Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 8206
RFC mise à jour : 8205
Catégorie : Sur la voie de la normalisation
ISSN: 2070-1721

W. George, Neustar
S. Murphy, PARSONS, Inc.

septembre 2017
Traduction Claude Brière de L'Isle

Considérations de BGPsec pour la migration des systèmes autonomes (AS)

Résumé
Le présent document discute les considérations et méthodes pour prendre en charge et sécuriser une méthode commune pour la migration des systèmes autonomes (AS, *Autonomous System*) au sein du protocole BGPsec.

Statut de ce mémoire
Ceci est un document de l'Internet en cours de normalisation.

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). Tous les documents approuvés par l'IESG ne sont pas candidats à devenir une norme de l'Internet ; voir 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/rfc8206

Notice de droits de reproduction
Copyright (c) 2017 IETF Trust et les personnes identifiées comme auteurs du document. Tous droits réservés.

Le présent document est soumis au BCP 78 et aux dispositions légales de l'IETF Trust qui se rapportent aux documents de l'IETF (http://trustee.ietf.org/license-info) en vigueur à la date de publication de ce document. Prière de revoir ces documents avec attention, car ils décrivent vos droits et obligations par rapport à ce document. Les composants de code extraits du présent document doivent inclure le texte de licence simplifié de BSD comme décrit au paragraphe 4.e des dispositions légales du Trust et sont fournis sans garantie comme décrit dans la licence de BSD simplifiée.

Table des matières

1. Introduction

Une méthode de gestion de la migration des numéros de système autonome BGP (ASN, *Autonomous System Number*) est décrite dans la [RFC7705]. Comme elle concerne le traitement des attributs AS_PATH, il est nécessaire de s'assurer que le traitement et les caractéristiques sont bien prise en charge dans BGPsec [RFC8205] parce que BGPsec est explicitement conçu pour protéger contre les changements dans le AS_PATH BGP, que ce soit par choix, par mauvaise configuration, ou par une intention malveillante. Il est critique que le cadre du protocole BGPsec soit capable de prendre en charge cet outil de fonctionnement nécessaire sans créer un risque inacceptable pour la sécurité ou une exploitation du processus.

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.

1.2 Note de documentation

Le présent document utilise les ASN de la gamme réservée pour la documentation comme décrit dans la [RFC5398]. Dans les exemples utilisés, ils sont destinés à représenter des ASN uniques au monde, pas des ASN réservés à usage privé comme documenté à la Section 10 de la [RFC1930].

2. Scénario général

Le présent document suppose que le lecteur a lu et compris la méthode de migration des ASN discutée dans la [RFC7705] incluant ses exemples (voir la Section 2 du document référencé) car il y sera largement fait référence ici. Le cas d'utilisation discuté dans la [RFC7705] est comme suit : pour une raison quelconque, un fournisseur est en train de fusionner deux AS ou plus, où l'un d'eux se substitue finalement à l'autre. Les confédérations d'AS BGP [RFC5065] ne sont pas activées entre les AS, mais un mécanisme est utilisé pour modifier le comportement BGP par défaut et permettre au routeur du fournisseur bordure (PE, *Provider Edg*e) migrant de se faire passer pour l'ancien ASN pour la session eBGP (BGP externe) de fournisseur bordure à consommateur bordure (PE-CE, *Provider-Edge-to-Customer-Edge*) ou de manipuler le AS_PATH, ou les deux. Alors que BGPsec [RFC8205] a bien une méthode pour traiter les mises en œuvre de confédération standard, elle n'est pas applicable dans ce cas précis. Cette migration exige une solution légèrement différente dans BGPsec que dans une confédération standard parce que à la différence d'une confédération, les homologues eBGP peuvent ne pas échanger du trafic avec l'ASN externe "correct", et les mises à jour signées vers l'avant sont pour un ASN public, plutôt que pour un ASN privé, de sorte qu'on ne peut s'attendre à ce que le locuteur BGP supprime les signatures affectées avant de propager le chemin à ses voisins eBGP.

Dans les exemples du paragraphe 5.4, AS64510 est englobé par AS64500, et les deux ASN représentent le réseau d'un fournisseur de service (SP, *Service Provider*) (voir les Figures 1 et 2 dans la [RFC7705]). AS64496 et 64499 représentent les réseaux de consommateur d'extrémité. Les références à PE, CE, et aux routeurs P réflètent les diagrammes et références de la RFC 7705.

3. Considérations sur RPKI

Les méthodes et la mise en œuvre discutées dans la [RFC7705] sont largement utilisées durant les intégrations de réseaux résultant de fusions et d'acquisitions, ainsi que de réseaux redessinés ; donc, il est nécessaire de prendre en charge cette capacité sur tous les routeurs/ASN à capacité BGPsec. Ce qui suit est une discussion des problèmes potentiels à considérer sur comment la migration d'ASN et la validation BGPsec [RFC8205] peuvent interagir.

Un des principaux problèmes de ce document sur la migration est que les fournisseurs de service (SP) s'arrêtent rarement après une fusion/acquisition/dépossession ; ils finissent par accumuler plusieurs ASN traditionnels au fil du temps. Comme les SP utilisent des méthodes de migration qui sont transparentes aux consommateurs et n'exigent donc pas de coordination avec eux, ils ont beaucoup moins de contrôle sur la longueur de la période de transition qu'ils en auraient avec quelque chose qui serait complètement soumis à leur contrôle administratif (par exemple, un roulement de clé). Parce qu'ils ne forcent pas à une migration simultanée (c'est-à-dire, où les deux extrémités passent au nouvel ASN à un moment choisi

d'un commun accord) il n'y a pas d'incitation pour un certain client de réaliser le mouvement du vieil ASN au nouveau. Cela laisse de nombreux SP avec plusieurs ASN traditionnels qui ne disparaissent pas très vite, sinon pas du tout. Comme des solutions ont été proposées pour les mises en œuvre d'infrastructure de clé publique de ressource (RPKI, *Resource Public Key Infrastructure*) pour résoudre ce cas de transition, le groupe de travail a examiné avec attention la complexité du fonctionnement et les problèmes d'adaptation de matériel associés au maintien de plusieurs clés d'ASN traditionnels sur les routeurs dans le réseau combiné. Alors que les SP qui choisissent de rester indéfiniment dans cette phase de transition courent des risques supplémentaires à cause de la complexité de fonctionnement et des considérations d'adaptation associées au maintien de multiples clés d'ASN traditionnels sur les routeurs à travers le réseau combiné, dire "ne faites pas cela" est une solution d'une utilité limitée. Par suite, cette solution tente de minimiser la complexité supplémentaire durant la période de transition, avec l'hypothèse qu'elle sera probablement prolongée. Noter que bien que le présent document traite principalement de considérations de fournisseur de service, il n'est pas seulement applicable aux SP, car les entreprises migrent souvent entre des ASN en utilisant la même fonctionnalité. Ce qui suit est une discussion des fonctions de validation de l'origine et du chemin et de la façon dont elles interagissent avec les migrations d'ASN.

3.1 Validation de l'origine

La validation de l'origine du chemin définie par la [RFC6480] n'exige pas de modification pour permettre la migration d'AS, car le protocole et la procédure existants permettent une solution. Dans le scénario discuté dans la [RFC7705], AS64510 est remplacé par AS64500. Si il y a des chemins existants générés par AS64510 sur le routeur qui est déplacé dans le nouvel ASN, de nouvelles autorisations de génération de chemin (ROA, *Route Origination Authorization*) pour les chemins avec le nouvel ASN devraient être générées, et elles devraient être traitées comme de nouvelles routes à ajouter à AS64500. Cependant, on doit aussi considérer la situation où un ou plusieurs autres PE sont encore dans AS64510 et génèrent une ou plusieurs routes qui peuvent être distinctes de toutes celles que le routeur qui migre génère. PE1 (qui fait maintenant partie de AS64500 et reçoit pour instruction d'utiliser "Remplacer le vieil AS" comme défini dans la [RFC7705] pour retirer AS64510 du chemin) doit être capable de traiter correctement les routes générées de AS64510. Si la route se révèle maintenant comme générée de AS64500, toutes les vérifications de validation des homologues en aval vont échouer sauf si une ROA est *aussi* disponible pour AS64500 comme ASN d'origine. En plus de générer une ROA pour 65400 pour tous les préfixes générés par le routeur qui est déplacé, il peut être nécessaire de générer des ROA pour 65400 pour les prefixes qui ont leur origine sur des routeurs qui sont encore en 65410, car la fonction de remplacement d'AS va changer l'AS d'origine dans certains cas. Cela signifie qu'il va y avoir plusieurs ROA montrant des AS différents autorisés à générer les mêmes préfixes jusqu'à ce que tous les routeurs qui génèrent des préfixes à partir de AS64510 aient migré sur AS64500. Plusieurs ROA de ce type sont permises selon le paragraphe 3.2 de la [RFC6480] de sorte que la gestion de la validation d'origine durant une migration comme celle-ci est simplement l'application du cas défini où un ensemble de préfixes sont générés à partir de plus d'un ASN. Donc, pour chaque ROA qui autorise le vieil ASN (par exemple, AS64510) à générer un préfixe, une nouvelle ROA DOIT aussi être créée qui autorise l'ASN remplaçant (par exemple, AS64500) à générer le même préfixe.

3.2 Validation de chemin

La validation de chemin BGPsec exige que chaque routeur dans le chemin d'AS signe cryptographiquement sa mise à jour pour affirmer que "chaque système autonome (AS) sur le chemin des AS dont la liste figure dans le message UPDATE a explicitement autorisé l'annonce de la route à l'AS suivant dans le chemin" (voir la Section 1 de la [RFC8205]). Comme la technique de migration de l'AS référencé modifie explicitement le AS_PATH entre deux homologues eBGP qui ne se coordonnent pas avec un autre (ne sont pas dans le même domaine administratif) aucun niveau de confiance ne peut être supposé ; donc, il peut être difficile d'identifier une manipulation légitime de l'AS_PATH pour des activités de migration d'une manipulation due à une mauvaise configuration ou à une intention malveillante.

3.2.1 Annonces sortantes (PE-->CE)

Quand PE1 est déplacé de AS64510 à AS64500, il va être provisionné avec les clés appropriees pour AS64500 pour lui permettre de transmettre-signer les routes utilisant AS64500. Cependant, il n'y a pas de lignes directrices dans la spécification du protocole BGPsec [RFC8205] sur si la valeur de l'ASN transmis-signé doit obligatoirement correspondre à l'AS configuré à distance pour se valider correctement. C'est-à-dire, si la session BGP de CE1 est configurée comme "AS 64510 distant", la présence de "AS 64510 local" sur PE1 va assurer qu'il n'y a pas de discordance d'ASN sur la session BGP elle-même, mais si CE1 reçoit des mises à jour transmises signées de son voisin distant (PE1) provenant de AS64500, on ne sait pas si le valideur BGPsec sur CE1 les considère encore comme valides par défaut. Le paragraphe 6.3 de la [RFC4271] mentionne cette correspondance entre l'ASN de l'homologue et les données de AS_PATH, mais elle est mentionnée comme validation facultative, plutôt que comme une exigence. On ne peut pas supposer que cette discordance va être permise par les mises en œuvre des fabricants, de sorte que l'utiliser comme moyen de résoudre ce cas de migration va probablement

être problématique.

3.2.2 Annonces entrantes (CE-->PE)

L'entrée est plus compliquée, parce que le CE ne sait pas que PE1 a changé d'ASN, de sorte qu'il transmet-signe toutes ses routes avec AS64510, et non AS64500. Le locuteur BGPsec ne peut pas manipuler les signatures précédentes et ne peut donc pas manipuler le chemin d'AS précédent sans causer une dicordance qui va invalider le chemin. Si les mises à jour sont simplement laissées intactes, le FAI aurait quand même besoin de publier et maintenir des clés publiques valides et actives pour AS 64510 si il doit apparaître dans la signature BGPsec_PATH afin que les receveurs puissent valider que la signature de BGPsec_PATH est arrivée intacte/entière. Cependant, si les mises à jour sont laissées intactes, cela va être cause que la longueur du chemin d'AS est augmentée, ce qui est inacceptable comme expliqué dans la [RFC7705].

4. Exigences

Pour être déployable, toute solution au problème décrit doit considérer les exigenes suivantes, données sans ordre particulier. BGPsec:

- DOIT prendre en charge la migration d'AS pour les annonces de chemin entrant et sortant (voir les paragraphes 3.2.1 et 3.2.2) sans réduire les protections de BGPsec pour le chemins.
- NE DOIT PAS exiger de reconfiguration sur le voisin eBGP distant (CE).
- NE DEVRAIT PAS exiger de changements globaux (c'est-à-dire, à l'échelle du réseau) de configuration pour prendre en charge la migration. Le but est de limiter les changements de configuration exigés pour les appareils (PE) qui migrent.
- NE DOIT PAS allonger le chemin de l'AS durant la migration.
- DOIT opérer au sein des limites de confiance existantes, par exemple, ne peut s'attendre à ce que le côté distant accepte un pCount=0 (voir le paragraphe 4.2 de la [RFC8205]) de la part d'un voisin qui n'est pas de confiance/non de confédération.

5. Solution

Comme noté au paragraphe 4.2 de la [RFC8205], BGPsec a déjà une solution pour cacher les ASN lorsque il n'est pas souhaitable d'augmenter la longueur du chemin d'AS. Donc une solution simple serait de conserver les clés pour AS64510 sur PE1 et de transmettre-signer vers CE1 avec AS64510 et pCount=0. Cependant, cela signifierait de passer un pCount=0 entre deux ASN qui sont dans des domaines administratifs et de confiance différents ce qui pourrait représenter un vecteur d'attaque significatif pour manipuler les chemins signés de BGPsec. Les attentes des instances légitimes de pCount=0 (pour rendre invisible un serveur de chemin qui ne fait pas partie du chemin de transit) sont qu'il y ait une sorte de relation de confiance existante entre les opérateurs du serveur de chemins et les homologues en aval afin que les homologues puissent être explicitement configurés par leur politique à n'accepter les annonces de pCount=0 que sur les sessions où ils sont attendus. Pour la même raison que des choses comme "AD local" [RFC7705] sont utilisées pour la migration d'ASN sans coordination avec l'utilisateur final, il n'est pas réaliste de supposer une telle sorte de coordination entre le SP et les administrateurs de CE1 pour s'assurer qu'ils vont selon leur politique accepter des signatures pCount=0 durant la période de transition ; donc, ce n'est pas une solution praticable.

Une meilleure solution se présente quand on considère comment traiter les routes qui vont du CE au PE, où les routes sont transmises-signées à AS64510, mais vont finalement devoir montrer AS64500 dans l'annonce de route sortante. Parce que AS64500 et AS64510 sont tous deux dans le même domaine administratif, une signature transmise-signée de AS64510 à AS64500 avec pCount=0 va être acceptable comme si elle était dans la limite de confiance appropriee de sorte que chaque locuteur BGP puisse être explicitlement configuré à accepter pCount=0 lorsque approprié entre les deux ASN. Au plus simple, ceci pourrait être utilisé à la frontière eBGP entre les deux ASN durant la migration. Comme la manipulation AS_PATH décrite ci-dessus arrive habituellement au routeur PE sur la base de la session et n'arrive pas simultanément à l'échelle du réseau, il n'est généralement pas approprié d'appliquer cette technique de dissimulation d'AS à travers toutes les routes échangées entre les deux ASN, car il peur en résulter des boucles d'acheminement et autres comportements indésirables. Donc, l'endroit le plus approprié pour mettre en œuvre cela est sur le PE local qui a encore des sessions eBGP avec les homologues qui s'attendent à échanger du trafic avec AS64510 (en utilisant les mécanismes de transition détaillés dans la [RFC7705]). Comme ce PE s'est déplacé à AS64500, il ne lui est pas possible de transmettre-signer AS64510 avec pCount=0 sans quelques changements mineurs au comportement de BGPsec pour traiter ce cas d'utilisation.

La migration d'AS utilise AS_PATH et la manipulation d'AS distant pour agir comme si un PE en cours de migration

existait simultanément dans les deux ASN même si il est seulement configuré avec un ASN global. Le présent document décrit l'application d'une technique similaire aux signatures BGPsec générées pour les mises à jour d'acheminement traitées au moyen de cette machinerie de migration. Chaque mise à jour d'acheminement qui est reçue de ou destinée à un voisin eBGP qui utilise encore le vieil ASN (64510) va être signée deux fois, une avec l'ASN à cacher, et une avec l'ASN qui va rester visible. On traite essentiellement la mise à jour comme si le PE avait un bond BGP interne et si la mise à jour était passée à travers une session eBGP entre AS64500 et AS64510, configurée à utiliser et accepter pCount=0, tout en éliminant les frais généraux de traitement et de mémorisation de la création d'une session eBGP réelle entre les deux ASN au sein du routeur PE. Il va en résulter un chemin d'AS correctement sécurisé dans les mises à jour de chemin affectées, parce que le routeur PE va être provisionné avec des clés valides pour les deux AS64500 et AS64510. Une distinction importante est ici que alors que la migration d'AS sous BGP4 standard manipule l'attribut AS_PATH, BGPsec utilise un attribut appelé "Secure_Path" (voir au paragraphe 3.1 de la [RFC8205]) et les voisins à capacité BGPsec n'échangent pas d'informations de AS_PATH dans leurs annonces de chemin. Cependant, un voisin BGPsec qui échange du trafic avec un voisin sans capacité BGPsec va utiliser les informations trouvées dans le Secure_Path pour reconstruire un AS_PATH standard pour les mises à jour envoyées à ce voisin. À la différence du Secure_Path où l'ASN à cacher est toujours présent mais ignoré quand on considère le chemin d'AS (à cause du pCount=0) quand on reconstruit un AS_PATH pour un voisin non BGPsec, les ASN avec pCount=0 ne vont pas apparaître du tout dans l'AS_PATH (voir le paragraphe 4.4 de la [RFC8205]). Le présent document ne change pas le comportement existant de reconstruction d'AS_PATH, il le souligne simplement pour l'éclairer.

La procédure pour prendre en charge la migration d'AS dans BGPsec est légèrement différente selon que le PE migrant reçoit les routes d'un de ses homologues eBGP ("entrant" comme au paragraphe 3.2.2) ou destinées aux homologues eBGP ("sortants" comme au paragraphe 3.2.1).

5.1 Sortant (PE-->CE)

Quand un routeur PE reçoit une mise à jour destinée à un voisin eBGP qui est localement configuré avec les mécanismes de migration d'AS discutés dans la [RFC7705], il DOIT générer une signature BGPsec valide, comme défini dans la [RFC8205] pour les deux ASN configurés. Il DOIT générer une signature depuis le nouvel ASN (global) de transmission-signature à l'ancien ASN (local) avec pCount=0, et ensuite il DOIT générer une signature de transmission depuis l'ancien ASN (local) à l'ASN eBGP cible avec un pCount=1 normal.

5.2 Entrant (CE-->PE)

Quand un routeur PE reçoit une mise à jour d'un voisin eBGP qui est localement configuré avec des mécanismes de migration d'AS (c'est-à-dire, la direction opposée du précédent flux de routes) il DOIT générer une signature de l'ancien (local) ASN de transmission-signature au nouvel ASN (global) avec pCount=0. Il n'est pas nécessaire de générer la seconde signature provenant du nouvel ASN (global) parce que le routeur frontière de système autonome (ASBR, *Autonomous System Border Router*) va générer cela quand il transmet-signe vers ses homologues eBGP comme défini dans le fonctionnement normal BGPsec. Noter qu'une signature n'est normalement pas ajoutée quand une mise à jour d'acheminement est envoyée à travers une session iBGP (BGP interne). L'exigence de signer les mises à jour dans iBGP représente un changement du comportement normal pour ce seul scénario spécifique de migration d'AS.

5.3 Autres considérations

Dans le cas entrant discuté au paragraphe 5.2, le PE ajoute les attributs BGPsec aux routes reçues de ou destinées à un voisin iBGP et qui utilisent pCount=0 pour les masquer. Bien que ceci ne soit pas interdit par BGPsec [RFC8205], les routeurs sans capacité BGPsec qui reçoivent des mises à jour de voisins iBGP à capacité BGPsec DOIVENT accepter les mises à jour avec de nouveaux attributs BGPsec (correctement formés) incluant la présence de pCount=0 sur une signature précédente, ou ils vont interférer avec cette méthode. De façon similaire, tous les réflecteurs de chemin à capacité BGPsec dans le chemin de ces mises à jour DOIVENT les refléter de façon transparente à leurs clients à capacité BGPsec.

Pour sécuriser cet ensemble de signatures, le routeur PE DOIT être provisionné avec des clés valides pour les deux ASN configurés (ancien et nouveau) et la clé pour l'ancien ASN DOIT être gardée valide jusqu'à ce que toutes les sessions eBGP aient migré sur le nouvel ASN. Les voisins en aval vont voir cela comme un chemin BGPsec valide, car ils vont simplement avoir confiance que leur voisin amont a accepté pCount=0 parce que il était explicitement configuré à le faire sur la base d'une relation de confiance et de relations d'affaire entre ce voisin amont et son voisin (les anciens et nouveaux ASN).

De plus, la Section 4 de la [RFC7705] discute les méthodes par lesquelles les migrations d'AS peuvent être réalisées pour

les homologues iBGP de façon telle qu'une session entre deux routeurs soit traitée comme iBGP même si l'ASN du voisin n'est pas le même ASN sur la configuration globale de chaque homologue. Pour autant que BGPsec est concerné, cela exige la même procédure que quand les routeurs qui migrent appliquent les mécanismes de migration d'AS aux homologues eBGP, mais le routeur qui fonctionne comme "ASBR" entre l'ancien et le nouvel ASN est différent. Dans eBGP, le routeur qui migre a des sessions eBGP directes à l'ancien ASN et signe de l'ancien ASN au nouveau avec pCount=0 avant de passer la mise à jour aux routeurs supplémentaires dans son ASN global (nouveau). Dans iBGP, le routeur qui migre reçoit des mises à jour (qui peuvent avoir pour origine des voisins eBGP ou d'autres voisins iBGP) de la part de ses voisins en aval dans le vieil ASN et DOIT signer ces mises à jour du vieil ASN au nouveau avec pCount=0 avant de les envoyer aux autres homologues.

5.4 Exemple

L'exemple suivant va illustrer la méthode utilisée ci-dessus. Comme avec les exemples précédents, PE1 est le routeur qui migre, AS64510 est le vieil ASN, qui va être absorbé par AS64500, l'ASN qui va être conservé en permanence. 64505 est un autre homologue externe, utilisé pour montrer ce à quoi vont ressembler les annonces à un homologue tiers qui n'a aucune part à la migration. Des notations supplémentaires sont utilisées pour préciser les détails de chaque signature :

Le segment de signature BGPsec d'origine prend la forme : sig(ASN cible, (pCount,...,ASN d'origine), NLRI) clé.

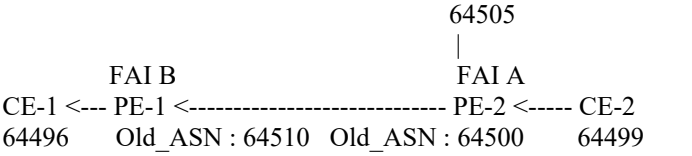
Les segments de signature BGPsec intermédiaires prennent la forme sig(ASN cible,..,(pCount,..,ASN du signataire),..,NLRI) clé.

(pCount,...,ASN) se réfère au nouveau segment Secure_Path ajouté à l'attribut BGPsec_PATH par l'ASN (ASN d'origine ou ASN du signataire).

"AS_PATH équivalent" se réfère à ce à quoi ressemblerait le AS_PATH si il était reconstruit pour être envoyé à un homologue non BGPsec, tandis que le Securedpath montre le chemin d'AS tel que représenté entre homologues BGPsec.

Note : la représentation de la generation du segment de signature est un peu simplifiée ici par souci de concision ; les détails réels du processus de signature sont décrits aux paragraphes 4.1 et 4.2 de la [RFC8205]. Par exemple, ce qui est couvert pas la signature inclut aussi les fanions, l'identifiant de suite d'algorithme, la longueur du NLRI, etc. Aussi, la clé n'est pas portée dans la mise à jour ; l'identifiant de clé sujette (SKI) est poté à la place.

Avant la fusion



CE-2 à PE-2 : sig(64500, (pCount=1,...,64499), N)K_64499-CE2
AS_PATH équivalent = (64499)
Securedpath = (64499)
longueur = sum(pCount)=1

PE-2 à 64505 : sig(64505,...,(pCount=1,...,64500),...,N)K_64500-PE2
sig(64500, (pCount=1,...,64499), N)K_64499-CE2
AS_PATH équivalent = (64500,64499)
Securedpath = (64500,64499)
longueur = sum(pCount)=2

PE-2 à PE-1 : sig(64510,...,(pCount=1,...,64500),...,N)K_64500-PE2
sig(64500, (pCount=1,...,64499), N)K_64499-CE2
AS_PATH équivalent = (64500,64499)
Securedpath = (64500,64499)
longueur = sum(pCount)=2

PE-1 à CE-1 : sig(64496,...,(pCount=1,...,64510),...,N)K_64510-PE1
sig(64510,...,(pCount=1,...,64500),...,N)K_64500-PE2

sig(64500, (pCount=1,...,64499), N)K_64499-CE2
AS_PATH équivalent = (64510,64500,64499)
Securedpath = (64510,64500,64499)
longueur = sum(pCount)=3

Migration, flux de routes sortant de PE-1 à CE-1

```
                                        64505
                                         |
          FAI A'                         FAI A'
CE-1 <--- PE-1 <------------------------- PE-2 <--- CE-2
64496   Old_ASN : 64510   Old_ASN :  64500    64499
          New_ASN : 64500  New_ASN : 64500
```

CE-2 à PE-2 : sig(64500, (pCount=1,...,64499), N)K_64499-CE2
AS_PATH équivalent = (64499)
Securedpath = (64499)
longueur = sum(pCount)=1

PE-2 à 64505 : sig(64505,...,(pCount=1,...,64500),...,N)K_64500-PE2
sig(64500, (pCount=1,...,64499), N)K_64499-CE2
AS_PATH équivalent = (64500,64499)
Securedpath = (64500,64499)
longueur = sum(pCount)=2

PE-2 à PE-1 : sig(64500, (pCount=1,...,64499), N)K_64499-CE2
AS_PATH équivalent = (64499)
Securedpath=(64499)
longueur = sum(pCount)=1
#PE-2 envoie à PE-1 (dans iBGP) exactement la même mise à jour que reçue de AS64499.

PE-1 à CE-1 : sig(64496,...,(pCount=1,...,64510),...,N)K_64510-PE1
sig(64510,...,(pCount=0,...,64500),...,N)K_64500-PE2 (*)
sig(64500, (pCount=1,...,64499), N)K_64499-CE2
AS_PATH équivalent = (64510,64499)
Securedpath = (64510, 64500 (pCount=0),64499)
longueur = sum(pCount)=2 (longueur n'est PAS 3)
#PE-1 ajoute le segment Secure_Path dans (*) agissant comme AS64500
#PE-1 accepte (*) avec pCount=0 agissant comme AS64510, comme si il avait reçu (*) d'un homologue eBGP.

Migration, flux de routes entrant de CE-1 à PE-1

```
                                        64505
                                         |
          FAI A'                         FAI A'
CE-1 ---> PE-1 -------------------------> PE-2 ---> CE-2
64496   Old_ASN : 64510   Old_ASN :  64500    64499
          New_ASN : 64500  New_ASN : 64500
```

CE-1 à PE-1 : sig(64510, (pCount=1,...,64496), N)K_64496-CE1
AS_PATH équivalent = (64496)
Securedpath = (64496)
longueur = sum(pCount)=1

PE-1 à PE-2 : sig(64500,...,(pCount=0,...,64510),...,N)K_64510-PE1 (**)
sig(64510, (pCount=1,...,64496), N)K_64496-CE1
AS_PATH équivalent = (64496)
Securedpath=(64510 (pCount=0),64496)
longueur = sum(pCount)=1 (longueur n'est PAS 2)
#PE-1 ajoute le segment Secure_Path dans (**) agissant comme AS64510
#PE-1 accepte (**) avec pCount=0 agissant comme AS64500,comme si il avait reçu (**) d'un homologue eBGP

#PE-1, comme AS64500, envoie la mise à jour incluant (**) à PE-2 (dans iBGP)

PE-2 à 64505 : sig(64505,...,(pCount=1,...,64500),...,N)K_64500-PE2
sig(64500,...,(pCount=0,...,64510),...,N)K_64510-PE1
sig(64510, (pCount=1,...,64496), N)K_64496-CE1
AS_PATH équivalent = (64500,64496)
Securedpath=(64500,64510 (pCount=0), 64496)
longueur = sum(pCount)=2 (longueur n'est PAS 3)

PE-2 à CE-2 : sig(64499,...,(pCount=1,...,64500),...,N)K_64500-PE2
sig(64500,...,(pCount=0,...,64510),...,N)K_64510-PE1
sig(64510, (pCount=1,...,64496), N)K_64496-CE1
AS_PATH équivalent = (64500,64496)
Securedpath = (64500, 64510 (pCount=0), 64496)
longueur = sum(pCount)=2 (longueur n'est PAS 3)

6. Considérations relatives à l'IANA

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

7. Considérations sur la sécurité

La [RFC7705] discute un processus par lequel un ASN migre dans un autre qui l'englobe. Parce que ce processus implique de manipuler le AS_Path dans un chemin BGP pour le faire dévier du chemin actuel qu'il a pris à travers le réseau, ce processus de migration tente de faire exactement ce que BGPsec essaye d'empêcher. BGPsec DOIT être capable de gérer cette utilisation légitime de la manipulation d'AS_Path sans générer une vulnérabilité dans l'infrastructure de sécurité de route RPKI, et le présent document a été rédigé pour définir la méthode par laquelle le protocole peut satisfaire ce besoin.

La solution discutée ci-dessus est considérée comme raisonnablement sûre contre l'exploitation par un acteur malveillant parce que elle exige que les deux signatures soient sécurisées comme si elles étaient trannsmises-signées entre deux voisins eBGP. Cela exige que tout routeur qui utilise cette solution soit provisionné avec des clés valides pour les deux ASN, le migrant et l'englobé, afin qu'il puisse générer des signatures valides pour chacun des deux ASN qu'il ajoute au chemin. Si les clés de l'AS sont compromises, ou si des clés de longueur zéro sont permises, cela ouvre la potentialité d'une attaque en raccourcissement de l'AS_PATH, mais ce risque existe déjà pour BGPsec.

8. Références

8.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", DOI 10.17487/RFC2119, BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC7705] W. George, S. Amante, "Mécanismes de migration de système autonome et leurs effets sur l'attribut AS_PATH de BGP", novembre 2015. DOI 10.17487/RFC7705, *(P.S. ; MàJ* RFC4271*)*

[RFC8174] B. Leiba, "Ambiguïté des mots clés en majuscules ou minucules dans la RFC2119", mai 2017. BCP14. DOI 10.17487/RFC8174, *(MàJ* 2119)

[RFC8205] M. Lepinski, K. Sriram, "Spécification du protocole BGPsec", septembre 2017. DOI 10.17487/RFC8205, *(P.S. ; MàJ par* RFC8206)

8.2 Références pour information

[RFC1930] J. Hawkinson, T. Bates, "Lignes directrices pour la création, sélection, et enregistrement d'un système autonome (AS)", mars 1996. (BCP0006). DOI 10.17487/RFC1930.

[RFC4271] Y. Rekhter, T. Li et S. Hares, "Protocole de routeur frontière version 4 (BGP-4)", janvier 2006. DOI 10.17487/RFC4271, *(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.)*

[RFC5398] G. Huston, "Réservation de numéro de système autonome (AS) à usage documentaire", décembre 2008. DOI 10.17487/RFC5398, *(Information)*

[RFC6480] M. Lepinski, S. Kent, "Infrastructure pour la prise en charge de l'acheminement Internet sécurisé", février 2012. DOI 10.17487/RFC6480, *(Info.)*

Remerciements

Merci à Kotikalapudi Sriram, Shane Amante, Warren Kumari, Terry Manderson, Keyur Patel, Alia Atlas, et Alvaro Retana pour leurs commentaires.

Les authors souhaite remercier particulièrement Kotikalapudi Sriram, Oliver Borchert, et Michael Baer de leur relecture et suggestions pour les exemples du paragraphe 5.4, qui fait une importante contribution à la qualité du texte.

De plus, la solution présentée dans ce document est an amalgame de plusieurs discussions de la réunion intermédiare sur l'acheminement interdomaines sécurisé (SIDR, *Secure Inter-Domain Routing*) plus une discussion à l'IETF 85, collectées et articulées grâce à Sandy Murphy.

Adresse des auteurs

Wesley George
Neustar
45980 Center Oak Plaza
Sterling, VA 20166
United States of America
mèl : wesgeorge@puck.nether.net

Sandy Murphy
PARSONS, Inc.
7110 Samuel Morse Drive
Columbia, MD 21046
United States of America
mèl : sandy@tislabs.com