allot
See. Control. Secure.

Cas d'usage

Administrations publiques

Entreprise

INTRODUCTION

Ce document fournit une sélection de cas d'usage pratiques applicables aux administrations publiques locales ou nationales. Chaque cas présente un problème spécifique rencontré par les administrations publiques et fournit une description détaillée des produits disponibles qui peuvent être utilisés pour leur apporter des solutions.

Les solutions d'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, 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 conformément à vos priorités métiers. En outre, les solutions Allot diminuent 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 pour mieux satisfaire leurs utilisateurs.

Vision claire et précise de l'utilisation du réseau. Armés de ces précieuses informations, les responsables informatiques peuvent contrôler dynamiquement la livraison des applications critiques pour se conformer aux SLA, protéger les actifs du réseau contre les attaques et accélérer le retour sur investissement (ROI) effectué sur 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, les soins de santé, l'enseignement supérieur, l'hôtellerie, les médias et les 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 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 non professionnelle d'un réseau
- Améliore la productivité et la satisfaction des utilisateurs

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
- Limite ou Bloque l'utilisation d'applications et de contenus inappropriés et risqués dans un réseau d'entreprise

Généré par Secure Service Gateway (SSG) d'Allot

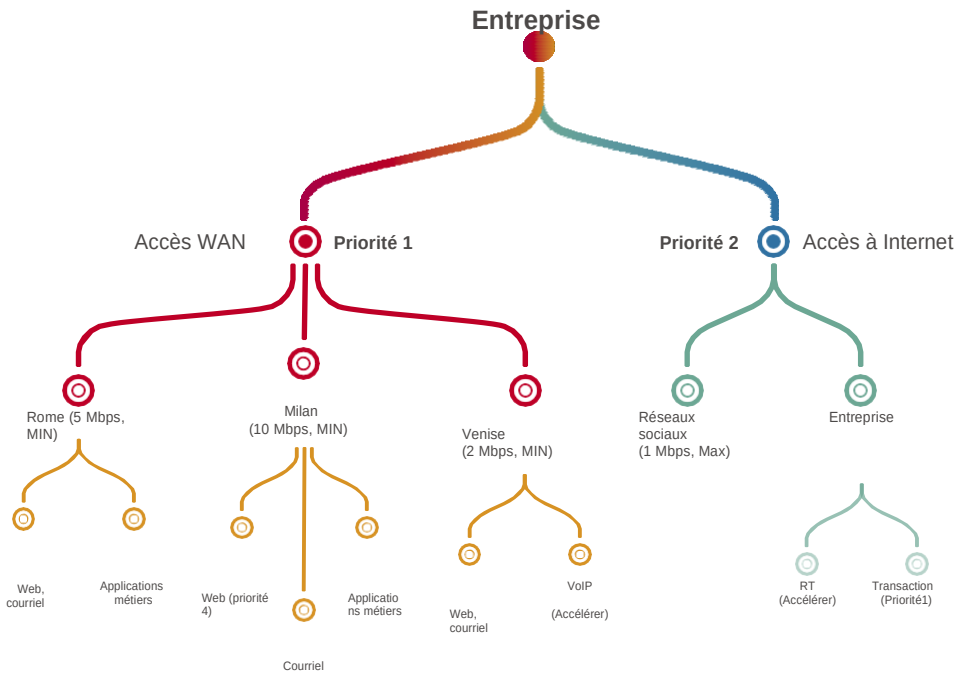
- Gestionnaire de passerelle Allot
- ClearSee Analytics d'Allot

ADMINISTRATIONS PUBLIQUES LOCALES ET NATIONALES

GESTION EQUITABLE DES RESSOURCES

La connectivité Internet est essentielle au succès de toute entreprise. Les entreprises peuvent gérer cette ressource en établissant une politique optimale de répartition des ressources pour les différents départements, services, utilisateurs et applications. Par exemple, il est conseillé à la direction de limiter fortement les téléchargements P2P de contenu partagé avec des applications telles que BitTorrent qui consomment trop de bande passante, peuvent être utilisées pour externaliser des informations d'entreprise confidentielles et 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 d'utilisation adéquates, les entreprises peuvent empêcher le trafic non professionnel et certaines applications consommatrices 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 des investissements coûteux en infrastructure.

GESTION DU TRAFIC PAR REGLES DE CONTRÔLE DE QOS



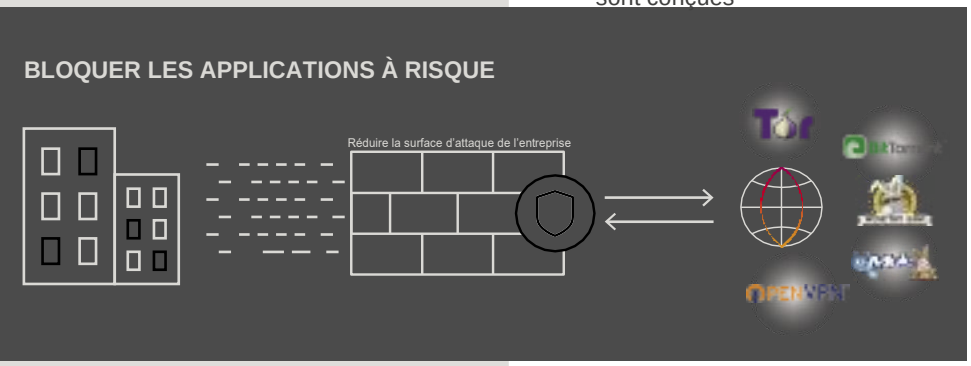
> Le patriotisme soutient votre pays tout le temps et votre gouvernement quand il le mérite.
>
> Mark Twain

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, Les applications P2P et de partage de fichiers
- Mises à jour bimensuelles 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

ADMINISTRATIONS PUBLIQUES LOCALES ET NATIONALES

CONTRÔLEZ LES APPLICATIONS À RISQUE NON AUTORISEES

L'utilisation intensive d'applications et de sites web non professionnels ou de loisir consomme une bande passante considérable qui peut entraîner la congestion du trafic et nuire aux opérations de votre réseau. De plus, certaines applications présentent des niveaux de risque élevés, comme par exemple :
Les applications peer-to-peer qui fournissent une porte dérobée pour héberger des données accessibles à toute personne sur le réseau peer-to-peer, et des programmes ou contenus téléchargés qui peuvent inclure des logiciels malveillants ou violer les droits d'auteur.
De plus, les tunnels d'anonymisation/VPN sont généralement utilisés pour cacher l'identité d'un utilisateur et sont utilisés par certains pour accéder à du contenu illégal ou acheter des marchandises illégales, telles que des drogues.
Bien que ces applications puissent servir la confidentialité de l'entreprise, 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-feux et les systèmes de détection d'intrusions (IDS). Elles parviennent à la dissimulation en utilisant le cryptage et le camouflage et il est difficile de les identifier. Allot emploie des mécanismes automatiques 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 :

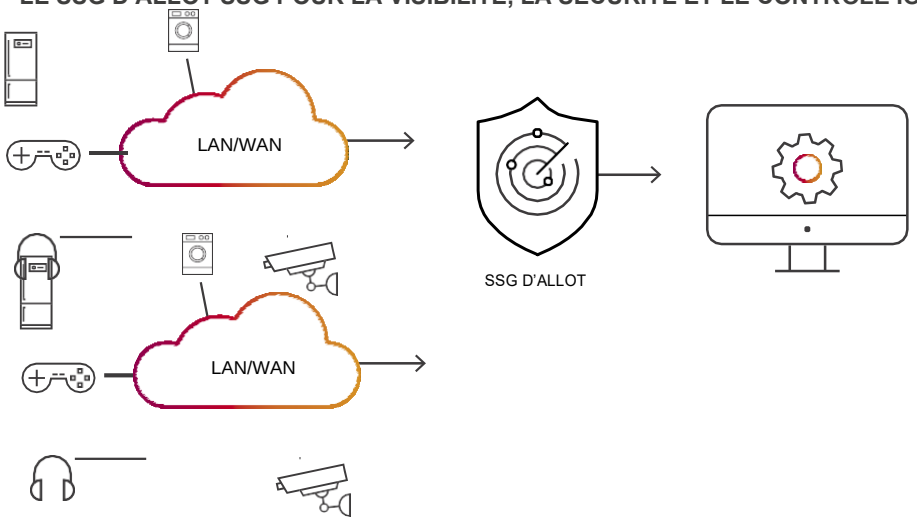
- Statistiques sur le trafic
- Détection de l'indicateur de nom de serveur (SNI)
- Algorithmes automatiques d'apprentissage.
- Détection de modèle
- Analyse des certificats
- Analyse des extensions Secure Sockets Layer (SSL)
- Heuristique du trafic

ADMINISTRATIONS PUBLIQUES LOCALES ET NATIONALES

L'INTELLIGENCE INTERNET DES OBJETS (IOT)

Les périphériques IoT sont généralement conçus dans un but précis et utilisent le plus souvent un ensemble limité de protocoles et d'applications lors de la communication avec leurs serveurs principaux. Cela permet à l'entreprise de réduire la surface Des attaques lors des déploiements IoT en appliquant une stratégie qui contrôle l'accès aux serveurs autorisés et limite les modèles de communication au comportement normal défini comme référence. De plus, le SSG fournit 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'à des moyens d'identification et de mise en quarantaine des équipements infectés par des logiciels malveillants avant qu'ils n'affectent le déploiement IoT, ainsi que les performances et l'intégrité du réseau. Les solutions de sécurité Allot surveillent les taux d'établissement de connexion et d'autres symptômes de comportements anormaux des utilisateurs, permettant ainsi aux services informatiques de traiter chirurgicalement la cause racine (c'est-à-dire l'hôte infecté) sans avoir à recourir à des mesures plus larges telles que le blocage de sous-réseaux entiers, des liens WAN ou des ports. La détection des anomalies basée sur le comportement améliore les couches de sécurité existantes grâce à une mitigation de première ligne des bots et d'autres logiciels malveillants.

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



Atouts majeurs

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

Internet des objets – L'Intelligence en action

- Applique le contrôle d'accès et la politique de QoS du trafic au comportement attendu des déploiements IoT
- Détecte le comportement anormal de l'hôte infecté par des logiciels malveillants
- Identifie les logiciels malveillants (serveurs de nom de domaine de masse (DNS), les 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 de référence
- Informe les services de contrôle de toute activité anormale

Généré par Secure Service Gateway (SSG) d'Allot

- DDoS Secure d'Allot
- Moteur d'analyse

Atouts majeurs

- Accepte un large éventail de charges de travail des salariés
- Aligne l'accès à Internet et l'allocation des ressources aux priorités de l'entreprise
- Contrôle les coûts d'accès au Cloud

Gérer la migration vers le Cloud

- Priorise les applications Cloud et limite le trafic Internet non professionnel
- Applique un contrôle dynamique de la congestion de trafic basé sur la qualité d'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

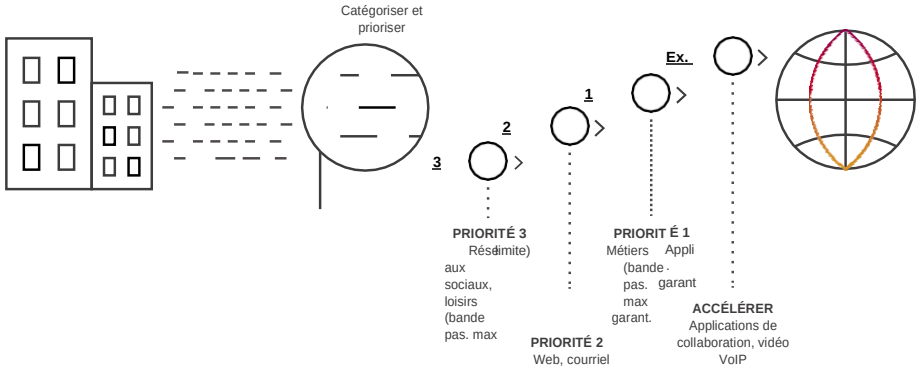
- Gestionnaire de passerelle Allot
- ClearSee Analytics d'Allot

ADMINISTRATIONS PUBLIQUES LOCALES ET NATIONALES

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 CRM sur site avec Salesforce. Les avantages de la migration vers le Cloud sont : un coût réduit, un accès universel et une maintenance zéro. Pourtant de nombreuses entreprises ont eu une mauvaise surprise en recevant une facture élevée en raison d'une utilisation excessive. Par ailleurs, elles peinent souvent à maintenir un niveau élevé de qualité d'expérience utilisateur (QoE). Les solutions de gestion du trafic et de contrôle de QoS basées sur le DPI permettent aux entreprises de surveiller l'utilisation et le comportement des applications basées sur le Cloud et d'appliquer des priorités et des débits garantis (bande passante Internet) pour les applications métiers en dépit du trafic non professionnel. Le contrôle de congestion basé sur la QoE priorise dynamiquement l'accès à Internet en fonction des priorités établies en mesurant plusieurs métriques et en notant la QoE perçue qui serait reçue par l'utilisateur final. Grâce aux rapports d'utilisation granulaires, des mises à niveau peuvent être effectuées lorsqu'elles sont jugées nécessaires par les services informatiques.

MIGRATION VERS LE CLOUD DES APPLICATIONS MÉTIERS

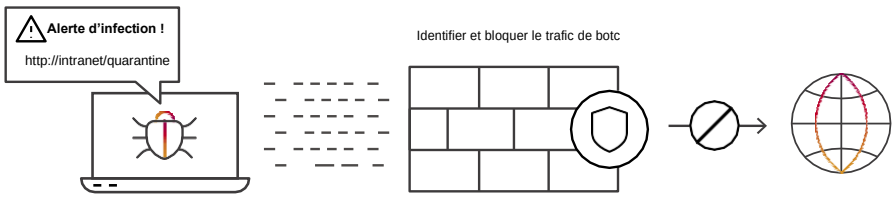


ADMINISTRATIONS PUBLIQUES LOCALES ET NATIONALES

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 consomme une bande passante précieuse 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 basées sur le comportement améliore la sécurité en effectuant un premier "dégraissage" des bots et d'autres logiciels malveillants.

ALERTE AUX INFECTIONS



Atouts majeurs

- Protection de l'intégrité du réseau grâce au traitement rapide des infections dues aux bots
- Productivité garantie de l'entreprise en identifiant les hôtes infectés
- Réduction du temps passé par le service d'assistance sur les problèmes liés aux logiciels malveillants
- Permet d'investir au besoin dans l'expansion de l'infrastructure pour répondre aux exigences de l'entreprise

Confinement des bots en temps réel

- Détection d'un comportement anormal de l'hôte lié à des 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 les utilisateurs et les 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 panne
- Permet de gagner en visibilité sur les attaquants et leurs cibles dans le Cloud

Atténuation des attaques DDoS en temps réel en action

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

Généré par Secure Service Gateway (SSG) d'Allot

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

ADMINISTRATIONS PUBLIQUES LOCALES ET NATIONALES

MITIGATION DES ATTAQUES DDOS EN TEMPS RÉEL

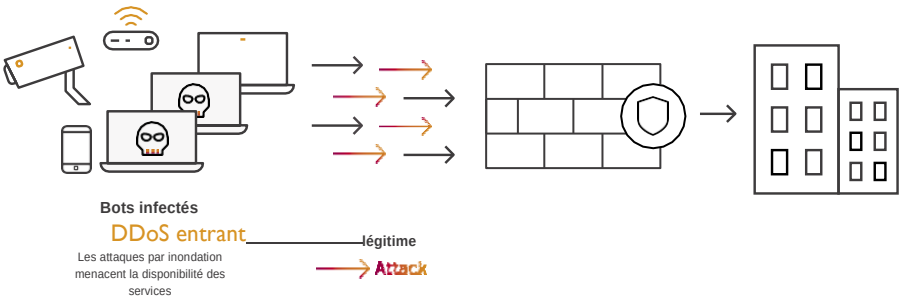
Les attaques DDoS gagnent en intensité et en sophistication chaque année, comme les attaques « memcached » et les attaques de courte durée qui se confondent avec les solutions de mitigation DDoS basées sur le Cloud. Alors que les centres de données sont au cœur du fonctionnement des entreprises modernes, même quelques minutes d'indisponibilité peuvent entraîner une perte de revenus importante. En combinant la gestion avancée du trafic avec la détection et la mitigation comportementale du déni de service distribué (DDoS), zéro temps d'arrêt peut être atteint même en cas d'attaque contre des applications métiers critiques. La protection DoS/DDoS en ligne neutralise les attaques par inondation dans les secondes qui suivent leur arrivée 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 mitigation en ligne bloquent les attaques en quelques secondes

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

Assurent la disponibilité des services grâce à une gestion dynamique de la congestion et une priorisation des applications critiques



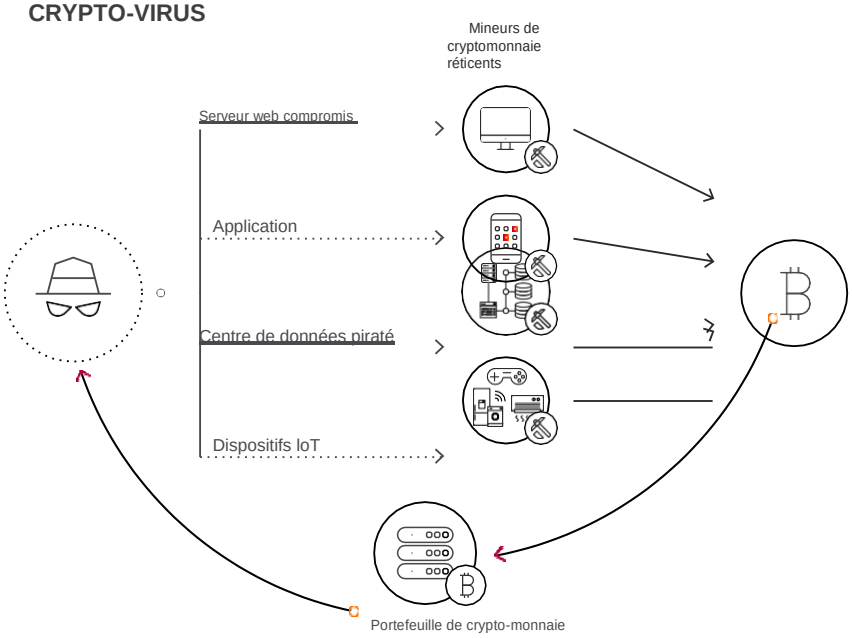
ADMINISTRATIONS PUBLIQUES LOCALES ET NATIONALES

IDENTIFICATION ET MITIGATION 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'exploitation gratuit la puissance CPU et GPU située dans les entreprises et les 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. NetworkSecure et Secure Service Gateway d'Allot peuvent identifier cette activité 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 reconnaissance des protocoles et des applications de minage de crypto-monnaie
- Empêche le piratage des ressources des serveurs Et 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 Mitigation du crypto-jacking

- 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 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 grâce à votre réseau qui l'activité se porte bien.

Comme il est démontré dans les cas d'utilisation présentés dans cette brochure, le SSG d'Allot apporte une forte valeur ajoutée aux opérations, à la planification et à votre entreprise. Tous nos clients ont constaté des avantages immédiats dès qu'ils ont braqué les projecteurs sur leur réseau 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.

En général, la performance des processus métiers laisse à désirer pour les raisons suivantes :

- Le flux des applications qui composent le processus est rompu
- Le réseau connaît des congestions et d'autres problèmes de trafic ou d'équipement
- Des anomalies liées à la sécurité affectent le service ou provoquent un déni de service

Des solutions 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. 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 de mesurer tout élément de politique statique ou dynamique que vous aurez défini.

Le plus apporté par la Visibilité fournira également au service informatique des informations sur la manière d'augmenter les performances du réseau. Par exemple, en voyant quels employés utilisent quelles applications et quand, vous pourrez hiérarchiser le trafic et définir des politiques de gestion du trafic qui répondent à vos objectifs métiers et aux attentes des utilisateurs, ainsi que prendre des décisions en toute 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