



Validation VPN Nomade

Wireguard/Mikrotik

Auteur Anthony CLAIRON

Date : 14/05/2024

Sommaire

1. Introduction.....	2
2. Configuration serveur (Mikrotik).....	3
3. Configuration client	4
4. Specs.....	7

1. Introduction

Cette feature est validée afin de pouvoir continuer à proposer du VPN Nomade sur la solution Yugo, même après le passage en mikrotik.

Wikipédia :

il est conçu avec les objectifs de facilité d'utilisation, de performances et de surface d'attaque basse. Il vise une meilleure performance et une plus grande économie d'énergie que les protocoles IPsec et OpenVPN Tunneling.

Informations de crypto : <https://www.wireguard.com/protocol/>

Wireguard propose des protocoles par défaut, ce qui en plus de simplifier la configuration, permet d'éviter l'utilisation de protocoles « faibles ».

2. Configuration serveur (Mikrotik)

Pour commencer à monter un VPN Nomade avec Wireguard, il faut créer un serveur (variables en orange) :

```
/interface wireguard
add listen-port=13231 mtu=1314 name=VPN-Nomade
/ip firewall filter add action=accept chain=input dst-port=13231 protocol=udp
place-before=0 comment="wireguard"
```

(<https://lists.zx2c4.com/pipermail/wireguard/2017-December/002201.html>,
mtu 4G = 1394, je pars du principe que dans le futur on utilisera peut-être de
l'ipv6).

Puis lui assigner un subnet, que les clients utiliseront.

```
/ip address add address=172.16.255.1/24 interface=VPN-Nomade network=172.16.255.0
```

3. Configuration client

Wireguard est disponible sur de multiples plateformes,

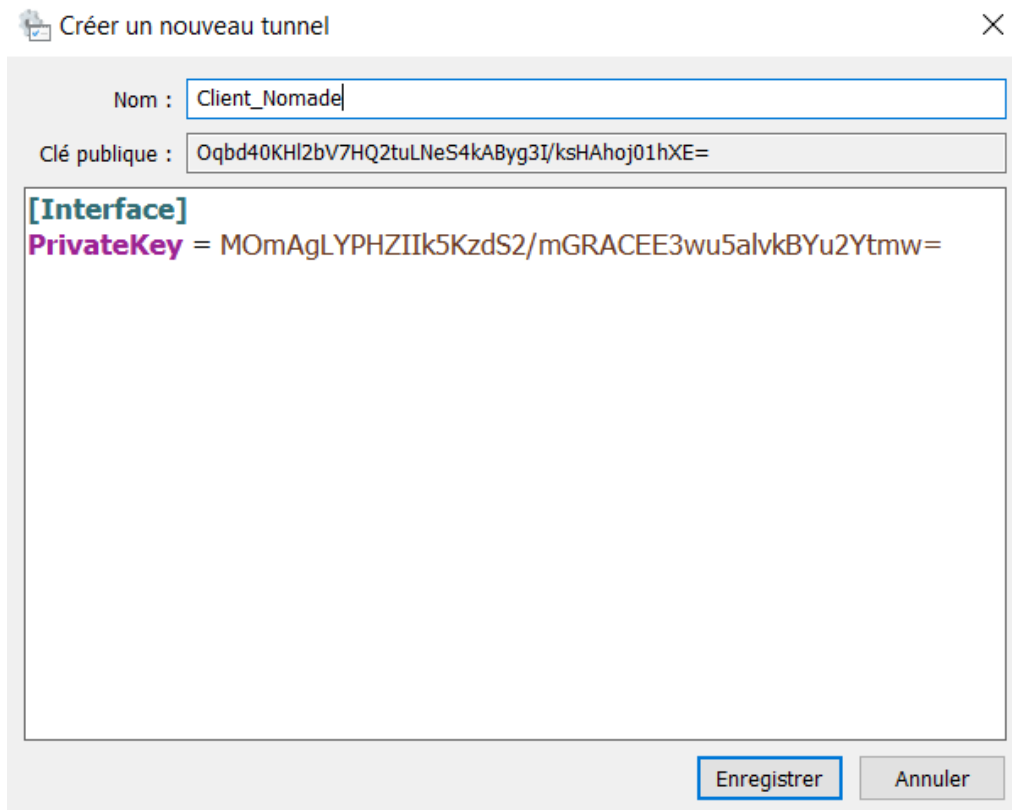
<https://www.wireguard.com/install/>

Pour ma part, j'ai effectué cette validation en utilisant mon poste de travail, Windows.

Une fois le logiciel lancé, cliquer sur ajouter un tunnel vide afin d'en créer un.



Cela va créer par défaut une clé privée ainsi qu'une clé publique :



Créer un nouveau tunnel

Nom : Client_Nomade

Clé publique : Oqbd40KHI2bV7HQ2tuLNeS4kAByg3I/ksHAhoj01hXE=

[Interface]
PrivateKey = MOmAgLYPHZIIk5KzdS2/mGRACEE3wu5alvkBYu2Ytmw=

Enregistrer Annuler

Retourner ensuite sur le routeur pour afficher la clé publique du serveur :

```
/interface wireguard  
print
```

```
[admin@TEST-YUGO_FIBRE] /interface/wireguard> print  
Flags: X - disabled; R - running  
0 R name="VPN-Nomade" mtu=1314 listen-port=13231  
   private-key="IHvwds881B8h3GsdUse5RMA09sRlgrAOQ2/lxPGjiWI="  
   public-key="mgHM352Z3G/xD+lgYeIGkfJZqJF+Nr4C4ps1Cy/eWmo="
```

Puis revenir sur le client (avec la clé pub du serveur) et y inscrire les renseignements ci-dessous :

```
[Interface]
PrivateKey = MOmAgLYPHZIIk5KzdS2/mGRACEE3wu5alvkBYu2Ytmw=
Address = 172.16.255.2/32
DNS = 172.16.255.1
[Peer]
AllowedIPs = 172.16.255.0/24, 192.168.1.0/24
Endpoint = 185.182.107.126:13231
PublicKey = mgHM352Z3G/xD+1gYeIGkfJZqJF+Nr4C4ps1Cy/eWmo=
```

Les champs [interface] contiennent :

- La clé privée générée automatiquement
- L'adresse IP du client Nomade
- Un serveur DNS

Les champs [peer] contiennent :

- Les subnets que l'on va chercher à atteindre via le tunnel (possibilité d'ajouter 0.0.0.0/0 pour faire transiter tout le trafic par le VPN)
- L'adresse et le port d'écoute du serveur
- La clé publique du serveur

Enfin, il faut créer le client sur le serveur :

```
/interface wireguard peers
add allowed-address=172.16.255.2/32 interface=VPN-Nomade public-key="
Oqbd40KH12bV7HQ2tuLNeS4kAByg3I/ksHAhoj01hXE="
```

[Client] Cliquer sur Activer :

Interface : Client_Nomade

État : ☐ Éteinte

Clé publique : Oqbd40KHI2bV7HQ2tuLNeS4kAByg3I/ksHAhoj01hXE=

Adresses : 172.16.255.2/32

Serveurs DNS : 172.16.255.1

Activer

4. Specs

<https://www.wireguard.com/performance/>

Vielles données, mais donne une idée

