



pfSense

GUIDE D'INSTALLATION & CONFIGURATION

Réalisé par :
Thanina ZERGUINI
Mohand KELALI

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...). 😊

A 3D rectangular block, tilted slightly upwards and to the right, with the word "Firewall" written in white, bold, sans-serif font on its top surface. The block is dark blue with a white outline.

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

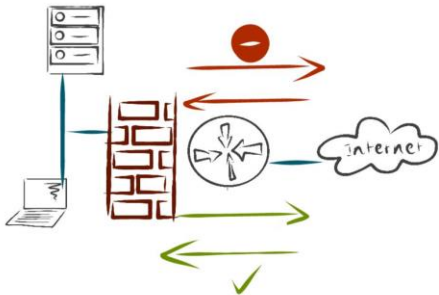
- Un firewall qui se base sur les couches 3 et 4 permet de contrôler les adresses IP et les ports, alors qu'un firewall qui se base sur la couche 7 permet de bloquer l'utilisation d'un logiciel.

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.

Architecture simple :

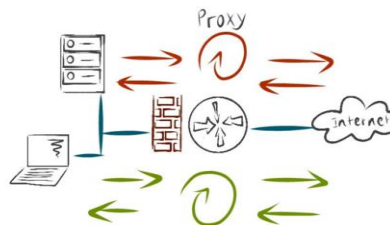
Le firewall est positionné entre le LAN et le WAN. Basée sur les couches réseau et transport et ne permet pas de filtrer au niveau applicatif.



Architectures Firewall

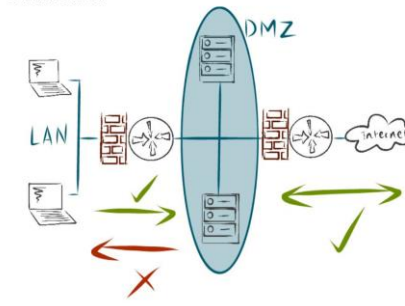
Architecture proxy :

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.



Zone dématérialisée :

La DMZ est une architecture qui permet de sécuriser un réseau local, que sera accessible sur Internet.



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.

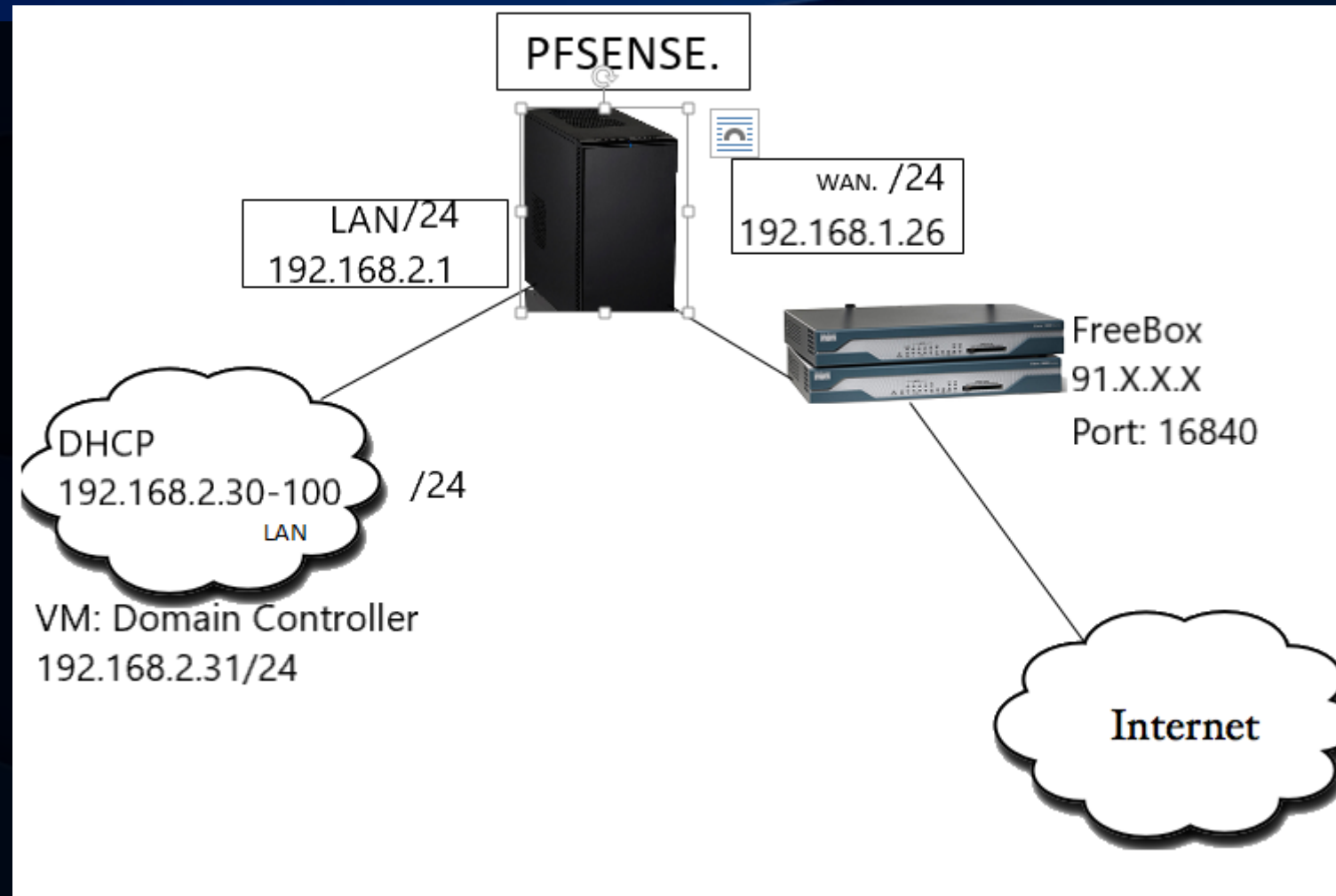
Scénarios de déploiement

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

Mode d'administration

- Console.
- WebGUI.

Schématiquement



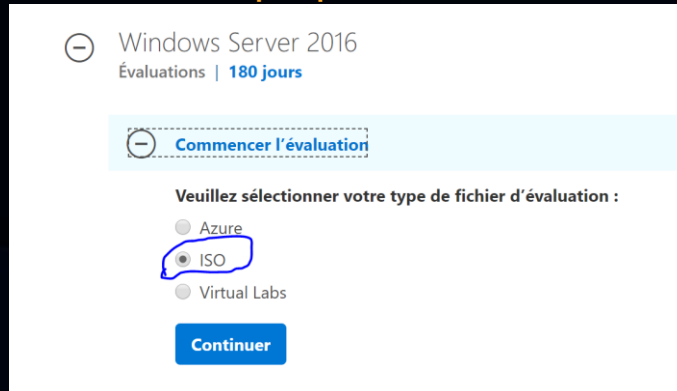
Domain Controller

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



Installation pfSense



1. ISO pfSense

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

Select Image To Download

Version: 2.4.5

Architecture: AMD64 (64-bit) ▼ ⓘ

Installer: CD Image (ISO) Installer ▼

Mirror: Frankfurt, Germany ▼

[Supported by netgate](#)

[SHA256 Checksum](#) for compressed (.gz) file:
fda93684669ad0b2b9e314a53d5c7272076484a6b714d60d5e06f14e1c7ce049

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



pfSense Installer

Copyright and distribution notice

pfSense is Copyright 2004-2019 Rubicon Communications, LLC (Netgate).

pfSense is a federally registered trademark of Electric Sheep Fencing, LLC. Any unauthorized use of this trademark is prohibited by state and federal law and international law. Refer to our Trademark Usage Guidelines for how to properly use the marks. All rights reserved.

Absolutely No Commercial Distribution Is Allowed.

<Accept>

pfSense Installer

Welcome

Welcome to pfSense!

Install

Rescue Shell

Recover config.xml

Install pfSense

Launch a shell for rescue operations

Recover config.xml from a previous install

< OK >

<Cancel>

Installation pfSense



```
pfSense Installer

Keymap Selection
The system console driver for pfSense defaults to standard "US"
keyboard map. Other keymaps can be chosen below.
( ) Czech (QWERTZ, accent keys)
( ) Danish
( ) Danish (accent keys)
( ) Danish (macbook)
( ) Dutch (accent keys)
( ) Estonian
( ) Finnish
( ) French
( ) French (accent keys)
( ) French Canadian (accent keys)
( ) French Dvorak-like
( ) French Dvorak-like (accent keys)
38%

[Select]      <Cancel>
[Press arrows, TAB or ENTER]
```

fr.kbd: French

```
pfSense Installer

Keymap Selection
The system console driver for pfSense defaults to standard "US"
keyboard map. Other keymaps can be chosen below.
>>> Continue with fr.kbd keymap
->- Test fr.kbd keymap
( ) Armenian phonetic layout
( ) Belarusian
( ) Belgian
( ) Belgian (accent keys)
( ) Brazilian (accent keys)
( ) Brazilian (without accent keys)
( ) Bulgarian (BBS)
( ) Bulgarian (Phonetic)
( ) Canadian Bilingual
( ) Central European
13%

[Select]      <Cancel>
[Press arrows, TAB or ENTER]
```

Installation pfSense



pfSense Installer

Partitioning

How would you like to partition your disk?

Auto (UFS)	Guided Disk Setup
Manual	Manual Disk Setup (experts)
Shell	Open a shell and partition by hand
Auto (ZFS)	Guided Root-on-ZFS

< **OK** > <Cancel>

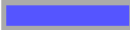
pfSense Installer

Archive Extraction

Extracting distribution files...

base.txz...

Overall Progress:

 42%

9817 files read @ 516.0 files/sec.

Installation pfSense



pfSense Installer

Manual Configuration

The installation is now finished.
Before exiting the installer, would
you like to open a shell in the new
system to make any final manual
modifications?

< Yes > **< No >**

10-Refresh Display

Reboot

This machine is about to be shut down.
After the machine has reached its
shutdown state, you may remove the CD
from the CD-ROM drive tray and press
Enter to reboot from the HDD.

< Reboot > < Return to Select Task >

Configuration pfSense



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

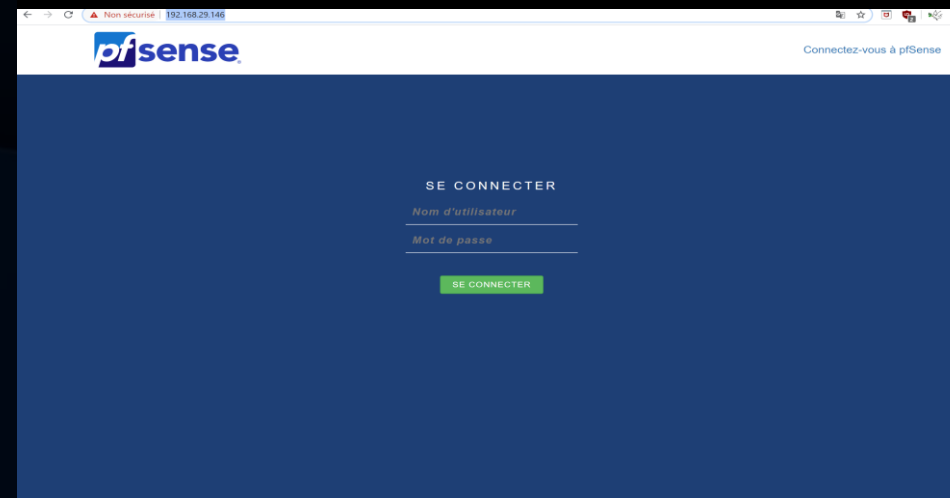
- Entrer le chiffre 8, pour activer le mode shell.
- Taper la commande suivante : `pfSsh.php playback enableallowallwan`
- Taper ensuite la commande : `exit`
- Ouvrir un navigateur web et taper le lien suivant sur la barre de recherche (@IP WAN pfSense): <https://192.168.1.26/>
- L'accès vers l'interface 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

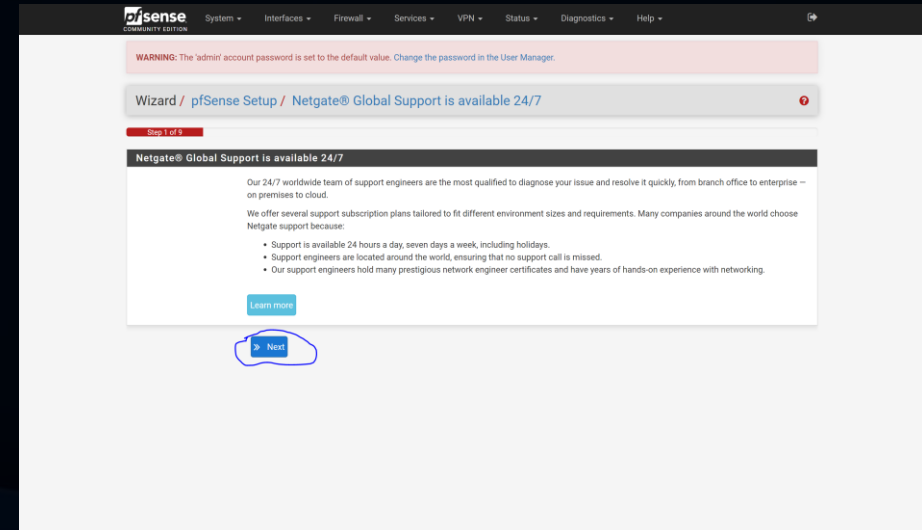
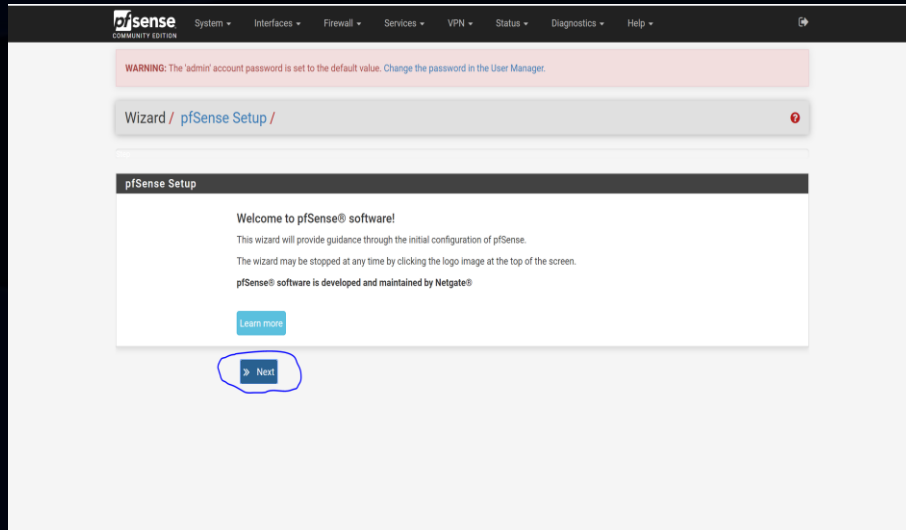
Enter an option: 8

[2.4.5-RELEASE][root@pfsense.localdomain]/root: pfS
pfSctl                               pfSense-upgrade
pfSense-dhclient-script pfSsh.php
[2.4.5-RELEASE][root@pfsense.localdomain]/root: pfSsh.php playback enableallowallwan
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[3621]: /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



Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname:
EXAMPLE: myserver

Domain:
EXAMPLE: mydomain.com

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.

Primary DNS Server:

Secondary DNS Server:

Override DNS: ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

[Next](#)

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname:
Enter the hostname (FQDN) of the time server.

Timezone:

[Next](#)

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: xxxxxxxxxx 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).

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

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

Subnet Mask

[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

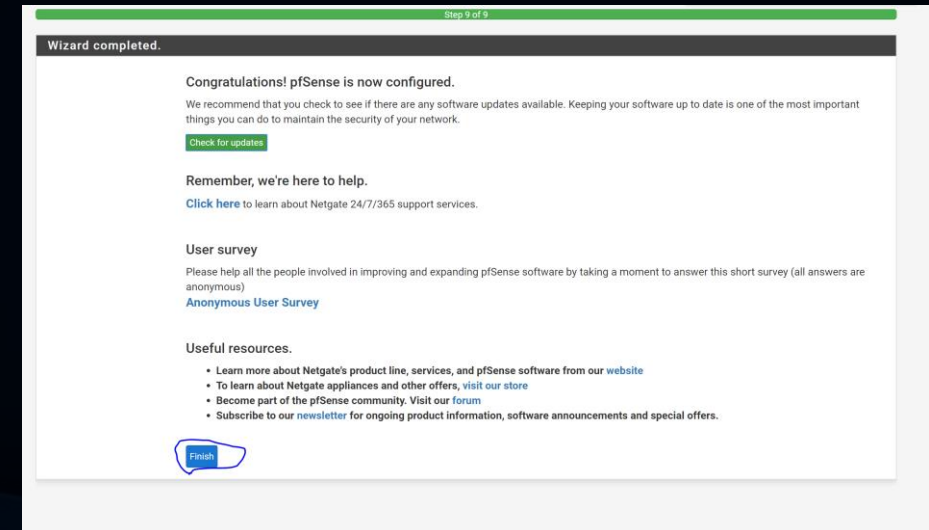
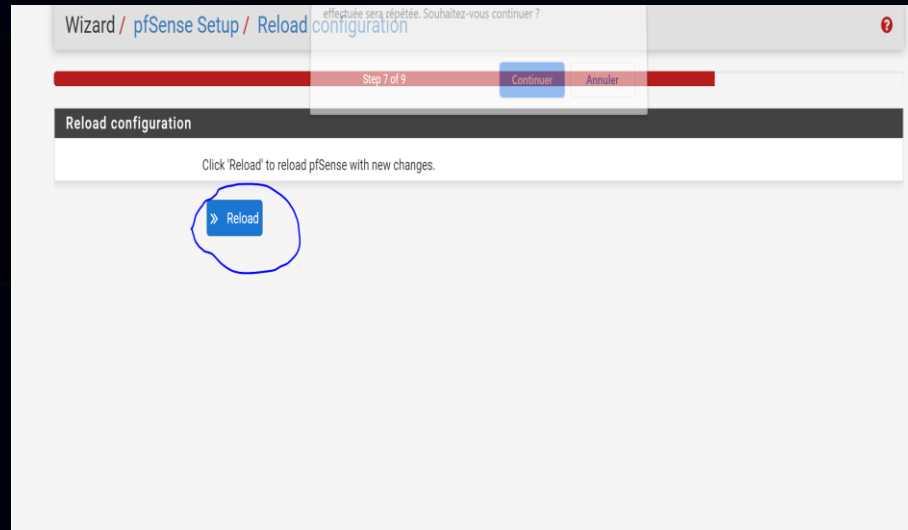
On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password

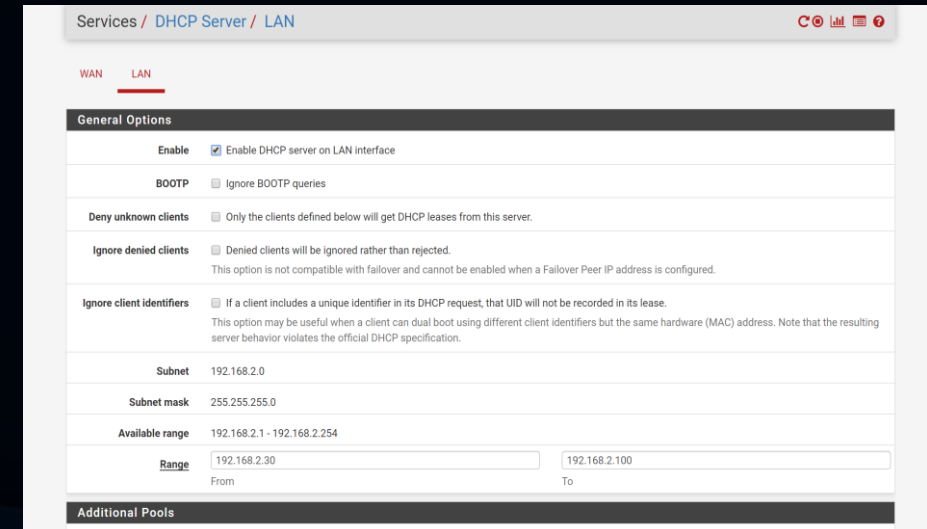
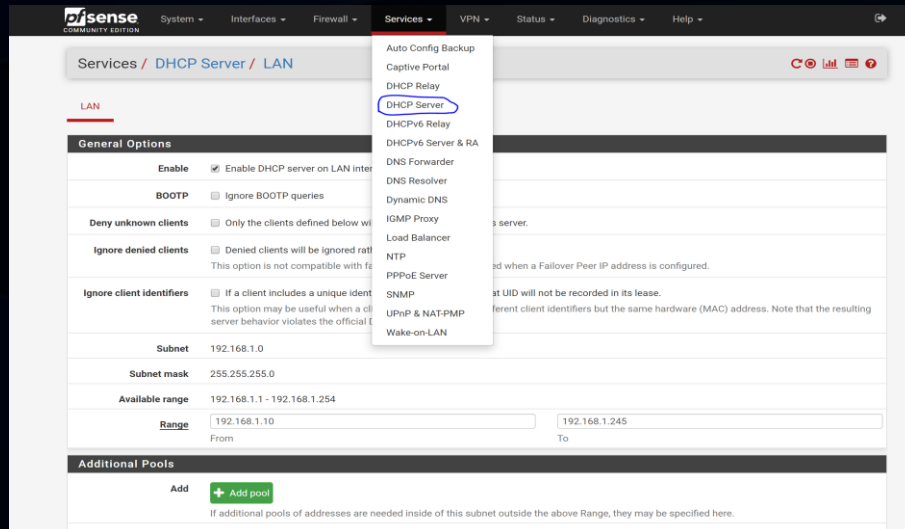
Admin Password AGAIN

[Next](#)

Configuration pfSense



pfSense DHCP Server



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

pfSense DHCP Server



Servers

WINS servers

WINS Server 1

WINS Server 2

DNS servers

192.168.2.1

DNS Server 2

DNS Server 3

DNS Server 4

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

192.168.2.1

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

formation.local

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 dhcpd sends a ping to the address being assigned, and if no response has been heard, it assigns the address. Enabled by default.

Dynamic DNS

Display Advanced

MAC address control

Display Advanced

NTP

Display Advanced

TFTP

Display Advanced

LDAP

Display Advanced

Network Booting

Display Advanced

Additional BOOTP/DHCP Options

Display Advanced

Save

DHCP Static Mappings for this Interface

Static ARP	MAC address	IP address	Hostname	Description
<div>+ Add</div>				

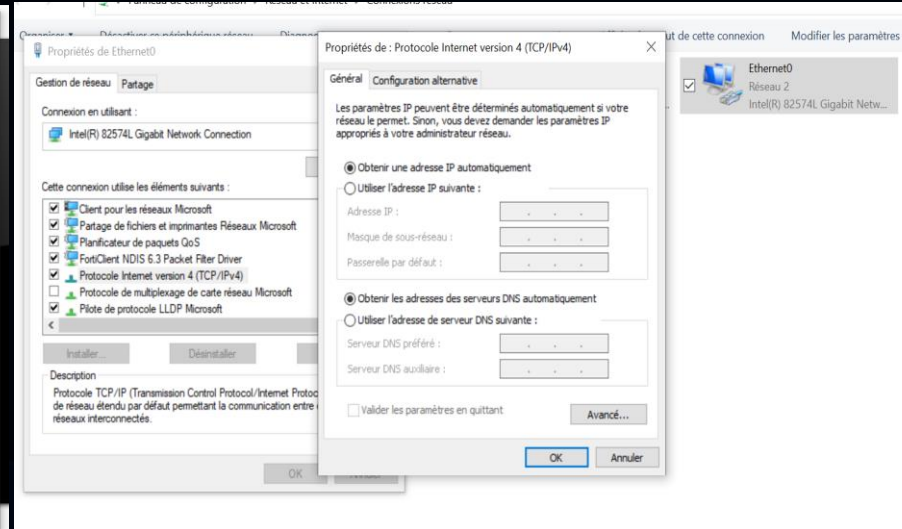
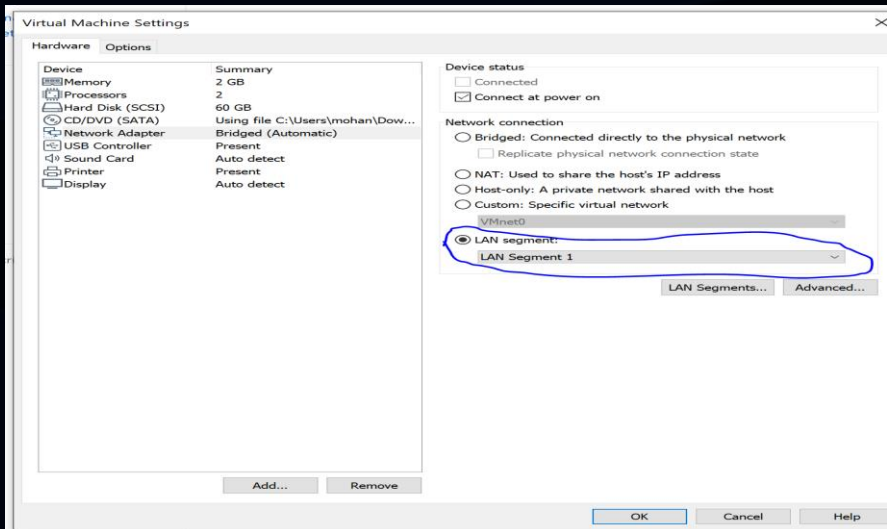
@IP serveur DNS : 192.168.2.1-> pfSense LAN

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.

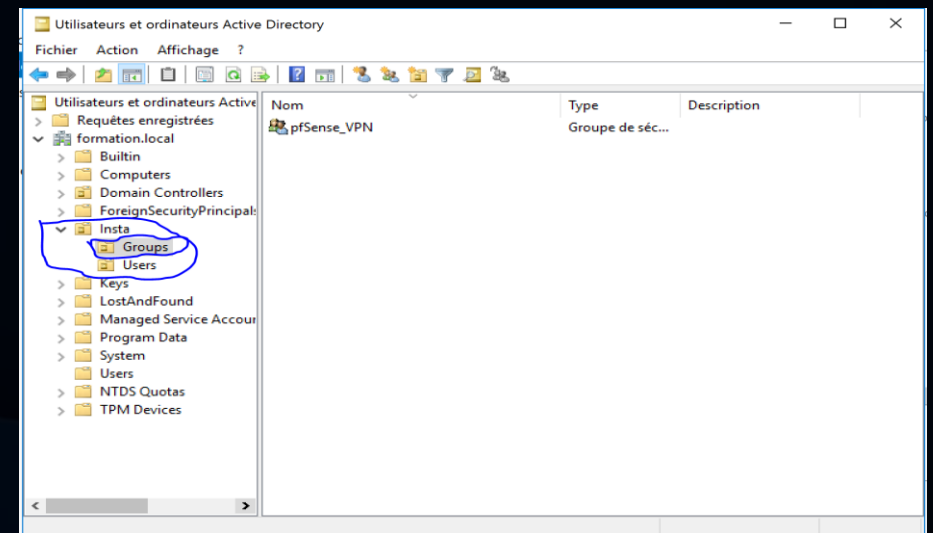
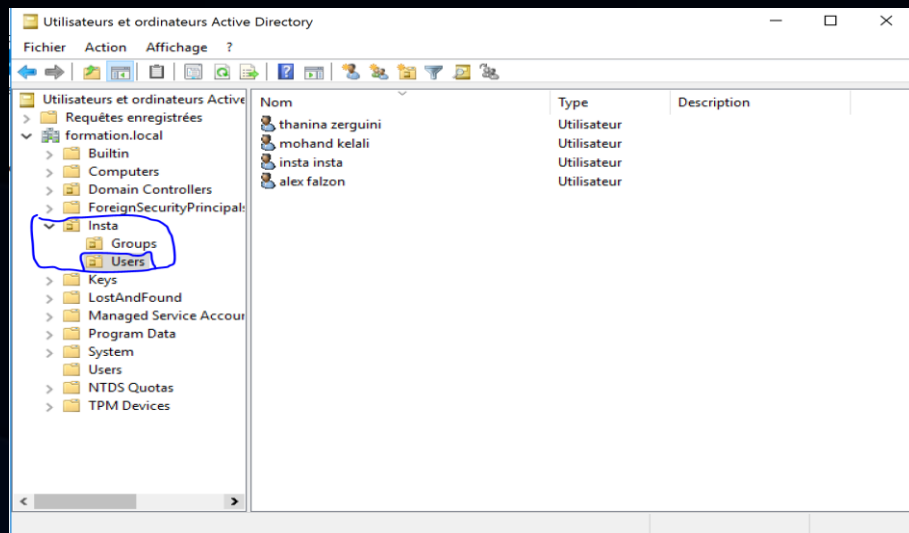
A faire :

- 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.



Intégration avec LDAP

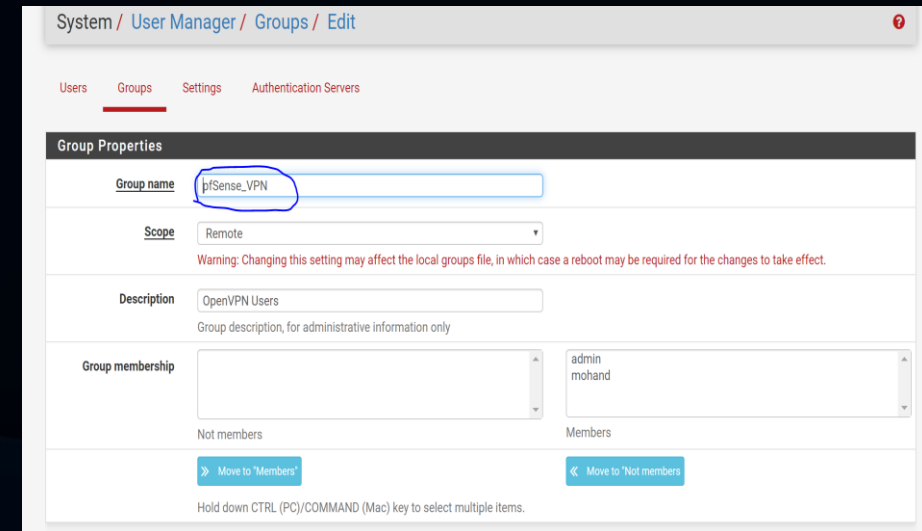
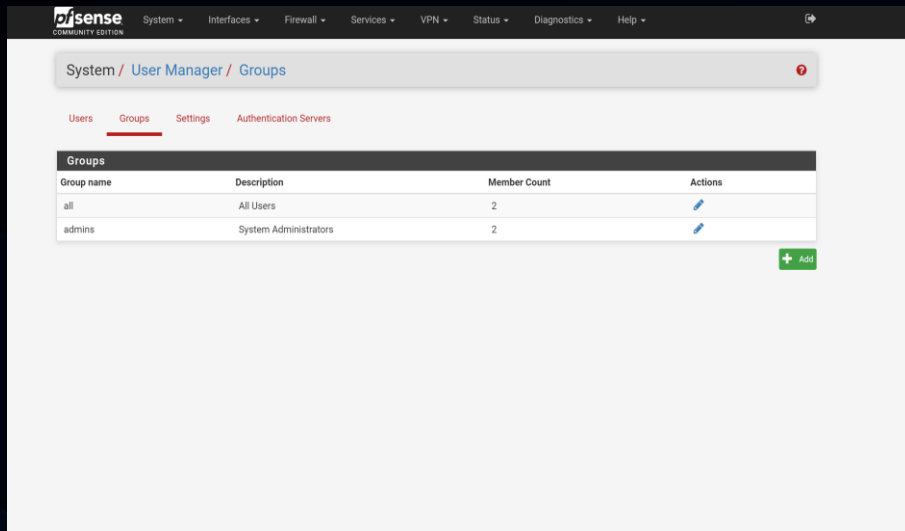
- OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel.
- L'objectif c'est de réaliser une connexion OpenVPN via un compte AD.



A partir de l'active directory :

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

Intégration avec LDAP

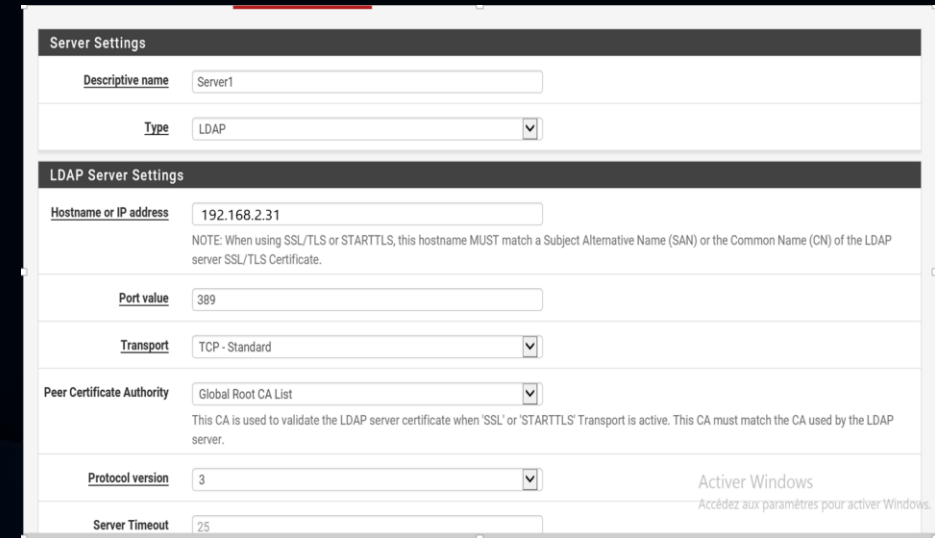
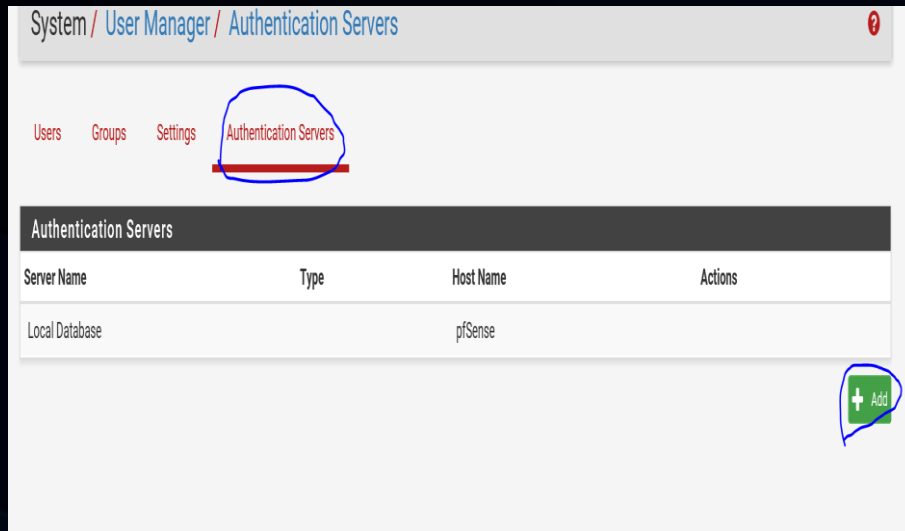


A partir de l'interface WebGUI :

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

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).



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

Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component.
Example: CN=Users,DC=example,DC=com or OU=Staff,OU=Freelancers

Extended query

☒ Enable extended query

Query

memberOf=CN=pfSense_VPN,OU=Groups,OU=Insta,DC=formation,DC=

Example: memberOf=CN=Groupname,OU=MyGroups,DC=example,DC=com

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
RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).

Group Object Class

posixGroup

Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

UTF8 Encode

☒ UTF8 encode LDAP parameters before sending them to the server.
Required to support international characters, but may not be supported by every LDAP 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
RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).

Group Object Class

posixGroup

Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

UTF8 Encode

☐ UTF8 encode LDAP parameters before sending them to the server.
Required to support international characters, but may not be supported by every LDAP server.

Username Alterations

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

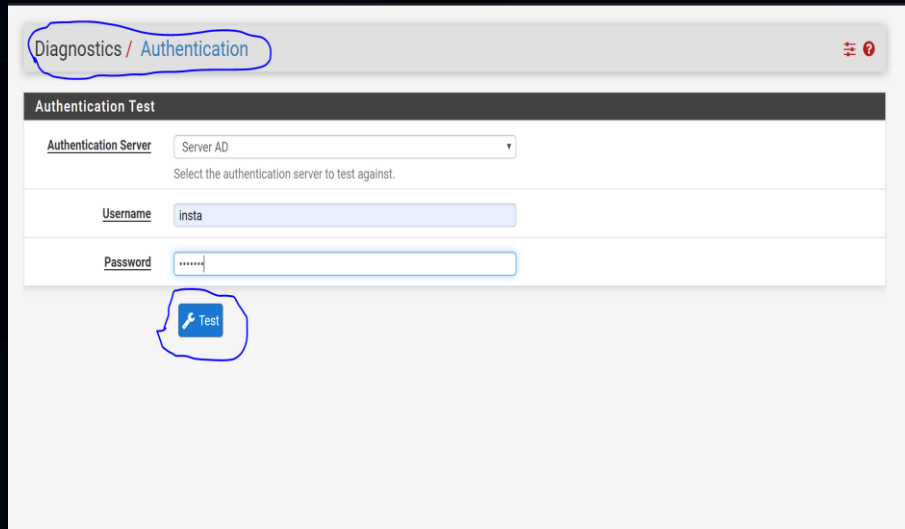
Could not connect to the LDAP server. Please check the LDAP configuration.

Save

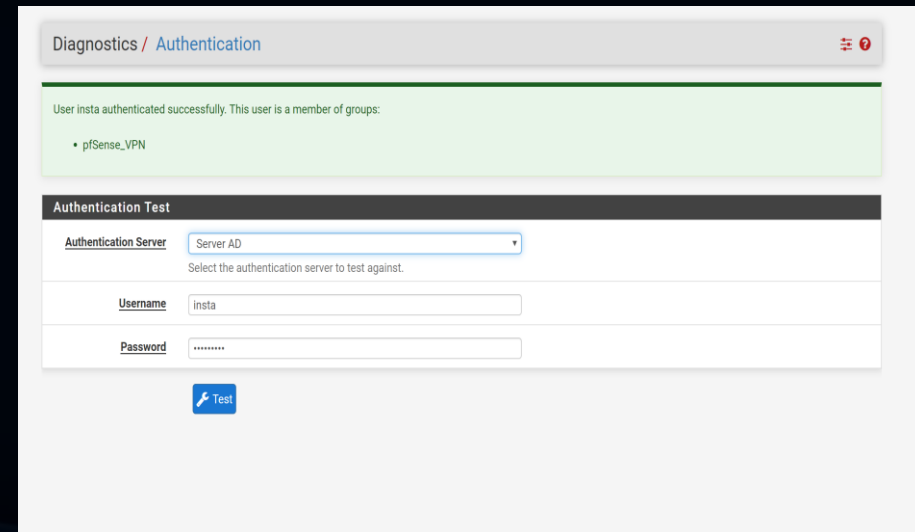
Activer Windows
Accédez aux paramètres pour activer Windows

- 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.

Tester la connexion LDAP



The screenshot shows the 'Diagnostics / Authentication' page in pfSense. The 'Authentication Test' section is active. The 'Authentication Server' dropdown is set to 'Server AD'. The 'Username' field contains 'insta' and the 'Password' field contains masked characters. A blue circle highlights the 'Test' button at the bottom.

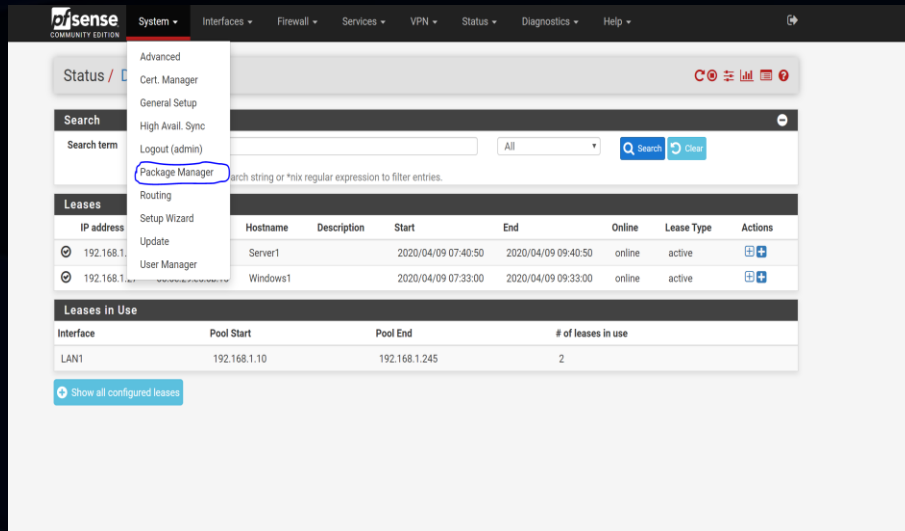


The screenshot shows the same 'Diagnostics / Authentication' page after a successful test. A green message box at the top states: 'User insta authenticated successfully. This user is a member of groups: • pfSense_VPN'. The 'Authentication Test' form below remains the same, but the 'Test' button is no longer highlighted.

A faire :

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

Installer le package OpenVPN



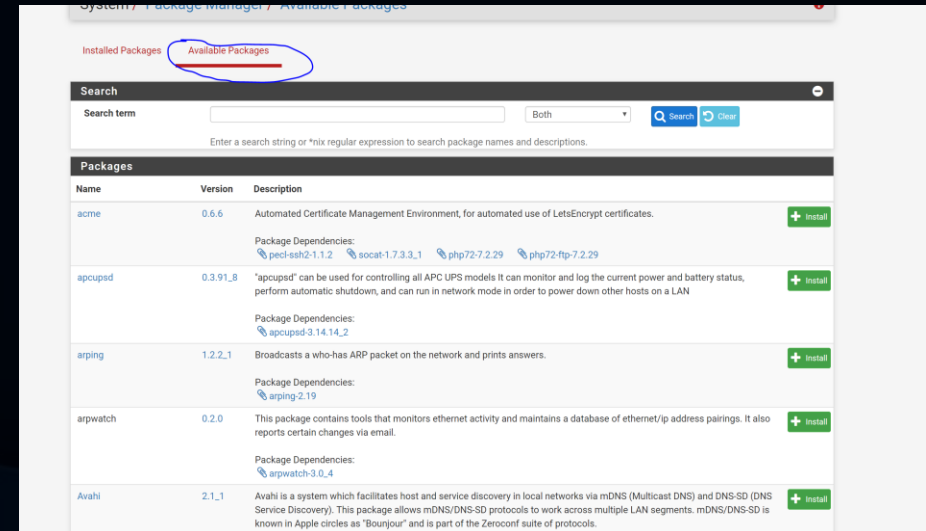
The screenshot shows the pfSense web interface. The 'System' menu is open, and 'Package Manager' is highlighted. The left sidebar shows 'Status / System' selected. The main content area displays a table of leases.

Hostname	Description	Start	End	Online	Lease Type	Actions
Server1		2020/04/09 07:40:50	2020/04/09 09:40:50	online	active	[+]
Windows1		2020/04/09 07:33:00	2020/04/09 09:33:00	online	active	[+]

Below the leases table, there is a section for 'Leases in Use' with columns: Interface, Pool Start, Pool End, and # of leases in use.

Interface	Pool Start	Pool End	# of leases in use
LAN1	192.168.1.10	192.168.1.245	2

A button 'Show all configured leases' is located at the bottom left of the leases section.

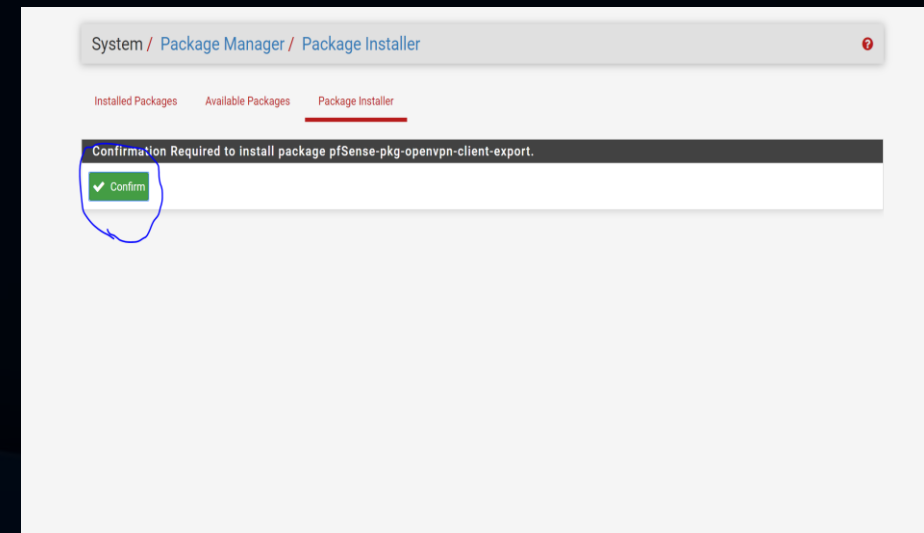


The screenshot shows the 'Available Packages' page in the pfSense Package Manager. The 'Available Packages' tab is selected. The page includes a search bar and a table of available packages.

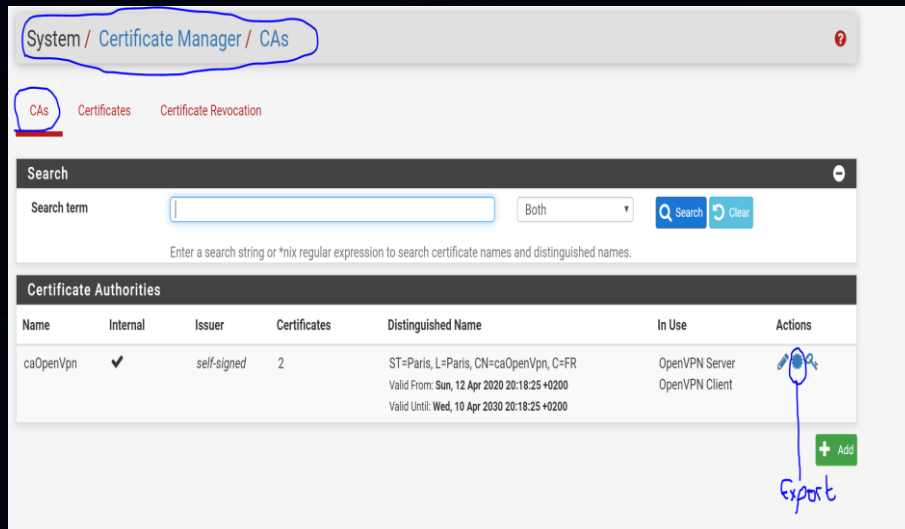
Name	Version	Description	Actions
acme	0.6.6	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates.	[+ Install]
apcupsd	0.3.91.8	'apcupsd' can be used for controlling all APC UPS models. It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN.	[+ Install]
arping	1.2.2.1	Broadcasts a who-has ARP packet on the network and prints answers.	[+ Install]
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.	[+ Install]
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.	[+ Install]

Installer le package OpenVPN

ntopng	0.8.13_3	ntopng (replaces ntop) is a network probe that shows network usage in a way similar to what top does for processes. In interactive mode, it displays the network status on the user's terminal. In Web mode it acts as a Web server, creating an HTML dump of the network status. It sports a NetFlow/sFlow emitter/collector, an HTTP-based client interface for creating ntop-centric monitoring applications, and RRD for persistently storing traffic statistics.	+ install
Package Dependencies: webfonts-0.30_14 ntopng-3.8.d20191111,1 libmaxminddb-1.4.2 graphviz-2.42.2_3 redis-5.0.7_2 gdbm-1.18.1_1			
nut	2.7.4_7	Network UPS Tools provides support for monitoring of Uninterruptible Power Supplies. It supports UPS units attached locally via USB or serial, and remote units via the SNMP protocol, the APCUPSD protocol or the NUT protocol.	+ install
Package Dependencies: nut-2.7.4_13			
Open-VM-Tools	10.1.0.2_1	VMware Tools is a suite of utilities that enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine.	+ install
Package Dependencies: open-vm-tools-nox11-11.0.1_2.2			
OpenBGPD	0.11_11	OpenBGPD is a free implementation of the Border Gateway Protocol, version 4. It allows ordinary machines to be used as routers exchanging routes with other systems speaking the BGP protocol. Conflicts with Quagga_OSPF and FRR, these packages cannot be installed at the same time.	+ install
Package Dependencies: openbgpd-5.2.20121209_3,1			
openvpn-client-export	1.4.21	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.	+ install
Package Dependencies: openvpn-client-export-2.4.8 openvpn-2.4.8 zip-3.0_1 p7zip-16.02_2			
pfBlockerNG	2.1.4_22	pfBlockerNG is the Next Generation of pfBlocker. Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats. GeoIP database by MaxMind Inc. (GeoLite2 Free version). De-Duplication, Suppression, and Reputation enhancements. Provision to download from diverse List formats. Advanced integration for Proofpoint ET IQRisk IP Reputation Threat Sources. Domain Name (DNSBL) blocking via Unbound DNS Resolver.	+ install
Package Dependencies: libnet-1.4.5_4 libidn2-2.3.17 libmaxminddb-1.4.2 openvpn-2.4.8 quagga-1.6.1 open77-7.7.39			

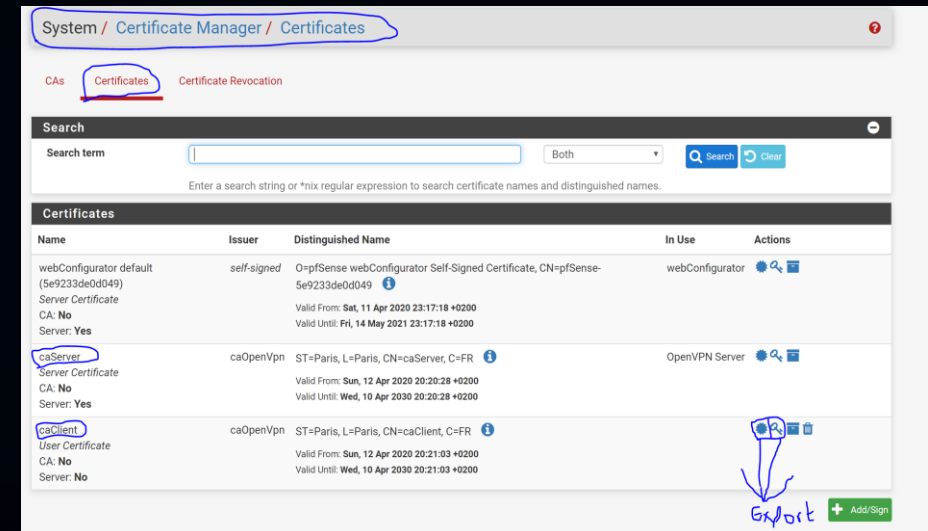


Générer les certificats



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	Export

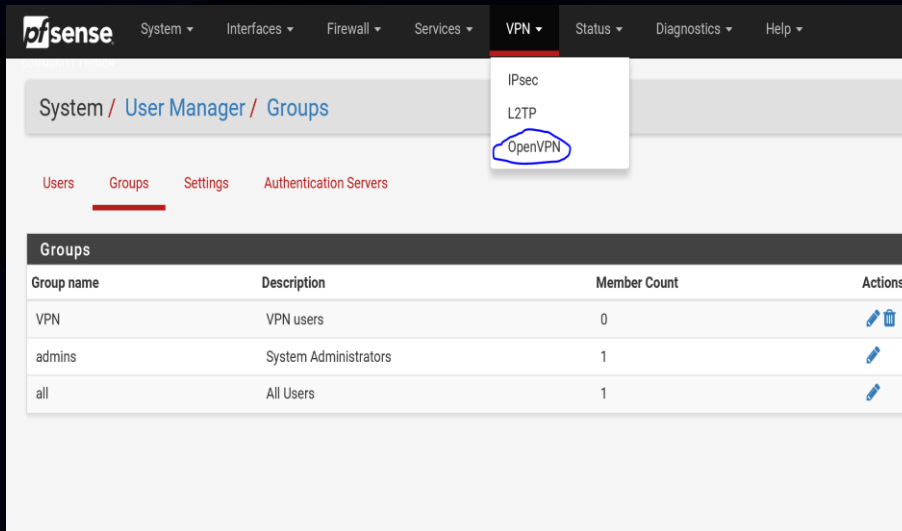
- Créer un certificat d'autorité et l'exporter par la suite.







Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (5e9233de0d049) Server Certificate CA: No Server: Yes	self-signed	OpenSense webConfigurator Self-Signed Certificate, CN=pfSense-5e9233de0d049 Valid From: Sat, 11 Apr 2020 23:17:18 +0200 Valid Until: Fri, 14 May 2021 23:17:18 +0200	webConfigurator	Export
caServer Server Certificate CA: No Server: Yes	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	OpenVPN Server	Export
caClient User Certificate CA: No Server: No	caOpenVpn	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		Export

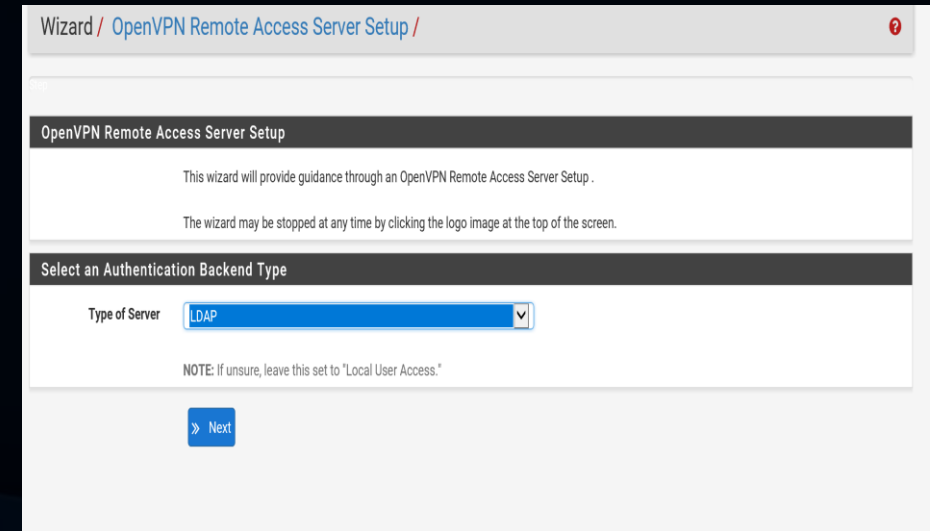
- Créer un certificat pour les clients et un autre pour le serveur OpenVPN.
- Exporter la clé publique et privée du client.

Créer un tunnel VPN



The screenshot shows the pfSense web interface. The top navigation bar includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The VPN menu is open, showing options for IPsec, L2TP, and OpenVPN (which is circled in blue). Below the navigation bar, the breadcrumb trail is System / User Manager / Groups. The main content area shows the 'Groups' tab selected, with a table listing existing groups.

Group name	Description	Member Count	Actions
VPN	VPN users	0	 
admins	System Administrators	1	
all	All Users	1	



The screenshot shows the 'OpenVPN Remote Access Server Setup' wizard in pfSense. The breadcrumb trail is Wizard / OpenVPN Remote Access Server Setup. The wizard provides guidance on setting up an OpenVPN Remote Access Server. It includes a note that the wizard can be stopped at any time by clicking the logo image at the top of the screen. The 'Select an Authentication Backend Type' section shows a dropdown menu for 'Type of Server' set to 'LDAP'. A note below the dropdown states: 'NOTE: If unsure, leave this set to "Local User Access."' A 'Next' button is visible at the bottom.

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

Créer un tunnel VPN

Wizard / OpenVPN Remote Access Server Setup / Server Setup

Step 9 of 11

Server Setup

OpenVPN Remote Access Server Setup 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	1194
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	
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	<input checked="" type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
Redirect IPv6 Gateway	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
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. 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	
Specify the maximum number of clients allowed to concurrently connect to this server.	
Compression	Omit Preference (Use OpenVPN Default)
Compress tunnel packets using the LZO 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 Setup 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

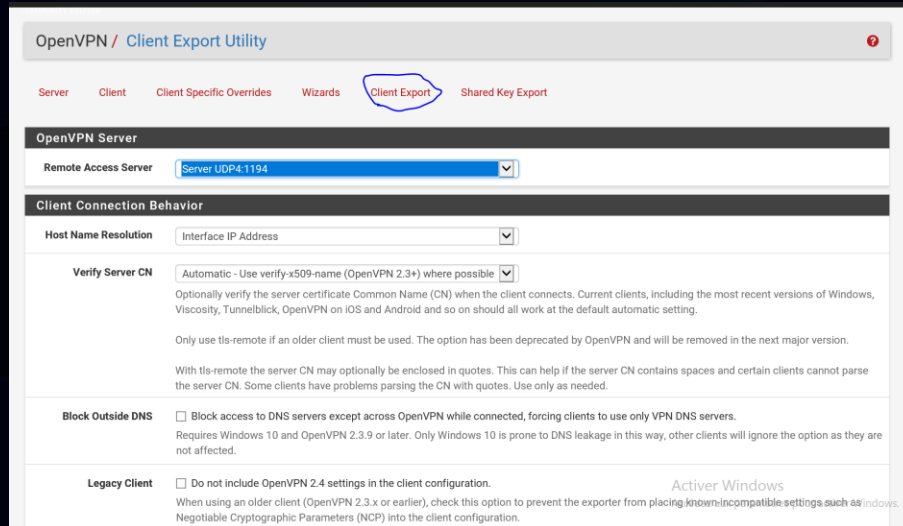
Firewall Rule	<input checked="" type="checkbox"/>
Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.	

Traffic from clients through VPN

OpenVPN rule	<input checked="" type="checkbox"/>
Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.	

Next

OpenVPN client



OpenVPN / Client Export Utility

Server Client Client Specific Overrides Wizards **Client Export** Shared Key Export

OpenVPN Server

Remote Access Server: Server UDP4:1194

Client Connection Behavior

Host Name Resolution: Interface IP Address

Verify Server CN

Automatic - Use verify-x509-name (OpenVPN 2.3+) where possible ☒

Optionally verify the server certificate Common Name (CN) when the client connects. Current clients, including the most recent versions of Windows, Viscosity, Tunnelblick, OpenVPN on iOS and Android and so on should all work at the default automatic setting.

Only use tls-remote if an older client must be used. The option has been deprecated by OpenVPN and will be removed in the next major version.

With tls-remote the server CN may optionally be enclosed in quotes. This can help if the server CN contains spaces and certain clients cannot parse the server CN. Some clients have problems parsing the CN with quotes. Use only as needed.

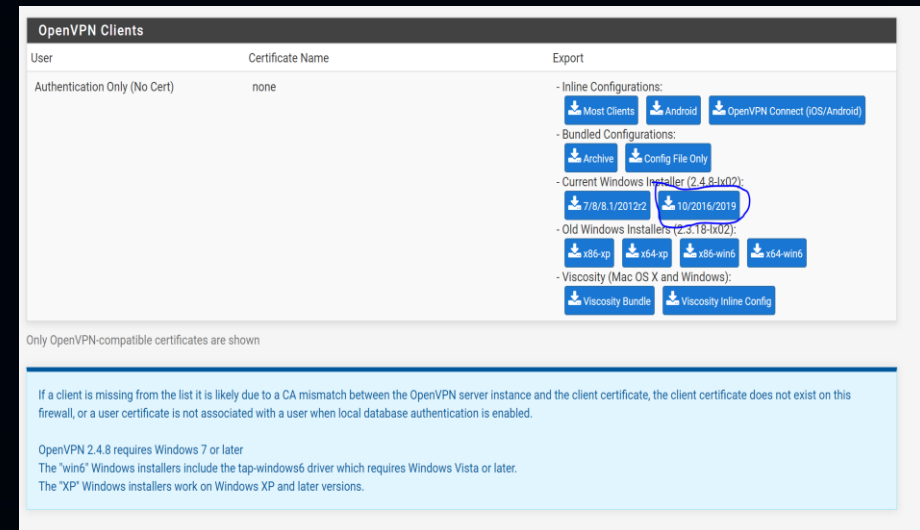
Block Outside DNS

☐ Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Legacy Client

☐ Do not include OpenVPN 2.4 settings in the client configuration. When using an older client (OpenVPN 2.3.x or earlier), check this option to prevent the exporter from placing known-incompatible settings such as Windows Negotiable Cryptographic Parameters (NCP) into the client configuration.

Active Windows



OpenVPN Clients

User	Certificate Name	Export
Authentication Only (No Cert)	none	<p>- Inline Configurations:</p> <p>Most Clients Android OpenVPN Connect (iOS/Android)</p> <p>- Bundled Configurations:</p> <p>Archive Config File Only</p> <p>- Current Windows Installers (2.4.8-ix02):</p> <p>7/8.1/2012-2 10/2016/2019</p> <p>- Old Windows Installers (2.3.18-ix02):</p> <p>x86-xp x64-xp x86-win6 x64-win6</p> <p>- Viscosity (Mac OS X and Windows):</p> <p>Viscosity Bundle Viscosity Inline Config</p>

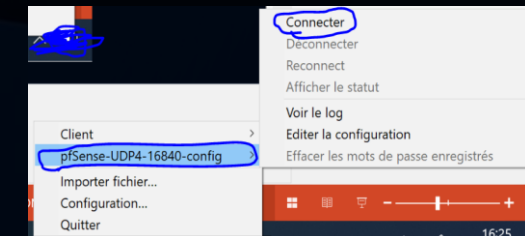
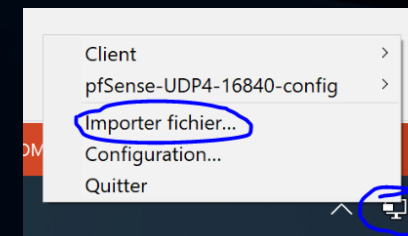
Only OpenVPN-compatible certificates are shown

If a client is missing from the list it is likely due to a CA mismatch between the OpenVPN server instance and the client certificate, the client certificate does not exist on this firewall, or a user certificate is not associated with a user when local database authentication is enabled.

OpenVPN 2.4.8 requires Windows 7 or later
The "win6" Windows installers include the tap-windows6 driver which requires Windows Vista or later.
The "XP" Windows installers work on Windows XP and later versions.

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 ☺ .



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

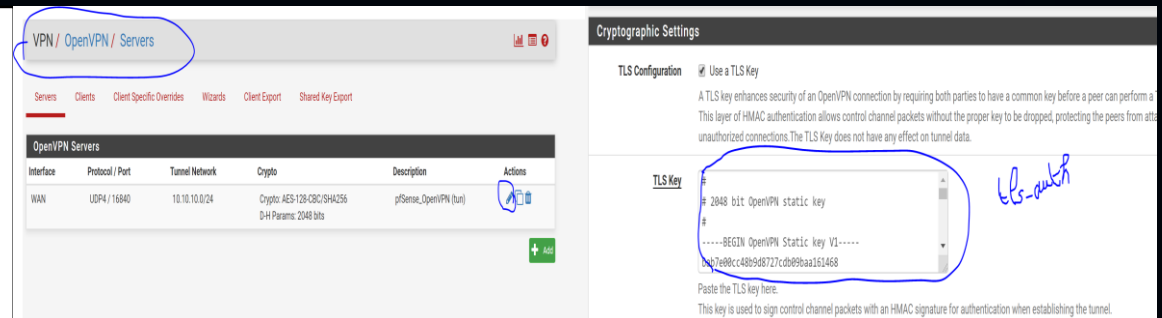
```
</cert>
```

```
<key>
```

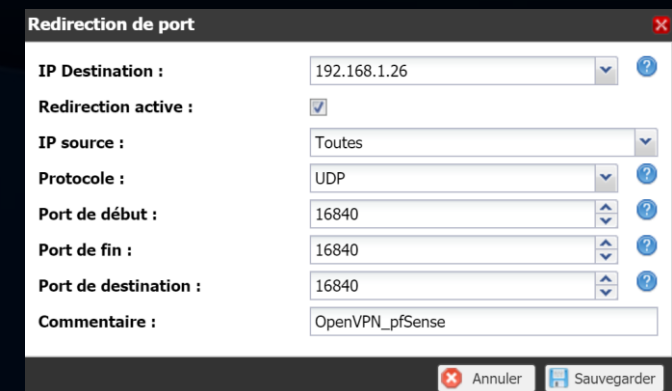
Contenu du fichier Client.key

```
</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

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 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 [Add pool](#)

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

Servers

WINS servers WINS Server 1 WINS Server 2

DNS servers 192.168.2.1 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 pfSense.format.local none

Address Hostname Gateway

2-Vérifier que le DNS Resolver est activé

Services / DNS Resolver / General Settings

General Settings Advanced Settings Access Lists

General DNS Resolver Options

Enable ☒ Enable DNS resolver

Listen Port 53

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

Enable SSL/TLS Service ☐ Respond to incoming SSL/TLS queries from local clients

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

SSL/TLS Certificate webConfigurator default (5e9233de0d049)

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

SSL/TLS Listen Port 853

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

Host Overrides

Host	Parent domain of host	IP to return for host	Description	Actions
pfSense	formation.local	192.168.2.1		edit delete

Enter 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.

[Add](#)

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

pfSense Portail Captif + LDAP



4-Création de certificats

System / Certificate Manager / CAs

CA's Certificates Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

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 2020 20:18:25 +0200	OpenVPN Server OpenVPN Client	
ca_portail	✓	self-signed	1	ST=Paris, L=Paris, CN=pfSense.formation.local, C=FR Valid From: Tue, 14 Apr 2020 00:12:47 +0200 Valid Until: Fri, 12 Apr 2020 00:12:47 +0200		

+ Add

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

System / Certificate Manager / Certificates

CA's Certificates Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (SelfSigned)	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense- SelfSigned0049 Valid From: Sat, 11 Apr 2020 22:17:18 +0200 Valid Until: Fri, 14 May 2021 22:17:18 +0200	webConfigurator	
caServer Server Certificate	caOpenVpn	ST=Paris, L=Paris, CN=caServer, C=FR Valid From: Sun, 12 Apr 2020 20:20:28 +0200 Valid Until: Wed, 10 Apr 2020 20:20:28 +0200	OpenVPN Server	
caClient User Certificate	caOpenVpn	ST=Paris, L=Paris, CN=caClient, C=FR Valid From: Sun, 12 Apr 2020 20:21:03 +0200 Valid Until: Wed, 10 Apr 2020 20:21:03 +0200		
ca_portail Server Certificate	ca_portail	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 2020 00:15:46 +0200	Captive Portal	

+ Add/Sign

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

Status / Dashboard

System Information

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
+ Add				

Services / Captive Portal / Add Zone

Add Captive Portal Zone

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

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

[Save & Continue](#)


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).

 Save

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
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 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.

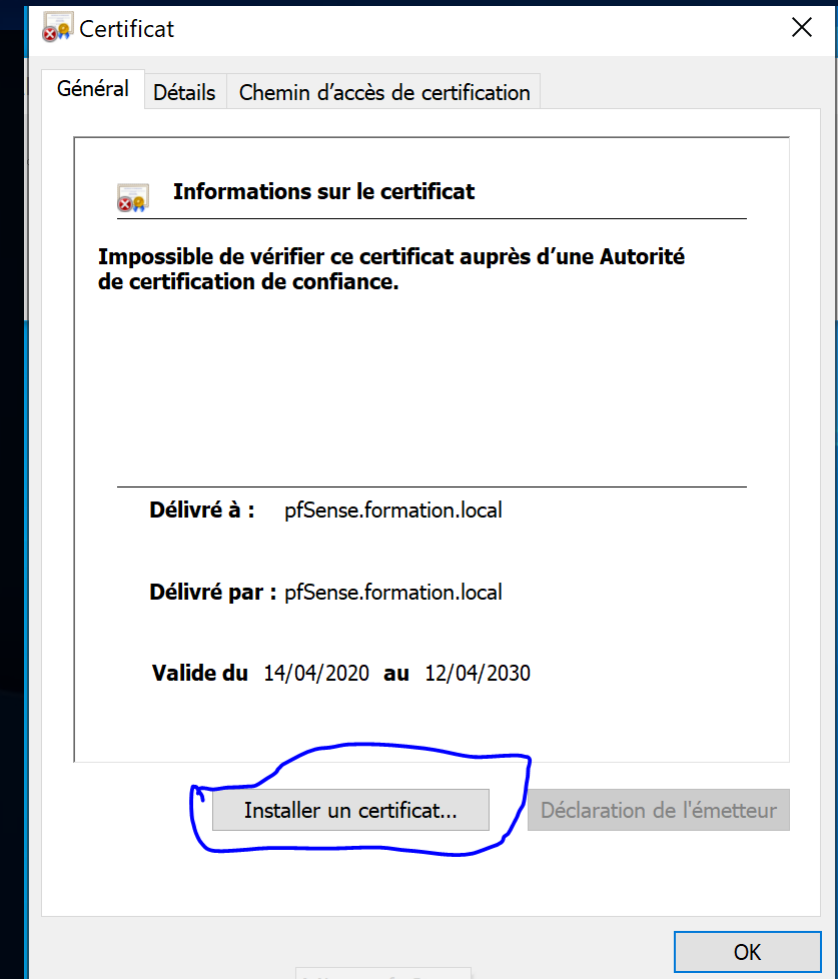
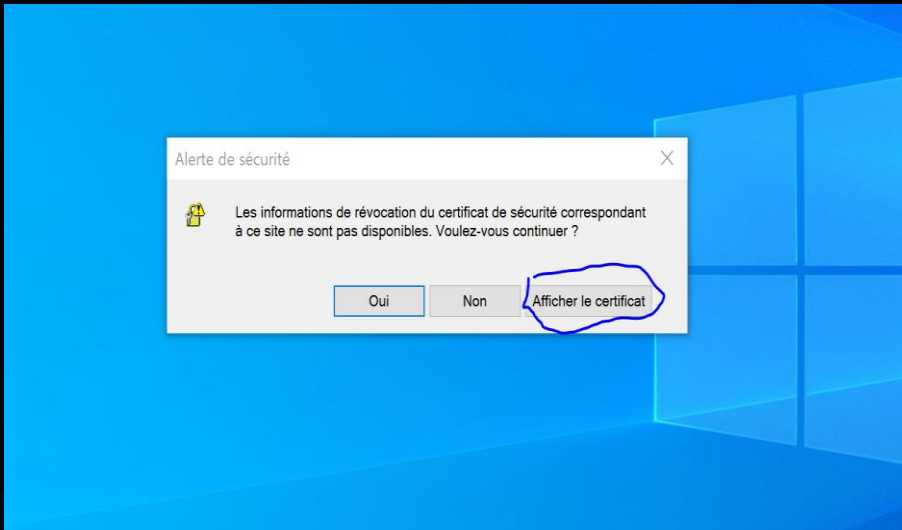
5-Création du portail captif

Pass-through credits per MAC address.	<input type="text"/>	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)	<input type="text"/>	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	<input type="checkbox"/> 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	<input checked="" type="checkbox"/> 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	<input type="text"/>	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_REDIREURL\$ variable in captiveportal's HTML pages.
After authentication redirection URL	<input type="text"/>	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	<input type="text"/>	Blocked MAC addresses will be redirected to this URL when attempting access.
Concurrent user logins	<input type="checkbox"/> 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	<input type="checkbox"/> 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	<input type="checkbox"/> Enable Pass-through MAC automatic additions	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.

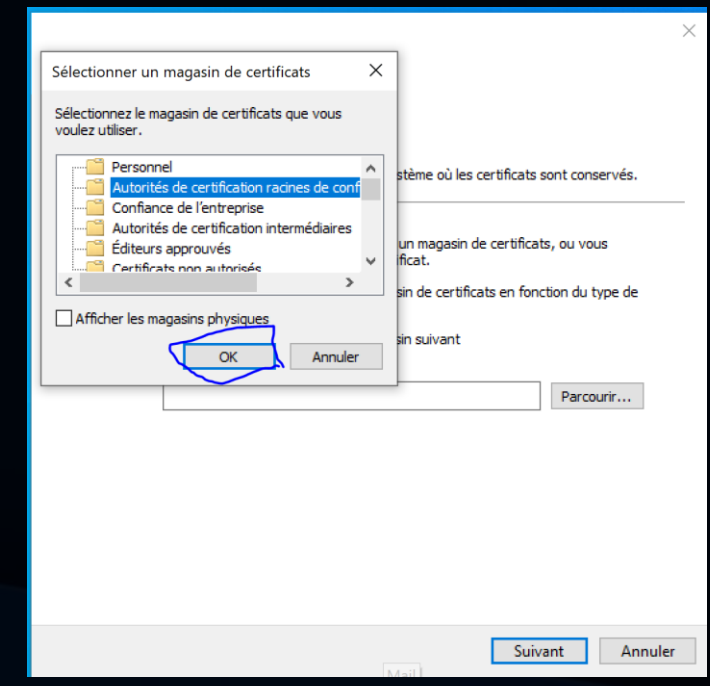
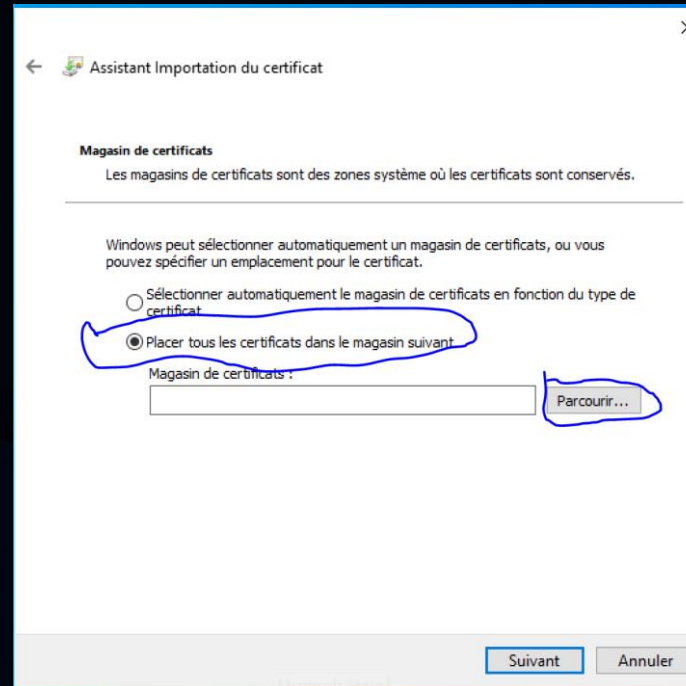
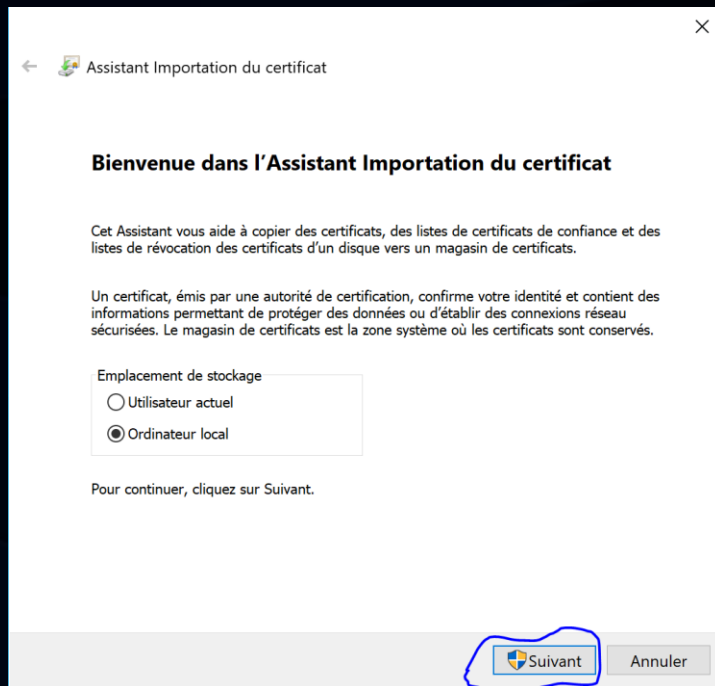
Authentication Method	<div>Use an Authentication backend</div> <div>Select an Authentication Method to use for this zone. One method must be selected. - "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers. - "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.</div>
Authentication Server	<div>Server AD: Local Database</div> <div>You can add a remote authentication server in the User Manager. Vouchers could also be used, please go to the Vouchers Page to enable them.</div>
Secondary authentication Server	<div>Server AD: Local Database</div> <div>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.</div>
Reauthenticate Users	<div><input type="checkbox"/> Reauthenticate connected users every minute</div> <div>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.</div>
HTTPS Options	
Login	<div><input checked="" type="checkbox"/> Enable HTTPS login</div> <div>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.</div>
HTTPS server name	<div>pfSense.formation.local</div> <div>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.</div>
SSL/TLS Certificate	<div>cert_portal</div> <div>If no certificates are defined, one may be defined here: System > Cert. Manager</div>
HTTPS Forwards	<div><input type="checkbox"/> Disable HTTPS Forwards</div> <div>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.</div>
<div>Save</div>	

6-Installation du certificat coté client

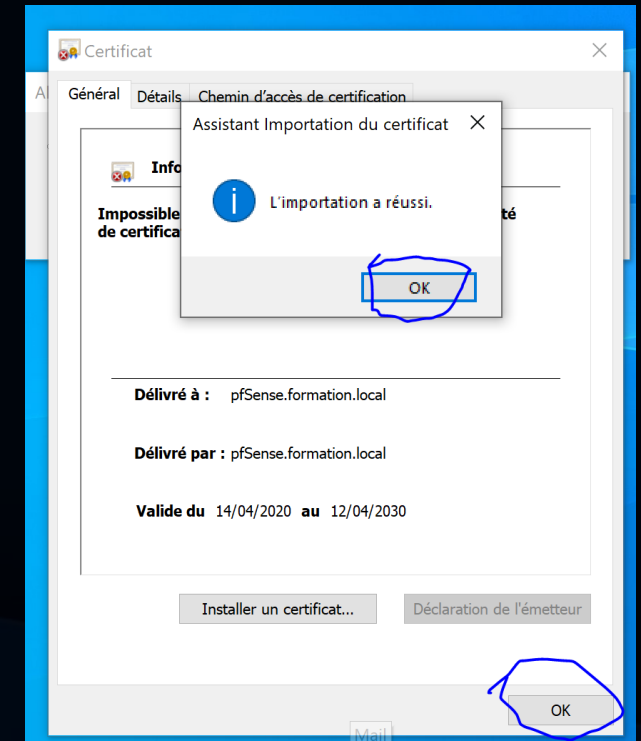
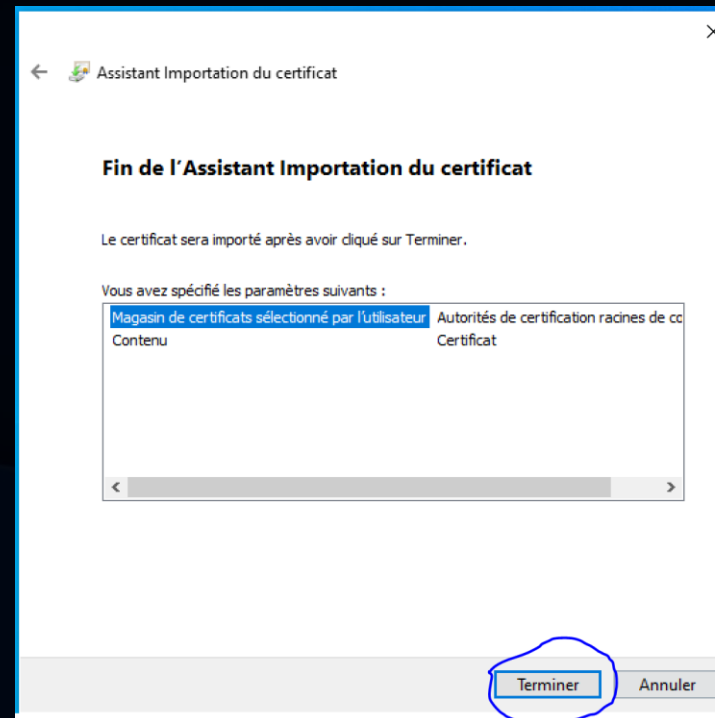
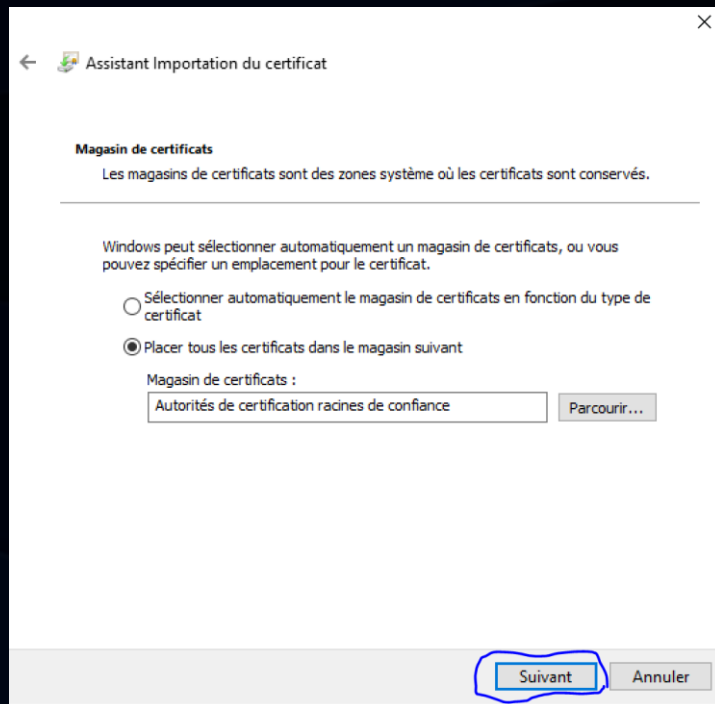
Cette étape nécessite le redémarrage du poste client après l'installation du service portail captif.



6-Installation du certificat coté client



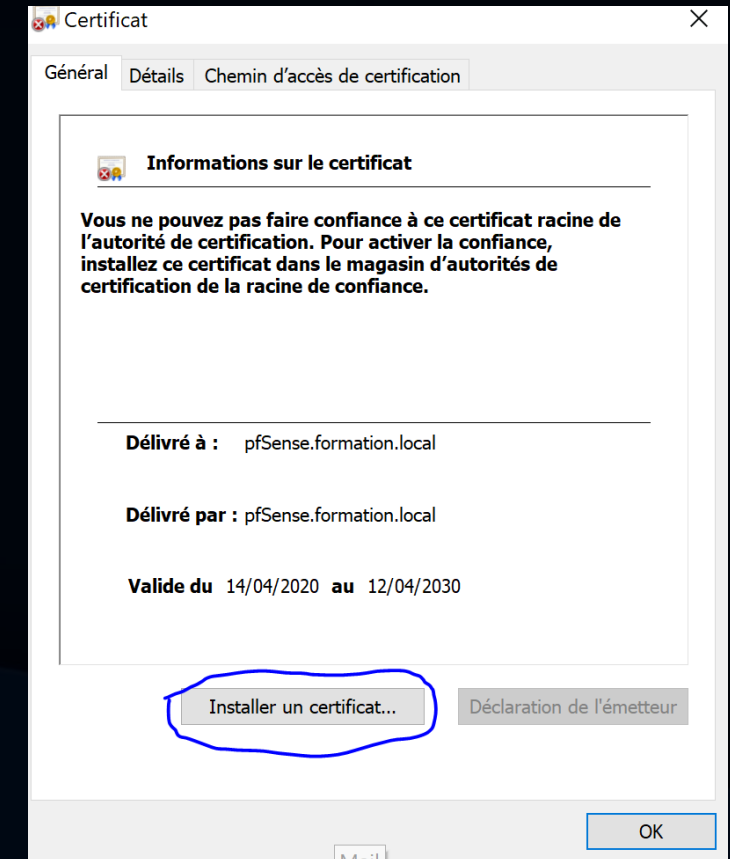
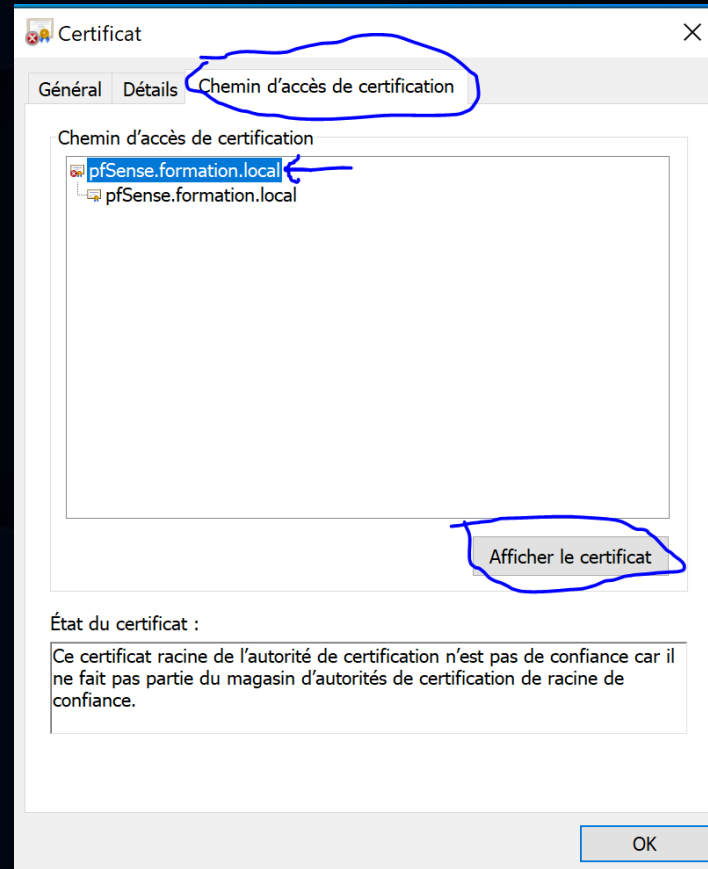
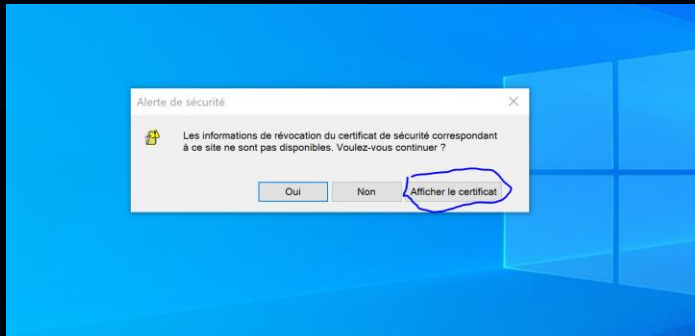
6-Installation du certificat coté client



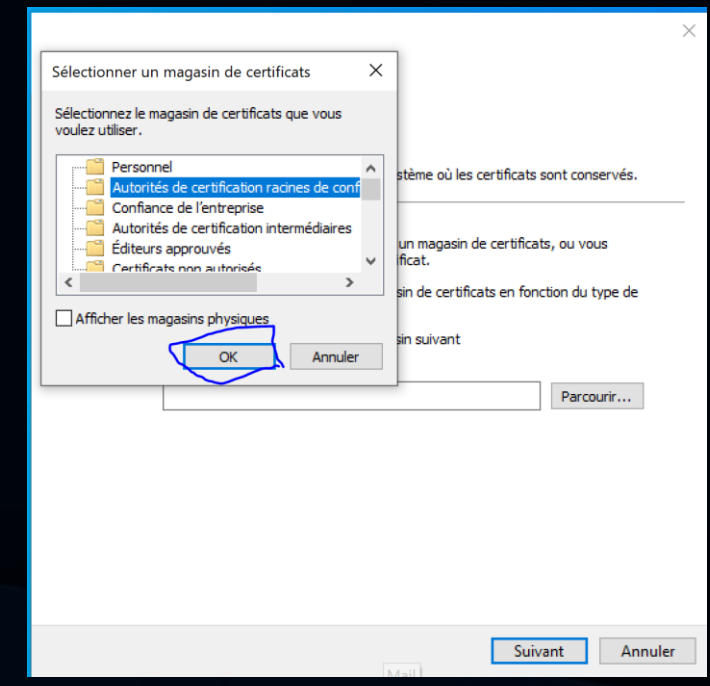
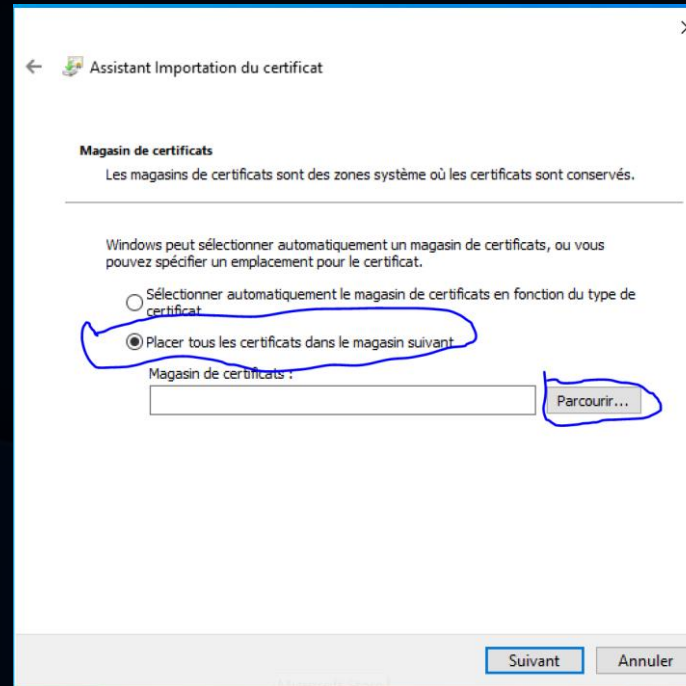
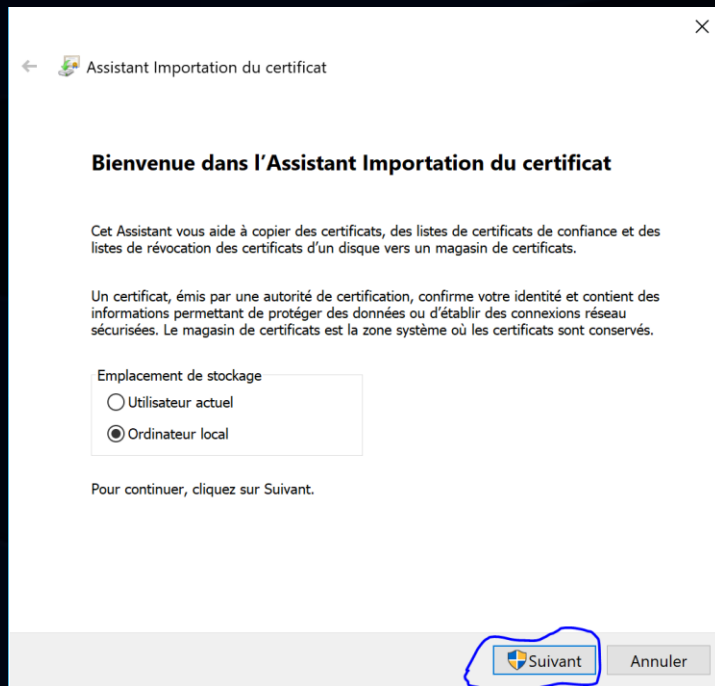
pfSense Portail Captif + LDAP



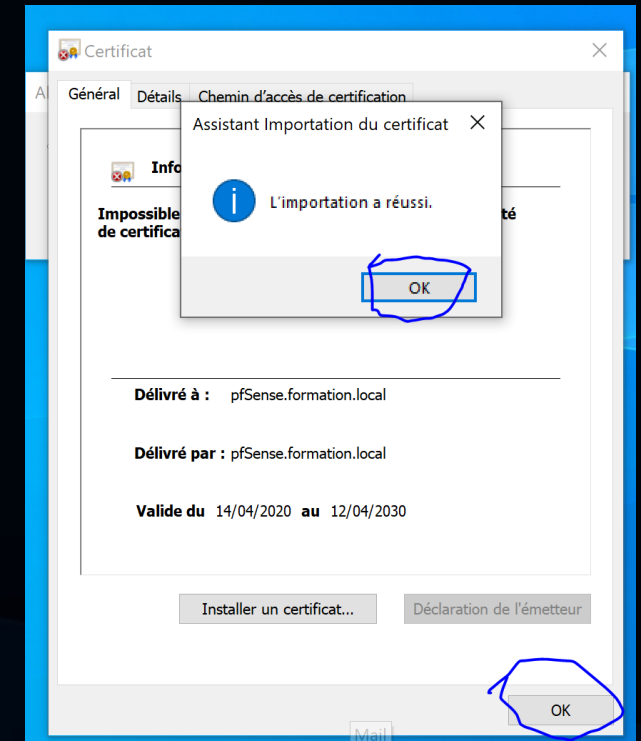
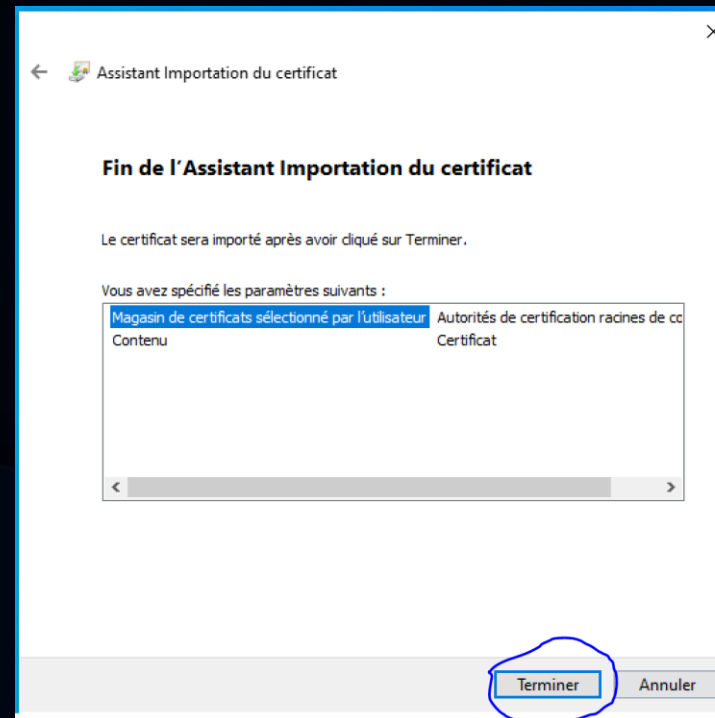
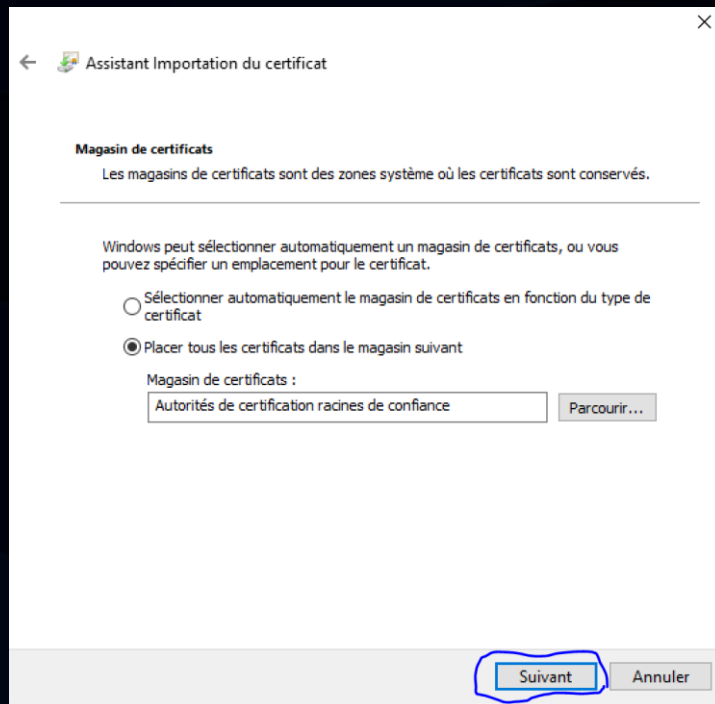
6-Installation du certificat coté client



6-Installation du certificat coté client



6-Installation du certificat coté client

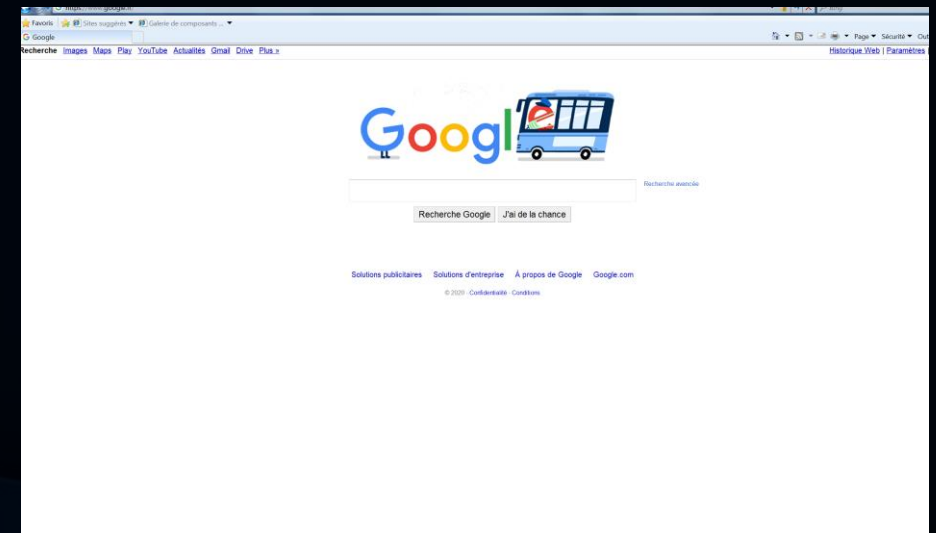
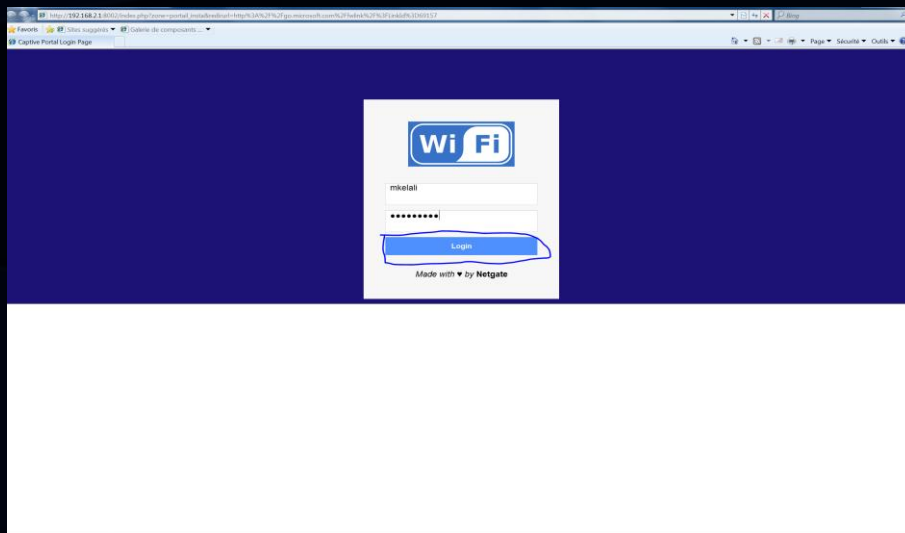


pfSense Portail Captif + LDAP



7-Tester via un navigateur Web

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



Load Balancing - Failover

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