Apache et le module GnuTLS

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 avril 2008. Dernière mise à jour le 4 décembre 2008

https://www.bortzmeyer.org/apache-et-gnutls.html

Pour faire du TLS sur un serveur HTTP Apache, la solution la plus connue est le module `mod_ssl`. Mais il en existe une autre, le module GnuTLS <http://www.outoforder.cc/projects/apache/mod_gnutls/>.

GnuTLS est une mise en œuvre libre du protocole TLS (ex-SSL, protocole normalisé dans le RFC 5246 [1]). Étant sous licence GPL, il peut être utilisé par des programmes GPL (alors que OpenSSL a une licence incompatible avec la GPL, ce qui a entrainé des problèmes pour plusieurs projets). GnuTLS offre également des possibilités qui sont absentes d'OpenSSL, comme la possibilité d'utiliser des clés PGP (RFC 5081) en sus des certificats X.509.

Sur une machine Debian, où tout est déjà compilé et empaqueté, l'installation du module `mod_gnutls` d'Apache est triviale. Un coup de aptitude install, puis `ln -s ../mods-available/gnutls.load /etc/apache2/mods-enabled` (Sébastien Tanguy me fait remarquer à juste titre qu'il existe une méthode de plus haut niveau, la commande `a2enmod`) et recharger Apache. Sa configuration peut être aussi courte que :

```
GnuTLSEnable  on
GnuTLSCertificateFile /etc/ssl/certs/ssl-cert-Example.pem
GnuTLSKeyFile /etc/ssl/private/ssl-cert-Example.key
GnuTLSPriorities NORMAL
```

Et hop, ça marche avec des clients HTTP utilisant GnuTLS comme avec ceux utilisant OpenSSL comme Konqueror.

Une des forces de GnuTLS est qu'il permet l'utilisation de l'extension de TLS SNI ("*Server Name Indication*" <http://www.gnu.org/software/gnutls/manual/html_node/Core-functions.html#gnutls_005fserver_005fname_005fget>) qui permet de mettre plusieurs certificats différents <https://www.bortzmeyer.org/auth-x509-plusieurs-noms.html> à des "*Virtual Host*" Apache se partageant une seule adresse IP. Il suffit de mettre une directive `GnuTLSCertificateFile` différente par "*Virtual Host*" :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5246.txt`

```
<VirtualHost _default_:443>
        # Site par défaut. Son certificat sera envoyé aux clients
# non-SNI
        ...
        GnuTLSCertificateFile /etc/ssl/certs/ssl-cert-DEFAULT.example.net.pem
...
<VirtualHost *:443>
        ...
        ServerName svn.example.net
        GnuTLSCertificateFile /etc/ssl/certs/ssl-cert-svn.example.net.pem
...
<VirtualHost *:443>
        ...
        ServerName viewvc.example.net
        GnuTLSCertificateFile /etc/ssl/certs/ssl-cert-viewvc.example.net.pem
...
```