Groupe de travail Réseau	P. Ferguson, Cisco Systems, Inc.
Request for Comments : 2827	D. Senie, Amaranth Networks Inc.
RFC rendue obsolète : 2267	mai 2000
BCP : 38	
Catégorie : Bonne pratiques actuelles	Trazduction Claude Brière de L'Isle

Filtrage d'entrée de réseau : Combattre les attaques de déni de service qui utilisent l'usurpation d'adresse de source IP

Statut du présent mémoire
Le présent document spécifie les bonne pratiques actuelles de l'Internet pour la communauté de l'Internet , et appelle à des discussions et suggestions pour son amélioration. La distribution de ce m"moire n'est soumise à aucune restriction.

Résumé
L'occurrence récente de diverses attaques de déni de service (DoS, *Denial of Service*) qui ont utilisé de fausses adresses de source se sont révélées être une source d'ennuis pour les fournisseurs d'accès Internet (FAI) et la communauté de l'Internet toute entière. Le présent article discute d'une méthode simple, efficace, et directe d'utilisation du filtrage du trafic entrant pour interdire les attaques de DoS qui utilisent de fausses adresses IP pour se propager de "derrière" un point d'agrégation d'un fournisseur d'accès Internet.

Table des Matières

1. Introduction
2. Fondements
3. Interdire le trafic falsifié
4. Autres capacités possibles pour les équipements de réseautage
5. Responsabilités
6. Résumé
7. Considérations pour la sécurité
8. Remerciements
9. Références
10. Adresse des auteurs
11. Déclaration complète de droits de reproduction

1. Introduction

Une résurgence d'attaques de déni de service [1] visant diverses cibles de l'Internet a lancé de nouveaux défis aux communautés des fournisseurs d'accès Internet (FAI) et de la sécurité des réseaux pour trouver des méthodes nouvelles et innovantes afin de contrer ces types d'attaques. Les difficultés pour atteindre ce but sont nombreuses ; certains outils simples existent déjà pour limiter l'efficacité et la portée de ces attaques, mais elles n'ont pas été largement mises en œuvre.

Cette méthode d'attaque est connue depuis un certain temps. Se défendre contre elle est cependant toujours un problème. Bill Cheswick est cité dans [2] comme disant qu'il a retiré à la dernière minute un chapitre de son livre "Pare-feu et sécurité Internet" [3] parce qu'il n'y a aucun moyen pour un administrateur de système qui subit une attaque de défendre efficacement le système. Il craignait que mentionner la méthode n'encourage son utilisation.

Bien que la méthode de filtrage discutée dans le présent document ne fasse absolument rien pour protéger contre les attaques qui inondent de trafic dont l'origine est dans des préfixes valides (des adresses IP) elle va interdire à un attaquant de l'intérieur du réseau générateur de lancer une attaque de cette nature en utilisant des adresses de source falsifiées qui ne se conforment pas aux règles de filtrage d'entrée. Tous les fournisseurs d'accès Internet sont instamment invités à mettre en œuvre le filtrage décrit dans ce document pour interdire aux attaquants d'utiliser des adresses de source falsifiées qui ne résident pas dans une gamme de préfixes légitimement annoncés. En d'autres termes, si un FAI agrège des annonces d'acheminement pour plusieurs réseaux en aval, un filtrage strict du trafic devrait être utilisé pour interdire le trafic qui affiche d'avoir été généré à l'extérieur de ces annonces agrégées.

Un avantage supplémentaire de la mise en œuvre de ce type de filtrage est qu'il permet à celui qui génère le trafic d'être

retracé jusqu'à sa vraie source, car l'attaquant devra utiliser une adresse de source valide, et légitimement accessible.

2. Fondements

Un diagramme simplifié du problème de l'inondation de SYN TCP est décrit ci-dessous :

```
                                                                                    204.69.207.0/24
    hôte <---------- routeur <---------- Internet <---------- routeur <---------- attaquant

                                          TCP/SYN
      <-------------------------------------------------------------------------------------------------
                                      Source: 192.168.0.4/32
    SYN/ACK
    pas de chemin
                                          TCP/SYN
        <-------------------------------------------------------------------------------------------------
                                      Source: 10.0.0.13/32
    SYN/ACK
    pas de chemin
                                          TCP/SYN
        <-------------------------------------------------------------------------------------------------
                                      Source: 172.16.0.2/32
    SYN/ACK
    pas de chemin
[etc.]
```

Supposons que :
- o "hôte" est la machine visée ;
- o l'attaquant réside au sein du préfixe "valide" 204.69.207.0/24 ;
- o l'attaquant lance l'attaque en utilisant des adresses dont la source change au hasard ; dans cet exemple, les adresses de source sont décrites comme venant de l'intérieur [4], qui ne sont pas généralement présentes dans les tableaux d'acheminement de l'Internet mondial, et donc inaccessibles. Cependant, tout préfixe inaccessible pourrait être utilisé pour perpétrer cette méthode d'attaque.

Il vaut aussi la peine de mentionner un cas dans lequel l'adresse de source est falsifiée pour paraître avoir été générée de l'intérieur d'un autre réseau légitime qui apparaît dans les tableaux d'acheminement mondiaux. Par exemple, un attaquant qui utilisé une adresse réseau valide pourrait accomplir des ravages en faisant apparaître l'attaque comme venant d'une organisation qui n'a pas, en fait, généré l'attaque et est complètement innocente. Dans de tels cas, l'administrateur d'un système attaqué peut être incité à filtrer tout le trafic venant de la source apparente de l'attaque. L'ajout d'un tel filtre résulterait alors en un déni de service à l'égard des systèmes d'extrémité légitimes et non hostiles. Dans ce cas, l'administrateur du système attaqué devient le complice involontaire de l'attaquant.

Pour compliquer un peu plus les choses, les attaques par inondation de SYN TCP vont résulter en paquets SYN-ACK qui sont envoyés à un ou de nombreux hôtes qui n'ont aucune implication dans l'attaque, mais qui en deviennent les victimes secondaires. Cela permet aux attaques de toucher deux ou plusieurs systèmes à la fois.

Des attaques similaires ont été tentées en utilisant l'inondation UDP et ICMP. La première attaque (l'inondation UDP) utilise des paquets falsifiés pour essayer de se connecter au service de comptabilité UDP au service d'écho UDP de l'autre site. Les administrateurs de systèmes ne devraient JAMAIS permettre à des paquets UDP destinés aux accès de diagnostic système provenant de l'extérieur de leur domaine administratif d'atteindre leur système. La seconde attaque (inondation ICMP) utilise une caractéristique insidieuse des mécanismes de réplication de la diffusion de sous réseau IP. Cette attaque s'appuie sur un routeur qui dessert un grand réseau de diffusion multi accès pour transposer ne adresse de diffusion IP (comme celle destinée à 10.255.255.255) en une trame de diffusion de couche 2 (pour ethernet, FF:FF:FF:FF:FF:FF). Le matériel NIC Ethernet (précisément le matériel de couche MAC) va seulement écouter des adresses choisies en fonctionnement normal. La seule adresse MAC que partagent tous les appareils en fonctionnement normal est celle du support de diffusion, ou FF:FF:FF:FF:FF:FF. Dans ce cas, un appareil va prendre le paquet et va envoyer une interruption pour traitement. Donc, une inondation de ces trames de diffusion va consommer toutes les ressources disponibles d'un système d'extrémité [9]. Il serait peut-être prudent que les administrateurs de système envisagent de s'assurer que leurs routeurs frontières ne permettent pas que les paquets de diffusion dirigés soient transmis par défaut à travers leurs routeurs.

Lorsque une attaque de SYN TCP est lancée en utilisant une adresse de source injoignable, l'hôte cible tente de réserver des ressources pour une réponse. L'attaquant change constamment la fausse adresse de source sur chaque nouveau paquet qu'il

envoie, épuisant ainsi des ressources supplémentaires chez l'hôte.

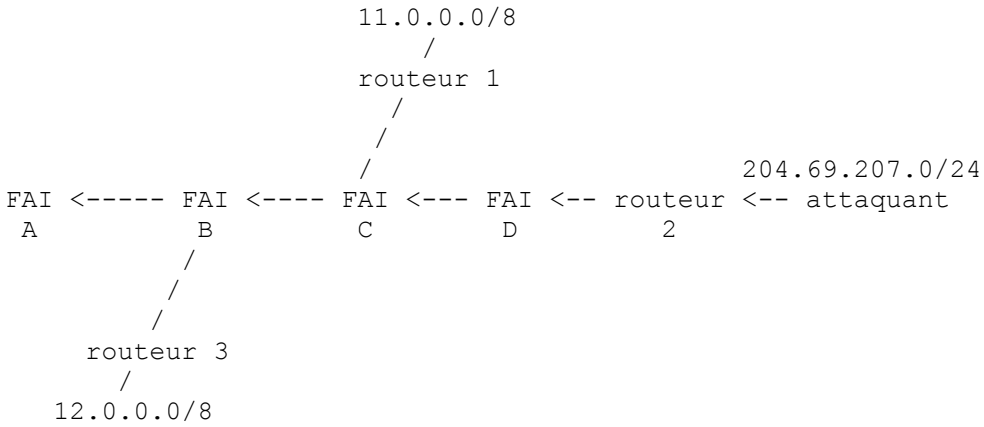
Autrement, si l'attaquant utilise l'adresse d'hôte valide de quelqu'un d'autre comme adresse de source, le système attaqué va envoyer un grand nombre de paquets SYN/ACK à ce qu'il croit être le générateur de la séquence d'établissement de la connexion. De cette façon, l'attaquant cause des dommages à deux systèmes : le système de destination cible, ainsi que le système qui utilise en fait l'adresse usurpée dans le système d'acheminement mondial.

Le résultat des deux méthodes d'attaque est une extrême dégradation des performances, ou pire, l défaillance du système.

En réponse à cette menace, la plupart des fabricants de systèmes d'exploitation ont modifié leur logiciel pour permettre aux serveurs visés de résister aux attaques avec des taux très élevés de tentative de connexion. C'est une partie bienvenue et nécessaire de la solution au problème. Il faudra du temps pour mettre en œuvre le filtrage entrant de façon généralisée et parfaitement efficace, mais les extensions aux systèmes d'exploitation peuvent être mises en œuvre rapidement. Cette combinaison devrait se montrer efficace contre l'usurpation d'adresse de source. Voir dans [1] les informations sur les mises à jour des fabricants et des logiciels.

3. Interdire le trafic falsifié

Les problèmes rencontrés avec ce type d'attaque sont nombreux, et impliquent des défauts dans les mises en œuvre des logiciels des hôtes, dans les méthodologies d'acheminement, et dans les protocoles TCP/IP eux-mêmes. Cependant, en interdisant le trafic de transit généré dans un réseau vers l'aval pour des préfixes connus et annoncés intentionnellement, le problème de l'usurpation d'adresse de source peut être virtuellement éliminé dans ce scénario d'attaque.



Dans l'exemple ci-dessus, l'attaquant réside au 204.69.207.0/24, pour laquelle le FAI D fournit la connexité Internet. Un filtre de trafic entrant sur la liaison d'entrée du "routeur 2", qui fournit la connexité au réseau de l'attaquant, restreint le trafic pour ne permettre que le trafic originaire des adresses de source au sein du préfixe 204.69.207.0/24, et interdit à un attaquant d'utiliser des adresses de source "invalides" qui résident en-dehors de cette gamme de préfixe.

En d'autres termes, le filtre d'entrée "routeur 2" ci-dessus va vérifier :

SI l'adresse de source des paquets vient de l'intérieur de 204.69.207.0/24
ALORS transmettre comme prévu
SI l'adresse de source des paquets est n'importe quoi d'autre
ALORS refuser le paquet

Les administrateurs de réseau devraient enregistrer les informations sur les paquets qui sont abandonnés. Cela donne une base à la surveillance des activités suspectes.

4. Autres capacités possibles pour les équipements de réseautage

Des fonctions supplémentaires devraient être envisagées pour les futures mises en œuvre de plates-formes. On peut noter la suivante :

o La mise en œuvre du filtrage automatique sur les serveurs d'accès distant. Dans la plupart des cas, un usager qui fait le numéro d'un serveur d'accès est un usager individuel sur un seul micro ordinateur. La SEULE adresse IP de source

valide pour les paquets générés à partir de ce micro ordinateur est celle allouée par le FAI (de façon statique ou dynamique). Le serveur d'accès distant pourrait vérifier tout paquet entrant pour s'assurer que l'usager n'usurpe pas l'adresse de source sur les paquets qu'il génère. Évidemment, il faut aussi prendre des dispositions pour les cas où le consommateur se rattache légitimement à un réseau ou sous réseau distant via un routeur distant, mais cela peut certainement être mis en œuvre comme paramètre facultatif. On nous a rapporté que certains fabricants et certains FAI commencent déjà à mettre en œuvre cette capacité.

On avait envisagé de suggérer aussi que les routeurs valident l'adresse IP de source de l'envoyeur comme suggéré dans [8], mais cette méthodologie ne va pas bien fonctionner dans les réseaux réels d'aujourd'hui. La méthode suggérée est de regarder les adresses de source pour voir si le chemin de retour pour cette adresse va passer par la même interface que celle sur laquelle le paquet est arrivé. Avec le nombre de chemins asymétriques qu'il y a dans l'Internet, ce serait très problématique.

5. Responsabilités

Un filtrage de cette nature peut éventuellement casser certains types de services "particuliers". Il est dans l'intérêt des FAI qui offrent ces types de services particuliers de considérer cependant des méthodes de remplacement pour mettre en œuvre ces services pour éviter qu'ils soient affectés par le filtrage du trafic d'entrée.

IP mobile, tel que défini dans [6], est particulièrement affecté par le filtrage du trafic d'entrée. Comme il est spécifié, le trafic vers le nœud mobile est tunnelé, mais le trafic provenant du nœud mobile n'est pas tunnelé. Il en résulte que les paquets qui proviennent du ou des nœuds mobiles ont des adresses de source qui ne correspondent pas au réseau où la station est rattachée. Pour s'accommoder du filtrage à l'entrée et autres soucis, le groupe de travail Mobile IP a développé une méthodologie pour les "tunnels inverses", spécifiée dans [7]. Elle donne une méthode pour que les données transmises par le nœud mobile soient tunnelées à l'agent de rattachement avant transmission à l'Internet. Il y a des avantages supplémentaires au schéma de tunnelage inverse, y compris un meilleur traitement du trafic en diffusion groupée. Ceux qui mettent en œuvre des systèmes IP mobile sont encouragés à mettre en œuvre cette méthode de tunnelage inverse.

Comme mentionné précédemment, alors que le filtrage du trafic entrant réduit de façon drastique le succès de l'usurpation d'adresse de source, il n'empêche pas une attaque qui utilise une fausse adresse de source d'un autre hôte de l'intérieur de la gamme permise des préfixes filtrés. Il assure bien, cependant, que lorsque une attaque de cette nature survient, un administrateur de réseau peut être sûr que l'attaque est en fait générée de l'intérieur des préfixes connus qui sont annoncés. Cela simplifie le traçage du coupable, et au pire, l'administrateur peut bloquer une gamme d'adresses de source jusqu'à la solution du problème.

Si le filtrage des entrées est utilisé dans un environnement où DHCP ou BOOTP sont utilisés, l'administrateur de réseau serait bien avisé de s'assurer que les paquets qui ont une adresse de source de 0.0.0.0 et une destination de 255.255.255.255 sont autorisés à atteindre l'agent de relais dans les routeurs lorsque c'est approprié. La portée de la réplication de diffusion dirigée devrait être cependant contrôlée, et non transmise arbitrairement.

6. Résumé

Le filtrage du trafic entrant à la périphérie des réseaux connectés à l'Internet va réduire l'efficacité des attaques de déni de service fondées sur l'usurpation d'adresse de source. Les fournisseurs et administrateurs de services réseau ont déjà commencé à mettre en œuvre ce type de filtrage sur les routeurs périphériques, et il est recommandé que tous les fournisseurs de service le fassent aussi aussitôt que possible. En plus d'aider la communauté globale de l'Internet à vaincre cette méthode d'attaque, il peut aussi aider les fournisseurs de service à localiser la source de l'attaque si les fournisseurs de services peuvent démontrer catégoriquement que leur réseau a déjà en place le filtrage entrée sur les liaisons terminales.

Les administrateurs de réseaux d'entreprises devraient mettre en œuvre le filtrage pour s'assurer que leurs réseaux d'entreprise ne sont pas la source de ces problèmes. Bien sûr, le filtrage pourrait être utilisé au sein d'une organisation pour garantir que les utilisateurs ne causent pas de problèmes en rattachant de façon inappropriée des systèmes aux mauvais réseaux.

Le filtrage pourrait aussi, en pratique, empêcher des employés mécontents de lancer des attaques anonymes.

Il est de la responsabilité de tous les administrateurs de réseau de s'assurer qu'ils ne deviennent pas la source involontaires d'attaques de cette nature.

7. Considérations pour la sécurité

L'intention principale du présent document est d'augmenter de façon inhérente la conscience et les pratiques de sécurité de la communauté de l'Internet dans son ensemble, car plus les fournisseurs d'accès Internet et les administrateurs de réseau d'entreprise mettront en œuvre le filtrage d'entrées, plus se réduira l'opportunité pour des attaquants d'utiliser de fausses adresses de source comme méthode d'attaque. Le traçage de la source d'une attaque est simplifié lorsque la source a une forte probabilité d'être "valide". En réduisant le nombre et la fréquence des attaques dans l'Internet global, il y aura plus de ressources pour traquer les attaques qui finissent par subsister.

8. Remerciements

Il revient au groupe des opérateurs de réseau Nord Américains (NANOG) [5] une mention particulière pour sa discussion ouverte de ces questions et pour avoir activement recherché les solutions possibles. Nos remerciements à Justin Newton [Priori Networks] et à Steve Bielagus [IronBridge Networks] pou leurs commentaires et contributions.

9. Références

[1] CERT Advisory CA-96.21 ; "TCP SYN Flooding and IP Spoofing Attacks" ; 24 september 1996.

[2] B. Ziegler, "Hacker Tangles Panix Web Site", Wall Street Journal, 12 septembre 1996.

[3] "Firewalls and Internet Security: Repelling the Wily Hacker" ; William R. Cheswick and Steven M. Bellovin, Addison-Wesley Publishing Company, 1994 ; ISBN 0-201-63357-4.

[4] Y. Rekhter et autres, "Allocation d'adresse pour les internets privés", RFC1918, BCP 5, février 1996.

[5] The North American Network Operators Group ; http://www.nanog.org .

[6] C. Perkins, éd., "Prise en charge de la mobilité sur IP", RFC2002, octobre 1996. (*Obsolète, voir* RFC3220) *(P.S.)*

[7] G. Montenegro, éd., "Tunnelage inverse pour IP mobile", RFC2344, mai 1998. *Obsolète, voir* RFC3024) *(P.S.)*

[8] F. Baker, "Exigences pour les routeurs IP version 4", RFC1812, juin 1995. *(Mise à jour par la RFC 2644)*

[9] Merci à : Craig Huegen ; voir : http://www.quadrunner.com/~chuegen/smurf.txt .

10. Adresse des auteurs

Paul Ferguson
Cisco Systems, Inc.
13625 Dulles Technology Dr.
Herndon, Virginia 20170 USA
mél : ferguson@cisco.com

Daniel Senie
Amaranth Networks Inc.
324 Still River Road
Bolton, MA 01740 USA
mél : dts@senie.com

11. Déclaration complète de droits de reproduction

Remerciement

Le finacement de la fonction d'éditeur des RFC est actuellement fourni par la Internet Society.