Documentation technique

Mise en place de sites web sous certificat HTTPS et d'un reverse proxy Pfsense (environnement Proxmox).

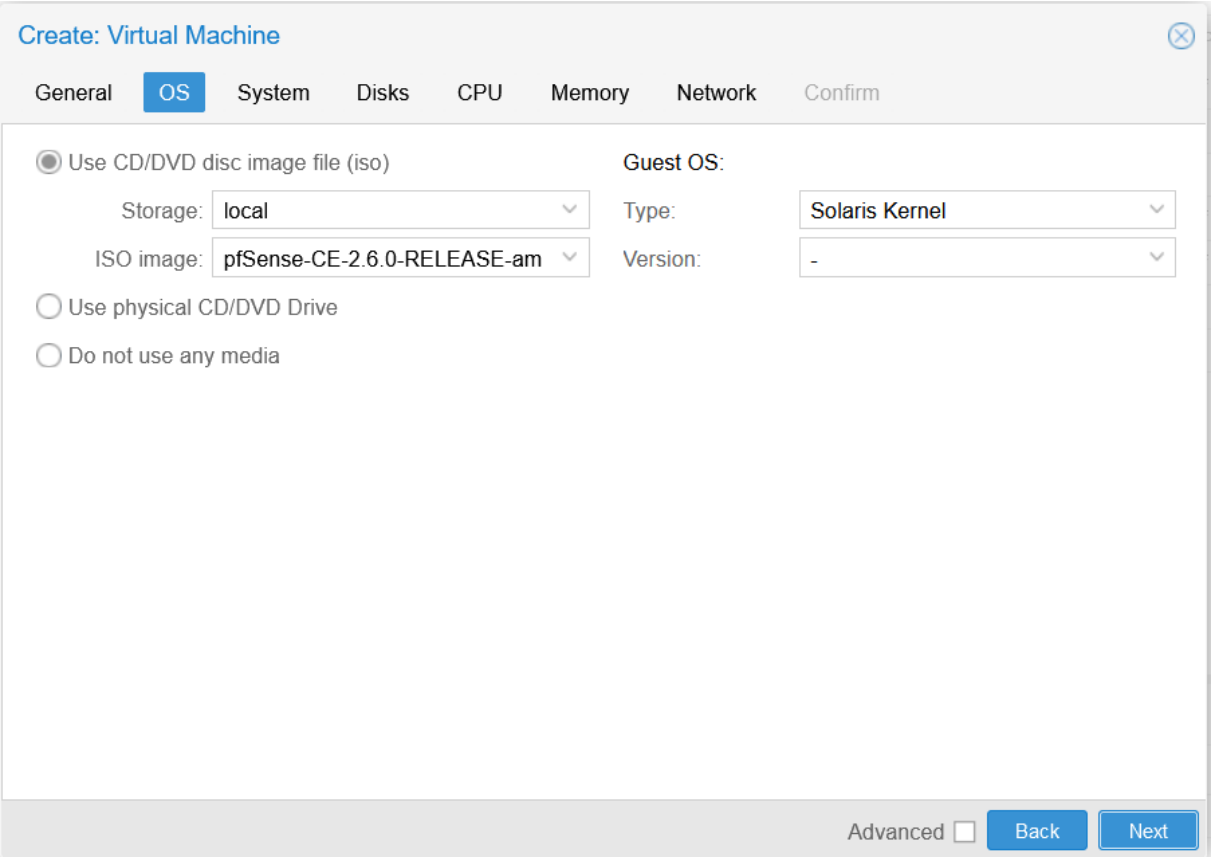
Table des matières :

ETAPE 1 – Installation de Pfsense

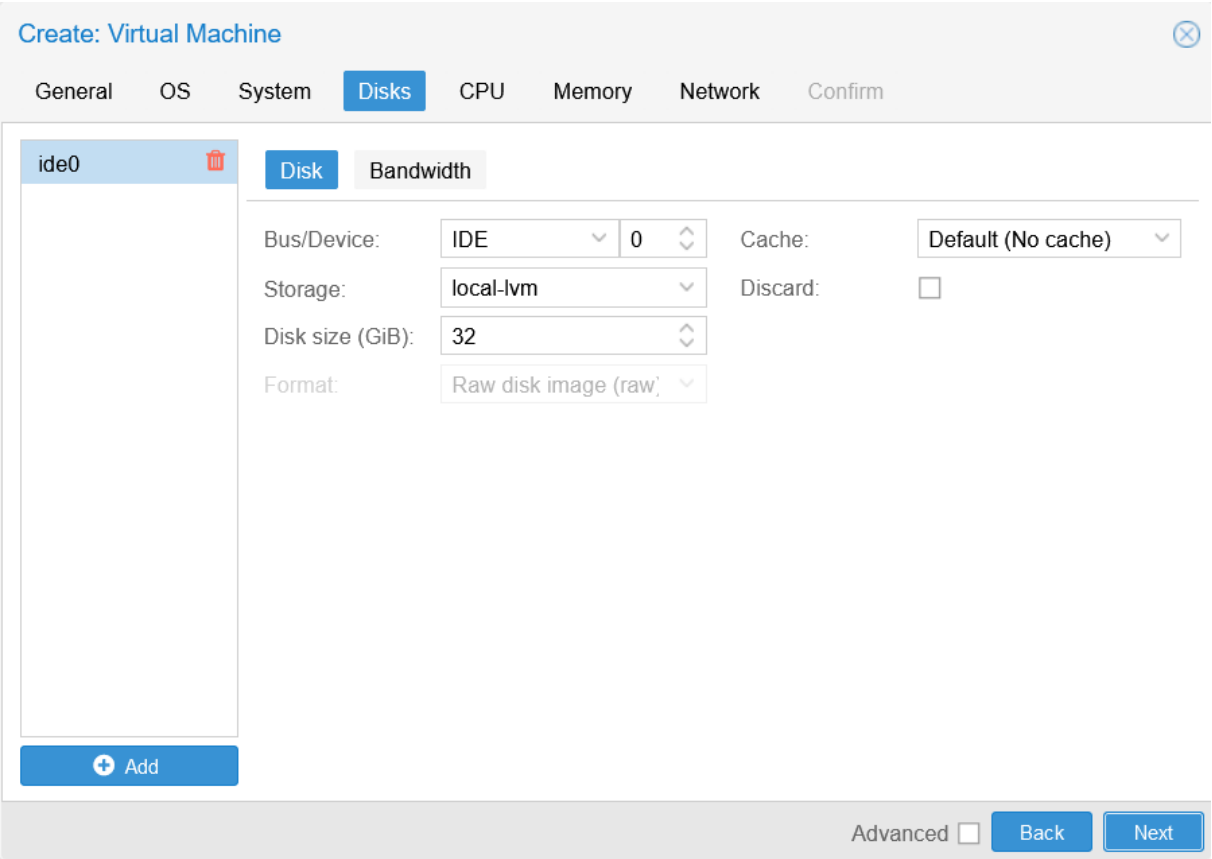
Partie proxmox :

On va tout d'abord créer notre VM dans Proxmox en sélectionnant "Create a VM".

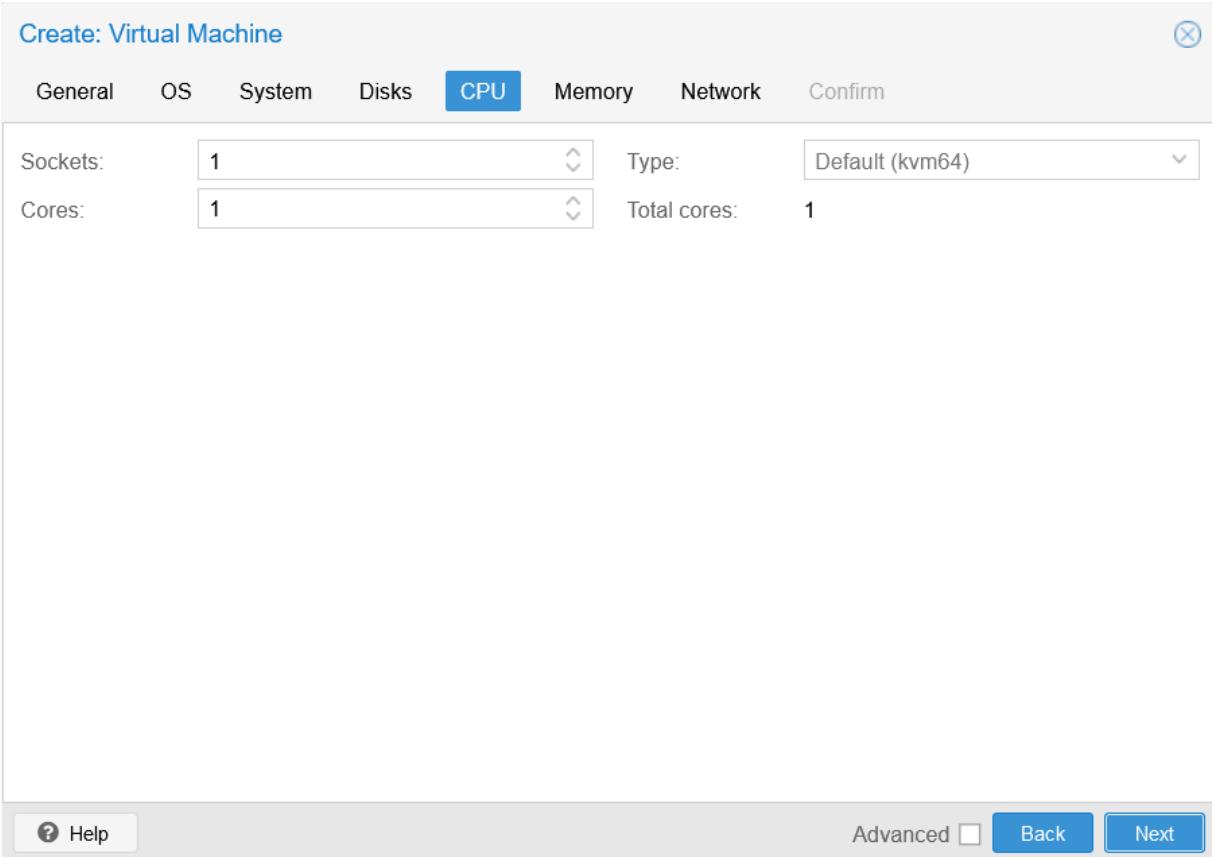
Puis dans "OS", sélectionnez votre ISO pfSense préalablement téléchargé et le type d'OS "Solaris Kernel".



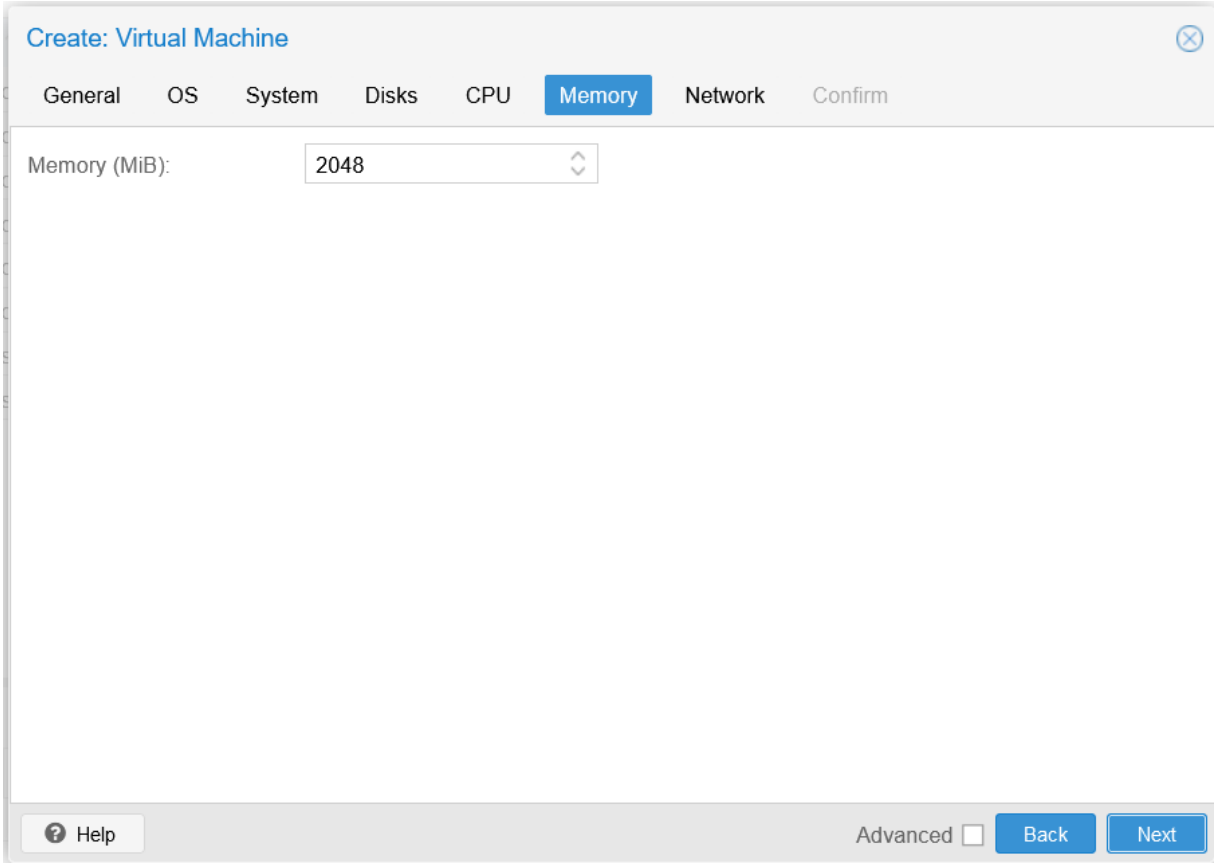
Dans “disks”, indiquez une taille de disque de 32 Go.



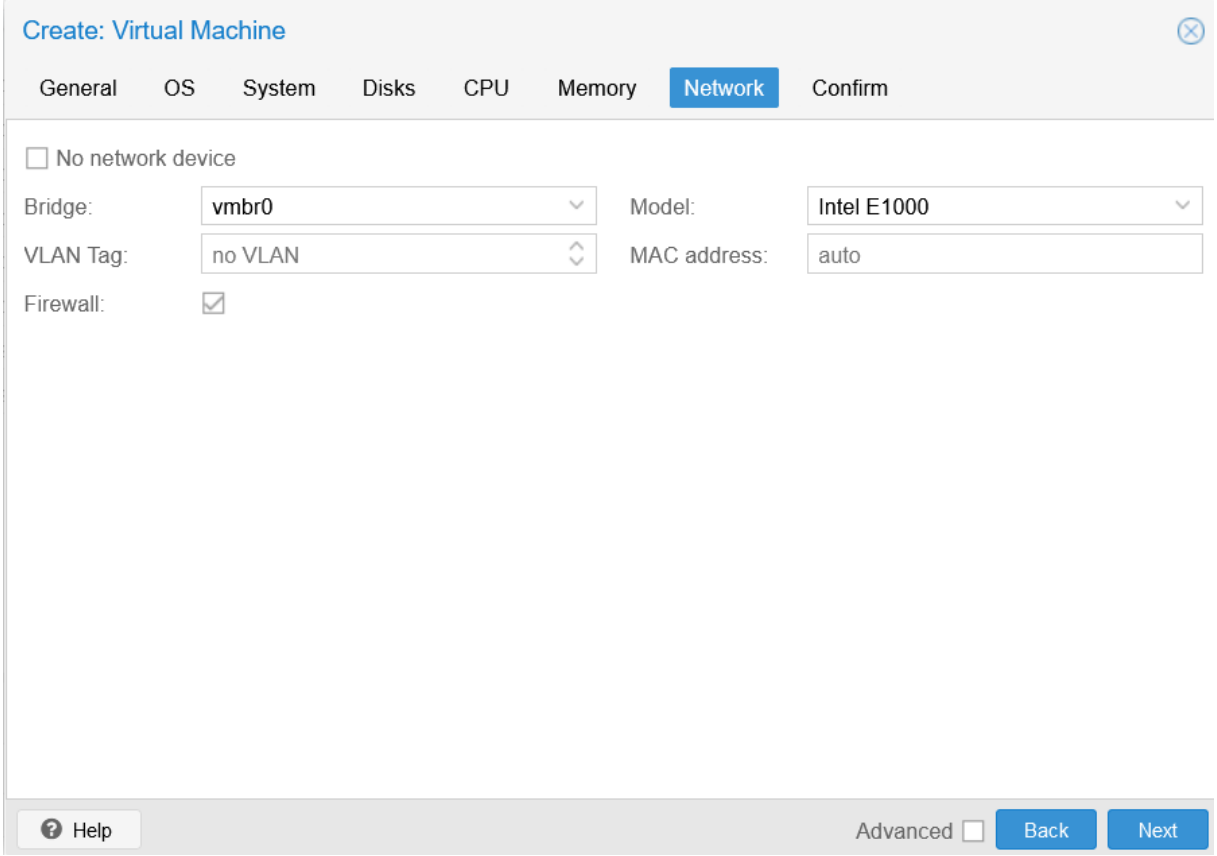
Dans “CPU”, sélectionnez 1 socket et 1 cœur.



Dans “Memory”, mettez environ 2048 MiB.

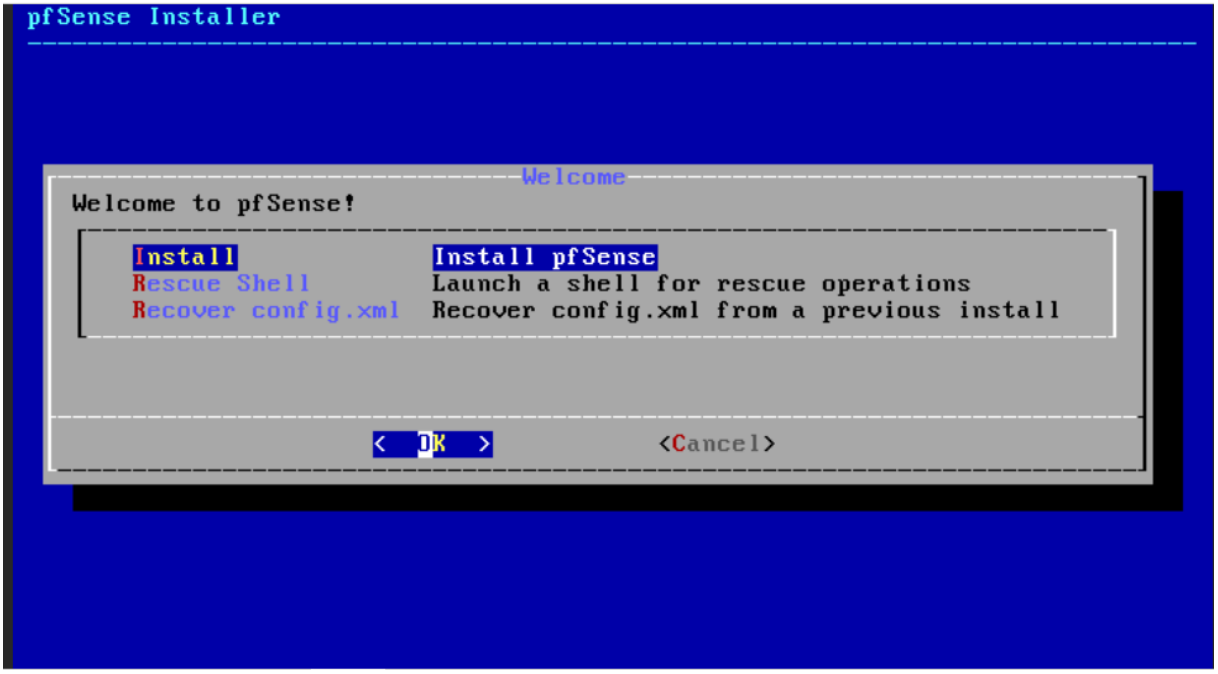


Dans “Network”, sélectionner le bridge existant. Le paramétrage de la VM est alors terminé. Les paramètres vus dans cette partie peuvent évidemment varier selon les besoins.

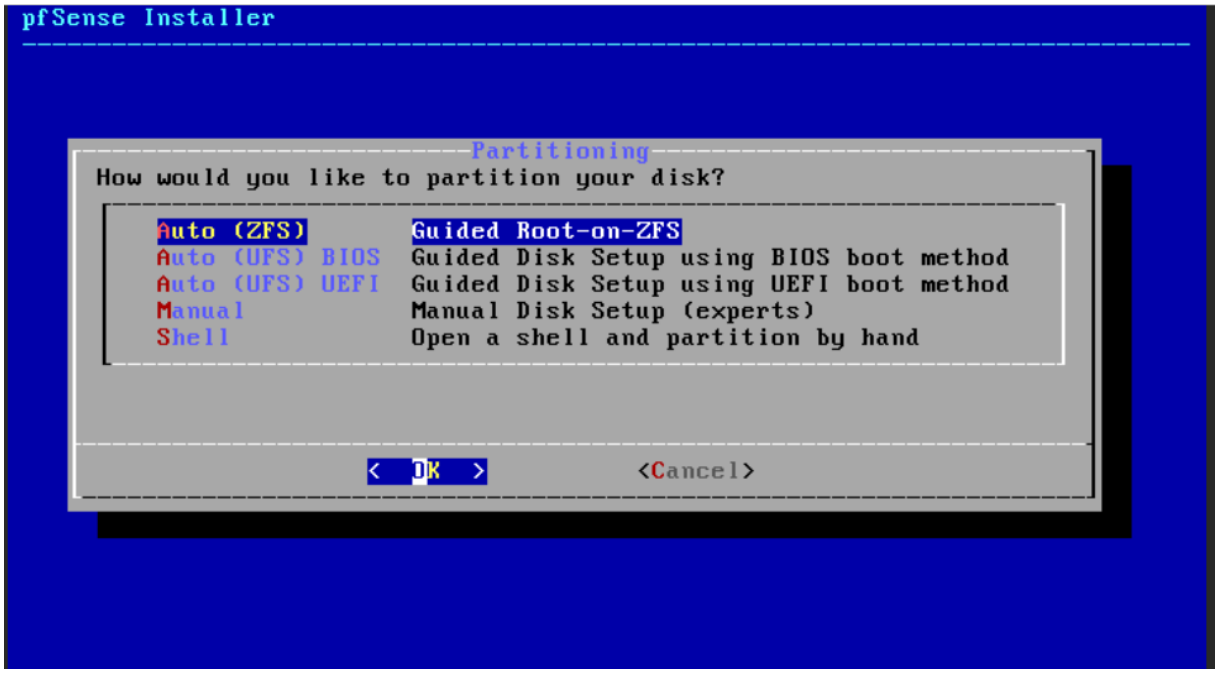


Partie ligne de commande Pfsense :

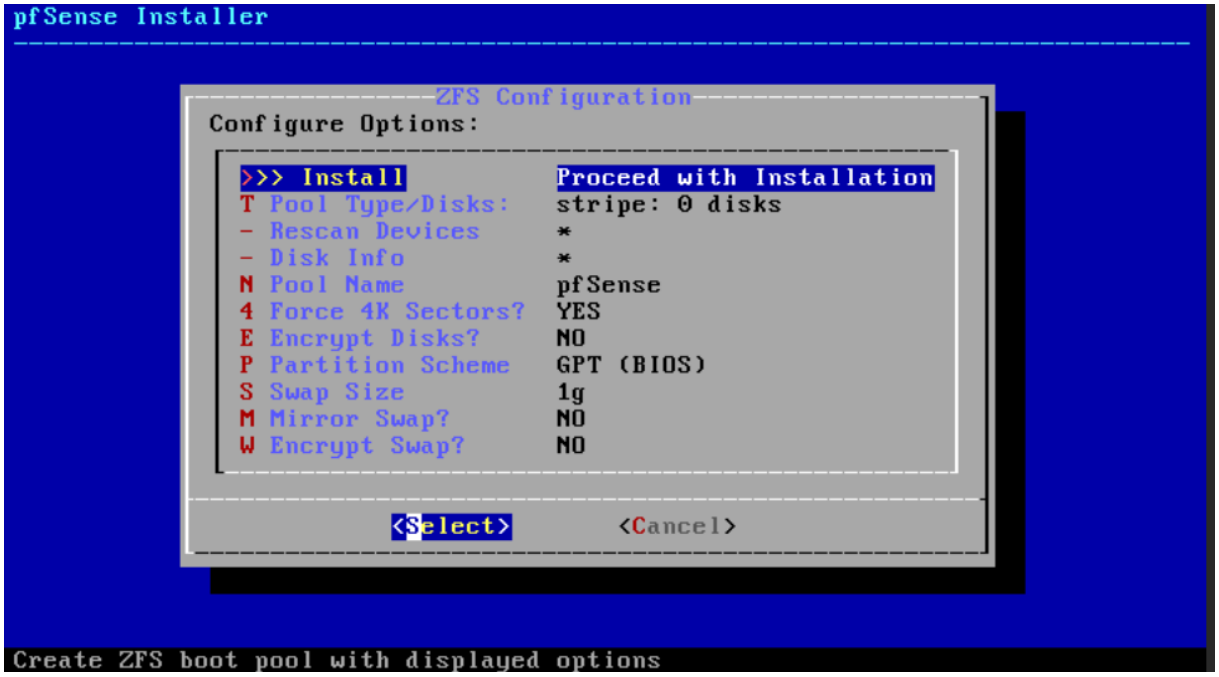
Choisir l'option "Install pfSense".



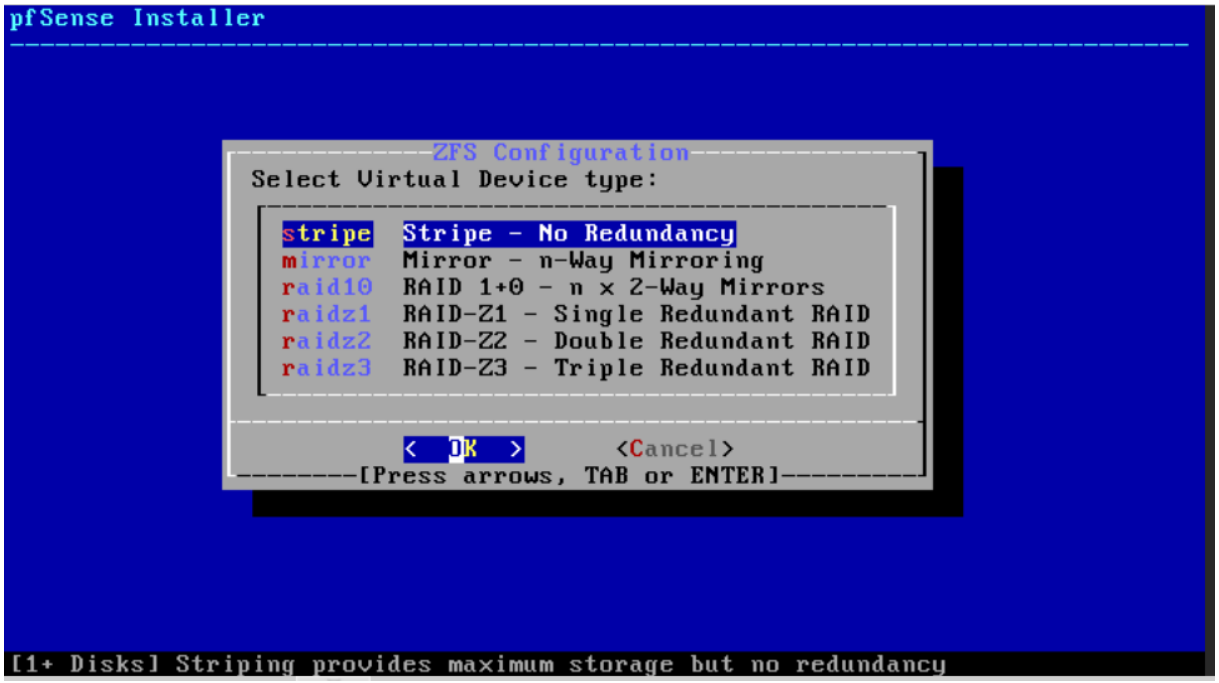
Sélectionner la langue puis appuyer 2 fois sur entrer.



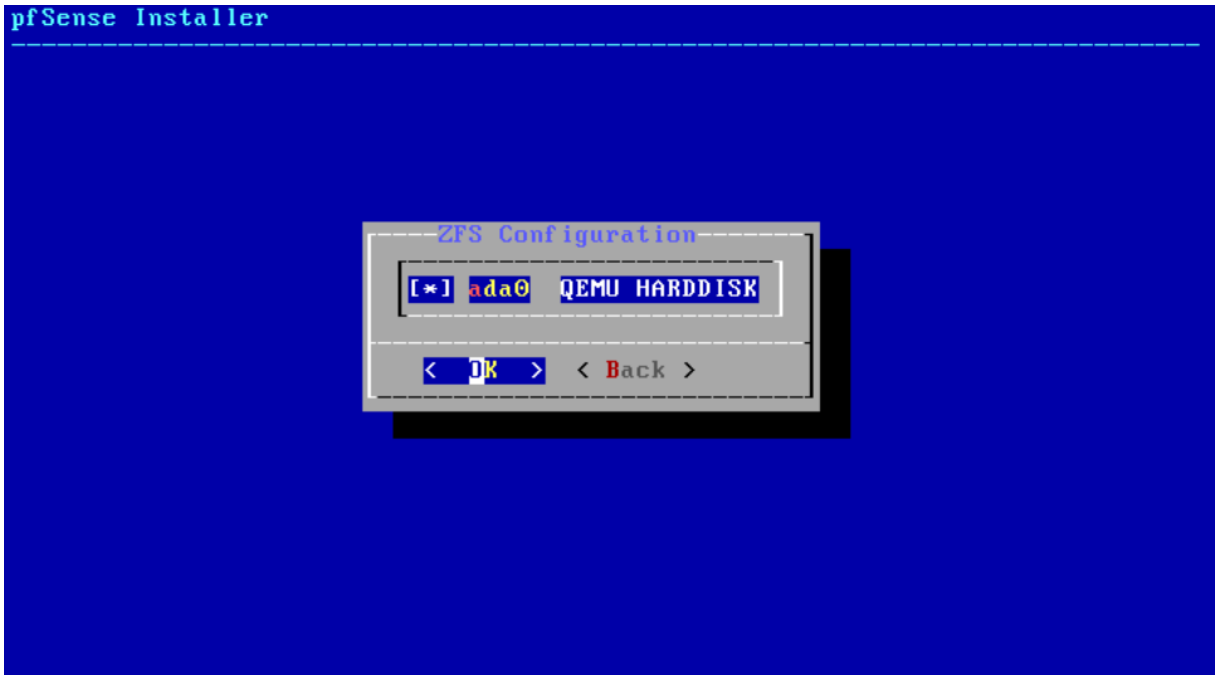
Sélectionner “proceed with Installation” puis appuyer 2 fois sur entrer.



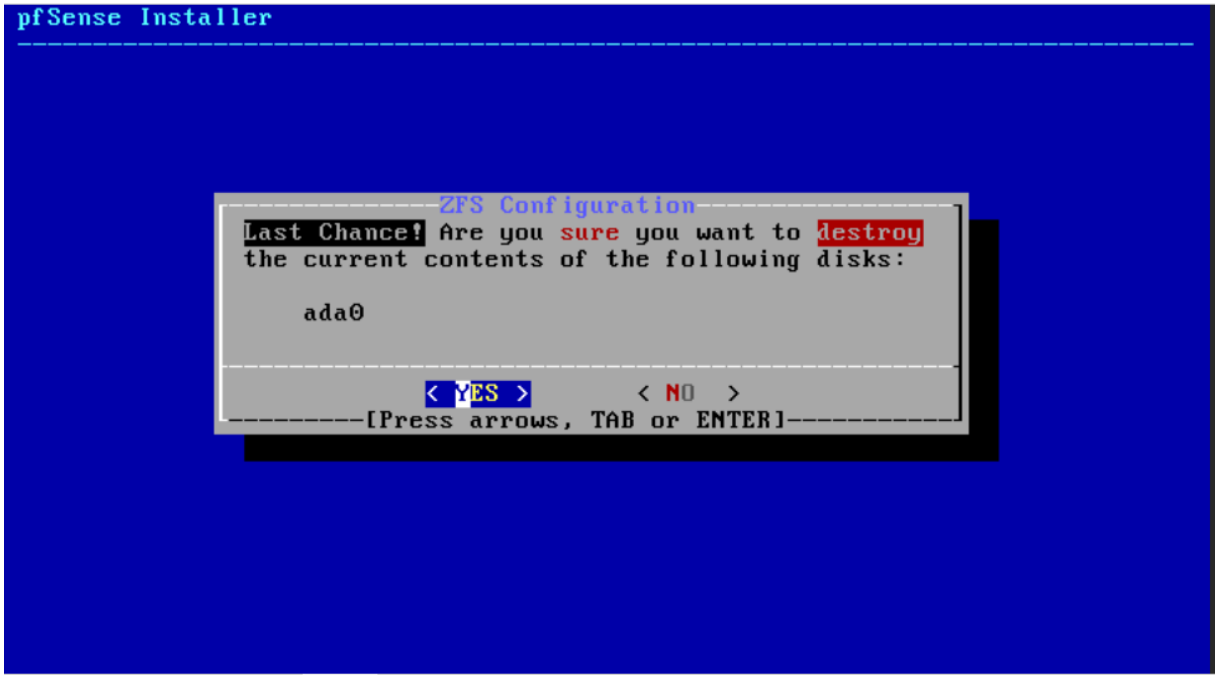
Sélectionner “stripe - No Redundancy” (On ne créer pas de raid lors de cette étape).



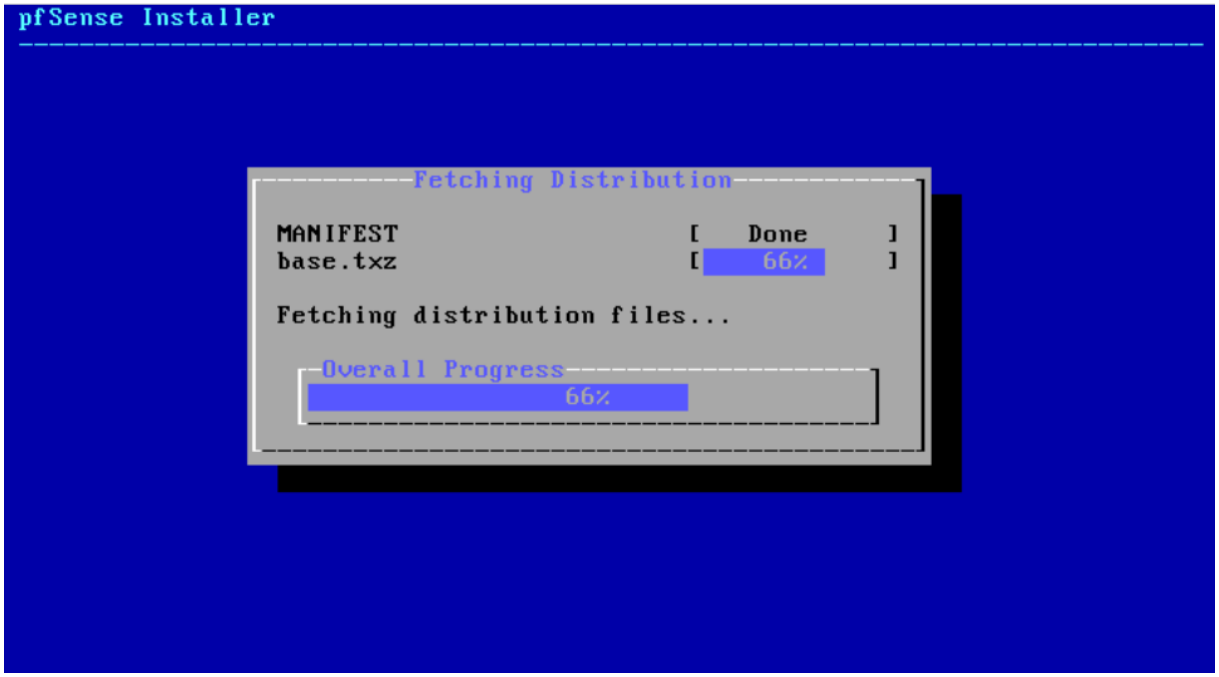
Appuyer sur espace puis sur entrer pour sélectionner le disque puis passer à l'étape suivante.



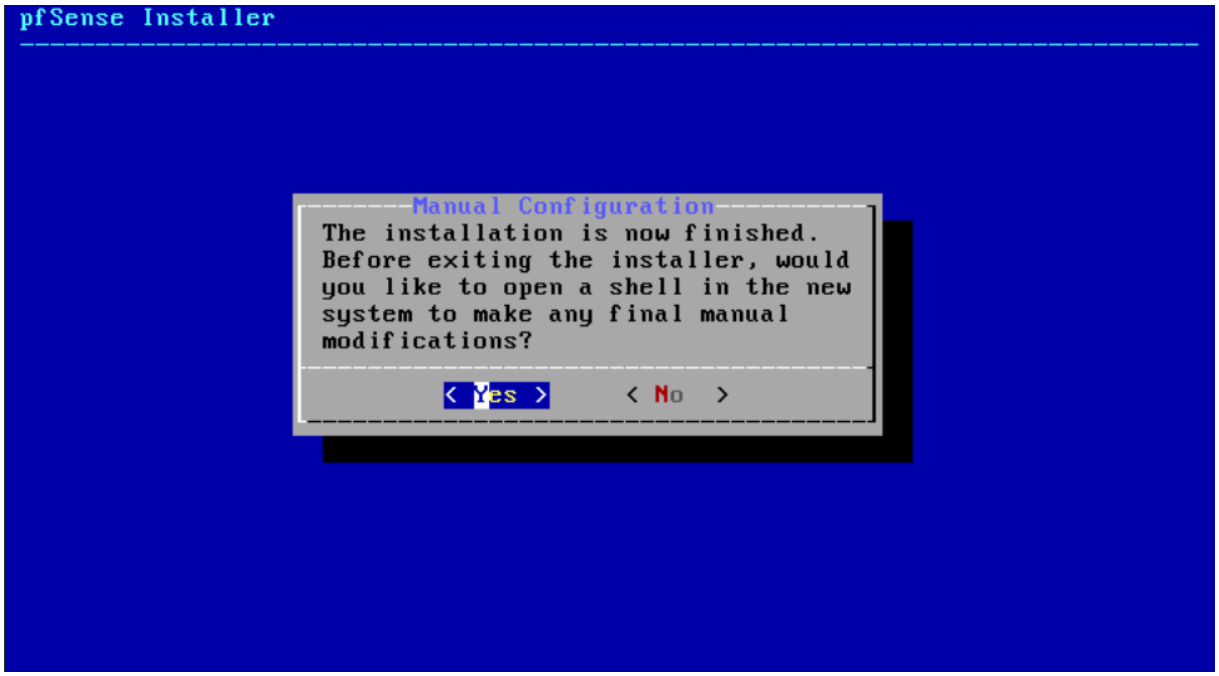
Valider en sélectionnant "Yes".



La barre de progression de l'installation va se lancer.



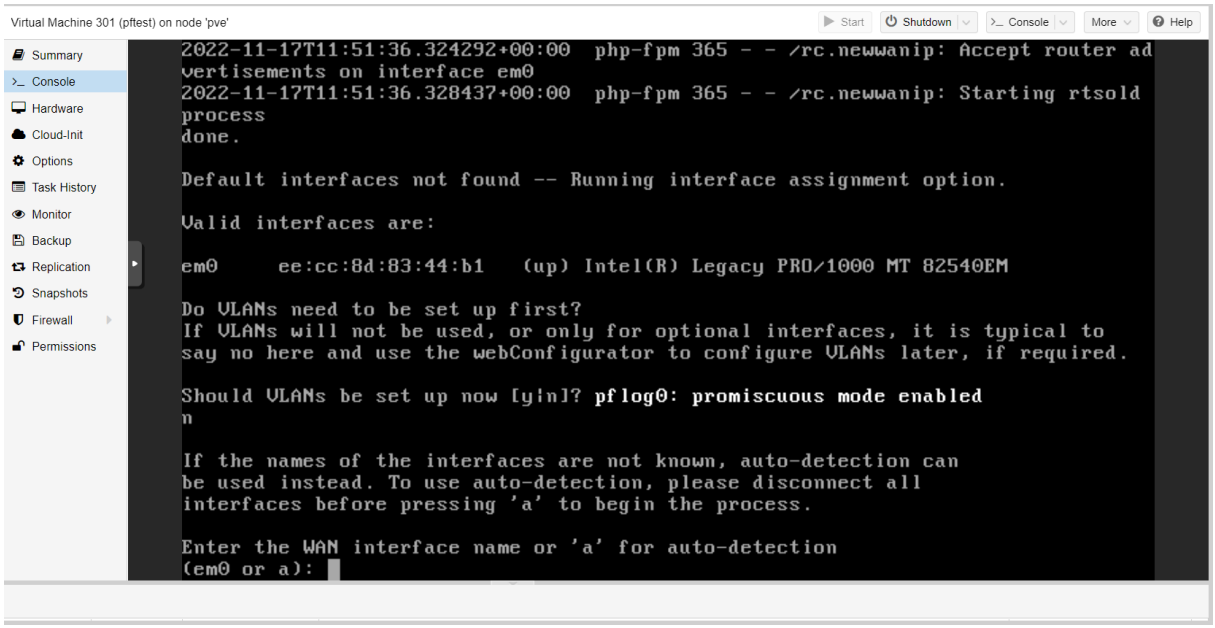
Une fois l'installation terminée, l'assistant d'installation propose d'ouvrir le Shell. Sélectionner "Yes".



Après ouverture de Shell tapez la commande “exit” afin de sorte de Shell, la machine redémarrera automatiquement.

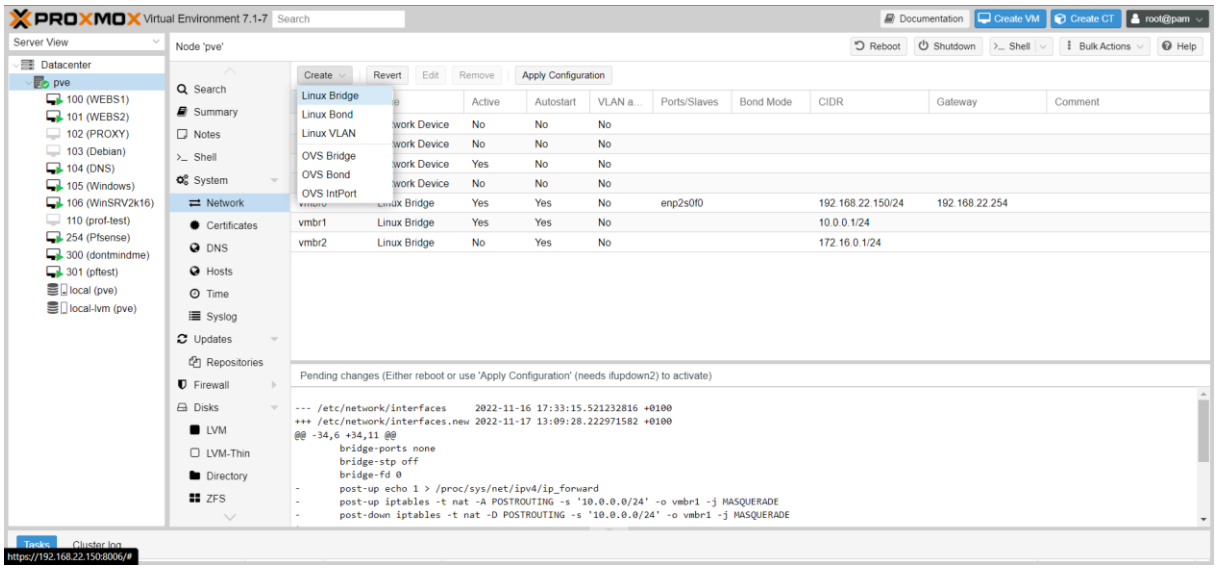
```
When finished, type 'exit' to reboot.
#
```

Une fois la machine redémarrer, vous vous retrouvez sur cette interface.

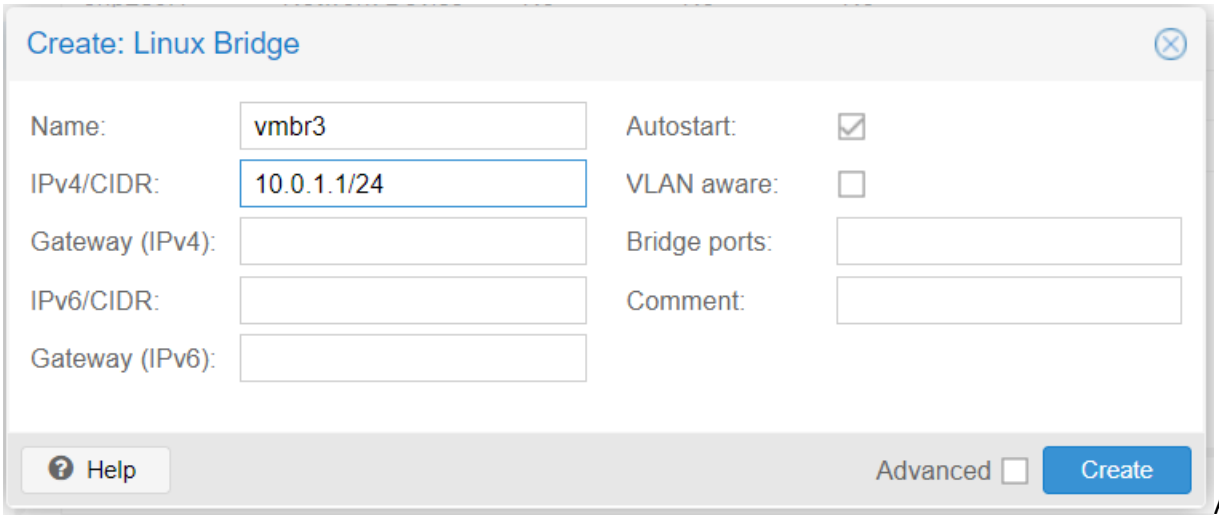


Pour la suite de notre manipulation nous aurons besoin de rajouter une LAN. Pour cela aller dans le « pve » puis, dans la section « Network ».

Cliquer ensuite sur « Create » et selectionner « Linux Bridge » .

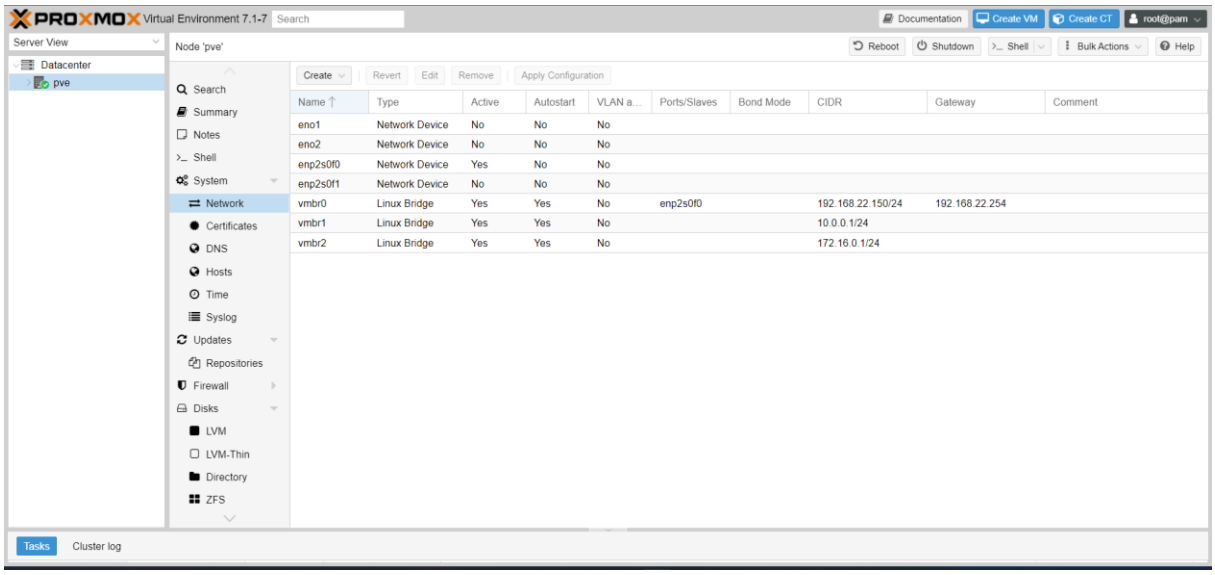


Entrer l'adresse IP et le masque de sous réseau de votre LAN. Vous pouvez également renommer votre LAN mais cela est optionnel.

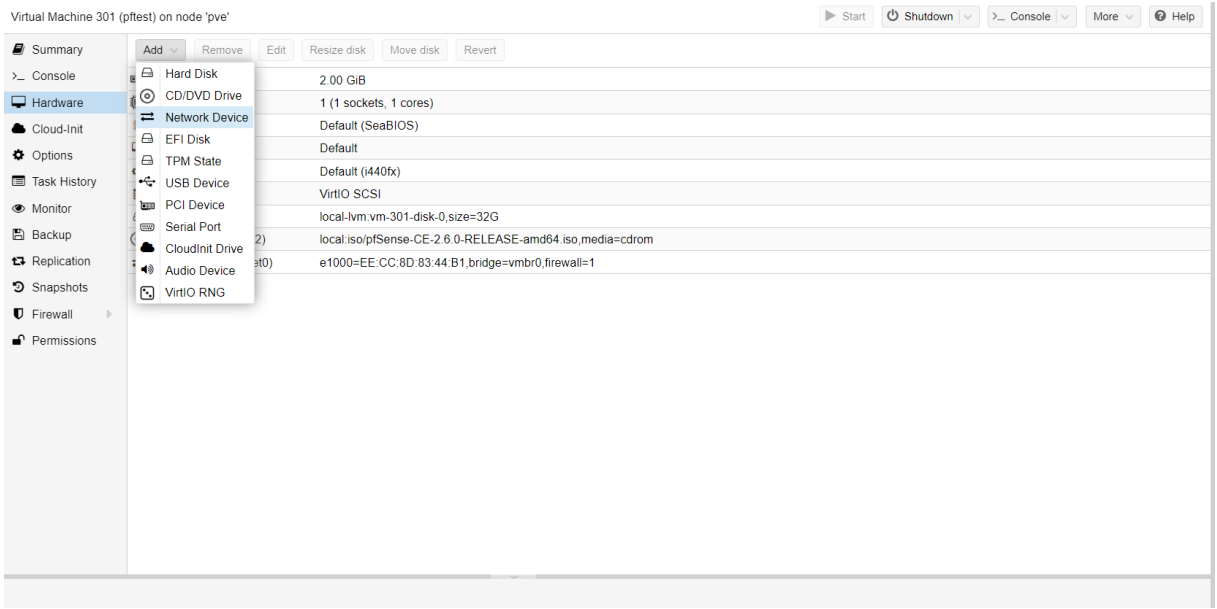


Après la

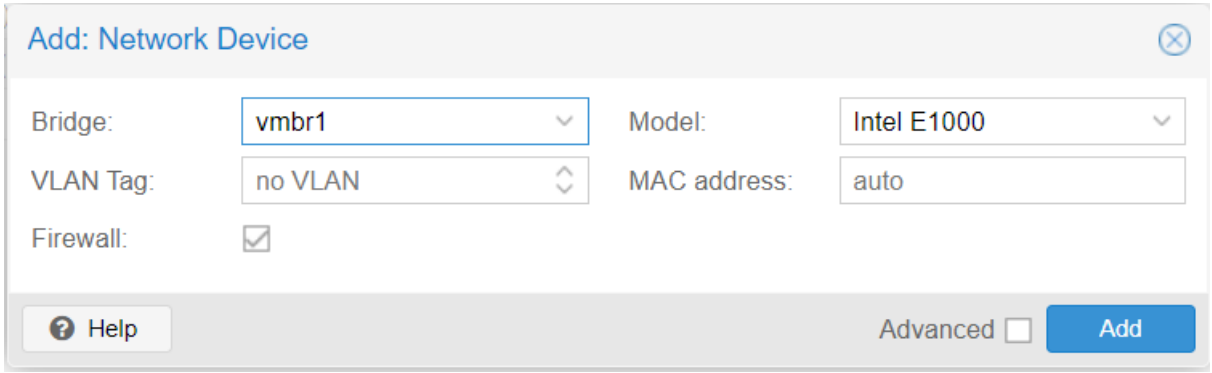
Création de la LAN, cliquer sur « Apply Configuration » pour confirmer la création de votre LAN et l'activer.



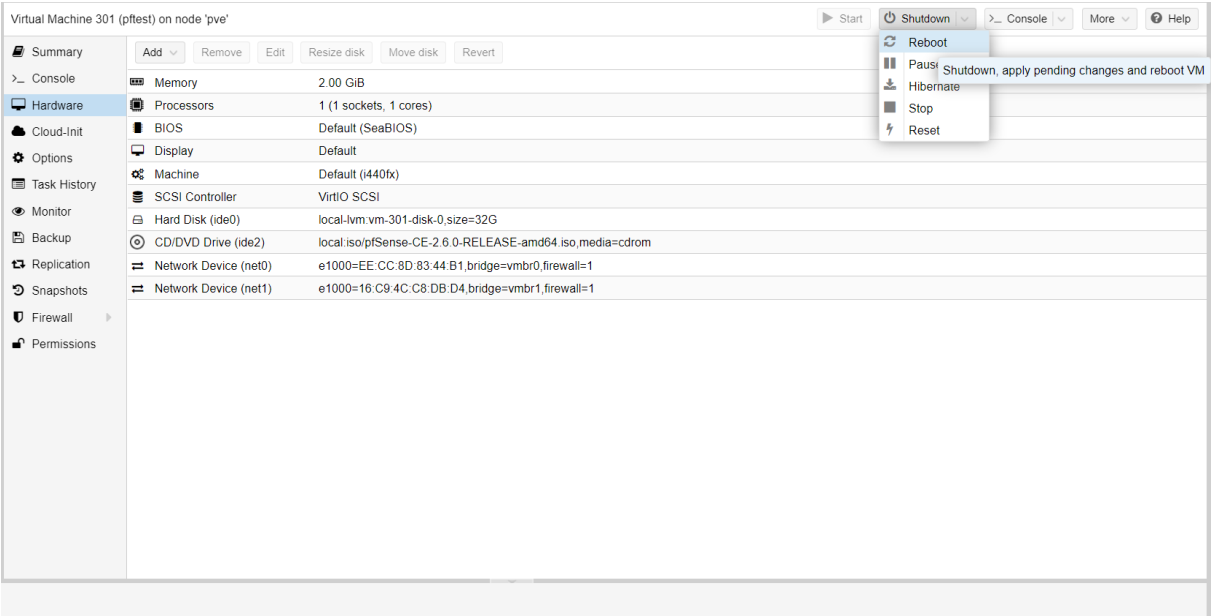
Dirigez-vous ensuite sur votre machine dans l'onglet « Hardware ». Cliquez sur « Add » puis « Network ».



Ajoutez la LAN que vous venez de créer.

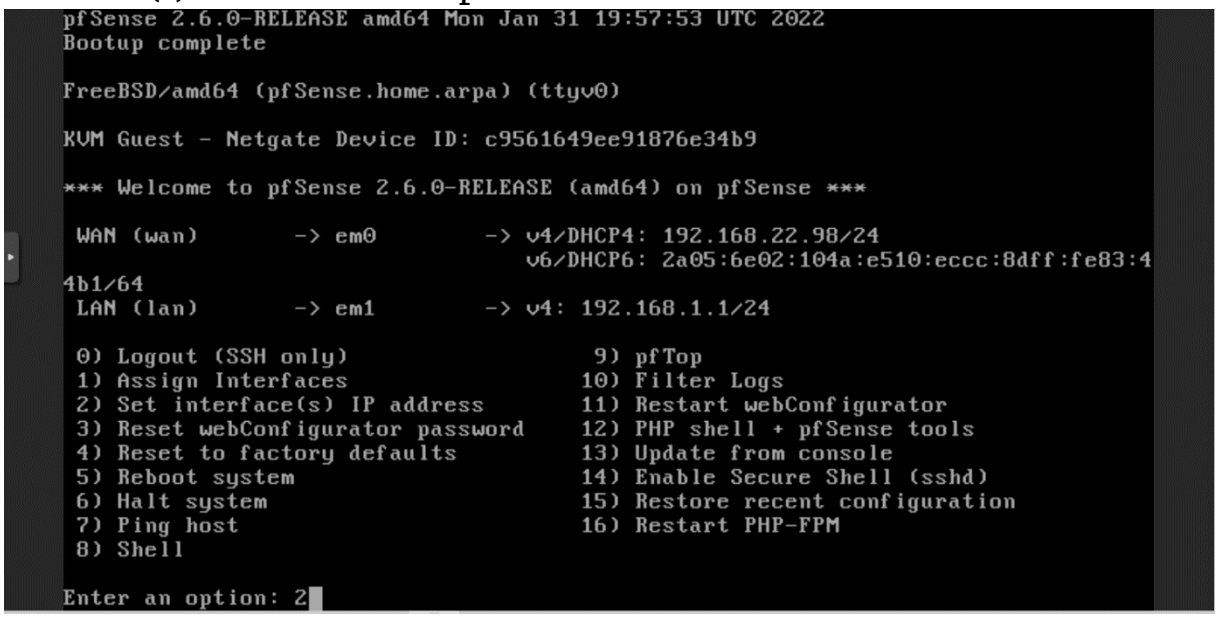


Redémarrer votre machine afin que les modifications apporter soient prises en compte.



Une fois la VM redémarrée, vous remarquerez que l'adresse IP de votre LAN n'est pas cela que vous lui avez donné.

Il faudra donc le modifier manuellement. Pour cela, dirigez-vous dans la section « Set interface(s) IP address » en tapant la commande 2.



Vous aurez le choix de modifier l'adresse IP de votre WAN et votre LAN. Tapez la commande 2 afin de configurer votre LAN.

```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.22.98/24
                                  v6/DHCP6: 2a05:6e02:104a:e510:eccc:8dff:fe83:4
4b1/64
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24

 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 (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

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

Tapez l'adresse IP de votre LAN, puis son masque de sous-réseau.
Tapez ensuite l'adresse IP de la paserelle.
Laissez la section IPv6 vide et appuyez sur entrée pour passer cette étape.

```
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
You cannot set network address to an interface
Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 172.16.0.1

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

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:
> 172.16.0.254

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

La VM vous demandera si vous voulez le DHCP du LAN dont nous n'aurons pas besoin alors tapez la commande "n".

```
> 172.16.0.1

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

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:
> 172.16.0.254

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
```

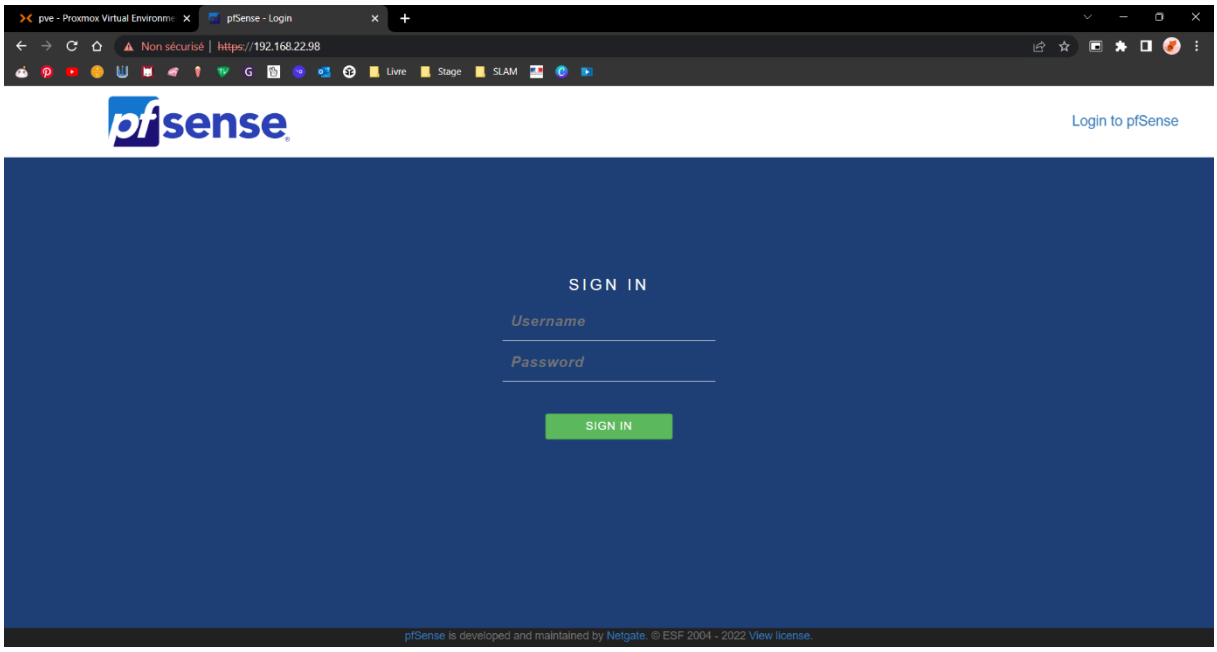
L'adresse IP de votre LAN a bien été changée.

```
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://172.16.0.1/

Press <ENTER> to continue.
KVM Guest - Netgate Device ID: e002dee83994e92c1ab8

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.22.98/24
                                  v6/DHCP6: 2a05:6e02:104a:e510:eccc:8dff:fe83:4
4b1/64
 LAN (lan)       -> em1        -> v4: 172.16.0.1/24

 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:
```

Afin de pouvoir accéder à l'interface pfsense nous avons besoin d'en accorder l'accès, pour cela tapez la commande "8" pour aller dans la catégorie "Shell"

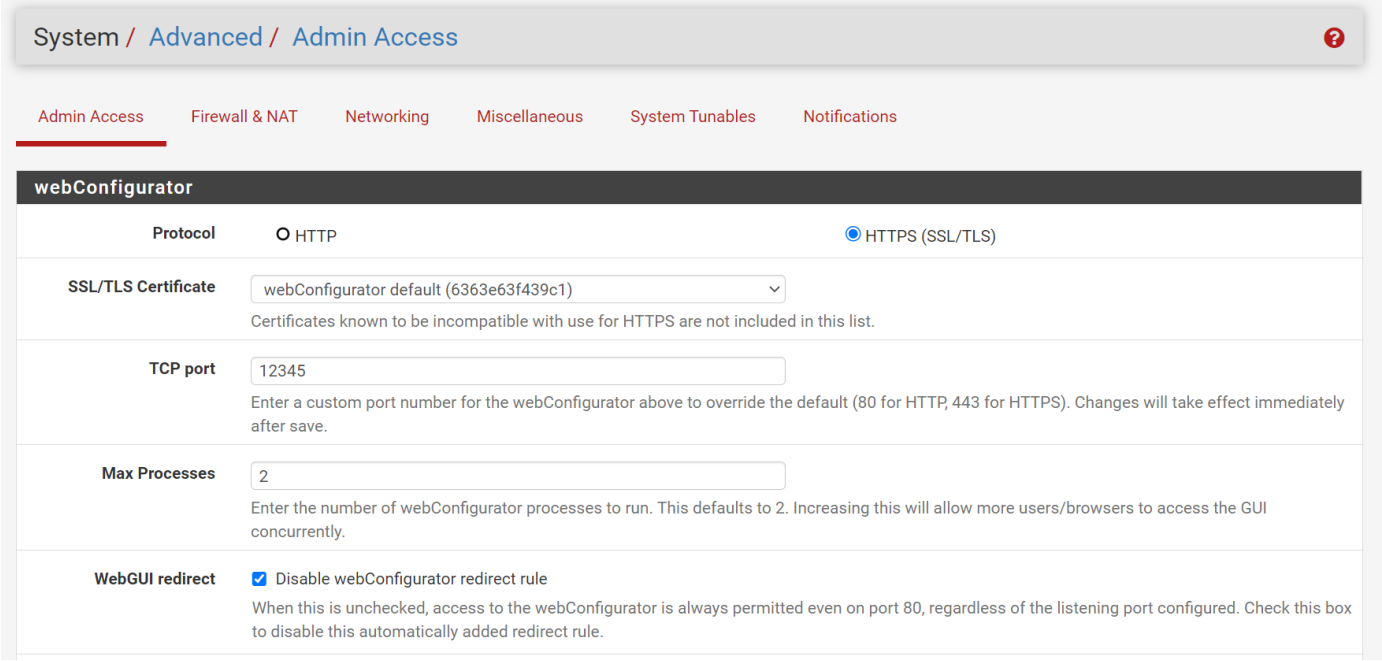
```
Press <ENTER> to continue.
KVM Guest - Netgate Device ID: e002dee83994e92c1ab8

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 192.168.22.98/24
                                  v6/DHCP6: 2a05:6e02:104a:e510:eccc:8dff:fe83:4
4b1/64
 LAN (lan)       -> em1        -> v4: 172.16.0.1/24

 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: 8

[2.6.0-RELEASE][root@pfSense.home.arpa]/root: pfctl -d
pf disabled
[2.6.0-RELEASE][root@pfSense.home.arpa]/root:
```

Vous pouvez maintenant entrer l'adresse IP WAN de votre pfsense dans la barre de recherche de votre navigateur et ainsi accéder à l'interface de connexion de pfsense.

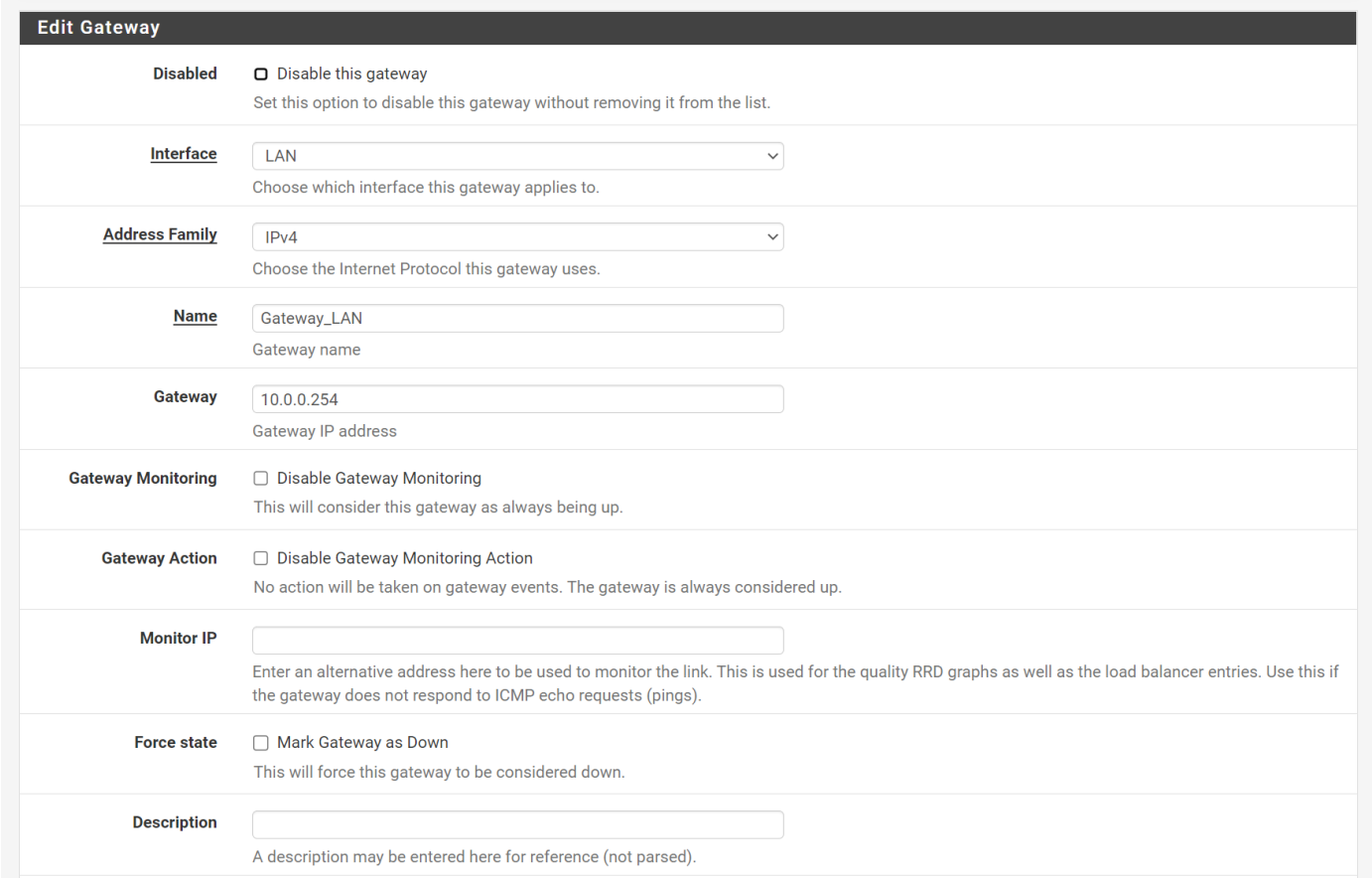


ETAPE 2 – CONFIGURATION DU PFSENSE PAR L'INTERFACE

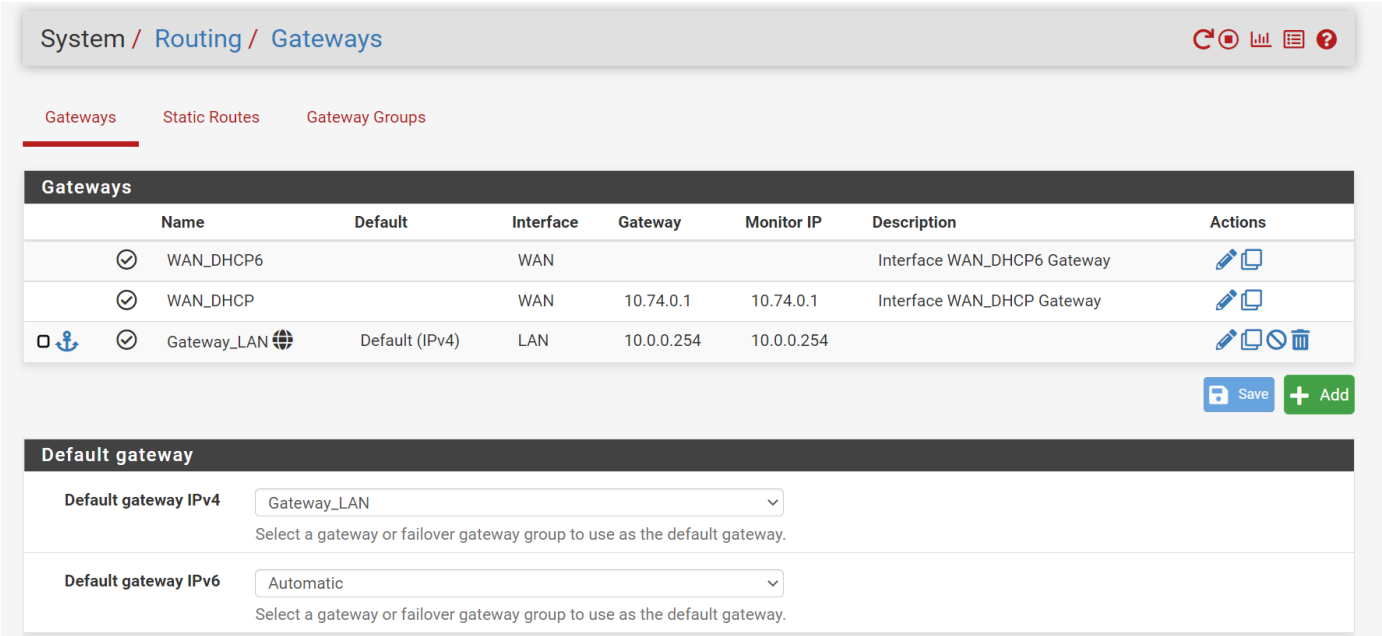
Sur l'interface Pfense allez dans System, Advanced puis Admin access. Dans les paramètres qui s'affichent cochez le HTTPS, changez votre port admin selon votre préférence (pas de 80 ou 443), et cochez « Disable webConfigurator redirect rule ». Cela va empêcher la connexion en cas d'échec sur le port 80.



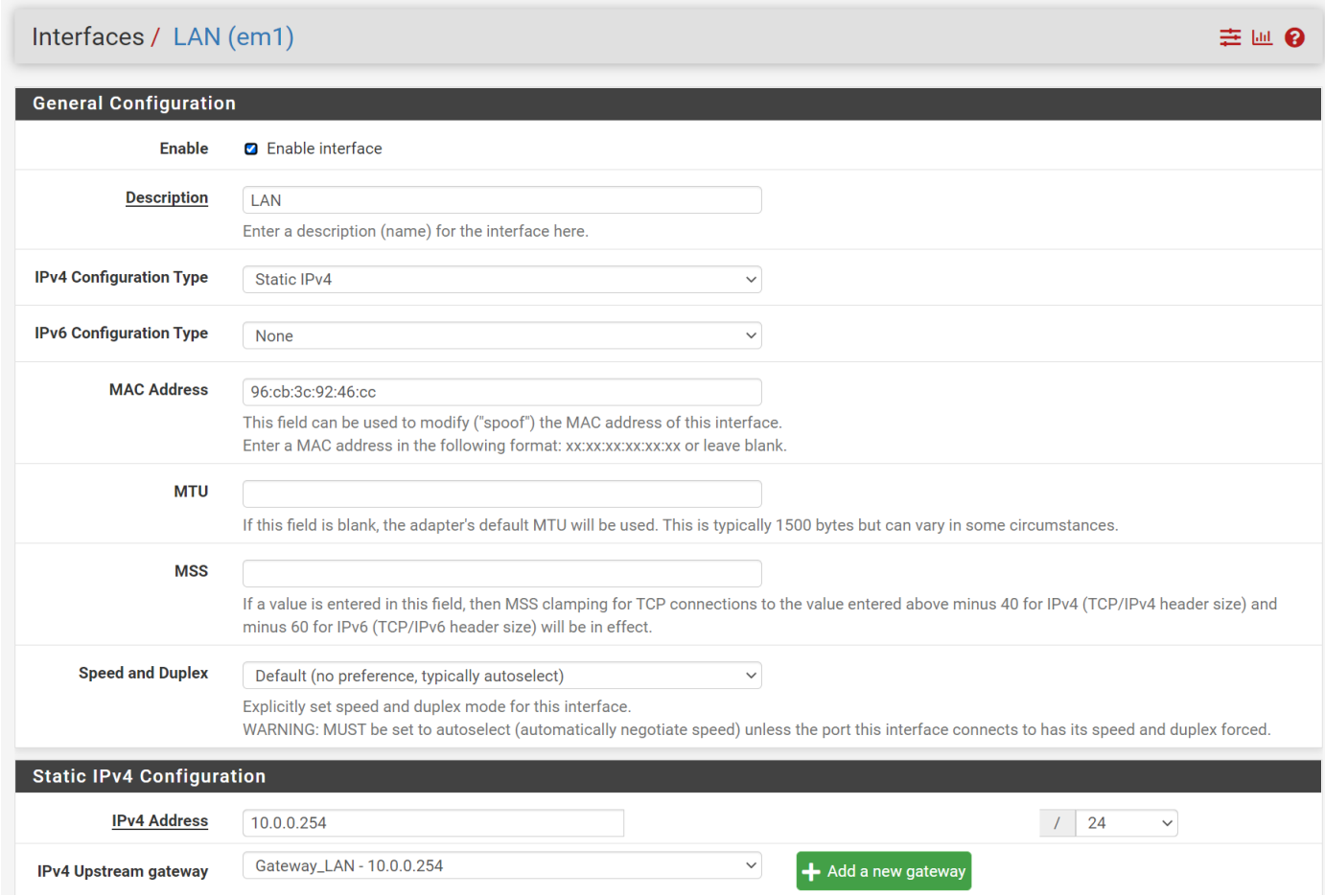
Aller dans System, Routing puis Gateways. Ici nous allons créer une règle de Gateway en appuyant sur « Add ». Une fenêtre de paramètres va s'ouvrir. Dans interface on met LAN, dans l'Address Family on choisit IPv4, on attribue un nom et une adresse IP à la gateway. Ensuite on save en bas de page.



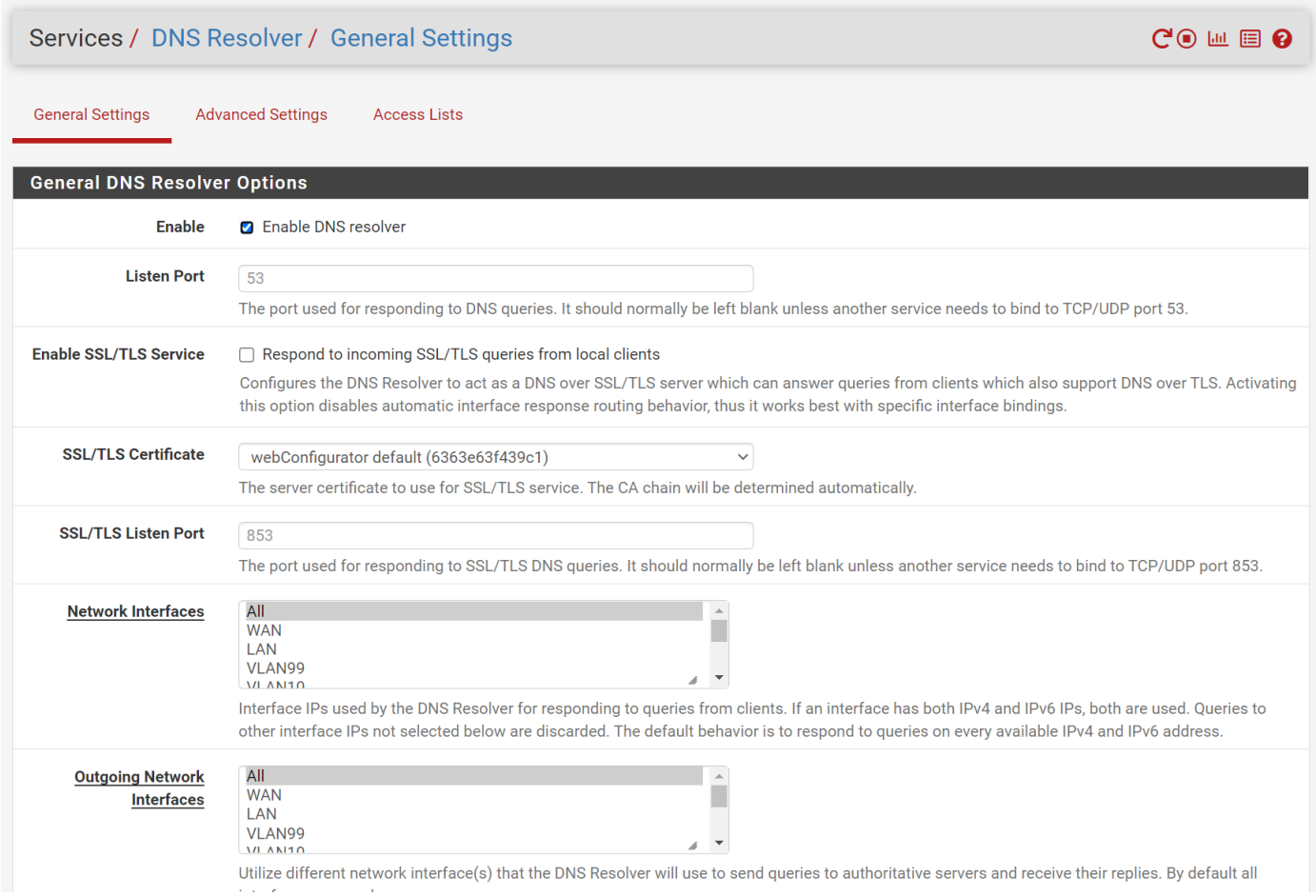
Dans la liste des Gateways une nouvelle ligne s'affiche. Dans la Default gateway IPv4 sélectionnez celle que nous venons de créer.

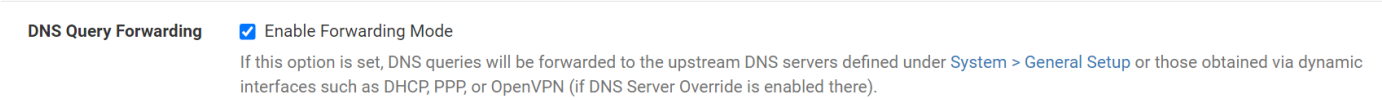


Aller dans Interfaces, LAN (em1). Une fenêtre de paramètres s'ouvre. Il faut cocher Enable interface, préciser Static Ipv4 dans le General Configuration. Plus bas dans Static Ipv4 Configuration, on entre l'adresse IP de notre Gateway précédente et on la sélectionne. On finit par Save.

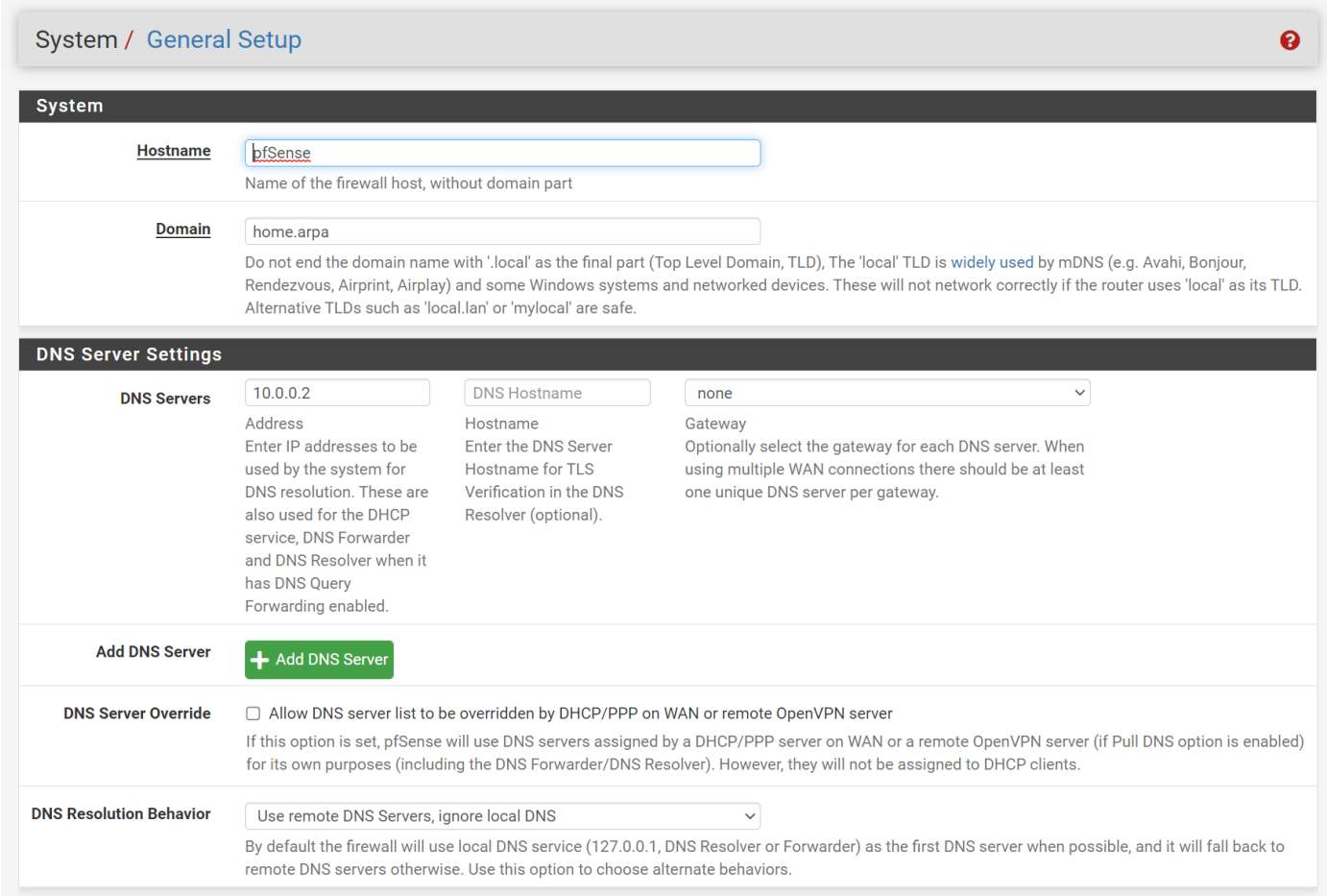


Maintenant que la gateway este fait nous allons configurer le DNS. Dans Services, DNS Resolver, General Settings, on coche Enable DNS Resolver. Puis on coche plus bas Enable Forwading Mode dans DNS Query Forwading. Puis on save.

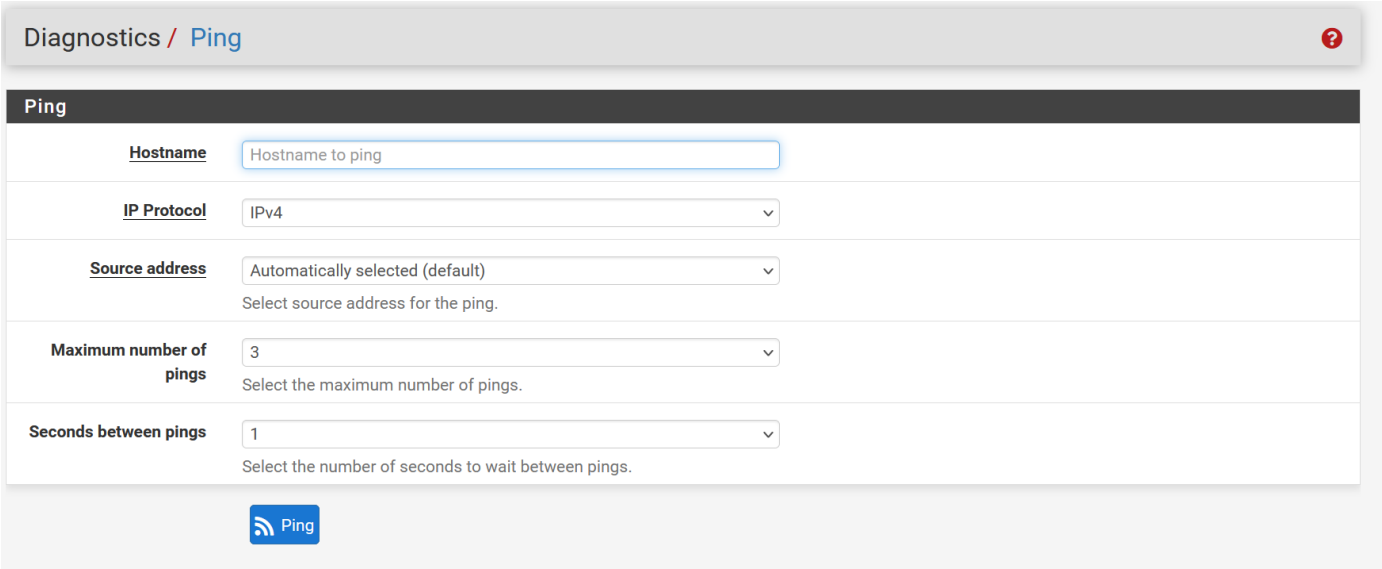




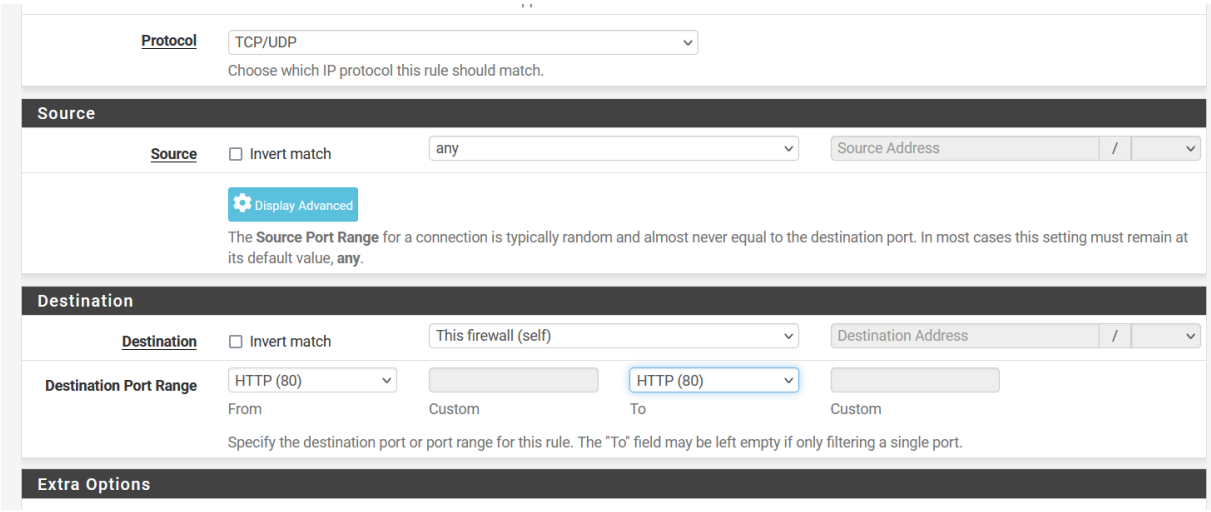
Désormais le pfsense sera capable de se rediriger vers le serveur DNS afin de résoudre les domains names connus. Dans System, General Setup, entrer l'adresse IP du serveur DNS en question. Et sélectionner « Use remote DNS Servers, ignore local DNS ».

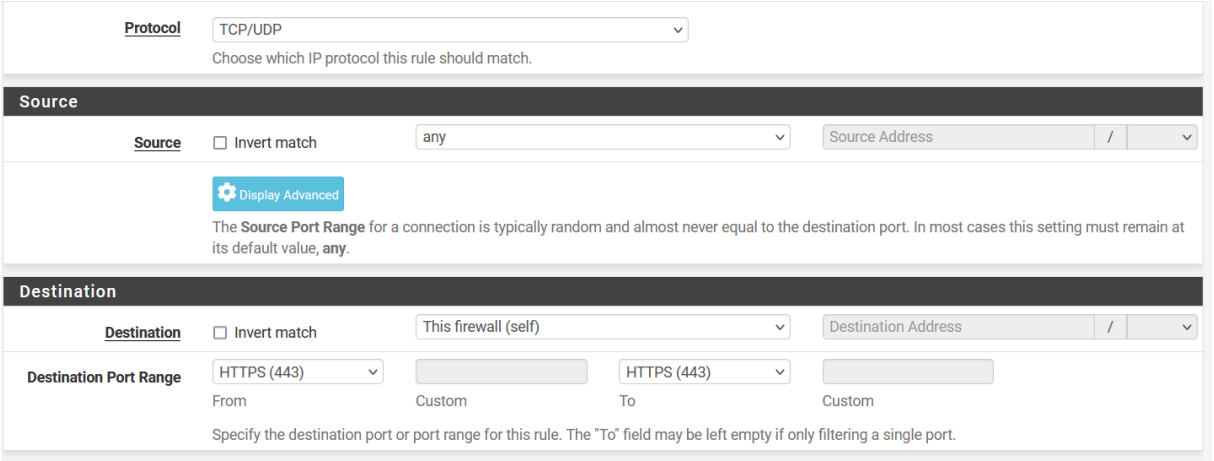


Si les configurations ont bien été faites, dans Diagnostics, Ping, vous pourrez confirmer qu'il est possible de ping les serveurs web que ce soit par leur adresse IP ou par leurs noms suivi du nom de domaine. Sinon testez un « systemctl restart networking ».



Dans Firewall, Rules, WAN, assurez-vous d'autoriser les requêtes http et https sur le proxy. Il faut sélectionner TCP/UDP, de la source voulue, vers This firewall avec http et https. Rappel, leurs ports respectifs sont le port 80 et le port 443. A chaque fin d'ajout, n'oubliez pas de save en bas.





Le tableau de règles devrait ressembler à ceci :

Firewall / Rules / WAN

Floating | WAN | LAN | VLAN99 | VLAN10

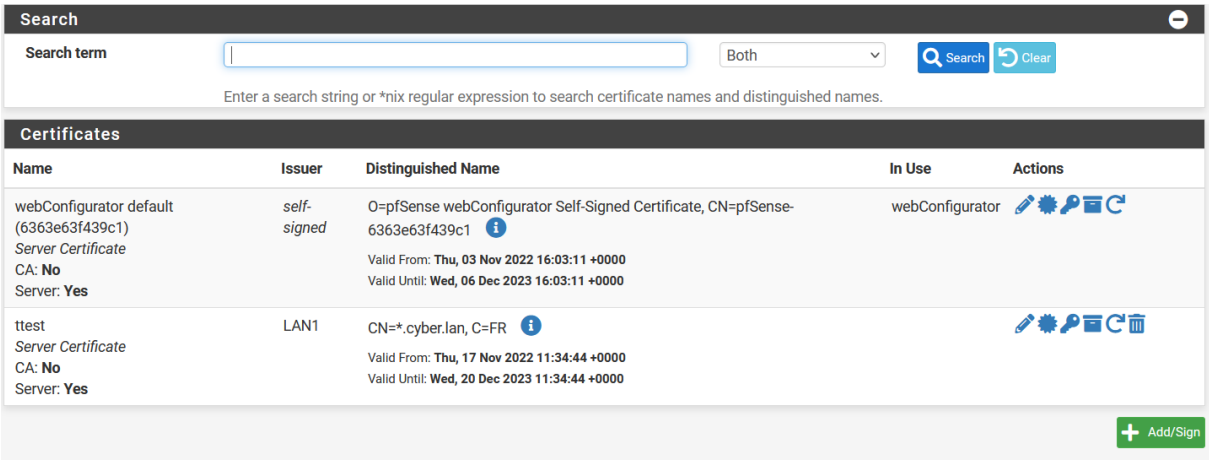
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0 /1.84 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
✓	0 /44 KiB	IPv4 TCP/UDP	*	*	This Firewall	443 (HTTPS)	*	none		HA proxy HTTPS	
✓	0 /24 KiB	IPv4 TCP/UDP	*	*	This Firewall	80 (HTTP)	*	none			
✓	2 /16.97 MiB	IPv4 TCP	*	*	*	12345	*	none			
✓	0 /520 B	IPv4 TCP/UDP	*	*	This Firewall	8080	*	none			

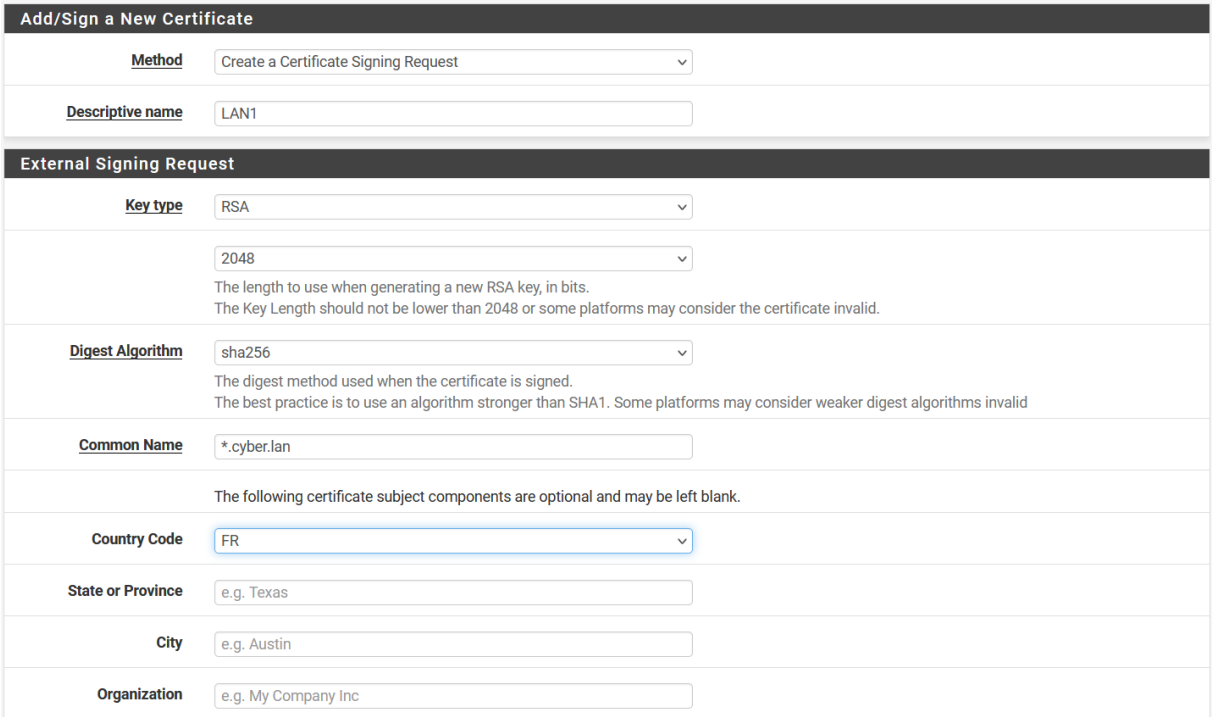
Add | Add | Delete | Save | Separator

ETAPE 3 – CREATION D'UN CERTIFICAT AUTO-SIGNE

On crée ensuite un certificat d'autorité. On va dans System, Certificate Manager, Certicate. Cliquer sur « add/sign ».



On crée un certificat CSR (Certificate Signing Request). Dans Common name il faut entrer *. suivi du nom de domaine. Plus bas sélectionnez Server Certificate. Remplissez Alternative name avec un nom de serveur et son adresse IP. Puis faites save. Attention, comme il ne s'agit pas d'un certificat d'autorité racine, par définition le navigateur vous dira à chaque fois qu'il ne provient pas d'une source sûre.

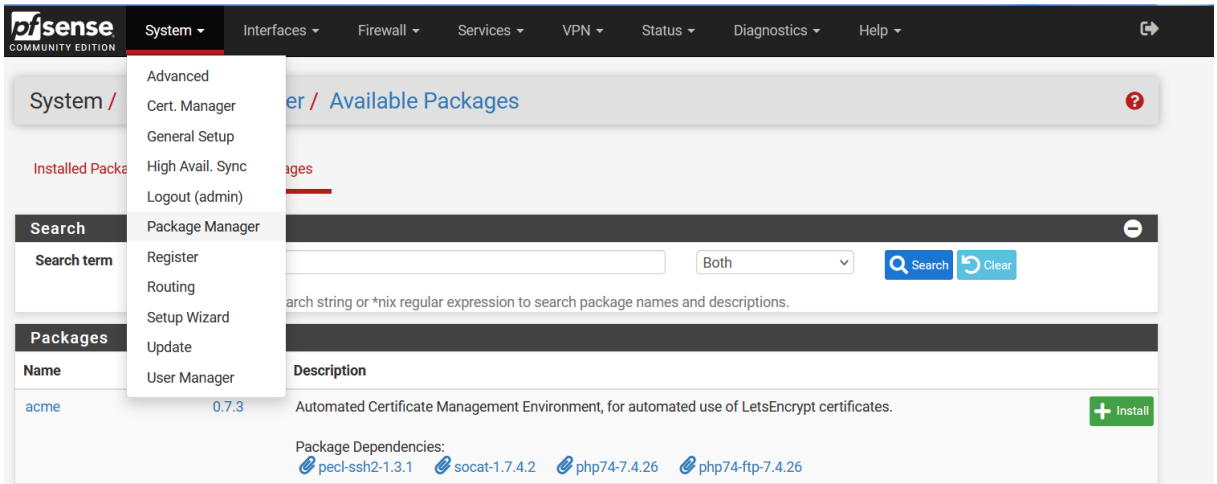


Certificate Attributes

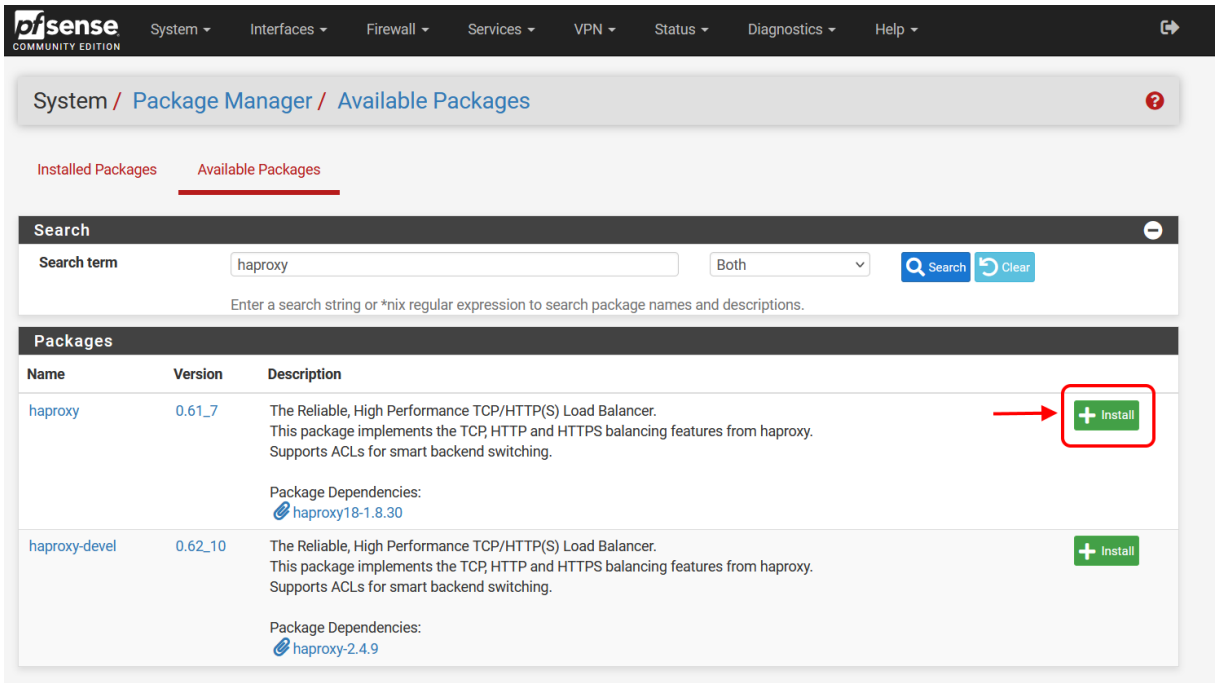
Attribute Notes	The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode. For Certificate Signing Requests, These attributes are added to the request but they may be ignored or changed by the CA that signs the request. If this CSR will be signed using the Certificate Manager on this firewall, set the attributes when signing instead as they cannot be carried over.
Certificate Type	Server Certificate Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.
Alternative Names	FQDN or Hostname — WEBS1 — Delete IP address — 10.0.0.91 — Delete Type — Value Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.
Add	Add

ETAPE 4 – INSTALLATION DE HAPROXY

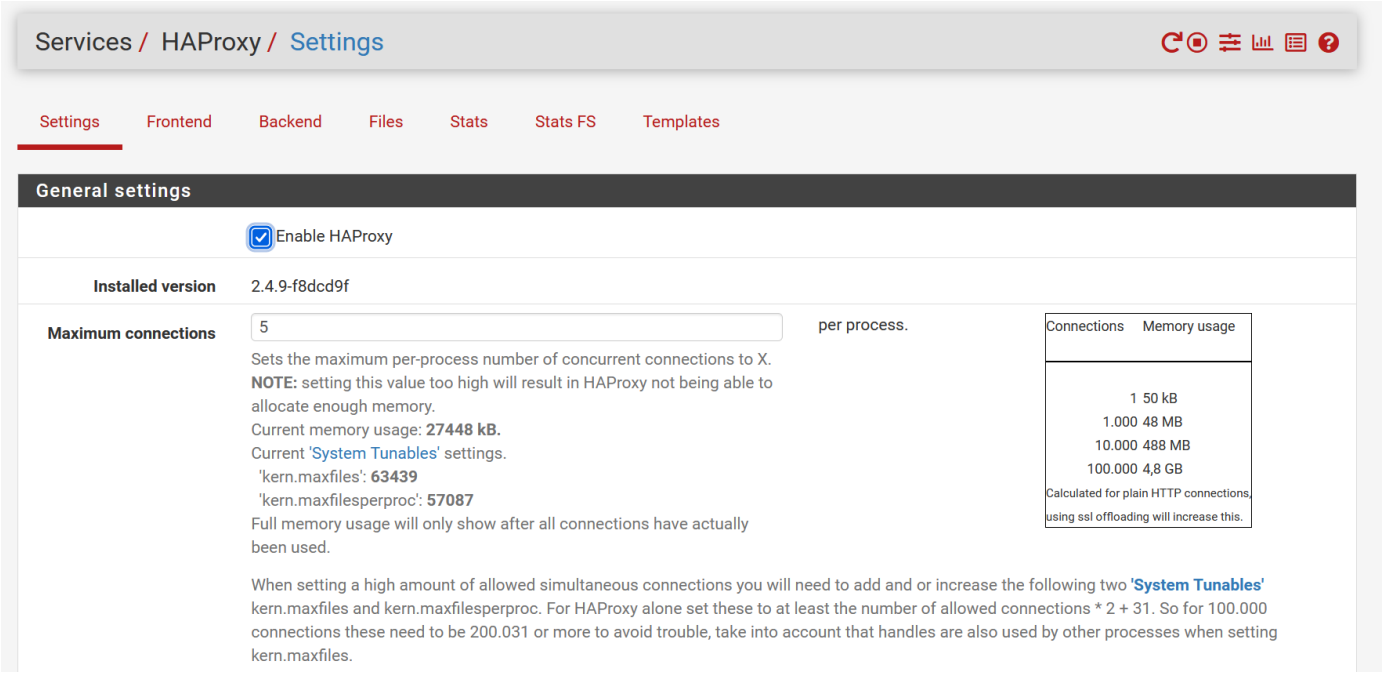
Afin d'accéder à l'installation de HAproxy, allez dans l'onglet System, Packet manager.



Dans la barre de recherche tapez haproxy et installez le premier.

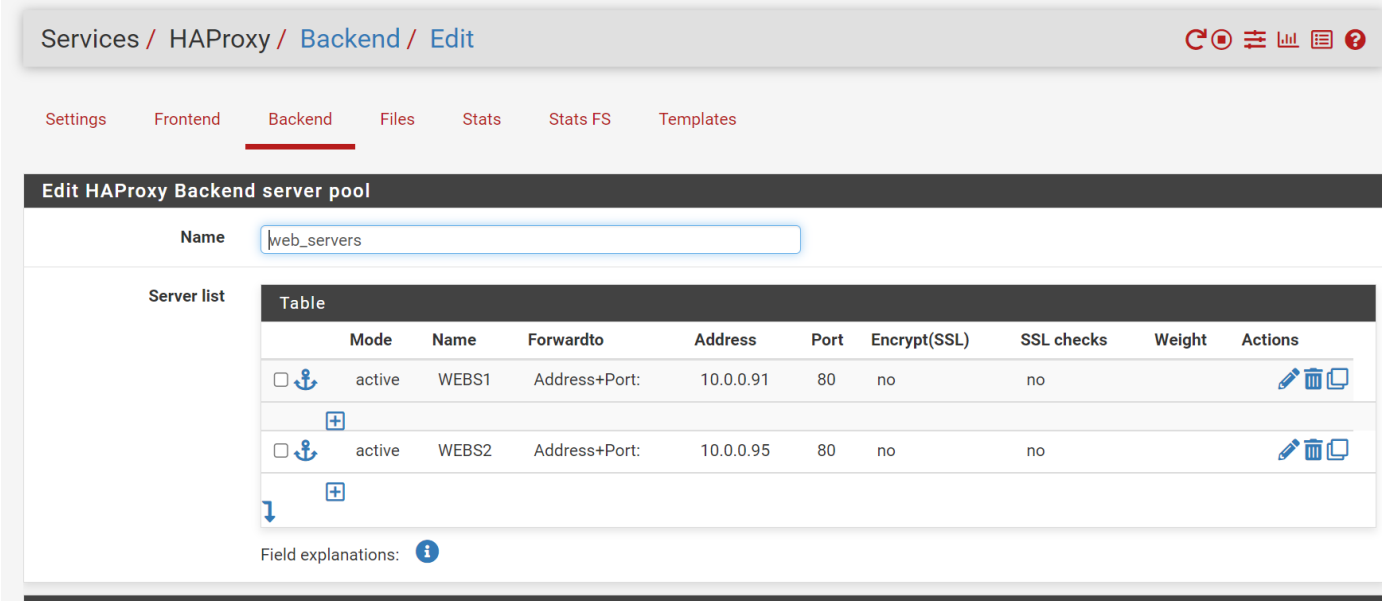


ATTENTION ! Une fois installé, n'oubliez pas d'aller dans Services, HAproxy, Settings et de cocher Enable HAproxy ! Puis faites save.

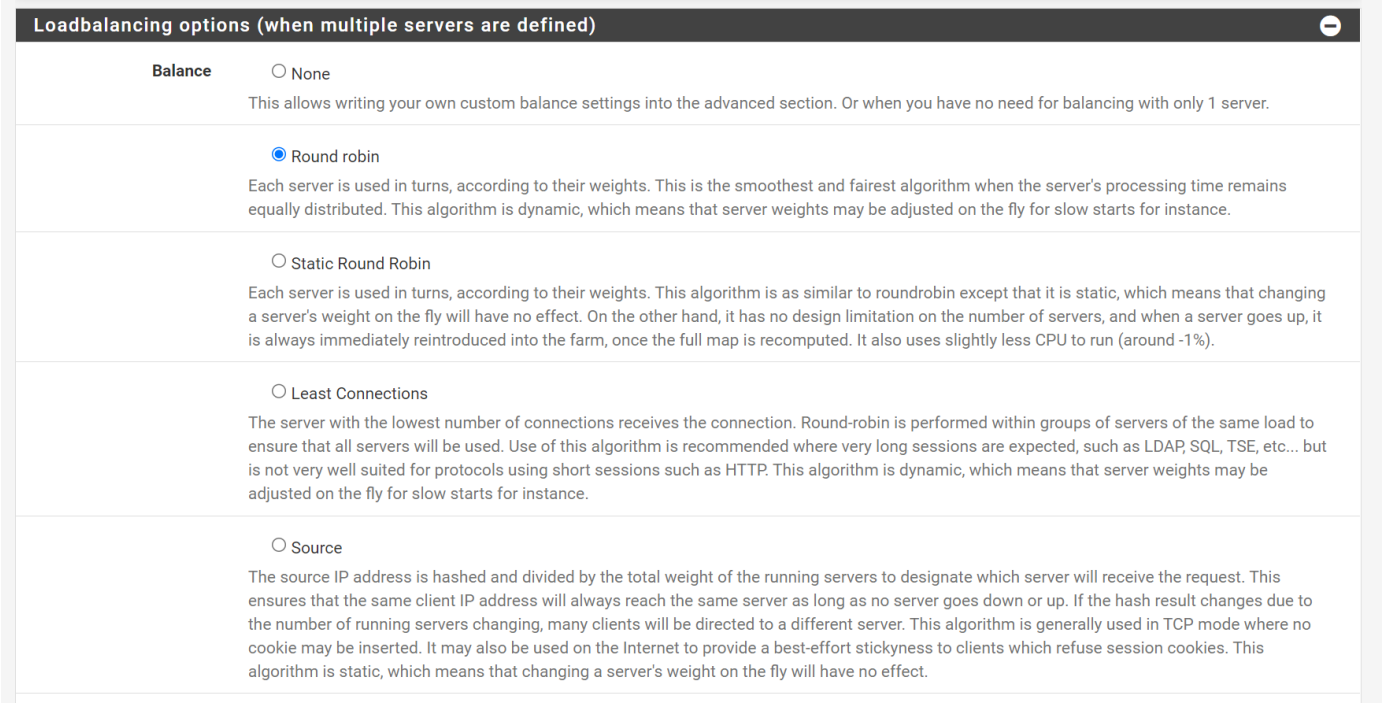


ETAPE 5 – MISE EN PLACE DU BACKEND

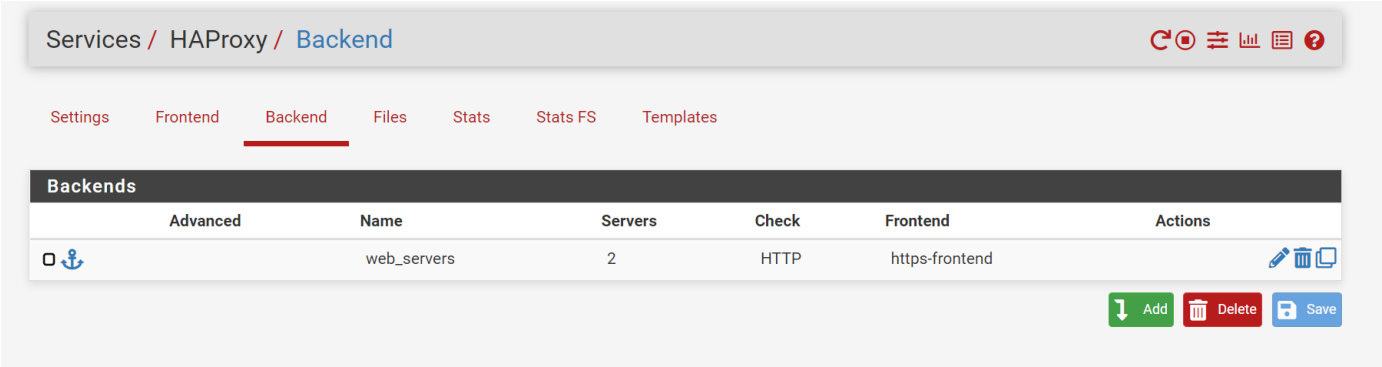
Nous allons maintenant configurer le Backend. C'est-à-dire le pool de serveurs sur lesquels on veut agir et activer du loadbalancing. Pour cela il faut aller dans Services, HAproxy, Backend et en ajouter un nouveau avec « Add ». Dans name on met le nom souhaité. Puis dans la serveur list on ajoute les serveur avec leur nom, leur adresse ip, leur port. Ici on se met en http donc 80.



On fait de même dérouler l'option Loadbalancing pour afficher la liste des options et on coche Round Robin.

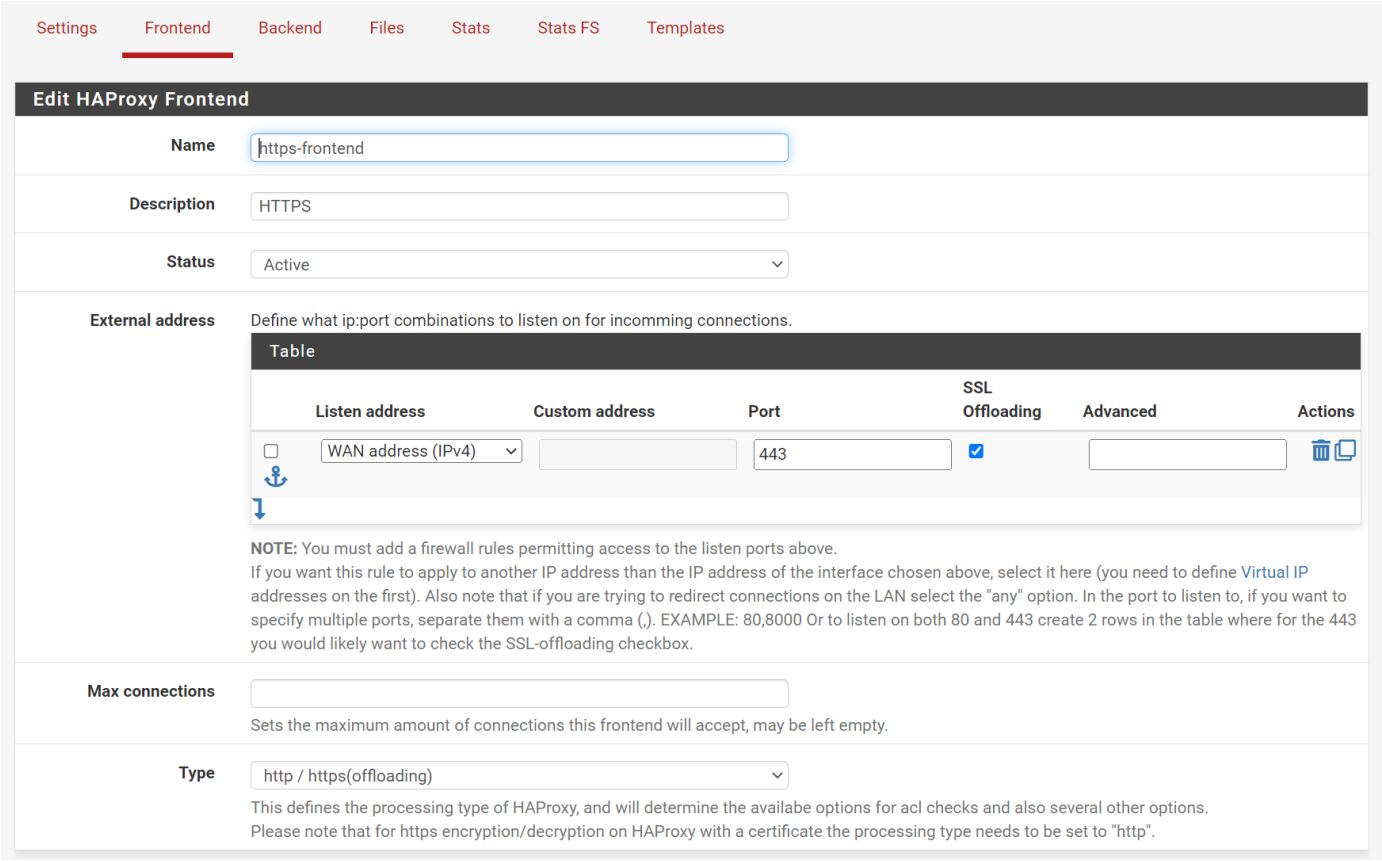


Voici à quoi devrait ressembler la liste des Backend après un save.

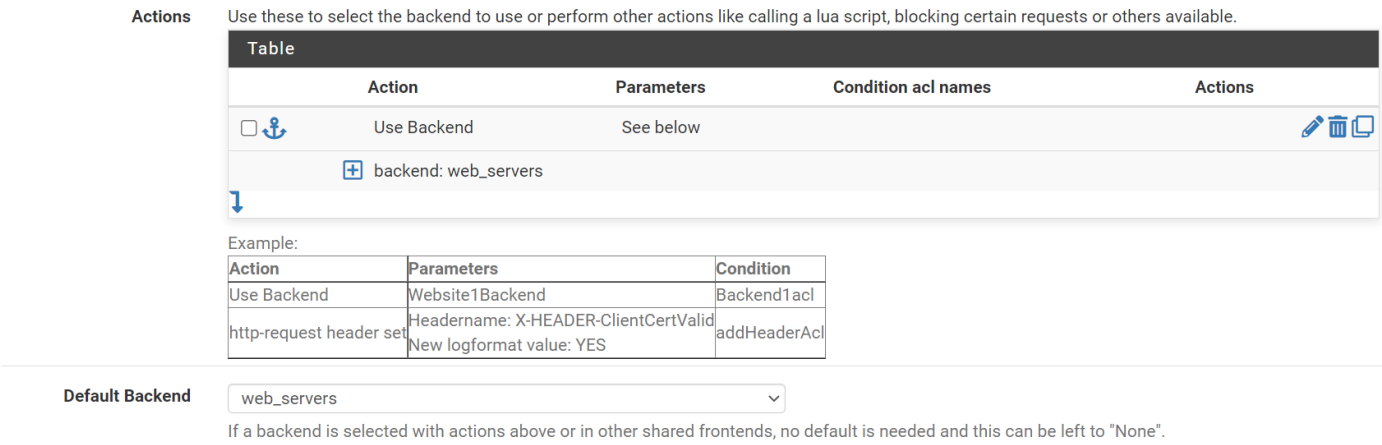


ETAPE 6 – MISE EN PLACE DU FRONTEND

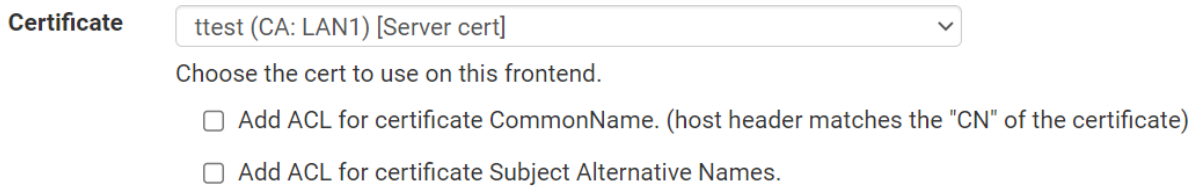
Nous allons maintenant configurer le Frontend. C'est-à-dire la redirection des requêtes issues de ports écoutés, vers les serveurs web souhaités. Pour cela il faut aller dans Services, HAproxy, Frontend et en ajouter un nouveau avec « Add ». Dans name et Description on met le contenu souhaité. Puis dans Status on sélectionne Active. Dans la table de External address on précise WAN address sur le port 443 (hhtps) et on coche SSL Offloading.



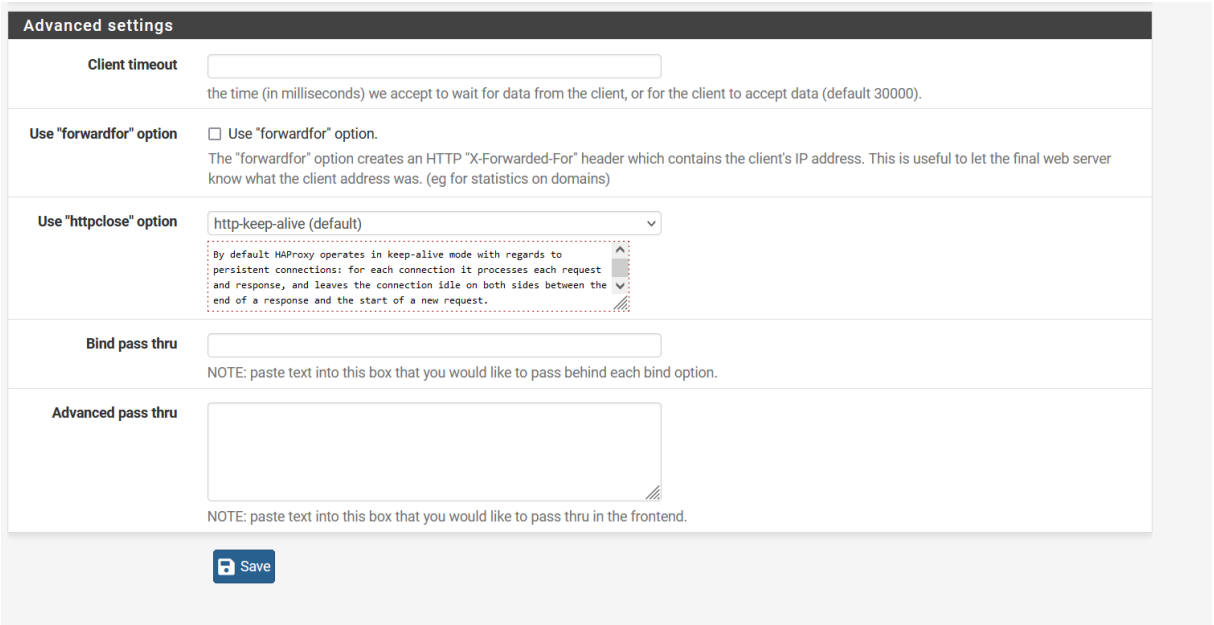
Plus bas dans la table des Actions, on précise Use Backend et on ajoute la règle du Backend créée précédemment.



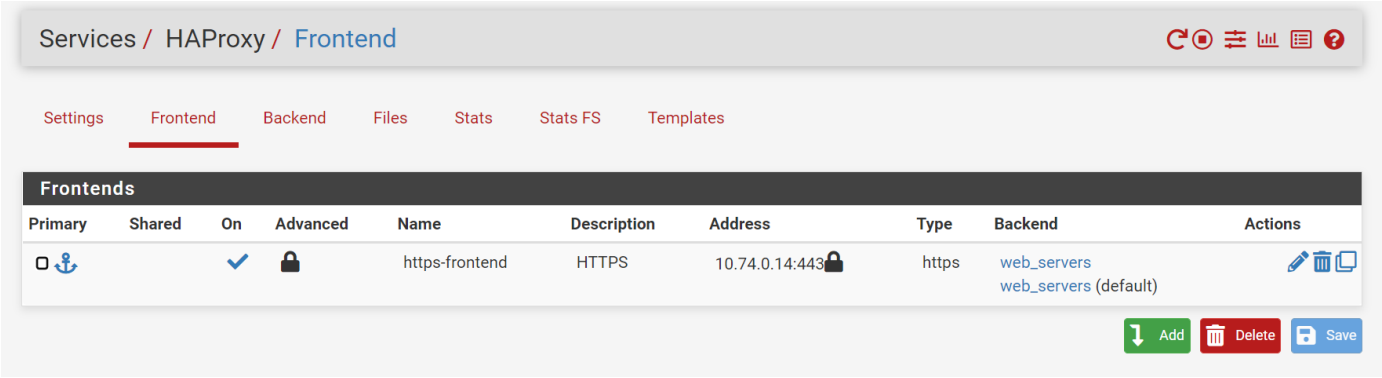
Si vous avez coché SSL Offloading plus haut, vous aurez l'occasion d'avoir accès aux options de certificats. Dans Certificate, sélectionnez le CRS créé précédemment.



Une fois tout fait, faites save.



Votre règle devrait ressembler à ceci.



ETAPE 7 – VERIFICATION DE L'ACCES SITE

Pour vérifier si votre configuration fonctionne, ouvrez une page internet et tapez dans la barre https://ip-address. Vous devriez obtenir un avertissement qui spécifie que ce lien n'est pas sûr, c'est à cause du certificat non officiel. Par définition, le navigateur considère donc que l'https qui en découle n'est pas sûr . Néanmoins il suffit simplement de faire « avancé » et de continuer il n'y a aucun risque. Le résultat devrait ressembler à la page ci-dessous. Vous pouvez modifier l'affichage de l'un de vos serveurs web afin de confirmer si en rafraîchissant le site le Round robin fonctionne bien et que vous alternez sur la redirection entre les 2 serveurs web.