DOCUMENTATION TECHNIQUE – MISE EN PLACE D'UN VPN

CONTEXTE :

Ce projet a été réalisé dans le cadre d'un **projet étudiant** ayant pour but de mettre en œuvre un **VPN personnel** en utilisant la solution libre **OpenVPN**. L'objectif principal est de permettre à un utilisateur de se connecter à distance à son réseau local (domicile, etc.) de manière sécurisée, même s'il ne se trouve pas sur le même réseau (Wi-Fi extérieur, réseau mobile, etc.).
L'installation a été effectuée à des fins pédagogiques et personnelles, et ne constitue pas une solution professionnelle. Le matériel utilisé (serveur personnel, box Internet, etc.) n'est pas conçu pour des performances élevées, une tolérance aux pannes ou un usage à grande échelle.

Ce projet s'adresse à toute personne souhaitant :

- accéder à son réseau domestique depuis l'extérieur (NAS, caméra IP, imprimante, fichiers partagés, etc.),
- renforcer la sécurité de sa connexion sur des réseaux publics (Wi-Fi d'hôtel, aéroport, etc.),
- découvrir concrètement le fonctionnement et la configuration d'un VPN basé sur **OpenVPN.**

⚠️ **Avertissement**
Ce projet étant un travail étudiant, il peut présenter certaines limites de fiabilité ou de sécurité. Il n'a pas été testé dans des conditions de production professionnelle et peut ne pas parfaitement fonctionner dans tous les cas.
Il est fortement déconseillé de l'utiliser pour des données sensibles ou des environnements critiques.

MATÉRIEL NÉCESSAIRE :

MACHINE VIRTUEL :

Oracle VM Virtualbox(lien cliquable) dans l'onglet **VirtualBox Platform Packages**, choisissez la version qui correspond à l'OS de votre PC et exécutez l'installateur

VirtualBox Extension Pack(lien cliquable) dans l'onglet **VirtualBox Extension Pack**, cela permet à ta VM de reconnaitre si une clé usb est branché et donc d'échanger des fichiers entre votre VM et votre PC. Pour voir comment l'implémenté merci de vous rendre au 1. b) clé usb

ISO Ubuntu Server(lien cliquable)

OUTILS:

Clé USB pour pouvoir échanger des fichiers entre votre PC et la VM

OPTIONNEL :

Si vous souhaitez pouvoir utilisez le VPN de n'importe où (**à distance**) sans avoir la VM sur votre PC, vous aurez besoin d'un **autre PC** qui assez performant pour faire tourner la VM en permanence, donc branché et connecté à votre box

MATÉRIEL NÉCESSAIRE :

1. CRÉATION DE LA MACHINE VIRTUELLE:

A) Paramétrage à la création

Nom	**vpn-server**
ISO Image	**Ubuntu Server** (fichier téléchargé plus haut)
Type	**Linux**
Version	**Ubuntu (64-bit)**
RAM	**2048 Mo** (1024 devrait être suffisant mais pas sureté)
Processeurs	**2** (Idem que la RAM pour 1 seul processeur)
Disque dur	**25 Go** (Idem, 10 devrait suffire)

B) Paramétrage post création

Réseau - Accès par pont :

Cliquez sur : **Configuration → Réseau → Mode d'accès réseau → Accès par ponts**

Clé USB :

Allez dans vos fichiers, double cliquez l'extension que vous avez téléchargez précédemment, cette dernière vous renverra sur Virtualbox, cliquez sur le bouton mise à jour. Après cela cliquez sur **Configuration → USB**, activez le **contrôleur usb** et mettez le en **2.0** puis après avoir branché votre clé usb appuyer sur le logo de **câble usb avec une croix verte,** sur la droite (2ème icône en partant du haut) et cliquez sur l'élément qui correspond à votre clé usb

2. INSTALLATION UBUNTU SERVER DANS LA VM

Langue	**Français**
Clavier	**Français - Français** (la vm peut vous faire passez un petit test pour déterminer exactement le clavier que vous possédez)
Ubuntu Classic	**Oui**
Ubuntu minimized	**Non**
Ubuntu Pro	**Non**
Installation SSH	**Oui**
Ajout de clé	**Non**
nom du serveur	**vpn-serveur** (à votre choix)
login	**vpnadmin** (à votre choix)
password	**azertyvpn** (à votre choix)

2. INSTALLATIONS

A) Mise à jour :

sudo apt update && sudo apt upgrade -y

B) Installation OpenVPN + EasyRSA :

udo apt install openvpn
sudo apt install easy-rsa

3. GÉNÉRATION DES CERTIFICATS

sudo make-cadir ~/openvpn-ca
cd ~/openvpn-ca/
.easyrsa init-pki
.easyrsa build-ca
New CA Key Passphrase: azerty01 (au choix)
Common Name : vpn-ca
.easyrsa gen-req server nopass
common Name : passnote
.easyrsa sign-req server server
yes
azerty01 (CA Key Passphrase)
.easyrsa gen-dh
openvpn --genkey secret ta.key
mv ta.key pki/
.easyrsa gen-req client1 nopass
Common Name : clio1 (au choix)
.easyrsa sign-req client client1
yes
azerty01 (CA Key Passphrase)

4. . CONFIGURATION DU SERVEUR VPN

A)Copie des fichiers dans /etc/openvpn :

sudo cp pki/ca.crt pki/issued/server.crt pki/private/server.key pki/dh.pem pki/ta.key /etc/openvpn/

B) Création des fichiers de config serveur :

sudo nano /etc/openvpn/server.conf
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt

key server.key
dh dh2048.pem
auth SHA256
tls-auth ta.key 0
server 10.8.0.0 255.255.255.0
push "dhcp-option DNS 1.1.1.1"
keepalive 10 120
data-ciphers AES-256-GCM:AES-128-GCM
data-ciphers-fallback AES-256-GCM
persist-key
persist-tun
status openvpn-status.log
log-append /var/log/openvpn.log
verb 3

CTRL + s (sauvegarder les modifications du fichier)
CTRL + x (fermer l'outils d'édition)

sudo cp /etc/openvpn/server.conf /etc/openvpn/vpnadmin.conf (par sureté du mauvais conf)
sudo cp /etc/openvpn/server.conf /etc/openvpn/vpn-server.conf (idem)

5. CONFIGURATION DU ROUTAGE & DU FIREWALL

A) Activation du routage IP :

sudo nano /etc/sysctl.conf
Enlevez : net.ipv4.ip_forward=1

CTRL + s
CTRL + x

B. Autorisation du trafic NAT :

sudo sysctl -p
sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o enp0s3 -j MASQUERADE
(Remplace enp0s3 par le nom de ton interface réseau (trouve-le avec ip a))
azertyvpn (mot de passe utilisateur paramétré sur la vm au démarrage)
sudo apt install iptables-persistent
NO
sudo netfilter-persistent save

6. DÉMARRAGE DU VPN

sudo systemctl start openvpn@server

sudo systemctl enable openvpn@server
sudo systemctl start openvpn@vpnadmin
sudo systemctl enable openvpn@vpnadmin
sudo systemctl start openvpn@vpn-server
sudo systemctl enable openvpn@vpn-server

7. CRÉATION DU FICHIER CLIENT

A) Copie des certificats :

mkdir -p ~/client-configs/files

cp ~/openvpn-ca/pki/ca.crt ~/client-configs/files/
cp ~/openvpn-ca/pki/issued/client1.crt ~/client-configs/files/
cp ~/openvpn-ca/pki/private/client1.key ~/client-configs/files/
sudo cp /etc/openvpn/ta.key ~/client-configs/files/ //sans faire exprès copier le fichier en mettant comme propriétaire root
sudo cp /etc/openvpn/ta.key ~/client-configs/files/
sudo chown vpnadmin:vpnadmin ~/client-configs/files/ta.key

B) Création du fichier client1.ovpn :

mkdir -p ~/client-configs
nano ~/client-configs/base.conf
dedans :

```
client
dev tun
proto udp
remote <IP_de_ta_VM> 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
auth SHA256
data-ciphers AES-256-GCM:AES-128-GCM
data-ciphers-fallback AES-256-GCM
key-direction 1
verb 3

<ca>
</ca>
<cert>
</cert>
<key>
</key>
```

<tls-auth>
</tls-auth>

⚠️Important :

Remplace VOTRE_IP_PUBLIQUE par l'adresse IP publique de ton serveur (ou un nom de domaine si tu en as un). (tu peux le voir avec "curl ifconfig.me") (82.124.180.105 pour moi)
Le key-direction 1 doit être là si tu utilises tls-auth. (Regarde dans ton fichier /etc/openvpn/server.conf si tu utilise tls-auth ta.key 0)

nano ~/client-configs/make_config.sh
dedans :

```
#!/bin/bash

# Usage: ./make_config.sh client1

KEY_DIR=~/client-configs/files
OUTPUT_DIR=~/client-configs/files
BASE_CONFIG=~/client-configs/base.conf

cat ${BASE_CONFIG} \sud
<(echo -e '<ca>') \
${KEY_DIR}/ca.crt \
<(echo -e '</ca>\n<cert>') \
${KEY_DIR}/$1.crt \
<(echo -e '</cert>\n<key>') \
${KEY_DIR}/$1.key \
<(echo -e '</key>\n<tls-auth>') \
${KEY_DIR}/ta.key \
<(echo -e '</tls-auth>') \
> ${OUTPUT_DIR}/$1.ovpn
```

```
sudo chmod +x ~/client-configs/make_config.sh

cd ~/client-configs
./make_config.sh client1
```

Tu obtiendra ~/client-configs/files/client1.ovpn et si tu l'ouvre tu retrouvera le contenu de base.ovpm avec ceux de ca.crt ta.key client1.key et client1.ctr
ouvrez avec sudo nano client1.ovpn pour voir si il n'a pas doublé les <> (un vide celui que vous avez repli et un rempli fait par make_config.sh)

C) transfert du fichier client (client1.ovpn) :

Comme vous avez installez l'extention de virtualbox et l'avait paramétré, branché votre clé usb au pc, puis tapé les ligne de commandes suivantes :

lsblk (affiche les périphérique branché (je crois))

Si la clé usb est reconnue, vous aurez un périphérique sous sdb0 à l'intitulé sdb1 (personnellement), si à la fi de cette ligne il n'y a aucun chemin défini comme pour les autres péréphériques, tapez les commandes :

sudo mkdir /mnt/
sudo mkdir /mnt/usb/
sudo mound /dev/sdb1/ /mnt/usb/

puis déplacé avec cp votre fichier client1.ovpn dans ce nouveau dossier auquel l'on à attribuer le port de votre clé usb et ù vous trouverez tous les fichiers de votre clé

8. CONNECTION AU VPN (CLIENT)

A. Installation du client OpenVPN sur ton PC hôte :

OPenVPN Connect: (meilleur interface)

- Windows : https://openvpn.net/client/
- Linux : sudo apt install openvpn
- Android/iOS : "OpenVPN Connect"

OPenVPN GUI: (meilleur terminal, recommandé pour trouver les erreurs)

- Windows : https://openvpn.net/community-downloads/

9. TESTS

Une fois connecté :

- Ping 10.8.0.1 (le serveur VPN)
- Vérifie ton IP sur https://monip.org pour voir si tu passes par la VM
- Essaie d'accéder à d'autres machines internes si configurées

*. VÉRIFICATIONS ET MANIPULATIONS DIVERSES

Durant mes problèmes sur ma vm, j'ai rencontré certains problèmes que je ne saurais me rappeler totalement ou les placer, voici donc une liste de commande pour faire des est et modifications diverses :

VPN Server :

sudo systemctl status openvpn@NOM_DU_VPN affiche le status de votre server (si mauvais non testé avec nom utilisateur aussi
sudo systemctl enable openvpn@NOM_DU_VPN active le VPN
sudo systemctl disable openvpn@NOM_DU_VPN désactive le VPN
sudo systemctl start openvpn@NOM_DU_VPN lance le VPN
sudo systemctl restart openvpn@NOM_DU_VPN relance le VPN

FireWall :

sudo ufw status permet de voir le status des ports que vous utilisez
sudo ufw disable désactive les firewalls
sudo ufw enable active les firewalls
sudo ufw allow 1194/udp ouvre le port 1194 en UDP (n'exempte pas de devoir le faire sur la box)
sudo iptables -L -n -v | grep 1194 affiche des règles concernant le port 1194 (grep 1194)
sudo netstat -tulnp | grep 1194 affichage de l'état((ouver, écoute,...) du port 1194

IP :

ipconfig (Windows) donne les ips liés à votre pc, (votre ip pc est l'ipv4 tout en haut, c'est l'ip qui changera
ip a (Linux) donne les ips liés à votre machine, celui du 2: correspond à l'ip de la machine le 3: (10.8.0.1 pour moi) à l'ip du serveur celui à ping pour tester
ping ton.ip.à.viser envoie des fichiers test à une adrèsse ip pour tester la commuication entre ces 2 p&riphérique

Box internet :

https://VOTRE_IP (dans le moteur de recherche) permet d'accéder à l'interface de votre box pour pouvoir gérer/ouvrir les ports

Gestion fichier :

cp /emplacement/fichier /emplacement/nouveau/fichier copie d'un fichier
chmod 777 /emplacement/fichier modification des permissions d'un fichier ou dossier (777=tous les droits)
chown utilisateur2:utilisateur2 /emplacement/fichier passage de la possession du fichier à un autre utilisateur
l**s -l /emplacement** affichage des fichiers et dossier contenues à l'emplacement donné

Vérifications Logs :

sudo journalctl -xeu openvpn affiche le journal de log du serveur, permet aussi de voir les erreurs rencontrées
sudo tail -f /var/log/openvpn.log Idem mais pou si OpenVPN est dans un fichier log

<u>Manipulation fichier:</u>

sudo nano /emplacement/fichier permet d'ouvrir un outilts d'édition du contenu du fichier (crée le fichier si non existant)

SI certaines manque, je vous prie de m'excuser, je les ais soit jugé pas nécessaire de vous les notez soit je les ait oubliées

Par Raphaël PHAN, Lucie BARREZ et Thibaud TABARD