

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.

Студентка гр. 1304

Чернякова В.А.

Преподаватель

Ефремов М.А.

Санкт-Петербург

2023

Цель работы.

Целью работы является изучение принципов работы с сетевыми экранами.

Задание.

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

Выполнение работы.

В соответствии с заданием, были развёрнуты три виртуальные машины U1, U2 и U3 со следующими сетевыми конфигурациями:

Устройство	U1	U2	U3
IP-адрес	15.0.3.14	15.0.3.2	15.0.3.112
Маска подсети	255.255.255.0		

По умолчанию у устройств свободный доступ друг к другу:

```
lera2003@Valeriya:~$ ping 15.0.3.2
PING 15.0.3.2 (15.0.3.2) 56(84) bytes of data.
64 bytes from 15.0.3.2: icmp_seq=1 ttl=64 time=1.25 ms
64 bytes from 15.0.3.2: icmp_seq=2 ttl=64 time=0.472 ms
64 bytes from 15.0.3.2: icmp_seq=3 ttl=64 time=0.317 ms
64 bytes from 15.0.3.2: icmp_seq=4 ttl=64 time=0.285 ms
64 bytes from 15.0.3.2: icmp_seq=5 ttl=64 time=0.544 ms
64 bytes from 15.0.3.2: icmp_seq=6 ttl=64 time=0.258 ms
```

Рисунок 1 – доступ с U1 на U2.

```
lera2003@Valeriya:~$ ping 15.0.3.112
PING 15.0.3.112 (15.0.3.112) 56(84) bytes of data.
64 bytes from 15.0.3.112: icmp_seq=1 ttl=64 time=0.300 ms
64 bytes from 15.0.3.112: icmp_seq=2 ttl=64 time=0.773 ms
64 bytes from 15.0.3.112: icmp_seq=3 ttl=64 time=0.321 ms
64 bytes from 15.0.3.112: icmp_seq=4 ttl=64 time=0.370 ms
64 bytes from 15.0.3.112: icmp_seq=5 ttl=64 time=0.342 ms
64 bytes from 15.0.3.112: icmp_seq=6 ttl=64 time=0.432 ms
```

Рисунок 2 – доступ с U1 на U3.

1. Заблокировать доступ по IP-адресу ПК Ub1 к Ub3.

Заблокируем доступ по IP-адресу с 15.0.3.14 на 15.0.3.112. Для этого воспользуемся следующей командой:

```
sudo iptables -A OUTPUT -d 15.0.3.112 -j DROP
```

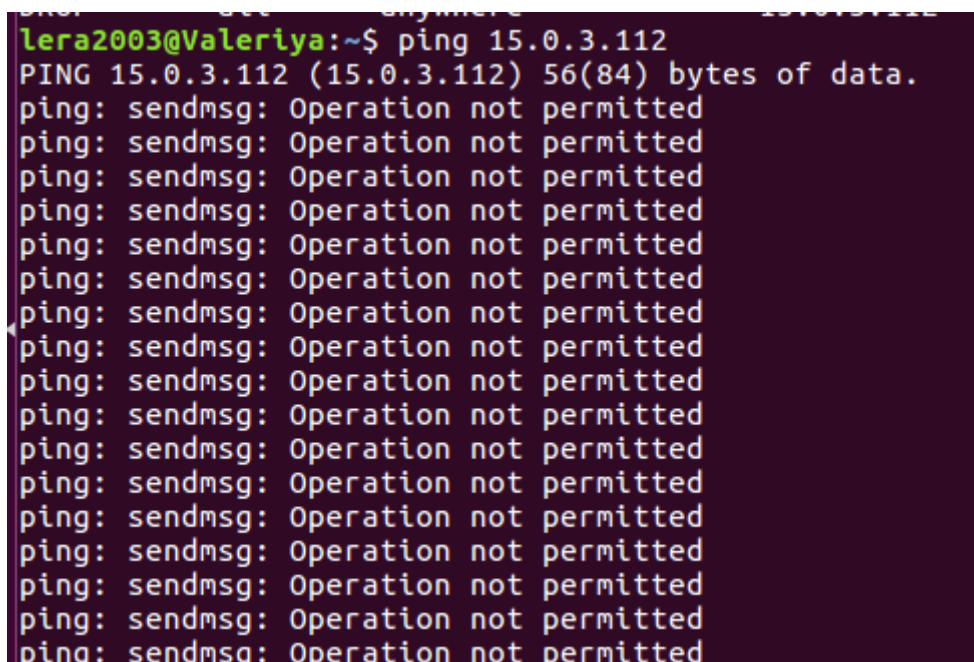
-A – добавление правила в конец списка.

OUTPUT – исходящие пакеты.

-d – адрес назначения.

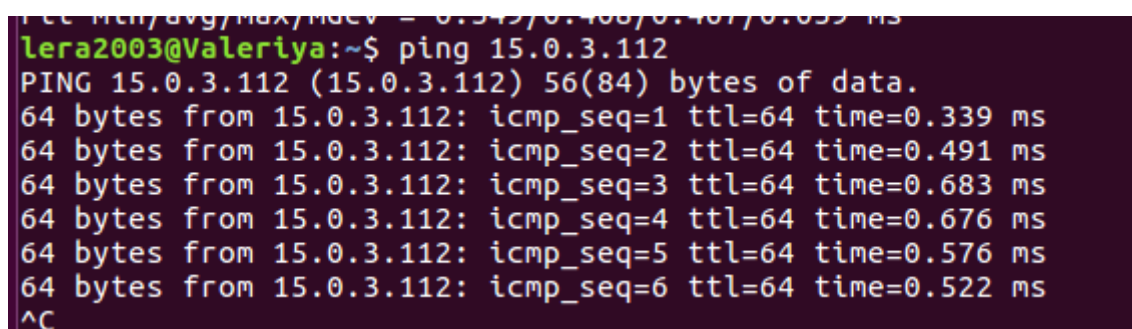
-j – указание допустимых действий.

DROP – запрещает пакет.



A terminal window with a dark purple background. The prompt is `lera2003@Valeriya:~$`. The user enters `ping 15.0.3.112`. The output shows the first line of a ping command: `PING 15.0.3.112 (15.0.3.112) 56(84) bytes of data.` followed by 15 lines of `ping: sendmsg: Operation not permitted`.

Рисунок 3 – доступ с U1 на U3.



A terminal window with a dark purple background. The prompt is `lera2003@Valeriya:~$`. The user enters `ping 15.0.3.112`. The output shows the first line of a ping command: `PING 15.0.3.112 (15.0.3.112) 56(84) bytes of data.` followed by 6 lines of successful ping responses: `64 bytes from 15.0.3.112: icmp_seq=1 ttl=64 time=0.339 ms`, `64 bytes from 15.0.3.112: icmp_seq=2 ttl=64 time=0.491 ms`, `64 bytes from 15.0.3.112: icmp_seq=3 ttl=64 time=0.683 ms`, `64 bytes from 15.0.3.112: icmp_seq=4 ttl=64 time=0.676 ms`, `64 bytes from 15.0.3.112: icmp_seq=5 ttl=64 time=0.576 ms`, and `64 bytes from 15.0.3.112: icmp_seq=6 ttl=64 time=0.522 ms`. The prompt `^C` is visible at the bottom.

Рисунок 4 – доступ с U2 на U3.

2. Заблокировать доступ по 21-му порту на Ub1.

Для того, чтобы заблокировать доступ по 21 порту на U1 воспользуемся следующей командой:

```
sudo iptables -A INPUT -p tcp --dport 21 -j REJECT
```

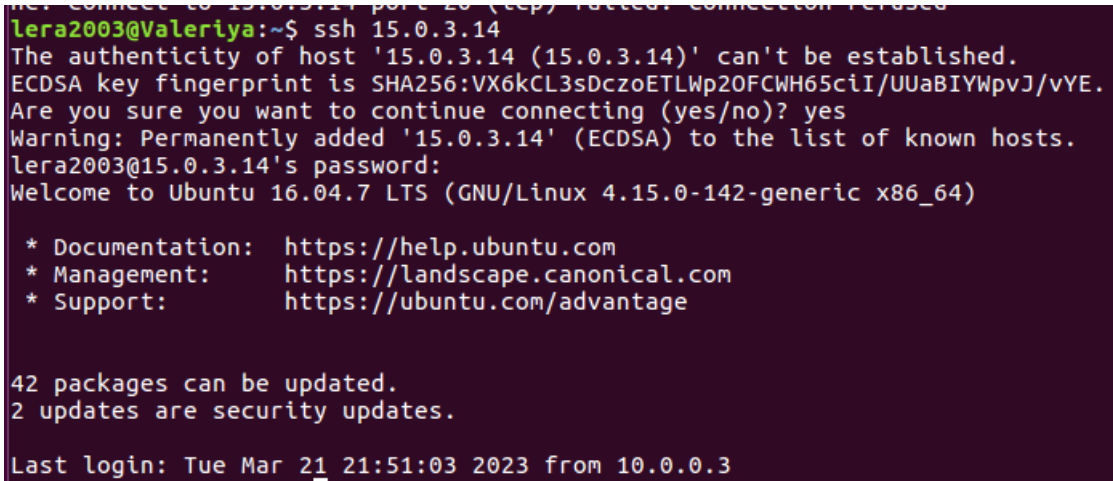
INPUT – входящие пакеты.

-p – вручную установить протокол (в данном случае TCP).

--dport – порт назначения.

REJECT – запрещает отправку пакета с отправкой сообщения источнику.

Проверим доступность U1 по ssh.



```
net connect to 15.0.3.14 port 22 (tcp) failed: connection refused
lera2003@Valeriya:~$ ssh 15.0.3.14
The authenticity of host '15.0.3.14 (15.0.3.14)' can't be established.
ECDSA key fingerprint is SHA256:VX6kCL3sDczoETLWp20FCWH65ciI/UUaBIYWpvJ/vYE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '15.0.3.14' (ECDSA) to the list of known hosts.
lera2003@15.0.3.14's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-142-generic x86_64)

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

42 packages can be updated.
2 updates are security updates.

Last login: Tue Mar 21 21:51:03 2023 from 10.0.0.3
```

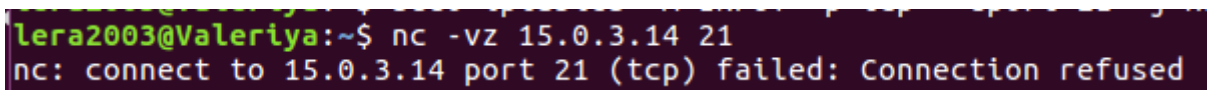
Рисунок 5 – доступ по ssh на U1.

Для проверки недоступности по 21-му порту на U1 воспользуемся утилитой Ubuntu nc. Команда nc (netcat) служит для передачи и получения данных посредством протоколов TCP и UDP.

Использовались следующие ключи:

-v – подробный режим. Используется при сканировании портов;

-z – отключить отправку данных. Используется при сканировании портов.



```
lera2003@Valeriya:~$ nc -vz 15.0.3.14 21
nc: connect to 15.0.3.14 port 21 (tcp) failed: Connection refused
```

Рисунок 6 – недоступность по 21-му порту U1.

3. Разрешить доступ только по ssh на Ub2.

Введем команды, блокирующие все пакеты, кроме ssh-соединений:

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

ACCEPT – разрешение пакетов.

Так как ssh-сервер слушает 22-й порт, то первая команда разрешает для TCP-протокола (ключ -p) 22-й порт назначения, а второе правило блокирует все пакеты.

Важен порядок применения правил. Второе правило добавляется в конце таблицы, поэтому первое правило применяется сначала.

```
lera2003@Valeriya:~$ ssh 15.0.3.2
The authenticity of host '15.0.3.2 (15.0.3.2)' can't be established.
ECDSA key fingerprint is SHA256:VX6kCL3sDczoETLWp20FCWH65ciI/UUaBIYWpvJ/vYE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '15.0.3.2' (ECDSA) to the list of known hosts.
lera2003@15.0.3.2's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-142-generic x86_64)

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

Могут быть обновлены 42 пакета.
2 обновления касаются безопасности системы.

Last login: Tue Mar 21 20:34:23 2023 from 10.0.1.2
```

Рисунок 7 – доступ к U2 по ssh.

```
lera2003@Valeriya:~$ ping 15.0.3.2
PING 15.0.3.2 (15.0.3.2) 56(84) bytes of data.
^C
--- 15.0.3.2 ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10352ms
```

Рисунок 8 – доступ с U1 на U2.

4. Запретить ICMP-запросы на IP-адрес 8.8.8.8 двумя способами.

В начале создадим правило в цепочке INPUT, для запрета принятия пакетов. Команда будет выглядеть так:

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

-s – адрес источника.

```
lera2003@Valeriya:~$ sudo iptables -A INPUT -p icmp -s 8.8.8.8 -j REJECT
lera2003@Valeriya:~$ 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 6343ms
```

Рисунок 9 – доступ с U3 к 8.8.8.8 после применённого INPUT правила.

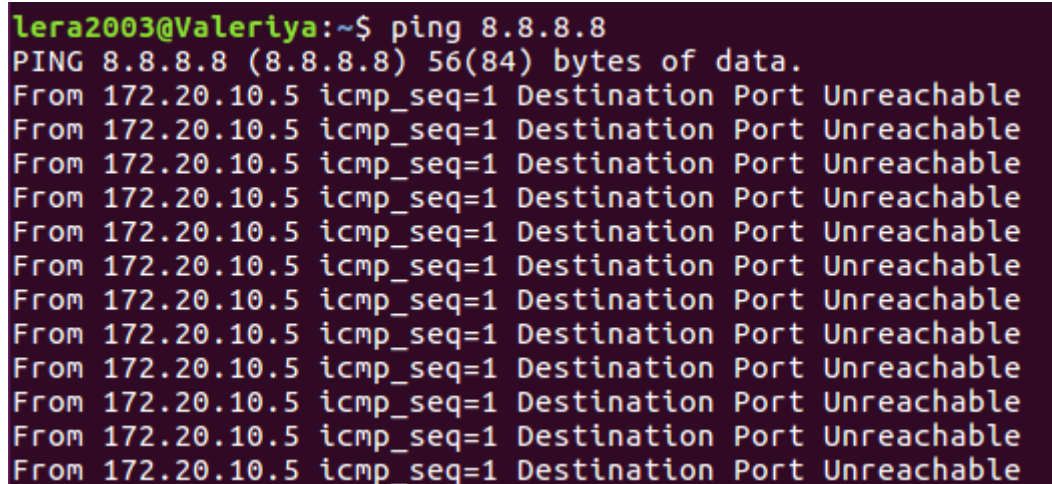
Рассмотрим с помощью Wireshark работу хоста при отправке данного запроса.

1	2023-0...	172.20.10.5	8.8.8.8	ICMP	98 Echo (ping) request	id=0x1994, seq=7/1792, ttl=64 (reply ...
2	2023-0...	8.8.8.8	172.20.10.5	ICMP	98 Echo (ping) reply	id=0x1994, seq=7/1792, ttl=106 (reque...
3	2023-0...	172.20.10.5	8.8.8.8	ICMP	126 Destination unreachable (Port unreachable)	
4	2023-0...	172.20.10.5	8.8.8.8	ICMP	98 Echo (ping) request	id=0x1994, seq=8/2048, ttl=64 (reply ...
5	2023-0...	8.8.8.8	172.20.10.5	ICMP	98 Echo (ping) reply	id=0x1994, seq=8/2048, ttl=106 (reque...
6	2023-0...	172.20.10.5	8.8.8.8	ICMP	126 Destination unreachable (Port unreachable)	
7	2023-0...	172.20.10.5	8.8.8.8	ICMP	98 Echo (ping) request	id=0x1994, seq=9/2304, ttl=64 (reply ...
8	2023-0...	8.8.8.8	172.20.10.5	ICMP	98 Echo (ping) reply	id=0x1994, seq=9/2304, ttl=106 (reque...
9	2023-0...	172.20.10.5	8.8.8.8	ICMP	126 Destination unreachable (Port unreachable)	
10	2023-0...	172.20.10.5	8.8.8.8	ICMP	98 Echo (ping) request	id=0x1994, seq=10/2560, ttl=64 (reply...
11	2023-0...	8.8.8.8	172.20.10.5	ICMP	98 Echo (ping) reply	id=0x1994, seq=10/2560, ttl=106 (requ...
12	2023-0...	172.20.10.5	8.8.8.8	ICMP	126 Destination unreachable (Port unreachable)	

Рисунок 10 – работа хоста при отправке пакетов с U3 на 8.8.8.8 после применённого INPUT правила.

Теперь создадим правило в цепочке OUTPUT, для запрета отправки пакетов. Команда будет выглядеть следующим образом:

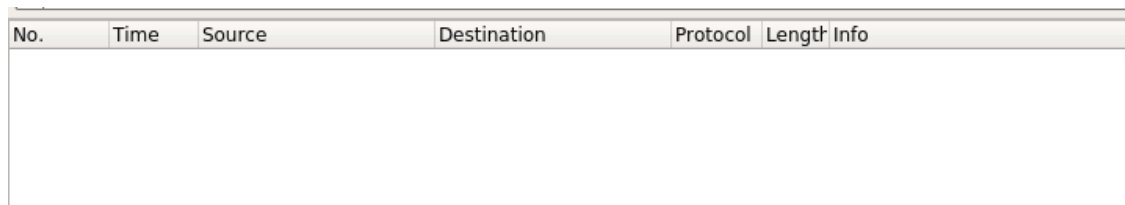
```
sudo iptables -A OUTPUT -p icmp -d 8.8.8.8 -j REJECT
```



A terminal window showing the command 'ping 8.8.8.8' being executed. The output shows 'PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.' followed by 12 lines of 'From 172.20.10.5 icmp_seq=1 Destination Port Unreachable'.

Рисунок 11 – доступ с U3 к 8.8.8.8 после применённого OUTPUT правила.

Рассмотрим с помощью Wireshark работу хоста при отправке данного запроса.



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

Рисунок 12 – работа хоста при отправке пакетов с U3 на 8.8.8.8 после применённого OUTPUT правила.

Таким образом, можно сделать вывод, что способ запрета ICMP запросов через цепочку правил в OUTPUT более выгодный. В таком случае пакеты вообще не выходят (как видно, консоль в Wireshark в таком случае пуста), общий трафик в подсети не увеличивается.

5. Полностью запретить доступ к U3. Разрешить доступ по ICMP протоколу.

Для того, чтобы полностью запретить доступ к U3 и разрешить доступ по ICMP введем команды в следующем порядке:


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

Рисунок 13 – попытка ssh и icmp подключения к U3 с U1.

6. Запретить подключение к Ub1 по порту 80. Настроить логирование попыток подключения по 80-му порту.

С помощью следующей команды запретим по 80 порту подключение к U1. Также настроим логирование попыток подключения по данному порту.

```
sudo iptables -A INPUT -p tcp --dport 80 -j LOG --log-prefix
"Package received at port 80"
```

```
sudo iptables -A INPUT -p tcp --dport 80 -j REJECT
```

Первое правило сначала записывает событие, означающее, что происходит подключение по 80 порту. Второе правило блокирует его. Посмотреть логи можно в этом файле: `/var/log/kern.log`.

telnet – команда для проверок, связанных с ТСР-протоколом.

```
lera2003@Valeriya:~$ telnet 15.0.3.14 80
Trying 15.0.3.14...
telnet: Unable to connect to remote host: Connection refused
```

Рисунок 14 – подключение к U1 через 80 порт.

[illegible]

Рисунок 15 – содержимое файла /var/log/kern.log

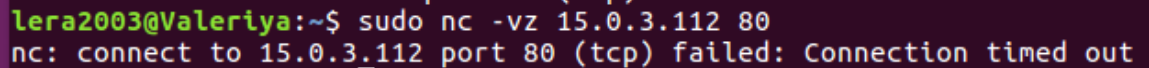
7. Заблокировать доступ по 80-му порту к Ub3 с Ub1 по его МАСадресу.
Заблокируем доступ по 80-му порту к U3 с U1 по его МАСадресу.

MACадрес U3 - 08:00:27:aa:bb:cc.

Введем следующую команду, чтобы осуществить ранее описанные действия:

```
sudo iptables -A INPUT -p tcp --sport 80 -m mac --mac-source 08:00:27:aa:bb:cc -j REJECT
```

Данное правило запретит прием пакетов для 80 порта от узла с указанным MAC-адресом.

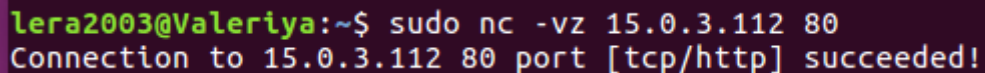


```
lera2003@Valeriya:~$ sudo nc -vz 15.0.3.112 80
nc: connect to 15.0.3.112 port 80 (tcp) failed: Connection timed out
```

Рисунок 16 – подключение по 80 порту с U3 к U1.

Изменим MACадрес U3 и повторим эксперимент.

Измененный MACадрес U3 – 08:00:27:ab:b8:eb.



```
lera2003@Valeriya:~$ sudo nc -vz 15.0.3.112 80
Connection to 15.0.3.112 80 port [tcp/http] succeeded!
```

Рисунок 17 – подключение по 80 порту с U3 к U1 после изменения MACадреса.

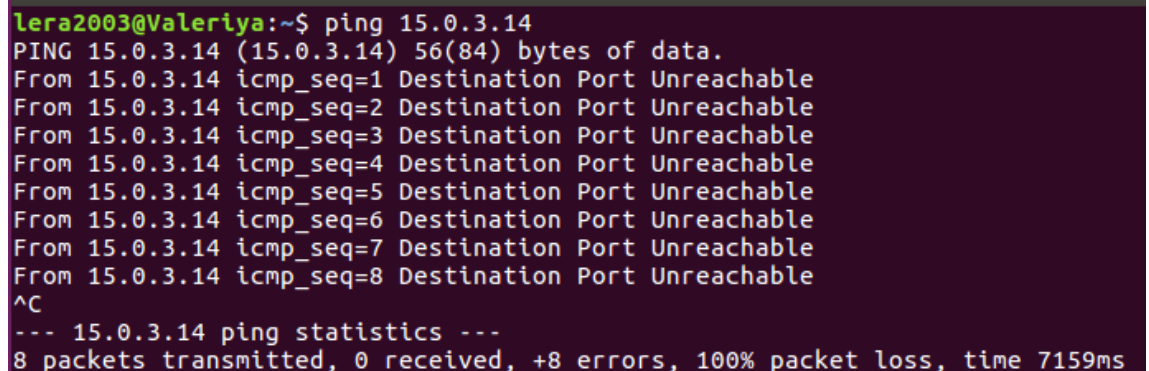
Таким образом, запросы блокируются с конкретного MAC. IP адрес роли не играет.

8. Полностью закрыть доступ к Ub1. Разрешить доступ для Ub3 к Ub1, используя диапазон портов 20–79.

Полностью закроем доступ к U1, лишь разрешив доступ для U3 к U1 по диапазону портов 20-79. Для этого введем команду:

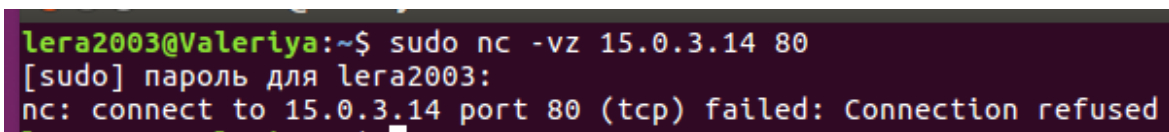
```
sudo iptables -A INPUT -p tcp -s 15.0.3.112 --dport 20:79 -j ACCEPT
sudo iptables -A INPUT -j REJECT
```

Проверим корректность работы данного правила.



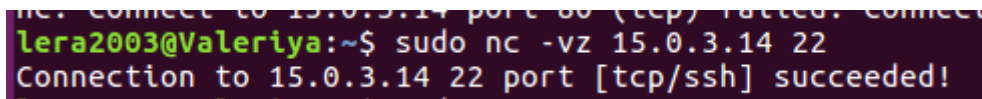
```
lera2003@Valeriya:~$ ping 15.0.3.14
PING 15.0.3.14 (15.0.3.14) 56(84) bytes of data.
From 15.0.3.14 icmp_seq=1 Destination Port Unreachable
From 15.0.3.14 icmp_seq=2 Destination Port Unreachable
From 15.0.3.14 icmp_seq=3 Destination Port Unreachable
From 15.0.3.14 icmp_seq=4 Destination Port Unreachable
From 15.0.3.14 icmp_seq=5 Destination Port Unreachable
From 15.0.3.14 icmp_seq=6 Destination Port Unreachable
From 15.0.3.14 icmp_seq=7 Destination Port Unreachable
From 15.0.3.14 icmp_seq=8 Destination Port Unreachable
^C
--- 15.0.3.14 ping statistics ---
8 packets transmitted, 0 received, +8 errors, 100% packet loss, time 7159ms
```


Рисунок 18 – попытка отправки запроса с U2 на U1.



```
lera2003@Valeriya:~$ sudo nc -vz 15.0.3.14 80
[sudo] пароль для lera2003:
nc: connect to 15.0.3.14 port 80 (tcp) failed: Connection refused
```

Рисунок 19 – недоступность для U3 к U1 по 80 порту.



```
lera2003@Valeriya:~$ sudo nc -vz 15.0.3.14 22
Connection to 15.0.3.14 22 port [tcp/ssh] succeeded!
```

Рисунок 20 – доступ для U3 к U1 по 22 порту(ssh).

9. Разрешить только одно ssh-подключение к Ub3.

Для того чтобы разрешить только одно ssh подключение введем следующую команду:

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

--syn – первый пакет, который отправляется при установке нового соединения.

-m – подключает указанный модуль.

connlimit – позволяет ограничить количество параллельных подключений к серверу.

--connlimit-above 1 – совпадение, если количество соединений превышает один.

--connlimit-mask 0 – группировка хостов, используя длину префикса.

Для проверки корректности работы правила подключимся с помощью ssh соединения к U1 с U3, и не выходя из сессии попробуем сделать тоже самое с U2.

```

lera2003@Valeriya:~$ ssh 15.0.3.112
The authenticity of host '15.0.3.112 (15.0.3.112)' can't be established.
ECDSA key fingerprint is SHA256:VX6kCL3sDczoETLWp20FCWH65ciI/UUaBIYWpvJ/vYE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '15.0.3.112' (ECDSA) to the list of known hosts.
lera2003@15.0.3.112's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-142-generic x86_64)

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

Могут быть обновлены 42 пакета.
2 обновления касаются безопасности системы.

Last login: Thu Mar 16 06:14:15 2023
lera2003@Valeriya:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:ab:b8:eb
          inet addr:15.0.3.112  Bcast:15.0.3.255  Mask:255.255.255.0

```

21 рисунок – подключение по ssh с U3 к U1.

```

lera2003@Valeriya:~$ ssh 15.0.3.112
ssh: connect to host 15.0.3.112 port 22: Connection refused

```

22 рисунок – параллельное подключение по ssh с U2 на U1.

Таким образом, правило, описанное выше разрешает одновременное подключение только одно подключение по ssh.

Выводы.

В ходе работы были изучены принципы работы с сетевыми экранами. Были развёрнуты три виртуальные машины, и с помощью утилиты iptables был выполнен ряд задач по фильтрации сетевого трафика.