

OPNsense

- [Installation sur proxmox](#)

Installation sur proxmox

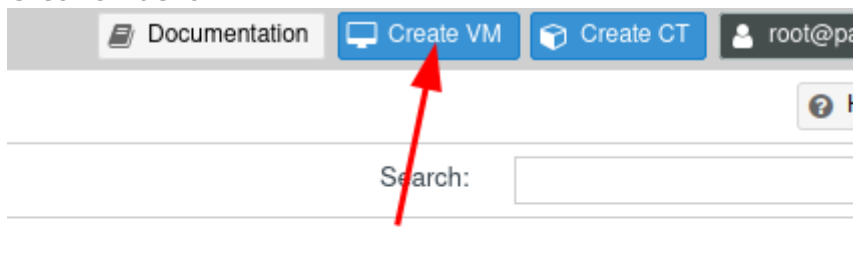
Prérequis:

- Avoir au moins deux virtual switch de créés
- Avoir l'ISO d'installation que l'on peut trouver via ce lien

<https://mirror.vraphim.com/opnsense/releases/23.1/OPNsense-23.1-OpenSSL-dvd-amd64.iso.bz2>.

Installation:

- Création de la VM.



- Nommage de la VM.

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Node: Resource Pool:

VM ID:

Name:

1

2

Help Advanced Back Next

- Sélection de l'ISO et du type de machine.

Create: Virtual Machine

General **OS** System Disks CPU Memory Network Confirm

Use CD/DVD disc image file (iso)

Storage: local

ISO image: e-23.1-OpenSSL-dvd-amd64.iso

Use physical CD/DVD Drive

Do not use any media

Guest OS:

Type: Linux


Version: 5.x - 2.6 Kernel

Advanced Back Next

- Pour la partie system laissez par défaut.
- Sélection du disque et de sa taille.

Create: Virtual Machine

General OS System **Disks** CPU Memory Network Confirm

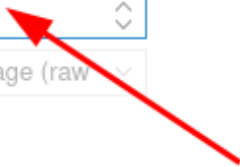
scsi0 

Disk Bandwidth


Bus/Device: SCSI 0 Cache: Default (No cache)




SCSI Controller: VirtIO SCSI single Discard:

Storage: local-lvm IO thread:

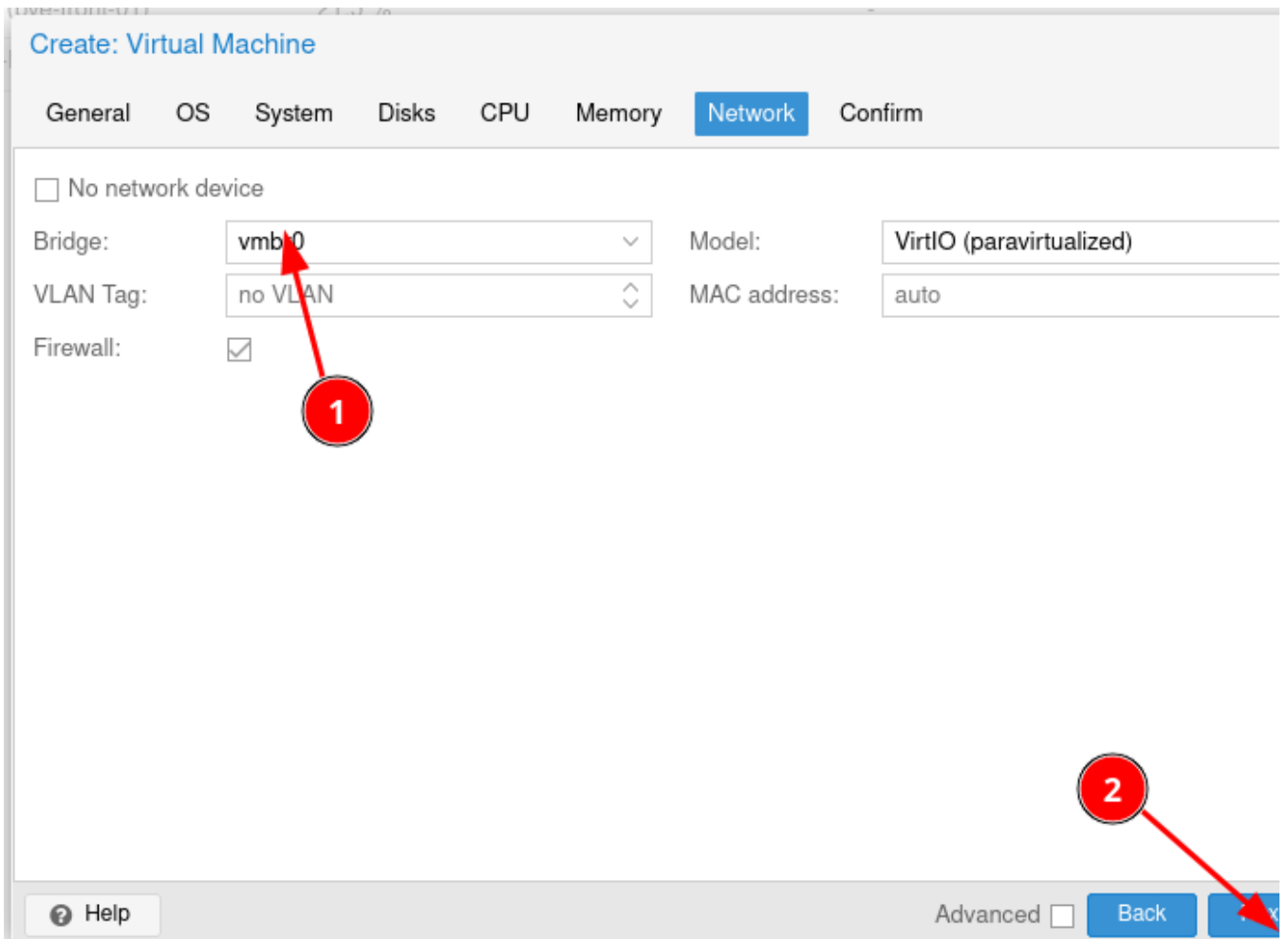
Disk size (GiB): 8 

Format: Raw disk image (raw)

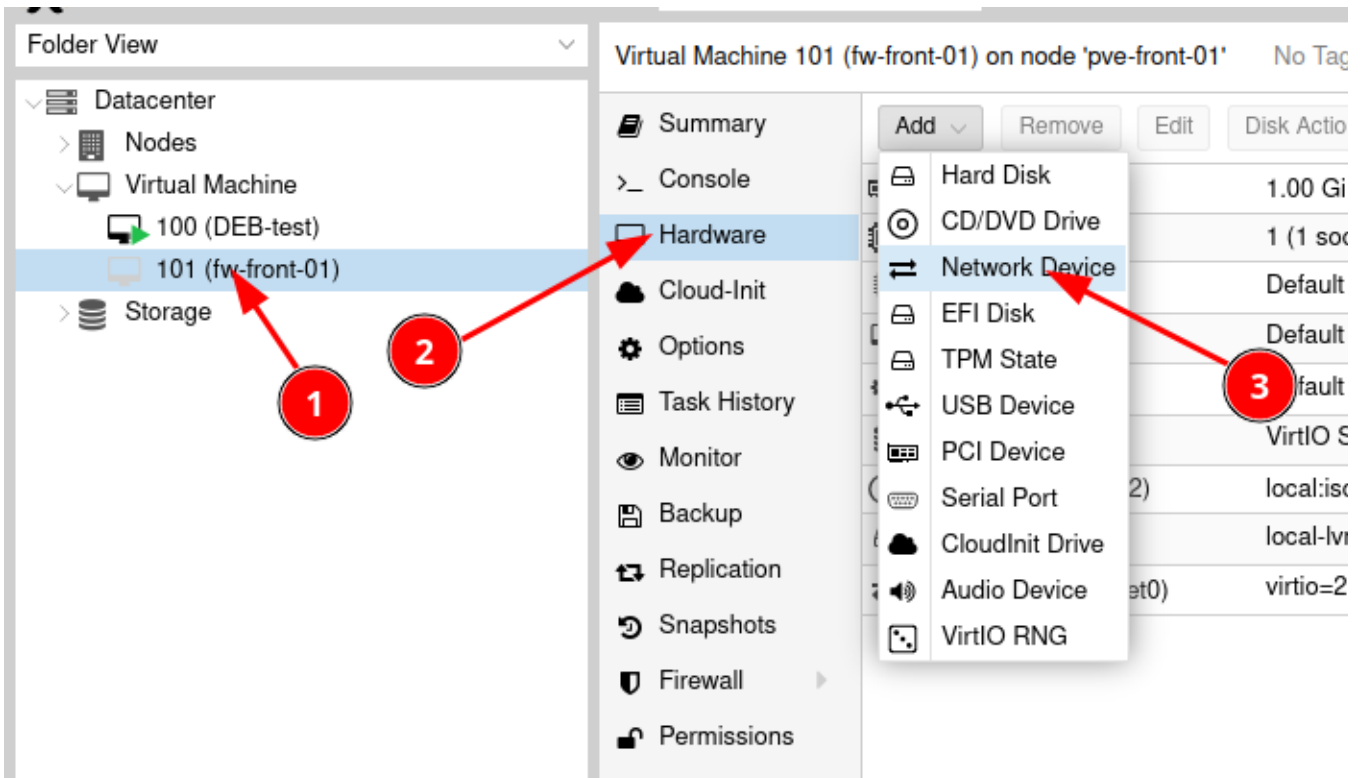
 Add

 Help Advanced  Back  Next

- Pour la partie CPU on la laisse par défaut.
- Pour la RAM on va mettre 1024 (1Go).
- Pour le réseau on va lui mettre l'interface vmbro



- On confirme la création mais on ne démarre pas de suite la machine.
- On modifie la configuration de la machine virtuelle afin de lui ajouter une carte pour le réseau LAN.



Add: Network Device ✕

Bridge: Model:

VLAN Tag: MAC address:

Firewall:

Advanced

- On démarre la VM.
- On se connecte à la console pour l'installation.
- Ne pas configurer les Vlans.

```

QEMU (fw-front-01) - noVNC — Mozilla Firefox
https://192.168.1.179:8006/?console=kvm&novnc=1&vmid=101&vmname=fw-front-01&...
Generating configuration: OK
>>> Invoking early script 'backup'
>>> Invoking backup script 'captiveportal'
>>> Invoking backup script 'dhcpleases'
>>> Invoking backup script 'duid'
>>> Invoking backup script 'netflow'
>>> Invoking backup script 'rrd'
>>> Invoking early script 'carp'
RP event system: OK
▶ unching the init system...done.
initializing.....done.
Starting device manager...intsmb0: <Intel PIIX4 SMBUS Interface> irq 9 at d
1.3 on pci0
intsmb0: intr IRQ 9 enabled revision 0
smbus0: <System Management Bus> on intsmb0
uhid0 on uhub0
uhid0: <QEMU QEMU USB Tablet, class 0/0, rev 2.00/0.00, addr 2> on usb0
done.
Configuring login behaviour...done.

Default interfaces not found -- Running interface assignment option.

Press any key to start the manual interface assignment: 3
Do you want to configure LAGGs now? [y/N]:
Do you want to configure VLANs now? [y/N]: █

```

- Sélectionner l'interface WAN (pour nous vtnet0).

```

Valid interfaces are:
vtnet0          26:2a:01:01:8d:bd VirtIO Networking Adapter
vtnet1          66:ad:a5:3a:6c:41 VirtIO Networking Adapter

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: █

```

- On configure la LAN (pour nous vtnet1).

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): vtnet1
```

- On ne met aucune interface optionnelle.
- On met oui à la question voulez-vous continuer.

```
The interfaces will be assigned as follows:

WAN  -> vtnet0
LAN  -> vtnet1

Do you want to proceed? [y/N]: y
```

- À la fin de l'installation, vous devriez avoir quelque chose qui ressemble à ça.

```
*** OPNsense.localdomain: OPNsense 23.1 ***

LAN (vtnet1)    -> v4: 192.168.1.1/24
WAN (vtnet0)    -> v4/DHCP4: 192.168.1.48/24
                v6/DHCP6: 2a01:e0a:2d2:d880:242a:1ff:fe01:8dbd/64

HTTPS: SHA256 C7 D3 A9 B5 1A C2 B7 98 49 0B 9E F6 3A 2D 0D A5
                32 26 D8 C0 6B 1B 73 C5 3E 60 43 D3 68 A1 4D D0
SSH:   SHA256 3gVsBdEroaLCsUXsxBcEyN84T23pQe/nHmRnZM3XsbE (ECDSA)
SSH:   SHA256 ke9CInhRSfvPXfG1ugRtyU6kg15LHnyiPm6QDfPt3uA (ED25519)
SSH:   SHA256 twfswSyLcGmzHT6yafs54w3YD0vidlhVvJKdiI/PZDk (RSA)

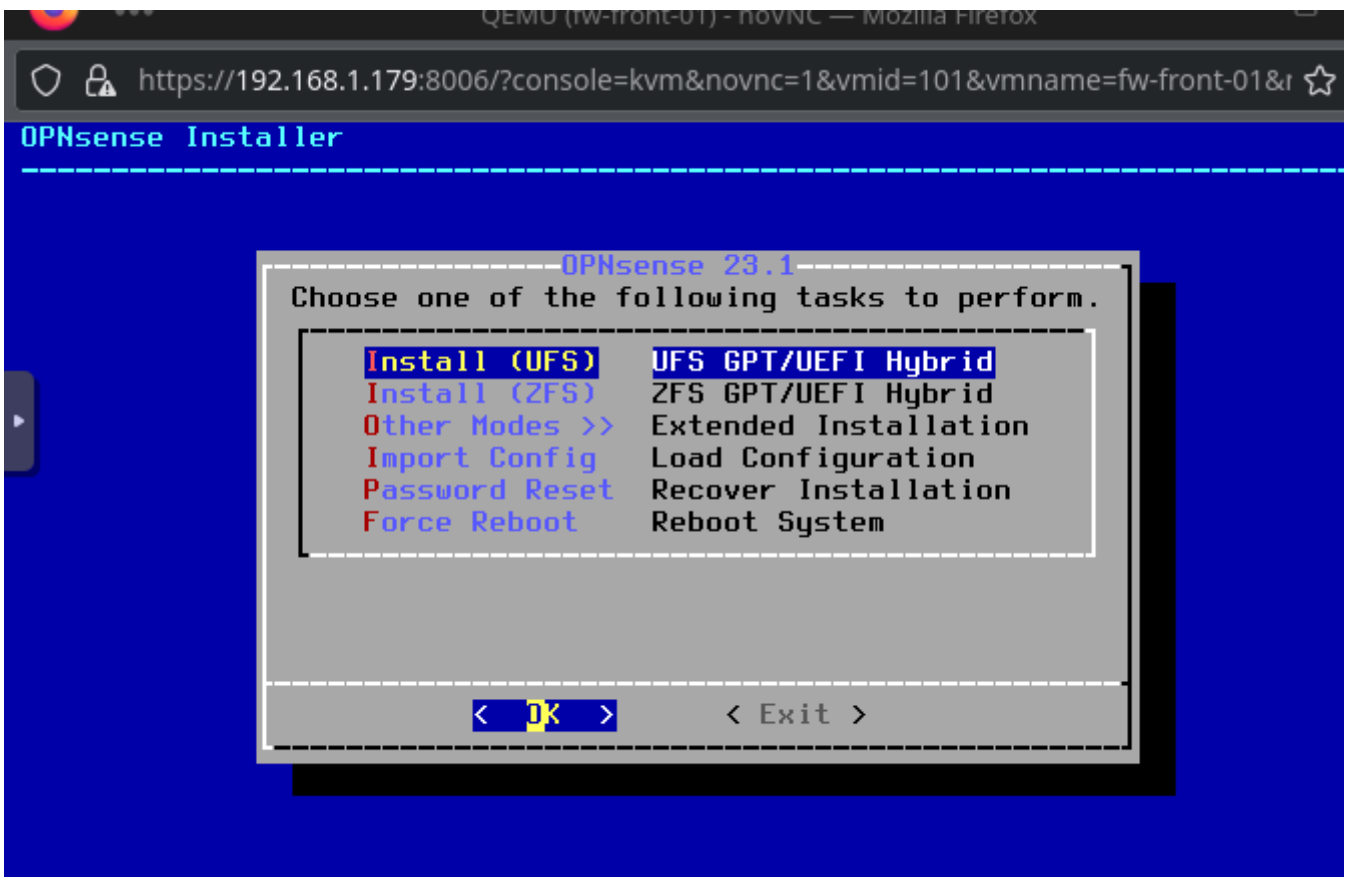
Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)

login: 
```

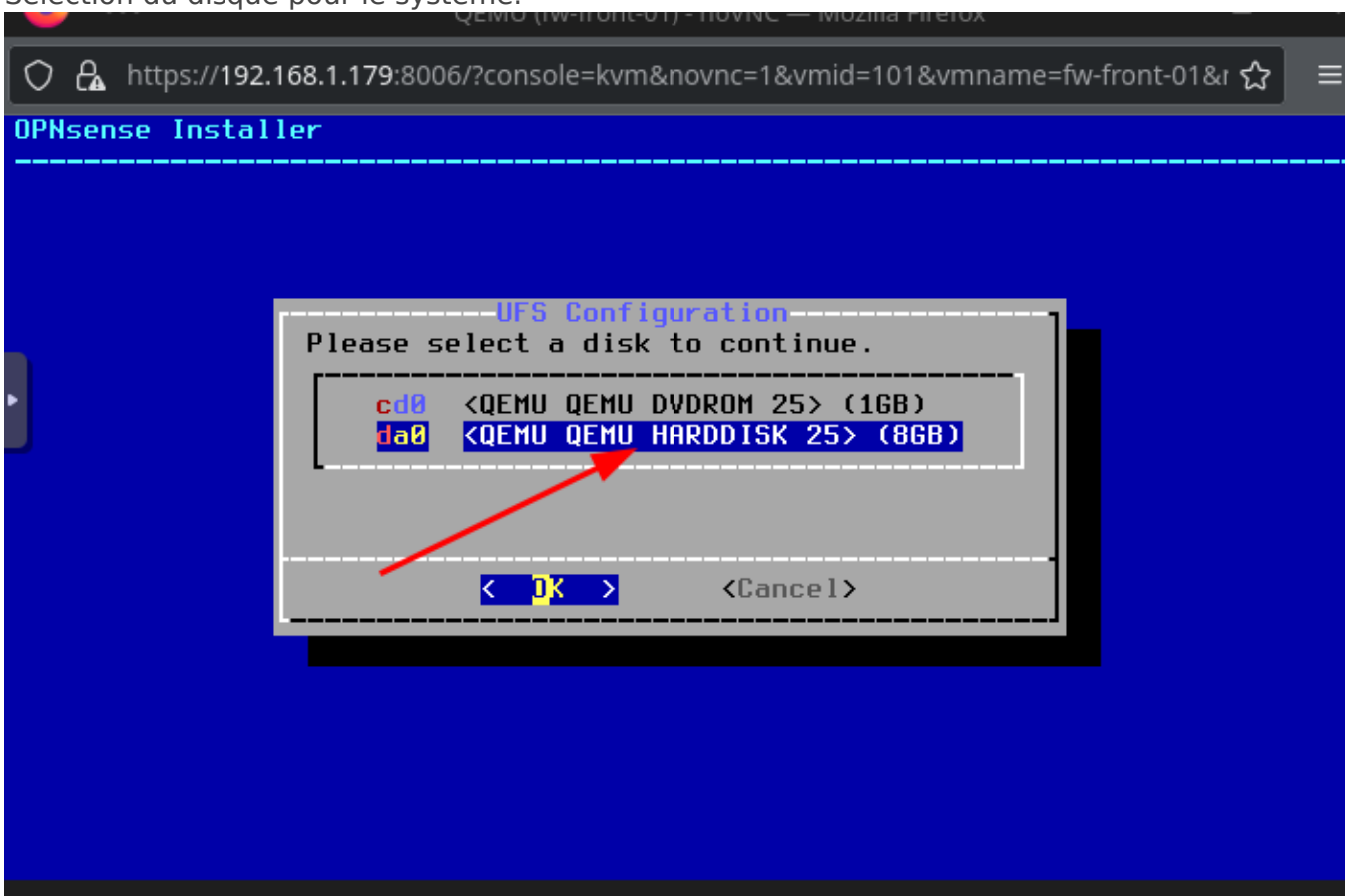
L'utilisateur est installer est le mot de passe opnsense

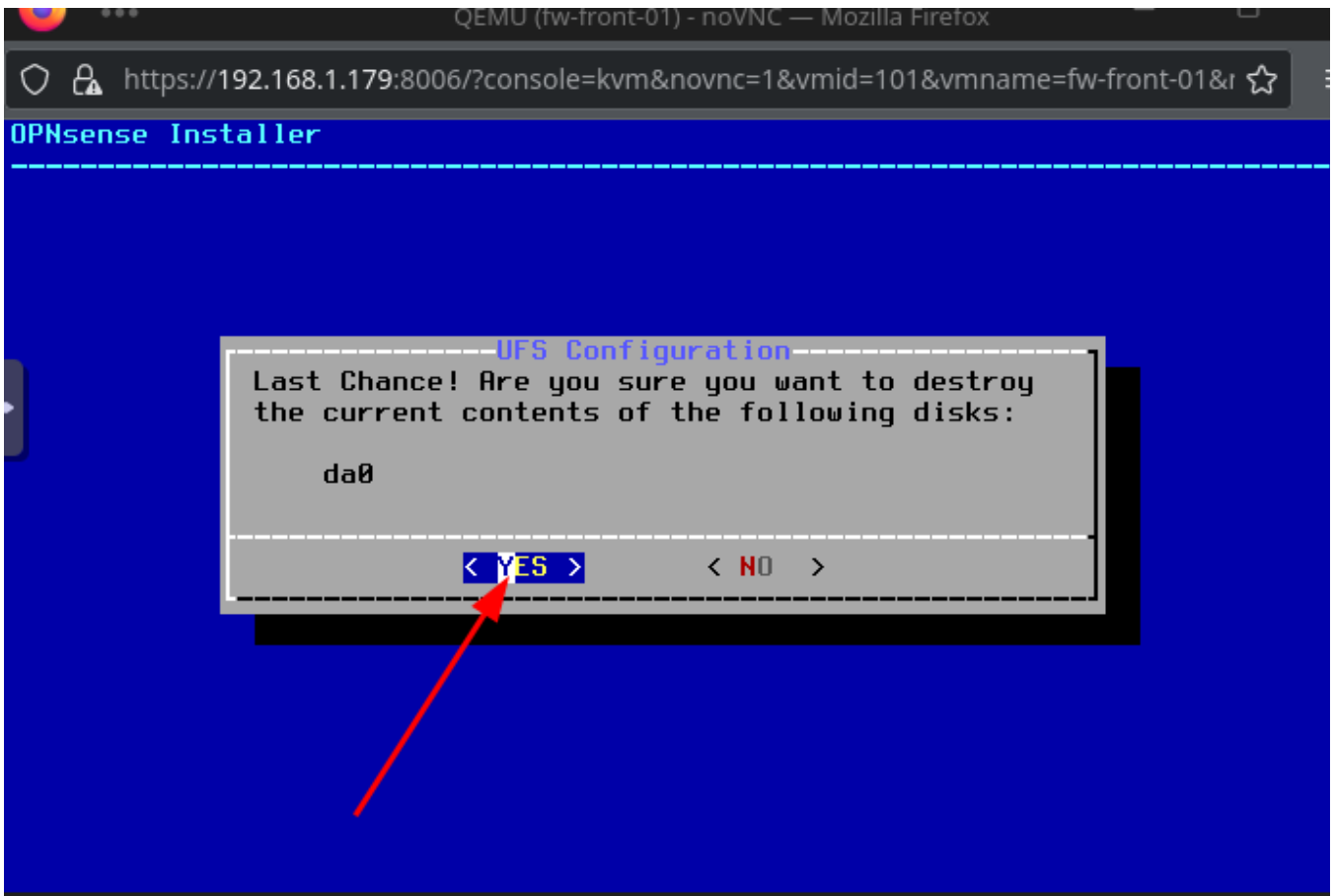
- Choisir Le clavier par défaut.
- Choisir install (UFS)



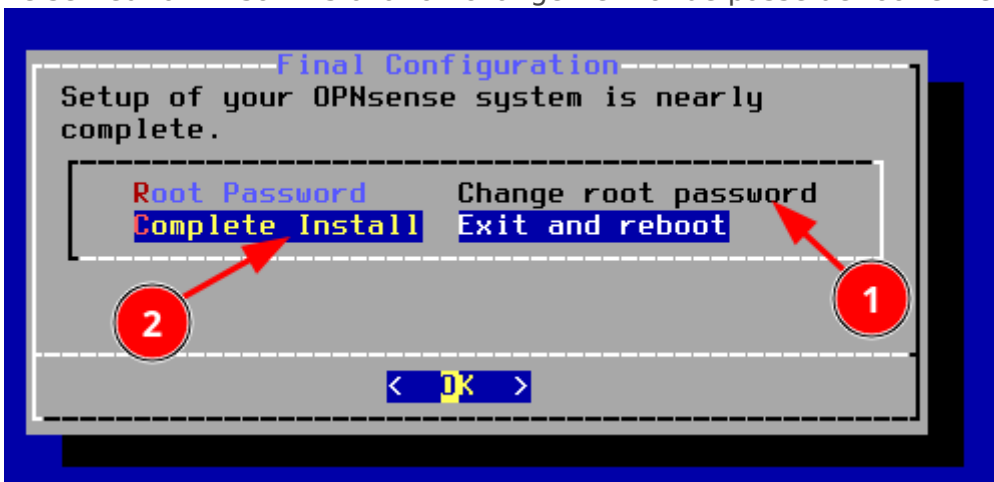
Une alerte va vous être afficher concernant la RAM, n'en tenez pas compte.

- Sélection du disque pour le système.

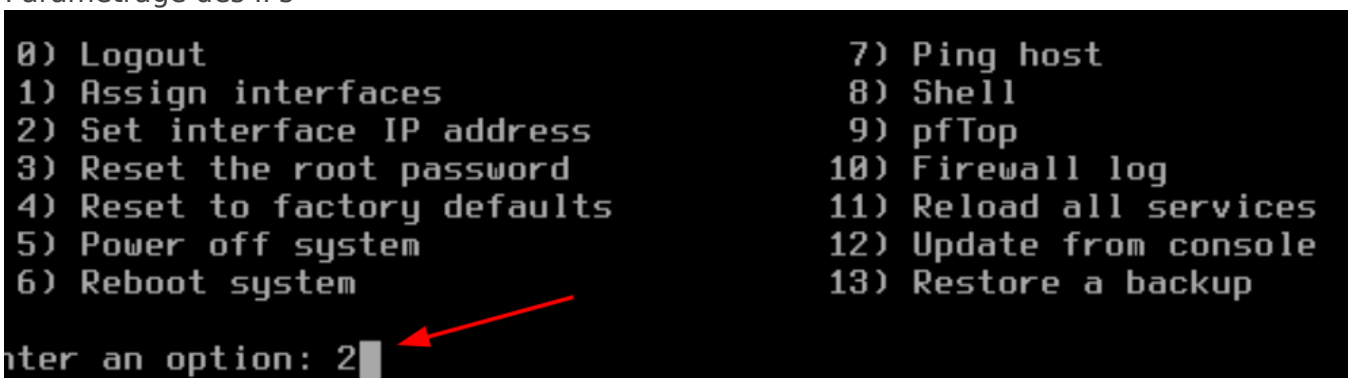




- Le serveur a fini son installation changer le mot de passe de root et redémarrer le serveur.



- Paramétrage des IPs



```
1 - LAN (vtnet1 - static, track6)
2 - WAN (vtnet0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1
```

- Ne pas configurer l'interface en DHCP mais en statique

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 172.16.250.1

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0    = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 26

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

- Ne rien mettre en IPV6
- Activer le reverse HTTP/HTTPS
- Désactiver le firewall pour accéder à la page de connexion (Dans notre cas et pour le moment aucune interface de notre réseau ne peut accéder au réseau que l'on vient de créer.

```
pfctl -d
```

```
0) Logout                7) Ping host
1) Assign interfaces     8) Shell
2) Set interface IP address
3) Reset the root password
4) Reset to factory defaults
5) Power off system      10) Firewall log
6) Reboot system         11) Reload all services
                          12) Update from console
                          13) Restore a backup

Enter an option: 8

root@OPNsense:~ # pfctl -d
pf disabled
root@OPNsense:~ #
```

- Accéder à la page web de OPNsense via l'IP de la WAN sur votre navigateur favoris et se connecter.

```
LAN (vtnet1) -> v4: 172.16.250.1/26
WAN (vtnet0) -> v4/DHCP4: 192.168.1.48/24
                v6/DHCP6: 2ad1:e0a:2d2:d880:242a:1ff:fe01:8dbd/
```

0) Logout
1) Assign interfaces
2) Set interface IP address
7) Ping host
8) Shell
9) pfTop

192.168.1.48

OPNsense

Username:
root

Password:

Login

OPNsense (c) 2014-2023 Deciso B.V.

The image shows a terminal window at the top with network configuration details. The WAN interface (vtnet0) is configured with a v4/DHCP4 address of 192.168.1.48/24, which is highlighted with a red box. Below the terminal is a browser window showing the OPNsense web interface. The address bar contains 192.168.1.48. The main content area displays the OPNsense logo and a login form. The login form has a red box around the Username and Password fields. The Username field contains 'root' and the Password field contains '*****'. A red arrow points from a red circle with the number '1' to the browser address bar. Another red arrow points from a red circle with the number '2' to the Username field. A third red arrow points from a red circle with the number '3' to the Login button. At the bottom of the page, there is a bullet point in French: 'Faites le wizard proposé en mettant bien le domaine, le nom du serveur et les DNS.'

- Faites le wizard proposé en mettant bien le domaine, le nom du serveur et les DNS.

System: Wizard: General Information

General Information

Hostname: ← 1

Domain: ← 2

Language:

Primary DNS Server: ← 3

Secondary DNS Server:

Override DNS: Allow DNS servers to be overridden by DHCP/PPP on WAN

Unbound DNS

Enable Resolver:

Enable DNSSEC Support:

Harden DNSSEC data:

← 4

System: Wizard: Time Server Information

Time server hostname:

Enter the hostname (FQDN) of the time server.

Timezone:

- Ne pas toucher à l'interface WAN sur le wizard sauf pour décocher Block RFC1918.

RFC1918 Networks

Block RFC1918 Private Networks: Block private networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback ad (127/8) and Carrier-grade NAT addresses (100.64/10). This option should only be set for WAN interfaces that use the public IP address space.

Block bogon networks

- Ne pas toucher à la LAN non plus.
- Vous aller modifier votre première règle firewall afin de pouvoir accéder à votre bon vouloir à OPNsense via la WAN.

OPNsense root@fw-front-01.megaproduction.local

Firewall: Rules: WAN

Select category

No WAN rules are currently defined. All incoming connections on this interface will be blocked until you add a pass rule. Exceptions for automatically generated rules may apply.

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
pass	block		reject				log
pass (disabled)	block (disabled)		reject (disabled)				log (disabled)

WAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is explicitly passed is blocked by default.

Firewall: Rules: WAN

Edit Firewall rule

Action Pass 1

Disabled Disable this rule

Quick Apply the action immediately on match.

Interface WAN 2

Direction in 3

TCP/IP Version IPv4

Protocol TCP 4

Source / Invert

Source any

Source

Destination / Invert

Destination This Firewall 5

Destination port range from: HTTP 6 to: HTTP

Log Log packets that are handled by this rule

Category

Description

Advanced features

No XMLRPC Sync

Schedule none

Gateway default

Advanced Options 7