brabeum.com

UFW Cheat Sheet – Brabeum

6-8 minutes

Since the introduction by Ubuntu of UFW (Uncomplicated FireWall) back in 2008 it has been my tool of choice for simple firewall configuration. Whilst it may lack the depth and sophistication of an enterprise level product, its simplicity makes it straight-forward and quick to secure servers in simple use-cases.

Scenario

You have a newly spun up server/vps without any other local firewall products install. You want to install UFW and allow access to some common ports. For some time now, UFW also has ipv6 enabled out of the box.

Basic Usage

Installation

If you are using Ubuntu then UFW will be installed by default. If you are using Debian or a derivative, then you can install UFW by entering the following

```
root@host:~# apt-get install ufw
```

UFW is not available in CentOS, and although you can install it from source, that is outside the scope of this tutorial.

Checking status

When you check the status, UFW will either tell you that it is inactive,

```
root@host:~# ufw status
 Status: inactive
```

or it will tell you it is active and list the firewall rules.

```
root@host:~# ufw status
 Status: active
 To                           Action      From
 --                           ------      ----
 22/tcp                       ALLOW       Anywhere
 22/tcp (v6)                  ALLOW       Anywhere
(v6)
```

Rules can also be numbered, which is particularly useful when you wish to delete one.

```
root@host:~# ufw status numbered
 Status: active
  To                           Action      From  --
------      ----
 [ 1] WWW Full                     ALLOW IN
Anywhere
 [ 2] WWW Full (v6)                ALLOW IN
Anywhere (v6)
```

Not that if you have no rules enables, you will just be told it is active

```
root@host:~# ufw status
 Status: active
```

Enable and disable

Enabling and disabling are from the following commands. **Warning**; if you are working on a remote system, allow the SSH rule **before** you enable UFW or you risk losing your shell access.

```
root@host:~# ufw enable
 Firewall is active and enabled on system startup
```

```
root@host:~# ufw disable
 Firewall stopped and disabled on system startup
```

Deleting rules

The easiest way to delete a rule is to delete it by number, but you can also delete it by definition.

```
sroot@host:~# ufw status numbered
 Status: active
  To                           Action      From  --
------      ----
 [ 1] 22/tcp                       ALLOW IN
Anywhere
 [ 2] 22/tcp (v6)                  ALLOW IN
Anywhere (v6)
```

Note that as there are 2 rules (ipv4 and ipv6) for every pre-defined service, delete will only remove the rule for one protocol.

```
root@host:~# ufw delete 2
 Deleting:
  allow 22/tcp
 Proceed with operation (y|n)? y
 Rule deleted (v6)
```

Logging

Logging is on by default, but can rapidly fill your log files with noise. Enable and disable thusly

```
root@host:~# ufw logging on
 Logging enabled
```

```
root@host:~# ufw logging off
 Logging disabled
```

You can also change the logging levels if necessary, but `low` is the default.

```
root@host:~# ufw logging medium
 Logging enabled
```

Pre-defined rules

One of the strengths for sysadmins who may only infrequently change firewall rules is the set of pre-defined rules that UFW ships with. These obviously assume that you are running services on default ports and will NOT work if you have tried to obfuscate by assigning non-default ports. They also assume you will be allowing ALL traffic to these port (see later for how to restrict traffic sources and destinations.

```
root@host:~# ufw app list
 Available applications:
   AIM
   Bonjour
   CIFS
   CUPS
   DNS
```

```
Deluge
IMAP
IMAPS
IPP
KTorrent
Kerberos Admin
Kerberos Full
Kerberos KDC
Kerberos Password
LDAP
LDAPS
LPD
MSN
MSN SSL
Mail submission
NFS
POP3
POP3S
PeopleNearby
SMTP
SSH
Socks
Telnet
Transmission
Transparent Proxy
VNC
WWW
WWW Cache
WWW Full
WWW Secure
```

```
   XMPP
   Yahoo
   qBittorrent
   svnserve
```

You can see a full list of these and their definitions in `/etc/ufw/applications.d`.

SSH

If you are running a remote server, you almost certainly want this rule enabled.

```
 root@host:~# ufw allow ssh
 Rule added
 Rule added (v6)
```

```
root@host:~# ufw status
 Status: active
 To                         Action      From
 --                         ------      ----
 22/tcp                     ALLOW       Anywhere
 22/tcp (v6)                ALLOW       Anywhere
(v6)
```

http(s)

You can enable both port 80 (http) and 443 (https) in one go with the following command, but there are options to only enable one

```
root@host:~# ufw allow www\ full
 Rules updated
 Rules updated (v6)
```

```
root@host:~# ufw status
 [sudo] password for simon:
 Status: active
 To                           Action      From
 --                           ------      ----
 WWW Full                     ALLOW       Anywhere
 WWW Full (v6)                ALLOW       Anywhere
(v6)
```

More complex usage

Port and protocol

```
root@host:~# ufw allow 45/tcp
 Rule added
 Rule added (v6)
```

Source and Destination

Allow only from an IP

```
root@host:~# ufw allow from 192.168.1.1 port 62
 Rule added
```

```
root@host:~# ufw status
 Status: active
 To                           Action      From
 --                           ------      ----
 Anywhere                     ALLOW
192.168.1.1 62
```

Allow only to a certain local interface

```
root@host:~# ufw allow to 127.0.0.2 port 62
```

```
 Rule added
root@host:~# ufw status
 Status: active
 To                         Action      From
 --                         ------      ----
 127.0.0.2 62               ALLOW       Anywhere
```

Protocol only

If you have followed my ipsec tutorial, you will need the firewall ports open to establish the key exchange – this is one of the few protolcols which do not require a port number.

```
root@host:~# ufw allow to 127.0.0.3 proto esp
 Rule added

root@host:~# ufw allow to 127.0.0.3 proto ah
 Rule added
root@host:~# ufw status
 Status: active
 To                         Action      From
 --                         ------      ----
 127.0.0.3/esp              ALLOW       Anywhere
 127.0.0.3/ah               ALLOW       Anywhere
```

But note that you need a destination in this instance.