

## Paramétrage VPN IPSEC

Le paramétrage IPSEC est une demande d'un de nos clients.

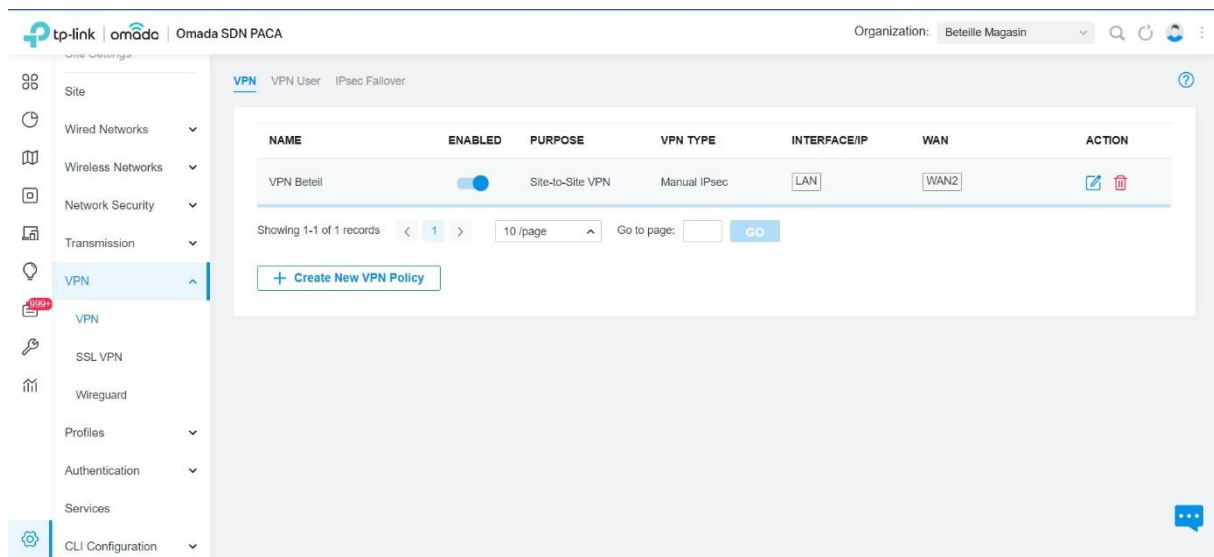
Je suis sur le controller Cloud Omada par TpLink, hébergé sur un de nos serveur Linux.

J'ai ainsi la possibilité de paramétrer le VPN, via un routeur TpLink de la gamme Omada précédemment installé chez notre client.

Je me rends dans la rubrique VPN, puis crée une nouvelle politique de VPN.

Le but étant de mettre à disposition pour le client un tunnel communiquant entre les deux sites : Beteille Magasin et Beteille Siege.

VPN Beteille est le nom attribué sur le client Beteille Magasin.



Voici le paramétrage appliqué :

Choix du VPN Site-to-Site

Type IPSEC

La passerelle du réseau local qui sera disponible sera en 192.168.1.1 (elle doit être différente de la passerelle de notre routeur déjà en place qui est en 192.168.2.1).

Je sélectionne le WAN2 correspondant à l'arrivée fibre du client.

Enfin la PRE SHARED KEY est créée.

Je laisse les autres paramètres par défaut en place.

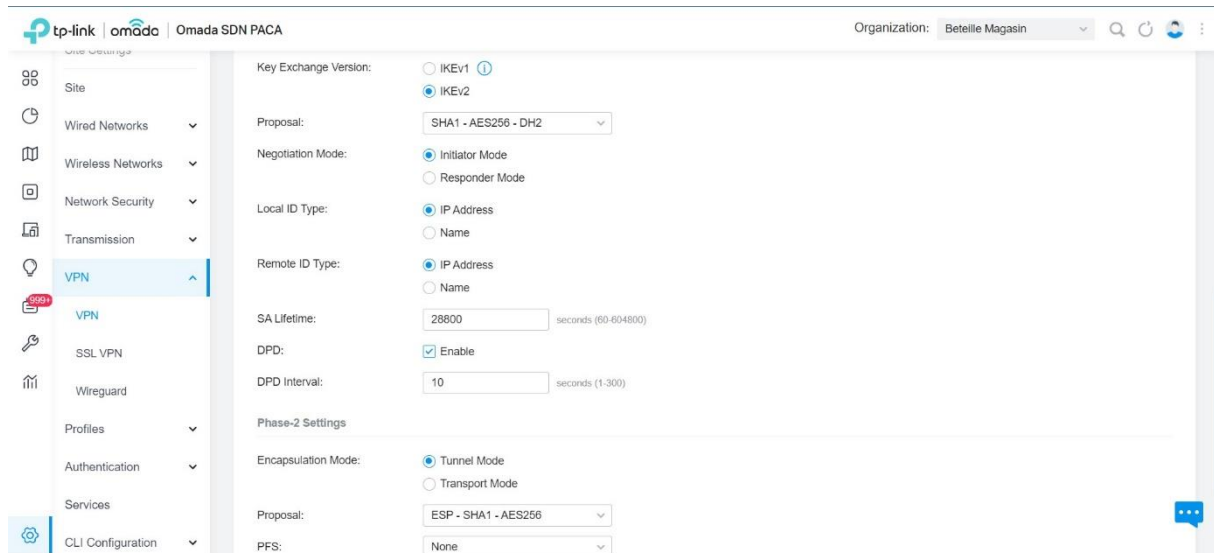
The screenshot shows the Omada SDN PACA web interface for configuring a VPN. The left sidebar contains a navigation menu with options like Site, Wired Networks, Wireless Networks, Network Security, Transmission, VPN (selected), SSL VPN, Wireguard, Profiles, Authentication, Services, and CLI Configuration. The main panel is titled 'Edit VPN Policy' and contains the following settings:

- Name: VPN Betell
- Status: ☒ Enable
- Purpose: ☒ Site-to-Site VPN, ☐ Client-to-Site VPN
- VPN Type: ☐ Auto IPsec, ☒ Manual IPsec
- Remote Gateway: 94.187.139.66
- Remote Subnets: 192 . 168 . 1 . 1 / 24 (with an 'Add Subnet' button)
- Local Network Type: ☒ Network, ☐ Custom IP
- Local Networks: All (with an information icon)
- Pre-Shared Key: [Redacted]
- WAN: WAN2

Le protocole de chiffrement est en Ikev2

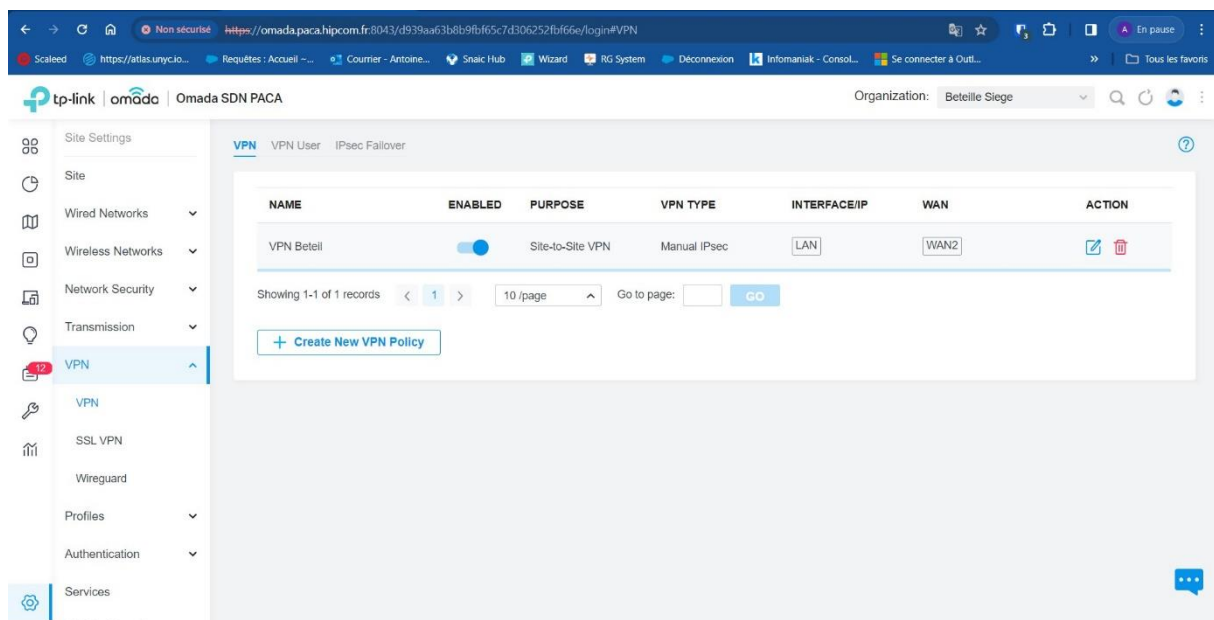
SHA1 AES256

Les autres paramètres restent également par défaut.



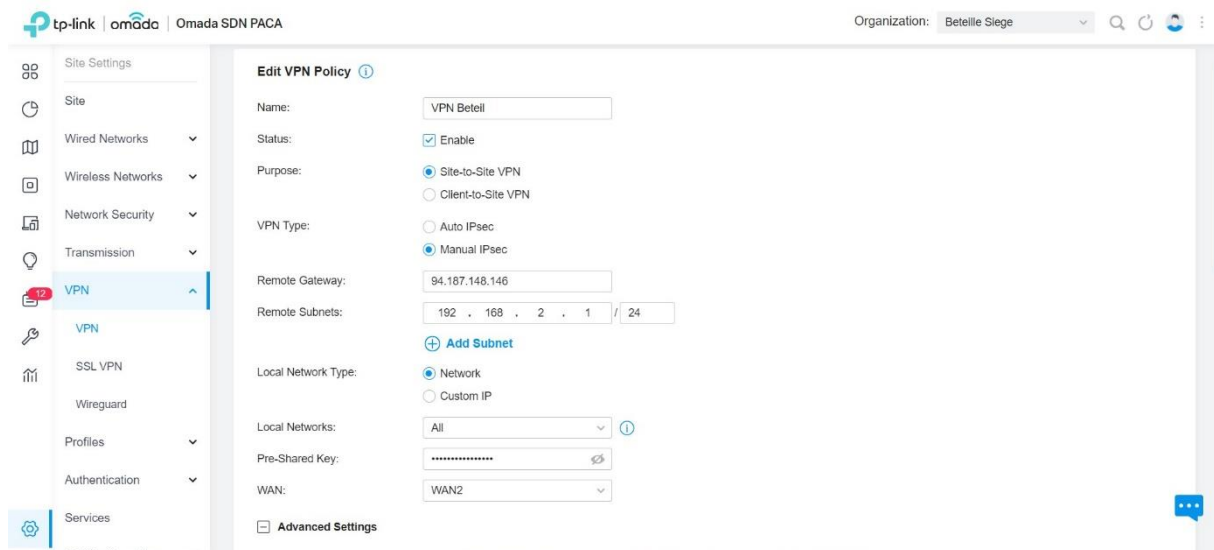
Je me retrouve sur le site de notre client Beteille Siege.

Il suffit d'appliquer les mêmes paramètres que sur le site Beteille Magasin précédemment configuré.



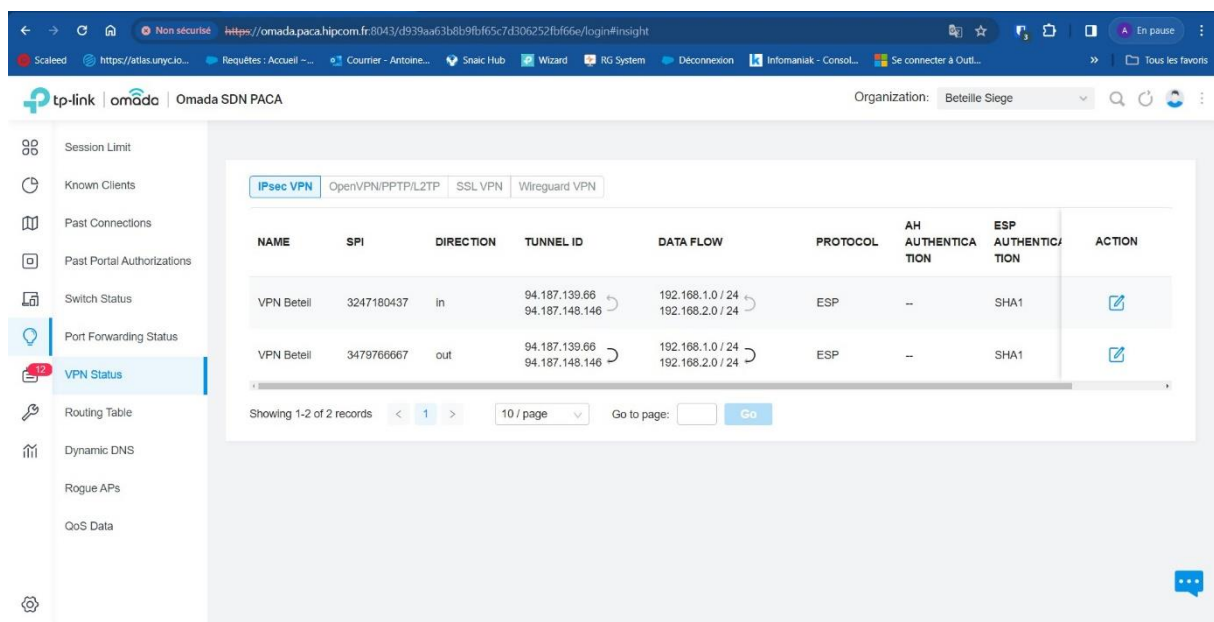
Antoine Gargi  
Aristee Formation  
2022-2024

L'important est de bien modifier la passerelle du remote subnets qui est en 192.168.2.1 afin de ne pas être en conflit avec la passerelle du LAN de notre routeur en place qui est ici en 192.168.1.1

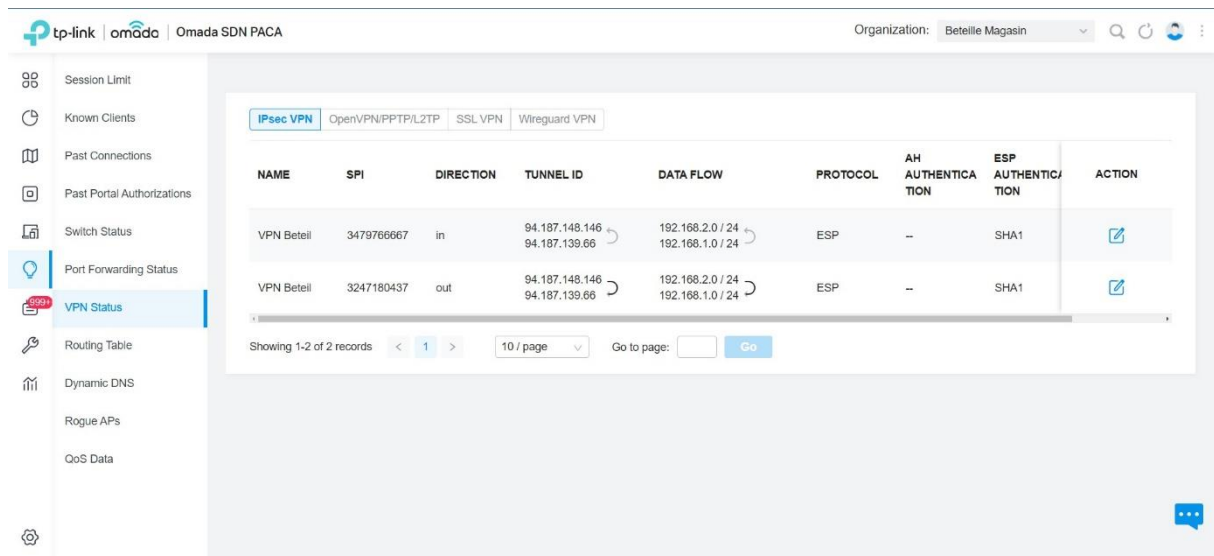


Enfin, j'effectue les tests avec le client à distance, il nous confirme que cela est bien fonctionnel.

Afin de vérifier techniquement que cela est en place, l'interface status sur le site Beteille Siege nous montre les connexions en cours et ainsi le tunnel qui comunique bien en atteignant les IP publics des deux sites Beteille.



En se rendant sur status du VPN de Beteille Magasin :



Voici un exemple de paramétrage d'un VPN Client-Serveur en dur sur un routeur TP-Link Omada ER-605 :

Je me rends sur le lien IP du client voulu.

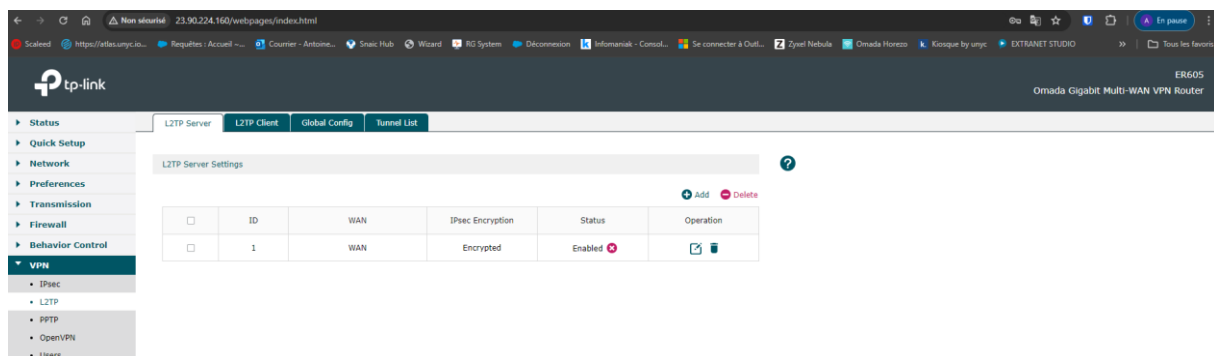
Je me rends dans VPN, L2TP (étant le protocole que nous allons utiliser) et je configure le serveur sur l'interface WAN de notre client.

WAN : WAN

IPSEC Encryption : Encrypted

Pre-Shared-key : \*\*\*\*\*

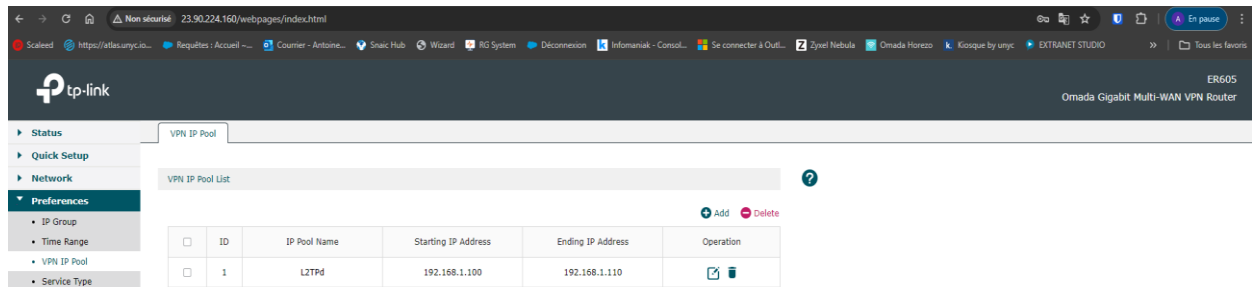
Status : Enables



Antoine Gargi  
Aristee Formation  
2022-2024

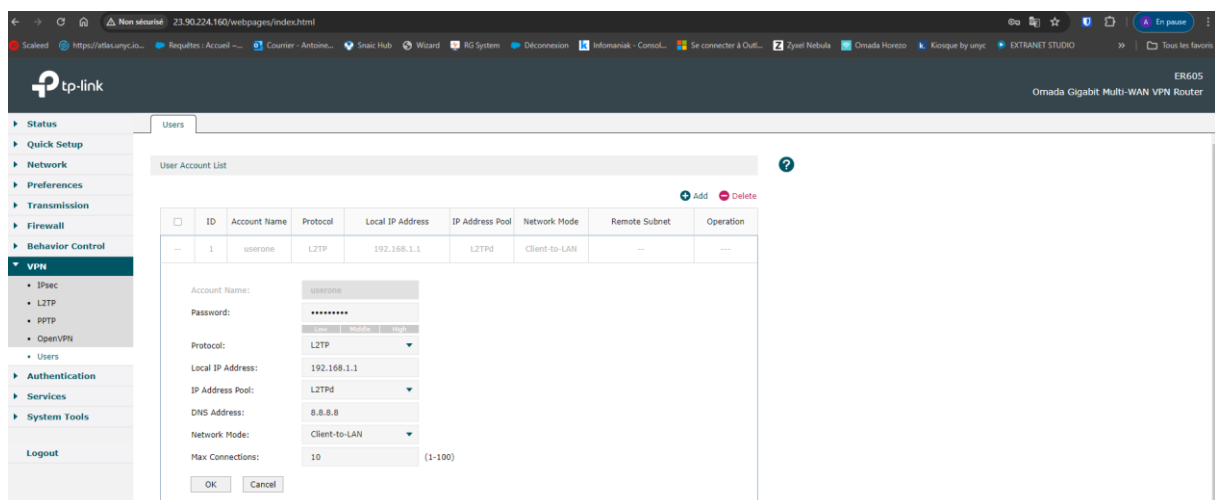
Je me rends ensuite dans *Préférences* puis je crée dans un premier temps un *VPN IP Pool*

Je nomme l'IP Pool, puis choisis un début d'adresse en 192.168.1.100 jusqu'à 192.168.1.110



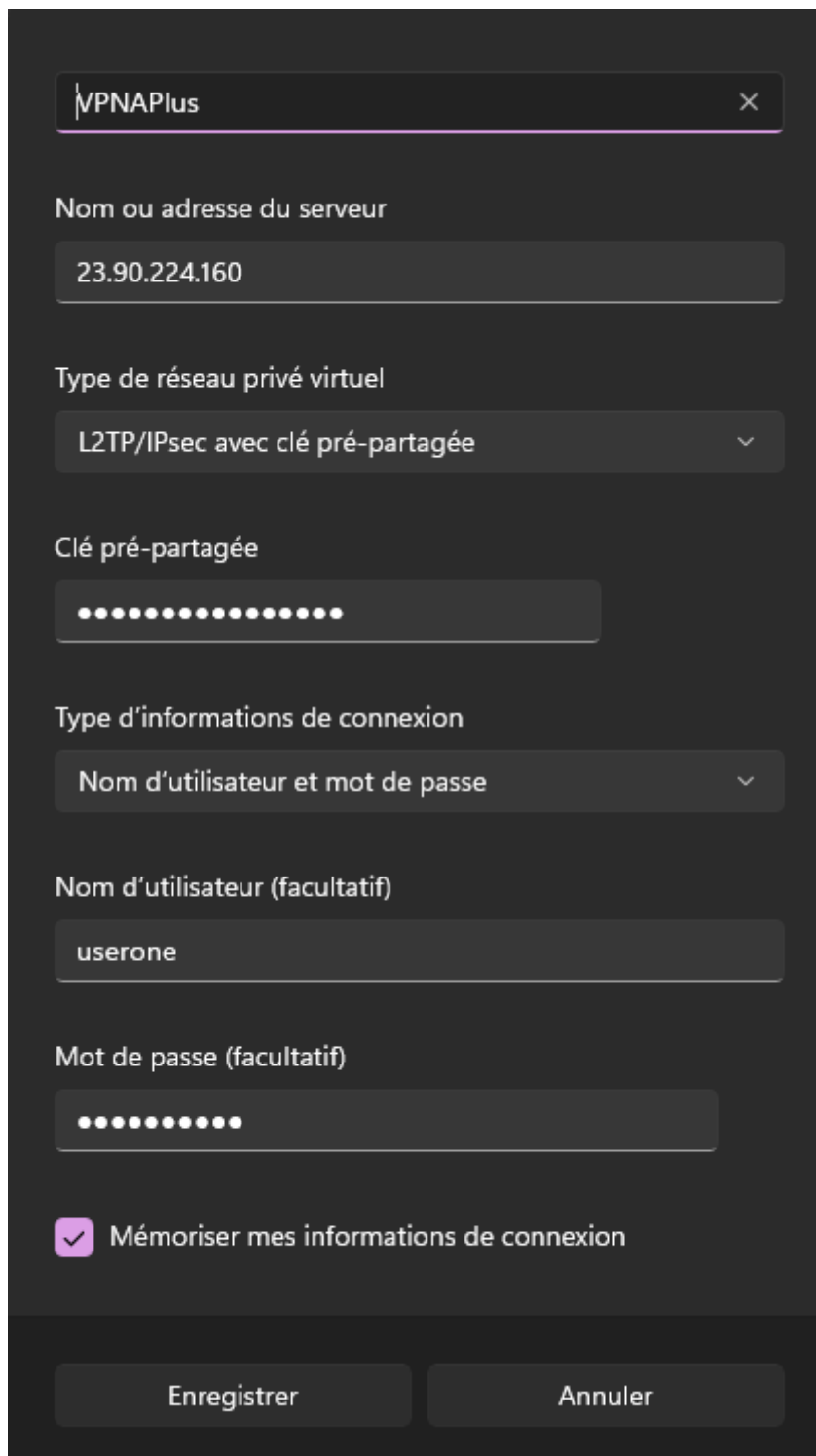
Je me rends ensuite dans *Users* et crée un utilisateur « userone » avec un mot de passe attribué.

Je choisis le protocole L2TP, j'indique l'adresse IP de la passerelle du LAN (192.168.1.1), j'associe le Pool VPN précédemment créé, indique un DNS en (8.8.8.8) et choisis un VPN Type Client-to-LAN.



Je peux me rendre sur mon PC dans les paramètres Windows afin de paramétrer le VPN créé :

J'entre ici le nom du VPN (non obligatoire), l'adresse IP publique sur lequel le serveur est configuré, le type de serveur VPN (L2TP), la clé pré partagée configurée en amont et le nom de l'utilisateur (non obligatoire ici).



The image shows a Windows Settings window for configuring a new VPN connection. The window has a dark theme. At the top, there is a search bar with the text "VPNAPIus" and a close button (X). Below this, the settings are organized into sections:

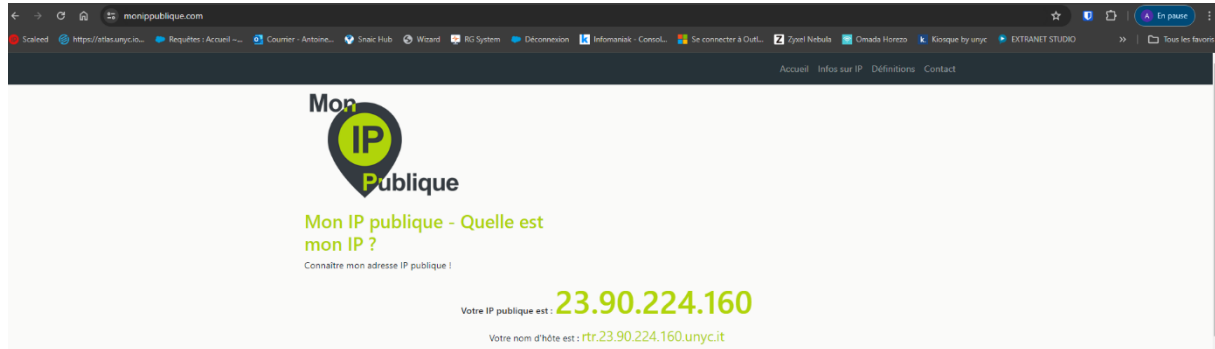
- Nom ou adresse du serveur:** A text field containing "23.90.224.160".
- Type de réseau privé virtuel:** A dropdown menu showing "L2TP/IPsec avec clé pré-partagée".
- Clé pré-partagée:** A text field filled with 16 dots, representing a masked password.
- Type d'informations de connexion:** A dropdown menu showing "Nom d'utilisateur et mot de passe".
- Nom d'utilisateur (facultatif):** A text field containing "userone".
- Mot de passe (facultatif):** A text field filled with 8 dots, representing a masked password.
- Mémoriser mes informations de connexion:** A checkbox that is checked (indicated by a purple checkmark icon).

At the bottom of the window, there are two buttons: "Enregistrer" (Save) and "Annuler" (Cancel).

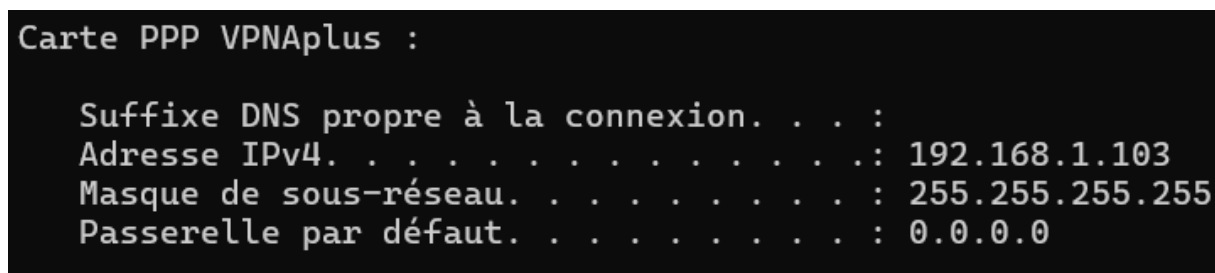
La connexion au VPN doit être fonctionnelle



Je vérifie en tapant *monippublique* si l'adresse IP correspond bien à celle de notre client.



Je peux également vérifier en local via CMD *ipconfig*, la carte PPP VPNAPlus indique que nous sommes connectés.



Si on vérifie de nouveau dans le Tunnel List du routeur, on aperçoit également bien notre connexion active :

