Routage BGP sûr et efficace

Le protocole BGP (Border Gateway Protocol) est une caractéristique fondamentale de l'Internet, qui contribue essentiellement à rassembler la pléthore de réseaux qui composent le Web et à transporter les vastes quantités de trafic qui sillonnent le globe chaque jour.

En tant que pièce essentielle du puzzle de l'Internet, il est impératif que celuici fonctionne sans heurts et évite les vulnérabilités, les interruptions et les problèmes de sécurité.

Le réseau Internet dépend fortement des opérateurs qui font ce qu'il faut pour s'assurer que les informations correctes soient transmises aux parties concernées. Cependant, la mise en place d'un filtrage de routes BGP robuste et infaillible représente un défi pour de nombreuses organisations.

Le protocole BGP fonctionne très bien, mais il existe depuis bien avant les problèmes de sécurité spécifiques d'aujourd'hui et fonctionne en coordination avec des réseaux dispersés dans le monde entier, ce qui le rend potentiellement vulnérable aux détournements et aux fuites. L'Internet Society a estimé, par exemple, qu'il y a eu plus de 5 000 fuites et usurpations de routes en 2017.

Les informations recueillies par la division Global IP Network de NTT sur ce phénomène ont montré certaines tendances aux États-Unis : la plupart de ces fuites semblent se produire au milieu de la semaine, vers le mardi, mais il y a aussi un pic le vendredi, juste avant le début du week-end. Il faut donc faire preuve d'une grande vigilance durant ces périodes.

Les fuites de routes BGP impliquent une mauvaise configuration accidentelle ou une annonce illégitime des préfixes, ou des blocs d'adresses IP, qui se propagent sur les réseaux et entraînent un routage sous-optimal ou une usurpation de trafic.

Ces types de fuites ont continué à se produire au cours de la dernière décennie, année après année. Il est donc important de mettre en place des filtres pour contrecarrer les problèmes que cela peut causer.

Il existe un certain nombre de mécanismes de ce type qui peuvent contribuer à protéger contre ces fuites : des méthodes auxquelles NTT et Global IP Network sont parfaitement préparés pour apporter leur aide.

Peerlock « Lite »

Une façon de filtrer, en utilisant une méthode que NTT appelle Peerlock « Lite », consiste à rejeter les préfixes qui sont passés par des réseaux Tier 1 reçus de clients ou de pairs (voir le lien pour les réseaux les plus couramment considérés comme faisant partie de ce Tier).

Par exemple, NTT n'est accessible que par le biais d'un appairage sans règlement. Par conséquent, toutes les routes vers NTT que vous recevez d'un client ou d'un pair sont des fuites. En utilisant les mécanismes de protection déployés au niveau des échanges privés ou des échanges Internet pour refuser ces réseaux Tier 1, il est possible de bloquer assez facilement de nombreux problèmes potentiels avant même qu'ils ne se produisent.

> “ En utilisant les mécanismes de protection déployés au niveau des échanges privés ou des échanges Internet… il est possible de **bloquer assez facilement de nombreux problèmes potentiels** avant même qu'ils ne se produisent.

L'inconvénient de cette méthode est qu'elle nécessite une liste statique de numéros de systèmes autonomes (ASN), qui sont des numéros identifiant des réseaux particuliers. Sa nature statique signifie que si la fonction d'un de ces réseaux est modifiée ou s'il cesse d'être sans transit, la liste doit être mise à jour. Il est donc essentiel de veiller à ce qu'un examen semestriel ou annuel soit effectué pour maintenir l'exactitude de la liste. Elle exige également une connaissance inférée ou explicite des relations de transit des ASN verrouillées. Néanmoins, cette méthode est l'un des moyens les plus efficaces de mettre fin aux fuites de route.

Communautés BGP

Une autre méthode pour bloquer les fuites consiste à s'assurer que les préfixes reçus des partenaires d'appairage sans règlement ne sont jamais annoncés aux autres partenaires d'appairage de ce type. Un moyen d'y parvenir est de marquer les routes avec des communautés BGP, ou des labels pour les routes qui partagent une propriété commune. Les filtres peuvent alors être réglés de manière à ce que les préfixes sans les communautés appropriées soient rejetés à la sortie d'un routeur frontalier.

En outre, si aucune communauté n'est associée à des routes particulières, il serait souhaitable que celles-ci ne soient pas annoncées à une autre partie. Ainsi, si ces préfixes pénètrent d'une manière ou d'une autre dans votre réseau, celui-ci ne les propagera jamais. De cette façon, l'utilisation des communautés BGP peut être un outil clé pour prévenir les fuites de route.

Parmi les communautés BGP les plus connues, on trouve « no-export » et « noadvertise ». La première est associée aux routes qui ne doivent pas être annoncées au-delà de l'ASN de l'entreprise et la seconde à celles qui ne doivent pas être annoncées au-delà du routeur de réception. Il est important de comprendre le comportement de ces communautés avant de les utiliser, ce qui permet de s'assurer que le niveau de disponibilité requis est maintenu sur les routes.

Les communautés peuvent être spécifiées pour des catégories telles que le lieu où les routes ont été apprises (comme un client de transit ou un partenaire d'appairage) ou pour des lieux tels que l'Europe ou une ville particulière. Cependant, l'éventail des possibilités pour les communautés BGP est large, cette flexibilité offrant une marge de manoeuvre importante pour les exploiter.

À titre d'exemple de l'utilisation de telles communautés, NTT en a une qui peut être appliquée pour la suppression des annonces aux partenaires d'appairage de l'opérateur. Un client peut l'utiliser si, par exemple, il veut détourner le trafic d'un réseau pair impacté par une congestion de trafic ou qui subit une panne, et le diriger vers un autre. Une autre option permet de détourner le trafic, mais de laisser les annonces de routage vers le pair comme sauvegarde de dernier recours en cas de problèmes de connexion avec d'autres pairs également.

Ces options peuvent être appliquées à tous les pairs ou seulement à certains d'entre eux, dans le but de donner aux clients un maximum de souplesse pour déterminer comment les annonces d'itinéraires sont traitées de la manière qui correspond le mieux à leurs besoins commerciaux.

Parallèlement, NTT propose des communautés plus larges pour les choix régionaux et le blackholing déclenché par la communauté également, y compris le blackholing sélectif et régional, qui fournit des outils aux clients avec des options encore plus granulaires.

Listes blanches

Une autre approche consiste à appliquer une « liste blanche » de préfixes qu'un client peut annoncer à chaque session BGP externe (eBGP), ce qui rend les opérations un peu plus sûres.

C'est une méthode que NTT emploie pour toutes ces sessions en utilisant les données des registres de routage Internet (IRR). En effet, la société utilise une liste blanche unique pour chaque client, ce qui réduit considérablement les risques et l'étendue des dommages, et lui permet de contrôler étroitement les routes qu'elle accepte de ses clients.

Outre les mécanismes proposés par NTT pour traiter ce problème, il existe un certain nombre d'outils en open source qui peuvent être utiles pour appliquer des filtres de préfixes et qui peuvent être convertis dans un format adapté à la plateforme de routage particulière, comme BGPQ3.

> “
>
> NTT utilise une liste blanche **unique** pour **chaque client,** ce qui réduit considérablement les risques et l'étendue des dommages.

Limites maximales de préfixes

Une autre méthode pour prévenir les fuites sur les routes consiste à appliquer des limites maximales de préfixes. Par exemple, une limite de 1 000 routes peut être appliquée pour une session eBGP, de sorte que la session serait automatiquement fermée si ce nombre est dépassé.

Ces limites de préfixes constituent une mesure de sécurité essentielle pour aider le réseau à réagir de manière à causer le moins de dommages possible au système de routage mondial et à prévenir les fuites, en protégeant les routeurs et les réseaux. Elles peuvent constituer un moyen très efficace de protéger le réseau s'il y a effectivement une fuite de route, car elles empêchent sa propagation.

Les limites maximales des préfixes peuvent être appliquées soit avant soit après la politique, bien que l'effet maximum puisse être obtenu en faisant cela avant la politique pour aider à éviter tout problème important avant qu'il ne se produise, plutôt que de risquer que certains préfixes ayant pu fuire soient autorisés à passer. Néanmoins, les politiques de filtrage des préfixes varient selon la plateforme de routage, certaines ne permettant de le faire qu'après la politique.

Peerlocking

NTT a déployé avec succès une forme plus complète de Peerlocking. L'utilisation de ce système peut réduire considérablement le risque, à l'échelle mondiale, que des préfixes soient acceptés par des routes non autorisées.

L'essence de cette approche est de « mettre en réseau ce que les humains vous ont dit ». En termes simples, ce système repose sur des partenaires d'appairage qui indiquent à NTT quels réseaux, le cas échéant, sont des fournisseurs de transit autorisés, les partenaires qui fournissent ces informations étant appelés « ASN protégés ». Les routes peuvent alors être « verrouillées » si elles proviennent de fournisseurs de transit non autorisés.

Il est fortement recommandé d'informer les réseaux que vous essayez de protéger et d'accepter que ces filtres soient déployés, afin qu'il n'y ait pas de surprises en cours de route, encore une fois en s'appuyant sur la communication avec les pairs. Les partenaires doivent toujours être conscients de ce qui se passe avec le réseau, et l'engagement est essentiel à cet égard.

> “
>
> Le mécanisme de Peerlocking de NTT peut donc **réduire considérablement l'impact** et la prolifération des fuites de route.

Il est également essentiel que ces filtres Peerlock soient appliqués à chaque session eBGP, qu'elle soit orientée vers le client ou qu'elle fasse l'objet d'un appairage, afin de garantir que ce mécanisme de protection des clés soit pleinement utilisé.

En bref, le Peerlocking de NTT offre une méthode très efficace pour stopper les fuites de route, et la société a remarqué des améliorations significatives pour les réseaux qui ont accepté de devenir des ASN protégés.

Flexibilité

NTT répond à des attentes régionales, offrant ainsi une certaine flexibilité à ses pairs mondiaux sans règlement s'ils gèrent leurs opérations différemment sur différents continents. NTT dispose également d'un manuel généré pour chaque pair pour lequel il permet le verrouillage. Cela est utile pour établir la documentation sur les tenants et aboutissants de la technologie et son fonctionnement, ainsi que pour qu'une entreprise puisse conserver ces connaissances au fur et à mesure que les employés vont et viennent.

En définitive, le mécanisme de Peerlocking de NTT peut donc réduire de manière significative l'impact et la prolifération des fuites de routes, en aidant par une surveillance active de la zone sans défaut.

L'une des clés de la réussite de NTT dans le déploiement de ces technologies est son contrôleur SDN leader du secteur, GIN Unified Management System (GUMS). L'utilisation du GUMS permet à NTT de déployer de manière programmatique les changements apportés aux listes blanches, aux communautés, au Peerlocking et aux politiques BGP en général. Cela conduit à des configurations déployées de manière cohérente et à des taux d'erreur de configuration beaucoup plus faibles.

Les opérateurs apportent des modifications dans l'interface Web GUMS et déploient leurs modifications à partir du serveur GUMS plutôt que de se connecter aux routeurs et d'apporter des modifications manuellement. Cette possibilité rend le processus plus efficace, ce qui améliore l'efficacité du système dans son ensemble.

Pour en savoir plus ou pour nous faire part de vos commentaires, contactez-nous à l'adresse suivante:

gin@ntt.net
gin.ntt.net
@GinNTTnet #globalipnetwork #AS2914

