**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.**

| Студент гр. 1303 |  | Чубан Д.В. |
| --- | --- | --- |
| Преподаватель |  | Борисенко К.А. |

Санкт-Петербург

2023

* 1. **Цель работы.**
  2. Изучение принципов работы с сетевыми экранами. Освоить блокирование и разрешение приема и отправки пакетов с помощью iptables, а также настройку логирования событий.
  3. З**адание.**

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

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

3. Разрешить доступ только по ssh на Ub2.

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

5. Полностью запретить доступ к Ub3.

6. Запретить подключение к Ub1 по порту 80.

7. Заблокировать доступ по 80-му порту к Ub3 с Ub1 по его MAC-адресу.

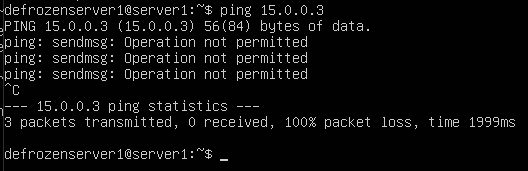
8. Полностью закрыть доступ к Ub1. Разрешить доступ для Ub3 к Ub1,

используя диапазон портов 20–79.

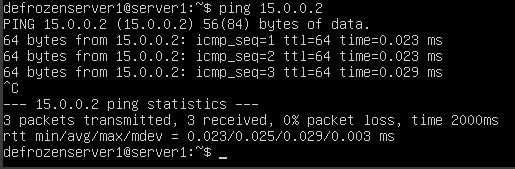
9. Разрешить только одно ssh-подключение к Ub3.

* 1. **Выполнение работы.**
     1. Были развернуты три виртуальные машины с адресами 15.0.0.1/24 (Ub1),
     2. 15.0.0.2/24 (Ub2), 15.0.0.3/24 (Ub3).
     3. 1. Был заблокирован доступ по IP-адресу Ub1 к Ub3, для чего на Ub1
     4. было объявлено правило в цепочке OUTPUT на IP-адрес Ub3. Запрет был
     5. поставлен с помощью команды:
     6. sudo iptables –A OUTPUT –d 15.0.0.3 –j DROP

Были проведены проверки доступности к Ub3 с Ub1 и Ub2.



Доступность Ub3 с Ub1



Доступность Ub3 с Ub2

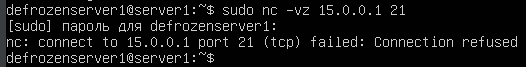
Как можно видеть, Ub3 не доступна с Ub1, но доступна с Ub2.

2. Был заблокирован доступ к 21-му порту на Ub1. Далее был проверен

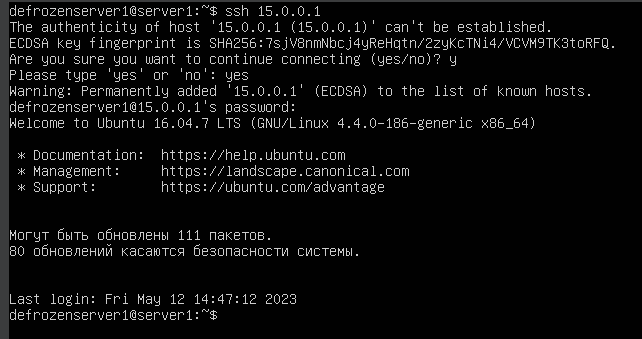
доступ с Ub3 на Ub1 через ssh и через порт 21. Для блокировки доступа была

применена команда:

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



Проверка доступности к 21-му порту Ub1



Доступность к Ub1 через ssh.

Можно заметить, что доступ по ssh не блокируется. Однако порт 21

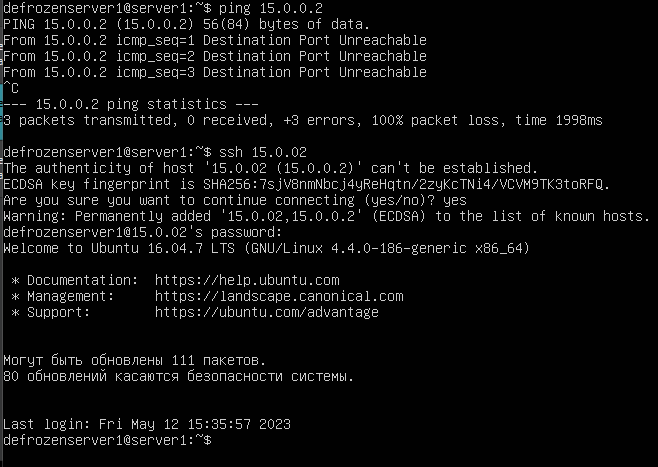
заблокирован.

3. Был разрешен доступ только по ssh на Ub2. Были разрешены пакеты через ssh, а затем запрещены все остальные. Команды представлены ниже.

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

sudo iptables –A INPUT –j REJECT

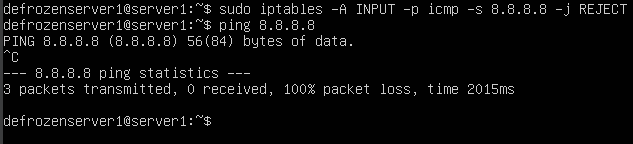
Для проверки корректности настроек через Ub1 была произведена попытка доступа с помощью команды ping, а после через ssh.



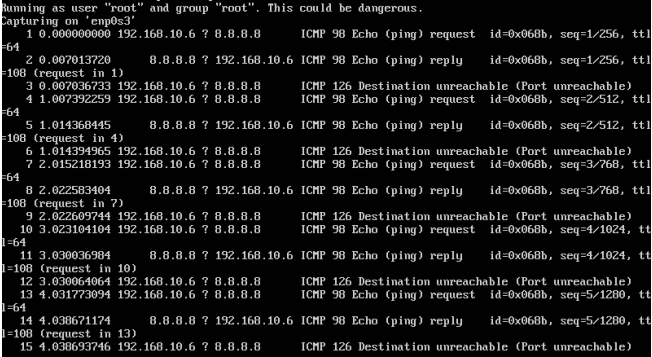
Проверка доступности Ub2 по ping и ssh.

Можно заметить, что доступ возможен только по ssh.

4. Сначала на Ub1 были запрещены ICMP запросы на 8.8.8.8 через правило в цепочке INPUT. Затем таблицы были обновлены и запрет был обеспечен через правило в цепочке OUTPUT.

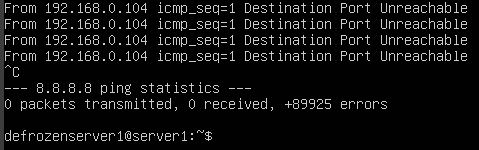


Запрет ICMP-запросов на 8.8.8.8 через INPUT.



Отправка и прием ICMP запросов на 8.8.8.8 при запрете через INPUT.

С помощью программы Wireshark были получены результаты работы первого и второго случаев запретов. На рисунке видно, что запросы отправляются на 8.8.8.8 и оттуда приходят ответы, которые затем отклоняются.



Запрет ICMP-запросов на 8.8.8.8 через OUTPUT.



Отправка и прием ICMP-запросов на 8.8.8.8 при запрете через OUTPUT.

В то же время при запрете через OUTPUT пакеты вовсе не отправляются.

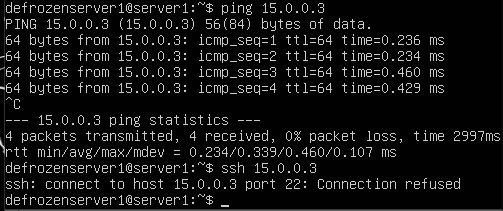
По результатам проверки, можно сказать, что второй вариант (через OUTPUT) эффективнее, так как лишние ICMP-запросы не нагружают сеть.

5. Был полностью запрещен доступ к Ub3, за исключением доступа по ICMP протоколу. Были использованы следующие команды:

sudo iptables –A INPUT –p icmp –j ACCEPT

sudo iptables –A INPUT –j REJECT

Для проверки, были использованы ssh и ping.



Как видно ssh не дает нам доступ, его можно получить только через ping,

т.е. через ICMP протокол.

6. Было запрещено подключение к Ub1 по порту 80, а также настроено логирование попыток провести такое подключение. Использовались команды:

sudo iptables –A INPUT –p tcp —dport 80 –j LOG —log-prefix “80logprefix”

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

По итогу выполнения запросов к Ub1 по порту 80, были составлены логи, находящиеся в файле /var/log/kern.log, в котором демонстрируется отклоненные попытки подключения.

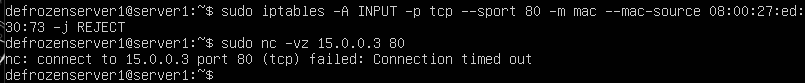


Попытка подключения к Ub1 с Ub2

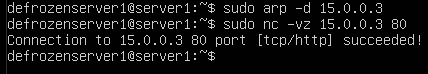


Лог на Ub1

7. Был заблокирован доступ по порту 80 с Ub1 к Ub3 по его MAC-адресу. Затем у Ub3 был изменен MAC-адрес и снова проведена проверка.



Недоступность Ub3 с Ub1



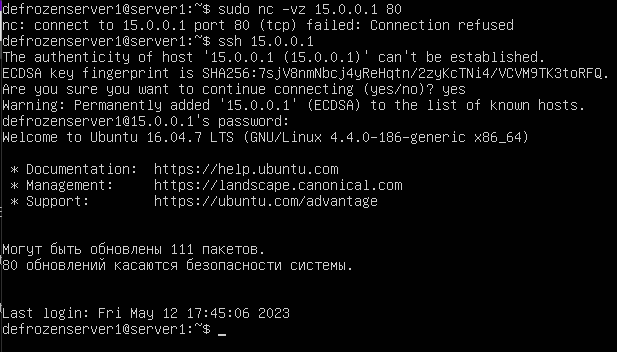
Проверка доступа после смены МАС-адреса

Как видно из результатов, блокируются только запросы с конкретного MAC-адреса независимо от IP-адреса.

8. Был полностью закрыт доступ к Ub1, но разрешен доступ для Ub3 к Ub1, используя диапазон портов 20-79.

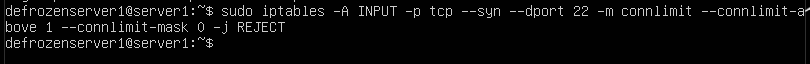


Была проверена невозможность подключения к порту 80 и возможность подключения по ssh.

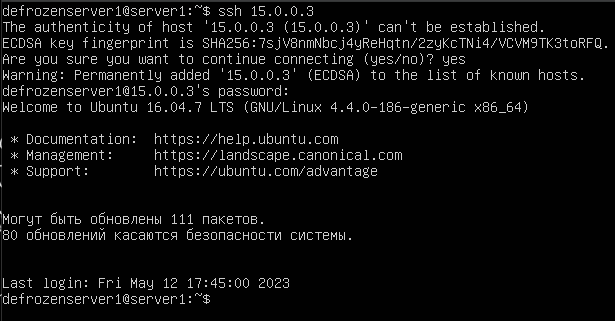


Проверка доступа по 80 порту и ssh.

9. Было разрешено только одно ssh подключение к Ub3



Для проверки было создано ssh подключение к Ub3 с Ub1, а затем была произведена попытка создать еще одно ssh подключение с Ub2.



Подключение по ssh с Ub1



Попытка подключения по ssh с Ub2

Как видно по рисункам выше, Ub3 не позволяет создать второе подключение по ssh.

**Выводы.**

В ходе данной лабораторной работы были изучены принципы работы с сетевыми экранами и освоена утилита iptables, а также выполнены поставленные задачи.