Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 8207
BCP 211
Catégorie : Bonnes pratiques actuelles
ISSN : 2070-1721

R. Bush
Internet Initiative Japan

septembre 2017
Traduction Claude Brière de L'Isle

Considérations sur le fonctionnement de BGP

Résumé
Le déploiement de l'architecture et des protocoles de BGPsec soulève de nombreuses considérations de fontionnement. Le présent document tente de collecter et présenter les plus critiques et universelles. Les pratiques de fontionnement sont supposées évoluer lorsque BGPsec sera formalisé et déployé initialement.

Statut de ce mémoire
Le présent mémoire documente les bonnes pratiques actuelles de l'Internet.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Plus d'informations sur les normes de l'Internet sont disponibles à la Section 2 de la [RFC5741].

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc8207

Table des matières

1. Introduction

La validation d'origine fondée sur l'infrastructure de clé publique de ressource (RPKI, *Resource Public Key Infrastructure*) [RFC6811] est dans ses phases de début. Comme BGPsec [RFC8205] peut exiger de grosses mémoires et/ou des CPU plus modernes, il est prévu un déploiement par incréments sur une longue durée. BGPsec est un nouveau protocole avec de nombreuses considérations de fonctionnement que le présent document tente de décrire. Comme avec la plupart des pratiques de fonctionnement, celles-ci vont probablement changer au fil du temps.

BGPsec s'appuie sur une large propagation de la RPKI [RFC6480]. Comment la RPKI est distribuée et maintenue globalement au sein d'une infrastructure d'opérateur peut être différent pour BGPsec que pour la validation d'origine.

BGPsec doit être appliqué seulement par les routeurs frontières à capacité eBGP de système autonome (AS, *Autonomous System*). Il est conçu de façon à pouvoir être utilisé pour protéger les annonces qui sont générées par des routeurs de bordure à contraintes de ressources. Ceci pose des problèmes de fonctionnement particuliers, voir la Section 6.

Des préfixes différents peuvent avoir des problèmes différents de temps et de protection contre la répétition.

1.1 Langage des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119], [RFC8174] quand, et seulement quand ils apparaissent tout en majuscules, comme montré ci-dessus.

2. Lectures suggérées

On suppose que le lecteur a connaisance de BGP [RFC4271], BGPsec [RFC8205], de la RPKI [RFC6480], de la structure de répertoire RPKI [RFC6481], et des autorisations d'origine de chemin (ROA, *Route Origin Authorization*) [RFC6482].

3. Distribution et maintenance de RPKI

Les considérations pour les objets RPKI (certificats, listes de révocation de certificat (CRL, *Certificate Revocation List*), les manifestes [RFC6481], et les enregistrements Ghostbusters [RFC6493]), les localisateurs d'ancre de confiance (TAL, *Trust Anchor Locator*) [RFC7730], les comportements de synchronisation d'antémémoire, et la validation provenant de la section Distribution et maintenance de RPKI [RFC7115] s'appliquent. Les considérations spécifiques relatives aux objets ROA ne s'appliquent pas au présent document.

4. Certificats d'AS/routeur

Comme décrit dans la [RFC8635], les routeurs locuteurs BGPsec sont capables de générer leurs propres paires de clés publiques/privées et d'avoir leurs certificats signés et publiés dans la RPKI par le système d'autorité de certification (CA, *Certification Authority*) et/ou de recevoir leurs paires de clé publique/privée par l'opérateur.

Un site/opérateur peut utiliser un seul certificat/clé dans tous ses routeurs, un certificat/clé par routeur, ou toutes les situations intermédiaires.

Un grand opérateur, soucieux que la compromission de la clé d'un routeur rende les autres routeurs vulnérables, peut déployer un schéma de distribution de certificat/clé plus complexe pour réduire cette exposition.

À l'autre bout du spectre, un site frontière avec deux routeurs peut choisir d'utiliser un seul certificat/clé.

En prévision d'une éventuelle compromission de clé, un opérateur prudent DEVRAIT pré provisionner chaque "prochaine" clé de routeur dans la RPKI afin qu'il n'y ait pas de délai de propagation pour provisionner la nouvelle clé.

5. Au sein d'un réseau

BGPsec est parlé par les routeurs de bordure d'un réseau, spécifiquement ceux qui bordent d'autres réseaux/AS.

Dans un AS où les routeurs de bordure parlent BGPsec et donc, injectent des chemins BGPsec dans le BGP interne (iBGP, *BGP internal*), les réflecteurs de chemins (RR, *Route Reflector*) DOIVENT avoir BGPsec activé si et seulement si ils sont des locuteurs BGP externes (eBGP, *external BGP*) dans leur cône de client, c'est-à-dire, un client de RR ou la clôture transitive des consommateurs d'un client.

Un routeur à capacité BGPsec PEUT utiliser les données qu'il reçoit pour influencer la politique locale au sein de son réseau, voir la Section 7. Dans le déploiement, cette politique devrait tenir dans la politique, les préférences, etc, existantes de l'AS. Cela permet à un réseau de déployer par incréments les routeurs bordures à capacité BGPsec.

Les locuteurs eBGP qui sont en face d'homologues plus critiques ou amont ou aval seraient des candidats pour un déploiement précoce. Sécuriser ses propres annonces et valider les annonces reçues devrait être considéré dans un déploiement partiel.

Un opérateur devrait être conscient que BGPsec, comme tout autre changement de politique, peut causer des glissements de trafic dans son réseau. Et, comme avec une pratique normale de glissement de politique, un opérateur prudent a les outils et les méthodes pour prédire, mesurer, modifier, etc.

Par ailleurs, un opérateour qui veut surveiller la charge des routeurs, les glissements de trafic, etc., peut déployer par incréments tout en observant ces effets et ceux similaires.

BGPsec ne signe pas sur les communautés, de sorte qu'elles ne sont pas formellement de confiance. De plus, l'externalisation de la vérification n'est pas une pratique de sécurité prudente. Donc, un écoutant de eBGP NE DEVRAIT PAS accorder une confiance aveugle à une signalisation de sécurité non signée, comme des communautés, reçues sur une frontière de confiance.

6. Considérations sur les sites de bordure

Un site de bordure qui ne fournit pas le transit et ne fait pas confiance à son ou ses homologues en amont peut seulement générer une annonce de préfixe signée et ne peut pas valider les annonces reçues.

Un opérateur peut avoir besoin d'utiliser un matériel avec des ressources limitées. Dans ce cas, la négociation de capacités du protocole BGPsec permet à un routeur de bordure à ressources contraintes de ne garder que sa ou ses propres clés de signature et de signer ses annonces, mais pas de recevoir des annonces signées.

Donc, le routeur n'aura pas à traiter la majorité de la RPKI, économisant potentiellement le besoin d'un matériel supplémentaire.

Comme la vaste majorité des AS sont d'extrémité, et qu'ils annoncent la majorité des préfixes, cela permet un déploiement par incréments plus simple et moins coûteux. Cela peut aussi signifier que les sites de bordure concernés par la sécurité de l'acheminement seront entraînés par l'amont qui prend en charge BGPsec.

7. Politique d'acheminement

Comme les chemins signés BGPsec ne peuvent pas traverser une topologie non BGPsec, un déploiement partiel de BGPsec forme des îlots de chemins assurés. Lorsque ces îlots croissent jusqu'à se toucher les uns les autres, ils deviennent de plus grandes îles.

À la différence de la validation d'origine fondée sur la RPKI, BGPsec marque une annonce reçue comme valide ou non valide, il n'y a pas d'état explicite "NotFound" *(pas trouvé)*. En un certain sens, un chemin BGP4 non signé est l'équivalent de NotFound. La façon d'utiliser cela dans l'acheminement relève de la politique locale de l'opérateur, similaire à la validation d'origine comme dans la [RFC6811].

Comme BGPsec sera déroulé au fil des ans et ne permet pas de routeurs bordures intermédiaires non signants, la couverture sera non intégrale pendant longtemps. Ici se pose un dilemme ; un routeur devrait il évaluer un BGPsec_PATH entrant comme non valide en étant très strict et l'éliminer ? Par ailleurs, ce peut être le seul chemin pour ce préfixe, et une très faible préférence locale ferait qu'il ne serait utilisé et propagé que si il n'y a pas de solution de remplacement. Les deux termes sont raisonnables, mais on recommande de d'éliminer à cause du point suivant.

Les opérateurs devraient être conscients qu'accepter des annonces "non valides", sans considération des préférences locales, va souvent être équivalent à les traiter comme pleinement "valides". La préférence locale affecte seulement les chemins pour le même ensemble de destinations. Considérons qu'on a une annonce valide venant du voisin V pour le préfixe 10.0.0.0/16 et une annonce non valide pour 10.0.666.0/24 venant du voisin I. Si la politique locale sur le routeur n'est pas configurée à éliminer l'annonce non valide venant de I, alors la transmission à la plus longue correspondance va envoyer les paquets au voisin I sans considération de la valeur de la préférence locale.

La validation des chemins signés est généralement déployée à la bordure eBGP.

La politique locale à la bordure eBGP PEUT porter l'état de validation d'un chemin signé par BGP à travers les mécanismes normaux de politique locale, par exemple, d'établir une communauté BGP pour usage interne, ou de modifier une valeur de métrique telle qu'une préférence locale ou un discriminant multi sorties (MED, *Multi-Exit Discriminator*). Certains peuvent choisir d'utiliser le gros marteau de la préférence locale. D'autres peuvent choisir de laisser la règle du chemin d'AS et régler leur métrique interne, qui vient après le chemin d'AS dans le processus de décision de BGP.

Comme le caractère légèrement aléatoire de la propagation de RPKI peut causer un biais de version à travers les routeurs, un chemin d'AS qui ne se valide pas au routeur R0 pourrait se valider à R1. Donc, les chemins signés qui sont "non valides" et sont quand même propagés (parce qu'ils sont choisis comme meilleur chemin) NE DOIVENT PAS avoir leur signature supprimée et DOIVENT être signés si ils sont envoyés à des locuteurs BGPsec externes.

Cela implique que les mises à jour qu'un locuteur juge être "non valides" PEUVENT être propagées aux homologues iBGP. Donc, sauf si la politique locale assure le contraire, un chemin signé appris via iBGP peut être "non valide". Si nécessaire, l'état de validation devrait être signalé par les mécanismes normaux de politique locale comme les communautés ou les métriques.

Par ailleurs, la politique locale sur la bordure eBGP peut empêcher l'annonce iBGP ou eBGP de chemins d'AS signés qui sont "non valides".

Un locuteur BGPsec qui reçoit un chemin DEVRAIT effectuer la validation de l'origine conformément aux [RFC6811] et [RFC7115].

Un serveur de chemin est généralement "transparent', c'est-à-dire, il n'insère pas un AS dans le chemin de façon à ne pas augmenter le compte de bonds d'AS, et affecter par là les choix de chemin en aval. Mais, avec BGPsec, un routeur client R doit être capable de valider les chemins qui sont transmis signés à R. Mais le routeur envoyeur ne peut pas générer de signatures à tous les clients possibles. Donc, un serveur de chemin à capacité BGPsec a besoin de valider le BGPsec_PATH entrant et de transmettre les mises à jour qui peuvent être validées par les clients qui doivent donc connaître l'AS du serveur de chemins. Cela implique que le serveur de chemins crée des signatures par client incluant son propre AS dans le BGPsec_PATH, et transmette la signature à chaque AS client, voir la [RFC8205]. Le serveur de chemin utilise un pCount de 0 pour ne pas augmenter le compte de bonds d'AS effectif, conservant par là l'intention de "transparence".

Si on sait qu'un voisin BGPsec est un serveur de chemin transparent, ou qu'il peut par ailleurs utiliser un pCount de 0 (par exemple, voir la [RFC8206]), le routeur DEVRAIT être configuré à accepter et traiter un pCount de 0 reçu. Les routeurs DOIVENT interdire par défaut un pCount de 0.

Pour prévenir l'exposition de l'intérieur des confédérations BGP [RFC5065], un locuteur BGPsec qui exporte à un non membre supprime tous les segments Secure_Path intra confédération. Donc, signer au sein de la confédération ne va pas causer de confusion externe même si des AS privés non uniques sont utilisés.

8. Notes

Pour la protection contre les attaques qui répètent des données BGP de l'ordre d'un jour ou plus vieilles, changer les clés des routeurs avec les nouvelles clés (précédemment) provisionnées dans la RPKI est suffisant. Sur cette approche, voir la [RFC8634].

Un routeur qui a négocié une fois (et/ou envoyé) BGPsec ne devrait pas être supposé le faire toujours.

Comme le DNS, la RPKI globale présente seulement une vue vaguement cohérente, dépendant de l'heure, des mises à jour, de l'étendue, etc. Donc, une antémémoire ou un routeur peut avoir des données différentes sur un préfixe ou routeur particulier qu'une autre antémémoire ou routeur. Il n'y a pas de remède à cela ; c'est la nature des données distribuées avec les antémémoires distribuées.

Les opérateurs qui gèrent les certificats DEVRAIENT avoir des enregistrements RPKI Ghostbuster (voir la [RFC6493]) signés indirectement par des certificats d'entité d'extrémité, pour les certificats dont dépend l'acheminement des autres pour la validation de certificat et/ou de ROA.

Les opérateurs devraient être conscients de l'imminence des transitions d'algorithme, qui seront rares et de rythme lent, voir la [RFC6916]. Ils devraient travailler avec leurs fournisseurs pour s'assurer de la prise en charge des nouveaux algorithmes.

Lorsque un routeur doit évaluer les certificats et les ROA qui dépendent du temps écoulé, les horloges des routeurs DOIVENT être correctes avec une tolérance d'approximativement une heure. L'approche courante est que les opérateurs déploient des serveurs qui fournissent le service de l'heure, comme celui de la [RFC5905], aux routeurs clients.

Si un routeur a des raisons de croire que son horloge est sérieusement incorrecte, par exemple, il a une date antérieure à 2011, il NE DEVRAIT PAS tenter de valider les mises à jour entrantes. Il DEVRAIT différer la validation jusqu'à ce qu'il estime être dans une tolérance de temps raisonnable.

9. Considérations sur la sécurité

Le présent document décrit les considérations de fonctionnement pour le déploiement de BGPsec. Les considérations sur la sécurité pour BGPsec sont décrites dans la [RFC8205].

10. Considérations relatives à l'IANA

Le présent document n'exige aucune action de la part de l'IANA.

11. Références

11.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997, DOI 10.17487/RFC2119.

[RFC6493] R. Bush, "Enregistrement Ghostbusters de l'infrastructure de clé publique de ressource (RPKI)", février 2012. *(P.S.)*

[RFC6811] P. Mohapatra, et autres, "Validation d'origine de préfixe BGP", janvier 2013. *(P;S; ; MàJ par* RFC8481, 8893)

[RFC7115] R. Bush, "Opération de validation d'origine fondée sur l'infrastructure de clé publique de ressource (RPKI)", janvier 2014, (BCP0185).

[RFC7730] G. Huston, et autres, "Localisateur d'ancre de confiance (TAL) pour l'infrastructure de clé publique de ressource (RPKI)", janvier 2016. *(P.S. ; Remplace* RFC6490 *: Remplacée par* RFC8630*)*

[RFC8174] B. Leiba, "Ambiguïté des mots clés en majuscules ou minuscules dans la RFC2119", mai 2017. BCP14. *(MàJ* 2119)

[RFC8205] M. Lepinski, K. Sriram, "Spécification du protocole BGPsec", septembre 2017. *(P.S. ; MàJ par* RFC8206)

11.2 Références pour information

[RFC4271] Y. Rekhter, T. Li et S. Hares, "Protocole de routeur frontière version 4 (BGP-4)", janvier 2006. *(D.S.) (MàJ par* RFC6608, RFC8212)

[RFC5065] P. Traina et autres, "Confédérations de systèmes autonomes pour BGP", août 2007. DOI 10.17487/RFC5065, (*Remplace* RFC3065) *(D.S.)*

[RFC5905] D. Mills, J. Martin, J. Burbank, W. Kasch, "Protocole de l'heure du réseau version 4 (NTPv4) : Spécification du protocole et des algorithmes ", juin 2010. (*Remplace* RFC1305, RFC4330) *(P. S ; MàJ par* RFC7822, RFC8573)

[RFC6480] M. Lepinski, S. Kent, "Infrastructure pour la prise en charge de l'acheminement Internet sécurisé", février 2012. *(Info.)*

[RFC6481] G. Huston, R. Loomans, G. Michaelson, "Profil pour structure de répertoire de certificats de ressource", février 2012. DOI 10.17487/RFC6481, *(P.S.)*

[RFC6482] M. Lepinski, S. Kent, D. Kong, "Profil d'autorisations d'origine de chemin (ROA)", février 2012. DOI 10.17487/RFC6482, *(P.S.)*

[RFC6916] R. Gagliano, S. Kent, S. Turner, "Procédure d'agilité d'algorithme pour l'infrastructure de clé publique de ressource (RPKI)", BCP0182, avril 2013. DOI 10.17487/RFC6916,

[RFC8206] W. George, S. Murphy, "Migration des systèmes autonomes sur BGPsec", septembre 2017. DOI 10.17487/RFC8206, *(P.S. ; MàJ* RFC8205*)*

[RFC8634] B. Weis, R. Gagliano, K. Patel, "Changement de clés de certificat de routeur BGPsec", août 2019. DOI 10.17487/RFC8634, *(P.S.)*

[RFC8635] R. Bush, S. Turner, K. Patel, "Chiffrement de routeur pour BGPsec", août 2019. DOI 10.17487/RFC8635, *(P.S.)*

Remerciements

L'auteur souhaite remercier Thomas King, Arnold Nipper, Alvaro Retana, et l'équipe de conception de BGPsec.

Adresse de l'auteur

Randy Bush
Internet Initiative Japan
5147 Crystal Springs
Bainbridge Island, Washington 98110
United States of America
mél : randy@psg.com