Использование NAT в перекрывающихся сетях

Содержание

Введение

В этом документе показано, как можно использовать преобразование сетевых адресов (NAT) для перекрывающихся сетей. Перекрывающиеся сети возникают, когда вы присваиваете устройству в вашей сети IP-адрес,уже находящийся в легальной собственности и присвоенный другому устройству в интернете или внешней сети. Перекрывающиеся сети также возникают, когда две компании, обе из которых в своих сетях используют RFC 1918 IP-адреса, сливаются. Эти две сети должны общаться, желательно без необходимости переадресации своих устройств.

Предварительные условия

Требования

Понимание основ IP-адресации, IP-маршрутизации и Domain Name System (DNS) поможет в понимании содержимого этого документа.

Используемые компоненты

Поддержка NAT началась в версии 11.2 программного обеспечения Cisco IOS. Для получения дополнительной информации о поддержке платформ посмотрите Часто задаваемое вопросы по преобразованию сетевых адресов (NAT).

Условные обозначения

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

Настройка

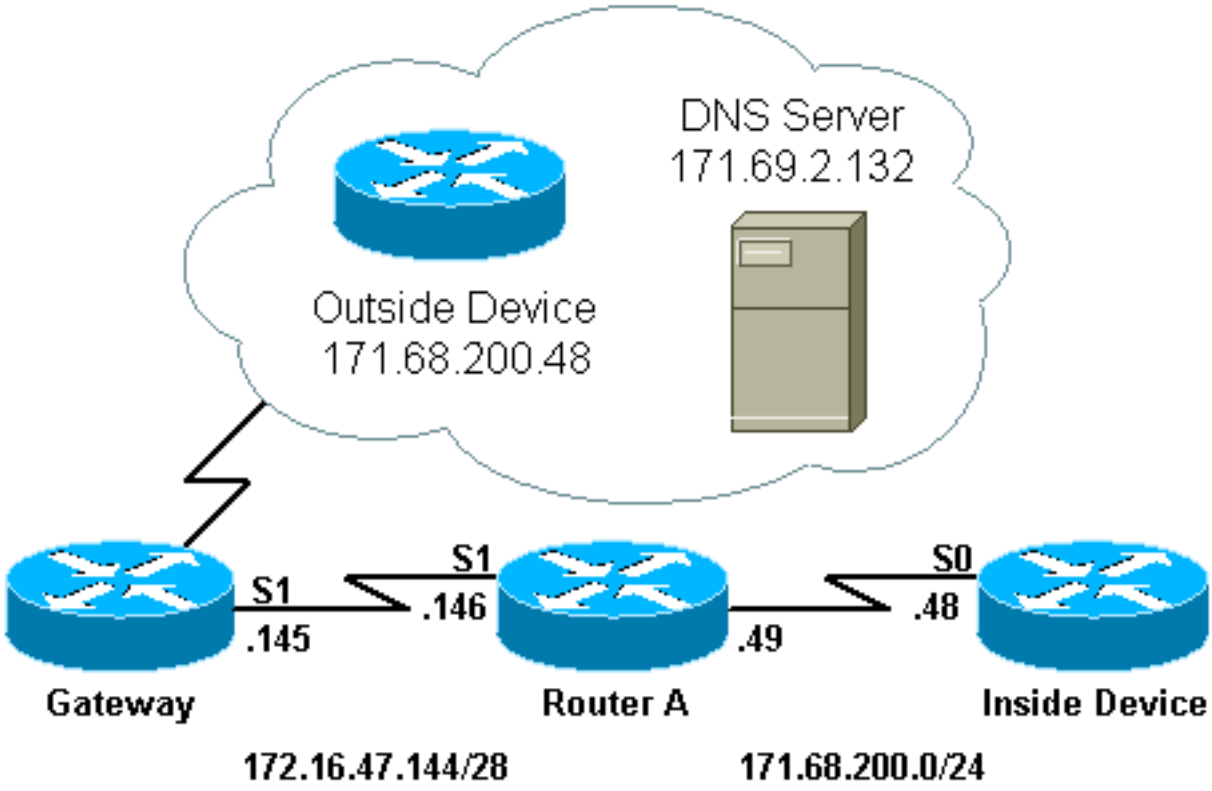
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" (Поиск команд) (только для зарегистрированных клиентов).

Схема сети

В данном документе используется сетевая установка, показанная на следующей схеме.

Обратите внимание, что внутреннее устройство и внешнее устройство, с которым оно связывается, имеют один и тот же IP-адрес.



Конфигурации

Маршрутизатор A настроен для NAT, такого, что это преобразовывает внутреннее устройство в адрес от пула "test-loop" и внешнее устройство к адресу от пула "тестовый dns". Пояснение того, как эта конфигурация помогает с наложением, придерживается таблицы конфигурации ниже.

Маршрутизатор A
`` ! version 11.2 no service udp-small-servers no service tcp-small-servers ```

```
!
hostname Router-A
!
!
ip domain-name cisco.com
ip name-server 171.69.2.132
!
interface Loopback0
 ip address 1.1.1.1 255.0.0.0
!
interface Ethernet0
 ip address 135.135.1.2 255.255.255.0
 shutdown
!
interface Serial0
 ip address 171.68.200.49 255.255.255.0
 ip nat inside
 no ip mroute-cache
 no ip route-cache
 no fair-queue
!
interface Serial1
 ip address 172.16.47.146 255.255.255.240
 ip nat outside
 no ip mroute-cache
 no ip route-cache
!
ip nat pool test-loop 172.16.47.161 172.16.47.165
prefix-length 28 ip nat pool test-dns 172.16.47.177
172.16.47.180 prefix-length 28 ip nat inside source list
7 pool test-loop ip nat outside source list 7 pool test-
dns ip classless ip route 0.0.0.0 0.0.0.0 172.16.47.145
access-list 7 permit 171.68.200.0 0.0.0.255 ! ! line con
0 exec-timeout 0 0 line aux 0 line vty 0 4 login ! end
```

Для вышеупомянутой конфигурации для помощи с наложением, когда внутреннее устройство связывается с внешним устройством оно должно использовать доменное имя внешнего устройства.

Внутреннее устройство не может использовать IP-адрес внешнего устройства, потому что это совпадает с адресом, назначенным на себя (внутреннее устройство). Поэтому внутреннее устройство передаст запрос DNS за доменным именем внешнего устройства. IP-адрес внутреннего устройства будет источником этого запроса, и тот адрес будет преобразован в адрес от пула "test-loop", потому что настроена **команда ip nat inside source list**.

Сервер DNS отвечает на адрес, который прибыл из пула "test-loop" с IP-адресом, привязанным к доменному имени внешнего устройства в информационном наполнении пакета. Адрес назначения (DA) пакета ответа преобразован назад в адрес внутреннего устройства, и адрес в информационном наполнении пакета ответа тогда преобразован в адрес от пула "тестовый dns" из-за **команды ip nat outside source list**. Поэтому внутреннее устройство узнает, что IP-адрес для внешнего устройства является одним из адресов от пула "тестового dns", и это будет использовать этот адрес при передаче с внешним устройством. Маршрутизатор рабочий NAT заботится о трансляциях на этом этапе.

Этот процесс может быть замечен подробно в разделе Устранения неполадок. Устройства с помощью совмещенных адресов могут связаться друг с другом без использования DNS, но в этом случае, статический NAT должен был бы быть настроен. Пример того, как это могло бы быть сделано, придерживается.

Маршрутизатор A

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
!
!

ip domain-name cisco.com
ip name-server 171.69.2.132
!
interface Loopback0
 ip address 1.1.1.1 255.0.0.0
!
interface Ethernet0
 ip address 135.135.1.2 255.255.255.0
 shutdown
!
interface Serial0
 ip address 171.68.200.49 255.255.255.0
 ip nat inside
 no ip mroute-cache
 no ip route-cache
 no fair-queue
!
interface Serial1
 ip address 172.16.47.146 255.255.255.240
 ip nat outside
 no ip mroute-cache
 no ip route-cache
!
ip nat pool test-loop 172.16.47.161 172.16.47.165
prefix-length 28
ip nat inside source list 7 pool test-loop ip nat
outside source static 171.68.200.48 172.16.47.177 ip
classless ip route 0.0.0.0 0.0.0.0 172.16.47.145 ip
route 172.16.47.160 255.255.255.240 Serial0 !--- This
line is necessary to make NAT work for return traffic.
!--- The router needs to have a route for the pool to
the inside !--- NAT interface so it knows that a
translation is needed. access-list 7 permit 171.68.200.0
0.0.0.255 ! ! line con 0 exec-timeout 0 0 line aux 0
line vty 0 4 login ! end
```

С вышеупомянутой конфигурацией, когда внутреннее устройство хочет связаться с внешним устройством, это может теперь использовать IP-адрес 172.16.47.177 и DNS в не необходимый. Как показано выше, трансляция адреса внутреннего устройства все еще сделана динамично, что означает, что маршрутизатор должен получить пакеты от внутреннего устройства, прежде чем будет создана трансляция. Поэтому внутреннее устройство должно инициировать все соединения для внутреннего устройства и внешнего устройства для передачи. Если бы это требовалось, что внешнее устройство инициирует соединения с внутренним устройством, то адрес для внутреннего устройства должен также быть статически настроен.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Процесс, которым внутреннее устройство использовало DNS для передачи с внешним устройством, как описано выше, может быть просмотрен подробно со следующим процессом устранения проблем.

На данный момент в таблице трансляций отсутствуют трансляции, которые можно просмотреть командой show ip nat translations. Примеры ниже используют **команды debug ip packet и debug ip nat** вместо этого.

Примечание: Команды отладки генерируют значительный объем выходных данных. Используйте эти команды только при незначительном объеме трафика в IP-сети, чтобы оказать отрицательного влияния на остальные виды активности системы.

```
Router-A# show ip nat translations Router-A# show debug Generic IP: IP packet debugging is on
(detailed) IP NAT debugging is on
```

Когда внутреннее устройство отправляет запрос DNS на сервер DNS, находящийся за пределами домена NAT, исходный адрес запроса DNS (адрес внутреннего устройства) транслируется благодаря элементу ip nat внутри команд. Это отображено в приведенных ниже данных отладки.

```
NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0]
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
    UDP src=6988, dst=53
```

Когда DNS-сервер посылает DNS-ответ, полезные данные ответа передаются благодаря командам ip nat outside.

Примечание: NAT не посмотрел на информационное наполнение ответа DNS, пока трансляция не происходит на IP - заголовке пакета ответа. **См. команду ip nat outside source list 7 pool в конфигурации маршрутизатора, приведенной выше.**

Первое сообщение NAT в следующих выходных данных отладки показывает, что маршрутизатор распознает ответ DNS и преобразует IP-адрес в полезных данных в 172.16.47.177. Второе сообщение NAT показывает, что маршрутизатор преобразует адрес назначения для ответа DNS, чтобы переслать ответ внутреннему устройству, подавшему запрос DNS. Часть назначения заголовка, внутреннего глобального адреса, преобразована во внутренний локальный адрес.

Транслируются полезные данные ответа DNS:

```
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
```

Часть IP-заголовка, содержащая место назначения, в пакете ответа DNS переносится:

```
NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65371]
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
    UDP src=53, dst=6988
```

Давайте посмотрим на другой запрос DNS и ответ:

```
NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0]
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
    UDP src=7419, dst=53
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
```

```
NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65388]
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
    UDP src=53, dst=7419
```

Теперь, когда полезная нагрузка DNS преобразована, в нашей таблице преобразования есть запись для внешних локального и глобального адресов внешнего устройства. С помощью этих записей в таблице можно полностью транслировать заголовок пакетов ICMP, которыми обмениваются внутреннее и внешнее устройства. Давайте рассмотрим такой обмен в приведенных ниже выходных данных отладки.

В приведенных ниже выходных данных показан передаваемый адрес источника (внутренний адрес устройства).

```
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [406]
```

Здесь, адрес назначения (DA) (внешний локальный адрес внешнего устройства) преобразован.

```
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [406]
```

После трансляции пакет IP похож на это:

```
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

Следующие выходные данные отображают преобразование исходного адреса (адрес внешнего устройства) в возвращаемом пакете.

```
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16259]
```

Теперь транслируется адрес назначения возвращаемого пакета (внутри глобального адреса устройства).

```
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16259]
```

После трансляции возвращаемый пакет похож на это:

```
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

Обмен пакетами между внутренним и внешним устройствами продолжается.

```
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [407]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [407]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16262]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16262]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [408]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [408]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16267]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16267]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [409]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [409]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16273]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16273]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
```

```
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [410]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [410]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16277]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16277]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

После завершения обмена пакетами между внешним и внутренним устройствами посмотрим на таблицу преобразования, которая содержит три записи. Первая запись была создана, когда внутреннее устройство отправило запрос DNS. Вторая запись была создана после трансляции полезных данных DNS-ответа. Когда эхо-запросом обменялись между внутренним устройством и внешним устройством, третья запись была создана. Третья запись является итоговой суммой первых двух записей и используется для более эффективных преобразований.

```
Router-A# show ip nat translations Pro Inside global Inside local Outside local Outside global -
-- 172.16.47.161 171.68.200.48 --- --- --- --- --- 172.16.47.177 171.68.200.48 --- 172.16.47.161
171.68.200.48 172.16.47.177 171.68.200.48
```

Важно обратить внимание, когда вы пытаетесь установить подключение между двумя наложениями сети путем выполнения динамического NAT на одиночном маршрутизаторе Cisco, необходимо использовать DNS для создания внешней стороны, локальной для внешнего глобального преобразования. Если вы не используете DNS, подключение может быть установлено со статическим NAT, но более трудно управлять.

Дополнительные сведения

- Страница поддержки NAT
- Техническая поддержка - Cisco Systems