

Урок 5. Настройка сети в Linux. Работа с IPtables

Задание

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

```
fred1@fred1: $ pwd
/home/fred1
fred1@fred1: $ cd /etc/netplan
fred1@fred1:/etc/netplan$ 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 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 fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4a:82:36 brd ff:ff:ff:ff:ff:ff
    inet 172.30.226.154/20 brd 172.30.239.255 scope global dynamic noprefixroute enp0s3
        valid_lft 82299sec preferred_lft 82299sec
    inet6 fe80::ed08:5795:653a:eda2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
fred1@fred1:/etc/netplan$ ip route
default via 172.30.224.1 dev enp0s3 proto dhcp metric 100
169.254.0.0/16 dev enp0s3 scope link metric 1000
172.30.224.0/20 dev enp0s3 proto kernel scope link src 172.30.226.154 metric 100
fred1@fred1:/etc/netplan$ ip route | grep default
default via 172.30.224.1 dev enp0s3 proto dhcp metric 100
fred1@fred1:/etc/netplan$ sudo nano 1-network-manager-all.yaml
fred1@fred1:/etc/netplan$
fred1@fred1:/etc/netplan$ sudo netplan apply
/etc/netplan/1-network-manager-all.yaml:5:5: Error in network definition: expected scalar
  enp0s3:
  ^
fred1@fred1:/etc/netplan$ sudo nano 1-network-manager-all.yaml
fred1@fred1:/etc/netplan$ sudo nano 1-network-manager-all.yaml
fred1@fred1:/etc/netplan$ fred1@fred1:/etc/netplan$ sudo netplan apply
/etc/netplan/1-network-manager-all.yaml:5:14: Invalid YAML: inconsistent indentation:
  ethernet:
  ^
fred1@fred1:/etc/netplan$ sudo nano 1-network-manager-all.yaml
fred1@fred1:/etc/netplan$ sudo netplan apply
/etc/netplan/1-network-manager-all.yaml:5:14: Invalid YAML: inconsistent indentation:
  ethernet:
  ^
fred1@fred1:/etc/netplan$ sudo nano 1-network-manager-all.yaml
fred1@fred1:/etc/netplan$ sudo netplan apply
/etc/netplan/1-network-manager-all.yaml:8:7: Error in network definition: unknown key 'gateway'
  gateway: 172.30.224.1
  ^
fred1@fred1:/etc/netplan$ sudo nano 1-network-manager-all.yaml
fred1@fred1:/etc/netplan$ sudo netplan apply
```

1. старый вариант

```
GNU nano 6.2 1-network-manager-all.yaml
# This network manager manages all devices on this system
network:
  version: 2
  renderer: networkd
  ethernet:
    enp0s3:
      addresses: [172.30.226.154/20]
      gateway4: 172.30.224.1
      nameservers:
        addresses: [1.1.1.1, 8.8.8.8]
```

Прочитано 10 строк

Справка Записать Поиск Вырезать Выполнить Позиция Отмена Установить На скобку
Выход ЧитФайл Замена Вставить Выводить К строке Повтор Копировать Обр. поиск

2. новый вариант

network:

version: 2

renderer: networkd

ethernets:

enp0s3: # имя интерфейса

addresses: [172.30.226.154/20] # статический IP и маску подсети

routes:

- to: default #0.0.0.0/0

via: 172.30.224.1 # IP шлюза (маршрута по умолчанию)

nameservers:

addresses: [1.1.1.1, 8.8.8.8] # DNS-серверы

```
GNU nano 6.2 1-network-manager-all
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3: # имя интерфейса
      addresses: [172.30.226.154/20] # статический IP и маску подсети
      routes:
        - to: default
          via: 172.30.224.1 # IP шлюза (маршрута по умолчанию)
      nameservers:
        addresses: [1.1.1.1, 8.8.8.8] # DNS-серверы
```

```
PS C:\Users\Fred1> ssh fred1@172.30.226.154
fred1@172.30.226.154's password:
Last login: Thu Sep 21 16:33:17 2023 from 172.30.224.1
fred1@fred1:~$ cd /etc/netpal
-bash: cd: /etc/netpal: Нет такого файла или каталога
fred1@fred1:~$ cd /etc/netplan
fred1@fred1:~$ cd /etc/netplan
fred1@fred1:~$ ls
1-network-manager-all.yaml
fred1@fred1:~$ cd /etc/netplan
fred1@fred1:~$ sudo nano 1-network-manager-all.yaml
[sudo] пароль для fred1:
fred1@fred1:~$ cd /etc/netplan
fred1@fred1:~$ netplan try
ERROR: cannot create file /run/systemd/system/netplan-ovs-cleanup.service: Failed to create file "/run/systemd/system/netplan-ovs-cleanup.se
rvce.JBWIB2": Permission denied

An error occurred: the configuration could not be generated

Reverting.
Something really bad happened while reverting config: [Errno 13] Permission denied: '10-netplan-enp0s3.network'
You should verify the netplan YAML in /etc/netplan and probably run 'netplan apply' again.
fred1@fred1:~$ cd /etc/netplan
fred1@fred1:~$ sudo !!
sudo netplan try
Do you want to keep these settings?

Press ENTER before the timeout to accept the new configuration

Changes will revert in 117 seconds
Configuration accepted.
fred1@fred1:~$ cd /etc/netplan
fred1@fred1:~$ sudo netplan apply
fred1@fred1:~$ cd /etc/netplan
fred1@fred1:~$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data:
64 bytes from 1.1.1.1: icmp_seq=1 ttl=56 time=60.0 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=56 time=58.9 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=56 time=59.3 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=56 time=60.8 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=56 time=61.7 ms
64 bytes from 1.1.1.1: icmp_seq=6 ttl=56 time=60.7 ms
^Z
```

```

fred1@fred1:~$ resolvectl dns
Global:
Link 2 (enp0s3): 1.1.1.1 8.8.8.8
fred1@fred1:~$ ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=57 time=61.7 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=57 time=63.3 ms
^Z
[6]+  Остановлен ping 1.1.1.1
fred1@fred1:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=49.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=53.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=52.5 ms
^Z

```

```

fred1@fred1:~$ ls
1-network-manager-all.yaml
fred1@fred1:~$ sudo nano 1-network-manager-all.yaml
fred1@fred1:~$ sudo nano 1-network-manager-all.yaml
fred1@fred1:~$ ping ya.ru
PING ya.ru (77.88.55.242) 56(84) bytes of data.
64 bytes from ya.ru (77.88.55.242): icmp_seq=1 ttl=246 time=95.4 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=2 ttl=246 time=94.7 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=3 ttl=246 time=94.0 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=4 ttl=246 time=92.6 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=5 ttl=246 time=91.6 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=6 ttl=246 time=91.3 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=7 ttl=246 time=91.7 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=8 ttl=246 time=95.4 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=9 ttl=246 time=92.4 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=10 ttl=246 time=92.4 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=11 ttl=246 time=97.4 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=12 ttl=246 time=95.2 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=13 ttl=246 time=93.9 ms
^Z
[6]+  Остановлен ping ya.ru
fred1@fred1:~$ ping google.com
PING google.com (142.250.74.46) 56(84) bytes of data.
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=1 ttl=115 time=87.5 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=2 ttl=115 time=87.5 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=3 ttl=115 time=88.1 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=4 ttl=115 time=89.3 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=5 ttl=115 time=88.3 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=6 ttl=115 time=89.3 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=7 ttl=115 time=86.6 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=8 ttl=115 time=85.3 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=9 ttl=115 time=86.5 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=10 ttl=115 time=84.7 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=11 ttl=115 time=88.2 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=12 ttl=115 time=85.5 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=13 ttl=115 time=88.9 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=14 ttl=115 time=86.6 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=15 ttl=115 time=88.6 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=16 ttl=115 time=87.5 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=17 ttl=115 time=87.3 ms
64 bytes from arn09s22-in-f14.1e100.net (142.250.74.46): icmp_seq=18 ttl=115 time=86.3 ms
^Z
[7]+  Остановлен ping google.com

```

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

1 - вариант

```

fred1@fred1:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
fred1@fred1:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
fred1@fred1:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
fred1@fred1:~$ sudo iptables -A OUTPUT -m --state RELATED,ESTABLISHED -j ACCEPT
iptables v1.8.7 (nf_tables): Couldn't load match `--state': No such file or directory

Try `iptables -h' or 'iptables --help' for more information.
fred1@fred1:~$ sudo iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
fred1@fred1:~$ sudo iptables -A OUTPUT -p tcp --dport 80 -d archive.ubuntu.com -j ACCEPT
iptables v1.8.7 (nf_tables): host/network 'archive.ubuntu.com' not found
Try `iptables -h' or 'iptables --help' for more information.
fred1@fred1:~$ sudo iptables -A OUTPUT -p tcp --dport 80 -d archive.ubuntu.com -j ACCEPT
fred1@fred1:~$ sudo iptables -A OUTPUT -p tcp --dport 80 -d security.ubuntu.com -j ACCEPT
fred1@fred1:~$ sudo iptables -P INPUT DROP
fred1@fred1:~$ sudo iptables -P FORWARD DROP
fred1@fred1:~$ sudo iptables -P OUTPUT DROP
fred1@fred1:~$

```

2- вариант , изменил первый

```
fred1@fred1:~$ sudo iptables -L -nv
Chain INPUT (policy ACCEPT 0 packets, 0 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
fred1@fred1:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
fred1@fred1:~$ sudo iptables -A INPUT -p tcp -m multiport --dport 80,443 -j ACCEPT
Bad argument 'm'
Try `iptables -h' or 'iptables --help' for more information.
fred1@fred1:~$ sudo iptables -A INPUT -p tcp -m multiport --dport 80,443 -j ACCEPT
fred1@fred1:~$ sudo iptables -L -nv
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
 209 14824 ACCEPT    tcp  --  *      *      0.0.0.0/0               0.0.0.0/0          tcp dpt:22
    0    0 ACCEPT    tcp  --  *      *      0.0.0.0/0               0.0.0.0/0          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 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
fred1@fred1:~$ sudo iptables -A INPUT -i lo -j ACCEPT
fred1@fred1:~$ sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
fred1@fred1:~$ sudo iptables -A OUTPUT -p tcp --dport 80 -d archive.ubuntu.com -j ACCEPT
fred1@fred1:~$ sudo iptables -A OUTPUT -p tcp --dport 80 -d security.ubuntu.com -j ACCEPT
fred1@fred1:~$ sudo iptables -P INPUT DROP
fred1@fred1:~$ 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
fred1@fred1:~$ sudo iptables -L -nv
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
 852 55076 ACCEPT    tcp  --  *      *      0.0.0.0/0               0.0.0.0/0          tcp dpt:22
    0    0 ACCEPT    tcp  --  *      *      0.0.0.0/0               0.0.0.0/0          multiport dports 80,443
    6   613 ACCEPT    all  --  lo     *      0.0.0.0/0               0.0.0.0/0
```

```
    0    0 ACCEPT    tcp  --  *      *      0.0.0.0/0               0.0.0.0/0          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 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
fred1@fred1:~$ sudo iptables -A INPUT -i lo -j ACCEPT
fred1@fred1:~$ sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
fred1@fred1:~$ sudo iptables -A OUTPUT -p tcp --dport 80 -d archive.ubuntu.com -j ACCEPT
fred1@fred1:~$ sudo iptables -A OUTPUT -p tcp --dport 80 -d security.ubuntu.com -j ACCEPT
fred1@fred1:~$ sudo iptables -P INPUT DROP
fred1@fred1:~$ 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
fred1@fred1:~$ sudo iptables -L -nv
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source                   destination
 852 55076 ACCEPT    tcp  --  *      *      0.0.0.0/0               0.0.0.0/0          tcp dpt:22
    0    0 ACCEPT    tcp  --  *      *      0.0.0.0/0               0.0.0.0/0          multiport dports 80,443
    6   613 ACCEPT    all  --  lo     *      0.0.0.0/0               0.0.0.0/0
   10   785 ACCEPT    all  --  *      *      0.0.0.0/0               0.0.0.0/0          state RELATED,ESTABLISHED

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
    0    0 ACCEPT    tcp  --  *      *      0.0.0.0/0               91.189.91.81        tcp dpt:80
    0    0 ACCEPT    tcp  --  *      *      0.0.0.0/0               91.189.91.82        tcp dpt:80
    0    0 ACCEPT    tcp  --  *      *      0.0.0.0/0               91.189.91.83        tcp dpt:80
    0    0 ACCEPT    tcp  --  *      *      0.0.0.0/0               185.125.190.36      tcp dpt:80
    0    0 ACCEPT    tcp  --  *      *      0.0.0.0/0               185.125.190.39      tcp dpt:80
    0    0 ACCEPT    tcp  --  *      *      0.0.0.0/0               91.189.91.82        tcp dpt:80
    0    0 ACCEPT    tcp  --  *      *      0.0.0.0/0               185.125.190.39      tcp dpt:80
    0    0 ACCEPT    tcp  --  *      *      0.0.0.0/0               185.125.190.36      tcp dpt:80
    0    0 ACCEPT    tcp  --  *      *      0.0.0.0/0               91.189.91.83        tcp dpt:80
    0    0 ACCEPT    tcp  --  *      *      0.0.0.0/0               91.189.91.81        tcp dpt:80
fred1@fred1:~$
```

```
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination tcp dpt:80
0 0 ACCEPT tcp -- * * 0.0.0.0/0 91.189.91.81
0 0 ACCEPT tcp -- * * 0.0.0.0/0 91.189.91.82
0 0 ACCEPT tcp -- * * 0.0.0.0/0 91.189.91.83
0 0 ACCEPT tcp -- * * 0.0.0.0/0 185.125.190.36
0 0 ACCEPT tcp -- * * 0.0.0.0/0 185.125.190.39
0 0 ACCEPT tcp -- * * 0.0.0.0/0 91.189.91.82
0 0 ACCEPT tcp -- * * 0.0.0.0/0 185.125.190.39
0 0 ACCEPT tcp -- * * 0.0.0.0/0 185.125.190.36
0 0 ACCEPT tcp -- * * 0.0.0.0/0 91.189.91.83
0 0 ACCEPT tcp -- * * 0.0.0.0/0 91.189.91.81
```

```
fred1@fred1:~$ sudo iptables-save > /etc/iptables.rules
-bash: /etc/iptables.rules: Отказано в доступе
fred1@fred1:~$ iptables-save > /etc/iptables.rules
-bash: /etc/iptables.rules: Отказано в доступе
fred1@fred1:~$ sudo iptables-save > /etc/iptables.rules
-bash: /etc/iptables.rules: Отказано в доступе
fred1@fred1:~$ sudo iptables-save > /etc/iptables.rules
-bash: /etc/iptables.rules: Отказано в доступе
fred1@fred1:~$ sudo -i
root@fred1:~# iptables-save > /etc/iptables.rules
root@fred1:~# exit
выход
fred1@fred1:~$ cat /etc/iptables.rules
```

```
# Generated by iptables-save v1.8.7 on Thu Sep 21 22:05:15 2023
*filter
:INPUT DROP [1:73]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m multiport --dports 80,443 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -d 91.189.91.81/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.82/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.83/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.36/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.39/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.82/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.39/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.36/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.83/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.81/32 -p tcp -m tcp --dport 80 -j ACCEPT
COMMIT
# Completed on Thu Sep 21 22:05:15 2023
fred1@fred1:~$
```

```
# Generated by iptables-save v1.8.7 on Thu Sep 21 22:05:15 2023
*filter
:INPUT DROP [1:73]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m multiport --dports 80,443 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -d 91.189.91.81/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.82/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.83/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.36/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.39/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.82/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.39/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.36/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.83/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.81/32 -p tcp -m tcp --dport 80 -j ACCEPT
COMMIT
Выбор ранее не выбранного пакета netfilter-persistent.
(Чтение базы данных ... на данный момент установлено 543592 файла и каталога.)
Подготовка к распаковке .../netfilter-persistent_1.0.16_all.deb ...
Распаковывается netfilter-persistent (1.0.16) ...
Выбор ранее не выбранного пакета iptables-persistent.
Подготовка к распаковке .../iptables-persistent_1.0.16_all.deb ...
Распаковывается iptables-persistent (1.0.16) ...
Настраивается пакет netfilter-persistent (1.0.16) ...
Created symlink /etc/systemd/system/multi-user.target.wants/netfilter-persistent.service → /lib/systemd/system/netfilter-persistent.service.
Настраивается пакет iptables-persistent (1.0.16) ...
update-alternatives: используется /lib/systemd/system/netfilter-persistent.service для предоставления /lib/systemd/system/iptables.service (
iptables.service) в автоматическом режиме
Обрабатываются триггеры для man-db (2.10.2-1) ...
fred1@fred1:~$
```

```
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Следующие НОВЫЕ пакеты будут установлены:
  iptables-persistent netfilter-persistent
Обновлено 0 пакетов, установлено 2 новых пакетов, для удаления отмечено 0 пакетов, и 413 пакетов не обновлено.
Необходимо скачать 13,9 kB архивов.
После данной операции объём занятого дискового пространства возрастёт на 93,2 kB.
Пол:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 netfilter-persistent all 1.0.16 [7.440 B]
Пол:2 http://archive.ubuntu.com/ubuntu jammy/universe amd64 iptables-persistent all 1.0.16 [6.488 B]
Получено 13,9 kB за 1с (20,6 kB/s)
Предварительная настройка пакетов ...
```



```

fred1@fred1:~$ cd /etc/iptables/
fred1@fred1:/etc/iptables$ ll
итого 20
drwxr-xr-x  2 root root  4096 сен 21 22:08 ./
drwxr-xr-x 149 root root 12288 сен 21 22:08 ../
-rw-r--r--  1 root root  1009 сен 21 22:08 rules.v4
-rw-r--r--  1 root root    0 сен 21 22:08 rules.v6
fred1@fred1:/etc/iptables$ cat rules.v4
# Generated by iptables-save v1.8.7 on Thu Sep 21 22:08:28 2023
*filter
:INPUT DROP [1:73]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m multiport --dports 80,443 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -d 91.189.91.81/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.82/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.83/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.36/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.39/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.82/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.39/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.36/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.83/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.81/32 -p tcp -m tcp --dport 80 -j ACCEPT
COMMIT
# Completed on Thu Sep 21 22:08:28 2023
fred1@fred1:/etc/iptables$

```

1. Создайте правило для разрешения входящих соединений на портах 22, 80 и 443:


```

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

```
2. Разрешите исходящие соединения:


```

sudo iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

```
3. Запретите все остальные входящие и исходящие соединения:


```

sudo iptables -P INPUT DROP
# sudo iptables -P FORWARD DROP
# sudo iptables -P OUTPUT DROP

```
4. Сохраните изменения, чтобы они пережили перезагрузку сервера:


```

sudo iptables-save > /etc/iptables.rules

```
5. Активируйте iptables при загрузке сервера:


```

sudo systemctl enable iptables

```
6. Запустите iptables:


```

sudo systemctl start iptables

```

* 3) Запретить любой входящий трафик с IP 3.4.5.6.

```
fred1@fred1:~$ sudo iptables -A INPUT -s 3.4.5.6 -j DROP
fred1@fred1:~$
```

Это правило добавляет запись, которая блокирует весь входящий трафик с IP-адреса 3.4.5.6. -s указывает на исходный IP-адрес, и -j DROP указывает, что все пакеты с этого IP будут отбрасываться.

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

```
fred1@fred1:~$ sudo sysctl net.ipv4.ip_forward=1
[sudo] пароль для fred1:
net.ipv4.ip_forward = 1
fred1@fred1:~$ sudo iptables -t nat -A PREROUTING -p tcp --dport 8090 -j REDIRECT --to-port 80
fred1@fred1:~$ sudo iptables-save > /etc/iptables.rules
-bash: /etc/iptables.rules: Отказано в доступе
fred1@fred1:~$ sudo !!
sudo sudo iptables-save > /etc/iptables.rules
-bash: /etc/iptables.rules: Отказано в доступе
fred1@fred1:~$ sudo -i
root@fred1:~# iptables-save > /etc/iptables.rules
root@fred1:~# exit
выход
fred1@fred1:~$ iptables -L -nv -t nat
iptables v1.8.7 (nf_tables): Could not fetch rule set generation id: Permission denied (you must be root)

fred1@fred1:~$ 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  tcp  --  *      *        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
fred1@fred1:~$
```

Включите маскирование (NAT) для IPv4, если оно ещё не включено. Это позволит перенаправлять трафик:

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

Чтобы сделать это изменение постоянным, отредактируйте файл `/etc/sysctl.conf` и установите значение `net.ipv4.ip_forward` в 1.

1. Добавьте правило iptables для перенаправления трафика с порта 8090 на порт 80:

```
sudo iptables -t nat -A PREROUTING -p tcp --dport 8090 -j REDIRECT --to-port 80
```

Это правило перенаправит все входящие TCP-запросы на порт 8090 на порт 80.

2. Сохраните изменения, чтобы они пережили перезагрузку сервера:

```
sudo iptables-save > /etc/iptables.rules
```

3. Активируйте iptables при загрузке сервера:

```
sudo systemctl enable iptables
```

4. Запустите iptables:

```
sudo systemctl start iptables
```

Теперь запросы на порт 8090 будут перенаправляться на порт 80 на том же сервере.

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

```
PS C:\Users\fred1> ssh fred1@172.30.226.154
fred1@172.30.226.154 s password:
Last login: Thu Sep 21 18:04:29 2023 from 172.30.224.1
fred1@fred1:~$ # sudo iptables -I INPUT -p TCP --dport 22 -j DROP
fred1@fred1:~$ sudo iptables -I INPUT -p tcp --dport 22 -s 172.30.226.154 -j ACCEPT
[sudo] пароль fred1:
fred1@fred1:~$ sudo iptables -I INPUT -p tcp --dport 22 -s 192.168.0.0/24 -j ACCEPT
fred1@fred1:~$ sudo iptables -L INPUT -nv
Chain INPUT (policy DROP 2 packets, 146 bytes)
  pkts bytes target     prot opt in     out     source            destination
    0     0 ACCEPT    tcp  --  *     *       192.168.0.0/24    0.0.0.0/0
    0     0 ACCEPT    tcp  --  *     *       172.30.226.154    0.0.0.0/0
  2718 171K ACCEPT    tcp  --  *     *       0.0.0.0/0         0.0.0.0/0
    0     0 ACCEPT    tcp  --  *     *       0.0.0.0/0         0.0.0.0/0
   89 10405 ACCEPT   all  --  lo    *       0.0.0.0/0         0.0.0.0/0
 1055 1915K ACCEPT   all  --  *     *       0.0.0.0/0         0.0.0.0/0
                                     state RELATED,ESTABLISHED
fred1@fred1:~$ sudo journalctl -xe | grep ssh
Subject: Начинается запуск юнита ssh.service
Начат процесс запуска юнита ssh.service.
сен 21 18:03:07 fred1 sshd[873]: Server listening on 0.0.0.0 port 22.
сен 21 18:03:07 fred1 sshd[873]: Server listening on :: port 22.
Subject: Запуск юнита ssh.service завершен
Процесс запуска юнита ssh.service был завершен.
сен 21 18:03:15 fred1 systemd[1627]: Listening on GnuPG cryptographic agent (ssh-agent emulation).
сен 21 18:03:25 fred1 systemd[1731]: Listening on GnuPG cryptographic agent (ssh-agent emulation).
сен 21 18:03:35 fred1 systemd[1627]: Closed GnuPG cryptographic agent (ssh-agent emulation).
сен 21 18:04:29 fred1 sshd[2553]: Accepted password for fred1 from 172.30.224.1 port 58143 ssh2
сен 21 18:04:29 fred1 sshd[2553]: pam_unix(sshd:session): session opened for user fred1(uid=1000) by (uid=0)
сен 21 22:44:15 fred1 sshd[2561]: Received disconnect from 172.30.224.1 port 58143:11: disconnected by user
сен 21 22:44:15 fred1 sshd[2561]: Disconnected from user fred1 172.30.224.1 port 58143
сен 21 22:44:15 fred1 sshd[2553]: pam_unix(sshd:session): session closed for user fred1
сен 21 22:44:24 fred1 sshd[5241]: Accepted password for fred1 from 172.30.224.1 port 54154 ssh2
сен 21 22:44:24 fred1 sshd[5241]: pam_unix(sshd:session): session opened for user fred1(uid=1000) by (uid=0)
fred1@fred1:~$ sudo -i
root@fred1:~# iptables-save > /etc/iptables.rules
root@fred1:~# exit
выход
fred1@fred1:~$ sudo cat /etc/iptables.rules
# Generated by iptables-save v1.8.7 on Thu Sep 21 23:04:42 2023
*filter
:INPUT DROP [3:219]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -s 192.168.0.0/24 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 172.30.226.154/32 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m multiport --dports 80,443 -j ACCEPT
-A INPUT -i lo -j ACCEPT
```

1. # sudo iptables -I INPUT -p TCP --dport 22 -j DROP
2. sudo iptables -I INPUT -p tcp --dport 22 -s 172.30.226.154 -j ACCEPT
3. sudo iptables -I INPUT -p tcp --dport 22 -s 192.168.0.0/24 -j ACCEPT
4. sudo iptables -L INPUT -nv
5. sudo journalctl -xe | grep ssh
6. sudo -i
7. iptables-save > /etc/iptables.rules
8. exit
9. sudo cat /etc/iptables.rules


```

fred1@fred1:~$ sudo -i
root@fred1:~# iptables-save > /etc/iptables.rules
root@fred1:~# exit
выход
fred1@fred1:~$ sudo cat /etc/iptables.rules
# Generated by iptables-save v1.8.7 on Thu Sep 21 23:04:42 2023
*filter
:INPUT DROP [3:219]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -s 192.168.0.0/24 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -s 172.30.226.154/32 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m multiport --dports 80,443 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -d 91.189.91.81/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.82/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.83/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.36/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.39/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.82/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.39/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 185.125.190.36/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.83/32 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 91.189.91.81/32 -p tcp -m tcp --dport 80 -j ACCEPT
COMMIT
# Completed on Thu Sep 21 23:04:42 2023
# Generated by iptables-save v1.8.7 on Thu Sep 21 23:04:42 2023
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -p tcp -m tcp --dport 8090 -j REDIRECT --to-ports 80
COMMIT
# Completed on Thu Sep 21 23:04:42 2023
fred1@fred1:~$

```

СПАСИБО за ВНИМАНИЕ !)