Infoblox
CONTROL YOUR NETWORK

LIVRE BLANC

Vaincre les attaques DoS/DDoS en temps réel

Résumé

La vulnérabilité des serveurs DNS des fournisseurs de services vis-à-vis des attaques DoS/DDoS est bien réelle et s'intensifie à un rythme effréné, mettant ainsi en péril l'expérience utilisateur des clients ainsi que la réputation des fournisseurs de services. Les techniques actuelles visent à arrêter les attaques en dotant le site du fournisseur de matériel supplémentaire ou en identifiant le coupable caché dans le logiciel malveillant sur le site du client. Cependant, ces deux méthodes sont onéreuses et ne permettent de résoudre le problème que partiellement. La nouvelle approche consiste à intégrer la protection contre les attaques DoS/DDoS directement dans un serveur cache DNS à haute fiabilité et à contrecarrer l'attaque en temps réel au moment où elle pénètre dans l'infrastructure, la désamorçant avant même qu'elle n'affecte les performances ou le service.

DNS : une vulnérabilité majeure des fournisseurs de services

Le serveur DNS est l'un des composants les plus critiques et les plus vulnérables de l'infrastructure. Il est la cible des attaques par déni de service et déni de service distribué (DoS/DDoS) dont sont victimes les fournisseurs de services. Les fournisseurs d'accès, les opérateurs de téléphonie et les fournisseurs de téléphonie mobile risquent à tout moment de subir des interruptions de service en raison d'une panne de leurs serveurs DNS sollicités par des requêtes malveillantes et d'autres attaques similaires. Le paysage actuel des menaces continue de s'étendre à mesure que ces attaques ont un impact sur les budgets, les réputations, les consommateurs et les clients.

Le coût d'une attaque se chiffre en millions de dollars, avec des actes malveillants allant de menaces criminelles, comme l'extorsion de fonds, aux attaques entraînant une perte des revenus directement liés à la connectivité, aux services Internet et aux sites Web. Des attaques efficaces se traduisent également par des pertes supplémentaires non pécuniaires, comme le mécontentement ou la perte des clients et, dans des cas plus extrêmes, finissent par anéantir totalement la réputation et l'image de la marque.

Dans le but de fidéliser leur clientèle et d'assurer leur croissance, les fournisseurs d'accès tendent à moderniser leur infrastructure afin de prendre en charge la demande croissante en bande passante, due principalement aux smartphones, aux médias sociaux et à la multitude d'appareils mobiles personnels. En procédant de la sorte, ils perdent de vue une menace bien plus importante pour la satisfaction du client : la connectivité. L'augmentation de la bande passante sont nécessaires mais ne constituent qu'une partie de l'avantage concurrentiel du fournisseur de service. De plus en plus exigeants, les consommateurs et les entreprises d'aujourd'hui ne tolèrent tout simplement aucune interruption des services. Les fournisseurs d'accès doivent protéger leur infrastructure Internet des attaques DoS/DDoS de plus en plus fréquentes et virulentes afin de garantir une connectivité permanente et de préserver l'expérience Internet de leurs clients, et par là même leur propre réputation.

Attaques DoS/DDoS : un court passé mais déjà de lourdes conséquences

Les attaques DoS/DDoS ne font parler d'elles que depuis peu. Mais en un peu moins d'une décennie, elles constituent une véritable menace mondiale qui ne semble montrer aucun signe d'affaiblissement ou d'atténuation. En fait, les attaques DoS/DDoS semblent s'amplifier à la fois en nombre et en virulence. Un rapport historique établi par Arbor Networks en 2008 avait anticipé avec beaucoup de clairvoyance l'explosion actuelle des attaques DoS/DDoS, en constatant que la taille des attaques DDoS (en gigabits) avait pratiquement doublé au cours de l'année 2007. Selon Arbor Networks, cette tendance n'a cessé de se confirmer depuis le début du siècle, comme le montre la figure 1.

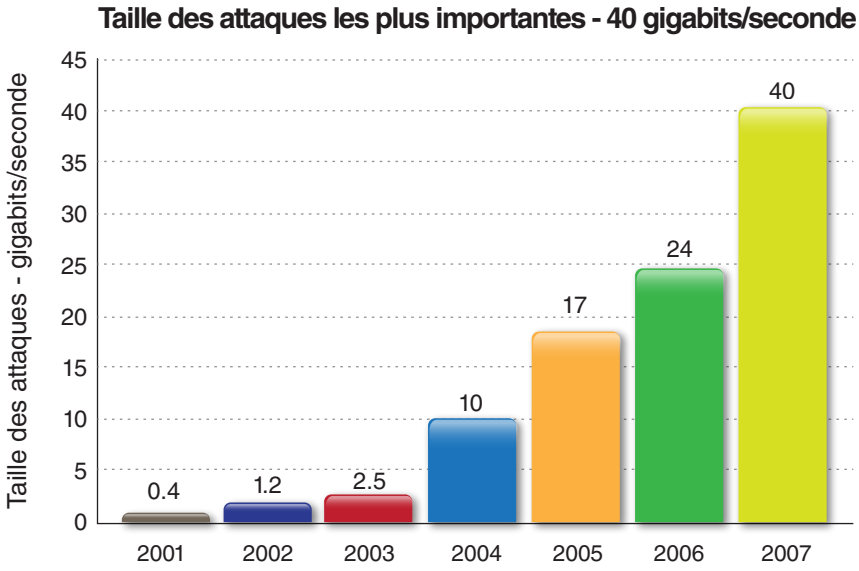

Figure 1. Les attaques DDoS se multiplient à grande vitesse depuis 2001 et ne montraient aucun signe d'affaiblissement en 2008. *(Crédit : Arbor Networks)*

Les études actuelles montrent que cette tendance antérieure n'a cessé de se confirmer. Le rapport intitulé « Quarterly Global DDoS Attack Report », publié en juillet 2012 par Prolexic Technologies, montrait que les attaques DDoS avaient augmenté de 10 % en seulement trois mois depuis le premier trimestre 2012, avec une augmentation de 8 % des attaques contre l'infrastructure des couches 3 et 4, et que la durée moyenne d'une attaque était à présent de 17 heures, la Chine étant le principal pays d'origine des attaques DDoS. Comparé au second trimestre 2011, le rapport constatait une augmentation de 50 % du nombre total d'attaques DDoS en une seule année, avec une augmentation de 63 % du volume de paquets par seconde au cours de la même période.

De plus, en juillet 2012, le rapport semestriel « DDoS Prevention Appliances » du cabinet Infonetics Research prévoyait en 2012 une croissance de 24 % du marché de la prévention des attaques DDoS par rapport à l'année 2011. Selon Infonetics, le marché de la prévention DDoS, tous segments confondus (centre de données, opérateurs, mobiles et gouvernements), atteindrait 420 millions de dollars d'ici 2016, les réseaux mobiles enregistrant, avec 30 %, la croissance la plus forte au cours de cette période.

En conclusion, loin de disparaître, le problème tend à s'aggraver.

Réponse lente aux attaques les plus courantes

Un grand nombre de fournisseurs d'accès ne détectent pas une attaque DoS/DDoS dès le début. Du fait de leur nature cumulative et ingrate, les attaques DoS/DDoS passent inaperçues tant qu'elles n'atteignent pas leur paroxysme et que les dégâts ne sont pas encore visibles. Il y a généralement suspicion d'une attaque lorsque les performances chutent ou que les réclamations des clients s'accumulent. Et c'est seulement après l'analyse des journaux des serveurs DNS par l'ingénieur, parfois plusieurs jours de travail, que l'attaque est confirmée. Le temps requis pour obtenir ces informations retarde souvent de 4 à 6 jours la mise en place d'une mesure corrective et l'interruption de service s'est souvent généralisée.

La plupart des fournisseurs d'accès exécutent leur DNS sur du matériel Hewlett-Packard ou Sun et utilisent principalement des logiciels DNS BIND libres. Ils ont pratiquement tous recours à plusieurs serveurs DNS et certains utilisent même un nombre élevé de serveurs DNS dans leurs centres de données. Ces configurations sont particulièrement vulnérables à trois des types d'attaques DoS/DDoS les plus fréquentes :

- Attaques par saturation TCP SYN
- Attaques par saturation UDP
- Usurpation d'adresse source/attaques LAND

Il existe de nombreuses autres façons de compromettre un serveur DNS et de nouvelles méthodes sont perpétuellement mises au point dans le monde obscur des ordinateurs zombies. Néanmoins, ces trois attaquent sont celles qui arrivent le plus souvent et partagent des caractéristiques avec bien d'autres types d'attaques.

Attaques par saturation TCP SYN : Bonjour... Pas de réponse

Les attaques par saturation TCP SYN sont des attaques DoS qui tentent de saturer le serveur DNS avec de nouvelles demandes de connexion TCP. Un client initie généralement une connexion TCP par le biais de trois messages d'établissement de liaison :

- Le client demande une connexion en envoyant un message SYN (synchroniser) au serveur.
- Le serveur accuse réception de la demande en renvoyant un message SYN-ACK au client.
- Le client répond en renvoyant à son tour un message ACK, ce qui a pour effet d'établir la connexion.

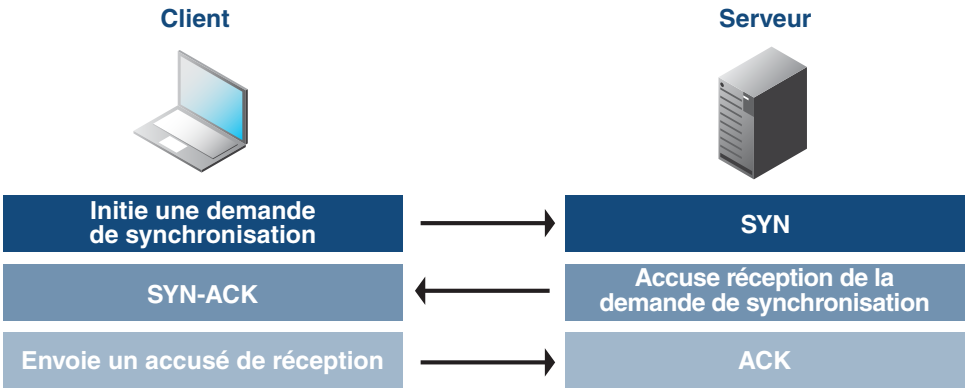

Figure 2 : Connexion TCP normale

Ce triple échange est à la base de toute connexion établie au moyen du protocole TCP (Transmission Control Protocol).

Une attaque par saturation TCP SYN consiste à envoyer des demandes SYN au serveur et à ne pas répondre au serveur avec le code ACK attendu. Le client malveillant peut tout simplement ne pas envoyer le message ACK final attendu ou il peut usurper l'adresse IP source dans le message SYN afin que le serveur envoie le message SYN-ACK à une adresse IP falsifiée. Le client correspondant à l'adresse IP falsifiée ne renvoie bien entendu pas le message ACK dans la mesure où il « sait » qu'il n'a jamais envoyé de message SYN. Ainsi, il existe plusieurs connexions « en suspens » non ouvertes sur le serveur qui attendent l'accusé de réception du client. Tandis que le serveur attend les messages ACK (ce qui entraîne une congestion du réseau ou des retards), un nombre croissant de connexions semi-ouvertes consomment les ressources sur le serveur jusqu'à ce qu'aucune nouvelle connexion ne puisse être établie. Cela se traduit alors par un déni de service pour le trafic légitime et finit par paralyser totalement le serveur.

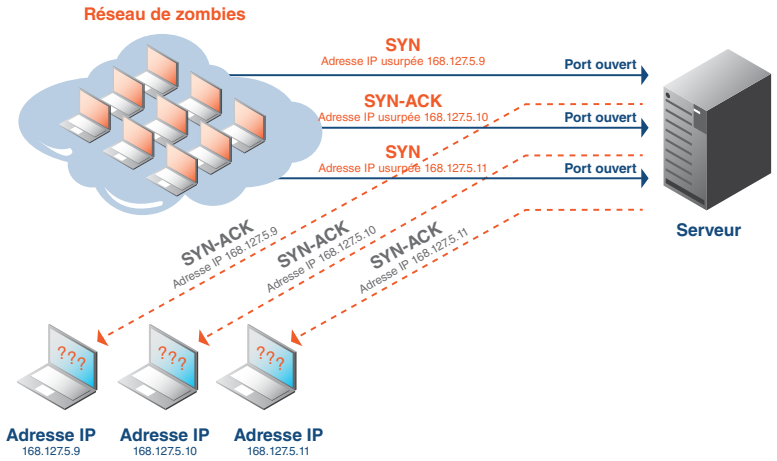

Figure 3 : Attaque par saturation TCP SYN

Attaque par saturation UDP : un port perdu dans un raz-de-marée de paquets

Une attaque par saturation UDP (User Diagram Protocol) peut être initiée en envoyant un nombre important de paquets UDP à des ports aléatoires sur l'hôte ciblé. L'hôte attaqué vérifie le trafic provenant de l'application qui écoute ce port. Lorsqu'il voit qu'aucune application n'écoute ce port, il répond en envoyant un message ICMP Destination Unreachable.

Ainsi, lorsqu'un volume important de paquets UDP est envoyé, le système attaqué renvoie un grand nombre de paquets ICMP et finit par devenir indisponible pour d'autres clients. L'attaquant peut également falsifier l'adresse IP des paquets UDP afin de s'assurer que les nombreux paquets ICMP envoyés en retour ne l'atteignent pas et de garder anonyme son emplacement réseau.

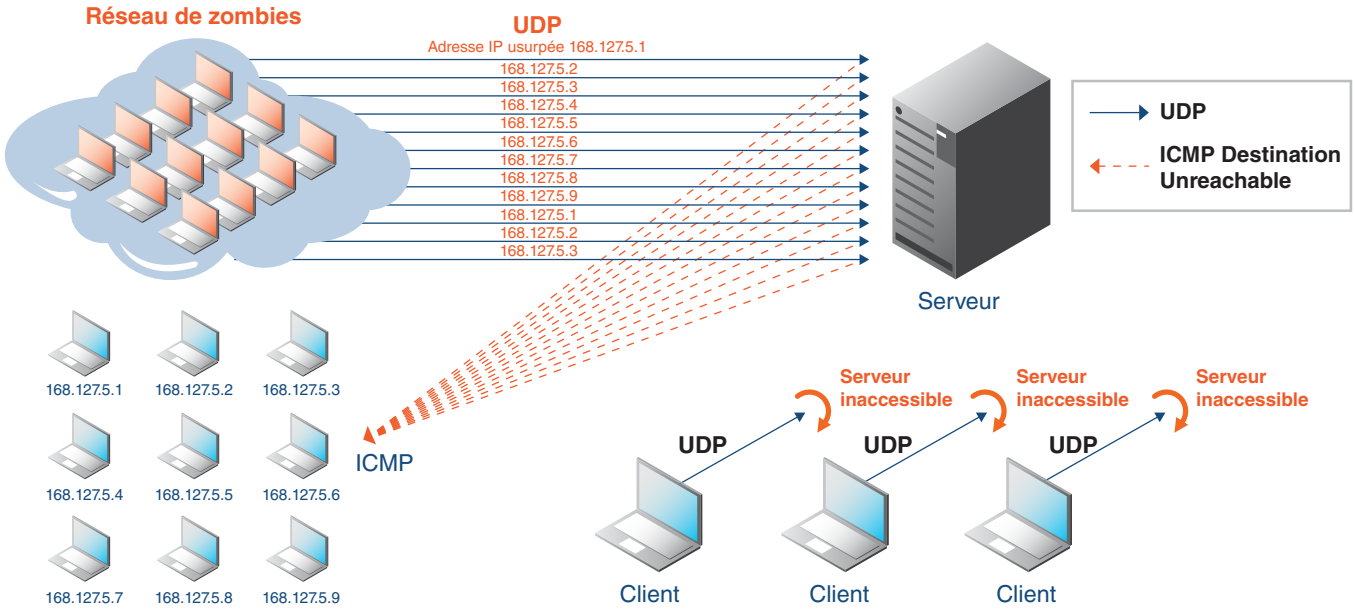

Figure 4 : Attaque par saturation UDP

Usurpation d'adresse source/Attaques LAND : des blessures auto-infligées

Une attaque LAND (Local Area Network Denial) est une forme courante d'attaque DoS où un paquet usurpé empoisonné est envoyé à un ordinateur, ce qui a pour effet de le bloquer. L'attaque consiste à envoyer un paquet TCP SYN usurpé (pour initier la connexion) vers un port ouvert en utilisant l'adresse IP de l'hôte cible à la fois comme source et comme destination. En cas d'attaque LAND, l'ordinateur victime se répond à lui-même continuellement.

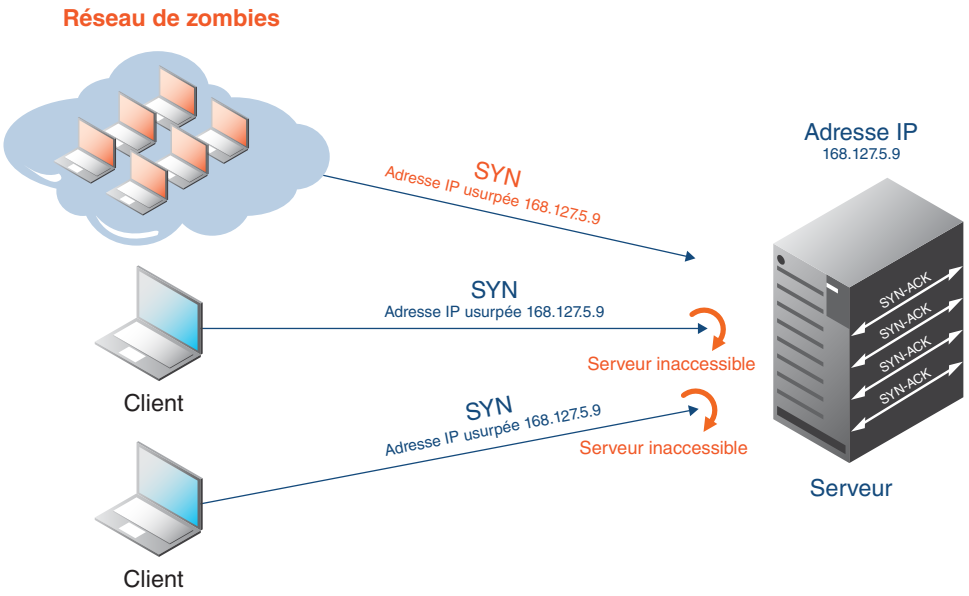

Figure 5 : Attaque LAND

Limites des méthodes disponibles

Jusqu'à présent, pour lutter contre de telles attaques et d'autres types d'attaques DoS/DDoS, deux types de méthodes distinctes étaient employées : contrecarrer l'attaque au niveau du fournisseur ou l'arrêter au niveau du client. Ces deux méthodes n'ont cependant pas permis d'obtenir des résultats probants et constants, et sont toutes deux très onéreuses.

L'ajout d'un équilibreur de charge sur le site du fournisseur pour répartir la charge entre plusieurs serveurs est une méthode qui est utilisée depuis un certain temps, mais qui finit par s'avérer inefficace. Les équilibreurs de charge peuvent à leur tour être surchargés et la vulnérabilité des serveurs est alors décuplée.

L'utilisation au niveau du fournisseur de plusieurs clusters de serveurs plus petits est devenue une pratique courante, mais qui présente rapidement des failles lorsque le nombre d'attaques dépasse la capacité des clusters. De plus, les clusters de petits serveurs encombrent le centre de données, occupent énormément d'espace rack, augmentent les coûts d'électricité et de climatisation et nécessitent un personnel important pour le déploiement continuel des correctifs et des mises à jour. Cette méthode atténue la vulnérabilité du fournisseur plutôt que de le protéger et a un coût qui est loin d'être négligeable.

En revanche, la protection peut être étendue directement aux clients en identifiant les utilisateurs dont l'équipement est infecté par le logiciel malveillant. Les utilisateurs infectés sont identifiés lorsqu'ils communiquent avec des sites Web et des domaines DNS malveillants connus abritant les contrôleurs d'ordinateurs zombies à l'origine des dégâts. Une fois identifié, le serveur DNS du fournisseur met fin à la communication avec le contrôleur d'ordinateurs zombies. Le processus d'identification des utilisateurs infectés peut, par ailleurs, recourir à une analyse de données et à une génération de rapports hors site et donc entraîner des risques considérables pour la sécurité. De plus, ce type de pratique n'est pas légal dans certains pays. Il existe également des risques en matière de satisfaction de la clientèle et de protection de la vie privée dans la mesure où les clients doivent être surveillés de très près, parfois même de manière invasive.

Cette méthode présente d'autres lacunes majeures. Pour commencer, les sites Web et les domaines DNS malveillants doivent être déjà connus. Or, peu sont connus car de nouveaux sites malveillants se développent tous les jours. De plus, cela implique de gérer et de mettre à jour de nombreuses listes noires. Enfin, chaque client doit être surveillé de manière indépendante. Outre le fait que cette technique est laborieuse, les sources de l'attaque ne peuvent être identifiées que si les délinquants sont connus à l'avance et si l'attaque est en cours depuis un certain temps.

Infrastructure de cache DNS à haute capacité

Une nouvelle façon d'appréhender les attaques DoS/DDoS consiste à intégrer l'antidote directement dans un boîtier appliance DNS performant et hautement redondant. Plutôt que d'essayer d'arrêter les attaques lorsqu'elles atteignent le client (ce qui s'est avéré très difficile à faire), cette méthode les intercepte lorsqu'elles pénètrent dans l'infrastructure du fournisseur, au niveau du serveur DNS. Au lieu d'ajouter d'autres serveurs génériques et des équilibreurs de charge (un effort inefficace et coûteux), cette solution installe une infrastructure DNS d'une grande fiabilité dédiée à cette tâche.

Une telle approche requiert un serveur DNS à haute capacité qui neutralise la plupart des attaques DoS/DDoS en se mettant à leur niveau, c'est-à-dire en utilisant la puissance nécessaire pour gérer l'augmentation de la charge. Cette méthode basée sur l'utilisation d'un boîtier peut également recourir à des algorithmes spéciaux pour reconnaître les attaques les plus courantes et renforcer l'infrastructure en conséquence. Afin de maintenir la continuité du service en cas de charge extrême, il est primordial que ces serveurs DNS ne s'arrêtent pas lorsqu'ils atteignent un point de saturation. Lorsque la charge des requêtes DNS dépasse les limites spécifiées, ce serveur DNS haute performance doit rester constant, avec une faible latence du cache DNS. Cette capacité nécessite généralement une mise en œuvre d'équipements utilisant des technologies de filtrage des paquets et de délestage de la charge évoluées qui ne peuvent de toute évidence être mises en œuvre en mode haut débit sur des serveurs logiciels.

Le boîtier de mise en cache DNS Infoblox IB-4030 : les ordinateurs zombies n'ont qu'à bien se tenir !

Infoblox a créé une toute nouvelle solution de cache DNS conçue spécialement pour répondre aux besoins des gros fournisseurs d'accès, des opérateurs de téléphonie et des fournisseurs de services mobiles. Le boîtier IB-4030 prend en charge un million de requêtes DNS par seconde, ce qui suffit largement à faire face à la plupart des attaques DoS/DDoS uniquement par la puissance de traitement. Le boîtier IB-4030 offre également une protection intégrée contre tous les types d'attaques DoS/DDoS décrits ci-dessus.

Cette technique permet aux fournisseurs d'accès et aux opérateurs de téléphonie mobile de faire évoluer leur infrastructure DNS afin de prendre en charge des milliards de requêtes par seconde. Cela fournit une extensibilité transactionnelle élevée dans des conditions de charges de trafic extrêmes, tout en permettant une plus grande extensibilité de la main d'œuvre grâce à la technologie Infoblox GridTM. Avec la solution Grid, les fournisseurs peuvent déployer à grande échelle une infrastructure DNS hautement distribuée mais gérable à distance, sans pour autant devoir recourir à un personnel supplémentaire pour les tâches d'administration et d'assistance.

Intrinsèquement fiable, sans accès root et avec des logiciels Infoblox préintégrés, le serveur Infoblox IB-4030 est un boîtier dédié performant qui intègre des alimentations CA et CC redondantes, des ventilateurs et des lecteurs de disques durs. Les fonctions de protection contre les attaques DoS/DDoS sont entièrement intégrées et automatisées et ne nécessitent ni installation de logiciel ni configuration manuelle supplémentaire, éliminant par là-même les erreurs de configuration manuelle. Le boîtier IB-4030 prend automatiquement en charge le protocole DNSSEC pour lutter contre les attaques de type Kaminsky qui polluent le cache DNS pour forcer la redirection vers des sites non autorisés ou malveillants.

Le boîtier IB-4030 intègre des contrôles d'accès basés sur les rôles afin de garantir que les utilisateurs/rôles accèdent uniquement aux fonctions pour lesquelles ils disposent des autorisations requises. De plus, toutes les modifications apportées aux paramètres du boîtier par les utilisateurs sont horodatées et consignées dans les journaux d'audit du boîtier.

La vulnérabilité laisse la place à la protection dans l'infrastructure DNS

L'augmentation constante des attaques DoS/DDoS sur l'infrastructure DNS des fournisseurs de services ne donne aucun signe de ralentissement. Au contraire, les attaques DoS/DDoS sont en passe de devenir le plus grand fléau de l'industrie. À mesure que les pirates redoublent d'ingéniosité et de machiavélisme, les moyens mis en œuvre pour combattre leurs attaques doivent également évoluer afin de conserver une longueur d'avance sur ces menaces. Du fait même de la nature de la connectivité, il n'est pas possible d'éviter tout simplement les attaques DoS/DDoS car le trafic reste du trafic tant que sa nature malveillante n'est pas détectée. Il est alors plus judicieux de contrecarrer, vaincre ou faire échouer ces attaques. Une solution offrant un cache DNS hautement fiable, comme le boîtier Infoblox IB-4030, est l'arme la plus moderne et la plus puissante dont on dispose aujourd'hui contre ce type d'attaque.

Découvrez les solutions Infoblox destinées aux fournisseurs de services :

Cache DNS à haute fiabilité avec une protection DoS/DDoS
www.infoblox.com/en/solutions/service-provider/high-performance-dns-caching.html

Résumé de la solution : Mise en cache DNS à haute fiabilité pour les fournisseurs de service
www.infoblox.com/content/dam/infoblox/documents/solution-notes/infoblox-note-dns-for-service-providers.pdf

Fiche produit : Boîtier Infoblox-4030 pour mise en cache DNS
www.infoblox.com/content/dam/infoblox/documents/datasheets/infoblox-datasheet-infoblox-4030.pdf

Solutions pour les fournisseurs de services filaires, mobiles et cloud
www.infoblox.com/sp

SIÈGE SOCIAL :

3111 Coronado Drive

Santa Clara

California 95054

USA

+1.408.986.4000

+1.866.463.6256

(sans frais pour les États-Unis et le Canada)

info@infoblox.com

www.infoblox.com

SIÈGE FRANCE :

Regus Business Center

168 avenue charles de Gaulle

92522 Neuilly sur Seine

France

+33.1.70.37.53.05

emea-seur@infoblox.com

www.infoblox.fr