Sécurité des Points d'échanges : BGP et BCP

Arnaud Fenioux et Will van Gulik
afenioux@franceix.net
will.van.gulik@ip-max.net

FranceIX / IP-Max

Résumé Les opéateurs Internet utilisent le protocole BGP (Border Gateway Protocol) afin d'échanger leurs informations de routage. Bien qu'étant ancien et n'utilisant pas de mécanisme de sécurité fort, ce protocole a su évoluer et de nombreuses recommandations BCP (Best Current Practices) et RFC ont été rédigées. Cette soumission a pour but d'expliquer les risques les plus souvent rencontrés sur les points d'échanges (IXP), ainsi que de présenter les solutions existantes afin de s'en prémunir. Cette approche sera composée d'un volet théorique et pratique (sous forme de retours d'expériences) afin d'appréhender les problématiques de sécurité rencontrées par les opérateurs se raccordant à un IXP.

1 Introduction

Afin de comprendre les termes et concepts utilisés par la suite, il est conseillé de lire l'article *Influence des bonnes pratiques sur les incidents BGP* [1] présenté au SSTIC en 2012. Nous présenterons tout de meme brièvement le protocole BGP et les Points d'échanges dans cette introduction.

1.1 Le protocole BGP

Chaque opérateur désirant se connecter à Internet dispose d'un numéro d'AS (*Autonomous System Number*) unique, ainsi que de plages d'adresses IP attribuées par un RIR (*Regional Internet Registry*). Le RIPE est chargé de gérer l'attribution de ces ressources pour l'Europe.

Pour échanger ces informations de routage entre eux, les opérateurs utilisent le protocole BGP (*Border Gateway Protocol*), chaque annonce BGP sera donc définie par au moins : un préfixe (numéro de réseau), un AS-PATH (liste des AS traversés pour arriver jusqu'à la destination), un NEXT-HOP (adresse IP du routeur le plus proche pour acheminer le trafic vers la destination).

1.2 Peering et points d'échanges

On parlera de *Transit* lorsqu'un opérateur paye un intermédiaire pour acheminer le trafic jusqu'à la destination. Et à contratio, de *Peering* lorsque deux opérateurs sont directement interconnectés entre eux pour échanger leur trafic respectif. Le peering est généralement un accord gratuit, alors que le transit est payant.

Les opérateurs souhaitant échanger du trafic entre eux (peerer) doivent être directement interconnectés, soit par l'utilisation d'un cable réseau entre leurs routeurs, soit par l'intermédiaire d'un point d'échange (aussi appelé IXP).

Les interconnexions directes (PNI *Private Network Interconnections*) ne sont généralement utilisées que lorsqu'il y a besoin d'échanger beaucoup de trafic. En effet, au niveau opérationnel, cela nécessiste de dédier un port sur le routeur et de maintenir une liaison par voisin (peer).

S'interconnecter à un point d'échange permet de joindre de nombreux peers via une seule liaison, l'IXP se comporte comme un switch virtuel de niveau 2 (tous les peers sont dans le même LAN/réseau).

NOTE

- Ajouter un Schéma !
- Expliquer les différents types d'acteurs présents sur un IXP : ISP, CDN, sites de e-commerce, Grand comptes...

2 Risques et contre-mesures

2.1 Static Routing

Un problème à envisager lorsque l'on est connecté sur un IXP est l'utilisation possible par certains de routes statiques.

Une fois connecté à un point d'échange chaque opérateur peut choisir de peerer avec les autres membres. Cela peut etre avec la totalité des membres si l'opérateur a une politique de peering ouverte, ou seulement une partie des membres si l'opérateur a une politique de peering selective. Ce choix s'effectue au cas par cas et selon des critères propres à chaque opérateur (critères politiques, techniques ou économiques) comme expliqué dans le livre *The Internet Peering Playbook* [2].

Un peer s'étant vu refuser une demande de peering peut aisément définir une route statique vers le routeur de cet opérateur afin de forcer tout le trafic qui lui est destiné à aller directement chez lui. Cette technique peut être détectée par une analyse poussée des statistiques NetFlow (ou IPFIX). L'attanquant perd alors une partie de la résiliance, car si la victime met en place un filtrage (uRPF *Unicast Reverse Path Forwarding* strict ou feasible path, ou une ACL *Access Control List* interdisant le trafic provenant de l'adresse MAC du routeur de l'attanquant) le trafic sera alors détruit (blackholé).

Si le routeur de l'opérateur cible contient toute les routes de l'Internet (full-table) et n'est pas correctement sécurisé, il est même possible de faire pointer une route par défaut vers ce routeur afin d'utiliser ses transitaires et obtenir un accès complet et gratuit à Internet. Cette technique plus grossière que la précédente est d'autant plus visible et risquée, et peut être facilement déjouée par la victime via l'utilisation de VRF (*Virtual Routing and Forwarding*), d'une prefix-list qui n'accepte que le trafic à destination de son propre réseau ou en s'assurant que le routeur connecté au point d'échange ne possède qu'un nombre limité de routes dans sa table de routage.

Tous ces mécanismes de protection sont expliqués dans la *BCP84* [3].

NOTE

— Détailer l'utilisation des ACL de niveau 2 (filtrage MAC) / ACL de niveau 3 (filtrage IP) et de uRPF.

2.2 BGP Hijacking

Un des incidents le plus fréquemment vu sur Internet est le leak de routes et l'usurpation de préfixes (annonces non autorisées). Cela est généralement dû à une erreur de configuration et est corrigé dans les heures qui suivent, mais il arrive que cela soit fait dans un but précis : soit pour annoncer des plages IP non utilisées afin d'envoyer du spam, soit pour détourner du trafic afin de l'analyser ou d'en tirer un bénéfice pécunaire.

BGP ne possède pas de mécanisme permettant de vérifier la validité des AS traversés, mais on peut tout de même appliquer des filtrages sur les sessions BGP établies avec ses peers afin de limiter fortement ces risques de détournement.

— Une solutions communément utilisée est de filtrer les routes recues de la part d'un client. Il s'agit alors d'aller requèter une IRR DB (*Internet Routing Registry DataBase*) afin de savoir quels sont les réseaux liés à un AS. Les informations enregistrées dans la base du RIPE sont vérifiés avant enregistrement et peuvent donc être considérées comme fiables, ce qui n'est pas le cas pour tous les IRR. Des outils comme *peval* de *IRRToolSet*[4] ou *bgpq3*[5] peuvent etre utilisés pour créer ces filtres facilement.

— Une autre solution consiste à vérifier que l'AS d'origine est autorisé à être la source de ces annonces, ce qui peut etre mis en place a l'aide de RPKI (*Resource Public Key Infrastructure*) / ROA (*Route Origin Authorization*) [6]. Cette technique n'est encore que peu adoptée par la communauté des opérateurs car elle est encore récente.

Tous ces mécanismes de protection sont expliqués dans la BCP IETF *BGP operations and security* [7] ainsi que dans le guide des *Bonnes pratiques de configuration de BGP* [8].

NOTE

— Détailler les mécanismes de filtrages (Upstream / Downstream/ Peers)
— Donner des exemples de filtrage a partir de la base du RIPE, et parler des AS-SET dans le cas de Sessions de peering.
— Expliquer le risque d'une grosse désagrégation de la table de routage (ex : cas des 512k route sur cisco 6500/7600) `http://www.potaroo.net/presentations/2014-05-12-bgp2013.pdf`
— Donner des exemples comme le vol de bitcoin ou hijack de youtube, et expliquer les causes et solutions `http://www.reddit.com/r/Bitcoin/comments/27vb4r/the_ghashio_cycle/` `http://research.dyn.com/2008/02/pakistan-hijacks-youtube-1/`

2.3 Risques lié a un raccordement sur un IXP

NOTE Section a rédiger !

— Router Advertisment en IPv6 acticé par défaut = annonce d'une default route -> blackhole de trafic possible (d'ou l'utilité du VLAN de quarantaine et du filtrages de types de paquets sur les IXP)
— multicast a filtrer : possibilité de faire monter 100% le CPU des routeurs
— Rate Limit du broadcast / storm-control et filtrage des addresse MAC
— Forger IP source, envoyer bcp de paquest RST -> Drop des sessions BGP non authentifiées avec MD5
— Pas de filtrage des annonces BGP sur les Route-serveurs ?!
— réannonce d'un préfixe plus spécifique d'un IXP -> DROP des sessions -> exemple de l'AMS-IX !

3 Conclusion

Cet article a permis de dresser une liste non exaustive des risques rencontrés par un opérateur se raccordant à un point d'échange ainsi que de montrer les contre-mesures existantes. Nous avons pu constater que même si une bonne configuration BGP de ses équipements permet de se prémunir des attaques les plus communes, il est aussi important d'activer des mécanismes de filtrages et de protection non directement relatifs à BGP.

Bien que ces mécanimes soient définis publiquement, implémentés et documentés depuis de nombreuses années, il est a noter qu'encore trop peu d'administrateurs réseaux les mettent en place. Cela peut etre expliqué par le manque de temps, la non connnaissance de ces risques et moyen de s'en protéger, ou que ces risques sont trop souvents considérés comme mineurs.

Références

1. F. Contat, S. Nataf, and G. Valadon, "Influence des bonnes pratiques sur les incidents BGP." `https://www.sstic.org/media/SSTIC2012/SSTIC-actes/influence_des_bonnes_pratiques_sur_les_incidents_b/SSTIC2012-Article-influence_des_bonnes_pratiques_sur_les_incidents_bgp-contat_valadon_nataf_2.pdf`, 2012. SSTIC.
2. W. B. Norton, "The internet peering playbook." `http://drpeering.net/core/bookOutline.html`, 2012.
3. F. Baker and P. Savola, "Ingress filtering for multihomed networks." `https://tools.ietf.org/html/bcp84`, 2004. Best Current Practice, Internet Engineering Task Force.

4. "Irrtoolset." http://irrtoolset.isc.org/. The IRRToolSet is a set of tools to work with Internet routing policies.
5. A. Snarskii, "bqgp3." https://github.com/job/bgpq3. The bgpq3 utility is used to generate Cisco and Juniper prefix-lists.
6. S. Bortzmeyer, "La longue marche de la sécurité du routage internet : une étape importante, rpki+roa." http://www.bortzmeyer.org/securite-routage-bgp-rpki-roa.html, 2012.
7. J. Durand, I. Pepelnjak, and G. Doering, "BGP operations and security." https://tools.ietf.org/html/rfc7454, 2015. Best Current Practice, Internet Engineering Task Force.
8. ANSSI, "Bonnes pratiques de configuration de BGP." http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_configuration_BGP.pdf, 2013.