RFC 5470 : Architecture for IP Flow Information Export

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 avril 2009

Date de publication du RFC : Mars 2009

https://www.bortzmeyer.org/5470.html

Voici donc les RFC décrivant le protocole IPFIX, le successeur normalisé de Netflow. Ce RFC particulier décrit l'architecture d'IPFIX.

Ces RFC sont bâtis sur le travail du groupe "ipfix" de l'IETF qui avait formalisé son cahier des charges dans le RFC 3917[1]. Il s'agissait de remplacer le protocole privé Netflow par un mécanisme ouvert et normalisé.

La section 2 du RFC décrit la terminologie utilisée. L'un des principaux termes est évidemment celui de **flot** ("*flow*") et on notera la définition très large choisie : en gros, un flot est n'importe quel ensemble de paquets pour lequel il existe un critère automatique permettant de tester leur appartenance au flot. Cela peut donc être l'adresse source, l'adresse destination, ou même des données qui n'apparaissent pas dans le paquet (comme l'adresse du routeur suivant).

Les autres concepts importants sont ceux d'**exporteur** ("*exporter*", nommé "*probe*" dans Netflow) et de **récolteur** ("*collector*"). Le premier (en général un routeur mais ce n'est pas obligé, le logiciel libre Ntop peut aussi servir d'exporteur) exporte des flots sous forme agrégée, le second les récolte et les traite.

On notera que le format des flots n'est pas complètement spécifié dans les RFC. En effet, chaque exporteur peut définir des **gabarits** ("*template*") décrivant les données transmises par le flot (section 5.6 du RFC).

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