



IHM Opios

Procédure de configuration des VPN OpenVPN (Road Warrior)

Auteurs :
Hozzy TCHIBINDA

04 Mars 2014
Version 1.3

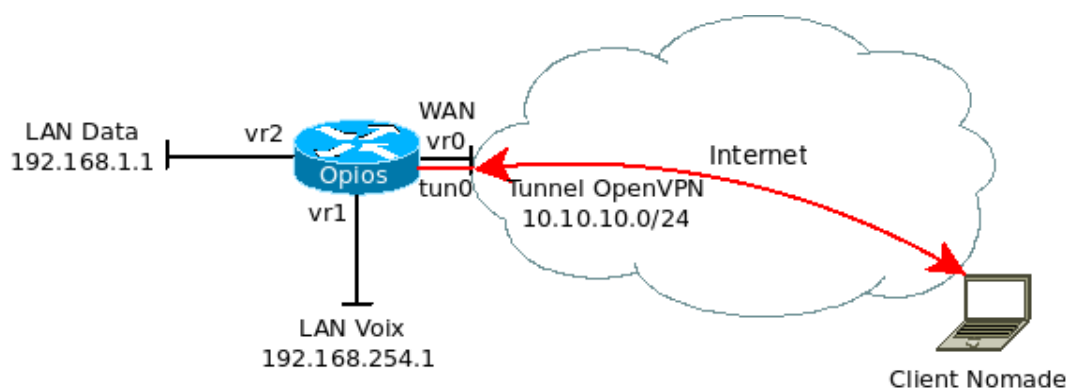
Table des matières

1	Présentation	2
2	Création des certificats	3
2.1	Création du certificat de l'autorité de certification	3
2.2	Création du certificat du serveur OpenVPN	4
2.3	Création du certificat du client nomade	5
3	Configuration du serveur OpenVPN	7
4	Activation de l'interface	10
5	Création des fichiers de configuration du client	12
5.1	Revalidation de la configuration du serveur	12
5.2	Récupération de la configuration du client nomade	12

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.

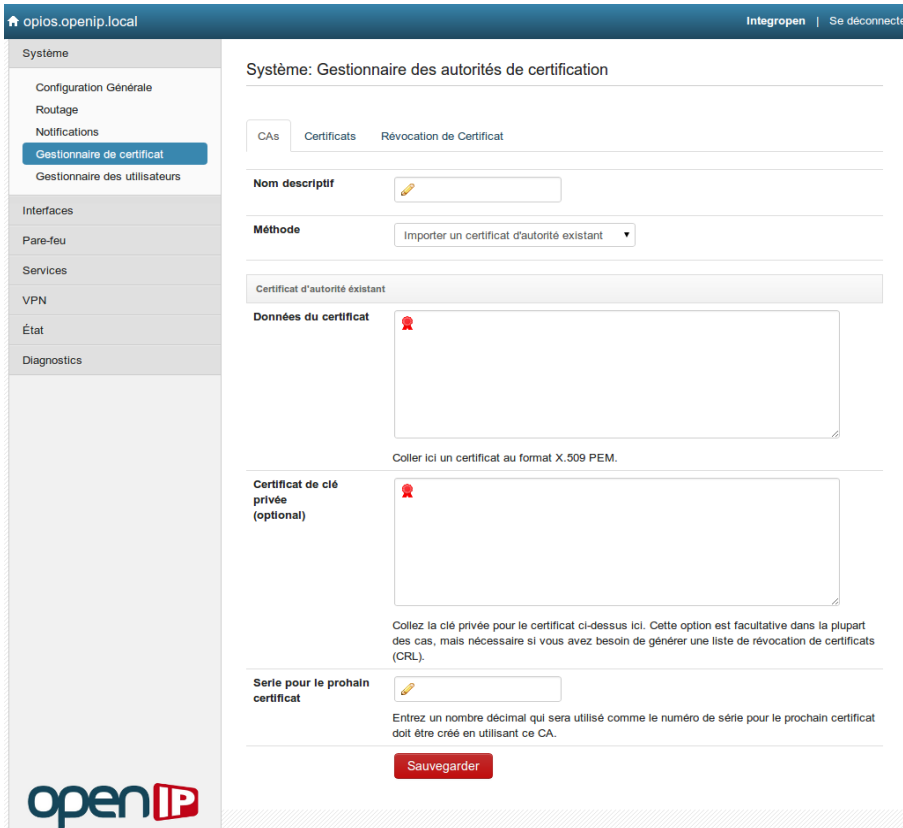
La création du certificat du client nomade se fait lors de la création du compte utilisateur de ce client dans la liste des utilisateurs de l'IHM.

Il est obligatoire 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'autorité de certification, il faut cliquer sur *Système* \Rightarrow *gestionnaire de certificat* qui redirige sur l'onglet **CAs**. En cliquant sur l'icône , la page suivante s'affiche :



opios.openip.local Integropen | Se déconnecter

Système

- Configuration Générale
- Routage
- Notifications
- Gestionnaire de certificat**
- Gestionnaire des utilisateurs

Interfaces

- Pare-feu
- Services
- VPN
- État
- Diagnostics


Système: Gestionnaire des autorités de certification

CAs Certificats Révocation de Certificat


Nom descriptif

Méthode Importer un certificat d'autorité existant

Certificat d'autorité existant

Données du certificat 

Coller ici un certificat au format X.509 PEM.


Certificat de clé privée (optional) 

Collez la clé privée pour le certificat ci-dessus ici. Cette option est facultative dans la plupart des cas, mais nécessaire si vous avez besoin de générer une liste de révocation de certificats (CRL).

Série pour le prochain certificat

Entrez un nombre décimal qui sera utilisé comme le numéro de série pour le prochain certificat doit être créé en utilisant ce CA.

Sauvegarder



Onglet CAs

La liste déroulante du champ **Méthode** 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 certificat 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 effectuées. Dans ce document, c'est la méthode **Créer un certificat d'autorité interne** qui sera utilisée.


Voici un exemple d'informations renseignées :

The screenshot shows the 'Gestionnaire de certificat' interface. The left sidebar contains a navigation menu with categories: 'Système' (Configuration Générale, Routage, Notifications, Gestionnaire de certificat, Gestionnaire des utilisateurs), 'Interfaces' (Pare-feu, Services, VPN, État, Diagnostics), and 'Diagnostics'. The main content area is titled 'Système: Gestionnaire des autorités de certification' and has three tabs: 'CAs', 'Certificats', and 'Révocation de Certificat'. The 'Certificats' tab is active. The form fields are as follows: 'Nom descriptif' (OplOS CA), 'Méthode' (créer un certificat d'autorité interne), 'Longueur de la clé' (2048 bits), 'Durée de vie' (3650 jours), and 'Nom unique' (Code Pays: FR, Etat ou région: france, Ville: Tours, Organisation: openip, Adresse mail: technique@openip.fr, Nom commun: internal-ca). A 'Sauvegarder' button is at the bottom.

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 sélectionner la méthode **Créer un certificat d'autorité interne** et enfin de cliquer sur **Sauvegarder**. Il s'affiche alors une interface similaire 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 :

The screenshot shows the 'Certificats' tab in the OpenVPN web interface. The left sidebar contains a menu with 'Gestionnaire de certificat' highlighted. The main content area is titled 'Certificats' and 'Révocation de Certificat'. The 'Méthode' is set to 'Créer un certificat interne'. The 'Nom descriptif' is 'Serveur CA'. The 'L'autorité de certification' is 'OpiOS CA'. The 'Longueur de la clé' is '2048 bits'. The 'Type de certificat' is 'Server Certificate'. The 'Durée de vie' is '3650 jours'. The 'Nom unique' section includes fields for 'Code Pays' (FR), 'Etat ou région' (france), 'Ville' (Tours), 'Organisation' (openip), 'Adresse mail' (technique@openip.fr), and 'Nom commun' (serveur-ca). A 'Sauvegarder' button is at the bottom.

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 **Systeme** \Rightarrow **Gestionnaire des utilisateurs** qui redirige sur l'onglet **Utilisateurs**. En cliquant sur l'icone , la page suivante s'affiche :

The screenshot shows the 'Utilisateurs' tab in the OpenVPN web interface. The left sidebar contains a menu with 'Gestionnaire des utilisateurs' highlighted. The main content area is titled 'Systeme: Gestionnaire des utilisateurs'. The 'Utilisateurs' tab is selected. The 'Défini par' is 'USER'. The 'Nom d'utilisateur' is 'integropen'. The 'Mot de passe' is masked with dots. The 'Nom complet' is empty. The 'Date d'expiration' is empty. The 'Adhésions au groupe' section shows 'Non-membre de' and 'Membre de' lists. The 'Certificat' checkbox is unchecked. The 'Clés autorisées' checkbox is unchecked. The 'Clé pré-partagée IPsec' is empty. A 'Sauvegarder' button is at the bottom.

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** \implies **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 "Authentication 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 sélectionner 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.

Paramètres du tunnel	
IPv4 Tunnel Réseau	<input type="text" value="10.10.10.0/24"/> <small>Ceci est le réseau virtuel IPv4 utilisé pour les communications privées entre ce serveur et les hôtes clients, exprimé en utilisant le CIDR (exemple : 10.0.8.0/24). La première adresse réseau sera assignée à l'interface virtuelle du serveur. Les adresses réseau restantes peuvent optionnellement être assignées aux clients se connectant. (voir le groupement d'adresses)</small>
Redirection de passerelle	<input type="checkbox"/> Forcer tout le trafic client généré à passer par le tunnel.
Réseau IPv4 local	<input type="text" value="192.168.1.0/24"/> <small>Ceci est le réseau qui sera accessible à partir de l'accès à distance. Exprimé comme une plage CIDR. Vous pouvez laisser ce champ blanc si vous ne voulez pas ajouter de route vers le réseau local à travers ce tunnel sur la machine distante. Ce champ est généralement renseigné pour un réseau LAN..</small>
Connexions simultanées	<input type="text" value="5"/> <small>Spécifiez le nombre maximum de clients autorisés à se connecter de façon simultanée au serveur.</small>
Compression	<input type="checkbox"/> Compresser les paquets du tunnel en utilisant l'algorithme LZO.
Type de service	<input type="checkbox"/> Réglez la valeur TOS de l'en-tête IP des paquets des tunnels pour correspondre à la valeur de paquet encapsulé.
Communication inter-client	<input type="checkbox"/> Autoriser les communications entre les clients connectés sur ce serveur
Connexions dupliquées	<input type="checkbox"/> Autoriser de multiples connexions pour les clients qui utilisent le même Nom Commun. <small>NOTE: Ceci n'est généralement pas recommandé, mais peut être nécessaire dans certains scénarios.</small>

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 accéder simultanément au serveur OpenVPN.

La configuration des autres champs dépend de la demande du client.

- Paramètres client

Paramètres client	
IP dynamique	<input type="checkbox"/> Autoriser les clients connectés à conserver leur connexion en cas de changement de leur adresse IP.
Pool d'adresse	<input checked="" type="checkbox"/> Fournir un adaptateur IP virtuel aux clients (voir Réseau Tunnel)
DNS Default Domain	<input type="checkbox"/> Indiquez un nom de domaine par défaut aux clients
Serveurs DNS	<input type="checkbox"/> Fournir une liste de serveur DNS aux clients
Serveurs NTP	<input type="checkbox"/> Fournir une liste de serveurs NTP aux clients
Options NetBIOS	<input type="checkbox"/> Activer NetBIOS par dessus TCP/IP <small>Si cette option n'est pas définie, toutes les options NetBIOS-sur-TCP/IP seront désactivées (y compris WINS).</small>

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

Configuration avancée

Avancé

```
push "route 192.168.254.0 255.255.255.0";
```

Saisissez ici toutes les options complémentaires que vous souhaitez ajouter à votre serveur OpenVPN, les valeurs doivent être séparés par un point-virgule
EXEMPLE : push "route 10.0.0.0 255.255.255.0";

Sauvegarder

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 :

The screenshot shows the 'OpenVPN: Serveur' configuration summary page. On the left is a navigation menu with categories: Système, Interfaces, Pare-feu, Services, VPN, IPsec, État, and Diagnostics. The 'VPN' category is expanded, and 'OpenVPN' is selected. The main content area shows the 'OpenVPN: Serveur' title and a 'Serveur' tab. Below the tab is a table with the following data:

Désactiver	Protocole / Port	Tunnel réseau	Description
NO	UDP / 1194	10.10.10.0/24	

Below the table, there is a note: 'Des serveurs OpenVPN complémentaires peuvent être ajoutés ici.' and a green plus icon.

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** \implies **Assignment**. 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	Port Réseau
WAN	vr0 (00:0d:b9:2e:39:10)
LAN_DATA	vr2 (00:0d:b9:2e:39:12)
LAN_VOIX	vr1 (00:0d:b9:2e:39:11)
OPT2	tun1 (0)

Les interfaces qui sont configurées comme membre d'une interface lagg(4) ne seront pas montrées.

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

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

Configuration générale

Activé **Activer l'interface**

Description
Entrer une description (un nom) pour cette interface.

Type de configuration IPv4

Adresse MAC
This field can be used to modify ("spoof") the MAC address of this interface (peut être nécessaire avec certaines connexions par câble)
 Entrez une adresse MAC au format suivant : xx:xx:xx:xx:xx:xx ou laisser blanc.

MTU
Si vous laissez ce champ blanc, la MTU par défaut de l'adaptateur sera utilisée. Il s'agit généralement de 1500 octets, mais cela peut varier dans certaines circonstances.

Configurer les paramètres Scrub

Sauvegarder **Annuler**

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* \Rightarrow *Règles* \Rightarrow 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** \implies **OpenVPN** qui affiche l'interface suivante :

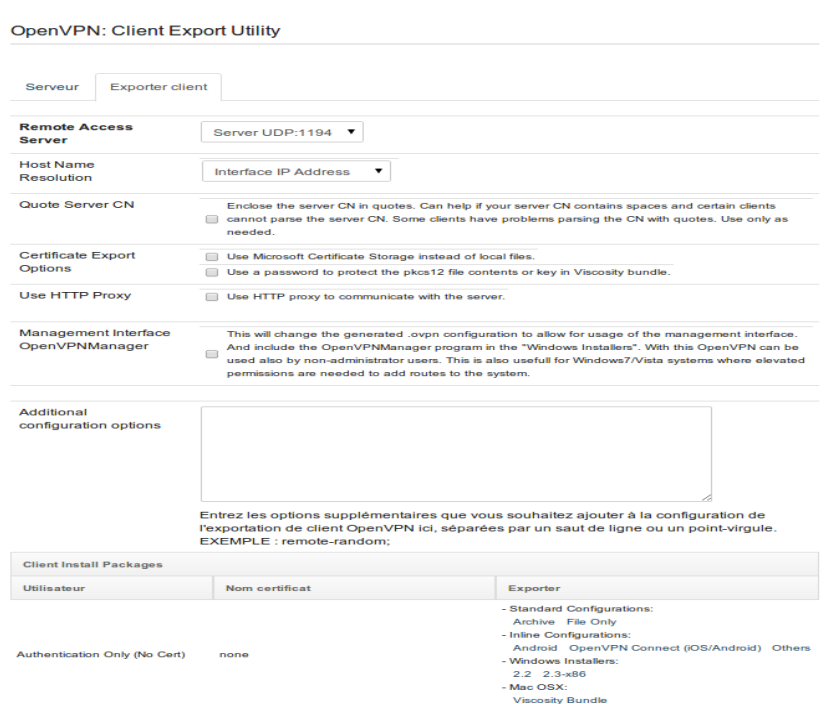


Revalidation de la configuration

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** \implies **OpenVPN** \implies **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 installateurs(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'effectuer 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** \implies **OpenVPN**. La page suivante s'affiche :

Server UDP:1194 Connexions clients					
Nom commun	Adresse réelle	Adresse virtuelle	Connecté depuis	Octets envoyés	Octets reçus
client	192.168.137.173:1194	10.10.10.6	Mon Apr 7 13:56:42 2014	4651	27001

Etat tunnels OpenVPN