QUELQUES PISTES SUR LE RENFORCEMENT DE LA SÉCURITÉ AUTOUR DU PROTOCOLE DE ROUTAGE BGP

Cédric Llorens, Denis Valois

mots-clés : ROUTAGE / CRYPTOGRAPHIE / SYSTÈME AUTONOME / ROA / AS

Le routage fait partie des éléments critiques de la disponibilité des réseaux. Le niveau de protection du routage a été souvent discuté et différentes pistes de renforcement de sa sécurité ont été étudiées. Nous décrirons succinctement le protocole BGP utilisé pour les échanges de routes sur Internet, puis nous détaillerons les mécanismes déjà mis en œuvre ainsi que les diverses approches sécuritaires étudiées.

1 Introduction

Le déploiement de réseaux IP de grande taille a rapidement nécessité la mise au point de protocoles de routage dynamique chargés de déterminer le plus efficacement possible la meilleure route pour atteindre une destination donnée. Par ailleurs, il a aussi été nécessaire de découper le réseau en différents systèmes autonomes (ou Autonomous System (AS)) afin de réduire cette complexité en taille.

Ces considérations ont donné lieu à une classification des protocoles de routage dynamique en deux grandes familles. Les protocoles de routage dynamique IGP (Interior Gateway Protocol) qui permettent d'échanger des informations d'accessibilité et de routage au sein d'un système autonome. Les protocoles de routage dynamique EGP (Exterior Gateway Protocol) qui permettent d'échanger des informations d'accessibilité et de routage entre systèmes autonomes.

Le protocole BGP établit une connexion TCP (port 179) entre deux routeurs et échange d'une manière dynamique et incrémentale les annonces de routes **[RFC4271]**.

Les calculs de routage effectués par BGP utilisent l'algorithme de Bellman-Ford étendu par l'annonce du chemin d'AS complet. BGP n'a pas de vision globale de la topologie de routage et envoie donc uniquement à ses voisins les annonces de routes. Pour notamment

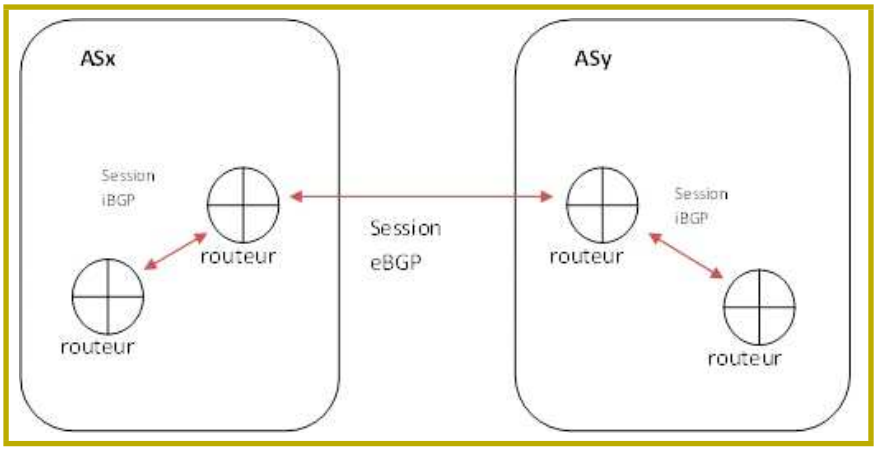

Figure 1 : Architecture BGP

éviter tout bouclage de routes, le protocole BGP gère un attribut contenant l'ensemble des AS traversés.

Les sessions BGP établies entre des routeurs appartenant à des AS distincts sont qualifiées de type eBGP (external BGP), alors que les connexions établies entre des routeurs BGP appartenant au même AS sont qualifiées de type iBGP (internal BGP) comme l'illustre la figure 1.

Sachant que toute attaque ou perturbation du routage peut impacter directement la disponibilité du réseau et de ses services, il est primordial de considérer les protocoles de routage comme des éléments-clés de la sécurité d'un réseau. Il doit être noté qu'il est possible de détourner du trafic par le routage à des fins de vol d'information.

2 Rappels sur quelques mécanismes actuels de sécurité

2.1 Le contrôle des topologies de routage

Les routes apprises par les sessions eBGP d'un système autonome doivent être propagées au sein du système autonome par le biais de sessions iBGP. Il s'agit effectivement de maintenir une vue cohérente de l'ensemble des routes externes au sein du système autonome pour l'ensemble des routeurs. Quels que soient les modèles de topologie iBGP considérés (modèle complet : chaque routeur communique avec tous les autres routeurs, ou réflecteur de routes : chaque routeur communique avec des réflecteurs de routes plutôt que de communiquer avec tous les autres **[WIKI RR]**), le contrôle des topologies de routage est primordial afin d'assurer la disponibilité du réseau et de ses services.

Ces contrôles de configuration sont possibles grâce à l'outil que nous avons développé HAWK qui permet une analyse des configurations des équipements réseaux **[HAWK]**.

2.2 Le contrôle par les secrets partagés

Le contrôle d'une session de routage BGP entre deux routeurs peut être réalisé par l'option d'empreinte MD5 véhiculée dans les paquets TCP. Il s'agit alors de vérifier en point à point les annonces de routes échangées entre deux routeurs à l'aide d'un secret partagé ou clé secrète **[RFC2385]**. Ce contrôle doit être mis en œuvre en priorité sur les sessions eBGP qui sont le plus à risque pour un AS. La configuration de ce contrôle s'écrit de la manière suivante en Cisco :

```
! association du routeur à l'AS
router bgp as

      ! partage du mot de passe avec le voisin de routage
      neighbor "destination_adresse" password "mot"
```

2.3 Le contrôle par les TTLs

Une autre méthode pour contrôler une session de routage BGP consiste à mettre en place un contrôle du TTL (Time To Live) contenu dans les paquets IP échangés par la session de routage BGP. Ce contrôle doit être mis en œuvre en priorité sur les sessions eBGP qui sont le plus à risque pour un AS. En effet, partant du principe que les sessions de routage BGP entre deux routeurs sont généralement directes, les paquets IP contenant des informations de routage BGP émis par un routeur doivent arriver à l'autre routeur avec un TTL = TTL -1. Comme une annonce de routes entre deux routeurs correspond à chaque fois à un nouveau paquet IP, le TTL du paquet IP émis sera par défaut égal à 255. Ainsi, si l'autre routeur reçoit des annonces de routes ayant un TTL qui n'est pas égal à 254, il peut en conclure que ce n'est pas le routeur avec lequel il a une session de routage qui a émis cette annonce. La configuration de ce contrôle s'écrit de la manière suivante en Cisco :

```
! association du routeur à l'AS
router bgp as

  ! attribution du nombre de saut ip avec le voisin de routage
      neighbor "destination_adresse " ttl-security hops "number"
```

GTSM (Generalized TTL Security Mechanism) permet de généraliser cette approche à plusieurs sauts possibles et autres protocoles **[RFC3682]**.

2.4 Le contrôle des annonces de routes eBGP

Les annonces de routes peuvent être soumises à une politique de filtrage définie par l'administrateur d'un système autonome. Cette politique peut à la fois s'appliquer aux annonces de routes reçues par un système autonome (routes transmises à l'intérieur d'un AS) ainsi qu'aux annonces de routes qu'émet le système autonome (routes émises à l'extérieur d'un AS). La configuration de ce contrôle s'écrit de la manière suivante en Cisco :

```
! association du routeur à l'AS
router bgp as

      ! application d'une liste de filtrage des annonces de routes
        entrants et sortantes
      neighbor "destination_adresse " prefix-list "nom_liste" in
      neighbor "destination_adresse " prefix-list "nom_liste_2" out

      ! definition des listes de filtrage
      ip prefix-list " nom_liste " seq " nombre " permit/deny " adresse "
      etc.
      ip prefix-list " nom_liste_2 " seq " nombre " permit/deny " adresse "
      etc.
```

2.5 Le contrôle des attaques de type Déni de Service

Le protocole BGP ne constitue pas une contre-mesure aux attaques de type Déni de Service vers des destinations clientes, mais peut aider à anticiper et limiter leurs effets **[RFC3882]**. Dans le cas d'une attaque de type Déni de Service, ce ne sont généralement pas les équipements réseau contenus au sein d'un AS qui sont visés (bien qu'ils soient une cible de choix pour ce type d'attaque, ils se protègent eux-aussi par divers mécanismes), mais plutôt les équipements (serveurs Web, de mail, etc.) de ses clients. Une telle attaque peut alors générer un trafic important qui dans le meilleur des cas saturera seulement le lien d'accès du client, et dans le pire des cas saturera un ou des liens d'infrastructure de l'opérateur de télécommunications. Deux techniques permettent de mitiger de telles attaques :

- BGP et puits de routage (black hole) : Dans le cas d'un système autonome avec de multiples points d'accès vers d'autres ASs, l'attaque peut venir de différentes sources et il n'est pas envisageable d'intervenir sur tous les routeurs d'interconnexion. Il suffit donc d'annoncer dans BGP l'adresse IP destinataire de l'attaque, avec comme point de sortie un puits de routage au lieu de l'interface cliente. Ce puits de routage met alors à la poubelle systématiquement tout le trafic qu'il reçoit. Il est cependant possible de faire plus simple et d'éviter de transporter ce flux inutile. Dans BGP, on va annoncer que le chemin pour atteindre l'adresse IP visée par l'attaque est une interface poubelle du routeur lui-même (null0 pour Cisco par exemple). Une fois que BGP aura propagé cette information, dès qu'un routeur recevra un paquet à destination de l'adresse attaquée, il le détruira. Cette option est brutale car tout le trafic est détruit, et donc ne protège pas réellement le service du client contre l'attaque DOS.
- BGP et puits de filtrage (sink hole) : Les routeurs IP n'ont pas la capacité à analyser le trafic pour séparer le trafic légitime de celui de l'attaque car cela nécessite d'inspecter le contenu du paquet IP alors que le rôle du routeur s'arrête à la couche IP. L'idée est donc de rediriger le trafic vers un équipement réseau dédié, qui lui aura cette capacité. Dans ce cas, BGP spécifie comme point de sortie l'adresse du « puits de filtrage ». Ainsi, tous les paquets à destination de l'adresse IP attaquée vont passer par cet équipement filtrant. Le système « puits de filtrage » permettra alors de déterminer exactement l'attaque à l'aide d'outils embarqués (Snort, Radware Defense Pro, etc.). Une fois les données analysées, le trafic épuré de l'attaque sera alors envoyé vers l'adresse IP destinatrice. D'un point de vue du routage BGP, on a tout d'abord routé le trafic externe vers le puits au sein de l'AS. Puis le puits route le trafic « nettoyé » vers le client, en général à travers un tunnel afin de cacher ce trafic au réseau (sinon le réseau routerait ce trafic à destination du client de nouveau vers le puits).

2.6 Conclusion

La sécurité du routage existe donc belle et bien à travers de nombreux contrôles mis en œuvre, cependant elle ne s'est pas attaquée aux deux problèmes principaux/fondamentaux du routage qui sont :

- La validité de l'origine d'une route.
- La validité d'un chemin suivi par une annonce de route.

Pour assurer la sécurité de ces deux problèmes, il est nécessaire de passer à la vitesse supérieure en terme de techniques et d'administration comme le détaille les mécanismes tels que: SBGP, soBGP, ROA, etc.

3 Les mécanismes de sécurité étudiés/futurs

3.1 Introduction

De nombreuses initiatives ont vu le jour pour authentifier l'origine d'une route et le chemin pris par une annonce de route. Cependant, aucune de ces solutions n'a été déployée à grandes échelles pour diverses raisons détaillées ci-après.

3.2 sBGP (secure BGP)

La première initiative a été le protocole sBGP (secure-BGP) qui permet à la fois de valider l'origine et le chemin pris par une annonce de route **[SBGP]**.

La validation de l'origine d'une route repose sur de la cryptographie à clé asymétrique nécessitant la mise en œuvre d'un système à clé publique où chaque système autonome possède alors un certificat électronique. La structure de gestion de clés proposée permet de traiter les extensions pour les blocs d'adresses certifiant l'appartenance d'une adresse à un AS. Un certificat est donc délivré à chaque organisme propriétaire d'un bloc d'adresse IP par l'entité responsable de l'attribution des adresses IP. En partant du haut, on trouve l'IANA (Internet Assigned Numbers Autority) qui gère l'espace d'adressage d'Internet et l'assignation des blocs de numéros d'AS. Elle est l'autorité de certification (AC) racine. On trouve au second niveau les registres Internet régionaux (RIR, Regional Internet Registry), qui allouent les blocs d'adresses IP et des numéros d'AS dans leurs zones géographiques. Enfin, les registres Internet locaux (LIR, local Internet Registry) qui sont généralement des fournisseurs d'accès à Internet (FAI) formant un troisième niveau.

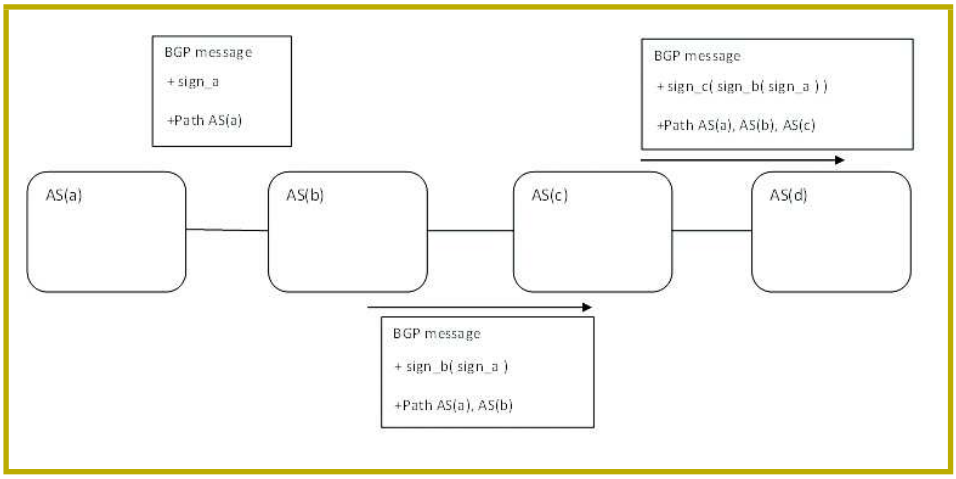

Figure 2 : sBGP et la validation de route

La validation du chemin pris par une annonce de route repose aussi sur de la cryptographie à clé asymétrique permettant de signer à chaque saut d'AS le chemin émis (avec sa clé privée) vers un autre système autonome comme l'illustre la figure 2 (les signatures s'empilent alors comme les couches d'un oignon).

Le protocole sBGP impose donc de modifier le protocole BGP pour intégrer ces notions d'authentification dans le format des messages. De plus, les équipements réseaux doivent embarquer au sein de leur système d'exploitation les librairies cryptographiques afin de mener les calculs nécessaires. Enfin, chaque session de routage entre deux équipements réseaux est réalisé via le protocole IPSEC pour renforcer la sécurité des échanges de routes entre deux ASs.

L'impact de ces calculs cryptographiques sur le processeur et la mémoire d'un équipement, couplé à l'impact sur le temps général de convergence des routes ont dissuadé les opérateurs à déployer le protocole sBGP.

3.3 soBGP (secure origin BGP)

Une autre initiative soBGP (Secure Origin BGP) de Cisco **[SO-BGP]** veut répondre aux mêmes besoins de sécurité que la solution sBGP mais par l'ajout d'une nouvelle primitive BGP (message de sécurité) et en ne dépendant pas d'une autorité centralisé (repose sur une notion de réseau de confiance appelé « web of trust ».).

Pour assurer l'authentification, chaque AS génère sa paire de clés et la fait signer par un autre membre de confiance (l'opération de signature de « confiance » est manuelle, non automatisé par le protocole). Ainsi le réseau de confiance se construit et permet la publication de certificats associant des AS à des adresses, mais aussi décrivant une politique pour un AS donné. Ces certificats sont déployés à l'aide d'un nouveau message BGP de sécurité (type 6).

La validation de l'origine d'une route nécessite de mettre en œuvre comme pour sBGP des primitives cryptographiques sur l'ensemble des équipements réseau participant au routage. La validation du chemin nécessite pour chaque équipement de construire en amont les topologies réseaux grâce aux certificats construits préalablement comme l'illustre la figure 3. Il est aussi possible de créer un serveur par AS dont les équipements lui envoient les messages BGP de sécurité (BGP Security) contenant les certificats et c'est ce serveur qui validera les auprès des équipements réseaux les messages BGP de mise à jour (BGP Update).

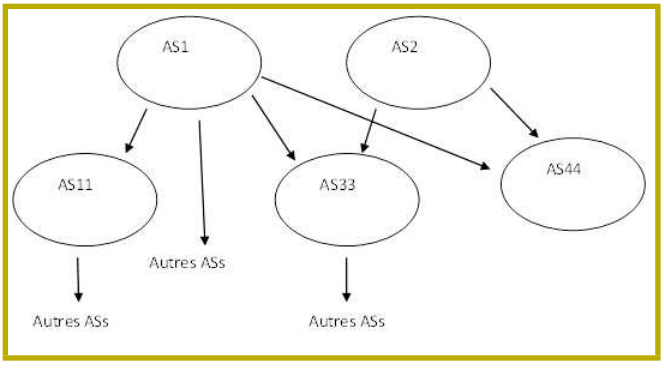

Figure 3 : Topologie des interconnexions des ASs

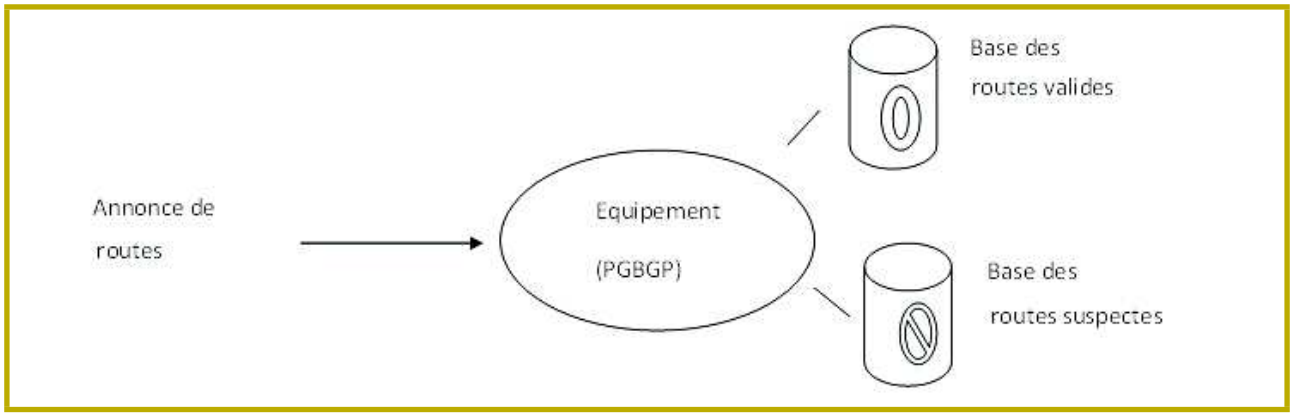

Figure 4 : Processus de PGBGP

Les impacts des primitives cryptographiques, la synchronisation parfaite nécessaire pour valider le chemin associé à une annonce de route grâce aux topologies réseaux (statique comparé à sBGP qui se base sur un calcul dynamique) ont aussi dissuadé les opérateurs à déployer le protocole soBGP.

3.4 Pretty Good BGP

Cette approche ne modifie ni le protocole BGP et ne repose pas sur des primitives cryptographiques, elle implémente seulement dans le système d'exploitation d'un équipement un algorithme assurant la fonction de validation de route (ou sur un serveur déporté de l'AS si on ne veut pas modifier les systèmes d'exploitation du réseau), mais aussi un mécanisme d'alerte informant les administrateurs d'une possible attaque détectée par ce nouvel algorithme **[PGBGP]**.

Pour initialiser notre algorithme, il est nécessaire que l'équipement réseau construise ses tables de routage avec ses différentes sessions BGP. Durant cette phase, aucune détection de route suspecte n'est possible. Une fois réalisé, on peut activer la fonction de détection de routes suspectes.

Cette nouvelle fonction agit lors de (comme illustré à la figure 4) :

- l'annonce d'une route pour un préfixe donné issu d'un AS différent de celui déjà présent dans les tables de routage du client. Un attaquant veut potentiellement voler cette route.
- l'annonce d'une route pour un sous-préfixe donné issu d'un AS différent de celui du préfixe agrégé déjà présent dans les tables de routage du client. Un attaquant veut potentiellement voler une partie d'un préfixe déjà annoncé, rappelons que BGP privilégie toujours le préfixe le plus faible lors de sa décision de routage.

Dans de tels cas, les routes ne sont pas prises en compte et mises dans en état nécessitant une « validation » par un opérateur. Cette période de « validation » dure un temps t et si elle est dépassée, alors la route est prise en compte et propagée.

Bien que a priori efficace pour maîtriser ce type de problème, elle nécessite une validation coûteuse en terme opérationnelle sachant que la plupart des routes suspectes ne le sont pas (l'attribution de préfixes originés par un AS bougent sans être pour autant des attaques). De plus, ce processus où « l'humain » intervient dégrade fortement la convergence des routes. Ces contraintes ont donc dissuadé les opérateurs à déployer PGBGP. En effet, les clients Entreprises (ou autres) à l'accès changent régulièrement d'opérateurs (changement de contrat, etc.) modifiant en conséquence les routes annoncées dans le processus et générant de nouveaux messages BGP.

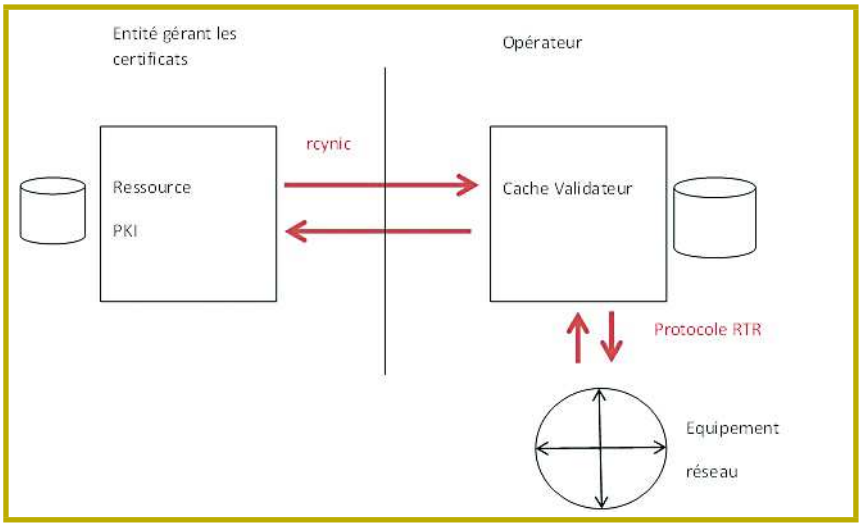

Figure 5 : ROAs et cache validateur

3.5 ROA (Route Origin Authorization)

Cette nouvelle initiative de l'IANA (groupe de travail sur la sécurité du routage inter-domaine (SIDR)) a pour objectif de limiter les impacts sur les équipements réseaux **[ROA_1]**. On ne veut aussi ni modifier le protocole BGP, ni impacter le routeur par des calculs cryptographiques. Enfin, on ne s'attaque qu'au problème de l'origine des routes.

Pour atteindre les objectifs fixés, il est nécessaire de faire tout le travail de validation en amont et d'appliquer aux équipements réseaux qu'une liste de filtrage limitant les impacts processeur et mémoire.

La solution repose sur :

- Une infrastructure de distribution de certificats numériques dont l'objectif est de prouver qu'un AS a le droit d'annoncer un préfixe. Elle s'appelle la RPKI (Resource Public Key Infrastructure) **[ROA_2]**.
- Le ROA (Route Origin Authorization) est un objet signé par une autorité indiquant que « le préfixe y peut être originé par un AS donné x ». Plus spécifiquement, il s'agit d'un fichier signé avec la clé du certificat de l'autorité donnant les AS qui peuvent être à l'origine d'un ou plusieurs préfixes.

L'autorité peut donc publier son certificat et ses ROAs dans des bases de données publiques (RIPE, etc.). A ce stade, il est donc possible de récupérer ces ROAs avec des outils de synchronisation tel que RPKI Validator du RIPE, rcynic de ISC/ARIN, etc. **[RPKI]**.

Ce sont les ROAs qui seront traduits en une liste de filtrage au niveau de l'équipement réseau. Cependant et comme l'injection de la liste de filtrage ROAs en mémoire sur un équipement semble dans bien des cas tout simplement impossible (tous les routeurs ne sont pas forcément puissants), une architecture via un cache-validateur semble donc être requise via le protocole RTR (RPKI/Router Protocol) comme l'illustre la figure 5.

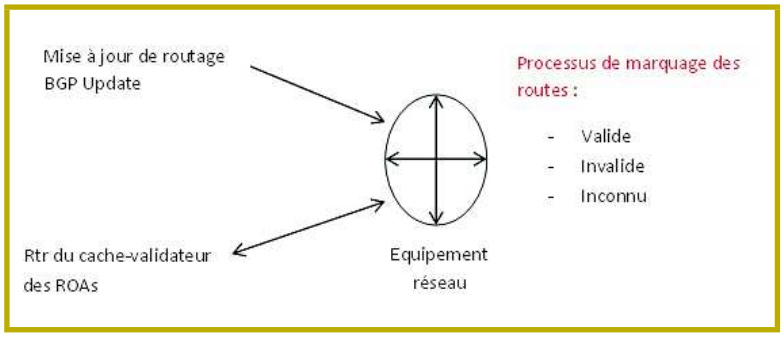

Figure 6 : Validation des routes par les ROAs

On a donc :

- Un cache/validateur, typiquement un serveur de type Unix que l'on appelle le serveur RTR.
- Le routeur, contenant une instance RTR que l'on appelle le client RTR.

La configuration pour récupérer les informations entre le routeur et le cache validateur s'exprime de la manière suivante en Juniper :

```
/* association du routeur à l'as */
routing-options {
    autonomous-system 64511;
    validation {

        /* description de la session avec le cache-validateur */
        group rpki-validator {
            session 10.0.0.1 {
                refresh-time 120;
                hold-time 180;
                port 8282;
                local-address 10.0.0.2;
            }
        }
    }
}
```

Le cache/validateur ne revoit que les ROAs pour des AS donnés, la décision de routage restant à la décision du routeur via sa configuration comme l'illustre la figure 6.

Lors de la validation d'une route à l'aide des ROAs, trois cas de figures peuvent arriver :

1. la route correspond à un ROA avec une correspondance du numéro d'AS.
2. la route correspond à un ROA avec aucune correspondance du numéro d'AS.
3. aucune correspondance à un ROA.

A ce stade, c'est la politique configurée par l'opérateur sur ces équipements qui décideront de la stratégie à mettre en place. Plusieurs stratégies sont possibles comme celle de type paranoïaque « je n'accepte que les routes dites valides », etc.

L'avantage principal de cette approche est que les impacts sur l'équipement réseau sont acceptables comparés aux calculs cryptographiques nécessaires des autres approches. L'inconvénient est que la mise à jour des ROAs doit être en temps réel pour éviter qu'une route ne soit pas prise en compte bien qu'elle soit légitime. Elle demande aussi l'adhésion de l'ensemble de la communauté, sinon chaque opérateur sera obligé d'accepter les routes non valides par défaut rendant la solution partielle.

4 Les recommandations de l'ANSSI

L'agence nationale de la sécurité des systèmes d'information vient de publier un guide des bonnes pratiques de configuration BGP. Il s'agit d'un guide pratique qui contient des exemples concerts de configuration de type Cisco, Juniper, Alcatel, etc. Après une présentation des différents types d'interconnexion BGP (peering privé entre deux AS, session établie en « multi-hop », etc.), le guide détaille un ensemble de recommandations ainsi que la matrice d'application de ces recommandations avec les différentes types d'interconnexion.

Voici quelques exemples de ces recommandations :

- Authentification des sessions (référence 2.2 dans cet article).
- Filtrage des annonces de routes (référence 2.4 dans cet article). Le guide aborde de plus la suppression des AS privés, le filtrage des routes par défaut, le filtrage sur l'AS path, etc.
- La journalisation des informations relatives à BGP à des fins de supervision active (détection de problème de stabilité, etc.).
- L'utilisation de mécanisme pour lutter contre l'usurpation d'adresses IP basé sur la technique dite de l'URPF (Unicast Reverse Path Forwarding). Elle consiste à ignorer un paquet s'il ne provient pas de l'interface que le routeur aurait utilisé pour router la source du paquet.
- Etc.

Le lecteur trouvera une description détaillée de chaque mécanisme dans ce guide qui a aussi pour vocation d'évoluer régulièrement **[ANSSI BGP]**. Sur un plan international, un draft IETF est aussi en cours d'élaboration sur le sujet **[IETF BGP SECURITY]**.

Conclusion

La sécurité du routage porte à la fois sur la sécurisation des sessions et des informations de routage échangées. Bien que la sécurisation des sessions permet de mettre en œuvre de nombreux mécanismes (TTL, MD5, etc.), la sécurisation des informations de routage est plus large et n'a pas atteint sa maturité.

Une analyse transversale montre que la vitesse de convergence des routes est critique et que le futur mécanisme de sécurité ne doit pas la freiner tout en assurant l'origine et le chemin pris par une annonce de route.

Enfin, cette future solution ne peut pas échapper à une administration «lourde» de gestion des adresses, AS, etc. impliquant aussi une distribution temps réelle avec les réseaux des opérateurs. ■

REMERCIEMENTS

Merci à la relecture attentive de Bruno Decraene et Benjamin Caillat.

RÉFÉRENCES

[ANSSI BGP] Guides de recommandations, http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/

[Bellman-Ford] Algorithme de Bellman-Ford, Wikipédia en français (http://fr.wikipedia.org/wiki/Algorithme_de_Bellman-Ford).

[HAWK] Les sources de HAWK sont disponibles sur le site web : https://sites.google.com/site/tableaudebordsecurite/home

C.Llorens, L.Levier, D.Valois ; B.Morin Tableaux de bord de la sécurité réseau, 3ème édition, Eyrolles, 562 pages, ISBN 2-212-12821-5, septembre 2010.

[IETF BGP SECURITY] J. Durand, I. Pepelnjak, G. Doering, BGP operations and security, IETF, draft, 2014, http://tools.ietf.org/html/draft-ietf-opsec-bgp-security-01

[PGBGP] Josh Karlin, Improving BGP by Cautiously Adopting Routes, 2006, http://dl.acm.org/citation.cfm?id=1318378

[RFC4271] Rekhter (Y.), Li (T)., A Border Gateway Protocol 4 (BGP-4), IETF, 2006, http://www.ietf.org/rfc/rfc4271.txt

[RFC3682] V. Gill, J. Heasley, D. Meyer, The Generalized TTL Security Mechanism (GTSM),IETF, 2004, http://www.ietf.org/rfc/rfc3682.txt

[RFC3882] D. Turk, Configuring BGP to Block Denial-of-Service Attacks, IETF, 2004, http://www.ietf.org/rfc/rfc3882.txt

[ROA_1] M. Lepinski, S. Kent, An Infrastructure to Support Secure Internet Routing, IEFT, 2012, http://tools.ietf.org/html/rfc6480.

[ROA_2] ripe, managing ROA, http://www.ripe.net/lir-services/resource-management/certification/resource-certification-roa-management

[RPKI] rpki.net project site, https://rpki.net/

[SBGP] Charles Lynn, Joanne Mikkelson, Karen Seo, IETF, 2003, http://tools.ietf.org/html/draft-clynn-s-bgp-protocol-01

[SO-BGP] R. White, IETF, 2006, http://tools.ietf.org/html/draft-white-sobgp-architecture-02

[WIKI RR] Réflecteurs de routes, http://fr.wikipedia.org/wiki/Route_reflector