OpenVPN

Information

OpenVPN est un logiciel libre permettant de créer, ou de se connecter a un VPN.

Ce logiciel permet a des utilisateurs de se connecter a un réseau de manière crypté, grâce a des Certificats, un login et un mot de passe. Il utilise de manière intensive la bibliothèque d'authentification OpenSSL ainsi que les protocoles SSLv3/TLSv1.

Disponible sur Linux / Windows / Mac OS X / iOS / Android, c'est l'une des solutions les plus sécurisés.

Mise en place d'une solution d'OpenVPN

1 - Préparation du serveur

L'installation du serveur ce fait sur Debian 8.5
Cette page peux se retrouver obsolète d'ici quelques mois, mais la procédure se retrouvera sensiblement identique.

2 - Installation de l'OpenVPN

OpenVPN étant certifié par la communauté Debian, le paquet est donc disponible librement sur leur dépôts officiel. Il suffi de rentrer :

```
apt-get update
apt-get install openvpn
```

Le paquet emporte avec lui de base des fichiers pour configurer le chiffrement par clé. la configuration de base y etant aussi importé, nous allons la copier au sein du répertoire OpenVPN.

```
mkdir /etc/openvpn/easy-rsa/
cp -r /usr/share/easy-rsa/* /etc/openvpn/easy-rsa/
```

Nous allons simplifier la création des clé chiffré avec l'ajout de paramètres de base, cela sera les information de l'entreprise par exemple:

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

Il faut modifier les valeurs suivantes:

```
export KEY_COUNTRY="FR"
export KEY_PROVINCE="06"
```

```
export KEY_CITY="Nissa"
export KEY_ORG="nicolargo.com"
export KEY_EMAIL="dtc@hadopi.fr"
```

On va créer la clé privé et publique du serveur:

```
cd /etc/openvpn/easy-rsa/
source vars
./clean-all
./build-dh
./pkitool --initca
./pkitool --server server
openvpn --genkey --secret keys/ta.key
```

On va déplacer la clé du serveurs ainsi que celle de chaques clients dans un dossier spécifiques

```
mkdir /etc/openvpn/clés
cp keys/ca.crt keys/ta.key keys/server.crt keys/server.key keys/dh2048.pem
/etc/openvpn/clés
```

VOIR FICHIER server.conf (modifier “route 10.0.0.1 netmask” par l'ip de ta gateway“)

```
sh -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'
```

```
iptables -I FORWARD -i tun0 -j ACCEPT
iptables -I FORWARD -o tun0 -j ACCEPT
iptables -I OUTPUT -o tun0 -j ACCEPT
```

```
iptables -A FORWARD -i tun0 -o eth0 -j ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
```

Pour activer la règle au reboot :

```
sh -c "iptables-save > /etc/iptables.rules"
```

Il faut rajouter cette ligne dans /etc/network/interfaces sous “iface eth0 inet ...”

```
pre-up iptables-restore < /etc/iptables.rules
```

Création clé utilisateur: Modifier l'ip dans clés/exemple.ovpn (ligne remote) le 1194 correspond au port

Il suffira de lancer le script newclient.sh pour obtenir une clé client (ca.crt et ta.key sont publique et commune a tous les utilisateurs)

le fichier “nom du clients”.ovpn peut etre lancer par le clients.
ATTENTION le client doit l'ouvrir avec C:\ProgramFiles\OpenVPN\bin\openvpn.exe (En administrateur)

Sources : Blog de Nicolargo (Obselete)

Note :

Règle iptables pour rediriger les requêtes vers une autre une ip (NAT 1.1) sans modification de l'adresse qui émet

```
iptables -t nat -A PREROUTING -p tcp -d 188.165.42.128 -j DNAT --to-destination 10.8.0.6
```

Note 2 :

Le packet Resolvconf installer nativement sur Debian bloque les modifications DNS invoqué par Openvpn. Pour outrepasser cela, il suffit de rajouter les lignes suivante dans le fichier de configuration du client :

```
script-security 2
up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf
```