


CONFIGURATION D'UN SERVEUR VPN

PARCOURS	SISR <input checked="" type="checkbox"/>	SLAM <input type="checkbox"/>
-----------------	---	--------------------------------------

Lieu de réalisation	Campus Montsouris	
Période de réalisation	Du : 24.01.2025	Au : 21.02.2025
Modalité de réalisation	SEUL <input checked="" type="checkbox"/>	EN EQUIPE <input type="checkbox"/>

Intitulé de la mission	Configuration d'un serveur VPN
Description du contexte de la mission	Installation, configuration et implémentation d'un serveur VPN ainsi que de clients sur les appareils des télétravailleurs de la société Belletable

Contraintes & Résultat	<div style="background-color: #d3d3d3; padding: 2px; text-align: center; font-size: small;">Ressources fournies / contraintes techniques / Résultats attendu</div> <div style="padding: 5px;">Proxmox, VM, Debian, Wireguard, Routeur</div>
Productions associées	<div style="background-color: #d3d3d3; padding: 2px; text-align: center; font-size: small;">Liste des documents produits et description</div> <div style="height: 40px;"></div>

Modalités d'accès aux productions	<div style="background-color: #d3d3d3; padding: 2px; font-size: small;">Identifiants, mots de passe, URL d'un espace de stockage et présentation de l'organisation du stockage</div> <div style="padding: 5px;"> <ul style="list-style-type: none"> - Adresse du routeur : 10.75.1.254 - Identifiant : admin - Mot de passe : admin123 </div>
--	--

Table des matières

1. Introduction	3
2. Installation	4
2.1. Choix d'une solution	4
2.2. Configuration du serveur VPN Wireguard	5
3. Installation et configuration du client VPN	8
3.1. Installation du client VPN.....	8
4. Ajout des pairs	11
5. Test de la configuration	13

1. Introduction

Dans un contexte où le télétravail devient une nécessité pour de nombreuses entreprises, la sécurisation des connexions distantes est un enjeu majeur. La société *Belletable*, soucieuse de garantir un accès sécurisé à son réseau interne pour ses employés travaillant à distance, a sollicité la société *Infoservices* pour la mise en place d'une solution VPN, *Virtual Private Network*.

Un VPN permet d'établir une connexion chiffrée entre les télétravailleurs et les ressources internes de l'entreprise, offrant ainsi une sécurité accrue contre les cybermenaces et garantissant l'intégrité des échanges de données. Après analyse des besoins de Belletable, le choix s'est porté sur WireGuard, une solution VPN moderne et performante, reconnue pour sa simplicité de configuration, sa rapidité et son niveau de sécurité élevé.

Cette documentation détaille les différentes étapes de la mise en place de cette solution, depuis l'installation du serveur VPN jusqu'à la configuration des clients distants, en passant par les tests de bon fonctionnement et l'intégration des télétravailleurs. L'objectif est d'assurer un accès fiable, sécurisé et optimisé aux ressources de l'entreprise, tout en garantissant une gestion efficace et évolutive de l'infrastructure VPN.

2. Installation

1.1. Choix d'une solution

Afin de garantir un accès à distance au réseau domestique d'entreprise, la société Belletable a demandé la mise en place d'une solution de VPN.

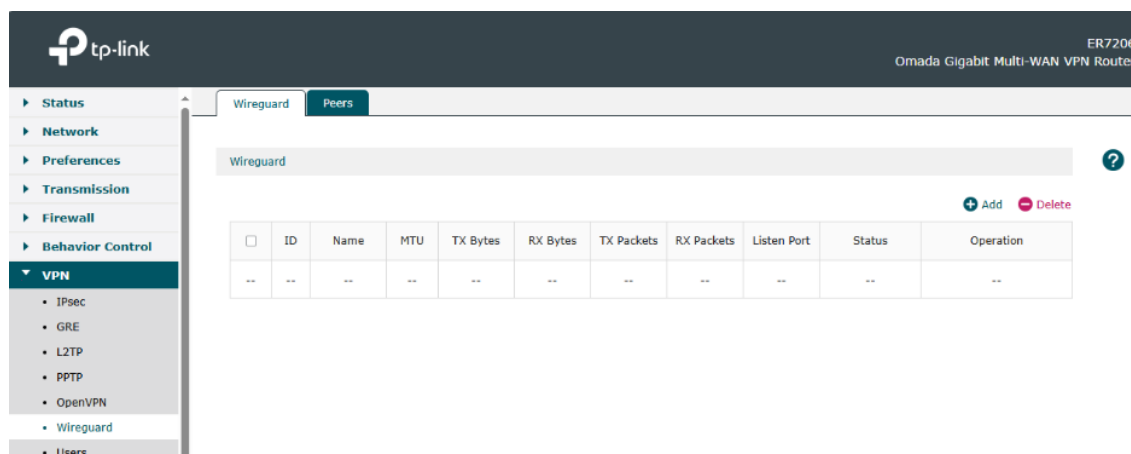
Un VPN, Virtual Private Network, est un service permettant de créer une connexion sécurisée et chiffrée entre un appareil et un réseau distant via Internet. Il masque l'adresse IP de l'utilisateur en redirigeant son trafic à travers un serveur distant, garantissant ainsi confidentialité, anonymat et protection des données contre les interceptions ou censures. Utilisé aussi bien pour sécuriser les connexions Wi-Fi publiques que pour accéder à des ressources distantes (réseau d'entreprise, sites géo-restreints), un VPN repose sur des protocoles comme WireGuard, OpenVPN ou IPsec pour assurer un haut niveau de sécurité et de performance.

Protocole	Sécurité	Vitesse	Facilité de configuration	Chiffrement	Utilisation courante
WireGuard	Très élevée	Très rapide	Facile	ChaCha20 (moderne et rapide)	VPN personnel, entreprise
OpenVPN	Élevée	Moyenne	Moyenne	AES-256	VPN sécurisé, accès distant
PPTP	Faible (obsolète)	Très rapide	Très facile	MPPE (faible)	Ancien, à éviter
L2TP	Moyenne (nécessite IPsec)	Moyenne	Moyenne	Aucun seul, souvent couplé à IPsec	VPN entreprise
GRE	Aucune (pas de chiffrement)	Rapide	Facile	Aucun	Tunnels sans chiffrement
IPsec	Très élevée	Moyenne	Complexe	AES-256	Sécurité réseau, VPN site à site

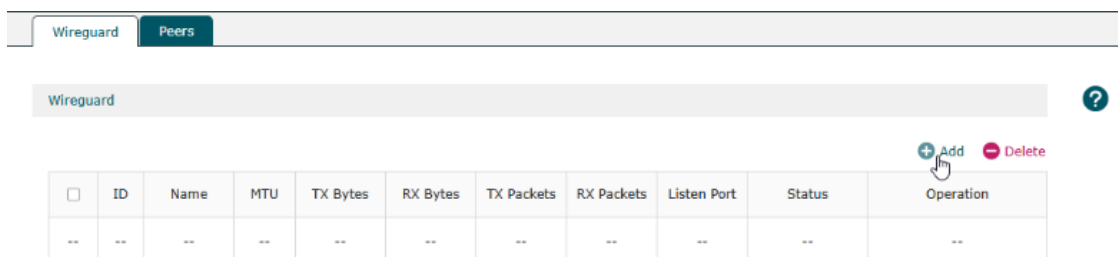
Configuration d'un serveur VPN

1.2. Configuration du serveur VPN Wireguard

On choisit d'installer la solution Wireguard.



On ajoute un tunnel, il faut cliquer sur "Add".



Ici, on nous demande de remplir 2 informations : le nom du serveur et son adresse IP.

This screenshot shows the 'Add' dialog box for the Wireguard configuration. It contains the following fields and options:

- Name: [Text input field]
- MTU: 1420 (576-1440)
- Listen Port: 51820 (1-65535)
- Private Key: [Text input field] (Optional)
- Public Key: EjNOQianZDJG3gYnIj4Xi6-
- Local IP Address: [Text input field]
- Status: ☒ Enable
- Buttons: OK, Cancel

Configuration d'un serveur VPN

Pour ces informations, nous allons remplir :

- **Nom** : VPN_Belletable
- **IP** : 10.75.10.1

Name:	VPN_Belletable	
MTU:	1420	(576-1440)
Listen Port:	51820	(1-65535)
Private Key:	(Optional)
Public Key:	qFAL5k2VYZUC/nu4xQ8AC	
Local IP Address:	10.75.10.1	
Status:	<input checked="" type="checkbox"/> Enable	
<div>OK Cancel</div>		

Les autres informations, pré-remplies, sont :

- Le **MTU**, *Maximum Transmission Unit*, est la taille maximale, en octets, d'un paquet pouvant être transmis sur un réseau sans fragmentation. Il est crucial pour un VPN car il impacte directement la performance, la stabilité et la sécurité de la connexion.
- Le **port écouté** : C'est le port de la carte réseau de la machine sur laquelle est installée le VPN (ici, le routeur) écouté pour la connexion.
- Clé **privée** et **publique** : Dans un VPN, la clé privée et la clé publique sont utilisées pour chiffrer et authentifier les communications entre le client et le serveur, garantissant ainsi la confidentialité et l'intégrité des données.





La clé privée est secrète, générée localement, et est utilisée pour signer les données et déchiffrer les messages reçus, tandis que la clé publique est partagée librement avec d'autres appareils, chiffre les messages à destination de l'appareil possédant la clé privée correspondante, et permet de vérifier l'authenticité des données signées avec la clé privée.

- **Statut** : On veut que le VPN soit actif, donc on clique sur "Enable".





Configuration d'un serveur VPN

On rentre les données en cliquant sur "OK".

La configuration du serveur a bien été prise en compte.

<input type="checkbox"/>	ID	Name	MTU	TX Bytes	RX Bytes	TX Packets	RX Packets	Listen Port	Status	Operation
<input type="checkbox"/>	1	VPN_Belletable	1420	443.4 MiB	12.4 MiB	369288	65983	51820	Enabled 	  

Maintenant, on importe le certificat. Cliquer sur le 2ème bouton sous "Operation".

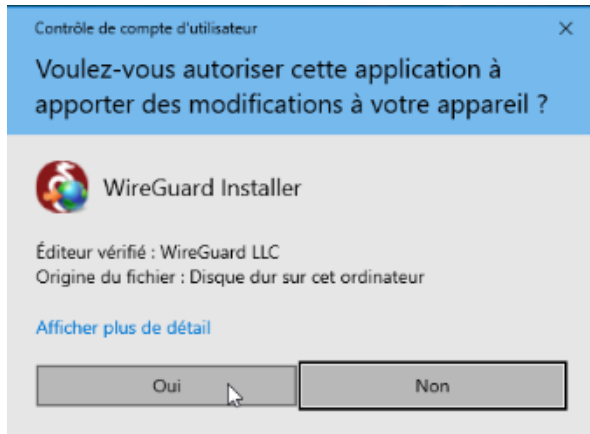
<input type="checkbox"/>	ID	Name	MTU	TX Bytes	RX Bytes	TX Packets	RX Packets	Listen Port	Status	Operation
<input type="checkbox"/>	1	VPN_Belletable	1420	443.4 MiB	12.4 MiB	369288	65983	51820	Enabled 	  

3. Installation et configuration du client VPN

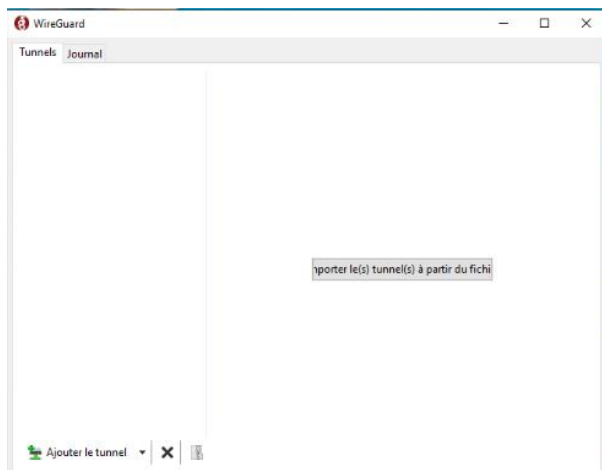
3.1. Installation du client VPN

Maintenant que le serveur a été configuré, on configure le client.

On va sur une machine cliente, et on installe le VPN.



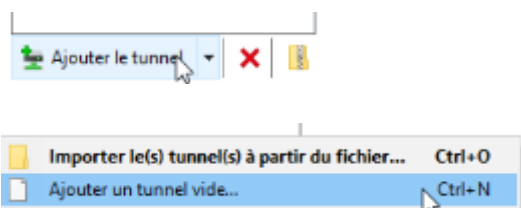
Une fois que le client a été installé, le logiciel ressemble à ceci :



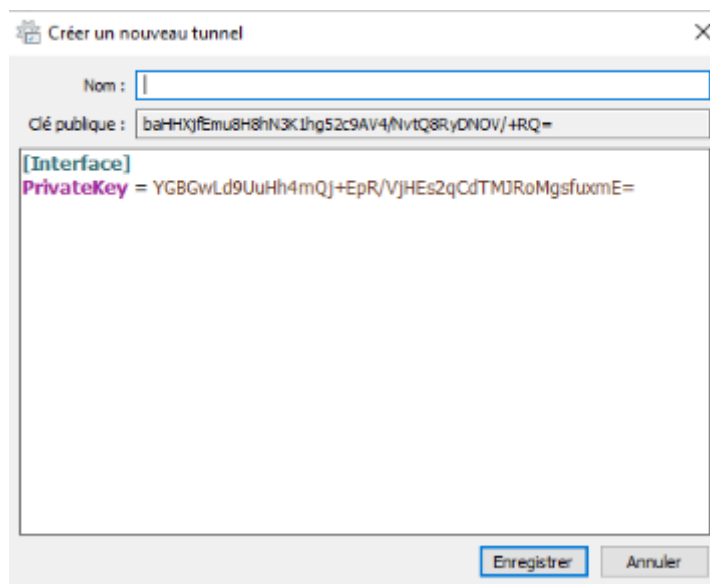
Maintenant, il va falloir importer le certificat depuis le serveur sur la machine cliente. En effet, l'architecture logicielle d'un VPN fonctionne sur la base serveur/client, avec un client qui importe le certificat et peut se connecter en tunnel depuis sa machine, même hors du réseau, au serveur VPN, simulant un réseau local même à des kilomètres.

Configuration d'un serveur VPN

On clique sur "Ajouter le tunnel", puis sur "Ajouter un tunnel vide".




On a d'abord une fenêtre quasiment vide.



Il faut remplir les informations suivantes :

- Nom : donner un nom au tunnel, ici on choisit "SRV_VPN"
- La première partie, [Interface]
 - o Clé privée : laisser l'information par défaut, elle va changer par la suite.
 - o Adresse : Entrer une adresse de la plage d'adresse VPN.
 - o DNS : rentrer l'adresse de la passerelle du réseau WAN, 192.168.16.201/24.
- La deuxième partie, [Peer]
 - o Clé publique : rentrer la clé publique téléchargée depuis le serveur
 - o Adresses autorisées : autoriser toute adresse, 0.0.0.0/0
 - o Endpoint : Mettre l'adresse publique (adresse côté WAN du routeur) et le numéro de port attribué, soit 192.168.16.201:51820.

Configuration d'un serveur VPN

 Modifier le tunnel ✕

Nom : VPN_Belletable

Clé publique : JP/ktXYrFFHwXns2tOPh5w3biogLnwybvnpP77ZVgFU=

[Interface]

PrivateKey = GAAXcEjkQ26Oc1VxnP9aqO1+LTpbQ8DcaPUWyFpMiEM=
ListenPort = 51820
Address = 10.75.10.10/24
DNS = 192.168.16.201

[Peer]

PublicKey = qFAL5k2VYZUC/nu4xQ8AOtK5xFdXbrviRuk8315Dq04=
AllowedIPs = 0.0.0.0/0
Endpoint = 192.168.16.201:51820

☒ Bloquer tous le trafic hors tunnel (interrupteur) Enregistrer Annuler

On enregistre. La configuration a bien été prise en compte. On active.

Interface : VPN_Belletable

État : ☐ Éteinte

Clé publique : JP/ktXYrFFHwXns2tOPh5w3biogLnwybvnpP77ZVgFU=

Port d'écoute : 51820

Adresses : 10.75.10.10/24

Serveurs DNS : 192.168.16.201

Activer

Homologue

Clé publique : qFAL5k2VYZUC/nu4xQ8AOtK5xFdXbrviRuk8315Dq04=

Adresses IP autorisées : 0.0.0.0/0

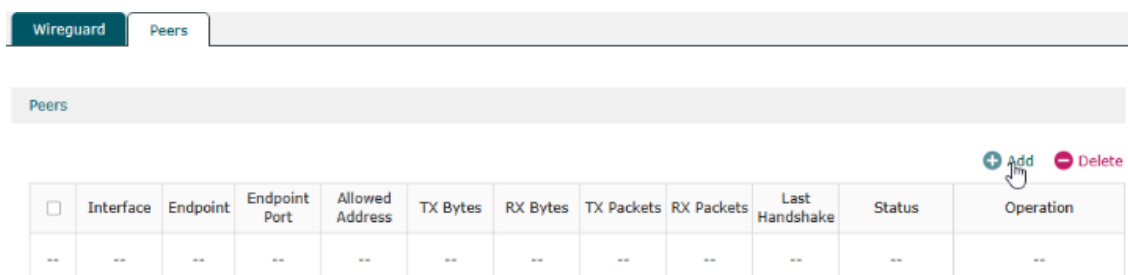
Point de terminaison : 192.168.16.201:51820

Configuration d'un serveur VPN

4. Ajout des pairs

Dans WireGuard, les connexions sont basées sur des paires de clés cryptographiques (clé privée et clé publique) utilisées pour authentifier et chiffrer les communications entre les pairs (peers).

On crée des pairs pour notre protocole Wireguard. Cliquer sur “Peers”, puis “Add”.

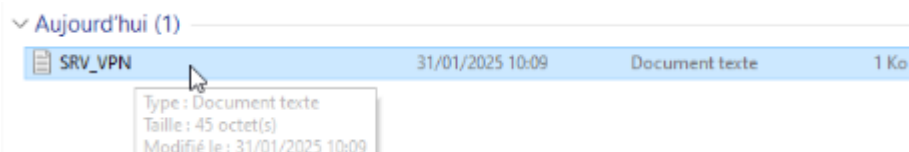


Différentes informations sont à remplir :

The screenshot shows the 'Add' dialog box in the WireGuard configuration interface. The dialog box has the following fields and controls:

- Interface: A dropdown menu with '---' selected.
- Public Key: A text input field.
- Endpoint: A text input field with '(Optional)' next to it.
- Endpoint Port: A text input field with '(Optional, 1-65535)' next to it.
- Allowed Address: A text input field with a slash '/' next to it.
- Preshared Key: A text input field with a checkmark icon and '(Optional)' next to it.
- Persistent Keepalive: A text input field with '25' and '(0-65535)' next to it.
- Comment: A large text area with a cursor and '(0-128 characters)' below it.
- Status: A checkbox labeled 'Enable' which is checked.
- Buttons: 'OK' and 'Cancel' at the bottom left.

- Interface : choisir SRV_VPN
- Public key : Prendre la clé publique dans le fichier qu'on a téléchargé précédemment du serveur



Configuration d'un serveur VPN

SRV_VPN - Bloc-notes

Fichier Edition Format Affichage Aide

nJ157HEzITPfspJ16AbHEBS1a6/Ra73Q3XpB3mPm4yM=

- Adresse autorisée : mettre l'adresse de la machine cliente, ici 10.75.1.21/24
- Statut : Laisser sur "Enable"

On valide en cliquant sur "Ok"

<input type="checkbox"/>	Interface	Endpoint	Endpoint Port	Allowed Address	TX Bytes	RX Bytes	TX Packets	RX Packets	Last Handshake	Status	Operation
...	VPN_Belletable	192.168.16.201	51820	10.75.10.0/24	451.2 MiB	14.6 MiB	380853	80224	1 minute, 25 seconds ago	Enabled	

Interface:

Public Key:

Endpoint: (Optional)

Endpoint Port: (Optional, 1-65535)

Allowed Address: /

Preshared Key: (Optional)

Persistent Keepalive: (0-65535)

Comment:

(0-128 characters)

Status: ☒ Enable

On clique sur "Ok"

Modifying the configuration may disconnect the tunnel before the next handshake of the peer end. Do you want to continue?

La configuration a bien été prise en compte.

<input type="checkbox"/>	Interface	Endpoint	Endpoint Port	Allowed Address	TX Bytes	RX Bytes	TX Packets	RX Packets	Last Handshake	Status	Operation
<input type="checkbox"/>	VPN_Belletable	192.168.16.201	51820	10.75.10.0/24	453.6 MiB	15.3 MiB	384001	82550	20 seconds ago	Enabled	

Configuration d'un serveur VPN

5. Test de la configuration

On active le tunnel.

Interface : VPN_Belletable

État :  Activée

Clé publique : JP/ktXYrfFHwXns2tOPh5w3biogLnwybvnpP77ZVgFU=

Port d'écoute : 51820

Adresses : 10.75.10.10/24

Serveurs DNS : 192.168.16.201

Désactiver

Homologue

Clé publique : qFAL5k2VYZUC/nu4xQ8AOtK5xFdX
brviRuk8315Dq04=

Adresses IP autorisées : 0.0.0.0/0

Point de terminaison : 192.168.16.201:51820

Dernier établissement d'une liaison : Il y a 5 secondes

Transfert : 3,78 Kio reçu(e), 18,68 Kio
envoyé(e)

Depuis notre machine physique, on peut accéder au domaine LAN Belletable. On peut ping le contrôleur de domaine :

```
C:\Users\kagem>ping 10.75.1.1
```

```
Envoi d'une requête 'Ping' 10.75.1.1 avec 32 octets de données :
```

```
Réponse de 10.75.1.1 : octets=32 temps=2 ms TTL=127
```

```
Réponse de 10.75.1.1 : octets=32 temps=1 ms TTL=127
```

```
Réponse de 10.75.1.1 : octets=32 temps=2 ms TTL=127
```

```
Réponse de 10.75.1.1 : octets=32 temps=2 ms TTL=127
```

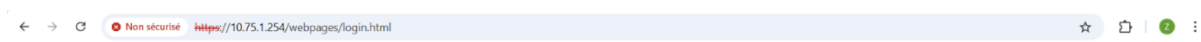
```
Statistiques Ping pour 10.75.1.1:
```

```
Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),  
Durée approximative des boucles en millisecondes :
```

```
Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
```

Configuration d'un serveur VPN

On peut se connecter au routeur :

A screenshot of a TP-Link login form. The form has a dark header with the TP-Link logo. Below the header, there are two input fields: "Username" and "Password". Below these fields are two buttons: "Log In" and "Clear".

tp-link

Username

Password