

# CHANTIER DE SÉCURISATION DE L'E-MAIL À L'EPFL

MARTIN.OUWEHAND@epfl.ch, SIC



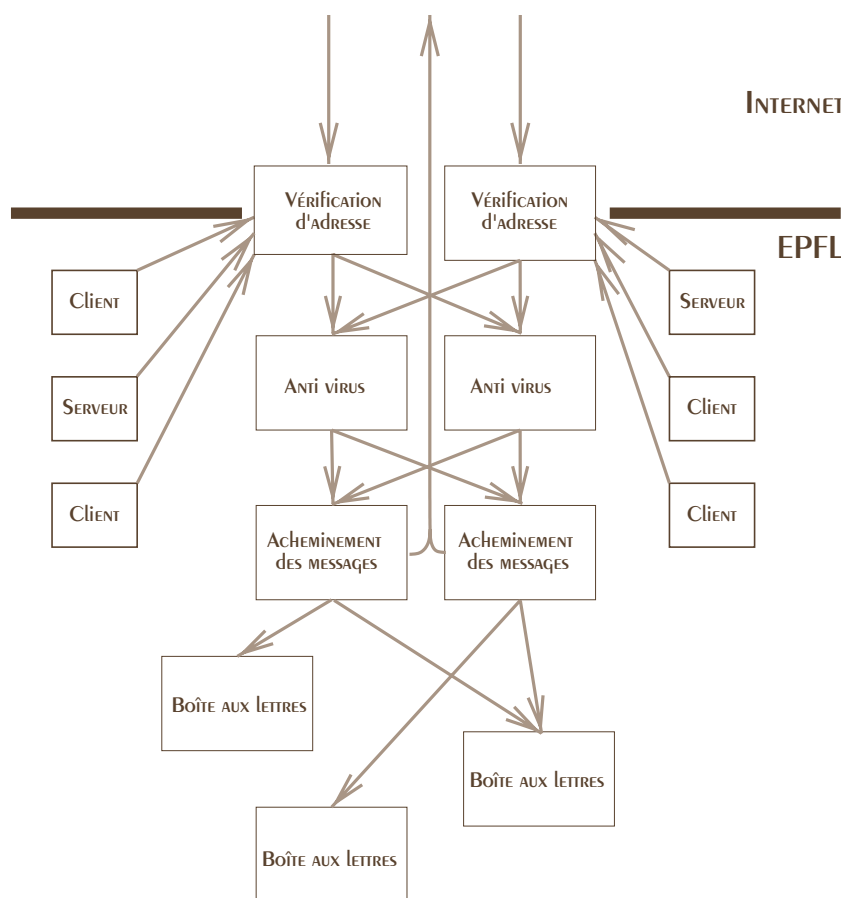
Cet article décrit quelques modifications qui vont prochainement être apportées à la configuration de l'e-mail à l'EPFL afin d'en augmenter la robustesse et la sécurité. Ces modifications seront transparentes pour la vaste majorité des membres de l'EPFL et cet article s'adresse avant tout aux administrateurs de serveurs e-mail.

L'e-mail à l'EPFL est maintenant largement centralisé: presque tous les membres de l'Ecole utilisent des adresses au format `xxx@epfl.ch` (voir <http://sic.epfl.ch/publications/FI00/fi-8-00/8-00-page11.html>) et plus de 90% des boîtes aux lettres derrière ces adresses résident sur **Mailbox** (autrefois connu sous le nom **Imap**), géré par le Service Informatique Central. Il s'agit là d'un développement relativement récent, sur les quatre dernières années environ, à partir d'une situation où l'e-mail était au contraire pris en charge par les département et les unités elles-mêmes. De cette histoire, il subsiste encore des serveurs e-mail en activité au quatre coins de l'Ecole, témoins parfois de l'esprit d'indépendance de telle unité ou peut-être de l'inertie de telle autre.

Quoi qu'il en soit, cette gestion éclatée de l'e-mail commence à poser quelques problèmes dans le contexte de plus en plus hostile de l'Internet d'aujourd'hui (avec ses virus et ses spammers), comme deux incidents récents permettront de l'illustrer. Dans un cas, un de ces serveurs *décentralisés* mal configuré en *relais ouvert* (voir <http://sic.epfl.ch/publications/FI99/fi-7-99/7-99-page1.html>) a accepté durant un week-end environ un million de spams de l'extérieur de l'EPFL et les a acheminé, à travers le serveur *outgoing mail.epfl.ch*, vers leurs cibles, également à l'extérieur de l'EPFL. Ceci a entraîné un ralentissement du courrier électronique en interne et des problèmes d'acheminement vers des sites externes qui avaient placé **mail.epfl.ch** dans leur liste noire. Certains virus, dont le récent Sobig.f, constituent un autre exemple: ils possèdent leur propre *moteur* d'acheminement des messages et peuvent se propager de l'EPFL vers l'extérieur (avec un impact négatif sur l'image de notre Ecole) parce que notre réseau est totalement ouvert dans ce sens, en partie pour laisser les serveurs décentralisés acheminer leur courrier externe indépendamment du serveur **mail.epfl.ch**.

Pour corriger ces problèmes, nous proposons de passer progressivement à une configuration où tous les messages,

aussi bien en entrée qu'en sortie, passent par un canal unique, où ils peuvent être soumis à un filtrage adéquat (*relaying* et virus). La conception générale est résumée dans la figure. Les serveurs notés **vérification d'adresse** sont le point d'entrée de tout message traité par le système, leur fonction étant de s'assurer, lors de connexions de serveurs externes, que les



adresses de destinataires existent vraiment à l'EPFL et, si ce n'est pas le cas, de l'annoncer tout de suite dans le dialogue SMTP (Simple Mail Transfer Protocol), sans quoi les spammers pourraient y faire disparaître comme dans un trou noir les messages d'erreur lorsqu'ils envoient leur camelote à des adresses inexistantes (voir <http://sic.epfl.ch/publications/FI99/fi-10-99/10-99-page11.html> et <http://www.ethlife.ethz.ch/articles/SpamETG.html> pour de tels incidents à l'EPFL et à l'EPFZ). A l'étape suivante, des filtres traitent les messages infectés par des virus connus ou comportant des annexes exécutables, potentiellement dangereuses. Enfin, les serveurs notés **Acheminement de message** envoient, le cas échéant après traduction d'adresse logique en adresse physique, les messages vers leur destination finale, soit vers des serveurs externes, soit vers les boîtes aux lettres des membres de

## CHANTIER DE SÉCURISATION DE L'E-MAIL À L'EPFL

l'EPFL. Les lignes noires séparant le réseau de l'EPFL du reste de l'Internet dénotent que toute connexion mail hors de ce système est bloquée au niveau du routeur d'entrée à notre réseau. On note également que pour réduire dans ce *montage en série* les risques de panne générale à cause de la panne d'un élément (un *single point of failure* en jargon anglo-informatique), chaque étage est constitué de deux serveurs indépendants, chacun d'entre eux pouvant communiquer avec n'importe lequel des deux serveurs de l'étage suivant, ce qui est symbolisé par les flèches croisées de la figure. C'est en faisant pointer le nom **mail.epfl.ch** vers les adresses IP des serveurs **vérification d'adresse** que ce projet de sécurisation sera transparent pour les utilisateurs, puisque c'est le nom

déjà mentionné comme serveur SMTP *outgoing* du logiciel de mail de la vaste majorité d'entre eux.

La mise en œuvre de ce système va se faire en deux étapes. Dans un premier temps, le point d'entrée unique pour tous les messages provenant de l'extérieur de l'EPFL va être mis en place. Pour cela il est nécessaire de connaître toutes les adresses qui doivent être considérées comme valables à l'EPFL: c'est l'objet de l'article **Recensement des adresses ne se terminant pas par @epfl.ch** suivant. Dans un deuxième temps, le passage par ce système de tous les messages envoyés par les membres de l'EPFL nécessitera une reconfiguration des serveurs e-mail décentralisés. Un second article apparaîtra ultérieurement à ce sujet, donnant les indications nécessaires à cet effet. ■