IHM OpIOS

Procédure de configuration des règles NAT et de filtrage

Auteur :
Hozzy TCHIBINDA

15 Avril 2014
Version 1.0

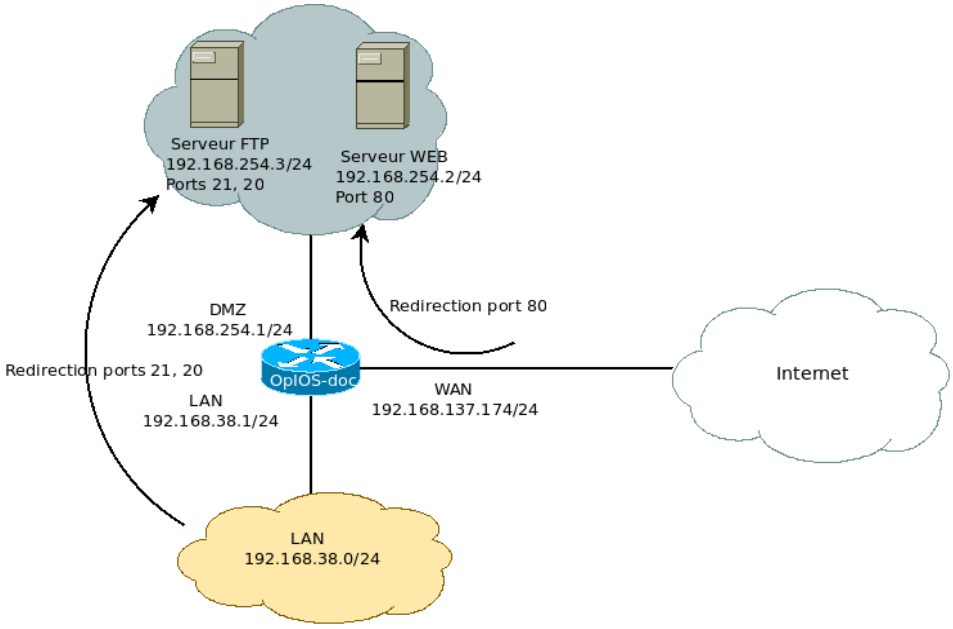
www.openip.fr

Table des matières

Présentation

Ce document destiné au Support Technique et aux partenaires présente la procédure à suivre afin de mettre en place des règles NAT et de filtrage sur un OpIOS via l'IHM.

Afin d'être plus pratique, la figure ci-dessous présente l'architecture sur laquelle vont se baser les procédures de configuration présentées dans ce document.



Architecture d'illustration

Dans cette architecture :

- Tout trafic FTP en provenance du réseau LAN et à destination de l'interface LAN de l'OpIOS est redirigé vers le serveur FTP qui est dans la DMZ,
- Tout trafic en provenance d'Internet et à destination du port 80 de l'OpIOS est redirigé vers le serveur WEB,
- Tout trafic provenant du LAN ou de la DMZ et à destination d'Internet est natté sur l'interface WAN de l'OpIOS,
- Interdiction à tout trafic provenant de l'hôte 94.38.42.12 (sur Internet) d'accéder au serveur WEB,
- Interdiction à tout trafic en provenance du reseau local LAN d'accéder à l'hôte 94.38.42.12.

Cette illustration permet de donner les bases nécessaires à la maitrise de la configuration des règles NAT et de filtrage.

Règles de filtrage

La configuration des règles de filtrage via l'IHM sur le routeur OpIOS est intuitive, cependant certains principes sont à connaitre pour un fonctionnement correct.

2.1 Principes de fonctionnement

Pour mettre en place des règles de filtrage de manière fiable sur un OpIOS, il faut savoir que :

- Par défaut, OpenIP à toujours accès au routeur sur l'interface (ou l'une des interfaces) WAN,
- L'ordre de définition des règles de filtrage est important dans la réalisation du filtrage par l'OpIOS,
- Le choix de l'interface sur laquelle seront définies les règles de filtrage est fonction du sens du trafic à filtrer.

2.1.1 Ordre de définition des règles

Lorsque plusieurs règles sont définies sur une interface, dès que l'une d'entre elles correspond aux cararctéristiques du paquet qui traverse l'interface est trouvée, l'OpIOS applique cette règle sans lire celles qui viennent après.
Par exemple, si sur l'interface WAN deux règles sont définies dans l'ordre suivant :

1. Tout trafic entrant est autorisé
2. Tout trafic en provenance de l'hôte 94.38.42.12 est bloqué.

Ce qui donne en image :

Exemple d'ordre de définition de règles

Dans une telle configuration, la deuxième règle ne sera jamais appliquée car lorsqu'un paquet provenant du 94.38.42.12 arrive sur l'interface WAN, la première règle l'autorise à accéder au réseau. Ainsi, l'OpIOS applique la règle sans lire la suite de la liste des règles. Par contre, si l'ordre des règles était inversé, tout paquet en provenance de 94.38.42.12 n'aura jamais accès au reseau local.

2.1.2 Choix de l'interface

La connaissance du sens d'un trafic pour lequel une règle de filtrage doit être définie est déterminant pour le choix de l'interface à laquelle cette règle sera associée.
En effet, sur l'IHM "***toute règle définie sur une interface ne concerne que le trafic entrant (sens du trafic) sur cette interface***".
Alors en considérant l'architecture d'illustration, voici comment se fera le choix des interfaces concernées par les deux dernieres règles suivantes (annoncées dans le chapitre 1) :

1. Interdiction à tout trafic provenant de l'hôte 94.38.42.12 (sur Internet) d'accéder au WEB
2. Interdiction à tout trafic en provenance du reseau local LAN d'accéder à l'hôte 94.38.42.12.

Le sens du trafic de la première règle étant entrant sur l'interface WAN, cette règle peut être définie sans aucun souci sur l'interface WAN.

Le sens du trafic de la deuxième règle étant sortant sur l'interface WAN, il n'est pas possible de définir cette règle sur l'interface WAN. Or ce trafic est entrant sur l'interface LAN, c'est donc sur l'interface LAN que sera définie la deuxième règle.

2.2 Configuration

Les deux règles de filtrage présentées dans la section 2.1.2 seront utilisées à titre d'exemple pour montrer comment configurer une règle de filtrage.
Il est donc question de configurer les règles suivantes :

1. Interdiction à tout trafic provenant de l'hôte 94.38.42.12 (sur Internet) d'accéder au WEB,
2. Interdiction à tout trafic en provenance du reseau local LAN d'accéder à l'hôte 94.38.42.12,
3. Tout autre trafic est autorisé (sur toutes les interfaces).

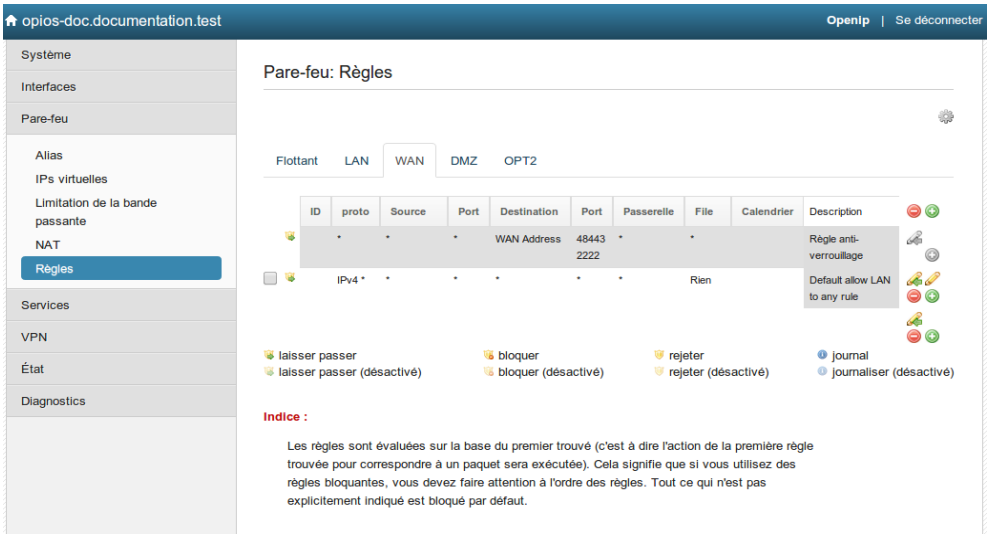
Pour configurer une règle de filtrage, il faut cliquer sur ***Pare-feu*** $\Longrightarrow$ ***Règles***. La page qui s'affiche par défaut est celle de l'interface WAN.

En considérant le choix des interfaces effectué dans la section 2.1.2, la règle 1 sera configurée sur l'interface WAN, la règle 2 sur l'interface LAN et la règle 3 sur toutes les interfaces.

En tenant compte du principe de l'ordre de définition de règles, sur les interfaces WAN et LAN, la règle 3 sera définit en deuxième position.

2.2.1 Configuration sur l'interface WAN

Après avoir cliqué sur ***Pare-feu*** $\Longrightarrow$ ***Règles***, une page semblable à celle ci-dessous s'affiche :



Règles sur l'interface WAN

La règle sur la deuxième ligne (de la figure ci-dessus) correspond à la règle 3 de la liste des règles à configurer. Alors, il ne reste plus qu'ajouter la règle 1 mais au dessus de la règle 3. Pour le faire, il suffit de cliquer sur l'icône  (tout au dessus c'est à dire le premier couple d'icônes ) et alors s'affiche une page possedant deux blocs :

- Editer la règle de pare-feu,
- Fonctionnalités avancées.

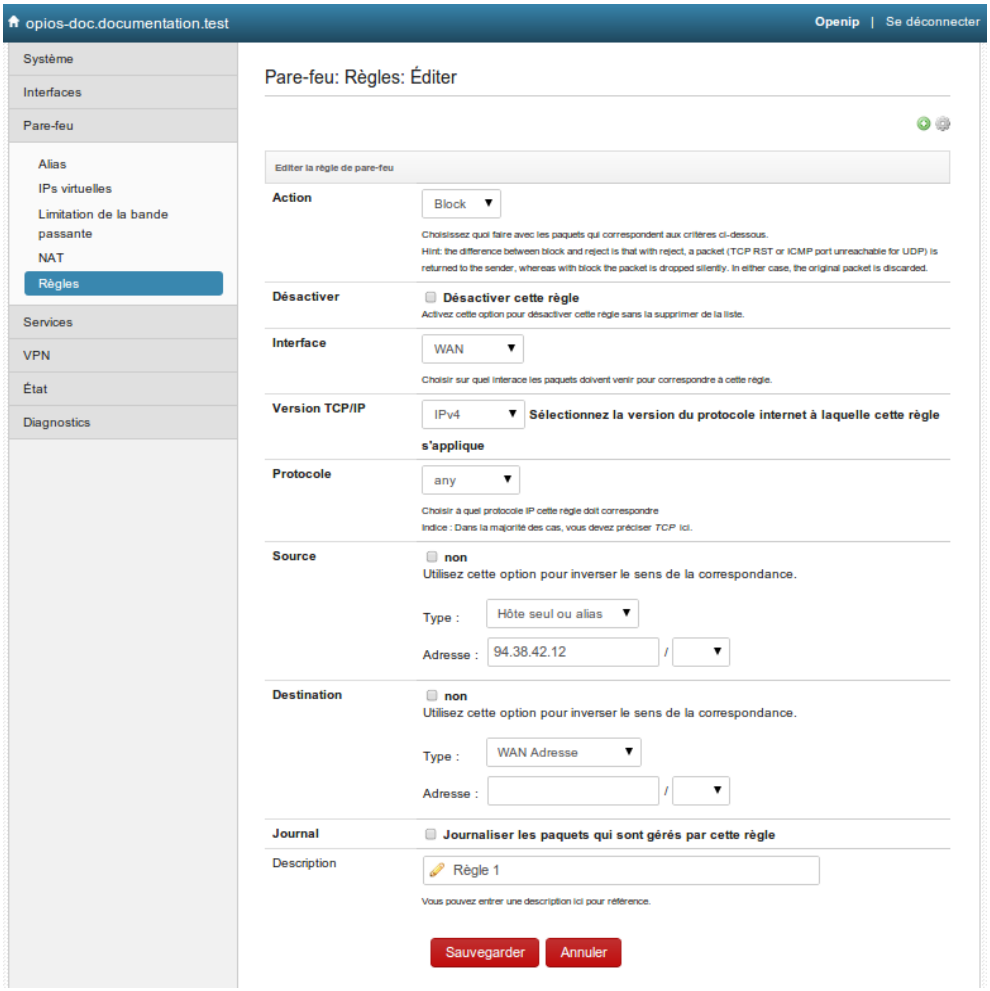
C'est le premier bloc qui sera le plus utilisé. Le deuxième n'est modifié que dans les cas très particuliers comme lors de la configuration d'un lien SDSL avec QoS.

Dans le premier bloc, il faut :

- Sélectionner une action (l'action Block pour ce document).
- Sélectionner ensuite **any** dans la liste déroulante du champ **Protocole**,
- Dans le champ **Source**, sélectionner le Type **Hôte seul ou alias** et saisr ensuite l'IP de la source (94.38.42.12 dans le cas de ce document),
- Dans le champ **Destination**, sélectionner le type **WAN Adresse**.

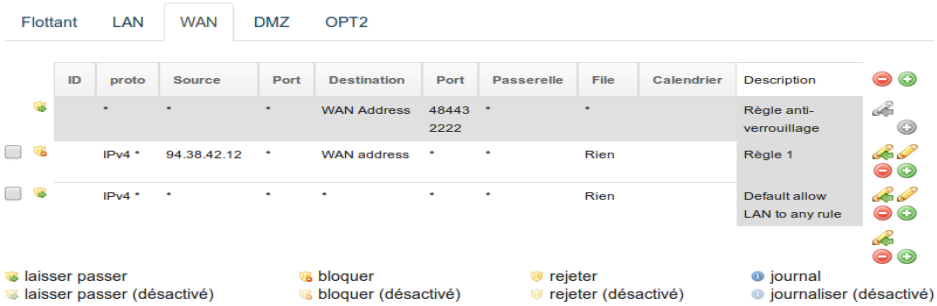
Il est ensuite possibe mais pas obligatoire de journaliser les paquets qui sont gérés par la règle, en cochant la case du champ **Journal** et de saisir une description dans le champ **Description**.

Voici à quoi ressemble le premier bloc après configuration :



Règle 1 sur l'interface WAN

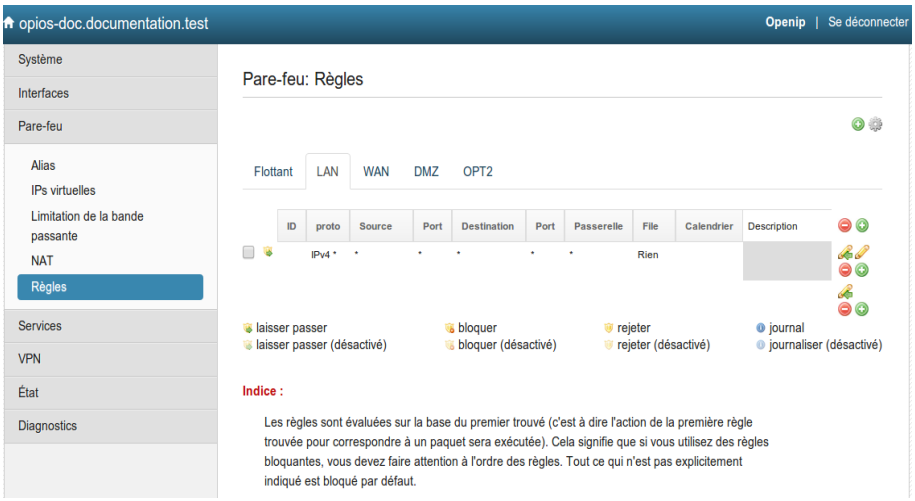
En cliquant sur **Sauvegarder** et ensuite sur **Appliquer les changements** , la page suivante s'affiche :



Résumé des règles sur l'interface WAN

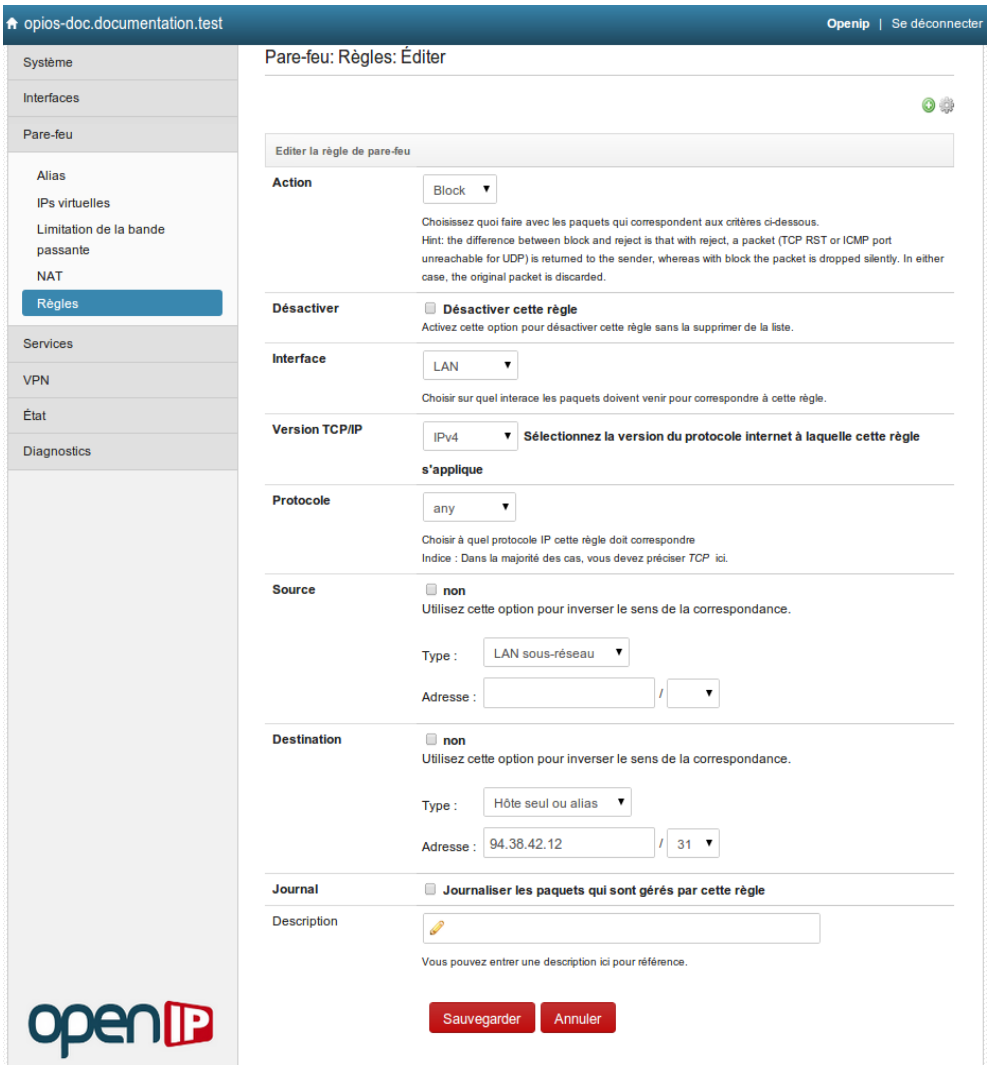
2.2.2 Configuration sur l'interface LAN

Après avoir cliqué sur ***Pare-feu*** $\Longrightarrow$ ***Règles***, une page semblable à celle ci-dessous s'affiche :



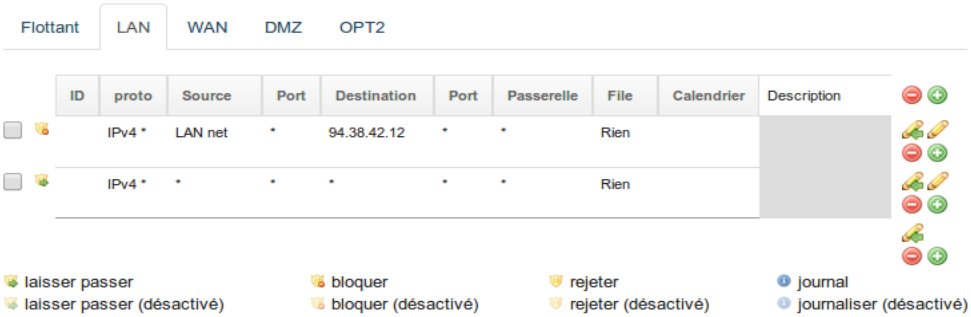
Règles sur l'interface LAN

Comme dans la section 2.2.1, la règle par défaut présente sur cette figure est la troisième de la liste des règles à configurer. Il faut juste ajouter la règle 2 de la liste en cliquant sur l'icône du premier couple d'icônes .
Après avoir saisi toutes les informations concernant le trafic, la page de configuration ressemble à ceci :



Règle 2 sur l'interface LAN

En cliquant sur **Sauvegarder** et ensuite sur **Appliquer les changements** , la page suivante s'affiche :



Résumé des règles sur l'interface LAN

.

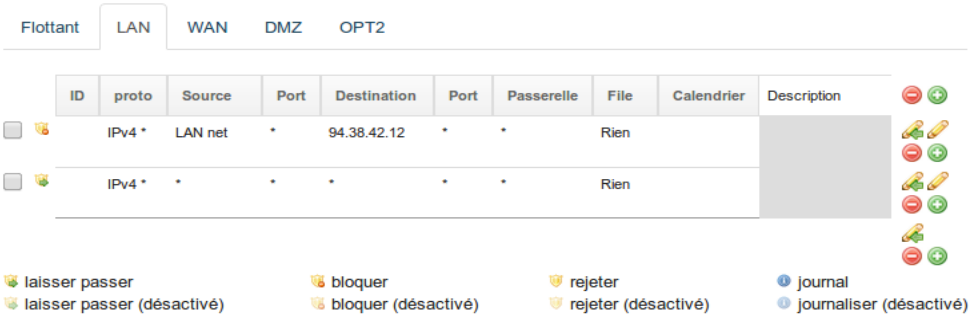
Remarques importantes :

1. Lorsqu'un OpIOS est livré, la configuration par défaut dispose des interfaces WAN, LAN_VOIX et LAN_DATA auxquelles est associée la règle de filtrage " ***Tout trafic est autorisé***", mais lorsqu'une nouvelle interface est ajoutée, aucune règle de filtrage n'est associée à celle-ci.

2. L'activation d'IPsec sur l'IHM génère automatiquement un nouvel onglet **IPSec** dans le sous-menu ***Règles*** du menu ***Pare-feu***.

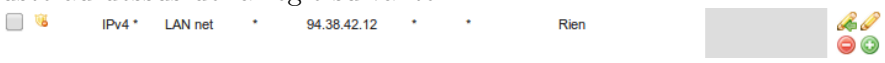
3. Il est possible de s'en passer du principe du ***choix de l'interface en fonction du sens du trafic*** grâce à l'onglet **Flottant**. Dans cet onglet, tout les sens de trafic sont pris en compte et toutes les interfaces sont présentes sur une liste d'interfaces. Ainsi la définition d'une règle peut être appliquée sur plusieurs interfaces simultanement et dans tous les sens de trafics possibles.
   Cet onglet est pratique pour ceux qui ne veulent pas se deplacer sur plusieurs onglets afin d'effectuer des configurations mais tout avoir sur un seul onglet.

4. La compréhension des différentes icônes facilite la manupilation de l'IHM dans la configuration des règles de filtrage. De ce fait, voici la présentation de quelques icônes, principalement celles utilisées pour créer, modifier et supprimer les règles de filtrage.
   Soit la configuration suivante :



Résumé des règles sur l'interface LAN

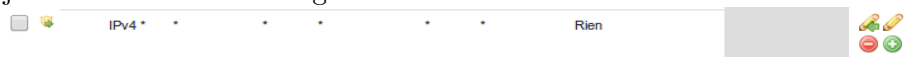
Le premier couple d'icônes permet de manupiler la tête de liste des règles. L'icône supprime toute règle dont la case tout à gauche est cochée, tandis que l'icône crée une nouvelle règle juste au-dessus de la règle suivante :



Le bloc d'icônes de la règle ci-dessus permet de la manipuler. L'icône supprime la règle, l'icône crée une règle totalement identique juste en-dessous et l'icône permet de modifier

la règle.

Le dernier couple d'icônes permet de manipuler le bas de liste des règles. L'icône supprime toute règle dont la case tout à gauche est cochée, tandis que l'icône crée une nouvelle règle juste en-dessous de la règle suivante :



L'icône dont le rôle est de deplacer les règles n'est pas encore fonctionnelle.

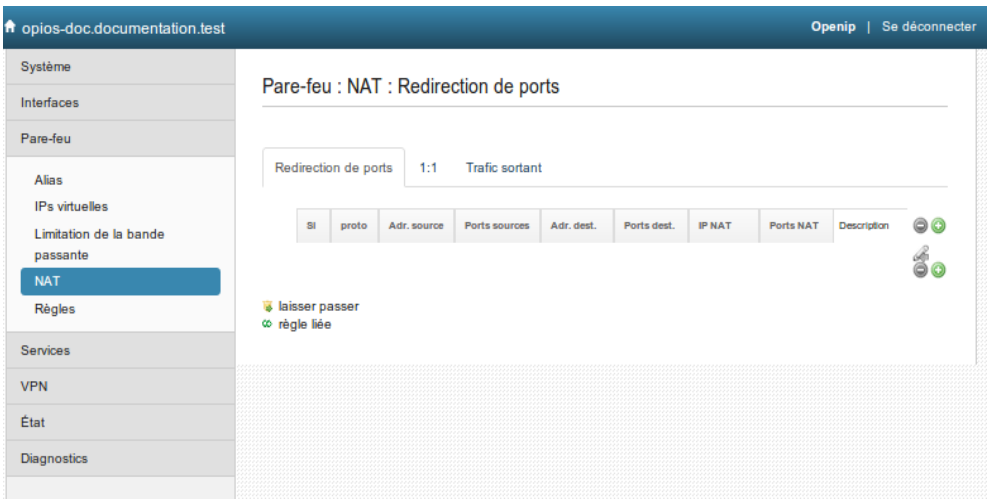
Règles NAT

Deux types de règles sont concernés par ce chapitre :

- Les règles de redirection de ports,
- Les règles de translation d'adresses des trafics sortants.

3.1 Règles de redirection de ports

Pour configurer une redirection de ports sur l'IHM, il faut cliquer sur ***Pare-feu*** $\Longrightarrow$ ***NAT*** et la page suivante s'affiche :



Page d'accueil pour redirection de ports

Dans ce document, les règles annoncées dans le chapitre 1 vont servirent d'exemple pour la configuration des redirections de ports. Il s'agit des règles suivantes :

1. Tout trafic en provenance d'Internet et à destination du port 80 de l'OpIOS est redirigé vers le serveur WEB,
2. Tout trafic FTP en provenance du réseau LAN et à destination de l'interface LAN de l'OpIOS est redirigé vers le serveur FTP qui est dans la DMZ.

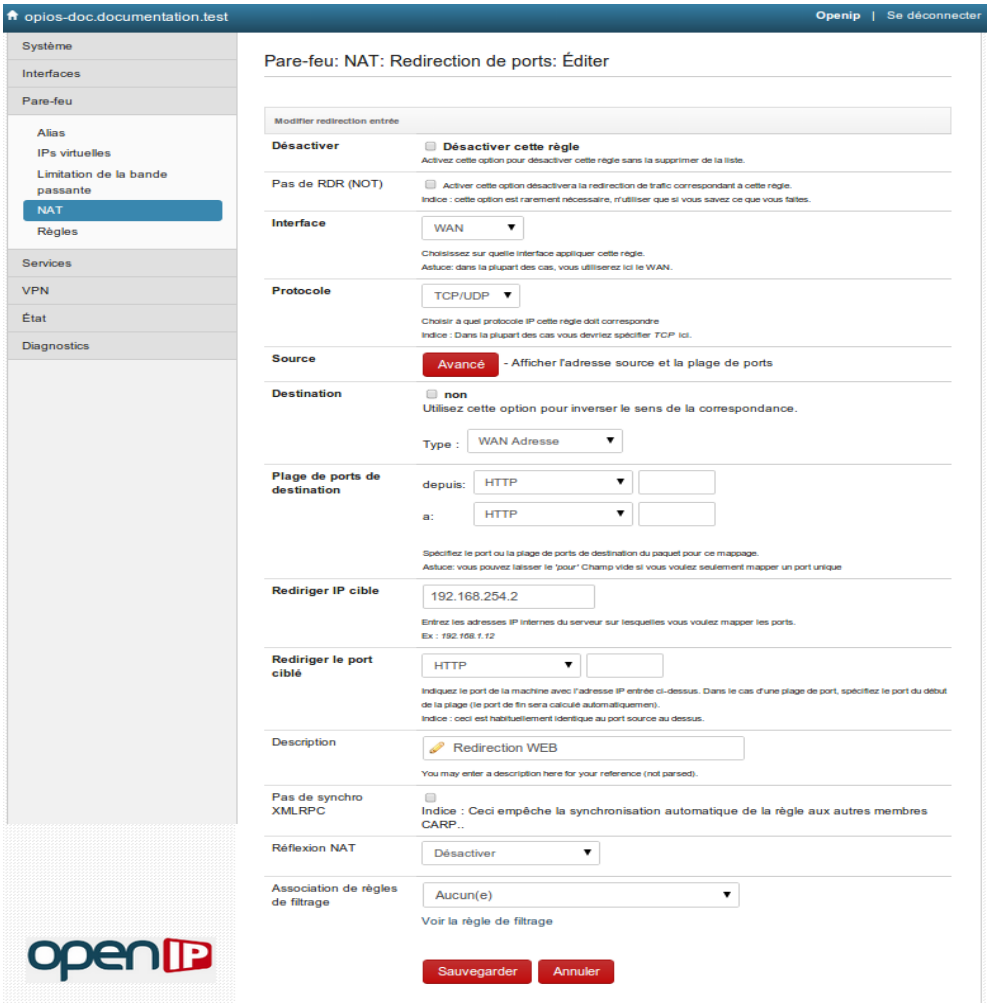
3.1.1 Redirection du port 80

Pour configurer la première règle, il faut cliquer sur l'icône . Sur la page qui s'affiche :

- Sélectionner l'interface concernée par la règle dans le champ **Interface**. Dans le cas de cet exemple, il s'agit de l'interface WAN,
- Sélectionner le protocole à utiliser dans la liste déroulante du champ **Protocole**,
- Dans le champ **Source**, cliquer sur **Avancé** pour saisir l'IP et si nécessaire le port de la source. Dans l'exemple de ce document, les valeurs par défaut seront conservées,
- Dans le champ **Destination**, sélectionner le type de destination,
- Sélectionner ou saisir le port de destination dans le champ **Plage de ports de destination**,
- Saisir dans le champ **Redirigé IP cible**, l'IP de la cible vers laquelle le trafic sera redirigé,

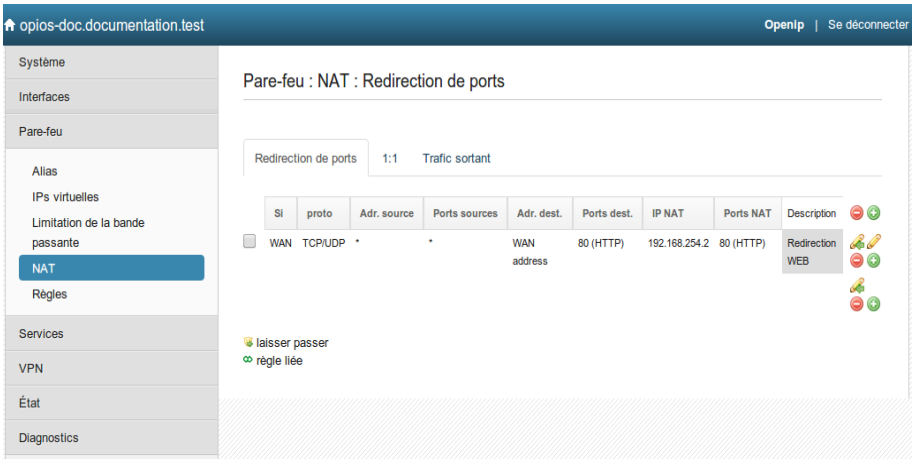
- Saisir dans le champ **Redirigé le port ciblé**, le port de la cible vers laquelle sera redirigé le trafic,
- Saisir une description dans le champ **Description**,
- Garder la valeur **Désactiver** dans le champ **Reflexion NAT**,
- Enfin, sélectionner la valeur **Aucun(e)** dans le champ **Association des règles de filtrage**, sauf si le trafic entrant concernée par cette règle n'est pas autorisé dans les règles de filtrage. Dans ce cas, il faut sélectionner la valeur **Ajouter une règle de filtrage associée**.

Voici l'image correspondant à cette configuration :



Redirection du port 80

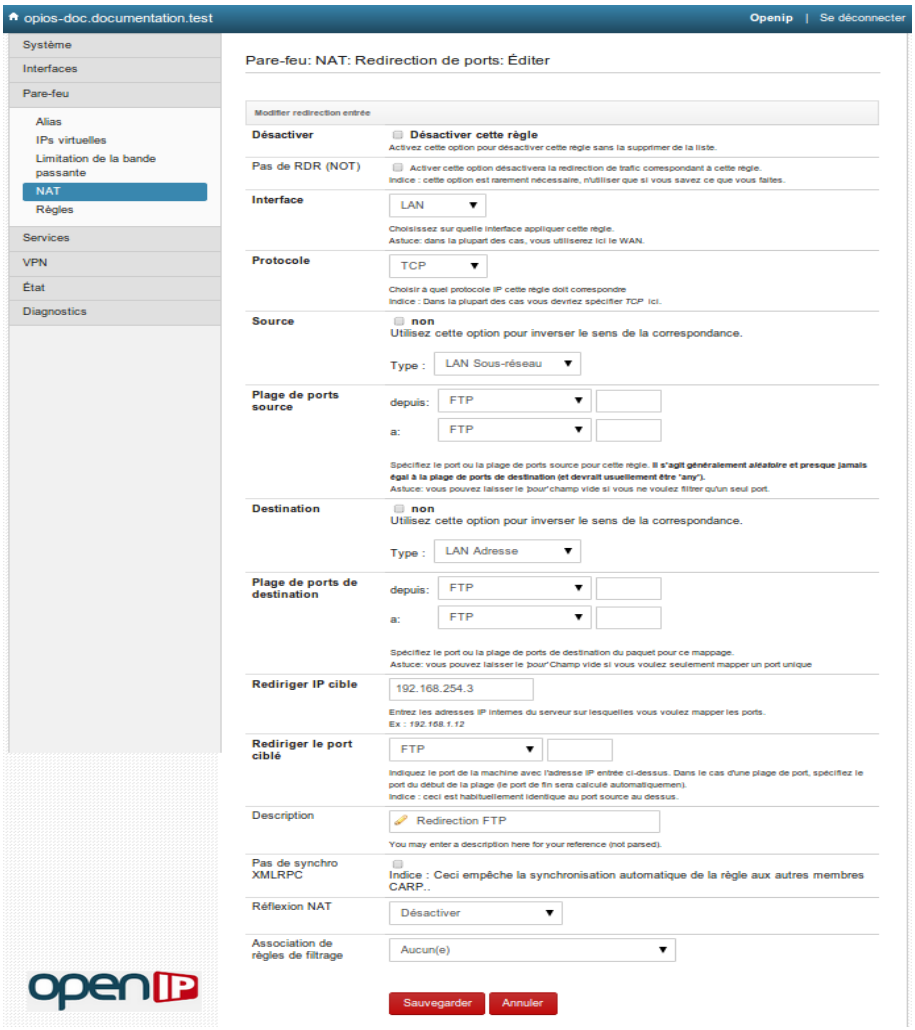
Il faut alors cliquer sur **Sauvegarder** et ensuite sur **Appliquer les changements** pour valider la configuration. La page suivante s'affiche :



Résumé de la liste des règles de redirection de port

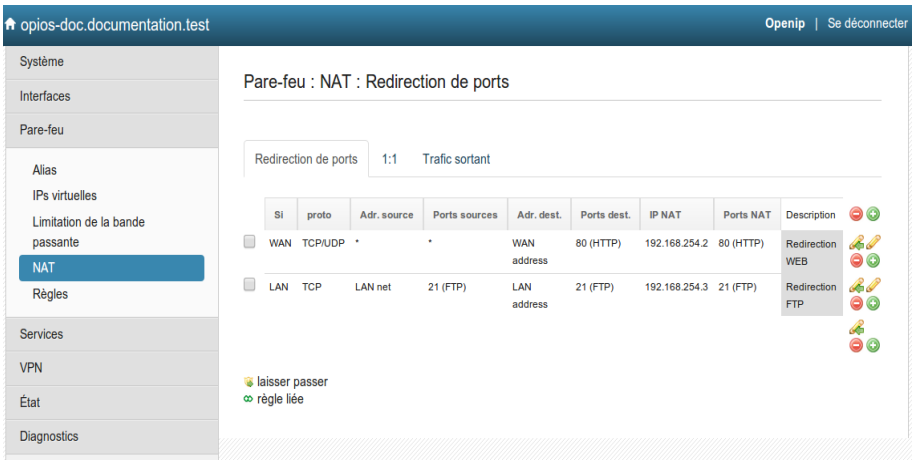
3.1.2 Redirection du trafic FTP

La configuration de la deuxième règle se fait de la manière suivante :



Redirection du trafic FTP

En cliquant sur **Sauvegarder** et ensuite sur **Appliquer les changements**, la page suivante s'affiche :



Liste des règles de redirection de ports

Remarques importantes :

1. Les règles de redirection de ports ne sont pas concernées par le principe de l'ordre de définition de règles. Cependant, lorsque la valeur du champ **Association des règles de filtrage** est **Ajouter une règle de filtrage associée**, il est important de tenir compte de la présence des autres règles de filtrage et de leur ordre.

2. Les icônes sont quasiment identiques à celles des pages de configuration des règles de filtrage.

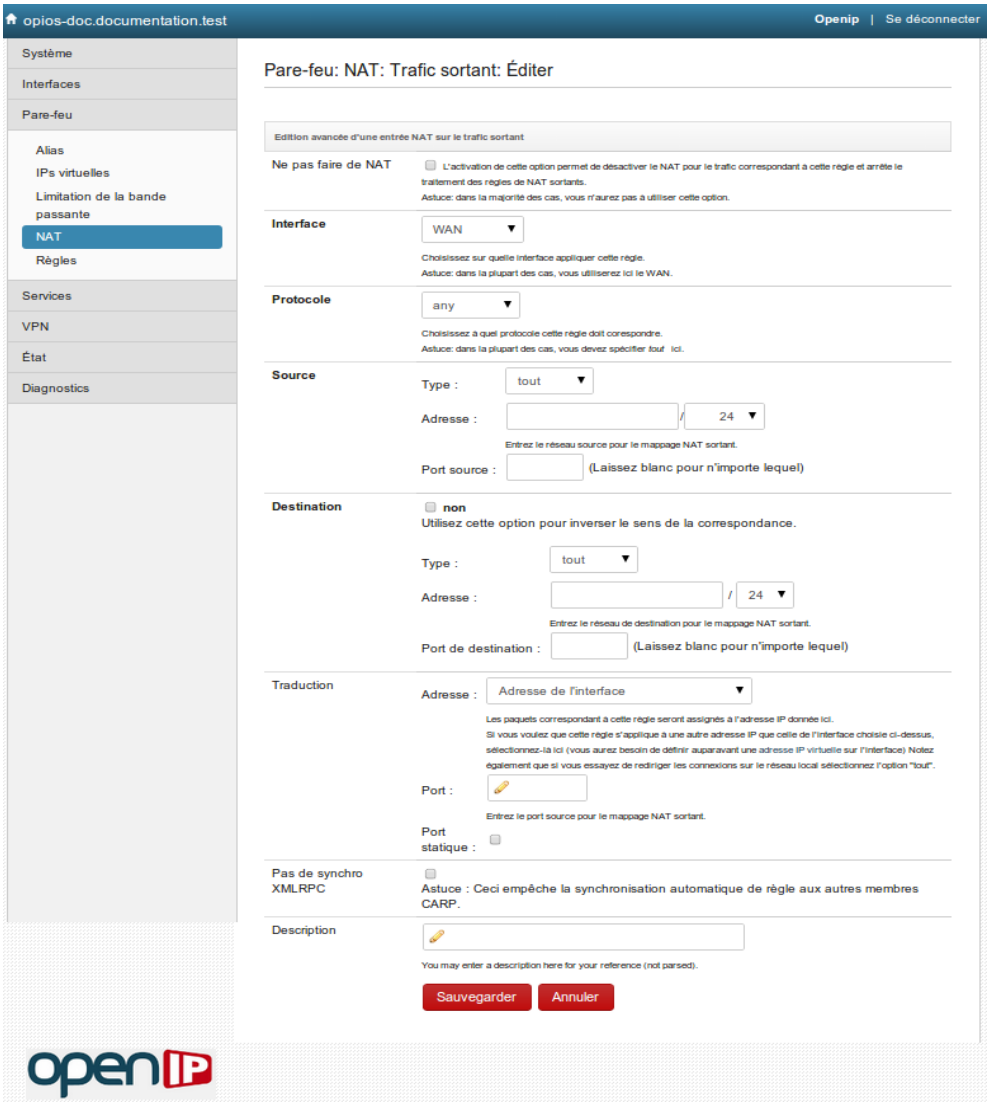
3.2 Règles NAT des trafics sortants

La règle NAT à configurer à titre d'exemple dans ce document est " **Tout trafic provenant du LAN ou de la DMZ et à destination d'Internet est natté sur l'interface WAN de l'OpIOS** " (voir chapitre 1).

Pour configurer des règles NAT sur du trafic sortant, il faut cliquer sur ***Pare-feu*** $\Longrightarrow$ ***NAT*** $\Longrightarrow$ Onglet ***Trafic sortant*** $\Longrightarrow$ Icône . Sur la page qui s'affiche :

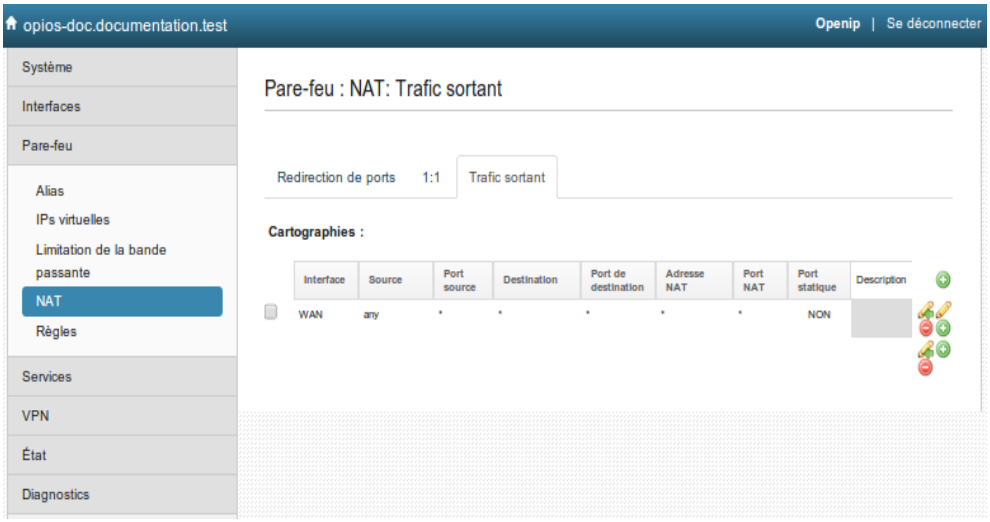
- Sélectionner l'interface concernée par la règle dans le champ **Interfaces**,
- Sélectionner le protocole dans la liste des protocoles disponibles du champ **Protocole**,
- Dans le champ **Source**, sélectionner le type d'information source, ensuite saisir l'adresse et si nécessaire le port source à mapper.
- Dans le champ **Destination**, sélectionner le type d'information de destination, ensuite saisir l'adresse et si nécessaire le port de destination.
- Dans le champ **Traduction**, sélectionner l'adresse qui remplacera celle de la source dans l'en-tête des paquets et qui sera vu par le(s) destinataire(s).
- Enfin, saisir une description à associer à la règle dans le champ **Description**.

La configuration de la règle ci-dessus correspond à ceci :



Règle NAT sur l'interface WAN

En cliquant sur **Sauvegarder** et ensuite sur **Appliquer les changements** , la page suivante s'affiche :



Résumé des règles NAT des trafics sortants