ADRAR FORMATION

Mis en place d'un VPN SLL Nomade

MARAVAL Liam
07/10/2024

Ce document sera décomposé en plusieurs chapitres :

1. Contexte : Définition des besoins ainsi que le choix des solutions en réponse à la demande client
2. Configuration technique : Procédure technique de mise en place des solutions
3. Conclusion : Conclusion du projet

Table des matières

1. Contexte

1.1 Demandes du client

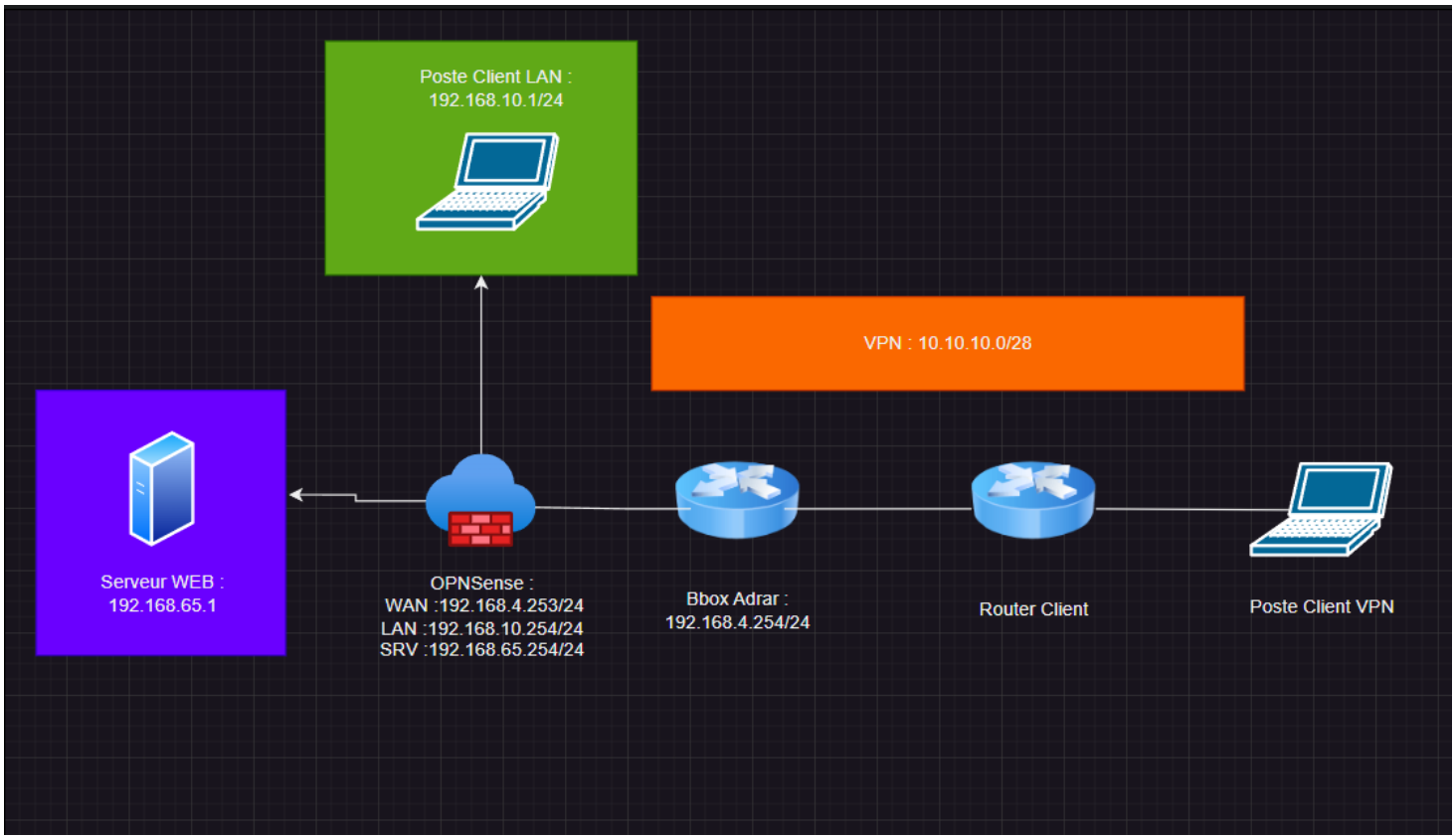
Nous sommes contactés par l'ADRAR afin de mettre en place un VPN SSL nomade.
Les télétravailleurs devant accéder au serveur de fichier en utilisant le bureau à distance Windows.

Voici l'infrastructure en place actuellement :

- Une sortie internet via une Bbox en 192.168.4.254/24
- Un serveur de fichier
- Des postes utilisateurs

1.2 Evolution de l'infrastructure

Pour mieux comprendre la mise en place de la nouvelle infrastructure, veuillez-vous référer au nouveau schéma effectué :



Afin de répondre au mieux à la demande, nous allons tout d'abord découper notre réseau global en 4 réseau différents :

- Un LAN pour les postes utilisateurs en 192.168.10.0/24
- Un LAN dédié aux serveurs en 192.168.65.0/24
- Un WAN qui restera sur le réseau historique en 192.168.4.0/24
- Un réseau virtuel pour notre tunnel VPN en 10.10.10.0/28

En effet, les serveurs étant initialement dans le LAN utilisateurs, nous avons ajouté un réseau dédié pour ceux-ci.
Cela est plus cohérent et sécurisé de dissocier les usages via des réseaux différents.

Afin de sécuriser les différents flux nous allons mettre en place un pare feu, nommé **« FW1 »,** qui portera également le serveur VPN.
Il sera composé de 3 cartes réseaux :

- WAN : 192.168.4.253/24
- LAN : 192.168.10.254/24
- SRV : 192.168.65.254/24

C'est lui qui assura le routage en interne ainsi que vers la sortie internet.

Le **« FW1 »** étant situé derrière la Bbox nous allons devoir configurer une règle NAT pour le trafic VPN.
Celle-ci permettra de rediriger toutes les demandes de connexion VPN vers l'IP publique de notre BBox sur l'interface WAN de notre pare feu :

IP Cible	Port Cible	IP de redirection	Port de redirection
IP Public Bbox	Port VPN : UDP 5103	Interface WAN Opnsense : 192.168.4.253/24	Port VPN : UDP 5103

1.3 Choix de la solution

Le pare feu choisi pour notre solution est un « **Provya pro-Middle** » disposant de :

- Un disque 120Go
- 8Go de RAM
- CPU 2 Core 4 Threads
- 4 ports réseau Gbps

Le choix de l'OS c'est porté sur **« OpnSense »** pour plusieurs raisons :

- ✓ Solution open source
- ✓ Mis à jour de sécurité régulières
- ✓ Facilité d'administration via une interface graphique complète et simple
- ✓ Documentation en ligne
- ✓ Communauté et support commercial
- ✓ Nombreuses fonctionnalités disponibles (Proxy, Pare-feu, VPN IPSEC et SSL, Filtrage de flux, détection d'intrusion, MFA, Failover, Load Balancing Multi-WAN…)

Ce pare feu nous permettra de sécuriser les flux dans le réseau interne et via le VPN, le tout à un prix abordable.
Cet équipement a été pensé pour évoluer facilement.
En effet, en cas de développement au sein de l'ADRAR, nous pourrons mettre en place des solutions comme :

- Configuration de VLAN
- Ajout d'une DMZ si des serveurs doivent être exposés sur internet
- Optimisation et sécurisation des flux web via un proxy ect…

En ce qui concerne le serveur VPN, nous avons opté pour **« OpenVPN »** en se basant sur les critères suivants :

- Solution Open source
- Large compatibilité avec les OS (Windows, MacOS, Linux, Android, IOS)
- Flexible et personnalisable selon les besoins
- Algorithme de chiffrement robuste garantissant la sécurité des données
- Authentification des pairs avancée via des certificats SSL

1.4 Sécurisation des accès

En nous appuyant sur les recommandations de l'ANSSI, nous allons utiliser les paramètres de sécurité suivants pour la configuration des certificats et du serveur VPN :

- Chiffrement symétrique : AES 256
- Chiffrement asymétrique : RSA 2048
- Hachage : SHA 256

En ce qui concerne l'authentification de nos utilisateurs, nous allons utiliser :

- Des certificats SSL assignés à nos utilisateurs
- Un login et mot de passe
- Un MFA que l'utilisateur devra configurer sur son téléphone.

Voici également un tableau récapitulatif des règles de pare feu qui seront mis en place :

LAN				
Protocol	IP Source	Port source	IP Destination	Port Destination
TCP	192.168.10.0/24	any	any	443
TCP	192.168.10.0/24	Any	Any	80
UDP	192.168.10.0/24	any	192.168.10.254/32	53
TCP	192.168.10.0/24	Any	192.168.65.1/32	3389

WAN				
Protocol	IP Source	Port source	IP Destination	Port Destination
UDP	any	any	192.168.4.253/32	5103

SRV				
Protocol	IP Source	Port source	IP Destination	Port Destination
UDP	192.168.65.0/24	Any	192.168.65.254/32	53

OpnVPN				
Protocol	IP Source	Port source	IP Destination	Port Destination
TCP	10.10.10.0/28	Any	192.168.65.1/32	3389
UDP	10.10.10.0/28	Any	192.168.65.254/32	53

1.5 Plan général de configuration

Voici le déroulement du déploiement de la solution :

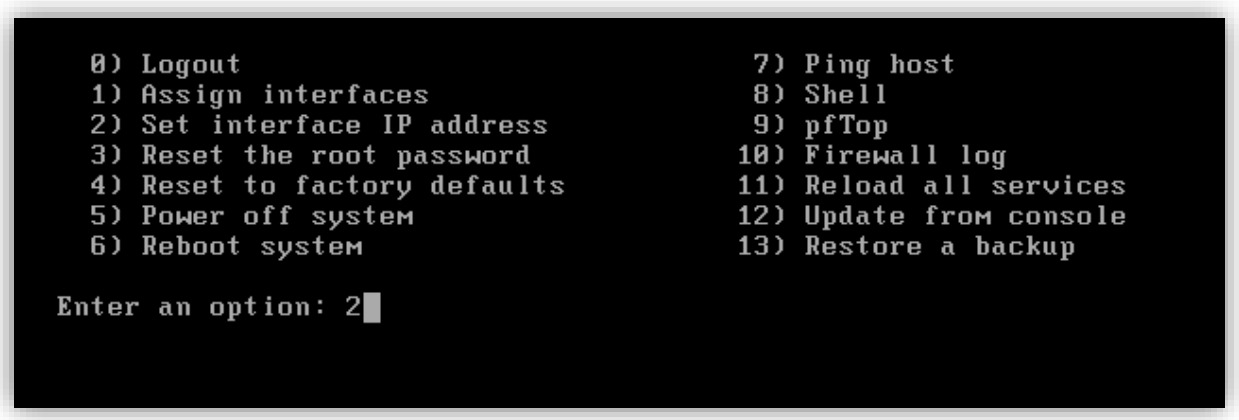
- Installation et configuration de base du Firewall (Nom, IP des interfaces, Compte d'administration ect…)
- Création d'une autorité de certification locale pour générer les certificats
- Création du serveur TOTP
- Création d'un utilisateur avec génération de son certificat SSL et MFA
- Génération du certificat SSL pout le serveur VPN
- Configuration du serveur VPN SSL
- Test de validation sur le LAN
- Test de validation externe via le WAN

2. Configuration technique

2.1 Installation et paramétrage de l'Opnsense

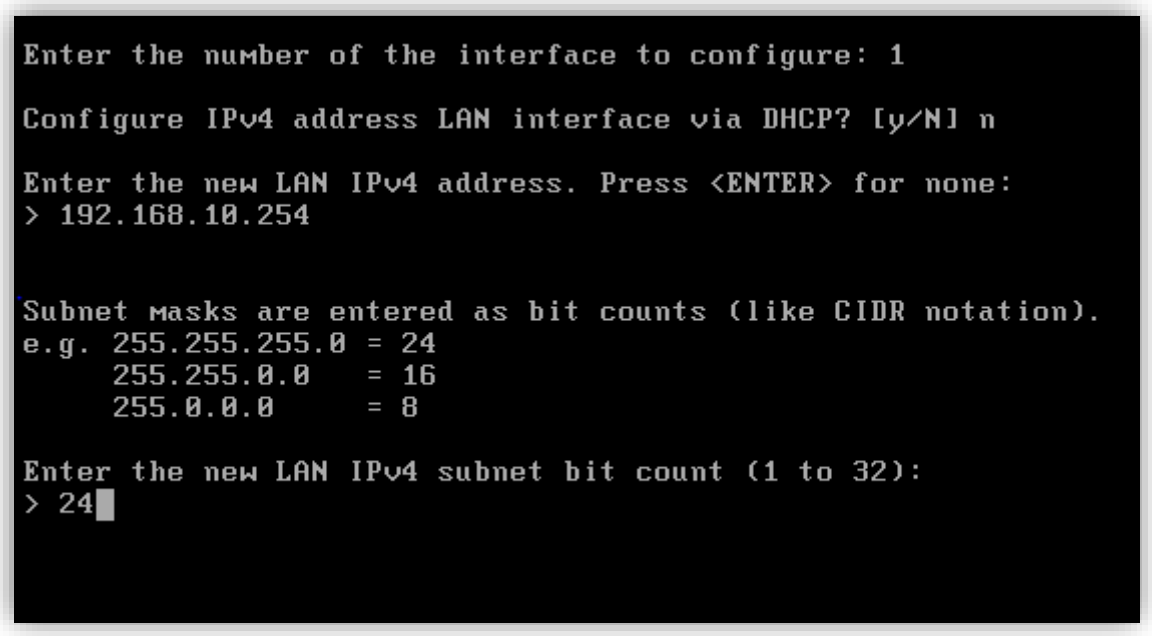
Concernant l'installation d'Opnsense, merci de vous référer à la documentation : https://www.it-connect.fr/tuto-installer-et-configurer-opnsense/#IV_Configuration_cible

Une fois celle-ci effectuée, nous commençons par attribuer les IP des interfaces via le terminal Opnsense.
Nous sélectionnons l'option 2 **« Set Interface IP address »** (Nous ne mettrons la procédure que pour une interface, les étapes seront identiques pour les autres) :



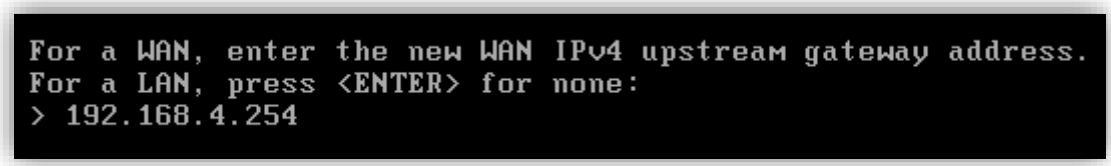
Nous sélectionnons l'interface à configurer **« 1 – LAN »** :

Plusieurs options vont être proposées, la 1ere sera de configurer l'interface en DHCP, que nous ne choisirons pas.
Ensuite, nous renseignons l'IP statique avec son masque :

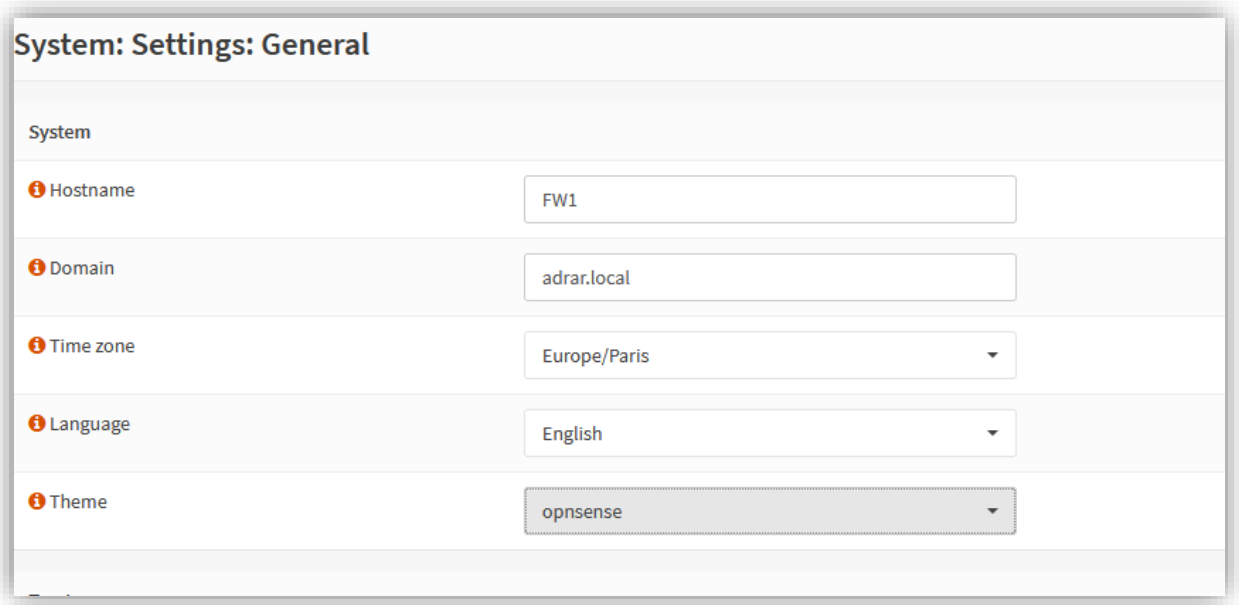


Le reste des options ne seront pas à configurer comme le serveur DHCP, la Gateway ainsi que l'attribution d'Ipv6 qui ne seront pas utilisées dans notre cas.

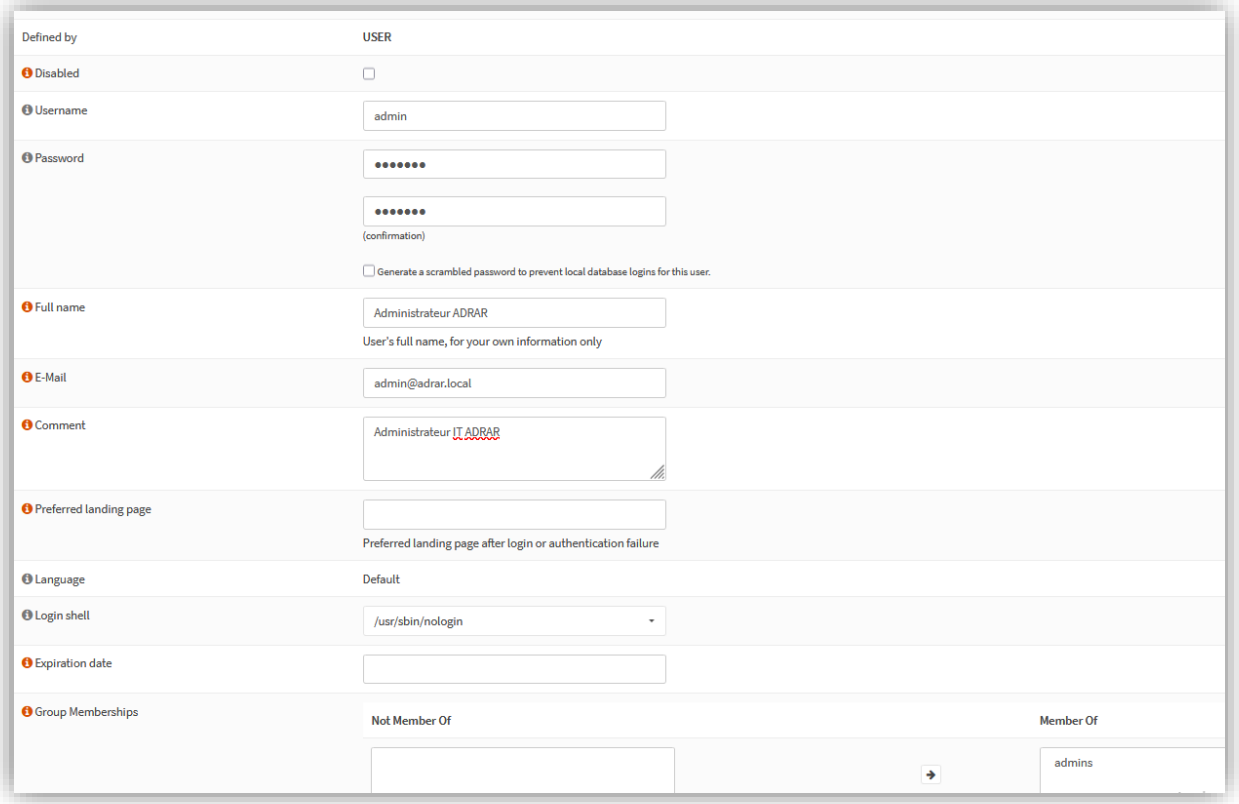
Nous allons répéter les mêmes étapes pour fixer les IP de nos interfaces **WAN** et **SRV**.
Seul changement pour le **WAN** sur lequel nous renseignerons la Gateway qui sera notre Bbox :



Nous pouvons désormais nous rendre sur l'interface graphique (IP du LAN) afin de configurer le nom, le domaine ect… :

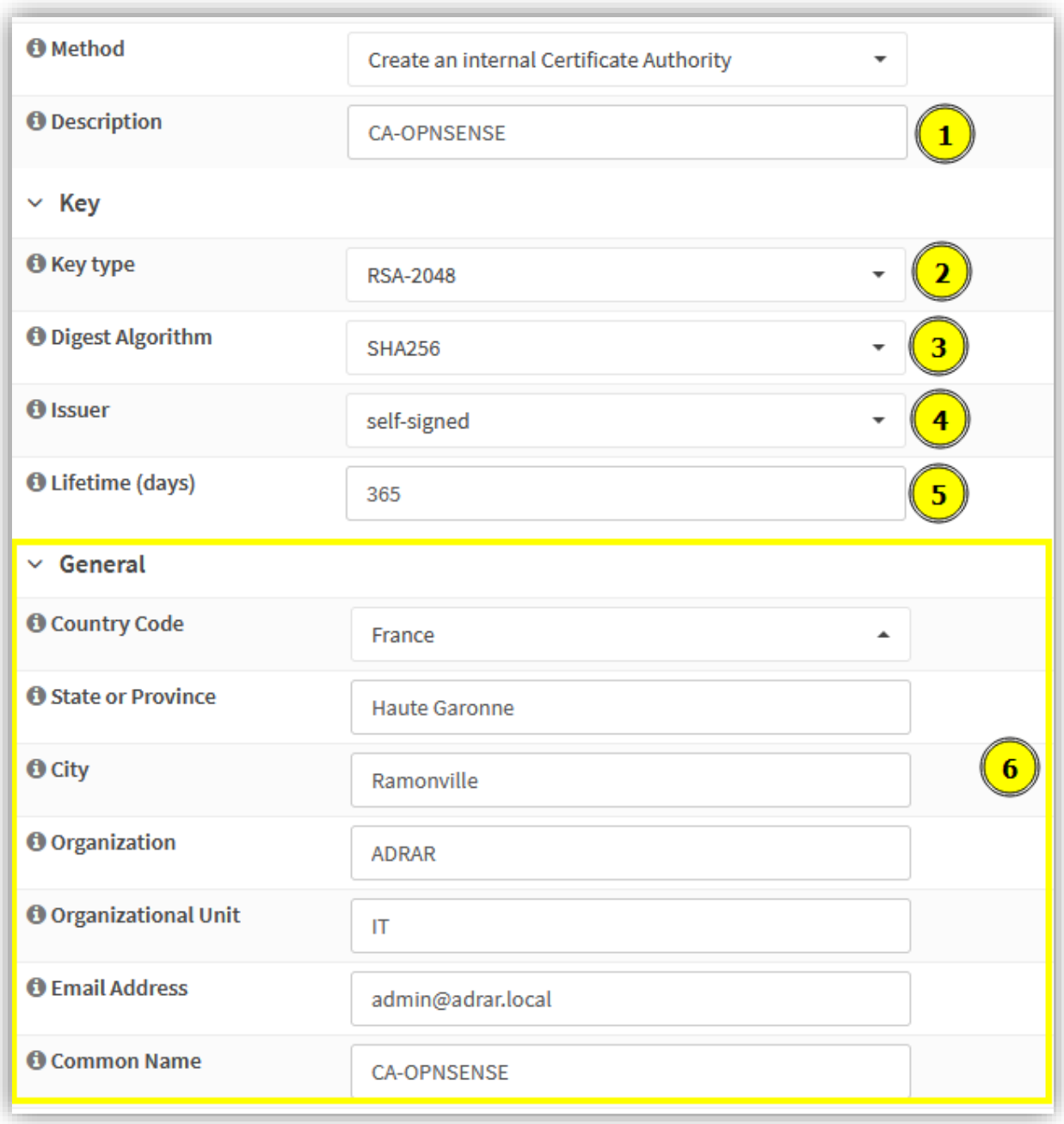


Une fois cela fait, nous allons créer un compte d'administration **« admin »** afin de ne pas utiliser le compte **« root »** par mesure de sécurité :



2.2 Mis en place de l'autorité de certification

Nous allons maintenant nous rendre dans le menu **« System –> Trust -> Authorities »** afin de créer notre autorité de certification pour délivrer nos certificats :

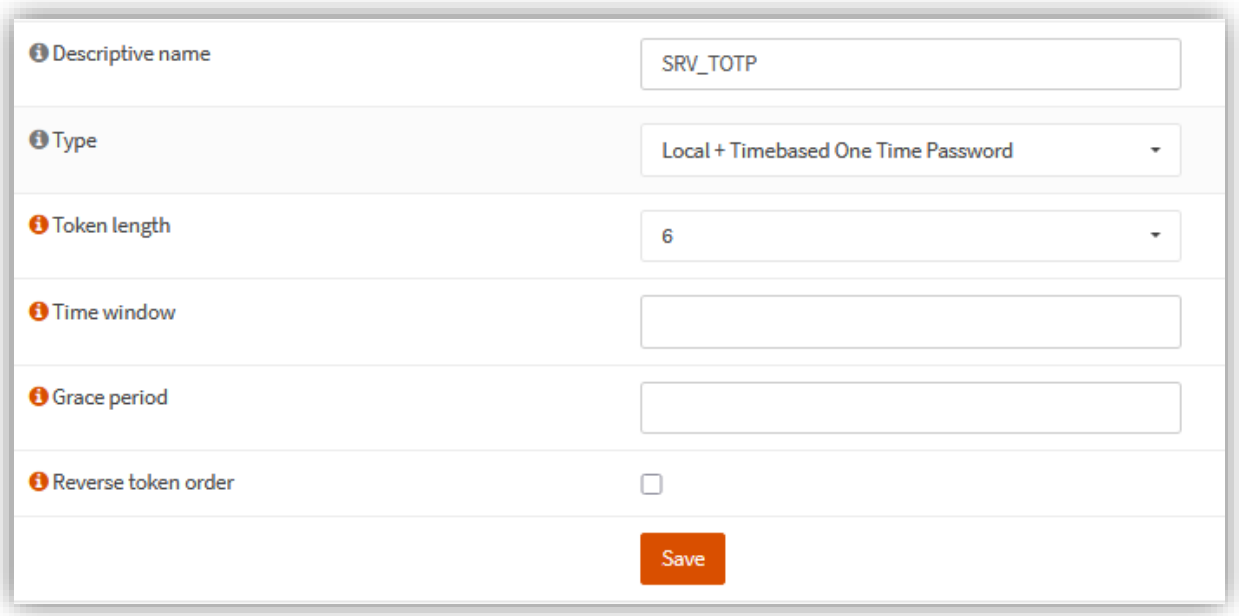


1. Description de l'autorité de certification
2. Génération des pairs de clefs via RSA 2048
3. Hachage via SHA256
4. Autorité auto signée
5. Durée de validité d'un certificat
6. Renseignement général à l'entreprise

2.3 Mis en place du serveur TOTP

Nous allons configurer notre serveur TOTP afin d'authentifier les utilisateurs locaux avec un login, mot de passe ainsi qu'un jeton à installer sur « **Google Authenticator ».**
La longueur de celui-ci sera de 6 chiffres.
Afin de se connecter, l'utilisateur devra renseigner **son jeton puis son mot de passe** dans cet ordre précis.

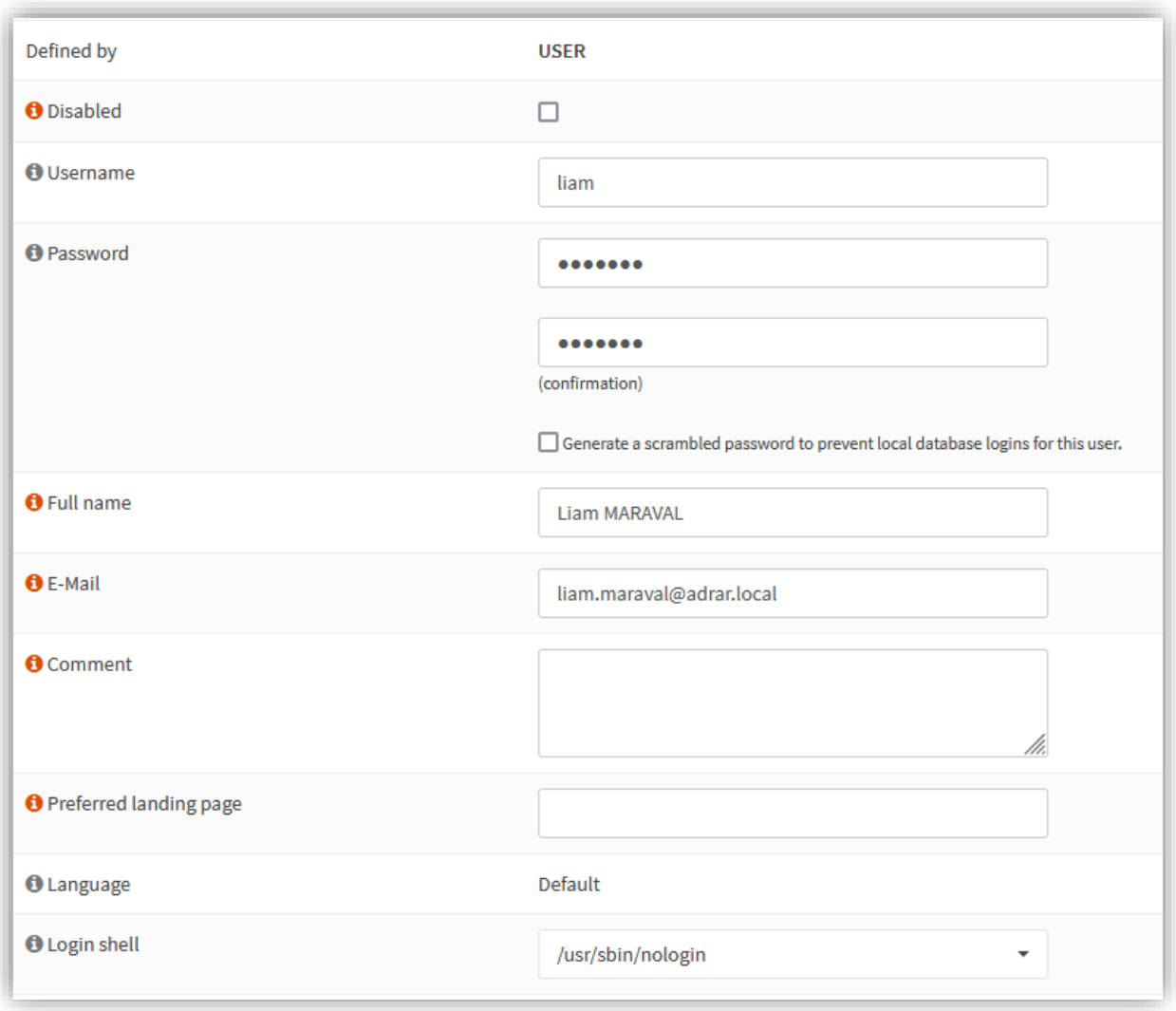
Pour configurer celui-ci, nous allons dans **« System -> Access -> Servers »** et nous cliquons sur **« Add ».**
Nous renseignons maintenant les différents champs :



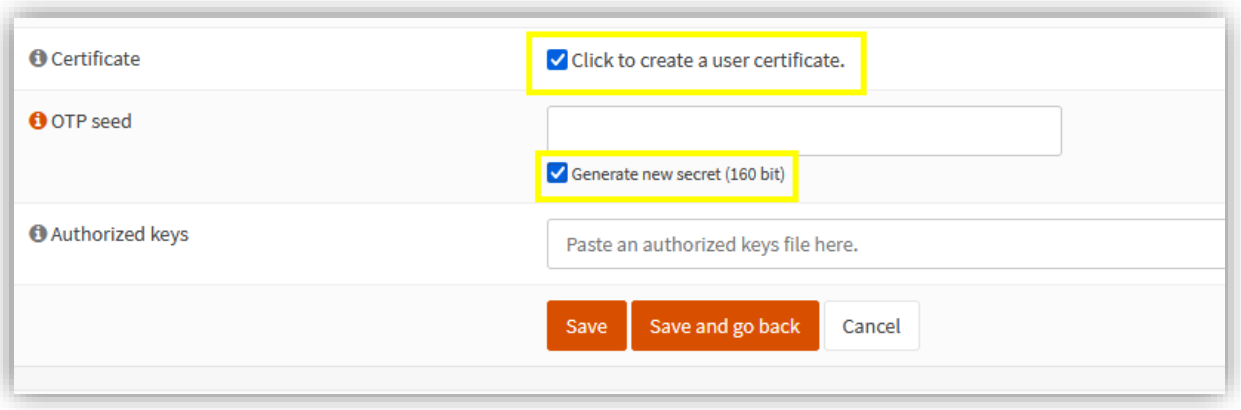
2.4 Création d'un utilisateur local avec certificat

Nous allons créer un utilisateur local pour notre VPN nomade.

Nous renseignons les informations basiques, nom, mot de passe, mail ect...

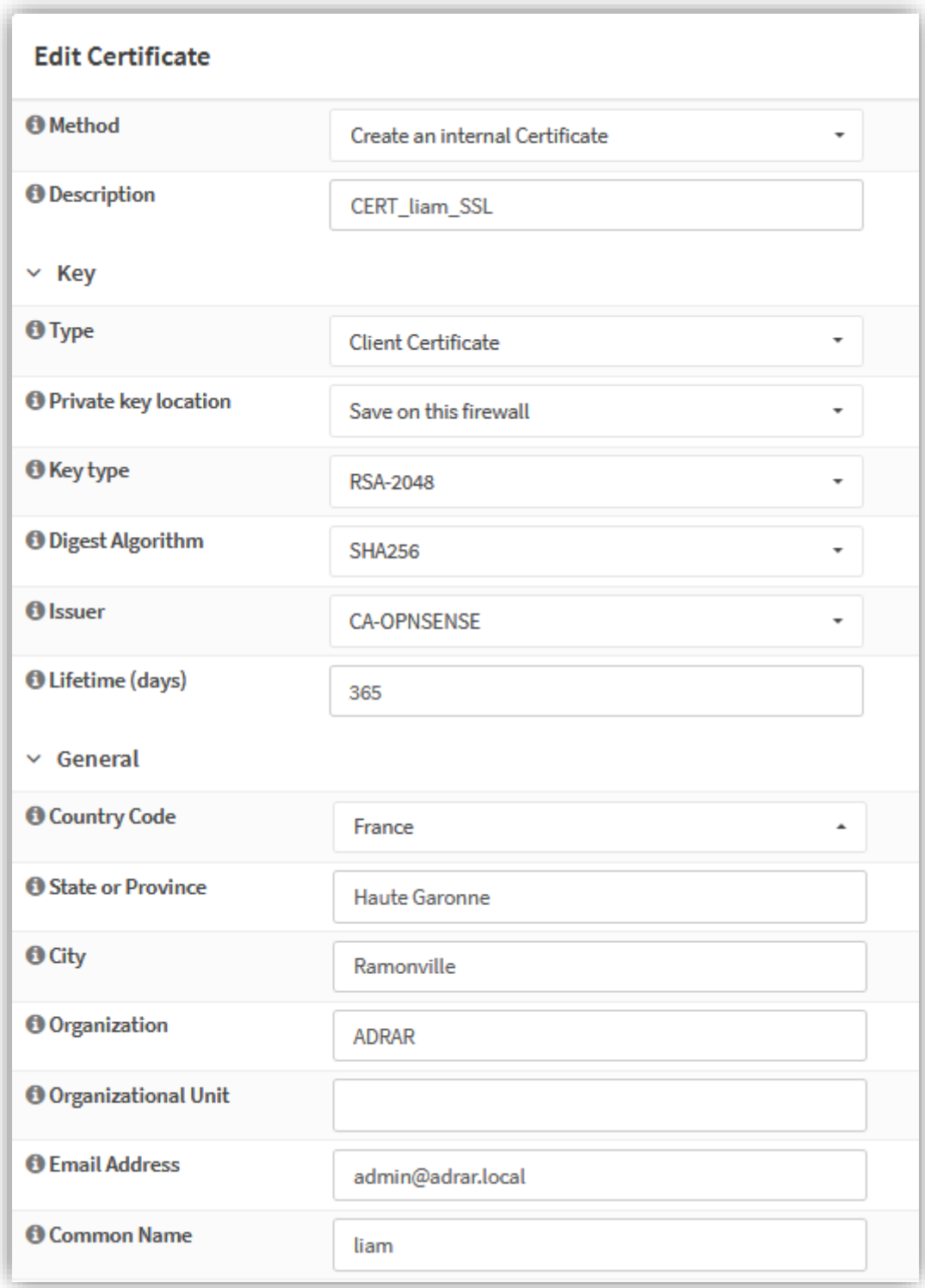


Deux cases vont être à cocher **« Certifcate »** ainsi que **« OTP Seed »**, celles-ci vont servir à créer le certificat pour l'utilisateur et à générer sa graine OTP pour le MFA :

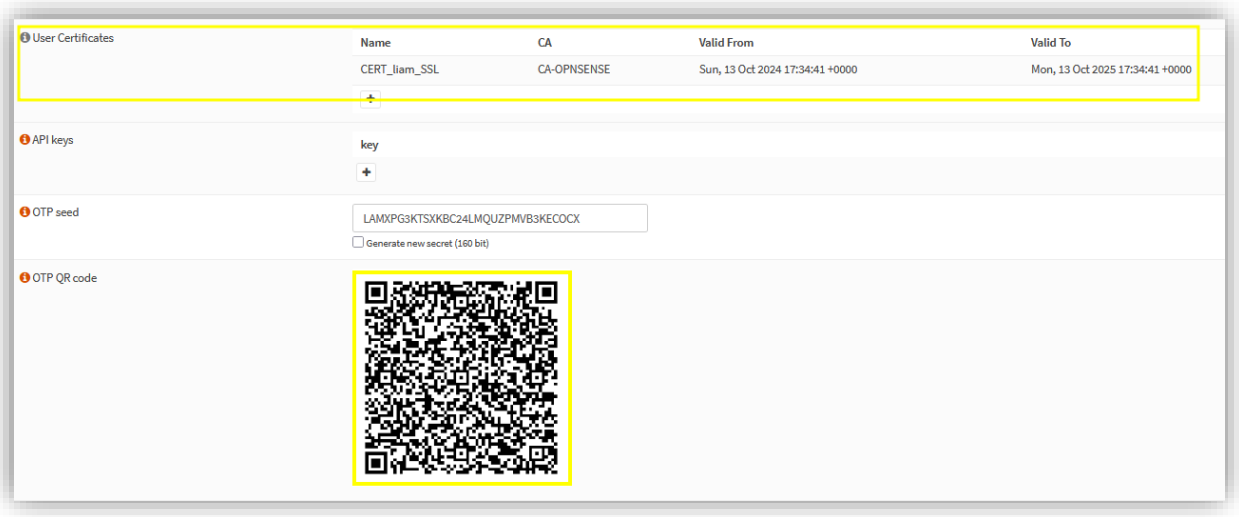


Nous cliquons sur **« Save »** et nous sommes directement redirigés sur la page de création de certificat pour l'utilisateur.

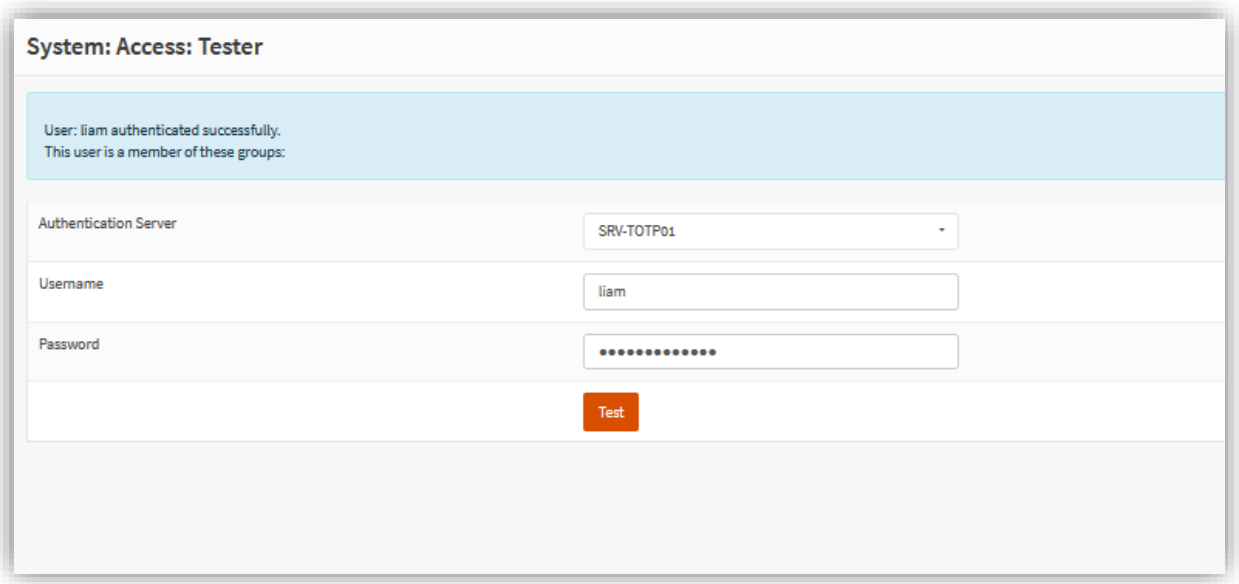
Nous renseignons le champ **« Description »** et en sélectionnant l'autorité de certification, précédemment créée, les autres champs vont se pré remplir.
Le **« Common Name »** est à laisser par défaut afin d'assigner le certificat au bon utilisateur.



Une fois cela fait, nous retournons sur la page de l'utilisateur.
Nous cliquons sur **« Click to unhide »** dans le champ **« OTP Seed ».** Un QR code apparait, que l'utilisateur devra scanner via son application **« Google Authenticator »** pour finaliser son MFA.
Nous voyons également le certificat assigné.



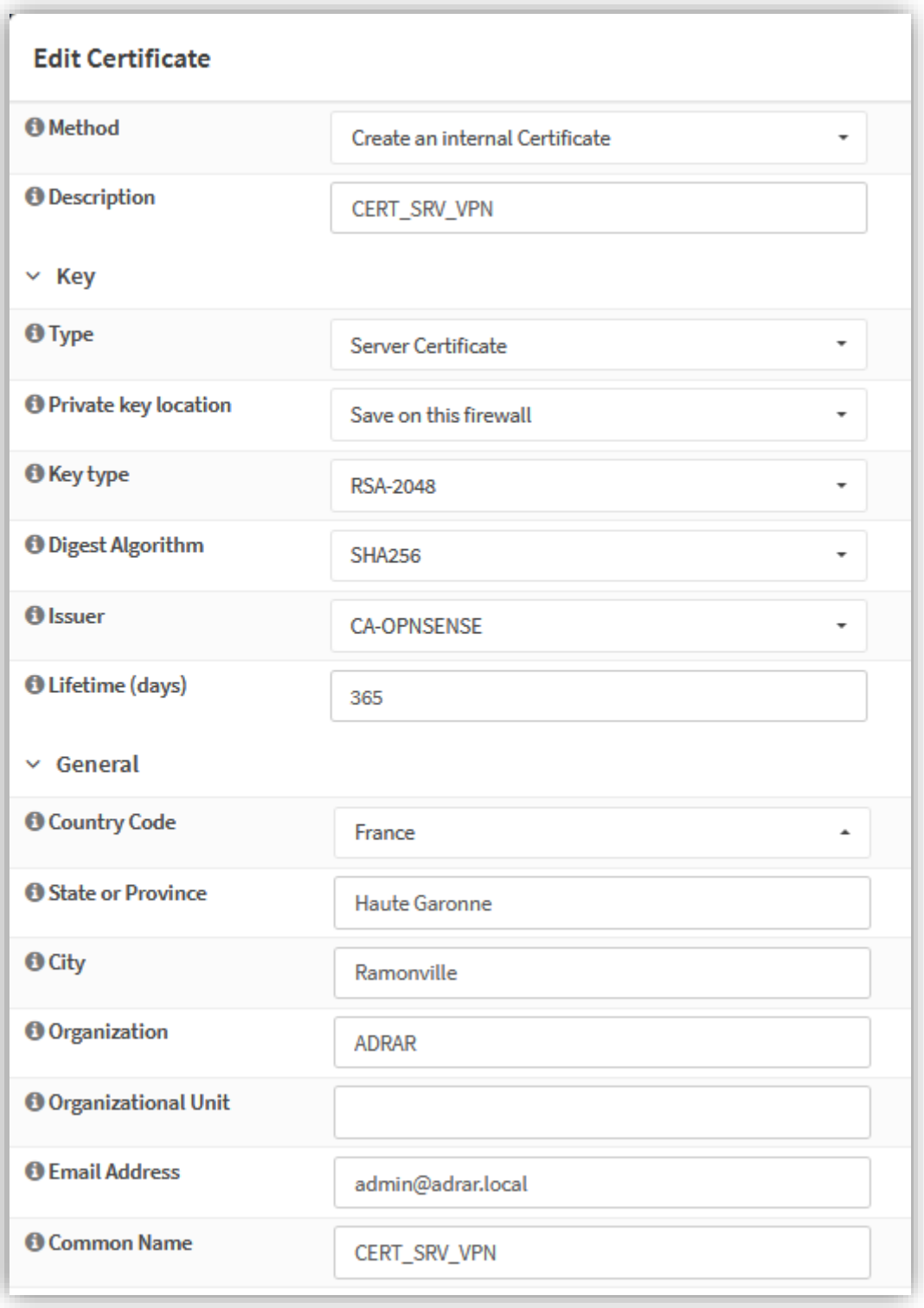
Nous allons nous rendre dans la rubrique **« System -> Access -> Tester »** afin de valider le bon fonctionnement du MFA (ne pas oublier de rentrer d'abord le jeton puis le mot de passe) :



2.5 Génération du certificat SSL pour le serveur VPN

Pour générer le certificat serveur, nous allons dans « **System –> Trust -> Certificate »**

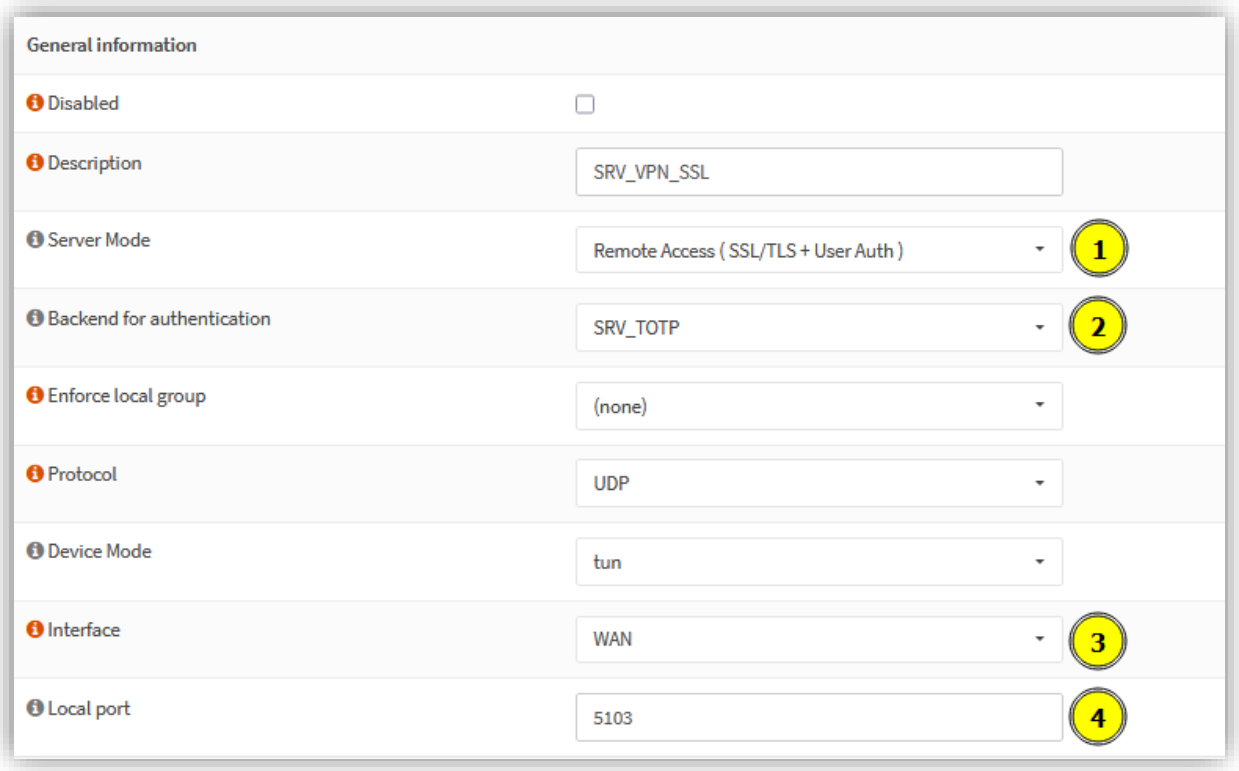
Nous sélectionnons le **« Type »** qui sera, cette fois-ci, **« Server Certificate ».**
Nous renseignons les champs **« Description »** et **« Common Name »** puis en sélectionnant notre autorité de certification les autres champs vont se pré remplir :



2.6 Configuration du serveur VPN

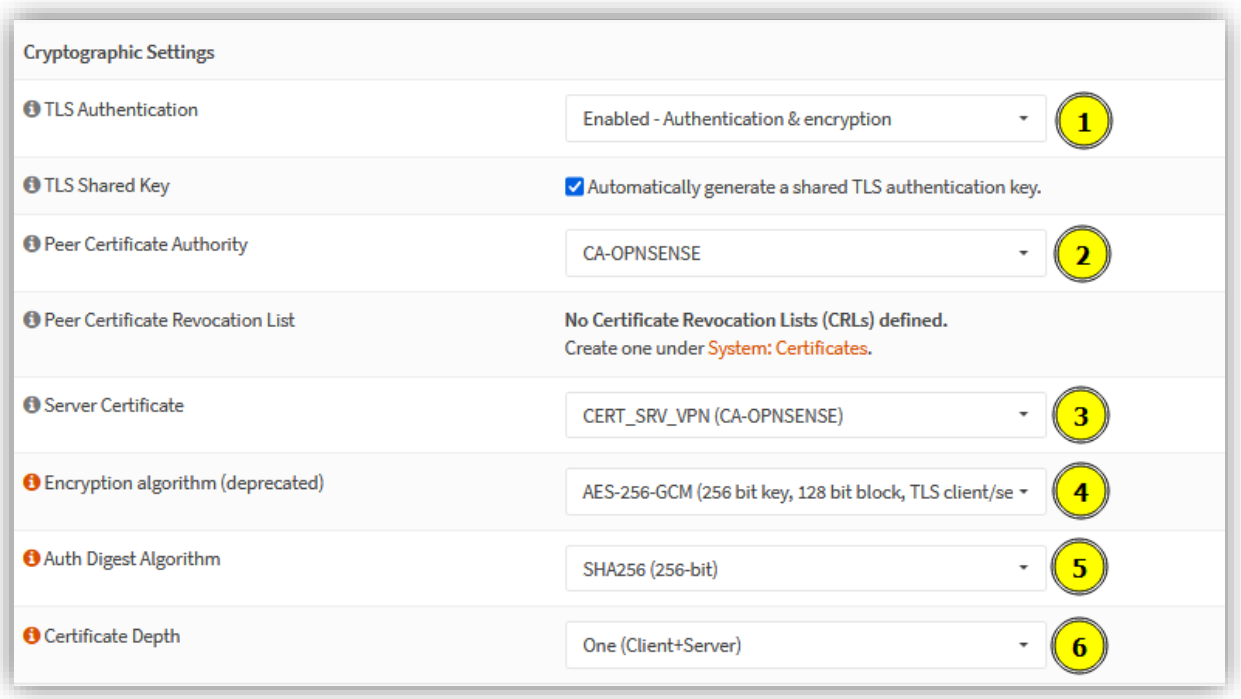
Nous allons maintenant créer notre serveur VPN. Pour cela nous allons dans le menu **« VPN -> OpenVPN -> Servers »**

Nous configurons les informations générales :



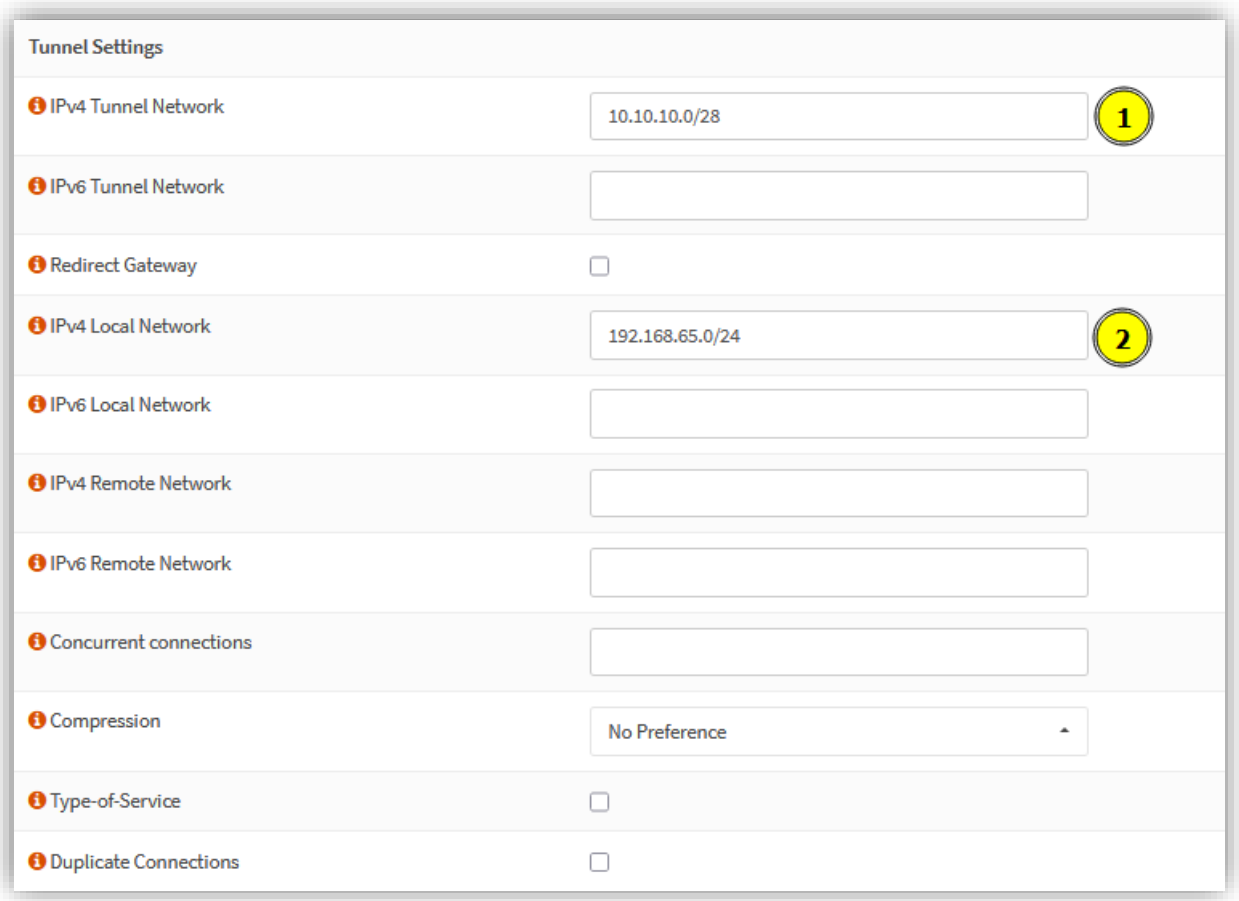
1. Mode d'authentification au serveur choisi : certificat SSL + authentification locale de l'utilisateur (via le MFA et le mot de passe définis plus haut).
2. Serveur d'authentification sélectionné qui sera notre serveur TOTP.
3. Interface de destination du tunnel VPN sur le pare feu
4. Port d'écoute personnalisé pour notre serveur VPN

Nous renseignons maintenant les paramètres de cryptographie :



1. Utilisation de TLS pour authentifier les connexions et chiffrer les données
2. Autorité de certification des pairs (client et serveur)
3. Certificat du serveur
4. Algorithme de chiffrement
5. Algorithme de hachage
6. Vérification des certificats client et serveur émis par l'autorité de certification racine ou intermédiaire

Puis enfin les réglages du tunnel :



1. Réseau du tunnel VPN
2. Réseau SRV à joindre via le VPN

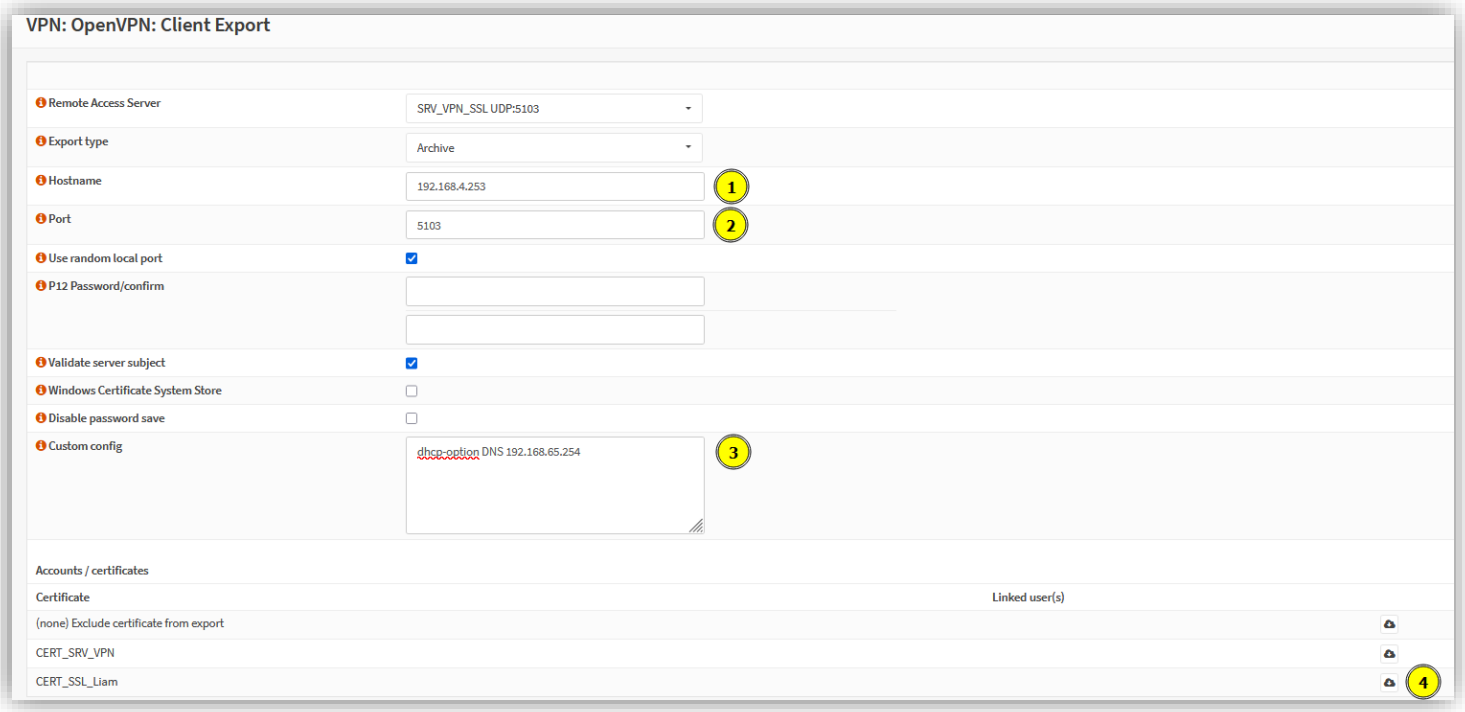
Nous allons maintenant pouvoir effectuer nos tests.

2.7 Test client via le LAN

Pour valider la configuration du VPN, nous avons mis des règles **« permit any – any »** sur nos interfaces.
Les ajustements de sécurité nécessaires seront effectués une fois la validation du VPN faite.

Nous commençons nos tests VPN en local sur notre réseau. Pour cela, nous allons dans le menu **« VPN -> OpenVPN -> Client Export »**

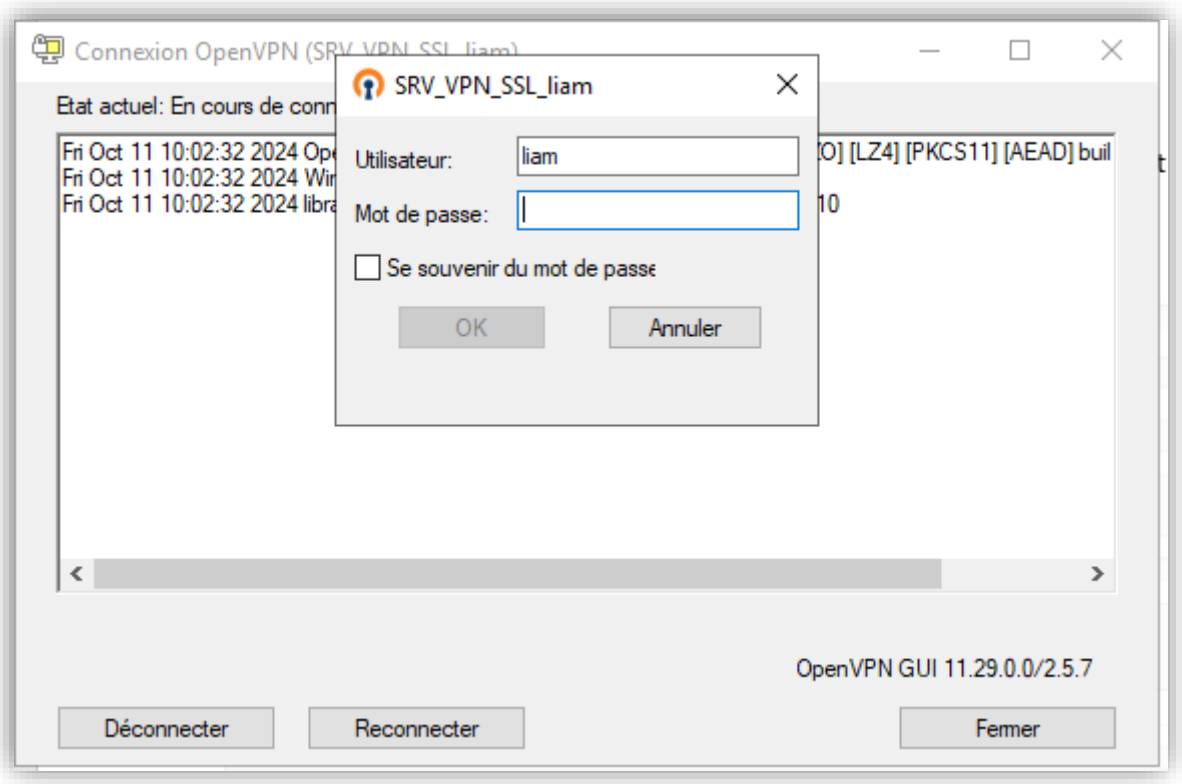
Nous exportons la configuration et renseignons l'IP cible qui est l'adresse WAN de notre pare feu :

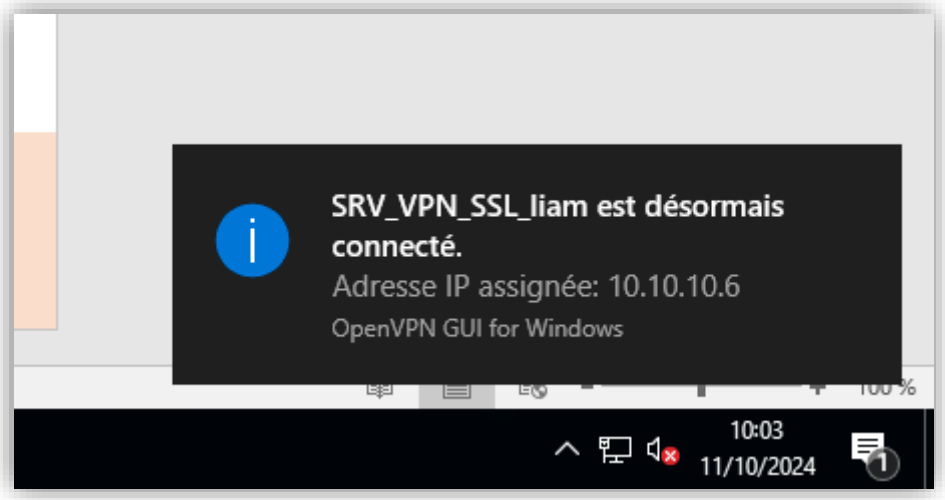


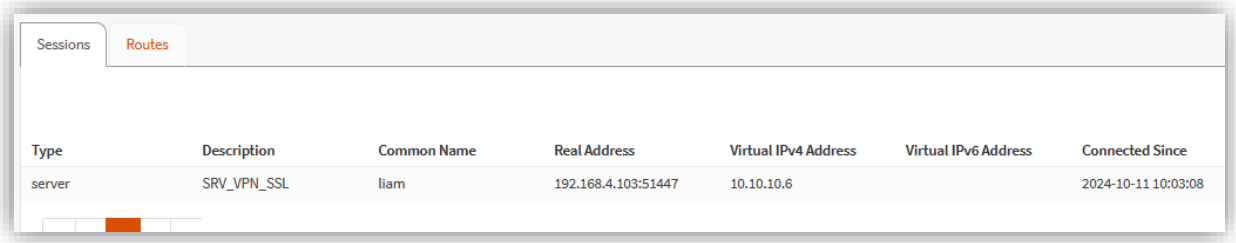
1. IP cible du tunnel VPN
2. Port d'écoute
3. Option pour pousser le serveur DNS dans la configuration client VPN
4. Configuration client à télécharger

Les fichiers de configuration **« cert_liam_ssl »** sont à copier dans le dossier **« %userprofile%\opnsense\config »**.

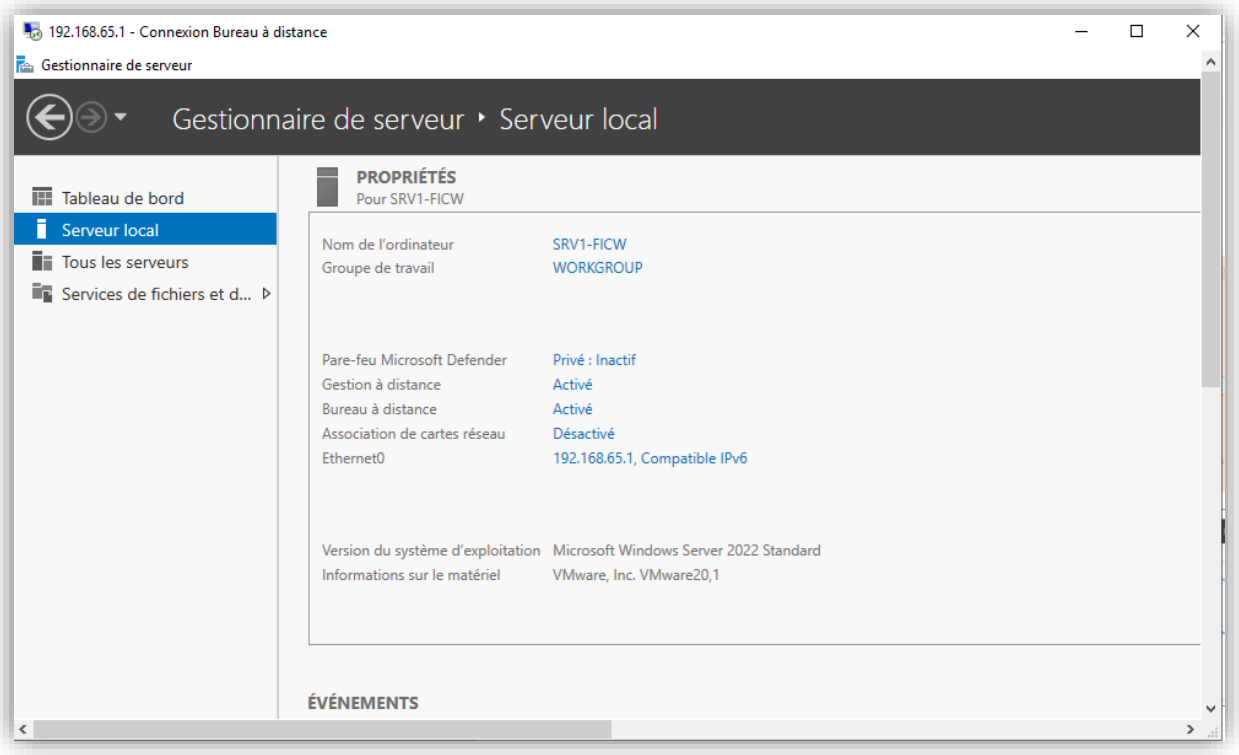
Nous nous connectons via le client OPNVPN :







La connexion de notre VPN a réussi, nous pouvons désormais tester le bureau distant vers le serveur de fichier :



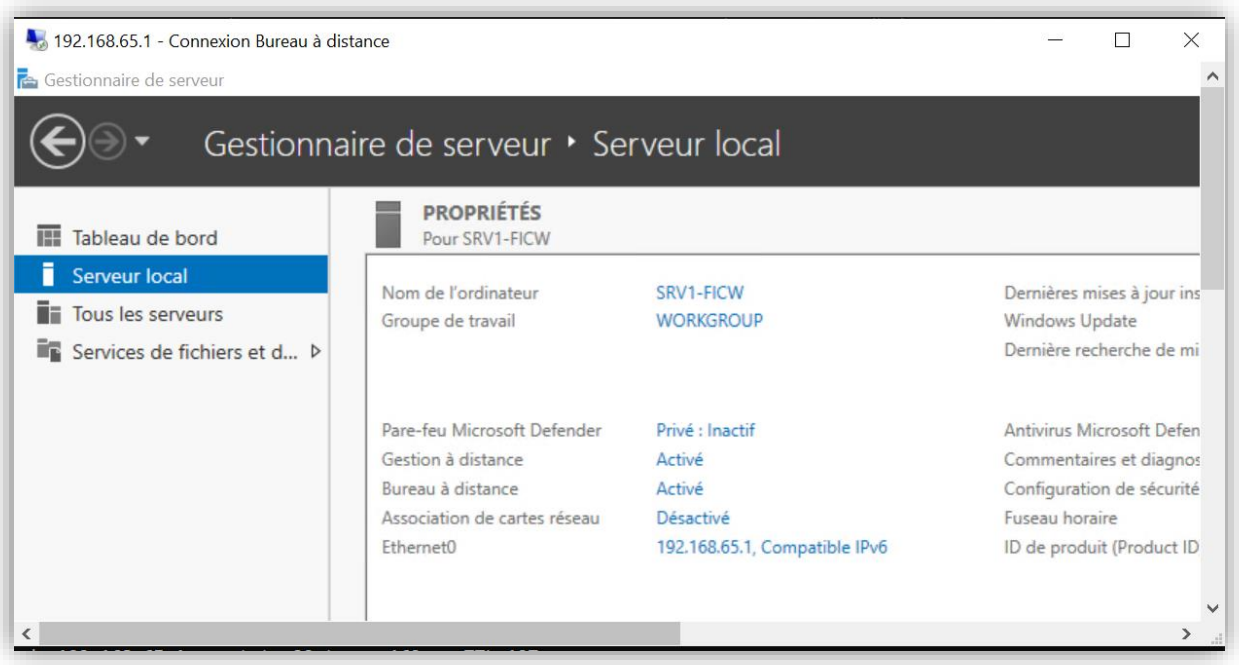
Tout est fonctionnel, nous allons pouvoir passer à la connexion VPN distante via IP publique.

2.8 Test client via le WAN

Comme pour les tests dans notre LAN, les règles de pare feu seront toujours en **« permit any - any »** le temps de la validation du POC.

Nous commençons par créer une règle NAT sur notre Bbox (pour plus d'information cf **1.3 Evolution de l'infrastructure)**

Nous exportons de nouveau notre configuration, comme vu ci-dessus.
Cette fois-ci, nous renseignons l'IP publique de la Bbox et effectuons nos tests via le bureau à distance :



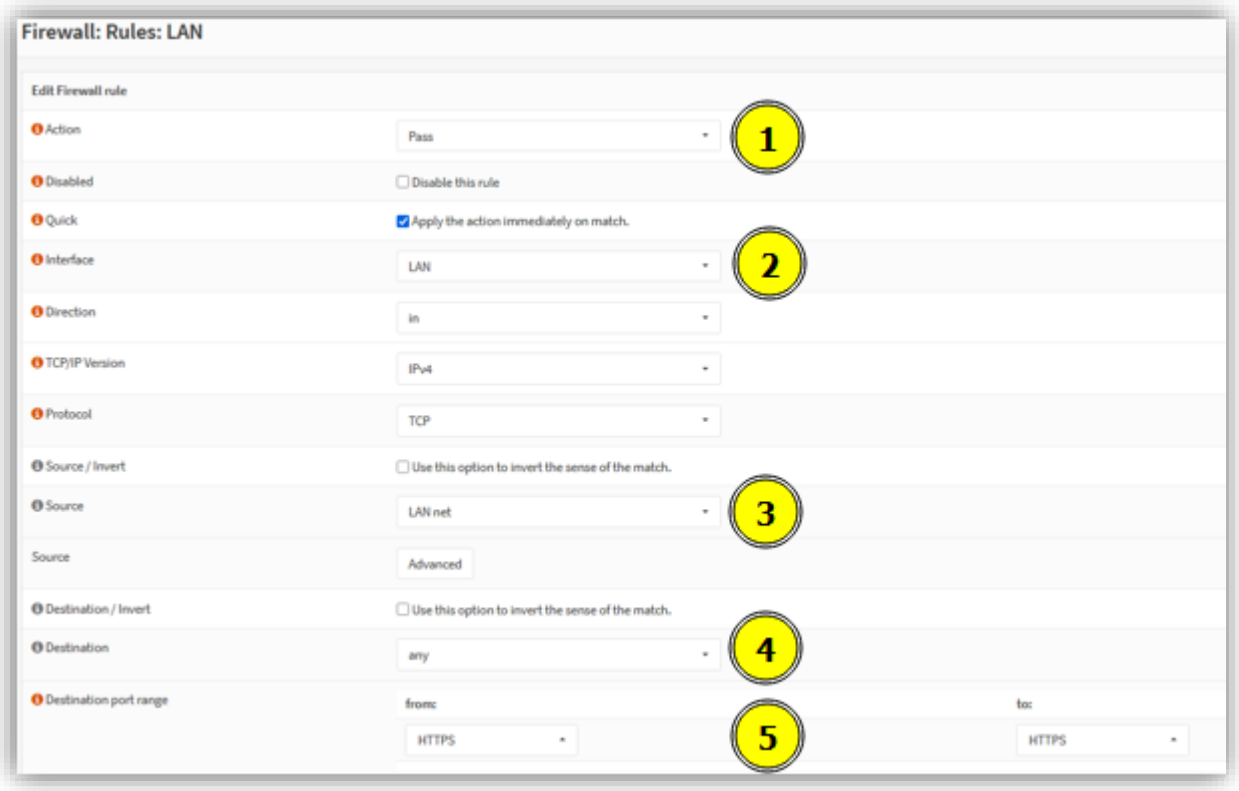
Maintenant que le fonctionnement de notre VPN est validé, nous pouvons mettre en place les règles de pare feu.

2.9 Mise en place des règles de pare feu

Pour plus de détail sur les règles en place, merci de vous référer au paragraphe

1.4 Sécurisation des accès.

Nous allons montrer un exemple de configuration pour une seule règle dans cette procédure, les

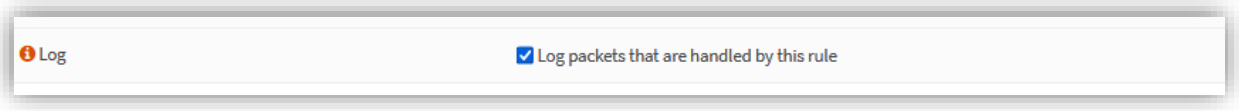


étapes étant identiques pour les autres règles à mettre en place.

Nous commençons par le LAN, l'exemple ci-dessous étant pour la navigation HTTPS :

1. Action de la règle, dans notre cas **« pass »** pour autoriser le flux
2. Interface d'assignation de la règle
3. Source
4. Destination
5. Port de destination

Ne pas oublier de cocher la case **« log »** pour que cette règle soit journalisée :



Voici la configuration des règles par interfaces ainsi que la vérification de leur fonctionnement (une seule règle est testée par interface dans cette procédure, les autres vérifications suivent le même principe) :

LAN

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules
	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	*	Allow_HTTPS
	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	*	Allow_HTTP
	IPv4 UDP	LAN net	*	LAN address	53 (DNS)	*	*	Allow_DNS
	IPv4 TCP	LAN net	*	192.168.65.1	3389 (MS RDP)	*	*	Permit_LAN_to_SRV_RDP

lan	2024-10-11T11:03:53	192.168.10.101:53305	192.168.65.1:3389	tcp	Permit_LAN_to_SRV_RDP
lan	2024-10-11T11:03:49	192.168.10.101:53304	192.168.65.1:3389	tcp	Permit_LAN_to_SRV_RDP

WAN

Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
							Automatically generated rules
IPv4 UDP	*	*	WAN address	5103	*	*	Permit_WAN_VPN

wan	2024-10-11T11:09:08	37.169.10.15:40687	192.168.4.253:5103	udp	Permit_WAN_VPN

SRV

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules
	IPv4 UDP	SRV net	*	SRV address	53 (DNS)	*	*	Permit_SRV_DNS

SRV	2024-10-11T11:14:32	192.168.65.1:57723	192.168.65.254:53	udp	Permit_SRV_DNS
SRV	2024-10-11T11:14:30	192.168.65.1:62395	192.168.65.254:53	udp	Permit_SRV_DNS

VPN

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules
	IPv4 TCP	VPN_Net	*	SRV net	3389 (MS RDP)	*	*	Permit_VPN_to_SRV_RDP
	IPv4 UDP	VPN_Net	*	SRV address	53 (DNS)	*	*	Permit_VPN_DNS

ovpns1	2024-10-11T11:23:38	10.10.10.6:32836	192.168.65.1:3389	tcp	Permit_VPN_to_SRV_RDP

3. Conclusion

Conformément à la demande de l’ADRAR nous avons mis en place et validé le bon fonctionnement du VPN SSL.

Cette solution assure un accès sécurisé aux ressources de l’entreprise, pour les collaborateurs effectuant du télétravail, tout en respectant les exigences de sécurité recommandées par l’ANSSI.