IHM Opios

Procédure de configuration des VPN OpenVPN (Road Warrior)

Auteurs :
Hozzy TCHIBINDA

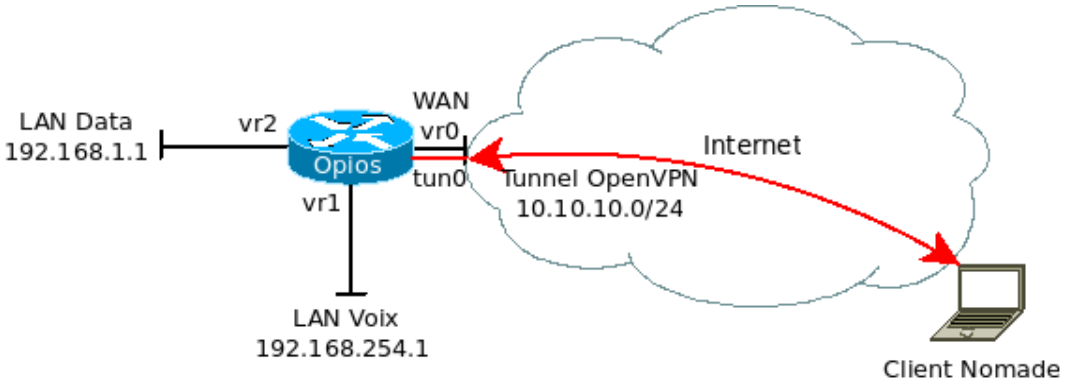
04 Mars 2014
Version 1.3

Table des matières

Présentation

Ce document destiné aux partenaires OpenIP est un guide de configuration d'un VPN pour les clients nomades. Il présente la procédure à suivre afin de mettre en place un tunnel OpenVPN sur un OpIOS via l'IHM.

Voici une architecture illustrant les différentes configurations qui seront mises en place tout au long de ce document :



Architecture d'illustration

Informations pratiques :

- Identifiants (Login/Mdp) du client nomade dans ce document : client/nomade
- Mode d'authentification serveur : accès distant via l'authentification utilisateur.
- Profondeur du certificat : One(Client+Serveur)
- Taille de la clé des certificats dans ce document : 2048.

Les valeurs du mode d'authentification serveur et de la profondeur du certificat doivent toujours être celles indiquées dans les informations pratiques ci-dessus.

Création des certificats

La configuration d'un tunnel OpenVPN via l'IHM commence par la création des certificats suivants :

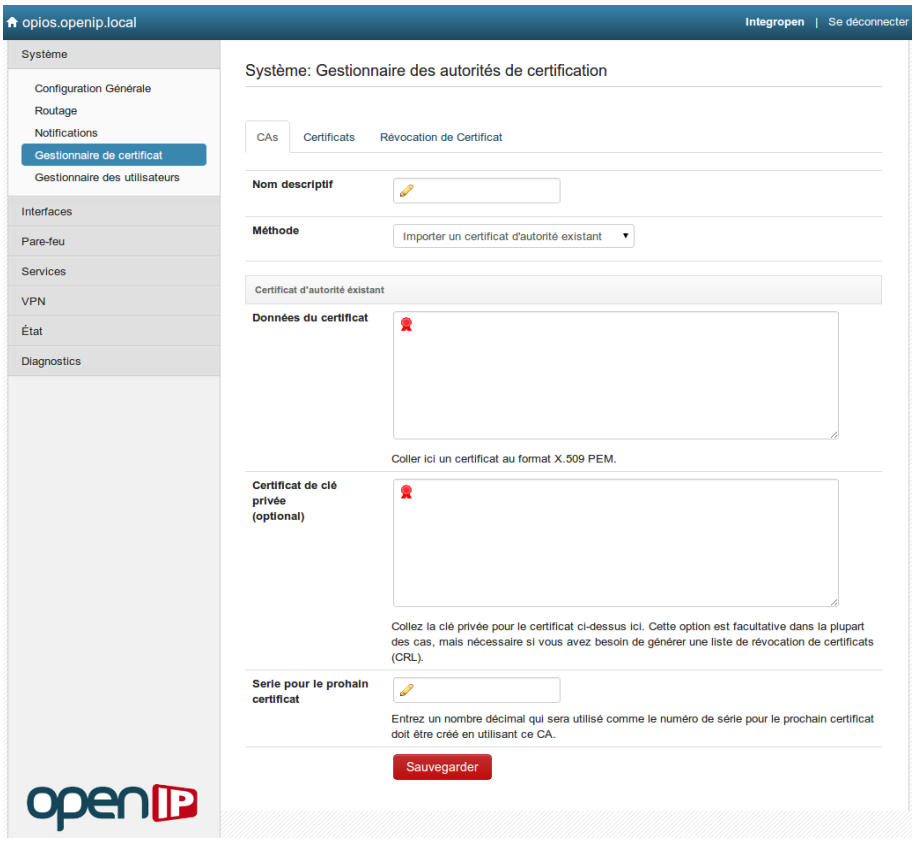
- Certificat de l'autorité de certification,
- Certificat du serveur OpenVPN,
- Certificat du client nomade.

La création du certificat du client nomade se fait lors de la création du compte utilisateur de ce client dans la liste des utilisateurs de l'IHM.
Il est obligtoire de créer le certificat de l'autorité de certification avant tous les autres certificats. De manière générale, l'OpIOS fait office d'autorité de certification.

Il convient de signaler également que lors de l'édition des certificats, la valeur du champ **Nom commun** doit être différente pour chaque certificat créé

2.1 Création du certificat de l'autorité de certification

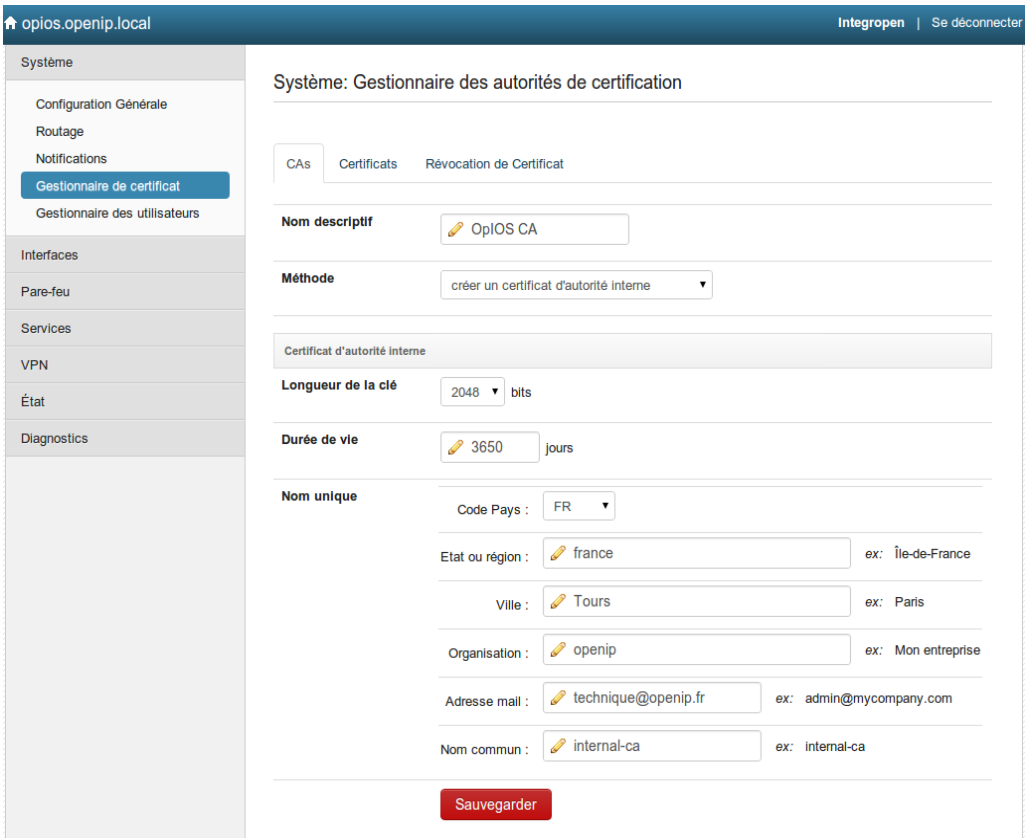
Afin de créer un certificat de l'autotité de certification, il faut cliquer sur ***Système*** $\Longrightarrow$ ***gestionnaire de certificat*** qui redirige sur l'onglet **CAs**. En cliquant sur l'icône , la page suivante s'affiche :



Onglet CAs

La liste déroulante du champ **Methode** présente trois choix possibles, mais à ce jour seules les méthodes **Importer un certificat d'autorité existant** et **Créer un certificat d'autorité interne** sont fonctionnelles.
La première permet de copier un certicat existant ainsi que sa clé privée, tandis que la deuxième permet de créer un nouveau certificat.

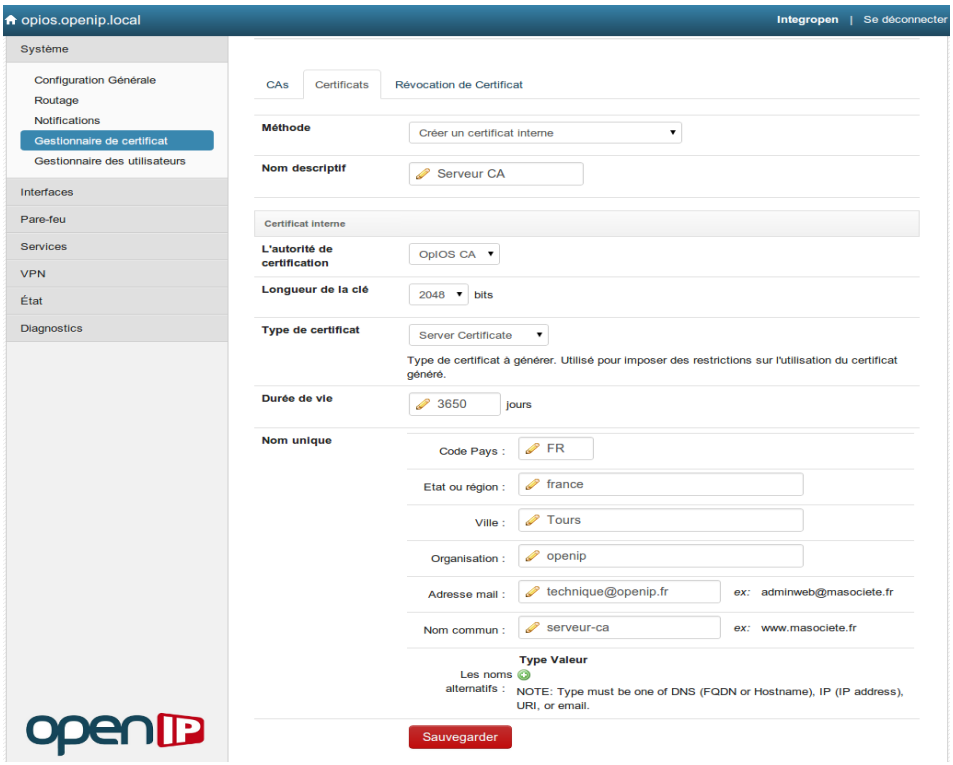
Quelque soit la méthode choisie, saisissez les informations à renseigner et cliquez sur **Sauvegarder** pour valider les modifications éffectuées. Dans ce document, c'est la méthode **Créer un certificat d'autorité interne** qui sera utilisée.
Voici un exemple d'informations renseignées :



Edition d'un nouveau certificat d'autorité de certification

2.2 Création du certificat du serveur OpenVPN

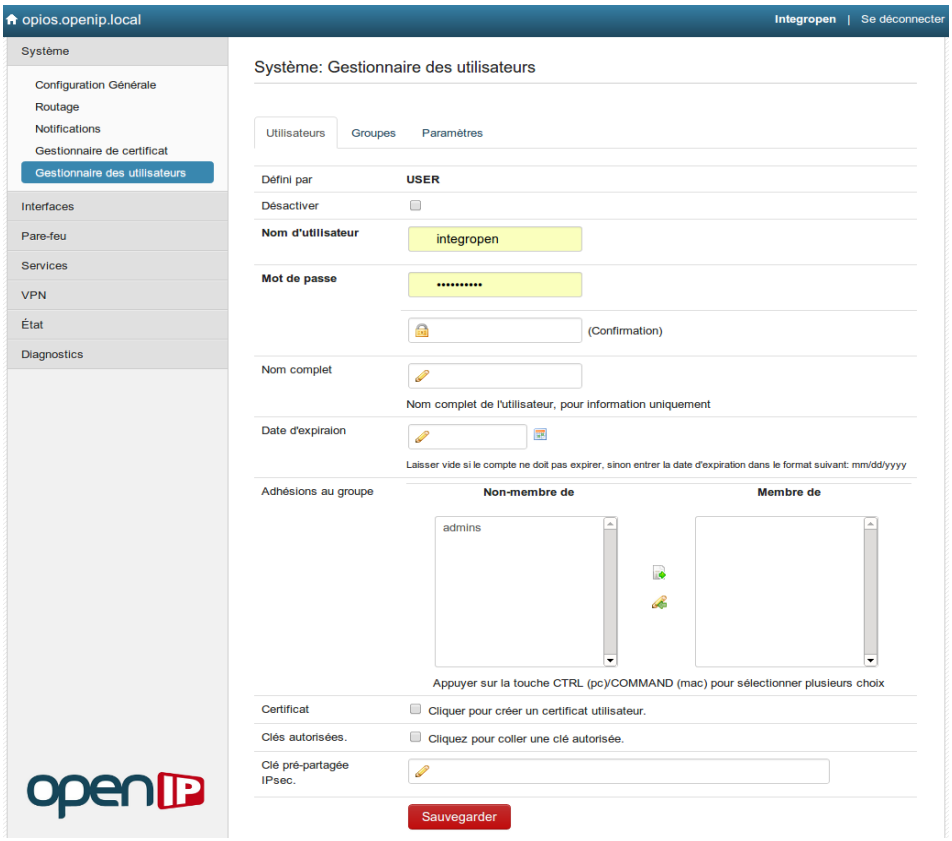
La procédure de création du certificat du serveur est la même que celle du certificat de l'autorité de certification.
Il suffit de cliquer sur l'onglet **Certificats**, ensuite sur l'icône , de selectionner la méthode **Créer un certificat d'autorité interne** et enfin de cliquer sur **Sauvegarder**. Il s'affiche alors une interface simulaire à celle de l'onglet **CAs** à l'exception de la présence de deux nouveaux champs : **L'autorité de certificat** et **Type de certificat**.
Le premier permet de choisir l'autorité de certificat à associer à ce certificat et le second de définir ce certificat comme étant le certificat du serveur OpenVPN. La page se présente de la manière suivante :



Edition d'un nouveau certificat du serveur OpenVPN

2.3 Création du certificat du client nomade

Pour créer le certificat d'un client distant ou nomade sur l'OpIOS, il faut cliquer sur ***Système*** $\Longrightarrow$ ***Gestionnaire des utilisateurs*** qui redirige sur l'onglet **Utilisateurs**. En cliquant sur l'icone , la page suivante s'affiche :



Onglet Utilisateur

Une fois sur cette page, il suffit de renseigner :

- Le nom d'utilisateur du client nomade (**client** d'après les informations pratiques de la page 1) ;
- Le mot de passe (**nomade** d'après les informations pratiques de la page 1).

Et optionnellement

- La date d'expiration ;
- L'adhésion au groupe (Ceci dans le cas où le client est un intégrateur).

Ensuite, il faut cocher la case du champ **Certificat** et renseigner les différentes informations demandées.

En cliquant sur **Sauvegarder**, le certificat du client s'ajoute dans la liste des certificats existants.

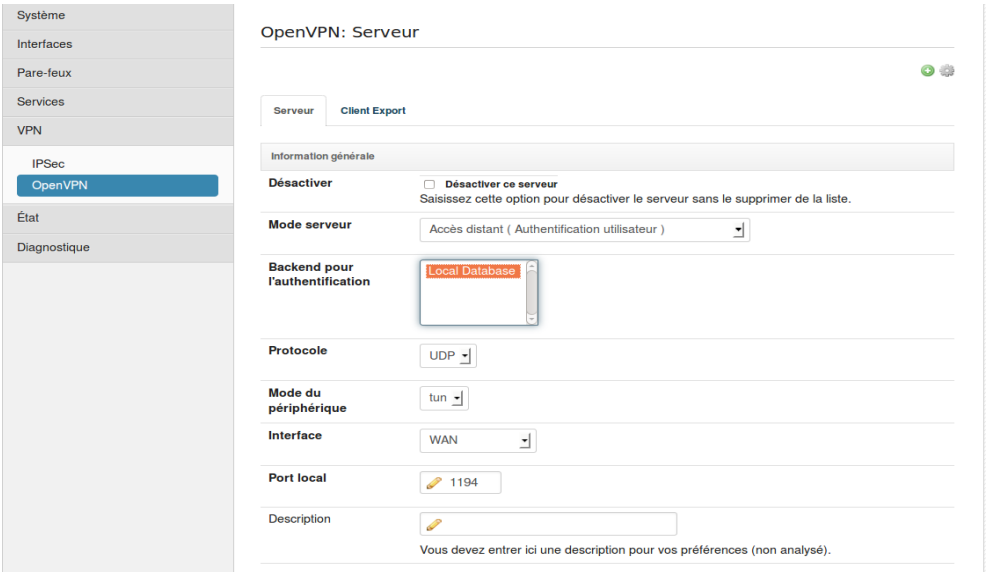
Résumé des certificats créés

Le résumé des certificats existants de l'autorité de certification s'affiche dans l'onglet **CAs**.

Configuration du serveur OpenVPN

Afin de configurer l'OpIOS comme étant un serveur OpenVPN, il faut cliquer sur : ***VPN*** $\Longrightarrow$ ***OpenVPN*** qui affiche par défaut le contenu de l'onglet **Serveur**. En cliquant sur l'icône , une page contenant plusieurs champs regroupés en 5 blocs s'affiche :

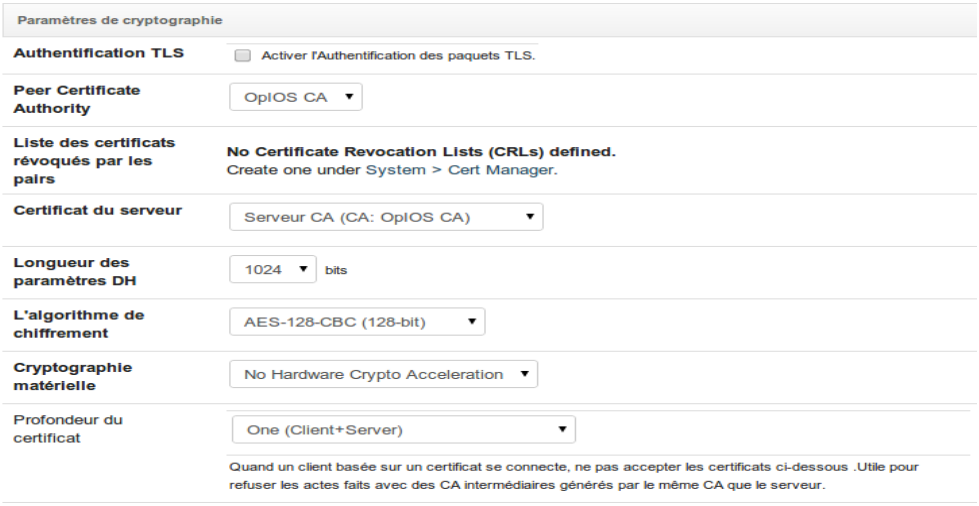
- Informations Générales



Bloc Informations générales

Il faut renseigner dans ce bloc : le mode d'authentification (mode serveur), le protocole de transport à utiliser (UDP ou TCP), le port et l'interface.
Actuellement, le seul mode d'authentification fonctionnel est "Authentification Utilisateur".

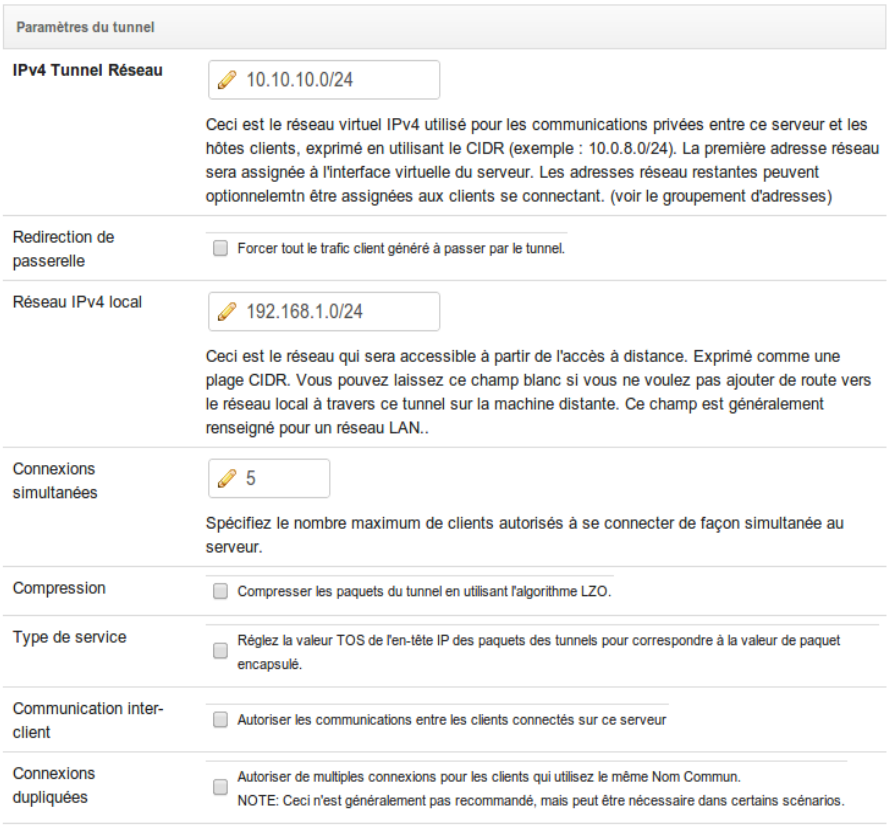
- Paramètres de cryptographie



Bloc Paramètres de cryptographie

Il faut donc décocher le champ **Authentification TLS** car les modes “SSL/TLS + Authentification Utilisateur” et “SSL/TLS” ne sont pas fonctionnels. Ensuite, il faut sélectionnner le certificat de l’autorité de certification et du serveur qui seront utilisés.
Les paramètres du reste des champs de ce bloc dépendent de la demande du client. Si le client n’impose aucun choix, les valeurs par défaut peuvent être conservées.

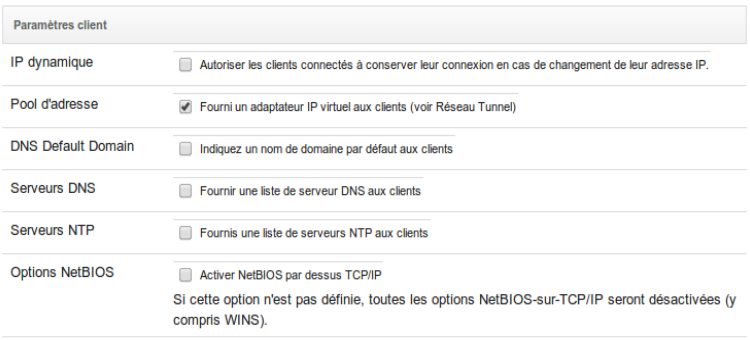
- Paramètres du tunnel.



Bloc Paramètres du tunnel

Dans ce bloc, les 3 champs à renseigner par défaut sont :
IPv4 Tunnel Réseau correspondant au réseau virtuel, **Réseau IPV4 local** correspondant au réseau privé qui sera accessible à travers le tunnel, et **Connexions simultanées** correspondant au nombre de clients nomades pouvant acceder simultanement au serveur OpenVPN.
La configuration des autres champs dépend de la demande du client.

- Paramètres client



Bloc Paramètres du client

Le seul champ à paramétrer par défaut dans ce bloc est “Pool adresse”, tout le reste dépend de la demande du client.

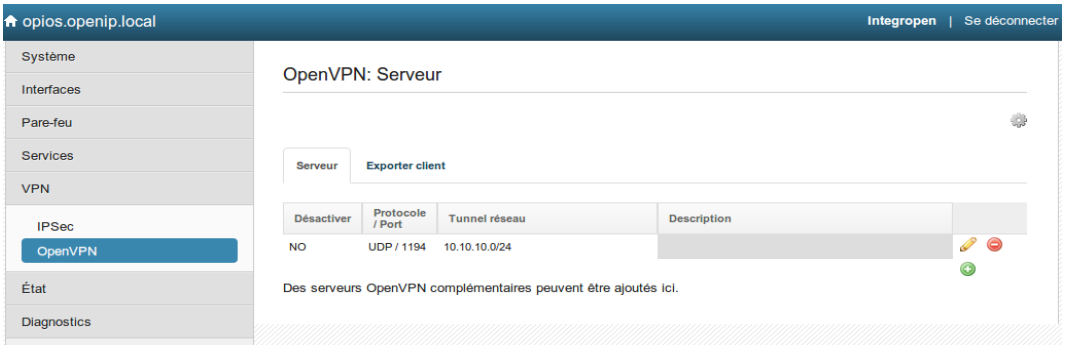
- Configuration avancée

Bloc Paramètres avancés

Ce bloc permet d'ajouter un ou plusieurs réseaux locaux que l'on souhaite rendre accessibles depuis le tunnel OpenVPN.

Une fois la configuration terminée, il faut cliquer sur **Sauvegarder**.

L'onglet **Serveur** devient alors :



Résumé configuration serveur

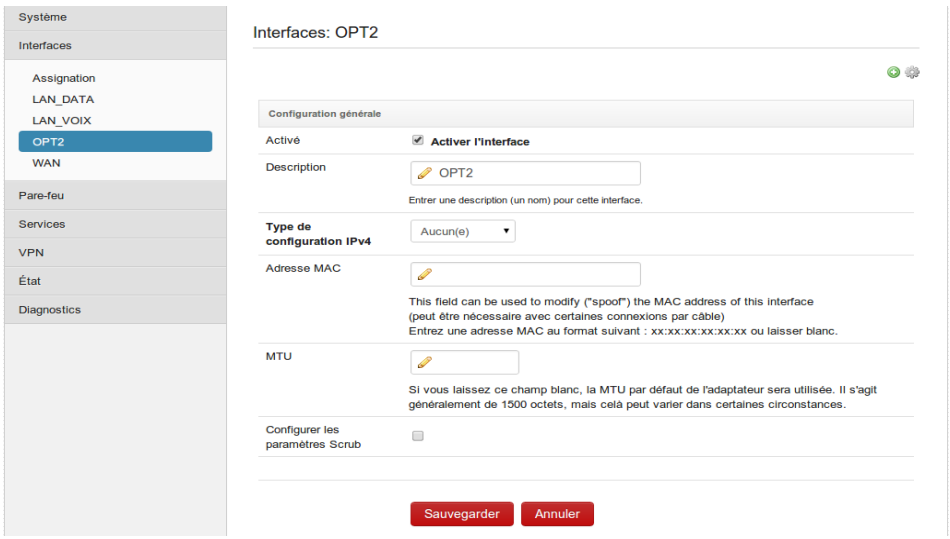
Activation de l'interface

La validation de la configuration d'un serveur OpenVPN telle que présentée dans le chapitre 3 crée une interface virtuelle **tun1** disponible sur ***Interface*** $\Longrightarrow$ ***Assignation***. Cette interface doit être activée afin d'avoir un tunnel OpenVPN opérationnel et sur lequel on peut appliquer des règles de filtrage.

La procédure d'activation de l'interface **tun1** est la même que celle des interfaces classiques, c'est-à-dire qu'il suffit de l'associer à une interface logique comme le montre la figure ci-dessous :

Interface tun1 **associée à l'interface l'ogique** ***OPT2***

Ensuite,cliquer sur **OPT2** et cocher la case **Activer l'interface** du champ **Activé**. La page suivante s'affiche :



Activation interface OPT2

Remarquez qu'il est possible de modifier le nom de l'interface logique en mettant par exemple OPENVPN dans le champ **Description**.
Enfin, valider cette modification en cliquant sur **Sauvegarder** et **Appliquer les changements**.

Après l'activation de l'interface **OPT2** ou **OPENVPN**, il faut définir dans ***Pare-feu*** $\Longrightarrow$ ***Règles*** $\Longrightarrow$ Onglet **OPT2** les règles de filtrage à appliquer sur le trafic passant sur cette interface. A titre d'exemple dans ce document, tous les trafics seront autorisés.

Création des fichiers de configuration du client

5.1 Revalidation de la configuration du serveur

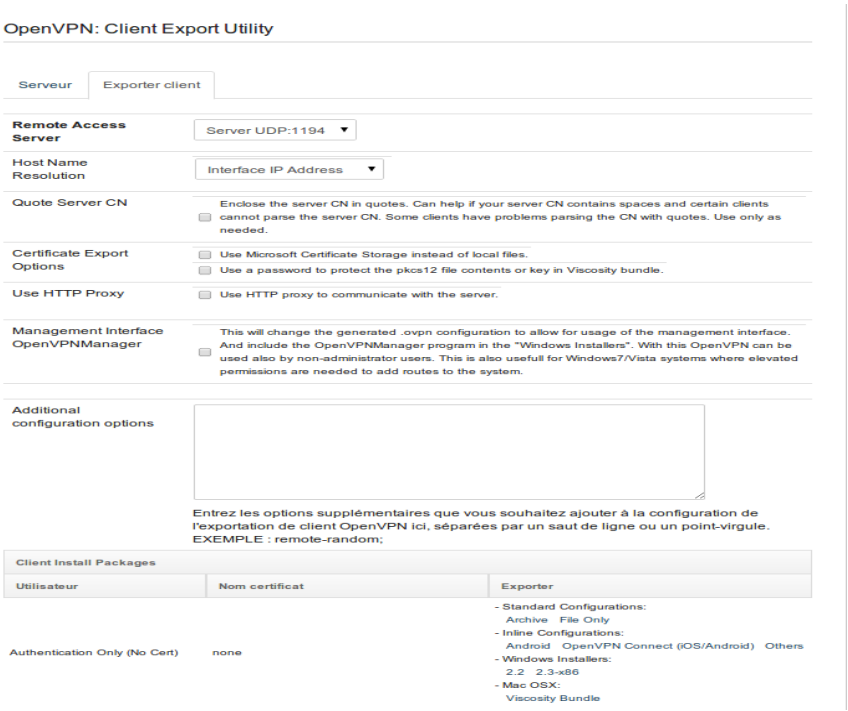
Après l'activation de l'interface tun1, il est obligatoire de revalider la configuration du serveur OpenVPN sans y porter de modifications. Il suffit juste de cliquer sur ***VPN*** $\Longrightarrow$ ***OpenVPN*** qui affiche l'interface suivante :

Revalidation de la configuration

Ensuite cliquer sur l'icône jaune (en forme de crayon) et enfin sur **Sauvegarder**.

5.2 Récupération de la configuration du client nomade

Les clients nomades doivent avoir la configuration correspondant à celle du serveur OpenVPN afin d'utiliser le tunnel. A cet effet, l'onglet ***VPN*** $\Longrightarrow$ ***OpenVPN*** $\Longrightarrow$ **Client Export** permet de générer tous les fichiers utiles au client et qui sont téléchargeables dans le bloc "Client Install Packages" de l'onglet **Client Export** suivant :



Onglet Export Client

Cinq types de fichiers correspondant chacun au type d'OS (linux, Windows, Mac et Autres) utilisé par le client sont disponibles.

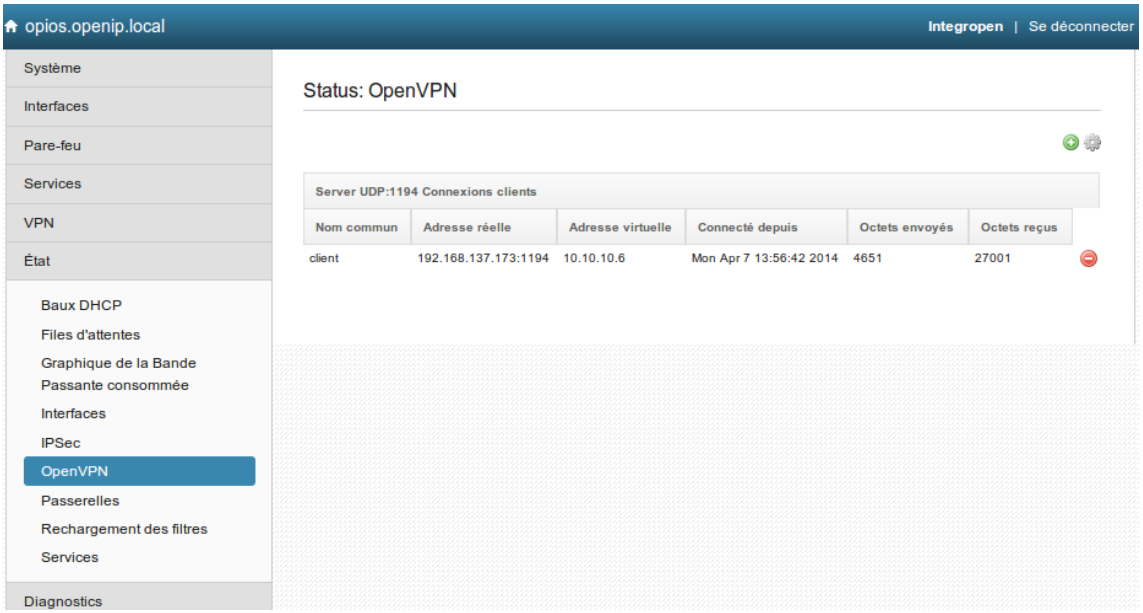
Actuellement les tests n'ont été effectués que sur les plateformes :

- Windows en utilisant les installeurs(fichiers) soit **2.2**, soit **2.3-x86** (cela dépend de l'architecture de l'ordinateur client)
- Linux en utilisant le fichier archivé du lien **File Only**.

Il est possible d'éffectuer plusieurs autres opérations sur ces fichiers mais cela dépend de la demande du client OpenIP. Si aucune demande n'est spécifiée, la configuration par défaut suffit pour faire fonctionner le tunnel.

Une fois le client OpenVPN lancé sur le poste distant, il faut :

- Sur les PC Windows, s'assurer que le lancement d'OpenVPN a été fait avec les droits administrateur.
- Ensuite sur l'OpIOS, vérifier que le tunnel est bien monté en cliquant sur l'onglet ***Etat*** $\Longrightarrow$ ***OpenVPN***. La page suivante s'affiche :



Etat tunnels OpenVPN