Устранение проблем конфигурации трансляции сетевых адресов ASA

Содержание

Введение
Конфигурация NAT устранения неполадок на ASA
Как Конфигурация ASA Используется для Построения Таблицы политики NAT
Как устранить неполадки проблем NAT
Используйте утилиту Packet Tracer
Просмотрите выходные данные команды Show Nat
Методика устранения проблем проблемы NAT
Типичные проблемы с конфигурациями NAT
Проблема: Трафик отказывает из-за Ошибки Сбоя обратного пути (RPF) NAT: Асимметричные правила NAT совпали для форварда и обратных потоков
Проблема: Ручные Правила NAT неисправны, который вызывает соответствия неверного пакета
Проблема: Правило NAT слишком широко и совпадает с некоторым трафиком непреднамеренно
Проблема: Правило NAT отклоняет трафик к неверному интерфейсу
Проблема: Правило NAT вызывает ASA к Протоколу разрешения proxy - адресации (ARP) для трафика на сопоставленном интерфейсе
Дополнительные сведения

Введение

Этот документ описывает, как устранить неполадки конфигурации Технологии NAT на устройстве адаптивной защиты Cisco (ASA) платформа. Этот документ допустим для Версии ASA 8.3 и позже.

> **Примечание:** Для некоторых базовых примеров конфигураций NAT, которые включают видео, которое показывает основную конфигурацию NAT, посмотрите Дополнительные сведения раздела у основания этого документа.

Конфигурация NAT устранения неполадок на ASA

При устранении проблем конфигураций NAT важно понять, как конфигурация NAT на ASA используется для построения Таблицы политики NAT.

Эти ошибки конфигурации составляют большинство проблем NAT, с которыми встречаются

администраторы ASA:

- Правила конфигурации NAT не работают. Например, ручное правило NAT размещено наверху таблицы NAT, которая заставляет более определенные правила, размещенные дальше вниз таблица NAT никогда не поражаться.
- Сетевые объекты, используемые в конфигурации NAT, слишком широки, который заставляет трафик непреднамеренно совпадать с этими правилами NAT и пропускать более определенные правила NAT.

Утилита Packet Tracer может использоваться для диагностирования большинства связанных с NAT проблем на ASA. Посмотрите следующий раздел для получения дополнительной информации о том, как конфигурация NAT используется для построения Таблицы политики NAT, и как устранить неполадки и решить определенные проблемы NAT.

Кроме того, **подробная** команда **nat показа** может использоваться для понимания, какие правила NAT поражены новыми соединениями.

Как Конфигурация ASA Используется для Построения Таблицы политики NAT

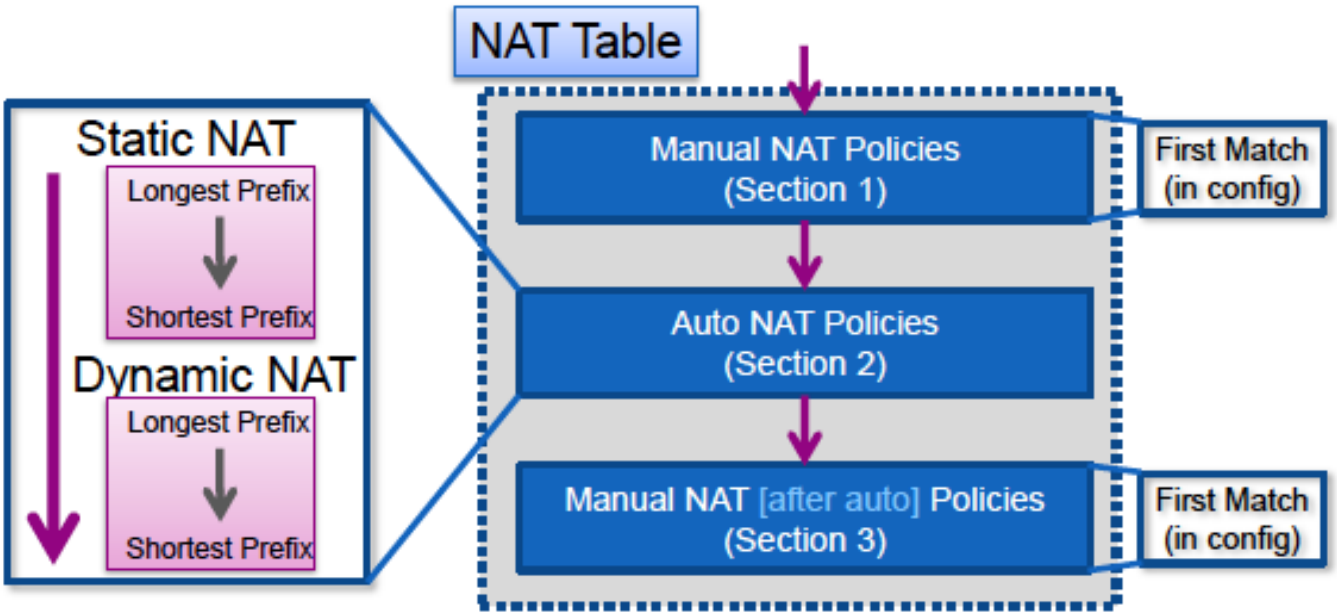
Все пакеты, обработанные ASA, оценены против таблицы NAT. Эта оценка запускается наверху (Раздел 1) и работает вниз, пока с правилом NAT не совпадают. Как только с правилом NAT совпадают, что правило NAT применено к соединению, и больше политики NAT не проверено против пакета.

Политика NAT на ASA создана из конфигурации NAT.

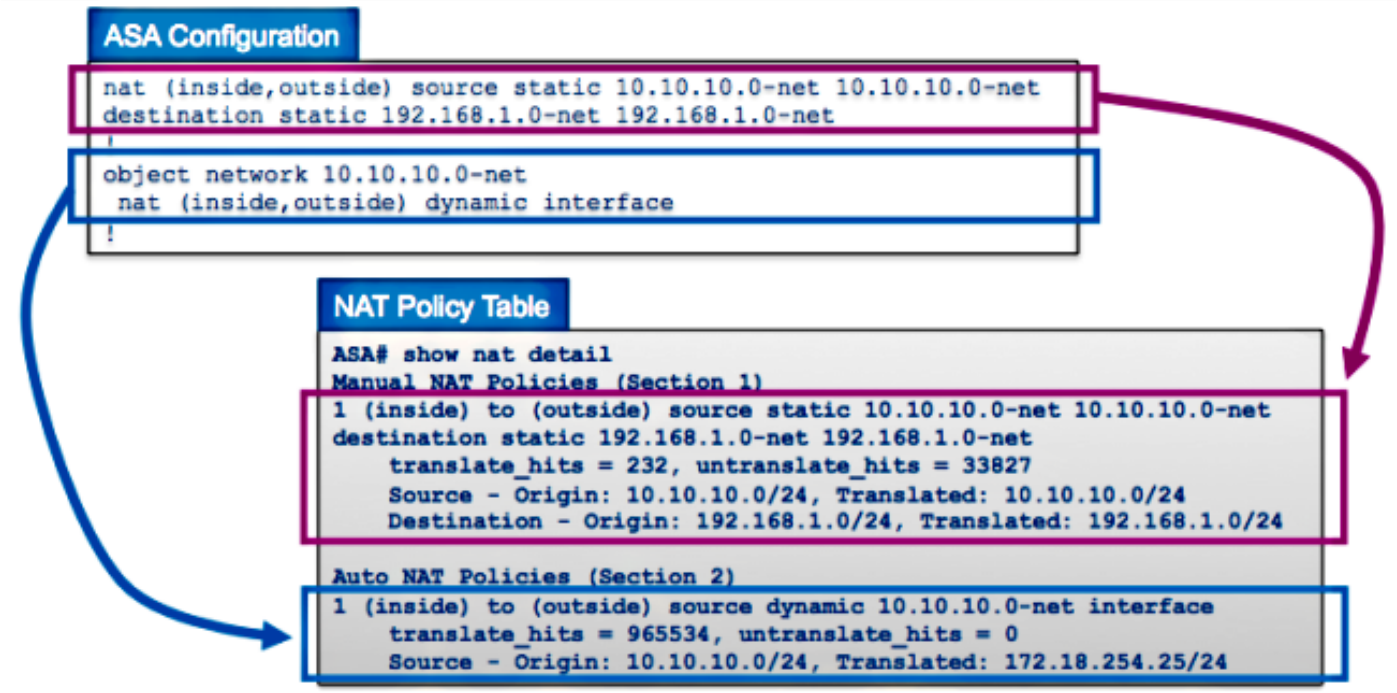
Три раздела ASA таблица NAT:

Раздел 1	**Ручная политика NAT** Они обработаны в заказе, в котором они появляются в конфигурации.
Раздел 2	**Автоматическая политика NAT** Они обработаны на основе типа NAT (статичный или динамичный) и префикс (маска подсе длина в объекте.
Раздел 3	**После - автоматическая ручная политика NAT** Они обработаны в заказе, в котором они появляются в конфигурации.

Эта схема показывает другие разделы NAT и как им упорядочивают:



Данный пример показывает, как конфигурация NAT ASA с двумя правилами (одно Ручное Выражение NAT и одна Автоматическая конфигурация NAT) представлена в таблице NAT:



Как устранить неполадки проблем NAT

Используйте утилиту Packet Tracer

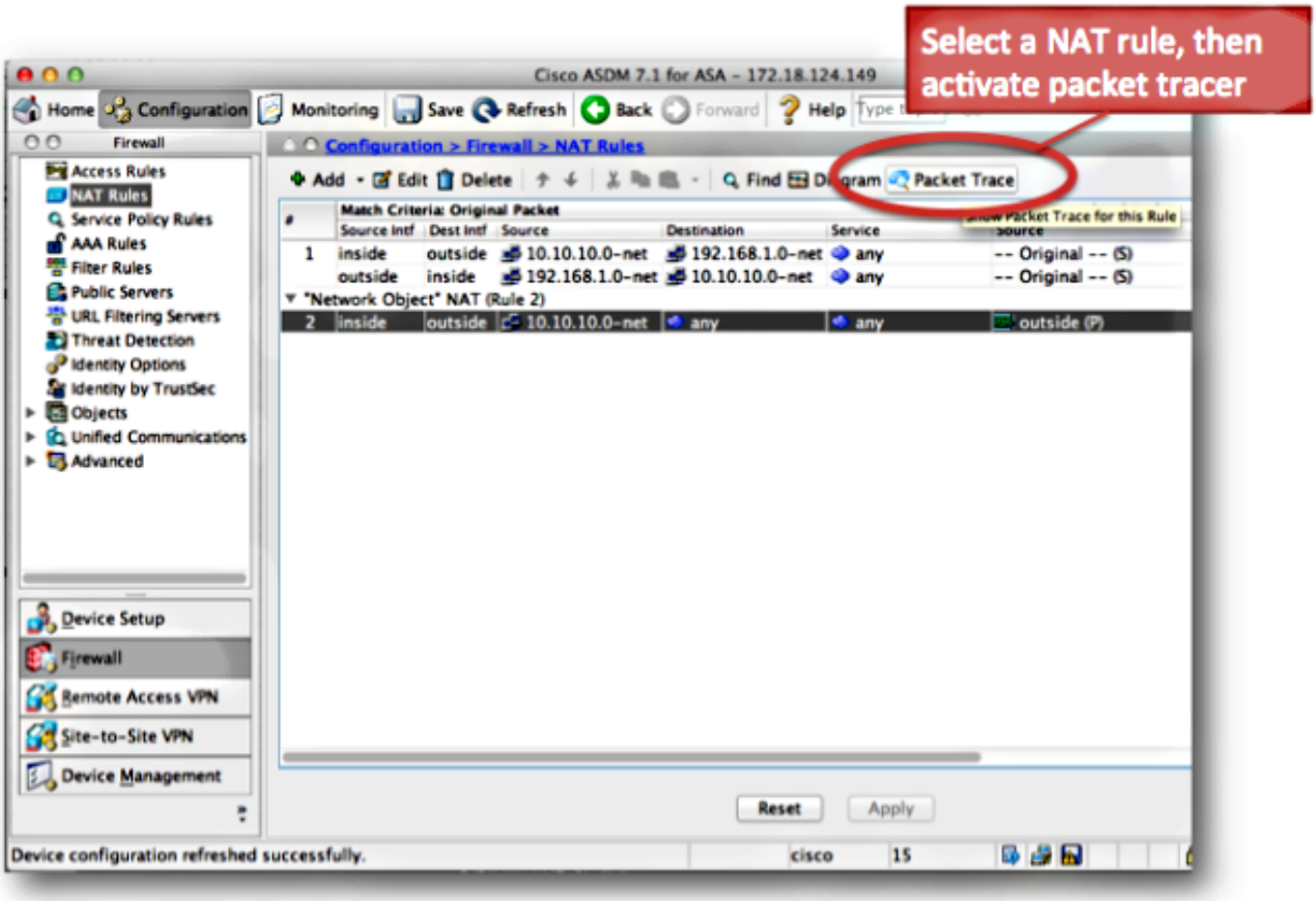
Для устренения проблем с конфигурациями NAT используйте **утилиту Packet Tracer**, чтобы проверить, что пакет поражает политику NAT. Пакетный трассировщик позволяет вам задавать типовой пакет, который вводит ASA, и ASA указывает на то, какая конфигурация применяется к пакету и если это разрешено или нет.

В примере ниже, дан типовой пакет TCP, который вводит внутренний интерфейс и

предназначен к хосту в Интернете. Утилита Packet Tracer показывает, что пакет совпадает с правилом динамического преобразования сетевых адресов (NAT) и преобразован во внешний IP - адрес 172.16.123.4:

```
ASA# packet-tracer input inside tcp 10.10.10.123 12345 209.165.200.123 80

...(output omitted)...

Phase: 2
Type: NAT
Subtype:
Result: ALLOW
Config:
object network 10.10.10.0-net
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 10.10.10.123/12345 to 172.16.123.4/12345

...(output omitted)...

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

ASA#
```

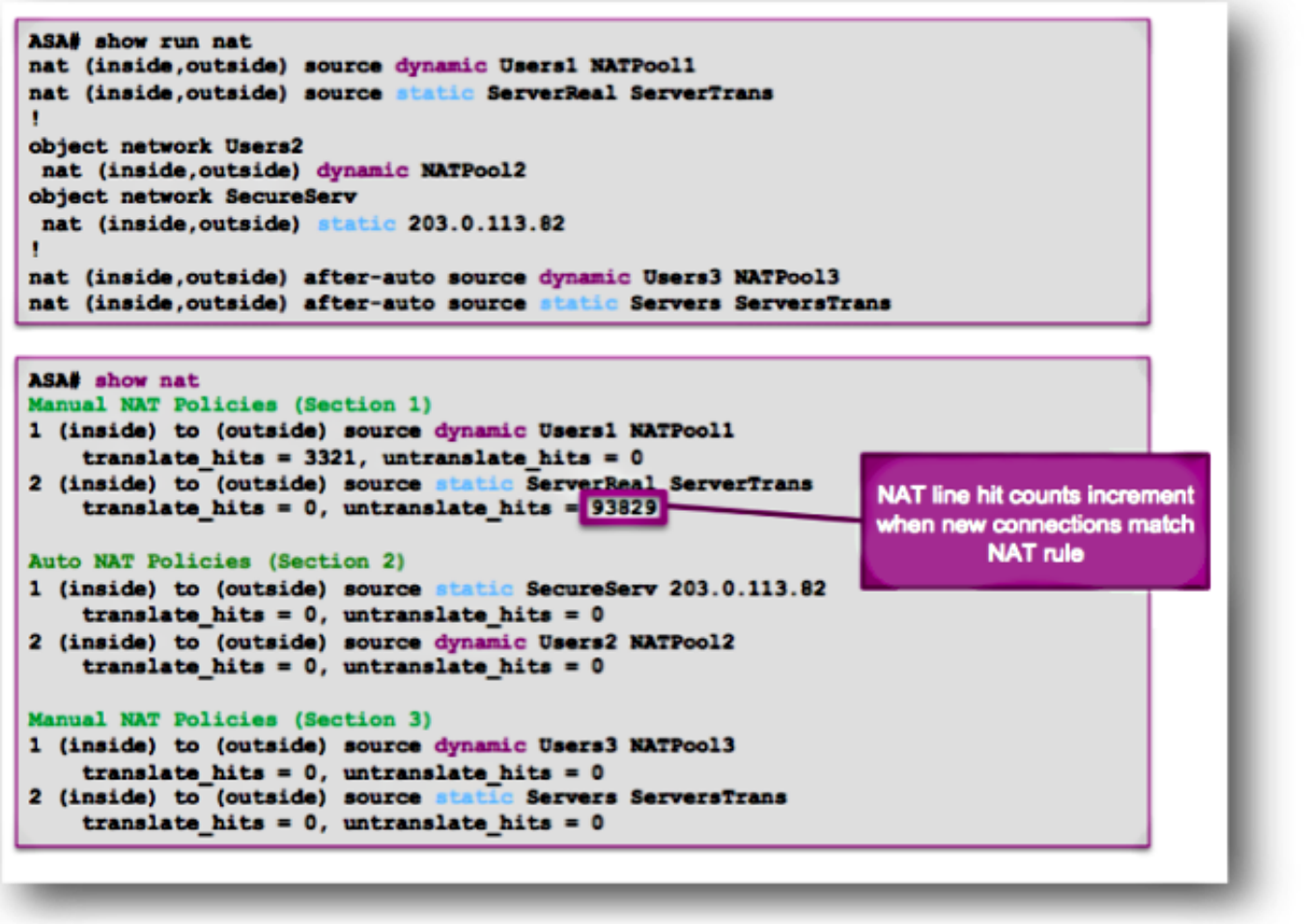
Выберите правило NAT и нажмите Packet Trace для активации пакетного трассировщика от Cisco Adaptive Security Device Manager (ASDM). Это использует IP-адреса, заданные в правиле NAT как вводы для пакетного программного средства трассировщика:



Просмотрите выходные данные команды Show Nat

Выходные данные **подробной** команды **nat показа** могут использоваться для просмотра Таблицы политики NAT. В частности **translate_hits** и счетчики **untranslate_hits** могут использоваться для определения, какие Записи NAT используются на ASA. Если вы видите, что ваше новое правило NAT не имеет никакого **translate_hits** или **untranslate_hits**, который означает, что или трафик не поступает в ASA, или возможно другое правило, которое имеет более высокий приоритет в таблице NAT, совпадает с трафиком.

Вот конфигурация NAT и Таблица политики NAT от другой конфигурации ASA:



В предыдущем примере существует шесть правил NAT, настроенных на этом ASA. **Выходные данные show nat** показывают, как эти правила используются для построения Таблицы политики NAT, а также количества **translate_hits** и **untranslate_hits** для каждого правила. Эти счетчики попаданий инкрементно увеличиваются только один раз в соединение. После того, как соединение создано через ASA, последующие пакеты, которые совпадают с тем текущим соединением, не инкрементно увеличивают линии NAT (во многом как способ, которым совершил нападки access-list, количество работает на ASA).

Translate_hits: количество новых соединений, которые совпадают с правилом NAT в прямом направлении.

"Прямое направление" означает, что соединение было создано через ASA в направлении интерфейсов, заданных в правиле NAT. Если правило NAT указало, что внутренний сервер преобразован во внешний интерфейс, заказ интерфейсов в правиле NAT является "nat (внутри, снаружи)..."; если тот сервер инициирует новое соединение к хосту на внешней стороне, инкрементах счетчика **translate_hit**.

Untranslate_hits: количество новых соединений, которые совпадают с правилом NAT в обратном направлении.

Если правило NAT указывает, что внутренний сервер преобразован во внешний интерфейс, заказ интерфейсов в правиле NAT является "nat (внутри, снаружи)..."; если клиент за пределами ASA инициирует новое соединение к серверу на внутренней части, инкрементах счетчика **untranslate_hit**.

Снова, если вы видите, что ваше новое правило NAT не имеет никакого **translate_hits** или

untranslate_hits, который означает, что или трафик не поступает в ASA, или возможно другое правило, которое имеет более высокий приоритет в таблице NAT, совпадает с трафиком.

Методика устранения проблем проблемы NAT

Используйте пакетный трассировщик, чтобы подтвердить, что типовой пакет совпадает с надлежащим правилом конфигурации NAT о ASA. Используйте **подробную** команду **nat показа** для понимания, какие правила политики NAT поражены. Если соединение совпадает с другой конфигурацией NAT, чем ожидаемый, устранение неполадок с этими вопросами:

- Существует ли другое правило NAT, которое имеет приоритет по правилу NAT, которое что вы предназначили трафик для удара?
- Существует ли другое правило NAT с определениями объекта, которые слишком широки (маска подсети слишком коротка, такой как 255.0.0.0), который заставляет этот трафик совпадать с неправильным правилом?
- Ручная политика NAT не в порядке, который заставляет пакет совпадать с неправильным правилом?
- Разве ваше правило NAT неправильно настроено, который вызывает правило не совпасть с вашим трафиком?

Посмотрите следующий раздел для примеров проблемы и решений.

Типичные проблемы с конфигурациями NAT

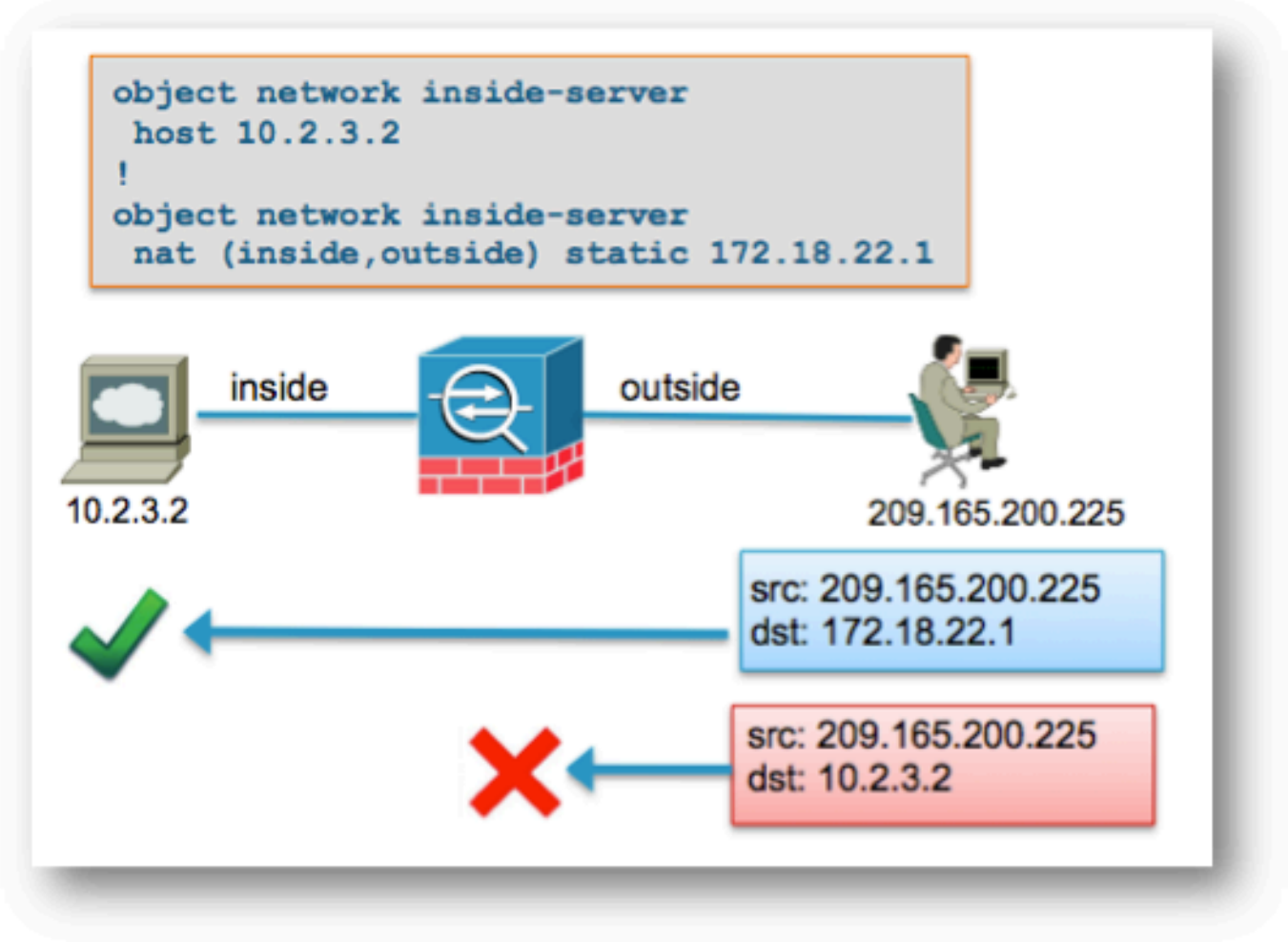
Вот некоторые типичные проблемы, испытанные при настройке NAT на ASA.

Проблема: Трафик отказывает из-за Ошибки Сбоя обратного пути (RPF) NAT: Асимметричные правила NAT совпали для форварда и обратных потоков

Проверка переадресации по обратному пути NAT гарантирует, что соединение, которое преобразовано ASA в прямом направлении, таком как TCP, синхронизируется (SYN), преобразован тем же правилом NAT в обратном направлении, таком как SYN/подтверждать TCP (ACK).

Обычно, эта проблема вызвана входящими подключениями, предназначенными к локальному (непреобразованному) адресу в Выражении NAT. На базовом уровне RPF NAT проверяет, что обратное подключение от сервера до клиента совпадает с тем же правилом NAT; если это не делает, сбои Проверки переадресации по обратному пути NAT.

Пример:



Когда внешний хост в **209.165.200.225** передает пакет, предназначенный непосредственно к локальному (непреобразованному) IP-адресу **10.2.3.2**, ASA отбрасывает пакет и регистрирует этот системный журнал:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows;
Connection for icmp src outside:209.165.200.225 dst inside:10.2.3.2 (type 8, code 0)
denied due to NAT reverse path failure
```

Решение:

Во-первых, гарантируйте, что хост передает данные к корректному глобальному адресу NAT. Если хост передает пакеты предназначенный верному адресу, проверьте правила NAT, которые поражены соединением. Проверьте, что правила NAT правильно определены, и что объекты, на которые ссылаются в правилах NAT, корректны. Также проверьте, что заказ правил NAT является соответствующим.

Используйте утилиту Packet Tracer для определения подробных данных отклоненного пакета. Пакетный трассировщик должен показать отброшенный пакет из-за сбоя Проверки переадресации по обратному пути. Затем, посмотрите на выходные данные пакетного трассировщика для наблюдения, какие правила NAT поражены в фазе NAT и фазе RPF NAT.

Если пакет совпадает с правилом NAT в фазе Проверки переадресации по обратному пути NAT, которая указывает, что обратный поток поразил бы преобразование NAT, но не совпадает с правилом в фазе NAT, которая указывает, что прямой поток НЕ поразил бы правило NAT, пакет отброшен.

Эти выходные данные совпадают со сценарием, показанным в предыдущей схеме, куда внешний хост неправильно передает трафик к local IP address сервера, а не глобальный (преобразовал) IP-адрес:

```
ASA# packet-tracer input outside tcp 209.165.200.225 1234 10.2.3.2 80

.....

Phase: 8
Type: NAT
Subtype: rpf-check
Result: DROP
Config:
object network inside-server
nat (inside,outside) static 172.18.22.1
Additional Information:
...
ASA(config)#
```

Когда пакет предназначен к корректному сопоставленному IP-адресу 172.18.22.1, пакет совпадает с корректным правилом NAT в фазе неNAT в прямом направлении и тем же правилом в фазе Проверки переадресации по обратному пути NAT:

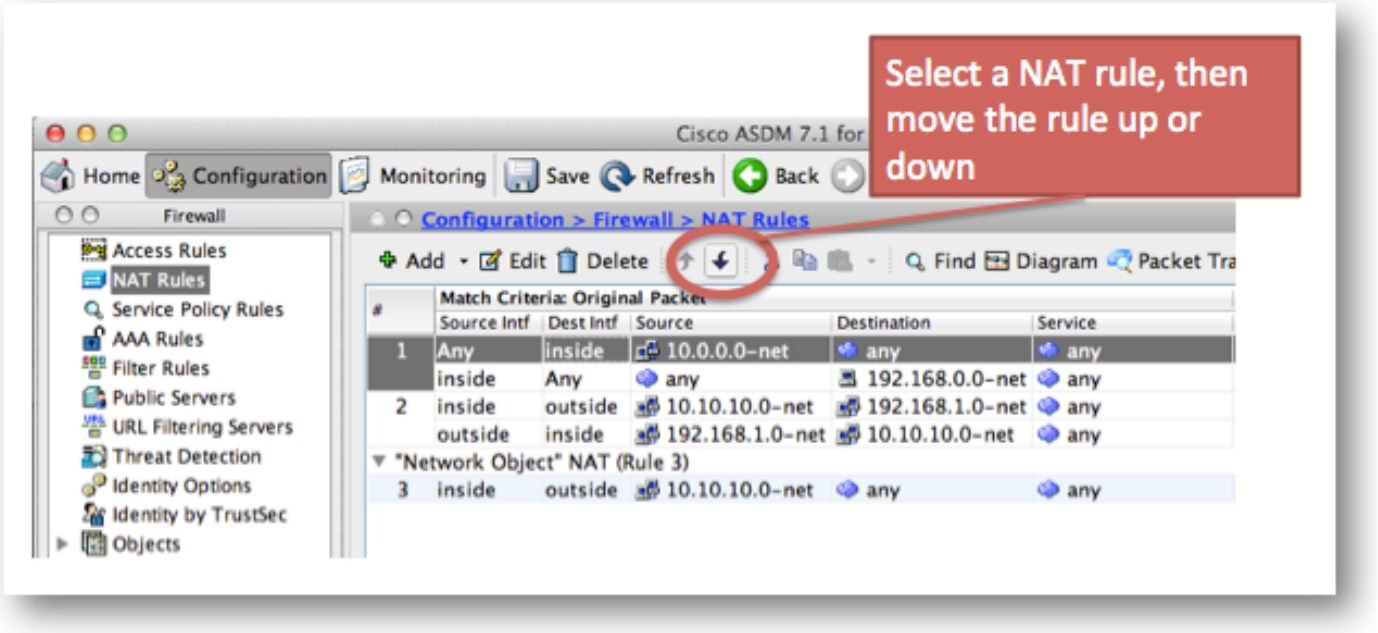
```
ASA(config)# packet-tracer input outside tcp 209.165.200.225 1234 172.18.22.1 80
...
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network inside-server
nat (inside,outside) static 172.18.22.1
Additional Information:
NAT divert to egress interface inside
Untranslate 172.18.22.1/80 to 10.2.3.2/80
...
Phase: 8
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network inside-server
nat (inside,outside) static 172.18.22.1
Additional Information:
...

ASA(config)#
```

Проблема: Ручные Правила NAT неисправны, который вызывает соответствия неверного пакета

Ручные правила NAT обработаны на основе их появления в конфигурации. Если очень широкое правило NAT перечислено сначала в конфигурации, оно могло бы отвергнуть другого, более определенное правило дальше вниз в таблице NAT. Используйте пакетный трассировщик для проверки, какое правило NAT трафик поражает; могло бы быть необходимо перестроить ручные Записи NAT к другому заказу.

Решение:

Переупорядочьте правила NAT с ASDM.



Решение:

Правила NAT могут быть переупорядочены с CLI, если вы удаляете правило и повторно вставляете его в определенном номере строки. Для вставки нового правила в определенной линии введите номер строки сразу после того, как заданы интерфейсы.

Пример:

```
ASA(config)# nat (inside,outside) 1 source static 10.10.10.0-net
10.10.10.0-net destination static 192.168.1.0-net 192.168.1.0-net
```

Проблема: Правило NAT слишком широко и совпадает с некоторым трафиком непреднамеренно

Иногда правила NAT созданы, что объекты использования, которые слишком широки. Если эти правила размещены около вершины таблицы NAT (наверху Раздела 1, например), они могли бы совпасть с большим количеством трафика, чем предназначенный и заставить правила NAT дальше вниз таблица никогда не поражаться.

Решение:

Используйте пакетный трассировщик, чтобы определить, совпадает ли ваш трафик с правилом с определениями объекта, которые слишком широки. Если это верно, необходимо уменьшить область тех объектов или переместить правила дальше вниз таблица NAT, или к после - автоматический раздел (Раздел 3) таблицы NAT.

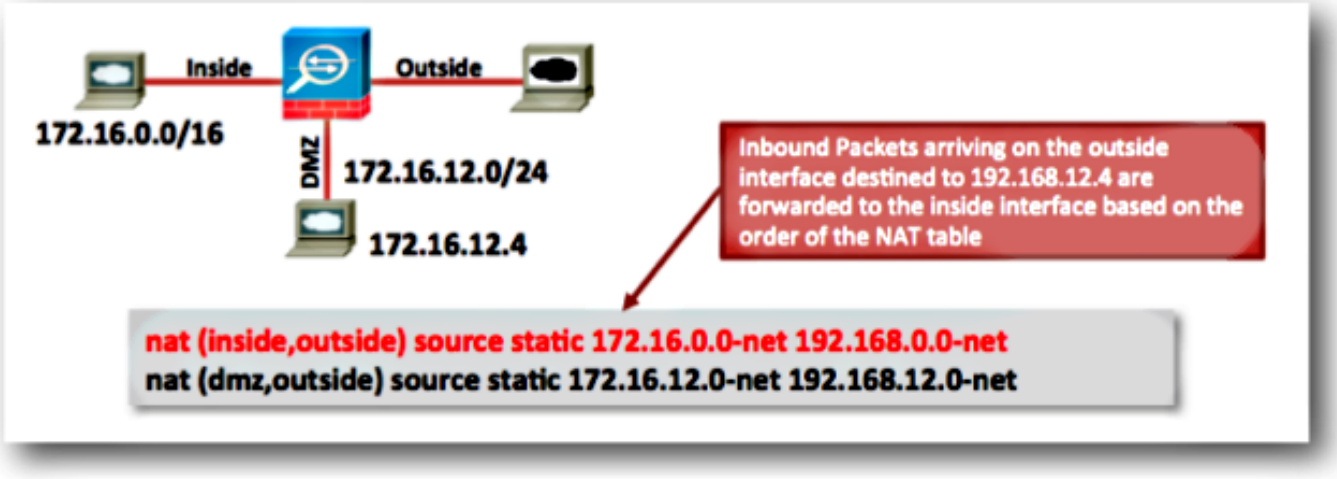
Проблема: Правило NAT отклоняет трафик к неверному интерфейсу

Правила NAT могут иметь приоритет по таблице маршрутизации, когда они определяют, какой интерфейс пакет будет выход ASA. Если входящий пакет совпадает с преобразованным IP-адресом в Выражении NAT, правило NAT используется для определения исходящего интерфейса.

NAT отклоняет проверку (который является тем, что может отвергнуть таблицу маршрутизации), проверки, чтобы видеть, существует ли какое-либо правило NAT, которое задает трансляцию адреса назначения (DA) для входящего пакета, который поступает в интерфейс. Если нет никакого правила, которое явно задает, как преобразовать IP - адрес назначения того пакета, то с таблицей глобальной маршрутизации консультируются для определения исходящего интерфейса. Если существует правило, которое явно задает, как преобразовать пакетный IP - адрес назначения, то правило NAT "вытягивает" пакет к другому интерфейсу в трансляции, и таблица глобальной маршрутизации эффективно обойдена.

Эта проблема чаще всего замечена для входящего трафика, который поступает во внешний интерфейс и обычно происходит из-за неисправных правил NAT, которые отклоняют трафик к непреднамеренным интерфейсам.

Пример:



Решения:

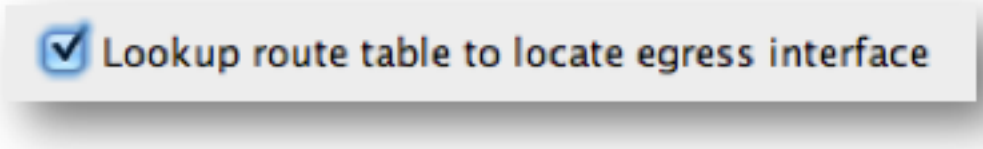
Эта проблема может быть решена с любым из этих действий:

- Переупорядочьте таблицу NAT так, чтобы больше специальной записи было перечислено сначала.
- Используйте неперекрывающиеся диапазоны глобального IP-адреса для Выражений NAT.

Обратите внимание на то, что, если правило NAT является идентификационным правилом, (что означает, что IP-адреса не изменены правилом), тогда, ключевое слово **поиска маршрута** может использоваться (это ключевое слово не применимо к приведенному выше примеру, так как правило NAT не является идентификационным правилом). Ключевое слово **поиска маршрута** заставляет ASA выполнять дополнительную проверку, когда это совпадает с правилом NAT. Это проверяет, что таблица маршрутизации ASA передает пакет к тому же исходящему интерфейсу, к которому эта конфигурация NAT отклоняет пакет. Если исходящий интерфейс таблицы маршрутизации не совпадает, NAT отклоняют интерфейс, с правилом NAT не совпадают (правило пропущено), и пакет продолжает вниз таблицу NAT, которая будет обработана более поздним правилом NAT.

Опция поиска маршрута только доступна, если правило NAT является 'идентичностью' правило NAT, что означает, что IP-адреса не изменены правилом. Опция **поиска маршрута** может быть включена на правило NAT, если вы добавляете **поиск маршрута** до конца линии

NAT, или если вы проверяете **таблицу маршрутизации Поиска для определения местоположения** флажка **исходящего интерфейса** в конфигурации правила NAT в ASDM:



Проблема: Правило NAT вызывает ASA к Протоколу разрешения proxy - адресации (ARP) для трафика на сопоставленном интерфейсе

Прокси - протоколы преобразования адресов ASA для глобального IP-адреса располагаются в Выражении NAT на глобальном интерфейсе. Если вы добавляете ключевое слово **без Proxy-arp** к Выражению NAT, эта функциональность Прокси - протокола преобразования адресов может быть отключена на основе правила на NAT.

Эта проблема также замечена, когда подсеть глобального адреса непреднамеренно создана, чтобы быть намного больше, чем это было предназначено, чтобы быть.

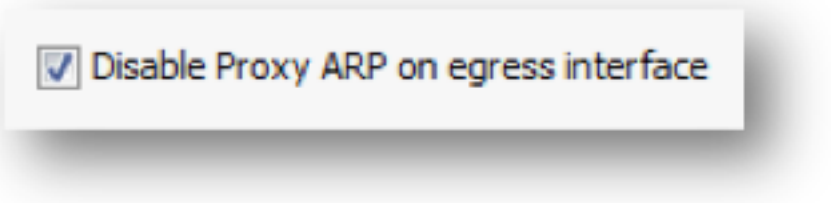
Решение:

Добавьте ключевое слово **без Proxy-arp** к линии NAT, если это возможно.

Пример:

```
ASA(config)# object network inside-server
ASA(config-network-object)# nat (inside,outside) static 172.18.22.1 no-proxy-arp
ASA(config-network-object)# end
ASA#
ASA# show run nat
object network inside-server
nat (inside,outside) static 172.18.22.1 no-proxy-arp
ASA#
```

Это может быть также выполнено с ASDM. В рамках правила NAT проверьте **Запрещать Прокси - протокол преобразования адресов на** флажке **исходящего интерфейса**.



Дополнительные сведения

- VIDEO: переадресация портов ASA для доступа сервера DMZ (версии 8.3 и 8.4)
- Основная Конфигурация NAT ASA: Веб-сервер в DMZ в Версии ASA 8.3 и позже
- Книга 2: руководство конфигурации интерфейса командой строки межсетевого экрана

серии Cisco ASA, 9.1
- Cisco Systems – техническая поддержка и документация