



16/01/2017

VPN

CONFIGURATION VPN – IPSEC

CONFIGURATION VPN – OPENVPN

CONFIGURATION VPN - ROADWARRIOR

Sommaire :

Page 2 : Présentation projet VPN

Page 3 : Configuration des machines (PfSense, Windows)

Page 4 : Configuration IPSEC

Page 5 : Configuration Firewall

Page 6 : Test IPSEC

Page 7 : Configuration OPENVPN Server

Page 8 : Configuration OPENVPN Client

Page 9 : Configuration du Tunnel

Page 10 : Configuration ROADWARRIOR

Page 11 : Configuration General Information

Page 12 : Création User

Page 13 : Test Connexion OpenVPN

Page 14 : Message de validation de connexion

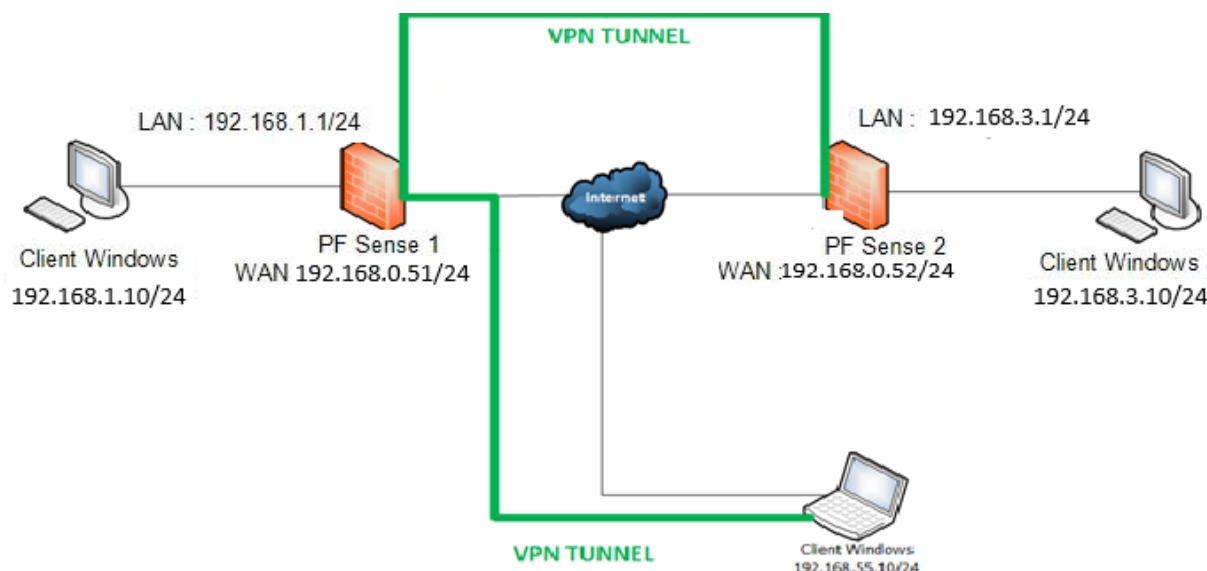
Présentation projet VPN

VPN Site à Site (IPsec)

Un VPN (Virtual Private Network) Site-to-Site (aussi appelé LAN-to-LAN) est un VPN qui permet de joindre deux réseaux de type LAN distants de manière à faire en sorte qu'ils puissent communiquer comme s'ils étaient sur le même réseau et qu'un simple routeur les sépareit. On peut trouver ce genre de VPN entre des agences et un siège d'entreprise par exemple. Les agences doivent pouvoir se connecter aux ressources du siège de manière transparente malgré leur distance. On établit alors un VPN au travers Internet afin de joindre les deux réseaux mais également de manière à sécuriser ces flux au travers un chiffrement.

Le projet que nous allons réaliser est la mise en place d'un VPN LAN-to-LAN. Afin de réaliser le projet, nous utiliser la fonctionnalité IPSEC (Internet Protocol Security) sur PfSense. Il fonctionne via des algorithmes permettant le transport de données sécurisés sur un réseau. Il se caractérise comme étant un standard ouvert travaillant sur la couche 3 et supportant de multiples algorithmes de chiffrement et d'authentification.

Voici un schéma d'ensemble du projet à réaliser sur le VPN :



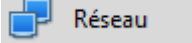

Configuration des machines :

Afin de configurer les machines PfSense il faudra configurer leurs cartes en réseau bridges, afin d'utiliser notre machine physique pour atteindre les 2 PfSense depuis une machine.

Pour cela il faudra mettre la première machine sur la carte réseau :

Activer la carte réseau
Mode d'accès réseau : Réseau privé hôte ▼
Nom : VirtualBox Host-Only Ethernet Adapter #2 ▼
[▶ Avancé](#)

Ensuite pour la seconde machine il faudra si vous ne l'avez pas créé une nouvelle carte réseau en

privé hôte. Pour cela il faudra appuyer sur **Ctrl+G**, puis dans  Réseau, il faudra cliquer sur  pour créer une nouvelle carte. Une fois la carte crée on pourra l'utiliser pour le 2eme PfSense.

Activer la carte réseau
Mode d'accès réseau : Réseau privé hôte ▼
Nom : VirtualBox Host-Only Ethernet Adapter #3 ▼

Maintenant crée et les carte réseaux entré nous configurerons les adresses IP des cartes réseau sur le bon réseau.

La deuxième carte réseau qui sera la carte réseau **LAN** sur la première machine PfSense sera comme ceci ; on utilisera la même carte réseaux pour la machine Windows :

Activer la carte réseau
Mode d'accès réseau : Réseau interne ▼
Nom : lan 1 ▼


La deuxième carte réseau qui sera la carte réseau **LAN** sur la deuxième machine PfSense sera comme ceci ; on utilisera la même carte réseaux pour la machine Windows :

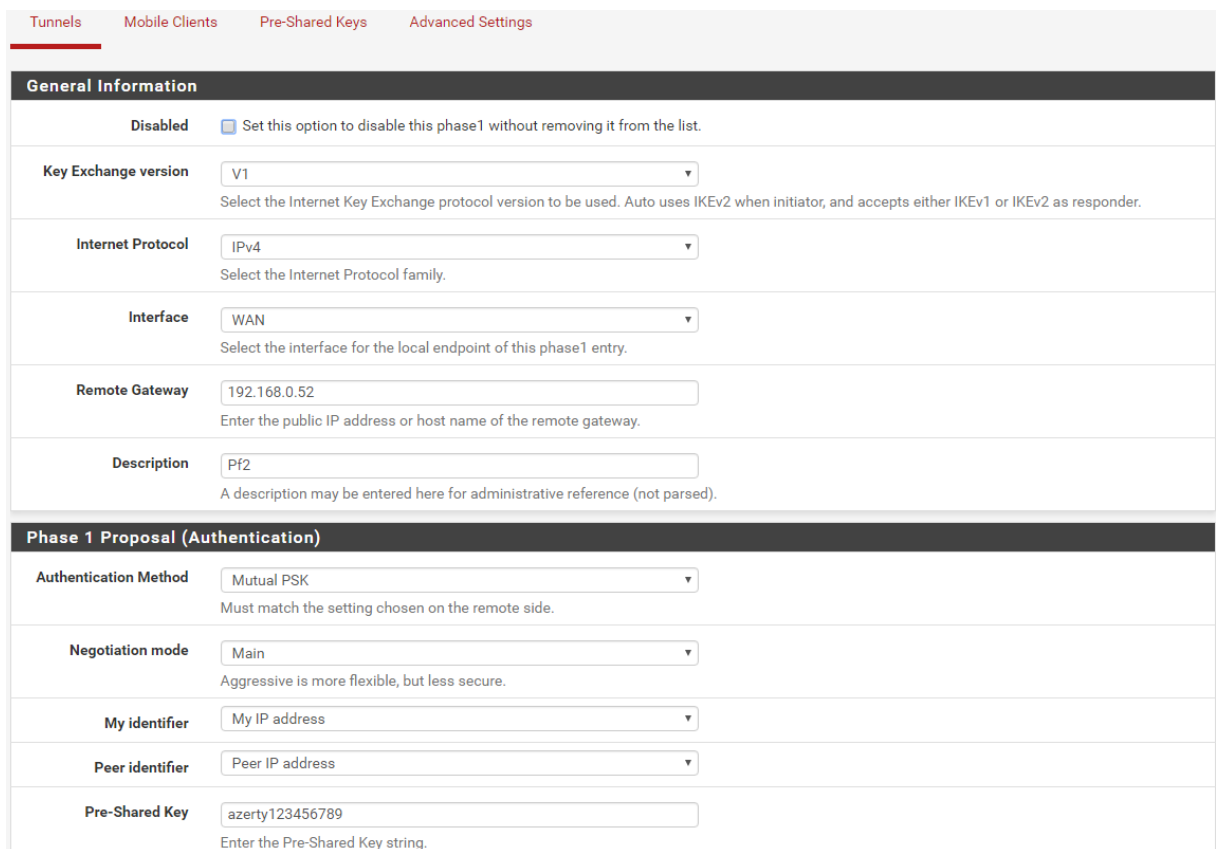
Activer la carte réseau
Mode d'accès réseau : Réseau interne ▼
Nom : lan 2 ▼

Nous nommerons la carte réseau de la machine Windows avec le même nom afin de les reconnaître.

Configuration de IPSEC :

Une fois les configurations réseaux configurés, il faudra configurer IPSEC selon les configurations de nos réseaux choisis.

- En premier lieu il faudra cliquer sur **VPN > IPSEC**. Dans les réglages IPSEC il faudra cliquer sur 
- Dans cette configuration il faudra configurer la **Remote Gateway** avec l'adresse IP **WAN** du 2^e PfSense qui est pour ma part **192.168.0.52**.
- Maintenant il faudra configurer un mot de passe qui sera identique au deuxième PfSense dans **Pre-Shared Key**.
- Nous devrions obtenir une configuration de ce genre :





The screenshot shows the IPsec configuration page in PfSense. The top navigation bar includes 'Tunnels', 'Mobile Clients', 'Pre-Shared Keys', and 'Advanced Settings'. The 'General Information' section is expanded, showing the following settings:

- Disabled:** Set this option to disable this phase1 without removing it from the list.
- Key Exchange version:** V1 (dropdown). Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.
- Internet Protocol:** IPv4 (dropdown). Select the Internet Protocol family.
- Interface:** WAN (dropdown). Select the interface for the local endpoint of this phase1 entry.
- Remote Gateway:** 192.168.0.52 (text input). Enter the public IP address or host name of the remote gateway.
- Description:** Pf2 (text input). A description may be entered here for administrative reference (not parsed).

The 'Phase 1 Proposal (Authentication)' section is also expanded, showing the following settings:

- Authentication Method:** Mutual PSK (dropdown). Must match the setting chosen on the remote side.
- Negotiation mode:** Main (dropdown). Aggressive is more flexible, but less secure.
- My identifier:** My IP address (dropdown).
- Peer identifier:** Peer IP address (dropdown).
- Pre-Shared Key:** azerty123456789 (text input). Enter the Pre-Shared Key string.

- Il faudra **Save** puis cliquer sur « **Apply changes** » 
- Maintenant nous cliquerons sur  afin de rajouter une règle pour configurer le tunnel.
- Nous devons sélectionner sur **Local Network** : « **LAN Subnet** » puis, dans **Remote Network** il faudra configurer le **Network** qui est le réseau du **LAN** du 2^e PfSense afin que, le tunnel acceptera le passage des paquets. Qui pour moi est **192.168.3.0 /24**
- Voici ce que nous devrions obtenir.

General Information

Disabled Disable this phase 2 entry without removing it from the list.

Mode Tunnel IPv4

Local Network LAN subnet / 0

Type Address

NAT/BINAT translation None / 0

Type Address

If NAT/BINAT is required on this network specify the address to be translated

Remote Network Network 192.168.3.0 / 24

Type Address

Description Net


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

- Nous cliquerons maintenant sur **Save & « Apply changes »**
- Nous devrions obtenir au final cette configuration :

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

IPsec Tunnels

IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 Description	Actions		
<input type="checkbox"/> Disable	V1 WAN 192.168.0.51	main	AES (256 bits)	SHA1				
		Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	P2 actions
<input type="checkbox"/> Disable		tunnel	LAN	192.168.1.0/24	ESP	AES (auto)	SHA1	
+ Add P2								

- Nous irons maintenant dans **Firewall > Rules > LAN** puis  .
- Il faudra sélectionner **Protocol : Any** puis dans **Source** dans le menu déroulant sélectionner **LAN net** puis dans **Destination : Any**. Puis **Save & « Applys changes »**.

Edit Firewall Rule

Action Pass

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 (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

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

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol any
Choose which IP protocol this rule should match.

Source

Source Invert match. LAN net / Source Address /

Destination

Destination Invert match. any / Destination Address /

- Désormais nous configurerons le **WAN** dans **Firewall > Rules**. Dedans nous devons configurer le **Protocol : TCP/UDP**. Dans **Source** nous sélectionnerons **Any**, puis dans **Destination** dans le menu déroulant nous sélectionnerons « **This firewall (self)** » puis laisser la configuration faite par défaut.
- Si tous est bien configurer nous devrions obtenir ceci dedans :

Edit Firewall Rule

Action Pass
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 (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

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

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP/UDP
Choose which IP protocol this rule should match.

Source

Source Invert match. any Source Address / ▼

Display Advanced ⚙ Display Advanced

Destination

Destination Invert match. This firewall (self) Destination Address / ▼

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

Il faudra configurer le 2^e PfSense de la même manière que celui-ci en modifiant selon les configurations réseaux.


*Afin de tester la fonctionnalité de IPSEC nous irons dans, **Status > IPSEC** ceci devrait apparaître :*

IPsec Status								
Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status
	192.168.0.52	192.168.0.52	192.168.0.51	192.168.0.51				Disconnected ➔ Connect VPN

Nous devons cliquer sur ➔ Connect VPN afin de les connecter. Si la liaison est bien effectuée nous obtiendrons ceci :

IPsec Status								
Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status
Pf2	192.168.0.51	192.168.0.51	192.168.0.52	192.168.0.52	IKEv1 responder	24793 seconds (06:53:13)	AES_CBC HMAC_SHA1_96 PRF_HMAC_SHA1 MODP_1024	ESTABLISHED 3115 seconds (00:51:55) ago 🗑 Disconnect

Configuration de OPENVPN Server :


- En premier lieu il faudra cliquer sur **VPN > OPENVPN > Server**. Dans les réglages **Server** il faudra cliquer sur .
- Dans les réglages il faudra dans **Server mode** sélectionner « **Peer to Peer (Shared Key)** » dans **Protocol** sélectionner **UDP** l'interface **WAN** puis le port sera « **1194** ».
- Il faudra cocher la case **Shared Key** puis **Save** et « **Apply changes** ».
- Il faudra maintenant retourner dedans puis la clé **Shared Key** sera à copier puis à coller dans le **Shared Key (du Client)**.
- Dans la configuration **Tunnel Settings**, il faudra dans **IPv4 Tunnel Network** rentrer l'adresse réseau **Tunnel** qui pour moi est **191.168.0.0/24**. Puis dans **IPv4 Remote network** entrer l'adresse réseau **LAN du client** qui est **192.168.3.0/24**.
- Vois ci une les configurations relatives :

General Information	
Disabled	<input type="checkbox"/> Disable this server Set this option to disable this server without removing it from the list.
Server mode	Peer to Peer (Shared Key)
Protocol	UDP
Device mode	tun
Interface	WAN
Local port	1194
Description	<input type="text"/> A description may be entered here for administrative reference (not parsed).

Cryptographic Settings	
Shared Key	<pre># # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- fd4e535fba3be7f1994ed1ec19c21d5c</pre> <p>Paste the shared key here</p>
Encryption Algorithm	AES-128-CBC (128-bit)
Auth digest algorithm	SHA1 (160-bit) Leave this set to SHA1 unless all clients are set to match. SHA1 is the default for OpenVPN.
Hardware Crypto	No Hardware Crypto Acceleration

Tunnel Settings	
IPv4 Tunnel Network	191.168.0.0/24 This is the IPv4 virtual network used for private communications between this server and client hosts expressed using CIDR (e.g. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients (see Address Pool).
IPv6 Tunnel Network	<input type="text"/> This is the IPv6 virtual network used for private communications between this server and client hosts expressed using CIDR (e.g. fe80::/64). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients (see Address Pool).
IPv4 Remote network(s)	192.168.3.0/24 IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.

Configuration de OPENVPN client :



- En premier lieu il faudra cliquer sur **VPN > OPENVPN > Clients**. Dans les réglages **Clients** il faudra cliquer sur  .
- Dans **Server mode** nous sélectionnerons « **Peer to Peer (Shared Key)**», ensuite le **Protocol** sera **UDP**, le **Device mode** : **Tun**, l'interface sélectionne sera l'interface **Wan**.
- Le protocole à choisir sera celui configuré dans le **OPENVPN Server** soit **1194**.
- Le **Server host or address** à remplir est l'adresse IP du **WAN** du **Pfsense 1** :

General Information	
Disabled	<input type="checkbox"/> Disable this client Set this option to disable this client without removing it from the list.
Server mode	Peer to Peer (Shared Key)
Protocol	UDP
Device mode	tun
Interface	WAN
Local port	1194 Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.
Server host or address	192.168.0.51
Server port	1194
Proxy host or address	
Proxy port	
Proxy Auth. - Extra options	none
Server hostname resolution	<input type="checkbox"/> Infinitely resolve server Continuously attempt to resolve the server host name. Useful when communicating with a server that is not permanently connected to the Internet.
Description	Client A description may be entered here for administrative reference (not parsed).

- Maintenant dans la partie **Cryptographic Settings**, puis dans **Shared Key** nous ferons un Coller du **Shared Key** que nous avons copié dans le **Shared Key Server**.
- Dans la partie **Tunnel Settings** nous entrerons comme plus haut, **IPv4 Tunnel Network** qui est l'adresse réseau du **Tunnel** soit **191.168.0.0/24** puis **IPv4 Remote Network** l'adresse réseau du **LAN** du PfSense 1.

Cryptographic Settings	
Peer Certificate Authority	No Certificate Authorities defined. One may be created here: System > Cert. Manager
Peer Certificate Revocation list	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager > Certificate Revocation
Auto generate	<input type="checkbox"/> Automatically generate a shared key
Shared Key	<pre># # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- fd4e535fba3be7f1994ed1ec19c21d5c -----</pre> <p>Paste the shared key here</p>
Encryption Algorithm	AES-128-CBC (128-bit)
Auth digest algorithm	SHA1 (160-bit) <small>Leave this set to SHA1 unless all clients are set to match. SHA1 is the default for OpenVPN.</small>
Hardware Crypto	No Hardware Crypto Acceleration
Tunnel Settings	
IPv4 Tunnel Network	191.168.0.0/24 <small>This is the IPv4 virtual network used for private communications between this client and the server expressed using CIDR (e.g. 10.0.8.0/24). The second network address will be assigned to the client virtual interface.</small>
IPv6 Tunnel Network	<input type="text"/> <small>This is the IPv6 virtual network used for private communications between this client and the server expressed using CIDR (e.g. fe80::/64). The second network address will be assigned to the client virtual interface.</small>
IPv4 Remote network(s)	192.168.1.0/24 <small>IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.</small>

Afin de vérifier la fonctionnalité il faudra aller dans Status > OPENVPN. Si le VPN est bien fonctionnel nous devrions obtenir ceci.

Servers Clients Client Specific Overrides Wizards			
OpenVPN Servers			
Protocol / Port	Tunnel Network	Description	Actions
UDP / 1194	191.168.0.0/24		 

Configuration de RoadWarrior :

La méthode RoadWarrior est utilisé principalement dans un contexte nomade.

Il a pour but d'établir une connexion VPN entre un appareil mobile et un réseau distant.













Il est surtout utilisé par les professionnels qui ont besoin d'accéder aux ressources de leur entreprise et ce peu importe leur situation géographique et le réseau sur lequel ils peuvent être contraint de se connecter (aéroport, hôtel, parc...).

C'est donc un VPN qui a pour but d'être temporaire contrairement aux deux précédentes méthodes. Bien sûr comme pour le cas précédent la connexion reste chiffré pour garantir une transmission des données sécurisé.




Il y'a plusieurs outils pour mettre en place la méthode RoadWarrior nous allons dans notre cas nous servir de OpenVPN.

Nous devons aller dans Système > Cert Manager

Ensuite nous devons remplir les différents champs à compléter selon nos désirs.

System / Certificate Manager / Certificates				
CA's	Certificates	Certificate Revocation		
Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (5878c62150360) Server Certificate CA: No, Server: Yes	self-signed	emailAddress=admin@pfSense.localdomain, ST=State, O=pfSense webConfigurator Self-Signed Certificate, L=Locality, CN=pfSense-5878c62150360, C=US Valid From: Fri, 13 Jan 2017 12:20:49 +0000 Valid Until: Wed, 06 Jul 2022 12:20:49 +0000	webConfigurator	  
Roadwarrior_Cert Server Certificate CA: No, Server: Yes	Roadwarrior_Ca	emailAddress=caca@caca.fr, ST=IDF, O=youcorporation, L=Paris, CN=Roadwarrior_Cert, C=FR Valid From: Fri, 13 Jan 2017 15:10:48 +0000 Valid Until: Mon, 11 Jan 2027 15:10:48 +0000	OpenVPN Server	  
Client-Windows User Certificate CA: No, Server: No	Roadwarrior_Ca	emailAddress=caca@caca.fr, ST=IDF, O=youcorporation, L=Paris, CN=Client-Windows, C=FR Valid From: Fri, 13 Jan 2017 15:11:33 +0000 Valid Until: Mon, 11 Jan 2027 15:11:33 +0000		  
ness User Certificate CA: No, Server: No	Roadwarrior_Ca	emailAddress=caca@caca.fr, ST=IDF, O=youcorporation, L=Paris, CN=ness, C=FR Valid From: Fri, 13 Jan 2017 17:43:52 +0000 Valid Until: Mon, 11 Jan 2027 17:43:52 +0000	User Cert	  

Dans **CA's** nous cliquons sur **ADD** afin d'ajouter une nouvelle certification.

CA's					
CA's	Certificates	Certificate Revocation			
Certificate Authorities					
Name	Internal	Issuer	Certificates	Distinguished Name	Actions
Roadwarrior_Ca	<input checked="" type="checkbox"/>	self-signed	3	emailAddress=caca@caca.fr, ST=IDF, O=youcorporation, L=Paris, CN=Roadwarrior_Ca, C=FR Valid From: Fri, 13 Jan 2017 15:10:08 +0000 Valid Until: Mon, 11 Jan 2027 15:10:08 +0000	  

Nous devons maintenant aller dans **VPN > OPENVPN**

- Nous devons cliquer sur « **Add** » afin de créer une nouvelle règle
- Dans le **Server mode** il faudra sélectionner « **Remote Access (SSL/TLS + User Auth)**,
- Ensuite il faudra configurer le **Protocol** sur **UDP**, **Device mode** sur **Tun**, puis **Interface** sur le **WAN**,
- Le local port sera le **443**.

Sur la partie Cryptographing Settings, laissez la case « Enable authentication of TLS packets » coché. Dans la même partie il faudra renseigner les différents certificats que l'on avait créé.

Maintenant il faudra configurer le tunnel sur le réseau LAN selon votre configuration.

Nous devrions obtenir cette configuration :

General Information	
Disabled	<input type="checkbox"/> Disable this server Set this option to disable this server without removing it from the list.
Server mode	Remote Access (SSL/TLS + User Auth) ▼
Backend for authentication	Local Database ▲▼
Protocol	UDP ▼
Device mode	tun ▼
Interface	WAN ▼
Local port	443
Description	Roadwarrior VPN A description may be entered here for administrative reference (not parsed).

Cryptographic Settings	
TLS authentication	<input checked="" type="checkbox"/> Enable authentication of TLS packets.
Key	<pre># # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- 8d25f8895a735fbd5bf34fafc3e1a4b</pre> <p>Paste the shared key here</p>
Peer Certificate Authority	Roadwarrior_Ca
Peer Certificate Revocation list	Roadwarrior_CRL (CA: Roadwarrior_Ca)
Server certificate	Roadwarrior_Cert (Server: Yes, CA: Roadwarrior_Ca, In Use)

Maintenant nous devons créer un user, pour cela nous devons aller dans **System > User Manager**, dans les configurations du **User** il faudra cocher la case « **click to create a user certificate** ». Puis sélectionner le nom du certificat créé.

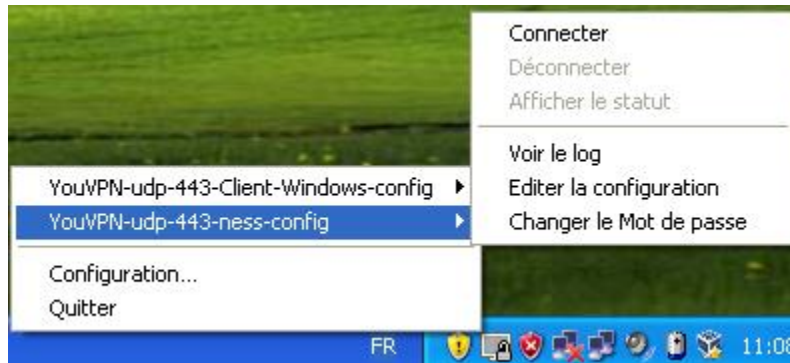
Create Certificate for User	
Descriptive name	youu
Certificate authority	Roadwarrior_Ca
Key length	2048 bits
Lifetime	3650

Afin de tester la configuration nous devons aller dans **System > Package Manager > Installed Packages** afin de télécharger puis installer le certificat pour le OpenVPN.

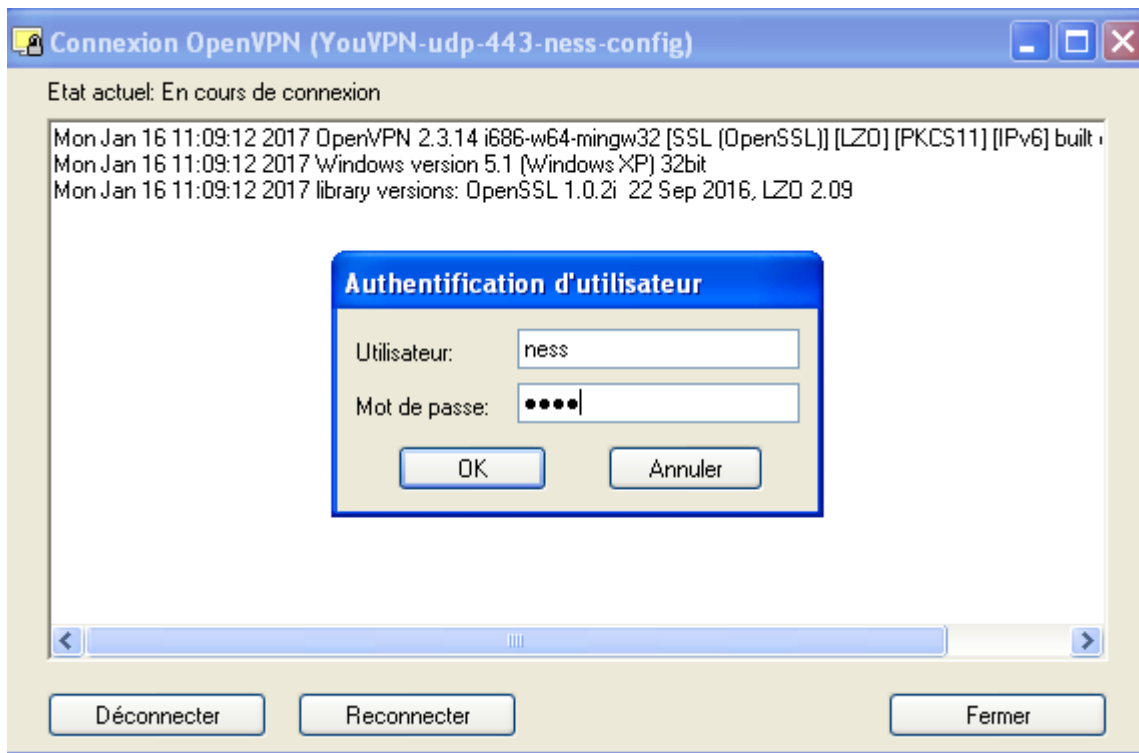
Une fois réalisé nous devons aller dans **OpenVPN > Client export**, une fois dedans il faudra aller tous en bas puis installer la configuration de notre système d'exploitation qui est Microsoft x64 du user créer.

(Photo)

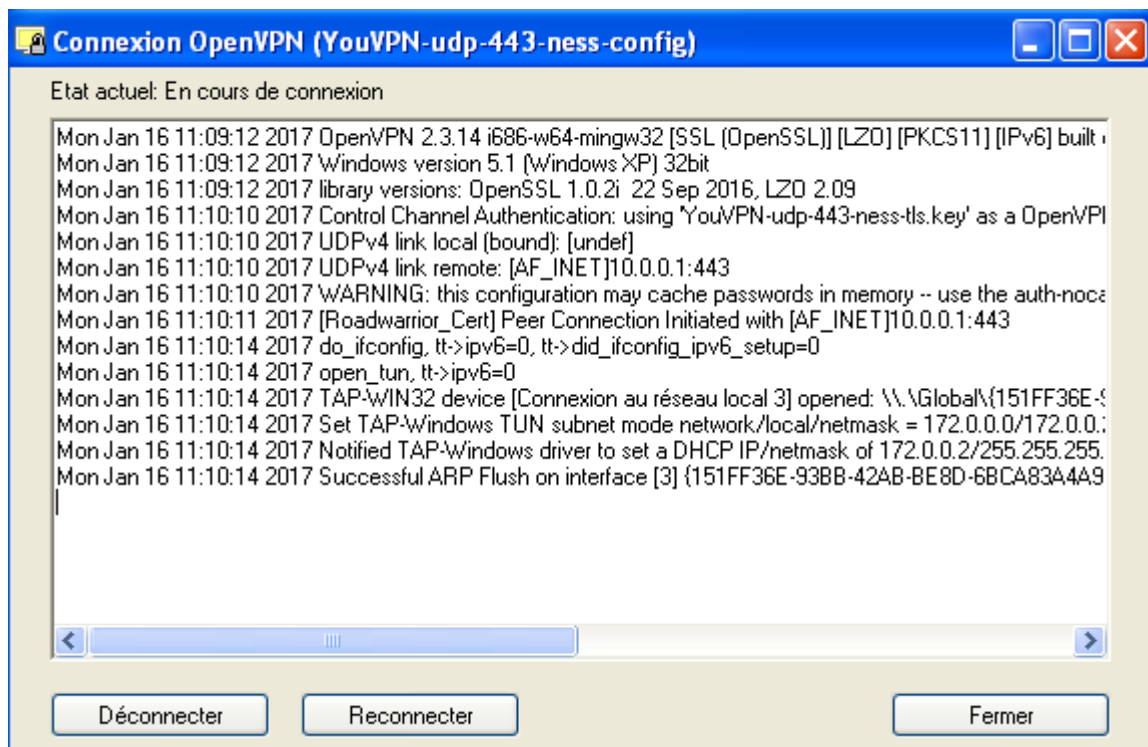
Nous devons maintenant aller sur notre machine cliente puis lancer OpenVPN et puis cliquer sur connecter.



Une page d'authentification s'ouvrira il faudra ensuite rentrer les identifiants afin de s'y connecter.



Si la connexion a bien été effectuée ce message devrait s'afficher :



L'icône devrait ensuite devenir comme ceci si la connexion bien été effectuée :

