

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. 1381

Рымарь М.И.

Преподаватель

Фирсов М.А.

Санкт-Петербург

2023

Цель работы.

Целью работы является изучение механизмов преобразования сетевых адресов: NAT, Masquerade. Подробно рассмотрены некоторые сетевые возможности VirtualBox, который будет использован для создания необходимой инфраструктуры. Необходимо решить следующие задачи:

1. Создать три виртуальные машины.
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.

Задание.

Необходимо решить следующие задачи:

1. Создать и настроить инфраструктуру для выполнения лабораторной работы. Развернуть три виртуальные машины (лаб. работа № 1). Настроить их в соответствии с подразделом «Построение инфраструктуры для выполнения работы».
2. Настройка доступа с ub1, ub2 в сеть Интернет с использованием Masquerade. Настройте ub-nat, используя Masquerade, так, чтобы машины ub1 и ub2 имели доступ в сеть Интернет.
3. Настройка доступа с ub1, ub2 в сеть Интернет с использованием

sNAT. Настройте ub-nat, используя sNAT, так, чтобы машины ub1 и ub2 имели доступ в сеть Интернет.

4. Настройка доступа с ub2 на ub1 с использованием dNAT. Настройте 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»`.

В результате подключения будет отображено имя виртуальной машины ub1. Пример:

```
root@ub2:/home/user# ssh user@10.0.2.100
```

```
user@10.0.2.100'spassword:
```

```
user@ub1:~$
```

В данном примере вторичный IP-адрес на ub-nat настроен на интерфейсе, подключенном к NAT-сети, – IP-адрес: 10.0.2.100. При правильной настройке ssh доступ к этому IP-адресу будет открывать сессию с ub1.

Выполнение работы.

1. Создана и настроена инфраструктура сети для выполнения лабораторной работы в соответствии со схемой на рисунке 1. Заданы файлы конфигурации для всех машин (рисунки 2-4 для машин ub1, ub2, ub-nat, соответственно).

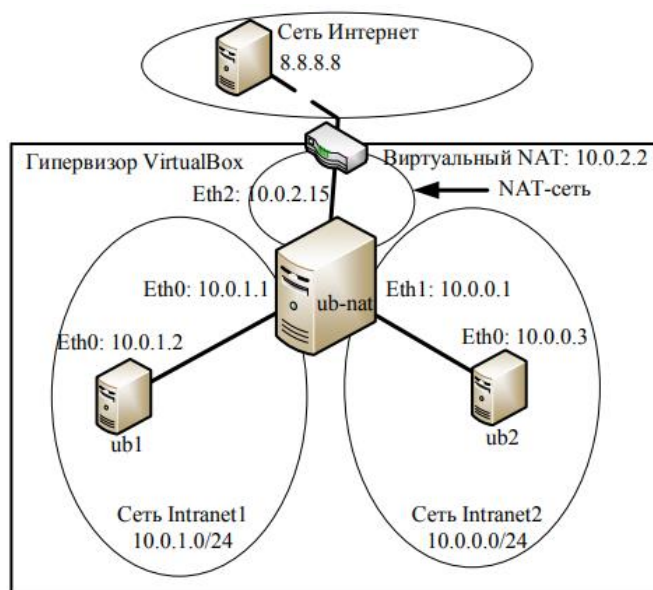


Рисунок 1 – Схема сети

С помощью iptables закроем прямой доступ для ub1 в Intranet2:

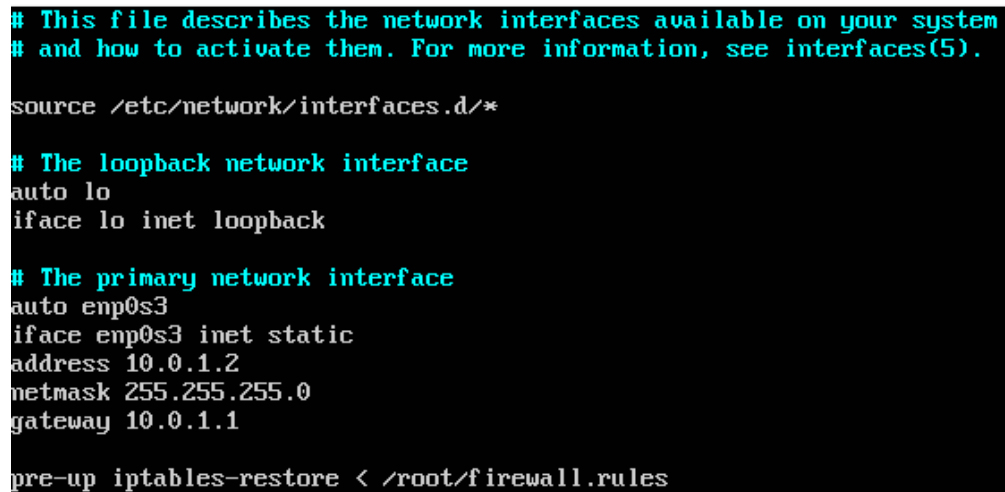
```
sudo -su root
```

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

```
iptables-save > /root/firewall.rules
```

В файл конфигураций ub1 /etc/network/interfaces добавим следующую строчку:

```
pre-up iptables-restore < /root/firewall.rules
```



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

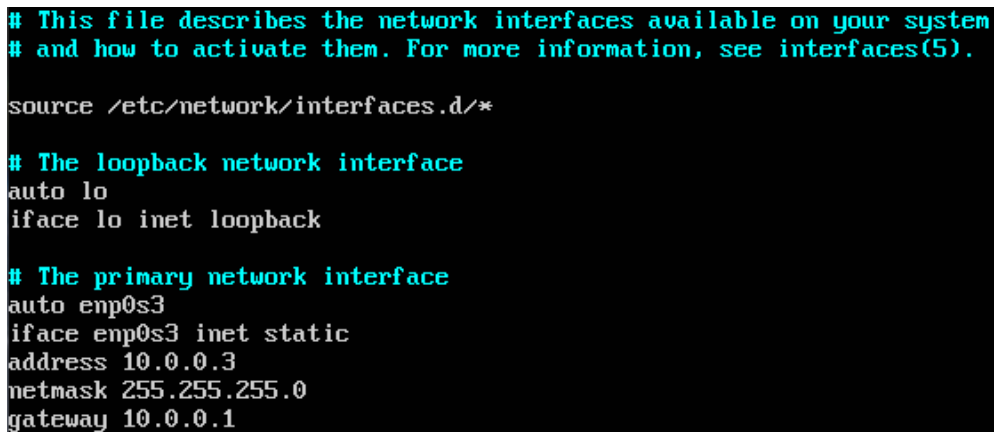
source /etc/network/interfaces.d/*

# 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
gateway 10.0.1.1

pre-up iptables-restore < /root/firewall.rules
```

Рисунок 2 – Файл конфигурации ub1



```
# 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
gateway 10.0.0.1
```

Рисунок 3 – Файл конфигурации ub2

```

# 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 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
gateway 10.0.1.1

auto enp0s3
iface enp0s3 inet dhcp
address 10.0.2.15
netmask 255.255.255.0

```

Рисунок 4 – Файл конфигурации ub-nat

На рисунке 5 показана проверка ub1 на допустимость/недопустимость к ub2, ub-nat, Google с помощью ping. На рисунке 6 показана проверка ub2 на допустимость/недопустимость к ub-nat, Google с помощью ping. На рисунке 7 показана проверка ub-nat на допустимость/недопустимость к ub1, ub2, Google с помощью ping.

```

rymar1@rymar1:~$ ping 10.0.0.3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 10.0.0.3 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2007ms

rymar1@rymar1:~$ ping 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=0.478 ms
64 bytes from 10.0.1.1: icmp_seq=2 ttl=64 time=0.533 ms
64 bytes from 10.0.1.1: icmp_seq=3 ttl=64 time=1.19 ms
^C
--- 10.0.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.478/0.733/1.190/0.324 ms
rymar1@rymar1:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4025ms

```

Рисунок 5 – Проверка соединений ub1

```

rymar2@rymar2:/etc/network$ ping 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=0.792 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.973 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.873 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=1.04 ms
64 bytes from 10.0.0.1: icmp_seq=5 ttl=64 time=1.19 ms
^C
--- 10.0.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 0.792/0.975/1.192/0.144 ms
rymar2@rymar2:/etc/network$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2015ms

```

Рисунок 6 – Проверка соединений ub2

```

rymar3@rymar3:/etc/network$ 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=0.888 ms
64 bytes from 10.0.1.2: icmp_seq=2 ttl=64 time=0.907 ms
64 bytes from 10.0.1.2: icmp_seq=3 ttl=64 time=0.972 ms
^C
--- 10.0.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.888/0.922/0.972/0.043 ms
rymar3@rymar3:/etc/network$ 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=0.443 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=64 time=0.939 ms
64 bytes from 10.0.0.3: icmp_seq=3 ttl=64 time=1.02 ms
^C
--- 10.0.0.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.443/0.801/1.021/0.255 ms
rymar3@rymar3:/etc/network$ 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=106 time=70.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=106 time=53.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=106 time=55.6 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 53.211/59.839/70.684/7.731 ms
rymar3@rymar3:/etc/network$

```

Рисунок 7 – Проверка соединений ub-nat

Был настроен доступ с ub1, ub2 в сеть Интернет с использованием Masquerade. Для этого был настроен маршрутизатор ub-nat следующим образом:

В файле /etc/sysctl.conf задали переменную net.ipv4.ip_forward = 1

В терминале:

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

Проверка доступности интернета на машинах ub1 и ub2 представлена на рисунках 8 и 9, соответственно.

```
rymar1@rymar1:~$ 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=105 time=66.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=105 time=66.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=105 time=88.6 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 66.506/73.982/88.671/10.389 ms
rymar1@rymar1:~$
```

Рисунок 8 – Проверка доступности сети Интернет с ub1

```
rymar2@rymar2:~$ 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=105 time=65.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=105 time=86.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=105 time=66.5 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 65.800/72.859/86.182/9.428 ms
rymar2@rymar2:~$
```

Рисунок 9 – Проверка доступности сети Интернет с ub2

3. Был настроен `ub-nat` с использованием `sNAT` так, чтобы машины `ub1` и `ub2` имели доступ в сеть Интернет. Для этого для начала были сброшены настройки `iptables` командами:

```
sudo iptables -F
```

```
sudo iptables -t nat -F
```

```
sudo iptables -t mangle -F
```

Далее в консоли `ub-nat` были добавлены два вторичных NAT-адреса на интерфейсе `enp0s3`. Команды показаны на рисунке 10. Также был настроен `sNAT`. Команды показаны на рисунке 11.

```

rymar3@rymar3:~$ sudo -i
root@rymar3:~# ip addr add 10.0.2.10/24 dev enp0s3
root@rymar3:~# ip addr add 10.0.2.11/24 dev enp0s3
root@rymar3:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:91:30:9f brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet 10.0.2.10/24 scope global secondary enp0s3
        valid_lft forever preferred_lft forever
    inet 10.0.2.11/24 scope global secondary enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe91:309f/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:c8:41:85 brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.1/24 brd 10.0.1.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fec8:4185/64 scope link
        valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:ee:4f:85 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.1/24 brd 10.0.0.255 scope global enp0s9
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feee:4f85/64 scope link
        valid_lft forever preferred_lft forever
root@rymar3:~# _

```

Рисунок 10 – Вторичные NAT-адреса

```

root@rymar3:~# iptables -t nat -A POSTROUTING -s 10.0.1.2/32 -o enp0s3 -j SNAT --to-source 10.0.2.10
root@rymar3:~# iptables -t nat -A POSTROUTING -s 10.0.0.3/32 -o enp0s3 -j SNAT --to-source 10.0.2.11
root@rymar3:~# _

```

Рисунок 11 – Настройка sNAT

Далее проверили доступность сети Интернет с ub1 и ub2 (показаны на рисунках 12 и 13, соответственно).

```

rymar1@rymar1:~$ 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=2 ttl=105 time=63.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=105 time=65.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=105 time=58.4 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=105 time=213 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4014ms
rtt min/avg/max/mdev = 58.454/100.136/213.254/65.356 ms
rymar1@rymar1:~$

```

Рисунок 12 – Проверка ub1


```

rymar2@rymar2:~$ 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=2 ttl=105 time=65.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=105 time=62.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=105 time=65.1 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3003ms
rtt min/avg/max/mdev = 62.669/64.514/65.729/1.342 ms
rymar2@rymar2:~$ _

```

Рисунок 13 – Проверка ub2

4. Был настроен `ub-nat` с использованием `dNAT` так, чтобы с машины `ub2` можно было получить доступ к `ub1`, используя IP-адрес из NAT-сети. Проверку успешности настроек можно, если с узла `ub2` отправить команду `ssh` “SecondaryNatIPAddress” или `ping`. На рисунке 14 показана настройка `dNAT`. На рисунке 15 показана проверка успешности настроек.

```

root@rymar3:~# sudo iptables -t nat -A PREROUTING -d 10.0.2.100 -j DNAT --to-destination 10.0.1.2
root@rymar3:~#

```

Рисунок 14 – Настройка dNAT

```

rymar2@rymar2:~$ ssh rymar1@10.0.2.10
The authenticity of host '10.0.2.10 (10.0.2.10)' can't be established.
ECDSA key fingerprint is SHA256:c01v02Ai/KkBc2DhKPuaroKK1zSheSYq81CX7IRyDBQ.
Are you sure you want to continue connecting (yes/no)? YES
Warning: Permanently added '10.0.2.10' (ECDSA) to the list of known hosts.
rymar1@10.0.2.10's password:
Permission denied, please try again.
rymar1@10.0.2.10'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

117 packages can be updated.
80 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Apr 12 17:35:20 2023
rymar1@rymar1:~$ _

```

Рисунок 15 – Проверка доступа к ub1

Выводы.

В ходе выполнения лабораторной работы были изучены механизмы преобразования сетевых адресов: NAT, Masquerade. Они были успешно использованы для создания заданной инфраструктуры в VirtualBox.