

МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра МО ЭВМ

ОТЧЕТ
по лабораторной работе №5
по дисциплине «Сети и телекоммуникации»
ТЕМА: ИЗУЧЕНИЕ МЕХАНИЗМОВ ТРАНСЛЯЦИИ СЕТЕВЫХ
АДРЕСОВ: NAT, MASQUERADE

Студентка гр. 2384

Соц Е.А.

Преподаватель

Борисенко К.А.

Санкт-Петербург

2024

Цель работы

Изучить механизмы преобразования сетевых адресов: NAT, Masquerade.

Задания

1. Создать три виртуальные машины (лаб. работа № 1).
2. Настроить имена, IP-адреса для каждой из подсетей в соответствии со схемой.
3. Настроить переадресацию пакетов между сетевыми интерфейсами для машины с NAT. Запретить прямой доступ между двумя частными подсетями (необходимо для воссоздания условий, приближенных к реальным).
4. Настроить Masquerade на NAT-машине и проверить доступ к сети Интернет с других машин и отсутствие доступа друг к другу.
5. Настроить доступ к сети Интернет для одной из машин с помощью sNAT.
6. Добавить вторичный IP-адрес на NAT-машину, по которому в дальнейшем будет отвечать на внешние запросы машина, указанная в п. 5.
7. Настроить dNAT для доступа к машине из внешней сети. Проверить настройки.

Выполнение работы

Инфраструктура сети представлена на рисунке 1:

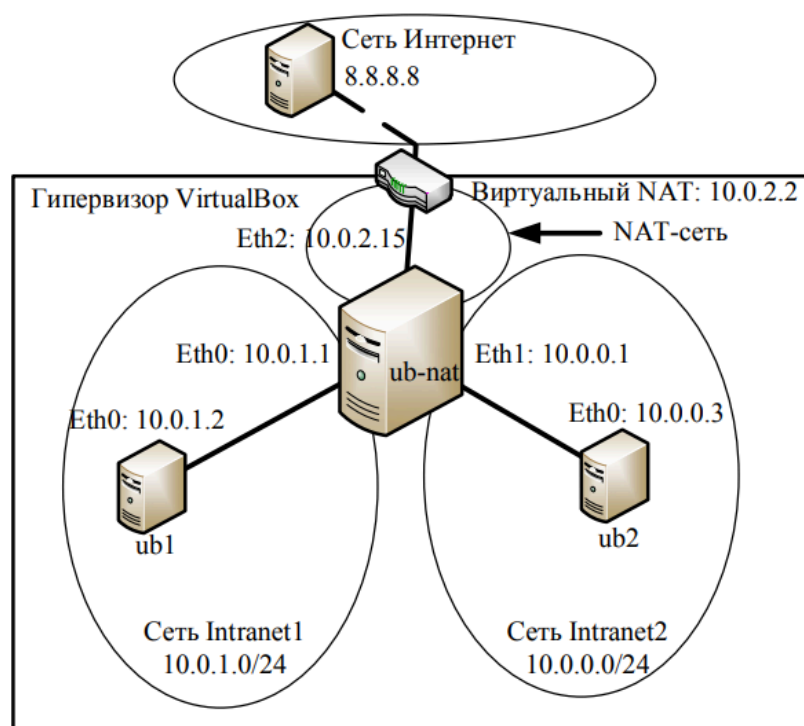


Рисунок 1 – Инфраструктура сети

Для создания данной топологии были использованы следующие типы подключения интерфейсов в VirtualBox:

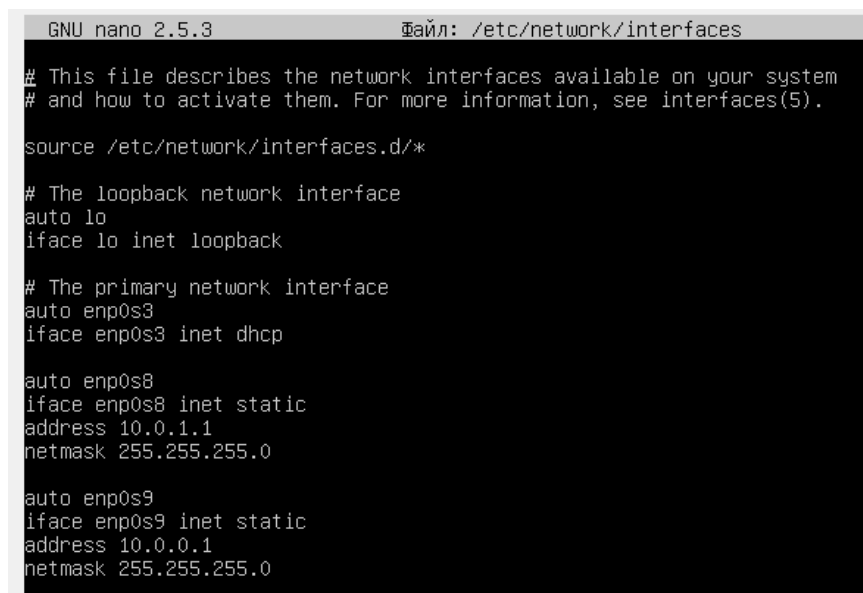
- Внутренняя сеть (Intranet1 и Intranet2). Внутренняя сеть, согласно руководству VirtualBox, является «программной сетью, которая может быть видима для выборочно установленных виртуальных машин, но не для приложений, работающих на хосте или на удаленных машинах, расположенных извне». Такая сеть представляет собой набор из хоста и нескольких виртуальных машин. Но ни одно из вышеперечисленных устройств не имеет выхода через физический сетевой адаптер – он полностью программный, используемый VirtualBox в качестве сетевого маршрутизатора. В целом получается частная локальная сеть только для гостевых операционных систем без доступа в Интернет.

- Трансляция сетевых адресов (NAT). Протокол NAT позволяет гостевой операционной системе выходить в Интернет, используя при этом

частный IP, который недоступен со стороны внешней сети или же для всех машин локальной физической сети. Такая сетевая настройка позволяет посещать web-страницы, скачивать файлы, просматривать электронную почту. И все это – используя гостевую операционную систему. Однако извне невозможно напрямую соединиться с такой системой, если она использует NAT. Можно провести аналогию с настройкой механизма sNAT, представленного ранее.

В качестве маршрутизатора будет выступать виртуальная машина «ub-nat», которая будет иметь выход в сеть Интернет посредством NAT-сети, а также подключена к двум внутренним сетям Intranet1 и Intranet2.

Для изменения настроек интерфейсов нужно использовать команду *sudo nano /etc/network/interfaces*. После изменения нужно осуществить перезагрузку интерфейсов, используя команду *sudo systemctl restart networking* и, при необходимости, перезагрузить ВМ. Команда *ifconfig* показывает настройки интерфейсов.

A screenshot of a terminal window showing the contents of the file /etc/network/interfaces. The window title is 'GNU nano 2.5.3' and the file path is '/etc/network/interfaces'. The text in the terminal is as follows:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet dhcp

auto enp0s8
iface enp0s8 inet static
address 10.0.1.1
netmask 255.255.255.0

auto enp0s9
iface enp0s9 inet static
address 10.0.0.1
netmask 255.255.255.0
```

Рисунок 2 – Добавление интерфейсов в ub-nat

```

GNU nano 2.5.3          Файл: /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
address 10.0.1.2
netmask 255.255.255.0

```

Рисунок 3 – Настройки ub1

```

GNU nano 2.5.3          Файл: /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
address 10.0.0.3
netmask 255.255.255.0

```

Рисунок 4 – Настройки ub2

Чтобы проверить доступность узлов, можно использовать команду `ping <IP>`. Результаты запросов с разных узлов приведены ниже.

```

rtt min/avg/max/mdev = 0.215/0.484/0.715/0.125 ms
katya@katyavm:~$ ping 10.0.1.2
PING 10.0.1.2 (10.0.1.2) 56(84) bytes of data.
64 bytes from 10.0.1.2: icmp_seq=1 ttl=64 time=0.237 ms
64 bytes from 10.0.1.2: icmp_seq=2 ttl=64 time=0.554 ms
64 bytes from 10.0.1.2: icmp_seq=3 ttl=64 time=0.548 ms
64 bytes from 10.0.1.2: icmp_seq=4 ttl=64 time=0.546 ms
64 bytes from 10.0.1.2: icmp_seq=5 ttl=64 time=0.540 ms
64 bytes from 10.0.1.2: icmp_seq=6 ttl=64 time=0.297 ms
64 bytes from 10.0.1.2: icmp_seq=7 ttl=64 time=0.558 ms

```

Рисунок 5 – Доступность ub1 из ub-nat

```

rtt min/avg/max/mdev = 0.221/0.433/0.884/0.183 ms
katya@katyavm:~$ ping 10.0.0.3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=64 time=0.536 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=64 time=0.512 ms
64 bytes from 10.0.0.3: icmp_seq=3 ttl=64 time=0.507 ms
64 bytes from 10.0.0.3: icmp_seq=4 ttl=64 time=0.490 ms
64 bytes from 10.0.0.3: icmp_seq=5 ttl=64 time=0.253 ms
64 bytes from 10.0.0.3: icmp_seq=6 ttl=64 time=0.280 ms

```

Рисунок 6 – Доступность ub2 из ub-nat

```

katya@katyavm:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=255 time=56.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=255 time=33.4 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=255 time=32.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=255 time=29.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=255 time=55.5 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=255 time=54.2 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=255 time=51.2 ms

```

Рисунок 7 – Доступность интернета из ub-nat

```

[-w deadline] [-W timeout] [hop1 ...] destination
katya@katyavm:~$ ping -c 2 8.8.8.8
connect: Network is unreachable
katya@katyavm:~$ ping -c 2 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.564 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.475 ms

--- 10.0.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.475/0.519/0.564/0.050 ms
katya@katyavm:~$ ping -c 2 10.0.1.2
connect: Network is unreachable
katya@katyavm:~$

```

Рисунок 8 – Доступности из ub2 (интернет недоступен)

```

katya@katyavm:~$ ping -c 2 8.8.8.8
connect: Network is unreachable
katya@katyavm:~$ ping -c 2 10.0.1.1
PING 10.0.1.1 (10.0.1.1) 56(84) bytes of data.
64 bytes from 10.0.1.1: icmp_seq=1 ttl=64 time=0.554 ms
64 bytes from 10.0.1.1: icmp_seq=2 ttl=64 time=0.595 ms

--- 10.0.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.554/0.574/0.595/0.031 ms
katya@katyavm:~$ ping -c 2 10.0.0.3
connect: Network is unreachable
katya@katyavm:~$

```

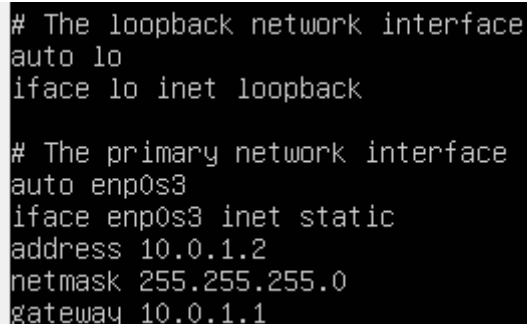
Рисунок 9 – Доступности из ub1 (интернет недоступен)

2. Необходимо настроить Masquerade на NAT-машине и проверить доступ к сети Интернет с других машин и отсутствие доступа друг к другу.

Для этого на ub-nat, используя Masquerade, была настроена таблица так, чтобы машины ub1 и ub2 имели доступ в сеть Интернет.

Для начала для ub1 и ub2 был добавлен шлюз по умолчанию на ub-nat. Таким образом виртуальные машины получили доступ к Интернету, однако так же и друг к другу. Для предотвращения последнего на машинах были введены команды для ограничения доступа соответственно:

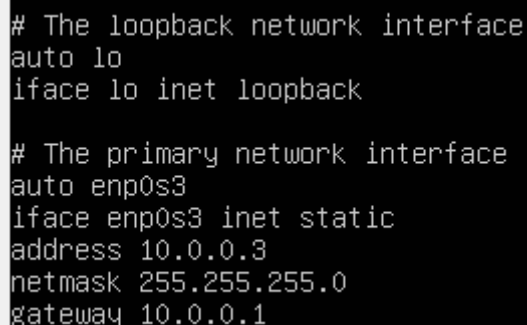
```
iptables -A OUTPUT -d 10.0.0.0/24 -j DROP
iptables -A OUTPUT -d 10.0.1.0/24 -j DROP
```

A screenshot of a terminal window showing network configuration for a virtual machine named ub1. The configuration includes the loopback interface 'lo' and the primary network interface 'enp0s3'. The 'enp0s3' interface is configured with a static IP address of 10.0.1.2, a netmask of 255.255.255.0, and a gateway of 10.0.1.1.

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
address 10.0.1.2
netmask 255.255.255.0
gateway 10.0.1.1
```

Рисунок 10 – настройка интерфейсов ub1 (добавление шлюза)

A screenshot of a terminal window showing network configuration for a virtual machine named ub2. The configuration includes the loopback interface 'lo' and the primary network interface 'enp0s3'. The 'enp0s3' interface is configured with a static IP address of 10.0.0.3, a netmask of 255.255.255.0, and a gateway of 10.0.0.1.

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
address 10.0.0.3
netmask 255.255.255.0
gateway 10.0.0.1
```

Рисунок 11 – настройка интерфейсов ub2 (добавление шлюза)

Для осуществления подмены ip-адресов источника у пакета, проходящего через ub-nat был использован механизм Masquerade. Для этого на ub-nat была прописана команда:

```
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

Данная команда меняет всем пакетам, проходящим через интерфейс enp0s3, IP-адрес источника на IP-адрес интерфейса enp0s3.

```
katya@katyavm:~$ sudo sysctl -w net.ipv4.ip_forward=1
[sudo] пароль для katya:
net.ipv4.ip_forward = 1
katya@katyavm:~$ sudo tcpdump -i enp0s3 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
00:08:58.285925 IP 10.0.1.2 > 8.8.8.8: ICMP echo request, id 1238, seq 1, length 64
00:08:58.353513 ARP, Request who-has 10.0.1.2 tell 10.0.2.2, length 46
00:08:58.357178 IP6 fe80::2 > ff02::1: ICMP6, router advertisement, length 56
00:08:59.285931 IP 10.0.1.2 > 8.8.8.8: ICMP echo request, id 1238, seq 2, length 64
00:08:59.369309 ARP, Request who-has 10.0.1.2 tell 10.0.2.2, length 46
00:09:41.500548 IP 10.0.0.3 > 8.8.8.8: ICMP echo request, id 1231, seq 1, length 64
00:09:41.662789 ARP, Request who-has 10.0.0.3 tell 10.0.2.2, length 46
00:09:42.508389 IP 10.0.0.3 > 8.8.8.8: ICMP echo request, id 1231, seq 2, length 64
00:09:42.965332 ARP, Request who-has 10.0.0.3 tell 10.0.2.2, length 46
```

Рисунок 12 – ub-nat до masquerade

```
0 packets dropped by kernel
katya@katyavm:~$ sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
katya@katyavm:~$ sudo tcpdump -i enp0s3 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
00:13:02.647469 IP 10.0.2.15 > 8.8.8.8: ICMP echo request, id 1262, seq 1, length 64
00:13:02.874038 IP 8.8.8.8 > 10.0.2.15: ICMP echo reply, id 1262, seq 1, length 64
00:13:03.648822 IP 10.0.2.15 > 8.8.8.8: ICMP echo request, id 1262, seq 2, length 64
00:13:03.756525 IP 8.8.8.8 > 10.0.2.15: ICMP echo reply, id 1262, seq 2, length 64
00:13:07.658347 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 28
00:13:07.658468 ARP, Reply 10.0.2.2 is-at 52:55:0a:00:02:02, length 50
00:13:27.935612 IP 10.0.2.15 > 8.8.8.8: ICMP echo request, id 1232, seq 1, length 64
00:13:28.030085 IP 8.8.8.8 > 10.0.2.15: ICMP echo reply, id 1232, seq 1, length 64
00:13:28.937153 IP 10.0.2.15 > 8.8.8.8: ICMP echo request, id 1232, seq 2, length 64
00:13:29.109205 IP 8.8.8.8 > 10.0.2.15: ICMP echo reply, id 1232, seq 2, length 64
00:13:32.938735 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 28
00:13:32.938863 ARP, Reply 10.0.2.2 is-at 52:55:0a:00:02:02, length 50
```

Рисунок 13 – ub-nat masquerade

Видно, что отправленные пакеты изменили адрес источника на адрес маршрутизатора 10.0.2.15.

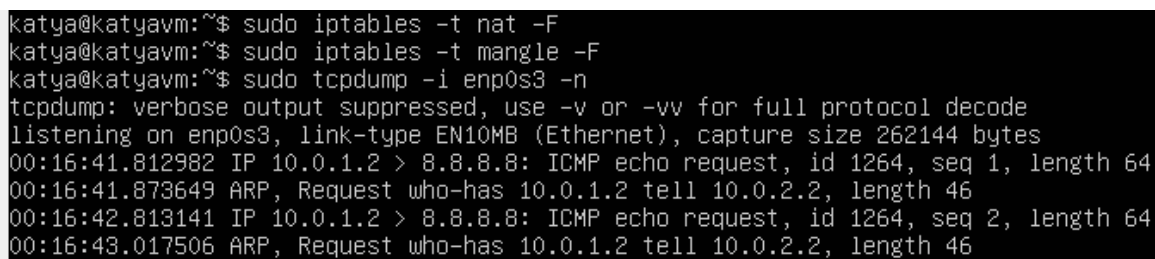
3. Необходимо настроить доступ к сети Интернет для машин с помощью sNAT.

Для этого была настроена ub-nat, используя sNAT, так, чтобы машины ub1 и ub2 имели доступ в сеть Интернет.

Будем использовать адрес 10.0.2.15 как фиксированный исходный адрес для всех пакетов, направленных в Интернет от ub1 и ub2. Введем следующую команду на ub-nat:

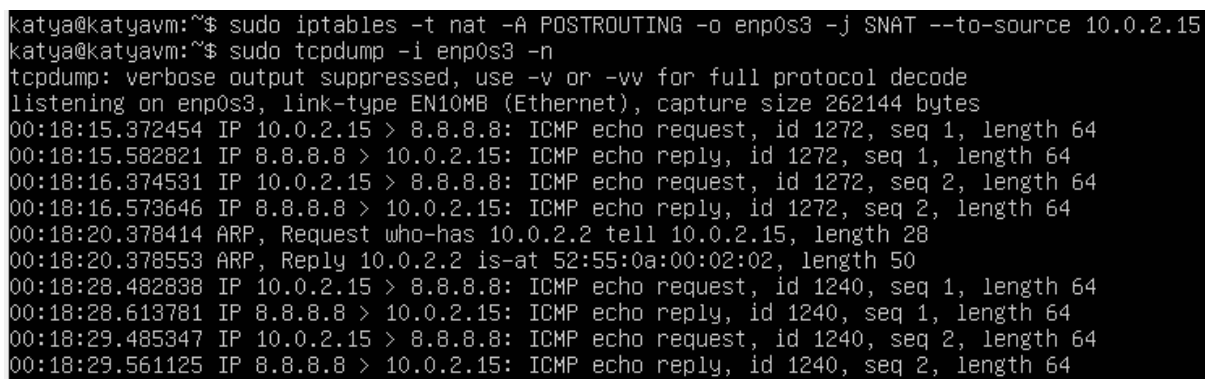

```
sudo iptables -t nat -A POSTROUTING -o enp0s3 -j SNAT
--to-source 10.0.2.15
```

Данное правило означает, что в цепочке NAT после обработки пакета для всех пакетов, отправленных на интерфейс `enp0s3`, будет происходить смена адреса источника на `10.0.2.15`. Благодаря этому правилу пакет, отправленный из частной сети, сможет дойти до необходимого узла во внешней сети и получить ответ.



```
katya@katyavm:~$ sudo iptables -t nat -F
katya@katyavm:~$ sudo iptables -t mangle -F
katya@katyavm:~$ sudo tcpdump -i enp0s3 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
00:16:41.812982 IP 10.0.1.2 > 8.8.8.8: ICMP echo request, id 1264, seq 1, length 64
00:16:41.873649 ARP, Request who-has 10.0.1.2 tell 10.0.2.2, length 46
00:16:42.813141 IP 10.0.1.2 > 8.8.8.8: ICMP echo request, id 1264, seq 2, length 64
00:16:43.017506 ARP, Request who-has 10.0.1.2 tell 10.0.2.2, length 46
```

Рисунок 14 – сброс masquerade



```
katya@katyavm:~$ sudo iptables -t nat -A POSTROUTING -o enp0s3 -j SNAT --to-source 10.0.2.15
katya@katyavm:~$ sudo tcpdump -i enp0s3 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
00:18:15.372454 IP 10.0.2.15 > 8.8.8.8: ICMP echo request, id 1272, seq 1, length 64
00:18:15.582821 IP 8.8.8.8 > 10.0.2.15: ICMP echo reply, id 1272, seq 1, length 64
00:18:16.374531 IP 10.0.2.15 > 8.8.8.8: ICMP echo request, id 1272, seq 2, length 64
00:18:16.573646 IP 8.8.8.8 > 10.0.2.15: ICMP echo reply, id 1272, seq 2, length 64
00:18:20.378414 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 28
00:18:20.378553 ARP, Reply 10.0.2.2 is-at 52:55:0a:00:02:02, length 50
00:18:28.482838 IP 10.0.2.15 > 8.8.8.8: ICMP echo request, id 1240, seq 1, length 64
00:18:28.613781 IP 8.8.8.8 > 10.0.2.15: ICMP echo reply, id 1240, seq 1, length 64
00:18:29.485347 IP 10.0.2.15 > 8.8.8.8: ICMP echo request, id 1240, seq 2, length 64
00:18:29.561125 IP 8.8.8.8 > 10.0.2.15: ICMP echo reply, id 1240, seq 2, length 64
```

Рисунок 15 – настройка и проверка SNAT

4. Необходимо настроить dNAT для доступа к машине из внешней сети.

Для выполнения нужно настроить `ub-nat`, используя dNAT, так, чтобы с машины `ub2` можно было получить доступ к `ub1`, используя IP-адрес из NAT-сети. Проверить успешность настроек можно, выполнив с узла `ub2` команду: `ssh «SecondaryNatIPAddress»`.

Создадим правило dNAT на `ub-nat` с помощью `iptables`, чтобы все входящие подключения на `ub-nat` к IP-адресу `10.0.2.100` по порту SSH (22)

перенаправлялись на ub1. Для этого будет выполнена следующая команда на ub-nat:

```
sudo iptables -t nat -A PREROUTING -d 10.0.2.100 -j DNAT --to-destination 10.0.1.2
```

Данное правило означает, что если из внешней («публичной») сети пакет будет отправлен на 10.0.2.100, то при прохождении через узел, на котором это правило настроено, произойдет подмена IP-адреса назначения, и пакет дойдет до требуемого узла в частной сети с IP-адресом 10.0.1.2.

Теперь можно протестировать подключение с ub2 к ub1 через IP-адрес 10.0.2.100:

```
katya@katyavm:~$ sudo iptables -F
katya@katyavm:~$ sudo iptables -t nat -F
katya@katyavm:~$ sudo iptables -t mangle -F
katya@katyavm:~$ sudo iptables -t nat -A PREROUTING -d 10.0.2.100 -j DNAT --to-destination 10.0.1.2
katya@katyavm:~$ sudo iptables -t nat -A POSTROUTING -d 10.0.1.2 -j MASQUERADE
katya@katyavm:~$
```

Рисунок 16 – Сброс настроек и подключение ub2 к ub1

```
katya@katyavm:~$ ssh katya@10.0.2.100
The authenticity of host '10.0.2.100 (10.0.2.100)' can't be established.
ECDSA key fingerprint is SHA256:MkZCKFBjJL18KVt+3kUCrkoeIieKqPsOLcGd6fFCmAE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.100' (ECDSA) to the list of known hosts.
katya@10.0.2.100's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-186-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Могут быть обновлены 114 пакетов.
80 обновлений касаются безопасности системы.

Last login: Tue Nov  5 00:03:27 2024
katya@katyavm:~$
```

Рисунок 17 – проверка подключения ub2 к ub1

Выводы

Были изучены механизмы преобразования сетевых адресов: NAT, Masquerade.