
Objectifs traités

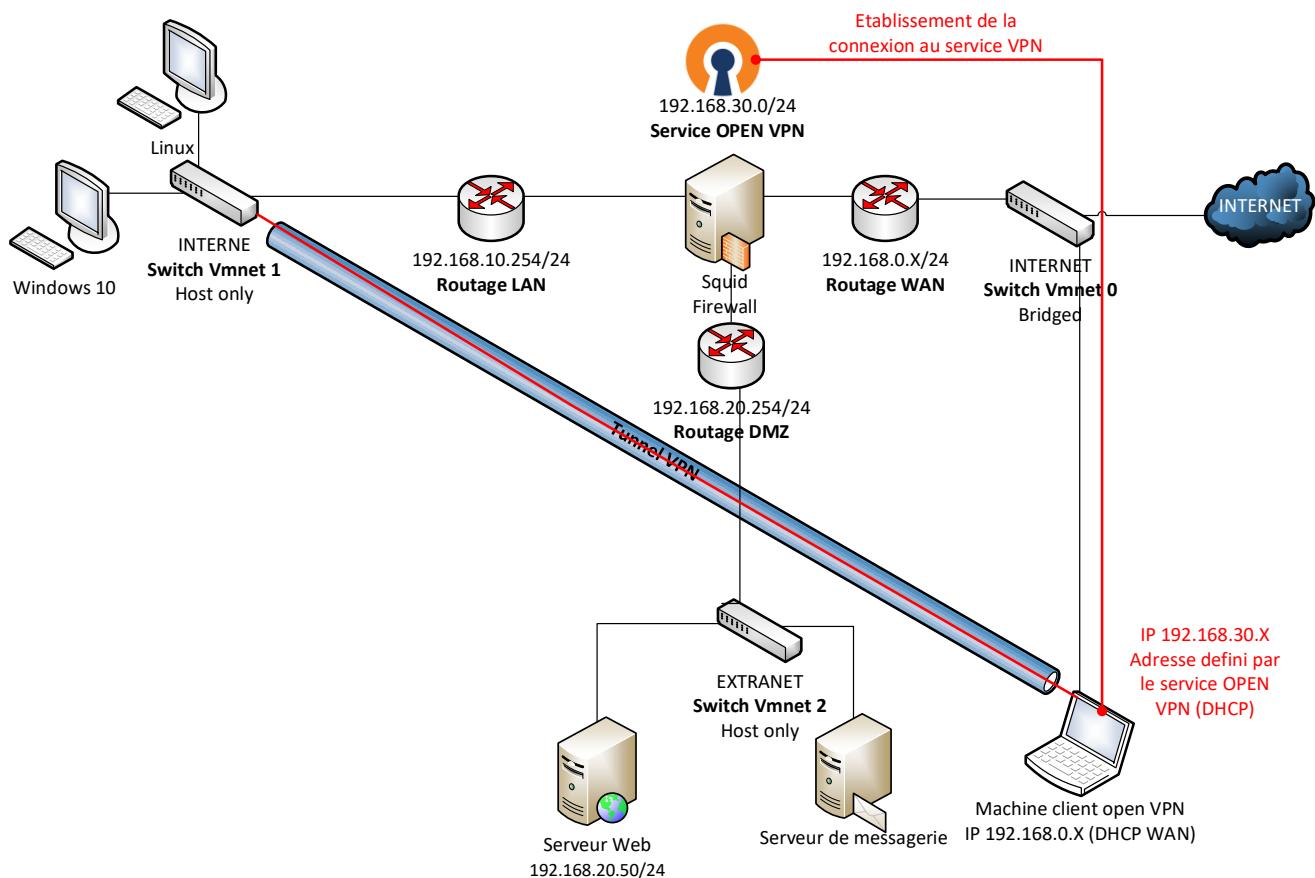
<i>Introduction OpenVPN.....</i>	3-2
<i>Configuration du serveur OpenVPN.....</i>	3-3
<i>Création d'un utilisateur VPN.....</i>	3-8
<i>Configuration et installation du client OpenVPN.....</i>	3-10

Introduction OpenVPN

OpenVPN est un service VPN libre (GNU GPL) permettant de connecter des utilisateurs distants sur un réseau d'entreprise avec un maximum de sécurité, en effet la connexion à celui-ci demande en plus d'un compte utilisateur et de mot de passe, un certificat délivré par le serveur qui devra être installé sur le client de connexion.

OpenVPN créera un sous réseau dans le tunnel (192.168.30.0 dans notre exemple) permettant ainsi de se connecter sur le réseau local en toute sécurité en utilisant OpenSSL contenant les protocoles de chiffrement (SSLv3/TLSv1 et création de certificat).

Le port par défaut OpenVPN est le 1194 en UDP



Configuration du serveur OpenVPN

Cliquer sur le menu **VPN** puis **OpenVPN**

The screenshot shows the Pfsense web interface. At the top, there's a navigation bar with links for Système, Interfaces, Pare-feu, Services, VPN (which is currently selected), État, Diagnostics, and Aide. Below the navigation bar, a red warning message says: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." On the left, there's a sidebar with "État / Tableau de bord". The main content area has two sections: "Informations système" (System Information) and "Netgate Services And Support". Under "Informations système", it shows "Nom" as "pfSense-luis.Formation" and "Utilisateur" as "admin@192.168.10.53 (Local Database)". Under "Netgate Services And Support", it shows "Contract type" as "Community Support" and "Community Support Only". A modal window titled "Outil Capture d'écran" is open in the top right corner.

A partir de là il faudra sélectionner **Assistants**

The screenshot shows the Pfsense web interface with the "VPN / OpenVPN / Serveurs" section selected. The "Assistants" tab is highlighted in yellow. Below it, there's a table titled "Serveurs OpenVPN" with columns for Interface, Protocole / Port, Réseau tunnel, Chiffrement, Description, and Actions. A green "Ajouter" button is visible at the bottom right of the table area.

Les utilisateurs seront ceux de Pfsense, cliquer ensuite sur **Next**

The screenshot shows the "OpenVPN Remote Access Server Setup" wizard. The current step is "Select an Authentication Backend Type". It shows a dropdown menu set to "Local User Access" and a note: "NOTE: If unsure, leave this set to "Local User Access."" A yellow "Next" button is at the bottom of the screen.

Ici c'est la création de l'autorité de certificat dans lequel on renseigne le Nom descriptif **CA-VPN**. Le code pays **FR** l'état ou province **Île-de-France**, la ville **Rubelles** et l'organisation **Formation** bien entendu ces infos seront différentes et pas obligatoire.

Cliquer ensuite sur **Add New CA**

Assistant / OpenVPN Remote Access Server Setup / Add Certificate Authority

Etape 6 de 11

Add Certificate Authority

OpenVPN Remote Access Server Setup Wizard

Create a New Certificate Authority (CA) Certificate

Nom descriptif: CA-VPN
A name for administrative reference, to identify this certificate. This is the same as common-name field for other Certificates.

Longueur de la clé: 2048 bit

Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see [keylength.com](#)

Durée de vie: 3650
Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)

Code du pays: FR
Two-letter ISO country code (e.g. US, AU, CA)

État ou province: Île-de-France
Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).

Ville: Rubelles
City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

Organisation: Formation
Organization name, often the Company or Group name.

» Add new CA

C'est ici que nous allons créer le certificat pour le serveur OpenVPN.
Il suffit de lui donner un autre nom ici **SVR-VPN** puis cliquer sur **Create new Certificate**

Assistant / OpenVPN Remote Access Server Setup / Add a Server Certificate

Etape 8 de 11

Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

Create a New Server Certificate

Nom descriptif: SVR-VPN
A name for administrative reference, to identify this certificate. This is also known as the certificate's "Common Name."

Longueur de la clé: 2048 bit

Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see [keylength.com](#)

Durée de vie: 398
Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Code du pays: FR
Two-letter ISO country code (e.g. US, AU, CA)

État ou province: Île-de-France
Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).

Ville: Rubelles
City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

Organisation: Formation
Organization name, often the Company or Group name.

» Create new Certificate

Nous voici arrivé au paramétrage du réseau.

Les connexions se feront par l'entrée **WAN** le protocole **UDP** et le port **1194** sont par défaut.
On peut rajouter une description ici **VPN-Formation**

General OpenVPN Server Information

Interface	WAN	▼
The interface where OpenVPN will listen for incoming connections (typically WAN.)		
Protocole	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	VPN-Formation	×
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.		

On laisse par défaut l'authentification TLS et la régénération de clef partagé.

Quand on reviendra à cet écran par la suite une suite de clefs sera régénérée et visible dans TLS Shared Key.

Paramètres cryptographiques

Authentification TLS	<input checked="" type="checkbox"/>	Enable authentication of TLS packets.
Generate TLS Key	<input checked="" type="checkbox"/>	Automatically generate a shared TLS authentication key.
TLS Shared Key	<input type="text"/>	
Paste in a shared TLS key if one has already been generated.		
DH Parameters Length	2048 bit	▼
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.		
Encryption Algorithm	AES-128-CBC (128 bit key, 128 bit block)	▼
The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.		
Auth Digest Algorithm	SHA256 (256-bit)	▼
The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.		
Chiffrement matériel	Pas d'accélération cryptographique matérielle	▼
The hardware cryptographic accelerator to use for this VPN connection, if any.		

Le réseau tunnel sera le réseau qui sera utilisé par le VPN ici un autre réseau **192.168.30.0/24** avec le CIDR.

Dans Local Network c'est tout simplement le réseau local que l'on souhaite atteindre donc ici **192.168.10.0/24** toujours le CIDR.

Définissez le nombre de connexion au réseau VPN maximum, ici **10**.

Paramètres du tunnel

Réseau tunnel	192.168.30.0/24	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.
Passerelle de redirection	<input type="checkbox"/>	Forcer tout le trafic générée par le client à travers le tunnel.
Local Network	192.168.10.0/24	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	10	Spécifier le nombre maximum de clients autorisés à se connecter en même temps à ce serveur.
Compression	<input checked="" type="checkbox"/> Ne pas préciser de préférence (Utilisation de OpenVPN par défaut)	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 de service	<input type="checkbox"/>	Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication	<input type="checkbox"/>	Allow communication between clients connected to this server.
Duplicate Connections	<input type="checkbox"/>	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 suffit ensuite de renseigner le DNS 1 **192.168.10.254** et éventuellement DNS 2 **8.8.8.8**

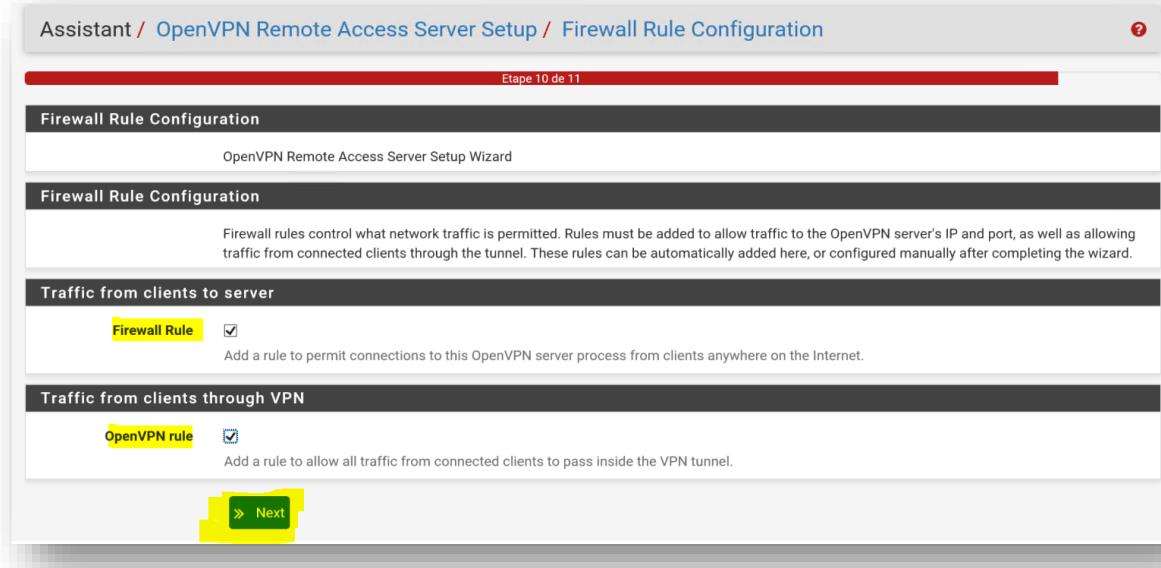
Cliquez sur Next

Paramètres du client

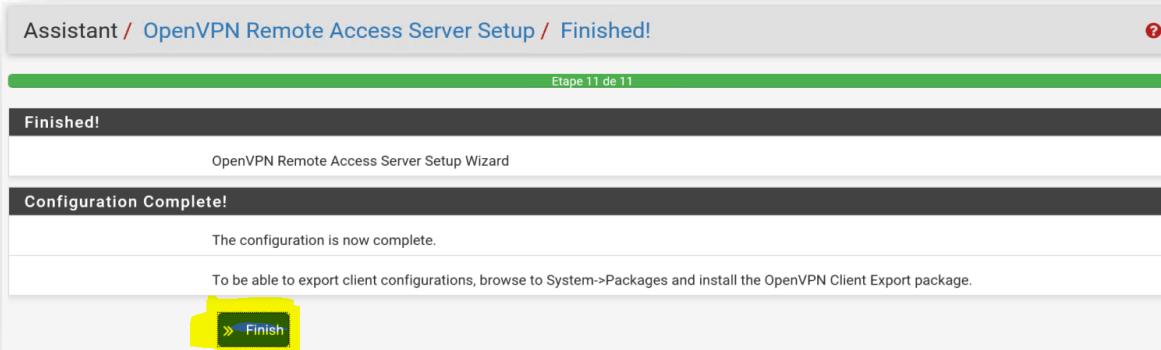
IP dynamique	<input checked="" type="checkbox"/>	Autoriser les clients connectés à conserver leurs connexions si leur adresse IP change.
Topologie	Sous-réseau – Une adresse IP par client dans ce sous-réseau	Specifies the method used to supply a virtual adapter IP address to clients when using tun mode 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".
Domaine DNS par défaut	<input type="text"/>	Provide a default domain name to clients.
Serveur DNS 1	192.168.10.254	DNS server IP to provide to connecting clients.
Serveur DNS 2	8.8.8.8	DNS server IP to provide to connecting clients.
Serveur DNS 3	<input type="text"/>	DNS server IP to provide to connecting clients.
Serveur DNS 4	<input type="text"/>	DNS server IP to provide to connecting clients.

Cocher ensuite les case **firewall rules** et **OpenVPN rules** ce qui permet d'autoriser le traffic à travers le FIREWALL.

Puis **Next**



Cliquer sur **Finish** pour terminer la configuration.



Voici la configuration du serveur terminé

VPN / OpenVPN / Serveurs					
Serveurs	Clients	Ré-écritures spécifiques au client	Assistants		
Serveurs OpenVPN					
Interface	Protocole / Port	Réseau tunnel	Chiffrement	Description	Actions
WAN	UDP4 / 1194	192.168.30.0/24	Crypto: AES-128-CBC/SHA256 D-H Params: 2048 bits	VPN-Formation (tun)	

Création d'un utilisateur VPN

Pour la création de l'utilisateur il faut aller dans **Système** puis **Gestionnaire d'usagers**

tunnel	Chiffrement	Description	Actions
8.30.0/24	Crypto: AES-128-CBC/SHA256 D-H Params: 2048 bits	VPN-Formation (tun)	

Puis cliquer sur **Ajouter**

Nom d'utilisateur	Nom complet	État	Groupes	Actions
admin	System Administrator	✓	admins	

Il faut créer un compte utilisateur et en même temps un certificat qui sera rattaché à cet utilisateur. Tout d'abord renseigner le nom de l'utilisateur ici **LUIS-VPN** ainsi que son **mot de passe**. Vous pouvez lui donner un **nom complet** ainsi que la **date d'expiration**. Enfin il faudra cocher la case **Certificat** pour générer le certificat de ce utilisateur.

Système / Gestionnaire d'usagers / Utilisateurs / Modifier

Utilisateurs Groupes Paramètres Serveurs d'authentification

Propriétés utilisateur

Défini par: USER

Désactivé: Cet utilisateur ne peut pas s'authentifier

Nom d'utilisateur: LUIS-VPN

Mot de passe: *****

Nom complet: Luis De Oliveira
Nom complet de l'utilisateur, à des fins administratives uniquement

Date d'expiration: 12/31/2020
Laissez vide si le compte ne doit pas expirer, sinon entrez la date d'expiration sous la forme MM/JJ/AAAA

Paramètres personnalisés: Utilisez les options GUI individuelles personnalisées et la disposition du tableau de bord pour cet utilisateur.

Appartenance à un groupe: admins

Pas un membre de: Membre de:

Maintenez la touche CTRL (PC)/COMMAND (Mac) enfournée pour sélectionner plusieurs éléments.

Certificat: Cliquez pour créer un certificat client

Puisque le certificat client a été coché il faut renseigner un nom descriptif **CA-LUIS-VPN** ainsi que l'autorité de certification **CA-VPN** créer précédemment puis cliquer sur **Enregistre**

Créer un certificat pour l'utilisateur

Nom descriptif: CA-LUIS-VPN

Autorité de certification: CA-VPN

Longueur de la clé: 2048 bits

Plus la clé est grande, plus la sécurité qu'elle offre, mais les clés plus importantes prennent beaucoup plus de temps à générer, et prennent un peu plus de temps pour valider, ce qui entraîne un léger ralentissement lors de la création de nouvelles sessions (pas toujours perceptible). À partir de 2016, 2048 bits est la sélection minimale et la plus commune et 4096 est le maximum d'utilisation courante. Pour plus d'informations, voir [keylength.com](#).

Durée de vie: 3650

Clés

Clés SSH autorisées: Entrez les clés SSH autorisées pour cet utilisateur

Clé pré-partagée IPsec:

Enregistrer

Voici le résultat que Final

Utilisateurs	Nom d'utilisateur	Nom complet	Etat	Groupes	Actions
LUIS-VPN	Luis De Oliveira	✓	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	
admin	System Administrator	✓	admins	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

Ajouter **Supprimer**

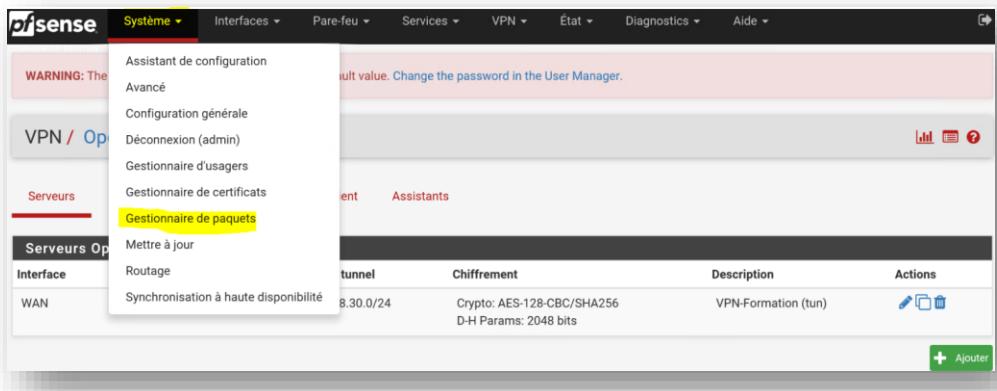
Configuration et installation du client OpenVPN

Il faut maintenant récupérer le client qui contient le certificat ainsi que toute la configuration pour qu'il puisse se connecter.

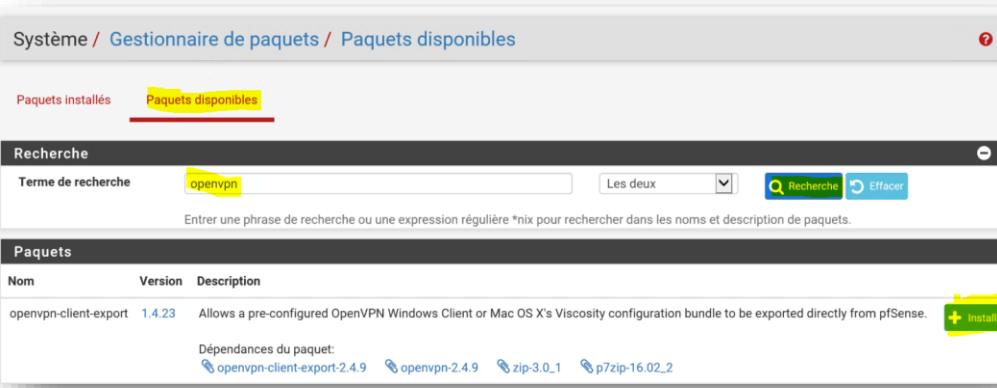
Pour l'installation du client, il existe un paquet d'export du certificat qui intègre le logiciel client.

Il va falloir installer ce paquet

L'installation se fait depuis **Système** puis **Gestionnaire de paquets**



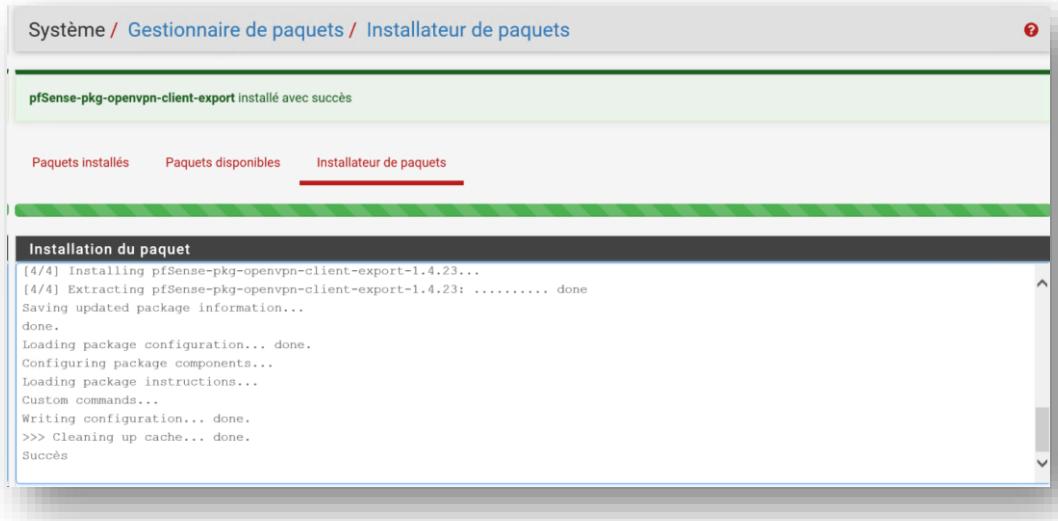
Ensute il suffit de sélectionner **Paquet disponibles** puis dans Terme de recherche taper **openvpn** et rechercher et enfin **Install** du paquet **openvpn-client-export**



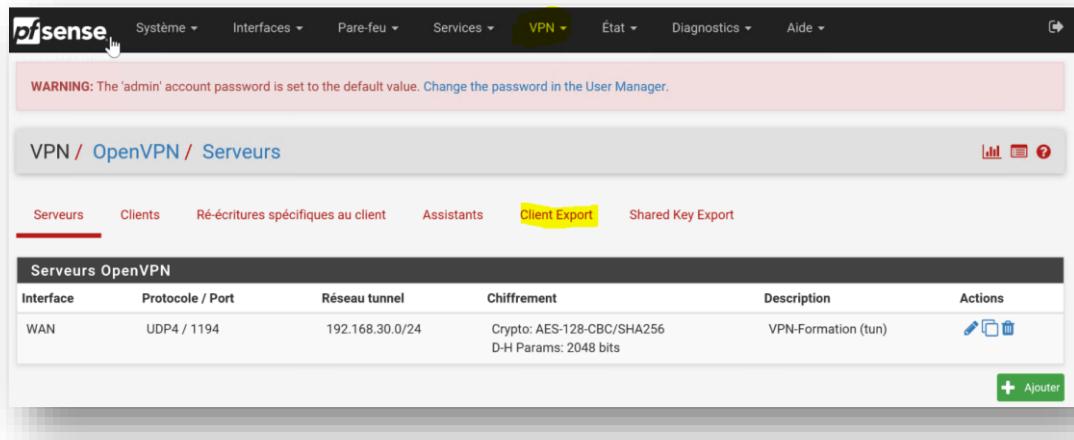
Cliquer sur **Confirmer**



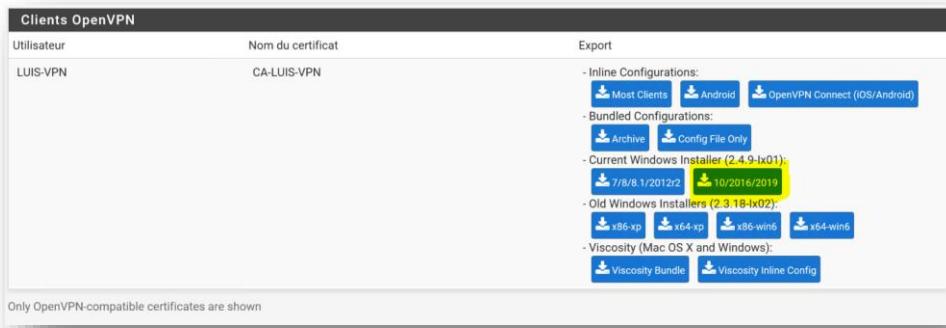
Un fois installé voici le résultat



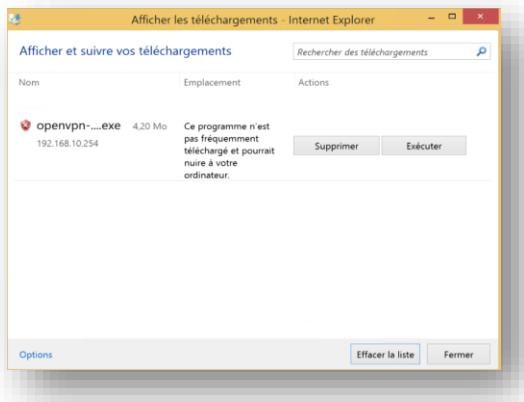
Il faut maintenant récupérer le client pour le transférer sur la machine qui sera client VPN.
Pour cela allez dans **VPN** puis **OPENVPN** et cliquer sur **Client Export** (c'est ce qu'il a été installé précédemment)



Rendez-vous sur Client OpenVPN puis sélectionner le client OpenVPN en fonction du système d'exploitation (**ici W10**)



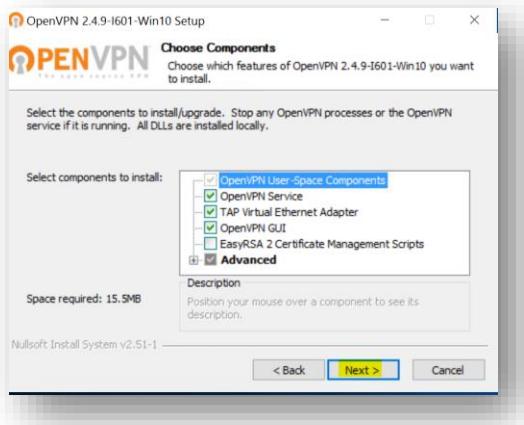
Une fois que le client a été téléchargé il est placé dans le répertoire des téléchargements.



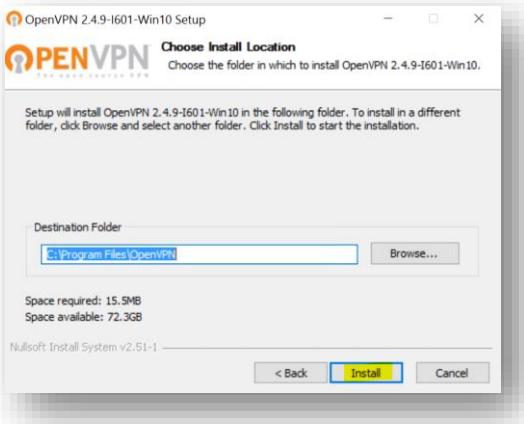
Prenez le fichier et installer le sur la machine qui sera client VPN.
Cliquer sur l'exécutable.



Cliquez sur **Next**



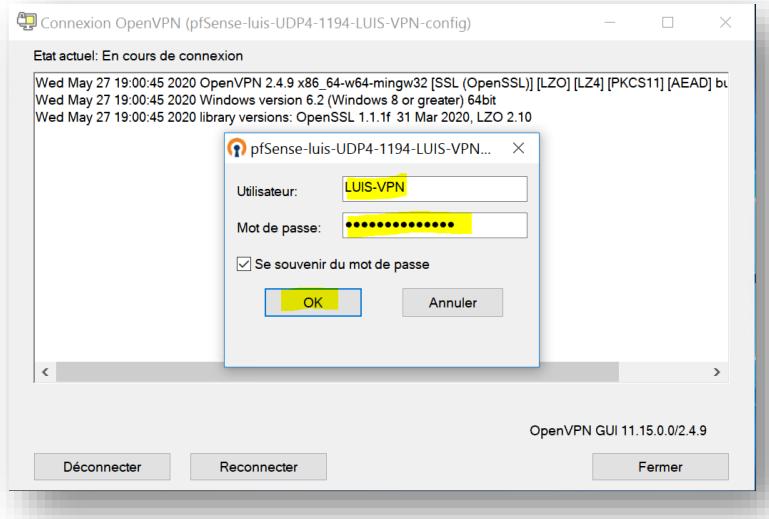
Puis **Install**



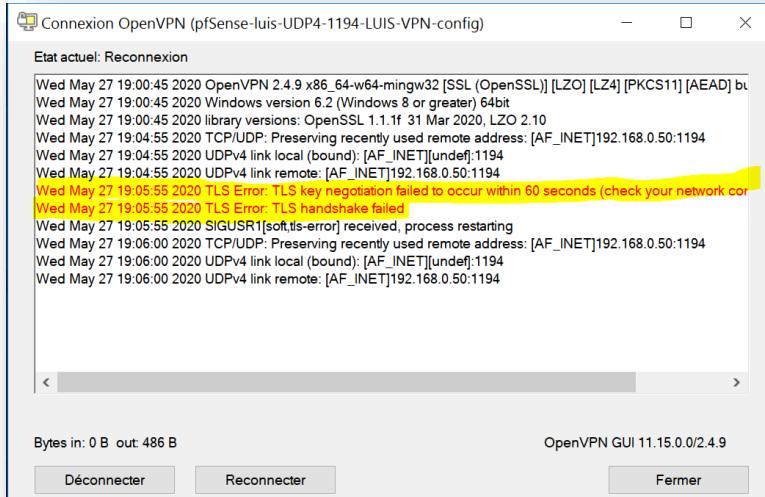


Pour le lancement du VPN cliquer sur l'icône

Puis renseigner les champs comme le compte **utilisateur** et le **mot de passe** puis **ok**



Si vous avez ces erreurs là en rouge c'est normal car PFSENSE bloque automatiquement depuis le LAN les réseau Privés



Il faut simplement dans la configuration du **pare feu** puis **Règles**



On s'aperçoit que la règle dans le WAN bloque les réseaux privés, ce qui est normal car une connexion client en VPN ne vient pas de ces réseaux mais de réseau Public.

Comme ici on fait du Lab ça bloque.

Il suffit de dé-valider cette règle pour que tout rentre dans l'ordre

Pour cela cliquer sur l'engrenage pour modifier les règles.

Etats	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
<input checked="" type="checkbox"/>	0 / 590 KIB	*	Réseaux RFC 1918	*	*	*	*	*	Bloquer les réseaux privés	
<input checked="" type="checkbox"/>	0 / 6 KIB	*	Réservee Non assignées par l'IANA	*	*	*	*	*	Bloquer les réseaux invalides	
<input type="checkbox"/>	0 / 0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	aucun	Assistant VPN-Formation OpenVPN	

Tout en bas du paramétrage **WAN** décocher **bloquer les réseaux privé et les adresse de loopback**
Puis n'oublier pas **d'enregistrer**

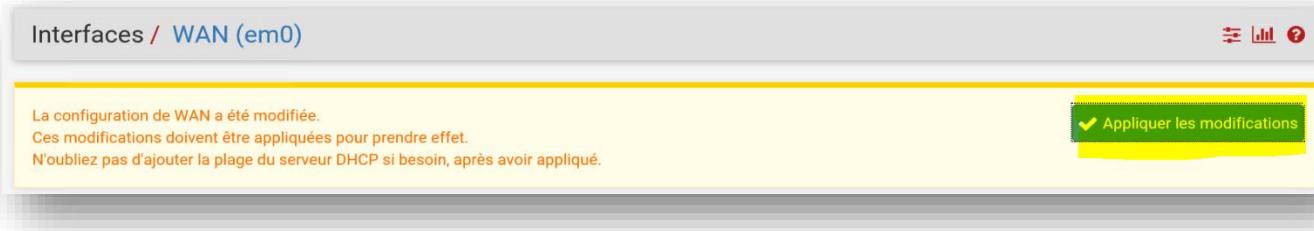
Réseaux réservés

Bloquer les réseaux privés et les adresses de loopback Bloque le trafic depuis des adresses IP qui sont réservées pour les réseaux privés (RFC 1918: 10/8, 172.16/12, 192.168/16), les adresses locales uniques (RFC 4193: fc00::/7) et les adresses de boucle locale (127/8). Cette option doit généralement être activée, sauf si l'interface réseau est également dans un réseau privé.

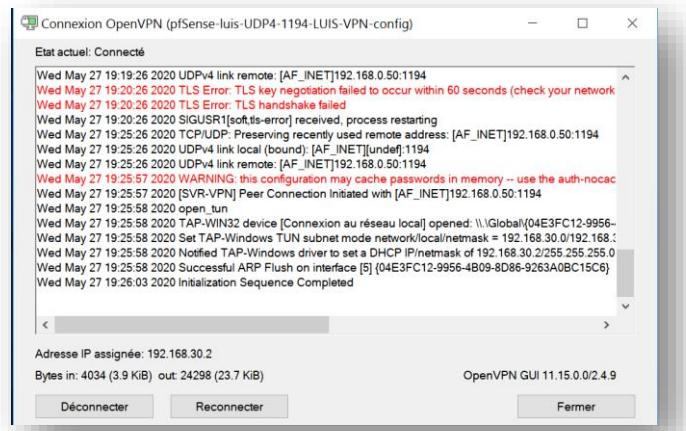
Bloquer les réseaux invalides Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Enregistrer **Activer Win**

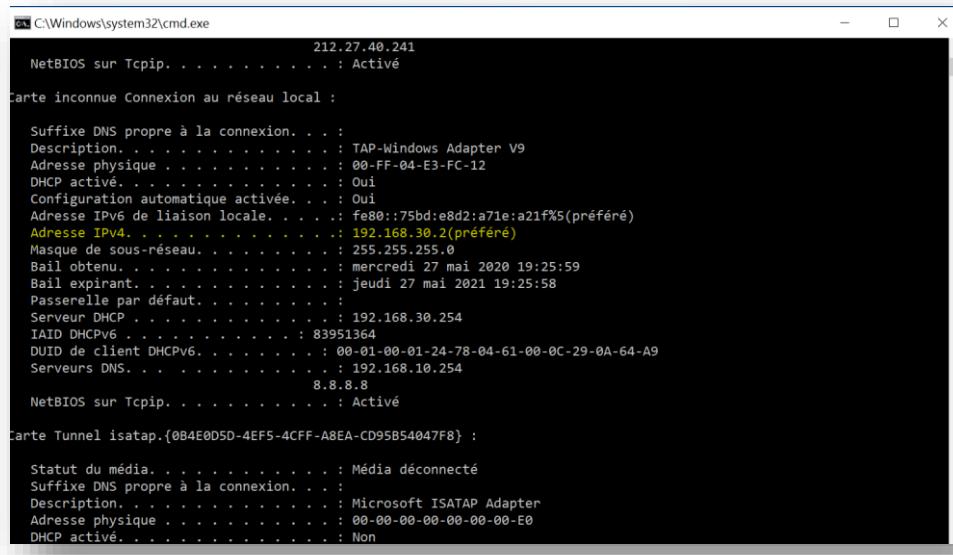
Et enfin en haut de page **d'appliquer les modifications**



Cette fois-ci si l'on retourne sur la machine cliente, la connexion est bien réalisée



Depuis la commande IPCONFIG /ALL la machine client à bien reçu une IP correspondante au réseau VPN qui était 192.168.30.0/24



Depuis la configuration de PFSENSE depuis le menu **Etat** puis **OpenVPN**



On visualise les connexions en cours

A screenshot of the 'OpenVPN' status page. The title bar says 'État / OpenVPN'. Below it is a table titled 'VPN-Formation UDP4:1194 Connections clients'. The table has columns: Nom commun, Adresse réelle, Adresse virtuelle, Connecté depuis, Bytes Sent, and Bytes Received. There is one entry: LUIS-VPN, 192.168.0.6:1194, 192.168.30.2, Wed May 27 17:25:56 2020, 7 KiB, 24 KiB. At the bottom left, it says 'État: ✓ Actions: C O'. At the bottom right, there is a link 'Afficher les tables de routage'.

Notes Personnel
