ufw 0.36 Cheatsheet (ingenieriainformatica.uniovi.es)

Tool to ease Ubuntu firewall management

https://launchpad.net/ufw

```
root@ssi18base:/etc/wireguard# ufw status
Status: active

To                         Action      From
--                         ------      ----
80/tcp                     ALLOW       Anywhere
443/tcp                    ALLOW       Anywhere
23/tcp                     ALLOW       Anywhere
```

GENERAL USAGE

ufw COMMAND

NOTES

ufw is not enabled by default in a typical Ubuntu installation

To use it you need to enable it first with: sudo ufw enable

It can be disabled at any time with: sudo ufw disable

OPTIONS

allow ARGS: add allow rule

default ARG: set default policy

delete RULE|NUM: delete RULE

deny ARGS: add deny rule

disable: disables the firewall

enable: enables the firewall

insert NUM RULE: insert RULE at NUM

limit ARGS: add limit rule

logging LEVEL: set logging to LEVEL

reject ARGS: add reject rule

reload: reload firewall

reset: reset firewall

route delete RULE|NUM: delete route RULE

route insert NUM RULE: insert route RULE at NUM

route RULE: add route RULE

show ARG: show firewall report

status numbered: show firewall status as numbered list of RULES

status verbose: show verbose firewall status

status: show firewall status

version: display version information

Application profile commands

app default ARG: set default application policy

app info PROFILE: show information on PROFILE

app list: list application profiles

app update PROFILE: update PROFILE

EXAMPLES

NOTE: All examples requires soor privileges (sudo)

DEFAULT BEHAVIOR POLICIES:

* **Deny all incoming traffic by default:** ufw default deny incoming
* **Allow all outgoing traffic by default**: ufw default allow outgoing

ALLOW SERVICES:

* **sudo ufw allow 22** (or ufw allow ssh)
* **ufw allow 'Apache Full'** *(there are application profiles available:* **sudo ufw app list**)
* **ufw allow 45/tcp** *(allow port and protocol)*
* **ufw allow from 192.168.1.1 port 62** *(Source and Destination (allow only from this IP))*
* **ufw allow to 127.0.0.2 port 62** *(allow from anywhere to a local interface only)*
* **ufw allow 80/tcp comment 'accept Apache'** *(comment a rule)*
* **ufw allow 1194/udp comment 'OpenVPN server'** *(Open UDP/1194 (OpenVPN) server and add a comment)*
* **ufw allow 3000:4000/tcp, sudo ufw allow 3000:4000/udp** *(allow port ranges; tcp and udp 3000 to 4000)*
* **sudo ufw allow from 156.35.94.10** *(allow ALL connections from 156.35.94.10)*
* **sudo ufw allow from 156.35.94.10 to any port 22 proto tcp** *(allow connections from 156.35.94.10 only to port 22)*
* **sudo ufw allow from 156.35.94.10 to 156.35.94.50 port 22 proto tcp** *(set destination IP too)*
* **sudo ufw allow in on wg0 to any port 22** *(open port 22 for wg0 interface only)*
* **ufw allow in on lxdbr0 from 10.100.12.29 to any port 3389 proto tcp** *(allow connection for TCP port 3389 on lxdbr0 interface from 10.100.12.29)*
* **ufw allow in on lxdbr0 from 10.100.12.0/24 to any port 3389 proto tcp** *(same as previous but allow whole network)*

DENY SERVICES:

* **ufw deny 21**
* **sudo ufw deny 25/tcp** *(deny port and protocol)*
* **sudo ufw deny from 156.35.94.10** *(deny from specific IP)*
* **sudo ufw deny from 156.35.0.0/16** *(deny from specific network, all hosts from the network)*
* **sudo ufw deny from 156.35.94.10 to any port 22 proto tcp** *(deny access only on port 22)*

ENABLE SPECIFIC PROTOCOLS:

* **ufw allow to 127.0.0.3 proto esp**
* **ufw allow to 127.0.0.3 proto ah**

To enable IPv6 support, edit /etc/default/ufw and ensure **IPV6=yes**

ENABLE CONNECTION LIMITS:

Allow connections but deny them if an IP attempts 6 or more connections within thirty seconds. I. e.: **sudo ufw limit ssh**

ROUTES (IP Masquerading with ufw):

Edit the /etc/ufw/sysctl.conf and make sure you have the following line not commented: **net/ipv4/ip_forward=1**

* **ufw route allow in on eth0 out on eth1 to any port 80 from any** *(forward all network requests running on eth1, port 80 to eth0)*

Apply both for incoming and outgoing traffic (bidirectional):

* **ufw route allow in on eth0 out on eth1 to 10.0.0.0/8 port 80 from 192.168.0.0/16**
* **ufw route allow in on eth1 out on eth0 from 10.0.0.0/8 to 192.168.0.0/16**

EGRESS FILTERING:

Block RFC1918 addresses (private IPs) going out of eth0 interfaces on your VM connected to the Internet.

* **ufw route reject out on eth0 to 10.0.0.0/8 comment 'RFC1918 reject'**
* **ufw route reject out on eth0 to 172.16.0.0/12 comment 'RFC1918 reject'**
* **ufw route reject out on eth0 to 192.168.0.0/16 comment 'RFC1918 reject'**

LOGGING:

* sudo ufw logging on (enable log)
* sudo ufw logging medium (log verbosity)

By default all UFW entries are logged into the /var/log/ufw.log file

RULE LIST:

* **ufw show listening**
* **ufw show added**

by José Manuel Redondo López