

Avis d'expert

Déni de service : le load balancer, premier rempart contre l'attaque

Par Baptiste Assmann, Chef de Produit, Exceliance

Conçu pour la répartition de charge et la haute disponibilité, un load balancer applicatif a de nombreux autres atouts. Bien utilisées, certaines de ces fonctionnalités peuvent d'avérer très utiles en matière de sécurité. En particulier en cas d'attaque en déni de service.

Les attaques en déni de service de nouveau à la mode

Les attaques en déni de service (DoS, denial of service ou DDos, Distributed Denial of Service), qui ont pour objet de saturer une ressource afin de rendre un site web ou un service indisponible, reviennent -malheureusement- sur le devant de la scène... Dernier exemple en date : celles des Anonymous, qui ont réussi à faire tomber le site du FBI et de l'Élysée, après l'annonce de la fermeture du site Megaupload. Œil pour œil...

Si les attaques en DoS pour des raisons idéologiques ou politiques sont très fortement médiatisées, elles peuvent avoir d'autres objectifs : le chantage, la dévalorisation d'une entreprise ou encore le leurre, pour détourner l'attention de l'équipe sécurité afin de procéder à des vols de données (exploitation de failles de sécurité) ou détourner les visiteurs en prétextant une panne (phishing).

Le point sur les principales techniques utilisées et le rôle qu'un load balancer applicatif peut jouer dans un dispositif de protection contre ces attaques...

Absorption du trafic vs saturation des connexions des serveurs d'applications

De Java à Apache en passant par Websphere et .Net, tous les serveurs d'applications ont un point commun : le nombre limité de leurs connexions concurrentes. Résultat : pour les pirates, il est assez facile de les faire tomber, sans même disposer de ressources très importantes. L'outil Slowloris, créé en 2009, s'en est d'ailleurs fait une spécialité. Son principe : ouvrir et laisser ouvertes de multiples connexions pour engorger le serveur, et même l'empêcher d'en ouvrir de nouvelles.

Une parade consiste à appliquer des *timeout* sur les serveurs, c'est-à-dire à couper la connexion après un temps d'inactivité trop long. Cette technique est efficace, mais de façon très relative : l'attaque par saturation des connexions est en effet capable d'envoyer régulièrement des « bouts de requête » afin de faire croire au serveur que la connexion est toujours active. Auquel cas, le serveur la maintient ouverte...

Un répartiteur de charge applicatif, placé en amont des serveurs d'application, est tout d'abord capable de supporter un nombre de connexions concurrentes bien plus élevé que ces serveurs et de jouer un rôle de tampon devant eux. En outre, grâce à ses fonctions de filtrage des requêtes, il peut repérer les « fausses » activités, rejeter les requêtes non complètes et/ou ne laisser passer que le trafic correspondant aux applications critiques.

Filtrage des requêtes vs saturation des ressources serveurs

Autre technique utilisée pour les attaques en DoS : l'envoi de requêtes très consommatrices en ressources pour saturer les serveurs. C'est le cas, par exemple, de la recherche d'un mot clé banal sur l'ensemble d'un site. Or, un simple script permet d'automatiser ce genre de requêtes...

Grâce à ses fonctions d'analyse protocolaire et de *content switching*, le load balancer est capable de diriger les flux sur différents serveurs en fonction de leur nature et du contenu demandé. Ces fonctionnalités peuvent être paramétrées pour mettre en file d'attente les requêtes les plus chronophages et les moins critiques, ou encore rejeter les requêtes http mal formées ou qui font appel à des éléments inexistantes.

En s'interposant entre les attaquants et les serveurs, le répartiteur peut ainsi bloquer les requêtes indésirables tout en maintenant le trafic sur les applications critiques.

Les moyens et du temps pour réagir

Le load balancer permet également de gagner du temps, grâce à la possibilité qu'il offre d'ajouter des serveurs à la volée : en cas d'attaque, les équipes informatiques peuvent augmenter rapidement les capacités globales de l'architecture, quitte à réintégrer d'anciens serveurs. En outre, il est aussi capable de simuler la réussite de l'attaque en renvoyant un message d'indisponibilité de service à l'attaquant.

Toutefois, un répartiteur ne pourra pas contenir à lui seul une attaque visant à saturer totalement le réseau. Ces attaques restent encore rares car elles nécessitent soit un dispositif soit des moyens financiers importants pour exploiter un très grand nombre de machines. Dans ce type d'attaque, seule une architecture distribuée sur plusieurs sites et/ou le recours aux solutions de continuité de service proposées par le fournisseur d'accès ou un tiers spécialisé pourront permettre de se protéger.

En conclusion, si les fonctions d'un load balancer peuvent être très utiles en cas d'attaque en déni de service, seul le travail des équipes humaines maintiendra cette efficacité dans le temps, en commençant par la surveillance des logs de l'outil pour affiner les paramétrages et les filtrages au fur et à mesure de l'évolution de la menace...

A propos d'Exceliance

Exceliance propose une gamme complète de répartiteurs de charge, pour améliorer les performances, garantir la qualité de service et assurer la disponibilité des applications et services Web d'entreprise.

Combinant performance de traitement, fiabilité et richesse fonctionnelle, elles sont proposées sous forme d'appliance matérielle rackable ou de machine virtuelle optimisée pour chaque hyperviseur, à des prix plus abordables que les autres solutions du marché.

Basée à Jouy-en-Josas (78), Exceliance compte aujourd'hui plus d'une centaine de clients dans les secteurs de la banque, de la grande distribution, de l'énergie, du e-commerce ou du secteur public. Ses solutions sont également installées chez de nombreux hébergeurs.

www.exceliance.fr

Contacts presse

Anjuna
Elodie Cassar
elodie.cassar@anjuna.fr
Tel : +33 9 65 24 97 58
GSM : +33 6 80 53 82 94

Exceliance
Christophe Pouillet
cpouillet@exceliance.fr
Tél.: +33 1 30 67 60 74