

Firewall Configuration (Kali Linux)

1. Enable Firewall (ufw)

Command - `sudo ufw enable`

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

2. List Current Firewall Rules

Command - `sudo ufw status verbose`

```
(kernal@system)-[~]  
$ sudo ufw allow 22/tcp  
Rules updated  
Rules updated (v6)
```

3. Add Rule To Block Inbound Traffic on Port 23

Command - `sudo ufw deny 23/tcp`

```
(kernal@system)-[~]  
$ sudo ufw deny 23/tcp  
Rules updated  
Rules updated (v6)  
  
(kernal@system)-[~]  
$
```

4. Testing blocked port (telnet)

Command - `telnet localhost 23`

```
(kernal@system)-[~]  
$ telnet localhost 23  
Trying ::1 ...  
Connection failed: Connection refused  
Trying 127.0.0.1 ...  
telnet: Unable to connect to remote host: Connection refused
```

5. Add Rule to Allow SSH

Command - `sudo ufw allow 22/tcp`

```
(kernal@system)-[~]  
$ sudo ufw allow 22/tcp  
Rule added  
Rule added (v6)
```

6. Delete Rule (talent)

Command - `sudo ufw delete deny 23/tcp`

```
(kernal@system)-[~]  
$ sudo ufw delete deny 23/tcp  
Rule deleted  
Rule deleted (v6)
```

7. Reset Firewall

Command - `sudo ufw reset`

```
(kernal@system)-[~]  
$ sudo ufw reset  
Resetting all rules to installed defaults. Proceed with operation (y|n)? y  
Backing up 'user.rules' to '/etc/ufw/user.rules.20250926_091902'  
Backing up 'before.rules' to '/etc/ufw/before.rules.20250926_091902'  
Backing up 'after.rules' to '/etc/ufw/after.rules.20250926_091902'  
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20250926_091902'  
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20250926_091902'  
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20250926_091902'
```