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

ОТЧЕТ

по лабораторной работе №3

по дисциплине «Сети и телекоммуникации»

Тема: Использование межсетевого экрана ОС Linux

Студент гр. 7383 _____ Левкович Д.В.

Преподаватель _____ Фирсов М.А.

Санкт-Петербург

2019

Цель работы.

Научиться создавать, удалять и изменять правила межсетевого экрана iptables (настройка блокировки трафика, разрешения принятия трафика, логгирования приходящих пакетов).

Задачи.

0. На всех машинах запустить скрипт toscrath.sh. Проверить, что таблицы ядра пусты.

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

2. Заблокировать доступ по порту X на Ub1.

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

4. Полностью запретить доступ к Ub3. Разрешить доступ к порту X.

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.

6. Запретить подключение к Ub1 по порту X. Настроить логгирование попыток подключения по порту X.

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

8. Полностью закрыть доступ к Ub1. Разрешить доступ для Ub3 к Ub1, используя диапазон портов X.

9. Разрешить только одно ssh подключение к UbR.

Вариант заданий.

Вариант заданий указан в табл. 1.

Таблица 1 – Вариант заданий

Вар.\Задание	2 X=	3 X=	4 X=	6 X=	7 X=	8 X=
10	30	80	30	80	20	20-80

Ход работы.

0. На каждой машине был запущен скрипт toscratch.sh. Для проверки того, что таблицы каждой машины пусты, была введена команда:

iptables -L

Вывод в консоли представлен на рис.1. По нему видно, что таблицы пусты.

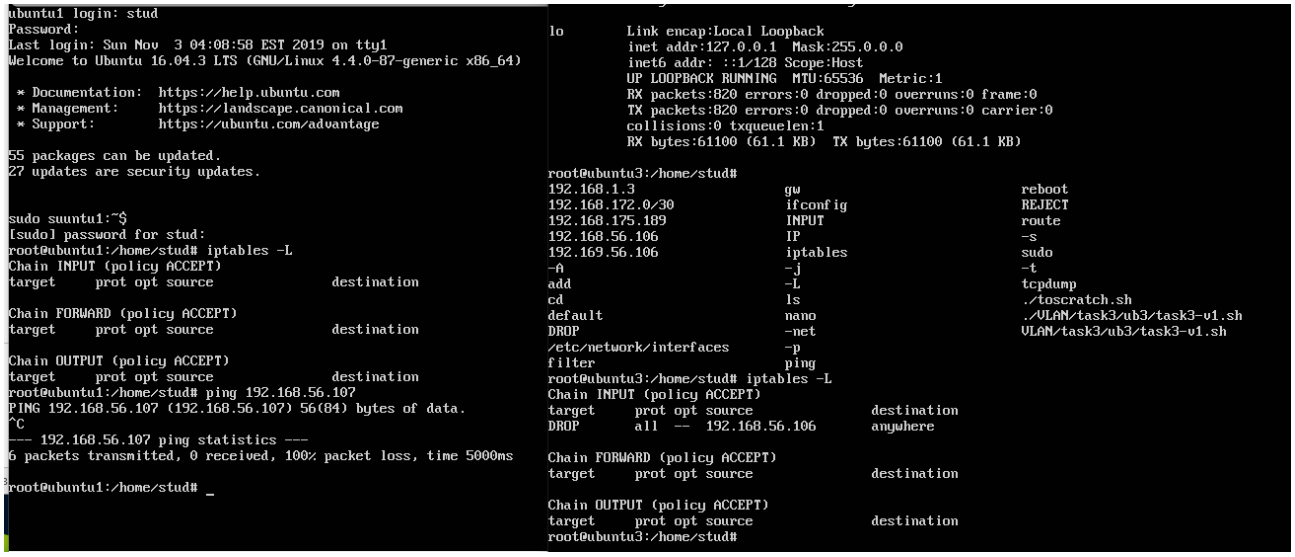

Рисунок 1 – Вывод консоли после выполнения команды чтения таблиц ядра

1. Для блокировки доступа по IP-адресу Ub1 к Ub3 на Ub3 была введена команда:

iptables -t filter -A INPUT -s 192.168.56.106 -j DROP,

где 192.168.56.106 – IP-адрес Ub1, который можно узнать с помощью команды ifconfig. В результате этой команды Ub1 не имеет доступа к Ub3, что видно при попытке отправить пакет с Ub1 на Ub3 командой ping, как показано на рис. 2.

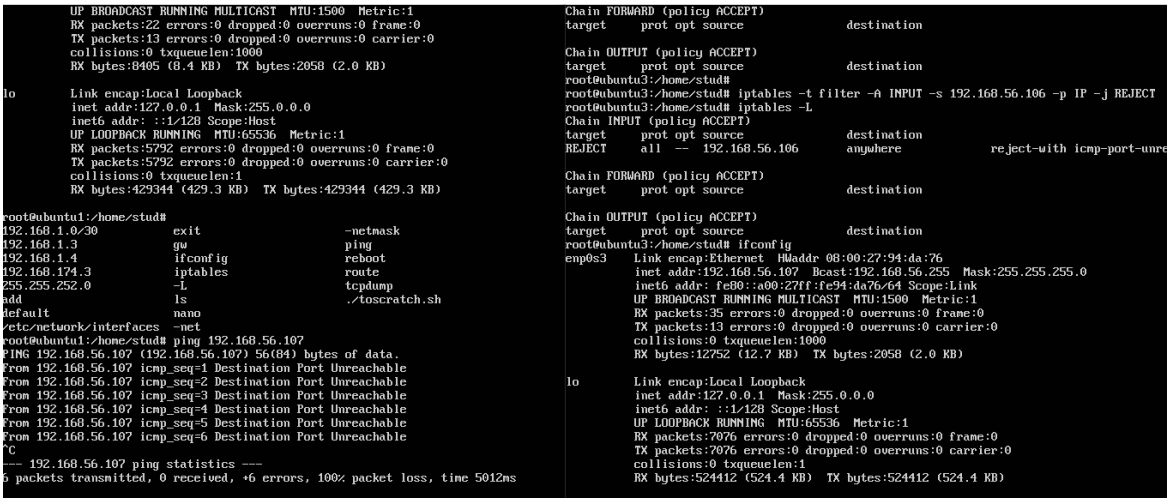

Рисунок 2 – Запрет входящий пакетов от Ub1 на Ub3

2. Для блокировки доступа по порту 30 на Ub1 была выполнена команда iptables –A INPUT –p tcp –dport 30 –j REJECT. Результат показан на рис. 3.

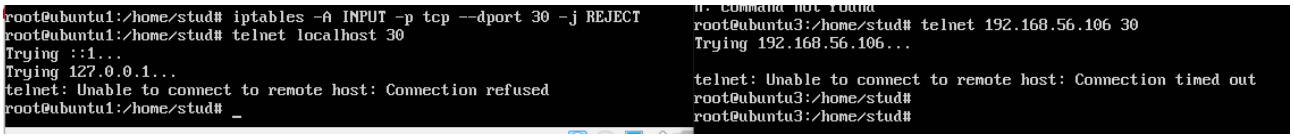

Рисунок 3 – Блокировка по порту 30 на Ub1.

3. Для блокировки доступа по порту 80 UbR к Ub3 была выполнена команда, показанная на рис. 4. Также на рис. 4 показано, что доступа от UbR нет, однако у Ub1 к Ub3 доступ есть.

Рисунок 4 – Запрет доступа UbR к Ub3 по порту 80

4. Для полной блокировки доступа на Ub3 была введена команда:

Iptables -t filter -P INPUT DROP.

Для разрешения доступа по порту 30 была введена команда:

Iptables -t filter -A INPUT -p tcp --dport 30 -j ACCEPT.

Таблица ядра и проверка соединения представлены на рис. 5.

Рисунок 5 – Запрет доступа на Ub3 и разрешение по порту 30

5. Для полной блокировки доступа на Ub3 были выполнены команды, показанные на рис. 6. Проверка ping показывает, что доступ по icmp открыт, но по tcp – закрыт.

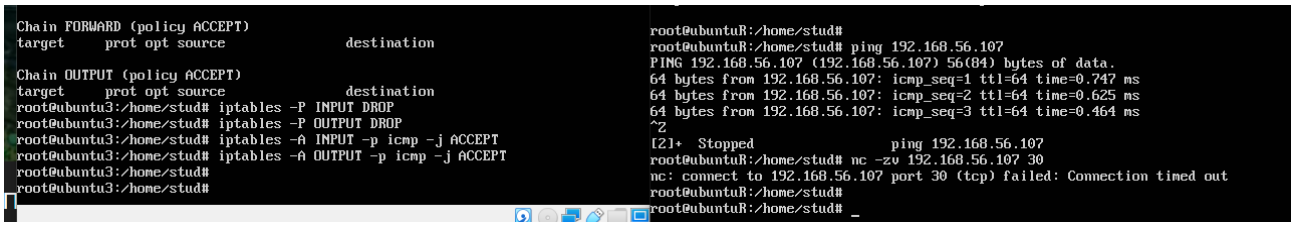

Рисунок 6 – Запрет доступа на Ub3 с разрешением ICMP

6. Для настройки логгирования были введены следующие команды:

iptables -A INPUT -p tcp --dport 80 -j LOG.

а для запрета подключения по порту 80:

iptables -A INPUT -p tcp --dport 80 -j REJECT.

Все логи будут сохранены в var/log/syslog.

Лог представлен на рис. 6.

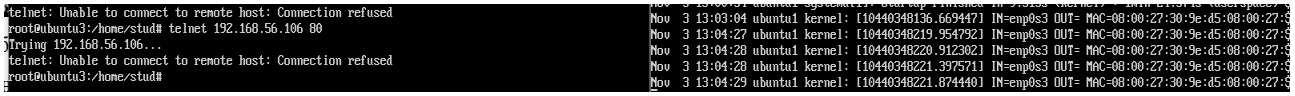

Рисунок 6 – Лог iptables

7. Для запрета доступа на Ub3 от Ub1 по MAC-адресу, была введена команда iptables –A INPUT –m mac –mac-source 08:00:27:30:9e:d5 –p tcp --dport 20 –j REJECT, показанная на рис. 7.

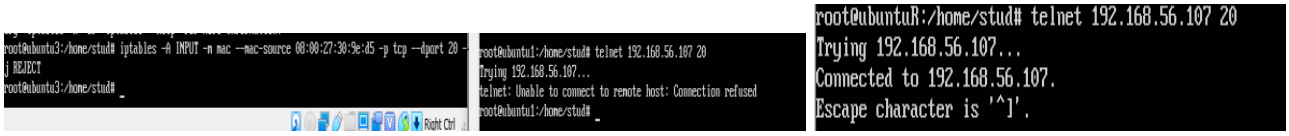

Рисунок 7 – Запрет доступа по MAC-адресу

8. Для разрешения соединений по портам 20-80 от Ub3 к Ub1 была введена команда:

iptables -A INPUT -m multiport -p tcp –dports 20:80 -s 192.168.56.107 -j ACCEPT,

а для запрета всех подключений была введена команда:

iptables -A INPUT -p all -j REJECT.

Попытки подключения представлены на рис. 8.

Рисунок 8 – Запрет доступа и разрешения по диапазону портов

9. Для запрета более 1 подключения по ssh, была введена команда, показанная на рис 9.

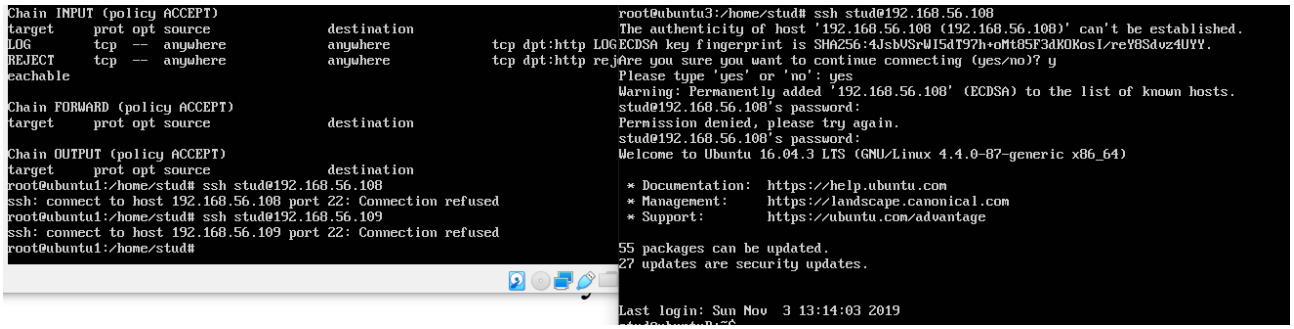

Рисунок 9 – Запрет более одного соединения по ssh

Выводы.

В процессе выполнения данной лабораторной работы были изучены создание, удаление и изменение правил межсетевого экрана iptables (настройка блокировки трафика, разрешения принятия трафика, логгирования приходящих пакетов).