# Настройте ASA для двойных внутренних сетей

## Содержание



## Введение

Этот документ описывает, как настроить устройство адаптивной защиты Cisco (ASA), который работает под управлением ПО версии 9.x для использования двух внутренних сетей.

## Предварительные условия

### Требования

Для этого документа отсутствуют особые требования.

### Используемые компоненты

Сведения в этом документе основываются на Cisco ASA, который работает под управлением ПО версии 9. x.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

### Условные обозначения

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

## Общие сведения

Когда вы добавляете вторую внутреннюю сеть позади межсетевого экрана ASA, рассматриваете эту важную информацию:

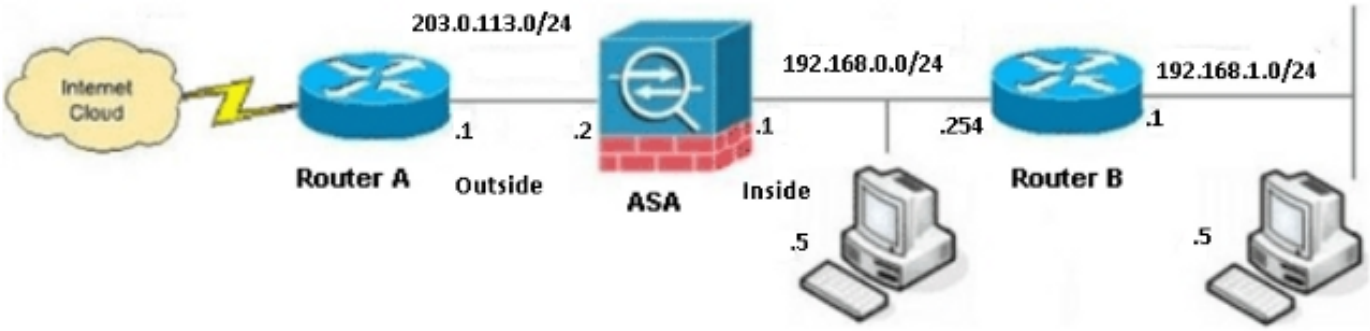
- ASA не поддерживает дополнительную адресацию.
- Маршрутизатор должен использоваться позади ASA для достижения маршрутизации между текущей сетью и недавно добавленной сетью.
- Шлюз по умолчанию для всех хостов должен указать к внутреннему маршрутизатору.
- Необходимо добавить маршрут по умолчанию на внутреннем маршрутизаторе, который указывает к ASA.
- Необходимо очистить кэш Протокола ARP на внутреннем маршрутизаторе.

## Настройка

Используйте информацию, которая описана в этом разделе для настройки ASA.

### Схема сети

Вот топология, которая используется для примеров всюду по этому документу:




**Примечание:** Схемы IP-адресации, которые используются в этой конфигурации, не юридически маршрутизируемы в Интернете. Они - адреса RFC 1918, которые используются в лабораторной среде.

## ASA 9.x конфигурация

Если у вас есть выходные данные **команды write terminal** от вашего устройства Cisco, можно использовать Средство интерпретации выходных данных (только зарегистрированные клиенты), чтобы отобразить потенциальные проблемы и исправляете.

Вот конфигурация для ASA, который работает под управлением ПО версии 9. x:

```
ASA Version 9.3(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- This is the configuration for the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

!--- This is the configuration for the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!

boot system disk0:/asa932-smp-k8.bin

!--- This creates an object called OBJ_GENERIC_ALL.
!--- Any host IP address that does not already match another configured
!--- object will get PAT to the outside interface IP address
!--- on the ASA (or 10.1.5.1), for Internet-bound traffic.


object network OBJ_GENERIC_ALL
```

```
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 203.0.113.1
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
```

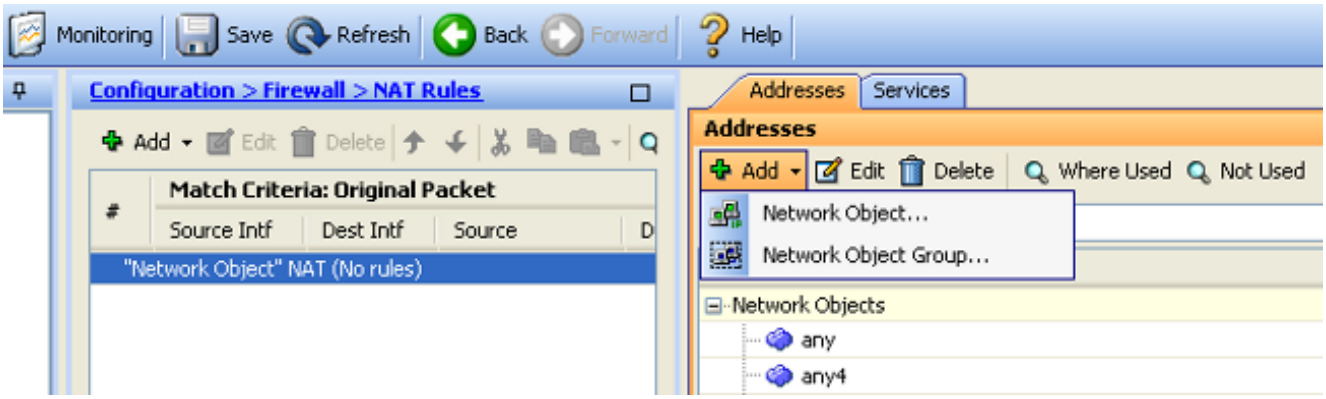
## Позвольте доступ для внутренних узлов внешним сетям с PAT

Если вы намереваетесь иметь внутренние хосты, совместно используют одиночный общий адрес для трансляции, используют Преобразование адресов портов (PAT). Одна из самых простых конфигураций PAT включает трансляцию всех внутренних хостов так, чтобы они,

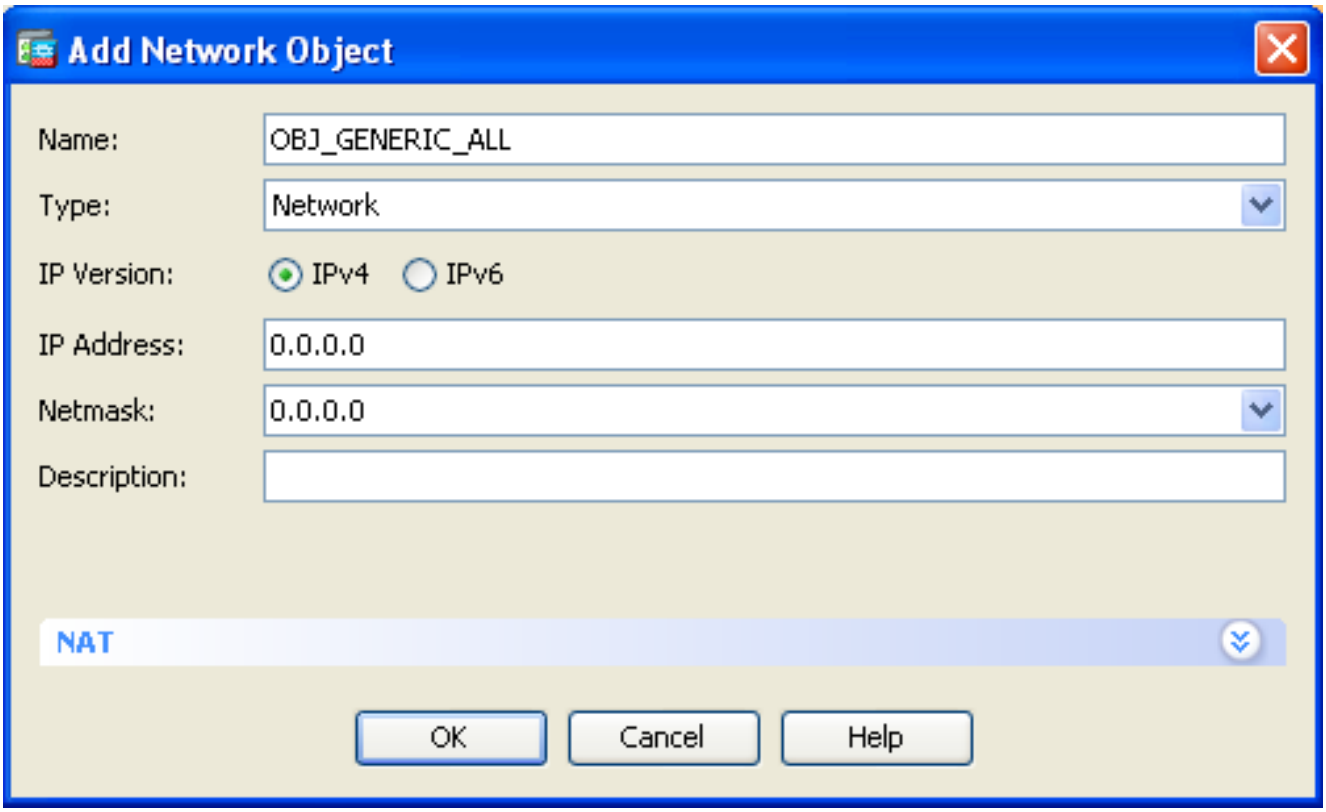
казалось, были IP внешнего интерфейса. Это - типичная конфигурация PAT, которая используется, когда количество маршрутизируемых IP - адресов, которые доступны от интернет-провайдера, ограничено только некоторыми, или всего один.

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

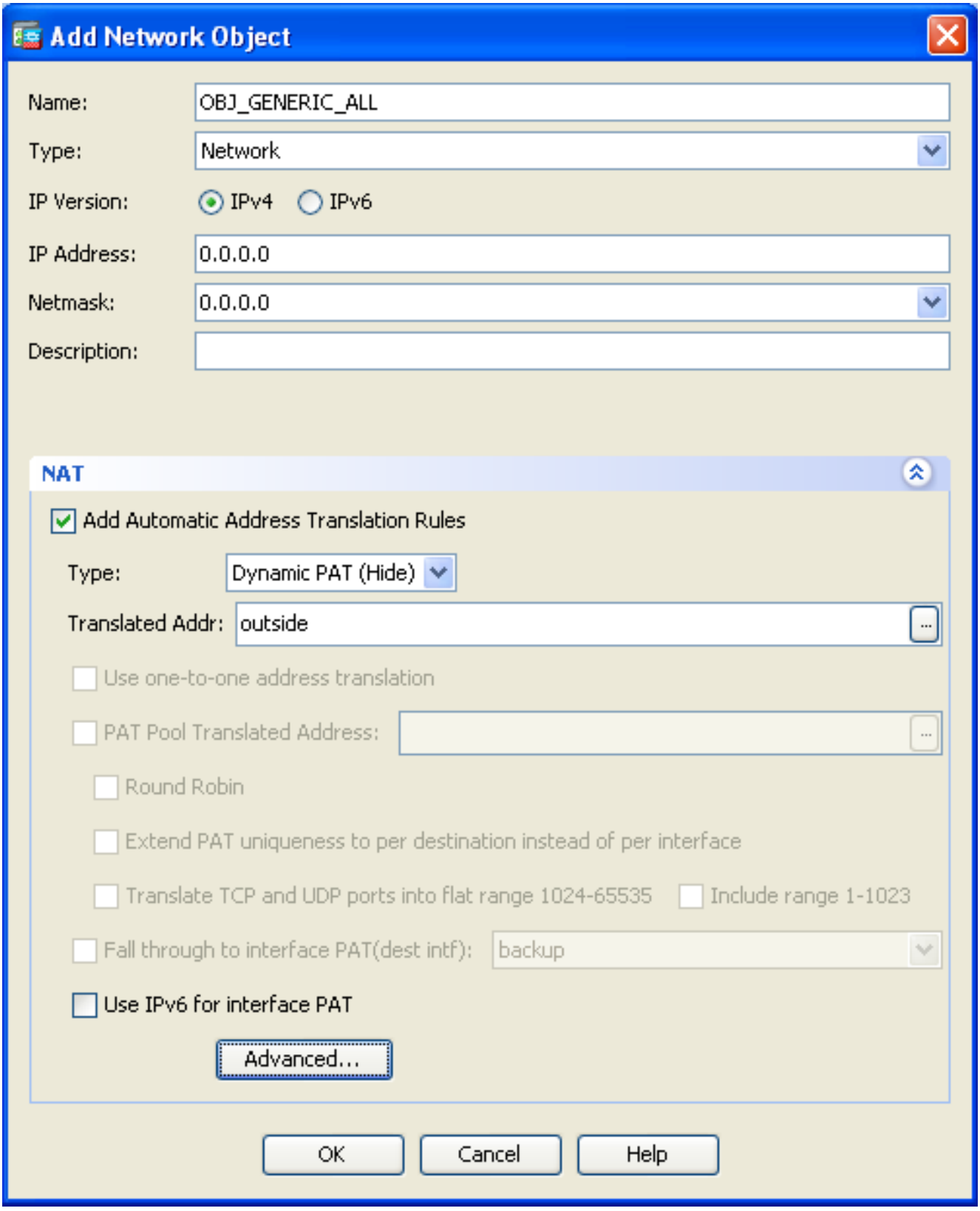
1. Перейдите к **Конфигурации> Межсетевой экран> Правила NAT**, **нажмите Add** и выберите **Network Object** для настройки правила динамического преобразования сетевых адресов (NAT):



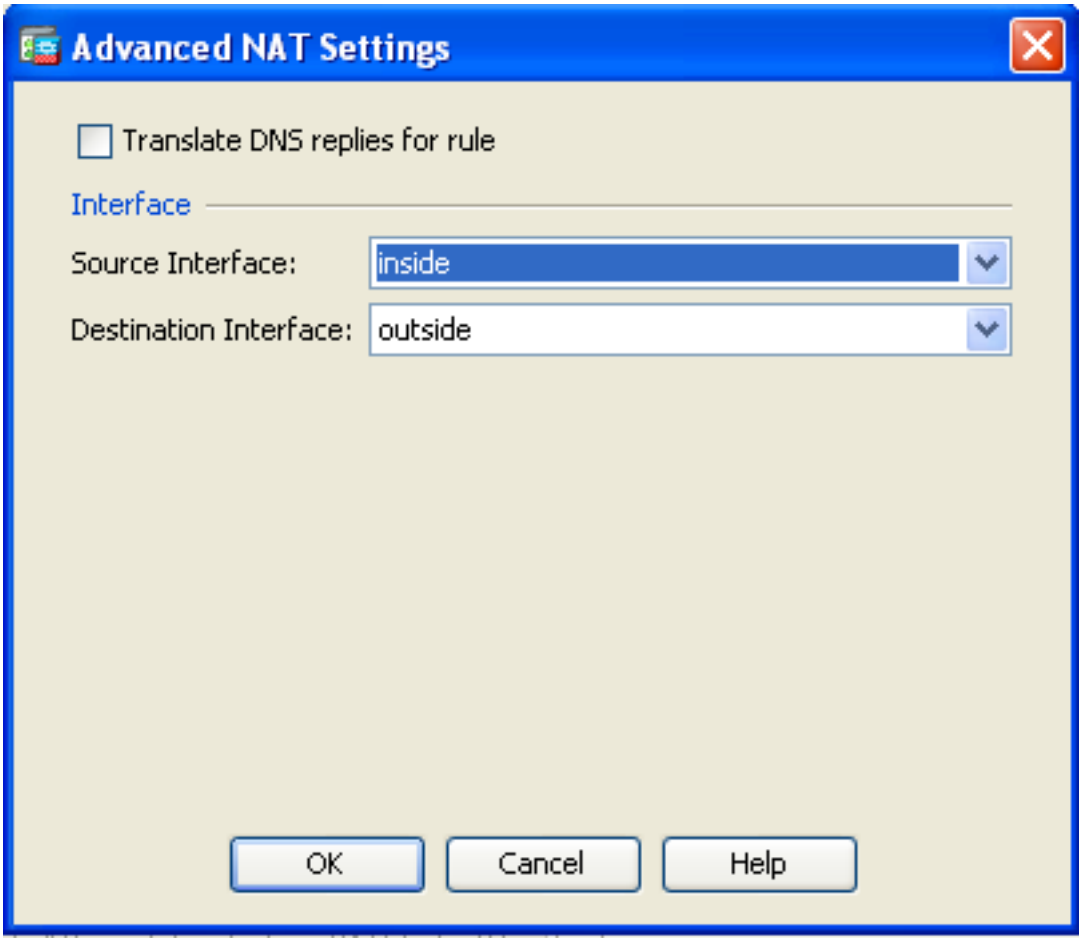

2. Настройте сеть/Хост/Диапазон, для которой требуется Динамический PAT. В данном примере были выбраны все внутренние подсети. Этот процесс должен быть повторен для определенных подсетей, которые вы хотите преобразовать этим способом:



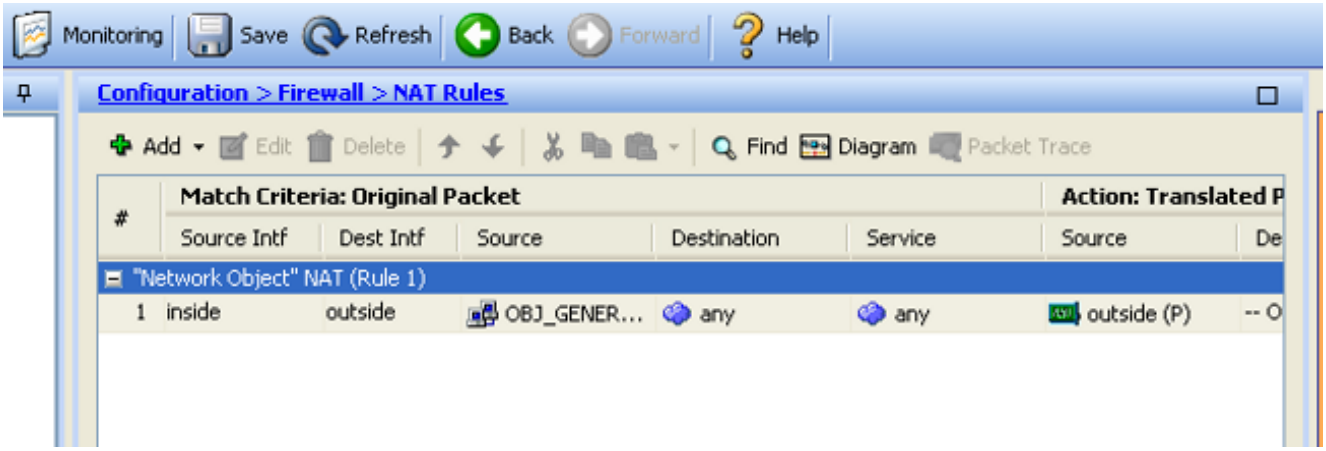

3. Нажмите **NAT**, проверьте флажок **Add Automatic Address Translation Rule**, введите **Динамичный,** и установите опцию **Translated Addr** так, чтобы это отразило внешний интерфейс. При нажатии кнопки замещающего знака она помогает вам выбирать предварительно сконфигурированный объект, такой как внешний интерфейс:




4. Нажмите **Advanced** для выбора источника и интерфейса назначения:




5. **Нажмите OK**, и затем нажмите **Apply** для применения изменений. Однажды завершенный, Менеджер устройств адаптивной безопасности (ASDM) (ASDM) показывает правило NAT:




## Конфигурация маршрутизатора B

Вот конфигурация для маршрутизатора B:

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-encryption
!
hostname Router B
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/1

!--- This assigns an IP address to the ASA-facing Ethernet interface.

ip address 192.168.0.254 255.255.255.0
no ip directed-broadcast

ip classless

!--- This route instructs the inside router to forward all of the
!--- non-local packets to the ASA.

ip route 0.0.0.0 0.0.0.0 192.168.0.1
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

# Проверка

Обратитесь к веб-сайту через HTTP через web-браузер, чтобы проверить, что ваша конфигурация работает должным образом.

Данный пример использует сайт, который размещен в IP-адресе *198.51.100.100*. Если соединение успешно, выходные данные, которые предоставлены в разделах, которые придерживаются, могут быть замечены на CLI ASA.

## Соединение

Введите команду **адреса show connection** для проверки соединения:

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 192.168.1.5:58799, 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 Списком контроля доступа (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.

> **Примечание:** См. Флаги TCP - подключения ASA (Наращивание соединения и разрушение) Документ Cisco для получения дополнительной информации о флагах соединения.

# Устранение неполадок

Используйте информацию, которая описана в этом разделе для устранения проблем проблем конфигурации.

## Системные журналы

Введите **команду show log** для просмотра системных журналов:

```
ASA(config)# show log | in 192.168.1.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
192.168.1.5/58799 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:192.168.1.5/58799 (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 *информационный уровень*.

В данном примере существует два генерируемые системных журнала. Первым является сообщение журнала, чтобы указать, что межсетевой экран создал трансляцию; в частности, динамическая трансляция TCP (PAT). Это указывает на IP - адрес источника и порт, а также 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

межсетевой экран был настроен для блокирования этой попытки подключения, или некоторый другой фактор запретил создание этого соединения (ограничения ресурса или вероятная неверная конфигурация), межсетевой экран не генерирует журнал, чтобы указать, что было создано соединение. Вместо этого это регистрирует причину для соединения, которое будет запрещено или индикация в отношении фактора, который запретил соединению то, чтобы быть созданным.

## Пакетные трассировщики

Введите эту команду для добавления пакетной функциональности трассировщика:

```
ASA(config)# packet-tracer input inside tcp 192.168.1.5 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 просматривать все различные шаги, проверки и функции, которые завершает 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 внутренний интерфейс.
- Протокол, который используется, является TCP.
- Моделируемый IP-адрес клиента 192.168.1.5.
- Клиент передает трафик, который получен 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 о внешнем интерфейсе в команде. Это происходит из-за пакетного дизайна трассировщика. Программное средство говорит вам, как межсетевой экран обрабатывает ту попытку типа соединения, которая включает, как это направило бы его, и из который интерфейс.

> **Совет:** Для получения дополнительной информации о пакетной функциональности трассировщика, обратитесь к пакетам Отслеживания с Пакетным разделом Трассировщика *руководства по настройке Cisco ASA 5500 с помощью CLI, 8.4 и 8.6*.

## Перехват

Введите эти команды для применения перехвата:

```
ASA# capture capin interface inside match tcp host 192.168.1.5 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 192.168.1.5.58799 > 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 > 192.168.1.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 192.168.1.5.58799 > 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 показывает конфигурацию двух перехватов, названных **capin** и **capout** на внутренних и внешних интерфейсах, соответственно. Команды **перехвата** используют ключевое слово **соответствия**, которое позволяет вам задавать трафик, который вы хотите перехватить.

Поскольку *capin* перехватывает пример, он обозначен, что вы хотите совпасть с трафиком, который замечен на внутреннем интерфейсе (вход или выход), который совпадает *с хостом 198.51.100.100 хоста 192.168.1.5 tcp*. Другими словами, вы хотите перехватить любой Трафик TCP, который передается от *хоста 192.168.1.5* до *хоста 198.51.100.100*, или наоборот. Использование ключевого слова **соответствия** позволяет межсетевому экрану перехватывать тот трафик двунаправленным образом. Команда **перехвата**, которая определена 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 можно тогда попытаться установить соединение снова и продолжить просматривать перехваты с командой ***<capture_name>* show capture**. В данном примере вы видите, что клиент в состоянии соединиться с сервером, как очевидный трехсторонним квитированием TCP, которое замечено в перехватах.

# Дополнительные сведения

- Диспетчер адаптивных устройств защиты Cisco (Cisco Adaptive Security Device Manager)
- Cisco ASA 5500-X Series межсетевые экраны следующего поколения

- Запросы на комментарий (RFC)
- Руководство по настройке интерфейса командной строки для Cisco ASA, 9.0 Статичных Настроек Г¦ и Маршруты по умолчанию
- Техническая поддержка и документация Г¦ C i s c o S y s t e m s