

Build and Configure a Firewall

Step 1: Install UFW (Uncomplicated Firewall)

```
dsalgado@kali: ~  
File Actions Edit View Help  
(dsalgado@kali)-[~]  
$ sudo apt install ufw  
[sudo] password for dsalgado:  
The following packages were automatically installed and are no longer required:  
libbftio1 libgles-dev libpaper1  
libc++1-19 libgles1 libsuperlu6  
libc++abi1-19 libglvnd-core-dev libunwind-19  
libegl-dev libglvnd-dev openjdk-23-jre  
libfmt9 libjxl0.9 openjdk-23-jre-headless  
libgl1-mesa-dev libmbc7t64 python3-appdirs  
Use 'sudo apt autoremove' to remove them.  
  
Installing:  
ufw  
  
Suggested packages:  
rsyslog  
  
Summary:  
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 20  
Download size: 169 kB  
Space needed: 880 kB / 8,006 MB available  
  
Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-8 [169 kB]  
Fetched 169 kB in 0s (556 kB/s)
```

2: Enable UFW (By default it comes disabled)

```
dsalgado@kali: ~  
File Actions Edit View Help  
  
Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-8 [169 kB]  
Fetched 169 kB in 0s (556 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package ufw.  
(Reading database ... 407507 files and directories currently installed.)  
Preparing to unpack .../archives/ufw_0.36.2-8_all.deb ...  
Unpacking ufw (0.36.2-8) ...  
Setting up ufw (0.36.2-8) ...  
Creating config file /etc/ufw/before.rules with new version  
Creating config file /etc/ufw/before6.rules with new version  
Creating config file /etc/ufw/after.rules with new version  
Creating config file /etc/ufw/after6.rules with new version  
update-rc.d: We have no instructions for the ufw init script.  
update-rc.d: It looks like a non-network service, we enable it.  
Created symlink '/etc/systemd/system/multi-user.target.wants/ufw.service' -> '/usr/lib/systemd/system/ufw.service'.  
Processing triggers for kali-menu (2024.4.0) ...  
Processing triggers for man-db (2.13.0-1) ...  
  
(dsalgado@kali)-[~]  
$ sudo ufw enable  
Firewall is active and enabled on system startup
```

3: Allow SSH connections

```
(dsalgado@kali)-[~]  
$ sudo ufw allow ssh  
Rule added  
Rule added (v6)
```

4: Allow service of HTTP and HTTPS

```
(dsalgado@kali)-[~]  
$ sudo ufw allow http  
Rule added  
Rule added (v6)  
  
(dsalgado@kali)-[~]  
$ sudo ufw allow https  
Rule added  
Rule added (v6)
```

5: Allow traffic only through port 8080

```
(dsalgado@kali)-[~]  
$ sudo ufw allow 8080/tcp  
Rule added  
Rule added (v6)
```

6: Allow traffic to a certain range of ports

```
(dsalgado@kali)-[~]  
$ sudo ufw allow 1000:2000/tcp  
Rule added  
Rule added (v6)
```

7: Allow a specific IP address (For example, 192.168.1.100)

```
(dsalgado@kali)-[~]  
$ sudo ufw allow from 192.168.1.100  
Rule added
```

8: Allow specific subnets

```
(dsalgado@kali)-[~]  
$ sudo ufw allow from 192.168.1.0/24  
Rule added
```

Now instead of allowing I will be denying different things

9: Deny a specific port

```
(dsalgado@kali)-[~]  
$ sudo ufw deny 23/tcp  
Rule added  
Rule added (v6)
```

10: Deny a specific IP address

```
(dsalgado@kali)-[~]  
$ sudo ufw deny from 203.0.113.0  
Rule added
```

11: View UFW status and rules

```
(dsalgado@kali)-[~]  
$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip
```

To	Action	From
--		
22/tcp	ALLOW IN	Anywhere
80/tcp	ALLOW IN	Anywhere
443	ALLOW IN	Anywhere
8080/tcp	ALLOW IN	Anywhere
1000:2000/tcp	ALLOW IN	Anywhere
Anywhere	ALLOW IN	192.168.1.100
Anywhere	ALLOW IN	192.168.1.0/24
23/tcp	DENY IN	Anywhere
Anywhere	DENY IN	203.0.113.0
22/tcp (v6)	ALLOW IN	Anywhere (v6)
80/tcp (v6)	ALLOW IN	Anywhere (v6)
443 (v6)	ALLOW IN	Anywhere (v6)
8080/tcp (v6)	ALLOW IN	Anywhere (v6)
1000:2000/tcp (v6)	ALLOW IN	Anywhere (v6)
23/tcp (v6)	DENY IN	Anywhere (v6)

12: If I want to delete and specific rule, I can number the rules by

```
(dsalgado@kali)-[~]
$ sudo ufw status numbered
Status: active
```

	To	Action	From
	--	-----	-----
[1]	22/tcp	ALLOW IN	Anywhere
[2]	80/tcp	ALLOW IN	Anywhere
[3]	443	ALLOW IN	Anywhere
[4]	8080/tcp	ALLOW IN	Anywhere
[5]	1000:2000/tcp	ALLOW IN	Anywhere
[6]	Anywhere	ALLOW IN	192.168.1.100
[7]	Anywhere	ALLOW IN	192.168.1.0/24
[8]	23/tcp	DENY IN	Anywhere
[9]	Anywhere	DENY IN	203.0.113.0
[10]	22/tcp (v6)	ALLOW IN	Anywhere (v6)
[11]	80/tcp (v6)	ALLOW IN	Anywhere (v6)
[12]	443 (v6)	ALLOW IN	Anywhere (v6)
[13]	8080/tcp (v6)	ALLOW IN	Anywhere (v6)
[14]	1000:2000/tcp (v6)	ALLOW IN	Anywhere (v6)
[15]	23/tcp (v6)	DENY IN	Anywhere (v6)

And then for example, I can erase rule #5 by

```
(dsalgado@kali)-[~]
$ sudo ufw delete 5
Deleting:
  allow 1000:2000/tcp
Proceed with operation (y|n)? y
Rule deleted
```

13: I can have advanced configurations to my firewall like for example logging by

```
(dsalgado@kali)-[~]
$ sudo ufw logging on
Logging enabled
```

14: I can set default policies too by

```
(dsalgado@kali)-[~]
$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

(dsalgado@kali)-[~]
$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
```

15: I can also check specific applications by

```
(dsalgado@kali)-[~]  
$ sudo ufw app list  
Available applications:  
AIM  
Apache  
Apache Full  
Apache Secure  
Bonjour  
CIFS  
DNS  
Deluge  
IMAP  
IMAPS  
IPP  
KTorrent  
Kerberos Admin  
Kerberos Full  
Kerberos KDC  
Kerberos Password  
LDAP  
LDAPS  
LPD  
MSN  
MSN SSL  
Mail submission  
NFS  
Nginx Full  
Nginx HTTP  
Nginx HTTPS  
Nginx QUIC  
OpenSSH  
POP3  
POP3S  
PeopleNearby  
SMTP  
SSH  
Samba  
Socks  
Telnet  
Transmission  
Transparent Proxy  
VNC  
WWW  
WWW Cache  
WWW Full  
WWW Secure  
XMPP  
Yahoo  
qBittorrent  
svnserve
```

And allow just one, for example by

```
(dsalgado@kali)-[~]  
$ sudo ufw allow 'Nginx Full'  
Rule added  
Rule added (v6)
```

Conclusion: I have successfully set up and configured a firewall using UFW. This setup will help me protect my network from unauthorized access and potential threats.