allot
See. Control. Secure.

Cas d'usage

Commerce électronique

Entreprise

INTRODUCTION

Ce document fournit une sélection de cas pratiques clients applicables au secteur du commerce électronique. Chaque cas décrit une problématique spécifique rencontrée par les sociétés de commerce électronique et fournit une description détaillée des produits disponibles qui se combinent pour apporter des solutions pérennes aux réseaux d'entreprise.

Les solutions Allot vous permettent d'augmenter la productivité et de protéger vos activités ainsi que vos utilisateurs contre les Ransomware, les attaques de déni de service et les infections par bot. En fournissant une visibilité complète et un contrôle granulaire des applications, des utilisateurs et de l'utilisation du réseau, la gamme Secure Service Gateway (SSG) d'Allot vous permet de supprimer les applications suspectes de votre réseau, de contrôler le trafic de loisir et, plus important encore, d'assurer que votre réseau fonctionne selon vos priorités métiers. En outre, les solutions Allot sont capables de réduire le coût total de possession de votre investissement en sécurité.

Allot est un fournisseur leader de solutions d'optimisation de services IP intelligentes qui aident les entreprises et les datacenters à gérer des réseaux plus efficaces pour mieux satisfaire leurs utilisateurs.

Allot exploite la technologie DPI et l'approche analytique du Big data pour fournir une vision claire et précise de l'utilisation du réseau. Armés de ces précieuses informations, les responsables informatiques peuvent contrôler dynamiquement la bonne marche des applications critiques pour se conformer aux SLA, protéger les actifs du réseau contre les attaques et accélérer le retour sur investissement (ROI) de leur infrastructure informatique.

Les solutions Allot sont déployées à travers le monde entier dans des centres de données et des réseaux d'entreprise opérant dans un large éventail de secteurs d'activité, notamment le commerce électronique, l'éducation, l'énergie, les services publics, la Finance, l'Administration publique, la Santé, l'Enseignement supérieur, l'Hôtellerie, les Médias et Télécommunications, les Commerces de détail et les Transports.

Les cas pratiques présentés dans cette brochure sont basés sur les principaux avantages qui peuvent être obtenus soit directement par une entreprise, soit par le biais de services managés d'opérateurs. Chaque cas tire profit des capacités en sécurité et en intelligence réseau liées au comportement des applications, des utilisateurs et des équipements, ainsi que du contrôle des entreprises pour :

- Comprendre comment les ressources réseau sont consommées avant d'investir dans l'infrastructure
- Définir des politiques de gestion du trafic en temps réel qui alignent les performances sur les priorités métiers de l'entreprise et ajustent en temps réel les flux de trafic IP lorsque les liaisons WAN sont en congestion
- Définir des politiques de gestion du trafic hiérarchiquement en fonction des niveaux de service individuels destinés à des profils utilisateur spécifiques
- Réduire la surface d'attaque de l'entreprise et augmenter la productivité en identifiant et en bloquant les applications à risques telles que les anonymiseurs et les applications peer-to-peer
- Contrôler l'utilisation des applications informatiques non autorisées telles que le stockage dans le cloud et les réseaux sociaux
- Augmenter la disponibilité globale grâce à une protection DDoS en temps réel combinée à une gestion du trafic pour supprimer automatiquement le trafic d'attaque DDoS en quelques secondes, tout en maintenant une Qualité d'Expérience (QoE) maximale pour tous les services réseau légitimes et critiques de l'entreprise
- Détecter et neutraliser les menaces web, le phishing, les ransomware, les botnets de quarantaine et les hôtes infectés par des logiciels malveillants

Atouts majeurs

- Assure la disponibilité et les temps de réponse des applications critiques
- Améliore la productivité et la satisfaction des utilisateurs
- Aligne les performances du réseau sur les priorités métiers de l'entreprise
- Permet d'investir, si nécessaire, dans l'expansion de l'infrastructure pour répondre aux exigences de l'entreprise

Agir sur la Priorisation des Applications métiers

- Analyse le taux d'utilisation et les performances des applications métiers et la qualité d'expérience (QoE) produite
- Définit et applique la qualité de service (QoS) bidirectionnelle prioritaire pour chaque application et la diffuse sur le réseau
- Applique un contrôle dynamique de la congestion basé sur la QoE alignée sur les priorités de l'entreprise
- Dépanne et réagit aux alertes lorsqu'elles surviennent

Généré par Secure Service Gateway (SSG) d'Allot

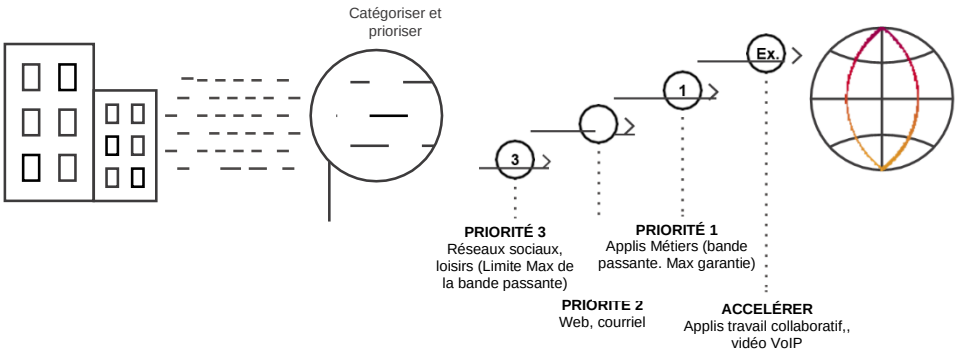
- Gestionnaire de passerelle Allot
- ClearSee Analytics d'Allot

COMMERCE ÉLECTRONIQUE

PRIORISATION DES APPLICATIONS MÉTIERS

Chaque entreprise s'appuie sur des applications en réseau pour mener ses activités avec succès. Dans le monde connecté d'aujourd'hui, les réseaux d'entreprise servent de nombreuses applications allant des loisirs aux applications critiques. Pour qu'une entreprise fonctionne efficacement, l'équipe informatique doit garantir la disponibilité des applications et le temps de réponse à tous les utilisateurs et à tous les modes d'accès. Le contrôle des applications commence en comprenant comment les applications critiques sont utilisées, comment elles fonctionnent en fonction des différentes conditions du réseau et quels sont les facteurs à contrôler pour garantir la meilleure efficacité.

MIGRATION VERS LE CLOUD, APPLICATIONS MÉTIERS



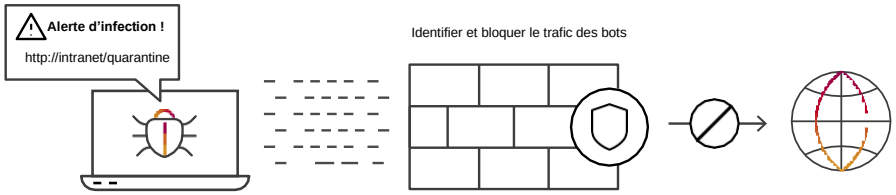
Sur la base de cette analyse, chaque application reçoit une politique de QoS personnalisée qui peut définir des seuils de congestion, ainsi qu'une certaine forme de "Expedited Forwarding" (en fonction de la sensibilité à la latence). Elle peut également définir une bande passante minimale garantie ou des débits de données séparés pour le trafic entrant et sortant. Ensemble, ces paramètres garantissent que les processus métiers et les utilisateurs de la gestion de la relation client (CRM), de la planification des ressources d'entreprise (ERP), de la Voix sur IP (VoIP), de la vidéoconférence et d'autres applications métiers peuvent fonctionner avec un meilleur rendement et une plus grande efficacité.

COMMERCE ÉLECTRONIQUE

CONFINEMENT DES BOTS EN TEMPS RÉEL

Il faut protéger le réseau d'entreprise contre les bots en neutralisant les hôtes infectés par des logiciels malveillants et l'activité des spams avant qu'ils n'affectent les performances et l'intégrité du réseau. Il faut aussi se prémunir contre les courriers indésirables et le protocole Internet (IP) qui consomme une bande passante précieuse en scannant le trafic de et identifier rapidement les hôtes infectés pour les nettoyer. Les solutions de sécurité Allot surveillent les taux d'établissement des connexions et analysent le comportement anormal des utilisateurs, permettant ainsi aux services informatiques de traiter chirurgicalement le problème à la racine (c'est-à-dire l'hôte infecté par un logiciel malveillant) sans avoir à recourir à des mesures plus larges telles que le blocage de sous-réseaux tout entiers, de liaisons WAN ou de ports. La détection des anomalies basée sur le comportement améliore la sécurité en effectuant un premier "dégraissage" des bots et d'autres logiciels malveillants.

ALERTE D'INFECTION



Atouts majeurs

- Protection de l'intégrité du réseau grâce au traitement rapide des infections par les bots
- Productivité garantie de l'entreprise en contenant les hôtes infectés
- Réduction du temps passé par le service d'assistance sur les problèmes résultant de logiciels malveillants

Confinement des bots en temps réel en action

- Détection d'un comportement anormal de l'hôte compatible avec les logiciels malveillants
- Identification de logiciels malveillants via le comportement du réseau (DNS de masse, robots anti-spam et analyse des ports)
- Bloque, limite ou met en quarantaine le trafic utilisateur en quelques secondes
- Informe l'utilisateur et le redirige vers le portail de nettoyage

Généré par Secure Service Gateway (SSG) d'Allot

- DDoS Secure d'Allot
- Moteur d'analyse du comportement de l'hôte

Atouts majeurs

- Protège la disponibilité et l'efficacité des datacenters
- Garantit les niveaux de service (SLA) des datacenters et minimise le risque de pannes
- Permet de gagner en visibilité sur les attaquants et leurs cibles dans le cloud

Agir en temps réel sur l'atténuation des attaques DDoS

- Détection et atténuation en ligne en quelques secondes. Assurance d'une correction immédiate pour les attaques de courte durée
- Détecte les anomalies de trafic reconnues comme des attaques DDoS, y compris les attaques zero-Day - bloque les attaques d'amplification "memcached" en première instance
- Crée des signatures de référence personnalisées pour filtrer précisément les paquets d'attaque
- Correction automatique des attaques ou par vérification manuelle
- Le système publie un rapport détaillé des attaques et des statistiques

Généré par Secure Service Gateway (SSG) d'Allot

- DDoS Secure d'Allot
- Moteur d'analyse comportementale du réseau

COMMERCE ÉLECTRONIQUE

BLOCAGE EN TEMPS RÉEL DES ATTAQUES DDOS

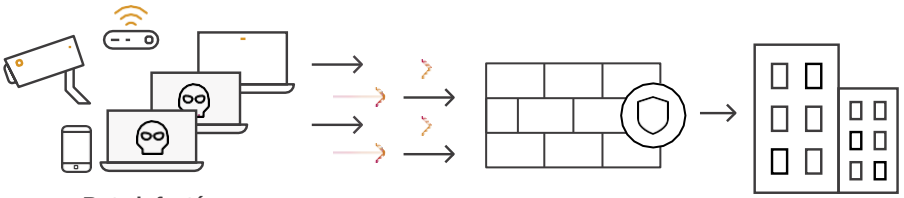
Les attaques DDoS gagnent en intensité et en sophistication chaque année, comme les attaques « memcached » et les attaques de courte durée qui contournent les solutions anti-DDoS qu'on trouve dans le Cloud. A une époque où les datacenters sont au cœur du fonctionnement des entreprises modernes, même quelques minutes d'indisponibilité peuvent entraîner des pertes de revenus importantes. En combinant la gestion avancée du trafic avec la détection et la correction sur une base comportementale des dénis de service distribués (DDoS), l'objectif de zéro temps d'arrêt peut être atteint en cours d'attaque pour les applications métiers critiques. La protection DoS/DDoS en ligne neutralise les attaques par "inondation" dans les secondes qui suivent leur occurrence en détectant, identifiant et filtrant rapidement les paquets DDoS, tout en permettant au trafic légitime de circuler librement.

PROTECTION ANTI-DDoS

La détection et l'atténuation en ligne bloquent les attaques en quelques secondes

Protège les périphériques tels que les pare-feu, sondes IDS/IPS, équilibreurs de charge

Assure la disponibilité des services grâce à une gestion dynamique des congestions et une priorisation des applications critiques



Bots infectés

DDoS entrant

Les attaques par inondation menacent la disponibilité des services

Légitime

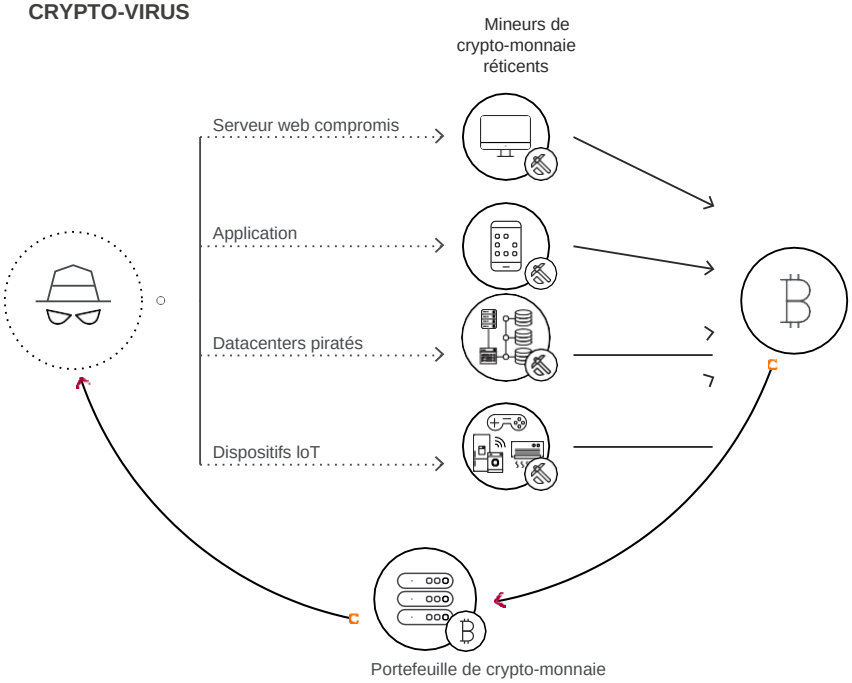
Attack

COMMERCE ÉLECTRONIQUE

IDENTIFICATION ET REPONSE TECHNIQUE AU CRYPTO-JACKING

Les détournements engendrés par les hackers de la crypto-monnaie, ou crypto-jacking, est l'une des principales menaces auxquelles les équipes informatiques d'entreprise sont confrontées aujourd'hui. Alors que le minage de crypto-monnaie nécessite des quantités importantes de ressources informatiques, les crypto-jackers ciblent comme moyen d'extraction gratuit la puissance CPU et GPU située dans les entreprises et toutes sortes d'organisations publiques ou privées. La surveillance du réseau est certainement le meilleur moyen de se protéger contre le crypto-jacking. Les crypto-jackers doivent pouvoir communiquer avec leurs serveurs cibles, recevoir de nouveaux hachages, les calculer et les renvoyer à leurs propres serveurs. Les plates-formes Allot NetworkSecure et Secure Service Gateway peuvent identifier cette activité malveillante et protéger les précieuses ressources de l'entreprise contre ces attaques de crypto-jacking.

ALERTE D'INFECTION AU CRYPTO-VIRUS



Atouts majeurs

- Isolation des bibliothèques « Coinhive » qui exploitent la crypto-monnaie « Monero »
- Large reconnaissance et application des politiques de protocoles et d'applications de minage de crypto-monnaie
- Empêche le piratage des ressources des serveurs ainsi que l'altération des performances des applications métiers
- Empêche que le précieux matériel réseau soit endommagé par une surchauffe et réduit les coûts de consommation électrique associés au minage de crypto-monnaie

L'identification et le blocage du crypto-jacking en action

- Identifie et bloque les logiciels malveillants de crypto-monnaie
- Bloque l'accès aux sites web qui injectent le logiciel de minage de crypto-monnaie
- Identifie et bloque les protocoles de minage de crypto-monnaie
- Identifie et bloque les P2P, les VPN et d'autres applications qui activent les attaques de crypto-jacking

Généré par Secure Service Gateway (SSG)

- Sécurité web Allot
- Visibilité et contrôle d'Allot

CONCLUSION

La véritable activité de votre réseau réside dans les processus métiers. La bande passante, le débit, la latence et d'autres métriques courants sont des aspects de l'évaluation de la façon dont votre réseau prend en charge vos processus internes et externes pour mener à bien votre activité. Et parfois, voire souvent, c'est votre réseau qui est au cœur de votre métier.

Comme il est démontré dans les cas d'usage présentés dans cette brochure, la gamme SSG d'Allot apporte une réelle valeur ajoutée aux opérations, à la planification et à votre entreprise. Tous nos clients ont constaté des avantages immédiats dès qu'ils ont braqué leurs projecteurs sur leurs réseaux et ont vu en direct le comportement des applications, des utilisateurs et du réseau lui-même. D'après notre expérience, il y a souvent un grand décalage entre la façon dont les entreprises pensent que leurs processus métiers fonctionnent et la façon dont ils fonctionnent réellement.

La performance des processus laisse généralement à désirer pour les raisons suivantes :

- Les flux des applications qui composent les processus s'interrompent intempestivement
- Le réseau connaît des congestions et d'autres problématiques liées au trafic ou aux équipements
- Des anomalies liées à la sécurité affectent les services ou provoquent des dénis de service

Nos solutions en termes de visibilité et de contrôle du réseau peuvent mettre en évidence toutes ces anomalies de fonctionnement en temps réel et fournir les outils nécessaires pour les résoudre. A titre d'exemple, grâce à nos solutions, votre équipe informatique sera en mesure d'identifier les protocoles et les applications spécifiques, chiffrés ou non, et de surveiller et mesurer l'impact des règles de politique statique ou dynamique que vous aurez définies préalablement.

Par ailleurs, en augmentant considérablement la visibilité d'ensemble du service informatique, on lui permet d'augmenter les performances du réseau. Par exemple, en voyant quels employés utilisent quelles applications et à quel moment, vous pourrez hiérarchiser votre trafic réseau et définir des politiques de gestion du trafic qui répondent à vos objectifs métiers et aux attentes des utilisateurs. De plus, le service informatique pourra prendre des décisions en connaissance de cause sur la taille et le calendrier des futurs investissements liés au réseau.

Pour plus d'informations, consultez https://www.allot.com/enterprise et http://www.merisac.com