Mise à disposition rapide et sécurisée des applications

Assurer la haute disponibilité et la sécurité accrue des applications vitales pour l'entreprise est un défi de taille. Les passerelles de services applicatifs unifiées (UASGs) y contribuent sensiblement – qu'il s'agisse de fournisseurs d'accès internet, d'opérateurs, de grandes entreprises ou de PME. Walter Benz

Il y a encore quelques années, les répartiteurs de charge (Server Load Balancer, SLB) constituaient la «référence ultime» pour le déploiement et l'accélération d'applications. En tant qu'interface entre utilisateurs et pool de serveurs, ils permettent d'optimiser la répartition de charge entre les différents serveurs, d'augmenter ainsi la disponibilité des applications et de minimiser le temps de latence. Les SLB ont rapidement été complété par les contrôleurs d'accélération applicative (Application Delivery Controller ADC). Ces dispositifs permettent le traitement intelligent des applications au niveau des couches 4 à 7. Ils interviennent lorsqu'il s'agit de déployer rapidement des applications de manière optimale et sécurisée. Les ADC ont trouvé leur place dans les entreprises, chez les opérateurs et fournisseurs de cloud – aussi bien dans le centre de données que dans la passerelle du réseau.

Un code malveillant qui est déjà repoussé au niveau du périmètre ou en amont du pare-feu prévient toute charge et menace inutile de l'infrastructure informatique et de réseau interne. Source: iStock

Outre leurs fonctionnalités centrales, les ADC consolident divers éléments complémentaires dans un système, notamment l'équilibrage de charge de la banque de données, de même que la répartition de charge sur plusieurs pare-feu disponibles. Souvent, les ADC supportent aussi ladite «partition de livraison d'applications (ADP)». Cette dernière permet de mettre à la disposition de différents groupes d'utilisateurs diverses applications et services sur une seule plateforme avec séparation complète du réseau. La plateforme devient donc multi-clients.

Appliance physique ou virtuelle – les fournisseurs innovants tels que nF5 Networks, A10 Networks et autres proposent aujourd'hui des contrôleurs d'accélération applicative ultra-performants, dont la performance est généralement le fruit de la combinaison d'une architecture de système moderne, de composants matériels performants et d'un système d'exploitation optimisé. Pour satisfaire les exigences de haute performance, les fabricants ont de plus en plus recours à des plateformes exploitant pleinement l'accélération matérielle. Elles délèguent des fonctions gourmandes en ressources processeur à des FPGA ou ASIC dédiés et déchargent ainsi les CPU système.

La performance des appliances de pointe permet désormais une étape de développement supplémentaire: l'extension des ADC en UASG. Les «Unified Application Service Gateway» peuvent être simplement définis comme des ADC offrant des fonctions améliorées en termes de sécurité et de réseau. Parallèlement à l'évolution dans le domaine de la sécurité informatique, où les pare-feu classiques se sont mutés en passerelles de sécurité intégrées haute performance – les appliances UTM – les ADC «classiques» sont enrichies d'une diversité de fonctions. Leur objectif est d'implanter des fonctionnalités de sécurité capitales aussi près que possible du périmètre ou au point le plus éloigné de la passerelle de l'entreprise. En effet, un code malveillant qui est déjà repoussé au niveau du périmètre ou en amont du pare-feu prévient toute charge et menace inutile de l'infrastructure informatique et de réseau interne. Parmi les éléments de sécurité typiques qui soutiennent les UASG figurent le pare-feu à filtrage applicatif assurant la protection web et DNS, la défense contre les attaques DDoS et la gestion d'accès à l'application (AAM) ou la pré-authentification. Les UASG sont de plus en mesure d'exécuter des services mobilisant des ressources système substantielles comme par exemple le SSL, et donc de décharger le réseau interne dans ce domaine. La possibilité de migration d'IPv4 vers IPv6 revêt d'autre part une importance capitale.

Sécurité au niveau de la passerelle de l'entreprise

Les passerelles de services applicatifs unifiées (UASG) intègrent plusieurs fonctions de sécurité dans un système et permettent de maximiser la protection du périmètre. Parmi les principaux éléments figurent:

Les Web Application Firewall (WAF) et DNS Application Firewall

Les pare-feu à filtrage applicatif assurent la

Walter Benz
Product Manager
A10 Networks,
BOLL Engineering AG

protection des applications web contre les attaques via HTTP, sécurisent les failles de code et empêchent les pertes de données. Les UASG dotées d'une fonction WAF permettent désormais d'identifier et de se défendre contre les attaques sur le serveur web. Elles analysent en outre le débit de données au niveau de l'application et préviennent le transfert de données indésirables. Les pare-feux applicatifs DNS sécurisent les infrastructures DNS. Il s'agit de contrer efficacement les attaques, même massives, sans surcharger les serveurs DNS. Les pare-feu d'applications DNS permettent d'optimiser les ressources existantes ou de minimiser les coûts de serveurs.

Application Access Management (AAM) pour l'authentification

Dans une UASG, les fonctionnalités d'authentification intégrées assurent qu'aucun trafic de données indésirable ou non authentifié ne parvienne aux serveurs back-end. Les modules AAM permettent de protéger les infrastructures des centres de calculs et d'augmenter l'efficacité des serveurs. En règle générale, les systèmes d'authentification et de sauvegarde tels que RADIUS, LDAP, Active Directory et Kerberos sont supportés sans adaptations supplémentaires des serveurs web ou de l'infrastructure.

Protection contre les attaques DDoS multicouches

Les dernières expériences de plusieurs Etats et éditeurs de journaux démontrent l'importance d'une défense efficace contre les attaques par déni de service (Denial of Service DoS). Les UASG combinent plusieurs technologies pour une prévention efficace contre les attaques basées sur le réseau ou l'application et contribuent sensiblement à la continuité des services. Parmi les mécanismes de défense typiques comptent la protection contre les attaques de type SYN-Flood (qui représentent 25% de tous les incidents DDoS), le filtrage géographique, la limitation des débits et des connexions, l'identification des attaques «Slow HTTP», les commandos aFleX.

Serveurs et réseau sans perte de performance

Décharger les serveurs d'application et des infrastructures réseau constitue une autre fonction qui incombe aux ADC et UASG. Les appliances correspondantes reprennent en outre les tâches gourmandes en ressources processeur et veillent à réduire le trafic de données grâce à des mécanismes intelligents. Les fonctions suivantes sont en général à disposition:

Réduction du volume des données

La compression des protocoles HTTP (compression HTTP) permet de réduire significativement le volume de données et les bandes passantes nécessaires. La mise en cache des requêtes (traffic caching) améliore la performance en minimisant le nombre de connexions aux serveurs. En outre, plusieurs connexions HTTP sont résumées en une session TPC (TCP Connection Reuse), résultant en une décharge supplémentaire des serveurs et réseau.

SSL Offloading

La terminaison des connexions client, avec l'utilisation des longueurs de clés actuelles, constitue une activité mobilisant des ressources système très élevées. Il est par conséquent conseillé de ne pas confier le chiffrement et le déchiffrement SSL au serveur web, mais d'assigner une UASG en amont, afin d'augmenter durablement la performance du serveur et d'exécuter efficacement le certificat SSL. La terminaison sécurisée SSL compte parmi les fonctions primaires de déchargement (offloading) SSL. Elle prend en charge le déchiffrement des données et les envoie de manière sécurisée au serveur correspondant. Tous les protocoles TCP connus sont généralement supportés.

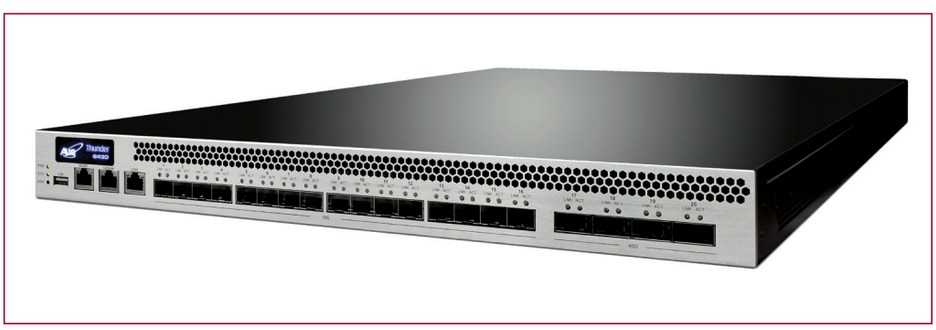
Le relais sécurisé (SSL Bridging) permet de vérifier si les données cryptées contiennent des codes défaillants – avant qu'elles n'atteignent le serveur. En outre, le code de la passerelle de service d'application unifiée est déchiffré, analysé au niveau du contenu, de nouveau chiffré et transmis au serveur. Ce processus continu bidirectionnel est difficilement imaginable sans la passerelle d'accélération matérielle UASG ou alors avec une perte sensible de performance.

Software Defined Networking (SDN)

Une tendance encore plus récente et révolutionnaire fait parler d'elle: les réseaux de nouvelle génération ou définis par logiciel (SDN). La transformation d'éléments statiques en infrastructures réseau dynamiques, extensibles, virtuelles et faciles à gérer devient un sujet central en matière de réseau. Dans ce contexte, il n'est pas étonnant que des fournisseurs innovants implémentent, aujourd'hui déjà, les éléments correspondants dans leurs UASG. Ces passerelles unifiées ont pour objectif de contrôler le réseau sur la base d'informations au niveau de la couche applicative et d'optimiser ainsi la performance de l'application.

IPv4/IPv6 – vive la convergence

Un thème brûlant actuellement est la migration de IPv4 à IPv6, qui peut également s'adresser via des passerelles applicatives unifiées. L'introduction conséquente d'IPv6 est dispendieuse en termes de temps et de coûts, elle exige d'importants investissements en composants matériels compatibles IPv6 et confronte les entreprises à d'importants défis financiers et logistiques. Dans ce contexte, les entreprises misent typiquement sur une introduction graduelle de l'IPv6, exigeant que les deux protocoles soient supportés en même temps. Les systèmes basés sur IPv4 et IPv6 doivent ensuite être en mesure de communiquer sans problème l'un avec l'autre. C'est à ce stade qu'interviennent les UASG modernes. En tant que passerelles, elles permettent une communication et connectivité probantes entre les deux protocoles et, par le biais des SLB-PT (Server Load Balancing with Protocol Translation), rendent les serveurs basés sur IPv4 et IPv6 accessibles à tous les clients externes – indépendamment du fait qu'ils utilisent IPv4 ou IPv6. NAT64/DNS64 est une solution pour les clients IPv6, qui assure l'accès aux environnements serveurs basés sur IPv4. Et dans le domaine des fournisseurs d'accès et des opérateurs, le Carrier Grade NAT (CGN ou CGNAT) permet, sans problème, la convergence des deux protocoles. <



Les passerelles de services applicatif unifiées innovantes maximisent la disponibilité des applications, augmentent la sécurité et permettent une migration IPv6 sans fil. Source: Boll Engineering