

## Лабораторная работа 7. Межсетевое экранирование и трансляция сетевых адресов в GNU/Linux (nftables /netfilter).

### Задание.

Использовать виртуальные машины из предыдущих лабораторных работ. Развернуть виртуальную машину и установить на ней ОС Debian GNU/Linux, установить веб-сервер Apache. Сконфигурировать сетевые интерфейсы на виртуальных машинах в соответствии со схемой на рис.1.

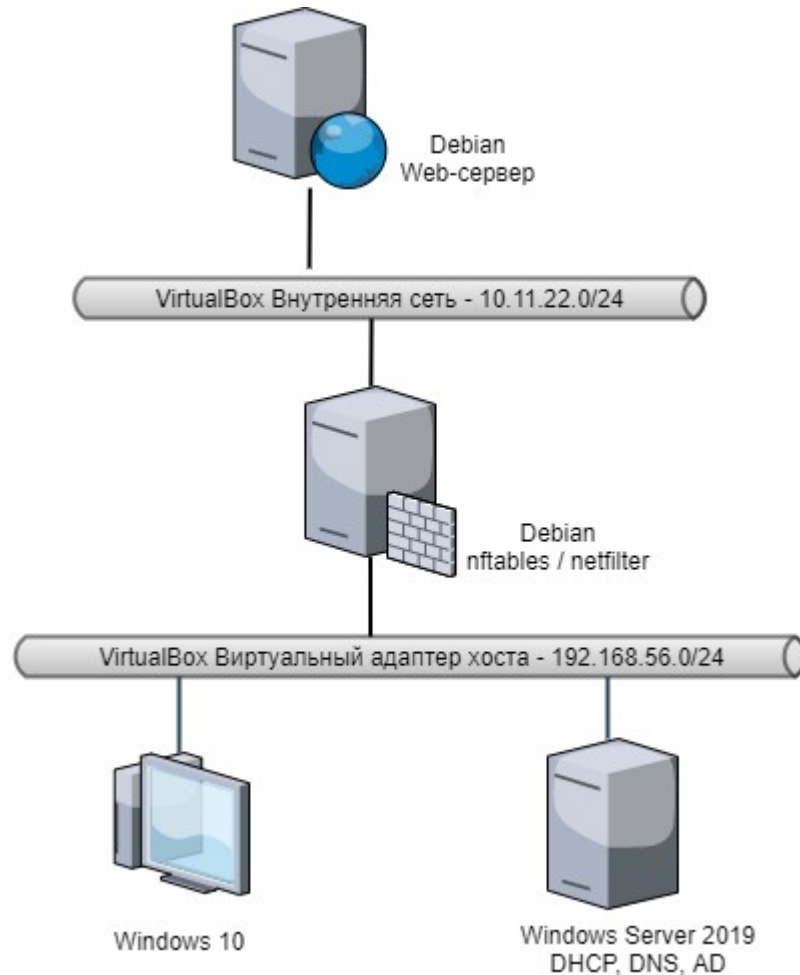


Рис. 1. Схема сети.

Условные обозначения:

Debian-Web — виртуальная машина, на которой разворачивается веб-сервер;

Debian-FW — виртуальная машина (из предыдущей лабораторной работы), на которой применяются правила межсетевого экранирования.

Настроить на Debian-FW пересылку пакетов между интерфейсами. Проверить полную доступность сетевых соединений между Windows 10 и Debian-Web. Настроить фильтрацию сетевых пакетов, а также трансляцию сетевых адресов на Debian-FW средствами nftables /netfilter. Провести повторные проверки сетевых соединений, а также анализ сетевых пакетов.

### Этапы выполнения.

- 1) В Oracle VM VirtualBox создать новую виртуальную машину для веб-сервера на ОС Debian GNU/Linux (Debian-Web). Параметры развертывания VM оставить в значениях по умолчанию.
- 2) Установить на созданной виртуальной машине ОС Debian GNU/Linux по рекомендациям из предыдущей лабораторной работы. На этапе выбора программного обеспечения оставить отмеченным только пункт «Стандартные системные утилиты».
- 3) В Oracle VM VirtualBox в настройках созданной виртуальной машины Debian-Web изменить тип сетевого подключения на «Внутреннюю сеть» (рис. 2.).

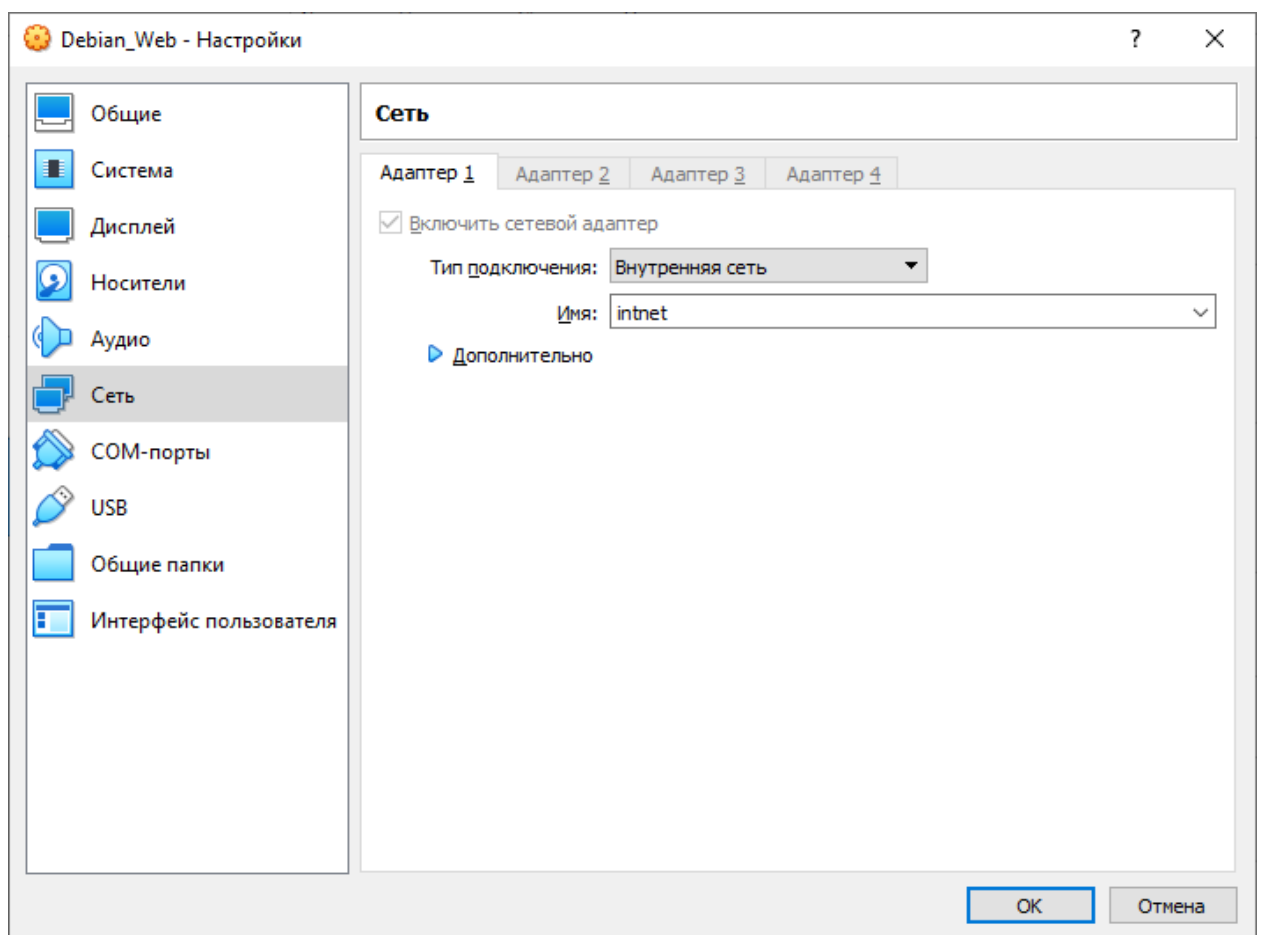


Рис. 2. Настройка сетевого адаптера.

- 4) Настроить статический IP-адрес на Debian-Web по рекомендациям из предыдущей лабораторной работы. Сетевые параметры, которые необходимо настроить:

IP-адрес — 10.11.22.33

Маска сети — 255.255.255.0

Шлюз — 10.11.22.101

Для применения новых сетевых настроек следует перезапустить службу networking:

```
sudo systemctl restart networking
```

5) Изменить сетевое имя узла Debian-Web на «debian-web». Для этого следует отредактировать файл /etc/hostname, и заменить «debian» на «debian-web». Такую же замену необходимо провести в файле /etc/hosts.

После этого перезагрузить ОС, командой «sudo reboot».

Содержимое файлов /etc/hostname и /etc/hosts после редактирования — на рис.3.

```
user@debian-web:~$ cat /etc/hostname
debian-web
user@debian-web:~$ cat /etc/hosts
127.0.0.1    localhost
127.0.1.1    debian-web

# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
user@debian-web:~$
```

Рис.3. Содержимое файлов /etc/hostname и /etc/hosts.

6) Установить на Debian-Web веб-сервер Apache:

```
sudo apt install apache2
```

Проверить статус установленной службы веб-сервера:

```
sudo systemctl status apache2
```

Проверить список TCP сокетов, ожидающих соединения:

```
ss -tln
```

Убедиться, что прослушивается стандартный для HTTP веб-сервера TCP порт 80 (рис.4.)

```
user@debian-web:~$ ss -tln
State      Recv-Q    Send-Q     Local Address:Port      Peer Address:Port
LISTEN     0          128             *:80                      *:*
```

Рис.4. Список открытых TCP портов.

С помощью утилиты Wget подключиться к веб-серверу и скачать стандартный файл главной страницы сайта (index.html):

```
wget 10.11.22.33
```

или

```
wget localhost
```

где «localhost» – обращение узла по петлевому интерфейсу к самому себе.

Результат работы — на рис.5. Файл будет загружен в текущий каталог.

```
user@debian-web:~$ wget 10.11.22.33
--2020-11-01 20:08:03-- http://10.11.22.33/
Подключение к 10.11.22.33:80... соединение установлено.
HTTP-запрос отправлен. Ожидание ответа... 200 OK
Длина: 10701 (10K) [text/html]
Сохранение в: «index.html»

index.html          100%[=====] 10,45K  --.-KB/s   за 0s
2020-11-01 20:08:03 (507 MB/s) - «index.html» сохранён [10701/10701]
```

Рис. 5. Загрузка файла с веб-сервера с помощью wget.

Вывод статуса службы веб-сервера (sudo systemctl status apache2) — в отчет.

7) В Oracle VM VirtualBox в настройках созданной в рамках предыдущей лабораторной работы виртуальной машины для Debian GNU/Linux (Debian-FW) добавить второй сетевой адаптер и установить для него тип подключения «Внутренняя сеть». (рис.6.) Имя сети должно совпадать с именем сети в виртуальной машине Debian-Web.

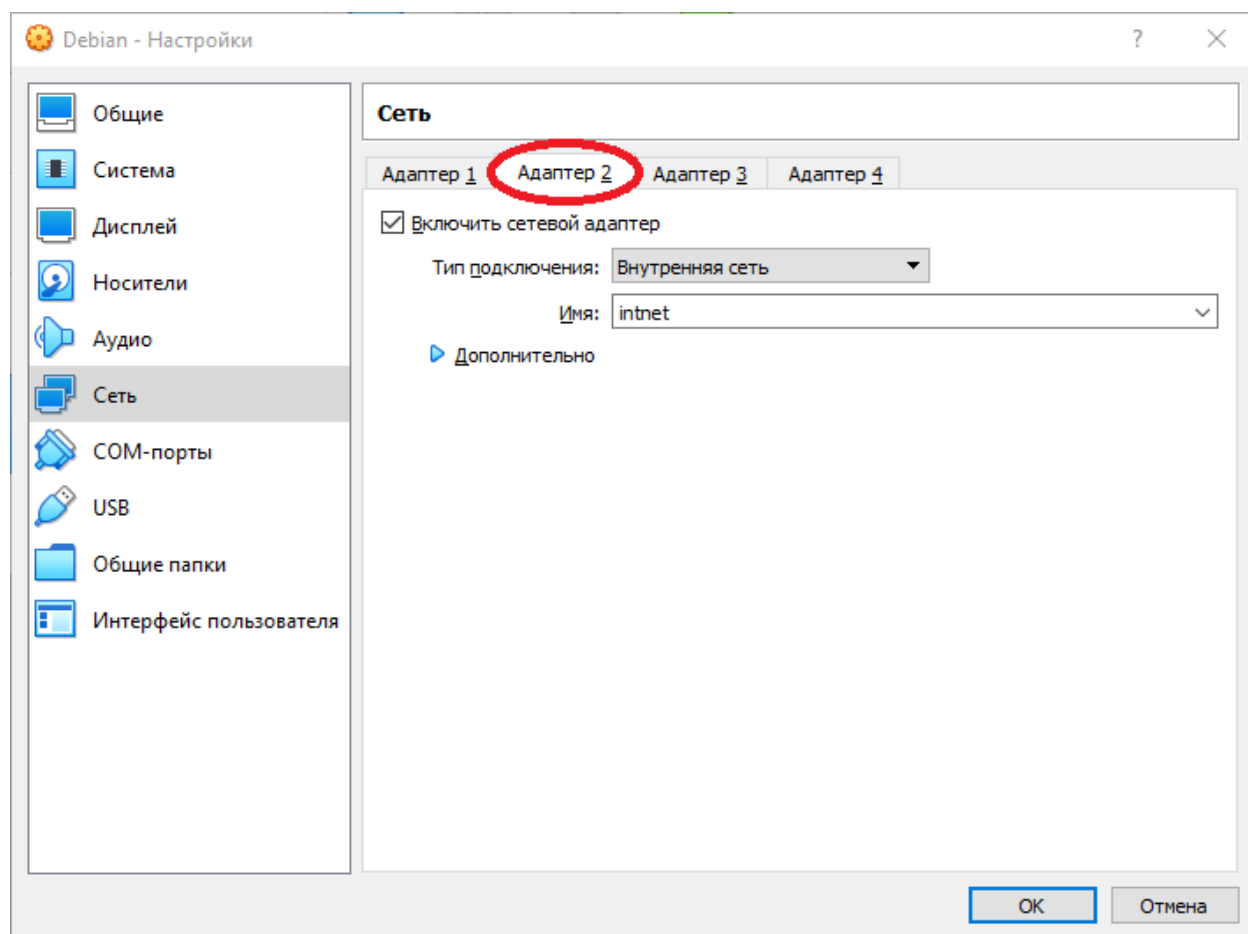


Рис. 6. Подключение второго сетевого адаптера.

8) Запустить VM Debian-FW. Проверить настройки сетевых интерфейсов:

`ip a`

Должен появиться новый сетевой интерфейс (рис.7).

```
user@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
000
    link/ether 08:00:27:bd:17:f5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.5/24 brd 192.168.56.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:febd:17f5/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default ql
link/ether 08:00:27:f2:b0:57 brd ff:ff:ff:ff:ff:ff
```

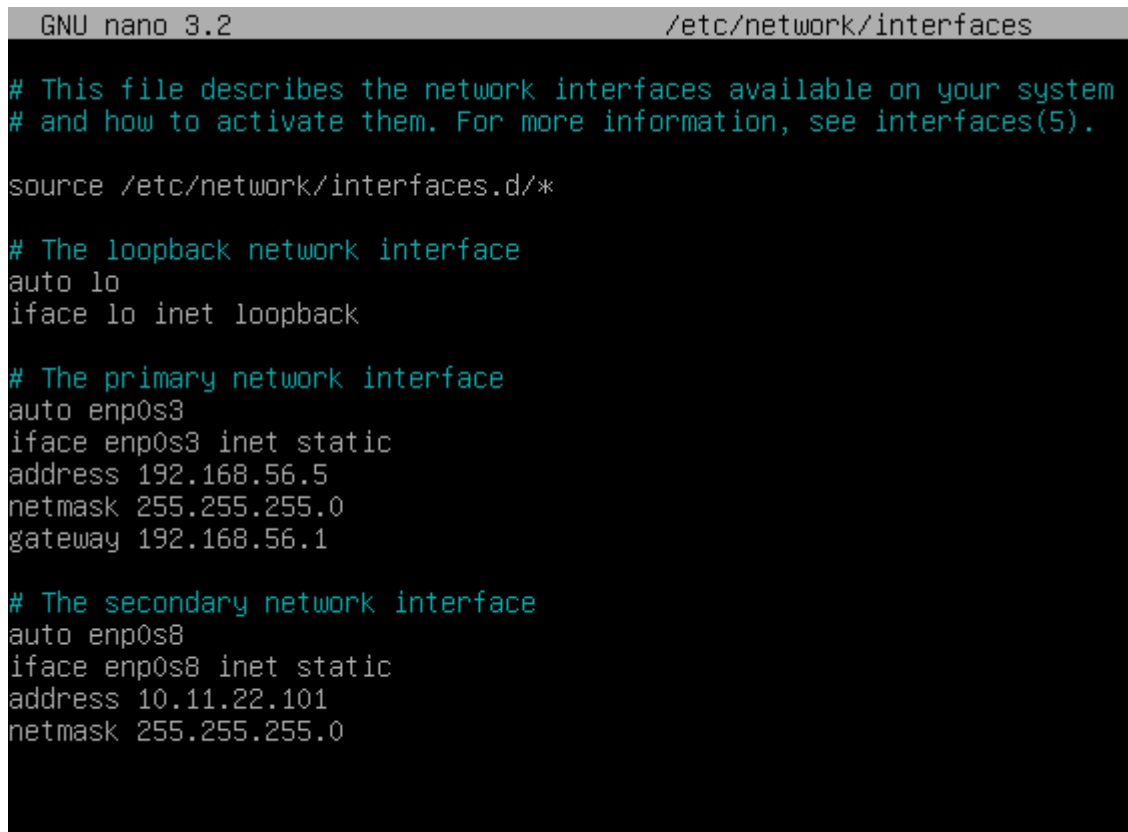
Рис.7. Проверка сетевых параметров.

Настроить на новом интерфейсе статические сетевые параметры, записав данные параметры в файл `/etc/network/interfaces`:

IP-адрес — 10.11.22.101

Маска сети — 255.255.255.0

Пример содержимого файла `/etc/network/interfaces` после внесения необходимых параметров — на рис.8.

A screenshot of a terminal window showing the contents of the file `/etc/network/interfaces` using the GNU nano 3.2 editor. The file contains configuration for three network interfaces: the loopback interface `lo`, a primary static interface `enp0s3` with IP `192.168.56.5` and netmask `255.255.255.0`, and a secondary static interface `enp0s8` with IP `10.11.22.101` and netmask `255.255.255.0`. The primary interface also has a gateway set to `192.168.56.1`.

```
GNU nano 3.2 /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
address 192.168.56.5
netmask 255.255.255.0
gateway 192.168.56.1

# The secondary network interface
auto enp0s8
iface enp0s8 inet static
address 10.11.22.101
netmask 255.255.255.0
```

Рис.8. Содержимое файла `/etc/network/interfaces` на Debian-FW.

9) Изменить сетевое имя узла Debian-FW на «debian-fw», отредактировав файлы `/etc/hostname` и `/etc/hosts`.

Перезапустить ОС.

10) Проверить применение новых сетевых параметров (рис.9).

```

user@debian-fw:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
    link/ether 08:00:27:bd:17:f5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.5/24 brd 192.168.56.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:febd:17f5/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
    link/ether 08:00:27:f2:b0:57 brd ff:ff:ff:ff:ff:ff
    inet 10.11.22.101/24 brd 10.11.22.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fef2:b057/64 scope link
        valid_lft forever preferred_lft forever

```

Рис. 9. Проверка сетевых параметров на Debian-FW

Проверить связь с узлом Debian-web, направив несколько ICMP эхо-запросов с помощью утилиты ping (рис.10.)

```

user@debian-fw:~$ ping 10.11.22.33
PING 10.11.22.33 (10.11.22.33) 56(84) bytes of data.
64 bytes from 10.11.22.33: icmp_seq=1 ttl=64 time=0.157 ms
64 bytes from 10.11.22.33: icmp_seq=2 ttl=64 time=0.222 ms
64 bytes from 10.11.22.33: icmp_seq=3 ttl=64 time=0.158 ms
64 bytes from 10.11.22.33: icmp_seq=4 ttl=64 time=0.149 ms
64 bytes from 10.11.22.33: icmp_seq=5 ttl=64 time=0.206 ms
^C
--- 10.11.22.33 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 100ms
rtt min/avg/max/mdev = 0.149/0.178/0.222/0.031 ms

```

Рис. 10. Проверка связи между узлами.

Вывод статуса сетевых интерфейсов (ip a) — в отчет.

11) На Debian-FW включить пересылку пакетов IPv4 между интерфейсами (маршрутизацию). Для этого необходимо в файле /etc/sysctl.conf раскомментировать строку с параметром «net.ipv4.ip\_forward=1» (убрать символ # в начале строки). Содержимое файла после редактирования — на рис.11.

```
GNU nano 3.2 /etc/sysctl.conf

#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

#####3
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
```

Рис. 11. Включение пересылки пакетов.

Перезапустить ОС. Либо для применения настроек без перезагрузки ввести команду:

```
sudo sysctl net.ipv4.ip_forward=1
```

12) Запустить виртуальную машину с Windows 10. Указать в настройках сетевого интерфейса адрес шлюза по умолчанию. Для сети, к которой принадлежит Windows 10 шлюзом будет IP-адрес сетевого интерфейса узла Debian-FW в сети 192.168.56.0/24 (например, 192.168.56.5).

Шлюз можно задать на DHCP-сервере в параметрах области — параметр «003 Маршрутизатор». Либо указать вручную (рис. 12).



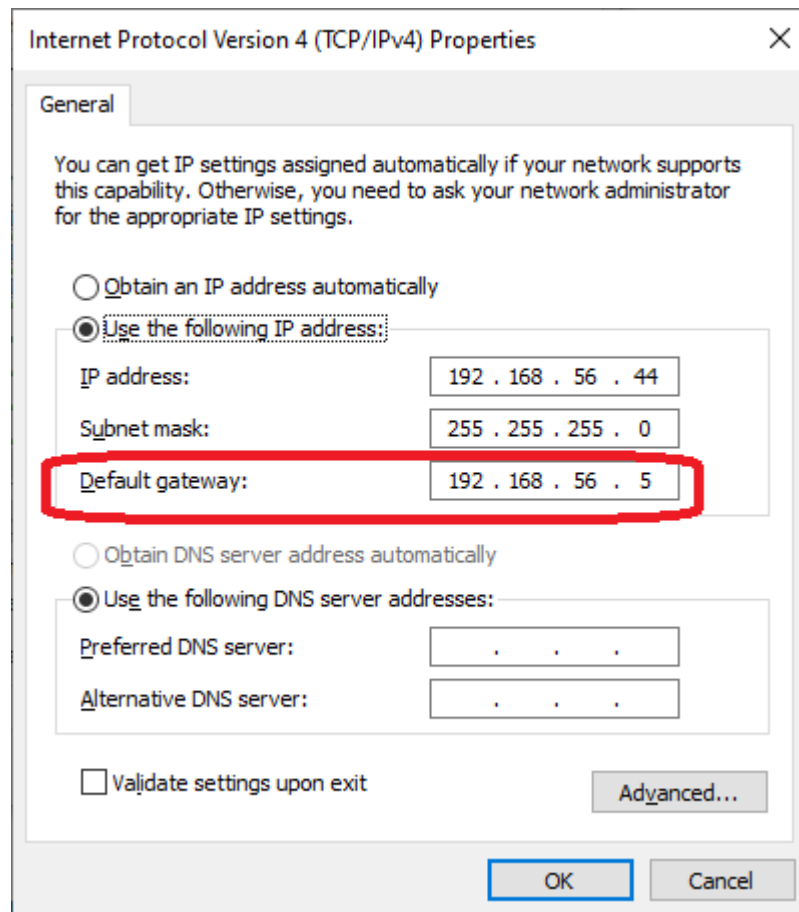


Рис. 12. Ручная настройка сетевого интерфейса.

Запустить трассировку маршрута до узла Debian-Web с помощью команды:  
`tracert -d 10.11.22.33`

Из результата работы команды видно, что маршрут следования пакетов до узла 10.11.22.33 (Debian-Web) проходит через узел 192.168.56.5 (Debian-FW).

```
C:\Users\user1>tracert -d 10.11.22.33

Tracing route to 10.11.22.33 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms    192.168.56.5
  2    <1 ms    <1 ms    <1 ms    10.11.22.33

Trace complete.
```

Рис.13. Трассировка маршрута.

Проверить доступность веб-сервера. Открыть браузер, в адресной строке указать IP-адрес узла Debian-Web. Будет загружена стандартная веб-страница сервера Apache (рис. 14.)

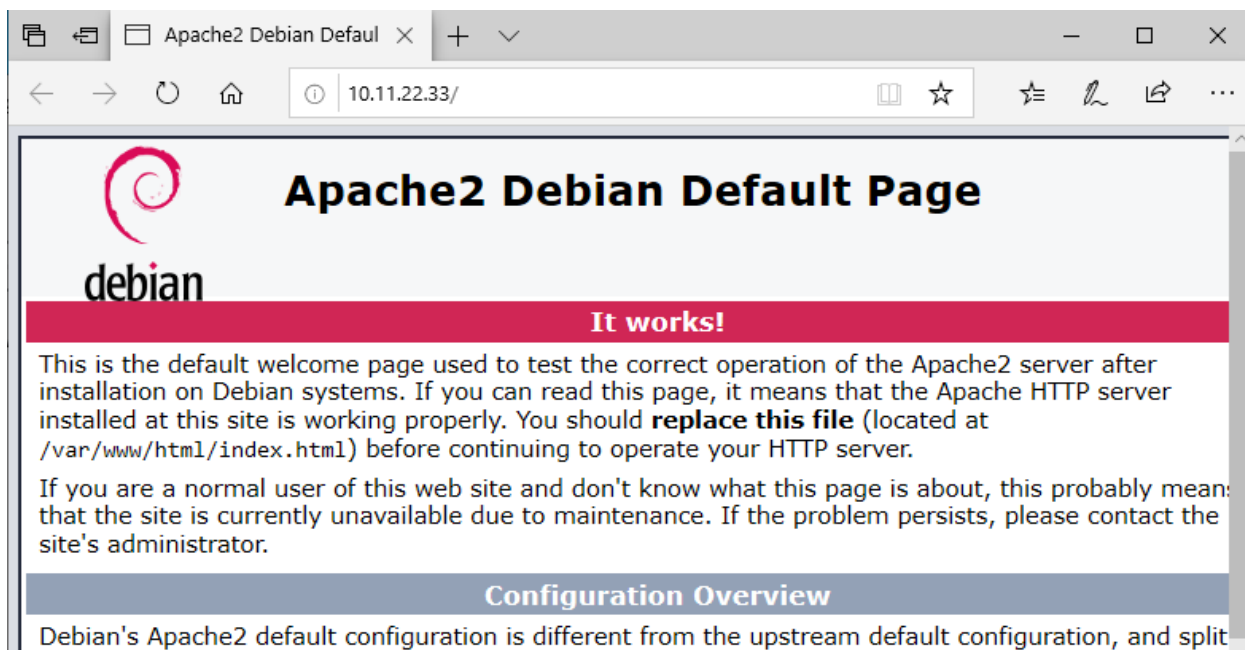


Рис.14. Проверка доступности веб-сервера.

Вывод команды «ipconfig» на Windows 10, трассировка маршрута до Debian-Web, а также снимок окна браузера с открытой страницей веб-сайта Debian-Web – в отчет.

13) На Windows 10 посмотреть список портов, ожидающих входящие соединения («открытые» порты) с помощью команды:

`netstat -an`

К примеру, среди прочих, прослушивается TCP порт 445 (рис. 15).

```
C:\Users\user1>netstat -an

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135              0.0.0.0:0               LISTENING
TCP   0.0.0.0:445              0.0.0.0:0               LISTENING
TCP   0.0.0.0:5040             0.0.0.0:0               LISTENING
TCP   0.0.0.0:49664            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49665            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49666            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49667            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49668            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49669            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49670            0.0.0.0:0               LISTENING
TCP   0.0.0.0:49671            0.0.0.0:0               LISTENING
TCP   192.168.56.44:139        0.0.0.0:0               LISTENING
TCP   [::]:135                [::]:0                  LISTENING
TCP   [::]:445                [::]:0                  LISTENING
TCP   [::]:49664              [::]:0                  LISTENING
TCP   [::]:49665              [::]:0                  LISTENING
```

Рис. 15. Список портов

14) На Debian-Web проверить доступность порта на Windows 10 с помощью утилиты nc (netcat):

```
nc -zvn <IP-адрес> <порт>
```

Например:

```
nc -zvn 192.168.56.44 445
```

Из вывода команды видно, что TCP порт 445 открыт и доступен по сети (рис.16.)

```
user@debian-web:~$ nc -zvn 192.168.56.44 445
(UNKNOWN) [192.168.56.44] 445 (microsoft-ds) open
```

Рис.16. Доступность порта удаленного сетевого узла.

15) Установить на Debian-FW утилиту для настройки встроенного в ядро Linux межсетевого экрана Netfilter — пакет nftables:

```
sudo apt install nftables
```

Включить службу для автоматического запуска и активации правил nftables:

```
sudo systemctl enable nftables
```

Запустить службу:

```
sudo systemctl start nftables
```

Проверить состояние службы:

```
sudo systemctl status nftables
```

Конфигурация правил, которая применяется при запуске службы nftables указана в файле /etc/nftables.conf. По умолчанию создана таблица filter с тремя цепочками (а также хуками) – input, forward и output, правила фильтрации отсутствуют (рис.17).

```
user@debian-fw:~$ cat /etc/nftables.conf
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
    chain input {
        type filter hook input priority 0;
    }
    chain forward {
        type filter hook forward priority 0;
    }
    chain output {
        type filter hook output priority 0;
    }
}
```

Рис.17. Конфигурация nftables по умолчанию.

Стандарные цепочки (хуки):

input — для входящих пакетов адресованных непосредственно локальному узлу, на котором применяется nftables;

forward — для пересылаемых (маршрутизируемых) пакетов;

output — для исходящих пакетов, генерируемых локальным узлом, на котором применяется nftables.

Сохранить данную конфигурацию в файл nftables.conf\_backup:

```
sudo cp /etc/nftables.conf /etc/nftables.conf_backup
```

Статус службы nftables (sudo systemctl status nftables) – в отчет.

16) Настроить правила межсетевого экранирования на Debian-FW.

Перейти в режим суперпользователя:

```
sudo -i
```

Очистить текущий набор правил:

```
nft flush ruleset
```

Добавить новую таблицу «filter»:

```
nft add table inet filter
```

Добавить базовые цепочки input, forward и output. Политика для входящих (input) и пересылаемых (forward) пакетов по умолчанию — drop (отбросить). Политика для исходящих (output) пакетов по умолчанию — accept (разрешить).

```
nft add chain inet filter input '{ type filter hook input priority 0 ; policy drop ; }'
```

```
nft add chain inet filter forward '{ type filter hook forward priority 0 ; policy drop ; }'
```

```
nft add chain inet filter output '{ type filter hook output priority 0 ; policy accept ; }'
```

Добавить правила в цепочки. Разрешить пакеты в состояниях RELATED — новый сеанс, связанный с уже открытым сеансом, и ESTABLISHED — часть уже существующего сеанса:

```
nft add rule inet filter input ct state related,established accept
```

Разрешить трафик на петлевой интерфейс:

```
nft add rule inet filter input iif lo accept
```

Разрешить ICMP пакеты:

```
nft add rule inet filter input icmp type echo-request accept
```

Разрешить доступ из сети 192.168.56.0/24 по SSH:

```
nft add rule inet filter input ip saddr 192.168.56.0/24 tcp dport 22 accept
```

Разрешить маршрутизируемые пакеты с источниками из сети 192.168.56.0/24:

```
nft add rule inet filter forward ip saddr 192.168.56.0/24 accept
```

Разрешить маршрутизируемые пакеты в состояниях RELATED и ESTABLISHED:

```
nft add rule inet filter forward ct state related,established accept
```

Сохранить текущую конфигурацию в файл /etc/nftables.conf. В первой строке указать ссылку на исполняемый файл nft:

```
echo '#!/usr/sbin/nft -f' > /etc/nftables.conf
```

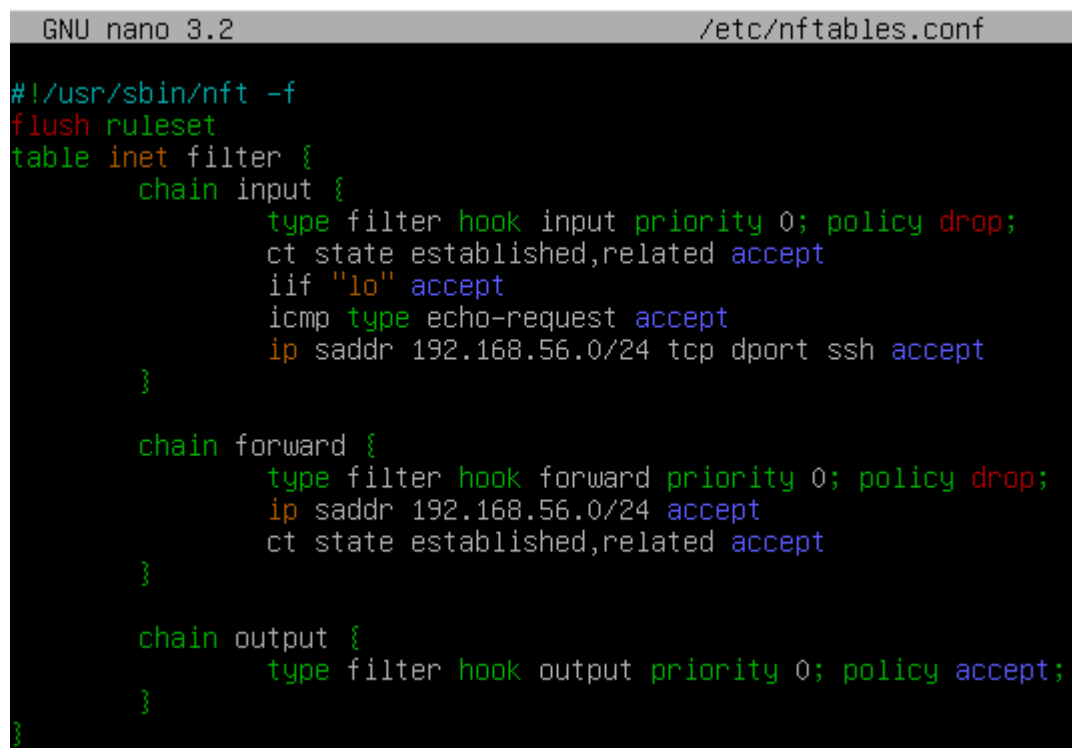
Во второй строке указать команду полной очистки текущей конфигурации nftables:

```
echo 'flush ruleset' >> /etc/nftables.conf
```

Далее в конец файла записать настроенные правила:

```
nft list ruleset >> /etc/nftables.conf
```

Содержимое файла /etc/nftables.conf после изменения конфигурации— на рис. 18.



```
GNU nano 3.2 /etc/nftables.conf

#!/usr/sbin/nft -f
flush ruleset
table inet filter {
    chain input {
        type filter hook input priority 0; policy drop;
        ct state established,related accept
        iif "lo" accept
        icmp type echo-request accept
        ip saddr 192.168.56.0/24 tcp dport ssh accept
    }

    chain forward {
        type filter hook forward priority 0; policy drop;
        ip saddr 192.168.56.0/24 accept
        ct state established,related accept
    }

    chain output {
        type filter hook output priority 0; policy accept;
    }
}
```

Рис. 18. Конфигурация nftables.

17) Повторно провести проверки соединений на Windows 10 и Debian-Web.

Список для проверки на Windows 10:

- успешно проверяется связь утилитой ping с Debian-Web и Debian-FW;
- успешно загружается веб-страница сайта Debian-Web;

- доступно подключение по SSH к Debian-FW и Debian-Web(если настроен сервер SSH).

Список для проверки на Debian-Web:

- успешно проверяется связь утилитой ping с Debian-FW;
- не проверяется связь утилитой ping с Windows 10;
- недоступно подключение к портам, ожидающим входящие соединения («открытым» портам) на Windows 10 (например, TCP порт 445);
- недоступно подключение по SSH к Debian-FW.

Снимки результатов проверок на Debian-Web – в отчет.

18) Установить на Debian-Web утилиту для анализа сетевого трафика — tcpdump:

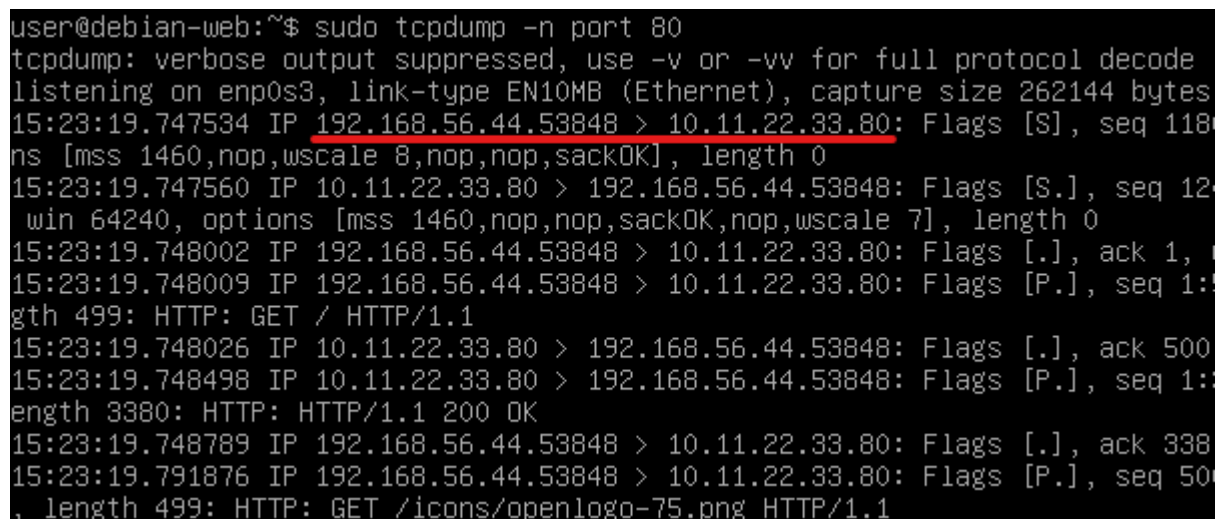
```
sudo apt install tcpdump
```

Начать перехват трафика с фильтрацией по порту 80 и без разрешения IP-адресов в имена:

```
tcpdump -n port 80
```

На Windows 10 открыть страницу веб-сайта на Debian-Web.

На Debian-Web в консоль будет выведена информация о перехваченных пакетах. К примеру, будет указан IP-адрес и порт источника, относящиеся к Windows 10, а также IP-адрес и порт назначения, относящиеся к Debian-Web (Рис. 19).

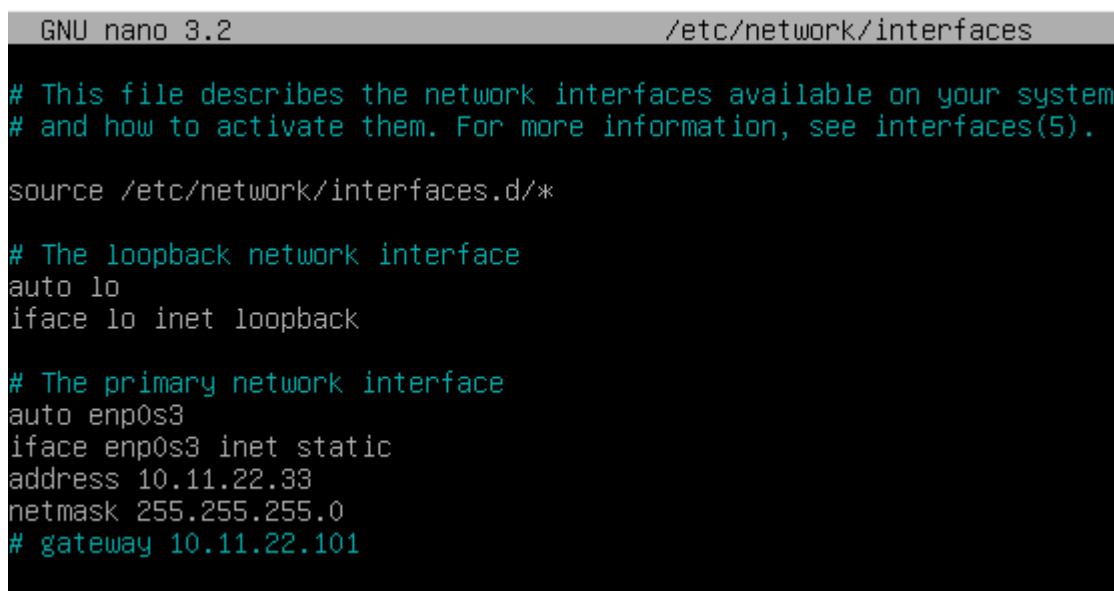


```
user@debian-web:~$ sudo tcpdump -n port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
15:23:19.747534 IP 192.168.56.44.53848 > 10.11.22.33.80: Flags [S], seq 118
ns [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
15:23:19.747560 IP 10.11.22.33.80 > 192.168.56.44.53848: Flags [S.], seq 12
win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
15:23:19.748002 IP 192.168.56.44.53848 > 10.11.22.33.80: Flags [.], ack 1,
15:23:19.748009 IP 192.168.56.44.53848 > 10.11.22.33.80: Flags [P.], seq 1:
gth 499: HTTP: GET / HTTP/1.1
15:23:19.748026 IP 10.11.22.33.80 > 192.168.56.44.53848: Flags [.], ack 500
15:23:19.748498 IP 10.11.22.33.80 > 192.168.56.44.53848: Flags [P.], seq 1:
length 3380: HTTP: HTTP/1.1 200 OK
15:23:19.748789 IP 192.168.56.44.53848 > 10.11.22.33.80: Flags [.], ack 338
15:23:19.791876 IP 192.168.56.44.53848 > 10.11.22.33.80: Flags [P.], seq 50
, length 499: HTTP: GET /icons/openlogo-75.png HTTP/1.1
```

Рис. 19. Пакеты, перехваченные tcpdump.

Завершить перехват пакетов комбинацией клавиш Ctrl+C.

19) Предположим, что узел Debian-Web находится в публичной сети Интернет. В таком случае, на этом узле не будет информации о маршруте в частную сеть 192.168.56.0/24. Для моделирования ситуации необходимо на Debian-Web удалить адрес шлюза из настроек сетевого интерфейса. Для этого следует отредактировать файл /etc/network/interfaces и закомментировать строку с gateway (поставить символ # в начале строки). Содержимое файла после редактирования — на рис. 20.



```
GNU nano 3.2 /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
address 10.11.22.33
netmask 255.255.255.0
# gateway 10.11.22.101
```

Рис. 20. Отключение параметра gateway.

Для применения настроек следует перезапустить службу networking.

После применения настроек Windows 10 потеряет связь с Debian-Web, поскольку Debian-Web не сможет направить ответные пакеты на Windows 10.

Для организации доступа к Debian-Web (условно, в публичной сети) из сети 192.168.56.0/24 (частной сети) необходимо настроить трансляцию сетевых адресов на Debian-FW – Source NAT, средствами nftables.

Для этого создать таблицу nat:

```
nft add table nat
```

Добавить цепочку postrouting:

```
nft 'add chain nat postrouting { type nat hook postrouting priority 100 ; }'
```

Добавить правило для трансляции адресов в пакетах, направленных из сети 192.168.56.0/24 на интерфейс, подключенный к условно публичной сети — enp0s8, с подстановкой IP-адреса 10.11.22.101:

```
nft add rule nat postrouting ip saddr 192.168.56.0/24 oif enp0s8 snat 10.11.22.101
```

Сохранить конфигурацию nftables:

```
echo '#!/usr/sbin/nft -f' > /etc/nftables.conf  
echo 'flush ruleset' >> /etc/nftables.conf  
nft list ruleset >> /etc/nftables.conf
```

Содержимое файла /etc/nftables.conf с правилами NAT – отчет.

21) Повторно начать перехват трафика на Debian-Web с фильтрацией по порту 80 и без разрешения IP-адресов в имена:

```
tcpdump -n port 80
```

На Windows 10 повторно открыть страницу веб-сайта на Debian-Web (в ряде случаев браузер загружает страницу из локального кэша, поэтому необходимо также нажимать кнопку обновления страницы).

На Debian-Web в консоль будет выведена информация о перехваченных пакетах. В данном случае IP-адрес и порт источника относятся к Debian-FW. (рис.21.)

```
user@debian-web:~$ sudo tcpdump -n port 80  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes  
16:17:33.530486 IP 10.11.22.101.53852 > 10.11.22.33.80: Flags [S], seq 39516  
s [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0  
16:17:33.530508 IP 10.11.22.33.80 > 10.11.22.101.53852: Flags [S.], seq 2191  
win 64240, options [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0  
16:17:33.532356 IP 10.11.22.101.53852 > 10.11.22.33.80: Flags [.], ack 1, wi  
16:17:33.532368 IP 10.11.22.101.53852 > 10.11.22.33.80: Flags [P.], seq 1:50  
th 499: HTTP: GET / HTTP/1.1  
16:17:33.532393 IP 10.11.22.33.80 > 10.11.22.101.53852: Flags [.], ack 500,  
16:17:33.532918 IP 10.11.22.33.80 > 10.11.22.101.53852: Flags [P.], seq 1:33  
ngth 3380: HTTP: HTTP/1.1 200 OK  
16:17:33.534028 IP 10.11.22.101.53852 > 10.11.22.33.80: Flags [.], ack 3381,  
16:17:33.559995 IP 10.11.22.101.53852 > 10.11.22.33.80: Flags [P.], seq 500:  
length 499: HTTP: GET /icons/openlogo-75.png HTTP/1.1  
16:17:33.560150 IP 10.11.22.33.80 > 10.11.22.101.53852: Flags [P.] seq 3381
```

Рис. 21. Пакеты, перехваченные tcpdump.

Завершить перехват пакетов комбинацией клавиш Ctrl+C.

Информация о перехваченных утилитой tcpdump пакетах (выделить IP-адрес, подставленный средствами NAT) — в отчет.

**Отчет:**

- статус службы веб-сервера (sudo systemctl status apache2) на Debian-Web;
- статус сетевых интерфейсов (ip a) на Debian-FW;



- вывод команды «ipconfig» на Windows 10, трассировка маршрута до Debian-Web, а также снимок окна браузера с открытой страницей веб-сайта Debian-Web;
- статус службы nftables (`sudo systemctl status nftables`) на Debian-FW;
- снимки результатов проверок на Debian-Web на этапе 17;
- содержимое файла `/etc/nftables.conf` на Debian-FW со всеми настроенными правилами, включая NAT;
- Информация о перехваченных утилитой `tcpdump` пакетах на Debian-Web (выделить IP-адрес, подставленный средствами NAT).