




Sécurisation des accès distants par VPN (La solution OpenVPN)

Ershad RAMEZANI



Table des matières

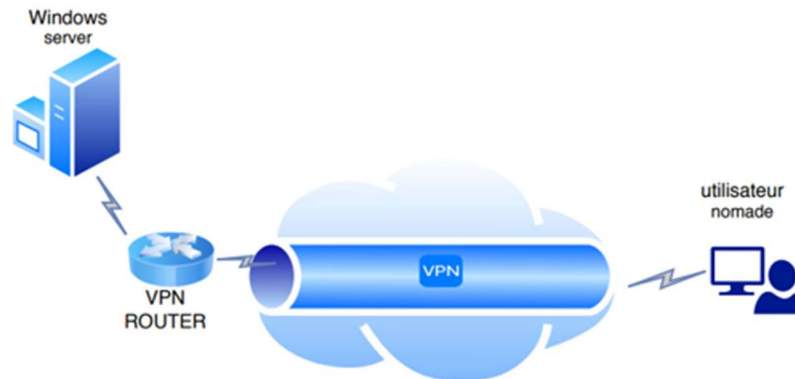
Introduction	4
La solution proposée.....	4
La mise en place de la solution	4
Mise en place du réseau	5
Le schéma du réseau.....	5
Configuration système et l'adressage IP.....	5
Installation d'un routeur Pfsense.....	5
Schéma de la création des certificats	6
Création de la « CA » (autorité de certification)	7
Création du serveur OpenVPN.....	8
Création de la paire clé/certificat pour le serveur OpenVPN	8
Installation du paquet OpenVPN	8
Diffie-Hellman	9
Ta.key	9
Server.conf.....	9
Activer l'OpenVPN.....	10
Fichier configuration .ovpn pour les clients.....	11
Création de la clé privée et du certificat pour le client.....	11
Le répertoire pour fichier .ovpn.....	11
Les clés nécessaires pour fichier .ovpn	11
Création d'un fichier script	12
Création d'un fichier base.conf.....	12
création de fichier .ovpn	13
Envoyer le fichier .ovpn au client.....	13
Teste depuis le client dans le même réseau	13
Teste depuis le client dans le réseau externe derrière pfsense avec NAT	14
Ajouter une règle NAT sur l'interface WAN de pfsense.....	14
Modifier le fichier stagiaire.ovpn.....	14
Teste de connexion	14
Test de RDP	15
Client-spécifique :	15
Définir les adresses pour les clients	15
Modifier le fichier server.conf	15
Créer les fichier config ccd pour chaque client spécifique	16
Créer les admin.ovpn et prestataire.ovpn	16
Test depuis client admin et client prestataire	16
Règles iptables pour limiter des accès.....	17
Les accès depuis tunnel OPENVPN	17



Mettre tous les stratégies en DROP	17
Redonner les accès aux réseaux internes	17
définir les accès pour les clients distants.....	18
Accès connexion sur le port 1194	18
Accès pour l'admin à distant.....	18
accès pour le prestataire à distant.....	18
accès pour les stagiaire à distant	18

Introduction

L'entreprise ADRARFORM souhaite mettre en place une solution permettant à ses employés d'accéder de manière sécurisée à son réseau local depuis un bureau à distance. Le serveur de fichiers, qui stocke les documents de tous les salariés, est situé dans le LAN. Chaque utilisateur dispose d'un compte sur le serveur Windows et n'a accès qu'aux documents auxquels il est autorisé.



La solution proposée

Pour répondre à ce cahier des charges, deux solutions VPN de type SSL sont proposées : OpenVPN et WireGuard. Tous deux utilisent des protocoles VPN open-source sécurisés s'ils sont correctement implémentés. WireGuard est plus récent et plus rapide qu'OpenVPN, grâce à ses algorithmes de chiffrement plus rapides. De plus, il est plus facile à entretenir. En revanche, OpenVPN est plus ancien et compatible avec des systèmes d'exploitation et des protocoles de chiffrement plus nombreux. Il est donc plus populaire et plus utilisé.

La mise en place de la solution

OpenVPN a été installé sur une machine virtuelle Debian qui joue le rôle de routeur et de serveur OpenVPN. Pour améliorer la sécurité, la configuration OpenVPN intègre des tunnels en fonction des profils utilisateurs. Les adresses IP VPN sont attribuées en fonction des profils et des clients connectés :

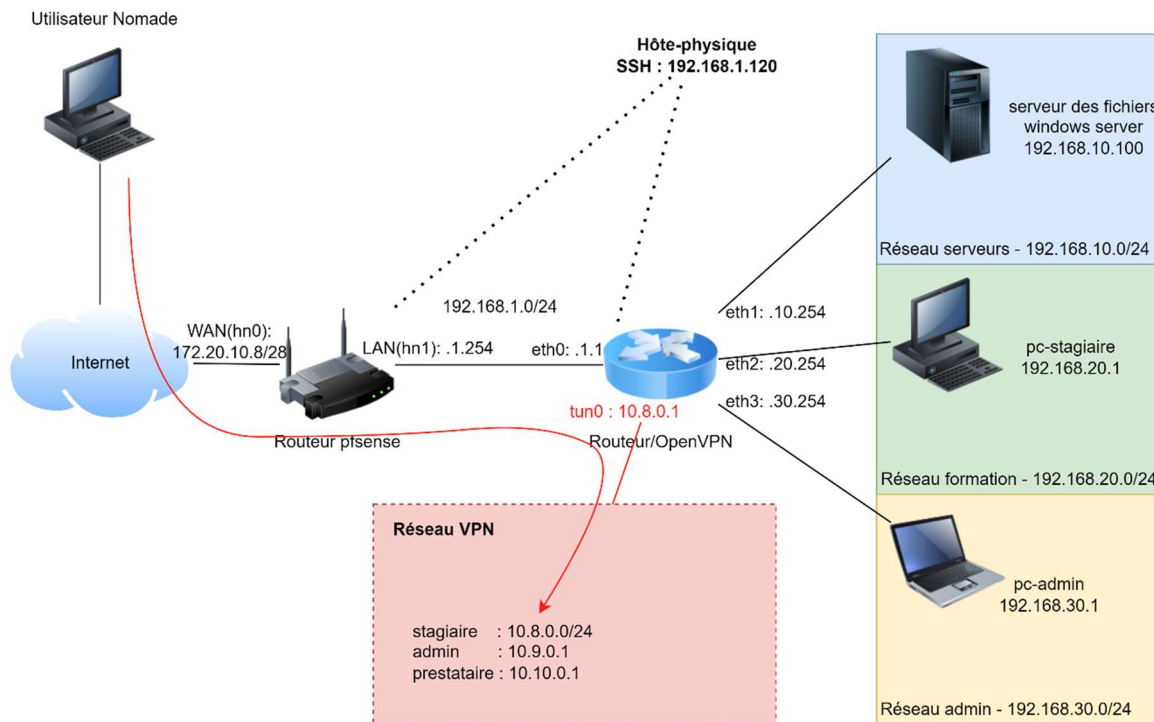
- 10.8.0.0/24 pour les utilisateurs nomades standards tels que les stagiaires,
- 10.9.0.0/30 pour l'administrateur,
- 10.10.0.0/30 pour le prestataire.

Ensuite, des règles iptables ont été mises en place sur le routeur/OpenVPN pour gérer les accès des différents utilisateurs aux différentes parties du réseau et renforcer la sécurité. Les NAT ont été configurés sur les box internet pour permettre l'accès distant au réseau interne.

Mise en place du réseau

Le schéma du réseau

Le schéma du réseau est le suivant :



Configuration système et l'adressage IP

La machine Debian est installée sur Hyper-V et possède 4 interfaces internes. L'interface eth0 est connectée au routeur PfSense, qui est une autre machine virtuelle et joue le rôle de routeur. Trois autres interfaces sont connectées aux réseaux *serveurs*, *formation* et *admin*.

Les machines dans les réseaux serveurs, formation et admin sont également des machines virtuelles installées sur le même Hyper-V et possèdent des interfaces en interne. L'interface interne de l'hôte physique est configurée en réseau 192.168.1.0 et peut se connecter au routeur/OpenVPN en SSH et au routeur PfSense en HTTPS.

Le routeur PfSense possède deux interfaces : une interne (LAN, hn1) vers le routeur/OpenVPN et une externe (WAN, hn0) vers le point d'accès Internet. L'interface LAN est configurée en statique et l'interface WAN a récupéré son adresse IP (172.20.10.8/28) par DHCP du réseau externe. Le serveur DHCP est activé sur l'interface LAN du routeur PfSense pour qu'il fournisse les adresses IP dans la plage 192.168.1.0/24. Cela permet au routeur/OpenVPN de récupérer une adresse IP sur l'interface eth0 au moment de l'installation.

Sur le routeur/OpenVPN, IPv4 IP forwarding et le NAT ont été configurés pour que les machines puissent communiquer entre elles et avec Internet.

Installation d'un routeur PfSense

Pour installer le routeur PfSense sur une machine virtuelle, il suffit de suivre ce lien :

<https://neptunet.fr/pfsense-install/>

Les interfaces WAN (par DHCP) et LAN (en statique) sont configurées, ainsi qu'un serveur DHCP sur l'interface LAN :

Interfaces		
WAN	10Gbse-T <full-duplex>	172.20.10.8
LAN	10Gbse-T <full-duplex>	192.168.1.254

Subnet	192.168.1.0
Subnet mask	255.255.255.0
Available range	192.168.1.1 - 192.168.1.254
Range	From 192.168.1.10 To 192.168.1.20

Les interfaces sur le routeur/OpenVPN

Lors de l'installation de la machine Debian, l'interface eth0 est choisie comme interface par défaut. Cette interface récupère son adresse IP depuis le routeur Pfsense et télécharge les paquets d'installation nécessaires. Les autres interfaces seront ajoutées manuellement dans le fichier `/etc/network/interfaces`.

IP forwarding sur le routeur/OpenVPN

Pour activer IP forwarding sur le routeur/OpenVPN, il faut modifier le fichier `sysctl.conf` avec la commande : `nano /etc/sysctl.conf`. Ensuite, décommentez la ligne `net.ipv4.ip_forward=1` et réactivez les règles avec la commande : `sysctl -p /etc/sysctl.conf`. À présent, la machine est un routeur.

Le NAT sur le routeur/OpenVPN

Les machines (serveurs, formation et admin) peuvent communiquer entre elles, mais elles ne peuvent pas communiquer avec le routeur Pfsense, car la passerelle du routeur Pfsense est le point d'accès Internet et il ne connaît pas les réseaux derrière le routeur/OpenVPN. Pour résoudre ce problème, il faut natter tous ces réseaux sur l'interface eth0 avec la commande suivante :

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Pour rendre cette règle de NAT permanente, il faut sauvegarder les règles iptables dans un fichier avec l'utilisateur root (il faut sauvegarder les règles à chaque fois que l'on ajoute une nouvelle règle) :

```
iptables-save > /etc/iptables-rules.save
```

Ensuite, il faut restaurer les règles au démarrage de la machine en ajoutant cette ligne à la fin du fichier interface :

```
post-up iptables-restore < /etc/iptables-rules.save
```

Pour vérifier le NAT après le redémarrage de la machine, on peut utiliser la commande suivante :

```
sudo iptables -t nat -L
```

Il faut ensuite vérifier que toutes les machines se voient en utilisant la commande ping.

```
# The primary network interface
allow-hotplug eth0
iface eth0 inet static
    address 192.168.1.1/24
    gateway 192.168.1.254
    dns-nameservers 8.8.8.8
    dns-search adrarform.local

allow-hotplug eth1
iface eth1 inet static
    address 192.168.10.254/24

allow-hotplug eth2
iface eth2 inet static
    address 192.168.20.254/24

allow-hotplug eth3
iface eth3 inet static
    address 192.168.30.254/24

post-up iptables-restore < /etc/iptables-rules.save
```

```
ladmin@rt-vpn:~$ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target prot opt source destination

Chain INPUT (policy ACCEPT)
target prot opt source destination

Chain POSTROUTING (policy ACCEPT)
target prot opt source destination
MASQUERADE all -- anywhere anywhere

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
ladmin@rt-vpn:~$
```

```
C:\Users\Administrateur.WIN-1I2H332VN80>ping 8.8.8.8

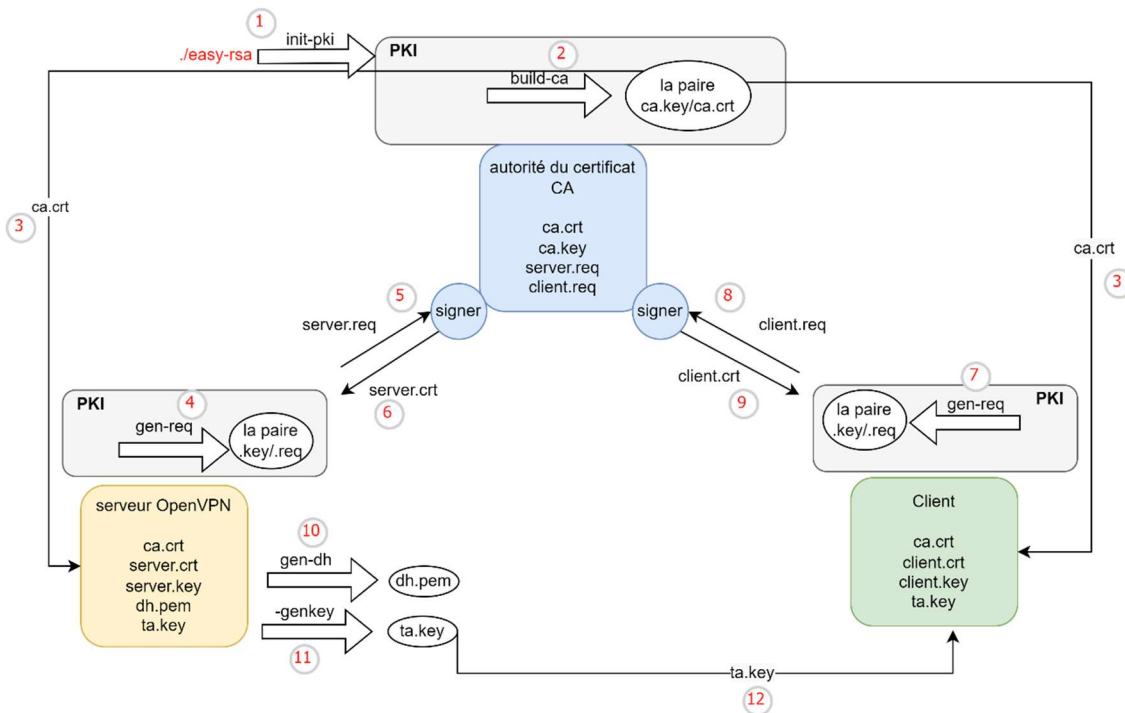
Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données
Réponse de 8.8.8.8 : octets=32 temps=94 ms TTL=108
Réponse de 8.8.8.8 : octets=32 temps=77 ms TTL=108
Réponse de 8.8.8.8 : octets=32 temps=82 ms TTL=108
Réponse de 8.8.8.8 : octets=32 temps=73 ms TTL=108

Statistiques Ping:
    Paquets : envoyés = 4, reçus = 4 (perte = 0%),
    Durée approximative :
    Minimum = 73ms, maximum = 94ms, Moyenne = 81ms
```

le serveur du fichiers peut aller jusqu'à Internet

Schéma de la création des certificats

OpenVPN est un protocole VPN qui utilise TLS/SSL pour sécuriser les connexions. En effet, il utilise des certificats pour crypter les échanges de données entre le serveur et les clients.



Création de la « CA » (autorité de certification)

Nous avons mis en place notre propre autorité de certification (CA) afin d'émettre des certificats de confiance. Pour cela, nous avons utilisé EasyRSA pour construire notre infrastructure à clés publiques (PKI) du CA.

La PKI est un groupe d'équipements physiques qui nous aide à créer des certificats numériques permettant de lier la clef publique d'un utilisateur à sa vraie identité. Nous utiliserons la PKI pour générer des clés privées et des certificats pour le serveur CA, le serveur OpenVPN et les clients.

Il est important de noter que bien que nous ayons créé le CA sur le routeur/OpenVPN, en production il est conseillé de le mettre sur un serveur autonome. En effet, la gestion de l'autorité de certification à partir d'une machine distincte sur le serveur OpenVPN permet de réduire les risques de corruption des certificats.

Voici les étapes pour installer EasyRSA sur le routeur/OpenVPN et créer notre propre CA :

1. Tout d'abord, installer le paquet EasyRSA en utilisant la commande suivante : **apt install easy-rsa**.
2. Ensuite, copier le dossier entier d'EasyRSA (/usr/share/easy-rsa) dans le répertoire personnel (/home/ladmin) en utilisant la commande suivante : **cp -r /usr/share/easy-rsa /home/ladmin/**.
3. Renommer le fichier vars.example en vars en utilisant la commande suivante : **mv /home/ladmin/easy-rsa/vars.example /home/ladmin/easy-rsa/vars**.
4. Modifier le fichier vars pour qu'il corresponde à notre entreprise. Cette étape est optionnelle mais recommandée pour des raisons de sécurité.
5. Aller dans le répertoire /home/ladmin/easy-rsa et créer le pki en utilisant la commande suivante : **./easyrsa init-pki**.
6. Créer le CA en utilisant la commande suivante : **./easyrsa build-ca nopass**. Cette commande créera deux fichiers : ca.crt et ca.key.

ca.crt : Le fichier ca.crt représente le certificat public de l'autorité de certification et il joue un rôle important dans le contexte d'OpenVPN. Il permet au serveur et au client de s'authentifier mutuellement en confirmant qu'ils font partie du même réseau de confiance. Par conséquent, pour que le système fonctionne correctement, chaque client et le serveur doivent disposer d'une copie de ce fichier.

ca.key : Quant au fichier `ca.key`, il s'agit de la clé privée utilisée par la machine CA pour signer les clés et les certificats des clients et des serveurs. Si un attaquant parvient à accéder à cette clé privée, il sera capable de signer des demandes de certificat et accéder au VPN, ce qui compromettra sa sécurité. Il est donc crucial de garder le fichier `ca.key` sur la machine CA uniquement et, si possible, de maintenir cette dernière hors ligne lorsqu'elle ne signe pas de demandes de certificat, afin de renforcer la sécurité du système.

```
ladmin@rt-vpn:~$ cd /home/ladmin
ladmin@rt-vpn:~$ tree
.
├── easy-rsa
│   ├── easyrsa
│   ├── openssl-easyrsa.cnf
│   ├── vars.example
│   └── x509-types
│       ├── ca
│       ├── client
│       ├── code-signing
│       ├── COMMON
│       ├── server
│       └── serverClient
```

```
pk
├── ca.crt
├── certs_by_serial
├── index.txt
├── issued
├── openssl-easyrsa.cnf
├── private
│   └── ca.key
├── renewed
│   ├── certs_by_serial
│   ├── private_by_serial
│   └── reqs_by_serial
├── reqs
├── revoked
│   ├── certs_by_serial
│   ├── private_by_serial
│   └── reqs_by_serial
├── safessl-easyrsa.cnf
└── serial
```

Création du serveur OpenVPN

Création de la paire clé/certificat pour le serveur OpenVPN

La création du serveur OpenVPN implique la création d'une paire clé/certificat. Pour ce faire, vous pouvez suivre ces étapes :

1. Accédez au répertoire `easy-rsa`.
2. Utilisez la commande `./easyrsa gen-req server nopass` pour créer une paire clé/req pour le serveur. Cette étape générera deux fichiers : `server.key` et `server.req`.
3. Signez le fichier `server.req` et créez le certificat `server.crt` en utilisant la commande `./easyrsa sign-req server server`. Notez que le premier `server` dans la commande est utilisé pour définir le type de requête, tandis que le deuxième fait référence au nom commun du serveur OpenVPN.

```
ladmin@rt-vpn:~/easy-rsa$ sudo ./easyrsa sign-req server server
Note: using Easy-RSA configuration from: ./vars
Using SSL: openssl OpenSSL 1.1.1n 15 Mar 2022

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 1080 days:
subject=
  commonName = server

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from /home/ladmin/easy-rsa/pki/safessl-easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName = ASN.1 #12: 'server'
```

```
pk
├── ca.crt
├── certs_by_serial
│   └── 6F3A7AD7D8F3D7E755A934468FFBB8D7.pem
├── extensions.temp
├── index.txt
├── index.txt.attr
├── index.txt.old
├── issued
│   └── server.crt
├── openssl-easyrsa.cnf
├── private
│   ├── ca.key
│   └── server.key
├── renewed
│   ├── certs_by_serial
│   ├── private_by_serial
│   └── reqs_by_serial
├── reqs
│   └── server.req
├── revoked
│   ├── certs_by_serial
│   ├── private_by_serial
│   └── reqs_by_serial
├── safessl-easyrsa.cnf
└── serial
    └── serial.old
```

Installation du paquet OpenVPN

Installer le paquet `openvpn`. Son répertoire sera au `/etc/openvpn`. Le serveur OpenVPN a besoin de sa paire clé/certificat et aussi le certificat de CA. Donc on va copier ces trois dans le répertoire d'OpenVPN.

**La version complète est disponible aussi
mais protégée par un mot de passe.**

Merci de me contacter par email :

Ershad.ra@gmail.com