

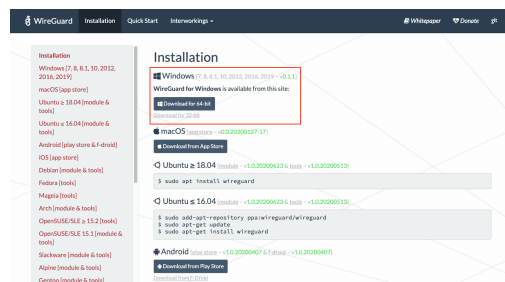
Le VPN avec Wireguard en Linux et Windows



WireGuard est une technologie de VPN (Virtual Private Network) qui est à la fois rapide, sécurisée, et simple à configurer par rapport à des solutions plus anciennes comme OpenVPN ou IPsec. Voici un guide pour configurer un VPN avec WireGuard sur Linux et Windows.

Installation et Configuration de WireGuard

1. Installation de WireGuard



Sur Linux:

La plupart des distributions Linux incluent WireGuard dans leurs dépôts officiels.

- **Ubuntu/Debian:**

```
sudo apt update
sudo apt install wireguard
```

- **CentOS/RHEL (via EPEL):**

```
sudo yum install epel-release
sudo yum install wireguard-tools
```

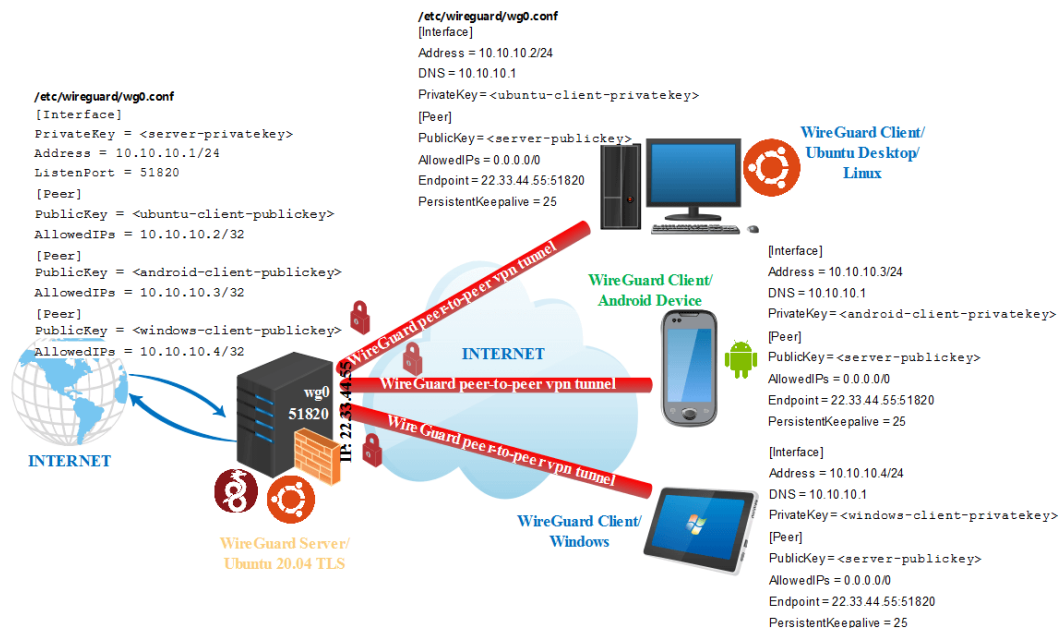
- Arch Linux:

```
sudo pacman -S wireguard-tools
```

Sur Windows:

- Téléchargez l'installateur officiel de WireGuard depuis le site web [wireguard.com](https://www.wireguard.com).
- Installez WireGuard en suivant les instructions à l'écran.

2. Configuration de WireGuard



Génération des clés

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

Sur **Linux** et **Windows**, vous pouvez générer ces clés en utilisant **wg** (le même processus pour les deux OS):

```
wg genkey | tee privatekey | wg pubkey > publickey
```

- **privatekey** contient votre clé privée.

- **publickey** contient votre clé publique.

Configuration du serveur (Linux)

1. Créer le fichier de configuration du serveur:

Par exemple, `/etc/wireguard/wg0.conf`:

```
[Interface]
Address = 10.0.0.1/24
ListenPort = 51820
PrivateKey = <clé_privée_du_serveur>

[Peer]
PublicKey = <clé_publique_du_client>
AllowedIPs = 10.0.0.2/32
```

2. Activer et démarrer l'interface WireGuard:

```
sudo wg-quick up wg0
```

3. Vérifier l'état de l'interface:

```
sudo wg
```

4. Configurer le pare-feu (optionnel):

Vous devez autoriser le port 51820 (ou celui que vous avez configuré) dans le pare-feu:

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

Configuration du client (Linux ou Windows)

1. Créer le fichier de configuration du client:

Par exemple, `wg-client.conf`:

```
[Interface]
Address = 10.0.0.2/24
PrivateKey = <clé_privée_du_client>
DNS = 8.8.8.8

[Peer]
```

```
PublicKey = <clé_publicque_du_serveur>
Endpoint = <adresse_ip_du_serveur>:51820
AllowedIPs = 0.0.0.0/0
PersistentKeepalive = 25
```

2. Sur Linux:

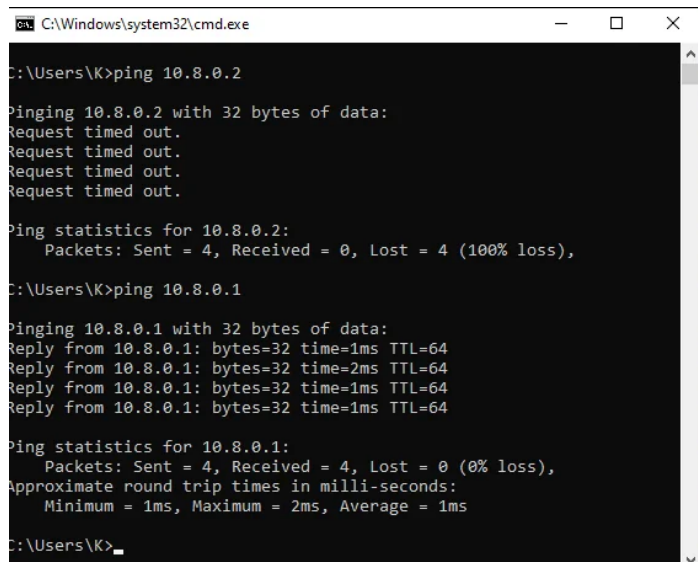
Démarrez l'interface avec:

```
sudo wg-quick up wg-client
```

3. Sur Windows:

- Importez la configuration dans l'application WireGuard.
- Activez l'interface via l'application en cliquant sur "Activate".

Vérification de la connexion



```
C:\Windows\system32\cmd.exe

C:\Users\K>ping 10.8.0.2

Pinging 10.8.0.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.8.0.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\K>ping 10.8.0.1

Pinging 10.8.0.1 with 32 bytes of data:
Reply from 10.8.0.1: bytes=32 time=1ms TTL=64
Reply from 10.8.0.1: bytes=32 time=2ms TTL=64
Reply from 10.8.0.1: bytes=32 time=1ms TTL=64
Reply from 10.8.0.1: bytes=32 time=1ms TTL=64

Ping statistics for 10.8.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\K>
```

- **Sur Linux:** Utilisez la commande `ping` pour vérifier la connectivité, par exemple:

```
ping 10.0.0.1
```

- **Sur Windows:** Ouvrez une invite de commande et utilisez également `ping`:

```
ping 10.0.0.1
```

Si tout fonctionne, votre client devrait pouvoir communiquer avec le serveur et naviguer sur Internet via le VPN.

Résumé

- Installez WireGuard sur les deux machines.
- Configurez le serveur avec une interface WireGuard.
- Configurez le client pour se connecter à cette interface.
- Vérifiez la connexion avec `ping` ou d'autres tests réseau.

Conclusion

Avec ces étapes, vous devriez être capable de configurer un VPN WireGuard fonctionnel entre un client Linux et un serveur (ou vice-versa).