

**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**  
**Вариант 27**

Студентка гр. 1381

\_\_\_\_\_

Рымарь М.И.

Преподаватель

\_\_\_\_\_

Фирсов 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.
2. Научиться блокировать и разрешать прием и отправку пакетов с помощью iptables, настраивать логирование событий.

### **Задание.**

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 продемонстрировать 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 продемонстрировать 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.

Комментарий: 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.

Вариант 27: X-47, Y-106, Z-20-105

### **Выполнение работы.**

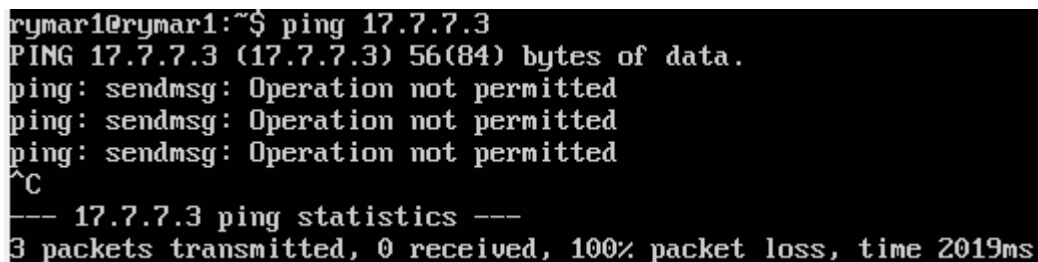
Для выполнения лабораторной работы были настроены три виртуальные машины ub1, ub2, ub3. Они находятся в одной подсети – 17.7.7.0. Адреса у машин соответственно – 17.7.7.1/24, 17.7.7.2/24, 17.7.7.3/24. Перед выполнением задач было установлено ПО с помощью следующей команды:

```
apt-get update && apt install apache2 ftpd -y
```

1. Заблокируем доступ по IP-адресу ub1 к ub3. Для этого объявим правило в цепочке OUTPUT на IP-адрес ub3. Запрет поставили с помощью команды:

```
sudo iptables -A OUTPUT -d 17.7.7.3 -j DROP
```

Проверим доступность с ub1 и ub2 на ub3. Результат проверки показан на рисунках 2-3.



```
rymar1@rymar1:~$ ping 17.7.7.3
PING 17.7.7.3 (17.7.7.3) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
^C
--- 17.7.7.3 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2019ms
```

Рисунок 1 – Ping с ub1 на ub3

```
rymar2@rymar2:~$ ping 17.7.7.3
PING 17.7.7.3 (17.7.7.3) 56(84) bytes of data.
64 bytes from 17.7.7.3: icmp_seq=1 ttl=64 time=0.453 ms
64 bytes from 17.7.7.3: icmp_seq=2 ttl=64 time=0.821 ms
64 bytes from 17.7.7.3: icmp_seq=3 ttl=64 time=1.18 ms
^C
--- 17.7.7.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.453/0.820/1.188/0.301 ms
```

Рисунок 2 – Ping с ub2 на ub3

По результатам отправки запросов видно, что с ub1 на ub3 невозможно отправить запрос, а с ub2 на ub3 возможно. Значит, получилось заблокировать доступ с помощью вышеописанной команды.

2. Заблокируем доступ по 47-му порту на ub1. Запрет поставлен с помощью команды:

```
sudo iptables -A INPUT -p tcp --dport 47 -j REJECT
```

Проверим доступ с ub2 на ub1 через 47 порт и через ssh. Проверки показаны на рисунках 3 и 4, соответственно.

```
rymar2@rymar2:~$ sudo nc -vz 17.7.7.1 47
nc: connect to 17.7.7.1 port 47 (tcp) failed: Connection refused
```

Рисунок 3 – Проверка доступности ub1 с ub2 по 47 порту

```
rymar2@rymar2:~$ ssh rymar1@17.7.7.1
rymar1@17.7.7.1'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

118 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: Thu Apr 27 00:34:59 2023
```

Рисунок 4 – Проверка доступности ub1 с ub2 по ssh

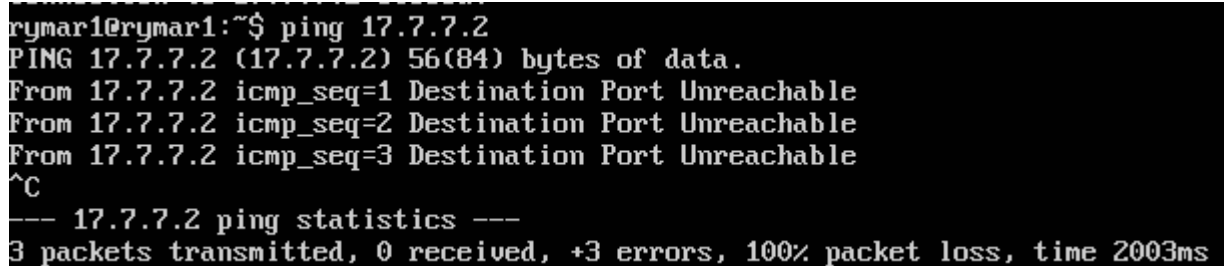
По результатам проверки видно, что с ub2 на ub1 по 47 порту заблокирован, но доступ с ub2 на ub1 по ssh возможен. Значит, доступ удалось заблокировать вышеописанной командой.

3. Разрешим доступ только по ssh на ub2. Сначала разрешим пакет через ssh, затем запретим всё остальные. Это было сделано с помощью следующих команд:

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

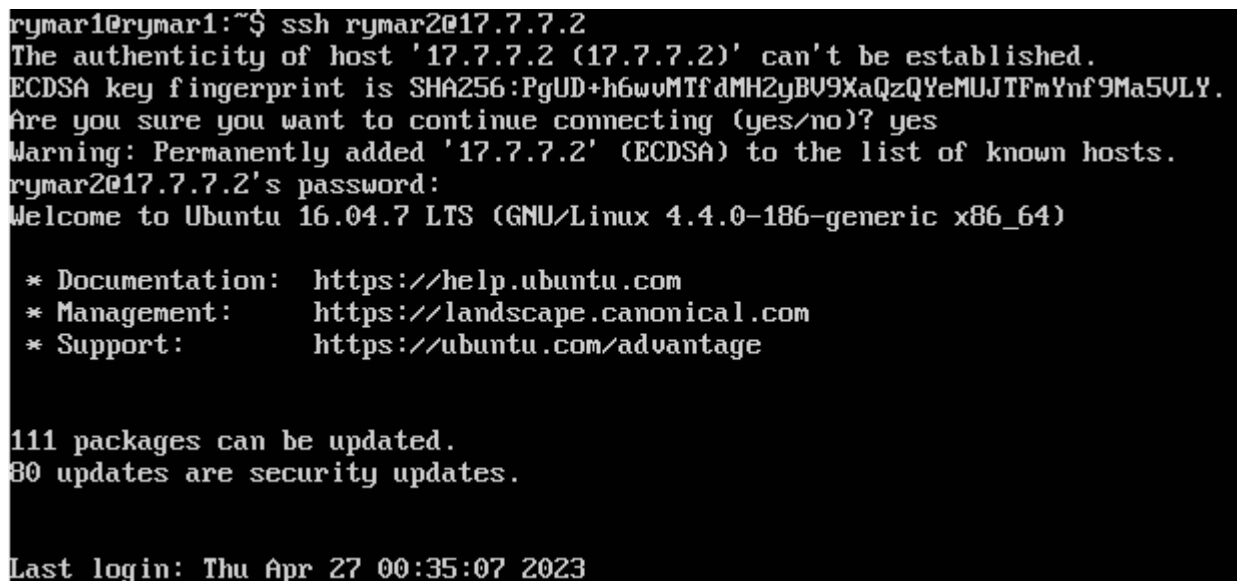
```
sudo iptables -A INPUT -j REJECT
```

Правильность настройки проверим отправкой ping с ub1 на ub2, потом проверим доступность через ssh. Результаты показаны на рисунках 5 и 6, соответственно.



```
rymar1@rymar1:~$ ping 17.7.7.2
PING 17.7.7.2 (17.7.7.2) 56(84) bytes of data.
From 17.7.7.2 icmp_seq=1 Destination Port Unreachable
From 17.7.7.2 icmp_seq=2 Destination Port Unreachable
From 17.7.7.2 icmp_seq=3 Destination Port Unreachable
^C
--- 17.7.7.2 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2003ms
```

Рисунок 5 – Проверка доступности ub2 с ub1 через ping



```
rymar1@rymar1:~$ ssh rymar2@17.7.7.2
The authenticity of host '17.7.7.2 (17.7.7.2)' can't be established.
ECDSA key fingerprint is SHA256:PgUD+h6wvMTfdMH2yBU9XaQzQYeMUJTFmYnf9Ma5VLY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '17.7.7.2' (ECDSA) to the list of known hosts.
rymar2@17.7.7.2'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

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

Last login: Thu Apr 27 00:35:07 2023
```

Рисунок 6 – Проверка доступности ub2 с ub1 через ssh

По результатам проверки видно, что всё настроено верно, так как доступ к ub2 возможен только через ssh.

4. Сначала запретим ICMP запросы на 8.8.8.8 через правило в цепочке INPUT с помощью следующей команды:

```
sudo iptables -A INPUT -p icmp -s 8.8.8.8 -j REJECT
```

Результат настройки показан на рисунках 7 и 8.

```

sudo iptables -A INPUT -p icmp -s 8.8.8.8 -j REJECT
[sudo] password for rymar1:
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 ---
7 packets transmitted, 0 received, 100% packet loss, time 5999ms

```

Рисунок 7 – Запрет ICMP-запросов на 8.8.8.8 через INPUT

ip.addr == 8.8.8.8						
No.	Time	Source	Destination	Protocol	Length	Info
105	4.324183	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=18/
106	4.393723	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=18/
192	5.332402	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=19/
196	5.384330	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=19/
231	6.340485	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=20/
233	6.394616	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=20/
250	7.348984	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=21/
251	7.422499	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=21/
310	8.356111	172.20.10.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=22/
314	8.410751	8.8.8.8	172.20.10.2	ICMP	98	Echo (ping) reply id=0x0001, seq=22/

Рисунок 8 – Отправка и приём ICMP-запросов на 8.8.8.8 при запрете через INPUT

Далее обновим таблицы, перезапустив `ub1`. Запретим ICMP-запросы на 8.8.8.8 через правило в цепочке OUTPUT с помощью следующей команды:

```
sudo iptables -A OUTPUT -p icmp -d 8.8.8.8 -j REJECT
```

Результат настройки показан на рисунках 9 и 10.

```

From 10.0.3.15 icmp_seq=1 Destination Port Unreachable
From 10.0.3.15 icmp_seq=1 Destination Port Unreachable
From 10.0.3.15 icmp_seq=1 Destination Port Unreachable
From 10.0.3.15 icmp_seq=1 Destination Port Unreachable
From 10.0.3.15 icmp_seq=1 Destination Port Unreachable
^C
--- 8.8.8.8 ping statistics ---
0 packets transmitted, 0 received, +3430 errors

```

Рисунок 9 – Запрет ICMP-запросов на 8.8.8.8 через OUTPUT

ip.addr == 8.8.8.8						
No.	Time	Source	Destination	Protocol	Length	Info

Рисунок 10 – Отправка и получение ICMP-запросов на 8.8.8.8 при запрете через OUTPUT

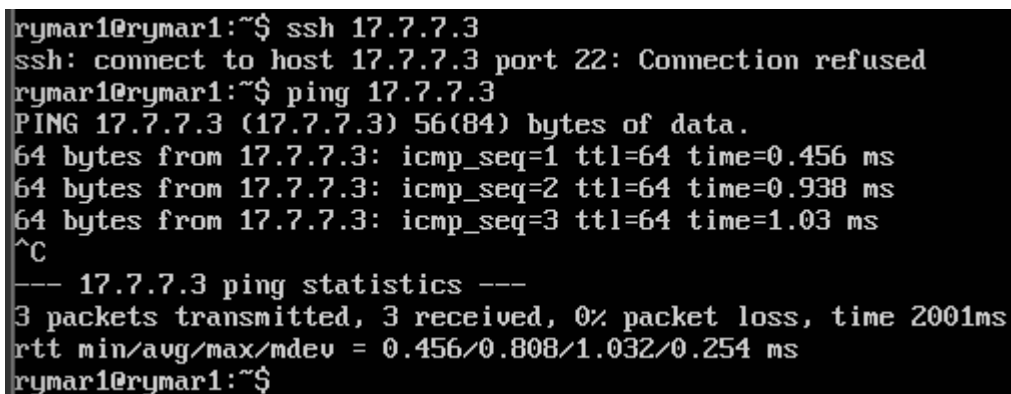
С помощью приложения Wireshark получены результаты запросов после запрета обоими способами. При запрете через правило в цепочке INPUT запросы отправляются на 8.8.8.8, оттуда приходят ответы, которые затем отклоняются. При отправке через правило в цепочке OUTPUT запросы не отправляются. Можно сделать вывод о том, что использование второго правила эффективнее, так как сеть не перегружается лишними ICMP-запросами.

5. Запретим полностью доступ к ub3 кроме ICMP-протокола с помощью следующих команд:

```
sudo iptables -A INPUT -p icmp -j ACCEPT
```

```
sudo iptables -A INPUT -j REJECT
```

Правильность настроек проверим с помощью отправки ping и ssh с ub1 на ub3. Результат показан на рисунке 11.



```
rymar1@rymar1:~$ ssh 17.7.7.3
ssh: connect to host 17.7.7.3 port 22: Connection refused
rymar1@rymar1:~$ ping 17.7.7.3
PING 17.7.7.3 (17.7.7.3) 56(84) bytes of data.
64 bytes from 17.7.7.3: icmp_seq=1 ttl=64 time=0.456 ms
64 bytes from 17.7.7.3: icmp_seq=2 ttl=64 time=0.938 ms
64 bytes from 17.7.7.3: icmp_seq=3 ttl=64 time=1.03 ms
^C
--- 17.7.7.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.456/0.808/1.032/0.254 ms
rymar1@rymar1:~$
```

Рисунок 11 – Проверка доступа к ub3

Результаты проверки показывают, что настройки корректны, так как ssh не даёт доступ к ub3, а ping был успешен. Значит, передача возможна только через ICMP-протокол.

6. Запретим подключение к ub1 по 106-му порту и настроим логирование попыток провести такое подключение с помощью следующих команд:

```
sudo iptables -A INPUT -p tcp --dport 106 -j LOG --log-prefix "106logprefix"
```

```
sudo iptables -A INPUT -p tcp --dport 106 -j REJECT
```

Проверим корректность настроек, выполнив запрос с ub2 на ub1 по 106-му порту. Результаты запроса показаны на рисунке 12. Логи, находящиеся в файле /var/log/kern.log на машине ub1, показаны на рисунке 13.

```
rymar2@rymar2:~$ sudo nc -vz 17.7.7.1 106
nc: connect to 17.7.7.1 port 106 (tcp) failed: Connection refused
rymar2@rymar2:~$
```

Рисунок 12 – Попытка подключения с ub2 на ub1 по 106 порту

```
Apr 27 03:37:44 rymar1 kernel: [ 1748.406387] 106logprefixIN=enp0s3 OUT= MAC=08:00:27:44:1c:8c:08:00
:27:d5:4d:cf:08:00 SRC=17.7.7.2 DST=17.7.7.1 LEN=60 TOS=0x00 PREC=0x00 TTL=64 ID=38957 DF PROTO=TCP
SPT=58842 DPT=106 WINDOW=29200 RES=0x00 SYN URG=0
```

Рисунок 13 – Лог в файле с заданным префиксом

По результатам проверки видно, что подключиться к ub1 по 106-му порту невозможно из-за установленного запрета. При этом происходит логирование попыток подключения по этому порту на заданной машине.

7. Заблокируем доступ по 106-му порту к ub3 с ub1 по его MAC-адресу 08:00:27:35:10:7D с помощью команды:

```
sudo iptables -A INPUT -p tcp --sport 106 -m mac --mac-source
08:00:27:35:10:7D -j REJECT
```

Корректность настроек проверена с помощью отправки запроса с ub1 на ub3 через 106 порт. После длительного ожидания пришлось прервать команду, подключение невозможно. Результат показан на рисунке 14.

```
rymar1@rymar1:~$ sudo iptables -A INPUT -p tcp --sport 106 -m mac --mac-source 08:00:27:35:10:7D -j
REJECT
rymar1@rymar1:~$ sudo nc -vz 17.7.7.3 106
^C
```

Рисунок 14 – Попытка подключения к ub3 с ub1 через 106-й порт

Сменим MAC-адрес ub3 через настройки виртуальной машины на сгенерированный – 08:00:27:7F:83:04. Попробуем подключиться снова. Результат показан на рисунке 15.

```
rymar1@rymar1:~$ sudo nc -vz 17.7.7.3 106
Connection to 17.7.7.3 106 port [tcp/poppassd] succeeded!
```

Рисунок 15 – Проверка доступа к ub3 с новым MAC-адресом с ub1 через 106-й порт

8. Закроем полностью доступ к ub1. Разрешим доступ для ub3 к ub1 через порты 20-105 с помощью следующих команд:

```
sudo iptables -A INPUT -p tcp -s 17.7.7.3/24 --dport 20:105 -j ACCEPT
sudo iptables -A INPUT -j REJECT
```



Проверим возможность подключения через 21-й и 105-й порты (из разрешённого диапазона) с помощью прослушивания, через 106-й порт и через ssh с ub3 к ub1. Результаты показаны на рисунке 16.

```
rymar3@rymar3:~$ sudo nc -vz 17.7.7.1 21
Connection to 17.7.7.1 21 port [tcp/ftp] succeeded!
rymar3@rymar3:~$ sudo nc -vz 17.7.7.1 105
Connection to 17.7.7.1 105 port [tcp/csnet-ns] succeeded!
rymar3@rymar3:~$ sudo nc -vz 17.7.7.1 106
nc: connect to 17.7.7.1 port 106 (tcp) failed: Connection refused
rymar3@rymar3:~$ ssh rymar1@17.7.7.1
rymar1@17.7.7.1'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

118 packages can be updated.
30 updates are security updates.

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

Last login: Thu Apr 27 11:08:18 2023 from 17.7.7.3
```

Рисунок 16 – Проверка доступа с ub3 на ub1 различными способами

По результатам проверки видно, что к ub1 невозможно подключиться по 106-му порту с ub3, так как установлен запрет, однако есть возможность подключиться через ssh (22 порт).

9. Разрешим только одно ssh-подключение к ub3 с помощью команды:

```
sudo iptables -A INPUT -p tcp --syn --dport 22 -m connlimit --connlimit-above 1 --connlimit-mask 0 -j REJECT
```

Проверим корректность настроек, запустив ssh-сессию с ub1 на ub3, что показано на рисунке 17, затем с ub2 на ub3, что показано на рисунке 18.

```

rymar1@rymar1:~$ sudo ssh rymar3@17.7.7.3
ssh: connect to host 17.7.7.3 port 22: Connection refused
rymar1@rymar1:~$ sudo ssh rymar3@17.7.7.3
The authenticity of host '17.7.7.3 (17.7.7.3)' can't be established.
ECDSA key fingerprint is SHA256:g0lTSb5jaAUlr7t1+PkgUfEkU7ygF7q/4oqPhm1WTck.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '17.7.7.3' (ECDSA) to the list of known hosts.
rymar3@17.7.7.3'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

111 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: Thu Apr 27 09:56:47 2023

```

Рисунок 17 – Подключение через ssh к ub3 с ub1

```

rymar2@rymar2:~$ ssh rymar3@17.7.7.3
ssh: connect to host 17.7.7.3 port 22: Connection refused
rymar2@rymar2:~$

```

Рисунок 18 – Подключение через ssh к ub3 с ub2

По результатам проверки можно сделать вывод о том, что настройки верны, так как с ub1 удалось подключиться к ub3, а с ub2 не удалось. Это произошло, потому что было установлено ограничение только на одно ssh-подключение.

## Выводы.

В ходе выполнения лабораторной работы были изучены принципы работы с сетевыми экранами. Также были созданы три виртуальные машины, заблокированы и разрешены приём и отправка пакетов с помощью iptables, настроено логирование событий.