

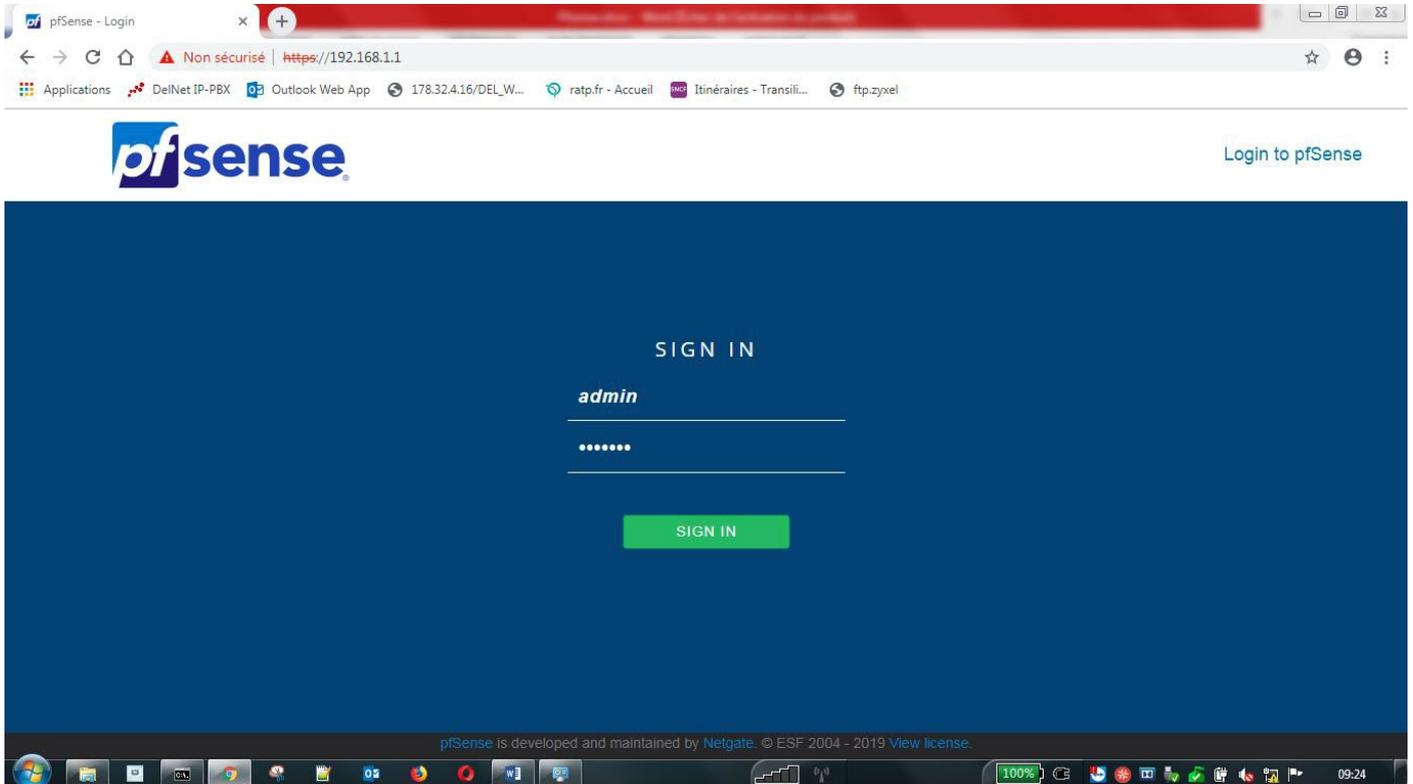
Procédure : Configuration pfSense.

Sommaire

1/- Configuration du pfSense.....	3
2/- Configuration de l'IDS SNORT.....	10
3/- Configuration du Proxy SQUID.....	18
4/- Configuration d'une connexion nomade - OpenVPN.....	29
5- Configuration d'une protection sur la page d'administration.....	37

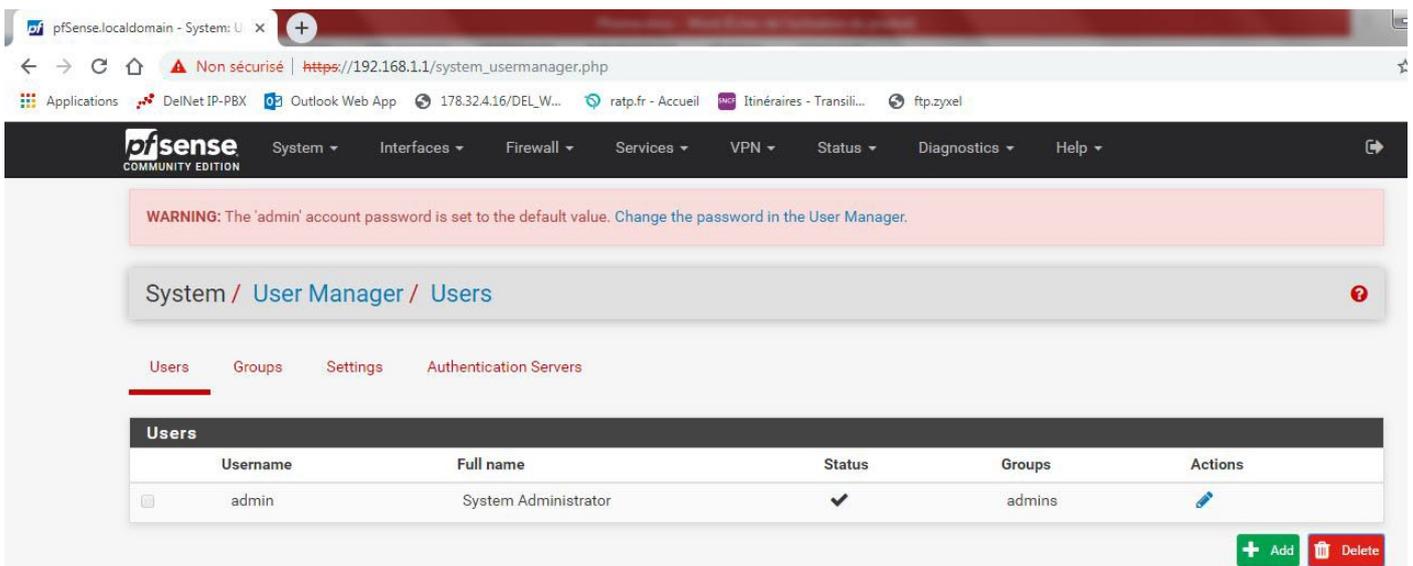
1/- Configuration du pfSense.

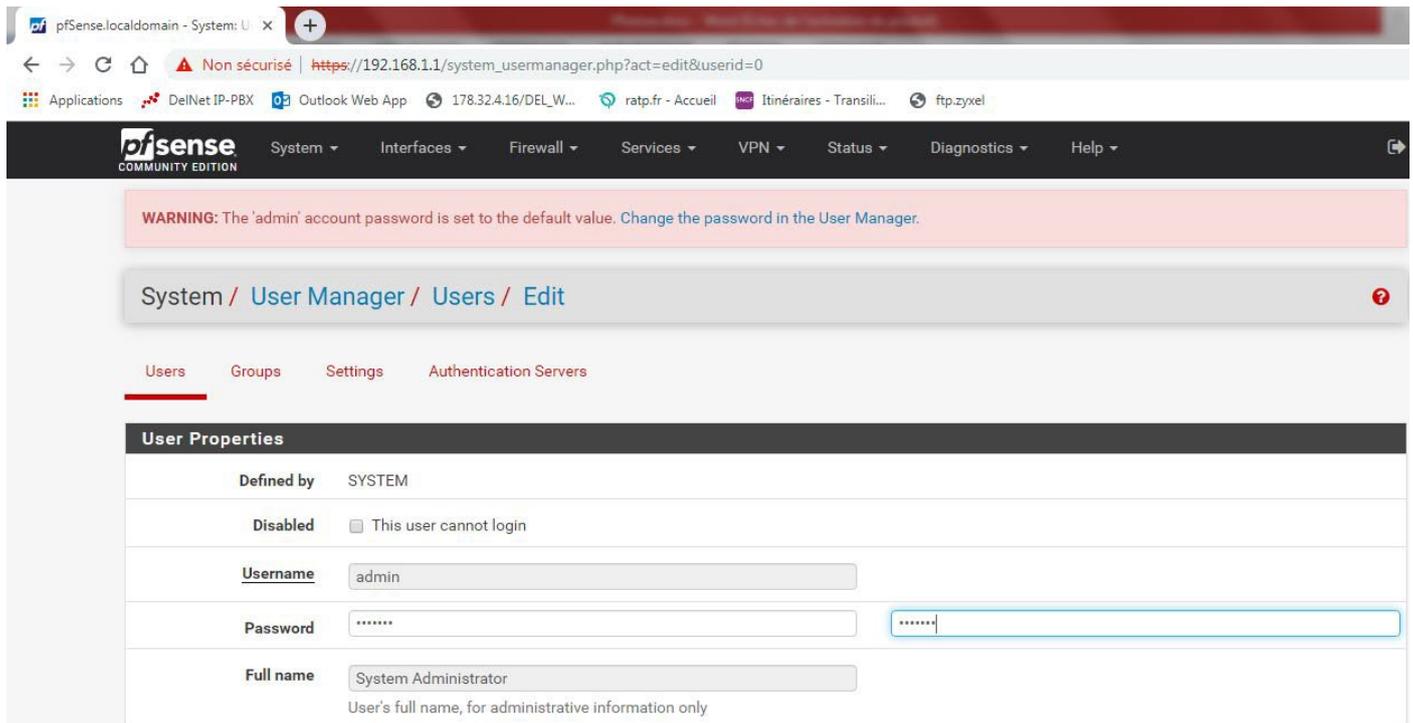
Se connecter sur la page de configuration du pfsense par défaut : <https://192.168.1.1> (avec DHCP) et entrer les identifiants par défaut : admin / pfsense.



Mot de passe :

Changer le mot de passe administrateur dans System > User Manager > Users.





Enregistrer le mot de passe en cliquant sur Save en bas de la page.

Configuration de base :

Aller dans System > General setup et donner un nom, une zone de temps et choisir une langue pour votre routeur.

Système	
Nom d'hôte	<input type="text" value="ROUTEUR"/> Nom d'hôte du pare-feu, sans le nom de domaine
Domaine	<input type="text" value="DEL-NET.COM"/> Ne pas utiliser '.local' comme la partie finale du domaine (TLD), le domaine '.local' est utilisé en mode large par mDNS (y compris Avahi et Apple OS X Bonjour / Rendezvous / Airprint / Airplay), et certains systèmes Windows et périphériques en réseau. Ceux-ci ne se connecteront pas correctement si le routeur utilise '.local'. Des alternatives telles que '.local.lan' ou '.mylocal' sont sécurisées.
Paramètres du serveur DNS	
Serveurs DNS	<input type="text" value="DNS Server"/> <input type="text" value="DNS Hostname"/> <input type="text" value="aucun"/>
Ajouter un serveur DNS	+ Ajouter un serveur DNS
Remplacer le serveur DNS	<input checked="" type="checkbox"/> Autoriser la liste des serveur DNS être écrasée par DHCP/PPP sur le WAN Si cette option est définie, pfSense utilisera des serveurs DNS attribués par un serveur DHCP/PPP sur le WAN pour ses propres besoins (y compris le DNS Forwarder / DNS Resolver). Cependant, ils ne seront pas affectés à des clients DHCP.
Désactiver le redirecteur DNS	<input type="checkbox"/> Ne pas utiliser le DNS Forwarder/DNS Resolver comme serveur DNS pour le pare-feu Par défaut, localhost (127.0.0.1) sera utilisé comme le premier serveur DNS dans lequel le DNS Forwarder et le DNS Resolver sont activés et réglés pour écouter sur localhost. Ainsi le système pourra utiliser le service DNS local pour effectuer ses recherches. Activer cette option retire localhost de la liste des serveurs DNS dans le fichier resolv.conf
Localisation	
Fuseau horaire	<input type="text" value="Europe/Paris"/> Sélectionner un nom de région géographique (Continent/Lieu) afin de déterminer le fuseau horaire pour le pare-feu. Choisir une zone spéciale ou "Etc" seulement dans le cas où la zone géographique ne gère pas convenablement le décalage d'horloge pour ce pare-feu.
Serveurs de temps	<input type="text" value="0.pfsense.pool.ntp.org"/> Utilisez un espace pour séparer plusieurs hôtes (un seul requis). Au moins un serveur DNS devra être configuré si vous entrez un nom d'hôte ici!
Langue	<input type="text" value="Français"/> Choisissez une langue pour le configurateur Web

Adresse IP routeur :

Allers dans Interface > LAN puis changer l'adresse IP du routeur sans appliquer les modifications.

Interfaces / LAN (em1)	
Configuration générale	
Activer	<input checked="" type="checkbox"/> Activer interface
Description	<input type="text" value="LAN"/> Entrez ici une description (nom) pour cette interface.
Type de configuration IPv4	<input type="text" value="IPv4 statique"/>
Type de configuration IPv6	<input type="text" value="Interface de suivie"/>
Adresse MAC	<input type="text" value="xxxxxxxxxxxx"/> Ce champ peut être utilisé pour modifier ("spoof") l'adresse MAC de cette interface. Entrez une adresse MAC au format suivant : xx:xx:xx:xx:xx:xx ou laissez vide.
MTU	<input type="text"/> Si ce champ est laissé vide, la valeur MTU par défaut de la carte réseau est utilisée. En général 1 500 octets, mais peut varier dans certaines circonstances.
MSS	<input type="text"/> Si vous renseignez ce champ, alors la valeur utilisée pour MSS clamping sera la valeur indiquée moins 40 (taille de l'entête TCP/IP).
Vitesse et Duplex	<input type="text" value="Par défaut (aucune préférence, habituellement une auto-sélection)"/> Forcer la vitesse et le mode duplex pour cette interface. ATTENTION: doit être défini sur autoselect (vitesse négociée automatiquement) à moins que la vitesse et duplex du port auquel cette interface est connectée soit aussi forcé.
Configuration statique IPv4	
Adresse IPv4	<input type="text" value="192.168.120.1"/> / <input type="text" value="24"/>

DHCP :

Aller dans Services > Serveur DHCP

Configurer la plage DHCP et renseigner passerelle et DNS.

Options générales	
Activer	<input checked="" type="checkbox"/> Activer le serveur DHCP sur l'interface LAN
BOOTP	<input type="checkbox"/> Ignorer les requêtes BOOTP
Rejeter les clients inconnus	<input type="checkbox"/> Seuls les clients définis ci-dessous obtiendront des bails DHCP de ce serveur.
Ignorer les clients inconnus	<input type="checkbox"/> Les clients refusés seront ignorés plutôt que rejetés Cette option n'est pas compatible avec le failover et ne peut pas être activée lorsqu'une adresse Failover Peer IP est configurée.
Ignorer les identifiants clients	<input type="checkbox"/> Si un client inclut un identifiant unique dans sa requête DHCP, cet UID ne sera pas enregistré dans son bail. Cette option peut être utile lorsqu'un client peut dual boot en utilisant différents identifiants client, mais avec la même adresse matérielle (MAC). Notez que ce comportement du serveur est contraire aux spécifications officielles de DHCP.
Sous-réseau	192.168.1.0
Masque de sous-réseau	255.255.255.0
Plage disponible	192.168.1.1 - 192.168.1.254
Plage	De <input type="text" value="192.168.120.100"/> À <input type="text" value="192.168.120.199"/>

Serveurs	
Serveurs WINS	<input type="text" value="WINS Server 1"/>
	<input type="text" value="WINS Server 2"/>
Serveurs DNS	<input type="text" value="192.168.120.1"/>
	<input type="text" value="8.8.8.8"/>
	<input type="text" value="DNS Server 3"/>
	<input type="text" value="DNS Server 4"/>
Laissez vide pour utiliser les serveurs DNS par défaut du système: l'IP de cette interface si DNS Forwarder ou Resolver est activé, sinon les serveurs sont configurés sur la page Système / Configuration Générale.	
Autres options	
Passerelle	<input type="text" value="192.168.120.1"/>
La valeur par défaut est d'utiliser l'IP sur cette interface du pare-feu en tant que passerelle. Spécifiez une autre passerelle ici si ce n'est pas la bonne passerelle pour le réseau. Tapez "none" si vous voulez affecter aucune passerelle.	

Option 66 – VOIP :

Dans Services > Serveur DHCP vous pouvez configurer des options.

Options BOOTP/DHCP additionnelles

Entrez le numéro de l'option DHCP et la valeur associée pour chaque élément à inclure dans les options de bail DHCP. Pour obtenir une liste des options, visitez cette URL .

Option	<input type="text" value="66"/>	<input type="text" value="Texte"/>	<input type="text" value="https://delnet3cx.my3cx"/>
	Nombre	Type	Valeur
Ajouter	<input type="button" value="+ Ajouter"/>		

Appliquer les modifications puis se connecter sur la nouvelle adresse IP :

Interfaces / LAN (em1) ☰ 📊 ⓘ

La configuration de LAN a été modifiée.
Ces modifications doivent être appliquées pour prendre effet.
N'oubliez pas d'ajouter la plage du serveur DHCP si besoin, après avoir appliqué.

Changer port :

Aller dans Système > Avancé > Accès Administrateur et changer le port de connexion au routeur.

Système / Avancé / Accès administrateur

Accès administrateur Pare-feu et NAT Mise en réseau Divers Ajustements Systèmes Notifications

webConfigurator

Protocole HTTP HTTPS

Certificat SSL

Port TCP

Entrez un numéro de port personnalisé pour le webCOnfigurator afin de remplacer celui par défaut (80 pour HTTP et 443 pour HTTPS). Les changements seront effectifs dès sauvegarde.

4/- Configuration d'une connexion nomade - OpenVPN.

Création d'une Autorité de certification :

Donner un nom à l'autorité de certification.

Système / Gestionnaire de certificats / ACs / Modifier ?

ACs Certificats Révocation de certificat

Créer / Modifier l'AC

Nom descriptif

Méthode

Autorité de certification interne

Longueur de la clé (bits)

Algorithme de hachage
REMARQUE: Il est recommandé d'utiliser un algorithme plus fort que SHA1 lorsque cela est possible.

Durée de vie (jours)

Nom commun

Les composantes suivantes de l'autorité de certification sont facultatives et peuvent être laissées vides.

Code du pays

Création d'un certificat pour le serveur VPN :

Donner un nom à notre certificat, sélectionner l'autorité de certification précédemment créée, choisir le type de certificat (serveur) et indiquer le nom et/ou adresse IP de la connexion WAN.

ACs **Certificats** Révocation de certificat

Ajouter/Signer un nouveau certificat

Méthode Créer un certificat interne ▼

Nom descriptif SRV-OpenVPN

Certificat interne

Autorité de certification PFSense-CA ▼

Longueur de la clé 2048 ▼

Algorithme de hachage sha256 ▼
REMARQUE: Il est recommandé d'utiliser un algorithme plus fort que SHA1 lorsque cela est possible.

Durée de vie (jours) 3650

Nom commun OpenVPN.del-net.com.fr

Les éléments suivants sont facultatifs et peuvent être laissés vides.

Code du pays FR ▼

Attributs de certificat

Notes d'attributs Les attributs suivants sont ajoutés aux certificats et aux requêtes lorsqu'ils sont créés ou signés. Ces attributs se comportent différemment en fonction du mode sélectionné.
Pour les certificats internes, ces attributs sont ajoutés directement au certificat comme indiqué.

Type de certificat Server Certificate ▼
Ajoutez les attributs d'utilisation spécifiques au certificat signé. Utilisé pour placer les restrictions d'utilisation ou l'octroi de capacités au certificat signé.

Noms alternatifs	Type	Valeur
Adresse IP ▼		92.154.37.50

Entrez des identifiants supplémentaires pour le certificat dans cette liste. Le champ Nom commun est automatiquement ajouté au certificat en tant que nom alternatif. La signature CA peut ignorer ou modifier ces valeurs.

Ajouter + Ajouter

📄 Enregistrer

Installation du paquet OpenVPN-Client-Export :

Système / Gestionnaire de paquets / Paquets disponibles

Paquets installés **Paquets disponibles**

Recherche

Terme de recherche Les deux

Entrer une phrase de recherche ou une expression régulière *nix pour rechercher dans les noms et description de paquets.

Paquets

Nom	Version	Description
openvpn-client-export	1.4.18_4	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.

+ Install

Dépendances du paquet:
[openvpn-client-export-2.4.7](#) [openvpn-2.4.6_1](#) [zip-3.0_1](#) [p7zip-16.02_1](#)

Lancement de l'assistant :

VPN > OpenVPN > Assistant :

Laisser Local User Access.

Assistant / OpenVPN Remote Access Server Setup /

OpenVPN Remote Access Server Setup

This wizard will provide guidance through an OpenVPN Remote Access Server Setup .

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Select an Authentication Backend Type

Type of Server

NOTE: If unsure, leave this set to "Local User Access."

Indiquer l'autorité de certification que nous avons créé.

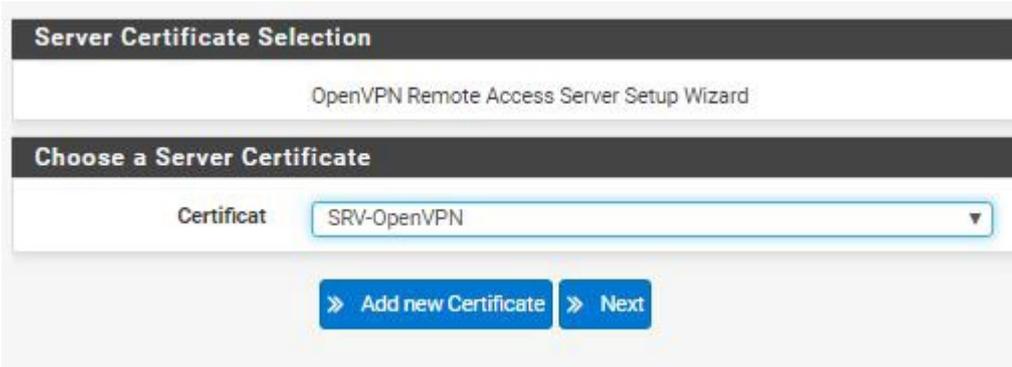
Certificate Authority Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Certificate Authority (CA)

Autorité de certification

Indiquer le certificat serveur que nous avons créé.



Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Server Certificate

Certificat: SRV-OpenVPN

» Add new Certificate » Next

Indiquer un port à utiliser pour le VPN qu'il faudra ouvrir dans le pare-feu.



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.)

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:
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.

Renseigner une adresse réseau pour le VPN.

Cocher la redirection du trafic.

Renseigner l'adresse réseau local à laquelle le VPN aura accès.

Renseigner les serveurs DNS.

Paramètres du tunnel	
Réseau tunnel	<input type="text" value="192.168.150.0/24"/> <small>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.</small>
Passerelle de redirection	<input checked="" type="checkbox"/> <small>Forcer tout le trafic généré par le client à travers le tunnel.</small>
Local Network	<input type="text" value="192.168.120.0/24"/> <small>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.</small>
Concurrent Connections	<input type="text"/> <small>Spécifier le nombre maximum de clients autorisés à se connecter en même temps à ce serveur.</small>
Compression	<input type="text" value="Ne pas préciser de préférence (Utilisation de OpenVPN par défaut)"/> <small>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.</small>
Type de service	<input type="checkbox"/> <small>Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.</small>
Inter-Client Communication	<input type="checkbox"/> <small>Allow communication between clients connected to this server.</small>
Duplicate Connections	<input type="checkbox"/> <small>Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.</small>

Paramètres du client	
IP dynamique	<input checked="" type="checkbox"/> <small>Autoriser les clients connectés à conserver leurs connexions si leur adresse IP change.</small>
Topologie	<input type="text" value="Sous-réseau – Une adresse IP par client dans ce sous-réseau"/> <small>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".</small>
Domaine DNS par défaut	<input type="text"/> <small>Provide a default domain name to clients.</small>
Serveur DNS 1	<input type="text" value="192.168.120.1"/> <small>DNS server IP to provide to connecting clients.</small>
Serveur DNS 2	<input type="text" value="8.8.8.8"/> <small>DNS server IP to provide to connecting clients.</small>

Cocher la configuration automatique des règles de pare-feu.

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

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

Traffic from clients through VPN

OpenVPN rule

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

[» Next](#)

Création d'un utilisateur pour l'accès au VPN :

Système / Gestionnaire d'utilisateurs / Utilisateurs

Utilisateurs Groupes Paramètres Serveurs d'authentification

Utilisateurs

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

[+ Ajouter](#) [Supprimer](#)

Donner un nom à votre utilisateur et un mot de passe.

Cocher la création d'un certificat et choisir l'autorité de certification.

Propriétés utilisateur	
Défini par	USER
Désactivé	<input type="checkbox"/> Cet utilisateur ne peut pas s'authentifier
Nom d'utilisateur	<input type="text" value="VPN-SEB"/>
Mot de passe	<input type="password" value="****"/> <input type="password" value="****"/>
Nom complet	<input type="text"/> Nom complet de l'utilisateur, à des fins administratives uniquement
Date d'expiration	<input type="text"/> Laissez vide si le compte ne doit pas expirer, sinon entrez la date d'expiration sous la forme MM/JJ/AAAA
Paramètres personnalisés	<input type="checkbox"/> Utilisez les options GUI individuelles personnalisées et la disposition du tableau de bord pour cet utilisateur.
Appartenance à un groupe	<input type="text" value="admins"/> <input type="text"/> Pas un membre de Membre de
	<input type="button" value="» Déplacer vers la liste 'Membre de'"/> <input type="button" value="« Déplacer vers la liste 'Non membre de'"/>
	Maintenez la touche CTRL (PC)/COMMAND (Mac) enfoncée pour sélectionner plusieurs éléments.
Certificat	<input checked="" type="checkbox"/> Cliquez pour créer un certificat client
Créer un certificat pour l'utilisateur	
Nom descriptif	<input type="text" value="VPN-SEB"/>
Autorité de certification	<input type="text" value="PfSense-CA"/>
Longueur de la clé	<input type="text" value="2048 bits"/>

Dans la partie OpenVPN > Client Export Utility, choisir Autre au niveau "Host Name Résolution" et renseigner l'adresse IP de votre interface WAN.

The screenshot shows the pfSense web interface for the OpenVPN Client Export Utility. The navigation menu includes System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main heading is 'OpenVPN / Client Export Utility'. Below the heading are tabs for Server, Client, Client-specific Overrides, Assistants, Client Export, and Shared Key Export. The 'Client Export' tab is active, showing the 'Client Connection Behavior' section. In this section, 'Host Name Resolution' is set to 'Autre', 'Nom d'hôte' is '92.154.37.50', and 'Verify Server CN' is set to 'Automatic - Use verify-x509-name (OpenVPN 2.3+) where possible'. A note explains that this option is deprecated and will be removed in the next major version.

Vous pouvez ensuite exporter votre configuration.

The screenshot shows the 'Clients OpenVPN' section of the pfSense web interface. It displays a table with columns for 'Utilisateur' and 'Nom du certificat'. The first row shows 'VPN-SEB' for both. To the right of the table is an 'Export' section with various download buttons for different client configurations and installers.

Utilisateur	Nom du certificat	Export
VPN-SEB	VPN-SEB	<ul style="list-style-type: none"> - Inline Configurations: <ul style="list-style-type: none"> Most Clients Android OpenVPN Connect (iOS/Android) - Bundled Configurations: <ul style="list-style-type: none"> Archive Config File Only - Current Windows Installer (2.4.7-1x03): <ul style="list-style-type: none"> Windows Vista and Later - Old Windows Installers (2.3.18-1x02): <ul style="list-style-type: none"> x86-xp x64-xp x86-win6 x64-win6 - Viscosity (Mac OS X and Windows): <ul style="list-style-type: none"> Viscosity Bundle Viscosity Inline Config

5- Configuration d'une protection sur la page d'administration.

Aller dans Système > Avancé

Puis dans la partie Login Protection, définir le seuil de tentative avant blocage à 10, le Blocktime à 300 et le Detection time à 1800.

Login Protection	
Seuil	<input type="text" value="10"/> Block attackers when their cumulative attack score exceeds threshold. Most attacks have a score of 10.
Blocktime	<input type="text" value="300"/> Block attackers for initially blocktime seconds after exceeding threshold. Subsequent blocks increase by a factor of 1.5. Attacks are unblocked at random intervals, so actual block times will be longer.
Detection time	<input type="text" value="1800"/> Remember potential attackers for up to detection_time seconds before resetting their score.
Pass list	<input type="text" value="Address"/> / 128 <input type="button" value="v"/> Addresses added to the pass list will bypass login protection.
Add address	<input type="button" value="+ Add address"/>