

**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. 1384

Усачева Д.В.

Преподаватель

Ефремов М. А.

Санкт-Петербург

2023

### **Цель работы.**

Целью работы является изучение принципов работы с сетевыми экранами.

Необходимо решить следующие задачи:

1. Создать три виртуальные машины (лаб. работа No 3).
2. Научиться блокировать и разрешать прием и отправку пакетов с помощью iptables, настраивать логирование событий.

### **Задание.**

Для выполнения лабораторной работы необходимо настроить три виртуальные 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. Продемонстрировать результаты с попыткой подключения Ub1 и Ub2 Ub3.
2. Заблокировать доступ по 21-му порту на Ub1. Продемонстрировать возможность доступа по ssh на Ub1 и невозможность доступа по 21-му порту.
3. Разрешить доступ только по ssh на Ub2. Предоставить результат.
4. Запретить ICMP-запросы на IP-адрес 8.8.8.8 двумя способами. Необходимо создать два правила: в цепочке INPUT и цепочке OUTPUT. С помощью Wireshark на хосте нужно продемонстрировать разницу между двумя способами 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 80. Настроить логирование попыток подключения по порту 80. Продемонстрировать результаты логирования.

7. Заблокировать доступ по 80-му порту к Ub3 с Ub1 по его MAC-адресу. Продemonстрировать результат, сменить MAC-адрес на Ub3 и продемонстрировать успешное подключение к Ub3 по 80-му порту.

8. Полностью закрыть доступ к Ub1. Разрешить доступ для Ub3 к Ub1, используя диапазон портов 20-79. В результате необходимо показать невозможность подключения к порту 80 и возможность – к ssh или ftp.

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

### **Выполнение работы.**

1. Были развернуты 3 виртуальные машины, находящиеся в одной подсети:

1. Ub1, ip 172.20.10.4, netmask 255.255.255.240
2. Ub2, ip 172.20.10.5, netmask 255.255.255.240
3. Ub3, ip 172.20.10.3, netmask 255.255.255.240

Заблокируем доступ по IP Ub1 к Ub3:

```
dari@dari:~$ sudo iptables -A INPUT -s 172.20.10.4 -j DROP
[sudo] password for dari:
dari@dari:~$ sudo iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source         destination
    0    0 DROP      all  --  *      *       172.20.10.4    0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source         destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source         destination
```

Рисунок 1 — Настройка iptables Ub3

```
dari@dari:~$ ping 172.20.10.3
PING 172.20.10.3 (172.20.10.3) 56(84) bytes of data.
^C
--- 172.20.10.3 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2016ms
```

Рисунок 2 — ping с Ub1 на Ub3

```

dari@dari:~$ ping 172.20.10.3
PING 172.20.10.3 (172.20.10.3) 56(84) bytes of data.
64 bytes from 172.20.10.3: icmp_seq=1 ttl=64 time=2.53 ms
64 bytes from 172.20.10.3: icmp_seq=2 ttl=64 time=0.814 ms
^C
--- 172.20.10.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1004ms
rtt min/avg/max/mdev = 0.814/1.673/2.533/0.860 ms

```

Рисунок 3 — ping с Ub2 на Ub3

2. Настроим сетевой экран на Ub1, чтобы никто из подсети не имел доступа по 21-ому порту. Проверим доступ к Ub1 через 22 порт(ssh) и отсутствие доступа по 21-ому порту с помощью команды telnet.

```

dari@dari:~$ sudo iptables -A INPUT -p tcp --dport 21 -j DROP
dari@dari:~$ sudo iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 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:21

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination
dari@dari:~$

```

Рисунок 4 — Настройка сетевого экрана на Ub1

```

dari@dari:~$ sudo ssh dari@172.20.10.4
The authenticity of host '172.20.10.4 (172.20.10.4)' can't be established.
ECDSA key fingerprint is SHA256:v/akQ4Fji4h5Gy2Ztd+LHRVLdvKkTriRvo4llsuQe7I.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '172.20.10.4' (ECDSA) to the list of known hosts.
dari@172.20.10.4'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

112 packages can be updated.
81 updates are security updates.

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

Last login: Sun May 21 20:20:50 2023

```

Рисунок 5 — Доступ к Ub1 через ssh

```
dari@dari:~$ sudo telnet 172.20.10.4 21
Trying 172.20.10.4...
^C
dari@dari:~$ sudo telnet 172.20.10.4 22
Trying 172.20.10.4...
Connected to 172.20.10.4.
Escape character is '^I'.
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.10
^C
Connection closed by foreign host.
```

Рисунок 6 — Доступ к Ub1 по 21-ому и 22-ому порту

3. Настроим сетевой экран на Ub2 так, чтобы доступ к нему был разрешен только через ssh.

```
dari@dari:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
dari@dari:~$ sudo iptables -A INPUT -j DROP
dari@dari:~$ sudo iptables -nL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0         0.0.0.0/0         tcp dpt:22
    0     0 DROP      all  --  *      *       0.0.0.0/0         0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination
```

Рисунок 7 — Настройка сетевого экрана на Ub2

```
dari@dari:~$ ping 172.20.10.5
PING 172.20.10.5 (172.20.10.5) 56(84) bytes of data.
^C
--- 172.20.10.5 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2009ms

dari@dari:~$ sudo ssh dari@172.20.10.5
[sudol] password for dari:
The authenticity of host '172.20.10.5 (172.20.10.5)' can't be established.
ECDSA key fingerprint is SHA256:v/akQ4Fji4h5Gy2Ztd+LHRVLdvKkTriRvo4llsuQe7I.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.20.10.5' (ECDSA) to the list of known hosts.
dari@172.20.10.5'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

112 packages can be updated.
81 updates are security updates.

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

Last login: Sun May 21 20:20:57 2023
```

Рисунок 8 — Проверка доступа к Ub2 через ping и ssh

4. Настроим сетевой экран на Ub1 так, чтобы он не имел доступа к 8.8.8.8 в цепочке INPUT.

```
root@dari:/home/dari# iptables -A INPUT -s 8.8.8.8 -j DROP
root@dari:/home/dari# iptables -nvL
Chain INPUT (policy ACCEPT 12 packets, 1040 bytes)
  pkts bytes target    prot opt in     out     source    destination
    0     0 DROP      all  --  *      *       8.8.8.8   0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source    destination

Chain OUTPUT (policy ACCEPT 12 packets, 1040 bytes)
  pkts bytes target    prot opt in     out     source    destination
root@dari:/home/dari# 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 2001ms
```

Рисунок 9 — Настройка Ub1 и недоступность 8.8.8.8

Теперь с помощью Wireshark проанализируем трафик между Ub1 и Интернетом.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.20.10.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x05a8, seq=25/6400, ttl=64 (reply in 2)
2	0.051782	8.8.8.8	172.20.10.4	ICMP	98	Echo (ping) reply id=0x05a8, seq=25/6400, ttl=109 (request in 1)
4	0.999711	172.20.10.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x05a8, seq=26/6656, ttl=64 (reply in 5)
5	1.055830	8.8.8.8	172.20.10.4	ICMP	98	Echo (ping) reply id=0x05a8, seq=26/6656, ttl=109 (request in 4)
7	2.000096	172.20.10.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x05a8, seq=27/6912, ttl=64 (reply in 8)
8	2.053816	8.8.8.8	172.20.10.4	ICMP	98	Echo (ping) reply id=0x05a8, seq=27/6912, ttl=109 (request in 7)
9	2.999620	172.20.10.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x05a8, seq=28/7168, ttl=64 (reply in 12)
12	3.051718	8.8.8.8	172.20.10.4	ICMP	98	Echo (ping) reply id=0x05a8, seq=28/7168, ttl=109 (request in 9)
13	3.999708	172.20.10.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x05a8, seq=29/7424, ttl=64 (reply in 14)
14	4.059904	8.8.8.8	172.20.10.4	ICMP	98	Echo (ping) reply id=0x05a8, seq=29/7424, ttl=109 (request in 13)
15	4.999783	172.20.10.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x05a8, seq=30/7680, ttl=64 (reply in 16)
16	5.053815	8.8.8.8	172.20.10.4	ICMP	98	Echo (ping) reply id=0x05a8, seq=30/7680, ttl=109 (request in 15)
17	5.999793	172.20.10.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x05a8, seq=31/7936, ttl=64 (reply in 18)
18	6.051982	8.8.8.8	172.20.10.4	ICMP	98	Echo (ping) reply id=0x05a8, seq=31/7936, ttl=109 (request in 17)
19	6.999680	172.20.10.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x05a8, seq=32/8192, ttl=64 (reply in 20)
20	7.056904	8.8.8.8	172.20.10.4	ICMP	98	Echo (ping) reply id=0x05a8, seq=32/8192, ttl=109 (request in 19)
23	7.999737	172.20.10.4	8.8.8.8	ICMP	98	Echo (ping) request id=0x05a8, seq=33/8448, ttl=64 (reply in 24)

Рисунок 10 — Анализ трафика в Wireshark

Как можно увидеть на рисунке, пакеты отправляются, но не доходит ответ от 8.8.8.8, из-за чего сеть нагружается бесполезными запросами. Теперь сбросим настройки iptables, заблокируем доступ к 8.8.8.8 в цепочке OUTPUT.

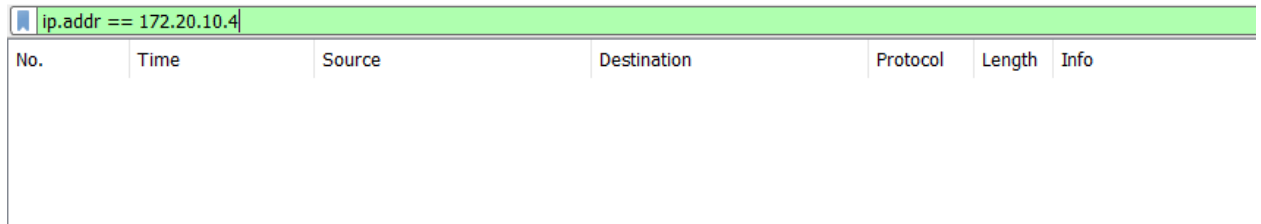
```
root@dari:/home/dari# iptables -A OUTPUT -d 8.8.8.8 -j DROP
root@dari:/home/dari# iptables -nvL
Chain INPUT (policy ACCEPT 42 packets, 3216 bytes)
  pkts bytes target    prot opt in     out     source    destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source    destination

Chain OUTPUT (policy ACCEPT 42 packets, 3216 bytes)
  pkts bytes target    prot opt in     out     source    destination
    0     0 DROP      all  --  *      *       0.0.0.0/0 8.8.8.8
```

Рисунок 11 — Настройка Ub1

Теперь проанализируем трафик с помощью Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

Рисунок 12 — Анализ трафика в Wireshark

Как можно заметить, пакеты не отправляются вовсе, что позволяет сделать вывод, что данный метод гораздо эффективнее, так как он не нагружает сеть бесполезными запросами.

5. Сбросим настройки iptables для Ub3, запретим к нему доступ всеми способами, кроме ICMP-протокола.

```
root@dari:/home/dari# iptables -F INPUT -p icmp -j ACCEPT
root@dari:/home/dari# iptables -F INPUT -j REJECT
root@dari:/home/dari# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source               destination
    0    0 ACCEPT    icmp -- *      *       0.0.0.0/0            0.0.0.0/0
    0    0 REJECT    all  -- *      *       0.0.0.0/0            0.0.0.0/0            reject-with
icmp-port-unreachable

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source               destination
```

Рисунок 13 — Настройка Ub3

Проверим доступность Ub3 через ping, ssh подключение и с помощью утилиты telnet, которая используется tcp протоколы.

```
root@dari:/home/dari# ping 172.20.10.3
PING 172.20.10.3 (172.20.10.3) 56(84) bytes of data:
64 bytes from 172.20.10.3: icmp_seq=1 ttl=64 time=2.41 ms
64 bytes from 172.20.10.3: icmp_seq=2 ttl=64 time=1.26 ms
64 bytes from 172.20.10.3: icmp_seq=3 ttl=64 time=0.881 ms
^C
--- 172.20.10.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.881/1.522/2.419/0.654 ms
root@dari:/home/dari# ssh dari@172.20.10.3
ssh: connect to host 172.20.10.3 port 22: Connection refused
```

Рисунок 14 — Проверка доступности Ub3

Как видно, через ping можно обратиться к Ub3, остальными способами нельзя.

6. Было запрещено подключение к ub1 по 80-ому порту, также настроено логирование попыток подключения по 80-ому порту.

```
root@dari:/home/dari# iptables -A INPUT -p tcp --dport 80 -j LOG --log-prefix "Logging 80 port"
root@dari:/home/dari# iptables -A INPUT -p tcp --dport 80 -j REJECT
root@dari:/home/dari# iptables -nvL
Chain INPUT (policy ACCEPT 12 packets, 1152 bytes)
  pkts bytes target     prot opt in     out     source            destination
   0    0 LOG         tcp  --  *      *       0.0.0.0/0         0.0.0.0/0         tcp dpt:80
LOG flags 0 level 4 prefix "Logging 80 port"
   0    0 REJECT      tcp  --  *      *       0.0.0.0/0         0.0.0.0/0         tcp dpt:80
reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination

Chain OUTPUT (policy ACCEPT 12 packets, 1152 bytes)
  pkts bytes target     prot opt in     out     source            destination
```

Рисунок 15 — Настройка Ub1

Теперь с помощью команды telnet выполним запрос к 80-ому порту с двух других ВМ, проверим файл /var/log/kern.log на наличие информации о нужном логировании.

```
root@dari:/home/dari# cat /var/log/kern.log | grep "Logging 80 port"
May 21 22:19:33 dari kernel: [ 7043.643040] Logging 80 port IN=enp0s3 OUT= MAC=08:00:27:80:8e:cc:08:0
0:27:06:9b:50:08:00 SRC=172.20.10.3 DST=172.20.10.4 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=41856 DF PRO
TO=TCP SPT=48386 DPT=80 WINDOW=29200 RES=0x00 SYN URG=0
May 21 22:23:47 dari kernel: [ 7297.100466] Logging 80 port IN=enp0s3 OUT= MAC=08:00:27:80:8e:cc:08:0
0:27:4a:5f:dd:08:00 SRC=172.20.10.5 DST=172.20.10.4 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=50704 DF PRO
TO=TCP SPT=55774 DPT=80 WINDOW=29200 RES=0x00 SYN URG=0
```

Рисунок 16 — Логирование о попытках доступа к 80-ому порту Ub1

7. Заблокируем доступ по 80-ому порту к Ub3 с Ub1 по его MAC-адресу.

```
root@dari:/home/dari# iptables -A INPUT -p tcp --sport 80 -m mac --mac-source 08:00:27:06:9b:50
root@dari:/home/dari# nc -vz 172.20.10.3 80
nc: connect to 172.20.10.3 port 80 (tcp) failed: Connection refused
```

Рисунок 17 — Настройка Ub1 и проверка недоступности порта

Теперь сменим MAC-адрес Ub3 и попробуем заново.

```
root@dari:/home/dari# nc -vz 172.20.10.3 80
Connection to 172.20.10.3 80 port [tcp/http] succeeded!
```

Рисунок 18 — Проверка доступности после смены MAC-адреса

Как можно заметить, блокируются только запросы с конкретного MAC-адреса независимо от IP.

8. Был полностью закрыт доступ к Ub1, но был разрешен доступ для Ub3 к Ub1 через порты 20-79.



```

root@dari:/home/dari# iptables -A INPUT -p tcp -s 172.20.10.3 --dport 20:79 -j ACCEPT
root@dari:/home/dari# iptables -A INPUT -p tcp -j REJECT
root@dari:/home/dari# iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
:79 0      0 ACCEPT     tcp  --  *      *       172.20.10.3          0.0.0.0/0          tcp dpts:20
0      0 REJECT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0          reject-with
icmp-port-unreachable
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source               destination

```

Рисунок 19 — Настройка Ub1

Теперь продемонстрируем недоступность 80 порта на Ub1 для Ub3 с помощью telnet.

```

root@dari:/home/dari# telnet 172.20.10.4 80
Trying 172.20.10.4...
telnet: Unable to connect to remote host: Connection refused

```

Рисунок 20 — Недоступность Ub1 по 80 порту

```

root@dari:/home/dari# telnet 172.20.10.4 21
Trying 172.20.10.4...
Connected to 172.20.10.4.
Escape character is '^I'.
220 dari FTP server (Version 6.4/OpenBSD/Linux-ftp-0.17) ready.
quit
221 Goodbye.
Connection closed by foreign host.
root@dari:/home/dari# ssh dari@172.20.10.4
The authenticity of host '172.20.10.4 (172.20.10.4)' can't be established.
ECDSA key fingerprint is SHA256:v/akQ4Fji4h5Gy2Ztd+LHRULdvKkTriRvo4llsuQe7I.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.20.10.4' (ECDSA) to the list of known hosts.
dari@172.20.10.4'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

112 packages can be updated.
81 updates are security updates.

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

Last login: Sun May 21 23:02:51 2023

```

Рисунок 21 — Доступность Ub1 по ssh и по 21 порту

9. Разрешим только одно ssh-подключение к Ub3.

```

root@dari:/home/dari# iptables -A INPUT -p tcp --syn --dport 22 -m connlimit --connlimit-above 1 --c
onnlimit-mask 0 -j REJECT
root@dari:/home/dari# iptables -nvL
Chain INPUT (policy ACCEPT 20 packets, 1440 bytes)
  pkts bytes target     prot opt in     out     source            destination
    0      0 REJECT     tcp  --  *      *      0.0.0.0/0         0.0.0.0/0         tcp dpt:22
flags:0x17/0x02 #conn src/0 > 1 reject-with icmp-port-unreachable
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target     prot opt in     out     source            destination
Chain OUTPUT (policy ACCEPT 10 packets, 1352 bytes)
  pkts bytes target     prot opt in     out     source            destination

```

Рисунок 22 — Настройка Ub3

Теперь подключимся по ssh с Ub1 на Ub3 и попытаемся сделать то же самое с Ub2.

```

root@dari:/home/dari# ssh dari@172.20.10.3
The authenticity of host '172.20.10.3 (172.20.10.3)' can't be established.
ECDSA key fingerprint is SHA256:v/akQ4Fji4h5GyZZtd+LHRVLDvKkTriRvo4llsuQe7I.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.20.10.3' (ECDSA) to the list of known hosts.
dari@172.20.10.3'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

112 packages can be updated.
81 updates are security updates.

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

Last login: Sun May 21 23:18:24 2023

```

Рисунок 23 — Подключение через ssh с Ub1

```

dari@dari:~$ sudo ssh dari@172.20.10.3
[sudo] password for dari:
ssh: connect to host 172.20.10.3 port 22: Connection refused

```

Рисунок 23 — Подключение через ssh с Ub2

Попытка не увенчалась успехом, так как Ub3 не дает сделать второе ssh-соединение.

### Выводы.

В ходе данной работы были изучены принципы работы с сетевыми экранами. Были решены следующие задачи:

1. Создание трех виртуальных машин.

2. Реализация блокирования и разрешения приема и отправки пакетов с помощью iptables, создание логирования событий.