How to Configure Firewall With UFW In Kali Linux

sobanmalikk.medium.com/how-to-configure-firewall-with-ufw-in-kali-linux-14ebbf498de2

Soban Malik

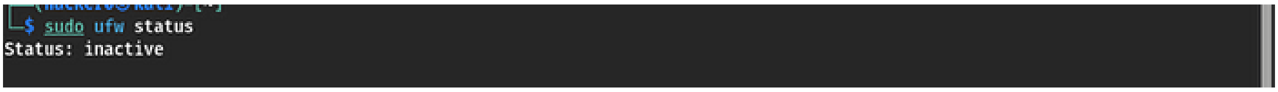
11 февраля 2024 г.

Soban Malik

UFW is an acronym for an uncomplicated firewall. Securing a network with an uncomplicated firewall is super easy and highly recommended.

Step 1 — Set Up default UFW policies

```
sudo apt update && sudo apt upgrade sudo apt-get install ufw sudo ufw status
```



```
└─$ sudo ufw status
Status: inactive
```

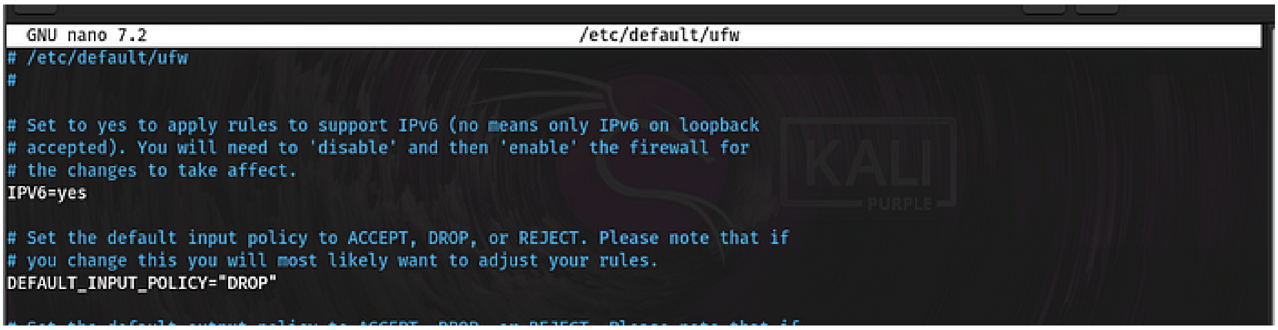
The default policy firewall works out great for both the servers and the desktop. It is always a good policy to close all ports on the server and open only the required ports one by one. Let us block all incoming connections and only allow outgoing connections

```
sudo ufw default allow outgoingsudo ufw default deny incoming
```

Enabling IPv6 support

Make sure the directive IPV6=yes: exists in the**/etc/default/ufw** file. For instance:

```
sudo nano /etc/default/ufw
```



```
  GNU nano 7.2                          /etc/default/ufw
# /etc/default/ufw
#

# Set to yes to apply rules to support IPv6 (no means only IPv6 on loopback
# accepted). You will need to 'disable' and then 'enable' the firewall for
# the changes to take affect.
IPV6=yes

# Set the default input policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_INPUT_POLICY="DROP"

# Set the default output policy to ACCEPT, DROP, or REJECT. Please note that if
```

Step 2 — Open SSH TCP port 22 connections:

The next logical step is to allow incoming SSH ports.OpenSSH provides TCP port forwarding, also known as tunneling, which allows other TCP applications to forward their network data over a secure SSH connection. We can easily open SSH TCP port 22 using UFW as follows

```
sudo ufw allow ssh
```

People like to move this port away to lower the number of attacks on the SSH port. you are running SSH on TCP port 2222 or TCP port 2323, enter:

```
sudo ufw allow 2222/tcpsudo ufw allow 2323/tcp
```

Some sysadmins have a static IP address (such as 202.54.2.5) at home or office locations. In that case, only allow SSH access from the static IP address such as 202.54.2.5 to the Kali Linux server IP address (such as 172.24.13.45):

```
ifconfig  sudo ufw allow proto tcp from 202.54.2.5 to 172.24.13.45 port 22
```

Next, let us limit the ssh port, run:

```
sudo ufw  ssh
```

You can add a limit rule. If only IPv4 (Internet Protocol version 4) is supported. With this syntax, you can deny connections from an IP address that has attempted to initiate 6 or more connections in the last 30 seconds. This option is very useful for services such as sshd(Secure Shell Daemon application (SSH daemon or sshd))as those are attacked by bots and other bad actors. Hence, we use a firewall to protect our server from brute-force attacks.

```
## ufw limit ssh various usage ##
ufw limit ssh



ufw limit ssh/tcp



ufw limit ssh comment 'Rate limit for openssh server'
```

```
 ufw  2022/tcp comment
```

Limiting SSH with UFW and other protocols

```
ufw  {service}ufw  25/tcpufw  httpufwufw  https
```

Step 3 — Turn on the firewall

```
sudo ufw
```

Remember, once UFW is enabled, it runs across system reboots too. We can verify that easily as follows using the systemctl command:

```
sudo systemctl status ufw.service
```

If you need to stop the firewall and **disable** on system startup, enter:

```
sudo ufw
```

Step 4 — Open specific incoming connections/ports

Let us add more rules. Say you want to open ports and allow IP address with ufw.

```
sudo ufw allow 80/tcp comment sudo ufw allow 443/tcp comment sudo ufw allow
1194/udp comment
```

We can allow port ranges to say, TCP and udp 2000to 3000

```
sudo ufw allow 2000:3000/tcpsudo ufw allow 2000:3000/udp
```

If u want to allow all connections from this IP address like(192.168.4.4)

```
sudo ufw allow from 192.168.4.4
```

Or to specify to allow IP address from this port

```
sudo ufw allow from 192.168.4.4 to any port 25 proto tcp
```

We can set destination IP 192.168.254.254 for port 25 too:

```
sudo ufw allow from 192.168.4.4to 192.168.254.254 port 25 proto tcp
```

Step 5 — Block and deny incoming connections/ports

Do you want to close ports and block certain IP addresses? The syntax is as follows to deny access. In other words, simply ignoring access to port 23:

```
sudo ufw deny 25/tcp
```

If you deny all connections from an IP/Subnet address called 192.1687.4.7/60enter:

```
sudo ufw deny from 192.1687.4.7/60
```

Step 6 — Verify the status of UFW

Use the status command as follows:

```
sudo ufw status



OR

sudo ufw status numbered
```

If u deleted the Rule:

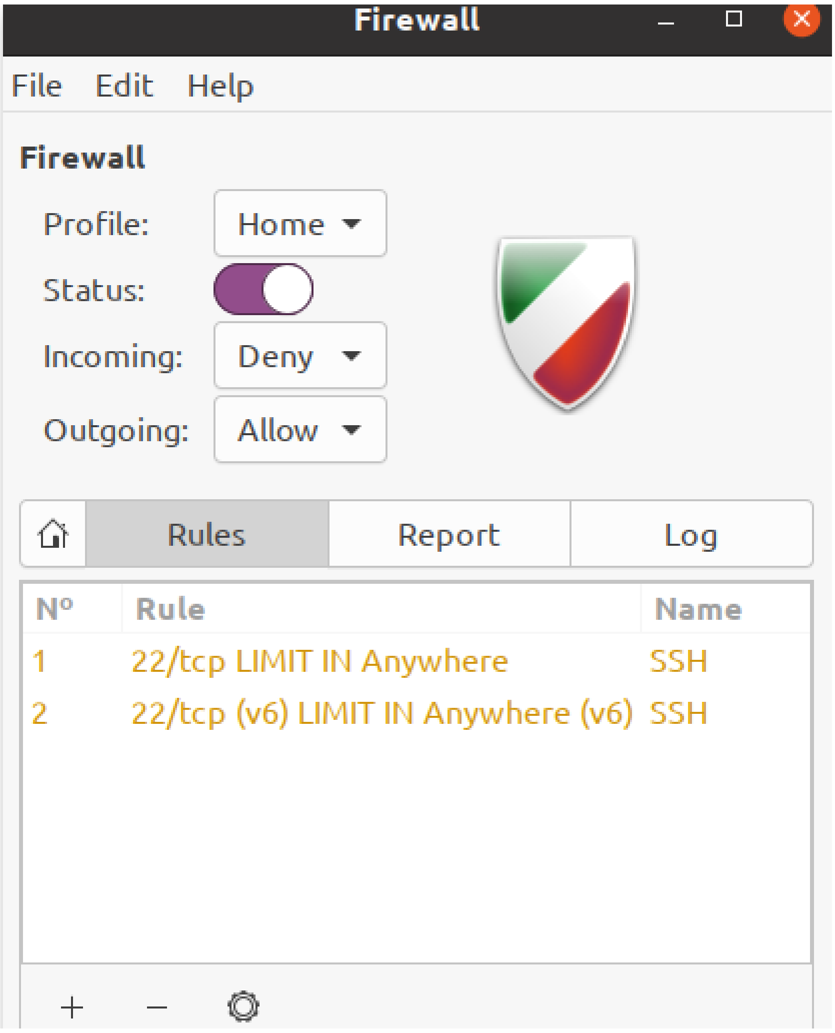
```
sudo ufw delete 6
```

Helpful Command for TroubleShooting

```
sudo ufw reset
OR



sudo ufw reload



#view log of the firewall

sudo more /var/log/ufw.logsudo  -f /var/log/ufw.log
```

If you want to install the **GUI version of UFW** then:

```
sudo apt- install gufw
```



Firewall

Profile: Home

Status:

Incoming: Deny

Outgoing: Allow

Nº	Rule	Name
1	22/tcp LIMIT IN Anywhere	SSH
2	22/tcp (v6) LIMIT IN Anywhere (v6)	SSH

Conclusion

In this quick tutorial, you learn how to secure your Kali Linux server or desktop with the help of UFW. Remember, while UFW provides essential firewall protection, it’s crucial to regularly review and update your firewall rules to adapt to changing security requirements.