interweb

Generated on 21/10/2026 17:20

KNOWLEDGE BASE · PUBLIC DOCUMENT

Keeping your VPS or dedicated server secure: the six that matter

VPS & Servers

CODE	VERSION	COUNTRY · LANGUAGE
RLX-MZ-KB-306	v2026.09.28	Mozambique · English

Interweb Mozambique
RLX Holdings, S.A. · Group RLX Holdings
Tax ID (NUIT) 401 191 607 · Legal entity no. (NUEL) 105 045 974 · Economic activity code (CAE) 62022

https://www.meu.interweb.co.mz/knowledgebase/306

Keeping your VPS or dedicated server secure: the six that matter

VPS & Servers Created on **September 10, 2026** Updated on **September 28, 2026** 6 min read



On a shared hosting plan the machine is ours and we are the ones keeping it shut. On a VPS or dedicated server, **the machine is yours** - and with it comes the part nobody mentions on the day of purchase: keeping the door locked is your job. Exactly where the line falls is in **managed or unmanaged VPS: who does what**.

This article is the short list. It is not a systems administration course - it is the six things that, once done, prevent nearly everything we actually see happen.

1. The operating system is the decision that weighs most

A system that no longer receives security updates cannot be protected by anything else: the holes found after end of life **will never be fixed**. No firewall covers that.

> **Careful when choosing on the order form.**
> The list of available systems still includes versions that have **reached end of life** - CentOS 7, Fedora 37 and 38, Ubuntu 21.04 and 23.04, Windows Server 2008 R2 and 2012 R2. They are there for historical reasons and can still be installed; **do not choose them for a new server**. If you already run one, talk to us before reinstalling - see **reinstalling or changing your VPS operating system**.

For a new server	Choose
Linux, with cPanel/WHM	**AlmaLinux 9** or **Rocky Linux 9**. These two are the best supported by cPanel today.
Linux, without a panel	**Debian 12** or **Ubuntu 22.04 LTS**. The LTS releases are the ones with years of updates still ahead.
Windows	**Windows Server 2022**. The earlier ones no longer get fixes.

The full choice, with what each one is good for, is in **which operating system to choose for your VPS or server**.

2. The server's first two hours

A new server starts being probed by automated scanners **minutes** after it goes live. That is not an exaggeration: it is what the logs show. Do this before installing anything at all.

1. **Update everything.** On AlmaLinux or Rocky: `dnf update -y`. On Debian or Ubuntu: `apt update && apt upgrade -y`. The image a server is born from is always weeks or months behind.

2. **Change the initial password** you were given, and pick a long one. A five-word phrase beats eight characters with symbols.

3. **Create a normal user for yourself** and use it day to day, elevating to administrator only when needed. Always logging in as *root* means any mistake of yours - or of a program - has full powers.

4. **Turn the firewall on** and close everything you do not use. It is step 4 and not step 1 because closing ports on an unpatched system achieves nothing.

3. SSH is the most attacked door. Treat it accordingly

The overwhelming majority of attempts a server receives are SSH password guessing, day and night, from all over the world. Three changes in `/etc/ssh/sshd_config` end the problem:

```
PermitRootLogin no
PasswordAuthentication no
Port 2222
```

The line	What it does
PermitRootLogin no	Nobody logs in directly as *root*. You log in as yourself and elevate afterwards. Cuts half the automated attacks at a stroke.
PasswordAuthentication no	Only **keys** get you in. A key cannot be guessed - and a password, given enough time, always can.
Port 2222	Changes the port. Not real security, but it clears the scanner noise that only looks at 22 - and it leaves the logs readable.

> **Do not close the session before testing. That is the classic mistake.**
> After `systemctl restart sshd`, **leave your current session open** and open a second one to test logging in. If the new one fails, you still have the first to undo it. Closing the only session you had and only then finding the key was wrong is exactly how people lose access to a server - see **I have lost SSH access to my server**.

Get the key working before disabling passwords.
Generate the key on **your** computer with `ssh-keygen -t ed25519`, copy it over with `ssh-copy-id user@your-ip`, and only once you get in without a password do you set `PasswordAuthentication no`. In that order you can never lock yourself out.

4. Firewall: close everything, open what you use

The rule is the same on any system: deny by default and open case by case. These are the ports a web server usually needs - and no others:

Port	What for
80 and 443	The website. 443 is the encrypted one and the one that matters; 80 stays open only to redirect to it.
22 (or the one you chose)	SSH. If you can, restrict it to the address you work from.
25, 465, 587, 993	Mail. Only if the server actually handles e-mail. If it does not, leave them closed.
2087 and 2083	WHM and cPanel, if you run a panel. These are administration ports - they deserve the same care as SSH.

Add a repeated-attempt blocker - *CSF* on cPanel servers, or *fail2ban* on the others. That is what stops someone guessing passwords before they get one right. For the other side of the same coin, when *you* are the one blocked, see **why your IP gets blocked by the firewall**.

5. Backups: on a VPS they are not automatic

This is what surprises people most.
VPS plans sell the machine - processor, memory, disk and connection. They **do not include backups** the way shared hosting does. If you did not take a managed plan and did not set backups up, **there are none**. Check today, not on the day you need one - see **managed or unmanaged VPS**.

A backup only counts if it lives **off the machine**. A copy kept on the server itself disappears with it - and it disappears in exactly the two cases where it was needed: the disk failing, or somebody getting in and encrypting everything. If your plan has **JetBackup** available, confirm it is switched on and that you know how to restore.

6. Knowing how to spot that they are already in

A compromised server rarely throws an error. It carries on serving the site - while doing something else underneath. These are the signs, in order of frequency:

Sign	What it usually is
Processor at 100% for no reason	Cryptocurrency mining. It is today the most common use of a broken-into server.
The IP has landed on a blocklist	The server is firing out spam. See **your server IP on a blocklist**
New files with small-hours timestamps	Somebody left something behind. Compare against an earlier copy.
Accounts or SSH keys you did not create	The door was left open for them to come back. Check */etc/passwd* and the *authorized_keys* files.

If you suspect something, do not clean up first.
Deleting the file you found solves nothing while the way in is still open - and it destroys the evidence of how they got in. Tell us, leave the server as it is, and handle the restore from a copy predating the suspicious date.

What stays with us

The network, the physical hardware and the availability of the machine are ours. The system inside it is yours - unless you have a managed plan. That does not mean you are on your own: if you are unsure about one of these changes, ask before touching it. It is far cheaper than repairing afterwards. If the server is new, start with **first steps with your VPS**; if something is already going wrong, **common VPS and Cloud errors**.

NEED A HAND?

Want us to go through your server configuration with you?

Talk to us →

interweb

Interweb Mozambique

RLX Holdings, S.A. · Group RLX Holdings

TAX ID (NUIT)	401 191 607
LEGAL ENTITY NO. (NUEL)	105 045 974
ECONOMIC ACTIVITY CODE (CAE)	62022
REGISTERED OFFICE	Bairro 7 de Setembro Vilankulo 1304 · CEP 0411-02, Inhambane, Mozambique
CONTACT	info@interweb.co.mz · +258 84 635 1111 · +258 86 635 1111 · www.interweb.co.mz
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-MZ-KB-306 · v2026.09.28 · Generated on 21/10/2026 17:20