**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 телкомуникации»**

**Тема:** **Сетевые экраны. IPTABLES.**

|  |  |  |
| --- | --- | --- |
| Студент гр. 1384 |  | Усачева Д.В. |
| Преподаватель |  | Ефремов М. А. |

Санкт-Петербург

2023

## Цель работы.

Целью работы является изучение принципов работы с сетевыми экранами.

Необходимо решить следующие задачи:

1. Создать три виртуальные машины (лаб. работа No 3).

2. Научиться блокировать и разрешать прием и отправку пакетов с

помощью iptables, настраивать логирование событий.

## Задание.

Для выполнения лабораторной работы необходимо настроить три виртуальные машины Ub1, Ub2 и Ub3 так, чтобы они находились в одной подсети. Кроме того, для некоторых пунктов необходимо установить дополнительные службы на виртуальные машины: apache2, ftpd – и выполнить следующие задачи:

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

2. Заблокировать доступ по 21-му порту на Ub1. Продемонстрировать возможность доступа по ssh на Ub1 и невозможность доступа по 21-му порту.

3. Разрешить доступ только по ssh на Ub2. Предоставить результат.

4. Запретить ICMP-запросы на IP-адрес 8.8.8.8 двумя способами. Необходимо создать два правила: в цепочке INPUT и цепочке OUTPUT. С помощью Wireshark на хосте нужно продемонстрировать разницу между двумя способами 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 80. Настроить логирование попыток подключения по порту 80. Продемонстрировать результаты логирования.

7. Заблокировать доступ по 80-му порту к Ub3 с Ub1 по его MACадресу. Продемонстрировать результат, сменить MAC-адрес на Ub3 и продемонстрировать успешное подключение к Ub3 по 80-му порту.

8. Полностью закрыть доступ к Ub1. Разрешить доступ для Ub3 к Ub1, используя диапазон портов 20-79. В результате необходимо показать невозможность подключения к порту 80 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.

## Выполнение работы.

1. Были развернуты 3 виртуальные машины, находящиеся в одной подсети:

1. Ub1, ip 172.20.10.4, netmask 255.255.255.240

2. Ub2, ip 172.20.10.5, netmask 255.255.255.240

3. Ub3, ip 172.20.10.3, netmask 255.255.255.240

Заблокируем доступ по IP Ub1 к Ub3:

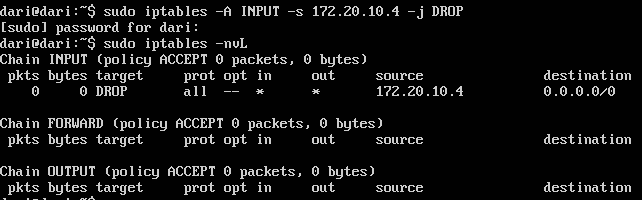


Рисунок 1 — Настройка iptables Ub3

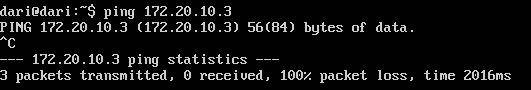


Рисунок 2 — ping c Ub1 на Ub3

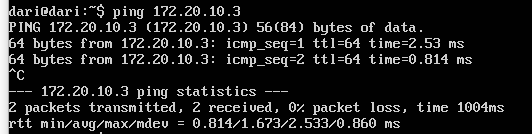


Рисунок 3 — ping c Ub2 на Ub3

2. Настроим сетевой экран на Ub1, чтобы никто из подсети не имел доступа по 21-ому порту. Проверим доступ к Ub1 через 22 порт(ssh) и отсутствие доступа по 21-ому порту с помощью команды telnet.

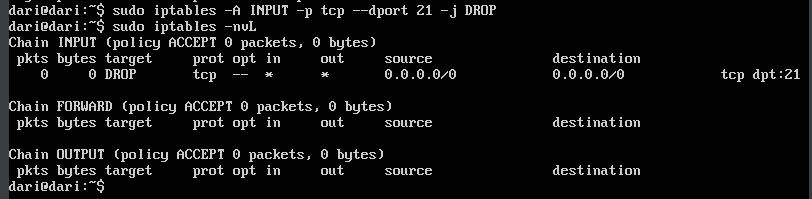


Рисунок 4 — Настройка сетевого экрана на Ub1

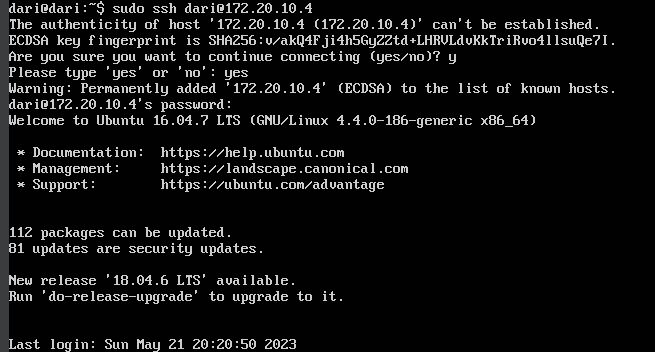


Рисунок 5 — Доступ к Ub1 через ssh

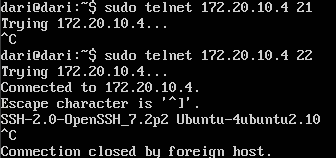


Рисунок 6 — Доступ к Ub1 по 21-ому и 22-ому порту

3. Настроим сетевой экран на Ub2 так, чтобы доступ к нему был разрешен только через ssh.

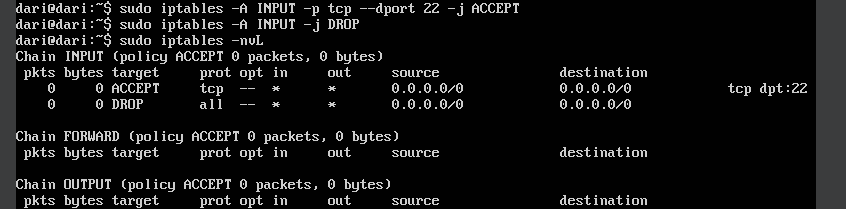


Рисунок 7 —Настройка сетевого экрана на Ub2

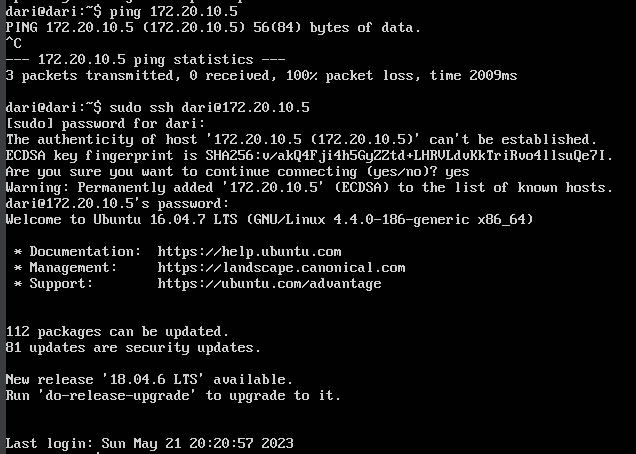


Рисунок 8 — Проверка доступа к Ub2 через ping и ssh

4. Настроим сетевой экран на Ub1 так, чтобы он не имел доступа к 8.8.8.8 в цепочке INPUT.

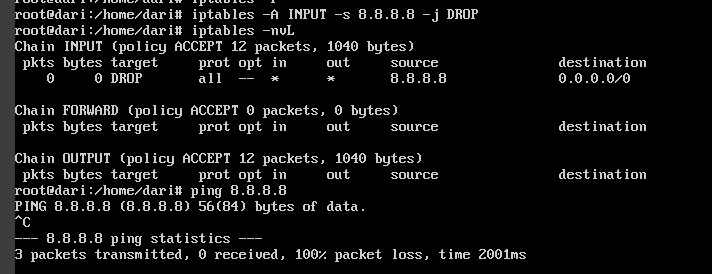


Рисунок 9 — Настройка Ub1 и недоступность 8.8.8.8

Теперь с помощью Wireshark проанализируем трафик между Ub1 и Интернетом.

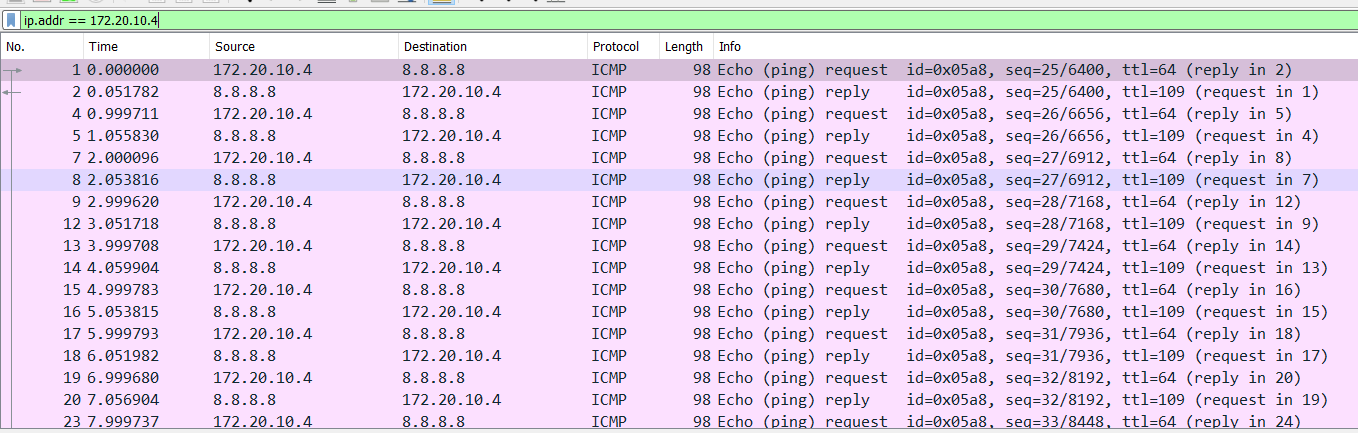


Рисунок 10 — Анализ трафика в Wireshark

Как можно увидеть на рисунке, пакеты отправляются, но не доходит ответ от 8.8.8.8, из-за чего сеть нагружается бесполезными запросами. Теперь сбросим настройки iptables, заблокируем доступ к 8.8.8.8 в цепочке OUTPUT.

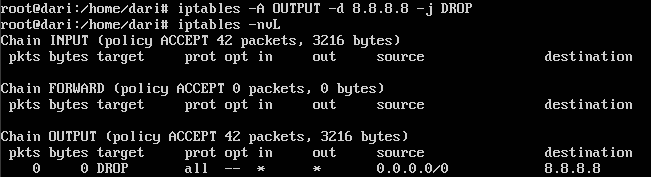


Рисунок 11 —Настройка Ub1

Теперь проанализируем трафик с помощью Wireshark.

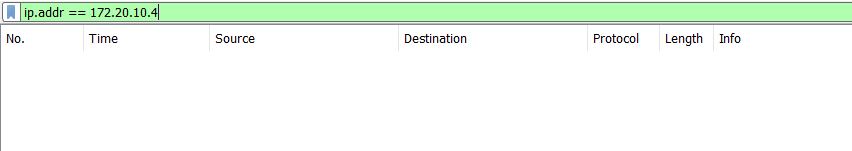


Рисунок 12 — Анализ трафика в Wireshark

Как можно заметить, пакеты не отправляются вовсе, что позволяет сделать вывод, что данный метод гораздо эффективнее, так как он не нагружает сеть бесполезными запросами.

5. Сбросим настройки iptables для Ub3, запретим к нему доступ всеми способами, кроме ICMP-протокола.

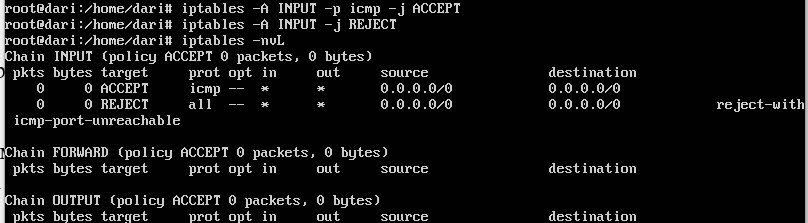


Рисунок 13 — Настройка Ub3

Проверим доступность Ub3 через ping, ssh подключение и с помощью утилиты telnet, которая использется tcp протоколы.

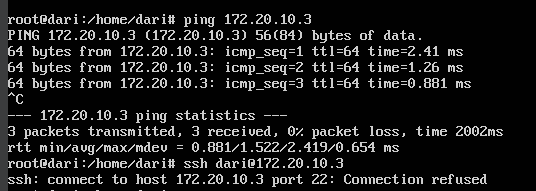


Рисунок 14 — Проверка доступности Ub3

Как видно, через ping можно обратиться к Ub3, остальными способами нельзя.

6. Было запрещено подключение к ub1 по 80-ому порту, также настроено логирование попыток подключения по 80-ому порту.

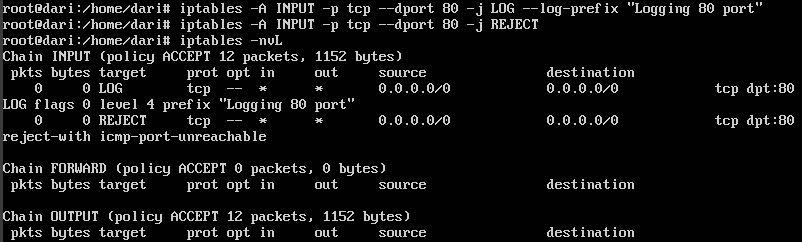


Рисунок 15 — Настройка Ub1

Теперь с помощью команды telnet выполним запрос к 80-ому порту с двух других ВМ, проверим файл /var/log/kern.log на наличие информации о нужном логировании.

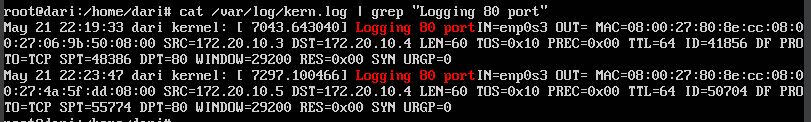


Рисунок 16 — Логирование о попытках доступа к 80-ому порту Ub1

7. Заблокируем доступ по 80-ому порту к Ub3 с Ub1 по его MAC-адресу.



Рисунок 17 — Настройка Ub1 и проверка недоступности порта

Теперь сменим MAC-адрес Ub3 и попробуем заново.



Рисунок 18 — Проверка доступности после смены MAC-адреса

Как можно заметить, блокируются только запросы с конкретного MAC-адреса независимо от IP.

8. Был полностью закрыт доступ к Ub1, но был разрешен доступ для Ub3 к Ub1 через порты 20-79.

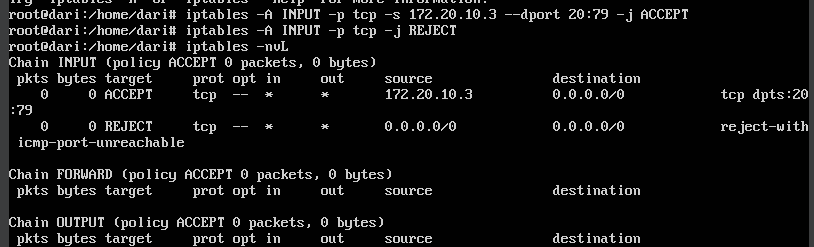


Рисунок 19 — Настройка Ub1

Теперь продемонстрируем недоступность 80 порта на Ub1 для Ub3 с

помощью telnet.



Рисунок 20 — Недоступность Ub1 по 80 порту

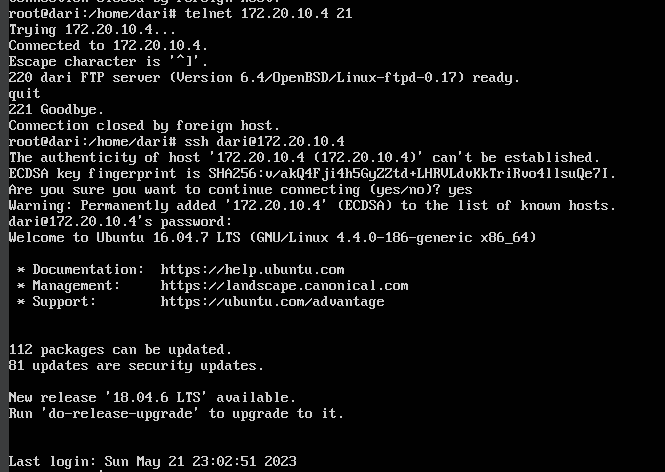


Рисунок 21 — Доступность Ub1 по ssh и по 21 порту

9. Разрешим только одно ssh-подключение к Ub3.

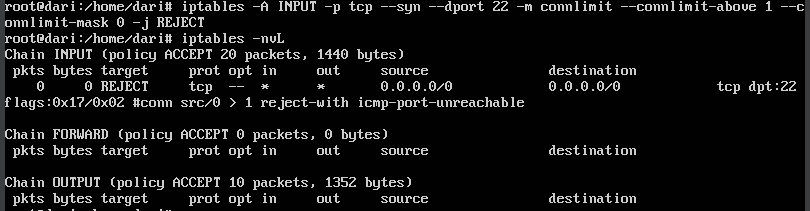


Рисунок 22 — Настройка Ub3

Теперь подключимся по ssh c Ub1 на Ub3 и попытаемся сделать то же самое с Ub2.

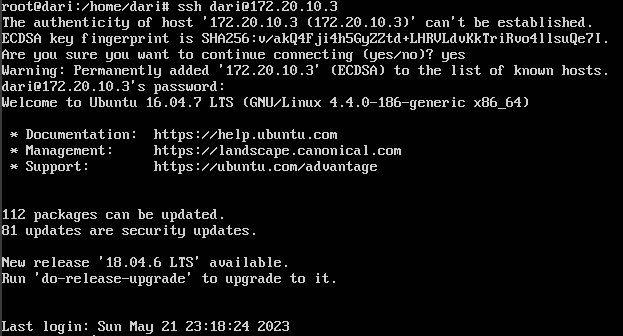


Рисунок 23 — Подключение через ssh с Ub1

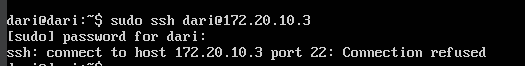


Рисунок 23 — Подключение через ssh с Ub2

Попытка не увенчалась успехом, так как Ub3 не дает сделать второе ssh-соединение.

## Выводы.

В ходе данной работы были изучены принципы работы с сетевыми экранами. Были решены следующие задачи:

1. Создание трех виртуальных машин.

2. Реализация блокирования и разрешения приема и отправки пакетов с помощью iptables, создание логирования событий.