SPF + DKIM + DMARC

messagerie, sécurité, SPF, DKIM, DMARC

Face au nombre exponentiel de spam, des méthodes ont été mises en place au fur et à mesure des années afin de s'assurer que l'expéditeur des courriels que nous recevons est bien celui qu'il prétend être. Pour nous aider, trois systèmes sont mis en oeuvre :

- SPF
- DKIM
- DMARC

SPF (Sender Policy Framework) est un système qui identifie aux serveurs de messagerie les hôtes autorisés à envoyer des emails pour un domaine donné. La configuration de SPF permet d'éviter que votre courrier électronique soit classé comme spam.

DKIM (DomainKeys Identified Mail) est un système qui permet à vos serveurs de messagerie officiels d'ajouter une signature aux en-têtes des messages sortants et d'identifier la clé publique de votre domaine afin que les autres serveurs de messagerie puissent vérifier la signature. Comme avec SPF, DKIM évite que votre courrier ne soit considéré comme du spam. Il permet également aux serveurs de messagerie de détecter le moment où votre courrier a été falsifié en transit.

DMARC (Domain Message Authentication, Reporting & Conformance) vous permet d'annoncer aux serveurs de messagerie quelles sont les stratégies de votre domaine concernant les messages qui échouent aux validations SPF et / ou DKIM. Il vous permet également de demander des rapports sur les messages ayant échoué aux serveurs de messagerie de réception.

Source : Linode

Installation

```
sudo aptitude update && sudo aptitude install opendkim opendkim-tools
postfix-policyd-spf-python postfix-pcre
```

Nous ajoutons l'utilisateur postfix au groupe opendkim

```
adduser postfix opendkim
```

Configuration

Éditez le fichier /etc/postfix/master.cf pour y ajouter ces lignes à la fin :

```
policyd-spf  unix  -       n       n       -       0       spawn
    user=policyd-spf argv=/usr/bin/policyd-spf
```

Nous ajoutons les entrées suivantes dans le champs smtpd_recipient_restrictions du fichier /etc/postfix/main.cf :

```
smtpd_recipient_restrictions=
  ...
  reject_unauth_destination,
  check_policy_service unix:private/policyd-spf
  ...
```

À la fin du fichier /etc/postfix/main.cf nous ajoutons :

```
# Milter configuration
# OpenDKIM
milter_default_action = accept
# Postfix ≥ 2.6 milter_protocol = 6, Postfix ≤ 2.5 milter_protocol = 2
milter_protocol = 6
smtpd_milters = local:/opendkim/opendkim.sock
non_smtpd_milters = local:/opendkim/opendkim.sock

#Milter
#smtpd_milters = inet:127.0.0.1:2500
#non_smtpd_milters = inet:127.0.0.1:2500

# SPF
policyd-spf_time_limit = 3600
```

Nous éditons le fichier /etc/opendkim.conf, et remplaçons son contenu par celui-ci :

```
# This is a basic configuration that can easily be adapted to suit a
standard
# installation. For more advanced options, see opendkim.conf(5) and/or
# /usr/share/doc/opendkim/examples/opendkim.conf.sample.

# Log to syslog
Syslog          yes
# Required to use local socket with MTAs that access the socket as a non-
# privileged user (e.g. Postfix)
UMask           002
# OpenDKIM user
# Remember to add user postfix to group opendkim
UserID          opendkim

# Map domains in From addresses to keys used to sign messages
KeyTable        /etc/opendkim/key.table
SigningTable        refile:/etc/opendkim/signing.table

# Hosts to ignore when verifying signatures
ExternalIgnoreList  /etc/opendkim/trusted.hosts
InternalHosts       /etc/opendkim/trusted.hosts

PidFile             /var/run/opendkim/opendkim.pid
Socket             local:/var/spool/postfix/opendkim/opendkim.sock
```

```
# Commonly-used options; the commented-out versions show the defaults.
Canonicalization    relaxed/simple
Mode            sv
SubDomains      no
#ADSPAction     continue
AutoRestart     yes
AutoRestartRate     10/1M
Background      yes
DNSTimeout      5
SignatureAlgorithm  rsa-sha256

# Always oversign From (sign using actual From and a null From to prevent
# malicious signatures header fields (From and/or others) between the signer
# and the verifier.  From is oversigned by default in the Debian package
# because it is often the identity key used by reputation systems and thus
# somewhat security sensitive.
OversignHeaders     From
```

Nous mettons les bons droits sur le fichier :

```
chmod u=rw,go=r /etc/opendkim.conf
```

Nous créons les répertoires qui vont accueillir les clés et informations opendkim.

```
mkdir /etc/opendkim
mkdir /etc/opendkim/keys
chown -R opendkim:opendkim /etc/opendkim
chmod go-rw /etc/opendkim/keys
```

Créez le fichier /etc/opendkim/signing.table et ajoutez-y les informations concernant vos domaines :

```
*@example.com   example
```

À suivre.

Ajout des informations DNS

Nous allons ajouter les informations dans la zone DNS de notre serveur de courriels :

```
@                       IN      TXT     "v=spf1 a:mail.loubrusc.org -all"
201811._domainkey       IN      TXT     ( "v=DKIM1; h=sha256; k=rsa;
s=email; "
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0c6vq2vr5EmhcgpJfiX2uyVMsEsai
abo5IjlkUdnMlQbD5fpsSQx3YOIrReFCZAW3nWfVLhcpig402fTmzvNFFw2o4o9aLFhJJgtGFI+w
KBQ0bc8vUMO5vxG4FzN15i+/F+Ao4ZvEkgurD+/rDwe6UCb8$
"7au+/HrdVq7SRk3nf1xHPHzQuKq0Be4+YjenERalDrqySuZvQ7F+xOTrT8K/0aXfPi6TeYS/6Av
TfZkmuH9kdNQAhbK1CmRUMAuSWa+vwe5FCfCVo7848EovkXt0znvrp0tuA/cwIDAQAB" )  ; --
--- DKIM key 201811 for loubrusc.org
```

```
_dmarc                  IN      TXT     "v=DMARC1; p=none"
```

Liens

- configure spf and dkim in postfix on debian 8
- configurer les enregistrements dkim spf et dmarc obligatoires pour l'email
- opendkim on Debian wiki
- configurez spf dkim dmarc pour l'envoi de vos emails
- test de conformité SPF DKIM DMARC
- autre site de test (limité à trois test par jour)