# ASA 8. 4 (4): определенная идентификационная запрещенная конфигурация NAT

## Содержание



## Введение

Устройства адаптивной безопасности (ASA), работающие 8.4 (4) или выше, могут отклонить определенные конфигурации NAT и отобразить сообщение об ошибках, подобное этому:

```
ERROR: <mapped address range> overlaps with <interface> standby interface
   address
ERROR: NAT Policy is not downloaded
```

Эта проблема может также появиться при обновлении ASA к 8.4 (4) или выше от предшествующего выпуска. Можно заметить, что некоторые команды NAT больше не присутствуют в running-config ASA. В этих экземплярах необходимо посмотреть на консольные сообщения, распечатанные, чтобы видеть, существует ли подарок сообщений в вышеупомянутом формате.

Другое заметное проявление состоит в том, что трафик для определенных подсетей за устройством ASA может перестать проходить через туннели VPN, оконечной точкой которых является ASA. Этот документ описывает, как решить эти проблемы.

## Перед началом работы

### Требования

Эти условия нужно соблюдать для обнаружения с этой проблемой:

- Рабочая версия 8.4 (4) ASA или выше, или обновленный к версии 8.4 (4) или выше от предшествующего выпуска.
- ASA, настроенный с резервным IP - адресом на по крайней мере одном из его

интерфейсов.
- NAT настроен с вышеупомянутым интерфейсом как сопоставленный интерфейс.

## Используемые компоненты

Сведения в этом документе основываются на этих версиях аппаратного программного обеспечения:

- ASA, работающие 8.4 (4) или выше

## Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

# Проблема

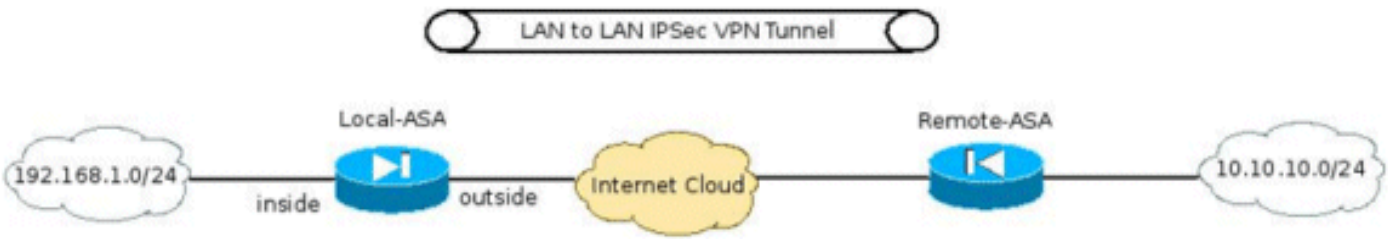
Как сообщение об ошибках предполагает, если сопоставленный диапазон адресов в статической инструкции NAT включает "резервный" IP-адрес, назначенный на сопоставленный интерфейс, команда NAT отклонена. Это поведение всегда существовало для перенаправления Статического порта, но это было представлено для Статических непосредственных Выражений NAT также с версией 8.4 (4) как исправление для идентификатора ошибки Cisco CSCtw82147 (только зарегистрированные клиенты).

Этот дефект был подан потому что до 8.4 (4) разрешенные пользователи ASA для настройки сопоставленного адреса в статической конфигурации NAT для совпадения с резервным IP - адресом, назначенным на сопоставленный интерфейс. Например, посмотрите на этот фрагмент конфигурации от ASA:

```
ciscoasa(config)# show run int e0/0 ! interface Ethernet0/0 nameif vm security-level 0 ip
address 192.168.1.1 255.255.255.0 standby 192.168.1.2 ciscoasa(config)# show run nat ! object
network obj-10.76.76.160 nat (tftp,vm) static 192.168.1.2
```

Даже при том, что команда принята, эта конфигурация NAT никогда не будет работать дизайном. В результате начинаясь 8.4 (4), ASA не позволяет такому правилу NAT быть настроенным во-первых.

Это привело к другой непредвиденной проблеме. Например, рассмотрите сценарий, где пользователь имеет VPN-туннель, завершающийся на ASA, и хочет позволить "внутренней" подсети быть в состоянии говорить с удаленной подсетью VPN.




Среди других команд, требуемых для настройки VPN-туннеля, одна из более важных конфигураций должна гарантировать, что трафик между подсетями VPN не становится преобразованным посредством NAT. Это внедрено с 8.3 и выше использования команды Manual/Twice NAT этого формата:

```
interface Ethernet0/0
 nameif inside
 security-level 0
 ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
object network obj-192.168.1.0
 description Inside subnet
 subnet 192.168.1.0 255.255.255.0
object network obj-10.10.10.0
 description Remote VPN subnet
 subnet 10.10.10.0 255.255.255.0
!
nat (inside,any) source static obj-192.168.1.0 obj-192.168.1.0 destination
   static obj-10.10.10.0 obj-10.10.10.0
!
object network obj-192.168.1.0
 nat (inside,outside) dynamic interface
```

Когда этот ASA будет обновлен к 8.4 (4) или выше, эта команда NAT не будет присутствовать в running-config ASA, и эта ошибка будет распечатана на консоли ASA:

```
ERROR: 192.168.1.0-192.168.1.255 overlaps with inside standby interface
   address
ERROR: NAT Policy is not downloaded
```

В результате трафик между подсетями 192.168.1.0/24 и 10.10.10.0/24 больше не будет течь через VPN-туннель.

## Решение

Существует два возможных обходной пути для этого условия:

- Сделайте команду NAT максимально определенной прежде, чем обновить к 8.4 (4), таким образом, сопоставленный интерфейс не "никто". Например, вышеупомянутая команда NAT может быть изменена на интерфейс, через который Удаленная подсеть VPN достижима (названный "снаружи" в вышеупомянутом сценарии):`nat (inside,outside) source static obj-192.168.1.0 obj-192.168.1.0 destination static obj-10.10.10.0 obj-10.10.10.0`
- Если вышеупомянутый обходной путь не возможен, выполните эти шаги:Когда ASA будет работать 8.4 (4) или выше, удалите резервный IP - адрес, назначенный на интерфейс.Примените команду NAT.Повторно примените резервный IP - адрес на интерфейсе.Пример:`ciscoasa(config)# interface Ethernet0/0 ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 ciscoasa(config-if)# exit ciscoasa(config)# nat (inside,any) 1 source static obj-192.168.1.0 obj-192.168.1.0 destination static obj-10.10.10.0 obj-10.10.10.0 ciscoasa(config)# interface Ethernet0/0 ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2`

# Дополнительные сведения

- Cisco Systems – техническая поддержка и документация