



IHM Opios

Procédure de configuration des VPN IPSec (Site à Site)

Auteur :
Hozzy TCHIBINDA

03 Mars 2014
Version 1.1

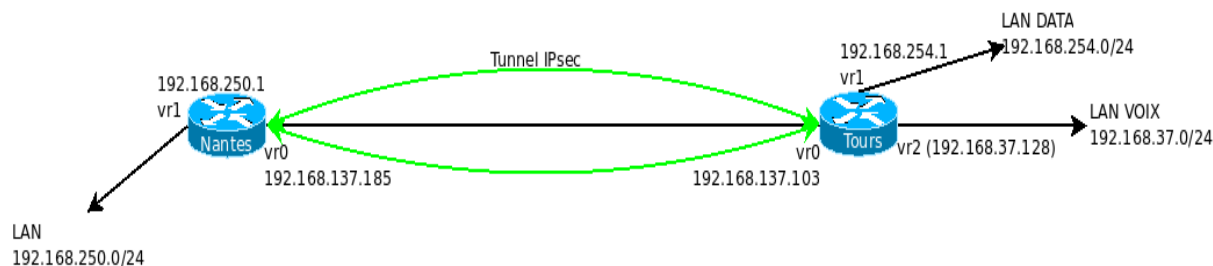
Table des matières

1	Présentation	2
2	Configuration du Tunnel IPSec	3
3	Création des règles de Pare-feu	6

Présentation

Ce document destiné au Support Technique et aux partenaires présente la procédure à suivre afin de configurer un tunnel IPSec (site à site) sur un OpIOS via l'IHM.

La figure ci-dessous présente l'architecture qui sera mise en place dans ce document.



Architecture d'illustration

Il est question de créer un tunnel VPN entre le LAN 192.168.250.0/24 et les LAN 192.168.254.0/24, 192.168.37.0/24.

Informations pratiques :

- Il faut toujours utiliser **ESP** comme protocole d'encapsulation
- A titre d'exemple, les valeurs des champs "**L'algorithme de chiffrement**", "**L'algorithme du hash**", "**Groupe de clef DH**" et "**Groupe de clef PFS**" seront respectivement 3DES, SHA1, 2(1024) et 2(1024). Elles concernent les deux phases IKE.
- La clé partagée sera **nantestours**.

Configuration du Tunnel IPSec

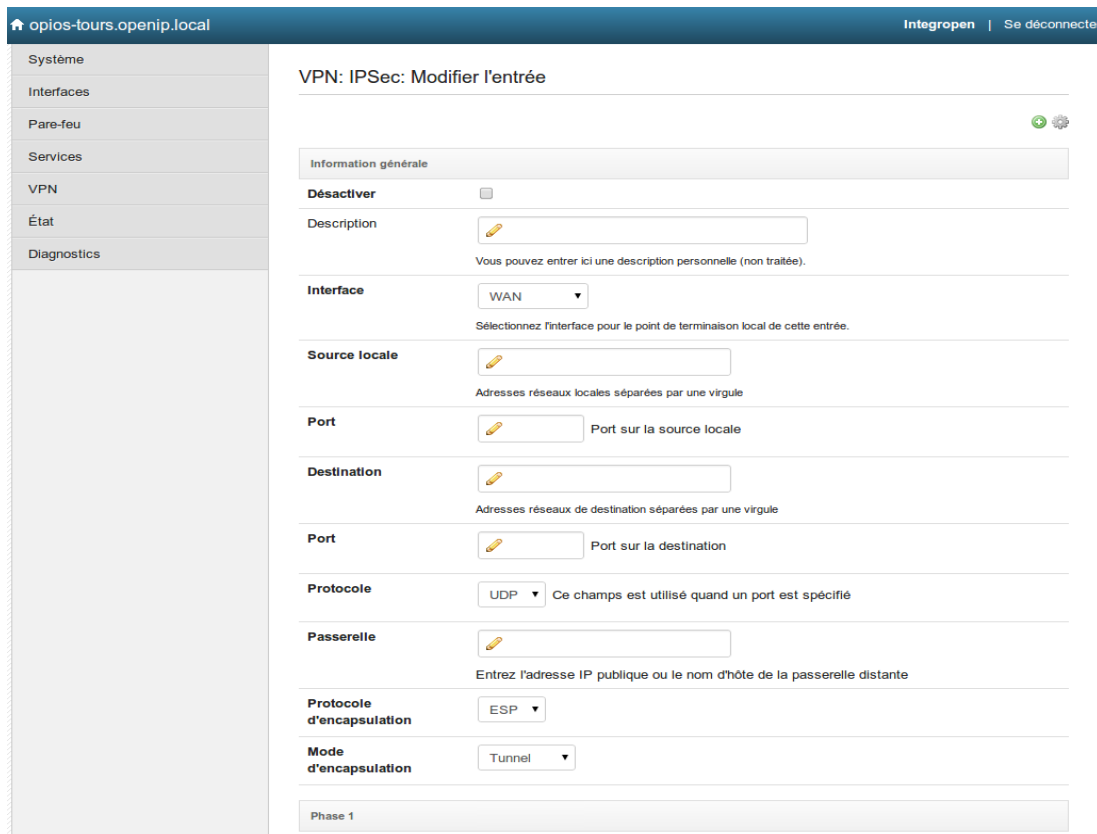
Pour créer un Tunnel IPSec, il faut que les deux routeurs qui servent de passerelles aient les mêmes paramètres cryptographiques afin de permettre la réussite des phases de négociation 1 et 2.

Afin de configurer IPSec sur l'OpIOS via l'IHM, il faut cliquer sur : **VPN** \Rightarrow **IPSec**, la page suivante s'affiche :



Page d'accueil IPSec configuration

Il faut ensuite cliquer sur l'icône  et la page suivante apparaît :



Configuration Générale IPSec

C'est sur cette page qu'il faut saisir les informations sur les Réseaux et les passerelles concernées par ce Tunnel VPN IPSec, ainsi que celles sur le protocole et le mode d'encapsulation de ce Tunnel.

Comme le présente la figure ci-dessus :


- Le champ **Source Locale** correspond aux réseaux locaux directement connectés au routeur de Tours.
- Le champ **Destination** correspond au réseau local du routeur distant (Nantes selon l'architecture d'illustration).
- Les champs **Port** permettent de spécifier si nécessaire, le type de service que l'on souhaite encapsuler. Il est à laisser vide dans le cas de l'architecture d'illustration de ce document.
- Lorsque les ports ont été saisis dans les champs précédents, il est impératif de sélectionner dans le champ **Protocole**, le protocole de transport supportant le service qui correspond aux numéros des ports. Cependant, sans ports ce champ n'a aucune importance ou influence. De manière générale, il faut sélectionner le protocole UDP.
- Sélectionner dans le champ **Interface**, l'interface WAN qui correspond au point de terminaison local du Tunnel.
- Sélectionner **ESP** comme protocole d'encapsulation dans le champ **Protocole d'encapsulation**.
- Garder le mode d'encapsulation par défaut du champ **Mode d'encapsulation**.
- Saisir l'IP de la passerelle dans le champ **Passerelle**. En considérant l'architecture d'illustration, il faut saisir 192.168.137.184 sur le routeur de Tours et 192.168.137.103 sur celui de Nantes.

Remarque importante :

Il est possible de saisir plusieurs adresses réseaux dans les champs **Source Locale** et **Destination** de la partie **Information Générale**. Pour le faire, il suffit de séparer sans espacement chaque adresse réseau déclarée des autres adresses réseaux par une virgule.


En considérant l'architecture d'illustration, sur le routeur de Tours le champ **Destination** aura pour valeur 192.168.250.0/24 et le champ **Source Locale** aura 192.1168.37.0/24,192.168.254.0/24.

Cependant, sur le routeur de Nantes le champ **Source Locale** aura pour valeur 192.168.250.0/24 et le champ **Destination** aura 192.1168.37.0/24,192.168.254.0/24 pour valeur.

La figure ci-dessous est la suite de la page présentée dans la figure **Configuration Générale IPSec** qui a été ouverte en cliquant sur l'icône  dans la figure **Page d'accueil IPSec configuration** :

Phase 1	
Méthode d'authentification	PSK <input type="text"/>
	<small>Doit correspondre à la position choisie sur le côté opposé.</small>
Mode de négociation	main <input type="text"/>
	<small>Agressif est plus souple, mais moins sécurisé.</small>
Mon identificateur	My IP address <input type="text"/>
Identificateur Peer	Peer IP address <input type="text"/>
La clé pré-partagée	<input type="text"/>
	<small>Entrez votre chaîne de la clé pré-partagée.</small>
L'algorithme de chiffrement	DES <input type="text"/>
L'algorithme du HASH	MD5 <input type="text"/>
	<small>Doit correspondre à la position choisie sur le côté opposé.</small>
Groupe de clé DH	1 (768 bit) <input type="text"/>
	<small>Doit correspondre à la position choisie sur le côté opposé.</small>
Phase 2	

Configuration IPSec de la Phase 1 IKE

Dans le cadre défini dans ce document, les paramètres cryptographiques par défaut vont être remplacés par ceux indiqués dans le chapitre 1. Il faut également saisir la clé partagée dans le champ **La clé pré-partagée**. Ensuite, configurer la phase 2 (figure ci-dessous) dans la suite de la page présentée dans la figure **Configuration IPSec de la phase 1 IKE** qui a été ouverte en cliquant sur  dans la figure **Page d'accueil IPSec configuration** :

Phase 2

Algorithme d'encryption

Indice : Utilisez 3DES pour une meilleure compatibilité ou si vous avez une carte matérielle avec accélération cryptographique. Blowfish est généralement le chiffrement logiciel le plus rapide..

Algorithmes de HASH

Groupe de clé PFS

Tag

Sauvegarder

Configuration IPSec de la Phase 2

A l'instar de la phase 1, les paramètres cryptographiques indiqués dans le chapitre 1 de ce document sont également à considérer pour la phase 2.

Après avoir effectué la configuration suivant les données de l'architecture d'illustration (chapitre 1), il faut cliquer sur **Sauvegarder** et **Appliquer les changements** pour valider la configuration. La page suivante s'affiche :




Passerelle distante	Source locale	Destination
WAN 192.168.137.184	192.168.254.0/24,192.168.37.0/24	192.168.250.0/24

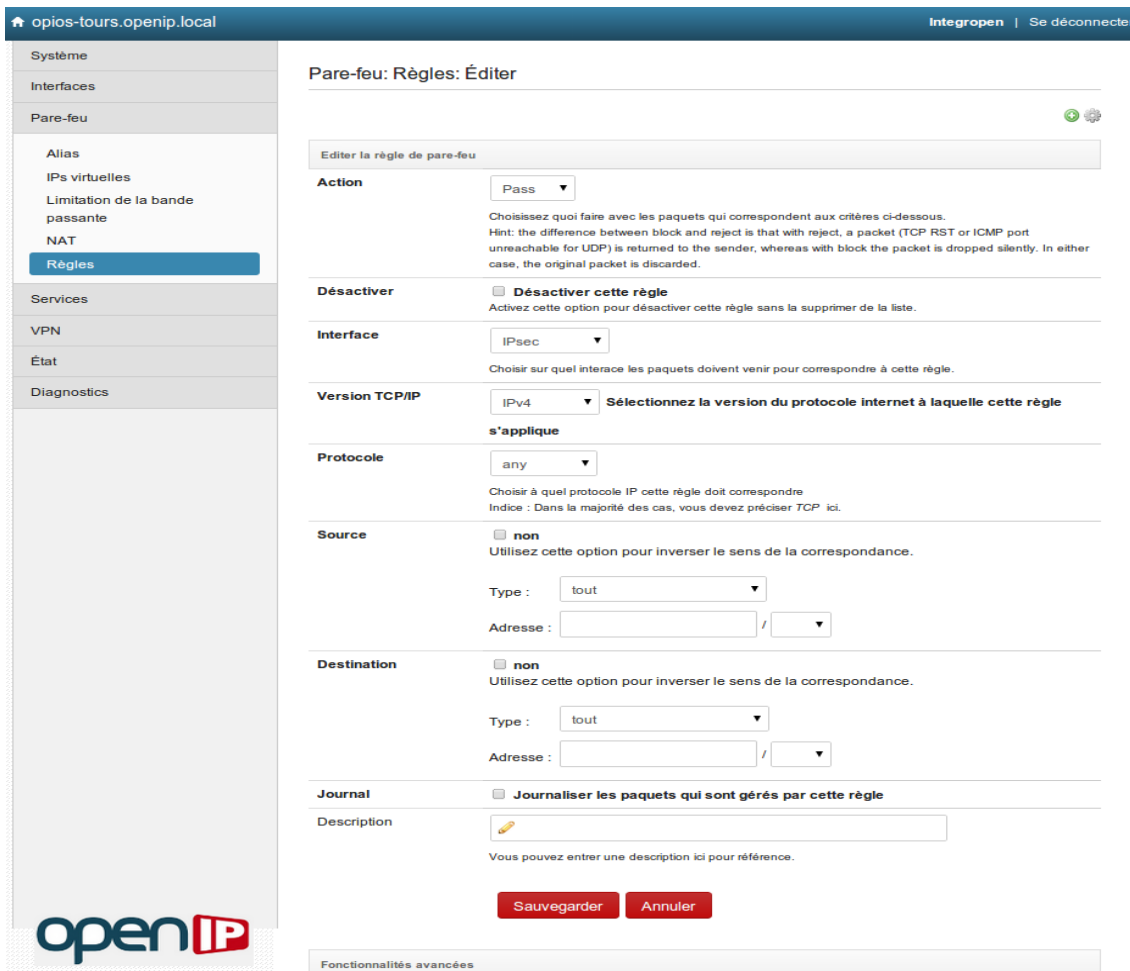
Résumé de la configuration IPSec

La page d'accueil d'IPSec affiche un résumé de la configuration effectuée. Afin d'activer le VPN IPSec, il faut cocher la case **Activer IPsec** et ensuite cliquer sur **Sauvegarder**.

La procédure de configuration présentée dans ce chapitre doit être appliquée aux deux routeurs (S'il s'agit de deux OpIOS avec IHM). L'une des bonnes pratiques est de toujours s'assurer que les paramètres renseignés sont identiques sur les deux routeurs.

Création des règles de Pare-feu

Le trafic IPSec passe par l'interface virtuelle **enc0** sur laquelle les règles de filtrage via PF peuvent être appliquées. Sur l'IHM, dès que IPSec est activé, un onglet **IPsec** apparaît dans la page de définition des règles de pare-feu. Dans ce document tout trafic sur l'interface enc0 correspondant à l'onglet **IPsec** sera autorisé. Pour le faire, il faut cliquer sur *Pare-feu* ⇒ *Règles* ⇒ *Onglet IPsec* ⇒ icône . La page suivante s'affiche :



opios-tours.openip.local Integropen | Se déconnecter

Système
Interfaces
Pare-feu
Alias
IPs virtuelles
Limitation de la bande passante
NAT
Règles
Services
VPN
État
Diagnostics

Pare-feu: Règles: Éditer

Editer la règle de pare-feu

Action Pass

Choisissez quoi faire avec les paquets qui correspondent aux critères ci-dessous.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Désactiver cette règle
Activez cette option pour désactiver cette règle sans la supprimer de la liste.

Interface IPsec
Choisir sur quel interface les paquets doivent venir pour correspondre à cette règle.

Version TCP/IP IPv4 Sélectionnez la version du protocole internet à laquelle cette règle s'applique

Protocole any
Choisir à quel protocole IP cette règle doit correspondre
Indice : Dans la majorité des cas, vous devez préciser TCP ici.

non
Utilisez cette option pour inverser le sens de la correspondance.

Type : tout

Adresse : /

non
Utilisez cette option pour inverser le sens de la correspondance.

Type : tout

Adresse : /

Journaliser les paquets qui sont gérés par cette règle

Description

Vous pouvez entrer une description ici pour référence.

Sauvegarder Annuler

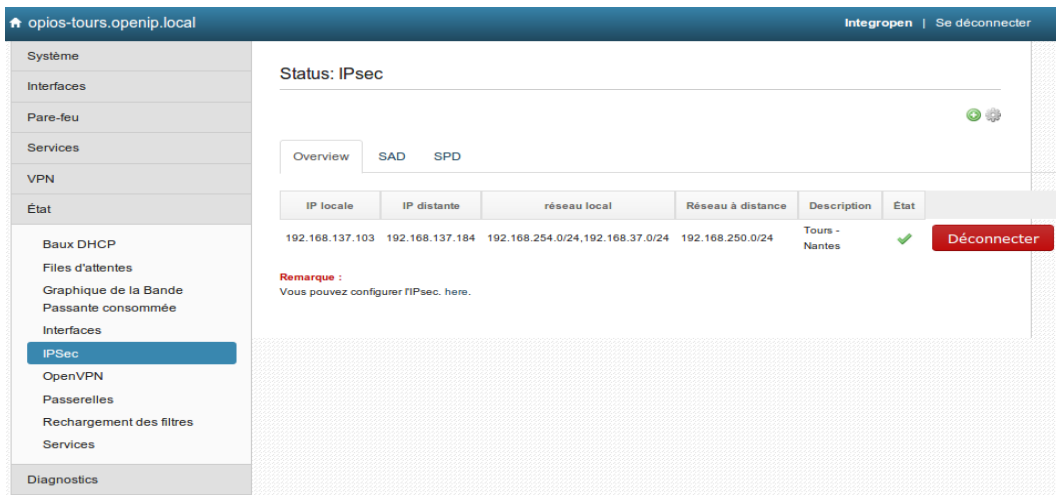
Fonctionnalités avancées

Regle de Pare-feu IPSec




Pour autoriser tout trafic entrant, il suffit de sélectionner *any* dans le champ **Protocole**. Garder les autres paramètres tels qu'ils sont. Cliquer sur **Sauvegarder** et **Appliquer les changements** pour valider la configuration.

Vérifications des Tunnels

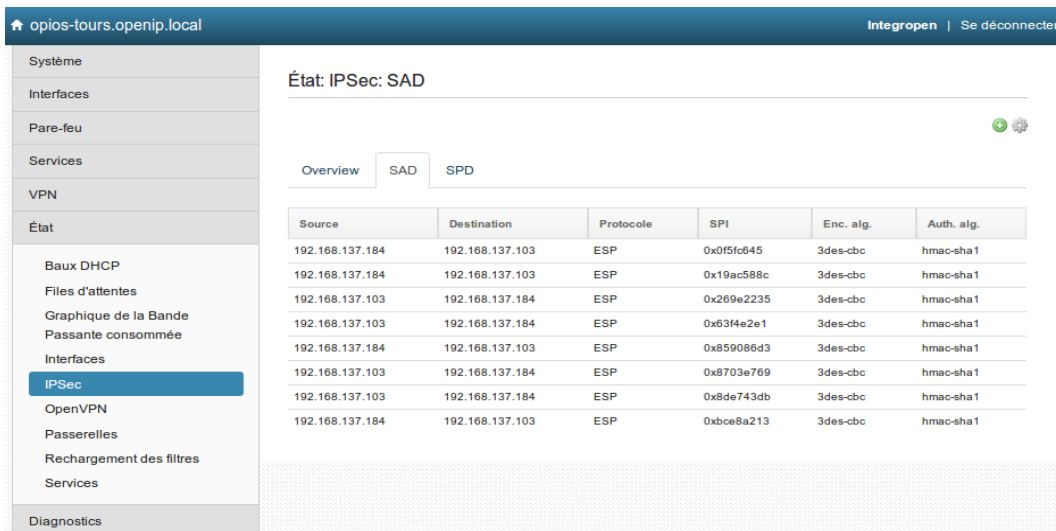
Afin de vérifier que le tunnel est bien créé, il faut cliquer sur *Etat* ⇒ *IPSec*. La page suivante apparaît :



Etat des tunnels IPsec

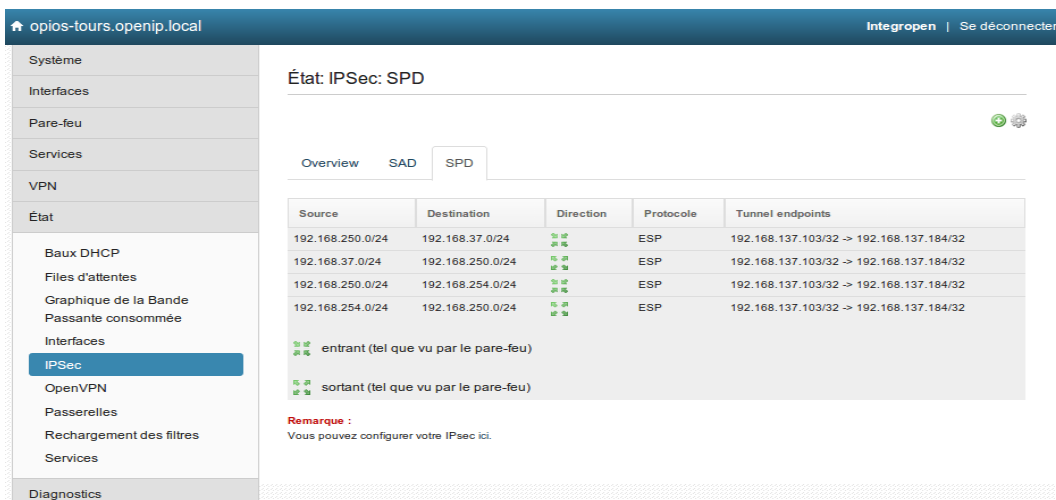
Lorsque le champ **Etat** de l'onglet **Overview** présente l'icône , alors le tunnel est bien créé. Tandis que, les icônes  (qui veut dire IPsec désactivé) et  (qui veut dire Erreur de configuration) signalent que le tunnel n'est pas créé ou ne fonctionne pas correctement.

Quand le tunnel est monté les onglets **SAD** et **SPD** affichent des informations de la forme suivante :



Etat SAD des tunnels IPsec

Et



Etat SPD des tunnels IPsec

Il est possible que les onglets **SAD** et **SPD** présentent un contenu alors que l'icône de l'onglet **Overview** est en mode Erreur de configuration. Dans ce cas, il faudrait vérifier la configuration pour trouver la cause de cette erreur mineure puisque les routeurs parviennent à monter la phase 2.

Troubleshooting

En général, une modification quelconque liée au réseau sur l'un ou les deux routeur(s) passerelles d'un tunnel IPsec peut entraîner un arrêt ou un dysfonctionnement du tunnel. Pour relancer le tunnel, il est conseillé de procéder de la manière suivante :

- Commencez avant tout par désactiver IPsec en décochant la case **Activer IPsec** de la page **VPN** \Rightarrow **IPsec** et en cliquant sur **sauvegarder**. Ensuite réactivez IPsec en cochant la case **Activer IPsec** et cliquez sur **sauvegarder**.

Vérifier ensuite l'état du tunnel.

- Si le premier point ne donne pas de résultats satisfaisants, pensez à redémarrer le routeur et/ou l'équipement concerné par le service délivré via le VPN.