# 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 ір 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 ІР 3.4.5.6	5
Задача 4	6
*Запросы на порт 8090 перенаправлять на порт 80 (на этом же сервере)	
Задача 5	7
*Разрешить подключение по SSH только из сети 192.168.0.0/24	7
Вывод	8
Литература	9

Настроить статическую конфигурацию (без DHCP) в Ubuntu через ір 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 накосячили 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).

```
uc@ubuntu-23-10: ~
uc@ubuntu-23-10:~$ sudo nano /etc/netplan/01-network-manager-all.yaml
uc@ubuntu-23-10:~$ sudo nano /etc/netplan/50-cloud-init.yaml
uc@ubuntu-23-10:~$ systemctl start systemd-resolved.service ==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units
Чтобы запустить «systemd-resolved.service», необходимо пройти аутентификацию.
Authenticating as: Evgeny (uc)
Password:
   === AUTHENTICATION COMPLETE ===
uc@ubuntu-23-10:~$ systemctl enable systemd-resolved.service
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-unit-files ====
 Authentication is required to manage system service or unit files.
 Authenticating as: Evgeny (uc)
Password:
  === AUTHENTICATION COMPLETE ==
==== AUTHENTICATING FOR org.freedesktop.systemd1.reload-daemon ==== Authentication is required to reload the systemd state.
 Authenticating as: Evgeny (uc)
 ==== AUTHENTICATION COMPLETE =
uc@ubuntu-23-10:~$ sudo netplan try
 ** (process:2166): WARNING **: 12:20:58.035: Permissions for /etc/netplan/01-network-manager-all.yaml are too open.
Netplan configuration should NOT be accessible by others.
** (generate:2167): WARNING **: 12:20:58.041: Permissions for /etc/netplan/01-network-manager-all.yaml are too open.
Netplan configuration should NOT be accessible by others.
Cannot call Open vSwitch: ovsdb-server.service is not running.
 ** (process:2166): WARNING **: 12:20:58.421: Permissions for /etc/netplan/01-network-manager-all.yaml are too open.
Netplan configuration should NOT be accessible by others.
 ** (process:2166): WARNING **: 12:20:58.482: Permissions for /etc/netplan/01-network-manager-all.yaml are too open.
Netplan configuration should NOT be accessible by others
** (process:2166): WARNING **: 12:20:58.482: Permissions for /etc/netplan/01-network-manager-all.yaml are too open. Netplan configuration should NOT be accessible by others.
Do you want to keep these settings?
Press ENTER before the timeout to accept the new configuration
Changes will revert in 70 seconds
Configuration accepted.
 uc@ubuntu-23-10:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000 link/loopback 00:00:00:00:00:00:00 brd 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 group default qlen 1000 link/ether 08:00:27:35:b2:5b brd ff:ff:ff:ff:ff
      inet 192.168.1.8/24 brd 192.168.1.255 scope global enp0s3
      valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fe35:b25b/64 scope link
          valid_lft forever preferred_lft forever
uc@ubuntu-23-10:~$ ip r
default via 192.168.1.1 dev enp0s3 proto static
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.8
 uc@ubuntu-23-10:~$ resolvectl dns
Global:
Link 2 (enp0s3): 1.1.1.1 8.8.8.8
Link 2 (enp0s3): 1.1.1.1 8.8.8.8 uc@ubuntu-23-10:~$ ping ya.ru

PING ya.ru (5.255.255.242) 56(84) bytes of data.

64 bytes from ya.ru (5.255.255.242): icmp_seq=1 ttl=53 time=22.4 ms

64 bytes from ya.ru (5.255.255.242): icmp_seq=2 ttl=53 time=23.0 ms

64 bytes from ya.ru (5.255.255.242): icmp_seq=3 ttl=53 time=23.0 ms

64 bytes from ya.ru (5.255.255.242): icmp_seq=4 ttl=53 time=22.8 ms

64 bytes from ya.ru (5.255.255.242): icmp_seq=5 ttl=53 time=22.5 ms

64 bytes from ya.ru (5.255.255.242): icmp_seq=5 ttl=53 time=22.5 ms
64 bytes from ya.ru (5.255.255.242): icmp_seq=6 ttl=53 time=22.5 ms
     ya.ru ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5015ms rtt min/avg/max/mdev = 22.372/22.688/23.007/0.244 ms uc@ubuntu-23-10:~$
```

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

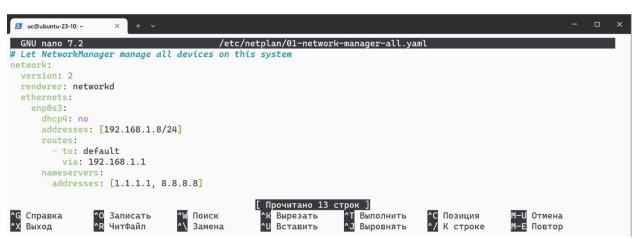


Рисунок 2 - Скриншот терминала PowerShell, редактирование файла 01-network-managerall.yaml. При выходе из редактора нажать Ctrl + O, Enter, Ctrl + X



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

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.

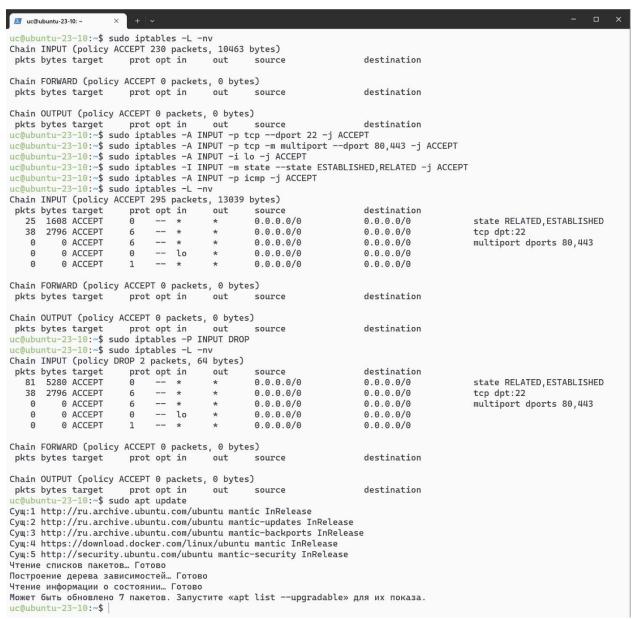


Рисунок 4 - Скриншот терминала PowerShell, настройка правил доступности сервисов

Запретить любой входящий трафик с ІР 3.4.5.6.

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

```
∠ uc@ubuntu-23-10: ~

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
                                                                                             state RELATED, ESTABLISHED
         52 ACCEPT
                                                 0.0.0.0/0
                                                                                             tcp dpt:22
    0
          0 ACCEPT
                                                 0.0.0.0/0
                                                                       0.0.0.0/0
                                                                                             multiport dports 80,443
                            -- lo
   89
      7077 ACCEPT
                        0
                                                 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)
                        prot opt in
                                                                       destination
 pkts bytes target
                                        out
                                                 source
Chain OUTPUT (policy ACCEPT 879 packets, 76308 bytes)
pkts bytes target prot opt in out source destiuc@ubuntu-23-10:~$ sudo iptables -t filter -I INPUT -s 3.4.5.6/32 -j DROPuc@ubuntu-23-10:~$ sudo iptables -L -nv
Chain INPUT (policy DROP 24 packets, 846 bytes)
                                      out
                                                                       destination
 pkts bytes target
                       prot opt in
                                                source
          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
                                                                                             state RELATED, ESTABLISHED
   1 52 ACCEPT
                                                                      0.0.0.0/0
                                                                                             tcp dpt:22
    0
          0 ACCEPT
                                                 0.0.0.0/0
                                                                      0.0.0.0/0
                                                                                            multiport dports 80,443
                            -- lo
   89 7077 ACCEPT
                        0
                                                 0.0.0.0/0
                                                                      0.0.0.0/0
                       1 -- *
    0
          0 ACCEPT
                                                 0.0.0.0/0
                                                                      0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
                       prot opt in
                                                                       destination
                                                 source
 pkts bytes target
                                        out
Chain OUTPUT (policy ACCEPT 909 packets, 80188 bytes)
 pkts bytes target
                       prot opt in
                                        out
                                                                       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

\*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
                                                                           destination
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
                        prot opt in
 pkts bytes target
                                         out
                                                                           destination
                                                    source
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target
                        prot opt in out
                                                                           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)
          es target prot opt in out

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

Рисунок 6 - Скриншот терминала PowerShell, перенаправление портов на сервере

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

```
uc@ubuntu-23-10: ~
  c@ubuntu-23-10:~$ sudo ss -ntlp
 [sudo] пароль для uc:
             Recv-Q Send-Q
                                         Local Address:Port
                                                                         Peer Address:Port
 State
                                                                                                    users:(("systemd-resolve",pid=405,fd=16))
users:(("cupsd",pid=873,fd=7))
users:(("systemd-resolve",pid=405,fd=14))
users:(("cupsd",pid=873,fd=6))
users:(("sshd",pid=1591,fd=3),("systemd",pid=1,fd=70
                                             127.0.0.54:53
127.0.0.1:631
 LISTEN
             0
                         4096
                                                                                0.0.0.0:*
 LISTEN
                         4096
                                                                                0.0.0.0:*
                                         127.0.0.53%lo:53
                          4096
ITSTEN
             0
                         4096
                                                    [::1]:631
                                                                                    [::]:*
             0
                         4096
LISTEN
 ))
uc@ubuntu-23-10:~$ sudo iptables -L -nv
Chain INPUT (policy DROP 64 packets, 9527 bytes)
 pkts bytes target
0 0 DROP
                                                      out
                                                                  source
                                prot opt in
                                                                                               destination
                                                                  3.4.5.6
                                                                                               0.0.0.0/0
   255 21016 ACCEPT
                                0
                                                                  0.0.0.0/0
                                                                                                                             state RELATED, ESTABLISHED
                                                                                                                            tcp dpt:22
multiport dports 80,443
     1
             52 ACCEPT
                                6
                                                                  0.0.0.0/0
                                                                                               0.0.0.0/0
              0 ACCEPT
                                6
                                                                  0.0.0.0/0
                                                                                               0.0.0.0/0
     52
         4842 ACCEPT
                                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
uc@ubuntu-23-10:~$ sudo iptables -D INPUT 1
uc@ubuntu-23-10:~$ sudo iptables -D INPUT 1
                                                                 source
                                                                                               destination
 uc@ubuntu-23-10:~$ sudo iptables -L -nv
Chain INPUT (policy DROP 79 packets, 10048 bytes)
 pkts bytes target
                                prot opt in
                                                                                               destination
                                                      out
                                                                 source
           456 ACCÉPT
                                                                  0.0.0.0/0
                                                                                                                             tcp dpt:22
      0
              O 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 ACCEPT
                                                                                               0.0.0.0/0
      0
                                                                  0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target
                               prot opt in
                                                      out
                                                                                               destination
                                                                  source
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
 pkts bytes target
                                prot opt in
                                                       out
      0
              0 DROP
                                                                  3.4.5.6
                                                                                               0.0.0.0/0
0.0.0.0/0
         3837 ACCEPT
                                                                  0.0.0.0/0
                                0
                                                                                                                            state RELATED, ESTABLISHED
                                                                                                                             tcp dpt:22
    14
         1044 ACCEPT
                                6
                                                                  192.168.1.0/24
                                                                                               0.0.0.0/0
                                                                                                                            multiport dports 80,443
     0
              0 ACCEPT
                                6
                                                                  0.0.0.0/0
                                                                                               0.0.0.0/0
          6131 ACCEPT
                                       -- lo
      0
              0 ACCEPT
                                                                  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)
   okts bytes target prot opt in
c@ubuntu-23-10:~$ sudo ss -ntlp
                                                                                               destination
 pkts bytes target
                                                      out
                                                                 source
                                        Local Address:Port
 State
             Recv-Q
                         Send-Q
                                                                         Peer Address:Port Process
                                          127.0.0.54:53
                         4096
LISTEN
                                                                                                    users:(("systemd-resolve",pid=405,fd=16))
             0
                                                                                0.0.0.0:*
                                                                                                    users:(("cupsd",pid=873,fd=7))
users:(("systemd-resolve",pid=405,fd=14))
users:(("cupsd",pid=873,fd=6))
                         4096
                                              127.0.0.1:631
                                                                                0.0.0.0:*
                                        127.0.0.53%lo:53
[::1]:631
LISTEN
             0
                         4096
                                                                                0.0.0.0:*
LISTEN
                         4096
                                                                                    [::]:*
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
```

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://gbcdn.mrgcdn.ru/uploads/record/246039/attachment/0bbae3dc0266d4ab0a39 dc0504954409.mp4
- GeekBrains. (17 12 2023 г.). Лекция 5. Сетевые возможности Linux. Получено из GeekBrains: https://gbcdn.mrgcdn.ru/uploads/asset/4327097/attachment/0c7e44f4cc0f4f2073d6dd 20338f46a2.pdf
- GeekBrains. (17 12 2023 г.). Сетевые возможности Linux (Презентация). Получено из GeekBrains: https://gbcdn.mrgcdn.ru/uploads/asset/4327093/attachment/2264165087c249d1b7b5 8353d6e84f5e.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-vosstanovit-ih-pri-zagruzke.html