Configuration vpn ssl/tls

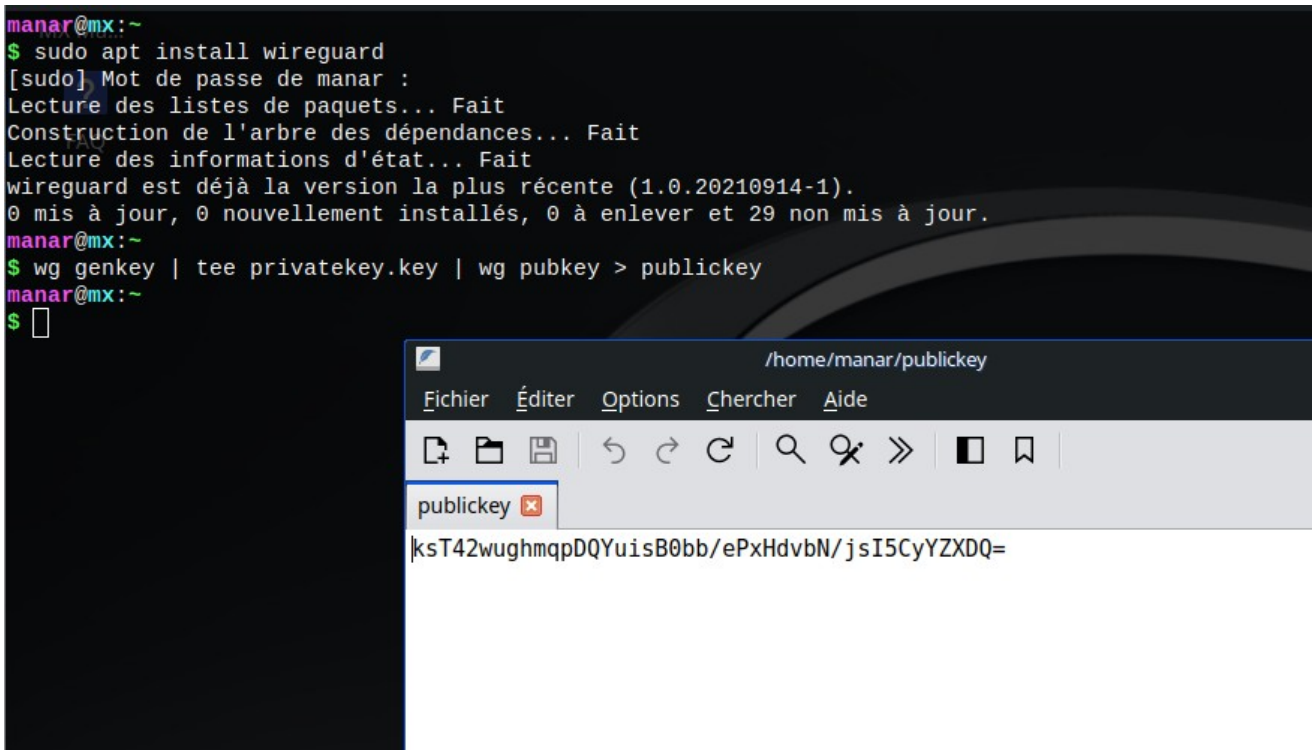
1) sudo apt update : Updates the local package list to ensure you have the latest versions of available software.
2) sudo apt install wireguard : Installs the WireGuard VPN software on your system.
3) wg –version : Displays the installed version of WireGuard.
4) wg genkey | tee privatekey.key | wg pubkey > publickey :

generates a private key for the WireGuard VPN interface

saves the private key to file named `privatekey`

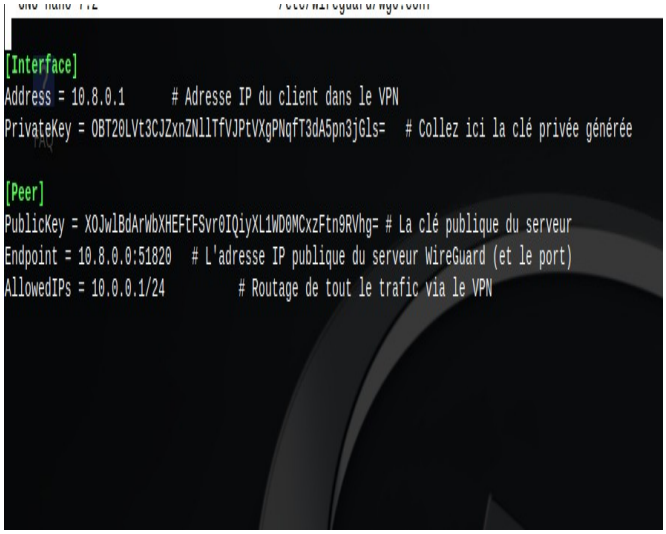
generates the corresponding public key from the private key.

writes the public key to the `publickey` file.

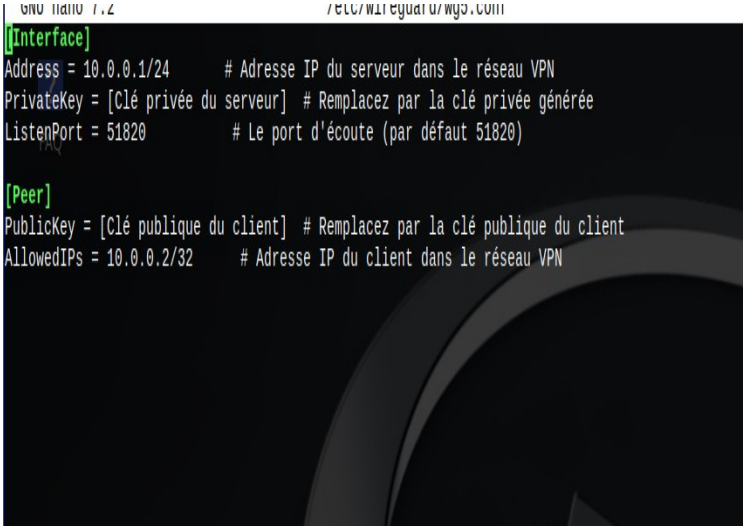


5) sudo nano /etc/wireguard/wg0.conf : Opens the WireGuard configuration file for editing using the nano text editor.

Client



serveur



------client------
[Interface]
Address = 10.0.0.1/24 # Adresse IP du client dans le réseau VPN
PrivateKey = [Clé privée du client] # Remplacez par la clé privée générée
[Peer]
PublicKey = [Clé publique du server] # Remplacez par la clé publique duclient
Endpoint=<ip_du_serveur>:51820
AllowedIPs = 0.0.0.0/0 # Adresse IP du client dans le réseau VPN

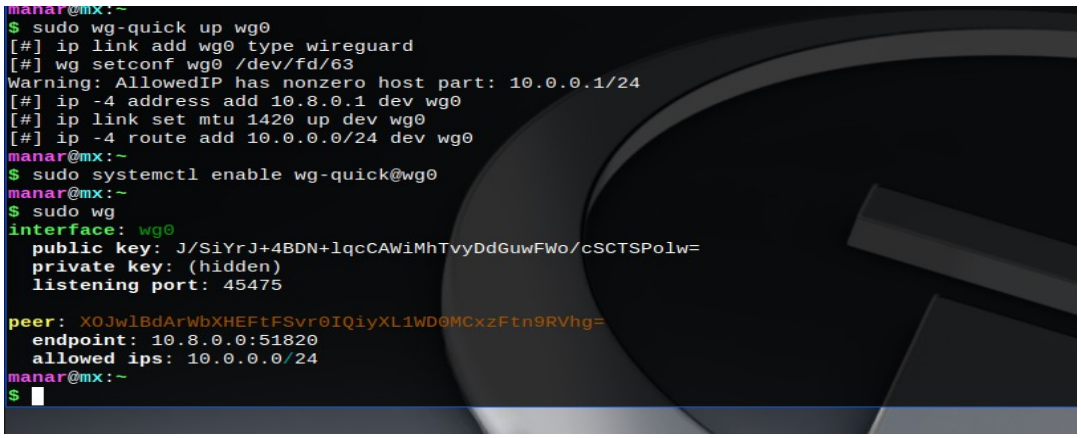
-----server----
[Interface]
Address = 10.0.0.1/24 # Adresse IP du serveur dans le réseau VPN
PrivateKey = [Clé privée du serveur] # Remplacez par la clé privée générée
ListenPort = 51820 # Le port d'écoute (par défaut 51820)

[Peer]
PublicKey = [Clé publique du client] # Remplacez par la clé publique du client
AllowedIPs = 10.0.0.2/32 # Adresse IP du client dans le réseau VPN

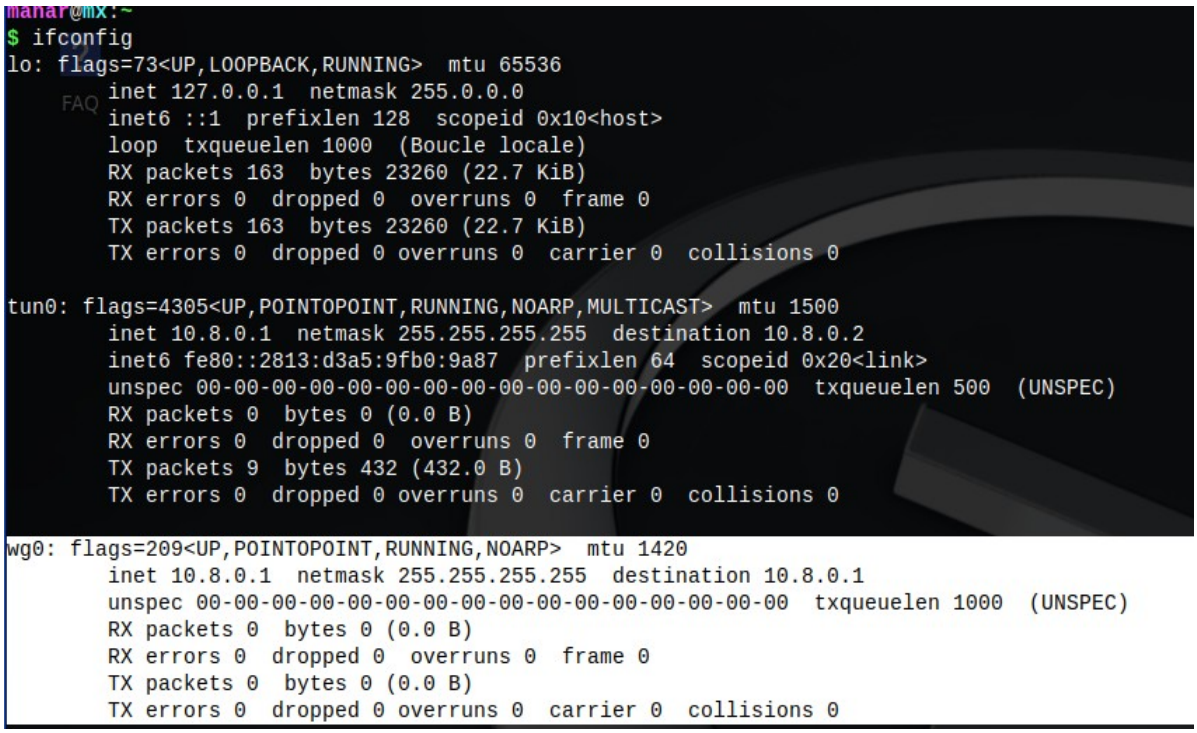
6) sudo wg-quick up wg0 : Brings up the WireGuard interface `wg0` and starts the VPN connection.

7) sudo systemctl enable wg-quick@wg0 : Enables the WireGuard VPN interface to automatically start at boot.

8) sudo wg : Displays the current status of the WireGuard VPN, including the active peers.



Verification :



SSL Encryption (OpenSSL)

1) sudo apt install openssl : Installs OpenSSL, a toolkit for Secure Sockets Layer (SSL) and public key cryptography

2) openssl genpkey -algorithm RSA -out private_key.pem -aes256 : Generates an RSA private key and encrypts it with AES-256

3) openssl rsa -pubout -in private_key.pem -out public_key.pem : Generates the corresponding public key from the private key.

*** Now ,the server send his public key to client , by :

4) scp /etc/wireguard/publickey.key user@client_ip:/path/to/destination

Client :

1) echo "ceci est un message sécurisé" > message.txt :Creates a file named `message.txt` and writes the encrypted message into it.

2) openssl pkeyutl -encrypt -inkey server_public.key -pubin -in message.txt -out message_encrypted.bin : Encrypts the contents of `message.txt` using the server's public key

3) scp %path/message_encrypted.bin user@server_ip:chemin : Uses SCP (Secure Copy Protocol) to transfer the encrypted file to the server

Server :

1) openssl rsaultl -decrypt -inkey server-private.key -in /tmp/message-encrypted.bin -out message_decrypted.txt : Decrypts the encrypted message file using the server's private key

2) cat message_decrypted.txt : Displays the contents of the decrypted message on the server.