

Configurer Postfix avec TLS / SSL

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 Février 2007. Dernière mise à jour le 1 Mars 2007

<http://www.bortzmeyer.org/postfix-tls.html>

La demande de sécurité dans les envois de courrier électronique fait que de plus en plus de serveurs SMTP activent l'option de cryptographie TLS (nouveau nom de SSL). Cette option est normalisée dans le RFC 3207¹.

Voici ce que j'ai configuré sur mon serveur Postfix. Cela permet la confidentialité (TLS chiffre la session) et, dans une certaine mesure, l'authentification des serveurs pairs (en revanche, TLS dans le courrier n'authentifie pas l'expéditeur, il faudrait utiliser PGP). Il faut avoir installé OpenSSL et compilé Postfix avec le support de SSL. Sur Debian, cela se fait en installant le paquetage postfix-tls. Sur Gentoo, en compilant Postfix en ayant l'option "ssl" dans les USE (par exemple, en le mettant dans /etc/make.conf).

J'ai créé une autorité de certification (ce qui est très simple mais Kim Minh Kaplan suggère que j'aurais pu utiliser une autorité gratuite et ouverte comme <<http://cacert.org/>>) et tous les exemples ci-dessous supposent l'utilisation de cette CA. Les certificats signés par des CA locales sont bien plus répandus pour le courrier (où aucune vérification n'est faite, en général), que sur le Web où le navigateur vous impose une demi-douzaine de confirmations si vous osez utiliser une autre CA que celles qui sont installées avec le logiciel :

```
/etc/ssl/misc/CA.pl -newca
```

et mis les fichiers (certificat de la CA, certificats signés, etc) dans /etc/ssl/CA.

Un utilisateur ordinaire peut ensuite, sur sa machine, générer une **demande** de certificat, ici pour mille jours :

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc3207.txt>

```
openssl req -config /etc/ssl/openssl.cnf -new -nodes -keyout monserveur.key -out monserveur.csr -days 1000
```

Cette demande doit ensuite être signée par la CA pour être un certificat valide :

```
openssl ca -config ../openssl.cnf -policy policy_anything -days 1000 -out certs/monserveur.crt -infiles ~/tr
```

Ces fichiers sont ensuite copiés là où Postfix les attend. Si on a mis dans le `main.cf` :

```
smtpd_tls_key_file = /etc/postfix/postfix-key.pem
smtpd_tls_cert_file = /etc/postfix/postfix-cert.pem
```

on copie la clé en `/etc/postfix/postfix-key.pem` et le certificat en `/etc/postfix/postfix-cert.pem`.

On peut vérifier ses certificats avec :

```
openssl x509 -text -noout -in postfix-cert.pem
```

Il affichera en clair toutes les informations contenues dans le certificat.

On peut alors configurer Postfix. Le serveur prend typiquement les paramètres suivants (notez que la configuration du serveur, `smtpd` et du client, `smtp` sont complètement indépendantes) :

```
# TLS non obligatoire, a la demande du client
smtpd_tls_security_level = may
smtpd_tls_auth_only = no

# Emplacement des clés et certificats
smtpd_tls_key_file = /etc/postfix/postfix-key.pem
smtpd_tls_cert_file = /etc/postfix/postfix-cert.pem
# Facultatif:
#smtpd_tls_CAfile = /etc/postfix/cacert.pem
# Si on veut authentifier les autres, il faut indiquer où trouver les certificats
# des CA :
#smtpd_tls_CApath = /etc/ssl/certs

# Enregistrer dans un en-tête Received
smtpd_tls_received_header = yes
smtpd_tls_loglevel = 1

# Divers
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
```

Le serveur, une fois rechargé, doit alors accepter les connexions TLS. On peut le vérifier avec `telnet` :

<http://www.bortzmeyer.org/postfix-tls.html>

```
% telnet munzer.example.org smtp
Trying 208.75.84.80...
Connected to munzer.example.org.
Escape character is '^]'.
220 munzer.example.org ESMTP Postfix
EHLO foo.bar.example
250-munzer.example.org
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

La ligne STARTTLS nous indique que le serveur est prêt à faire du TLS.

Pour configurer un **client** SMTP en TLS, on met dans le `main.cf` :

```
smtp_tls_security_level = may
smtp_tls_loglevel = 1

# Le client n'a pas forcément les memes certificats que le serveur
smtp_tls_cert_file = /etc/postfix/postfix-cert.pem
smtp_tls_key_file = /etc/postfix/postfix-key.pem
```

Désormais, en envoyant un message depuis ce client vers ce serveur, on aura dans le journal l'information que TLS a été utilisé :

```
Feb 28 14:34:16 munzer postfix/smtpd[17374]: TLS connection
established from foobar.example.net[192.0.2.53]: TLSv1 with cipher ADH-AES256-SHA
(256/256 bits)
```

La même information se retrouve dans les en-têtes du message :

```
Received: from mail.example.com (foobar.example.net [192.0.2.53])
        (using TLSv1 with cipher ADH-AES256-SHA (256/256 bits))
        (No client certificate requested)
        by munzer.example.org (Postfix) with ESMTP id CC60F8C021
        for <stephane@bortzmeyer.org>; Wed, 28 Feb 2007 14:34:16 +0100
(CET)
```

Si on demande un certificat au client :

```
smtpd_tls_ask_ccert = yes
```

on obtient un en-tête Received ainsi :

<http://www.bortzmeyer.org/postfix-tls.html>

```
Received: from mail.example.com (foobar.example.net [192.0.2.53])
  (using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
  (Client CN "smtp.bortzmeyer.org", Issuer "Stephane Bortzmeyer" (verified OK))
  by mail.bortzmeyer.org (Postfix) with ESMTP id 59E6F24080E
  for <stephane@bortzmeyer.org>; Thu, 1 Mar 2007 17:40:36 +0100 (CET)
```

et, dans le journal :

```
Mar 1 17:40:36 ariane postfix/smtpd[3356]: Verified: subject_CN=smtp.bortzmeyer
.eu, issuer=Stephane Bortzmeyer
Mar 1 17:40:36 ariane postfix/smtpd[3356]: TLS connection established from foobar.example.net [192.0.2.53]
its)
```

À noter qu'on peut tester TLS en ligne de commande avec :

```
% openssl s_client -connect MYMAILSERVER:smtp -starttls smtp -cert /etc/postfix/postfix-cert.pem -key /etc/p
```

Attention, par défaut, il vérifie le certificat du serveur, il faut donc avoir une chaîne de CA valides chez le client. Si on veut juste regarder le certificat, par exemple pour voir sa validité :

```
% openssl s_client -connect MYMAILSERVER:smtp -starttls smtp \
  -cert /etc/postfix/postfix-cert.pem -key /etc/postfix/postfix-key.pem \
  -CAfile /etc/postfix/cacert.pem & /dev/null | \
  openssl x509 -noout -subject -startdate -enddate
```

Un autre outil de test est `ssl-cert-check` <<http://prefetch.net/code/ssl-cert-check>> qui permet des choses comme :

```
% ssl-cert-check -s mail.bortzmeyer.org -p 25
```

Host	Status	Expires	Days
mail.bortzmeyer.org:25	Valid	Nov 10 2010	673

On trouvera beaucoup d'autres détails dans :

- "*Postfix TLS Support*" <http://www.postfix.org/TLS_README.html> (la documentation officielle),
- "*Be your own Certificate Authority (CA)*" <<http://www.g-loaded.eu/2005/11/10/be-your-own-ca/>> ,
- "*Postfix/TLS - Lutz's very short course on being your own CA*" <http://www.aet.tu-cottbus.de/personen/jaenicke/postfix_tls/doc/myownca.html> .

Et, naturellement, pour un test complet, on peut utiliser les auto-répondeurs de courrier <<http://www.bortzmeyer.org/repondeurs-courrier-test.html>> dont plusieurs acceptent TLS.