

Installation et configuration d'OpenVPN

Table des matières

1. Prérequis :	1
2. Configuration de PFSense :	1
3. Lien avec le DNS :	5
4. Création des certificats :	6
5. Création d'un utilisateur :	9
6. Installation d'OpenVPN :	11
7. Configuration d'OpenVPN :	12
8. Exportation du client :	15
9. Installation d'OpenVPN sur le poste client :	16

1. Prérequis :

Pour commencer l'installation de OpenVPN il vous faudra un Windows serveur qui servira d'host pour OpenVPN et il faudra aussi un ou plusieurs clients, si possible sous Windows 10 pour pouvoir utiliser OpenVPN.

2. Configuration de PFSense :

Il faudra d'abord vous connecter à PFSense sur le PC host en utilisant l'adresse localhost qui est en général 192.168.1.1.

Vous devrez ensuite vous connecter avec les identifiants administrateur de du PC. Vous arriverez alors sur cette page :

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

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

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](#)

Ici il faudra simplement laisser ce qu'il y a de base et cliquer sur « suivant ».

Vous arriverez alors sur cette page :

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

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

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](#)

Sur cette page on laissera le time server hostname par défaut et on ajustera seulement la timezone dans laquelle on se trouve. On peut ensuite cliquer sur « suivant ».

Vous arriverez alors sur cette page :

pfSense

COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Configure WAN Interface

?

Step 4 of 9

Configure WAN Interface

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

SelectedType

DHCP

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

Subnet Mask

32

PPPoe Password

Show PPPoE password

☐ Reveal password characters

PPPoE Service name

Hint: this field can usually be left empty

PPPoE 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.

PPPoE 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.

PPTP configuration

PPTP Username

PPTP Password

Show PPTP password

☐ Reveal password characters

PPTP Local IP Address

pptplcalsubnet

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

Il suffira de simplement cliquer sur « suivant » sans rien modifier.

Vous arriverez ensuite sur cette page :

The screenshot shows the pfSense Setup Wizard at Step 5 of 9, titled "Configure LAN Interface". At the top, a warning message states: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The breadcrumb trail is "Wizard / pfSense Setup / Configure LAN Interface". Below a progress bar, the title "Configure LAN Interface" is followed by the instruction: "On this screen the Local Area Network information will be configured." The form contains two fields: "LAN IP Address" with the value "192.168.1.1" and a subtext "Type dhcp if this interface uses DHCP to obtain its IP address.", and "Subnet Mask" with the value "24". A blue "Next" button with a right arrow is at the bottom.

Ici aussi il faudra juste cliquer sur le bouton « suivant ».
Vous arriverez ensuite sur cette page :

The screenshot shows the pfSense Setup Wizard at Step 6 of 9, titled "Set Admin WebGUI Password". A warning message at the top says: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." The breadcrumb trail is "Wizard / pfSense Setup / Set Admin WebGUI Password". Below a progress bar, the title "Set Admin WebGUI Password" is followed by the instruction: "On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled." The form has two password fields: "Admin Password" and "Admin Password AGAIN". A blue "Next" button with a right arrow is at the bottom.

Ici il faudra définir le mot de passe d'administration de PFSense puis cliquer sur « suivant ».

Vous arriverez ensuite sur cette page :

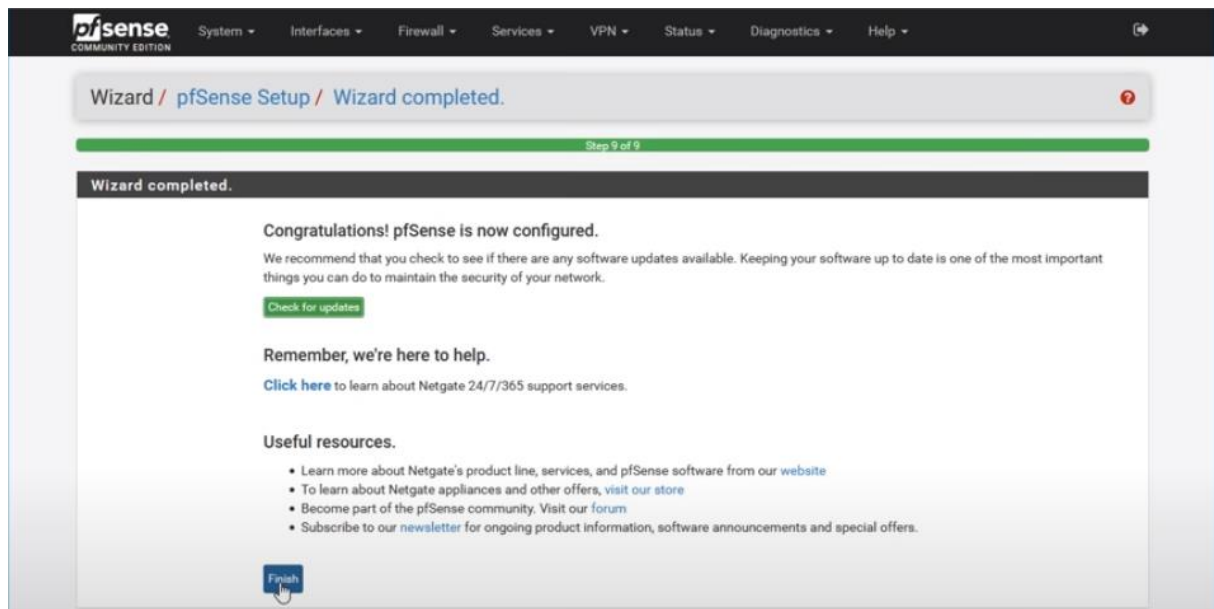
The screenshot shows the pfSense Setup Wizard at Step 7 of 9, titled "Reload configuration". The breadcrumb trail is "Wizard / pfSense Setup / Reload configuration". Below a progress bar, the title "Reload configuration" is followed by the instruction: "Click 'Reload' to reload pfSense with new changes." A blue "Reload" button with a right arrow is at the bottom.

Arrivé ici il faudra simplement cliquer sur le bouton « reload » pour relancer PFSense avec les nouvelles modifications.

Vous aurez donc le message suivant :



Une fois le reload fini vous arriverez sur cette page :



Cela signifie que la configuration de PFSense est terminée et qu'on peut donc passer à l'installation et la configuration de OpenVPN. Vous devez alors cliquer sur « finish ».

3. Lien avec le DNS :

Pour faire le lien avec le DNS vous devrez aller dans Services -> DNS Resolver -> General Settings puis dans Edit Host override. Une fois ici la page suivante s'ouvrira :

Services / DNS Resolver / General Settings / Edit Host Override

Host Override Options

Host

Name of the host, without the domain part
e.g. enter "myhost" if the full domain name is "myhost.example.com"

Domain

Parent domain of the host
e.g. enter "example.com" for "myhost.example.com"

IP Address

IPv4 or IPv6 address to be returned for the host
e.g.: 192.168.100.100 or fd00:abcd::1

Description

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

This page is used to override the usual lookup process for a specific host. A host entered as host='somesite' and parent domain='google.com'). Any attempt to look up the usual external lookup server for the domain will not be queried. Both the name and domain such as 'test', 'mycompany.localdomain', or '1.168.192.in-addr.arpa', as

Ici vous aurez simplement à mettre le nom d'hôte, le domaine et l'adresse ip du DNS. Une fois cela fait vous êtes lié au DNS de votre réseau.

4. Création des certificats :

Ensuite il faudra aller dans « General setup » comme le montre le screen ci-dessous :

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / **Dynamic DNS Clients**

Dynamic DNS Clients

Check IP Services

Hostname	Cached IP	Description	Actions
ceos3c.hopto.org	87.143.146.180	No-IP DynDNS	Edit Refresh Delete

+ Add

IP addresses appearing in green are up to date with Dynamic DNS provider. An update for an IP address can be forced on the edit page for that service.

Vous y trouverez les informations suivantes :

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / **General Setup**

System

Hostname

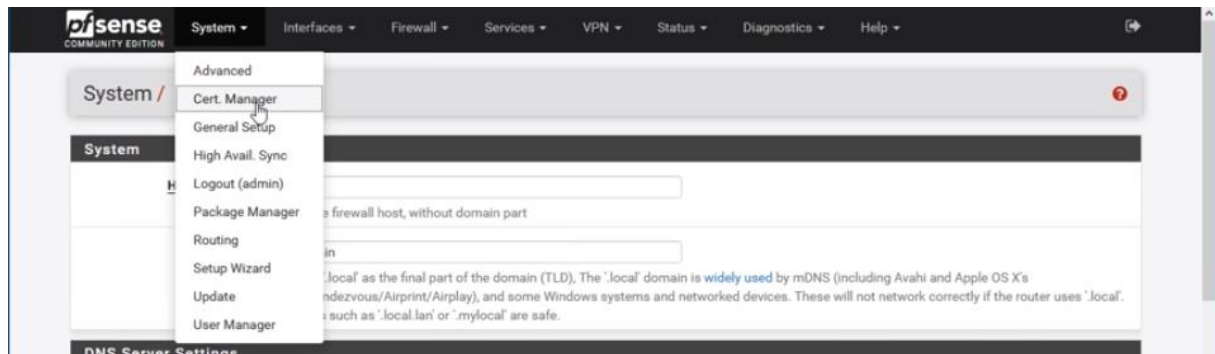
Name of the firewall host, without domain part

Domain

Do not use '.local' as the final part of the domain (TLD). The '.local' domain is widely used by mDNS (including Avahi and Apple OS X's Bonjour/Rendezvous/Airprint/Airplay), and some Windows systems and networked devices. These will not network correctly if the router uses '.local'. Alternatives such as '.local.lan' or '.mylocal' are safe.

Il faudra juste vérifier le domaine et retenir le nom de domaine, en principe localdomain.

Ensuite il faudra aller dans « certificate manager »

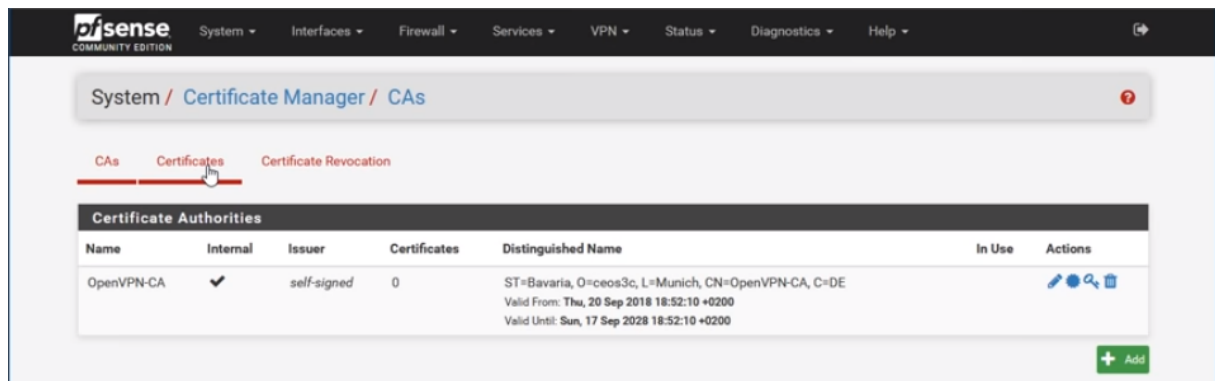


Vous arrivez alors sur cette page :

The screenshot shows the 'Create / Edit CA' page in pfSense. The 'Certificates' tab is selected. The form is titled 'Create / Edit CA'. It has two sections: 'Descriptive name' and 'Method'. The 'Descriptive name' field contains 'OpenVPN-CA'. The 'Method' dropdown is set to 'Create an internal Certificate Authority'. Below this is the 'Internal Certificate Authority' section. It contains several fields: 'Key length (bits)' set to 2048, 'Digest Algorithm' set to sha256 (with a note: 'NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.'), 'Lifetime (days)' set to 3650, 'Common Name' set to 'OpenVPN-CA'. Below these are optional fields for 'Country Code' (DE), 'State or Province' (Bavaria), 'City' (Munich), 'Organization' (ceos3c), and 'Organizational Unit' (e.g. My Department Name (optional)). A 'Save' button is at the bottom.

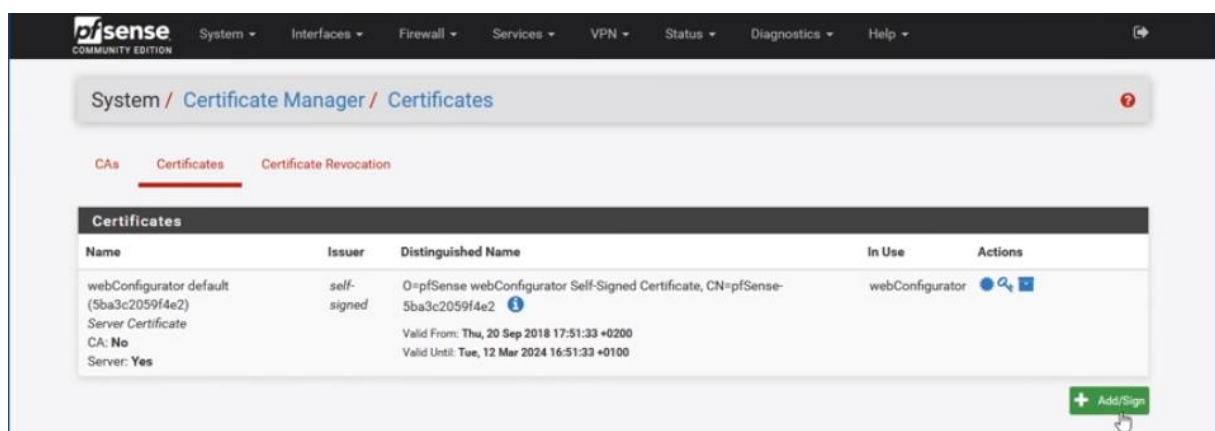
Vous devrez sur cette page mettre un « descriptive name » puis le copier-coller dans la case « common name », changer le country code pour mettre « FR » mettre le département, la ville et le nom de l'organisation qui dans notre cas est Animus. Puis ensuite cliquez sur « save ».

Vous arriverez sur cette page :



Vous aurez ici les informations sur le certificat d'autorité. Il faudra ensuite cliquer sur « Certificates » pour aller créer un autre certificat.

Vous arriverez sur la page ci-dessous et devrez cliquer sur « Add/Sign ».



Vous arriverez alors sur cette page :

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name OpenVPN-ServerCert

Internal Certificate

Certificate authority OpenVPN-CA

Key length 2048

Digest Algorithm sha256
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days) 3650

Common Name ceos3c.hq

The following certificate subject components are optional and may be left blank.

Country Code DE

State or Province Bavaria

City Munich

Organization ceos3c

Organizational Unit e.g. My Department Name (optional)

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names

Type Value

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add

Ici il faudra changer le « descriptive name » pour mettre ce qu'il y a sur le screen ou autre chose dont vous vous rappellerez. Il faudra ensuite vérifier que le certificat d'autorité est bien celui que nous avons créé juste avant. Il faudra changer le common name pour mettre l'adresse de notre DNS. Il faudra aussi mettre le type de certificat en « server certificate » puis cliquer sur « save ». Vous arriverez alors sur cette page :

System / Certificate Manager / Certificates

CA's Certificates Certificate Revocation

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (5ba3c2059f4e2) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-5ba3c2059f4e2 Valid From: Thu, 20 Sep 2018 17:51:33 +0200 Valid Until: Tue, 12 Mar 2024 16:51:33 +0100	webConfigurator	<input type="button" value="info"/> <input type="button" value="edit"/> <input type="button" value="delete"/>
OpenVPN-ServerCert Server Certificate CA: No Server: Yes	OpenVPN-CA	ST=Bavaria, O=ceos3c, L=Munich, CN=ceos3c.hopto.org, C=DE Valid From: Thu, 20 Sep 2018 18:53:29 +0200 Valid Until: Sun, 17 Sep 2028 18:53:29 +0200		<input type="button" value="info"/> <input type="button" value="edit"/> <input type="button" value="delete"/>

Vérifiez que le nouveau certificat est bien présent avec les bons noms donnés et qu'il est bien de type server.

5. Création d'un utilisateur :

System / Certificates

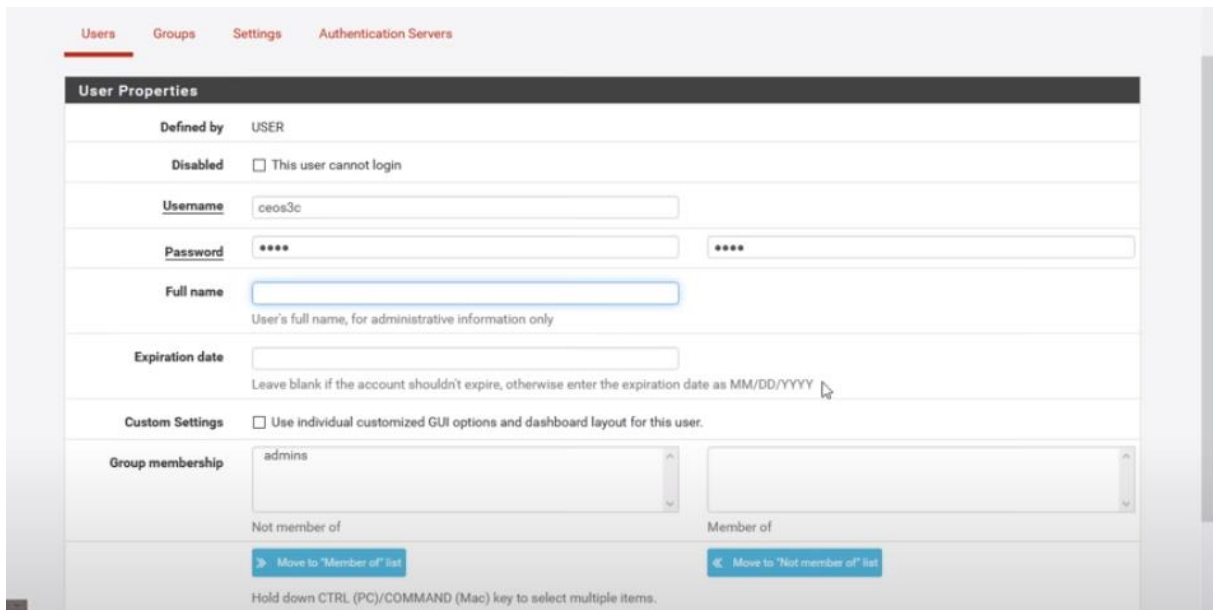
CA's Cert Certificate Revocation

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator (5ba3c2059f4e2) Server Certificate CA: No	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-5ba3c2059f4e2 Valid From: Thu, 20 Sep 2018 17:51:33 +0200	webConfigurator	<input type="button" value="info"/> <input type="button" value="edit"/> <input type="button" value="delete"/>

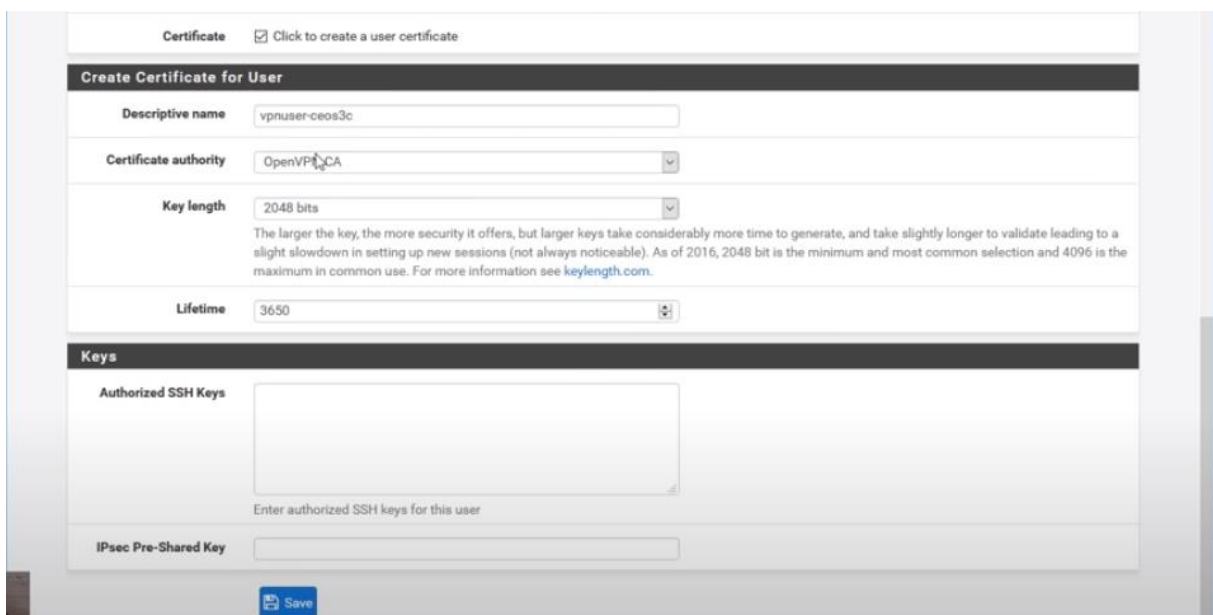
System

Il faudra ensuite cliquer sur « User manager » pour créer un nouvel utilisateur du VPN. Vous arriverez sur cette page :



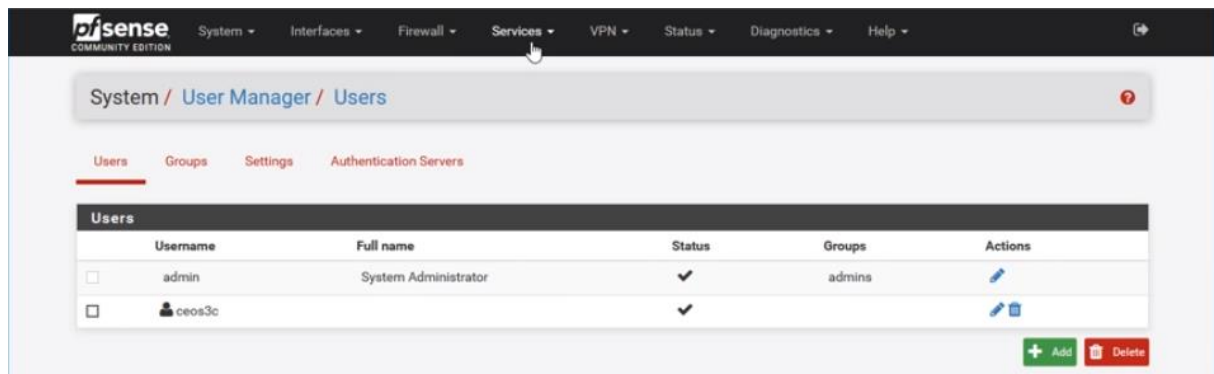
The screenshot shows the 'User Properties' form in a VPN management interface. The form is divided into several sections: 'Defined by' (USER), 'Disabled' (checkbox), 'Username' (ceos3c), 'Password' (masked with ****), 'Full name' (empty field), 'Expiration date' (empty field), 'Custom Settings' (checkbox), and 'Group membership' (admins). There are also buttons for 'Move to "Member of" list' and 'Move to "Not member of" list'. The form is titled 'User Properties' and has tabs for 'Users', 'Groups', 'Settings', and 'Authentication Servers'.

Il faudra remplir le nom de l'utilisateur « username » et son mot de passe et on va ensuite cocher la case « certificate » comme ci-dessous :



The screenshot shows the 'Create Certificate for User' form in a VPN management interface. The form is divided into several sections: 'Certificate' (checkbox), 'Descriptive name' (vpnuser-ceos3c), 'Certificate authority' (OpenVPN CA), 'Key length' (2048 bits), 'Lifetime' (3650), 'Keys' (Authorized SSH Keys), and 'IPsec Pre-Shared Key'. There is a 'Save' button at the bottom. The form is titled 'Create Certificate for User' and has a checkbox for 'Click to create a user certificate'.

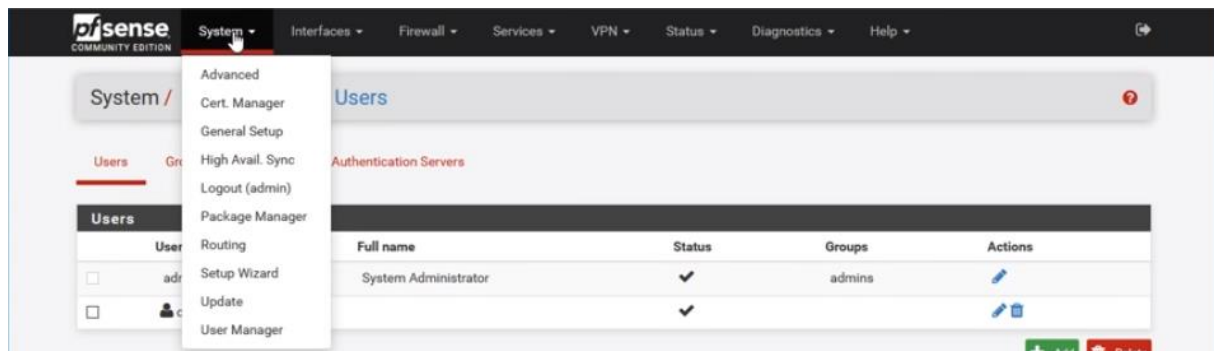
Il faudra vérifier que le certificat d'autorité est celui créé juste avant et après nous pouvons cliquer sur « Save ». Vous arriverez sur cette page :



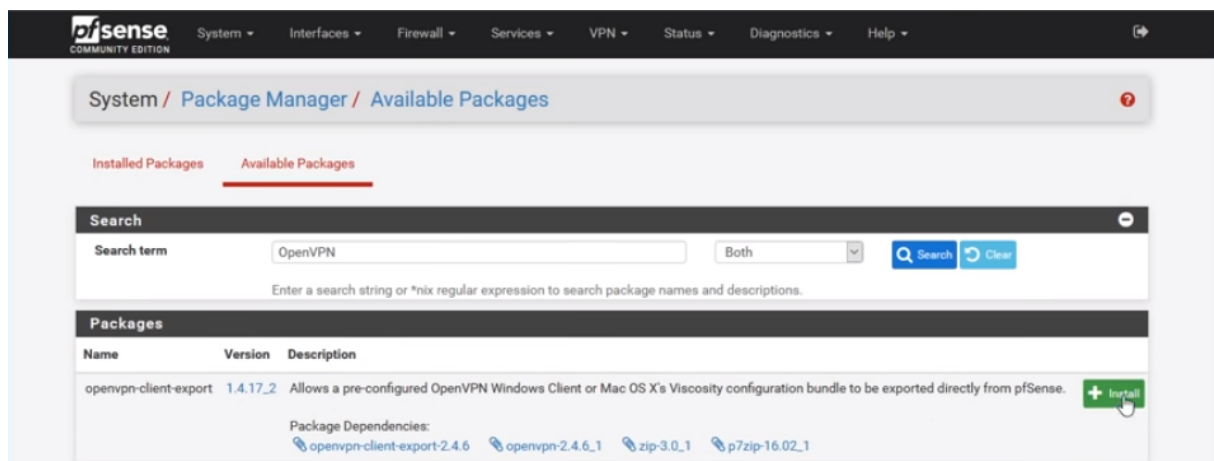
On peut y voir qu'il y a l'administrateur que l'on a configuré au tout début et l'utilisateur que l'on vient juste de créer.

6. Installation d'OpenVPN :

Ensuite il faudra aller dans « package manager » comme ci-dessous :

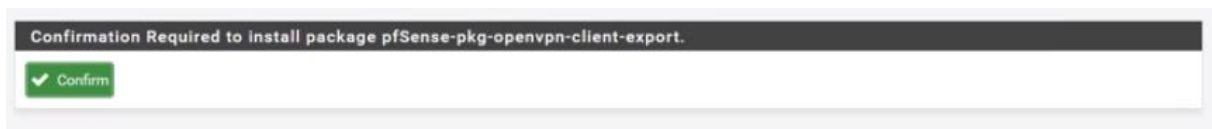


Il faudra ensuite aller dans « Available packages » et chercher dans la barre de recherche le package OpenVPN



Arrivé ici il faudra cliquer sur « Install » pour pouvoir installer le package d'OpenVPN.

Vous devrez alors cliquer le bouton « confirm » comme ci-dessous :



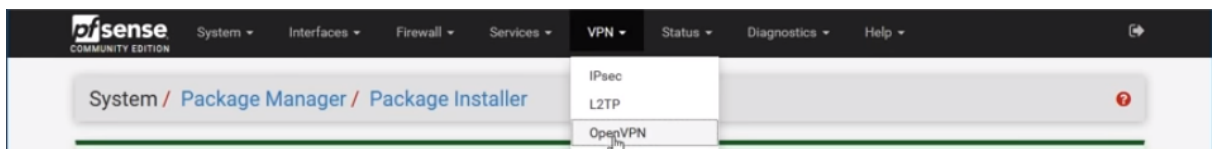
Une fois le bouton cliqué l'installation va se lancer.

Vous devriez avoir ceci qui apparait en haut une fois terminé :

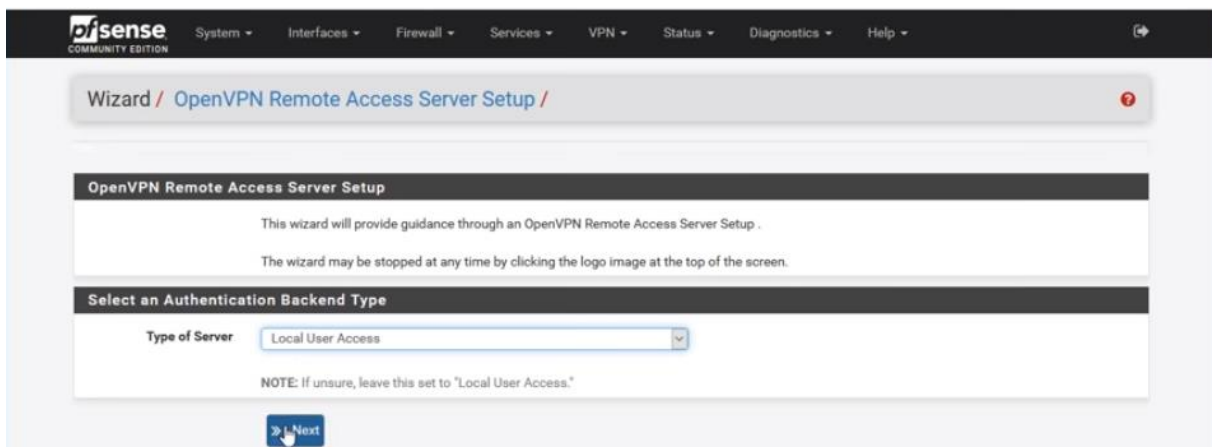


7. Configuration d'OpenVPN :

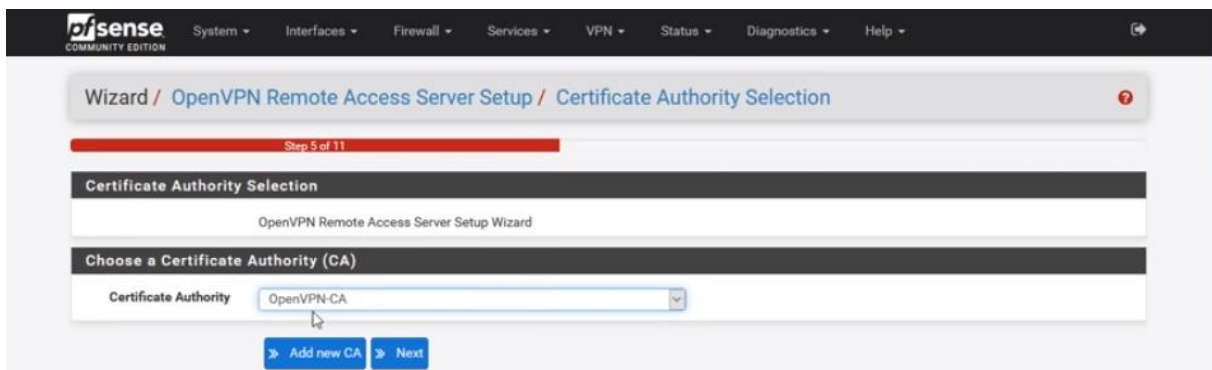
Une fois l'installation terminée il faudra aller dans le menu de configuration d'OpenVPN comme-dessous :



Ensuite il faudra aller dans Wizard et vous arriverez sur la page ci-dessous :



Il faudra laisser « Local User Access » et cliquer sur « suivant ». Vous arriverez sur cette page :



Il faudra ici vérifier que le certificat d'autorité est bien celui que nous avons créé précédemment puis cliquer sur « suivant ». Vous arriverez alors sur cette page :

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: OpenVPN-ServerCert

Il faudra ici encore vérifier si le certificat est le bon qui est censé être le certificat de serveur et cliquer sur « suivant ». Vous arriverez sur la page de configuration d'OpenVPN. Il faut tout laisser par défaut jusqu'à arriver à « Tunnel Settings ».

Tunnel Network 192.168.2.0/24
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.

Redirect Gateway ☒
Force all client generated traffic through the tunnel.

Local Network 192.168.1.0/24
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent Connections 1
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. 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.

Type-of-Service ☐
Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.

Inter-Client Communication ☐
Allow communication between clients connected to this server.

Duplicate Connections ☐
Allow multiple concurrent connections from clients using the same Common Name.
NOTE: This is not generally recommended, but may be needed for some scenarios.

Il faudra entrer en réseau l'adresse ip qu'il faut utiliser pour arriver sur le site de PFSense et en mettre le masque. Il faudra aussi cocher « Redirect Gateway » et « Inter-client Communication ».

En dessous dans la partie « Client settings » il faudra faire comme ci-dessous :

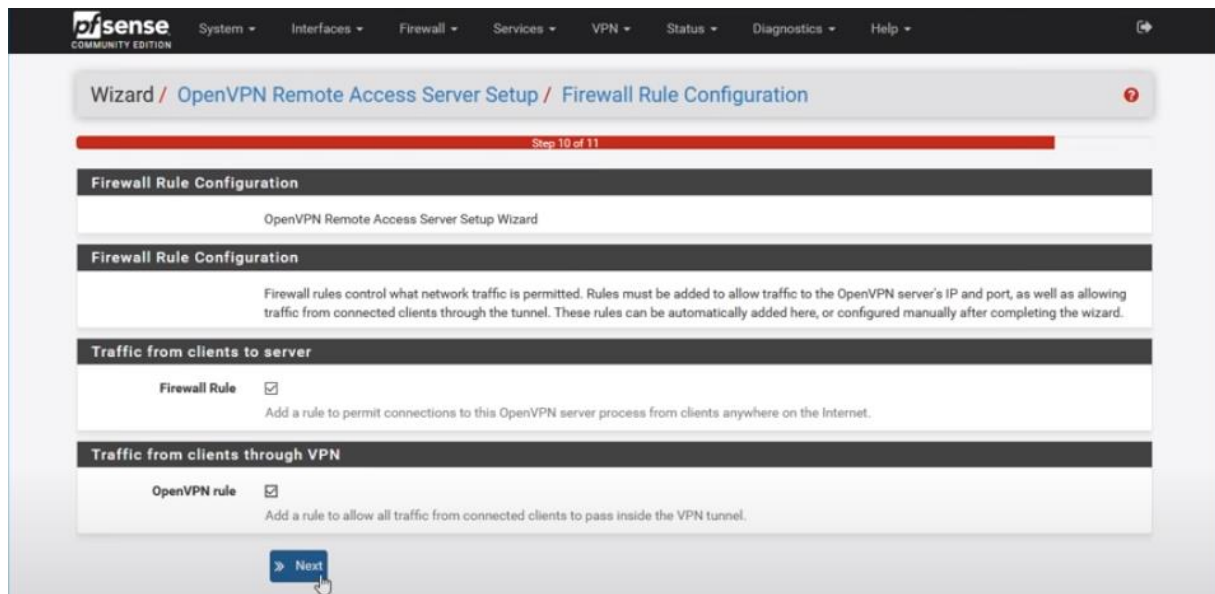
Dynamic IP ☒
Allow connected clients to retain their connections if their IP address changes.

Topology Subnet - One IP address per client in a common subnet
Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

DNS Default Domain localdomain
Provide a default domain name to clients.

DNS Server 1 192.168.1.1
DNS server IP to provide to connecting clients.

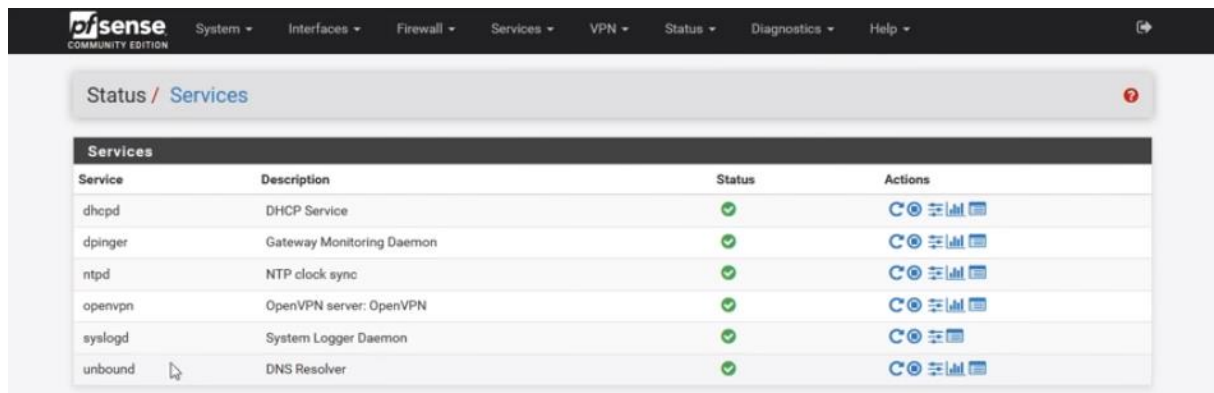
Il faudra laisser les deux premières lignes par défaut, mettre le domaine du DNS et mettre l'adresse IP de PFSense. Ensuite il faudra scroller vers le bas et cliquer sur « suivant ». Vous arriverez sur cette page :



Il faudra ici cocher les deux cases et cliquer sur « suivant ». Et cliquer sur « Finish » sur la page suivante.
En principe l'OpenVPN est créé et fonctionnel il faudra ensuite aller dans « Services » comme ci-dessous :



Vous arriverez donc sur cette page :



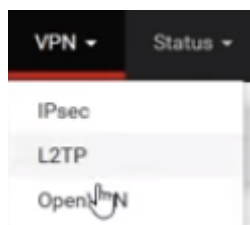
The screenshot shows the 'Services' tab in the Pfsense web interface. A table lists several services, all of which are running, indicated by green checkmarks in the 'Status' column.

Service	Description	Status	Actions
dhcpcd	DHCP Service	✓	[Icons]
dpinger	Gateway Monitoring Daemon	✓	[Icons]
ntpd	NTP clock sync	✓	[Icons]
openvpn	OpenVPN server: OpenVPN	✓	[Icons]
syslogd	System Logger Daemon	✓	[Icons]
unbound	DNS Resolver	✓	[Icons]

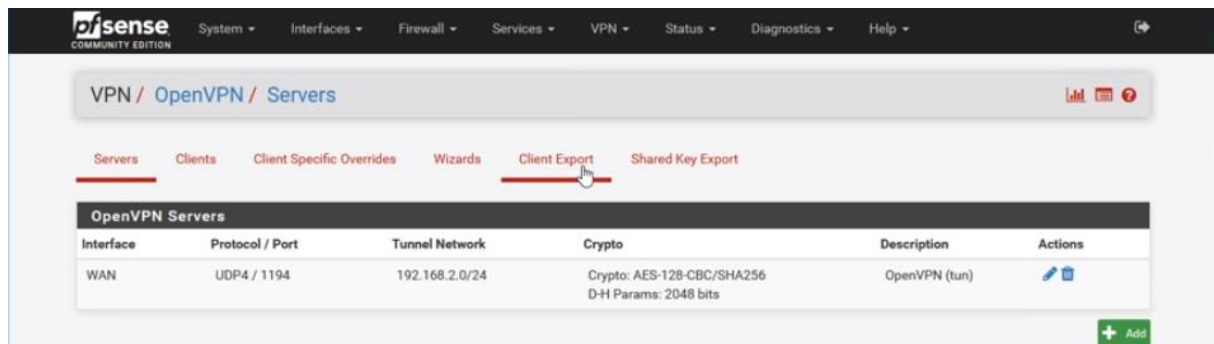
On peut voir ici qu'il y a une ligne OpenVPN et que le statut est vert donc running.

8. Exportation du client :

Ensuite il faudra retourner dans OpenVPN.



Et aller dans « Export client ».



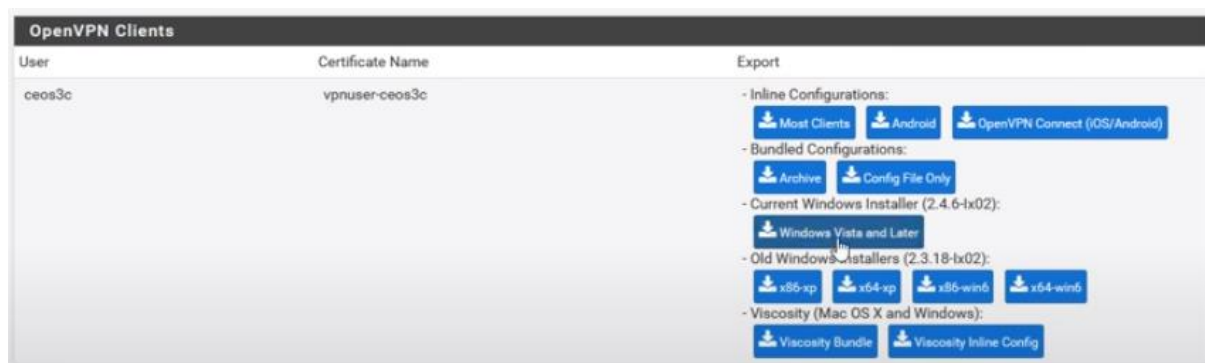
The screenshot shows the 'Client Export' tab in the Pfsense OpenVPN configuration page. It displays a table for 'OpenVPN Servers' with one server configured.

Interface	Protocol / Port	Tunnel Network	Crypto	Description	Actions
WAN	UDP4 / 1194	192.168.2.0/24	Crypto: AES-128-CBC/SHA256 D-H Params: 2048 bits	OpenVPN (tun)	[Icons]

At the bottom right of the table, there is a green '+ Add' button.

Vous arriverez sur une page et vous devrez tout laisser par défaut, aller tout en bas et cliquer sur « Save as default ».

Vous allez revenir sur la page précédente et il faudra descendre jusqu'à « OpenVPN Clients » comme ci-dessous :



Il faudra ensuite cliquer sur « Windows Vista and Later » pour pouvoir le mettre sur un client sous Windows.

9. Installation d'OpenVPN sur le poste client :

Une fois l'installateur téléchargé mettez-le sur le PC en utilisateur en question et lancer le en tant qu'administrateur. Il faudra ensuite tout laisser par défaut et simplement cliquer sur « Install » puis faire suivant, « I agree » et « install » jusqu'au bouton « Finish ». Une fois cela fait vous aurez le GUI de OpenVPN qui aura son icone en bas à droite et vous n'aurez plus qu'à faire clic droit et « connect » pour ensuite y entrer les informations du compte utilisateur créé jusque précédemment.

Voilà vous êtes maintenant connecté à votre VPN.