

Содержание

Задача	2
Ход работы	2
Установка FTP сервера	2
Конфигурирование iptables	3
Заключение	10

Задача

Изучить настройку Firewall в ОС Linux

Шаги:

1. Посмотреть правила firewall по умолчанию
2. Разрешить доступ со всех адресов, но оставить только 22 порт для SSH
3. Запретить доступ со всех ip-адресов кроме своего
4. Установить FTP сервер (например proftpd), настроить его работу в пассивном режиме, открыть в фаерволле порты, необходимые для его работы

Ход работы

Установка FTP сервера

В качестве “испытательного полигона (сервера)” будем использовать виртуальную машину с дистрибутивом Ubuntu. Подробные шаги установки системы и настройки ssh приведены в отчёте по лабораторной работе №7.

1. Подключаемся к виртуальной машине (серверу) и выполняем команду по обновлению пакетов и зависимостей:

```
$ sudo apt-get update && sudo apt-get upgrade
```

2. После обновления системы в качестве ftp-сервера устанавливаем ProFTPD командой

```
$ sudo apt install proftpd-basic
```

3. Открываем файл конфигурации ProFTPD

```
$ sudo vi /etc/proftpd/proftpd.conf
```

Раскомментируем значение **PassivePorts** и изменим значение с “49152 65534” на “50000 50535”. Данный промежуток портов будет использован далее при конфигурировании iptables.

```
# In some cases you have to specify passive ports range to by-pass
# firewall limitations. Ephemeral ports can be used for that, but
# feel free to use a more narrow range.
PassivePorts 50000 50535
```

4. Перезагружаем ProFTPD командой

```
$ sudo systemctl restart proftpd.service
```

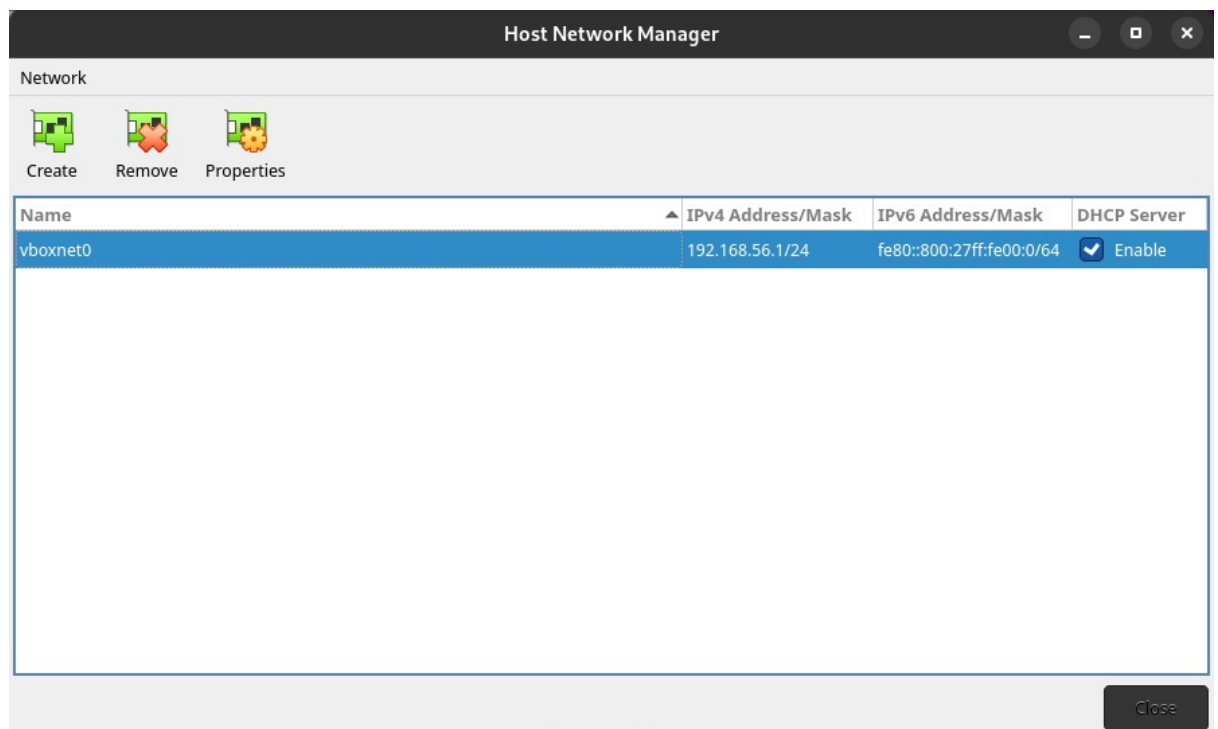
Конфигурирование iptables

Так как в качестве сервера была использована виртуальная машина, необходимо провести первоначальную настройку:

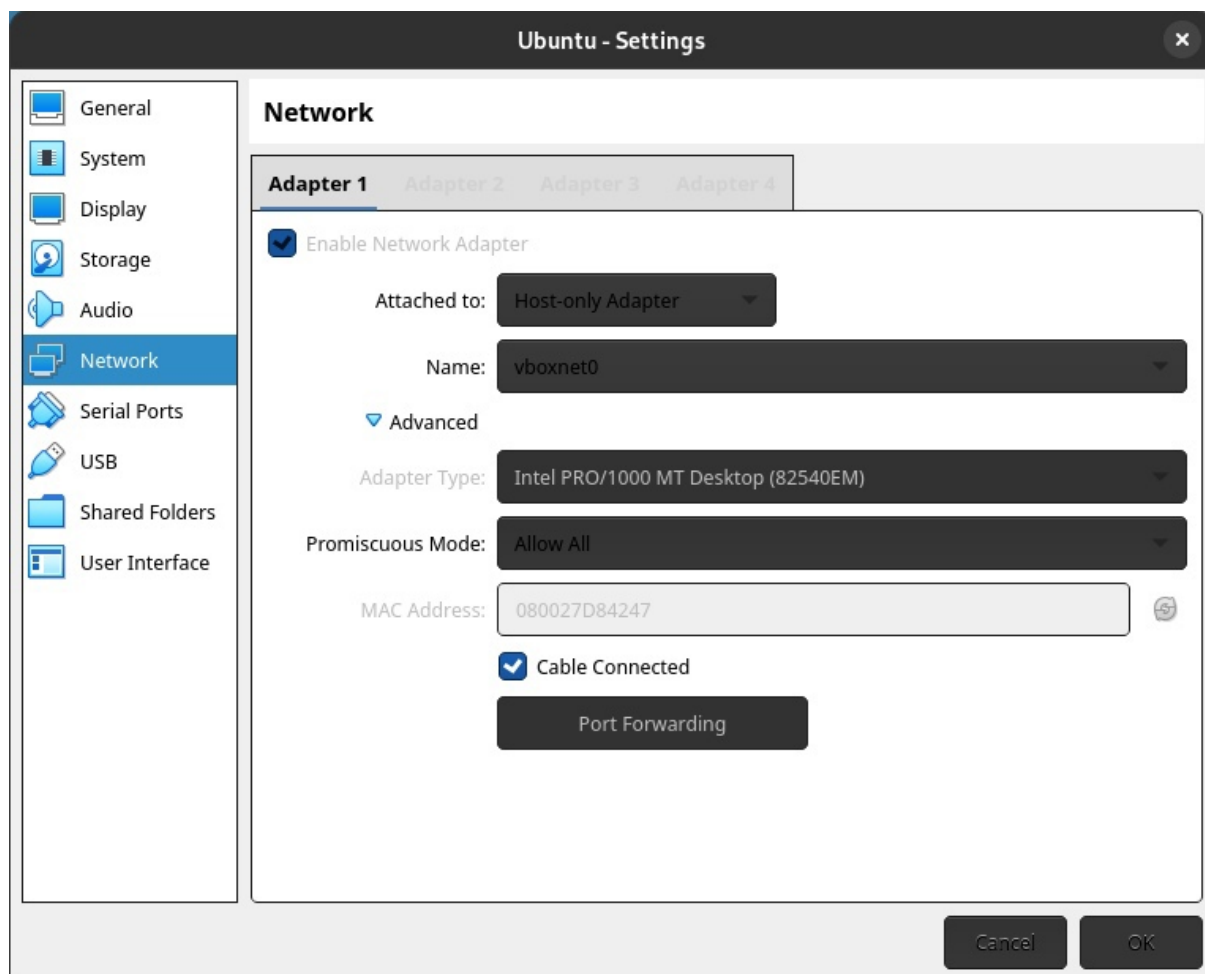
1. Выключаем систему (если она была запущена) командой

```
$ sudo shutdown now
```

2. Создадим виртуальный сетевой адаптер, для этого выполняем следующую последовательность действий: [File - Host Network Manager - Create]



- После этого переходим в настройки виртуальной машины во вкладку "Network" и устанавливаем Attached to: "Host-only Adapter", Name: ранее созданный адаптер (vboxnet0), а также Promiscuous Mode: "Allow all"



- Сохраняем конфигурацию и запускаем виртуальную машину

*Далее следуют специфичные шаги предварительной настройки (после которых firewall вернётся к исходным значениям)

- * Отключаем сервис UFW (интерфейс iptables для Ubuntu) командой

```
$ sudo systemctl disable ufw.service
```

- * Очищаем цепочки INPUT, FORWARD и OUTPUT командой

```
$ sudo iptables -F INPUT
```

```
$ sudo iptables -F FORWARD
```

```
$ sudo iptables -F OUTPUT
```

7. * Сохраним конфигурацию командой

```
$ sudo /sbin/iptables-save
```

Приступим к конфигурированию брандмауэра

8. Получим текущее состояние iptables (по умолчанию) командой

```
$ sudo iptables -L | grep policy
```

```
dmitriy@dsnet:~$ sudo iptables -L | grep policy
Chain INPUT (policy ACCEPT)
Chain FORWARD (policy ACCEPT)
Chain OUTPUT (policy ACCEPT)
```

Значения по умолчанию свидетельствуют о том, что каждая из цепочек принимает, пересылает и отправляет все пакеты (значения ACCEPT)

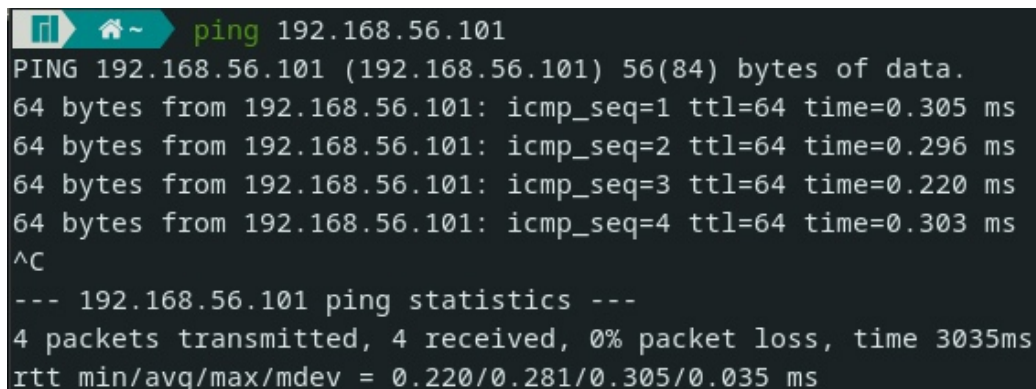
9. Проверим корректность настройки:

- а. Получим ip адрес машины командой ip addr

```
dmitriy@dsnet:~$ ip addr
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:d8:42:47 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
        valid_lft 356sec preferred_lft 356sec
    inet6 fe80::b61e:e2a9:136d:5d5/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

- b. Проверим соединение между основной системой и виртуальной машиной командой

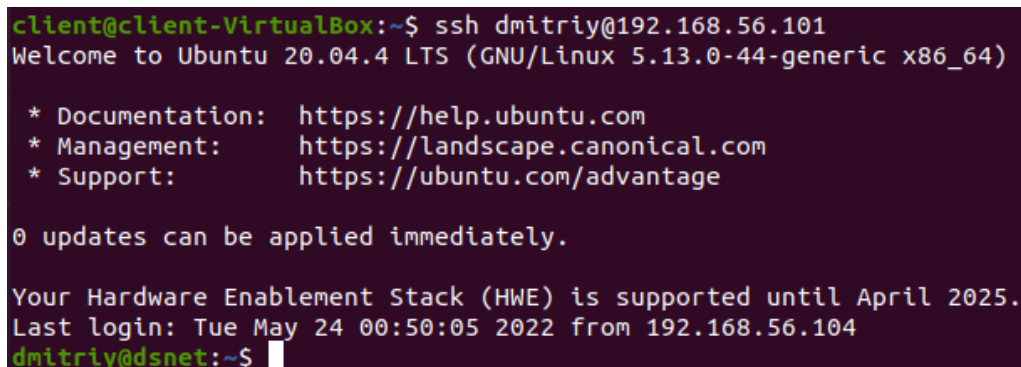
```
$ ping 192.168.56.101
```



```
ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.305 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.296 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.220 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.303 ms
^C
--- 192.168.56.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3035ms
rtt min/avg/max/mdev = 0.220/0.281/0.305/0.035 ms
```

* С основной системы, ip = 192.168.56.1

Вывод команды показывает, что машина успешно принимает и отправляет пакеты. Кроме того, успешно обрабатываются пакеты и устанавливаются соединения с других ip адресов:



```
client@client-VirtualBox:~$ ssh dmitriy@192.168.56.101
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-44-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 updates can be applied immediately.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue May 24 00:50:05 2022 from 192.168.56.104
dmitriy@dsnet:~$
```

* С другой виртуальной машины, ip = 192.168.56.104

10. Добавим возможность подключения через ssh (порт 22) командой

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

11. Также разрешим доступ с ip адреса основной системы (можно узнать командой ip add) командой

```
$ sudo iptables -A INPUT -s 192.168.56.1 -j ACCEPT
```

12. Наконец, добавим возможность подключения к ftp-серверу командами

```
$ sudo iptables -A INPUT -p tcp -m tcp --dport 21 -j ACCEPT
```

```
$ sudo iptables -A INPUT -p tcp -m tcp --dport 20 -j ACCEPT
```

*Для активного режима

```
$ sudo iptables -A INPUT -p tcp -m tcp --dport 50000:50534 -j ACCEPT
```

13. После этого устанавливаем блокирующее поведение (всё, что не запрещено, то разрешено) по умолчанию для цепочки INPUT командой

```
$ sudo iptables -P INPUT DROP
```

14. Получим информацию о конфигурации iptables командой

```
$ sudo iptables -L
```

```
dmitriy@dsnet:~$ sudo iptables -L
[sudo] password for dmitriy:
Chain INPUT (policy DROP)
target     prot opt source                destination            tcp dpt:ssh
ACCEPT     tcp  --  anywhere              anywhere               tcp dpt:ftp
ACCEPT     tcp  --  192.168.56.1          anywhere              tcp dpt:ftp-data
ACCEPT     tcp  --  anywhere              anywhere              tcp dpts:50000:50534

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
dmitriy@dsnet:~$
```

15. Сохраним конфигурацию командой

```
$ sudo /sbin/iptables-save
```

16. Проверим корректность настройки:

С основной системы (192.168.56.1):

- Ping

```
~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.296 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.272 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.297 ms
64 bytes from 192.168.56.101: icmp_seq=4 ttl=64 time=0.332 ms
^C
--- 192.168.56.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3032ms
rtt min/avg/max/mdev = 0.272/0.299/0.332/0.021 ms
~$
```

- SSH

```
~$ ssh dmitriy@192.168.56.101
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-44-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 updates can be applied immediately.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue May 24 00:28:33 2022 from 192.168.56.1
dmitriy@dsnet:~$
```


- FTP

```
ftp> open 192.168.56.101
Connected to 192.168.56.101.
220 ProFTPD Server (Lab_ftp) [::ffff:192.168.56.101]
Name (192.168.56.101:dstakheev): dmitriy
331 Password required for dmitriy
Password:
230 User dmitriy logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x  3 dmitriy  dmitriy      4096 Apr 19 22:17 Desktop
drwxr-xr-x  2 dmitriy  dmitriy      4096 Mar 24 18:36 Documents
drwxr-xr-x  2 dmitriy  dmitriy      4096 May 21 14:37 Downloads
drwxr-xr-x  2 dmitriy  dmitriy      4096 Mar 24 18:36 Music
drwxr-xr-x  2 dmitriy  dmitriy      4096 May 21 22:54 Pictures
drwxrwxr-x  6 dmitriy  dmitriy      4096 Mar 24 22:10 pt
drwxr-xr-x  2 dmitriy  dmitriy      4096 Mar 24 18:36 Public
drwx----- 4 dmitriy  dmitriy      4096 Apr 17 16:46 snap
drwxr-xr-x  2 dmitriy  dmitriy      4096 Mar 24 18:36 Templates
drwxr-xr-x  2 dmitriy  dmitriy      4096 May 23 21:16 test_dir_ftp
drwxr-xr-x  2 dmitriy  dmitriy      4096 Mar 24 18:36 Videos
226 Transfer complete
ftp> █
```

С дополнительной виртуальной машины (192.168.56.104):

- Ping

```
client@client-VirtualBox:~$ ping 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
```

- SSH

```
client@client-VirtualBox:~$ ssh dmitriy@192.168.56.101
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-44-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 updates can be applied immediately.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Tue May 24 00:46:50 2022 from 192.168.56.1
dmitriy@dsnet:~$
```

- FTP

```
client@client-VirtualBox:~$ ftp
ftp> open 192.168.56.101
Connected to 192.168.56.101.
220 ProFTPD Server (Lab_ftp) [::ffff:192.168.56.101]
Name (192.168.56.101:client): dmitriy
331 Password required for dmitriy
Password:
230 User dmitriy logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x  3 dmitriy  dmitriy      4096 Apr 19 22:17 Desktop
drwxr-xr-x  2 dmitriy  dmitriy      4096 Mar 24 18:36 Documents
drwxr-xr-x  2 dmitriy  dmitriy      4096 May 21 14:37 Downloads
drwxr-xr-x  2 dmitriy  dmitriy      4096 Mar 24 18:36 Music
drwxr-xr-x  2 dmitriy  dmitriy      4096 May 21 22:54 Pictures
drwxrwxr-x  6 dmitriy  dmitriy      4096 Mar 24 22:10 pt
drwxr-xr-x  2 dmitriy  dmitriy      4096 Mar 24 18:36 Public
drwx----- 4 dmitriy  dmitriy      4096 Apr 17 16:46 snap
drwxr-xr-x  2 dmitriy  dmitriy      4096 Mar 24 18:36 Templates
drwxr-xr-x  2 dmitriy  dmitriy      4096 May 23 21:16 test_dir_ftp
drwxr-xr-x  2 dmitriy  dmitriy      4096 Mar 24 18:36 Videos
226 Transfer complete
ftp> █
```

Из полученных данных можно сделать вывод о том, что виртуальная машина (сервер) корректно обрабатывает SSH и FTP соединения с любых ip адресов, а также блокирует все пакеты, приходящие НЕ с ip адреса основной системы.

Заключение

В результате выполнения работы был настроен Firewall OS Linux (Ubuntu) согласно спецификации, а также установлен ftp-сервер (ProFTPD).