**Sécuriser les accès distants via un VPN**

**Une image contenant texte, Police, Graphique, logo

Description générée automatiquement**

Apt-get update

Une image contenant texte, Police, capture d’écran, blanc

Description générée automatiquement

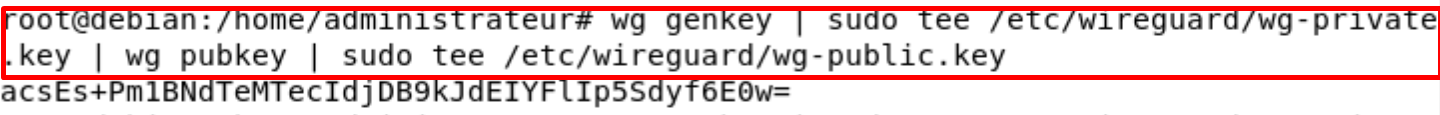
Apt-get install wireguard

Une image contenant texte, capture d’écran, Police, nombre

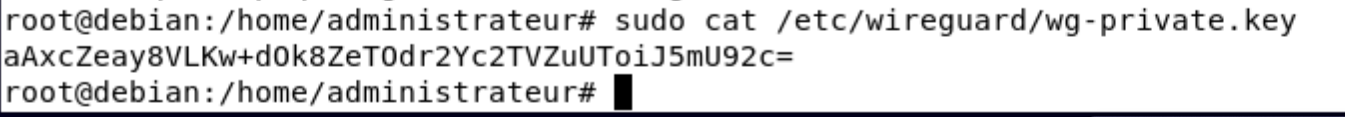
Description générée automatiquement

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 :



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



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

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Montage de l’interface wg0

sudo wg-quick up wg0

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

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

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

Afficher l’état de l’interface :

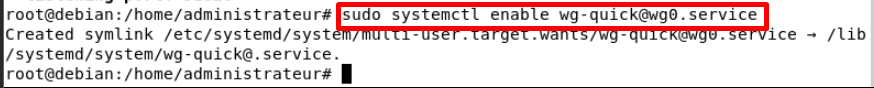
Sudo wg show wg0

Une image contenant texte, Police, capture d’écran

Description générée automatiquement

Démarrage automatique du service :

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



Activation de l’IP FORWARDING :

sudo nano /etc/sysctl.conf

Puis on décomment cette ligne

Une image contenant texte, Appareils électroniques, capture d’écran, ordinateur

Description générée automatiquement

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).

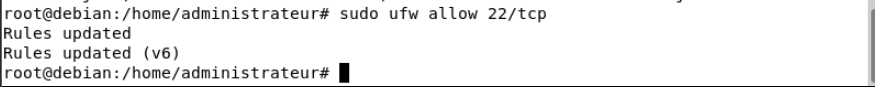
Si vous n'avez pas encore UFW et que vous souhaitez le mettre en place (vous pouvez aussi passer par Nftables), commencer par l'installer :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

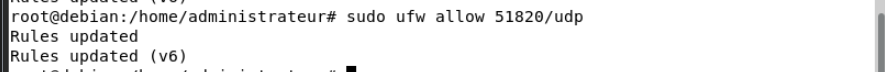
Ensuite il faut autoriser le SSH pour ne pas perdre la main sur le serveur distant :

sudo ufw allow 22/tcp



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

sudo ufw allow 51820/udp



sudo nano /etc/ufw/before.rules

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

# 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

Une image contenant texte, capture d’écran, affichage, logiciel

Description générée automatiquement

test