Mozout

Generated on 15/11/2026 00:40

KNOWLEDGE BASE · PUBLIC DOCUMENT

Setting up the ufw firewall on Ubuntu without locking yourself out

Security & Access

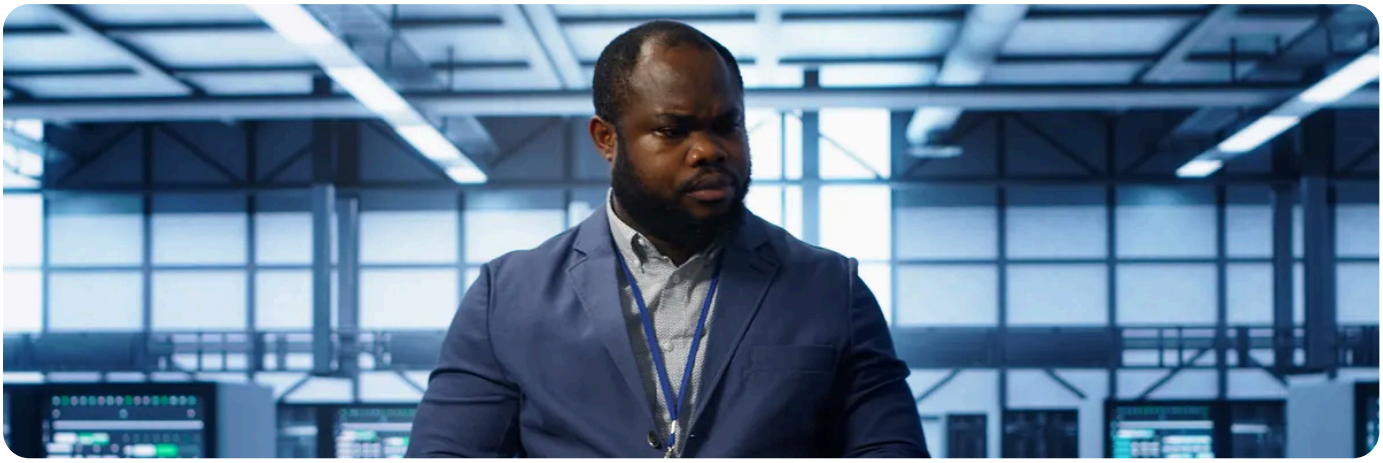
CODE	VERSION	COUNTRY · LANGUAGE
RLX-INT-KB-4182	v2026.10.10	International · English

MozOut International
RLX Holdings (Pty) Ltd. · Group RLX Holdings
Tax no. (SARS) 943 907 6234 · Registration no. (CIPC) 2025/667953/07

https://www.my.mozout.com/knowledgebase/4182

Setting up the ufw firewall on Ubuntu without locking yourself out

Security & Access Created on **October 10, 2026** 3 min read



ufw (Uncomplicated Firewall) is Ubuntu's simple firewall: it shuts everything coming in and opens only what you tell it. The golden rule fits in one line: **open the SSH port first, switch on afterwards**. Turning ufw on without that rule shuts the very door you are coming in through, and it is the number one cause of people losing access to a server (see **I have lost SSH access to my server**). The commands are yours, on your own server: support does not run them for you (see **how far our support goes**).

Step by step

1. **See whether it is installed and its state.** `sudo ufw status`. On Ubuntu it comes installed and inactive. On Debian, install it with `sudo apt install ufw`.

2. **Set the base policy:** `sudo ufw default deny incoming` and `sudo ufw default allow outgoing`. It blocks what comes in and lets through what goes out.

3. **Open SSH, before anything else:** `sudo ufw allow OpenSSH` (it assumes port 22). If your SSH uses another port, open that one: `sudo ufw allow 2222/tcp`, changing the number.

4. **Open what the server serves.** For a website: `sudo ufw allow 80/tcp` and `sudo ufw allow 443/tcp`. Only these, nothing else, unless you know what it is for.

5. **Switch it on:** `sudo ufw enable`. It will warn that it may cut the SSH connection; since you opened the port, answer `y`.

6. **Confirm in a new window, before closing the first:** `ssh user@YOUR.VPS.ADDRESS`. And look at the rules: `sudo ufw status verbose`.

Rules you will want next

I want to…	Command
Limit SSH attempts	`sudo ufw limit ssh` (it refuses an address that tries to connect too many times in a short while)
Let SSH in only from my address	`sudo ufw allow from 203.0.113.5 to any port 22 proto tcp` (the address is an example; swap in yours, and remove the more open SSH rule)
See the numbered rules	`sudo ufw status numbered`
Delete a rule	`sudo ufw delete 3` (the number from the list)
Switch the firewall off	`sudo ufw disable`
Start again from scratch	`sudo ufw reset` (deletes every rule and switches it off)

Docker ignores ufw.
A port published by a container (`-p 8080:80`) is open to the world even with no ufw rule, because Docker writes its own rules. See **ports and firewall on a VPS: why your app is not reachable**. AlmaLinux and Rocky do not use ufw but `firewalld` , explained in the same article.

If you got locked out, the panel console fixes it.
Through the console, `sudo ufw disable` switches the firewall off and lets you back in, to correct the rules at leisure. If with the port open on the server you still cannot connect, there may be another firewall outside the server, on the network: tell us and we will look from our side. See **keeping your VPS secure: the six that matter**.

NEED A HAND?

Switched the firewall on and lost access? Tell us the VPS address and the rule you were applying.

Open a support ticket →

SEE ALSO

Ports and firewall on a VPS: why your app is not reachable →

- I have lost SSH access to my server
- Installing fail2ban on a VPS to stop SSH password guessing
- Keeping your VPS or dedicated server secure: the six that matter

MozOut International

RLX Holdings (Pty) Ltd. · Group RLX Holdings

TAX NO. (SARS)	943 907 6234
REGISTRATION NO. (CIPC)	2025/667953/07
REGISTERED OFFICE	1111 Olive Street Saint Louis 63101, Missouri, United States
CONTACT	info@mozout.com · +27 78 823 3325 · www.mozout.com
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-INT-KB-4182 · v2026.10.10 · Generated on 15/11/2026 00:40