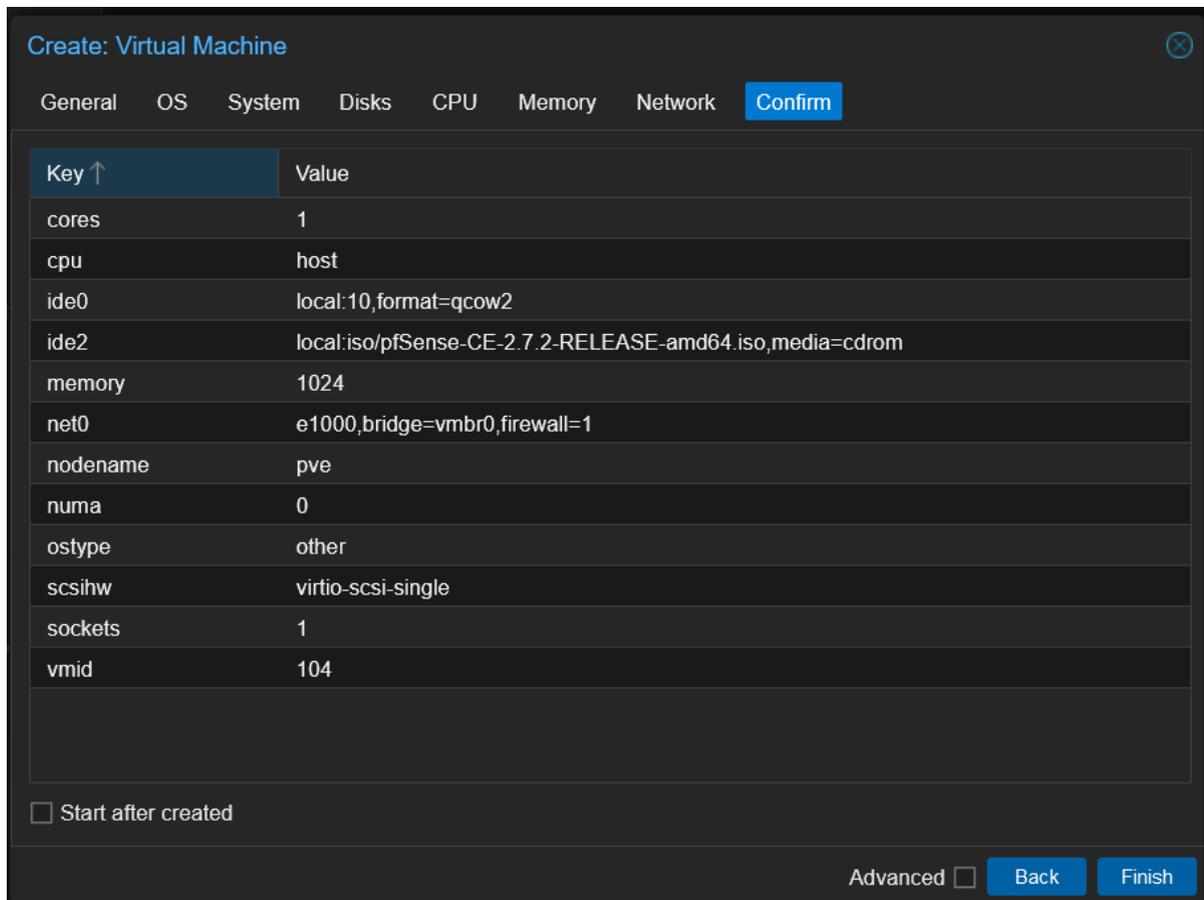


# Installation de PFSense sur PVE 8.2

## I ) Création de la VM

On commence par créer une VM PFSense en KVM en respectant les demandes de documentation.

On selection en premier lier l'ISO de PFSense dans ça version la plus récente ici la 2.7.2 Il suffit ensuite de remplir les demande de la documentation du TD dans la configuration



Key ↑	Value
cores	1
cpu	host
ide0	local:10,format=qcow2
ide2	local:iso/pfSense-CE-2.7.2-RELEASE-amd64.iso,media=cdrom
memory	1024
net0	e1000,bridge=vbr0,firewall=1
nodename	pve
numa	0
ostype	other
scsihw	virtio-scsi-single
sockets	1
vmid	104

Start after created

Advanced  [Back](#) [Finish](#)

(Le screen contient un résumé de la configuration port-cr ation de la VM)

## II ) Théorie des VLANs et Interfaces

Notre PfSense possède au total 5 interface réseaux

- WAN : Configurer en DHCP afin d'être le plus flexible | **DHCP**
- LAN : Configurer en statique (Sera placé par la suite dans le VLAN 30) | **IP Temporaire**
- VLAN 10 : Gateway et Serveur DNS du VLAN 10 | **192.168.10.0/24**
- VLAN 20 : Gateway et Serveur DNS du VLAN 20 | **192.168.20.0/24**
- VLAN 30 : Gateway et Serveur DNS du VLAN 30 | **192.168.30.0/24**

```
KVM Guest - Netgate Device ID: a806afbbf1484d522823
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.1.87/24
                v6/DHCP6: 2a01:cb08:1166:3000:be24:11ff:feec:5
96f/64
LAN (lan)      -> vtnet1      -> v4: 192.168.1.90/24
VLAN10 (opt1) -> vtnet2.10  -> v4: 192.168.10.254/24
VLAN20 (opt2) -> vtnet3.20  -> v4: 192.168.20.254/24
VLAN30 (opt3) -> vtnet4.30  -> v4: 192.168.30.254/24
```

Dans le WebGUI cette configuration est présentée sous cette forme

Ici on retrouve un résumé du screen supérieur avec la création des interfaces virtuelles dédiées au VLAN

Interface	Network port
WAN	vtnet0 (bc:24:11:ec:59:6f)
LAN	vtnet1 (bc:24:11:c5:99:20)
VLAN10	VLAN 10 on vtnet2 (VLAN-10 Serveur)
VLAN20	VLAN 20 on vtnet3 (VLAN-20 Client)
VLAN30	VLAN 30 on vtnet4 (VLAN-30 Administration)

VLAN Interfaces				
Interface	VLAN tag	Priority	Description	Actions
vtnet2	10		VLAN-10 Serveur	 
vtnet3	20		VLAN-20 Client	 
vtnet4	30		VLAN-30 Administration	 

Dans Proxmox, les interfaces sont référencées sous cette forme

L'interface LAN et l'interface WAN sont associées au **VMBR0**, ce qui leur permet d'accéder à Internet.

*(Cela permet également de gérer le pfSense sans quitter le réseau LAN, tout en maintenant l'accès à Internet.)*

Les interfaces virtuelles des VLAN, quant à elles, sont associées au **VMBR99**. Cela signifie que la seule manière pour ces réseaux de sortir est de passer par un NAT configuré sur l'interface WAN, laquelle est placée dans le **VMBR0**.

	Network Device (net0)	virtio=BC:24:11:EC:59:6F,bridge=vmbr0,firewall=1
	Network Device (net1)	virtio=BC:24:11:C5:99:20,bridge=vmbr0,firewall=1
	Network Device (net2)	virtio=BC:24:11:CD:04:FB,bridge=vmbr99,firewall=1
	Network Device (net3)	virtio=BC:24:11:65:8B:5E,bridge=vmbr99,firewall=1
	Network Device (net4)	virtio=BC:24:11:76:E7:EE,bridge=vmbr99,firewall=1

### III ) Mise en place des services (NAT/DNS Resolver)

## NAT

Pour paramétrer le NAT sur PFSense, il faut se rendre dans Firewall > NAT > Outbound. Dans notre cas, une configuration avancée n'est pas nécessaire : le NAT automatique sera suffisant.

Firewall / NAT / Outbound

Port Forward 1:1 **Outbound** NPt

#### Outbound NAT Mode

Mode

- Automatic outbound NAT rule generation. (IPsec passthrough included)
- Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
- Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
- Disable Outbound NAT rule generation. (No Outbound NAT rules)

[Save](#)

#### Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Ac
<a href="#">↑ Add</a> <a href="#">↓ Add</a> <a href="#">Delete</a> <a href="#">Toggle</a>									

#### Automatic Rules

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	
✓ WAN	127.0.0.0/8 ::1/128 192.168.1.0/24 192.168.20.0/24 192.168.30.0/24		192.168.10.0/24	*	*	500	WAN address	*	✓ Auto created r ISAKMP
✓ WAN	127.0.0.0/8 ::1/128 192.168.1.0/24 192.168.20.0/24 192.168.30.0/24		192.168.10.0/24	*	*	*	WAN address	*	✗ Auto created r

[i](#)

## DNS Resolver

Le DNS Resolver permet de transformer PFSense en serveur DNS pour n'importe quel client communiquant directement ou indirectement avec lui. À ne pas confondre avec le DNS Forwarder, qui se contente de rediriger les requêtes DNS, par exemple vers Cloudflare.

Il se trouve dans Services > DNS Resolver > General Settings  
Il suffit de l'activer et de vérifier que nos VLAN se trouve bien dans la liste "Network Interfaces"

The screenshot shows the pfSense web interface for the DNS Resolver General Settings. At the top, there is a breadcrumb trail: Services / DNS Resolver / General Settings. Below this is a yellow warning banner: "ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced >". The main navigation tabs are General Settings (selected), Advanced Settings, and Access Lists. The section title is "General DNS Resolver Options".

<b>Enable</b>	<input checked="" type="checkbox"/> Enable DNS resolver
<b>Listen Port</b>	53 <small>The port used for responding to DNS queries. It should normally be left blank unless</small>
<b>Enable SSL/TLS Service</b>	<input type="checkbox"/> Respond to incoming SSL/TLS queries from local clients <small>Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer this option disables automatic interface response routing behavior, thus it works by</small>
<b>SSL/TLS Certificate</b>	GUI default (677cea184a92a) <small>The server certificate to use for SSL/TLS service. The CA chain will be determined by</small>
<b>SSL/TLS Listen Port</b>	853 <small>The port used for responding to SSL/TLS DNS queries. It should normally be left blank</small>
<b>Network Interfaces</b>	All WAN LAN VLAN10 VLAN20 <small>Interface IP addresses used by the DNS Resolver for responding to queries from clients used. Queries to addresses not selected in this list are discarded. The default behavior is to</small>