**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. 9303 |  | Халилов Ш. А. |
| Преподаватель |  | Лавров А. А. |

Санкт-Петербург

2021

**Цель работы.**

Целью работы является изучение принципов работы с сетевыми экранами.

Для достижения поставленной цели необходимо решить следующие

**Постановка задачи.**

1. Создать три виртуальные машины из лабораторной 1

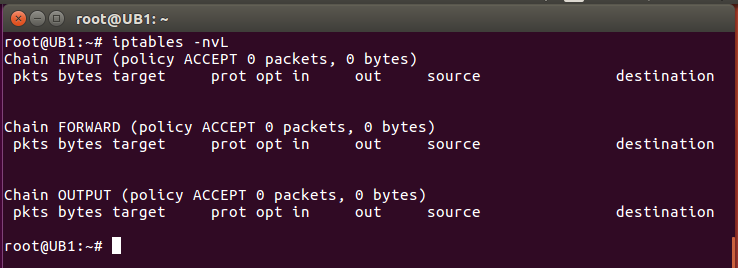
2. Научиться блокировать и разрешать прием и отправку пакетов с помощью iptables, настраивать логирование событий.

**Выполнение работы:**

Для лабораторных работ были развернуты 3 виртуальные машины UB1, UBR и UB3 с IP-адресами: 192.168.100.1 (UB1), 192.168.100.2 (UBR) и 192.168.100.3 (UB3). в дальнейшем на этих виртуальных машинах пошагово выполняются все условия лабораторной работы.

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

Чтобы заблокировать доступ к IP-адресу Ub1, к Ub3 была применена следующая команда ***iptables -A INPUT -s 192.168.100.1 -j DROP.***Результат работы см. на рисунках 1-4.

Рисунок №1 – таблица правил до начала работы.

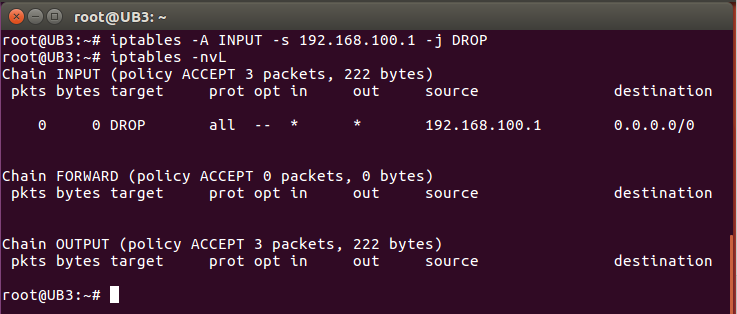


Рисунок №2 – команда для запрета и таблица правил после применения этой команды.

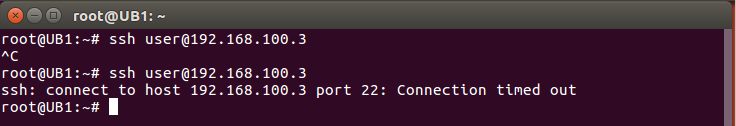


Рисунок №3 – результат ssh запроса с UB1 на UB3.

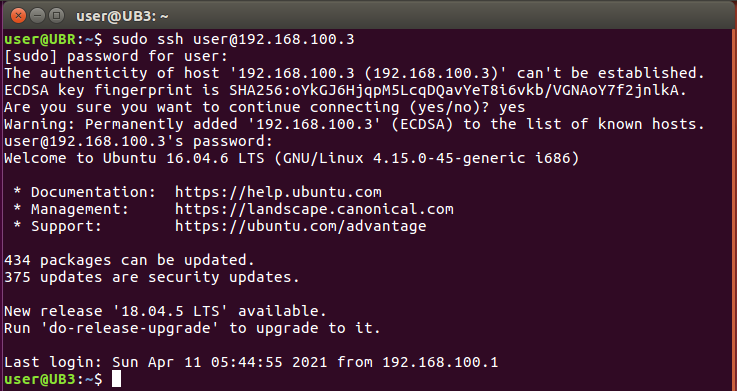


Рисунок №4 – результат ssh запроса с UBR на UB3.

По картинкам видно, что задача выполнена успешно.

**2. Заблокировать доступ по порту 25 на Ub1.**

Чтобы заблокировать доступ по порту 25 на Ub1, была применена следующая команда ***iptables -A INPUT -p tcp --dport 25 -j DROP.***Результат работы см. на рисунках 5-6.

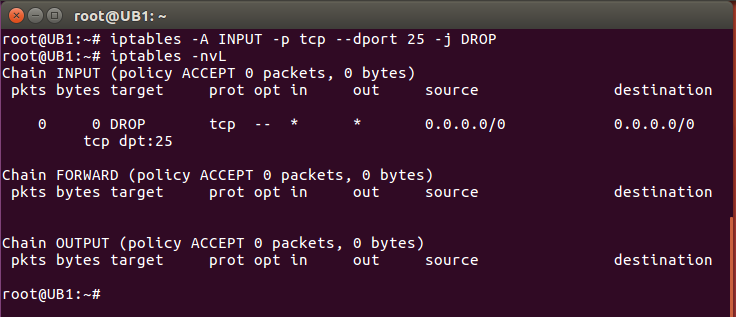


Рисунок №5 – команда для запрета и таблица правил после применения этой команды.

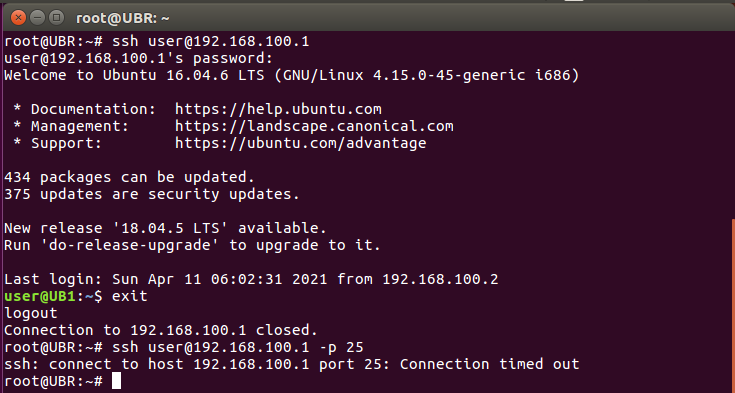


Рисунок №6 – результат ssh запроса с UBR на UB1.

На рисунках показано, что ssh-соединения проходили через порт по умолчанию и не проходили через порт 25.

**3. Заблокировать доступ к порту 75 на Ub3 от UbR. Проверить возможность доступа с Ub1.**

Чтобы заблокировать доступ к порту 75 на Ub3 от UbR, была применена следующая команда ***iptables -A INPUT -p tcp -s 192.168.100.2 --dport 75 -j DROP.***Результат работы см. на рисунках 7-9.

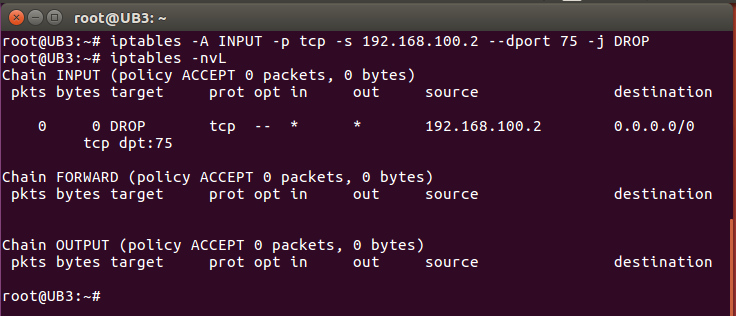


Рисунок №7 – команда для запрета и таблица правил после применения этой команды на UB3.

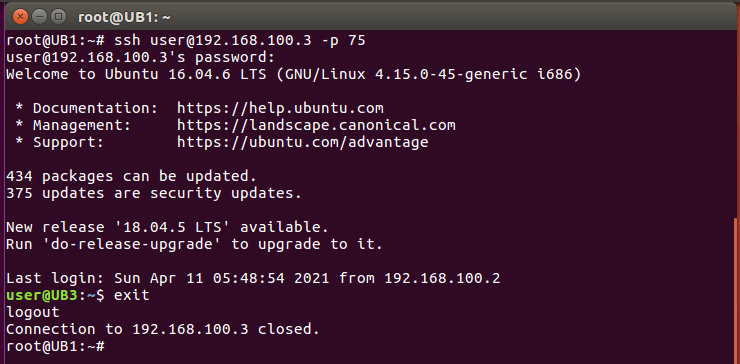


Рисунок №8 – результат ssh запроса с UB1 на UB3.

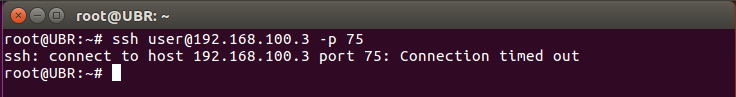


Рисунок №9 – результат ssh запроса с UBR на UB3.

**4. Полностью запретить доступ к Ub3. Разрешить доступ к порту 25.**

Для выполнения этой задачи, были применены следующие команды:

***iptables -A INPUT -j DROP,***

***iptables -I INPUT 1 -p tcp --dport 25 -j ACCEPT.***

Результат работы см. на рисунках 10-12.

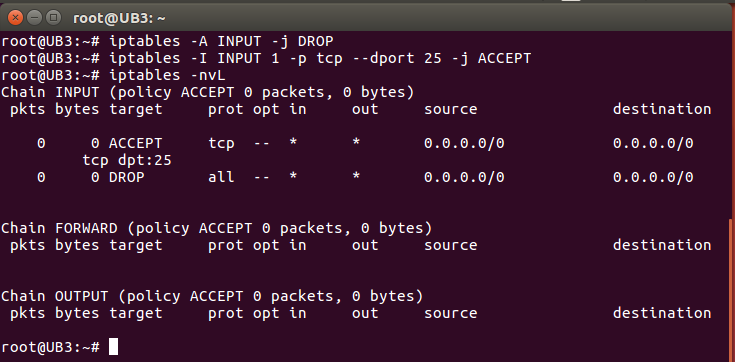


Рисунок №10 – команда для запрета и таблица правил после применения этой команды на UB3.

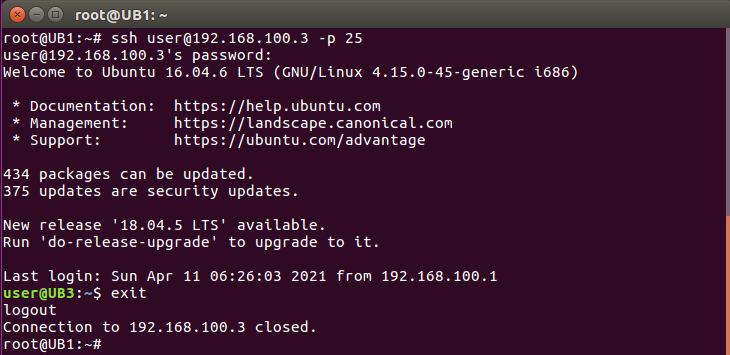


Рисунок №11 – результат ssh запроса с UB1 на UB3.

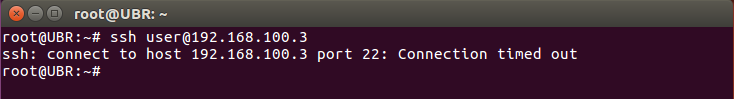


Рисунок №12 – результат ssh запроса с UBR на UB3.

**5. 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.**

Для выполнения этой задачи, сначала были разрешены *icmp* на вывод и ввод с помощью следующие команды:

***iptables -A INPUT -p icmp -j ACCEPT,***

***iptables -A OUTPUT -p icmp -j ACCEPT,***

Затем были запрещены полностью с помощью следующие команды:

***iptables -A OUTPUT DROP.***

***iptables -A INPUT DROP.***

Результат работы см. на рисунках 13-15.

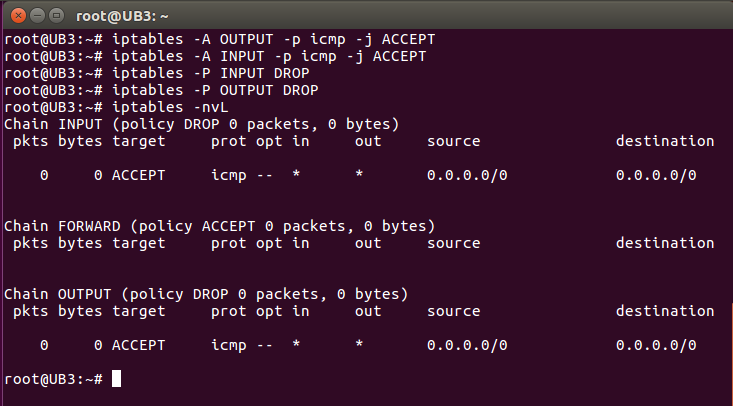


Рисунок №13 – команда для запрета и таблица правил после применения этой команды на UB3.

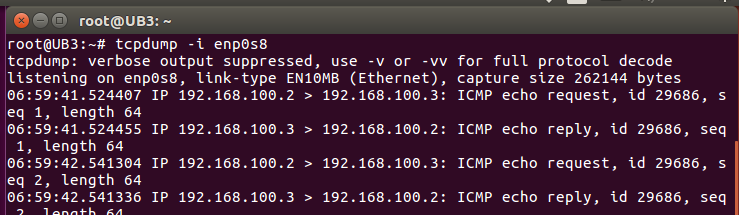


Рисунок №14 – мониторинг запросов на интерфейсе enp0s8 у UB3.

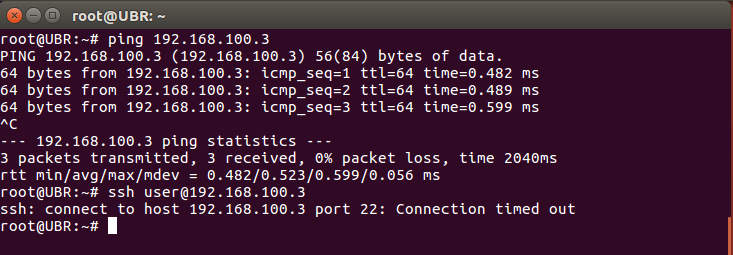


Рисунок №15 – результаты запросов с UBR на UB3.

**6. Запретить подключение к Ub1 по порту 75. Настроить легирование попыток подключения по порту 75.**

Для выполнения этой задачи, были применены следующие команды:

***iptables -A INPUT -i enp0s8 -p tcp –dport 75 -j LOG –log-prefix “Logging info”,***

***iptables -A INPUT -i enp0s8 -p tcp –dport 75 -j DROP.***

Результат работы см. на рисунках 16-18.

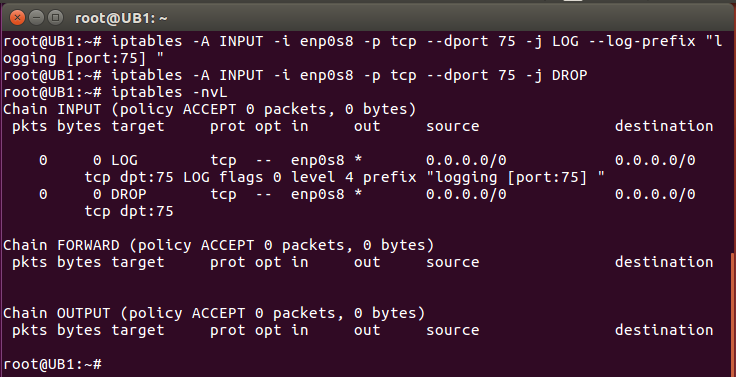


Рисунок №16 – команда для запрета и таблица правил после применения этой команды на UB1.

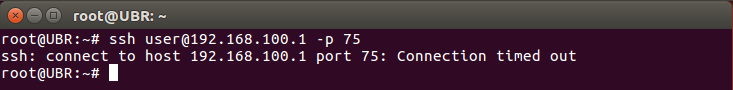


Рисунок №17 – результаты запросов с UBR на UB1.

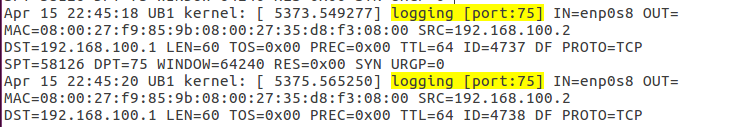


Рисунок №18 – результат логирование на UB1.

**7. Заблокировать доступ по порту 15 к Ub3 с Ub1 по его MAC-адресу.**

Для выполнения этой задачи, сначала на UB3 был запрещен UB1 по мас-адресу с помощью следующую команду:

***iptables -A INPUT -p tcp –dport 15 -m mac –mac-source 08:00:27:27:53:d1 -j DROP***

Было сделано несколько запросов, но запросы не были успешными, пока мас-адрес не был изменен на другой. Результат работы см. на рисунках 19-23.

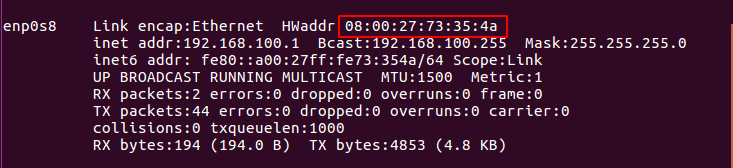


Рисунок №19 – мак-адрес интерфейса enp0s8 у UB1 до изменения.

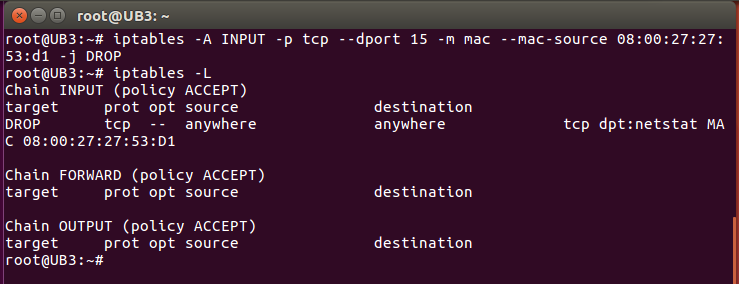


Рисунок №20 – команда запрета по мак-адресу и таблица правил после применения этой команды на UB3.

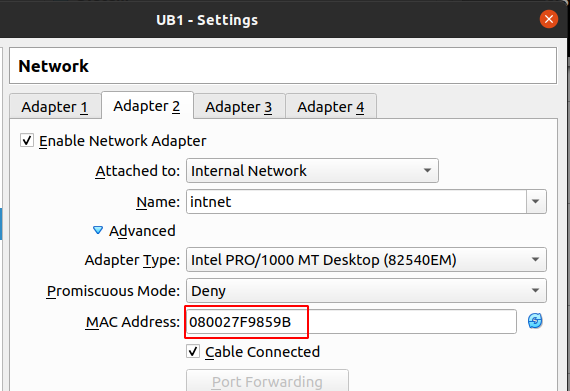


Рисунок №21 – новый мак-адрес интерфейса enp0s8 у UB1.

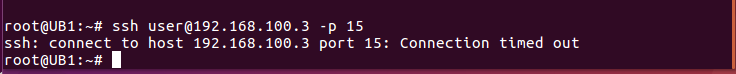


Рисунок №22 – результат запроса до изменения мас-адреса.

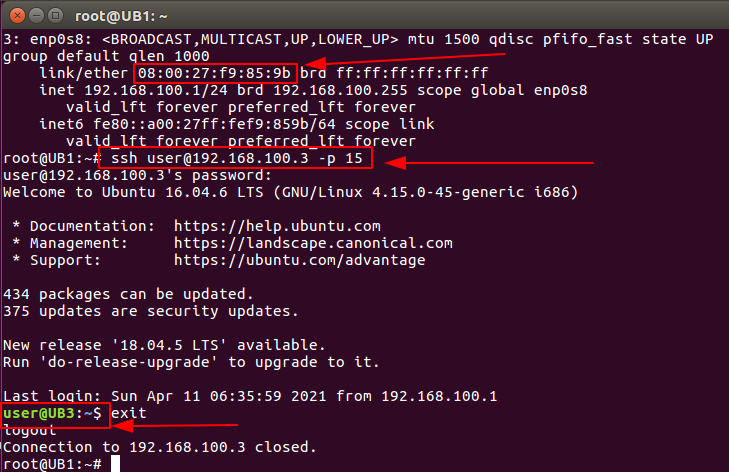


Рисунок №23 – результат запроса после изменения мас-адреса.

**8. Полностью закрыть доступ к Ub1. Разрешить доступ для Ub3 к Ub1, используя диапазон портов 15-75.**

Для решения этой задачи были применены следующие команды:

***iptables -A INPUT -j DROP***

***iptables -I INPUT 1 -s 192.168.100.3 -p tcp –dport 15:75 -j ACCEPT*** . Результат работы см. на рисунках 24-26.

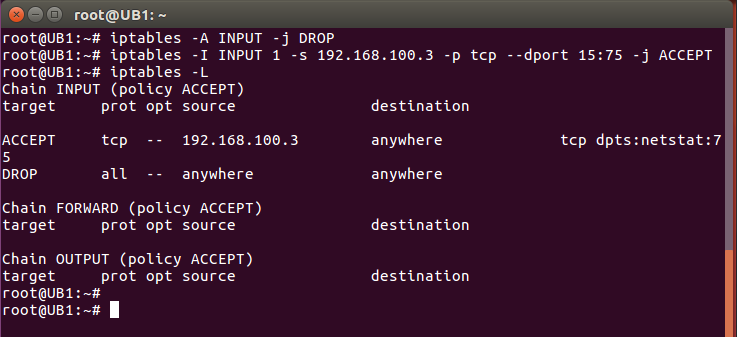


Рисунок №24 – команда запрета полностью и разрешения доступа UB3 к UB1 для портов 15-75.

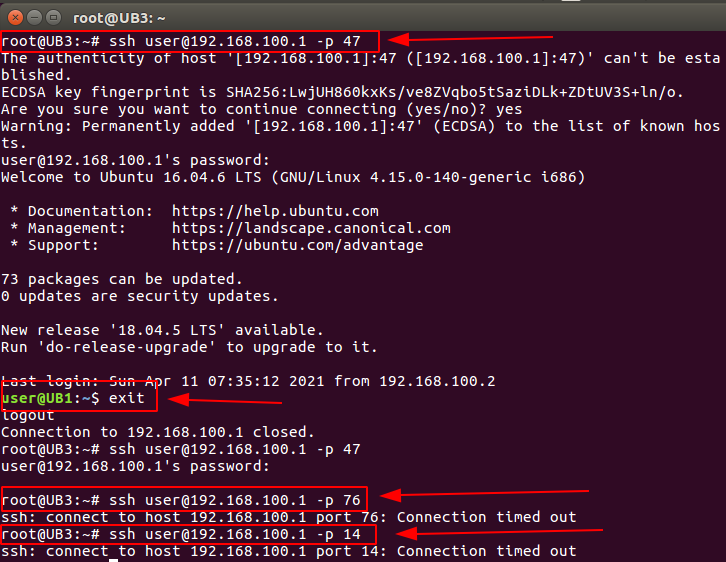


Рисунок №25 – запросы с UB3 на UB1 через разные порты.

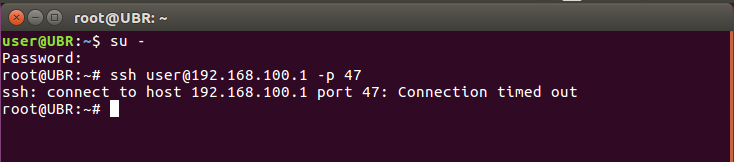


Рисунок №26 – запрос с UBR на UB1.

**9. Разрешить только одно ssh подключение к UbR:**

Чтобы решить эту проблему, была использована следующую команду:

***Iptables –A INPUT -p tcp --syn --dport ssh -m connlimit --connlimit-above 1 --connlimit-mask 0 -j DROP***

Результат работы см. на рисунках 27-29.

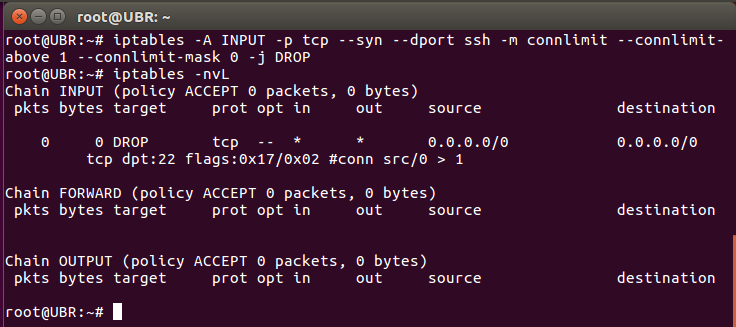


Рисунок №26 – применения команды для разрешения доступ только к одному ssh-соединению.

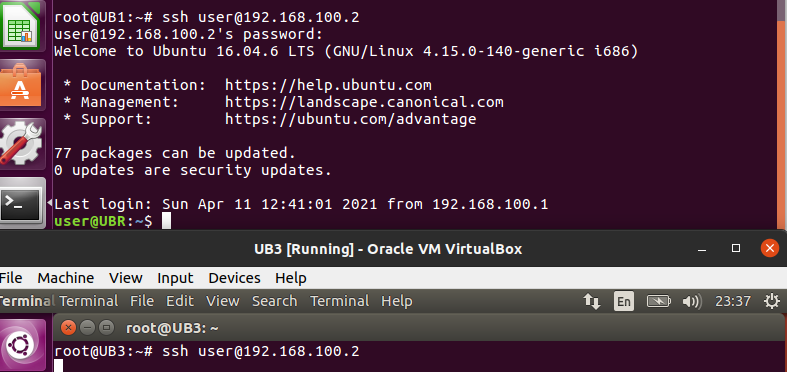


Рисунок №27 – ssh соединения UB1 на UBR и ожидания UB3.

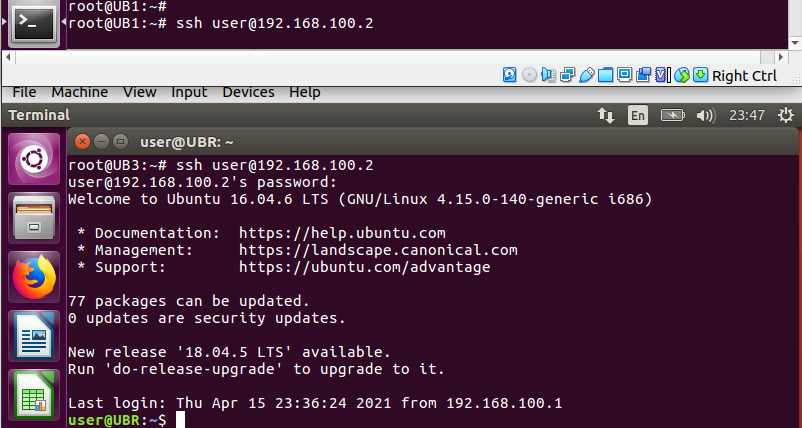


Рисунок №28 – ssh соединения UB3 на UBR и ожидания UB1.

**Выводы.**

Были изучены принципы работы с сетевыми экранами.