# Installation et configuration d'un serveur VPN SSL (v4.4)

Tutorial conçu et rédigé par Michel de CREVOISIER –

## SOURCES

*Man OpenVPN :*

- http://lehmann.free.fr/openvpn/OpenVPNMan/OpenVPNMan-1.5.0.fr.1.0.html

*Howto :*

- http://openvpn.net/index.php/open-source/documentation/howto.html#numbering

# INDEX

# Préambule

L'objectif de ce tutorial est de vous présenter la mise en place d'un « *VPN SSL* » via le logiciel *OpenVPN*. L'avantage de ce type de VPN est, en plus d'une sécurité accrue, de ne pas être bloqué dans les cyber-cafés, aéroports ou tout autre lieu public … Notez toutefois que sur certaines « a*ppliance »* avancées, les connexions à des sites « *https* » peuvent être autorisées sans pour autant que le *VPN SSL* soit fonctionnel.

**Attention !** Si votre serveur est hébergé sur une plateforme virtuelle de type « *OpenVZ* », sachez que des manipulations supplémentaires non détaillées seront à effectuer (sources ici et ici).

L'installation du VPN s'effectuera sur la version « *Lenny AMD64 » de Debian* (téléchargement ici).

# 1. Installation du serveur

Commencez par installer les paquets suivants (inclut *bridge-utils)* :

```
aptitude install openvpn openssl
```

Créez un nouveau dossier pour *OpenVPN* :

```
mkdir /etc/openvpn/easy-rsa/
```

Copiez les fichiers de configuration dans ce nouveau répertoire :

```
cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /etc/openvpn/easy-rsa/
```

Modifiez les droits sur le répertoire :

```
chown -R $USER /etc/openvpn/easy-rsa/
```

# 2. Configuration du serveur

## 2.1 Initialisation

Initialisez les variables par défaut situées dans le fichier suivant :

```
nano /etc/openvpn/easy-rsa/vars
```

… en modifiant les informations suivantes à votre convenance (en bas de page) :

```
export KEY_COUNTRY="FR"
export KEY_PROVINCE="00"
export KEY_CITY="ville"
export KEY_ORG="organisation"
export KEY_EMAIL="mail.domaine.com"
```

Initialisez ensuite les variables des scripts grâce à la commande ***source*** :

```
cd /etc/openvpn/easy-rsa/
source vars
```

Réinitialisez le sous-dossier keys :

```
./clean-all
```

## 2.2 Génération des clefs et certificats

### *2.2.1 Autorité de certification racine*

Générez le certificat racine « **ca.cert** » ainsi que la clef d'autorité de certification racine « **ca.key** » :

```
./build-ca
```

### *2.2.2 Serveur OpenVPN*

Générez le certificat «**nom_srv_vpn.crt** » ainsi que la clef «**nom_srv_vpn.key** » :

```
./pkitool --server <nom_srv_vpn>
```

### 2.2.3 Paramètres « Diffie Hellman »

Générez le fichier « **dh1024.pem** » contenant les paramètres *Diffie Hellman* :

```
./build-dh
```

### 2.2.4 Clef statique « Man in the middle »

Cette commande crée une clef statique permettant d'éviter les attaques de type « *Man in the middle* » :

```
openvpn --genkey --secret keys/ta.key
```

## 2.3 Copie des clefs et certificats

### 2.3.1 Récapitulatif

A ce stade, vous devez disposer des fichiers suivants dans **/etc/openvp/easy-rsa/keys** :

- Certificat du serveur de certification (CA) : **ca.crt**
- Clef du serveur de certification (CA) : **ca.key**
- Certificat du serveur OpenVPN : **<srv_vpn_ssl>.crt**
- Clef du serveur OpenVPN : **<srv_vpn_ssl>.key**
- Paramètre *Diffie Hellman* : **dh1024.pem**
- Clef d'autorisation pour accès au démon : **ta.key**

### 2.3.2 Copie des fichiers

Copiez les fichiers du point précédent dans le répertoire ci-indiqué :

```
cd /etc/openvpn/easy-rsa/keys
cp ca.crt /etc/openvpn/
cp ca.key /etc/openvpn/
cp <srv_vpn_ssl>.crt /etc/openvpn/
cp <srv_vpn_ssl >.key /etc/openvpn/
cp dh1024.pem /etc/openvpn/
cp ta.key /etc/openvpn
```

## 2.4 Fichier de configuration serveur

### 2.4.1 Récupération d'un modèle

Vous pouvez récupérer un modèle de configuration dans le dossier ci-dessous :

```
cd /usr/share/doc/openvpn/examples/sample-config-files/
gunzip server.conf.gz
cp server.conf /etc/openvpn/
```

### 2.4.2 Paramètres

Une fois le fichier **server.conf** créé, adaptez le à votre besoin à l'aide de la configuration suivante :

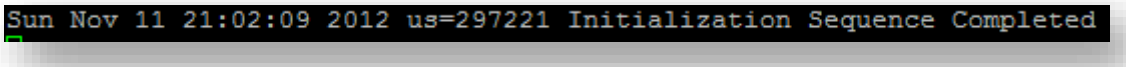
**################ CONFIG SERVEUR ################**
mode server
port 443
proto tcp-server
dev tun
**################ CLEFS ET CERTIFICATS ################**
ca /etc/openvpn/ca.crt
cert /etc/openvpn**/< srv_vpn_ssl >.**crt
key /etc/openvpn**/< srv_vpn_ssl >.**key
dh /etc/openvpn/dh1024.pem
tls-auth /etc/openvpn/ta.key 0
cipher AES-128-CBC
**################ PARAMETRES RESEAU ################**
***# Pool d'IP des clients VPN***
server **172.16. 0.0** 255.255.255.0
***#Paramètre DNS***
push "dhcp-option DNS 8.8.8.8"
***# Routage intégral du trafic via le tunnel VPN***
push "redirect-gateway def1 bypass-dhcp"
**################ LOGS ################**
***# Niveau log***
verb 4
***# Type de log***
log openvpn.log
***# Etat du serveur***
status openvpn-status.log
**################ AUTRES ################**
***# Ping toute les 10s et arrêt au bout de 2min***
keepalive 10 120
***# Activation compression (à activer également coté client)***
comp-lzo
***# Limites l'accès à certaines ressources lors du redémarrage***
persist-key
persist-tun

### 2.4.3 Vérifications

Une fois votre fichier de configuration terminé, exécutez la commande suivante pour vérifier sa configuration :

```
cd /etc/openvpn
openvpn server.conf
```

S'il a bien été configuré, la ligne suivante doit apparaitre en bas du *shell* :




**Attention !** Exécutez cette commande qu'après avoir copié votre fichier de configuration. Dans le cas contraire l'erreur du point 8.2 apparaîtra.

## 2.5 Génération des clefs et certificats

Pour terminer, générez le certificat et la clef pour l'utilisateur « pierre » :

```
cd /etc/openvpn/easy-rsa/
./build-key pierre
```

## 2.6 Transfert des fichiers

A l'aide de la commande *SCP* ou de **WinSCP**, transférez ces fichiers sur votre ordinateur :

- Certificat : **ca.crt**
- Certificat : **<user>.crt**
- Clef : **<user>.key**
- Clef : **ta.key**

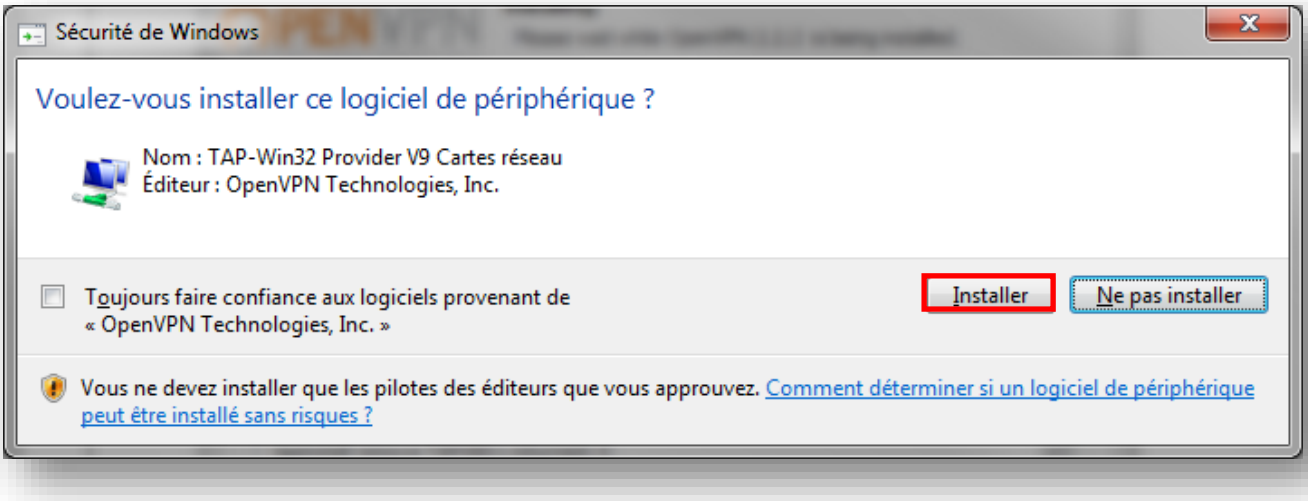
# 3. Installation du client

## 3.1 Client Windows « OpenVPN GUI »

### *3.1.1 Installation*

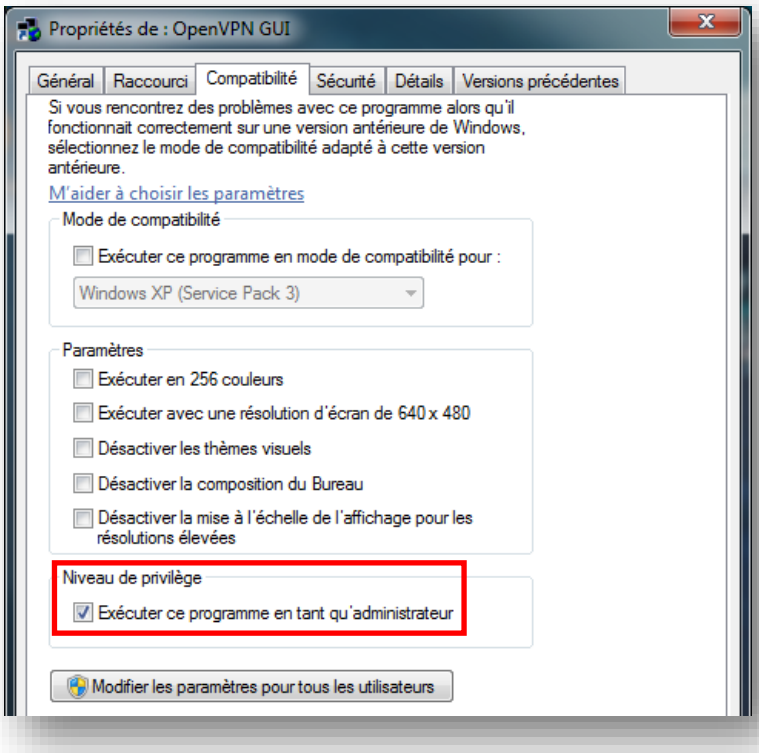
Le client sera installé sur un *Windows 7 SP1 x64*. Pour cela :

- Télécharger et installez le client *OpenVPN* ici
- Acceptez l'ajout d'une carte réseau de type « *TAP-Win32* »




### *3.1.2 Raccourci « administrateur »*

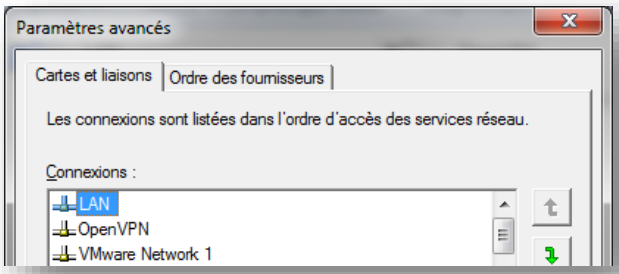
Modifiez le raccourci du programme afin de l'exécuter en tant qu'administrateur (*Vista, Seven* ou supérieur uniquement). Autrement, l'erreur du point 8.4 apparaîtra.



### 3.1.3 Ordonnancement des cartes réseau

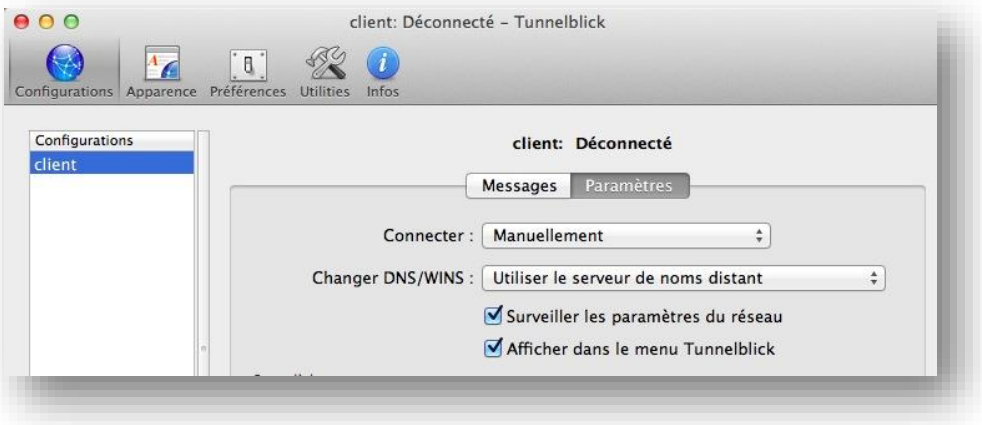
Modifiez l'ordre des adaptateurs réseaux de façon à placer votre carte réseau (WIFI et/ou Ethernet) avant l'adaptateur « Tap » créé par *OpenVPN.* Pour cela, allez dans :

- **Centre de réseau et partage >** touche *« Alt »* **> Avancé > Paramètres avancés**



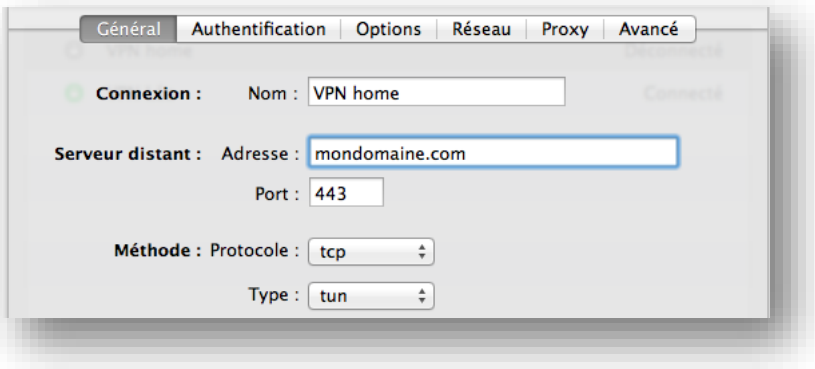

## 3.2 Client Mac « Tunnelblick »

Le client VPN par excellence pour Mac est sans aucun doute **Tunnelblick**. Il est gratuit et téléchargeable ici.




## 3.3 Client Mac & Windows « Viscosity » alternatif

Disposant d'une interface et d'une ergonomie beaucoup plus claire que « *Tunnelblick* », ce client VPN multiplateforme est probablement l'un des plus optimisés. Malgré le fait d'être payant (8$), il offre l'avantage d'éditer vos fichiers de configuration client en mode graphique…. De quoi ravir les utilisateurs les plus néophytes.




Téléchargement

# 4. Configuration du client

## 4.1 Fichier de configuration client

Créez un fichier nommé **config.ovpn** et copiez les paramètres suivants en les adaptant à votre besoin :

**################ CLEFS ET CERTIFICATS ################**
cert **<user>.**crt
key **<user>.**key
ca ca.crt
tls-auth ta.key 1
tls-client
cipher AES-128-CBC
persist-key
persist-tun
;tls-remote <X509>
**################ RESEAU ################**
remote **<nom de domaine>** 443
redirect-gateway def1
dev tun
resolv-retry 1
proto tcp-client
**################ AUTRES ################**
verb 3
comp-lzo
pull
nobind

## 4.2 Proxy

Si vous passez par un serveur proxy, vous devrez ajouter les lignes ci-dessous dans votre fichier de configuration client. Quant au fichier « authfile.txt », il devra contenir sur deux lignes votre login et votre mot de passe. Enfin, n'oubliez pas de **NE PAS renseigner de proxy** dans votre navigateur.

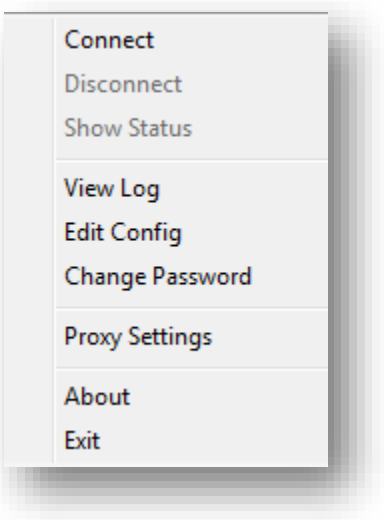
**################ PROXY ################**
;http-proxy **<IP proxy> <port>** authfile.txt basic **OU** ;http-proxy **<IP proxy> <port>** stdin basic
;http-proxy-retry
;http-proxy-option AGENT "Mozilla/5.0 (Windows; U; Windows NT 6.1; fr; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13 GTB7.1"

## 4.3 Client Windows « OpenVPN GUI »

### *4.3.1 Copie des fichiers*

Copiez les fichiers du point 2.6 dans le répertoire **C:\Program Files (x86)\OpenVPN\config**

### *4.3.2 Connexion*




## 4.4 Client Mac « Tunnelblick »

- Allez dans *Library/Application Support/Tunnelblick/Users/<user>*
- Créez un répertoire portant le nom de votre configuration (« VPN-maison » par exemple)
- Copiez les fichiers du point 2.6 dans ce répertoire
- Ajoutez l'extension « .tblk » à la fin du nom de ce répertoire
- Double cliquez sur ce dernier et validez la demande d'ajout
- Votre profil est dorénavant opérationnel

# 5. Routage

## 5.1 Routage interne

### 5.1.1 Activation du « forwarding »

Activez le routage de façon permanente :

```
nano /etc/sysctl.conf
```

Et dé-commentez la ligne ci-dessous :

```
net.ipv4.ip_forward=1
```

Vérification de l'état du routage (0 : désactivé, 1 : activé) :

```
cat /proc/sys/net/ipv4/ip_forward
```

ou

```
sysctl net.ipv4.ip_forward
```

### 5.1.2 Activation du NAT

L'ensemble du trafic de vos clients est dorénavant routé vers votre VPN. Toutefois, le réseau indiqué dans le fichier de configuration du serveur (option « **server 172.16.0.0 255.255.255.0** ») n'est pas connu par votre interface physique **eth0**. Il sera donc nécessaire de configurer le « routage » et le « NATage » des clients VPN vers cette interface. Pour cela exécutez la commande suivante :

```
iptables -t nat -A POSTROUTING -s 172.16.0.0/24 -o eth0 -j MASQUERADE
```

Notez toutefois que cette règle sera effacée au redémarrage du serveur. Vous devrez donc le rendre persistante dans votre fichier *iptables*.

## 5.2 Routage extérieur

Pour que votre VPN soit accessible depuis l'extérieur, il est nécessaire d'ouvrir le port 443 sur votre Box et de le rediriger vers l'IP de votre serveur VPN.

# 6. Sécurisation du serveur

## 6.1 Révocation des certificats

Si vous souhaitez révoquer un certificat utilisateur, exécutez la commande suivante et redémarrez le service *OpenVPN* :

Dans **server.conf**, ajouter la ligne suivante :

```
crl-verify easy-rsa/keys/crl.pem
```

Initialiser la variable *easy-rsa* :

```
source /etc/openvpn/easy-rsa/rsa
```

Révoquer le certificat du client :

```
./revoke-full <user>
service openvpn restart
```

## 7. Logs et débogage

Pour redémarrer le service OpenVPN :

```
/etc/init.d/openvpn restart
```

Pour vérifier que le service OpenVPN est bien lancé :

```
ps aux | grep openvpn
```

Pour afficher les processus utilisant le port 443 :

```
cat /etc/services|grep 443
```

Pour afficher les logs :

```
tail -f /etc/openvpn/openvpn.log
```

Pour afficher les interfaces réseau (dont **tun0**) :

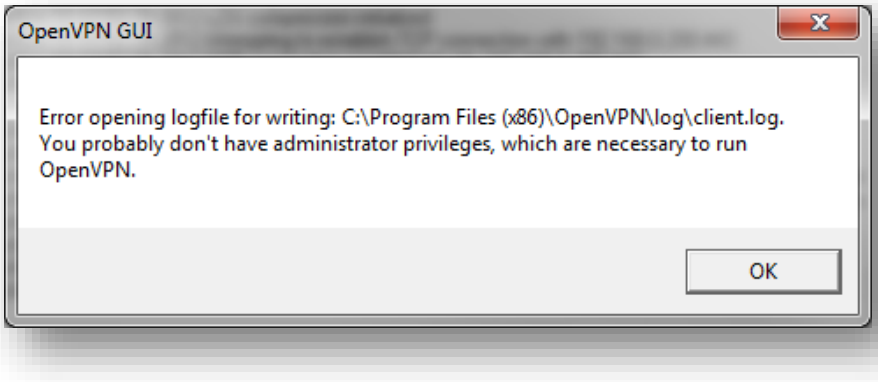
```
ifconfig
```

```
tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet adr:172.16.1.1  P-t-P:172.16.1.2  Masque:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

# 8. Erreurs

## 8.1 Logfile client

Lors du lancement de l'application (*XP* ou *Seven*), l'erreur suivante peut apparaître :




Dans ce cas, arrêtez le service *OpenVPN* dans les services Windows.

## 8.2 Socket bind on local adress

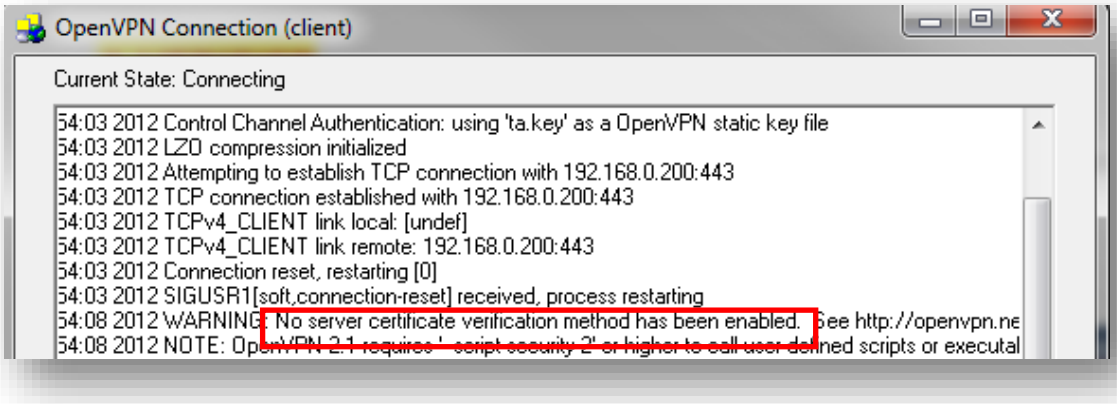
*TCP/UDP: Socket bind failed on local address [undef]: Address already in use*

Si vous avez exécutez la commande du *2.4.3* sans avoir copié le fichier de configuration, le service ne démarrera pas. Il se peut également qu'un autre processus (SSL, Apache) soit déjà en écoute sur ce port.

## 8.3 No certification verification

Cet avertissement est normal dans la mesure où vous ne disposez pas d'une vraie autorité de certification :

*WARNING: No server certificate verification method has been enabled*



## 8.4 Route failed

*Windows route add command failed : returned code 1*

*OpenVPN* n'a pas suffisant de droits pour ajouter des routes dans votre table de routage. Pour parer à ce problème, exécutez-le en tant qu'administrateur comme indiqué au point **3.1.2**.

## 8.5 UDP : connection reset by peer

L'erreur suivante apparaît :

*UDPv4: Connection reset by peer (WSAECONNRESET) (code=10054)*

Et un coup de sniffer vous montre ceci :

| | | |
|---|---|---|
| ICMP DestUnreach | Port unreachable: 192.168.0.150 | ICMP Port Unreachable |
| HTTPS | Src= 1194,Dst= 443 ,L= 14 | |
| ICMP DestUnreach | Port unreachable: 192.168.0.150 | ICMP Port Unreachable |

Cette erreur vient du fait que vous n'avez pas spécifié le protocole à utiliser (UDP ou TCP). Hors si aucun paramètre n'est spécifié, l'UDP est utilisé par défaut. Vérifiez alors la présence des paramètres **proto tcp-client** et **proto tcp-server** dans vos fichiers de configuration.

*N'hésitez pas m'envoyer vos commentaires ou retours à l'adresse suivante :*

m.decrevoisier *A-R-0-B-A-5* outlook . com

*Soyez-en d'ores et déjà remercié*