Création d’un VPN Wireguard.

// EMERSON FRANCISCO

Pour commencer, nous rentrons dans « sources.list »

```
root@VPN-MAISON:~# nano /etc/apt/sources.list
```

Ensuite nous allons commencer par désactiver les MAJ via les dépôts du CD. Une fois mis les lignes, vous pouvez sauvegarder

```
  GNU nano 5.4                  /etc/apt/sources.list
# deb cdrom:[Debian GNU/Linux 11.3.0 _Bullseye_ - Official amd64 DVD Binary-1 2>

#deb cdrom:[Debian GNU/Linux 11.3.0 _Bullseye_ - Official amd64 DVD Binary-1 20>

deb http://debian.proxad.net/debian/ bullseye main
deb-src http://debian.proxad.net/debian/ bullseye main

deb http://security.debian.org/debian-security bullseye-security main contrib
deb-src http://security.debian.org/debian-security bullseye-security main contr>

# bullseye-updates, to get updates before a point release is made;
# see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#_updates>
deb http://debian.proxad.net/debian/ bullseye-updates main contrib
deb-src http://debian.proxad.net/debian/ bullseye-updates main contrib




                [ Lecture de 14 lignes ]
^G Aide       ^O Écrire     ^W Chercher   ^K Couper     ^T Exécuter   ^C Emplacement
^X Quitter    ^R Lire fich. ^\ Remplacer  ^U Coller     ^J Justifier  ^_ Aller ligne
```

Commençons l’installation de Wireguard :

sudo apt-get install wireguard

```
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  wireguard-tools
Paquets suggérés :
  openresolv | resolvconf
Les NOUVEAUX paquets suivants seront installés :
  wireguard wireguard-tools
0 mis à jour, 2 nouvellement installés, 0 à enlever et 46 non mis à jour.
Il est nécessaire de prendre 94,3 ko dans les archives.
Après cette opération, 344 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://ftp.fr.debian.org/debian bullseye/main amd64 wireguard-tools amd64 1.0.20210223-1 [86,2 kB]
Réception de :2 http://ftp.fr.debian.org/debian bullseye/main amd64 wireguard all 1.0.20210223-1 [8□164 B]
94,3 ko réceptionnés en 0s (2□110 ko/s)
Sélection du paquet wireguard-tools précédemment désélectionné.
(Lecture de la base de données... 52862 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../wireguard-tools_1.0.20210223-1_amd64.deb ...
Dépaquetage de wireguard-tools (1.0.20210223-1) ...
Sélection du paquet wireguard précédemment désélectionné.
Préparation du dépaquetage de .../wireguard_1.0.20210223-1_all.deb ...
Dépaquetage de wireguard (1.0.20210223-1) ...
Paramétrage de wireguard-tools (1.0.20210223-1) ...
wg-quick.target is a disabled or a static unit, not starting it.
Paramétrage de wireguard (1.0.20210223-1) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
```

Puis crée les clefs privés et public via cette commande :

wg genkey | sudo tee /etc/wireguard/wg-private.key

wg pubkey | sudo tee /etc/wireguard/wg-public.key

Puis regarder la valeur de celle-ci via la commande :

cat /etc/wireguard/wg-private.key

Puis copier la

```
 GNU nano 5.4                    /etc/wireguard/wg0.conf *
[Interface]
Address = 192.168.11.254/24
SaveConfig = true
ListenPort = 51820
PrivateKey =
```

Grace à la commande :

nano /etc/wireguard/wg0.conf pour crée une interface wg0, renseignez son adresse IP, Son port d'écoute (par défaut 51820), puis renseigner sa clef privée

```
root@VPN-MAISON:~# wg-quick up wg0
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 192.168.11.254/24 dev wg0
[#] ip link set mtu 1420 up dev wg0
root@VPN-MAISON:~#
```

Puis il faut monter l'interface crée via cette commande :

Pour voir si notre interface a bien été créé et a bien été monter on peut faire un ip a

```
root@VPN-MAISON:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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
       valid_lft forever preferred_lft forever
2: enp0s25: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
 group default qlen 1000
    link/ether 00:0f:fe:c8:09:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.254/24 brd 192.168.1.255 scope global noprefixroute enp0s25
       valid_lft forever preferred_lft forever
    inet6 fe80::20f:feff:fec8:987/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
4: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN gro
up default qlen 1000
    link/none
    inet 192.168.11.254/24 scope global wg0
       valid_lft forever preferred_lft forever
root@VPN-MAISON:~#
```

```
root@VPN-MAISON:~# systemctl enable wg-quick@wg0.serv
root@VPN-MAISON:~#
```

Par la suite, il faut activer le lancement automatique du service au démarrage

Puis nous allons installer ufw pour se faire faite :

apt install ufw

On ajoute des règles sur le pare feu crée comme SSH et Wireguard :

ufw allow 22/tcp

ufw allow 51820/udp

Éditer le fichier sysctl.conf et activer ip_forward pour se faire rajouter cette ligne à la fin du fichier : *net.ipv4.ip_forward = 1*

```
  GNU nano 5.4                          /etc/sys
# Do not send ICMP redirects (we are not a
#net.ipv4.conf.all.send_redirects = 0
#
# Do not accept IP source route packets (w
#net.ipv4.conf.all.accept_source_route = 0
#net.ipv6.conf.all.accept_source_route = 0
#
# Log Martian Packets
#net.ipv4.conf.all.log_martians = 1
#

###################################################################
# Magic system request Key
# 0=disable, 1=enable all, >1 bitmask of sysrq functions
# See https://www.kernel.org/doc/html/latest/admin-guide/sysrq.html
# for what other values do
#kernel.sysrq=438

net.ipv4.ip_forward = 1

^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^\ Remplacer ^U Coller    ^J Justifier ^_ Aller ligne
```

```
2: enp0s25: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
 group default qlen 1000
    link/ether 00:0f:fe:c8:09:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.254/24 brd 192.168.1.255 scope global noprefixroute enp0s25
       valid_lft forever preferred_lft forever
    inet6 fe80::20f:feff:fec8:987/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
root@VPN-MAISON:~# nano /etc/ufw/before.rules
```

Puis copier le nom de votre interface physique pour pouvoir router les paquets entre les deux interfaces pour ce faire faite un nano /etc/ufw/before.rules et mettez cela à la fin :

NAT - IP masquerade

```
# NAT - IP masquerade
*nat
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -o enp0s25 -j MASQUERADE

# End each table with the 'COMMIT' line or these rules won't be processed
COMMIT
```

NAT - IP masquerade

*nat

:POSTROUTING ACCEPT [0:0]

-A POSTROUTING -o MonInterface -j MASQUERADE

End each table with the 'COMMIT' line or these rules won't be processed
COMMIT

Ensuite rajoutez les réseaux que nous autorisons à notre pare-feu via ces lignes :

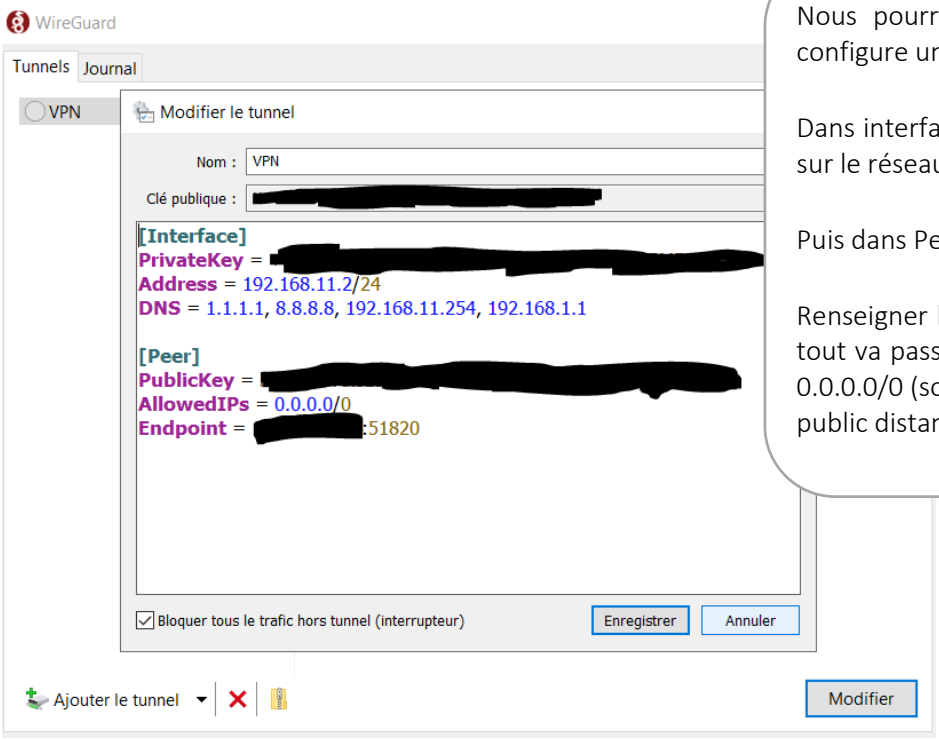
-A ufw-before-forward -s MONRESEAU/MASQUE -j ACCEPT

-A ufw-before-forward -d MONRESEAU/MASOUE -i ACCEPT

```
# allow forwarding for trusted network
-A ufw-before-forward -s 192.168.1.0/24 -j ACCEPT
-A ufw-before-forward -d 192.168.1.0/24 -j ACCEPT
-A ufw-before-forward -s 192.168.11.0/24 -j ACCEPT
-A ufw-before-forward -d 192.168.11.0/24 -j ACCEPT
```

Puis on active notre pare-feu avec cette commande :

```
root@VPN-MAISON:~# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
root@VPN-MAISON:~# systemctl restart ufw
root@VPN-MAISON:~#
```



Nous pourrons ensuite installer le client et on configure un nouveau tunnel.

Dans interface renseigner l'adresse qui va prendre sur le réseau du VPN et les DNS à utiliser

Puis dans Peer

Renseigner la clef publique du serveur, on dit que tout va passer par le VPN via la ligne AllowedIPs = 0.0.0.0/0 (son point de terminaison est l'adresse IP public distante avec son port)

Ensuite on éteint l'interface pour pouvoir configurer le Peer

```
root@VPN-MAISON:~# wg-quick down wg0
[#] wg showconf wg0
[#] ip link delete dev wg0
root@VPN-MAISON:~#
```

Dans le Peer on renseigne la clef publique de L'hôte et l'adresse IP qu'il doit prendre

```
root@VPN-MAISON:~# wg-quick up wg0
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 192.168.11.254/24 dev wg0
[#] ip link set mtu 1420 up dev wg0
root@VPN-MAISON:~#
```

On redémarre L'interface et on regarde si le Peer a bien été pris en compte (sauvegarder les informations)

```
root@VPN-MAISON:~# wg show
interface: wg0
  public key:
  private key:
  listening port: 51820
  fwmark: 0xca6c

peer:
  endpoint:              :56454
  allowed ips: 192.168.11.2/32
root@VPN-MAISON:~#
```

Nous sécurisons les 2 dossier nécessaire au bon fonctionnement du VPN grâce à ces commandes

```
root@VPN-MAISON:~# chmod 600 /etc/wireguard/ -R
root@VPN-MAISON:~# chmod 600 /etc/ufw/ -R
root@VPN-MAISON:~#
```

Puis sur notre BOX nous effectuons une redirection du port 51820 arrivant de l'extérieur vers le port 51820 interne de mon interface physique ou se trouve mon VPN

Redirection de ports

Un usage excessif des plages de ports peut réduire les performances de cet équipement. La plage maximale autorisée est de 100 ports

Service	Adresse IP du serveur	Protocole	Ports externes	Ports internes	Activer la règle
Utilisateur					
WG	192.168.1.254	UDP	51820 • 51820	51820 • 51820	on

Pour finir, on se connecte depuis un autre réseau et connecte à notre VPN. On essaie de ping l'interface physique se trouvant dans le réseau local.

```
Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::34b5:5c6a:1f3d:9119%3
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.43.50
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.43.1

Carte Ethernet Connexion réseau Bluetooth :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

C:\Users\theo7>ping 192.168.1.254

Envoi d'une requête 'Ping'  192.168.1.254 avec 32 octets de données :
Réponse de 192.168.1.254 : octets=32 temps=70 ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps=230 ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps=94 ms TTL=64
Réponse de 192.168.1.254 : octets=32 temps=245 ms TTL=64

Statistiques Ping pour 192.168.1.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 70ms, Maximum = 245ms, Moyenne = 159ms
```

Vous êtes maintenant connecter au VPN !