

Artica

Lutte contre le SPAM avec PostScreen

Révision Du 03 Février 2011 version 1.5.020317

Artica

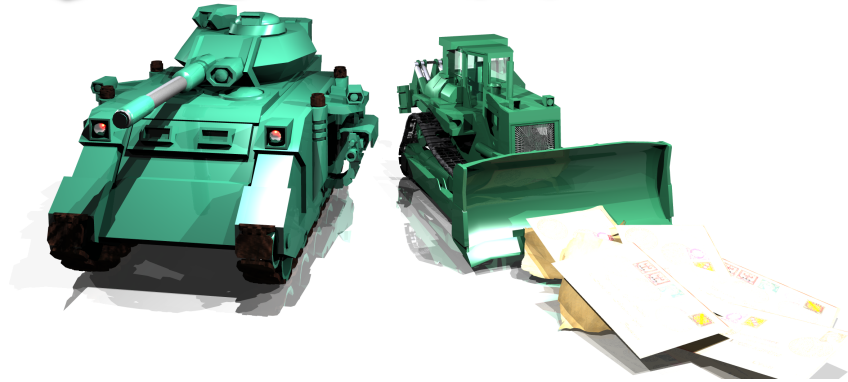


Table des matières

Introduction :	2
Historique du projet :	2
A qui s'adresse Artica ?	2
Licence et support	2
Que fait Artica ?	3
Lutte contre le SPAM avec PostScreen	4
Les Zombies et BotNets, 99% du Spam reçu	4
PostScreen, une solution	5
Les différents tests effectués par PostScreen.....	5
Les lignes « vides ».....	5
Le half-duplex.....	5
Les commandes NON-SMTP.....	5
Requêtes sur les serveurs DNS Blacklist.....	6
Mise en place de PostScreen	7
Les protocoles de tests.....	8
Les serveurs de blacklist DNSBL	9

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
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 **cache**s, 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

Lutte contre le SPAM avec PostScreen

Les Zombies et BotNets, 99% du Spam reçu.

La version 2.8 de Postfix dispose désormais d'une nouvelle fonctionnalité contre 99% du SPAM.

Cette fonctionnalité se présente sous la forme de 3 démons « postscreen » qui effectue des tests sur le protocole SMTP, « dnsblog » qui est chargé des vérifications des émetteurs avec les serveurs de blacklist DNS et « tlsproxy » permettant de prendre en charge le STARTTLS du protocole SMTP.

Wietse, le fondateur de Postfix dit : “Zombies suck the life out of the mail server.” pendant la conférence des serveurs de messagerie en 2009 en collaboration avec IBM research.

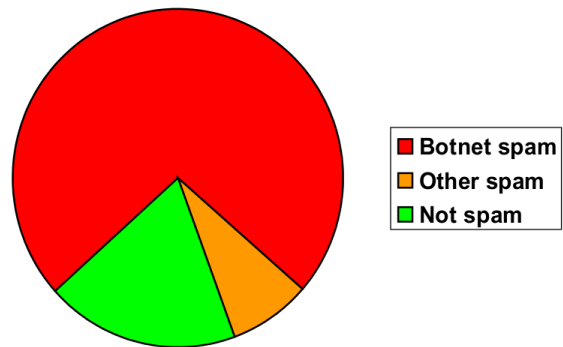
Il exprime en ces termes que les Zombies ou Botnets sont la cause de 99% du spam reçu.

Les Zombies ou Botnets sont des programmes malicieux installés sur des ordinateurs dont le but est d'utiliser la puissance et la bande passante de son hôte afin d'envoyer des pourriels à toutes destinations.

MessageLabs en 2008 confirmait déjà cette tendance.

81% of email is spam, 90% is from botnets¹

Celle-ci s'est amplifiée depuis...

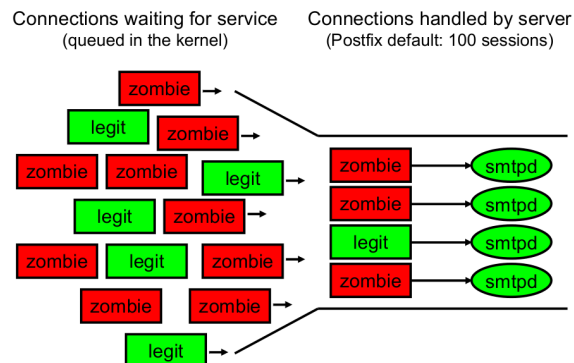


¹MessageLabs 2008 annual report

Même si des ressources et filtres sont ajoutés afin d'endiguer l'émission du SPAM, les zombies engorgent les connecteurs SMTP et ralentissent considérablement le traitement des messages de production.

Zombies keep mail server ports busy

En effet, les connecteurs de sessions SMTP sont occupés à traiter des connexions illégitimes.

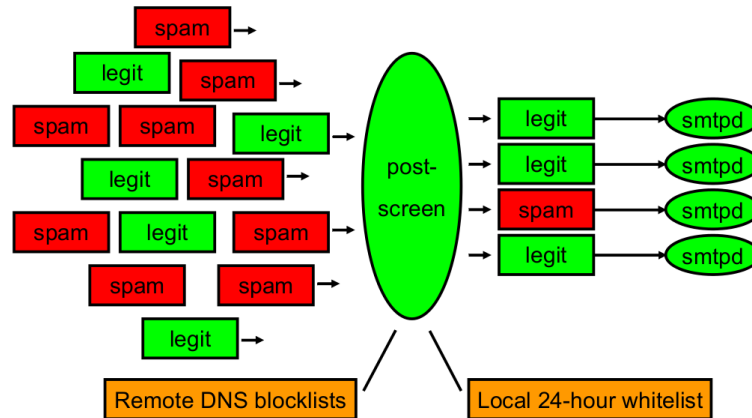


Changing threats

PostScreen, une solution

Les recherches de Weitse, l'ont amené à élaborer un nouveau processus qui sera en charge d'effectuer un filtre en amont des connecteurs SMTP.

Persistent overload - before-smtpd connection filter
Prior work: OpenBSD spamd, MailChannels TrafficControl, M.Tokarev



Ce démon est développé afin d'effectuer des vérifications rapides pour déterminer si l'émetteur est un Zombie ou pas. Ces tests rapides sont accompagnés d'une gestion de cache qui assure un bon niveau de performances de traitement.

Les différents tests effectués par PostScreen

PostScreen s'attarde sur 4 niveaux de vérifications :

Les lignes « vides »

Le protocole SMTP est un protocole qui utilise des retours chariots de type CRL+LF avec une taille de ligne déterminée.

Beaucoup de Botnets corromps cette « tradition » par l'utilisation unique d'un LF. Cette forme de fin de ligne est souvent acceptée par les serveurs de messagerie.

Cette première détection permet de rejeter un grand nombre d'émetteurs « non-conformes »

Le half-duplex

Le protocole SMTP est un protocole de communication bi-latérale, l'émetteur se doit d'envoyer une commande SMTP et d'en attendre la réponse du récepteur.

Pour les botnets, il est plus facile d'envoyer les commandes SMTP et les données du message en une seule fois dans la session SMTP en lieu et place d'un vrai processus de communication avec le serveur récepteur (ce qui complique la codification d'un moteur de messagerie et alourdit le code viral).

Cette seconde détection détermine si l'émetteur du message utilise les normes de communication et est développé en tant que vrai processus d'émission de message.

Les commandes NON-SMTP

Beaucoup de BotNets utilisent un proxy pour sortir sur Internet afin d'émettre des messages de Spam.

L'utilisation d'un proxy rajoute des commandes non standard comme « CONNECT », « GET »... Ces commandes relatives au protocole HTTP sont généralement ignorées par les serveurs de messagerie et les messages peuvent être transmis.

Dans le cadre de l'utilisation de PostScreen, la détection de ces commandes assurent le rejet de la session SMTP et endigue le SPAM.

Requêtes sur les serveurs DNS Blacklist

Les adresses réseau des mauvais émetteurs sont référencés dans des bases disponibles sur Internet et pouvant être consultées par le protocole DNS.

PostScreen via le démon `dnsmlog` permet de consulter ces bases et de s'assurer que l' émetteur n'est pas référencé en tant que mauvais émetteur.

L'association de cette technologie avec un outil Anti-Spam de « contenu » tel que SpamAssassin ou Kaspersky Anti-Spam permet de rapprocher le taux de rejet de pourriels à 100%

Artica assure le maintient et la mise en place de ces technologies.

La mise en place de PostScreen dans Artica à la fois supportée en utilisant une seule instance du moteur Postfix mais aussi en utilisant le principe des multi-instances.

Vous pouvez retrouver les déclarations de Weitse sur PostScreen à cette adresse : <http://www.artica.fr/download/postscreen.pdf> et

La documentation en ligne technique et mise en place en ligne de commande à cette adresse :

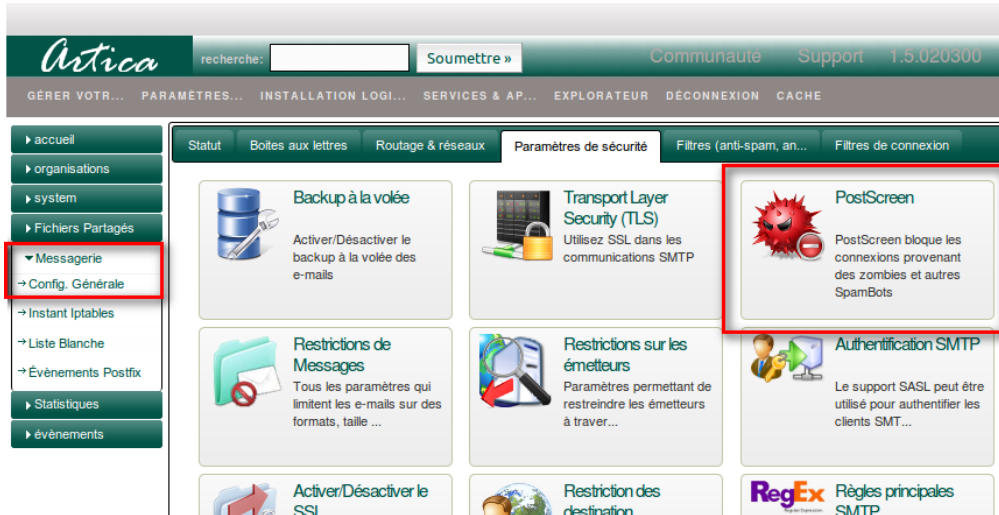
http://www.postfix.org/POSTSCREEN_README.html

Mise en place de PostScreen

Vous devez vous assurer que votre serveur Postfix est en version 2.8.

Utilisez alors le gestionnaire d'installation afin de mettre à jour Postfix.

Une fois cette opération et après avoir « vidé le cache de la console », placez-vous dans la section « **Paramètres de sécurité** »



Un nouvel icône « **PostScreen** » apparaît. Cliquez sur cet icône.

Activez le service PostScreen en passant en vert le rond rouge et cliquez sur « **appliquer** »



Les protocoles de tests

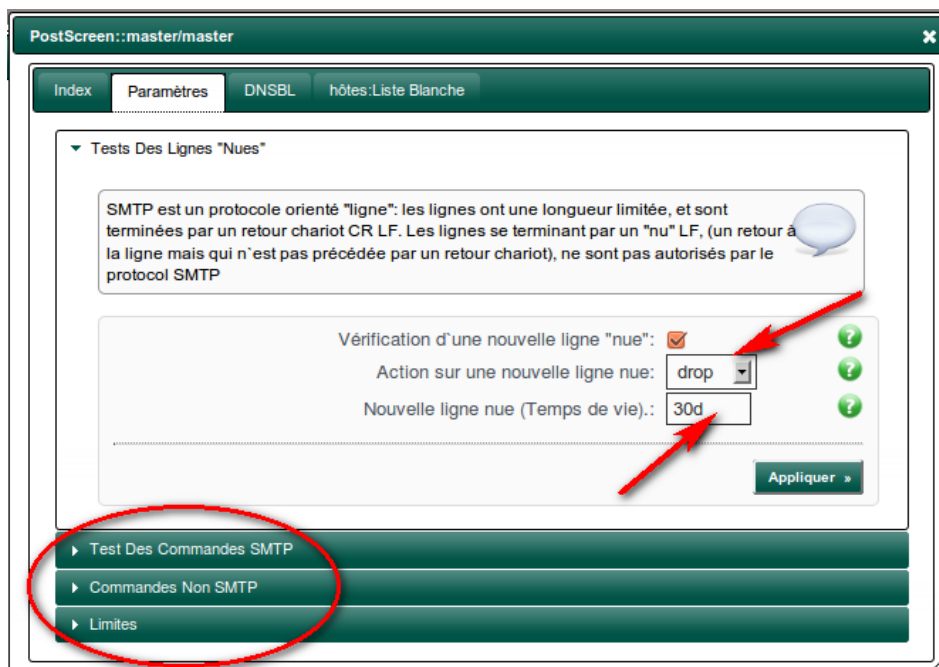
Cliquez sur l'onglet « Paramètres »

Dans cette section vous pourrez activer ou désactiver les **3 principaux protocoles** de tests de PostScreen :

Les lignes « nues » (non CR+LF), les commandes SMTP (half-duplex) et les commandes Non SMTP.

Chaque protocole de test vous permet de définir une action à entreprendre si le serveur émetteur fait correspondre une détection.

- « **drop** » : rejette la session et met en cache, le rejet. A la prochaine connexion, l'émetteur sera directement rejeté sans le tester.
- « **ignore** » : une trace est générée dans les logs mais le serveur passe au protocole de test suivant, très utile pour tester avant de bloquer.
- « **enforce** » : Autorise PostScreen à lancer les autres vérifications mais rejettera les tentatives de livraison des courriers en émettant une réponse SMTP 550, inscrit les informations dans le journal. Il n'y a pas de mise en cache, a la prochaine tentatives ce test sera à nouveau effectué.



Chaque protocole de test dispose d'un « **temps de vie** » (ou TTL). Le résultat est alors enregistré pendant un période déterminée ce qui permet à PostScreen de ne pas refaire le test à la prochaine connexion.

Le serveur sera rejeté ou accepté directement si il revient émettre un message.

Les serveurs de blacklist DNSBL

Cliquez sur l'onglet « DNSBL »

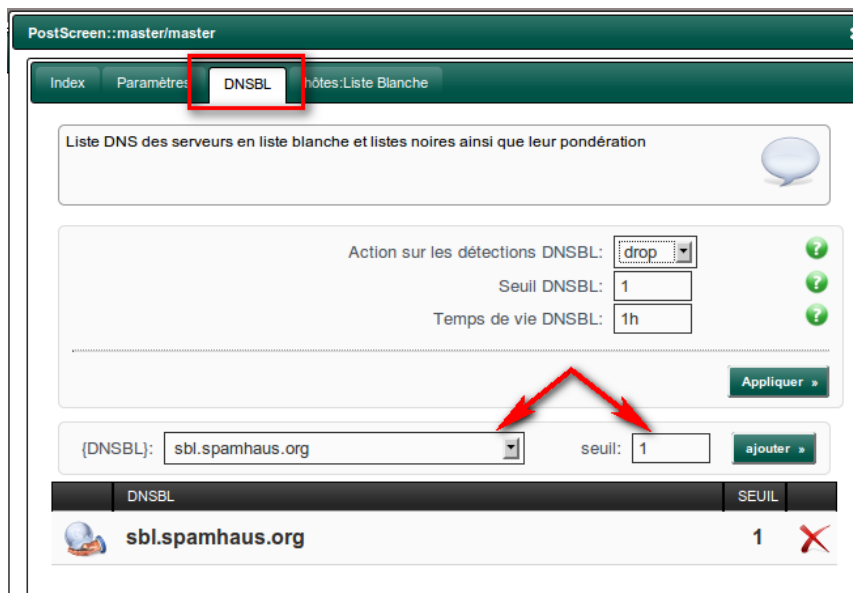
Cette section vous permet d'ajouter des services sur Internet nommés serveurs DNS de Blacklist (DNSBL) qui seront questionnés par PostScreen à chaque connexion d'un nouvel émetteur de messages.

Indiquez un note globale des réponses DNSBL dans le champ « Seuil DNSBL ».

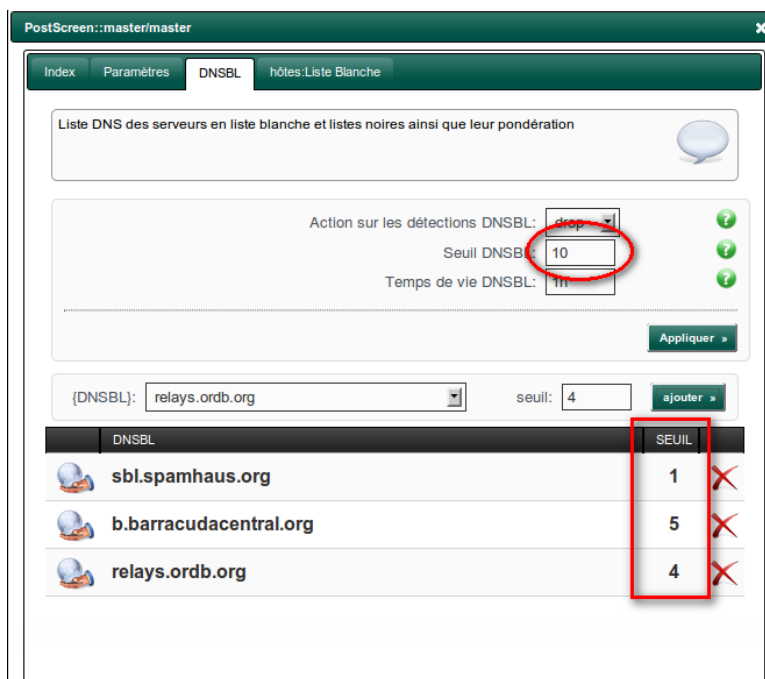
Par exemple, si vous indiquez 5, le serveur émetteur devra disposer de 5 points pour être rejetés.

Utilisez la liste déroulante DNSBL qui vous permet d'ajouter les serveurs DNS de base de données.

Ajoutez un point de détection dans le champs « seuil »



Dans notre exemple précédent si nous indiquons une note globale de 5, l'émetteur doit, par exemple, correspondre à 5 serveurs de listes avec une note de 1 ou bien deux serveurs de liste dont la première note est 3 et la deuxième note est 2



Cette méthode permet de faire confiance à la totalité des serveurs de blacklist avec des préférences afin d'éviter le principe des « fausses alertes » à travers un serveur de liste qui n'est pas mis à jour régulièrement