

Documentation d'installation de OPNsense

Version : Avril 2025
Auteur : Alizée LECERF

Sommaire

1. Prérequis
2. Installation de OPNsense
3. Configuration initiale via l'interface web
4. Création d'un Alias
5. Création d'une catégorie
6. Création d'une règle de pare-feu

1. Prérequis

- Un ordinateur ou une VM avec les ressources nécessaires
- L'image ISO d'OPNsense, téléchargeable sur le site officiel

2. Installation de OPNsense

1. Démarrez votre machine sur l'image ISO d'OPNsense.
2. Une série de lignes de commande s'affichera. Patientez jusqu'à la fin du chargement.



```

sd0 at ata0 bus 0 scbus0 target 0 lun 0
sd0: <NECUMWar VMware IDE CDR00 1.00> Removable CD-ROM SCSI device
sd0: Serial Number 00000000000000000001
sd0: 33.300MB/s transfers (UDMA2, ATAPI 12bytes, PIO 65534bytes)
sd0: Attempt to query device size failed: NOT READY, Medium not present
sd1 at ata0 bus 0 scbus0 target 1 lun 0
sd1: <NECUMWar VMware IDE CDR01 1.00> Removable CD-ROM SCSI device
sd1: Serial Number 01000000000000000001
sd1: 33.300MB/s transfers (UDMA2, ATAPI 12bytes, PIO 65534bytes)
sd1: 2081MB (1065774 2048 byte sectors)
da0 at mpt0 bus 0 scbus2 target 0 lun 0
da0: <VMware Virtual disk 2.0> Fixed Direct Access SPC-4 SCSI device
da0: 300.000MB/s transfers
da0: Command Queuing enabled
da0: 51200MB (104857600 512 byte sectors)
da0: quirks=0x140<RETRY_BUSY, STRICT_UNMAP>
Mounting filesystems...
Setting hostuid: a9633578-9041-2e4e-9a21-7b9110e50f84.
Setting hostid: 0x269de716.
Press any key to start the configuration importer: ....

```

Connectez-vous avec l'identifiant : installer et le mot de passe : opnsense (clavier QWERTY).

```

>>> Invoking start script 'openvpn'
>>> Invoking start script 'sysctl'
Service 'sysctl' has been restarted.
>>> Invoking start script 'beep'
Root file system: /dev/iso9660/OPNSENSE_INSTALL
Thu Jan 23 07:54:52 UTC 2025

*** OPNsense.localdomain: OPNsense 24.7 ***

LAN (vmx0)      -> v4: 192.168.1.1/24

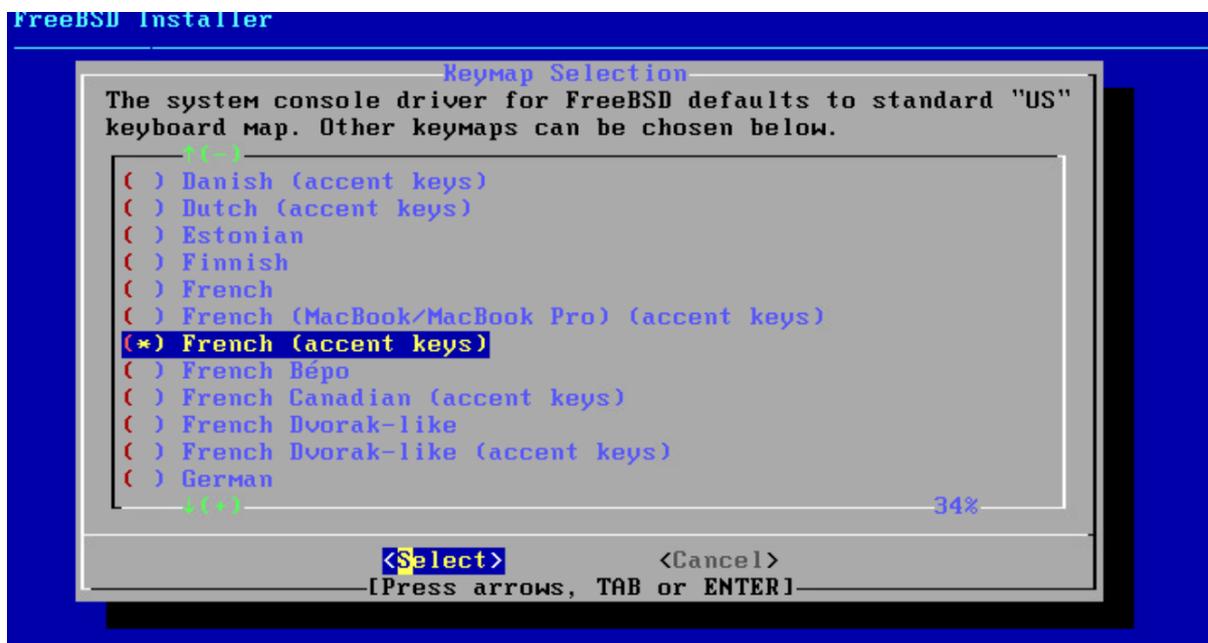
HTTPS: sha256 98 C4 3B 37 7D DD 7A 1B 03 45 33 0B A9 2B 96 C5
        7B 07 A4 AB 14 A9 72 B3 43 FE 79 68 D6 BB 06 E1
SSH:   SHA256 Lkk4Y5SpiADY/1Um5Bi+/8RpSQ52CUUUNzB0C61rUvA (ECDSA)
SSH:   SHA256 dsN2WICYWjln5nX72zHt0NwIN6qEXpVKKHU5ZwQegTg (ED25519)
SSH:   SHA256 +Kkmp/z0F0hQPXCEZ0220UEcUefU46XSaMEQ0Y2nKdE (RSA)

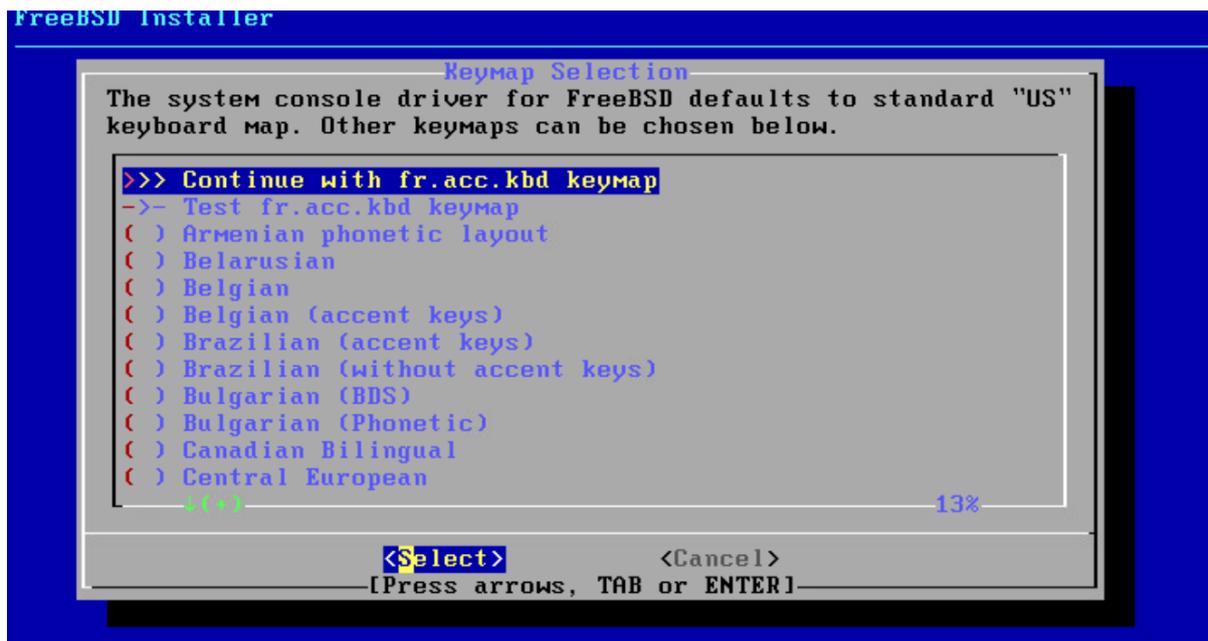
Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login: █

```

1. Choisissez le clavier 'french (accent keys)' avec les flèches, puis appuyez sur Entrée.
2. Sélectionnez « continue with fr.acc.kbd keymap ». Appuyez sur Entrée.

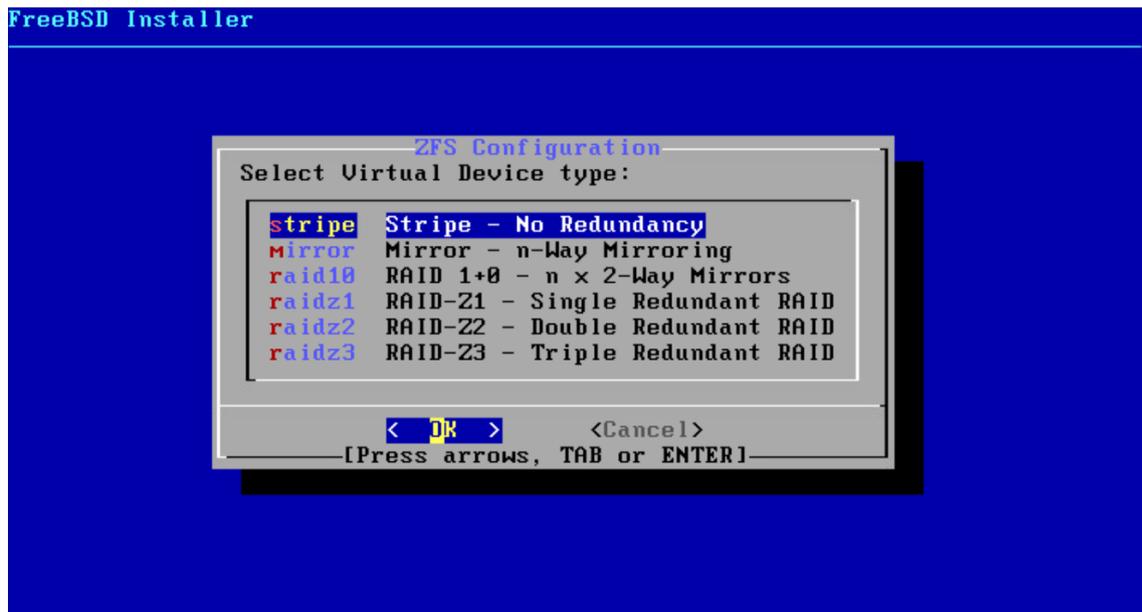




Choisissez l'option 'Install ZFS'.



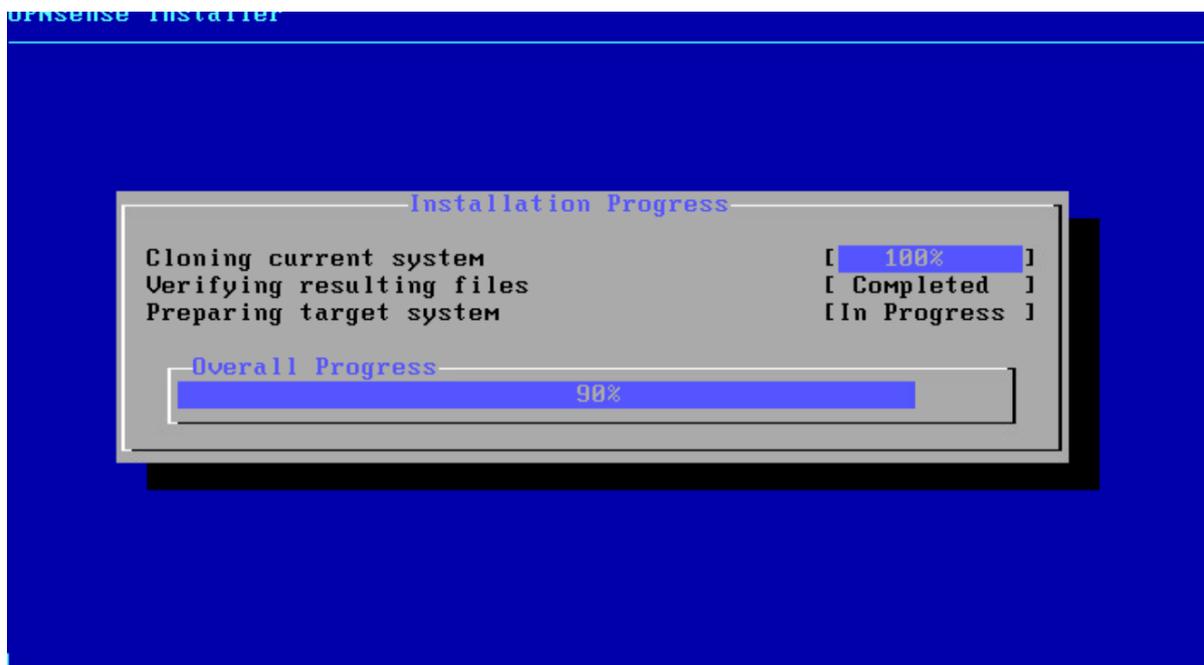
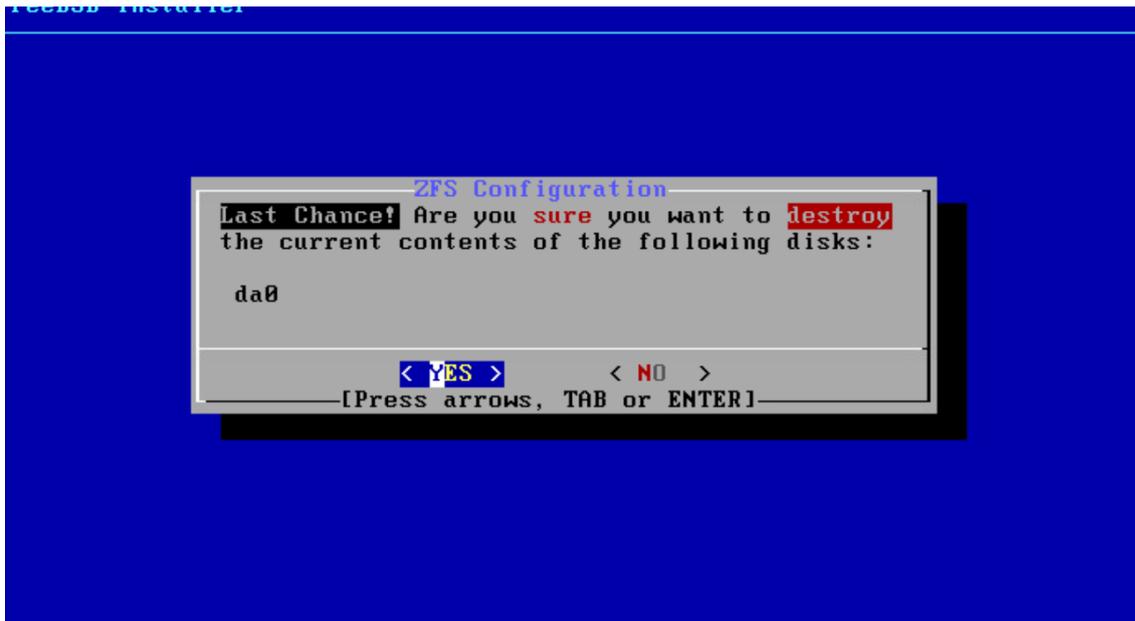
Sélectionnez 'stripe' (pour un seul disque)



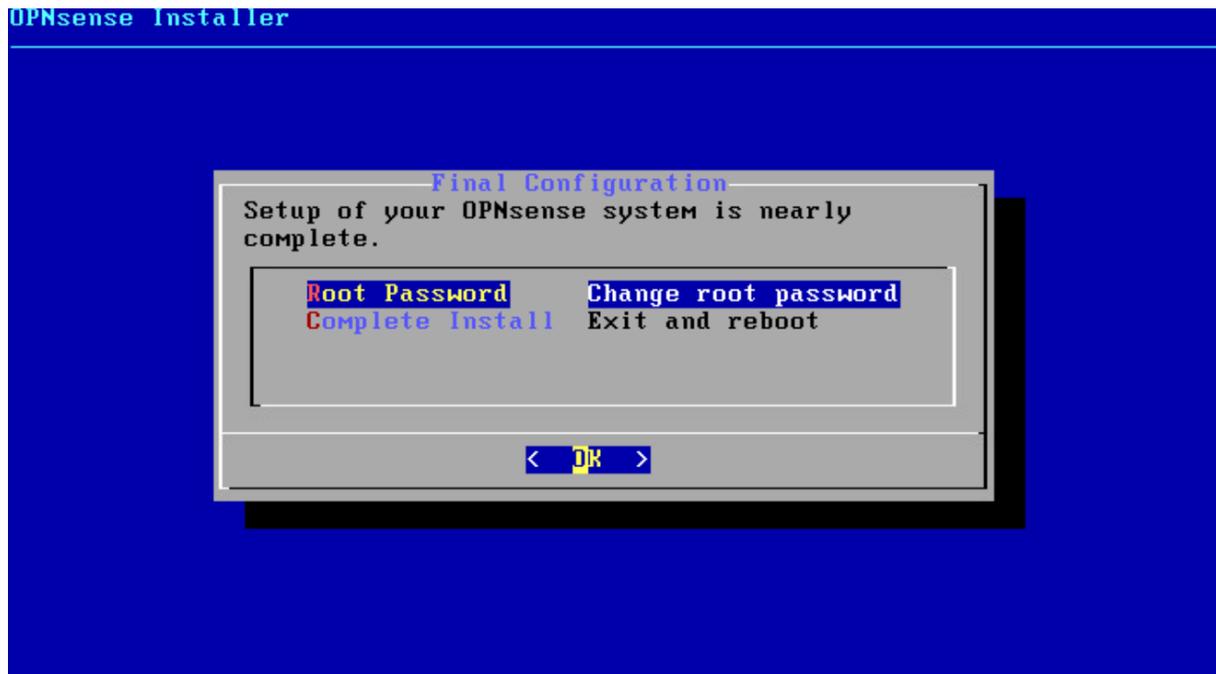
Cochez le disque (ex. : VMware Virtual Disk) avec la barre d'espace puis validez avec OK



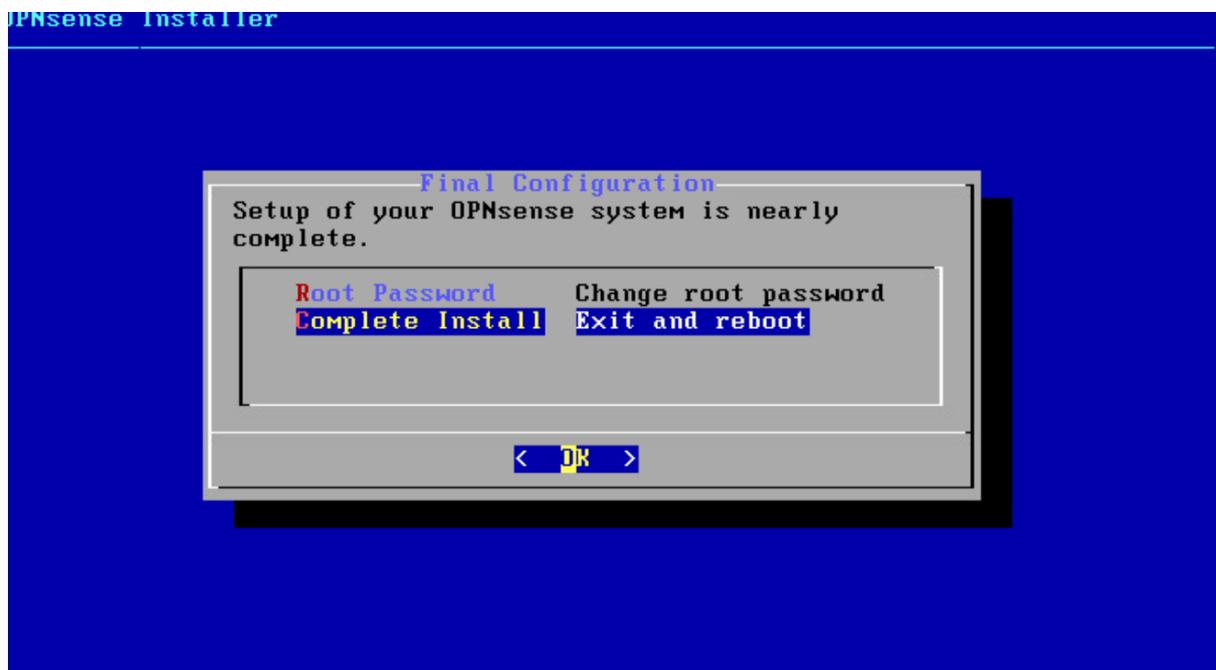
Confirmez l'installation avec 'Yes'.



Une fois l'installation terminée, changez le mot de passe root si souhaité.



Choisissez 'Complete Install' pour redémarrer la machine.



3. Configuration initiale via l'interface web

Au redémarrage, sélectionnez l'option 1 pour assigner les interfaces (ex. : WAN, LAN).

```

      Hello, this is OPNsense 24.7
-----
Website:  https://opnsense.org/
Handbook:  https://docs.opnsense.org/
Forums:    https://forum.opnsense.org/
Code:      https://github.com/opnsense
Twitter:   https://twitter.com/opnsense

*** OPNsense.localdomain: OPNsense 24.7 ***

LAN (vmx0)      -> v4: 192.168.1.1/24

HTTPS: sha256 98 C4 3B 37 7D DD 7A 1B 03 45 33 0B A9 2B 96 C5
        7B 07 A4 AB 14 A9 72 B3 43 FE 79 68 D6 BB 06 E1

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

Enter an option: 1
```

Attribuez un nom à chaque interface, puis confirmez avec Y.

Enter an option: 1

Do you want to configure LAGGs now? [y/N]: n

Do you want to configure VLANs now? [y/N]: n

Valid interfaces are:

```
vmx0          02:00:c2:38:be:ca VMware VMXNET3 Ethernet Adapter
vmx1          02:00:ba:3b:b6:ab VMware VMXNET3 Ethernet Adapter
vmx2          02:00:fa:48:4a:62 VMware VMXNET3 Ethernet Adapter
vmx3          02:00:33:db:c0:7d VMware VMXNET3 Ethernet 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: █

Do you want to configure LAGGs now? [y/N]: n

Do you want to configure VLANs now? [y/N]: n

Valid interfaces are:

```
vmx0          02:00:c2:38:be:ca VMware VMXNET3 Ethernet Adapter
vmx1          02:00:ba:3b:b6:ab VMware VMXNET3 Ethernet Adapter
vmx2          02:00:fa:48:4a:62 VMware VMXNET3 Ethernet Adapter
vmx3          02:00:33:db:c0:7d VMware VMXNET3 Ethernet 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: vmx1

Enter the LAN interface name or 'a' for auto-detection

NOTE: this enables full Firewalling/NAT mode.

(or nothing if finished): vmx2

Enter the Optional interface 1 name or 'a' for auto-detection

(or nothing if finished): vmx3

Enter the Optional interface 2 name or 'a' for auto-detection

(or nothing if finished): vmx0 █

hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: vmx1

Enter the LAN interface name or 'a' for auto-detection

NOTE: this enables full Firewalling/NAT mode.

(or nothing if finished): vmx2

Enter the Optional interface 1 name or 'a' for auto-detection

(or nothing if finished): vmx3

Enter the Optional interface 2 name or 'a' for auto-detection

(or nothing if finished): vmx0

Enter the Optional interface 3 name or 'a' for auto-detection

(or nothing if finished):

The interfaces will be assigned as follows:

WAN -> vmx1

LAN -> vmx2

OPT1 -> vmx3

OPT2 -> vmx0

Do you want to proceed? [y/N]: y █

Choisissez l'option 2 pour configurer les adresses IP de chaque interface.

```
OPT3 (vnx3)
WAN (vnx1) -> v4/DHCP4: 10.192.0.149/24

HTTPS: sha256 EC 9F 0D EB A5 08 02 B4 D4 BD 22 F2 C8 1F 7F AE
        B0 4E C4 08 4D 06 7F 65 41 32 54 C3 46 0C FD 48

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

Enter an option: 2
```

```
2 - OPT2 (vnx3)
3 - OPT3 (vnx0)
4 - WAN (vnx1 - dhcp, dhcp6)

Enter the number of the interface to configure: 1

Configure IPv4 address OPT1 interface via DHCP? [y/N] n

Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 192.168.2.254

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 OPT1 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via WAN tracking? [Y/n] n
```

```
For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via WAN tracking? [Y/n] n
Configure IPv6 address OPT1 interface via DHCP6? [y/N] n

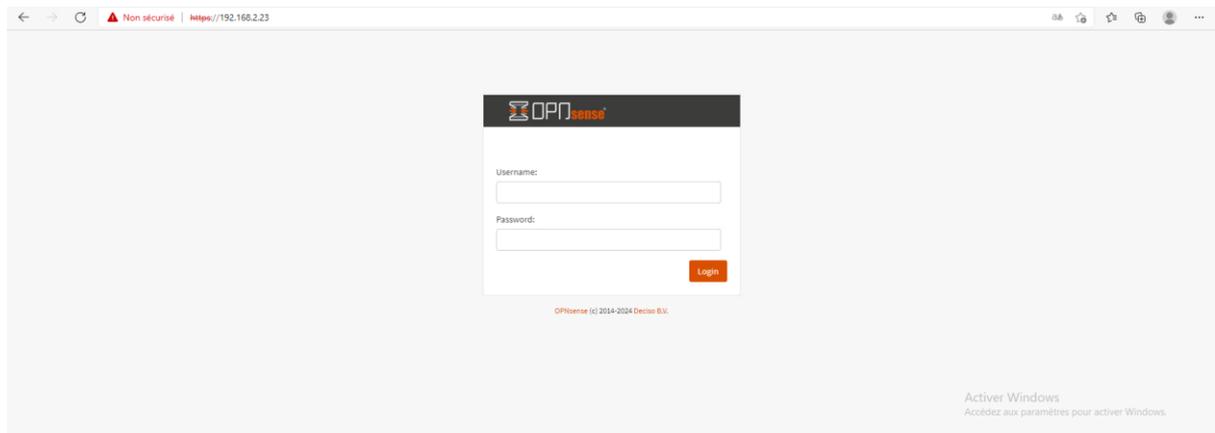
Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT1? [y/N] n

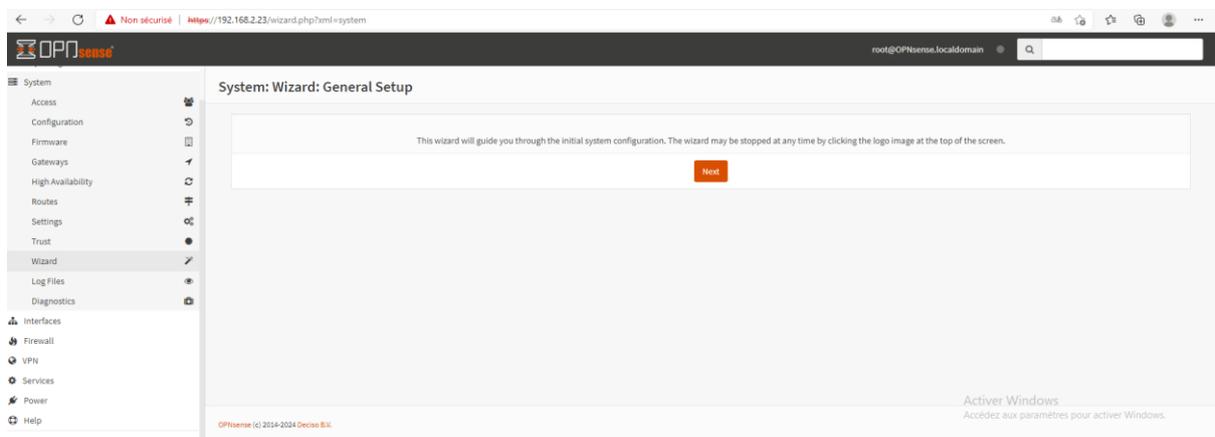
Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] y
Restore web GUI access defaults? [y/N] y

Writing configuration...done.
Generating /etc/resolv.conf...done.
Generating /etc/hosts...done.
Configuring OPT1 interface...done.
Setting up routes for opt1...done.
Starting Unbound DNS...done.
Configuring firewall.....done.
Starting web GUI...done.
```

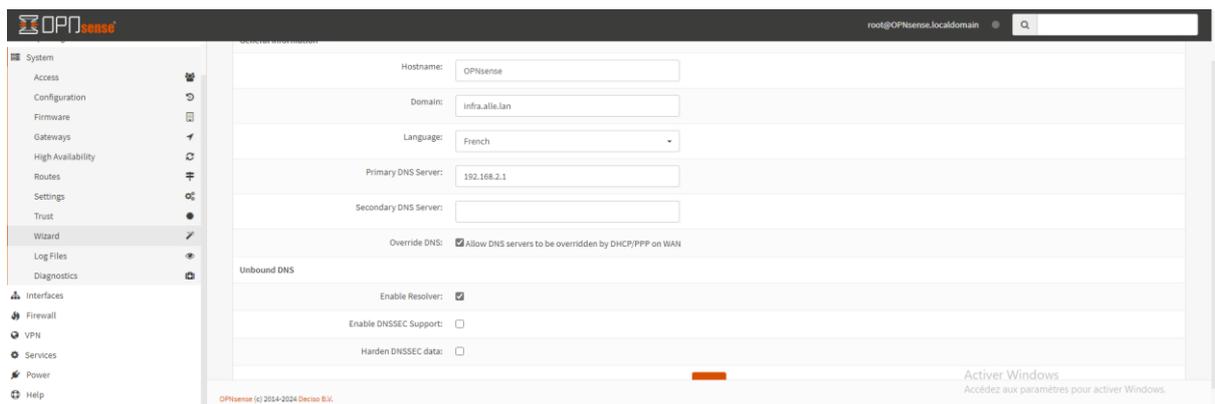
1. Accédez à l'interface web via l'adresse indiquée (ex. : <https://192.168.2.23>).
2. Connectez-vous avec root et le mot de passe défini.



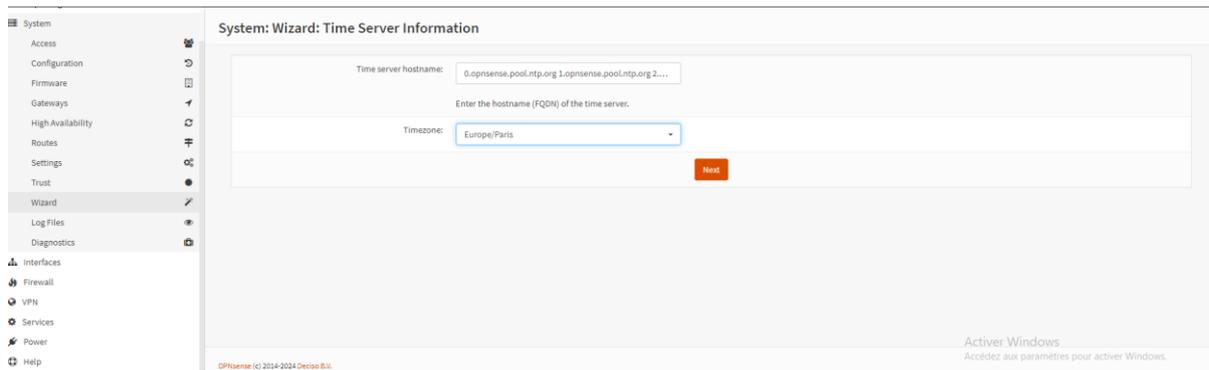
Suivez l'assistant de configuration initiale (Wizard).



Définissez le nom de domaine, la langue, l'adresse IP du domaine et cliquez sur Next.

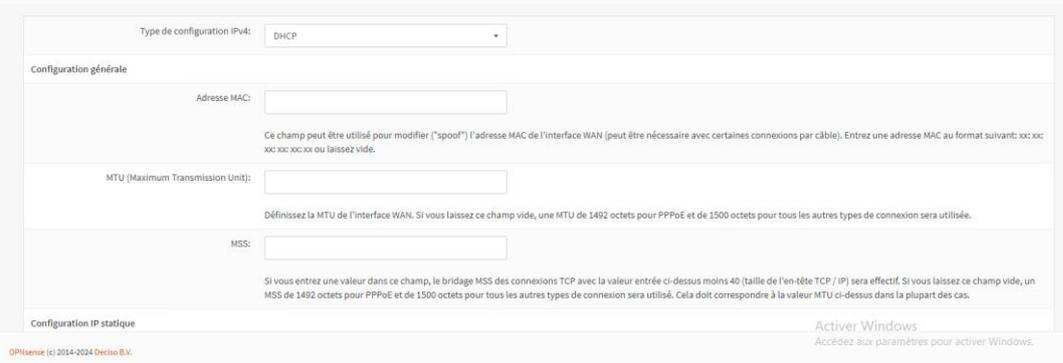


Choisissez la timezone : Europe/Paris.



Pour l'interface WAN : décochez l'option 'Bloquer l'accès des réseaux privés'.

Système: Assistant: Configurer l'interface WAN



Pour l'interface LAN : configurez l'adresse IP et le masque de sous-réseau.

Système: Assistant: Configurer l'interface LAN

Adresse IP LAN:	<input type="text" value="192.168.2.254"/>
	(Laisser vide pour aucun)
Masque de sous-réseau:	<input type="text" value="24"/>
	<input type="button" value="Suivant"/>

Définissez un nouveau mot de passe root (optionnel).

Système: Assistant: Définir le Mot de passe Root

Mot de passe Root:	<input type="text"/>
	(Laisser vide pour garder l'actuel(le))
Confirmation Mot de passe Root:	<input type="text"/>
	<input type="button" value="Suivant"/>

Terminez l'assistant et rechargez la configuration lorsque demandé.

Système: Assistant: Recharger la Configuration

Cliquez 'Recharger' pour appliquer les changements.

Systeme: Assistant: Rechargement en cours

Un rechargement est en cours. L'assistant vous redirigera vers le tableau de bord une fois ce rechargement terminé.

Configuration initiale terminée!



Félicitations! OPNsense est maintenant configuré.

Veuillez envisager de faire un don au projet pour nous aider à payer nos frais généraux. Consultez [notre site internet](#) pour faire un don ou acheter des services d'assistance OPNsense disponibles.

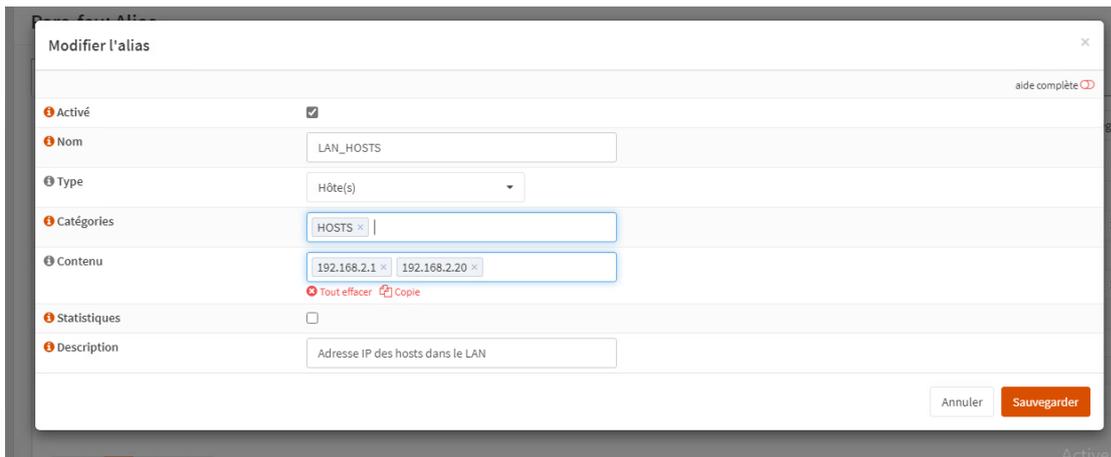
Cliquez pour continuer vers le [tableau de bord](#). Ou cliquez sur [check for updates](#).

4. Création d'un Alias

1. Allez dans le menu Pare-feu > Alias.
2. Cliquez sur le bouton « + ».

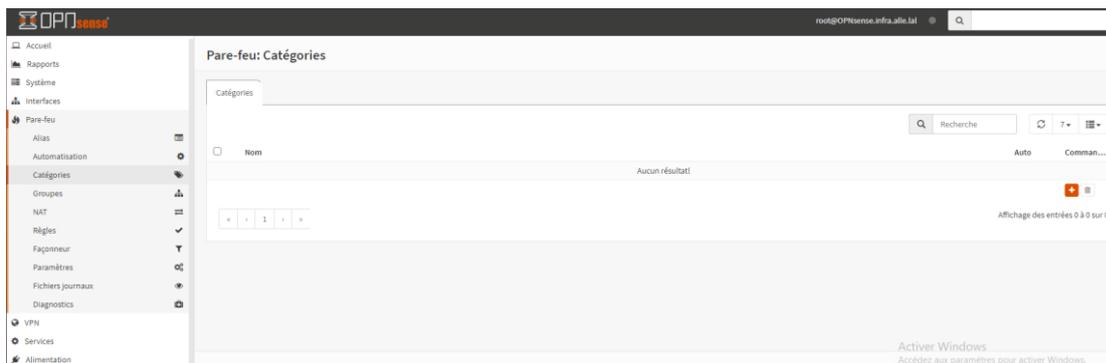
Activé	Nom	Type	Description	Contenu	Chargé	Dernière mise à jour	Commandes
<input checked="" type="checkbox"/>	PORTS_WEB	Port(s)	Ports pour le web	80 443 8080			
<input checked="" type="checkbox"/>	SRV_HOSTS	Hôte(s)	Hosts du SRV (proximox)	192.168.3.1 192.168.3.2 192.168...	3	2025-02-10 09:33:23	
<input checked="" type="checkbox"/>	PORTS_PROXIMOX	Port(s)	Ports pour proximox	8006 8007			
<input checked="" type="checkbox"/>	DMZ_HOSTS	Hôte(s)		192.168.4.1 192.168.4.2 192.168...	3	2025-02-12 09:46:36	
<input checked="" type="checkbox"/>	bogons	Externe (avancé)	bogon networks (internal)		10		
<input checked="" type="checkbox"/>	bogonsv6	Externe (avancé)	bogon networks IPv6 (internal)		76		
<input checked="" type="checkbox"/>	virusprot	Externe (avancé)	overflow table for rate limiting (L...		0		

1. Saisissez un nom, choisissez un type (IP, Port, etc.).
2. Optionnel : attribuez une catégorie.
3. Ajoutez les contenus (adresses IP ou ports).
4. Ajoutez une description, puis cliquez sur Enregistrer.

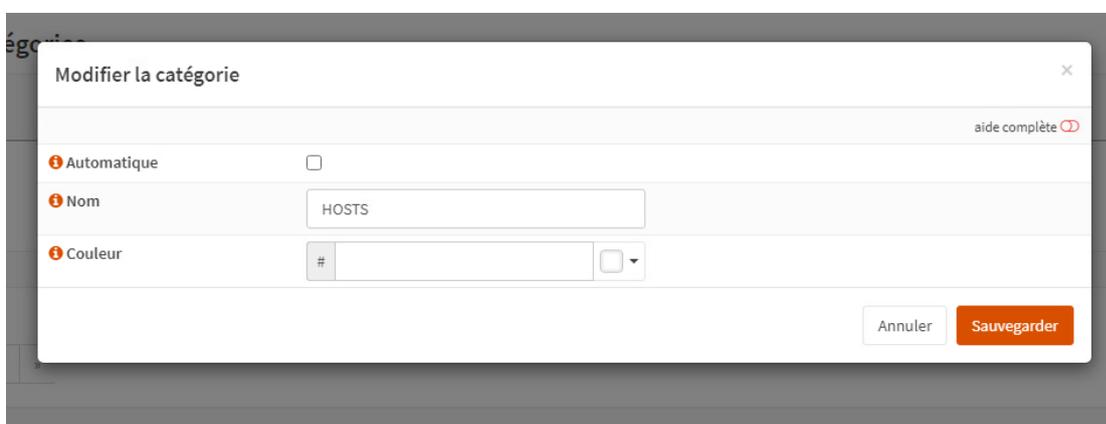


5. Création d'une catégorie

1. Allez dans le menu Pare-feu > Catégories.
2. Cliquez sur le bouton « + ».

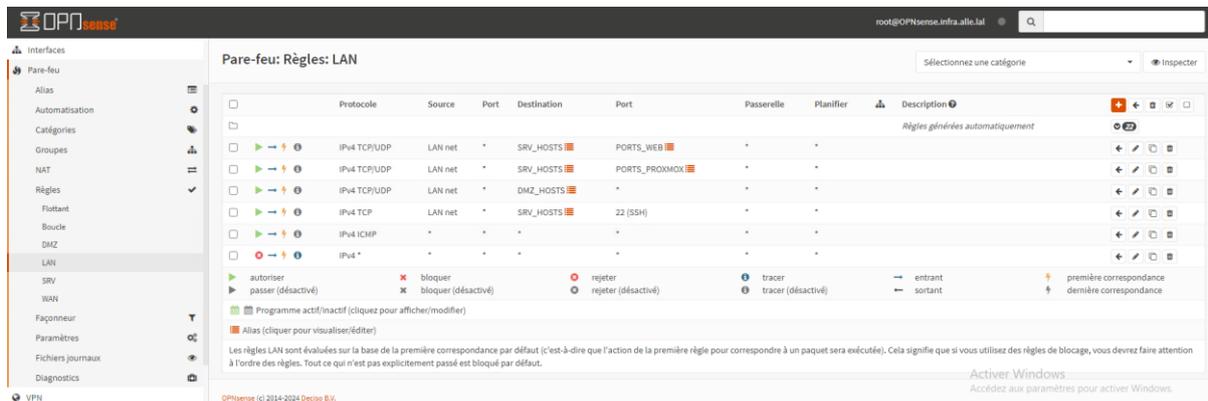


1. Saisissez le nom et choisissez une couleur.
2. Cliquez sur Enregistrer.



6. Création d'une règle de pare-feu

1. Allez dans Pare-feu > Règles.
2. Choisissez l'interface (ex. : LAN) puis cliquez sur « + ».



1. Sélectionnez l'action (autoriser, rejeter, bloquer).
2. Définissez le protocole (ex. : TCP/UDP), source et destination.

Éditer la règle du pare-feu

Action	Autoriser
Désactivé	<input type="checkbox"/> Désactiver cette règle
Rapide	<input checked="" type="checkbox"/> Appliquer l'action immédiatement sur la correspondance.
Interface	LAN
Direction	in
Version TCP/IP	IPv4
Protocole	TCP/UDP
Source / Inverser	<input type="checkbox"/> Utilisez cette option pour inverser le sens de la correspondance.
Source	LAN net

Source: LAN net

Source: Avancé

Destination / Inverser: Utilisez cette option pour inverser le sens de la correspondance.

Destination: any

Plage de ports de destination: de: PORTS_WEB à: PORTS_WEB

Journaliser: Journaliser les paquets gérés par cette règle

Catégorie:

Description: Autoriser les hosts de LAN à aller sur internet

1. Optionnel : ajoutez une catégorie et une description.
2. Cliquez sur Enregistrer.

Plage de ports de destination: de: PORTS_WEB à: PORTS_WEB

Journaliser: Journaliser les paquets gérés par cette règle

Catégorie:

Description: Autoriser les hosts de LAN à aller sur internet

Pas de Sync XMLRPC:

Planifier: aucun(e)

Passerelle: défaut

Fonctionnalités avancées: Afficher/Masquer

[Sauvegarder](#) [Annuler](#)

Active Accède:

OPNsense (c) 2014-2024 Deciso B.V.

1. Positionnez la règle à l'endroit souhaité dans la liste.
2. Cliquez sur « Appliquer les changements ».

OPNsense root@OPNsense.infra.adts.lal

Pare-feu: Règles: LAN

Sélectionnez une catégorie Inspecter

La configuration des règles de pare-feu a été modifiée. Vous devez appliquer les modifications afin qu'elles prennent effet. [Appliquer les changements](#)

	Protocole	Source	Port	Destination	Port	Passerelle	Planifier	Description	
Règles générées automatiquement									
<input type="checkbox"/>	IPV4 TCP/UDP	LAN net	*	SRV_HOSTS	PORTS_WEB	*	*		<input type="checkbox"/>
<input type="checkbox"/>	IPV4 TCP/UDP	LAN net	*	SRV_HOSTS	PORTS_PROXMOX	*	*		<input type="checkbox"/>
<input type="checkbox"/>	IPV4 TCP/UDP	LAN net	*	PORTS_WEB	*	*	*	Autoriser les hosts de LAN à aller sur internet	<input type="checkbox"/>
<input type="checkbox"/>	IPV4 TCP/UDP	LAN net	*	DMZ_HOSTS	*	*	*		<input type="checkbox"/>
<input type="checkbox"/>	IPV4 TCP	LAN net	*	SRV_HOSTS	22 (SSH)	*	*		<input type="checkbox"/>
<input type="checkbox"/>	IPV4 ICMP	*	*	*	*	*	*		<input type="checkbox"/>
<input type="checkbox"/>	IPV4 *	*	*	*	*	*	*		<input type="checkbox"/>

autoriser bloquer bloquer (désactivé) rejeter rejeter (désactivé) tracer tracer (désactivé) entant première correspondance sortir dernière correspondance

OPNsense (c) 2014-2024 Deciso B.V. Active Windows Accédez aux paramètres pour activer Windows.

Vous savez désormais comment installer OPNsense, créer un Alias, une catégorie, et configurer des règles de pare-feu.