

UFW Essentials: Common Firewall Rules and Commands

```
kali@kali: ~  
File Actions Edit View Help  
-(kali@kali)-[~]  
$ sudo ufw enable  
Firewall is active and enabled on system startup  
  
-(kali@kali)-[~]  
$ sudo ufw status verbose  
Status: active  
Logging: on (low)  
Default: deny (incoming), allow (outgoing), disabled (routed)  
New profiles: skip  
  
-(kali@kali)-[~]  
$ sudo ufw disable  
Firewall stopped and disabled on system startup  
  
-(kali@kali)-[~]  
$ sudo ufw deny from 203.0.113.100  
Rules updated  
  
-(kali@kali)-[~]  
$ sudo ufw status  
Status: inactive  
  
-(kali@kali)-[~]  
$ sudo ufw enable  
Firewall is active and enabled on system startup  
  
-(kali@kali)-[~]
```

```
kali@kali: ~  
File Actions Edit View Help  
Status: inactive  
-(kali@kali)-[~]  
$ sudo ufw enable  
Firewall is active and enabled on system startup  
  
-(kali@kali)-[~]  
$ sudo ufw deny from 203.0.113.100  
Skipping adding existing rule  
  
-(kali@kali)-[~]  
$ sudo ufw default deny outgoing  
Default outgoing policy changed to 'deny'  
(be sure to update your rules accordingly)  
  
-(kali@kali)-[~]  
$ sudo ufw default allow outgoing  
Default outgoing policy changed to 'allow'  
(be sure to update your rules accordingly)  
  
-(kali@kali)-[~]  
$ sudo ufw deny out from 192.168.1.100  
Rule added  
  
-(kali@kali)-[~]  
$ sudo ufw allow out from 192.168.1.100  
Rule updated
```

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~  
$ sudo ufw deny from 203.0.113.100  
Skipping adding existing rule  
kali@kali: ~  
$ sudo ufw deny from 203.0.113.0/24  
Rule added  
kali@kali: ~  
$ sudo ufw deny in on eth0 from 203.0.113.100  
Rule added  
kali@kali: ~  
$ sudo ufw allow from 203.0.113.101  
Rule added  
kali@kali: ~  
$ sudo ufw status  
Status: active  


| To               | Action | From           |
|------------------|--------|----------------|
| Anywhere         | DENY   | 203.0.113.100  |
| Anywhere         | DENY   | 203.0.113.0/24 |
| Anywhere on eth0 | DENY   | 203.0.113.100  |
| Anywhere         | ALLOW  | 203.0.113.101  |


```

```
kali@kali: ~  
File Actions Edit View Help  
Anywhere on eth0  
$ sudo ufw allow in on eth0 from 203.0.113.102  
Rule added  
kali@kali: ~  
$ sudo ufw status  
Status: active  


| To               | Action | From           |
|------------------|--------|----------------|
| Anywhere         | DENY   | 203.0.113.100  |
| Anywhere         | DENY   | 203.0.113.0/24 |
| Anywhere on eth0 | DENY   | 203.0.113.100  |
| Anywhere         | ALLOW  | 203.0.113.101  |
| Anywhere on eth0 | ALLOW  | 203.0.113.102  |

  
Anywhere  
$ sudo ufw delete allow from 203.0.113.101  
Rule deleted  
kali@kali: ~
```

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo ufw status numbered  
Status: active  


|       | To               | Action    | From                |
|-------|------------------|-----------|---------------------|
| [ 1 ] | Anywhere         | DENY IN   | 203.0.113.100       |
| [ 2 ] | Anywhere         | ALLOW OUT | 192.168.1.100 (out) |
| [ 3 ] | Anywhere         | DENY IN   | 203.0.113.0/24      |
| [ 4 ] | Anywhere on eth0 | DENY IN   | 203.0.113.100       |
| [ 5 ] | Anywhere on eth0 | ALLOW IN  | 203.0.113.102       |

  
(kali@kali)-[~]  
$ sudo ufw delete 1  
Deleting:  
deny from 203.0.113.100  
Proceed with operation (y/n)? y  
Rule deleted  
  
(kali@kali)-[~]  
$ sudo ufw app list  
Available applications:  
AIM  
Bonjour  
CIFS  
DNS  
Deluge
```

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo ufw status numbered  
Status: active  


|       | To               | Action    | From                |
|-------|------------------|-----------|---------------------|
| [ 1 ] | Anywhere         | DENY IN   | 203.0.113.100       |
| [ 2 ] | Anywhere         | ALLOW OUT | 192.168.1.100 (out) |
| [ 3 ] | Anywhere         | DENY IN   | 203.0.113.0/24      |
| [ 4 ] | Anywhere on eth0 | DENY IN   | 203.0.113.100       |
| [ 5 ] | Anywhere on eth0 | ALLOW IN  | 203.0.113.102       |

  
(kali@kali)-[~]  
$ sudo ufw delete 1  
Deleting:  
deny from 203.0.113.100  
Proceed with operation (y/n)? y  
Rule deleted  
  
(kali@kali)-[~]  
$ sudo ufw app list  
Available applications:  
AIM  
Bonjour  
CIFS  
DNS  
Deluge
```

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ sudo ufw allow "OpenSSH"  
ERROR: Bad port  
[kali@kali]~  
$ sudo ufw allow "CIFS"  
ERROR: Bad port  
[kali@kali]~  
$ sudo ufw allow "AIM"  
ERROR: Bad port  
[kali@kali]~  
$ sudo ufw status  
Status: active  


| To               | Action    | From           |
|------------------|-----------|----------------|
| Anywhere         | DENY      | 203.0.113.0/24 |
| Anywhere on eth0 | DENY      | 203.0.113.100  |
| Anywhere on eth0 | ALLOW     | 203.0.113.102  |
| Anywhere         | ALLOW OUT | 192.168.1.100  |


```

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ sudo ufw allow OpenSSH  
Rule added  
Rule added (v6)  
[kali@kali]~  
$ sudo ufw allow 22  
Rule added  
Rule added (v6)  
[kali@kali]~  
$ sudo ufw allow from 203.0.113.103 proto tcp to any port 22  
Rule added  
[kali@kali]~  
$ sudo ufw allow from 203.0.113.0/24 proto tcp to any port 22  
Rule added  
[kali@kali]~  
$ sudo ufw allow from 203.0.113.103 to any port 873  
Rule added  
[kali@kali]~  
$ sudo ufw allow from 203.0.113.0/24 to any port 873  
Rule added
```

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo ufw allow from 203.0.113.0/24 to any port 873 -oNginx
Rule added

(kali@kali)-[~]
$ sudo ufw app list | grep Nginx
Nginx Full
Nginx HTTP
Nginx HTTPS

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

(kali@kali)-[~]
$ sudo ufw app list | grep Apache

(kali@kali)-[~]
$ sudo ufw app list | grep Apache

(kali@kali)-[~]
$ sudo ufw allow "Nginx Full"
Skipping adding existing rule
Skipping adding existing rule (v6)
```

```
File Actions Edit View Help
Skipping adding existing rule (v6)
(kali@kali)-[~]
$ sudo ufw allow http
Rule added
Rule added (v6)

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

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

(kali@kali)-[~]
$ sudo ufw allow 443
Skipping adding existing rule
Skipping adding existing rule (v6)

(kali@kali)-[~]
$ sudo ufw allow proto tcp from any to any port 80,443
Rule added
Rule added (v6)
```

```
kali@kali: ~  
File Actions Edit View Help  
Rule added  
Rule added (v6) Inter → Exploit-DB → Google Hacking DB → ONSec  
  
(kali@kali)-[~]  
$ sudo ufw allow from 203.0.113.103 to any port 3306  
Rule added ok  
  
(kali@kali)-[~]  
$ sudo ufw allow from 203.0.113.0/24 to any port 3306  
Rule added  
  
(kali@kali)-[~]  
$ sudo ufw allow from 203.0.113.103 to any port 5432  
Rule added  
  
(kali@kali)-[~]  
$ sudo ufw allow from 203.0.113.0/24 to any port 5432  
Rule added  
  
(kali@kali)-[~]  
$ sudo ufw deny out 25  
Rule added  
Rule added (v6)  
  
(kali@kali)-[~]  
$
```