BCP 38, ne pas laisser des adresses IP usurpées sortir de son réseau

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 décembre 2016

http://www.bortzmeyer.org/bcp38.html

Qu'est-ce que ça peut bien être, « BCP 38 » ? Ce terme désigne un ensemble de documents de bonnes pratiques pour les acteurs de l'Internet, plus spécialement les opérateurs réseaux : **il ne faut pas laisser sortir de son réseau des paquets ayant une adresse source usurpée**. Le respect de ce principe permettrait de lutter contre certaines attaques par déni de service sur l'Internet. Ce principe est formalisé dans deux RFC, les RFC 2827[1] et RFC 3704.

« BCP » veut dire « "*Best Current Practice*" ». Le but de cet étiquetage est de pointer vers le ou les RFC qui décrivent la pratique en question. En effet, un RFC, une fois publié, n'est jamais modifié, alors que le monde, lui, change. C'est ainsi que le RFC 7525, parlant de TLS est décrit par l'étiquette BCP 195 <https://www.rfc-editor.org/info/bcp195> : les bonnes pratiques, en matière de cryptographie, changent vite. Une étiquette BCP peut pointer plusieurs RFC. Un bon exemple est le BCP 47 <https://www.rfc-editor.org/info/bcp47>, sur les étiquettes de langue, qui pointe vers les RFC 5646 et RFC 4647.

C'est également le cas de BCP 38 <https://www.rfc-editor.org/info/bcp38>, qui désigne le RFC 2827, avec les additions du RFC 3704.

Le problème que vise à résoudre ce BCP est celui de l'usurpation d'adresse IP <http://www.bortzmeyer.org/usurpation-adresse-ip.html> par un attaquant qui voudrait faire du déni de service sans révéler son adresse, ou bien en faisant une attaque par réflexion <http://www.bortzmeyer.org/attaques-reflexio.html>. Par défaut, dans l'Internet, il est trivial d'émettre des datagrammes avec une adresse source mensongère. BCP 38 dit que les opérateurs réseaux devraient interdire cette pratique, en configurant leurs routeurs à cette fin. Par exemple, si un FAI a deux préfixes IP, 192.0.2.0/24 et 2001:db8::/32, il n'y a aucune raison valable de laisser sortir du réseau du FAI des paquets ayant comme adresse IP source, mettons, 203.0.113.65.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2827.txt

Notons qu'un déploiement systématique de BCP 38 résoudrait un certain nombre de problèmes de sécurité sur l'Internet, mais pas tous. Ainsi, si l'attaquant dispose d'un botnet, et fait une attaque directe (pas par réflexion), il n'a pas vraiment besoin de mentir sur ses adresses IP source, ce ne sont pas les siennes, de toute façon (usurper l'adresse source aurait quand même quelques avantages, ça dépend des cas).

Aujourd'hui, le déploiement de BCP 38 dans l'Internet n'est pas inexistant mais il est très inégal. Par exemple, la situation est bien meilleure en Europe qu'en Asie. Un attaquant qui veut faire de l'usurpation d'adresses IP a donc encore pas mal de réseaux à sa disposition.

Pourquoi est-ce que tout le monde n'a pas déployé BCP 38, malgré le très large consensus qui existe parmi les professionnels ? La principale raison est économique. Un opérateur qui déploie BCP 38 (tous les routeurs permettent de le faire, soit en n'autorisant que ses propres préfixes, soit par des astuces comme RPF) aide les autres. Imaginez l'ingénieur allant voir le directeur financier et lui disant « on va dépenser de l'argent, et le ROI ira entièrement à nos concurrents »... Comme en écologie, c'est donc un cas typique où le sacro-saint marché ne peut pas aboutir à une bonne solution.

Notez que tester si un FAI donné met en œuvre ou pas BCP 38 est un peu plus compliqué que cela peut sembler au premier abord. Je connais par exemple une "*box*" très utilisée en France qui bloque les paquets IPv4 ayant une adresse IP source usurpée (par effet de bord du NAT) mais qui ne le fait que pour des flots existants ou pour des paquets de début d'un flot. Si on envoie un paquet TCP sans bit `SYN`, il passe malgré son adresse usurpée...

Quelques lectures pour approfondir :

— Un site d'informations <`http://www.bcp38.info/`> rassemblant des informations diverses sur cette bonne pratique de filtrage,
— Le projet Spoofer <`https://www.caida.org/projects/spoofer/`> de mesure du déploiement de BCP 38. Voyez par exemple les dernières mesures en France <`https://spoofer.caida.org/recent_tests.php?country_include=fra&no_block=1`>.