Cas d'usage

Énergie et services publics

Entreprise

Contactez MERISAC pour une étude de votre projet
"See, Control, Secure" dans le Cloud/Datacenter :

merisac@merisac.com
Bureau : 01 49 33 737 5
Mobile : 06 60 12 64 51

MERISAC INSTRUMENTS
Intégrateur de Services WAN & Datacenter

Traduction française assurée par les sociétés
translated.
MERISAC INSTRUMENTS
Intégrateur de Services WAN & Datacenter

INTRODUCTION

Ce document fournit une sélection de cas d'usage clients applicables au secteur de l'énergie et des services publics. Chaque cas présente une problématique spécifique rencontrée par les sociétés de ce secteur et fournit une description détaillée des produits disponibles qui peuvent être utilisés pour apporter des solutions 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 par déni de service et les infections par bot. En fournissant une visibilité totale et un contrôle granulaire des applications, des utilisateurs et de l'utilisation du réseau, 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 conformément à vos priorités métiers. En outre, les solutions Allot réduisent le coût total de possession de votre investissement en sécurité. Allot tire parti de la technologie DPI et de l'approche analytique du Big data pour fournir une

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

vision claire et précise de l'utilisation du réseau. Armés de ces informations précieuses, 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 les télécommunications, le commerce 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 des services managés d'opérateurs. Chaque cas tire profit des capacités de sécurité et d'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 de réinvestir dans l'infrastructure
- Définir des politiques de gestion du trafic en temps réel qui alignent les performances sur les priorités de l'entreprise et ajustent dynamiquement 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 risque telles que les anonymiseurs et les applications P2P
- Contrôler l'utilisation des applications informatiques non autorisées telles que le stockage dans le Cloud et les réseaux sociaux
- Augmenter la disponibilité grâce à une protection DDoS en temps réel combinée à une gestion du trafic afin de supprimer automatiquement le trafic des attaques DDoS en quelques secondes, tout en maintenant une qualité d'expérience (QoE) maximale de 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

- Empêche l'utilisation excessive et extérieure à l'entreprise d'un réseau
- Améliore la productivité et la satisfaction des utilisateurs
- Optimise les performances des liaisons Internet

Agir sur la répartition équitable des ressources

- Définit des niveaux d'utilisation et des quotas équitables pour le trafic non lié à l'entreprise
- Attribue des niveaux de bande passante appropriés à un utilisateur, un service ou un équipement
- Applique automatiquement un taux d'utilisation adéquat en temps réel
- Bloque l'utilisation d'applications et de contenus inappropriés et risqués dans un réseau d'entreprise

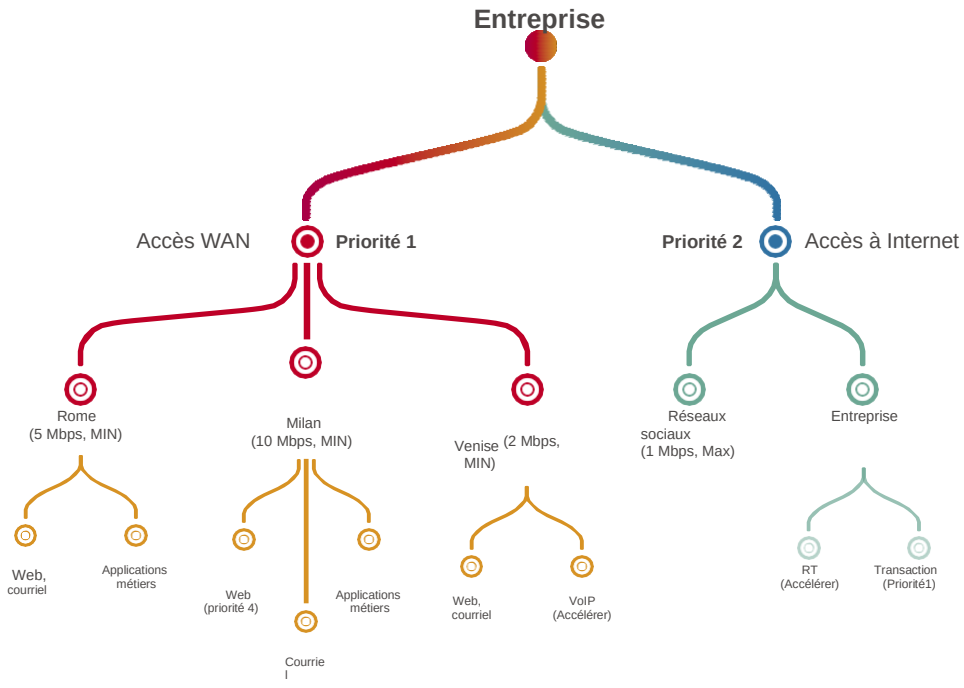
Généré par Secure Service Gateway (SSG) d'Allot

- Gestionnaire de passerelle Allot
- ClearSee Analytics d'Allot

ÉNERGIE ET SERVICES PUBLICS
GESTION EQUITABLE DES RESSOURCES

La connectivité Internet est essentielle au succès de toute entreprise. Les entreprises peuvent gérer cette ressource en établissant une politique de répartition des ressources optimale pour les différents départements, services, utilisateurs et applications.
Par exemple, il est conseillé à la direction de bloquer les téléchargements P2P de contenu partagé avec des applications telles que BitTorrent qui consomment trop de bande passante, et peuvent être utilisées pour pirater des informations d'entreprise confidentielles et peuvent favoriser l'introduction de logiciels malveillants. En outre, l'entreprise peut limiter l'accès ou attribuer des quotas aux réseaux sociaux pendant les heures ouvrables, et prioriser les applications métiers par rapport au reste du trafic Internet. Grâce à des règles de contrôle adéquates, les entreprises peuvent empêcher les particuliers et certaines applications de monopoliser la bande passante Internet, garantir la qualité de service pour tous les utilisateurs et minimiser les activités Internet non utiles à l'entreprise afin d'améliorer la productivité et, ainsi, reporter les investissements coûteux en infrastructure.

GESTION DU TRAFIC PAR HIERARCHIE DES REGLES DE CONTRÔLE DE QOS



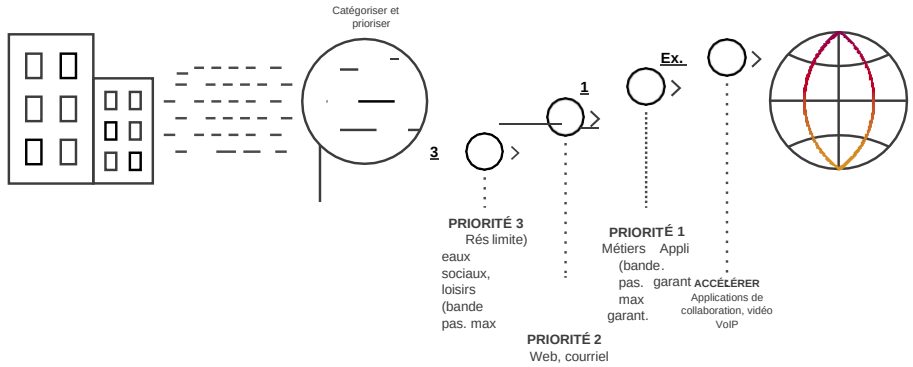
ÉNERGIE ET SERVICES PUBLICS

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 déploient 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 par comprendre comment les applications critiques sont utilisées, comment elles fonctionnent dans différentes conditions de réseau et quels sont les facteurs que le service informatique peut contrôler pour garantir leur bon fonctionnement. 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 d'accélération des données (en fonction de la sensibilité aux retards). 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 métier 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 de manière plus productive et plus efficace.

MIGRATION VERS LE CLOUD, APPLICATION MÉTIER



Atouts majeurs

- Assure la disponibilité et le 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 besoin, dans l'expansion de l'infrastructure pour répondre aux exigences de l'entreprise

Priorisation des applications métier en action

- Analyse les performances des applications métiers et la qualité d'expérience (QoE) qu'elles offrent aux utilisateurs
- Définit la qualité de service (QoS) prioritaire pour chaque application et l'applique sur le réseau
- Applique un contrôle dynamique de la congestion basé sur la QoE aligné sur les priorités métiers de l'entreprise
- Dépanne et réagit aux alertes dès qu'elles se produisent

Généré par Secure Service Gateway (SSG) d'Allot

- Gestionnaire de passerelle Allot
- ClearSee Analytics d'Allot

Atouts majeurs

- Prendre en compte un large éventail de charges de travail client
- Aligne l'accès à Internet et l'allocation des ressources aux priorités métiers
- Contrôle les coûts d'accès au cloud

Gère la migration vers le cloud en action

- Priorise les applications cloud et limite le trafic Internet non lié à l'organisation
- Applique un contrôle dynamique de l'encombrement basé sur la qualité de l'expérience
- Fait respecter les priorités pour des applications et/ou des utilisateurs spécifiques
- Permet de bénéficier d'une visibilité granulaire sur l'utilisation des applications cloud

Généré par Secure Service Gateway (SSG) d'Allot

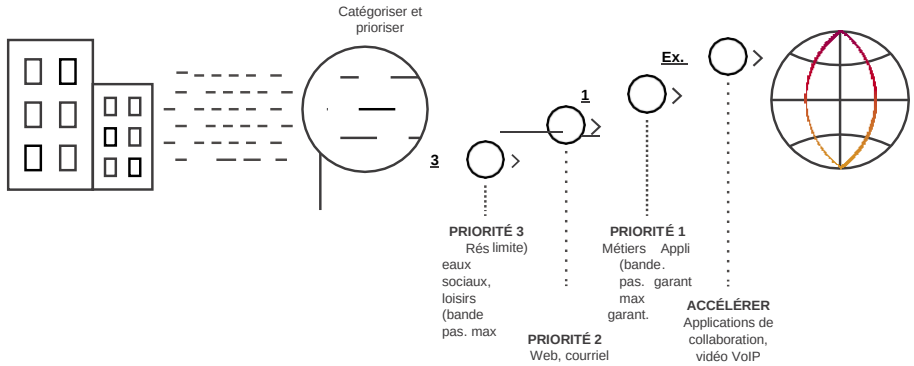
- Gestionnaire de passerelle Allot
- ClearSee Analytics d'Allot

ÉNERGIE ET SERVICES PUBLICS

GÉRER LA MIGRATION VERS LE CLOUD

De nombreuses entreprises migrent les applications de leurs centres de données privés vers des applications basées sur le Cloud. Par exemple, les serveurs d'échange et de collaboration sont remplacés par Office 365 et les CRM sur site par Salesforce. Les avantages de la migration vers le Cloud sont : un coût réduit, un accès universel et une maintenance zéro, et pourtant de nombreuses entreprises ont déjà eu une mauvaise surprise en recevant une facture élevée en raison d'une utilisation inattendue. Par ailleurs, elles peinent souvent à maintenir un niveau élevé de qualité d'expérience utilisateur (QoE). C'est pourquoi, les solutions de gestion du trafic et de contrôle des politiques basées sur DPI permettent aux entreprises de surveiller l'utilisation et le comportement des applications du Cloud et d'appliquer au contenu personnel les priorités et les débits de données engagés (bande passante Internet) pour les applications métiers.
Le contrôle de congestion basé sur la QoE priorise dynamiquement l'accès à Internet en fonction des priorités éducatives en mesurant plusieurs métriques et en notant la QoE qui serait reçue par l'utilisateur final. Grâce à des rapports d'utilisation granulaires et des mises à jour effectuées uniquement lorsqu'elles sont nécessaires le réseau d'entreprise est maintenu à un haut niveau de qualité.

MIGRATION VERS LE CLOUD DES APPLICATIONS MÉTIERS

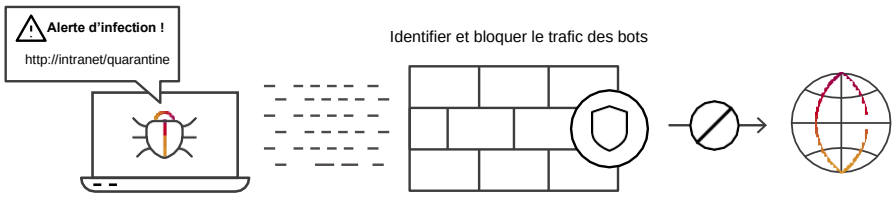


ÉNERGIE ET SERVICES PUBLICS

CONFINEMENT DES BOTS EN TEMPS RÉEL

Protégez votre réseau contre les bots en neutralisant les hôtes infectés par des logiciels malveillants ainsi que 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 consomment une précieuse bande passante en scannant le trafic 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 bot
- Productivité garantie pour l'entreprise en se préservant des hôtes infectés
- Réduction du temps passé par le service d'assistance sur les problèmes liés aux logiciels malveillants

Confinement des bots en temps réel en action

- Détection d'un comportement anormal de l'hôte suspectant un logiciel malveillant
- Identification de logiciels malveillants via le comportement du réseau (DNS de masse, robots antispams 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

- Protection de la disponibilité et de l'efficacité du centre de données
- Garantit les accords de niveau de service (SLA) du centre de données et minimise le risque de pannes
- Permet de gagner en visibilité sur les attaquants et leurs cibles dans votre cloud

Atténuation des attaques DDoS en temps réel en action

- Détection et limitation en ligne en quelques secondes. Fournit une correction immédiate pour les attaques de courte durée
- Détecte les anomalies de trafic susceptibles d'être des attaques DDoS, y compris les attaques zero-day - bloque les attaques d'amplification memcached en première intention
- Crée des signatures personnalisées pour filtrer précisément les paquets d'attaque
- Correction appliquée automatiquement ou lors d'une vérification manuelle
- Le système publie un rapport d'attaque et des statistiques détaillés

Généré par Secure Service Gateway (SSG) d'Allot

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

ÉNERGIE ET SERVICES PUBLICS

BLOCAGE EN TEMPS REEL DES ATTAQUES DDOS

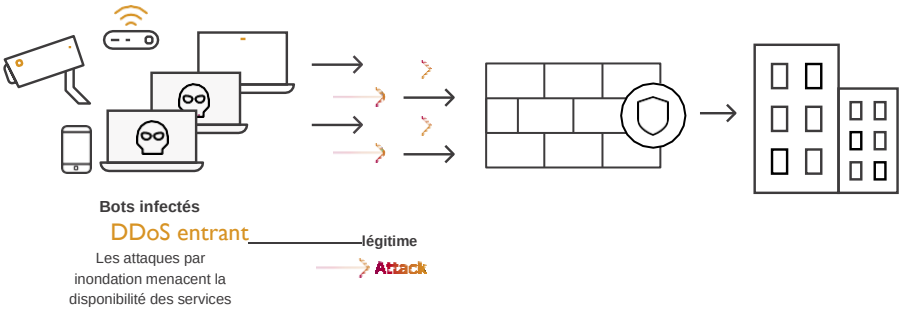
Les attaques DDoS gagnent en intensité et en sophistication chaque année, comme les attaques « memcached » et les attaques de courte durée qui contournent les solutions anti-DDoS qu'on trouve dans le Cloud. A une époque où les datacenters sont au coeur du fonctionnement des entreprises modernes, même 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 la limitation en ligne bloquent les attaques en quelques secondes

Protègent les périphériques tels que le pare-feu, IP et les équilibreurs de charge

Assurent la disponibilité des services grâce à une gestion dynamique de l'encombrement et une priorisation des applications critiques



ÉNERGIE ET SERVICES PUBLICS

CONTRÔLEZ LES APPLICATIONS À RISQUE NON AUTORISEES

L'utilisation intensive d'applications et de sites web non prioritaires ou de loisir consomme une bande passante considérable et peut entraîner des congestions de trafic et nuire aux opérations de votre réseau. De plus, certaines applications présentent des niveaux de risque élevés. Par exemple, les applications peer-to-peer fournissent une porte dérobée pour que les données hébergées soient accessibles à toute personne sur le réseau peer-to-peer, et les programmes ou contenus téléchargés peuvent inclure des logiciels malveillants ou violer les droits d'auteur.

Les tunnels d'anonymisation/VPN sont généralement utilisés pour cacher l'identité d'un utilisateur et sont utilisés par des personnes peu scrupuleuses pour accéder à du contenu illégal ou acheter des marchandises illégales, telles que des drogues.

Bien que ces applications puissent servir à des fins de confidentialité, elles sont également utilisées pour masquer des activités illégales ou sont exploitées pour des cyberattaques. Par nature, elles sont conçues pour contourner les contrôles de sécurité conventionnels tels que les pare-feu et le système de détection d'intrusion (IDS). Elles parviennent à se dissimuler en utilisant le cryptage des données il est difficile de les identifier.

Allot utilise des mécanismes avancés pour détecter les applications cryptées, qui permettent à l'entreprise d'identifier les applications à risque et/ou malveillantes sans avoir à les décrypter. Ces méthodes, qui incluent les procédures ci-après, s'appliquent au trafic HTTP et non HTTP chiffré :

- Détection de modèle
- Analyse des certificats
- Analyse des extensions Secure Sockets Layer (SSL)
- Heuristique du trafic
- Statistiques sur le trafic
- Détection de l'indicateur de nom de serveur (SNI)
- Algorithmes d'apprentissage automatique

Atouts majeurs

- Réduit la surface des attaques en bloquant les applications risquées
- Identifie et contrôle l'utilisation des applications à risque et des applications informatiques non autorisées, des réseaux privés virtuels (VPN) et des anonymiseurs
- Bloque le trafic qui contourne les contrôles de sécurité

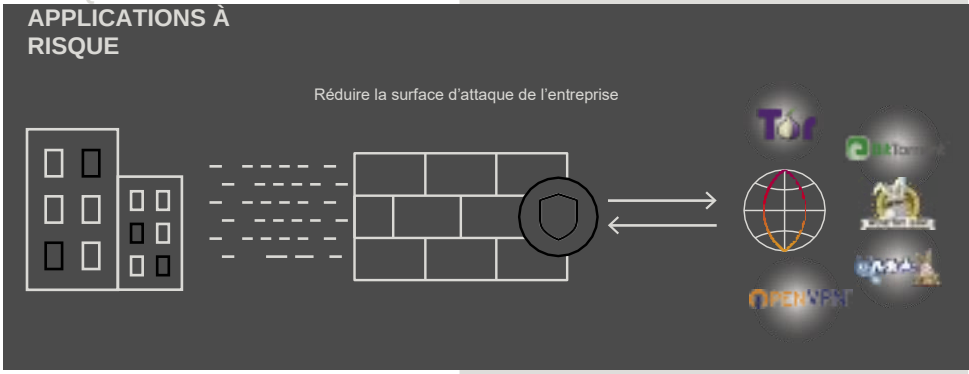
Contrôle les applications risquées et non autorisées en action

- Détecte et contrôle une gamme d'anonymiseurs, Des applications peer-to-peer et de partage de fichiers
- Mises à jour bimensuelle de reconnaissance des applications
- Bloque et limite le trafic utilisateur qui utilise des applications informatiques non autorisées

Généré par Secure Service Gateway (SSG) d'Allot

- Gestionnaire de passerelle Allot
- ClearSee Analytics d'Allot

BLOQUER LES APPLICATIONS À RISQUE



Atouts majeurs

- Surveillance et sécurité des capteurs IoT
- Alertes et rapports d'anomalies
- Prévention de l'encombrement de la bande passante et amélioration de la qualité d'expérience (QoE, Quality of Experience) pour assurer un fonctionnement correct des capteurs

Internet des objets Intelligence en action

- Applique le contrôle d'accès et la stratégie de trafic au comportement attendu des déploiements IoT
- Détecte le comportement anormal de l'hôte compatible avec les logiciels malveillants
- Identifie les logiciels malveillants (serveurs de nom de domaine de masse (DNS), robots de spam et analyse des ports)
- Mesure le temps de réponse du capteur et alloue la bande passante à chaque capteur en fonction de son fonctionnement défini
- Informe les services de contrôle de toute activité anormale

Généré par Secure Service Gateway (SSG) d'Allot

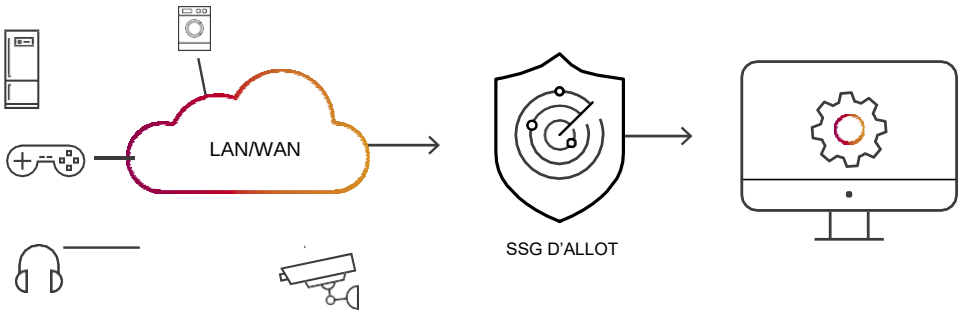
- DDoS Secure d'Allot
- Moteur d'analyse comportementale du réseau
- Moteur d'analyse du comportement de l'hôte
- ClearSee Analytics

ÉNERGIE ET SERVICES PUBLICS

INTELLIGENCE INTERNET DES OBJETS (IOT)

Les appareils IoT sont généralement conçus dans un but spécifique et utilisent le plus souvent un ensemble limité de protocoles et d'applications lors de la communication avec leurs serveurs principaux. Cette caractéristique permet à une entreprise de réduire la surface d'attaque des déploiements IoT en appliquant une stratégie qui contrôle l'accès aux serveurs autorisés et limite les modèles de communication au comportement normal attendu. En outre, le SSG offre une défense proactive de votre réseau contre les robots IoT tels que Reaper et Mirai grâce à des capacités anti-malware et anti-bot en ligne, ainsi qu'au moyen de l'identification et de la mise en quarantaine des équipements infectés par des logiciels malveillants avant qu'ils n'affectent le déploiement de l'IoT, les performances et l'intégrité du réseau.

LE SSG D'ALLOT SSG POUR LA VISIBILITÉ, LA SÉCURITÉ ET LE CONTRÔLE IOT



Les solutions de sécurité Allot surveillent les taux d'établissement des connexions et d'autres symptômes de comportement anormal des utilisateurs, permettant ainsi aux entreprises de traiter chirurgicalement la source du problème (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 entiers, de liens ou de ports. La détection des anomalies basée sur le comportement améliore les couches de sécurité existantes grâce à une correction en première ligne des robots DDoS et d'autres logiciels malveillants.

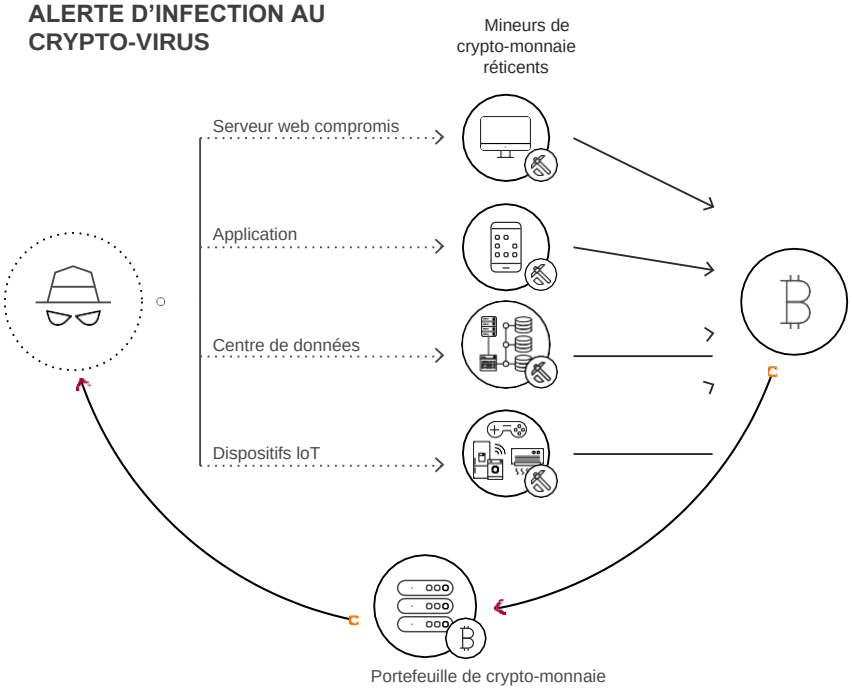
ÉNERGIE ET SERVICES PUBLICS

IDENTIFICATION ET ATTÉNUATION DU CRYPTO-JACKING

Le détournement de 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 massives de ressources de traitement informatique, les crypto-jackers ciblent comme moyen d'extraction gratuite la puissance CPU et GPU située dans les entreprises et les organisations.

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. NetworkSecure et Secure Service Gateway d'Allot peuvent identifier ces échanges et protéger les précieuses ressources de l'entreprise contre les attaques de crypto-jacking.

ALERTE D'INFECTION AU CRYPTO-VIRUS



Atouts majeurs

- Isolation des bibliothèques « Coinhive » qui exploitent la crypto-monnaie Monero
- Large identification 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

Identification et atténuation 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 le P2P, les VPN et d'autres applications qui activent les attaques de crypto-jacking

Généré par Secure Service Gateway (SSG) d'Allot

- Sécurité web Allot
- Visibilité et contrôle par Allot

CONCLUSION

La véritable activité des réseaux d'entreprise réside dans les processus métiers. La bande passante, le débit, la latence et d'autres mesures de communication courantes 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, c'est votre réseau qui est au centre de votre activité.

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 aux entreprises. Tous nos clients ont constaté des avantages immédiats dès qu'ils ont braqué les projecteurs sur leurs réseaux et ont vu en direct le comportement des applications, des utilisateurs et du réseau. D'après notre expérience, il y a souvent un 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 sessions applicatives qui composent les processus sont coupées
- Le réseau connaît des congestions et d'autres problématiques surviennent sur le trafic ou les équipements
- Des anomalies liées à la sécurité affectent les services ou provoquent des dénis de service

Des solutions efficaces en termes de visibilité et de contrôle du réseau peuvent mettre en évidence tous ces problèmes en temps réel et fournir les outils nécessaires pour les résoudre. Votre équipe informatique sera en mesure d'identifier les protocoles et les applications spécifiques, chiffrés ou non, de surveiller et mesurer tout élément de politique statique ou dynamique que vous aurez mis en oeuvre.

La visibilité analytique fournira également au service informatique des informations sur la meilleure manière d'augmenter les performances du réseau. Par exemple, en voyant quels employés utilisent quelles applications et à quel moment, vous pourrez hiérarchiser l'accès et définir des politiques de gestion du trafic qui répondent à vos objectifs métiers et aux attentes des utilisateurs, ainsi que pour la prise de décision en connaissance de cause sur la taille et le calendrier des futurs investissements liés à votre infrastructure réseau.

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