RFC 5101 : Specification of the IPFIX Protocol for the Exchange of IP Traffic Flow Information

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 février 2008

Date de publication du RFC : Janvier 2008

https://www.bortzmeyer.org/5101.html

Le système IPFIX, successeur de Netflow est désormais normalisé. Des routeurs de différentes marques peuvent donc désormais envoyer des informations statistiques à des machines d'administration de différentes origines.

Un cahier des charges pour IPFIX avait été spécifié dans le RFC 3917[1]. Le système lui-même est désormais normalisé, ce RFC prenant en charge le protocole d'autres RFC s'occupant du modèle d'informations ou bien de l'architecture des différents composants d'IPFIX. Une nouvelle série de RFC IPFIX est sortie en septembre 2013 donc ce RFC n'a plus qu'un intérêt historique, il faut désormais consulter le RFC 7011.

Notre RFC normalise donc le format des paquets (section 3). Comme avec d'autres protocoles, les paquets commencent par un numéro de version, 10 ici, IPFIX marquant sa descendance depuis Netflow, dont la dernière version était la 9. Le RFC décrit aussi l'encodage des données exportées par l'observateur IPFIX (section 6).

Enfin, notre RFC décrit le mécanisme de transport, au dessus d'UDP, le protocole traditionnel de Netflow, mais aussi de TCP ou bien du protocole recommandé, SCTP. Pour répondre au cahier des charges, qui insistait sur la sécurité, la section 10.4 décrit aussi l'utilisation de TLS.

IPFIX est déjà mis en œuvre dans plusieurs systèmes et l'annonce de l'IESG approuvant le RFC précise que deux tests d'interopérabilité ont eu lieu, avec cinq logiciels différents, et que tout marchait bien. Un exemple de mise en œuvre en logiciel libre est Maji <http://research.wand.net.nz/software/maji.php>. Toutefois, mi-2012, des années après la sortie du RFC, il semble que peu de routeurs soient capables de faire de l'IPFIX (v10). La plupart sont restés bloqués sur Netflow (v9).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3917.txt