

Paramétrage VPN IPSEC

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

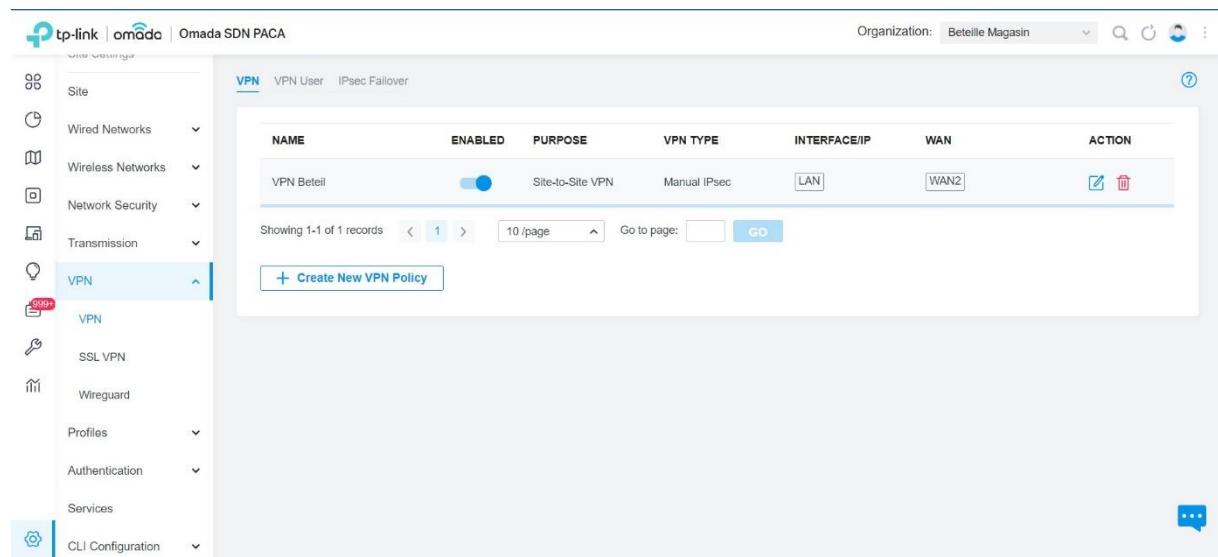
Je suis sur le controller Cloud Omada par TpLink, hébergé sur un de nos serveur Linux.

J'ai ainsi la possibilité de paramétriser 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.



NAME	ENABLED	PURPOSE	VPN TYPE	INTERFACE/IP	WAN	ACTION
VPN Beteille	<input checked="" type="checkbox"/>	Site-to-Site VPN	Manual IPsec	LAN	WAN2	

Voici le paramétrage appliqué :

Choix du VPN Site-to-Site

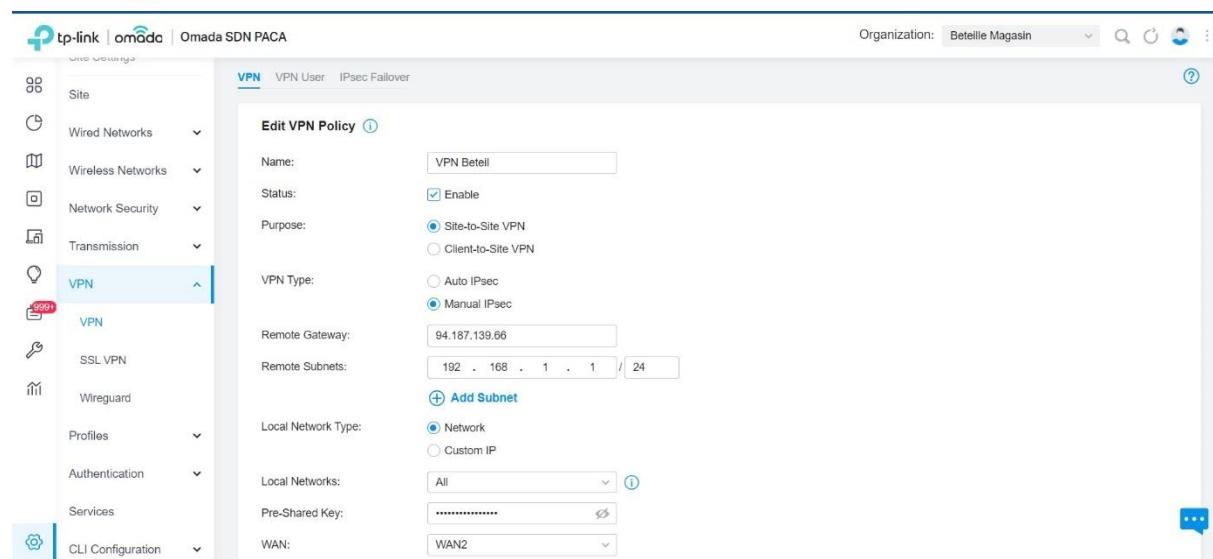
Type IPSEC

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.

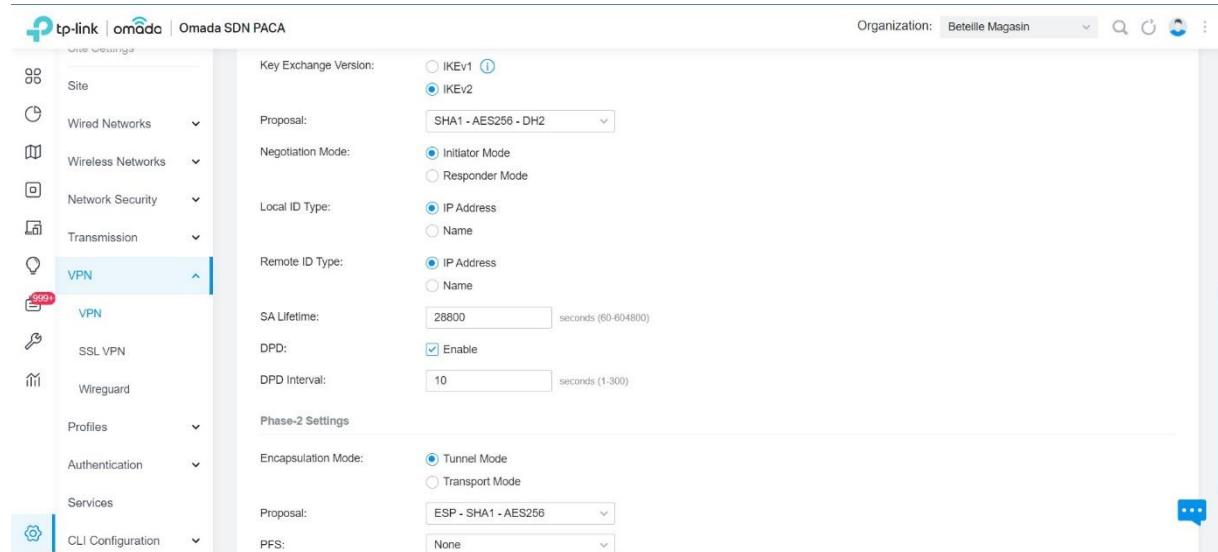


The screenshot shows the 'Edit VPN Policy' configuration for a Site-to-Site VPN. The 'Name' is set to 'VPN Betelle'. The 'Status' is checked as 'Enable'. The 'Purpose' is set to 'Site-to-Site VPN'. The 'VPN Type' is set to 'Manual IPsec'. The 'Remote Gateway' is '94.187.139.66'. The 'Remote Subnets' is '192 . 168 . 1 . 1 / 24'. The 'Local Network Type' is set to 'Network'. The 'Local Networks' dropdown is set to 'All'. The 'Pre-Shared Key' field contains '*****'. The 'WAN' dropdown is set to 'WAN2'. The left sidebar shows the navigation menu with 'VPN' selected.

Le protocole de chiffrement est en Ikev2

SHA1 AES256

Les autres paramètres restent également par défaut.



tp-link | omada | Omada SDN PACA

Organization: Beteille Magasin

Key Exchange Version: IKEv1 IKEv2

Proposal: SHA1 - AES256 - DH2

Negotiation Mode: Initiator Mode Responder Mode

Local ID Type: IP Address Name

Remote ID Type: IP Address Name

SA Lifetime: 28800 seconds (60-604800)

DPD: Enable

DPD Interval: 10 seconds (1-300)

Phase-2 Settings

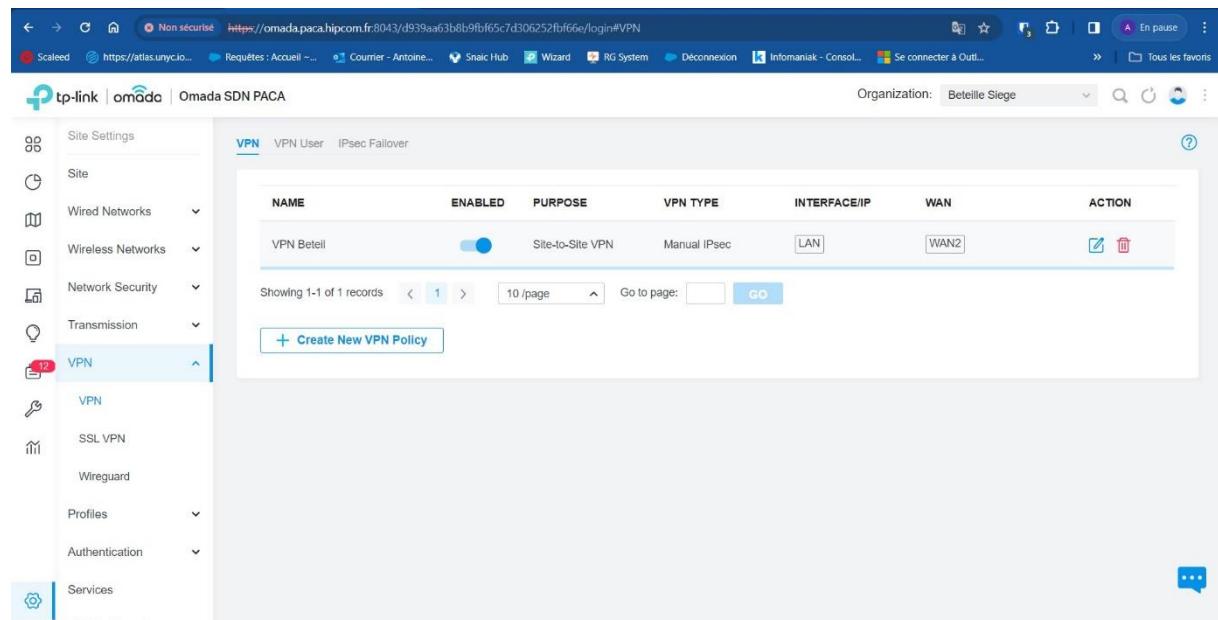
Encapsulation Mode: Tunnel Mode Transport Mode

Proposal: ESP - SHA1 - AES256

PFS: None

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.



tp-link | omada | Omada SDN PACA

Organization: Beteille Siege

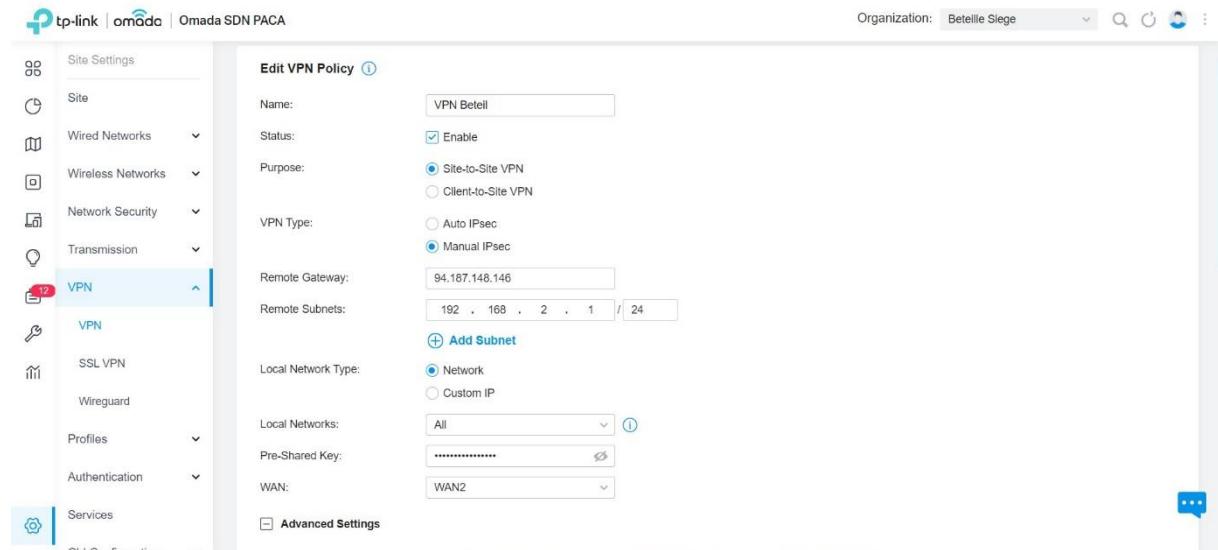
Site Settings **VPN** VPN User IPsec Failover

NAME	ENABLED	PURPOSE	VPN TYPE	INTERFACE/IP	WAN	ACTION
VPN Beteil	<input checked="" type="checkbox"/>	Site-to-Site VPN	Manual IPsec	LAN	WAN2	

Showing 1-1 of 1 records

+ Create New VPN Policy

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



Site Settings

Site

Wired Networks

Wireless Networks

Network Security

Transmission

VPN

SSL VPN

Wireguard

Profiles

Authentication

Services

Organization: Beteille Siege

Name: VPN Beteill

Status: Enable

Purpose: Site-to-Site VPN Client-to-Site VPN

VPN Type: Auto IPsec Manual IPsec

Remote Gateway: 94.187.148.146

Remote Subnets: 192 . 168 . 2 . 1 / 24

Local Network Type: Network Custom IP

Local Networks: All

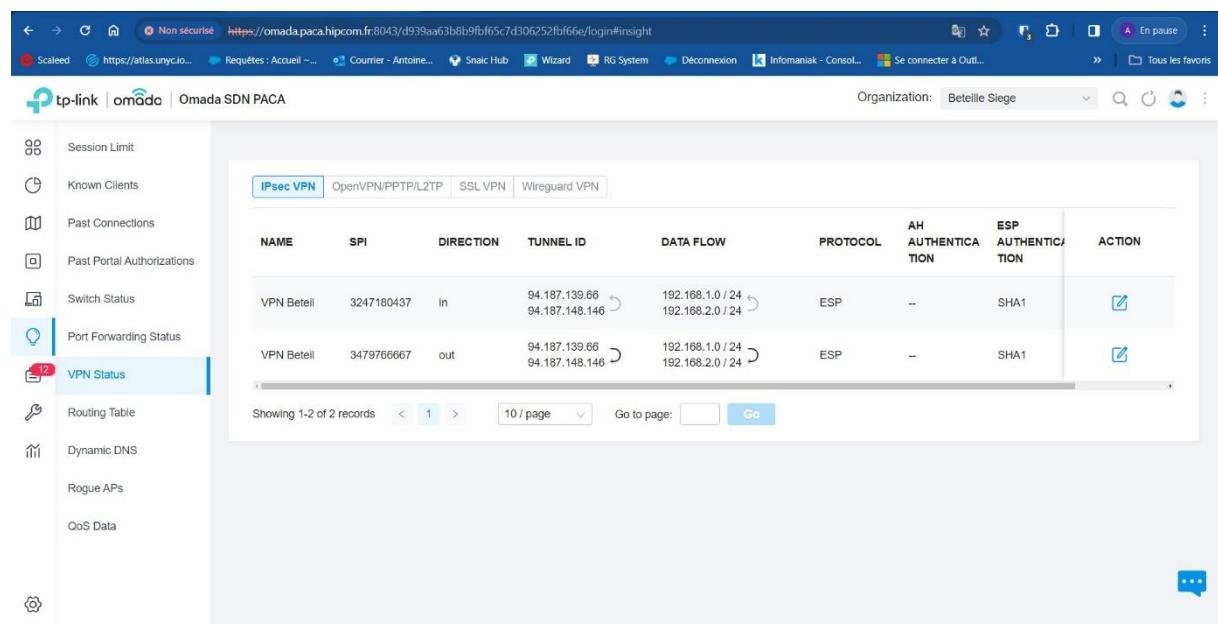
Pre-Shared Key: *****

WAN: WAN2

Advanced Settings

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.



Session Limit

Known Clients

Past Connections

Past Portal Authorizations

Switch Status

Port Forwarding Status

VPN Status

Routing Table

Dynamic DNS

Rogue APs

QoS Data

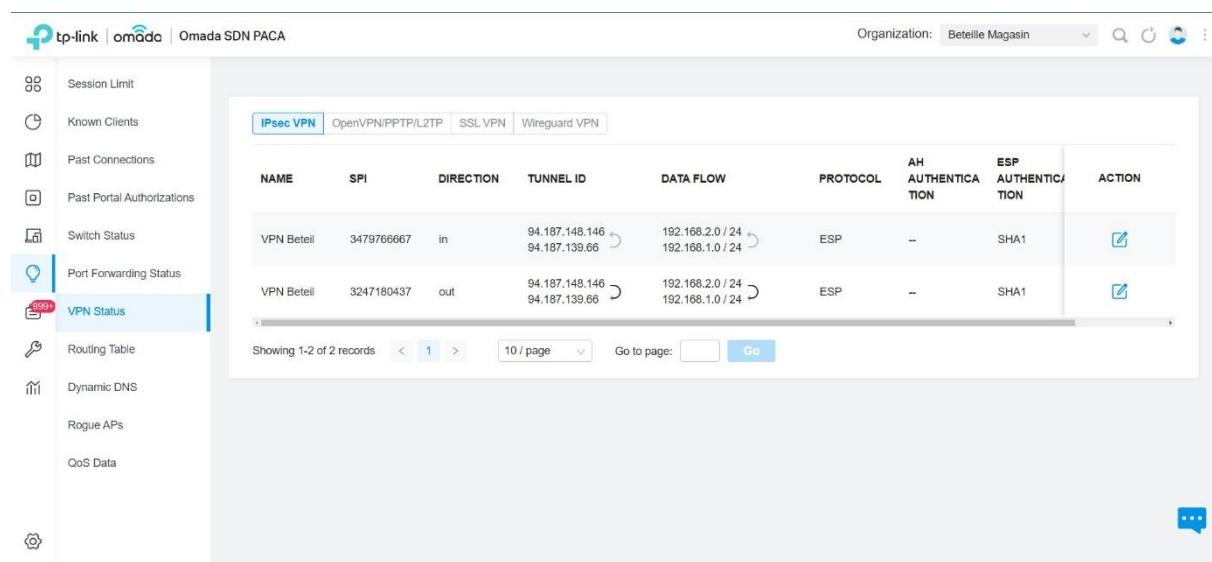
Organization: Beteille Siege

IPsec VPN

NAME	SPI	DIRECTION	TUNNEL ID	DATA FLOW	PROTOCOL	AH AUTHENTICATION	ESP AUTHENTICATION	ACTION
VPN Beteill	3247180437	in	94.187.139.66 94.187.148.146	192.168.1.0 / 24 192.168.2.0 / 24	ESP	--	SHA1	
VPN Beteill	3479766667	out	94.187.139.66 94.187.148.146	192.168.1.0 / 24 192.168.2.0 / 24	ESP	--	SHA1	

Showing 1-2 of 2 records

En se rendant sur status du VPN de Beteille Magasin :



NAME	SPI	DIRECTION	TUNNEL ID	DATA FLOW	PROTOCOL	AH AUTHENTICATION	ESP AUTHENTICATION	ACTION
VPN Beteil	3479766667	in	94.187.148.146	192.168.2.0/24 192.168.1.0/24	ESP	--	SHA1	
VPN Beteil	3247180437	out	94.187.148.146	192.168.2.0/24 192.168.1.0/24	ESP	--	SHA1	

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.

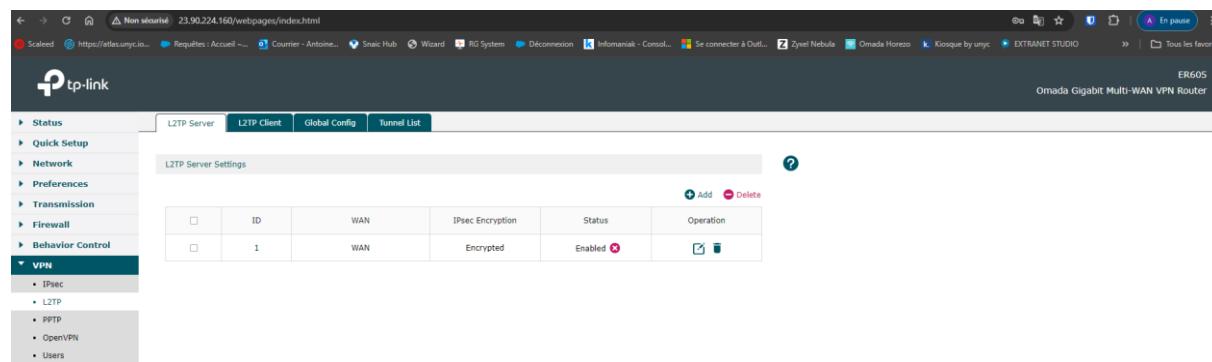
Je me rends dans VPN, L2TP (étant le protocole que nous allons utiliser) et je configure le serveur sur l'interface WAN de notre client.

WAN : WAN

IPSEC Encryption : Encrypted

Pre-Shared-key : *****

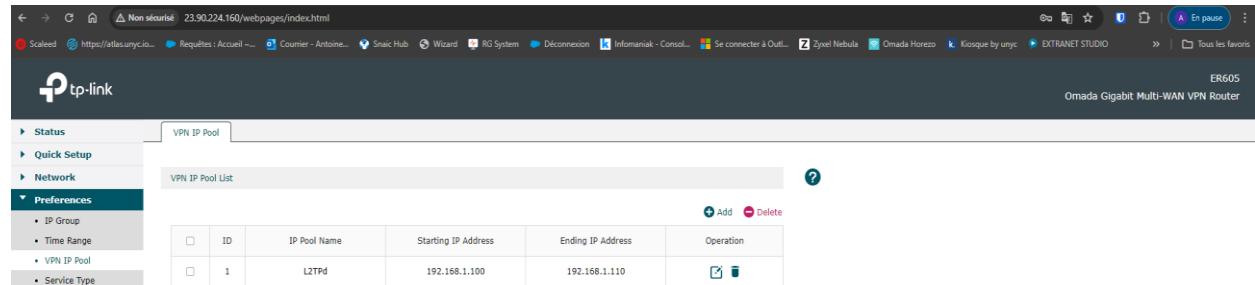
Status : Enables



ID	WAN	IPsec Encryption	Status	Operation
1	WAN	Encrypted	Enabled	 

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

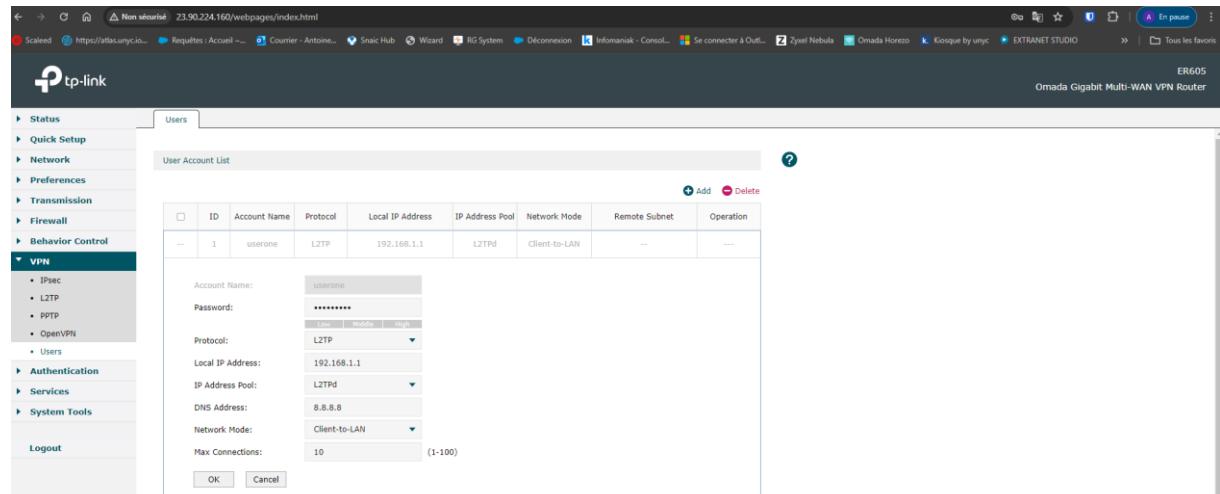
Je nomme l'IP Pool, puis choisi un début d'adresse en 192.168.1.100 jusqu'à 192.168.1.110



ID	IP Pool Name	Starting IP Address	Ending IP Address	Operation
1	L2TPd	192.168.1.100	192.168.1.110	

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

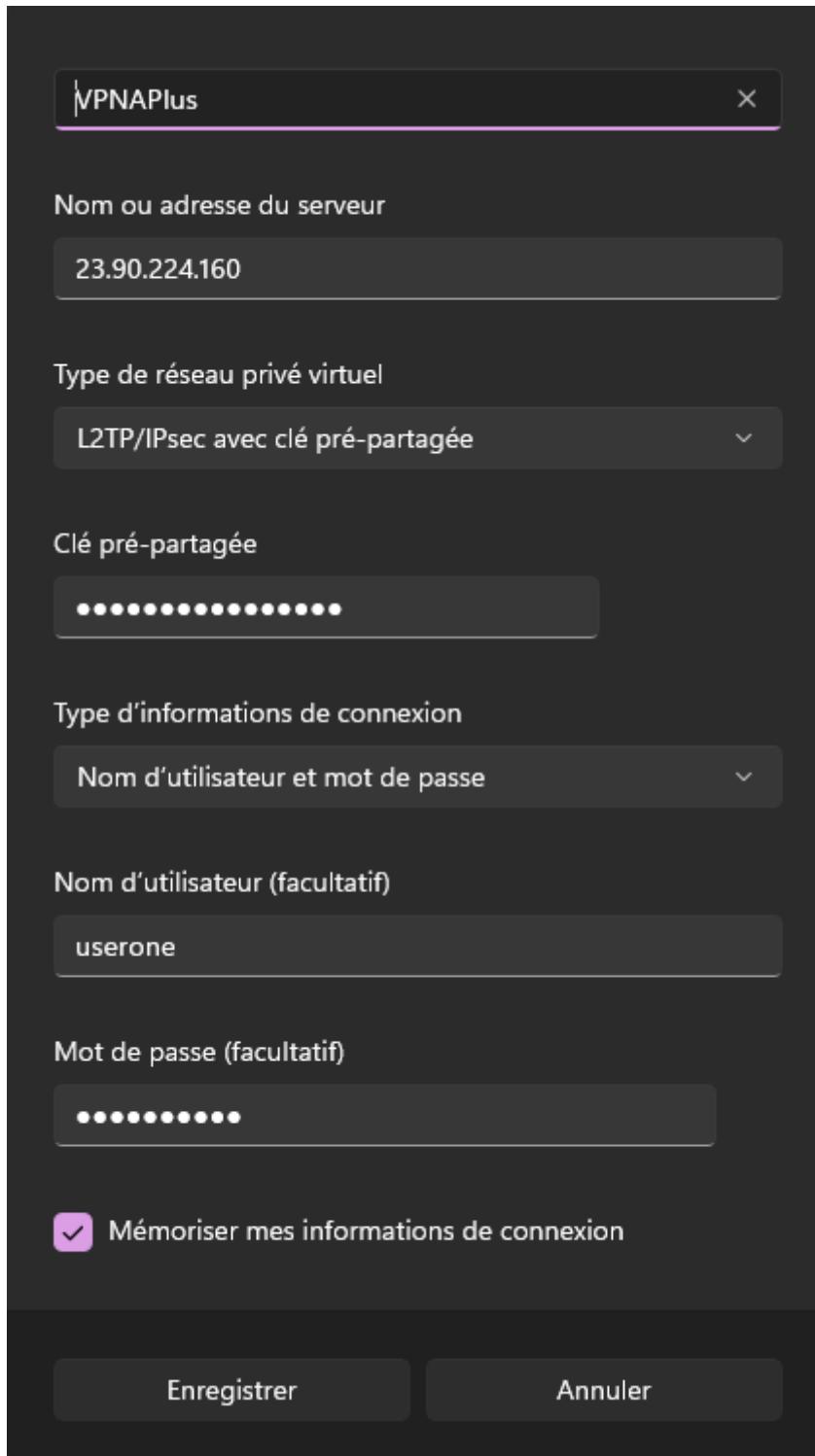
Je choisis le protocole L2TP, j'indique l'adresse IP de la passerelle du LAN (192.168.1.1), j'associe le Pool VPN précédemment créé, indique un DNS en (8.8.8.8) et choisis un VPN Type Client-to-LAN.



ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operation
1	userone	L2TP	192.168.1.1	L2TPd	Client-to-LAN	—	—

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

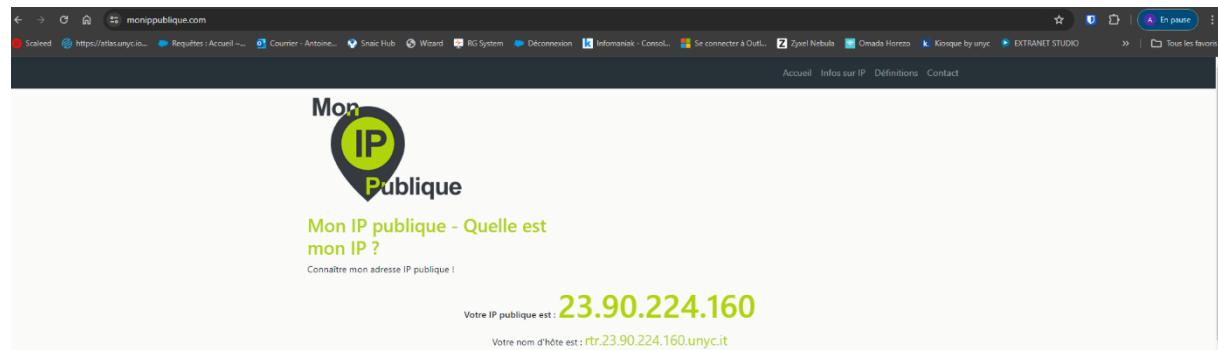
J'entre ici le nom du VPN (non obligatoire), l'adresse IP publique sur lequel le serveur est configuré, le type de serveur VPN (L2TP), la clé pré partagée configurée en amont et le nom de l'utilisateur (non obligatoire ici).



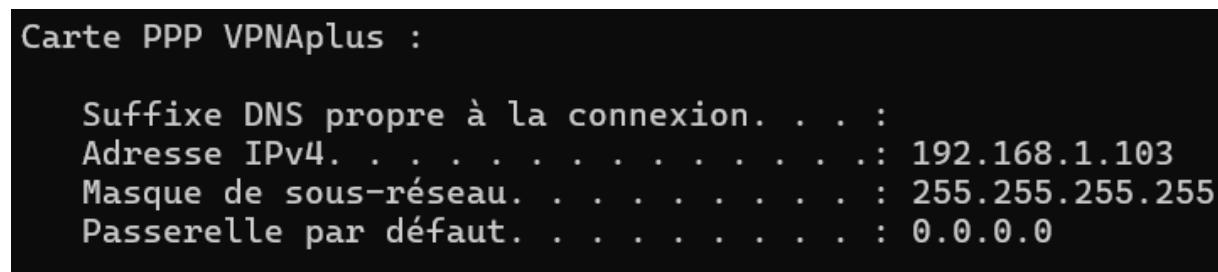
La connexion au VPN doit être fonctionnelle



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 :

