

## Installing and configuring the ufw firewall package.

Sudo apt-get install ufw

```
afnog@pc39:~$ sudo apt-get install ufw
```

Enable the firewall after installation using the command below.

ufw enable

```
afnog@pc39:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
ERROR: initcaps
[Errno 2] iptables v1.4.21: can't initialize iptables table `filter': Table does not exist (do you need to insmod?)
Perhaps iptables or your kernel needs to be upgraded.
```

In case you get the following errors above, perform the following steps below to enable UFW

Edit file ufw in the following directory as below and change the IPV6=yes to IPV6=no as below.

```
afnog@pc39:~$ sudo vi /etc/default/ufw
```

```
IPV6=no
```

When you check the status again, it should show active

ufw status verbose

```
afnog@pc39:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing)
New profiles: skip
afnog@pc39:~$
```

The first thing you want to do is how to check help manual.

ufw --help

```
afnog@pc39:~$ sudo ufw --help
Usage: ufw COMMAND

Commands:
  enable                enables the firewall
  disable              disables the firewall
  default ARG          set default policy
  logging LEVEL        set logging to LEVEL
  allow ARGS           add allow rule
  deny ARGS            add deny rule
  reject ARGS         add reject rule
  limit ARGS          add limit rule
  delete RULE|NUM     delete RULE
  insert NUM RULE     insert RULE at NUM
  reset               reset firewall
  status              show firewall status
  status numbered    show firewall status as numbered list of RULES
  status verbose     show verbose firewall status
  show ARG           show firewall report
  version            display version information
```

How do we add rules to allow and deny packets?

There are three methods which are allow, deny or reject

Deny drops packets without any message

Reject drops packets with a message

To allow a web server packet which is port 80 for example, you issue command below.

ufw allow 80

```
afnog@pc39:~$ sudo ufw allow 80
Rule added
```

You can check the rule table by using command below  
ufw status numbered

```
afnog@pc39:~$ sudo ufw status numbered
Status: active

      To      Action      From
      --      -
[ 1] 80      ALLOW IN   Anywhere

afnog@pc39:~$
```

To reject port 8080 for example can be achieved using  
command bellow

Ufw reject 8080

```
afnog@pc39:~$ sudo ufw reject 8080
Rule added
```

Ufw deny 8081

```
afnog@pc39:~$ sudo ufw status numbered
Status: active

      To      Action      From
      --      -
[ 1] 80      ALLOW IN   Anywhere
[ 2] 8080    REJECT IN  Anywhere
[ 3] 8081    DENY IN   Anywhere
```

Check the rule table to see your firewall rule addition for the  
previous rule as above

If you want to specify a particular protocol and that can be achieved with below command

ufw allow to any port 9000 proto udp

```
afnog@pc39:~$ sudo ufw allow to any port 9000 proto udp
Rule added
```

```
afnog@pc39:~$ sudo ufw status numbered
Status: active

      To      Action      From
      --      -
[ 1] 80      ALLOW IN    Anywhere
[ 2] 8080     REJECT IN   Anywhere
[ 3] 8081     DENY IN     Anywhere
[ 4] 9000/udp ALLOW IN    Anywhere
```

To block SSH protocol, you issue command below.

Ufw deny ssh

```
afnog@pc39:~$ sudo ufw deny ssh
Rule added
```

```
afnog@pc39:~$ sudo ufw status numbered
Status: active

      To      Action      From
      --      -
[ 1] 80      ALLOW IN    Anywhere
[ 2] 8080     REJECT IN   Anywhere
[ 3] 8081     DENY IN     Anywhere
[ 4] 9000/udp ALLOW IN    Anywhere
[ 5] 22      DENY IN     Anywhere
```

To completely deny ssh as in IN and OUT, then the following command applies. That implies SSH is deny in both directions.

Ufw deny OUT 22

```
afnog@pc39:~$ sudo ufw deny OUT 22
Rule added
```

```
afnog@pc39:~$ sudo ufw status numbered
Status: active

      To      Action      From
      --      -
[ 1] 80      ALLOW IN   Anywhere
[ 2] 8080     REJECT IN  Anywhere
[ 3] 8081     DENY IN   Anywhere
[ 4] 9000/udp ALLOW IN   Anywhere
[ 5] 22      DENY IN   Anywhere
[ 6] 22      DENY OUT   Anywhere (out)
```

Another thing you want to be able to do is control which IP address comes in or out of your server.

For example you want to block all incoming connection from an IP address, the command below applies

ufw deny from 196.200.219.101 to any

```
afnog@pc39:~$ sudo ufw deny from 196.200.219.101 to any
Rule added
```

```
afnog@pc39:~$ sudo ufw status numbered
Status: active

      To      Action      From
      --      -
[ 1] 80      ALLOW IN    Anywhere
[ 2] 8080     REJECT IN   Anywhere
[ 3] 8081     DENY IN     Anywhere
[ 4] 9000/udp ALLOW IN    Anywhere
[ 5] 22      DENY IN     Anywhere
[ 6] 22      DENY OUT    Anywhere (out)
[ 7] Anywhere DENY IN     196.200.219.101
```

For example if you want to block all outgoing connection from the same IP address above, the command below applies.

ufw deny OUT from any to 196.200.219.101

```
afnog@pc39:~$ sudo ufw deny OUT from any to 196.200.219.101
Rule added
```

```
afnog@pc39:~$ sudo ufw status numbered
Status: active

      To      Action      From
      --      -
[ 1] 80      ALLOW IN    Anywhere
[ 2] 8080     REJECT IN   Anywhere
[ 3] 8081     DENY IN     Anywhere
[ 4] 9000/udp ALLOW IN    Anywhere
[ 5] 22      DENY IN     Anywhere
[ 6] 22      DENY OUT    Anywhere (out)
[ 7] Anywhere DENY IN     196.200.219.101
[ 8] 196.200.219.101 DENY OUT    Anywhere (out)
```

If you want to allow in and out from a particular port, the following command applies.

ufw allow OUT from any port 8080 to 196.200.219.102

```
afnog@pc39:~$ sudo ufw allow OUT from any port 8080 to 196.200.219.102
Rule added
```

```
afnog@pc39:~$ sudo ufw status numbered
Status: active
```

|      | To              | Action    | From            |
|------|-----------------|-----------|-----------------|
|      | --              | -----     | ----            |
| [ 1] | 80              | ALLOW IN  | Anywhere        |
| [ 2] | 8080            | REJECT IN | Anywhere        |
| [ 3] | 8081            | DENY IN   | Anywhere        |
| [ 4] | 9000/udp        | ALLOW IN  | Anywhere        |
| [ 5] | 22              | DENY IN   | Anywhere        |
| [ 6] | 22              | DENY OUT  | Anywhere (out)  |
| [ 7] | Anywhere        | DENY IN   | 196.200.219.101 |
| [ 8] | 196.200.219.101 | DENY OUT  | Anywhere (out)  |
| [ 9] | 196.200.219.102 | ALLOW OUT | 8080 (out)      |

ufw allow IN from from 196.200.219.102 to any port 8080

```
afnog@pc39:~$ sudo ufw allow IN from 196.200.219.102 to any port 8080
Rule added
```

```
afnog@pc39:~$ sudo ufw status numbered
Status: active

      To Action From
      --
[ 1] 80 ALLOW IN Anywhere
[ 2] 8080 REJECT IN Anywhere
[ 3] 8081 DENY IN Anywhere
[ 4] 9000/udp ALLOW IN Anywhere
[ 5] 22 DENY IN Anywhere
[ 6] 22 DENY OUT Anywhere (out)
[ 7] Anywhere DENY IN 196.200.219.101
[ 8] 196.200.219.101 DENY OUT Anywhere (out)
[ 9] 196.200.219.102 ALLOW OUT 8080 (out)
[10] 8080 ALLOW IN 196.200.219.102
```

For instance if you want to remove any particular rule, the following command applies.

```
ufw delete 2
```

Where 2 is the status number for rule rejecting port 8080

Check the status for the firewall and you will see that rule deleted permanently.

```
afnog@pc39:~$ sudo ufw delete 2
Deleting:
  reject 8080
Proceed with operation (y|n)? y
Rule deleted
```



```
afnog@pc39:~$ sudo ufw status numbered
Status: active

      To      Action      From
      --      -
[ 1] 80      ALLOW IN   Anywhere
[ 2] 8081     DENY IN   Anywhere
[ 3] 9000/udp ALLOW IN   Anywhere
[ 4] 22      DENY IN   Anywhere
[ 5] 22      DENY OUT   Anywhere (out)
[ 6] Anywhere DENY IN   196.200.219.101
[ 7] 196.200.219.101 DENY OUT Anywhere (out)
[ 8] 196.200.219.102 ALLOW OUT  8080 (out)
[ 9] 8080     ALLOW IN   196.200.219.102
```

To prevent ping to the server the following file edit can help achieve it.

Test to ensure you can first ping your server as below

```
C:\Users\franko>ping 196.200.219.139

Pinging 196.200.219.139 with 32 bytes of data:
Reply from 196.200.219.139: bytes=32 time=1ms TTL=62
Reply from 196.200.219.139: bytes=32 time=1ms TTL=62
Reply from 196.200.219.139: bytes=32 time=1ms TTL=62
Reply from 196.200.219.139: bytes=32 time=1ms TTL=62

Ping statistics for 196.200.219.139:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Vi /etc/ufw/before.rules

```
afnog@pc39:~$ sudo vi /etc/ufw/before.rules
```

You can either comment that line out or change the ACCEPT to DROP as shown below

```
# ok icmp codes
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-input -p icmp --icmp-type source-quench -j ACCEPT
-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-input -p icmp --icmp-type parameter-problem -j DROP
-A ufw-before-input -p icmp --icmp-type echo-request -j DROP
```

Please note that you need to disable and enable the ufw to let the rule work.

```
afnog@pc39:~$ sudo ufw disable
```

to disable firewall

```
afnog@pc39:~$ sudo ufw enable
```

to enable firewall

If you want to remove all rules, you can issues command below.

Ufw reset

```
afnog@pc39:~$ sudo ufw reset
Resetting all rules to installed defaults. This may disrupt existing ssh
connections. Proceed with operation (y/n)? y
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20170522_083837'
Backing up 'before.rules' to '/etc/ufw/before.rules.20170522_083837'
Backing up 'user6.rules' to '/lib/ufw/user6.rules.20170522_083837'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20170522_083837'
Backing up 'after.rules' to '/etc/ufw/after.rules.20170522_083837'
Backing up 'user.rules' to '/lib/ufw/user.rules.20170522_083837'
```

