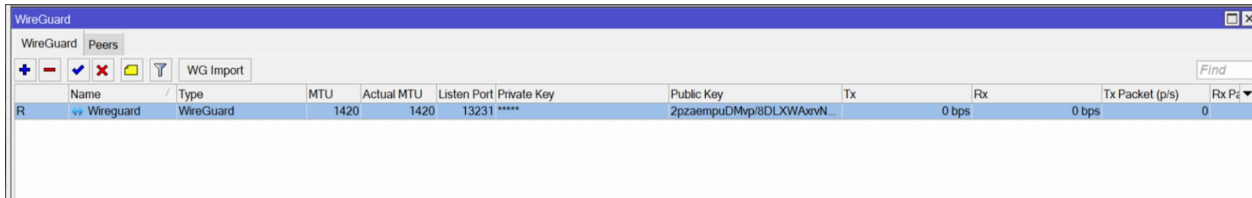


Configuration Wireguard

- [Wireguard](#)
- [Configurer Wireguard Server + Peer](#)
- [WireGuard Site-à-Site \(MikroTik à MikroTik\)](#)

Wireguard

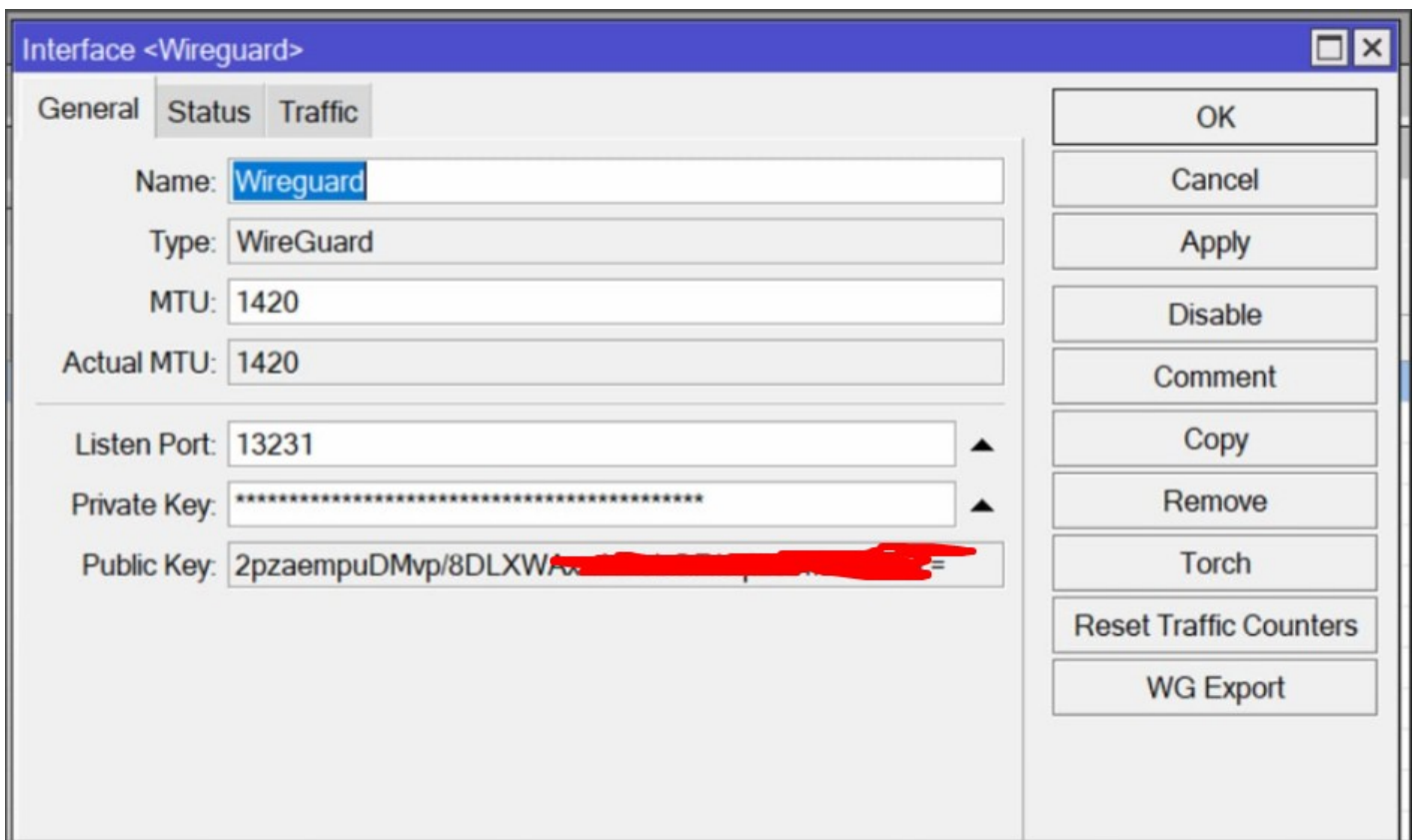
Client Wireguard : <https://www.wireguard.com/install/>



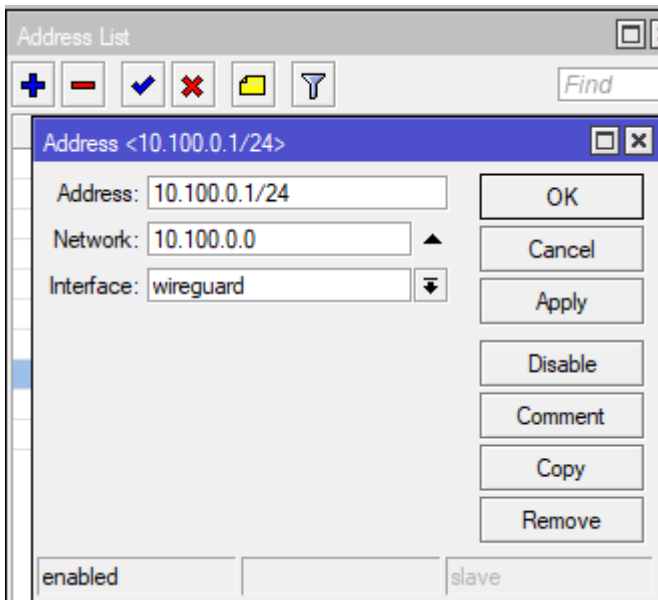
Donner le nom Wireguard

Entrer le port 13231

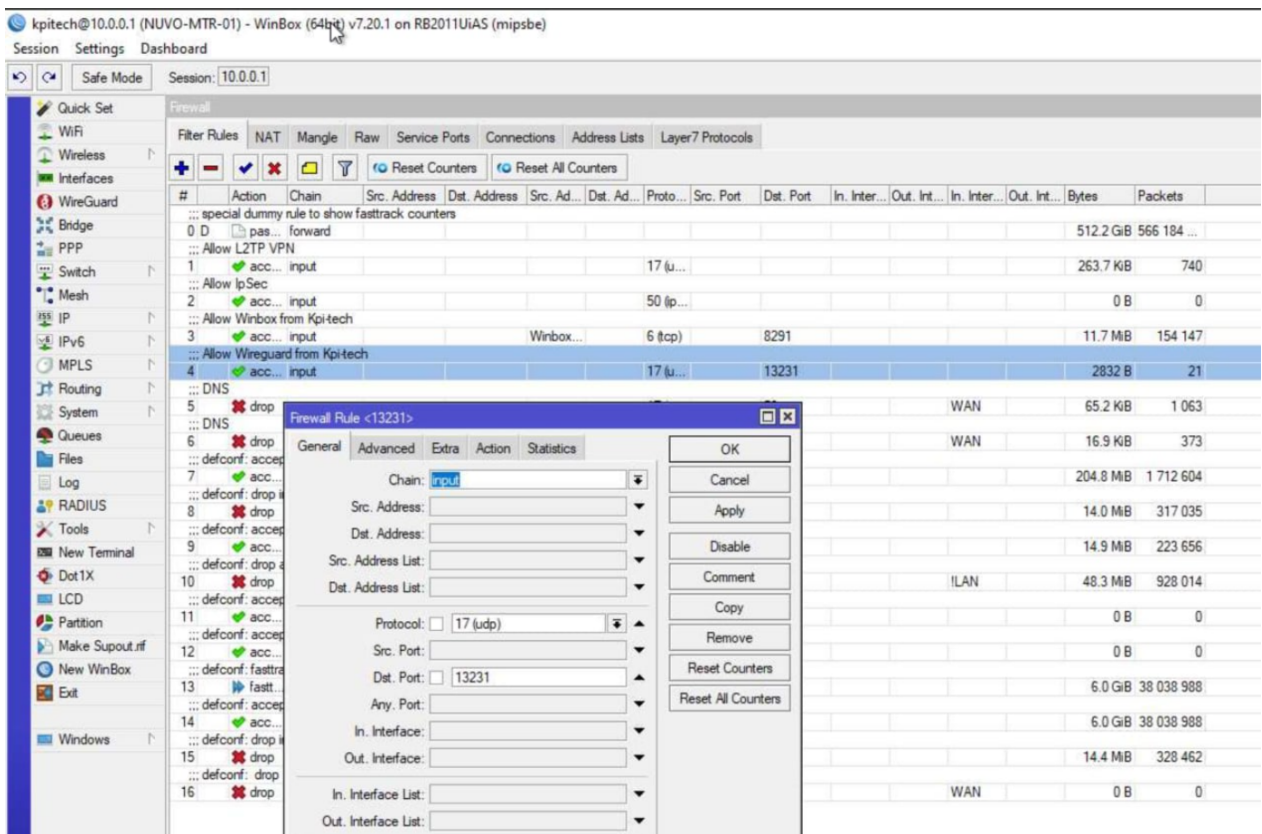
Faire OK



IP / Addresses / +

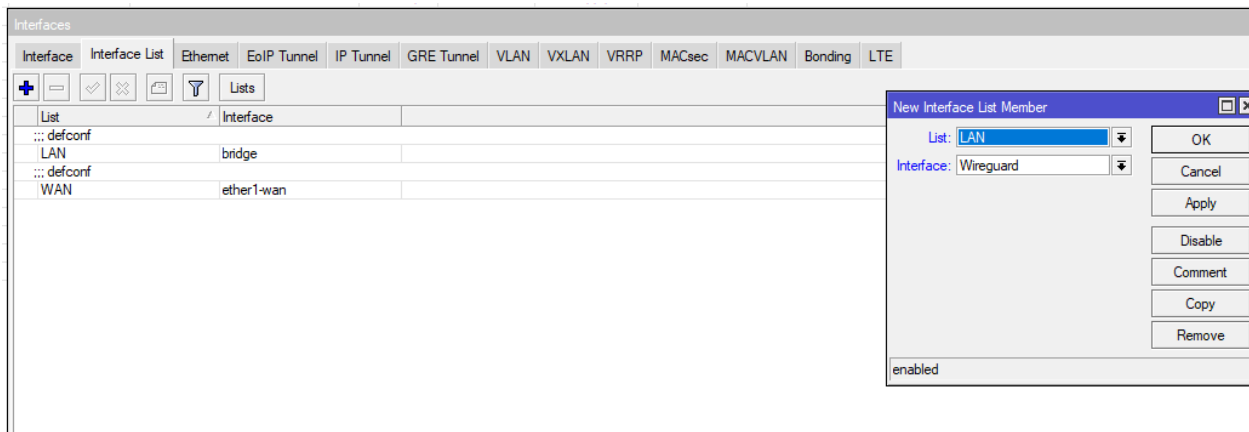


Menu IP/firewall/filter rules/+

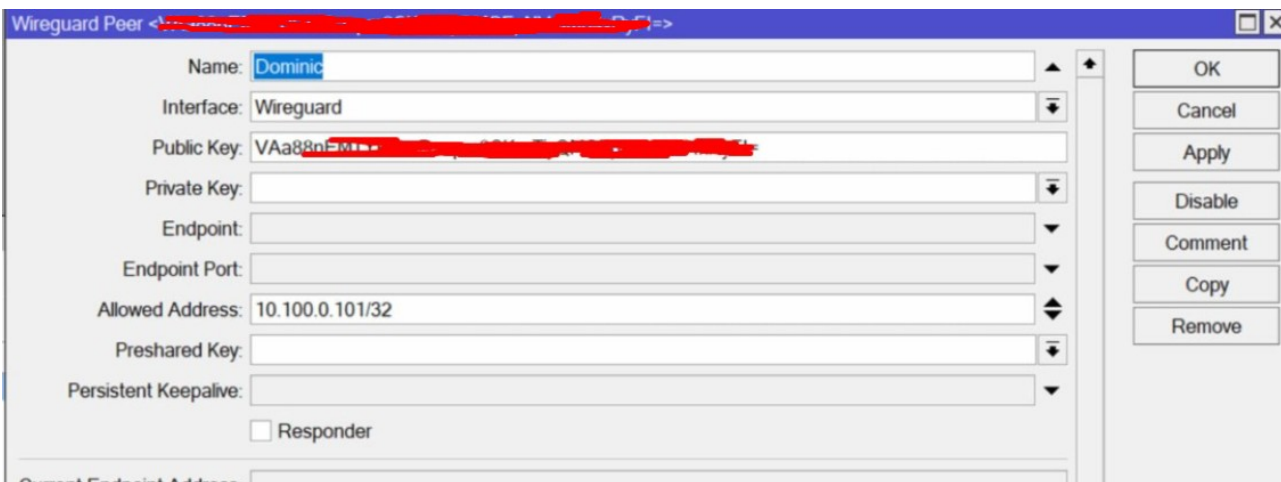


Monter la règle dans la liste en #2 ou #3

Ajouter le wireguard dans l'address list pour l'accès à Winbox over VPN



Menu Wireguard/peer/+



Dans la configuration du client Wireguard Windows, ajouter un tunnel vide

[Interface]

Address = 10.100.0.101/32 (l'adresse du peer de la personne qui se connecte)

DNS = 10.0.0.1 (adresse du routeur Mikrotik local)

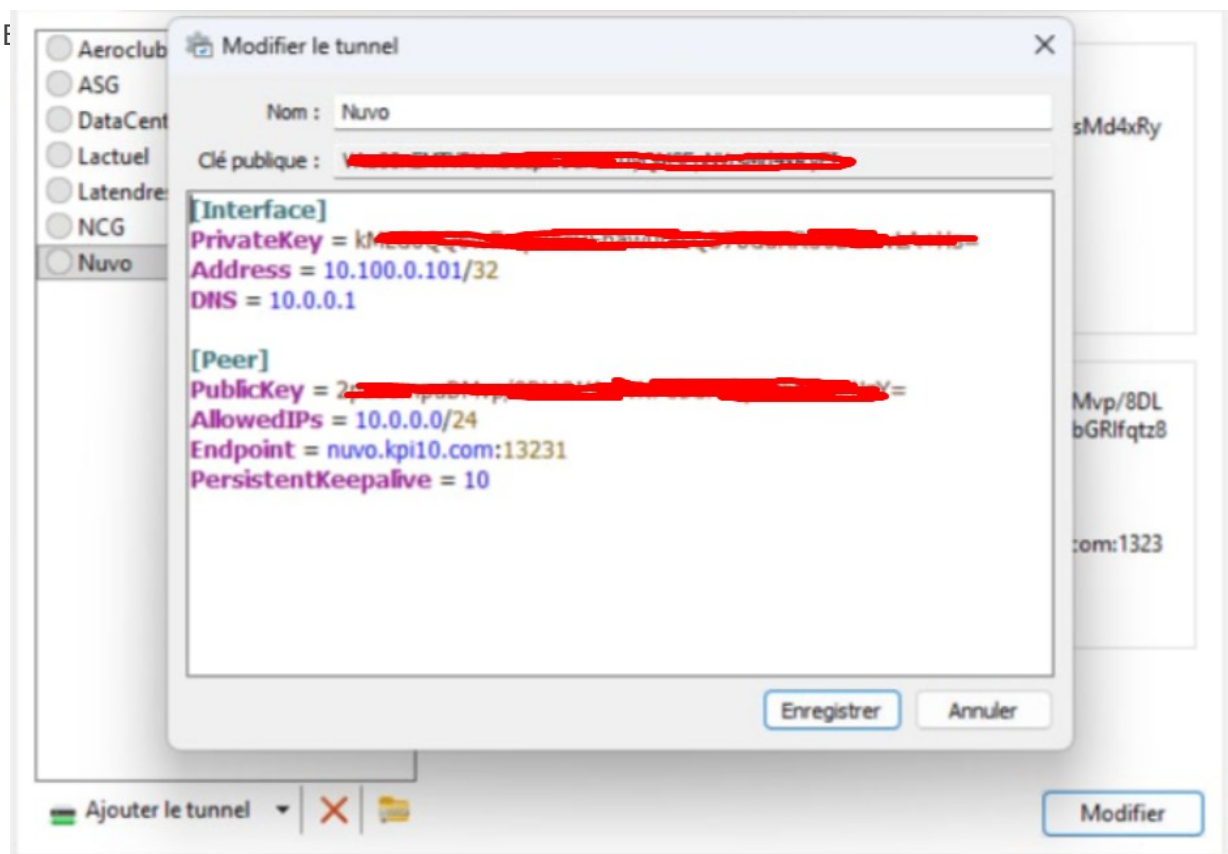
[Peer]

Publickey = Publique Key du routeur :

AllowedIPs = 192.168.1.0/24 (Reseau local du client)

Endpoint = fizzanoelectrique.kpi10.com:13231 (DNS du client)

PersistentKeepalive = 10



Configurer Wireguard Server + Peer

1. Règle du Pare-feu (Firewall)

Il est essentiel d'autoriser le trafic WireGuard avant toute chose. Cette règle permet au routeur de recevoir les connexions entrantes.

- **Chaîne (Chain) :** input

The screenshot shows the 'Firewall Rule <13231>' configuration window with the 'General' tab selected. The 'Chain' is set to 'input'. The 'Protocol' is set to '17 (udp)'. The 'Src. Port' is empty, and the 'Dst. Port' is set to '13231'. The 'Any. Port' is empty. The 'In. Interface' and 'Out. Interface' are empty. The 'In. Interface List' and 'Out. Interface List' are empty. The 'Packet Mark', 'Connection Mark', and 'Routing Mark' are empty. The 'Connection Type', 'Connection State', and 'Connection NAT State' are empty. The 'enabled' checkbox is checked.

The screenshot shows the 'Firewall Rule <13231>' configuration window with the 'Action' tab selected. The 'Action' is set to 'accept'. The 'Log' checkbox is unchecked. The 'Log Prefix' is empty. The 'enabled' checkbox is checked.

2. Création du Serveur WireGuard

1. Cliquez sur le menu **WireGuard** dans WinBox.
2. Dans l'onglet **WireGuard**, créez une nouvelle interface (le serveur).

3. Notez la **Public Key** générée automatiquement. Vous en aurez besoin pour configurer chaque client (peer).

Interface <wireguard-home>

General Status Traffic

Name: wireguard-home

Type: WireGuard

MTU: 1420

Actual MTU: 1420

Listen Port: 13231

Private Key: [masked]

Public Key: 6T... [redacted]

OK Cancel Apply Disable Comment Copy Remove Torch Reset Traffic Counters WG Export

enabled running slave passthrough inactive

3. Ajout des Clients (Peers) sur le MikroTik

Dans l'onglet **Peers**, créez une entrée pour chaque appareil distant (ordinateur, téléphone, etc.).

- **Name** : Identifiant clair (ex: Simon-Laptop).
- **Interface** : Sélectionnez le serveur créé précédemment.
- **Public Key** : Collez ici la clé publique générée par l'appareil distant (ex: celle du laptop).
- **Endpoint Port** : 13231 .
- **Allowed Address** : L'adresse IP fixe que le tunnel attribuera à ce client. Utilisez un masque /32 (ex: 10.98.0.51/32).

Wireguard Peer

Name: Gab-Phone

Interface: wireguard-home

Public Key: mgd... [redacted]

Private Key: [masked]

Endpoint: [empty]

Endpoint Port: 13231

Allowed Address: 10.98.0.51/32

Preshared Key: [masked]

Persistent Keepalive: [empty]

☐ Responder

OK Cancel Apply Disable Comment Copy Remove

4. Configuration de l'appareil distant (Client)

Téléchargez l'application WireGuard (Windows, Android ou iOS) et créez une nouvelle configuration vide.

Section [Interface]

- **Name** : Nom du serveur de destination.
- **Public Key** : Une clé sera générée par l'application. **Copiez cette clé et collez-la dans la configuration "Peer" du MikroTik** (étape 3).
- **Addresses** : L'IP attribuée au client (ex: `10.98.0.51/32`).
- **Port d'écoute** : `51750` (par défaut).
- **Serveur DNS** : `8.8.8.8` (ou l'IP locale du routeur si configuré).

Section [Peer]

- **Public Key** : Collez la clé publique du **serveur MikroTik** (étape 2).
 - **Endpoint (Point de terminaison)** : L'adresse IP publique ou le DNS du MikroTik suivi du port (ex: `simon.kpi10.com:13231`).
 - **Allowed IPs** : `0.0.0.0/0, ::/0` (pour faire passer tout le trafic par le VPN) ou spécifiez vos sous-réseaux locaux (ex: `192.168.10.0/24`).
-

Exemple de fichier de configuration (.conf)

Sur un PC, vous pouvez copier, coller et adapter ce modèle :

Créer un nouveau tunnel

Nom : test

Clé publique : [REDACTED]

[Interface]
PrivateKey = [REDACTED]
Address = 10.98.0.51/32
DNS = 8.8.8.8

[Peer]
PublicKey = 6T [REDACTED]
AllowedIPs = 0.0.0.0/0, ::/0
Endpoint = simon.kpi10.com:13231
PersistentKeepalive = 10

☒ Bloquer tous le trafic hors tunnel (interrupteur)

Enregistrer Annuler

Ini, TOML

```
[Interface]
PrivateKey = <Clé_Privée_Générée_Automatiquement>
Address = 10.98.0.51/32
DNS = 8.8.8.8

[Peer]
PublicKey = <Clé_Publique_Du_MikroTik>
AllowedIPs = 10.10.10.0/24, 10.30.0.0/24, 192.168.10.0/24
Endpoint = simon.kpi10.com:13231
PersistentKeepalive = 10
```

WireGuard Site-à-Site (MikroTik à MikroTik)

Cette configuration permet de relier deux bureaux (Router1 et Router2) pour que les réseaux `10.0.0.0/24` et `10.11.0.0/24` communiquent de façon transparente.

**S'assurer que les 2 plages d'adresse des routeur a fusionner soit différent*

**Pour un exemple de configuration connectez vous a `clubb.kpi10.com` (routeur 1) et `clubb-marina.kpi10.com` (routeur 2)*

1. Configuration du Serveur (Routeur 1 principal)

A. Firewall (Autoriser l'entrée)

- **Chain :** `input` | **Protocol :** `17 (udp)` | **Dst. Port :** `13231` | **Action :** `accept`.

B. Interface WireGuard

- Créez une interface nommée `wireguard-SV`.
- **Listen Port :** `13231`.
- **Notez la Public Key** du serveur.

C. Ajout du Peer (Le routeur 2)

- **Interface :** `wireguard-SV`.
- **Public Key :** Collez la clé publique du routeur 2. (étape 2A)
- **Allowed Address :** Ajoutez deux lignes (via la flèche bleue) :
 1. `10.98.0.10/32` (IP du tunnel du client).
 2. `10.11.0.0/24` (Réseau local de la Marina).

D. IP & Routage

- **IP Address :** Ajoutez `10.98.0.1/24` sur l'interface `wireguard-SV`.

- **IP Route** : Ajoutez une route : `Dst. Address: 10.11.0.0/24` | `Gateway: wireguard-SV`.
-

2. Configuration du Client (Routeur 2)

A. Interface WireGuard

- Créez une interface nommée `wireguard-to-Router1`.
- **Listen Port** : `13231`.
- **Notez la Public Key** pour la donner au serveur.

B. Ajout du Peer (Vers le serveur)

- **Interface** : `wireguard-to-Resto`.
- **Public Key** : Collez la clé publique du serveur (router 1).
- **Endpoint** : L'adresse IP publique ou DNS du serveur (ex: `clubb.kpi10.com`).
- **Endpoint Port** : `13231`.
- **Allowed Address** : Ajoutez deux lignes :
 1. `10.98.0.0/24` (Réseau du tunnel).
 2. `10.0.0.0/24` (Réseau local du serveur).
- **Persistent Keepalive** : `00:00:25` (Crucial pour maintenir la connexion).

C. IP & Routage

- **IP Address** : Ajoutez `10.98.0.10/24` sur l'interface `wireguard-to-Router1`.
 - **IP Route** : Ajoutez une route : `Dst. Address: 10.0.0.0/24` | `Gateway: wireguard-to-Router1`.
-

3. Sécurité Forward (Sur les DEUX routeurs)

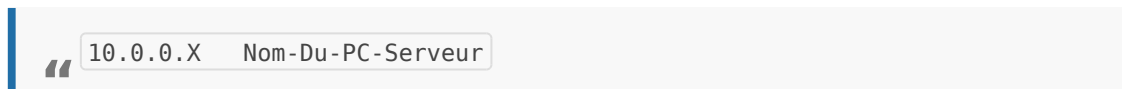
Pour que les ordinateurs puissent se parler à travers le routeur, vous devez ajouter deux règles dans **IP > Firewall > Filter Rules** (à placer en haut de liste) :

1. **Autoriser l'entrée du VPN** : `Chain: forward` | `In. Interface: (votre interface WireGuard)` | `Action: accept`.
2. **Autoriser la sortie vers le VPN** : `Chain: forward` | `Out. Interface: (votre interface WireGuard)` | `Action: accept`.

4. Résolution de noms (Accès par Nom du PC)

Puisque les noms de réseau ne traversent pas naturellement le tunnel, utilisez la méthode du fichier **Hosts** sur les postes de travail Windows qui doivent accéder au logiciel.

1. Sur le PC client, cherchez **Bloc-notes**, faites un clic droit et choisissez **Exécuter en tant qu'administrateur**.
2. Ouvrez le fichier suivant : `C:\Windows\System32\drivers\etc\hosts`.
3. À la toute fin du fichier, ajoutez l'adresse IP du serveur suivie de son nom :



```
10.0.0.X    Nom-Du-PC-Serveur
```

4. Enregistrez et fermez.
5. Vous pouvez maintenant accéder au logiciel via `\\Nom-Du-PC-Serveur` au lieu de l'adresse IP.

Note finale : Assurez-vous que le Pare-feu Windows sur le PC serveur autorise les connexions entrantes venant du sous-réseau distant (`10.11.0.0/24`).