

Manuel d'utilisation



MTW/006F • V1.0 • 01/2022



www.wit.fr

SOMMAIRE

1	Introduction.....	3
	Généralités	3
	Zoom sur l'OpenVPN	3
	Prérequis matériel	3
	Prérequis logiciel	4
2	Configurer un serveur OpenVPN	5
	Architecture réseau	5
	Paramétrage de la connexion	5
	Paramètres	6
	Paramètre de la connexion	6
	Paramètre du réseau VPN créé	7
	Téléchargement du fichier de configuration pour les clients VPN	7
	Onglet Connexion.....	8
3	Configurer un client OpenVPN	9
	Architecture réseau	9
	Paramétrage de la connexion	9
4	Configurer une connexion inter-sites	12
	Architecture réseau	12
	Paramétrage de la connexion	12
5	Se connecter à un REDY avec un poste de supervision	14
6	Dépannage.....	15

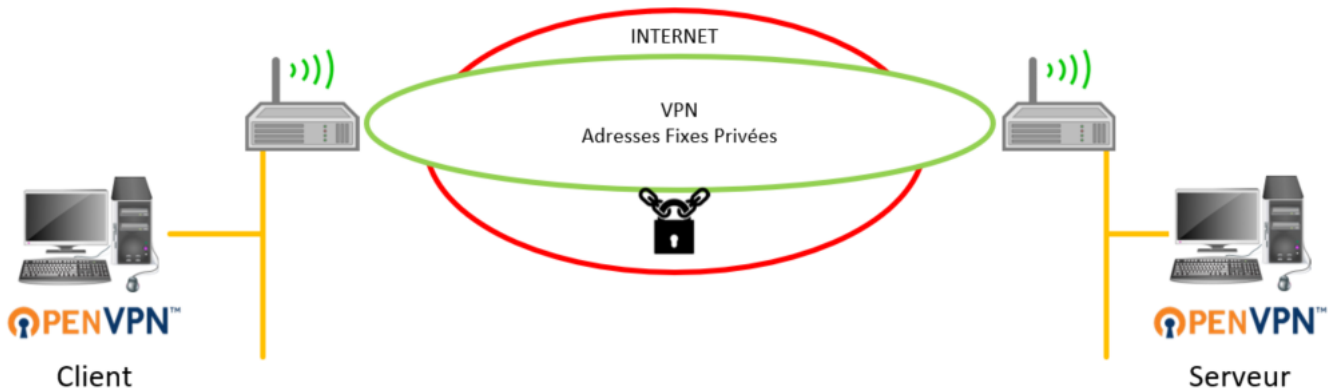
1 Introduction

Généralités

Ce document a pour but d'expliquer comment configurer et utiliser l'OpenVPN (client et serveur) dans l'environnement REDY.

Zoom sur l'OpenVPN

OpenVPN est un protocole VPN, qui permet de créer un réseau privé virtuel (virtual private network), afin de renforcer la sécurité d'une connexion Internet, et ainsi empêcher la fuite ou la captation de données.



Prérequis matériel

Les produits suivant sont compatibles :

UC	Référence
PLUG REDY-MONITOR XS LAN	PLUG701
PLUG REDY-MONITOR XS 3G	PLUG702
PLUG REDY-MONITOR XS 4G	PLUG703
PLUG REDY-MONITOR XS 3G/4G	PLUG704
PLUG REDY-PROCESS XS LAN	PLUG801
PLUG REDY-PROCESS XS 3G	PLUG802
PLUG REDY-PROCESS XS 4G	PLUG803
PLUG REDY-PROCESS XS 3G/4G	PLUG804



La fonctionnalité OpenVPN est compatible avec la gamme **REDY de type K7** uniquement (vendu à partir de janvier 2018).

Prérequis logiciel

Versions minimales

Type	Version
Applicatif REDY	V14.2.0
OS REDY	V2.4.2



La connexion OpenVPN ne nécessite pas d'ADD logiciel.

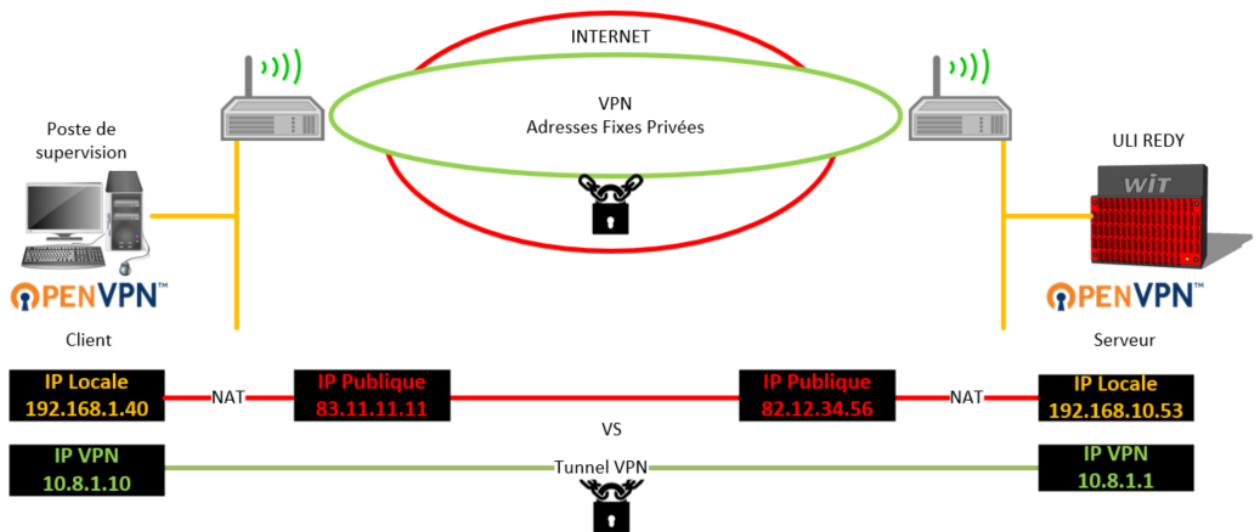
Horloge système

Avant d'effectuer le paramétrage des réseaux VPN, il est important de s'assurer que les ULI REDY concernées par le réseau VPN soient à l'heure. La synchronisation de l'horloge via NTP n'est pas obligatoire mais conseillée.

2 Configurer un serveur OpenVPN

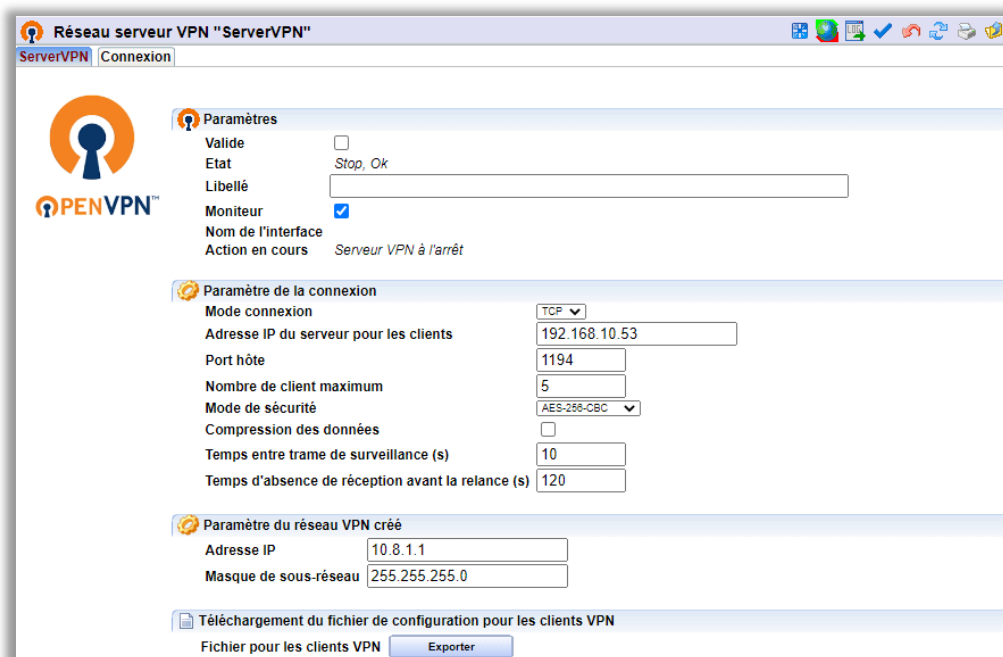
Architecture réseau

L'ULI REDY est à configurer en tant que **serveur OpenVPN** lorsqu'il sera en attente d'une autre connexion cliente OpenVPN :



Paramétrage de la connexion

Dans l'onglet **Configuration / Réseau**, cliquer sur le réseau **Serveur VPN** puis configurer le réseau selon le besoin :



Paramètres

Valide	Démarrer le serveur OpenVPN
Etat	Synthèse de l'état du serveur OpenVPN (actuellement arrêté)
Libellé	Libellé personnalisable du serveur OpenVPN
Moniteur	Afficher les trames d'échanges horodatés
Nom de l'interface	Affichage du nom de la connexion (actuellement vide car pas de libellé)
Action en cours	Etat détaillé du serveur OpenVPN

Paramètre de la connexion

Mode connexion	TCP ou UDP. L'ANSI préconise l'UDP. Selon la configuration de réseau où se situe le REDY.
Adresse IP du serveur pour les clients	Cette adresse représente l'IP auquel les clients VPN vont se connecter. Si le REDY serveur VPN se trouve dans un réseau privé, cette adresse IP doit correspondre à l'adresse extérieure du routeur donnant accès au réseau privé.
Port hôte	Numéro du port du REDY serveur VPN auquel les clients VPN vont se connecter.
Nombre de client maximum	Nombre de client que le REDY serveur VPN autorise simultanément. Par défaut la valeur est 5. Le maximum est 20.
Mode de sécurité	Ce choix permet de sélectionner le mode d'encryptage mis en œuvre pour sécuriser le VPN. Par défaut le mode AES-256-CBC est le mode le plus sécurisé. Le REDY serveur VPN autorise les modes suivants : DES-CBC CAST5-CBC RC2-CBC RC2-40-CBC DES-EDE-CBC RC2-64-CBC DES-EDE3-CBC AES-128-CBC DESX_CBC AES-192-CBC BF-CBC AES-256-CBC
Compression des données	Pour minimiser le volume de données échangés entre le serveur et le client, il est possible d'activer la compression. Cela peut être très utile pour les connexions modems, sans dégrader les performances.
Temps être trame de surveillance	Temps entre l'envoi de trames de surveillance aux clients.

Temps d'absence de réception avant la relance

Temps au bout duquel, sans réception de réponse au trames de surveillance du client, le serveur redémarre.

Paramètre du réseau VPN créé

Adresse IP

Cette Adresse IP représente l'adresse du serveur VPN pour les clients, mais aussi la première adresse de la plage d'adresse IP que le serveur va fournir aux différents clients.

Masque de sous-réseau

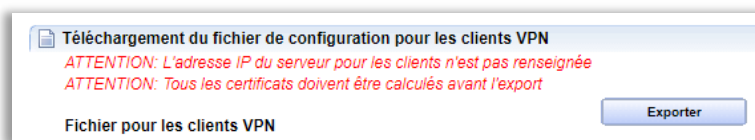
En lien avec l'adresse IP ci-dessus, ce masque permet de connaître le préfixe du sous-réseau VPN




Téléchargement du fichier de configuration pour les clients VPN


Fichier pour les clients VPN

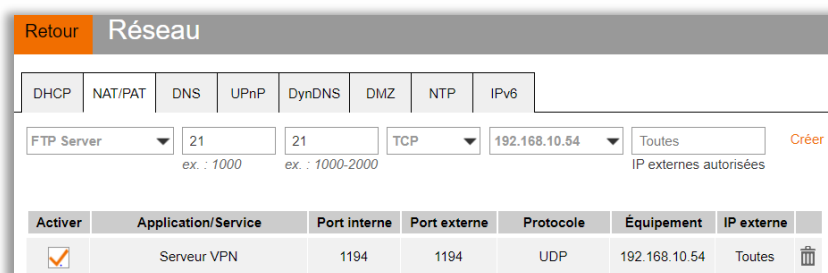
Une fois le paramétrage complet du serveur VPN, il est possible de télécharger sur le PC le fichier de configuration qu'il faut fournir au client pour établir la connexion. Ce fichier se nomme « REDY-xxxx-xxxx.ovpn » où xxxx-xxxx représente le numéro de série du REDY serveur VPN. Afin de télécharger ce fichier d'export, la connexion a besoin de calculer ses certificats :

- Cette opération ne peut pas fonctionner avec REDY-PC.
- Il est nécessaire d'attendre la fin de cette opération pour effectuer l'export, si cette opération n'est pas terminée le message suivant apparaît :



 Il est possible d'afficher le moniteur du serveur VPN en cochant sa case et en cliquant sur l'icone : 
Il est possible d'exporter le fichier d'échange (log) fourni par le serveur en cliquant sur l'icone : 

 Afin d'autoriser la connexion VPN sur un REDY serveur du réseau public vers le réseau privé, il est nécessaire d'ouvrir le port (par défaut 1194 sur l'IP locale du REDY) sur la BOX concernée. Le protocole à sélectionner est TCP ou UDP. Exemple sur une LiveBOX :

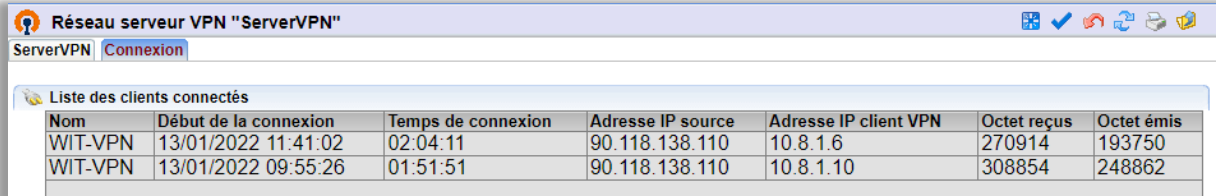


Onglet Connexion


L'onglet connexion permet de connaître en temps réels les clients connectés au serveur.

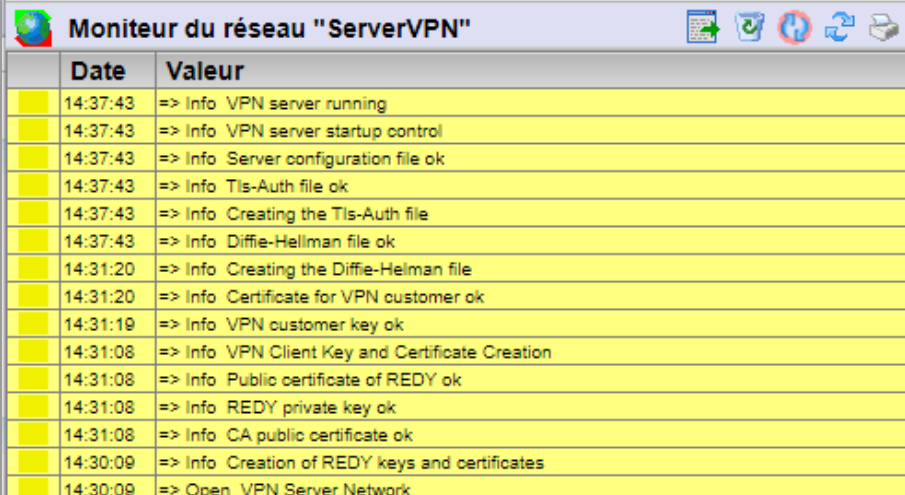
Les informations disponibles sont :

- La date et heure de début de la connexion
- La durée de la connexion
- L'adresse IP du client vu sur le réseau internet
- L'adresse IP du client fourni par le serveur VPN
- Le nombre d'octets reçu du client
- Le nombre d'octets émis vers le client



Nom	Début de la connexion	Temps de connexion	Adresse IP source	Adresse IP client VPN	Octet reçu	Octet émis
WIT-VPN	13/01/2022 11:41:02	02:04:11	90.118.138.110	10.8.1.6	270914	193750
WIT-VPN	13/01/2022 09:55:26	01:51:51	90.118.138.110	10.8.1.10	308854	248862

 Lors du premier démarrage du serveur VPN, celui-ci a besoin d'un ensemble de clés de sécurité et de certificat. Pour calculer ces informations cela peut prendre entre 5 à 10 minutes. Afin de suivre l'évolution, toutes les opérations effectuées sont affichées dans le moniteur, les démarrages suivants sont beaucoup plus rapides :

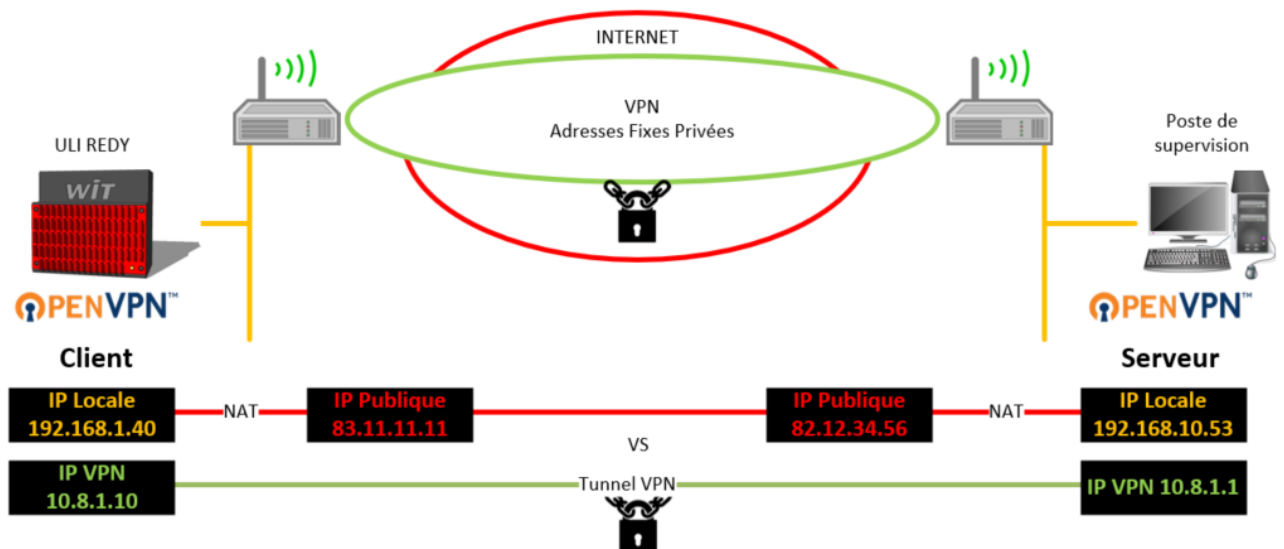


Date	Valeur
14:37:43	=> Info VPN server running
14:37:43	=> Info VPN server startup control
14:37:43	=> Info Server configuration file ok
14:37:43	=> Info Tls-Auth file ok
14:37:43	=> Info Creating the Tls-Auth file
14:37:43	=> Info Diffie-Hellman file ok
14:31:20	=> Info Creating the Diffie-Helman file
14:31:20	=> Info Certificate for VPN customer ok
14:31:19	=> Info VPN customer key ok
14:31:08	=> Info VPN Client Key and Certificate Creation
14:31:08	=> Info Public certificate of REDY ok
14:31:08	=> Info REDY private key ok
14:31:08	=> Info CA public certificate ok
14:30:09	=> Info Creation of REDY keys and certificates
14:30:09	=> Open VPN Server Network

3 Configurer un client OpenVPN

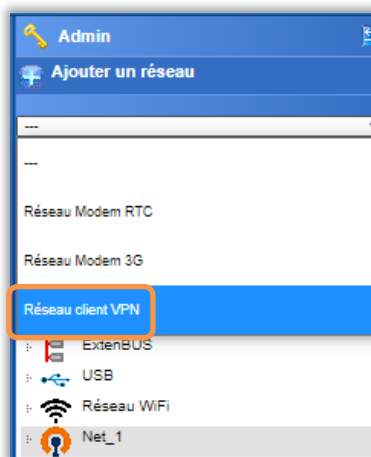
Architecture réseau

L'ULI REDY est à configurer en tant que **client OpenVPN** lorsqu'il voudra se connecter sur un réseau serveur OpenVPN :

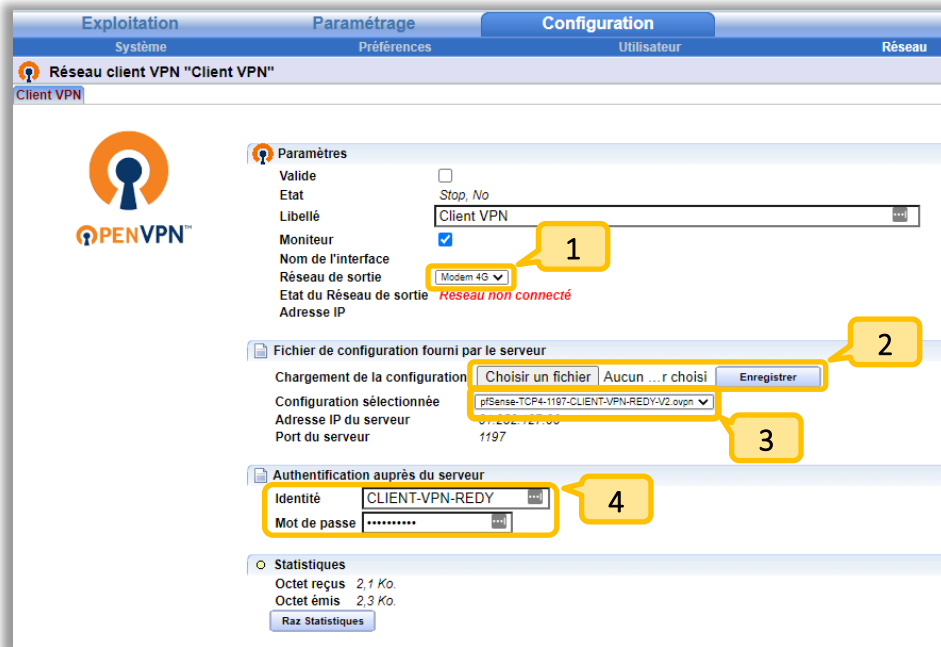


Paramétrage de la connexion




Etape 1 Dans Configuration / Réseau, sélectionner le dans la liste déroulante Réseau client VPN :




Etape 2 Cliquer sur le **Réseau client VPN** puis renseigner les paramètres suivants :

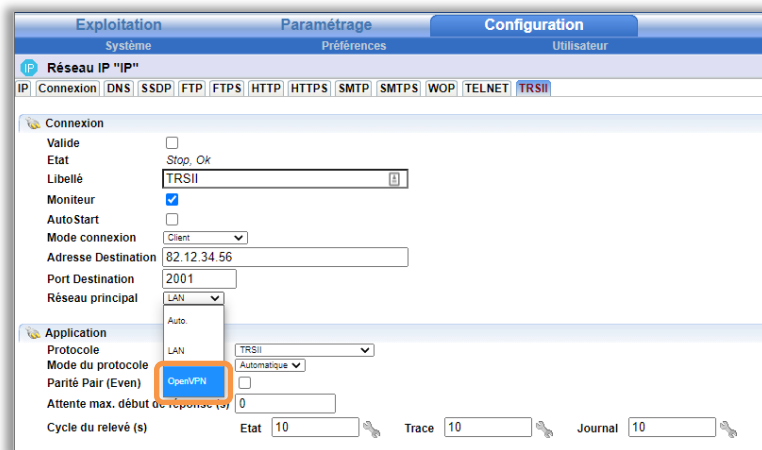


- 1 Sélectionner le réseau qui permettra de sortir du REDY (Auto, LAN ou 4G ; en automatique le réseau LAN sera préféré).
- 2 Sélectionner le fichier de configuration OpenVPN (l'extension de fichier autorisée est **.ovpn**, fourni par le serveur OpenVPN) puis enregistrer (tous les fichiers intégrés seront stockés dans Configuration/Gestionnaire/Projets).
- 3 Sélectionner le fichier de configuration dans le menu déroulant.
- 4 Renseigner les paramètres d'authentification si nécessaire (optionnel).

 Il est possible d'afficher le moniteur du REDY en cochant sa case et en cliquant sur l'icone : 
Il est possible d'exporter le fichier d'échange (log) fourni par le VPN en cliquant sur l'icone : 

 Le support technique ne pourra être effectué sur un fichier **.ovpn** non fonctionnel, sauf si celui-ci provient d'un autre REDY. Dans le premier cas, il sera nécessaire de demander une assistance à l'administrateur système gérant le réseau VPN.

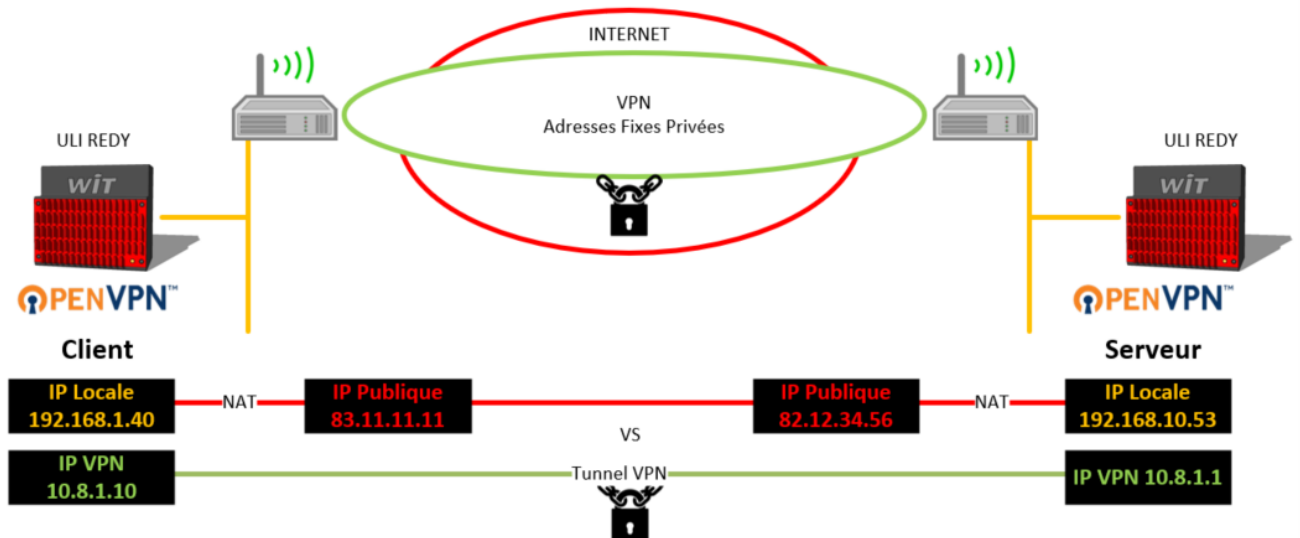
Etape 4 Il est désormais possible de sélectionner le réseau VPN dans chaque connexions sortantes le nécessitant.
Exemple :



4 Configurer une connexion inter-sites

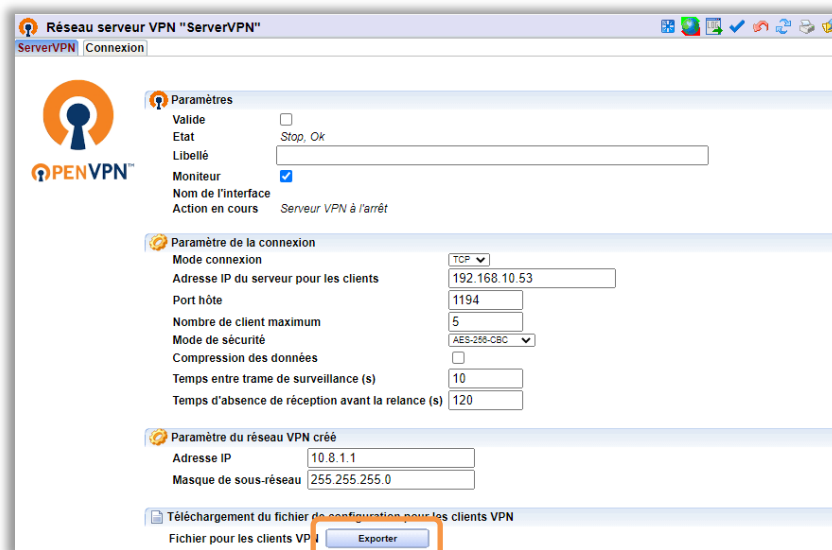
Architecture réseau

Deux ULI REDY s'échangent des données à travers un réseaux VPN. Dans ce cas il est nécessaire de configurer le REDY à l'initiative de la communication en **client**, le REDY récepteur sera lui configuré en tant que **serveur** :

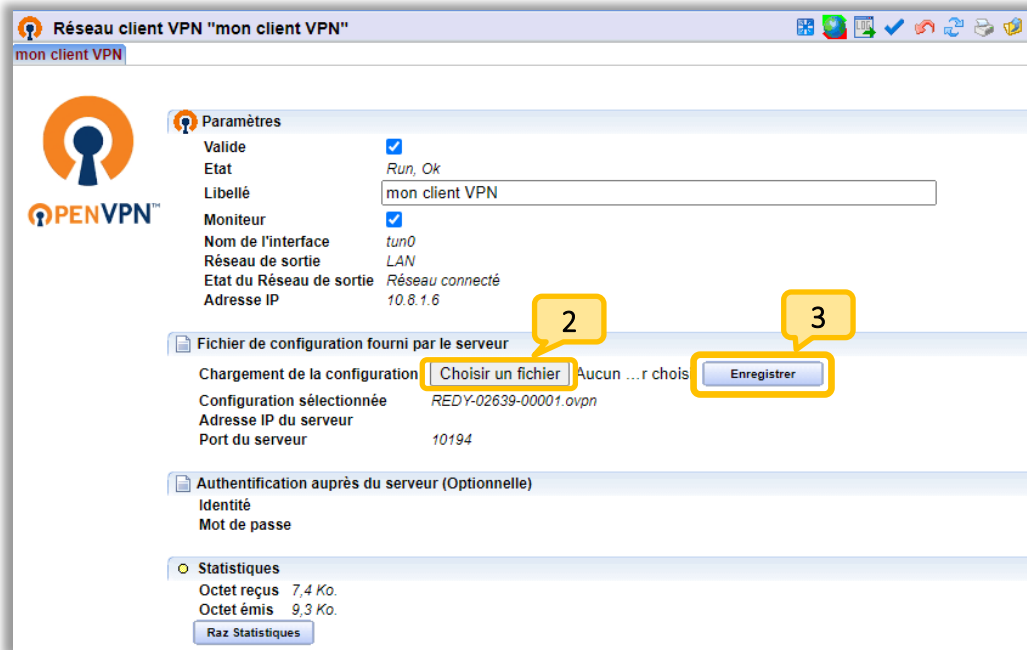


Paramétrage de la connexion

Etape 1 Sur le REDY Serveur, exporter le fichier de configuration :

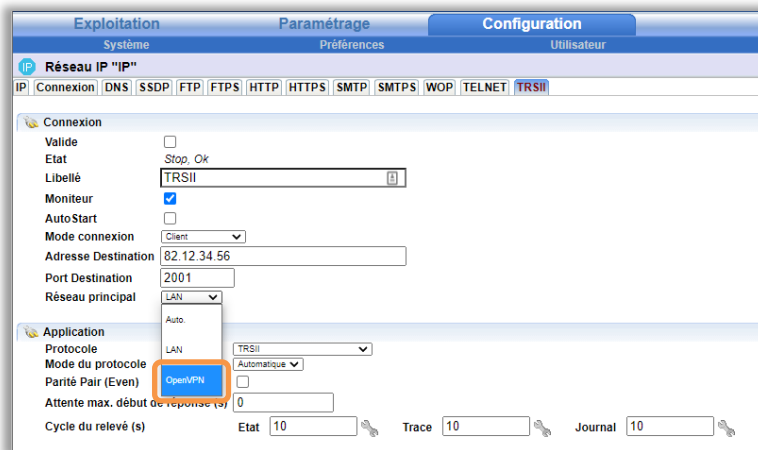


Etape 2 Sur le REDY client, importer le fichier de configuration précédemment exporté :



La connexion s'établit automatiquement.

Etape 3 Il est désormais possible de sélectionner le réseau VPN dans chaque connexion sortantes le nécessitant.
Exemple :

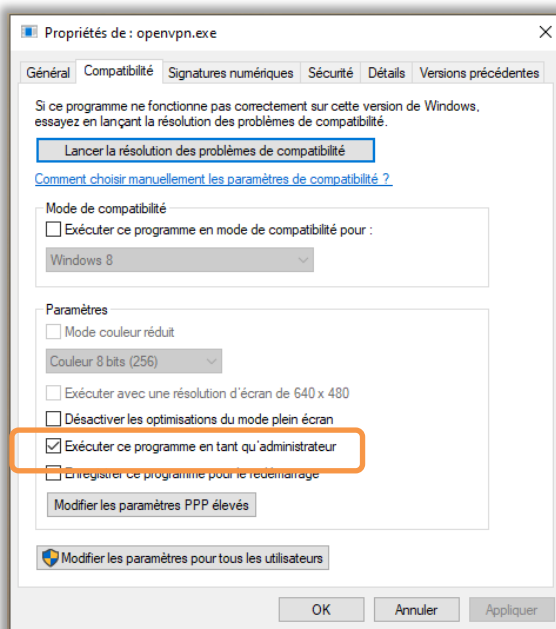


5 Se connecter à un REDY avec un poste de supervision

Pour accéder à l'interface WEB du REDY à travers le VPN, il est possible d'installer sur son PC un client OpenVPN réalisant la connexion au serveur du REDY. Pour cette opération il serait nécessaire d'être **administrateur** de son poste.

Etape 1 Télécharger et installer l'OpenVPN : <https://openvpn.net/community-downloads/>

Etape 2 Programmer l'utilisation du logiciel en tant qu'administrateur en faisant un clic droit et en choisissant **Propriété** sur le fichier openVPN.exe (par défaut *C:\Program Files\OpenVPN\bin*). Puis sélectionner l'onglet **Compatibilité**, enfin cocher **Exécuter ce programme en tant qu'administrateur** :



Etape 3 Lancer le réseau OpenVPN du serveur REDY et exporter le fichier de configuration.


Etape 4 Effectuer un clic droit sur le fichier téléchargé dans le PC et choisir **Start OpenVPN on this config file**. Une fenêtre console apparaît décrivant les étapes de la connexion :

```
2022-01-13 11:40:32 OpenVPN 2.5.0 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [LZ4] [PKCS11] [AEAD] built on Oct 28 2020
2022-01-13 11:40:32 Windows version 10.0 (Windows 10 or greater) 64bit
2022-01-13 11:40:32 library versions: OpenSSL 1.1.1h 22 Sep 2020, LZO 2.10
2022-01-13 11:40:32 WARNING: No server certificate verification method has been enabled. See http://openvpn.net/howto.html#mitm for more info.
2022-01-13 11:40:32 TCP/UDP: Preserving recently used remote address: [AF_INET]81.252.127.66:10194
2022-01-13 11:40:32 UDP link local: (not bound)
2022-01-13 11:40:32 UDP link remote: [AF_INET]81.252.127.66:10194
2022-01-13 11:40:32 [WIT-CA] Peer Connection Initiated with [AF_INET]81.252.127.66:10194
2022-01-13 11:40:32 open_tun
2022-01-13 11:40:32 tap-windows6 device [Connexion au réseau local] opened
2022-01-13 11:40:32 Modified TAP-Windows driver to set a DHCP IP/netmask of 10.8.1.10/255.255.255.252 on interface {8F28802A-A377-4607-82C0-41BACFA82037} [DHCP-serv: 10.8.1.9, lease-time: 31536000]
2022-01-13 11:40:32 Successful ARP Flush on interface [21] {8F28802A-A377-4607-82C0-41BACFA82037}
2022-01-13 11:40:32 IPv4 MTU set to 1500 on interface 21 using SetIpInterfaceEntry()
2022-01-13 11:40:37 Initialization Sequence Completed
```

Etape 5 Le REDY contenant le serveur VPN est désormais accessible à l'adresse IP du réseau VPN créé. C'est-à-dire l'adresse **10.8.1.1** par défaut. Pour stopper la connexion, faire 2 fois Ctrl-C.

6 Dépannage

Le bon fonctionnement de la connexion doit être assuré en respectant les instructions présentes dans ce manuel. Si toutefois des problèmes apparaissent, se reporter au tableau ci-dessous :

Erreur	Cause possible	Solution
Je ne peux pas sélectionner mon fichier de configuration	La coche valide est active	Décocher la coche valider et valider avec le check bleu  .
	Le fichier intégré n'était pas au format .ovpn	Charger un fichier au format .ovpn. Consulter la liste des fichiers chargés dans Configuration/Gestionnaire/Projets.
Je ne peux pas exporter mon fichier de configuration	Utilisation de REDY-PC	Utiliser un REDY de type K7 physique. En effet sans connexion, REDY-PC ne pourra pas recevoir de certificats et donc pas générer de fichier de configuration.
	Certificats non reçus	Attendre entre 5 et 10min pour récupérer les certificats à la première connexion.
Je ne peux plus me connecter en local sur mon REDY	L'adresse du serveur VPN est dans la même zone que le REDY et la connexion s'effectue en UDP	Passer la connexion en TCP à la place de l'UDP dans le fichier de configuration du serveur VPN.
		Faire en sorte que le réseau du serveur VPN soit différent de celui du REDY.
La connexion VPN ne fonctionne pas sur mon REDY serveur	Le port sur la BOX n'est pas ouvert	Effectuer le routage du port concerné sur la BOX.



Pour tout renseignement complémentaire, notre support technique se tient à votre disposition par e-mail à hot-line@wit.fr ou par téléphone au +33 (0)4 93 19 37 30.