Antoine Gargi
Aristee Formation
2022-2024

Paramétrage VPN IPSEC

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

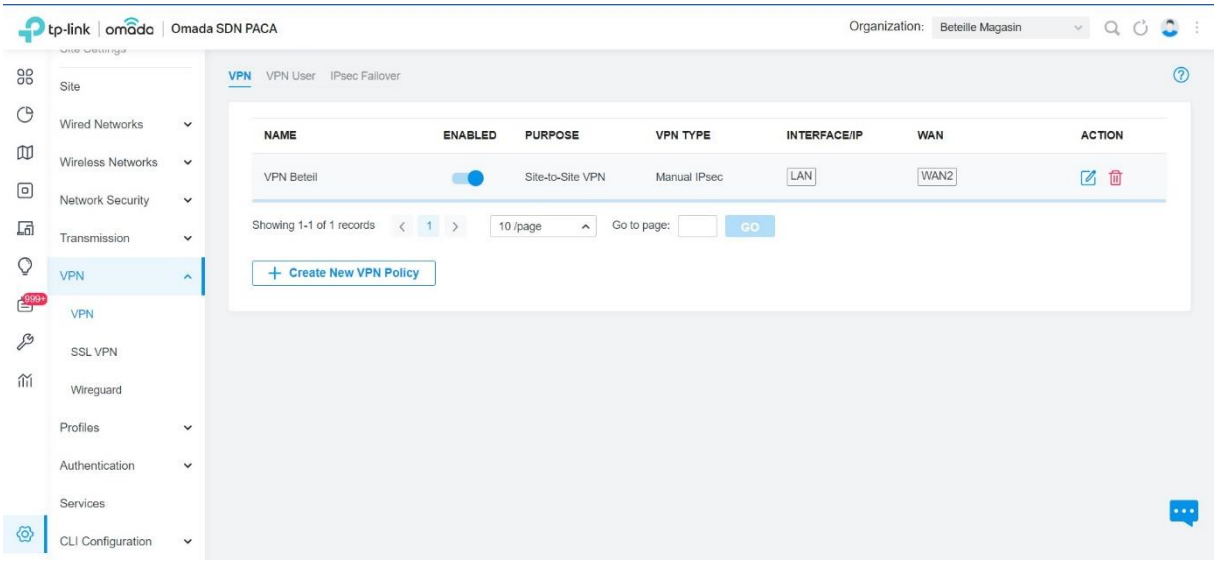
Je suis sur le controller Cloud Omada par TpLink, hebergé sur un de nos serveur Linux.

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 créé 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.



Antoine Gargi
Aristee Formation
2022-2024

Voici le paramétrage appliqué :

Choix du VPN Site-to-Site

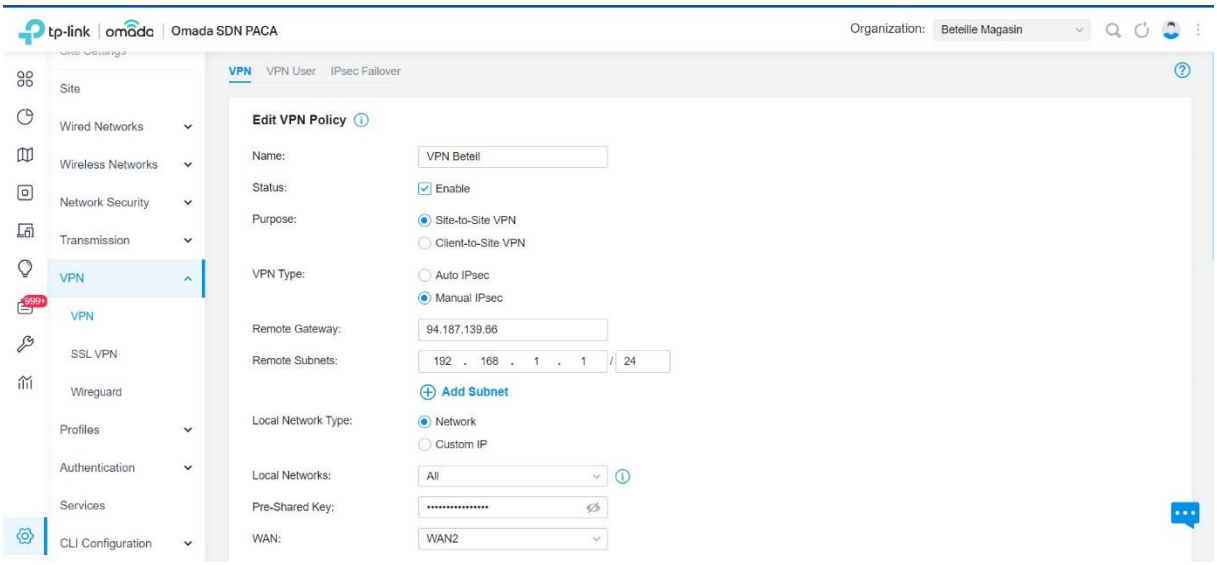
Type IPSEC

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.

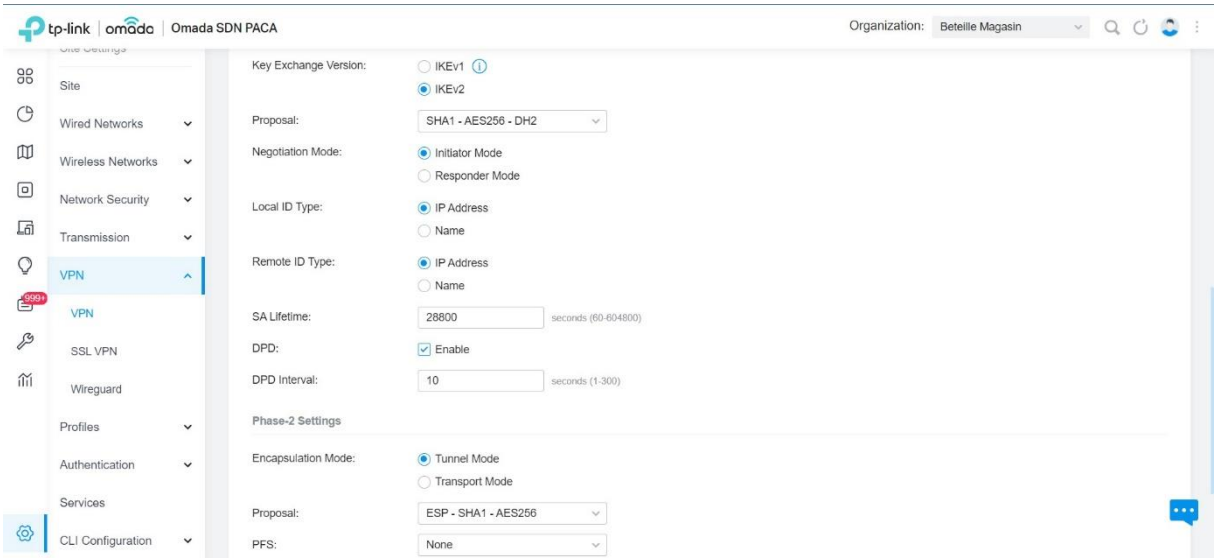
Je laisse les autres paramètres par défaut en place.



Le protocole de chiffrement est en Ikev2

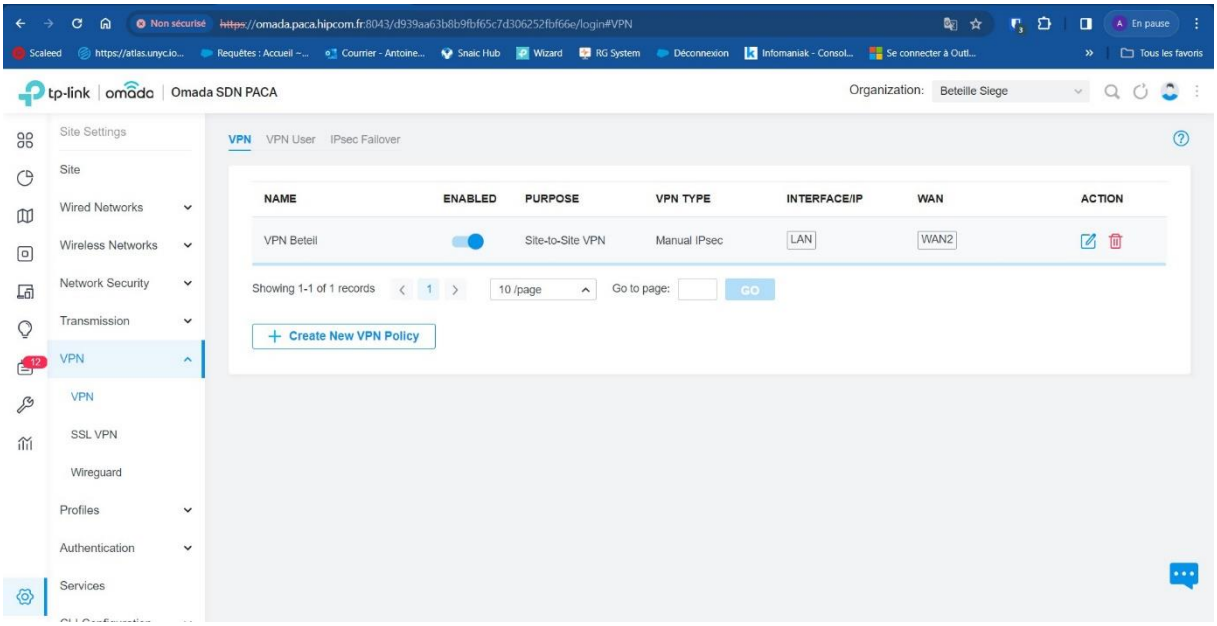
SHA1 AES256

Les autres paramètres restent également par défaut.

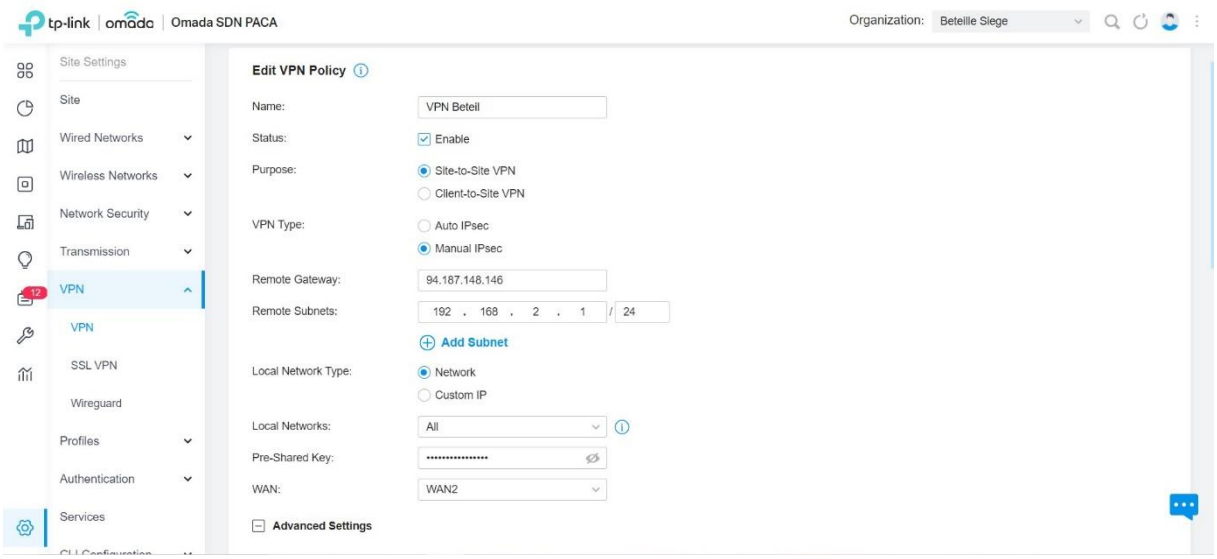


Je me retrouve sur le site de notre client Beteille Siege.

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

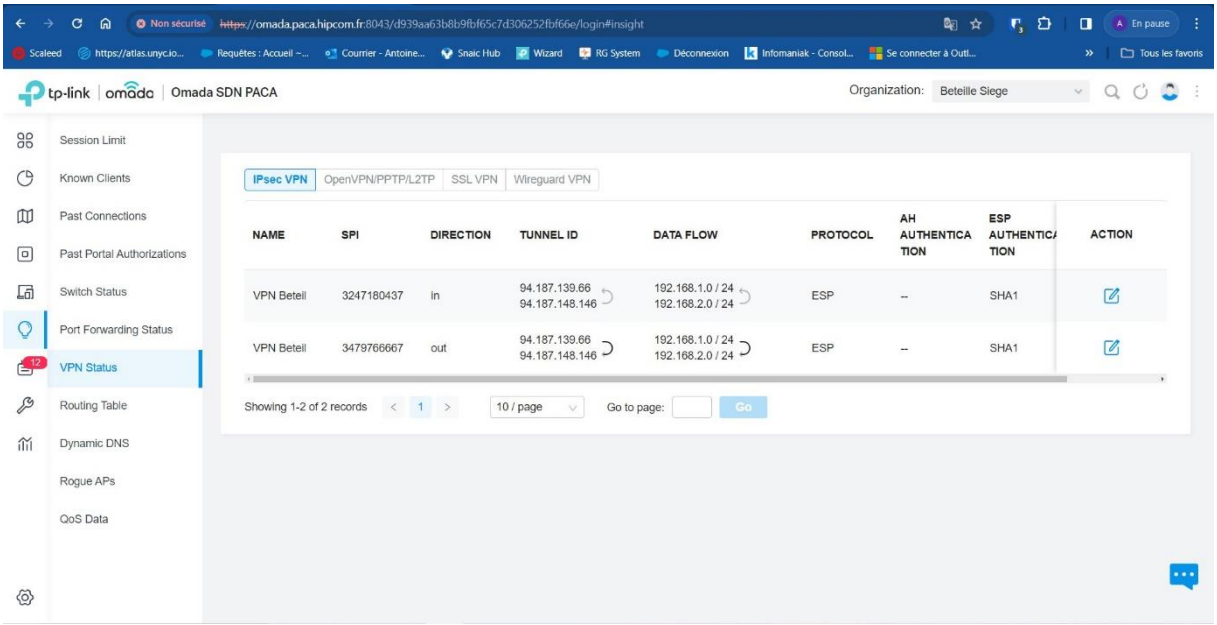


L'important est de bien modifier la passerelle du remote subnets qui est en 192.168.2.1 afin de ne pas être en conflit avec la passerelle du LAN de notre routeur en place qui est ici en 192.168.1.1



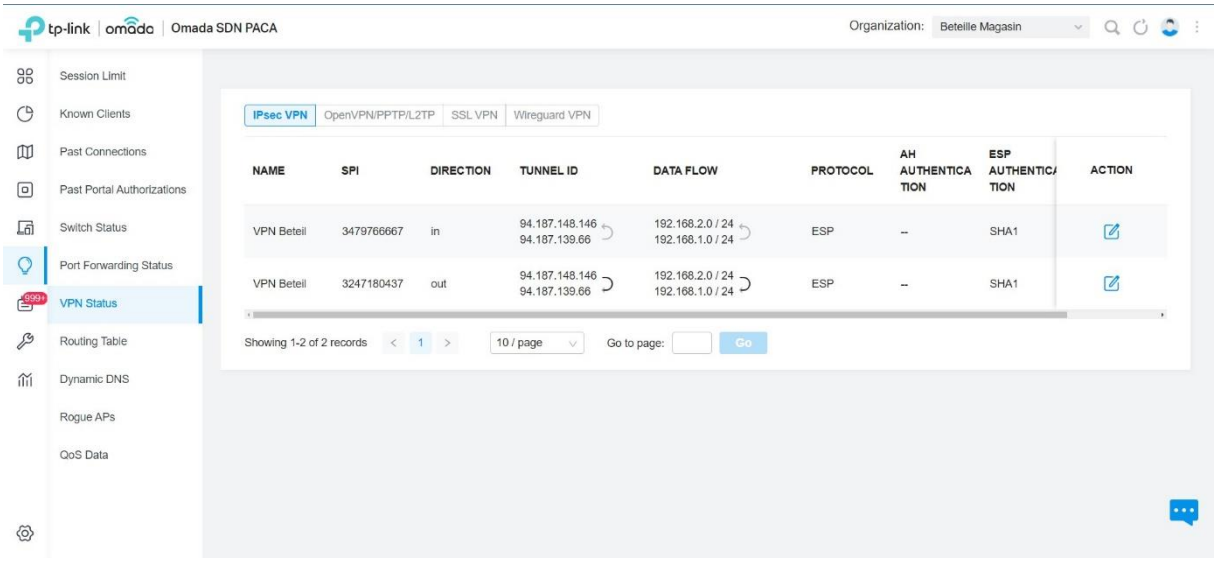
Enfin, j'effectue les tests avec le client à distance, il nous confirme que cela est bien fonctionnel.

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.



Antoine Gargi
Aristee Formation
2022-2024

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.

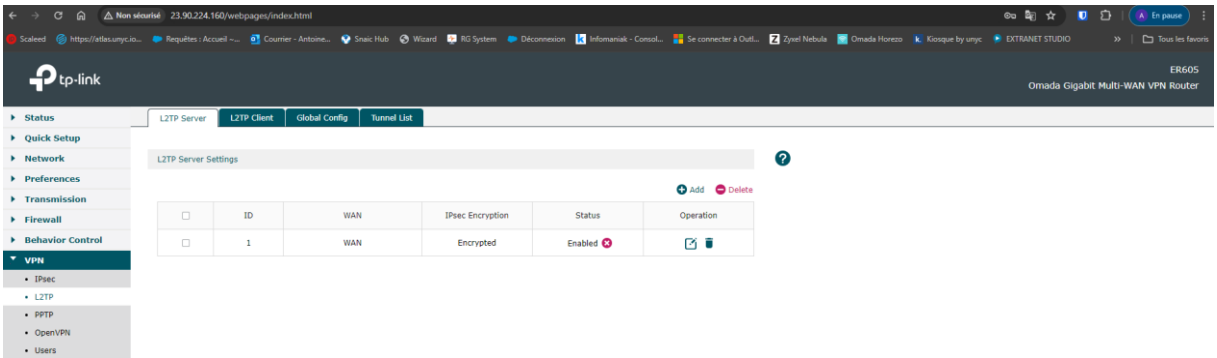
Je me rends dans VPN, L2TP (étant le protocole que nous allons utiliser) et je configure le serveur sur l'interface WAN de notre client.

WAN : WAN

IPSEC Encryption : Encrypted

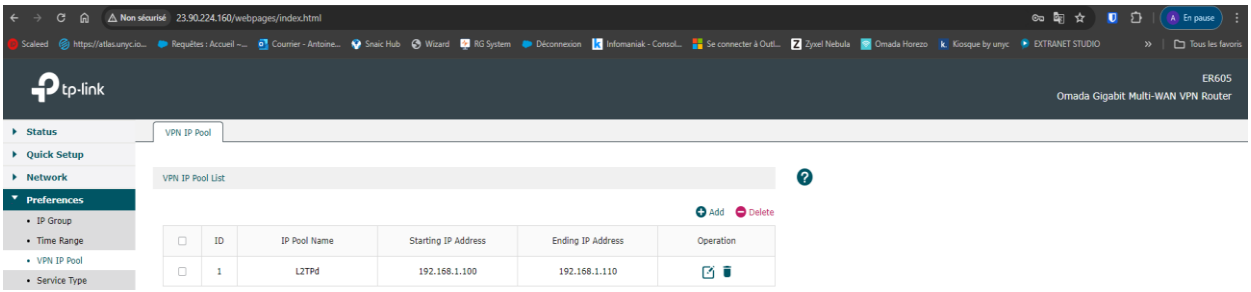
Pre-Shared-key : *****

Status : Enables



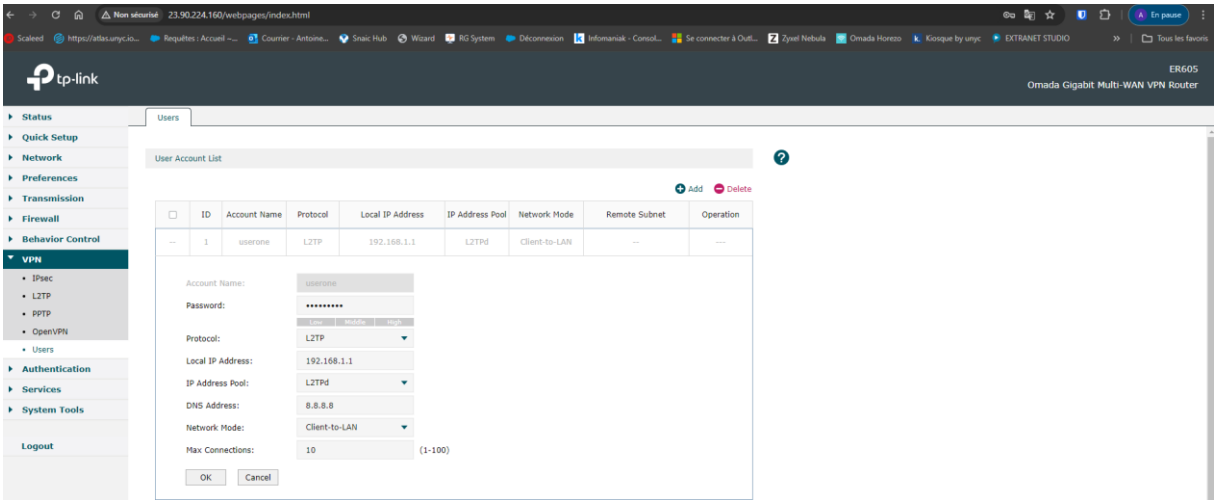
Je me rends ensuite dans *Préférences* puis je crée dans un premier temps un *VPN IP Pool*

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



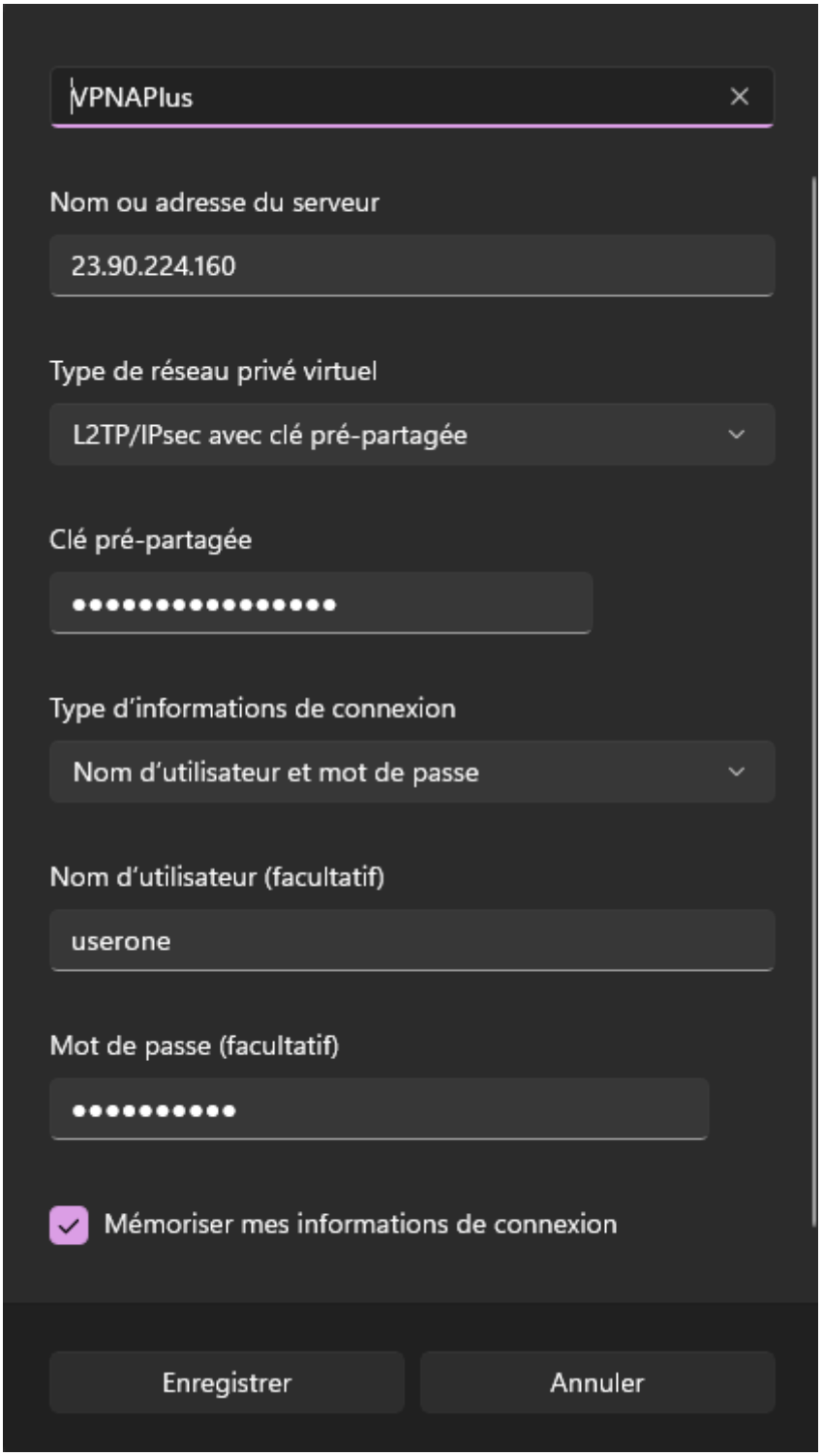
Je me rends ensuite dans *Users* et crée un utilisateur « userone » avec un mot de passe attribué.

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.



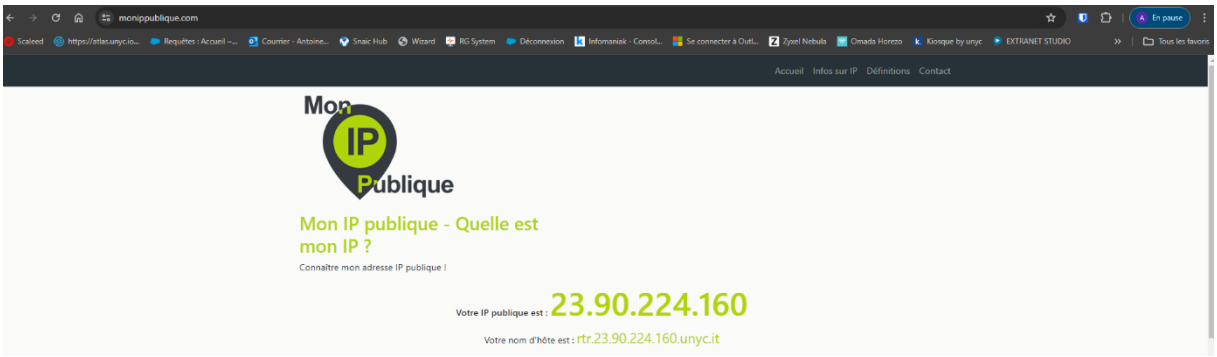
Je peux me rendre sur mon PC dans les paramètres Windows afin de paramétrer le VPN créé :

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).

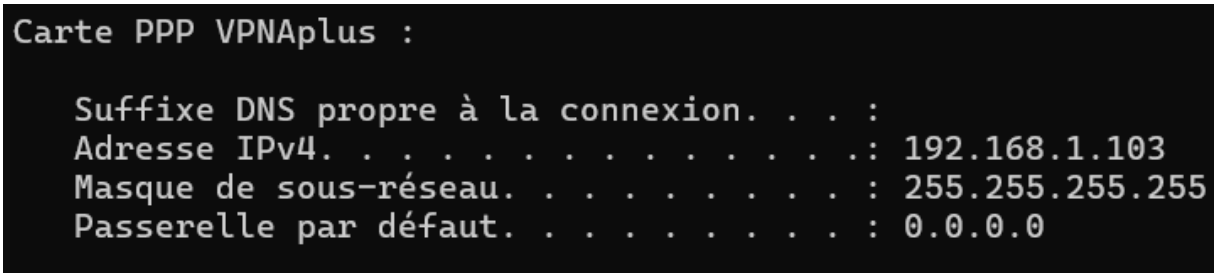


La connexion au VPN doit être fonctionnelle

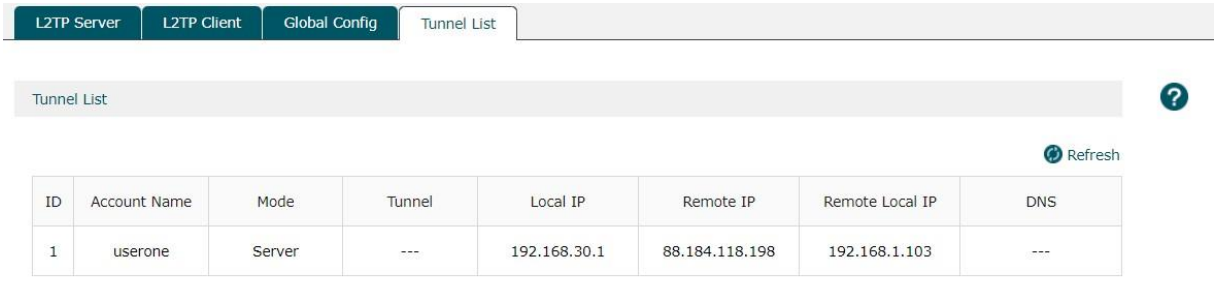
Je vérifie en tapant *monippublique* si l'adresse IP correspond bien à celle de notre client.



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 :



ID	Account Name	Mode	Tunnel	Local IP	Remote IP	Remote Local IP	DNS
1	userone	Server	---	192.168.30.1	88.184.118.198	192.168.1.103	---