WireGuard Client Installation

ÉTAPE 1 : INSTALLER WIREGUARD

1. Mettez à jour votre système :

   `sudo apt update && sudo apt upgrade -y`
2. Installez WireGuard :

   `sudo apt install wireguard`

> **Si vous n'avez pas le paquet resolvconf d'installer installez le également avec : " apt install resolvconf -y "**

ÉTAPE 2 : GÉNÉRER LES CLÉS POUR LE CLIENT

WireGuard utilise une paire de clés publique/privée pour l'authentification.

1. Accédez au répertoire de configuration de WireGuard :

   `cd /etc/wireguard`
2. Générez les clés :

   ```
   umask 077
   wg genkey | tee private.key | wg pubkey > public.key
   ```
3. Vérifiez les clés générées :
   - Clé privée :

     `cat private.key`
   - Clé publique :

`cat public.key`

4. Conservez la clé publique, car elle devra être partagée avec le serveur WireGuard.

ÉTAPE 3 : CRÉER LE FICHIER DE CONFIGURATION DU CLIENT

1. Créez un fichier de configuration pour l'interface WireGuard (par exemple `wg0.conf`) :

   `sudo nano /etc/wireguard/wg0.conf`
2. Ajoutez le contenu suivant au fichier (adaptez selon vos besoins) :

   ```
   [Interface]
   PrivateKey = <clé_privée_du_client> # Remplacez par la clé privée générée (fichier private.key)
   Address = 192.168.110.2/24          # Adresse IP privée du client dans le tunnel VPN
   DNS = 192.168.110.1                 # (Optionnel) Serveur DNS à utiliser via le VPN

   [Peer]
   PublicKey = <clé_publique_du_serveur> # Clé publique fournie par le serveur WireGuard
   Endpoint = <ip_publique_du_serveur>:51820 # Adresse IP ou nom de domaine et port du serveur WireGuard
   AllowedIPs = 0.0.0.0/0, ::/0          # Acheminer tout le trafic via le VPN
   ```
3. Remplacez `<clé_privée_du_client>` et `<clé_publique_du_serveur>` par les valeurs appropriées.
4. Sauvegardez et fermez le fichier (`Ctrl+O`, puis `Ctrl+X`).

ÉTAPE 4 : ACTIVER ET TESTER LA CONNEXION

1. Activez l'interface WireGuard :

   `sudo wg-quick up wg0`
2. Vérifiez que l'interface est active :

   `ip a show wg0`
3. Testez la connectivité en pingant une adresse IP via le VPN (par exemple, l'adresse IP privée du serveur ou une ressource accessible uniquement via le VPN) :

   `ping 192.168.110.1`

1. Pour désactiver la connexion VPN :

   `sudo wg-quick down wg0`

ÉTAPE 5 : ACTIVER LE DÉMARRAGE AUTOMATIQUE (OPTIONNEL)

Si vous souhaitez que l'interface VPN démarre automatiquement au démarrage du système :

1. Activez le service WireGuard associé à `wg0` :

   `sudo systemctl enable wg-quick@wg0.service`
2. Désactivez-le si nécessaire :

   `sudo systemctl disable wg-quick@wg0.service`

NOTES IMPORTANTES

- **Clé publique du client** : Vous devrez fournir cette clé au serveur WireGuard pour qu'il puisse autoriser votre connexion.
  - Pour afficher la clé publique du client, utilisez :

    `cat /etc/wireguard/public.key`
- **Sécurité des clés** : Assurez-vous que les fichiers contenant vos clés privées sont protégés avec des permissions strictes.

  `chmod 600 /etc/wireguard/private.key /etc/wireguard/wg0.conf`

Dans le fichier /etc/wireguard/wg0.conf, vous pouvez rajouter ceci à la fin si vous voulez maintenir une connexion permanente au vpn PersistentKeepalive = 25

Cela envoie un paquet keepalive toutes les 25 secondes pour maintenir la connexion active.
Avec ces étapes, votre machine Linux sera configurée comme un client VPN WireGuard et pourra se connecter à un serveur WireGuard distant pour sécuriser ses communications réseau !

Revision #6
Created 15 January 2025 14:38:30 by Bibi
Updated 11 September 2025 11:57:25 by Bibi