Hairpin NAT – делаем доступ к сервисам пользователям из LAN используя внешний IP

Hairpin NAT очень полезная штука в случае когда надо дать доступ внутренним сервисам (находящимся в LAN) друг к другу, используя внешний IP адрес (например, “для единообразия” или если не хочется заморачиваться с DNS).

Делается это просто:

```
iptables -t nat -A PREROUTING -d ${extip} -p tcp -m tcp --dport ${extport} -j DNAT --to-destination ${localhostip}
iptables -t nat -A POSTROUTING -s ${intnet} -d ${localhostip} -p tcp -m tcp --dport ${intport} -j MASQUERADE
```

Где:

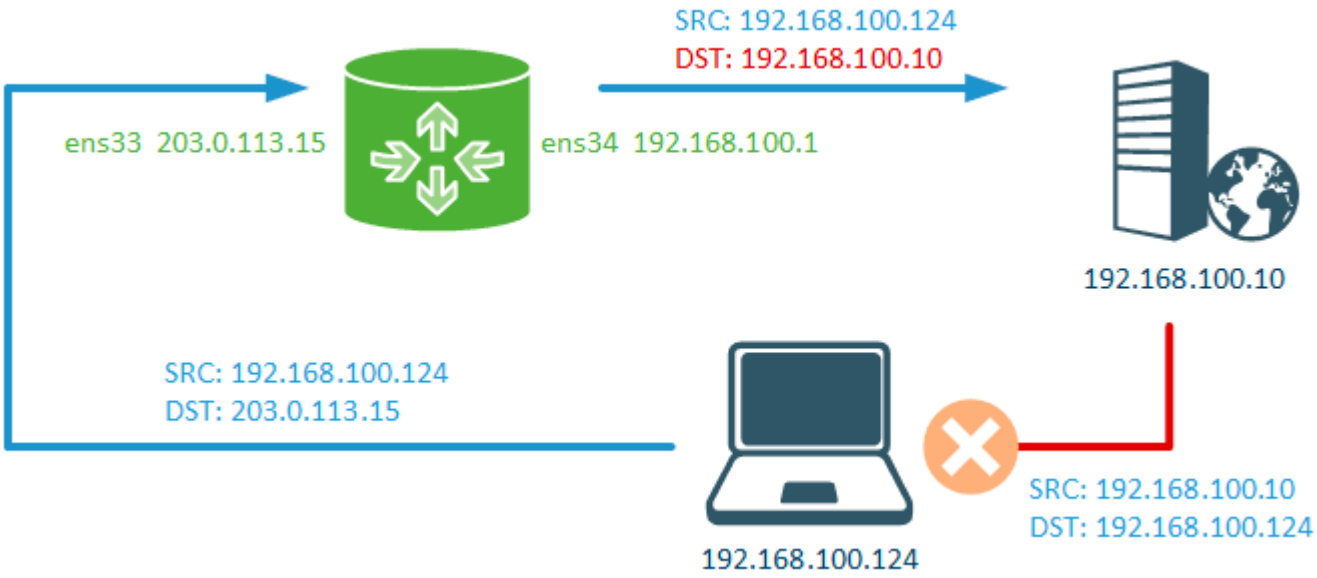
- extip – внешний IP адрес.
- extport – внешний порт.
- intport – порт сервера в локальной сети.
- localhostip – IP адрес сервера в локальной сети.
- intnet – внутренняя подсеть (например, 192.168.0.0/24).

Не добавляйте соответствие интерфейсов (параметр -i) в правило, это сделает Hairpin NAT нерабочим в большинстве случаев!

NAT loopback или Hairpin NAT

Несмотря на интересное название, это очень распространенный случай. Мобильный клиент, для которого настроен проброс портов на внешнем интерфейсе приходит в офис и у него внезапно все перестает работать. Можно, конечно, настроить несколько вариантов подключения, для нахождения в офисе и для нахождения вне его, но зачем?

Прежде всего давайте разберемся, почему вдруг все сломалось, для этого внимательно рассмотрим следующую схему:



Мобильный клиент, с адресом принадлежащим офисной сети, обращается к серверу в этой же сети, но через внешний интерфейс маршрутизатора. Маршрутизатор привычно выполнит **DNAT** и отправит пакет серверу, который увидит, что адрес источник находится в одной сети с ним и пошлет обратный пакет напрямую, минуя маршрутизатор.

Но клиент устанавливал соединение с узлом **203.0.113.15**, а получает пакет от узла **192.168.100.10**, такой пакет получит статус **INVALID** и будет отброшен. Понятно, что ничего работать не будет.

Как избежать этой ситуации? Нужно сделать так, чтобы обратный пакет не отправлялся напрямую клиенту, а был возвращен маршрутизатору, для этого снова используем **SNAT**. Обратите внимание, что к этому времени пакет уже пройдет цепочку PREROUTING и в критериях нам следует оперировать внутренним адресом и портом назначения.

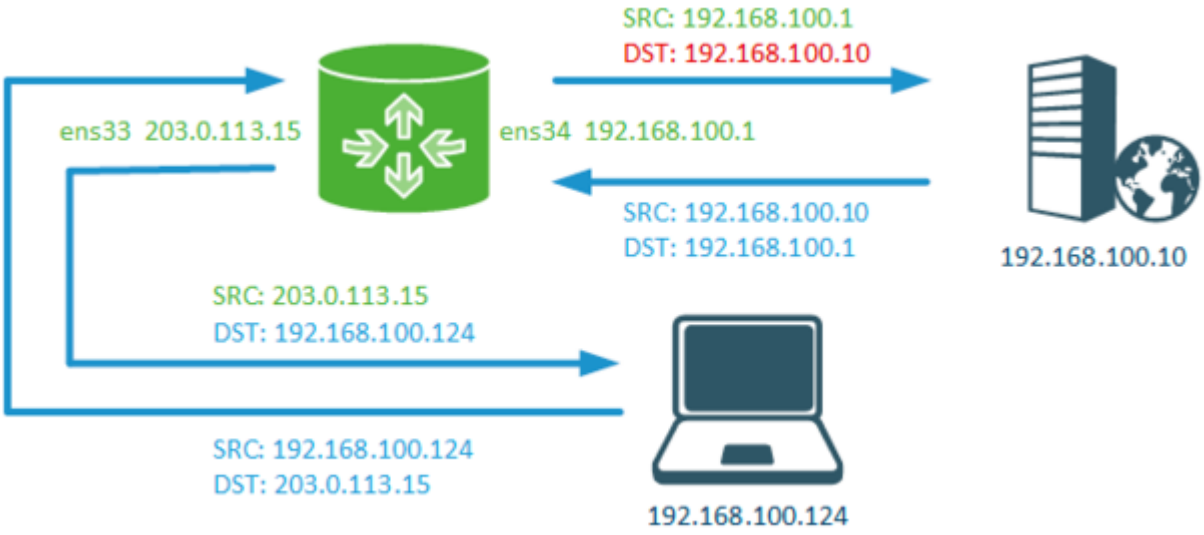
Правило **DNAT** при этом не меняется:

```
iptables -t nat -A PREROUTING -i ens35 -p tcp --dport 443 -j DNAT --to-destination 192.168.100.10
```

А вот в цепочку POSTROUTING мы добавляем следующее правило:

```
iptables -t nat -A POSTROUTING  -s 192.168.100.0/24 -d 192.168.100.10 -p tcp --dport 443 -j SNAT --to-source 192.168.100.1
```

Что оно делает? Все пакеты, проходящие через маршрутизатор и имеющие в качестве адреса источника диапазон локальной сети и предназначенные серверу 192.168.100.10 в этой же сети, будут подвергнуты преобразованию адреса источника SNAT, который будет заменен на внутренний адрес маршрутизатора.



Для обратного пакета будет выполнена автоматическая замена на основании таблицы трансляции NAT, и он будет возвращен клиенту с внешнего адреса маршрутизатора, несмотря на то что клиент находится во внутренней сети.