

ДЗ по "Операционные системы и виртуализация (Linux) (семинары)"

Настройка сети в Linux. Работа с IPtables

Оглавление

Задача 1	3
Настроить статическую конфигурацию (без DHCP) в Ubuntu через ip и netplan. Настроить IP, маршрут по умолчанию и DNS-серверы (1.1.1.1 и 8.8.8.8). Проверить работоспособность сети.	3
Задача 2	4
Настроить правила iptables для доступности сервисов на TCP-портах 22, 80 и 443. Также сервер должен иметь возможность устанавливать подключения к серверу обновлений. Остальные подключения запретить.	4
Задача 3	5
Запретить любой входящий трафик с IP 3.4.5.6.....	5
Задача 4	6
*Запросы на порт 8090 перенаправлять на порт 80 (на этом же сервере).....	6
Задача 5	7
*Разрешить подключение по SSH только из сети 192.168.0.0/24.....	7
Вывод	8
Литература.....	9

Задача 1

Настроить статическую конфигурацию (без DHCP) в Ubuntu через ip и netplan. Настроить IP, маршрут по умолчанию и DNS-серверы (1.1.1.1 и 8.8.8.8). Проверить работоспособность сети.

Отредактируем 2-а файла конфигурации сети в nano, 01-network-manager-all.yaml (рисунок 2) и 50-cloud-init.yaml (рисунок 3). При запуске команды ‘sudo netplan try’ будет происходить тестовое применение сетевых настроек, если при этом произошел разрыв связи с сервером, значит мы напортачили с настройками и через некоторое время настройки вернуться в прежнее состояние. Если мы нажали ‘Enter’, то сетевые настройки применяются. При перезагрузке все настройки в файлах конфигурации применяются в автоматическом режиме. Ниже показан рисунок настройки и тестирования сетевых параметров (GeekBrains, 2023), (GeekBrains, 2023), (GeekBrains, 2023).



Рисунок 1 - Скриншот терминала PowerShell, настройка и тестирование сетевой конфигурации

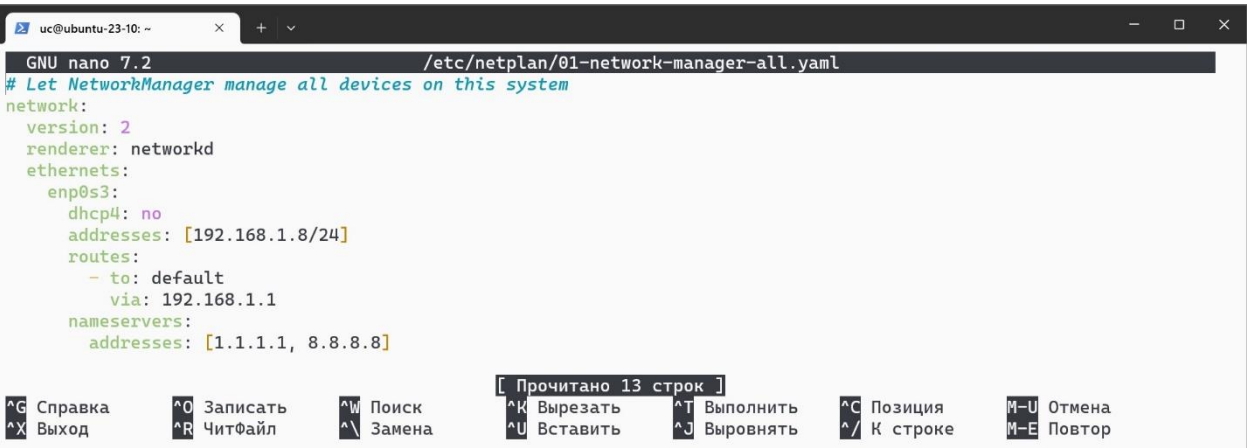


Рисунок 2 - Скриншот терминала PowerShell, редактирование файла 01-network-manager-all.yaml. При выходе из редактора нажать Ctrl + O, Enter, Ctrl + X

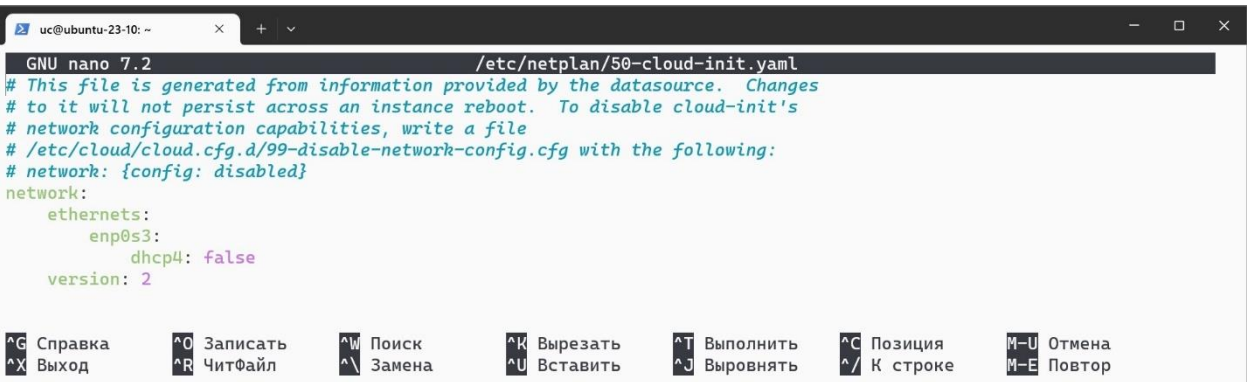
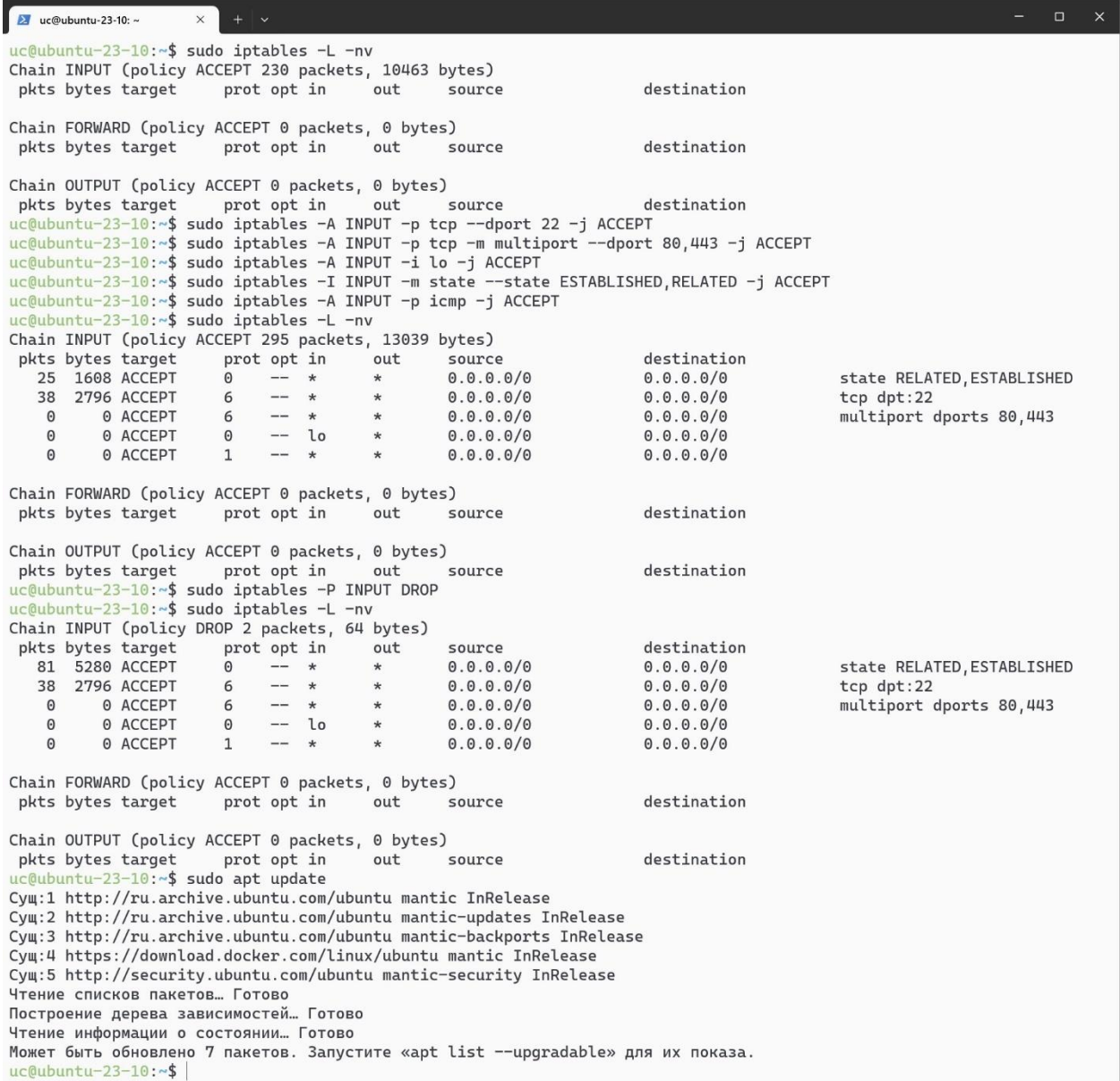


Рисунок 3 - Скриншот терминала PowerShell, редактирование файла 50-cloud-init.yaml. При выходе из редактора нажать Ctrl + O, Enter, Ctrl + X

Задача 2

Настроить правила iptables для доступности сервисов на TCP-портах 22, 80 и 443. Также сервер должен иметь возможность устанавливать подключения к серверу обновлений. Остальные подключения запретить.



```
uc@ubuntu-23-10: ~$ sudo iptables -L -nv
Chain INPUT (policy ACCEPT 230 packets, 10463 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
uc@ubuntu-23-10:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
uc@ubuntu-23-10:~$ sudo iptables -A INPUT -p tcp -m multiport --dport 80,443 -j ACCEPT
uc@ubuntu-23-10:~$ sudo iptables -A INPUT -i lo -j ACCEPT
uc@ubuntu-23-10:~$ sudo iptables -I INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
uc@ubuntu-23-10:~$ sudo iptables -A INPUT -p icmp -j ACCEPT
uc@ubuntu-23-10:~$ sudo iptables -L -nv
Chain INPUT (policy ACCEPT 295 packets, 13039 bytes)
 pkts bytes target    prot opt in     out     source                   destination
   25  1608 ACCEPT     0    --    *      *       0.0.0.0/0               0.0.0.0/0               state RELATED,ESTABLISHED
   38  2796 ACCEPT     6    --    *      *       0.0.0.0/0               0.0.0.0/0               tcp dpt:22
    0    0 ACCEPT     6    --    *      *       0.0.0.0/0               0.0.0.0/0               multiport dports 80,443
    0    0 ACCEPT     0    --    lo     *       0.0.0.0/0               0.0.0.0/0
    0    0 ACCEPT     1    --    *      *       0.0.0.0/0               0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
uc@ubuntu-23-10:~$ sudo iptables -P INPUT DROP
uc@ubuntu-23-10:~$ sudo iptables -L -nv
Chain INPUT (policy DROP 2 packets, 64 bytes)
 pkts bytes target    prot opt in     out     source                   destination
   81  5280 ACCEPT     0    --    *      *       0.0.0.0/0               0.0.0.0/0               state RELATED,ESTABLISHED
   38  2796 ACCEPT     6    --    *      *       0.0.0.0/0               0.0.0.0/0               tcp dpt:22
    0    0 ACCEPT     6    --    *      *       0.0.0.0/0               0.0.0.0/0               multiport dports 80,443
    0    0 ACCEPT     0    --    lo     *       0.0.0.0/0               0.0.0.0/0
    0    0 ACCEPT     1    --    *      *       0.0.0.0/0               0.0.0.0/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination

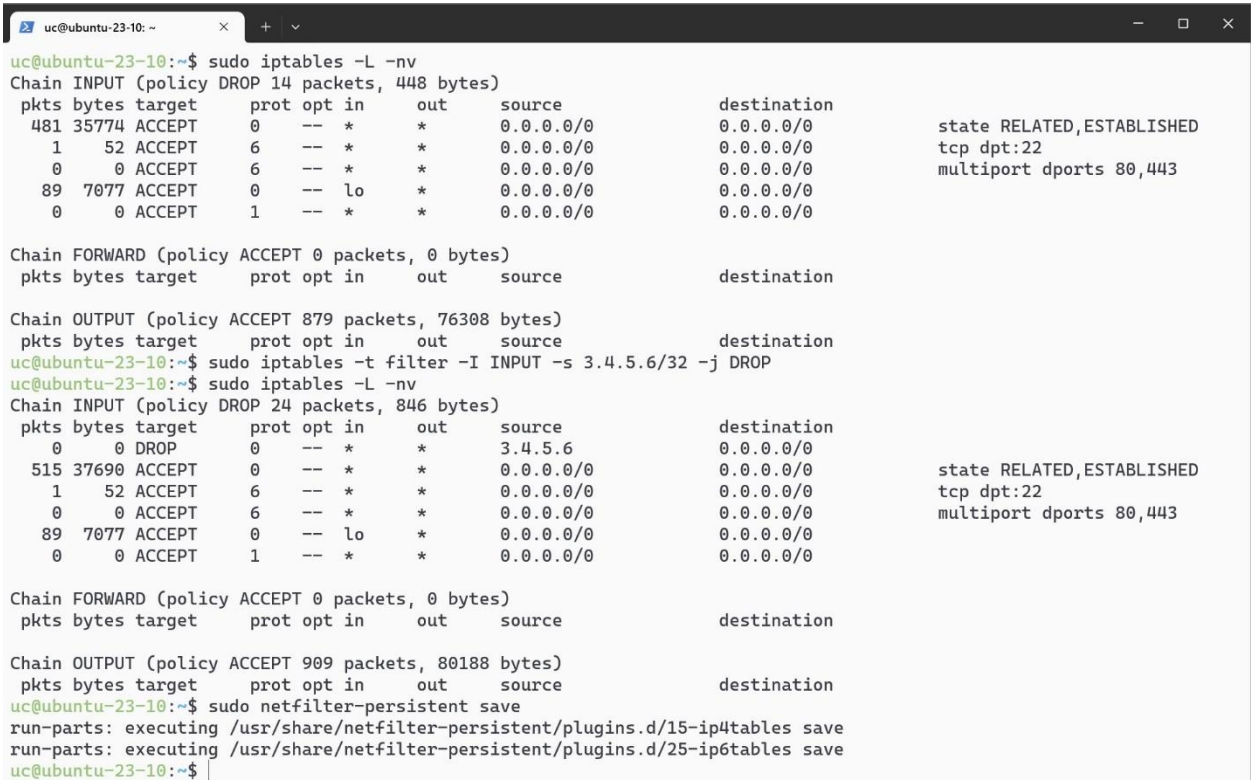
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
uc@ubuntu-23-10:~$ sudo apt update
Сущ:1 http://ru.archive.ubuntu.com/ubuntu mantic InRelease
Сущ:2 http://ru.archive.ubuntu.com/ubuntu mantic-updates InRelease
Сущ:3 http://ru.archive.ubuntu.com/ubuntu mantic-backports InRelease
Сущ:4 https://download.docker.com/linux/ubuntu mantic InRelease
Сущ:5 http://security.ubuntu.com/ubuntu mantic-security InRelease
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Может быть обновлено 7 пакетов. Запустите «apt list --upgradable» для их показа.
uc@ubuntu-23-10:~$
```

Рисунок 4 - Скриншот терминала PowerShell, настройка правил доступности сервисов

Задача 3

Запретить любой входящий трафик с IP 3.4.5.6.

Установим пакет 'iptables-persistent' (ООО "Интерфейс", 2023), чтобы при перезагрузке системы заданные правила автоматически применялись.



```
uc@ubuntu-23-10: ~$ sudo iptables -L -nv
Chain INPUT (policy DROP 14 packets, 448 bytes)
pkts bytes target      prot opt in     out    source            destination
481 35774 ACCEPT      0     -- *     *      0.0.0.0/0          0.0.0.0/0
1    52 ACCEPT      6     -- *     *      0.0.0.0/0          0.0.0.0/0
0    0 ACCEPT      6     -- *     *      0.0.0.0/0          0.0.0.0/0
89  7077 ACCEPT      0     -- lo    *      0.0.0.0/0          0.0.0.0/0
0    0 ACCEPT      1     -- *     *      0.0.0.0/0          0.0.0.0/0
state RELATED,ESTABLISHED
tcp dpt:22
multiport dports 80,443

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out    source            destination

Chain OUTPUT (policy ACCEPT 879 packets, 76308 bytes)
pkts bytes target      prot opt in     out    source            destination
uc@ubuntu-23-10:~$ sudo iptables -t filter -I INPUT -s 3.4.5.6/32 -j DROP
uc@ubuntu-23-10:~$ sudo iptables -L -nv
Chain INPUT (policy DROP 24 packets, 846 bytes)
pkts bytes target      prot opt in     out    source            destination
0    0 DROP        0     -- *     *      3.4.5.6            0.0.0.0/0
515 37690 ACCEPT      0     -- *     *      0.0.0.0/0          0.0.0.0/0
1    52 ACCEPT      6     -- *     *      0.0.0.0/0          0.0.0.0/0
0    0 ACCEPT      6     -- *     *      0.0.0.0/0          0.0.0.0/0
89  7077 ACCEPT      0     -- lo    *      0.0.0.0/0          0.0.0.0/0
0    0 ACCEPT      1     -- *     *      0.0.0.0/0          0.0.0.0/0
state RELATED,ESTABLISHED
tcp dpt:22
multiport dports 80,443

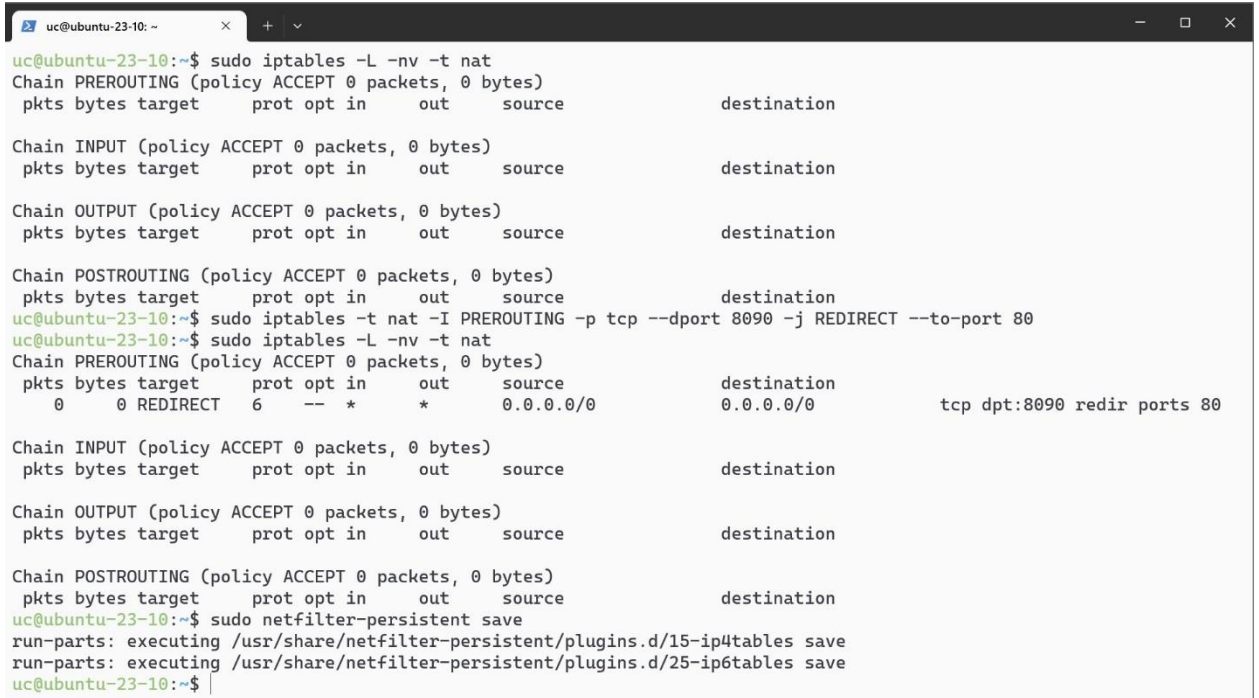
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out    source            destination

Chain OUTPUT (policy ACCEPT 909 packets, 80188 bytes)
pkts bytes target      prot opt in     out    source            destination
uc@ubuntu-23-10:~$ sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
uc@ubuntu-23-10:~$
```

Рисунок 5 - Скриншот терминала PowerShell, запрет входящего трафика с IP адреса

Задача 4

*Запросы на порт 8090 перенаправлять на порт 80 (на этом же сервере).



```
uc@ubuntu-23-10: ~  
uc@ubuntu-23-10:~$ sudo iptables -L -nv -t nat  
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target      prot opt in     out     source        destination  
  
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target      prot opt in     out     source        destination  
  
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target      prot opt in     out     source        destination  
  
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target      prot opt in     out     source        destination  
uc@ubuntu-23-10:~$ sudo iptables -t nat -I PREROUTING -p tcp --dport 8090 -j REDIRECT --to-port 80  
uc@ubuntu-23-10:~$ sudo iptables -L -nv -t nat  
Chain PREROUTING (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target      prot opt in     out     source        destination  
    0    0 REDIRECT    6    --    *      *      0.0.0.0/0     0.0.0.0/0          tcp dpt:8090 redir ports 80  
  
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target      prot opt in     out     source        destination  
  
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target      prot opt in     out     source        destination  
  
Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target      prot opt in     out     source        destination  
uc@ubuntu-23-10:~$ sudo netfilter-persistent save  
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save  
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save  
uc@ubuntu-23-10:~$
```

Рисунок 6 - Скриншот терминала PowerShell, перенаправление портов на сервере

Задача 5

*Разрешить подключение по SSH только из сети 192.168.0.0/24.

```
uc@ubuntu-23-10: ~  
uc@ubuntu-23-10:~$ sudo ss -ntlp  
[sudo] пароль для uc:  
State Recv-Q Send-Q Local Address:Port Peer Address:Port Process  
LISTEN 0 4096 127.0.0.54:53 0.0.0.0:* users:(("systemd-resolve",pid=405,fd=16))  
LISTEN 0 4096 127.0.0.1:631 0.0.0.0:* users:(("cupsd",pid=873,fd=7))  
LISTEN 0 4096 127.0.0.53%lo:53 0.0.0.0:* users:(("systemd-resolve",pid=405,fd=14))  
LISTEN 0 4096 [::1]:631 [::]:* users:(("cupsd",pid=873,fd=6))  
LISTEN 0 4096 *:22 *:~ users:(("sshd",pid=1591,fd=3),("systemd",pid=1,fd=70))  
uc@ubuntu-23-10:~$ sudo iptables -L -nv  
Chain INPUT (policy DROP 64 packets, 9527 bytes)  
pkts bytes target prot opt in out source destination  
0 0 DROP 0 -- * * 3.4.5.6 0.0.0.0/0  
255 21016 ACCEPT 0 -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED  
1 52 ACCEPT 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22  
0 0 ACCEPT 6 -- * * 0.0.0.0/0 0.0.0.0/0 multiport dports 80,443  
52 4842 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0  
0 0 ACCEPT 1 -- * * 0.0.0.0/0 0.0.0.0/0  
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination  
Chain OUTPUT (policy ACCEPT 337 packets, 32695 bytes)  
pkts bytes target prot opt in out source destination  
uc@ubuntu-23-10:~$ sudo iptables -D INPUT 1  
uc@ubuntu-23-10:~$ sudo iptables -D INPUT 1  
uc@ubuntu-23-10:~$ sudo iptables -L -nv  
Chain INPUT (policy DROP 79 packets, 10048 bytes)  
pkts bytes target prot opt in out source destination  
8 456 ACCEPT 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22  
0 0 ACCEPT 6 -- * * 0.0.0.0/0 0.0.0.0/0 multiport dports 80,443  
53 4915 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0  
0 0 ACCEPT 1 -- * * 0.0.0.0/0 0.0.0.0/0  
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination  
Chain OUTPUT (policy ACCEPT 370 packets, 36837 bytes)  
pkts bytes target prot opt in out source destination  
uc@ubuntu-23-10:~$ sudo iptables -I INPUT -s 192.168.1.0/24 -p tcp --dport 22 -j ACCEPT  
uc@ubuntu-23-10:~$ sudo iptables -I INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT  
uc@ubuntu-23-10:~$ sudo iptables -t filter -I INPUT -s 3.4.5.6/32 -j DROP  
uc@ubuntu-23-10:~$ sudo iptables -D INPUT -p tcp --dport 22 -j ACCEPT  
uc@ubuntu-23-10:~$ sudo iptables -L -nv  
Chain INPUT (policy DROP 306 packets, 22528 bytes)  
pkts bytes target prot opt in out source destination  
0 0 DROP 0 -- * * 3.4.5.6 0.0.0.0/0  
54 3837 ACCEPT 0 -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED  
14 1044 ACCEPT 6 -- * * 192.168.1.0/24 0.0.0.0/0 tcp dpt:22  
0 0 ACCEPT 6 -- * * 0.0.0.0/0 0.0.0.0/0 multiport dports 80,443  
67 6131 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0  
0 0 ACCEPT 1 -- * * 0.0.0.0/0 0.0.0.0/0  
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination  
Chain OUTPUT (policy ACCEPT 513 packets, 50289 bytes)  
pkts bytes target prot opt in out source destination  
uc@ubuntu-23-10:~$ sudo ss -ntlp  
State Recv-Q Send-Q Local Address:Port Peer Address:Port Process  
LISTEN 0 4096 127.0.0.54:53 0.0.0.0:* users:(("systemd-resolve",pid=405,fd=16))  
LISTEN 0 4096 127.0.0.1:631 0.0.0.0:* users:(("cupsd",pid=873,fd=7))  
LISTEN 0 4096 127.0.0.53%lo:53 0.0.0.0:* users:(("systemd-resolve",pid=405,fd=14))  
LISTEN 0 4096 [::1]:631 [::]:* users:(("cupsd",pid=873,fd=6))  
LISTEN 0 4096 *:22 *:~ users:(("sshd",pid=1591,fd=3),("systemd",pid=1,fd=70))  
uc@ubuntu-23-10:~$ sudo netfilter-persistent save  
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save  
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save  
uc@ubuntu-23-10:~$
```

Рисунок 7 - Скриншот терминала PowerShell, настройка правил для ssh

Вывод

Изучил азы конфигурирования сетевых настроек и правил сервера Ubuntu. Познакомился с пакетом 'iptables-persistent' и др.

Литература

- GeekBrains. (17 12 2023 г.). *Лекция (Видео)*. Получено из GeekBrains:
<https://gbcndn.mrgcdn.ru/uploads/record/246039/attachment/0bbae3dc0266d4ab0a39dc0504954409.mp4>
- GeekBrains. (17 12 2023 г.). *Лекция 5. Сетевые возможности Linux*. Получено из GeekBrains:
<https://gbcndn.mrgcdn.ru/uploads/asset/4327097/attachment/0c7e44f4cc0f4f2073d6dd20338f46a2.pdf>
- GeekBrains. (17 12 2023 г.). *Сетевые возможности Linux (Презентация)*. Получено из GeekBrains:
<https://gbcndn.mrgcdn.ru/uploads/asset/4327093/attachment/2264165087c249d1b7b58353d6e84f5e.pdf>
- ООО "Интерфейс". (17 12 2023 г.). *Основы iptables для начинающих. Как сохранить правила и восстановить их при загрузке*. Получено из Записки IT специалиста:
https://interface31.ru/tech_it/2021/12/osnovy-iptables-dlya-nachinayushhih-kak-sohranit-pravila-i-vozstanovit-ih-pri-zagruzke.html