

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	2
1.1 Demandes du client.....	2
1.2 Evolution de l'infrastructure	2
1.3 Choix de la solution	3
1.4 Sécurisation des accès.....	4
1.5 Plan général de configuration	5
2. Configuration technique.....	5
2.1 Installation et paramétrage de l'Opnsense	5
2.2 Mis en place de l'autorité de certification	9
2.3 Mis en place du serveur TOTP	10
2.4 Création d'un utilisateur local avec certificat.....	11
2.5 Génération du certificat SSL pour le serveur VPN.....	15
2.6 Configuration du serveur VPN.....	16
2.7 Test client via le LAN	19
2.8 Test client via le WAN.....	22
2.9 Mise en place des règles de pare feu	24
3. Conclusion	26

1. Contexte

1.1 Demandes du client

Nous sommes contactés par l'ADRAR afin de mettre en place un VPN SSL nomade.

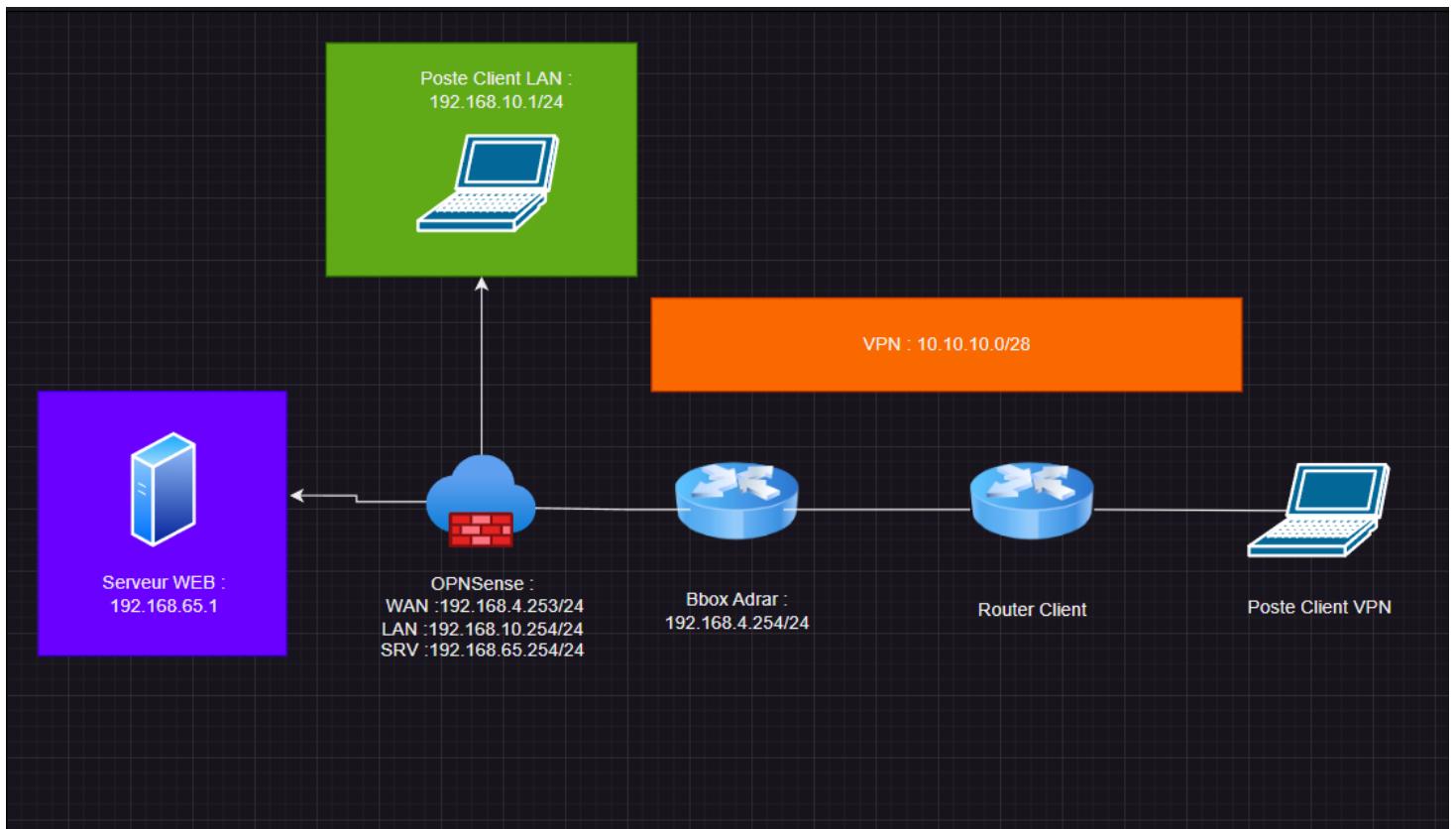
Les télétravailleurs devant accéder au serveur de fichier en utilisant le bureau à distance Windows.

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 « **Provy 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 « **OpenSense** » 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

OpenVPN				
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 pour 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) :

```
0) Logout                                7) Ping host
1) Assign interfaces                      8) Shell
2) Set interface IP address               9) pfTop
3) Reset the root password                10) Firewall log
4) Reset to factory defaults             11) Reload all services
5) Power off system                      12) Update from console
6) Reboot system                          13) Restore a backup

Enter an option: 2
```

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

```
0) Logout                                7) Ping host
1) Assign interfaces                      8) Shell
2) Set interface IP address               9) pfTop
3) Reset the root password                10) Firewall log
4) Reset to factory defaults             11) Reload all services
5) Power off system                      12) Update from console
6) Reboot system                          13) Restore a backup

Enter an option: 2

Available interfaces:

1 - LAN (em1 - static)
2 - OPT1 (em2 - static)
3 - WAN (em0 - static)

Enter the number of the interface to configure: 1
```

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 :

```
Enter the number of the interface to configure: 1
Configure IPv4 address LAN interface via DHCP? [y/N] n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.254

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

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 :

```
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.4.254
```

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

System: Settings: General

System

Hostname	FW1
Domain	adrar.local
Time zone	Europe/Paris
Language	English
Theme	opnsense

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

Defined by	USER
Disabled	<input type="checkbox"/>
Username	admin
Password	***** ***** (confirmation)
<input type="checkbox"/> Generate a scrambled password to prevent local database logins for this user.	
Full name	Administrateur ADRAR User's full name, for your own information only
E-Mail	admin@adrar.local
Comment	Administrateur IT ADRAR
Preferred landing page	Preferred landing page after login or authentication failure
Language	Default
Login shell	/usr/sbin/nologin
Expiration date	
Group Memberships	Not Member Of Member Of admins

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 :

Method	Create an internal Certificate Authority
Description	CA-OPNSENSE
Key	
Key type	RSA-2048
Digest Algorithm	SHA256
Issuer	self-signed
Lifetime (days)	365
General	
Country Code	France
State or Province	Haute Garonne
City	Ramonville
Organization	ADRAR
Organizational Unit	IT
Email Address	admin@adrar.local
Common Name	CA-OPNSENSE

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 :

The screenshot shows a configuration form for a new server. The fields and their values are:

Descriptive name	SRV_TOTP
Type	Local + Timebased One Time Password
Token length	6
Time window	(empty)
Grace period	(empty)
Reverse token order	<input type="checkbox"/>

At the bottom right is a red "Save" button.

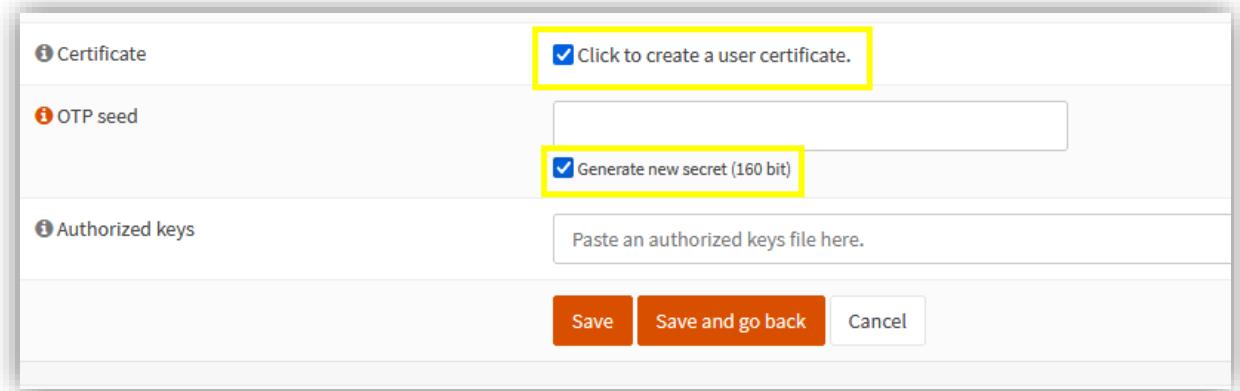
2.4 Crédation d'un utilisateur local avec certificat

Nous allons créer un utilisateur local pour notre VPN nomade.

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

Defined by	USER
Disabled	<input type="checkbox"/>
Username	liam
Password	••••••• ••••••• (confirmation)
<input type="checkbox"/> Generate a scrambled password to prevent local database logins for this user.	
Full name	Liam MARAVAL
E-Mail	liam.maraval@adrar.local
Comment	
Preferred landing page	
Language	Default
Login shell	/usr/sbin/nologin

Deux cases vont être à cocher « **Certificate** » 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.

Edit Certificate

Method	Create an internal Certificate
Description	CERT_liam_SSL
Key	
Type	Client Certificate
Private key location	Save on this firewall
Key type	RSA-2048
Digest Algorithm	SHA256
Issuer	CA-OPENSENSE
Lifetime (days)	365
General	
Country Code	France
State or Province	Haute Garonne
City	Ramonville
Organization	ADRAR
Organizational Unit	
Email Address	admin@adrar.local
Common Name	liam

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.

The screenshot shows the OpenSense interface with several sections highlighted by yellow boxes:

- User Certificates:** A table with one row: Name: CERT_lliam_SSL, CA: CA-OPENSENSE, Valid From: Sun, 13 Oct 2024 17:34:41 +0000, Valid To: Mon, 13 Oct 2025 17:34:41 +0000.
- API keys:** A section with a key field and a '+' button.
- OTP seed:** A section with a text input field containing LAMXPG3KTSXKBC24LMQUZPMVB3KECOCK and a checkbox for "Generate new secret (160 bit)".
- OTP QR code:** A large QR code.

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**) :

The screenshot shows the "System: Access: Tester" page with the following details:

- User:** liam authenticated successfully.
This user is a member of these groups:
- Authentication Server:** SRV-TOTP01
- Username:** liam
- Password:** (redacted)
- Test:** A red button.

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 :

Edit Certificate

Method	Create an internal Certificate
Description	CERT_SRV_VPN
Key	
Type	Server Certificate
Private key location	Save on this firewall
Key type	RSA-2048
Digest Algorithm	SHA256
Issuer	CA-OPENSENSE
Lifetime (days)	365
General	
Country Code	France
State or Province	Haute Garonne
City	Ramonville
Organization	ADRAR
Organizational Unit	
Email Address	admin@adrar.local
Common Name	CERT_SRV_VPN

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 :

General information	
! Disabled	<input type="checkbox"/>
! Description	SRV_VPN_SSL
! Server Mode	Remote Access (SSL/TLS + User Auth) 1
! Backend for authentication	SRV_TOTP 2
! Enforce local group	(none)
! Protocol	UDP
! Device Mode	tun
! Interface	WAN 3
! Local port	5103 4

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 :

The screenshot shows the 'Cryptographic Settings' configuration page. It lists several parameters with their current values and some descriptive text or status indicators. Yellow circles with numbers 1 through 6 are overlaid on the right side of the page, pointing to specific fields:

- 1**: TLS Authentication dropdown set to "Enabled - Authentication & encryption".
- 2**: Peer Certificate Authority dropdown set to "CA-OPENSENSE".
- 3**: Server Certificate dropdown set to "CERT_SRV_VPN (CA-OPENSENSE)".
- 4**: Encryption algorithm dropdown set to "AES-256-GCM (256 bit key, 128 bit block, TLS client/se...)".
- 5**: Auth Digest Algorithm dropdown set to "SHA256 (256-bit)".
- 6**: Certificate Depth dropdown set to "One (Client+Server)".

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 :

Tunnel Settings

1 IPv4 Tunnel Network	10.10.10.0/28	1
1 IPv6 Tunnel Network		
1 Redirect Gateway	<input type="checkbox"/>	
1 IPv4 Local Network	192.168.65.0/24	2
1 IPv6 Local Network		
1 IPv4 Remote Network		
1 IPv6 Remote Network		
1 Concurrent connections		
1 Compression	No Preference	
1 Type-of-Service	<input type="checkbox"/>	
1 Duplicate Connections	<input type="checkbox"/>	

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 :

VPN: OpenVPN: Client Export

① Remote Access Server: SRV_VPN_SSL UDP:5103

② Export type: Archive

③ Hostname: 192.168.4.253 (1)

④ Port: 5103 (2)

⑤ Use random local port:

⑥ P12 Password/confirm:

⑦ Validate server subject:

⑧ Windows Certificate System Store:

⑨ Disable password save:

⑩ Custom config: dhcp-option DNS 192.168.65.254 (3)

Accounts / certificates

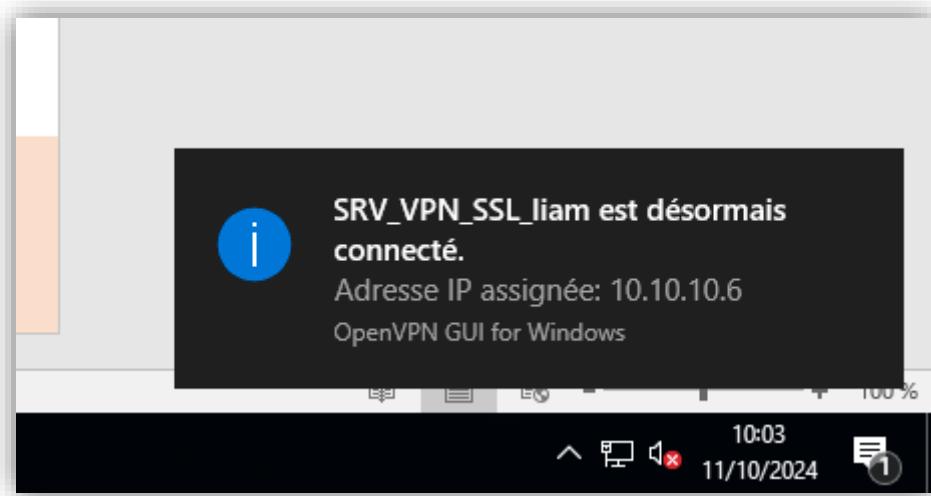
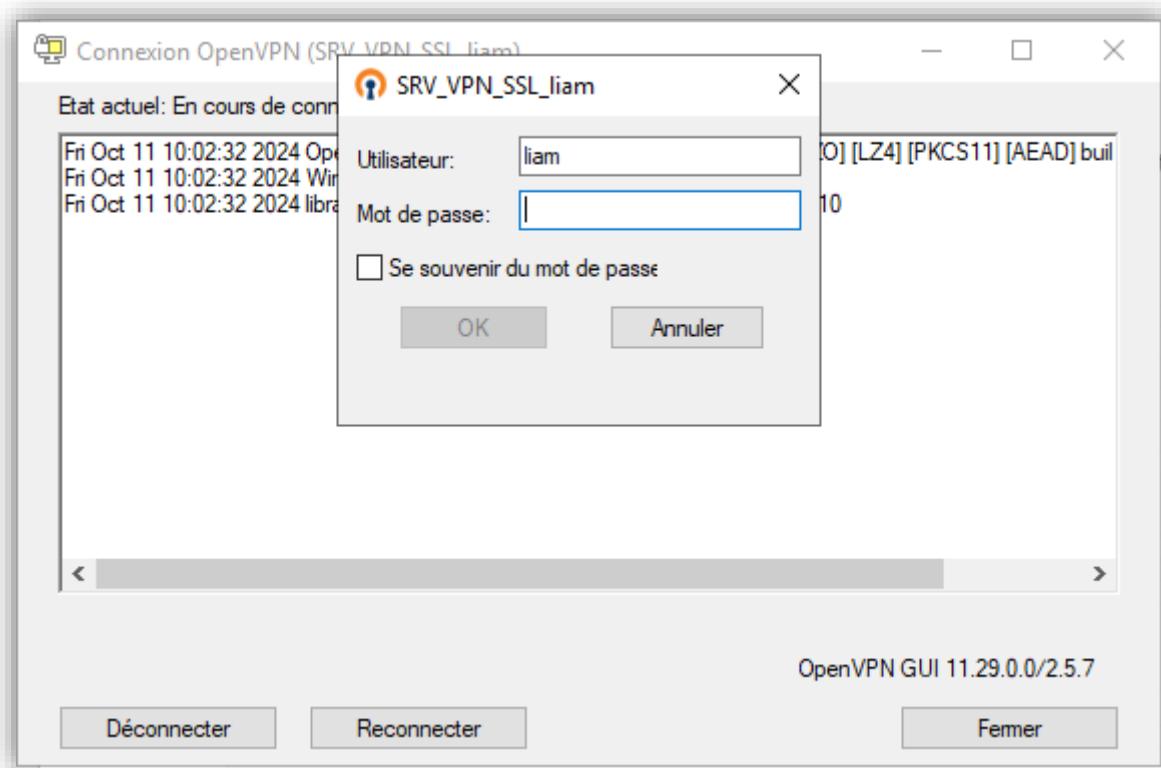
Certificate: CERT_SRV_VPN, CERT_SSL_Liam

Linked user(s): (4)

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

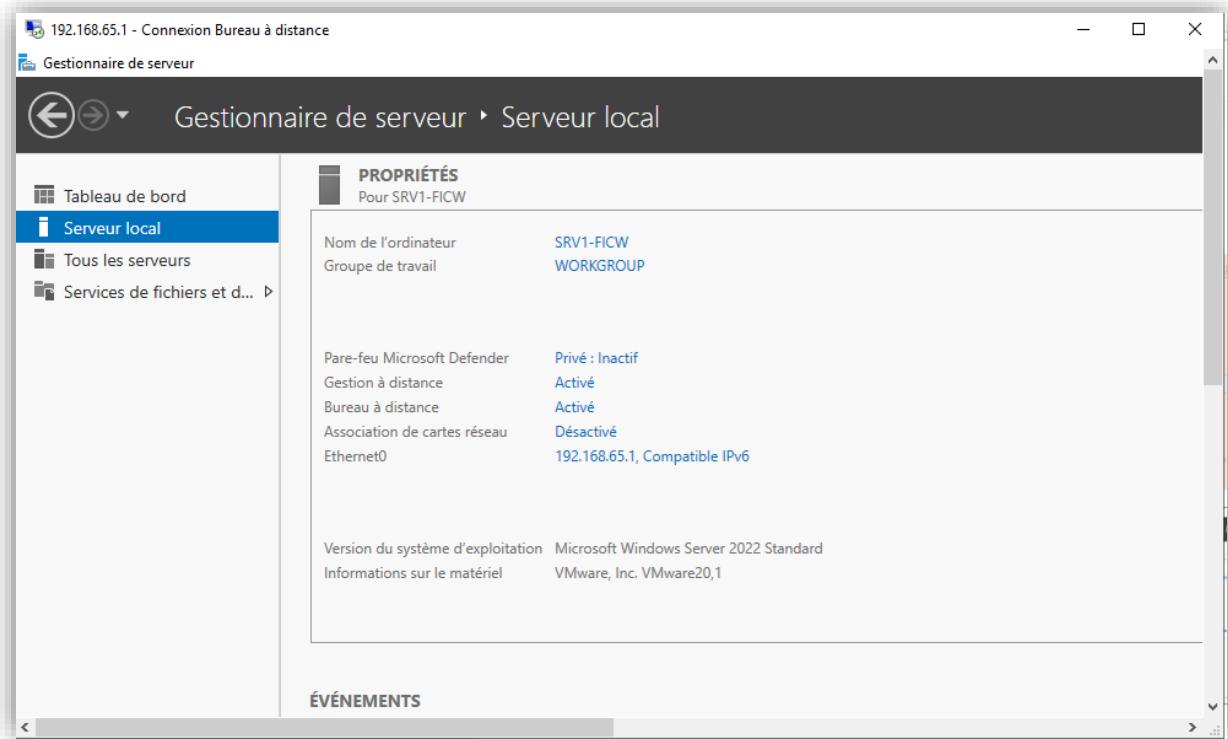
Les fichiers de configuration « **cert_liam_ssl** » sont à copier dans le dossier « **%userprofile%\opnsense\config** ».

Nous nous connectons via le client OPNVPN :



Sessions	Routes					
Type	Description	Common Name	Real Address	Virtual IPv4 Address	Virtual IPv6 Address	Connected Since
server	SRV_VPN_SSL	liam	192.168.4.103:51447	10.10.10.6		2024-10-11 10:03:08

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

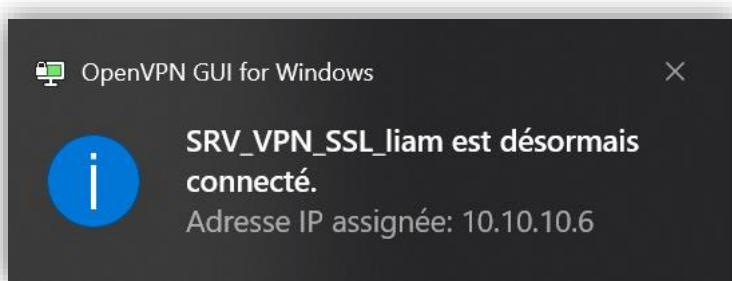
Comme pour les tests dans notre LAN, les règles de pare feu seront toujours en « **permit any - any** » le temps de la validation du POC.

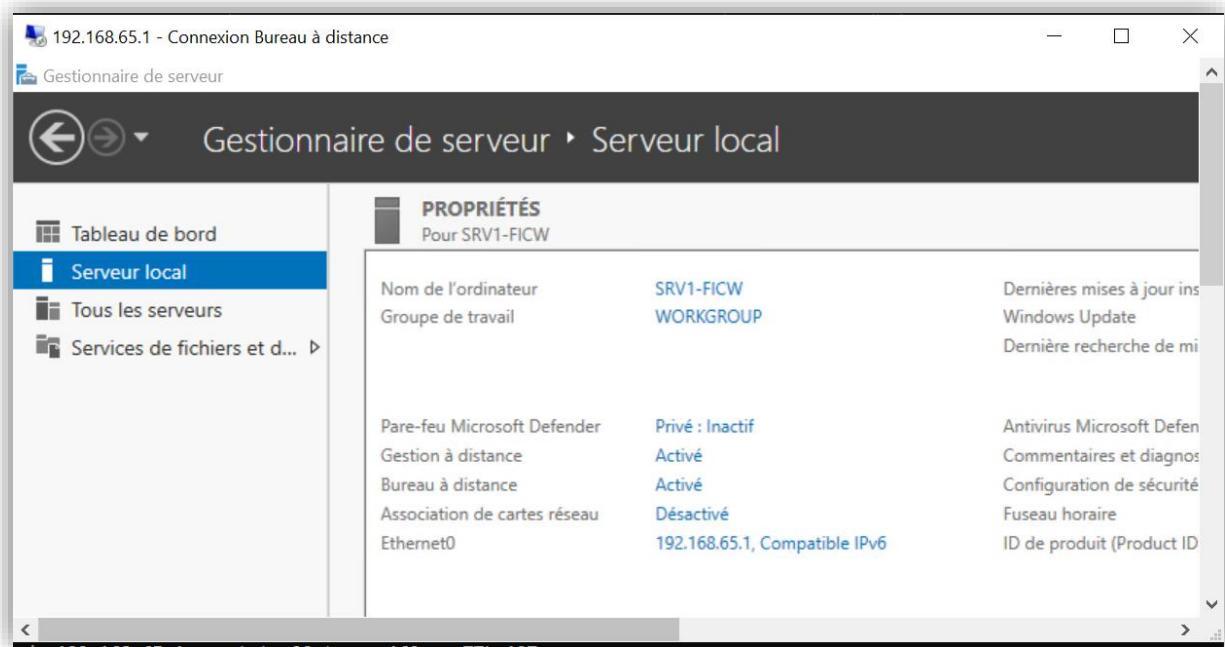
Nous commençons par créer une règle NAT sur notre Bbox (pour plus d'information cf **1.3 Evolution de l'infrastructure**)



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

Firewall: Rules: LAN

Edit Firewall rule

1 Action: Pass

2 Interface: LAN

3 Source: LAN net

4 Destination: any

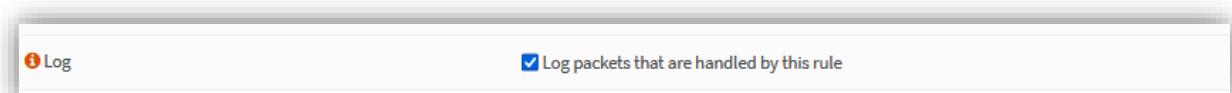
5 Destination port range: from: HTTPS, to: HTTPS

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				
<i>Automatically generated rules</i>													
	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					
<i>Automatically generated rules</i>													
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				
<i>Automatically generated rules</i>													
	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				
<i>Automatically generated rules</i>													
	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				
▶ ovpn1		→	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.