

Introduction Pfsense



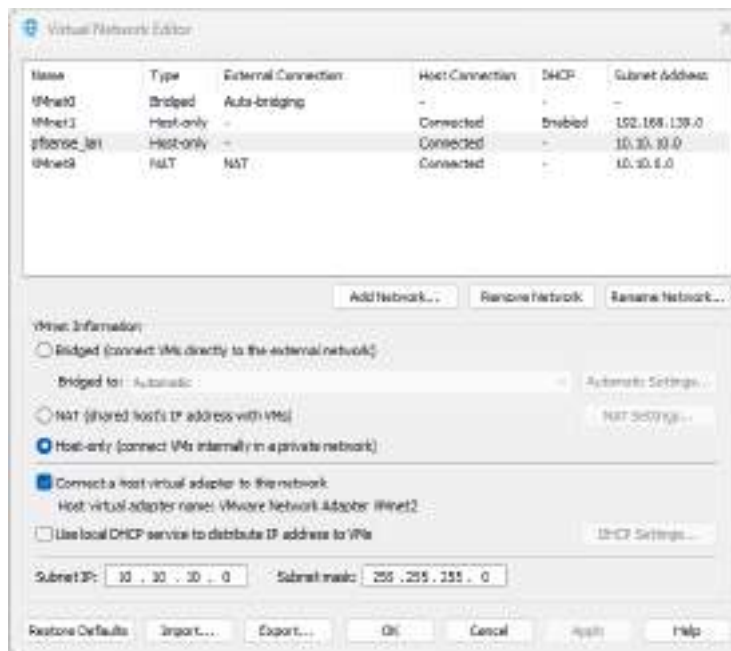
SOMMAIRE

I. Installation initiale	2
II. Configuration basique	5
a. IP statique pour le LAN	5
b. Interface web	6
c. IP statique pour le WAN	7
III. Configurer l'accès à l'interface web de Pfsense depuis le WAN (temporairement)	8
d. Augmenter le nombre de connexions simultanées à l'interface web	11
e. Configuration de la redirection de port sur la box (Livebox orange)	11
IV. OpenVPN	12
a. Créer le certificat	12
b. Créer les utilisateurs	13
c. Création du serveur OpenVPN	14
V. IPsec	20

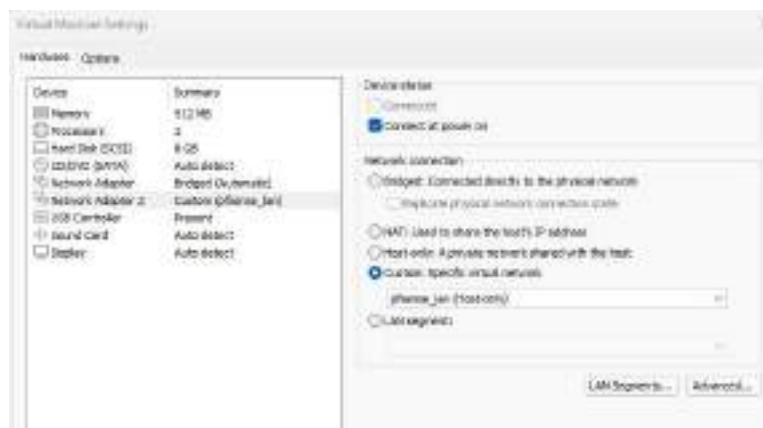
I. Installation initiale

Nécessite :

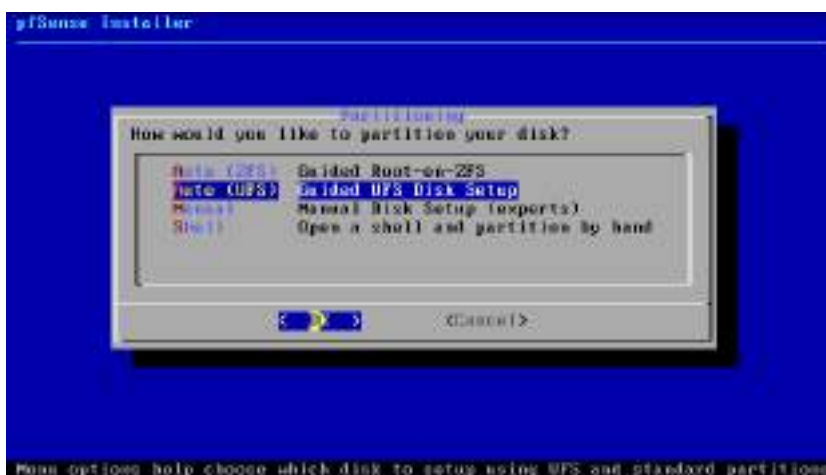
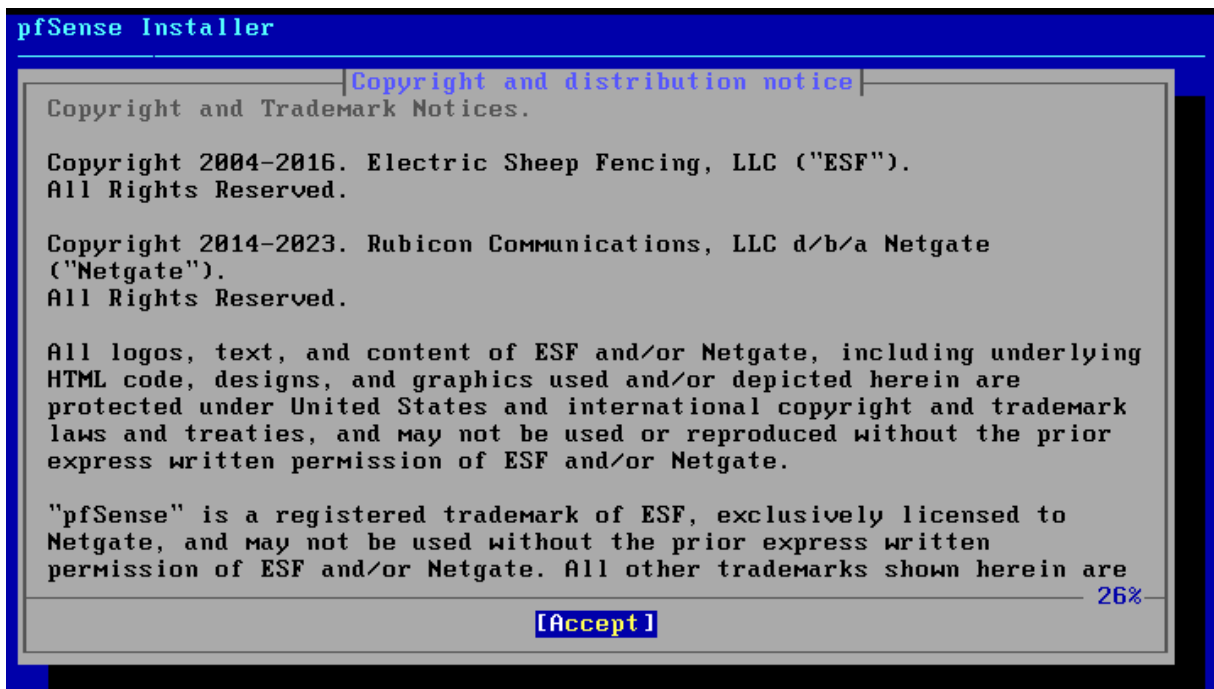
- ISO de pfsense
- Installation sur une VM :
 - o Linux
 - o Mémoire : 512 MB
 - o Disque : 8 GB
 - o Network adapter : Bridged
- Création d'un commutateur virtuel :
 - o Sans DHCP
 - o En Host-Only



- Ajout d'une seconde carte réseau à la VM avec le commutateur LAN



Lancer la VM et suivre l'installateur :





```
Enter the WAN interface name or 'a' for auto-detection
(le0 le1 or a): a

Connect the WAN interface now and make sure that the link is up.
Then press ENTER to continue.

No link-up detected.

Enter the WAN interface name or 'a' for auto-detection
(le0 le1 or a): le0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(le1 a or nothing if finished): le1
```

II. Configuration basique

a. IP statique pour le LAN

```
FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 903f76f43632c830785f
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> le0          -> v4/DHCP4: 192.168.1.54/24
                v6/DHCP6: 2a01:cb10:840:9e00:20c:29ff:fe32:f39
1/64
LAN (lan)      -> le1          -> v4: 192.168.1.1/24
                v6/t6: 2a01:cb10:840:9ed8:20c:29ff:fe32:f39b/6
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: █
```

Entrer 2, mettre 10.10.10.254 en adresse IP et 24 :

```
Available interfaces:
1 - WAN (le0 - dhcp, dhcp6)
2 - LAN (le1 - 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:
> 10.10.10.254

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) █
```

Répondre oui pour l'activation du DHCP sur le LAN et mettre 10.10.10.100-10.10.10.200 en range :

```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.10.10.100
Enter the end address of the IPv4 client address range: 10.10.10.200
Disabling IPv6 DHCPD...
```

Répondre non à la question Do you want revert to http :

```
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 10.10.10.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    https://10.10.10.254/

Press <ENTER> to continue. █
```

b. Interface web

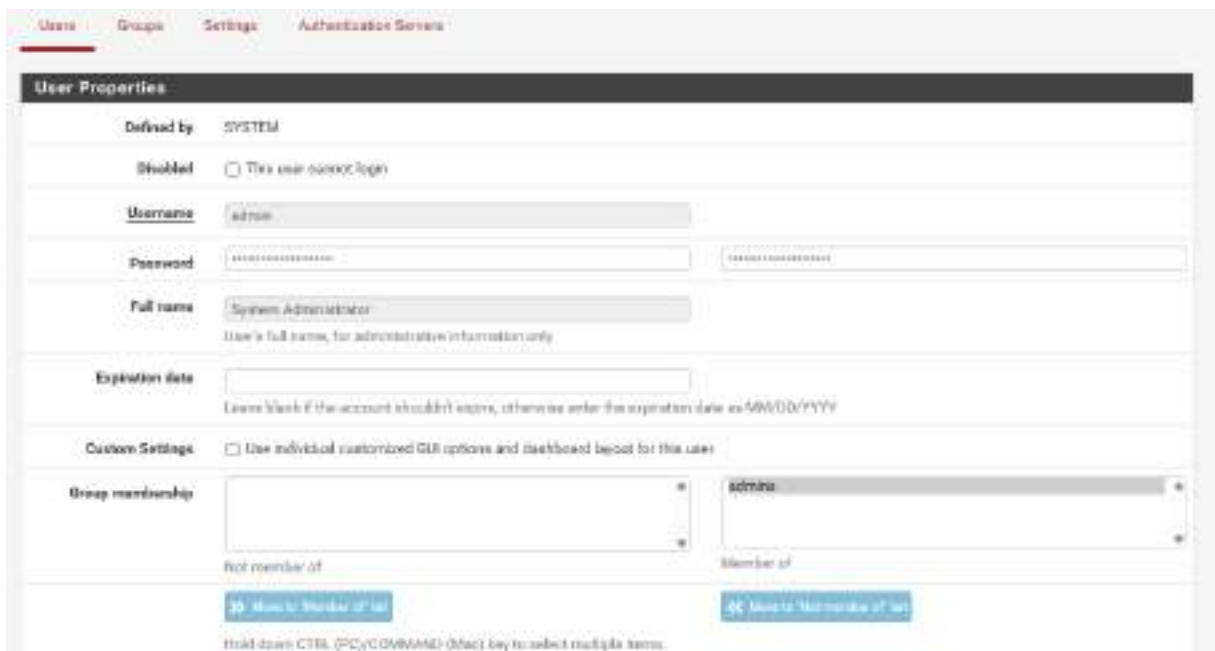
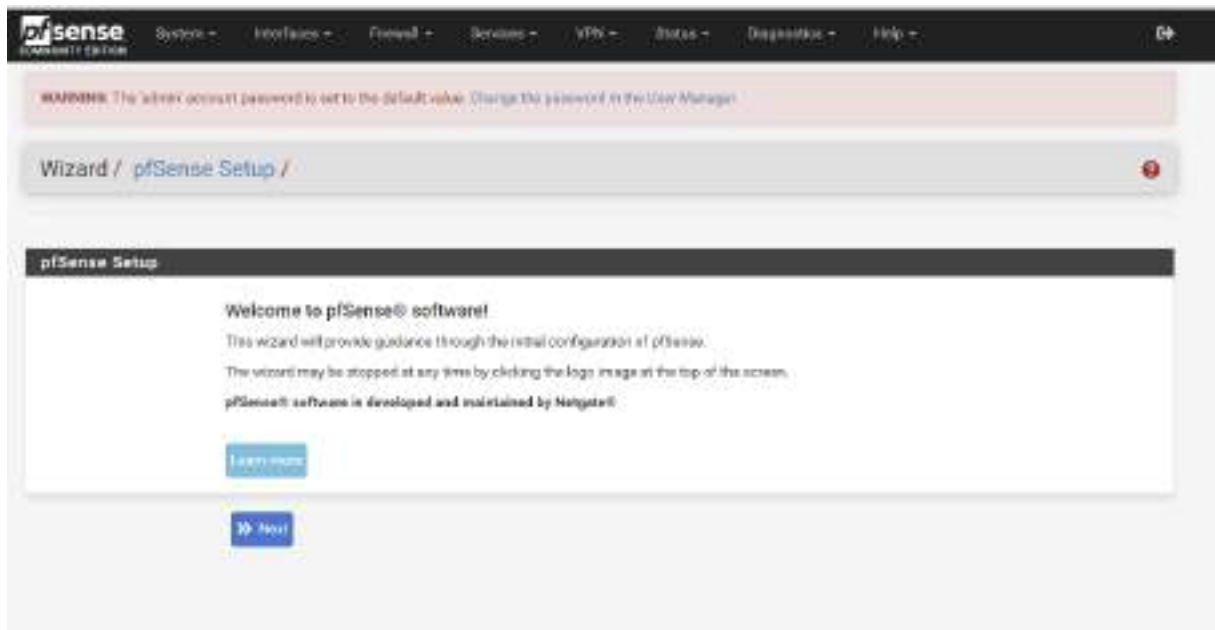
Aller sur <https://10.10.10.254/>:



Login et mot de passe par défaut : admin / pfsense



Changer le mot de passe :



c. IP statique pour le WAN

Mettre en Static IPv4, désactiver IPv6, renseigner l'adresse voulue et mettre le masque en /24 :

General Configuration

Enable Enable interface

Description WAN
Enter a descriptive (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

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 60 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex Default (no preference, typically autoselect)
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

Cliquer sur Add a new gateway et renseigner l'adresse de la box :

New IPv4 Gateway

Default Default gateway

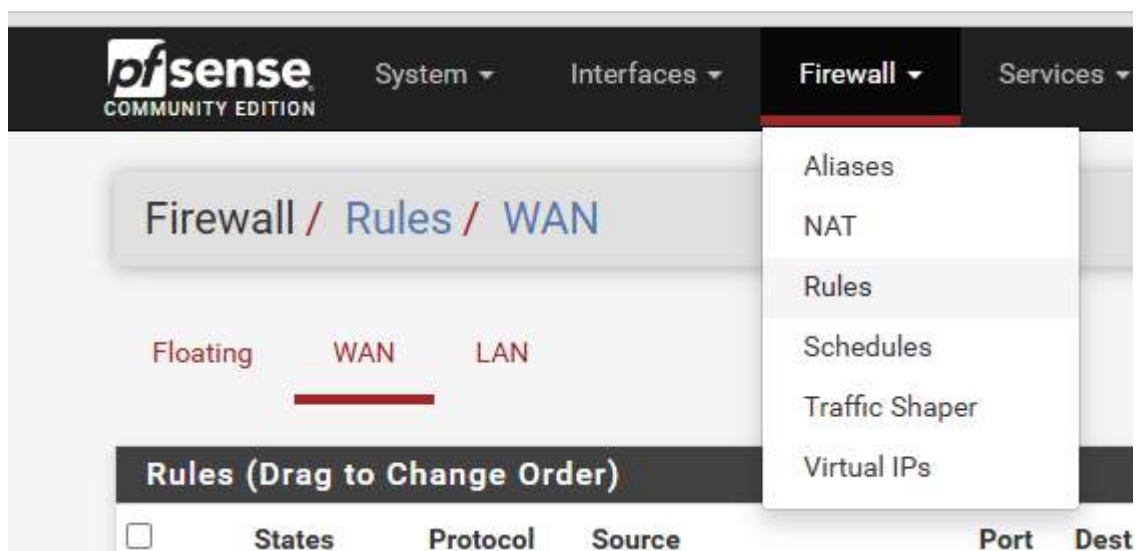
Gateway name WANGW

Gateway IPv4 192.168.1.1

Description IP box

III. Configurer l'accès à l'interface web de Pfsense depuis le WAN (temporairement)

Aller dans Firewall, Rules, WAN :



Cliquer sur Add, choisir WAN Address en destination, HTTPS (443) en Destination Port Range et cocher Log :

Edit Firewall Rule

Action
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

Interface
Choose the interface from which packets must come to match this rule.

Address Family
Select the Internet Protocol version this rule applies to.

Protocol
Choose which IP protocol this rule should match.

Source

Source **Invert match**

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

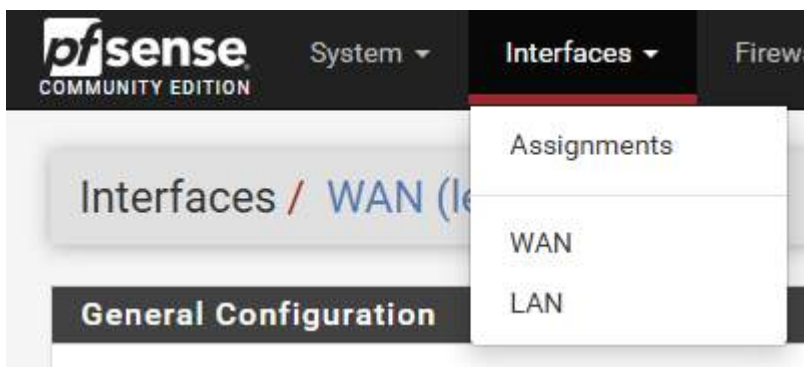
Extra Options

Log **Log packets that are handled by this rule**
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status > System Logs > Settings page).

Faire save puis cliquer sur Apply Changes :



Aller dans Interfaces, WAN :



Décocher Block private networks et Block bogon networks:



Connexion possible de l'adresse IP wan (ici 192.168.1.100) :



d. Augmenter le nombre de connexions simultanées à l'interface web

Aller dans System, Advanced et mettre le nombre souhaité dans Max processes (ici 10) :

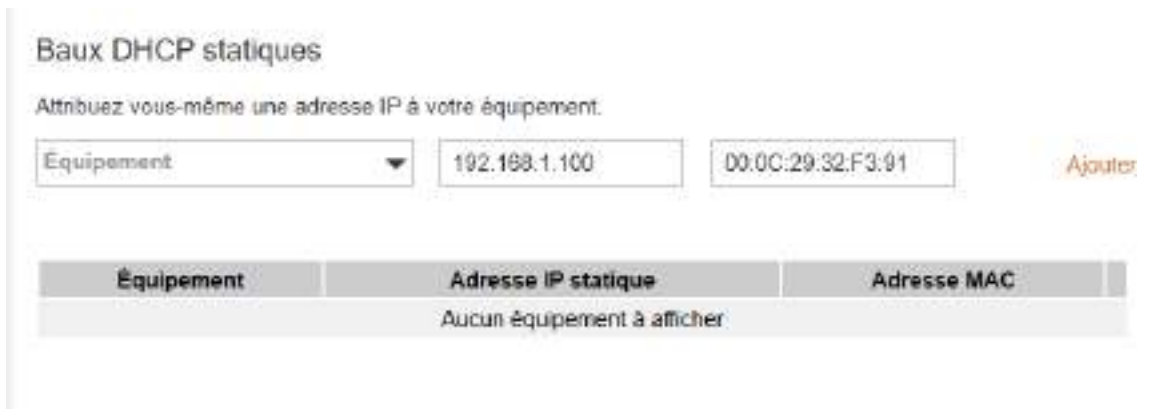


e. Configuration de la redirection de port sur la box (Livebox orange)

Se connecter à l'interface d'administration de la box :

192.168.1.1 Aller dans paramètres avancés, réseau :

Indiquer l'adresse statique de l'interface wan :

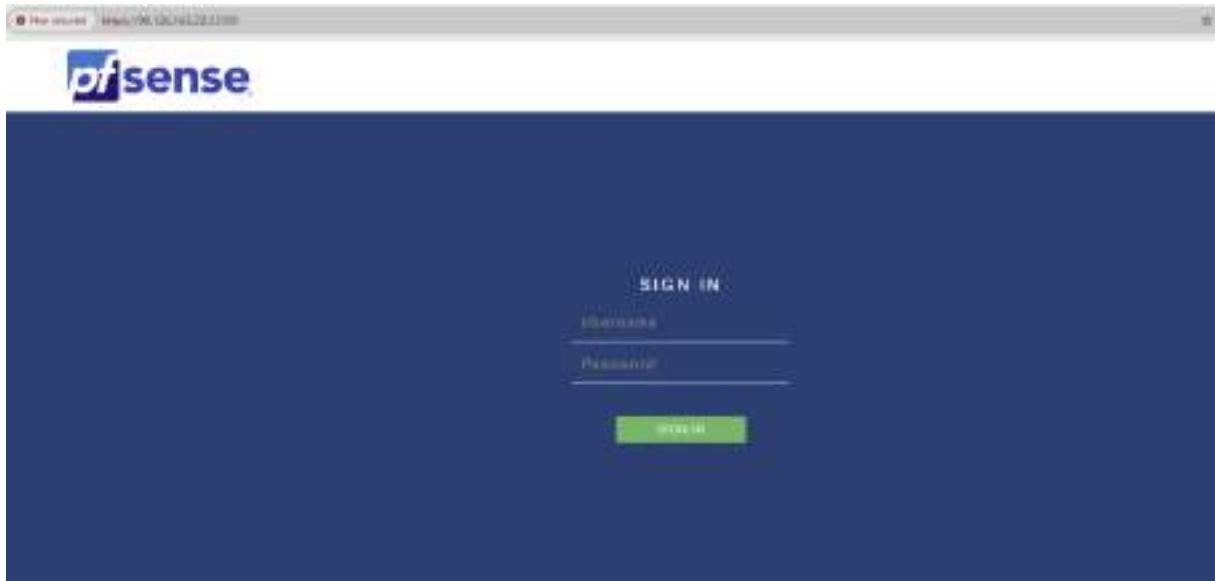


Équipement	Adresse IP statique	Adresse MAC	
pfSense	192.168.1.100	00:0C:29:32:F3:91	

Aller dans Réseau, NAT/PAT, créer la règle suivante :

Activer	Application/Service	Port interne	Port externe	Protocole	Équipement	IP externe	
<input checked="" type="checkbox"/>	pfSense3	443	22000	TCP	pfSense	Toutes	

Cela permet de se connecter à partir de <https://ippublic:22000> vers l'interface web du pfSense.



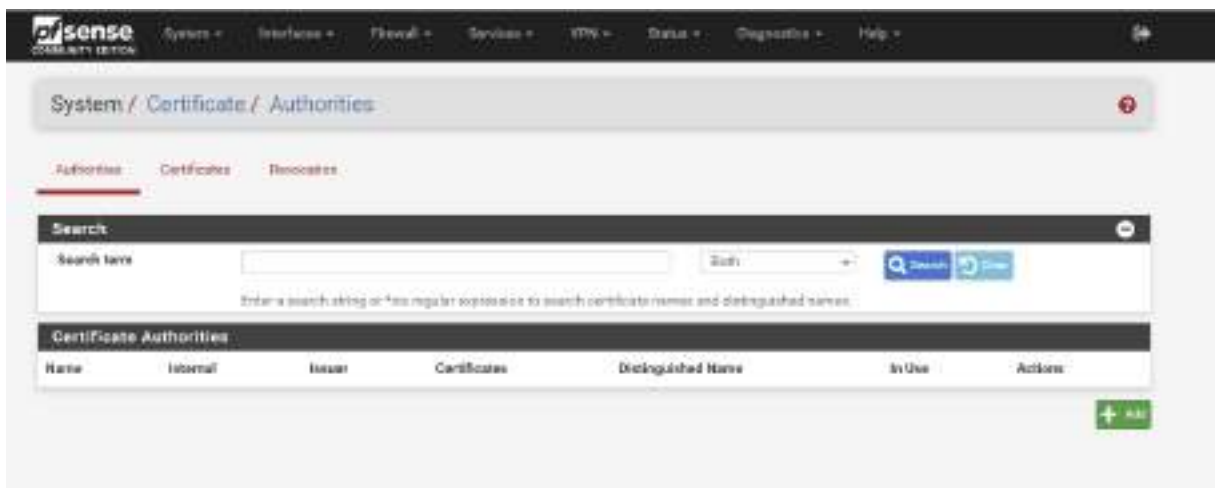
Si cette accès n'est plus nécessaire, supprimer la règle de redirection sur la livebox et aller sur l'interface de pfsense, dans Firewall, rules, WAN et supprimer la règle suivante :



IV. OpenVPN

a. Créer le certificat

Aller dans System, certificates, Authorities et cliquer sur Add :



Renseigner les informations comme suit :

Create / Edit CA

Descriptive name VPN Server CA
The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: !, ", &, ' , /, \, |, ^, ` , ~

Method Create an Internal Certificate Authority

Trust State Add this Certificate Authority to the Operating System Trust State
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial Use random serial numbers when signing certificates.
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness (instead of using the sequential value from Next Certificate Serial).

Internal Certificate Authority

Key Size RSA

Key Length 2048
The length to use when generating a new RSA key, in bits.
The key length should not be lower than 2048 in some platforms may consider the certificate invalid.

Digest Algorithm sha256
The digest method used when the CA is signed.
The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Lifetime (days) 3650

Common Name VPNCA
The following certificate authority subject components are optional and may be left blank:

Country Code FR

State or Province France

City e.g. Austin

Résultat :

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
VPN Server CA	<input checked="" type="checkbox"/>	self signed	0	ST=France, CN=VPNCA, C=FR Valid From: Tue, 18 Nov 2025 11:50:32 +0000 Valid Until: Fri, 18 Nov 2031 11:50:32 +0000	<input checked="" type="checkbox"/>	

b. Créer les utilisateurs

Aller dans System, User Manager, Users :

System / User Manager / Users

Users Groups Settings Authentication Servers

Username	Full name	Status	Groups	Actions
admin	System Administrator	<input checked="" type="checkbox"/>	admin	

Cliquer sur Add, remplir les informations nécessaires et cocher Click to create a user certificate :

Cliqu

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

User Properties

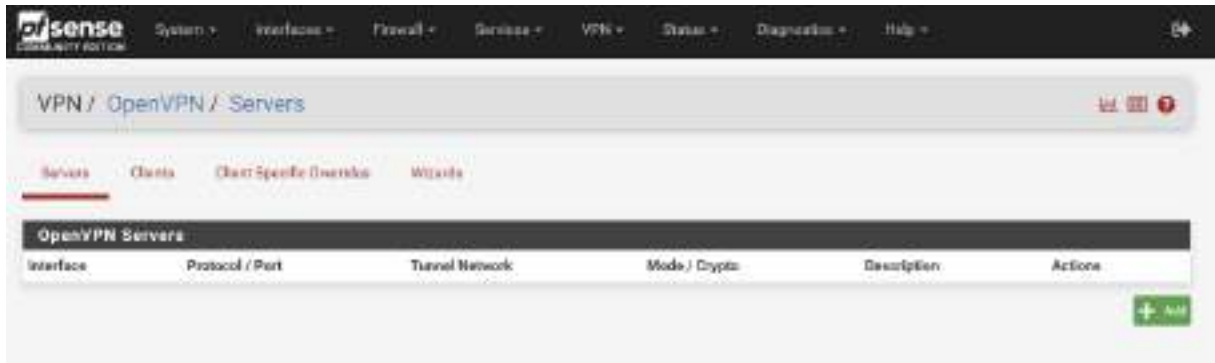
Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	<input type="text" value="josed"/>
Password	<input type="password" value="....."/> <input type="password" value="....."/>
Full name	<input type="text" value="josephed"/> <small>User's full name, for administrative information only.</small>
Expiration date	<input type="text"/> <small>Leave blank if the account should not expire, otherwise enter the expiration date as MM/DD/YYYY</small>
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.
Group membership	<input type="text" value="admins"/> <input type="text"/> <small>Not member of</small> <small>Member of</small>
	<input type="button" value="Add to Selection of list"/> <input type="button" value="Remove from Selection of list"/> <small>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items</small>
Certificate	<input checked="" type="checkbox"/> Click to create a user certificate

Create Certificate for User

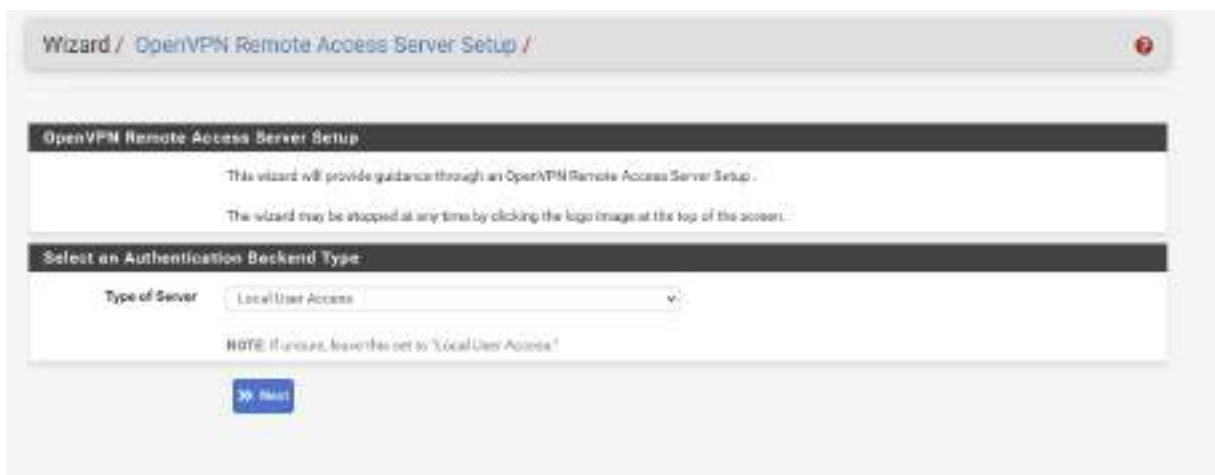
Descriptive name	<input type="text" value="VPNcert"/>
Certificate authority	<input type="text" value="VPN Server CA"/>
Key type	<input type="text" value="RSA"/>
	<input type="text" value="2048"/> <small>The length to use when generating a new RSA key in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.</small>
Digest Algorithm	<input type="text" value="sha256"/> <small>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.</small>
Lifetime	<input type="text" value="3650"/>

c. Création du serveur OpenVPN

Aller dans VPN, OpenVPN et cliquer sur Wizards :



Suivre le wizard :



Ensuite cliquer sur Add new certificate :



Create a New Server Certificate	
Descriptive name	<input type="text" value="CertOpenVPNprincipal"/> <p>A name for administrative reference, to identify this certificate.</p>
Key length	<input type="text" value="2048 bit"/> <p>Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the maximum and most common selection and 1024 is the minimum in common use. For more information see keylength.com.</p>
Lifetime	<input type="text" value="365"/> <p>Lifetime in days. Server certificates should not have a lifetime over 366 days or some platforms may consider the certificate invalid.</p>
Common Name	<input type="text"/> <p>The internal name of the server certificate, used as a part of the certificate subject. Typically set to the hostname of the system. This value is also used as a Subject Alternative Name (SAN). If left blank, the Descriptive Name value will be used for the Common Name and SAN instead.</p>
Country Code	<input type="text" value="FR"/> <p>Two letter ISO country code (e.g. US, AU, CA)</p>
State or Province	<input type="text" value="France"/> <p>Full State or Province name, not abbreviated (e.g. Texas, Indiana, Ontario).</p>
City	<input type="text"/> <p>City or other Locality name (e.g. Austin, Indianapolis, Toronto).</p>
Organization	<input type="text"/> <p>Organization name, often the company or group name.</p>
Organizational Unit	<input type="text"/> <p>Organizational Unit name, often a department or team name.</p>

Renseigner le nom :

Wizard / OpenVPN Remote Access Server Setup / Server Setup	
Step 3 of 11	
Server Setup	
OpenVPN Remote Access Server Setup Wizard	
General OpenVPN Server Information	
Description	<input type="text" value="OpenVPN"/> <p>A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote-Accessal (001)"). It is also used by OpenVPN Client Export to identify this VPN on clients.</p>
Endpoint Configuration	
Protocol	<input type="text" value="UDP on IPv4 only"/> <p>Protocol to use for OpenVPN connections, if unset, leave this set to UDP.</p>
Interface	<input type="text" value="WAN"/> <p>The interface where OpenVPN will listen for incoming connections (typically WAN).</p>
Local Port	<input type="text" value="1194"/> <p>Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.</p>

Renseigner la partie Tunnel settings comme suit :

Tunnel Settings	
IPv4 Tunnel Network	10.10.11.0/24 <small>This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.0.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.</small>
Redirect IPv4 Gateway	<input type="checkbox"/> Force all client generated traffic through the tunnel.
IPv4 Local Network	10.10.10.0/24 <small>This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</small>
Concurrent Connections	5 <small>Specify the maximum number of clients allowed to concurrently connect to this server.</small>
Allow Compression	<input type="checkbox"/> Refuse any form of compression (Most secure) <small>Allow compression to be used with this VPN instance, which is potentially insecure.</small>
Compression	Disable Compression (Best Preference) <small>Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may corrupt data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.</small>
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Intra-Client Communication	<input type="checkbox"/> Allow communication between clients connected to this server.
Duplicate Connections	<input type="checkbox"/> Allow multiple concurrent connections from clients using the same Common Name. <small>NOTE: This is not generally recommended, but may be needed for some scenarios.</small>
Duplicate Connection Limit	<input type="text"/> <small>Limit the number of concurrent connections from the same user.</small>

Mettre 10.10.10.254 en serveur DNS et faire next :

Advanced Client Settings	
DNS Default Domain	<input type="text"/> <small>Provide a default domain name to clients.</small>
DNS Server 1	10.10.10.254 <small>DNS server IP to provide to connecting clients.</small>
DNS Server 2	<input type="text"/> <small>DNS server IP to provide to connecting clients.</small>

Cocher Firewall Rule et OpenVPN Rule:

Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration ?

Step 11 of 11

Firewall Rule Configuration

OpenVPN Remote Access Server Firewall Rules

Rules control passing or blocking network traffic as it flows through the firewall.

Rules must be added which allow traffic to reach the OpenVPN server IP address and port, as well as to allow traffic from connected clients inside the OpenVPN tunnel.

The options on this step can add automatic rules to pass this traffic, or rules can be configured manually after completing the wizard.

Traffic from clients to server

Firewall rule Add a rule to permit connections to this OpenVPN server instance from clients anywhere on the Internet.

Traffic from clients through VPN

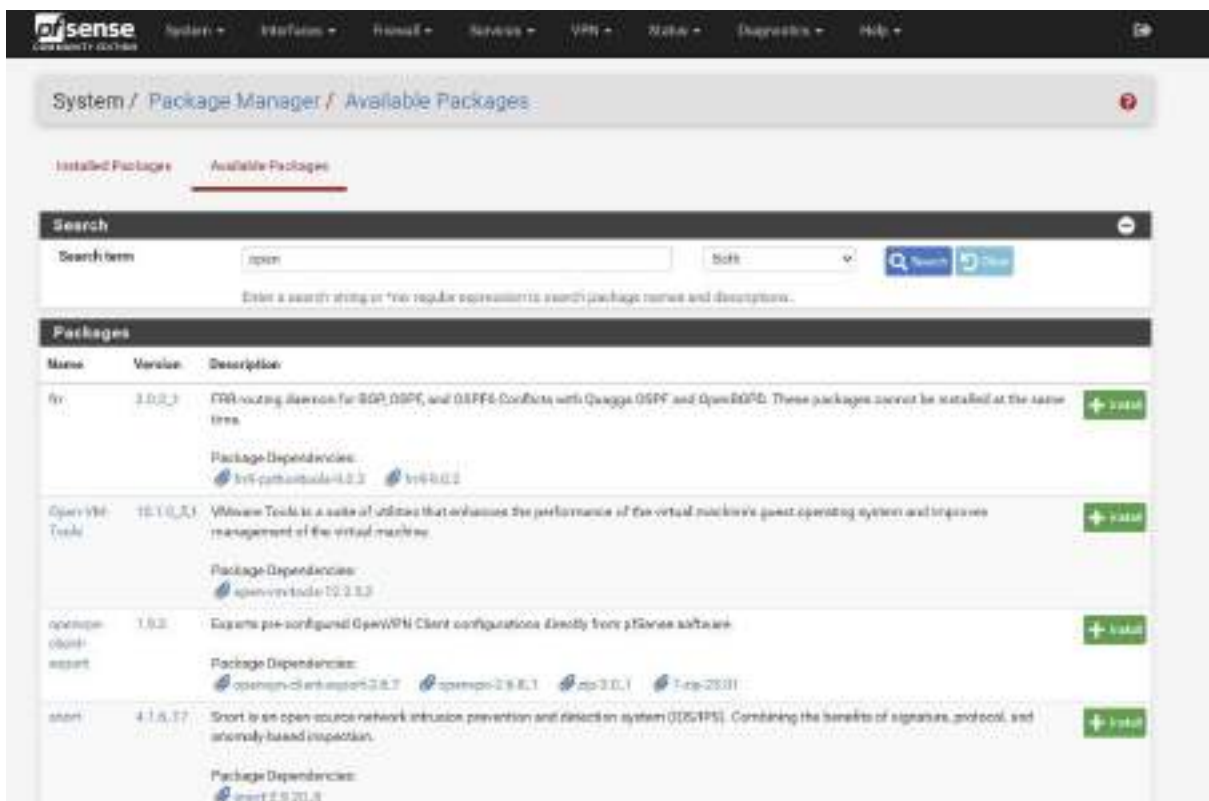
OpenVPN rule Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

[Next](#)

Terminer le wizard:



Aller dans System, Package Manager, Available packages et installer open-vpn-client-export en cliquant sur install :



Ensuite aller dans VPN, OpenVPN, Client export et défilez jusqu'à OpenVPN Clients :

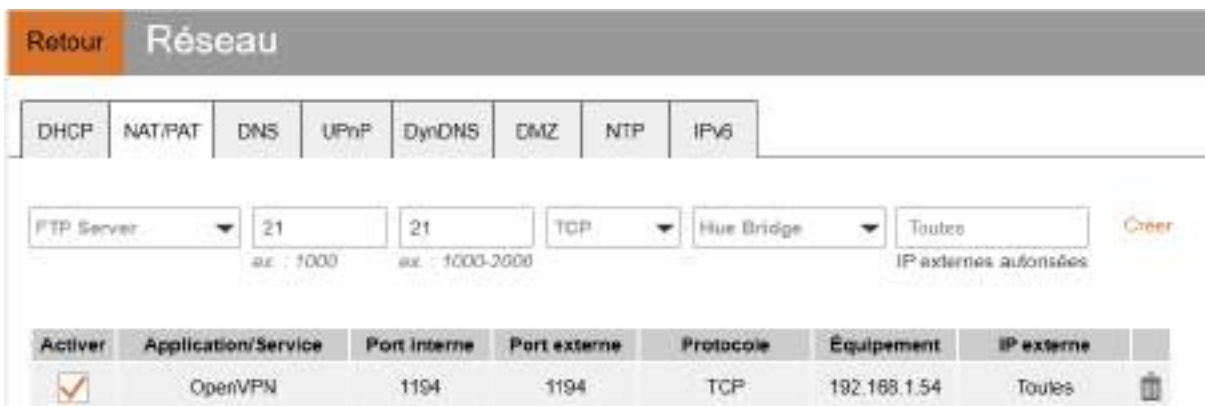


Télécharger le client adapté et l'installer sur le poste cible.

Ensuite vérifier que la règle concernant le VPN s'est bien créée dans Firewall, Rules: WAN :



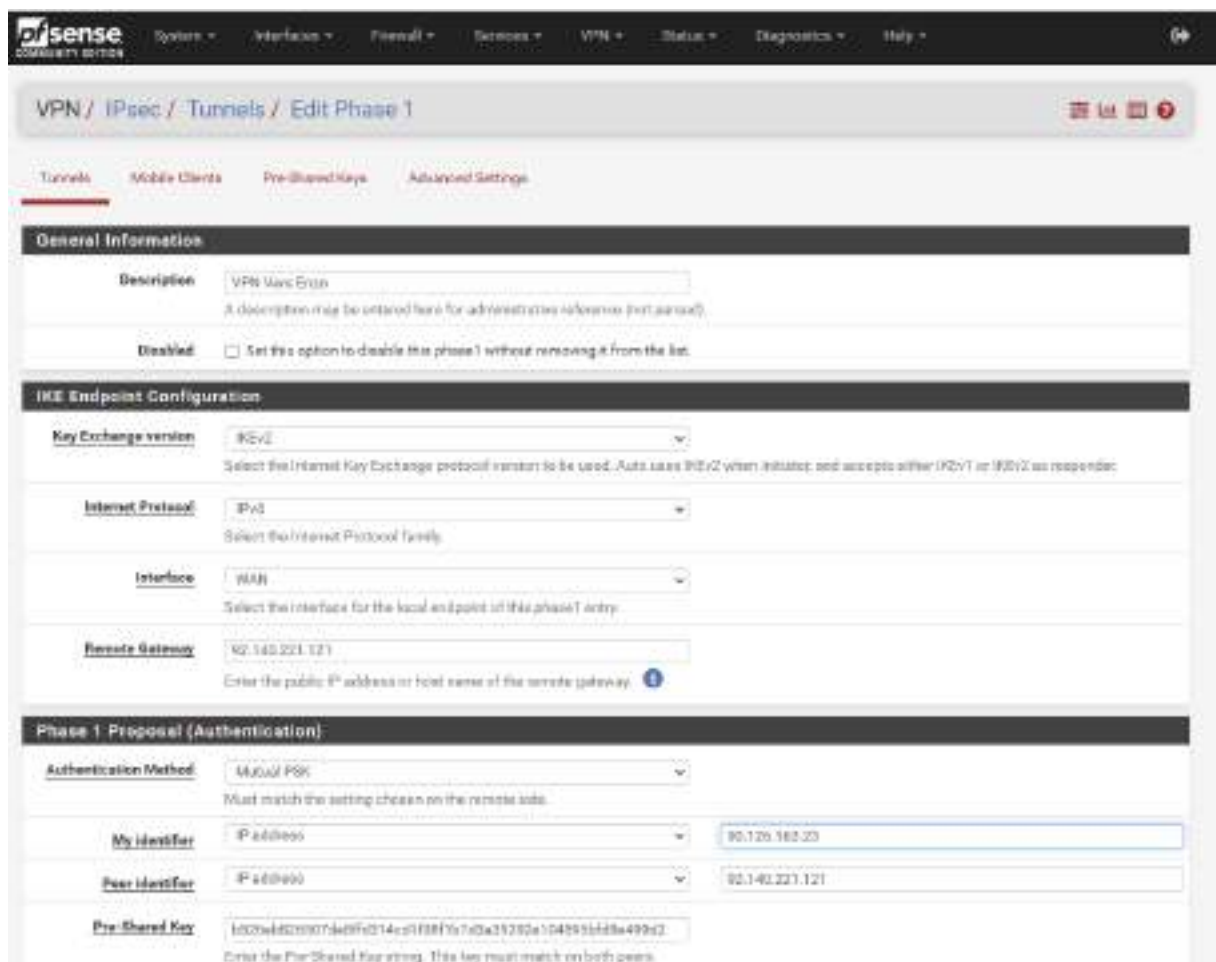
Configurer les règles de redirection sur la box :



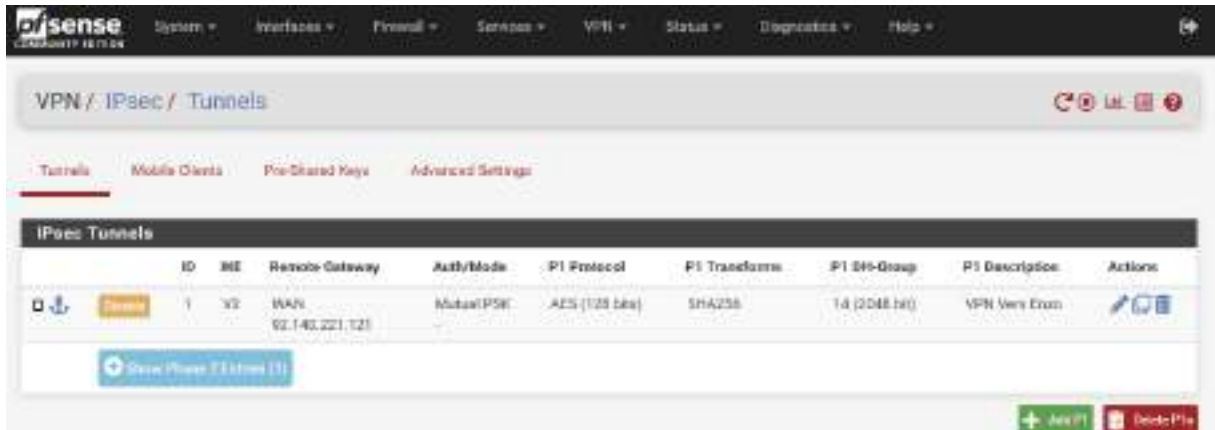
V. IPsec



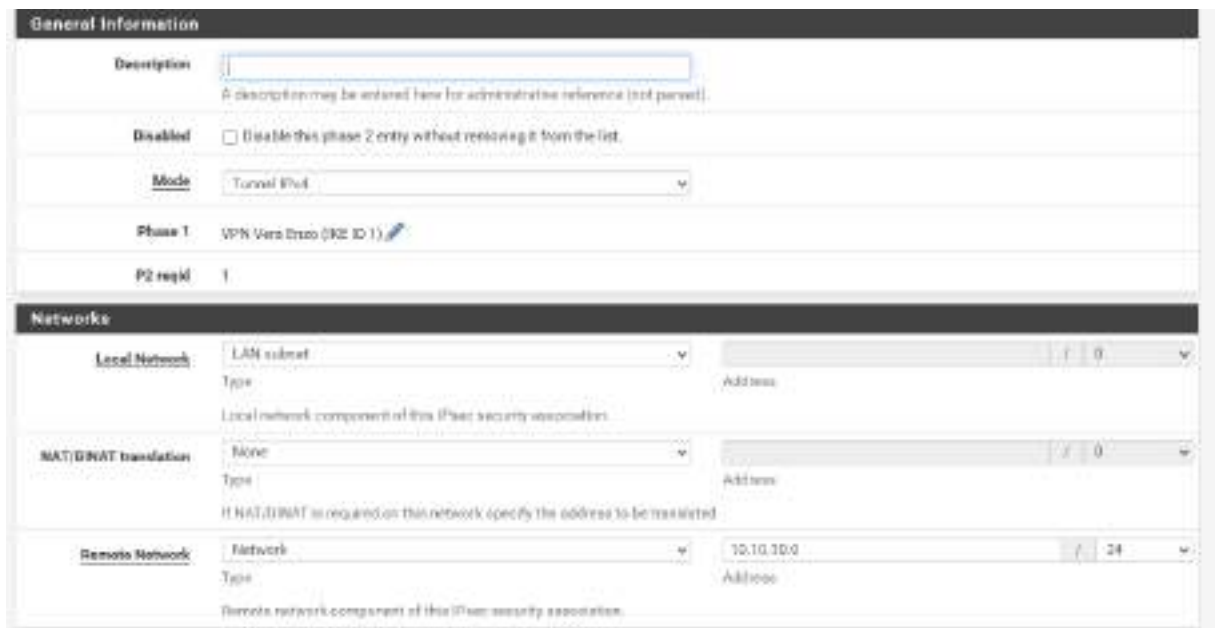
Cliquer sur Add P1 et renseigner les informations suivantes :



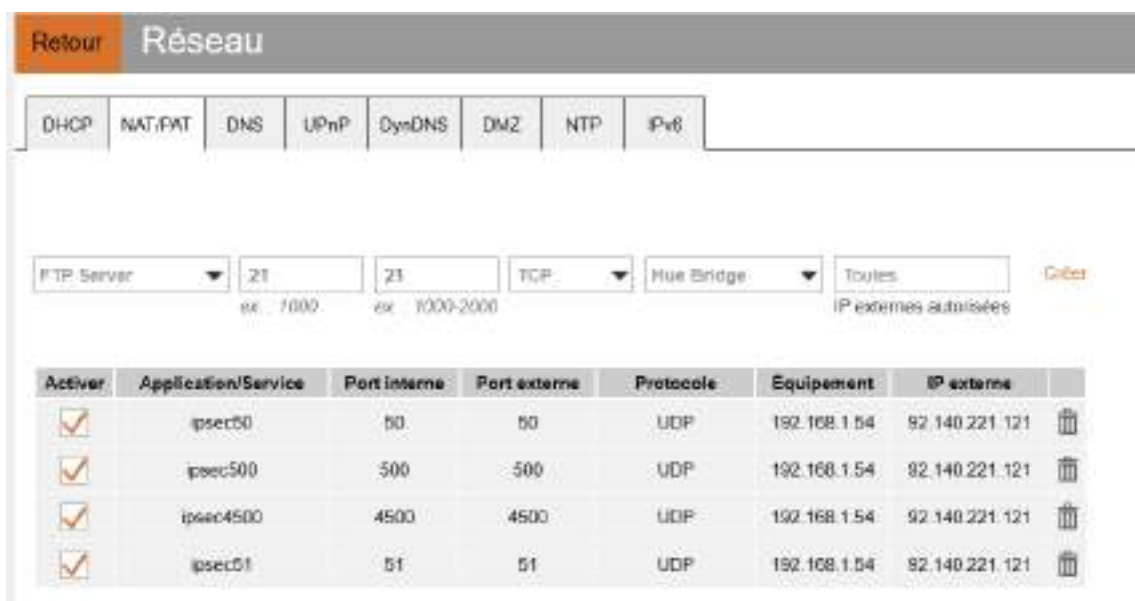
Cliquer sur Show Phase 2 entries puis Add p2 :



Dans P2, mettre l'adresse LAN du site distant :



Mettre en place les redirections nécessaires sur la box :



Ensuite aller sur Pfsense dans Status, Ipsec, le tunnel devrait être apparu :



Cliquer sur Connect P1 en même temps que le pfsense du site distant. Il est alors indiqué que le tunnel est Established.

Pour tester aller dans Diagnostics, Ping, indiquer l'adresse IP LAN de l'autre pfsense et mettre LAN en source address :

