pfSense

GUIDE D'INSTALLATION & CONFIGURATION

Réalisé par :

Thanina ZERGUINI

Mohand KELALI

Introduction

Ce document a pour but d'installer et d'administrer un Firewall pfSense, suivant un certain nombre d'étapes.

La réalisation de ce document nécessite un baguage technique en réseau (protocoles réseaux, configuration commutateur et routeur…) ainsi qu'en système (OS, Rôles et fonctionnalités, Machines virtuelles…). ☺


Firewall

Présentation Firewall

C’est quoi ?

- Un pare-feu est un logiciel et/ou un matériel qui permet de sécuriser un réseau, en définissant quels sont les types de communications autorisées sur ce réseau informatique.

Modèle OSI & Firewall

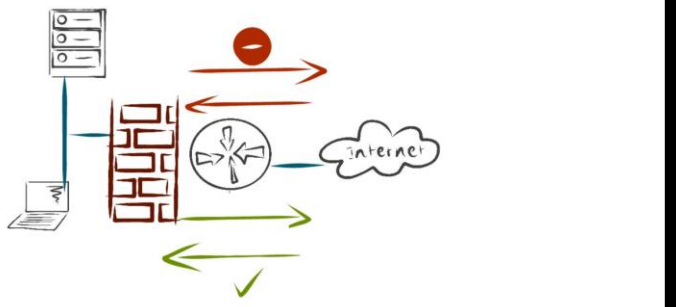
- Un firewall qui se base sur les couches 3 et 4 permet de contrôler les adresses IP et les ports, alors qu’un firewall qui se base sur la couche 7 permet de bloquer l’utilisation d’un logiciel.

La politique de sécurité

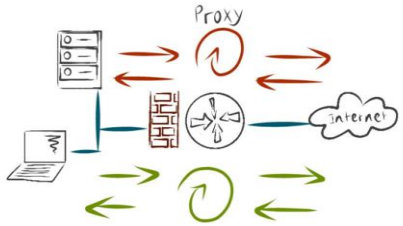
- Il existe deux façons de procéder pour fixer une politique de sécurité dans une entreprise, tout autoriser et bloquer les services dangereux ou tout bloquer et autoriser les services nécessaires à l’entreprise.

Architectures Firewall

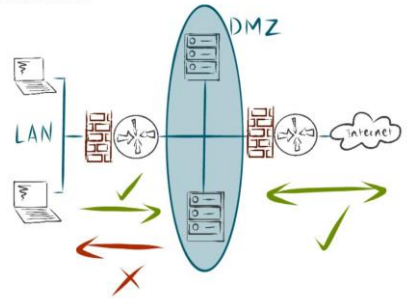
- **Architecture simple :**
  Le firewall est positionné entre le LAN et le WAN. Basée sur les couches réseau et transport et ne permet pas de filtrer au niveau applicatif.



- **Architecture proxy :**
  La même architecture que l’architecture simple mais on ajoute un filtre, au niveau de la couche applicative. Ceci va permettre d'empêcher l’utilisation du peer-to-peer.



- **Zone dématérialisé :**
  La DMZ est une architecture qui permet de sécuriser un réseau local, que sera accessible sur Internet.




TP

Présentation TP

Enoncé

- Dans ce TP nous allons voir comment mettre en place et gérer un firewall : pfSense.

pfSense

- Un routeur / pare-feu, anciennement nommé OpenBSD packet filter.

Pourquoi pfSense ?

- Open Source.
- Stable.
- Multifonctions.

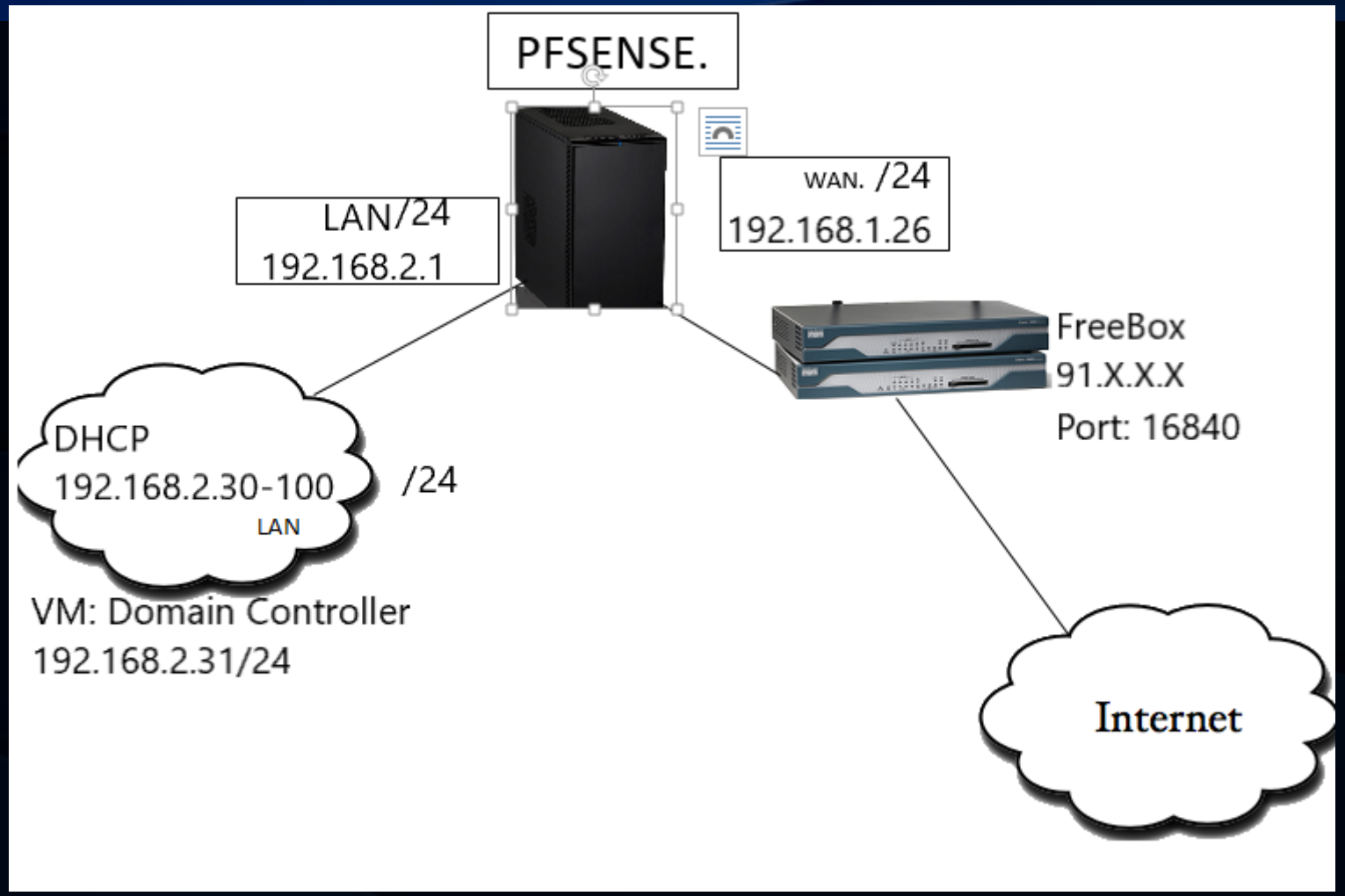
Scénarios de déploiement

- Firewall.
- Routeur & Switch.
- Modem.
- VPN.

Mode d'administration

- Console.
- WebGUI.

Schématiquement

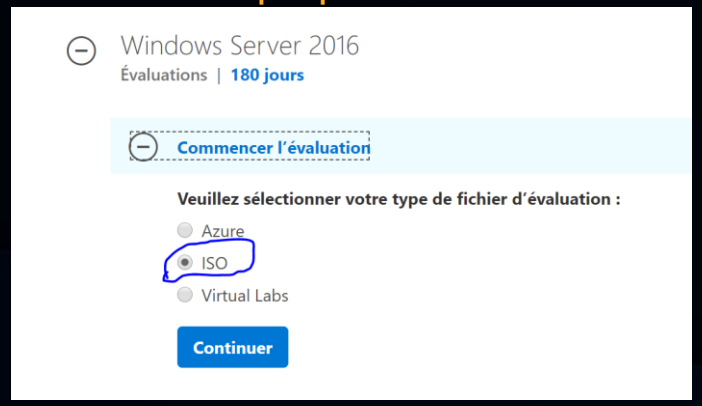



Domain Controller

Installation Domain Controller

1. ISO Windows Server 2016

- Télécharger l'ISO Windows Server 2016 via le lien suivant : https://www.microsoft.com/fr-fr/evalcenter/evaluate-windows-server-2016/, en sélectionnant les propriétés ci-dessous :



2. Création d'une VM

- Procéder à la création d'une VM DomainController_Server sous VMware.
- Caractéristiques de la VM :

RAM	2Go
HDD	40Go
Processeurs	2
NIC(LAN)	LAN Segment 1

3. Lancer l'installation

- Cliquer sur le bouton démarrer.
- Suivre les étapes d'installation via le lien: https://www.windows8facile.fr/installer-windows-server-2016/

Configuration Domain Controller

1. Mettre à jour l'OS

2. Ajouter le rôle Services AD DS

- Nom du domaine : formation.local
- Nom de la machine : DC
- @IP statique : 192.168.2.31 / 24
- Passerelle(LAN pfSense): 192.168.2.1 / 24
- @IP DNS : 192.168.2.31 / 24
- L'adresse IP statique du serveur est fixée après l'installation du serveur pfSense.

3. Désactiver la sécurité internet explorer

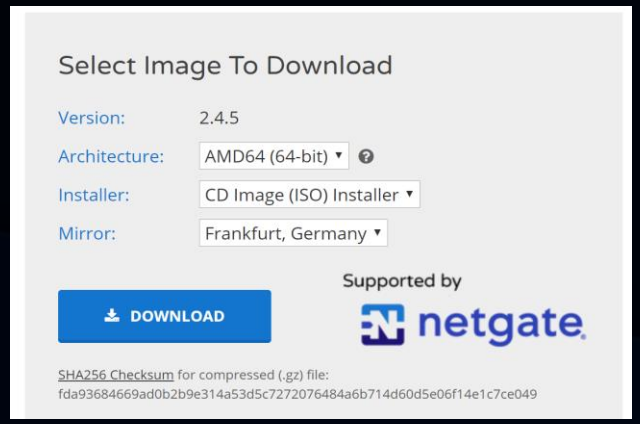
4. Désactiver le pare-feu


pfSense

Installation pfSense

1. ISO pfSense

- Télécharger l'ISO pfSense via le lien suivant : www.pfsense.org/download/, en sélectionnant les propriétés ci-dessous :



2. Création d'une VM

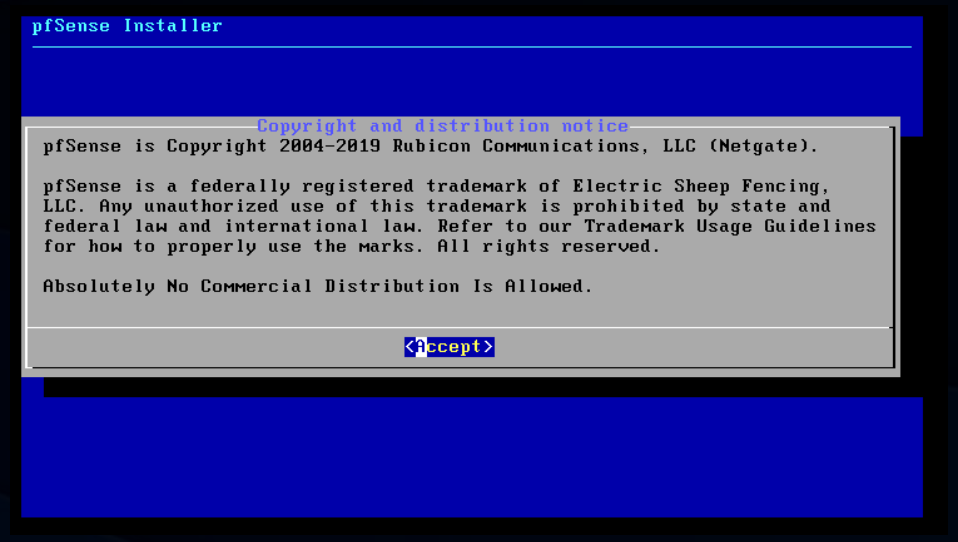
- Procéder à la création d'une VM pfSense_Server sous VMware.
- Caractéristiques de la VM :

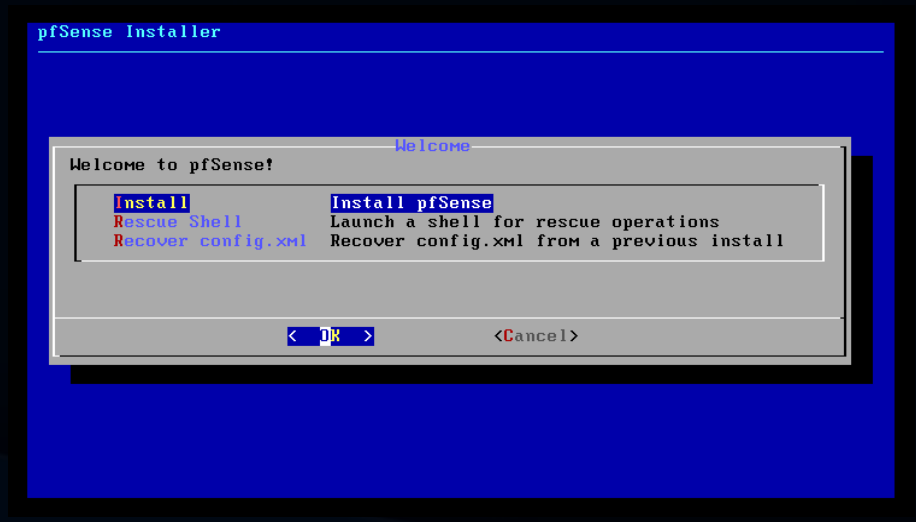
RAM	2Go
HDD	40Go
Processeurs	2
NIC1(WAN)	Bridge
NIC2(LAN)	LAN Segment 1

3. Lancer l'installation

- Cliquer sur le bouton démarrer.
- Suivre les étapes d'installation de pfSense en se basant sur les captures ci-dessous.

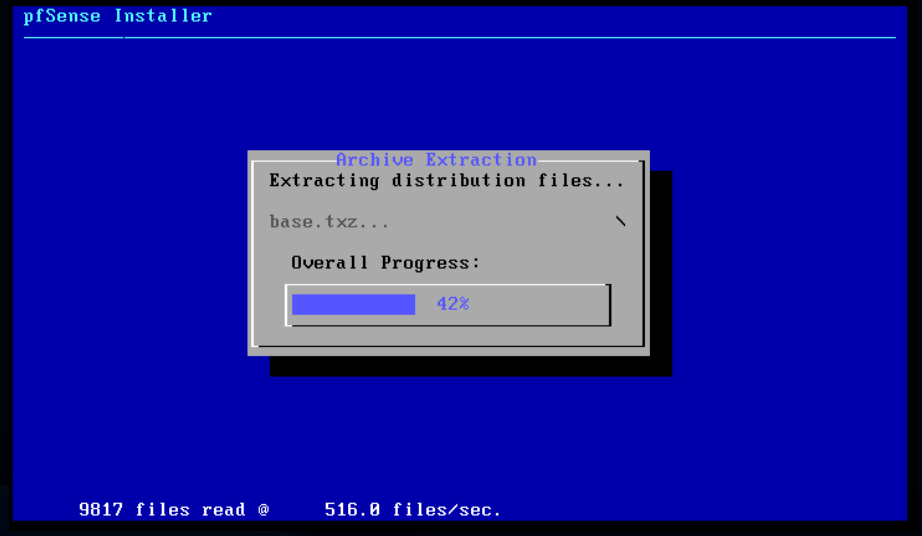
Installation pfSense





Installation pfSense

Installation pfSense



Installation pfSense

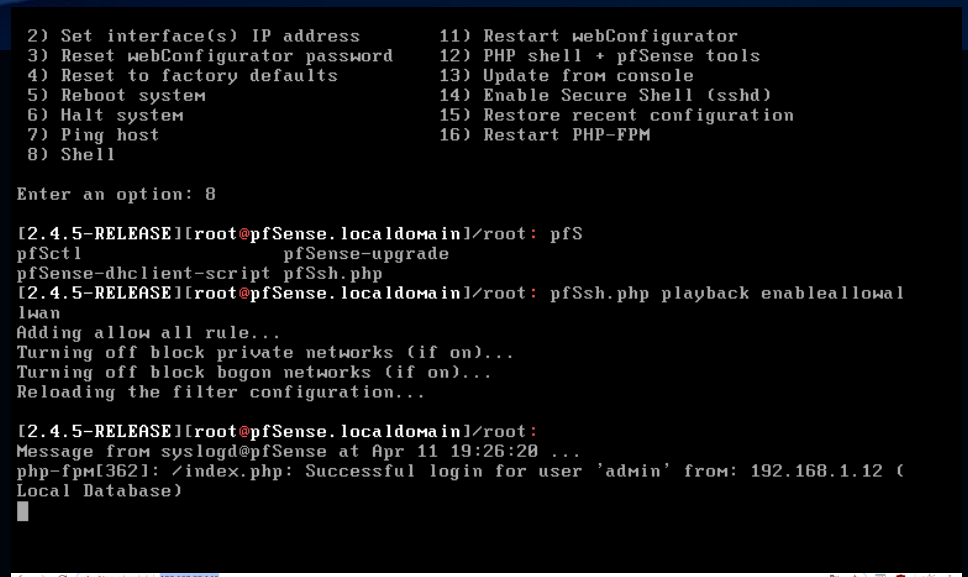
Configuration pfSense

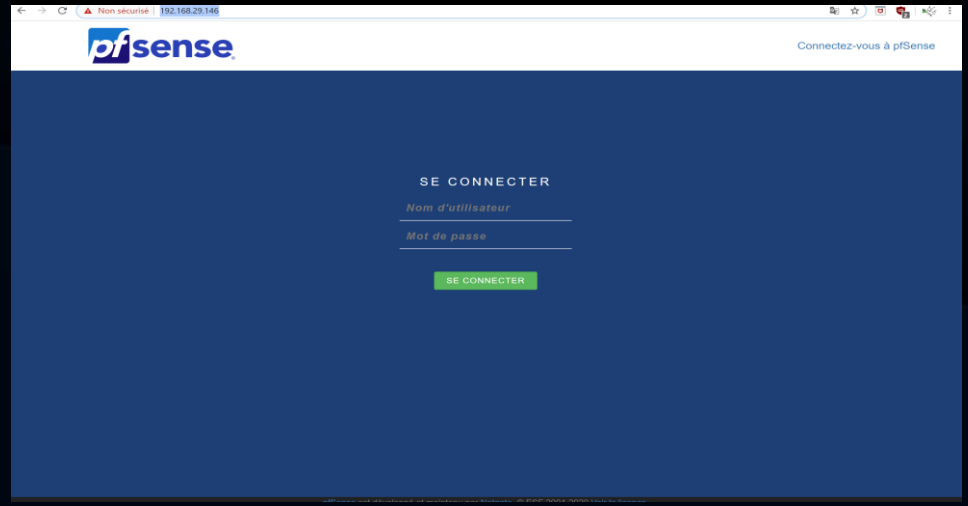
Autoriser l'accès à l'interface WebGUI depuis le WAN

- Entrer le chiffre 8, pour activer le mode shell.
- Taper la commande suivante : pfSsh.php playback enableallowallwan
- Taper ensuite la commande : exit
- Ouvrir un navigateur web et taper le lien suivant sur la barre de recherche (@IP WAN pfSense): https://192.168.1.26/
- L'accès vers l'interface WebGUI de pfSense est activé.
- Les identifiants par défaut pour se connecter à la plateforme:

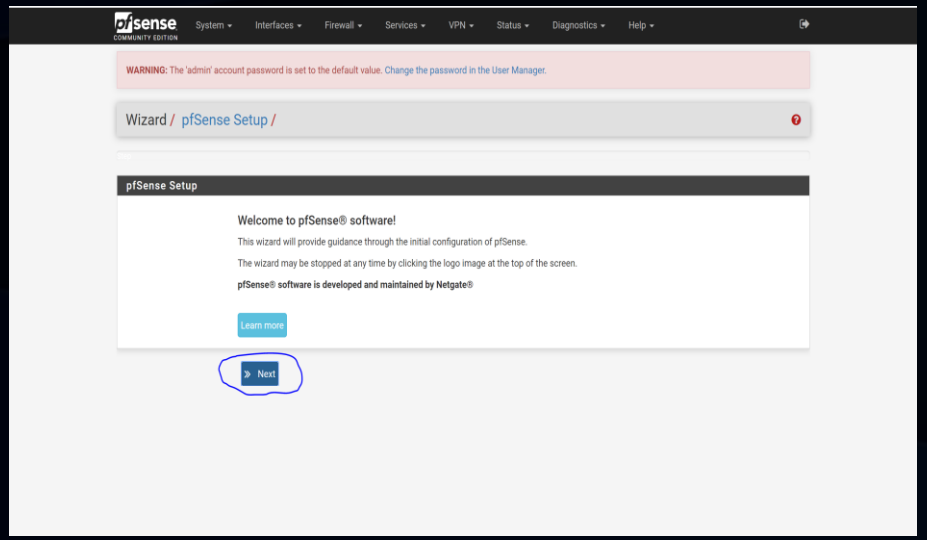
  Login : admin

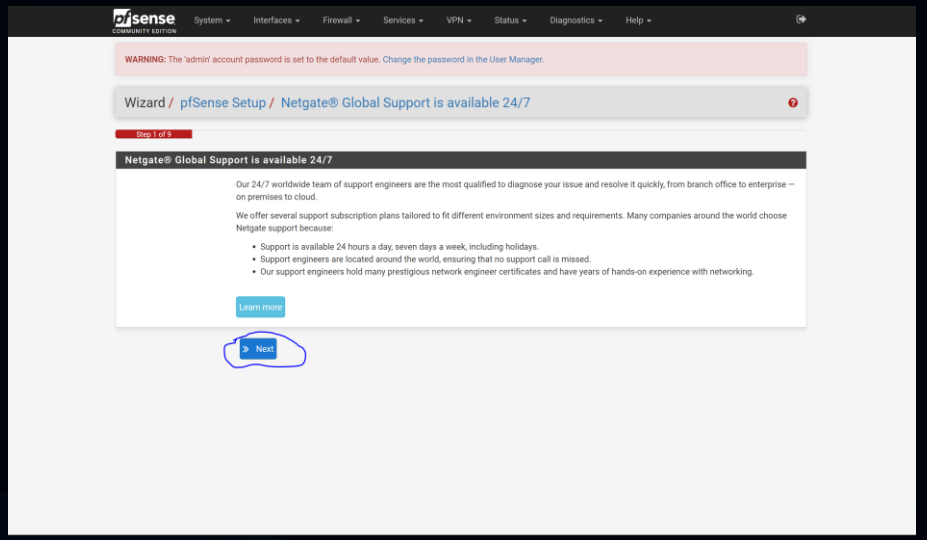
  Password : pfsense
- Pour les configurations qui suivent, à consulter les étapes ci-dessous (captures d'écran).





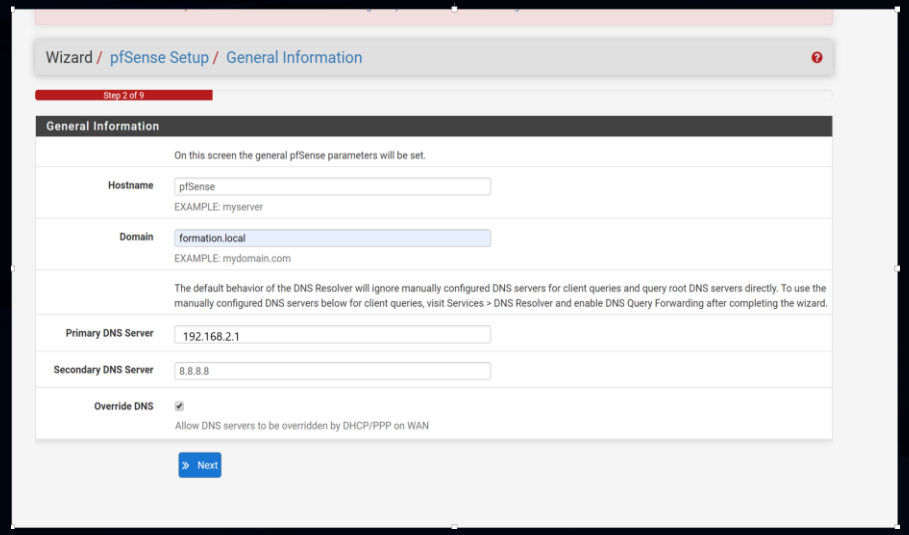
Configuration pfSense

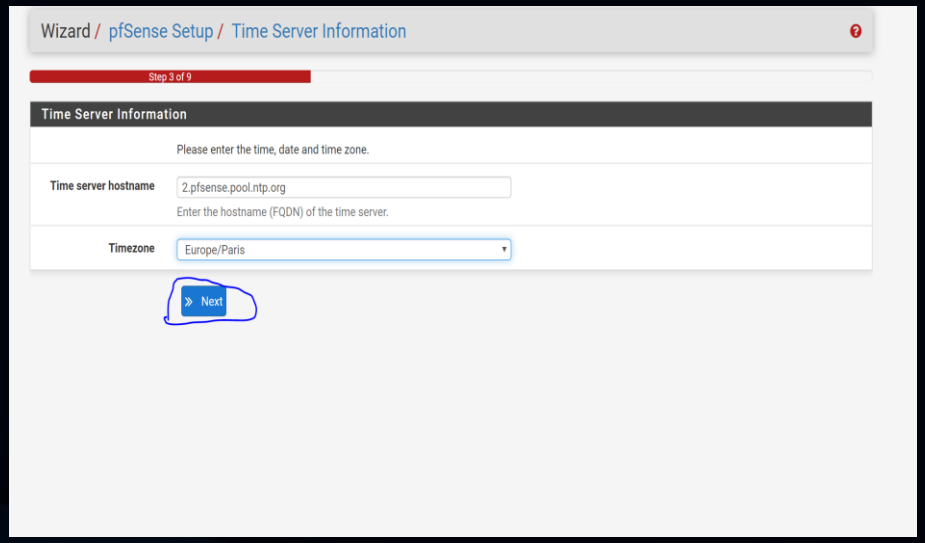




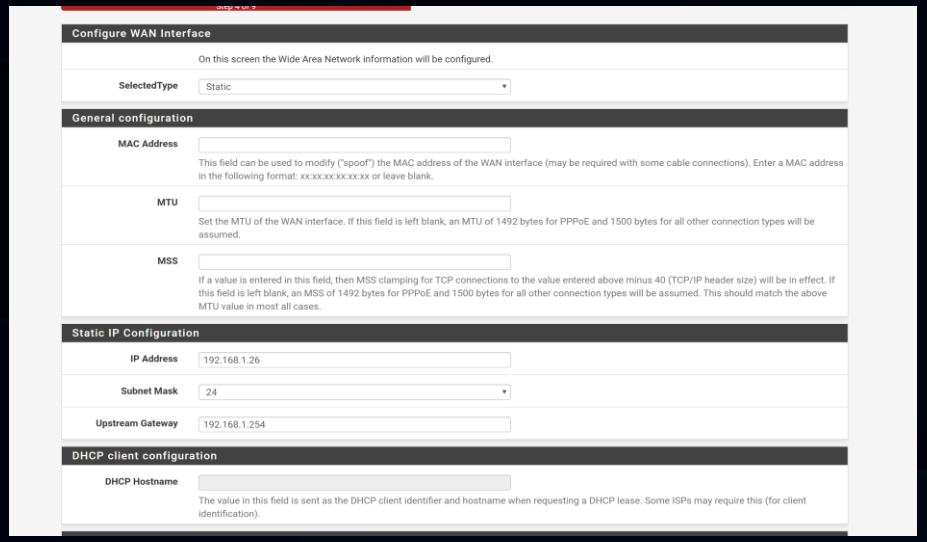
- IP WAN : 192.168.1.26/24 celle connectée à la box.
- IP LAN: 192.168.1.1/24 celle connectée au réseau local, switch.
- IP LAN: à modifier par 192.168.2.1/24

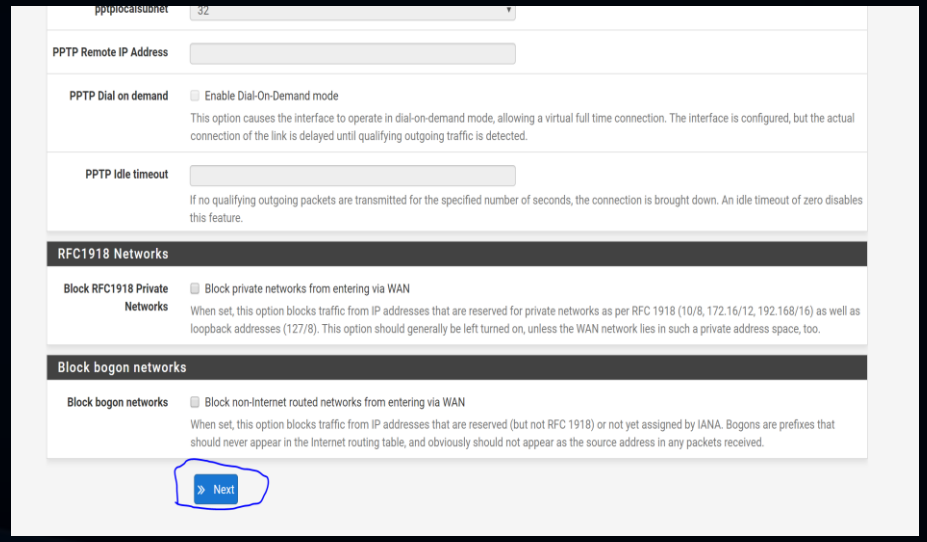
Configuration pfSense



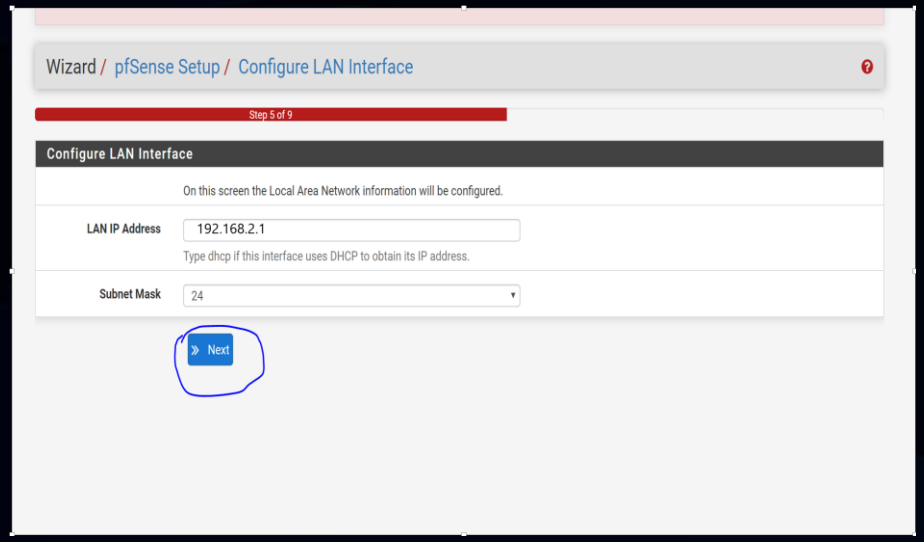


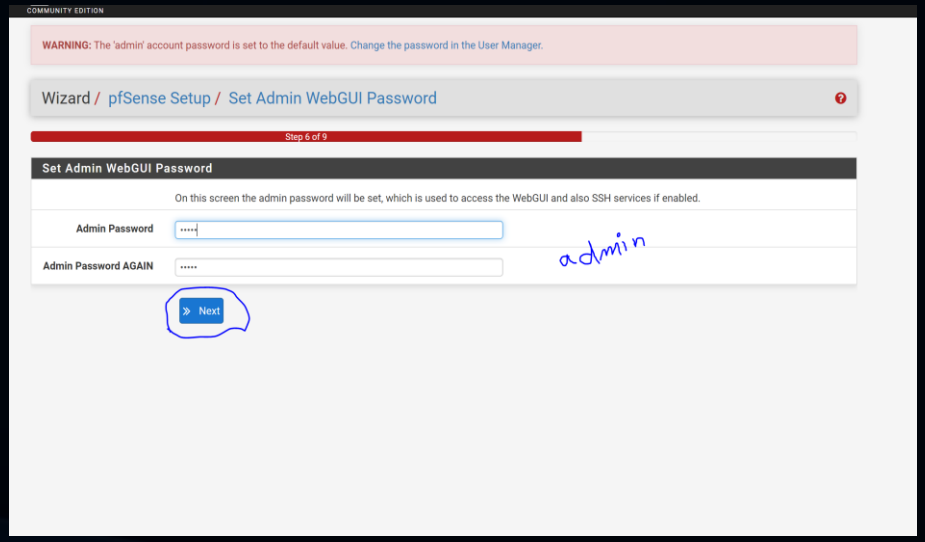
Configuration pfSense



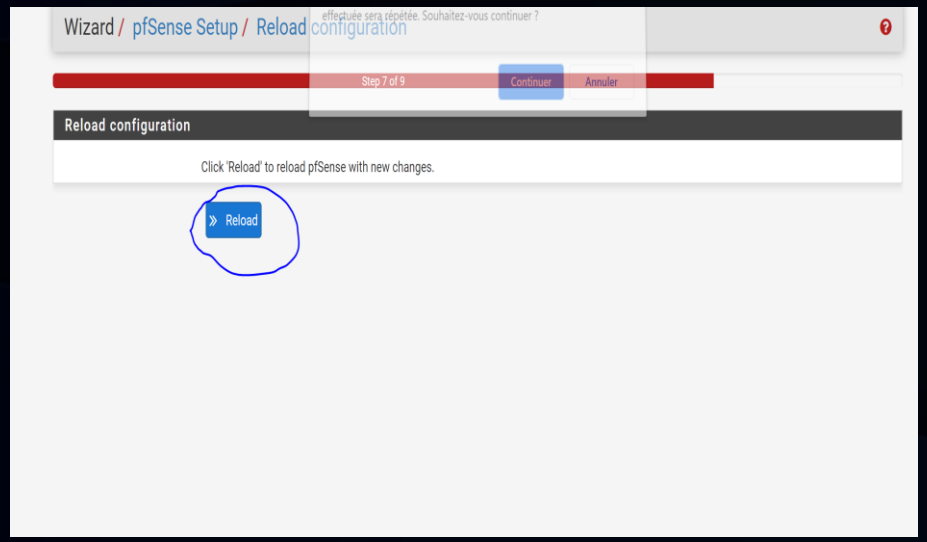


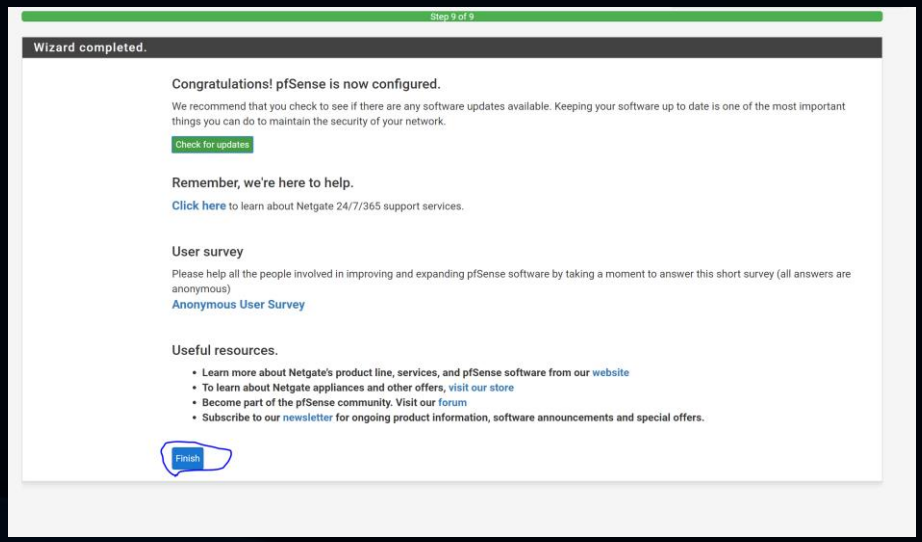
Configuration pfSense



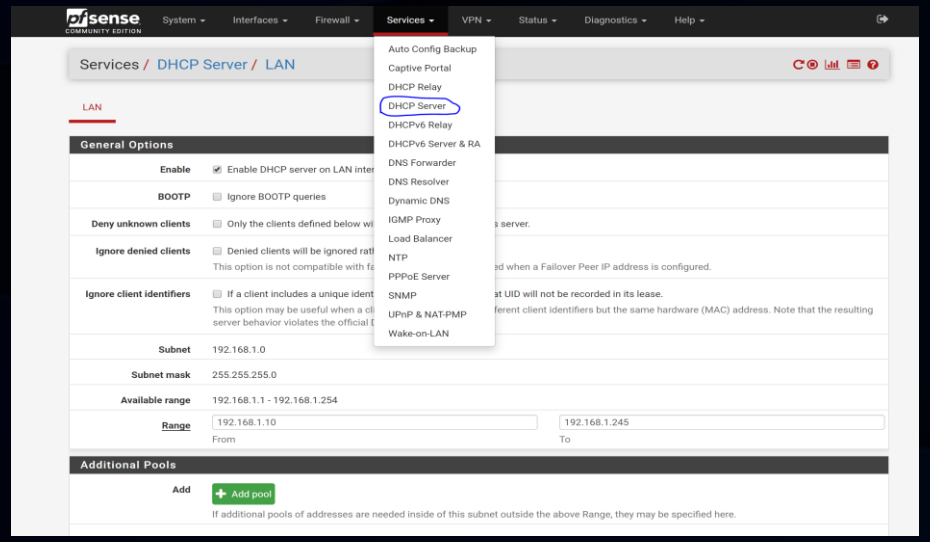


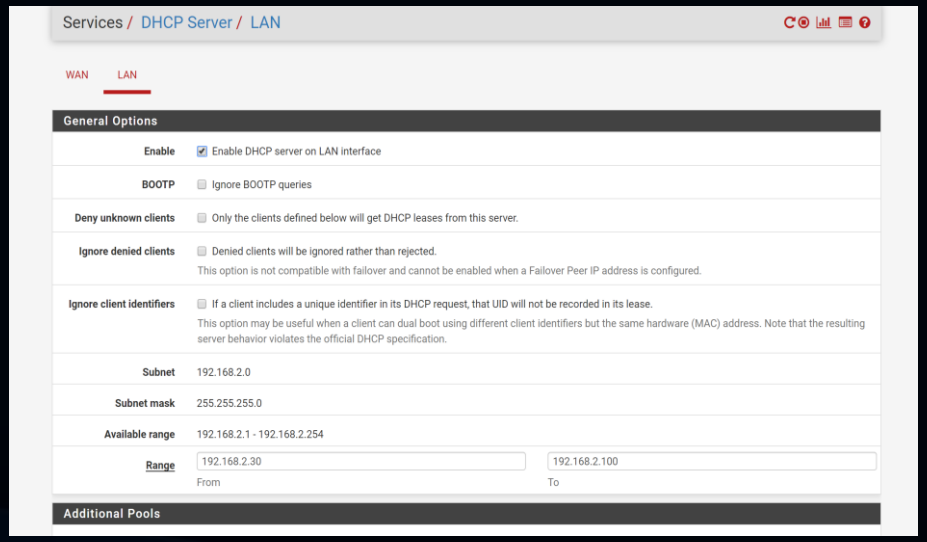
Configuration pfSense





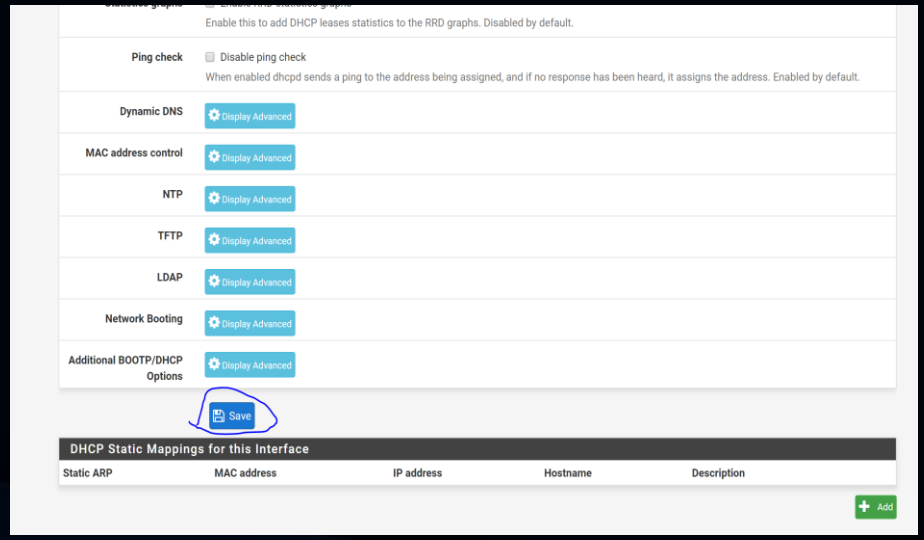
pfSense DHCP Server





- Mettre en place un serveur DHCP.
- Plage d’adresse : 192.168.2.30 - 100 / 24

pfSense DHCP Server

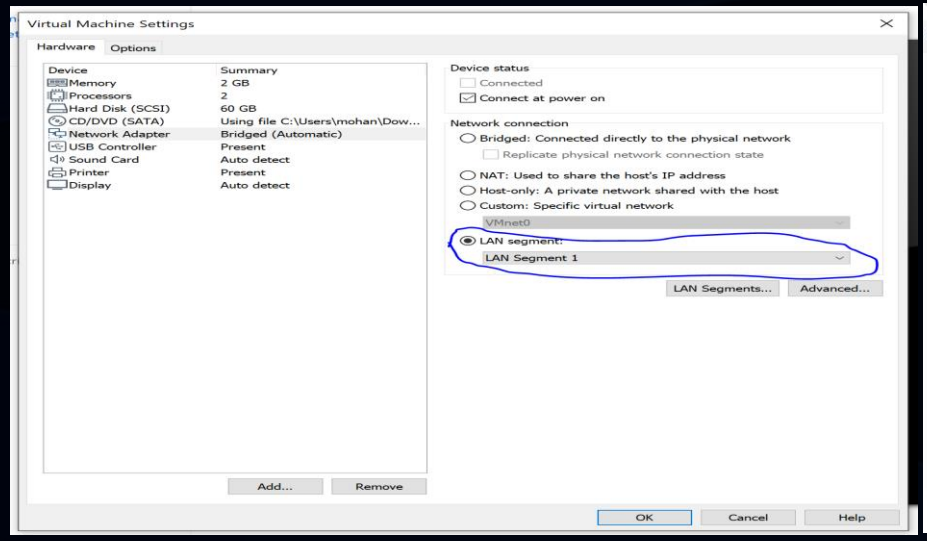


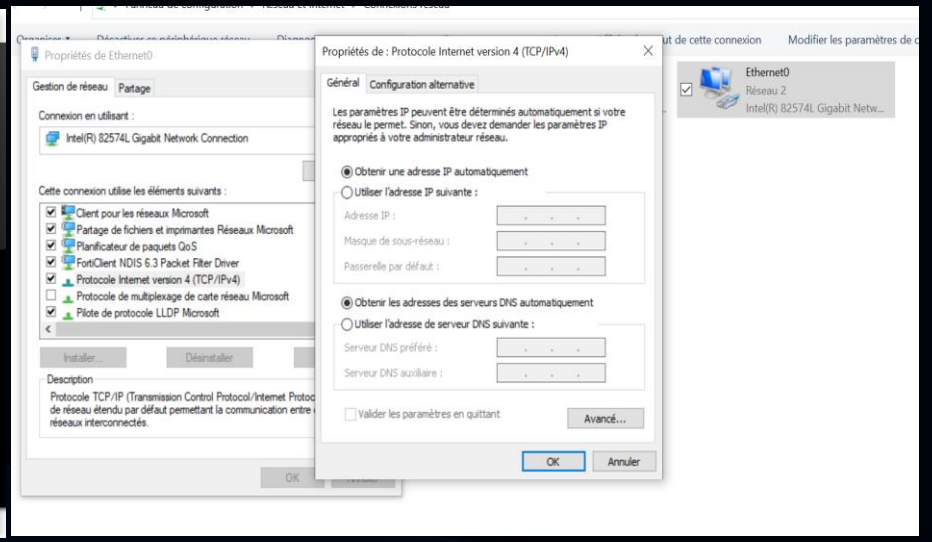
@IP serveur DNS : 192.168.2.1-> pfSense LAN


Machine Cliente

Installation & Configuration(sous Windows 7)

- Changer les paramètres de la carte réseau au niveau des postes clients





- Consulter, DHCP Leases à partir de l'interface WebGUI, onglet Status, pour constater l'affectation d'une adresse IP à la machine cliente.

A faire :

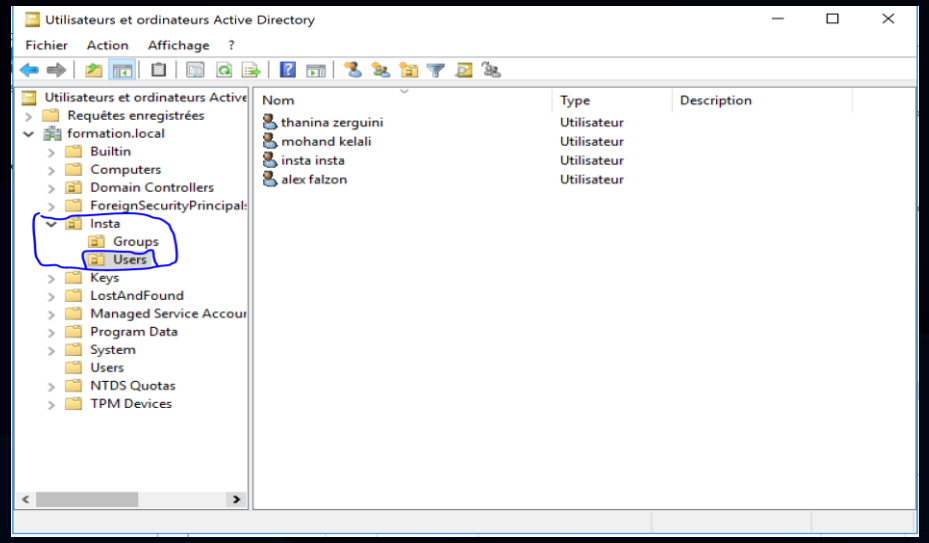
- Ajouter la machine dans le domaine formation.local
- Afin de contourner un problème d'ajout au domaine, à fixer @IP du DNS par: 192.168.2.31.
- Une fois ajoutée, remettre @IP DNS en automatique.

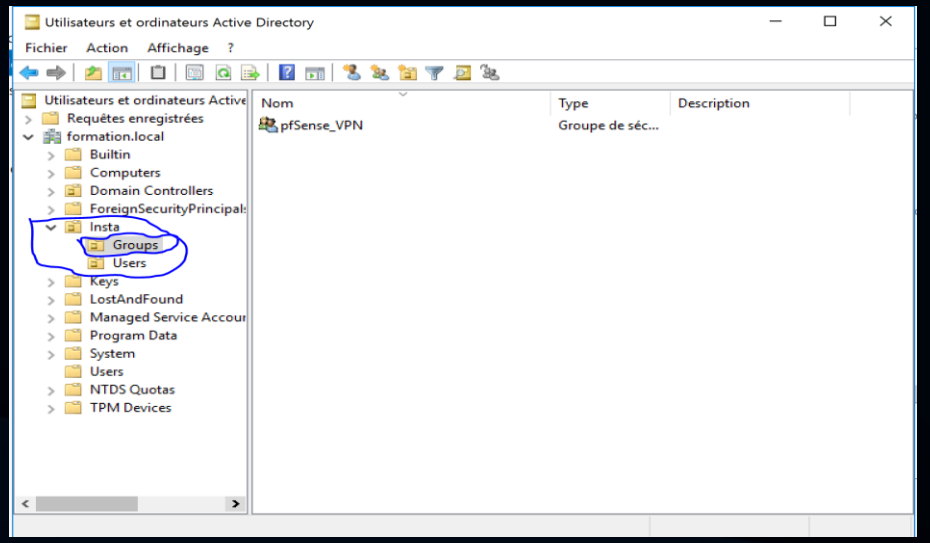

VPN

pfSense OpenVPN

Intégration avec LDAP

- OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel.
- L'objectif c'est de réaliser une connexion OpenVPN via un compte AD.



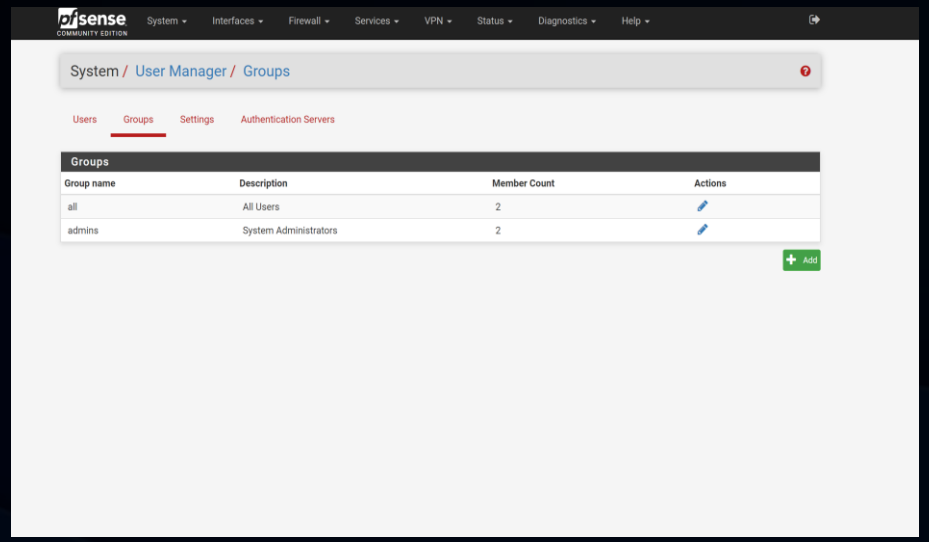


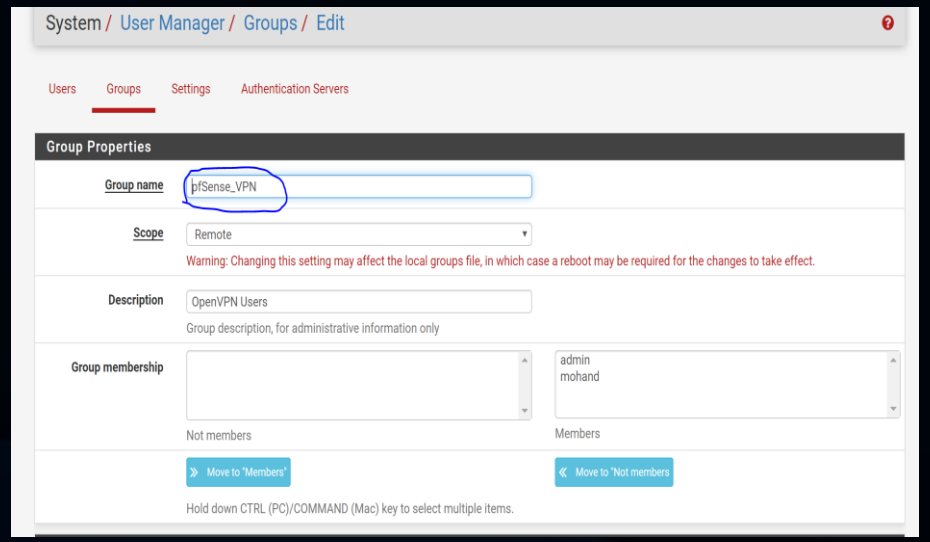
A partir de l'active directory :

- Créer des utilisateurs.
- Créer un groupe d'utilisateurs nommé : pfSense_VPN .
- Intégrer les utilisateurs dans le groupe.

pfSense OpenVPN

Intégration avec LDAP





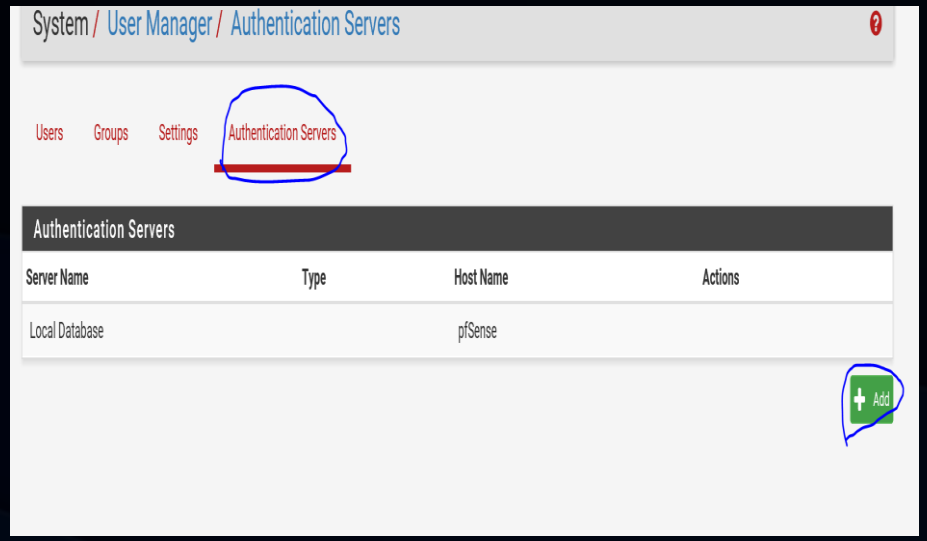
A partir de l'interface WebGUI :

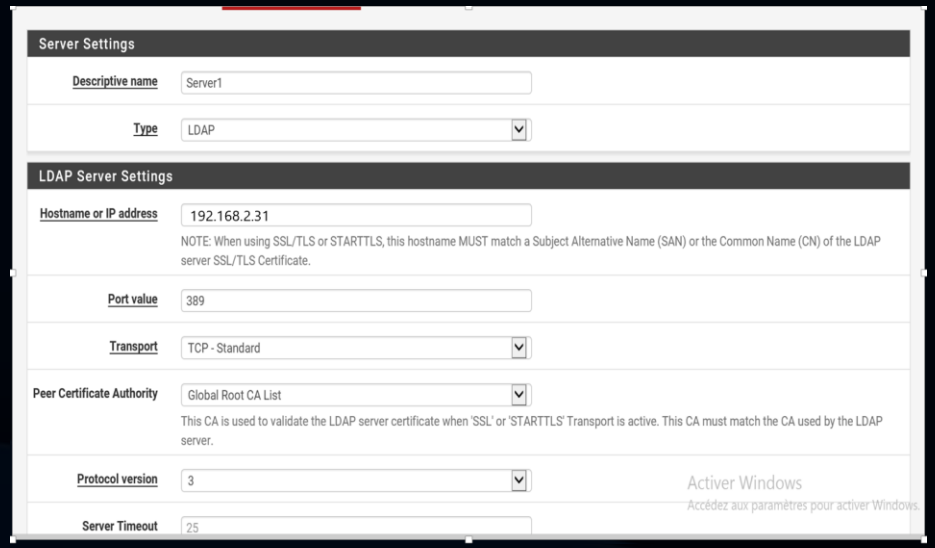
- Créer un groupe d'utilisateurs nommé : pfSense_VPN de même nom que celui sur l'AD.

pfSense OpenVPN

Intégration avec LDAP

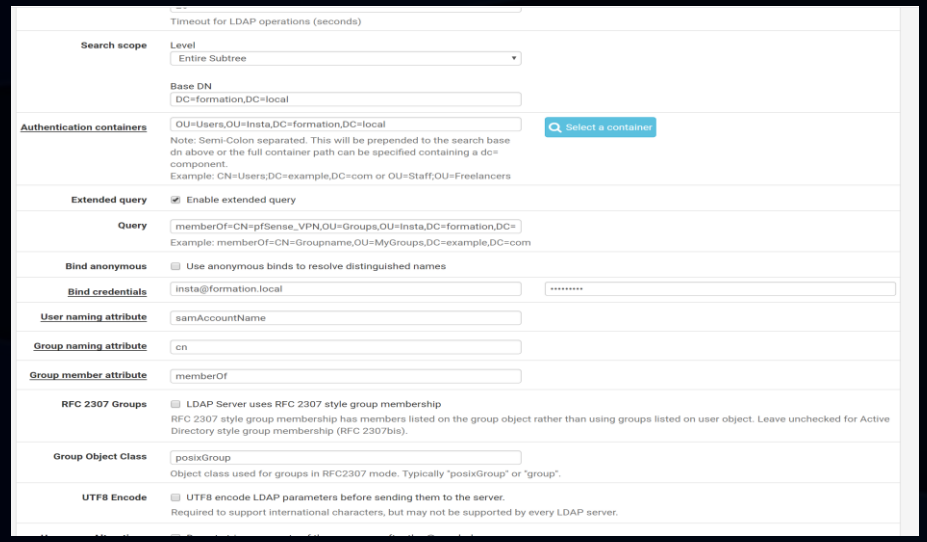
- Préparer l'authentification au serveur LDAP, Domain Controller d'adresse IP : 192.168.2.31
- Ouvrir le port 389/TCP au niveau du serveur DC (pare feu).

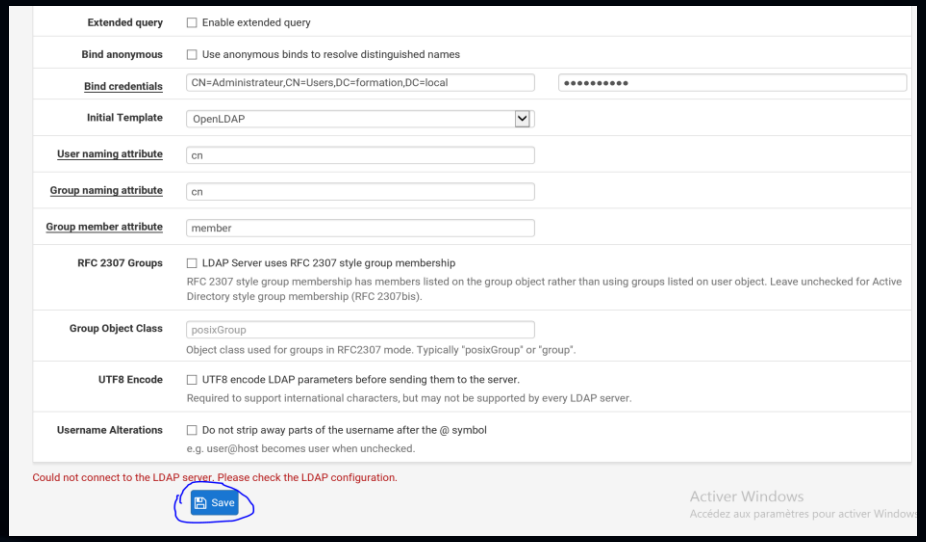




pfSense OpenVPN

Intégration avec LDAP

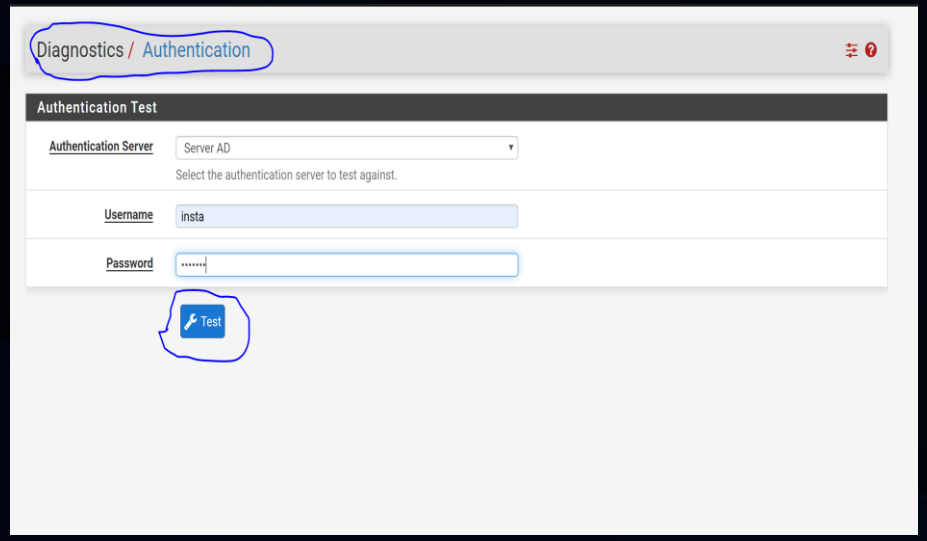


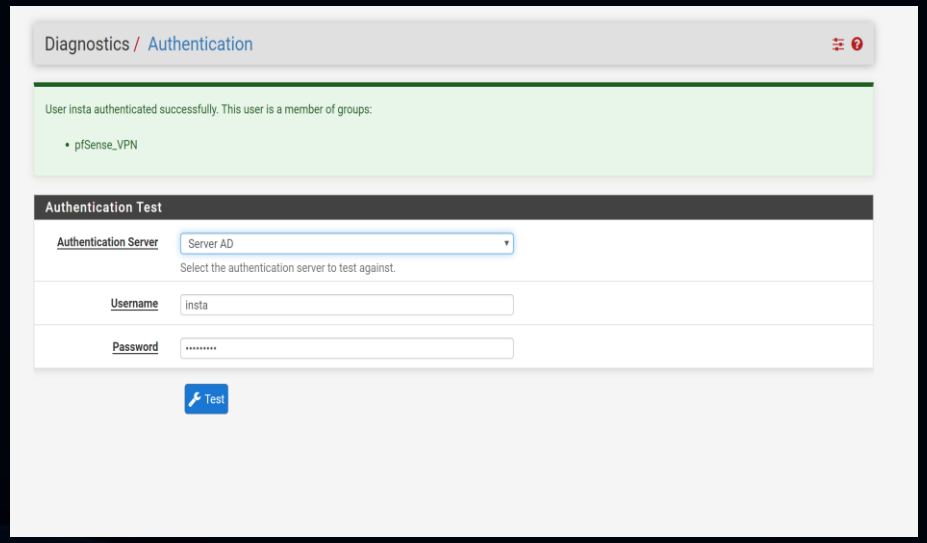


- DC=formation,DC=local : Base DN.
- OU=Users,OU=Insta,DC=formation,DC=local : l'emplacement des utilisateurs sur l'AD.
- memberOf=CN=pfSense_VPN,OU=Groups,OU=Insta,DC=formation,DC=local : l'emplacement du groupe pfSense_VPN sur l'AD.
- insta@formation.local : un utilisateur faisant parti du groupe pfSense_VPN.

pfSense OpenVPN

Tester la connexion LDAP



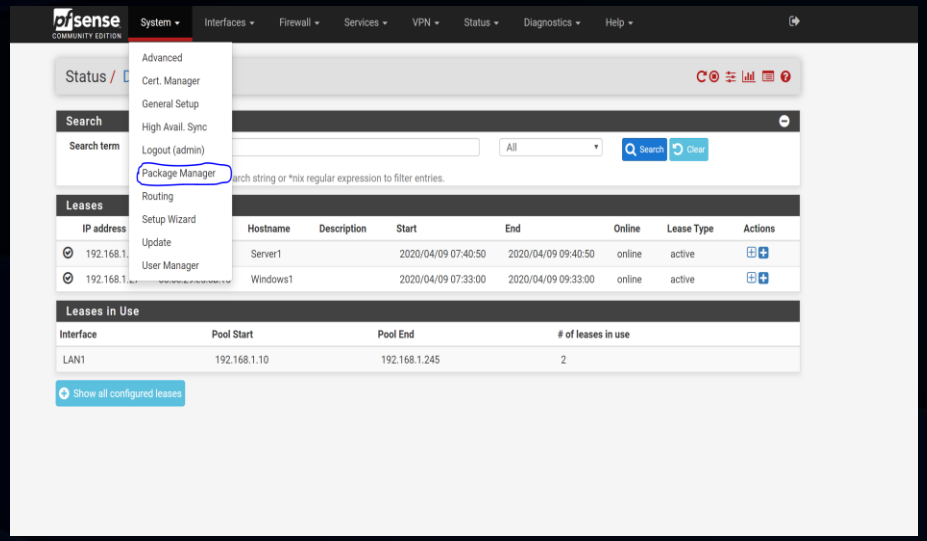


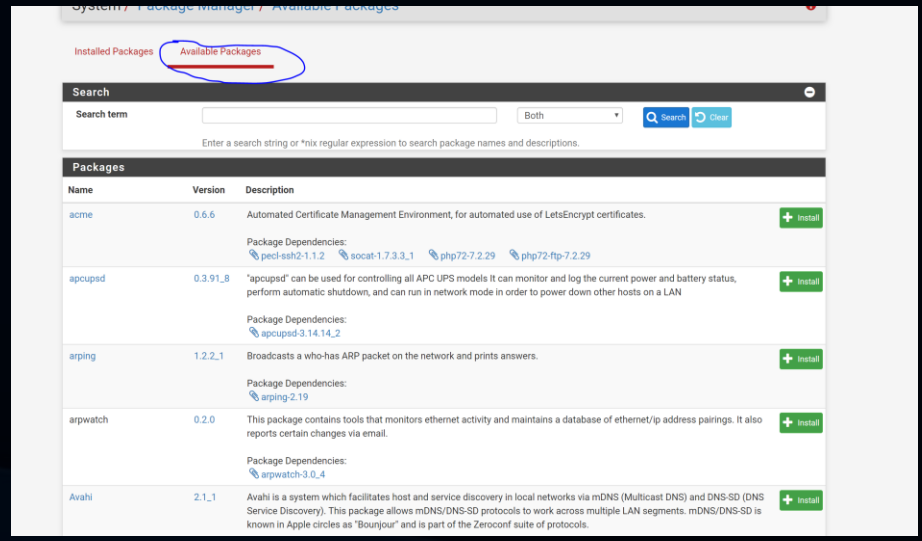
A faire :

- L'ajout d'un utilisateur dans l'AD (dans la même OU) → L'ajout de l'utilisateur dans le groupe pfSense_VPN.

pfSense OpenVPN

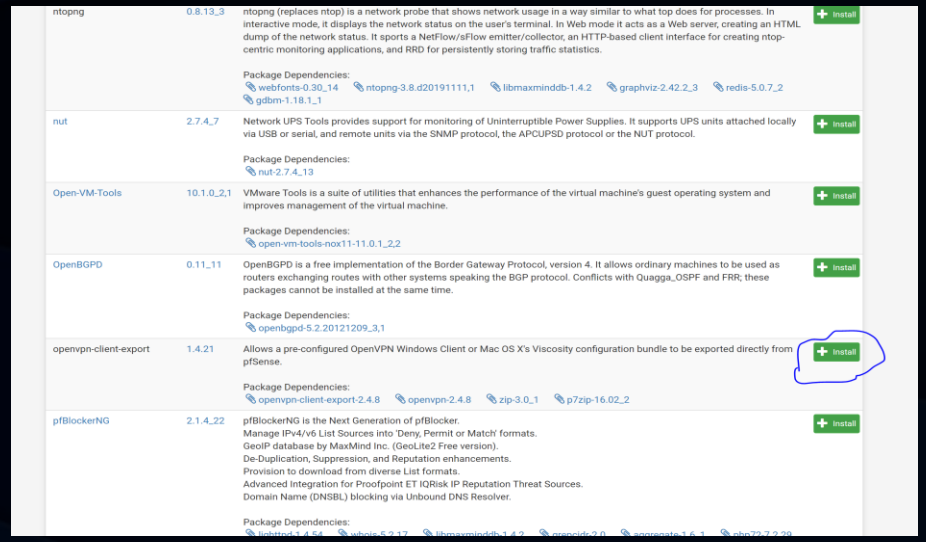
Installer le package OpenVPN

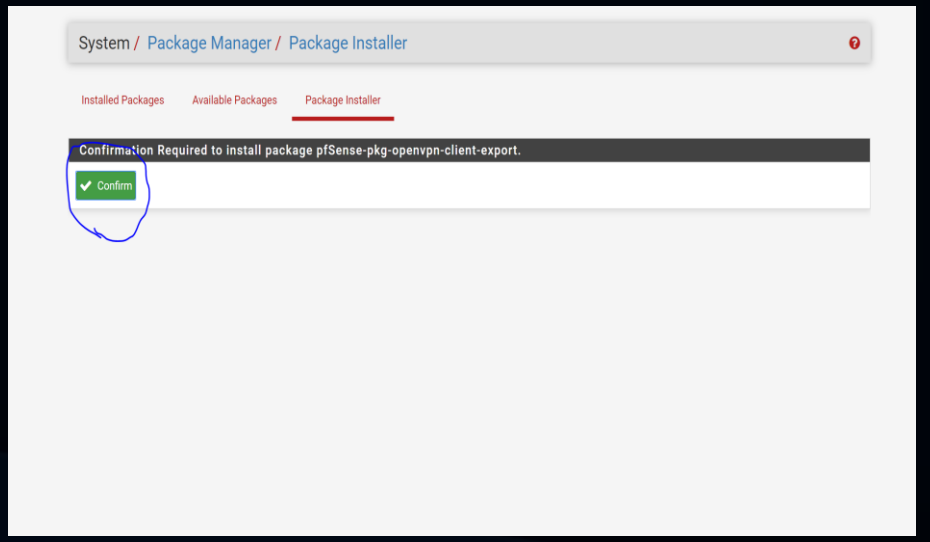




pfSense OpenVPN

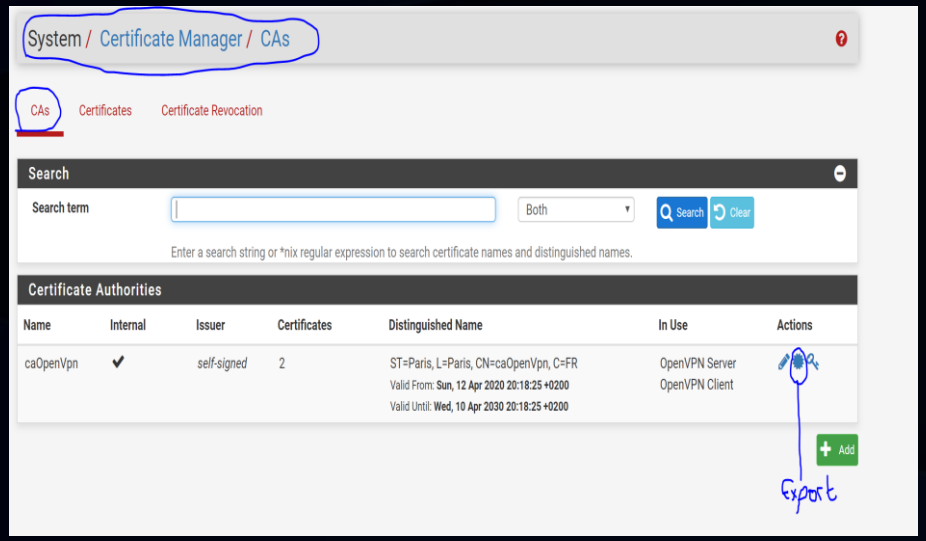
Installer le package OpenVPN



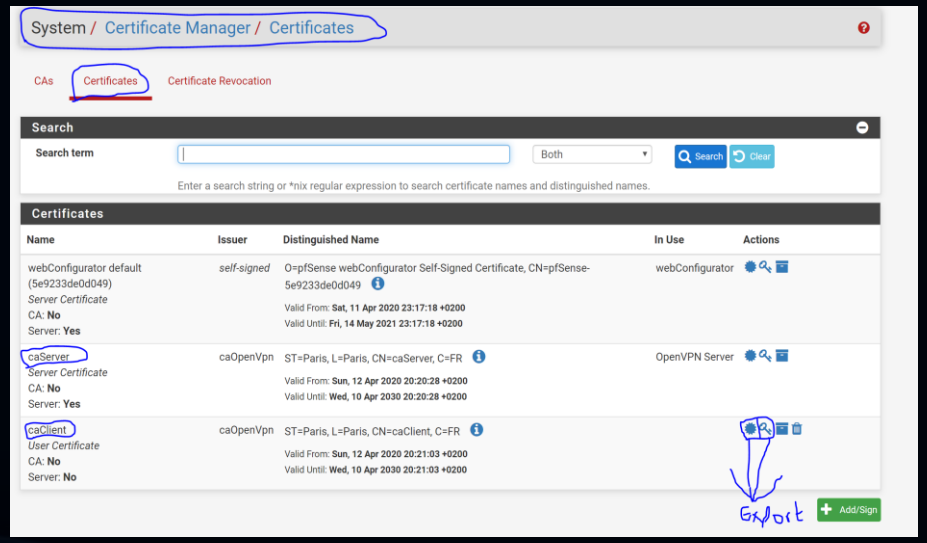


pfSense OpenVPN

Générer les certificats



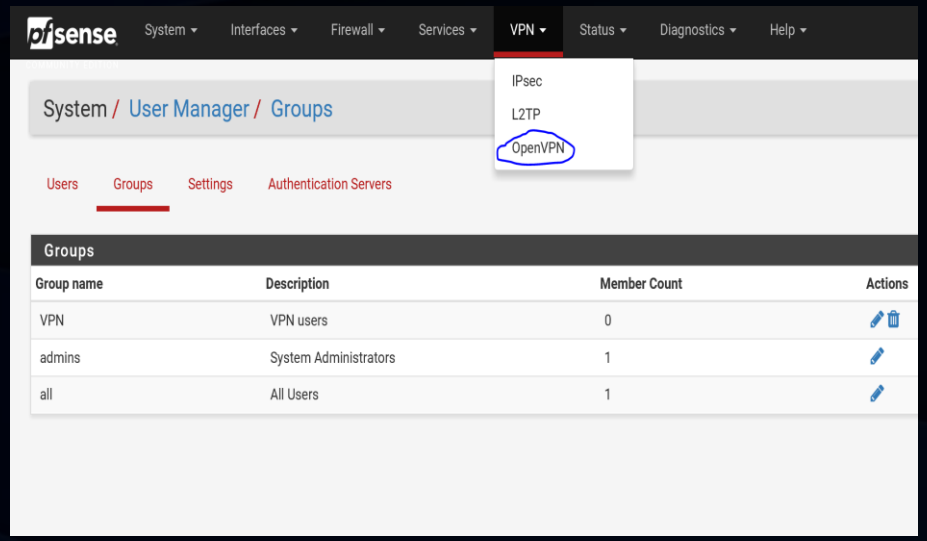
- Créer un certificat d'autorité et l'exporter par la suite.

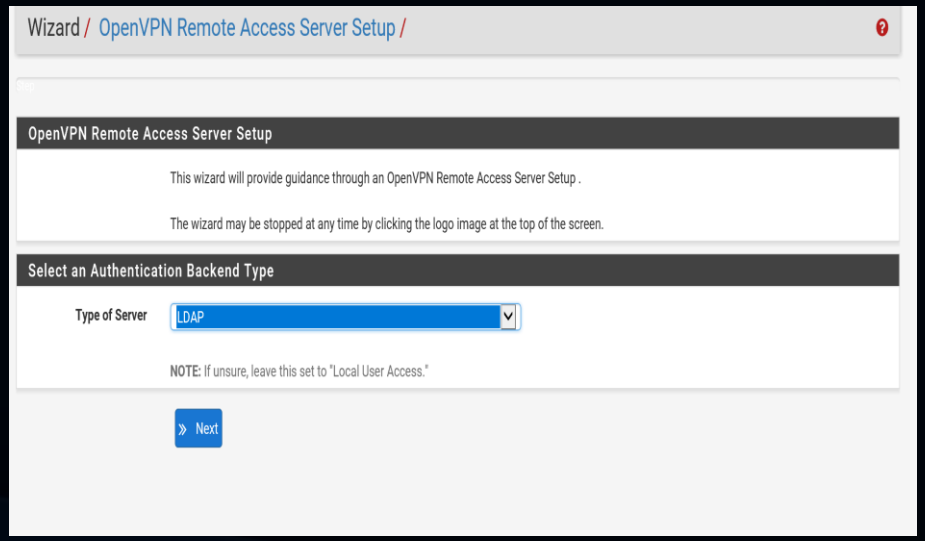


- Créer un certificat pour les clients et un autre pour le serveur OpenVPN.
- Exporter la clé publique et privée du client.

pfSense OpenVPN

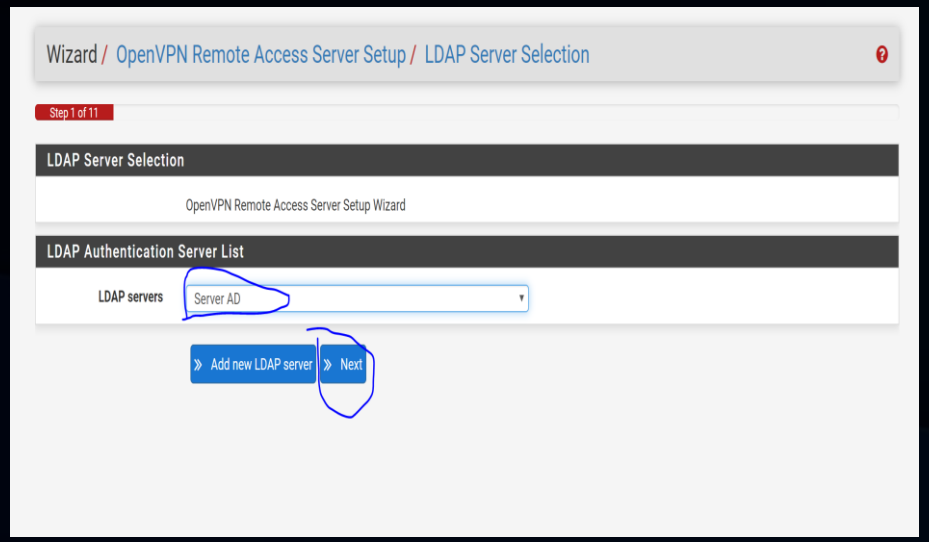
Créer un tunnel VPN

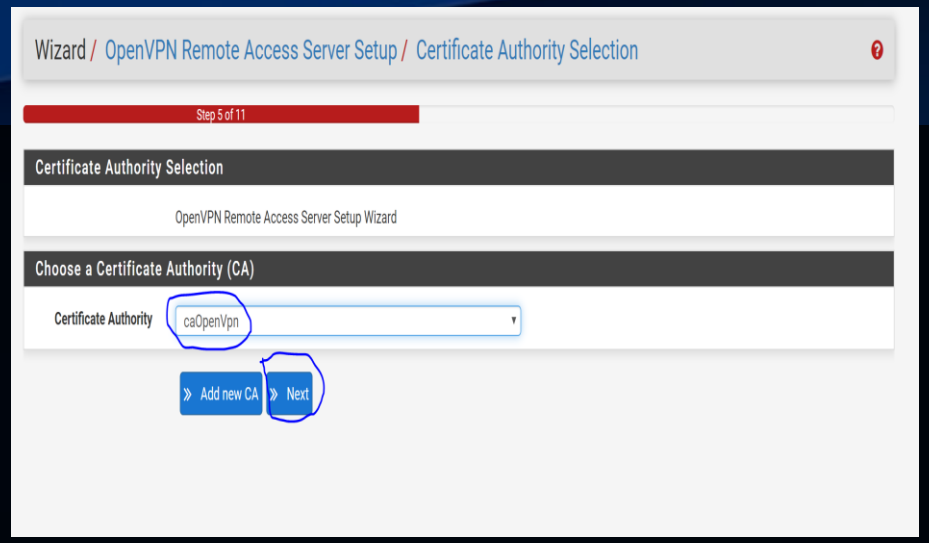


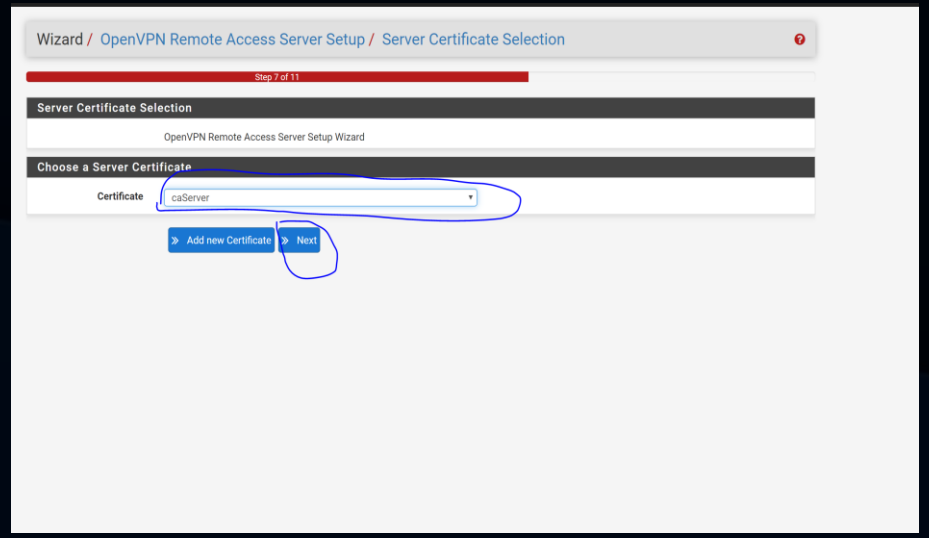


pfSense OpenVPN

Créer un tunnel VPN

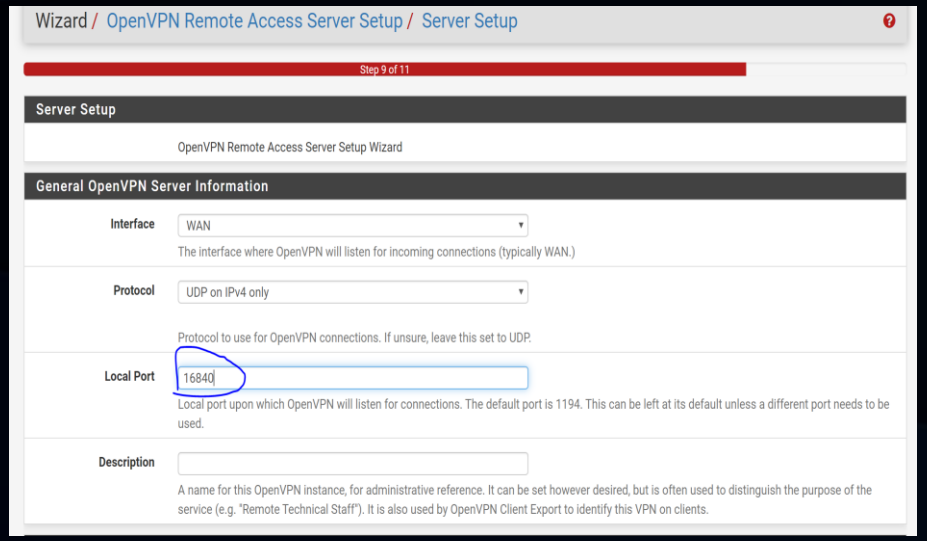


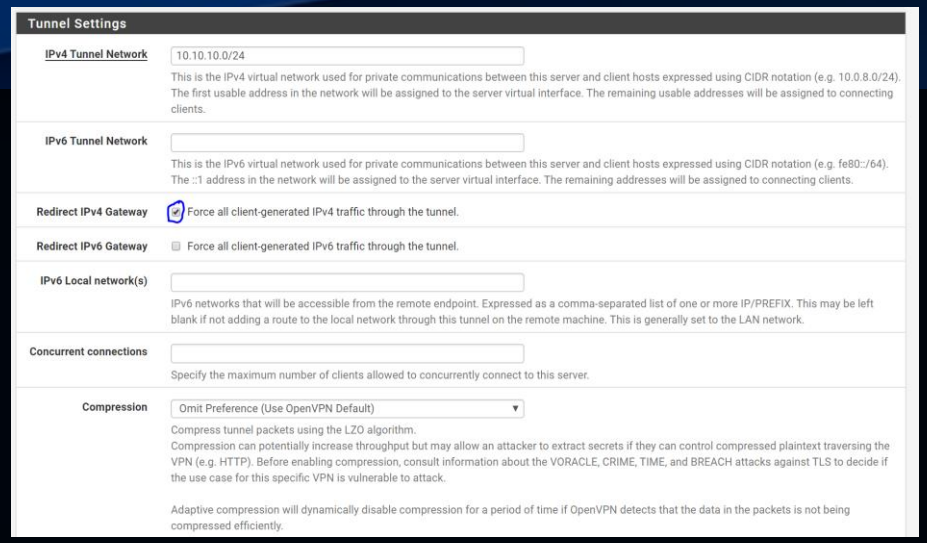


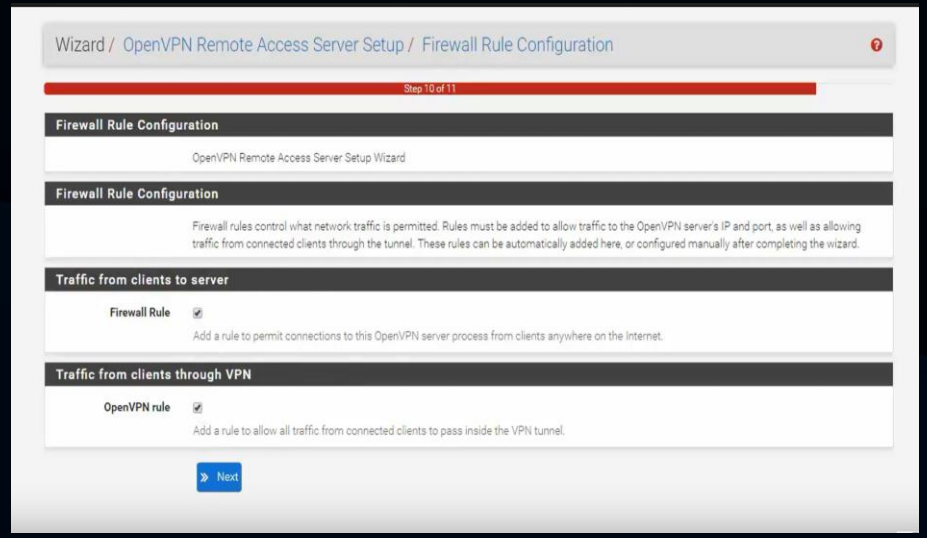


pfSense OpenVPN

Créer un tunnel VPN

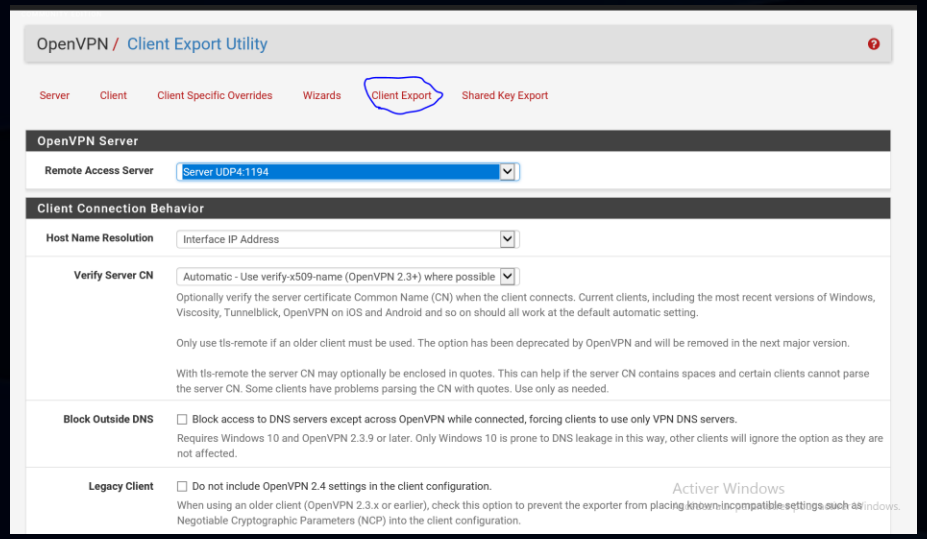


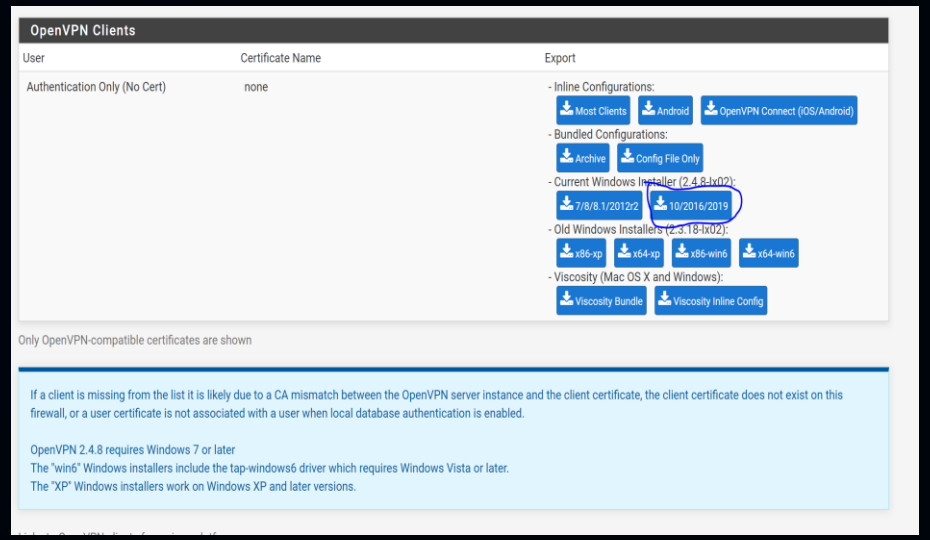




pfSense OpenVPN

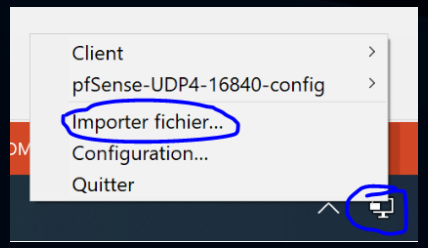
OpenVPN client

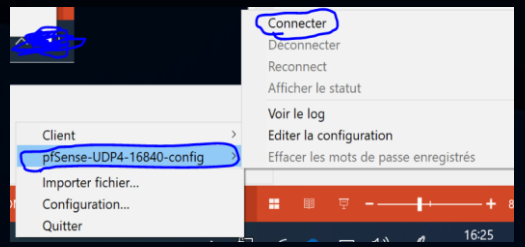




A faire :

- Télécharger le setup OpenVPN client selon son OS.
- L'installer sur la machine cliente.
- Créer un fichier de configuration client.ovpn et l'importer à partir de la console OpenVPN Client.
- Enfin se connecter au VPN ☺ .



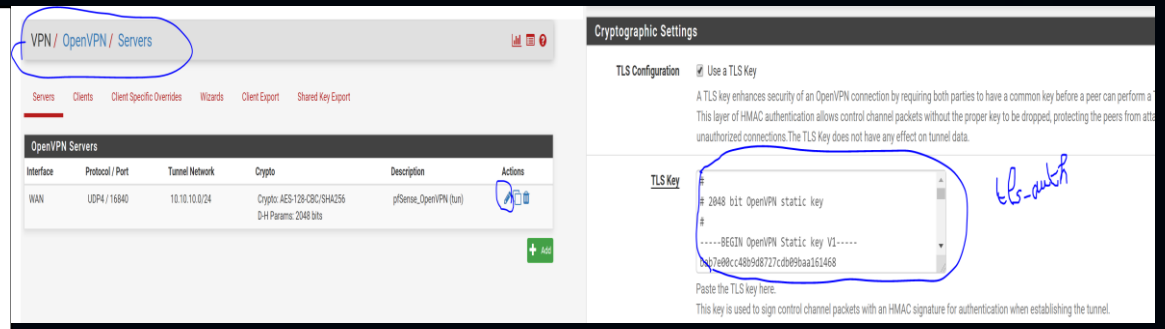


pfSense OpenVPN

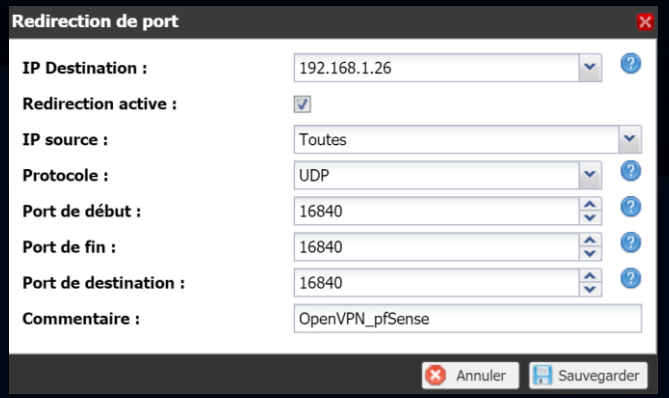
Fichier de configuration client.ovpn

```
dev tun
persist-tun
persist-key
cipher AES-128-CBC
ncp-ciphers AES-128-GCM
auth SHA256
tls-client
client
resolv-retry infinite
remote 91.X.X.X16840 udp4
auth-user-pass
key-direction 1
```

```
La suite…..
<tls-auth>
A récupérer au niveau de la configuration du serveur OpenVPN →
</tls-auth>
<ca>
Contenu du fichier certificat d'autorité .ca
</ca>
<cert>
Contenu du fichier Client.ca
</cert>
<key>
Contenu du fichier Client.key
</key>
remote-cert-tls server
```



- @IP de la box : 91.X.X.X
- Port ouvert : 16840
- Redirection vers @IP WAN pfSense :192.168.1.26

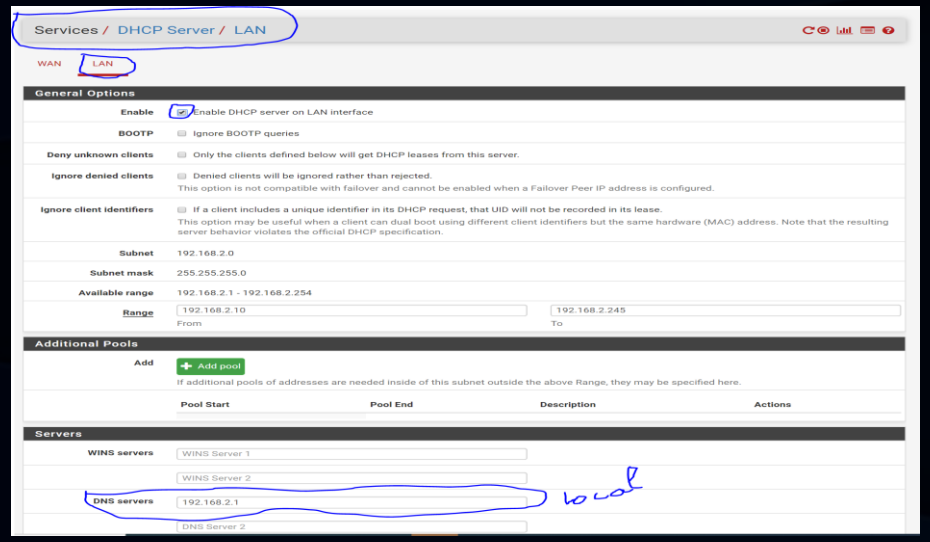


Portail Captif + LDAP

pfSense Portail Captif + LDAP

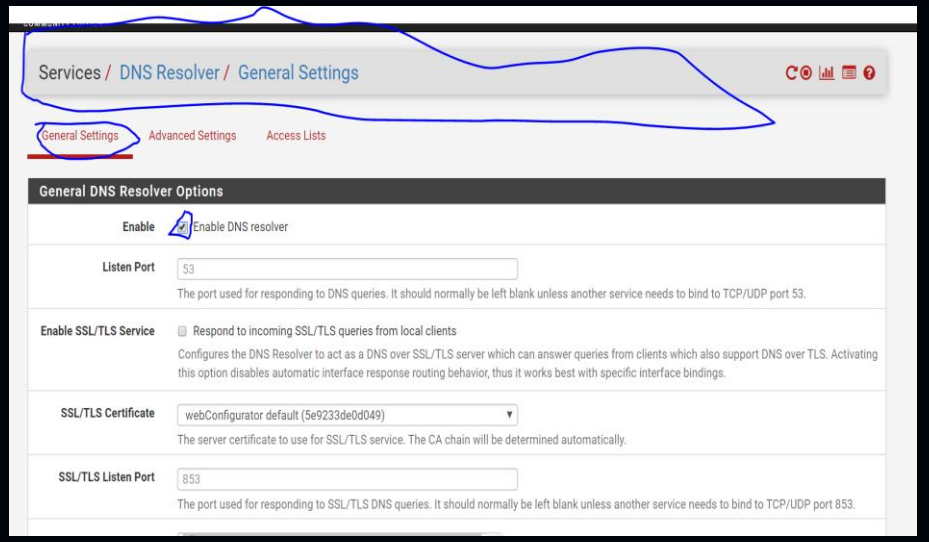
Un portail captif est une technique consistant à forcer les clients HTTP d'un réseau de consultation à afficher une page web spéciale avant d'accéder à Internet normalement.

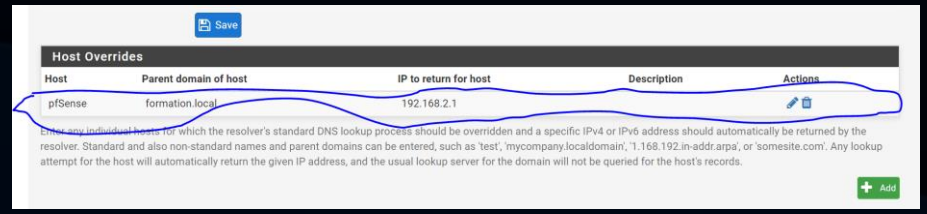
1-Vérifier que le DHCP est activé



L'adresse IP du serveur DNS = @IP LAN pfSense

2-Vérifier que le DNS Resolver est activé

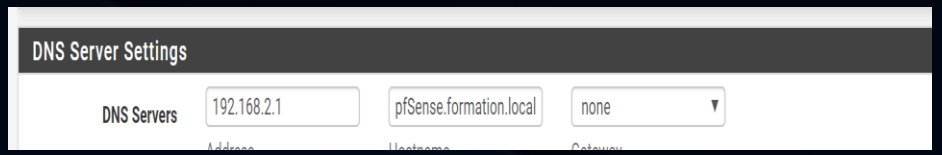




Créer une nouvelle ligne dans Host Overrides en remplissant les informations LAN du pfSense.

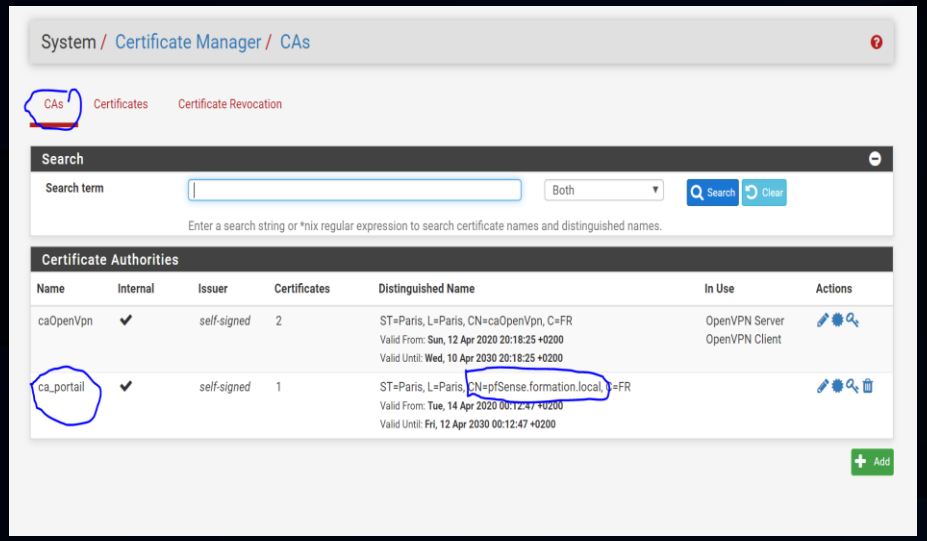
3-Informations DNS

Attention : Vérifier dans General Setup les informations du serveur

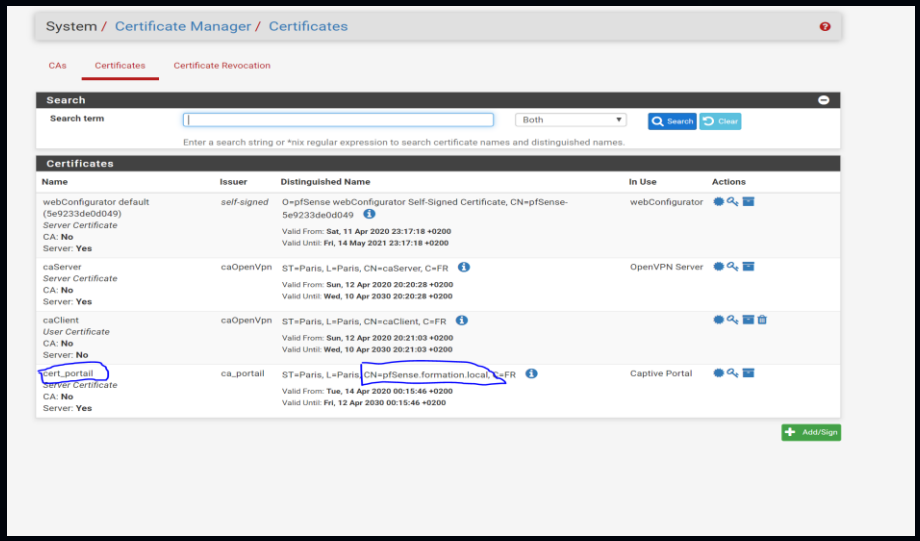


pfSense Portail Captif + LDAP

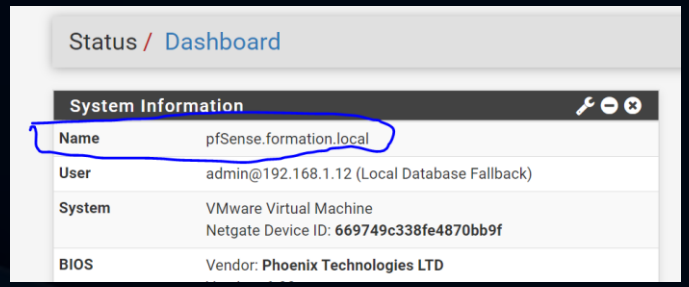
4-Création de certificats



- Certificat d'autorité.
- Common Name = pfSense.formation.local

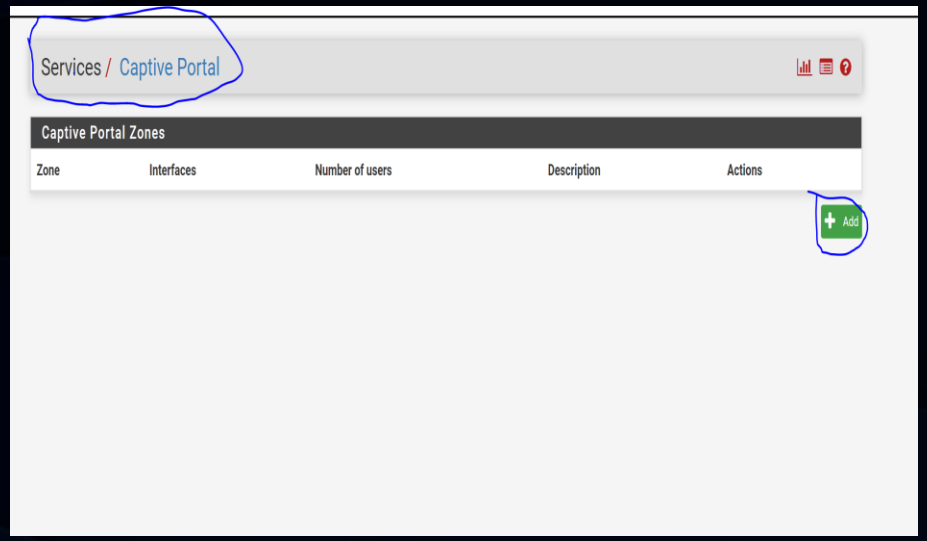


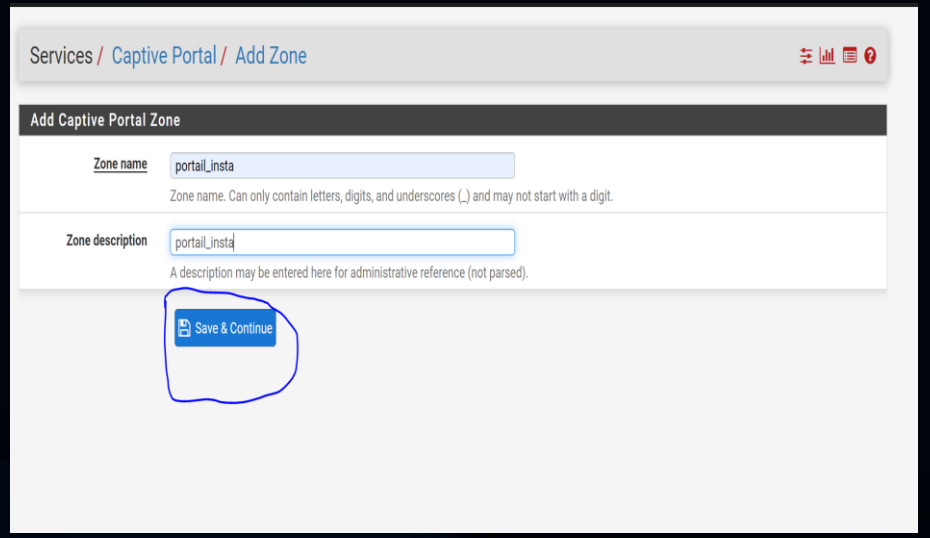
- Type certificat : User certificat.
- Common Name = pfSense.formation.local



pfSense Portail Captif + LDAP

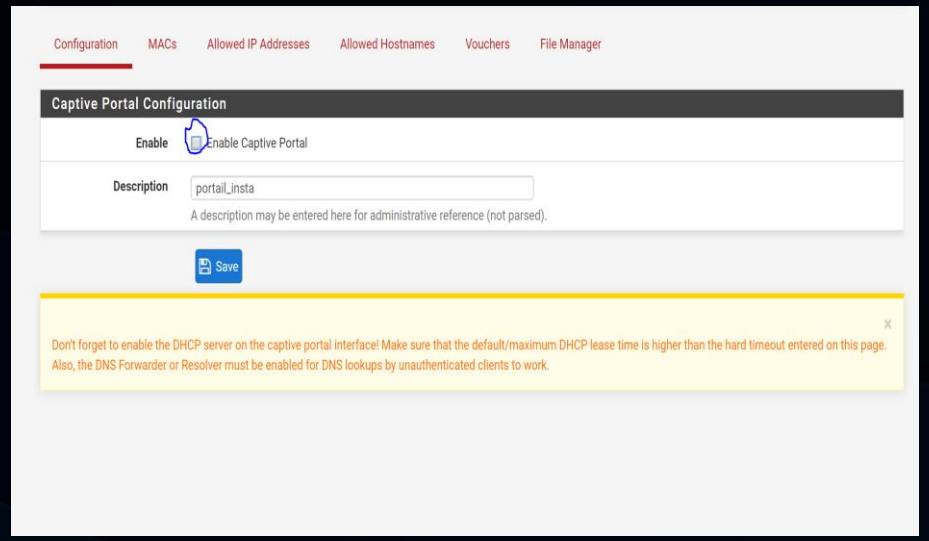
5-Création du portail captif

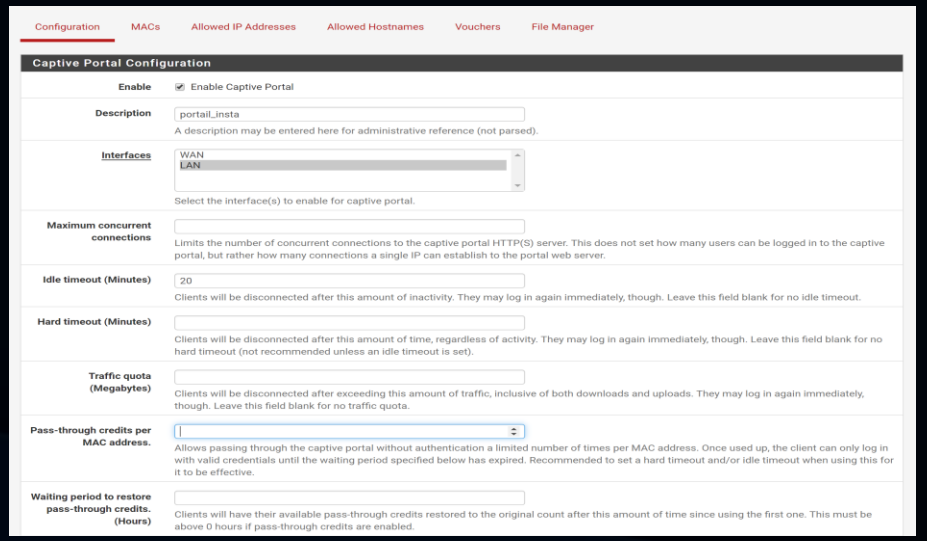




pfSense Portail Captif + LDAP

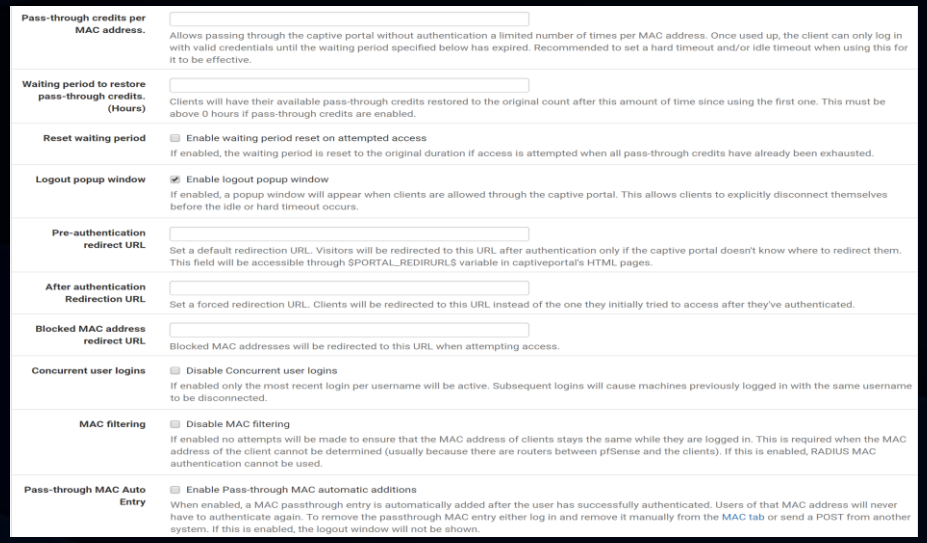
5-Création du portail captif

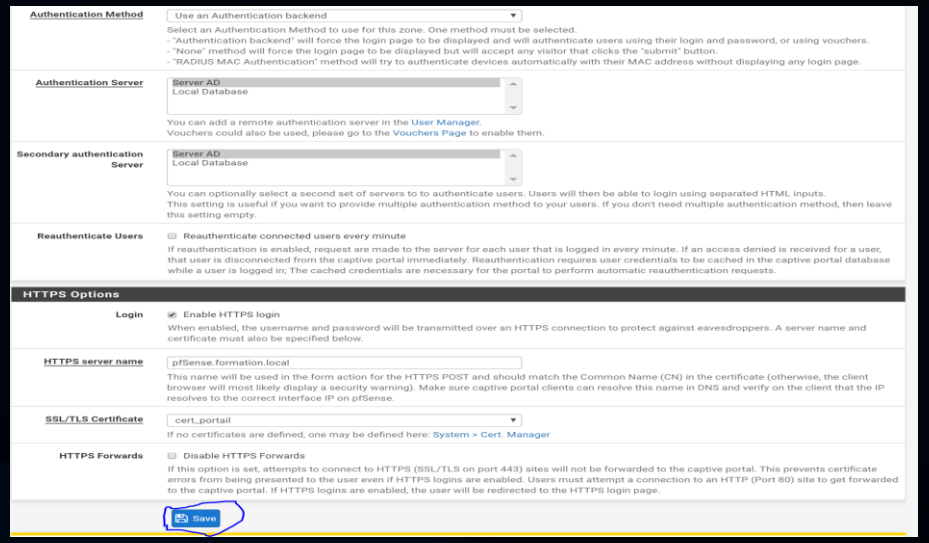




pfSense Portail Captif + LDAP

5-Création du portail captif

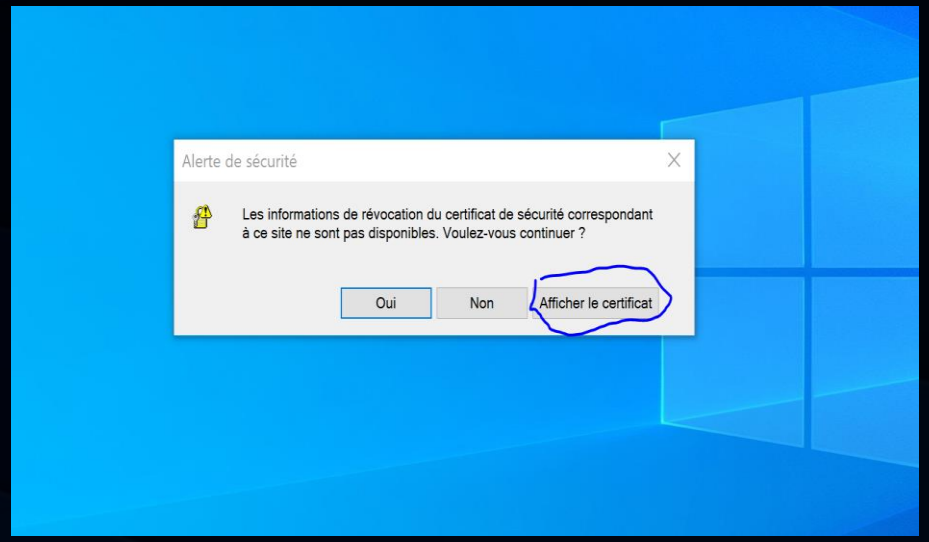


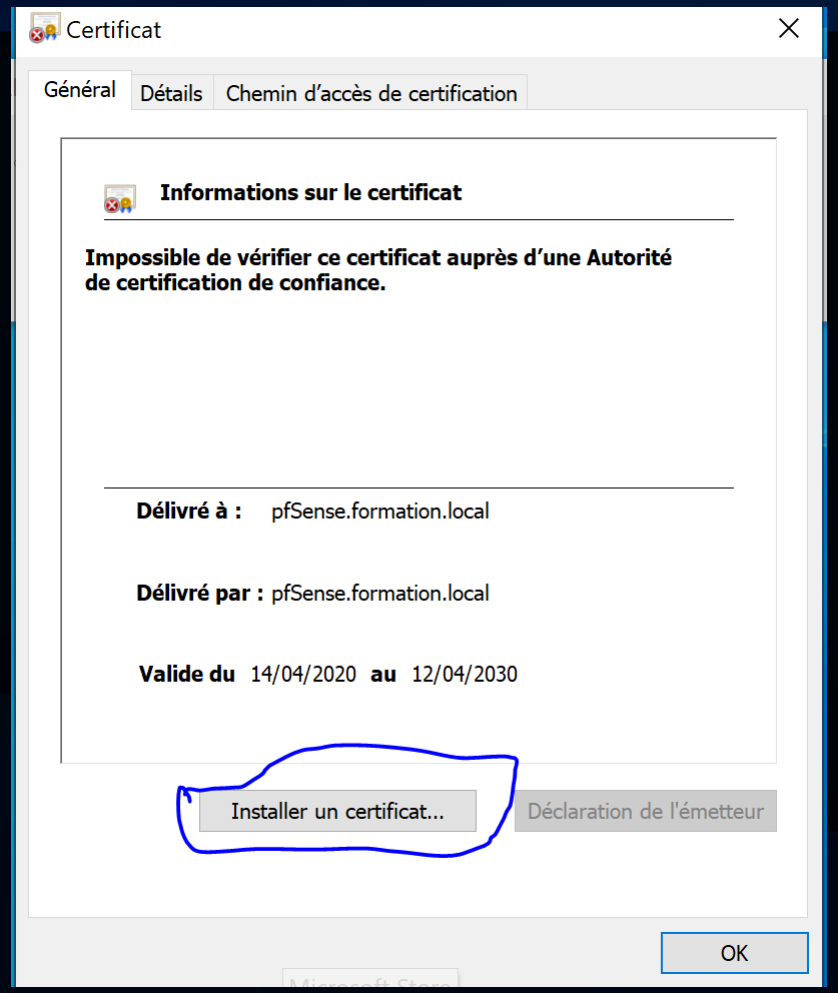


pfSense Portail Captif + LDAP

6-Installation du certificat coté client

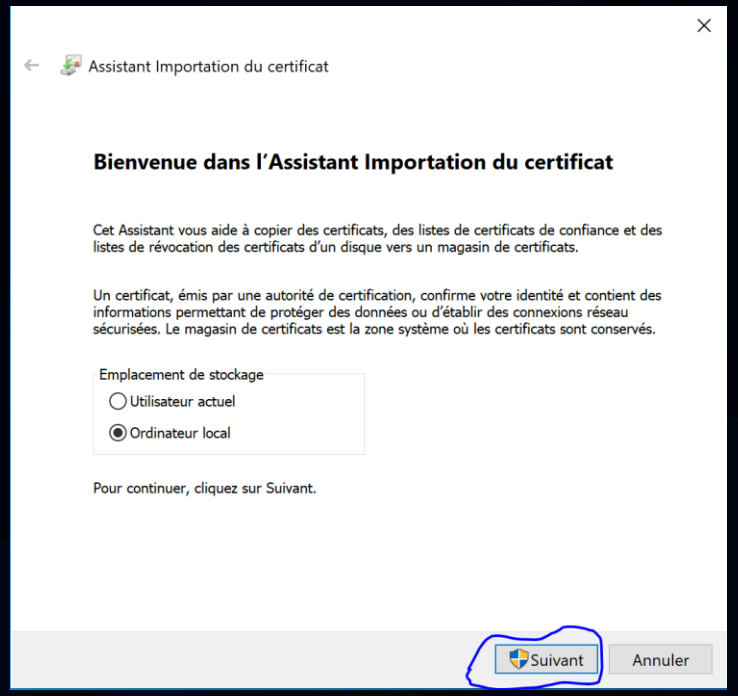
Cette étape nécessite le redémarrage du poste client après l'installation du service portail captif.

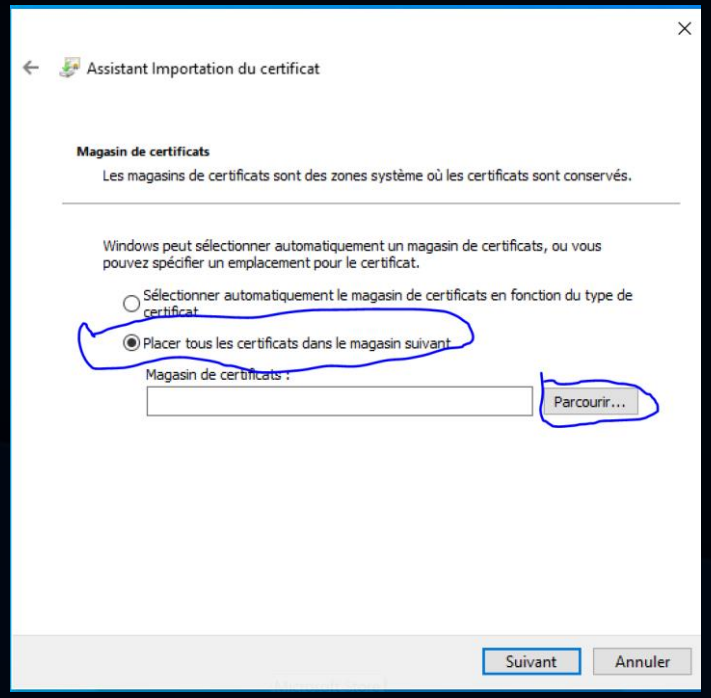


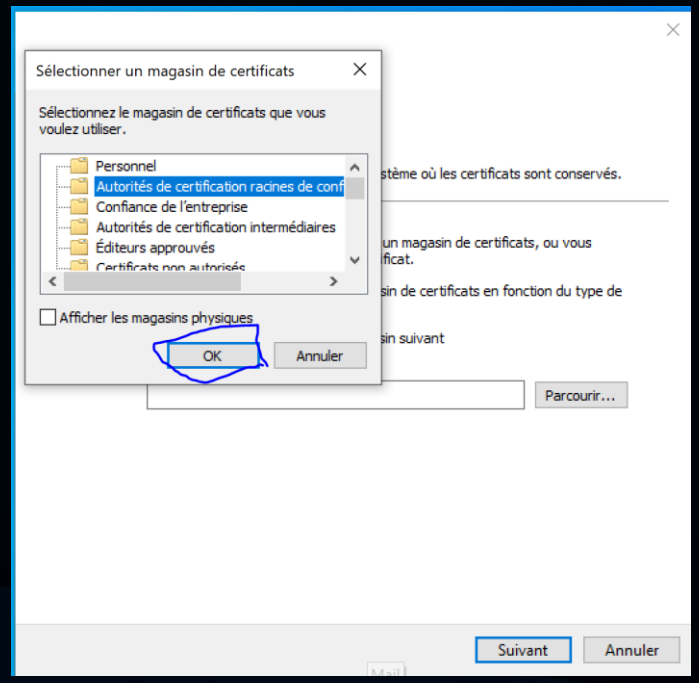


pfSense Portail Captif + LDAP

6-Installation du certificat coté client

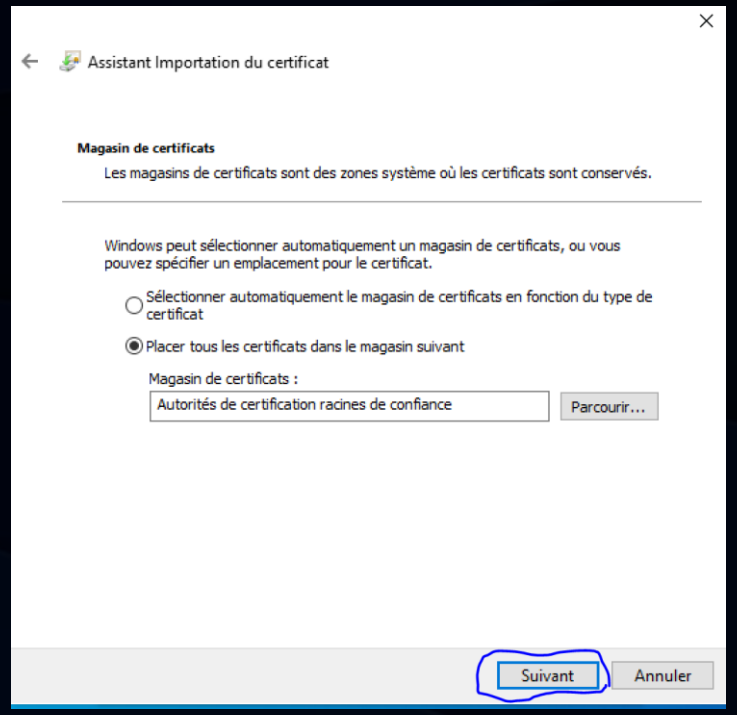


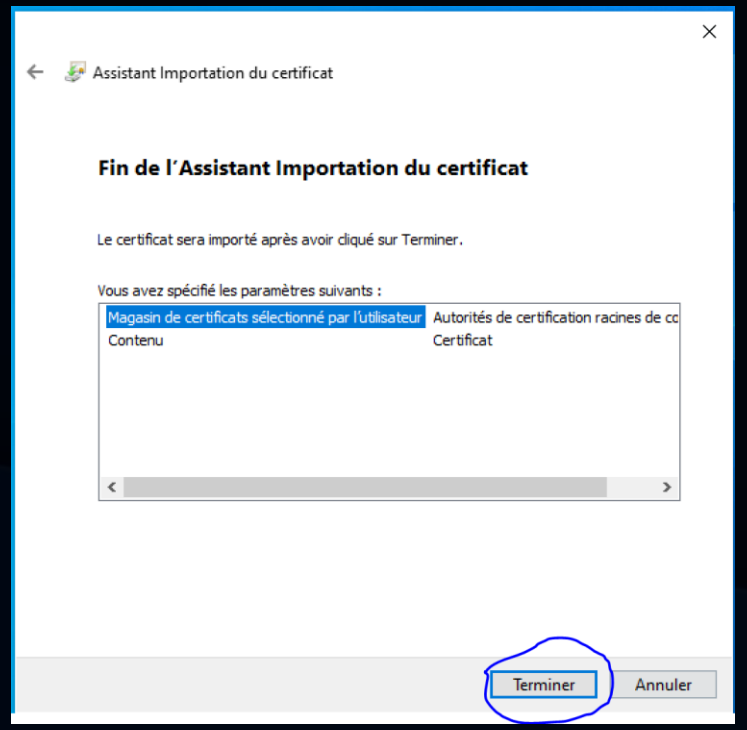


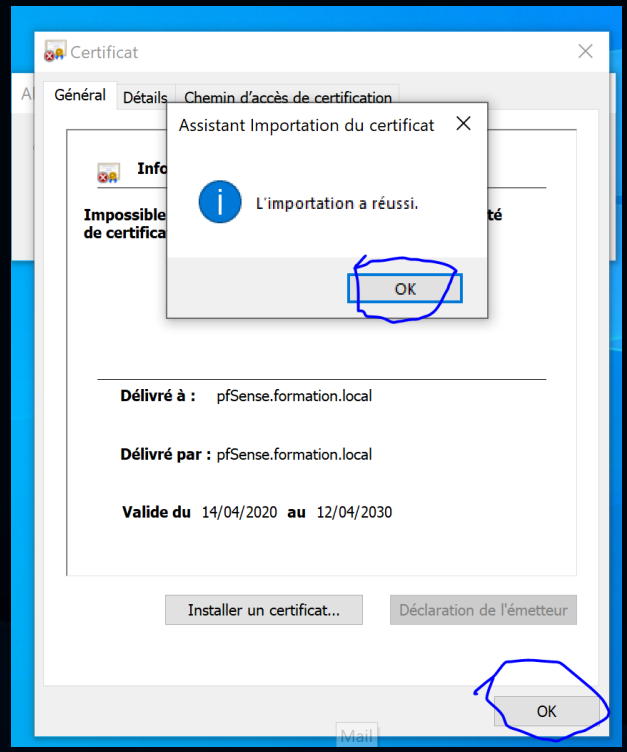


pfSense Portail Captif + LDAP

6-Installation du certificat coté client

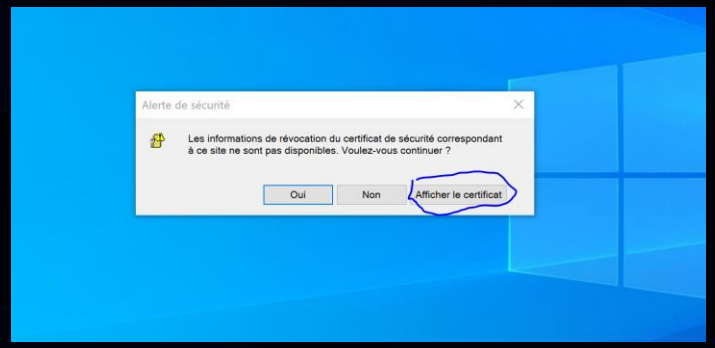


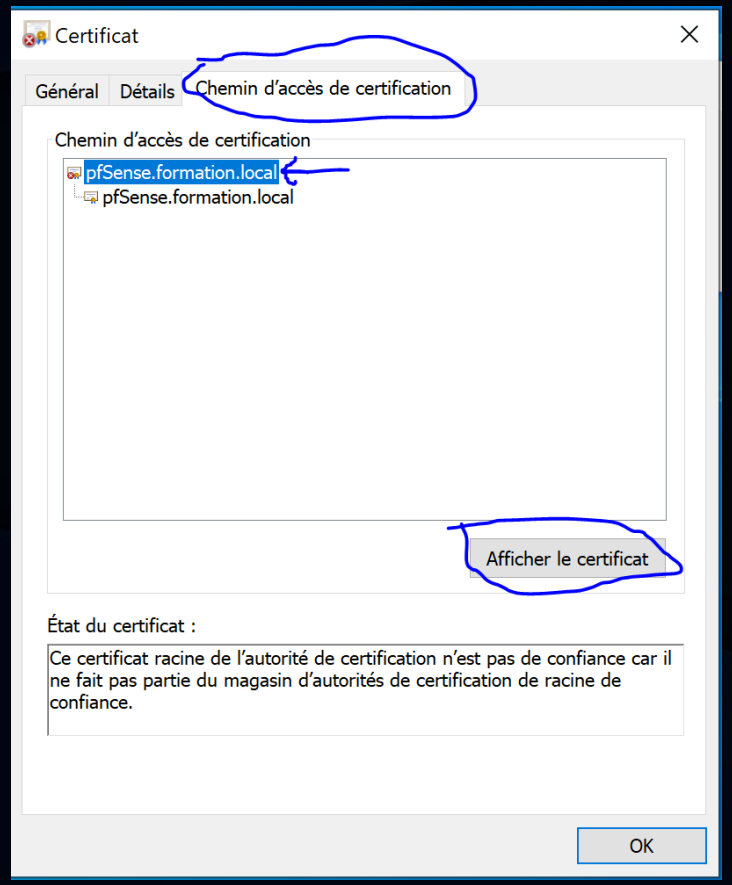


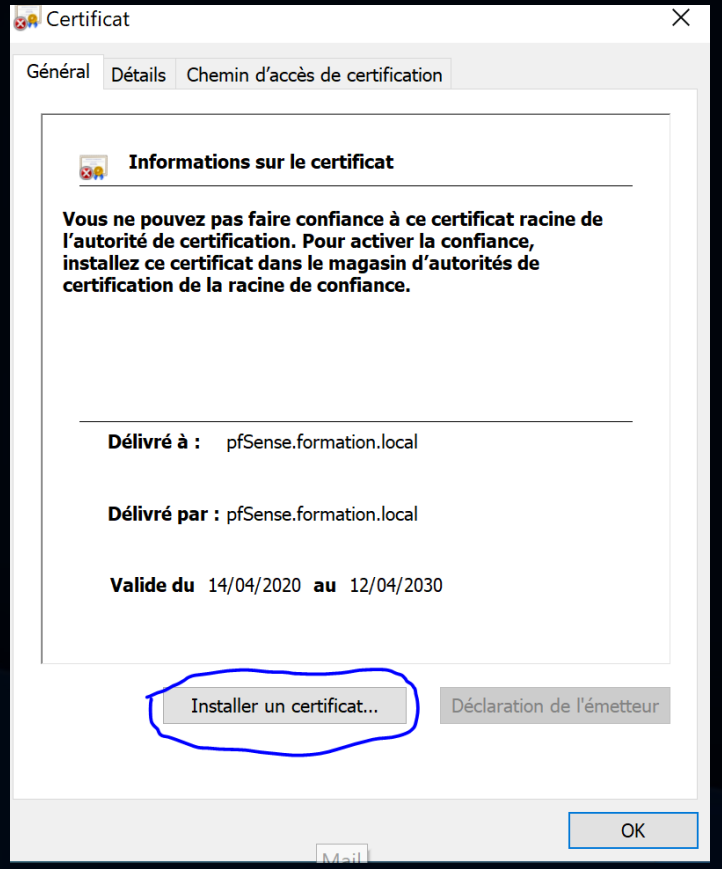


pfSense Portail Captif + LDAP

6-Installation du certificat coté client

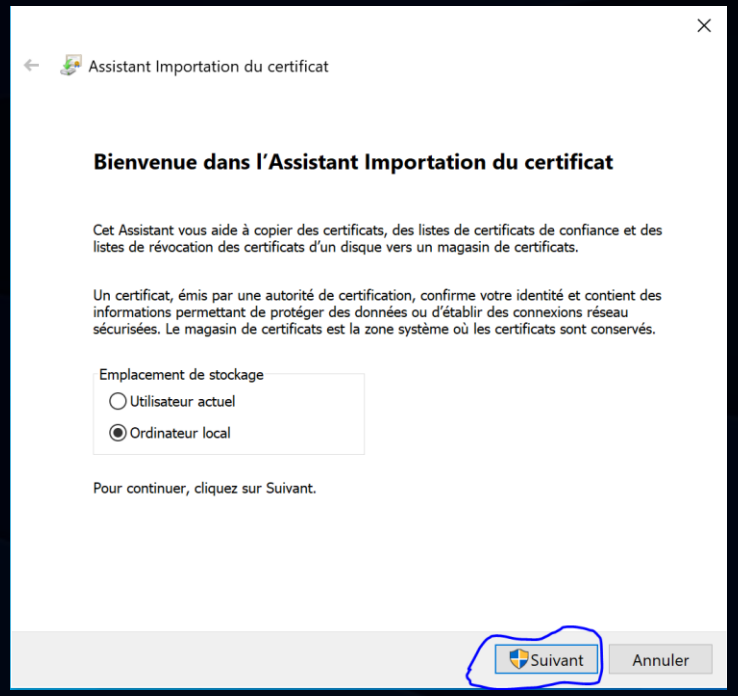


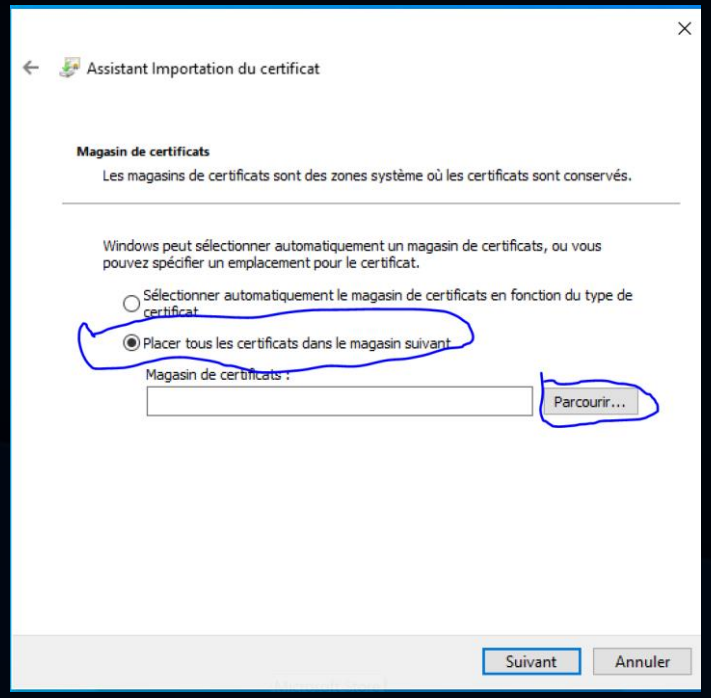


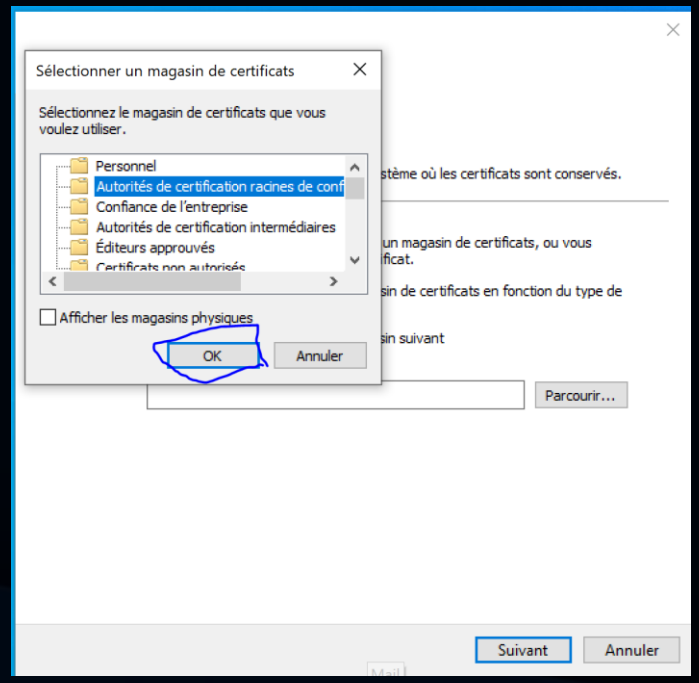


pfSense Portail Captif + LDAP

6-Installation du certificat coté client

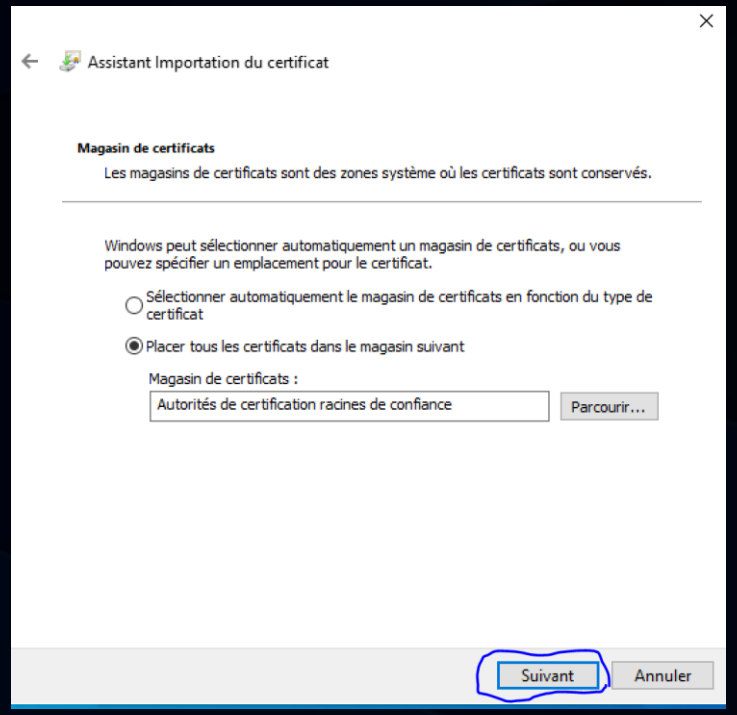


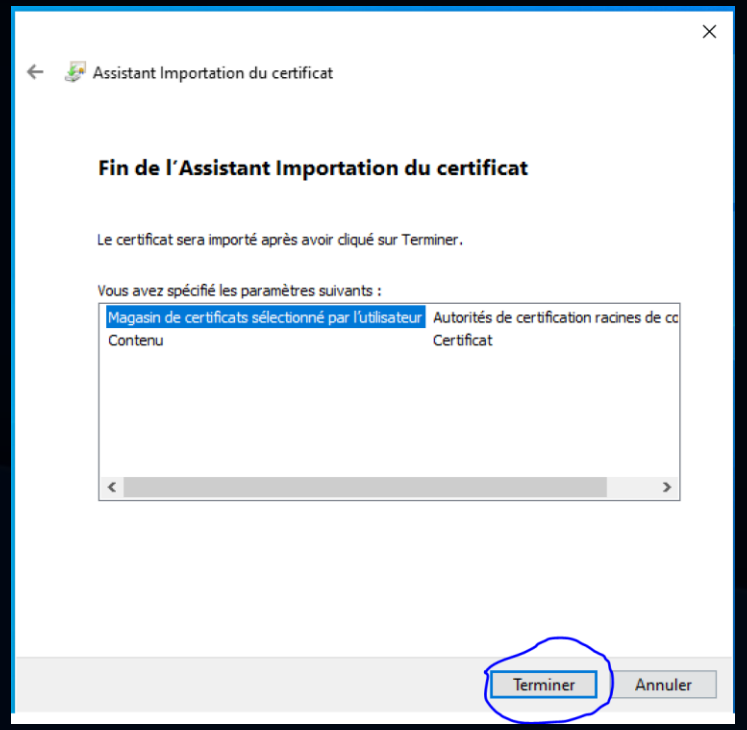


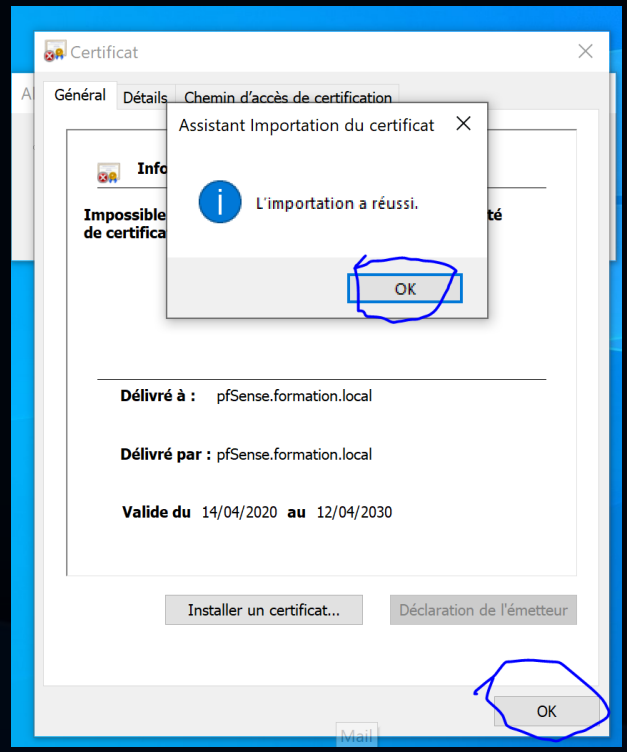


pfSense Portail Captif + LDAP

6-Installation du certificat coté client



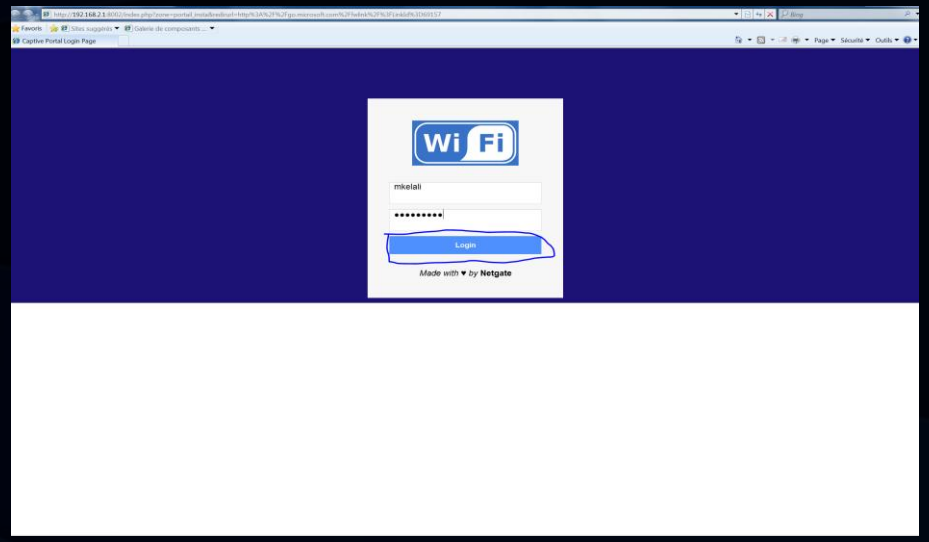


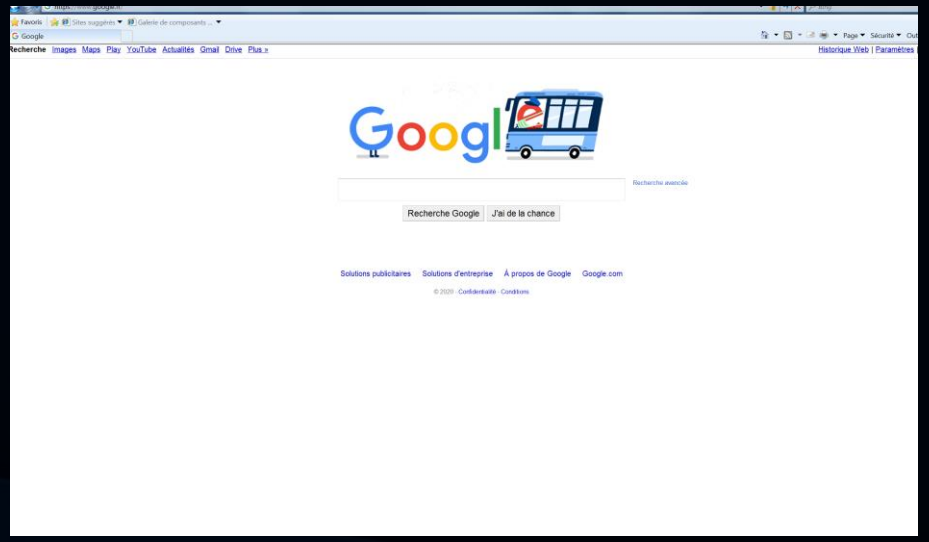


pfSense Portail Captif + LDAP

7-Tester via un navigateur Web

Le login et le mot de passe ceux du compte AD.





Suivre les étapes du tutoriel suivant : https://www.youtube.com/watch?v=_e1eWvA3FFg