

## Firewall Rule Set Up (UFW-Linux)

### 1. Download and Install UFW

```
(admin_red@kali)-[~]  
$ sudo apt-get install ufw  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
ufw is already the newest version (0.36.1-4).  
0 upgraded, 0 newly installed, 0 to remove and 926 not upgraded.
```

### 2. Enable and check UFW Status

```
(admin_red@kali)-[~]  
$ sudo ufw enable  
Firewall is active and enabled on system startup  
  
(admin_red@kali)-[~]  
$ ufw status  
ERROR: You need to be root to run this script  
  
(admin_red@kali)-[~]  
$ sudo ufw status  
Status: active  
  
(admin_red@kali)-[~]  
$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip
```

### 3. Create Default Deny all incoming/allow outgoing rules, check to confirm

```
(admin_red@kali)-[~]  
$ sudo ufw default deny incoming  
Default incoming policy changed to 'deny'  
(be sure to update your rules accordingly)  
  
(admin_red@kali)-[~]  
$ sudo ufw default allow outgoing  
Default outgoing policy changed to 'allow'  
(be sure to update your rules accordingly)  
  
(admin_red@kali)-[~]  
$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip
```

4. Create a rule to SSH between specific IP using TCP

```
(admin_red@kali)-[~]
$ sudo ufw allow from 10.0.3.15 to any port 22 proto tcp
Rule added

(admin_red@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 10.0.3.15
```

5. Create Rules for http/https access, check/view rule list

```
(admin_red@kali)-[~]
$ sudo ufw allow 443
Rule added
Rule added (v6)

(admin_red@kali)-[~]
$ sudo ufw allow 80
Rule added
Rule added (v6)

(admin_red@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 10.0.3.15
443 ALLOW IN Anywhere
80 ALLOW IN Anywhere
443 (v6) ALLOW IN Anywhere (v6)
80 (v6) ALLOW IN Anywhere (v6)
```