

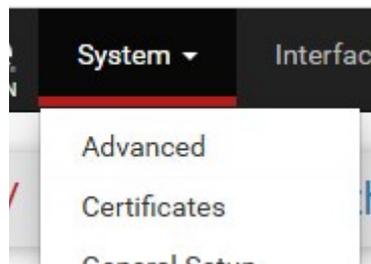
Configuration d'un VPN-SSL client-to-site avec OpenVPN :

Introduction :

Dans ce TP, nous allons effectu ,

TP :

Pour d biter ce TP, Nous allons cr   une autorit  de certification sur notre pare-feu Pfsense.
Pour cela nous nous rendons dans « systeme » puis « certificate »



En premier lieu nous lui donnons un nom et prenons une autorit  de certification interne

Create / Edit CA	
Descriptive name	<input type="text" value="CA-POLOGNE"/> <small>The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ' , "</small>
Method	<input type="text" value="Create an internal Certificate Authority"/>
Trust Store	<input type="checkbox"/> Add this Certificate Authority to the Operating System Trust Store <small>When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.</small>
Randomize Serial	<input type="checkbox"/> Use random serial numbers when signing certificates <small>When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.</small>

Ensuite, il nous reste plus qu'a rentrer les informations du certificat et notre autorit  sera cr  er

Internal Certificate Authority	
Key type	<input type="text" value="RSA"/>
	<input type="text" value="2048"/> <small>The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.</small>
Digest Algorithm	<input type="text" value="sha256"/> <small>The digest method used when the CA is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid</small>
Lifetime (days)	<input type="text" value="3650"/>
Common Name	<input type="text" value="pologne"/> <small>The following certificate authority subject components are optional and may be left blank.</small>
Country Code	<input type="text" value="FR"/>
State or Province	<input type="text" value="Moselle"/>
City	<input type="text" value="Metz"/>
Organization	<input type="text" value="pologne"/>

Passons maintenant à la création du certificat, dans l'onglet « certificat »

The screenshot shows the 'Certificates' tab in a management interface. At the top, there are tabs for 'Authorities', 'Certificates', and 'Certificate Revocation'. Below the tabs is a search bar with a 'Search term' input field, a 'Both' dropdown, and 'Search' and 'Clear' buttons. A note below the search bar says: 'Enter a search string or *nix regular expression to search certificate names and distinguished names.' Below the search bar is a table of certificates with the following data:

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (67332dd1910bd) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-67332dd1910bd ⓘ Valid From: Tue, 12 Nov 2024 09:28:33 -0100 Valid Until: Mon, 15 Dec 2025 09:28:33 -0100	webConfigurator	

At the bottom right of the table area is a green '+ Add/Sign' button.

Nous refaisons les mêmes manipulations que précédemment, le petit changement sera à la fin. Nous devons choisir le type de certificat, nous choisissons un certificat de serveur

The screenshot shows the 'Certificate Attributes' configuration page. It contains the following sections:

- 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:** A dropdown menu set to 'Server Certificate'. Below it, a note says: 'Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.'
- Alternative Names:** A dropdown menu set to 'FQDN or Hostname' and an empty input field for the value. Below it, a note says: '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 SAN Row:** A green '+ Add SAN Row' button.

À présent, nous allons créer un utilisateur dans l'onglet « système » puis « user manager »

The screenshot shows the 'System' dropdown menu in the management interface. The menu is open, showing the following options:

- Advanced
- Certificates
- General Setup
- High Availability
- Package Manage
- Register
- Routing
- Setup Wizard
- Update
- User Manager

Pour créer un utilisateur, il faudra lui donner un nom ainsi qu'un mot de passe. Nous pouvons aussi cocher la case certifi-

cat afin de lui créer un certificat utilisateur directement depuis l'interface de création de l'utilisateur. Il nous suffira juste de rentrer le nom du certificat.

User Properties	
Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	<input type="text" value="vpn.pologne"/>
Password	<input type="password" value="....."/> <input type="password" value="....."/>
Full name	<input type="text"/>

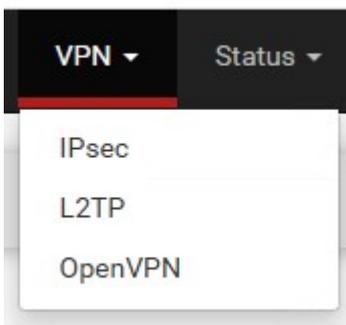
Certificate Click to create a user certificate

Create Certificate for User

Descriptive name

Création de la configuration de OpenVPN :

Pour créer la configuration il faudra aller dans l'onglet « VPN » puis « OpenVPN »



En mode de serveur nous prendrons « remote access (SSL/TLS + User auth) » qui est un accès à distance basée sur certificat et compte utilisateur. Nous prendrons la base de donnée local, si nous avons un annuaire LDAP nous le retrouvons aussi a cette endroit.

General Information	
Description	<input type="text" value="VPN-pologne"/> <small>A description of this VPN for administrative reference.</small>
Disabled	<input type="checkbox"/> Disable this server <small>Set this option to disable this server without removing it from the list.</small>

Mode Configuration	
Server mode	<input type="text" value="Remote Access (SSL/TLS + User Auth)"/>
Backend for authentication	<input type="text" value="Local Database"/>
Device mode	<input type="text" value="tun - Layer 3 Tunnel Mode"/> <small>"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)</small>

Au niveau de « server certificat » nous sélectionnons le certificat de serveur que nous avons créé précédemment

Server certificate	Certificat-OpenVPN (Server: Yes, CA: CA-POLOGNE) ▼
DH Parameter Length	===== Server Certificates ===== webConfigurator default (67332dd1910bd) (Server: Yes, In Use) Certificat-OpenVPN (Server: Yes, CA: CA-POLOGNE) ===== Non-Server Certificates =====
ECDH Curve	Certificat-VPN-pologne (Server: NO, CA: CA-POLOGNE, In Use)

Nous prendrons la méthode de chiffrement ci-dessous, elle est plus lourde mais plus sécuriser

Fallback Data Encryption Algorithm AES-256-CBC (256 bit key, 128 bit block) ▼

The Fallback Data Encryption Algorithm used for data channel packets when negotiation (e.g. Shared Key). This algorithm is automatically included in the

Passons aux paramètre IP, le tunnel network sera l'ip de notre VPN et l'ip local network sera la plage d'ip de destination de notre.

Tunnel Settings

IPv4 Tunnel Network
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

IPv6 Tunnel Network
This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The first usable address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway Force all client-generated IPv6 traffic through the tunnel.

IPv4 Local network(s)
IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network

Nous cochons, la case IP dynamic afin que les clients puisse garder leur connexion au VPN.
 Pour la topology nous prendrons en /30 afin que tous les clients soit sur un sous réseaux différent.

Client Settings

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

Topology
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".

Ici, nous rentrons le domaine ainsi que les DNS

Advanced Client Settings

DNS Default Domain Provide a default domain name to clients

DNS Default Domain

DNS Server enable Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.

DNS Server 1

DNS Server 2

DNS Server 3

DNS Server 4

Dans les custom option, nous indiquons l'option « auth-nocache » qui évite la mise en cache des identifiants, ce qui offre plus de sécurité

Advanced Configuration

Custom options

La configuration de OpenVPN côté serveur est finie, nous allons voir comment exporter cette configuration car de base PfSense ne le prend pas en charge. Pour cela nous allons aller dans le « package manager », dans la barre de recherche nous écrivons OpenVPN et nous trouverons « openvpn-client-export » et nous l'installons.

Search

Search term Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
openvpn-client-export	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.	<input type="button" value="+ Install"/>
Package Dependencies:			
openvpn-client-export-2.6.7 openvpn-2.6.8_1 zip-3.0_1 7-zip-23.01			

Dans l'onglet OpenVPN nous retrouvons un nouveau onglet « client export », dans celui-ci nous pouvons laisser les paramètres par défaut, il faudra juste à nouveau écrire « auth-nocache » dans les configurations supplémentaires

Advanced

Additional configuration options

Pour obtenir la configuration, nous descendons en bas de page et prenons l'archive des configurations liées

User	Certificate Name	Export
vpn.pologne	Certificat-VPN-pologne	- Inline Configurations: Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive Config File Only - Current Windows Installers (2.6.7-1x001):

Passons a la création des règles de pare-feu.

Nous allons créé une nouvelle règle UDP sur l'interface WAN

Firewall / Rules / WAN

Floating **WAN** LAN OpenVPN

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/35 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0/1 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Protocol

UDP

Choose which IP protocol this rule should match.

En destination nous prenons la WAN adress et pour le port, le port OpenVPN

Destination					
Destination	<input type="checkbox"/> Invert match	WAN address		Destination Address	/
Destination Port Range		OpenVPN (119)	From	OpenVPN (119)	To
		Custom		Custom	

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

La prochaine règle sert a autoriser les ressources, Nous prendrons l'interface OpenVPN

Action
 Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet is returned to the sender, whereas with block the packet is dropped silently.

Disabled Disable this rule
 Set this option to disable this rule without removing it from the list.

Interface
 Choose the interface from which packets must come to match this rule.

Address Family
 Select the Internet Protocol version this rule applies to.

Protocol
 Choose which IP protocol this rule should match.

Dans la destination nous autoriserons le protocole rdp (port 3389) sur notre poste client

Destination

Destination Invert match /

Destination Port Range
 From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Ensuite, nous créons une règle sur l'interface OpenVPN pour le DNS, en destination j'ai pris un groupe créé au préalable nommé « DNS » qui regroupe mes trois serveurs DNS. En port, nous prenons le port DNS (53)

Destination

Destination Invert match /

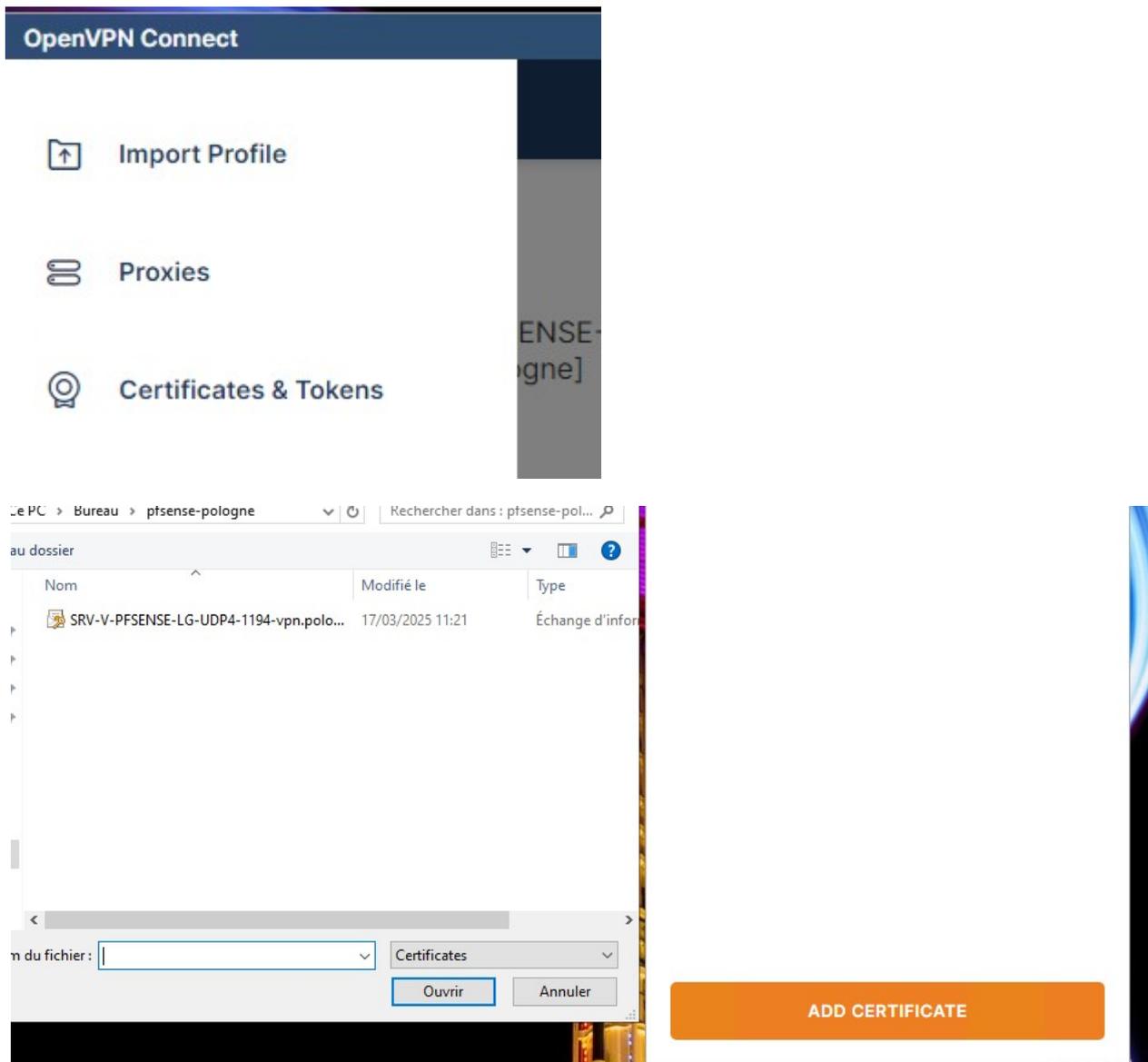
Destination Port Range
 From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Passons sur le poste client à présent afin d'installer OpenVPN



Sur l'application, nous allons ajouter le certificat pour cela nous allons dans l'onglet « certificates & tokens » → « add certificate » puis nous prenons le certificat qui se trouve dans le fichier export télécharger au préalable.



Après il ne suffit plus que se connecter au poste.