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. De nombreux articles ont été rédigés sur la sécurité de BGP, il s'agit ici de présenter aussi les risques et solutions concernant des problématiques de sécurité de niveau 2.

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 Internet et BGP

Chaque opérateur (aussi appelé ISP) 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) et un NEXT-HOP (adresse IP du routeur le plus proche pour acheminer le trafic vers la destination). Ces attributs sont définis en tant que *Well-Known, Mandatory*, c'est à dire que tous les routeurs doivent les comprendre, tel que décrit dans la *RFC4271* [2].

1.2 Types d'interconnexion

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 (on dit qu'ils *peerent*) 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 (aussi appelé *peer*).

1.3 Switching et IXP

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). Cela permet donc de mutualiser/réduire les couts.

Dans le cas le plus simple, le point d'échange peut n'être composé que d'un seul switch ; mais s'il y a plusieurs PoP (*Point of Presence*) il faut que tous les switchs soient reliés entre eux. La disponibilité étant critique sur ce type d'infrastructure, il est donc primodial d'avoir une plateforme stable et résiliante. Avoir plusieurs liens entre chaque site (PoP) et utiliser un protocol de detection de panne à convergence rapide sont des pré-requis.

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* [3].

NOTE
- Ajouter un Schéma !
- Expliquer les différents types d'acteurs présents sur un IXP : ISP, CDN, sites de e-commerce, Grand comptes...
- Parler des RS : mutualisation BGP
- Peering Local VS Remote peering / Interco IXP
- Ecosysteme : Euro-IX (nombre d'IXP / Traff)

2 Risques et contre-mesures du point de vue d'un ISP

2.1 Problématique de Static Routing + redirect

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

NOTE
- EXPLIQUER ROUTE STATIQUE
- EXPLIQUER ROUTE par défaut

Si le routeur de l'opérateur cible contient toute les routes de l'Internet (full-table) et n'est pas correctement sécurisé, il est 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 pour envoyer son trafic. Cette technique relativement grossière 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. Mais ces protections ne sont pas efficaces dans tous les cas.

En effet, 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 lui étant destiné à aller directement chez lui. Cette technique peut être détectée par une analyse des volumes de trafic par AS (et/ou par préfixe) source. Ces statistiques peuvent être collectées par NetFlow, Sflow ou IPFIX si le routeur supporte ces protocoles. 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).

Tous ces mécanismes de protection sont expliqués dans la *BCP84* [4].

NOTE
- Détailer l'utilisation des ACL de niveau 2 (filtrage MAC)
- ACL de niveau 3 (filtrage IP)
- uRPF (+ RFC)
- Schéma
- Ne pas accepter les ICMP(6) redirect ni le RA ! -> MITM (rédiger une sub-section pour ca)

2.2 Problématiques BGP

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.

NOTE
- Avec 1 seul Transit, et pas de peering, pas réellement besoin de filtrage, mais attention danger pour la suite (si + de tranit ou ajout peers).
- Max-prefix
- Filtrage AS_PATH (vide et seulement AS des CUST en OUT) / longeur en IN
- Prefix List IN : Bogon, Trop spécifiques, PFL par peer (liste des réseaux via contrat ou par mail ?)
- Filter ses interco ! si annonce plus spécifique -> Boum ! exemple AMS-IX lors de la renumérotation
- Prefix List OUT : comme pour transit, sinon Leak
- expliquer les impactes d'un leak : (Indosat / Level3) -> Free
- Donner des exemples comme le vol de bitcoin pour montrer la différence d'un hijack avec un leak `http://www.reddit.com/r/Bitcoin/comments/27vb4r/the_ghashio_cycle/` `http://research.dyn.com/2008/02/pakistan-hijacks-youtube-1/`

Tous ces mécanismes de protection sont expliqués dans la BCP 194 *BGP operations and security* [5] qui pointe de nombreux cas d'usage intéressants. Ainsi que dans le guide des *Bonnes pratiques de configuration de BGP* [6] qui contient de nombreux exemples de configuration pour différents constructeurs et logiciels. Nous vous encourageons d'ailleurs vivement à lire ces documents.

Il est important pour un ISP de se protéger correctement et d'appliquer des filtrages stricts lorsqu'il se raccorde à un point d'échange. Car lorsqu'il était raccordé à un transitaire, il pouvait se reposer sur la confiance qu'il avaient en son fournisseur, mais sur un IXP, c'est comme arriver dans le cours des grands, si vous ne faites pas attention, personne ne le fera pour vous.

3 Risques et contre-mesures du point de vue d'un IXP

3.1 Route Servers

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*[7] ou *bgpq3*[8] peuvent etre utilisés pour créer ces filtres facilement.

NOTE
- Définir IRR DB
- Insiter sur bgpq3 (rapidité, facilité des config)
- Pointer IRR Explorer et parler rapidement de la qualité des merges des IRR (RAdb)

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*) [9]. Cette technique n'est encore que peu adoptée par la communauté des opérateurs car elle est encore récente.

3.2 Protections sur ports d'acces à l'IXP

NOTE

— Filtrage addr MAC via L2 ACL pour éviter boucle et empécher MAC spoofing (MITM L2)
— 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)
— IP Spoofing D.A.I / IPv6 FHS (Filtrage ARP Reply : couple SHA/SPA différent de IP/MAC si attaque)
— multicast a filtrer : possibilité de faire monter 100% le CPU des routeurs (MLD Snooping, mais attention TCAM)
— Broadcast a filtrer : pas besoin, juste de l'ARP
— Unknown unicast a rate-limiter -> CPU ou petit port full sinon (expliquer le terme BUM)
— Rate Limit du ARP / storm-control -> sinon CPU a 100% | Parler ARP Sponge AMS-IX et E-VPN / proxy ARP | parler en nombre de la quantité de pkt/s visibles et "encaissables par un petit routeur"
— Forger IP source, envoyer bcp de paquest RST (RST Blind). Quazi impossible a cause du numéro de séquence TCP et du port SRC a trouver, mais MD5 pas cher a configuré (contrainte opérationelle légère néanmoins)

4 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 à 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. Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)." http://tools.ietf.org/html/rfc4271, 2006. Request for Comments, Internet Engineering Task Force.
3. W. B. Norton, "The internet peering playbook." http://drpeering.net/core/bookOutline.html, 2012.
4. F. Baker and P. Savola, "Ingress filtering for multihomed networks." https://tools.ietf.org/html/bcp84, 2004. Best Current Practice, Internet Engineering Task Force.
5. 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.
6. ANSSI, "Bonnes pratiques de configuration de BGP." http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_configuration_BGP.pdf, 2013.
7. "Irrtoolset." http://irrtoolset.isc.org/. The IRRToolSet is a set of tools to work with Internet routing policies.
8. A. Snarskii, "bqgp3." https://github.com/job/bgpq3. The bgpq3 utility is used to generate Cisco and Juniper prefix-lists.
9. 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.