

**Министерство науки и высшего образования Российской Федерации  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет безопасности информационных технологий**

**Дисциплина:**

«Вычислительные сети и контроль безопасности в компьютерных сетях»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №3**

«Настройка межсетевого экрана»

**Выполнили:**

Чу Ван Доан, студент группы N3347



---

(подпись)

Чан Бао Линь, студентка группы N3346



---

(подпись)

**Проверил:**

Савков Сергей Витальевич, инженер факультета БИТ

---

(отметка о выполнении)

---

(подпись)

Санкт-Петербург

2025 г.

## СОДЕРЖАНИЕ

<b>Содержание.....</b>	<b>2</b>
<b>Введение.....</b>	<b>3</b>
<b>1. Задание.....</b>	<b>4</b>
<b>2. Ход работы.....</b>	<b>5</b>
2.1. Подготовка практического стенда.....	5
2.1.1. Создание виртуальной машины Firewall.....	5
2.1.2. Создание виртуальной машины RemoteServerVM.....	7
2.1.3. Создание виртуальной машины ClientVM.....	8
2.1.4. Предисловие (выполняется на FirewallVM).....	9
2.2. Блокировка всех входящих Telnet-соединений с адреса 10.10.10.10.....	10
2.3. Блокировка входящих TCP-запросов, не иницирующих новое соединение и не относящихся к установленным соединениям.....	11
2.3.1. Блокировка пакетов в состоянии INVALID.....	12
2.3.2. Блокировка TCP-пакетов в состоянии NEW, но без флага SYN.....	12
2.4. Ограничить количество параллельных соединений к серверу SSH для одного адреса - не более 3 соединений одновременно.....	15
2.5. Ограничение ICMP echo-request (ping) до 1 раза в секунду.....	19
2.5.1. Разрешено максимум 1 ping-пакет в секунду.....	19
<b>Заключение.....</b>	<b>23</b>

## **ВВЕДЕНИЕ**

Цель работы – Изучить на примере netfilter/iptables основные принципы работы межсетевых экранов. Освоить базовую настройку правил iptables

Для достижения поставленной цели необходимо решить следующие задачи:

- Настроить лабораторный стенд, включающий:
  - Локальный сервер / Межсетевой экран
  - Клиент
  - Удаленный сервер
- Настроить маршрутизацию проходящего трафика на локальном сервере;
- Выполнить необходимые настройки межсетевого экрана на локальном сервере в соответствии с заданием;
- Протестировать работу выполненных настроек;
- Результаты выполнения работы оформить в виде отчета.

## 1. Задание

Вариант 3:

- Заблокировать все входящие Telnet-соединения с адреса 10.10.10.10
- Установить блокировку для входящих запросов TCP не открывающих новое соединение и не принадлежащих никакому из установленных соединений
- Ограничить количество параллельных соединений к серверу SSH для одного адреса - не более 3 соединений одновременно
- Необходимо сделать так, чтобы ICMP пакеты типа echo- request принимались не более одного раза в секунду

## 2. Ход работы

### 2.1. Подготовка практического стенда

Установим гипервизор Oracle VirtualBox. Хостовая машина - GNU/Linux на основе Debian.

Подготовленный стенд состоит из трёх Ubuntu машин:

Локальный сервер (Local Server / Firewall)

- Установлена операционная система Linux (например: Ubuntu, Debian, CentOS...)
- Включена функция IP forwarding, чтобы можно было маршрутизировать пакеты между сетями.
- Здесь мы будем настраивать iptables в качестве межсетевого экрана.

Клиентская машина (Client)

- Предполагаемый IP-адрес: 10.10.10.10
- Попытка подключиться по Telnet, SSH, Ping — для проверки правил фаервола.

Удалённый сервер (Remote Server)

- Предполагаемый IP-адрес: 192.168.100.100 (или другой, в зависимости от цели).
- Выполняет роль сервера для проверки SSH, Telnet и других сетевых пакетов.

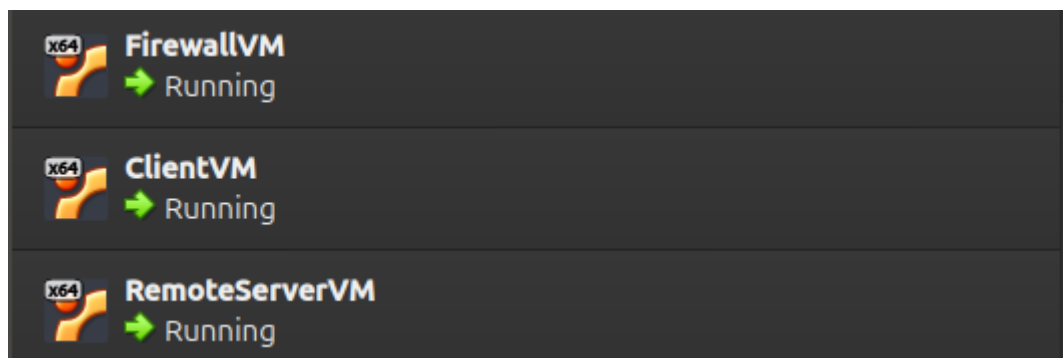


Рисунок 1 – Список виртуальных машин

#### 2.1.1. Создание виртуальной машины Firewall

- Создание виртуальной машины (VM) “FirewallVM”
- Настройка сетевых адаптеров (Network Adapter):
  - Адаптер 1: Подключён к Internal Network, Имя: intnetA
  - Адаптер 2: Подключён к Internal Network, Имя: intnetB

- Таким образом, у этой виртуальной машины два сетевых адаптера, каждый из которых подключён к разной «внутренней сети».

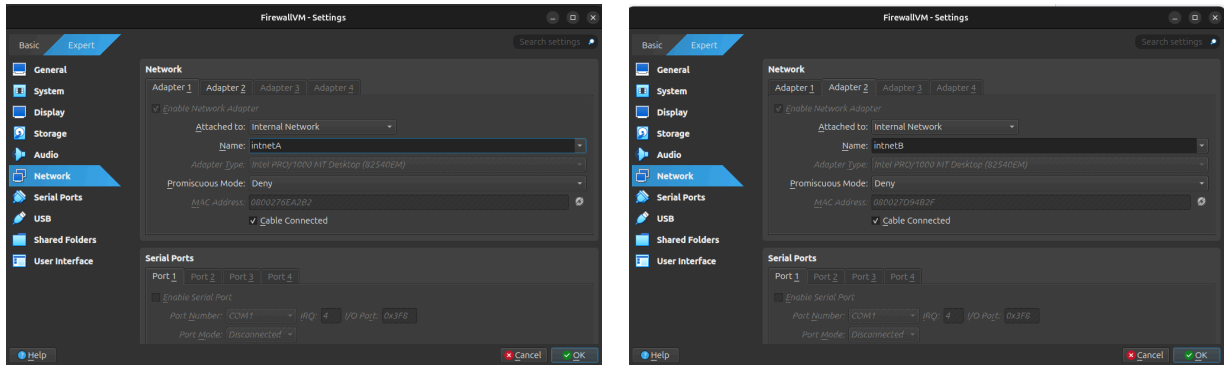


Рисунок 2 – Настройка сетевых адаптеров на виртуальной машине FirewallVM

- Конфигурация сети:

```
sudo nano /etc/network/interfaces
```

```
# Loopback interface
```

```
auto lo
```

```
iface lo inet loopback
```

```
# Configuration for eth0
```

```
auto eth1
```

```
iface eth1 inet static
```

```
address 10.10.10.1
```

```
netmask 255.255.255.0
```

```
# Configuration for eth1
```

```
auto eth2
```

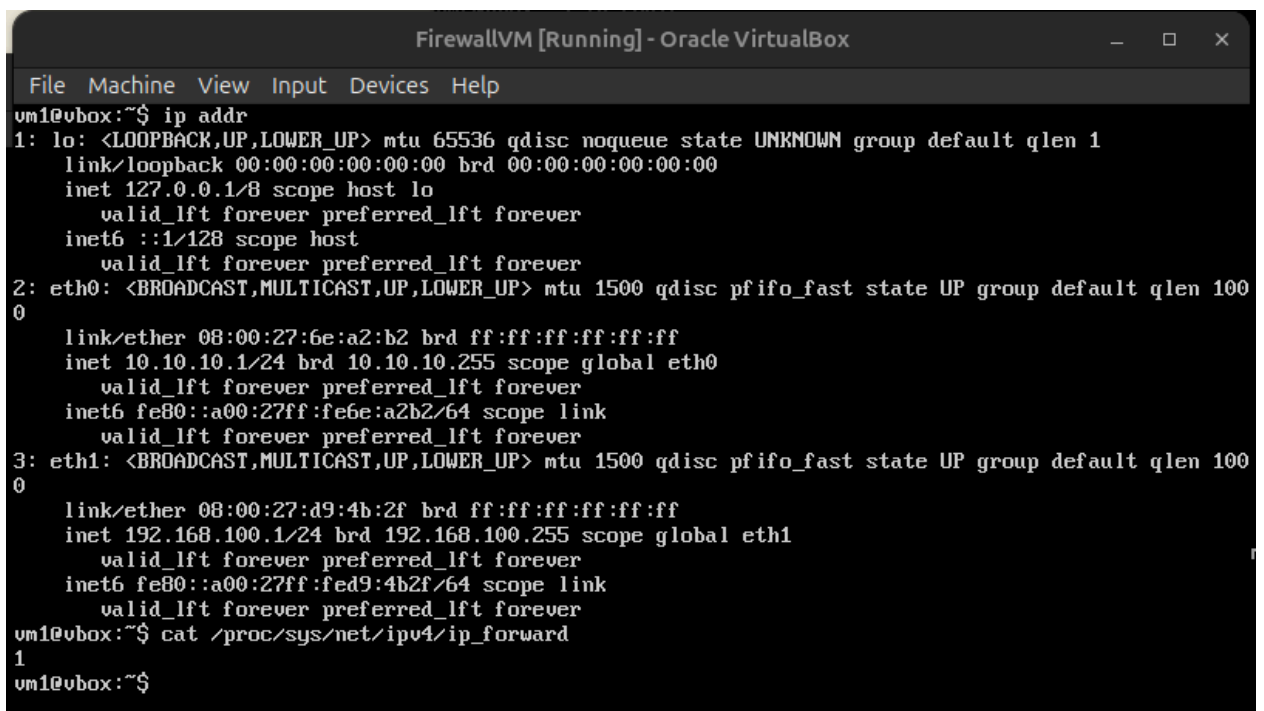
```
iface eth2 inet static
```

```
address 192.168.100.1
```

```
netmask 255.255.255.0
```

- Мы включим IP forwarding: Чтобы FirewallVM выполняла роль маршрутизатора между двумя сетями 10.10.10.0/24 и 192.168.100.0/24

```
net.ipv4.ip_forward = 1
```



```
File Machine View Input Devices Help
vm1@vbox:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:6e:a2:b2 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.1/24 brd 10.10.10.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe6e:a2b2/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d9:4b:2f brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.1/24 brd 192.168.100.255 scope global eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed9:4b2f/64 scope link
        valid_lft forever preferred_lft forever
vm1@vbox:~$ cat /proc/sys/net/ipv4/ip_forward
1
vm1@vbox:~$
```

Рисунок 3 – Настройка сетевых машине FirewallVM

### 2.1.2. Создание виртуальной машины RemoteServerVM

- Создание виртуальной машины (VM) RemoteServerVM
- Адаптер 1: Подключён к **Internal Network**
- Имя: intnetB (та же сеть, что и интерфейс eth1 на Firewall)

#### # Loopback interface

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet static

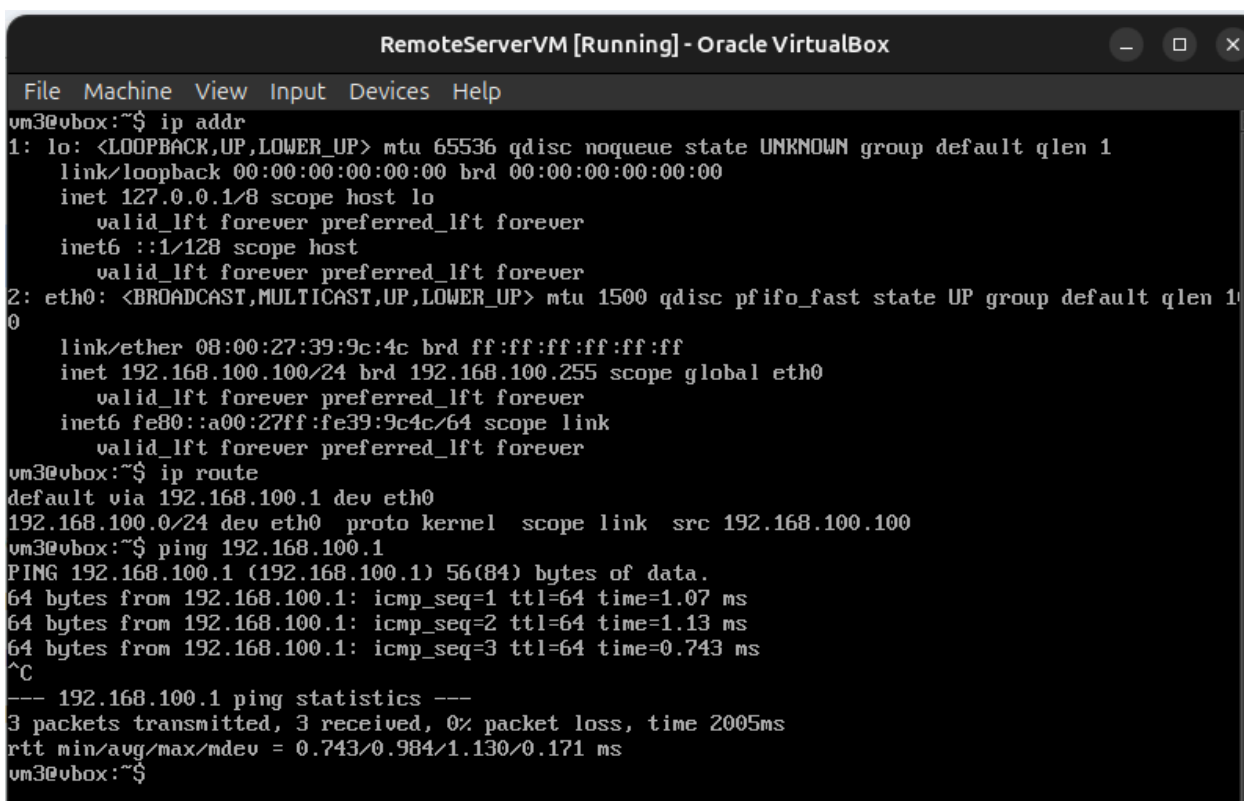
address 192.168.100.100

netmask 255.255.255.0

gateway 192.168.100.1

dns-nameservers 8.8.8.8 1.1.1.1

- Провести проверку соединения



```
RemoteServerVM [Running] - Oracle VirtualBox
File Machine View Input Devices Help
vm3@vbox:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1
    link/ether 08:00:27:39:9c:4c brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.100/24 brd 192.168.100.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe39:9c4c/64 scope link
        valid_lft forever preferred_lft forever
vm3@vbox:~$ ip route
default via 192.168.100.1 dev eth0
192.168.100.0/24 dev eth0 proto kernel scope link src 192.168.100.100
vm3@vbox:~$ ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
64 bytes from 192.168.100.1: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=64 time=1.13 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=64 time=0.743 ms
^C
--- 192.168.100.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.743/0.984/1.130/0.171 ms
vm3@vbox:~$
```

Рисунок 4 – Настройка сетевых машине RemoteServerVM

### 2.1.3. Создание виртуальной машины ClientVM

- Создание виртуальной машины (VM) ClientVM.
- Настройка сетевого адаптера:
  - Адаптер 1: Подключён к Internal Network
  - Имя: intnetA (та же сеть, что и интерфейс eth0 на Firewall)

nano /etc/network/interfaces

# Loopback interface

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet static

address 10.10.10.10

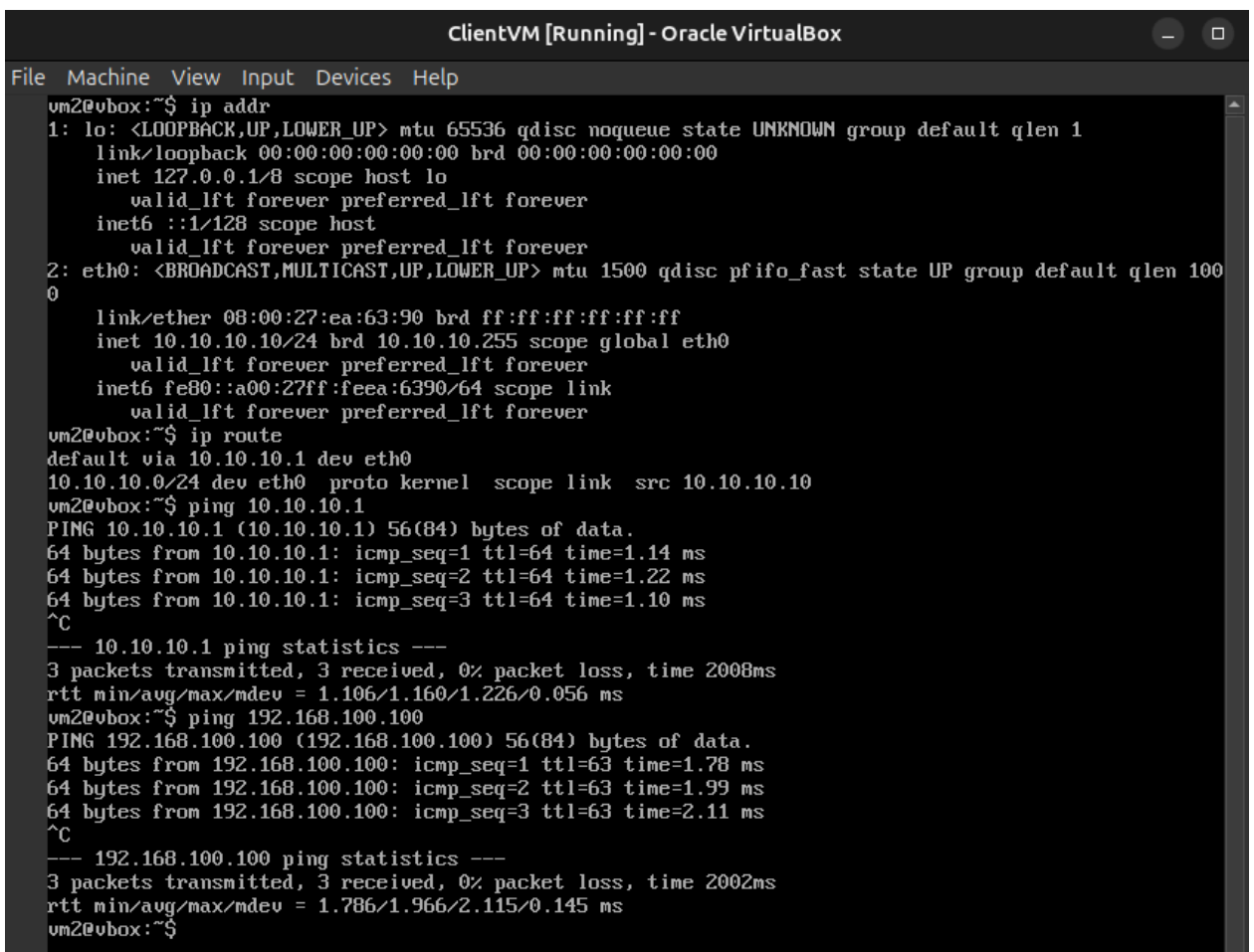
netmask 255.255.255.0

gateway 10.10.10.1

dns-nameservers 8.8.8.8 1.1.1.1

- Провести проверку соединения





```
ClientVM [Running] - Oracle VirtualBox
File Machine View Input Devices Help
vm2@vbox:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:ea:63:90 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.10/24 brd 10.10.10.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feea:6390/64 scope link
        valid_lft forever preferred_lft forever
vm2@vbox:~$ ip route
default via 10.10.10.1 dev eth0
10.10.10.0/24 dev eth0 proto kernel scope link src 10.10.10.10
vm2@vbox:~$ ping 10.10.10.1
PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_seq=1 ttl=64 time=1.14 ms
64 bytes from 10.10.10.1: icmp_seq=2 ttl=64 time=1.22 ms
64 bytes from 10.10.10.1: icmp_seq=3 ttl=64 time=1.10 ms
^C
--- 10.10.10.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 1.106/1.160/1.226/0.056 ms
vm2@vbox:~$ ping 192.168.100.100
PING 192.168.100.100 (192.168.100.100) 56(84) bytes of data.
64 bytes from 192.168.100.100: icmp_seq=1 ttl=63 time=1.78 ms
64 bytes from 192.168.100.100: icmp_seq=2 ttl=63 time=1.99 ms
64 bytes from 192.168.100.100: icmp_seq=3 ttl=63 time=2.11 ms
^C
--- 192.168.100.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.786/1.966/2.115/0.145 ms
vm2@vbox:~$
```

Рисунок 5 – Настройка сетевых машине ClientVM

#### 2.1.4. Предисловие (выполняется на FirewallVM)

- Прежде чем настраивать конкретные правила, рекомендуется сбросить iptables и установить политики по умолчанию:
- Шаг 1: Сброс и установка политик по умолчанию

# Выполнять с root-правами

```
iptables -F
```

```
iptables -X
```

```
iptables -t nat -F
```

```
iptables -t nat -X
```

# Политики по умолчанию:

```
iptables -P INPUT DROP
```

```
iptables -P FORWARD DROP
```

```
iptables -P OUTPUT ACCEPT
```

- Шаг 2: Разрешить допустимые и необходимые подключения

# Разрешить loopback-интерфейс

```
iptables -A INPUT -i lo -j ACCEPT
```

# Разрешить пакеты, относящиеся к уже установленным соединениям

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

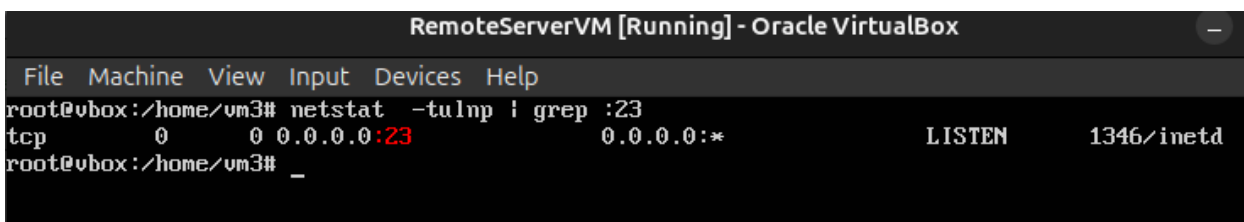
```
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

# Разрешить SSH-доступ к самому Firewall (если вы подключаетесь по SSH)

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

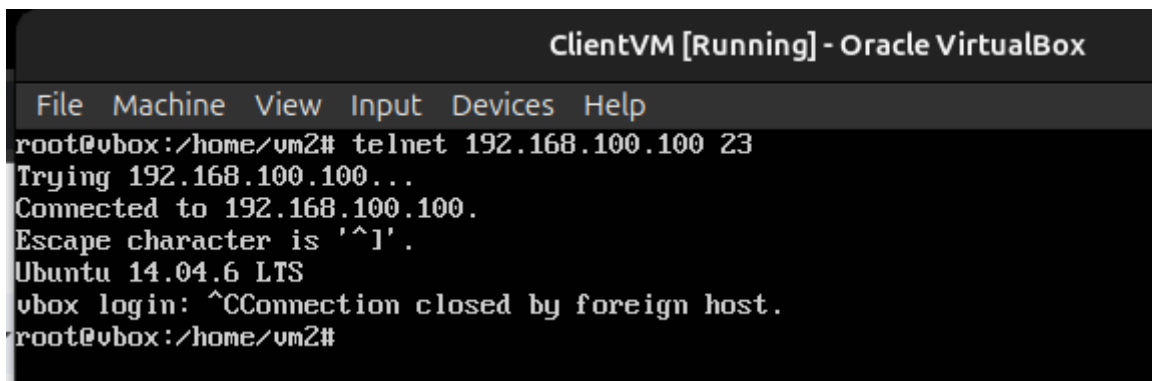
## 2.2. Блокировка всех входящих Telnet-соединений с адреса 10.10.10.10

- Перед настройкой:



```
RemoteServerVM [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox:/home/vm3# netstat -tulnp | grep :23
tcp        0      0 0.0.0.0:23 0.0.0.0:*        LISTEN      1346/inetd
root@vbox:/home/vm3# _
```

Рисунок 6 – Telnet-сервер запущен и слушает

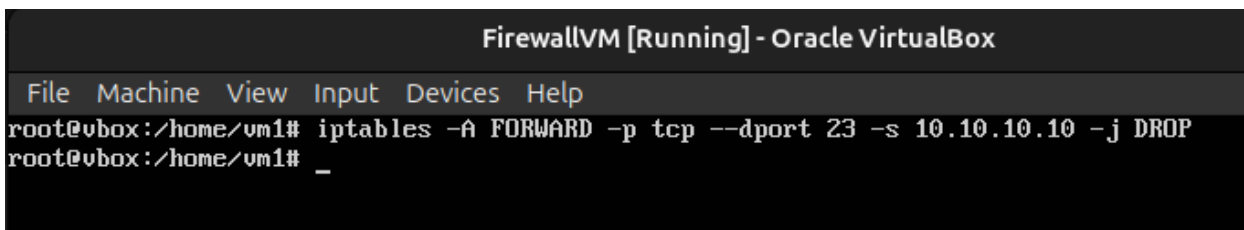


```
ClientVM [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox:/home/vm2# telnet 192.168.100.100 23
Trying 192.168.100.100...
Connected to 192.168.100.100.
Escape character is '^I'.
Ubuntu 14.04.6 LTS
vbox login: ^CConnection closed by foreign host.
root@vbox:/home/vm2#
```

Рисунок 7 – Telnet работает успешно

- Telnet использует порт TCP 23.
- Поскольку клиент хочет подключиться к RemoteServer через Firewall, мы блокируем в **FORWARD chain**.

```
iptables -A FORWARD -p tcp --dport 23 -s 10.10.10.10 -j DROP
```



```
FirewallVM [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox:/home/vm1# iptables -A FORWARD -p tcp --dport 23 -s 10.10.10.10 -j DROP
root@vbox:/home/vm1# _
```

Рисунок 8 – Настройка машины FirewallVM

- Просмотр списка правил с нумерацией строк:

```
sudo iptables -L -v --line-numbers
```

```

FirewallVM1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox:/home/vm1# iptables -L -v --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source destination
1      0      0 DROP      tcp  --  any    any     10.10.10.10 anywhere
t:telnet
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source destination
root@vbox:/home/vm1#

```

Рисунок 9 – Просмотр списка правил с нумерацией строк

- Проверка на ClientVM:

```
telnet 192.168.100.100 23
```

```

ClientVM [Running] - Oracle VirtualBox
File Machine View Input Devices Help
vm2@vbox:~$ telnet 192.168.100.100 23
Trying 192.168.100.100...

```

Рисунок 10 – Проверка на ClientVM

Результат — зависание → это правильно

### 2.3. Блокировка входящих TCP-запросов, не иницирующих новое соединение и не относящихся к установленным соединениям.

- Блокировать входящие TCP-пакеты, которые:
  - Не относятся к существующему соединению
  - Не иницируют новое соединение корректным образом
  - Или находятся в состоянии **INVALID**
- Существуют 4 основных состояния:

Состояние	Значение
NEW	Первый пакет для установления нового соединения
ESTABLISHED	Пакет, относящийся к уже установленному и принятому соединению

<b>RELATED</b>	Связанный пакет (например, FTP data, связанный с FTP control)
<b>INVALID</b>	Пакет не соответствует никакому состоянию — обычно ошибочный, поддельный или недопустимый

Нам нужно:

- Блокировать все пакеты в состоянии INVALID
- Блокировать пакеты в состоянии NEW, но без флага SYN (так как пакет, открывающий новое соединение, всегда должен содержать SYN)

### 2.3.1. Блокировка пакетов в состоянии INVALID

- Настройка iptables – На FirewallVM:

```
sudo iptables -A FORWARD -m state --state INVALID -j DROP
```

```

File Machine View Input Devices Help
root@vbox:/home/vm1# iptables -A FORWARD -m state --state INVALID -j DROP
root@vbox:/home/vm1# iptables -L -v --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source         destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source         destination
1    15   900 DROP      tcp  --  any    any     10.10.10.10    anywhere      tcp dp
t:telnet
2     0     0 DROP      all  --  any    any     anywhere      anywhere      state
INVALID
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source         destination
root@vbox:/home/vm1#

```

Рисунок 11 – Настройка блокировки пакетов в состоянии INVALID на FirewallVM

### 2.3.2. Блокировка TCP-пакетов в состоянии NEW, но без флага SYN

- Если это начальный TCP-пакет (NEW), но без флага SYN → блокировать.
- Корректное TCP-соединение всегда начинается с пакета с флагом SYN
- Если пакет имеет состояние NEW (то есть инициирует новое соединение), но не содержит флага SYN, то: Это может быть ошибочный, поддельный пакет или признак атаки (например, spoofing).

```
sudo iptables -A FORWARD -p tcp -m state --state NEW ! --syn -j DROP
```

```

FirewallVM1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox:/home/vm1# iptables -A FORWARD -p tcp -m state --state NEW ! --syn -j DROP
root@vbox:/home/vm1# iptables -L -v --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source                 destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source                 destination
1    15   900 DROP      tcp  --  any    any    10.10.10.10            anywhere             tcp dp
t:telnet
2     0     0 DROP      all  --  any    any    anywhere               anywhere             state
INVALID
3     0     0 DROP      tcp  --  any    any    anywhere               anywhere             state
NEW tcp flags:!FIN,SYN,RST,ACK/SYN
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source                 destination
root@vbox:/home/vm1#

```

Рисунок 12 – Настройка блокировки подозрительных TCP-соединений на FirewallVM

### 2.3.3. Проверка отправки TCP-пакетов без флага SYN с ClientVM

- Установка утилиты hping3 на ClientVM:
- Отправка пользовательских пакетов (TCP, UDP, ICMP) → Позволяет проверить, как firewall, маршрутизатор или система обрабатывают различные типы пакетов.
- Тестирование межсетевого экрана (Firewall Testing) → Можно моделировать нестандартные соединения, например, TCP-пакеты без флага SYN, чтобы проверить правила iptables.
- Пентест (тестирование на проникновение):
  - Генерация пакетов TCP SYN, FIN, NULL, XMAS для проверки устойчивости к атакам.
  - Отправка фрагментированных пакетов, спуфинг IP-адресов (подделка IP).
- Проверка производительности и задержек (Latency, Packet Loss) → Похоже на ping, но с большим контролем: можно задавать порт, флаги TCP, размер пакета и т. д.

```

ClientVM [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox:/home/vm2# apt-get install hping3
Reading package lists... Done
Building dependency tree
Reading state information... Done
hping3 is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 27 not upgraded.
root@vbox:/home/vm2#

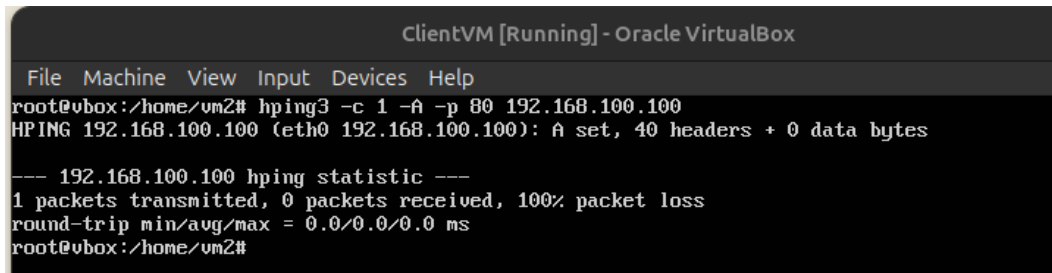
```

Рисунок 13 – Установка hping3 на ClientVM

```
sudo hping3 -c 1 -A -p 80 192.168.100.100
```

Пояснение:

- -c 1: отправить 1 пакет
- -A: только флаг ACK, без SYN
- -p 80: использовать порт 80 на сервере
- 192.168.100.100: IP-адрес сервера.



```
ClientVM [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox:/home/vm2# hping3 -c 1 -A -p 80 192.168.100.100
HPING 192.168.100.100 (eth0 192.168.100.100): A set, 40 headers + 0 data bytes

--- 192.168.100.100 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@vbox:/home/vm2#
```

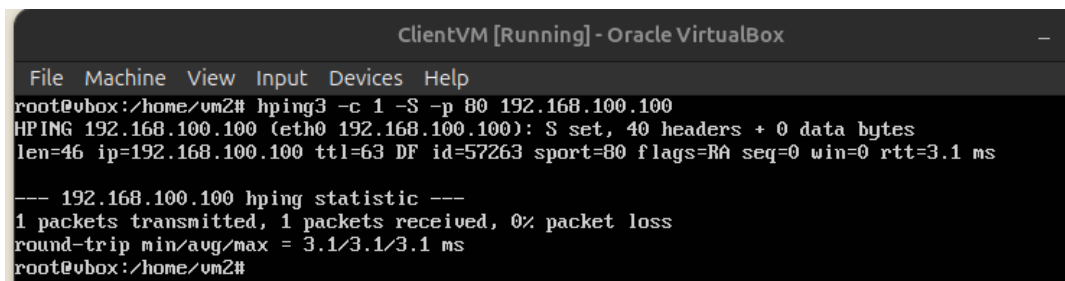
Рисунок 14 – Проверка отправки TCP-пакетов без флага SYN с ClientVM

-> Этот пакет будет отброшен (DROP), потому что он не содержит SYN, но имеет состояние NEW

- Отправка обычного SYN-пакета (для сравнения):

```
sudo hping3 -c 1 -S -p 80 192.168.100.100
```

-S: отправить пакет с флагом SYN



```
ClientVM [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox:/home/vm2# hping3 -c 1 -S -p 80 192.168.100.100
HPING 192.168.100.100 (eth0 192.168.100.100): S set, 40 headers + 0 data bytes
len=46 ip=192.168.100.100 ttl=63 DF id=57263 sport=80 flags=RA seq=0 win=0 rtt=3.1 ms

--- 192.168.100.100 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.1/3.1/3.1 ms
root@vbox:/home/vm2#
```

Рисунок 15 – Проверка отправки TCP-пакетов флага SYN с ClientVM

Это корректный пакет для установления соединения → не будет заблокирован

Проверка статистики iptables На FirewallVM:

```
sudo iptables -L -v --line-numbers
```

```

FirewallVM1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox:/home/vm1# iptables -L -v --line-numbers
Chain INPUT (policy ACCEPT 2 packets, 140 bytes)
num  pkts bytes target    prot opt in     out     source                 destination
Chain FORWARD (policy ACCEPT 889 packets, 897K bytes)
num  pkts bytes target    prot opt in     out     source                 destination
1    15  900 DROP      tcp  --  any    any    10.10.10.10            anywhere        tcp dp
t:telnet
2    0    0 DROP      all  --  any    any    anywhere               anywhere        state
INVALID
3    1    40 DROP      tcp  --  any    any    anywhere               anywhere        state
NEW tcp flags:!FIN,SYN,RST,ACK/SYN
Chain OUTPUT (policy ACCEPT 2 packets, 140 bytes)
num  pkts bytes target    prot opt in     out     source                 destination
root@vbox:/home/vm1#

```

Рисунок 16 – Проверка статистики iptables На FirewallVM

## 2.4. Ограничить количество параллельных соединений к серверу SSH для одного адреса - не более 3 соединений одновременно.

Ограничение количества одновременных SSH-соединений от одного клиента к RemoteServerVM через FirewallVM до трёх

Мы будем использовать модуль connlimit для ограничения количества одновременных подключений (то есть в один и тот же момент времени, не по времени).

Мы будем выполнять это на FirewallVM

`sudo iptables -A FORWARD -p tcp --dport 22 -m connlimit --connlimit-above 3 -j REJECT`

- `-p tcp`: применяется к протоколу TCP
- `--dport 22`: применяется к порту SSH
- `-m connlimit`: используется модуль ограничения соединений
- `--connlimit-above 3`: если количество соединений  $> 3 \rightarrow$  применяется действие
- `-j REJECT`: отклонить соединение (в отличие от DROP, REJECT отправляет пакет RST в ответ)

```
FirewallVM1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox:/home/vm1# iptables -A FORWARD -p tcp --dport 22 -m connlimit --connlimit-above 3 -j REJECT
root@vbox:/home/vm1# iptables -L -v --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination
1    15   900 DROP      tcp  --  any    any    10.10.10.10          anywhere        tcp dpt:telnet
2     0     0 DROP      all  --  any    any    anywhere             anywhere        state INVALID
3     1     40 DROP      tcp  --  any    any    anywhere             anywhere        state NEW tcp flags: !FIN,SYN,RST,ACK/SYN
4     0     0 REJECT    tcp  --  any    any    anywhere             anywhere        tcp dpt:ssh #conn src/32 > 3 reject-with icmp-port-unreachable
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination
root@vbox:/home/vm1# _
```

Рисунок 17 – Конфигурация на FirewallVM

Мы будем проверить:

- Убедитесь, что SSH запущен на RemoteServerVM

```
sudo apt-get install openssh-server
```

```
sudo service ssh restart
```

```
RemoteServerVM [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@vbox:/home/vm3# netstat -tulnp | grep :22
tcp        0      0 0.0.0.0:22          0.0.0.0:*        LISTEN      1946/sshd
tcp6       0      0 :::22             :::*             LISTEN      1946/sshd
root@vbox:/home/vm3# _
```

Рисунок 18 – Тест SSH запущен на RemoteServerVM

```
root@vbox:/home/vm2# ssh vm3@192.168.100.100
vm3@192.168.100.100's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
Last login: Fri Apr  4 01:06:32 2025
vm3@vbox:~$
```

Рисунок 19 – Подключите ClientVM к RemoteServerVM через SSH в первый раз



```
ClientVM [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Ubuntu 14.04.6 LTS vbox tty2
vbox login: vm2
Password:
Last login: Fri Apr 4 00:53:38 MSK 2025 on tty1
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
vm2@vbox:~$ su
Password:
root@vbox:/home/vm2# ssh vm3@192.168.100.100
vm3@192.168.100.100's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
Last login: Fri Apr 4 02:39:33 2025 from 10.10.10.10
vm3@vbox:~$ _
```

Рисунок 20 – Подключите ClientVM к RemoteServerVM через SSH в второй раз

```
ClientVM [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Ubuntu 14.04.6 LTS vbox tty3
vbox login: vm2
Password:
Last login: Fri Apr 4 02:39:58 MSK 2025 on tty2
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
vm2@vbox:~$ su
Password:
root@vbox:/home/vm2# ssh vm3@192.168.100.100
vm3@192.168.100.100's password:
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
Last login: Fri Apr 4 02:40:34 2025 from 10.10.10.10
vm3@vbox:~$ _
```

Рисунок 21 – Подключите ClientVM к RemoteServerVM через SSH в третий раз

```
ClientVM [Running] - Oracle VirtualBox
File Machine View Input Devices Help

Ubuntu 14.04.6 LTS vbox tty4

vbox login: vm2
Password:
Last login: Fri Apr  4 02:42:14 MSK 2025 on tty3
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
vm2@vbox:~$ su
Password:
root@vbox:/home/vm2# ssh vm3@192.168.100.100
ssh: connect to host 192.168.100.100 port 22: Connection refused
root@vbox:/home/vm2# _
```

Рисунок 22 – Подключите ClientVM к RemoteServerVM через SSH в четвертый раз  
-> Мы видим, что к RemoteServerVM одновременно можно подключить не более 3 пользователей.

```
RemoteServerVM [Running] - Oracle VirtualBox
File Machine View Input Devices Help

root@vbox:/home/vm3# who
vm3      tty1      2025-04-04 01:06
vm3      pts/0      2025-04-04 02:39 (10.10.10.10)
vm3      pts/1      2025-04-04 02:40 (10.10.10.10)
vm3      pts/3      2025-04-04 02:42 (10.10.10.10)
root@vbox:/home/vm3#
```

Рисунок 23 –Только три пользователя вошли в систему

```
FirewallVM1 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

root@vbox:/home/vm1# iptables -L -v --line-numbers
Chain INPUT (policy ACCEPT 1 packets, 70 bytes)
num  pkts bytes target    prot opt in     out     source         destination
Chain FORWARD (policy ACCEPT 496 packets, 745K bytes)
num  pkts bytes target    prot opt in     out     source         destination         tcp dp
1    15   900 DROP      tcp  --  any    any    10.10.10.10    anywhere            tcp dp
t:telnet
2     0     0 DROP      all  --  any    any    anywhere       anywhere            state
INVALID
3     1    40 DROP      tcp  --  any    any    anywhere       anywhere            state
NEW tcp flags:!FIN,SYN,RST,ACK/SYN
4     1    60 REJECT    tcp  --  any    any    anywhere       anywhere            tcp dp
t:ssh #conn src/32 > 3 reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT 2 packets, 158 bytes)
num  pkts bytes target    prot opt in     out     source         destination
root@vbox:/home/vm1# _
```

Рисунок 24 – Просмотр статистики iptables на FirewallVM

- Как выйти из сеанса SSH: Ctrl + D

## 2.5. Ограничение ICMP echo-request (ping) до 1 раза в секунду

### Цель:

Предотвратить **ping flood**, ограничив количество ICMP echo-request (ping) пакетов на сервер до **максимум 1 пакета в секунду**

(Тип пакета: ping, ICMP type 8)

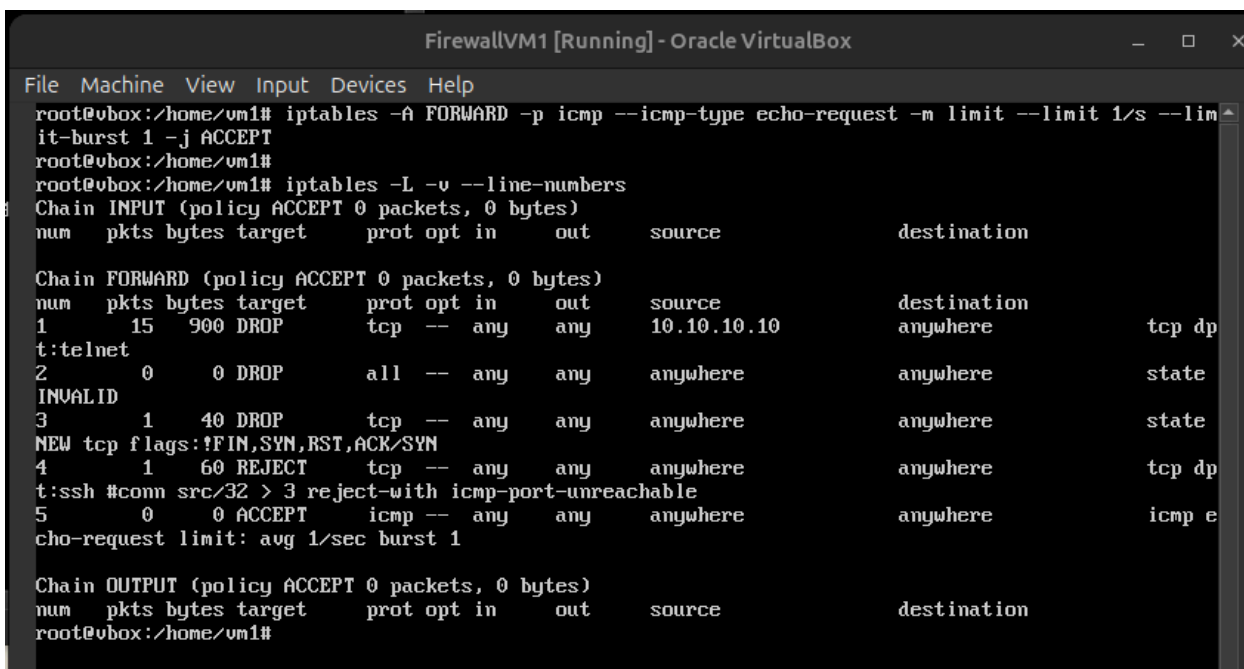
### Используемая техника:

Применяется модуль **limit** в iptables, позволяющий ограничить **частоту обработки пакетов**.

#### 2.5.1. Разрешено максимум 1 ping-пакет в секунду:

```
sudo iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s --limit-burst 1 -j ACCEPT
```

- --limit 1/s: ограничение обработки — не более 1 пакета в секунду
- --limit-burst 1: разрешить только 1 пакет сразу, затем — не более 1 пакета в секунду



```
File Machine View Input Devices Help
root@vbox:/home/vm1# iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s --limit-burst 1 -j ACCEPT
root@vbox:/home/vm1#
root@vbox:/home/vm1# iptables -L -v --line-numbers
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination
1    15   900 DROP      tcp  --  any    any    10.10.10.10         anywhere             tcp dptelnet
2      0      0 DROP      all  --  any    any    anywhere            anywhere             state INVALID
3      1     40 DROP      tcp  --  any    any    anywhere            anywhere             state NEW tcp flags:FIN,SYN,RST,ACK/SYN
4      1     60 REJECT    tcp  --  any    any    anywhere            anywhere             tcp dpt:ssh #conn src/32 > 3 reject-with icmp-port-unreachable
5      0      0 ACCEPT    icmp --  any    any    anywhere            anywhere             icmp echo-request limit: avg 1/sec burst 1
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target    prot opt in     out     source               destination
root@vbox:/home/vm1#
```

Рисунок 25 – Настройка допускает максимум 1 ping-пакет в секунду.

#### 2.5.2. Блокировать все остальные ICMP-пакеты

```
sudo iptables -A FORWARD -p icmp --icmp-type echo-request -j DROP
```

- Любой ping-пакет, превышающий вышеуказанное ограничение, будет отброшен (DROP).



- Только несколько! показать (пинг успешный)

-> Вывод: брандмауэр блокирует большинство пингов

- Подсчитайте ping на FirewallVM с помощью tcpdump:

`sudo tcpdump -i eth1 icmp`

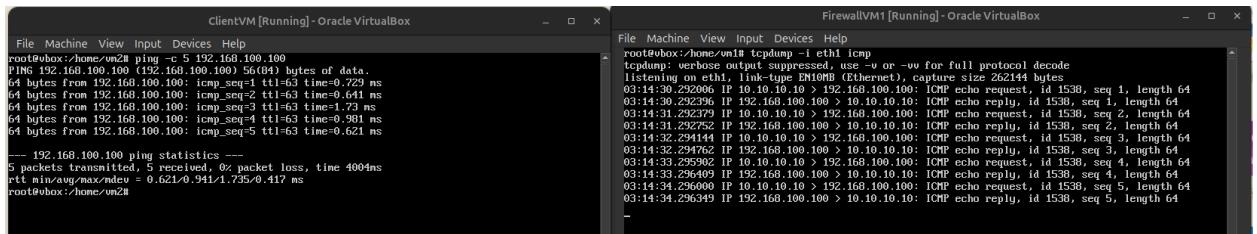


Рисунок 29 - Расчет ping на FirewallVM с помощью tcpdump

`sudo watch -n 1 "iptables -L -v --line-numbers"`

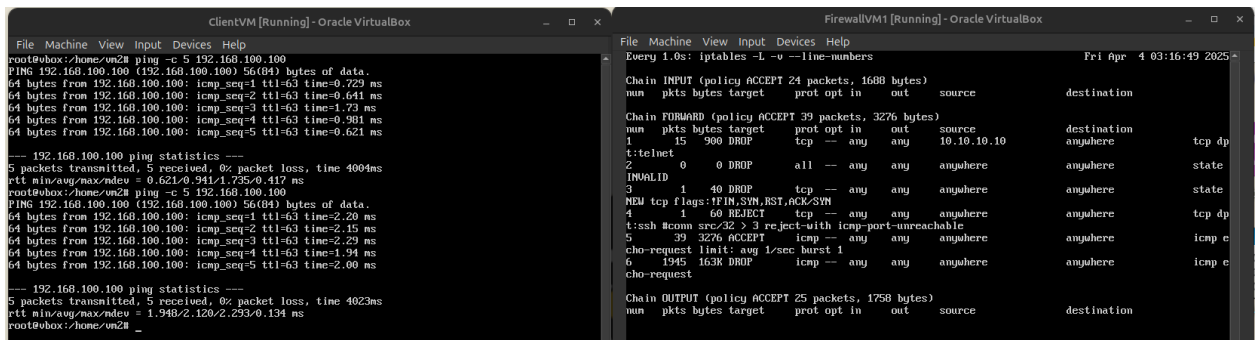


Рисунок 30 - Расчет ping на FirewallVM

## ЗАКЛЮЧЕНИЕ

В ходе выполнения данной лабораторной работы была изучена архитектура и принципы работы сетевого экрана на базе подсистемы **netfilter/iptables** в операционной системе Linux. Были реализованы основные правила фильтрации трафика, направленные на защиту локальной сети от нежелательной активности.

В частности, были выполнены следующие задачи:

- Реализована блокировка Telnet-соединений с заданного IP-адреса;
- Настроены правила для отбрасывания TCP-пакетов, не относящихся к существующим или правильно инициализированным соединениям;
- Установлено ограничение на количество одновременных SSH-соединений от одного клиента (не более трёх);
- Настроена фильтрация ICMP-запросов (ping) с ограничением частоты – не более одного запроса в секунду.

В процессе конфигурирования был построен виртуальный стенд, включающий **три виртуальные машины**: клиент, сервер и межсетевой экран. Проведено детальное тестирование каждого правила с использованием стандартных сетевых утилит (ping, ssh, telnet, hping3, tcpdump), что позволило убедиться в корректной работе настроек.

Таким образом, лабораторная работа позволила не только закрепить знания по работе с iptables, но и на практике реализовать ключевые принципы сетевой безопасности: фильтрацию по IP-адресу, по протоколу, по состоянию соединения и ограничение частоты доступа. Полученные навыки могут быть применены при построении защищённых сетевых инфраструктур.