RFC 8956 : Dissemination of Flow Specification Rules for IPv6

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 janvier 2021

Date de publication du RFC : Décembre 2020

https://www.bortzmeyer.org/8956.html

Il existe un mécanisme de diffusion des règles de filtrage IP, FlowSpec, normalisé dans le RFC 8955 [1]. Ce mécanisme permet d'utiliser BGP pour envoyer à tous les routeurs d'un AS les mêmes règles, ce qui est très pratique, par exemple pour bloquer une attaque sur tous les routeurs d'entrée du domaine. Le FlowSpec original ne gérait qu'IPv4, voici son adaptation à IPv6.

En fait, il n'y avait pas grand'chose à faire. Après tout, IPv6 n'est pas un nouveau protocole, juste une nouvelle version du même protocole IP. Des concepts cruciaux, comme la définition d'un préfixe en préfixe/longueur, ou comme la règle du préfixe le plus spécifique restent les mêmes. Ce RFC est donc assez simple. Il ne reprend pas l'essentiel du RFC 8955, il ajoute juste ce qui est spécifique à IPv6. (À l'IETF, il avait été proposé de fusionner les deux documents mais, finalement, il y a un RFC générique + IPv4, le RFC 8955, et un spécifique à IPv6, notre RFC 8956.)

Petit rappel sur FlowSpec : les règles de filtrage sont transportées en BGP, les deux routeurs doivent annoncer la capacité « multi-protocole » (les capacités sont définies dans le RFC 5492) définie dans le RFC 4760, la famille de l'adresse (AFI pour "*Address Family Identifier*") est 2 (qui indique IPv6 <https://www.iana.org/assignments/address-family-numbers/address-family-numbers.xml#address-family-numbers-2>) et le SAFI ("*Subsequent Address Family Identifier*") est le même qu'en IPv4, 133 <https://www.iana.org/assignments/safi-namespace/safi-namespace.xml#safi-namespace-

Le gros de notre RFC (section 3) est l'énumération des différents types d'identifiant <https://www.iana.org/assignments/flow-spec/flow-spec.xml#flow-spec-2> d'un trafic à filtrer. Ce sont les mêmes qu'en IPv4 mais avec quelques adaptations. Ainsi, le type 1, « préfixe de destination » permet par exemple de dire à ses routeurs « jette à la poubelle tout ce qui est destiné à

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc8955.txt

2001:db:96b:1::/64 ». Son encodage ressemble beaucoup à celui en IPv4 mais avec un truc en plus, le décalage ("*offset*") depuis le début de l'adresse. Avec un décalage de 0, on est dans le classique préfixe/longueur mais on peut aussi ignorer des bits au début de l'adresse avec un décalage non-nul.

Le type 3, « protocole de niveau supérieur » est l'un de ceux dont la définition IPv6 est la plus différente de celle d'IPv4. En effet, IPv6 a les en-têtes d'extension (RFC 8200, section 4), une spécificité de cette version. Le champ « "*Next header*" » d'IPv6 (RFC 8200, section 3) n'a pas la même sémantique que le champ « Protocole » d'IPv4 puisqu'il peut y avoir plusieurs en-têtes avant celui qui indique le protocole de couche 4 (qui sera typiquement TCP ou UDP). Le choix de FlowSpec est que le type 3 désigne le dernier champ « "*Next header*" », celui qui identifie le protocole de transport, ce qui est logique, c'est bien là-dessus qu'on veut filtrer, en général. Rappelez-vous au passage que d'analyser les en-têtes d'extension IPv6 pour arriver au protocole de transport n'est hélas pas trivial <https://www.bortzmeyer.org/analyse-pcap-ipv6.html>. Et il y a d'autres pièges, expliqués dans les RFC 7112 et RFC 8883.

Autre type d'identifiant qui est différent en IPv6, le type 7, ICMP. Si le protocole est très proche, les types et les codes ne sont en effet pas les mêmes. Ainsi, l'un des types les plus célèbres, "*Echo Request*", utilisé par ping, vaut 8 en IPv4 <https://www.iana.org/assignments/icmp-parameters/icmp-parameter
xml#icmp-parameters-codes-8> et 138 en IPv6 <https://www.iana.org/assignments/icmpv6-parame
icmpv6-parameters.xml#icmpv6-parameters-codes-6>.

Les autres types se comportent en IPv6 exactement comme en IPv4. Par exemple, si vous voulez dire à vos routeurs de filtrer sur le port, les types 4, 5 et 6, dédiés à cet usage, ont le même encodage et la même sémantique qu'en IPv4 (ce qui est logique, puisque le port est un concept de couche 4).

FlowSpec est aujourd'hui largement mis en œuvre dans les logiciels de routage, y compris en IPv6. Vous pouvez consulter à ce sujet le rapport de mise en œuvre <https://trac.ietf.org/trac/idr/wiki/draft-ietf-idr-flow-spec-v6%20implementations>. Si vous voulez jouer avec FlowSpec, le code Python d'exemple de l'annexe A est disponible en ligne <https://github.com/stoffi92/draft-ietf-idr-flow-spec-v6/tree/master/flowspec-cmp>.