



Table des matières

Introduction.....	2
Architecture.....	2
Mise en place coté serveur	2
Activer la configuration et l'interface.....	4
Configuration du client.....	4

Introduction

Ces dernières années un nouveau type de vpn a fait son apparition c'est wireguard qui utilise des algorithmes inédits et ce veut plus plus simple d'utilisation que le vpn SSL et aussi plus rapide

Avec wireguard il n'ya pas de relation client-to-server mais peer-to-peer

Architecture

2 machines

Machine 01 : 192.168.1.80

Machine 02 : 192.168.1.81

Réseau wireguard : 50.0.0.0 /24

Mise en place coté serveur

Ne pas oublier d'activer l'ipv4 forwarding avant tout

Il faut d'abord installer wireguard

```
apt install wireguard
```

Ensuite il faut générer la clef publique et la mettre dans un fichier ainsi que la clef privée

```
root@node2:~# wg genkey > /etc/wireguard/private.key
Warning: writing to world accessible file.
Consider setting the umask to 077 and trying again.
root@node2:~# cat /etc/wireguard/private.key | wg pubkey > /etc/wireguard/public.key
root@node2:~#
```

On a généré la clef privée et sa clef public correspondante

Ensuite la clef privée on l'affiche ici très important

```
root@node2:/etc/wireguard# cat private.key
MAFaYSZsbN9nMoNZbpCNFqY1UwdifN3u0xsq/D5b03o=
root@node2:/etc/wireguard#
```

Ensuite on met en place le fichier de conf de wireguard

nano /etc/wireguard/wg0.conf

Mieux vaut utiliser Debian 12 que 11

```
GNU nano 7.2                               wg0.conf
[Interface]
#Adresse du serveur dans le réseau VPN_
Address = 60.0.0.1/24
SaveConfig = true
ListenPort = 51194
PrivateKey = +JNEPULW2heNXTQETIOq0RWEKCo3xBTr1wNUssx0hno=
```

Dans WireGuard, l'option SaveConfig dans le fichier de configuration (comme wg0.conf que vous avez montré) a une fonction très spécifique. Quand SaveConfig est défini sur true, cela signifie que les modifications apportées à la configuration du VPN pendant son fonctionnement seront sauvegardées dans le fichier de configuration lorsque le VPN sera arrêté.

Activer la configuration et l'interface

Wg-quick up wg0

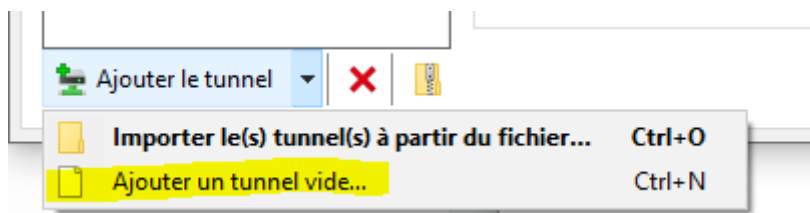
Et pour désactiver

Wg-quick down wg0

```
root@debian:/etc/wireguard# wg-quick up wg0
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 60.0.0.1/24 dev wg0
[#] ip link set mtu 1420 up dev wg0
root@debian:/etc/wireguard# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:00:01:2f brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.177/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 42627sec preferred_lft 42627sec
    inet6 2a01:e0a:2e2:afb0:215:5dff:fe00:12f/64 scope global dynamic mngtmpaddr
        valid_lft 86266sec preferred_lft 86266sec
    inet6 fe80::215:5dff:fe00:12f/64 scope link
        valid_lft forever preferred_lft forever
4: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN group default qlen 1000
    link/none
    inet 60.0.0.1/24 scope global wg0
        valid_lft forever preferred_lft forever
root@debian:/etc/wireguard#
```

Configuration du client

J'ai installé le client sur un windows 10



Modifier le tunnel

Nom : test

Clé publique : BiY+VxngafPujehEyPfb5YNRq3BOPQIqWwCDUjwZaT4=

[Interface]
 PrivateKey = 2CIsc32nIx/qhBX5nkShcDHO1K1NOa1HzwIRJJPmymc=
 Address = 60.0.0.2/32

[Peer]
 PublicKey = JCj1IAKAZ+K+udfQ8xUY62w4g6xi7fYZkasGYEfKQk=
 AllowedIPs = 0.0.0.0/0, 60.0.0.0/24
 Endpoint = 192.168.1.177:51194
 PersistentKeepalive = 20

Bloquer tous le trafic hors tunnel (interrupteur)

Il y'a maintenant une clef publique tout en haut qui est très important qui sera placée dans le fichier de conf du serveur apres

On a ensuite une clef privée qui existe par défaut et on définit l'adresse dans le tunnel

Ensuite dans la section [Peer] c'est les infos du serveur

On a la clef publique du serveur a renseigné ici ensuite les réseaux par lesquelles il faudra passer par le tunnel pour y accéder pour faire passer tout le trafic mettre 0.0.0.0/0

Et le endpoint c'est l'ip accessible du serveur et le port sur lequel il écoute

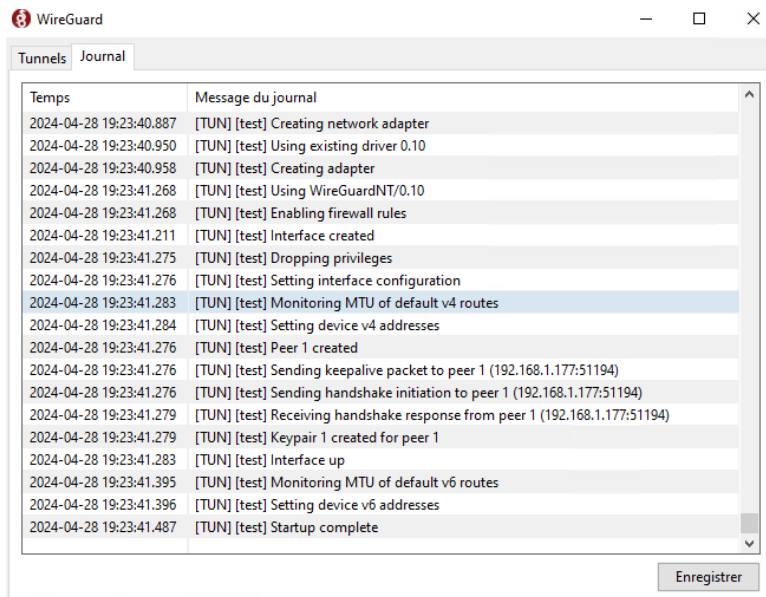
Du coté du serveur voila notre configuration

```
[Interface]
Address = 60.0.0.1/24
ListenPort = 51194
PrivateKey = +JNEPULW2heNXTQETIOq0RWEKCo3xBTr1wNUsx0hno=

[Peer]
PublicKey = BiY+VxngafPujehEyPfb5YNRq3BOPQIqWwCDUjwZaT4=
AllowedIPs = 192.168.110.2/32, 0.0.0.0/0, 60.0.0.2/32
```

Nous avons juste rajouter une case « Peer » dans laquelle nous avons renseigné la clef public du client + les IP par lesquelles il a le droit de ce connecter

Dans le journal coté client voila ce que nous pouvons observer



The screenshot shows the WireGuard application window with the 'Journal' tab selected. The window title is 'WireGuard'. The log contains the following entries:

Temps	Message du journal
2024-04-28 19:23:40.887	[TUN] [test] Creating network adapter
2024-04-28 19:23:40.950	[TUN] [test] Using existing driver 0.10
2024-04-28 19:23:40.958	[TUN] [test] Creating adapter
2024-04-28 19:23:41.268	[TUN] [test] Using WireGuardNT/0.10
2024-04-28 19:23:41.268	[TUN] [test] Enabling firewall rules
2024-04-28 19:23:41.211	[TUN] [test] Interface created
2024-04-28 19:23:41.275	[TUN] [test] Dropping privileges
2024-04-28 19:23:41.276	[TUN] [test] Setting interface configuration
2024-04-28 19:23:41.283	[TUN] [test] Monitoring MTU of default v4 routes
2024-04-28 19:23:41.284	[TUN] [test] Setting device v4 addresses
2024-04-28 19:23:41.276	[TUN] [test] Peer 1 created
2024-04-28 19:23:41.276	[TUN] [test] Sending keepalive packet to peer 1 (192.168.1.177:51194)
2024-04-28 19:23:41.276	[TUN] [test] Sending handshake initiation to peer 1 (192.168.1.177:51194)
2024-04-28 19:23:41.279	[TUN] [test] Receiving handshake response from peer 1 (192.168.1.177:51194)
2024-04-28 19:23:41.279	[TUN] [test] Keypair 1 created for peer 1
2024-04-28 19:23:41.283	[TUN] [test] Interface up
2024-04-28 19:23:41.395	[TUN] [test] Monitoring MTU of default v6 routes
2024-04-28 19:23:41.396	[TUN] [test] Setting device v6 addresses
2024-04-28 19:23:41.487	[TUN] [test] Startup complete

An 'Enregistrer' button is located at the bottom right of the window.