Министерство науки и высшего образования Российской Федерации
Калужский филиал
федерального государственного автономного
образовательного учреждения высшего образования
«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
(КФ МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ ***ИУК «Информатика и управление»***

КАФЕДРА ***ИУК4 «Программное обеспечение ЭВМ, информационные технологии»***

ЛАБОРАТОРНАЯ РАБОТА 2

ДИСЦИПЛИНА: «Технологии системного программного обеспечения»

Выполнил: студент гр. ИУК4-62Б _____ (____Губин Е.В._____)
(Подпись) (Ф.И.О.)

Проверил: _____ (___Красавин Е.В.___)
(Подпись) (Ф.И.О.)

Дата сдачи (защиты):

Результаты сдачи (защиты):

- Балльная оценка:
- Оценка:

Калуга , 2025

Цель: получение практических навыков по настройке межсетевого экрана.

Задача: научиться использовать и настраивать межсетевой экран в ОС FreeBSD на примере IPFW.

Ход выполнения работы

1. Включить IPFW и указать тип межсетевого экрана. Настройка производится в файле /etc/rc.conf, после чего необходимо перезапустить систему.

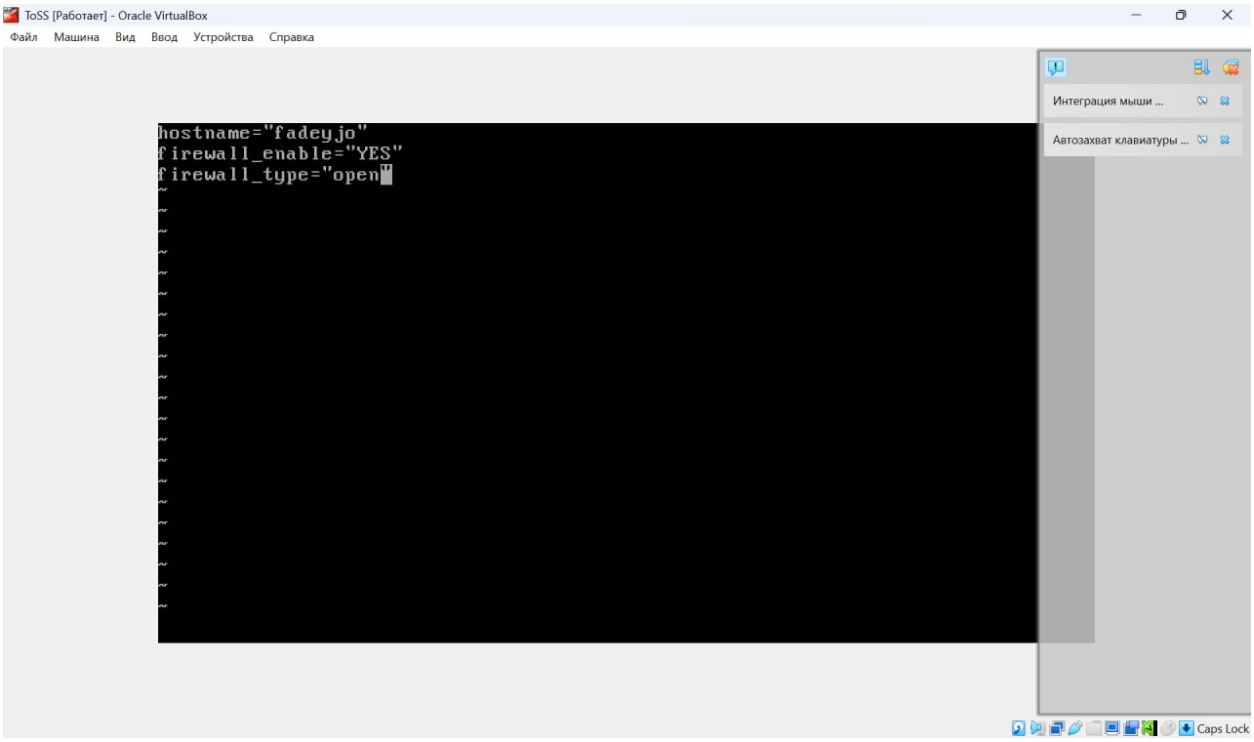

Рисунок 1: Настройка IPFW

2. Вывести полный список существующих планов

```
# ipfw list
00100 allow ip from any to any via lo0
00200 deny ip from any to 127.0.0.0/8
00300 deny ip from 127.0.0.0/8 to any
00400 deny ip from any to ::1
00500 deny ip from ::1 to any
00600 allow ipv6-icmp from :: to ff02::/16
00700 allow ipv6-icmp from fe80::/10 to fe80::/10
00800 allow ipv6-icmp from fe80::/10 to ff02::/16
00900 allow ipv6-icmp from any to any icmp6types 1
01000 allow ipv6-icmp from any to any icmp6types 2,135,136
65000 allow ip from any to any
65535 deny ip from any to any
```

Рисунок 2: Список действующих правил

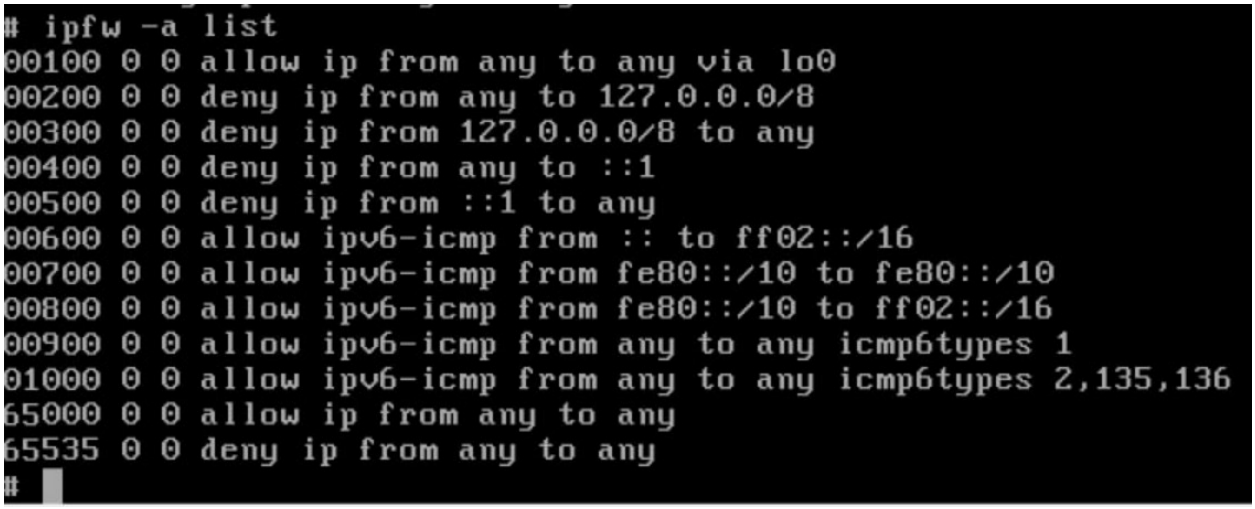

Рисунок 3: Полный список действующих правил

3. Включить протоколирование сообщений межсетевого экрана. Оно включается в файле /etc/rc.conf и /etc/sysctl.conf.

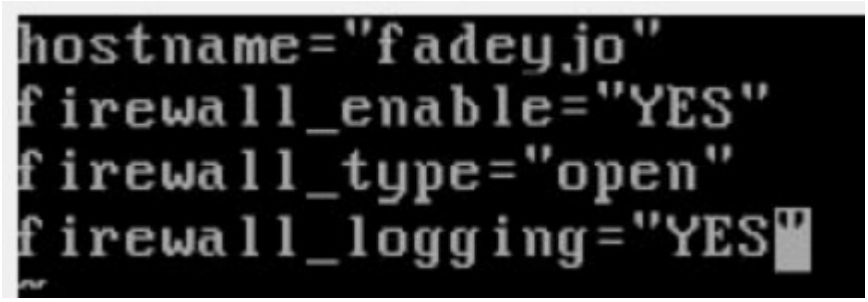

Рисунок 4: Включение логирования в /etc/rc.conf

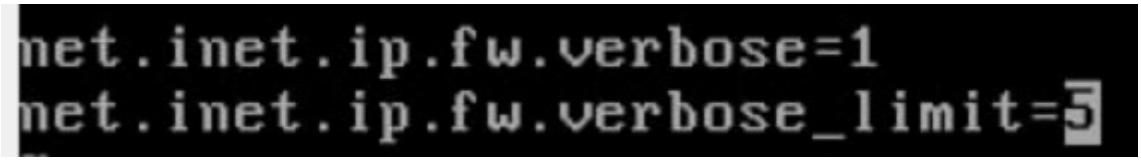

Рисунок 5: Настройка логирования в /etc/sysctl.conf

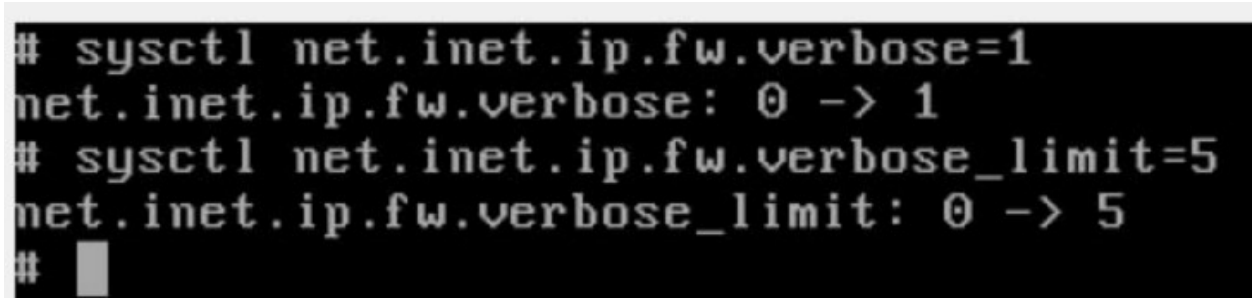

Рисунок 6: Включение логирования "на лету"

4. Задать правило с сохранением состояния. Создадим правило, которое разрешает выход SSH (порт 22) с сохранением состояния (keep-state).

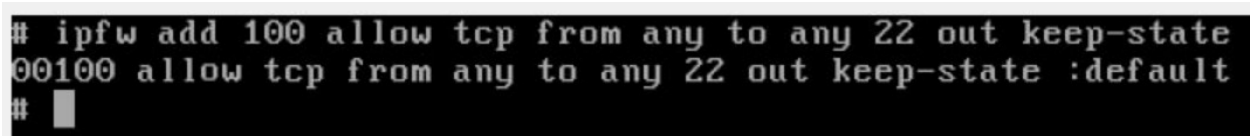

Рисунок 7: Создание правила с сохранением состояния

5. Задать правило без сохранения состояния. Разрешает HTTP-трафик на порту 80 без сохранения состояния.

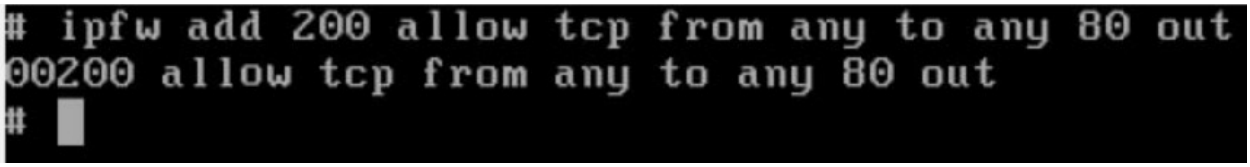

Рисунок 8: Создание правила без сохранения состояния

6. Скрипт правил по представленному примеру. Создадим /etc/ipfw.rules и будем прописывать туда правила. Так же необходимо выдать права на исполнение этого скрипта и добавить в /etc/rc.conf запуск этого скрипта. Этот скрипт означает:

- Проверка состояний (динамических соединений).
- Разрешает пакеты, которые уже находятся в установленной сессии.
- Запрещает входящие TCP-пакеты с установленными соединениями, если они не соответствуют состоянию (keep-state).
- Запрещает фрагментированные пакеты, чтобы предотвратить атаки на фрагменты.
- Разрешает исходящий HTTP-трафик (порт 80) через интерфейс em0, устанавливая состояние (keep-state).
- Разрешает обращения к DNS-серверу 8.8.8.8 по TCP и UDP для разрешения доменных имён.

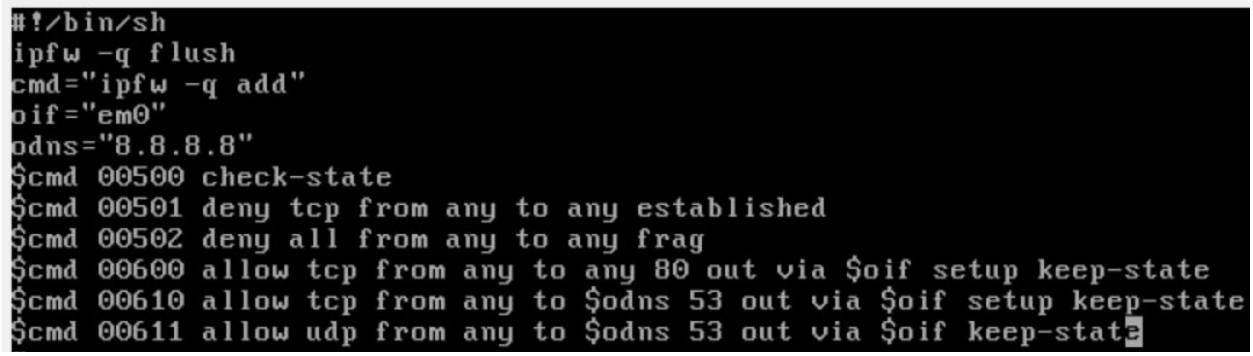

Рисунок 9: Создание скрипта правил из методички

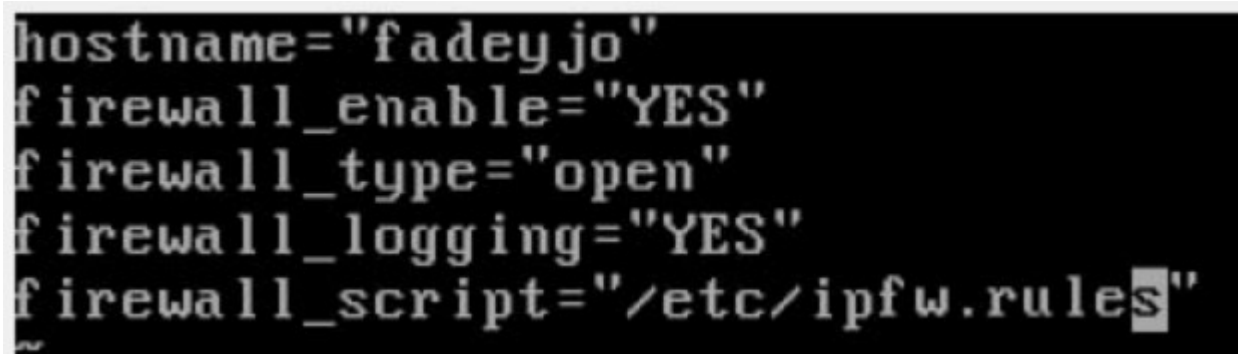

Рисунок 10: Добавление запуска скрипта в /etc/rc.conf

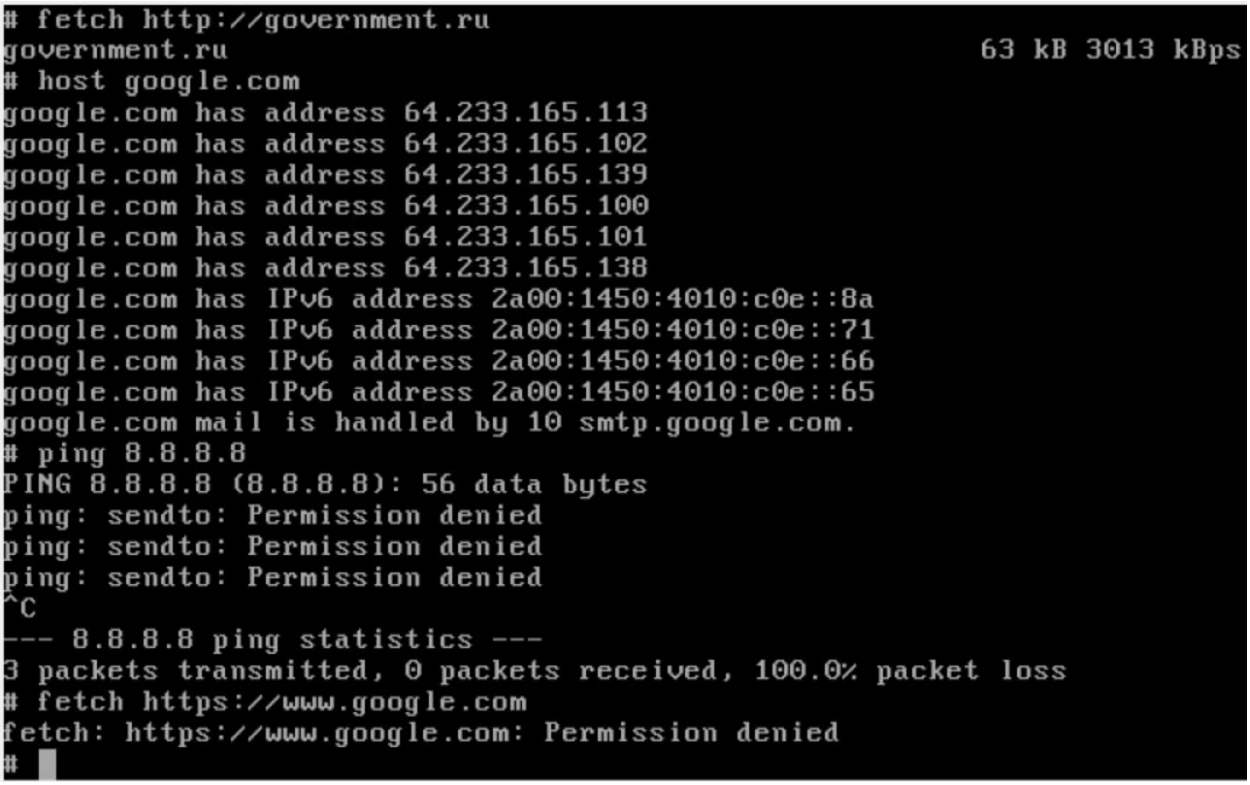

Рисунок 11: Запуск и проверка скрипта

7. Скрипт правил для межсетвого экрана закрытого типа. Этот скрипт:

- Разрешить весь трафик через интерфейс loopback (lo0).
- Проверка существующих состояний соединений.
- Разрешить исходящий HTTP-трафик (порт 80), с сохранением состояния (keep-state).
- Разрешить исходящий HTTPS-трафик (порт 443), тоже с сохранением состояния.
- Разрешить исходящий DNS-запрос (порт 53 по UDP) — чтобы могли разрешаться доменные имена (google.com, yandex.ru и т.д.).
- Всё остальное запрещено и логируется (deny log).
- Любой другой трафик будет заблокирован и записан в лог (/var/log/security).

```
#!/bin/sh
ipfw -q flush
cmd="ipfw -q add"
$cmd 00100 allow all from any to any via lo0
$cmd 00110 check-state
$cmd 00200 allow tcp from any to any 80 out setup keep-state
$cmd 00210 allow tcp from any to any 443 out setup keep-state
$cmd 00220 allow udp from any to any 53 out keep-state
$cmd 00300 deny log all from any to any
```

Рисунок 12: Скрипт для межсетевого экрана закрытого типа

```
# sh /etc/ipfw.rules
# fetch http://government.ru
government.ru                                          63 kB 9105 kBps
# fetch https://www.google.com
fetch: https://www.google.com: size of remote file is not known
www.google.com                                         19 kB   12 MBps
# host google.com
google.com has address 142.250.75.238
google.com has IPv6 address 2a00:1450:4007:813::200e
google.com mail is handled by 10 smtp.google.com.
# telnet 8.8.8.8 23
Trying 8.8.8.8...
telnet: connect to address 8.8.8.8: Permission denied
telnet: Unable to connect to remote host
```

Рисунок 13: Запуск и проверка скрипта

8. Скрипт правил с сохранением состояния и поддержкой NAT. Для данного скрипта нужно включить natd в /etc/rc.conf. Данный скрипт:

- NAT: направить все IP-пакеты через natd на интерфейсе em0.
- Проверка состояний (stateful inspection).
- Разрешить исходящий HTTP (порт 80) с установлением состояния (keep-state).
- Разрешить исходящий HTTPS (порт 443) с установлением состояния.
- Разрешить исходящие DNS-запросы (порт 53 UDP).

```
natd_enable="YES"
natd_interfacce="em0"
natd_flags="-dynamic -m"
```

Рисунок 14: Включение natd в /etc/rc.conf

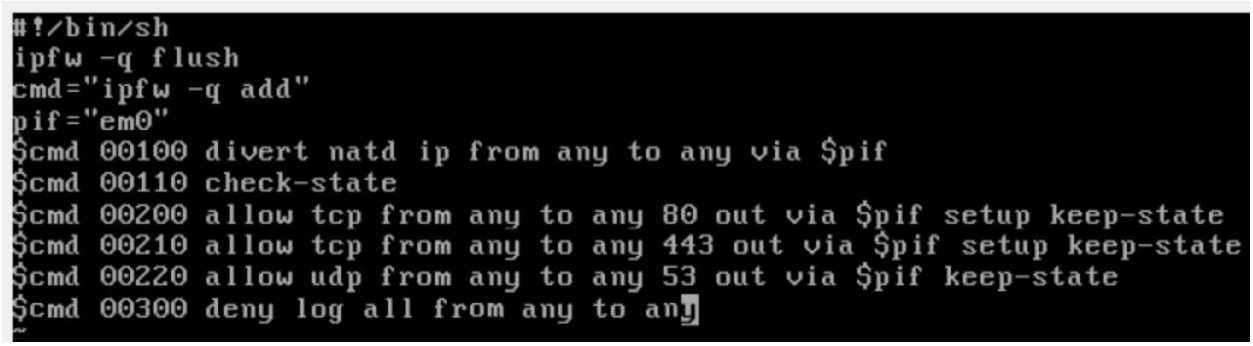

Рисунок 15: Скрипт с поддержкой NAT

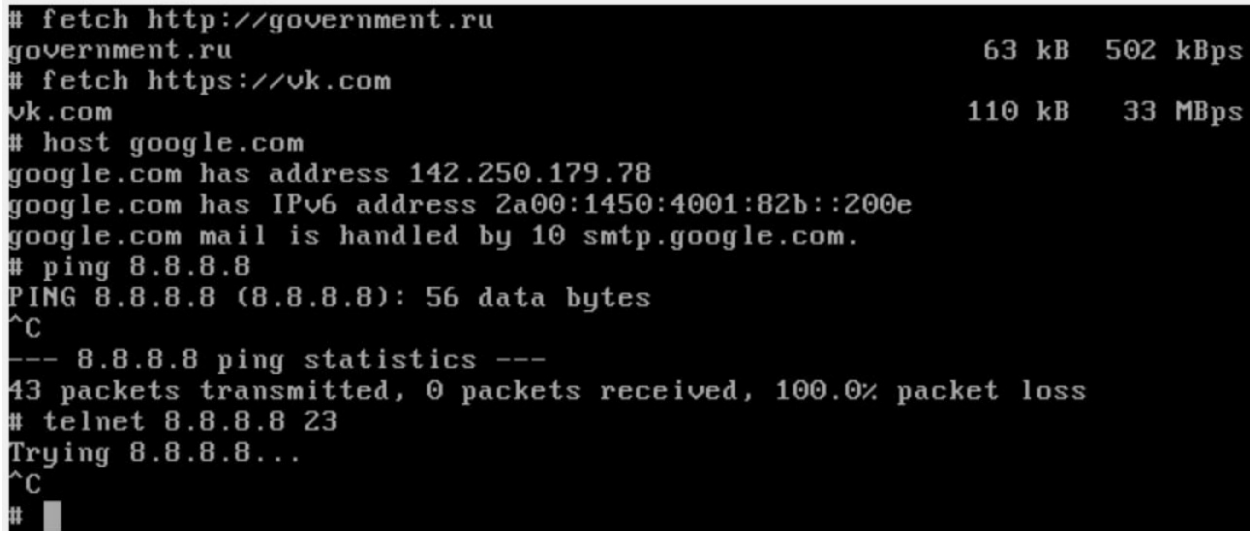

Рисунок 16: Проверка работоспособности

9. Проверка файла логов. В этом файле (/var/log/security) описаны показаны логи с неудавшимися запросами.

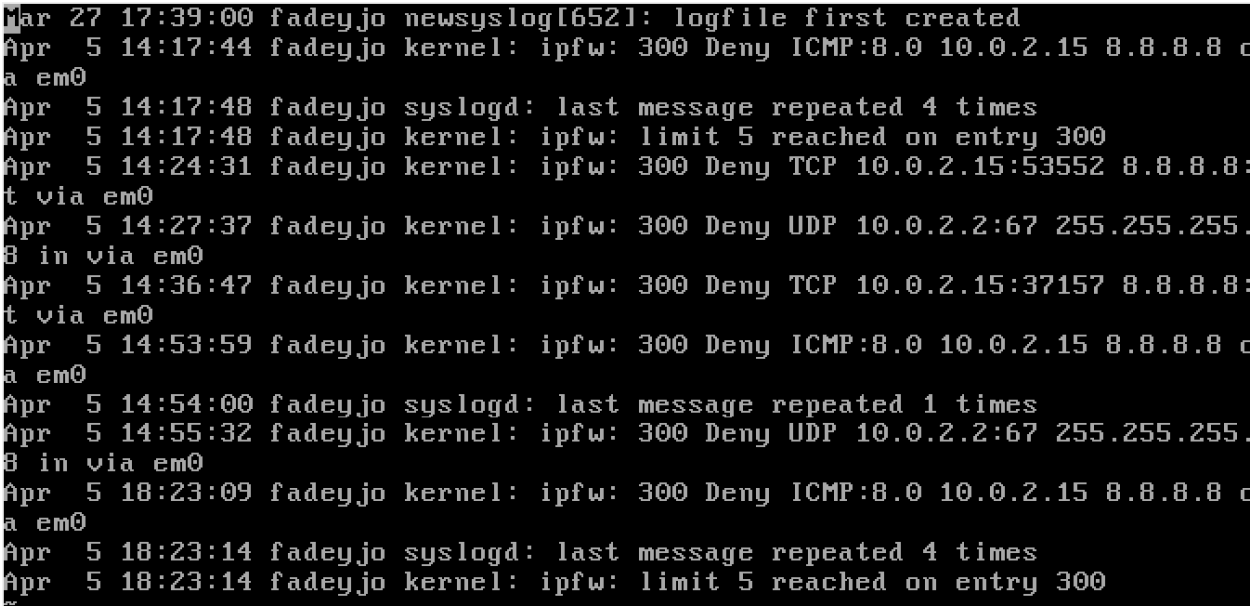

Рисунок 17: Проверка файла логов

Вывод: в ходе лабораторной работы были настроены различные варианты firewall типа IPFW.