



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.

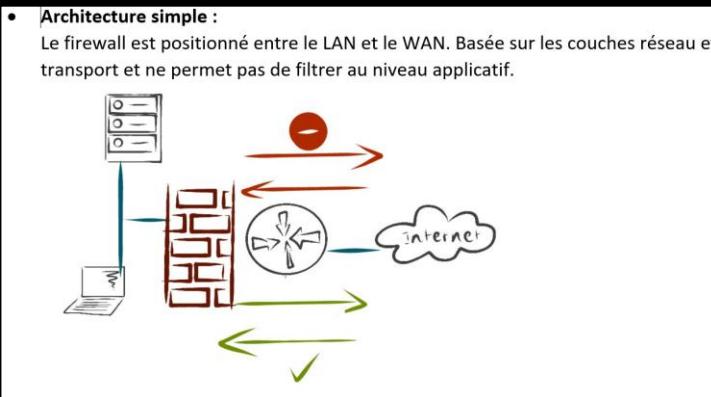
La réalisation de ce document nécessite un baguage technique en réseau (protocoles réseaux, configuration commutateur et routeur...) ainsi qu'en système (OS, Rôles et fonctionnalités, Machines virtuelles...). ☺

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.



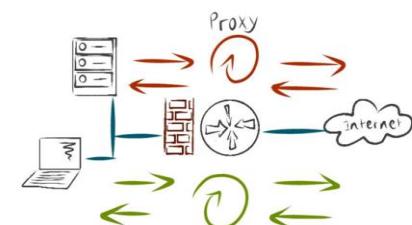
4

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.

Architectures Firewall

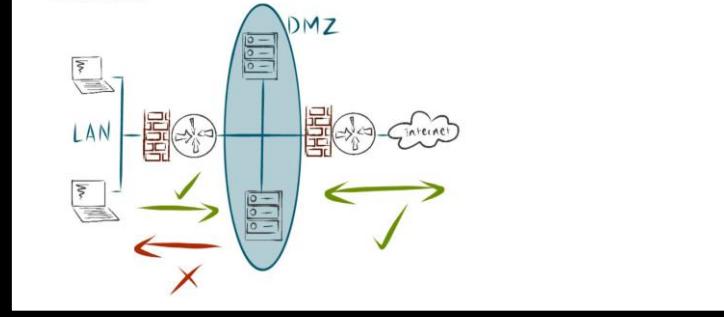
- **Architecture proxy :**
La même architecture que l'architecture simple mais on ajoute un filtre, au niveau de la couche applicative. Ceci va permettre d'empêcher l'utilisation du peer-to-peer.



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.

- **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, autrefois nommé OpenBSD packet filter.

Pourquoi pfSense ?

- Open Source.
- Stable.
- Multifonctions.

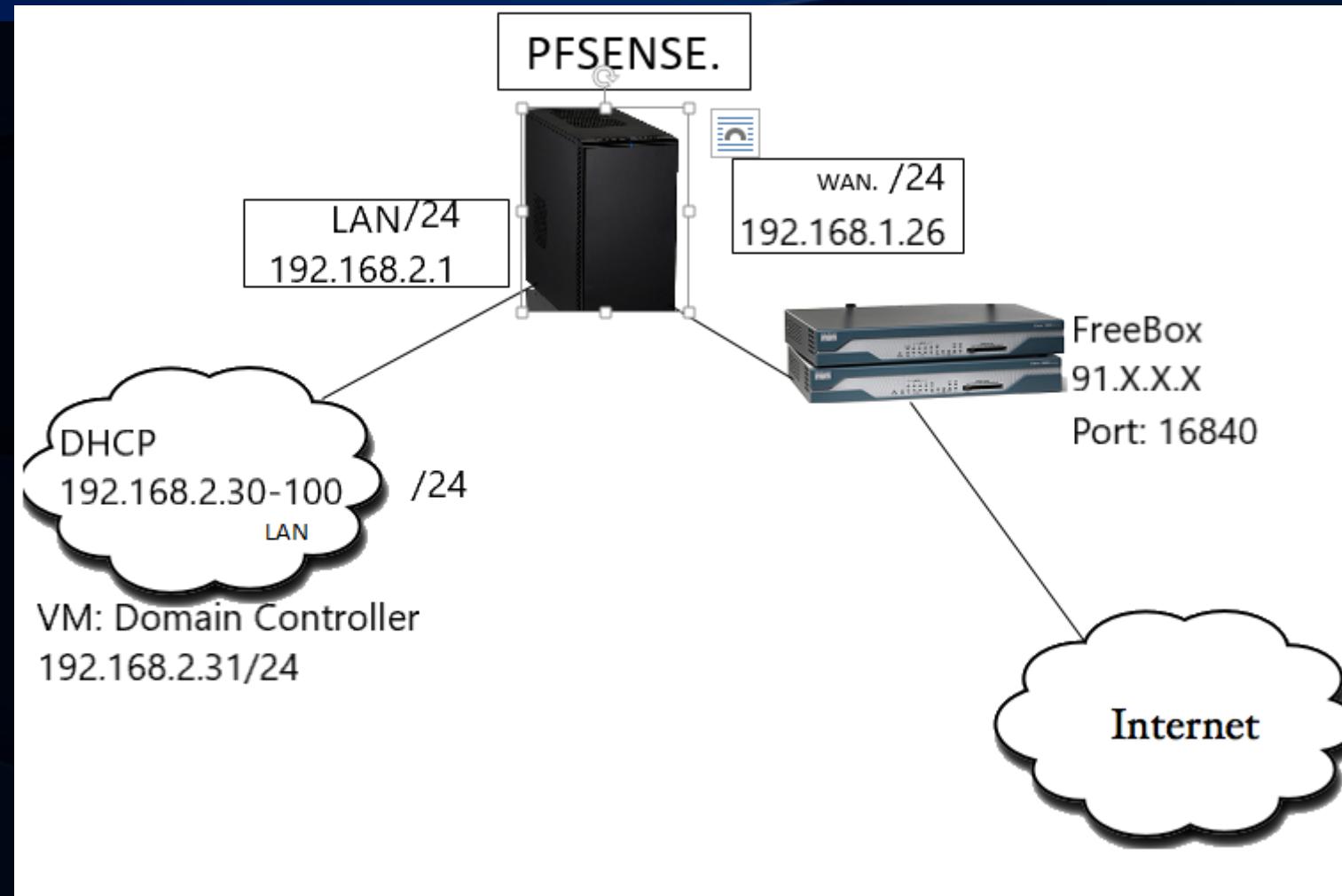
Scénarios de déploiement

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

Mode d'administration

- Console.
- WebGUI.

Schématiquement

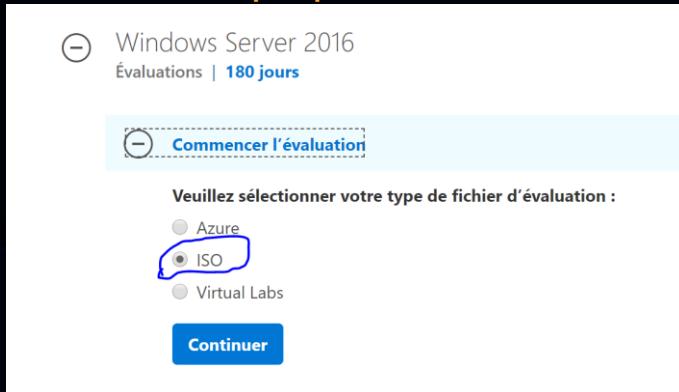


Domain Controller

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/aller-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

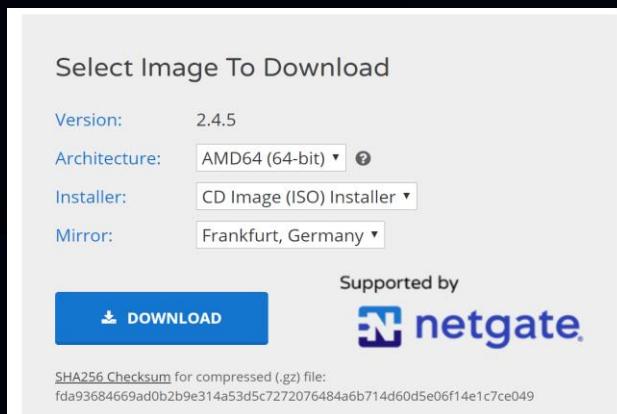
4. Désactiver le pare-feu



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

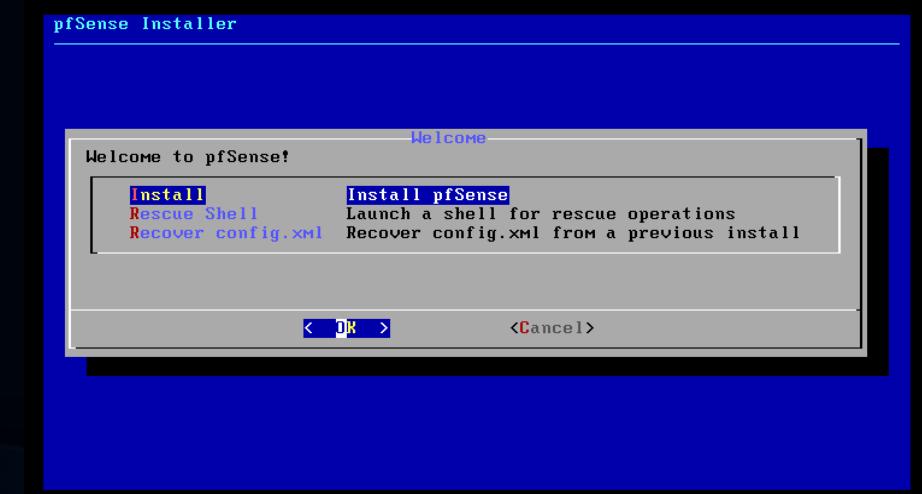
- Procéder à la création d'une VM pfSense_Server sous VMware.
- Caractéristiques de la VM :

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.

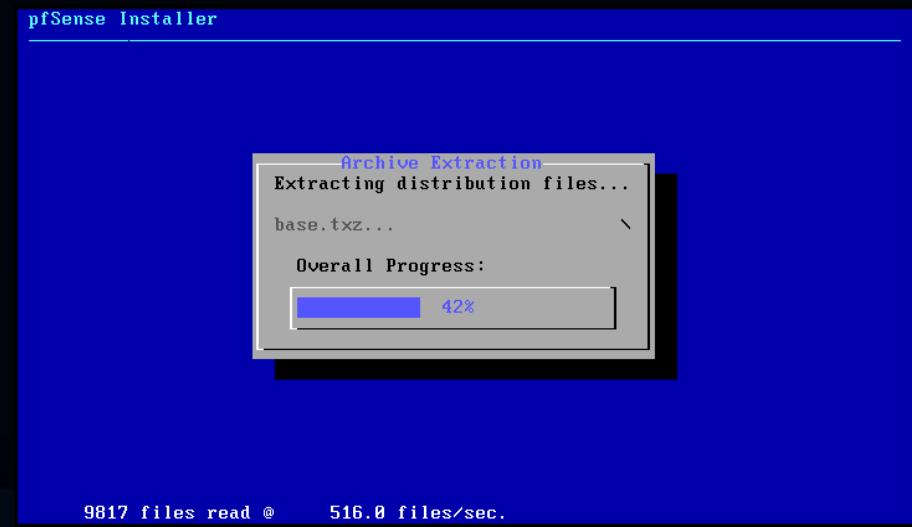
Installation pfSense



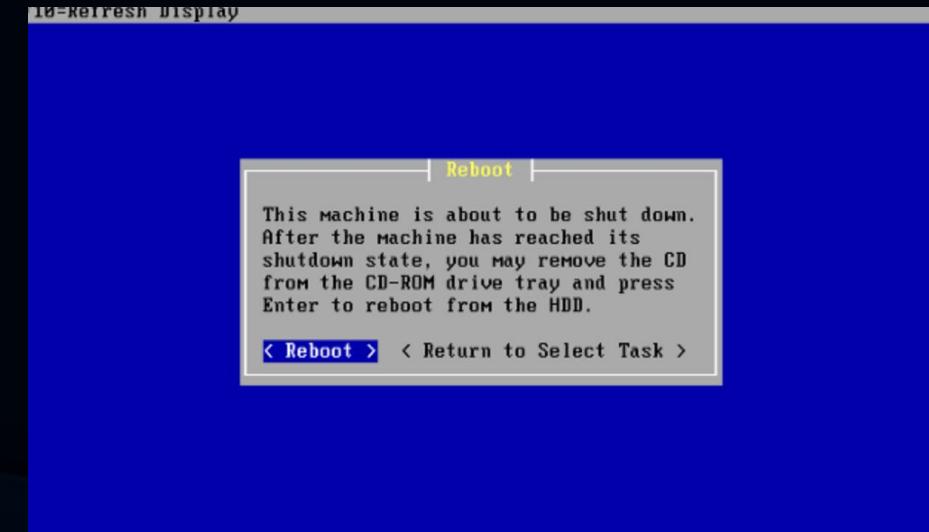
Installation pfSense



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

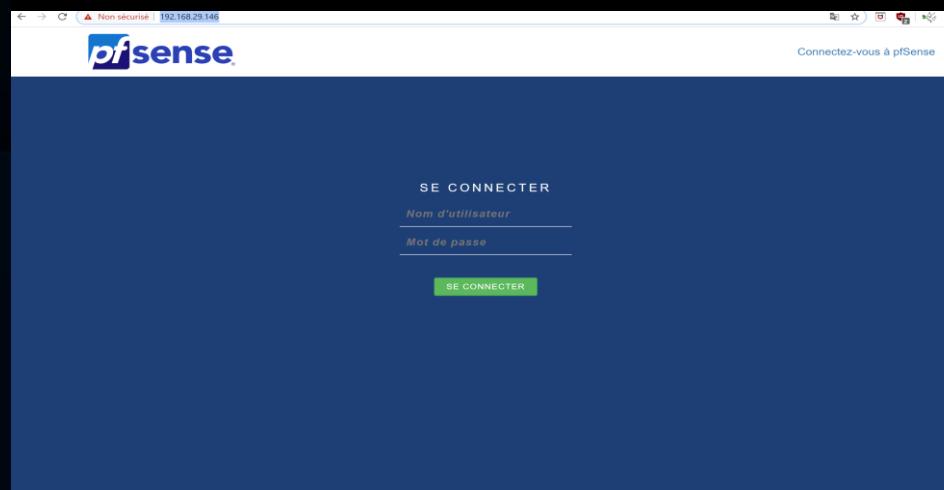
- Pour les configurations qui suivent, à consulter les étapes ci-dessous (captures d'écran).

```
2) Set interface(s) IP address           11) Restart webConfigurator
3) Reset webConfigurator password       12) PHP shell + pfSense tools
4) Reset to factory defaults           13) Update from console
5) Reboot system                      14) Enable Secure Shell (sshd)
6) Halt system                         15) Restore recent configuration
7) Ping host                           16) Restart PHP-FPM
8) Shell

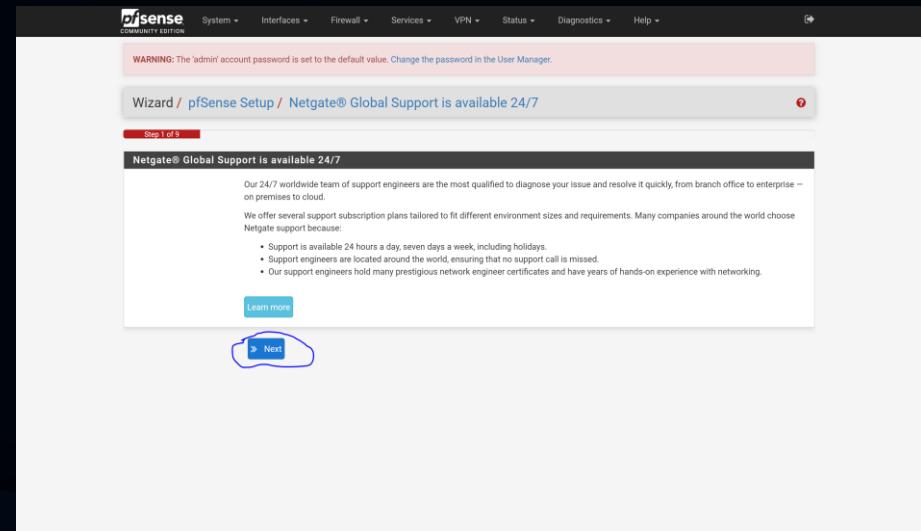
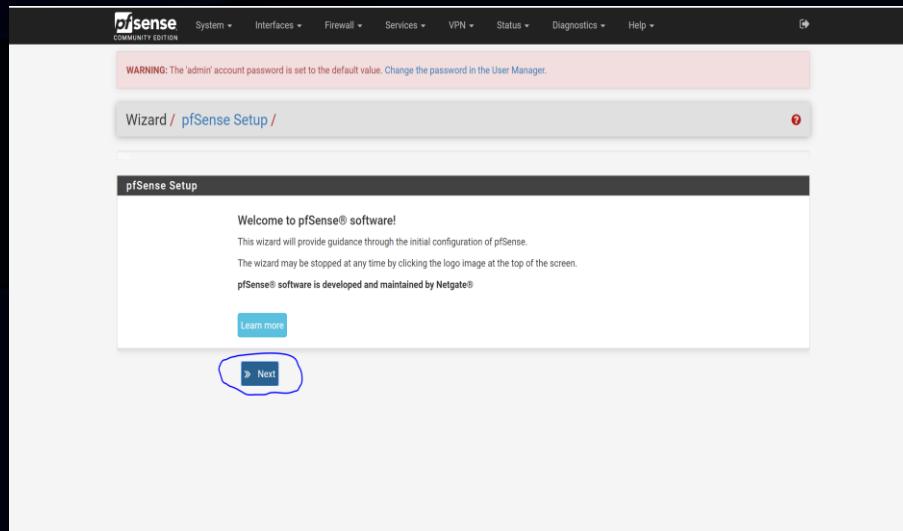
Enter an option: 8

[2.4.5-RELEASE][root@pfSense.localdomain]#root: pfS
pfSctl                               pfSense-upgrade
pfSense-dhcclient-script pfSsh.php
[2.4.5-RELEASE][root@pfSense.localdomain]#root: pfSsh.php playback enableallowall
wan
Adding allow all rule...
Turning off block private networks (if on)...
Turning off block bogon networks (if on)...
Reloading the filter configuration...

[2.4.5-RELEASE][root@pfSense.localdomain]#root:
Message from syslogd@pfSense at Apr 11 19:26:20 ...
php-fpm[362]: /index.php: Successful login for user 'admin' from: 192.168.1.12 (Local Database)
```

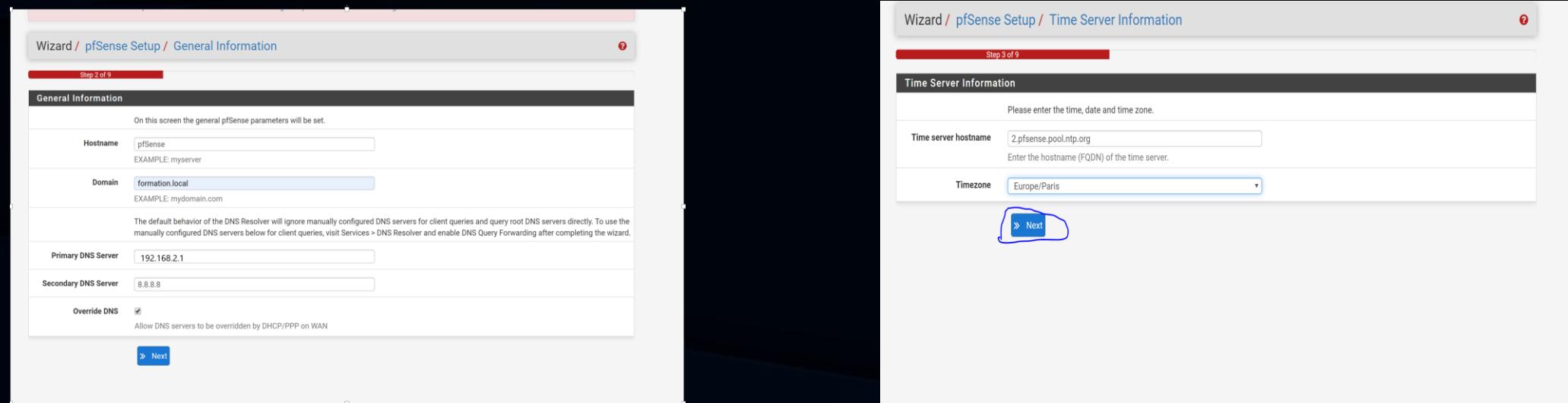


Configuration pfSense



- 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



The image shows two screenshots of the pfSense Setup wizard.

Left Screenshot: General Information (Step 2 of 9)

This screen allows setting general pfSense parameters. It includes fields for Hostname (pfSense), Domain (formation.local), Primary DNS Server (192.168.2.1), Secondary DNS Server (8.8.8.8), and an Override DNS checkbox. A note at the bottom states: "The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard."

Right Screenshot: Time Server Information (Step 3 of 9)

This screen requires entering time, date, and time zone information. It shows a Time server hostname field containing "2.pfsense.pool.ntp.org" and a Timezone dropdown set to "Europe/Paris". A blue oval highlights the "» Next" button at the bottom right of the screen.

Configuration pfSense

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType: Static

General configuration

MAC Address:

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xxxxxxxx:xxxx or leave blank.

MTU:

Set the MTU of the WAN interface. If this field is left blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS:

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If this field is left blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

Static IP Configuration

IP Address: 192.168.1.26

Subnet Mask: 24

Upstream Gateway: 192.168.1.254

DHCP client configuration

DHCP Hostname:

The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

ppplocalsubnet 32

PPTP Remote IP Address:

PPTP Dial on demand: Enable Dial-On-Demand mode
This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

PPTP Idle timeout:

If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

RFC1918 Networks

Block RFC1918 Private Networks: Block private networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Block bogon networks

Block bogon networks: Block non-Internet routed networks from entering via WAN
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

>> Next

Configuration pfSense

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address: 192.168.2.1

Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 24

» Next

COMMUNITY EDITION

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

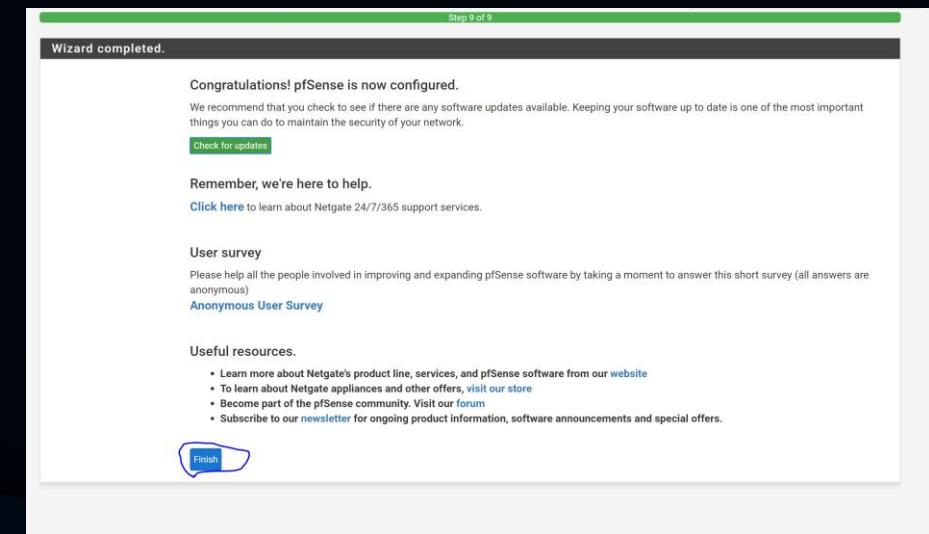
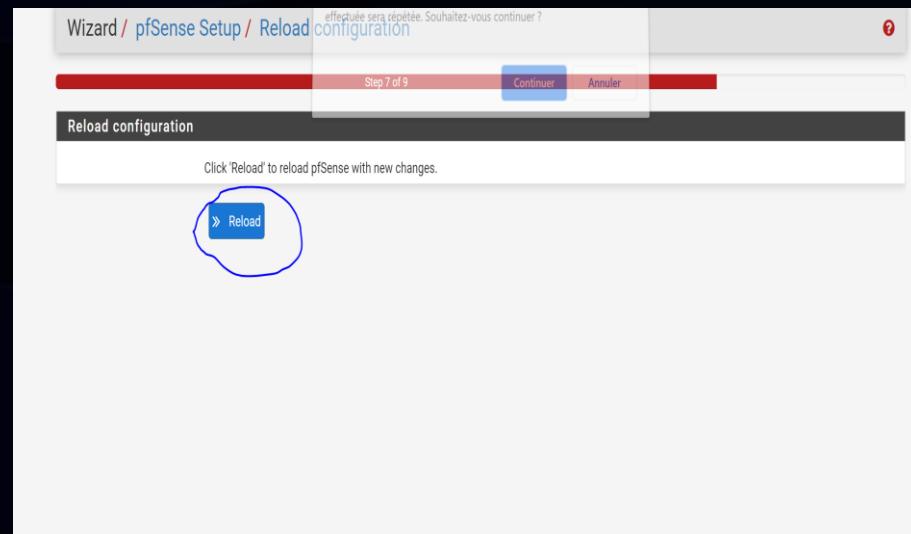
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password: *admin*

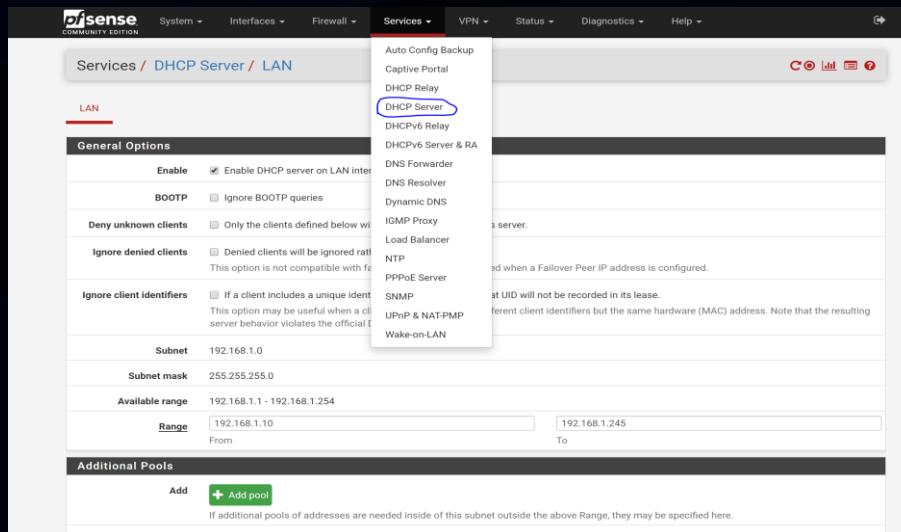
Admin Password AGAIN:

>> Next

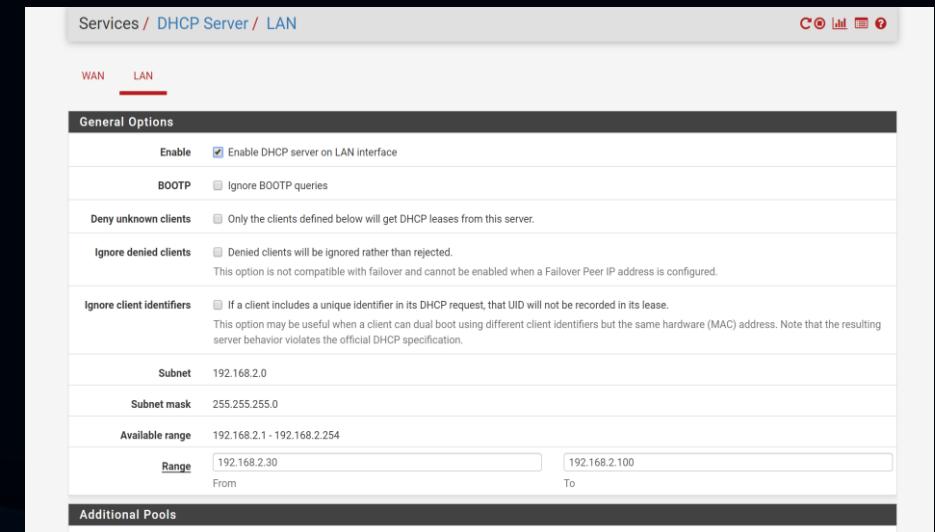
Configuration pfSense



pfSense DHCP Server



The screenshot shows the pfSense DHCP Server configuration for the LAN interface. The 'General Options' section is active, with the 'Enable' checkbox checked. Other options like 'BOOTP', 'Deny unknown clients', and 'Ignore denied clients' are also present. The 'Subnet' is set to 192.168.1.0 and the 'Subnet mask' is 255.255.255.0. The 'Available range' is specified as 192.168.1.1 - 192.168.1.254. A 'Range' field shows 'From' as 192.168.1.10 and 'To' as 192.168.1.245. An 'Additional Pools' section at the bottom allows for specifying ranges outside the main subnet.



This screenshot shows a similar configuration page but with different settings. The 'General Options' section has the 'Enable' checkbox checked. Under 'BOOTP', the 'Ignore BOOTP queries' checkbox is checked. The 'Subnet' is set to 192.168.2.0 and the 'Subnet mask' is 255.255.255.0. The 'Available range' is specified as 192.168.2.1 - 192.168.2.254. A 'Range' field shows 'From' as 192.168.2.30 and 'To' as 192.168.2.100. The 'Additional Pools' section is identical to the first screenshot.

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

pfSense DHCP Server

Servers

WINS servers

DNS servers

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

Other Options

Gateway
The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

Domain name
The default is to use the domain name of this system as the default domain name provided by DHCP. An alternate domain name may be specified here.

Domain search list
The DHCP server can optionally provide a domain search list. Use the semicolon character as separator.

Default lease time
This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.

Enable this to add DHCP leases statistics to the RRD graphs. Disabled by default.

Ping check Disable ping check
When enabled dhcpcd sends a ping to the address being assigned, and if no response has been heard, it assigns the address. Enabled by default.

Dynamic DNS

MAC address control

NTP

TFTP

LDAP

Network Booting

Additional BOOTP/DHCP Options

DHCP Static Mappings for this Interface

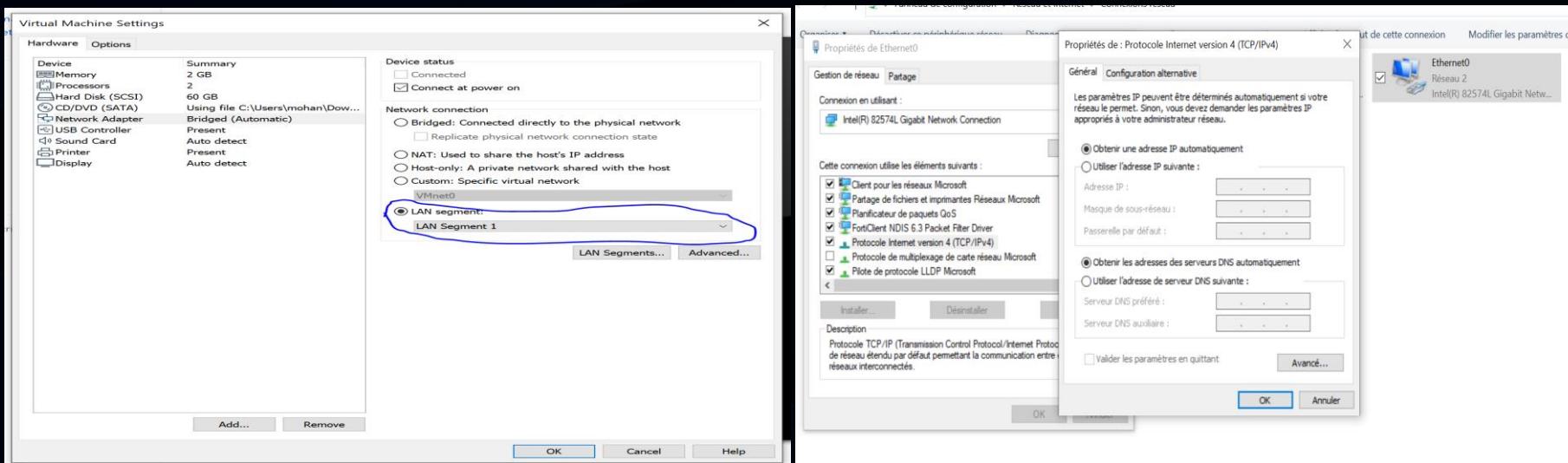
Static ARP	MAC address	IP address	Hostname	Description

@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 :

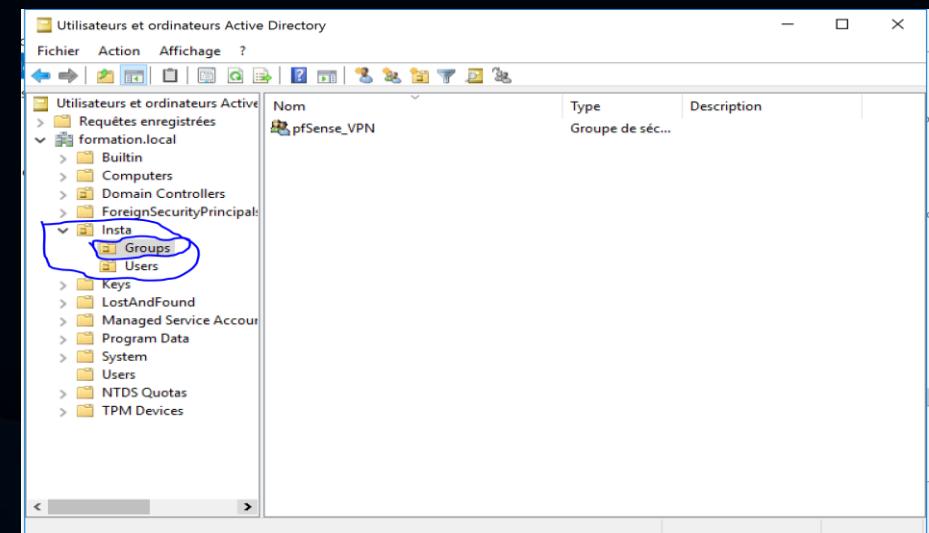
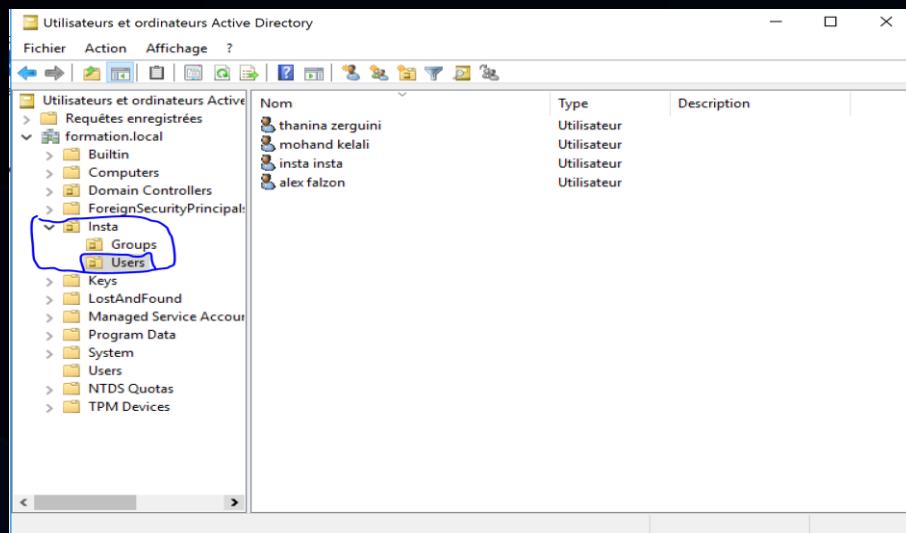
- Ajouter la machine dans le domaine formation.local
- Afin de contourner un problème d'ajout au domaine, à fixer @IP du DNS par: 192.168.2.31.
- Une fois ajoutée, remettre @IP DNS en automatique.



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.

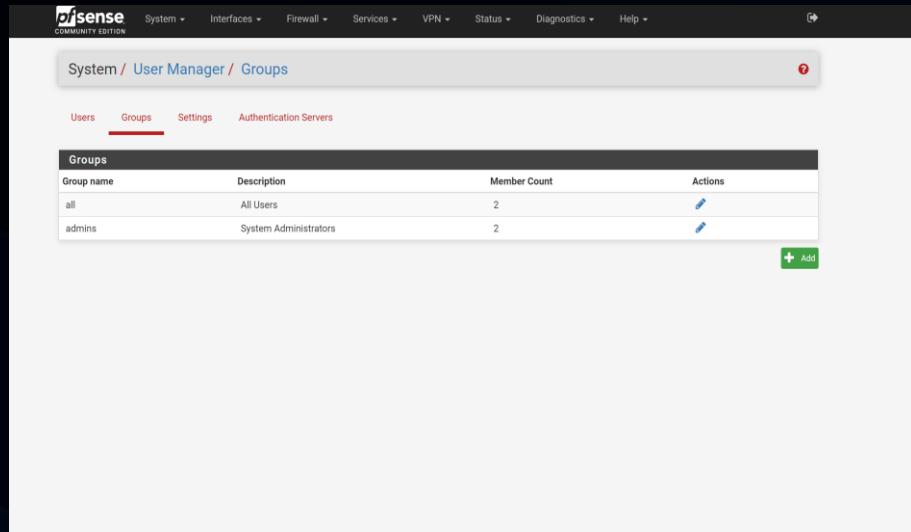


A partir de l'active directory :

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

pfSense OpenVPN

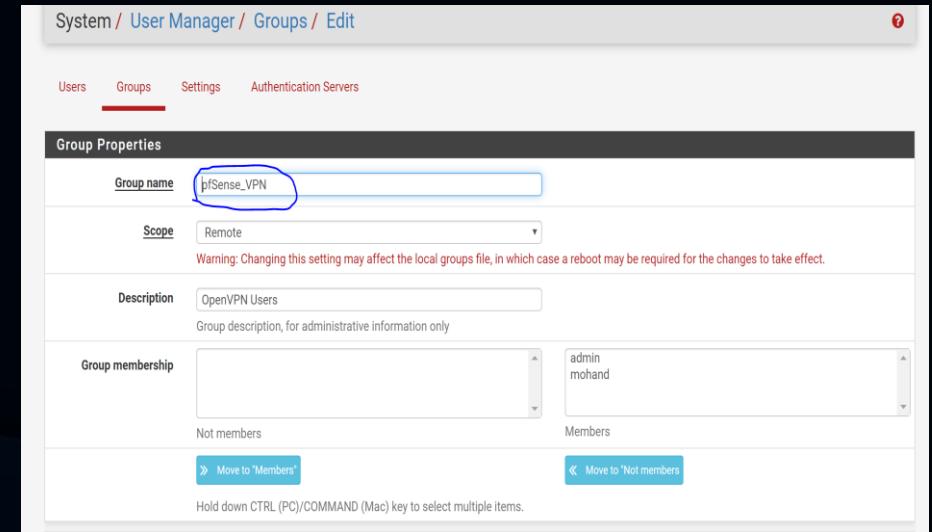
Intégration avec LDAP



The screenshot shows the pfSense WebGUI interface. In the top navigation bar, the 'User Manager / Groups' section is selected. Below it, there are tabs for 'Users', 'Groups' (which is highlighted in red), 'Settings', and 'Authentication Servers'. The main content area displays a table titled 'Groups' with two entries:

Group name	Description	Member Count	Actions
all	All Users	2	
admins	System Administrators	2	

A green '+' button labeled 'Add' is located at the bottom right of the table.



The screenshot shows the 'Edit Group Properties' dialog from the pfSense WebGUI. The 'Groups' tab is selected in the top navigation. The 'Group Properties' section includes fields for 'Group name' (set to 'pfSense_VPN'), 'Scope' (set to 'Remote'), and 'Description' (set to 'OpenVPN Users'). The 'Group membership' section lists 'admin' and 'mohand' under the 'Members' tab. At the bottom, there are buttons for 'Move to "Members"' and 'Move to "Not members"'.

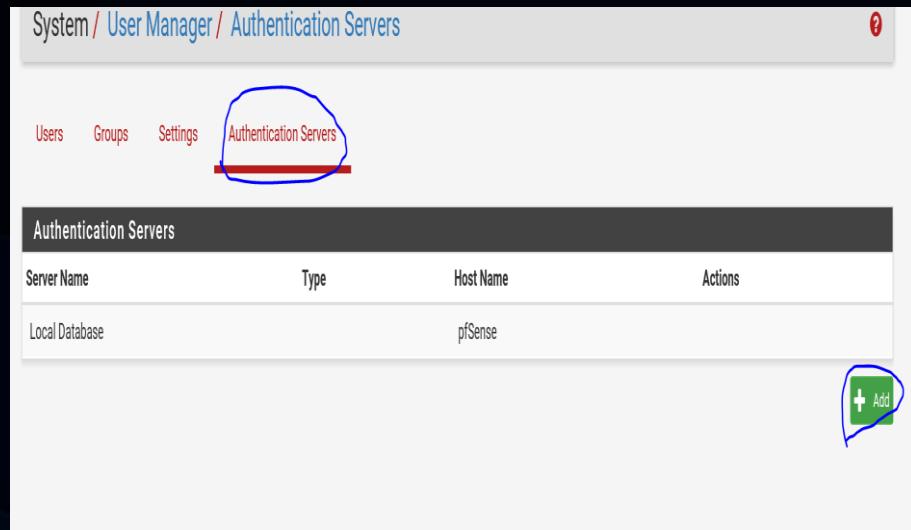
A partir de l'interface WebGUI :

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

pfSense OpenVPN

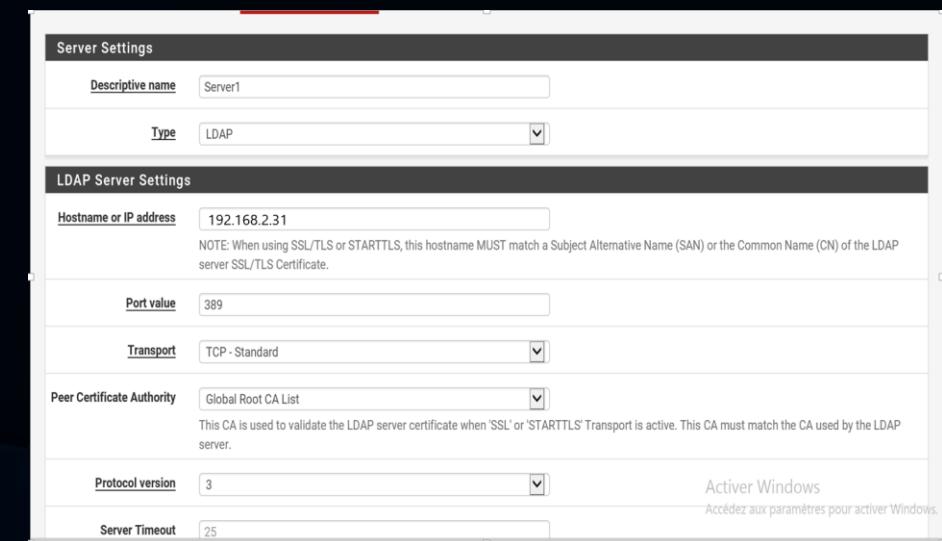
Intégration avec LDAP

- 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).



The screenshot shows the pfSense User Manager Authentication Servers interface. At the top, there are tabs for Users, Groups, Settings, and Authentication Servers, with 'Authentication Servers' being the active tab. A blue circle highlights the 'Authentication Servers' tab. Below it, a table lists an 'Authentication Servers' entry:

Server Name	Type	Host Name	Actions
Local Database	pfSense		



The screenshot shows the 'Server Settings' dialog for an LDAP server. The 'Descriptive name' is set to 'Server1' and the 'Type' is 'LDAP'. The 'LDAP Server Settings' section includes:

- Hostname or IP address: 192.168.2.31
- Port value: 389
- Transport: TCP - Standard
- Peer Certificate Authority: Global Root CA List
- Protocol version: 3
- Server Timeout: 25

A note at the bottom right says 'Activer Windows' (Activate Windows) and 'Accédez aux paramètres pour activer Windows.' (Access the settings to activate Windows.)

pfSense OpenVPN

Intégration avec LDAP

Timeout for LDAP operations (seconds)

Search scope: Level Entire Subtree

Base DN: DC=formation,DC=local

Authentication containers: OU=Users,OU=Insta,DC=formation,DC=local

Extended query: Enable extended query

Query: memberOf=CN=pfSense_VPN,OU=Groups,OU=Insta,DC=formation,DC=local

Bind anonymous: Use anonymous binds to resolve distinguished names

Bind credentials: insta@formation.local

User naming attribute: samAccountName

Group naming attribute: cn

Group member attribute: memberOf

RFC 2307 Groups: LDAP Server uses RFC 2307 style group membership

Group Object Class: posixGroup

UTF8 Encode: UTF8 encode LDAP parameters before sending them to the server.

Extended query: Enable extended query

Bind anonymous: Use anonymous binds to resolve distinguished names

Bind credentials: CN=Administrateur,CN=Users,DC=formation,DC=local

Initial Template: OpenLDAP

User naming attribute: cn

Group naming attribute: cn

Group member attribute: member

RFC 2307 Groups: LDAP Server uses RFC 2307 style group membership

Group Object Class: posixGroup

UTF8 Encode: UTF8 encode LDAP parameters before sending them to the server.

Username Alterations: Do not strip away parts of the username after the @ symbol
e.g. user@host becomes user when unchecked.

Save

Activer Windows
Accédez aux paramètres pour activer Windows

- 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

Diagnostics / Authentication

Authentication Test

Authentication Server: Server AD
Select the authentication server to test against.

Username: insta

Password:


Diagnostics / Authentication

User insta authenticated successfully. This user is a member of groups:

- pfSense_VPN

Authentication Test

Authentication Server: Server AD
Select the authentication server to test against.

Username: Insta

Password:



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

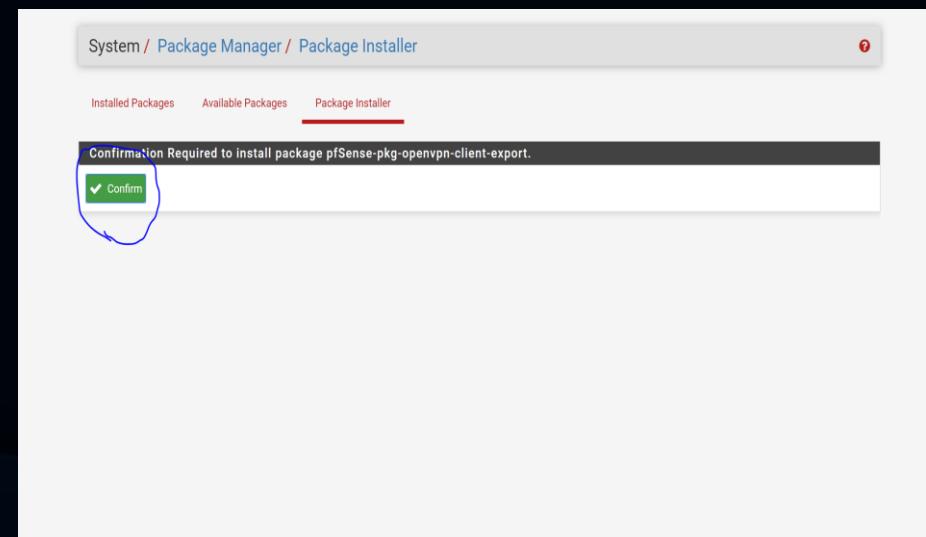
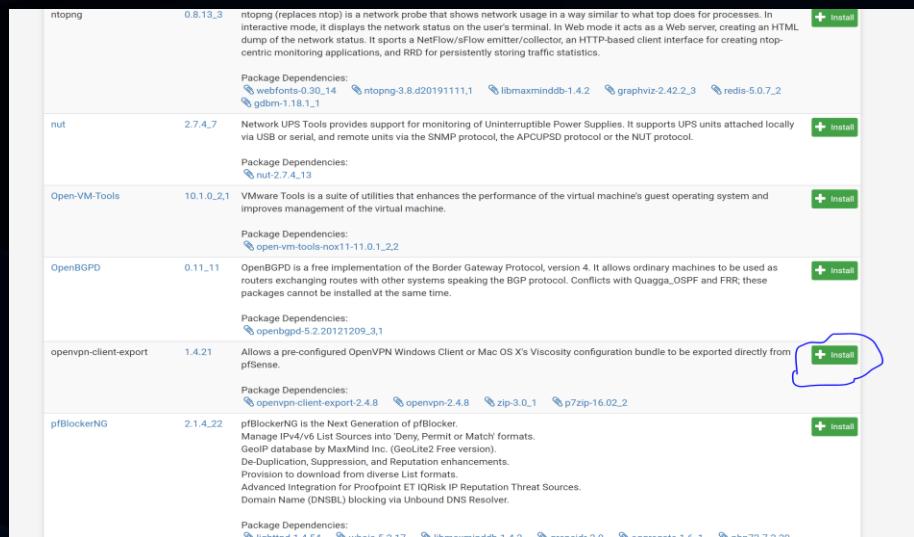
The screenshot shows the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. On the left, a sidebar menu lists various system management options like Advanced, Cert. Manager, General Setup, High Avail. Sync, Logout (admin), and Package Manager (which is highlighted with a blue oval). Below this are sections for Leases, IP address, and Leases in Use. The main content area displays a table of leases with columns for Hostname, Description, Start, End, Online, Lease Type, and Actions.

The screenshot shows the pfSense Package Manager interface. At the top, there are tabs for 'Installed Packages' and 'Available Packages' (which is highlighted with a red oval). Below is a search bar and a table of packages. The table has columns for Name, Version, and Description. Each package entry includes a green '+' button labeled 'Install'. The packages listed include acme, apcupsd, arping, arpwatch, and Avahi.

Name	Version	Description
acme	0.6.6	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates. Package Dependencies: • pecl-ssh2-1.1.2 socat-1.7.3.3.1 php72-7.2.29 php72-ftp-7.2.29
apcupsd	0.3.91_8	"apcupsd" can be used for controlling all APC UPS models. It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN. Package Dependencies: • apcupsd-3.14.14_2
arping	1.2.2.1	Broadcasts a who-has ARP packet on the network and prints answers. Package Dependencies: • arping-2.19
arpwatch	0.2.0	This package contains tools that monitors ethernet activity and maintains a database of ethernet/ip address pairings. It also reports certain changes via email. Package Dependencies: • arpwatch-3.0.4
Avahi	2.1_1	Avahi is a system which facilitates host and service discovery in local networks via mDNS (Multicast DNS) and DNS-SD (DNS Service Discovery). This package allows mDNS/DNS-SD protocols to work across multiple LAN segments. mDNS/DNS-SD is known in Apple circles as "Bonjour" and is part of the Zeroconf suite of protocols.

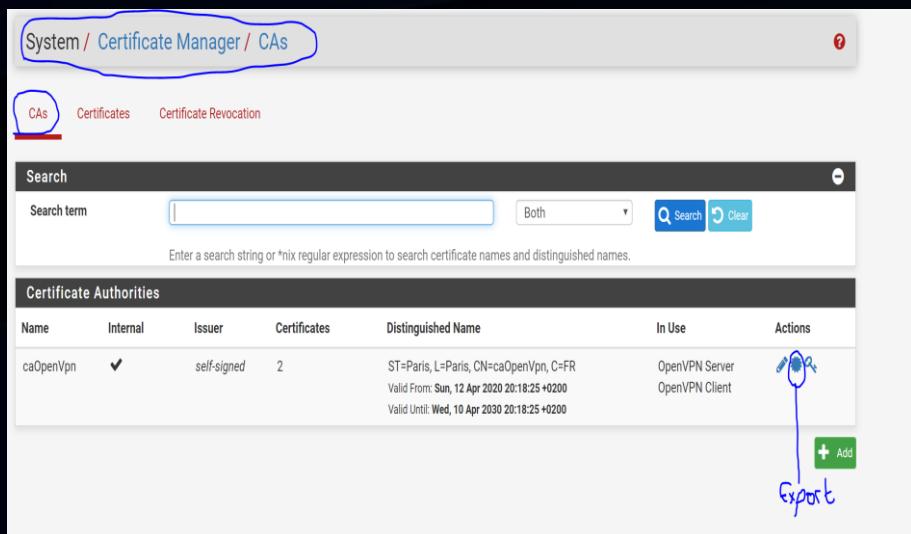
pfSense OpenVPN

Installer le package OpenVPN



pfSense OpenVPN

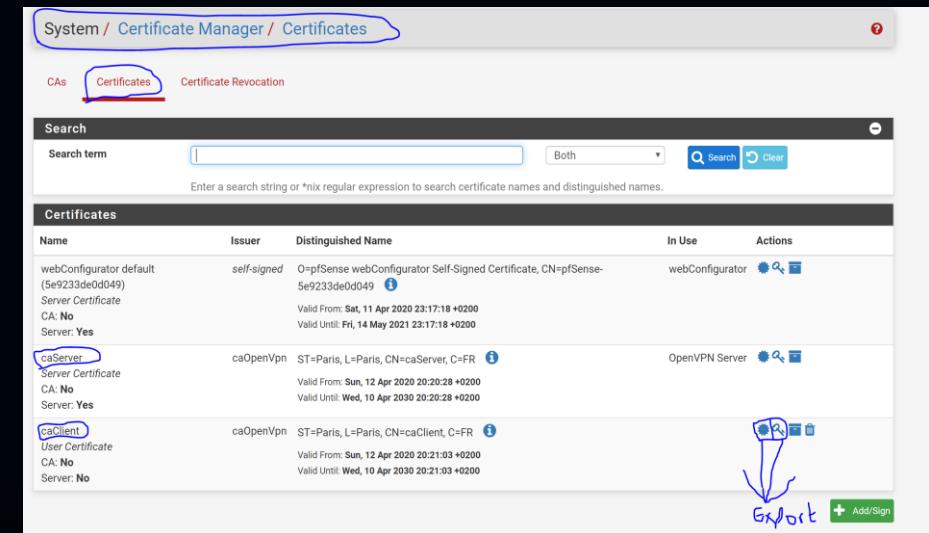
Générer les certificats



The screenshot shows the 'System / Certificate Manager / CAs' interface. The 'CAs' tab is selected. A blue box highlights the top navigation bar. A blue arrow points from the 'caOpenVpn' row in the table to the 'Export' button at the bottom right.

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
caOpenVpn	✓	self-signed	2	ST=Paris, L=Paris, CN=caOpenVpn, C=FR Valid From: Sun, 12 Apr 2020 20:18:25 +0200 Valid Until: Wed, 10 Apr 2030 20:18:25 +0200	OpenVPN Server OpenVPN Client	

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



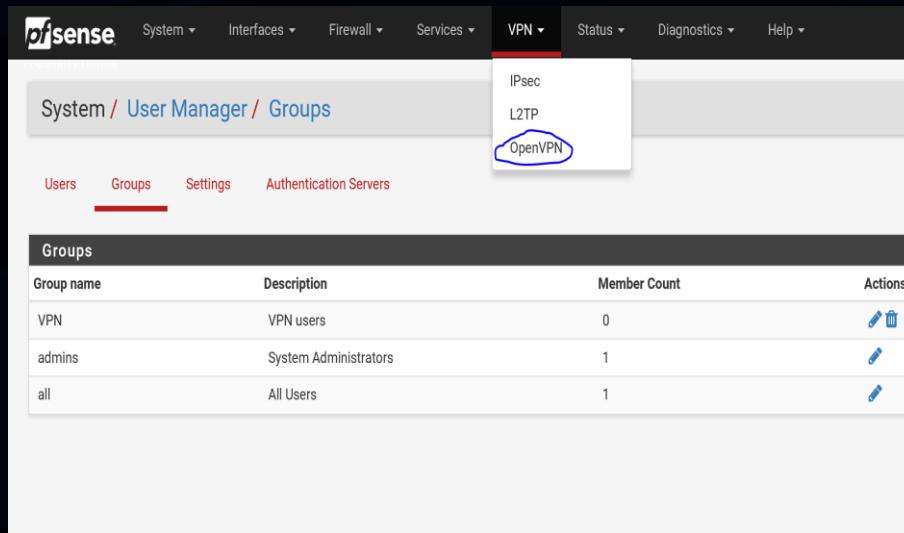
The screenshot shows the 'System / Certificate Manager / Certificates' interface. The 'Certificates' tab is selected. A blue box highlights the top navigation bar. A blue arrow points from the 'caServer' row in the table to the 'Export' button at the bottom right.

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (5e9233de0d049)	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-5e9233de0d049		
caOpenVpn	ST=Paris, L=Paris, CN=caServer, C=FR	Valid From: Sun, 12 Apr 2020 20:20:28 +0200 Valid Until: Wed, 10 Apr 2030 20:20:28 +0200		
caClient	ST=Paris, L=Paris, CN=caClient, C=FR	Valid From: Sun, 12 Apr 2020 20:21:03 +0200 Valid Until: Wed, 10 Apr 2030 20:21:03 +0200		

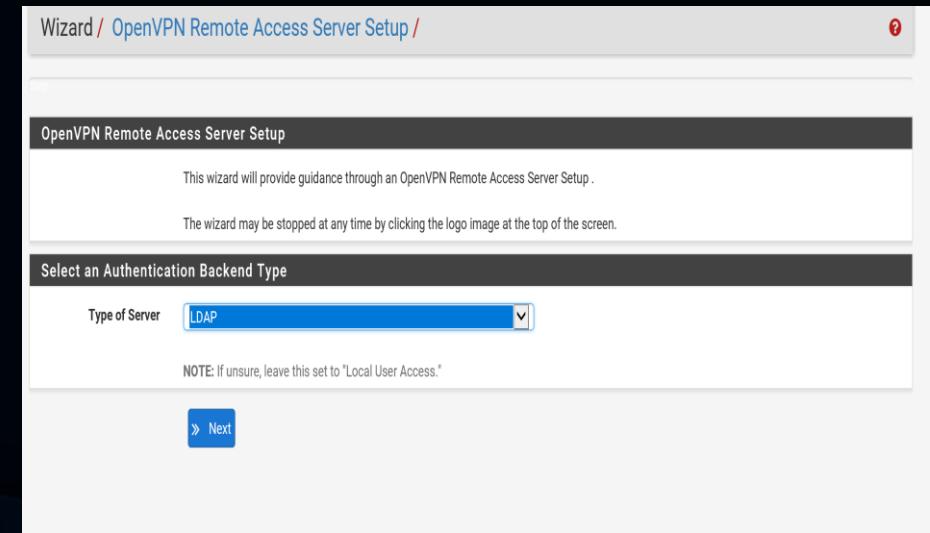
- Créer un certificat pour les clients et un autre pour le serveur OpenVPN.
- Exporter la clé publique et privée du client.

pfSense OpenVPN

Créer un tunnel VPN



The screenshot shows the pfSense User Manager Groups interface. At the top, there is a navigation bar with links for System, Interfaces, Firewall, Services, VPN (which is currently selected), Status, Diagnostics, and Help. A dropdown menu under the VPN link shows options for IPsec, L2TP, and OpenVPN, with OpenVPN highlighted by a blue oval. Below the navigation bar, the main content area displays a table of user groups. The table has columns for Group name, Description, Member Count, and Actions. There are three entries: 'VPN' (Description: 'VPN users', Member Count: 0), 'admins' (Description: 'System Administrators', Member Count: 1), and 'all' (Description: 'All Users', Member Count: 1). Each entry has edit and delete icons in the Actions column.



The screenshot shows the first step of the 'OpenVPN Remote Access Server Setup' wizard. The title bar says 'Wizard / OpenVPN Remote Access Server Setup /'. The main content area is titled 'OpenVPN Remote Access Server Setup' and contains the message: 'This wizard will provide guidance through an OpenVPN Remote Access Server Setup.' It also states: 'The wizard may be stopped at any time by clicking the logo image at the top of the screen.' Below this, there is a section titled 'Select an Authentication Backend Type' with a dropdown menu labeled 'Type of Server' set to 'LDAP'. A note below the dropdown says: 'NOTE: If unsure, leave this set to "Local User Access."'. At the bottom right, there is a blue '» Next' button.

pfSense OpenVPN

Créer un tunnel VPN

Wizard / OpenVPN Remote Access Server Setup / LDAP Server Selection

Step 1 of 11

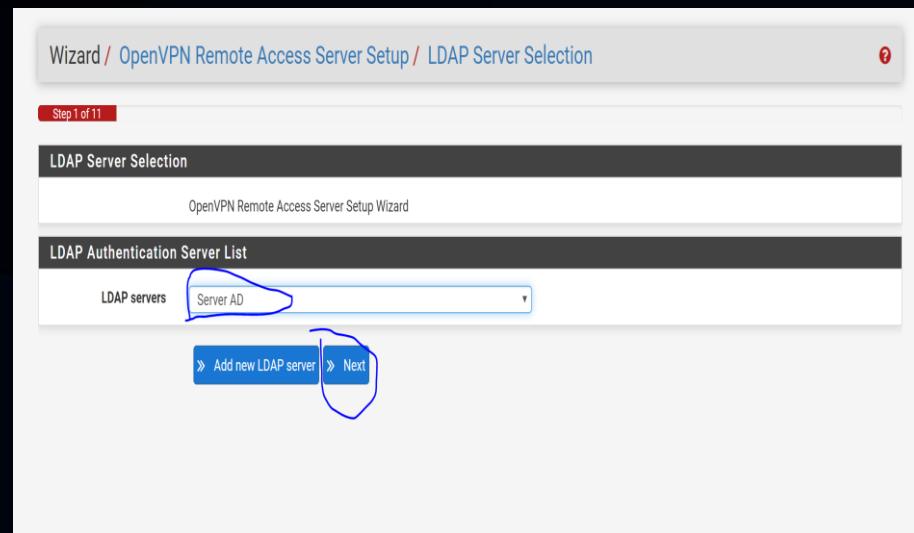
LDAP Server Selection

OpenVPN Remote Access Server Setup Wizard

LDAP Authentication Server List

LDAP servers: Server AD

Add new LDAP server > Next >



Wizard / OpenVPN Remote Access Server Setup / Certificate Authority Selection

Step 5 of 11

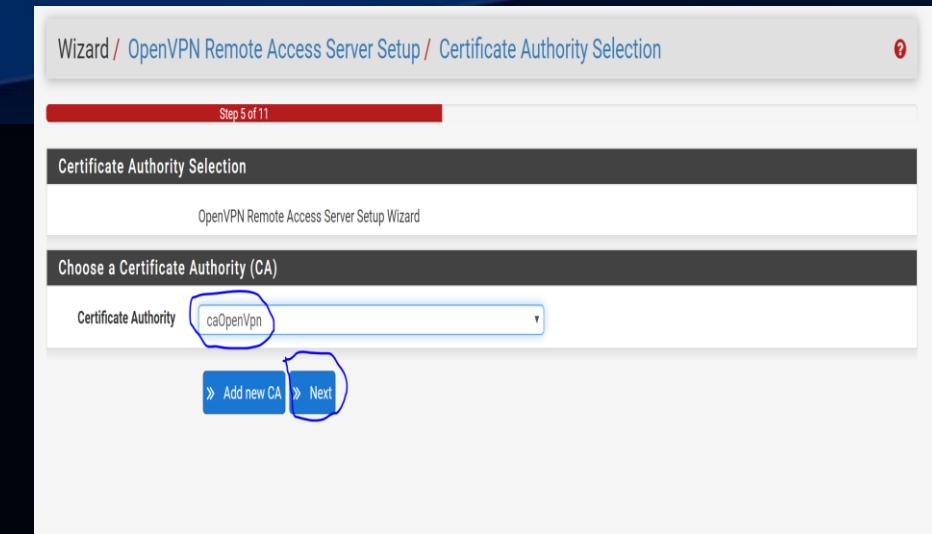
Certificate Authority Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Certificate Authority (CA)

Certificate Authority: caOpenVpn

Add new CA > Next >



Wizard / OpenVPN Remote Access Server Setup / Server Certificate Selection

Step 7 of 11

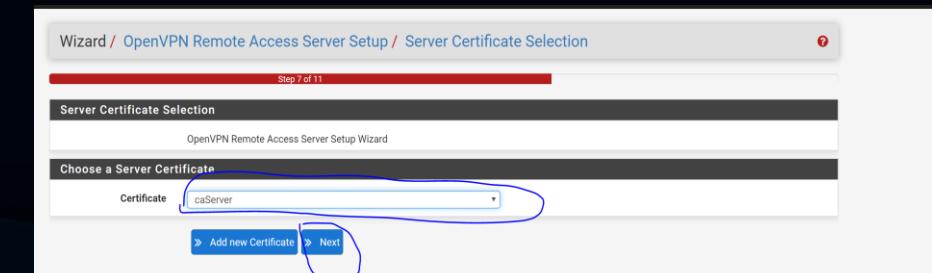
Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Server Certificate

Certificate: caServer

Add new Certificate > Next >



pfSense OpenVPN

Créer un tunnel VPN

Wizard / OpenVPN Remote Access Server Setup / Server Setup

Step 9 of 11

Server Setup

OpenVPN Remote Access Server Wizard

General OpenVPN Server Information

Interface: WAN

The interface where OpenVPN will listen for incoming connections (typically WAN).

Protocol: UDP on IPv4 only

Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.

Local Port: 16840

Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.

Description:

A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

Tunnel Settings

IPv4 Tunnel Network: 10.10.10.0/24
This is the IPv4 virtual network 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.

IPv6 Tunnel Network: [empty]
This is the IPv6 virtual network 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.

IPv6 Local network(s): [empty]
IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX. 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: [empty]
Specify the maximum number of clients allowed to concurrently connect to this server.

Compression: Omit Preference (Use OpenVPN Default)
Compress tunnel packets using the LZ algorithm.
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.

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.

Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration

Step 10 of 11

Firewall Rule Configuration

OpenVPN Remote Access Server Wizard

Firewall Rule Configuration

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

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

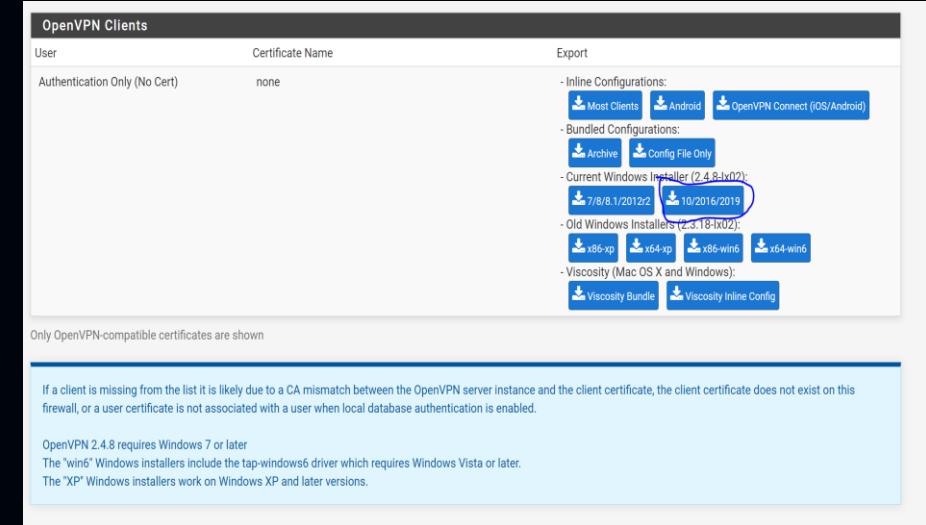
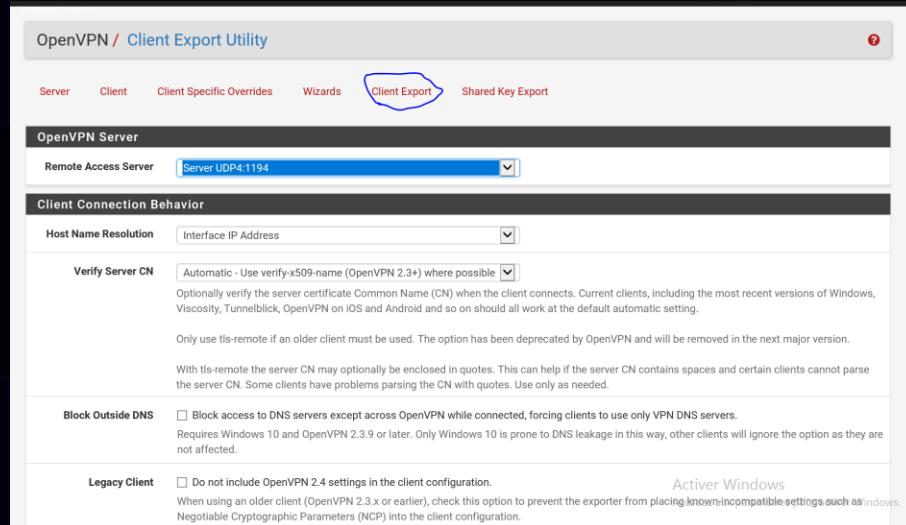
Traffic from clients through VPN

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

Next

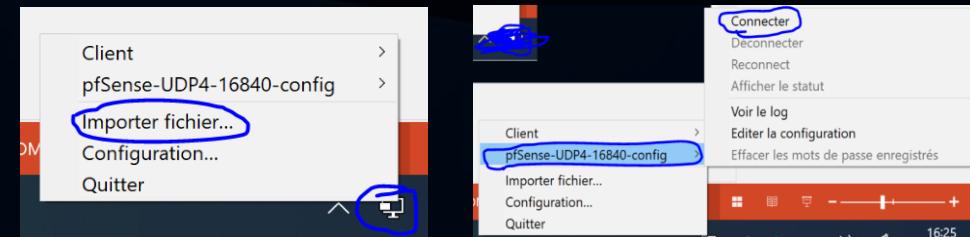
pfSense OpenVPN

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 ☺ .



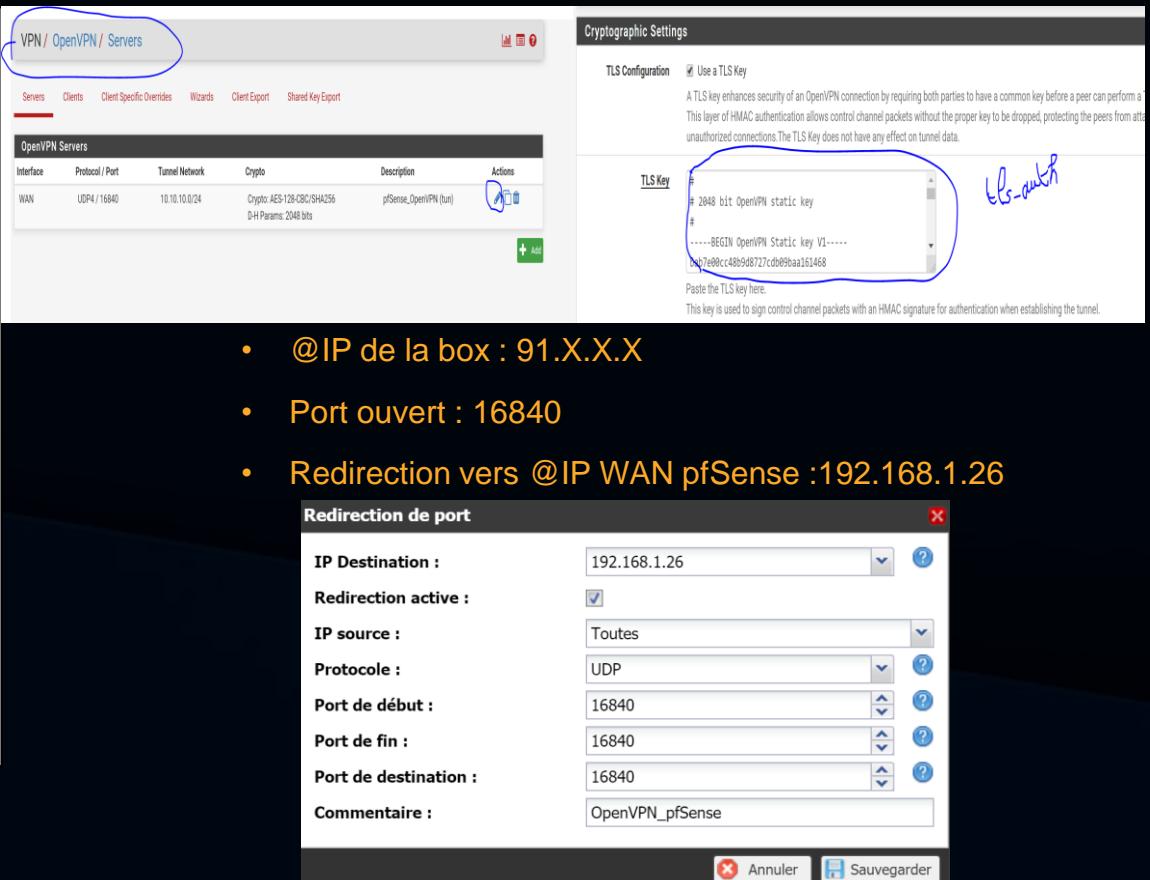
pfSense OpenVPN

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.16840 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
```



The screenshot shows the pfSense OpenVPN configuration interface. The main window displays the 'OpenVPN Servers' table with one entry:

Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
IWAN	UDP/16840	10.10.10.0/24	Crypto: AES-128-CBC/SHA256 D-H Params: 2048 bits	pfSense_OpenVPN (tun)	Edit Delete

The 'TLS Configuration' section is visible, showing a 'TLS Key' field containing a static key. A blue circle highlights the 'TLS Key' field, and handwritten text 'tls-auth' is written next to it.

The 'Redirection de port' dialog box is open, showing port forwarding rules:

IP Destination :	Redirection active :
192.168.1.26	<input checked="" type="checkbox"/>
IP source :	Toutes
Protocole :	UDP
Port de début :	16840
Port de fin :	16840
Port de destination :	16840
Commentaire :	OpenVPN_pfSense

Buttons at the bottom of the dialog box include 'Annuler' (Cancel) and 'Sauvegarder' (Save).

- @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

Services / DHCP Server / LAN

General Options

- Enable Enable DHCP server on LAN interface
- BOOTP Ignore BOOTP queries
- Deny unknown clients Only the clients defined below will get DHCP leases from this server.
- Ignore denied clients Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
- Ignore client identifiers If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet

- Subnet 192.168.2.0
- Subnet mask 255.255.255.0
- Available range 192.168.2.1 - 192.168.2.254
- Range From 192.168.2.10 To 192.168.2.245

Additional Pools

- Add
- If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.

Pool Start	Pool End	Description	Actions
WINS servers	WINS Server 1		
DNS servers	192.168.2.1	local	
DNS Server 2			

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

3-Informations DNS

Attention : Vérifier dans General Setup les informations du serveur

DNS Server Settings

DNS Servers 192.168.2.1

2-Vérifier que le DNS Resolver est activé

Services / DNS Resolver / General Settings

General Settings

- Enable Enable DNS resolver
- Listen Port 53
- Enable SSL/TLS Service Respond to incoming SSL/TLS queries from local clients
- SSL/TLS Certificate webConfigurator default (5e9233de0d049)
- SSL/TLS Listen Port 853

Host Overrides

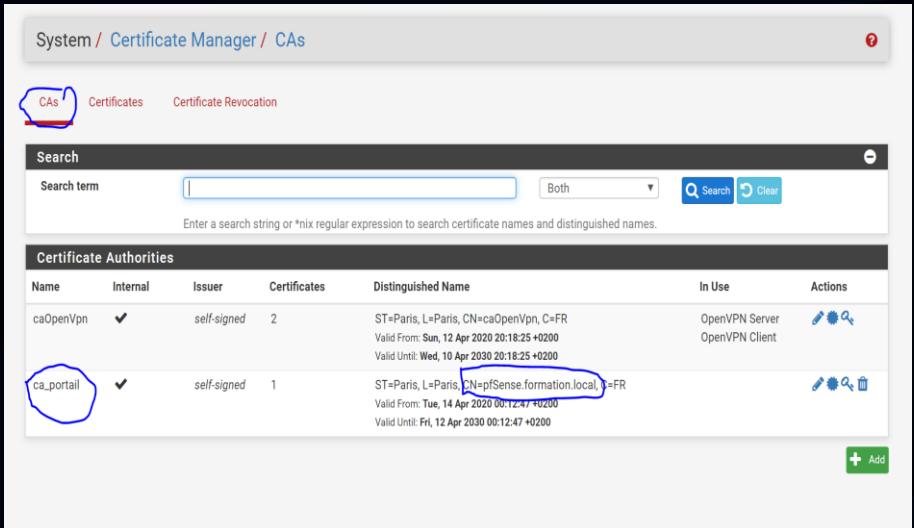
Host	Parent domain of host	IP to return for host	Description	Actions
pfSense	formation.local	192.168.2.1		<input type="button" value="Edit"/>

Create any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.

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

pfSense Portail Captif + LDAP

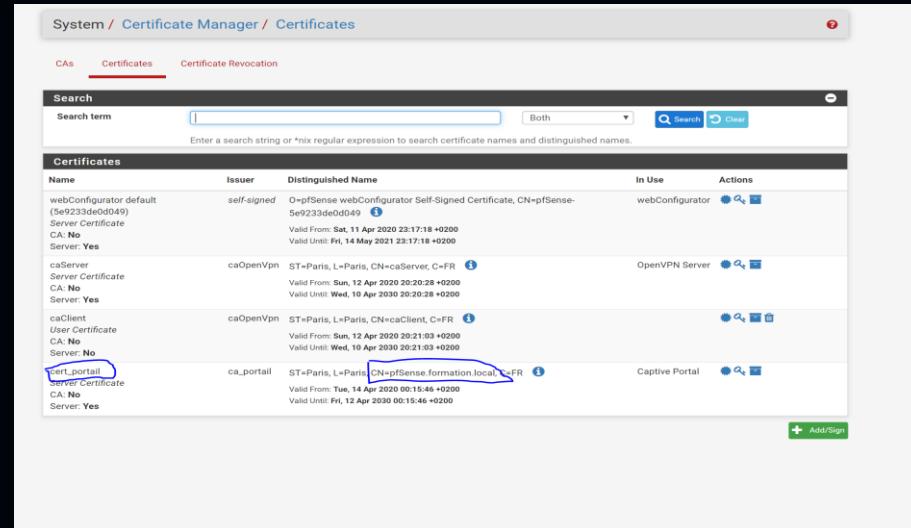
4-Création de certificats



The screenshot shows the 'Certificates' tab in the pfSense Certificate Manager. It lists two certificate authorities:

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
caOpenVpn	✓	self-signed	2	ST=Paris, L=Paris, CN=caOpenVpn, O=FR Valid From: Sun, 12 Apr 2020 20:18:25 +0200 Valid Until: Wed, 10 Apr 2030 20:18:25 +0200	OpenVPN Server OpenVPN Client	
ca_portal	✓	self-signed	1	ST=Paris, L=Paris, CN=pfSense.formation.local, O=FR Valid From: Tue, 14 Apr 2020 00:12:47 +0200 Valid Until: Fri, 12 Apr 2030 00:12:47 +0200		

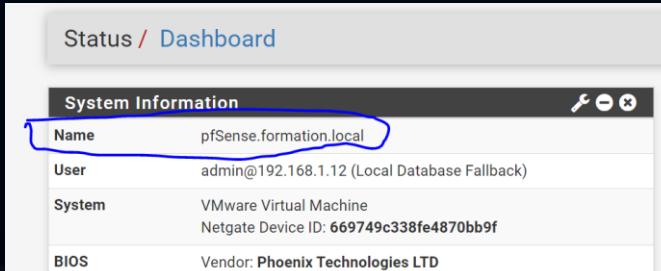
- Certificat d'autorité.
- Common Name = pfSense.formation.local



The screenshot shows the 'Certificates' tab in the pfSense Certificate Manager. It lists several certificates:

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-webConfigurator	webConfigurator	
caServer	CA: No	Server Certificate		
caOpenVpn	ST=Paris, L=Paris, CN=caServer, C=FR	Valid From: Sun, 12 Apr 2020 23:17:18 +0200 Valid Until: Fri, 14 May 2021 23:17:18 +0200	OpenVPN Server	
caUser	CA: No	User Certificate		
caOpenVpn	ST=Paris, L=Paris, CN=caClient, C=FR	Valid From: Sun, 12 Apr 2020 20:20:28 +0200 Valid Until: Wed, 10 Apr 2030 20:20:28 +0200		
caPortal	CA: No	caPortal		
ca_portal	ST=Paris, L=Paris, CN=pfSense.formation.local, C=FR	Valid From: Tue, 14 Apr 2020 00:15:46 +0200 Valid Until: Fri, 12 Apr 2030 00:15:46 +0200	Captive Portal	

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

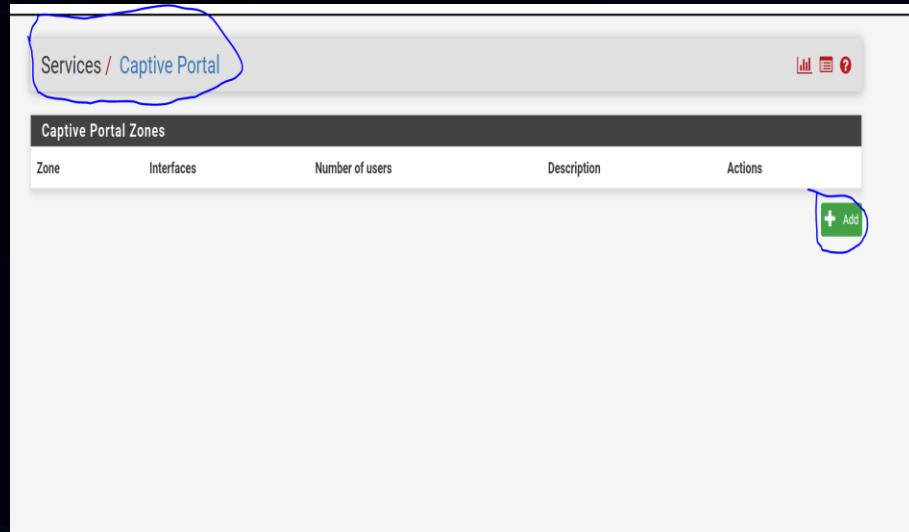


The screenshot shows the 'System Information' section of the pfSense Status / Dashboard. It displays the following details:

Name	Value
Name	pfSense.formation.local
User	admin@192.168.1.12 (Local Database Fallback)
System	VMware Virtual Machine Netgate Device ID: 669749c338fe4870bb9f
BIOS	Vendor: Phoenix Technologies LTD

pfSense Portail Captif + LDAP

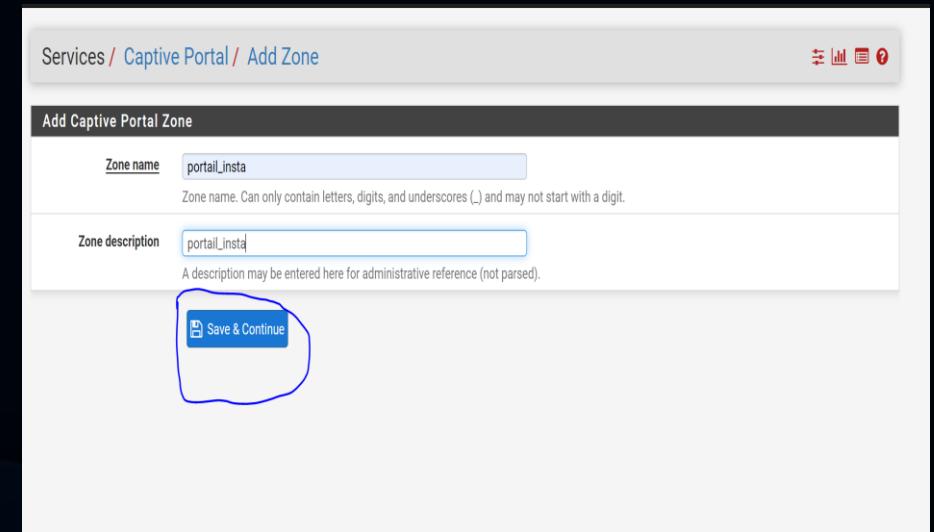
5-Création du portail captif



Services / Captive Portal

Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
				



Services / Captive Portal / Add Zone

Add Captive Portal Zone

Zone name: portail_insta
Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit.

Zone description: portail_insta
A description may be entered here for administrative reference (not parsed).



pfSense Portail Captif + LDAP



5-Création du portail captif

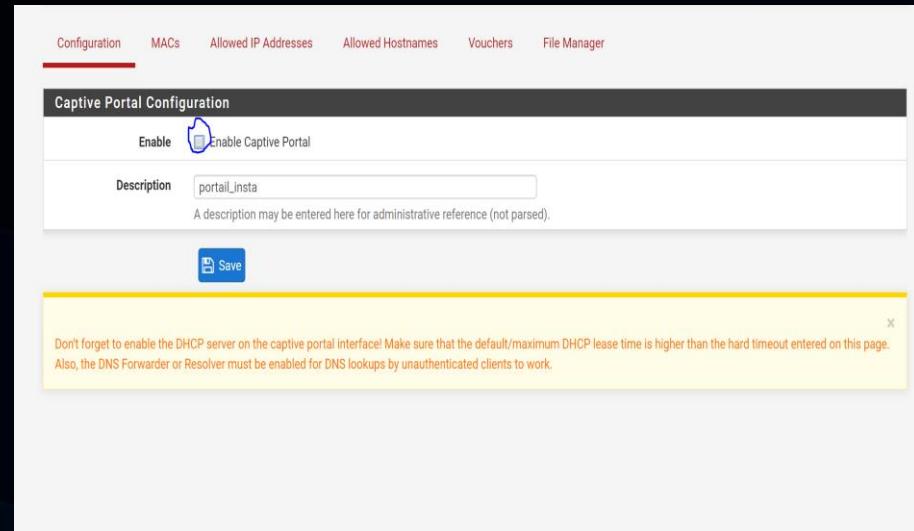
Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers File Manager

Captive Portal Configuration

Enable Enable Captive Portal

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

Don't forget to enable the DHCP server on the captive portal interface! Make sure that the default/maximum DHCP lease time is higher than the hard timeout entered on this page. Also, the DNS Forwarder or Resolver must be enabled for DNS lookups by unauthenticated clients to work.



Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers File Manager

Captive Portal Configuration

Enable Enable Captive Portal

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

Interfaces WAN LAN Select the interface(s) to enable for captive portal.

Maximum concurrent connections Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.

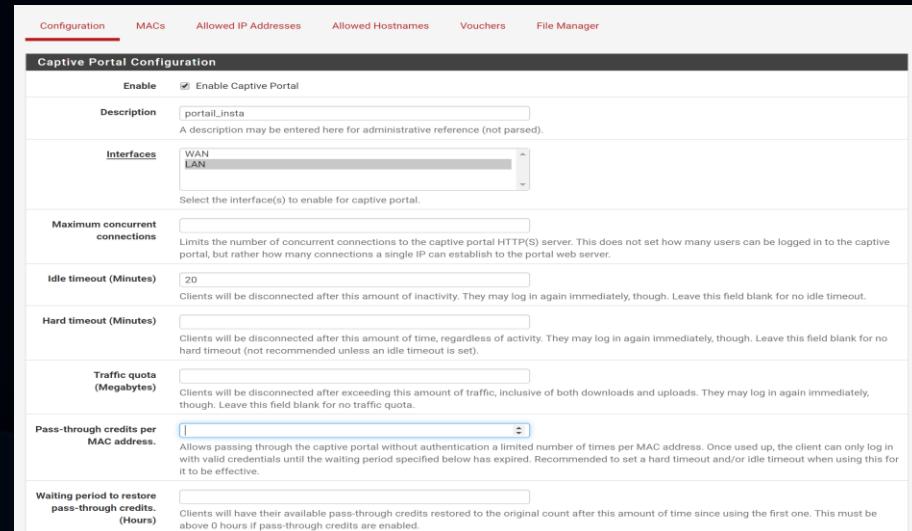
Idle timeout (Minutes) Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

Hard timeout (Minutes) Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).

Traffic quota (Megabytes) Clients will be disconnected after exceeding this amount of traffic, inclusive of both downloads and uploads. They may log in again immediately, though. Leave this field blank for no traffic quota.

Pass-through credits per MAC address. Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this feature.

Waiting period to restore pass-through credits. (Hours) Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.



pfSense Portail Captif + LDAP



5-Création du portail captif

Pass-through credits per MAC address.

Allows passing through the captive portal without authentication a limited number of times per MAC address. Once used up, the client can only log in with valid credentials until the waiting period specified below has expired. Recommended to set a hard timeout and/or idle timeout when using this for it to be effective.

Waiting period to restore pass-through credits. (Hours)

Clients will have their available pass-through credits restored to the original count after this amount of time since using the first one. This must be above 0 hours if pass-through credits are enabled.

Reset waiting period

Enable waiting period reset on attempted access

If enabled, the waiting period is reset to the original duration if access is attempted when all pass-through credits have already been exhausted.

Logout popup window

Enable logout popup window

If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.

Pre-authentication redirect URL

Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \$PORTAL_REDIRURLS variable in captiveportal's HTML pages.

After authentication Redirection URL

Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.

Blocked MAC address redirect URL

Blocked MAC addresses will be redirected to this URL when attempting access.

Concurrent user logins

Disable Concurrent user logins

If enabled only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.

MAC filtering

Disable MAC filtering

If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

Pass-through MAC Auto Entry

Enable Pass-through MAC automatic addition

When enabled, a MAC passthrough entry is automatically added after the user has successfully authenticated. Users of that MAC address will never have to authenticate again. To remove the passthrough MAC entry either log in and remove it manually from the MAC tab or send a POST from another system. If this is enabled, the logout window will not be shown.

Authentication Method

Select an Authentication Method to use for this zone. One method must be selected.

- "Authenticating backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers.
- "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button.
- "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.

Authentication Server

Server AD: Local Database

Secondary authentication Server

Server AD: Local Database

You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.

Reauthenticate Users

Reauthenticate connected users every minute

If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; The cached credentials are necessary for the portal to perform automatic reauthentication requests.

HTTPS Options

Login

Enable HTTPS login

When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.

HTTPS server name

pfSense formation.local

This name will be used in the form action for the HTTPS POST and should match the Common Name (CN) in the certificate (otherwise, the client browser will most likely display a security warning). Make sure captive portal clients can resolve this name in DNS and verify on the client that the IP resolves to the correct interface IP on pfSense.

SSL/TLS Certificate

cert_portail

If no certificates are defined, one may be defined here: System > Cert. Manager

HTTPS Forwards

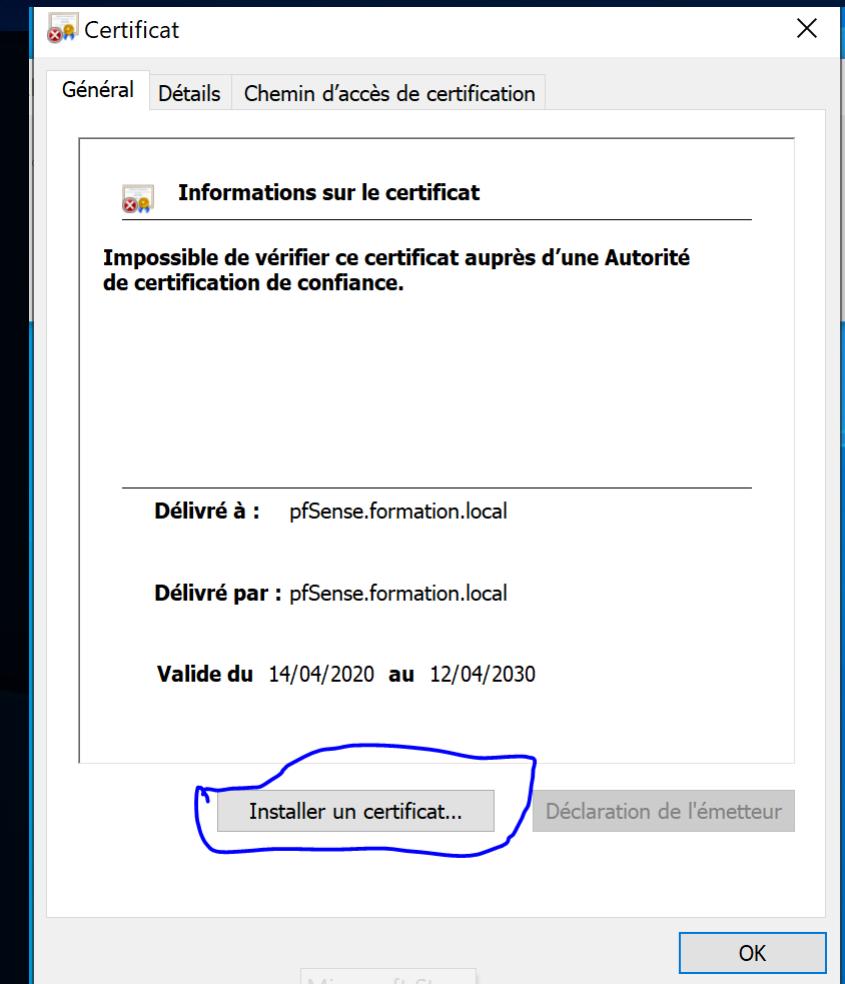
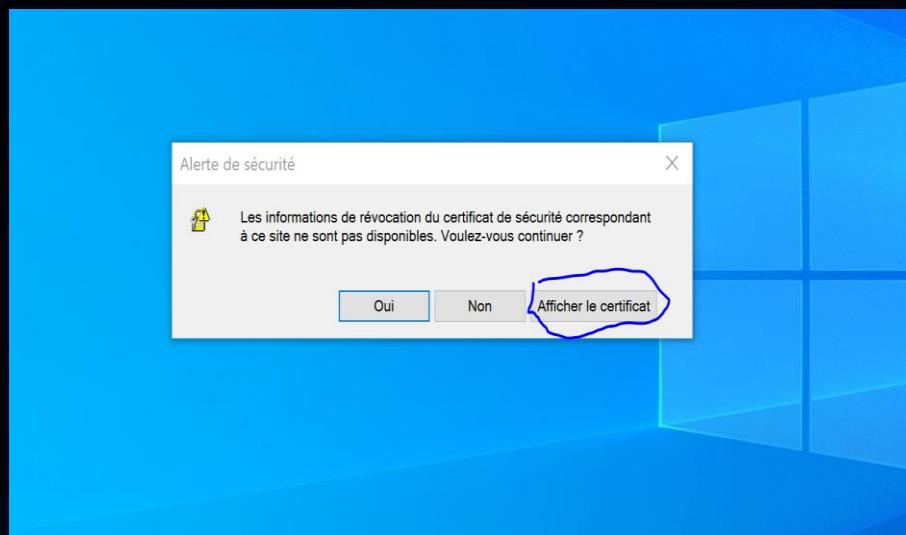
Disable HTTPS Forwards

If this option is set, attempts to connect to HTTPS (SSL/TLS on port 443) sites will not be forwarded to the captive portal. This prevents certificate errors from being presented to the user even if HTTPS logins are enabled. Users must attempt a connection to an HTTP (Port 80) site to get forwarded to the captive portal. If HTTPS logins are enabled, the user will be redirected to the HTTPS login page.

pfSense Portail Captif + LDAP

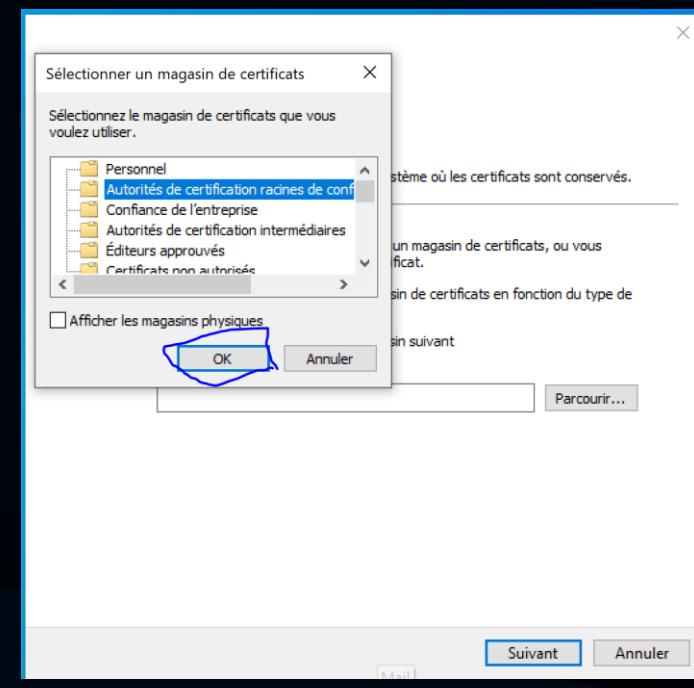
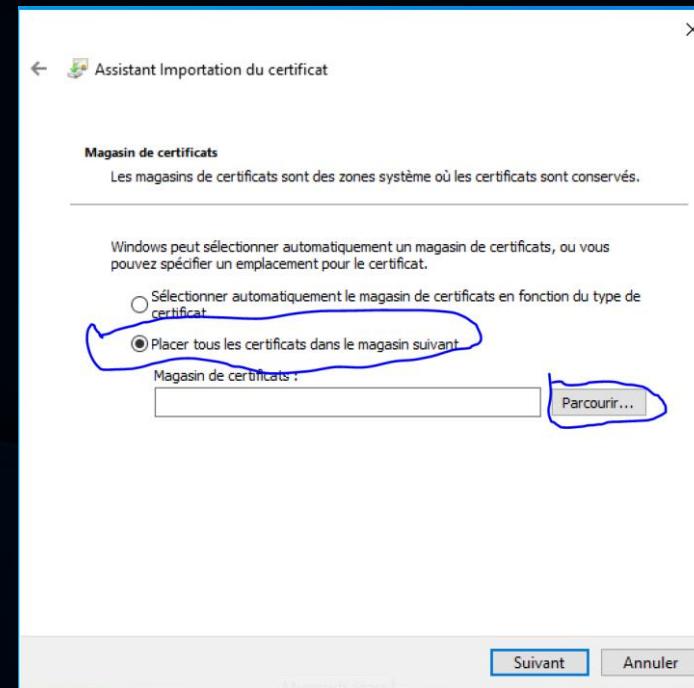
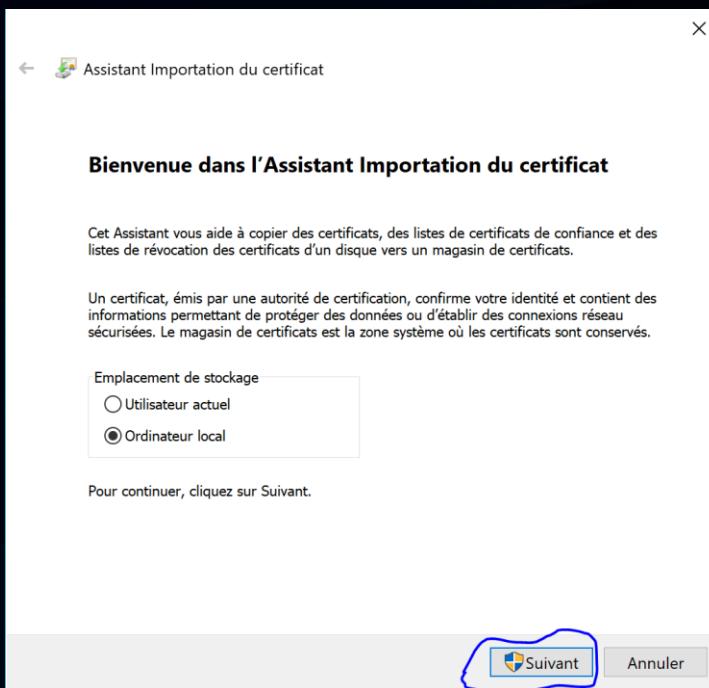
6-Installation du certificat côté client

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



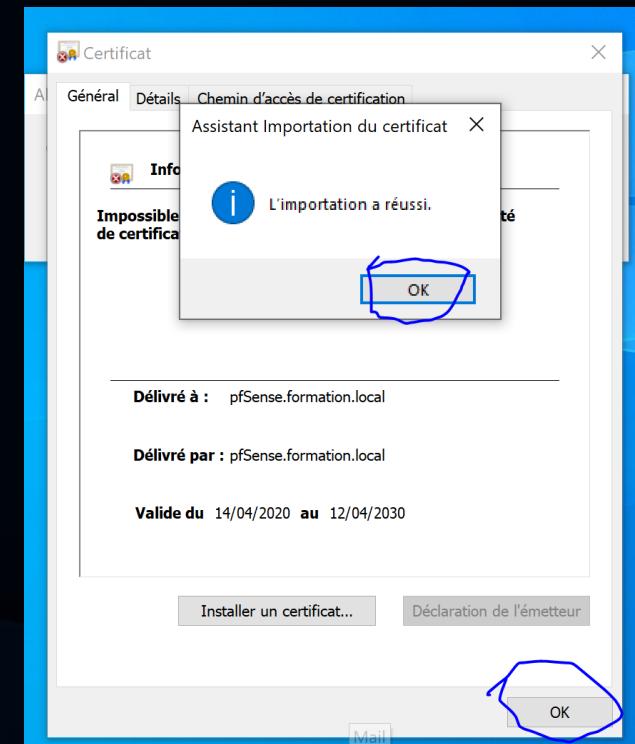
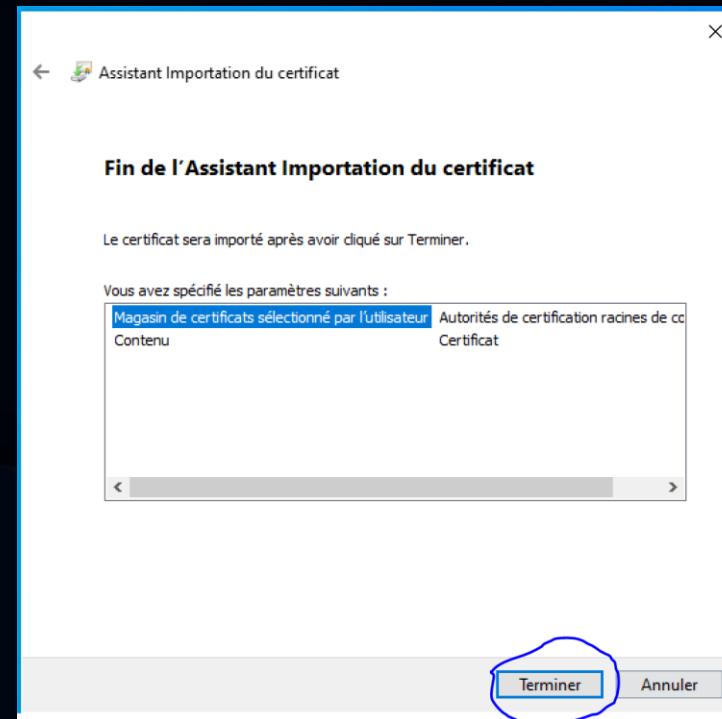
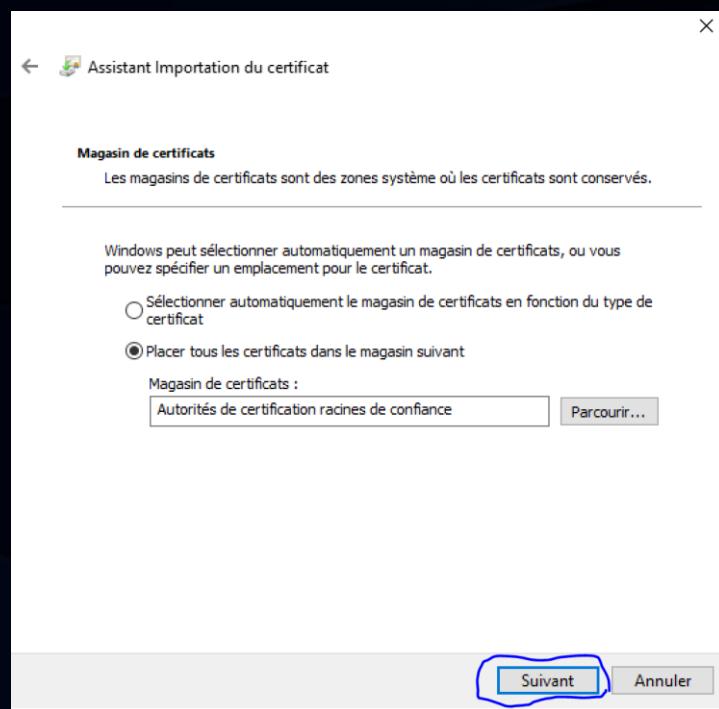
pfSense Portail Captif + LDAP

6-Installation du certificat côté client



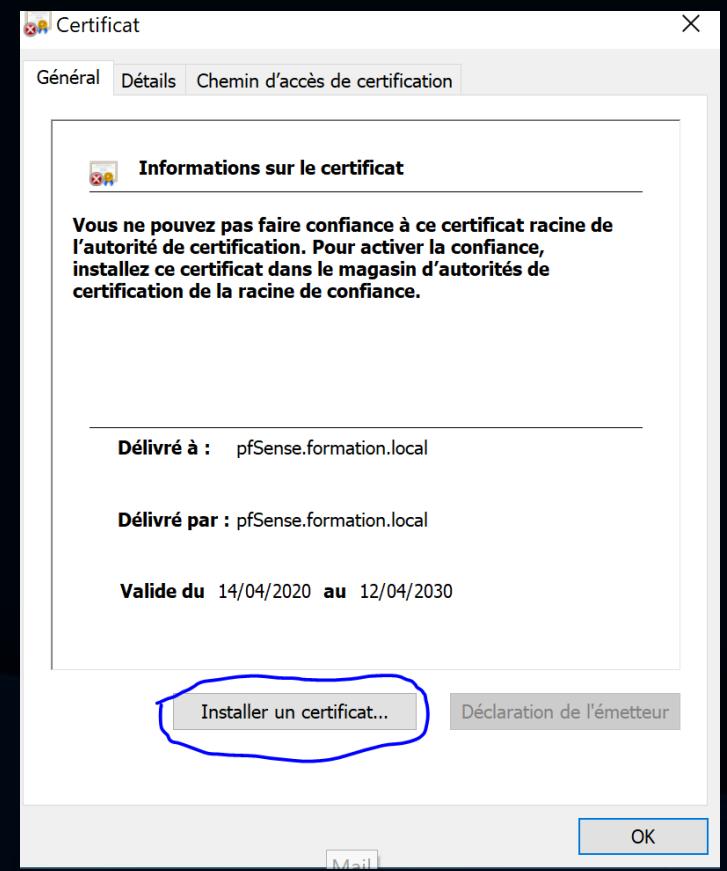
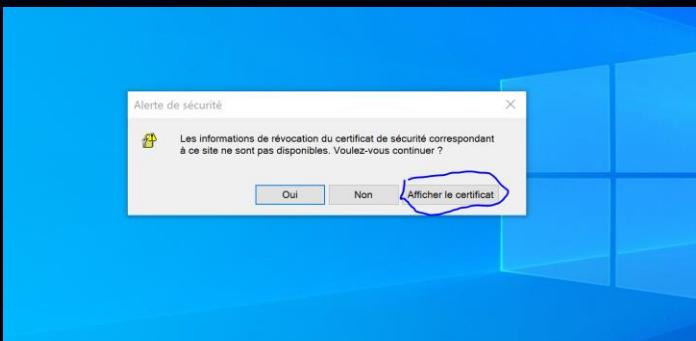
pfSense Portail Captif + LDAP

6-Installation du certificat côté client



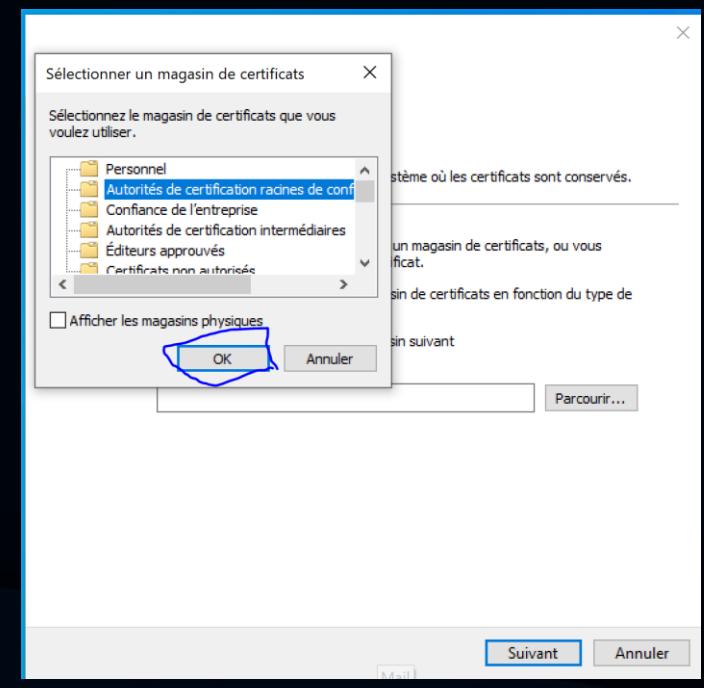
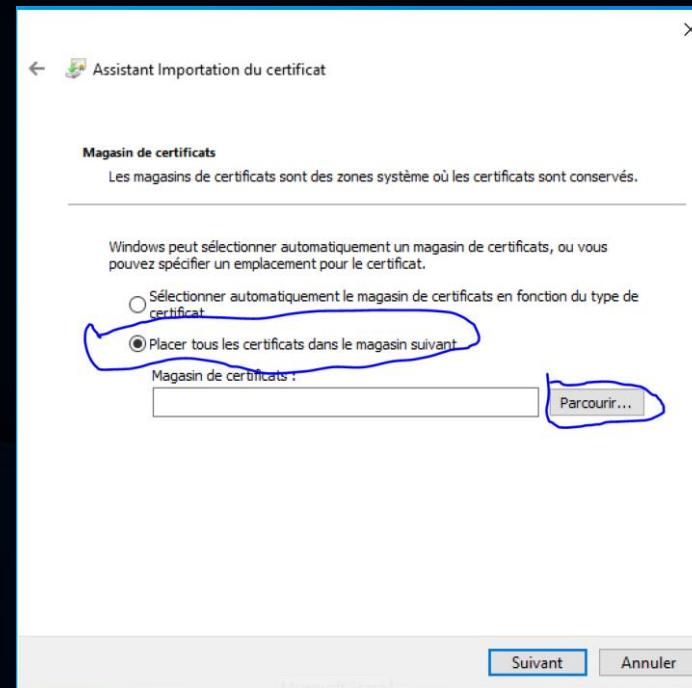
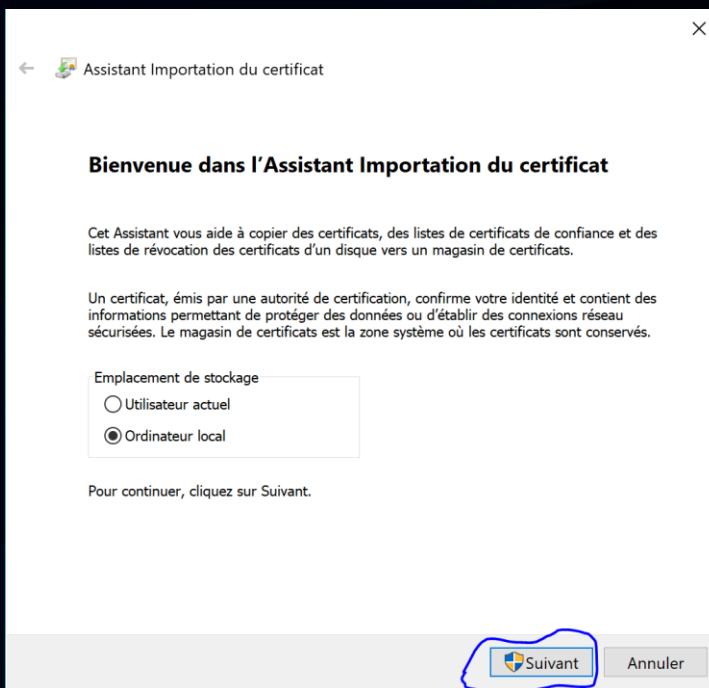
pfSense Portail Captif + LDAP

6-Installation du certificat côté client



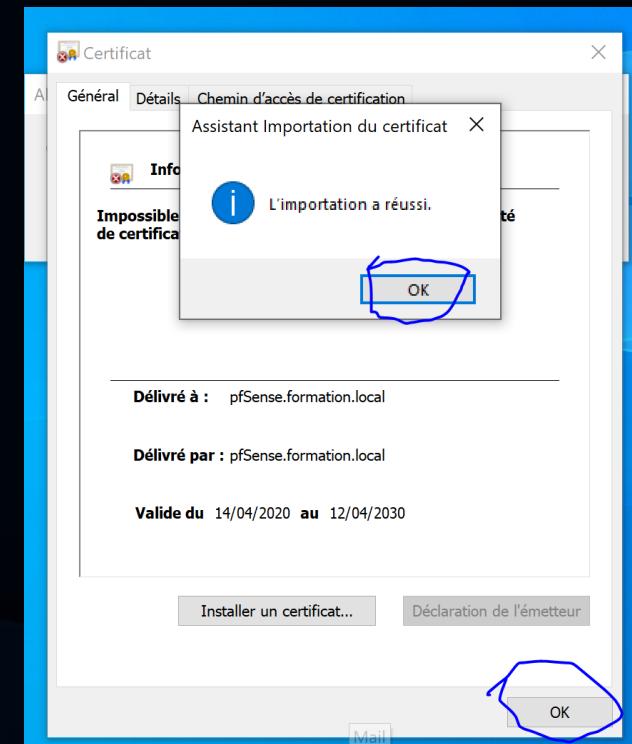
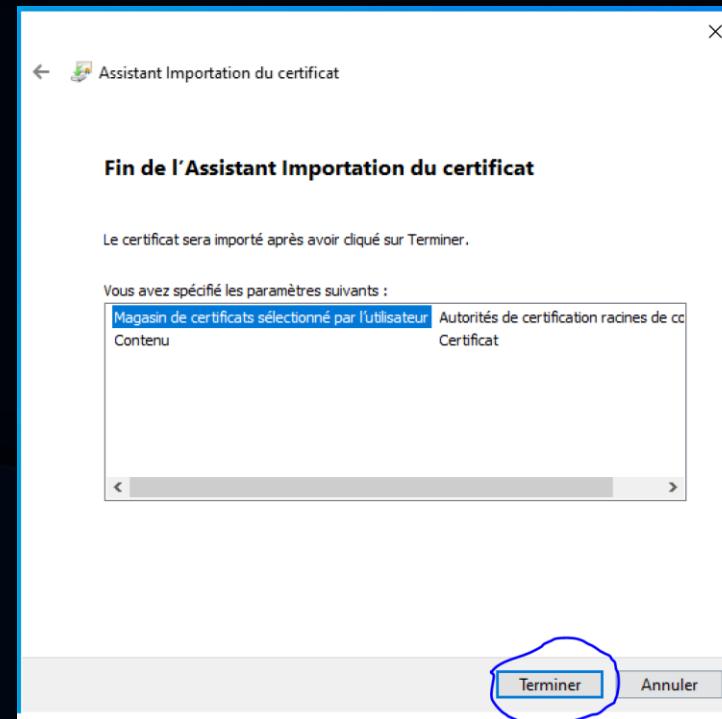
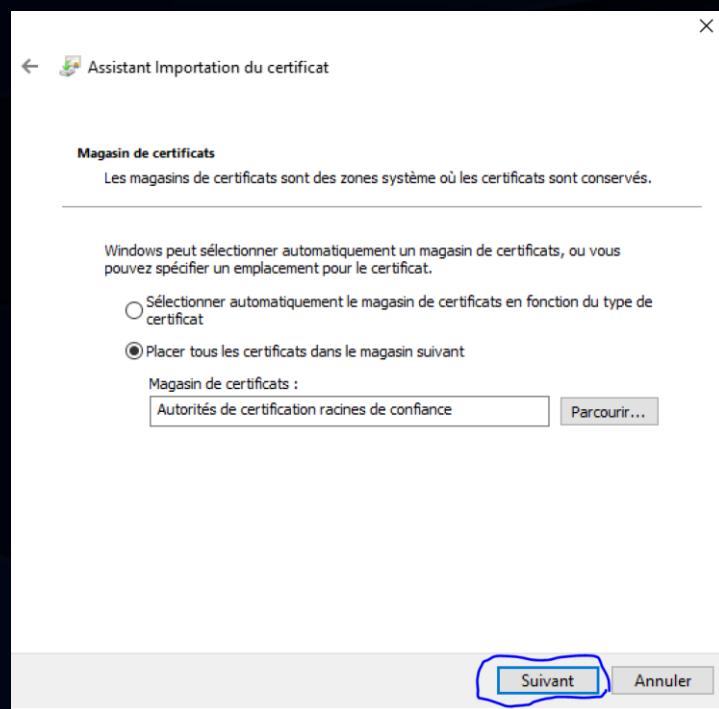
pfSense Portail Captif + LDAP

6-Installation du certificat côté client



pfSense Portail Captif + LDAP

6-Installation du certificat côté client



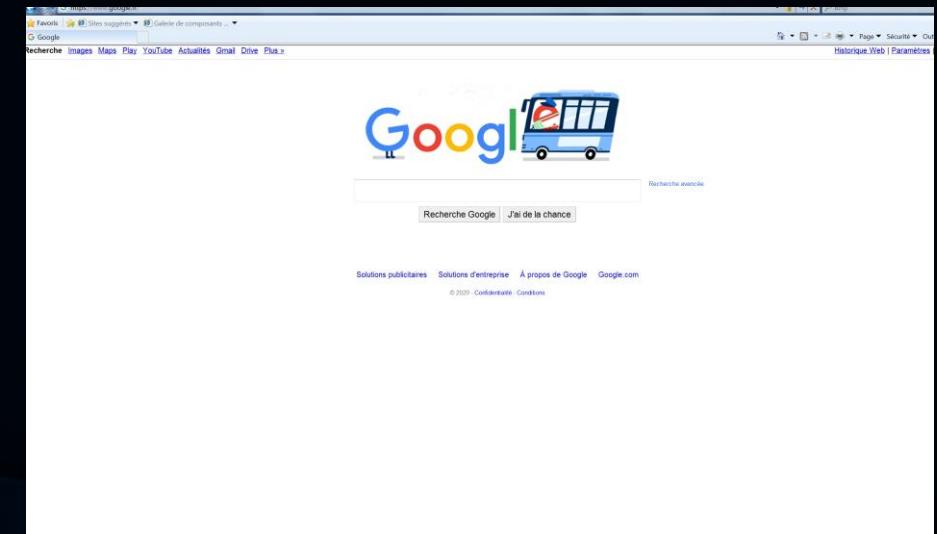
pfSense Portail Captif + LDAP



7-Tester via un navigateur Web

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

The screenshot shows a captive portal login interface. At the top is a WiFi icon. Below it is a form with two input fields: one for the username ('mikeali') and one for the password (represented by a series of asterisks). A blue 'Login' button is at the bottom. The page is framed by a white border.



Load Balancing - Failover

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