

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

ОТЧЕТ
по лабораторной работе №7
по дисциплине «Сети и телекоммуникации»
ТЕМА: СЕТЕВЫЕ ЭКРАНЫ. IPTABLES.

Студент гр.0382

Кривенцова Л.С.

Преподаватель

Фирсов М.А.

Санкт-Петербург

2022

Цель работы.

Изучение принципов работы с сетевыми экранами.

Задание.

Вариант 13.

Вариант	X	Y	Z
13	33	92	20-91

Для выполнения лабораторной необходимо настроить три виртуальных машины Ub1, Ub2 и Ub3 так, чтобы они находились в одной подсети. Кроме того, для некоторых пунктов необходимо установить дополнительные службы на виртуальные машины: apache2, ftpd и выполнить следующие задачи:

1. «Заблокировать доступ по IP-адресу ПК Ub1 к Ub3». Продemonстрировать результаты с попыткой подключения Ub1 и Ub2 к Ub3.
2. «Заблокировать доступ по порту X на Ub1». Продemonстрировать возможность доступа по ssh на Ub1 и невозможность доступа по порту X.
3. «Разрешить доступ только по ssh на Ub2». Продemonстрировать результат.
4. «Запретить icmp запросы на IP-адрес 8.8.8.8 двумя способами». Необходимо создать 2 правила: в цепочке INPUT и цепочке OUTPUT. С помощью Wireshark на хосте нужно продemonстрировать разницу в двух способах блокировки и сделать вывод о том, какой вариант эффективнее.
5. «Полностью запретить доступ к Ub3». Разрешить доступ по ICMP протоколу.
6. «Запретить подключение к Ub1 по порту Y». Настроить логирование попыток подключения по порту Y. Продemonстрировать результаты логирования.
7. «Заблокировать доступ по порту Y к Ub3 с Ub1 по его MAC-адресу». Продemonстрировать результат, сменить MAC-адрес на Ub3 и продemonстрировать успешное подключение к Ub3 по порту Y.
8. «Полностью закрыть доступ к Ub1. Разрешить доступ для Ub3 к Ub1,

используя диапазон портов Z». В результате необходимо показать невозможность подключения к порту Y и возможность к ssh или ftp.

9. «Разрешить только одно ssh подключение к Ub3». Продемонстрировать результат попытки подключения с Ub2 при наличии открытой ssh-сессии с Ub1 к Ub3.

Для проверки доступности портов можно использовать утилиту Netcat.

На проверяемой машине нужно запустить nc с ключом -l для прослушивания порта, а затем с другой машины попытаться подключиться, запустив nc с ключом -vz.

Теоретические сведения.

5 базовых цепочек:

INPUT - обрабатывает входящие пакеты и подключения. Например, если какой-либо внешний пользователь пытается подключиться к вашему компьютеру по ssh или любой веб-сайт отправит вам свой контент по запросу браузера. Все эти пакеты попадут в эту цепочку;

FORWARD - эта цепочка применяется для проходящих соединений. Сюда попадают пакеты, которые отправлены на ваш компьютер, но не предназначены ему, они просто пересылаются по сети к своей цели. Как я уже говорил, такое наблюдается на маршрутизаторах или, например, если ваш компьютер раздает wifi;

OUTPUT - эта цепочка используется для исходящих пакетов и соединений. Сюда попадают пакеты, которые были созданы при попытке выполнить ping losst.ru или когда вы запускаете браузер и пытаетесь открыть любой сайт.

PREROUTING - в эту цепочку пакет попадает перед обработкой iptables, система еще не знает куда он будет отправлен, в input, output или forward;

POSTROUTING - сюда попадают все проходящие пакеты, которые уже прошли цепочку FORWARD.

Таблицы iptables:

1. **raw** – просматривается до передачи пакета системе определения состояний. Используется редко, например, для маркировки пакетов, которые НЕ должны обрабатываться системой определения состояний. Для этого в правиле указывается действие NOTRACK. Содержит цепочки PREROUTING и OUTPUT.

2. **mangle** – содержит правила модификации (обычно заголовка) IP-пакетов. Среди прочего поддерживает действия TTL (Time to Live), TOS (Type of Service) и MARK (для изменения полей TTL и TOS и для изменения маркеров пакета). Содержит все пять стандартных цепочек.

3. **nat** – просматривает только пакеты, создающие новое соединение (согласно системе определения состояний). Поддерживает действия DNAT, SNAT, MASQUERADE, REDIRECT. Содержит цепочки PREROUTING, OUTPUT и POSTROUTING.

4. **filter** – основная таблица, используется по умолчанию, если название таблицы не указано. Содержит цепочки INPUT, FORWARD и OUTPUT.

Правила:

ACCEPT - разрешить прохождение пакета дальше по цепочке правил;

DROP - удалить пакет;

REJECT - отклонить пакет, отправителю будет отправлено сообщение, что пакет был отклонен;

LOG - сделать запись о пакете в лог файл;

QUEUE - отправить пакет пользовательскому приложению.

Основные действия, которые позволяет выполнить iptables:

-A - добавить правило в цепочку;

-C - проверить все правила;

-D - удалить правило;

-I - вставить правило с нужным номером;

-L - вывести все правила в текущей цепочке;

-S - вывести все правила;

- F - очистить все правила;
- N - создать цепочку;
- X - удалить цепочку;
- P - установить действие по умолчанию.

Дополнительные опции для правил:

- p - указать протокол, один из tcp, udp, udplite, icmp, icmpv6, esp, ah, sctp, mh;
- s - указать ip адрес устройства-отправителя пакета;
- d - указать ip адрес получателя;
- i - входной сетевой интерфейс;
- o - исходящий сетевой интерфейс;
- j - выбрать действие, если правило подошло.

Обычно команда имеет такой общий вид:

```
$ iptables -t <таблица> <действие> <цепочка>
<дополнительные_параметры>
```

Выполнение работы.

Конфигурация сети:

Настройки узла Ub1:

```
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
```

Настройки узла Ub2:

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

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

auto enp0s8
iface enp0s8 inet static
address 10.0.0.1
netmask 255.255.255.0
```

Настройки узла Ub3:

```
# 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
~
~
```

Данная конфигурация обеспечивает связь всех устройств сети.

1. Заблокировать доступ по IP-адресу Ubu1 к Ubu3.

Для выполнения задания на Ubu1 выполняется команда:

```
iptables -A OUTPUT -d 10.0.0.3 -j DROP
```

Запрос с Ubu1 на Ubu3 до настройки:

```
lyubava@ubuntu:~$ 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=0.564 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=64 time=0.817 ms
64 bytes from 10.0.0.3: icmp_seq=3 ttl=64 time=0.502 ms
64 bytes from 10.0.0.3: icmp_seq=4 ttl=64 time=0.574 ms
64 bytes from 10.0.0.3: icmp_seq=5 ttl=64 time=0.579 ms
64 bytes from 10.0.0.3: icmp_seq=6 ttl=64 time=0.670 ms
^C
--- 10.0.0.3 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5003ms
rtt min/avg/max/mdev = 0.502/0.617/0.817/0.105 ms
lyubava@ubuntu:~$ _
```

Запрос с Ubu1 на Ubu3 после настройки:

```

lyubava@ubuntu:~$ sudo iptables -A OUTPUT -d 10.0.0.3 -j DROP
[sudo] пароль для lyubava:
lyubava@ubuntu:~$ 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
ping: sendmsg: Operation not permitted
^C
--- 10.0.0.3 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3025ms
lyubava@ubuntu:~$

```

Сигнал не посылается на Ubu3.

Запрос с Ubu2 на Ubu3 после настройки:

```

lyubava@ubuntu:~$ 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=1.07 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=64 time=0.857 ms
64 bytes from 10.0.0.3: icmp_seq=3 ttl=64 time=0.937 ms
64 bytes from 10.0.0.3: icmp_seq=4 ttl=64 time=0.970 ms
^C
--- 10.0.0.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.857/0.958/1.071/0.085 ms
lyubava@ubuntu:~$

```

При отправке сигнала с Ubu3 на Ubu1 ответ не придет.

После каждого задания выполняется команда `iptables -F`, и правила сбрасываются:

```
iptables -F
```

2. «Заблокировать доступ по порту 33 на Ubu1». Продемонстрировать возможность доступа по ssh на Ubu1 и невозможность доступа по порту 33.

Для выполнения задания на Ubu1 выполняется команда:

`iptables -A INPUT -p tcp --dport 33 -j DROP:`

```

lyubava@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 33 -j DROP
lyubava@ubuntu:~$ sudo su
root@ubuntu:/home/lyubava# iptables -nvl
Chain INPUT (policy ACCEPT 320 packets, 23680 bytes)
 pkts bytes target    prot opt in     out     source                   destination
    0      0 DROP      tcp  --  *      *       0.0.0.0/0                0.0.0.0/0                tcp dpt:33
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
Chain OUTPUT (policy ACCEPT 320 packets, 23680 bytes)
 pkts bytes target    prot opt in     out     source                   destination
    4    336 DROP      all  --  *      *       0.0.0.0/0                10.0.0.3
    0      0 DROP      all  --  *      *       0.0.0.0/0                10.0.0.3
root@ubuntu:/home/lyubava#

```

Ssh-соединение ubu3 к ubu1 по порту 22 после настройки:

```
lyubava@ubuntu:~$ ssh 10.0.1.2
The authenticity of host '10.0.1.2 (10.0.1.2)' can't be established.
ECDSA key fingerprint is SHA256:ga1adLcSF9T0CrWycv17GQDKIXCjALB2yqx324sbyAw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.2' (ECDSA) to the list of known hosts.
lyubava@10.0.1.2'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 113 пакетов.
80 обновлений касаются безопасности системы.

Last login: Sat Apr 30 20:08:16 2022
```

Отсутствие ssh-соединения ubu3 с ubu1 по порту 33 после настройки:

```
lyubava@ubuntu:~$ nc -vz 10.0.1.2 33
nc: connect to 10.0.1.2 port 33 (tcp) failed: Connection timed out
```

3. «Разрешить доступ только по ssh на Ub2». Продемонстрировать результат.

Для выполнения этой задачи требуется выполнить следующие команды на Ubu2:

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -j DROP
```

```
root@ubuntu:/home/lyubava# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
root@ubuntu:/home/lyubava# iptables -A INPUT -j DROP
```

Результат ip-запроса к Ubu2 с Ubu1 и результат подключения Ubu1 к Ubu2 по ssh-соединению по порту 22:


```

lyubava@ubuntu:~$ ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
^C
--- 10.0.0.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2000ms

lyubava@ubuntu:~$ ssh lyubava@10.0.0.1
The authenticity of host '10.0.0.1 (10.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:ga1adLcSF9T0CrWycv17GQDKIXCjALB2yqx324sbyAw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.0.1' (ECDSA) to the list of known hosts.
lyubava@10.0.0.1'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 113 пакетов.
30 обновлений касаются безопасности системы.

Last login: Wed May 25 17:07:35 2022 from 10.0.1.2
lyubava@ubuntu:~$

```

4. «Запретить icmp запросы на IP-адрес 8.8.8.8 двумя способами». Необходимо создать 2 правила: в цепочке INPUT и цепочке OUTPUT. Продемонстрировать разницу в двух способах блокировки и сделать вывод о том, какой вариант эффективнее.

1) Создадим на Ubu1 запрещающее правило в INPUT.

`iptables -A INPUT -s 8.8.8.8 -j DROP`

Тогда устройство тратит ресурсы на создание соединения, отправку сигнала, а когда приходит ответ, сбрасывает его.

```

RX packets:240 errors:0 dropped:0 overruns:0 frame:0
TX packets:240 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:19120 (19.1 KB) TX bytes:19120 (19.1 KB)

lyubava@ubuntu:~$ sudo iptables -A INPUT -p icmp -s 8.8.8.8 -j DROP
sudo: пароль для lyubava:
ad argument 'enp0s3'
ly 'iptables -h' or 'iptables --help' for more information.
lyubava@ubuntu:~$ sudo iptables -A INPUT -p icmp -i enp0s3 -j DROP
lyubava@ubuntu:~$ 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 ---
12 packets transmitted, 0 received, 100% packet loss, time 111460ms

lyubava@ubuntu:~$ _

lyubava@ubuntu:~$ sudo tcpdump -p icmp -i enp0s3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
10:10:48.961270 IP 10.0.1.2 > 8.8.8.8: ICMP echo request, id 1309, seq 1, length 64
10:10:48.961626 IP 10.0.1.1 > 10.0.1.2: ICMP net 8.8.8.8 unreachable, length 92
10:10:48.961371 IP 10.0.1.2 > 8.8.8.8: ICMP echo request, id 1309, seq 2, length 64
10:10:48.961764 IP 10.0.1.1 > 10.0.1.2: ICMP net 8.8.8.8 unreachable, length 92
10:10:50.961101 IP 10.0.1.2 > 8.8.8.8: ICMP echo request, id 1309, seq 3, length 64
10:10:50.961761 IP 10.0.1.1 > 10.0.1.2: ICMP net 8.8.8.8 unreachable, length 92
10:10:51.961481 IP 10.0.1.2 > 8.8.8.8: ICMP echo request, id 1309, seq 4, length 64
10:10:51.962144 IP 10.0.1.1 > 10.0.1.2: ICMP net 8.8.8.8 unreachable, length 92
10:10:52.960996 IP 10.0.1.2 > 8.8.8.8: ICMP echo request, id 1309, seq 5, length 64
10:10:53.961146 IP 10.0.1.2 > 8.8.8.8: ICMP echo request, id 1309, seq 6, length 64
10:10:54.960860 IP 10.0.1.2 > 8.8.8.8: ICMP echo request, id 1309, seq 7, length 64
10:10:55.961170 IP 10.0.1.2 > 8.8.8.8: ICMP echo request, id 1309, seq 8, length 64
^C
12 packets captured
12 packets received by filter
0 packets dropped by kernel
lyubava@ubuntu:~$

```

2) Создадим на Ubu1 запрещающее правило в OUTPUT.

`iptables -A OUTPUT -d 8.8.8.8 -j DROP`

Устройство сразу видит в таблице правил, что сообщение с данным адресом запрещено, не формирует соединение и не разрешает связь. Этот способ эффективнее (не тратятся ресурсы устройства).

Трафик на enp0s3 интерфейсе Ubu1 после настройки правил:

```
root@ubuntu:/home/lyubava# sudo iptables -A OUTPUT -p icmp -o enp0s3 -j DROP
root@ubuntu:/home/lyubava# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 8.8.8.8 ping statistics ---
0 packets transmitted, 0 received, 100% packet loss, time 7025ms
root@ubuntu:/home/lyubava#
```

```
18:11:28.587655 IP 10.0.1.1.53654 > 10.0.1.2:SSH: Flags [I], ack 1772872, win 290
TS val 1129379 ecr 97966, nop, nop, sack 1 ([1772772:1772872]), length 0
18:11:28.607588 IP 10.0.1.1.53654 > 10.0.1.2:ssh: Flags [P.], seq 289:325, ack 17
tions [nop,nop,TS val 1129384 ecr 97966], length 36
^C
1501 packets captured
1737 packets received by filter
136 packets dropped by kernel
root@ubuntu:/home/lyubava# ^C
root@ubuntu:/home/lyubava# ^C
root@ubuntu:/home/lyubava# ^C
root@ubuntu:/home/lyubava# tcpdump -p icmp -i enp0s3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

5. «Полностью запретить доступ к Ub3». Разрешить доступ по ICMP протоколу.

Для выполнения этой задачи требуется выполнить следующие команды на Ubu3:

```
root@ubuntu:/home/lyubava# sudo iptables -A INPUT -p icmp -j ACCEPT
root@ubuntu:/home/lyubava# sudo iptables -A INPUT -j DROP
root@ubuntu:/home/lyubava#
```

Доступ с Ubu1 по ICMP и отсутствие доступа по ssh на Ubu3:

```
root@ubuntu:/home/lyubava# 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=63 time=1.10 ms
64 bytes from 10.0.0.3: icmp_seq=2 ttl=63 time=0.804 ms
64 bytes from 10.0.0.3: icmp_seq=3 ttl=63 time=1.34 ms
64 bytes from 10.0.0.3: icmp_seq=4 ttl=63 time=0.778 ms
^C
--- 10.0.0.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.778/1.007/1.346/0.235 ms
root@ubuntu:/home/lyubava# ssh lyubava@10.0.0.3
_
```

6. «Запретить подключение к Ub1 по порту 92». Настроить логирование попыток подключения по порту 92. Продемонстрировать результаты логирования.

Для выполнения этой задачи требуется выполнить следующие команды на Ubu1:

```
root@ubuntu:/home/lyubava# sudo iptables -A INPUT -p tcp --dport 92 -j LOG --log-prefix "Logging in"
root@ubuntu:/home/lyubava# sudo iptables -A INPUT -p tcp --dport 92 -j DROP
```

Отсутствие ssh соединения Ubu2 к Ubu1 по порту 92:

```
lyubava@ubuntu:~$ ssh lyubava@10.0.1.2 -p 92
^C
lyubava@ubuntu:~$
```

Отсутствие ssh соединения Ubu3 к Ubu1 по порту 92:

```
@root@ubuntu:/home/lyubava# ssh lyubava@10.0.1.2 -p 92
^C
root@ubuntu:/home/lyubava# _
```

Запись о событиях в лог файле /var/log/syslog Ubu1:

```
00:00:00:08:00 SRC=10.0.1.2 DST=10.0.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=24073 DF PROTO=TCP SPT=
59110 DPT=92 WINDOW=43690 RES=0x00 SYN URG=0
May 25 18:24:27 ubuntu kernel: [ 1471.335882] Logging infoIN=lo OUT= MAC=00:00:00:00:00:00:00:00:
00:00:00:08:00 SRC=10.0.1.2 DST=10.0.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=24074 DF PROTO=TCP SPT=
59110 DPT=92 WINDOW=43690 RES=0x00 SYN URG=0
May 25 18:24:44 ubuntu kernel: [ 1487.367593] Logging infoIN=lo OUT= MAC=00:00:00:00:00:00:00:00:
00:00:00:08:00 SRC=10.0.1.2 DST=10.0.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=24075 DF PROTO=TCP SPT=
59110 DPT=92 WINDOW=43690 RES=0x00 SYN URG=0
May 25 18:27:07 ubuntu systemd[1]: Started Session 4 of user lyubava.
May 25 18:28:07 ubuntu kernel: [ 1691.260458] Logging infoIN=enp0s3 OUT= MAC=08:00:27:70:07:7d:08:00
:27:d0:3e:88:08:00 SRC=10.0.1.1 DST=10.0.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=61396 DF PROTO=TCP
SPT=36798 DPT=92 WINDOW=29200 RES=0x00 SYN URG=0
May 25 18:28:08 ubuntu kernel: [ 1692.259569] Logging infoIN=enp0s3 OUT= MAC=08:00:27:70:07:7d:08:00
:27:d0:3e:88:08:00 SRC=10.0.1.1 DST=10.0.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=61397 DF PROTO=TCP
SPT=36798 DPT=92 WINDOW=29200 RES=0x00 SYN URG=0
May 25 18:28:10 ubuntu kernel: [ 1694.264577] Logging infoIN=enp0s3 OUT= MAC=08:00:27:70:07:7d:08:00
:27:d0:3e:88:08:00 SRC=10.0.1.1 DST=10.0.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=61398 DF PROTO=TCP
SPT=36798 DPT=92 WINDOW=29200 RES=0x00 SYN URG=0
May 25 18:28:14 ubuntu kernel: [ 1698.271014] Logging infoIN=enp0s3 OUT= MAC=08:00:27:70:07:7d:08:00
:27:d0:3e:88:08:00 SRC=10.0.1.1 DST=10.0.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=61399 DF PROTO=TCP
SPT=36798 DPT=92 WINDOW=29200 RES=0x00 SYN URG=0
May 25 18:28:50 ubuntu kernel: [ 1733.931424] Logging infoIN=enp0s3 OUT= MAC=08:00:27:70:07:7d:08:00
:27:d0:3e:88:08:00 SRC=10.0.0.3 DST=10.0.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=53567 DF PROTO=TCP
SPT=46100 DPT=92 WINDOW=29200 RES=0x00 SYN URG=0
May 25 18:28:51 ubuntu kernel: [ 1734.930643] Logging infoIN=enp0s3 OUT= MAC=08:00:27:70:07:7d:08:00
:27:d0:3e:88:08:00 SRC=10.0.0.3 DST=10.0.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=53568 DF PROTO=TCP
SPT=46100 DPT=92 WINDOW=29200 RES=0x00 SYN URG=0
May 25 18:28:53 ubuntu kernel: [ 1736.934038] Logging infoIN=enp0s3 OUT= MAC=08:00:27:70:07:7d:08:00
:27:d0:3e:88:08:00 SRC=10.0.0.3 DST=10.0.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=53569 DF PROTO=TCP
SPT=46100 DPT=92 WINDOW=29200 RES=0x00 SYN URG=0
May 25 18:28:57 ubuntu kernel: [ 1740.938406] Logging infoIN=enp0s3 OUT= MAC=08:00:27:70:07:7d:08:00
:27:d0:3e:88:08:00 SRC=10.0.0.3 DST=10.0.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=53570 DF PROTO=TCP
SPT=46100 DPT=92 WINDOW=29200 RES=0x00 SYN URG=0
May 25 18:29:05 ubuntu kernel: [ 1748.953827] Logging infoIN=enp0s3 OUT= MAC=08:00:27:70:07:7d:08:00
:27:d0:3e:88:08:00 SRC=10.0.0.3 DST=10.0.1.2 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=53571 DF PROTO=TCP
SPT=46100 DPT=92 WINDOW=29200 RES=0x00 SYN URG=0
root@ubuntu:/home/lyubava#
```

7. «Заблокировать доступ по порту 92 к Ub3 с Ub1 по его MAC-адресу».

Продемонстрировать результат, сменить MAC-адрес на Ub1 и продемонстрировать успешное подключение к Ub3 по порту 92.

Mac-адрес Ubu1:

```
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:70:07:7d  
          inet addr:10.0.1.2  Bcast:10.0.1.255  Mask:255.255.25
```

Ssh соединение Ubu1 к Ubu3 по порту 92 перед настройкой:

```
root@ubuntu:/home/lyubava# ssh lyubava@10.0.0.3 -p 92  
The authenticity of host '[10.0.0.3]:92 ([10.0.0.3]:92)' can't be established.  
ECDSA key fingerprint is SHA256:ga1adLcSF9T0CrWycv17GQDKIXCjALB2yqx324sbyAw.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '[10.0.0.3]:92' (ECDSA) to the list of known hosts.  
lyubava@10.0.0.3'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 113 пакетов.  
80 обновлений касаются безопасности системы.  
  
Last login: Wed May 25 19:32:45 2022  
lyubava@ubuntu:~$ ip route  
default via 10.0.0.1 dev enp0s3 onlink  
10.0.0.0/24 dev enp0s3 proto kernel scope link src 10.0.0.3  
lyubava@ubuntu:~$
```

Для выполнения этой задачи требуется выполнить следующие команды на Ubu3:

```
root@ubuntu:/home/lyubava# sudo iptables -A INPUT -p tcp --dport 92 -m mac --mac-source 08:00:27:70:07:7d -j DROP  
root@ubuntu:/home/lyubava#
```

Отсутствие ssh соединения Ubu1 к Ubu3 по порту 92 после настройки:

```
root@ubuntu:/home/lyubava# nc -v -z 10.0.0.3 92  
nc: connect to 10.0.0.3 port 92 (tcp) failed: Connection refused  
root@ubuntu:/home/lyubava#
```

```
lyubava@ubuntu:~$ ssh lyubava@10.0.0.3 -p 92
```

Ssh соединение Ubu2 к Ubu3 по порту 92 после настройки:

```

lyubava@ubuntu:~$ ssh lyubava@10.0.0.3 -p 92
The authenticity of host '[10.0.0.3]:92 ([10.0.0.3]:92)' can't be established.
ECDSA key fingerprint is SHA256:ga1adLcSF9T0CrWycv17GQDKIXCjALB2yqx324sbyAw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.0.0.3]:92' (ECDSA) to the list of known hosts.
lyubava@10.0.0.3'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 113 пакетов.
80 обновлений касаются безопасности системы.

Last login: Wed May 25 19:33:35 2022 from 10.0.0.3
lyubava@ubuntu:~$ ip route
default via 10.0.0.1 dev enp0s3 onlink
10.0.0.0/24 dev enp0s3 proto kernel scope link src 10.0.0.3
lyubava@ubuntu:~$

```

С помощью VirtualBox был сгенерирован новый mac-адрес для Ub1:

```

ubuntu:~$ ifconfig
Link encap:Ethernet HWaddr 06:00:27:70:07:7d
inet addr:10.0.1.2 Bcast:10.0.1.255 Mask:255.255.

```

Ssh соединение Ubu1 к Ubu3 по порту 92 после настройки и смены mac-адреса:

```

root@ubuntu:/home/lyubava# ssh lyubava@10.0.0.3 -p 92
The authenticity of host '[10.0.0.3]:92 ([10.0.0.3]:92)' can't be established.
ECDSA key fingerprint is SHA256:ga1adLcSF9T0CrWycv17GQDKIXCjALB2yqx324sbyAw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.0.0.3]:92' (ECDSA) to the list of known hosts.
lyubava@10.0.0.3'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 113 пакетов.
80 обновлений касаются безопасности системы.

Last login: Wed May 25 19:32:45 2022
lyubava@ubuntu:~$ ip route
default via 10.0.0.1 dev enp0s3 onlink
10.0.0.0/24 dev enp0s3 proto kernel scope link src 10.0.0.3

```

8. «Полностью закрыть доступ к Ub1. Разрешить доступ для Ub3 к Ub1, используя диапазон портов 20-91». В результате необходимо показать невозможность подключения к порту 92 и возможность к ssh.

Для выполнения этой задачи требуется выполнить следующие команды на Ubu1:

```

root@ubuntu:/home/lyubava# sudo iptables -A INPUT -j DROP
root@ubuntu:/home/lyubava# sudo iptables -I INPUT 1 -s 10.0.0.3 -p tcp --dport 20:91 -j ACCEPT

```

Отсутствие возможности icmp запроса от Ubu3 к Ubu1. Отсутствие ssh соединения Ubu3 к Ubu1 по порту 92:

```
lyubava@ubuntu:~$ ping 10.0.1.2
PING 10.0.1.2 (10.0.1.2) 56(84) bytes of data.
^C
--- 10.0.1.2 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1007ms

lyubava@ubuntu:~$ ssh lyubava@10.0.1.2 -p 92
```

Ssh соединение Ubu3 с Ubu1 по порту 22 (из разрешенного диапазона):

```
lyubava@ubuntu:~$ ssh lyubava@10.0.1.2 -p 22
The authenticity of host '10.0.1.2 (10.0.1.2)' can't be established.
ECDSA key fingerprint is SHA256:ga1adLcSF9T0CrWycv17GQDKIXCjALB2yqx324sbyAw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.1.2' (ECDSA) to the list of known hosts.
lyubava@10.0.1.2'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 113 пакетов.
80 обновлений касаются безопасности системы.

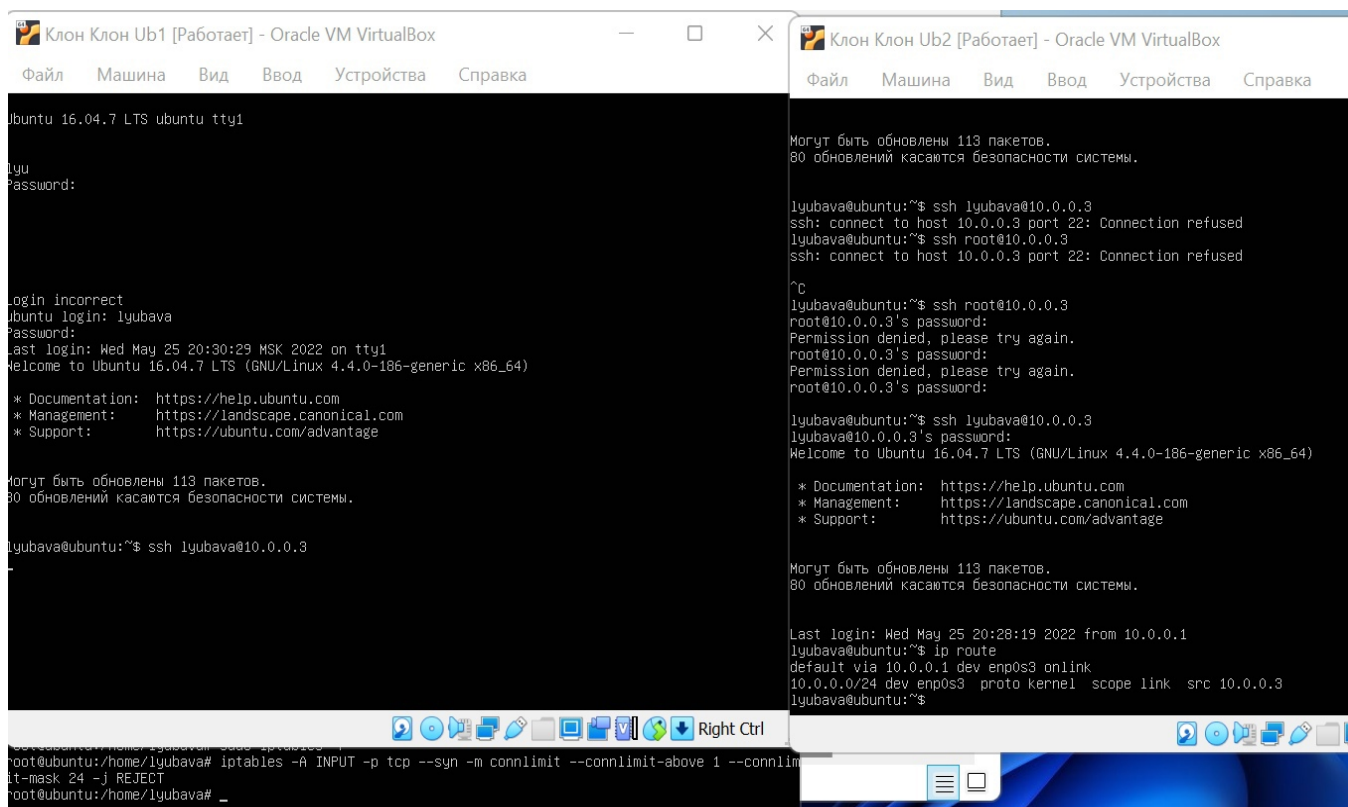
Last login: Wed May 25 19:38:26 2022
lyubava@ubuntu:~$ ip route
default via 10.0.1.1 dev enp0s3 onlink
10.0.1.0/24 dev enp0s3 proto kernel scope link src 10.0.1.2
lyubava@ubuntu:~$
```

9. «Разрешить только одно ssh подключение к Ub3». Продемонстрировать результат попытки подключения с Ub2 при наличии открытой ssh-сессии с Ub1 к Ub3.

Для выполнения этой задачи требуется выполнить следующую команду на Ubu3:

```
lyubava@ubuntu:~$ sudo iptables -A INPUT -p tcp --syn -m connlimit --connlimit-above 1 --connlimit-max 24 -j REJECT
[sudo] пароль для lyubava:
lyubava@ubuntu:~$ _
```

Возможность только одного ssh подключения при соединении к Ub3:



```
Клон Клон Ub1 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

ubuntu 16.04.7 LTS ubuntu tty1

lyu
Password:

Login incorrect
ubuntu login: lyubava
Password:
Last login: Wed May 25 20:30:29 MSK 2022 on tty1
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 113 пакетов.
80 обновлений касаются безопасности системы.

lyubava@ubuntu:~$ ssh lyubava@10.0.0.3
-

Клон Клон Ub2 [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Могут быть обновлены 113 пакетов.
80 обновлений касаются безопасности системы.

lyubava@ubuntu:~$ ssh lyubava@10.0.0.3
ssh: connect to host 10.0.0.3 port 22: Connection refused
lyubava@ubuntu:~$ ssh root@10.0.0.3
ssh: connect to host 10.0.0.3 port 22: Connection refused
^C
lyubava@ubuntu:~$ ssh root@10.0.0.3
root@10.0.0.3's password:
Permission denied, please try again.
root@10.0.0.3's password:
Permission denied, please try again.
root@10.0.0.3's password:
lyubava@ubuntu:~$ ssh lyubava@10.0.0.3
lyubava@10.0.0.3'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 113 пакетов.
80 обновлений касаются безопасности системы.

Last login: Wed May 25 20:28:19 2022 from 10.0.0.1
lyubava@ubuntu:~$ ip route
default via 10.0.0.1 dev enp0s3 onlink
10.0.0.0/24 dev enp0s3 proto kernel scope link src 10.0.0.3
lyubava@ubuntu:~$
```

Выводы.

Были изучены принципы работы с сетевыми экранами.