PIX/ASA 7.x и FWSM: NAT и инструкции PAT

Содержание

Введение

В этом документе показаны основные примеры конфигурации преобразования сетевых адресов (NAT) и преобразования адресов портов (PAT) на устройствах защиты Cisco PIX/ASA. Предоставляются диаграммы упрощенной сети. Консультируйтесь с документацией PIX/ASA для своей версии программного обеспечения PIX/ASA для получения дальнейшей информации.

Дополнительную информацию о командах nat, global, static, conduit и access-list и перенаправлении портов в PIX для ПО PIX 5.x и выше см. в разделе Использование команд nat, global, static, conduit, access-list и функции перенаправления портов в PIX.

Дополнительную информацию об основных конфигурациях NAT и PAT для брандмауэра Cisco Secure PIX см. в документе Использование инструкций NAT и PAT для брандмауэра Cisco Secure PIX.

Для получения дополнительной информации о конфигурации NAT в версии ASA 8.3 и позже, обратитесь к информации О NAT.

Примечание: NAT в прозрачном режиме поддерживается от версии 8 PIX/ASA. x. См. NAT в Прозрачном режиме для получения дополнительной информации.

Предварительные условия

Требования

Читатели данной документации должны быть хорошо осведомлены об Устройстве безопасности PIX/ASA Cisco.

Используемые компоненты

Сведения в этом документе основываются на Версии программного обеспечения 7.0 устройства защиты Cisco PIX серии 500 и позже.

Примечание: Этот документ повторно сертифицировался с версией 8 PIX/ASA. x.

Примечание: Команды, используемые в них, документируют, применимы к Модулю Сервиса межсетевого экрана (FWSM).

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.

Команда nat-control

Команда nat-control на PIX/ASA указывает, что весь трафик через межсетевой экран должен иметь определенное транслируемое значение (**выражение NAT** с соответствующим **глобальным** или **статическое состояние**) для того трафика для прохождения через межсетевой экран. **Команда nat-control обеспечивает такой же способ преобразования, как и в брандмауэрах PIX с версиями ПО, предшествующими 7.0**. Конфигурация по умолчанию версии 7.0 PIX/ASA и позже является спецификацией **команды no nat-control**. С версией 7.0 PIX/ASA и позже, можно изменить это поведение при запуске **команды nat-control**.

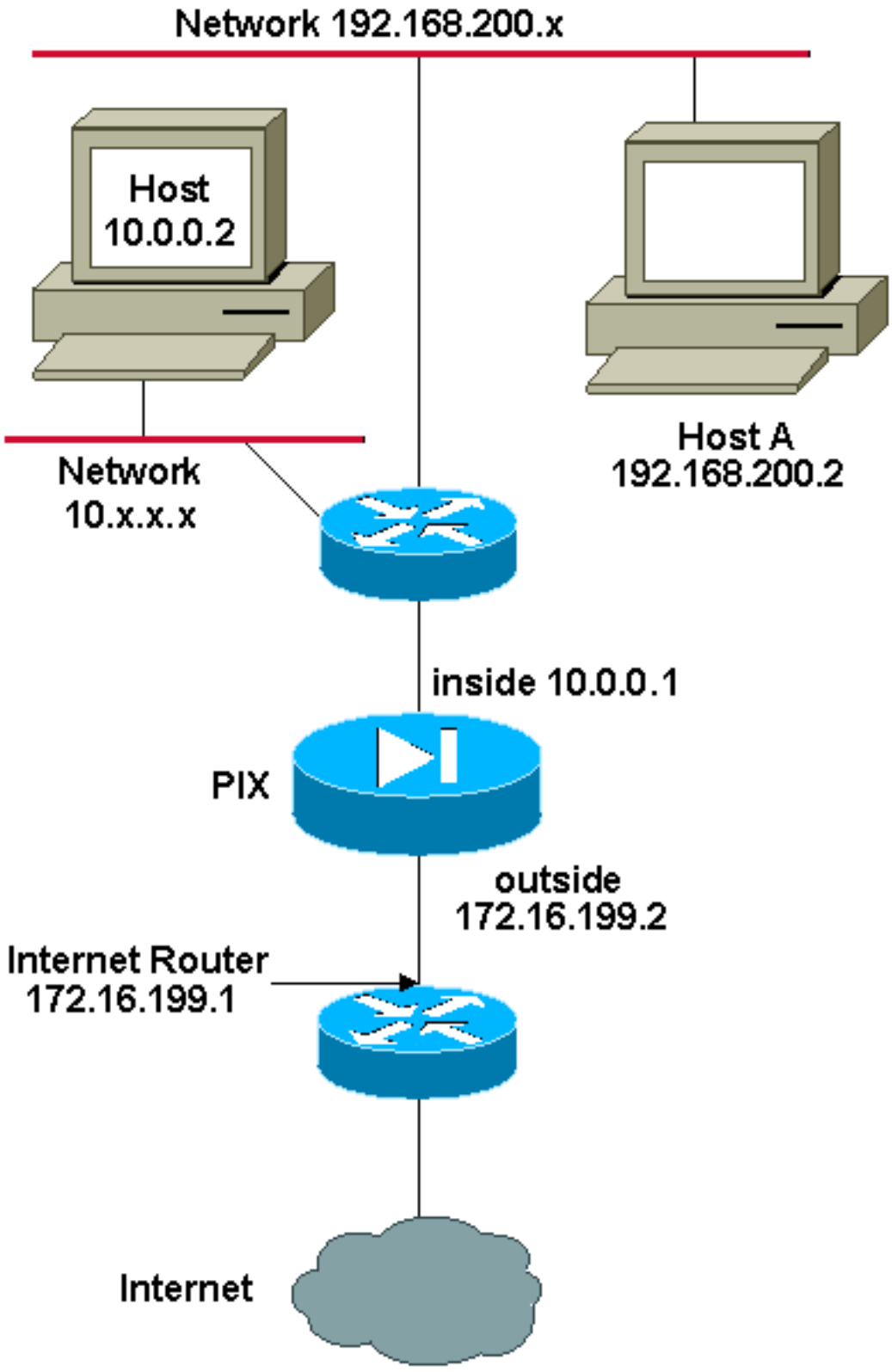
С отключенным **nat-control** PIX/ASA передает пакеты от интерфейса с более высоким уровнем безопасности до более низкого без определенного транслируемого значения в конфигурации. Для того, чтобы трафик проходил с менее защищенного интерфейса на

более защищенный, необходимо использовать списки доступа. PIX/ASA тогда передает трафик. Этот документ фокусируется на поведении устройства безопасности PIX/ASA с включенным **nat-control**.

Примечание: Если вы хотите удалить или отключить оператор nat-control в PIX/ASA, необходимо удалить все Выражения NAT из устройства безопасности. В целом необходимо удалить NAT, прежде чем вы выключите управление NAT. Необходимо реконфигурировать Выражение NAT в PIX/ASA для работы как ожидалось.

Несколько инструкций NAT с NAT 0

Схема сети



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

В данном примере интернет-провайдер предоставляет менеджеру сети диапазон адресов от 172.16.199.1 до 172.16.199.63. Менеджер сети решает назначить 172.16.199.1 на внутренний интерфейс на Интернет-маршрутизаторе и 172.16.199.2 к внешнему интерфейсу PIX/ASA.

Администратору сети уже назначили адрес Класса C на сеть, 192.168.200.0/24, и имеет

некоторые рабочие станции, которые используют эти адреса для доступа к Интернету. Эти рабочие станции не должны быть преобразованным адресом. Однако новым рабочим станциям назначают адреса в 10.0.0.0/8 сети, и они должны быть преобразованы.

Для размещения этой организации сети администратор сети должен использовать два Выражения NAT и один глобальный пул в конфигурации PIX/ASA как показано в выходных данных ниже:

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 192.168.200.0 255.255.255.0 0 0

nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

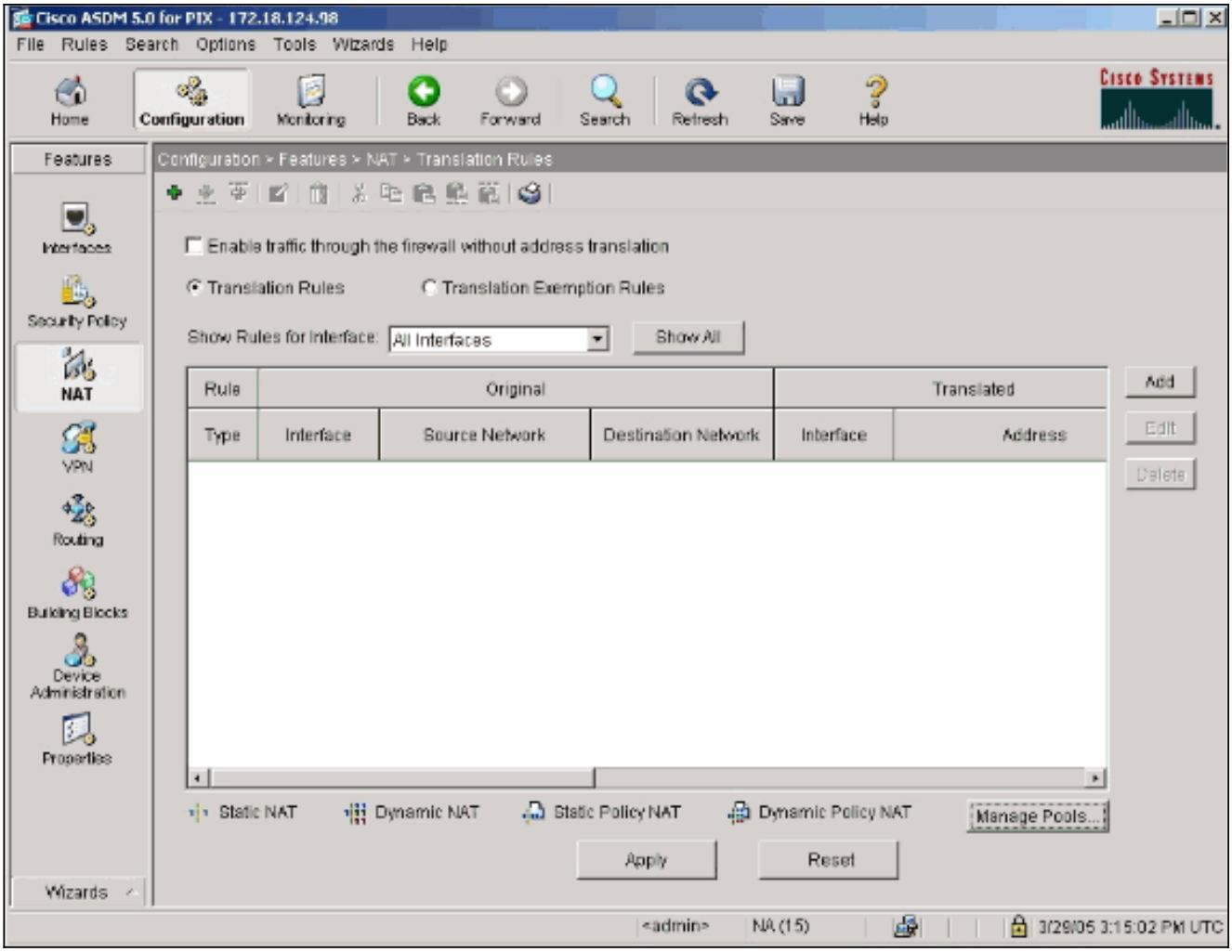
Эта конфигурация не преобразовывает адрес источника никакого исходящего трафика от 192.168.200.0/24 сети. Это преобразовывает адрес источника в 10.0.0.0/8 сети в адрес из диапазона 172.16.199.3 к 172.16.199.62.

Ниже приведено подробное разъяснение применения этой конфигурации с использованием Adaptive Security Device Manager (ASDM).

Примечание: Выполните все изменения конфигурации с использованием либо интерфейса командной строки, либо ASDM. Использование для изменения конфигурации и интерфейса командной строки, и ASDM может привести к неустойчивой работе с параметрами, измененными при помощи ASDM. Это не является ошибкой, но происходит вследствие особенностей работы ASDM.

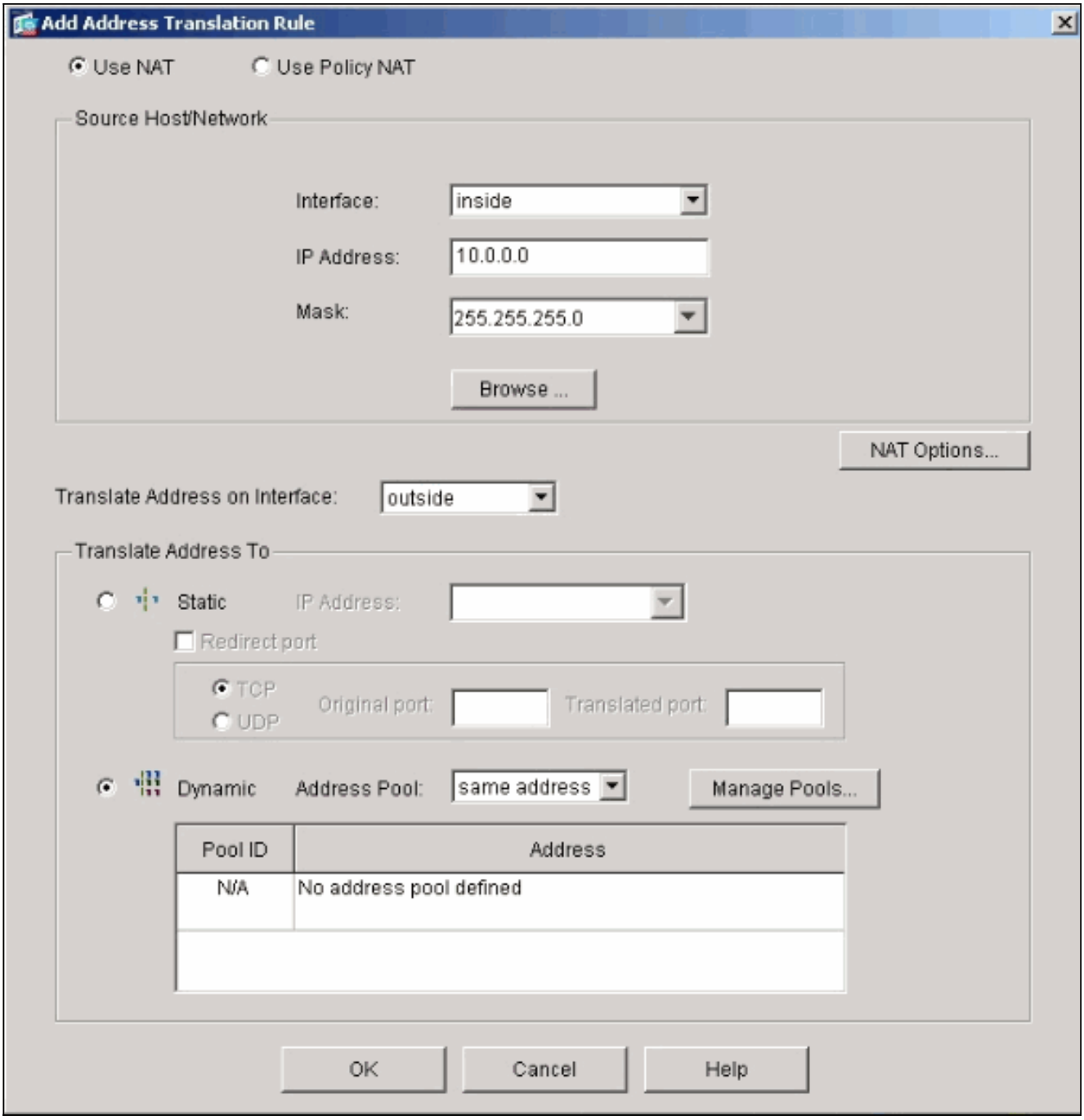
Примечание: Когда вы делаете и применяете изменения, при открытии ASDM он импортирует текущую конфигурацию из PIX/ASA и работает от той конфигурации. Если изменение внесено на PIX/ASA, в то время как сеанс ASDM открыт, то ASDM больше не работает с тем, что это "думает", текущая конфигурация PIX/ASA. Обязательно закройте любые сеансы ASDM, если вы изменяете конфигурацию через CLI. Откройте снова ASDM, когда вы захотите работать через GUI.

1. **Запустите ASDM, перейдите на вкладку Configuration и щелкните NAT.**
2. **Для создания нового правила щелкните Add.**

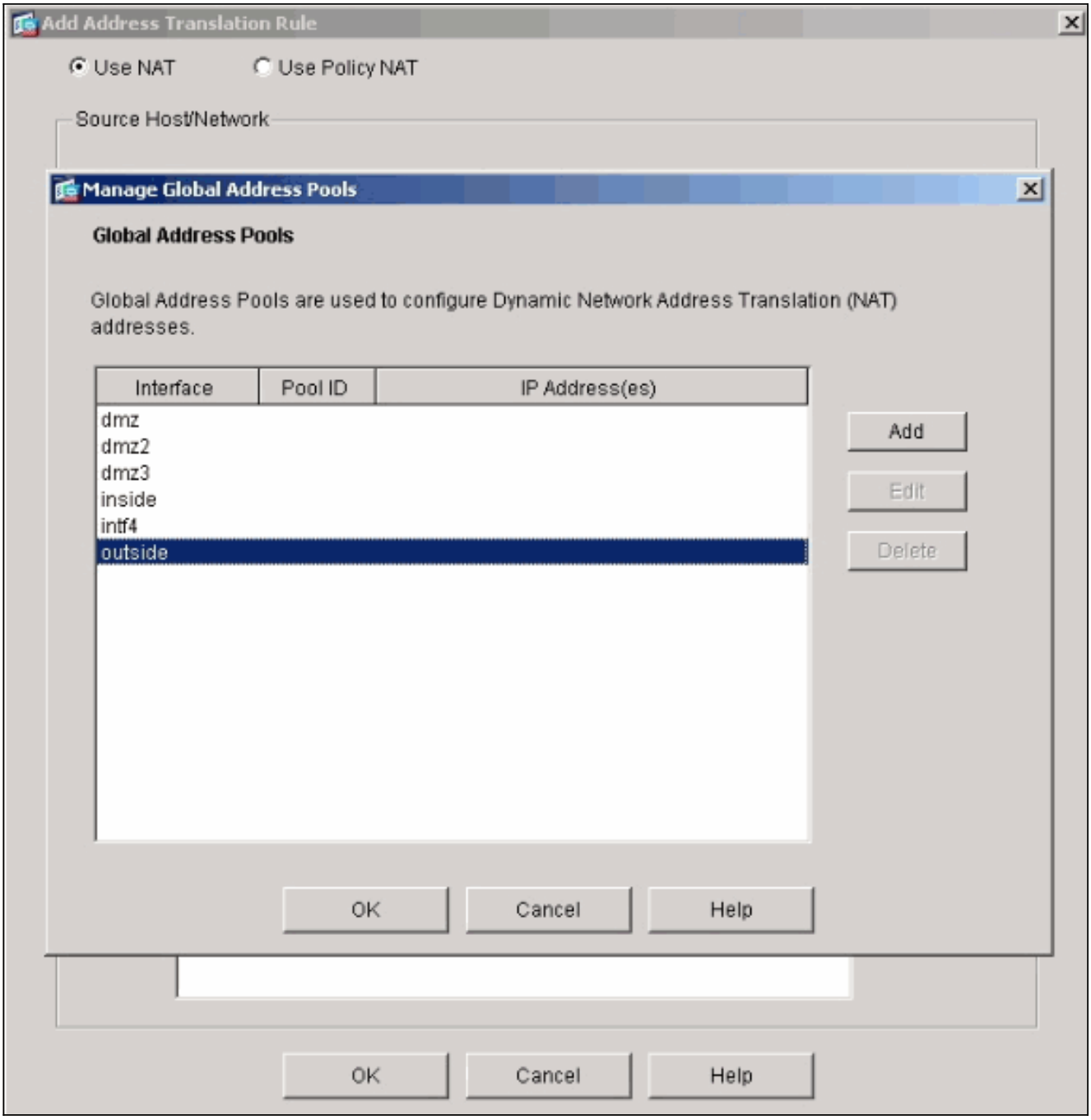


Новое окно появляется, который позволяет пользователю изменять параметры NAT для этой Записи NAT. В данном примере используйте NAT для пакетов, поступающих на внутренний интерфейс, источником которых является сеть 10.0.0.0/24.PIX/ASA преобразовывает эти пакеты в пул Динамического IP на внешнем интерфейсе. После ввода информации, описывающей трафик, подвергающийся NAT, следует определить пул IP-адресов для преобразуемого трафика.

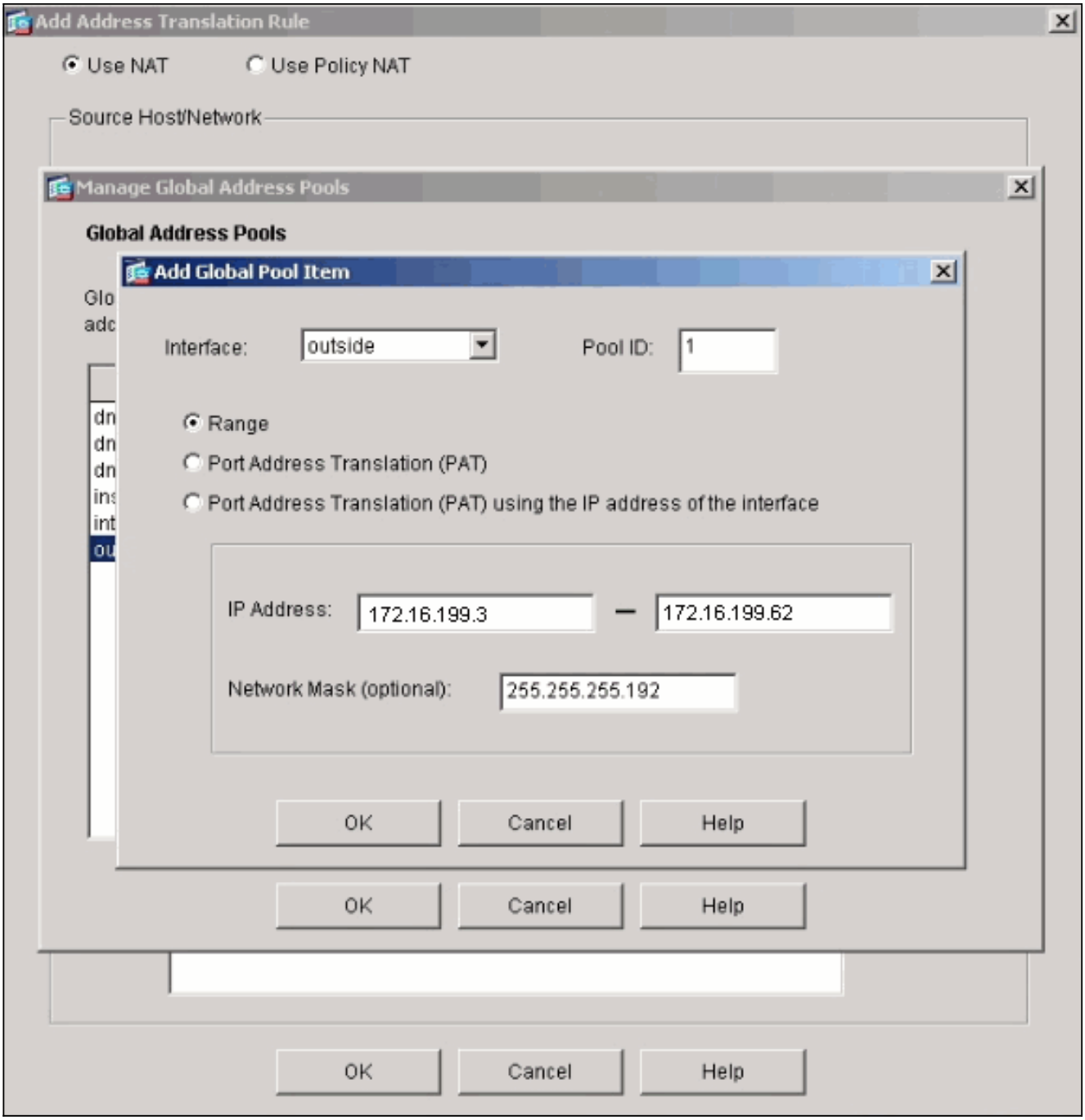
3. **Для добавления нового пула IP-адресов щелкните Manage Pools.**



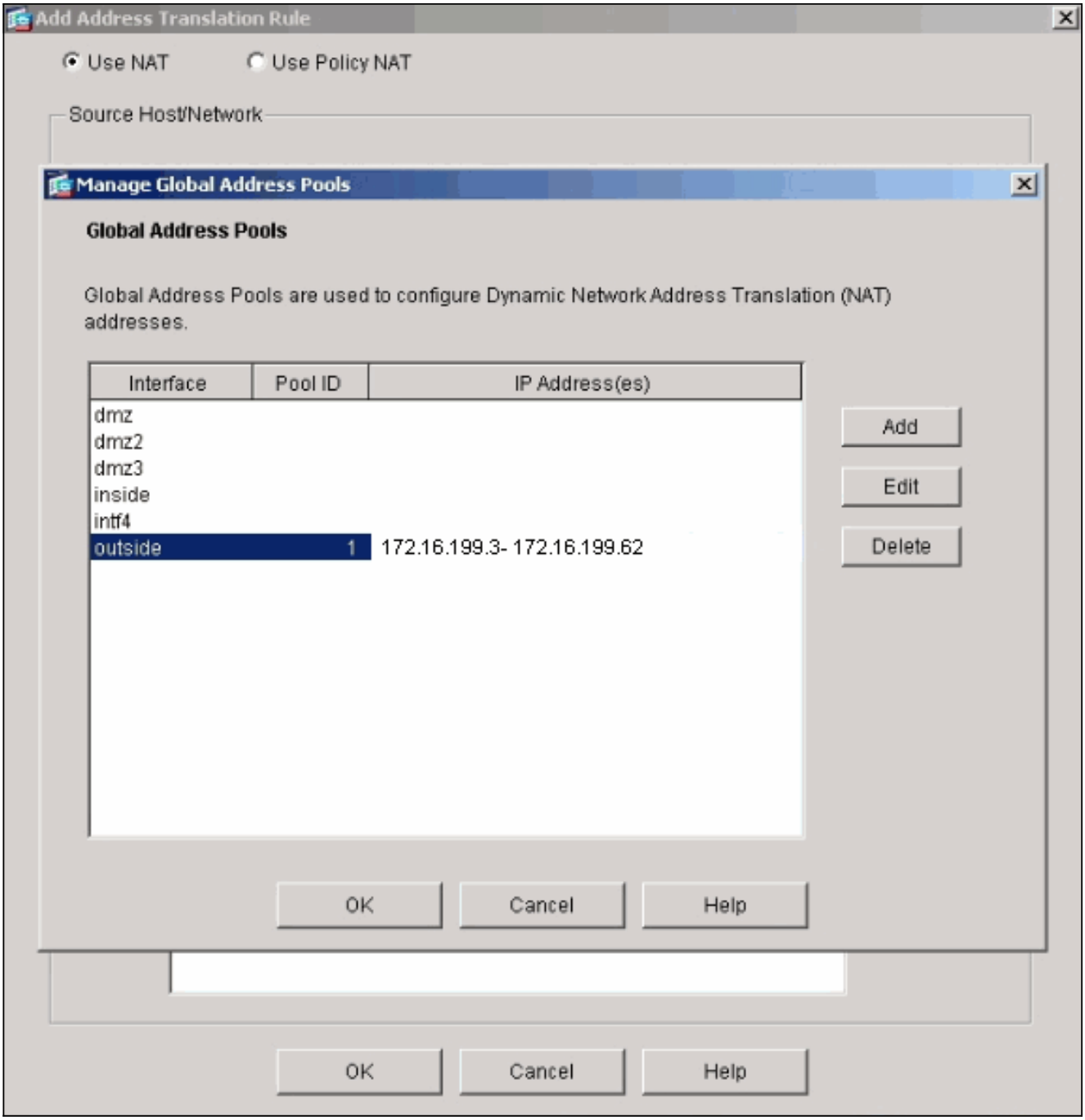
4. **Выберите outside и щелкните Add.**



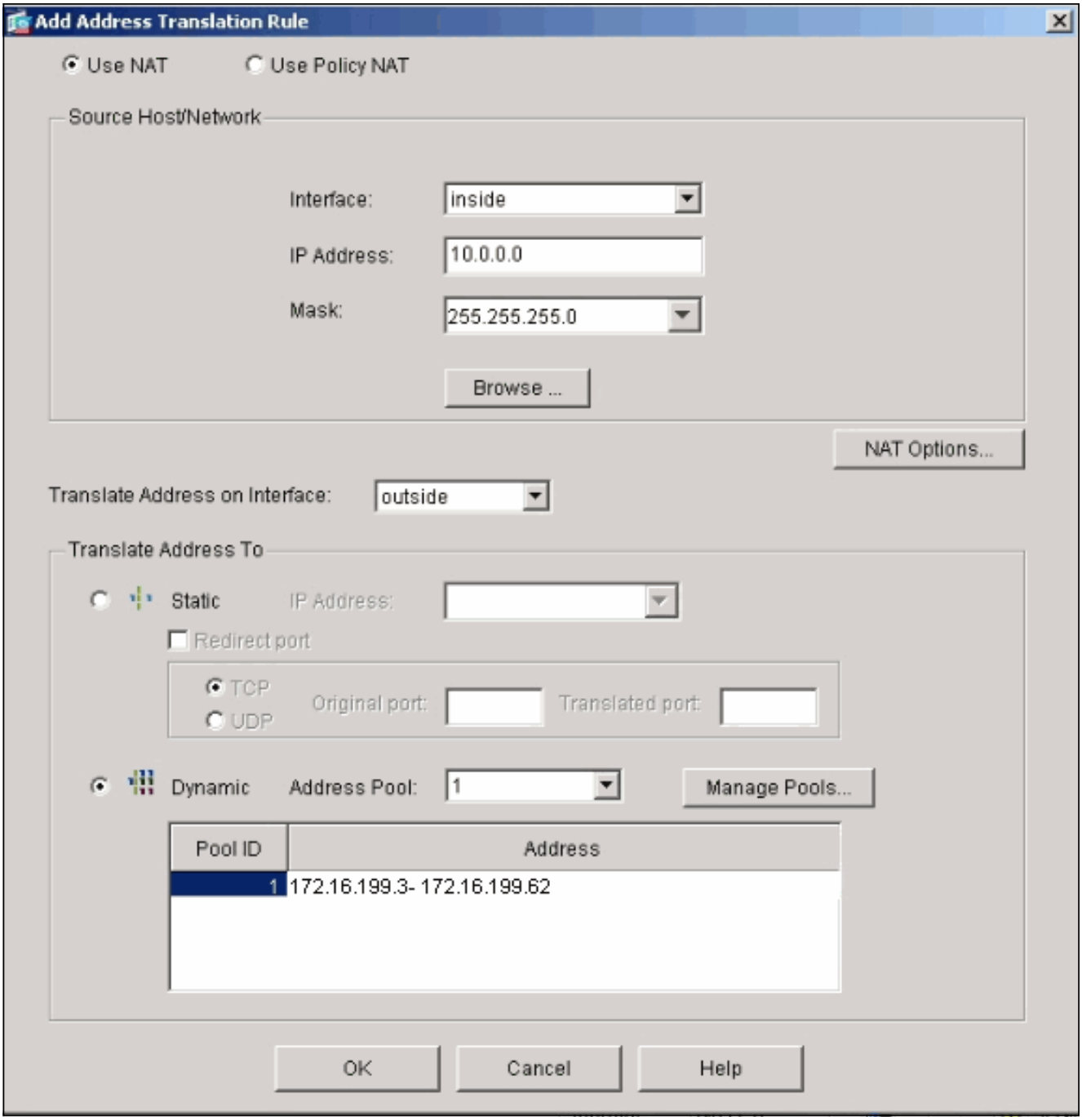
5. Укажите диапазон IP-адресов для пула и присвойте пулу уникальный целочисленный идентификатор.



6. Введите соответствующие значения и нажмите **OK**.Новый пул определен для внешнего интерфейса.

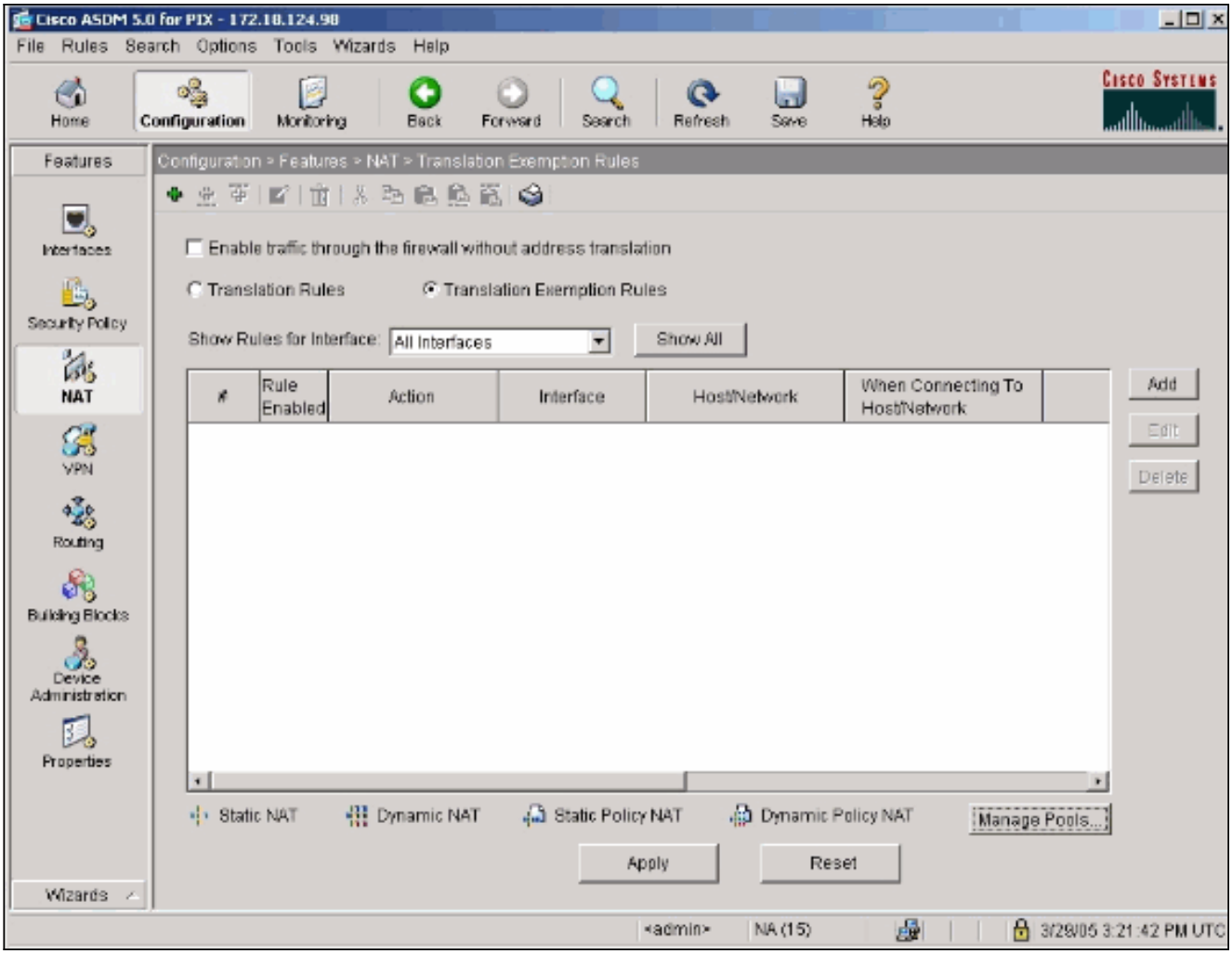


7. **После определения пула щелкните OK, чтобы вернуться к окну настройки правил NAT.**Удостоверьтесь, что выбрали корректный пул, который вы просто создали под выпадающим списком Пула
адресов.

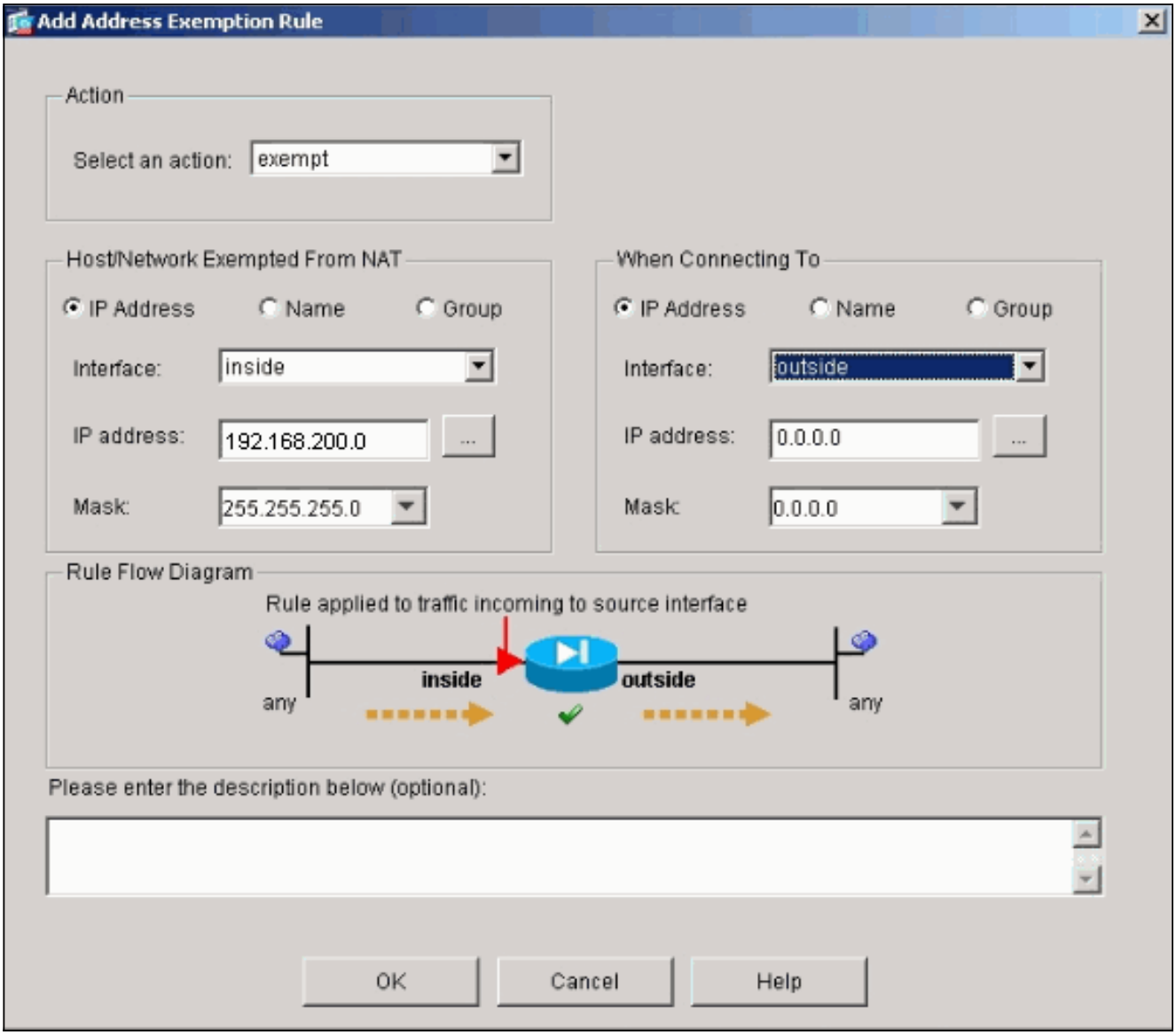


Вы теперь создали преобразование NAT через устройство безопасности. Однако необходимо создать запись NAT, которая определяет трафик, не подвергающийся NAT.

8. Нажмите **Translation Exemption Rules**, расположенный наверху окна, и затем **нажмите Add** для создания нового
правила.



9. Выберите *внутренний интерфейс* в качестве источника и задайте **192.168.200.0/24** подсеть. Оставьте установленные по умолчанию значения поля "When connecting".



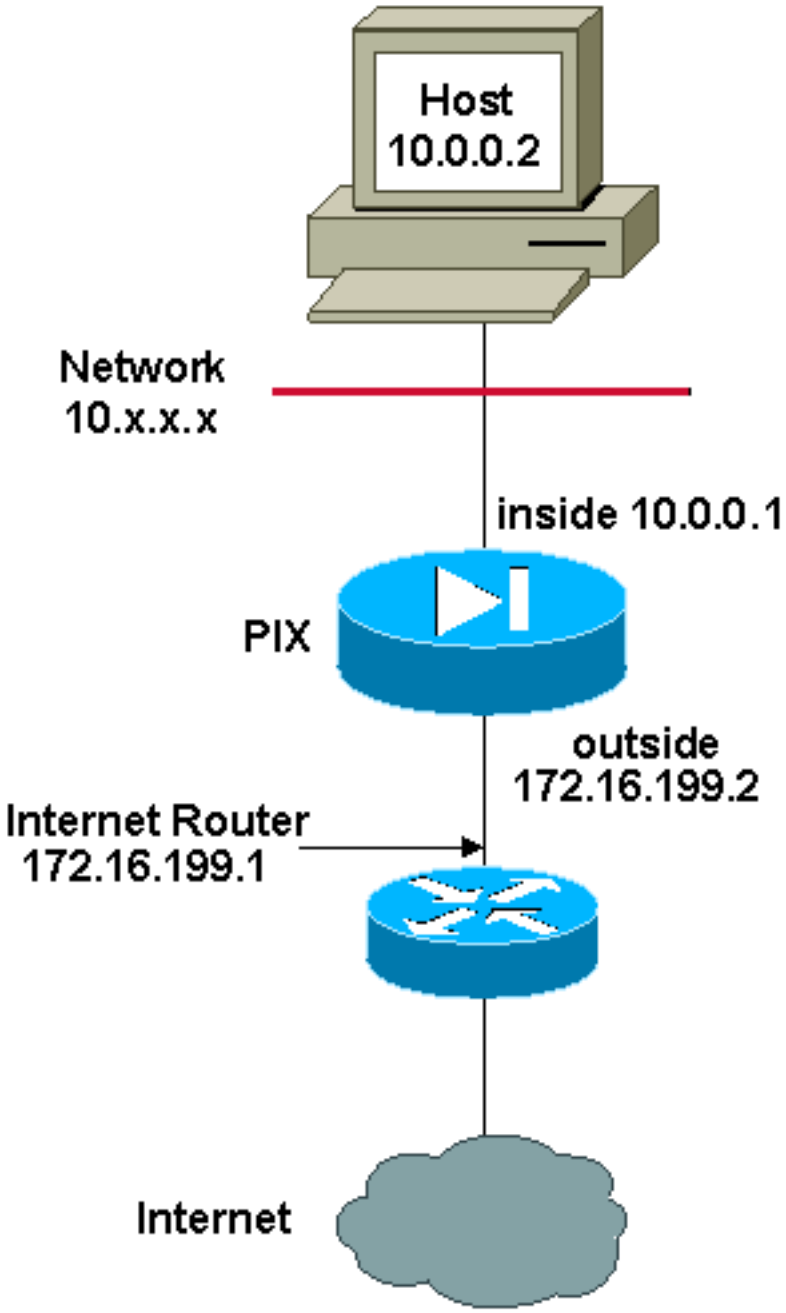
На данном этапе определены правила NAT.

10. Нажмите **Apply** для применения изменений к текущей рабочей конфигурации устройства безопасности.Эти выходные данные показывают реальные прибавления, которые применены к конфигурации PIX/ASA. Их вид немного отличается от результатов команд, введенных вручную, однако сами данные одинаковы.`access-list inside_nat0_outbound extended permit ip 192.168.200.0 255.255.255.0 any`

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 10.0.0.0 255.255.255.0
```

Несколько глобальных пулов

Схема сети



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

В этом примере диспетчер сети имеет два диапазона IP-адресов, зарегистрированных для Интернета. Диспетчер сети должен преобразовывать все внутренние адреса из диапазона 10.0.0.0/8 в зарегистрированные адреса. Диапазоны IP-адресов, которые должен использовать менеджер сети, 172.16.199.1 до 172.16.199.62 и 192.168.150.1 до 192.168.150.254. Диспетчер сети может сделать это следующим образом:

```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

global (outside) 1 192.168.150.1-192.168.150.254 netmask 255.255.255.0

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

В динамическом NAT более определенный оператор является тем, который имеет приоритет, когда вы используете тот же интерфейс на глобальном.

```
nat (inside) 1 10.0.0.0 255.0.0.0
```

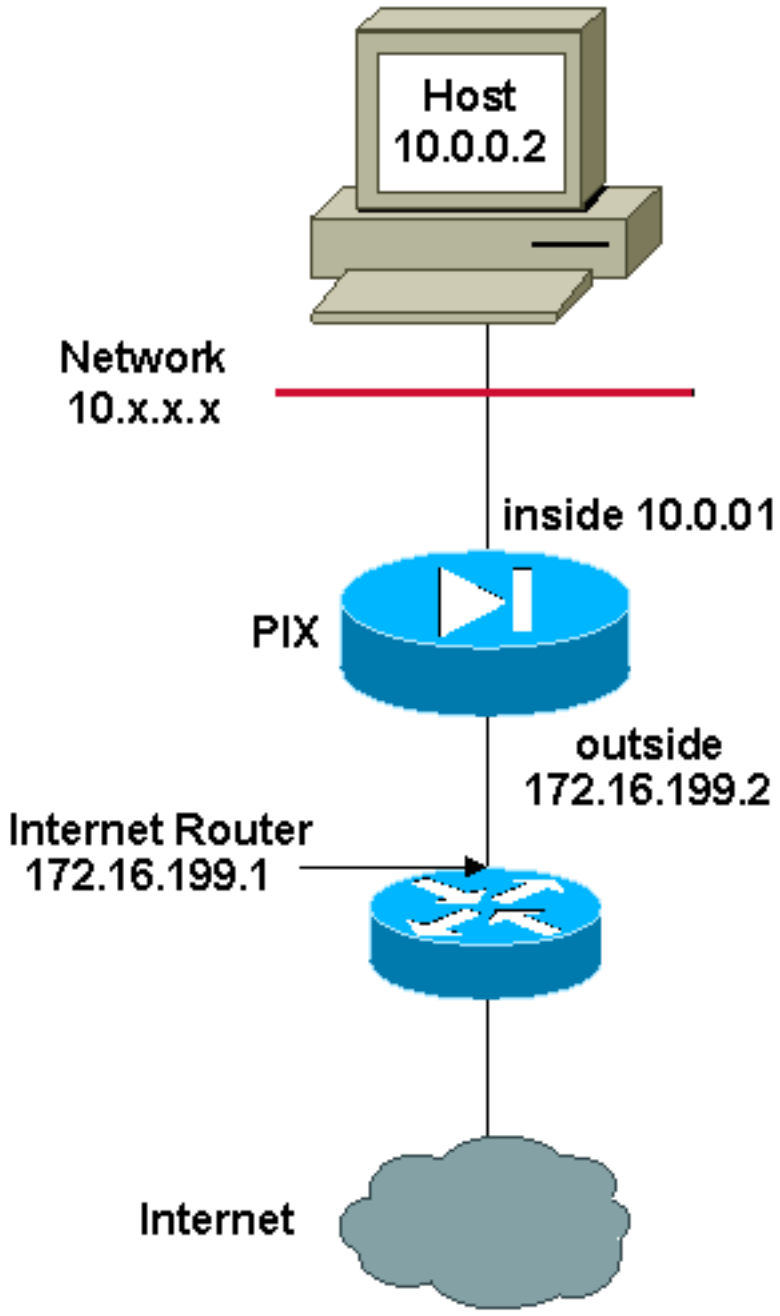
```
nat (inside) 2 10.1.0.0 255.255.0.0
global (outside) 1 172.16.1.1
global (outside) 2 192.168.1.1
```

Если у вас есть внутренняя сеть как 10.1.0.0, глобальный NAT 2 имеет приоритет более чем 1, поскольку это является более определенным для трансляции.

Примечание: Схема адресации с помощью подстановочных знаков используется в Выражении NAT. Этот оператор говорит PIX/ASA преобразовывать любой адрес внутреннего ресурса, когда это выходит в Интернет. При необходимости в этой команде можно указывать более конкретный адрес.

Смешанное использование глобальных инструкций NAT и PAT

Схема сети



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

В данном примере интернет-провайдер предоставляет менеджеру сети диапазон адресов от 172.16.199.1 до 172.16.199.63 для использования компании. Менеджер сети решает использовать 172.16.199.1 для внутреннего интерфейса на Интернет-маршрутизаторе и 172.16.199.2 для внешнего интерфейса на PIX/ASA. Вас оставляют с 172.16.199.3 до 172.16.199.62 использовать для пула NAT. Однако менеджер сети знает, что в любой момент может быть больше чем шестьдесят человек, которые пытаются выйти из PIX/ASA. Поэтому менеджер сети решает взять 172.16.199.62 и сделать его Адресом PAT так, чтобы несколько пользователей могли совместно использовать один адрес в то же время.

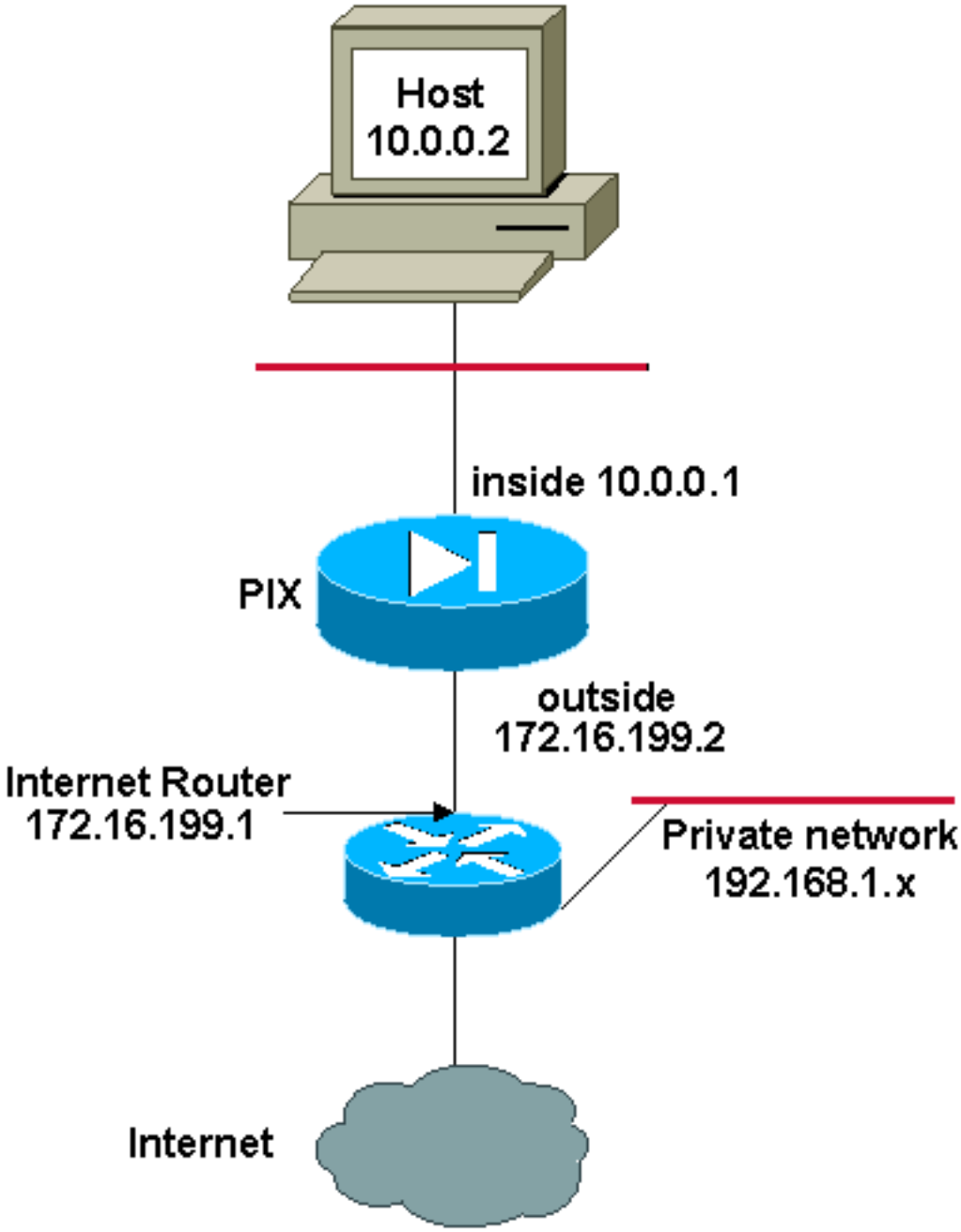
```
global (outside) 1 172.16.199.3-172.16.199.61 netmask 255.255.255.192

global (outside) 1 172.16.199.62 netmask 255.255.255.192

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

Эти команды дают PIX/ASA команду преобразовывать адрес источника в 172.16.199.3 до 172.16.199.61 для первых пятидесяти девяти внутренних пользователей, которые пройдут через PIX/ASA. После того, как эти адреса исчерпаны, PIX тогда преобразовывает все последующие адреса источника в 172.16.199.62, пока один из адресов в пуле NAT не становится свободным.

Примечание: Схема адресации с помощью подстановочных знаков используется в Выражении NAT. Этот оператор говорит PIX/ASA преобразовывать любой адрес внутреннего ресурса, когда это выходит в Интернет. При необходимости в этой команде можно указывать более конкретный адрес.

Несколько инструкций NAT со списком доступа NAT 0

Схема сети



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

В данном примере интернет-провайдер предоставляет менеджеру сети диапазон адресов от 172.16.199.1 до 172.16.199.63. Менеджер сети решает назначить 172.16.199.1 на внутренний интерфейс на Интернет-маршрутизаторе и 172.16.199.2 к внешнему интерфейсу PIX/ASA.

Однако в этом случае другой сегмент частной локальной сети размещен за Интернет-маршрутизатором. Диспетчер сети предпочитает не использовать адреса из глобального пула, если узлы в этих двух сетях обмениваются данными между собой. Диспетчеру сети по-прежнему необходимо преобразовывать адреса источников для всех внутренних пользователей (10.0.0.0/8) при их подключении к Интернету.

```
access-list 101 permit ip 10.0.0.0 255.0.0.0 192.168.1.0 255.255.255.0
```

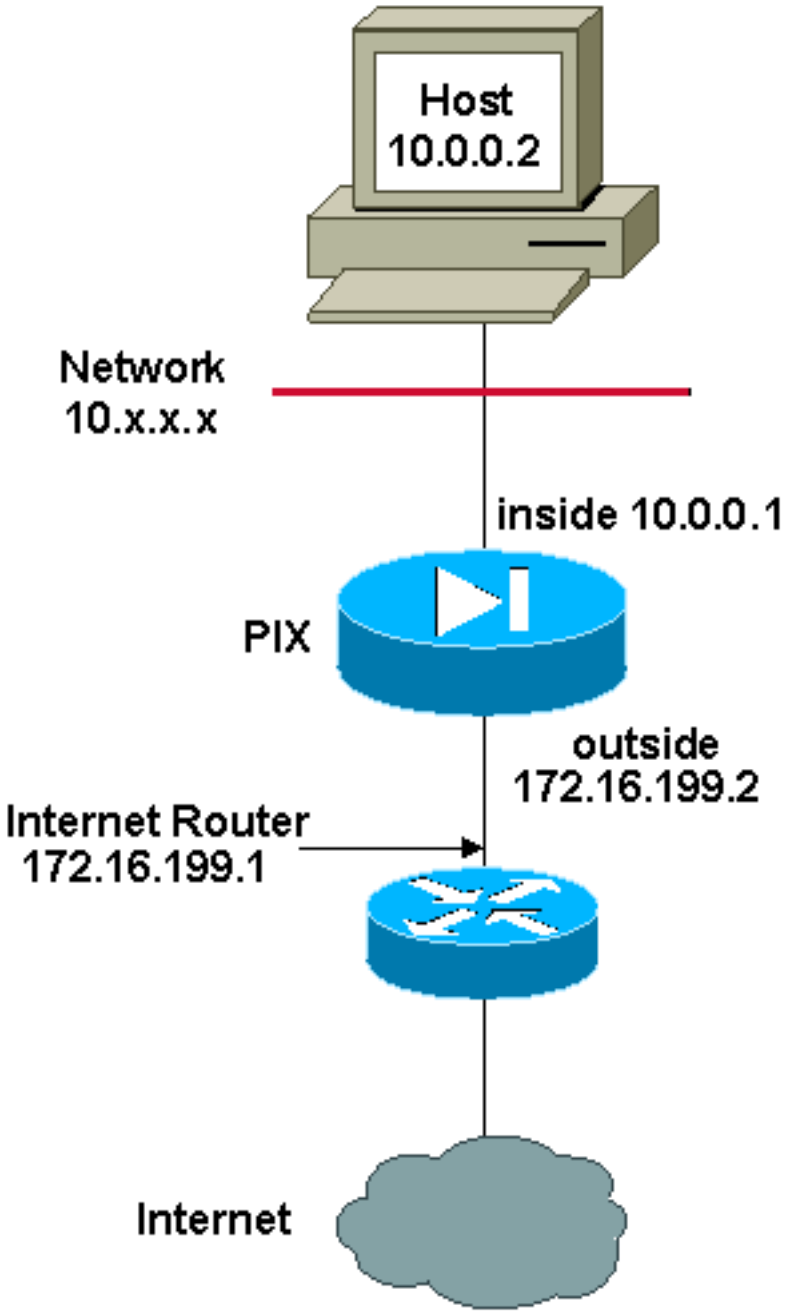
```
global (outside) 1 172.16.199.3-172.16.199.62 netmask 255.255.255.192

nat (inside) 0 access-list 101

nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

Эта конфигурация не преобразует адреса, где адрес источника 10.0.0.0/8, а адрес назначения 192.168.1.0/24. Это преобразовывает адрес источника от любого трафика, инициировал из 10.0.0.0/8 сети и предназначил для где угодно кроме 192.168.1.0/24 в адрес из диапазона 172.16.199.3 до 172.16.199.62.

При наличии результата выполнения команды write terminal для устройства Cisco можно использовать средство интерпретации выходных данных (только для зарегистрированных пользователей).

Использование политики NAT

Схема сети



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

При использовании списка доступа с командой nat для любого идентификатора NAT, отличного от 0, включается политика NAT.

Примечание: Политика NAT была представлена в версии 6.3.2.

Политика NAT позволяет распознавать локальный трафик, предназначенный для преобразования адресов при указании адресов (или портов) источника и места назначения в списке доступа. В обычном режиме NAT использует только исходные адреса/порты, тогда как политика NAT использует адреса/порты как источника, так и места назначения.

Примечание: Политику NAT поддерживают все типы NAT кроме исключений NAT (nat 0 access-list). Исключение NAT использует список контроля доступа, чтобы идентифицировать локальные адреса, но отличается от policy NAT тем, что не использует порты.

Используя policy NAT можно создавать несколько NAT или статических инструкций, которые идентифицируют один и тот же локальный адрес, пока комбинация источник/порт и назначение/порт остается уникальной для каждой инструкции. Затем можно сопоставить разные глобальные адреса каждой паре источник/порт и назначение/порт.

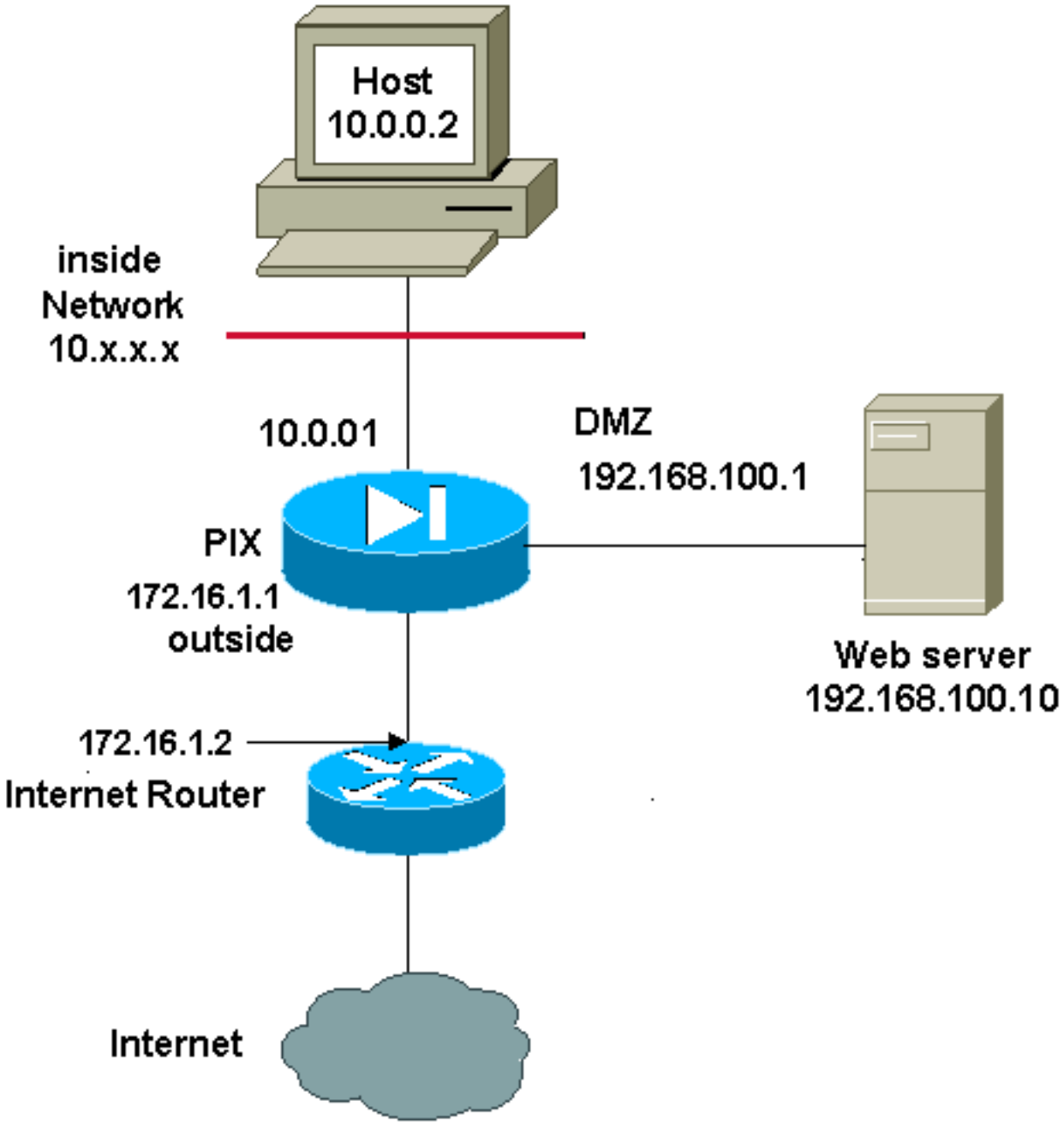
В данном примере менеджер сети предоставляет доступ для IP - адреса назначения 192.168.201.11 для порта 80 (сеть) и порт 23 (Telnet), но должен использовать два других IP-адреса в качестве адреса источника. IP-адрес 172.16.199.3 используется в качестве адреса источника для сети. IP-адрес 172.16.199.4 используется для Telnet и должен преобразовать все внутренние адреса, которые находятся в диапазоне 10.0.0.0/8. Диспетчер сети может сделать это следующим образом:

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
255.255.255.255 eq 80

access-list TELNET permit tcp 10.0.0.0 255.0.0.0 192.168.201.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB

nat (inside) 2 access-list TELNET

global (outside) 1 172.16.199.3 netmask 255.255.255.192

global (outside) 2 172.16.199.4 netmask 255.255.255.192
```

Вы можете использовать средство интерпретации выходных данных (только для зарегистрированных пользователей) для выявления проблем и поиска их решений.

Статический NAT

Схема сети



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

Конфигурация статического NAT создает сопоставление "один к одному" и преобразует определенный адрес в другой адрес. Данный тип конфигурации создает в таблице NAT постоянную запись, существующую до тех пор, пока существует конфигурация, и разрешает инициировать соединения как внутренним, так и внешним хостам. Обычно это используется для хостов, на которых запущены службы, например, электронная почта, веб-сервер, FTP и другие. В данном примере статические инструкции NAT настроены так, чтобы позволять внутренним и внешним пользователям получать доступ к веб-серверу в демилитаризованной зоне.

Приведенные выходные данные демонстрируют построение статической инструкции. Следует помнить о порядке сопоставленных и реальных IP-адресов.

```
static (real_interface,mapped_interface) mapped_ip real_ip netmask mask
```

Ниже приведен пример статического преобразования, созданного для того, чтобы пользователи с внутреннего интерфейса могли получить доступ к серверу в демилитаризованной зоне. Здесь создается сопоставление между внутренним адресом и адресом сервера в демилитаризованной зоне. При этом внутренние пользователи могут получать доступ к серверу в демилитаризованной зоне с использованием внутреннего адреса.

```
static (DMZ,inside) 10.0.0.10 192.168.100.10 netmask 255.255.255.255
```

Ниже приведен пример статического преобразования, созданного для того, чтобы пользователи с внешнего интерфейса могли получить доступ к серверу в демилитаризованной зоне. Здесь создается сопоставление между внешним адресом и адресом сервера в демилитаризованной зоне. При этом внешние пользователи могут получать доступ к серверу в демилитаризованной зоне с использованием внешнего адреса.

```
static (DMZ,outside) 172.16.1.5 192.168.100.10 netmask 255.255.255.255
```

Примечание: Поскольку уровень защиты внешнего интерфейса ниже уровня защиты демилитаризованной зоны, необходимо также создать список доступа, позволяющий внешним пользователям подключаться к серверу в демилитаризованной зоне. **Список доступа должен предоставлять пользователям доступ к сопоставленному адресу в статическом преобразовании.** Рекомендуется делать этот список доступа как можно более конкретным. В данном случае любой хост может получить доступ только к портам 80 (www/http) и 443 (https) веб-сервера.

```
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq www
access-list OUTSIDE extended permit tcp any host 172.16.1.5 eq https
```

Список доступа также необходимо применить к внешнему интерфейсу.

```
access-group OUTSIDE in interface outside
```

Дополнительные сведения по командам access-list и access-group см. в документах access-list extended и access-group.

Как обойти NAT

В этом разделе описывается обойти NAT. Вы могли бы хотеть обойти NAT при включении управления NAT. Можно использовать Идентичность NAT, Статическая Идентичность NAT или освобождение NAT для обхода NAT.

Настройте идентичность NAT

Идентичность NAT преобразовывает реальный IP - адрес в тот же IP-адрес. Только "преобразованные" хосты могут создать преобразования NAT, и ответный трафик позволен назад.

Примечание: Если вы изменяете конфигурацию NAT, и вы не хотите ждать существующих преобразований для таймаута, прежде чем новые данные NAT будут использоваться, вы используете **команду clear xlate** для очистки таблицы преобразования. Однако все текущие соединения, которые используют трансляции, разъединены при очистке таблицы преобразования.

Для настройки идентичности NAT введите эту команду:

```
hostname(config)#nat (real_interface) 0 real_ip [mask [dns] [outside] [norandomseq] [[tcp]
```

tcp_max_conns [emb_limit]] [udp udp_max_conns]
Например, для использования идентичности NAT для внутренней части 10.1.1.0/24 сеть, введите эту команду:

```
hostname(config)#nat (inside) 0 10.1.1.0 255.255.255.0
```
См. Справочник по командам Cisco Security Appliance, Версию 7.2 для получения дополнительной информации о **туземной** команде.

Настройте статическую идентичность NAT

Статическая идентичность NAT преобразовывает реальный IP - адрес в тот же IP-адрес. Трансляция всегда активна, и оба "преобразованные" и удаленные хосты могут инициировать соединения. Статическая идентичность NAT позволяет вам использовать обычный NAT или политику NAT. NAT политики позволяет вам определить real и адреса назначения (DA) при определении действительных адресов для перевода (см. Политику Использования раздел NAT для получения дополнительной информации о политике NAT). Например, можно использовать политику статическая идентичность NAT для внутреннего адреса, когда это обращается к внешнему интерфейсу, и назначение является сервером A, но используйте обычную трансляцию при доступе к внешнему серверу B.

Примечание: При удалении статической команды на текущие соединения, которые используют трансляцию, не влияют. Для удаления этих соединений введите **команду clear local-host**. Вы не можете очистить статические преобразования от таблицы преобразования с **командой clear xlate**; необходимо удалить статическую команду вместо этого. Только динамические преобразования, созданные nat и командами global, могут быть удалены с командой clear xlate.

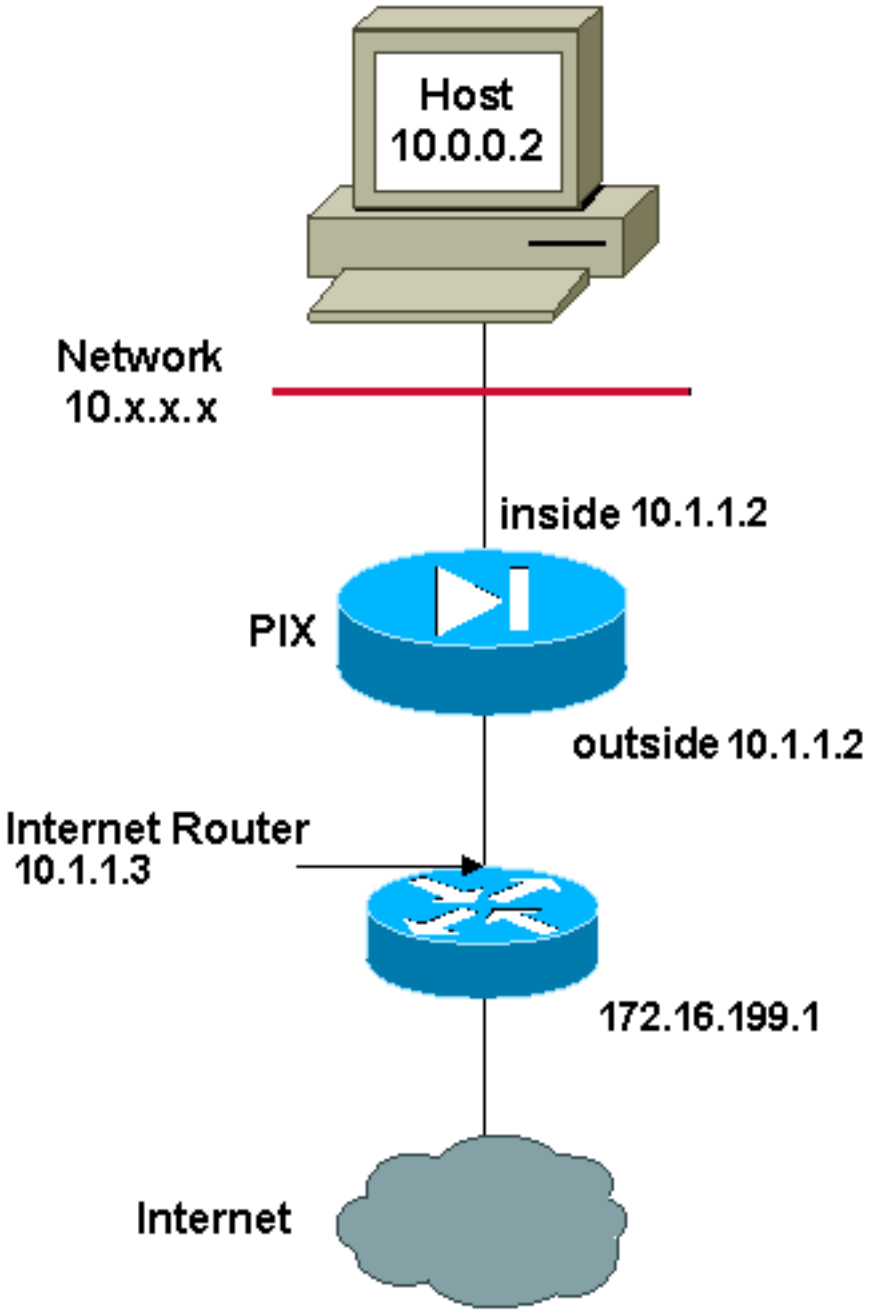
Для настройки политики статическая идентичность NAT введите эту команду:

```
hostname(config)#static (real_interface,mapped_interface) real_ip access-list acl_id [dns]
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```
Используйте **команду access-list extended** для создания расширенного списка доступа. Этот список доступа должен включать только ACE разрешения. Удостоверьтесь, что адрес источника в списке доступа совпадает с real_ip в этой команде. Политика NAT не рассматривает неактивных ключевых слов или ключевых слов time-range; все ACE, как полагают, активны для конфигурации NAT политики. Посмотрите Политику Использования раздел NAT для получения дополнительной информации.

Для настройки обычной статической идентичности NAT введите эту команду:

```
hostname(config)#static (real_interface,mapped_interface) real_ip real_ip [netmask mask] [dns]
[norandomseq] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns]
```
Задайте тот же IP-адрес для обоих real_ip аргументы.

Схема сети



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

Например, эта команда использует статическую идентичность NAT для внутреннего IP-адреса (10.1.1.2), когда обращено внешней стороной:

```
hostname(config)#static (inside,outside) 10.1.1.2 10.1.1.2 netmask 255.255.255.255
```

См. Справочник по командам Cisco Security Appliance, Версию 7.2 для получения дополнительной информации о **статической** команде.

Эта команда использует статическую идентичность NAT для внешнего адреса (172.16.199.1), когда обращено внутренней частью:

```
hostname(config)#static (outside,inside) 172.16.199.1 172.16.199.1 netmask 255.255.255.255
```

Эта команда статически сопоставляет подсеть в целом:

```
hostname(config)#static (inside,dmz) 10.1.1.2 10.1.1.2 netmask 255.255.255.0
```

Этот статический пример преобразования NAT политики идентификации показывает одиночный действительный адрес что идентичность использования NAT при доступе к одному адресу назначения (DA) и трансляции при доступе к другому:

```
hostname(config)#access-list NET1 permit ip host 10.1.1.3 172.16.199.0 255.255.255.224
hostname(config)#access-list NET2 permit ip host 10.1.1.3 172.16.199.224 255.255.255.224
hostname(config)#static (inside,outside) 10.1.1.3 access-list NET1 hostname(config)#static
(inside,outside) 172.16.199.1 access-list NET2
```

Примечание: Для получения дополнительной информации о **статической** команде, обратитесь Справочник по командам многофункционального устройства защиты Cisco ASA серии 5580, Версию 8.1.

Примечание: Для получения дополнительной информации о access-lists, обратитесь Руководство по конфигурации Командной строки многофункционального устройства защиты Cisco ASA серии 5580, Версию 8.1.

Освобождение NAT Настройки

Освобождение NAT освобождает адреса от трансляции и позволяет и real и удаленным хостам инициировать соединения. Освобождение NAT позволяет вам задать real и адреса назначения (DA) при определении реального трафика для освобождения (подобный политике NAT), таким образом, вы имеете больший контроль с помощью освобождения NAT, чем идентичность NAT. Однако, в отличие от политики NAT, освобождение NAT не рассматривает порты в списке доступа. Используйте статическую идентичность NAT для рассмотрения портов в списке доступа.

Примечание: При удалении конфигурации освобождения NAT на существующие соединения, которые используют освобождение NAT, не влияют. Для удаления этих соединений введите команду clear local-host.

Для настройки освобождения NAT введите эту команду:

```
hostname(config)#nat (real_interface) 0 access-list acl_name [outside]
```

Создайте расширенный список доступа с помощью **команды access-list extended**. Этот список доступа может включать и ACE разрешения и запретить ACE. Не задавайте real и порты назначения в списке доступа; освобождение NAT не рассматривает порты. Освобождение NAT также не рассматривает неактивных ключевых слов или ключевых слов time-range; все ACE, как полагают, активны для конфигурации освобождения NAT.

По умолчанию эта команда освобождает трафик изнутри к внешней стороне. Если вы хотите, чтобы трафик снаружи к внутренней части обошел NAT, то добавьте дополнительную **туземную** команду и войдите снаружи для определения экземпляра NAT как вне NAT. Если вы настраиваете динамический NAT для внешнего интерфейса и хотите освободить другой трафик, вы могли бы хотеть использовать внешнее освобождение NAT.

Например, для освобождения внутренней сети при доступе к любому адресу назначения (DA), введите эту команду:

```
 hostname(config)#access-list EXEMPT permit ip 10.1.1.0 255.255.255.0 any hostname(config)#nat
(inside) 0 access-list EXEMPT
```

Чтобы использовать динамичный вне NAT для сети DMZ и освободить другую сеть DMZ, введите эту команду:

```
 hostname(config)#nat (dmz) 1 10.1.1.0 255.255.255.0 outside dns hostname(config)#global
(inside) 1 10.1.1.2 hostname(config)#access-list EXEMPT permit ip 10.1.1.0 255.255.255.0 any
hostname(config)#nat (dmz) 0 access-list EXEMPT
```

Для освобождения внутреннего адреса при доступе к двум другим адресам назначения (DA) введите это команды:

```
hostname(config)#access-list NET1 permit ip 10.1.1.0 255.255.255.0 172.16.199.0 255.255.255.224
hostname(config)#access-list NET1 permit ip 10.1.1.0 255.255.255.0 172.16.199.224
255.255.255.224 hostname(config)#nat (inside) 0 access-list NET1
```

Проверка

Трафик, который течет через устройство безопасности, скорее всего, подвергается NAT. См. PIX/ASA: Монитор и Проблемы производительности Устранения неполадок для проверки трансляций, которые используются на устройстве безопасности.

Команда show xlate count отображает ток и максимальное число трансляций через PIX. Трансляция является сопоставлением внутреннего адреса к внешнему адресу и может быть однозначным сопоставлением, таким как NAT или сопоставление многие к одному, такое как PAT. Эта команда является поднабором команды show xlate, которая выводит каждую трансляцию через межсетевой экран PIX. В выходных данных команды отображаются «используемые» трансляции, к которым относятся активные трансляции в PIX при выполнении команды, и «наиболее используемые» — максимальное число трансляций, которое наблюдалось в PIX с момента включения.

Устранение неполадок

Сообщение об ошибках, полученное при добавлении Статического PAT для порта 443

Проблема

Когда вы добавляете статическое PAT для порта 443, вы получаете это сообщение об ошибках:

```
[ERROR] static (INSIDE,OUTSIDE) tcp interface 443 192.168.1.87 443 netmask 255.255.255.255 tcp 0
0 udp 0

unable to reserve port 443 for static PAT

:
```

Решение

Когда или ASDM или WEBVPN работают на 443 портах, это сообщение об ошибках происходит. Для решения этого вопроса войдите к межсетевому экрану и выполните один из этих шагов:

- Для изменения порта ASDM на что-либо кроме 443, выполните эти команды:`ASA(config)#no http server enable ASA(config)#http server enable 8080`
- Для изменения порта WEBVPN на что-либо кроме 443, выполните эти команды:`ASA(config)#webvpn ASA(config-webvpn)#enable outside ASA(config-webvpn)#port 65010`

После того, как вы выполняете эти команды, должна существовать возможность для добавления NAT/PAT на порту 443 к другому серверу. Когда вы попытаетесь использовать ASDM для управления ASA в будущем, задайте новый порт как 8080.

Ошибка: сопоставленный адресный конфликт с существующими помехами

Проблема

Когда вы добавляете статическое состояние на ASA, вы получаете эту ошибку:

:

Решение

Проверьте, что запись уже не существует для статического источника, который вы хотите добавить.

Дополнительные сведения

- Страница поддержки PIX
- Справочник по командам PIX
- Страница технической поддержки ASA
- Справочники по командам ASA
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация