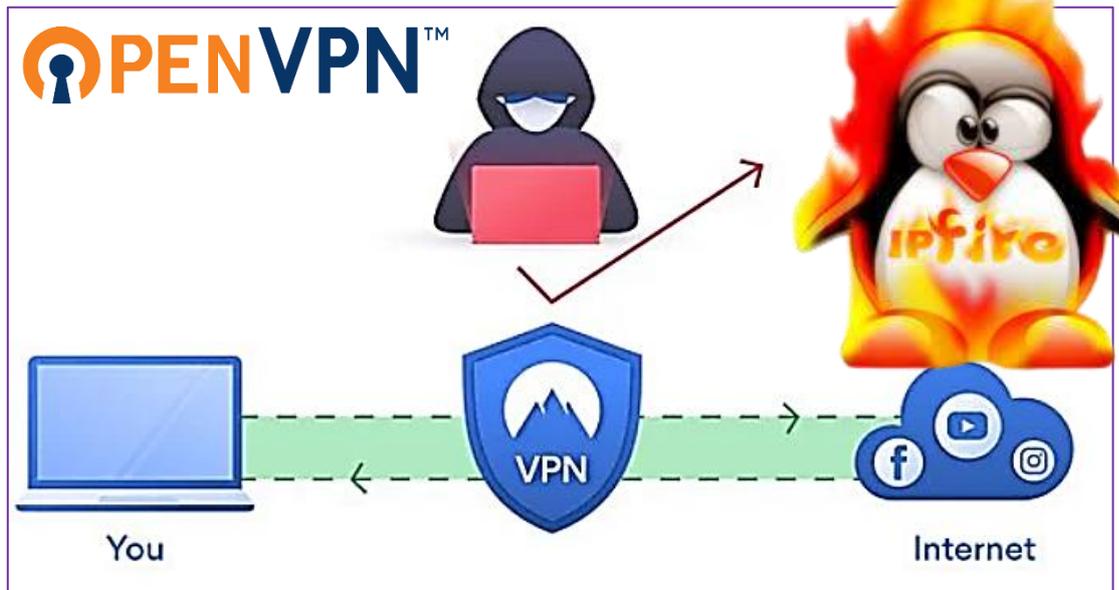


IPFIRE 2.27

Mettre en place un VPN de type
« ROAD WARRIOR »



SOMMAIRE

1. C'EST QUOI UN VPN ?
2. LES PRINCIPAUX TYPES DE VPN UTILISES
3. LE CHIFFREMENT DU TUNNEL VPN
4. MISE EN PLACE DU VPN « ROAD WARRIOR » AVEC IPFIRE
- 5.

© tutos-info.fr - 07/2022



DIFFICULTE



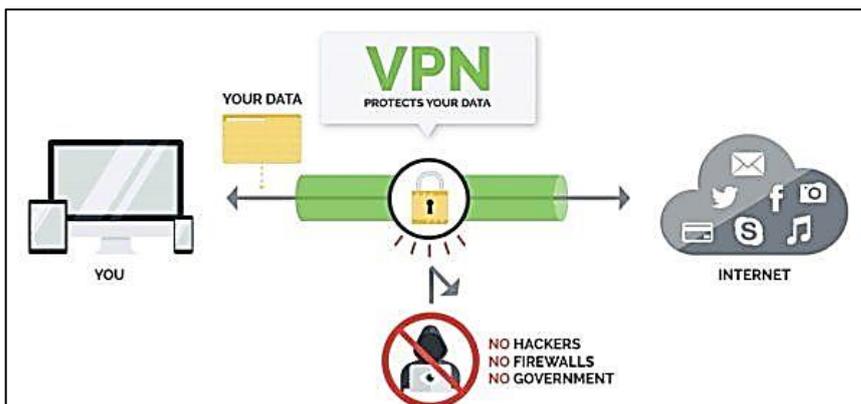
UTILISATION COMMERCIALE INTERDITE

1 - UN VPN C'EST QUOI ?



VPN est l'abréviation de « Virtual Private Network » (réseau privé virtuel) et désigne un service qui protège votre connexion Internet et votre confidentialité en ligne. Il crée un tunnel chiffré pour vos données, protège votre identité en ligne en masquant votre adresse IP.

Le VPN modifie votre adresse IP et masque votre emplacement virtuel.



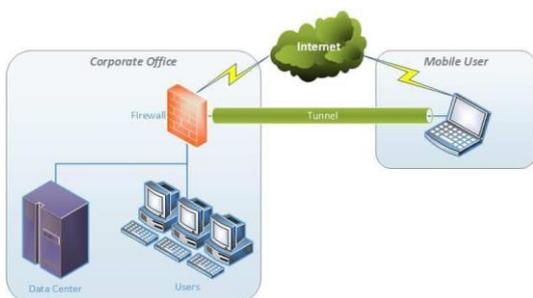
Les personnes travaillant dans des pays où la liberté d'expression est limitée dépendent d'une connexion Internet privée pour leur travail. Leur vie peut même parfois en dépendre. Les personnes qui vivent sous un régime autoritaire devraient utiliser un VPN pour masquer leur adresse IP et garantir une sécurité supplémentaire pour leurs messages sensibles. Le VPN chiffre les données et protège les appareils.

Voici ce qui se passe en coulisses :

1. Lorsque vous vous connectez à un service de réseau privé virtuel, celui-ci authentifie votre client auprès d'un serveur VPN.
2. Le serveur applique ensuite un protocole de chiffrement à toutes les données que vous envoyez et recevez.
3. Le service VPN crée un « tunnel » chiffré sur Internet. Cela sécurise les données qui circulent entre vous et votre destination.
4. Pour garantir la sécurité de chaque paquet de données, un VPN l'enveloppe dans un paquet externe, qui est ensuite chiffré par encapsulation. C'est l'élément central du tunnel VPN, qui assure la sécurité des données pendant leur transfert.
5. Lorsque les données parviennent au serveur, le paquet externe est supprimé via un processus de déchiffrement.

2 - LES PRINCIPAUX TYPES DE VPN UTILISES EN ENTREPRISE

LE VPN DE TYPE « ROAD WARRIOR » (accès distant)

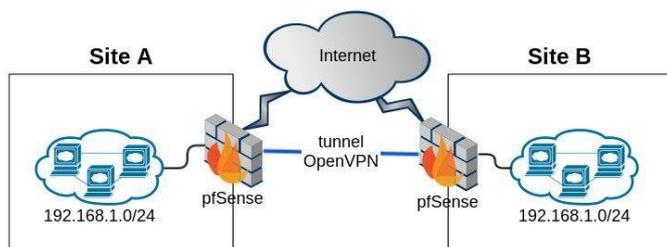


Un **VPN d'accès à distance** (« road warrior ») permet aux utilisateurs de se connecter à un réseau distant, généralement en utilisant un logiciel particulier.

Il rend le télétravail plus sûr et plus facile, car les employés peuvent accéder aux données et aux ressources de l'entreprise où qu'ils soient.



LE VPN DE TYPE « SITE A SITE »



connecter tous les bureaux et de permettre aux différentes succursales de partager en toute sécurité des ressources et des informations.

Les VPN « site à site » sont principalement utilisés par les entreprises, en particulier les grandes entreprises.

Ils permettent aux utilisateurs dans certains emplacements sélectionnés d'accéder aux réseaux des autres en toute sécurité. C'est un excellent moyen de

3 - LE CHIFFREMENT DU TUNNEL VPN

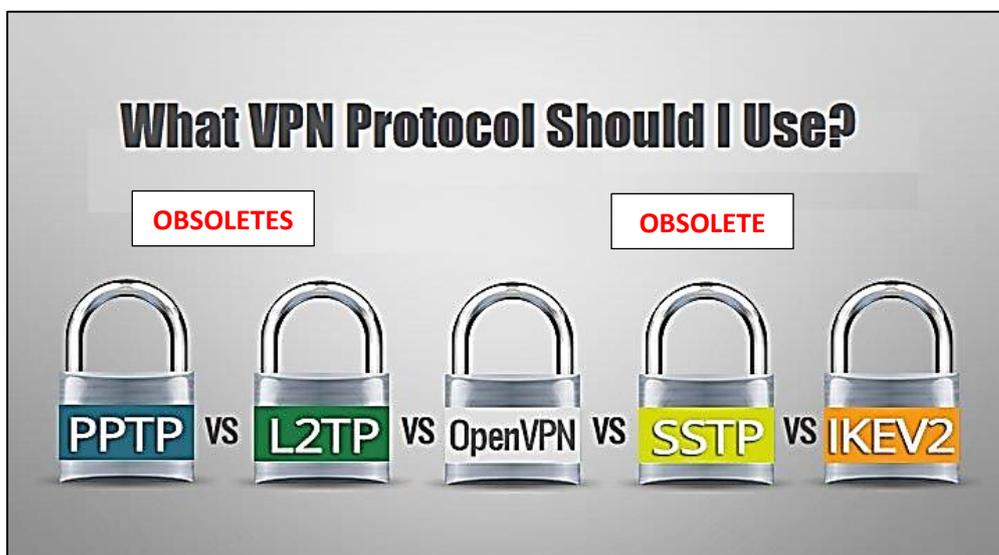
Les utilisateurs de VPN ont comme principale préoccupation la confidentialité.

OpenVPN est le protocole de chiffrement le plus populaire, actuellement utilisé par la majorité des fournisseurs de VPN dans le monde.

L'une des plus grandes forces d'OpenVPN est qu'il est hautement configurable. Il offre également un bon équilibre entre vitesse et sécurité, car vous pouvez l'utiliser à la fois sur les ports TCP et UDP. Si le port TCP est une option plus sûre, l'UDP est plus rapide.

Il existe d'autres protocoles de chiffrement parmi lesquels **IKEv2**.

IKEv2 est un protocole de tunneling, qui est **généralement associé à IPSec** pour le chiffrement. Il présente de nombreux avantages, tels que la capacité de restaurer une connexion sécurisée après des interruptions d'Internet. Il s'adapte également bien à l'évolution des réseaux. Il constitue donc un excellent choix pour les utilisateurs de téléphone qui passent souvent d'une connexion Wi-Fi domestique à une connexion mobile ou se déplacent entre des points d'accès.



Dans ce guide, nous allons étudier la mise en place d'un tunnel VPN chiffré avec le protocole le plus utilisé : **OpenVPN**.



Pour réaliser ce TP nous utiliserons le logiciel de virtualisation © Virtualbox.

Afin de pouvoir réaliser ce TP, il faut que vous ayez au préalable installé et configuré une machine virtuelle IPFire (voir guide « Installer IPFire »). Vous devez donc disposer :

- D'une machine virtuelle IPFire fonctionnelle configurée en mode « GREEN + RED ». On veillera à configurer une carte réseau en « mode pont » (interface « red ») pour la connexion Internet et une carte réseau en mode « réseau privé hôte » (interface « green ») pour le réseau local.
- D'une machine virtuelle Windows 10 (en version 21H2) avec une carte réseau connectée sur l'interface « green » en mode « réseau privé hôte ».

1^{ère} étape : installation des machines virtuelles

- Installez IPFire en mode « red + green » (voir guide « Installer IPFire »).
- Installez Windows 10 (sur l'interface « green ») en vous assurant que la carte réseau soit configurée en mode « réseau privé hôte ».

2^{ème} étape : configuration du VPN sur IPFire

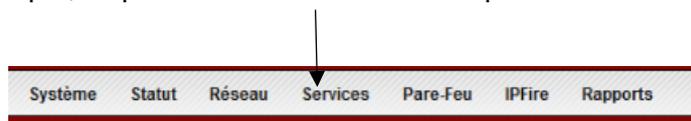
Dans ce TP, nous allons mettre en place un VPN utilisant le protocole OpenVPN. Pour configurer ce VPN, nous utiliserons le service OpenVPN offert par IPFire.

GUIDE COMPLET – MISE EN PLACE OpenVPN sur IPFire

Dans ce tutoriel, nous allons mettre en place un VPN de type nomade (« road warrior ») entre une machine hôte de la salle 136 et une machine Windows 10 virtuelle.

Après avoir installé et configuré IPFire, connectez-vous à l'interface web d'IPFire en saisissant l'adresse de votre routeur sous la forme : <https://xxx.xxx.x.x:444>

- Dans le menu principal, cliquez sur « Services » et « OpenVPN » :



- La fenêtre de configuration du service OpenVPN s'affiche :

Vous pouvez choisir le mode de chiffrement souhaité (plus vous demandez un chiffrement complexe et plus votre connexion sera ralentie).

Adresse de l'interface « red » (fournie par IPFire dans le menu d'accueil)

Adresse du tunnel VPN

4. Statut OpenVPN / Configuration :

Configuration générale

Statut actuel du serveur OpenVPN : **ARRETER**

OpenVPN sur RED

Nom d'hôte IP du VPN local :

Protocole : UDP

Taille du MTU : 1400

Compression-LZO :

Sous-réseau OpenVPN (c.a.d. 10.0.10.0/255.255.255.0) :

Port de destination :

Chiffre :

Sauvegarder Static IP address pools Options avancées du serveur Démarrer serveur OpenVPN

Autorité de certification

Nom	Sujet	Action
Certificat root:	Absent	
Certificat hôte:	Absent	
Diffie-Hellman parameters:	Absent	
TLS-Authentication-Key:	Absent	

Générer des certificats Root/Hôte

1 - Création des certificats « Root/Hôte »

- Cliquez le bouton « Générer des certificats Root/Hôte » :

Autorité de certification

Nom	Sujet	Action
Certificat root:	Absent	
Certificat hôte:	Absent	
Diffie-Hellman parameters:	Absent	
TLS-Authentication-Key:	Absent	

Générer des certificats Root/Hôte

- Complétez les champs pour la création des certificats « Root/Hôte » :

OpenVPN

Générer des certificats Root/Hôte:

Nom Organisation: *

Nom d'hôte d'IPFire: *

Votre adresse de courriel:

Votre Département:

Ville:

Etat ou Région:

Pays:

Diffie-Hellman parameters length:

Générer des certificats Root/Hôte

* Required field

Saisir, ici, le nom désiré.

Il s'agit ici de l'adresse de l'hôte (lien avec l'interface « red »).

Générer les certificats en cliquant ce bouton.

- Complétez la fenêtre principale en vérifiant que la case « OpenVPN sur RED » est bien cochée, puis terminez en cliquant le bouton « Démarrer le serveur OpenVPN » de manière à obtenir ceci (voir page suivante) :

Statut actuel du serveur OpenVPN : **EN FONCTION**

OpenVPN sur RED

Nom d'hôte/IP du VPN local:

Protocole:

Taille du MTU:

Compression-LZO:

Sous-réseau OpenVPN (c.a.d. 10.0.10.0/255.255.255.0):

Port de destination:

Chiffrer:

Etat et contrôle de connexion : Les certificats root et hôte générés précédemment s'affichent ici.

Autorité de certification

Nom	Sujet	Action
Certificat root	C=FR, O=vpnprof, CN=vpnprof CA	<input type="button" value="i"/> <input type="button" value="d"/>
Certificat hôte	C=FR, O=vpnprof, CN=109.190.23.144	<input type="button" value="i"/> <input type="button" value="d"/>
Diffie-Hellman parameters	DH Parameters: (1024 bit)	<input type="button" value="i"/>
TLS-Authentication-Key	2048 bit OpenVPN static key	<input type="button" value="i"/> <input type="button" value="d"/>

Légende: Montrer le certificat Téléchargez le certificat

2 - Création de la connexion VPN pour le client

- Cliquez le bouton « Ajouter » dans la rubrique « Etat et contrôle de connexion » :

Etat et contrôle de connexion :

- Sélectionnez le type de VPN souhaité : ici nous choisissons « Road warrior » (VPN nomade)
- Cliquez le bouton « Ajouter » :

OpenVPN

Type de Connexion

Type de Connexion:

Virtual Private Network (VPN) de l'hôte au net (RoadWarrior)

Net-a-Net Réseau Privé Virtuel (VPN)

Net-a-Net Réseau Privé Virtuel (VPN) (Upload Client Package)

Aucun fichier sélectionné.

Import Connection Name Default: Client Packagename

- Complétez les champs de manière à obtenir ceci (ne compléter que les champs marqués d'un astérisque rouge car ce sont des champs obligatoires) (voir page suivante) :

OpenVPN

Connexion:

Nom: *

Remarque:

Activé:

Choose network

Dynamic OpenVPN IP address pool (10.217.216.0/255.255.255.0)

Authentification :

Envoyer une demande de certificat : Aucun fichier sélectionné.

Envoyer un certificat :

Générer un certificat

Nom d'utilisateur complet ou nom d'hôte du système: *

Adresse E-mail de l'utilisateur:

Département de l'utilisateur:

Nom Organisation:

Ville:

Etat ou Région:

Pays:

Valide jusqu'au (days):

Fichier mot de passe PKCS12:

Fichier mot de passe PKCS12: (confirmation)

* Required field

Saisir un mot de passe d'au moins 5 caractères pour pouvoir valider la génération du certificat client.

- Dans les options avancées, cliquez la case « Redirect Gateway »
- Indiquez les réseaux auxquels le client aura accès : ici, on indiquera que le client peut accéder au réseau « Green » (réseau LAN)
- Spécifiez le DNS (adresse IP de votre routeur IPFire)
- Cliquez le bouton « Sauvegarder » ; vous devriez obtenir ceci (voir page suivante) :

Options avancées du client:

Redirect Gateway:

Routage :

IPFire a accès à ces réseaux sur le site du client

Le client a accès à ces réseaux sur le site d'IPFire

Aucun
VERT

Attention ! Si vous modifiez ces paramètres, vous devez redémarrer le serveur OpenVPN pour que les modifications prennent effet !

Adresse IP de votre routeur IPFire

DNS1: 192.168.1.1

DNS2:

WINS:

Sauvegarder Annuler

- Après avoir cliqué le bouton « Sauvegarder », vous devriez revenir sur l'écran de configuration et obtenir ceci :

Etat et contrôle de connexion :

Dynamic OpenVPN IP address pool

Nom	type	Remarque	Statut	Action
clientvpn	Hôte (Certif)		DECONNECTE	

Légende: Activé (cliquer pour désactiver) Montrer le certificat Editer Enlever
 Désactivé (cliquer pour activer) Téléchargez le certificat Téléchargez le paquet client (zip)

3 - Téléchargement du paquet zip « certificat client » (pour la machine cliente)

Afin de pouvoir, depuis une machine cliente, vous connecter au VPN, il faut télécharger les fichiers nécessaires. Ces fichiers devront ensuite être décompressés et sauvés dans un dossier spécifique sur la machine cliente.

- Cliquez sur la petite disquette qui se trouve ici :

Etat et contrôle de connexion :

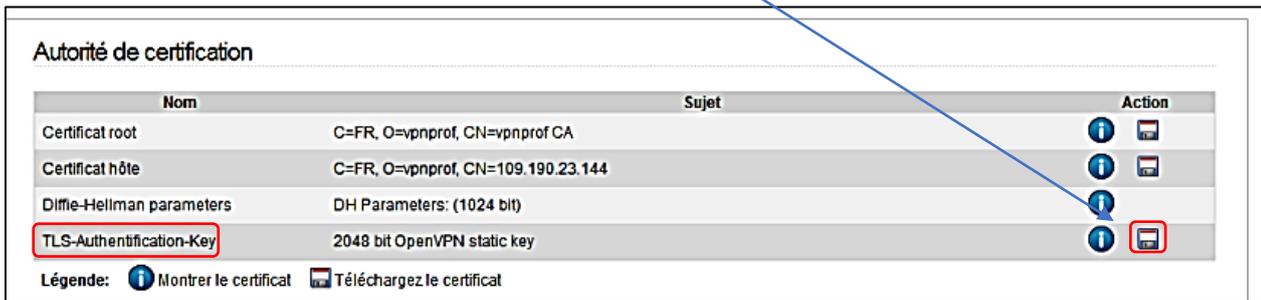
Dynamic OpenVPN IP address pool

Nom	type	Remarque	Statut	Action
clientvpn	Hôte (Certif)		DECONNECTE	

Légende: Activé (cliquer pour désactiver) Montrer le certificat Editer Enlever
 Désactivé (cliquer pour activer) Téléchargez le certificat Téléchargez le paquet client (zip)

En cliquant sur la petite disquette, vous allez télécharger un fichier « zip » qui contient le profil VPN et les identifiants de connexion au VPN (pour le client).

- Téléchargez, également, le fichier « TLS-Authentification-Key » :



Vous devriez vous retrouver avec 3 fichiers comme ci-dessous :

Nom	Modifié le	Type
clientvpn	21/03/2016 18:45	Échange d'inform...
clientvpn-TO-IPFire.ovpn	21/03/2016 18:45	Fichier OVPN
ta	21/03/2016 18:45	Fichier KEY

Ce fichier contient l'ensemble des informations de connexion au VPN.

4 - Ajout d'une règle dans le pare-feu d'IPFire pour la connexion au VPN

Il faut maintenant autoriser les connexions des clients au VPN nomade, en ouvrant le port UDP 1194 dans votre routeur IPFire.

- Cliquez, dans le menu principal d'ipFire, sur « Pare-feu » et « Règles de pare-feu »
- Cliquez sur « Nouvelle règle »
- Il faut configurer la règle de manière à obtenir ceci :

Firewall Rules

Source

Source address (MAC/IP address or network):

Standard networks: **OpenVPN (10.217.216.0/24)**

GeolP: **A1 - Anonymous Proxy**

NAT

Use Network Address Translation (NAT)

Destination NAT (Port forwarding)

Source NAT: New source IP address: **VERT (192.168.0.1)**

Destination

Destination address (IP address or network):

Standard networks: **VERT (192.168.0.0/24)**

GeolP: **A1 - Anonymous Proxy**

Protocol

UDP Source port: 1194 Destination port: 1194
External port (NAT):

Additional settings

Remarque:

Rule position:

Log rule
 Use time constraints
 Limit concurrent connections per IP address
 Rate-limit new connections

Ajouter Back

Après avoir cliqué le bouton « Ajouter », vous devriez obtenir ceci :

Firewall Rules

New rule Apply changes

Firewall Rules

#	Protocole	Source	Log	Destination	Action
1	UDP	OpenVPN (10.217.216.0/24): 1194 ->VERT	<input type="checkbox"/>	VERT: 1194	<input checked="" type="checkbox"/>
		VERT	Internet (Allowed)		Politique: Allowed

- Cliquez le bouton « Apply changes » pour valider la nouvelle règle

Le service OpenVPN est prêt. Il faut maintenant intervenir sur la machine qui se connectera au VPN.

5 - Préparation de la machine cliente qui se connectera au VPN

Pour fonctionner, votre VPN nécessite un **client OpenVPN** que vous pouvez télécharger à cette adresse : <https://openvpn.net/community-downloads/>. Dans notre cas, nous téléchargerons l'archive suivante :

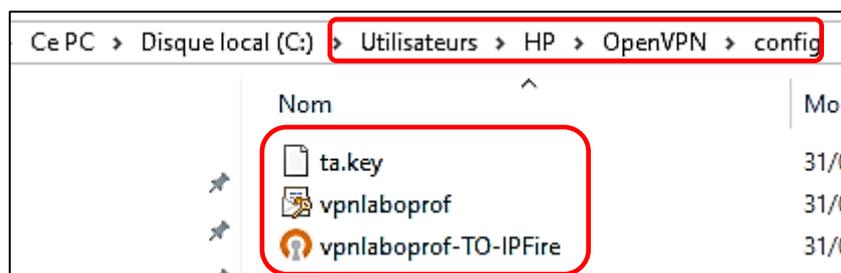
OpenVPN 2.5.5 -- Released 15 Dec, 2021

Une fois le client OpenVPN téléchargé, installez l'application sur la machine cliente qui se connectera au VPN précédemment créé (pas de difficultés particulières). Acceptez, si un message vous le demande, la création d'une carte réseau virtuelle « TAP » qui permettra la connexion au VPN.

Lancez l'application OpenVPN client : une petite icône apparaît à côté de l'heure système :



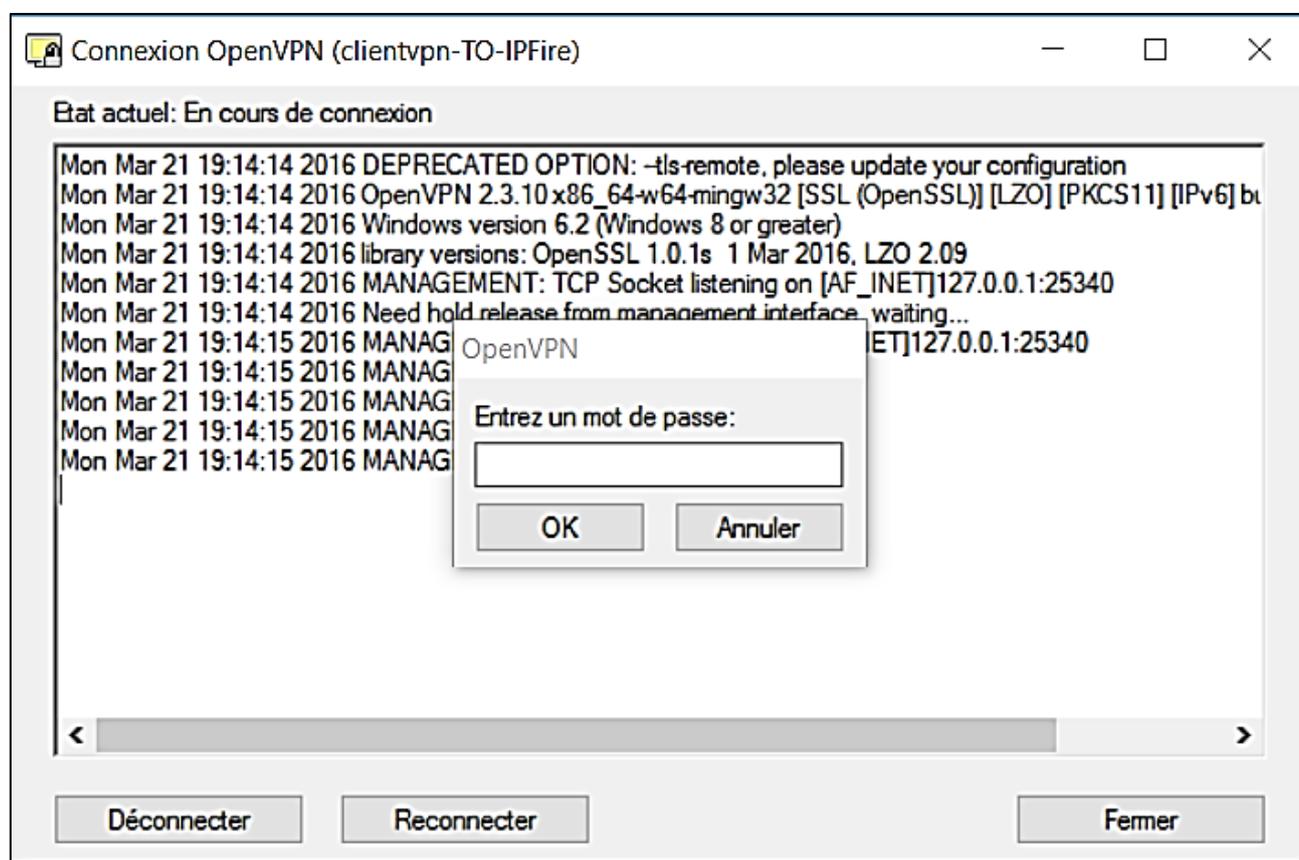
Nous allons maintenant copier les 3 fichiers de configuration du certificat client générés précédemment dans le dossier de l'utilisateur de la machine cliente (dossier « config » du dossier OpenVPN) :



Votre VPN est prêt !

6 - Test de connexion au VPN depuis une machine cliente

- Depuis le pc client, faites un clic droit sur l'icône OpenVPN et cliquez « Connecter » ; si tout se passe bien, vous devriez obtenir la fenêtre d'authentification suivante ; saisissez le mot de passe défini lors de la génération du certificat client :



Si votre connexion VPN est acceptée, un message s'affiche et l'icône OpenVPN client s'affiche en vert :



A ce stade, votre machine est connectée à la machine distante via un tunnel VPN fonctionnant avec le protocole OpenVpn.

7 - Test du VPN

Il est possible d'afficher les négociations entre votre machine et la machine distante en faisant un clic droit sur l'icône OpenVPN et en cliquant « Voir le log » ; vous obtenez ceci :

```
Mon Mar 21 19:18:04 2016 UDPv4 link local: [undef]
Mon Mar 21 19:18:04 2016 UDPv4 link remote: [AF_INET]109.190.23.144
Mon Mar 21 19:18:04 2016 MANAGEMENT: >STATE:1458584284,MANAGEMENT
Mon Mar 21 19:18:04 2016 MANAGEMENT: >STATE:1458584284,MANAGEMENT
Mon Mar 21 19:18:04 2016 TLS: Initial packet from [AF_INET]109.190.23.144
Mon Mar 21 19:18:05 2016 VERIFY OK: depth=1, /C=FR/O=vpnprof.
Mon Mar 21 19:18:05 2016 VERIFY OK: nsCertType=SERVER
Mon Mar 21 19:18:05 2016 VERIFY X509NAME OK: /C=FR/O=vpnprof.
Mon Mar 21 19:18:05 2016 VERIFY OK: depth=0, /C=FR/O=vpnprof.
Mon Mar 21 19:18:05 2016 Data Channel Encrypt: Cipher 'AES-256-CBC'
Mon Mar 21 19:18:05 2016 Data Channel Encrypt: Using 256 bit message
Mon Mar 21 19:18:05 2016 Data Channel Decrypt: Cipher 'AES-256-CBC'
Mon Mar 21 19:18:05 2016 Data Channel Decrypt: Using 256 bit message
Mon Mar 21 19:18:05 2016 Control Channel: TLSv1, cipher TLSv1/SSLv3
Mon Mar 21 19:18:05 2016 [109.190.23.144] Peer Connection Initiated with [AF_INET]109.190.23.144
Mon Mar 21 19:18:06 2016 MANAGEMENT: >STATE:1458584286,MANAGEMENT
```

On voit bien ici les « négociations » entre la machine cliente et le serveur VPN (encryptage et décryptage) avec l'algorithme de chiffrement choisi lors de la création du VPN.

```
Etat actuel: Connecté
Mon Mar 21 19:18:08 2016 ROUTE_GATEWAY 192.168.1.254/255.255.255.0 I=4 HWADDR=7c:7a:91:12:00:00
Mon Mar 21 19:18:08 2016 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Mon Mar 21 19:18:08 2016 MANAGEMENT: >STATE:1458584288,ASSIGN_IP,,10.217.216.6,
Mon Mar 21 19:18:08 2016 open tun, tt->ipv6=0
Mon Mar 21 19:18:08 2016 TAP-WIN32 device [Ethernet] opened: \\.\Global\{E690D530-C32C-4A4A-96D0-B48088F0}
Mon Mar 21 19:18:08 2016 TAP-Windows Driver Version 9.21
Mon Mar 21 19:18:08 2016 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.217.216.6/255.255.255.255
Mon Mar 21 19:18:08 2016 Successful ARP Flush on interface [24] {E690D530-C32C-4A4A-96D0-B48088F0}
Mon Mar 21 19:18:13 2016 TEST ROUTES: 2/2 succeeded len=2 ret=1 a=0 u/d=up
Mon Mar 21 19:18:13 2016 MANAGEMENT: >STATE:1458584293,ADD_ROUTES,...
Mon Mar 21 19:18:13 2016 C:\Windows\system32\route.exe ADD 10.217.216.1 MASK 255.255.255.255 10.217.216.6
Mon Mar 21 19:18:13 2016 ROUTE: CreateIpForwardEntry succeeded with dwForwardMetric1=20 and dwForwardMetric2=20
Mon Mar 21 19:18:13 2016 Route addition via IPAPI succeeded [adaptive]
Mon Mar 21 19:18:13 2016 C:\Windows\system32\route.exe ADD 192.168.0.0 MASK 255.255.255.0 10.217.216.6
Mon Mar 21 19:18:13 2016 ROUTE: CreateIpForwardEntry succeeded with dwForwardMetric1=20 and dwForwardMetric2=20
Mon Mar 21 19:18:13 2016 Route addition via IPAPI succeeded [adaptive]
Mon Mar 21 19:18:13 2016 Initialization Sequence Completed
Mon Mar 21 19:18:13 2016 MANAGEMENT: >STATE:1458584293,CONNECTED,SUCCESS,10.217.216.6,
```

Ouverture du tunnel après « négociations » entre la machine cliente et le serveur VPN.

Adresse IP virtuelle affectée à notre machine cliente qui vient de se connecter au tunnel VPN.

La connexion VPN étant établie, vous pouvez tenter un test de « ping » sur la machine distante (exemple : ping 192.168.x.xxx). Logiquement la machine cliente doit répondre au ping (si ce n'est pas le cas, vérifiez le pare-feu de la machine distante).

Test du ping vers la machine distante :

```
Envoi d'une requête 'Ping' 192.168.0.101 avec 32 octets de données :
Réponse de 192.168.0.101 : octets=32 temps=119 ms TTL=127
Réponse de 192.168.0.101 : octets=32 temps=116 ms TTL=127
Réponse de 192.168.0.101 : octets=32 temps=120 ms TTL=127
Réponse de 192.168.0.101 : octets=32 temps=121 ms TTL=127

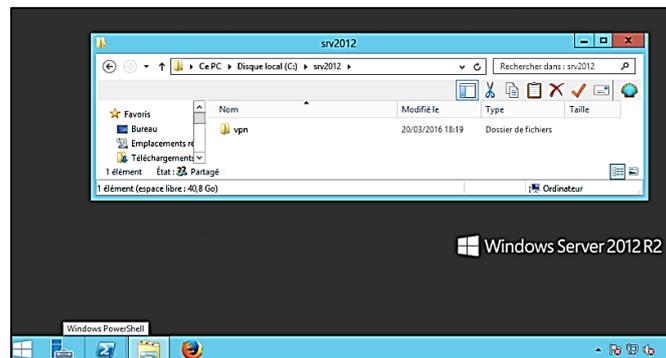
Statistiques Ping pour 192.168.0.101:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 116ms, Maximum = 121ms, Moyenne = 119ms
```

La carte « TAP » virtuelle de notre machine est bien active avec l'adresse IP du tunnel :

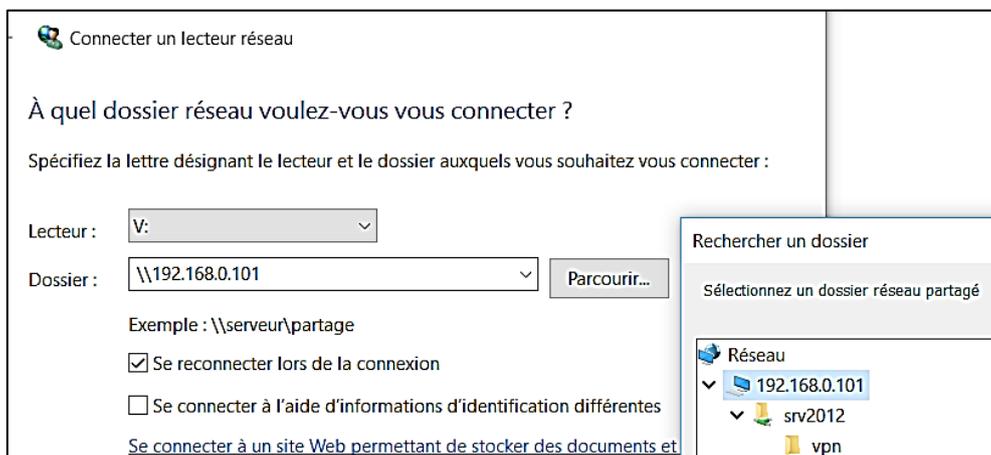
```
Carte Ethernet Ethernet :  
  
Suffixe DNS propre à la connexion. . . . :  
Description. . . . . : TAP-Windows Adapter V9  
Adresse physique . . . . . : 00-FF-E6-90-D5-30  
DHCP activé. . . . . : Oui  
Configuration automatique activée. . . . : Oui  
Adresse IPv6 de liaison locale. . . . . : fe80::f484:40af:a141:66da%24(préféré)  
Adresse IPv4. . . . . : 10.217.216.6(préféré)  
Masque de sous-réseau. . . . . : 255.255.255.252  
Bail obtenu. . . . . : lundi 21 mars 2016 19:18:09  
Bail expirant. . . . . : mardi 21 mars 2017 19:18:08  
Passerelle par défaut. . . . . :  
Serveur DHCP . . . . . : 10.217.216.5  
IAID DHCPv6 . . . . . : 402718694  
DUID de client DHCPv6. . . . . : 00-01-00-01-1D-AE-CE-FE-7C-7A-91-12-57-4B  
Serveurs DNS. . . . . : fec0:0:0:ffff::1%1  
                        fec0:0:0:ffff::2%1  
                        fec0:0:0:ffff::3%1  
  
NetBIOS sur Tcpi. . . . . : Activé
```

8 – Connexion d'un lecteur réseau via le VPN

- Créez un lecteur sur la machine virtuelle Windows 10 et partagez-le en accordant les autorisations de partage nécessaires :



- Depuis la machine cliente, connectez le lecteur réseau (en faisant un clic droit sur « Ce pc » et « Connecter un lecteur réseau ») et saisissez les paramètres nécessaires pour vous connecter à votre lecteur réseau partagé :



Si les paramètres saisis sont corrects, vous devriez pouvoir vous connecter au lecteur réseau de votre machine virtuelle via votre tunnel VPN :



ATTENTION – POINT IMPORTANT

Afin de ne pas rencontrer d'erreur lors de la connexion VPN entre votre machine et la machine distante, vous ne devez pas être sur le même réseau que la machine distante (adresses IP locales différentes) !