



# Procédure OpenVPN

Configurer un serveur VPN Linux en  
utilisant OpenVPN

Florent Spring

GRUPE SCOLAIRE LA SALLE TROYES

# Sommaire

<b>II) DEFINITION .....</b>	<b>1</b>
<b>III) LES PREREQUIS.....</b>	<b>1</b>
<b>IV) CONFIGURER UN SERVEUR VPN LINUX AVEC UN SERVEUR D'ACCES OPENVPN .....</b>	<b>2</b>
<b>V) CONFIGURER UN SERVEUR VPS LINUX AVEC OPENVPN POUR LE TUNNELLING .....</b>	<b>5</b>
<b>V. COMMENT CONNECTER VOTRE SERVEUR VPN LINUX A D'AUTRES DISPOSITIFS AVEC OPENVPN.....</b>	<b>8</b>
1. COMMENT INSTALLER ET CONNECTER LE CLIENT OPENVPN SOUS WINDOWS.....	8
2. COMMENT INSTALLER ET CONNECTER LE CLIENT OPENVPN SOUS LINUX .....	8
3. COMMENT INSTALLER ET CONNECTER LE CLIENT OPENVPN SOUS ANDROID.....	9
4. COMMENT INSTALLER ET CONNECTER LE CLIENT OPENVPN SOUS IOS .....	9
<b>VII) PARAMETRES DE COMPRESSION DU SERVEUR VPN LINUX .....</b>	<b>10</b>
<b>VIII) AJOUTER DES UTILISATEURS AU SERVEUR VPN LINUX UTILISANT OPENVPN .....</b>	<b>11</b>
<b>IX) CONFIGURER DES PROFILS DE CONNEXION AUTOMATIQUE POUR UN SERVEUR VPN LINUX AVEC OPENVPN .....</b>	<b>12</b>
<b>X) COMMENT TESTER UN SERVEUR VPN LINUX SOUS OPENVPN .....</b>	<b>13</b>
<b>XI) CONCLUSION.....</b>	<b>14</b>
<b>XII) BIBLIOGRAPHIE .....</b>	<b>14</b>

## I) Définition

**VPN** est l'abréviation de **Virtual Private Network** (réseau privé virtuel). Parmi ces logiciels **VPN** open source, on trouve **OpenVPN**, qui peut fonctionner comme un serveur VPN Linux. Le **VPN** permet de sécuriser les connexions en créant une connexion sécurisée point à point. L'utilisation d'un **VPN** sous **Linux** est l'un des meilleurs moyens de sécuriser les connexions sur Internet ou sur un réseau ouvert. Dans ce tutoriel, nous allons voir comment installer votre propre serveur **VPN Linux** en utilisant **OpenVPN**. Transformez votre **VPS** (Virtual Private Server « serveur privé virtuel ») en une incroyable mesure de sécurité !

## II) Les prérequis

1. Vous devez avoir un accès root ou le privilège sudo.
2. **OpenVPN** ne devrait pas être préinstallé.
3. Le pare-feu devrait permettre le trafic TCP sur le port 943 et le trafic UDP sur le port 1194. Il est recommandé d'utiliser **UFW** (Uncomplicated Firewall).

### III) Configurer un serveur VPN Linux avec un serveur d'accès OpenVPN

*D'abord, mettons à jour le système. Pour CentOS, utilisez la commande suivante :*

```
yum -y update
```

*Pour Ubuntu et Debian, mettez à jour les index en utilisant :*

```
sudo apt update
```

L'installation d'**OpenVPN** nécessite le **package net-tools**. Installez-le si vous ne l'avez pas préinstallé. Le **paquet net-tools** contient **ifcfg** qui est nécessaire pour l'installation du serveur **OpenVPN**.

*Vous pouvez l'installer sur **CentOS** en utilisant :*

```
sudo yum install net-tools
```

*Pour **Ubuntu** et **Debian**, vous pouvez utiliser la commande ci-dessous :*

```
sudo apt install net-tools
```

Vous pouvez télécharger le client **OpenVPN** pour votre distribution à partir du [site web OpenVPN](http://swupdate.openvpn.org/as/openvpn-as-2.5.2-Debian9.amd_64.deb). Vous pouvez obtenir le lien ici et l'utiliser avec la commande **curl**.

*Un exemple de commande **curl** pour **Ubuntu** est présenté ci-dessous :*

```
curl -O http://swupdate.openvpn.org/as/openvpn-as-2.5.2-Debian9.amd_64.deb
```

*Pour **CentOS**, la commande **curl** sera :*

```
curl -O http://swupdate.openvpn.org/as/openvpn-as-2.7.3-CentOS7.x86_64.rpm
```

*Ici, vous pouvez ajouter l'URL à votre distribution. Pour vérifier que la bonne installation est bien téléchargée, il faut contrôler la somme de contrôle **SHA256**. Vous pouvez utiliser la commande ci-dessous :*

```
sha256sum openvpn-as-*
```

*Ceci imprimera la somme de contrôle comme indiqué ci-dessous :*

```
6354ac41be811829e60b028d3a7a527e839232d7f782c1d29bb4d8bd32bf24d5  openvpn-as-2.7.3-CentOS7.x86_64.rpm
```

Vous pouvez comparer la somme de contrôle de ce binaire téléchargé avec celle fournie sur le [site d'OpenVPN](#). Si la somme de contrôle correspond, on peut installer.

*Pour l'installer sous **CentOS**, utilisez cette commande :*

```
sudo rpm --install openvpn-as-*.rpm
```

*De même, dans **Ubuntu** et **Debian**, vous pouvez utiliser la commande ci-dessous dans la ligne de commande :*

```
sudo dpkg -i openvpn-as-*.deb
```

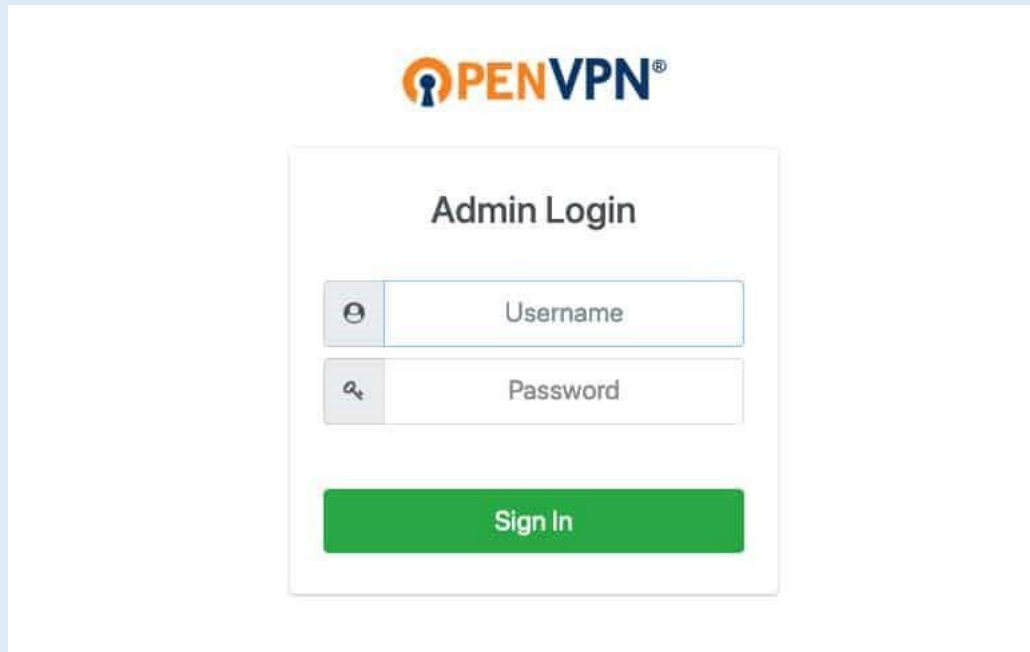
L'installation prendra un certain temps. Une fois cette opération terminée, l'interface d'administration et l'interface client s'affichent. Par défaut, un utilisateur **openvpn** sera créé lors de cette installation.

*Vous pouvez définir le mot de passe pour cet utilisateur en utilisant cette commande :*

```
passwd openvpn
```

Ceci définira votre nouveau mot de passe. Mémoisez le mot de passe puisqu'il sera utilisé pour se connecter. Utilisez l'URL d'administration pour vous connecter et terminer le processus d'installation. Dans notre cas, l'URL d'administration est – `https://31.220.111.160:943/admin`. Normalement l'URL est simplement l'adresse IP de votre **VPS** plus le port :943 avec /admin à la fin, comme dans l'exemple.

*Vous verrez un écran comme indiqué ci-dessous :*



**OPENVPN®**

### Admin Login

**Sign In**

Le nom d'utilisateur est **openvpn** comme mentionné précédemment et le mot de passe est celui que vous venez de définir pour cet utilisateur. Une fois connecté, vous trouverez une page de Conditions Générales d'Utilisation. Lisez-la et appuyez sur le bouton Accepter pour continuer. La page suivante vous fournira les détails de la configuration et vous indiquera l'état du serveur.

Les paramètres par défaut sont suffisamment bons et peuvent permettre à **MacOS, Linux, Windows, Android** et **iOS** de se connecter au serveur **VPN Linux**. Si vous souhaitez modifier des paramètres, assurez-vous de cliquer sur « Appliquer » et mettre à jour le serveur en cours d'exécution pour activer les modifications.

L'installation par défaut est terminée. Ensuite, nous allons mettre en place le tunnel **OpenVPN**.

## IV) Configurer un serveur VPS Linux avec OpenVPN pour le tunnelling

Activez la redirection d'IP dans votre noyau en utilisant la commande ci-dessous :

```
echo 'net.ipv4.ip_forward=1' | sudo tee -a /etc/sysctl.d/99-sysctl.conf
```

Cela permet de rediriger le trafic sur IPv4. Pour appliquer ces modifications, utilisez la commande ci-dessous :

```
sudo sysctl -p
```

**OpenVPN** ne supporte pas les tunnels simultanés sur IPv6 et IPv4, vous pouvez donc désactiver l'utilisation d'IPv6 :

```
sudo sysctl -w net.ipv6.conf.all.disable_ipv6=1
```

```
sudo sysctl -w net.ipv6.conf.default.disable_ipv6=1
```

Pour désactiver IPv6 manuellement, ajoutez les paramètres suivants qui doivent être définis au démarrage. Ces paramètres doivent être ajoutés au fichier **99-sysctl.conf** situé dans **/etc/sysctl.d/**. Utilisez simplement la commande **cd** pour accéder au dossier, et utilisez votre éditeur de texte (**notepad++** par exemple) pour éditer le fichier. N'oubliez pas de sauvegarder les changements effectués !

```
net.ipv6.conf.all.disable_ipv6 = 1  
  
net.ipv6.conf.default.disable_ipv6 = 1  
  
net.ipv6.conf.lo.disable_ipv6 = 1  
  
net.ipv6.conf.eth0.disable_ipv6 = 1
```

Ensuite, vous pouvez activer les nouveaux paramètres en utilisant :

```
sysctl -p
```

Ensuite, dans le fichier **hosts** situé dans **/etc/**, commentez la ligne de résolution IPv6 comme indiqué ci-dessous :

```
#::1    localhost ip6-localhost ip6-loopback
```

Avec cela, nous avons désactivé l'IPv6. Ensuite, connectez-vous à nouveau à l'URL d'administration du serveur et ouvrez les paramètres du **VPN**.

Log Reports  
**Configuration**  
License  
TLS Settings  
Network Settings  
**> VPN Settings**  
Advanced VPN  
Web Server  
Client Settings  
Failover

### VPN IP Network

Specify the addresses and netmasks for the virtual networks created for VPN clients

#### Dynamic IP Address Network

When a user does not have a specific VPN IP address configured on the **User Permissions** page, the user's VPN client is assigned an address from this network.

Network Address	# of Netmask bits
<input type="text" value="172.27.224.0"/>	<input type="text" value="20"/>

#### Static IP Address Network (Optional)

Any static VPN IP addresses specified for particular users on the **User Permissions** page must be within this network

Network Address	# of Netmask bits
<input type="text" value="Network Address"/>	<input type="text" value="CIDR netmask"/>

Dans la section Routage, l'option **Should VPN clients have access to private subnets** (non-public networks on the server side) ? doit être définie sur **No** :

### Routing

Should VPN clients have access to private subnets (non-public networks on the server side)?

☒ No
☐ Yes, using NAT
☐ Yes, using Routing

L'option **Should client Internet traffic be routed through the VPN ?** doit être définie sur **Yes**.

Should client Internet traffic be routed through the VPN?

☒ Yes

Pour éviter les fuites DNS, modifiez les paramètres du résolveur DNS. Sélectionner l'option **Have clients to use the same DNS servers as the Access Server host** :

### DNS Settings

Pushing DNS servers to clients is optional, unless clients' Internet traffic is to be routed through the VPN

Do not alter clients' DNS server settings

☐ No

Have clients use the same DNS servers as the Access Server host

☒ Yes

Have clients use specific DNS servers

☐ No



Enregistrez ces paramètres et n'oubliez pas de cliquer sur **Update Running Server**. Vous pouvez redémarrer le serveur **OpenVPN** en utilisant l'onglet **Status** de la console d'administration. Vous pouvez alors arrêter le serveur et le redémarrer.



Ceci complète notre configuration pour le serveur **OpenVPN**. Ensuite, nous pouvons vérifier les installations des clients.

## V. Comment connecter votre serveur VPN Linux à d'autres dispositifs avec OpenVPN

Maintenant que votre serveur est opérationnel, nous pouvons y connecter des dispositifs !

### 1. Comment installer et connecter le client OpenVPN sous Windows

- Ouvrez l'URL du client **OpenVPN**, vous pourrez voir les liens des téléchargements des clients pour les différents systèmes d'exploitation.
- Choisissez la version de **Windows** et exécutez l'installation.
- Une fois l'installation terminée, vous serez invité à saisir le nom d'utilisateur et le mot de passe **OpenVPN**. L'adresse IP du serveur sera remplie automatiquement.
- Vous pouvez utiliser l'icône **OpenVPN** de votre barre de tâches Windows pour vous déconnecter, vous reconnecter et afficher l'état de la connexion.
- Comment installer et connecter le client **OpenVPN** sous **MacOS**
- Connectez-vous à l'interface utilisateur du client **OpenVPN** puis cliquez sur le lien pour télécharger le logiciel **OpenVPN** pour **MacOS**. Une fois ce paquet téléchargé, une fenêtre s'ouvrira avec l'icône du paquet d'installation.
- Suivez la procédure standard d'installation des applications sous **MacOS**.
- Double-cliquez sur l'icône de cet installateur et cliquez sur Ouvrir pour lancer l'installation.
- Une fois l'installation terminée, vous pourrez voir l'icône **OpenVPN** sur votre barre de tâches **MacOS**. Vous pouvez faire un clic droit sur cette icône pour voir les différentes options. De là, vous pouvez vous connecter à **OpenVPN**.
- Une fois que vous cliquez sur l'option Se connecter, vous verrez un popup vous demandant le nom d'utilisateur et le mot de passe **OpenVPN**. Ici, vous devez entrer les informations d'identification et cliquer sur Connecter pour établir la connexion au serveur **VPN Linux**.

### 2. Comment installer et connecter le client OpenVPN sous Linux

Téléchargez et installez le client **OpenVPN** sur **CentOS** en utilisant la commande ci-dessous :

```
sudo yum install OpenVPN
```

Pour **OpenVPN** sur **Debian** ou **Ubuntu** en utilisant la commande ci-dessous :

```
sudo apt-get install openvpn
```

Ouvrez l'interface client d'**OpenVPN** et téléchargez le profil approprié pour votre système d'exploitation. Vous pouvez aussi utiliser la commande **wget** ou **curl** et fournir l'URL pour télécharger le logiciel.

Copiez le profil téléchargé dans l'emplacement **/etc/openvpn** et renommez-le en **client.conf**. Vous pouvez démarrer le service **OpenVPN** Tunnel où vous serez invité à saisir le nom d'utilisateur et le mot de passe.

Lancez l'opération en utilisant la commande suivante :

```
sudo service openvpn start
```

Vous pouvez utiliser **ipconfig** ou **ip addr** pour afficher les connexions réseau. Une fois que l'interface **VPN** est disponible, vous verrez une interface **tun0** ajoutée à la liste existante affichée dans le résultat.

### 3. Comment installer et connecter le client OpenVPN sous Android

Tout d'abord, visitez la boutique **Google Play** et recherchez l'application **OpenVPN Connect** et installez-la.

Une fois l'application ouverte, vous verrez trois options :

- Private Tunnel
- Access Server
- OpenVPN Pro le.

Sélectionnez **Access Server** et remplissez tous les détails manuellement :

- Title (titre) – définissez votre nom préféré pour la connexion
- Access Server Hostname – l'IP de votre serveur **VPN Linux**
- Port – le port 934 de votre serveur **VPN Linux**
- Username – le nom d'utilisateur défini sur votre serveur (**openvpn** par défaut) Password – le mot de passe que vous avez défini dans la console lors de la configuration du serveur **VPN Linux** dans le terminal

### 4. Comment installer et connecter le client OpenVPN sous iOS

Comme pour les appareils **Android**, vous pouvez installer l'application **OpenVPN** à partir de l'**App Store**.

Terminez l'installation et ouvrez l'application nouvellement installée. Il vous sera demandé de remplir les informations du profil, ou de télécharger le fichier de profil de la même manière que la version **Android**.

Une fois qu'ils sont ajoutés, vous pouvez commencer à utiliser **OpenVPN** sur votre **iPhone** ou **iPad**.

## VI) Paramètres de compression du serveur VPN Linux

Si vous êtes connecté au **VPN** et que vous ne pouvez pas naviguer sur Internet, vous pouvez consulter les logs d'**OpenVPN** sur **/var/log/openvpnas.log** dans votre **VPS**.

*Si vous trouvez des entrées similaires à celle présentée ci-dessous, il est fort probable que vous rencontriez des problèmes de compression :*

```
2019-03-23 18:24:05+0800 [-] OVPN 11 OUT: 'Mon Mar 23 08:59:05 2016 guest/123.45.67.89:55385 Bad  
compression stub decompression header byte: 251'
```



Pour résoudre ce problème, vous pouvez désactiver la compression. Cela peut être fait à partir de l'interface d'administration. Ouvrez l'interface d'administration et cliquez sur **Advanced VPN** (VPN avancé).

Passez à **Default Compression Settings** (Paramètres de compression par défaut). Désactivez ici l'option **Support compression on client VPN connections**.

## VII) Ajouter des utilisateurs au serveur VPN Linux utilisant OpenVPN

Le client **OpenVPN** gratuit supporte deux utilisateurs. Pour créer plus d'utilisateurs, vous devez sélectionner l'un des plans payants. Vous pouvez ajouter des utilisateurs supplémentaires à partir de l'interface d'administration. Naviguez vers l'onglet **User Management**, et cliquez sur le lien **User Permissions**.

Saisissez le nouveau nom d'utilisateur comme indiqué ci-dessous :

Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
openvpn	No Default Group		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
NEW USER	No Default Group		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Pour ce nouvel utilisateur, configurer des paramètres supplémentaires en cliquant sur le lien **More Settings**. Ici, vous pouvez fournir le mot de passe et d'autres détails.

Local Password:

( No Password Set )

Select IP Addressing:

☒ Use Dynamic ☐ Use Static

**Access Control**

Select addressing method:

☒ Use NAT ☐ Use routing

Allow **Access To** these Networks:

Allow **Access From**:

☐ all server-side private subnets

Allow **Access From**:

☐ all other VPN clients

**VPN Gateway**

Configure VPN Gateway:

☒ No ☐ Yes

**DMZ settings**

Configure DMZ IP address:

☒ No ☐ Yes

Enregistrez ces paramètres et cliquez sur l'option **Update Running Server**.

## VIII) Configurer des profils de connexion automatique pour un serveur VPN Linux avec OpenVPN

Avec **OpenVPN**, vous pouvez également configurer des profils de connexion automatique. Cela fera en sorte que tout votre trafic non local sera automatiquement routé via un **VPN**. Si vous souhaitez activer ou désactiver manuellement le **VPN**, vous pouvez utiliser des profils verrouillés d'utilisateur ou de serveur.

Pour définir la connexion automatique, ouvrez l'interface d'administration, puis sélectionnez le lien **User Permissions**. Ici, vous pouvez cocher la case **Allow Auto-login** (Autoriser la connexion automatique).

## IX) Comment tester un serveur VPN Linux sous OpenVPN

Pour tester si **OpenVPN** fonctionne comme prévu, connectez le client **VPN** et vérifiez votre adresse IP. Vous pouvez utiliser le site web de test de fuite DNS et IP depuis le navigateur (<https://browserleaks.com/ip>).

## X) Conclusion

Dans ce tutoriel, vous avez appris comment configurer un serveur **VPN Linux** exécutant **OpenVPN** et comment le connecter en utilisant différents clients comme **Windows, Linux, Android, iPhone** ou **iPad**, et **MacOS**.

Maintenant que vous connaissez tous les tenants et aboutissants de base, vous pouvez naviguer sur Internet en toute sécurité avec votre tout nouveau serveur **VPN Linux**. Pour en savoir plus, vous pouvez lire le manuel officiel **d'OpenVPN**, qui se trouve dans l'interface d'administration.

## XI) Bibliographie

<https://www.hostinger.fr/tutoriels/>

