

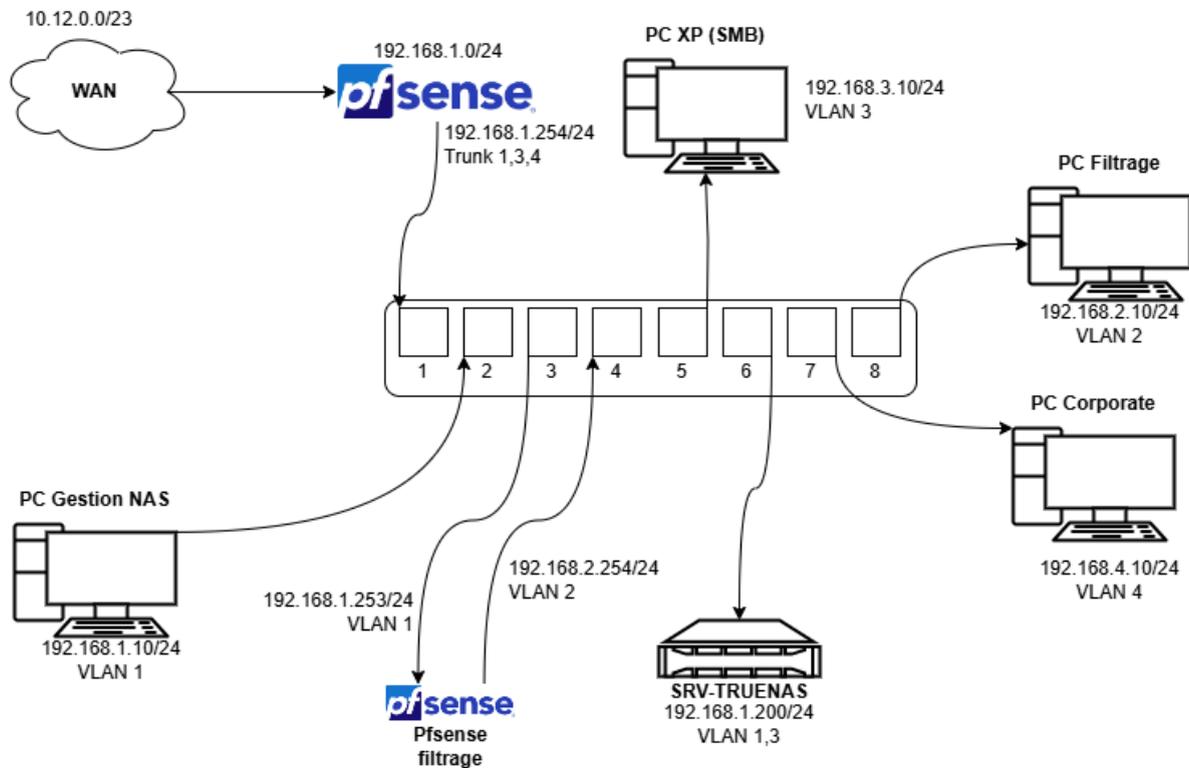
# Rapport de configuration du réseau Laboratoire

---

## Sommaire :

<b>I. Plan du réseau.....</b>	<b>2</b>
<b>II. Adressage réseau IP   VLAN.....</b>	<b>3</b>
1. Adressage IP.....	3
2. VLAN.....	3
<b>III. Configuration des VSwitch.....</b>	<b>4</b>
1. VSwitch WAN.....	4
2. VSwitch LAN.....	5
<b>IV. Configuration du Pfsense frontière.....</b>	<b>6</b>
1. Création des cartes réseau/adressage.....	6
→ Carte WAN.....	6
→ Carte LAN.....	7
Affectation IP sur les cartes via la console.....	9
→ Création VLAN.....	11
<b>V. Création des hôtes.....</b>	<b>14</b>
1. Création des PC Clients.....	14
→ Adressage IP.....	14
→ Adressage VLAN.....	15
2. Création serveur NAS.....	16
→ Configuration réseau NAS.....	21
Configurer un adressage IP TRUENAS.....	21
→ Configuration VLAN.....	23
3. Configuration de la banque de données.....	24
→ Modification ACL.....	28
4. Création du partage SMB.....	29
→ Activation SMBv1.....	30
5. Création des utilisateurs/groupes.....	31
→ Créer un groupe d'utilisateur.....	31
→ Créer un utilisateur.....	32
→ Test de connexion + transfert de données.....	33
<b>VI. Configuration du Pfsense Filtrage.....</b>	<b>36</b>
1. Création carte réseau.....	36
→ Carte WAN.....	36
→ Carte LAN.....	37
2. Adressage IP des cartes.....	38
→ Carte WAN.....	38
→ Interface LAN.....	40
3. Création du proxy.....	42
→ Installation de Squid sur PfSense.....	42
→ Configurer Squid (Proxy) sur PfSense.....	43
→ Créer l'autorité de certification PfSense.....	49
→ SSL Inspection avec Squid.....	49
→ Installation de Squid Guard sur PfSense.....	51
→ Configuration de Squid Guard sur PfSense.....	52
→ Test du proxy.....	57

# I. Plan du réseau



Le **réseau** sera entièrement **virtualisé** sur un **hyperviseur** en **Windows Server 2022**.

## II. Adressage réseau IP | VLAN

### 1. Adressage IP

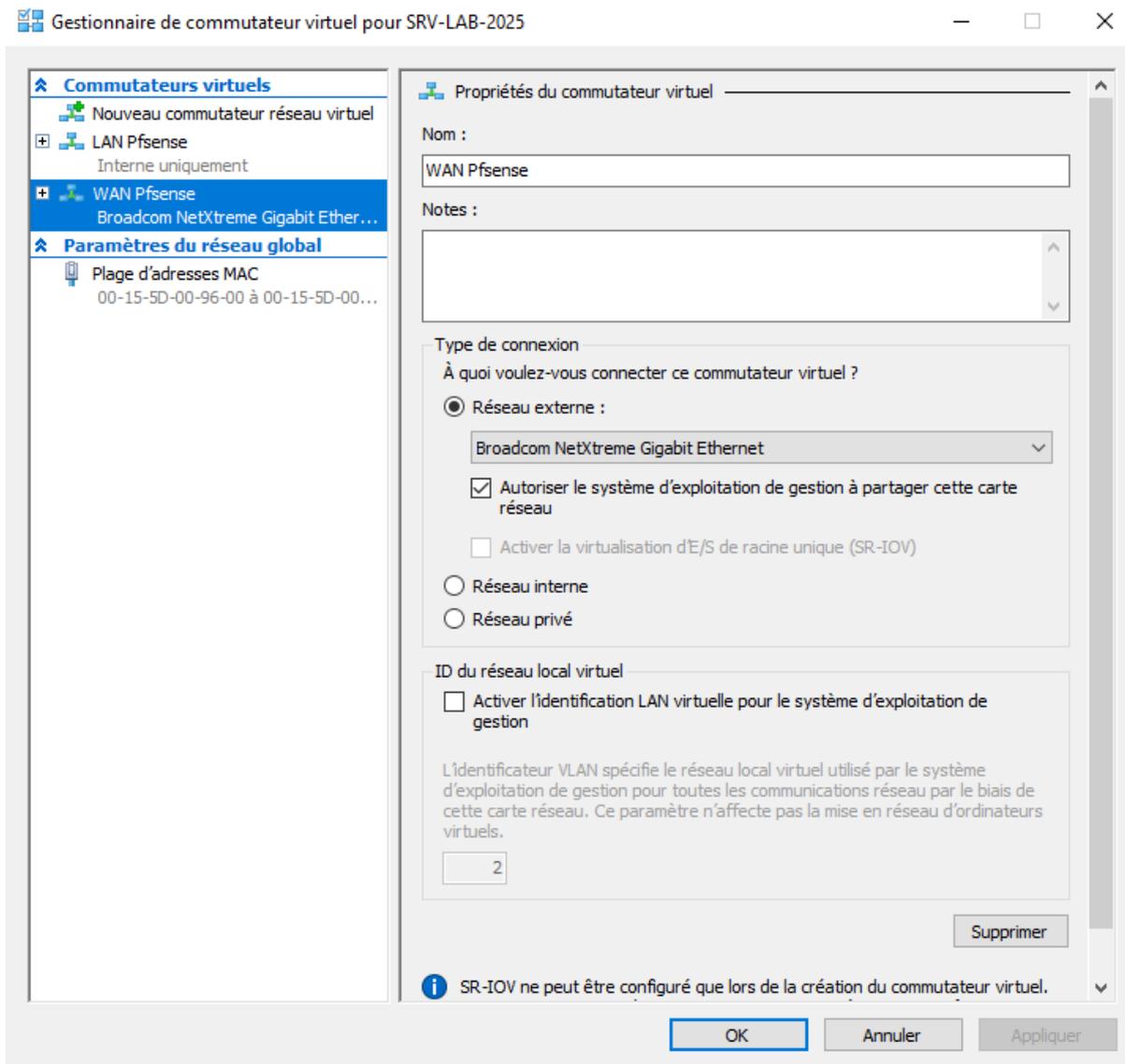
Nom Réseau	Adresse IP	Passerelle	Hôtes
Gestion	192.168.1.0/24	192.168.1.254	- PC Gestion NAS - SRV-TRUENAS
Filtrage	192.168.2.0/24	192.168.2.254	- PC Filtrage
XP	192.168.3.0/24	192.168.3.254	- PC XP
Corporate	192.168.4.0/24	192.168.4.254	- PC Corporate

### 2. VLAN

Réseau	VLAN
192.168.1.0/24	1
192.168.2.0/24	2
192.168.3.0/24	3
192.168.4.0/24	4

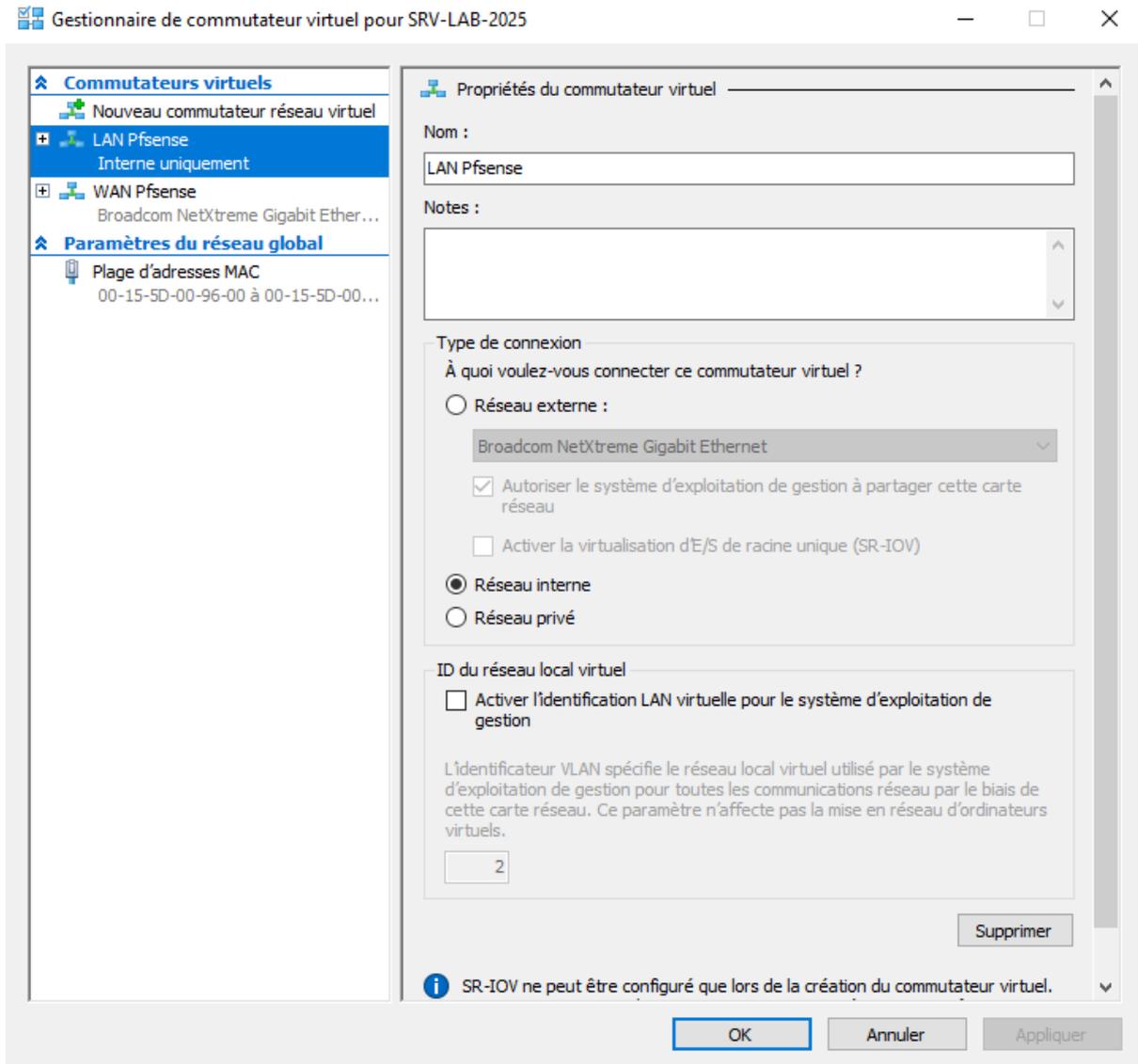
# III. Configuration des VSwitch

## 1. VSwitch WAN



Premièrement, le **VSwitch** côté **WAN** afin de posséder un accès à **internet**, accès par pont via une **carte réseau physique** du serveur sans configuration particulière.

## 2. VSwitch LAN



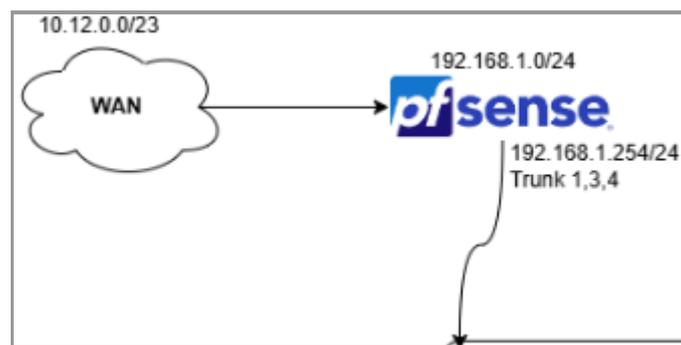
Un **VSwitch** afin de pouvoir y connecter nos **VMs**, en connexion **interne** afin d'isoler notre réseau de l'extérieur mais de pouvoir communiquer nos **VMs** entre elles.

# IV. Configuration du Pfsense frontière

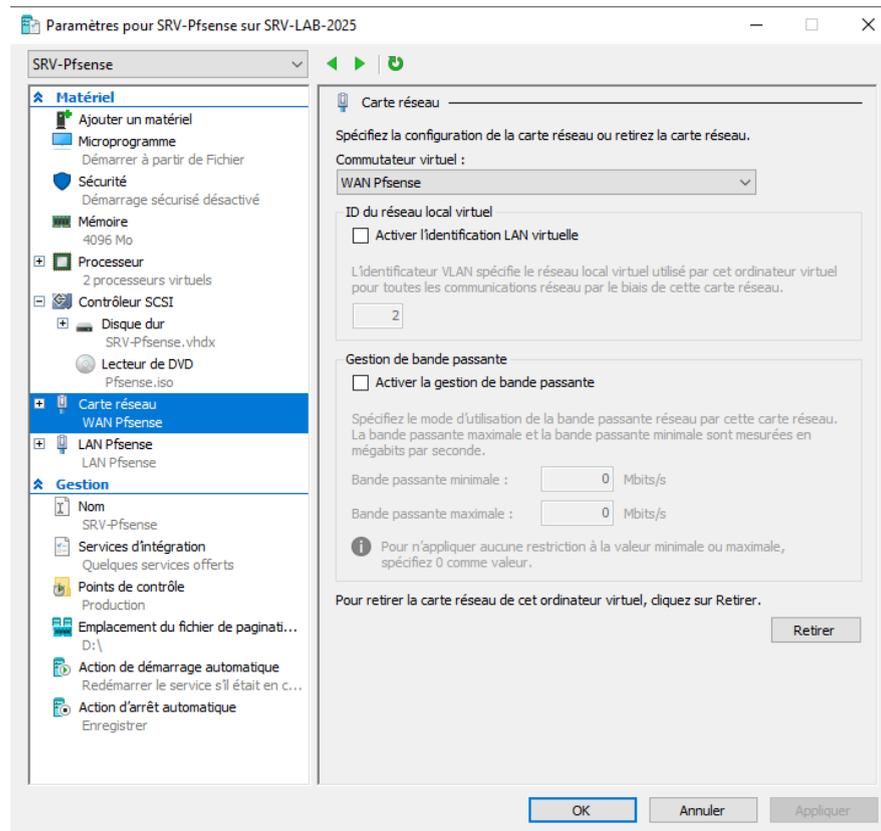
## 1. Création des cartes réseau/adressage

→ Carte WAN

Pour créer notre **Pfsense** frontière entre l'extérieur et l'intérieur de notre réseau, nous avons quelques configurations à réaliser.



Pour la carte **WAN**, on crée une **carte simple** sur notre hyperviseur sans configuration particulière en lui spécifiant le **commutateur WAN** que l'on a créé.



On affecte pas d'**adresse IP fixe**, on laisse la carte en mode **DHCP**.

```
WAN (wan) -> hn0 -> v4/DHCP4: 10.12.0.140/23
```

## → Carte LAN

La création de la carte du côté **LAN** de notre réseau requiert un peu plus de manipulation, il faut tout d'abord créer la **carte réseau** en précisant les **VLAN** auxquels elle va être affectée sur notre **VSwitch**, soit le **VLAN 1, 3 et 4**.

Pour pouvoir créer un **lien agrèger** sur notre **carte réseau**, il faut la créer via **Powershell** :

```
Add-VMNetworkadapter -VMName "nomVM" -Name "nomAdaptateur"
```

Ce qui nous donne dans notre exemple :

```
Add-VMNetworkadapter -VMName "SRV-Pfsense" -Name "LAN Pfsense"
```

Et par la suite, on **agrège** les **VLAN** à notre **carte** :

```
set-VMNetworkAdapterVlan -VMName "nomVM" -VMNetworkAdapterName  
"nomadaptateur" -Trunk -AllowedVlanIdList "numéroVLAN"  
-NativeVlanId numéroVLANnatif
```

Ce qui nous donne dans notre exemple :

```
set-VMNetworkAdapterVlan -VMName "SRV-Pfsense"  
-VMNetworkAdapterName "LAN Pfsense" -Trunk -AllowedVlanIdList "3,4"  
-NativeVlanId 1
```

On peut vérifier par la suite si notre commande à bien marché en exécutant la commande :

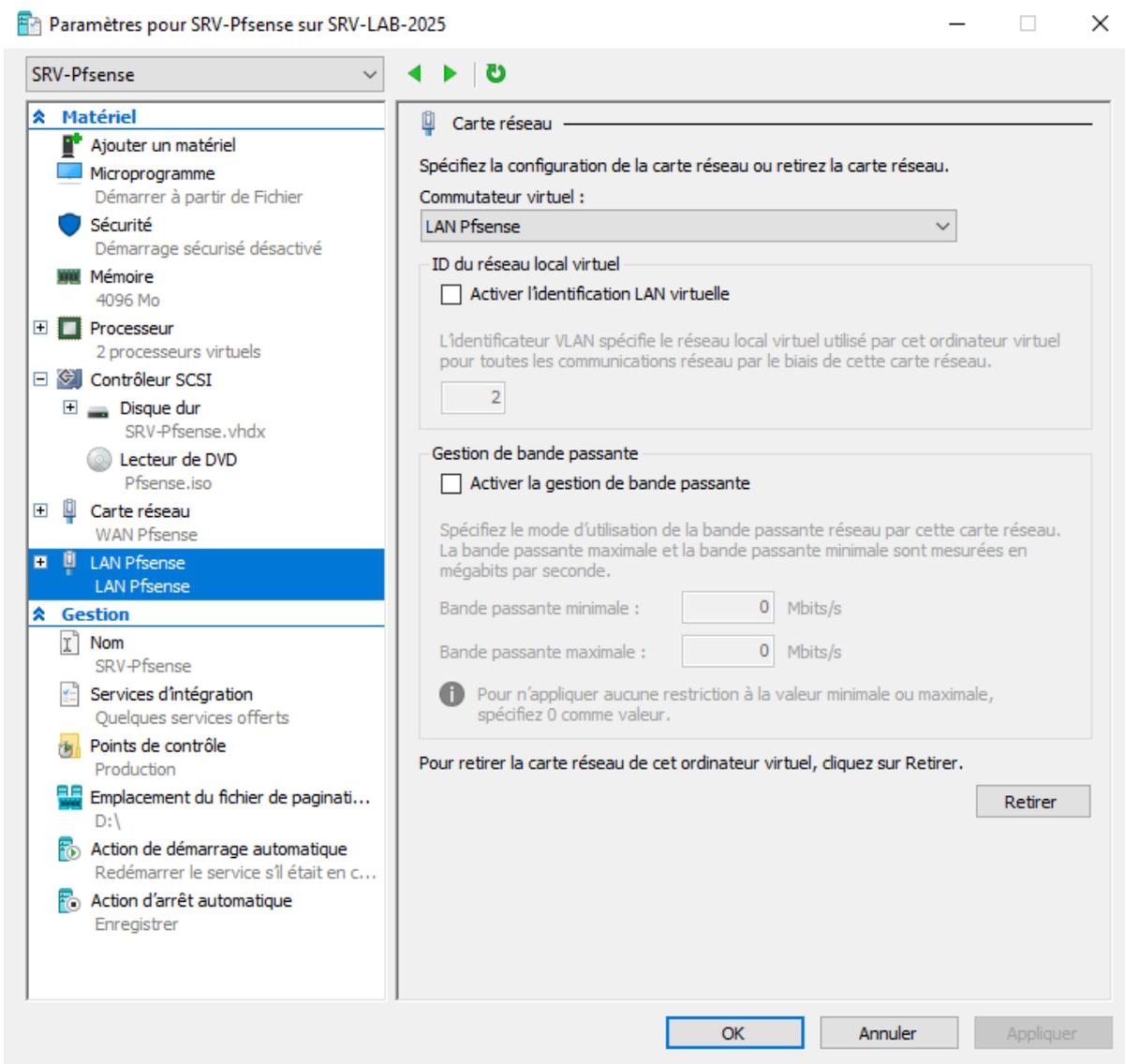
```
Get-VMNetworkAdapterVlan -VMName "SRV-TRUENAS"
```

```
PS C:\Users\Administrateur> Get-VMNetworkAdapterVlan -VMName SRV-Pfsense
```

VMName	VMNetworkAdapterName	Mode	VlanList
SRV-Pfsense	Carte réseau	Untagged	
SRV-Pfsense	LAN Pfsense	Trunk	1,3-4

On voit notre première carte (**WAN**) en mode **'Untagged'** (affectée à aucun **VLAN**).

Et on voit notre deuxième carte (**LAN**) en mode **'Trunk'** sur les **VLAN 1, 3 et 4**.



On vérifie aussi qu'elle est bien créée et on affecte cette carte à notre **VSwitch LAN** créé précédemment.

Par la suite, on y affecte une **adresse IP** via la **console**.

```
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system             14) Enable Secure Shell (sshd)
6) Halt system              15) Restore recent configuration
7) Ping host                16) Restart PHP-FPM
8) Shell
Enter an option: 2

Available interfaces:

1 - WAN (hn0 - dhcp, dhcp6)
2 - LAN (hn1 - static)
3 - LAN_XP (hn1.3 - static)
4 - LAN_CORPORATE (hn1.4 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
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):
> 24

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

Configure IPv6 address LAN interface via DHCP6? (y/n) n

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

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

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.1.254/24
You can now access the webConfigurator by opening the following URL in your web browser:

    https://192.168.1.254/

Press <ENTER> to continue.█
```

## Explication :

1. On tape **2** pour choisir la troisième option du système '**Set interface(s) IP address**'.
2. On tape sur **2** encore une fois pour sélectionner la deuxième **carte réseau**.
3. À ce moment-là, **Pfsense** demande quelle est l'adresse que l'on veut affecter à notre **carte réseau** (cette adresse sera la **passerelle** de notre réseau), d'après notre schéma réseau on y affecte l'adresse '**192.168.1.254**'.
4. **Pfsense** nous demande le **masque** de notre réseau en format **CIDR**, on choisit **24** dans notre cas pour un réseau local **classe C**.
5. Ici, vu que l'on configure une interface **LAN**, on passe cette étape en appuyant sur '**Entrer**'.
6. Dans notre cas, on ne veut pas d'adresse en format **IPV6**, on appuie sur '**N**' pour ne pas activer le serveur **DHCP en IPV6**.
7. Par la suite, on nous demande si on veut activer le serveur **DHCP en IPV4**, dans notre cas, on ne veut tout simplement pas de **DHCP** dans le réseau donc on appuie encore une fois '**N**'.
8. La dernière question nous demande si l'on veut désactiver l'accès à l'interface web en **HTTPS**, bien sûr on répond **non** à des fins de sécurité.

On appuie sur la touche '**Entrer**' et voici notre **carte LAN** configurée et fonctionnelle.

```
LAN (lan)      -> hn1      -> v4: 192.168.1.254/24
```

## → Création VLAN

Pour créer les **VLAN**, on va le faire via le **terminal de PfSense**.

```
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system             14) Enable Secure Shell (sshd)
6) Halt system               15) Restore recent configuration
7) Ping host                 16) Restart PHP-FPM
8) Shell
Enter an option: 1

Valid interfaces are:

hn0      00:15:5d:00:96:1e   (up) Hyper-V Network Interface
hn1      00:15:5d:00:96:1f (down) Hyper-V Network Interface

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y/n]? y

VLAN Capable interfaces:

hn0      00:15:5d:00:96:1e   (up)
hn1      00:15:5d:00:96:1f   (up)

Enter the parent interface name for the new VLAN (or nothing if finished): hn1
Enter the VLAN tag (1-4094): 3

VLAN Capable interfaces:

hn0      00:15:5d:00:96:1e   (up)
hn1      00:15:5d:00:96:1f   (up)

Enter the parent interface name for the new VLAN (or nothing if finished): hn1
Enter the VLAN tag (1-4094): 4

VLAN Capable interfaces:

hn0      00:15:5d:00:96:1e   (up)
hn1      00:15:5d:00:96:1f   (up)

Enter the parent interface name for the new VLAN (or nothing if finished): █
```

Enter the parent interface name for the new VLAN (or nothing if finished):

VLAN interfaces:

```
hn1.3          VLAN tag 3, parent interface hn1
hn1.4          VLAN tag 4, parent interface hn1
```

If the names of the interfaces are not known, auto-detection can be used instead. To use auto-detection, please disconnect all interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection (hn0 hn1 hn1.3 hn1.4 or a): hn0

Enter the LAN interface name or 'a' for auto-detection NOTE: this enables full Firewalling/NAT mode. (hn1 hn1.3 hn1.4 a or nothing if finished): hn1

Enter the Optional 1 interface name or 'a' for auto-detection (hn1.3 hn1.4 a or nothing if finished): hn1.3

Enter the Optional 2 interface name or 'a' for auto-detection (hn1.4 a or nothing if finished): hn1.4

The interfaces will be assigned as follows:

```
WAN  -> hn0
LAN  -> hn1
OPT1 -> hn1.3
OPT2 -> hn1.4
```

Do you want to proceed [y|n]? █

Writing configuration...done.

One moment while the settings are reloading... done!

Hyper-V Virtual Machine - Netgate Device ID: 5f9d636c17f32dfd35c6

\*\*\* Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense \*\*\*

```
WAN (wan)      -> hn0          -> v4/DHCP4: 10.12.0.150/23
LAN (lan)      -> hn1          -> v4: 192.168.1.254/24
OPT1 (opt1)    -> hn1.3         ->
OPT2 (opt2)    -> hn1.4         ->
```

```
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

Enter an option: █

## Explication :

1. On tape **1** pour choisir l'option '**Assign Interfaces**' afin d'assigner de nouvelles interfaces virtuelles pour nos **VLAN**.
2. **Pfsense** nous demande si l'on veut déployer des **VLAN** maintenant, on tape '**y**' pour **yes**.
3. Par la suite, **Pfsense** veut savoir quelle est la carte réseau qui va être parente de nos interfaces virtuelles, on veut créer nos interfaces virtuelles sur le **LAN**, on sélectionne donc la carte **LAN** en tapant son identifiant (soit '**hn1**' dans notre exemple).
4. À ce moment-là, on nous demande quel **ID** on veut donner à notre **VLAN**, d'après notre tableau et notre schéma, ce **Pfsense** doit avoir un **trunk** sur 3 **VLAN (VLAN 1, 3, 4)**, la carte réseau physique de notre **Pfsense** est de base configurée sur le **VLAN 1** (d'où l'adressage en **192.168.1.0** qu'on lui a donnée), il nous reste donc qu'à créer le **VLAN 3** et **VLAN 4**.
5. À chaque fois, on a juste à sélectionner l'interface où l'on veut créer nos interfaces virtuelles et taper l'**ID** du **VLAN** que l'on veut créer sur cette interface. Quand c'est fini, appuyer sur '**Entrer**'.
6. À cet instant, il faut que l'on '**catégorise**' nos interfaces, récapitulons :
  - a. **HNO -> WAN**
  - b. **HN1 -> LAN (VLAN 1)**
  - c. **HN1.3 -> LAN (VLAN 3)**
  - d. **HN1.4 -> LAN (VLAN 4)**
    - On procède donc dans cet ordre, en premier on nous demande l'interface **WAN** donc on tape **HNO**.
    - En deuxième, notre interface **LAN parente** donc **HN1**.
    - En troisième, notre interface **LAN du VLAN 3** donc **HN1.3**.
    - En quatrième, notre interface **LAN du VLAN 4** donc **HN1.4**.
7. Pour que nos **VLAN** soient assignés à une adresse **IP**, on suit la procédure d'assignation comme les autres cartes.

# V. Création des hôtes

## 1. Création des PC Clients

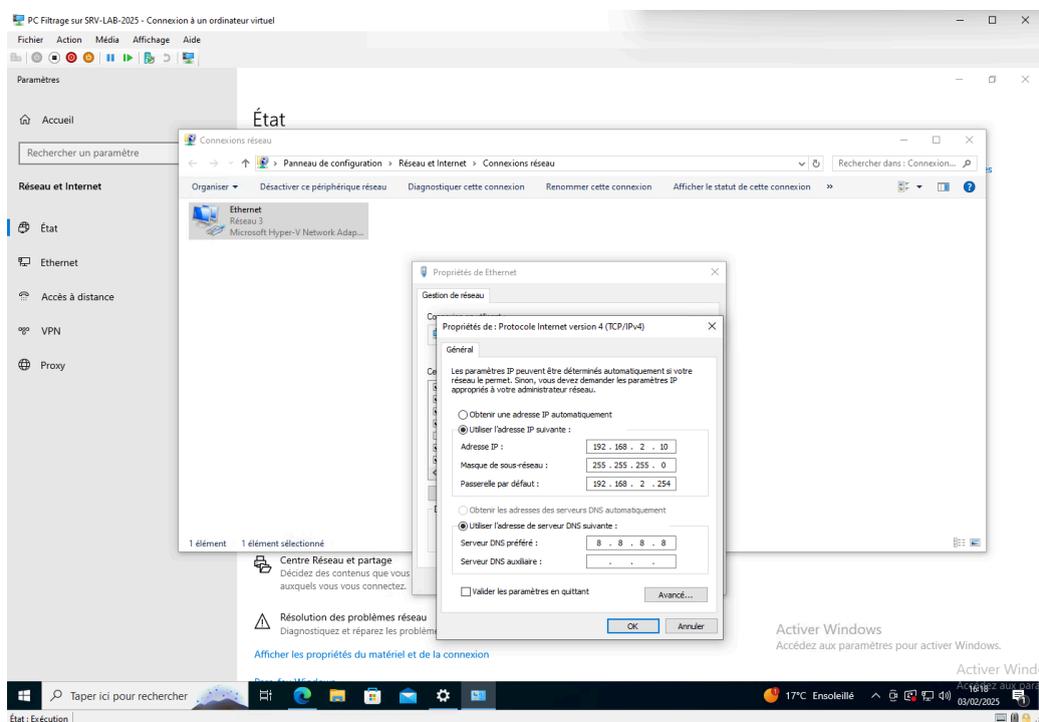
→ Adressage IP

Les **PC clients** sont tous des clients **Windows 10 Pro**, cependant sur notre infrastructure chaque poste contient un **adressage IP** différent.

Nom d'hôte	Adresse IP	Passerelle	N°VLAN
PC Gestion NAS	192.168.1.10 /24	192.168.1.254	1
PC Filtrage	192.168.2.10 /24	192.168.2.254	2
PC XP	192.168.3.10 /24	192.168.3.254	3
PC Corporate	192.168.4.10 /24	192.168.4.254	4

Pour chaque **PC** :

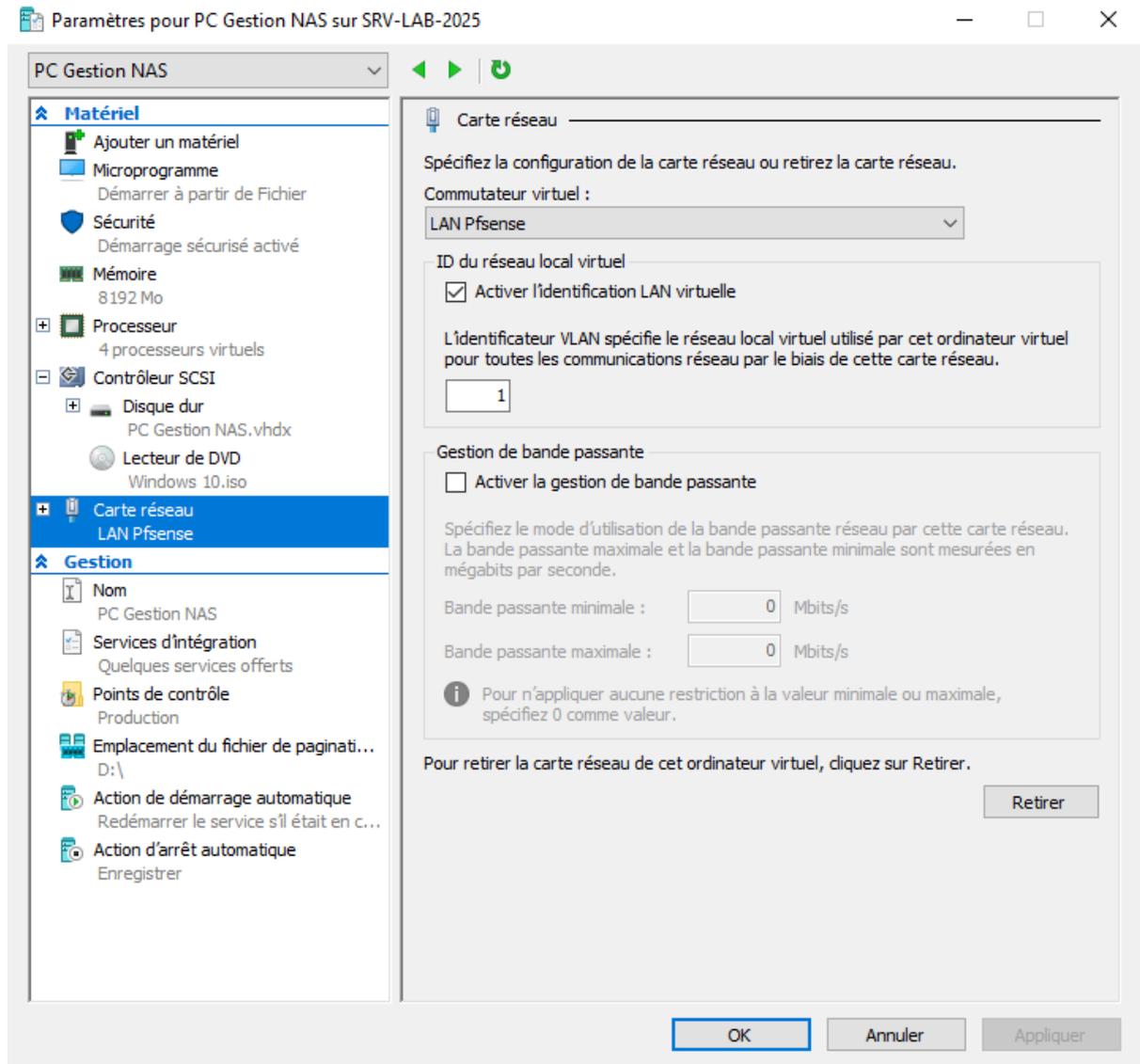
**Clic droit** sur le logo **internet** -> **Ouvrir paramètre** et **Internet** -> **Modifier les options d'adaptateur** -> **Clic droit** sur la **carte réseau** -> **Propriété** -> double clic sur **Protocole Internet Version 4 (TCP / IPv4)**.



On sélectionne **“utiliser l'adresse IP suivante”** et on rentre l'adresse pour chaque **hôte** comme convenu dans le tableau. Dû à l'absence de **serveur DNS** dans notre réseau, on préférera utiliser **8.8.8.8** pour assurer l'accès à internet (**DNS Google**).

## → Adressage VLAN

Pour pouvoir affecter chaque **carte réseau** à leurs **VLAN**, il faut pour chaque **hôte** :



On affecte ici pour chaque poste son **VLAN**, dans mon exemple **PC Gestion NAS** sur le **VLAN 1**.

## 2. Création serveur NAS



**Attention** à bien enlever le **démarrage sécurisé**.

The screenshot shows a terminal window titled "o sur SRV-LAB-2025 - Connexion à un ordinateur virtuel". The terminal displays the TrueNAS logo and the "TrueNAS Installer" menu. The menu options are:

```
1. Boot TrueNAS Installer [Enter]           :dd dd:
2. Boot TrueNAS Installer (Serial Console)  :ddMdd dMdd::
3. Escape to loader prompt                 :dMMMMMdd :dMMMMMdd::
4. Reboot                                   :ddMdd ::: ddMdd :
Options:                                    Md: : :dMMMM: : :dd
5. Kernel: default/kernel (1 of 1)         MddMdd : :dMMMM: :dMMMM
6. Boot Options                             :dMMMMMdd ::: :dMMMMMdd
                                           :dMMMMMdd :dMMMMMdd:
                                           :ddMdd dMdd:
                                           :dd dd:\
```

Below the menu, it says "Autoboot in 6 seconds. [Space] to pause". The status bar at the bottom indicates "État: Exécution".

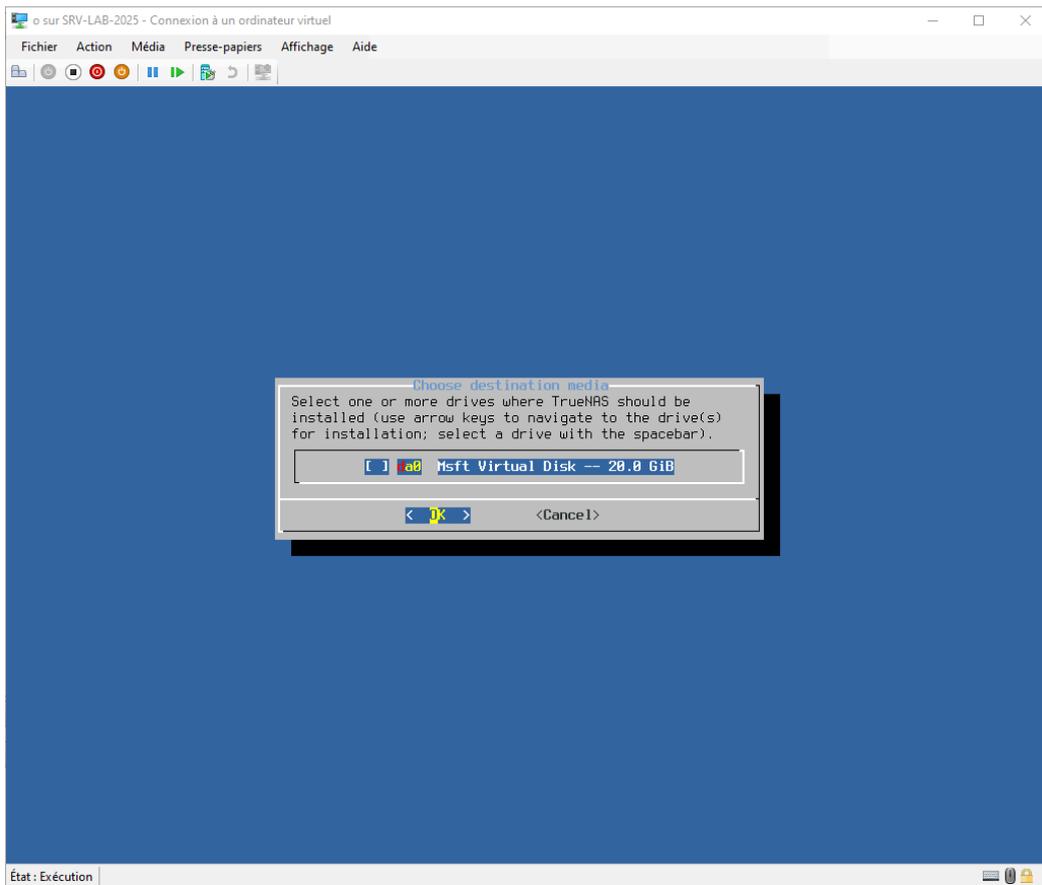
On clique sur 1 pour **procéder à l'installation** :

The screenshot shows a terminal window titled "o sur SRV-LAB-2025 - Connexion à un ordinateur virtuel". The terminal displays the "TrueNAS 13.0-U6.7 Console Setup" menu. The menu options are:

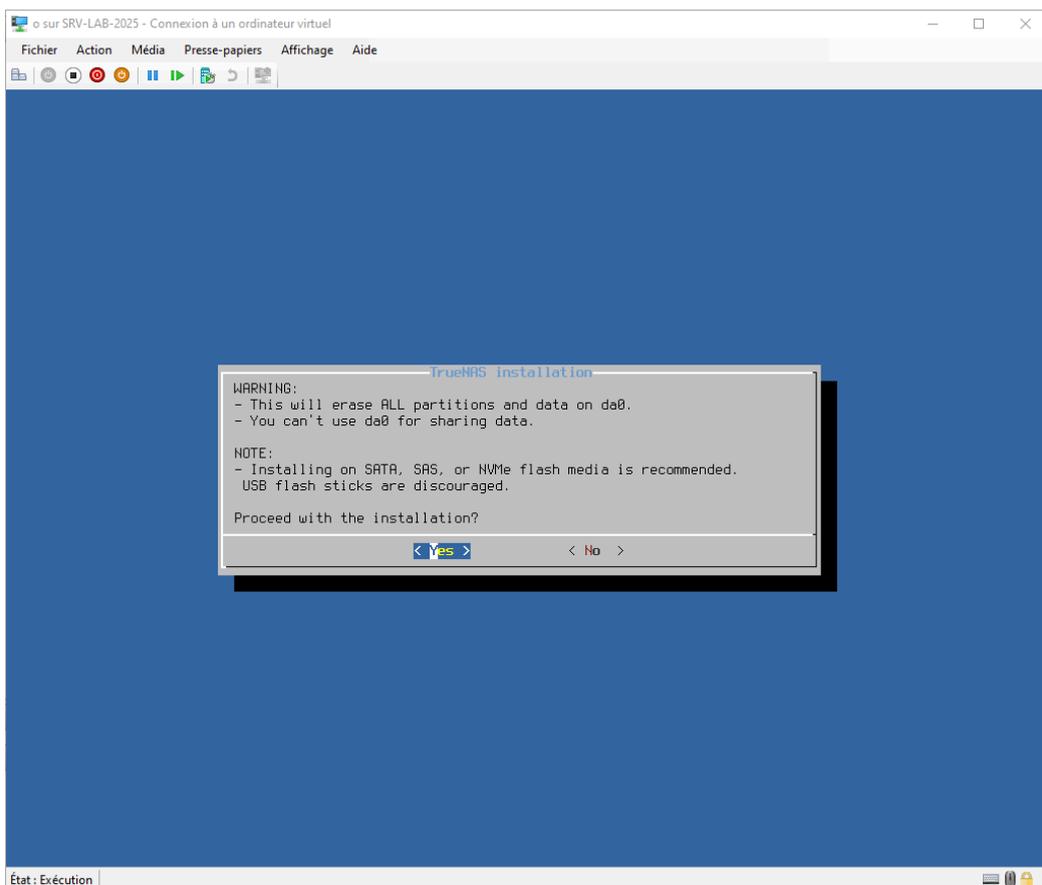
```
1 Install/Upgrade
2 Shell
3 Reboot System
4 Shutdown System
```

At the bottom, there are navigation options: "< OK >" and "<Cancel>". The status bar at the bottom indicates "État: Exécution".

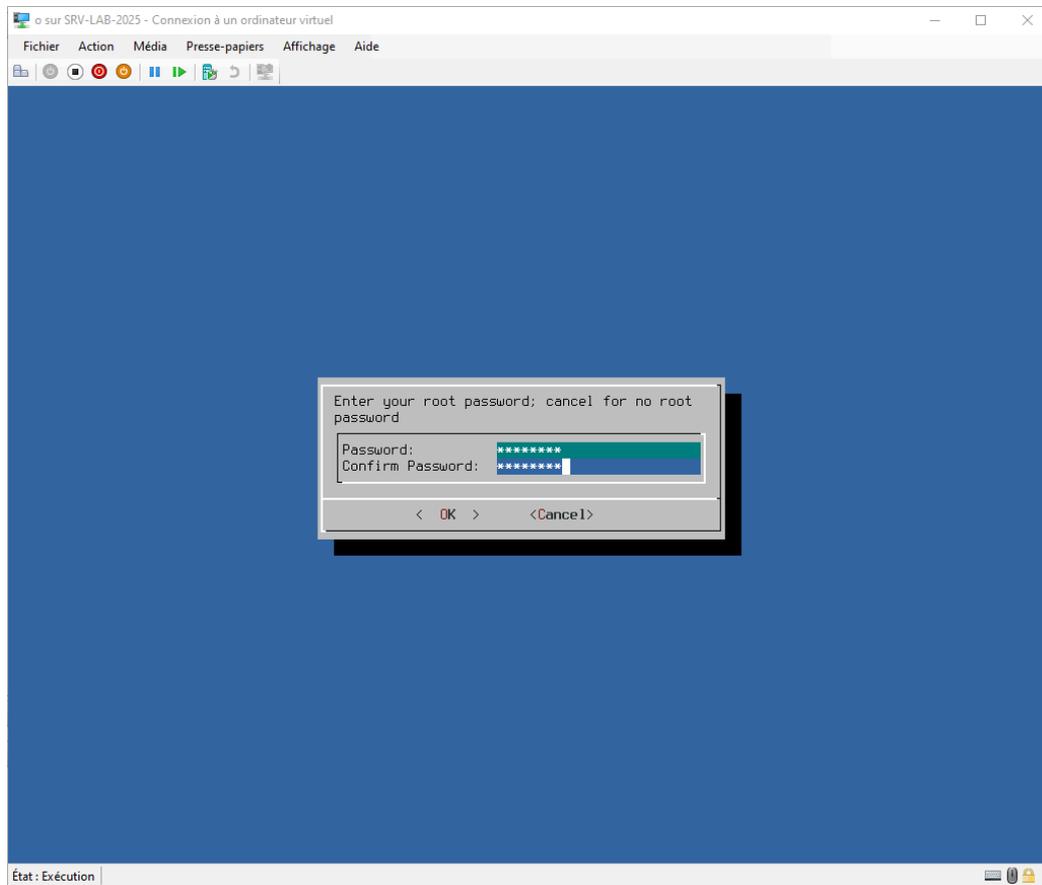
On sélectionne le **seul disque** que l'on a monté comme **disque d'OS**



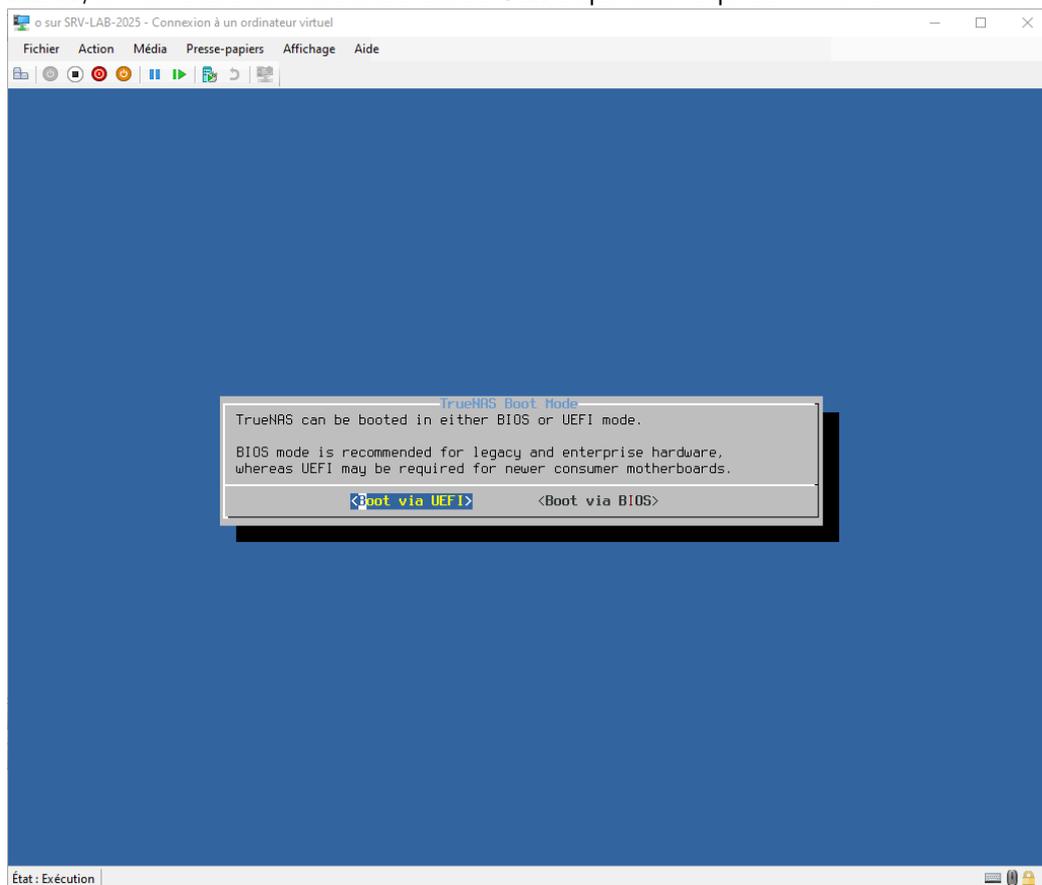
On sélectionne **'Yes'** comme quoi on est bel et bien conscient que l'on va effacer toutes les **données** présentes sur le **disque dur** pour l'installation.



On rentre un **mot de passe** qui sera le mot de passe **administrateur** du serveur ainsi que le mot de passe servant à l'**authentification** sur la page web de management.



**Par la suite**, on choisit le mode de boot **UEFI** qui est le plus récent.

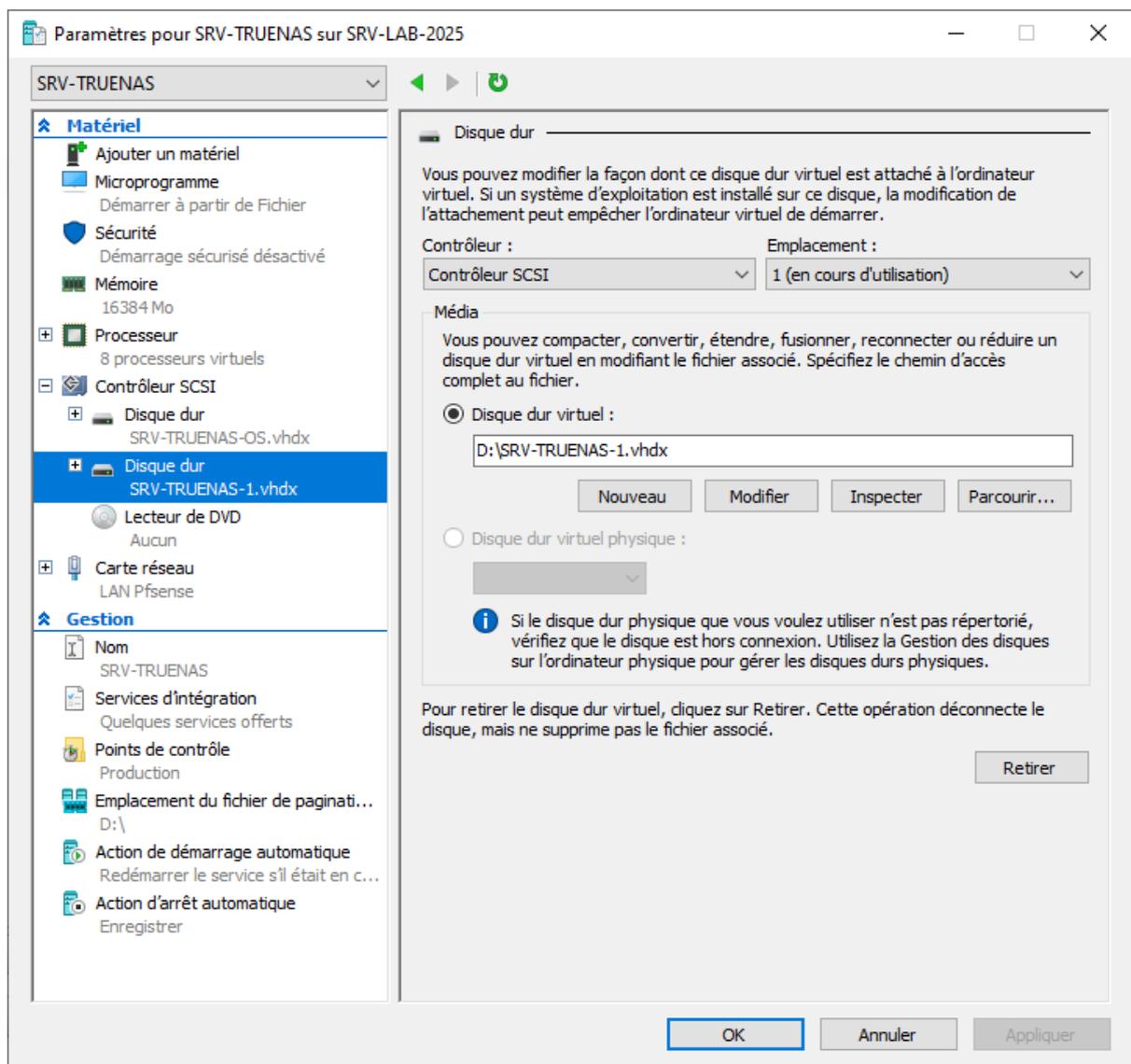


The TrueNAS installation on ada0 succeeded!  
Please reboot and remove the installation media.

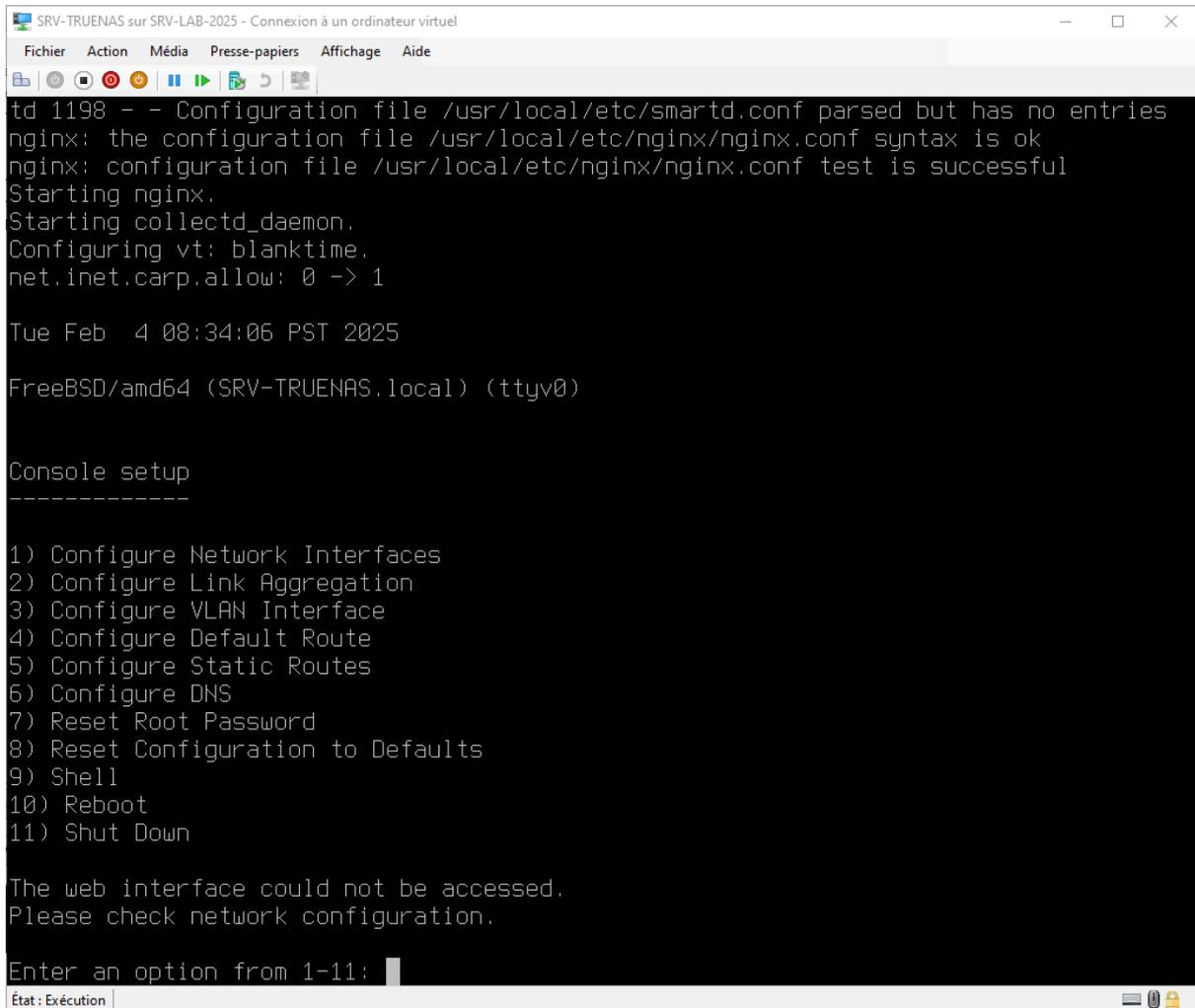
< OK >

## L'installation est terminée !

On éteint le serveur, on enlève l'ISO du lecteur DVD et l'on ajoute le **disque dur** qui servira à stocker les données de notre partage, puis on démarre le serveur.



Après le redémarrage du serveur, on tombe sur cette page :



```
SRV-TRUENAS sur SRV-LAB-2025 - Connexion à un ordinateur virtuel
Fichier Action Média Presse-papiers Affichage Aide
td 1198 -- Configuration file /usr/local/etc/smartd.conf parsed but has no entries
nginx: the configuration file /usr/local/etc/nginx/nginx.conf syntax is ok
nginx: configuration file /usr/local/etc/nginx/nginx.conf test is successful
Starting nginx.
Starting collectd_daemon.
Configuring vt: blanktime.
net.inet.carp.allow: 0 -> 1

Tue Feb  4 08:34:06 PST 2025

FreeBSD/amd64 (SRV-TRUENAS.local) (ttyv0)

Console setup
-----

1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset Configuration to Defaults
9) Shell
10) Reboot
11) Shut Down

The web interface could not be accessed.
Please check network configuration.

Enter an option from 1-11: |
```

On constate que le serveur ne possède **aucune adresse IP** d'où le message **“The web interface could not be accessed, please check network configuration”**.

Pour y remédier, on va procéder comme ceci :

## → Configuration réseau NAS

### Configurer un adressage IP TRUENAS

```
Console setup
-----

1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset Configuration to Defaults
9) Shell
10) Reboot
11) Shut Down

The web interface could not be accessed.
Please check network configuration.

Enter an option from 1-11: 1
1) hn0
Select an interface (q to quit): 1
Remove the current settings of this interface? (This causes a momentary disconnection
of the network.) (y/n) n
Configure interface for DHCP? (y/n) n
Configure IPv4? (y/n) y
Interface name:hn0
Several input formats are supported
Example 1 CIDR Notation:
  192.168.1.1/24
Example 2 IP and Netmask separate:
  IP: 192.168.1.1
  Netmask: 255.255.255.0, /24 or 24
IPv4 Address:192.168.1.200/24
Saving interface configuration: Ok
Configure IPv6? (y/n) n
Restarting network: ok

Console setup
-----

1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset Configuration to Defaults
9) Shell
10) Reboot
11) Shut Down

The web user interface is at:

http://192.168.1.200
https://192.168.1.200

Enter an option from 1-11: S
```

### Explication :

1. On tape **'1'** pour choisir la fonction **"Configure Network Interfaces"** afin de pouvoir configurer nos interfaces réseaux.
2. Vu que nous avons qu'une seule carte réseau est présente sur notre serveur, on **tape '1'** encore une fois pour **sélectionner la carte réseau 'Hn0'**
3. On choisit l'option **'N'** car nous ne **voulons pas supprimer** les **paramètres réseaux** mais seulement les **remplacer**.
4. On ne veut **pas configurer l'interface** en mode **DHCP** vu que celui-ci est **désactiver** sur notre **LAN**
5. On veut **configurer** notre interface en **IPv4** donc on tape **'Y'**
6. On peut **renommer** le **nom de l'interface** sur notre système, ici, inutile de changer donc on retape **'hn0'**.
7. A partir de ce moment la on **renseigne l'adresse IP** que nous voulons **assigner à notre serveur** soit **'192.168.1.200/24'** conformément au [schéma réseau](#)
8. On ne veut **pas d'adressage IPv6**, donc on tape **'N'** pour **refuser**
9. La **configuration réseau est finie**, on peut voir que nos **interfaces redémarrent** et que l'**adressage est bien pris en compte**

## → Configuration VLAN

Notre serveur **NAS** doit être accessible par le **VLAN 1** et le **VLAN 3** comme indiqué sur le plan. Actuellement, il est configuré seulement pour être accessible sur le **VLAN 1**, pour y remédier, on va configurer notre carte existante en mode **'TRUNK'**.

On va procéder quasiment de la même manière que pour le **TRUNK** du serveur **Pfsense**, cependant, notre carte réseau existe déjà, donc pas besoin de la créer. Il faut juste agréer les **VLAN 1** et **3** à la carte. :

```
set-VMNetworkAdapterVlan -VMName SRV-TRUENAS -VMNetworkAdapterName  
"Carte réseau" -Trunk -AllowedVlanIdList "3" -NativeVlanId 1
```

On peut **vérifier** par la suite si **notre commande** a bien été prise en compte **avec la commande** :

```
Get-VMNetworkAdapterVlan -VMName SRV-TRUENAS
```

```
PS C:\Users\Administrateur> Get-VMNetworkAdapterVlan -VMName SRV-TRUENAS  
  
VMName      VMNetworkAdapterName Mode  VlanList  
-----  
SRV-TRUENAS Carte réseau      Trunk 1,3
```

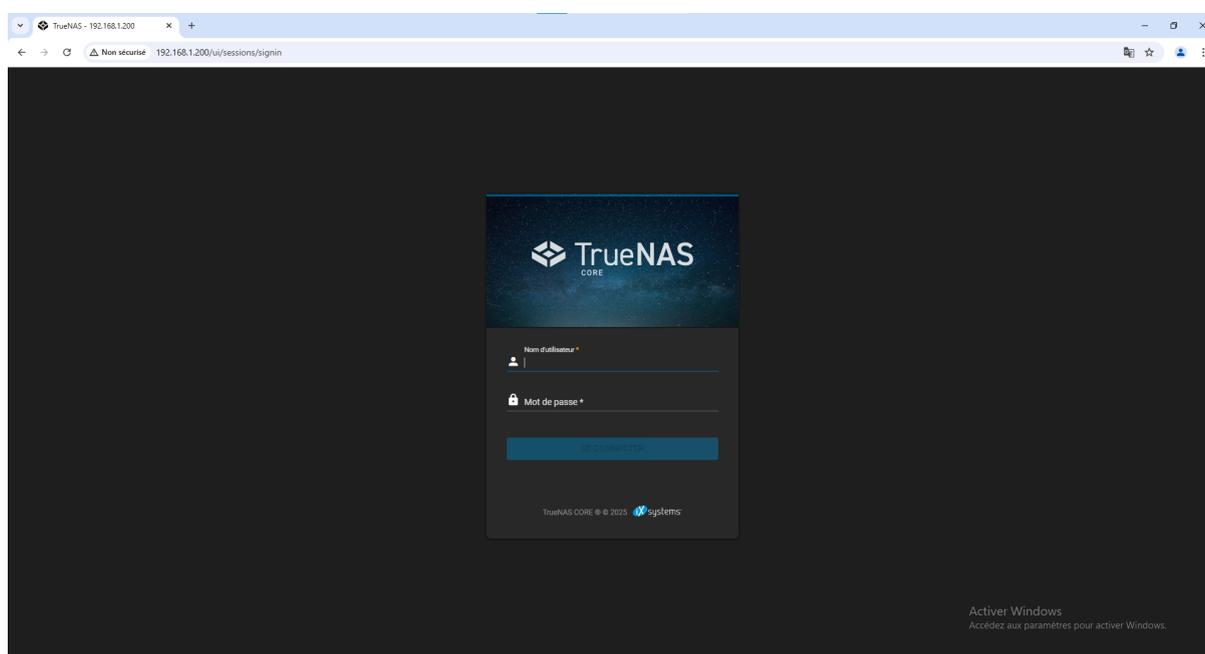
Notre **TRUNK** est bien créé et fonctionnel !

### 3. Configuration de la banque de données

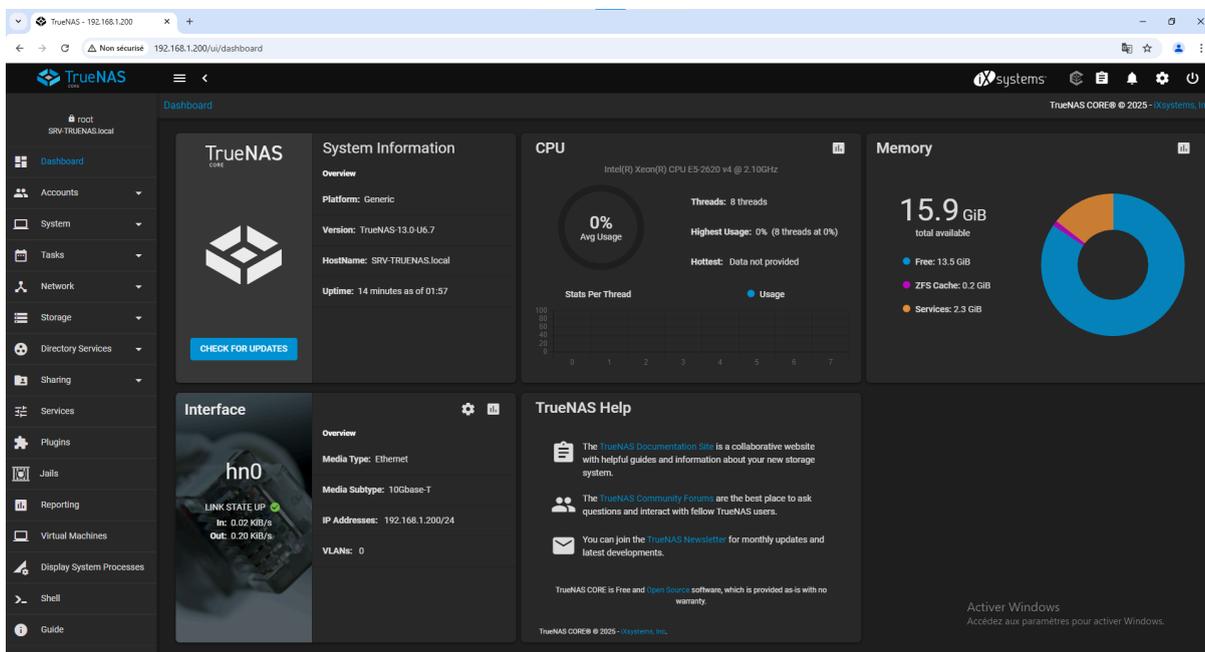
Pour pouvoir configurer un **partage** sur notre serveur, nous devons nous connecter sur l'**interface WEB** de **TRUENAS**.

Pour s'y faire, on se connecte à l'hôte '**PC Gestion NAS**' et on ouvre une page web en tapant l'adresse IP de notre **NAS** dans la barre de recherche.

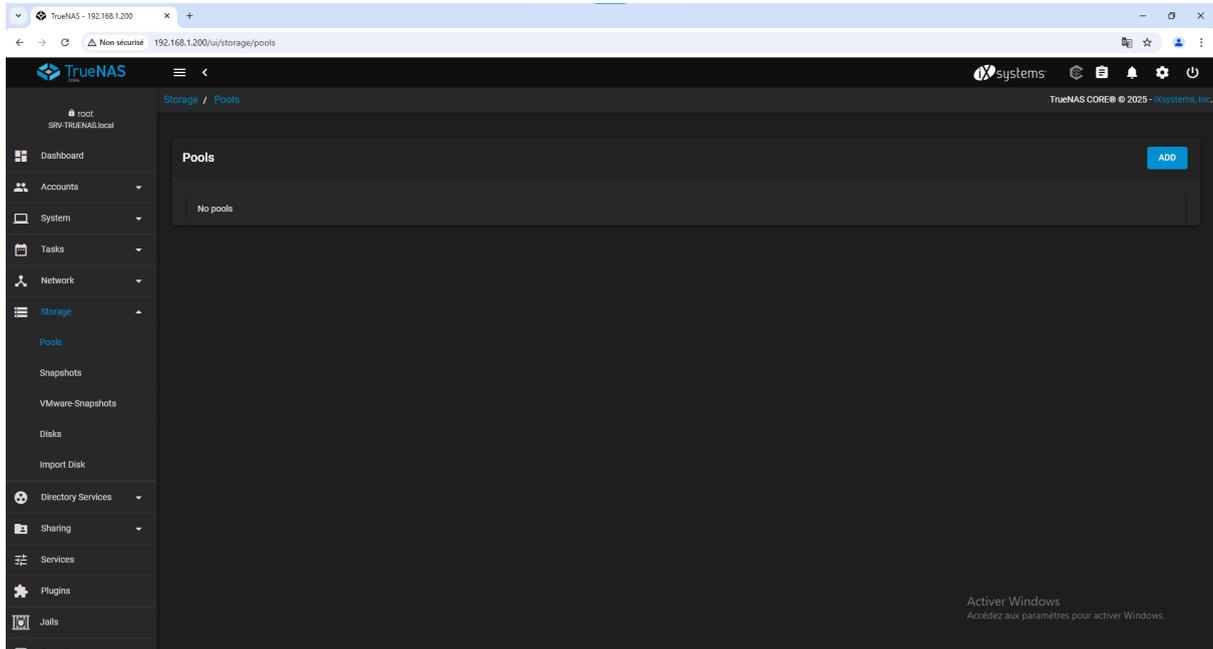
Ici, le nom d'utilisateur par défaut est '**root**' et le mot de passe est celui que l'on a tapé pendant l'installation de **TRUENAS**.



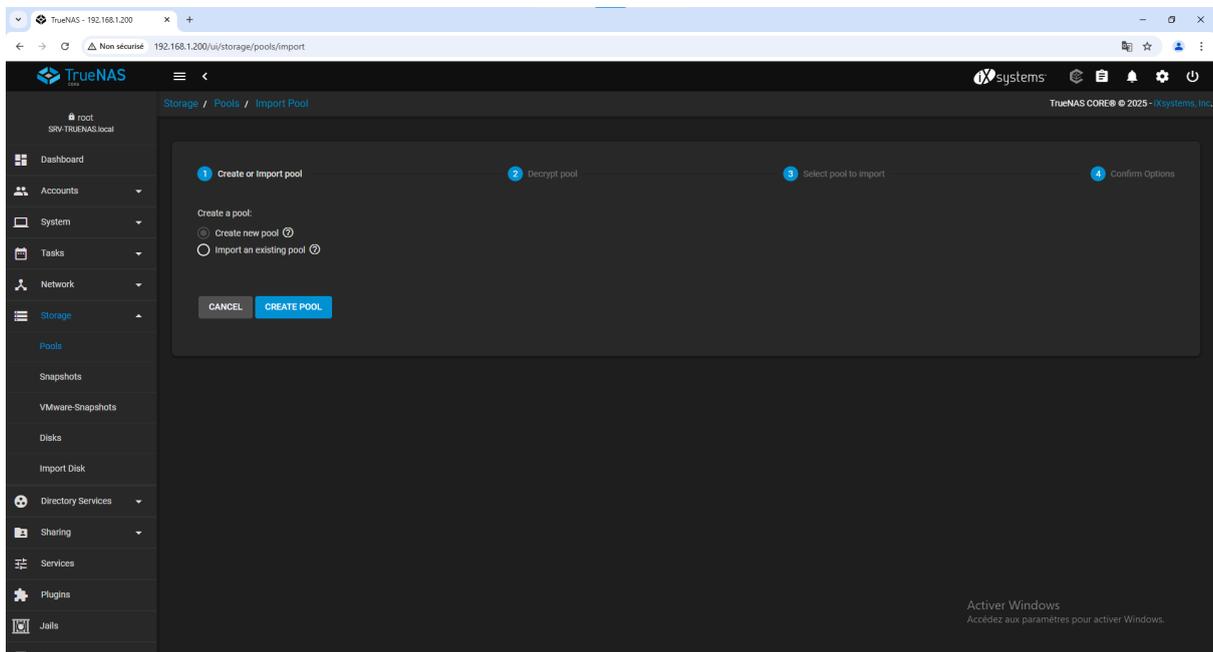
On se retrouve sur la **page d'administration** de notre serveur :



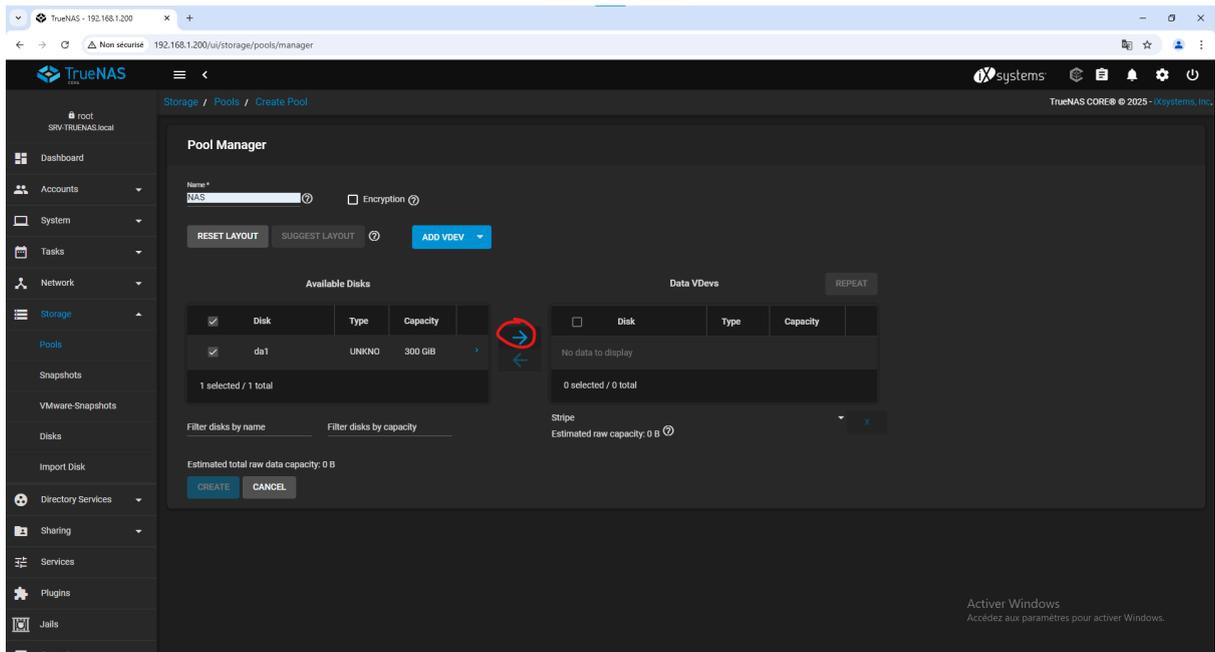
Tout d'abord, on va créer un **groupe de disques ( Pool )**, pour s'y faire il faut se rendre dans le menu **Storage -> Pools** :



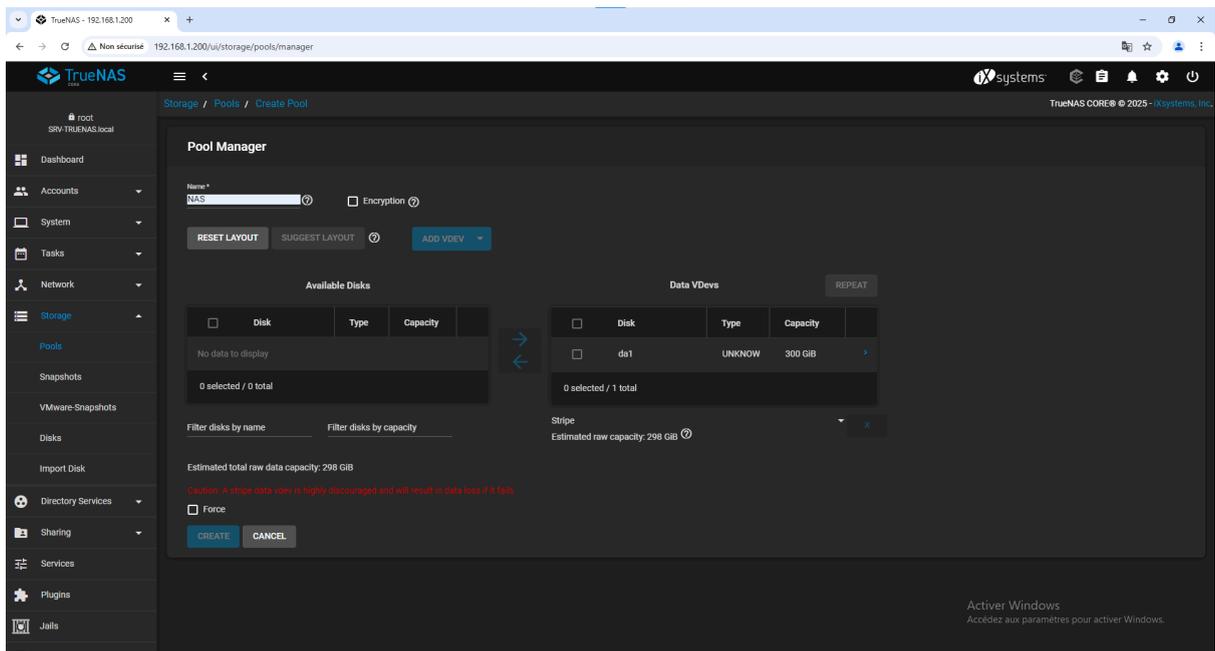
On clique sur **ADD** afin de **créer un pool** :



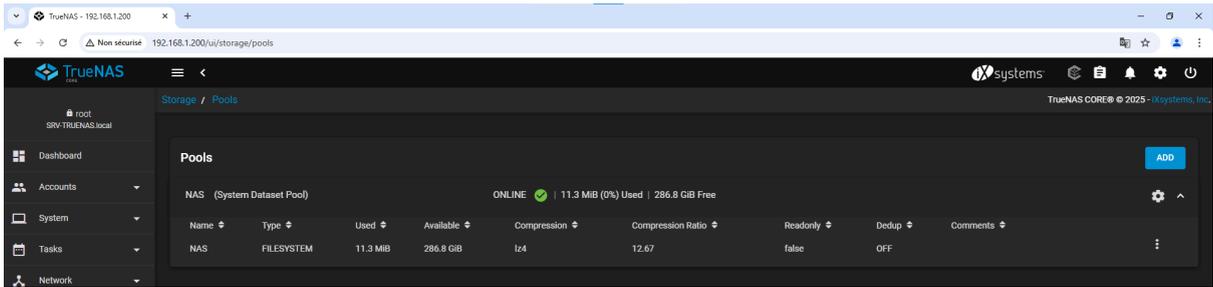
On a le choix entre **créer ou importer** un **pool**, on choisit de **créer un pool**



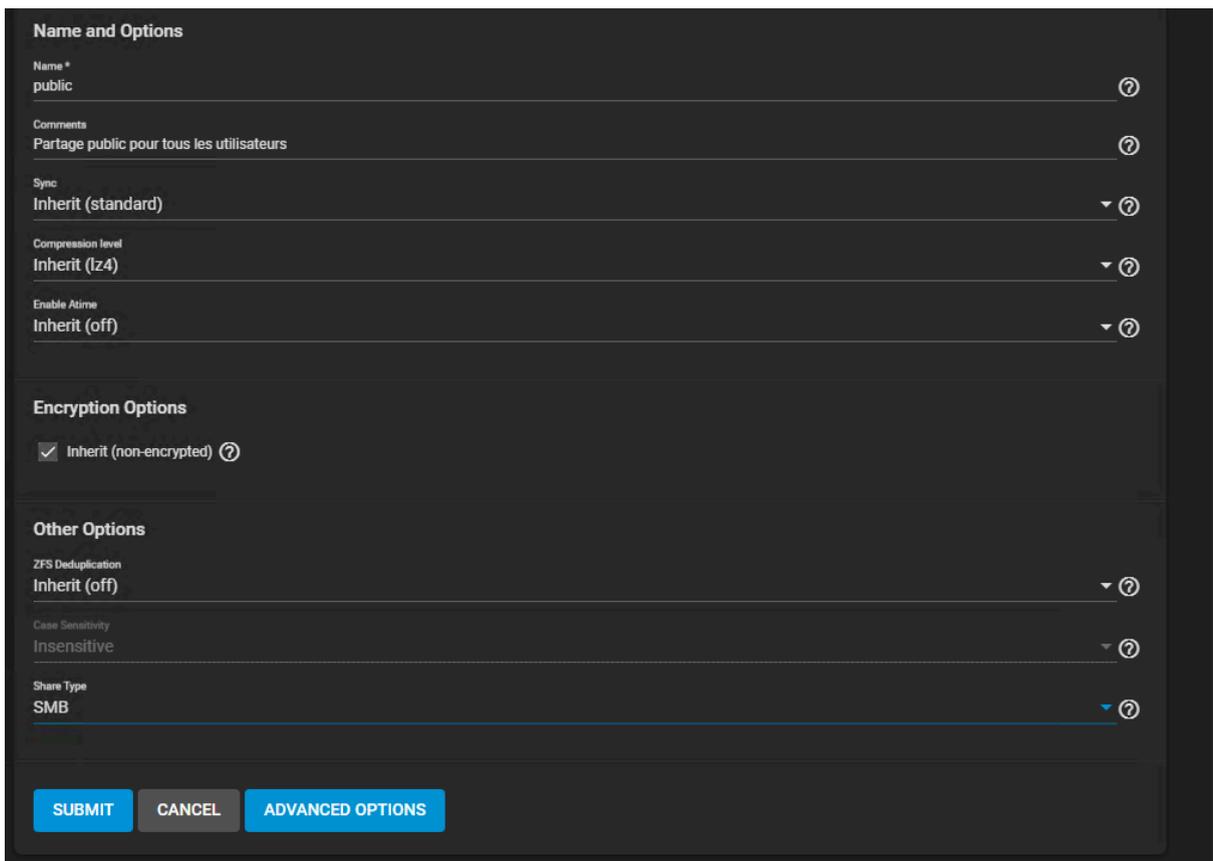
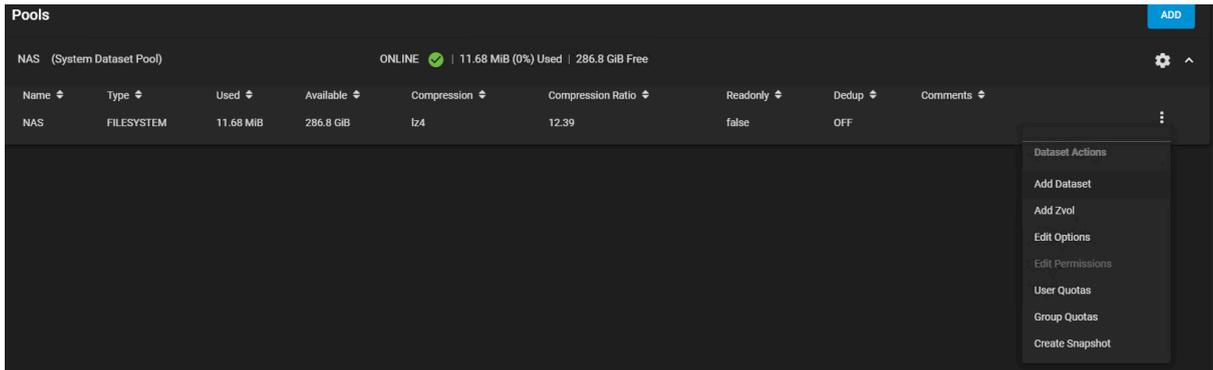
On nomme notre partage **'NAS'** et on sélectionne le **disque dur** que l'on avait ajouté à notre serveur précédemment



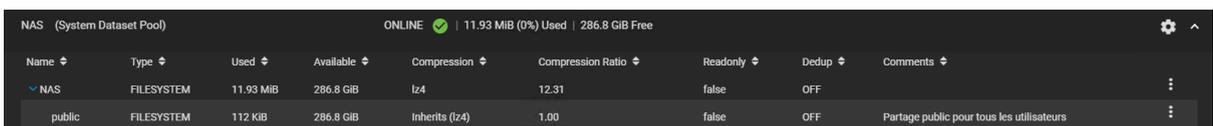
Il faut cliquer sur la **flèche** afin que le disque soit catégorisé dans les disques **VDevs**. Dans notre cas, on doit aussi cliquer sur **"Force"** car nous n'avons qu'un seul disque, pratique qui n'est pas sécurisée car si le disque vient à être défectueux, toute la **pool** sera corrompue. On coche donc la case **"Force"** afin de forcer la création d'un **pool** contenant qu'un seul disque.



Notre **pool** est bien créé, on va donc maintenant créer notre ensemble de données en cliquant sur les **3 petits points** à droite puis **'Add Dataset'**.



Dans cette situation, on veut **créer** un espace de **partage public** pour nos **deux VLAN**, on le nomme donc **'Public'** et on définit **'Share Type'** en mode **'SMB'**.

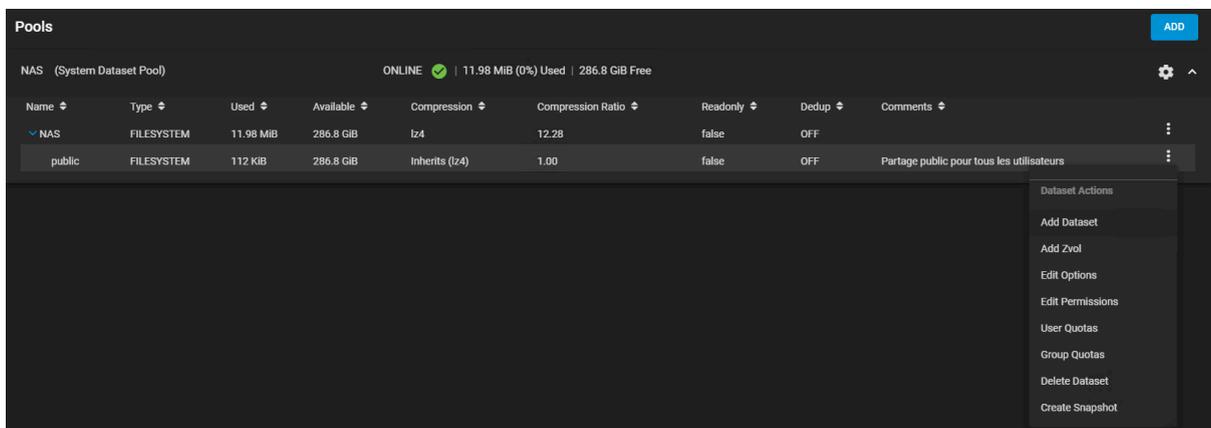


## → Modification ACL

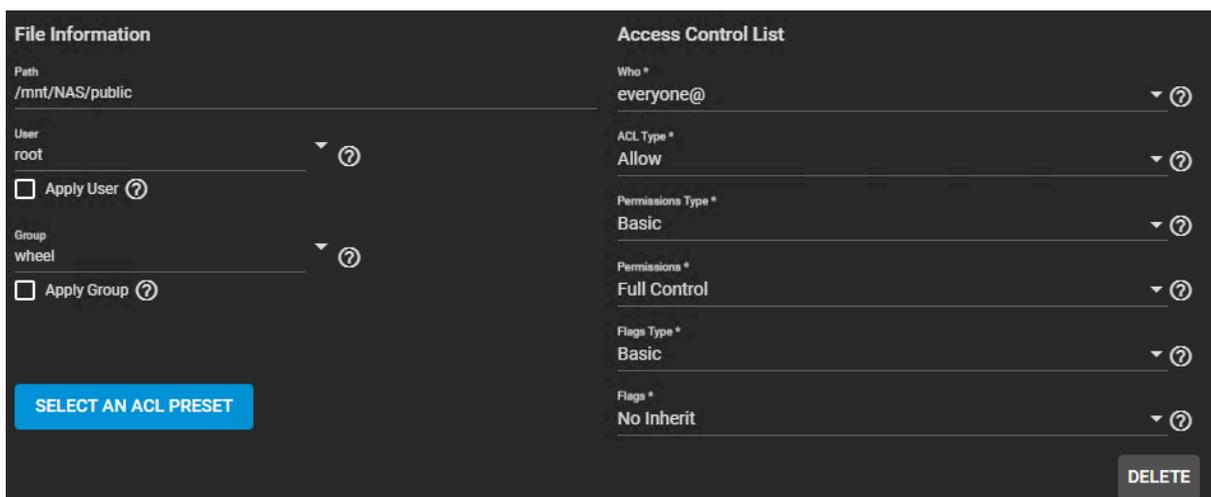
Une **ACL** ou **“Access Control List”** est un ensemble de règles qui définissent les autorisations d'accès à des ressources (comme des fichiers ou des réseaux), spécifiant qui peut y accéder et quelles actions peuvent être effectuées (lecture, écriture, exécution).

Dans notre cas, nous voulons que notre partage **“public”** soit accessible en **lecture, écriture, exécution** pour tous les utilisateurs.

Pour modifier les **ACL**, on se rend dans **Storage -> Pools**.



Puis on **clique** sur **“Edit Permissions”** :

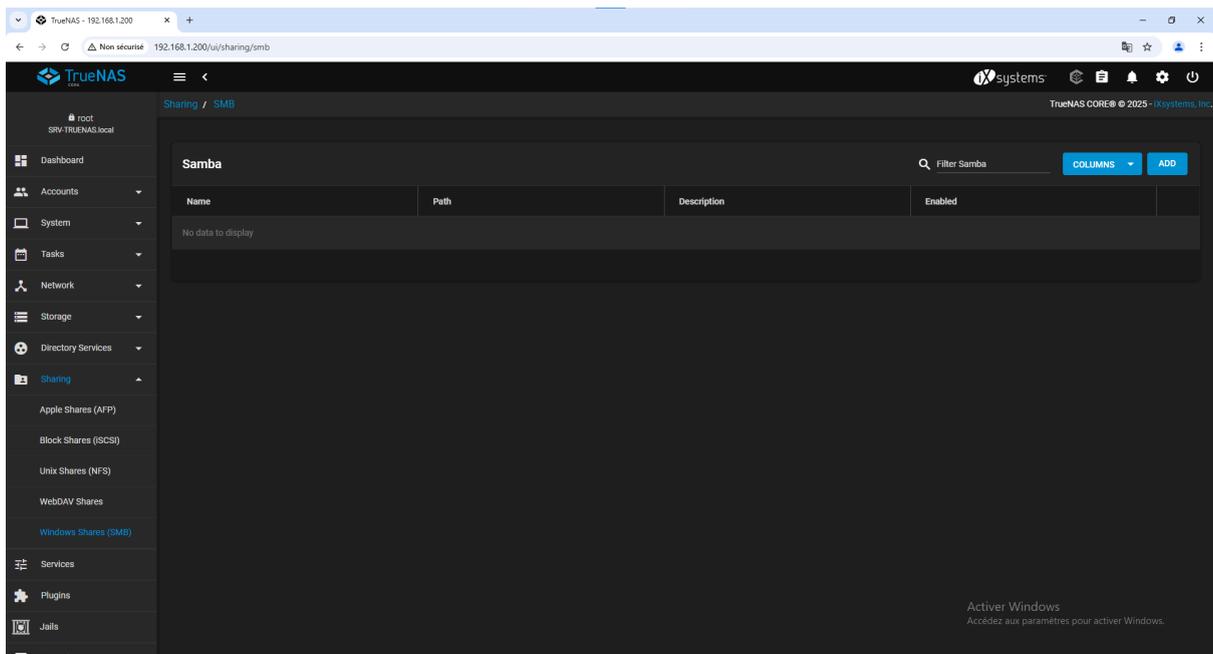


Dans notre cas, on veut que tous les utilisateurs aient toutes les permissions, on sélectionne donc **“Everyone”** dans **“Who”** et dans **“Permission”** on met **“Full Control”** et on clique sur **“Save”** pour sauvegarder.

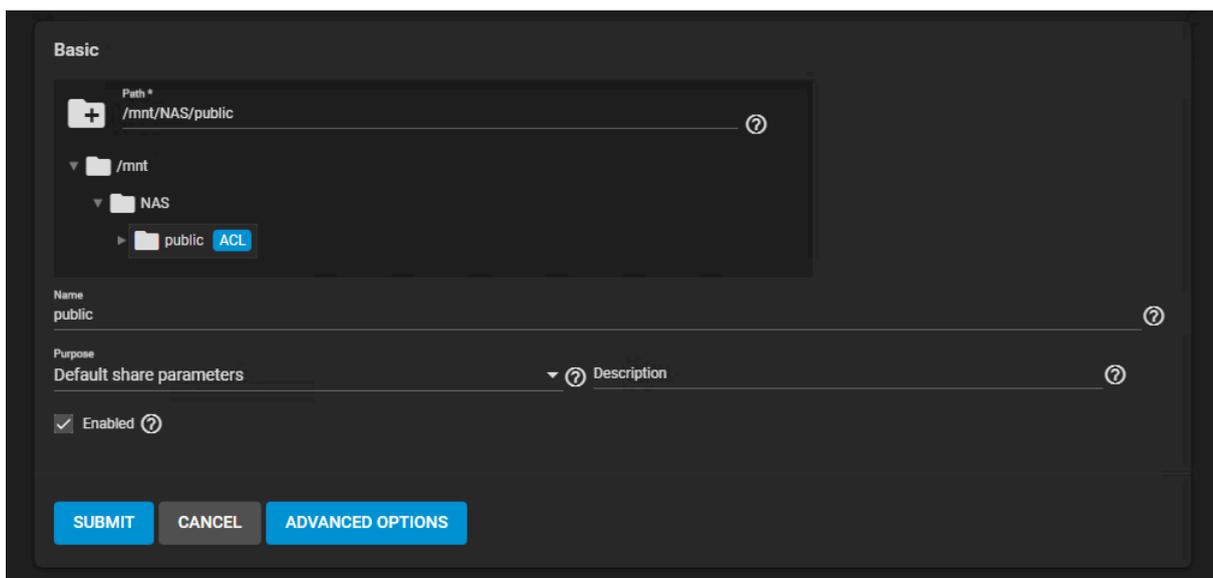
## 4. Création du partage SMB

Nous allons donc **mettre à disposition** notre **banque de données** via un **partage SMB**.

Pour le **créer** on va se rendre dans **Sharing -> Windows Shares (SMB)**.



On clique sur **ADD** pour **créer un nouveau partage** :



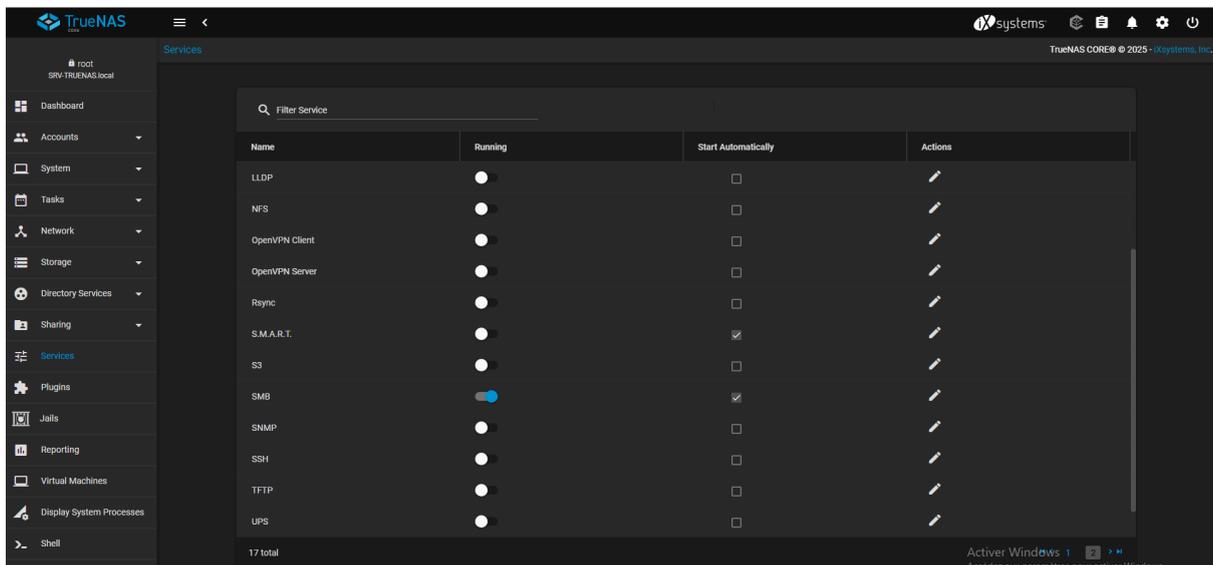
On **parcourt l'arborescence** pour **trouver** notre **banque de données 'public'** et on **clique** sur **'Submit'** pour le **créer**.

→ Activation SMBv1

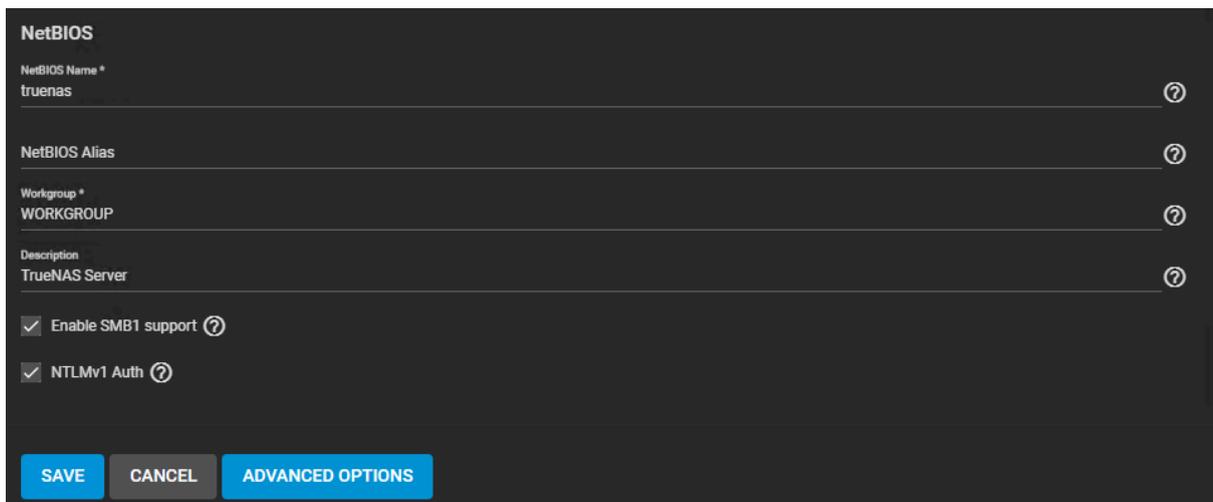
⚠ **Attention**, le protocole **SMBv1** est **obsolète** et **vulnérable** à des attaques. Il manque de **chiffrement** et de protections modernes. L'utiliser expose donc les systèmes à des risques de **sécurité élevés**. ⚠

Un souci s'oppose à nous, **PC XP** ne peut pas accéder au partage car **Windows XP** ne prend pas en charge le protocole **SMB** au-dessus de la version **1**.

Pour pallier ce problème, nous allons forcer l'activation **SMBv1** en allant dans l'onglet '**Service**'.



Ensuite, **cliquez** sur le **crayon** à la **ligne SMB**

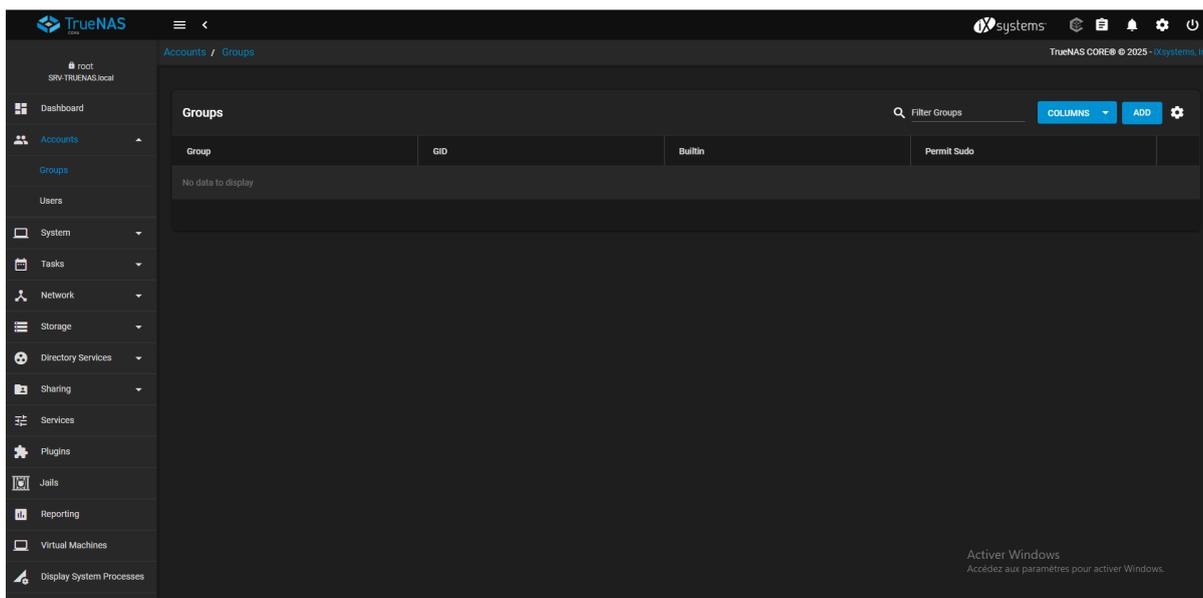


**Cochez** la case "**Enable SMB1 support**" et "**NTLMv1 Auth**" et cliquez sur "**Save**"

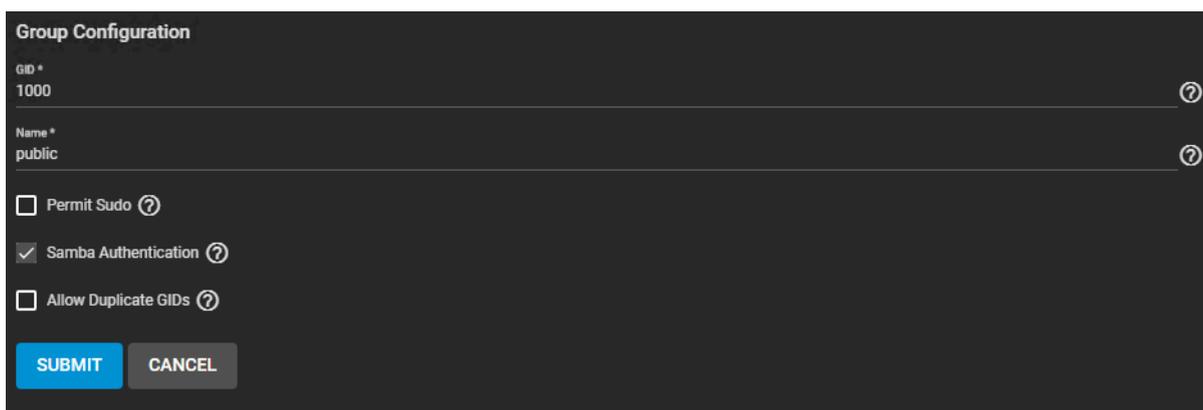
## 5. Création des utilisateurs/groupes

→ Créer un groupe d'utilisateur

Pour **tester notre NAS** nous allons **créer deux utilisateurs**, ces **deux utilisateurs doivent faire partie d'un groupe**. Pour **créer un groupe** on se rend dans la catégorie **Account -> Groups**



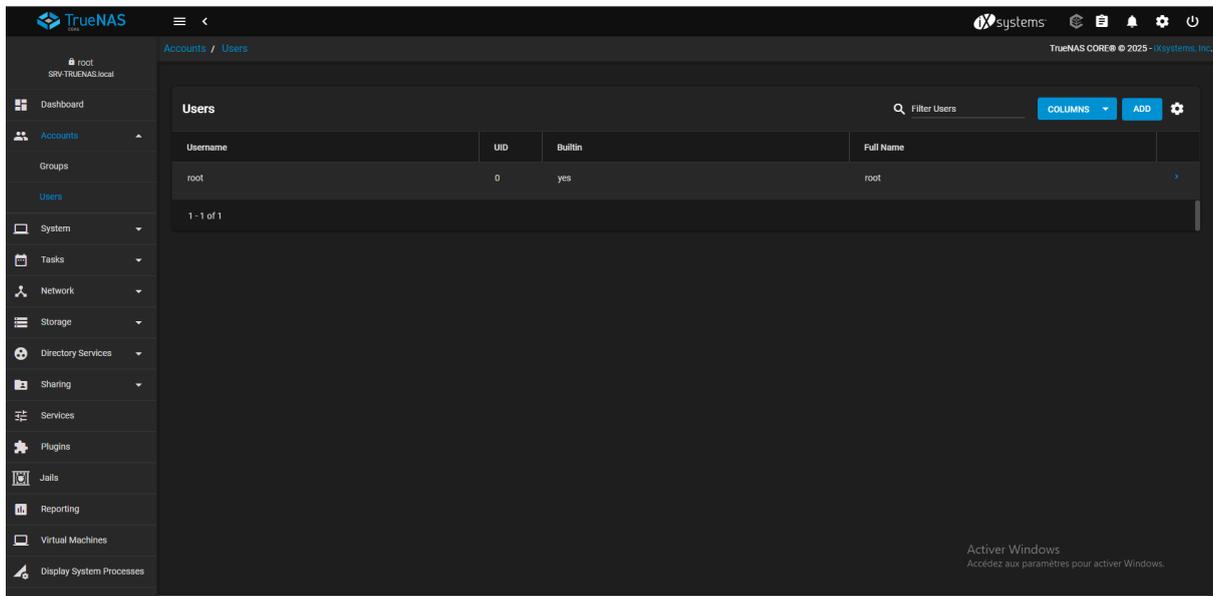
On **clique sur ADD** en haut à droite afin de **créer un nouveau groupe** :

The screenshot shows the 'Group Configuration' form. It has a dark theme. The 'GID' field is set to '1000' and the 'Name' field is set to 'public'. There are three checkboxes: 'Permit Sudo' (unchecked), 'Samba Authentication' (checked), and 'Allow Duplicate GIDs' (unchecked). At the bottom, there are two buttons: 'SUBMIT' (highlighted in blue) and 'CANCEL'.

Dans notre cas, on nomme **le groupe "Public"** et on **clique sur "Submit"**.

→ Créer un utilisateur

Pour **créer nos utilisateurs**, on se rend dans l'onglet **Account -> Users** :



On clique sur **ADD** pour **créer un nouvel utilisateur** :

**Identification**

Full Name \*  
test

Username \*  
test

Email  
?

Password \*  
\*\*\*\*

Confirm Password \*  
\*\*\*\*

**User ID and Groups**

User ID \*  
1000

New Primary Group ?

Primary Group  
public

Auxiliary Groups

**Directories and Permissions**

Home Directory  
/nonexistent

▶ /mnt

Home Directory Permissions ?

	Read	Write	Execute
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Other	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**Authentication**

SSH Public Key

Disable Password  
No

Shell  
sh

Lock User ?

Permit Sudo ?

Microsoft Account ?

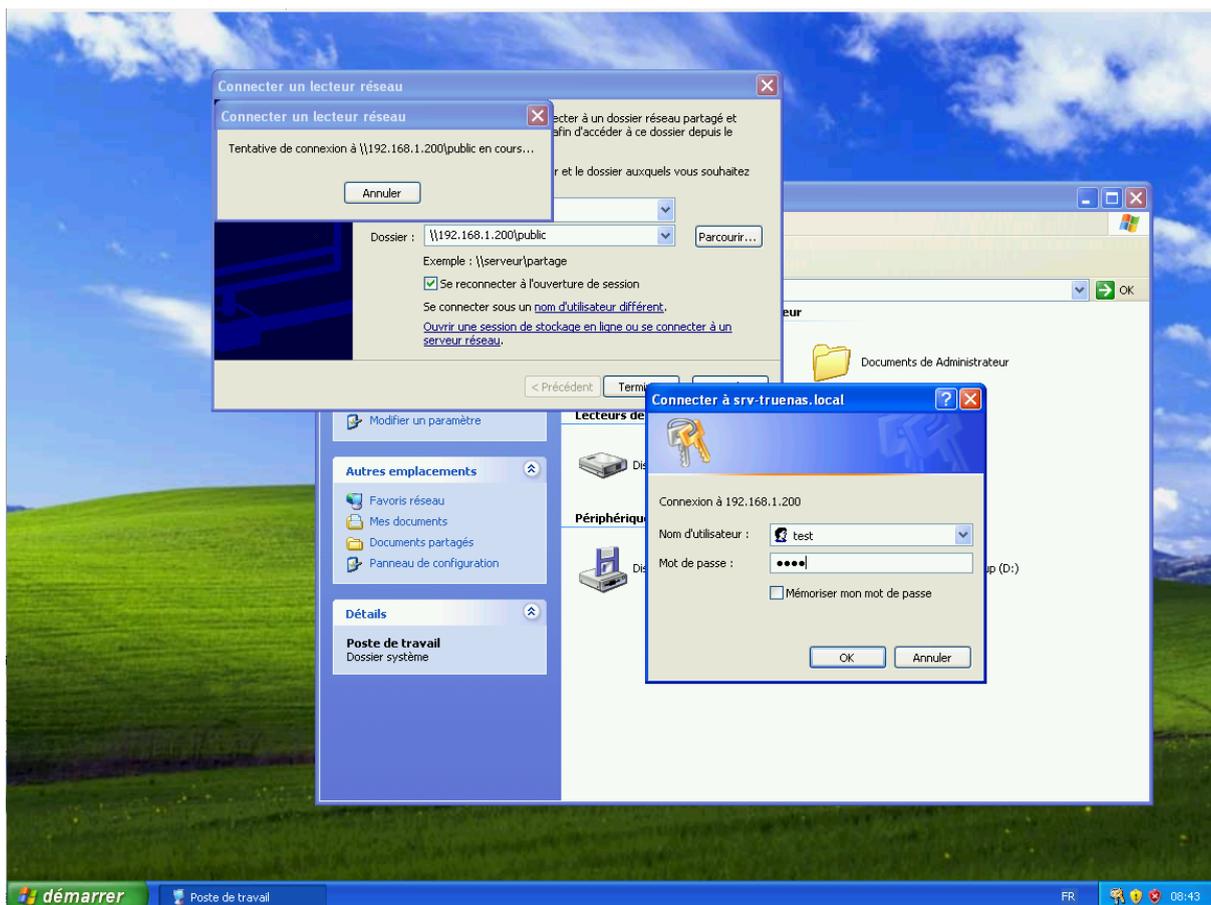
Samba Authentication ?

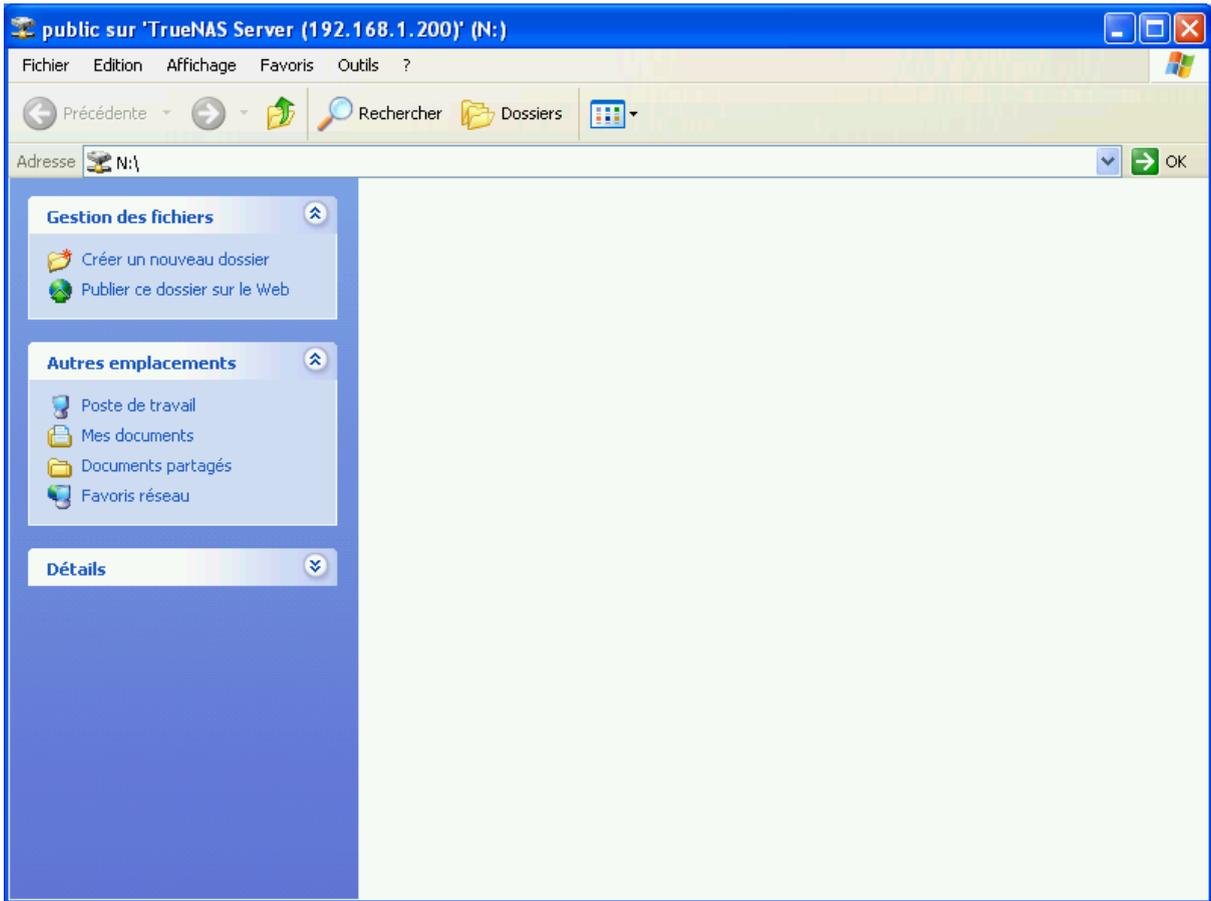
Pour **tester nos droits** on va **créer deux utilisateurs** avec les **mêmes configuration** :

- Nos utilisateurs **“test” et “test1”** doivent appartenir au groupe **“public”** comme **groupe primaire**
- Nous ne voulons **pas que nos utilisateurs possèdent de répertoire nominatif**, donc dans la section **“Directories and Permissions”** et dans le champ **“Home Directory”**, on tape **“/nonexistent”**.

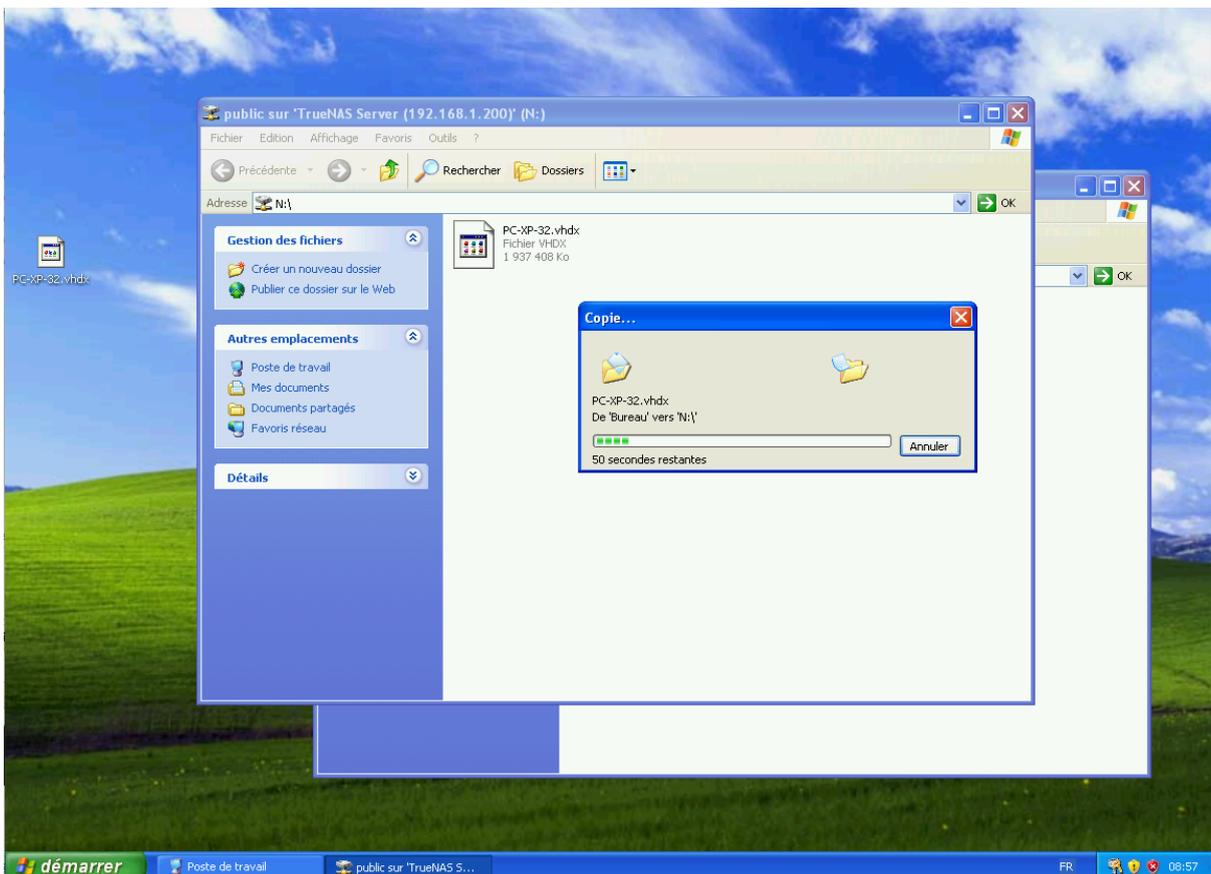
→ Test de connexion + transfert de données

On va tout d’abord essayer de se connecter du **“PC XP”** sur le **NAS** :

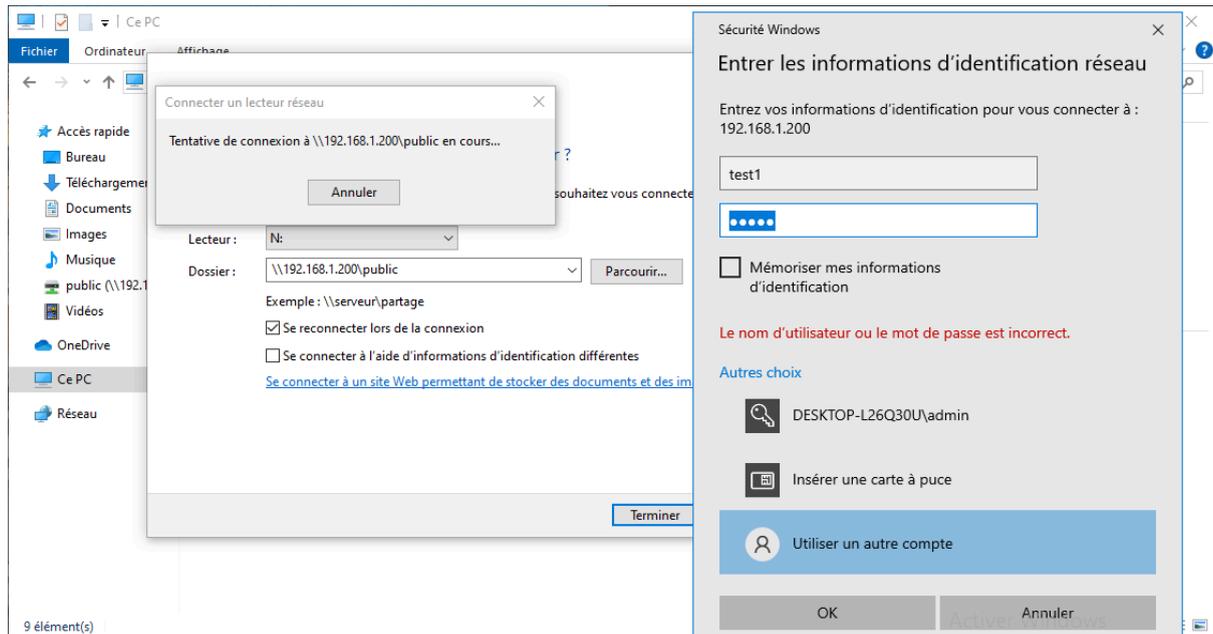




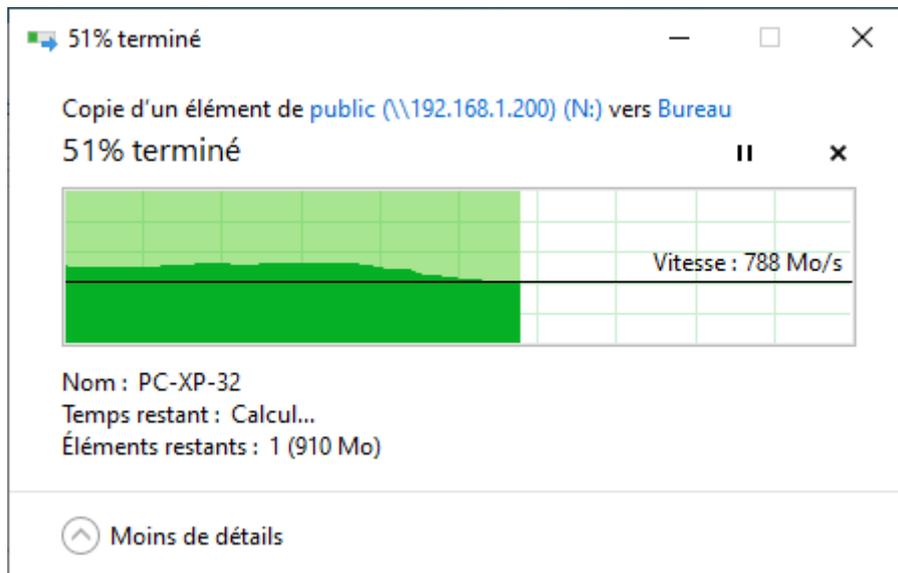
On est bien connecté, notre **utilisateur** a bien accès au **partage**, on va tester nos **droits** en essayant un **transfert de fichier** :



On fait pareil pour le **“PC Gestion NAS”** :



On récupère le **fichier** que l'on a posé avec le **PC-XP** :



On voit que nos **droits** fonctionnent correctement malgré qu'on ne les ait pas tous **testés**.

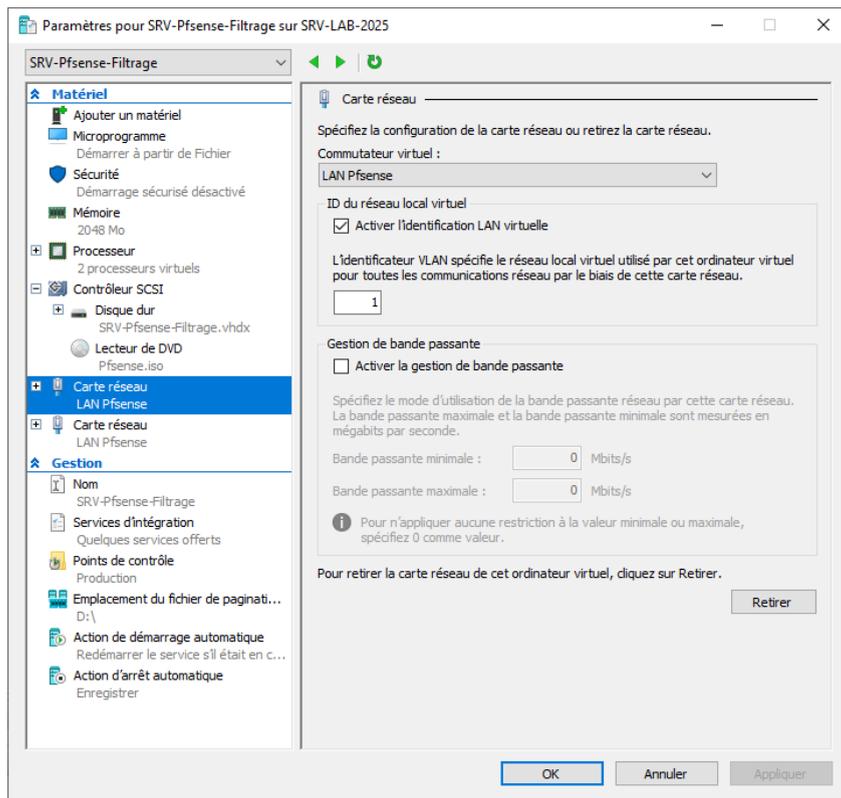
# VI. Configuration du Pfsense Filtrage

Dans notre [schéma](#), on a un **PfSense** qui sert de serveur proxy sur le **VLAN 2**.

Pour le créer, on procède comme ceci :

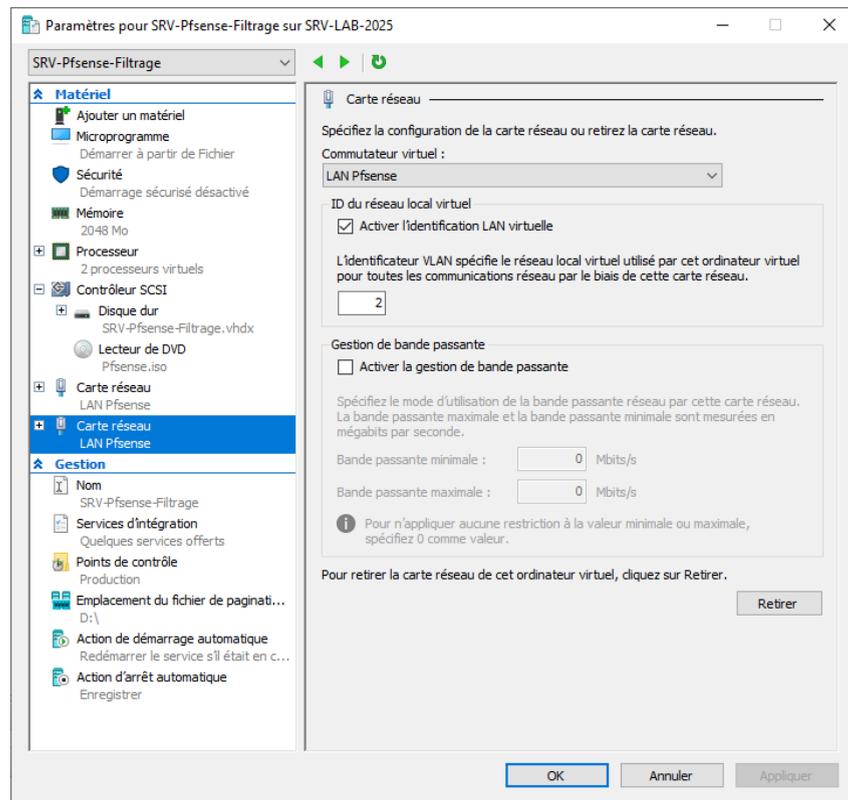
## 1. Création carte réseau

→ Carte WAN



On crée notre première carte côté **WAN**, celle-ci doit être sur le **VLAN 1** conformément à notre schéma.

→ Carte LAN



Comme pour la carte **WAN**, il faut mettre la carte **LAN** dans son **VLAN** respectif, donc le **n°2** dans ce cas-ci.

## 2. Adressage IP des cartes

→ Carte WAN

```
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system             14) Enable Secure Shell (sshd)
6) Halt system               15) Restore recent configuration
7) Ping host                 16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (hn0 - static)
2 - LAN (hn1 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.1.253

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

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.254

Should this gateway be set as the default gateway? (y/n) y

Configure IPv6 address WAN interface via DHCP6? (y/n) n

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

Do you want to enable the DHCP server on WAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 WAN address has been set to 192.168.1.253/24

Press <ENTER> to continue. █
```

## Explication :

1. On tape **2** pour choisir la troisième option du système '**Set interface(s) IP address**'.
2. On tape sur **1** pour sélectionner la première carte réseau.
3. À ce moment-là, **PfSense** demande quelle est l'adresse que l'on veut affecter à notre carte réseau, d'après notre schéma réseau, on y affecte l'adresse '**192.168.1.253**'.
4. **PfSense** nous demande le masque de notre réseau en format **CIDR**, on choisit **24** dans notre cas pour un réseau local classe C.
5. Ici, vu que l'on configure une interface **WAN** dans un réseau existant, on doit définir la passerelle en amont, on tape donc l'adresse IP de notre passerelle soit **192.168.1.254**.
6. Dans notre cas, on ne veut pas d'adresse en format **IPV6**, on appuie sur '**N**' pour ne pas activer le serveur **DHCP en IPV6**.
7. Par la suite, on nous demande si on veut activer le serveur **DHCP en IPV4**, dans notre cas, on veut tout simplement pas de **DHCP** dans le réseau, donc on appuie encore une fois '**N**'.
8. La dernière question nous demande si l'on veut désactiver l'accès à l'interface web en **HTTPS**, bien sûr, on répond **non** à des fins de sécurité.

## → Interface LAN

```
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system             14) Enable Secure Shell (sshd)
6) Halt system               15) Restore recent configuration
7) Ping host                 16) Restart PHP-FPM
8) Shell
```

Enter an option: 2

Available interfaces:

```
1 - WAN (hn0 - static)
2 - LAN (hn1 - static)
```

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

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

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.  
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):  
> 24

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

Configure IPv6 address LAN interface via DHCP6? (y/n) n

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

Do you want to enable the DHCP server on LAN? (y/n) n  
Disabling IPv4 DHCPD...  
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n  
Please wait while the changes are saved to LAN...  
Reloading filter...  
Reloading routing configuration...  
DHCPD...

The IPv4 LAN address has been set to 192.168.2.254/24  
You can now access the webConfigurator by opening the following URL in your web browser:

<https://192.168.2.254/>

Press <ENTER> to continue.

## Explications

1. On tape **2** pour choisir la troisième option du système '**Set interface(s) IP address**'.
2. On tape sur **2** encore une fois pour sélectionner la deuxième carte réseau.
3. À ce moment-là, **PfSense** demande quelle est l'adresse que l'on veut affecter à notre carte réseau (cette adresse sera la passerelle de notre réseau), d'après notre schéma réseau, on y affecte l'adresse '**192.168.2.254**'.
4. **PfSense** nous demande le masque de notre réseau en format **CIDR**, on choisit **24** dans notre cas pour un réseau local classe C.
5. Ici, vu que l'on configure une interface **LAN**, on passe cette étape en appuyant sur '**Entrer**'.
6. Dans notre cas, on ne veut pas d'adresse en format **IPV6**, on appuie sur '**N**' pour ne pas activer le serveur DHCP en **IPV6**.
7. Par la suite, on nous demande si on veut activer le serveur **DHCP en IPV4**, dans notre cas, on ne veut tout simplement pas de **DHCP** dans le réseau, donc on appuie encore une fois '**N**'.
8. La dernière question nous demande si l'on veut désactiver l'accès à l'interface web en **HTTPS**, bien sûr, on répond **non** à des fins de sécurité.

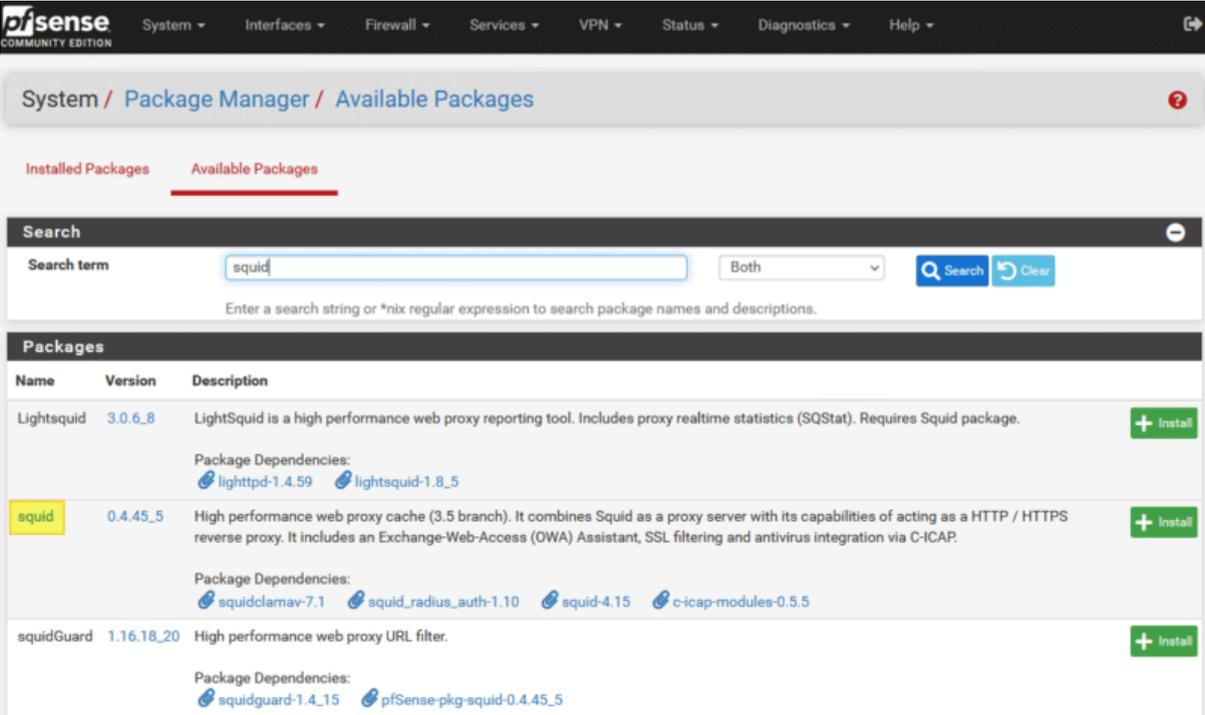
### 3. Création du proxy

→ Installation de Squid sur PfSense

Connectez-vous sur l'interface d'administration de **PfSense** afin d'installer le paquet "**squid**". Pour cela, sous "**System**", cliquez sur "**Package Manager**" et ensuite sur l'onglet "**Available Packages**".

**System > Package Manager > Available Packages**

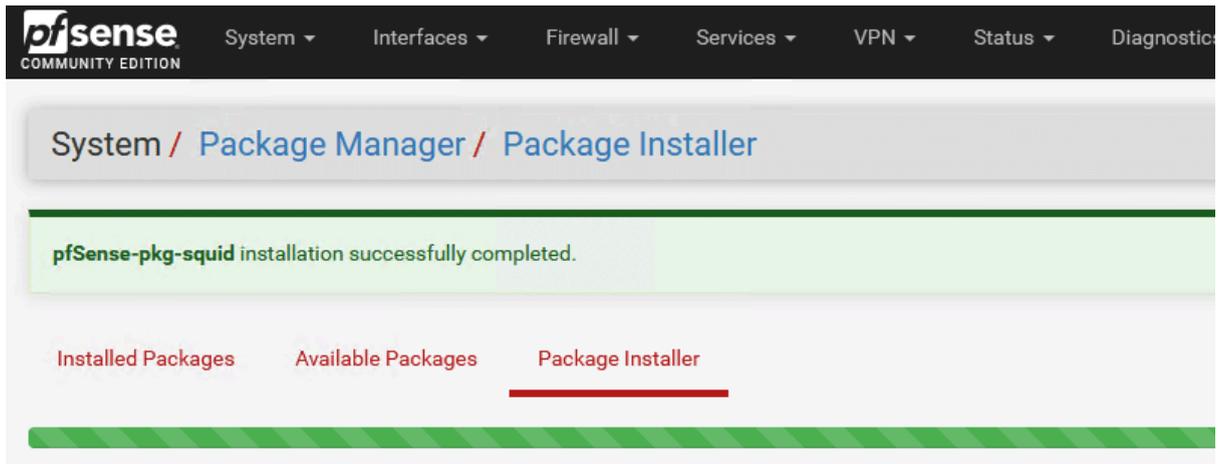
Recherchez "**squid**" et cliquez sur le bouton "**Install**" à droite, au niveau de la ligne correspondante.



The screenshot shows the PfSense Package Manager interface. At the top, there is a navigation bar with the PfSense logo and menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation bar, the breadcrumb path is "System / Package Manager / Available Packages". There are two tabs: "Installed Packages" and "Available Packages", with the latter being selected. A search bar is present with the search term "squid" entered. Below the search bar, there is a table of packages. The table has three columns: Name, Version, and Description. The "squid" package is highlighted in yellow. To the right of each package entry is a green "+ Install" button.

Name	Version	Description	Action
Lightsquid	3.0.6.8	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. Package Dependencies: <a href="#">lighttpd-1.4.59</a> <a href="#">lightsquid-1.8_5</a>	+ Install
squid	0.4.45_5	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP. Package Dependencies: <a href="#">squidclamav-7.1</a> <a href="#">squid_radius_auth-1.10</a> <a href="#">squid-4.15</a> <a href="#">c-icap-modules-0.5.5</a>	+ Install
squidGuard	1.16.18_20	High performance web proxy URL filter. Package Dependencies: <a href="#">squidguard-1.4_15</a> <a href="#">pfSense-pkg-squid-0.4.45_5</a>	+ Install

À la fin de l'installation, le message "**pfSense-pkg-squid installation successfully completed**" doit s'afficher.



Le paquet étant installé, on peut passer à la **configuration**.

→ Configurer Squid (Proxy) sur PfSense

La configuration de **Squid** s'effectue via le menu "**Services**" :

**Services > Squid Proxy Server**

La configuration est découpée en plusieurs onglets. Afin de pouvoir activer **Squid**, il faut configurer le **cache local** sinon le démarrage du processus **Squid** échouera. Cliquez sur l'onglet "**Local Cache**". Comme pour chaque section, nous retrouvons de nombreux paramètres... Pour le cache, j'attire votre attention sur ces options :

- **Hard Disk Cache Size** : par défaut sur "**100**" pour **100 Mo**, cette valeur correspond à la taille maximale du cache sur l'espace disque. Vous pouvez augmenter cette valeur à **1024 Mo** pour avoir **1 Go** de cache.
- **Hard Disk Cache Location** : l'emplacement du cache, à savoir par défaut **"/var/squid/cache"**.

Que vous décidiez de modifier ou non l'un des paramètres de la section "**Local Cache**", vous devez cliquer sur le bouton "**Save**" en bas de la page.

Package / Proxy Server: Cache Management / Local Cache

General Remote Cache **Local Cache** Antivirus ACLs Traffic Mgmt Authentication Us

### Squid Cache General Settings

**Disable Caching**  Disable caching completely.  
This may be required if Squid is only used as a proxy to audit website access.

**Cache Replacement Policy** Heap LFUDA  
The cache replacement policy decides which objects will remain in cache and which objects are evicted.  
heap LFUDA ⓘ

**Low-Water Mark in %** 90  
The low-water mark for AUFS/UFS/diskd cache object eviction by the cache\_replacement\_policy.

Ensuite, cliquez sur l'onglet "**General**". Là encore, il y a de nombreuses options.

Voici ce qu'il faut configurer à minima :

- **Enable Squid Proxy** : cochez la case pour activer **Squid** sur le pare-feu, ce qui signifie qu'il va démarrer.
- **[facultatif] Listen IP Version** : écouter en **IPv4**, en **IPv6** ou les deux.
- **Proxy interface(s)** : sur quelle interface souhaitez-vous activer le proxy ? Ici, ce sera seulement sur l'interface "**LAN**" donc je la sélectionne. Vous pouvez en sélectionner plusieurs si besoin, mais dans tous les cas le "**WAN**" ne sera pas sélectionné.
- **Proxy Port** : on laisse le port par défaut, à savoir **3128**, mais il ne devra pas être déclaré sur les postes clients puisque l'on va configurer **Squid** en mode **proxy transparent**.
- **Allow Users on interface** : cochez cette case pour **autoriser implicitement** les utilisateurs connectés sur le réseau "**LAN**" à utiliser le proxy. Cela évite de déclarer le réseau dans un second temps.

Squid General Settings	
Enable Squid Proxy	<input checked="" type="checkbox"/> Check to enable the Squid proxy. <b>Important:</b> If unchecked, ALL Squid services will be disabled and stopped.
Keep Settings/Data	<input checked="" type="checkbox"/> If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls. <b>Important:</b> If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.
Listen IP Version	<input type="text" value="IPv4"/> Select the IP version Squid will use to select addresses for accepting client connections.
CARP Status VIP	<input type="text" value="none"/> Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status. <b>Important:</b> Don't forget to generate Local Cache on the secondary node and configure <b>XMLRPC Sync</b> for the settings synchronization.
Proxy Interface(s)	<input type="text" value="WAN"/> <input checked="" type="text" value="LAN"/> <input type="text" value="loopback"/> The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces.
Outgoing Network Interface	<input type="text" value="Default (auto)"/> The interface the proxy server will use for outgoing connections.
Proxy Port	<input type="text" value="3128"/> This is the port the proxy server will listen on. Default: 3128
ICP Port	<input type="text"/> This is the port the proxy server will send and receive ICP queries to and from neighbor caches. Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.
Allow Users on Interface	<input checked="" type="checkbox"/> If checked, the users connected to the interface(s) selected in the 'Proxy interface(s)' field will be allowed to use the proxy. There will be no need to add the interface's subnet to the list of allowed subnets.
Patch Captive Portal	<b>This feature was removed - see Bug #5594 for details!</b>

Activer W  
Accédez aux

Descendez dans la page... et cochez l'option **"Transparent HTTP Proxy"** pour activer le mode **proxy transparent** pour le protocole **HTTP**. Pour l'activer pour le protocole **HTTPS**, il faudra cocher une autre option (nous en parlerons par la suite).

Dans le même esprit qu'au début de la configuration, sélectionnez **"LAN"** pour l'option **"Transparent Proxy Interface(s)"**.

En configurant l'option **"Bypass Proxy for these Source IPs"**, vous avez la possibilité de déclarer des **adresses IP sources** (ou un **sous-réseau source**) qui peuvent passer outre le proxy et accéder en direct à Internet. Dans le même esprit, l'option **"Bypass Proxy for these Destination IPs"** permet d'outrepasser le proxy pour certaines destinations.

## Transparent Proxy Settings

### Transparent HTTP Proxy

Enable transparent mode to forward all requests for destination port 80 to the proxy server.



Transparent proxy mode works without any additional configuration being necessary on clients.

**Important:** Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.

**Hint:** In order to proxy both HTTP and HTTPS protocols **without intercepting SSL connections**, configure WPAD/PAC options on your DNS/DHCP servers.

### Transparent Proxy Interface(s)

WAN  
LAN

The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.

### Bypass Proxy for Private Address Destination

Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations.

Destinations in Private Address Space (RFC 1918 and IPv6 ULA) are passed directly through the firewall, not through the proxy server.

### Bypass Proxy for These Source IPs

Do not forward traffic from these **source** IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall.

**Applies only to transparent mode.** Separate entries by semi-colons (;)

### Bypass Proxy for These Destination IPs

Do not proxy traffic going to these **destination** IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall.

**Applies only to transparent mode.** Separate entries by semi-colons (;)

Pour le moment, laissez l'option "**Enable SSL filtering**" décochée.

## SSL Man In the Middle Filtering

### HTTPS/SSL Interception

Enable SSL filtering.

### SSL/MITM Mode

Splice Whitelist, Bump Otherwise

The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle' Default: Splice Whitelist, Bump Otherwise. [Click Info for details.](#)

### SSL Intercept Interface(s)

WAN  
LAN

The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select mult

Continuez de descendre dans la page... Activez les **journaux** comme ceci :

- **Enable Access Logging** : cochez l'option pour activer les **journaux**, ce qui va permettre de savoir qui fait quoi sur Internet.
- **Rotate Logs** : pendant combien de jours souhaitez-vous conserver les **logs** ? Pour les **établissements scolaires**, c'est pendant **365 jours** qu'il faut conserver les logs (sauf erreur de ma part).

Logging Settings	
<b>Enable Access Logging</b>	<input checked="" type="checkbox"/> This will enable the access log. <b>Warning:</b> Do NOT enable if available disk space is low.
<b>Log Store Directory</b>	<input type="text" value="/var/squid/logs"/> The directory where the logs will be stored; also used for logs other than the Access Log above. <b>Default:</b> /var/squid/logs <b>Important:</b> Do NOT include the trailing / when setting a custom location.
<b>Rotate Logs</b>	<input type="text" value="365"/> Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Ensuite, la section **"Headers Handling, Language and Other Customizations"** permet de configurer les messages **Squid**. Le champ **"Visible Hostname"** correspond au **nom d'hôte** qui peut s'afficher côté client, notamment sur les pages de blocage **Squid**, tout comme l'**e-mail** spécifié pour l'option **"Administrator's Email"**. Pour les messages d'erreurs justement, précisez la **langue française** au niveau de l'option **"Error Language"**.

Pour des raisons de sécurité, on va masquer les informations sur **Squid**, notamment la **version**, en cochant l'option **"Suppress Squid Version"**. Ce qui donne :

Headers Handling, Language and Other Customizations	
<b>Visible Hostname</b>	<input type="text" value="Proxy IT-Connect"/> <small>This is the hostname to be displayed in proxy server error messages.</small>
<b>Administrator's Email</b>	<input type="text" value="admin@it-connect.fr"/> <small>This is the email address displayed in error messages to the users.</small>
<b>Error Language</b>	<input type="text" value="fr"/> <small>Select the language in which the proxy server will display error messages to users.</small>
<b>X-Forwarded Header Mode</b>	<input type="text" value="(on)"/> <small>Choose how to handle X-Forwarded-For headers. Default: on <a href="#">i</a></small>
<b>Disable VIA Header</b>	<input type="checkbox"/> If not set, Squid will include a Via header in requests and replies as required by RFC2616 <a href="#">i</a>
<b>URI Whitespace Characters Handling</b>	<input type="text" value="strip"/> <small>Choose how to handle whitespace characters in URL. Default: strip <a href="#">i</a></small>
<b>Suppress Squid Version</b>	<input checked="" type="checkbox"/> Suppresses Squid version string info in HTTP headers and HTML error pages if enabled.

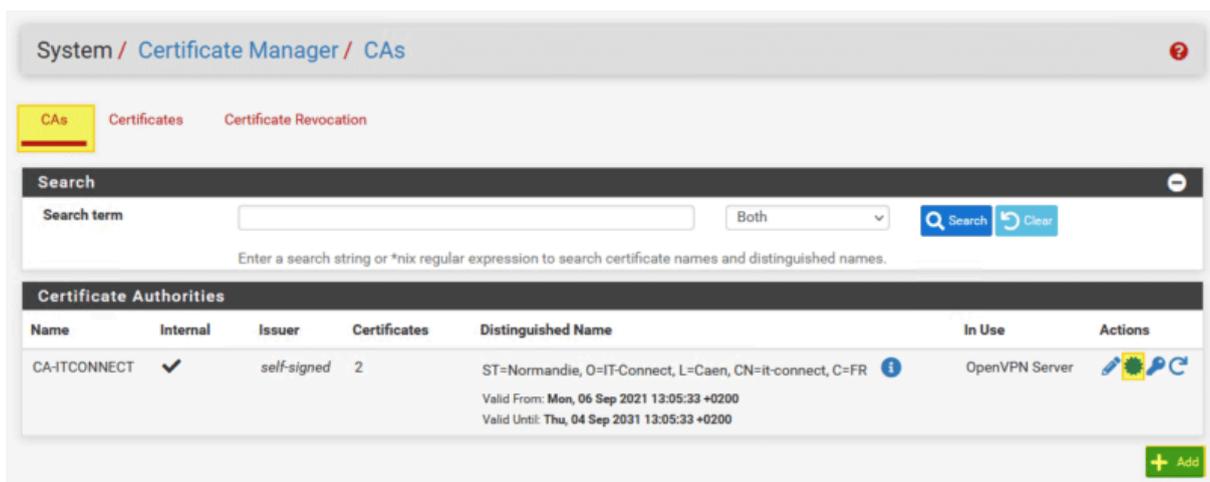
Voilà, on est arrivé au bout de la page de configuration ! Cliquez sur **"Save"** pour appliquer cette nouvelle configuration.

## → Créer l'autorité de certification PfSense

Pour commencer, il faut créer une **autorité de certification** sur notre pare-feu **PfSense**. Rendez-vous dans le menu "**System**" puis "**Cert. Manager**" et dans l'onglet "**CAs**". Cliquez sur "**Add**" et renseignez les différents champs : c'est tout simple.

**Note** : si vous avez une **autorité de certification Active Directory**, il doit être possible d'ajouter un **certificat existant** directement.

Vous obtenez une **autorité de certification**, comme la mienne nommée "**CA-ITCONNECT**" et qui existait déjà sur mon pare-feu, car je l'utilise pour le **VPN client-to-site**.



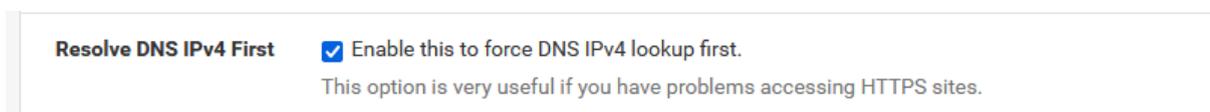
The screenshot shows the PfSense web interface for Certificate Authorities. The breadcrumb trail is "System / Certificate Manager / CAs". There are three tabs: "CAs" (selected), "Certificates", and "Certificate Revocation". Below the tabs is a search bar with a "Search term" input, a "Both" dropdown, and "Search" and "Clear" buttons. A note below the search bar says "Enter a search string or \*nix regular expression to search certificate names and distinguished names." Below the search bar is a table titled "Certificate Authorities".

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-ITCONNECT	<input checked="" type="checkbox"/>	self-signed	2	ST=Normandie, O=IT-Connect, L=Caen, CN=it-connect, C=FR Valid From: Mon, 06 Sep 2021 13:05:33 +0200 Valid Until: Thu, 04 Sep 2031 13:05:33 +0200	OpenVPN Server	  

At the bottom right of the table area is a green "+ Add" button.

## → SSL Inspection avec Squid

Retournez dans la configuration de **Squid**, via le menu "**Services**". Cochez l'option "**Resolve DNS IPv4 First**" pour activer la **résolution DNS en amont du filtrage**, ce qui est recommandé lorsque l'on filtre le **HTTPS** (ce que l'on s'apprête à faire).



The screenshot shows a configuration option for Squid: "Resolve DNS IPv4 First". It has a checked checkbox and the text "Enable this to force DNS IPv4 lookup first." Below this is a note: "This option is very useful if you have problems accessing HTTPS sites."

Ensuite, activez l'option **"Enable SSL filtering"**. Pour le mode **"SSL/MITM Mode"**, choisissez le mode **"Splice All"** : c'est le mode le moins contraignant à mettre en œuvre, car il ne nécessite pas de déployer le **certificat de l'autorité de certification** sur l'ensemble des postes clients. C'est aussi le mode recommandé lorsque l'on prévoit de déployer **Squid Guard**, ce qui sera le cas dans la seconde partie de ce tutoriel.

**Remarque** : si vous prenez l'autre mode, il faut exporter le certificat de la **CA créée précédemment** et le déployer sur toutes les machines qui vont passer par le **proxy transparent**.

Sélectionnez l'**autorité de certification** créée précédemment au niveau de l'option **"CA"**.

**SSL Man in the Middle Filtering**

**HTTPS/SSL Interception**  Enable SSL filtering.

**SSL/MITM Mode** Splice All  
The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled. Default: Splice Whitelist, Bump Otherwise. [Click Info for details.](#) ⓘ

**SSL Intercept Interface(s)** WAN  
LAN  
The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.

**SSL Proxy Port**   
This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129

**SSL Proxy Compatibility Mode** Modern  
The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. [Click Info for details.](#) ⓘ

**DHParams Key Size** 2048 (default)  
DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.

**CA** CA-ITCONNECT  
Select Certificate Authority to use when SSL interception is enabled. ⓘ

**SSL Certificate Daemon Children**   
This is the number of SSL certificate daemon children to start. May need to be increased in busy environments. Default: 5

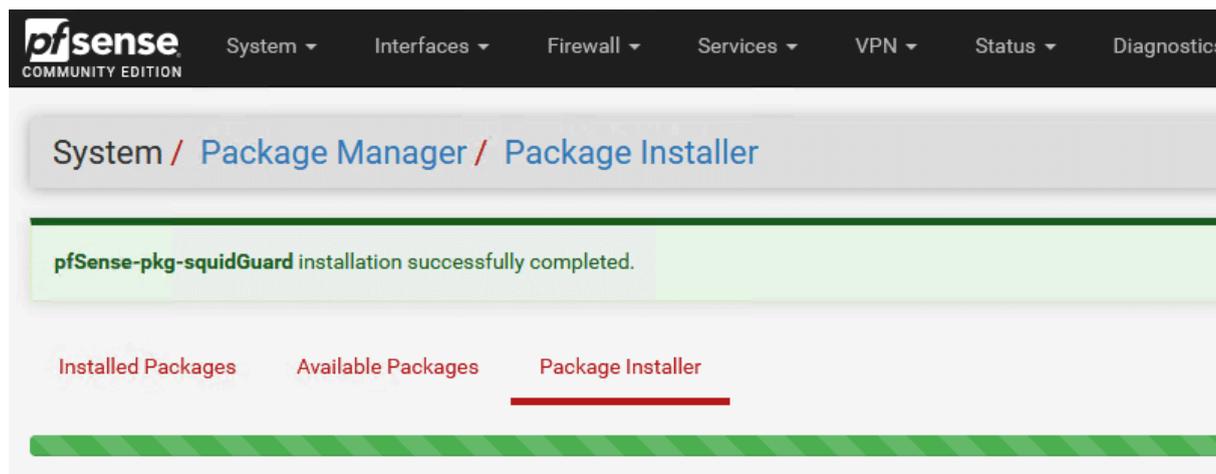
**Remote Cert Checks** Accept remote server certificate with errors  
Do not verify remote certificate  
Select remote SSL certificate checks to perform. Use CTRL + click to select multiple options.

**Certificate Adapt** Sets the "Not After" (setValidAfter)  
Sets the "Not Before" (setValidBefore)  
Sets CN property (setCommonName)  
See [ssiproxy\\_cert\\_adapt directive documentation](#) and [Mimic original SSL server certificate wiki article](#) for details.

**Sauvegardez** via le bouton en bas de page.

## → Installation de Squid Guard sur PfSense

L'installation de ce paquet sur **PfSense** passe par le menu habituel sous "**System**", puis "**Package manager**". Dans la section "**Available Packages**", recherchez "**squid**" et vous devriez voir le paquet **Squid Guard** apparaître. Il ne reste plus qu'à cliquer sur le bouton "**Install**".



Une fois que c'est fait, nous pouvons passer à la configuration via le menu "**Services**" où se trouve une entrée "**SquidGuard Proxy Filter**".

## → Configuration de Squid Guard sur PfSense

Pour le moment, on va s'intéresser à l'onglet "**General Settings**". N'allez pas trop vite : ne cochez pas l'option "**Check this option to enable SquidGuard**" pour le moment, car il faut le **préconfigurer** avant de l'activer.

The screenshot shows the PfSense configuration interface for the Proxy filter SquidGuard. The breadcrumb trail is "Package / Proxy filter SquidGuard: General settings / General settings". The "General settings" tab is selected. Under "General Options", the "Enable" checkbox is checked, and the option "Check this option to enable squidGuard." is highlighted in yellow. Below this, there is an important note: "Important: Please set up at least one category on the 'Target Categories' tab before enabling. See this link for details. The Save button at the bottom of this page must be clicked to save configuration changes. To activate squidGuard configuration changes, the Apply button must be clicked." There is a green "Apply" button and a status bar indicating "SquidGuard service state: STOPPED". Under "LDAP Options", the "Enable LDAP Filter" checkbox is unchecked. The "LDAP DN" field is empty, with a hint: "Configure your LDAP DN (ex: cn=Administrator,cn=Users,dc=domain)".

Cochez les deux options suivantes pour activer les **logs** : "**Enable GUI Log**" et "**Enable log**".

The screenshot shows the "Logging options" section of the Proxy filter SquidGuard configuration. Under "Service options", there are three input fields: "Rewrite process children" (16), "Rewrite process children startup" (8), and "Rewrite process children idle" (4). Under "Logging options", the "Enable GUI log" checkbox is checked, and the option "Check this option to log the access to the Proxy Filter GUI." is highlighted in yellow. The "Enable log" checkbox is also checked, and the option "Check this option to log the proxy filter settings like blocked websites in Common ACL, Group ACL and Target Categories. This option is usually used to check the filter settings." is highlighted in yellow. The "Enable log rotation" checkbox is unchecked. Under "Miscellaneous", the "Clean Advertising" checkbox is unchecked.

Au sein de la section "**Blacklist**", cochez l'option "**Check this option to enable blacklist**" afin d'activer l'utilisation d'une **blacklist**, c'est-à-dire une liste noire. Nous allons utiliser la **liste noire de L'Université Toulouse Capitole**, car elle est **française, fiable** et existe depuis plusieurs années. Elle contient de nombreuses **catégories** afin de répartir les sites et permettre un **blocage ciblé** selon certaines catégories.

Ensuite, renseignez l'option "**Blacklist URL**" avec l'URL suivante :

[http://dsi.ut-capitole.fr/blacklists/download/blacklists\\_for\\_pfsense.tar.gz](http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz)

Enfin, cliquez sur le bouton "**Save**".

**Miscellaneous**

**Clean Advertising**  Check this option to display a blank gif image instead of the default block page. With this option the user ge

**Blacklist options**

**Blacklist**  Check this option to enable blacklist

**Blacklist proxy**

Blacklist upload proxy - enter here, or leave blank.  
Format: host:[port login:pass] . Default proxy port 1080.  
Example: '192.168.0.1:8080 user:pass'

**Blacklist URL**

Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or l your pfsense (/tmp/blacklist.tar.gz).

Maintenant, basculez sur l'onglet "**Blacklist**" de **SquidGuard**. Cliquez sur le bouton "**Download**" pour télécharger la dernière version de la **liste noire** que nous avons renseignée dans les **paramètres de SquidGuard**.

Package / SquidGuard / Blacklists

General settings Common ACL Groups ACL Target categories Times Rewrites **Blacklist** Log X

**Blacklist Update**

Blacklist DB rebuild progress

1%

Enter FTP or HTTP path to the blacklist archive here.

**Blacklist update Log**

```
Begin blacklist update
Start download.
Download archive http://dsi.ut-capitole.fr/blacklists/download
/blacklists_for_pfsense.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 63 items.
Start rebuild DB.
Completed 1 %
```

Afin d'exploiter la **liste noire**, nous devons créer des règles sous la forme d'**ACL**. Cliquez sur **"Common ACL"** afin de créer une règle de base et commune au sein de **Squid**, tandis que la section **"Groups ACL"** permet de créer des **ACL ciblées** avec plusieurs critères (par exemple : **"bloquer une catégorie selon une plage horaire spécifique"** ou **"bloquer une catégorie à tous les membres d'un groupe Active Directory"**).

Au sein du champ **"Target Rules List"**, vous avez la liste de toutes les **catégories récupérées** à partir de la **blacklist toulousaine**.

Package / Proxy filter SquidGuard: Common Access Control List (ACL) / Common ACL ?

General settings **Common ACL** Groups ACL Target categories Times Rewrites Blacklist Log XMLRPC Sync

**General Options**

Target Rules

**Target Rules List** + -

ACCESS: 'whitelist' - always pass; 'deny' - block; 'allow' - pass, if not blocked.

**Target Categories**

[blk_blacklists_adult]	access	deny	▼
[blk_blacklists_agressif]	access	---	▼
[blk_blacklists_arjel]	access	---	▼
[blk_blacklists_associations_religieuses]	access	---	▼
[blk_blacklists_astrology]	access	---	▼
[blk_blacklists_audio-video]	access	---	▼
[blk_blacklists_bank]	access	---	▼
[blk_blacklists_bitcoin]	access	---	▼
[blk_blacklists_blog]	access	---	▼
[blk_blacklists_celebrity]	access	---	▼
[blk_blacklists_chat]	access	---	▼
[blk_blacklists_child]	access	---	▼
[blk_blacklists_cleaning]	access	---	▼
[blk_blacklists_cooking]	access	---	▼
[blk_blacklists_cryptojacking]	access	---	▼
[blk_blacklists_publicite]	access	---	▼
[blk_blacklists_radio]	access	---	▼
[blk_blacklists_reaffected]	access	---	▼
[blk_blacklists_redirector]	access	---	▼
[blk_blacklists_remote-control]	access	---	▼
[blk_blacklists_residential-proxies]	access	---	▼
[blk_blacklists_sect]	access	---	▼
[blk_blacklists_sexual_education]	access	deny	▼
[blk_blacklists_shopping]	access	---	▼
[blk_blacklists_shortener]	access	---	▼
[blk_blacklists_social_networks]	access	---	▼
[blk_blacklists_special]	access	---	▼
[blk_blacklists_sports]	access	---	▼
[blk_blacklists_stalkerware]	access	---	▼
[blk_blacklists_strict_redirector]	access	---	▼
[blk_blacklists_strong_redirector]	access	---	▼
[blk_blacklists_translation]	access	---	▼
[blk_blacklists_tricheur]	access	---	▼
[blk_blacklists_tricheur_pix]	access	---	▼
[blk_blacklists_update]	access	---	▼
[blk_blacklists_vpn]	access	---	▼
[blk_blacklists_warez]	access	---	▼
[blk_blacklists_webmail]	access	---	▼
Default access [all]	access	allow	▼

Dans notre cas, nous devons bloquer la catégorie "**Pornographie**" correspondante à "**[blk\_blacklists\_adult]**" et "**[blk\_blacklists\_sexual\_education]**", il faut donc modifier la valeur du champ "**access**" pour préciser "**deny**".

En complément, pensez à configurer la valeur du champ "**Default access [all]**" sur "**allow**" pour autoriser toutes les autres catégories (par défaut).

Afin d'éviter qu'un petit malin contourne la restriction en précisant l'adresse **IP du serveur distant** à la place du nom de domaine, cochez l'option "**Do not allow IP-Addresses in URL**".

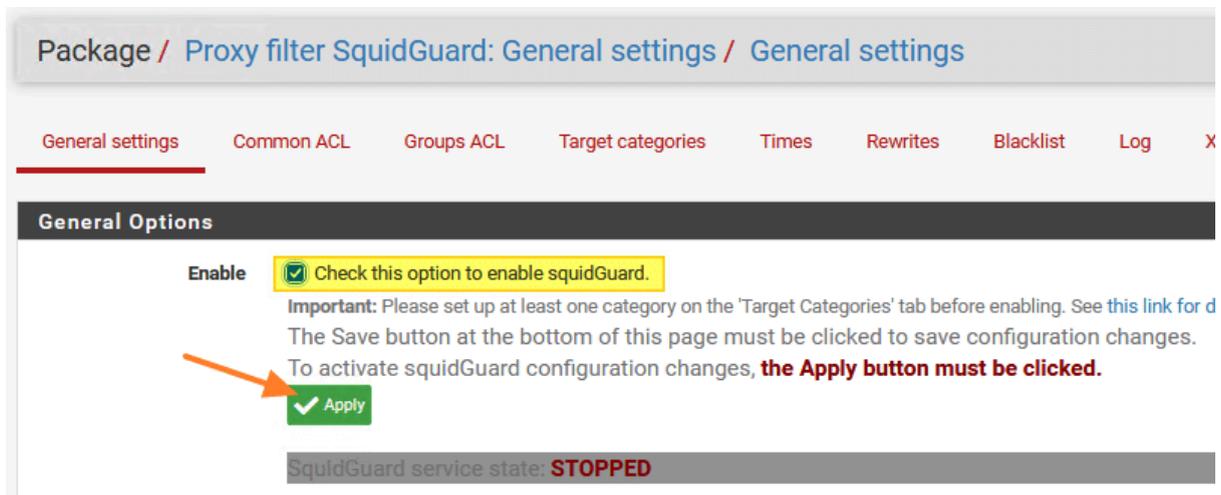
En complément, si vous souhaitez utiliser la fonction **SafeSearch** des moteurs de recherche, cochez la case "**Use SafeSearch Engine**", tout en sachant que cela permet d'utiliser **Google, Bing, DuckDuckGo, Qwant**, etc.

<b>Do not allow IP-Addresses in URL</b>	<input checked="" type="checkbox"/> To make sure that people do not bypass the URL filter by simply using the IP-Addresses instead of the FQDN you can check this option. This option has no effect on the whitelist.
<b>Proxy Denied Error</b>	<input type="text"/> The first part of the error message displayed to clients when access was denied. Defaults to "Request denied by \$g[product_name] proxy"
<b>Redirect mode</b>	<input type="text" value="int error page (enter error message)"/> Select redirect mode here. Note: if you use 'transparent proxy', then 'int' redirect mode will not be accessible. Options: <a href="#">ext url err page</a> , <a href="#">ext url redirect</a> , <a href="#">ext url as 'move'</a> , <a href="#">ext url as 'found'</a> .
<b>Redirect info</b>	<input type="text"/> Enter external redirection URL, error message or size (bytes) here.
<b>Use SafeSearch engine</b>	<input checked="" type="checkbox"/> Enable the protected mode of search engines to limit access to mature content. At the moment it is supported by Google, Yandex, Yahoo, MSN, Live Search, Bing, DuckDuckGo, OneSearch, Rambler, Ecosia and Qwant. Make sure that the search engines can be accessed. It is recommended to prohibit access to others. Note: This option overrides 'Rewrite' setting.
<b>Rewrite</b>	<input type="text" value="none (rewrite not defined)"/> Enter the rewrite condition name for this rule or leave it blank.

**Enfin**, activez les **logs** pour cette règle en cochant l'option "**Log**" tout en bas, puis cliquez sur "**Save**".

<b>Log</b>	<input checked="" type="checkbox"/> Check this option to enable logging for this ACL.
<input type="button" value="Save"/>	

La configuration étant prête, retournez dans "General Settings", cochez l'option "Check this option to enable SquidGuard" et cliquez sur "Apply".



Package / Proxy filter SquidGuard: General settings / General settings

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log X

**General Options**

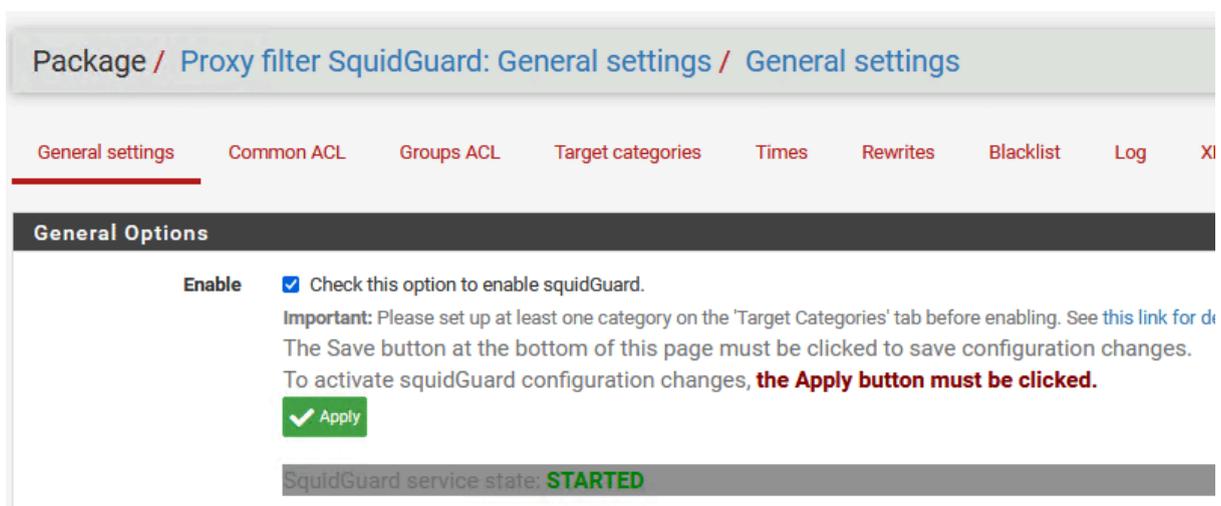
Enable  Check this option to enable squidGuard.

**Important:** Please set up at least one category on the 'Target Categories' tab before enabling. See [this link for d](#)  
The Save button at the bottom of this page must be clicked to save configuration changes.  
To activate squidGuard configuration changes, **the Apply button must be clicked.**

SquidGuard service state: **STOPPED**

Le statut du service SquidGuard doit changer et passer sur "STARTED". Si ce n'est pas le cas, vérifiez que Squid a bien démarré de son côté.

**Remarque importante :** à chaque fois que vous modifiez la configuration de SquidGuard (exemple : bloquer une catégorie supplémentaire), il faut impérativement venir dans l'onglet "General Settings" pour cliquer sur le bouton "Apply" sinon les modifications ne sont pas prises en compte !



Package / Proxy filter SquidGuard: General settings / General settings

General settings Common ACL Groups ACL Target categories Times Rewrites Blacklist Log X

**General Options**

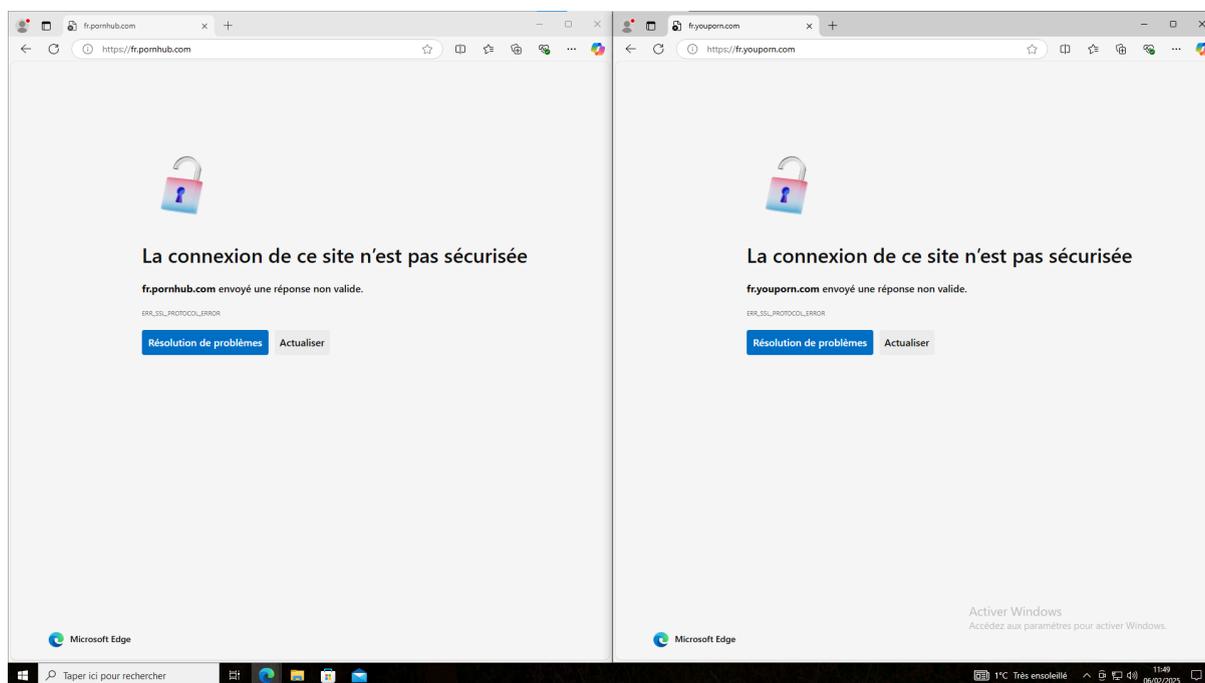
Enable  Check this option to enable squidGuard.

**Important:** Please set up at least one category on the 'Target Categories' tab before enabling. See [this link for d](#)  
The Save button at the bottom of this page must be clicked to save configuration changes.  
To activate squidGuard configuration changes, **the Apply button must be clicked.**

SquidGuard service state: **STARTED**

→ Test du proxy

**Pour tester si notre filtrage fonctionne correctement**, on va devoir consulter des **sites pornographiques** pour voir si le **proxy bloque bien** le site :



**Après avoir testé deux sites pornographiques différents**, on voit que **les sites se sont bien fait bloquer** et sont **inaccessibles**.