ASA 8. 3 (x) динамический PAT с двумя внутренними сетями и интернет-примером конфигурации

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
!--- конфигурацию
Схема сети
Конфигурация ASA в интерфейсе командной строки
Настройка посредством ASDM
Проверка
Проверка правила PAT общего назначения
Проверка определенного правила PAT
Устранение неполадок
Дополнительные сведения

Введение

Этот документ предоставляет пример конфигурации для динамического PAT на устройстве адаптивной защиты Cisco (ASA), который работает под управлением ПО версии 8.3 (1). Динамический PAT преобразовывает множественные действительные адреса в одиночный сопоставленный IP-адрес путем перевода адреса фактического источника и исходного порта к сопоставленному адресу и уникальному сопоставленному порту. Каждое соединение требует отдельного сеанса преобразования, потому что исходный порт в каждом соединении будет различен.

Предварительные условия

Требования

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

- Удостоверьтесь, что внутренняя сеть имеет две сети, расположенные на внутренней части ASA:192.168.0.0/24 — Сеть, непосредственно связанная с ASA.192.168.1.0/24 — Сеть на внутренней части ASA, но позади другого устройства (например,

маршрутизатор).
- Удостоверьтесь, что внутренние пользователи получают PAT следующим образом:Хосты на 192.168.1.0/24 подсети получат PAT к запасному IP-адресу, данному интернет-провайдером (10.1.5.5).Любой другой хост позади внутренней части ASA получит PAT к IP-адресу внешнего интерфейса ASA (10.1.5.1).

Используемые компоненты

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

- Устройство адаптивной защиты Cisco (ASA) с версией 8.3 (1)
- Версия 6.3 (1) ASDM

Примечание: Сведения о том, как разрешить настройку ASA с помощью ASDM см. в документе Включение HTTPS-доступа для ASDM.

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.

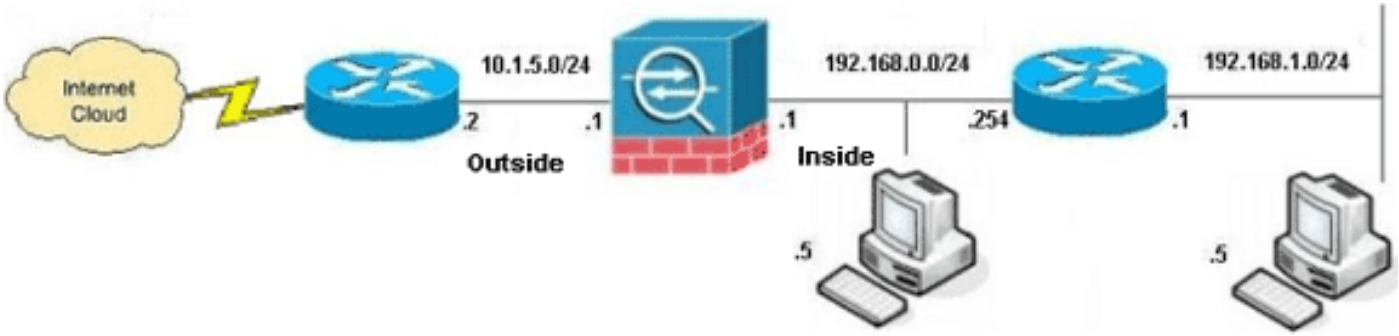
Условные обозначения

См. Cisco Technical Tips Conventions для получения информации об условных обозначениях в документации.

!--- конфигурацию

Схема сети

В настоящем документе используется следующая схема сети:



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

- Конфигурация ASA в интерфейсе командной строки
- Настройка посредством ASDM

Конфигурация ASA в интерфейсе командной строки

В данном документе используются следующие конфигурации.

ASA динамическая конфигурация PAT

```
ASA#configure terminal Enter configuration commands, one per line. End with CNTL/Z. !--- Creates an object called OBJ_GENERIC_ALL. !--- Any host IP not already matching another configured !--- object will get PAT to the outside interface IP !--- on the ASA (or 10.1.5.1), for internet bound traffic. ASA(config)#object network OBJ_GENERIC_ALL ASA(config-obj)#subnet 0.0.0.0 0.0.0.0 ASA(config-obj)#exit ASA(config)#nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface !--- The above statements are the equivalent of the !--- nat/global combination (as shown below) in v7.0(x), !--- v7.1(x), v7.2(x), v8.0(x), v8.1(x) and v8.2(x) ASA code: nat (inside) 1 0.0.0.0 0.0.0.0 global (outside) 1 interface !--- Creates an object called OBJ_SPECIFIC_192-168-1-0. !--- Any host IP facing the the 'inside' interface of the ASA !--- with an address in the 192.168.1.0/24 subnet will get PAT !--- to the 10.1.5.5 address, for internet bound traffic. ASA(config)#object network OBJ_SPECIFIC_192-168-1-0 ASA(config-obj)#subnet 192.168.1.0 255.255.255.0 ASA(config-obj)#exit ASA(config)#nat (inside,outside) source dynamic OBJ_SPECIFIC_192-168-1-0 10.1.5.5 !--- The above statements are the equivalent of the nat/global !--- combination (as shown below) in v7.0(x), v7.1(x), v7.2(x), v8.0(x), !--- v8.1(x) and v8.2(x) ASA code: nat (inside) 2 192.168.1.0 255.255.255.0 global (outside) 2 10.1.5.5
```

ASA 8. 3 (1) рабочий Config

```
ASA#show run : Saved : ASA Version 8.3(1) ! hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted names ! !--- Configure the outside interface. ! interface GigabitEthernet0/0 nameif outside security-level 0 ip address 10.1.5.1 255.255.255.0 !--- Configure the inside interface. ! interface GigabitEthernet0/1 nameif inside security-level 100 ip address 192.168.0.1 255.255.255.0 ! interface GigabitEthernet0/2 shutdown no nameif no security-level no ip address ! interface GigabitEthernet0/3 shutdown no nameif no security-level no ip address ! interface Management0/0 shutdown no nameif no security-level no ip address management-only ! boot system disk0:/asa831-k8.bin ftp mode passive object network OBJ_SPECIFIC_192-168-1-0 subnet 192.168.1.0 255.255.255.0 object network OBJ_GENERIC_ALL subnet 0.0.0.0 0.0.0.0 pager lines 24 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-631.bin no asdm history enable arp timeout 14400 nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface nat (inside,outside) source dynamic OBJ_SPECIFIC_192-168-1-0 10.1.5.5 route inside 192.168.1.0 255.255.255.0 192.168.0.254 1 route outside 0.0.0.0 0.0.0.0 10.1.5.2 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute timeout tcp-proxy-reassembly 0:01:00 dynamic-access-policy-record DfltAccessPolicy http
```

```
server enable http 192.168.0.0 255.255.254.0 inside no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart crypto ipsec security-association lifetime
seconds 28800 crypto ipsec security-association lifetime
kilobytes 4608000 telnet timeout 5 ssh timeout 5 console
timeout 0 threat-detection basic-threat threat-detection
statistics access-list no threat-detection statistics
tcp-intercept ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum
client auto message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
preset_dns_map inspect ftp inspect h323 h225 inspect
h323 ras inspect rsh inspect rtsp inspect esmtp inspect
sqlnet inspect skinny inspect sunrpc inspect xdmcp
inspect sip inspect netbios inspect tftp inspect ip-
options ! service-policy global_policy global prompt
hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f : end
```

Настройка посредством ASDM

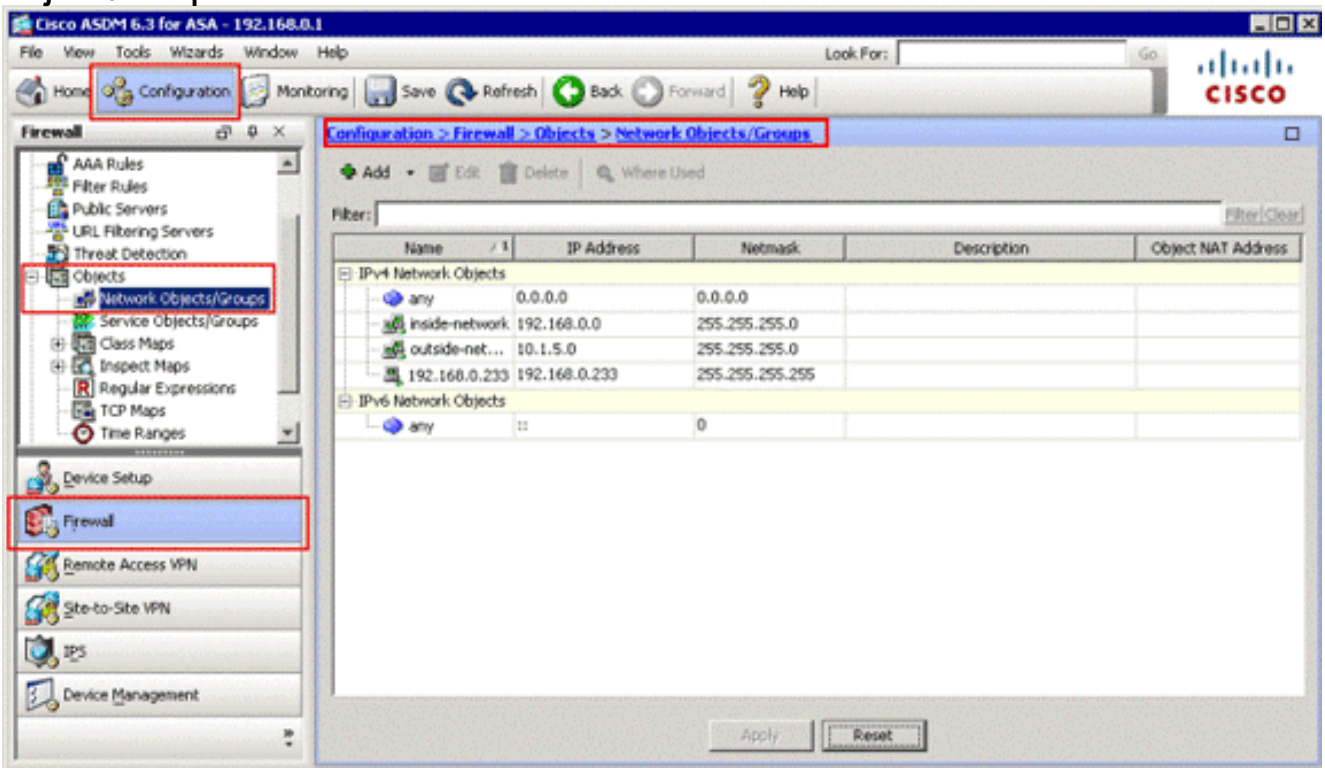
Для завершения этой конфигурации через интерфейс ASDM вы должны:

1. Добавьте три сетевых объекта; данные примеры добавляют эти сетевые объекты:OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-010.1.5.5
2. Создайте два правила NAT/PAT; данные примеры создают правила NAT для этих сетевых объектов:OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-0

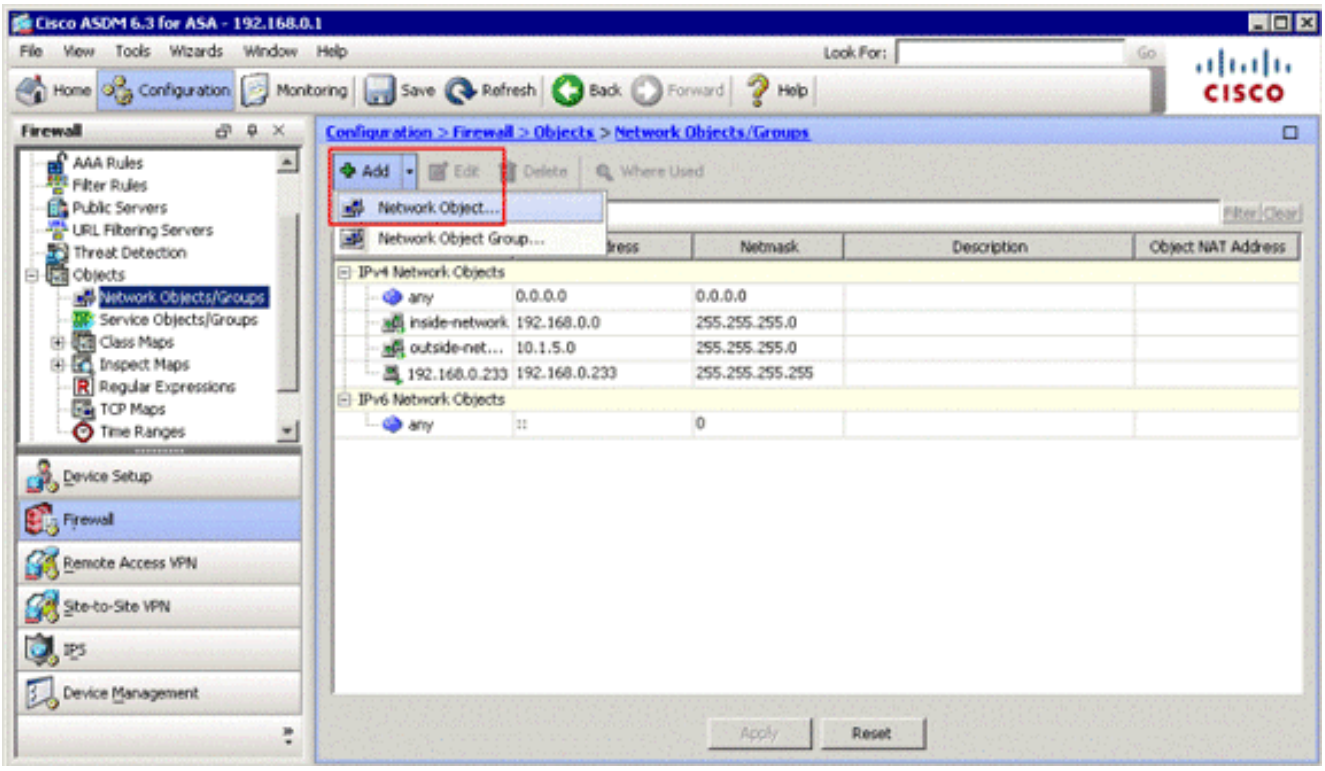
Добавьте сетевые объекты

Выполните эти шаги для добавления сетевых объектов:

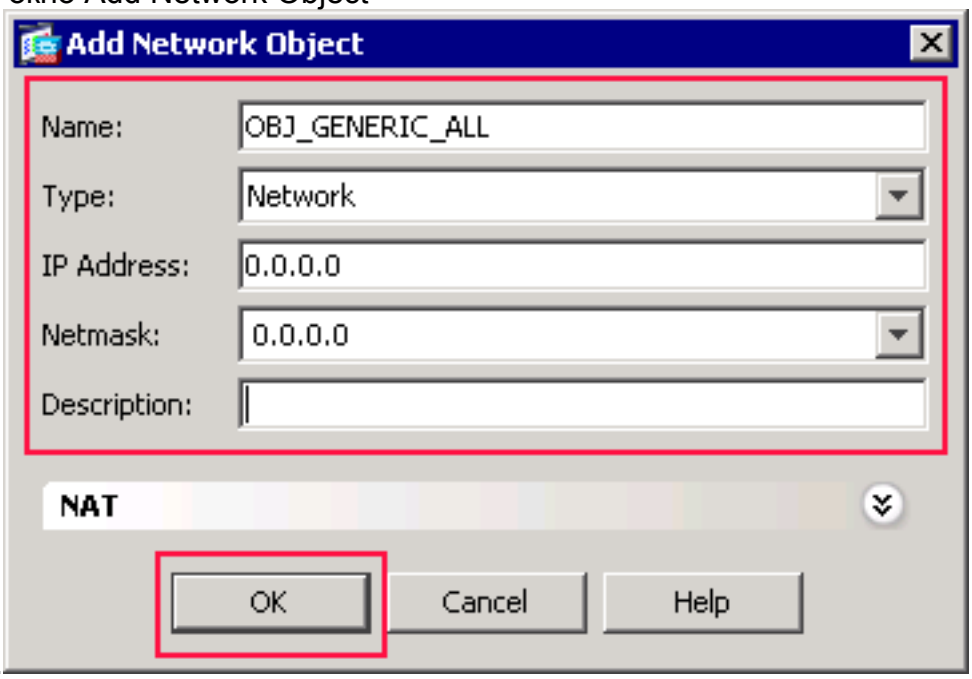
1. Войдите к ASDM и выберите **Configuration> Firewall> Objects> Network Objects/Groups**.



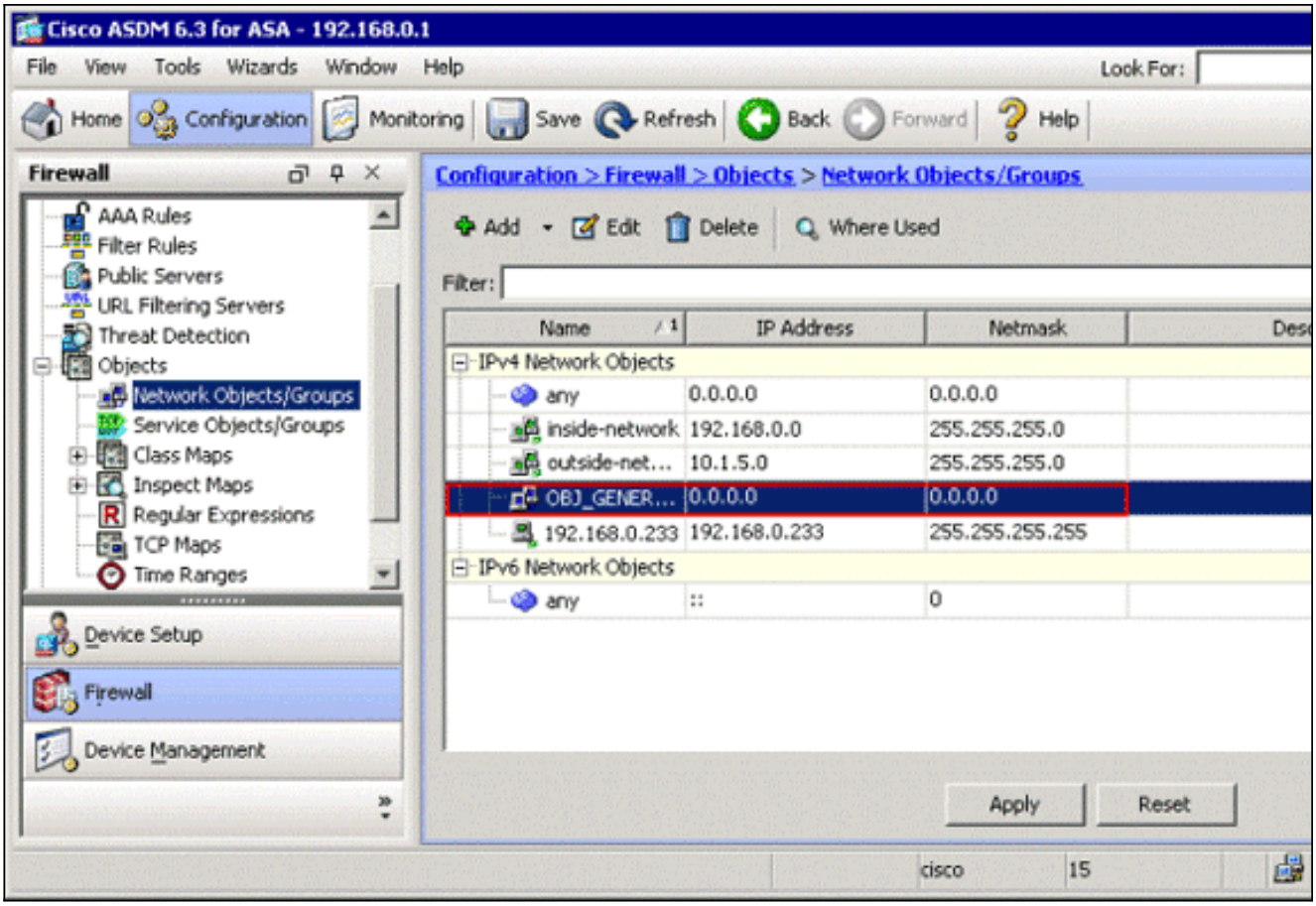
2. Выберите **Add> Network Object** для добавления сетевого объекта.



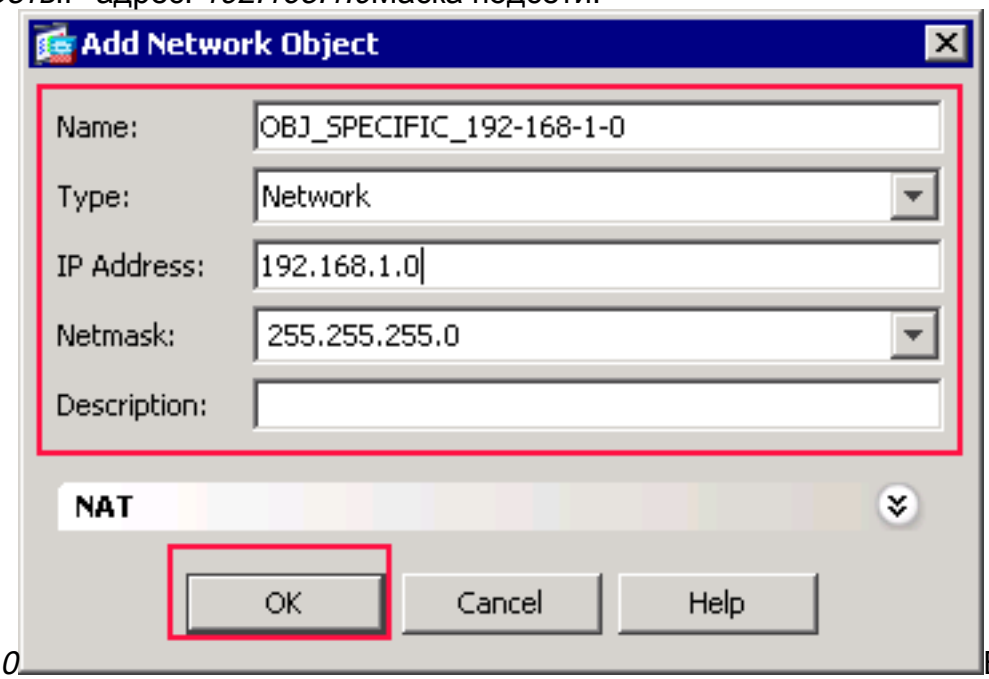
Диалоговое окно Add Network Object появляется.



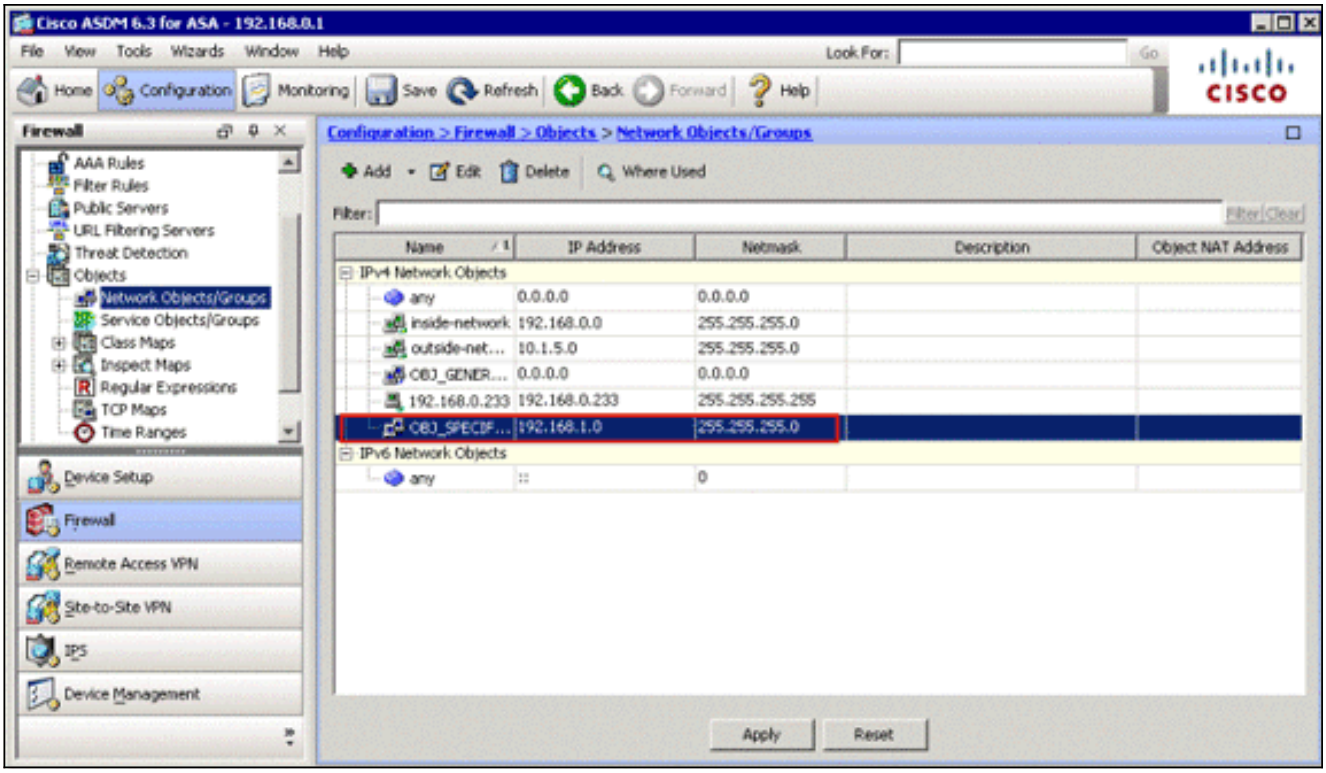
3. Введите эту информацию в диалоговое окно Add Network Object:Название сетевого объекта. (Данный пример использует *OBJ_GENERIC_ALL*.)Объект типа сети. (Данный пример использует *Сеть*.)IP-адрес для сетевого объекта. (Данный пример использует *0.0.0.0*.)Маска подсети для сетевого объекта. (Данный пример использует *0.0.0.0*.)
4. **Нажмите кнопку OK.**Сетевой объект создан и появляется в Сетевом списке Объектов/Групп, как показано в этом образе:



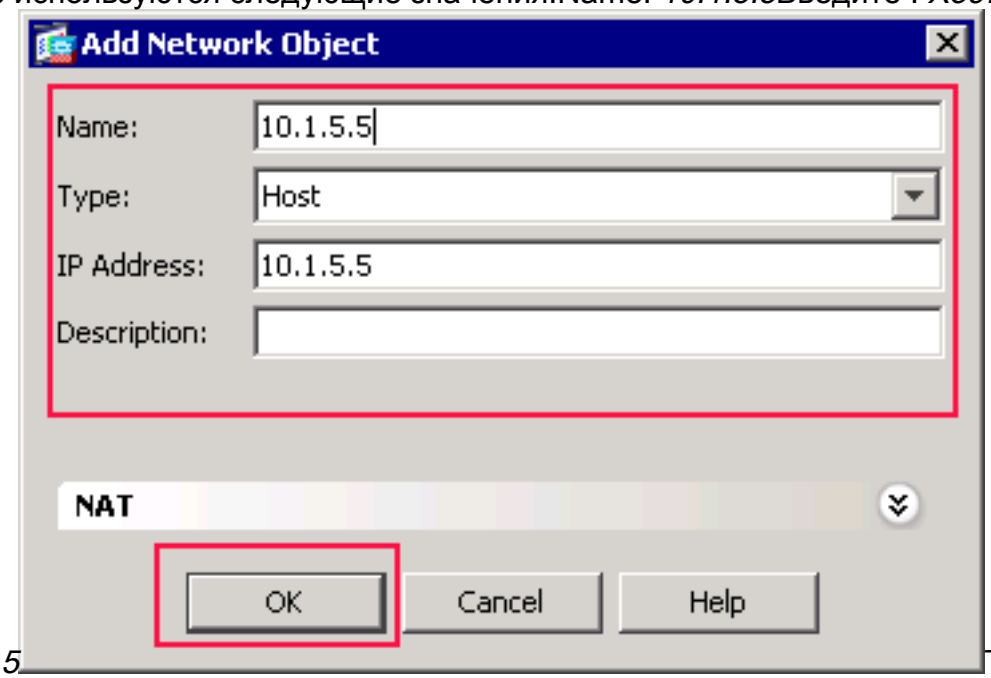
5. Повторите предыдущие шаги, чтобы добавить второй сетевой объект и нажать **OK**.В этом примере используются следующие значения:Name: *OBJ_SPECIFIC_192-168-1-0*Введите : *Сеть*IP-адрес: *192.168.1.0*Маска подсети:



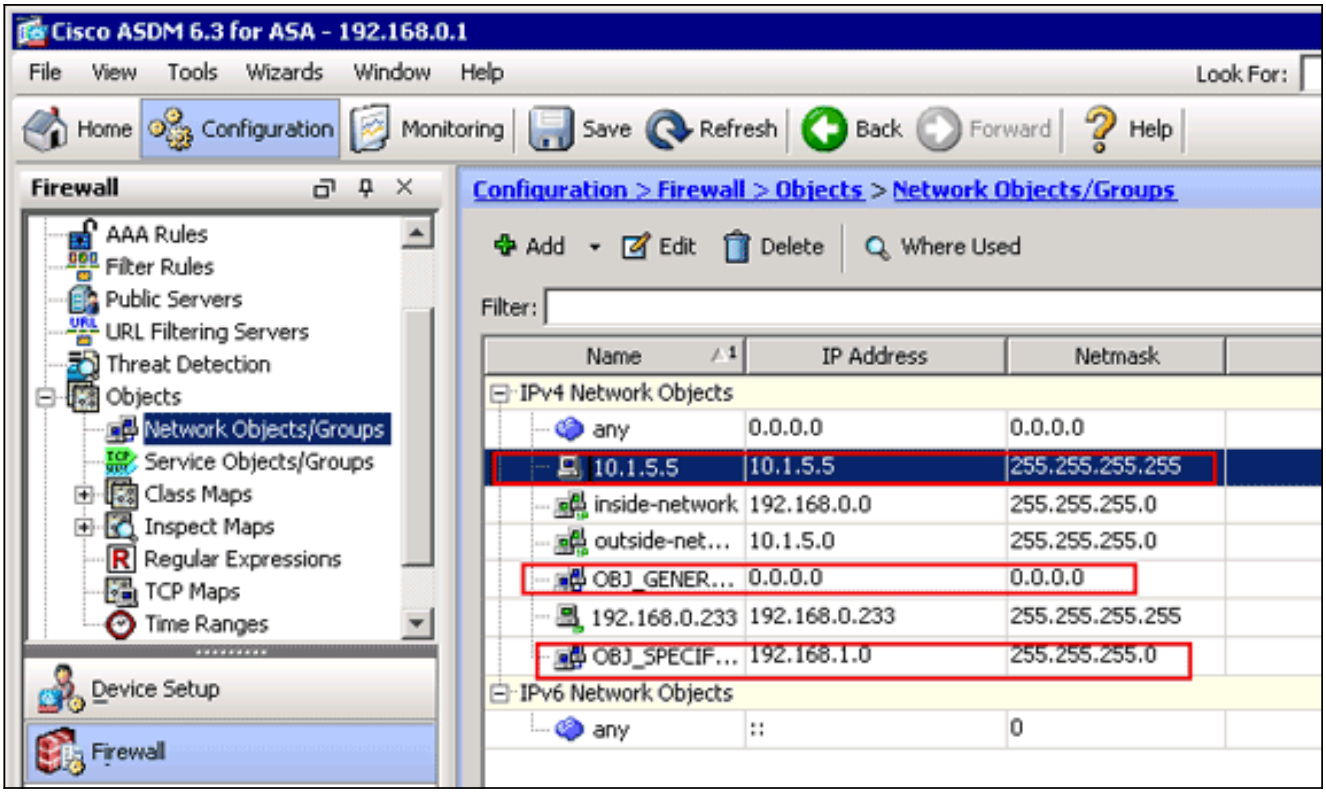
*255.255.255.0*Второй объект создан и появляется в Сетевом списке Объектов/Групп, как показано в этом образе:



6. Повторите предыдущие шаги, чтобы добавить третий сетевой объект и нажать **OK**.В этом примере используются следующие значения:Name: *10.1.5.5*Введите : *Хост*IP-адрес: *10.1.5.5*



Третьи сетевые объекты созданы и появляются в Сетевом списке Объектов/Групп.

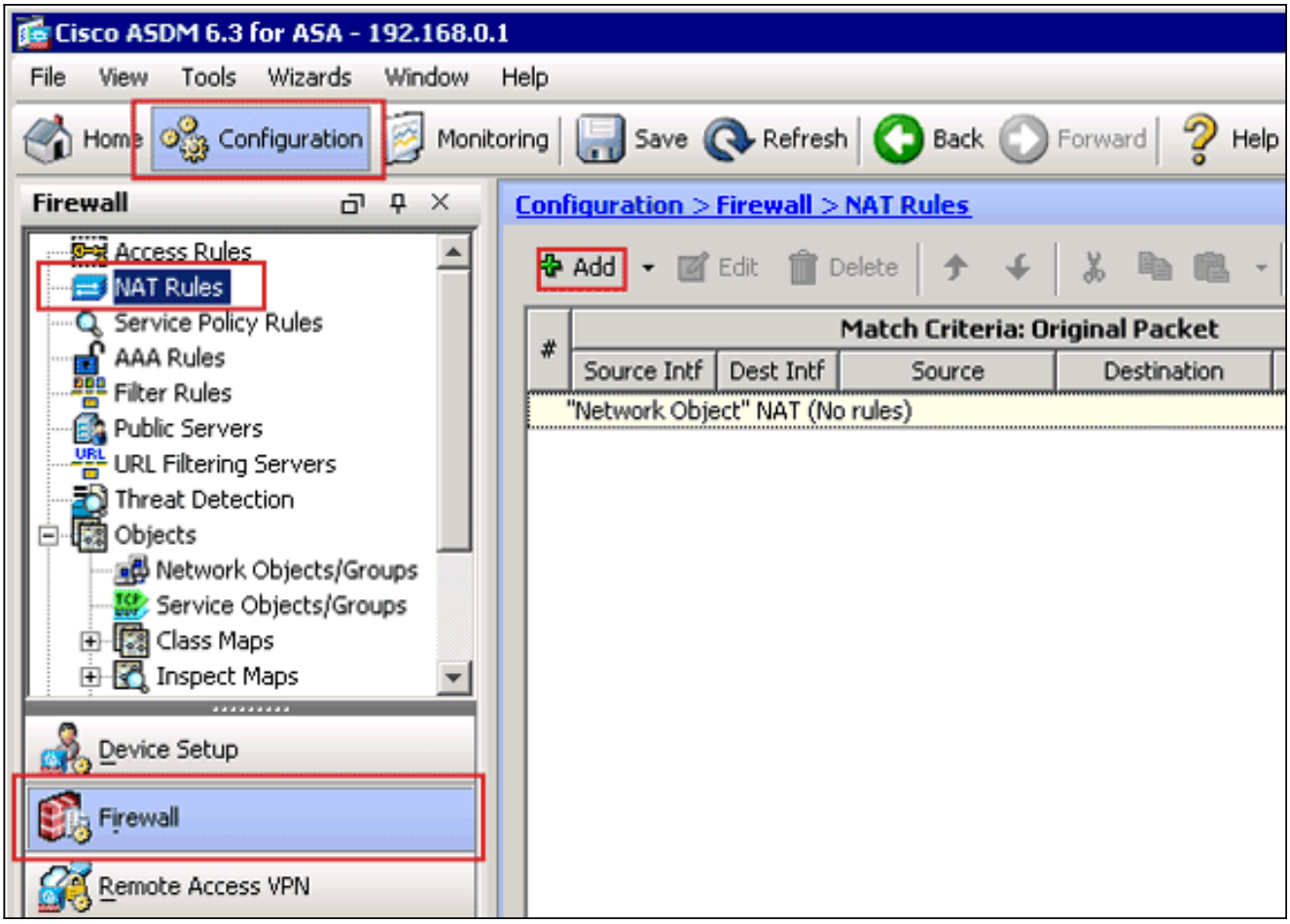


Сетевой список Объектов/Групп должен теперь включать эти три требуемых объекта, необходимые для правил NAT сослаться.

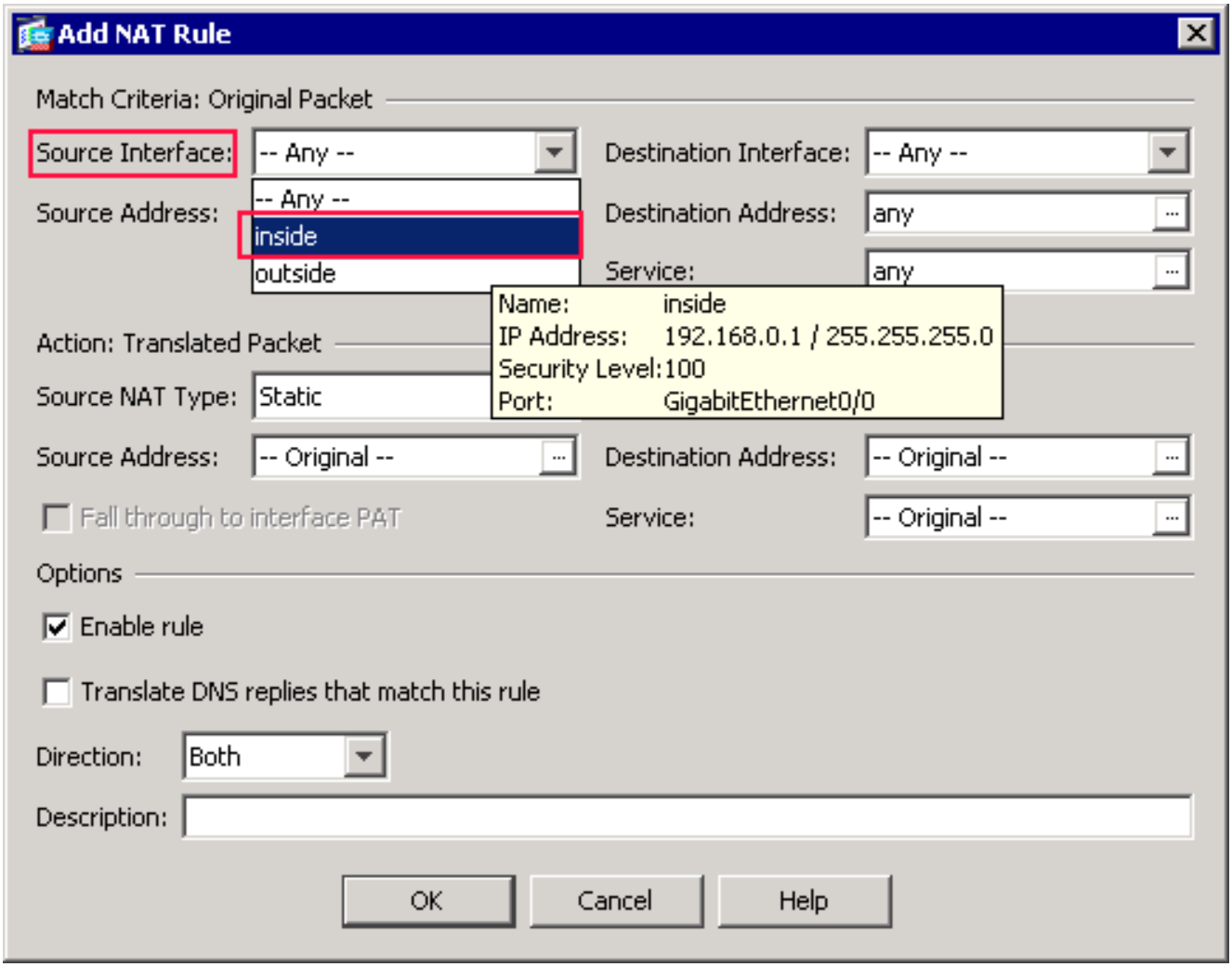
Создайте Правила NAT/PAT

Выполните эти шаги для создания правил NAT/PAT:

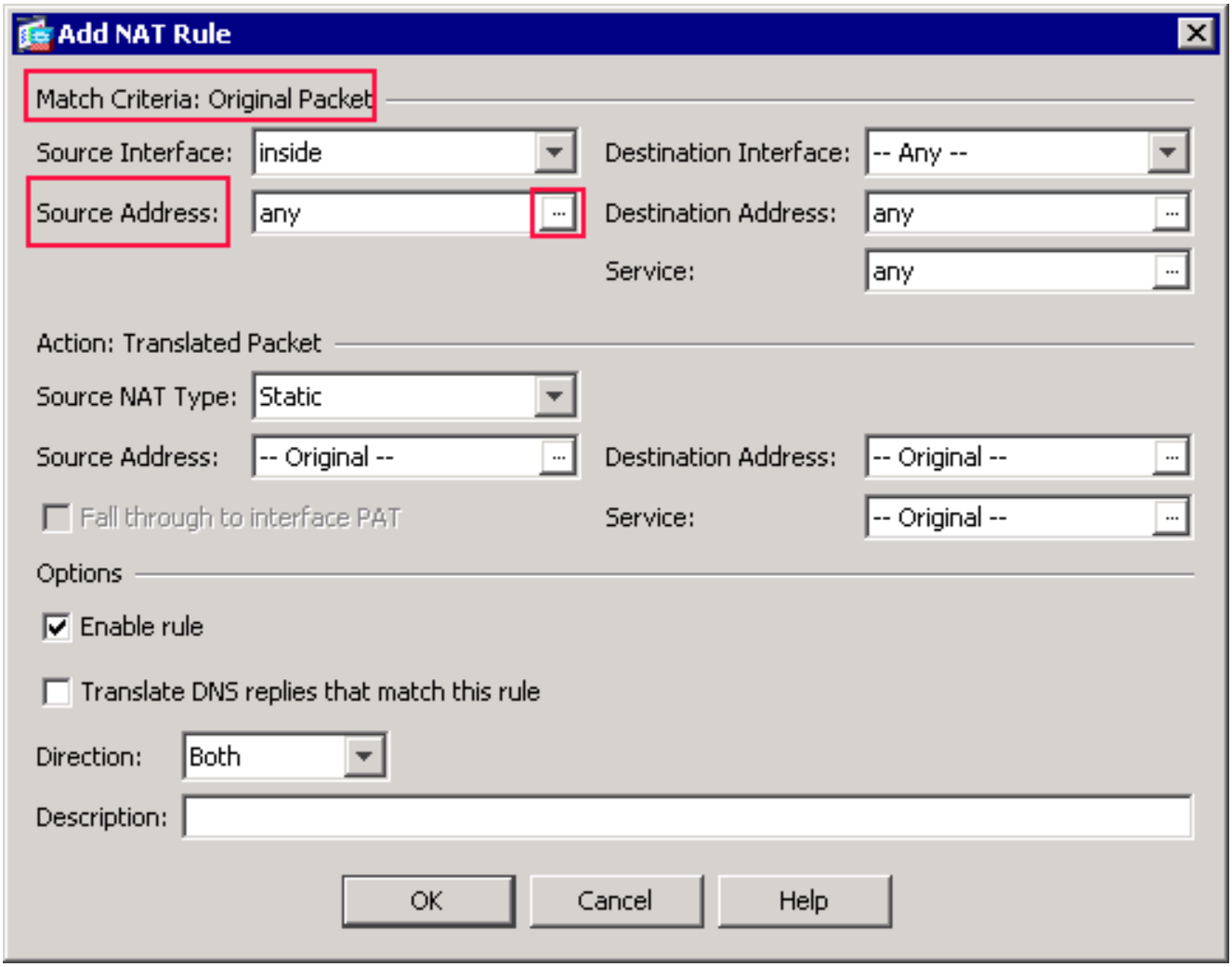
1. Создайте первое правило NAT/PAT:В ASDM выберите **Configuration> Firewall> NAT Rules** и **нажмите**
   Add.



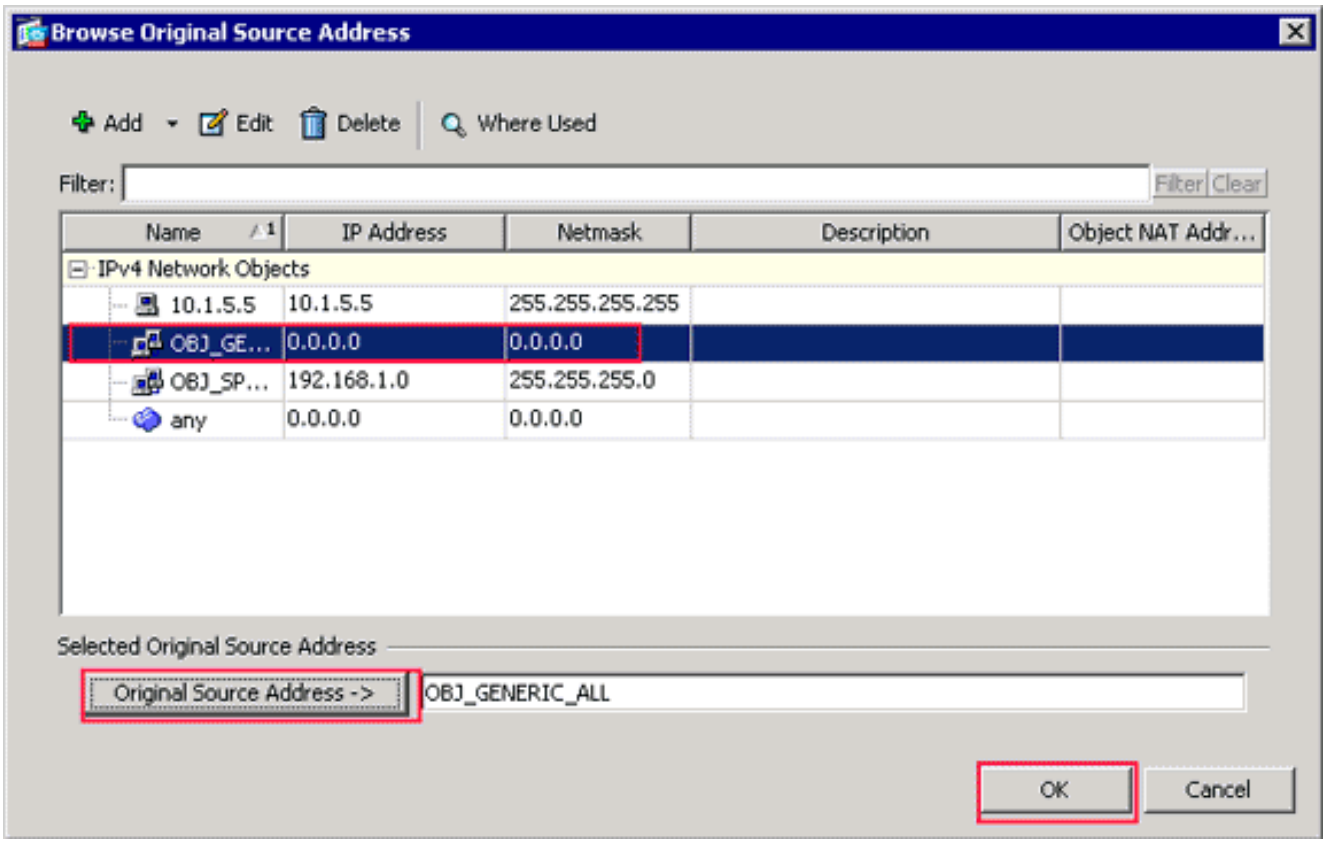
Диалоговое окно Add NAT Rule появляется.



В Условиях соответствия: область Original Packet диалогового окна Add NAT Rule, выберите **внутри** из выпадающего списка Исходного интерфейса.

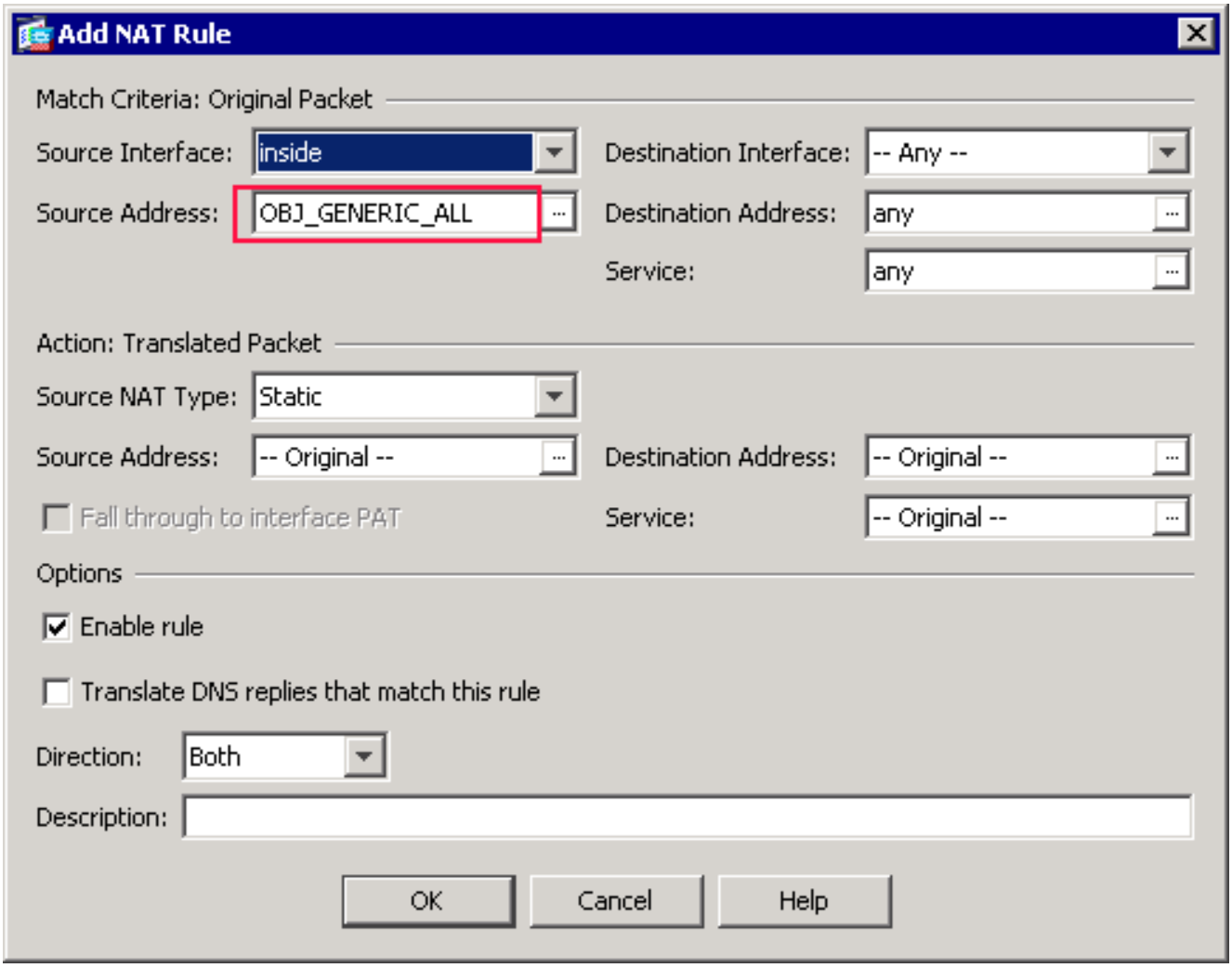


Нажмите обзор (...) кнопка, расположенная направо от текстового поля Адреса источника.Диалоговое окно Browse Original Source Address появляется.

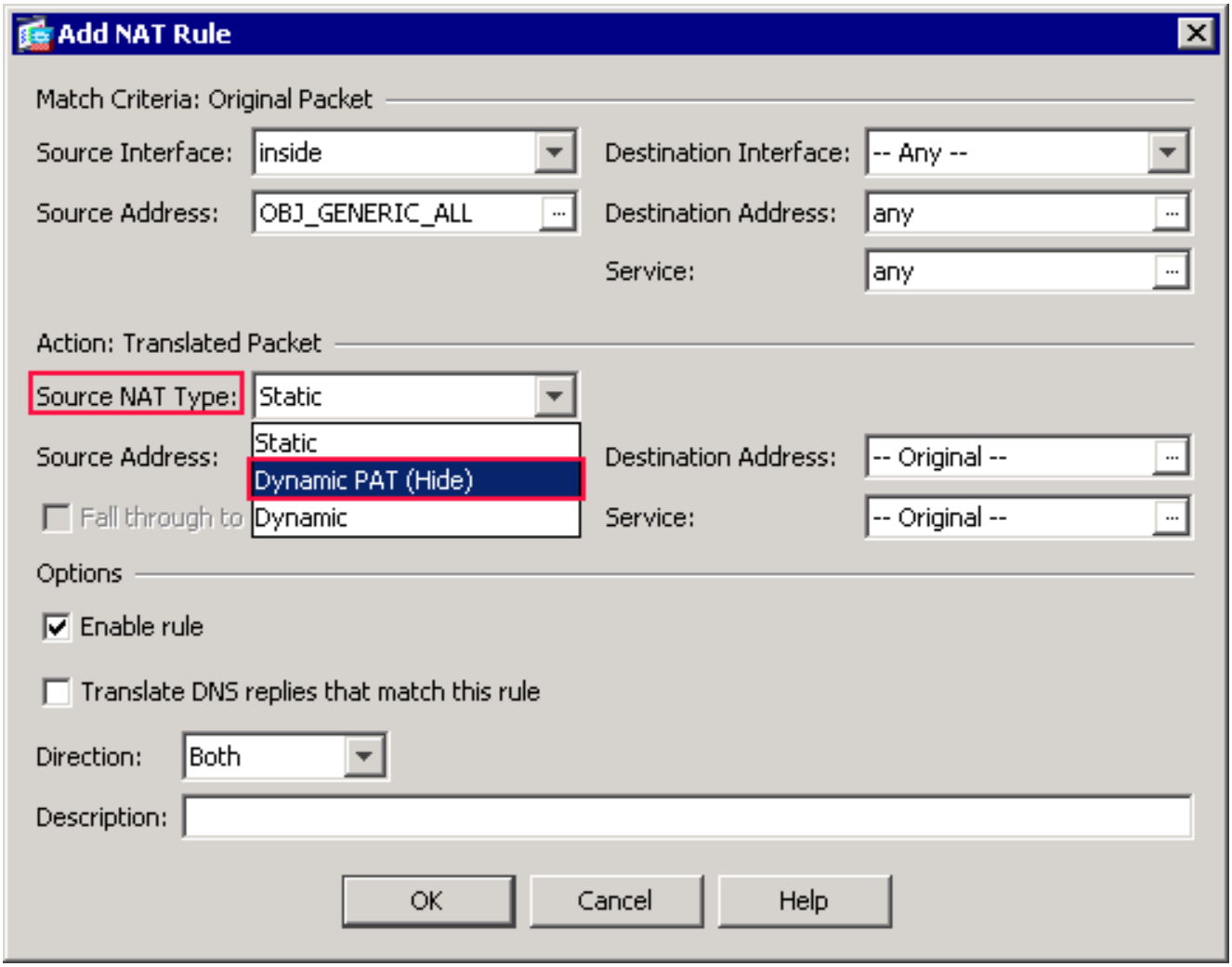


В диалоговом окне Browse Original Source Address выберите первый сетевой объект,

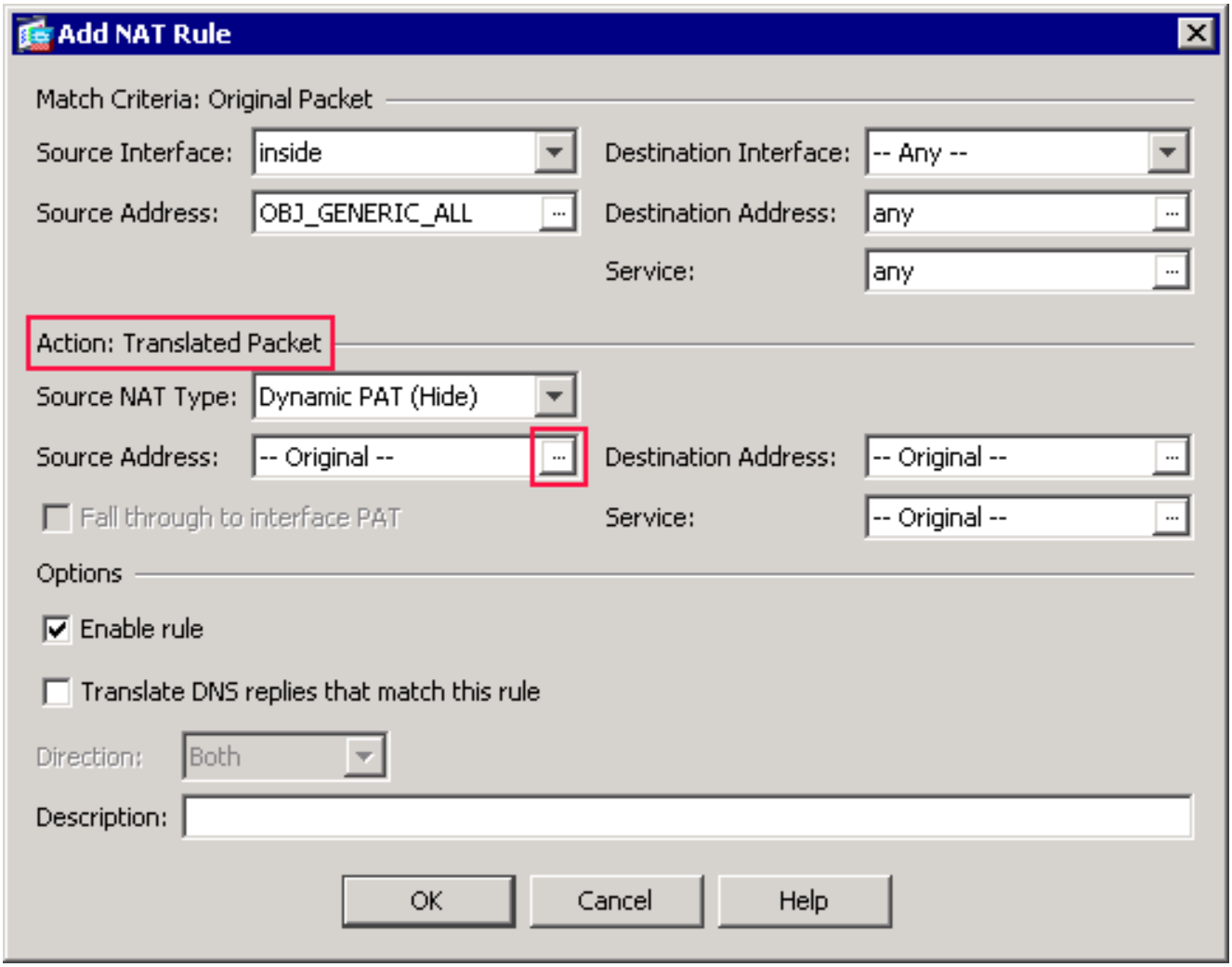
который вы создали. (Для данного примера выберите **OBJ_GENERIC_ALL**.)Нажмите **Original Source Address** и нажмите **OK**.Сетевой объект *OBJ_GENERIC_ALL* теперь появляется в Поле исходного адреса в Условиях соответствия: область Original Packet диалогового окна Add NAT
Rule.



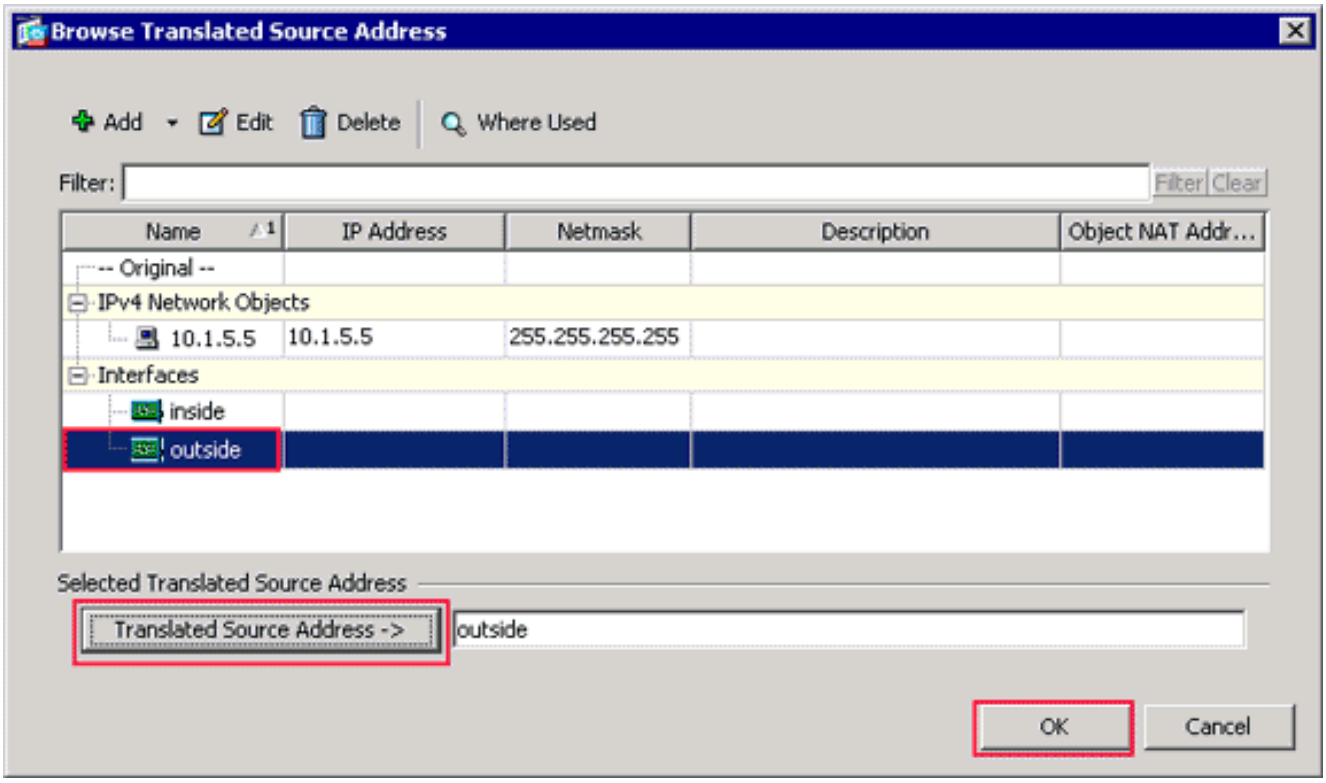
В Действии: Преобразованная область Packet диалогового окна Add NAT Rule, выберите **Dynamic PAT (Hide)** из диалогового окна Source NAT
Type.



Нажмите обзор (**...**) кнопка, расположенная направо от Поля исходного адреса.

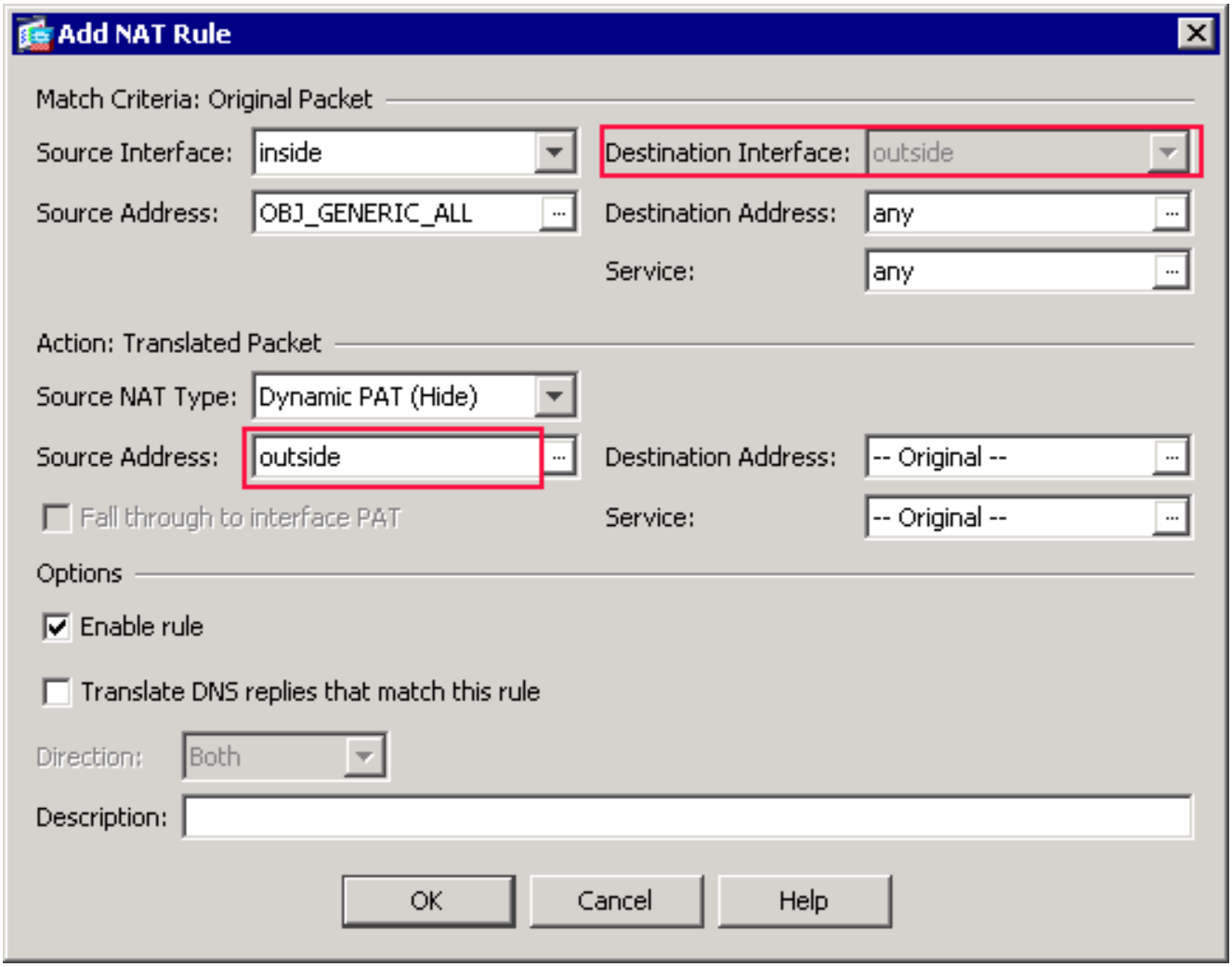


Обзор Преобразованное диалоговое окно Source Address появляется.

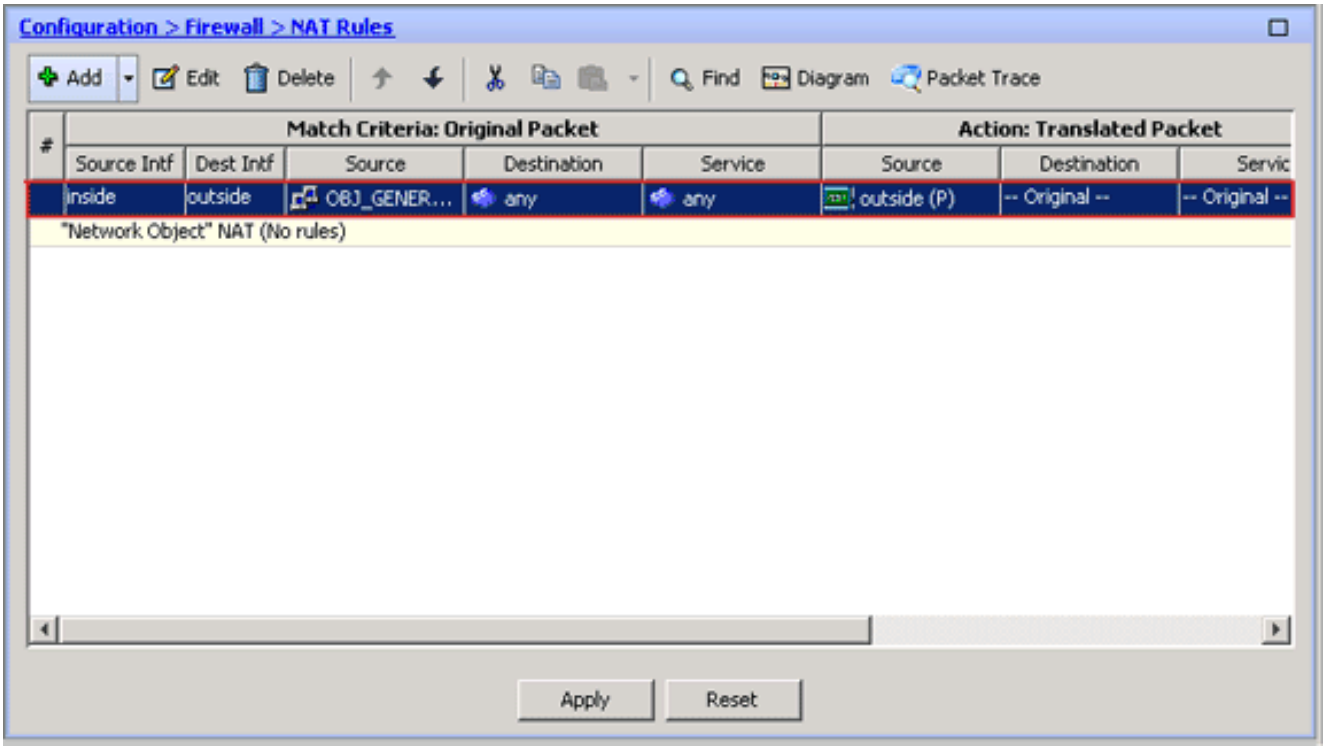


В Обзоре Преобразованное диалоговое окно Source Address выберите объект **внешнего интерфейса**. (Этот интерфейс был уже создан, потому что это - часть оригинальной конфигурации.)Нажмите **Translated Source Address** и нажмите

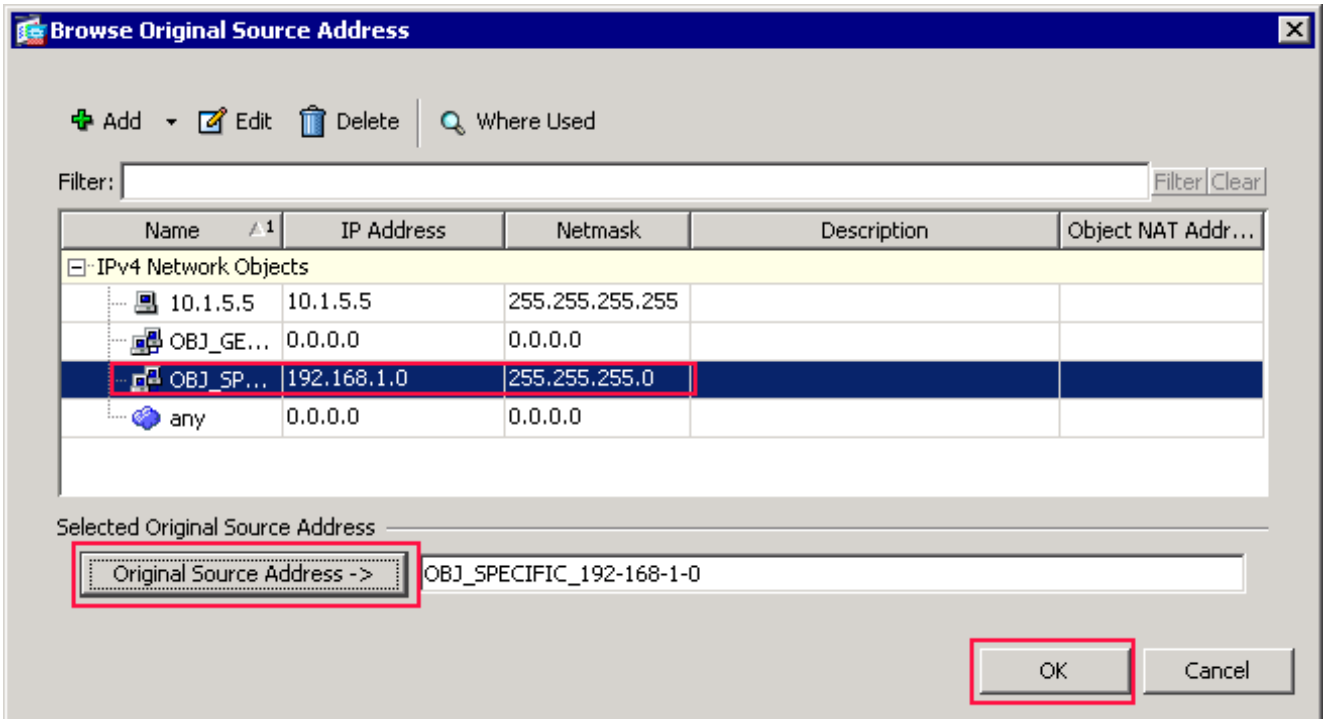
OK.Внешний интерфейс теперь появляется в Поле исходного адреса в Действии: Преобразованная область Packet на диалоговом окне Add NAT Rule.



Примечание: Поле *Destination Interface* также изменяется на внешний интерфейс.Проверьте, что первое завершенное Правило PAT появляется следующим образом:В Условиях соответствия: область Original Packet, проверьте эти значения:Исходный интерфейс = внутриАдрес источника = OBJ_GENERIC_ALLАдрес назначения (DA) = любойСервис = любойВ Действии: Преобразованная область Packet, проверьте эти значения:Источник тип NAT = динамический PAT (скрывается)Адрес источника = снаружиАдрес назначения (DA) = исходныйСервис = исходный**Нажмите кнопку OK.**Первое правило NAT появляется в ASDM, как показано в этом
образе:

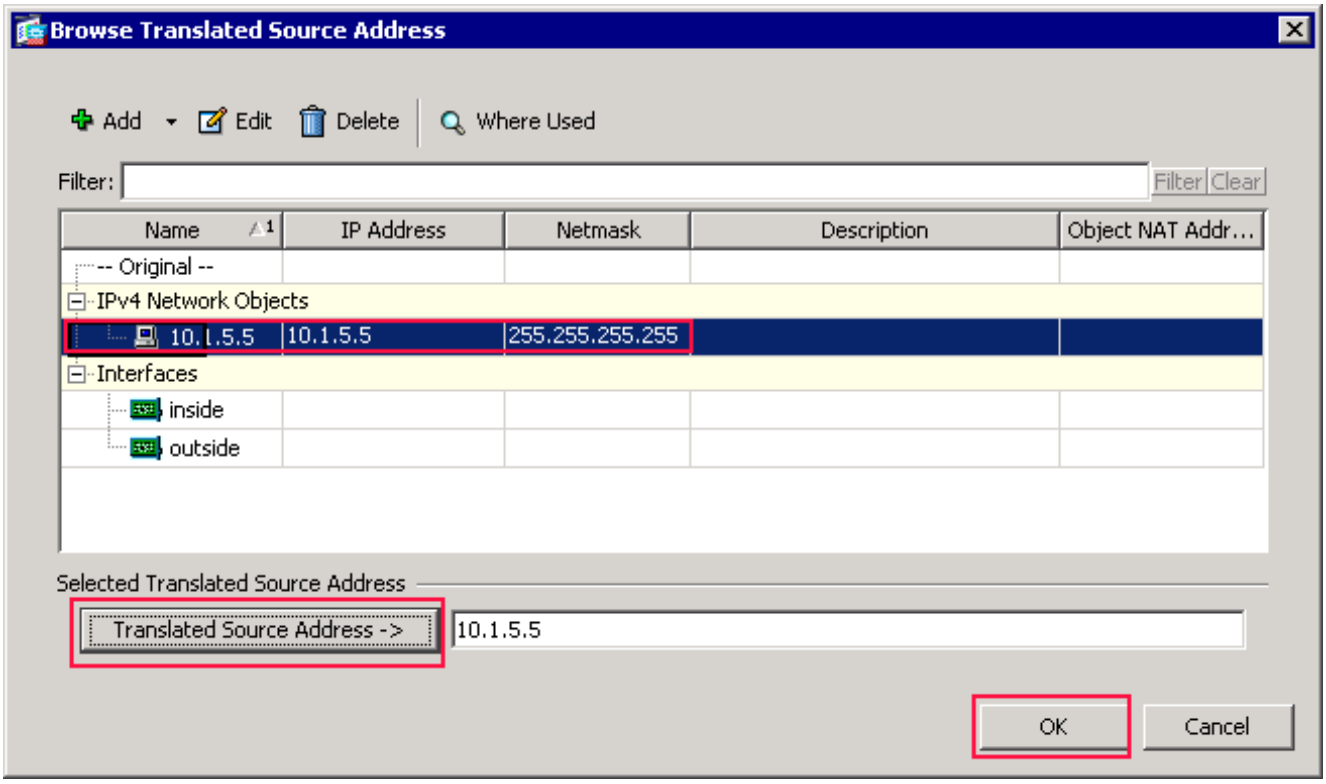


2. Создайте второе правило NAT/PAT:В ASDM выберите **Configuration> Firewall> NAT Rules** и **нажмите Add**.В Условиях соответствия: область Original Packet диалогового окна Add NAT Rule, выберите **внутри** из выпадающего списка Исходного интерфейса.Нажмите обзор **(...)** кнопка, расположенная направо от Поля исходного адреса.Диалоговое окно Browse Original Source Address появляется.

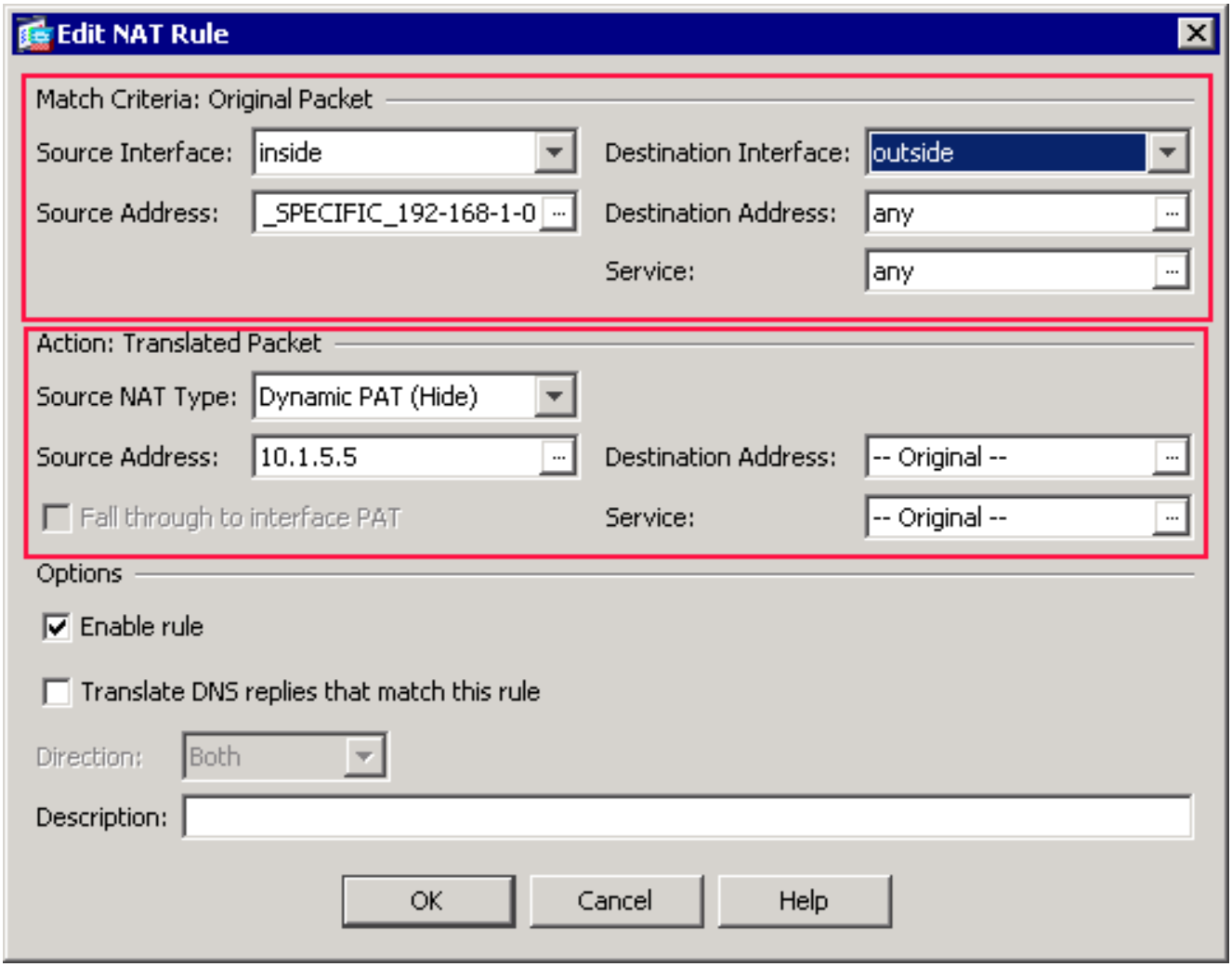


В диалоговом окне Browse Original Source Address выберите второй объект, который вы создали. (Для данного примера выберите **OBJ_SPECIFIC_192-168-1-0**.)Нажмите **Original Source Address** и нажмите **OK**.*OBJ_SPECIFIC_192-168-1-0* сетевой объект появляется в Поле исходного адреса в Условиях соответствия: область Original Packet диалогового окна Add NAT Rule..В Действии: Преобразованная область Packet диалогового окна Add NAT Rule, выберите **Dynamic PAT (Hide)** из диалогового окна Source NAT Type.Нажмите **...** кнопку, расположенную направо от Поля исходного

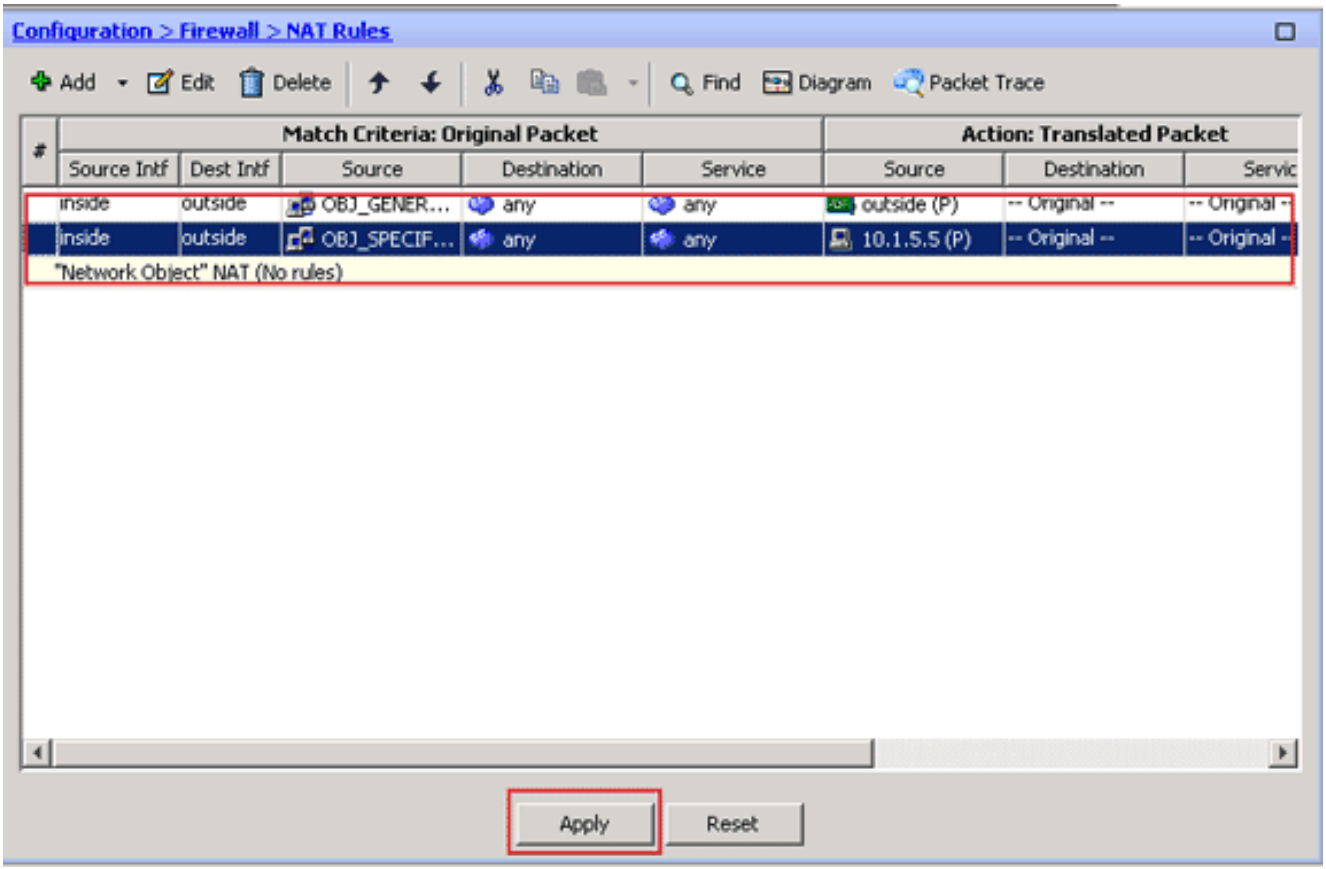
адреса.Обзор Преобразованное диалоговое окно Source Address появляется.



В Обзоре Преобразованное диалоговое окно Source Address выберите эти **10.1.5.5** объектов. (Этот интерфейс был уже создан, потому что это - часть оригинальной конфигурации).Нажмите **Translated Source Address**, и затем нажмите **OK**.**10.1.5.5** сетевых объектов появляются в Поле исходного адреса в Действии: Преобразованная область Packet диалогового окна Add NAT Rule..В Условиях соответствия: область Original Packet, выберите **снаружи** из выпадающего списка Интерфейса назначения.**Примечание:** Если вы не выберете *снаружи* для этой опции, то интерфейс назначения сошлется *на*
Любого.



Проверьте, что второе завершенное правило NAT/PAT появляется следующим образом:В Условиях соответствия: область Original Packet, проверьте эти значения:Исходный интерфейс = внутриАдрес источника = OBJ_SPECIFIC_192-168-1-0Адрес назначения (DA) = снаружиСервис = любойВ Действии: Преобразованная область Packet, проверьте эти значения:Источник тип NAT = динамический PAT (скрывается)Адрес источника = 10.1.5.5Адрес назначения (DA) = исходныйСервис = исходный**Нажмите кнопку OK.**Завершенная конфигурация NAT появляется в ASDM, как показано в этом
образе:



3. Нажмите кнопку **Apply** для применения изменений к рабочей конфигурации.

Это завершает конфигурацию динамического PAT на устройстве адаптивной защиты Cisco (ASA).

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

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

Проверка правила PAT общего назначения

- show local-host — Показывает состояния сети локальных хостов.ASA#**show local-host**
  Interface outside: 1 active, 2 maximum active, 0 denied local host: <125.252.196.170>, TCP flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark = unlimited UDP flow count/limit = 0/unlimited *!--- The TCP connection outside address corresponds !--- to the actual destination of 125.255.196.170:80* Conn: **TCP outside 125.252.196.170:80 inside 192.168.0.5:1051**, idle 0:00:03, bytes 13758, flags UIO TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04, bytes 11896, flags UIO Interface inside: 1 active, 1 maximum active, 0 denied local host: <192.168.0.5>, TCP flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark = unlimited UDP flow count/limit = 0/unlimited *!--- The TCP PAT outside address corresponds to the !--- outside IP address of the ASA – 10.1.5.1.* Xlate: TCP **PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988** flags ri idle 0:00:17 timeout 0:00:30 TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags ri idle 0:00:17 timeout 0:00:30 Conn: TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:03, bytes 13758, flags UIO TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04, bytes 11896, flags UIO
- show conn — Показывает состояние соединения для определяемого типа

соединения.
```
ASA#show conn 2 in use, 3 most used TCP outside 125.252.196.170:80 inside
192.168.0.5:1051, idle 0:00:06, bytes 13758, flags UIO TCP outside 125.252.196.170:80 inside
192.168.0.5:1050, idle 0:00:01, bytes 13526, flags UIO
```

- show xlate информацию о слотах преобразования.
```
ASA#show xlate 4 in use, 7 most used
Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity, T - twice TCP PAT from
inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags ri idle 0:00:23 timeout 0:00:30 TCP
PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags ri idle 0:00:23 timeout
0:00:30
```

Проверка определенного правила PAT

- show local-host — Показывает состояния сети локальных хостов.
```
ASA#show local-host
Interface outside: 1 active, 2 maximum active, 0 denied local host: <125.252.196.170>, TCP
flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark =
unlimited UDP flow count/limit = 0/unlimited !--- The TCP connection outside address
corresponds to !--- the actual destination of 125.255.196.170:80. Conn: TCP outside
125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07, bytes 13758, flags UIO TCP outside
125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03, bytes 11896, flags UIO Interface
inside: 1 active, 1 maximum active, 0 denied local host: <192.168.0.5>, TCP flow count/limit
= 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark = unlimited UDP flow
count/limit = 0/unlimited !--- The TCP PAT outside address corresponds to an !--- outside IP
address of 10.1.5.5. Xlate: TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961
flags ri idle 0:00:17 timeout 0:00:30 TCP PAT from inside:192.168.1.5/1066 to
outside:10.1.5.5/23673 flags ri idle 0:00:17 timeout 0:00:30 Conn: TCP outside
125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07, bytes 13758, flags UIO TCP outside
125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03, bytes 11896, flags UIO
```

- show conn — Показывает состояние соединения для определяемого типа соединения.
```
ASA#show conn 2 in use, 3 most used TCP outside 125.252.196.170:80 inside
192.168.1.5:1067, idle 0:00:07, bytes 13653, flags UIO TCP outside 125.252.196.170:80 inside
192.168.1.5:1066, idle 0:00:03, bytes 13349, flags UIO
```

- show xlate информацию о слотах преобразования.
```
ASA#show xlate 3 in use, 9 most used
Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity, T - twice TCP PAT from
inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags ri idle 0:00:23 timeout 0:00:30 TCP
PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/29673 flags ri idle 0:00:23 timeout
0:00:30
```

Устранение неполадок

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

Дополнительные сведения

- Диспетчер адаптивных устройств защиты Cisco (Cisco Adaptive Security Device Manager)
- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация