


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 :
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	Ressources fournies / contraintes techniques / Résultats attendu
	Proxmox, VM, Debian, Wireguard, Routeur
Productions associées	Liste des documents produits et description

Modalités d'accès aux productions	Identifiants, mots de passe, URL d'un espace de stockage et présentation de l'organisation du stockage
	<ul style="list-style-type: none"> - Adresse du routeur : 10.0.75.254 - Identifiant : - Mot de passe :

Table des matières

Tapez le titre du chapitre (niveau 1)	1
Tapez le titre du chapitre (niveau 2)	2
Tapez le titre du chapitre (niveau 3)	3
Tapez le titre du chapitre (niveau 1)	4
Tapez le titre du chapitre (niveau 2)	5
Tapez le titre du chapitre (niveau 3)	6

Configuration d'un serveur VPN

Configuration d'un serveur VPN

1. Installation

1.1. Connexion au routeur

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.

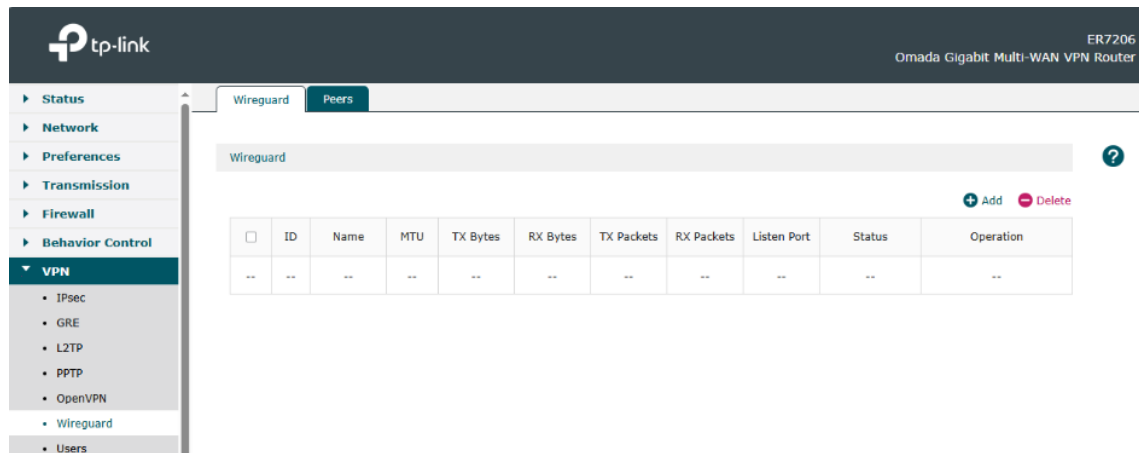
Un VPN, Virtual Private Network, est un service permettant de créer une connexion sécurisée et chiffrée entre un appareil et un réseau distant via Internet. Il masque l'adresse IP de l'utilisateur en redirigeant son trafic à travers un serveur distant, garantissant ainsi confidentialité, anonymat et 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

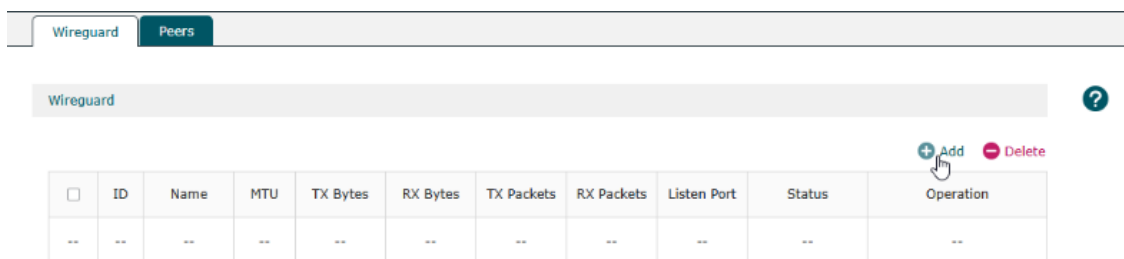
Configuration d'un serveur VPN

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.

The screenshot shows the 'Add' dialog box for a new Wireguard peer. The dialog box has the following fields and values:

- Name: (empty)
- MTU: 1420 (576-1440)
- Listen Port: 51820 (1-65535)
- Private Key: (empty) (Optional)
- Public Key: EjNOQianZDJG3gYnIj4Xig-
- Local IP Address: (empty)
- Status: ☒ Enable

There are 'OK' and 'Cancel' buttons at the bottom of the dialog box.

Configuration d'un serveur VPN

Pour ces informations, nous allons remplir :

- **Nom** : SRV-VPN
- **IP** : 10.75.1.13

Wireguard

+ Add - Delete

<input type="checkbox"/>	ID	Name	MTU	TX Bytes	RX Bytes	TX Packets	RX Packets	Listen Port	Status	Operation
<div><div>Name:</div><div>SRV_VPN</div><div>MTU:</div><div>1420</div><div>(576-1440)</div><div>Listen Port:</div><div>51820</div><div>(1-65535)</div><div>Private Key:</div><div>*****</div><div>(Optional)</div><div>Public Key:</div><div>9nBvZ215C0Th4y+dLFRj2</div><div>Local IP Address:</div><div>10.75.1.13</div><div>Status:</div><div><input checked="" type="checkbox"/> Enable</div><div>OK</div><div>Cancel</div></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.

Wireguard

+ Add - Delete

<input type="checkbox"/>	ID	Name	MTU	TX Bytes	RX Bytes	TX Packets	RX Packets	Listen Port	Status	Operation
<input type="checkbox"/>	1	SRV_VPN	1420	0.0 B	0.0 B	0	0	51820	Enabled	

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

Wireguard

Peers

Wireguard

+ Add - Delete

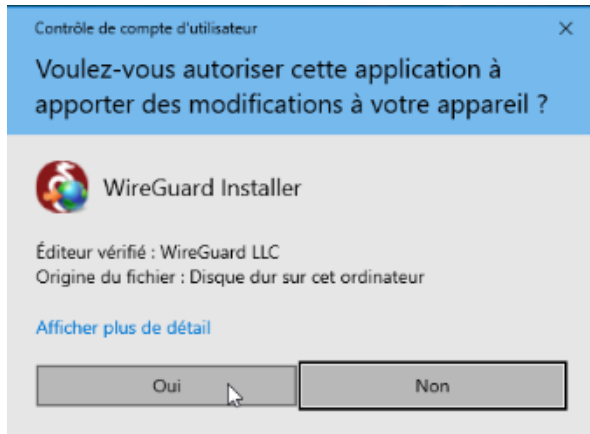
<input type="checkbox"/>	ID	Name	MTU	TX Bytes	RX Bytes	TX Packets	RX Packets	Listen Port	Status	Operation
<input type="checkbox"/>	1	SRV_VPN	1420	0.0 B	0.0 B	0	0	51820	Enabled	

2. Installation et configuration du client VPN

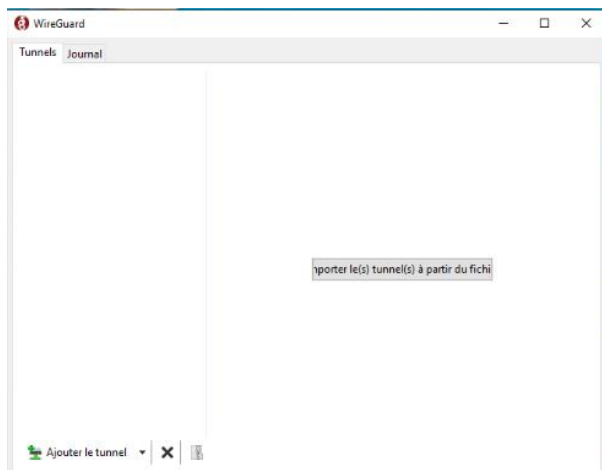
2.1. Installation du client VPN

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

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



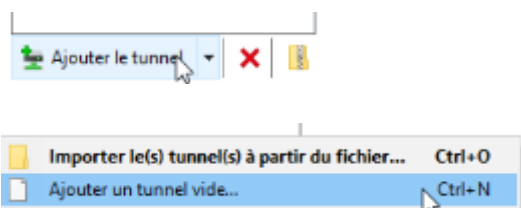
Une fois que le client a été installé, le logiciel ressemble à ceci :



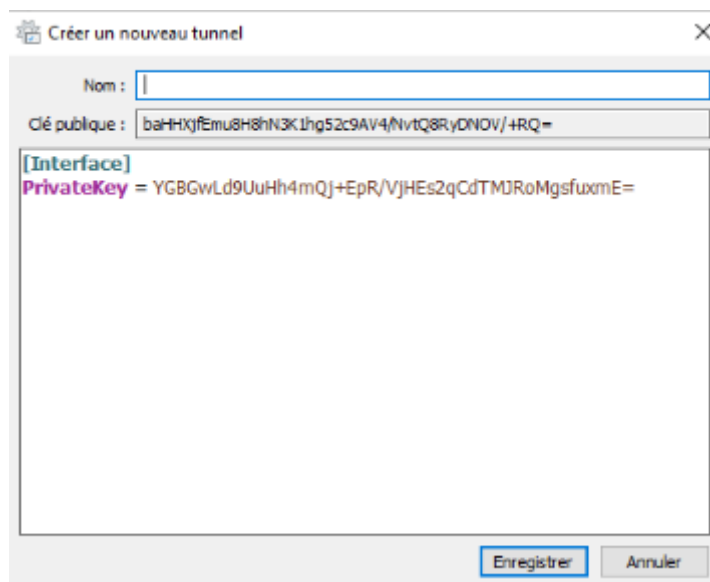
Maintenant, il va falloir importer le certificat depuis le serveur sur la machine cliente. En effet, l'architecture logicielle d'un VPN fonctionne sur la base serveur/client, avec un client qui importe le certificat et peut se connecter en tunnel depuis sa machine, même hors du réseau, au serveur VPN, 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 : rentrer une adresse différente de celle du routeur
 - o DNS : rentrer l'adresse d'internet, 8.8.8.8
- 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 du routeur et son port utilisé, 192.168.16.254:51820.

Configuration d'un serveur VPN

Modifier le tunnel

Nom : SRV_VPN

Clé publique : 6CwEDkO7tc+HbbiTu7MsOSwShZFFYwH5Mn00LLWBw=

[Interface]
PrivateKey = aAkASmmSWlDdemTr/auRG4sIjJunkFumpRf4JludEQ=
Address = 10.75.1.21/24
DNS = 8.8.8.8

[Peer]
PublicKey = nJi57HEzITPfspJi6AbHEBSla6/Ra73Q3XpB3mPm4yM=
AllowedIPs = 10.75.1.21/24
Endpoint = 192.168.16.254:51820

Enregistrer Annuler

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

Tunnels Journal

SRV_VPN

Interface : SRV_VPN

État : Éteinte

Clé publique : 6CwEDkO7tc+HbbiTu7MsOSwShZFFYwH5Mn00LLWBw=

Adresses : 10.75.1.21/24

Serveurs DNS : 8.8.8.8

Activer

Homologue

Clé publique : nJi57HEzITPfspJi6AbHEBSla6/Ra73Q3XpB3mPm4yM=

Adresses IP autorisées : 10.75.1.21/24

Point de terminaison : 192.168.16.254:51820

Le tunnel est actif.

Tunnels Journal

SRV_VPN

Interface : SRV_VPN

État : Activée

Clé publique : 6CwEDkO7tc+HbbiTu7MsOSwShZFFYwH5Mn00LLWBw=

Port d'écoute : 61636

Adresses : 10.0.0.1/24

Serveurs DNS : 8.8.8.8

Désactiver

Homologue

Clé publique : nJi57HEzITPfspJi6AbHEBSla6/Ra73Q3XpB3mPm4yM=

Adresses IP autorisées : 0.0.0.0/0

Point de terminaison : 192.168.16.254:51820

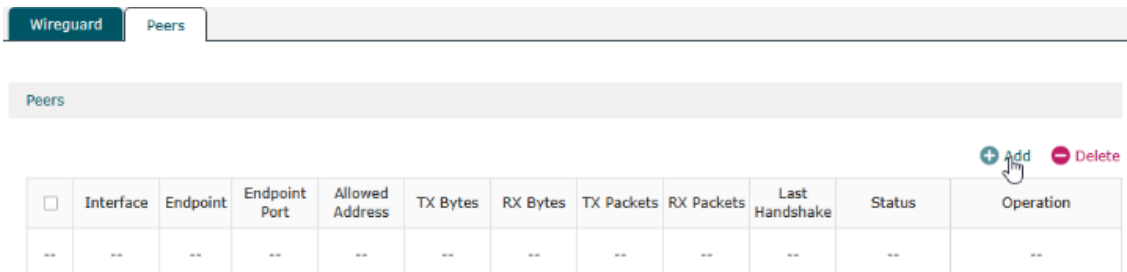
Transfert : 0 o reçu(e), 148 o envoyé(e)

Configuration d'un serveur VPN

3. 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).

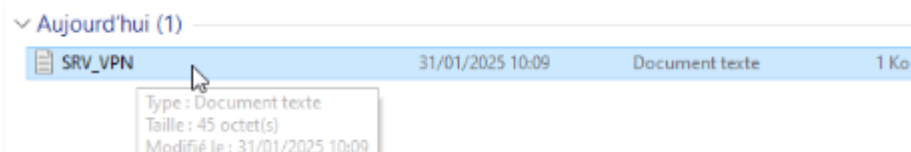
On crée des pairs pour notre protocole Wireguard. Cliquer sur "Peers", puis "Add".



Différentes informations sont à remplir :



- 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"

Wireguard Peers

Interface: SRV_VPN

Public Key: nJ157HEzITPfspJ16AbHEBS1a6/Ra73Q3XpB3mPm4yM=

Endpoint: (Optional)

Endpoint Port: (Optional, 1-65535)

Allowed Address: 10.0.0.1 / 24

Preshared Key: (Optional)

Persistent Keepalive: 25 (0-65535)

Comment: (0-128 characters)

Status: ☒ Enable

OK Cancel

Activer Windows

On clique sur "Ok"

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

Yes No

La configuration a bien été prise en compte.

	Interface	Endpoint	Endpoint Port	Allowed Address	TX Bytes	RX Bytes	TX Packets	RX Packets	Last Handshake	Status	Operation
<input type="checkbox"/>	SRV_VPN	---	---	10.0.0.0/24	---	---	---	---	---	Enabled ✗	

4. Test de la configuration
