Firewall

1. Uncomplicated Firewall (**UFW**) is a tool configure ***iptables*** firewall.

2. To install ufw:

   sudo apt install ufw

3. By default, it is disabled. To the status:

   sudo ufw status

```
royal@polarbear:~$ sudo ufw status
Status: inactive
royal@polarbear:~$ _
```

   If firewall is enabled, a list of rules will be displayed.

```
royal@polarbear:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       192.168.30.0/24
Anywhere                   ALLOW       192.168.30.104
80                         DENY        Anywhere
80 (v6)                    DENY        Anywhere (v6)

royal@polarbear:~$ _
```

   Rules can be displayed as numbered format.

```
royal@polarbear:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22                         ALLOW IN    192.168.30.0/24
[ 2] Anywhere                   ALLOW IN    192.168.30.104
[ 3] 80                         DENY IN     Anywhere
[ 4] 80 (v6)                    DENY IN     Anywhere (v6)

royal@polarbear:~$
```

4. Examples of configuration.

   a. To allow ssh traffic:

      sudo ufw allow ssh

```
royal@polarbear:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
royal@polarbear:~$ _
```

      NOTE: this allows ssh connection from anywhere, which will increase the security risks.

b. To allow specific port:

sudo ufw allow *port_number*

sudo ufw allow *port_number/protocol*

Examples:
sudo ufw allow 22
sudo ufw allow 80/tcp

```
royal@polarbear:~$ sudo ufw allow 80/tcp
Rule added
Rule added (v6)
royal@polarbear:~$ _
```

c. To remove a rule:

sudo ufw delete *rule*

sudo ufw delete *rule_number*

Example: sudo ufw delete allow ssh

```
royal@polarbear:~$ sudo ufw delete allow ssh
Rules updated
Rules updated (v6)
royal@polarbear:~$ _
```

Example: sudo ufw delete 2

```
royal@polarbear:~$ sudo ufw delete 2
Deleting:
 allow from 192.168.30.104
Proceed with operation (y|n)? y
Rule deleted
royal@polarbear:~$
```

d. To allow ssh traffic from a specific IP address:

sudo ufw allow from *IP* to *IP* port *number*

Example: sudo ufw allow from 192.168.30.103 to any port 22

any – any IP address

```
royal@polarbear:~$ sudo ufw allow from 192.168.30.103 to any port 22
Rules updated
royal@polarbear:~$
```

e. To allow ssh traffic from a subnet:

sudo ufw allow from *subnet* to *IP* port *number*

Example: sudo ufw allow from 192.168.30.0/24 to any port 22

```
royal@polarbear:~$ sudo ufw allow from 192.168.30.0/24 to any port 22
Rules updated
royal@polarbear:~$ _
```

f. To allow traffic from a specific IP to access anything:

sudo ufw allow from *IP*

Example: sudo ufw allow from 192.168.30.103

NOTE: Consider and evaluate the risks of allowing access to anything on the server.

g. To allow tcp traffic from a specific IP/port to a host/port:

sudo ufw proto tcp from *IP* port *number* to *IP* port *number*

Example: sudo ufw proto tcp from 192.168.30.105 port 18080 to any port 18080

```
royal@polarbear:~$ sudo ufw allow proto tcp from 192.168.30.106 port 18080 to any port 18080
Rule added
royal@polarbear:~$
```

h. To deny traffic from a specific subnet to a specific host:

sudo ufw deny from *subnet* to *IP* port *number*

Example: sudo ufw deny from 10.0.0.0/8 to 192.168.30.102 port 22

```
royal@polarbear:~$ sudo ufw deny from 10.0.0.0/8 to 192.168.30.102 port 22
Rule added
royal@polarbear:~$ _
```

i. To close an opened port:

sudo ufw deny *port_number*

Example: sudo ufw deny 80

```
royal@polarbear:~$ sudo ufw deny 80
Rules updated
Rules updated (v6)
royal@polarbear:~$ _
```

j. Rule can also be applied on specific network interface:

sudo ufw *option* on *interface*

Example, deny incoming traffic on an interface: sudo ufw deny in on enp0s3

in – incoming traffic
out – outgoing traffic

```
royal@polarbear:~$ sudo ufw deny in on enp0s3
Rule added
Rule added (v6)
royal@polarbear:~$ _
```

5. It's better to configure the firewall before it is activated. To enable the firewall:

sudo ufw enable

```
royal@polarbear:~$ sudo ufw enable
Firewall is active and enabled on system startup
royal@polarbear:~$ _
```

6. To disable the firewall

sudo ufw disable

7. Application that opens a port can install an ufw profile into /etc/ufw/applications.d

   a. To view which application has installed a profile:

      sudo ufw app list

```
royal@polarbear:~$ sudo ufw app list
[sudo] password for royal:
Available applications:
  Apache
  Apache Full
  Apache Secure
  Bind9
  Dovecot IMAP
  Dovecot POP3
  Dovecot Secure IMAP
  Dovecot Secure POP3
  OpenLDAP LDAP
  OpenLDAP LDAPS
  OpenSSH
  Postfix
  Postfix SMTPS
  Postfix Submission
  Samba
royal@polarbear:~$
```

   b. Profile can be used to allow/deny traffic.

      sudo ufw *option app_name*

      Examples:

      sudo ufw allow Samba

```
royal@polarbear:~$ sudo ufw allow Samba
[sudo] password for royal:
Rule added
Rule added (v6)
royal@polarbear:~$
```

      sudo ufw allow from 192.168.30.0/24 to any app Samba

```
royal@polarbear:~$ sudo ufw allow from 192.168.30.0/24 to any app Samba
Rule added
royal@polarbear:~$
```

```
royal@polarbear:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22                         ALLOW IN    192.168.30.0/24
[ 2] 80                         DENY IN     Anywhere
[ 3] 192.168.30.102 22          DENY IN     10.0.0.0/8
[ 4] Anywhere on enp0s3         DENY IN     Anywhere
[ 5] 80/tcp                     ALLOW IN    Anywhere
[ 6] 18080/tcp                  ALLOW IN    192.168.30.106 18080/tcp
[ 7] Samba                      ALLOW IN    192.168.30.0/24
[ 8] 80 (v6)                    DENY IN     Anywhere (v6)
[ 9] Anywhere (v6) on enp0s3    DENY IN     Anywhere (v6)
[10] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
```

c. To view the details of an application profile:

sudo ufw app info *app_name*

Example: sudo ufw app info Apache

```
royal@polarbear:~$ sudo ufw app info Apache
Profile: Apache
Title: Web Server
Description: Apache v2 is the next generation of the omnipresent Apache web
server.

Port:
  80/tcp
royal@polarbear:~$
```

d. The syntax of an application profile:

[name]
title=
description=
ports=

Example:

```
royal@polarbear:~$ cat /etc/ufw/applications.d/apache2-utils.ufw.profile
[Apache]
title=Web Server
description=Apache v2 is the next generation of the omnipresent Apache web server.
ports=80/tcp

[Apache Secure]
title=Web Server (HTTPS)
description=Apache v2 is the next generation of the omnipresent Apache web server.
ports=443/tcp

[Apache Full]
title=Web Server (HTTP,HTTPS)
description=Apache v2 is the next generation of the omnipresent Apache web server.
ports=80,443/tcp
royal@polarbear:~$
```

Multiple ports are separated by '|'. Example:
ports=22/udp|35|66,70:79/tcp

Homework:
Study iptables and its commands.