Министерство науки и высшего образования Российской Федерации
Калужский филиал
федерального государственного бюджетного
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 №4

«Основы безопасности. Использование межсетевого экрана»

ДИСЦИПЛИНА: «Операционные системы»

Выполнил: студент гр. ИУК4-62Б _____ (Калашников А.С.)
(Подпись) (Ф.И.О.)

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

Дата сдачи (защиты):

Результаты сдачи (защиты):

- Балльная оценка:
- Оценка:

Калуга, 2023

Цель: получение практических навыков по настройке межсетевого экрана.

Задачи:

1. Научиться использовать и настраивать межсетевой экран в ОС FreeBSD на примере IPFW

Задание:

Под руководством преподавателя произвести настройку межсетевого экрана.

1. Включить IPWF.
2. Указать тип межсетевого экрана.
3. Вывести полный список существующих правил.
4. Включить протоколирование сообщений межсетевого экрана.
5. Задать правило с сохранением состояния.
6. Задать правило без сохранения состояния.
7. Написать скрипт правил по предоставленному примеру.
8. Написать правила для межсетевого экрана закрытого типа.
9. Написать правила с сохранением состояний и поддержкой NAT.
10. После установки каждого правила необходимо проверить, что правила работают корректно (попытаться обратиться по сети к другому компьютеру).
11. Завершить работу с FreeBSD.

Ответить на контрольные вопросы и подготовить отчет.

Результат работы:

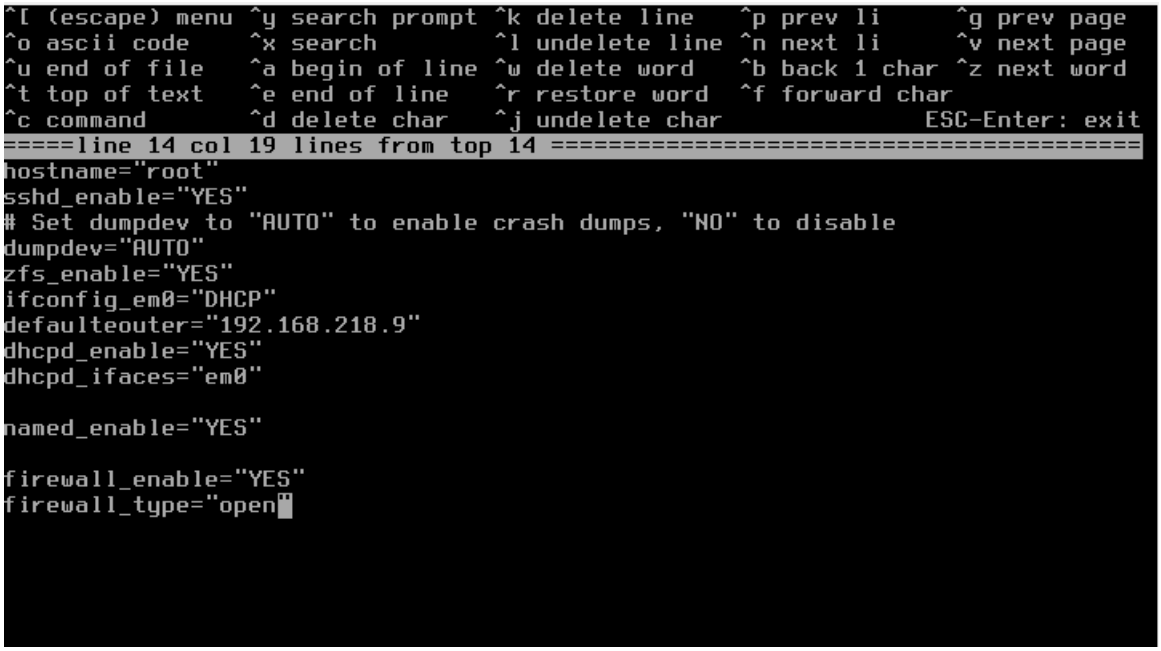

Рис. 1. Включение IPFW в файле rc.conf и указание типа

```
Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with:  pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed:  freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages:  man man
FreeBSD directory layout:      man hier

To change this login announcement, see motd(5).
root@root:~ # 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
root@root:~ #
```

Рис. 3. Просмотр списка установленных правил

```
^[ (escape) menu ^y search prompt ^k delete line   ^p prev li     ^g prev page
^o ascii code    ^x search        ^l undelete line ^n next li     ^v next page
^u end of file   ^a begin of line ^w delete word   ^b back 1 char ^z next word
^t top of text   ^e end of line   ^r restore word  ^f forward char
^c command       ^d delete char   ^j undelete char              ESC-Enter: exit
=====line 15 col 21 lines from top 15 ========================================
hostname="root"
sshd_enable="YES"
# Set dumpdev to "AUTO" to enable crash dumps, "NO" to disable
dumpdev="AUTO"
zfs_enable="YES"
ifconfig_em0="DHCP"
defaulteouter="192.168.218.9"
dhcpd_enable="YES"
dhcpd_ifaces="em0"

named_enable="YES"

firewall_enable="YES"
firewall_type="open"
firewall_logging="YES"
```

Рис. 4. Включение протоколирования сообщений межсетевого экрана в файле rc.conf

```
root@root:/etc # ipfw add allow tcp from any to any setup keep-state
00000 allow tcp from any to any setup keep-state :default
root@root:/etc #
```

Рис. 5. Добавления правила с сохранением состояния

```
root@root:/etc # ipfw add allow in
65200 allow in
root@root:/etc # ipfw add allow out
65300 allow out
root@root:/etc #
```

Рис. 6. Добавление правил без сохранения состояния

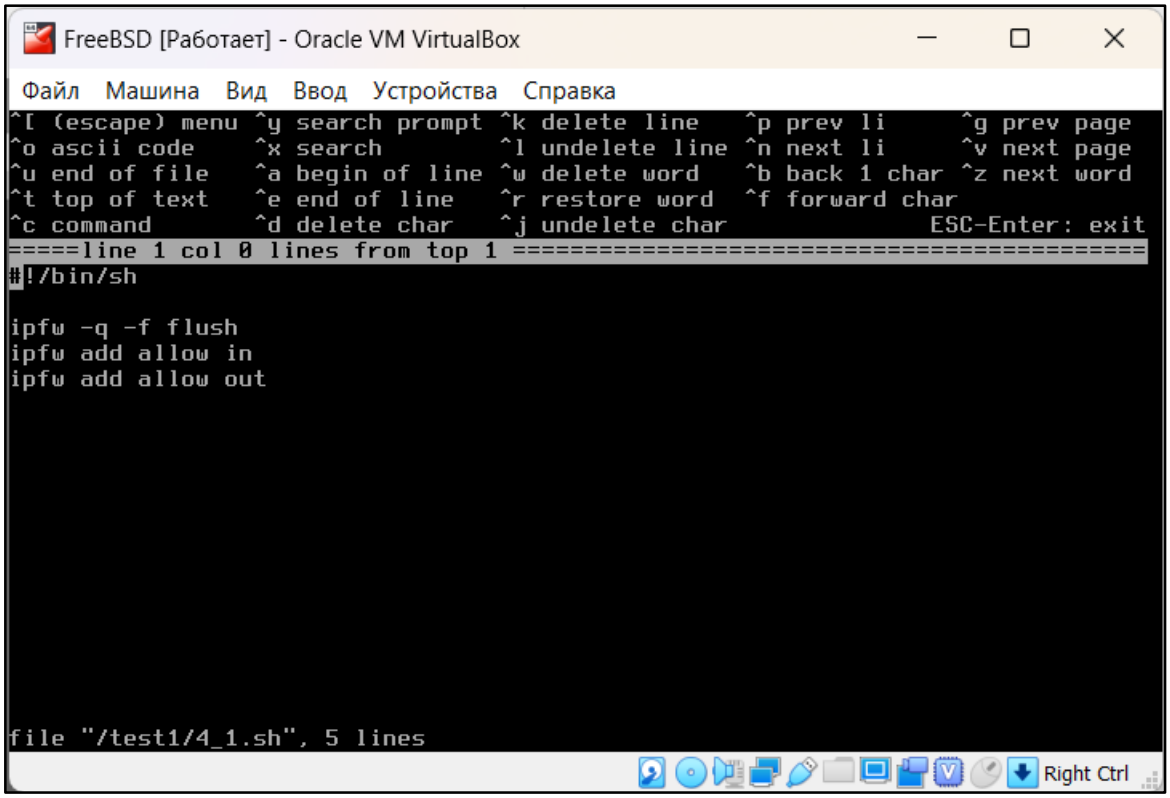

Рис. 7. Демонстрация написанного скрипта правил

```
root@root:~/script # ./1_4_1.sh
00100 allow in
00200 allow out
```

Рис. 8. Демонстрация работы скрипта правил

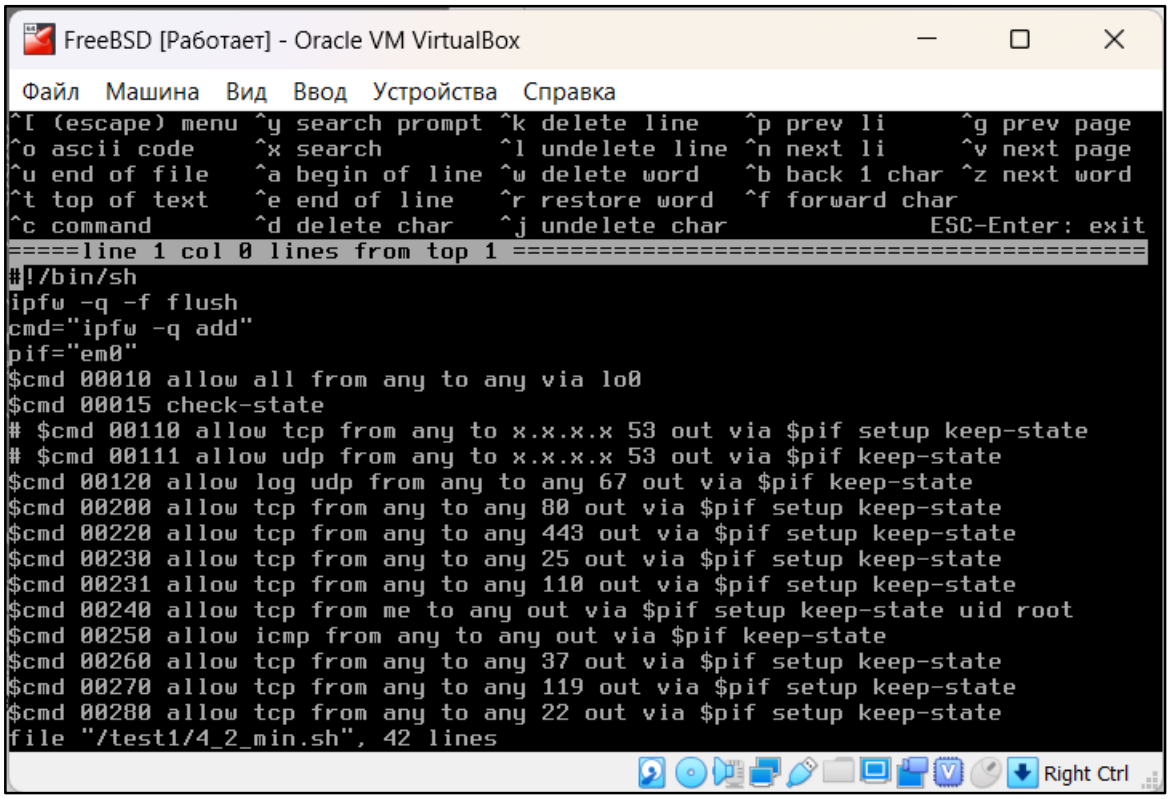

Рис. 9. Демонстрация правил для межсетевого экрана закрытого типа

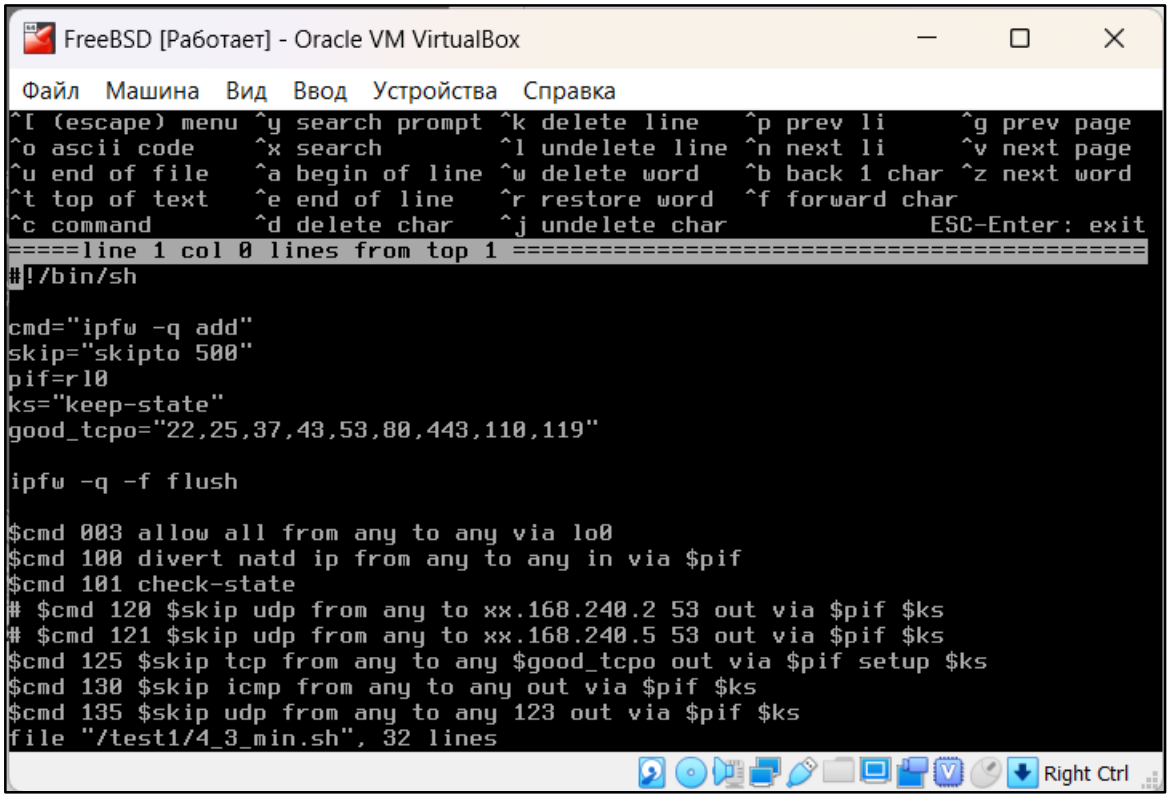

Рис. 10. Демонстрация правил с сохранением состояний и поддержкой NAT

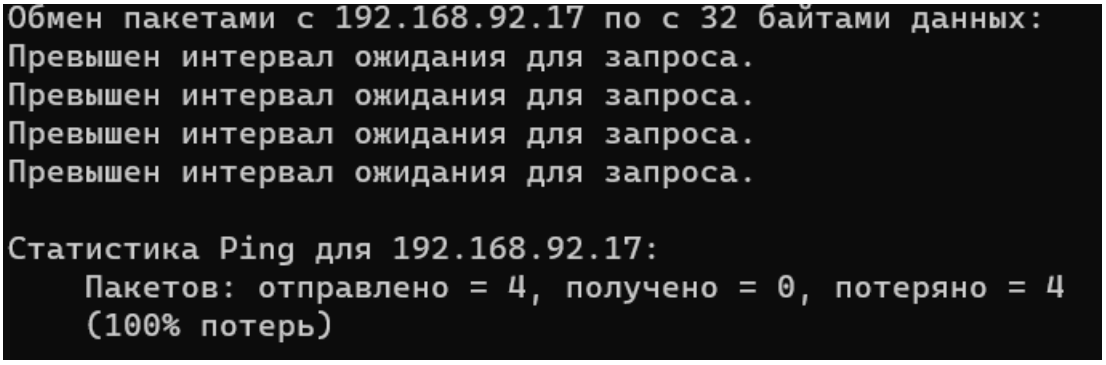

Рис. 11. Попытка обратиться по сети к виртуальной машине

Вывод: в ходе выполнения данной лабораторной работы были приобретены практические навыки по настройке межсетевого экрана.

Контрольные вопросы:

1. Опишите назначение межсетевого экрана.

Межсетевые экраны (firewall, брандмауэр) делают возможной фильтрацию входящего и исходящего трафика, идущего через систему. Межсетевой экран использует один или более наборов "правил" для проверки сетевых пакетов при их входе или выходе через сетевое соединение, он или позволяет прохождение трафика или блокирует его. Правила межсетевого экрана могут проверять одну или более характеристик пакетов, включая, но не ограничиваясь типом протокола, адресом хоста источника или назначения и портом источника или назначения.

2. Назовите задачи, которые выполняет межсетевой экран.

Межсетевые экраны могут серьезно повысить уровень безопасности хоста или сети. Они могут быть использованы для выполнения одной или более нижеперечисленных задач: для защиты и изоляции приложений, сервисов и машин во внутренней сети от нежелательного трафика, приходящего из внешней сети интернет. Для ограничения или запрещения доступа хостов внутренней сети к сервисам внешней сети интернет. Для поддержки преобразования сетевых адресов (network address translation, NAT), что позволяет использование во внутренней сети приватных IP адресов (либо через один выделенный IP адрес, либо через адрес из пула автоматически присваиваемых публичных адресов).

3. Опишите принцип работы межсетевого экрана.

Существует два основных способа создания наборов правил межсетевого экрана: "включающий" и "исключающий". Исключающий межсетевой экран позволяет прохождение всего трафика, за исключением трафика, соответствующего набору правил. Включающий межсетевой экран действует прямо противоположным образом. Он пропускает только трафик, соответствующий правилам, и блокирует все остальное. Включающий межсетевой экран обеспечивает гораздо большую

степень контроля исходящего трафика. Поэтому включающий межсетевой экран является лучшим выбором для систем, предоставляющих сервисы в сети Интернет. Он также контролирует тип трафика, порождаемого вне и направляющегося в вашу приватную сеть. Трафик, не попавший в правила, блокируется, а в файл протокола вносятся соответствующие записи. Включающие межсетевые экраны обычно более безопасны, чем исключающие, поскольку они существенно уменьшают риск пропуска межсетевым экраном нежелательного трафика.

4. Назовите существующие пакеты межсетевого экрана.

В FreeBSD встроено три программных межсетевых экрана. Это IPFILTER (известный также как IPF), IPFIREWALL (известный также как IPFW) и OpenBSDPacketFilter (также известный как PF). Помимо этого, FreeBSD содержит два пакета ограничения трафика (шейпера): altq и dummynet. Dummynet традиционно сильно связан с IPFW, а ALTQ с PF. В настоящее время IPFILTER не поддерживает ограничение пропускной способности сетевого соединения. Для реализации этой функции предлагается использовать IPFILTER совместно с одним из двух существующих пакетов ограничения трафика. Конфигурация следующая: IPFILTER задействуется для фильтрации и трансляции трафика, а IPFW с dummynetили PF с ALTQ — для контроля пропускной способности сетевого соединения. IPFW и PF для контроля исходящих и входящих пакетов используют наборы правил, хотя и разными способами с разным синтаксисом правил.

5. Опишите синтаксис правил межсетевого экрана.

- `CMD` – каждое новое правило должно начинаться с префикса `add` для добавления во внутреннюю таблицу.
- RULE_NUMBER – каждое правило обозначено номером в диапазоне 1...65535.
- `ACTION` – при соответствии пакета описанным в правиле критериям фильтрации будет выполнено одно из действий.
- `LOGGING` – когда пакет совпадает с правилом, содержащим ключевое слово `log`, информация об этом событии записывается в syslogd с пометкой SECURITY.
- `SELECTION` – ключевые слова, представленные в этом разделе, используются для описания атрибутов пакета, по которым проверяется условие срабатывания того или иного правила.
- `STATEFUL` – с точки зрения фильтрации по правилам с сохранением состояния весь трафик выглядит как двусторонний обмен пакетами, включая данные о сессиях. При такой фильтрации у нас есть средства сопоставления и определения корректности процедуры двустороннего обмена пакетами между стороной, породившей пакет, и стороной-получателем. Любые

пакеты, которые не подходят под шаблон сессии, автоматически отбрасываются как злонамеренные. Параметр `check-state` служит для указания места в наборе правил IPFW, в котором пакет будет передан на поиск соответствий динамическим правилам. В случае совпадения пакет пропускается, при этом создается новое динамическое правило для следующего пакета, принадлежащего данной двусторонней сессии. В противном случае пакет движется по обычным правилам, начиная со следующей позиции.

6. Дайте определение NAT.

Это механизм в сетях TCP/IP, позволяющий изменять IP-адрес в заголовке пакета, проходящего через устройство маршрутизации трафика. Также имеет названия IP Masquerading, Network Masquerading и Native Address Translation.

7. Охарактеризуйте понятие «Правило с сохранением состояния»

Такой межсетевой экран сохраняет информацию об открытых соединениях и разрешает только трафик через открытые соединения или открытие новых соединений. Недостаток межсетевого экрана с сохранением состояния в том, что он может быть уязвим для атак DoS (DenialofService, отказ в обслуживании), если множество новых соединений открывается очень быстро. Большинство межсетевых экранов позволяют комбинировать поведение с сохранением 8 состояния и без сохранения состояния, что позволяет создавать оптимальную конфигурацию для каждой конкретной системы.

8. Охарактеризуйте понятие «Правило без сохранения состояния»

Правила без сохранения состояния обеспечивают расширенные возможности фильтрации, которые намного превосходят уровень знаний обычного пользователя межсетевого экрана.

9. Изложите концепцию межсетевого экрана открытого типа.

Открытый межсетевой экран позволяет прохождение всего трафика, за исключением трафика, соответствующего набору правил.

10. Изложите концепцию межсетевого экрана закрытого типа.

Закрытый межсетевой экран пропускает только трафик, соответствующий правилам, и блокирует все остальное.

11. Объясните, как включить IPWF.

IPFW включён в базовую установку FreeBSD в виде отдельного подгружаемого модуля. Система динамически загружает модуль ядра, когда в rc.conf присутствует

строка firewall_enable="YES". Если использовать функциональность NAT не планируется, то в этом случае дополнительно компилировать IPFW в состав ядра FreeBSD не требуется.

12. Опишите процесс настройки межсетевого экрана.

Первый вариант — использовать настройки, предлагаемые в файле /etc/rc.firewall. Для это — указываем тип нашего фаервола:

- open — пропускаем весь траффик;
- client — будет защищать только эту машину;
- simple — защита всей сети;
- closed — полностью выключает весть IP траффик; исключая loopback интерфейс.

В таком случае, опция в /etc/rc.conf будет выглядеть, например, так: firewall_type="open".
Более правильный вариант — переопределить файл настроек IPFW, и создать собственный набор правил. Для этого указываем опцию: firewall_script="/etc/ipfw.rules", где /etc/ipfw.rules — наш созданный файл с правилами.