

UFW Commando's

UFW staat voor Uncomplicated FireWall en is de standaard firewall van Ubuntu. Eigenlijk is het een front-end om de standaard firewall configuratie in Linux (IPTables) te vergemakkelijken. Hier onder volgen veel gebruikte commando's en voorbeelden.

UFW inschakelen

```
ufw enable
```

UFW uitschakelen

```
ufw disable
```

Status checken

```
ufw status verbose
```

Bekijk de regels in /etc/ufw (.rules)

```
ufw show raw
```

UFW Allow syntax en voorbeelden

```
ufw allow <port>/<optional: protocol>
```

Voorbeeld: To allow incoming tcp and udp packet on port 53

```
ufw allow 53
```

Voorbeeld: To allow incoming tcp packets on port 53

```
ufw allow 53/tcp
```

Voorbeeld: To allow incoming udp packets on port 53

```
ufw allow 53/udp
```

UFW Deny syntax en voorbeelden

```
ufw deny <port>/<optional: protocol>
```

Voorbeeld: To deny tcp and udp packets on port 53

```
ufw deny 53
```

Voorbeeld: To deny incoming tcp packets on port 53

```
ufw deny 53/tcp
```

Voorbeeld: To deny incoming udp packets on port 53

```
ufw deny 53/udp
```

Bestaande regels verwijderen

To delete a rule, simply prefix the original rule with delete. For example, if the original rule was:

```
ufw deny 80/tcp
```

Use this to delete it:

```
ufw delete deny 80/tcp
```

Port ranges

For port ranges you can use the colon (:) to separate the lowest and the highest port in the range.

For example:

```
ufw allow 10000:15000/udp
```

```
ufw deny 8000:8100/tcp
```

Comments

Example: Open port 53 and write a comment about rule too

```
ufw allow 53 comment 'open tcp and udp port 53 for dns'
```

UFW services

You can also allow or deny by service name since ufw reads from /etc/services

To see get a list of services:

```
less /etc/services
```

Allow by Service Name

```
ufw allow <service name>
```

Voorbeeld: to allow ssh by name

```
ufw allow ssh
```

Deny by Service Name

```
ufw deny <service name>
```

Voorbeeld: to deny ssh by name

```
ufw deny ssh
```

UFW Logging

To enable logging use:

```
ufw logging on
```

To disable logging use:

```
ufw logging off
```

UFW Advanced Syntax: Allow

Allow by Specific IP:

```
ufw allow from <ip address>
```

Voorbeeld: To allow packets from 207.46.232.182:

```
ufw allow from 207.46.232.182
```

Allow by Subnet:

You may use a net mask :

```
ufw allow from 192.168.1.0/24
```

Allow by specific port and IP address:

```
ufw allow from <target> to <destination> port <port number>
```

Voorbeeld: allow IP address 192.168.0.4 access to port 22 for all protocols

```
ufw allow from 192.168.0.4 to any port 22
```

Allow by specific port, IP address and protocol:

```
ufw allow from <target> to <destination> port <port number> proto <protocol name>
```

Voorbeeld: allow IP address 192.168.0.4 access to port 22 using TCP

```
ufw allow from 192.168.0.4 to any port 22 proto tcp
```

UFW Advanced Syntax: Deny

Deny by specific IP:

```
ufw deny from <ip address>
```

Voorbeeld: To block packets from 207.46.232.182:

```
ufw deny from 207.46.232.182
```

Deny by specific port and IP address:

```
ufw deny from <ip address> to <protocol> port <port number>
```

Voorbeeld: deny ip address 192.168.0.1 access to port 22 for all protocols

```
ufw deny from 192.168.0.1 to any port 22
```

Advanced Example

Scenario: You want to block access to port 22 from 192.168.0.1 and 192.168.0.7

but allow all other 192.168.0.x IPs to have access to port 22 using tcp

```
ufw deny from 192.168.0.1 to any port 22
```

```
ufw deny from 192.168.0.7 to any port 22
```

```
ufw allow from 192.168.0.0/24 to any port 22 proto tcp
```

Laat de regels zien met een regelnummer

```
ufw status numbered
```

Regels verwijderen of tussenvoegen op basis van regelnummers

You may then delete rules using the number.

This will delete the first rule and rules will shift up to fill in the list:

```
ufw delete 1
```

Insert numbered rule:

```
ufw insert 1 allow from <ip address>
```

Enable Ping

Note: Security by obscurity may be of very little actual benefit with modern cracker scripts.

By default, UFW allows ping requests. You may find you wish to leave (icmp) ping requests enabled to diagnose networking problems.

In order to disable ping (icmp) requests, you need to edit `/etc/ufw/before.rules` and remove the following lines:

```
# ok icmp codes
```

```
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT
```

```
-A ufw-before-input -p icmp --icmp-type source-quench -j ACCEPT
```

```
-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
```

```
-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT
```

```
-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT
```

or change the "ACCEPT" to "DROP"

```
# ok icmp codes
```

```
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j DROP
```

```
-A ufw-before-input -p icmp --icmp-type source-quench -j DROP
```

```
-A ufw-before-input -p icmp --icmp-type time-exceeded -j DROP
```

```
-A ufw-before-input -p icmp --icmp-type parameter-problem -j DROP
```

```
-A ufw-before-input -p icmp --icmp-type echo-request -j DROP
```

Reload UFW

When you edit UFW configuration files, you need to run reload command.

For example, you can edit `/etc/ufw/before.rules`, enter:

```
nano /etc/ufw/before.rules
```

After saving the changes reload UFW with:

ufw reload

Resetting UFW to defaults and make inactive

ufw reset

Bron:

<https://help.ubuntu.com/community/UFW>

Revision #2

Created 12 September 2023 13:25:27 by Alex

Updated 12 September 2023 15:47:25 by Alex