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

ОТЧЕТ

по лабораторной работе №7
по дисциплине «Сети и телекоммуникации»
Тема: Сетевые экраны. IPTABLES

Студент гр. 0382 _____ Корсунов А.А.

Преподаватель _____ Фирсов М.А.

Санкт-Петербург
2022

Цель работы.

Целью работы является изучение принципов работы с сетевыми экранами.

Задачи.

1. Создать три виртуальные машины (лаб. Работа № 1).

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

Порядок выполнения работы.

Требуется создать три виртуальные машины Ub1, UbR, Ub3. Необходимо решить следующие задачи:

1. **«Заблокировать доступ по IP-адресу ПК Ub1 к Ub3».** Продемонстрировать результаты с попыткой подключения Ub1 и Ub2 к Ub3.
2. **«Заблокировать доступ по порту X на Ub1».** Продемонстрировать возможность доступа по ssh на Ub1 и невозможность доступа по порту X.
3. **«Разрешить доступ только по ssh на Ub2».** Продемонстрировать 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. Продемонстрировать результаты логирования.
7. **«Заблокировать доступ по порту Y к Ub3 с Ub1 по его MAC-адресу».** Продемонстрировать 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.

Вариант 12. X = 32; Y = 91; Z = 20-90

Выполнение работы.

Были созданы три виртуальные машины:

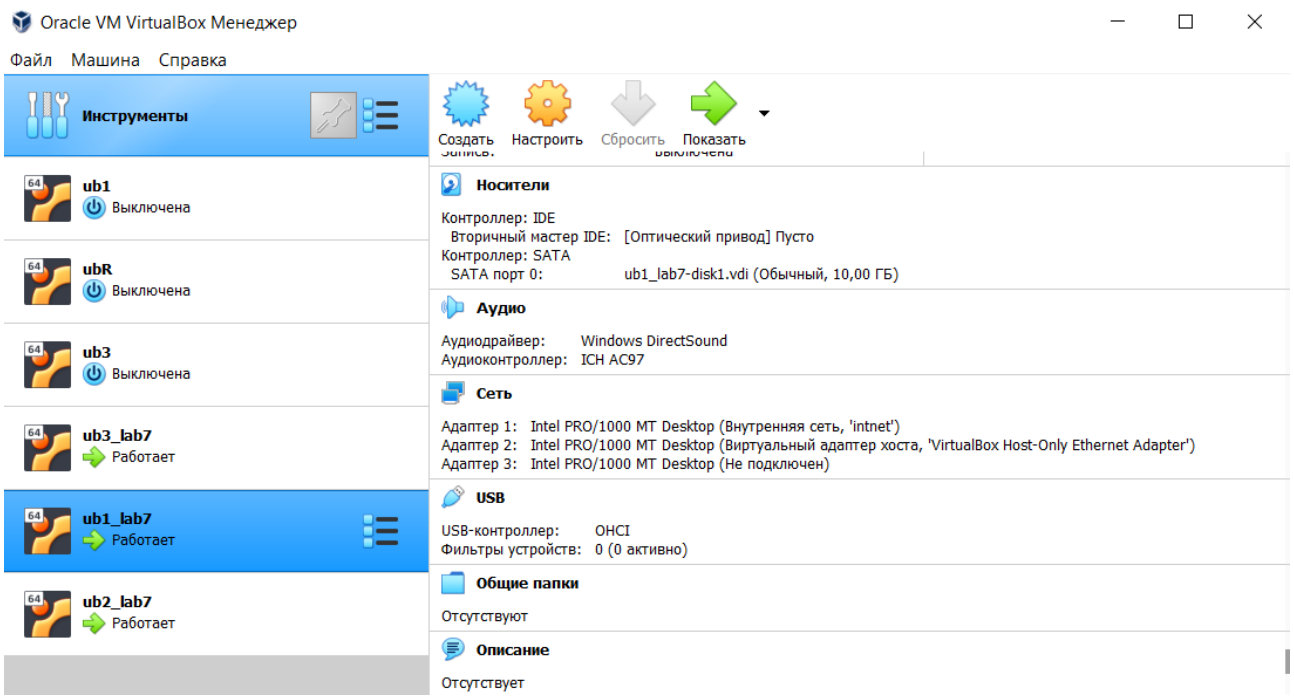


Рисунок 1 — Демонстрация работоспособности машины ub1_lab7

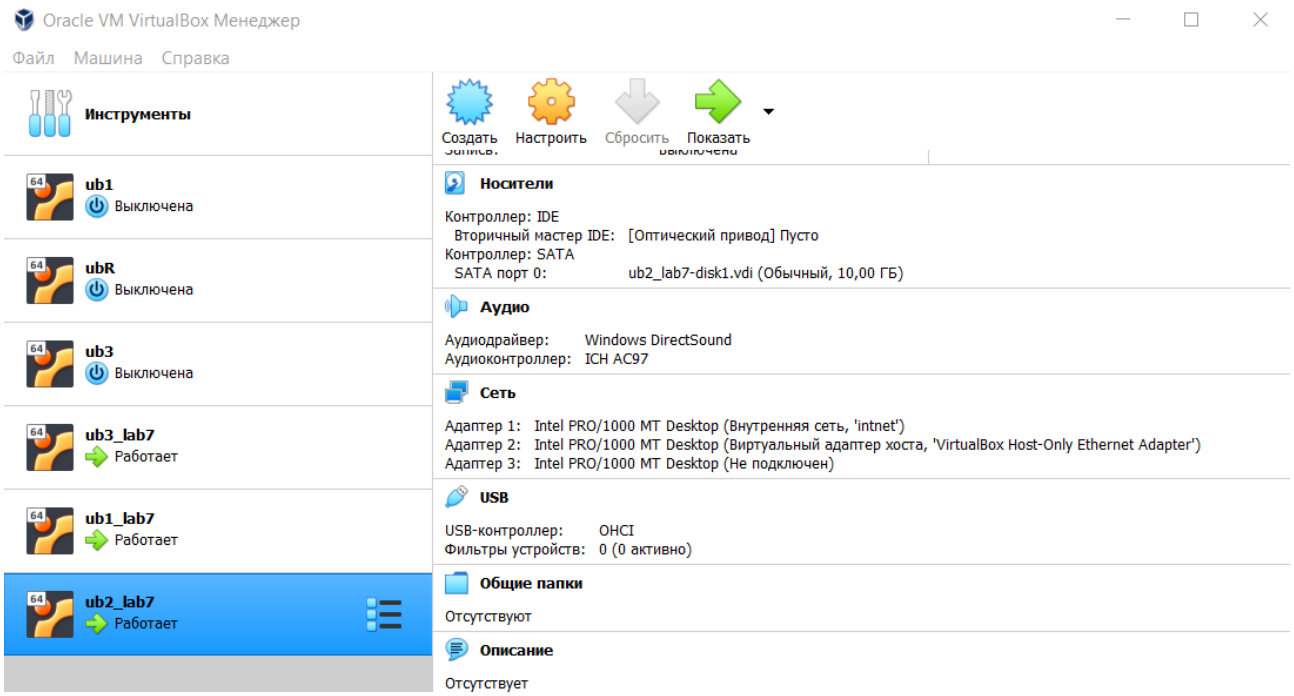


Рисунок 2 — Демонстрация работоспособности машины ub2_lab7

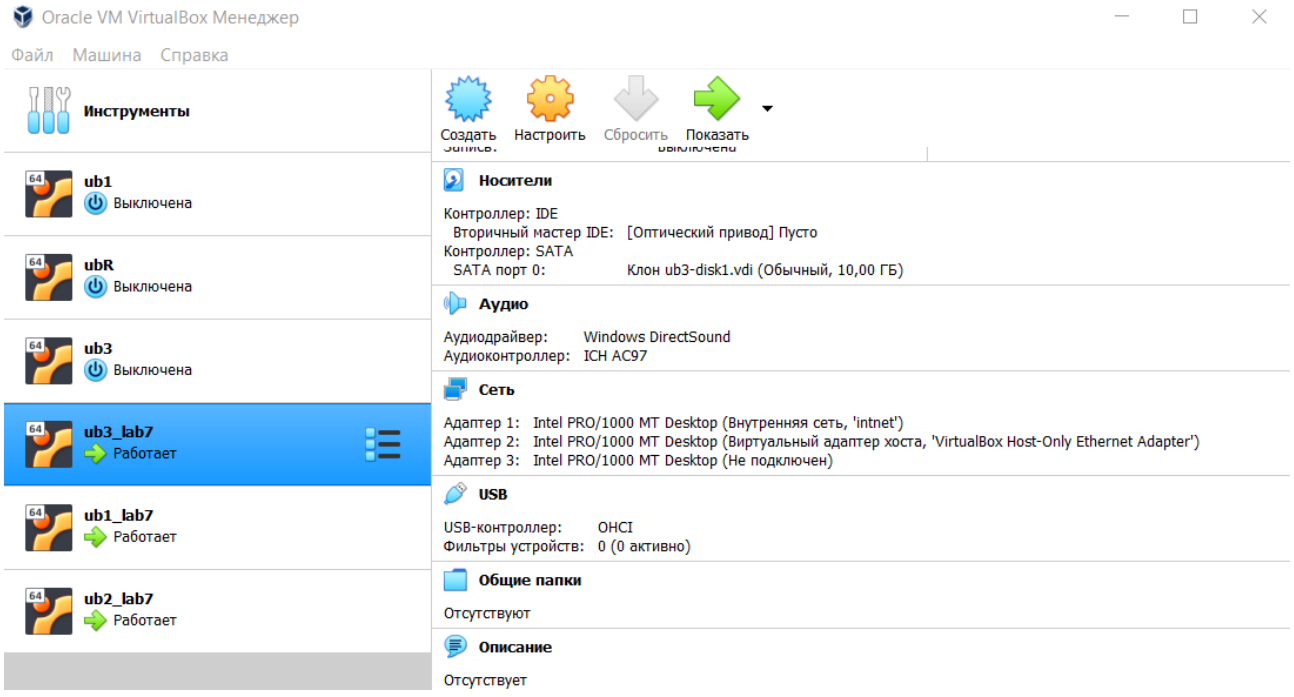


Рисунок 3 — Демонстрация работоспособности машины ub3_lab7

```
root@ub1_lab7:~# ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:96:fa:7b
          inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe96:fa7b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:316 (316.0 B)  TX bytes:11002 (11.0 KB)

enp0s8    Link encap:Ethernet  HWaddr 08:00:27:0e:27:b9
          inet addr:192.168.56.105  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe0e:27b9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7109 (7.1 KB)  TX bytes:4548 (4.5 KB)

lo        Link encap:Локальная петля (Loopback)
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:12257 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12257 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:908688 (908.6 KB)  TX bytes:908688 (908.6 KB)

root@ub1_lab7:~#
```

Рисунок 4 — Конфигурация сетевых интерфейсов на ub1_lab7

```
root@ub2_lab7:~# ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:4f:d1:1d
          inet addr:10.0.0.2  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4f:d11d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:131 errors:0 dropped:0 overruns:0 frame:0
          TX packets:44 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:40930 (40.9 KB)  TX bytes:11062 (11.0 KB)

enp0s8    Link encap:Ethernet  HWaddr 08:00:27:cd:3c:68
          inet addr:192.168.56.107  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fecd:3c68/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:32265 (32.2 KB)  TX bytes:15462 (15.4 KB)

lo        Link encap:Локальная петля (Loopback)
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:50673 errors:0 dropped:0 overruns:0 frame:0
          TX packets:50673 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:3751488 (3.7 MB)  TX bytes:3751488 (3.7 MB)

root@ub2_lab7:~# _
```

Рисунок 5 — Конфигурация сетевых интерфейсов на ub2_lab7

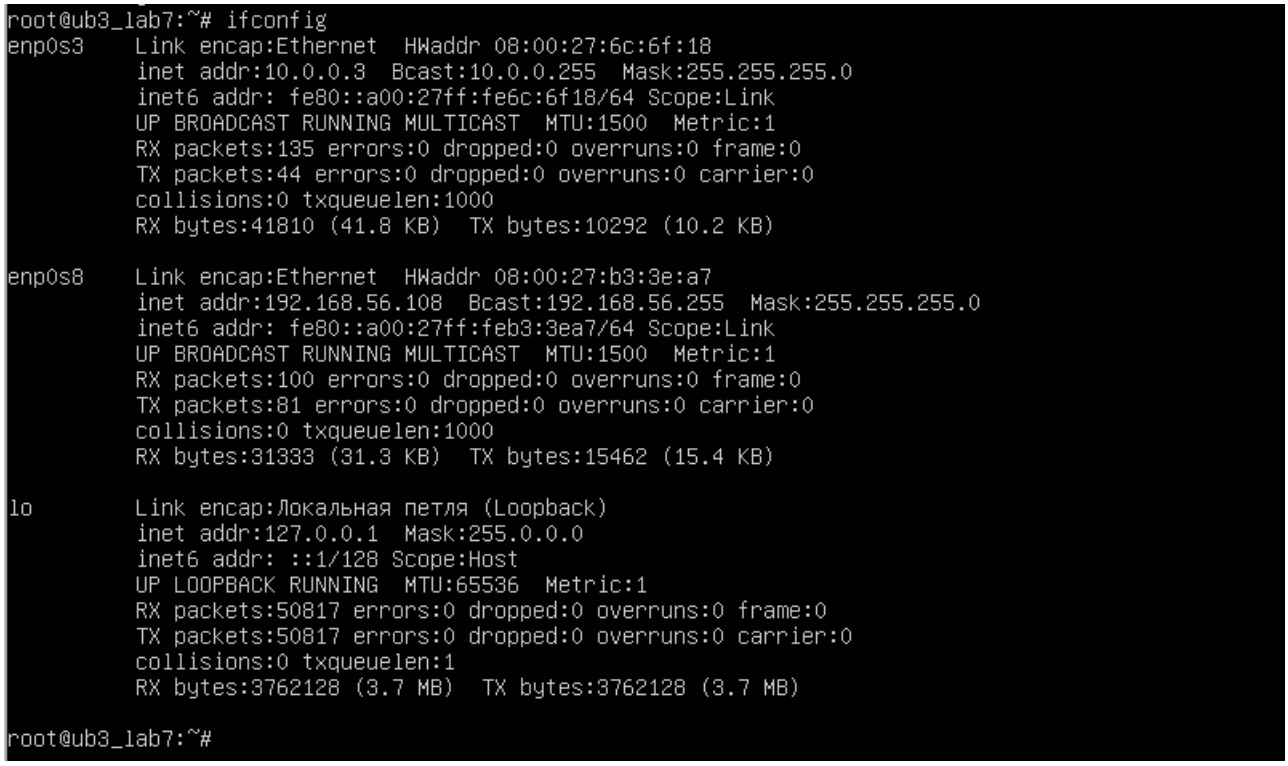


Рисунок 6 — Конфигурация сетевых интерфейсов на ub3_lab7

1. **«Заблокировать доступ по IP-адресу ПК Ub1 к Ub3».** Продемонстрировать результаты с попыткой подключения Ub1 и Ub2 к Ub3.

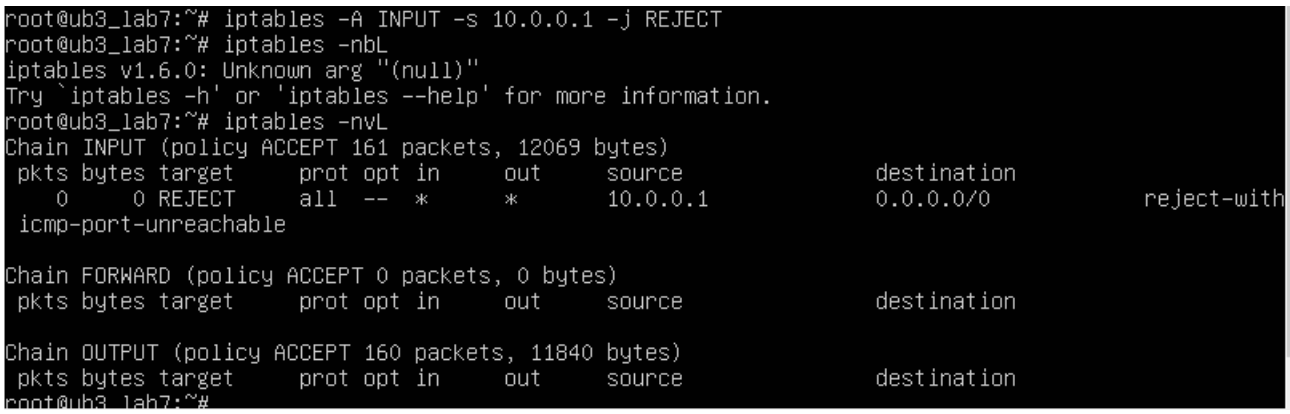


Рисунок 7 — Демонстрация блокировки всех входящих пакетов на ub3_lab7 с IP-адресом 10.0.0.1

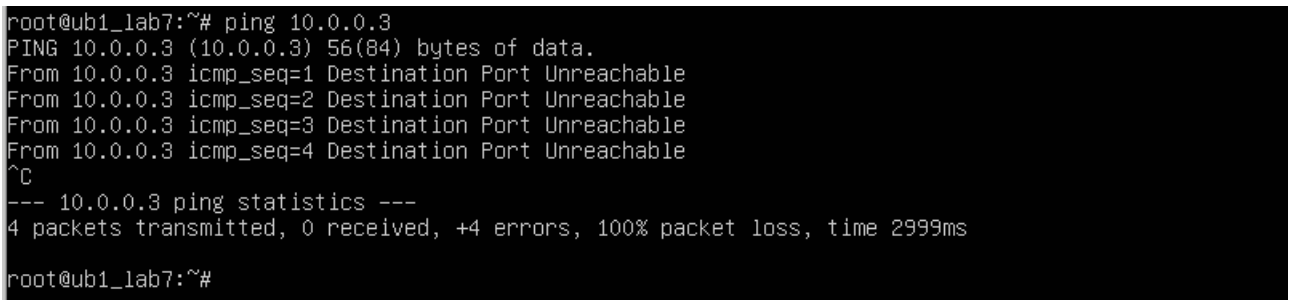


Рисунок 8 — Демонстрация невозможности пинга с IP-адреса 10.0.0.1 ub1_lab7 до ub3_lab7

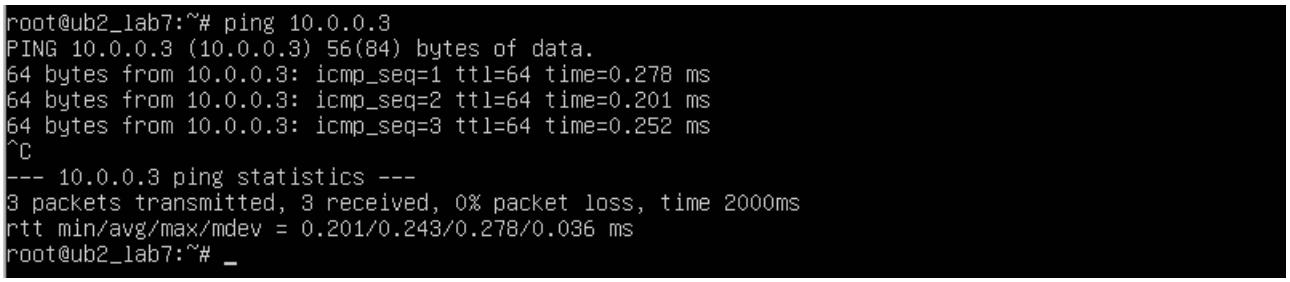


Рисунок 9 — Демонстрация успешных Echo-запросов с ub2_lab7 до ub3_lab7

2. **«Заблокировать доступ по порту X на Ub1».** Продемонстрировать возможность доступа по ssh на Ub1 и невозможность доступа по порту X.

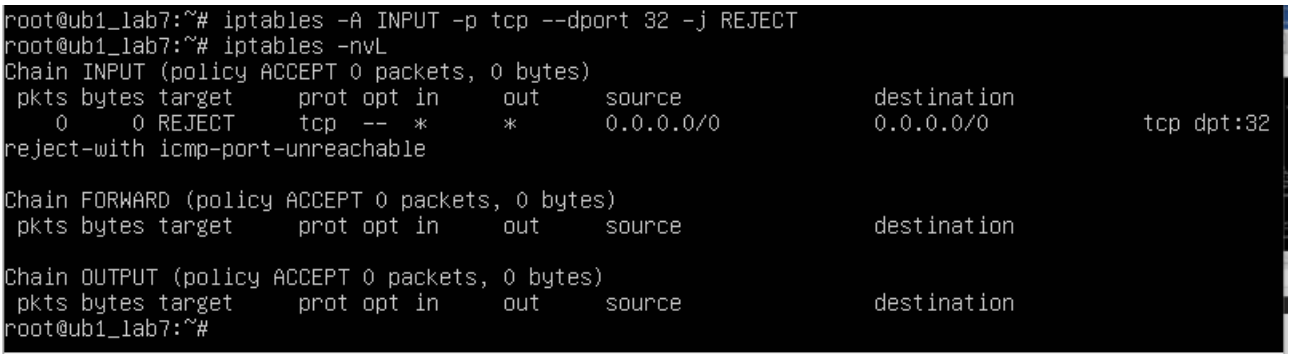


Рисунок 10 — Демонстрация блокировки для TCP-протокола 32-го порта назначения на ub1_lab7

Рисунок 11 — Демонстрация успешной установки удаленного доступа с ub2_lab7 до ub1_lab7 по ssh

Рисунок 12 — Демонстрация невозможности подключения к 10.0.0.1 по 32-му порту с ub2_lab7

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

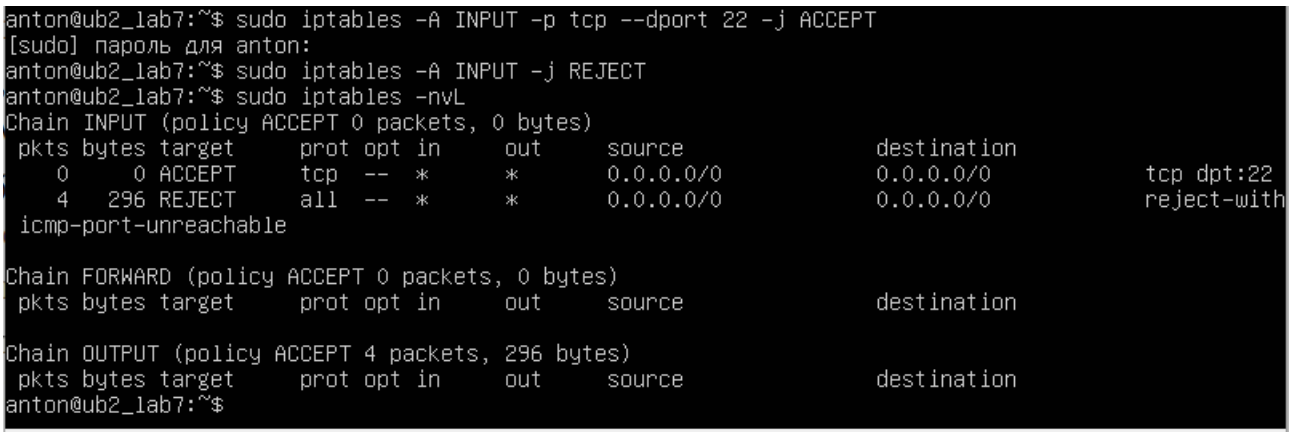


Рисунок 13 — Демонстрация допуска для TCP-протокола 22-го порта (ssh слушает 22-ой порт) и запрет всех входящих пакетов на ub2_lab7

Допуск до 22-го порта — первое правило, поэтому оно будет применяться раньше второго правила.

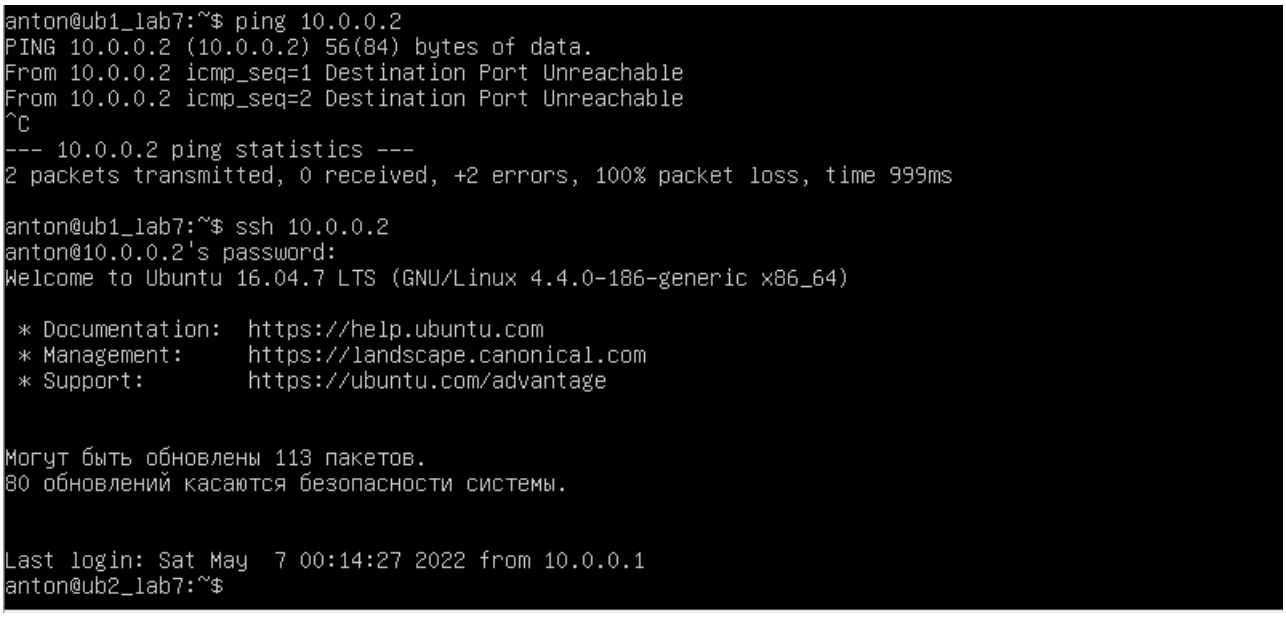


Рисунок 14 — Демонстрация невозможности пинга и успешной установки удаленного доступа с ub1 до ub2

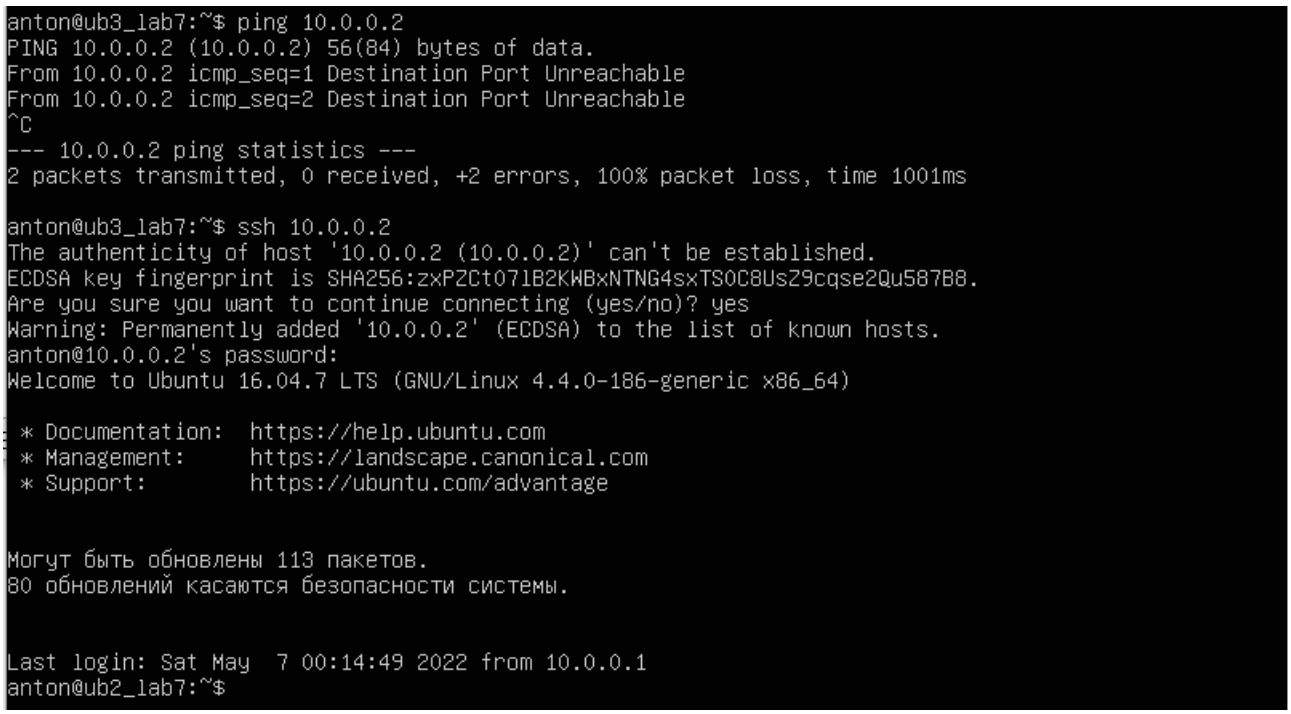


Рисунок 15 — Демонстрация невозможности пинга и успешной установки удаленного доступа с ub3 до ub2

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.

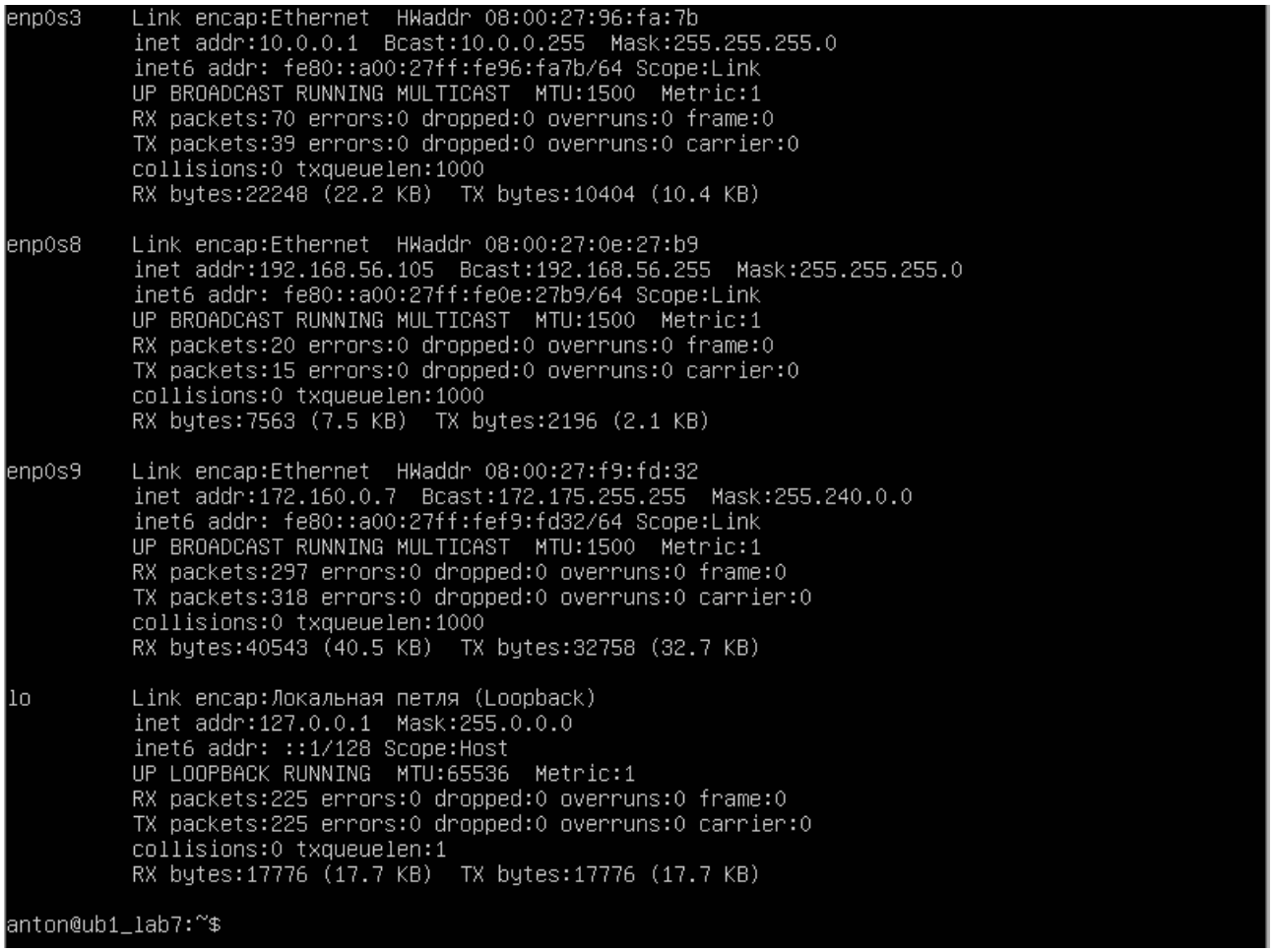


Рисунок 16 — Добавление интерфейса на ub1_lab7, который имеет доступ в Интернет

```
anton@ub1_lab7:~$ sudo iptables -A INPUT -s 8.8.8.8 -j REJECT
anton@ub1_lab7:~$ sudo iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     all  --  *      *       8.8.8.8              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
anton@ub1_lab7:~$
```

Рисунок 17 — Демонстрация запрета всех входящих пакетов с IP-адреса 8.8.8.8

```
anton@ub1_lab7:~$ 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 3999ms

anton@ub1_lab7:~$ _
```

Рисунок 18 — Пинг 8.8.8.8 с ub1_lab7

54	15.147604	167.86.70.20	192.168.5.60	ICMP	174	Destination unreachable (Port unreachable)
85	31.488549	192.168.5.60	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=280/6145, ttl=63 (reply in 86)
86	31.493048	8.8.8.8	192.168.5.60	ICMP	98	Echo (ping) reply id=0x0001, seq=280/6145, ttl=110 (request in 85)
93	32.487588	192.168.5.60	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=281/6401, ttl=63 (reply in 94)
94	32.492020	8.8.8.8	192.168.5.60	ICMP	98	Echo (ping) reply id=0x0001, seq=281/6401, ttl=110 (request in 93)
97	33.488368	192.168.5.60	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=282/6657, ttl=63 (reply in 98)
98	33.492817	8.8.8.8	192.168.5.60	ICMP	98	Echo (ping) reply id=0x0001, seq=282/6657, ttl=110 (request in 97)
101	34.488482	192.168.5.60	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=283/6913, ttl=63 (reply in 102)
102	34.492951	8.8.8.8	192.168.5.60	ICMP	98	Echo (ping) reply id=0x0001, seq=283/6913, ttl=110 (request in 101)
106	35.487727	192.168.5.60	8.8.8.8	ICMP	98	Echo (ping) request id=0x0001, seq=284/7169, ttl=63 (reply in 107)
107	35.492178	8.8.8.8	192.168.5.60	ICMP	98	Echo (ping) reply id=0x0001, seq=284/7169, ttl=110 (request in 106)

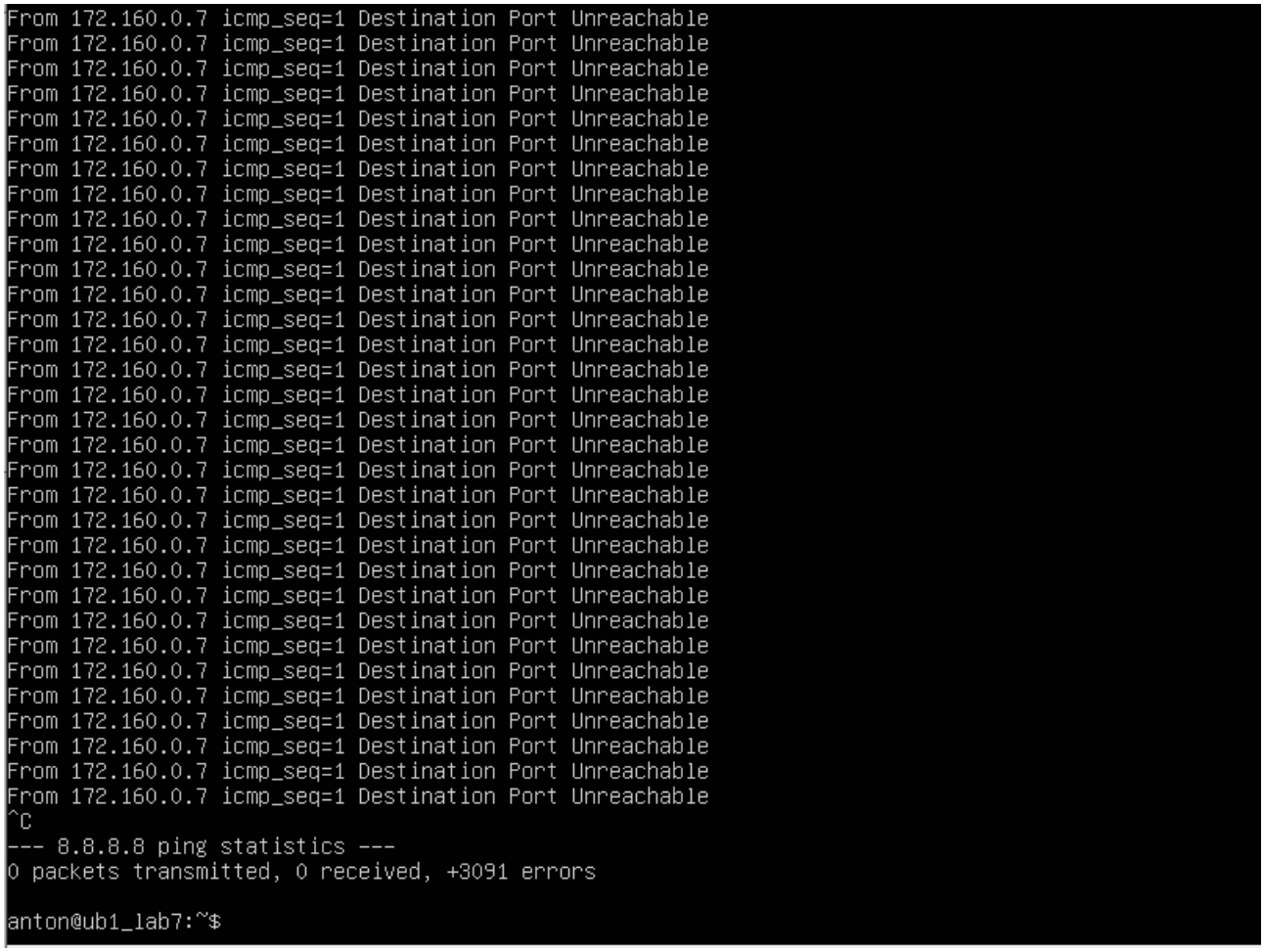
Рисунок 19 — Перехват трафика с помощью программы “Wireshark” в момент пинга с ub1_lab7

```
anton@ub1_lab7:~$ sudo iptables -D INPUT -s 8.8.8.8 -j REJECT
anton@ub1_lab7:~$ sudo iptables -A OUTPUT -d 8.8.8.8 -j REJECT
anton@ub1_lab7:~$ sudo iptables -nvL
Chain INPUT (policy ACCEPT 0 packets, 0 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 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     all  --  *      *       0.0.0.0/0            8.8.8.8              reject-with
 icmp-port-unreachable
anton@ub1_lab7:~$
```

Рисунок 20 - Демонстрация запрета всех исходящих пакетов в IP-адрес 8.8.8.8



```
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
From 172.160.0.7 icmp_seq=1 Destination Port Unreachable
^C
--- 8.8.8.8 ping statistics ---
0 packets transmitted, 0 received, +3091 errors

anton@ub1_lab7:~$
```

Рисунок 21 — Пинг 8.8.8.8 с ub1_lab7 (во втором случае)

icmp

Рисунок 22 — Перехват трафика с помощью программы “Wireshark” в момент пинга с ub1_lab7

Какой вариант эффективнее?

Ответ: эффективнее второй вариант в силу того, что во втором варианте пакет отбрасывается на узле, на котором он создается, (т. е. он даже не попадает на 8.8.8.8), в первом же варианте пакет отсылается на 8.8.8.8, там он принимается, обрабатывается, после чего отправляется ответ, а уже ответ с пакетом отбрасывается на узле на узле ub1 в цепочке INPUT.

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

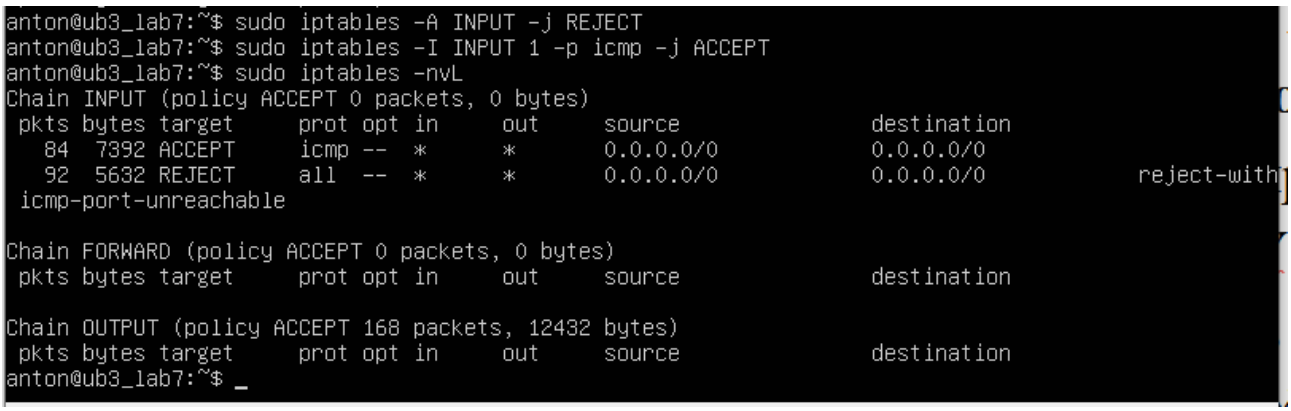


Рисунок 23 — Демонстрация запрета всех входящих пакетов, а также разрешение всех пакетов ICMP-протокола

В силу того, что порядок правил в цепочках имеет значение, правило с ICMP-протоколом было вставлено на первую строчку

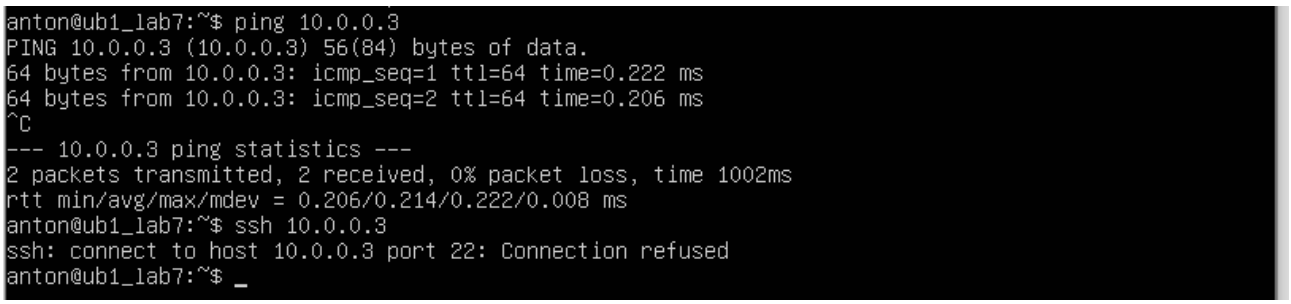


Рисунок 24 — Демонстрация успешных Echo-запросов (протокол icmp) и невозможности подключения ssh (протокол tcp) с ub1_lab7

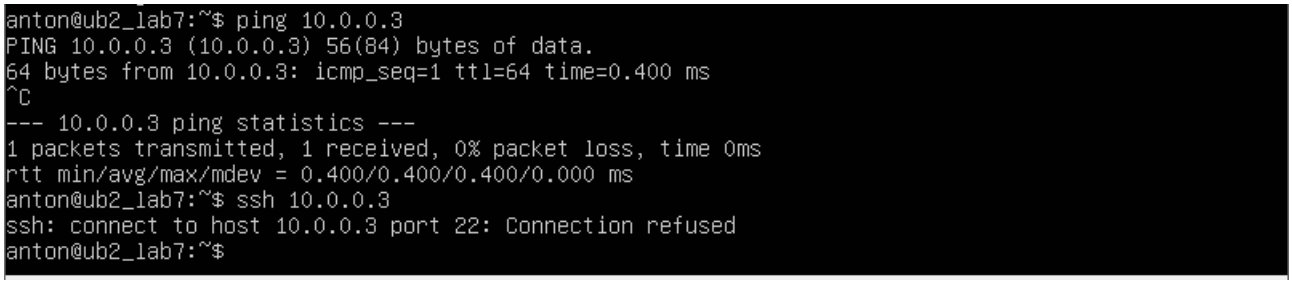


Рисунок 25 — Демонстрация успешных Echo-запросов (протокол icmp) и невозможности подключения ssh (протокол tcp) с ub2_lab7

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

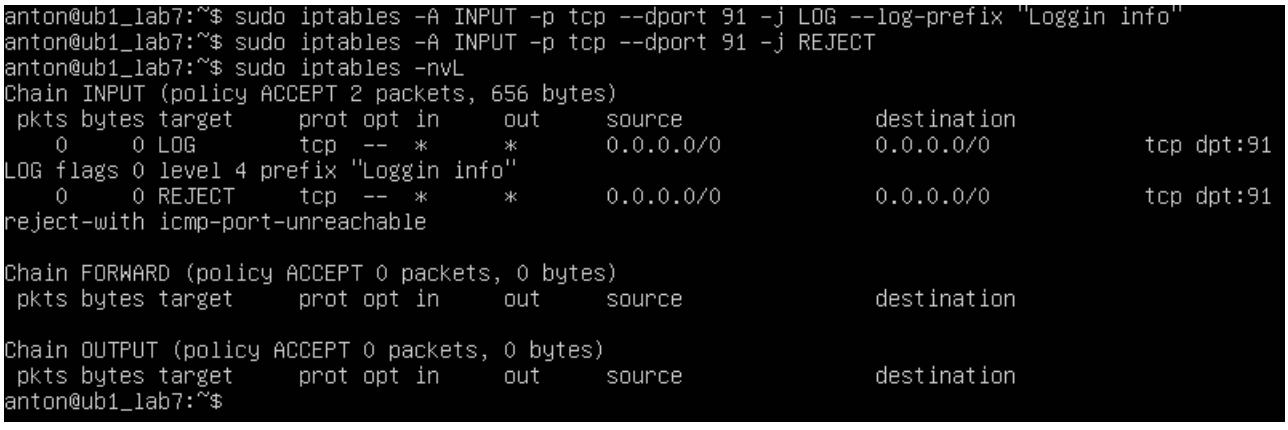


Рисунок 26 — Настройка логирования и запрет для порта 91 TCP-протокола всех входящих пакетов на ub1_lab7

```
anton@ub2_lab7:~$ nc -vz 10.0.0.1 91
nc: connect to 10.0.0.1 port 91 (tcp) failed: Connection refused
anton@ub2_lab7:~$
```

Рисунок 27 — Демонстрация невозможности подключения к 10.0.0.1 по 91-му порту с ub2_lab7 до ub1_lab7

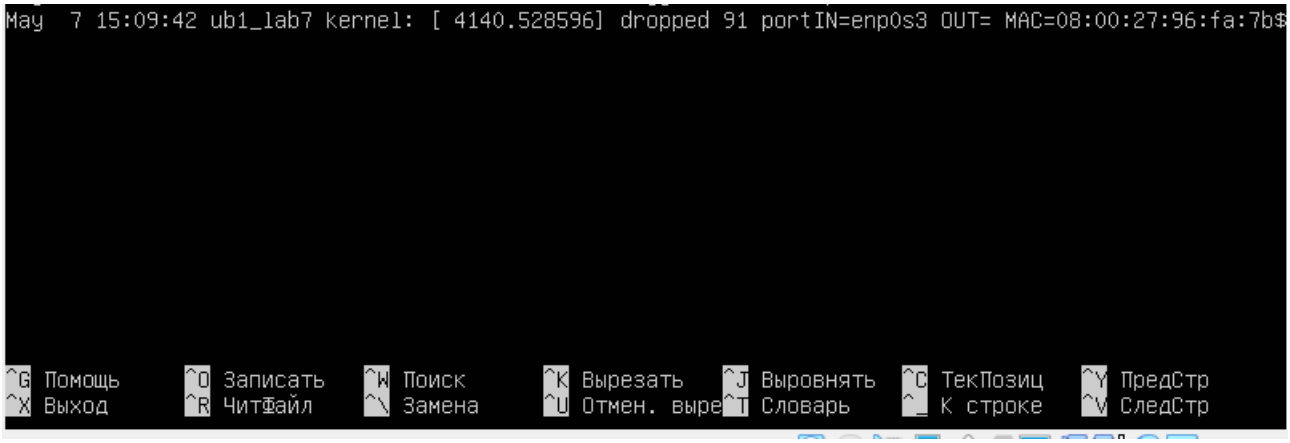


Рисунок 28 — Последняя строка в файле var/log/kern.log

7. **«Заблокировать доступ по порту Y к Ub3 с Ub1 по его MAC-адресу».** Продемонстрировать результат, сменить MAC-адрес на Ub3 и продемонстрировать успешное подключение к Ub3 по порту Y.

```
anton@ub1_lab7:~$ sudo iptables -A INPUT -m mac --mac-source 08:00:27:6c:6f:18 -p tcp --dport 91 -j
REJECT
anton@ub1_lab7:~$ sudo iptables -nvL
Chain INPUT (policy ACCEPT 1 packets, 328 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           MAC 08:00:2
7:6C:6F:18 tcp dpt:91 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
anton@ub1_lab7:~$
```

Рисунок 29 — Демонстрация запрета доступа по порту 91 к ub3_lab7 с ub1_lab7 по его MAC-адресу

Рисунок 30 — Демонстрация невозможности подключения к 10.0.0.3 по 91-му порту с ub1_lab7 до ub3_lab7 (пакеты доходят до ub3_lab7, на ub3_lab7 формируется и отправляется ответ к ub1_lab7, а там он дропается при прохождении цепочки правил INPUT)

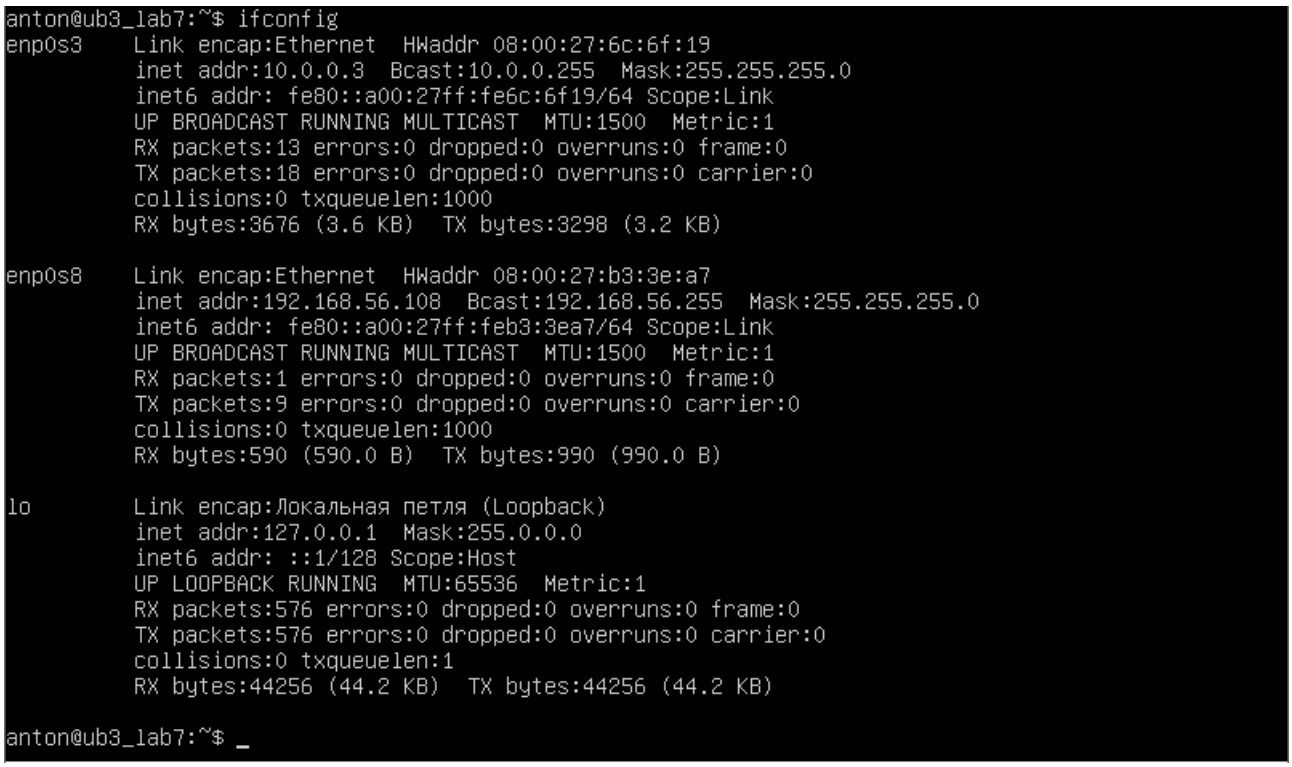


Рисунок 31 — Смена MAC-адреса enp0s3 на ub3_lab7

Рисунок 32 - Демонстрация успешного подключения к 10.0.0.3 по 91-му порту с ub1_lab7 по ub3_lab7

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.

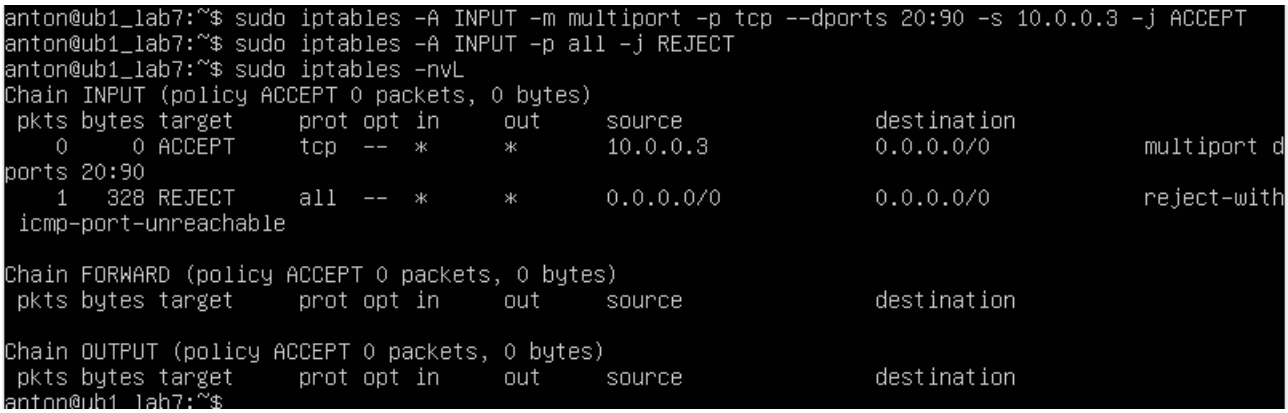


Рисунок 33 — Демонстрация доступа с IP-адреса 10.0.0.3 ub3_lab7 до ub1_lab7 по портам 20-90 и запрет подключений по всем портам (первое правило стоит первым, значит оно и будет применяться первым)

Рисунок 34 - Демонстрация невозможности подключения к 10.0.0.1 по 91-му порту

Рисунок 35 — Демонстрация успешной установки удаленного доступа до ub1_lab7 с ub3_lab7

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

```
anton@ub3_lab7:~$ sudo iptables -A INPUT -p tcp --syn --dport 22 -m connlimit --connlimit-above 1 --
connlimit-mask 24 -j REJECT
[sudo] пароль для anton:
anton@ub3_lab7:~$ sudo iptables -nvL
Chain INPUT (policy ACCEPT 161 packets, 12168 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/24 > 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 160 packets, 11840 bytes)
 pkts bytes target     prot opt in     out     source               destination
anton@ub3_lab7:~$
```

Рисунок 36 — Ограничение одновременных подключений к порту 22 (connlimit позволяет ограничивать число одновременных соединений TCP)

```
anton@ub1_lab7:~$ ssh 10.0.0.3
anton@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: Sat May  7 16:44:10 2022 from 10.0.0.2
anton@ub3_lab7:~$ _
```

Рисунок 37 — Демонстрация успешной установки удаленного доступа с ub1_lab7 до ub3_lab7

```
anton@ub2_lab7:~$ ssh 10.0.0.3
ssh: connect to host 10.0.0.3 port 22: Connection refused
anton@ub2_lab7:~$
```

Рисунок 38 — Демонстрация невозможности открытия соединения с ub2_lab7 до ub3_lab7

Вывод.

Было произведено изучение принципов работы с сетевыми экранами.