Groupe de travail Réseau
Request for Comments : 3704
RFCmise à jour : 2827
BCP : 84
Catégorie : Bonne practiques actuelles

F. Baker, Cisco Systems
P. Savola, CSC/FUNET
mars 2004

Traduction Claude Brière de L'Isle

Filtrage d'entrée pour réseaux multi rattachements

Résumé
Le BCP 38, RFC2827, est conçu pour limiter l'impact d'attaques réparties de déni de service, en refusant l'accès au réseau au trafic avec des adresses usurpées, et pour aider à assurer que le trafic peut être suivi à la trace jusqu'à son réseau source correct. Comme effet collatéral de la protection de l'Internet contre de telles attaques, le réseau qui met en œuvre cette solution se protège aussi lui-même de cette attaque et d'autres, telles que l'usurpation d'accès de gestion à des équipements de réseautage. Il y a des cas où ceci peut créer des problèmes, par exemple, avec le multi rattachement. Le présent document décrit les mécanismes opérationnels actuels de filtrage d'entrée, examine les questions générales en rapport avec le filtrage d'entrée, et creuse en particulier la question des effets sur le multi rattachement. Ce mémoire met à jour la RFC2827.

Table des matières

1. Introduction

Le BCP 38, [RFC2827], a été conçu pour limiter l'impact des attaques réparties de déni de service, en refusant l'accès au réseau au trafic avec des adresses usurpées, et pour aider à s'assurer que le trafic peut être suivi à la trace jusqu'à son réseau de source correct. Par un effet collatéral de la protection de l'Internet contre de telles attaques, le réseau qui met en œuvre cette solution se protège aussi lui-même contre cela et contre d'autres attaques, telles que de l'usurpation d'accès de gestion aux équipements de réseautage. Il y a des cas où cela peut créer des problèmes, par exemple, avec le multi rattachement. Le présent document décrit les mécanismes opérationnels actuels de filtrage d'entrée, examine les questions générales qui se rapportent au filtrage d'entrée et creuse en particulier la question des effets sur le multi rattachement.

La RFC2827 recommande aux FAI (fournisseurs d'accès Internet) de réguler le trafic de leurs abonnés en éliminant le trafic qui entre dans leurs réseaux et qui vient d'une adresse de source qui n'est pas légitimement utilisée par le réseau de l'abonné. Le filtrage inclut, mais ne s'y limite en aucune façon, le trafic dont l'adresse de source est ce qu'on appelle une "adresse martienne" – une adresse qui est réservée [RFC3330], y compris toute adresse dans les 0.0.0.0/8, 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 224.0.0.0/4, ou 240.0.0.0/4.

Le raisonnement qui est derrière la procédure de filtrage d'entrée est que les attaques réparties de déni de service usurpent souvent les adresses de source d'autres systèmes, en plaçant un nombre aléatoire dans le champ. Dans certaines attaques, le nombre aléatoire est volontairement dans la gamme du réseau cible, attaquant simultanément une ou plusieurs machines et causant l'attaque par ces machines d'autres machines avec des messages ICMP ou d'autre trafic ; dans ce cas, les sites attaqués peuvent se protéger par un filtrage approprié, en vérifiant que leurs préfixes ne sont pas utilisés dans les adresses de source des paquets reçus de l'Internet. Dans d'autres attaques, l'adresse de source est littéralement un nombre aléatoire de 32 bits, d'où il résulte que la source de l'attaque est difficile à retracer. Si le trafic qui quitte un réseau bordure et entre dans celui d'un FAI peut être limité au trafic qu'il envoie légitimement, les attaques peuvent être quelque peu atténuées : le trafic avec des adresses de source aléatoires ou impropres peut être supprimé avant qu'il ne cause de dommages significatifs, et les attaques peuvent être directement retracées au moins jusqu'à leur réseau source.

Le présent document vise les FAI et opérateurs de réseau bordure qui 1) aimeraient en savoir plus sur les méthodes de filtrage d'entrée en général, ou 2) utilisent déjà le filtrage d'entrée dans une certaine mesure mais voudraient étendre son usage et veulent éviter les pièges du filtrage d'entrée dans les scénarios de multi rattachement ou asymétriques.

La section 2 décrit plusieurs façons de mettre en œuvre le filtrage d'entrée et les examine dans le contexte général. La section 3 donne quelques éclaircissements sur l'applicabilité des méthodes de filtrage d'entrée. La section 4 analyse le filtrage d'entrée en détails du point de vue du multi rattachement. La section 5 identifie des conclusions et futures pistes de travaux potentielles.

2. Différentes façons de mettre en œuvre le filtrage d'entrée

Cette section sert d'introduction aux différentes techniques de fonctionnement utilisées pour mettre en œuvre le filtrage d'entrée au moment de la rédaction du présent mémoire. Les mécanismes sont décrits et analysés en termes généraux, et les questions spécifiques du multi rattachement sont décrites à la section 4.

Il y a au moins cinq façon de mettre en œuvre la RFC2827, avec des impacts variés. Cela inclut (les noms sont d'usage relativement courant) :
- o les listes d'accès d'entrée,
- o la transmission sur le chemin inverse (RPF, *Reverse Path Forwarding*) strict,
- o la transmission sur le chemin inverse sur le chemin faisable,
- o la transmission sur le chemin inverse lâche,
- o la transmission sur le chemin inverse lâche ignorant les chemins par défaut.

D'autres mécanismes sont aussi possibles, et bien sûr, il y a un certain nombre de techniques qui pourraient tirer profit d'études, spécifications, mises en œuvre, et/ou déploiements plus approfondis ; voir la section 6. Cependant, ils sortent du domaine d'application de ce document.

2.1 Listes d'accès d'entrée

Une liste d'accès d'entrée est un filtre qui confronte l'adresse de source de tout message reçu sur une interface réseau à une liste de préfixes acceptables, éliminant tout paquet qui ne correspond pas au filtre. Bien que ce ne soit en aucune façon la seule manière de mettre en œuvre un filtre d'entrée, c'est celle qui est proposée par la [RFC2827], et en un sens, la plus déterministe.

Cependant, les listes d'accès d'entrée sont normalement tenues à la main ; par exemple, oublier de mettre la liste à jour chez les FAI si l'ensemble de préfixes change (par exemple, par suite de multi rattachement) peut conduire à éliminer les paquets si ils ne passent pas le filtre d'entrée.

Naturellement, ce problème n'est pas limité aux listes d'accès d'entrée – il est inhérent au filtrage d'entrée lorsque le filtre d'entrée n'est pas complet. Cependant, les listes d'accès d'entrée ne sont normalement pas plus difficiles à tenir que les autres mécanismes, et avoir une liste qui n'est plus à jour peut empêcher l'accès légitime.

2.2 Transmission sur le chemin inverse strict

La transmission sur le chemin inverse strict (RPF strict) est une façon simple pour mettre en œuvre le filtre d'entrée. Elle est conceptuellement identique à l'utilisation des listes d'accès pour le filtrage d'entrée, sauf que la liste d'accès est dynamique. Cela peut aussi être utilisé pour éviter des configurations dupliquées (par exemple, de maintenir à la fois des chemins statiques ou des filtres de liste de préfixe BGP et des listes d'accès d'interface). La procédure est que l'adresse de source est recherchée dans la base de données d'informations de transmission (FIB, *Forwarding Information Base*) - et si le paquet est reçu sur l'interface qui aurait été utilisée pour transmettre le trafic à la source du paquet, la vérification est réussie.

La transmission sur le chemin inverse strict est une approche très raisonnable en présence de toute sorte de réseau bordure ; en particulier, elle est très supérieure aux listes d'accès d'entrée lorsque la bordure de réseau annonce plusieurs préfixes qui utilisent BGP. Cela va pour un filtre simple, bon marché, rapide, et dynamique.

Mais la transmission sur le chemin inverse strict pose par elle même certains problèmes. D'abord, l'essai n'est applicable qu'aux endroits où l'acheminement est symétrique – lorsque les datagrammes IP dans une direction et les réponses provenant de l'autre direction suivent de façon déterministe le même chemin. Bien que ceci soit courant sur les interfaces de bordure de réseau avec leur FAI, cela n'est pas du tout la règle entre les FAI, qui utilisent normalement des acheminements asymétriques du style "patate chaude". Ainsi, si BGP porte des préfixes et que des préfixes légitimes ne sont pas annoncés ou ne sont pas acceptés par le FAI en fonction de sa politique, l'effet sera le même que celui du filtrage d'entrée utilisant une liste d'accès incomplète : du trafic légitime est filtré par manque d'un chemin dans la base de données d'informations de transmission du routeur qui filtre.

Il y a des techniques opératoires, en particulier avec BGP, mais aussi applicables d'une certaine manière à d'autres protocoles d'acheminement, pour faire mieux fonctionner RPF strict dans le cas de trafic asymétrique ou multi rattachement. Le FAI alloue une meilleure métrique qui n'est pas propagée en dehors du routeur, soit une "pondération" spécifique du fabricant, soit une disposition de distance dans le protocole pour préférer les chemins reçus directement. Avec BGP et la machinerie suffisante déjà en place, le réglage de préférences pourrait même être automatisé, en utilisant les communautés BGP de la [RFC1997]. De cette façon, le chemin sera toujours le meilleur de la FIB, même dans les scénarios où seulement la connexité principale serait utilisée et où normalement aucun paquet ne passerait à travers l'interface. Cette méthode suppose qu'il n'y a pas de filtrage RPF strict entre le routeur bordure principal et le routeur bordure secondaire ; en particulier, lorsque elle est appliquée au multi rattachement à des FAI différents, cette hypothèse peut se révéler fausse.

2.3 Transmission sur le chemin inverse faisable

La transmission sur le chemin inverse faisable (RPF faisable) est une extension de la RPF stricte. L'adresse de source est toujours recherchée dans la FIB (ou un tableau spécifique de RPF équivalent) mais au lieu de juste insérer là le meilleur chemin, les chemins de remplacement (s'il y en a) sont également ajoutés, et leur prise en considération est valide. La liste est remplie en utilisant les méthodes spécifiques des protocoles d'acheminement, par exemple en incluant tout ou N (où N est inférieur à tout) chemins BGP faisables dans la base de données d'informations d'acheminement (RIB). Parfois, cette méthode a été mise en œuvre au titre de la RPF stricte.

Dans le cas d'acheminement asymétrique et/ou de multi rattachement à la bordure du réseau, cette approche donne un moyen relativement facile de traiter les plus gros problèmes de RPF strict.

Il est d'une importance critique de comprendre le contexte dans lequel fonctionne RPF faisable. Le mécanisme s'appuie sur la propagation des annonces de chemins cohérents (c'est-à-dire, de même préfixes, à travers tous les chemins) à tous les routeurs qui effectuent la vérification de RPF faisable. Par exemple, cela peut ne pas tenir dans le cas où un FAI secondaire ne propage pas l'annonce BGP au FAI principal, par exemple, à cause d'un manque de mise à jour de transpositions de chemin ou d'autres politiques d'acheminement. Les modes de défaillance sont normalement similaires au "RPF strict à fonctionnement amélioré", comme décrit ci-dessus.

Comme ligne directrice générale, si une annonce est filtrée, les paquets seront filtrés aussi.

Par conséquent, RPF faisable correctement défini est un outil très puissant dans certaines sortes de scénarios d'acheminement asymétrique, mais il est important de mieux comprendre son rôle opérationnel et son applicabilité.

2.4 Transmission sur le chemin inverse lâche

La transmission sur le chemin inverse lâche (RPF lâche) est algorithmiquement similaire à la RPF stricte, mais en diffère en ce qu'elle ne vérifie que l'existence d'un chemin (même un chemin par défaut, si applicable) et non vers où le chemin mène. En pratique, cela pourrait être considéré comme une "vérification de présence de chemin" ("RPF lâche est un nom

trompeur en un sens parce qu'il n'y a pas de vérification du "chemin inverse" en premier lieu).

L'avantage discutable de RPF lâche se trouve dans les situations d'acheminement asymétrique : un paquet est abandonné si il n'y a pas de chemin du tout, comme pour les "adresses martiennes" ou les adresses qui ne sont actuellement pas acheminées, mais il n'est pas abandonné si un chemin existe.

La transmission sur le chemin inverse lâche a cependant des problèmes. Comme elle sacrifice la directionnalité, elle perd la capacité à limiter le trafic d'un réseau bordure au trafic généré légitimement à partir de ce réseau, dans la plupart des cas, rendant le mécanisme inutile comme mécanisme de filtrage d'entrée.

Aussi, de nombreux FAI utilisent les chemins par défaut pour divers objets comme la collecte du trafic illégitime sur des systèmes dit "pot de miel" ou pour éliminer tout trafic pour lequel ils n'ont pas de "vrai" chemin, et de plus petits FAI peuvent très bien acheter des capacités de transit et utiliser un chemin par défaut à un plus gros fournisseur. Au moins, quelques mises en œuvre de RPF lâche vérifient sur quoi pointe le chemin par défaut. Si le chemin pointe sur l'interface où la RPF lâche est activée, tout paquet provenant de cette interface est permis ; si il ne pointe nulle part ou sur quelque autre interface, les paquets avec les adresses de source défectueuses seront éliminés à l'interface RPF lâche même en présence d'un chemin par défaut. Si une vérification d'une granularité aussi fine n'est pas mise en œuvre, la présence d'un chemin par défaut annule complètement l'effet de la RPF lâche.

Un cas où la RPF lâche pourrait bien convenir serait celui d'un FAI qui filtre les paquets provenant de ses fournisseurs amont, pour se débarrasser des paquets qui ont des adresses "martiennes" ou autres non acheminables.

Si les autres approches ne conviennent pas, RPF lâche pourrait être utilisé comme une forme de vérification de contrat : l'autre réseau est supposé certifier qu'il a fourni des règles appropriées de filtrage d'entrée, de sorte que le réseau qui effectue le filtrage a seulement besoin de vérifier le fait et réagir si des paquets qui constitueraient une rupture du contrat étaient détectés. Bien sûr, ce mécanisme ne montrerait que si les adresses de source utilisées sont des adresses "martiennes" ou autres adresses non acheminées – et pas si elles sont de l'espace d'adresses de quelqu'un d'autre.

2.5 Transmission sur le chemin inverse lâche en ignorant les chemins par défaut

La cinquième technique de mise en œuvre peut être caractérisée comme RPF lâche en ignorant les chemins par défaut, c'est-à-dire, en "vérification explicite de présence de chemin". Dans cette approche, le routeur recherche l'adresse de source dans le tableau d'acheminements, et conserve le paquet si il trouve un chemin. Cependant, dans la recherche, les chemins par défaut sont exclus. Donc, la technique est principalement utilisable dans les scénarios où les chemins par défaut ne sont utilisés que pour capturer le trafic qui a des fausses adresses de source, avec une liste extensive (ou même pleine) de chemins explicites pour couvrir le trafic légitime.

Comme avec RPF lâche, ceci est utile dans les endroits où on trouve un acheminement asymétrique, comme sur les liaisons entre FAI. Cependant, comme avec RPF lâche, dans la mesure où il sacrifie la directionnalité, il perd la capacité de limiter le trafic d'un réseau bordure au trafic généré légitimement à partir de ce réseau.

3. Précisions sur l'applicabilité du filtrage d'entrée

Ce qui peut n'être pas directement apparent est que le filtrage d'entrée n'est pas seulement appliqué à la "dernière" interface entre le FAI et l'utilisateur final. Il est parfaitement sain, et recommandé, d'effectuer aussi le filtrage d'entrée aux bordures des FAI lorsque c'est approprié, aux routeurs qui connectent des LAN à un réseau d'entreprise, etc. – cela augmente la défense en profondeur.

3.1 Filtrage d'entrée à plusieurs niveaux

À cause du plus large déploiement du filtrage d'entrée, la question est récurrente. Le filtrage d'entrée doit fonctionner partout où il est utilisé, et pas seulement entre les deux premières parties. C'est-à-dire que si un usager négocie un arrangement de filtrage d'entrée particulier avec son FAI, il devrait aussi s'assurer (ou s'assurer que le FAI s'assure) que les mêmes arrangements s'appliquent aussi aux liaisons amont et d'échange de trafic du FAI, si le filtrage d'entrée est utilisé -- ou va être utilisé, à un moment futur ; comme avec les FAI amont et les homologues d'échange de trafic.

Par conséquent, les modèles manuels qui ne propagent pas automatiquement les informations à toutes les parties où devraient aller les paquets et où le filtrage d'entrée pourrait être appliqué ont seulement une utilité générique limitée.

3.2 Filtrage d'entrée pour protéger sa propre infrastructure

Une autre caractéristique qui découle du plus large déploiement du filtrage d'entrée peut n'être pas directement apparente. Les routeurs et autres infrastructures de FAI sont vulnérables à plusieurs sortes d'attaques. La menace est normalement atténuée en restreignant qui peut accéder à ces systèmes.

Cependant, sauf si le filtrage d'entrée (ou au moins, un sous-ensemble limité de celui-ci) a été déployé à chaque frontière (vers les abonnés, vers les homologues et vers l'amont) – bloquant l'utilisation de vos propres adresses comme adresses de source -- les attaquants peuvent être capables de circonvenir les protections de l'équipement d'infrastructure.

Donc, en déployant le filtrage d'entrée, on n'aide pas seulement l'Internet dans son ensemble, mais on se protège aussi contre plusieurs classes de menaces contre sa propre infrastructure.

3.3 Filtrage d'entrée sur des liaisons d'échange de trafic

Le filtrage d'entrée sur les liaisons d'échange de trafic, que ce soit par les FAI ou par les sites d'extrémité, n'est en réalité pas très différent du filtrage d'entrée plus typique "vers l'aval" ou "vers l'amont".

Cependant, il est important de noter qu'avec un mélange de liaisons vers l'amont/aval et d'échange de trafic, les différentes liaisons peuvent avoir des propriétés différentes (par exemple, par rapport aux contrats, à la confiance, à la viabilité du mécanisme de filtrage d'entrée, etc.). Dans le cas le plus normal, en utilisant juste un mécanisme de filtrage d'entrée à l'égard d'un homologue (par exemple, RPF strict) fonctionne très bien tant que l'acheminement entre les homologues conserve une raisonnable symétrie. Il pourrait même être considéré comme utile d'être capable de filtrer les adresses de source venant d'une liaison amont qui auraient dû venir sur une liaison d'échange de trafic (ce qui implique que quelque chose comme la RPF stricte est utilisée à l'égard de l'amont) – mais ceci est un sujet plus complexe et il est considéré comme sortant du domaine d'application de ce document ; voir la Section 6.

4. Solutions au filtrage d'entrée avec multi rattachement

Tout d'abord, on doit se demander pourquoi un site fait un multi rattachement ; par exemple, le réseau bordure pourrait :
- o utiliser deux FAI pour sauvegarder la connexité Internet afin d'assurer la robustesse,
- o utiliser tout FAI qui offre le service TCP le plus rapide du moment,
- o avoir besoin de plusieurs points d'accès à l'Internet dans des endroits où aucun FAI n'offre de service, ou
- o être en train de changer de FAI (et donc, le multi rattachement n'est que temporaire).

On peut imaginer un certain nombre d'approches pour contourner les limitations des filtres d'entrée pour les réseaux multi rattachement. On a comme options :
1. de ne pas faire de multi rattachement,
2. de ne pas utiliser de filtre d'entrée,
3. accepter que le service soit incomplet,
4. sur certaines interfaces, affaiblir le filtrage d'entrée en utilisant une forme appropriée de vérification de RPF lâche, comme décrit au paragraphe 4.1,
5. s'assurer, par BGP ou par contrat, que chaque filtre d'entrée de FAI est complet, comme décrit au paragraphe 4.2,
6. s'assurer que les réseaux bordure ne livrent à leurs FAI que le trafic qui passe en fait le filtre d'entrée, comme décrit au paragraphe 4.3.

Les trois premières ne sont évidemment mentionnées que pour être complet ; elles ne sont et ne peuvent être des positions viables ; les trois dernières sont examinées ci-dessous.

La quatrième et la cinquième doivent être assurées aussi chez le FAI amont, comme décrit au paragraphe 3.1.

Ensuite nous allons examiner les façons viables pour traiter des effets collatéraux des filtres d'entrée.

4.1 Utiliser RPF lâche quand c'est approprié

Lorsque l'acheminement asymétrique est préféré ou est inévitable, le filtrage d'entrée peut être difficile à déployer en utilisant un mécanisme comme la RPF stricte qui exige que les chemins soient symétriques. Dans de nombreux cas, utiliser des méthodes opérationnelles ou RPF faisable assure que le filtre d'entrée est complet, comme décrit ci-dessous. Faute de quoi, les seules options réelles sont de ne pas effectuer de filtrage d'entrée, d'utiliser une liste d'accès manuelle (éventuellement en plus de quelques autres mécanismes) ou d'utiliser une forme de vérification de RPF lâche.

Manquer à fournir aucun filtre d'entrée revient essentiellement à s'en remettre au réseau aval pour le faire lui-même, ce qui n'est pas la façon la plus sage de se comporter. Cependant, spécialement dans le cas de très grands réseaux de centaines ou même de milliers de préfixes, tenir manuellement des listes d'accès est sans doute trop demander.

L'utilisation de la RPF lâche ne semble pas un bon choix entre le réseau bordure et le FAI, car cela perd la directionnalité de la vérification. Cela plaide en faveur de l'utilisation d'un filtre complet dans le réseau amont ou de s'assurer dans le réseau aval que les paquets que le réseau amont va rejeter ne vont jamais l'atteindre.

Donc, l'utilisation de la RPF lâche ne peut pas être recommandée, sauf comme moyen de mesurer si des adresses "martiennes" ou autres adresses non acheminables sont utilisées.

4.2 S'assurer que le filtre d'entrée de chaque FAI est complet

Pour le réseau bordure, si le multi rattachement est utilisé pour des raisons de robustesse ou pour changer l'acheminement de temps en temps selon le comportement mesuré du FAI, la plus simple approche sera de s'assurer que ses FAI portent en fait ses adresses dans l'acheminement. Cela exige souvent que le réseau bordure utilise des préfixes indépendants du fournisseur et échange des chemins avec ses FAI au moyen de BGP, pour s'assurer que son préfixe est porté en amont aux FAI de transit majeurs. Cela implique nécessairement que le réseau bordure soit de taille et compétence technique à se qualifier pour une allocation d'adresse distincte et un numéro de système autonome de la part de son RIR *(?)*.

Il y a un certain nombre de techniques qui rendent plus facile de s'assurer que le filtre d'entrée du FAI est complet. La RPF faisable et la RPF stricte avec des techniques opérationnelles fonctionnent toutes deux assez bien pour les scénarios de multi rattachement ou asymétrique entre le FAI et un réseau bordure.

Lorsque un protocole d'acheminement n'est pas utilisé, mais que plutôt les informations du consommateur sont générées à partir de bases de données telles que Radius, TACACS, ou Diameter, le filtrage d'entrée peut être très facilement assuré et gardé à jour avec la RPF stricte ou des listes d'accès d'entrée générées automatiquement à partir de telles bases de données.

4.3. Envoyer le trafic en utilisant le préfixe d'un fournisseur seulement pour ce fournisseur

Pour les réseaux bordure plus petits qui utilisent un adressage fondé sur le fournisseur et dont les FAI mettent en œuvre des filtres d'entrée (ce qu'ils devraient faire) la troisième option est d'acheminer le trafic qui est originaire de l'espace d'adresses d'un certain fournisseur à ce fournisseur.

Ce n'est pas une procédure compliquée, mais elle exige une planification et une configuration soigneuses. Pour la robustesse, le réseau bordure peut choisir de se connecter à chacun de ses FAI à travers deux points de présence *(POP)* différents ou plus, de sorte que si un des POP ou ligne subit une panne, une autre liaison pour le même FAI peut être utilisée. Autrement, un ensemble de tunnels pourrait être configuré à la place de multiples connexions au même FAI [RFC2260], [RFC3178]. De cette façon, les routeurs bordure sont configurés pour inspecter d'abord l'adresse de source d'un paquet destiné à un FAI et pour l'envoyer dans le tunnel ou interface approprié vers le FAI.

Si un tel scénario est appliqué de façon exhaustive, de sorte qu'un routeur de sortie soit choisi dans le réseau bordure pour chaque préfixe qu'utilise le réseau, le trafic originaire de tout autre préfixe peut être sommairement éliminé au lieu d'être envoyé à un FAI.

5. Considérations pour la sécurité

Le filtrage d'entrée est normalement effectué pour s'assurer que le trafic qui arrive sur une interface réseau vient légitimement d'un ordinateur qui réside sur un réseau accessible à travers cette interface.

Plus le filtrage d'entrée est effectué près de la source réelle, plus il est efficace. On pourrait souhaiter que le routeur de premier bond s'assure que le trafic généré par les systèmes de son voisinage a été correctement adressé ; un routeur qui se trouve plus loin peut seulement s'assurer qu'il est possible qu'il y a bien un tel système au sein du préfixe indiqué. Donc, le filtrage d'entrée devrait être fait à plusieurs niveaux, avec différents niveaux de granularité.

Il importe de garder à l'esprit qu'alors que le but du filtrage d'entrée est de rendre les attaques retraçables, il est impossible de savoir si un attaquant particulier "quelque part dans l'Internet" va être filtré en entrée ou non. Donc, on peut seulement faire des suppositions sur ce que les adresses de source ont été usurpées ou non : dans tous les cas, obtenir un possible fil conducteur -- par exemple, contacter une source potentielle pour lui demander si elle observe ou non une attaque – est encore valable, et encore plus lorsque le filtrage d'entrée est plus largement déployé.

En conséquence, chaque domaine administratif devrait essayer de s'assurer d'un niveau suffisant de filtrage d'entrée sur ses frontières.

Les propriétés de sécurité et l'applicabilité des différents types de filtrage d'entrée diffèrent un peu.

- Les listes d'accès d'entrée requièrent normalement une maintenance manuelle, mais elles sont les plus éprouvées lorsque elles sont faites correctement ; normalement, les listes d'accès d'entrée vont le mieux entre la bordure et le FAI lorsque la configuration n'est pas trop dynamique si la RPF stricte n'est pas une option, entre les FAI si le nombre de préfixes utilisés est faible, ou a une couche supplémentaire de protection.

- La vérification de RPF stricte est un moyen très facile et sûr de mettre en œuvre le filtrage d'entrée. Elle convient normalement entre le réseau bordure et le FAI. Dans de nombreux cas, une simple RPF stricte peut être augmentée de procédures de fonctionnement dans le cas de schémas de trafic asymétriques, ou la technique de la RPF faisable peut aussi être prise en compte pour les autres chemins de remplacement.

- La vérification de la RPF de chemin faisable est une extension de la RPF stricte. Elle convient dans tous les scénarios où est la RPF stricte, sauf en particulier les scénarios de multi rattachement ou asymétriques. Cependant, on doit se rappeler que la RPF faisable suppose une génération et une propagation cohérentes des informations d'acheminement pour fonctionner ; les implications de cela doivent être comprises en particulier si une annonce de préfixe passe par des tiers.

- La RPF lâche filtre principalement des préfixes non acheminés tels que les adresses martiennes. Elle peut être appliquée dans les interfaces amont pour réduire la taille des attaques de déni de service avec des adresses de source non acheminées. Dans les interfaces aval, elle peut seulement être utilisée comme vérification de contrat, que l'autre réseau a effectué au moins un certain filtrage d'entrée.

Quand on pèse le pour et le contre des différents mécanismes de filtrage d'entrée, les propriétés de sécurité d'une approche plus souple devraient être considérées avec attention avant de l'appliquer. En particulier lorsqu'elle est appliquée par un FAI à l'égard d'un réseau bordure, il ne semble pas qu'il y ait beaucoup de raisons pour qu'une forme plus stricte de filtrage d'entrée ne soit pas appropriée.

6. Conclusions et travaux futurs

Le présent mémoire décrit les techniques de filtrage d'entrée en général et les options pour les réseaux multi rattachement en particulier.

Il est important pour les FAI de mettre en œuvre le filtrage d'entrée pour empêcher que soient utilisées des adresses usurpées, à la fois pour décourager les attaques de déni de service et pour les rendre plus traçables, et pour protéger leur propre infrastructure. Le présent mémoire décrit les mécanismes qui pourraient être utilisés pour réaliser cela, ainsi que les avantages et inconvénients de ces mécanismes.

Pour résumer :
- Le filtrage d'entrée devrait toujours être effectué entre le FAI et un réseau bordure à rattachement unique.
- Le filtrage d'entrée de RPF faisable ou techniques similaires à la RPF stricte pourrait presque toujours être aussi appliqué entre le FAI et les réseaux bordure multi rattachement.
- Les FAI et les réseaux bordure devraient tous deux vérifier que leurs propres adresses ne sont pas utilisées dans des adresses de source de paquets qui viennent d'en dehors de leur réseau.
- Une certaine forme de filtrage d'entrée est aussi raisonnable entre les FAI, en particulier si le nombre de préfixes est faible.

Le présent mémoire va abaisser la barre pour l'adoption du filtrage d'entrée en particulier dans des scénarios de réseaux asymétriques/multi rattachement où la croyance générale a été que le filtrage d'entrée est difficile à mettre en œuvre.

On peut identifier plusieurs domaines dans lesquels d'autres travaux seraient utiles :

- Spécifier plus en détails les mécanismes : ils y a des variantes entre les mises en œuvre, par exemple, sur la question de savoir si le trafic pour des adresses de destination en diffusion groupée vont toujours passer le filtre de RPF stricte ou non. En spécifiant formellement ces mécanismes, les mises en œuvre pourraient être harmonisées.

- Étudier et spécifier les mécanismes de RPF fondés sur la base de données d'informations d'acheminement (RIB) par

exemple, la RPF de chemin faisable, plus en détails. En particulier, considérer sous quelles hypothèses ces mécanismes fonctionnent comme prévu et sous lesquelles ils ne le font pas.

- Écrire sur les mécanismes de filtrage d'entrée une note plus générale que le présent mémoire, après avoir étoffé la taxonomie et les détails des mécanismes (les points ci-dessus).

- Considérer le cas plus complexe où un réseau a la connexité avec des propriétés différentes (par exemple, avec des homologues et avec des réseaux amont) et veut s'assurer que le trafic généré avec l'adresse d'un homologue ne devrait pas être acceptée si elle vient de l'amont.

7. Remerciements

Rob Austein, Barry Greene, Christoph Reichert, Daniel Senie, Pedro Roque, et Iljitsch van Beijnum ont relu ce document et ont aidé à l'améliorer. Thomas Narten, Ted Hardie, et Russ Housley ont fourni des réactions utiles qui ont aidé à finaliser le document.

8. Références

[RFC1997] R. Chandra, P. Traina, T. Li, "Attribut Community de BGP", août 1996. *(P.S.)*

[RFC2260] T. Bates, Y. Rekhter, "Prise en charge échelonnable de la connexité multi rattachement multi fournisseur", janvier 1998. *(Information)*

[RFC2827] P. Ferguson, D. Senie, "Filtrage d'entrée de réseau : Combattre les attaques de déni de service qui utilisent l'usurpation d'adresse de source IP", mai 2000. (*MàJ par* RFC3704) (BCP0038)

[RFC3178] J. Hagino, H. Snyder, "Prise en charge du multi rattachement IPv6 aux routeurs de sortie de site", octobre 2001. *(Info.)*

[RFC3330] IANA, "Adresses IPv4 d'usage particulier", septembre 2002. *(Information) (Remplacée par* RFC5735)

9. Adresse des auteurs

Fred Baker
Cisco Systems
Santa Barbara, CA 93117
USA
mél : fred@cisco.com

Pekka Savola
CSC/FUNET
Espoo
Finland
mél : psavola@funet.fi

10. Déclaration complète de droits de reproduction

des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur le répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous droits de reproduction, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.