

UFW - Basic Setup

1. Installation and Configuration

First, install UFW

```
sudo apt -y install ufw
```

Before enabling the setup, we will set up some basic rules. I will deny all outgoing, as well as all incoming traffic as a default. After that we have to make sure, that we enable all the necessary protocols to communicate, otherwise, basic services, like DNS resolution no longer work. UFW is basically just a script, that generates IP-Table entries for you.

Disable all outgoing and incoming traffic:

```
sudo ufw default deny incoming
sudo ufw default deny outgoing
```

Now enable logging

```
sudo ufw logging FULL
```

Next, you have to decide, which outgoing traffic to allow. Here is an overview of **some** services, and which default ports and protocols they use. This overview is only for **OUTGOING** traffic.

Service	Port	Protocol
SMTP	25	tcp/udp
SMTPs	465	tcp/udp
DNS	53	tcp/udp
HTTP	80	tcp (UDP usually not needed)
HTTPS	443	tcp (UDP usually not needed)

You can enable outgoing traffic like this:

```
sudo ufw allow out PORT/Protocol
```

So to enable DNS, run

```
sudo ufw allow out 53
```

To enable ICMP, you'll have to edit the IP-Tables yourself, since UFW doesn't offer you this feature. Just add the following lines to `/etc/ufw/before.rules` and `/etc/ufw/before6.rules`

```
-A ufw-before-output -p icmp -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
-A ufw-before-output -p icmp -m state --state ESTABLISHED,RELATED -j ACCEPT
```

After that, you can enable incoming traffic. On a freshly installed system, that's usually just SSH, but if you are running, e.g. a webserver, you should also enable traffic on Ports 80 and 443. UFW comes with an App-List, which makes adding UFW rules for default ports easier. You can view the list by running

```
sudo ufw app list
```

Allow incoming traffic like this:

```
sudo ufw allow in Port/Protocol
```

If you want to allow a range of ports, you can use `PORTX:PORTY`. If you want only a certain host to be able to connect to your client via some Port, you can use the following rule:

```
sudo ufw allow in from 10.10.10.10 to any port 22
```

You can also use netmasks in CIDR format

You can do much more. I recommend you to read through this [manpage](#).

Lastly, to enable UFW, run

```
sudo ufw enable
```

2. Tips and Tricks

To quickly delete all rules for a port, you can use the following script:

```
#!/bin/bash
for NUM in $(ufw status numbered | grep "$1" | awk -F"[][]" '{print $2}' | tr --delete
[:blank:] | sort -rn); do
```

```
ufw --force delete "$NUM"  
done
```

This will instantly delete all rules for the specified ports, without any prompts.

You can simply delete all rules for e.g. Port 80, by running.

```
sudo ./your-script-name.sh 80
```

Revision #2

Created 24 November 2024 18:16:35 by Nicolas

Updated 13 February 2025 22:16:34 by Nicolas