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

ОТЧЕТ

по лабораторной работе №7

по дисциплине «Сети и телекоммуникации»

Тема: Сетевые экраны. Iptables

Студент гр. 0303 _____ Калмак Д.А.

Преподаватель _____ Борисенко К.А.

Санкт-Петербург

2022

Цель работы.

Изучить принципы работы с сетевыми экранами. Научиться блокировать и разрешать прием и отправку пакетов с помощью iptables, настраивать логирование событий.

Порядок выполнения работы.

1. Создать три виртуальные машины (лаб. работа № 1).
2. Заблокировать доступ по IP-адресу Ub1 к Ub3.
3. Заблокировать доступ по порту X на Ub1.
4. Заблокировать доступ к порту X на Ub3 от UbR. Проверить возможность доступа с Ub1.
5. Полностью запретить доступ к Ub3. Разрешить доступ к порту X.
6. С помощью правила по умолчанию обеспечить блокировку всех входящих и исходящих пакетов узла Ub3, исключая пакеты управления сетью (протокол ICMP). Убедиться, что Ub3 принимает и отвечает на запросы команды ping, но не отвечает на запросы протокола TCP.
7. Запретить подключение к Ub1 по порту X. Настроить логгирование попыток подключения по порту X.
8. Заблокировать доступ по порту X к Ub3 с Ub1 по его MAC-адресу.
9. Полностью закрыть доступ к Ub1. Разрешить доступ для Ub3 к Ub1, используя диапазон портов X.
10. Разрешить только одно ssh подключение к UbR.

Выполнение работы.

1. Создадим три виртуальные машины и настроим их.

   Настройки ub1, ub2 и ub3 представлены на рис. 1.

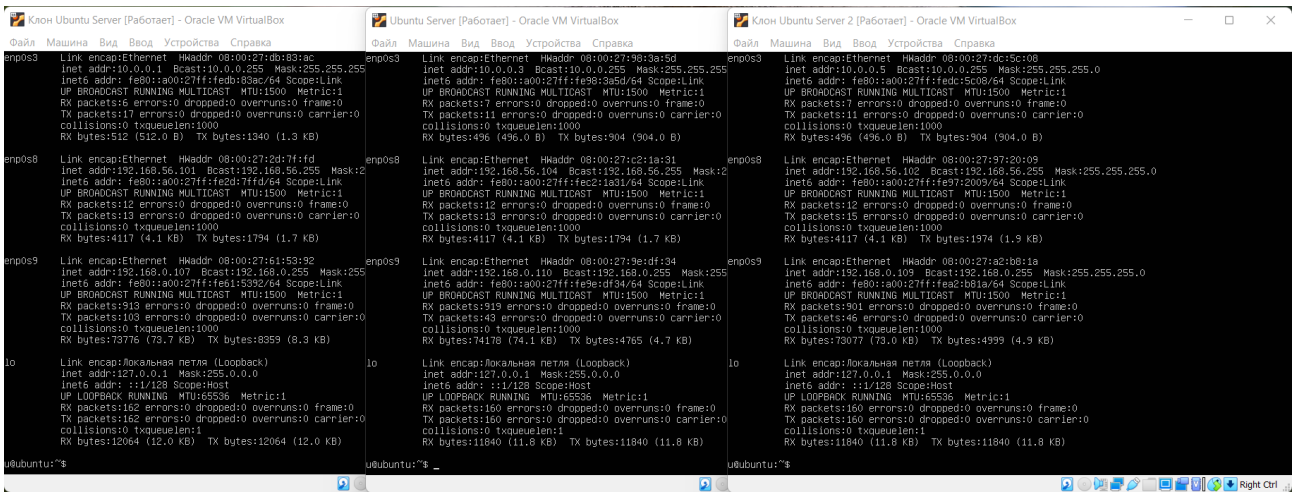

Рисунок 1 – Виртуальные машины ub1, ub2 и ub3

2. Заблокируем доступ по IP-адресу 10.0.0.5 Ub1 к Ub3. (см. рис. 2)

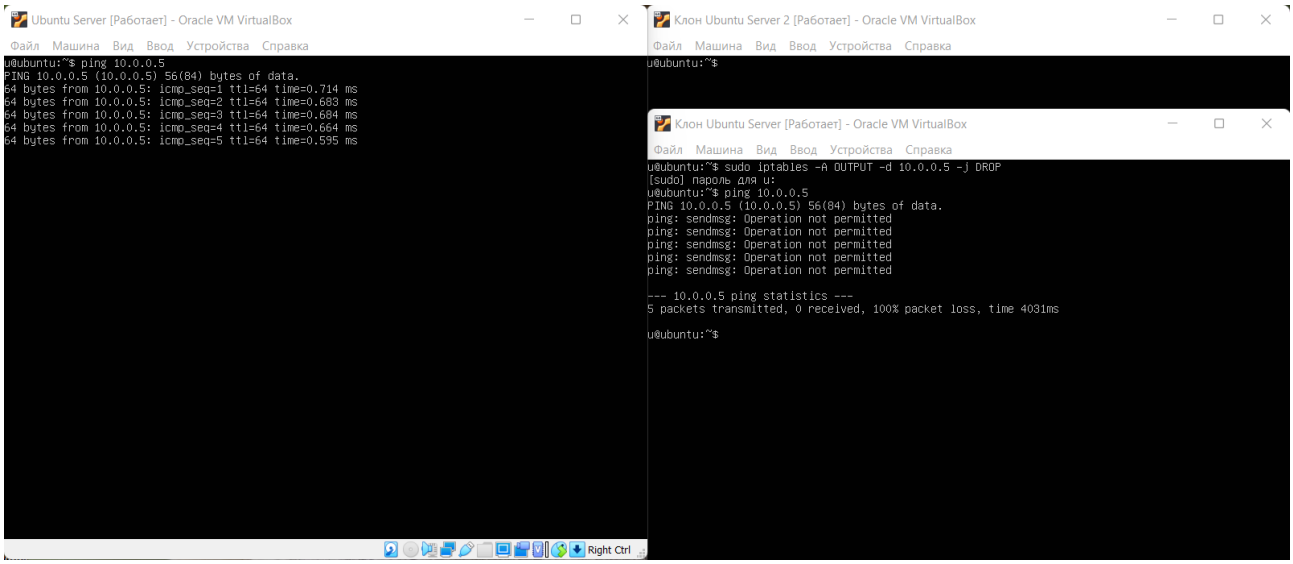

Рисунок 2 – Заблокирован доступ по IP-адресу 10.0.0.5 Ub1 к Ub3

3. Заблокируем доступ по порту 29 на Ub1. (см. рис. 3-4)

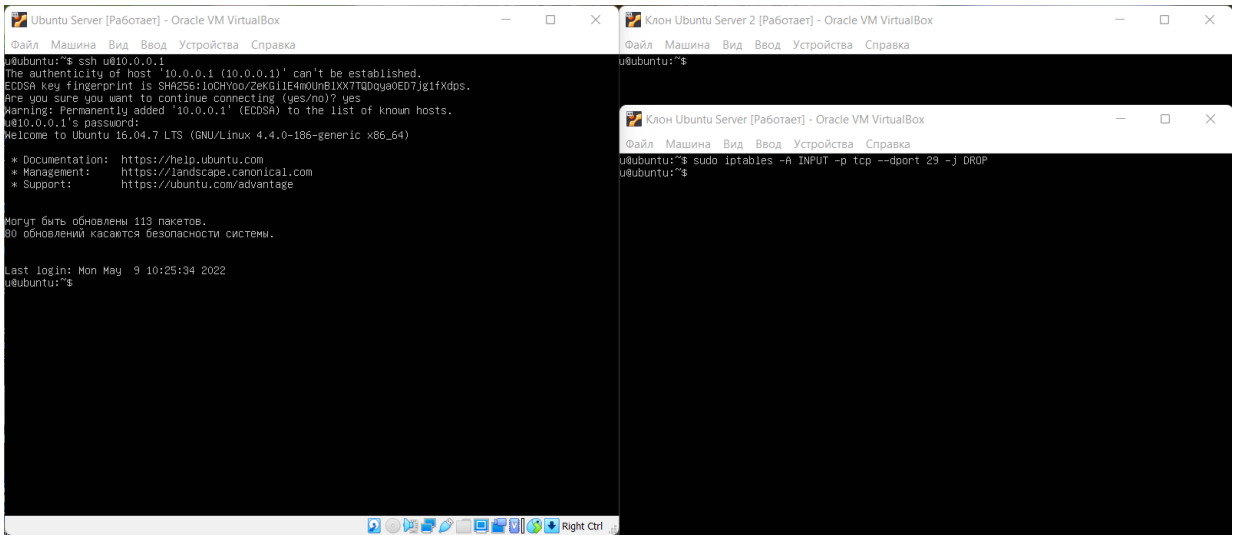

Рисунок 3 – Заблокирован доступ по порту 29 на Ub1 и остался доступ соединения по ssh

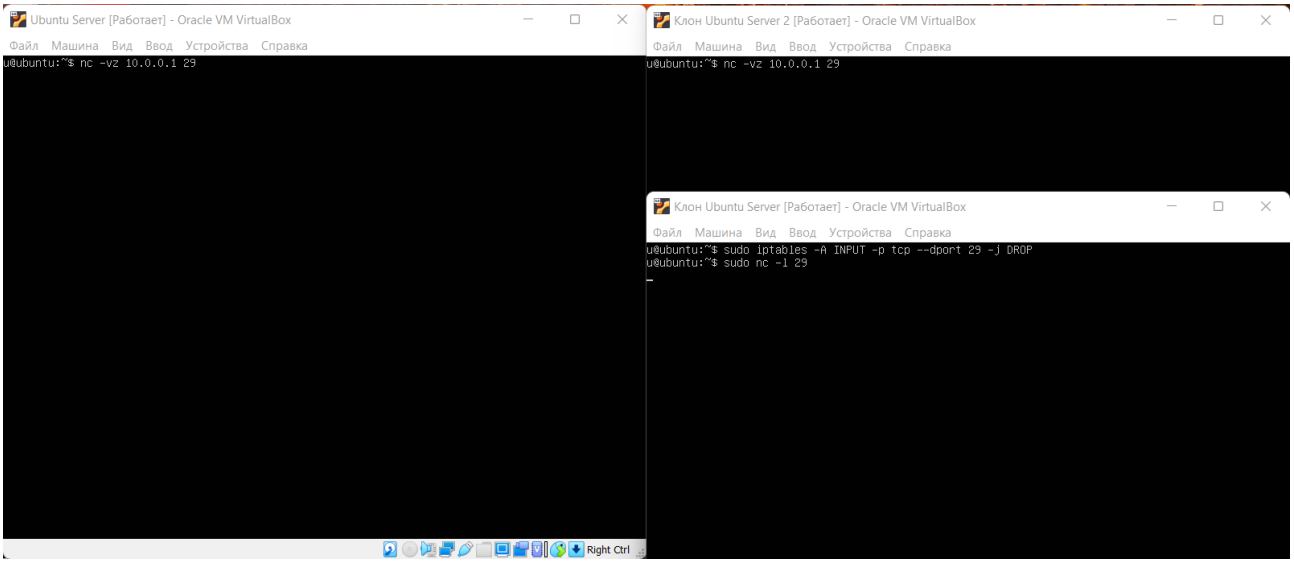

Рисунок 4 – Заблокирован доступ по порту 29 на Ub1 и к нему доступа нет

4. Заблокируем доступ к порту 79 на Ub3 от UbR. Есть доступ к Ub1. (см. рис. 5)

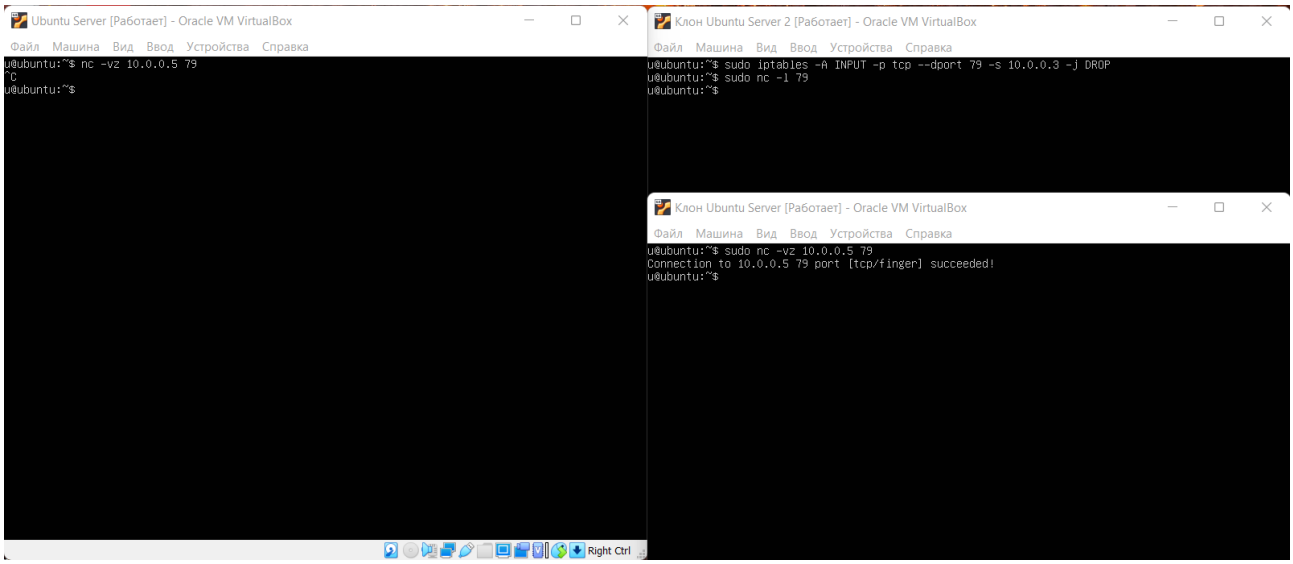

Рисунок 5 – Заблокирован доступ к порту 79 на Ub3 от UbR и доступ к порту 79 у Ub1 остался

5. Полностью запретим доступ к Ub3. Разрешим доступ к порту 29. (см. рис. 6)

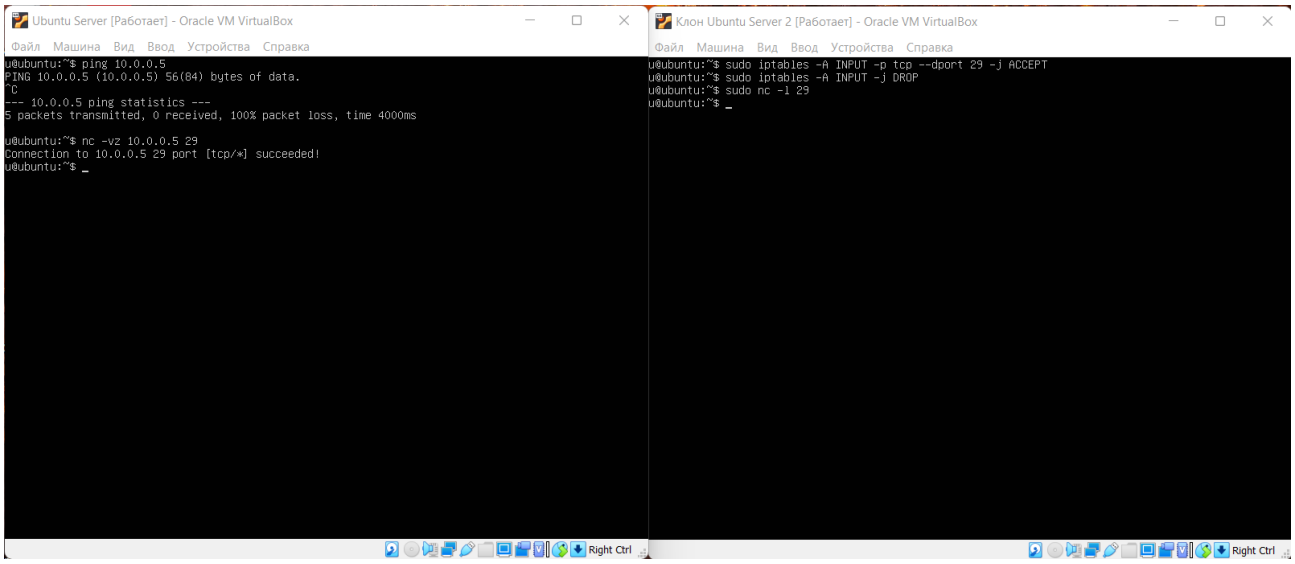

Рисунок 6 – Полностью запрещен доступ к Ub3 и разрешен доступ к порту 29

6. С помощью правила по умолчанию обеспечим блокировку всех входящих и исходящих пакетов узла Ub3, исключая пакеты управления сетью (протокол ICMP). Ub3 принимает и отвечает на запросы команды ping, но не отвечает на запросы протокола TCP. (см. рис. 7)

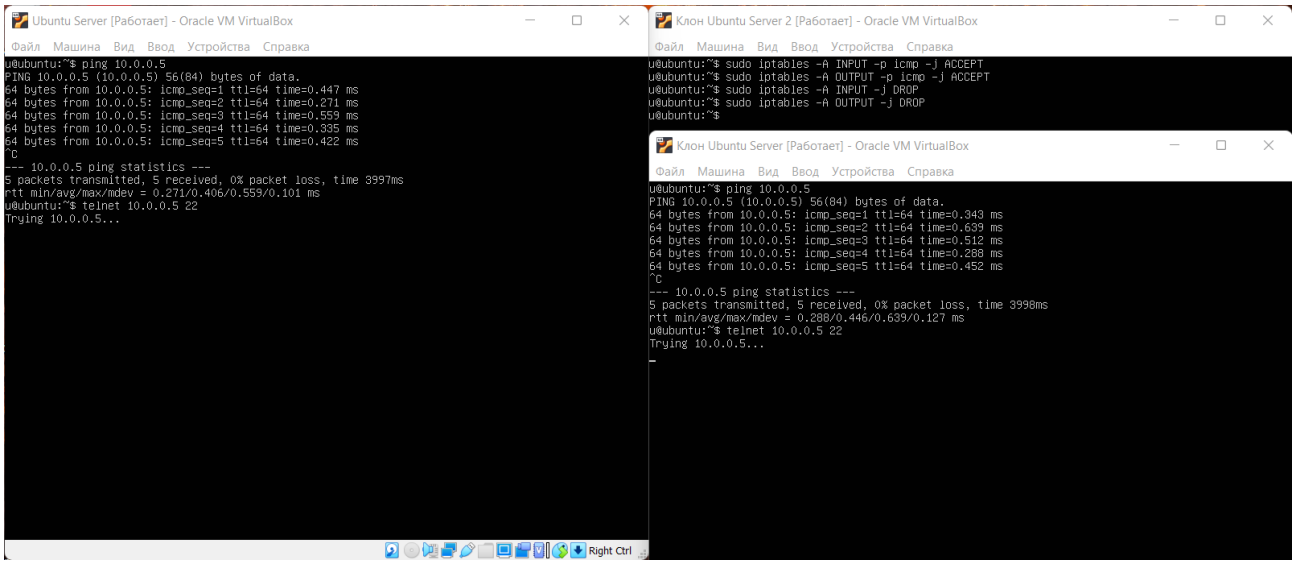

Рисунок 7 – Обеспечена блокировка всех входящих и исходящих пакетов узла Ub3, исключая пакеты управления сетью (протокол ICMP). Ub3 принимает и отвечает на запросы команды ping, но не отвечает на запросы протокола TCP

7. Запретим подключение к Ub1 по порту 79. Настроим логгирование попыток подключения по порту 79. (см. рис. 8-9)

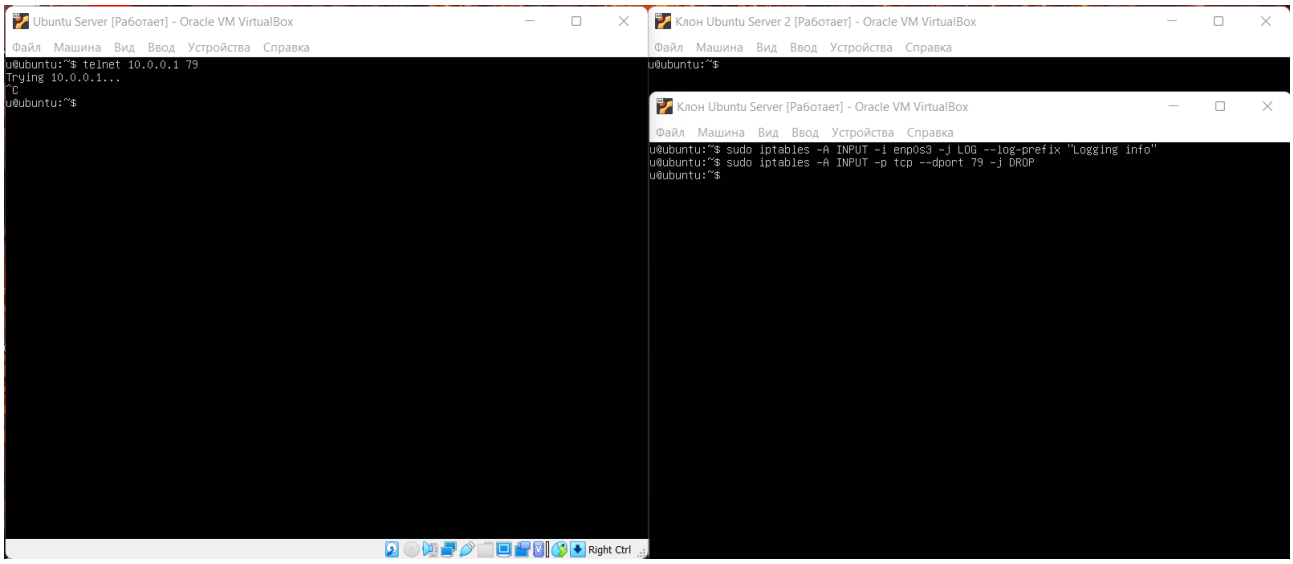

Рисунок 8 – Запрещен подключение к Ub1 по порту 79. Доступа к нему нет

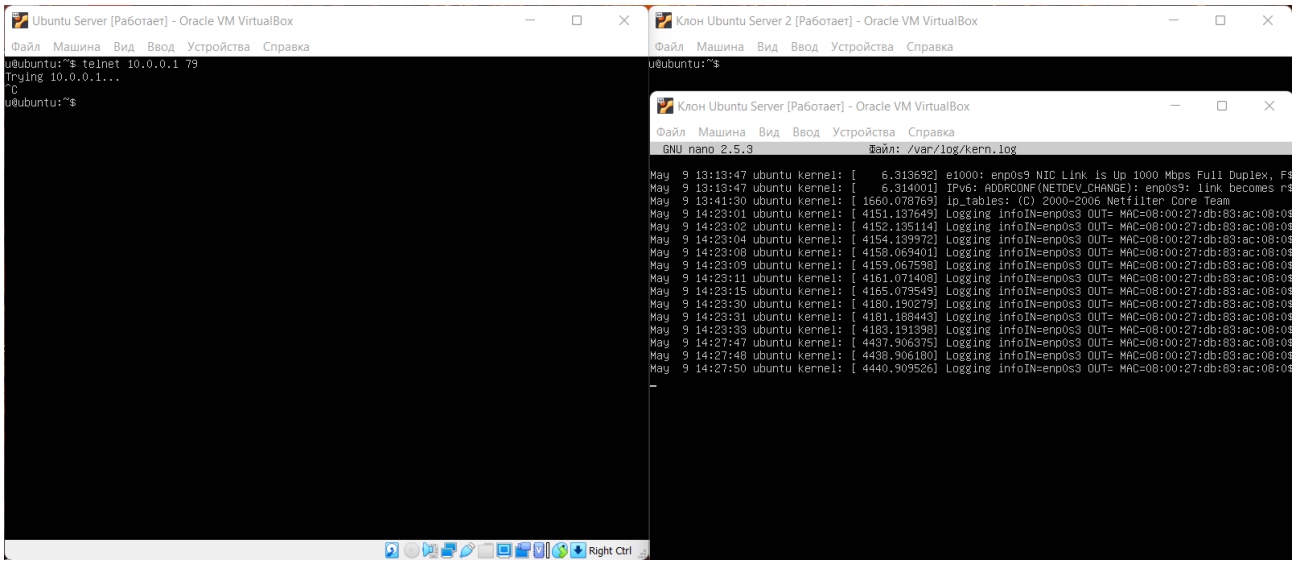

Рисунок 9 – Настроено логгирование попыток подключения по порту 79

8. Заблокируем доступ по порту 19 к Ub3 с Ub1 по его MAC-адресу. (см. рис. 10)

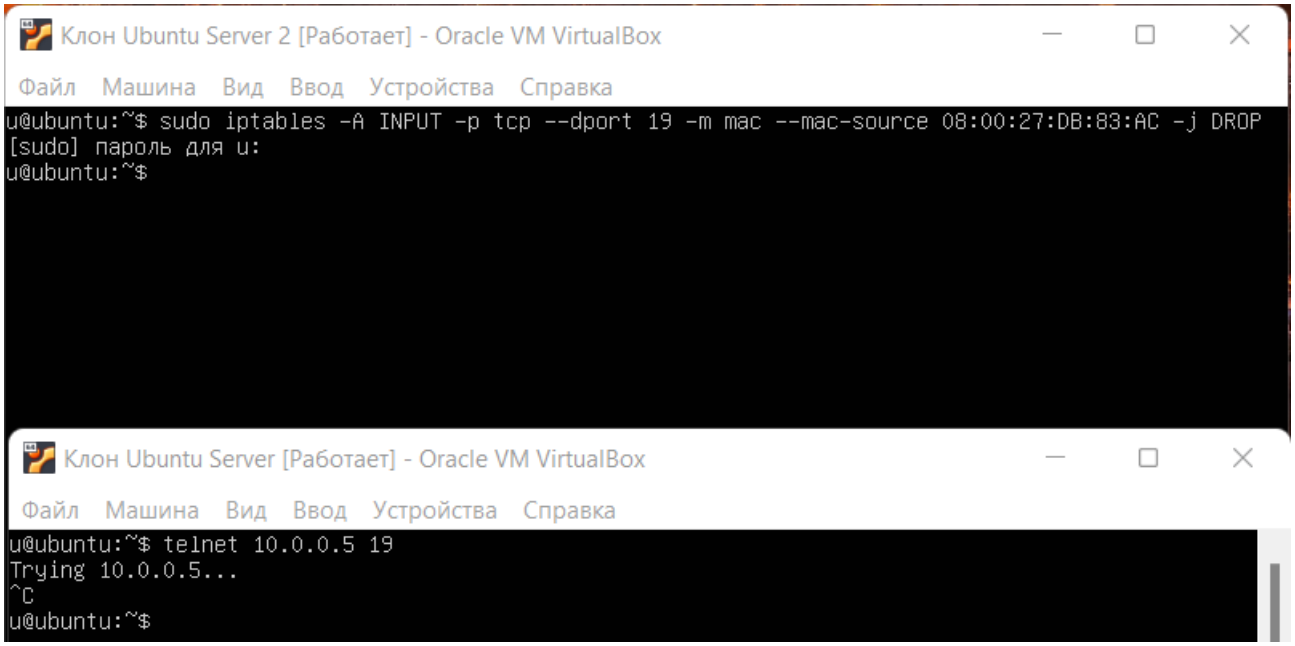

Рисунок 10 – Заблокирован доступ по порту 19 к Ub3 с Ub1 по его MAC-адресу и доступа по порту 19 у Ub1 нет

9. Полностью закроем доступ к Ub1. Разрешим доступ для Ub3 к Ub1, используя диапазон портов 19-79. (см. рис. 11)

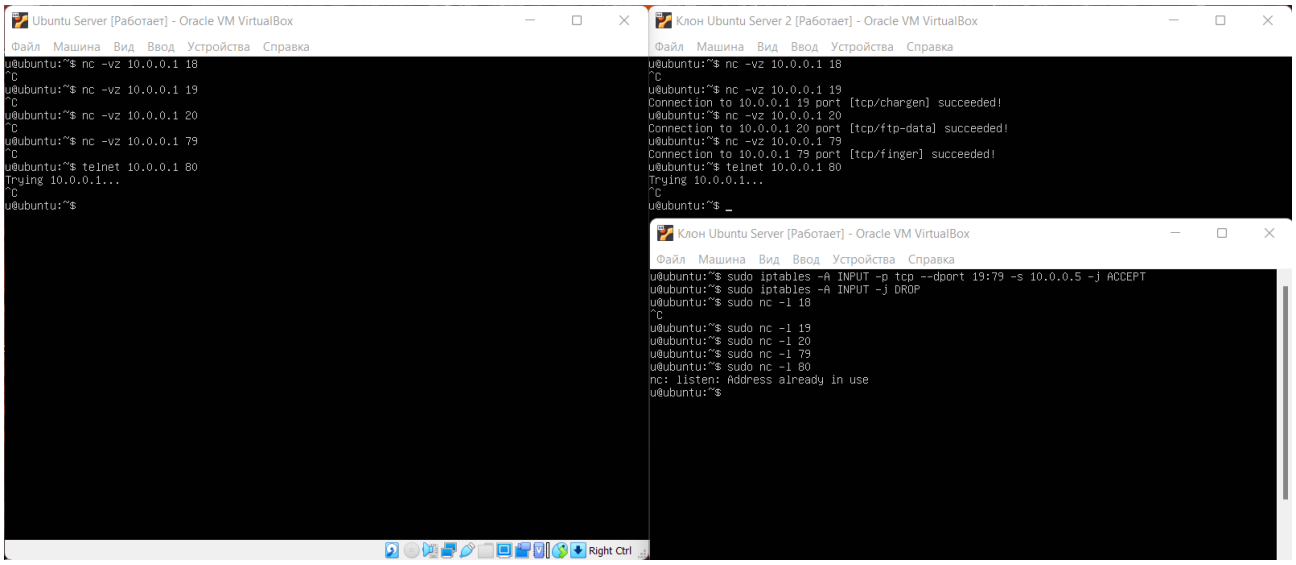

Рисунок 11 – Полностью закрыт доступ к Ub1, есть доступ для Ub3 к Ub1 по портам в диапазоне 19-79

10. Разрешим только одно ssh подключение к UbR. (см. рис. 12)

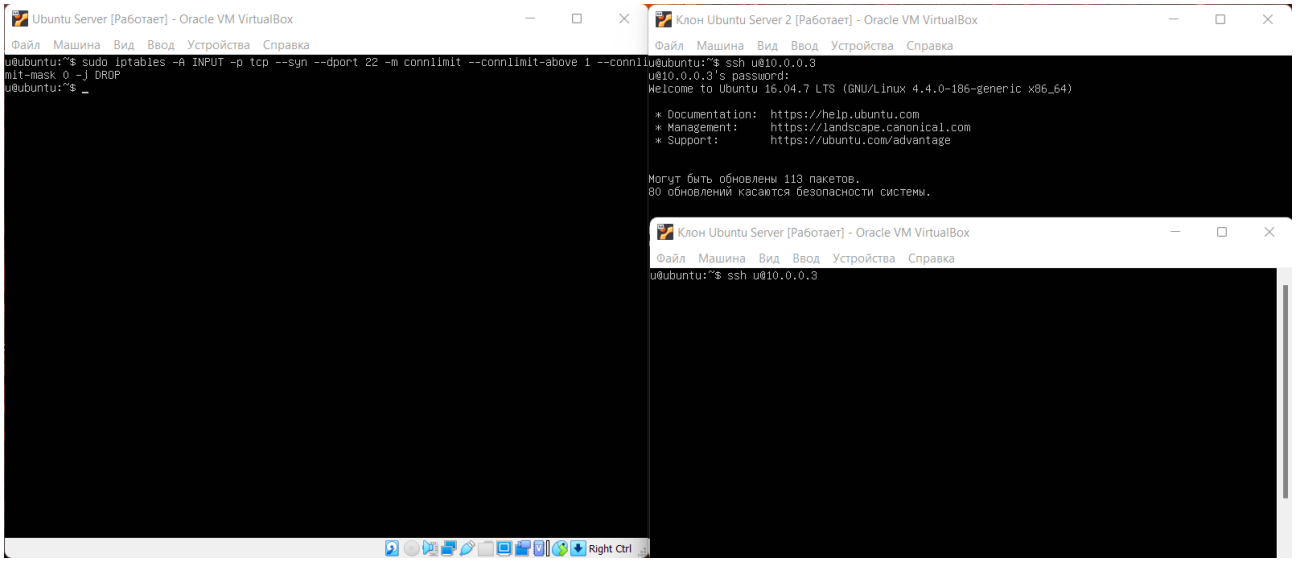

Рисунок 12 – Разрешено только одно ssh подключение к UbR

Выводы.

Таким образом, были изучены принципы работы с сетевыми экранами. В работе блокировался и разрешался прием и отправка пакетов с помощью iptables, было настроено логирование событий.