



## Sécuriser les accès distants via un VPN



**WIREGUARD**  
FAST, MODERN, SECURE VPN TUNNEL

## Apt-get update

```
root@debian:/home/administrateur# apt-get update
Atteint :1 http://deb.debian.org/debian bullseye InRelease
Réception de :2 http://security.debian.org/debian-security bullseye-security InRelease [48,4 kB]
Atteint :3 http://deb.debian.org/debian bullseye-updates InRelease
48,4 ko réceptionnés en 1s (79,5 ko/s)
Lecture des listes de paquets... Fait
root@debian:/home/administrateur# █
```

## Apt-get install wireguard

```
root@debian:/home/administrateur# 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 12 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 ? [0/n] o
Réception de :1 http://deb.debian.org/debian bullseye/main amd64 wireguard-tools amd64 1.0.20210223-1 [86,2 kB]
Réception de :2 http://deb.debian.org/debian bullseye/main amd64 wireguard all 1
```

À l'aide de la commande "wg" nous devons générer une clé privée et une clé publique : indispensable pour l'authentification entre deux paires, c'est-à-dire le serveur et un client (qui devra aussi disposer d'un couple de clés).

Nous allons créer la clé privée "/etc/wireguard/wg-private.key" et la clé publique "/etc/wireguard/wg-public.key" grâce à cet enchaînement de commandes :

```
root@debian:/home/administrateur# wg genkey | sudo tee /etc/wireguard/wg-private.key | wg pubkey | sudo tee /etc/wireguard/wg-public.key
acsEs+Pm1BNdTeMTecIdjDB9kJdEIYfLIp5Sdyf6E0w=
```

Sudo cat /etc/wireguard/wg-private.key

```
root@debian:/home/administrateur# sudo cat /etc/wireguard/wg-private.key
aAxcZeay8VLKw+d0k8ZeT0dr2Yc2TVZuUToiJ5mU92c=
root@debian:/home/administrateur# █
```

Il est temps de créer un fichier de configuration dans "/etc/wireguard/". Par exemple, nous pouvons nommer ce fichier "wg0.conf", si l'on estime que l'interface réseau associée à WireGuard sera "wg0", sur le même principe que l'on trouve "eth0", par exemple.



sudo nano /etc/wireguard/wg0.conf

```
administrateur@debian: ~
GNU nano 5.4 /etc/wireguard/wg0.conf
[Interface]
Address = 192.168.110.121/24
SaveConfig = true
ListenPort = 51820
PrivateKey = aAxcZey8VLKw+d0k8ZeT0dr2Yc2TVZuUToiJ5mU92c=
```

Montage de l'interface wg0

sudo wg-quick up wg0

```
root@debian:/home/administrateur# sudo wg-quick up wg0
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 192.168.110.121/24 dev wg0
[#] ip link set mtu 1420 up dev wg0
root@debian:/home/administrateur#
```

Ip a pour verifier que l'interface a bien été montée.

```
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 00:0c:29:09:f3:c3 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.94.151/24 brd 192.168.94.255 scope global dynamic ens33
        valid_lft 1628sec preferred_lft 1628sec
    inet6 fe80::20c:29ff:fe09:f3c3/64 scope link
        valid_lft forever preferred_lft forever
3: ens36: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 00:0c:29:09:f3:cd brd ff:ff:ff:ff:ff:ff
    altname enp2s4
    inet 192.168.1.254/24 brd 192.168.1.255 scope global ens36
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe09:f3cd/64 scope link
        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 192.168.110.121/24 scope global wg0
        valid_lft forever preferred_lft forever
root@debian:/home/administrateur#
```



Afficher l'état de l'interface :

Sudo wg show wg0

```
root@debian:~/home/administrateur# sudo wg show wg0
interface: wg0
  public key: 05UaWNPIq1m6K0pHqFrngYshEKI5/CDYsHh8gYG0QQ=
  private key: (hidden)
  listening port: 51820
root@debian:~/home/administrateur#
```

Démarrage automatique du service :

sudo systemctl enable [wg-quick@wg0.service](#)

```
root@debian:~/home/administrateur# sudo systemctl enable wg-quick@wg0.service
Created symlink /etc/systemd/system/multi-user.target.wants/wg-quick@wg0.service → /lib/systemd/system/wg-quick@.service.
root@debian:~/home/administrateur#
```

Activation de l'IP FORWARDING :

sudo nano /etc/sysctl.conf

Puis on décomment cette ligne

```
administrateur@debian: ~
GNU nano 5.4 /etc/sysctl.conf *

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
# based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1

#####
# Additional settings - these settings can improve the network
# security of the host and prevent against some network attacks
# including spoofing attacks and man in the middle attacks through
# redirection. Some network environments, however, require that these
# settings are disabled so review and enable them as needed.
#
# Do not accept ICMP redirects (prevent MITM attacks)
#net.ipv4.conf.all.accept_redirects = 0
#net.ipv6.conf.all.accept_redirects = 0

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



Activation de l'IP masquerade :

Pour que notre serveur puisse router correctement les paquets et que le LAN distant soit accessible à la machine Windows, il faut activer l'IP Masquerade sur notre serveur Debian. C'est en quelque sorte l'activation du NAT. Je vais effectuer cette configuration sur le pare-feu Linux au travers d'UFW que j'ai l'habitude d'utiliser (tutoriel ufw sur Debian).

Si vous n'avez pas encore UFW et que vous souhaitez le mettre en place (vous pouvez aussi passer par Nftables), commencer par l'installer :

```
root@debian:/home/administrateur# sudo apt install ufw
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
ufw est déjà la version la plus récente (0.36-7.1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 12 non mis à jour.
root@debian:/home/administrateur#
```

Ensuite il faut autoriser le SSH pour ne pas perdre la main sur le serveur distant :

```
sudo ufw allow 22/tcp
```

```
root@debian:/home/administrateur# sudo ufw allow 22/tcp
Rules updated
Rules updated (v6)
root@debian:/home/administrateur#
```

On doit aussi autoriser le port 51820 en UDP car c'est le port qu'on utilise pour WireGuard :

```
sudo ufw allow 51820/udp
```

```
root@debian:/home/administrateur# sudo ufw allow 51820/udp
Rules updated
Rules updated (v6)
```



sudo nano /etc/ufw/before.rules

```
#
# rules.before
#
# Rules that should be run before the ufw command line added rules. Custom
# rules should be added to one of these chains:
#   ufw-before-input
#   ufw-before-output
#   ufw-before-forward
#
# Don't delete these required lines, otherwise there will be errors
*filter
:ufw-before-input - [0:0]
:ufw-before-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-not-local - [0:0]
# End required lines

# allow all on loopback
```

[ Lecture de 75 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

# NAT - IP masquerade

\*nat

:POSTROUTING ACCEPT [0:0]

-A POSTROUTING -o ens192 -j MASQUERADE

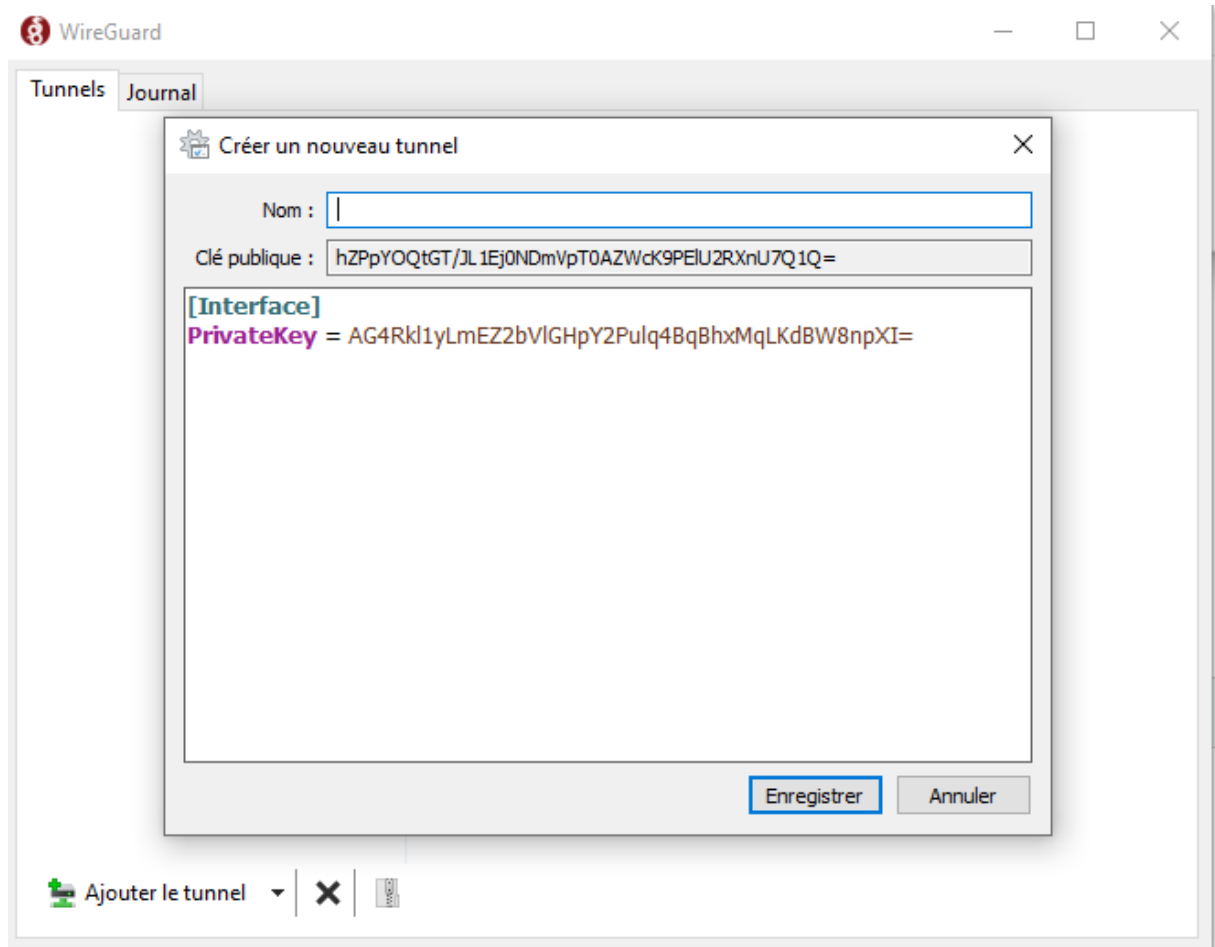
# End each table with the 'COMMIT' line or these rules won't be processed

COMMIT



Installer WIREGUARD sur poste utilisateur windows

Ajouter un tunnel vide



test