



IHM OpIOS

Procédure de configuration des règles NAT et de filtrage

Auteur :
Hozzy TCHIBINDA

15 Avril 2014
Version 1.0

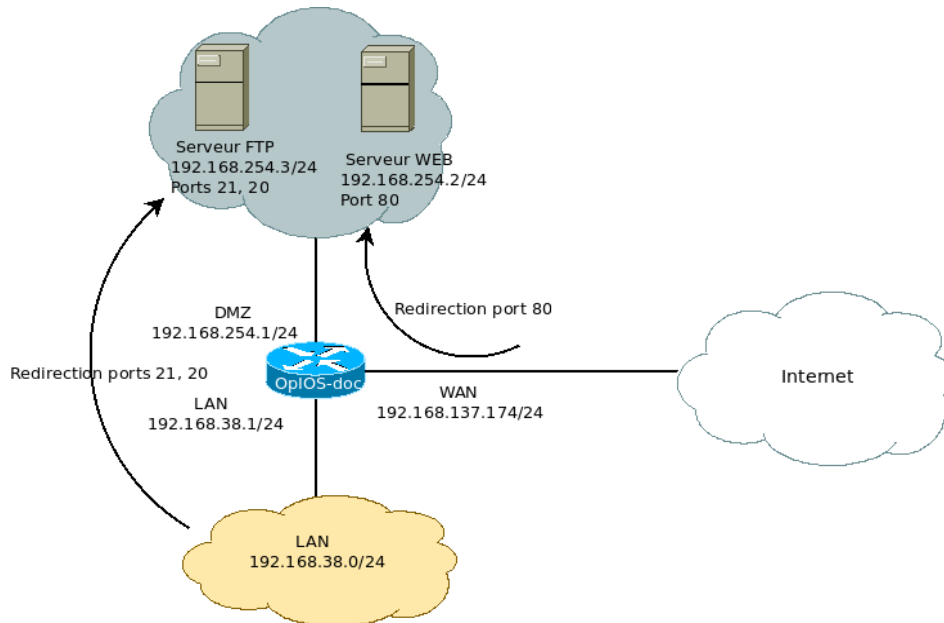
Table des matières

1	Présentation	2
2	Règles de filtrage	3
2.1	Principes de fonctionnement	3
2.1.1	Ordre de définition des règles	3
2.1.2	Choix de l'interface	3
2.2	Configuration	4
2.2.1	Configuration sur l'interface WAN	4
2.2.2	Configuration sur l'interface LAN	6
3	Règles NAT	9
3.1	Règles de redirection de ports	9
3.1.1	Redirection du port 80	9
3.1.2	Redirection du trafic FTP	11
3.2	Règles NAT des trafics sortants	12

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 naté 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 réseau local LAN d'accéder à l'hôte 94.38.42.12.

Cette illustration permet de donner les bases nécessaires à la maîtrise 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 connaître 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 caractéristiques 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 :

<input type="checkbox"/>		IPV4 *	*	*	*	*	Rien	Default allow LAN to any rule			
<input type="checkbox"/>		IPV4 *	94.38.42.12	*	*	*	Rien	Default allow LAN to any rule			

Exemple d'ordre de définition de règles

Dans une telle configuration, la deuxième règle ne sera jamais appliquée car lorsqu'un paquet provenant de 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 réseau 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 dernières 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 réseau 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).

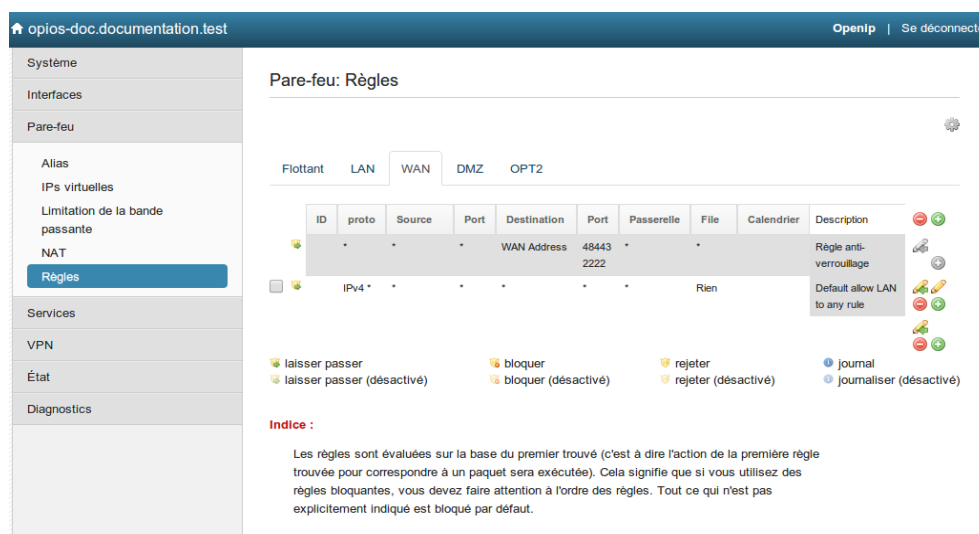
Pour configurer une règle de filtrage, il faut cliquer sur *Pare-feu* \Rightarrow *Règles*. La page qui s'affiche par défaut est celle de l'interface WAN.

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 définie en deuxième position.

2.2.1 Configuration sur l'interface WAN

Après avoir cliqué sur *Pare-feu* \Rightarrow *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 \oplus (tout au dessus c'est à dire le premier couple d'icônes $\ominus \oplus$) et alors s'affiche une page possédant 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 saisir 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 possible 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 :

The screenshot shows the Mikrotik WinBox interface for editing a firewall rule. The left sidebar contains navigation options like 'Système', 'Interfaces', 'Pare-feu', 'Alias', 'IPs virtuelles', 'Limitation de la bande passante', 'NAT', 'Règles', 'Services', 'VPN', 'État', and 'Diagnostics'. The main area is titled 'Pare-feu: Règles: Éditer'. The rule configuration is as follows:

- Action:** Block
- Désactiver:** Désactiver cette règle
- Interface:** WAN
- Version TCP/IP:** IPv4
- Protocole:** any
- Source:** non, Type: Hôte seul ou alias, Adresse: 94.38.42.12
- Destination:** non, Type: WAN Adresse, Adresse: [empty]
- Journal:** Journaliser les paquets qui sont gérés par cette règle
- Description:** Règle 1

Règle 1 sur l'interface WAN

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

The screenshot shows the Mikrotik WinBox interface for the Firewall Rule list on the WAN interface. The table below shows the configured rules:

ID	proto	Source	Port	Destination	Port	Passerelle	File	Calendrier	Description
	*	*	*	WAN Address	48443	*	*		Règle anti-verrouillage
	IPv4 *	94.38.42.12	*	WAN address	*	*	Rien		Règle 1
	IPv4 *	*	*	*	*	*	Rien		Default allow LAN to any rule

Legend for rule actions:

- laisser passer
- laisser passer (désactivé)
- bloquer
- bloquer (désactivé)
- rejeter
- rejeter (désactivé)
- journal
- journaliser (désactivé)

Résumé des règles sur l'interface WAN

2.2.2 Configuration sur l'interface LAN

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

opios-doc.documentation.test Openip | Se déconnecter

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

Pare-feu: Règles

Flottant LAN WAN DMZ OPT2

ID	proto	Source	Port	Destination	Port	Passerelle	File	Calendrier	Description
1	IPv4	*	*	*	*	*	*	*	Rien

laisser passer bloquer rejeter journal
laisser passer (désactivé) bloquer (désactivé) rejeter (désactivé) journaliser (désactivé)

Indice :
Les règles sont évaluées sur la base du premier trouvé (c'est à dire l'action de la première règle trouvée pour correspondre à un paquet sera exécutée). Cela signifie que si vous utilisez des règles bloquantes, vous devez faire attention à l'ordre des règles. Tout ce qui n'est pas explicitement indiqué est bloqué par défaut.

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 \oplus du premier couple d'icônes $\ominus \oplus$.

Après avoir saisi toutes les informations concernant le trafic, la page de configuration ressemble à ceci :

opios-doc.documentation.test Openip | Se déconnecter

Pare-feu: Règles: Éditer

Editer la règle de pare-feu

Action Block

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

Interface LAN
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.

Source non
Utilisez cette option pour inverser le sens de la correspondance.
Type : LAN sous-réseau
Adresse : /

Destination non
Utilisez cette option pour inverser le sens de la correspondance.
Type : Hôte seul ou alias
Adresse : 94.38.42.12 / 31

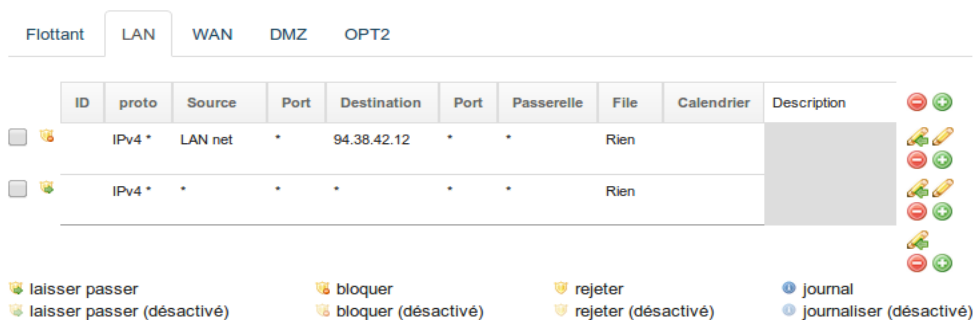
Journal Journaliser les paquets qui sont gérés par cette règle

Description
Vous pouvez entrer une description ici pour référence.

openIP Sauvegarder Annuler

Règle 2 sur l'interface LAN

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

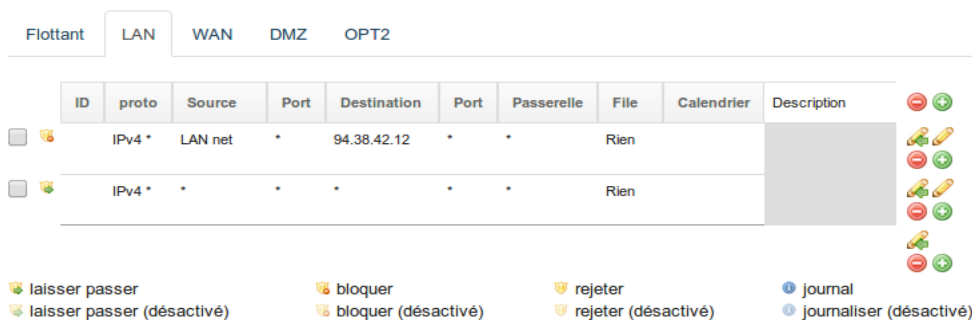


Résumé des règles sur l’interface LAN

Remarques importantes :

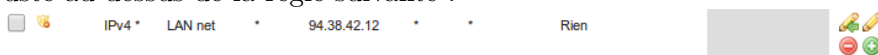
1. Lorsqu’un OpIOS est livré, la configuration par défaut dispose des interfaces WAN, LAN_VOIX et LAN_DATA auxquelles est associée la règle de filtrage “ **Tout trafic est autorisé**”, mais lorsqu’une nouvelle interface est ajoutée, aucune règle de filtrage n’est associée à celle-ci.
2. L’activation 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 simultanément et dans tous les sens de trafics possibles. Cet onglet est pratique pour ceux qui ne veulent pas se déplacer sur plusieurs onglets afin d’effectuer des configurations mais tout avoir sur un seul onglet.
4. La compréhension des différentes icônes facilite la manipulation 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

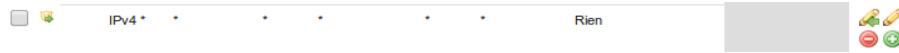
Le premier couple d’icônes permet de manipuler la tête de liste des règles. L’icône supprime toute règle dont la case tout à gauche est cochée, tandis que l’icône crée une nouvelle règle juste au-dessus de la règle suivante :




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 déplacer les règles n'est pas encore fonctionnelle.

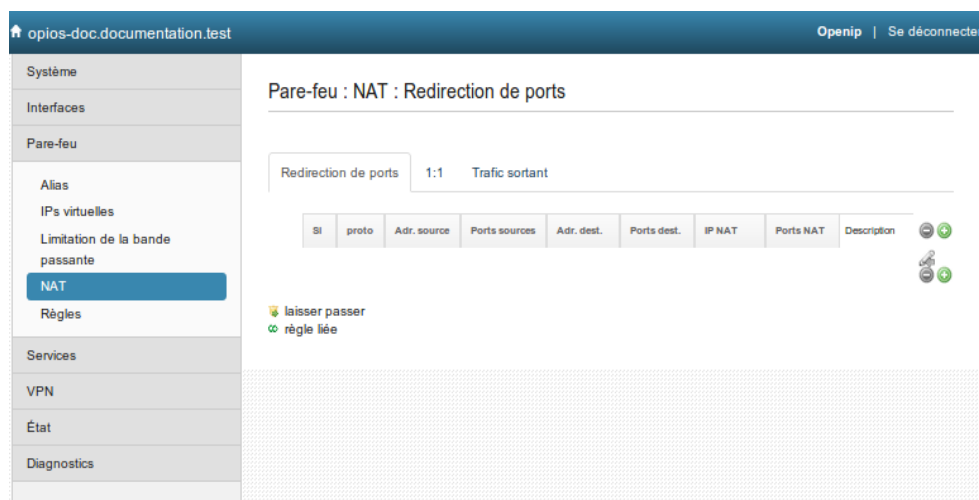
Règles NAT

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* \implies *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 servir 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 :

Si	proto	Adr. source	Ports sources	Adr. dest.	Ports dest.	IP NAT	Ports NAT	Description
<input type="checkbox"/>	WAN	TCP/UDP	•	WAN address	80 (HTTP)	192.168.254.2	80 (HTTP)	Redirection WEB

laisser passer
 règle liée

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 :

opios-doc.documentation.test Openip | Se déconnecter

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

Pare-feu: NAT: Redirection de ports: Éditer

Modifier redirection entrée

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

Pas de RDR (NOT)
Activez cette option désactivera la redirection de trafic correspondant à cette règle.
Indice : cette option est rarement nécessaire, n'utiliser que si vous savez ce que vous faites.

Interface
LAN

Choisissez sur quelle interface appliquer cette règle.
Astuce : dans la plupart des cas, vous utiliserez ici le WAN.

Protocole
TCP

Choisir à quel protocole IP cette règle doit correspondre
Indice : Dans la plupart des cas vous devrez spécifier TCP ici.

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

Type : LAN Sous-réseau

Plage de ports source
depuis: FTP
a: FTP

Spécifiez le port ou la plage de ports source pour cette règle. Il s'agit généralement aléatoire et presque jamais égal à la plage de ports de destination (et devrait usuellement être "any").
Astuce : vous pouvez laisser le "pour" champ vide si vous ne voulez filtrer qu'un seul port.

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

Type : LAN Adresse

Plage de ports de destination
depuis: FTP
a: FTP

Spécifiez le port ou la plage de ports de destination du paquet pour ce mappage.
Astuce : vous pouvez laisser le "pour" champ vide si vous voulez seulement mapper un port unique

Rediriger IP cible
192.168.254.3

Entrez les adresses IP internes du serveur sur lesquelles vous voulez mapper les ports.
Ex : 192.168.1.12

Rediriger le port cible
FTP

Indiquez le port de la machine avec l'adresse IP entrée ci-dessus. Dans le cas d'une plage de port, spécifiez le port du début de la plage (le port de fin sera calculé automatiquement).
Indice : ceci est habituellement identique au port source au dessus.

Description
Redirection FTP
You may enter a description here for your reference (not parsed).

Pas de synchro XMLRPC
 Indice : Ceci empêche la synchronisation automatique de la règle aux autres membres CARP..

Réflexion NAT
Désactiver

Association de règles de filtrage
Aucun(e)

Sauvegarder Annuler

Redirection du trafic FTP

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

opios-doc.documentation.test Openip | Se déconnecter

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

Pare-feu : NAT : Redirection de ports

Redirection de ports 1:1 Trafic sortant

Si	proto	Adr. source	Ports sources	Adr. dest.	Ports dest.	IP NAT	Ports NAT	Description
<input type="checkbox"/>	WAN TCP/UDP	*	*	WAN address	80 (HTTP)	192.168.254.2	80 (HTTP)	Redirection WEB
<input type="checkbox"/>	LAN TCP	LAN net	21 (FTP)	LAN address	21 (FTP)	192.168.254.3	21 (FTP)	Redirection FTP

laisser passer
règle liée

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.

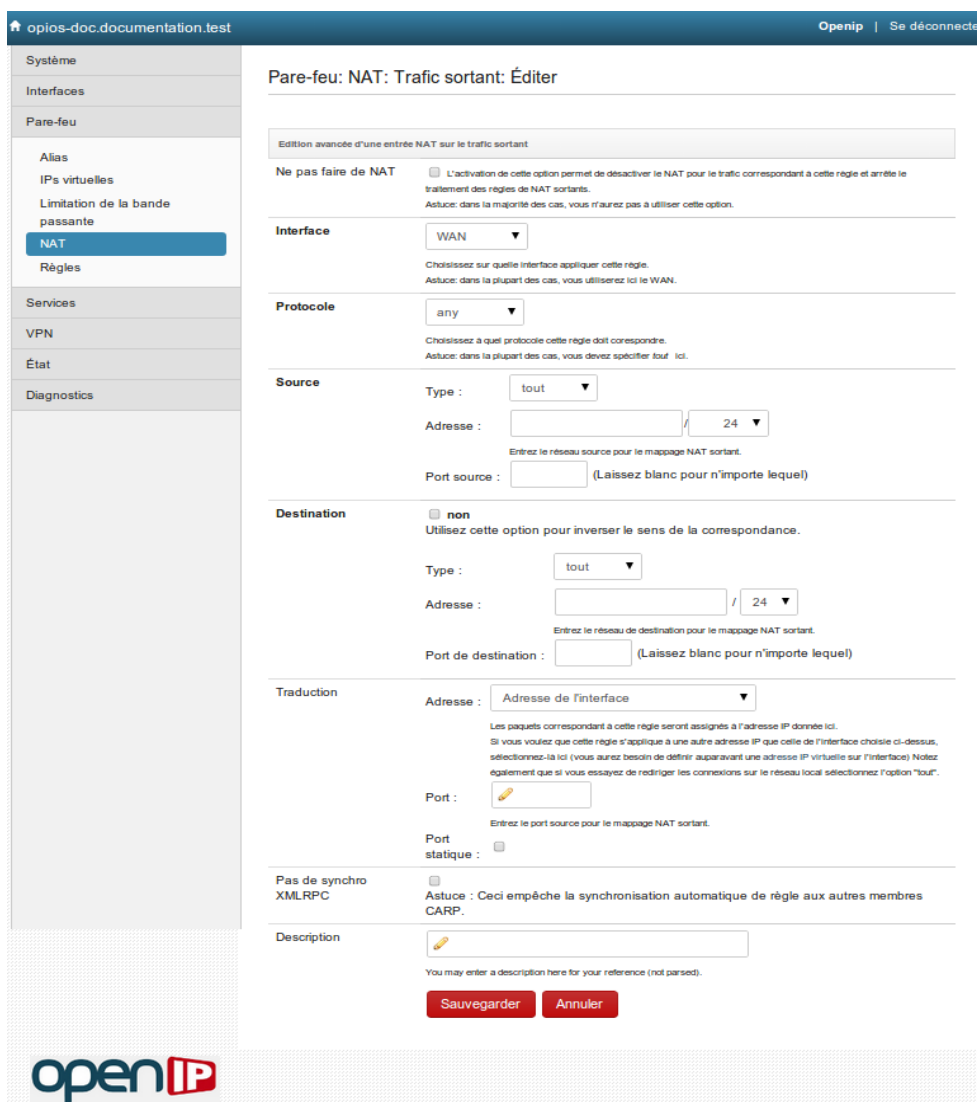
3.2 Règles NAT des trafics sortants

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* ⇒ *NAT* ⇒ Onglet *Trafic sortant* ⇒ 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 :



The screenshot shows the configuration page for a NAT rule in the OpenIP interface. The page title is "Pare-feu: NAT: Trafic sortant: Éditer". On the left is a navigation menu with categories like "Système", "Interfaces", "Pare-feu", "Services", etc., and "NAT" is selected. The main content area is titled "Edition avancée d'une entrée NAT sur le trafic sortant". It contains several sections: "Ne pas faire de NAT" (unchecked), "Interface" (set to "WAN"), "Protocole" (set to "any"), "Source" (Type: "tout", Adresse: [input] / 24, Port source: [input]), "Destination" (checked "non", Type: "tout", Adresse: [input] / 24, Port de destination: [input]), "Traduction" (Adresse: "Adresse de l'interface", Port: [input]), "Pas de synchro XMLRPC" (checked), and "Description" (empty text area). At the bottom are "Sauvegarder" and "Annuler" buttons.

Règle NAT sur l'interface WAN

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

The screenshot shows the OpenIP web interface for configuring NAT. The browser address bar shows 'opios-doc.documentation.test' and the user is logged in as 'Openip'. The left sidebar contains a menu with items: Système, Interfaces, Pare-feu, Alias, IPs virtuelles, Limitation de la bande passante, NAT (highlighted), Règles, Services, VPN, État, and Diagnostics. The main content area is titled 'Pare-feu : NAT: Trafic sortant'. Below the title, there are tabs for 'Redirection de ports' and '1:1', with '1:1' selected. Underneath, there are tabs for 'Trafic sortant' and 'Trafic entrant', with 'Trafic sortant' selected. A section titled 'Cartographies :' contains a table with the following columns: Interface, Source, Port source, Destination, Port de destination, Adresse NAT, Port NAT, Port statique, and Description. The table has one row with the following values: WAN, any, *, *, *, *, *, NON, and an empty description cell. To the right of the table are several icons for editing and deleting the rule.

Résumé des règles NAT des trafics sortants