Projet NovaResQ

BTS SIO 2025 Option SISR

Documentation Technique Situation Professionnelle 2

Table des matières

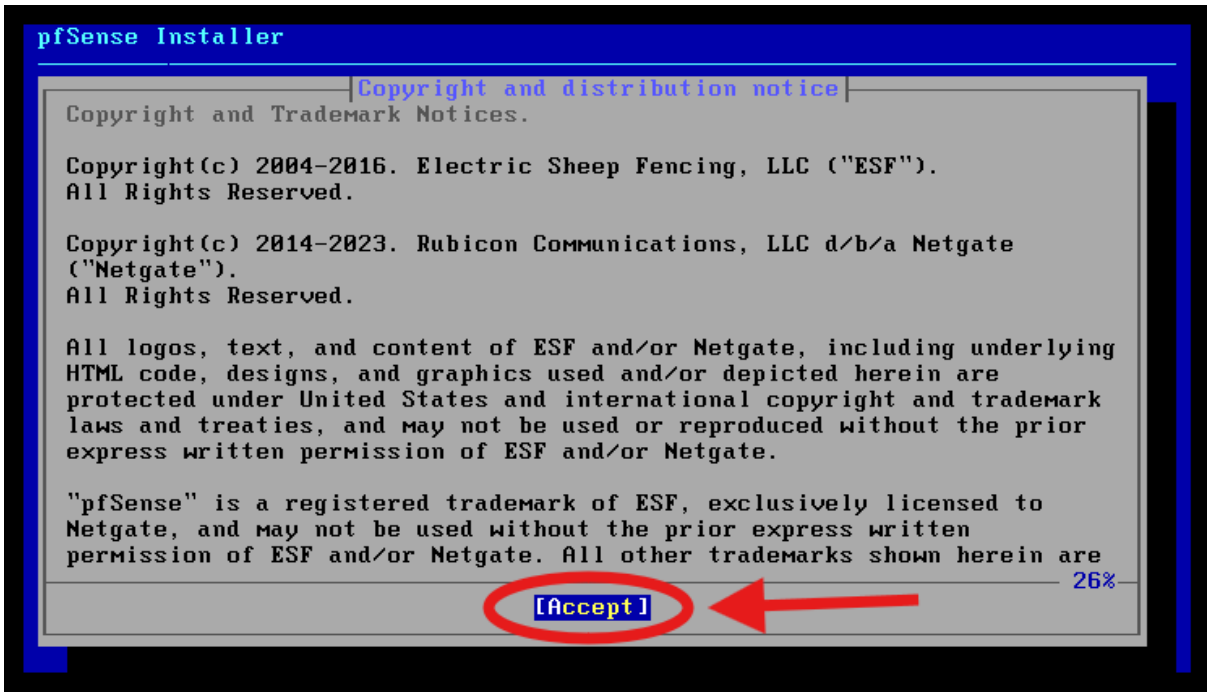
Configuration des routeurs PfSense

09/04/2025

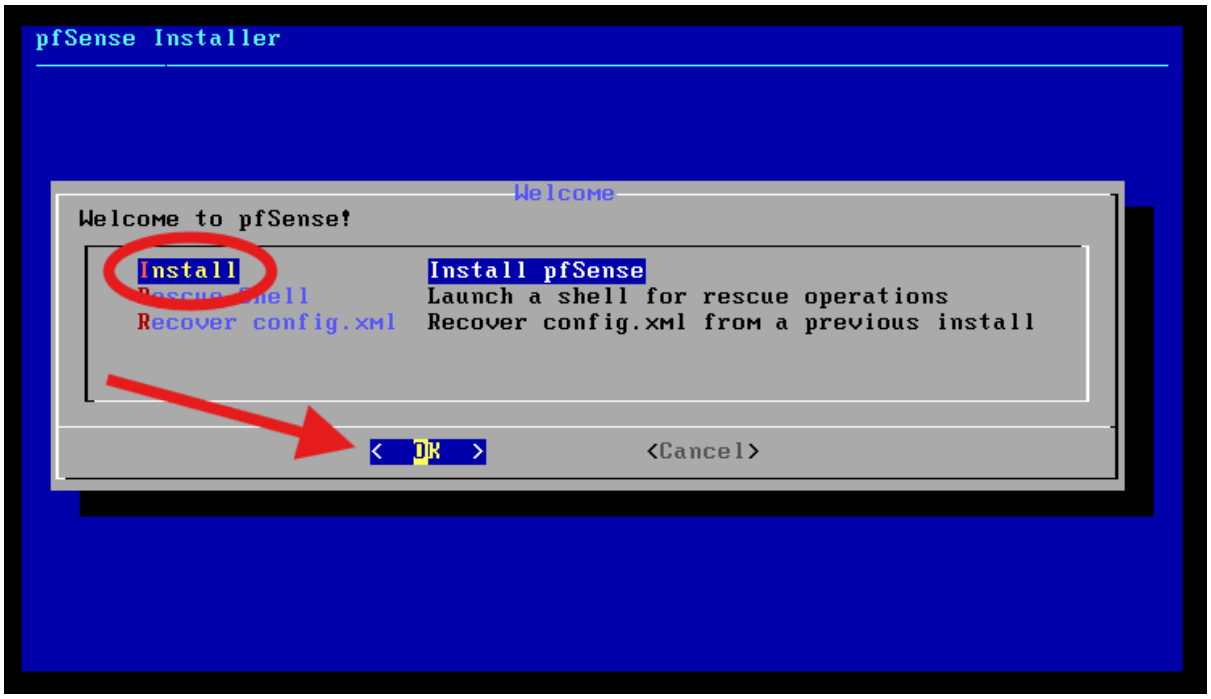
1) Préparation des routeurs

A) Initialisation de PfSense

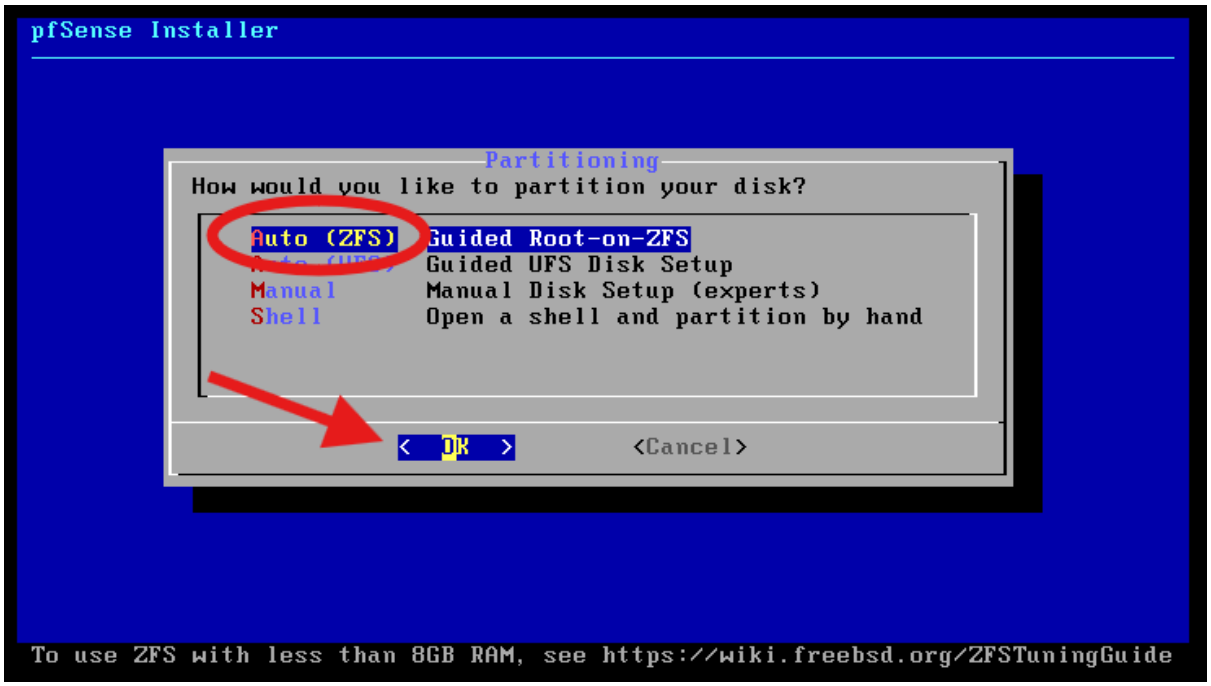
Cliquer sur Accept.



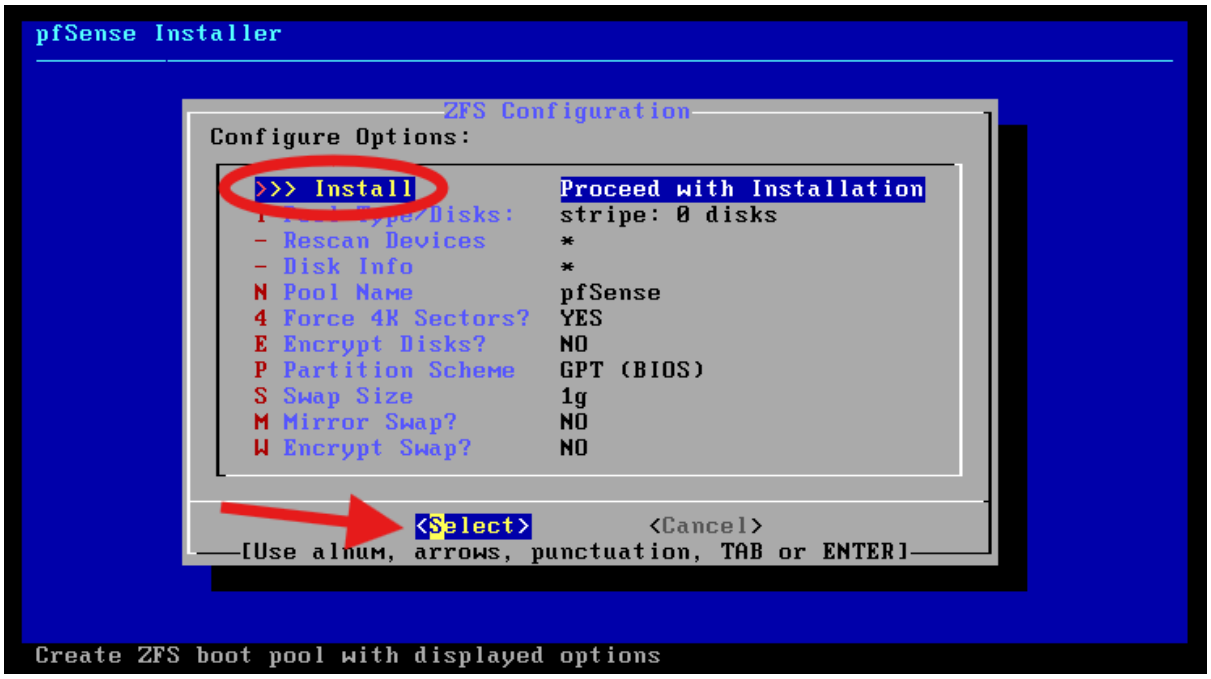
Choisir Install puis valider.



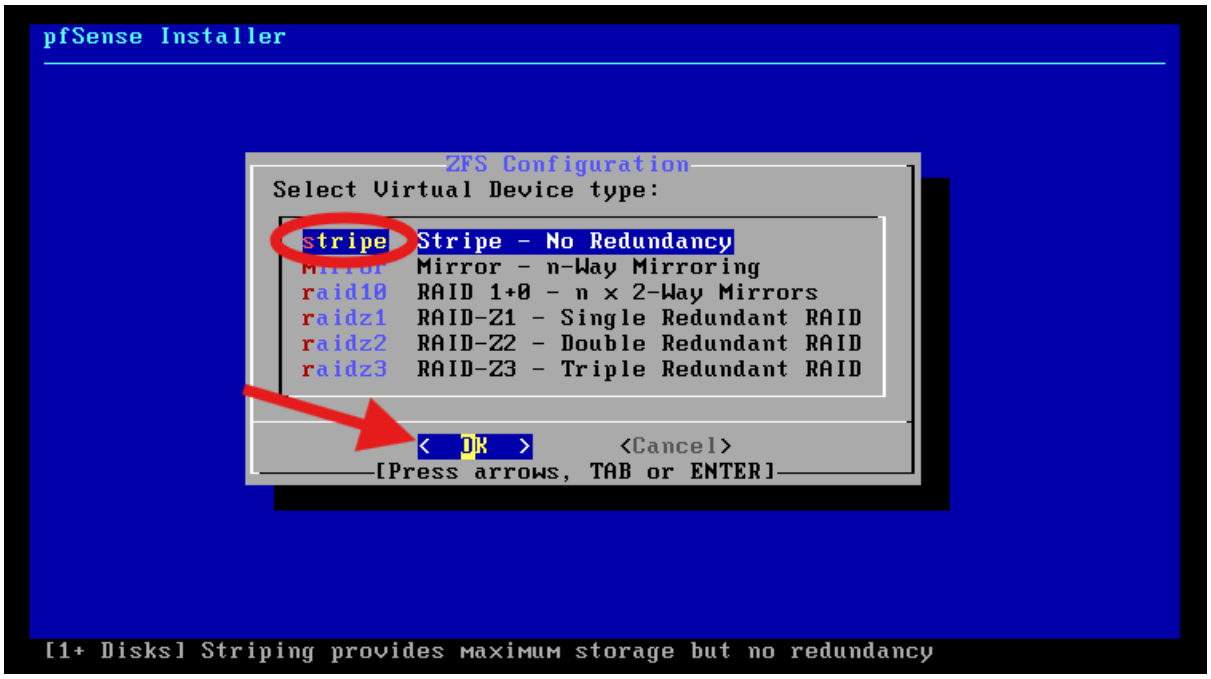
Choisir Auto (ZFS) puis valider.



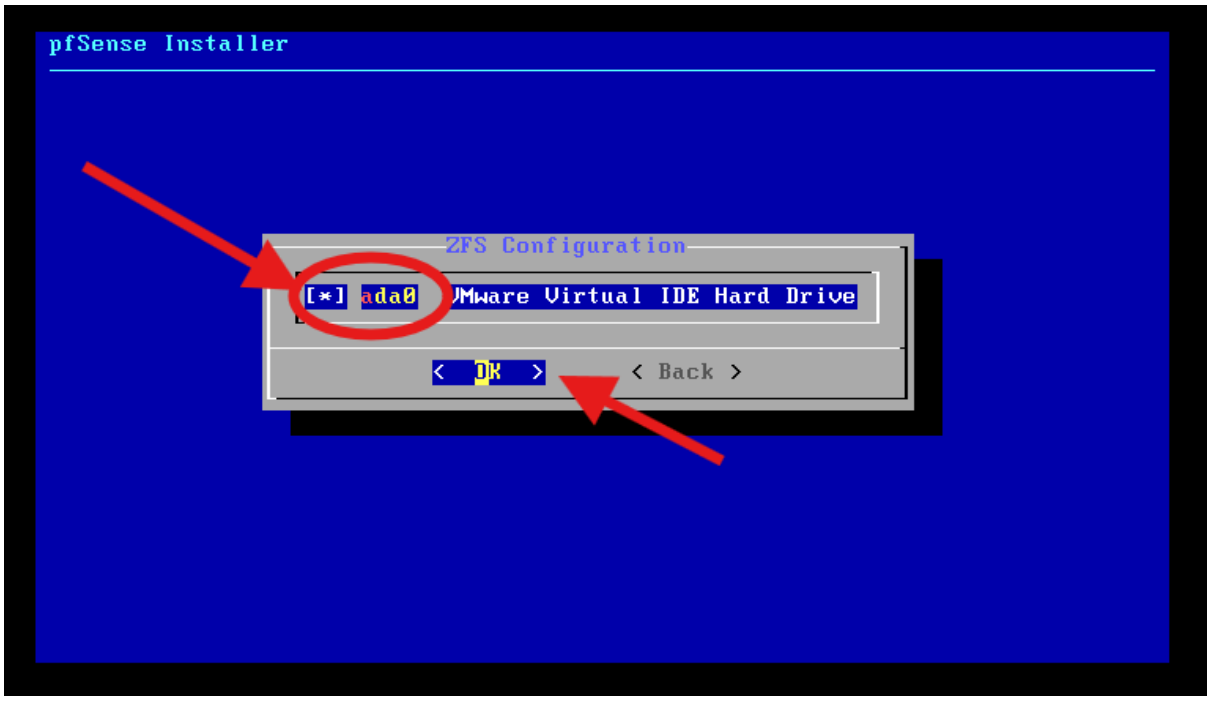
Sélectionner Install



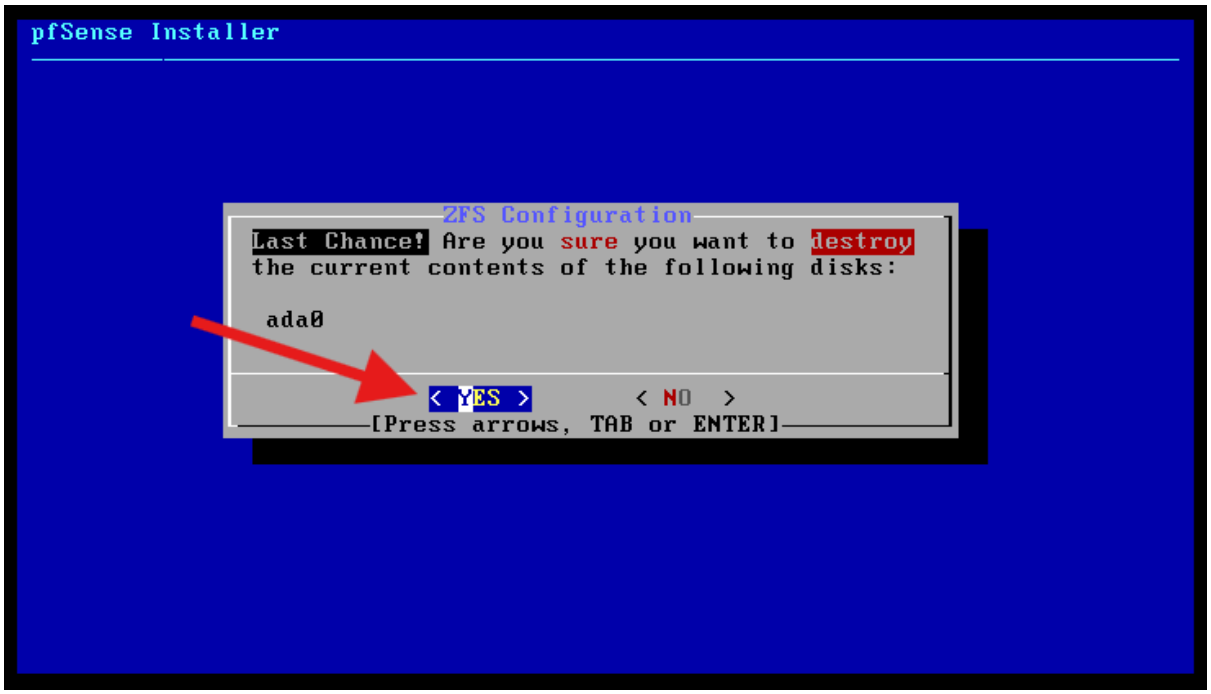
Choisir Stripe et valider.



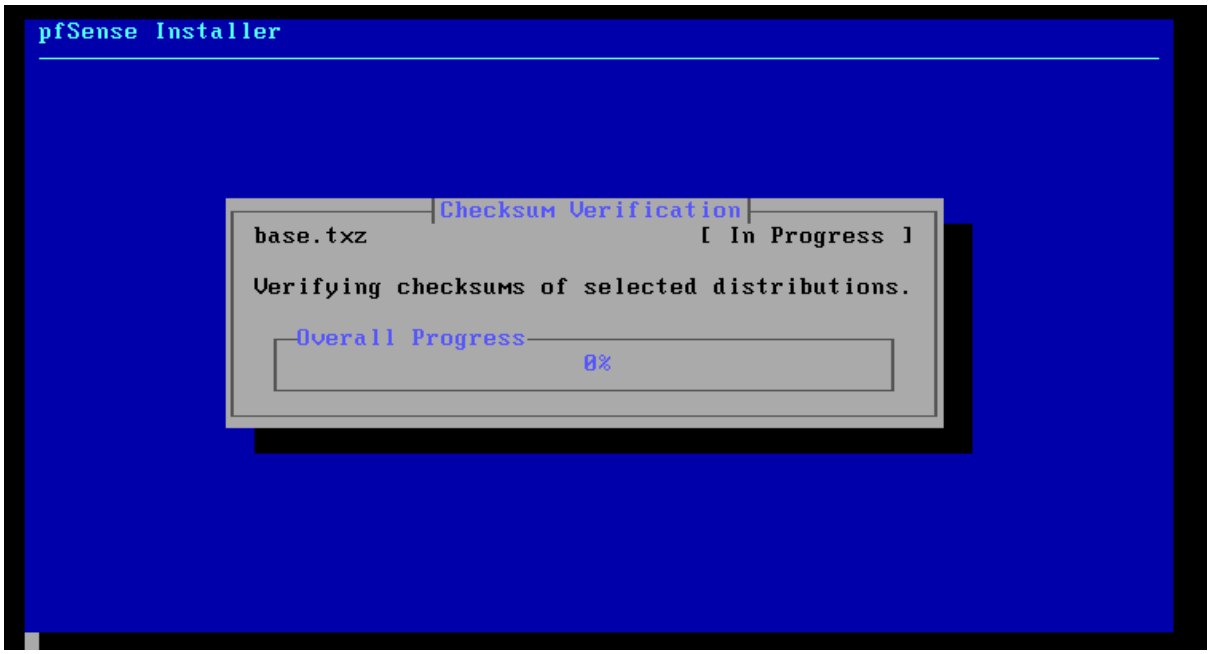
Choisir le disque et valider.



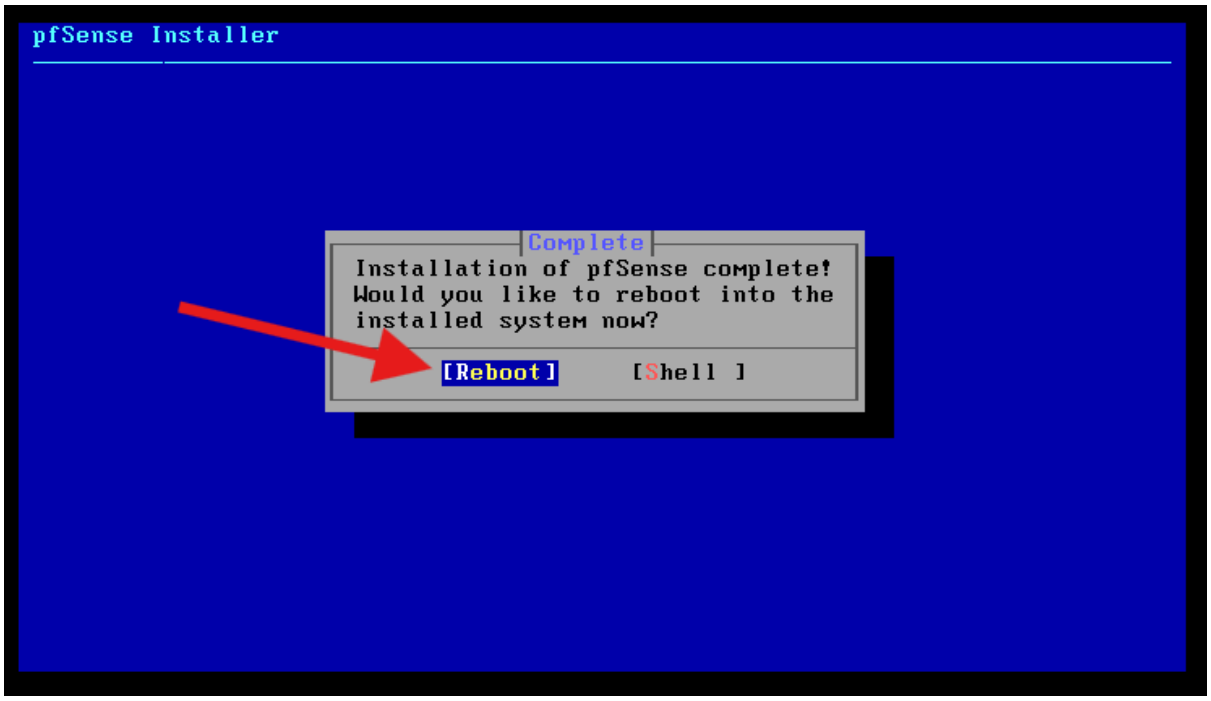
Cliquer sur OK pour valider.



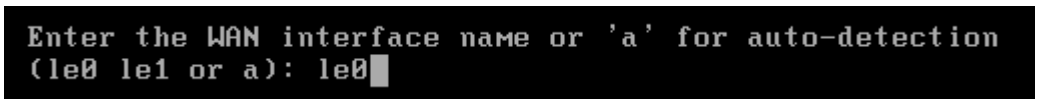
Attendre la fin du téléchargement.



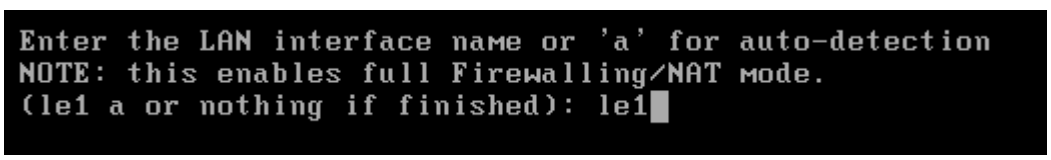
Cliquer sur Reboot pour redémarrer et finaliser l'installation. Attendre ensuite jusqu'à la prochaine étape.



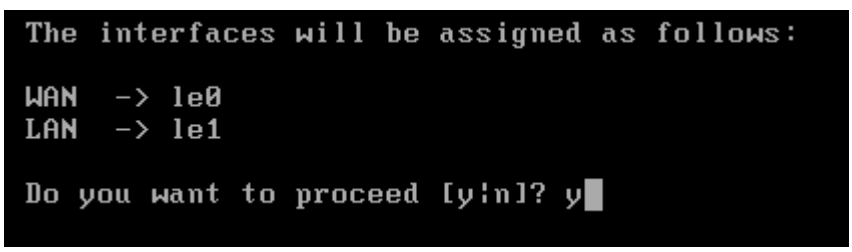
Choisir le0 pour configurer le WAN.



Choisir ensuite le1 pour l'interface LAN.

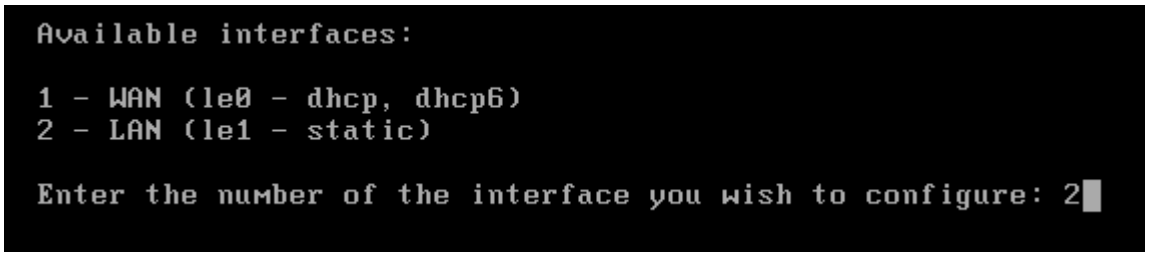


Valider en tapant y. Attendre ensuite la fin de la configuration.



Voici le menu de PfSense. Choisir 2 pour modifier les adresses IP des interfaces.

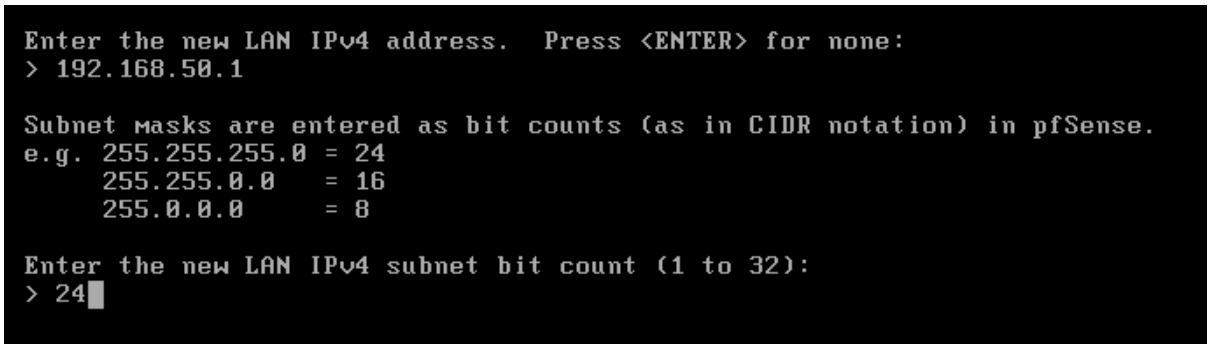
Sélectionner le LAN (2).


Available interfaces:
1 - WAN (le0 - dhcp, dhcp6)
2 - LAN (le1 - static)
Enter the number of the interface you wish to configure: 2

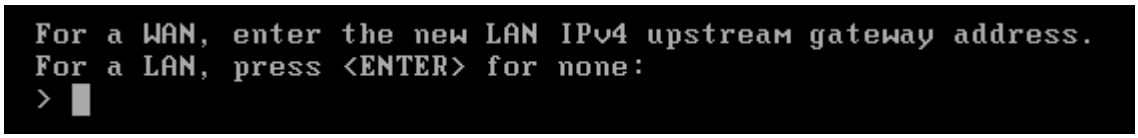
Choisir no.


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

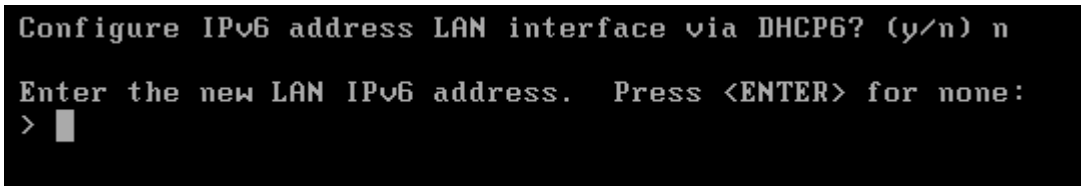
Entrer la nouvelle adresse LAN puis sélectionner le port 24.



Appuyer sur la touche enter.



Choisir no et appuyer sur enter à la prochaine étape.



Choisir no aux 2 prochaines étapes.

Appuyer sur enter pour valider tous les changements.

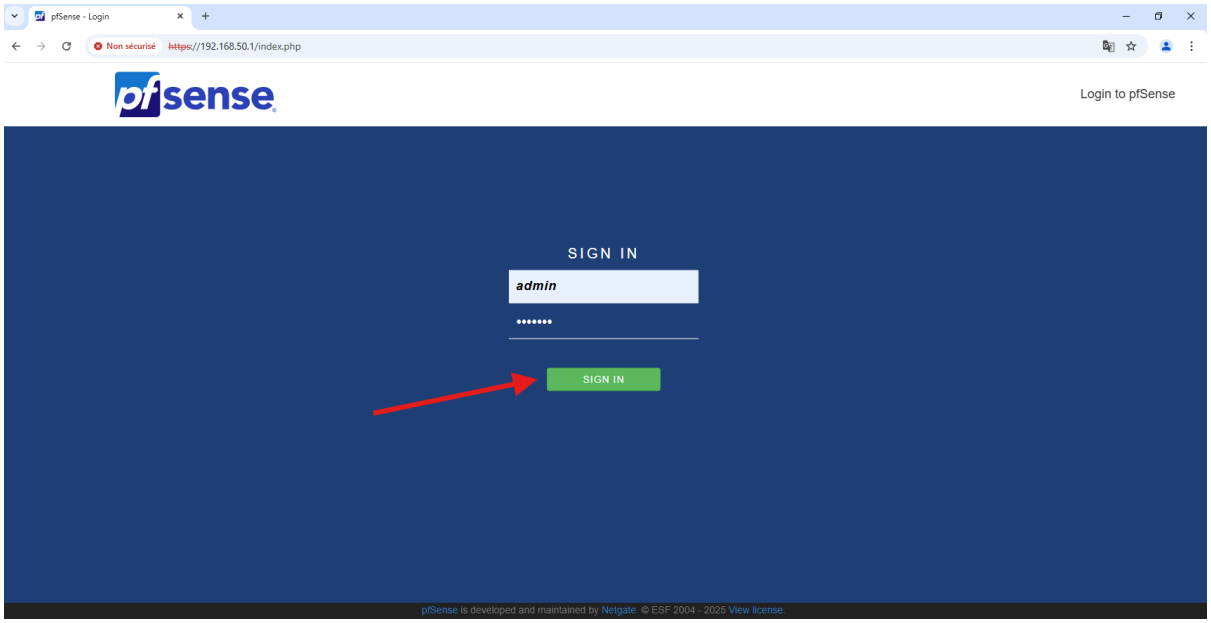
❗ IL FAUT REALISER LE MEME PROCESSUS POUR LE 2EME ROUTEUR EN REMPLACANT L'ADRESSE LAN PAR UNE AUTRE (ex : 192.168.50.2). ❗

2) Configuration des PfSense

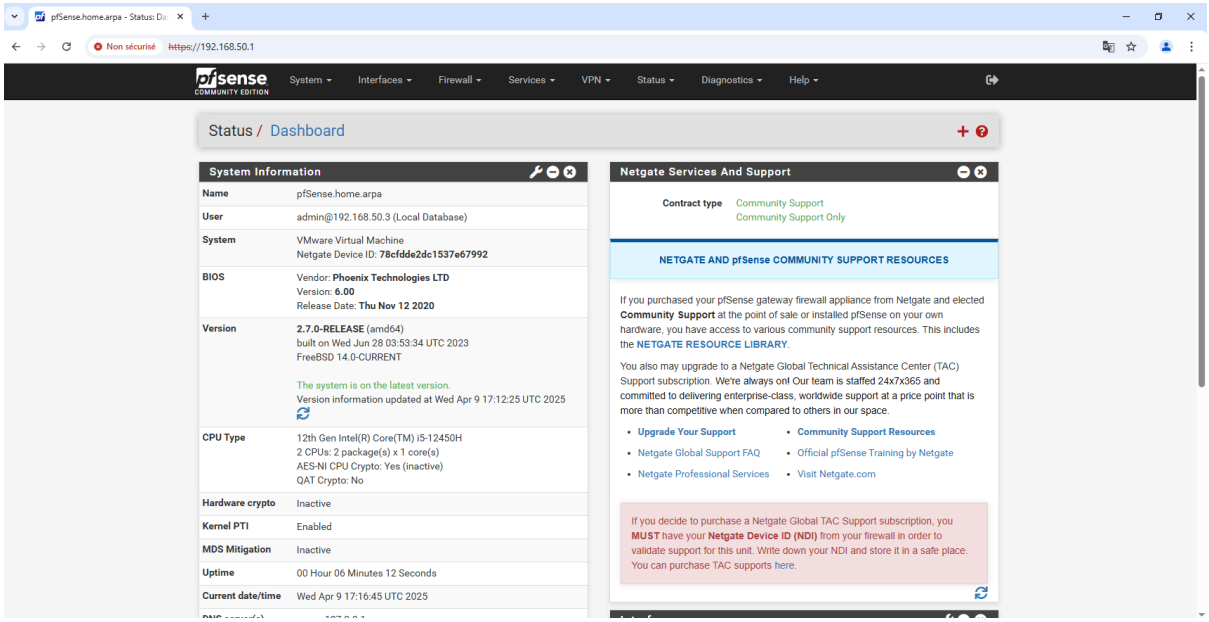
A) Première connexion + changement de mot de passe

Accéder maintenant à l'interface web du PfSense Master (192.168.50.1) via un navigateur sur un poste client.

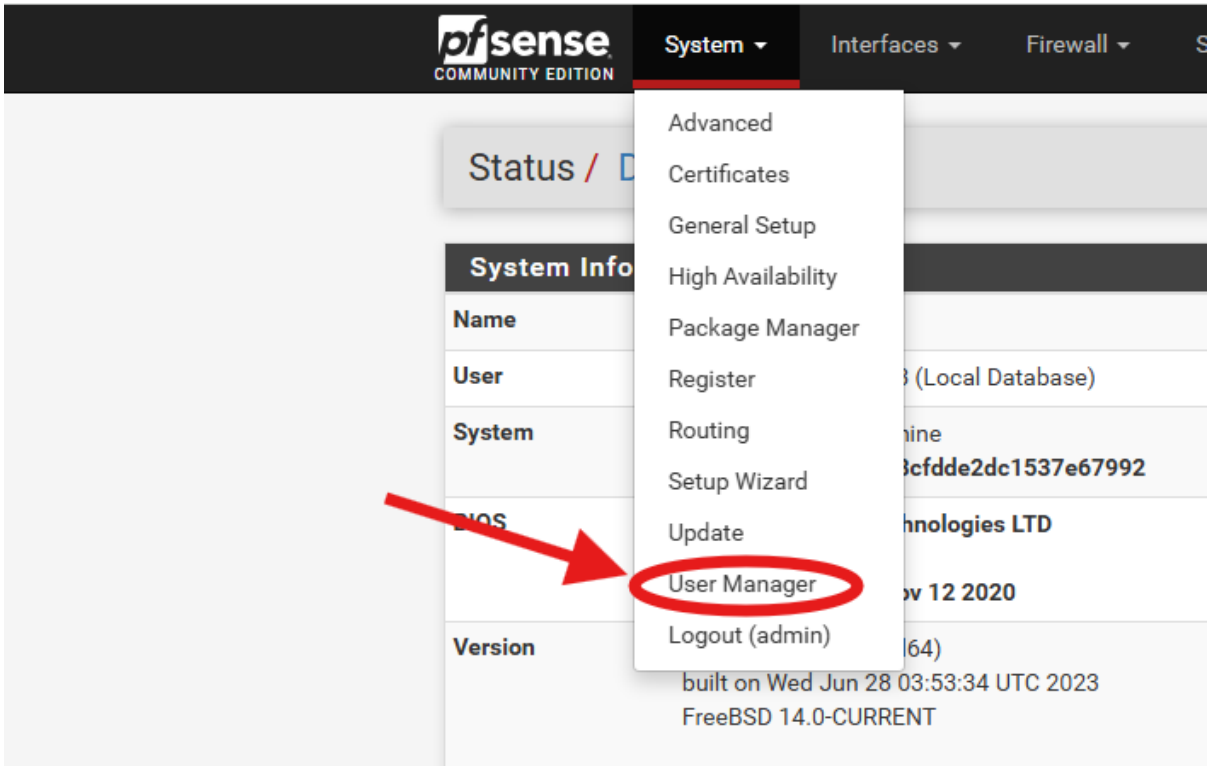
Rentrer l'identifiant "admin" avec le mot de passe de base "pfsense" puis cliquer sur sign in.



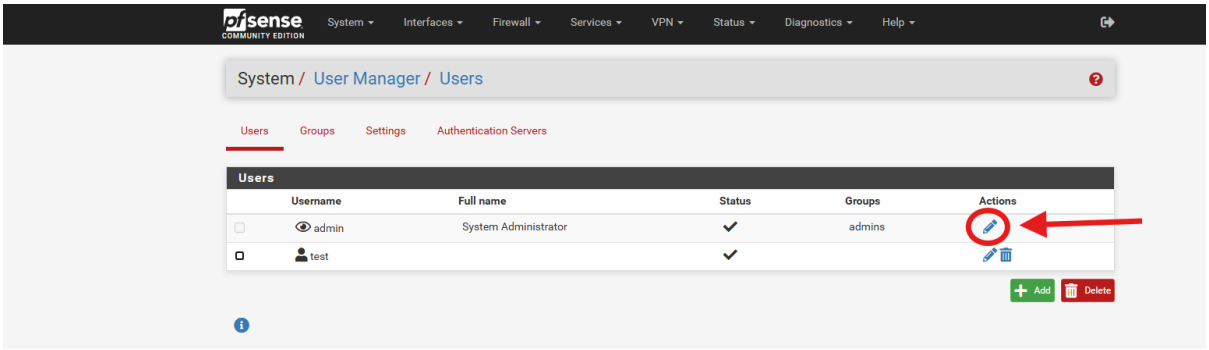
Voici la page d'accueil de PfSense. Nous allons maintenant changer le mot de passe de base pour accéder à PfSense en tant qu'admin.



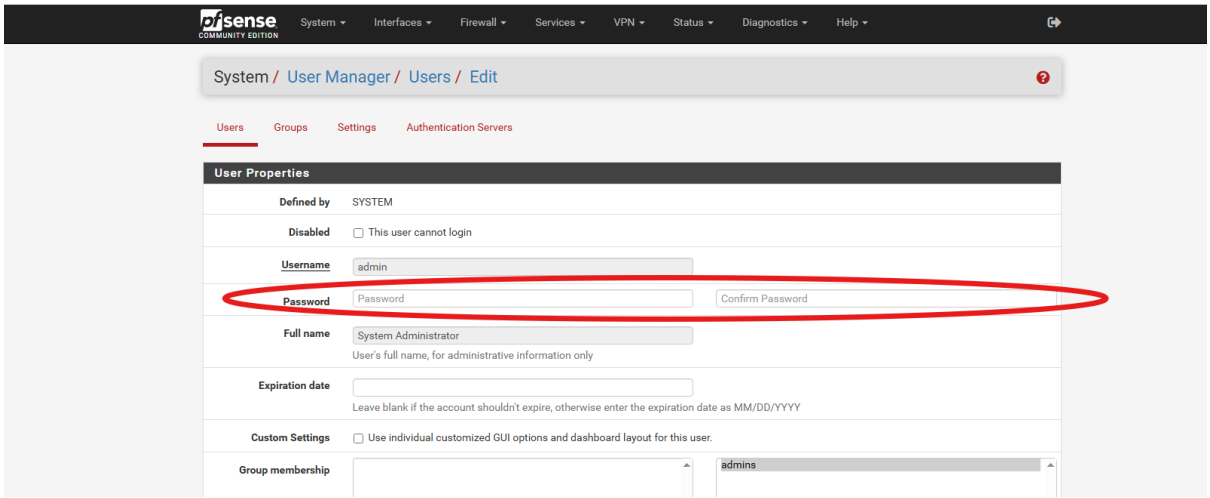
Aller dans System puis dans User Manager.



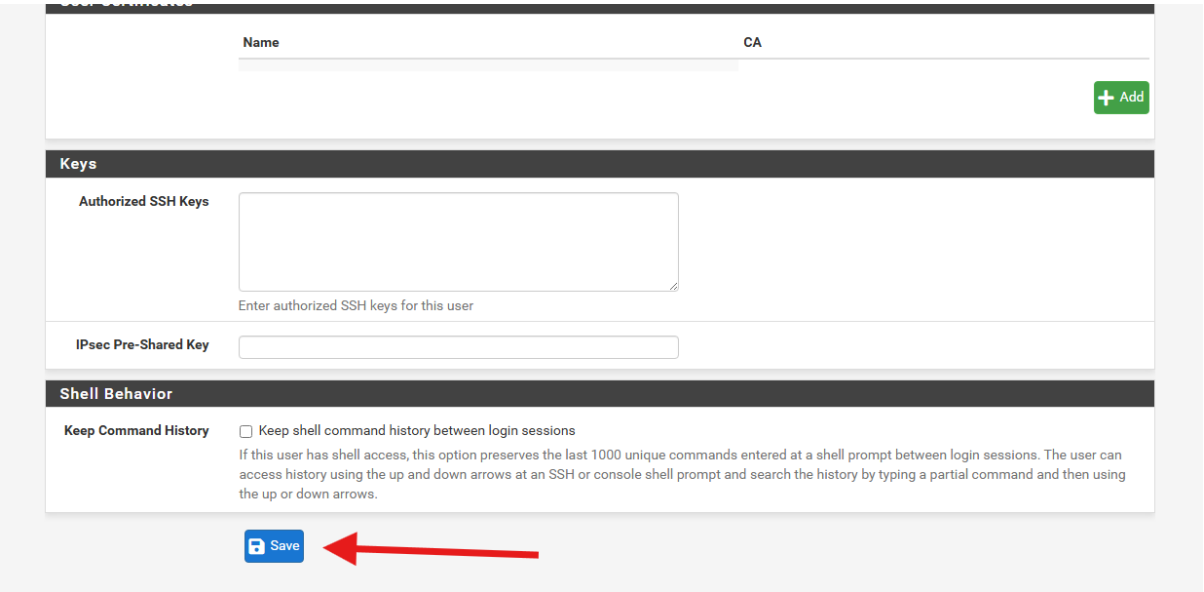
Cliquer sur l'icône du petit crayon pour accéder aux paramètres du compte admin de PfSense.



Entrer un nouveau mot de passe et confirmer le.



Descendre tout en bas de la page et cliquer sur Save.



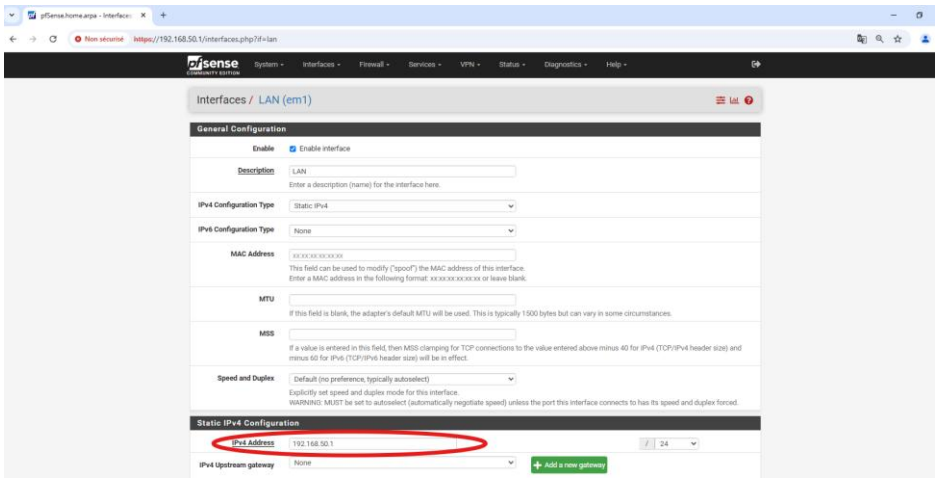
Une fois cette opération ayant été effectué, votre mot de passe a été changé.

❗ Cette opération est aussi à réaliser sur le deuxième PfSense en inscrivant le même mot de passe que sur le PfSense Master. ❗

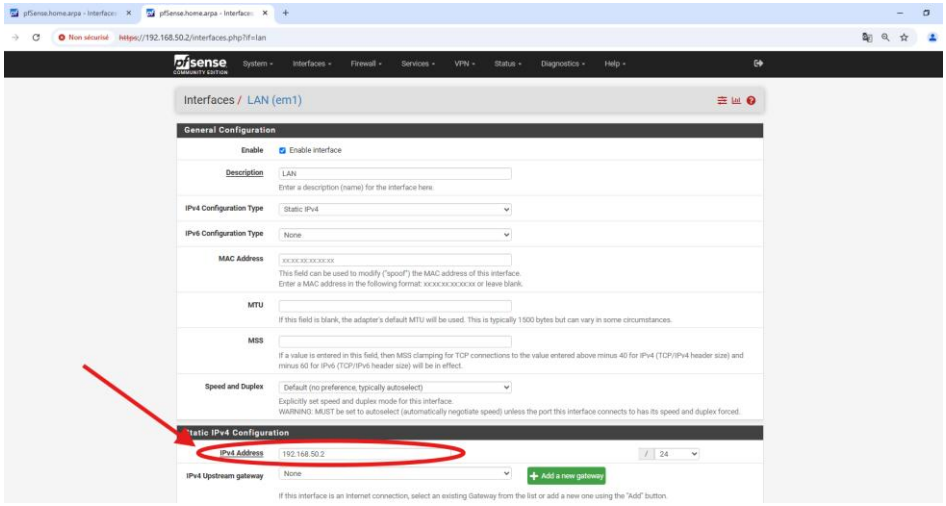
B) CARP LAN + High Availability

Avant de commencer cette étape, voici un rappel de la configuration des deux cartes LAN sur les 2 pfsense. On peut regarder ça en allant dans Interfaces, puis Assignements. Ensuite il faut cliquer sur em1 (LAN).

Voici la carte LAN sur le PfSense Master :



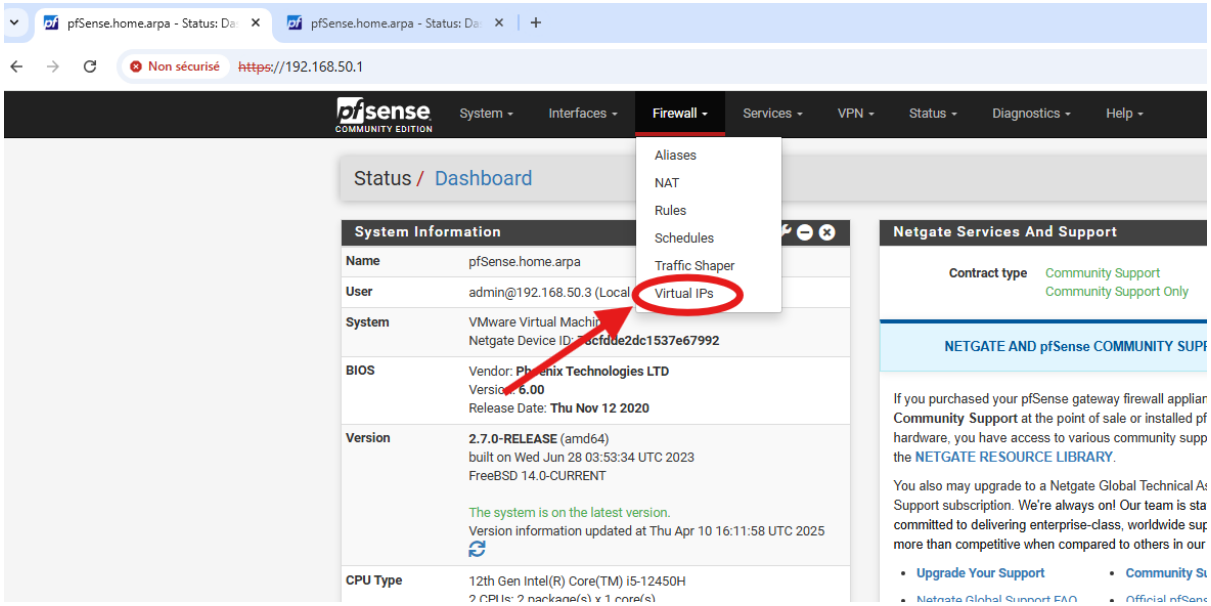
Voici la carte LAN sur le PfSense Backup :



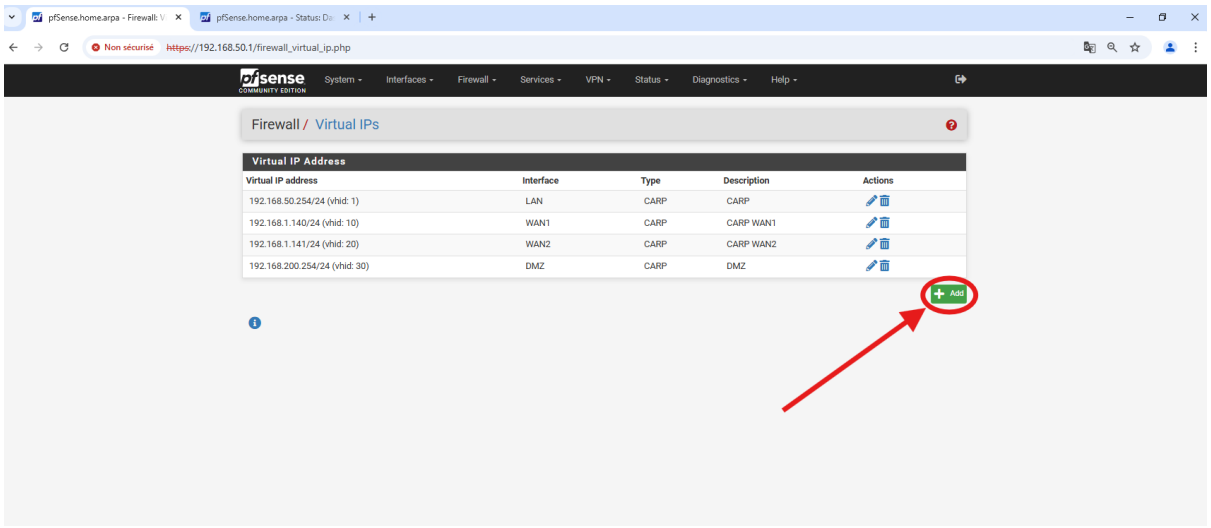
Ici, on peut voir que les deux cartes LAN sont sur la même plage d'adresse.

Pour créer notre CARP LAN, il faut d'abord configurer une IP virtuelle sur notre plage d'adresse.

Pour ce faire, aller dans Firewall puis Virtual IPs sur le PfSense Master.



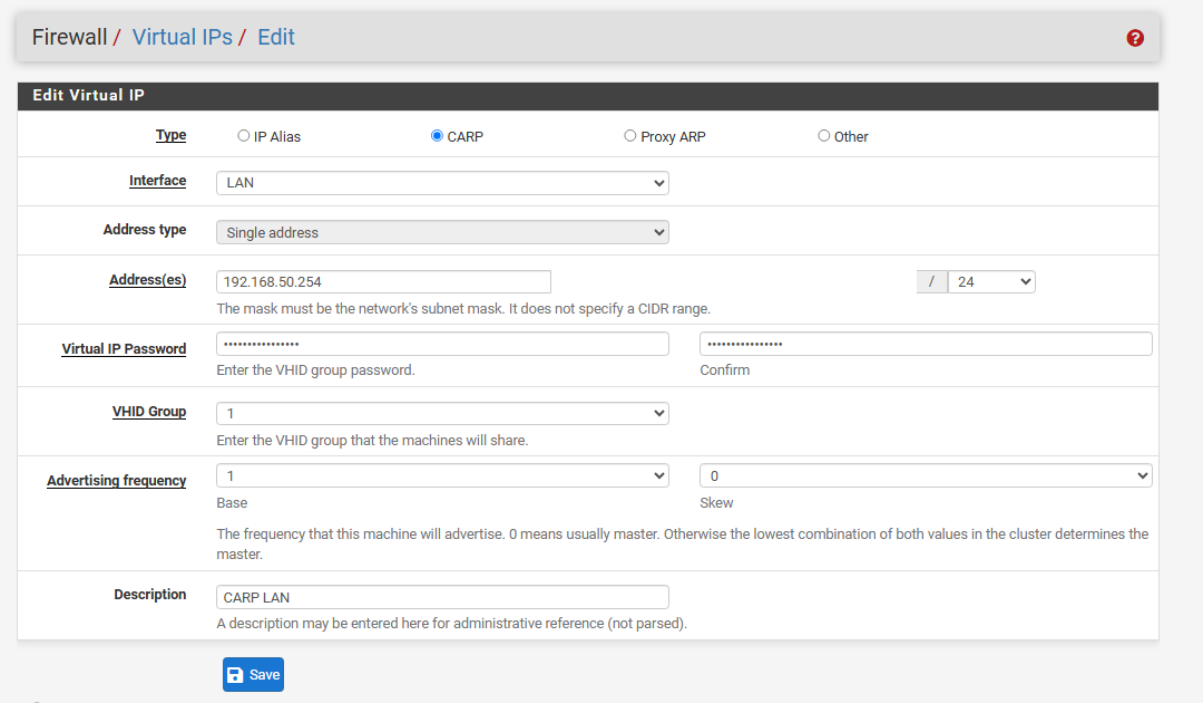
Cliquer sur le bouton ADD.



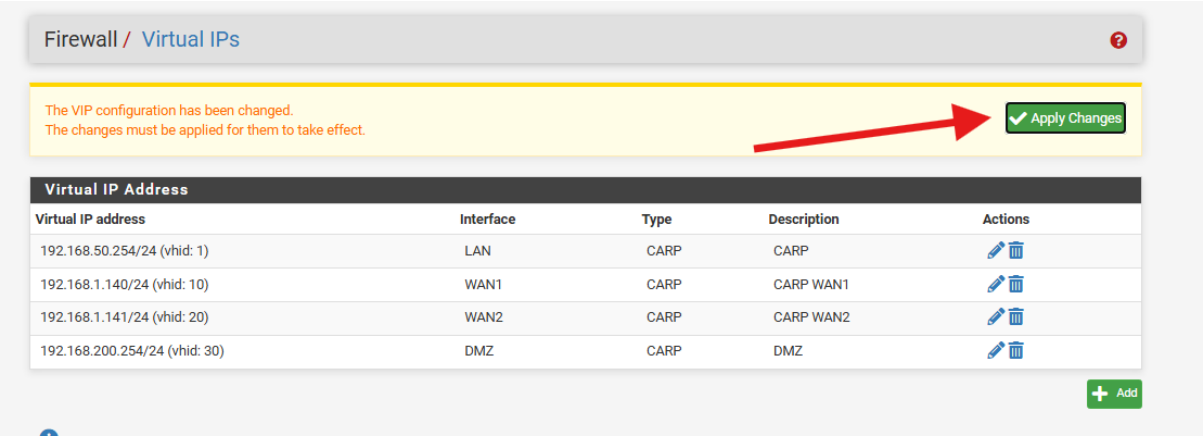
Voici, dans mon cas, les paramètres à entrer (à adapter en fonction de la plage d'adresse IP du LAN).

Une fois les paramètres remplis, cliquer sur Save.

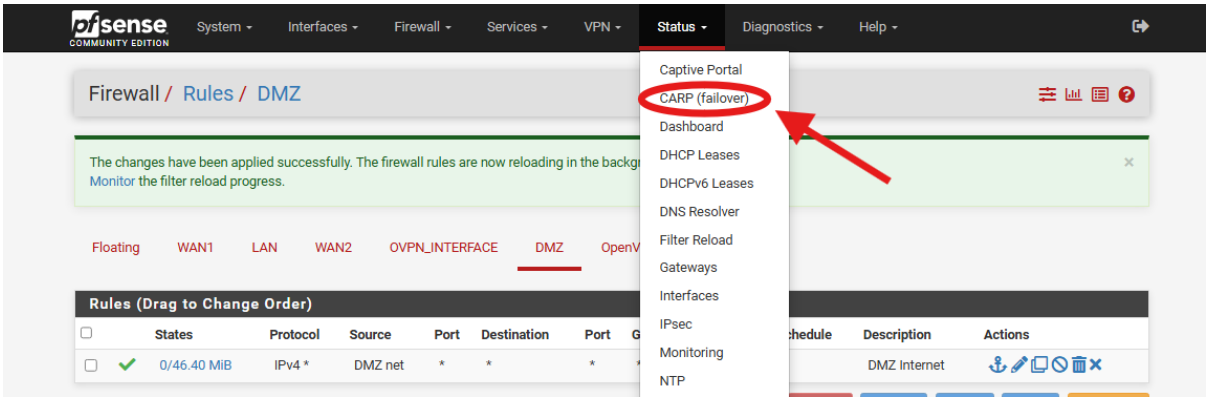
Cette opération est aussi à effectuer sur le PfSense Backup en remplaçant seulement Skew par 100 à la place de 0.



Cliquer ensuite sur Apply Changes pour appliquer les changements.

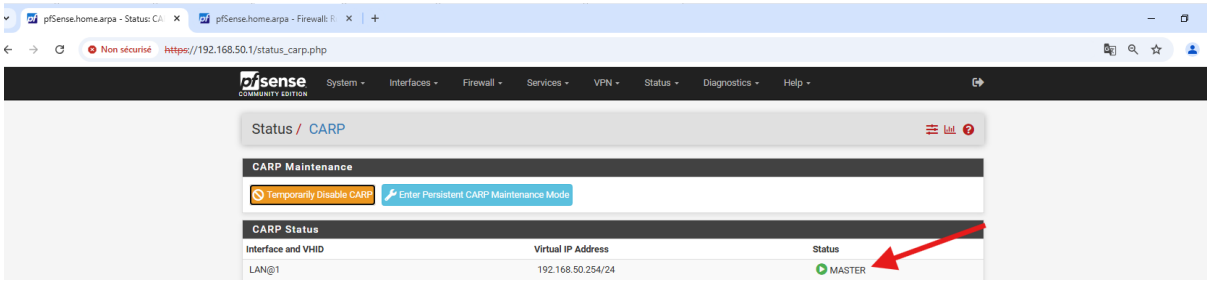


Aller ensuite dans Status puis CARP (failover).

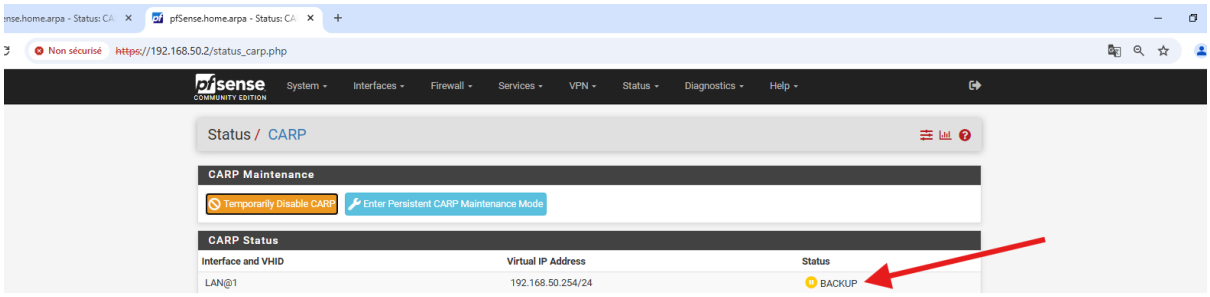


Si tout est normal, voici ce qui devrait s'afficher sur les deux PfSense.

- PfSense Master :

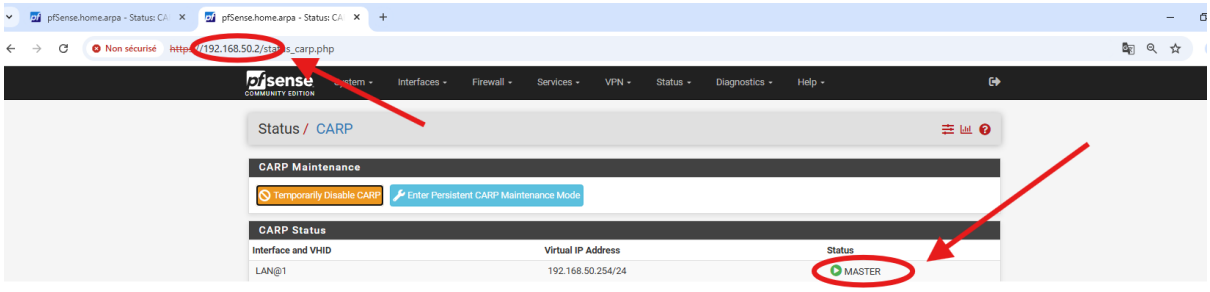


- PfSense Backup :



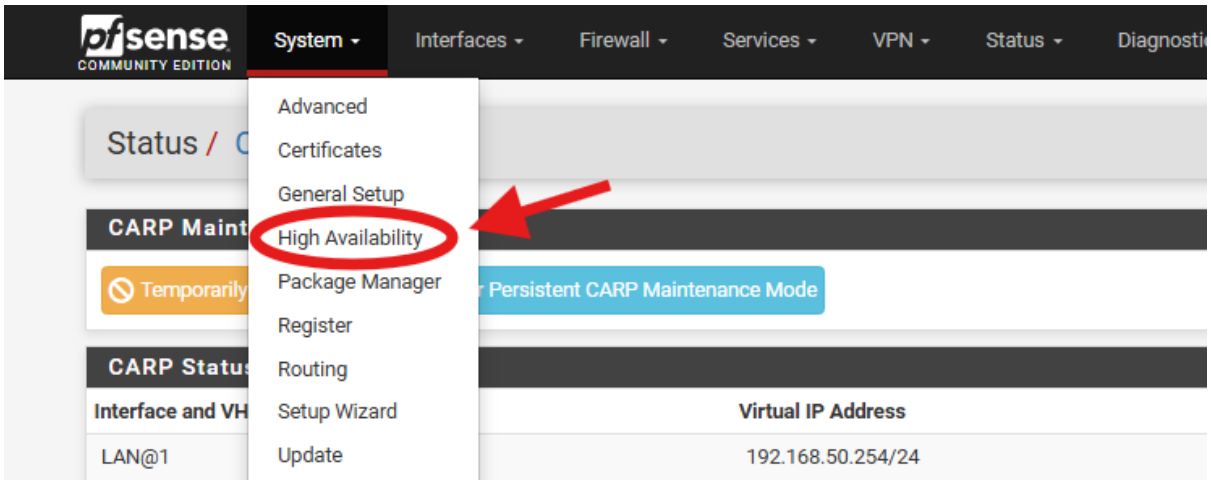
-> Explication : le routeur master (192.168.50.1) est pour l'instant actif. Si ce dernier tombe en panne, le routeur backup (192.168.50.2) prendra le relais en passant de backup à master.

Voici un exemple quand le routeur master est éteint.

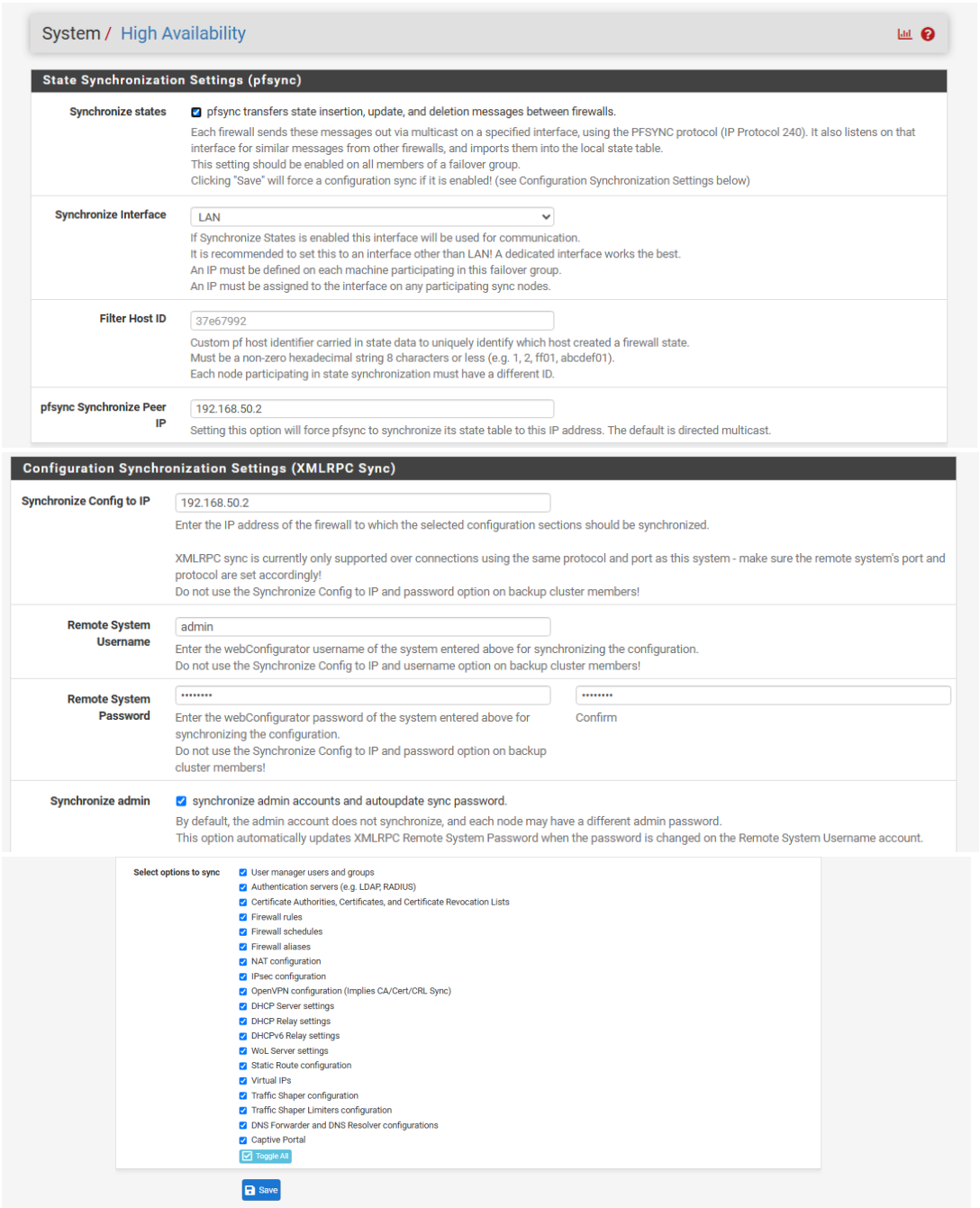


Passons maintenant à la configuration de la High Availability afin que les paramètres effectués sur le PfSense Master soit aussi appliqués sur le Backup.

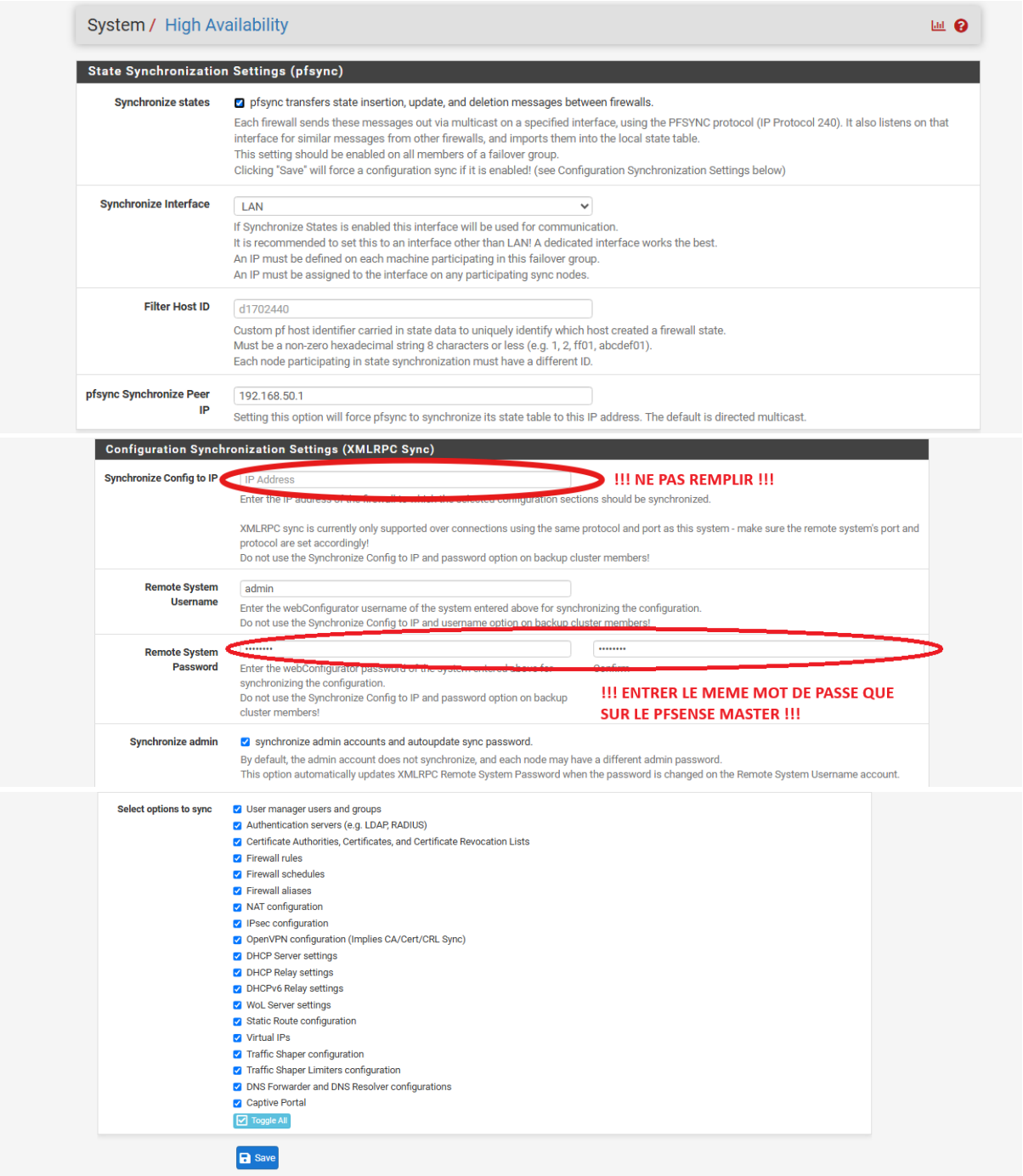
Aller dans System puis High Availability.



Voici les paramètres à rentrer dans le PfSense Master.



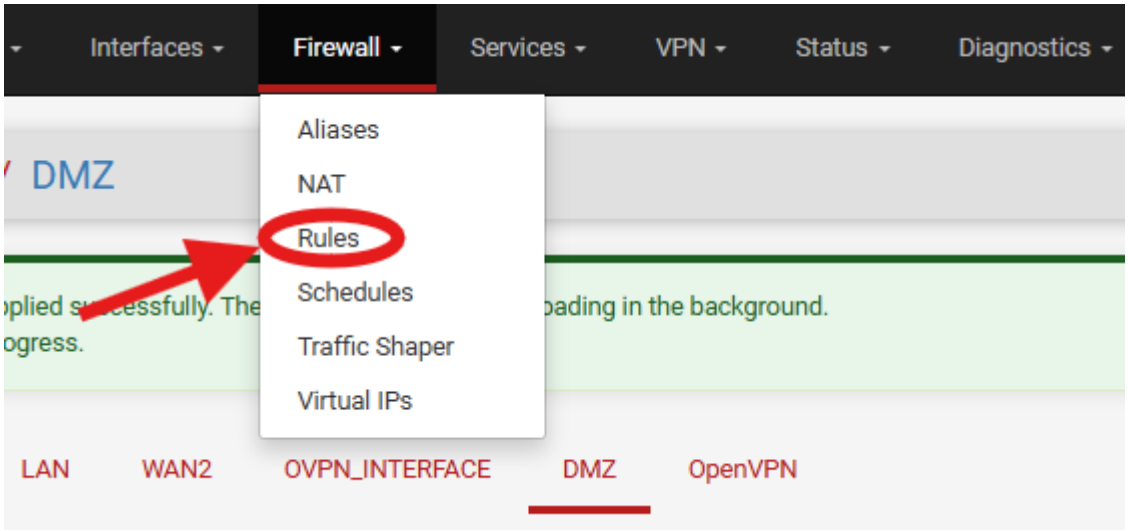
Voici les paramètres à rentrer dans le PfSense Backup.



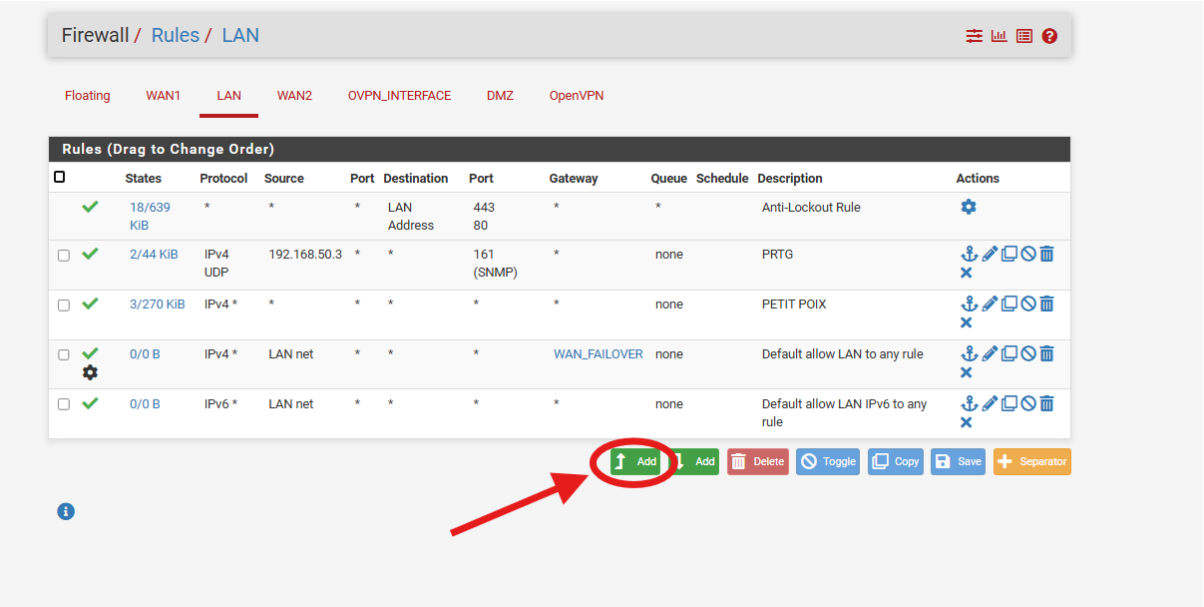
Cliquer sur Save pour valider les paramètres sur les deux PfSense. Une fois cela fait, les deux PfSense seront synchronisés.

Voici un test : Création d'une règle de pare-feu sur le PfSense Master qui va se répliquer sur le Backup.

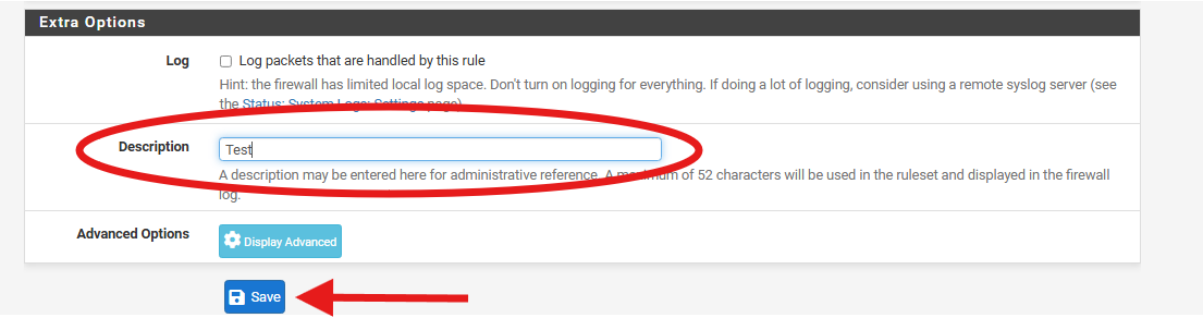
Dans le PfSense Master, aller dans Firewall puis Rules.



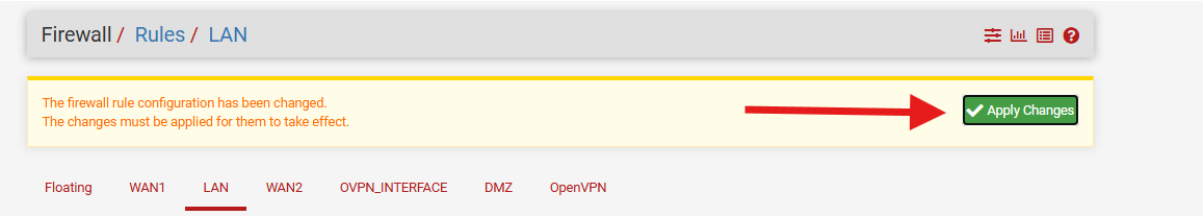
Cliquer sur Add pour ajouter une nouvelle règle (pour l'exemple, création d'une règle dans le LAN ici).



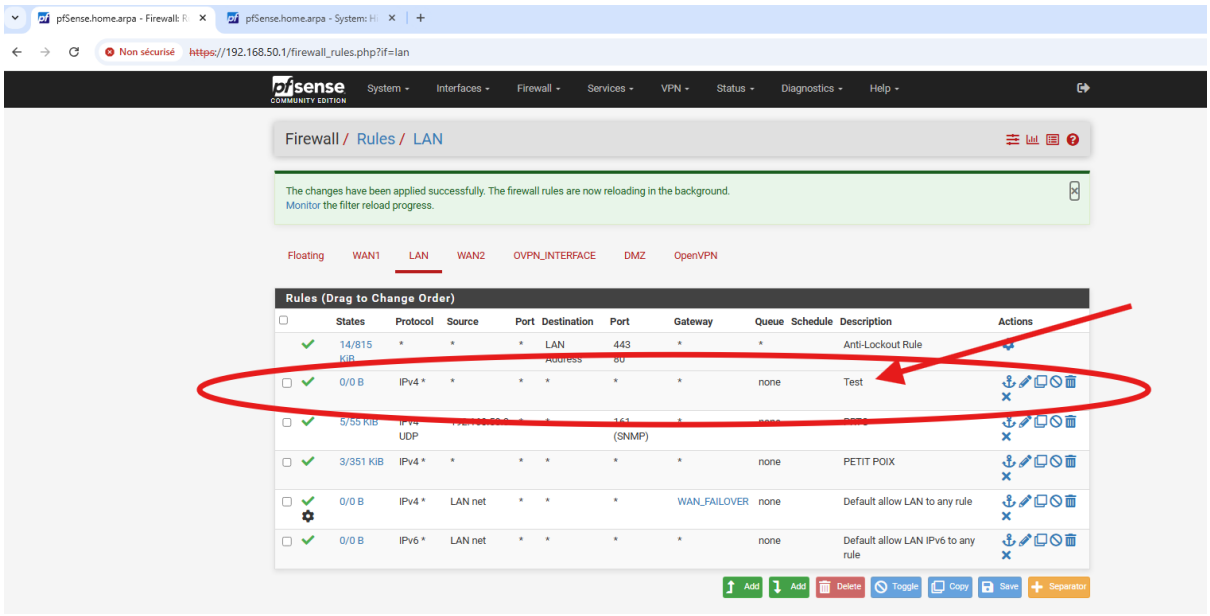
Descendre tout en bas, ajouter une description (Test dans l'exemple) et cliquer sur Save.



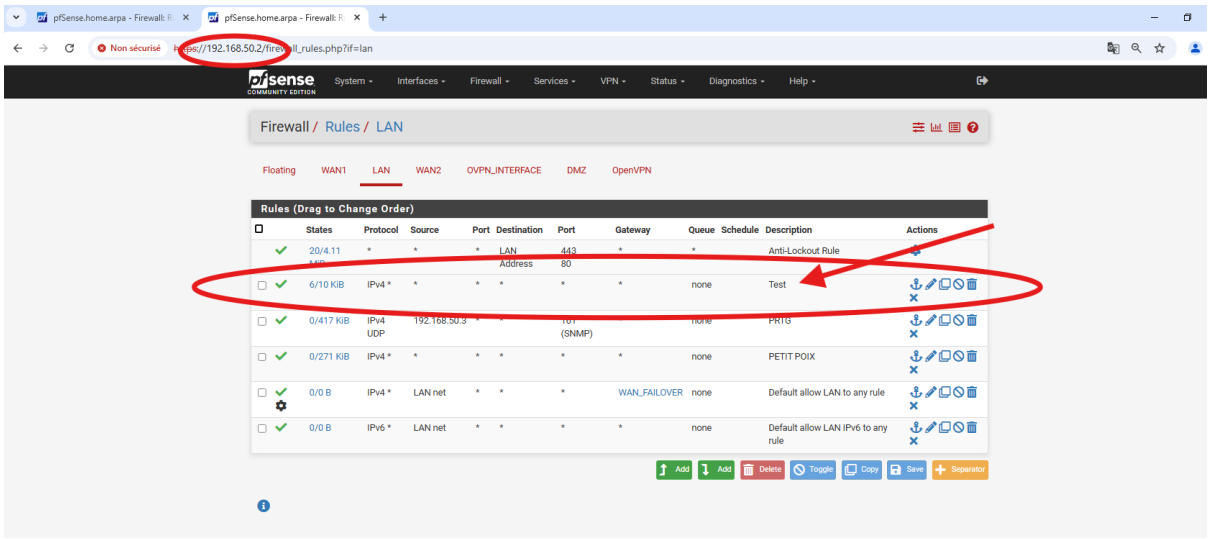
Cliquer sur Apply Changes.



La nouvelle règle “Test” apparaît dans la liste des règles sur le LAN.



Si tout fonctionne, la règle apparaît aussi sur le PfSense Backup.



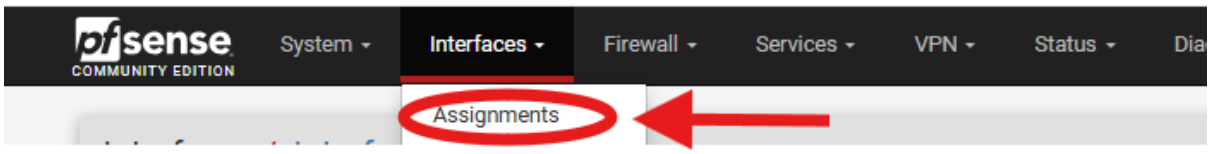
Vous pouvez ensuite supprimer la règle créée, c'était juste un exemple (elle va aussi se supprimer sur le PfSense Backup).

❗ ❗ Les règles appliquées sur le PfSense Master s'appliqueront aussi sur le Backup, mais cela ne marche pas inversement ! Seul le Pfsense Master peut influer sur le Backup. ❗ ❗

C) CARP WAN

Pour cette partie, chaque PfSense devra disposer chacun de deux cartes WAN distinctes sur la même plage d'adresse. Dans mon cas, cette plage sera en 192.168.1.0.

Aller dans Interfaces puis Assignements.

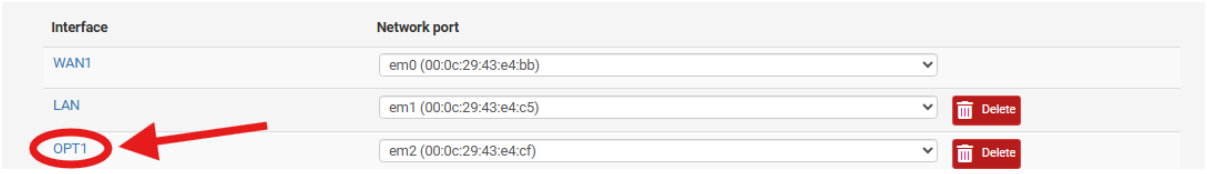


Ici, en ayant ajouté une troisième carte réseau sur le PfSense Master avec les mêmes propriétés que celle déjà existante en WAN, nous pouvons voir que em2 est disponible à la configuration (il reste un assignement réseau à ajouter grâce à l'ajout de notre nouvelle carte réseau). Cet assignement sera le 2ème WAN.

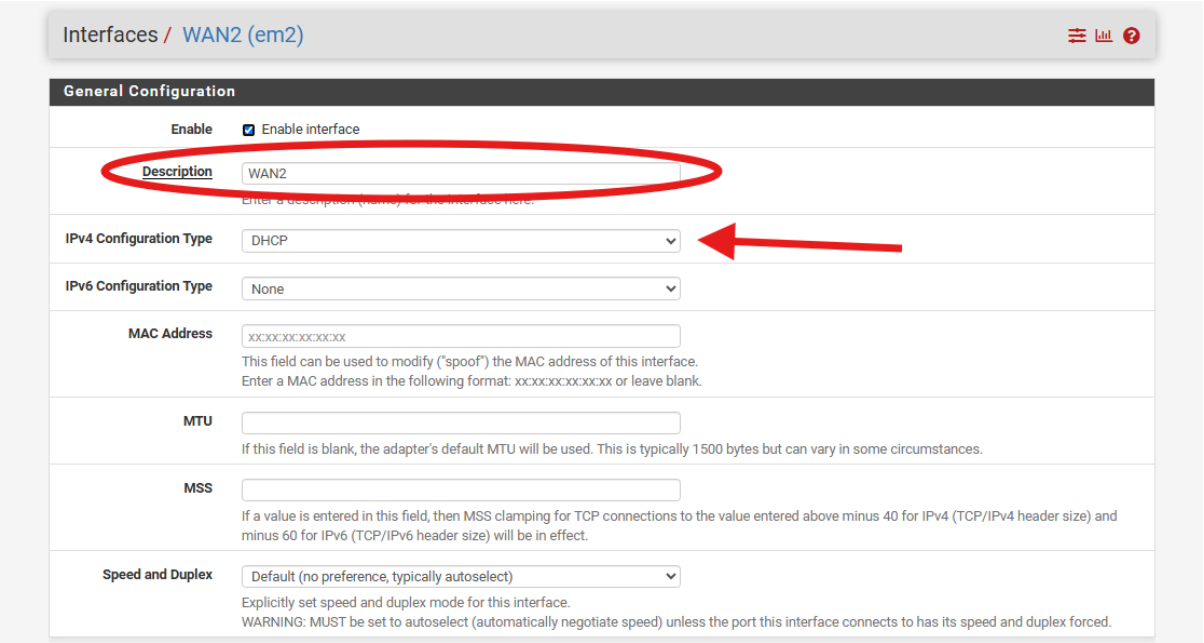
Cliquer sur Add.

Une fois après avoir créé une nouvelle interface, celle-ci s'est automatiquement renommée en "OPT1".

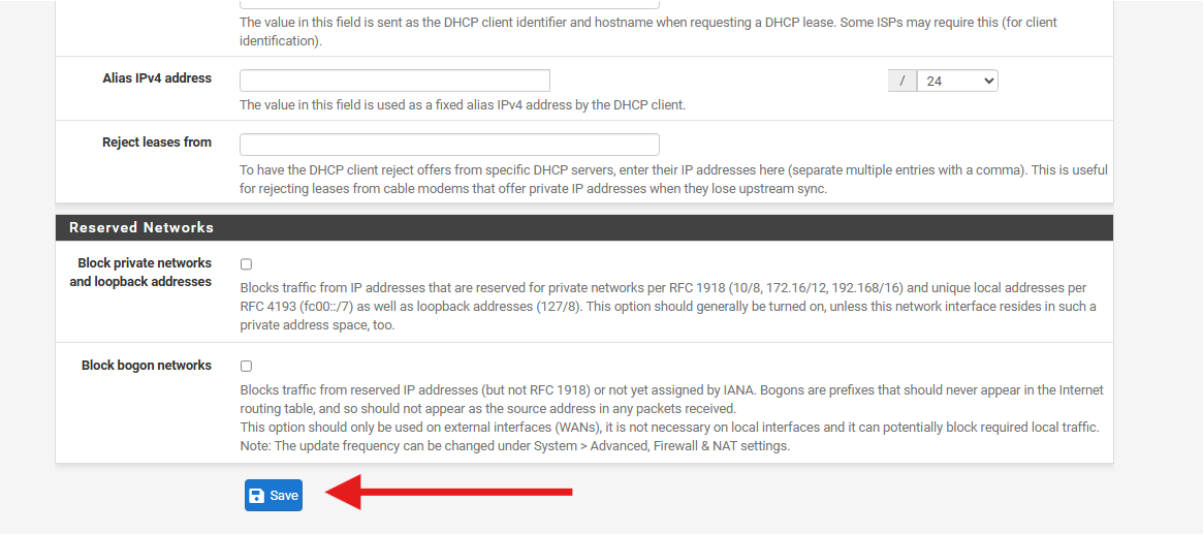
Cliquer dessus pour modifier ses paramètres.



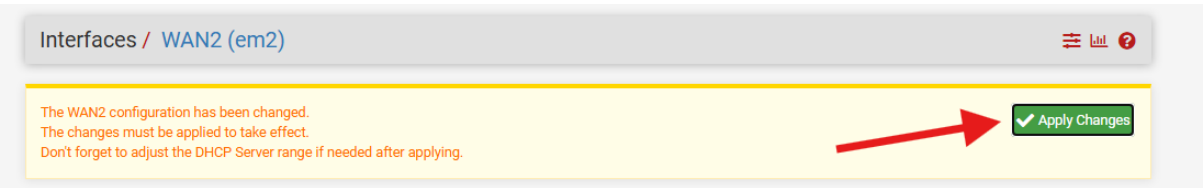
Cocher “Enable Interface”, renommer l’interface en “WAN2”, et changer la configuration IPv4 en DHCP (ou statique, même si l’adresse fourni en DHCP via PfSense ne changera jamais).



Descendre tout en bas et cliquer sur Save pour appliquer les changements sur l'interface.

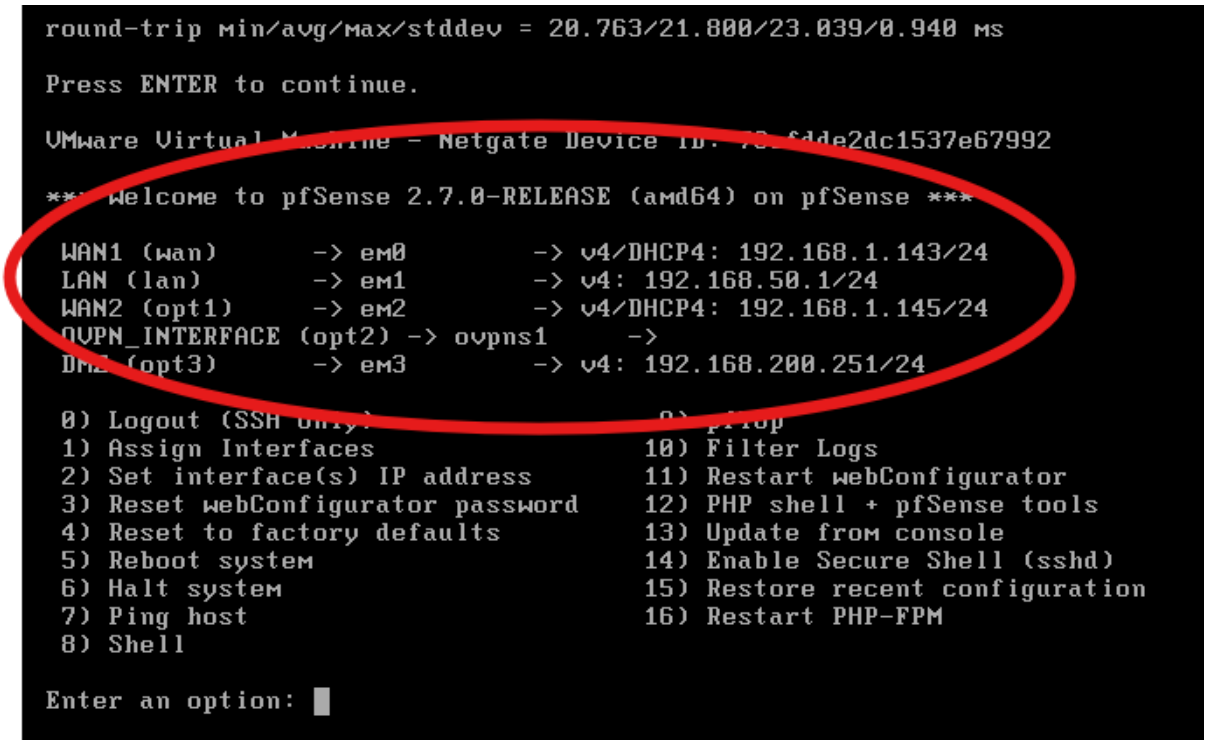


Cliquer sur Apply Changes.



Voici la configuration qui apparaît sur le menu du routeur PfSense Master.

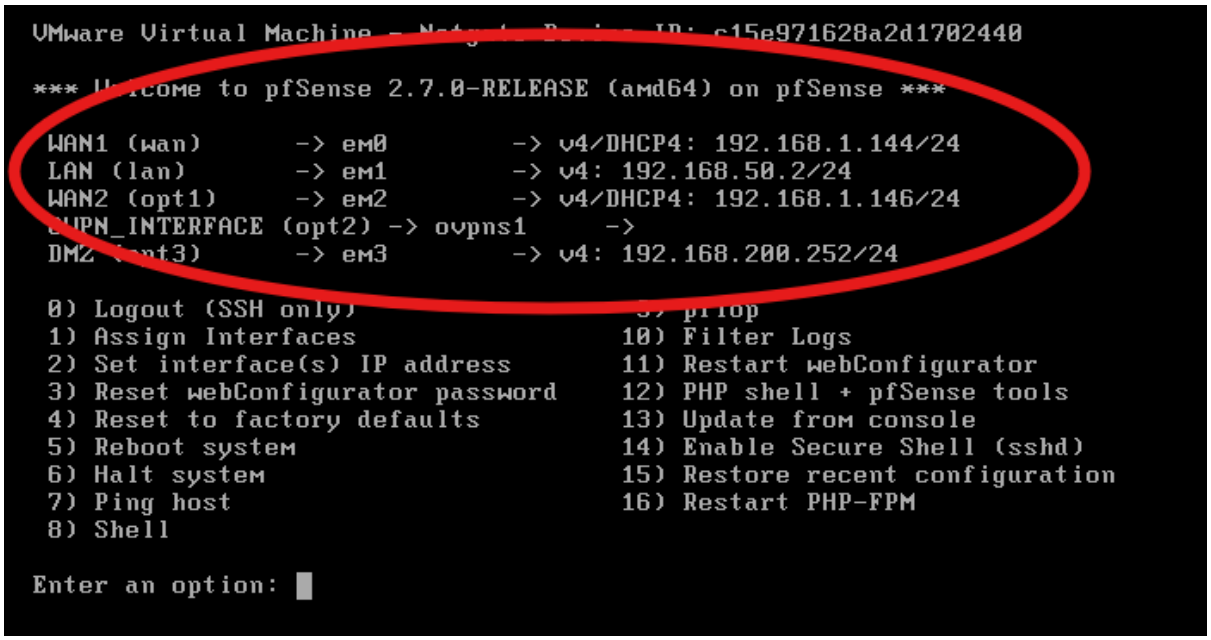
- WAN1 : 192.168.1.143
- WAN2 : 192.168.1.145



Répéter le même processus sur le routeur Backup.

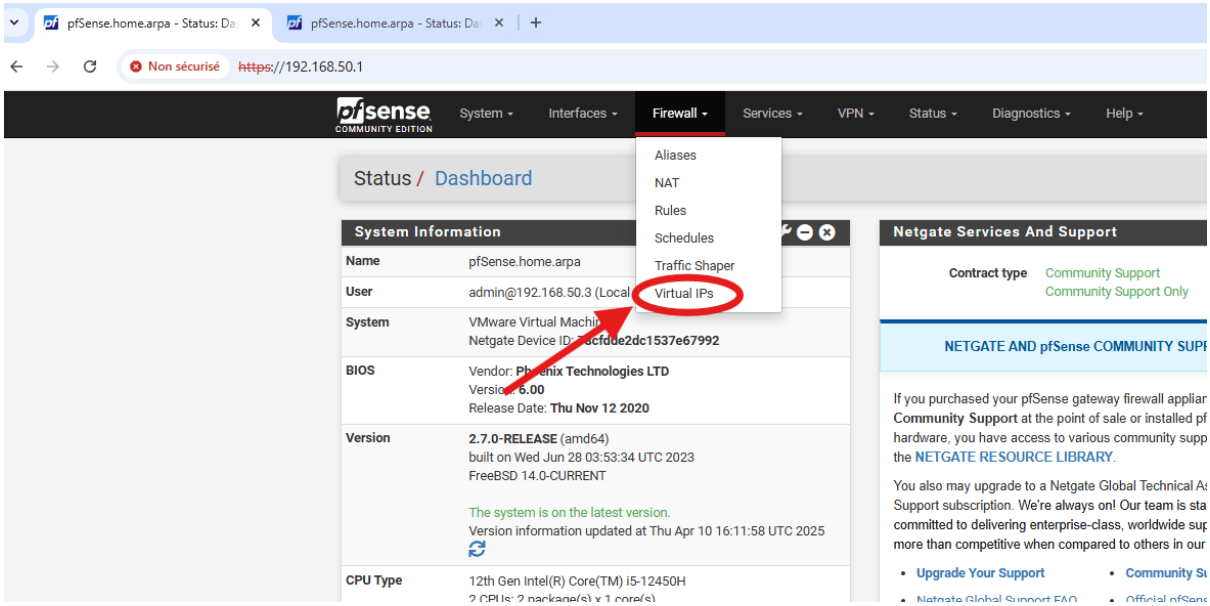
Voici la configuration qui apparaît sur le menu du routeur PfSense Backup.

- WAN1 : 192.168.1.144
- WAN2 : 192.168.1.146

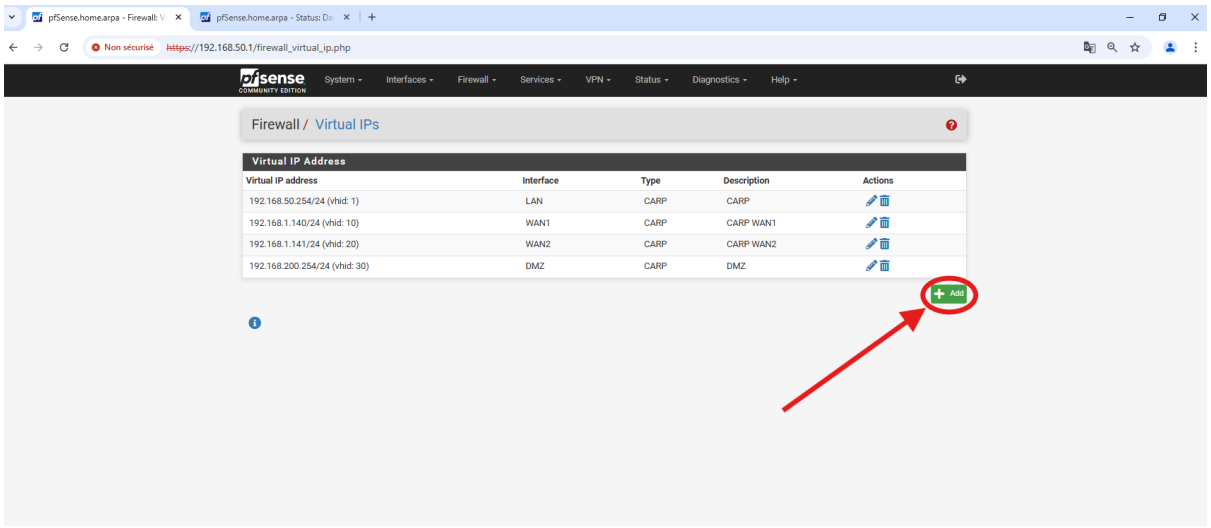


Nous allons maintenant créer 2 nouvelles IP virtuelles pour nos 2 CARP WAN.

Sur le PfSense Master, aller dans Firewall puis Virtual IPs.



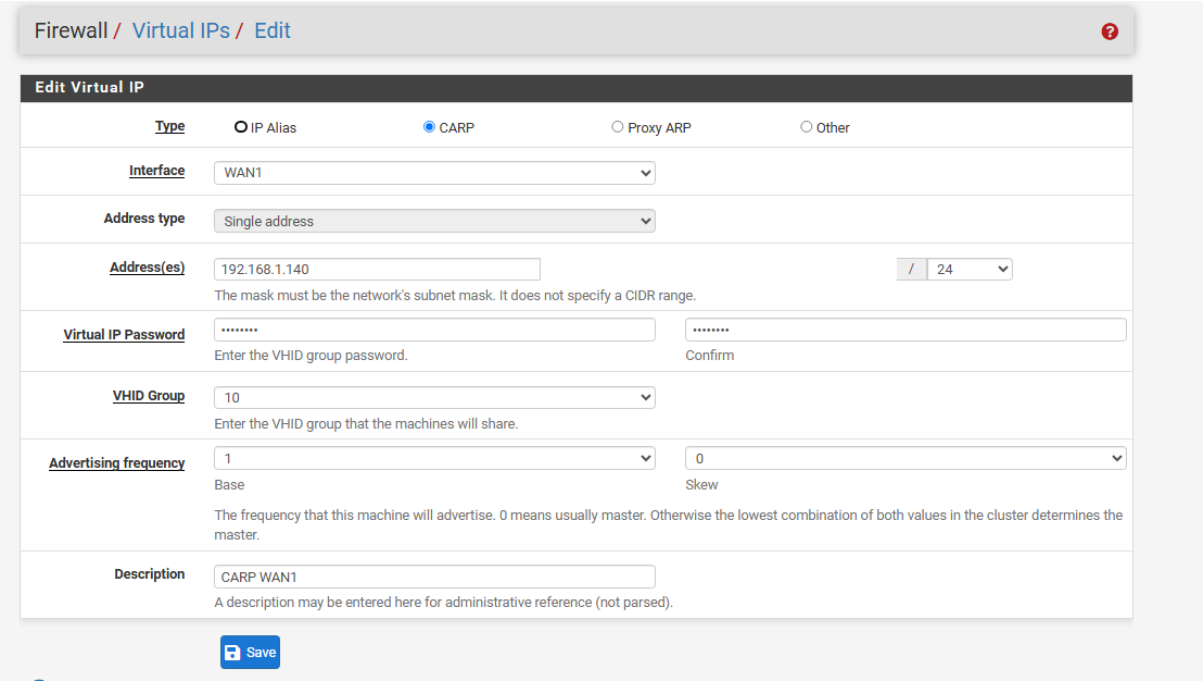
Cliquer sur le bouton Add.



Voici, dans mon cas, les paramètres à entrer (à adapter en fonction de la plage d'adresse IP du WAN).

Il ne faut pas remettre le même VHID Group sur l'IP virtuelle LAN (j'ai mis 10 ici).

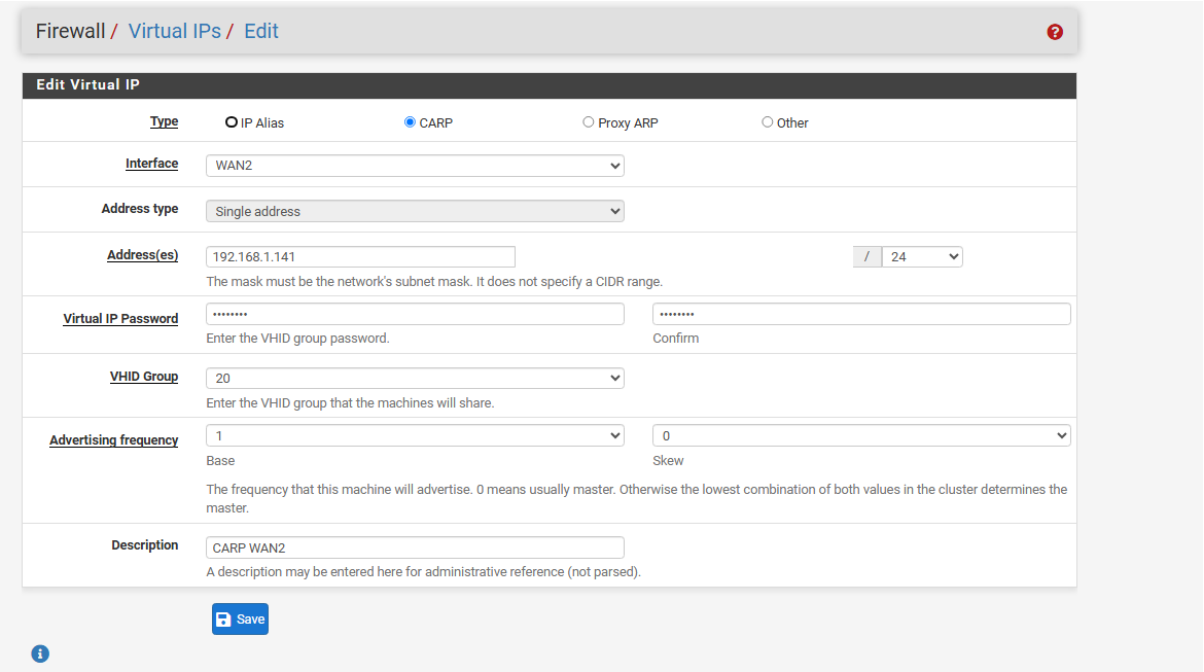
Une fois les paramètres remplis, cliquer sur Save.



Refaire la manipulation en créant une nouvelle IP virtuelle pour les 2ème WAN, tout en inscrivant un autre VHID Group comme pour le première IP virtuelle WAN (j'ai mis 20 ici).

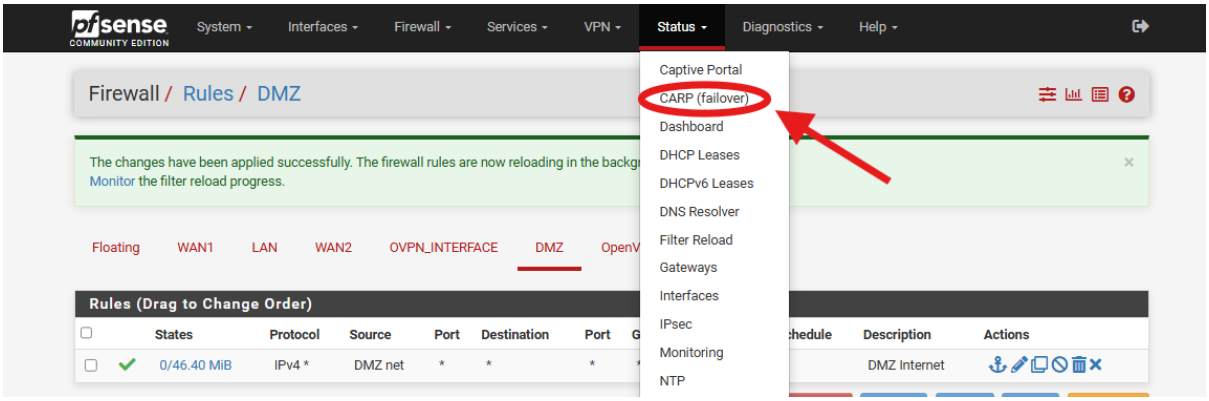
Voici, dans mon cas, les paramètres à entrer.

Une fois les paramètres remplis, cliquer sur Save.

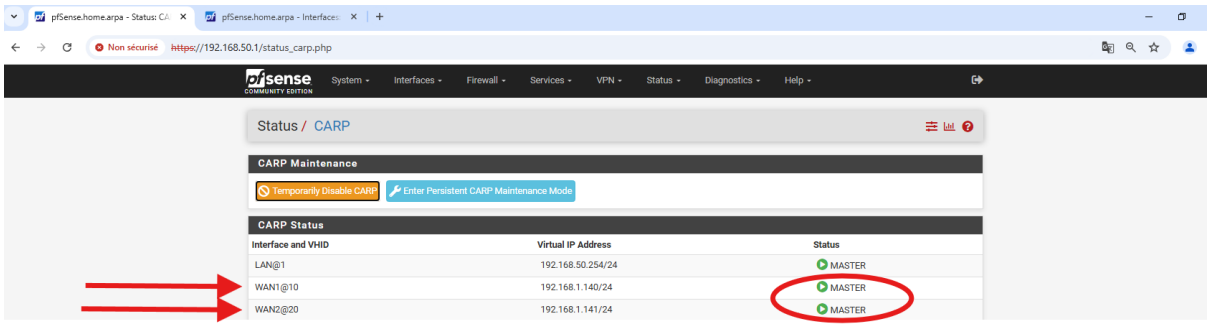


Cette opération n'est pas a effectué sur le Backup, grâce au High Availability, les paramètres se sont déjà répliqués.

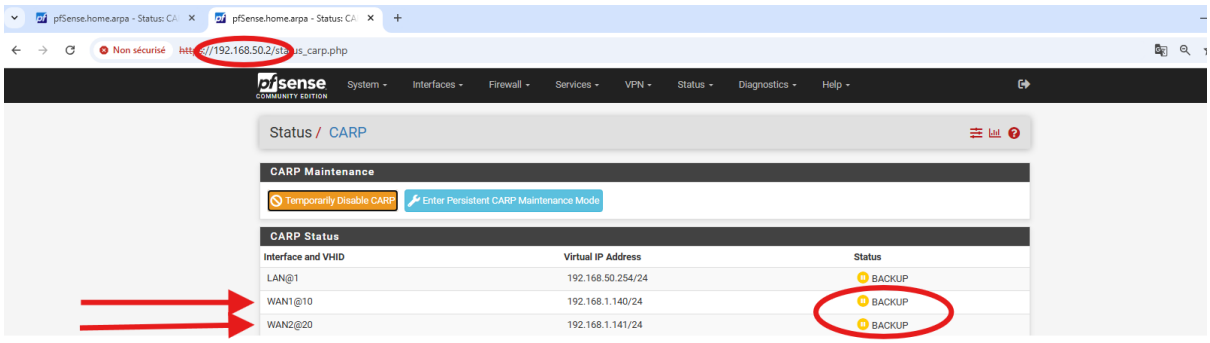
Sur le PfSense Master, retourner ensuite dans Status puis CARP (failover).



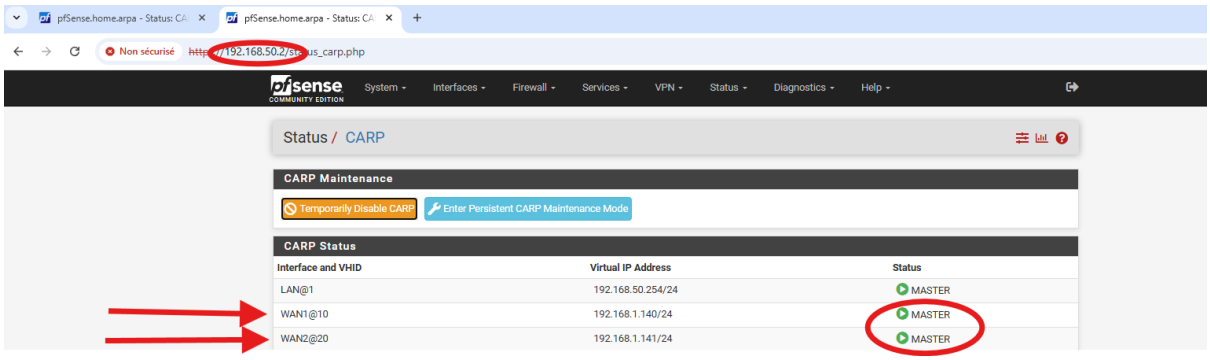
Les 2 CARP WAN sont bien présents en MASTER sur le PfSense Master.



Sur le PfSense Backup, les CARP WAN sont aussi présents mais en Backup.

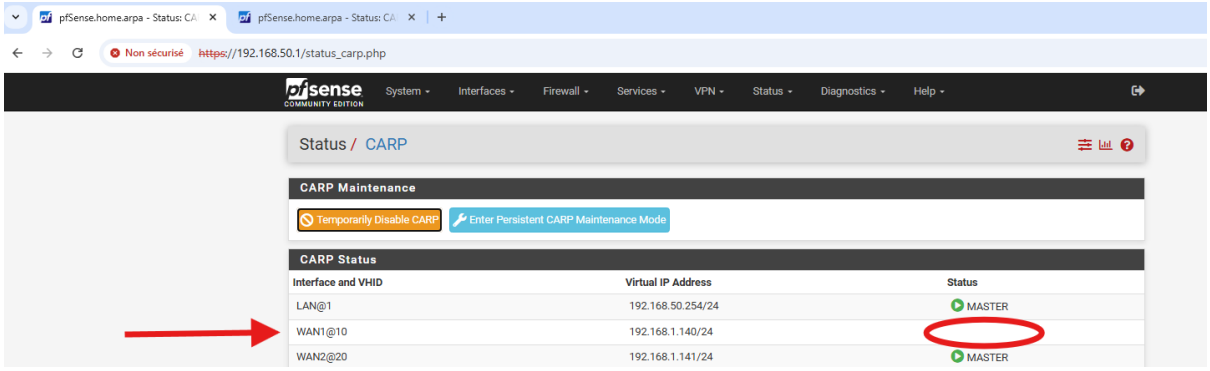


Si le routeur Master est en panne, le routeur Backup prend bien le relais.

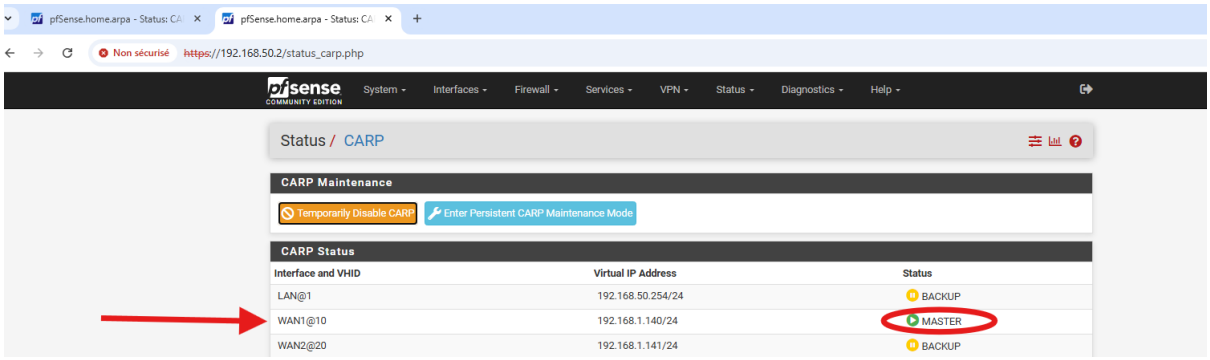


De même si l'on désactive une interface sur le PfSente Master (WAN1 ici), dans CARP (failover) WAN1 sera bien évidemment inactif sur le PfSense Master, et le WAN1 sur le PfSense Backup passera en MASTER.

- PfSense Master :



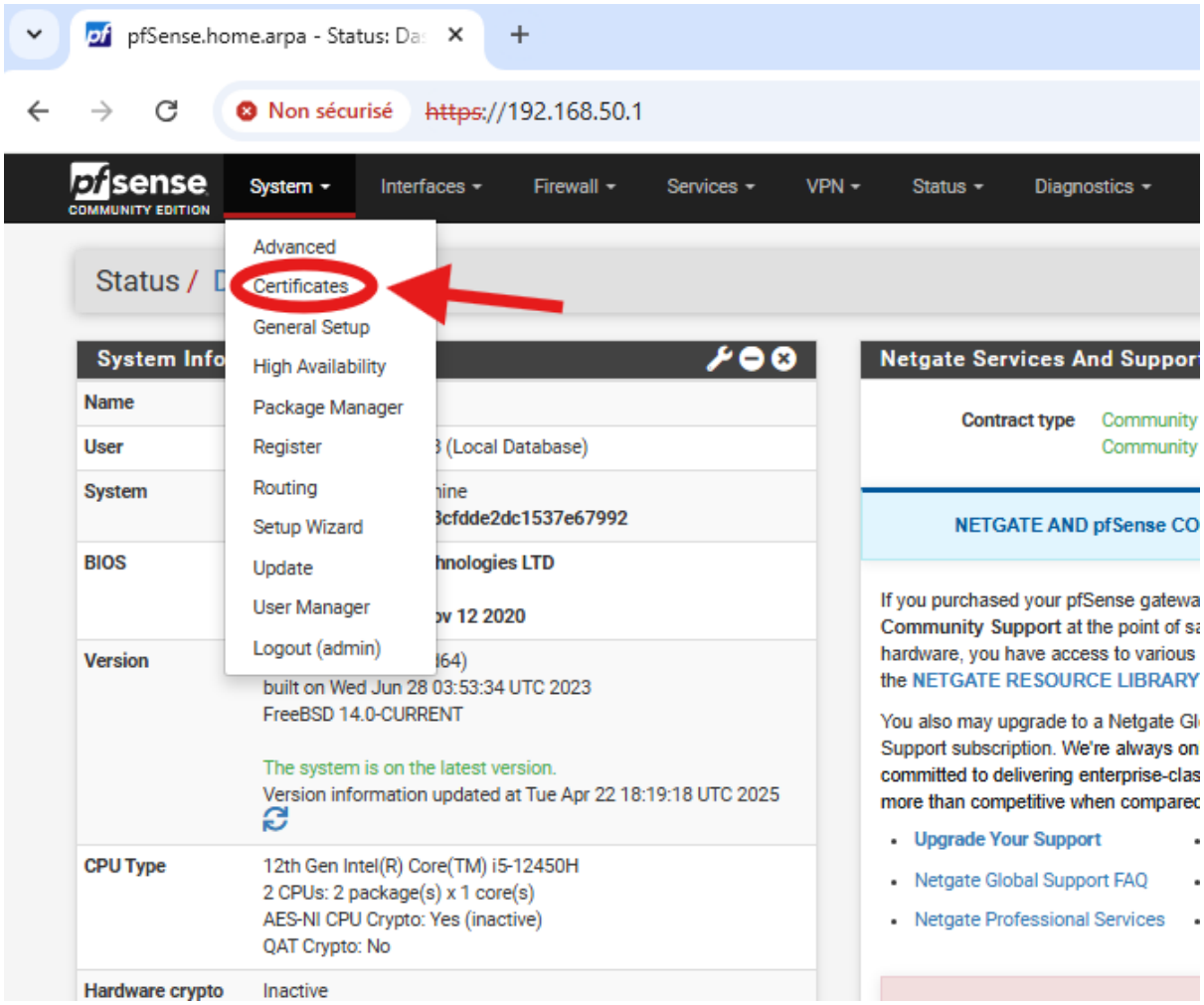
- PfSense Backup :



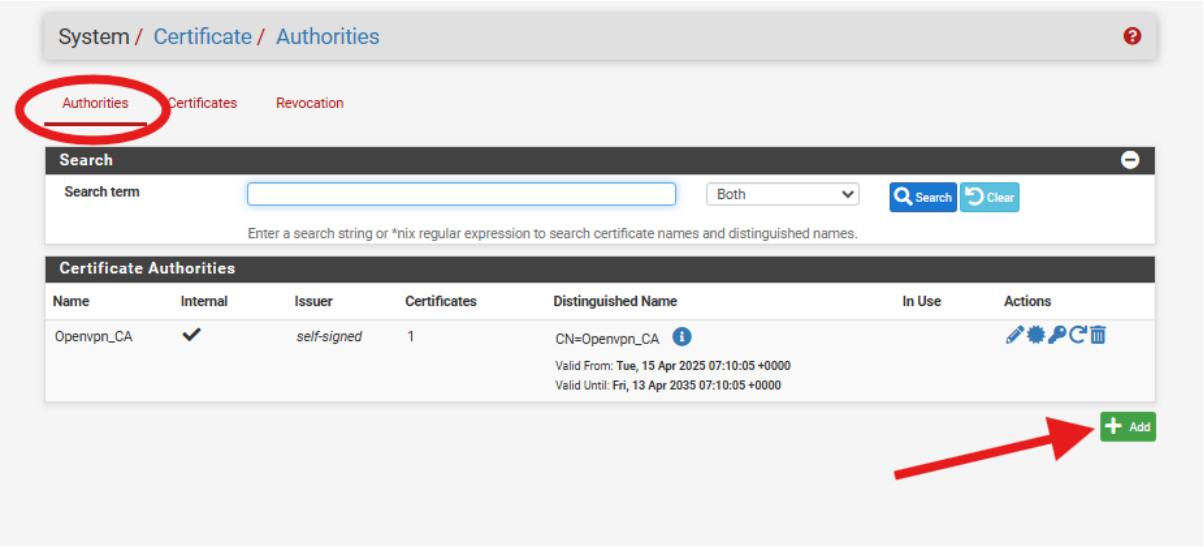
3) OpenVPN RW

❗ ❗ Cette partie est à réaliser seulement après avoir configurer ADDS sur le serveur Windows (voir doc associé) ❗ ❗

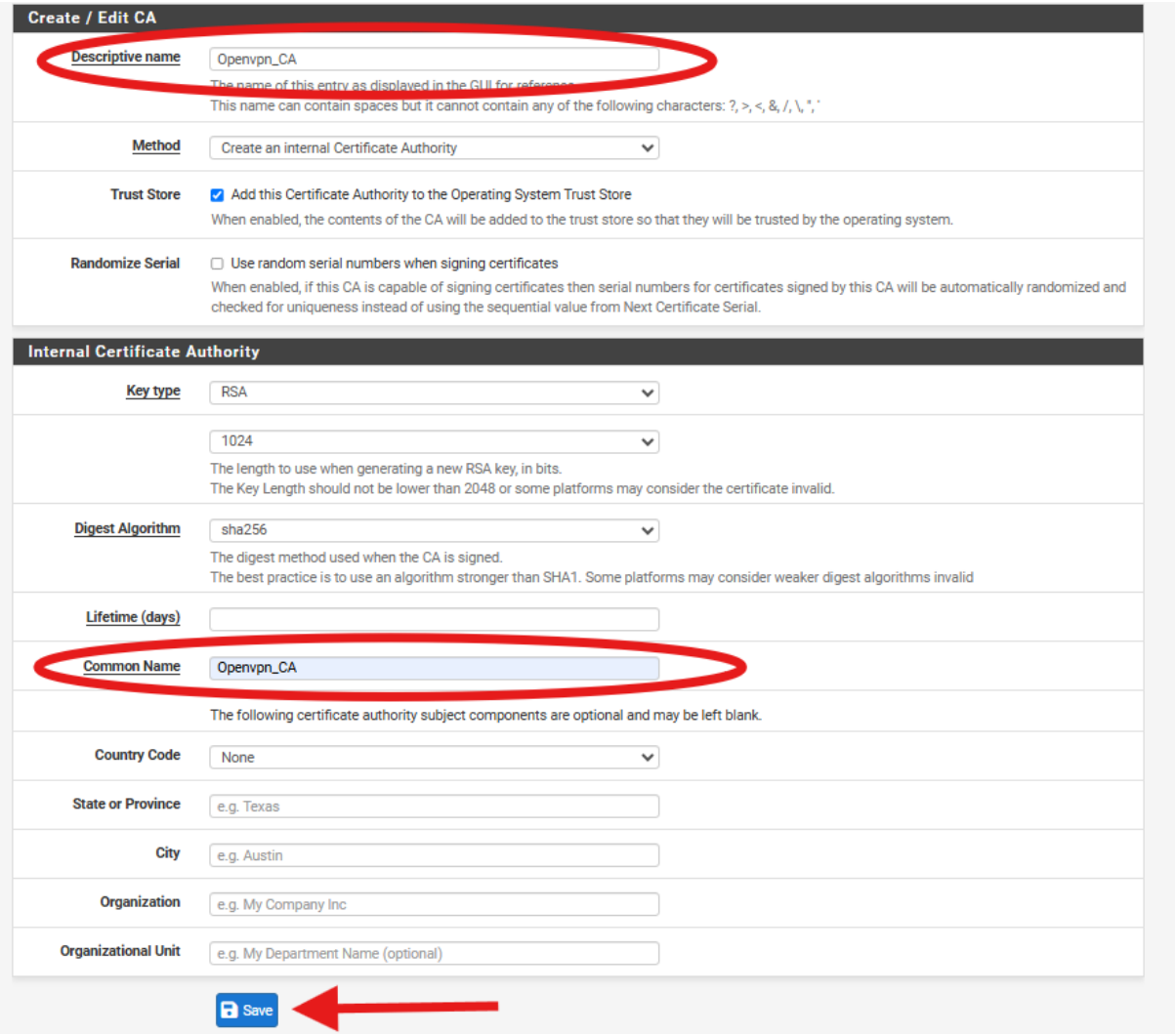
Il reste à configurer le VPN OpenVPN RW pour les clients distants. Premièrement, aller dans System puis Certificates.



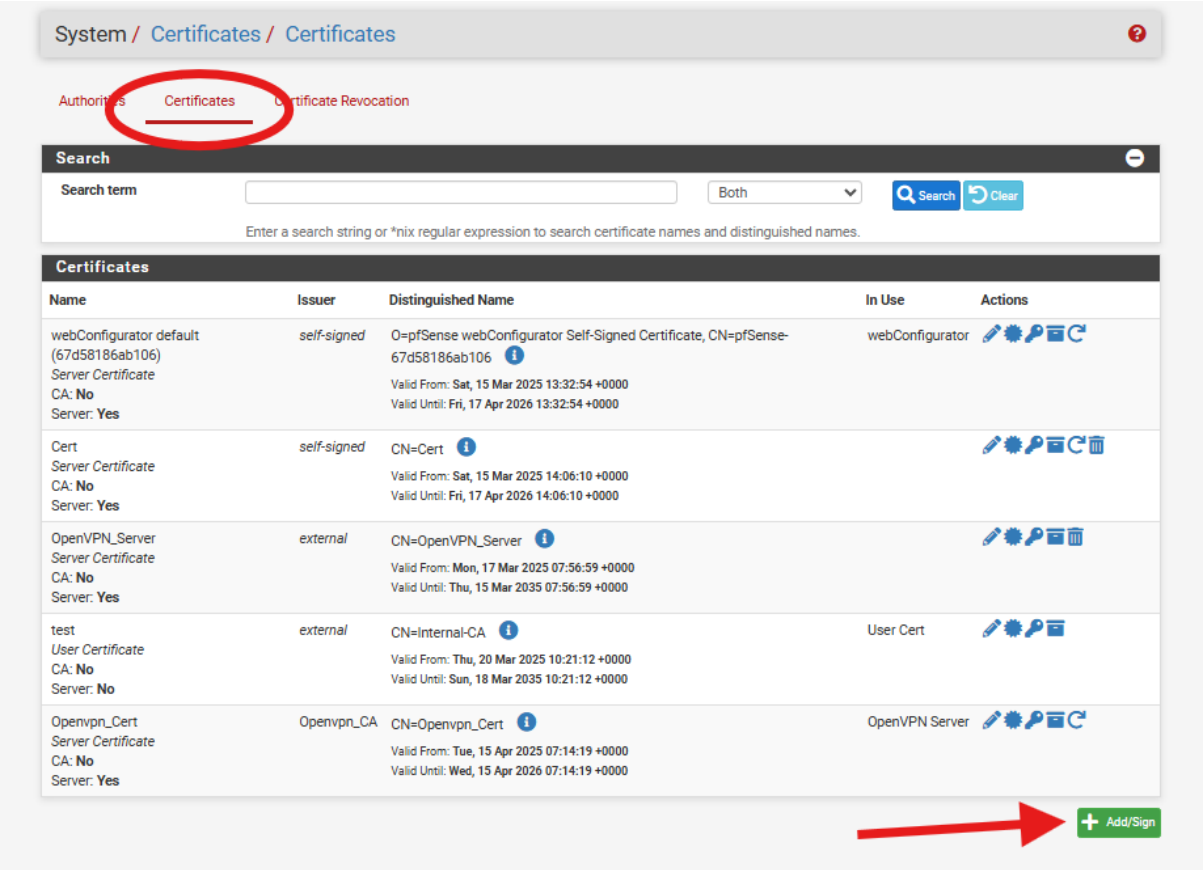
Dans la partie Authorities, cliquer sur Add pour rajouter un certificat d'autorité.



Rentrer les mêmes paramètres et cliquer sur Save.

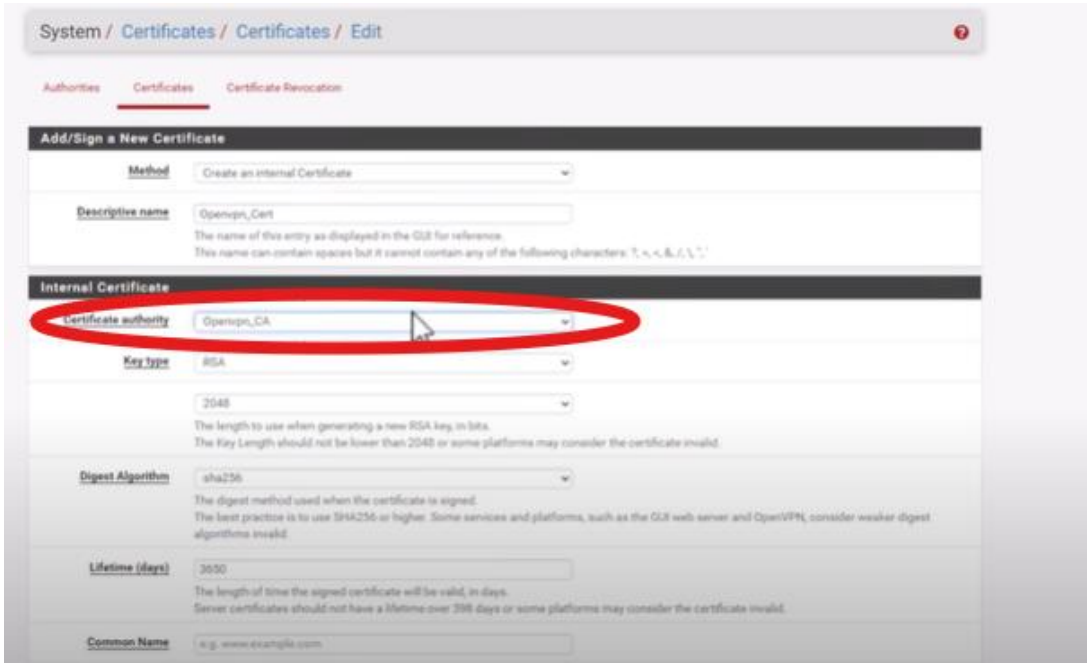


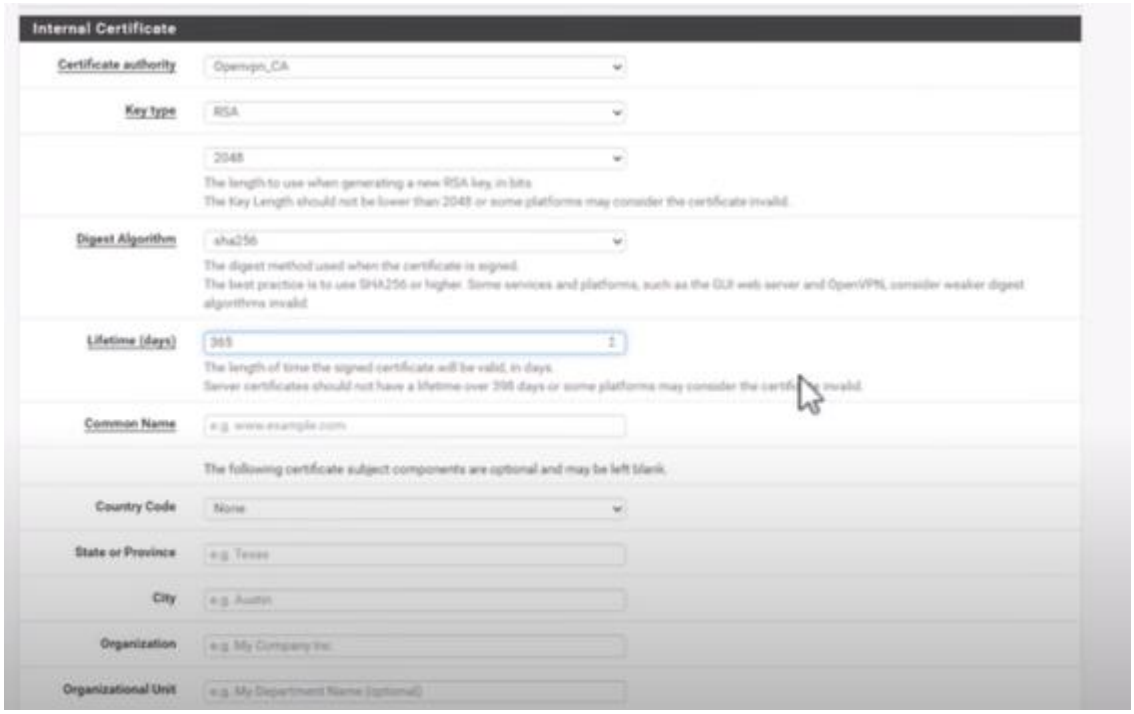
Aller ensuite dans Certificates puis cliquer sur Add/Sign pour ajouter un certificat.



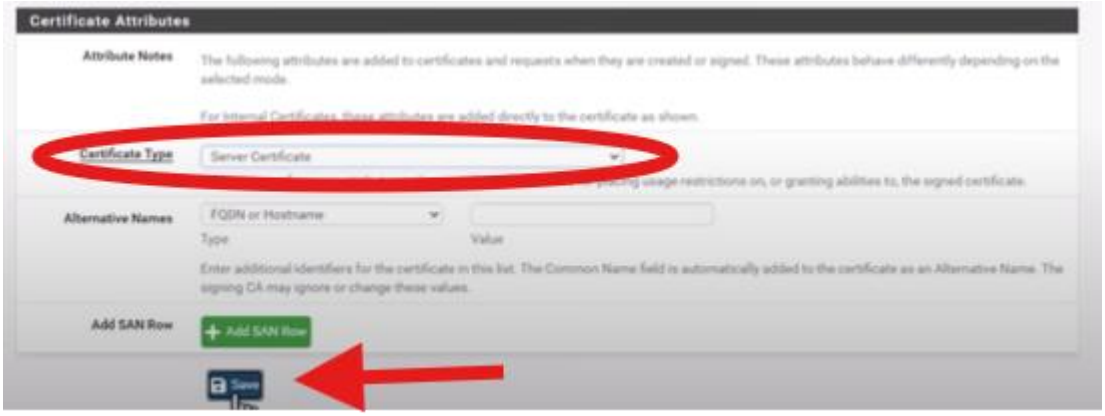
Rentrer ensuite ces paramètres.

Dans Certificate Authorities, sélectionner l'autorité de certificat créée avant (OpenVPN_CA).

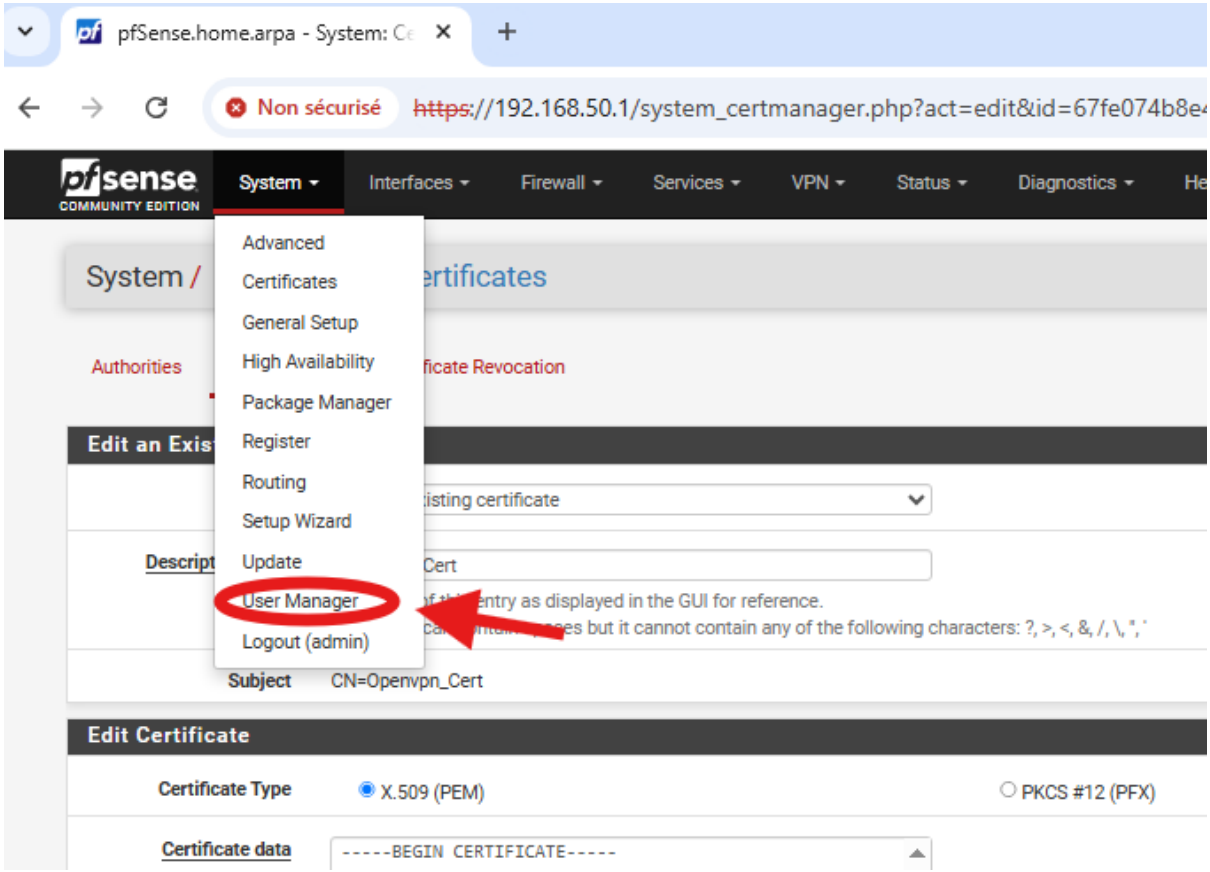




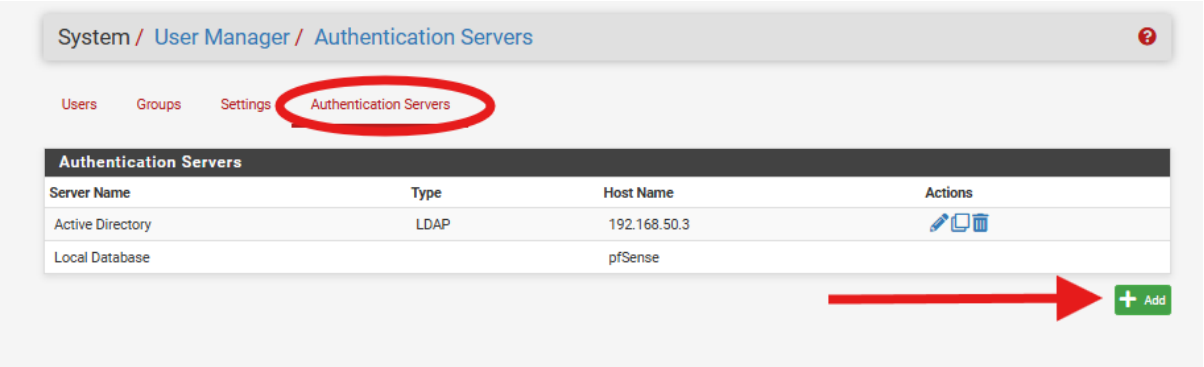
Veiller à bien choisir Server Certificate et cliquer sur Save.



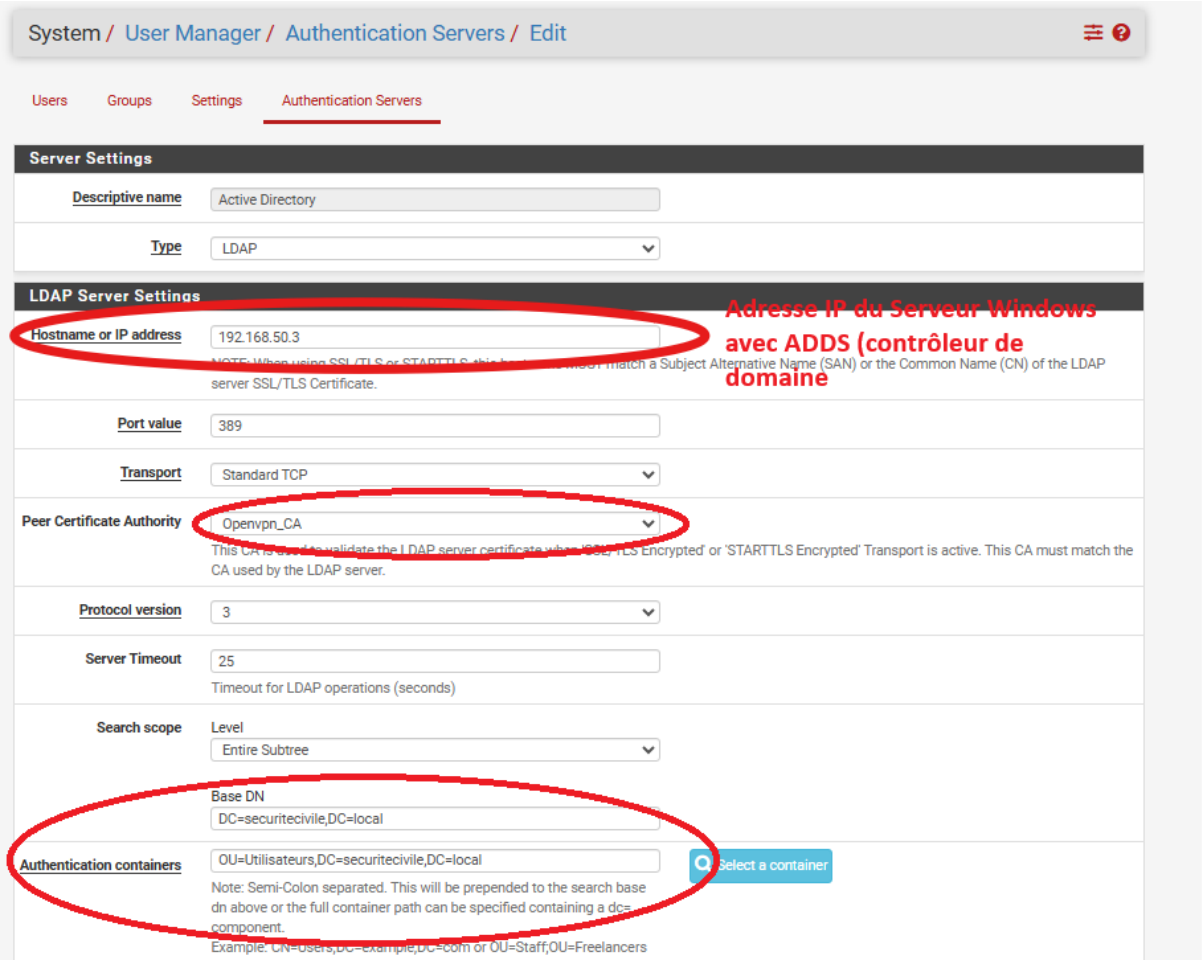
Aller ensuite dans System puis User Manager.



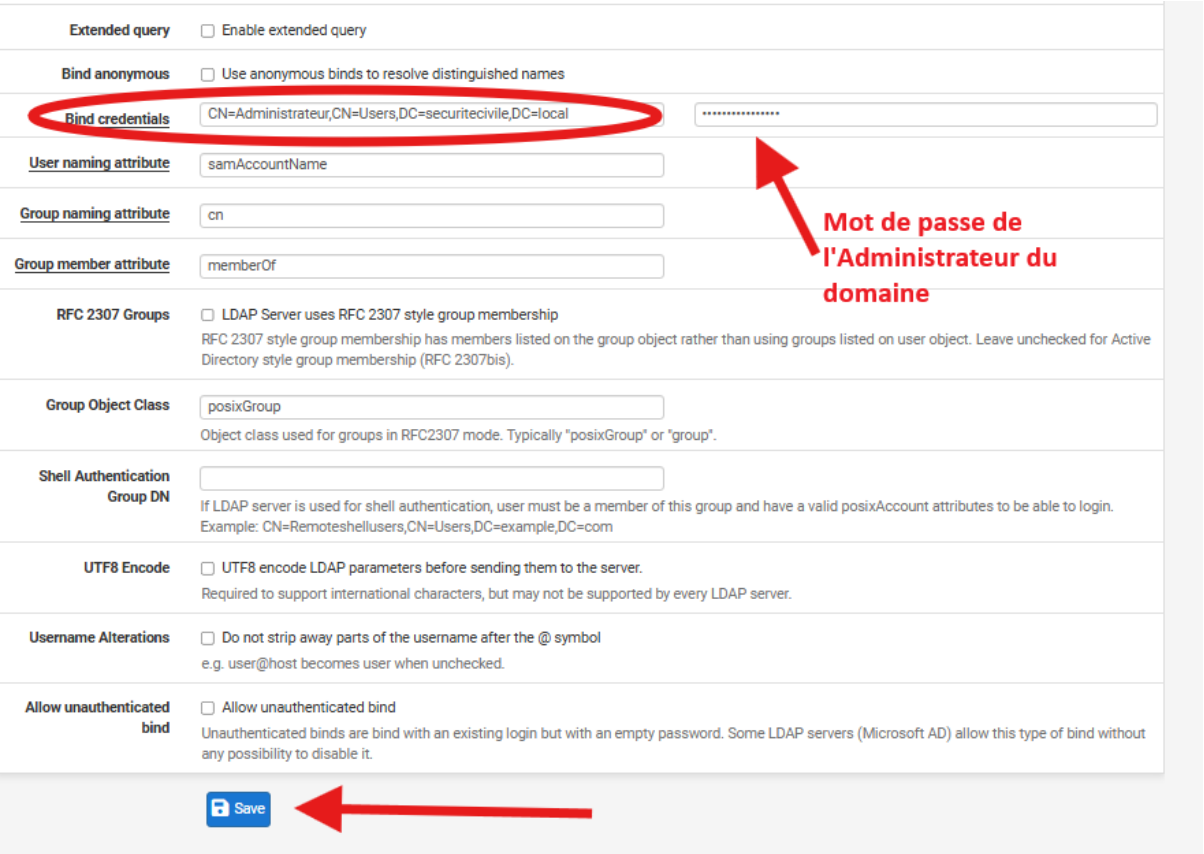
Aller dans Authentification Servers et cliquer sur Add.



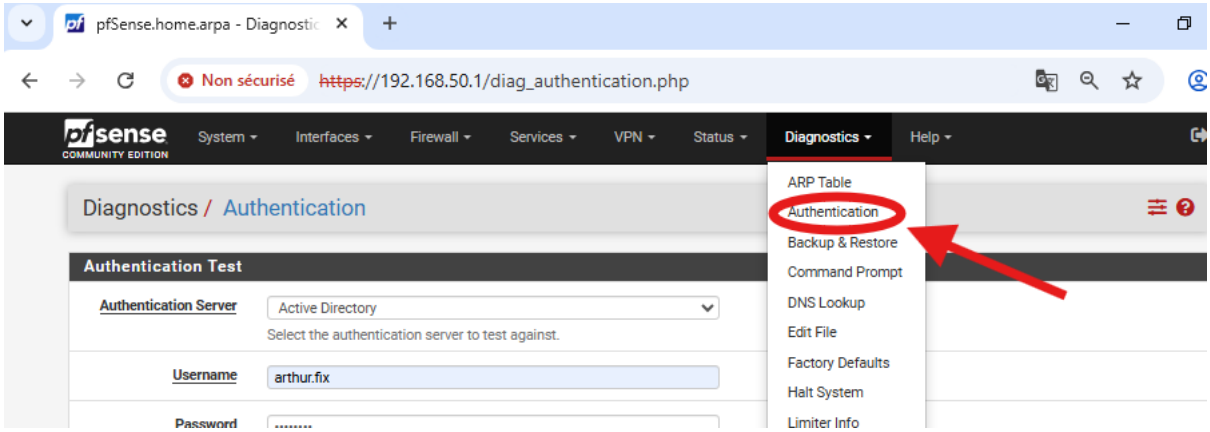
Entrer ces paramètres.



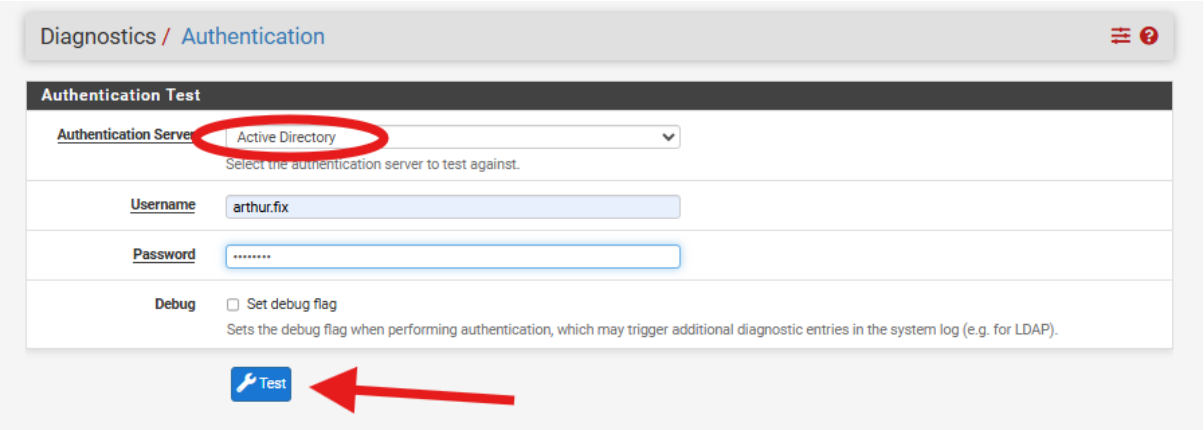
Une fois les paramètres rentrés, cliquer sur Save.



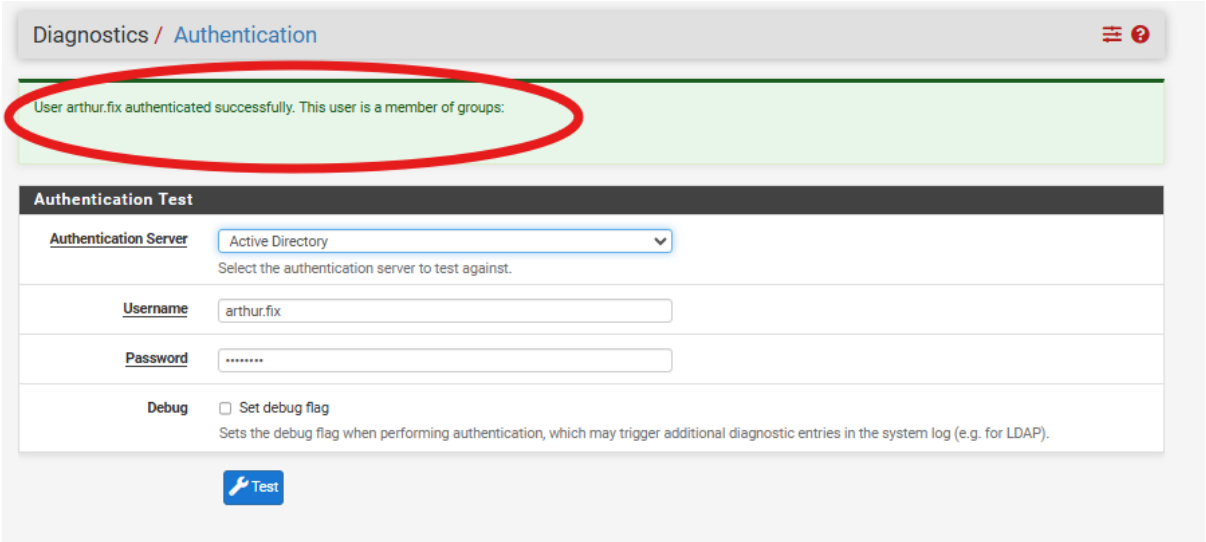
Pour tester si la connexion d'un utilisateur du domaine au PfSense fonctionne, aller dans Diagnostics puis Authentification.



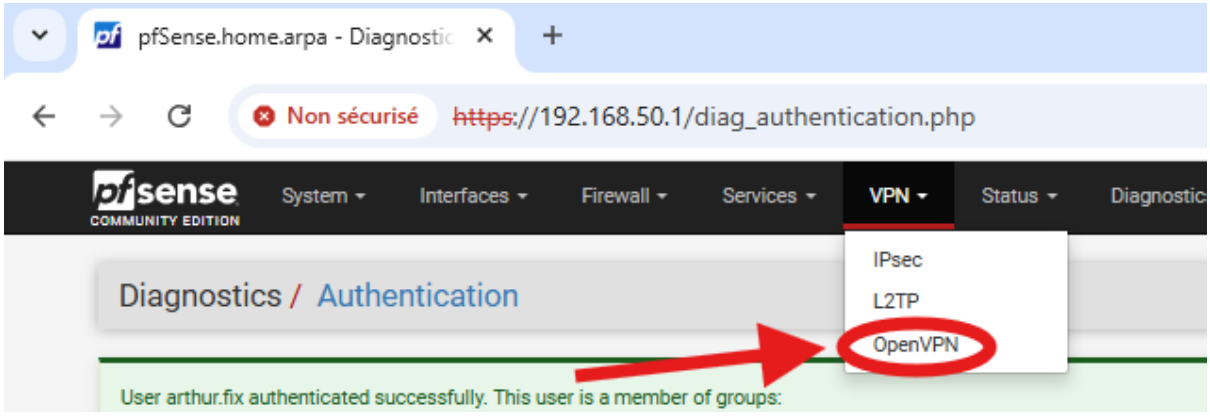
Sélectionner le serveur Active Directory, rentrer les identifiants d'un utilisateur du domaine et cliquer sur Test.



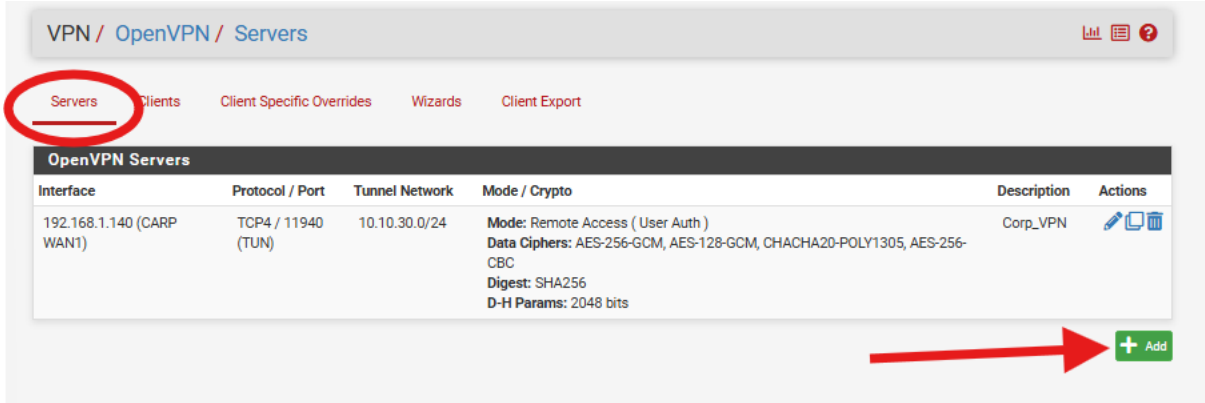
Si ce message s'affiche, alors la configuration est correcte.



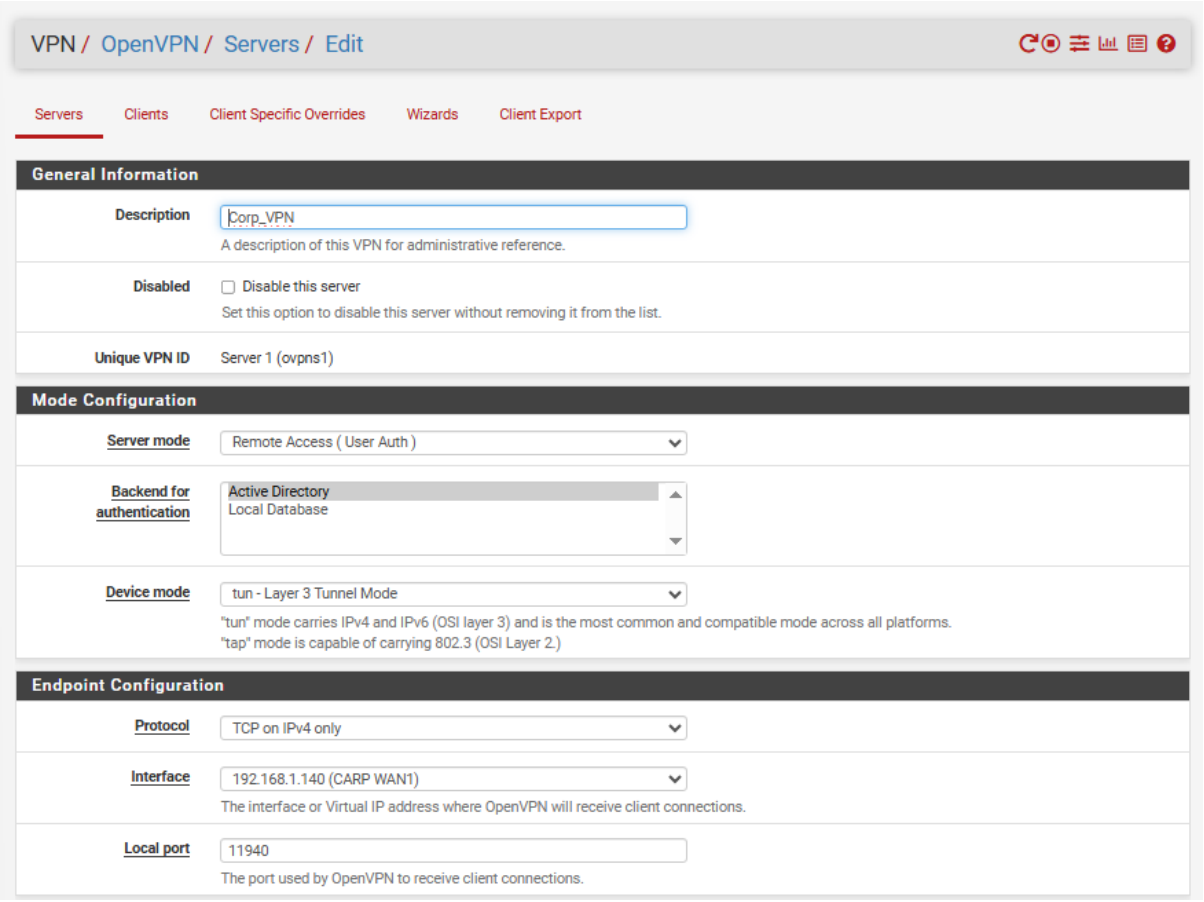
Aller dans VPN puis OpenVPN.

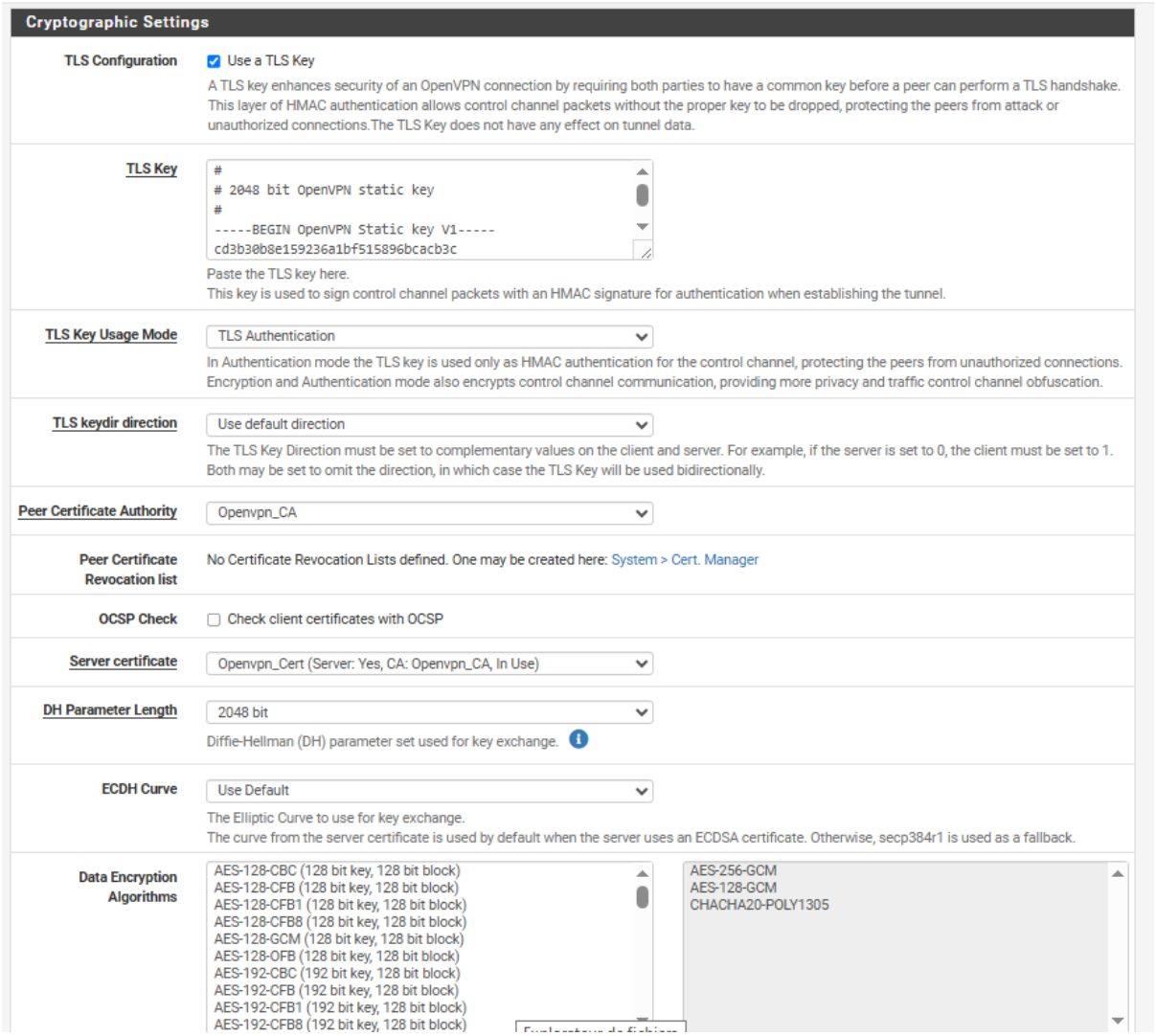


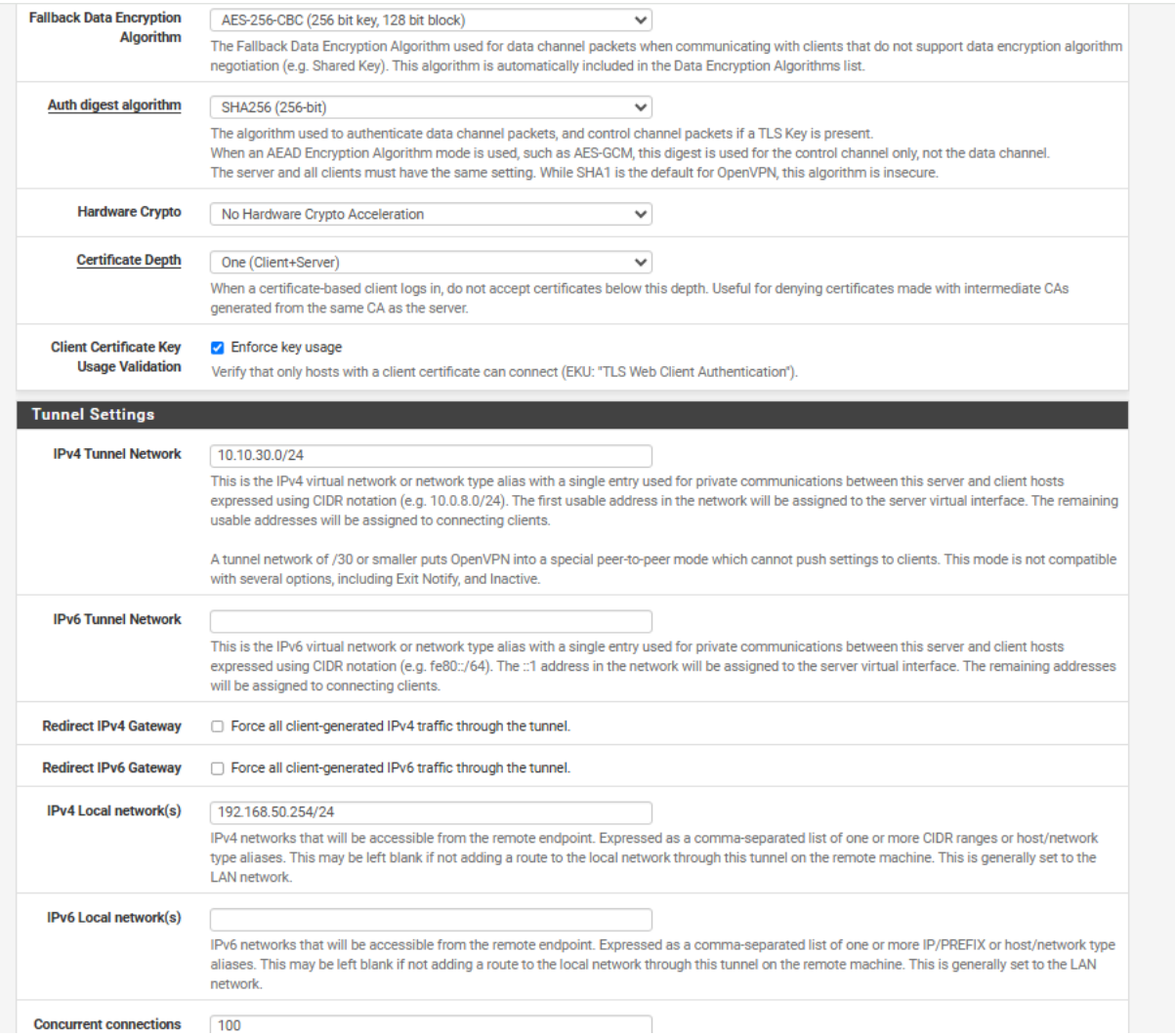
Dans la section Servers, cliquer sur Add.



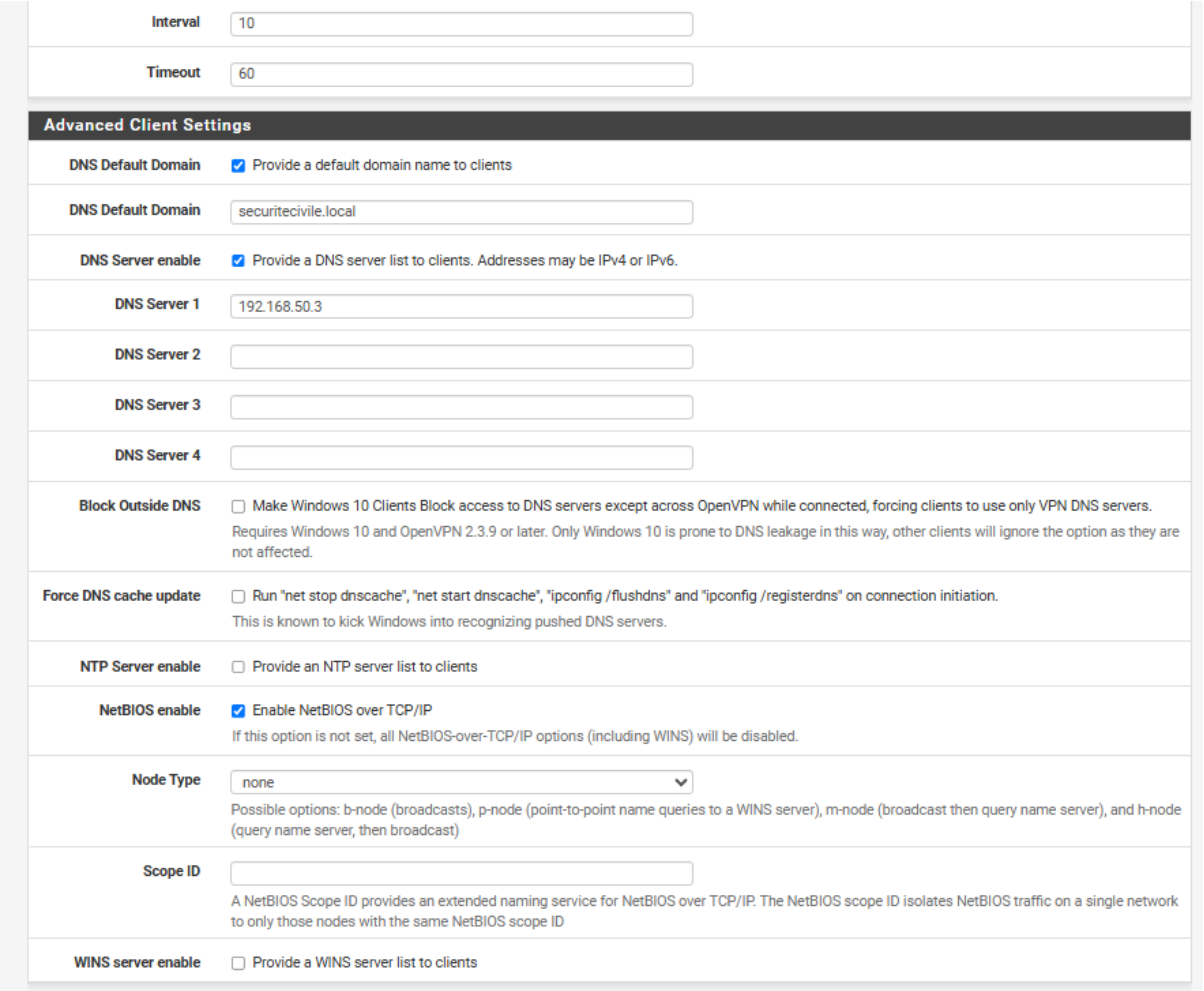
Voici la configuration à rentrer.


VPN / OpenVPN / Servers / Edit
Servers
Clients
Client Specific Overrides
Wizards
Client Export
General Information
Description
Corp_VPN
A description of this VPN for administrative reference.
Disabled
Disable this server
Set this option to disable this server without removing it from the list.
Unique VPN ID
Server 1 (ovpns1)
Mode Configuration
Server mode
Remote Access (User Auth)
Backend for authentication
Active Directory
Local Database
Device mode
tun - Layer 3 Tunnel Mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)
Endpoint Configuration
Protocol
TCP on IPv4 only
Interface
192.168.1.140 (CARP WAN1)
The interface or Virtual IP address where OpenVPN will receive client connections.
Local port
11940
The port used by OpenVPN to receive client connections.

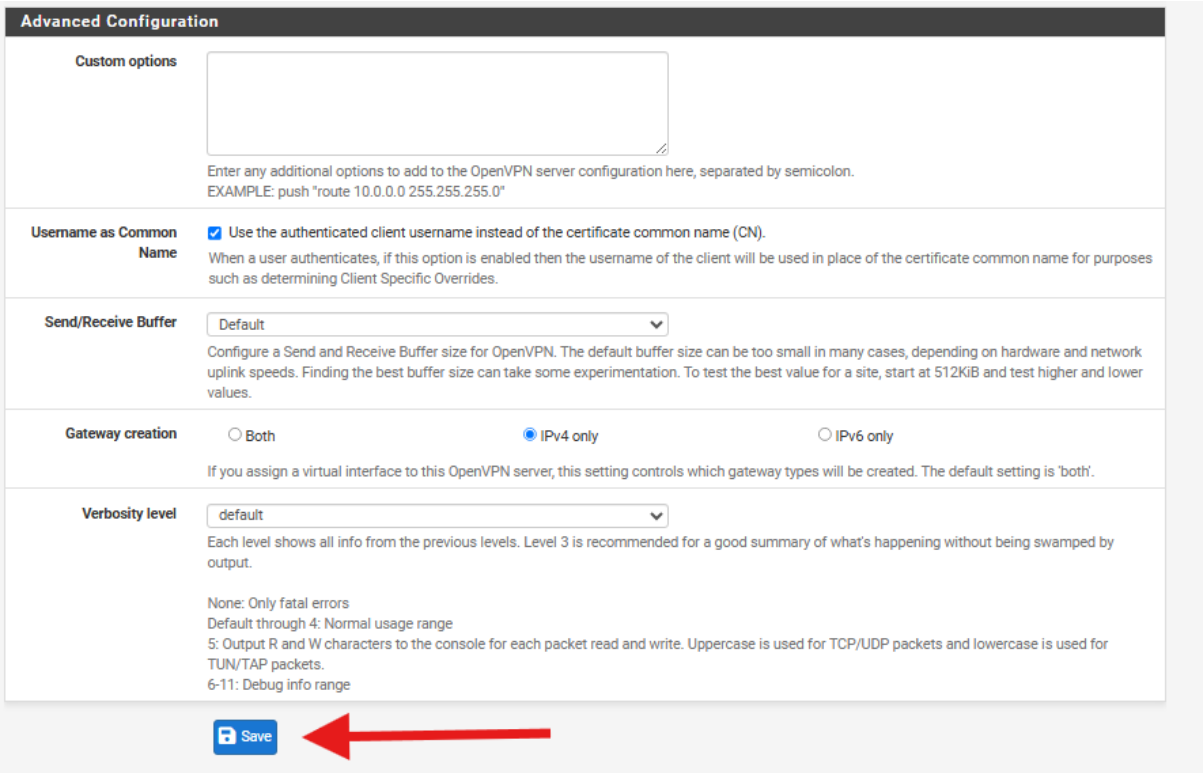

Cryptographic Settings
TLS Configuration
Use a TLS Key
A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections.The TLS Key does not have any effect on tunnel data.
TLS Key
#
2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
cd3b30b8e159236a1bf515896bcacb3c
Paste the TLS key here.
This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.
TLS Key Usage Mode
TLS Authentication
In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.
TLS keydir direction
Use default direction
The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.
Peer Certificate Authority
Openvpn_CA
Peer Certificate Revocation list
No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check
Check client certificates with OCSP
Server certificate
Openvpn_Cert (Server: Yes, CA: Openvpn_CA, In Use)
DH Parameter Length
2048 bit
Diffie-Hellman (DH) parameter set used for key exchange.
ECDH Curve
Use Default
The Elliptic Curve to use for key exchange.
The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
Data Encryption Algorithms
AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)
AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305


Fallback Data Encryption Algorithm
AES-256-CBC (256 bit key, 128 bit block)
The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.
Auth digest algorithm
SHA256 (256-bit)
The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.
Hardware Crypto
No Hardware Crypto Acceleration
Certificate Depth
One (Client+Server)
When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.
Client Certificate Key Usage Validation
Enforce key usage
Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").
Tunnel Settings
IPv4 Tunnel Network
10.10.30.0/24
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.
IPv6 Tunnel Network
This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
Redirect IPv4 Gateway
Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway
Force all client-generated IPv6 traffic through the tunnel.
IPv4 Local network(s)
192.168.50.254/24
IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. 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.
IPv6 Local network(s)
IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. 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.
Concurrent connections
100


Allow Compression
Decompress incoming, do not compress outgoing (Asymmetric)
Allow compression to be used with this VPN instance.
Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.
Asymmetric compression allows an easier transition when connecting with older peers.
Compression
Adaptive LZO Compression [Legacy style, comp-lzo adaptive]
Deprecated. Compress tunnel packets using the LZO algorithm.
Compression can potentially dangerous and insecure. See the note on the Allow Compression option above.
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.
Push Compression
Push the selected Compression setting to connecting clients.
Type-of-Service
Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
Inter-client communication
Allow communication between clients connected to this server
Duplicate Connection
Allow multiple concurrent connections from the same user
When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.
Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.
Client Settings
Dynamic IP
Allow connected clients to retain their connections if their IP address changes.
Topology
Subnet – One IP address per client in a common subnet
Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4.
Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".
Ping settings
Inactive
300
Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device.
Activity is based on the last incoming or outgoing tunnel packet.
A value of 0 disables this feature.
This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.
Ping method
keepalive – Use keepalive helper to define ping configuration
keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows:
ping = interval
Explorateur de fichiers

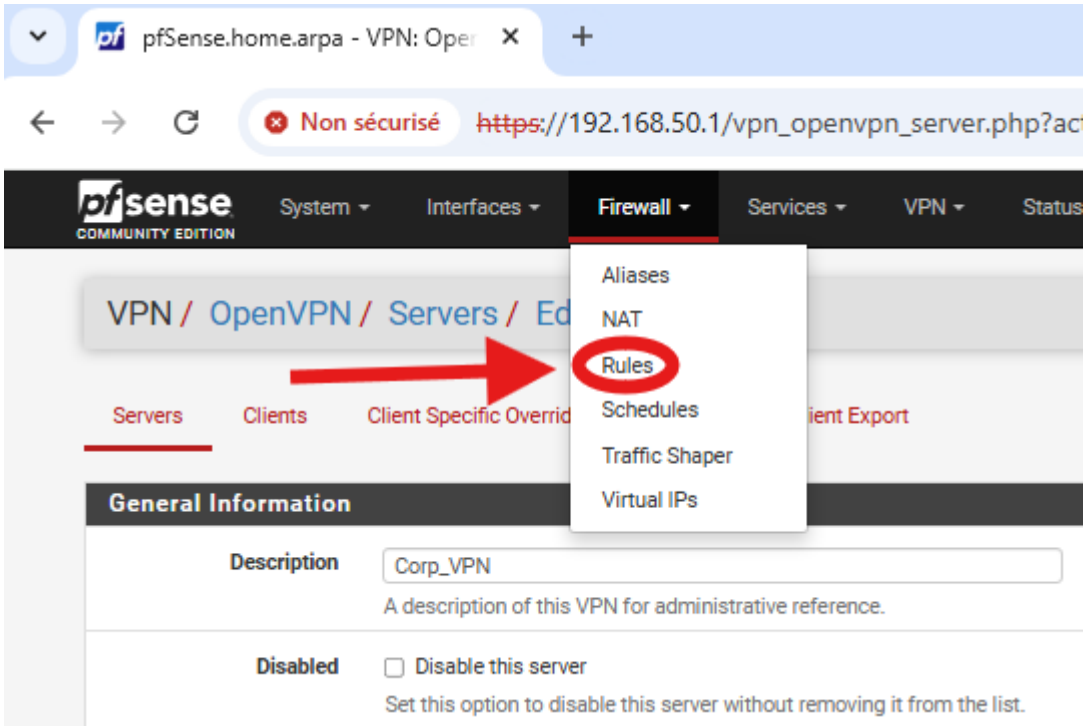


Une fois la configuration terminée, cliquer sur Save.

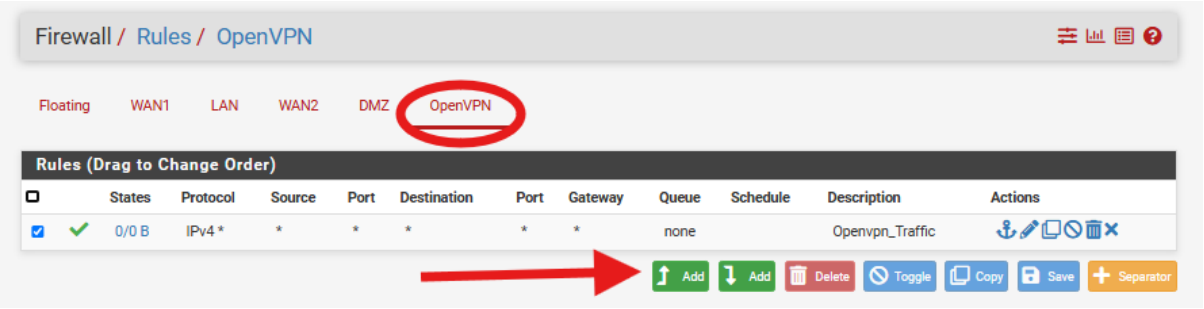


Il faut maintenant créer des règles afin que les clients à distance puissent se connecter via OpenVPN.

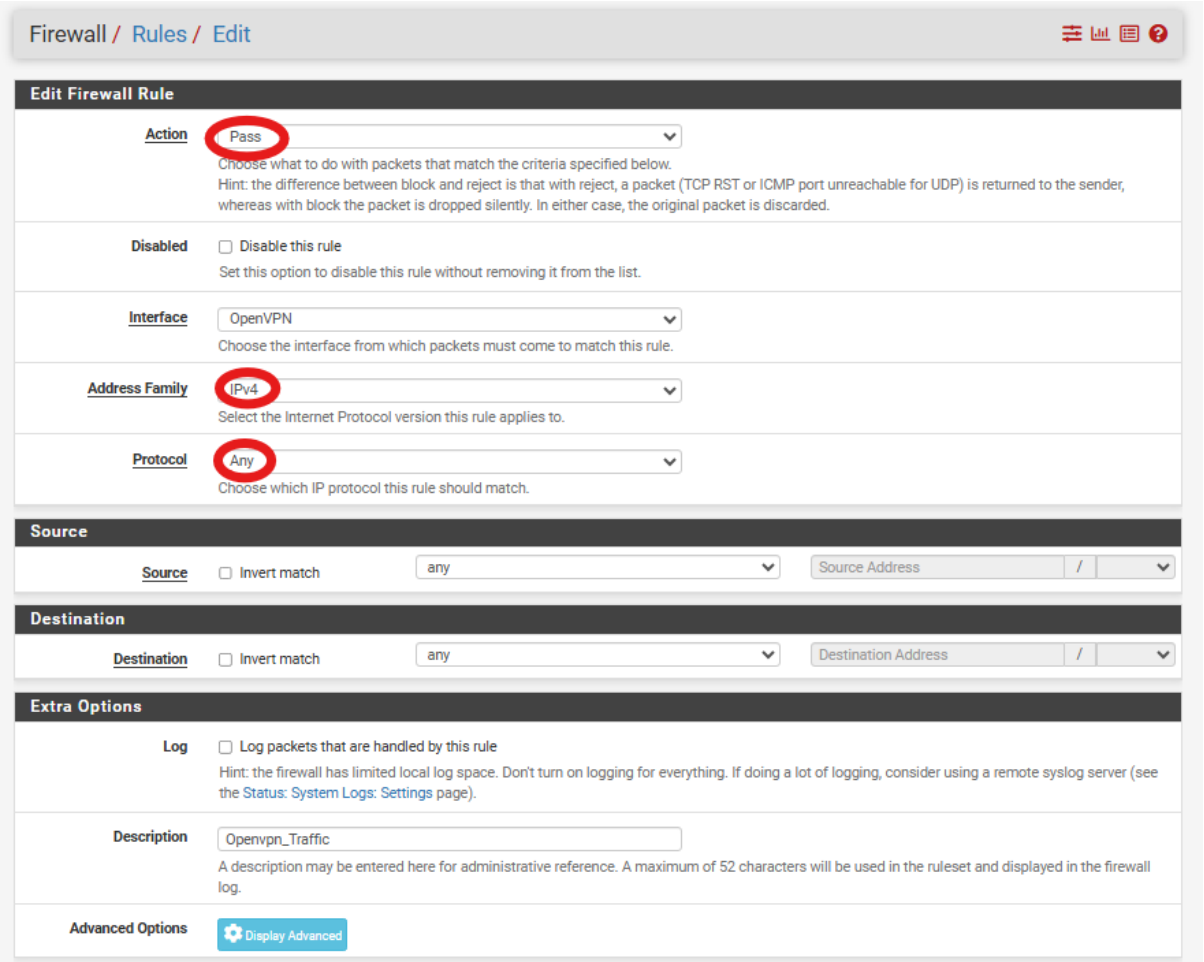
Aller dans Firewall puis Rules.



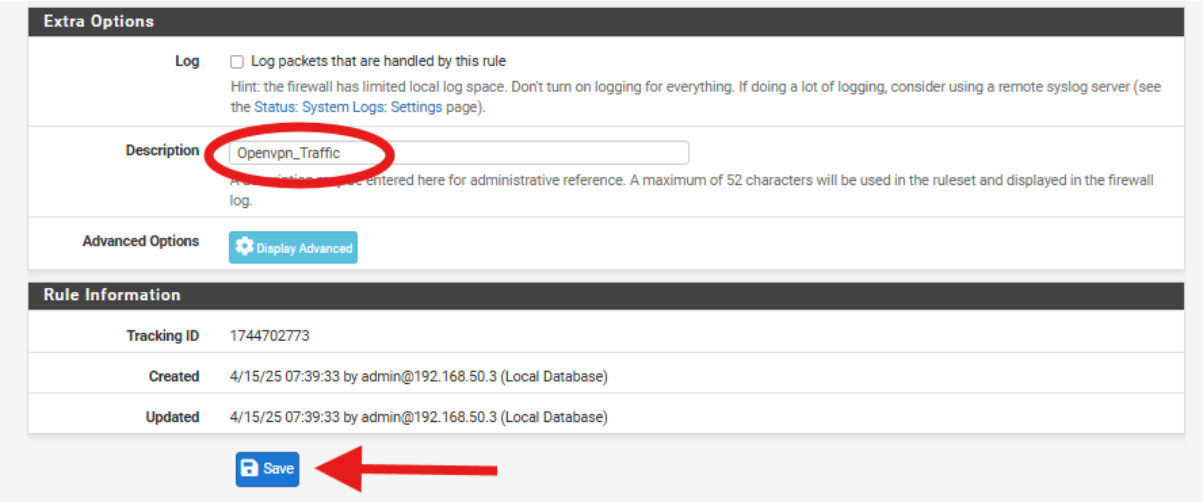
Aller dans la section OpenVPN puis cliquer sur Add pour ajouter une nouvelle règle.



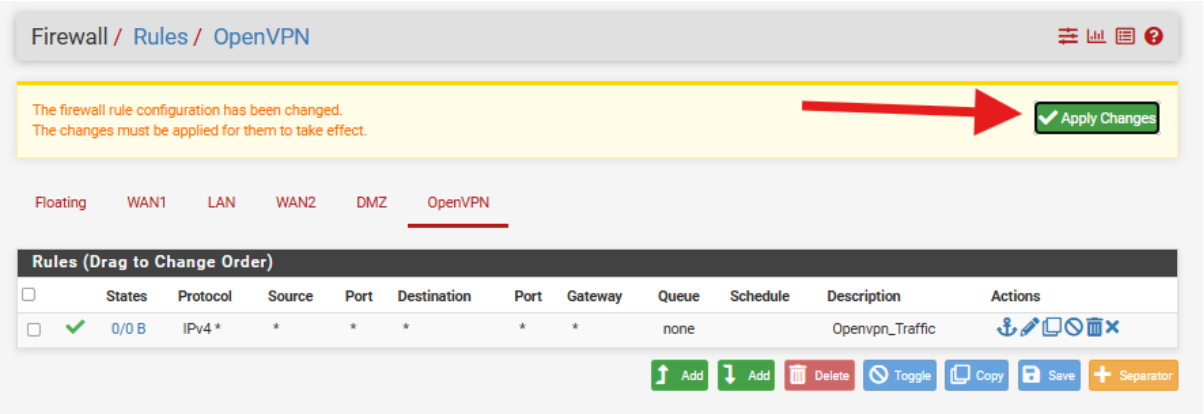
Sélectionner Pass pour Action, IPv4 pour la famille d'adresse, et Any pour Protocol.



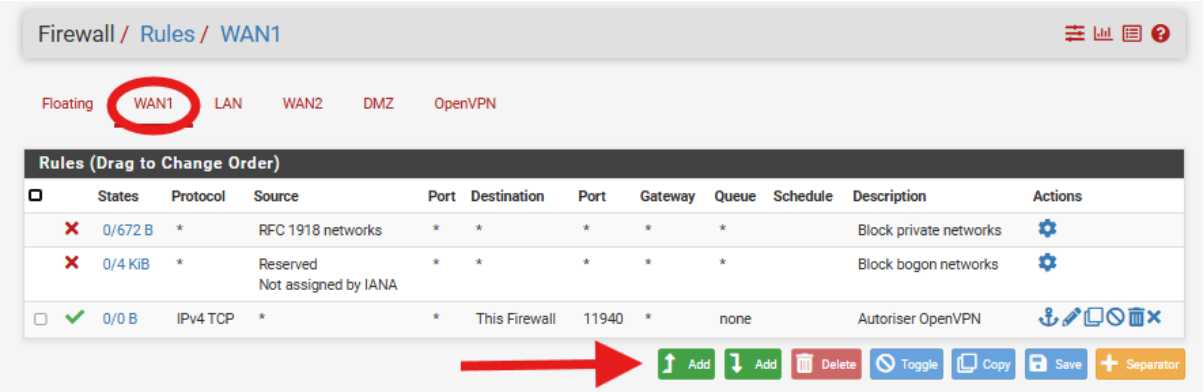
Ajouter une description à la règle et cliquer sur Save.



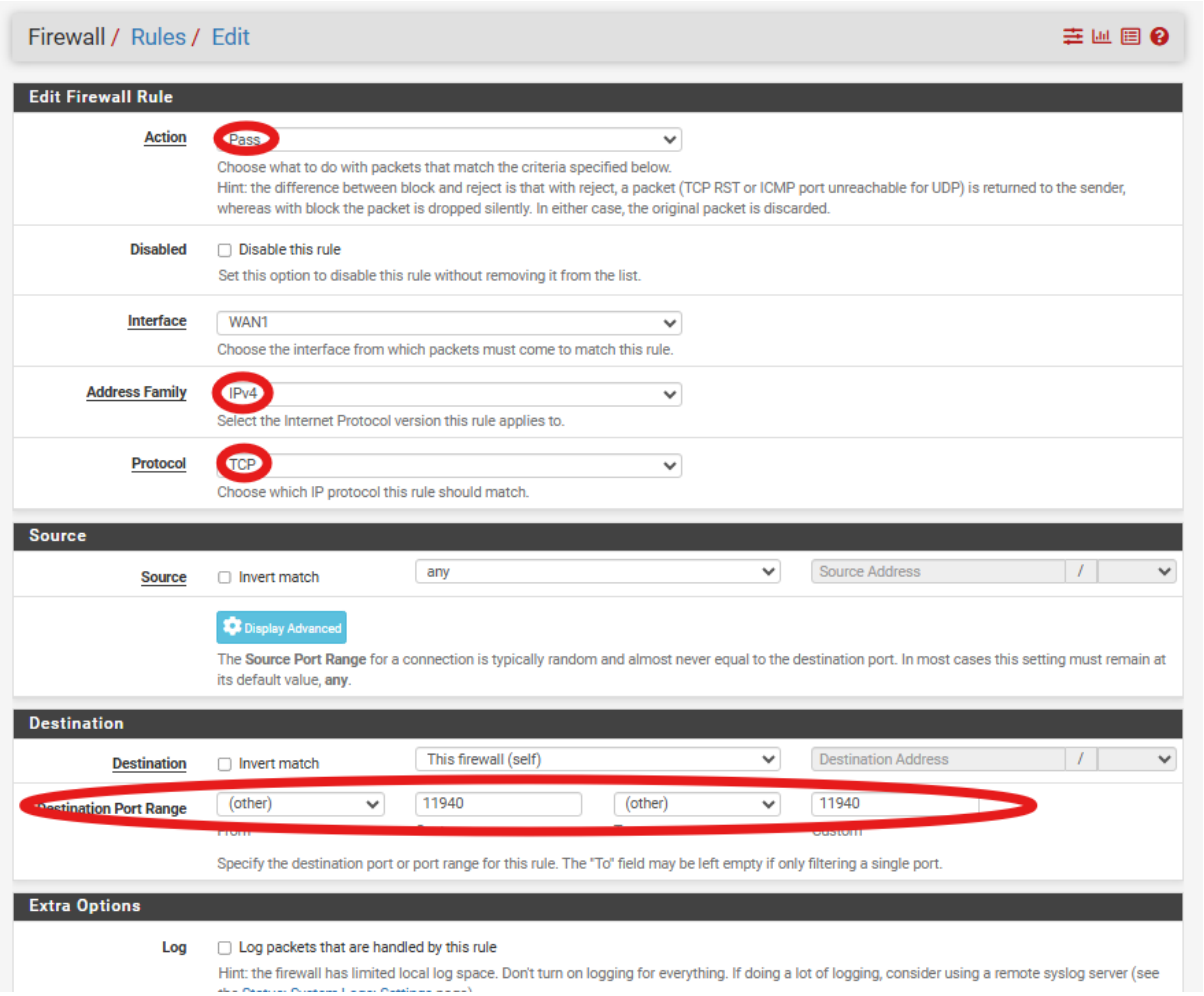
Cliquer sur Apply Changes.



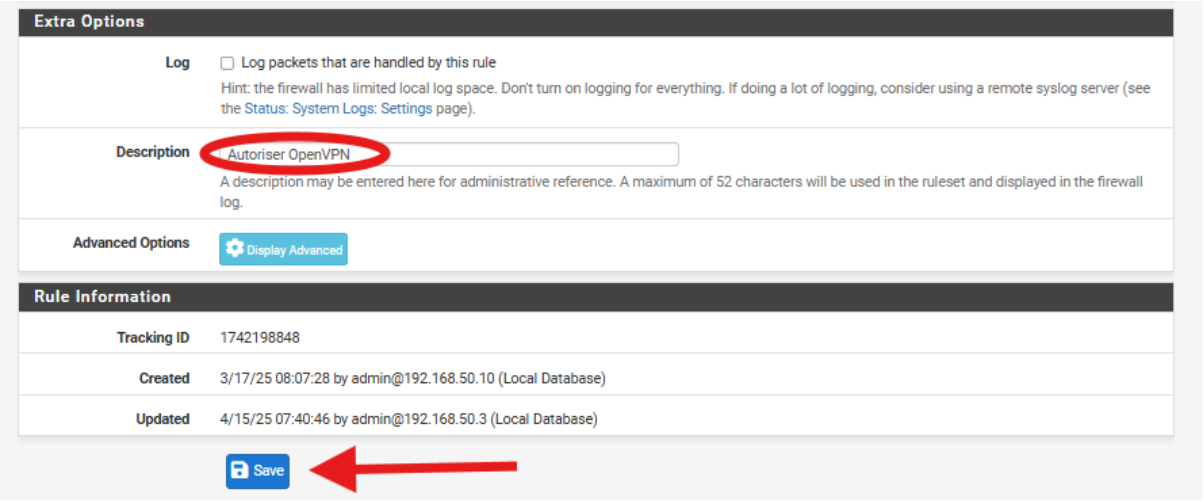
Aller ensuite sur l'interface WAN principale (WAN1) toujours dans les Rules. Cliquer sur Add pour ajouter une nouvelle règle.



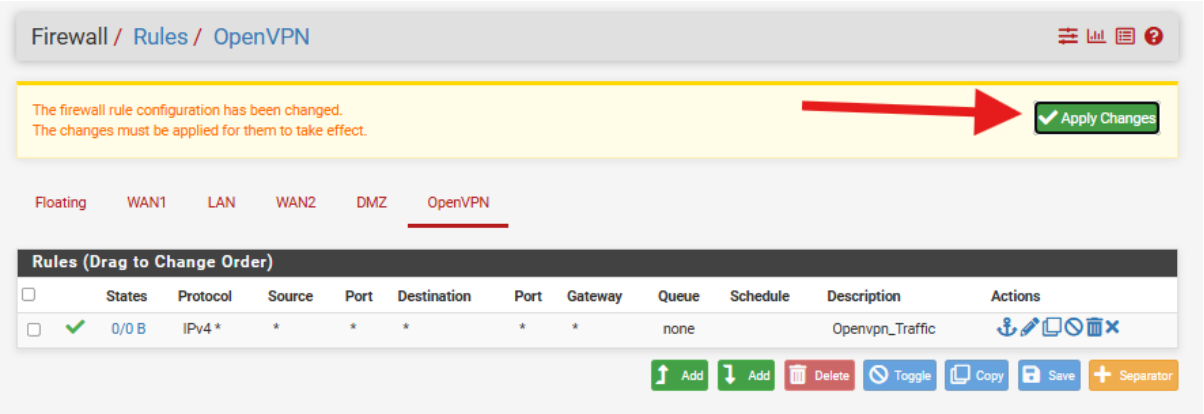
Choisir Pass en Action, IPv4 pour la famille d'adresse, TCP pour Protocol, et plus bas dans la section Destination, choisir le port 11940 pour le port de destination (celui que l'on a configuré et choisi avant dans la configuration de OpenVPN).



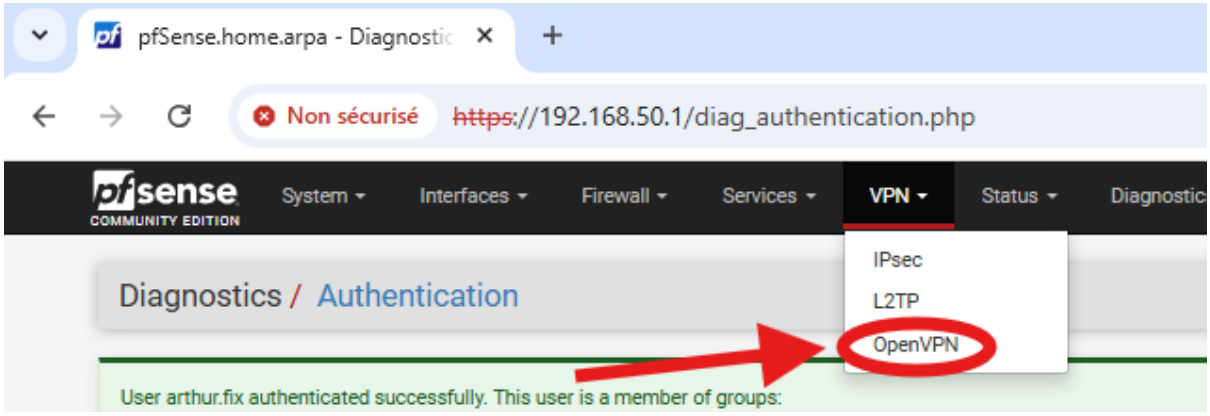
Ajouter une description et cliquer sur Save.



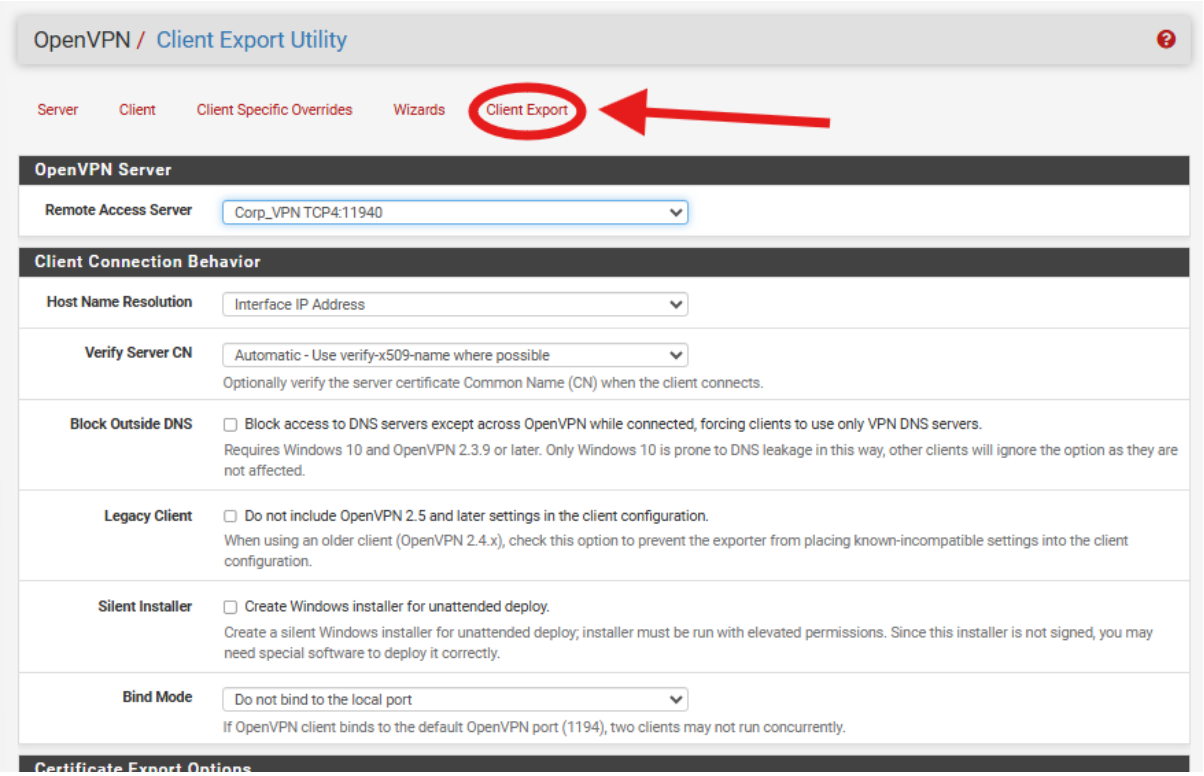
Cliquer sur Apply Changes.



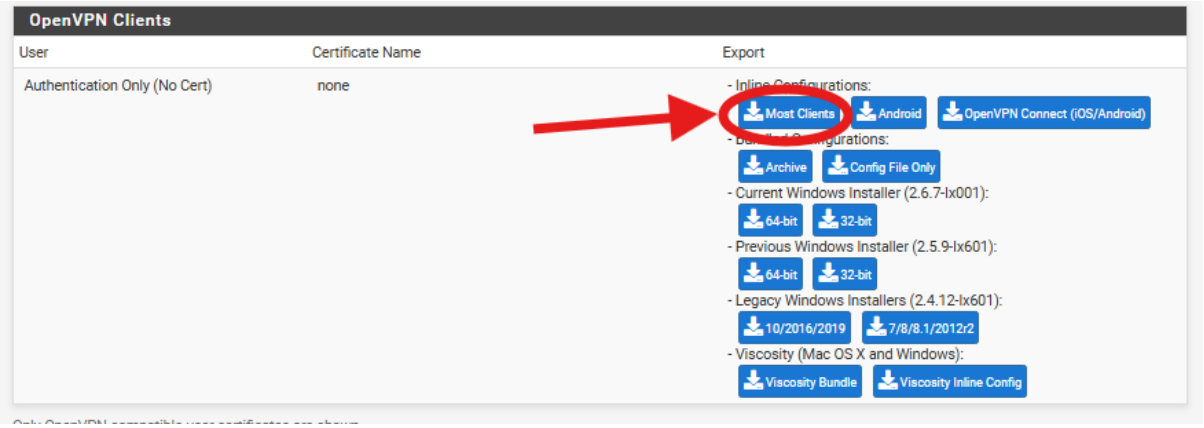
Retourner ensuite dans OpenVPN depuis la section VPN.



Aller sur Client Export.

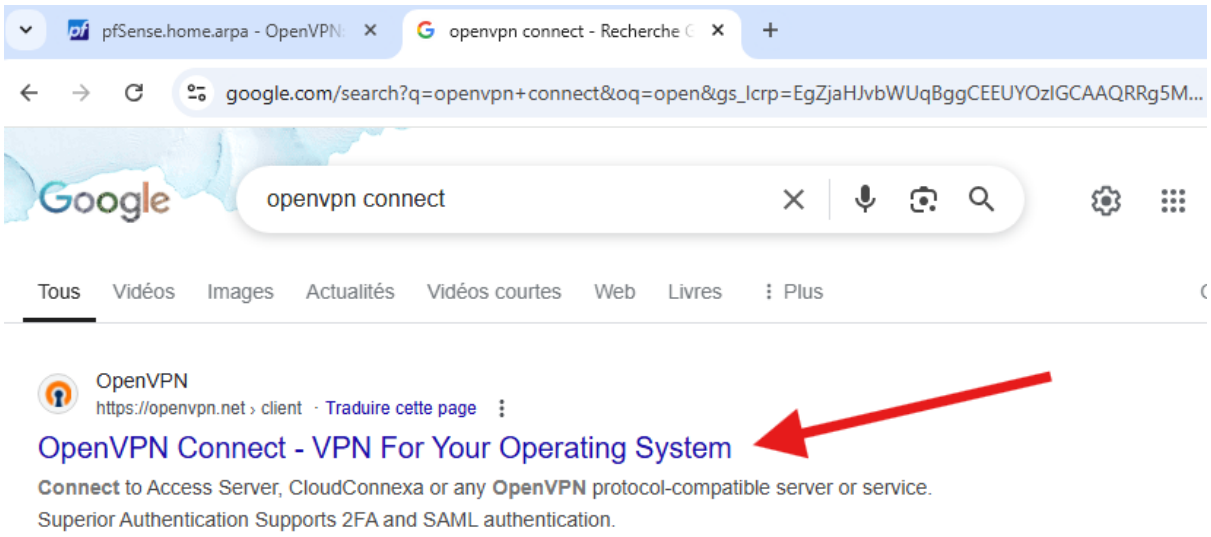


Il n'y a aucun paramètre à changer, aller tout en bas et sélectionner Most Clients pour installer le fichier de configuration de OpenVPN.

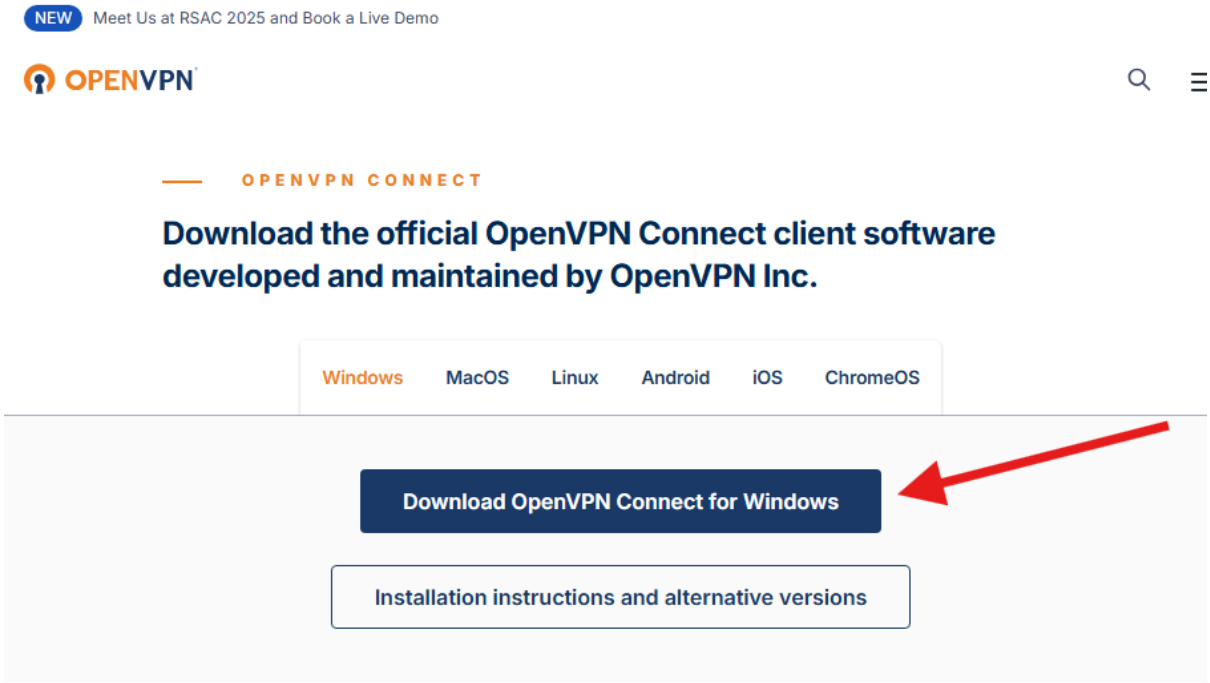


Il faut maintenant installer le client OpenVPN Connect pour tester si OpenVPN fonctionne (le client sera aussi à installer et à configurer sur les postes clients).

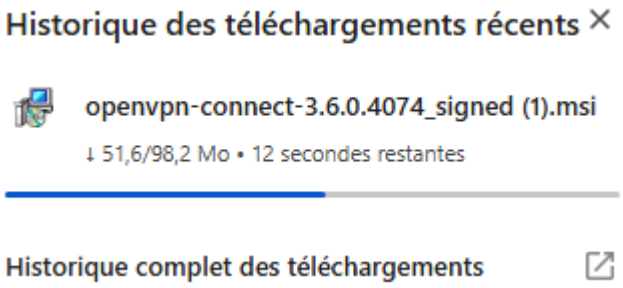
Sur le navigateur de recherche, rechercher openvpn connect et cliquer sur le premier lien.



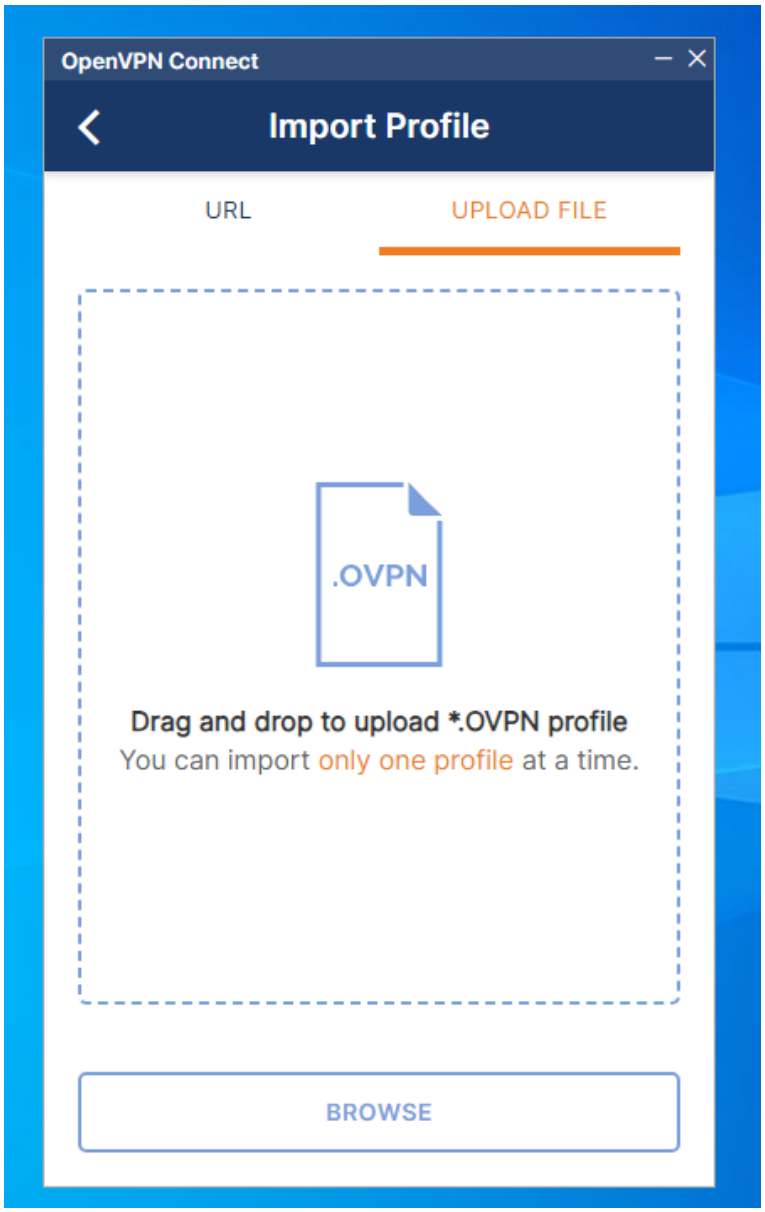
Cliquer sur le bouton d'installation.



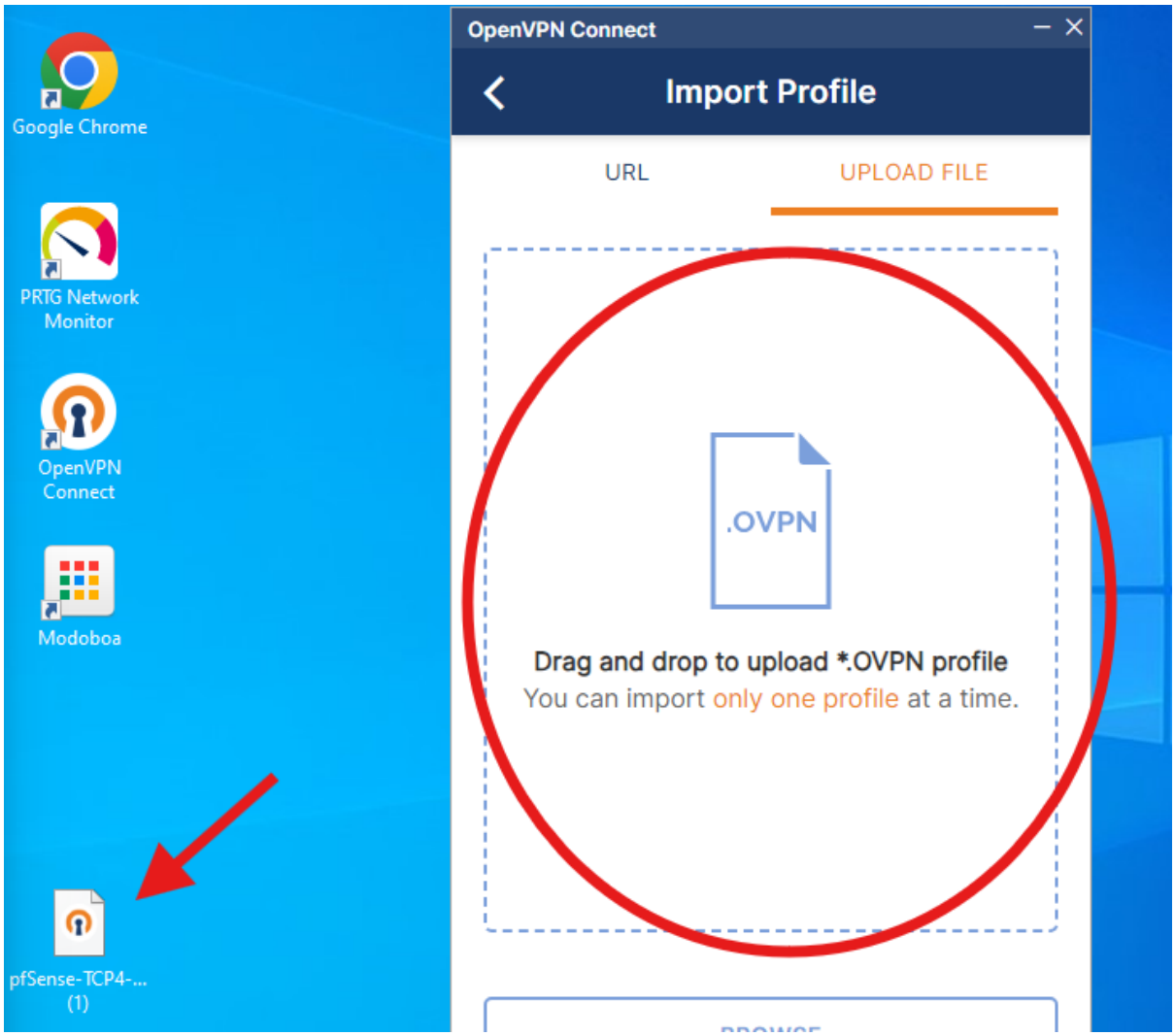
Une fois l'installation terminée, ouvrir l'installer et suivre les étapes d'installation.



Ouvrir OpenVPN Connect.

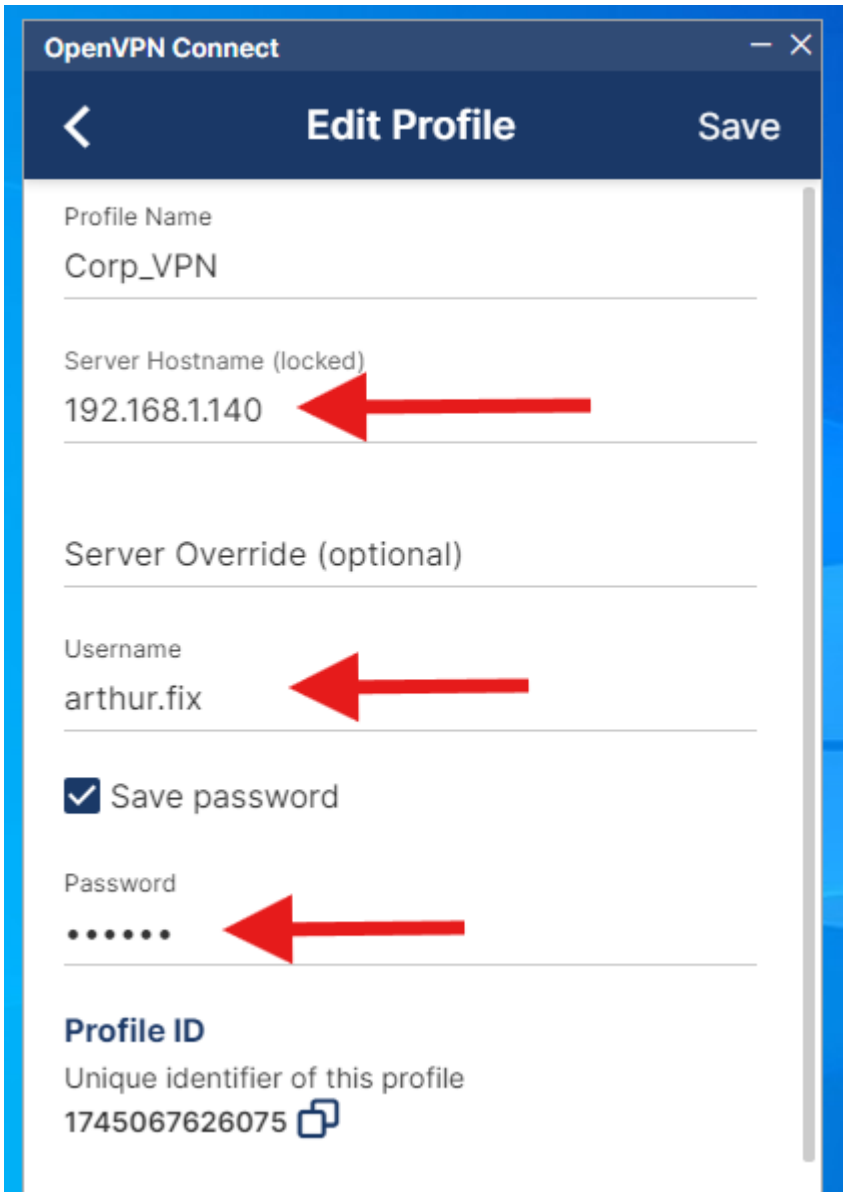

OpenVPN Connect
Import Profile
URL
UPLOAD FILE
.OVPN
Drag and drop to upload *.OVPN profile
You can import only one profile at a time.
BROWSE

Sélectionner le fichier de configuration de OpenVPN installé avant (se trouve sur mon bureau) et le glisser dans la zone d'upload de fichier de configuration sur OpenVPN Connect.

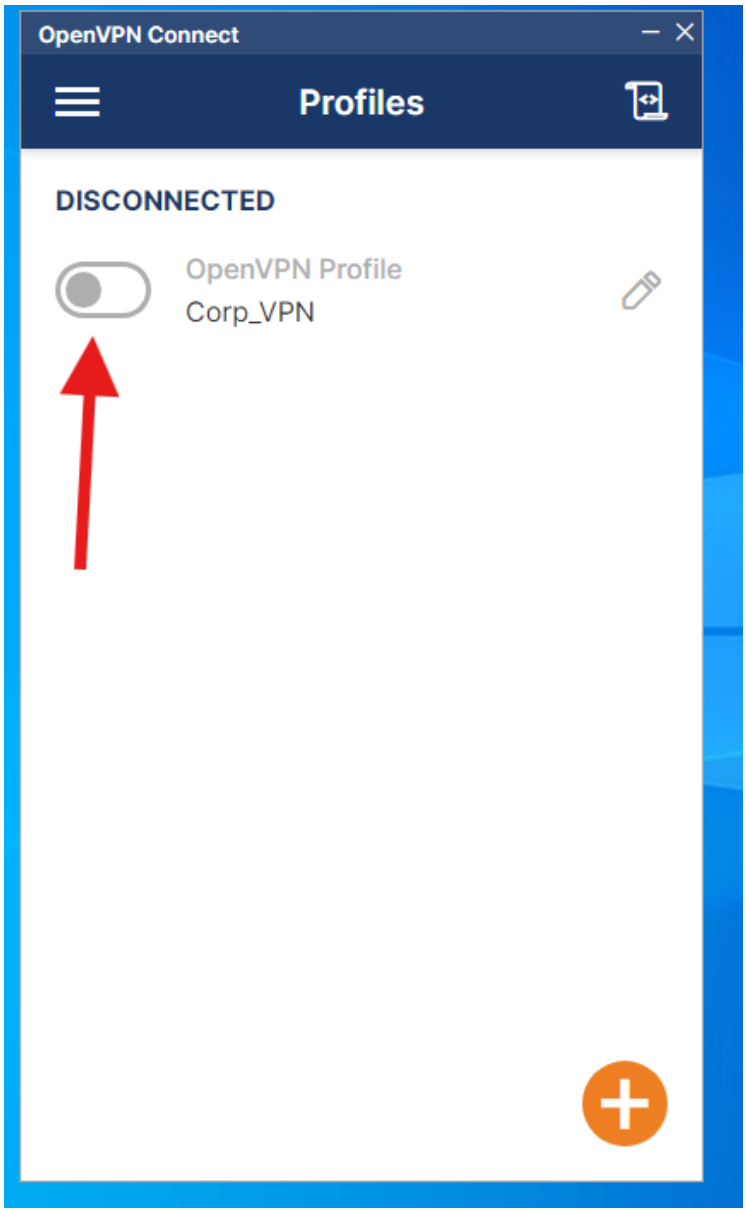


Entrer les paramètres suivants. Choisir 192.168.1.140 pour Server Hostname et utiliser les identifiants d'un utilisateur de l'AD pour se connecter.

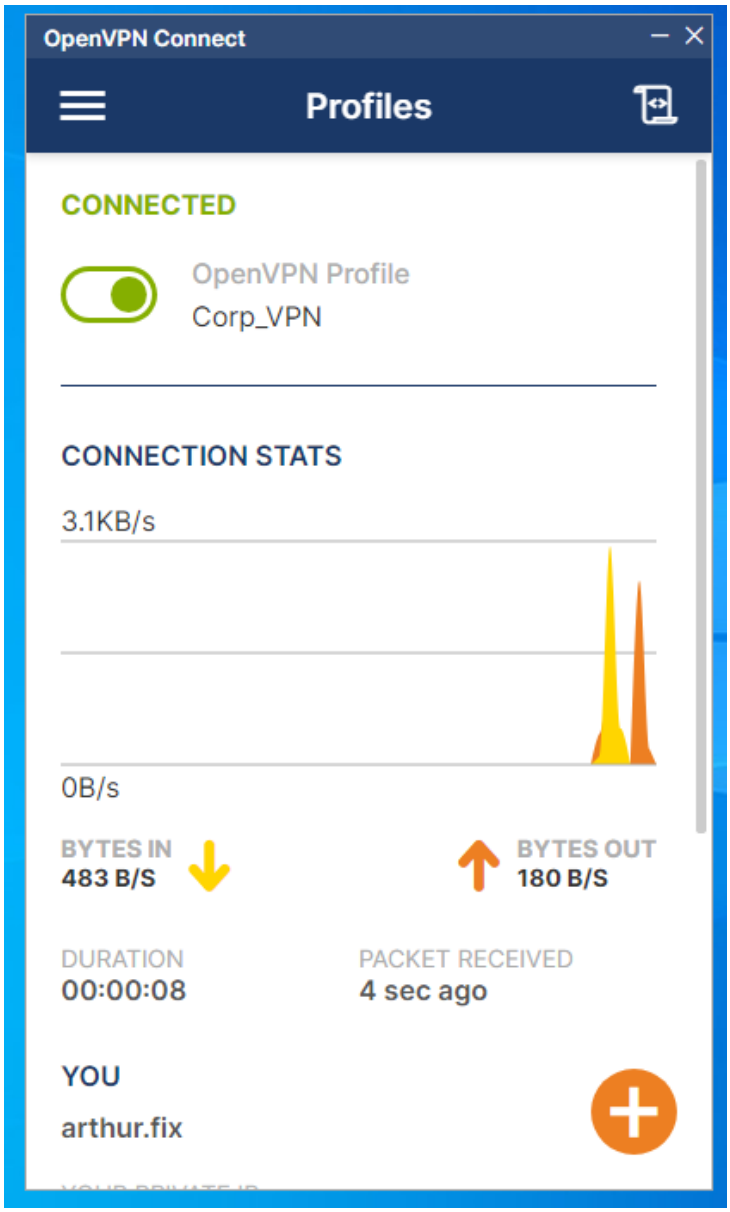
A la fin de la configuration, cliquer sur Save en haut à droite.



Cliquer ensuite sur le bouton de connexion.



Le VPN fonctionne.


OpenVPN Connect
Profiles
CONNECTED
OpenVPN Profile
Corp_VPN
CONNECTION STATS
3.1KB/s
0B/s
BYTES IN
483 B/S
BYTES OUT
180 B/S
DURATION
00:00:08
PACKET RECEIVED
4 sec ago
YOU
arthur.fix

Documentation d'exploitation, L’utilisation et la gestion du Lot 1

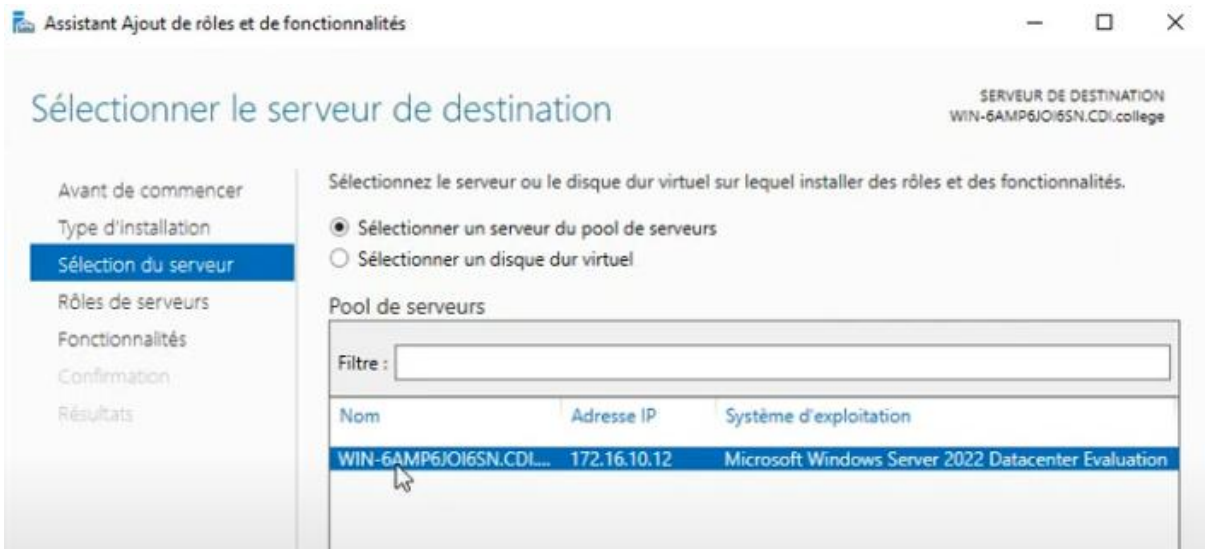
Introduction :

L’administration des réseaux informatiques repose sur des services essentiels qui assurent une gestion centralisée des utilisateurs, des ressources et des communications. Parmi ces services, Active Directory, DNS et DHCP jouent un rôle crucial. Active Directory permet de centraliser la gestion des comptes utilisateurs et des permissions, DNS assure la résolution des noms de domaine, tandis que DHCP automatise l’attribution des adresses IP dans le réseau. Ce document vous guidera à travers les étapes d'installation et d'utilisation de ces trois services fondamentaux, en mettant l’accent sur les bonnes pratiques pour garantir un fonctionnement optimal.

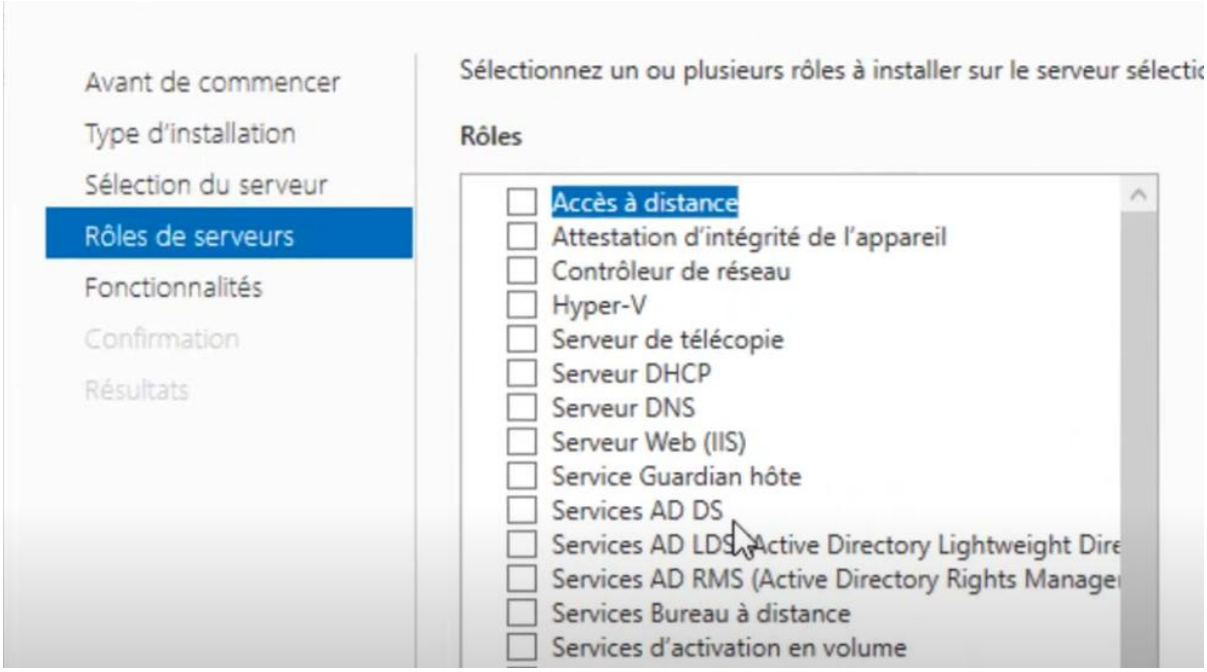
Installation des rôles

Lorsque vous allumez votre Windows Serveur cliquait sur Ajouter des rôles et des fonctionnalités.

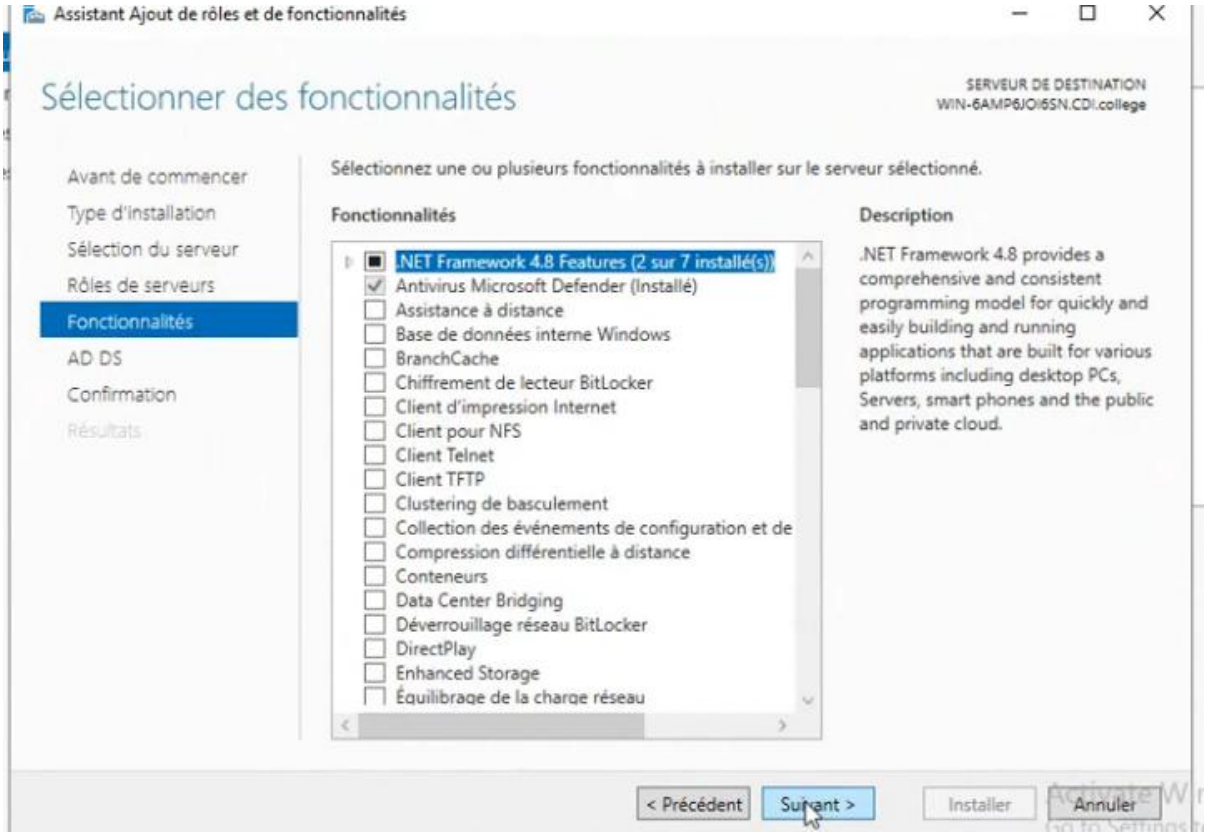
Cliquer deux fois sur suivant puis quand vous arrivez dans sélection du serveur sélectionnez votre serveur Windows.



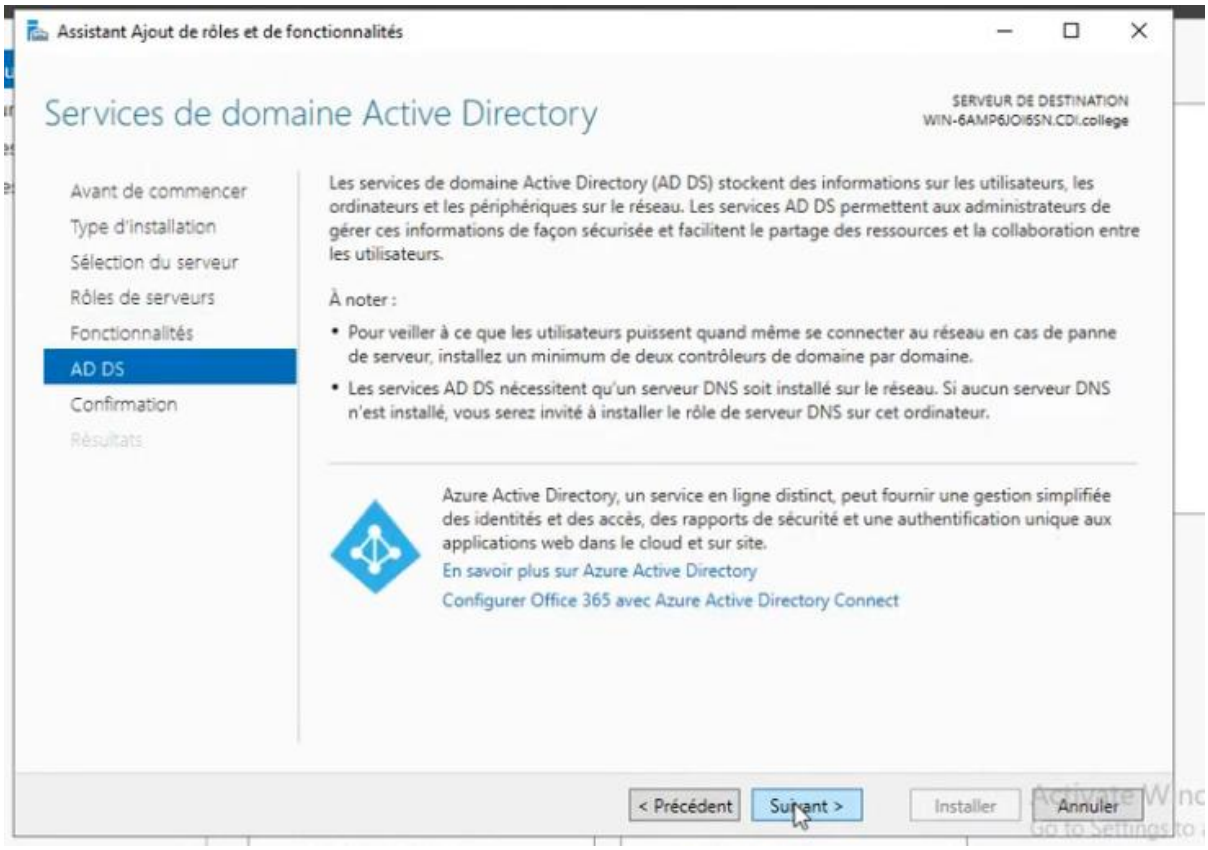
Dans rôles de serveurs sélectionnez les rôles Services AD DS et Serveur DHCP.


Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélecti
Rôles
Accès à distance
Attestation d'intégrité de l'appareil
Contrôleur de réseau
Hyper-V
Serveur de télécopie
Serveur DHCP
Serveur DNS
Serveur Web (IIS)
Service Guardian hôte
Services AD DS
Services AD LDS (Active Directory Lightweight Dire
Services AD RMS (Active Directory Rights Manage
Services Bureau à distance
Services d'activation en volume

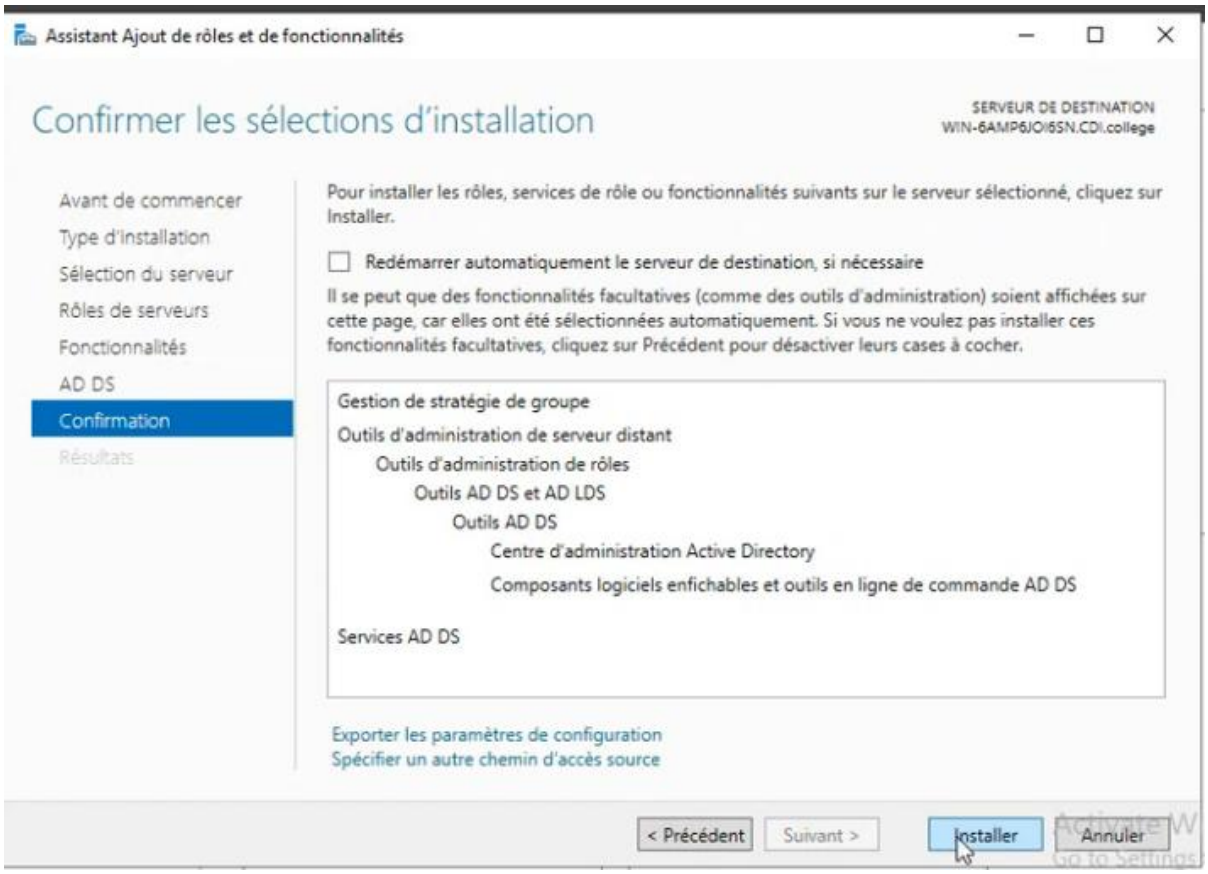
Cliquez sur suivant.



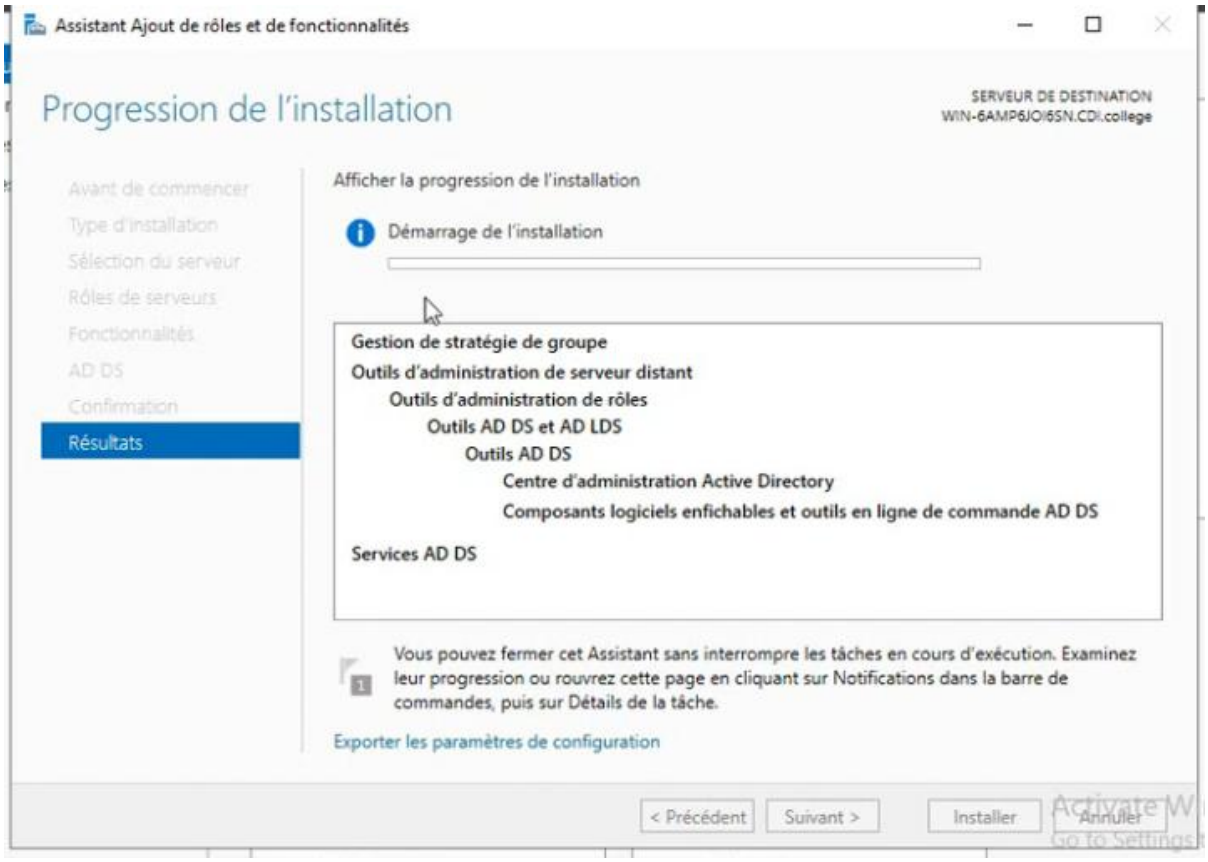
Cliquez sur suivant.



Cliquez sur installer.

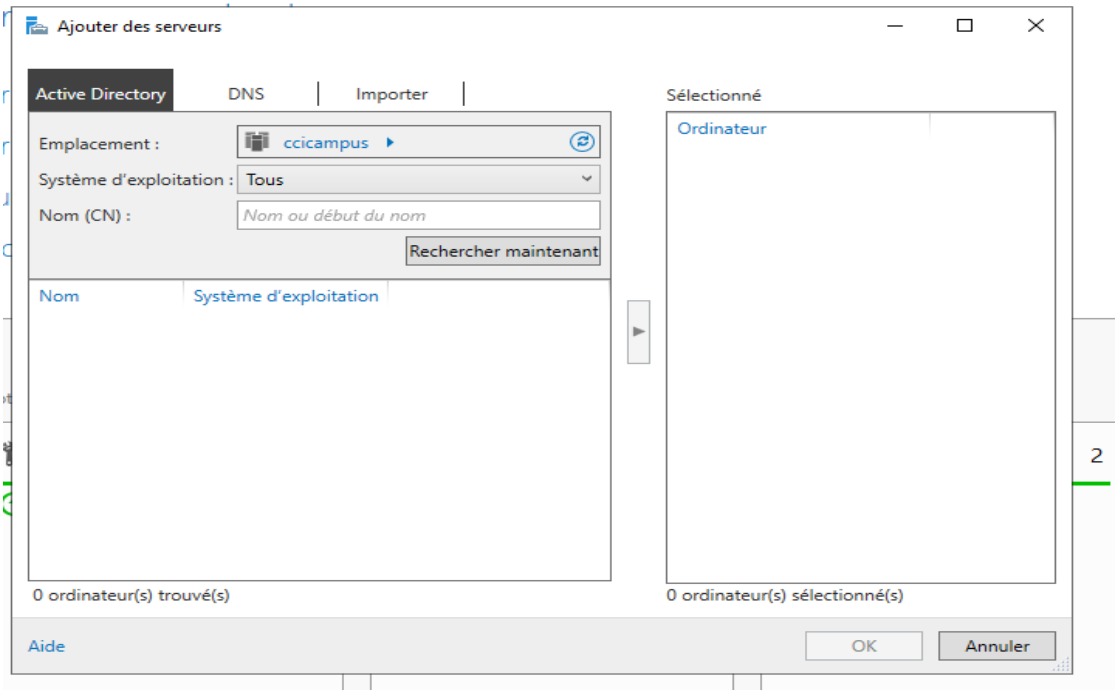


Attendez que l'installation se termine puis fermez la fenêtre lorsque c'est fini.



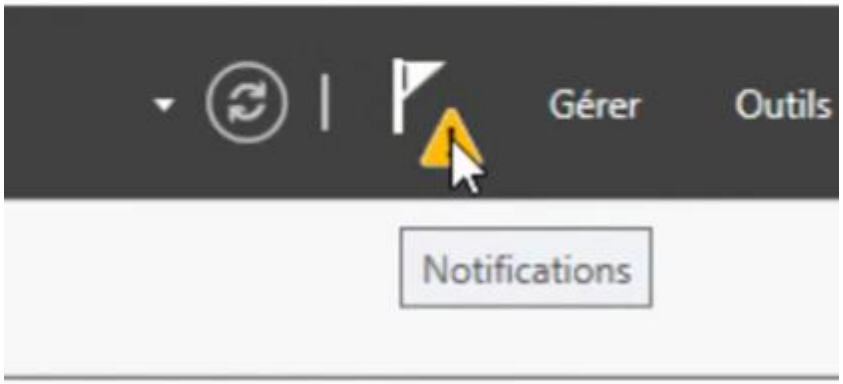
Pour installer des rôles sur un autre serveur (en l'occurrence le serveur secondaire en version core ici), cliquez sur "ajouter d'autres serveurs à gérer".

Recherchez ensuite le nom exact du serveur secondaire que vous voulez joindre et gérer à partir de votre serveur principal.



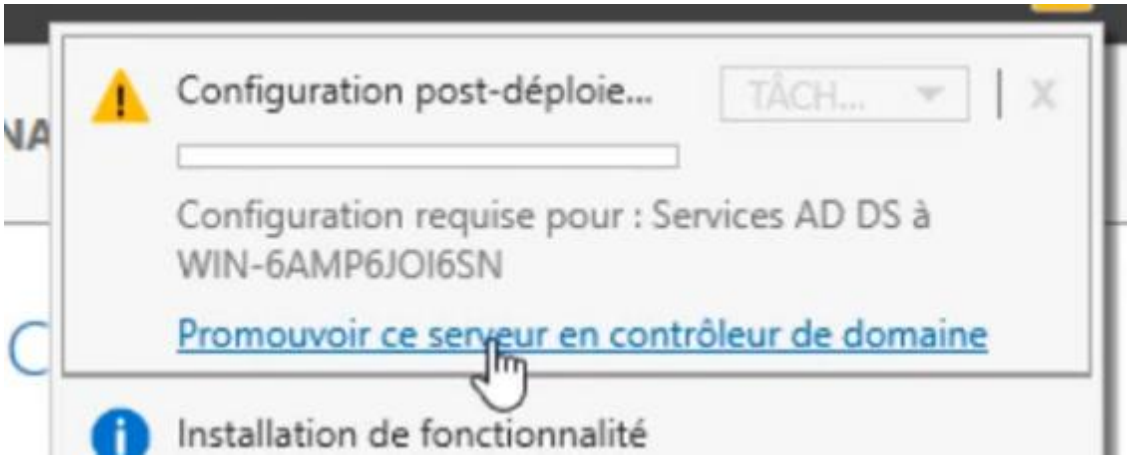
Installation de l'Active Directory et DNS

Cliquez sur le drapeau en haut.

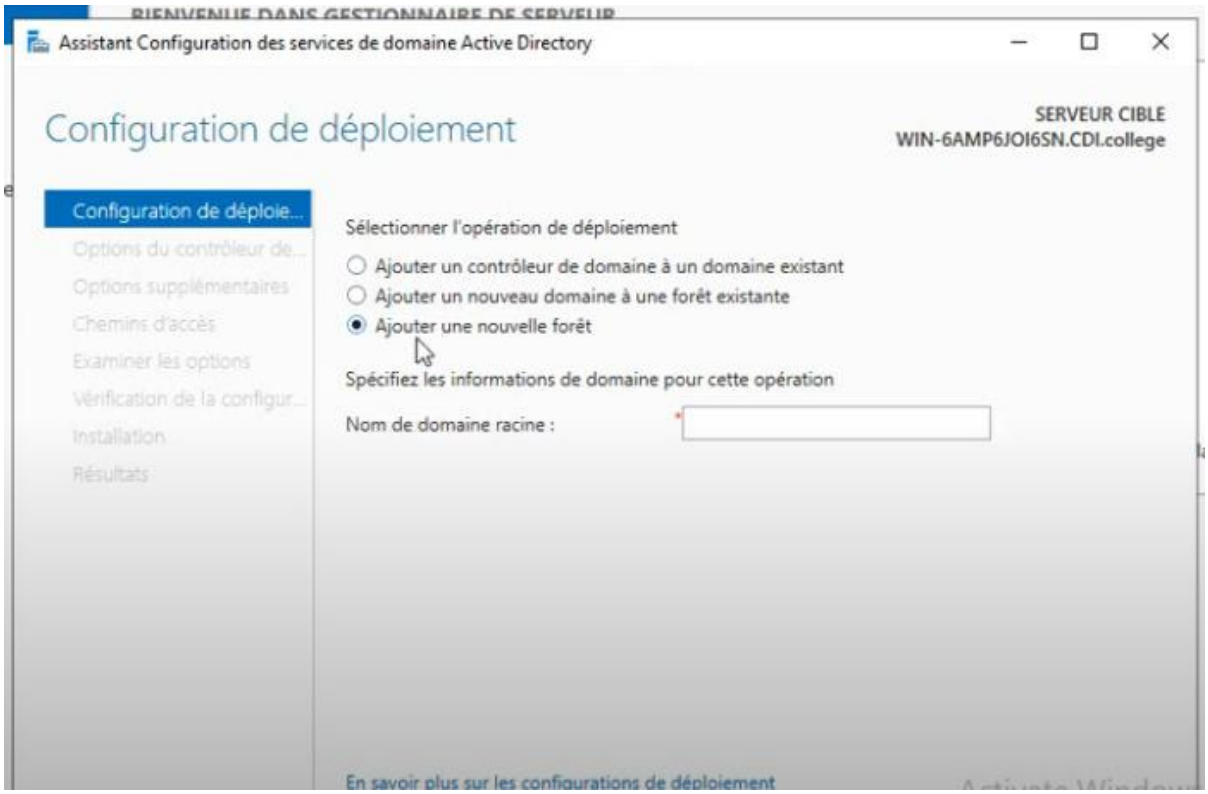


ur local

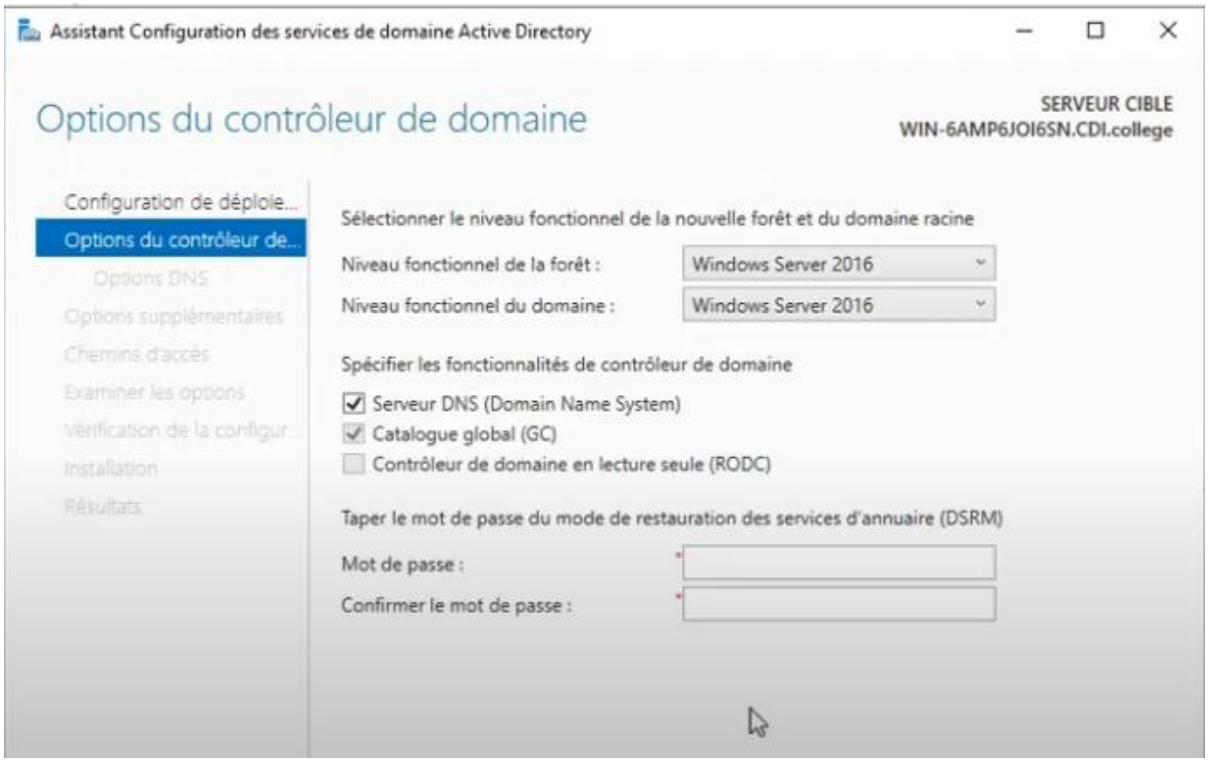
Cliquez sur promouvoir ce serveur en contrôleur de domaine.



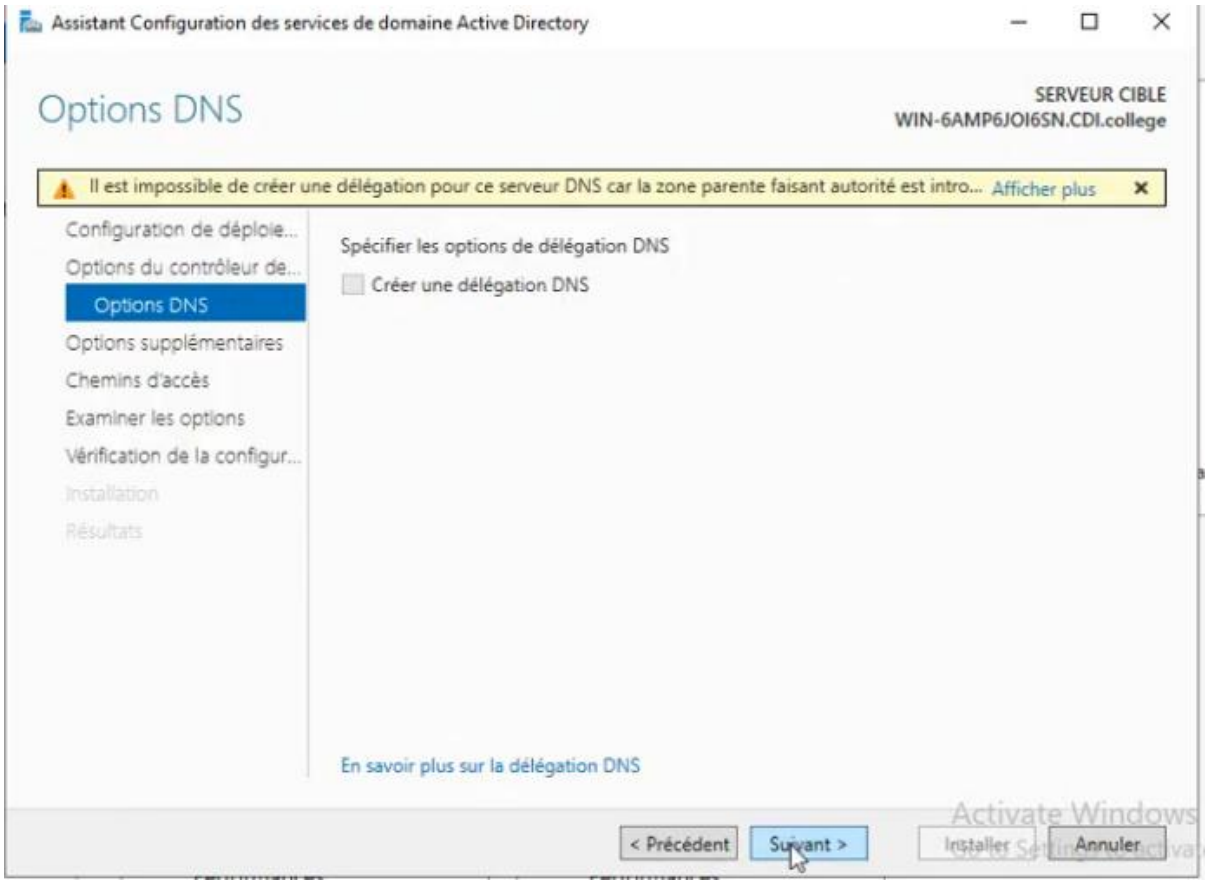
Sélectionnez Ajouter une nouvelle forêt puis entrez le nom de votre nouvelle forêt.



Mettez un mot de passe pour permettre de se connecter sur d'autres postes.

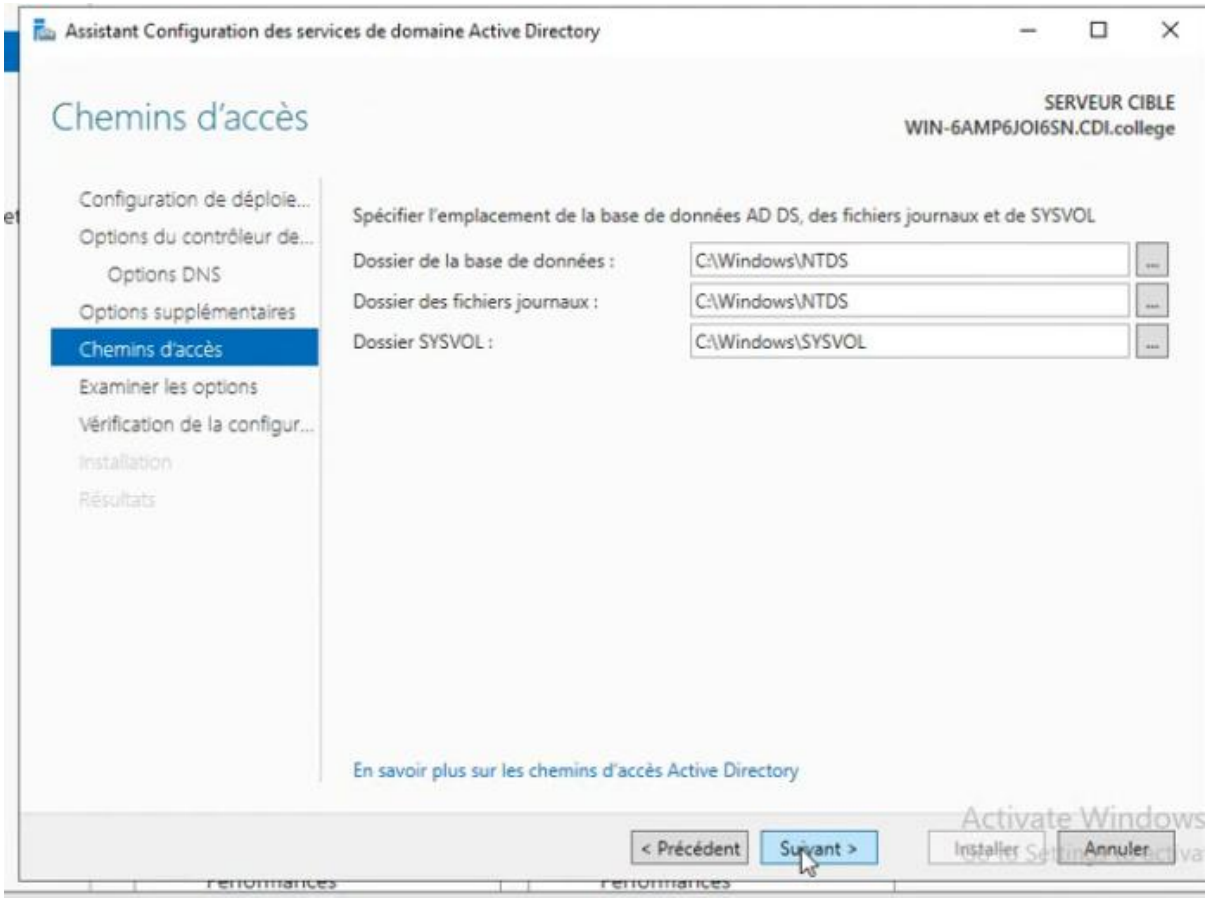


Cliquez sur suivant.

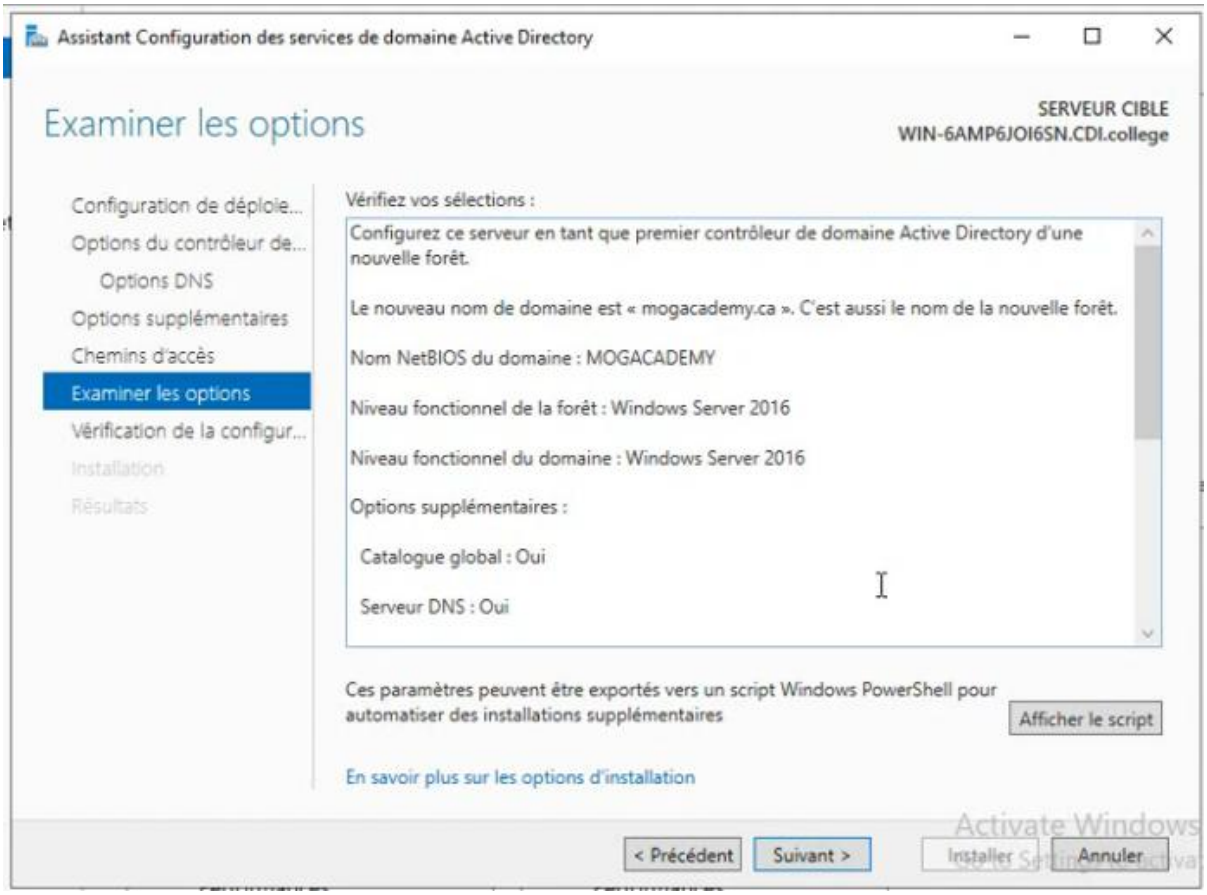


Attendez que Windows vous génère un nom de domaine.

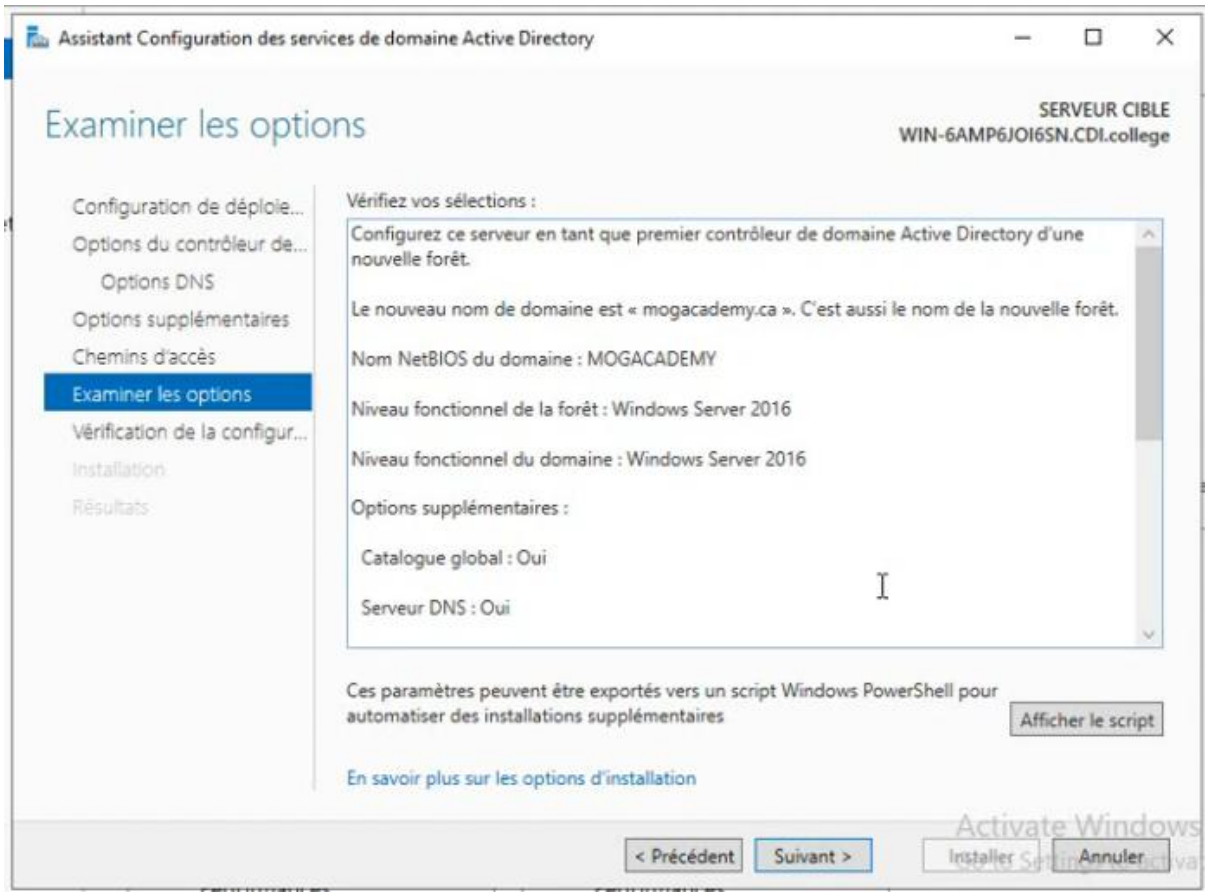
Cliquez sur suivant.



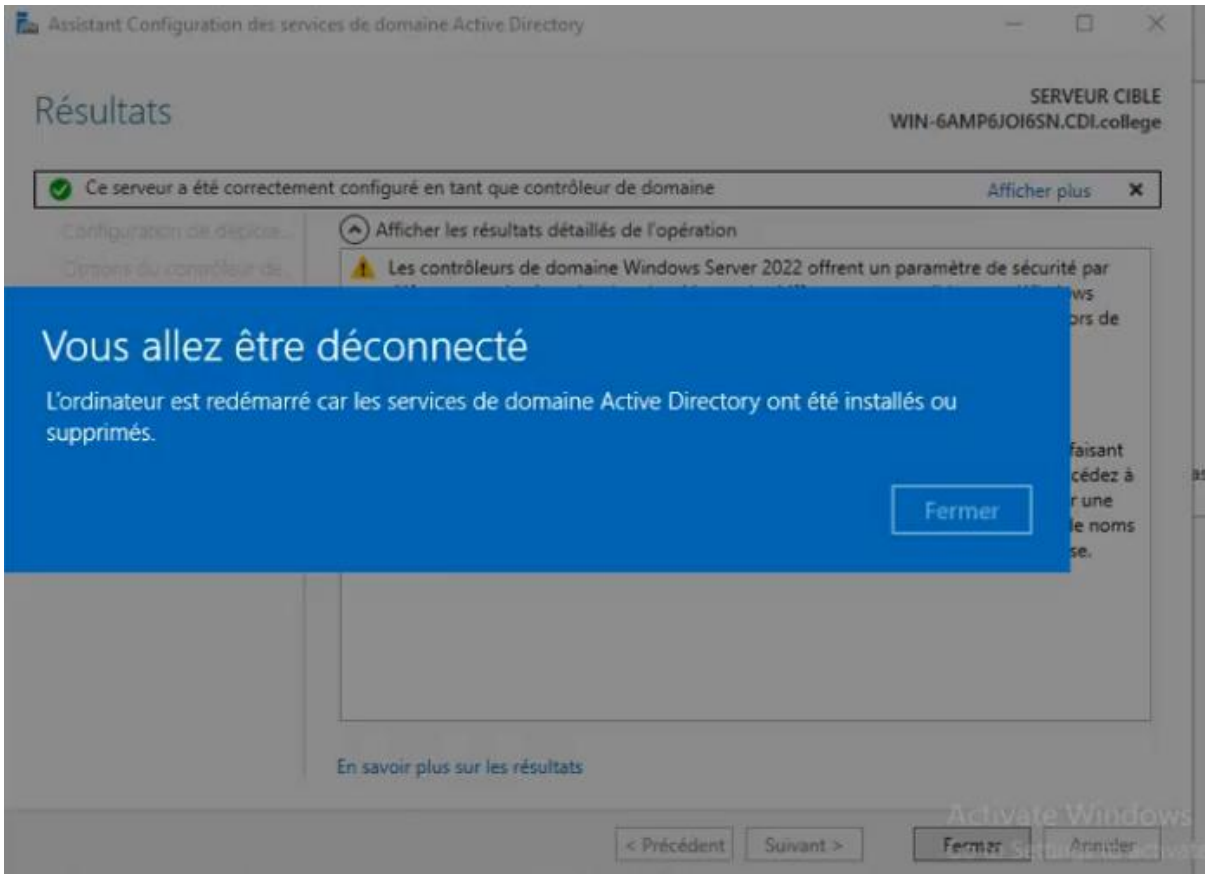
Cliquez sur suivant.



Puis cliquez sur suivant et Installer.



Attendez que ça s'installe puis fermer la fenêtre et redémarrez votre serveur.



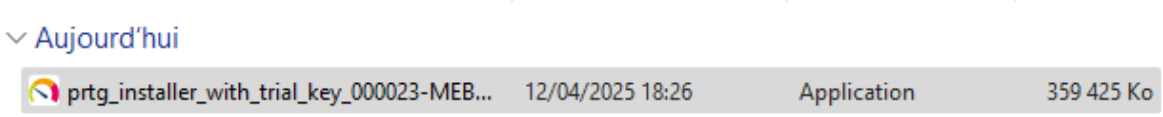
2. Installation PRTG

Aller sur le lien de téléchargement prtg:
https://www.paessler.com/fr/prtg

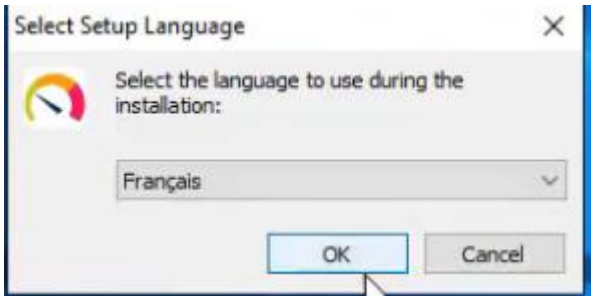
Cliquez ensuite sur “Téléchargement gratuit”:

Laissez l'installeur PRTG se télécharger :

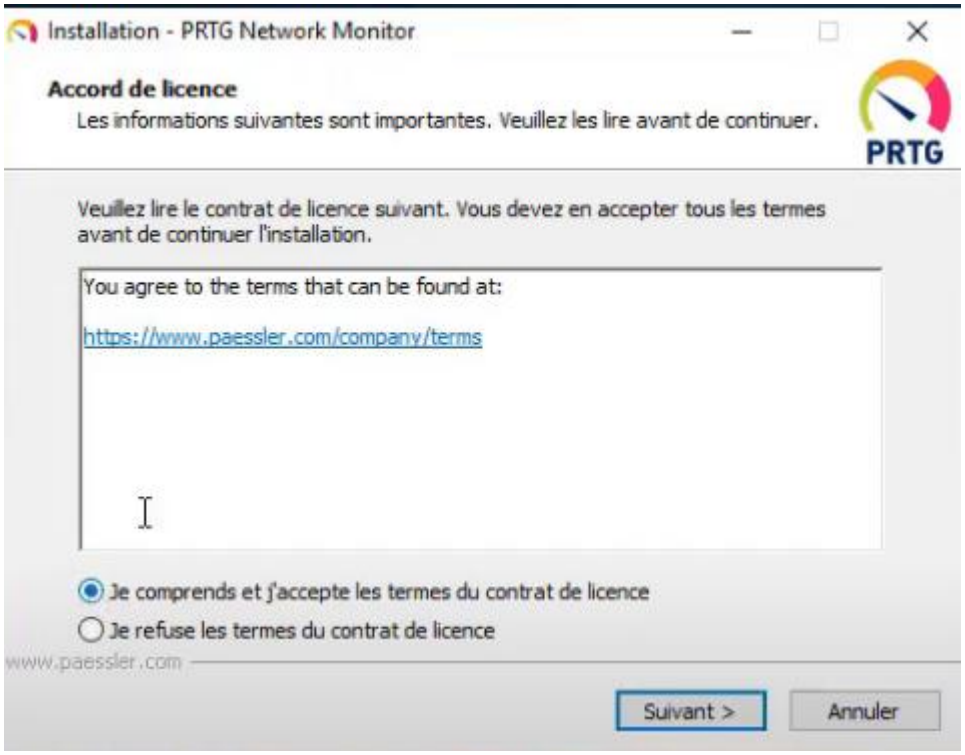
Cliquez sur l'installeur PRTG :



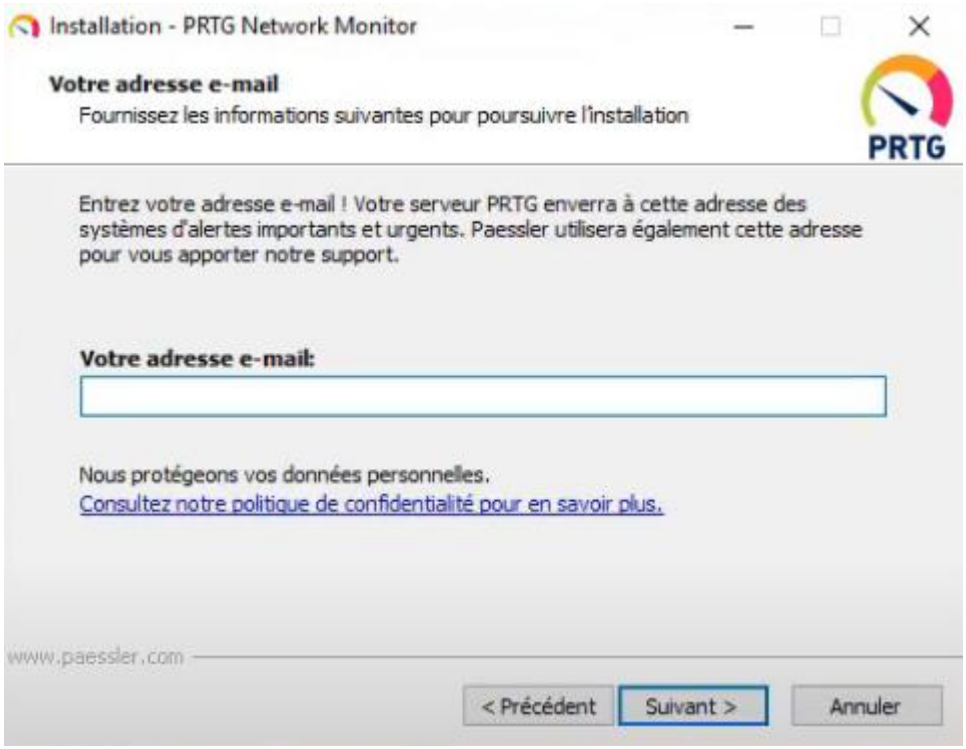
Choisissez votre langue en français :



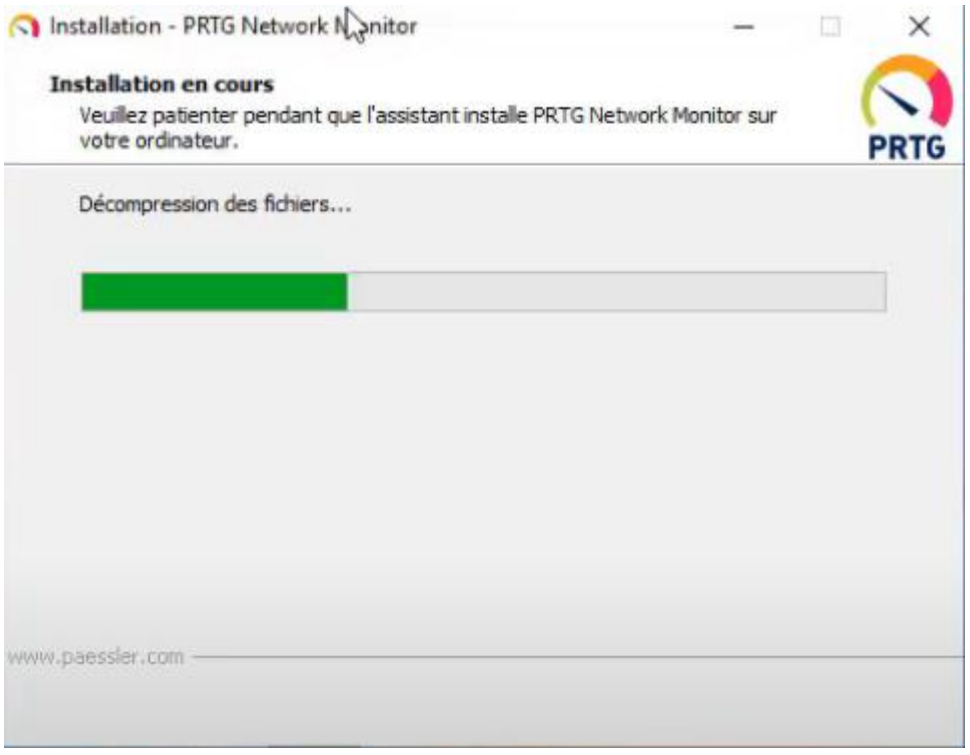
Acceptez les termes puis cliquez sur Suivant.



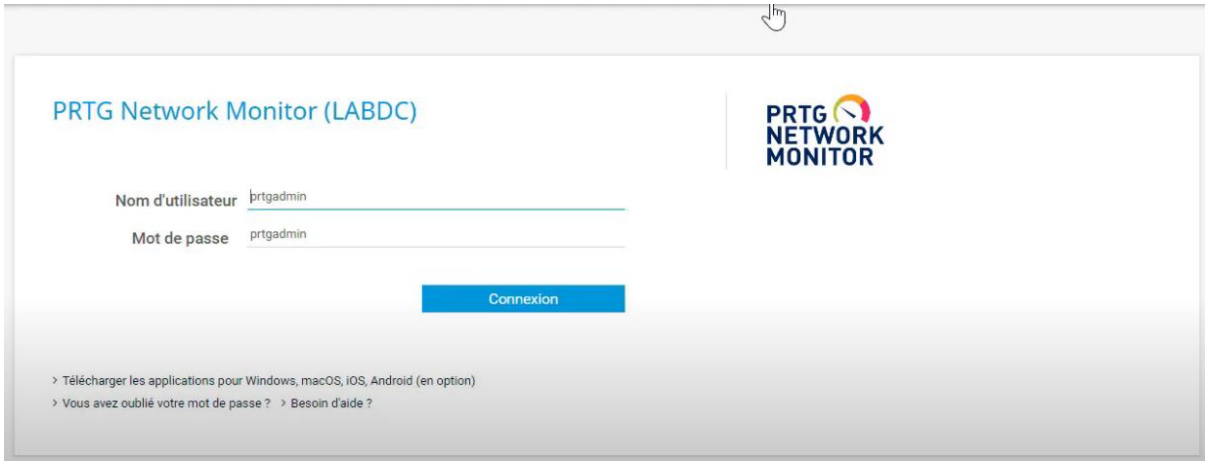
Mettez votre adresse mail (optionnel) puis cliquez sur Suivant.



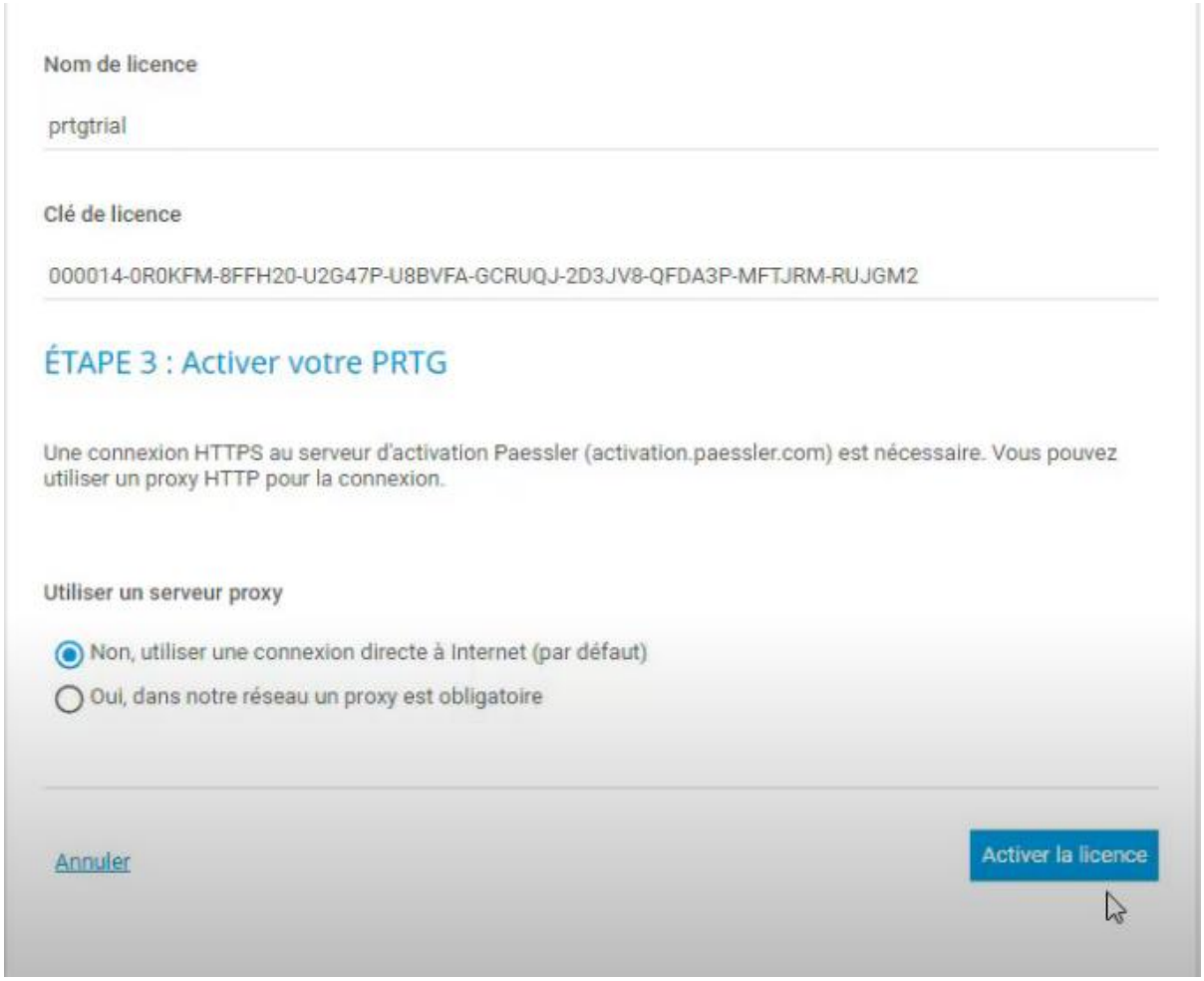
Attendez que PRTG s'installe.



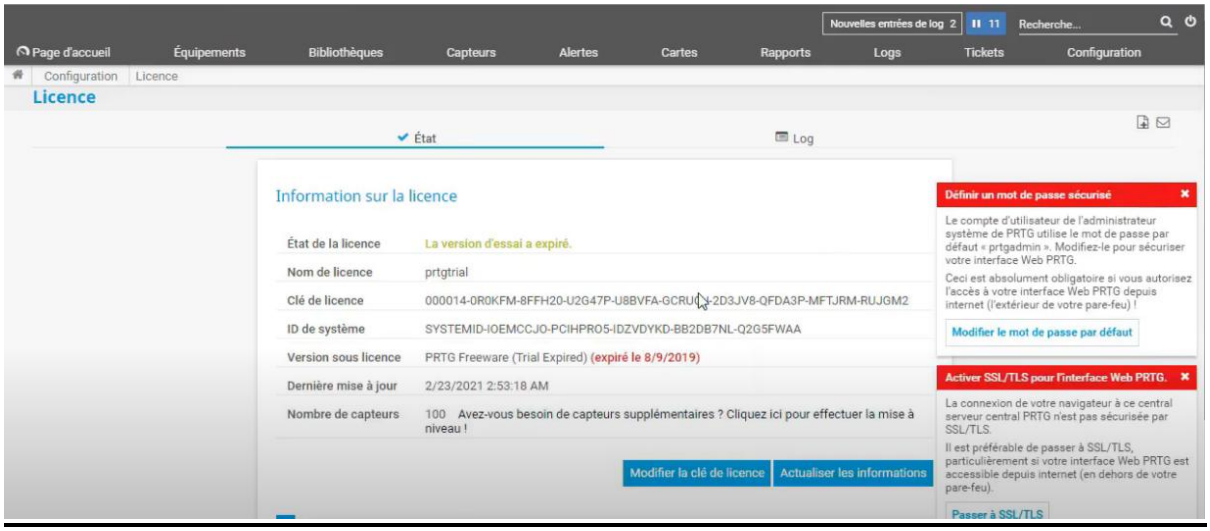
Entrez votre adresse IP pour sur un navigateur web puis entrez vos identifiants admin (par défaut prtgadmin), puis cliquez sur Connexion.



Entrez votre licence qui apparaissez lors du téléchargement de l'installeur PRTG puis cliquez sur Activer la licence.

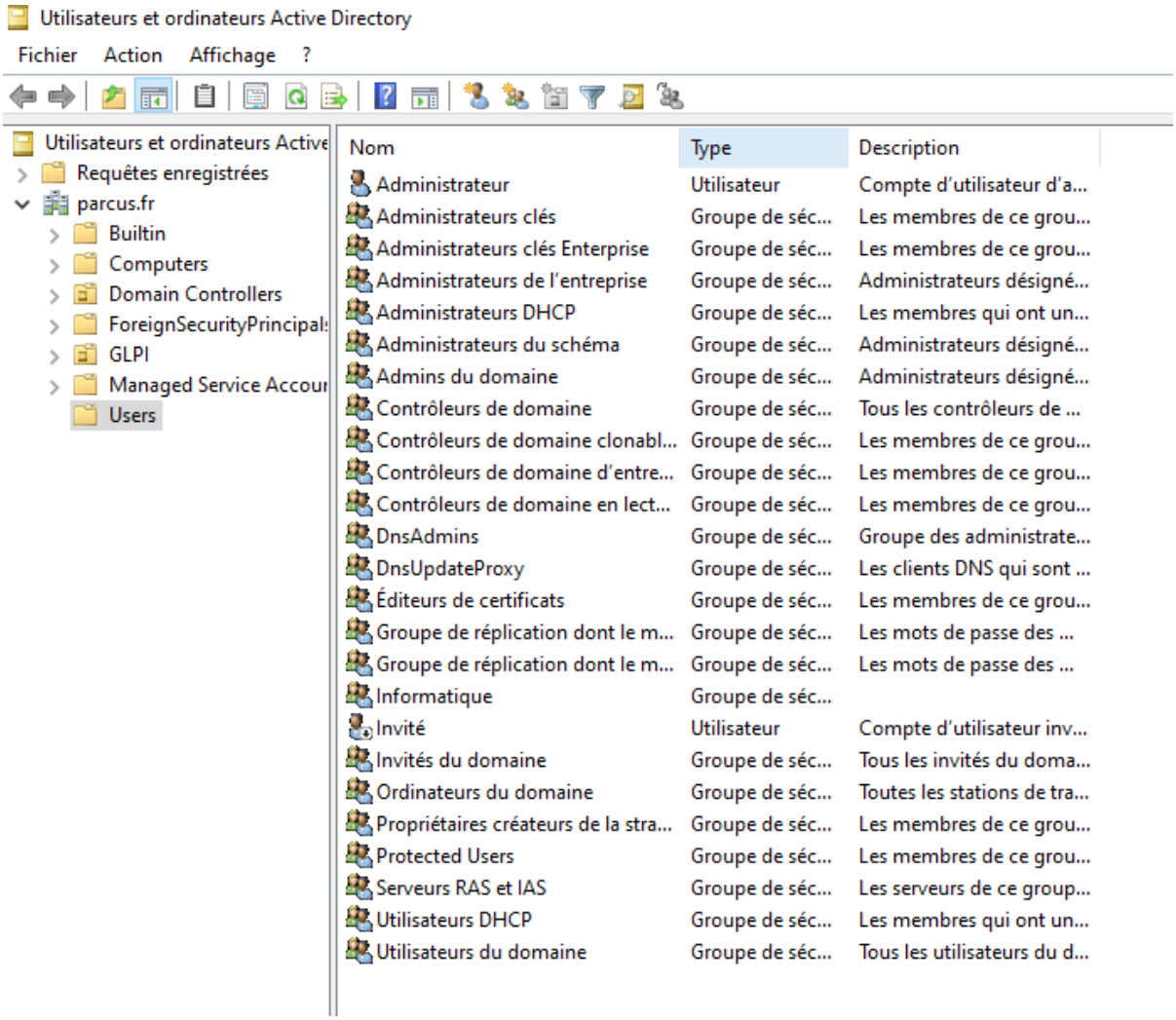


Vous êtes sur la page d'accueil PRTG.



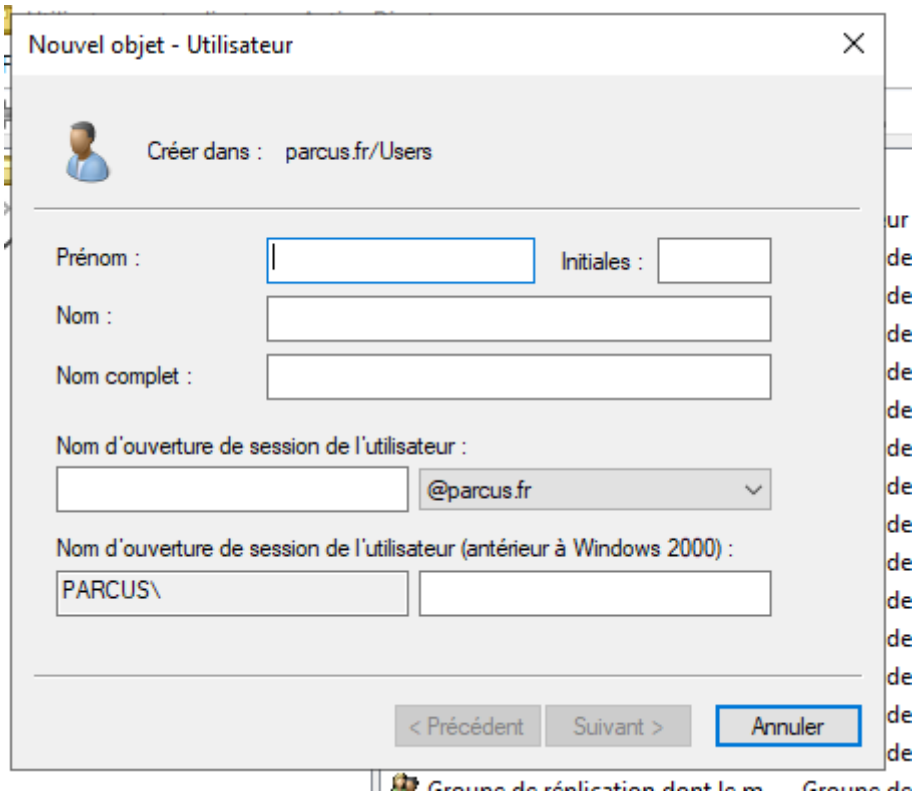
3. Gestion Active Directory

- Ouvrez "Utilisateurs et Ordinateurs Active Directory" (dsa.msc).
- Naviguez jusqu'à l'OU (Unité d'Organisation) où vous souhaitez créer l'utilisateur.

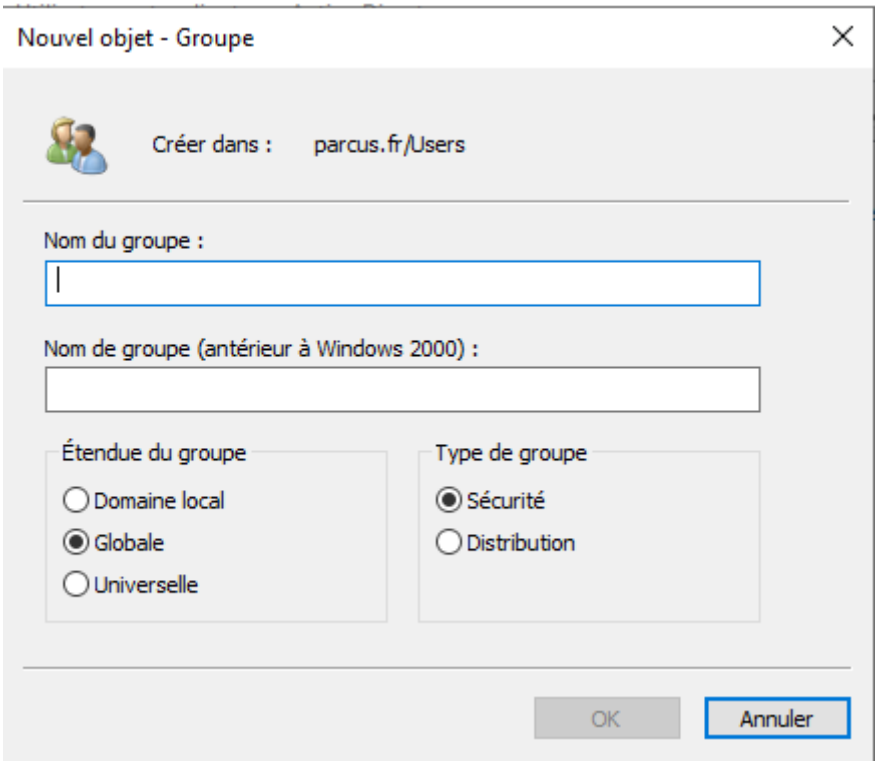


- Cliquez avec le bouton droit, sélectionnez "Nouveau" puis "Utilisateur".

- Remplissez les informations requises et suivez l'assistant pour créer le compte utilisateur.

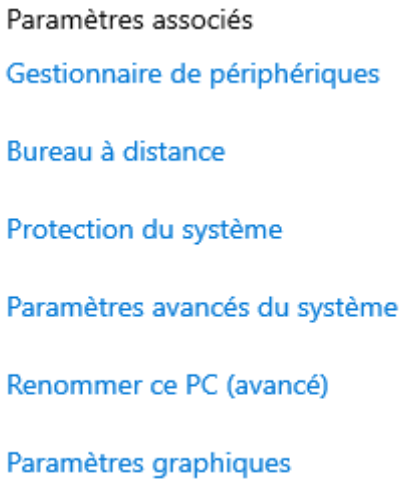


- Les groupes sont utilisés pour simplifier la gestion des permissions.
- Pour créer un groupe, ouvrez "Utilisateurs et Ordinateurs Active Directory".
- Cliquez avec le bouton droit sur l'OU appropriée, sélectionnez "Nouveau" puis "Groupe".
- Nommez le groupe et définissez son type (Distribution ou Sécurité) et sa portée (Domaine local, Global, Universel).

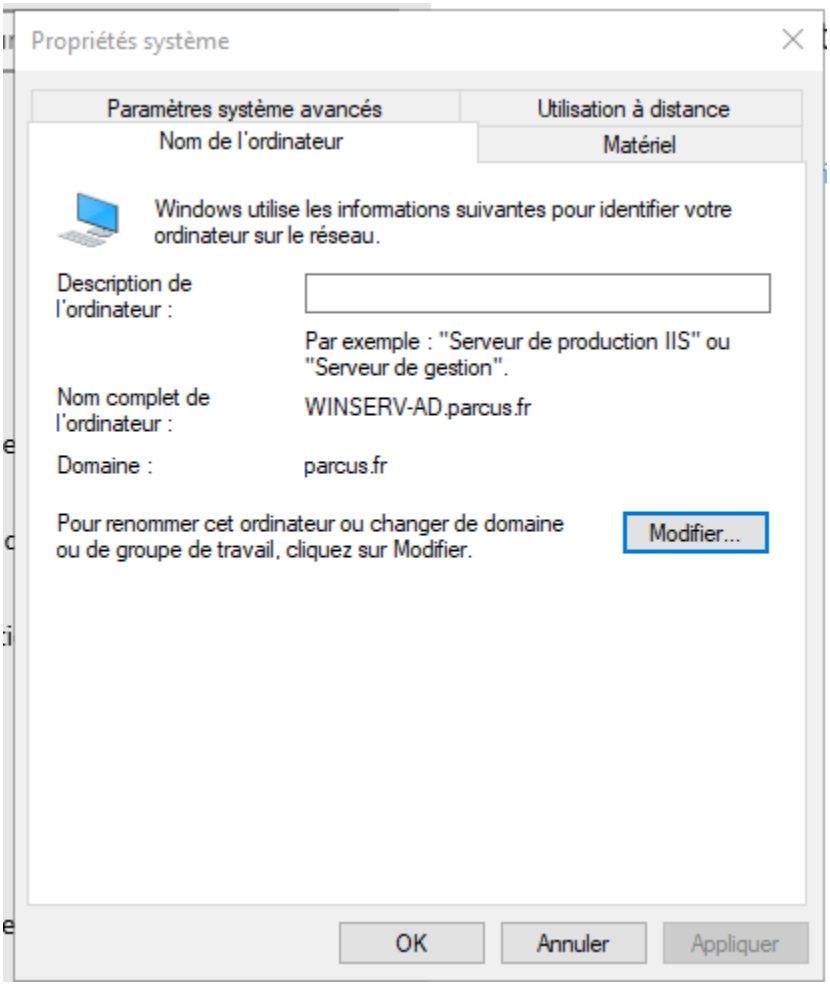

Nouvel objet - Groupe
Créer dans : parcus.fr/Users
Nom du groupe :
Nom de groupe (antérieur à Windows 2000) :
Étendue du groupe
Domaine local
Globale
Universelle
Type de groupe
Sécurité
Distribution
OK
Annuler

Ajout d'un Ordinateur au Domaine

- Sur le poste de travail ou le serveur à ajouter, accédez aux paramètres système.



- Cliquer sur "Renommer ce PC (avancé)".
- Sous "Nom de l'ordinateur", cliquez sur "Modifier".



- Sélectionnez "Domaine", entrez le nom de votre domaine, puis suivez les instructions pour redémarrer l'ordinateur.

Création et Gestion des OU

1. Les Unités d'Organisation permettent de structurer et de gérer les objets AD de manière hiérarchique.
2. Pour créer une OU, ouvrez "Utilisateurs et Ordinateurs Active Directory".
3. Cliquez avec le bouton droit sur le domaine ou l'OU existante, sélectionnez "Nouveau" puis "Unité d'Organisation".
4. Nommez l'OU et configurez les paramètres nécessaires.

Conclusion :

La mise en place et l'utilisation combinée d'Active Directory, DNS et DHCP renforcent la sécurité, la stabilité et l'efficacité des infrastructures réseau. Active Directory facilite la gestion centralisée des utilisateurs et des ressources, tandis que DNS et DHCP assurent respectivement une communication fiable et une configuration simplifiée des adresses IP. En suivant les étapes et les recommandations présentées dans ce guide, vous pourrez exploiter pleinement ces outils pour optimiser la gestion de votre réseau et améliorer l'expérience utilisateur.

Documentation d'installation Modoboa (Ubuntu)

Introduction

Modoboa est un serveur de messagerie 100% gratuit et open source. Il s'agit d'un serveur de messagerie Python hautement évolutif avec simplicité et vitesse à la base. Modoboa rassemble les meilleurs outils open source pour installer, configurer et sécuriser votre propre serveur de messagerie.

Installation

Installer python3:

```
root@mail:~# apt-get install python3-virtualenv python3-pip git curl gnupg2 -y
```

Installer le paquet Modoboa:

```
root@mail:~# git clone https://github.com/modoboa/modoboa-installer
```

Donner la permission au dossier modoboa-installer:

```
root@mail:~# chmod -R 777 modoboa-installer
```

Aller dans le dossier modoboa-installer:

```
root@mail:~# cd modoboa-installer
```

Créez un installeur modoboa:

```
root@mail:~/modoboa-installer# python3 ./run.py --stop-after-configfile-check yourdomain.com
Welcome to Modoboa installer!

Configuration file installer.cfg not found, creating new one.
```

Modifier le fichier d'installation créé :

```
root@mail:~/modoboa-installer# nano installer.cfg
```

```
[general]
hostname = mail.%(domain)s

[certificate]
generate = true
type = self-signed

[letsencrypt]
email = admin@example.com

[database]
engine = postgres
host = 127.0.0.1
install = true

[postgres]
user = postgres
password =

[mysql]
user = root
password = dnnUzG2BsM9RZ7PC
charset = utf8
collation = utf8_general_ci
```

Lancer l'installation de Modoboa:

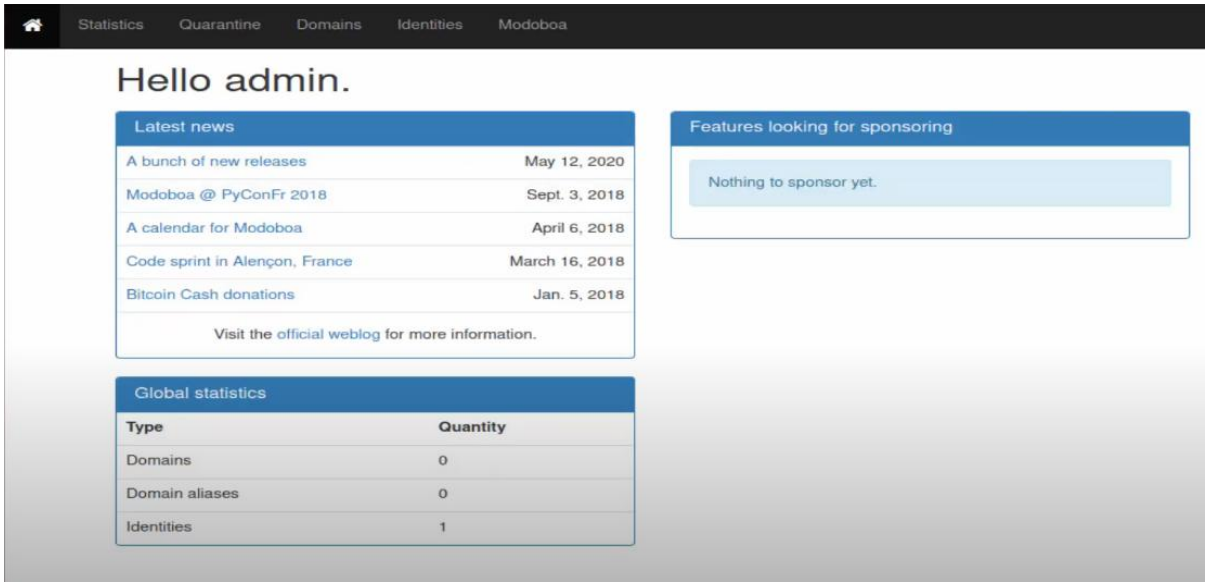
```
root@mail:~/modoboa-installer# python3 ./run.py --interactive yourdomain.com
Welcome to Modoboa installer!

Warning:
Before you start the installation, please make sure the following DNS records exist for domain 'yourdomain.c
om':
  mail IN A   <IP ADDRESS OF YOUR SERVER>
       IN MX  mail.yourdomain.com.

Your mail server will be installed with the following components:
modoboa automx amavis clamav dovecot nginx razor postfix postwhite spamassassin uwsgi radicale opendkim
Do you confirm? (Y/n)
```

Vérifier si le site modoboa est en ligne:

```
root@mail:~/modoboa-installer# systemctl restart nginx ; systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2022-02-07 18:47:35 PST; 7ms ago
       Docs: man:nginx(8)
    Process: 213638 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, statu
    Process: 213640 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0/SUCCE
   Main PID: 213641 (nginx)
      Tasks: 3 (limit: 4593)
     Memory: 3.4M
     CGroup: /system.slice/nginx.service
             ├─213641 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
             ├─213642 nginx: worker process
             └─213643 nginx: worker process
```

Allez dans un navigateur web est entrez l'adresse ip du serveur modoboa puis entrez vos identifiants admin :

Vous êtes maintenant dans Modoboa.



Configuration d’Asterisk

09/04/2025

1) Installation d'Asterisk

L'installation et la configuration d'Asterisk se fera sur le même serveur ubuntu que Modoboa, donc pas besoin de montrer comme configurer le serveur.

A) Mise à jour du serveur + installations des dépendances requises

Mettre à jour le serveur avec cette commande.

```
hollo@hollo:~$ sudo apt update && sudo apt upgrade -y
```

Installer les dépendances avec cette commande.

```
hollo@hollo:~$ sudo apt install build-essential git curl wget subversion libncurses5-dev libxml2-dev
 libsqlite3-dev uuid-dev libjansson-dev libssl-dev -y
```

B) Téléchargement et pré-installation de Asterisk

Accéder au répertoire /usr/src.

```
hollo@hollo:~$ cd /usr/src
hollo@hollo:/usr/src$
```

Télécharger le paquet de Asterisk via le site web officiel.

```
hollo@hollo:/usr/src$ sudo wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-20-cur
rent.tar.gz
```

L’installation n’est pas très longue.

```
--2025-04-12 14:12:47--  http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-20-current.ta
r.gz
Resolving downloads.asterisk.org (downloads.asterisk.org)... 2604:a880:400:d0::14:9001, 165.22.184.1
9
Connecting to downloads.asterisk.org (downloads.asterisk.org)|2604:a880:400:d0::14:9001|:80... conne
cted.
HTTP request sent, awaiting response... 200 OK
Length: 28412463 (27M) [application/octet-stream]
Saving to: ‘asterisk-20-current.tar.gz’

asterisk-20-current.tar.  22%[======>                          ]   6,05M   479KB/s    eta 26s    _
```

Extraire le paquet téléchargé dans le répertoire.

```
hollo@hollo:/usr/src$ sudo tar xvf asterisk-20-current.tar.gz
```

Accéder au répertoire de Asterisk.

```
hollo@hollo:/usr/src$ cd asterisk-20.13.0/
```

Démarrer la pré-installation de Asterisk en effectuant ces 2 commandes.

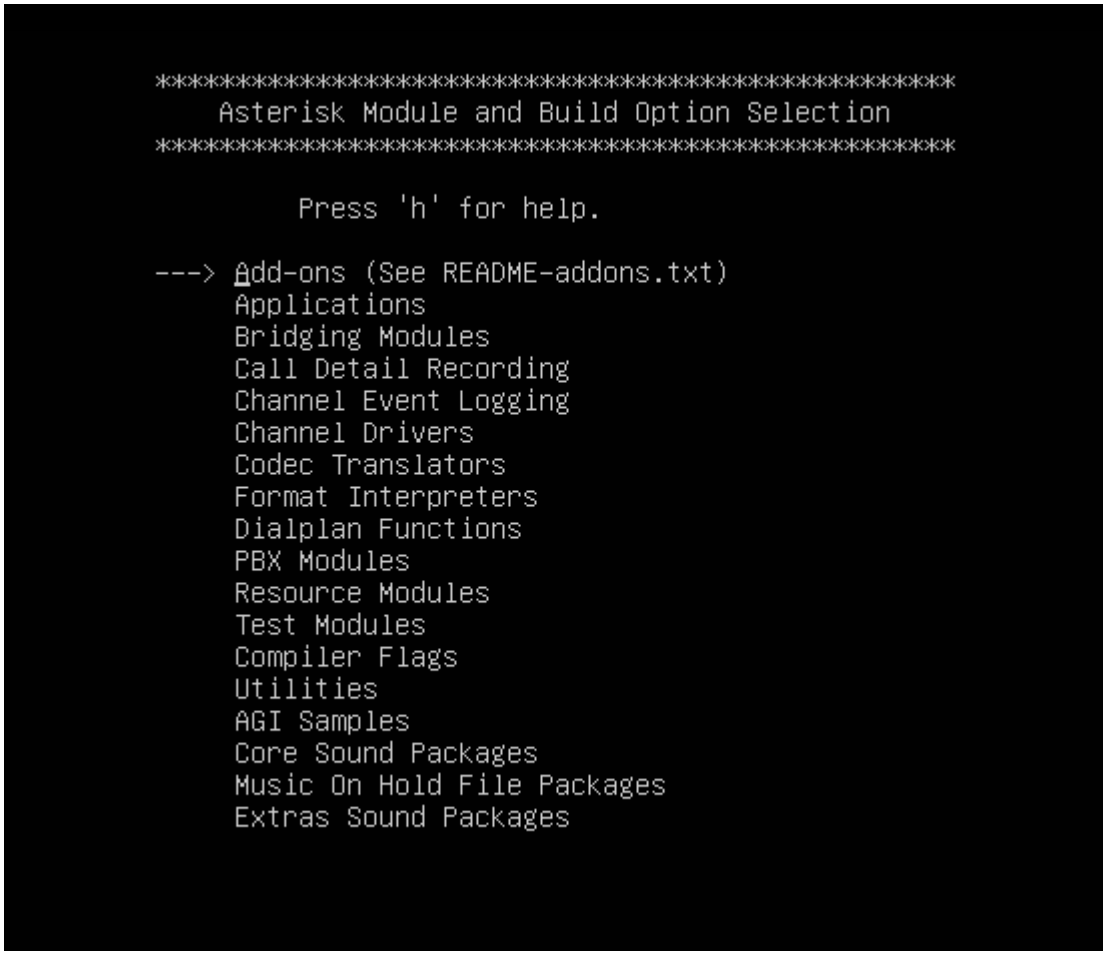
```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo contrib/scripts/install_prereq install
```

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo ./configure_
```

Effectuer cette commande.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo make menuselect
```

Une fois sur cette partie cliquer sur la touche S puis Q. Il n'y a aucune modification à apporter.



C) Compilation et installation de Asterisk

Effectuer cette commande.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo make -j$(nproc)_
```

Lancer cette commande.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo make install
```

Lancer cette commande.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo make samples_
```

Effectuer cette commande.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo make config
```

Lancer cette commande pour terminer l'installation de Asterisk.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo ldconfig_
```

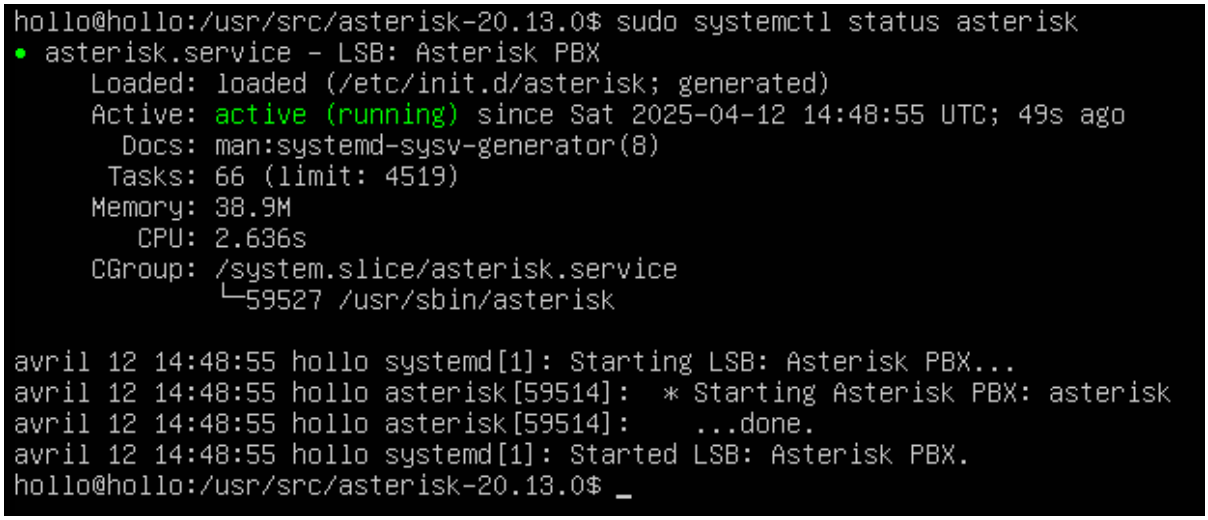
Démarrer Asterisk.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo systemctl start asterisk
```

Activer Asterisk.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo systemctl enable asterisk
```

Vérifier si Asterisk est bien actif.



Accéder à la console de Asterisk pour voir si ça fonctionne.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo asterisk -rvv
```

Si ceci s’affiche, Asterisk s’est bien installé.

```
Asterisk 20.13.0, Copyright (C) 1999 - 2025, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=========================================================================
Connected to Asterisk 20.13.0 currently running on hollo (pid = 59527)
hollo*CLI>
```

Faire exit pour quitter la console Asterisk.

```
hollo*CLI> exit
Asterisk cleanly ending (0).
Executing last minute cleanups
hollo@hollo:/usr/src/asterisk-20.13.0$ _
```

2) Configuration des utilisateurs SIP pour le softphone

Accéder au fichier de configuration pjsip.conf.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo nano /etc/asterisk/pjsip.conf
```

Chercher cette partie, il faut la modifier.

```
; Basic UDP transport
;
;[transport-udp]
;type=transport
;protocol=udp    ;udp,tcp,tls,ws,wss,flow
;bind=0.0.0.0
```

Voici le rendu final pour que le transport UDP fonctionne.

```
; Basic UDP transport
;
[transport-udp]
type=transport
protocol=udp    ;udp,tcp,tls,ws,wss,flow
bind=0.0.0.0
```

Descendre tout en bas du fichier pour ajouter un nouvel utilisateur SIP.

Voici un exemple de configuration pour un utilisateur (1001 ici).

```
[1001]
type=endpoint
context=internal
disallow=all
allow=ulaw
auth=auth1001
aors=1001

[auth1001]
type=auth
auth_type=userpass
username=1001
password=p@ssw0rd

[1001]
type=aor
max_contacts=1
```

Créer un deuxième utilisateur (1002 par exemple) afin de réaliser des tests plus tard.

Faire Ctrl + X, puis Y et Enter pour quitter et sauvegarder le fichier.

Accéder au fichier du plan de numérotation.

```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo nano /etc/asterisk/extensions.conf
```

Ajouter ces lignes à la fin du fichier puis quitter et sauvegarder.

```
[internal]
exten => 1001,1,Dial(PJSIP/1001)
exten => 1002,1,Dial(PJSIP/1002)
```

Redémarrer Asterisk.

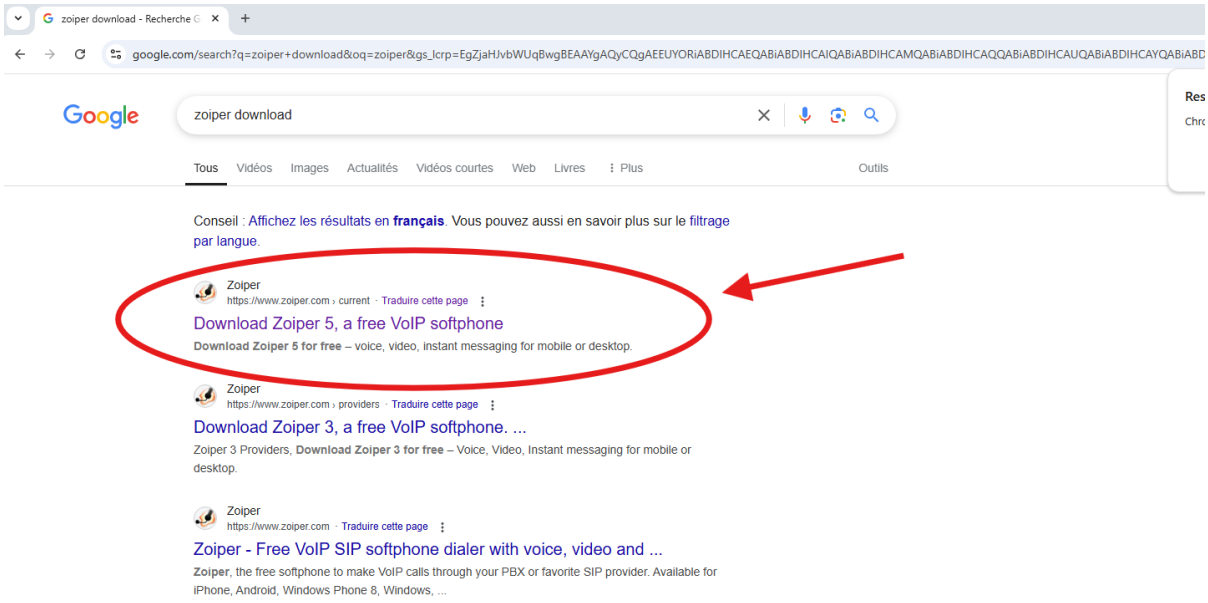
```
hollo@hollo:/usr/src/asterisk-20.13.0$ sudo systemctl restart asterisk
```

3) Installation et configuration d'un client Softphone

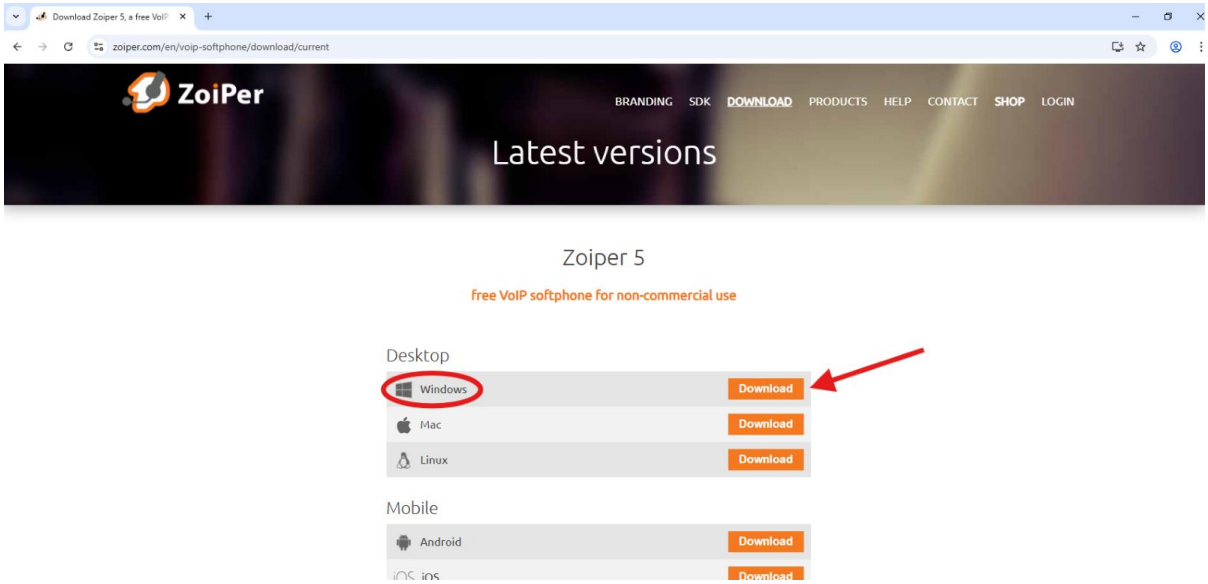
Accéder à une machine Windows Client connectée au domaine.

Nous allons installer Zoiper, un client Softpone très fiable et répandu.

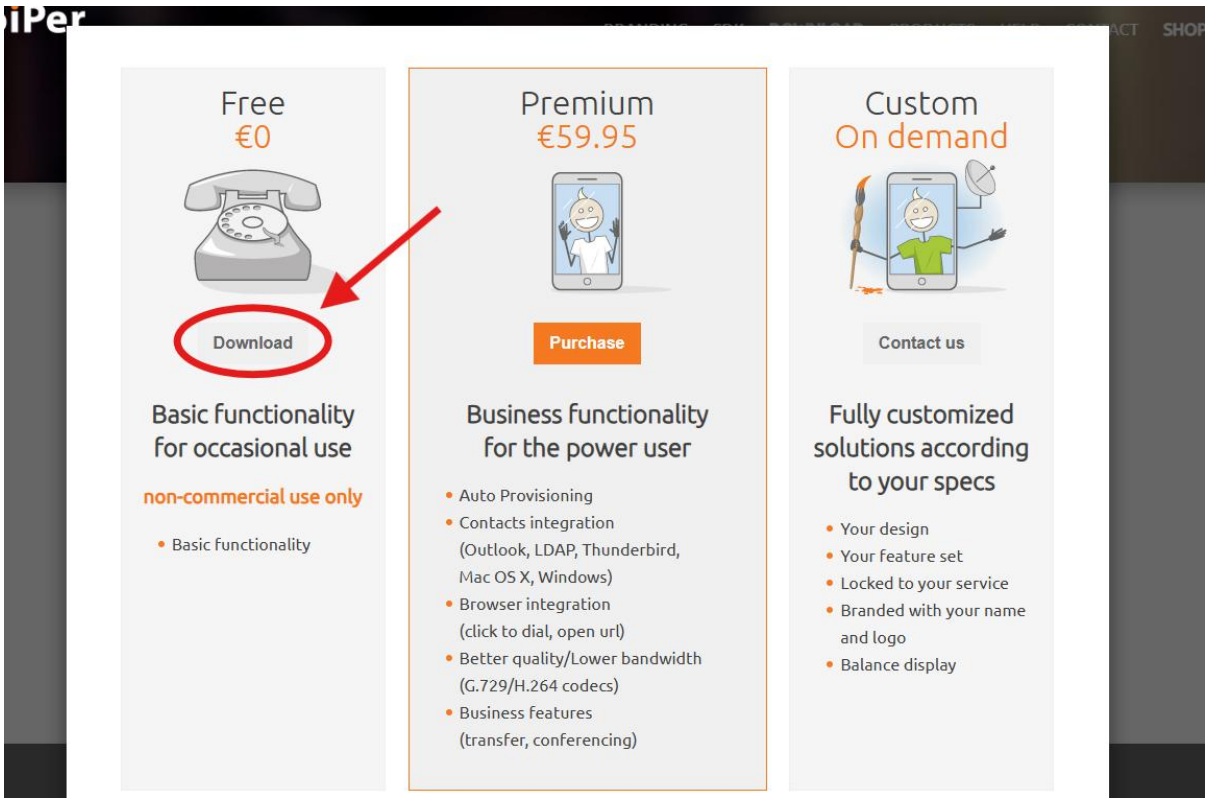
Rechercher Zoiper download et accéder au premier lien.



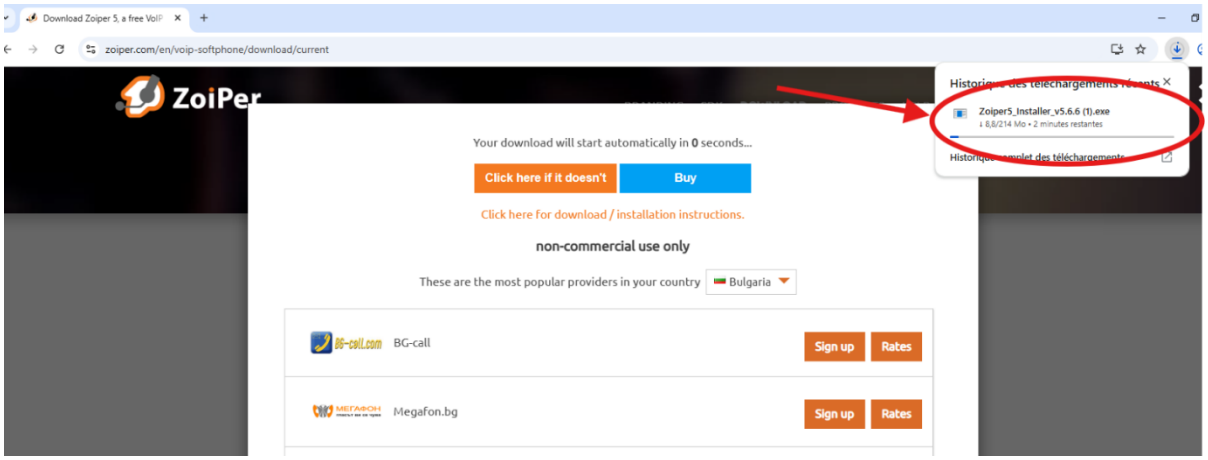
Choisir la version Windows.



Dans le cadre du projet, choisir la version gratuite.

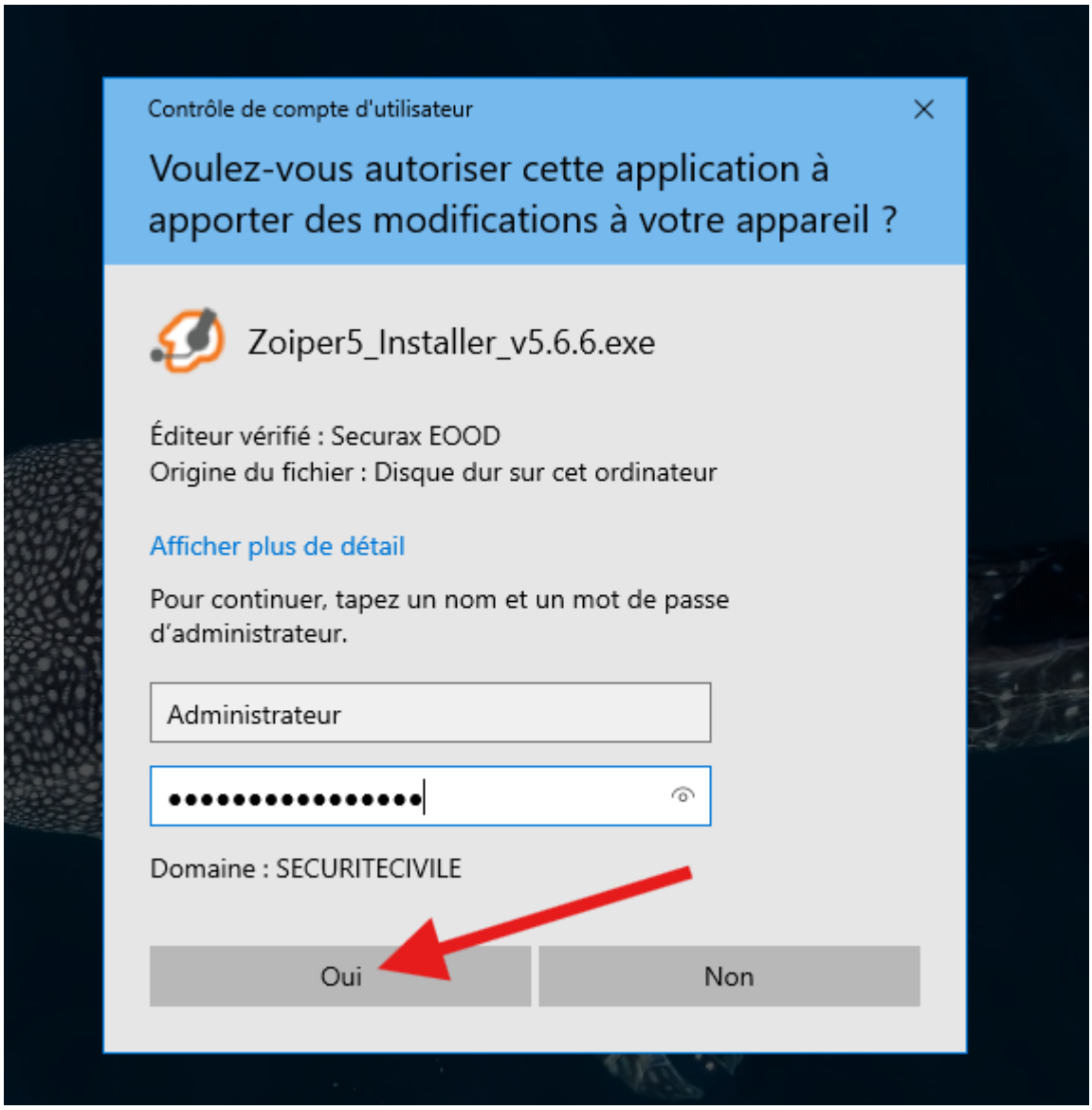


L’installation se lancera tout seul, attendre la fin.

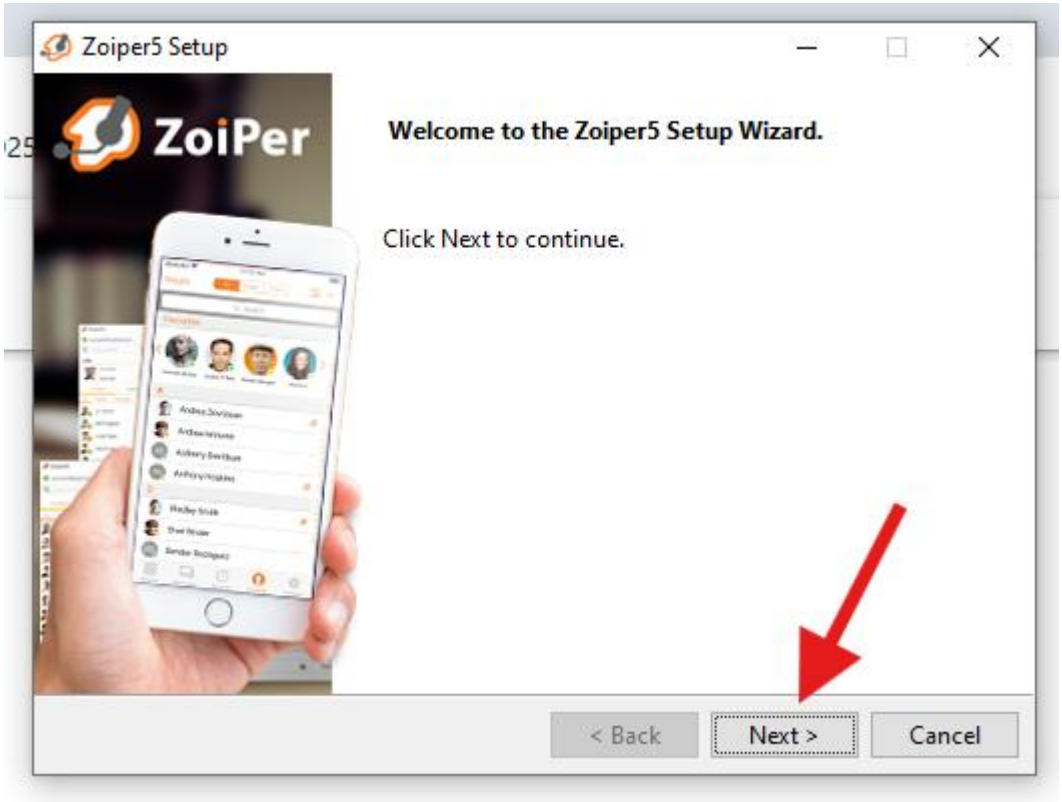


Une fois installer, lancer le programme d’installation de Zoiper.

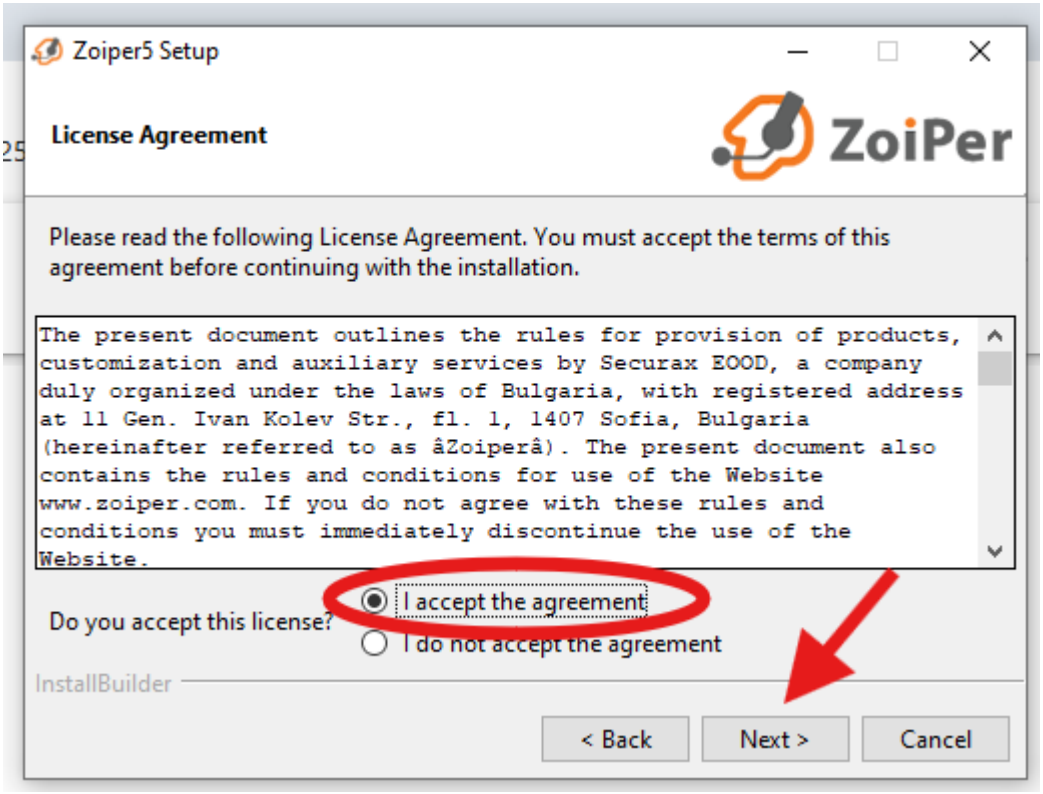
Entrer les droits admins puis cliquer sur OUI.



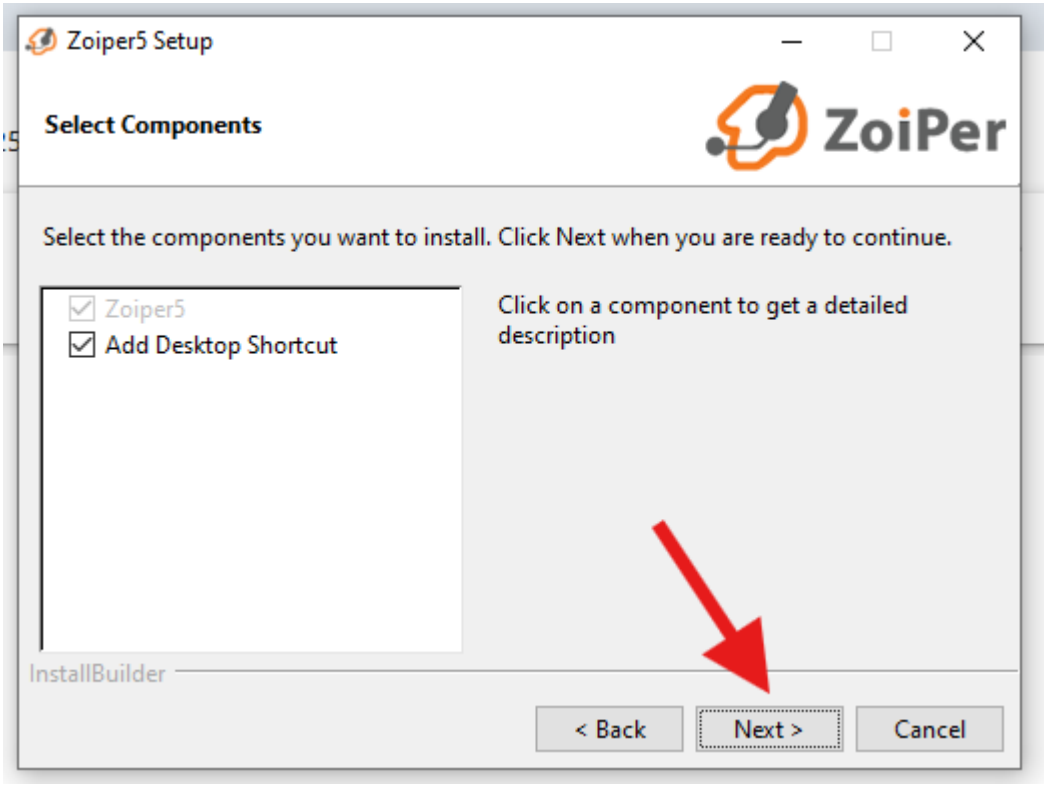
Cliquer sur Next.



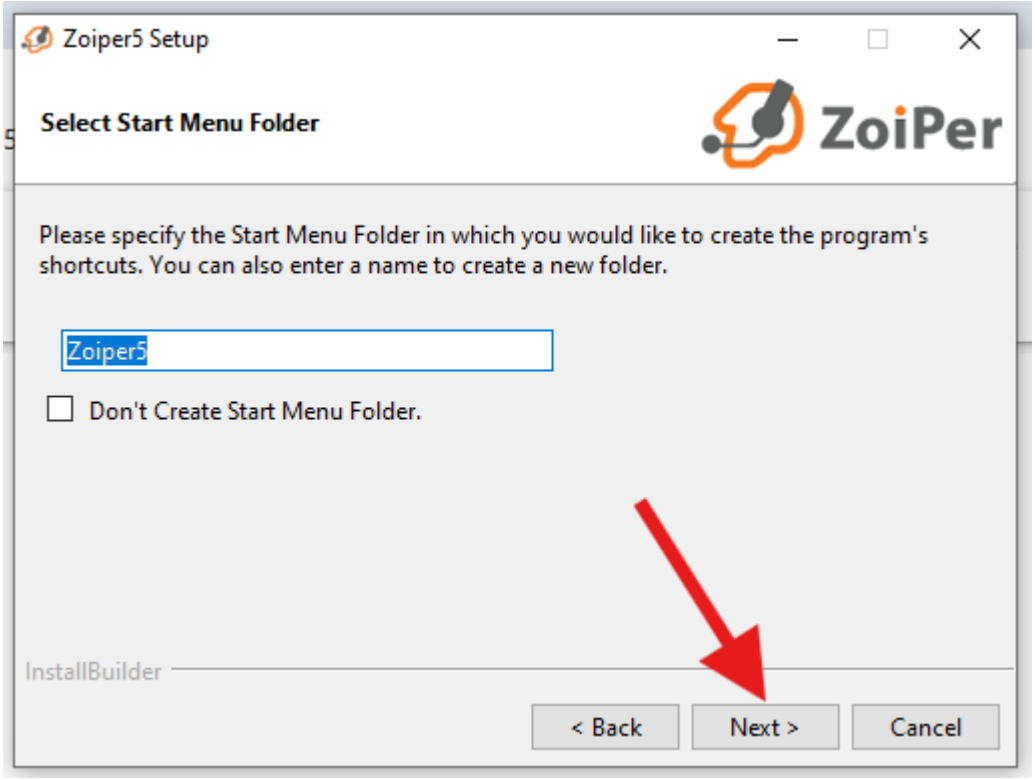
Accepter les termes de licence puis cliquer sur Next.


Zoiper5 Setup
License Agreement
ZoiPer
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
The present document outlines the rules for provision of products, customization and auxiliary services by Securax EOOD, a company duly organized under the laws of Bulgaria, with registered address at 11 Gen. Ivan Kolev Str., fl. 1, 1407 Sofia, Bulgaria (hereinafter referred to as âZoiperâ). The present document also contains the rules and conditions for use of the Website www.zoiper.com. If you do not agree with these rules and conditions you must immediately discontinue the use of the Website.
Do you accept this license?
I accept the agreement
I do not accept the agreement
InstallBuilder
< Back
Next >
Cancel

Cliquer sur Next.

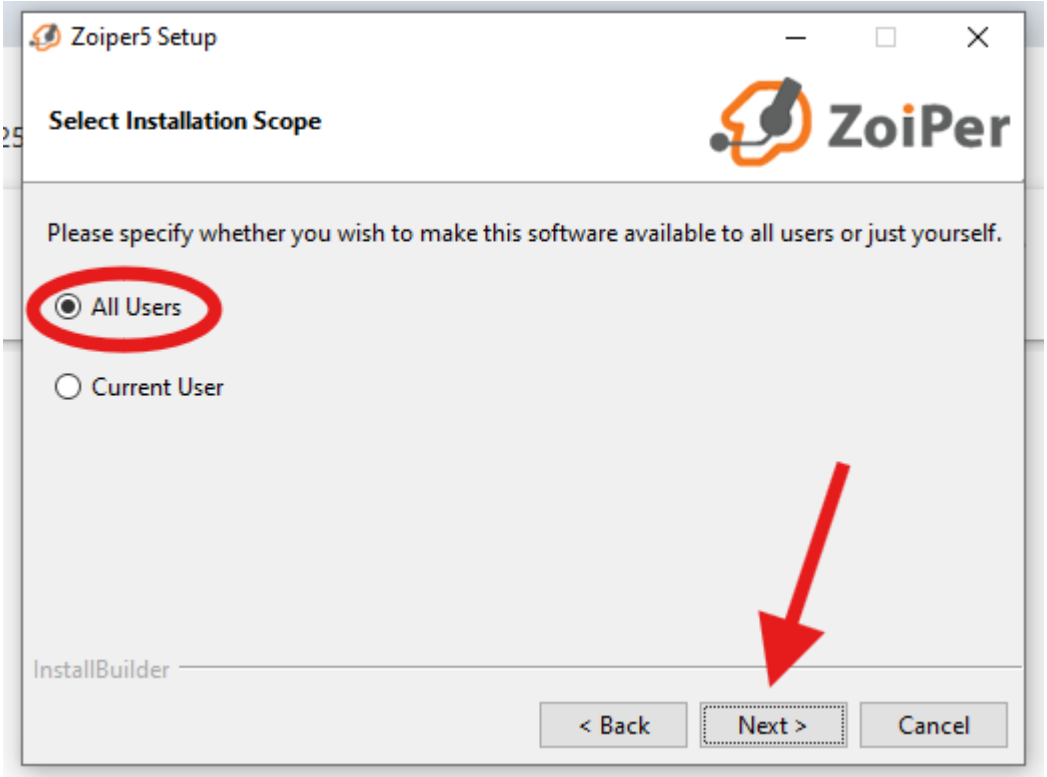


Cliquer sur Next.

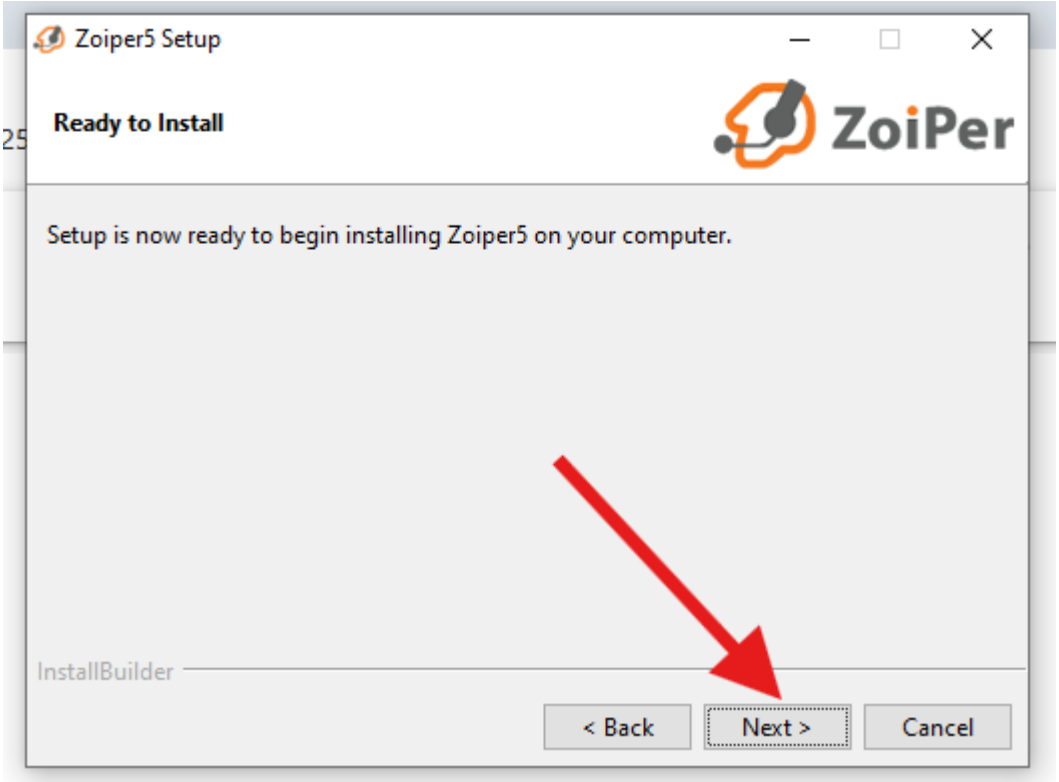


Sélectionner la version 64-bit et cliquer sur Next.

Sélectionner All Users et cliquer sur Next.

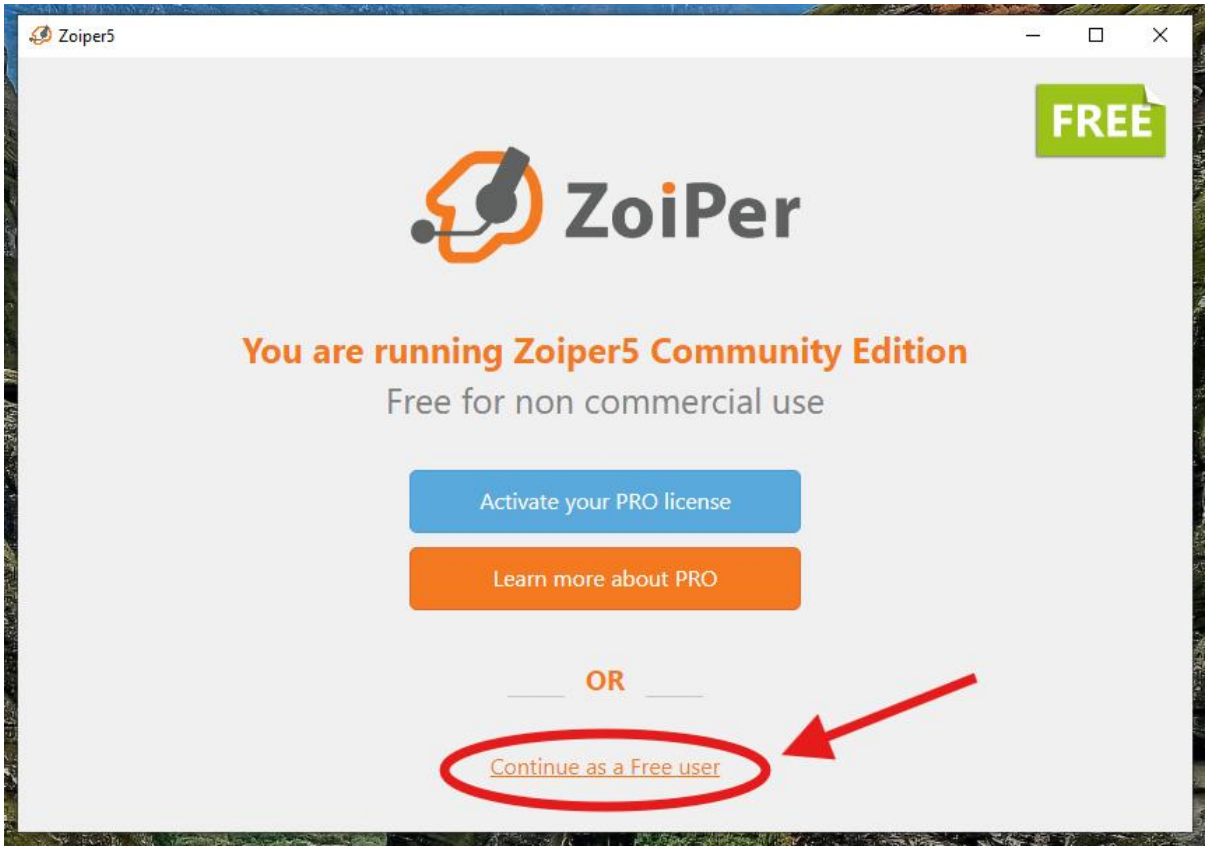


Cliquer sur Next.

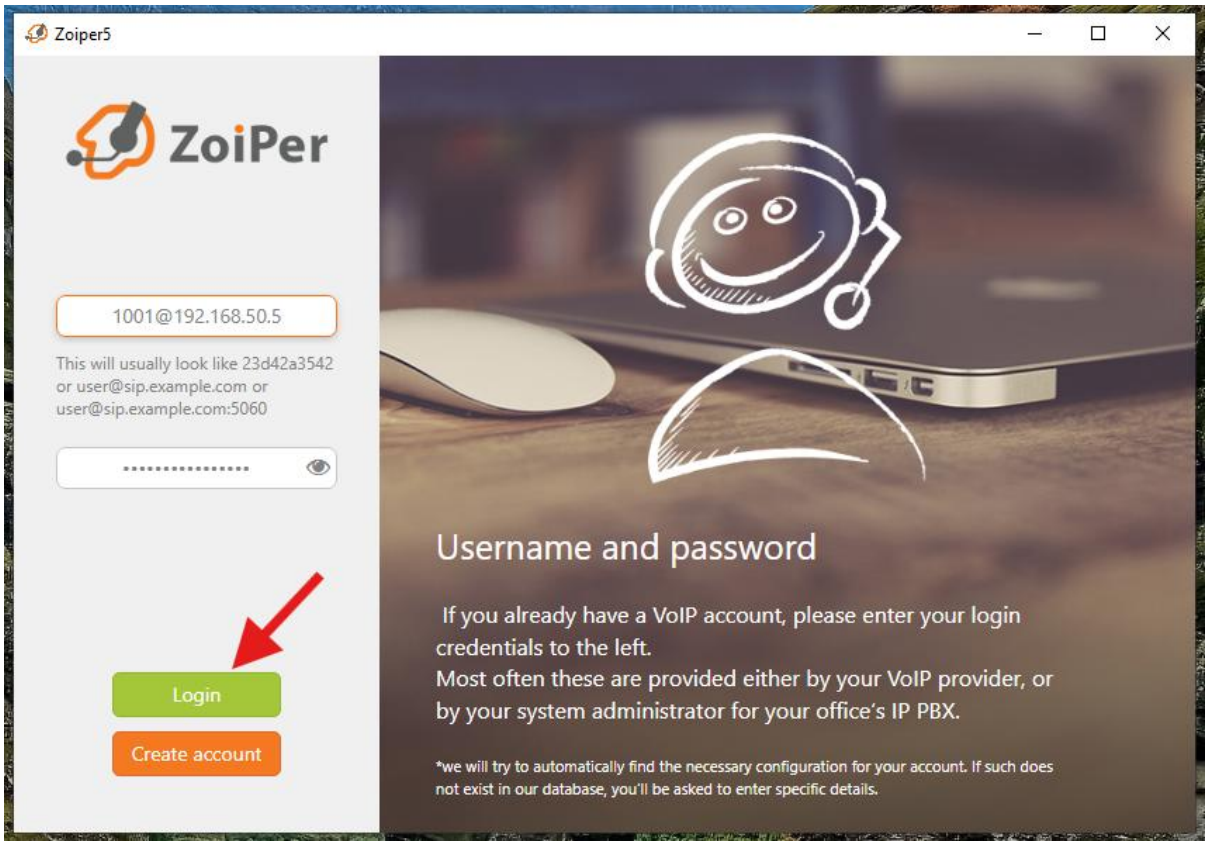


Attendre la fin de l'installation et cliquer sur Finish.

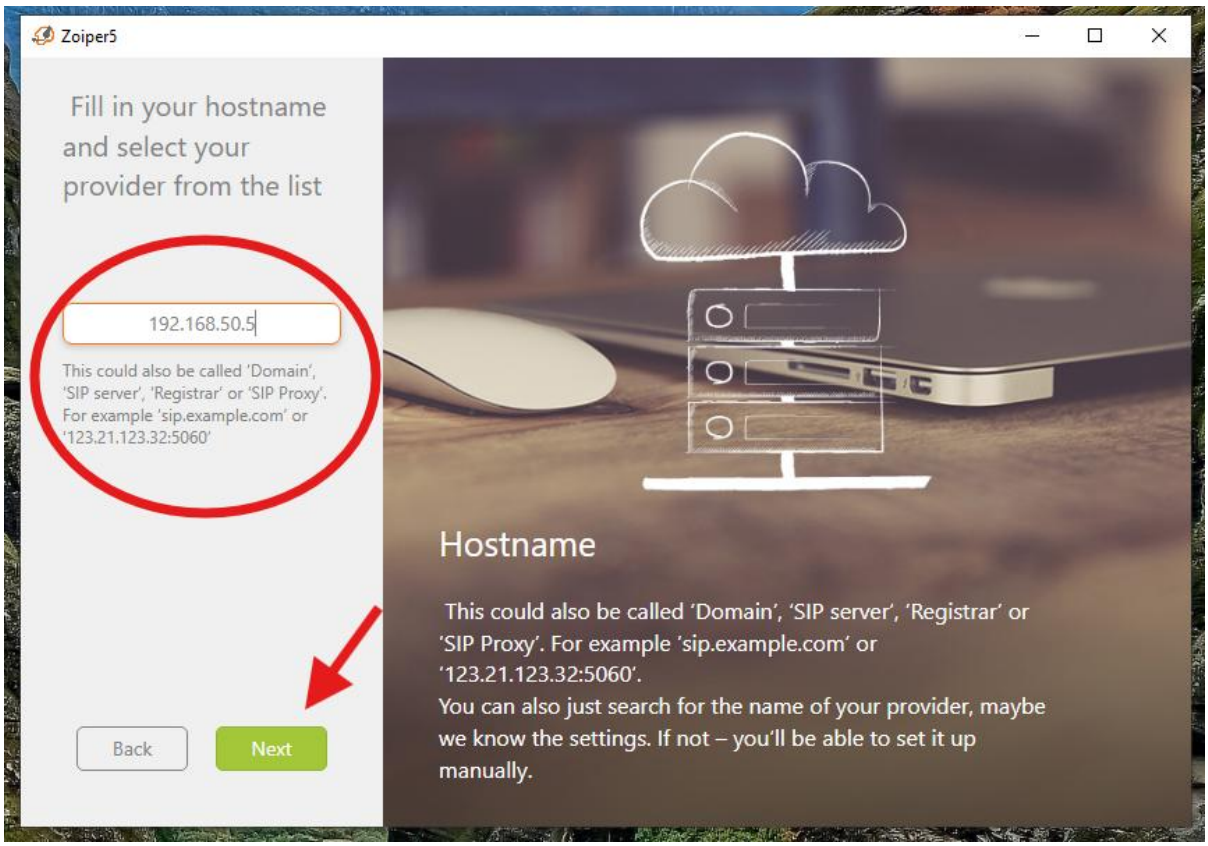
Ouvrir Zoiper et cliquer sur Continue as a Free user.



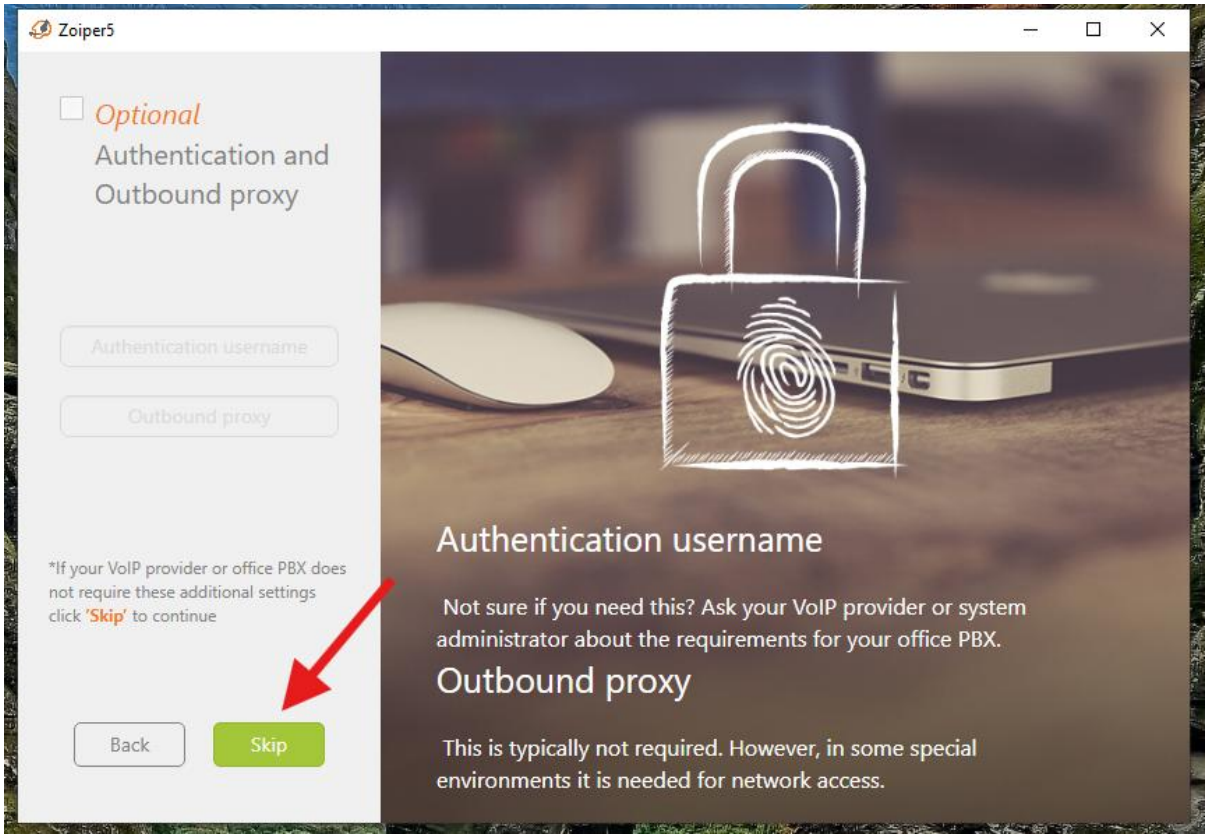
Se connecter en entrant le nom d'utilisateur (1001 par exemple) suivi de @192.168.50.5 (adresse IP du serveur Ubuntu). Rentrer aussi le mot de passe puis cliquer sur Login.



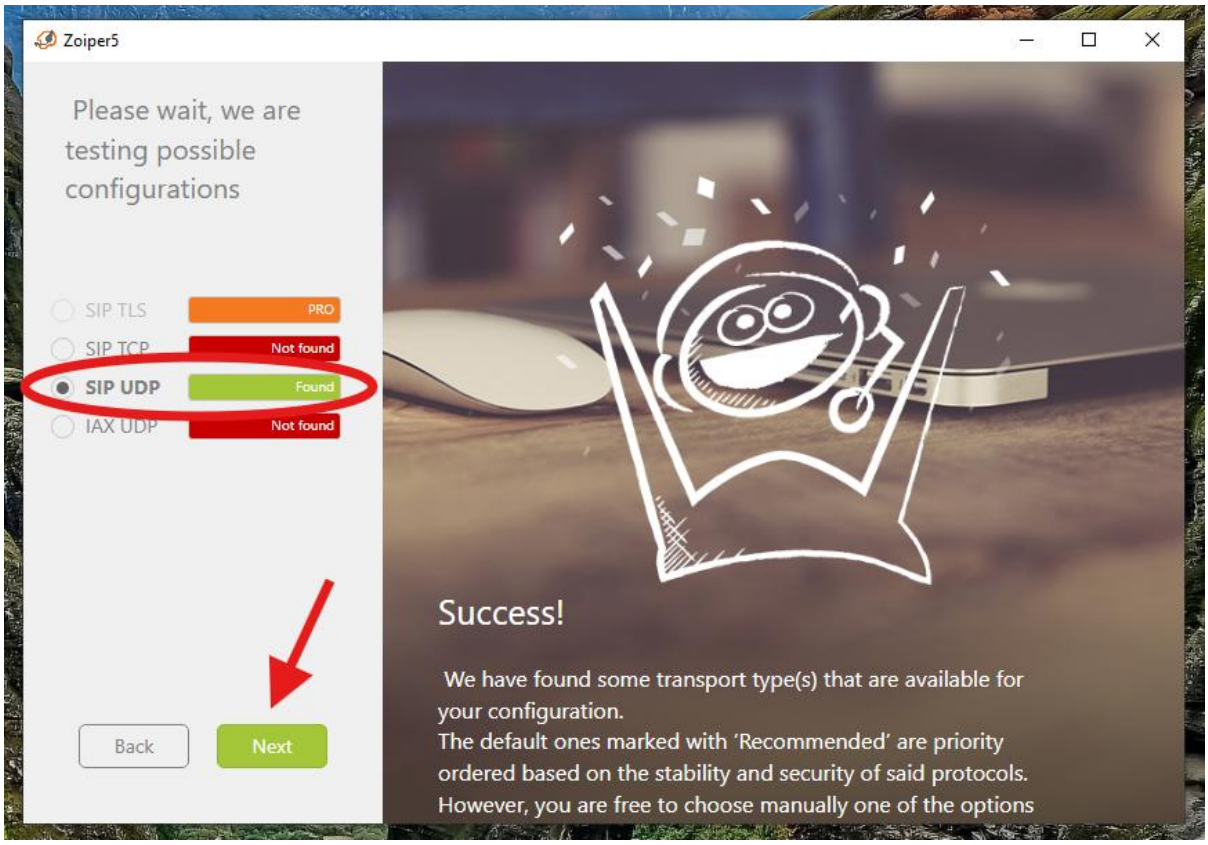
Rentrer à nouveau l'IP du serveur puis cliquer sur Next.



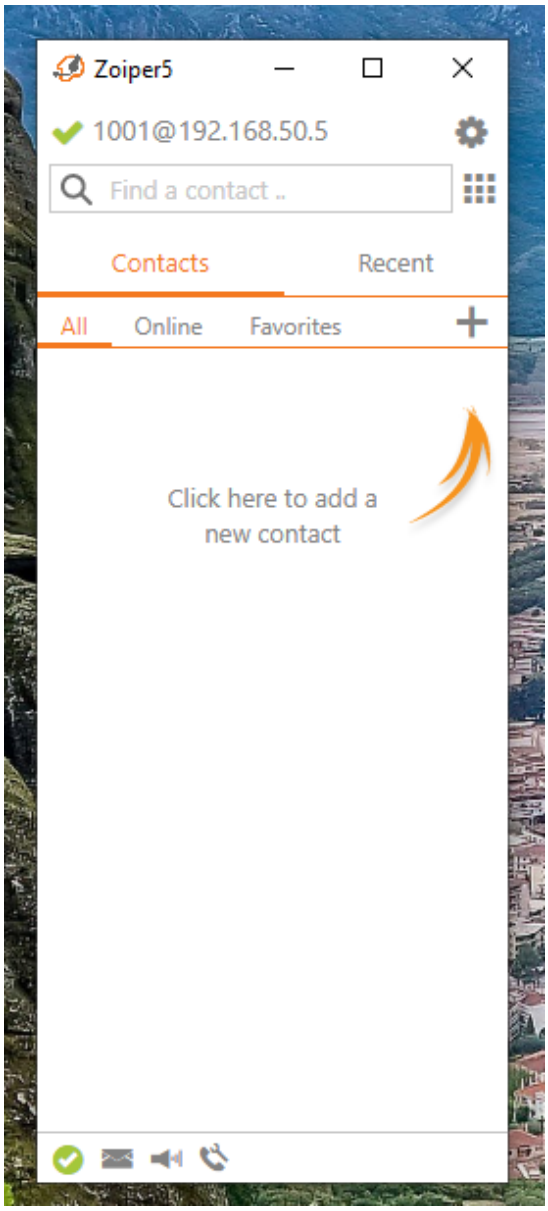
Cliquer sur Skip.



Sélectionner UDP pour le transfert et cliquer sur Next.



Nous avons réussi à nous connecter au compte SIP que l'on a créé avant.

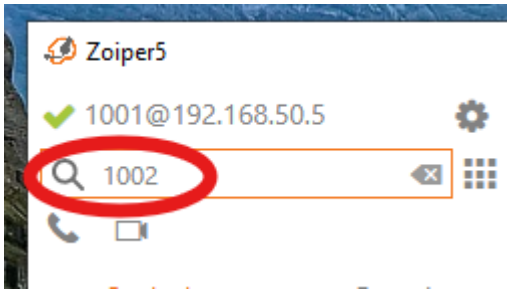

Zoiper5
1001@192.168.50.5
Find a contact ..
Contacts
Recent
All
Online
Favorites
Click here to add a
new contact

4) Tests

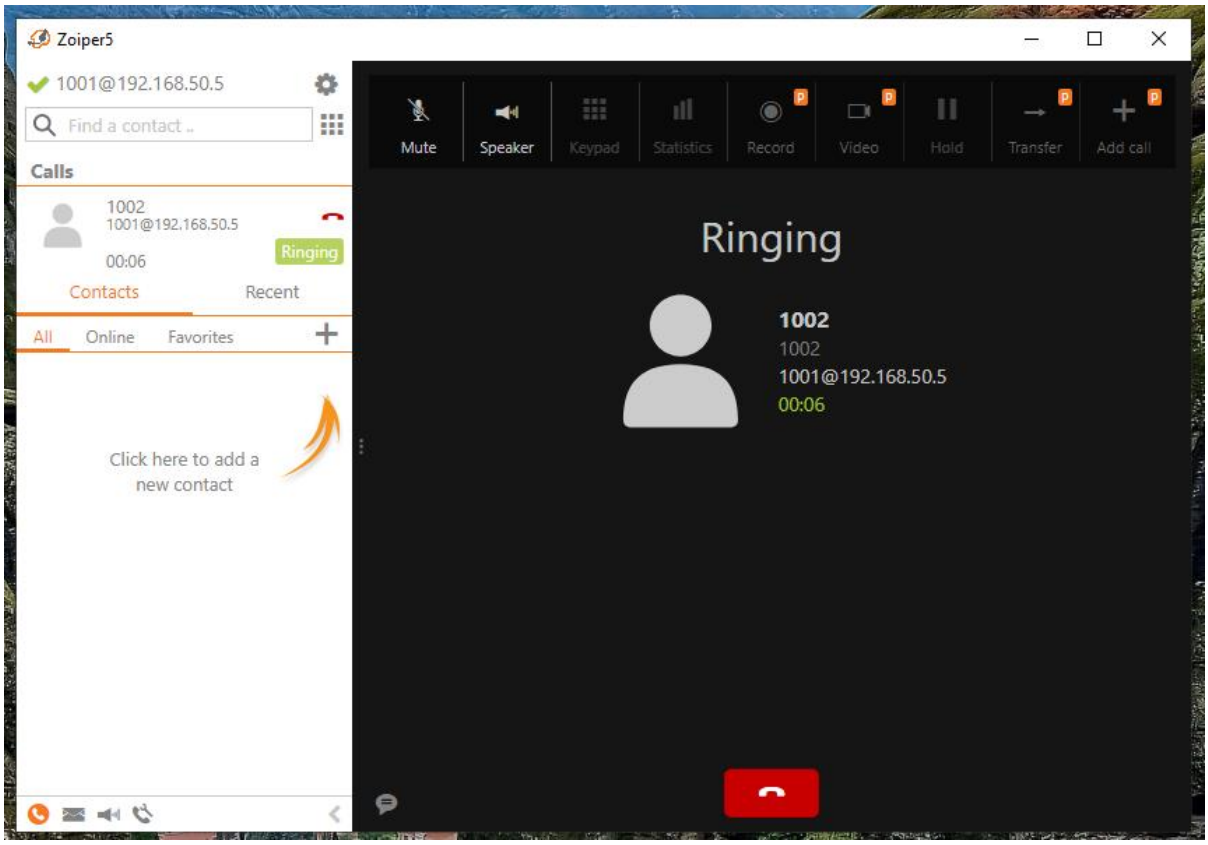
Sur un deuxième client Windows connecté au domaine, installer à nouveau Zoiper et se connecter avec le 2ème compte créé avant (1002 dans mon cas).

Essayer d'appeler 1002 sur le client Windows (sur le client Windows avec l'utilisateur 1001).

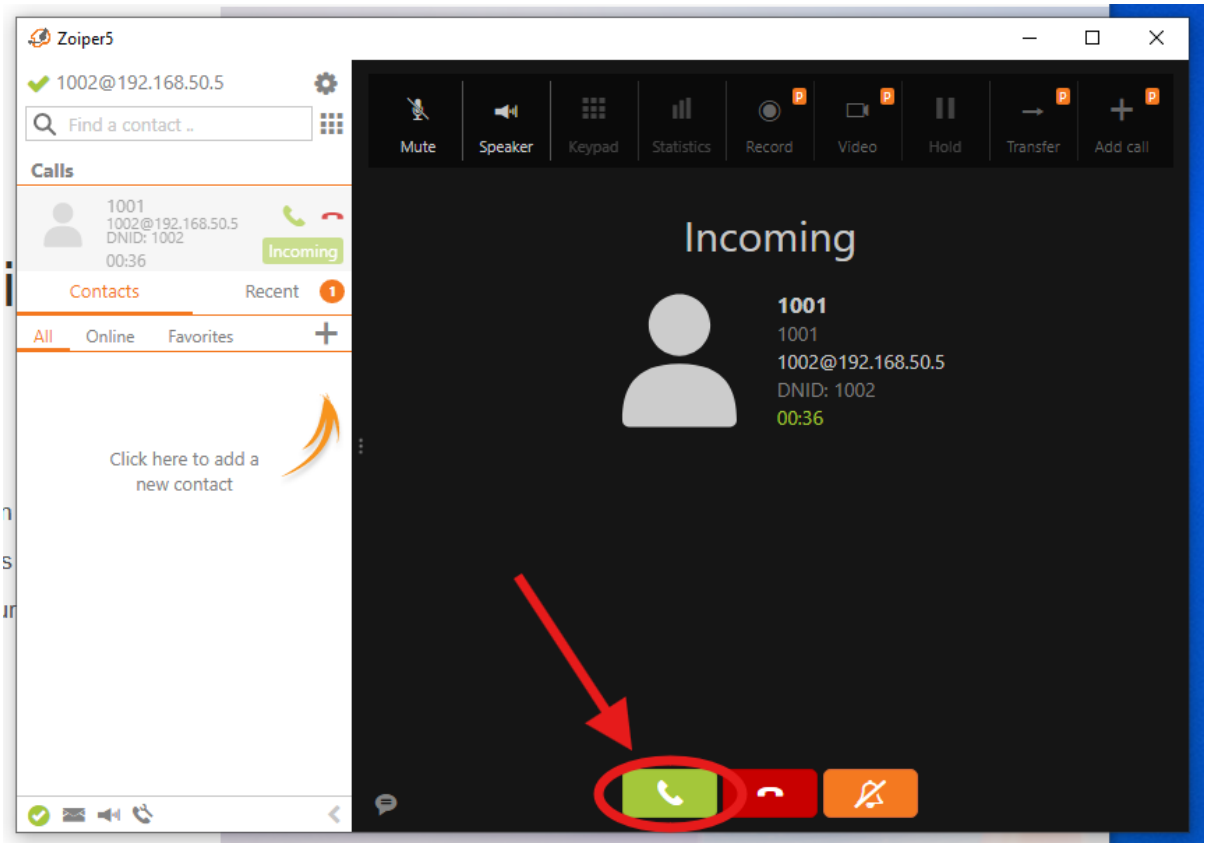
Rechercher 1002 puis cliquer sur Enter.



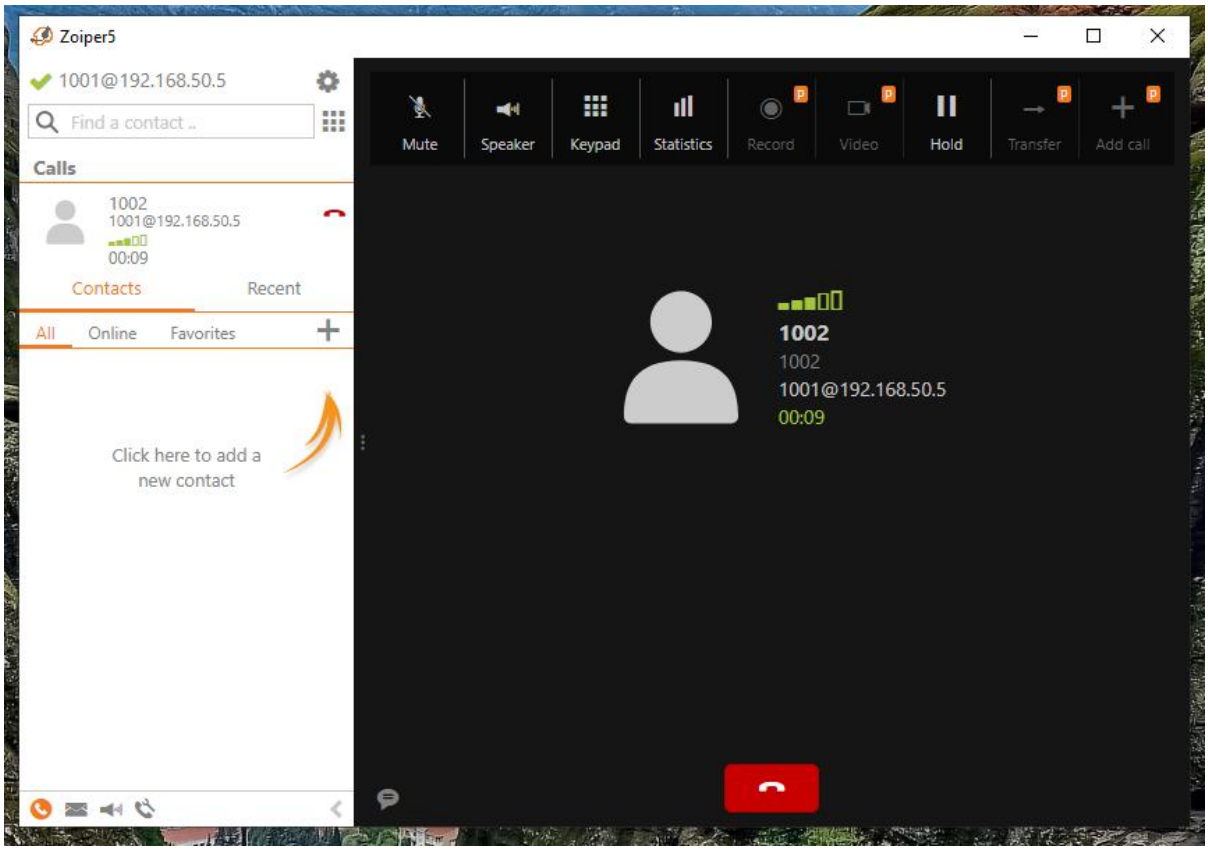
Le téléphone sonne bien.



Sur le deuxième client, décrocher en appuyant sur l'icône de téléphone vert.



Les appels fonctionnent.


Zoiper5
1001@192.168.50.5
Find a contact ..
Calls
1002
1001@192.168.50.5
00:09
Contacts
Recent
All
Online
Favorites
Click here to add a new contact
Mute
Speaker
Keypad
Statistics
Record
Video
Hold
Transfer
Add call
1002
1002
1001@192.168.50.5
00:09

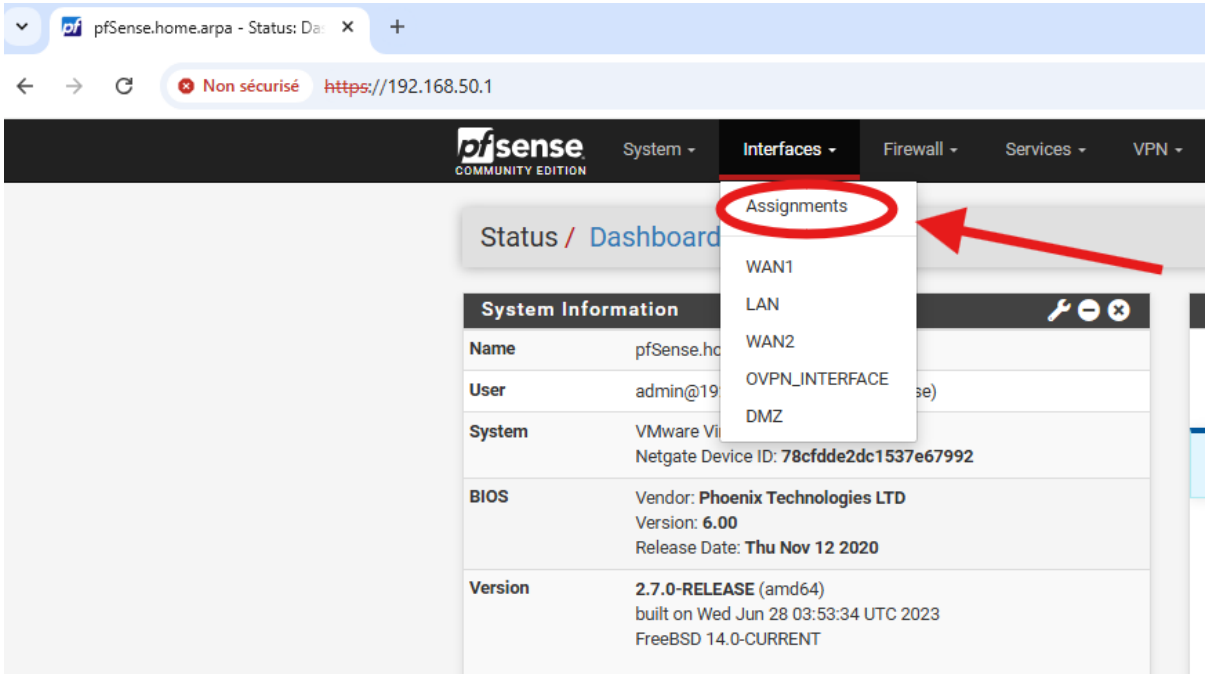
Configuration de eBrigade + DMZ

09/04/2025

1) Configuration de l'interface DMZ sur les routeurs

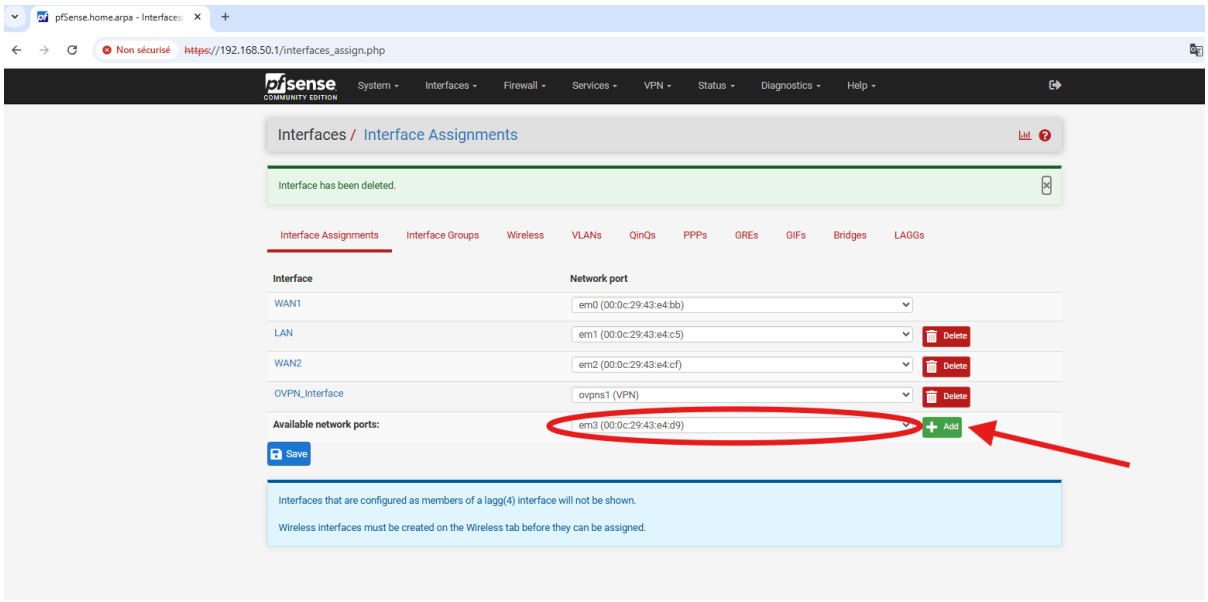
Après avoir ajouté une nouvelle carte réseau en host-only sur nos deux routeurs (avec une plage d'adresse différente de celle des LAN), on peut configurer l'interface DMZ.

Sur l'interface web de PfSense, aller dans Interfaces puis Assignments.



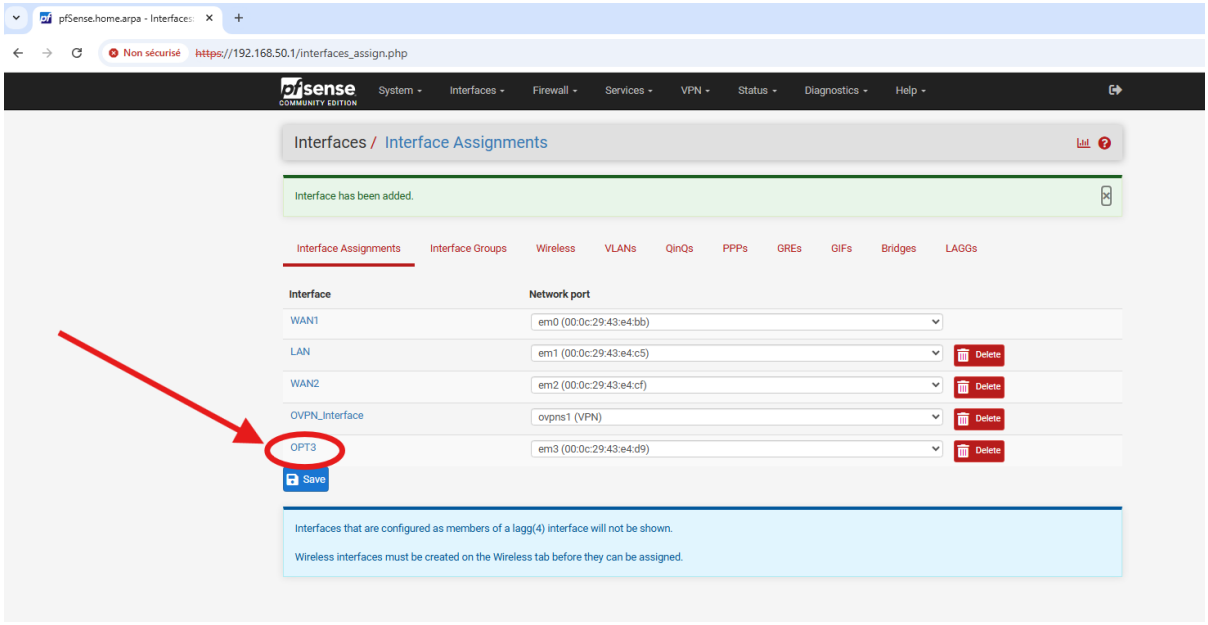
On peut voir qu'une interface est libre et prête à être configurée : c'est la carte réseau qui a été ajoutée.

Cliquer sur Add.

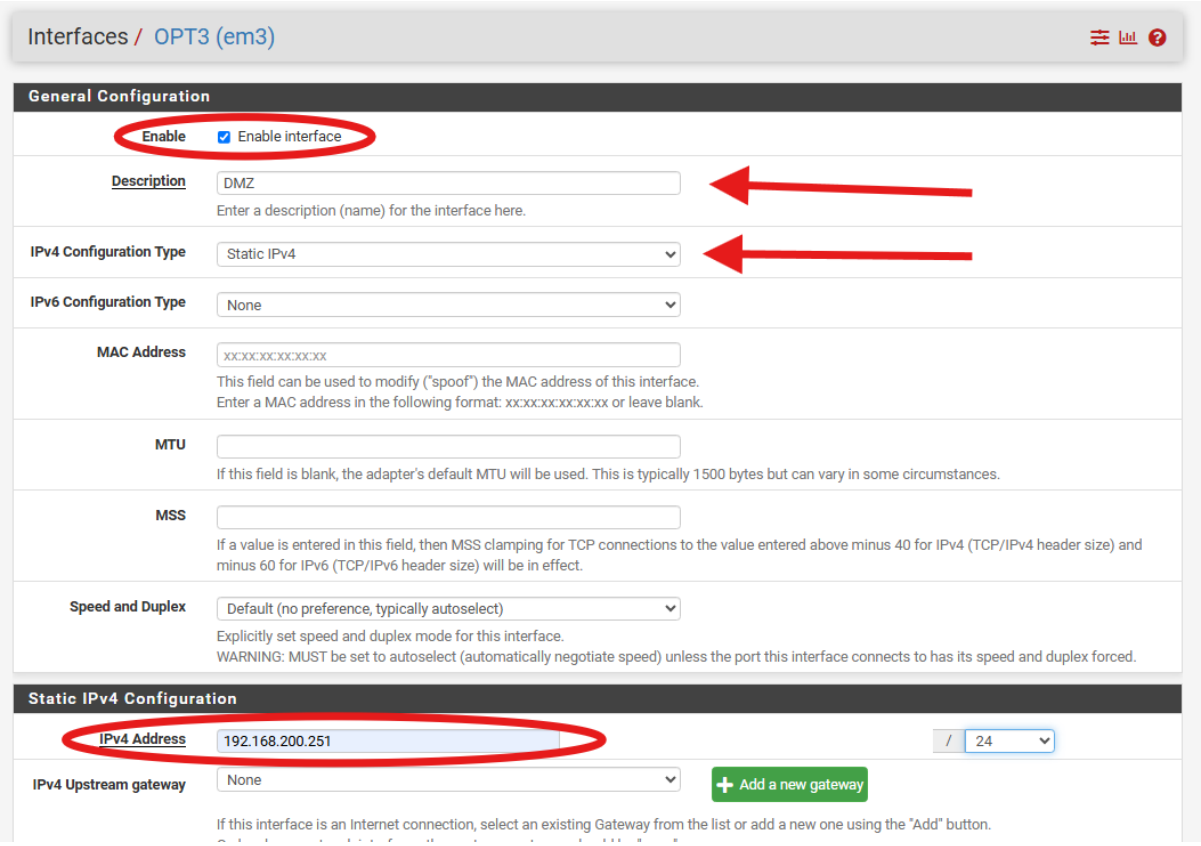


La nouvelle interface a été créée et s'appelle OPT3.

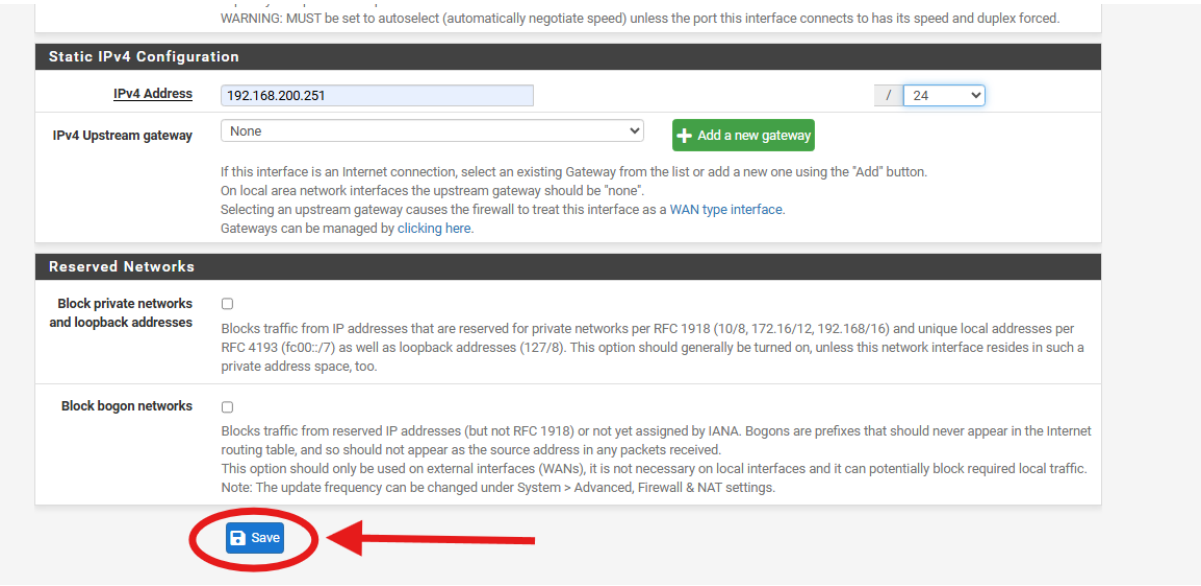
Cliquer dessus pour la configurer.



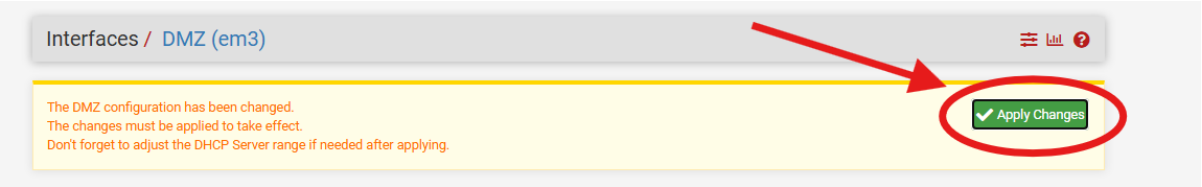
Activer l'interface en cochant enable, renommer l'interface en "DMZ", choisir Static IPv4 Pour la configuration IPv4, et entrer une adresse sur la plage de la nouvelle carte réseau (dans mon cas 192.168.200.0, j'ai mis 192.168.200.251).



Une fois les paramètres rentrés, cliquer sur Save.



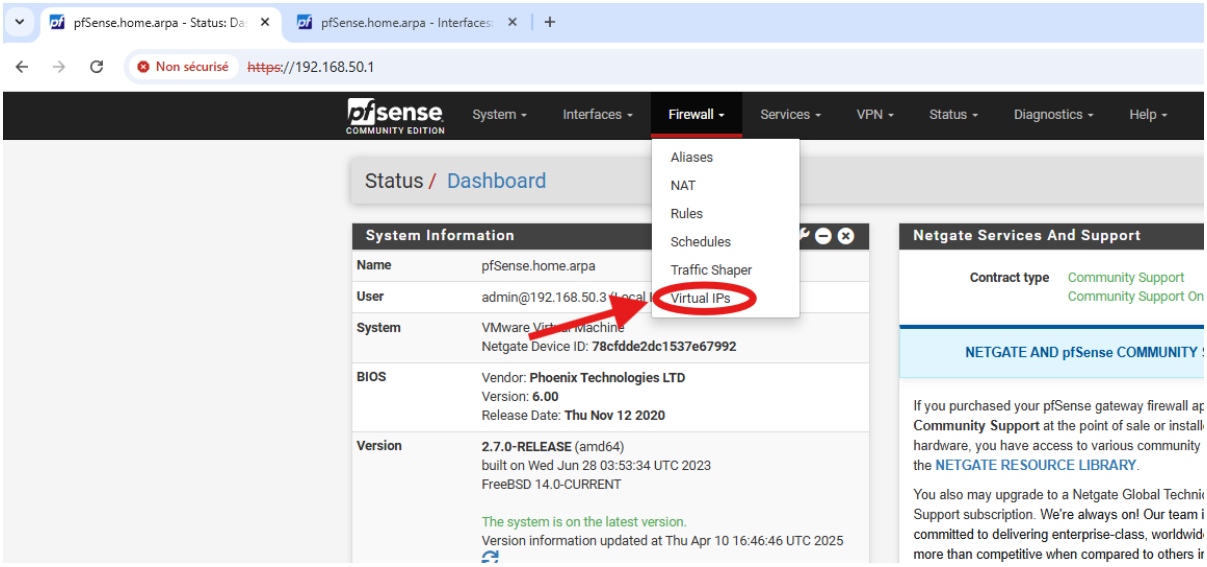
Cliquer sur Apply Changes pour appliquer les changements.



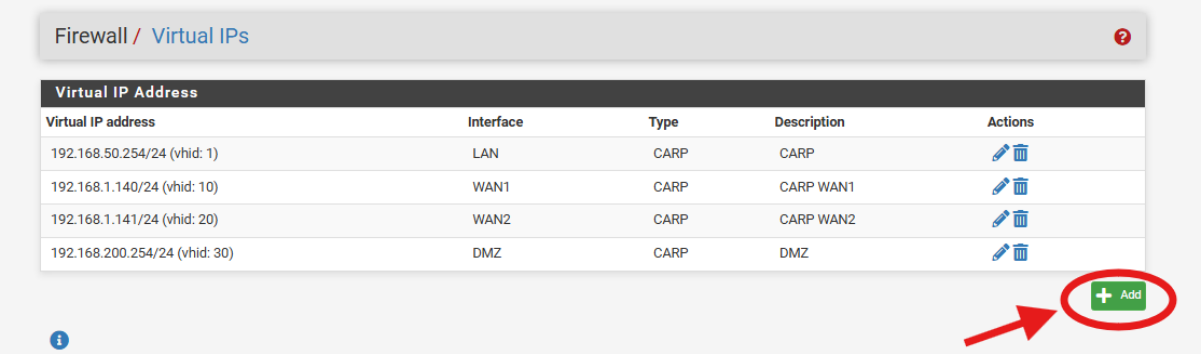
Il faut réaliser la même opération sur le PfSense Backup en rentrant une autre adresse IPv4 (192.168.200.252 dans mon cas).

Ensuite il faut configurer un CARP DMZ, de cette façon si le routeur Master tombe, notre DMZ sera toujours disponible via le routeur Backup.

Aller dans Firewall puis Virtual IPs.

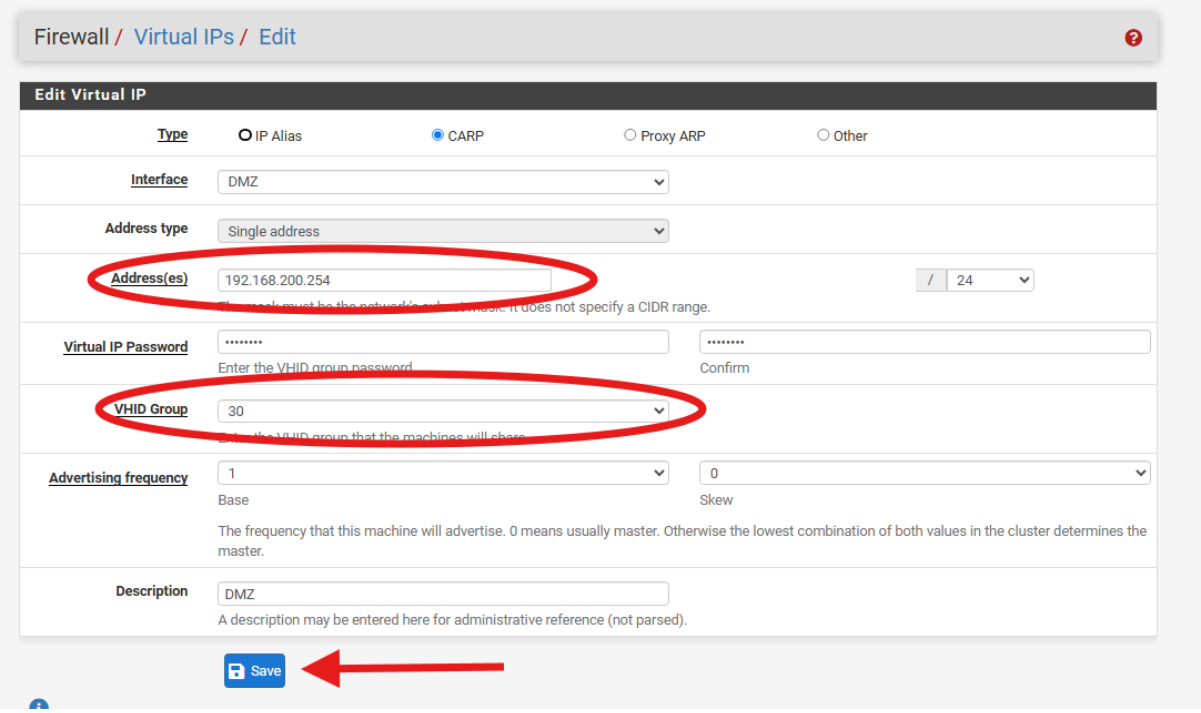


Cliquer sur Add.

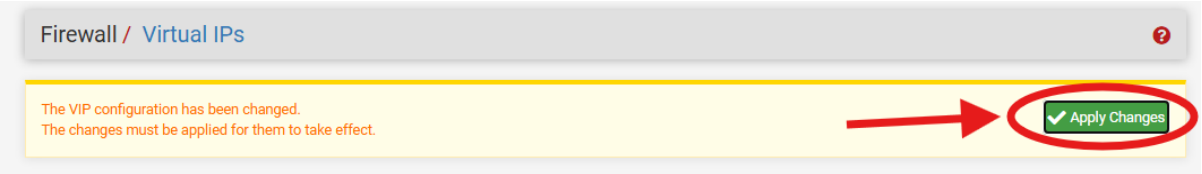


Voici les paramètres à rentrer (l'adresse est à ajuster en fonction de votre plage IP). Mettre aussi un VHID Group différent des autres IP virtuelles déjà présentes.

Une fois tous les paramètres remplis cliquer sur Save.

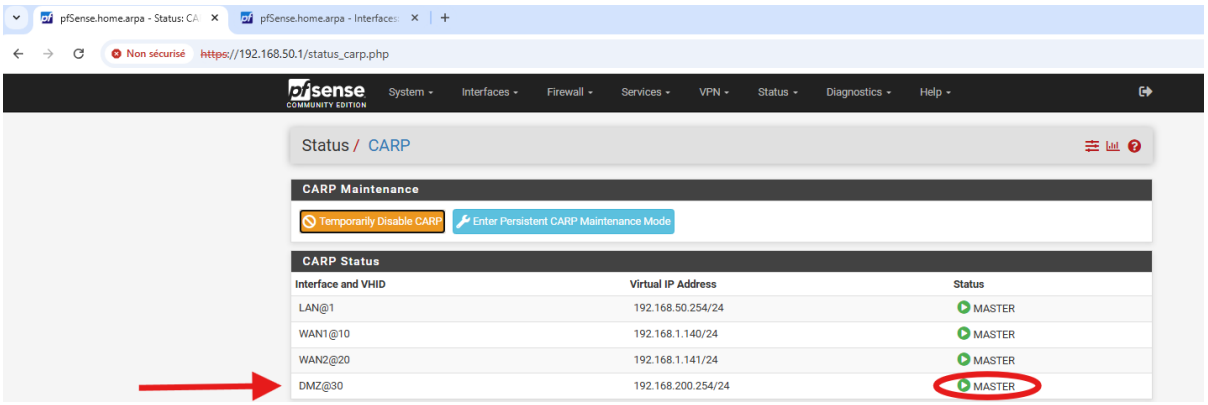


Cliquer sur Apply Changes pour appliquer les changements.

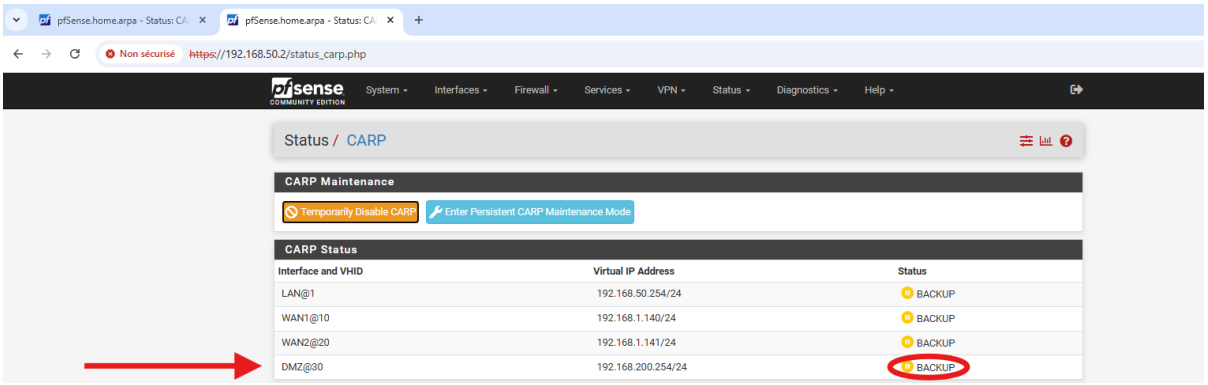


Si l'on va dans Status puis CARP (failover), on peut voir que :

- Sur le PfSense Master le CARP DMZ est bien en MASTER.



- Sur le PfSense Backup le CARP DMZ est bien en BACKUP.



La DMZ est bien configuré (nous reviendrons sur les règles de pare-feu plus tard).

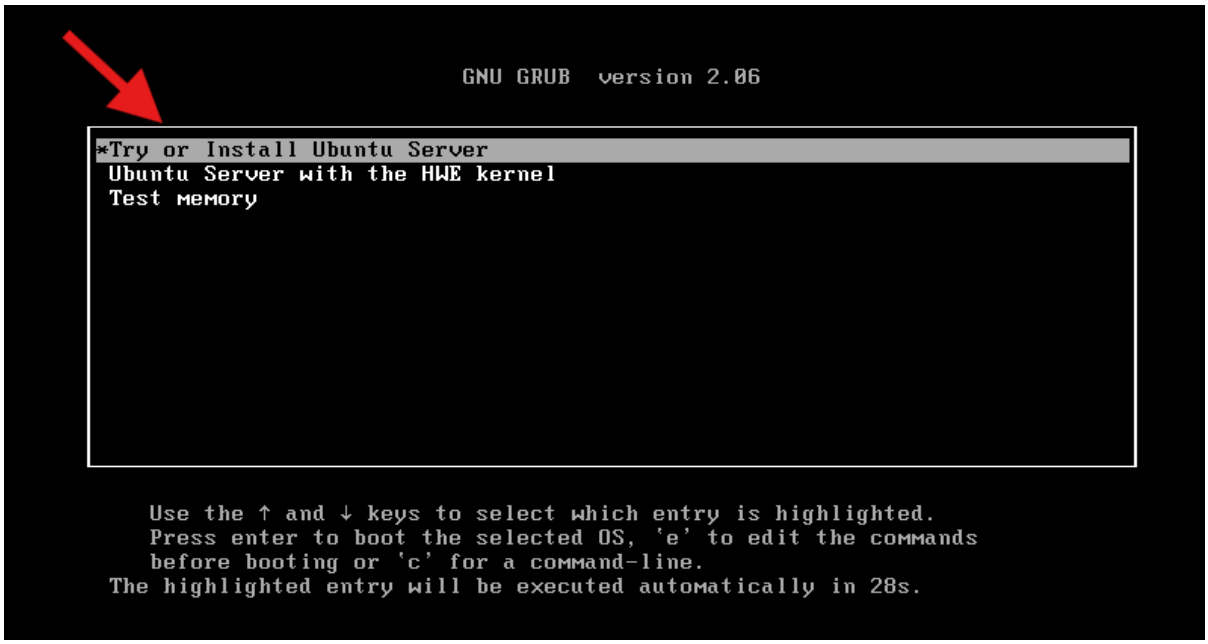
2) Configuration du serveur Ubuntu hébergeant eBrigade

A) Initialisation du serveur Ubuntu

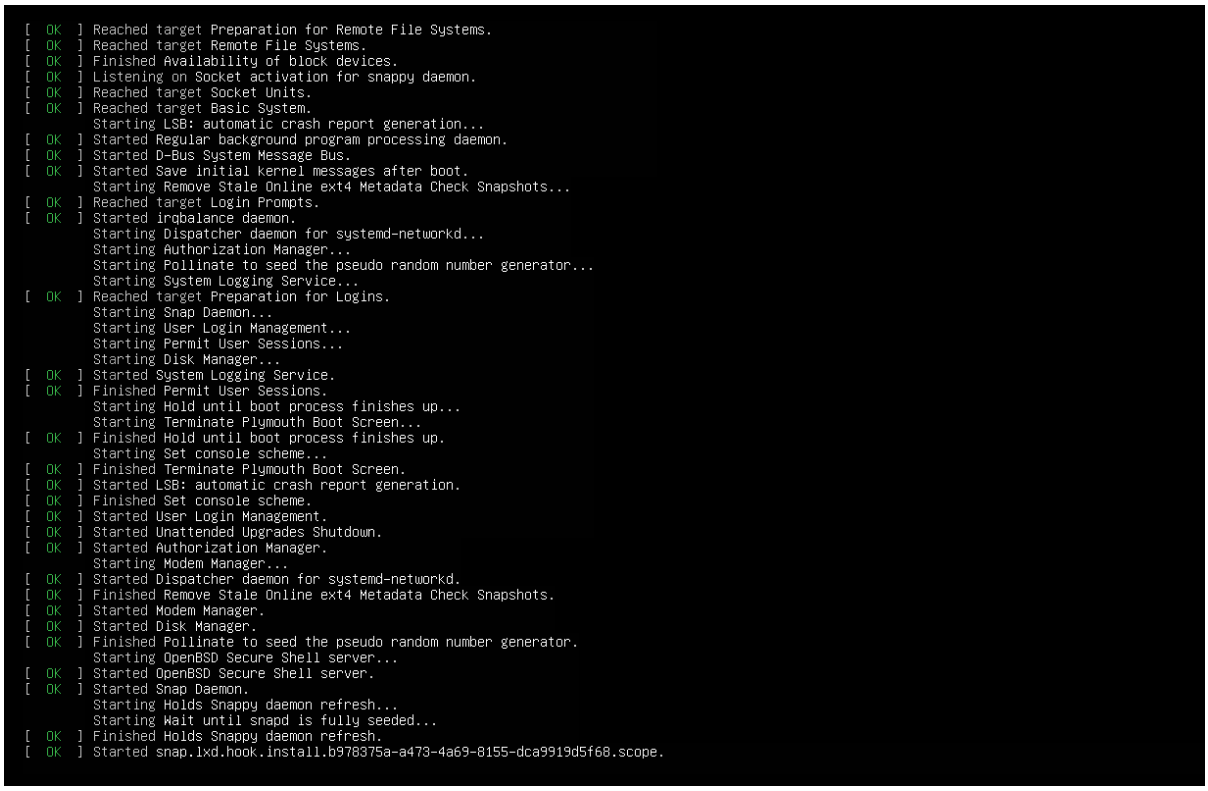
L'installation et la configuration de eBrigade doit se faire sur un serveur différent de celui hébergeant déjà Modoboa et Asterisk.

Avant de lancer le serveur, configurer une carte réseau en host-only ayant la même plage IP que celle de l'interface DMZ sur les deux routeurs.

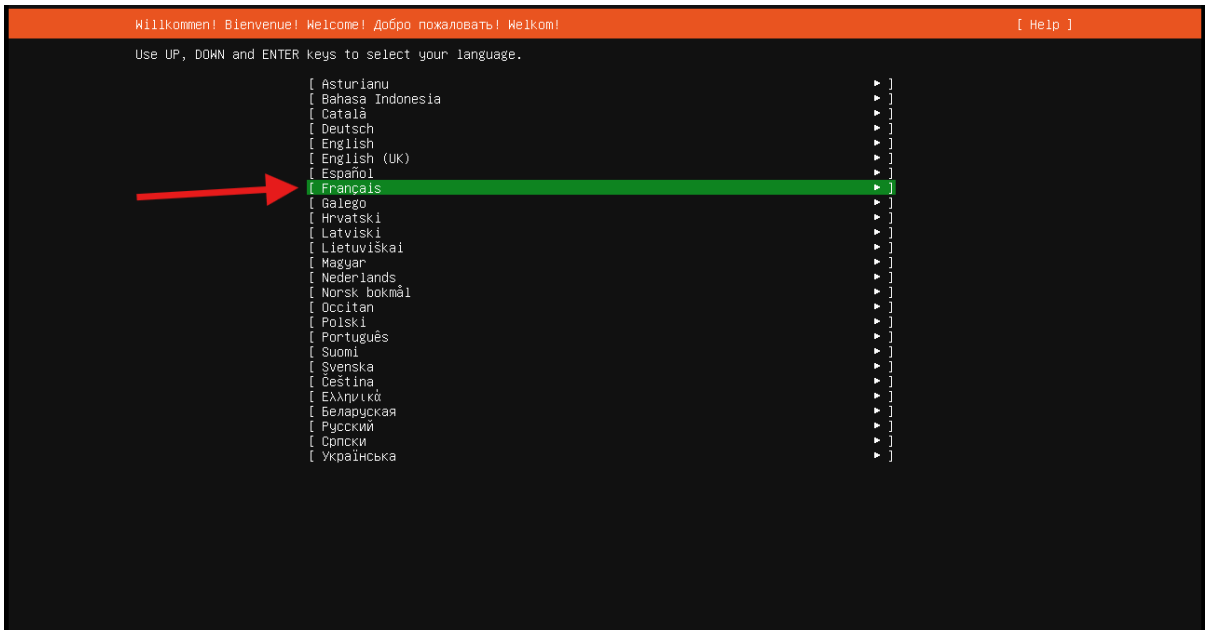
Une fois le serveur lancé, appuyer Enter sur l'option Try or Install Ubuntu Server.



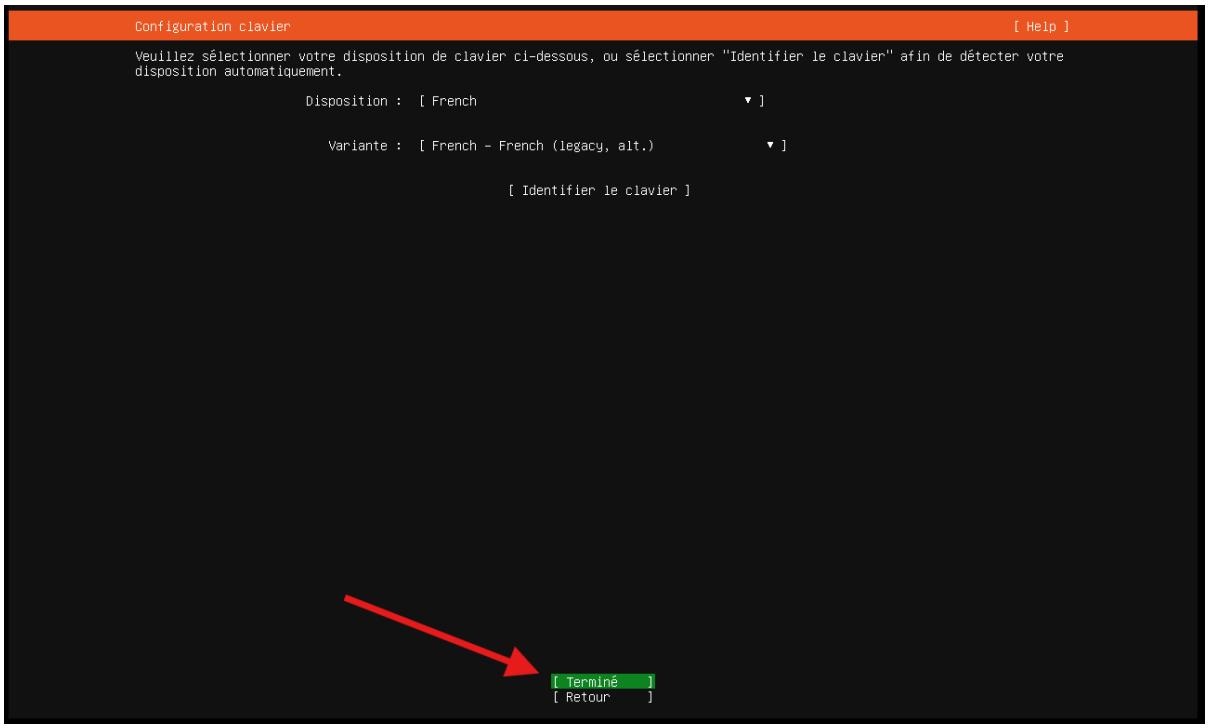
Attendre jusqu'à la prochaine étape.



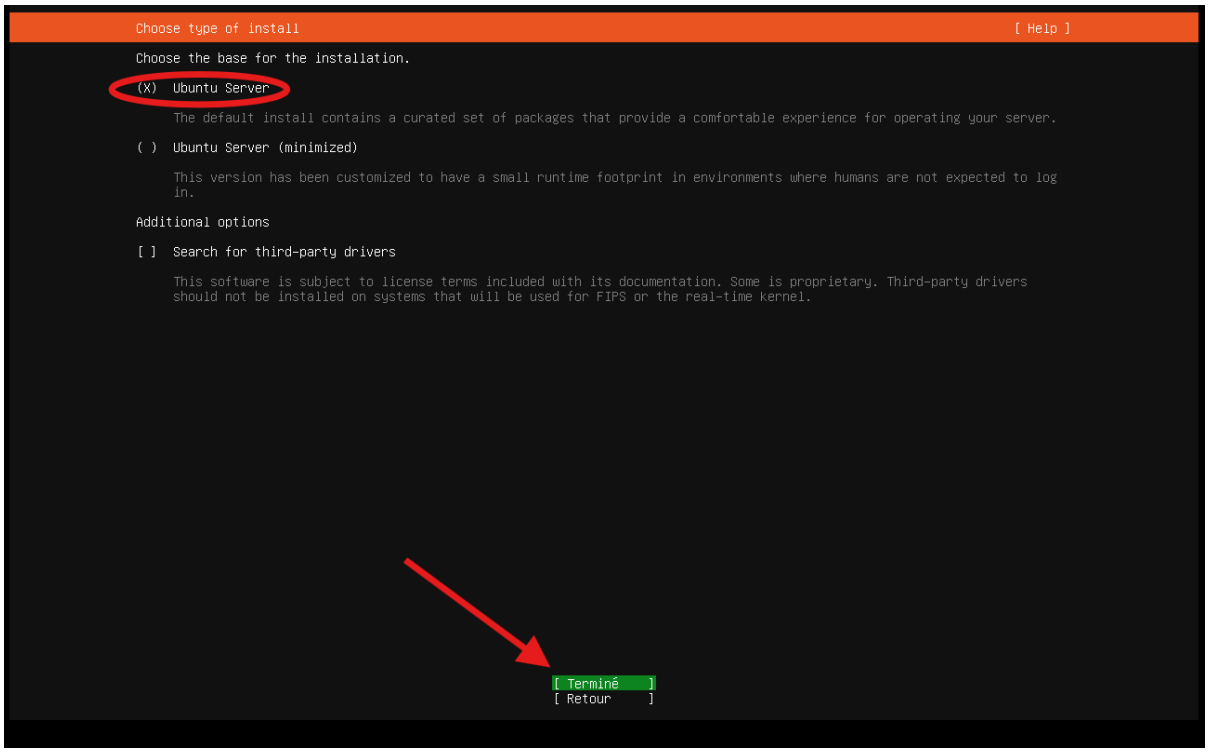
Sélectionner Français.



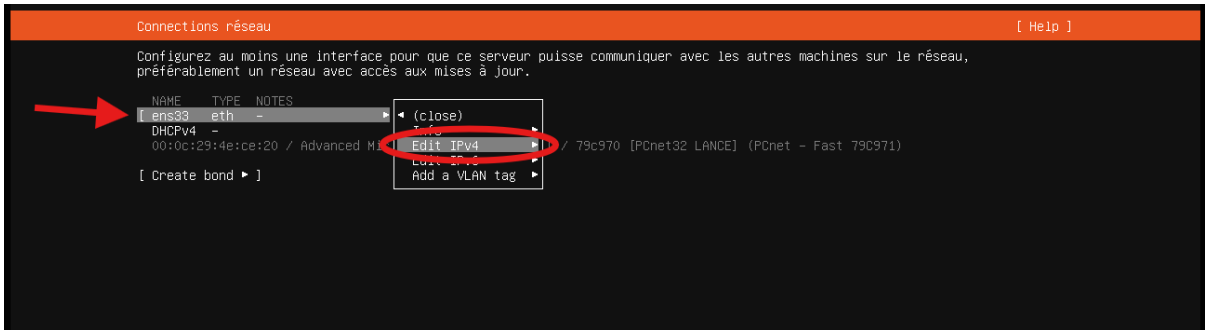
Appuyer sur Terminé.



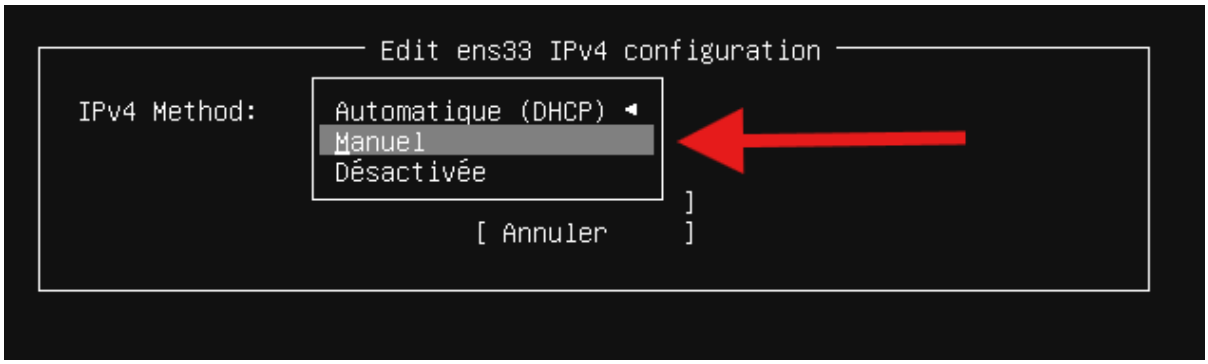
Sélectionner Ubuntu Server et appuyer sur Terminé.


Choose type of install
[Help]
Choose the base for the installation.
(X) Ubuntu Server
The default install contains a curated set of packages that provide a comfortable experience for operating your server.
( ) Ubuntu Server (minimized)
This version has been customized to have a small runtime footprint in environments where humans are not expected to log in.
Additional options
[ ] Search for third-party drivers
This software is subject to license terms included with its documentation. Some is proprietary. Third-party drivers should not be installed on systems that will be used for FIPS or the real-time kernel.
[Terminé]
[Retour]

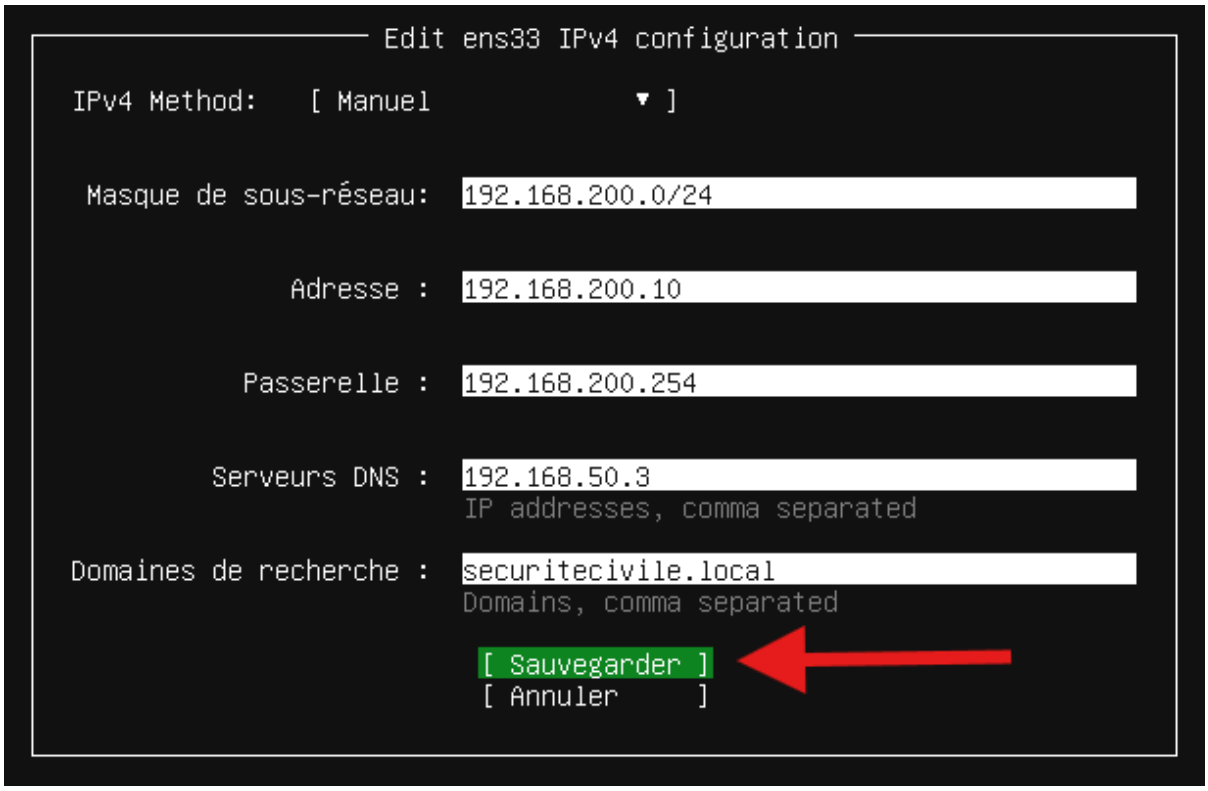
Une fois dans les paramètres réseaux, aller sur ens33 puis Edit IPv4.



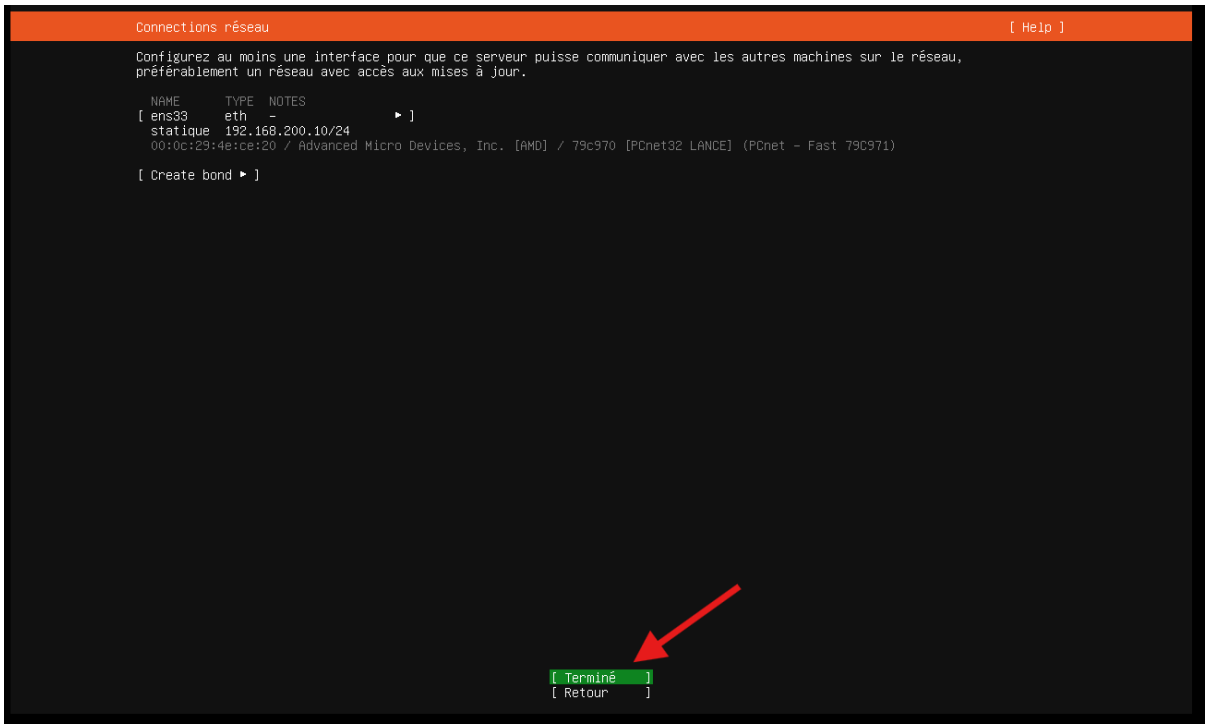
Choisir Manuel.



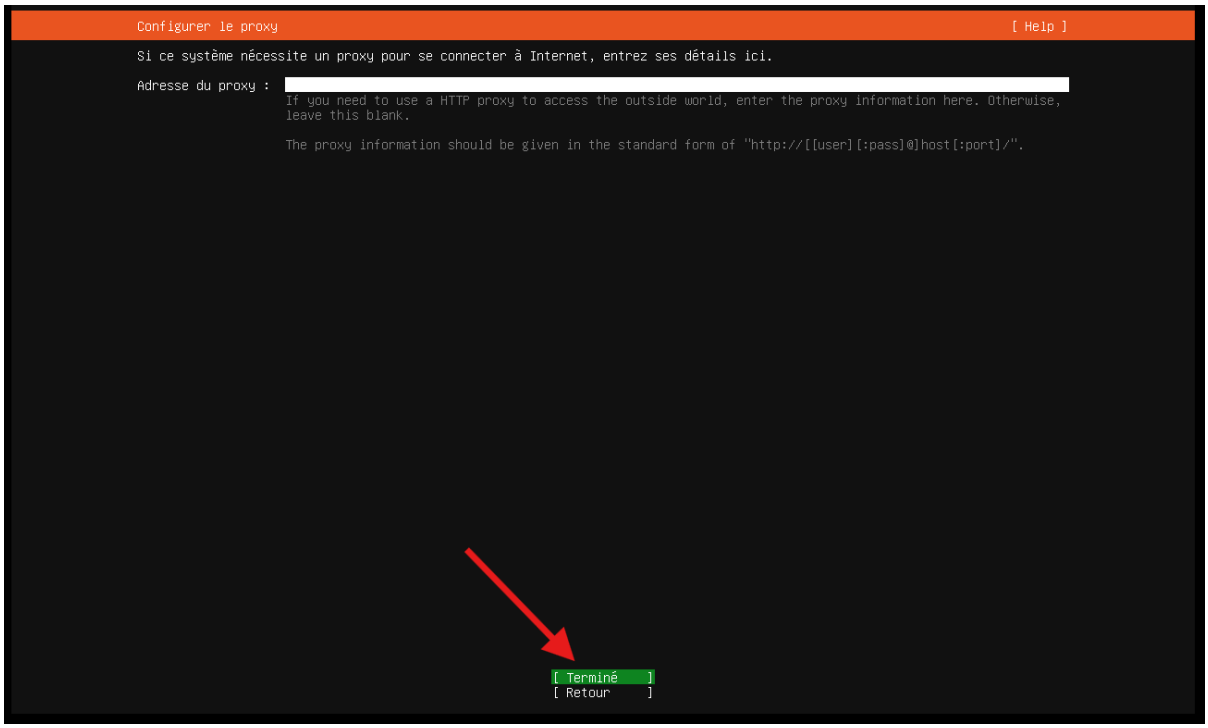
Remplir avec ces paramètres (serveur DNS = le Windows Server GUI contrôleur de domaine). Cliquer ensuite sur Sauvegarder.



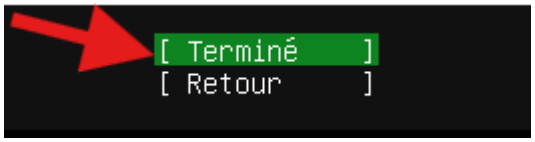
Attendre l'application des changements puis cliquer sur Terminé.



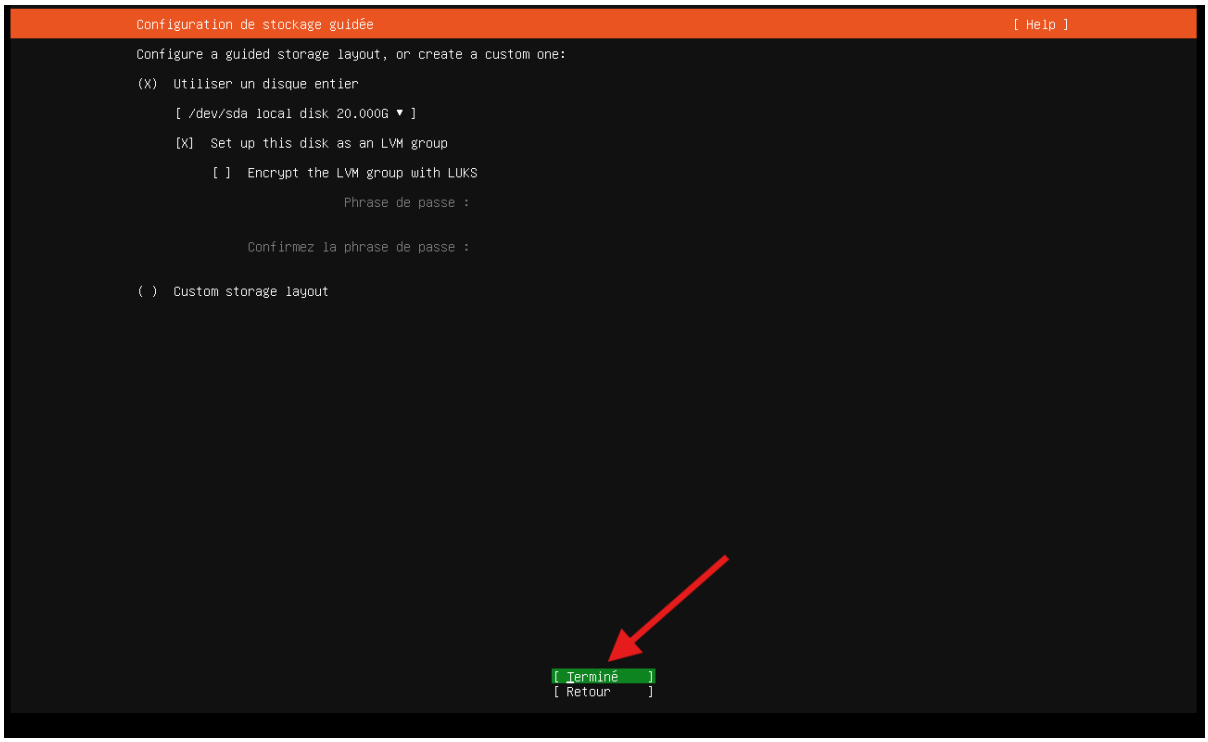
Appuyer sur Terminé.



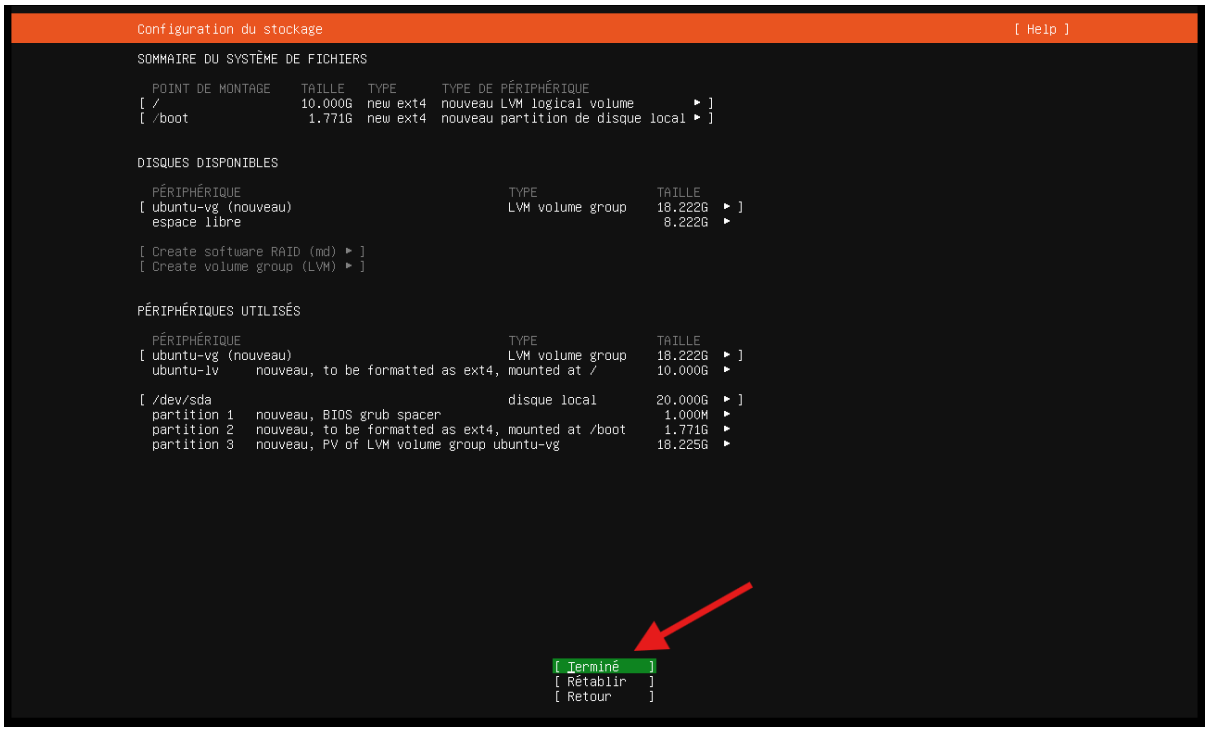
Attendre la fin du test miroir puis cliquer sur Terminé.



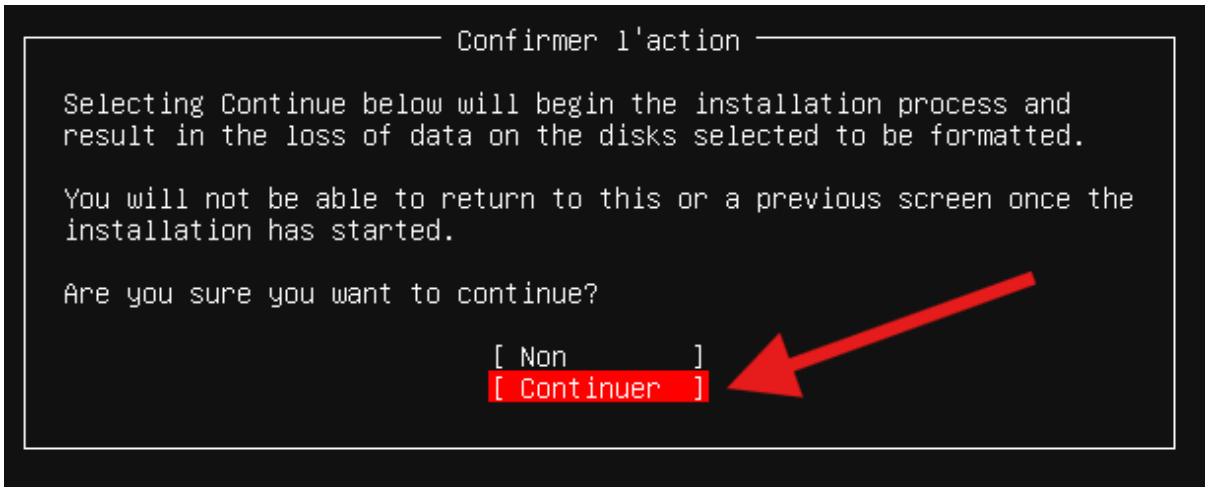
Appuyer sur Terminé.



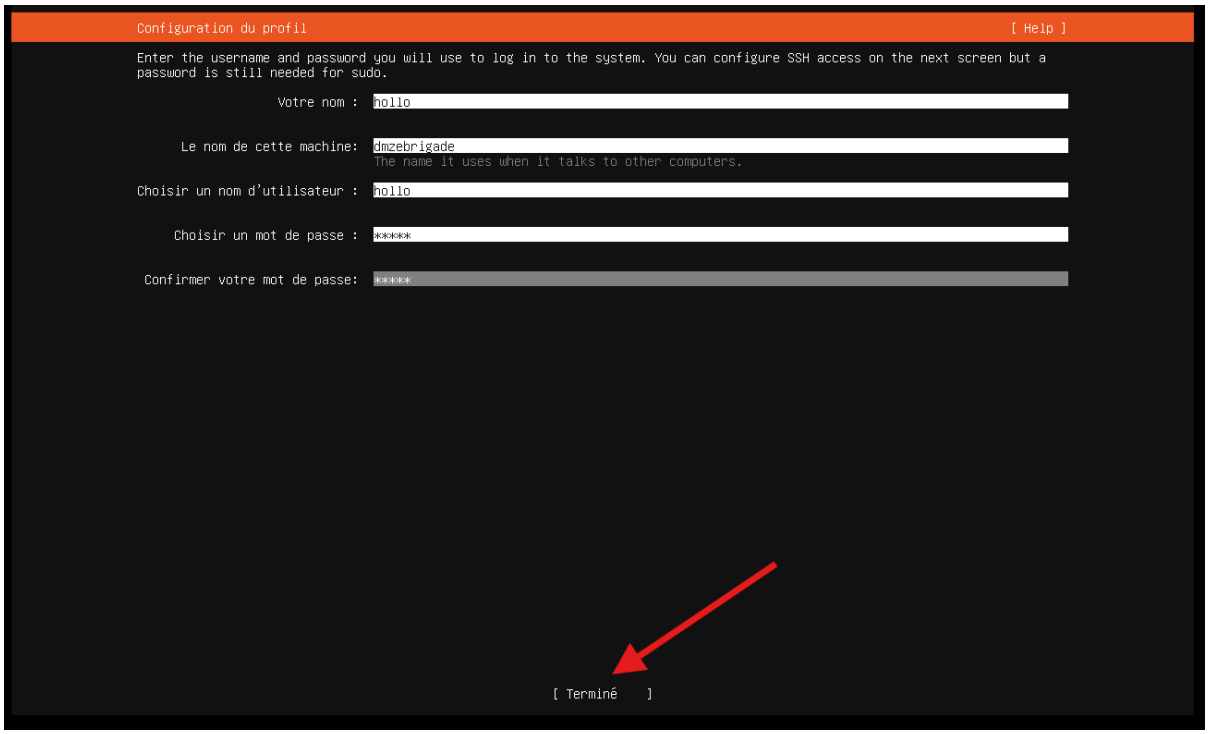
Appuyer sur Terminé.



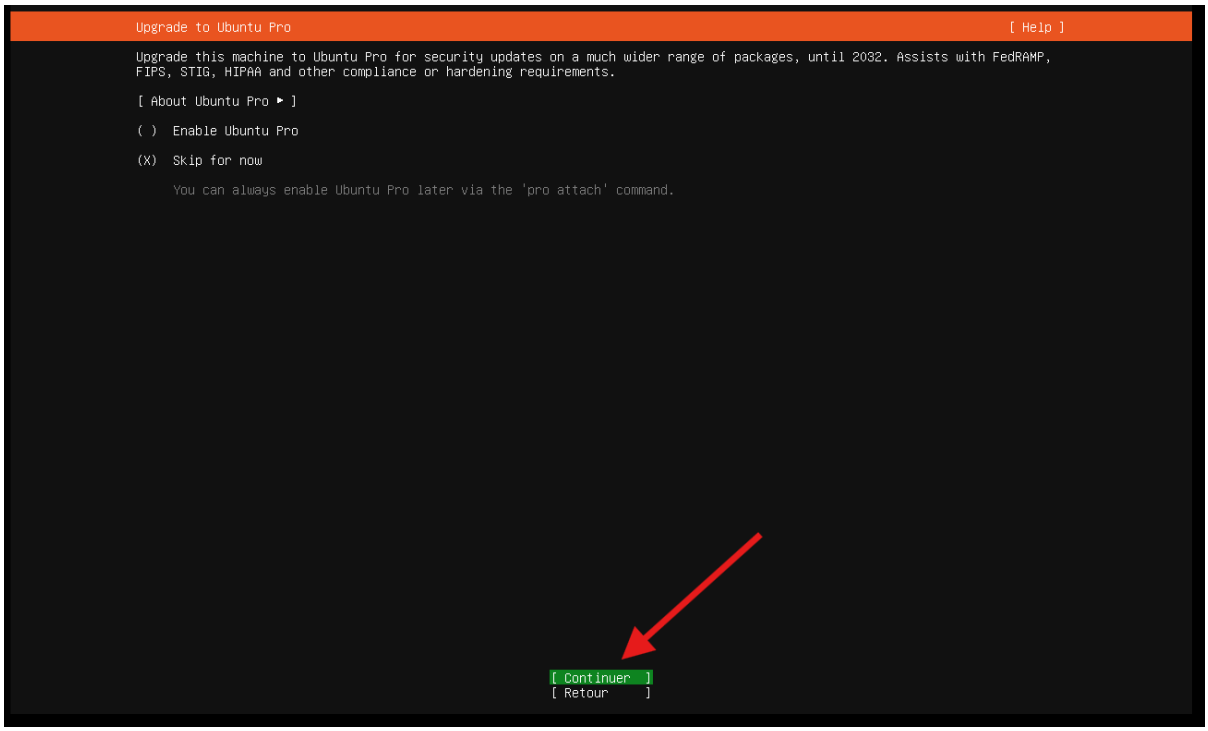
Sélectionner continuer.



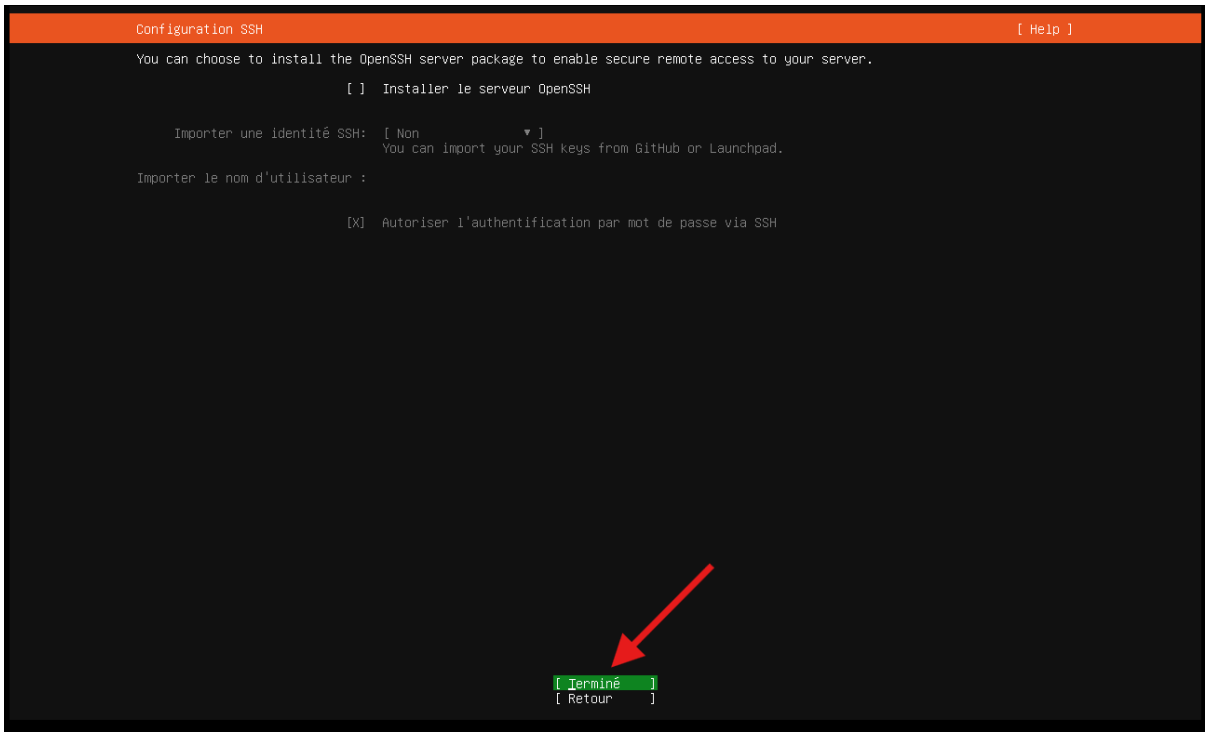
Entrer les identifiants puis cliquer sur Terminé.



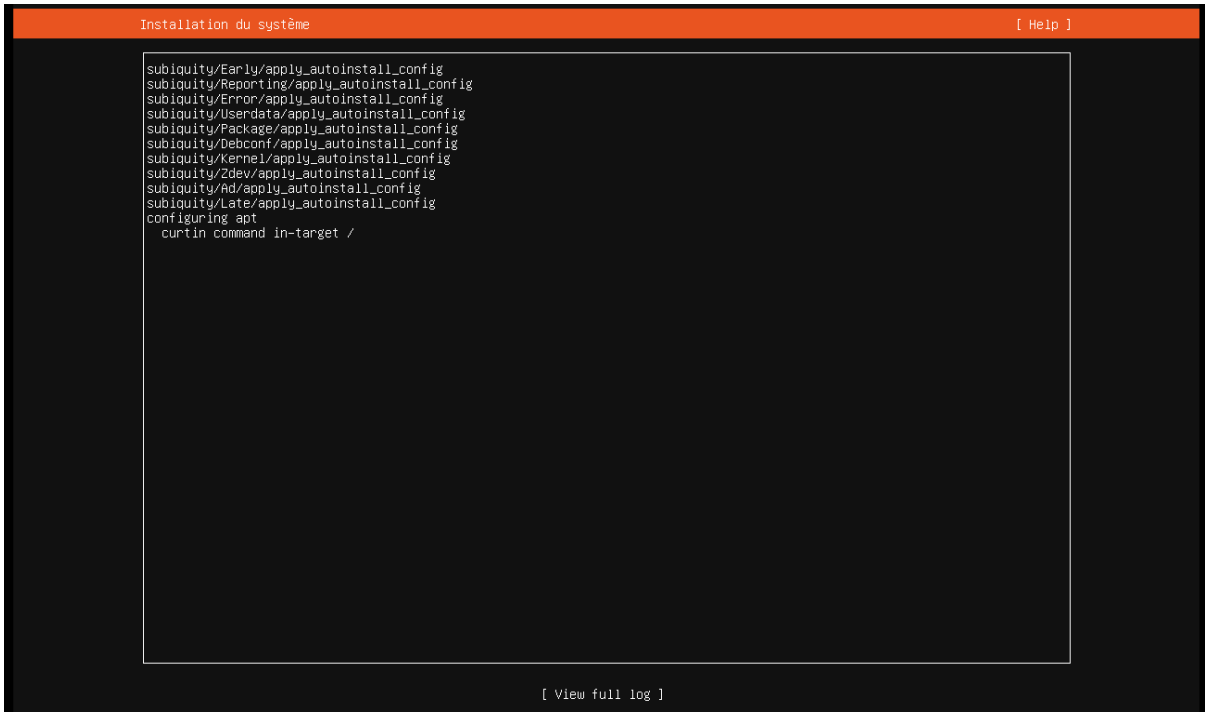
Sélectionner Continuer.



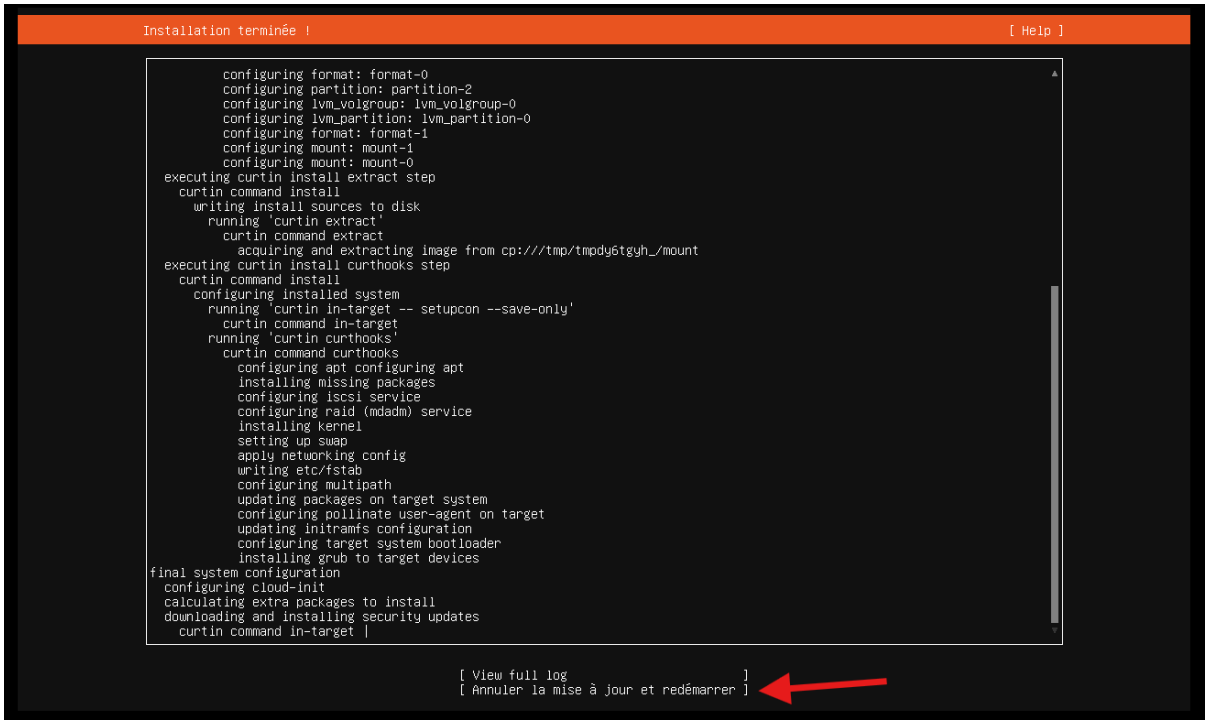
Appuyer sur Terminé, il n’y a pas besoin de OpenSSH.



Attendre la fin de l’installation.



Après avoir attendu, sélectionner Annuler la mise à jour et redémarrer.



Après s’être connecté avec les identifiants suite au redémarrage, mettre à jour le serveur avec cette commande.

```
hollo@dmz:~$ sudo apt update && sudo apt upgrade -y
```

B) Installation des dépendances requises

Ajouter le dépôt PPA Ondřej en effectuant ces commandes (nous servira à installer la version 7.4 de php).

```
hollo@dmz:~$ sudo apt install software-properties-common -y
```

```
hollo@dmz:~$ sudo add-apt repository ppa:ondrej/php -y_
```

```
hollo@dmz:~$ sudo apt update_
```

Installer les dépendances avec cette commande.

```
hollo@dmz:~$ sudo apt install apache2  mariadb-server php7.4 libapache2-mod-php7.4 php7.4-mysql php7
.4-xml php7.4-mbstring php7.4-curl php7.4-zip php7.4-gd unzip wget git -y
```

Activer les services apache2 et mariadb avec ces 2 commandes.

```
hollo@dmz:~$ sudo systemctl enable apache2
```

```
hollo@dmz:~$ sudo systemctl enable mariadb
```

Démarrer mariadb et apache2 avec cette commande.

```
hollo@dmz:~$ sudo systemctl start apache2 mariadb
```

(OPTIONNEL) Effectuer cette commande pour installer de manière sécurisé mariadb.

```
hollo@dmz:~$ sudo mysql_secure_installation
```

Effectuer cette commande pour entrer dans la console mariadb.

```
hollo@dmz:~$ sudo mysql -u root
```

Taper ces commandes à la suite pour créer la base de données ebrigade.

Créer la base de données.

```
MariaDB [(none)]> CREATE DATABASE ebrigade_db;_
```

Créer un utilisateur.

```
MariaDB [(none)]> CREATE USER 'arthur'@'localhost' IDENTIFIED BY 'Monsieursossou67';_
```

Accorder tous les privilèges au nouvel utilisateur créé.

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON ebrigade_db.* TO 'arthur'@'localhost';
```

Mettre à jour les privilèges.

```
MariaDB [(none)]> FLUSH PRIVILEGES;_
```

Quitter la base de donner en rentrant EXIT; .

```
MariaDB [(none)]> EXIT;
Bye
hollo@dmz:~$
```

C) Téléchargement et déploiement de eBrigade

Télécharger le paquet de eBrigade avec cette commande.

```
hollo@dmz:~$ sudo wget https://ciscoursegoules.fr/wp-content/uploads/2022/08/ebrigade-5.3.2.zip_
```

Décompresser le paquet de eBrigade avec cette commande.

```
hollo@dmz:~$ unzip ebrigade-5.3.2.zip_
```

Copier le répertoire de eBrigade dans le répertoire web.

```
hollo@dmz:~$ sudo cp -r ~/ebrigade-5.3.2 /var/www/html/ebrigade_
```

Accorder les droits et les privilèges au répertoire de eBrigade avec ces 2 commandes.

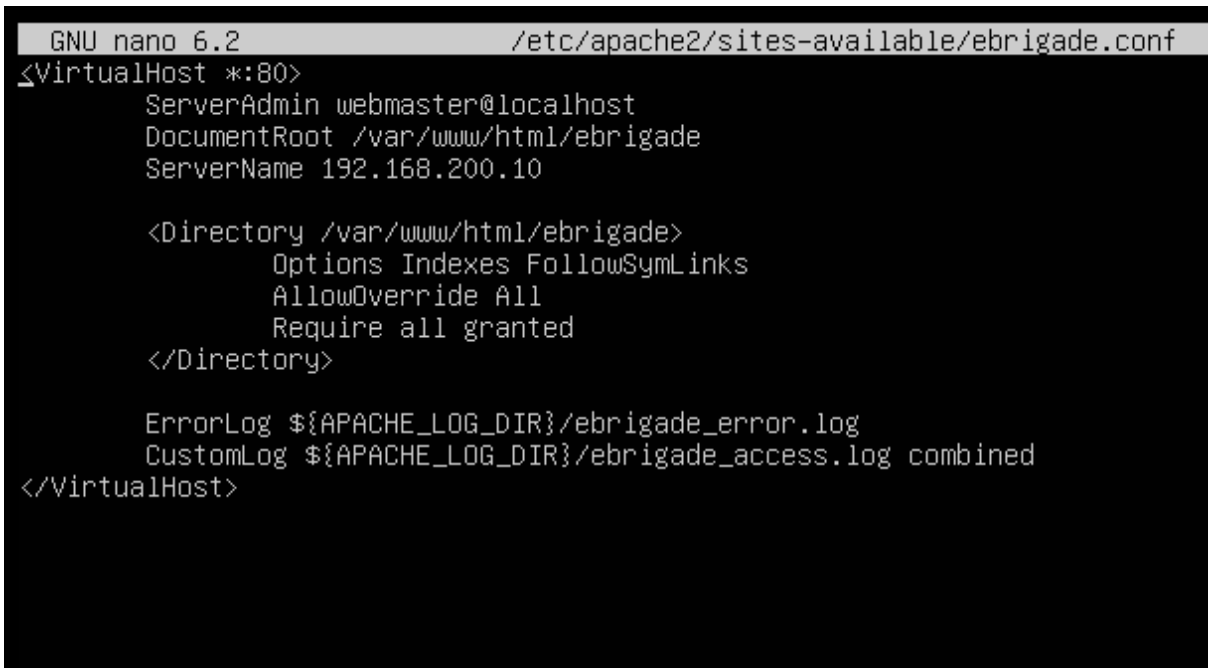
```
hollo@dmz:~$ sudo chown -R www-data:www-data /var/www/html/ebrigade
```

```
hollo@dmz:~$ sudo chmod -R 755 /var/www/html/ebrigade
```

Créer le fichier de configuration de eBrigade pour apache2.

```
hollo@dmz:~$ sudo nano /etc/apache2/sites-available/ebrigade.conf
```

Voici les paramètres à entrer (à adapter selon la configuration).



Faire CTRL + X, puis Y et Enter pour quitter et sauvegarder la configuration.

Activer le site en tapant ces commandes.

```
hollo@dmz:~$ sudo a2ensite ebrigade.conf
```

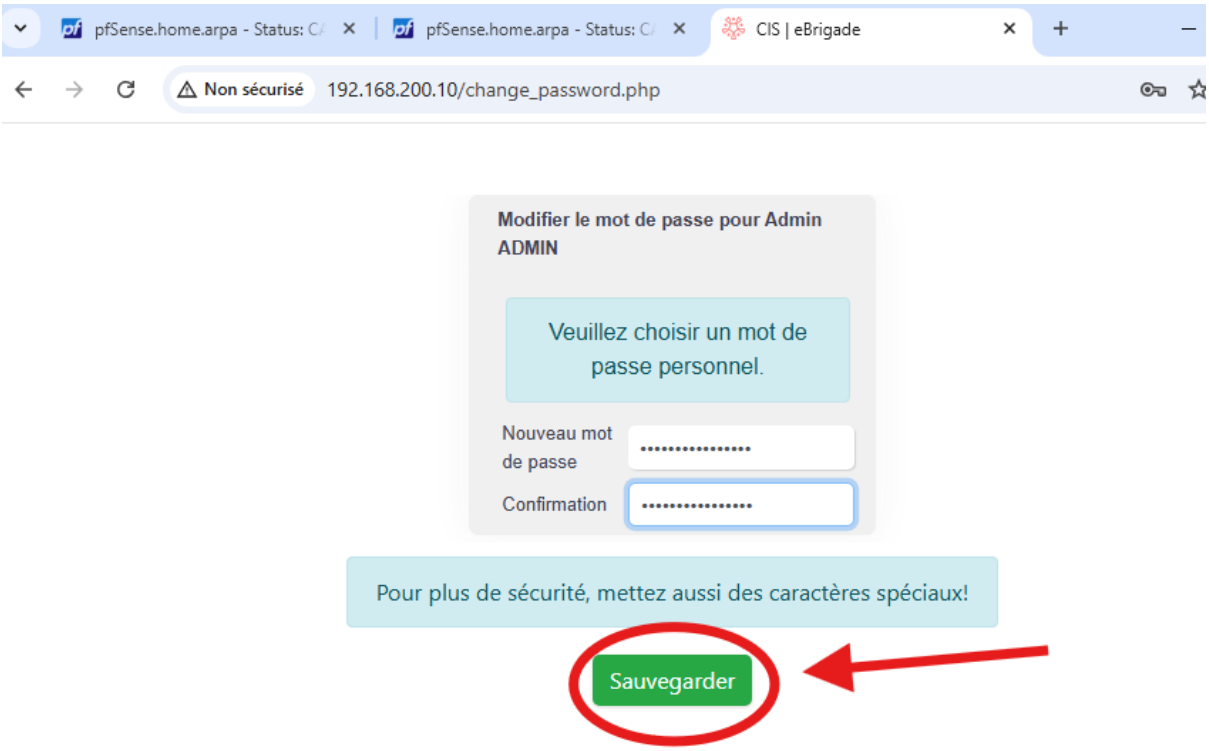
```
hollo@dmz:~$ sudo a2enmod rewrite
```

```
hollo@dmz:~$ sudo systemctl reload apache2
```

D) Première connexion à l'interface web de eBrigade

Depuis un client Windows, accéder à l'interface web de eBrigade via l'adresse IP du serveur (192.168.200.10 dans mon cas).

Entrer un nouveau mot de passe puis cliquer sur Sauvegarder.

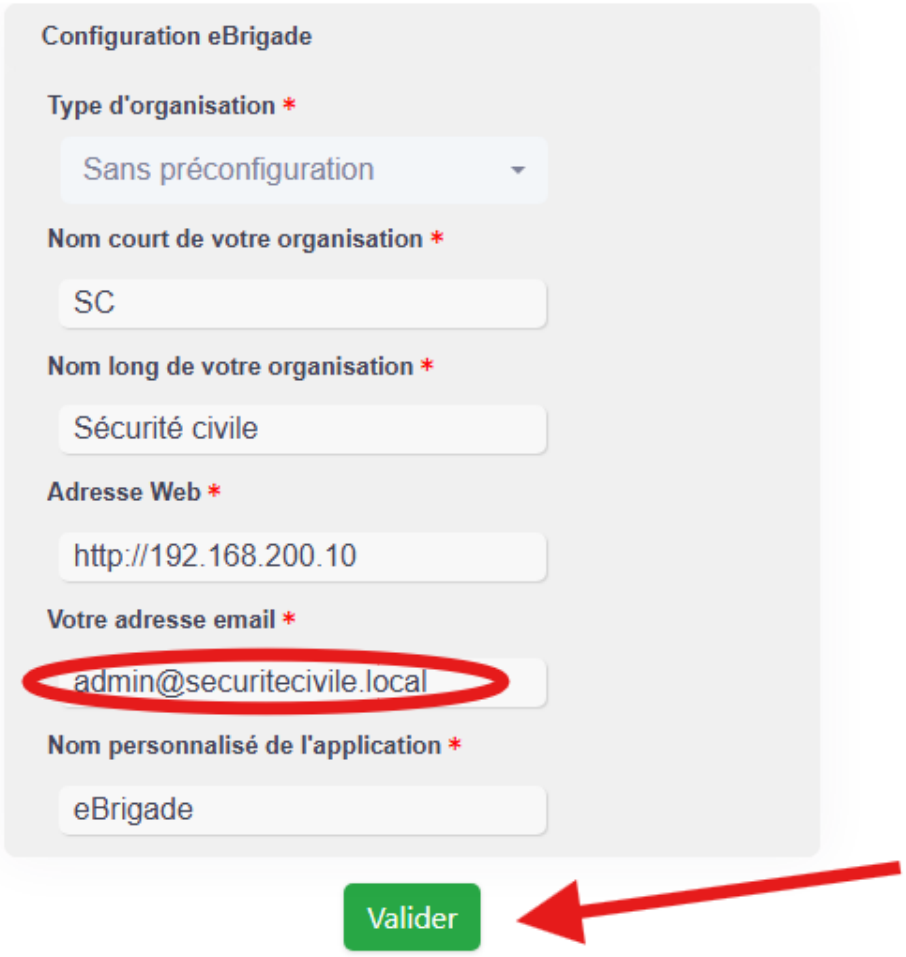


Cliquer sur Continuer.

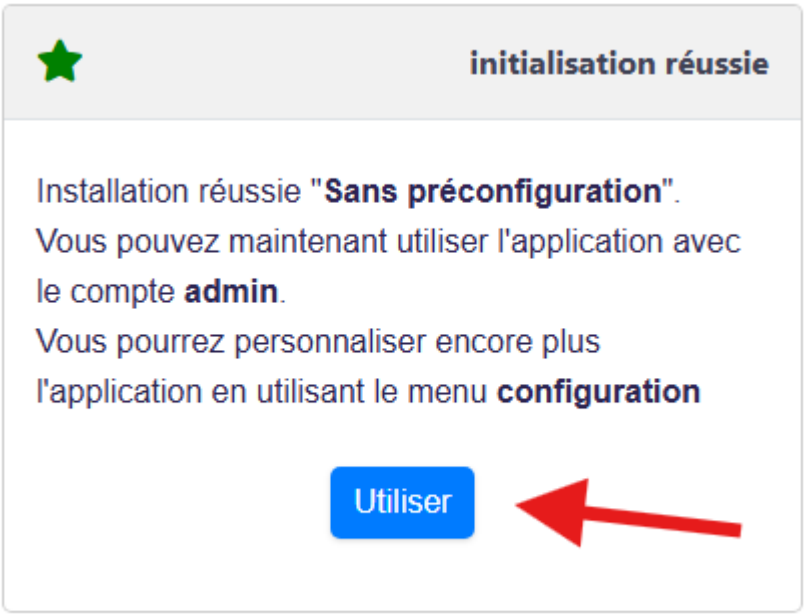
Voici les paramètres à entrer pour la configuration de eBrigade.

Ajouter l'adresse mail admin du serveur de messagerie Modoboa.

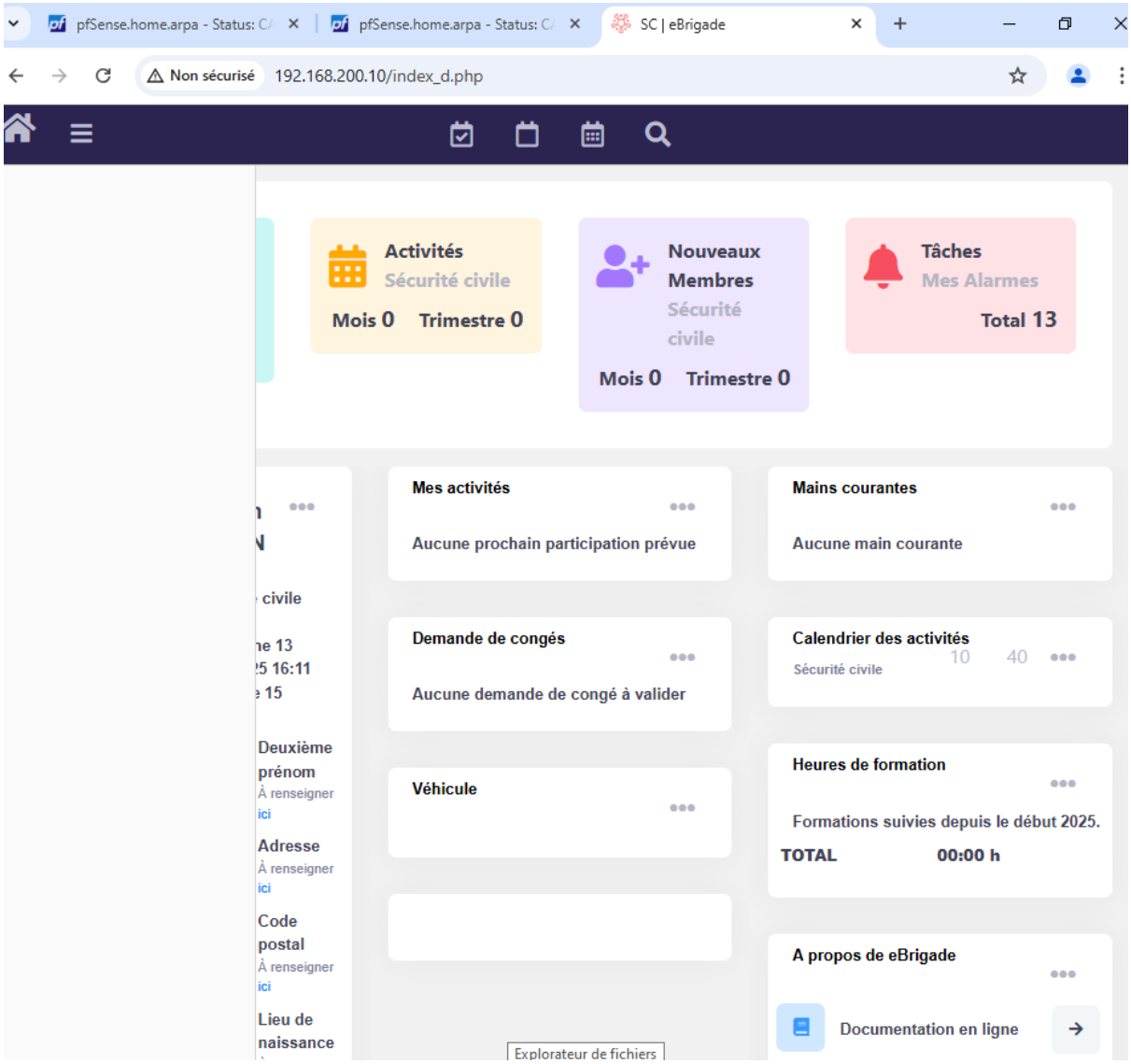
Cliquer ensuite sur Valider.



Cliquer sur Utiliser.

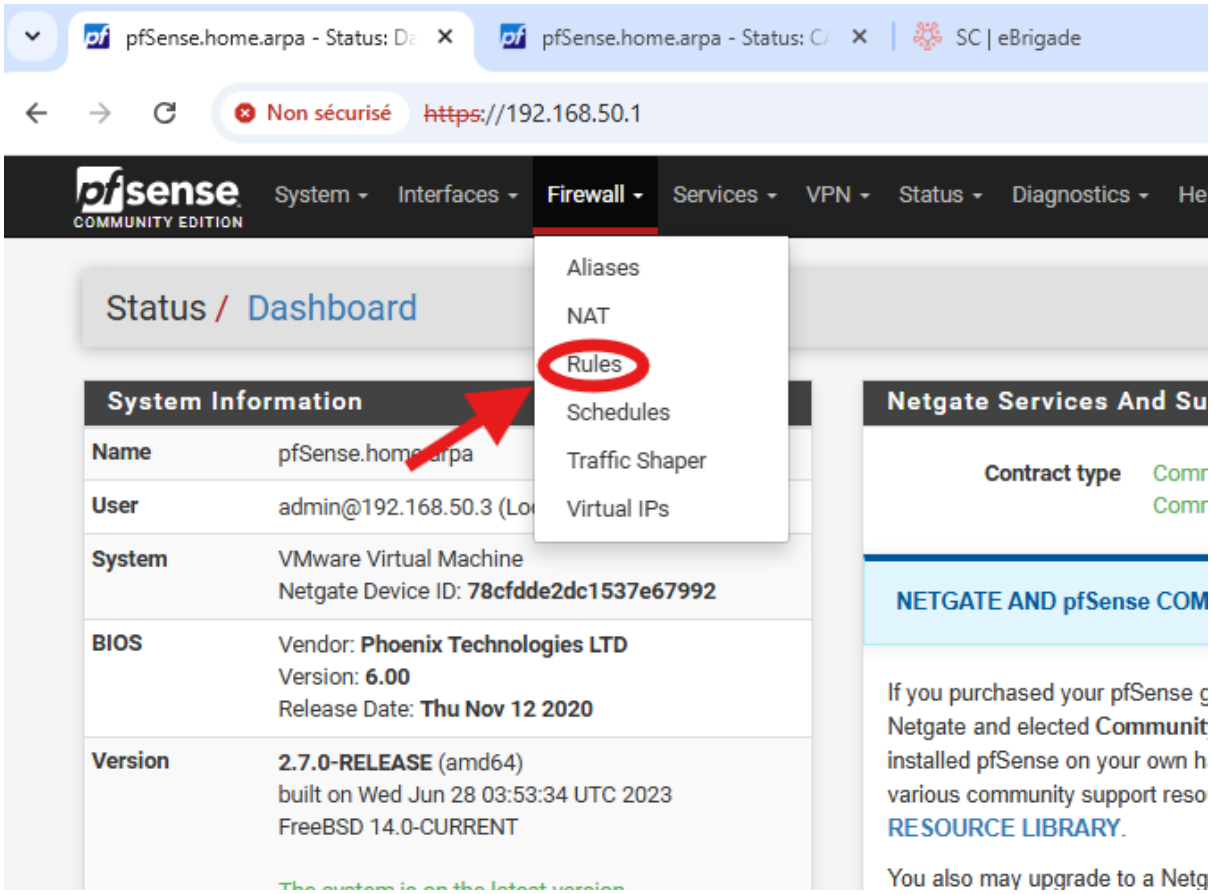


Nous sommes bien connectés à l'interface web de eBrigade.

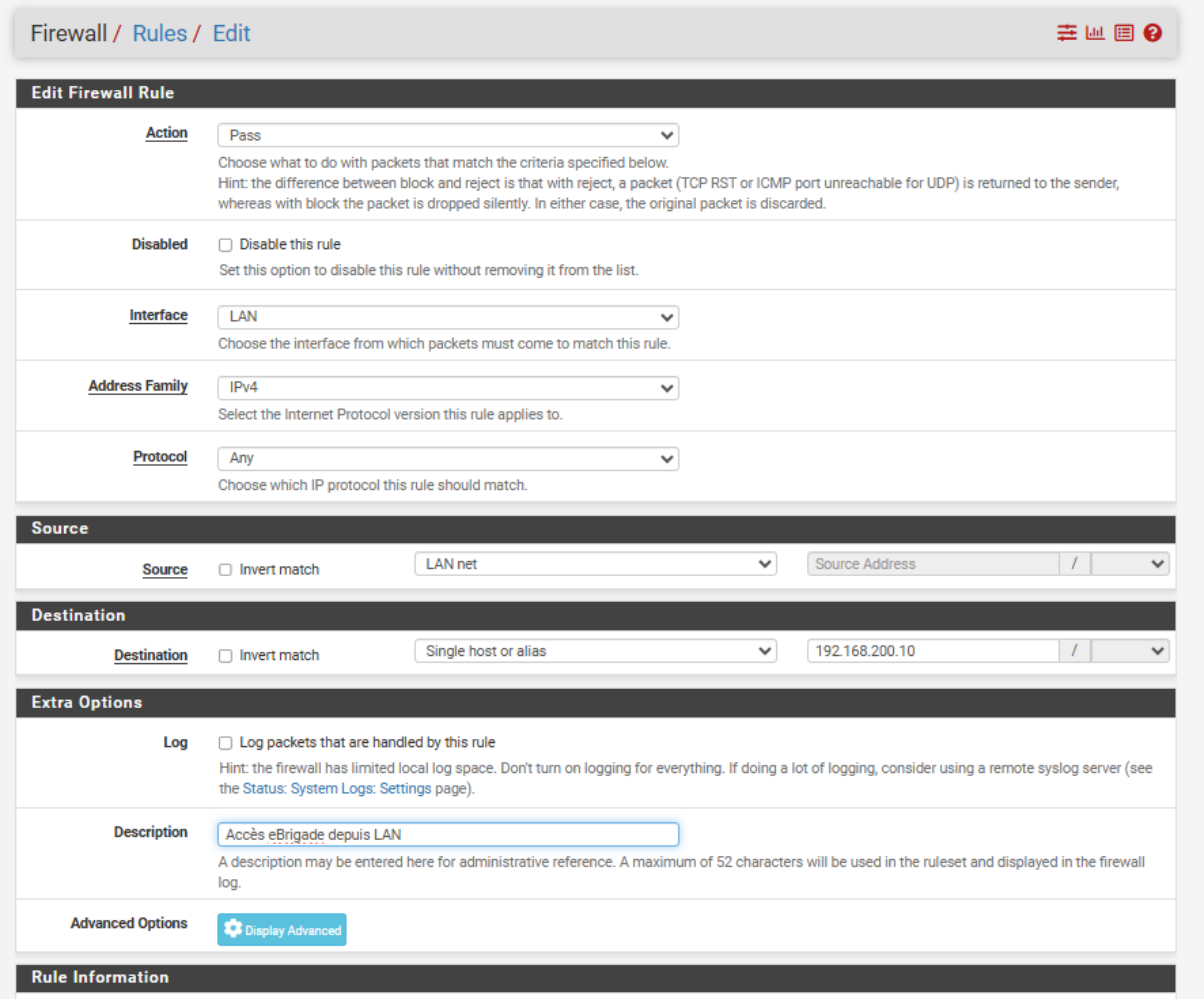


3) Règles de pare-feu sur PfSense

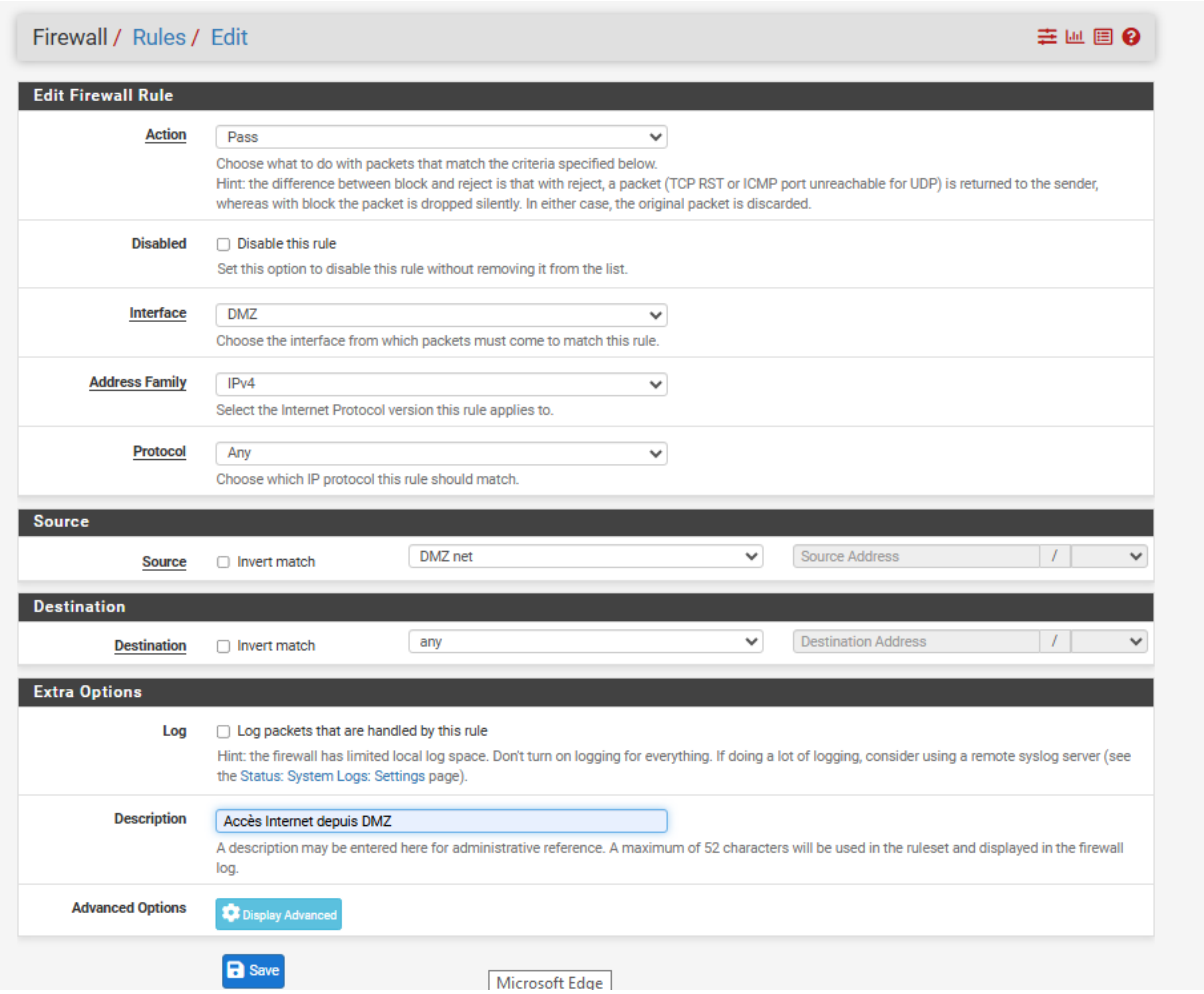
Sur le PfSense Master, aller dans Firewall puis Rules.



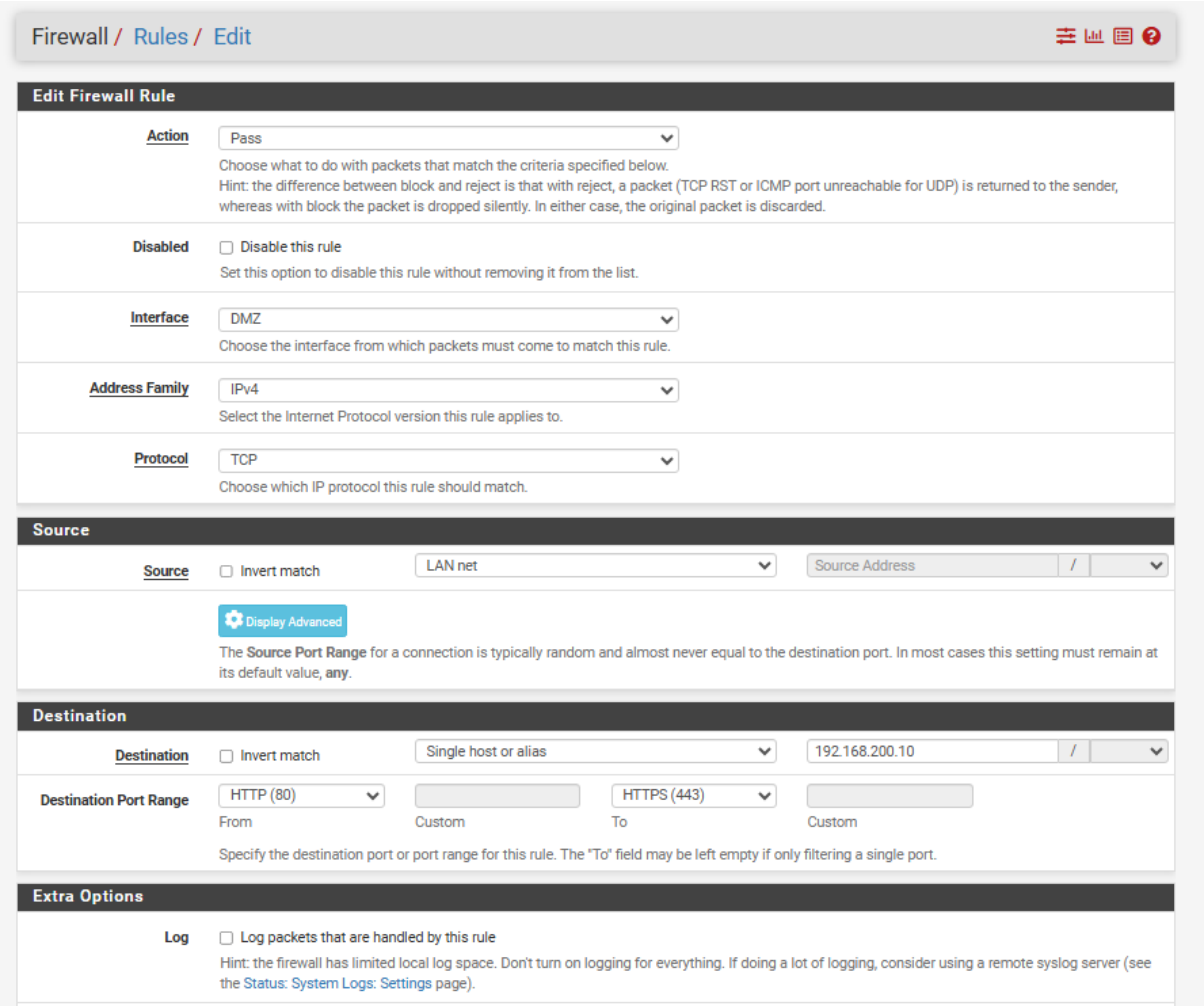
Ajouter une règle d'accès depuis LAN vers DMZ.



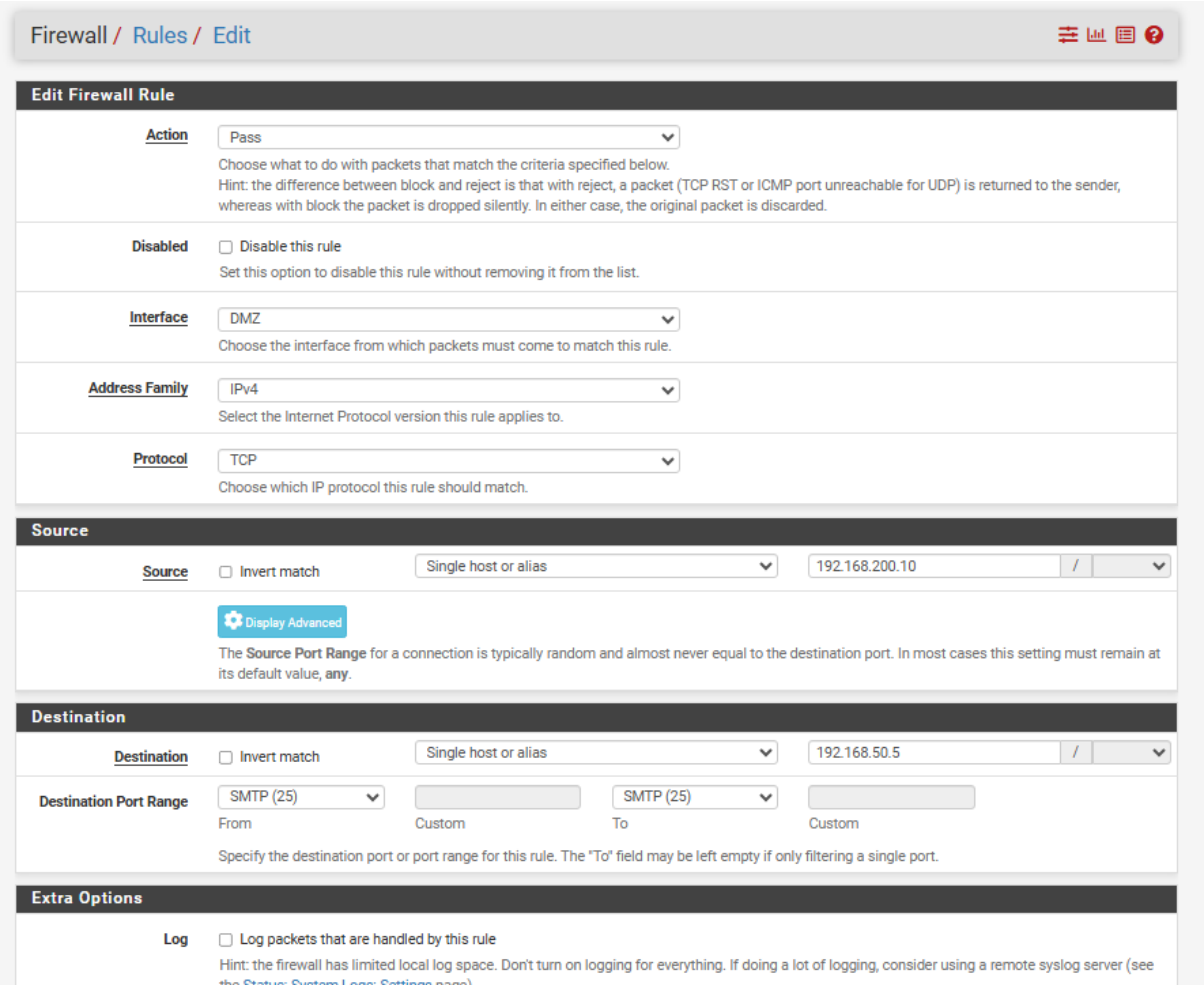
Ajouter une règle d'accès DMZ vers WAN.



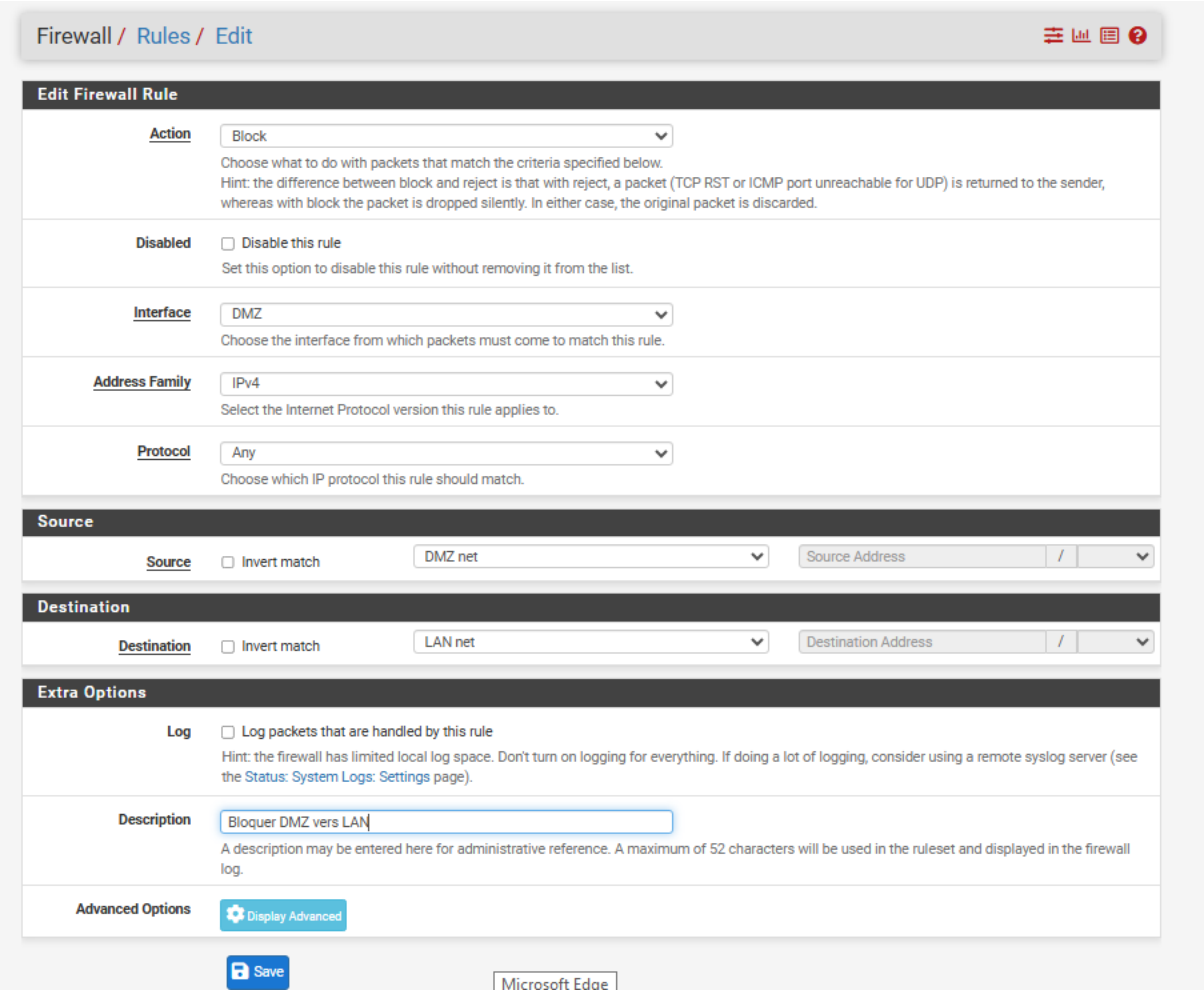
Ajouter une règle d’accès Web à eBrigade depuis LAN.



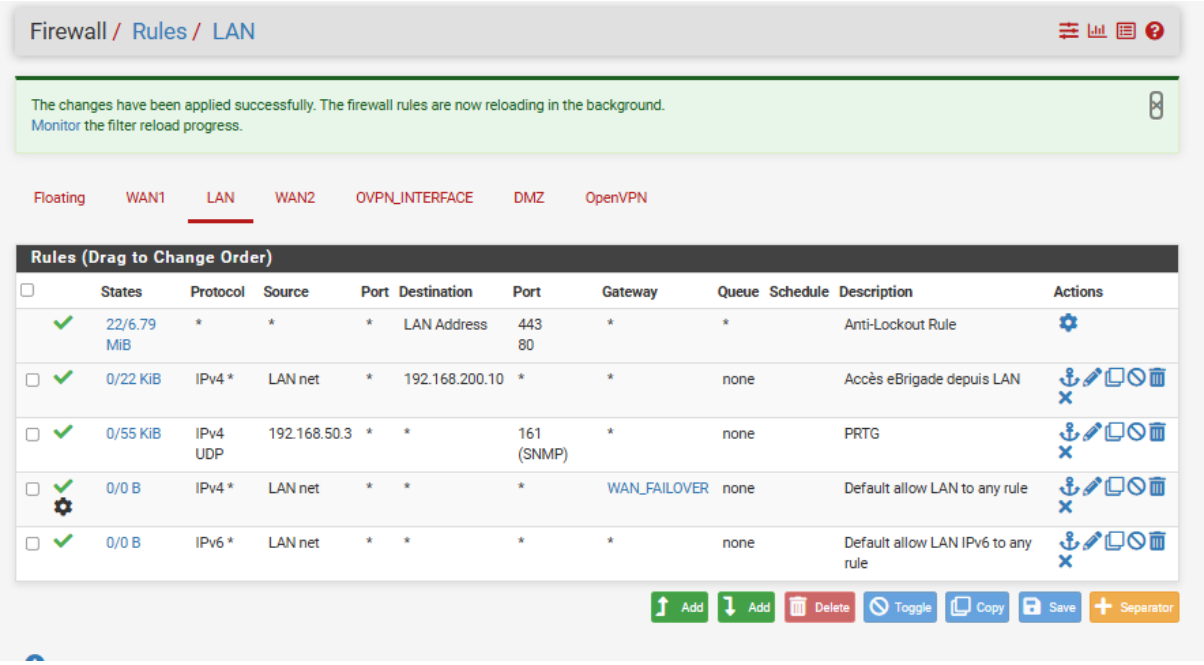
Ajouter une règle vers Modoboa.



Ajouter une règle qui bloque DMZ > LAN.



Voici un screen de la configuration des règles sur l'interface LAN.



Voici un screen de la configuration des règles sur l'interface DMZ.