RFC 9117 : Revised Validation Procedure for BGP Flow Specifications

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 28 septembre 2021

Date de publication du RFC : Août 2021

https://www.bortzmeyer.org/9117.html

Le RFC 8955[1] spécifie comment utiliser BGP pour diffuser des règles de filtrage (dites « FlowSpec ») aux routeurs. On voit facilement qu'une annonce de règles de filtrage maladroite ou malveillante pourrait faire bien des dégâts et c'est pour cela que le RFC 8955 insiste sur l'importance de **valider** ces annonces. Mais les règles de validation étaient trop strictes et ce nouveau RFC les adoucit légèrement.

Le changement ? Le RFC 8955 imposait que la machine qui annonce une règle de filtrage pour un préfixe de destination donné soit également le routeur suivant ("*next hop*") pour le préfixe en question. Cela limitait l'annonce aux routeurs situés sur le trajet des données. En iBGP (BGP interne à un AS, où les routeurs qui annoncent ne sont pas toujours ceux qui transmettent les paquets), cette règle était trop restrictive. (Pensez par exemple à un réflecteur de routes interne, par exemple géré par le SOC, réflecteur qui n'est même pas forcément un routeur.)

La règle nouvelle, plus libérale, ne concerne que du iBGP, interne à un AS ou à une confédération d'AS (RFC 5065). Entre des AS gérés par des organisations différentes (par exemple un AS terminal informant son opérateur Internet de ses désirs de filtrage), la règle de validation reste inchangée.

Plus formellement, la section 6 du RFC 8955, sur la validation des annonces de filtrage, est modifiée, l'étape « l'annonceur doit être également l'annonceur de la meilleure route » devient « l'annonceur doit être l'annonceur de la meilleure route **ou bien** le chemin d'AS doit être vide (ou n'inclure que des AS de la confédération, s'il y en a une) ». Le RFC précise également que cette validation relâchée doit pouvoir être désactivée par l'administrateur réseaux (s'ielle sait qu'il n'y aura pas d'annonces de filtrage par un

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

routeur qui n'est pas sur le chemin des paquets). Vous noterez plus bas que, pour l'instant, seul Huawei le permet.

Il y a également un léger changement des règles de validation du chemlin d'AS, pour les cas des serveurs de route (a priori, ils ne relaient pas ce genre d'annonces et peuvent donc les rejeter). Le RFC note que, même avec une validation stricte, certaines faiblesses de BGP permettent quand même dans certains cas à tort l'envoi de règles de filtrage. C'est un problème fondamental du RFC 8955, qui n'est donc pas nouveau.

Les nouvelles règles de ce RFC sont déjà largement mises en œuvre chez les routeurs <https://trac.ietf.org/trac/idr/wiki/draft-ietf-idr-bgp-flowspec-oid%20implementations>.