

# OpenBSD Spamd

Nicolas Greneche

MAPMO  
Projet SDS

Mathrice Rouen 2008

- 1 Introduction
- 2 Architecture et Algorithmes
- 3 Composants
- 4 Lancement et Paramètres
- 5 Exploitation

- Système d'exploitation
- Orienté sécurité
- Séparation système de base / ports
- Support des modèles MAC et DAC
- Audit strict de sécurité du système de base
- OpenBSD c'est Spamd ...

- Système d'exploitation
- Orienté sécurité
- Séparation système de base / ports
- Support des modèles MAC et DAC
- Audit strict de sécurité du système de base
- OpenBSD c'est Spamd ...
- ... mais aussi OpenSSH, OpenNTPD, OpenCVS, OpenBGPD et Packet Filter !

- Macros de remplacement (attribut unique ou liste)
- Redirections (NAT / RDR / BiNAT)
- Règles
- Tables (rapidité des lookups / dynamiques)
- Ancres (règles dynamiques)
- QoS
- authpf
- CARP & PFSync
- Port "expiretable"

## **Installation de spamd**

## **Installation de spamd**

→ Rien à faire, c'est dans le système de base

## **Configuration de spamd**

## Installation de spamd

→ Rien à faire, c'est dans le système de base

## Configuration de spamd

Dans `/etc/pf.conf` :

```
table <spamd-white> persist  
no rdr inet proto tcp from <spamd-white> to any port smtp  
rdr pass inet proto tcp from any to any port smtp → 127.0.0.1  
port spamd
```

## Installation de spamd

→ Rien à faire, c'est dans le système de base

## Configuration de spamd

Dans `/etc/pf.conf` :

```
table <spamd-white> persist  
no rdr inet proto tcp from <spamd-white> to any port smtp  
rdr pass inet proto tcp from any to any port smtp → 127.0.0.1  
port spamd
```

Dans `/etc/rc.conf.local` :

```
spamd_flags=""
```

## Installation de spamd

→ Rien à faire, c'est dans le système de base

## Configuration de spamd

Dans `/etc/pf.conf` :

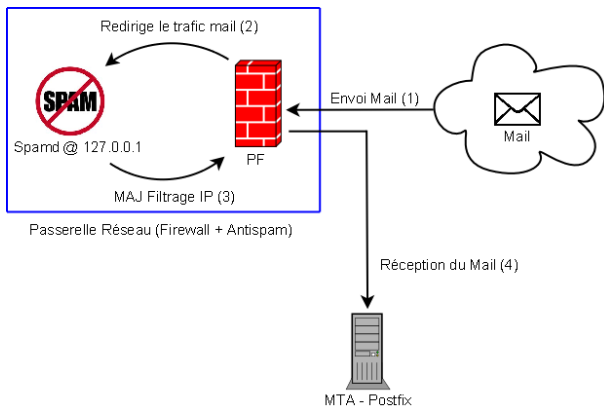
```
table <spamd-white> persist  
no rdr inet proto tcp from <spamd-white> to any port smtp  
rdr pass inet proto tcp from any to any port smtp → 127.0.0.1  
port spamd
```

Dans `/etc/rc.conf.local` :

```
spamd_flags=""
```

Merci de votre attention, des questions ?

# Architecture



## **Blacklist :**

- Stockée dans une table
- Alimentée par le spamd.conf et / ou par l'administrateur
- Hôtes de cette table ne parlent jamais au vrai MTA

## **Discussion :**

- Source des blacklist ?
- Fréquence de réassignation des IP par les FAI

## Whitelist :

- Stockée dans une table <spamd-white>
- Alimentée par le spamd.conf et / ou par l'administrateur
- Hôtes de cette table court-circuitent spamd pour parler directement avec le MTA

## Discussion :

- Combiner avec SPF (ou pas !)

## SPF - Sender Policy Framework

Pour lutter contre les utilisations erronées de noms de domaines dans les mails forgés, SPF propose d'associer une liste de MTA légitimes (autorisés à envoyer du courrier) à un nom de domaine dans le serveur DNS servant la zone associée au domaine. Pour récupérer ces enregistrements, il suffit de demander au DNS les enregistrements de type TXT.

- Listes maison

## Greylist :

- Refuse première transaction (erreur 451)
- Le MTA émetteur est stocké dans la base de données de spamd (spamdb) en attente d'une retransmission de messages
- Si le message est retransmis, alors l'émetteur passe en whitelist

## Discussion :

- Efficace : les 20% d'administration qui suppriment 80% du spam
- Attention aux MTA émetteurs mal configurés (et il y en a ...)
- Attention aux fermes de serveurs SMTP (multiple IP sources pour le même message)

## Greytrapping :

- Création d'une (ou plusieurs) adresse(s) bidon(s) pour capter le spam (honeypot à spam)
- Si une machine en greylist cherche à envoyer un message à cette adresse, alors elle est ajoutée dans la table <spamd-greytrap>
- Les réponses de spamd vers les machines de cette table sont tarpitées (réponses lentes)

## Discussion :

- Fun, surtout si l'adresse est inscrite dans les commentaires HTML de votre page web
- Attention à bien choisir une adresse qui ne sera jamais utilisée (gestion des mails séparée de création de comptes)
- Pourrir la vie des spammers

- **Spamd** : un faux MTA traditionnellement bindé sur l'interface de loopback. Son rôle est d'examiner les transactions mail (à destination du port smtp) passant par le pare-feu. Il va gérer les listes blanches, grises et noires.
- **Spamlogd** : programme qui surveille les requêtes mail (à destination du port smtp) sur l'interface pflog. C'est lui qui va entretenir la liste blanche propre à spamd. Les règles d'acceptation du trafic SMTP au niveau PF doivent être logguées.

Dans `/etc/rc.conf.local`

```
spamd_flags="-v -l 127.0.0.1 -n Postfix -h realmta.example.org -G  
7 :4 :864"
```

```
spamd_grey=YES
```

```
spamlogd_flags="-l pflog0"
```

Dans `/etc/rc.conf.local`

```
spamd_flags="-v -l 127.0.0.1 -n Postfix -h realmta.example.org -G  
7 :4 :864"  
spamd_grey=YES  
spamlogd_flags="-l pflog0"
```

## Triplet de temps

7 : Temps au delà duquel une tentative de reconnexion en liste grise fait passer la connexion en liste blanche (en minutes)

4 : Temps au delà duquel une connexion sur liste grise est supprimée de la base de données de Spamd (en heures)

864 : Temps d'inactivité maximum d'un hôte sur liste blanche (spamd-white) avant sa suppression

- `spamdb | grep GREY`
- `spamdb | grep nicolas.greneche@example.org`

- spamdb | grep GREY
- spamdb | grep nicolas.greneche@example.org

## Analyse de la sortie 1/2

```
GREY | 62.209.218.70 | usgs.gov | <jraber@valkyrie.net> |  
<nicolas.greneche@example.org> | 1194181594 | 1194195994 |  
1194195994 | 3 | 0
```

- Le type d'enregistrement (WHITE ou GREY)
- L'IP de l'émetteur du message
- Le message HELO envoyé par l'émetteur
- Adresse mail source
- Adresse mail destination

- spamdb | grep GREY
- spamdb | grep nicolas.greneche@example.org

## Analyse de la sortie 2/2

```
GREY | 62.209.218.70 | usgs.gov | <jraber@valkyrie.net> |  
<nicolas.greneche@example.org> | 1194181594 | 1194195994 |  
1194195994 | 3 | 0
```

- Date de la première entrée dans la spamdb (première tentative de connexion)
- Date à laquelle l'enregistrement sera promu sur liste blanche
- Date d'expiration de l'enregistrement dans la spamdb
- Nombre de fois où une telle connexion a reçu une temporary failure de Spamd
- Nombre de fois où une telle connexion est passée sur liste blanche

- `spamdb -a <IP_à_whitelister>`
- `pfctl -t spamd-white -T show`
- `pfctl -f /etc/pf.conf`
- `tcpdump -netti /dev/pflog0`