



CONFIGURATION D'UN SERVEUR VPN	
<i>Installation, configuration et gestion d'un serveur d'accès à distance sécurisée</i>	
	
Auteur : Zachary Winkler	Date de publication : 24.01.2025

Objectif	Permission d'un accès à distance sécurisé
Ressources	Proxmox, VM, Debian, Wireguard
Outils	Liste des outils complémentaires utilisés, que ce soit pour la réalisation de la procédure ou pour sa validation
URL	Listes d'URL utiles pour compléter la procédure
Autres	Autres informations complémentaires

Convention

Par convention, les informations particulières seront mises en avant tout au long de cette procédure en respectant les règles et mise en page ci-dessous :

TITRE DE LA PROCEDURE

1. LES DIFFERENTS CHAPITRES

A. Parties intermédiaires



Ce paragraphe apporte à l'utilisateur une information qui pourra l'aider ou lui rappeler un ou plusieurs points précis et utiles pour sa réalisation.

Ce paragraphe apporte à l'utilisateur une information importante sur un ou plusieurs points précis.

*Celle-ci est **indispensable** pour la bonne réalisation de la procédure.*

Table des matières

CONFIGURATION D'UN SERVEUR VPN	4
1. Installation	4
A. Choix d'une solution	4
B. Configuration du serveur VPN WireGuard	4
2. Installation et configuration du client vpn.....	9
C. Installation du client VPN.....	9
3. Ajout des pairs	12
4. Test de la configuration	14
5. Configuration de l'adressage dynamique : Serveur PPTP.....	16
D. Configuration du bassin d'adresses	16
E. Configuration du serveur VPN PPTP	18
F. Création d'un utilisateur VPN PPTP	20

CONFIGURATION D'UN SERVEUR VPN

1. INSTALLATION

A. Choix d'une solution

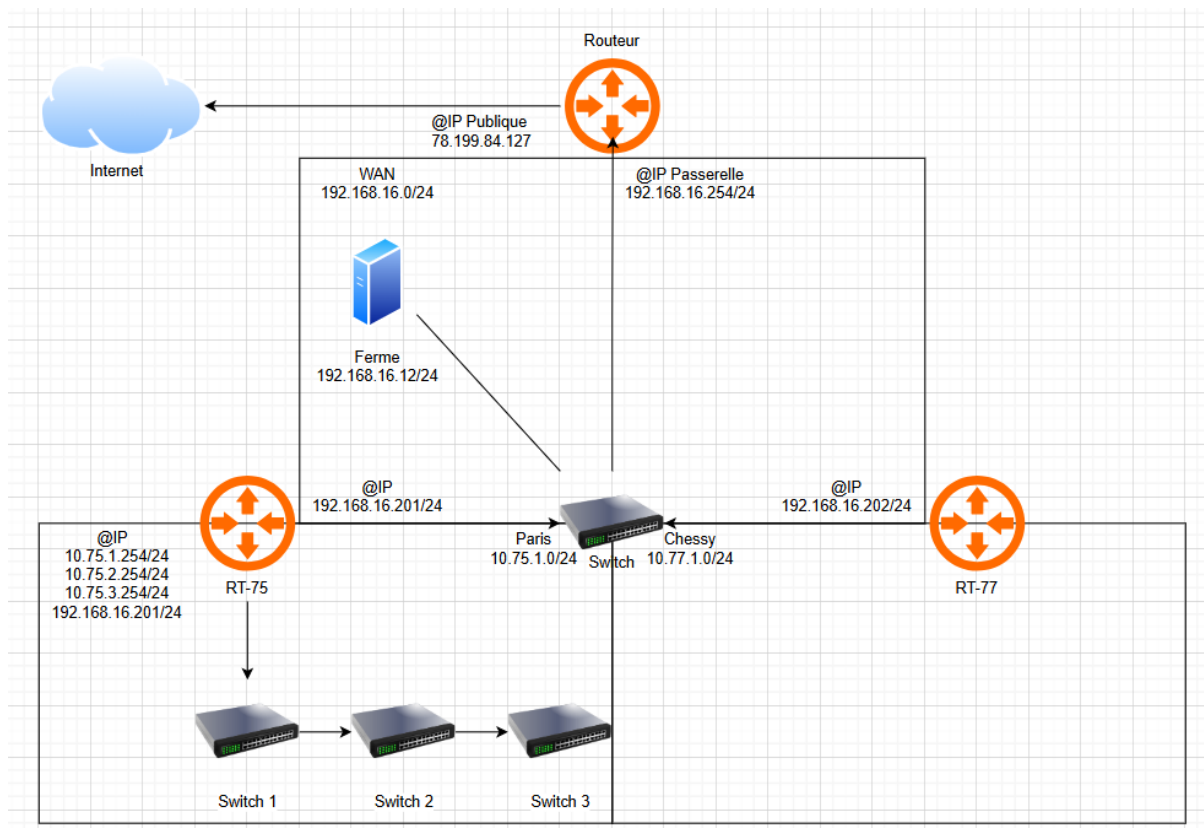
Afin de garantir un accès à distance au réseau domestique d'entreprise, la société Belletable a demandé la mise en place d'une solution de VPN.

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.

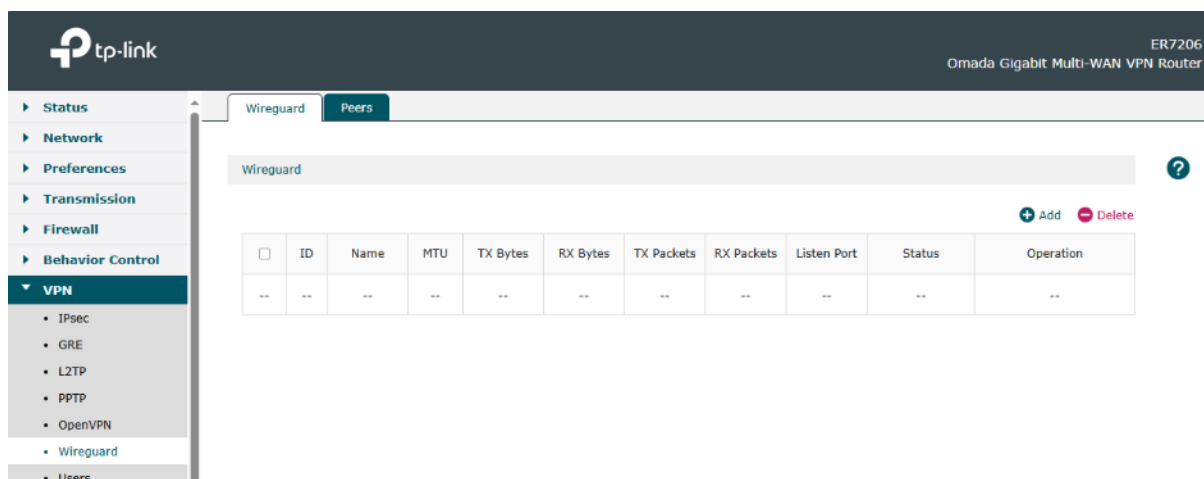
Protocole	Sécurité	Vitesse	Facilité de configuration	Chiffrement	Utilisation courante
WireGuard	Très élevée	Très rapide	Facile	ChaCha20 (moderne et rapide)	VPN personnel, entreprise
OpenVPN	Élevée	Moyenne	Moyenne	AES-256	VPN sécurisé, accès distant
PPTP	Faible (obsolète)	Très rapide	Très facile	MPPE (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

B. Configuration du serveur VPN WireGuard

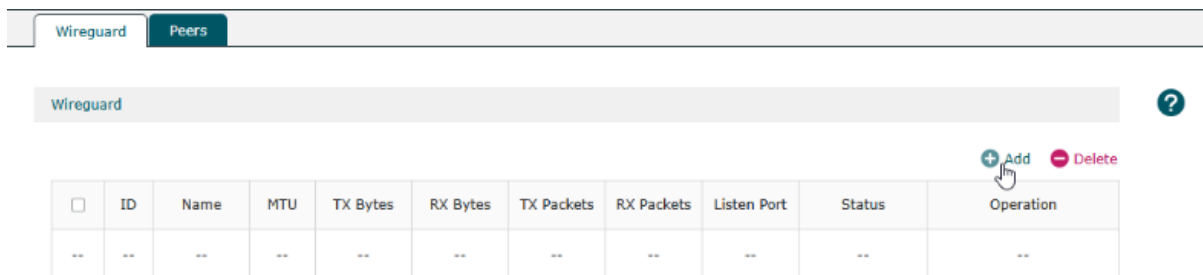
On choisit d'installer la solution Wireguard. Voici un schéma de notre réseau : en tant que machine dans le WAN, on cherche à avoir accès aux réseaux LAN Paris ou Chessy.



On se connecte au routeur.



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.

Name:
 MTU: (576-1440)
 Listen Port: (1-65535)
 Private Key: (Optional)
 Public Key:
 Local IP Address:
 Status: ☒ Enable
 OK Cancel

Pour ces informations, nous allons remplir :

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

Attention : Le protocole VPN installé sur le routeur doit se voir attribuer une adresse IP différente du routeur. C'est un autre réseau logique que l'on configure. Quand il sera configuré et actif, le routeur s'occupera automatiquement de faire le routage entre ce réseau logique et le réseau local LAN que l'on cherche à atteindre.

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</div> <div>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".

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	

On reçoit un fichier texte, contenant la clé publique.

VPN_Belletable.txt

×

+

Fichier Modifier Affichage

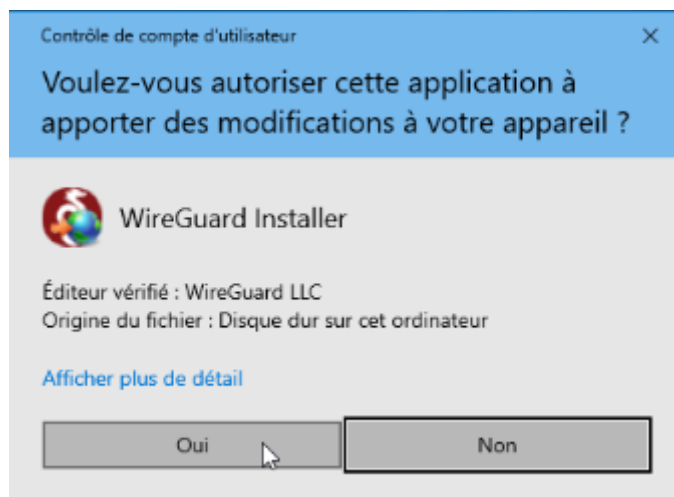
Ji/VLs2vMNRpoc+hxcg+ZH7RgjJy2hqks1NU45EmjQ4=

2. INSTALLATION ET CONFIGURATION DU CLIENT VPN

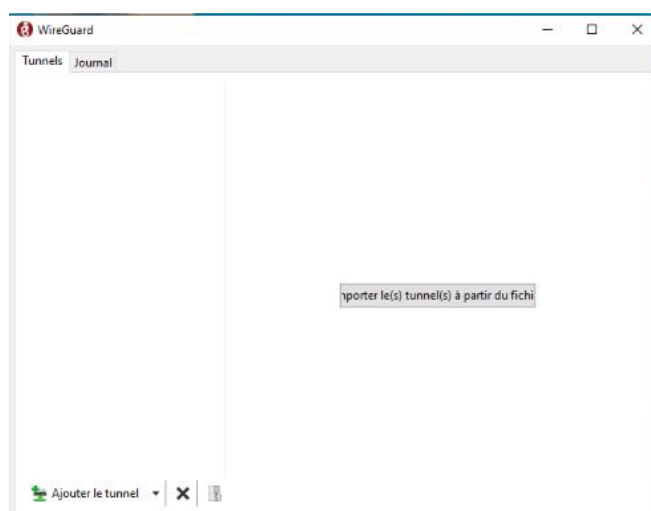
C. Installation du client VPN

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

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

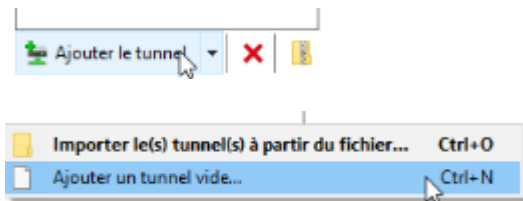


Une fois que le client a été installé, le logiciel ressemble à ceci :

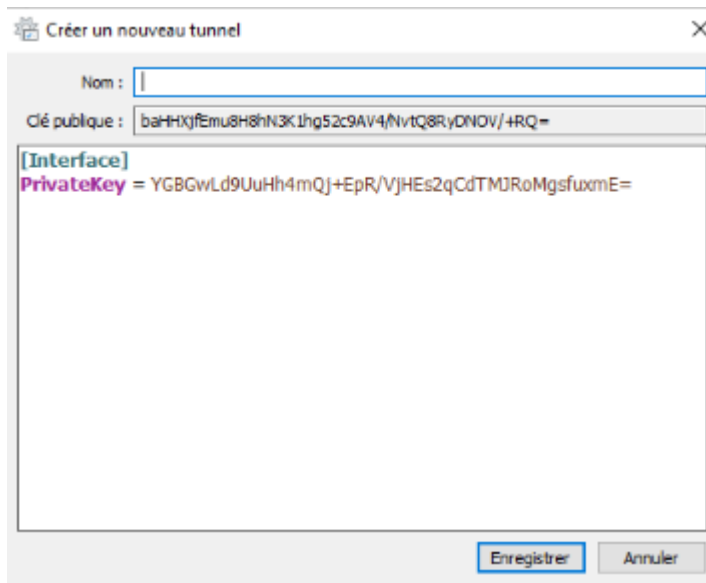


Maintenant, il va falloir importer le certificat depuis le serveur sur la machine cliente. En effet, l'architecture logicielle d'un VPN fonctionne sur la base serveur/client, avec un client qui importe le certificat et peut se connecter en tunnel depuis sa machine, même hors du réseau, au serveur VPN,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

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 du réseau VPN pour votre client. Ici, nous allons adresser le client en 10.75.10.11/24.
 - o **DNS** : rentrer l’adresse du port côté privé du routeur, ici 10.75.1.254.
- 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 le port utilisé par défaut Wireguard, 192.168.16.201:51820.

Modifier le tunnel

Nom : VPN_Belletable

Clé publique : o0RZmxXXciFfgLiRTLfGEYbfJJau/nWT3X1ueP7zXWo=

[Interface]

PrivateKey = eDIENlbcTTQXPa0kTQS0bD3FbmHexGaMHBE/jIXr8V4=

ListenPort = 51820

Address = 10.75.10.2/24

DNS = 192.168.16.201

[Peer]

PublicKey = FgvwyXXFQ5Y9JqSYIa35AxkBJ5gUYCfNlswPSiaIRFI=

AllowedIPs = 10.75.1.254/24

Endpoint = 192.168.16.201:51820

Enregistrer Annuler

Voici le script à copier/coller :

ListenPort = 51820

Address = 10.75.10.X/24

DNS = 192.168.16.201

[Peer]

PublicKey = Ji/VLs2vMNRpoc+hxcg+zH7RgjJy2hqks1NU45EmjQ4=

AllowedIPs = 0.0.0.0/0

Endpoint = 192.168.16.201:51820

Attention : Pour la ligne "Address", remplacer le X par un nombre compris entre 11 et 200. Il s'agit de la plage utilisable. Veiller à ce qu'elle ne soit pas déjà prise par un autre utilisateur

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

Interface : VPN_Belletable

État : ☐ Éteinte

Clé publique : o0RZmxXXciFfgLiRTLfGEYbfJJau/nWT3X1ueP7zXWo=

Port d'écoute : 51820

Adresses : 10.75.10.2/24

Serveurs DNS : 192.168.16.201

Activer

Homologue

Clé publique : FgwwyXXFQ5Y9JqSYla35AxkBJ5gUYCfNlswPSialR
FI=

Adresses IP autorisées : 10.75.1.254/24

Point de terminaison : 192.168.16.201:51820

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”.

Wireguard

Peers

Peers

+ Add

Delete

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

Différentes informations sont à remplir :

Wireguard Peers

Interface: ---

Public Key:

Endpoint: (Optional)

Endpoint Port: (Optional, 1-65535)

Allowed Address: /

Preshared Key: (Optional)

Persistent Keepalive: 25 (0-65535)

Comment:
 (0-128 characters)

Status: ☒ Enable

OK Cancel

- **Interface** : choisir VPN_Belletable
- **Public key** : Prendre la clé publique de l'interface de la machine qu'on a créée sur le client, celle de la première partie, "Interface", et la copier-coller ici.
- **Adresse autorisée** : mettre l'adresse du réseau client, ici 10.75.10.0/24.
- **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	10.75.10.2/32	9.9 MiB	1.9 MiB	11832	7278	55 seconds ago	Enabled	

Interface: VPN_Belletable

Public Key: o0RZmxXXciFfgLiRTLfGEYt

Endpoint: 192.168.16.201 (Optional)

Endpoint Port: 51820 (Optional, 1-65535)

Allowed Address: 10.75.10.2 / 32

Preshared Key: (Optional)

Persistent Keepalive: 25 (0-65535)

Comment:
 (0-128 characters)

Status: ☒ Enable

OK Cancel

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.

<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	10.75.10.2/32	12.4 MiB	2.2 MiB	14651	9040	23 seconds ago	Enabled	

4. TEST DE LA CONFIGURATION

On active le tunnel depuis le client.

Interface : VPN_Belletable

État : Activée

Clé publique : o0RZmxXXciFfgLiRTLfGEYbfJJau/nWT3X1ueP7zXWo=

Port d'écoute : 51820

Adresses : 10.75.10.2/24

Serveurs DNS : 192.168.16.201

Désactiver

Homologue

Clé publique : FgwwyXXFQ5Y9JqSYIa35AxkBJ5gUYCfNlswPSiaIRFI=

Adresses IP autorisées : 10.75.1.0/24

Point de terminaison : 192.168.16.201:51820

Dernier établissement d'une liaison : Il y a 44 secondes

Transfert : 982,18 Kio reçu(e), 149,98 Kio envoyé(e)

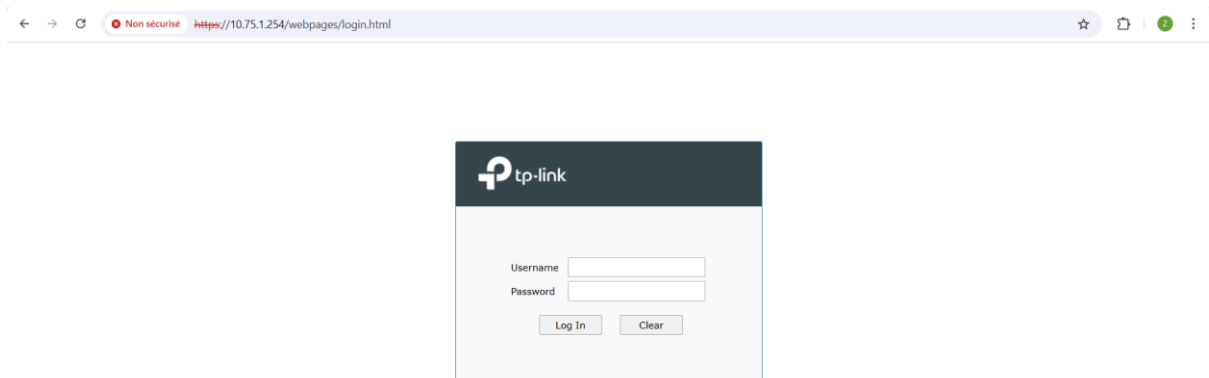
Depuis notre machine physique, on peut accéder au domaine LAN Belletable. On peut ping le contrôleur de domaine :

```
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
```

On peut se connecter au routeur :



D. Configuration du bassin d'adresses

Désormais, la suite de la solution consiste en la configuration d'une solution VPN dynamique, où chaque client aurait automatiquement un adressage VPN, sans intervention manuelle extérieure. Pour cela, il faut utiliser la fonction pool (bassin d'adresses) du routeur pour les VPN.

- ▼ **Preferences**
 - IP Group
 - IPv6 Group
 - Time Range
 - **VPN IP Pool**
 - Service Type
 - Location Group

VPN IP Pool List					
					+ Add - Delete
<input type="checkbox"/>	ID	IP Pool Name	Starting IP Address	Ending IP Address	Operation
<input type="checkbox"/>	--	--	--	--	--

Un menu apparaît, avec différentes informations à rentrer :

VPN IP Pool List

+

 Add

−

 Delete

<input type="checkbox"/>	ID	IP Pool Name	Starting IP Address	Ending IP Address	Operation
--	--	--	--	--	--

IP Pool Name:

Starting IP Address:

Ending IP Address:

OK

Cancel

- IP Pool name : le nom du pool d'adresses du réseau IP VPN que l'on configure. Ici, nous allons l'appeler VPN_Belletable.
- Starting IP address : c'est la première adresse utilisable de la plage que l'on configure. Ici, on va choisir 10.75.10.30/24.
- Ending IP address : c'est la dernière adresse utilisable de la plage que l'on configure. Ici, on va choisir 10.75.10.200/24.

VPN IP Pool List

+

 Add

−

 Delete

<input type="checkbox"/>	ID	IP Pool Name	Starting IP Address	Ending IP Address	Operation
--	--	--	--	--	--

IP Pool Name:

Starting IP Address:

Ending IP Address:

OK

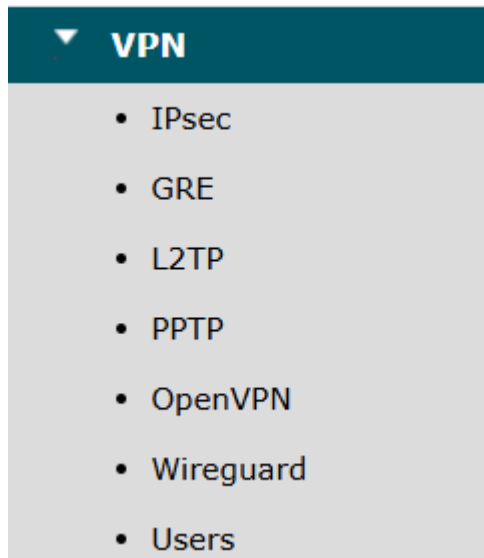
Cancel

Cliquer sur le bouton "Ok" en bas pour enregistrer.

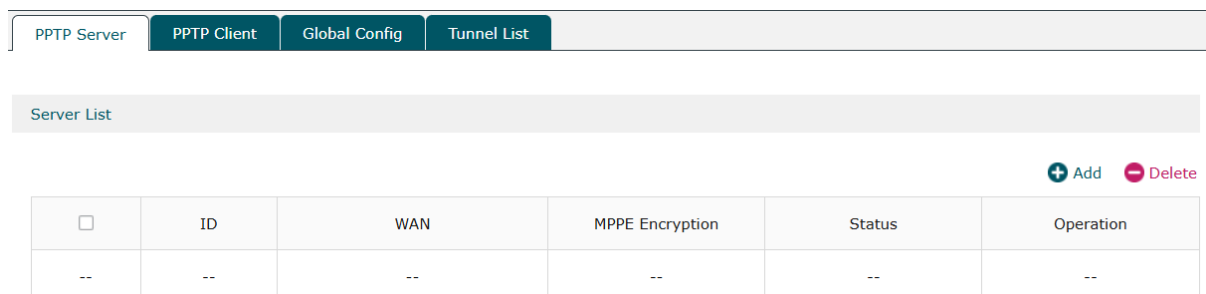
E. Configuration du serveur VPN PPTP

Maintenant il faut configurer le serveur PPTP.

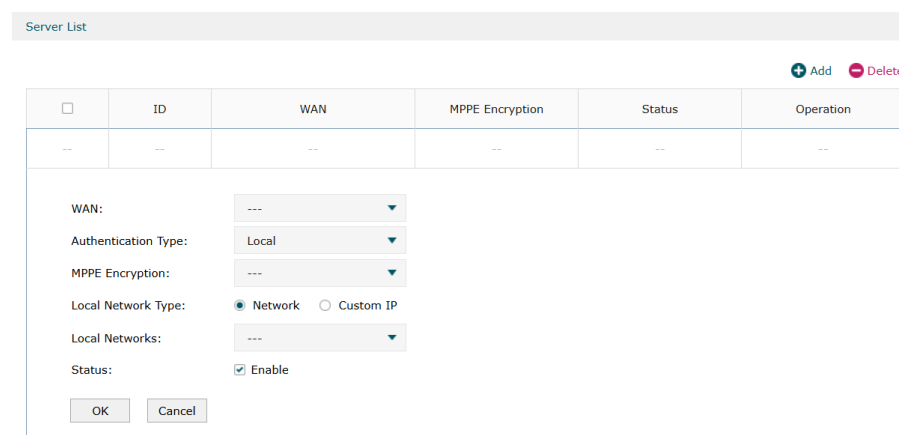
Dans le menu déroulant de gauche du routeur, aller dans VPN, puis PPTP.



Un menu apparaît, avec différents onglets. Dans le premier, sur lequel on arrive par défaut, PPTP Server, cliquer sur le bouton “Add” (ajouter) en bas à gauche.



Un menu apparaît.



Entrer les informations suivantes :

- WAN : Choisir dans le menu déroulant. Ici SFP WAN.
- MPPE Encryption : Encrypted.
- Local Networks : Choisir dans le menu déroulant. Ici info.

Server List

+

 Add

-

 Delete

<input type="checkbox"/>	ID	WAN	MPPE Encryption	Status	Operation
<input type="checkbox"/>	--	--	--	--	--

WAN:

SFP WAN

Authentication Type:

Local

MPPE Encryption:

Encrypted

Local Network Type:

☒ Network
 ☐ Custom IP

Local Networks:

info

Status:

☒ Enable

OK

Cancel

Cliquer sur OK en bas pour enregistrer. La configuration a bien été enregistrée.

Server List

+

 Add

-

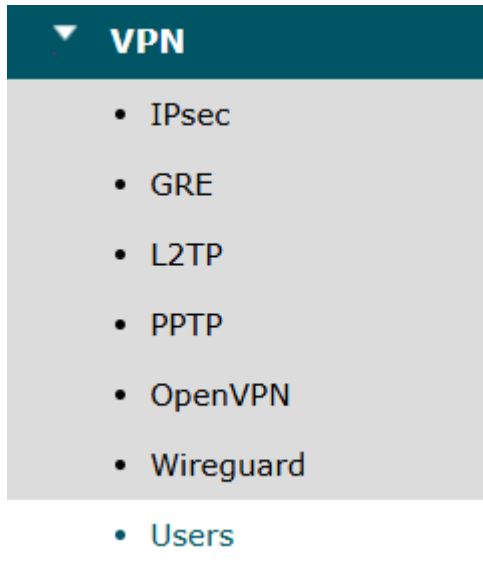
 Delete

<input type="checkbox"/>	ID	WAN	MPPE Encryption	Status	Operation
<input type="checkbox"/>	1	SFP WAN	Encrypted	Enabled	

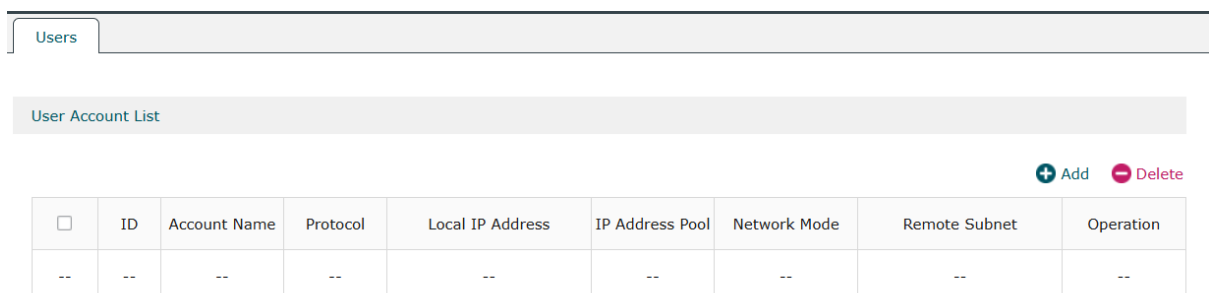
F. Création d'un utilisateur VPN PPTP

Il faut désormais configurer un utilisateur VPN PPTP.

Dans le menu déroulant du routeur, cliquer sur VPN, puis sur Users.



On arrive sur une page avec un menu. Cliquer sur “Add” pour ajouter un utilisateur.



Un nouveau menu s'ouvre, avec différentes informations à rentrer.

<input type="checkbox"/>	ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operation
--	--	--	--	--	--	--	--	--

Account Name:

Password: (1-128 characters)

Protocol: ▼

Local IP Address:

IP Address Pool: ▼

Primary DNS:

Secondary DNS: (Optional)

Network Mode: ▼

Max Connections: (1-100)

Remote Subnet: /

Il faut entrer ces informations :

- **Account Name** : Le nom de l'utilisateur. Ici, on va entrer "User_VPN"
- **Password** : configurer un mot de passe pour l'utilisateur.
- **Protocol** : choisir dans le menu déroulant le protocole utilisé. Ici, c'est PPTP.
- **Local IP Address** : rentrer l'adresse IP de l'adaptateur virtuel VPN, de préférence une adresse du réseau qu'on cherche à atteindre. Ici, 10.75.1.200.
- **IP address pool** : Choisir dans le menu déroulant le pool configuré. Ici, VPN_Belletable.
- **Primary DNS** : mettre l'adresse publique du routeur connectant Paris et le WAN. Ici, 192.168.16.201.
- **Network Mode** : dans le menu déroulant, choisir le mode Client-To-Lan.
- **Max Connections** : Choisir le nombre maximal de connexions. Ici, on met 10.

Cliquer sur OK en bas pour enregistrer.

<input type="checkbox"/>	ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operation
--	--	--	--	--	--	--	--	--

Account Name:

Password: (1-128 characters)
Low Middle High

Protocol: PPTP

Local IP Address:

IP Address Pool: VPN_Belletable

Primary DNS:

Secondary DNS: (Optional)

Network Mode: Client-to-LAN

Max Connections: (1-100)

La configuration a bien été prise en compte.

User Account List

+ Add - Delete

<input type="checkbox"/>	ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operation
<input type="checkbox"/>	1	User_VPN	PPTP	10.75.1.200	VPN_Belletable	Client-to-LAN	--	