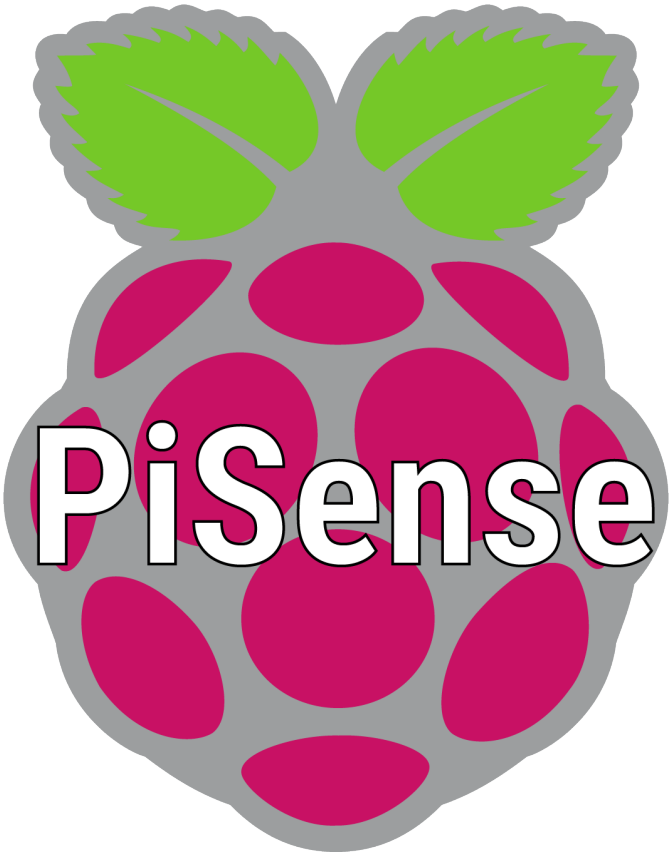
PiSense

Manual VPS security configuration

Melvin Campos Casares



26 february 2020

Manual - how to manually configure the security onto VPS

1 VPS security configuration

1.1 Create a new user

> NOTE: The root administrator is created by default on UNIX systems, he is the user who has the most rights on the system. It is not recommended, or even dangerous, to leave a VPS accessible only through this user, who can perform irreversible operations on the server.

We will therefore create a user with restricted access to perform common tasks and give administrator rights:

- `adduser user`
- Enter a secure password and press ENTER for each question to pass (or give the information asked), then validate the information with Y.
- `usermod -aG sudo user`

Commands requiring administrator rights will be preceded by the keyword `sudo` and the user's password will be requested.

1.1.1 SSH key for user connection

- `ssh-keygen -b 4096`
- It will ask for a location where to save it: `/home/user/.ssh/id_rsa`.
- It will ask for a passphrase, give it and then press ENTER.
- `ssh-copy-id user@vpsXXXX.ovh.net`
- It is also possible to perform this operation manually:

```
cat ~/.ssh/id_rsa.pub | ssh user@vpsXXXX.ovh.net "mkdir -p ~/.ssh && cat >>
↪  ~/.ssh/authorized_keys"
```

1.1.2 Connect to the VPS with the SSH key

- `ssh user@vpsXXXX.ovh.net`

On the first connection, a confirmation message will appear to add the fingerprint of the host inside the `~/.ssh/known_hosts` file.

You will have a message like this one:

```
The authenticity of host 'vpsXXXX.ovh.net (xxx.xxx.xxx.xxx)' can't be established.
ECDSA key fingerprint is SHA256:*****************************************.
Are you sure you want to continue connecting (yes/no)?
```

Simply enter `yes` and press ENTER to connect yourself. If you gave a password to your ssh account, it will be prompted.

1.1.3 Change root password

Even though we are going to block tuhe user *root* on SSH access, it's always better to change his password for security purpose.

- `passwd root`

The system will then ask to enter a new password twice to validate it. For security reasons, it will not be displayed when writing. You will therefore not be able to see the characters entered. It is very important to use a strong password.

> NOTE: A strong password is greater than 8 characters. It must combine lowercase, uppercase letters, numbers, special characters and/or accented letters. But also avoid using dictionary words, names/first names, company name, user name … The deliberate use of spelling mistakes is a good way to easily secure a password.

1.2 SSH connection (+ deactivate SSH access for root user)

It is also recommended to disable direct root user access via the SSH protocol.

To perform this operation, we first need to create a new user with granted administrator rights and copy the SSH key before modifying the SSH configuration file like below.

- `sudo vim /etc/ssh/sshd_config`
- Change or add those lines at the end of the configuration file to match with here:
- `PermitRootLogin no`
- `DenyUsers root`
- `PasswordAuthentication no`
- `/etc/init.d/ssh restart`

1.3 Fail2Ban

Fail2Ban is an intrusion prevention framework whose purpose is to block unknown IP addresses that try to enter your system. This package is recommended, even essential, to protect ourself against any attempt to brute force on our services.

> NOTE: Fail2Ban scans the logs and prohibits IP addresses which display malicious signs (too many password failures, wrong username …). In general, Fail2Ban is used to update the rules of the firewall to reject IP addresses for a specified period of time, although any other arbitrary action can also be configured. On the other hand, Fail2Ban comes with pre-configured filters for different services (Apache, NGINX, mail, FTP, SSH, etc.).

Here's what has been done with Fail2Ban:

- `sudo apt-get install fail2ban`
- `sudo vim /etc/fail2ban/jail.conf`
- ```
  # findtime is the period of examination of logs in seconds.
  # bantime is a specified time for a banned IP in seconds.
  [DEFAULT]
  ignoreip = 127.0.0.1/8 192.168.1.1/24 10.8.0.1/16
  findtime = 3600
  bantime = 86400
  ```
- `sudo vim /etc/fail2ban/jail.d/defaults-debian.conf`
- ```
  # 10 requests in 2 min -> ban for 30 minutes
  [sshd]
  enabled = true
  maxretry = 10
  findtime = 180
  bantime = 1200

  [sshd-ddos]
  enabled = true

  [recidive]
  enabled = true

  [nginx]
  enabled = true
  ```
- sudo /etc/init.d/fail2ban restart

1.4 Firewall

1.4.1 Uncomplicated Firewall (ufw)

- `sudo ufw allow {{80}}`
- `sudo ufw allow {{443}}`
- `sudo ufw allow proto {{tcp}} from {{any}} to {{any}} port {{22}}`
- `sudo ufw deny proto {{udp}} from {{any}} to {{any}} port {{22}}`
- `sudo ufw enable`

1.4.2 OVH

> Deactivated

1.5 Secure shared memory

Shared memory can be used during an attack on a running service.

In order to secure the shared memory:

- `sudo vim /etc/fstab`
- `tmpfs   /run/shm    tmpfs   defaults,noexec,nosuid  0   0`