

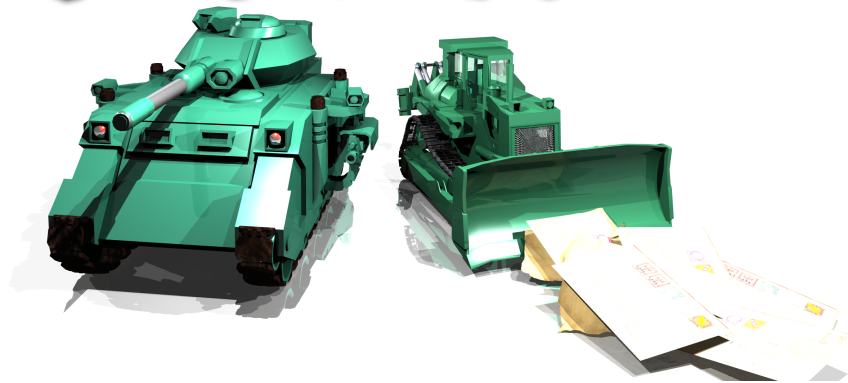
# Artica

---

## Lutte contre le Spam avec Postfix Instant IpTables

Révision Du 05 Février 2011 version 1.5.020514

*Artica*



# Table des matières

---

<b>Introduction :</b> .....	<b>2</b>
<b>Historique du projet :</b> .....	<b>2</b>
A qui s'adresse Artica ? .....	2
Licence et support .....	2
Que fait Artica ? .....	3
<b>Que fait Postfix Instant IpTables</b> .....	<b>4</b>
Quel est l'intérêt ? .....	4
Déchargez votre serveur ! .....	4
Assurez une bande passante .....	4
Comment ca marche ? .....	4
Esprit communautaire .....	5
<b>Mise en place avec Artica</b> .....	<b>5</b>
Personnaliser la sensibilité du scanner .....	5
Visualiser , désactiver les règles .....	6
Listes blanches .....	6

## Introduction :

### *Historique du projet :*

Le projet Open Source Artica est né en *Janvier 2004*.

Le projet Artica a pour but de valoriser les fonctionnalités offertes par la plate-forme Linux à travers une console d'administration locale installée sur le serveur Linux.

Cette console permettant alors de configurer un serveur Linux sans connaissances Unix particulières.

Artica propose alors la gestion de la messagerie, du partage de fichiers, des accès VPN, du proxy Internet avec les sécurités qui s'imposent comme l'anti-Spam, l'antivirus et le contrôle des sites web.

### **A qui s'adresse Artica ?**

Artica assure le paramétrage des logiciels Open Source et du système Linux.

De cette mission, toute personne ou entreprise désireuse de disposer d'un serveur de messagerie et/ou d'un serveur Web et/ou d'un serveur de fichiers et/ou d'un proxy Internet peut s'équiper du logiciel Artica.

### **Licence et support**

Artica est un logiciel libre, il peut être installé, déployé librement et sans contraintes de licence.

Artica Technology propose des services d'installation, de maintien et de support du logiciel Artica.

Elle propose aussi des services d'adaptation afin d'offrir des fonctionnalités spécifiques .

Aussi, si vous désirez revendre Artica en adaptant le logiciel à votre infrastructure.

Pour ce faire, veuillez contacter par eMail

Mr Tougeron Florent [ftougeron@artica-technology.com](mailto:ftougeron@artica-technology.com)

**Bur : 09.61.07.21.53**

**Mobile : 06.72.95.40.52**

## Que fait Artica ?

La force des logiciels Microsoft est de pouvoir fournir une interface IHM (Interface Homme/Machine) permettant à des personnes non familières à l'administration du système de pouvoir gérer, surveiller, administrer un serveur.

Artica a pour but de proposer les mêmes fonctionnalités sur des systèmes Linux.

Artica offre alors la possibilité de « **piloter** » un système Linux à travers une interface web SSL.

Des profils administrateurs peuvent être créés afin de pouvoir dédier les tâches d'administration à plusieurs personnes

Les tâches d'administration sont les suivantes :

- Administrer, surveiller les **mise à jour** du système.
- Administrer les paramètres **réseau** du serveur.
- Gérer les **comptes utilisateurs** à travers une base OpenLDAP.
- Administrer un serveur de **messagerie** complet comprenant la **gestion des boîtes aux lettres** (cyrus-imap ou bien Zarafa), le **roulage** de la messagerie (Postfix), l'**antispam** (Spamassassin, Kaspersky Anti-Spam Gateway, amavis, milter-greylist), la sécurité **antivirus** (ClamAv, Kaspersky For Linux mail server).
- Administrer un **Proxy Web** (Squid) comprenant la gestion des **caches**, le **filtrage d'URL** (ufdbguard, squidGuard), l'**antivirus** (C-ICAP, squidclamav, Kaspersky For Proxy server).
- Administrer un **serveur de fichiers** (Samba) qu'ils soit de façon autonome ou en **contrôleur de domaine** comprenant la gestion **antivirus** avec ClamAv et Kaspersky For Samba server.
- Administrer un serveur **VPN** (OpenVPN).
- Administrer un système de **virtualisation** (VirtualBox) et de VDI

## ***Que fait Postfix Instant IpTables***

« Postfix Instant IpTables » ou en français « Règles IpTables instantanées » permet de créer des règles de pare-feu sur un émetteur de façon instantanée en fonction d'évènements particuliers.

*IpTables est un par-feu installé de base sur un système Linux.*

*Sans le savoir un propriétaire d'un système Linux dispose déjà d'un pare-feux de très bonne qualité.*

### **Quel est l'intérêt ?**

Beaucoup d'adresses d'émetteurs sont des spammeurs.

Même si les paramètres de Postfix, Kaspersky Anti-Spam, Spamassassin ou Amavis permettent de bloquer les messages provenant de ces adresses, **votre serveur se fatigue énormément.**

En effet, lorsqu'un spammeur connu tente d'envoyer un Spam, votre serveur effectue ces mécanismes :

1. Ouverture du port sur le démon Postfix.
2. Écriture des premières commandes SMTP.
3. Vérification DNS, résolution du nom d'hôte, voir envoi les premières commandes aux filtres additionnels.
4. Rejet de la connexion

Ces 4 opérations vont se répéter autant de fois que l'émetteur souhaite émettre un message.

### ***Déchargez votre serveur !***

Multipliez ces 4 opérations par 500 voir 600 adresses de Spammeurs en même temps et vous retrouvez votre serveur ne faire que :

- Rejeter des connexions
- Ne faire que des requêtes sur les serveurs DNBSL
- Augmenter sa charge par la création de PIPE(S) vers Amavis, spamassassin ou Kaspersky.

Même si à la finalité vous ne recevez pas de SPAM !

L'idée de cette technologie est d'endiguer le phénomène par la création d'une règle de pare-feu sur les adresses IP de Spammeurs « habitués » à vous émettre du spam.

De ce fait, le noyau interdit l'ouverture du port et aucun processus n'est alors alerté d'une connexion.

*Ce principe se retrouve dans un produit bien connu nommé « Fail2Ban ». Toutefois Fail2ban ne propose pas l'esprit communautaire bien qu'il se peut qu'il soit intégré dans le futur.*

### ***Assurez une bande passante de qualité***

L'intérêt supplémentaire est de pouvoir décharger la bande passante. En effet les ouvertures de connexion sur le serveur, aussi infimes soit-elles, consomment de la bande passante de façon globale.

De surcroît la bande passante utilisée est la bande passante « montante » (upload), celle qui dans le cas d'une connexion ADSL est très limitée (quelques kb/s)

**Une règle de pare-feu enraye le phénomène définitivement.**

## Comment ça marche ?

Artica dispose d'un processus qui surveille en temps réel les événements de Postfix « postfix-logger ».

Une succession d'expressions régulières permet à ce processus de détecter un comportement anormal d'un serveur émetteur.

*Ce comportement anormal est notifié par Postfix mais cela ne veut pas dire que Postfix va rejeter la connexion. Il va simplement informer dans le système des événements.*

1. Il va ranger ces comportements anormaux dans des catégories que vous pouvez visualiser à travers l'interface.
2. Chaque catégorie dispose d'un seuil maximal de comportement détecté.
3. Lorsque le serveur dépasse le seuil, alors une règle de pare-feu est automatiquement ajoutée et le serveur est rejeté d'un point de vue réseau définitivement.

*Les règles créées se focalisent que sur le port 25...*

## Esprit communautaire

L'idée du principe est de « prévenir » d'une éventuelle connexion d'une adresse de spammeur.

Aussi Artica met en place un système « communautaire automatique ».

À fréquences régulières (environ toutes les 300 minutes), le script « `exec.smtp-hack.export.php` » est en charge d'exporter les règles que votre serveur a détecté vers le serveur central Artica et d'importer les règles des autres serveurs.

Au bout d'une heure environ, vous devriez retrouver des nouvelles règles dans le champ « communauté »

Postfix Instant IpTables is a feature that analyze mails history, when senders servers handle too many ban events, artica will add automatically the IP address of this server into the firewall with this feature you will increase performances by filter these spammers directly trough the network interface without stress your mail server.

Updated from community repository: **82 Rules**  
local: **0 Rules**

## Mise en place avec Artica

- Dans le menu de gauche, sélectionnez « **messaging** » puis « **Instant Iptables** »
- Passer le rond rouge à vert afin d'activer la fonctionnalité.

Artica recherche: [ ] Soumettre » Communauté Support 1.5.020501  
GERER VOTR... PARAMETRES... INSTALLATION LOGI... SERVICES & AP... EXPLORATEUR DECONNEXION CACHE

Statut scores et paramètres Gérer vos règles actives hôtes>Liste Blanche

Activez Postfix Instant IpTables  
Si vous activez en vert cette fonction, Artica sera en mesure de rajouter des règles dans le pare-feu afin d'interdire les serveurs émetteurs qui atteignent un nombre maximal d'erreurs de transfert.

Afficher dans le menu de gauche:

Appliquer »

Postfix Instant IpTables est une fonctionnalité qui analyse l'historique des messages. Lorsque les émetteurs font trop régrir les barrières de sécurité, Artica va automatiquement bannir l'adresse IP au moyen de règles de Pare-feux. Avec cette fonctionnalité vous allez augmenter les performances par le rejet des spammers directement par la pare-feu.

Mis à jour via la communauté: **0 Règles**  
local: **0 Règles**

## Personnaliser la sensibilité du scanner

L'onglet « Scores et paramètres » vous permet d'augmenter les seuils de détection et de création d'une règle automatique.

Le principe est simple :

*Au bout de combien d'erreurs dans chaque catégorie l'adresse de l'émetteur sera bloquée ?*

Si par exemple, vous indiquez la valeur « Trop de Timeout » à 2, au bout de deux messages tentés d'être émis mais avec un temps d'émission des données trop long, le serveur sera définitivement bloqué.

Indiquez les limites d'erreurs de connexions et scores qui vont correspondre à une règle

Indiquez les seuils du nombre maximal d'erreurs rencontrées par le moteur SMTP. Lorsque le seuil est atteint, un règle de pare-feux sera ajoutée. Si vous voulez désactiver la surveillance d'une erreur particulière, indiquez 0 dans le champs correspondant.

Impossible de résoudre le serveur émetteur:	10
Échec temporaire dans la résolution du nom:	2
Trop de timeout:	10
Trop d'erreurs dans le protocole SMTP:	10
Échec d'authentification SMTP:	15
Bloqué par les listes noires DNS:	5
Envoi à un destinataire inconnu:	10
Bloqué par le filtre anti-spam (amavis/spamassassin):	5

Appliquer

## Visualiser, désactiver les règles.

L'onglet « Gérer vos règles actives » vous permet d'influer sur le comportement du pare-feu.

Remarquez que certaines règles dispose de l'icône de suppression « grisé ».

Cela veut dire que la règle provient de la « communauté ».

*La supprimer n'a pas de sens puisqu'elle sera à nouveau ajoutée à la prochaine mise à jour.*

SERVEUR	ACTIVÉ	ÉVÉNEMENTS
94.96.17.189.dynamic.saudi.net.sa <small>94.96.17.189 ajouté le 2011-02-05 13:27:09</small>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
18912169103.user.veloxzone.com.br <small>189.12.169.103 ajouté le 2011-02-05 13:27:09</small>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
80.93.126.114.ett.ua <small>80.93.126.114 ajouté le 2011-02-05 13:27:09</small>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
net255-17.perm.ertelecom.ru <small>212.33.255.17 ajouté le 2011-02-05 13:27:09</small>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
bd782c6f.virtua.com.br <small>189.120.44.111 ajouté le 2011-02-05 13:27:09</small>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
178-171-56-187.goodline.info <small>178.171.59.187 ajouté le 2011-02-05 13:27:09</small>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
mario.130.50.vamion.com <small>203.99.130.50 ajouté le 2011-02-05 13:27:09</small>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
178-137-1-91-kie.broadband.kyivstar.net <small>178.137.1.91 ajouté le 2011-02-05 13:27:09</small>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

*Si vous désirez supprimer une règle de la « communauté », décochez alors la case « Activé » sur la règle. Elle sera alors retirée du pare-feu.*

## Listes blanches

Il se peut qu'un serveur de vos correspondants soit ajouté par le moteur. Mais comme vous le connaissez vous pouvez le désactiver complètement.

*En faites, la section « Hôtes:Liste Blanche » influe à la fois sur le moteur Instant IpTables mais aussi sur les autres filtres associés.*

Cliquez sur le bouton « ajouter » et indiquez l'adresse IP de l'émetteur qui doit être mis en liste blanche.

Donnez l'adresse IP du serveur qui ne sera jamais bloqué.

AJOUTEZ UN SERVEUR EN LISTE BLANCHE.

192.168.1.1 (192.168.1.1)

Annouce de la page https://192.168.1.108:9000 :

Donnez l'adresse IP du serveur qui ne sera jamais bloqué.

Annuler OK