Пример конфигурации с использованием команды ip nat outside source

Содержание

Введение

Данный документ содержит пример конфигурации с использованием команды **ip nat outside source list** и включает в себя краткое описание того, что происходит с IP–пакетами во время процесса NAT (Преобразование сетевых адресов). Эту команду можно использовать для трансляции адреса источника IP–пакетов, поступающих из внешней сети во внутреннюю сеть. Данное действие преобразует адрес назначения IP–пакетов, перемещаемых в противоположном направлении - из внутренней сети во внешнюю. Эта команда используется в таких ситуациях как наложение сетей, когда адреса внутренней сети перекрывают адреса внешней сети Рассмотрим схему сети в качестве примера.

Предварительные условия

Требования

Для данного документа нет особых требований.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к устройству или какой-либо версии ПО. Однако сведения, содержащиеся в данном документе, касаются следующих версий программного и аппаратного обеспечения:

- Маршрутизаторы серии Cisco 2500
- ПО Cisco IOS® версии 12.2 (24a) на всех маршрутизаторах

Данные для этого документа были получены при тестировании указанных устройств в специально созданных лабораторных условиях. Все устройства, описанные в данном документе, обладают ненастроенной (заданной по умолчанию) конфигурацией. При работе в действующей сети необходимо изучить все возможные последствия каждой команды.

Условные обозначения

Дополнительные сведения о применяемых в документе обозначениях см. в документе Условные обозначения, используемые в технической документации Cisco.

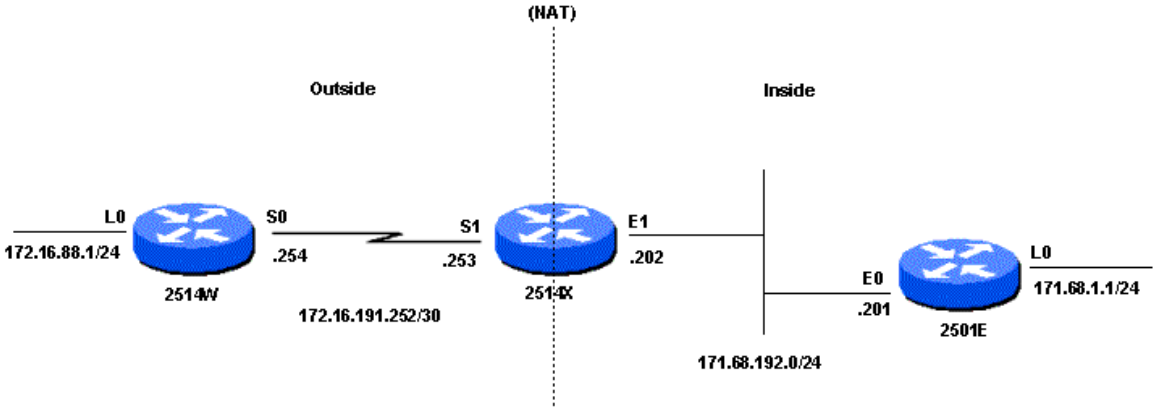
Настройка

В этом разделе приводится информация по настройке функций, описанных в данном документе.

Примечание. Дополнительную информацию о командах, используемых в данном документе, можно получить с помощью Средства поиска команд (только для зарегистрированных клиентов).

Схема сети

В данном документе используется следующая настройка сети:



Если команда ping отправлена с интерфейса Loopback0 (172.16.88.1) маршрутизатора 2514W на интерфейс Loopback0 (171.68.1.1) маршрутизатора 2501E, происходит следующее:

Маршрутизатор 2514W пересылает пакеты маршрутизатору 2514X, так как он настроен с использованием маршрута по умолчанию. Находясь на внешнем интерфейсе маршрутизатора 2514X, пакет имеет адрес источника (SA) 172.16.88.1 и адрес назначения (DA) 171.68.1.1. Так как адрес SA задан в списке доступа 1, который используется командой **ip nat outside source list**, он преобразуется в адрес из пула Net171 NAT. Отметим, что команда **ip nat outside source list** ссылается на пул "Net171" NAT. В этом случае адрес преобразуется в 171.68.16.10, который является самым первым доступным адресом в пуле NAT. После трансляции маршрутизатор 2514X отыскивает адрес назначения в таблице маршрутизации и определяет маршрут пакета. Маршрутизатор 2501E "видит" пакет на своем входящем интерфейсе с SA-адресом 171.68.16.10 и DA-адресом 171.68.1.1. В ответ он отправляет эхо-ответ ICMP (Протокол управляющих сообщений в Интернет-сети) на адрес 171.68.16.5. Если маршрут отсутствует, маршрутизатор отбрасывает пакет. В этом случае он имеет маршрут (по умолчанию) и отправляет пакеты на маршрутизатор 2545X, используя SA-адрес 171.68.1.1 и DA-адрес 171.68.16.10. Маршрутизатор 2514X "видит" пакет в своем внутреннем интерфейсе и проверяет маршрут для адреса 171.68.16.10. Если маршрут не найден, маршрутизатор посылает в ответ сообщение ICMP о недостижимости. В этом случае он имеет маршрут к адресу 171.68.16.10 (благодаря параметру **add-route** команды **ip nat outside source**, который добавляет маршрут хоста на основе преобразования внешнего глобального адреса во внешний локальный адрес), поэтому маршрутизатор снова преобразует пакет в адрес 172.16.88.1 и прокладывает его путь из внешнего интерфейса.

Конфигурации

Маршрутизатор 2514W
hostname 2514W ! *!--- Выходные данные команды подавлены.* interface Loopback0 ip address 172.16.88.1 255.255.255.0 !

```
!--- Выходные данные команды подавлены.

interface Serial0
ip address 172.16.191.254 255.255.255.252
no ip mroute-cache
!
!--- Выходные данные команды подавлены.

ip classless
ip route 0.0.0.0 0.0.0.0 172.16.191.253
!--- Маршрут по умолчанию для пересылки пакетов на 2514X.


!
!--- Выходные данные команды подавлены.
```

Маршрутизатор 2514X

```
hostname 2514X
!
!--- Выходные данные команды подавлены.

!
interface Ethernet1
ip address 171.68.192.202 255.255.255.0
ip nat inside
no ip mroute-cache
no ip route-cache
!
!--- Выходные данные команды подавлены.

interface Serial1
ip address 172.16.191.253 255.255.255.252
ip nat outside
no ip mroute-cache
no ip route-cache
clockrate 2000000
!
ip nat pool Net171 171.68.16.10 171.68.16.254 netmask 255.255.255.0
!--- Пул NAT определяет внешние локальные адреса для использования в преобразовании.

!
ip nat outside source list 1 pool Net171 add-route
!--- Настраивает преобразование внешних глобальных адресов
!--- с использованием пула NAT.


ip classless
ip route 172.16.88.0 255.255.255.0 172.16.191.254
ip route 171.68.1.0 255.255.255.0 171.68.192.201
!--- Статические маршруты для достижения интерфейсов обратной связи
!--- на 2514W и 2501E.


access-list 1 permit 172.16.88.0 0.0.0.255
!--- Список доступа определяет внешние глобальные адреса для преобразования.


!
!--- Выходные данные команды подавлены.

!
```

Маршрутизатор 2501E

```
hostname 2501E
!
!--- Выходные данные команды подавлены.

interface Loopback0
ip address 171.68.1.1 255.255.255.0
!
interface Ethernet0
```

```
ip address 171.68.192.201 255.255.255.0
!
!--- Выходные данные команды подавлены.

ip classless
ip route 0.0.0.0 0.0.0.0 171.68.192.202
!--- Маршрут по умолчанию для пересылки пакетов на 2514X.


!
!--- Выходные данные команды подавлены.
```

Проверка

В этом разделе приведена информация, которую можно использовать для проверки правильности работы конфигурации.

Некоторые команды **show** поддерживаются Интерпретатором выходных данных (только для зарегистрированных клиентов); это позволяет выполнять анализ выходных данных команды **show**.

Команда **show ip nat translations** используется для проверки записей трансляции, как показано в выходных данных ниже.

```
2514X# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 171.68.1.1          171.68.1.1         171.68.16.10       172.16.88.1
--- ---                 ---                171.68.16.10       172.16.88.1

2514X#
```

Как показано в выходных данных выше, внешний глобальный адрес 172.16.88.1, который является адресом интерфейса Loopback0 маршрутизатора 2514W, преобразуется во внешний глобальный адрес 171.68.16.10.

Для проверки записей таблиц маршрутизации можно использовать команду **show ip route**, как показано ниже:

```
2514X# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    171.68.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       171.68.192.0/24 is directly connected, Ethernet1
S       171.68.1.0/24 [1/0] via 171.68.192.201
S       171.68.16.10/32 [1/0] via 172.16.88.1
    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
S       172.16.88.0/24 [1/0] via 172.16.191.254
C       172.16.191.252/30 is directly connected, Serial1
2514X#
```

В выходных данных показан маршрут /32 для внешнего локального адреса 171.68.16.10, созданного благодаря использованию параметра **add-route** команды **ip nat outside source**. Этот маршрут используется для маршрутизации и трансляции пакетов, проходящих из внутренней сети во внешнюю.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Эти выходные данные получены в результате выполнения команд **debug ip packet** и **debug ip nat** на маршрутизаторе 2514X при посылке ping-запроса с адреса интерфейса loopback0 (172.16.188.1) маршрутизатора 2514W на адрес интерфейса loopback0 (171.68.1.1) маршрутизатора 2501E:

```
*Mar  1 00:02:48.079: NAT*: s=172.16.88.1->171.68.16.10, d=171.68.1.1 [95]
!--- Адрес источника в первом пакете, поступающем
!--- по внешнему интерфейсу, сначала преобразуется.


*Mar  1 00:02:48.119: IP: tableid=0, s=171.68.16.10 (Serial1), d=171.68.1.1 (Ethernet1), routed via
RIB
*Mar  1 00:02:48.087: IP: s=171.68.16.10 (Serial1), d=171.68.1.1 (Ethernet1), g=171.68.192.201, len
100, forward
!--- Пакет эхо-запроса ICMP с преобразованными адресом источника
!--- маршрутизируется и пересылается на внутренний интерфейс.


*Mar  1 00:02:48.095: IP: tableid=0, s=171.68.1.1 (Ethernet1), d=171.68.16.10 (Serial1), routed via
RIB
!--- Пакет это-ответа ICMP, поступающий по внутреннему интерфейсу,
!--- сначала маршрутизируется на основе адреса назначения.


*Mar  1 00:02:48.099: NAT: s=171.68.1.1, d=171.68.16.10->172.16.88.1 [95]
!--- Затем выполняется преобразование адреса назначения в пакете.


*Mar  1 00:02:48.103: IP: s=171.68.1.1 (Ethernet1), d=172.16.88.1 (Serial1), g=172.16.191.254, len 1
00, forward
!--- Пакет эхо-ответа ICMP с преобразованным адресом
!--- назначения пересылается на внешний интерфейс.
```

Вышеописанная процедура повторяется для каждого пакета, принятого на внешнем интерфейсе.

Краткие выводы

Главное отличие команды **ip nat outside source list** (динамическое преобразование NAT) от команды **ip nat outside source static** (статическое преобразование NAT) состоит в том, что записи в таблице преобразования отсутствуют до тех пор, пока маршрутизатор (настроенный для NAT) не проверит критерии преобразования пакета. В вышеуказанном примере пакет с SA-адресом 172.16.88.1 (поступающий из внешнего интерфейса маршрутизатора 2514X) соответствует списку доступа 1. Эти критерии используется командой **ip nat outside source list** . По этой причине пакеты, исходящие из внешней сети, должны существовать прежде, чем пакеты из внутренней сети смогут взаимодействовать с интерфейсом loopback0 маршрутизатора 2514W.

Обратите внимание на два важных момента в этом примере.

Во-первых, когда пакет поступает из внешней сети во внутреннюю, сначала происходит трансляция, а потом для определения места назначения проверяется таблица маршрутизации. Когда пакет поступает из внутренней сети во внешнюю, сначала для определения места назначения проверяется таблица маршрутизации, а потом происходит трансляция.

Во-вторых, необходимо определить, какая часть IP-пакета преобразуется при использовании каждой из описанных выше команд. В следующей таблице даны рекомендации:

Команда	Действие
ip nat outside source list	• транслирует источник пакетов IP, передаваемых из внешней сети во внутреннюю • транслирует назначение IP-пакетов, передаваемых из внутренней сети во внешнюю.

ip nat inside source list	• транслирует источник IP-пакетов, передаваемых из внутренней сети во внешнюю. • транслирует назначение пакетов IP, передаваемых из внешней сети во внутреннюю.

Из вышесказанного понятно, что существует несколько способов трансляции пакета. В зависимости от конкретных требований следует задать способ определения интерфейсов NAT (внутренний или внешний), а также какие маршруты должна содержать таблица маршрутизации до или после трансляции. Помните, что часть преобразуемого пакета зависит от направления передачи пакета и от настройки NAT.

Дополнительные сведения

- **Как работает NAT**
- **NAT: Локальные и глобальные определения**
- **Образец конфигурации с использованием команды ip nat outside source static**
- **Преобразование сетевых адресов: порядок работы**
- **Использование NAT в перекрывающихся сетях**
- **Преобразование сетевых адресов (NAT) на одном интерфейсе**
- **Страница поддержки технологии NAT**
- **Техническая поддержка – Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/10/107538/1.shtml