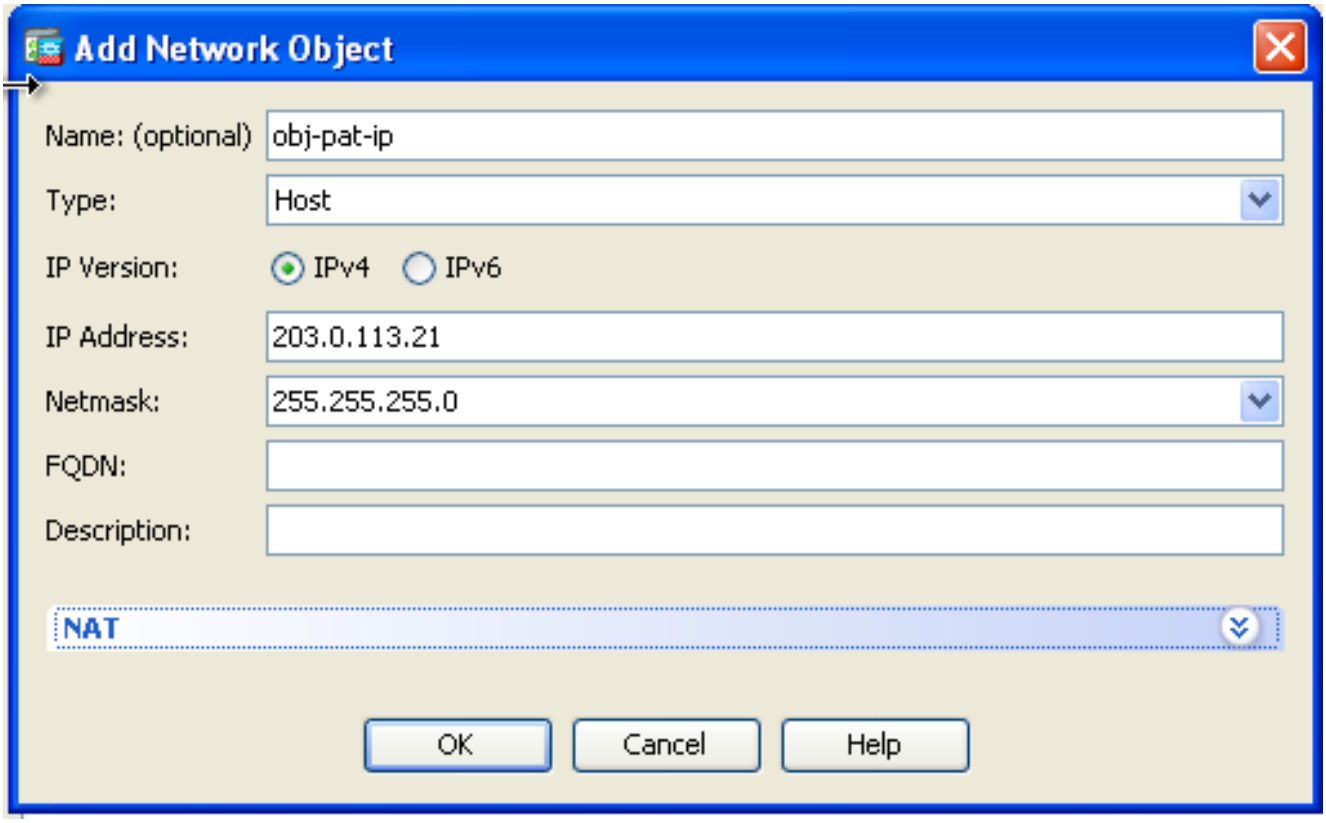


Это - эквивалентные выходные данные CLI для этой конфигурации ASDM:

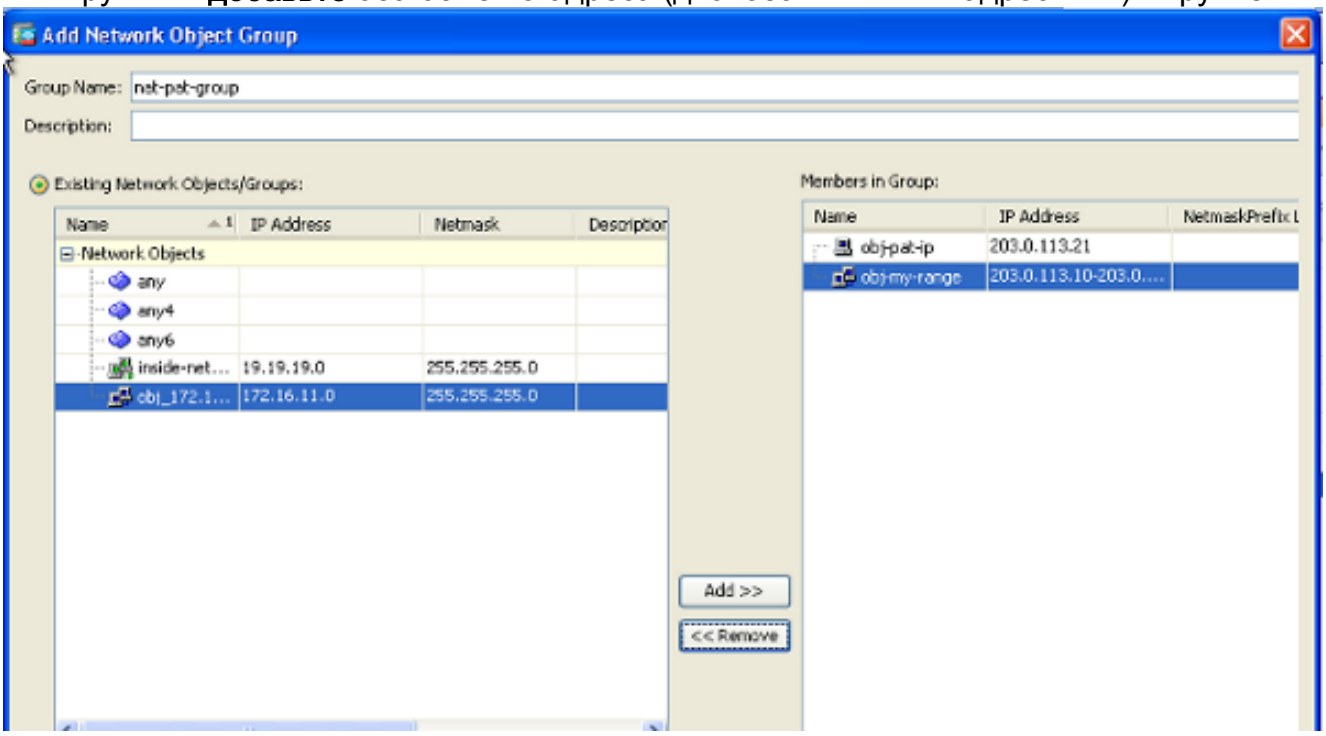
```
object network obj-my-range
range 203.0.113.10 203.0.113.20

object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
nat(inside,outside) dynamic obj-my-range
```

Согласно этой конфигурации, хосты в 172.16.11.0 сетях будут преобразованы в любой IP-адрес от пула NAT, 203.0.113.10 - 203.0.113.20. Если сопоставленный пул имеет меньше адресов, чем реальная группа, у вас могли бы закончиться адреса. В результате вы могли попытаться внедрить динамический NAT с динамической резервной копией PAT, или вы могли попытаться развернуть существующий пул.

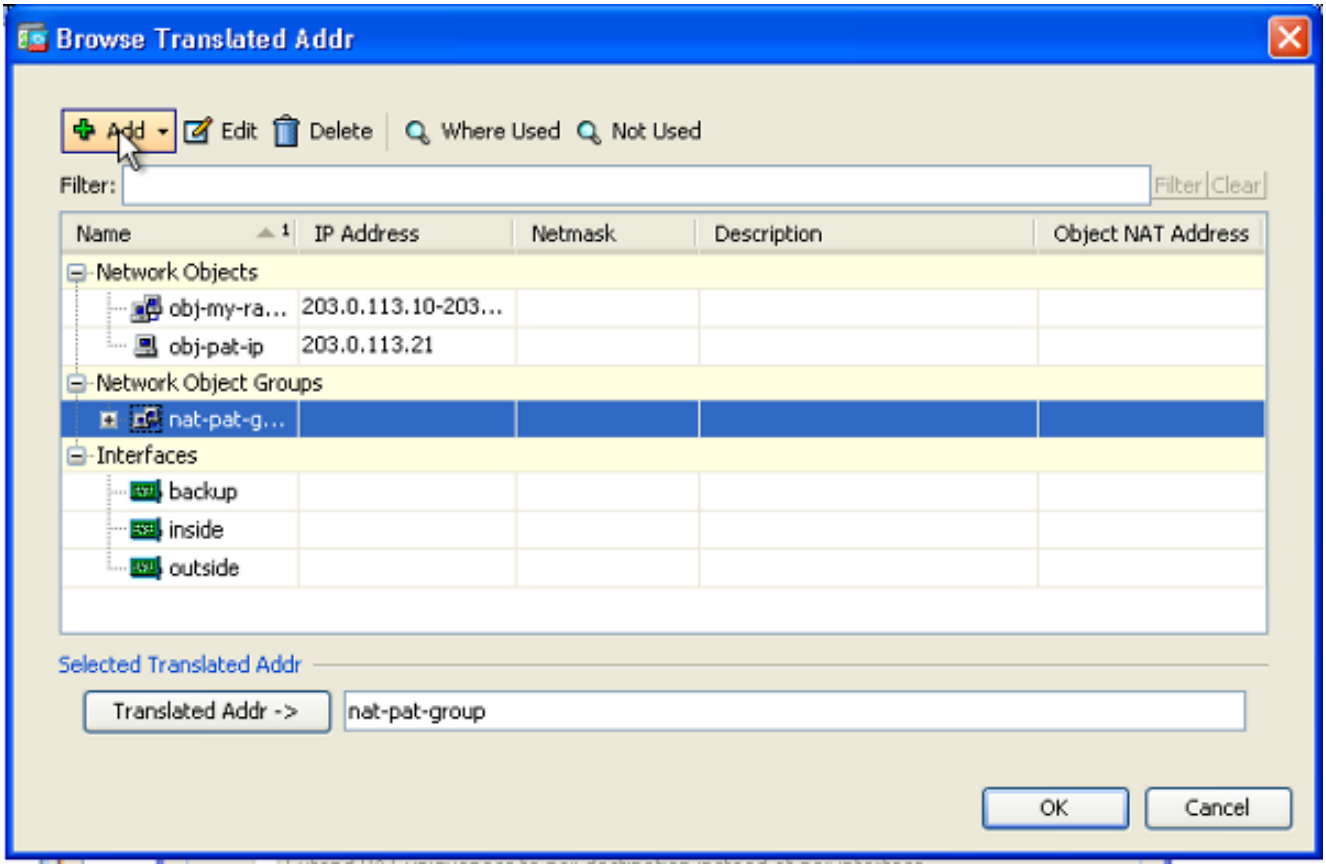
1. Повторите шаги 1 - 3 в предыдущую конфигурацию и **нажмите Add** еще раз для добавления сетевого объекта. В выпадающем списке Типа выберите **Host**. В поле IP Address войдите, PAT резервируют IP-адрес. **Нажмите кнопку OK.**



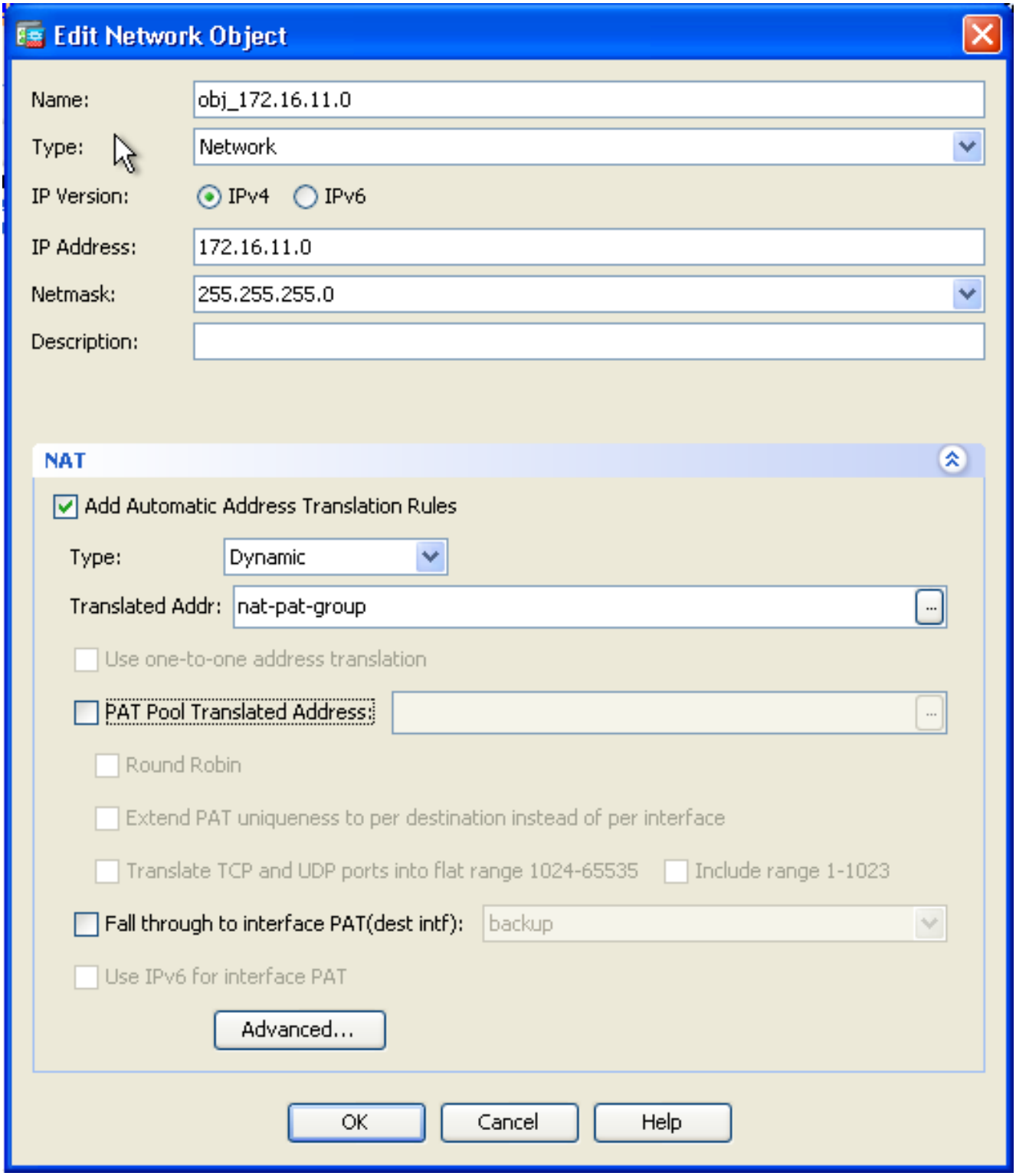
2. **Нажмите Add** для добавления группы сетевых объектов. В поле Group Name введите имя группы и **добавьте** оба объекта адреса (диапазон NAT и IP-адрес PAT) в группе.



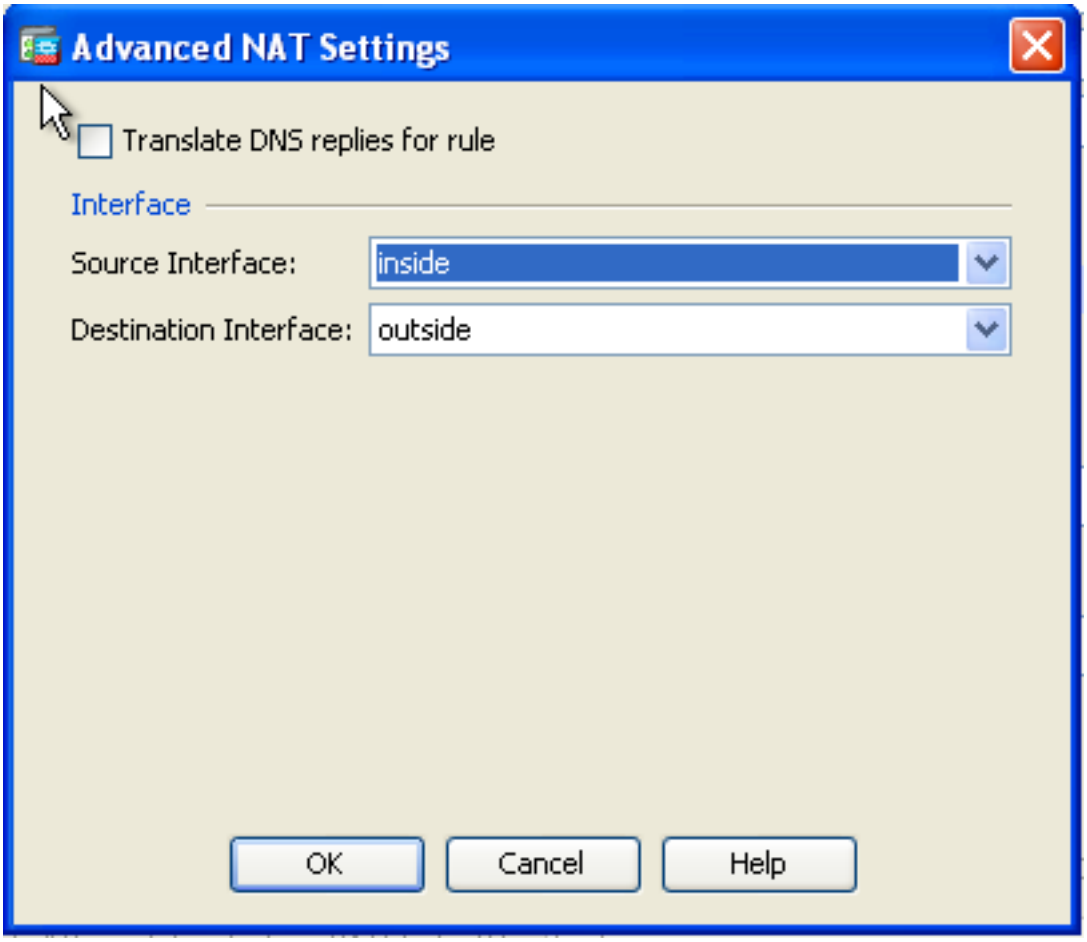
3. Выберите настроенное правило NAT и изменитесь, Преобразованный Addr, чтобы быть недавно настроенной группой 'туземная стандартная группа' (был ранее 'obj-my-range'). **Нажмите кнопку OK.**



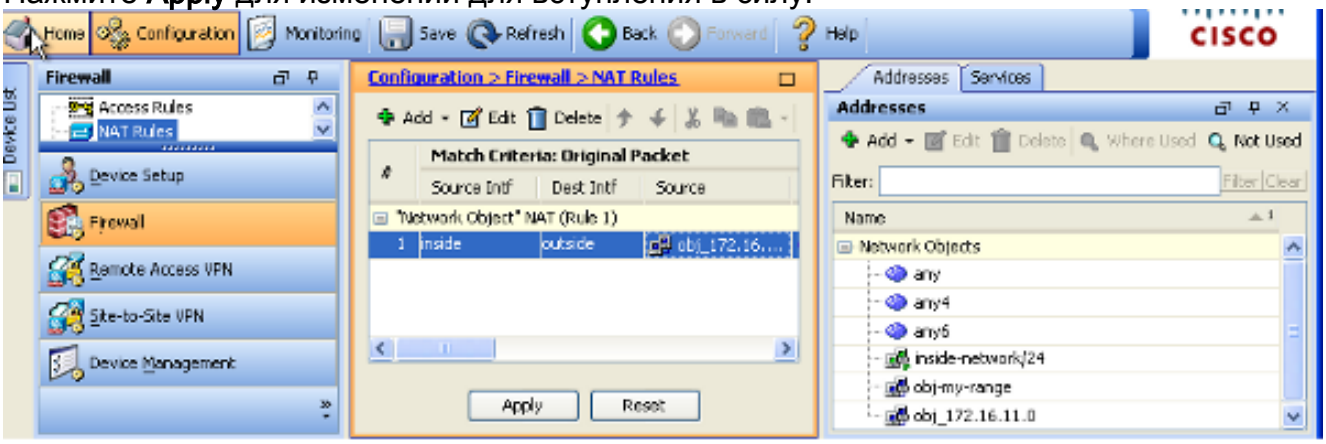
4. Нажмите **OK** для добавления правила NAT. Нажмите **Advanced** для выбора источника и интерфейсов назначения.



5. В выпадающих списках Исходного интерфейса и Интерфейса назначения выберите соответствующие интерфейсы. **Нажмите кнопку OK.**



6. Нажмите **Apply** для изменений для вступления в силу.



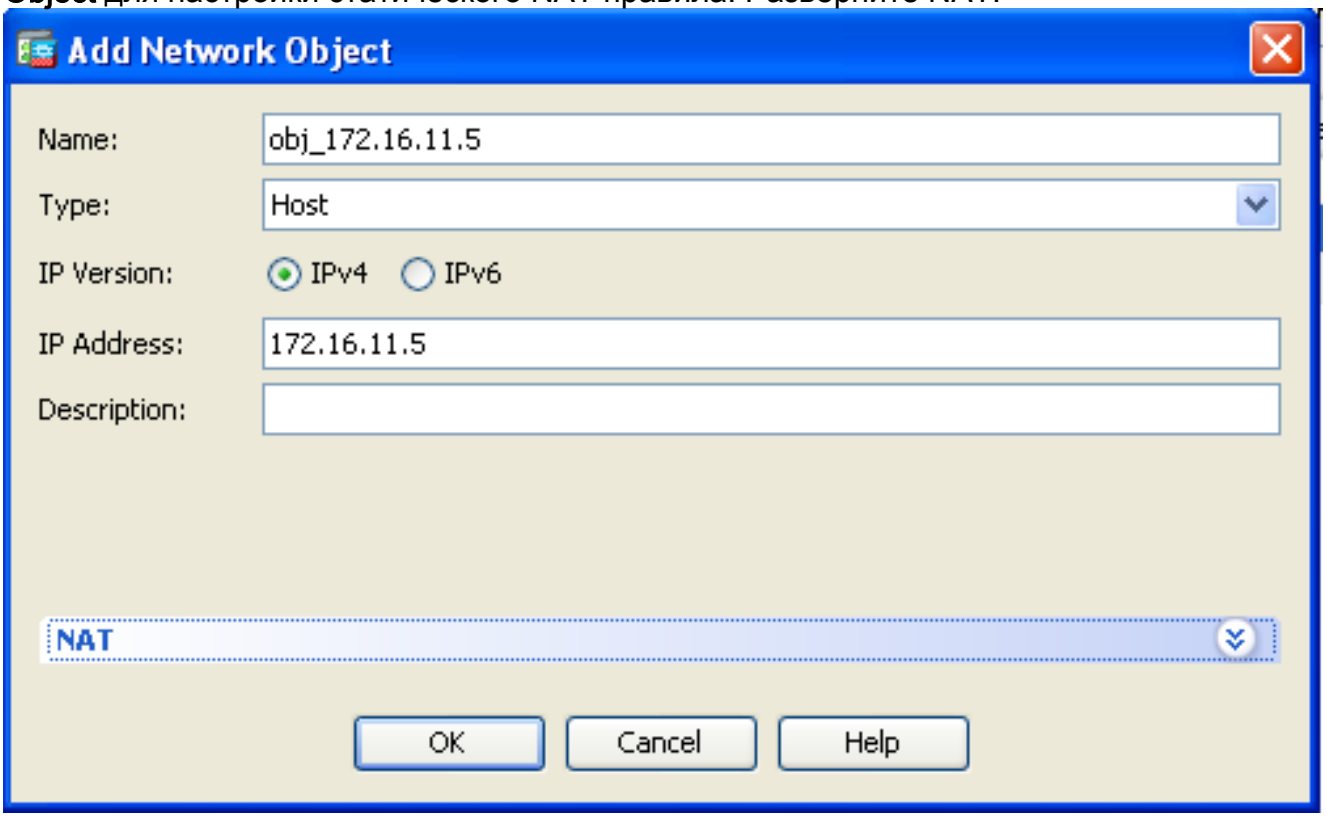
Это - эквивалентные выходные данные CLI для этой конфигурации ASDM:

```
object network obj-my-range
range 203.0.113.10 203.0.113.20

object network obj-pat-ip
host 203.0.113.21

object-group network nat-pat-group
network-object object obj-my-range
network-object object obj-pat-ip

object network obj_172.16.11.0
subnet 172.16.11.0 255.255.255.0
nat (inside,outside) dynamic nat-pat-group
```

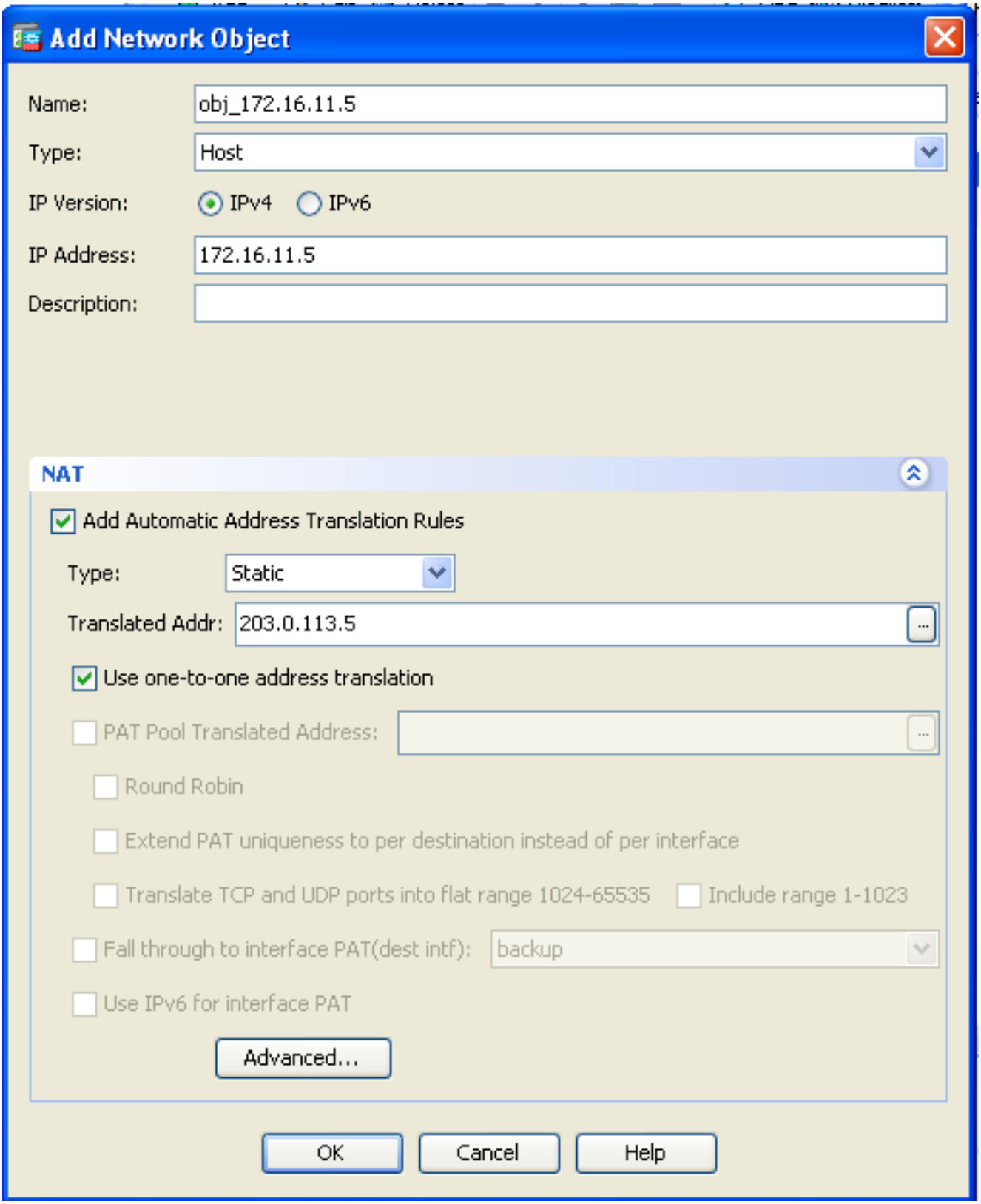
Разрешение доступа недоверенных узлов к узлам доверенной сети

Это может быть достигнуто через приложение статического преобразования NAT и правила доступа разрешить те хосты. Вы обязаны настраивать это каждый раз, когда внешний пользователь хотел бы обратиться к любому серверу, который находится в вашей внутренней сети. Сервер во внутренней сети будет иметь закрытый IP - адрес, который не маршрутизируем в Интернете. В результате необходимо преобразовать тот закрытый IP - адрес в открытый IP - адрес через статическое NAT правило. Предположим, что у вас есть внутренний сервер (172.16.11.5). Для создания этой работы необходимо преобразовать этот частный IP-адрес сервера в открытый IP - адрес. Данный пример описывает, как внедрить двунаправленное статическое NAT для перевода 172.16.11.5 в 203.0.113.5.

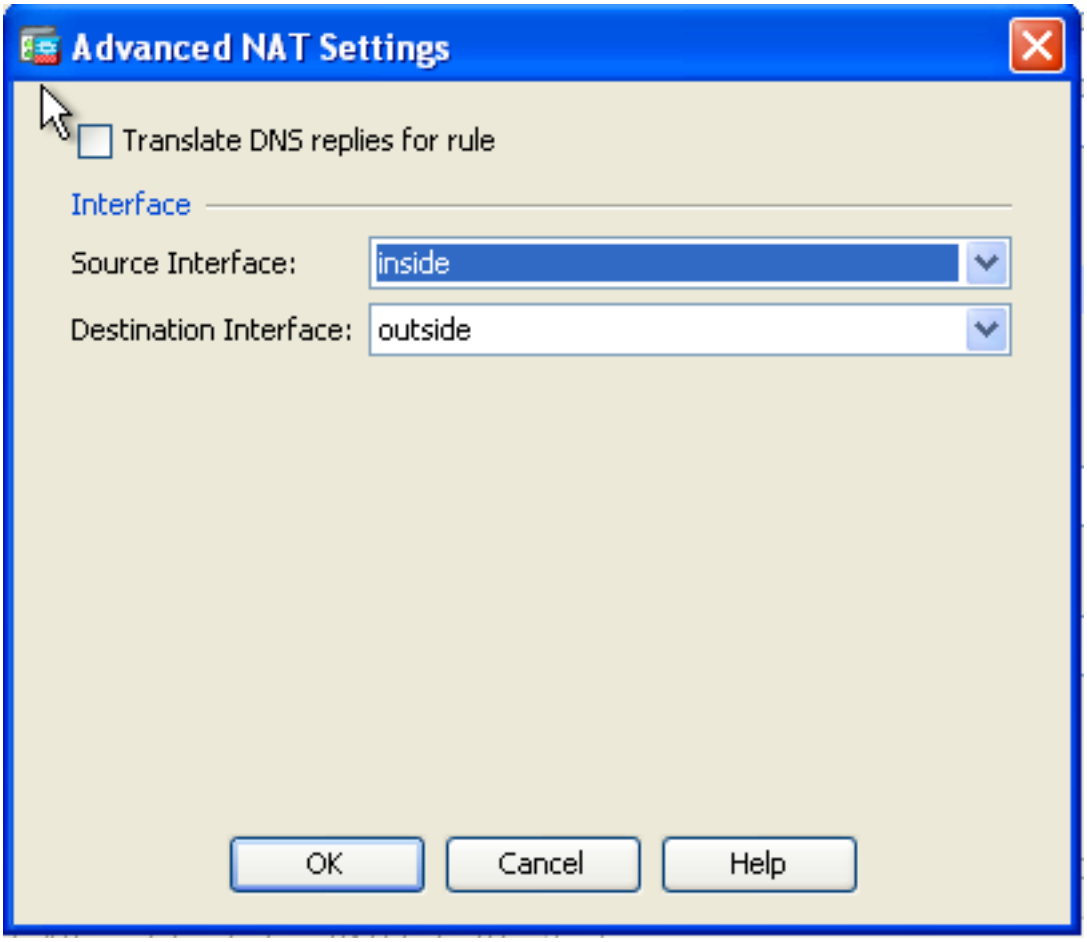
1. Выберите **Configuration> Firewall> NAT Rules**. **Нажмите Add** и затем выберите **Network Object** для настройки статического NAT правила. Разверните NAT.



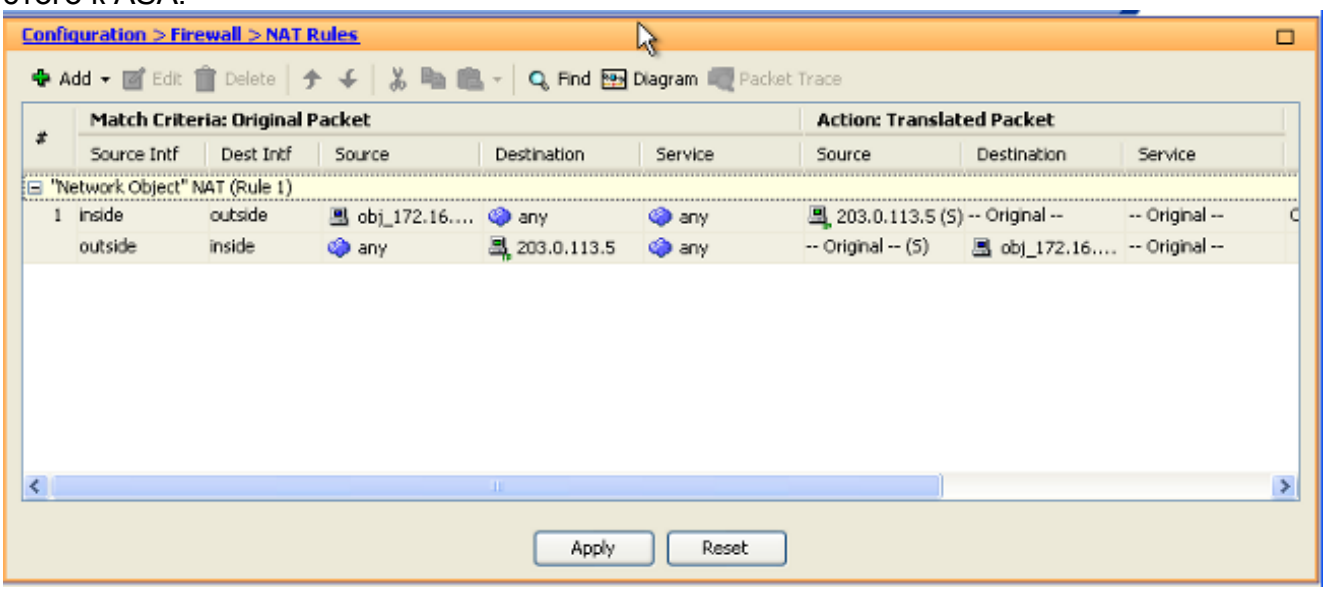
2. Проверьте флажок **Add Automatic Address Translation Rules**. В выпадающем списке Типа выберите **Static.** В поле Translated Addr введите IP-адрес. Нажмите **Advanced** для выбора источника и интерфейсов назначения.



3. В выпадающих списках Исходного интерфейса и Интерфейса назначения выберите соответствующие интерфейсы. **Нажмите кнопку OK.**



4. Вы видите настроенную статическую запись NAT здесь. Нажмите **Apply** для передачи этого к ASA.



Это - эквивалентные выходные данные CLI для этой конфигурации NAT:

```
object network obj_172.16.11.5
host 172.16.11.5
nat (inside,outside) static 203.0.113.5
```

Статическая идентичность NAT

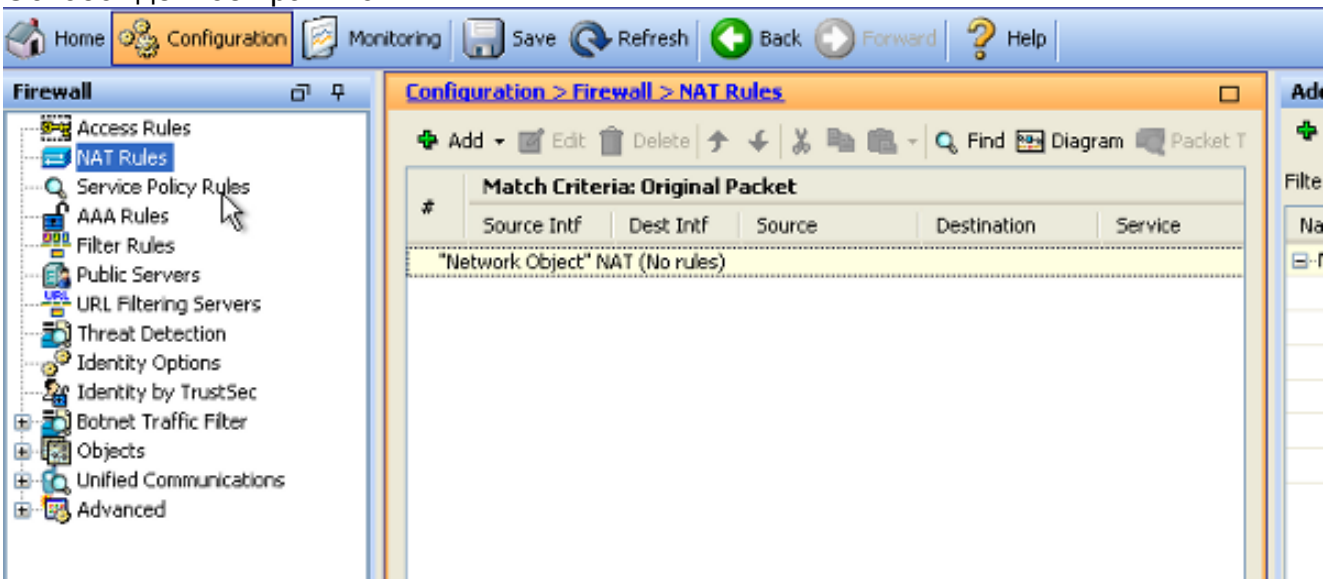
Освобожденный NAT является полезной возможностью, где внутренние пользователи пытаются обратиться к удаленному хосту/серверу VPN или некоторому хосту/серверу, размещенному позади любого другого интерфейса ASA без завершения NAT. Для

достижения этого внутренний сервер, который имеет закрытый IP - адрес, будет идентичностью, преобразованной в себя и которому в свою очередь позволяют обратиться к назначению, которое выполняет NAT.

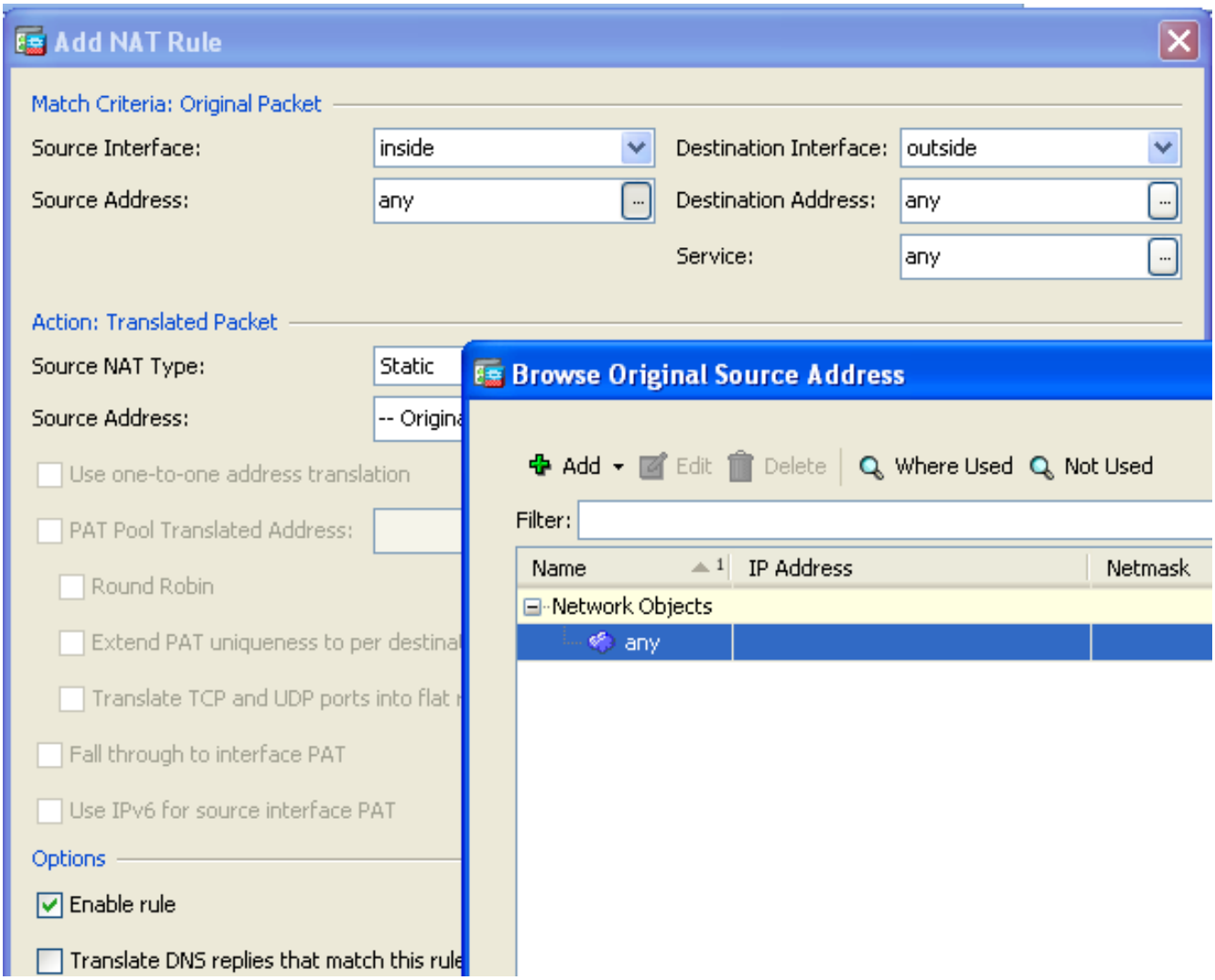
В данном примере, внутренний хост 172.16.11.15 потребностей обратиться к удаленному VPN-серверу 172.20.21.15.

Выполните эти шаги для разрешения доступа для внутренних узлов удаленной сети VPN с завершением NAT:

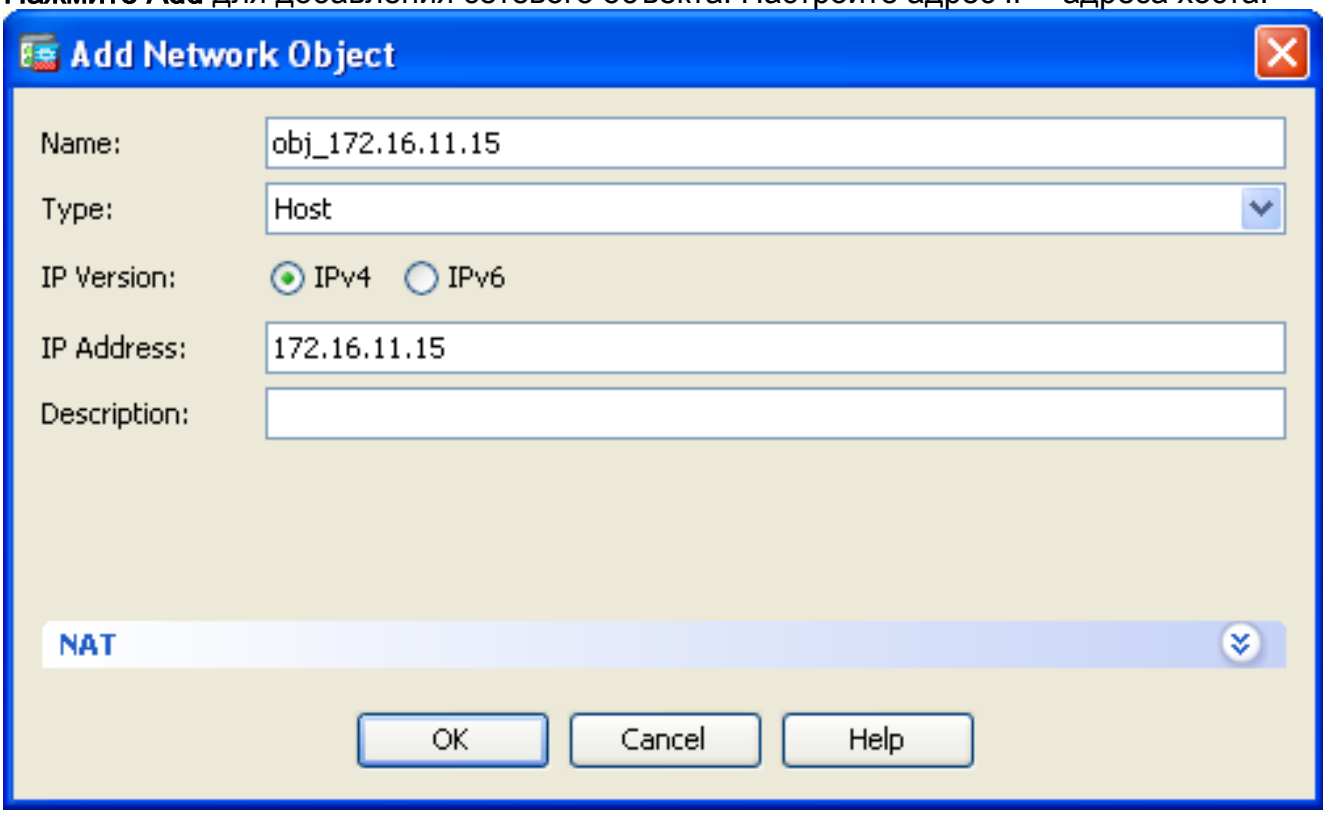
1. Выберите **Configuration> Firewall> NAT Rules**. **Нажмите Add** для настройки NAT Освобожденное правило.



2. В выпадающих списках Исходного интерфейса и Интерфейса назначения выберите соответствующие интерфейсы. В Поле исходного адреса выберите соответствующую запись.

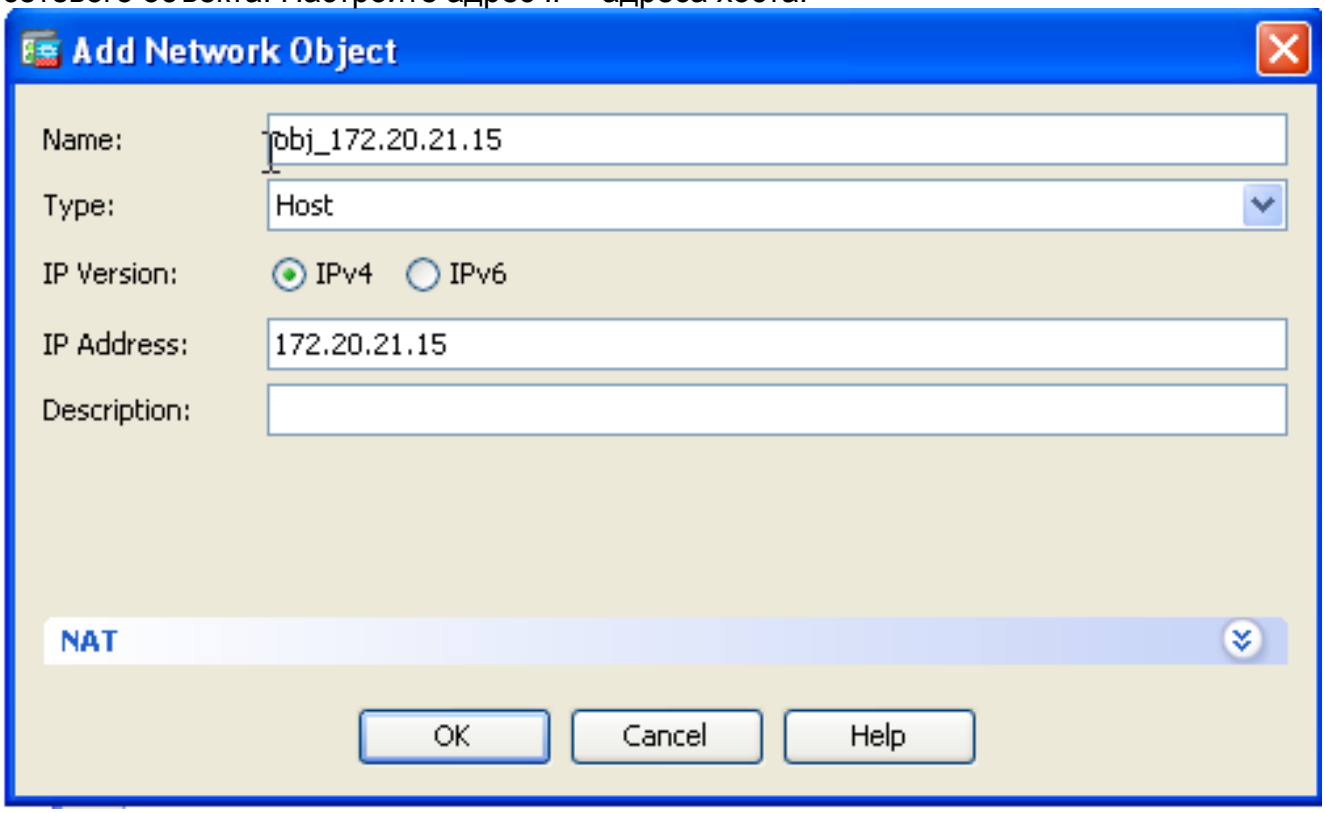


3. **Нажмите Add** для добавления сетевого объекта. Настройте адрес IP - адреса хоста.

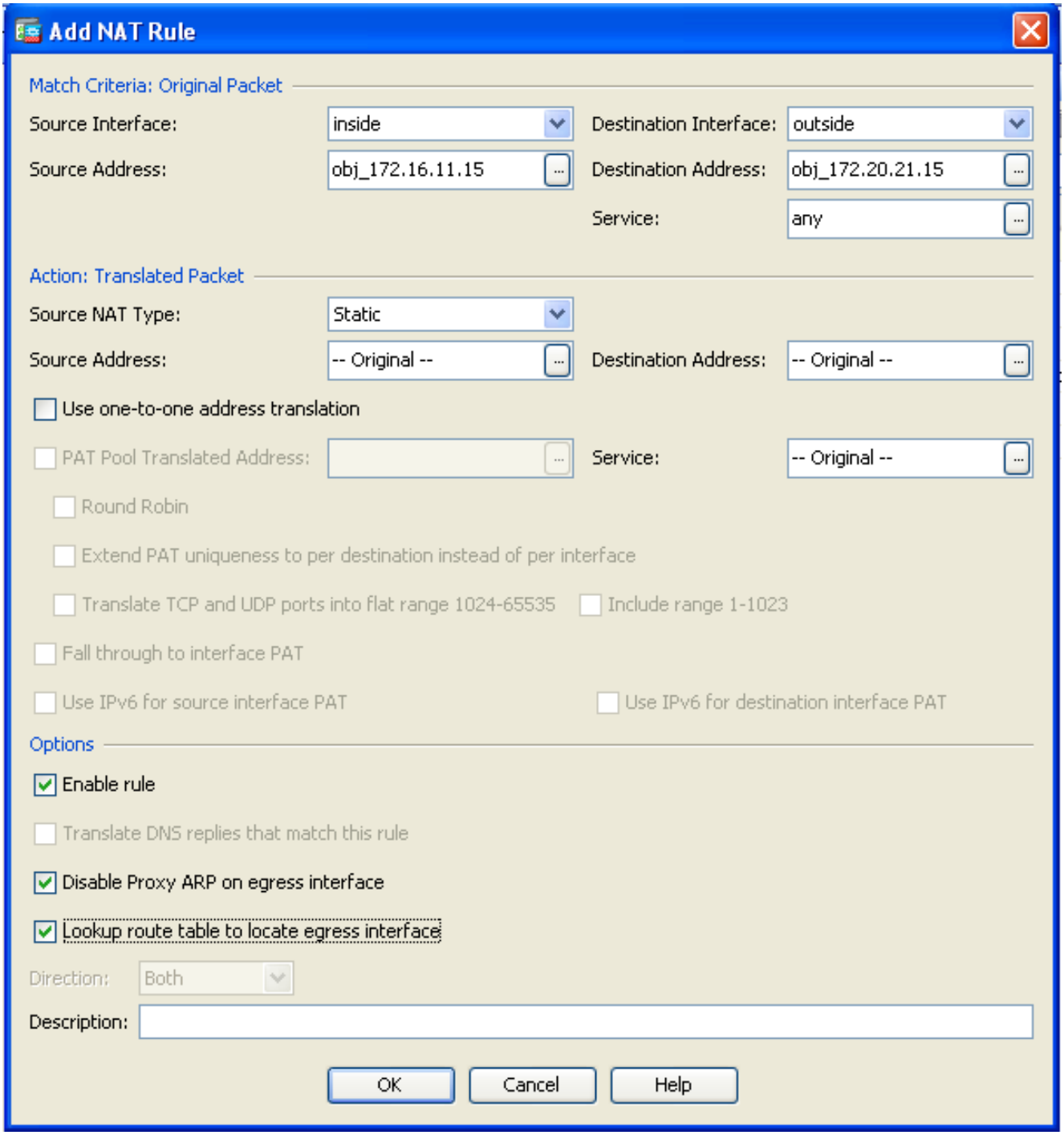


4. Точно так же просмотрите **Адрес назначения (DA)**. **Нажмите Add** для добавления

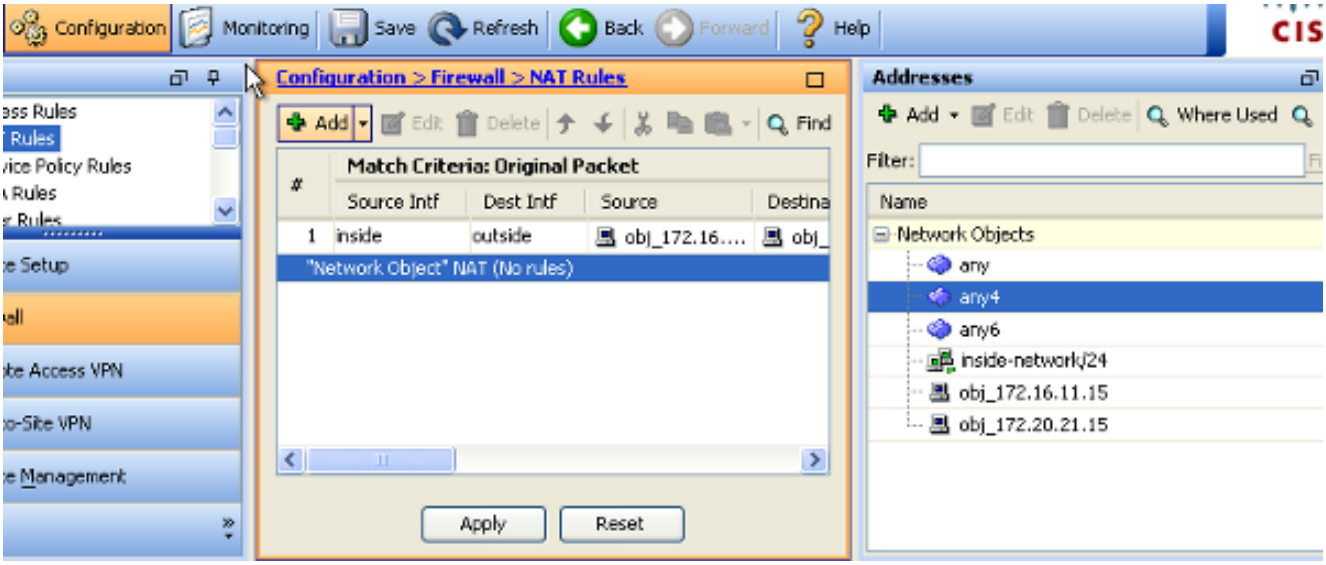
сетевого объекта. Настройте адрес IP - адреса хоста.



5. Выберите настроенные объекты Адреса источника и Адреса назначения (DA). Проверьте **Запрещать Прокси - протокол преобразования адресов на исходящем интерфейсе** и **таблице маршрутизации Поиска для определения местоположения** флажков **исходящего интерфейса**. **Нажмите кнопку ОК.**



6. Нажмите **Apply** для изменений для вступления в силу.



Это - эквивалентные выходные данные CLI для Освобожденного NAT или Идентификационная конфигурация NAT:

```
object network obj_172.16.11.15
host 172.16.11.15
object network obj_172.20.21.15
host 172.20.21.15

nat (inside,outside) source static obj_172.16.11.15 obj_172.16.11.15
destination static obj_172.20.21.15 obj_172.20.21.15 no-proxy-arp route-lookup
```

Перенаправление порта (передача) со статическим

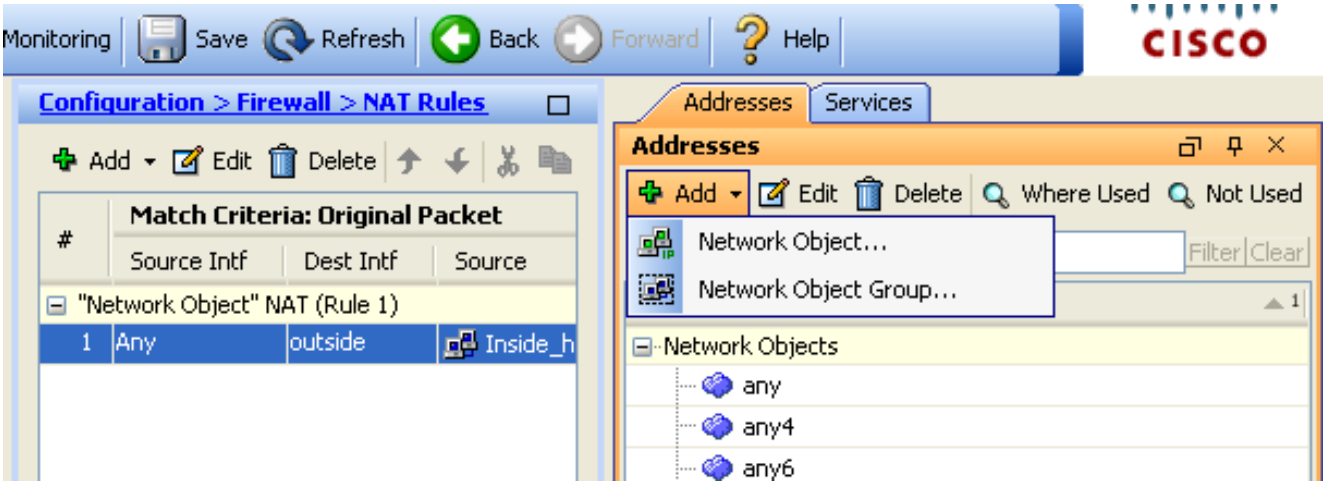
Переадресация портов или перенаправление порта являются полезной возможностью, где внешние пользователи пытаются обратиться к внутреннему серверу на определенном порту. Для достижения этого внутренний сервер, который имеет закрытый IP - адрес, будет преобразован в открытый IP - адрес, который в свою очередь является предоставленным доступом для определенного порта.

В данном примере внешний пользователь хочет обратиться к серверу SMTP, 203.0.115.15 в порту 25. Это выполнено в двух шагах:

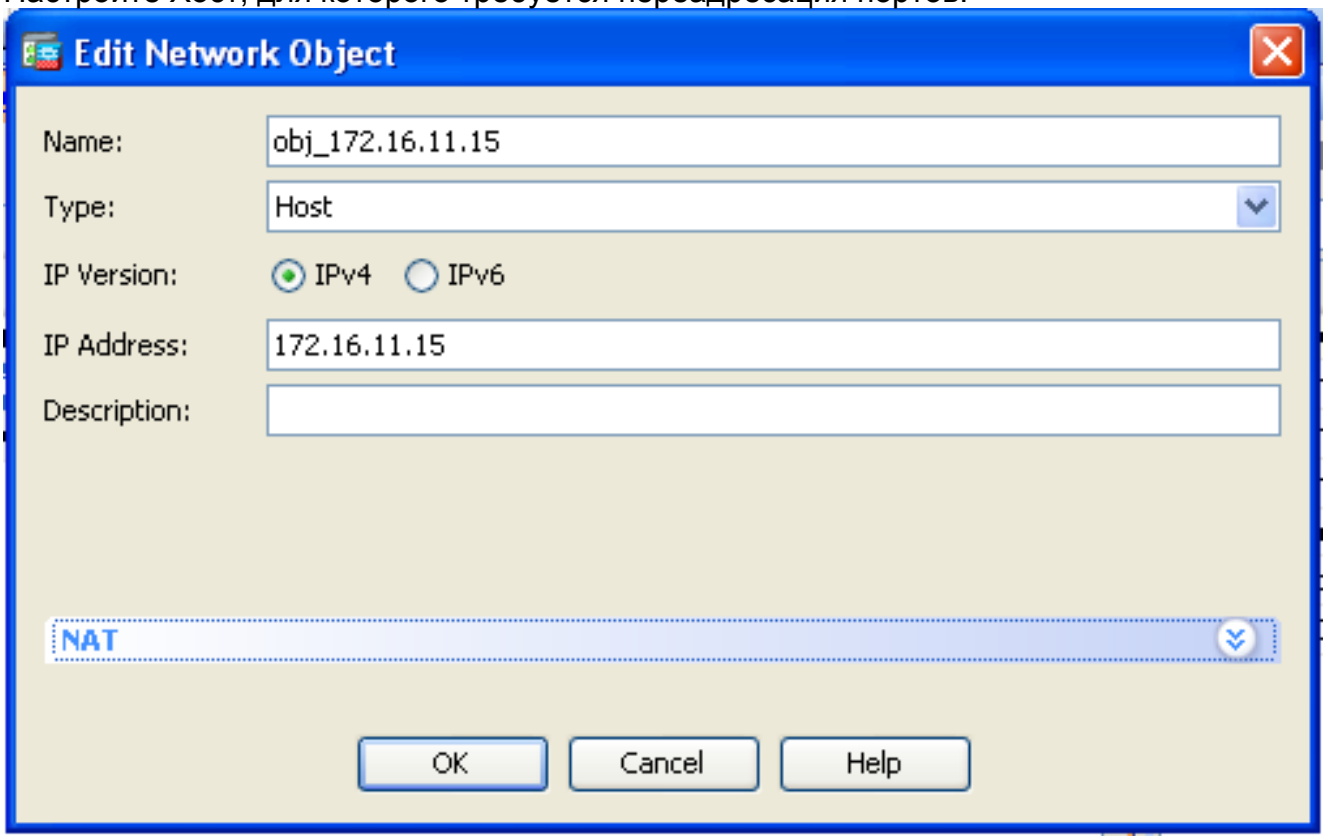
1. Преобразуйте внутренний сервер RADIUS, 172.16.11.15 на порту 25, к открытому IP - адресу, 203.0.115.15 в порту 25.
2. Предоставьте доступ к общему почтовому серверу, 203.0.115.15 в порту 25.

Когда внешний пользователь пытается обратиться к серверу, 203.0.115.15 в порту 25, этот трафик перенаправлен к внутреннему серверу RADIUS, 172.16.11 15 в порту 25.

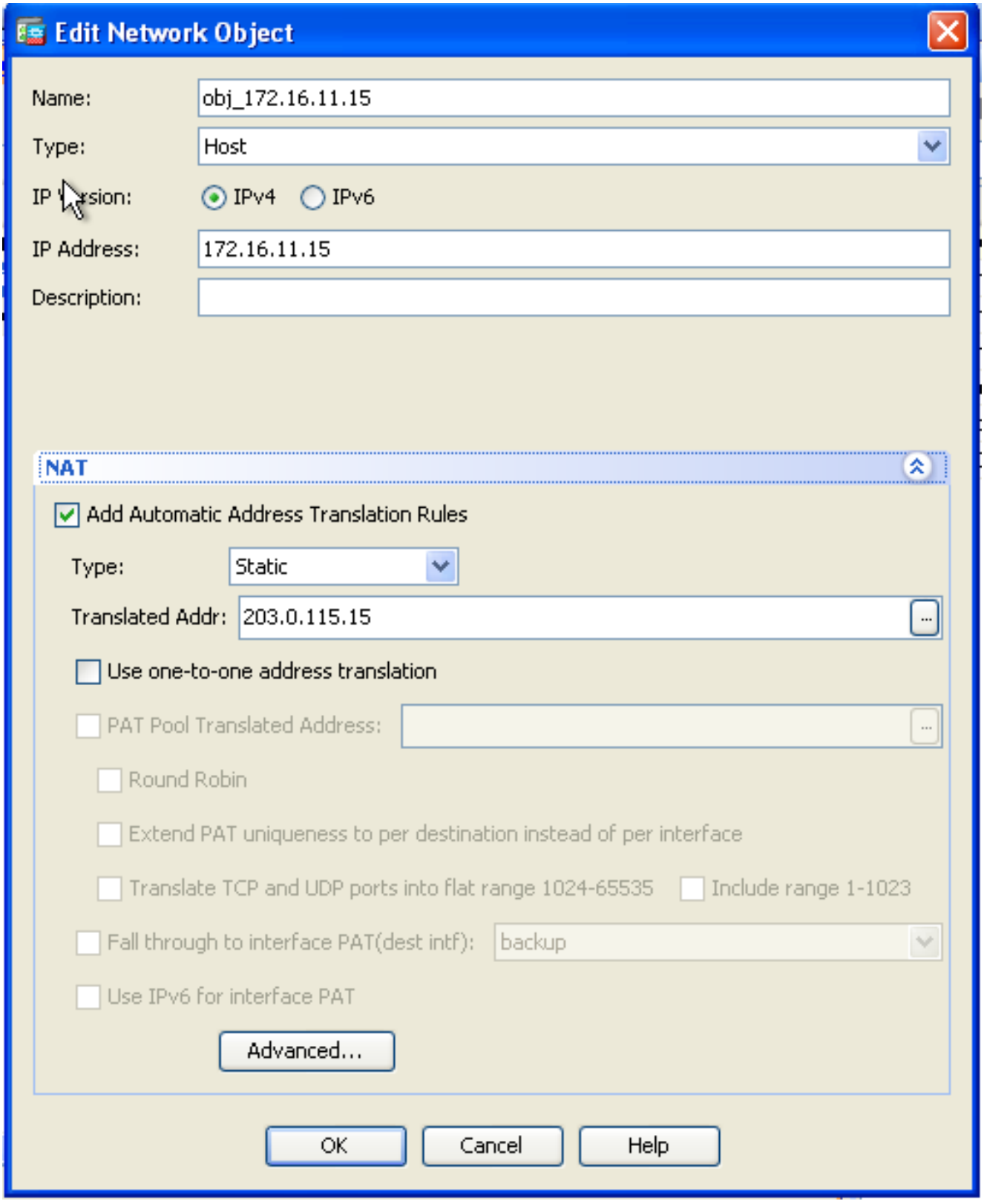
1. Выберите **Configuration> Firewall> NAT Rules**. **Нажмите Add** и затем выберите **Network Object** для настройки статического NAT правила.



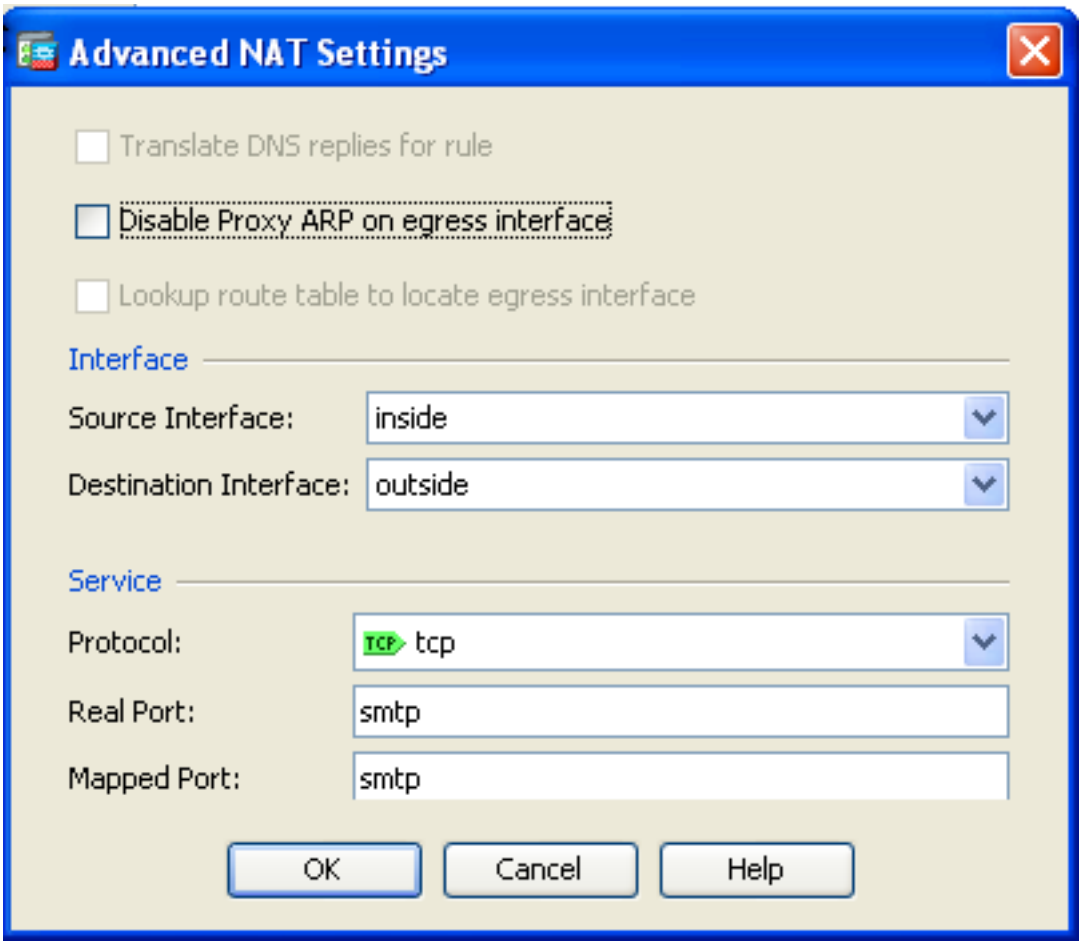
2. Настройте Хост, для которого требуется переадресация портов.



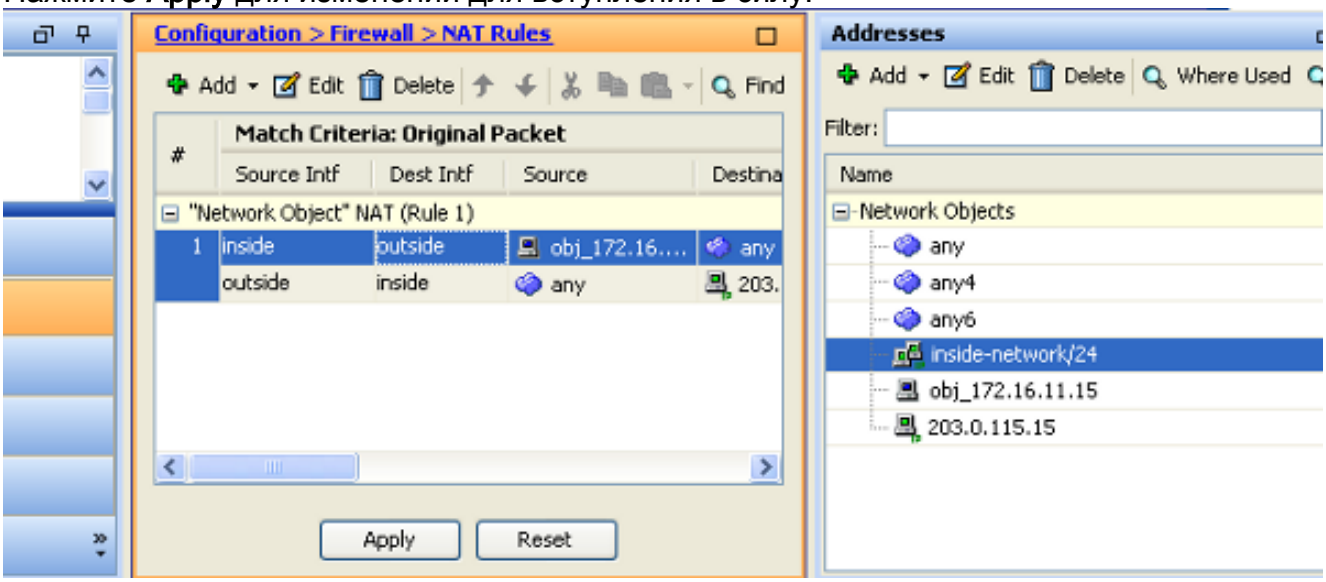
3. Разверните NAT. Проверьте флажок **Add Automatic Address Translation Rules**. В выпадающем списке Типа выберите **Static**. В поле Translated Addr введите IP-адрес. Нажмите **Advanced** для выбора сервиса и источника и интерфейсов назначения.



4. В выпадающих списках Исходного интерфейса и Интерфейса назначения выберите соответствующие интерфейсы. Настройка службы. **Нажмите кнопку ОК.**



5. Нажмите **Apply** для изменений для вступления в силу.



Это - эквивалентные выходные данные CLI для этой конфигурации NAT:

```
object network obj_172.16.11.15
host 172.16.11.15
nat (inside,outside) static 203.0.115.15 service tcp smtp smtp
```

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Cisco CLI Анализатор (только зарегистрированные клиенты) поддерживает **некоторые**

команды show. Используйте Cisco CLI Анализатор для **просматривания аналитику выходных данных команды show**.

Обратитесь к веб-сайту через HTTP с web-браузером. Данный пример использует сайт, который размещен в 198.51.100.100. Если соединение успешно, эти выходные данные могут быть замечены на CLI ASA.

Соединение

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 172.16.11.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

ASA является самонастраивающимся межсетевым экраном, и ответный трафик от Web-сервера позволен назад через межсетевой экран, потому что это совпадает ***с соединением*** в таблице подключений межсетевого экрана. Трафик, который совпадает с соединением, которое существует ранее, позволен через межсетевой экран, не будучи заблокированным интерфейсным ACL.

В предыдущих выходных данных клиент на внутреннем интерфейсе установил соединение с этими 198.51.100.100 хостами прочь внешнего интерфейса. Это соединение сделано с протоколом TCP и было простаивающим в течение шести секунд. Флаги соединения указывают на текущее состояние этого соединения. Дополнительные сведения о флагах соединения могут быть найдены во Флагах TCP - подключения ASA.

Системный журнал

```
ASA(config)# show log | in 172.16.11.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
172.16.11.5/58799 to outside:203.0.113.2/58799

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:172.16.11.5/58799 (203.0.113.2/58799)
```

Межсетевой экран ASA генерирует системные журналы во время нормальной работы. Системные журналы располагаются в многословии на основе конфигурации журнала. Выходные данные показывают два системных журнала, которые замечены на уровне шесть или 'информационном' уровне.

В данном примере существует два генерируемые системных журнала. Первым является сообщение журнала, которое указывает, что межсетевой экран создал трансляцию, в частности динамическую трансляцию TCP (PAT). Это указывает на IP - адрес источника и порт и преобразованный IP-адрес и порт, поскольку трафик пересекает от внутренней части до внешних интерфейсов.

Второй системный журнал указывает, что межсетевой экран создал соединение в своей таблице подключений для этого определенного трафика между клиентом и сервером. Если бы межсетевой экран был настроен для блокирования этой попытки подключения, или некоторый другой фактор запретил создание этого соединения (ограничения ресурса или вероятная неверная конфигурация), то межсетевой экран не генерировал бы журнал, который указывает, что было создано соединение. Вместо этого это регистрировало бы причину для соединения, которое будет запрещено или индикация о том, какой фактор запретил соединению то, чтобы быть созданным.

Средство трассировки пакетов

```
ASA(config)# packet-tracer input inside tcp 172.16.11.5 1234 198.51.100.100 80


--Omitted--

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Пакетная функциональность трассировщика на ASA позволяет вам задавать *моделируемый* пакет и видеть все различные шаги, проверки и функции, которые проходит межсетевой экран, когда это обрабатывает трафик. С этим программным средством полезно определить пример трафика, которому вы верите*, должен* быть позволен пройти через межсетевой экран и использование, что 5-tupple для моделирования трафика. В предыдущем примере пакетный трассировщик используется для моделирования попытки подключения, которая соответствует этим критериям:

- Моделируемый пакет поступает во внутреннюю часть.
- Используемый протокол является TCP.
- Моделируемый IP-адрес клиента 172.16.11.5.
- Клиент передает трафик, полученный от порта 1234.
- Трафик предназначен к серверу в IP-адресе 198.51.100.100.
- Трафик предназначен к порту 80.

Заметьте, что не было никакого упоминания об интерфейсе снаружи в команде. Это пакетным дизайном трассировщика. Программное средство говорит вам, как межсетевой экран обрабатывает ту попытку типа соединения, которая включает, как это направило бы его, и из который интерфейс. Дополнительные сведения о пакетном трассировщике могут быть найдены в Отслеживании Пакетов с Пакетным Трассировщиком.

Перехват

Примените перехват

```
ASA# capture capin interface inside match tcp host 172.16.11.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100ASA#show capture capin

3 packets captured

1: 11:31:23.432655 172.16.11.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 172.16.11.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 172.16.11.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768ASA#show capture capout

3 packets captured

1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
```

```
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

Межсетевой экран ASA может перехватить трафик, который вводит или оставляет его интерфейсы. Эта функциональность перехвата является фантастической, потому что может окончательно оказаться, поступает ли трафик в или уезжает от, межсетевой экран. Предыдущий пример показал конфигурацию двух перехватов, названных capin и capout на внутренних и внешних интерфейсах соответственно. Команды перехвата использовали ключевое слово соответствия, которое позволяет вам быть определенными, о каком трафике вы хотите перехватить.

Для capin перехвата вы указали, что хотели совпасть с трафиком, замеченным на внутреннем интерфейсе (вход или выход), который совпадает с хостом 198.51.100.100 хоста 172.16.11.5 TCP. Другими словами, вы хотите перехватить любой Трафик TCP, который передается от хоста 172.16.11.5 до хоста 198.51.100.100 или наоборот. Использование ключевого слова соответствия позволяет межсетевому экрану перехватывать тот трафик двунаправленным образом. Команда перехвата, определенная для внешнего интерфейса, не ссылается на IP-адрес внутреннего клиента, потому что межсетевой экран проводит PAT на том IP-адресе клиента. В результате вы не можете совпасть с тем IP-адресом клиента. Вместо этого данный пример использует любого, чтобы указать, что все возможные IP-адреса совпали бы с тем условием.

После настройки перехватов вы тогда попытались бы установить соединение снова и продолжить просматривать перехваты с командой ***<capture_name>*** **show capture**. В данном примере вы видите, что клиент смог соединиться с сервером как очевидный трехсторонним квитированием TCP, замеченным в перехватах.

Устранение неполадок

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

Дополнительные сведения

- Пример конфигурации системного журнала ASA
- Захваты пакета ASA с CLI и примером конфигурации ASDM
- Cisco Systems – техническая поддержка и документация