Uncomplicated Firewall

manera alternativa de montar reglas de acceso con una sintáxis más sencilla, monta tablas y cadenas a su antojo

sintaxis y argumentos

```
ufw [--dry-run] [options] [rule syntax]
```

- options:
  - allow
  - deny
  - reject
  - limit: bloquea el acceso después de 6 intentos de conexión en 30 segundos (sospechas)
  - status: displays if the firewall is active or inactive
  - show: displays the current running rules on your firewall
  - reset: disables and resets the firewall to default
  - reload: reloads the current running firewall
  - disable: disables the firewall

uso por defecto

- consultar:

```
grep 'DEFAULT_' /etc/default/ufw
```

- cambiar:

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

uso

- estado:

```
sudo ufw status verbose
sudo ufw status numbered
```

- reportes:

```
sudo ufw show added
sudo ufw show raw
sudo ufw show listening
sudo ufw show builtins
sudo ufw show before-rules
sudo ufw show user-rules
sudo ufw show after-rules
sudo ufw show logging-rules
```

- gestionar servicio/protocolo:

```
sudo ufw allow 22
sudo ufw deny 22
sudo ufw deny 22/tcp
sudo ufw allow ssh # /etc/services
```

- bloquear una ip+puerto a una ip específica:

```
sudo ufw deny from 192.168.2.100/8 to 192.168.2.101 port 25
```

- bloquear tráfico entrante, permitir saliente a un puerto:

```
sudo ufw allow out on eth0 to any port 25 proto tcp
sudo ufw deny in on eth0 from any 25 proto tcp
```

- eliminar una regla:

```
sudo ufw status numbered
sudo ufw delete NUM # según lista
```

- insertar una regla en una posición concreta:

```
sudo ufw insert 1 allow from 10.213.6.0/24 port ssh
```

/via: https://www.linux.com/learn/introduction-uncomplicated-firewall-ufw /via: https://www.cyberciti.biz/faq/howto-configure-setup-firewall-with-ufw-on-ubuntu-linux/

ficheros

- **/etc/default/ufw**: high level configuration, such as default policies, IPv6 support and kernel modules to use
  - `sudo sed -i s/IPV6=yes/IPV6=no/g /etc/default/ufw`
- **/etc/ufw/before[6].rules**: rules in these files are evaluated before any rules added via the ufw command
- **/etc/ufw/after[6].rules**: rules in these files are evaluated after any rules added via the ufw command
- **/etc/ufw/sysctl.conf**: kernel network tunables
- **/var/lib/ufw/user[6].rules** or **/lib/ufw/user[6].rules** (0.28 and later): rules added via the ufw command (should not normally be edited by hand)
- **/etc/ufw/ufw.conf**: sets whether or not ufw is enabled on boot, and in 9.04 (ufw 0.27) and later, sets the LOGLEVEL
- **/etc/ufw/after.init**: initialization customization script run after ufw is initialized (ufw 0.34 and later)
- **/etc/ufw/before.init**: initialization customization script run before ufw is initialized (ufw 0.34 and later)

sites

- https://www.digitalocean.com/community/tutorials/how-to-setup-a-firewall-with-ufw-on-an-ubuntu-and-debian-cloud-server
- https://wiki.ubuntu.com/UncomplicatedFirewall

ejemplos

- permitir acceso a un puerto desde un rango IP:

```
# ufw allow from 192.168.1.0/24 to 192.168.1.50 port ssh
```

- a partir de la regla de arriba (y tener el resto de puertos cerrados) ha salido este mensaje en `/var/log/syslog`:

```
Nov  8 17:28:44 macnux kernel: [10687.134802] [UFW BLOCK] IN=eth0 OUT=
MAC=01:00:5e:00:00:01:f8:8e:85:40:78:be:08:00 SRC=192.168.1.1
DST=224.0.0.1 LEN=32 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
```

- mirando por internet, se trata de multicast:
  - https://ubuntuforums.org/showthread.php?t=2195355
  - https://en.wikipedia.org/wiki/Multicast_address
- y de ahí he llegado a averiguar el rango de IPs que tiene facebook asignados: http://ipinfo.io/AS32934