

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

Table des matières :

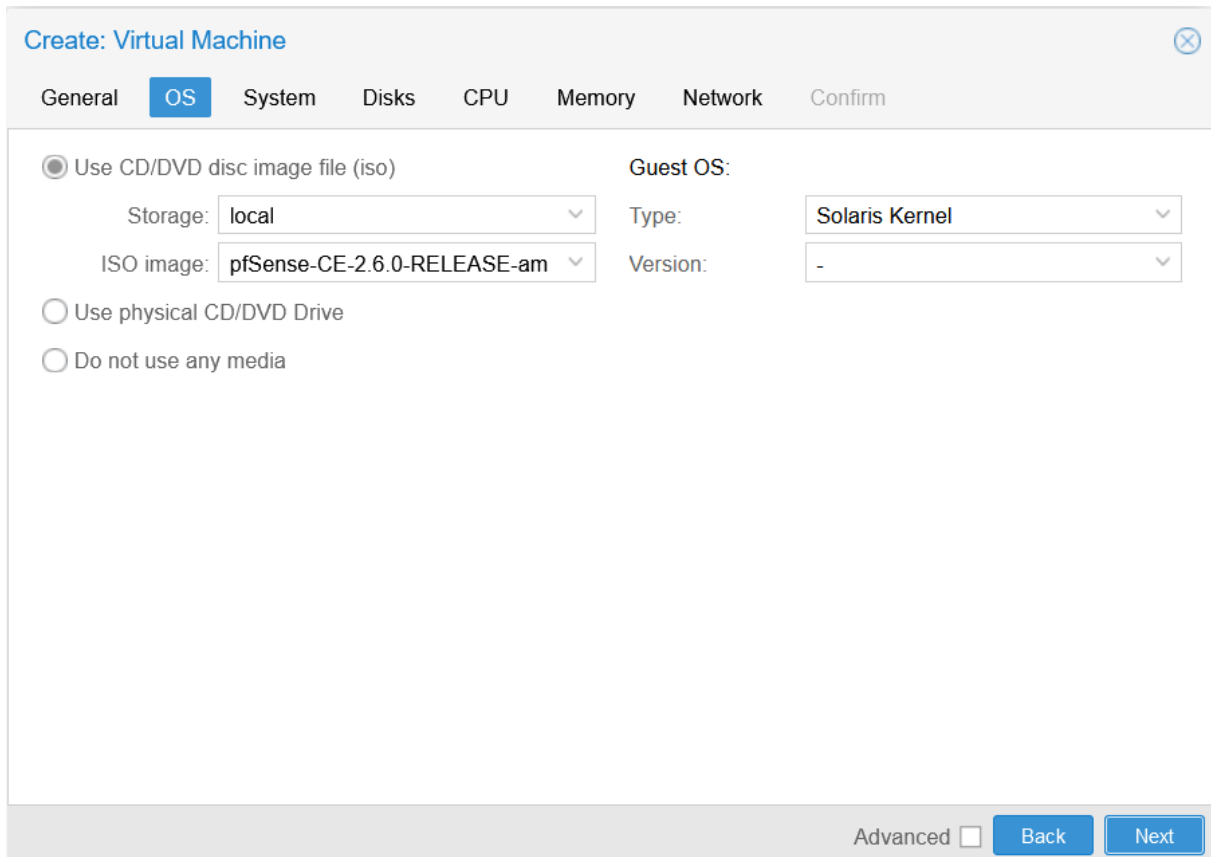
- **Etape 1 : Installation de Pfsense**
- **Etape 2 : Configuration du Pfsense par l'interface**
- **Etape 3 : Création d'un certificat auto-signé**
- **Etape 4 : Installation de Haproxy**
- **Etape 5 : Mise en place du Backend**
- **Etape 6 : Mise en place du Frontend**
- **Etape 7 : Vérification de l'accès site**

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".



The screenshot shows the 'Create: Virtual Machine' dialog box in Proxmox, with the 'OS' tab selected. The dialog has a title bar with a close button and a tabbed interface with 'General', 'OS', 'System', 'Disks', 'CPU', 'Memory', 'Network', and 'Confirm' tabs. The 'OS' tab is active, showing three radio button options: 'Use CD/DVD disc image file (iso)' (selected), 'Use physical CD/DVD Drive', and 'Do not use any media'. Under the selected option, there are two columns of settings. The left column has 'Storage:' set to 'local' and 'ISO image:' set to 'pfSense-CE-2.6.0-RELEASE-am'. The right column has 'Guest OS:' set to 'Solaris Kernel' and 'Version:' set to '-'. At the bottom right, there is an 'Advanced' checkbox (unchecked) and two buttons: 'Back' and 'Next'.

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

The screenshot shows the 'Create: Virtual Machine' wizard with the 'Disks' tab selected. The interface includes a list of disks on the left with 'ide0' selected. The 'Disk' sub-tab is active, showing configuration options: Bus/Device (IDE), Storage (local-lvm), Disk size (GiB) (32), and Format (Raw disk image (raw)). Other options include Cache (Default (No cache)) and Discard (unchecked). Navigation buttons 'Back' and 'Next' are visible at the bottom right.

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

The screenshot shows the 'Create: Virtual Machine' wizard with the 'CPU' tab selected. The configuration shows 1 socket and 1 core, resulting in 1 total core. The Type is set to 'Default (kvm64)'. A 'Help' button is located at the bottom left, and 'Back' and 'Next' buttons are at the bottom right.

Dans “Memory”, mettez environ 2048 MiB.

The screenshot shows the 'Create: Virtual Machine' dialog box with the 'Memory' tab selected. The 'Memory (MiB)' field is set to 2048. The dialog has tabs for General, OS, System, Disks, CPU, Memory, Network, and Confirm. At the bottom, there is a Help button, an 'Advanced' checkbox, and Back/Next buttons.

Tab	Value
General	
OS	
System	
Disks	
CPU	
Memory	2048
Network	
Confirm	

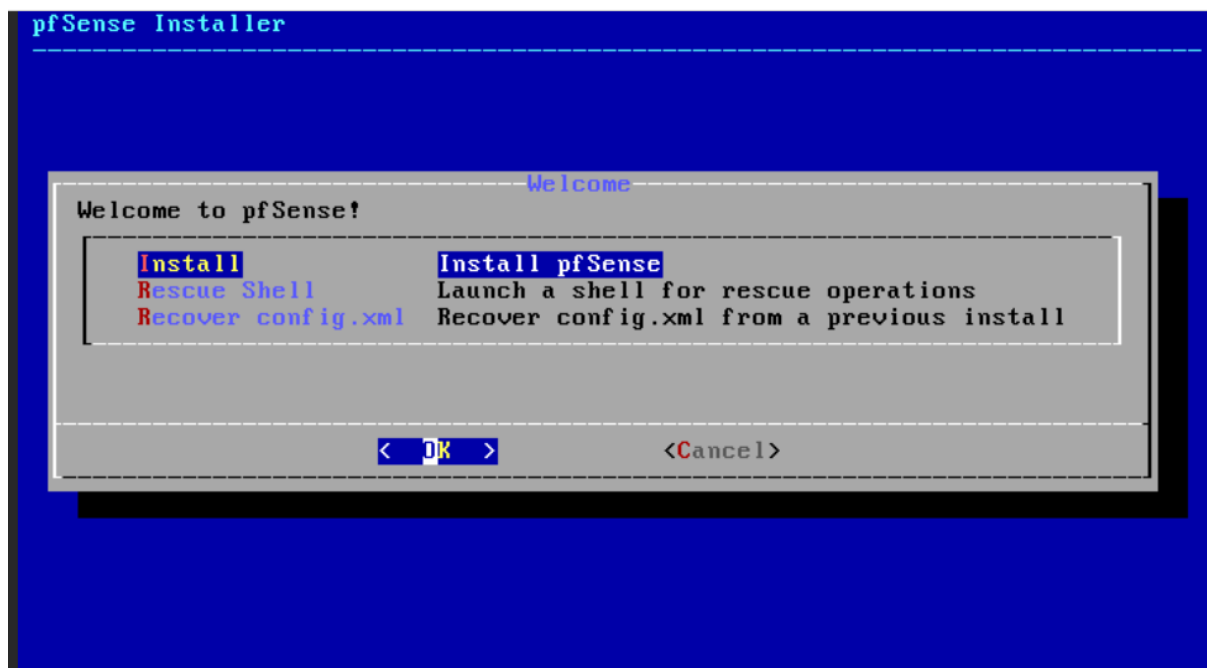
Dans “Network”, sélectionner le bridge existant. Le paramétrage de la VM est alors terminé. Les paramètres vus dans cette partie peuvent évidemment varier selon les besoins.

The screenshot shows the 'Create: Virtual Machine' dialog box with the 'Network' tab selected. The 'No network device' checkbox is unchecked. The 'Bridge' is set to vubr0, 'Model' to Intel E1000, 'VLAN Tag' to no VLAN, and 'MAC address' to auto. The 'Firewall' checkbox is checked. The dialog has tabs for General, OS, System, Disks, CPU, Memory, Network, and Confirm. At the bottom, there is a Help button, an 'Advanced' checkbox, and Back/Next buttons.

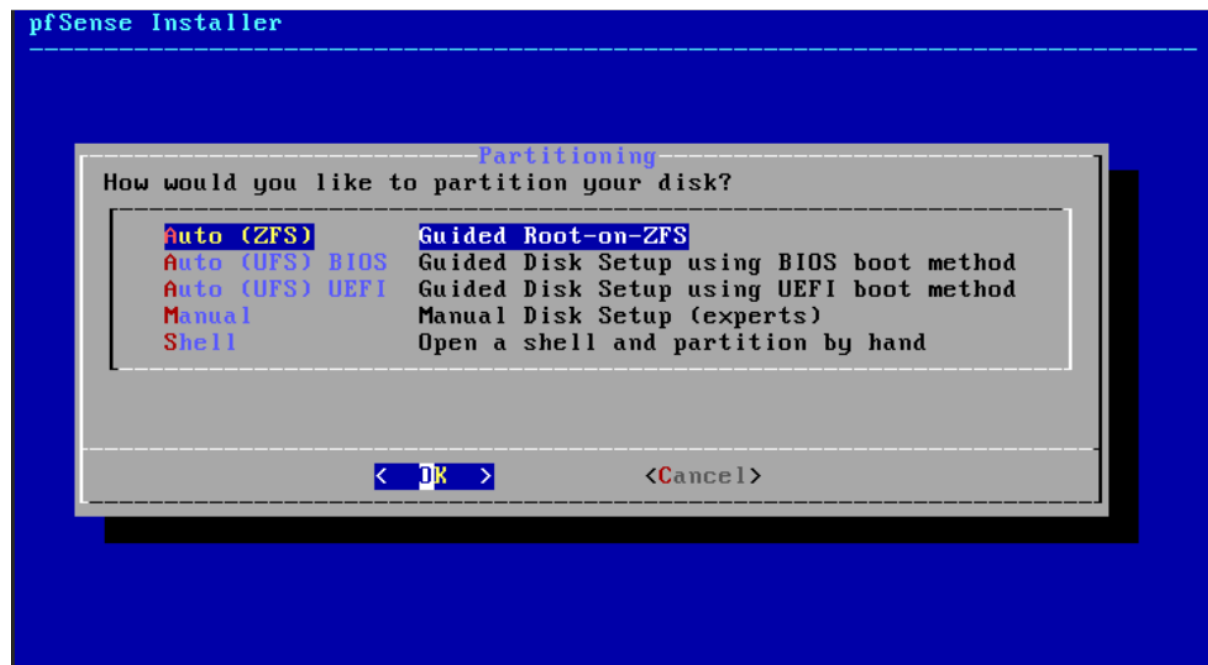
Tab	Value
General	
OS	
System	
Disks	
CPU	
Memory	
Network	<input type="checkbox"/> No network device Bridge: vubr0 Model: Intel E1000 VLAN Tag: no VLAN MAC address: auto Firewall: <input checked="" type="checkbox"/>
Confirm	

Partie ligne de commande Pfsense :

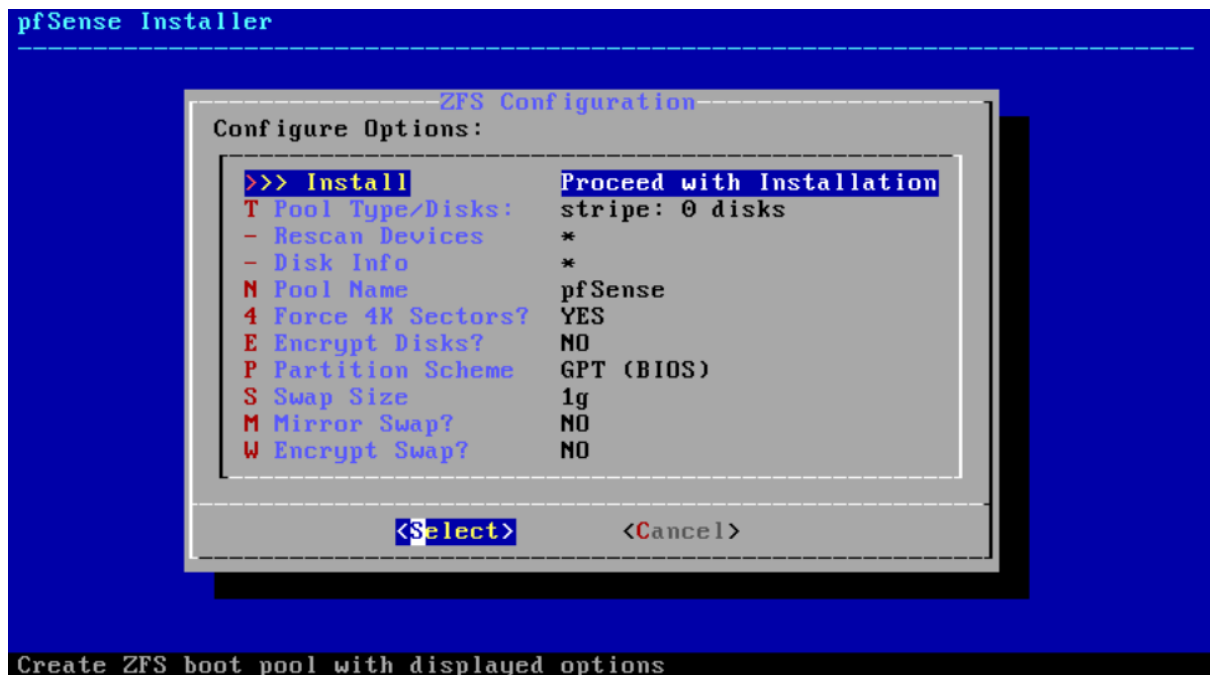
Choisir l'option "Install pfSense".



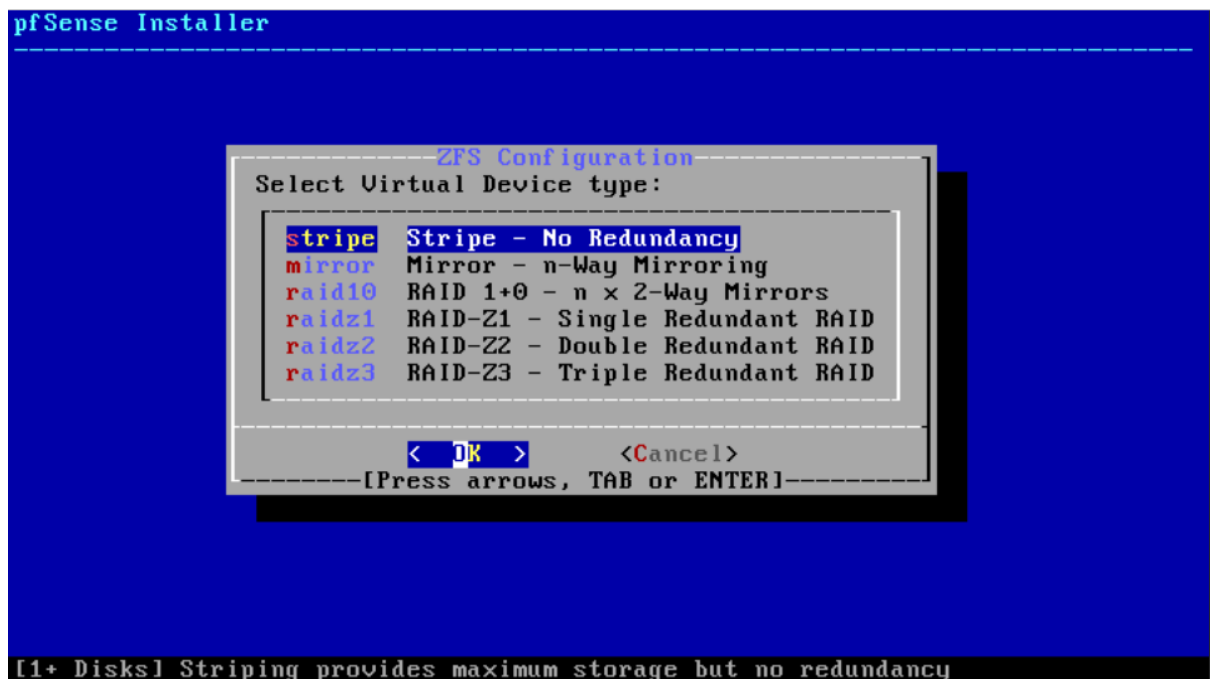
Sélectionner la langue puis appuyer 2 fois sur entrer.



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



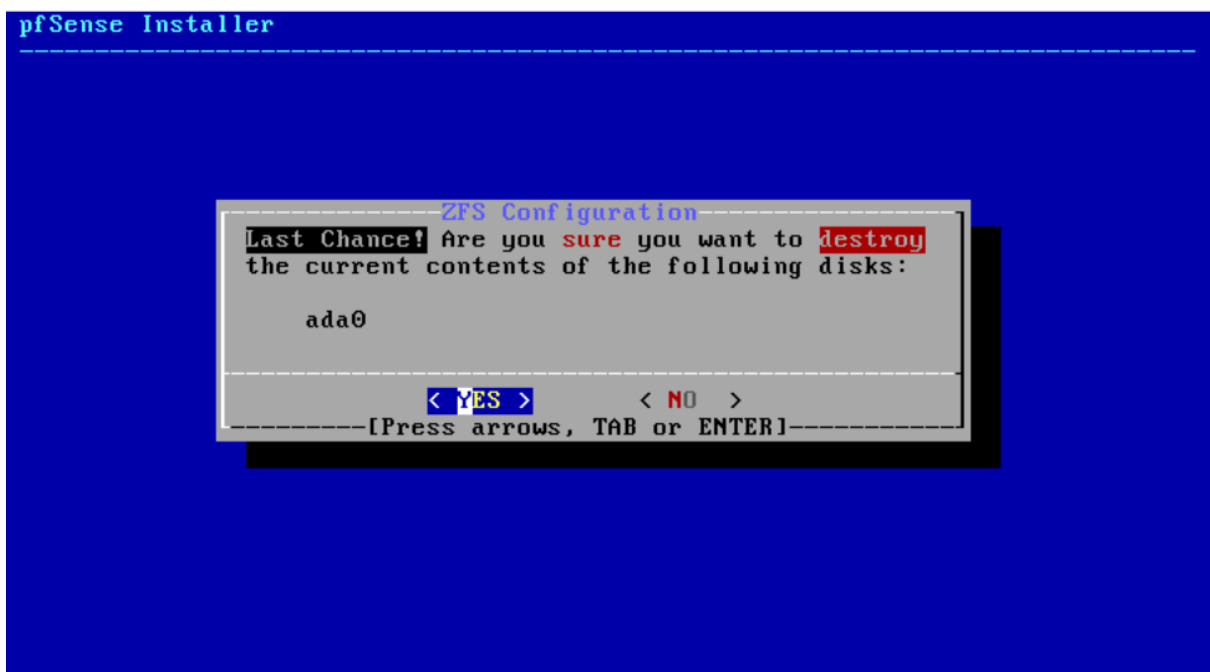
Sélectionner “stripe - No Redundancy” (On ne créer pas de raid lors de cette étape).



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".

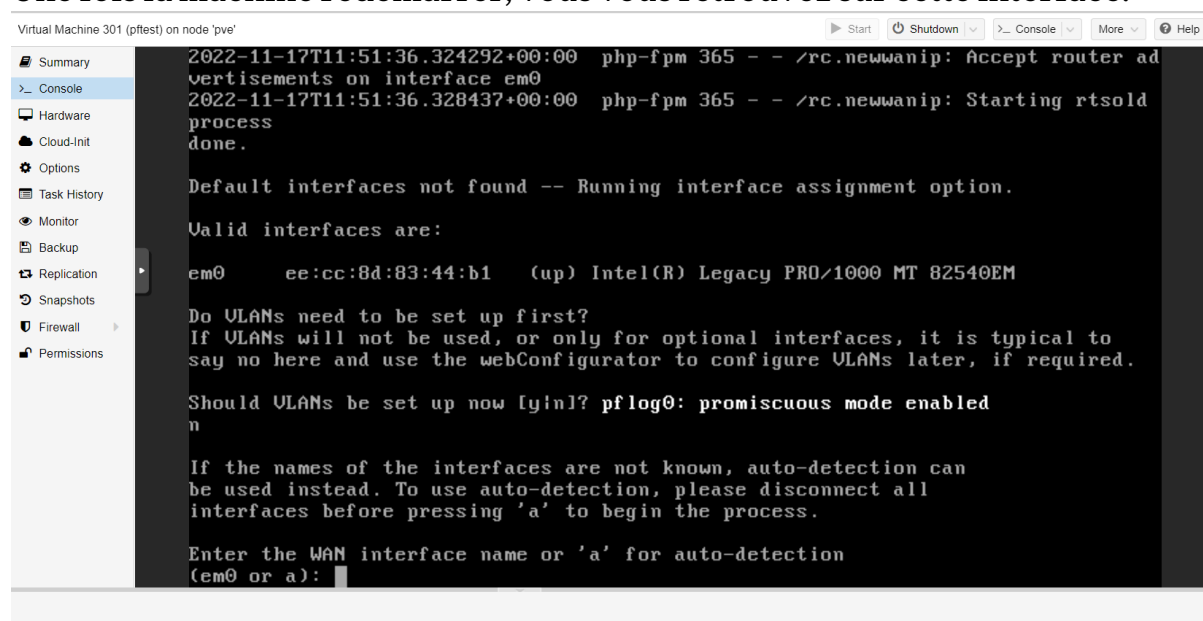


Après ouverture de Shell tapez la commande “exit” afin de sorte de Shell, la machine redémarrera automatiquement.

When finished, type 'exit' to reboot.

```
# █
```

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



Virtual Machine 301 (pfest) on node 'pve'

```
Start | Shutdown | Console | More | Help
```

```
2022-11-17T11:51:36.324292+00:00 php-fpm 365 - - /rc.newwanip: Accept router ad
vertisements on interface em0
2022-11-17T11:51:36.328437+00:00 php-fpm 365 - - /rc.newwanip: Starting rtsold
process
done.

Default interfaces not found -- Running interface assignment option.

Valid interfaces are:

em0      ee:cc:8d:83:44:b1  (up) Intel(R) Legacy PRO/1000 MT 82540EM

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.

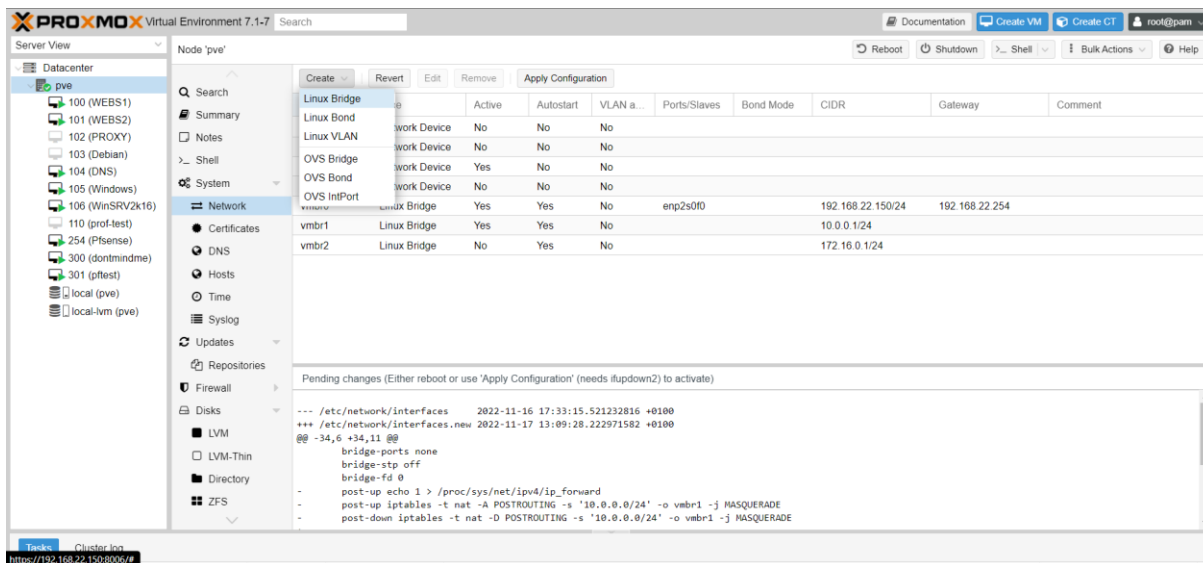
Should VLANs be set up now [y/n]? pflog0: promiscuous mode enabled
n

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.

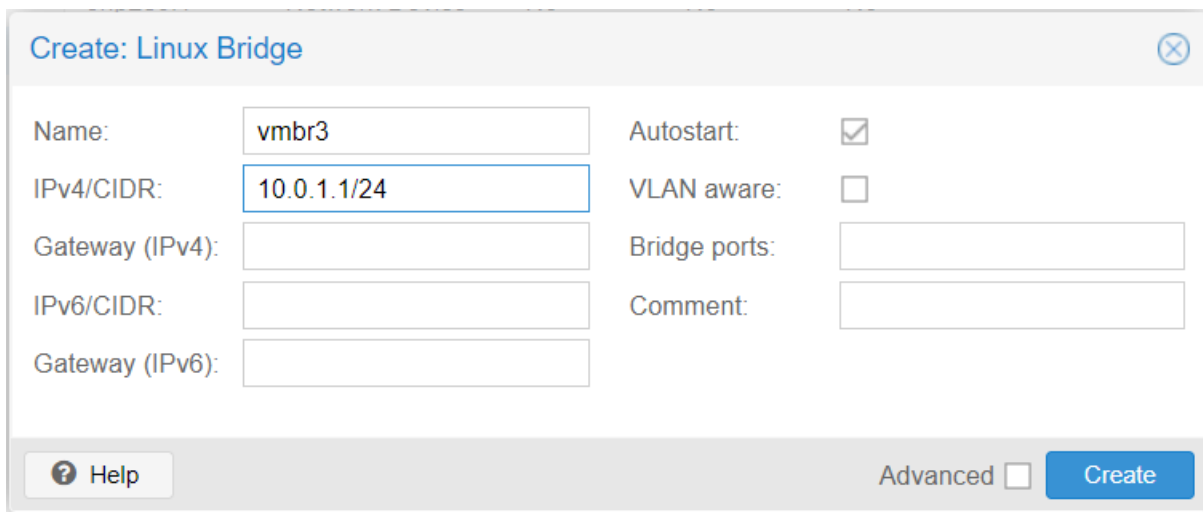
Enter the WAN interface name or 'a' for auto-detection
(em0 or a): █
```

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 sélectionner « Linux Bridge » .

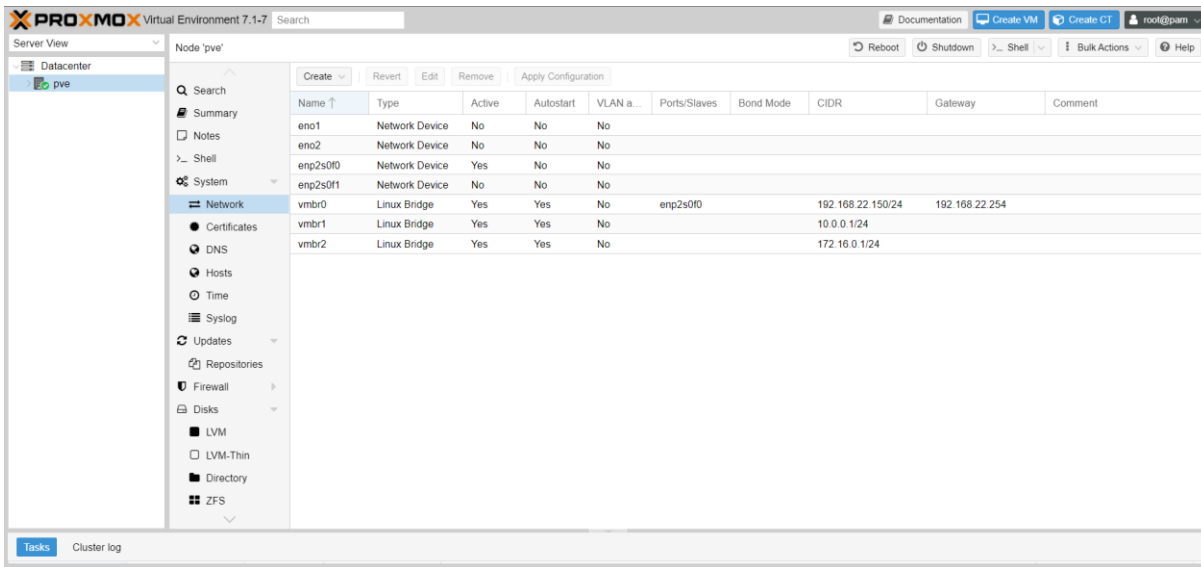


Entrer l'adresse IP et le masque de sous réseau de votre LAN. Vous pouvez également renommer votre LAN mais cela est optionnel.

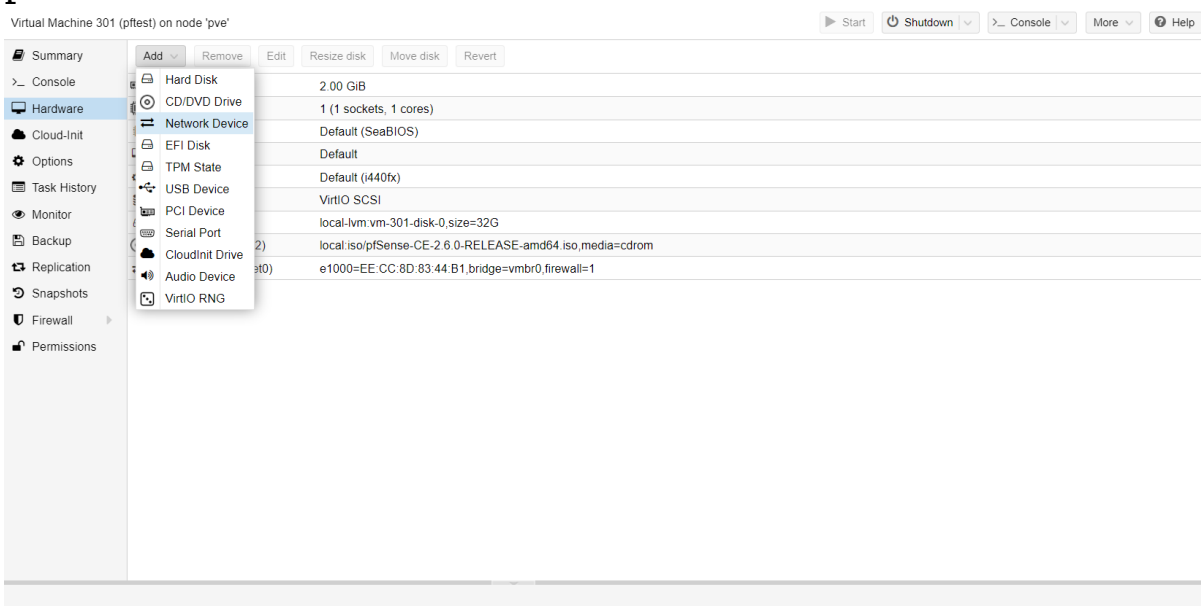


Après la

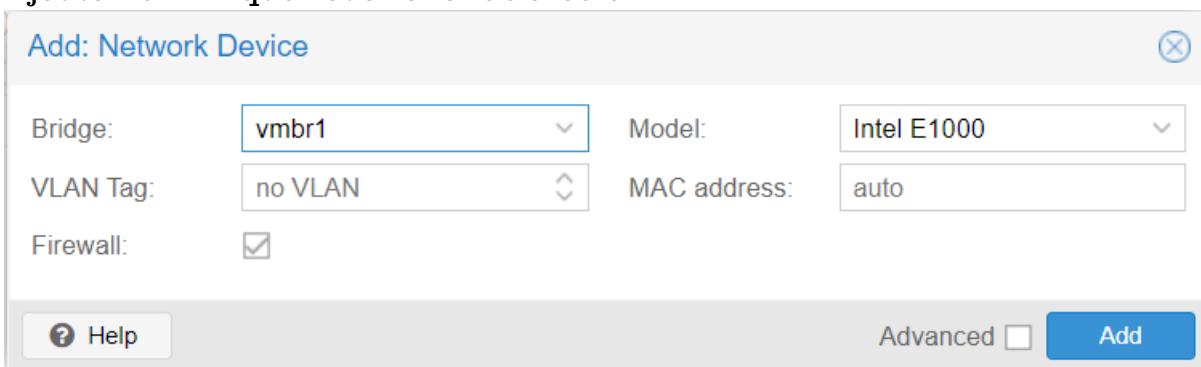
Création de la LAN, cliquer sur « Apply Configuration » pour confirmer la création de votre LAN et l'activer.



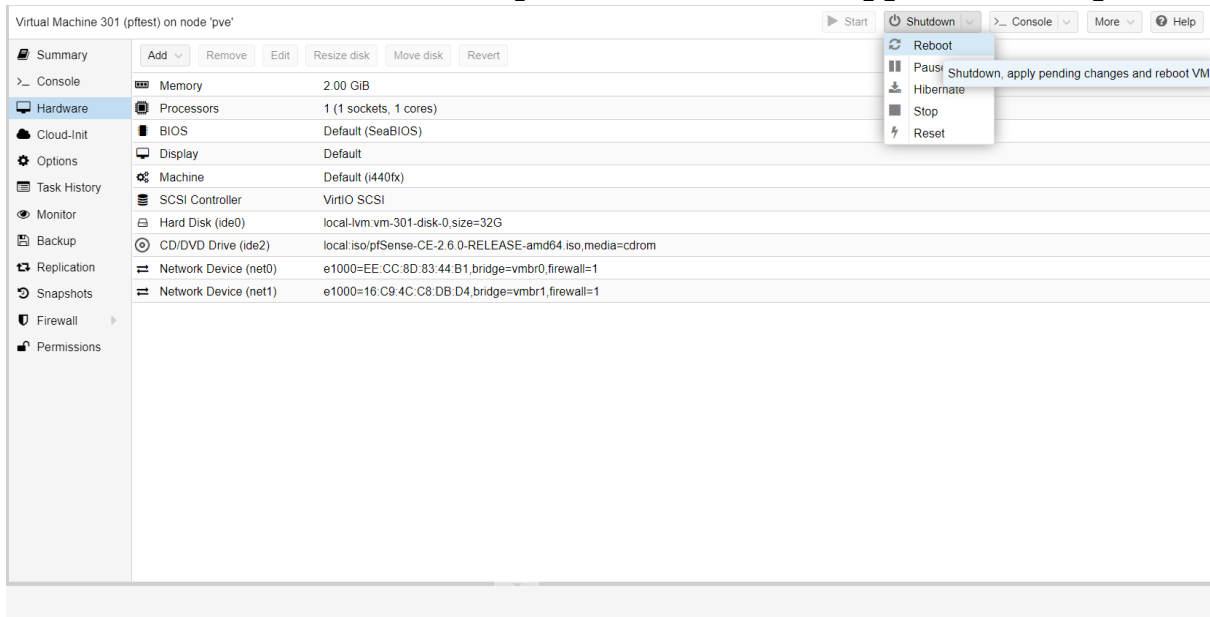
Dirigez-vous ensuite sur votre machine dans l'onglet « Hardware ». Cliquez sur « Add » puis « Network ».



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.

```
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
KUM Guest - Netgate Device ID: c9561649ee91876e34b9

*** 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
```

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 passerelle.

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.
KUM 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.
KUM Guest - Netgate Device ID: e002dee83994e92c1ab8

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

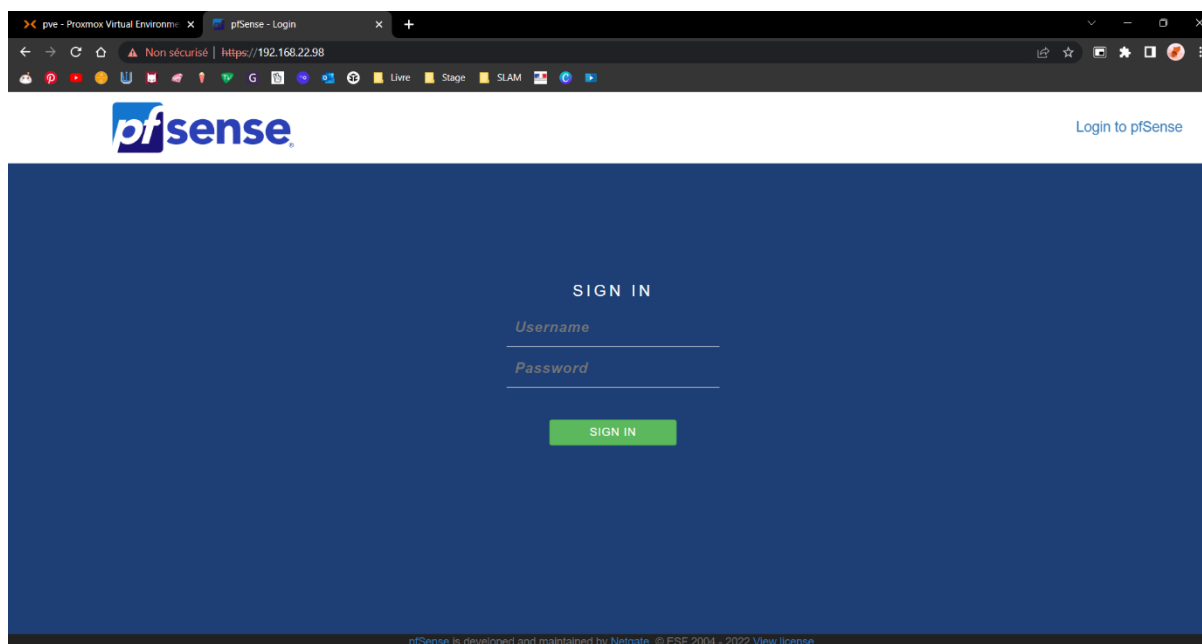
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.22.98/24
                v6/DHCP6: 2a05:6e02:104a:e510:eccc:8dff:fe83:4
4b1/64
LAN (lan)      -> em1      -> v4: 172.16.0.1/24

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

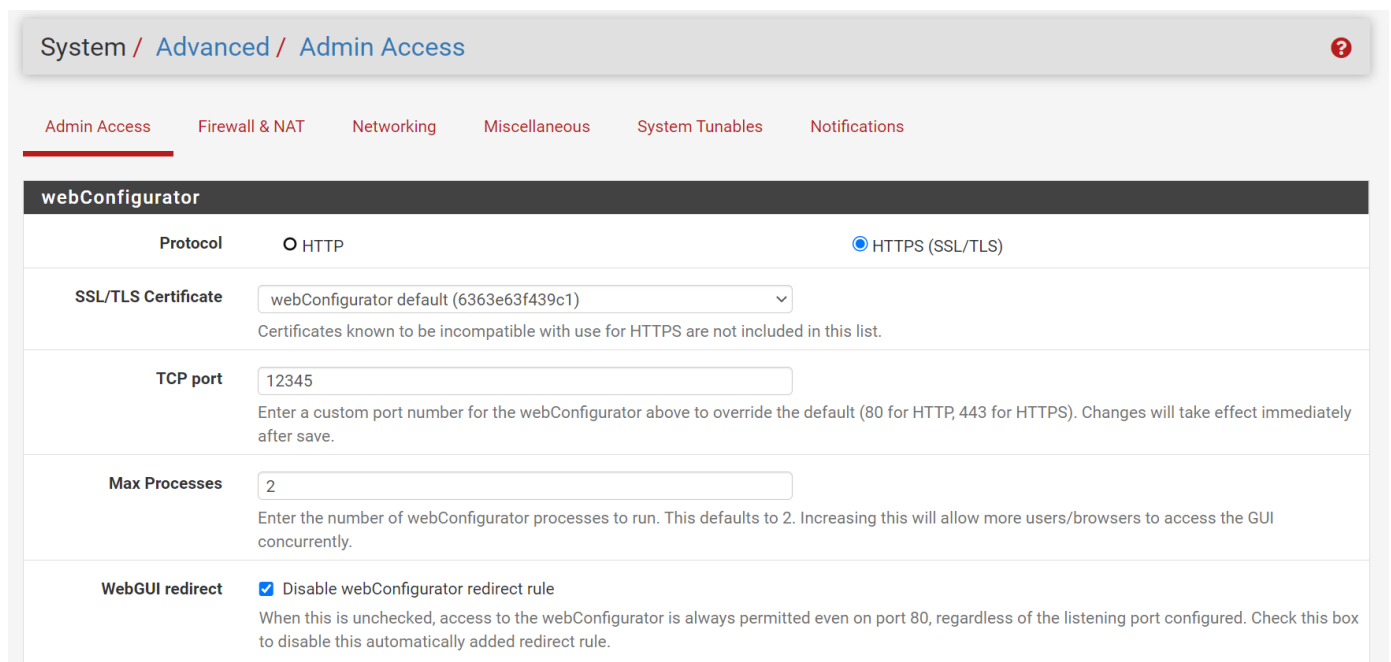
[2.6.0-RELEASE][root@pfSense.home.arpal/root: pfctl -d
pf disabled
[2.6.0-RELEASE][root@pfSense.home.arpal/root: |
```

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.



The screenshot shows the PfSense configuration interface for the webConfigurator. The breadcrumb trail is System / Advanced / Admin Access. The 'Admin Access' tab is selected. The 'webConfigurator' section is expanded, showing the following settings:

- Protocol:** HTTP, HTTPS (SSL/TLS)
- SSL/TLS Certificate:** webConfigurator default (6363e63f439c1) [dropdown]
Certificates known to be incompatible with use for HTTPS are not included in this list.
- TCP port:** 12345
Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.
- Max Processes:** 2
Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.
- WebGUI redirect:** Disable webConfigurator redirect rule
When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.

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.

Edit Gateway

Disabled Disable this gateway
Set this option to disable this gateway without removing it from the list.

Interface
Choose which interface this gateway applies to.

Address Family
Choose the Internet Protocol this gateway uses.

Name
Gateway name

Gateway
Gateway IP address

Gateway Monitoring Disable Gateway Monitoring
This will consider this gateway as always being up.

Gateway Action Disable Gateway Monitoring Action
No action will be taken on gateway events. The gateway is always considered up.

Monitor IP
Enter an alternative address here to be used to monitor the link. This is used for the quality RRD graphs as well as the load balancer entries. Use this if the gateway does not respond to ICMP echo requests (pings).

Force state Mark Gateway as Down
This will force this gateway to be considered down.

Description
A description may be entered here for reference (not parsed).

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

System / Routing / Gateways 🔄 📄 📊 📑 ?

Gateways **Static Routes** **Gateway Groups**

Gateways

	Name	Default	Interface	Gateway	Monitor IP	Description	Actions
<input checked="" type="checkbox"/>	WAN_DHCP6		WAN			Interface WAN_DHCP6 Gateway	
<input checked="" type="checkbox"/>	WAN_DHCP		WAN	10.74.0.1	10.74.0.1	Interface WAN_DHCP Gateway	
<input checked="" type="checkbox"/>	Gateway_LAN	Default (IPv4)	LAN	10.0.0.254	10.0.0.254		

Save
+ Add

Default gateway

Default gateway IPv4
Select a gateway or failover gateway group to use as the default gateway.

Default gateway IPv6
Select a gateway or failover gateway group to use as the default gateway.

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.

Interfaces / LAN (em1) ☰ 📊 ?

General Configuration

Enable Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway + Add a new gateway

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

Services / DNS Resolver / General Settings

General Settings Advanced Settings Access Lists

General DNS Resolver Options

Enable Enable DNS resolver

Listen Port
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.

Enable SSL/TLS Service Respond to incoming SSL/TLS queries from local clients
Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.

SSL/TLS Certificate
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.

SSL/TLS Listen Port
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.

Network Interfaces
WAN
LAN
VLAN99
VLAN100
Interface IPs used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 IPs, both are used. Queries to other interface IPs not selected below are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

Outgoing Network Interfaces
WAN
LAN
VLAN99
VLAN100
Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all

DNS Query Forwarding Enable Forwarding Mode
If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under [System > General Setup](#) or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).

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

The screenshot shows the 'System / General Setup' page in pfSense. The 'System' section includes fields for 'Hostname' (set to 'pfSense') and 'Domain' (set to 'home.arpa'). Below this is the 'DNS Server Settings' section, which contains several configuration options:

- DNS Servers:** A table with three columns: 'DNS Servers' (Address: 10.0.0.2), 'DNS Hostname' (Hostname: none), and 'Gateway' (Gateway: none). Descriptions are provided for each column.
- Add DNS Server:** A green button with a plus sign and the text '+ Add DNS Server'.
- DNS Server Override:** A checkbox labeled 'Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server'. Below it is a descriptive paragraph.
- DNS Resolution Behavior:** A dropdown menu currently set to 'Use remote DNS Servers, ignore local DNS'. Below it is a descriptive paragraph.

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 ».

The screenshot shows the 'Diagnostics / Ping' page in pfSense. It features a form with the following fields:

- Hostname:** A text input field containing 'Hostname to ping'.
- IP Protocol:** A dropdown menu set to 'IPv4'.
- Source address:** A dropdown menu set to 'Automatically selected (default)'. Below it is the text 'Select source address for the ping.'
- Maximum number of pings:** A dropdown menu set to '3'. Below it is the text 'Select the maximum number of pings.'
- Seconds between pings:** A dropdown menu set to '1'. Below it is the text 'Select the number of seconds to wait between pings.'

At the bottom of the form is a blue button with a ping icon and the text 'Ping'.

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.

Protocol TCP/UDP
Choose which IP protocol this rule should match.

Source

Source Invert match any Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination Invert match This firewall (self) Destination Address /

Destination Port Range HTTP (80) From Custom To HTTP (80) Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Protocol TCP/UDP
Choose which IP protocol this rule should match.

Source

Source Invert match any Source Address /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination

Destination Invert match This firewall (self) Destination Address /

Destination Port Range HTTPS (443) From Custom To HTTPS (443) Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Le tableau de règles devrait ressembler à ceci :

Firewall / Rules / WAN ☰ 📊 📄 ?

Floating WAN LAN VLAN99 VLAN10

Rules (Drag to Change Order)

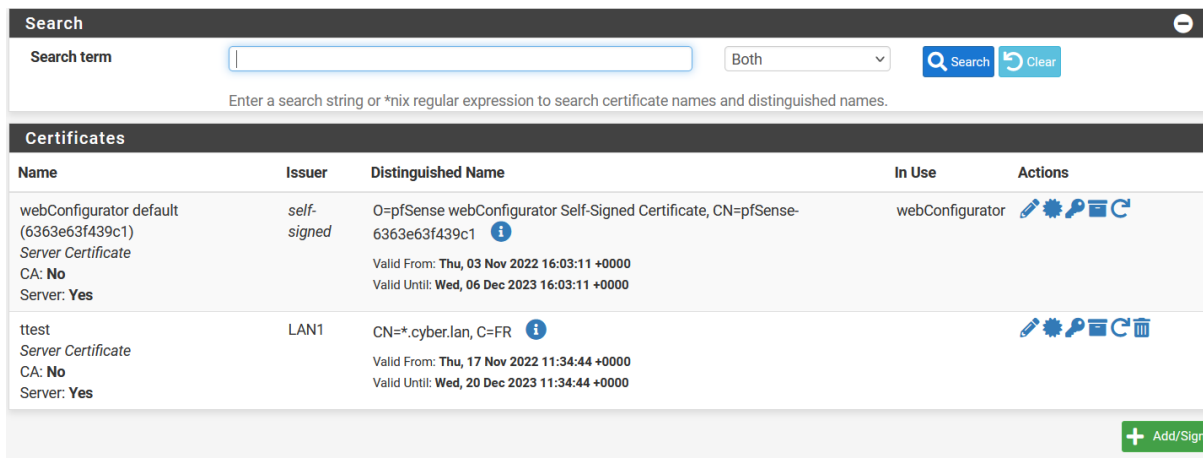
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 1.84 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙️
<input type="checkbox"/>	0 / 44 KiB	IPv4 TCP/UDP	*	*	This Firewall	443 (HTTPS)	*	none		HA proxy HTTPS	📌 ✎ 📄 🚫 🗑️
<input type="checkbox"/>	0 / 24 KiB	IPv4 TCP/UDP	*	*	This Firewall	80 (HTTP)	*	none			📌 ✎ 📄 🚫 🗑️
<input type="checkbox"/>	2 / 16.97 MiB	IPv4 TCP	*	*	*	12345	*	none			📌 ✎ 📄 🚫 🗑️
<input type="checkbox"/>	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, Certificate. Cliquer sur « add/sign ».

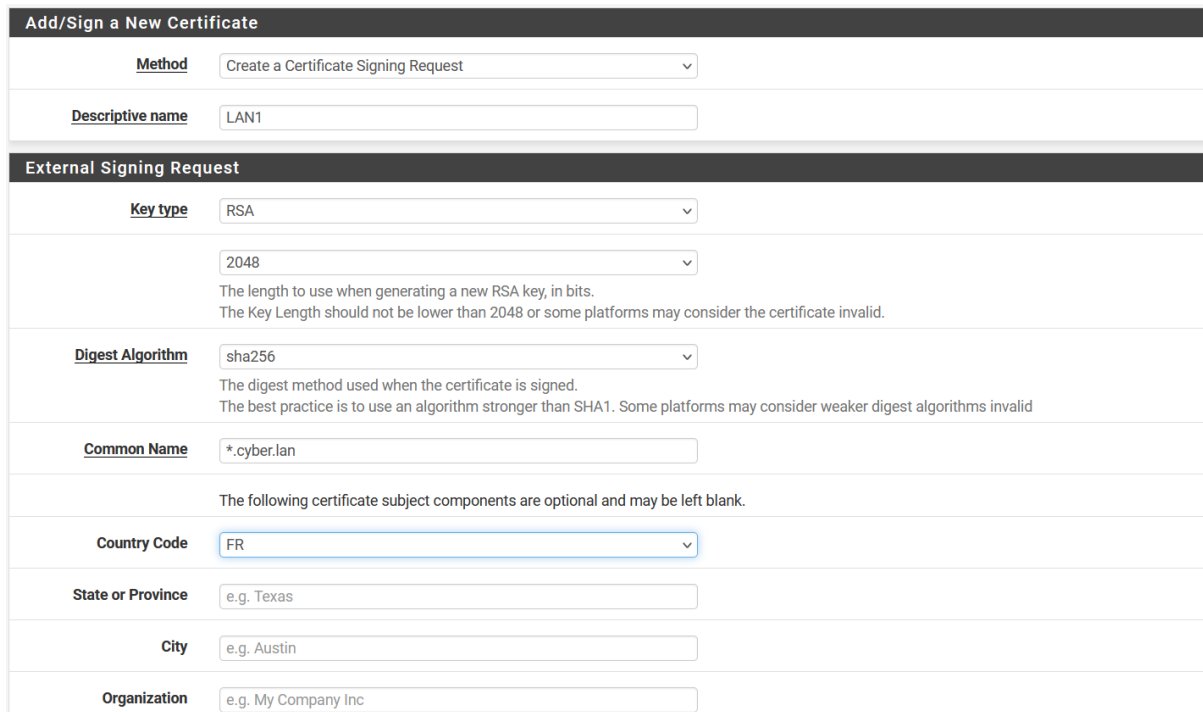


The screenshot shows the Certificate Manager interface. At the top, there is a search bar with a search term input field, a dropdown menu set to 'Both', and 'Search' and 'Clear' buttons. Below the search bar, there is a table of certificates with the following columns: Name, Issuer, Distinguished Name, In Use, and Actions.

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (6363e63f439c1) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-6363e63f439c1 Valid From: Thu, 03 Nov 2022 16:03:11 +0000 Valid Until: Wed, 06 Dec 2023 16:03:11 +0000	webConfigurator	   
ttest Server Certificate CA: No Server: Yes	LAN1	CN=*.cyber.lan, C=FR Valid From: Thu, 17 Nov 2022 11:34:44 +0000 Valid Until: Wed, 20 Dec 2023 11:34:44 +0000		   

At the bottom right of the table, there is a green button labeled '+ 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.



The screenshot shows the 'Add/Sign a New Certificate' form. It has a dark header with the title 'Add/Sign a New Certificate'. Below the header, there are several sections:

- Method:** A dropdown menu with 'Create a Certificate Signing Request' selected.
- Descriptive name:** A text input field containing 'LAN1'.
- External Signing Request:** A section with several fields:
 - Key type:** A dropdown menu with 'RSA' selected.
 - Key length:** A dropdown menu with '2048' selected. Below it, there is a note: 'The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.'
 - Digest Algorithm:** A dropdown menu with 'sha256' selected. Below it, there is a note: 'The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.'
 - Common Name:** A text input field containing '*.cyber.lan'.
 - A note: 'The following certificate subject components are optional and may be left blank.'
 - Country Code:** A dropdown menu with 'FR' selected.
 - State or Province:** A text input field with 'e.g. Texas' as a placeholder.
 - City:** A text input field with 'e.g. Austin' as a placeholder.
 - Organization:** A text input field with 'e.g. My Company Inc' as a placeholder.

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

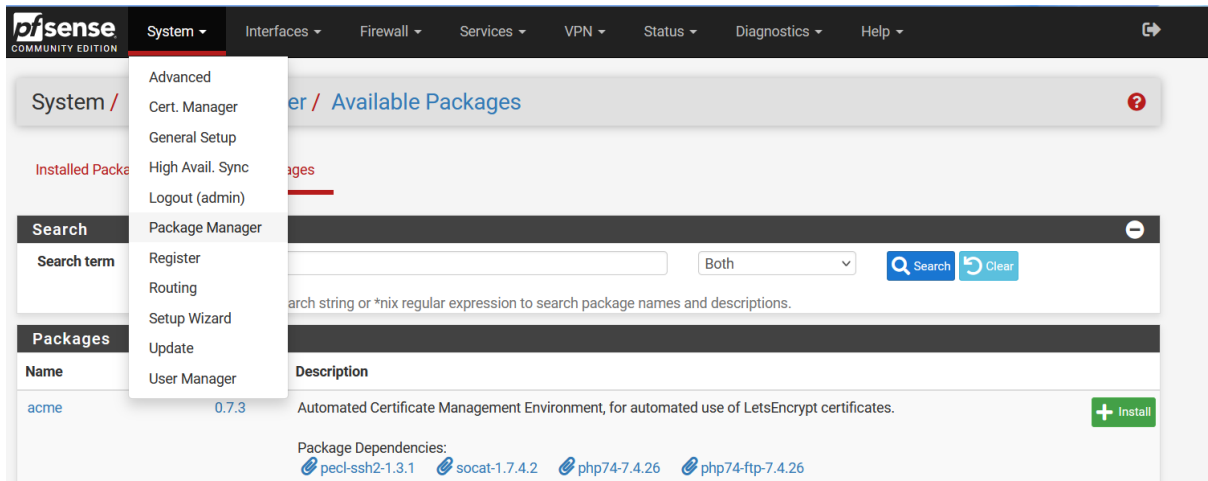
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add

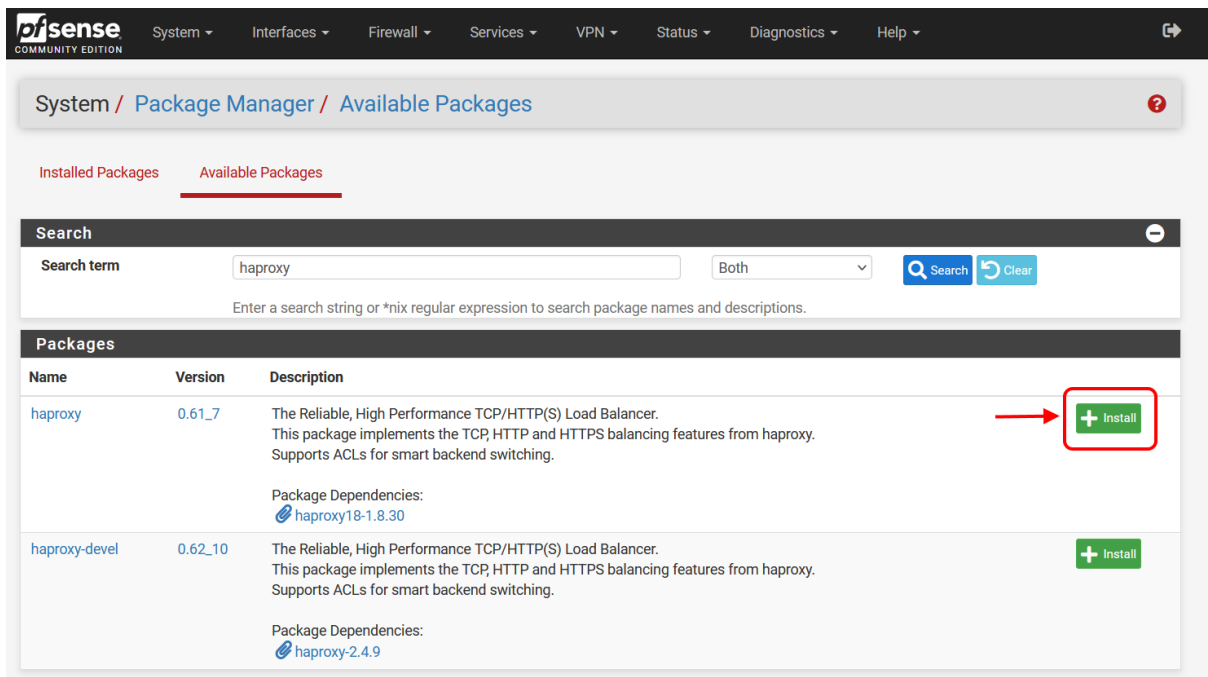
+ Add

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.

Services / HAProxy / Settings 🔄 🏠 📊 📄 ?

Settings Frontend Backend Files Stats Stats FS Templates

General settings

Enable HAProxy

Installed version 2.4.9-f8dcd9f

Maximum connections per process.

Sets the maximum per-process number of concurrent connections to X.
NOTE: setting this value too high will result in HAProxy not being able to allocate enough memory.
 Current memory usage: 27448 kB.
 Current 'System Tunables' settings:
 'kern.maxfiles': 63439
 'kern.maxfilesperproc': 57087
 Full memory usage will only show after all connections have actually been used.

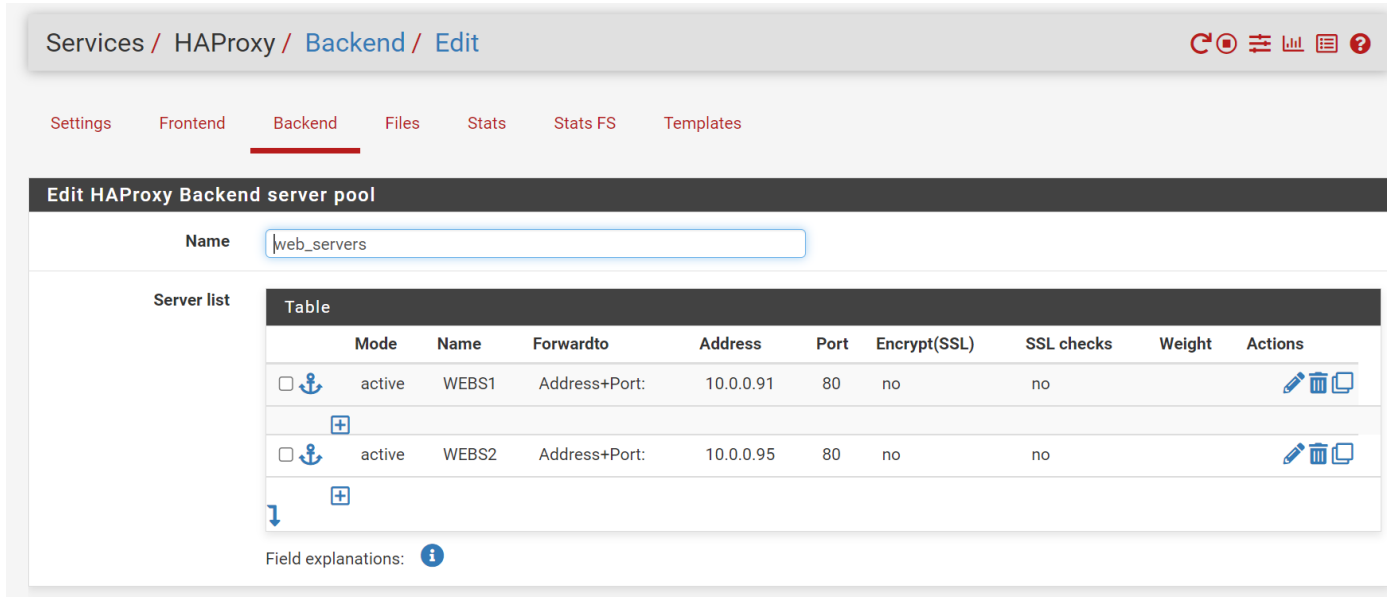
Connections	Memory usage
1	50 kB
1.000	48 MB
10.000	488 MB
100.000	4,8 GB

Calculated for plain HTTP connections, using ssl offloading will increase this.

When setting a high amount of allowed simultaneous connections you will need to add and or increase the following two 'System Tunables' kern.maxfiles and kern.maxfilesperproc. For HAProxy alone set these to at least the number of allowed connections * 2 + 31. So for 100.000 connections these need to be 200.031 or more to avoid trouble, take into account that handles are also used by other processes when setting kern.maxfiles.

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.

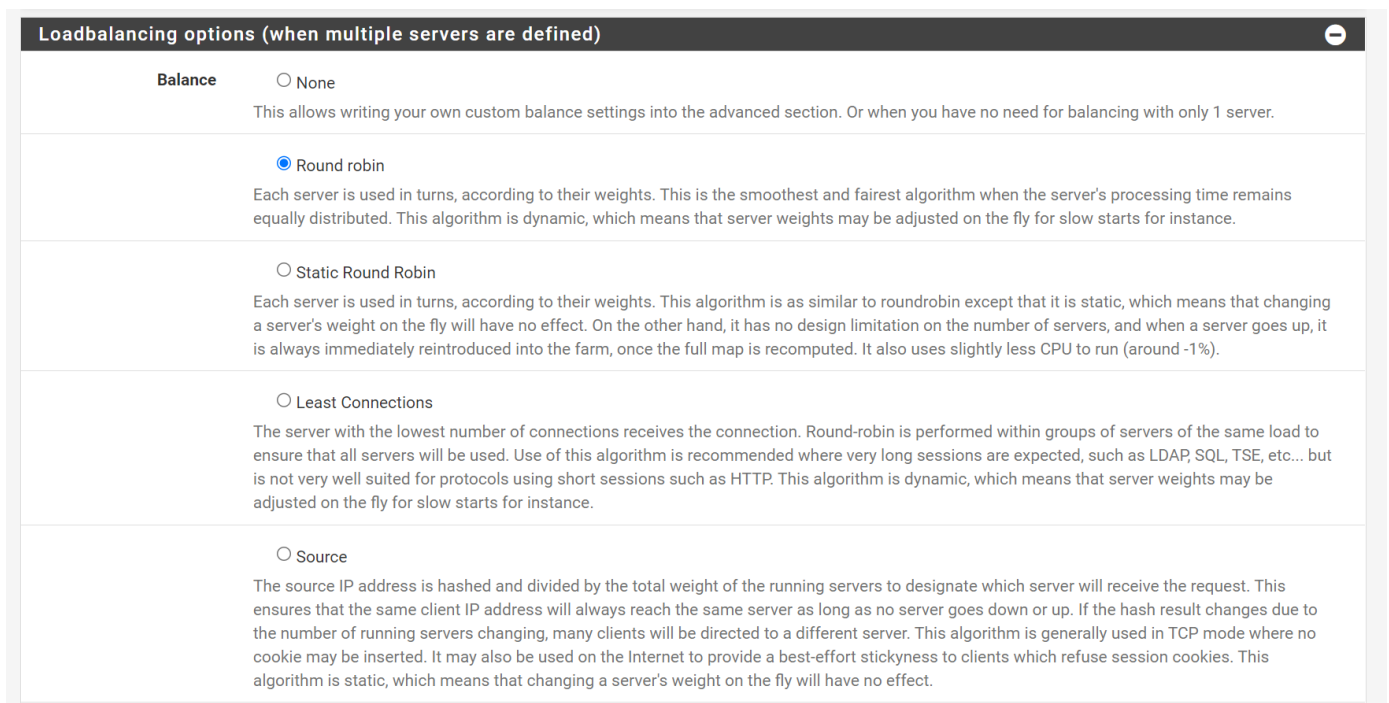


The screenshot shows the HAProxy configuration interface. The breadcrumb navigation is "Services / HAProxy / Backend / Edit". The "Backend" tab is selected. The "Name" field is set to "web_servers". Below it, the "Server list" section contains a table with two servers:

Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Actions
<input type="checkbox"/> active	WEBS1	Address+Port:	10.0.0.91	80	no	no		
<input type="checkbox"/> active	WEBS2	Address+Port:	10.0.0.95	80	no	no		

Field explanations:

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



The screenshot shows the "Loadbalancing options (when multiple servers are defined)" dialog box. The "Balance" section is expanded, showing five options:

- None: This allows writing your own custom balance settings into the advanced section. Or when you have no need for balancing with only 1 server.
- Round robin: Each server is used in turns, according to their weights. This is the smoothest and fairest algorithm when the server's processing time remains equally distributed. This algorithm is dynamic, which means that server weights may be adjusted on the fly for slow starts for instance.
- Static Round Robin: Each server is used in turns, according to their weights. This algorithm is as similar to roundrobin except that it is static, which means that changing a server's weight on the fly will have no effect. On the other hand, it has no design limitation on the number of servers, and when a server goes up, it is always immediately reintroduced into the farm, once the full map is recomputed. It also uses slightly less CPU to run (around -1%).
- Least Connections: The server with the lowest number of connections receives the connection. Round-robin is performed within groups of servers of the same load to ensure that all servers will be used. Use of this algorithm is recommended where very long sessions are expected, such as LDAP, SQL, TSE, etc... but is not very well suited for protocols using short sessions such as HTTP. This algorithm is dynamic, which means that server weights may be adjusted on the fly for slow starts for instance.
- Source: The source IP address is hashed and divided by the total weight of the running servers to designate which server will receive the request. This ensures that the same client IP address will always reach the same server as long as no server goes down or up. If the hash result changes due to the number of running servers changing, many clients will be directed to a different server. This algorithm is generally used in TCP mode where no cookie may be inserted. It may also be used on the Internet to provide a best-effort stickyness to clients which refuse session cookies. This algorithm is static, which means that changing a server's weight on the fly will have no effect.

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

Services / HAProxy / Backend

Settings Frontend **Backend** Files Stats Stats FS Templates

Backends						
	Advanced	Name	Servers	Check	Frontend	Actions
<input type="checkbox"/>		web_servers	2	HTTP	https-frontend	

Add Delete 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 (https) et on coche SSL Offloading.

Settings Frontend Backend Files Stats Stats FS Templates

Edit HAProxy Frontend

Name:

Description:

Status:

External address: Define what ip:port combinations to listen on for incoming connections.

Listen address	Custom address	Port	SSL Offloading	Advanced	Actions
<input type="checkbox"/> WAN address (IPv4)	<input type="text"/>	<input type="text" value="443"/>	<input checked="" type="checkbox"/>	<input type="text"/>	

NOTE: You must add a firewall rules permitting access to the listen ports above.
If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define [Virtual IP](#) addresses on the first). Also note that if you are trying to redirect connections on the LAN select the "any" option. In the port to listen to, if you want to specify multiple ports, separate them with a comma (.). EXAMPLE: 80,8000 Or to listen on both 80 and 443 create 2 rows in the table where for the 443 you would likely want to check the SSL-offloading checkbox.

Max connections:

Sets the maximum amount of connections this frontend will accept, may be left empty.

Type:

This defines the processing type of HAProxy, and will determine the available options for acl checks and also several other options. Please note that for https encryption/decryption on HAProxy with a certificate the processing type needs to be set to "http".

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

Actions: Use these to select the backend to use or perform other actions like calling a lua script, blocking certain requests or others available.

Action	Parameters	Condition acl names	Actions
<input type="checkbox"/> Use Backend	See below		
<input checked="" type="checkbox"/> backend: web_servers			

Example:

Action	Parameters	Condition
Use Backend	Website1Backend	Backend1acl
http-request header set	Headername: X-HEADER-ClientCertValid New logformat value: YES	addHeaderAcl

Default Backend:

If a backend is selected with actions above or in other shared frontends, no default is needed and this can be left to "None".

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.

Certificate

Choose the cert to use on this frontend.

- Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)
- Add ACL for certificate Subject Alternative Names.

Une fois tout fait, faites save.

Advanced settings

Client timeout
the time (in milliseconds) we accept to wait for data from the client, or for the client to accept data (default 30000).

Use "forwardfor" option Use "forwardfor" option.
The "forwardfor" option creates an HTTP "X-Forwarded-For" header which contains the client's IP address. This is useful to let the final web server know what the client address was. (eg for statistics on domains)

Use "httpclose" option
By default HAProxy operates in keep-alive mode with regards to persistent connections: for each connection it processes each request and response, and leaves the connection idle on both sides between the end of a response and the start of a new request.

Bind pass thru
NOTE: paste text into this box that you would like to pass behind each bind option.

Advanced pass thru
NOTE: paste text into this box that you would like to pass thru in the frontend.

Votre règle devrait ressembler à ceci.

Services / HAProxy / Frontend

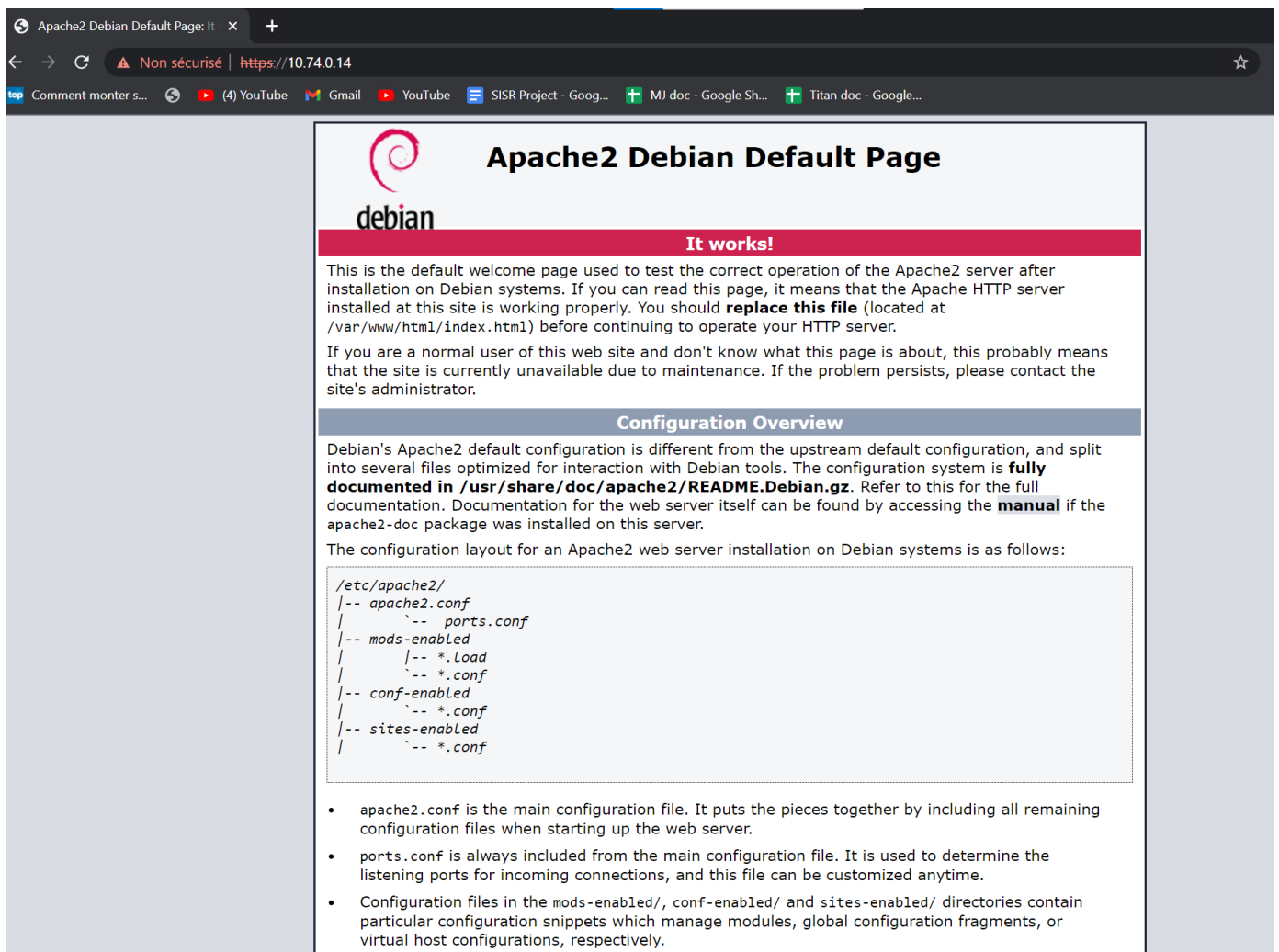
Settings Frontend Backend Files Stats Stats FS Templates

Frontends

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	https-frontend	HTTPS	10.74.0.14:443	https	web_servers web_servers (default)	<input type="button" value="edit"/> <input type="button" value="delete"/> <input type="button" value="copy"/>

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.



Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|   |-- ports.conf  
|-- mods-enabled  
|   |-- *.Load  
|   |-- *.conf  
|-- conf-enabled  
|   |-- *.conf  
|-- sites-enabled  
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.