Documentation Technique Complète – Projet VPN avec Tailscale

**1. Présentation du projet**

Ce projet consiste à **mettre en place un VPN sécurisé** permettant à plusieurs machines de se connecter via Internet à un réseau privé virtuel.  
L’objectif est de permettre à un utilisateur distant d’accéder à des ressources internes comme s’il était connecté localement.

**2. Choix de la technologie**

**Pourquoi Ngrok a été abandonné**

Nous avons initialement testé **Ngrok** pour exposer notre machine Ubuntu, mais cela a échoué pour plusieurs raisons :

* Impossibilité de créer un vrai réseau VPN entre plusieurs machines
* Limitation des ports
* Connexions instables
* Pas de communication bidirectionnelle simple

**Pourquoi Tailscale a été choisi**

Nous avons opté pour **Tailscale**, un outil basé sur **WireGuard**, car :

* Il crée un vrai **réseau VPN maillé** entre les machines
* Il utilise un **chiffrement fort** via WireGuard
* Il ne nécessite **aucune configuration réseau** (pas d’ouverture de port, ni de NAT)
* Il est **facile à utiliser**, même pour un débutant
* Il propose une **interface de gestion en ligne**

3. Matériel utilisé

| **Rôle** | **Machine** | **Système d'exploitation** | **IP Tailscale** |
| --- | --- | --- | --- |
| Serveur | mahdi-virtual-machine | Ubuntu 22.04 | 100.73.93.51 |
| Client | MSI | Windows 10 | 100.81.158.41 |

Client iphone ios 100.115.128.100

**4. Étapes détaillées d’installation et de configuration**

**Sur la machine Ubuntu (serveur VPN)**

**Installation de Tailscale :**

**sudo apt update**

**sudo apt install tailscale -y**

**Connexion au réseau VPN :**

**sudo tailscale up**

**Cela ouvre un lien dans le navigateur. Se connecter avec un compte Google ou GitHub.**

**Vérifier l’état de la connexion :**

**tailscale status**

**Tu dois voir une adresse IP 100.x.x.x attribuée et la liste des machines connectées.**

**Sur le PC Windows (client VPN)**

**Étapes :**

1. **Télécharger Tailscale depuis : https://tailscale.com/download**
2. **Installer le logiciel**
3. **Lancer l'application**
4. **Se connecter avec le même compte que celui utilisé sur Ubuntu**
5. **Vérifier que la machine est connectée dans l’interface : tailscale status**

**5. Commandes utiles**

| **Action** | **Commande (Ubuntu)** |
| --- | --- |
| **Lancer Tailscale** | **sudo tailscale up** |
| **Vérifier l’état** | **tailscale status** |
| **Arrêter Tailscale** | **sudo tailscale down** |
| **Redémarrer le service** | **sudo tailscaled restart** |
| **Ping une autre machine VPN** | **tailscale ping [IP\_Tailscale]** |
| **Afficher IP de la machine** | **tailscale ip** |

**6. Test de bon fonctionnement**

**Depuis Ubuntu :**

**tailscale ping 100.81.158.41**

**Réponse attendue :**

**pong from msi (100.81.158.41) via 192.168.1.X in XXms**

**Depuis Windows (cmd) :**

**ping 100.73.93.51**

**Réponse attendue :**

**Reply from 100.73.93.51: bytes=32 time=XXms TTL=...**

**8. Gestion et sécurité**

* **Le VPN est chiffré avec WireGuard**
* **L’accès est limité aux machines authentifiées via le compte Tailscale**
* **Possibilité d’activer le MFA (authentification à double facteur) depuis l’interface : https://login.tailscale.com**
* **Toutes les connexions et machines sont visibles et gérables depuis cette interface**

**9. Conclusion**

**Le projet est fonctionnel et respecte les critères attendus :**

**Réseau privé chiffré  
 Accès distant sécurisé  
 Documentation claire  
 Tests de ping et service validés**