allot
See. Control. Secure.

Cas d'usage

Enseignement supérieur

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 client applicables au secteur de l'enseignement supérieur. Chaque cas présente une problématique spécifique rencontrée par les entreprises 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 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 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.

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.

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

- Permet l'utilisation d'appareils personnels pour améliorer la productivité des employés de l'entreprise
- Assure que les appareils personnels ne perturbent pas le réseau
- Renforce les mesures de sécurité du réseau

Permet d'utiliser des dispositifs personnels à des fins professionnelles

- Tient compte des règles BYOD dans le cadre de la stratégie de gestion Wi-Fi
- Détecte automatiquement le trafic provenant d'appareils personnels
- Applique en temps réel les règles liées aux BYOD
- Examine les rapports d'utilisation du BYOD pour évaluer et affiner la politique

Généré par Secure Service Gateway (SSG) d'Allot

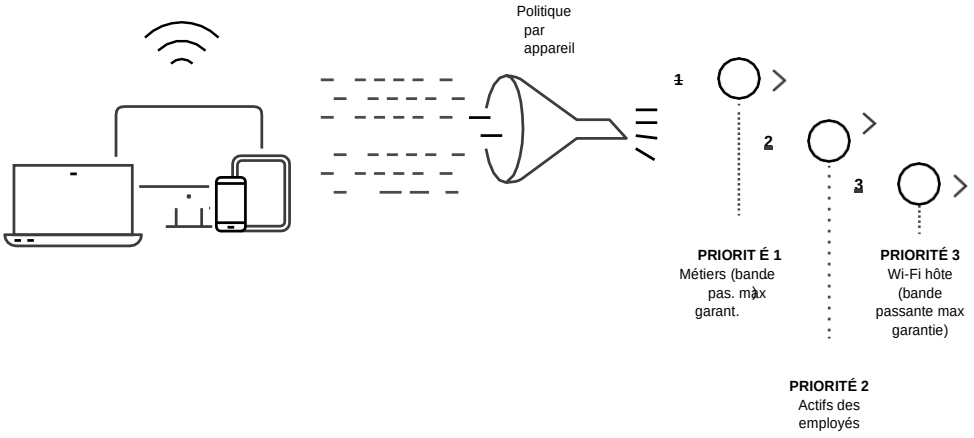
- Gestionnaire de passerelle Allot
- ClearSee Analytics d'Allot

ENSEIGNEMENT SUPÉRIEUR

BRING YOUR OWN DEVICE (BYOD) ou APPORTEZ VOTRE APPAREIL PERSONNEL

Alors que de nombreux responsables informatiques considèrent le Bring-Your-Own-Device (BYOD) comme un casse-tête de plus qui ouvre la porte à des risques de sécurité sur le réseau, les utilisateurs y voient une formidable source de productivité et d'efficacité personnelles. Les entreprises doivent pouvoir appliquer les règles de contrôle sur des appareils personnels nomades une fois qu'ils sont sur le réseau. Par exemple, les règles liées au BYOD peuvent inclure une limitation en cas d'utilisation intensive, l'allocation de plus de bande passante aux appareils professionnels des salariés par rapport aux appareils des clients et la priorité aux applications métiers. La haute technologie d'inspection approfondie des paquets (Deep Packet Inspection, DPI) d'Allot fournit des signatures d'équipements de la même manière qu'elle fournit des signatures d'applicatives qui sont mises à jour régulièrement par le net. Cela garantit une identification rapide et précise des appareils qui n'appartiennent pas à l'entreprise et de leur trafic réseau.

BYOD

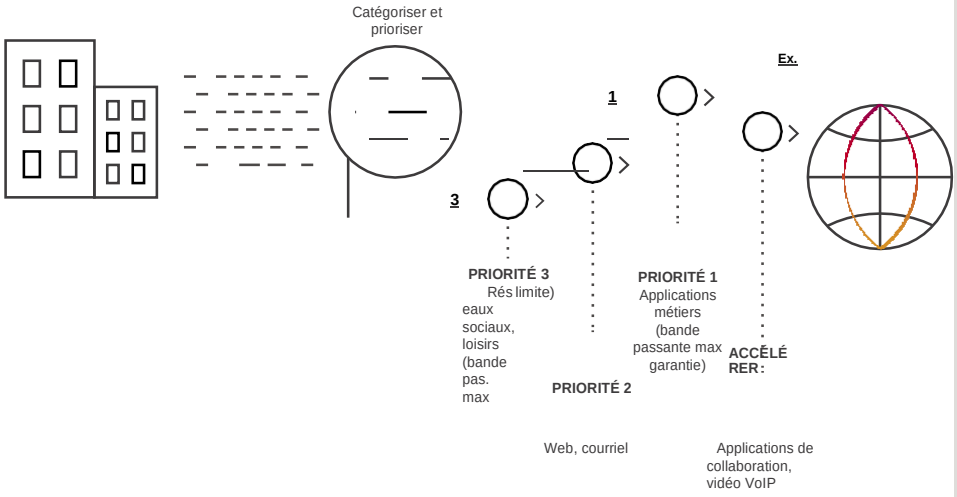


ENSEIGNEMENT SUPÉRIEUR

PRIORISATION DES APPLICATIONS MÉTIERS

Chaque entreprise s'appuie sur des applications en réseau pour mener à bien ses activités éducatives. Dans le monde connecté d'aujourd'hui, les réseaux informatiques utilisent de nombreuses applications allant des loisirs aux applications critiques pour l'entreprise. Pour qu'un établissement d'enseignement fonctionne efficacement, l'équipe informatique doit garantir la disponibilité des applications et le temps de réponse à tous les utilisateurs et à tous les accès distants, Internet et nomades. La Visibilité des applications permet de 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.

MIGRATION VERS LE CLOUD ET APPLICATIONS MÉTIERS



Sur la base d'une analyse approfondie, chaque application reçoit une politique de QoS personnalisée, qui peut définir des seuils de congestion ainsi qu'une certaine forme de transfert accéléré (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.

Dans l'ensemble, ces paramètres garantissent que les processus d'enseignement et de formation, la gestion des ressources humaines et les systèmes de contrôle financier et juridique peuvent fonctionner de manière plus productive et plus efficace.

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 de l'entreprise
- Permet d'investir au besoin dans l'expansion de l'infrastructure pour répondre aux exigences en matière d'éducation

Application métier Priorisation en action

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

Généré par Secure Service Gateway (SSG) d'Allot

- Gestionnaire de passerelle Allot
- ClearSee Analytics d'Allot

Atouts majeurs

- Garantit les performances des applications essentielles à l'éducation
- Réduit le temps et les coûts impliqués dans le dépannage d'un réseau de campus
- Permet d'éviter les mises à niveau coûteuses du réseau étendu (WAN)

Contrôle des congestions des campus

- Surveillance et analyse de l'utilisation du réseau
- Définit une politique de répartition des ressources équitable pour chaque campus, application, utilisateur et heure de la journée
- Applique la politique basée sur la congestion et d'autres déclencheurs temps réel
- Dépanne et réagit aux alertes lorsqu'elles se produisent

Généré par Secure Service Gateway (SSG) d'Allot

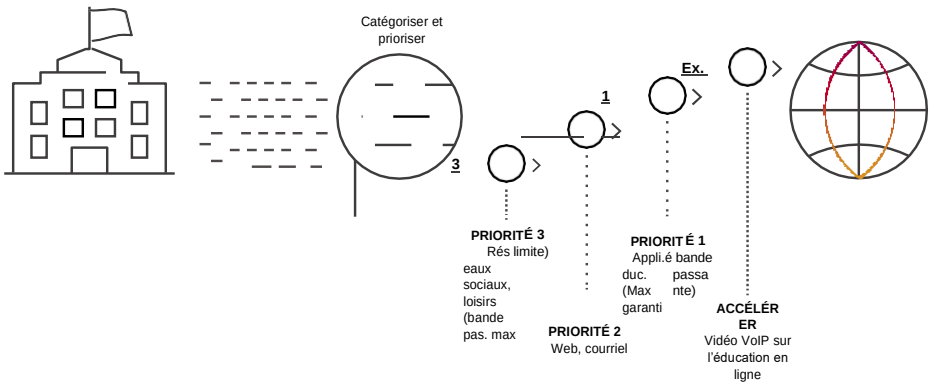
- Gestionnaire de passerelle d'Allot

ENSEIGNEMENT SUPÉRIEUR

CONTRÔLE DE CONGESTION DU TRAFIC DES CAMPUS

Les universités et les lycées se retrouvent dans le rôle de fournisseur de services Internet (ISP), délivrant des services réseau et Internet aux étudiants, aux facultés, aux administrateurs et aux invités situés sur plusieurs campus qui sont organisés autour d'une topologie WAN Au Hub principal du campus. La connectivité Internet, apparemment « gratuite » et omniprésente, peut facilement surcharger le WAN du campus avec le streaming vidéo/audio de loisir, les téléchargements P2P, les réseaux sociaux et les appels VoIP, en supplément des applications éducatives exigeantes qu'elle doit prendre en charge. Les solutions basées sur le DPI contrôlent avec succès la congestion du WAN en appliquant une politique équitable de répartition des ressources, qui peut inclure des limites d'utilisation, des trafics limités pour les applications de loisir, un transfert garanti pour les conférences vidéo et l'apprentissage à distance, ainsi que le blocage aux heures de pointe du trafic P2P.
Les réseaux de campus ont également été des victimes indirectes d'attaques DDoS liées aux activités de jeu en ligne des étudiants et des victimes directes d'activités malveillantes. Grâce à la combinaison d'une gestion avancée du trafic et d'une détection et d'une mitigation comportementales des DDoS, les plateformes Allot SSG peuvent protéger le réseau du campus et garantir un impact minimal sur les applications essentielles à l'éducation.

MIGRATION VERS LE CLOUD DES APPLICATIONS DU CAMPUS

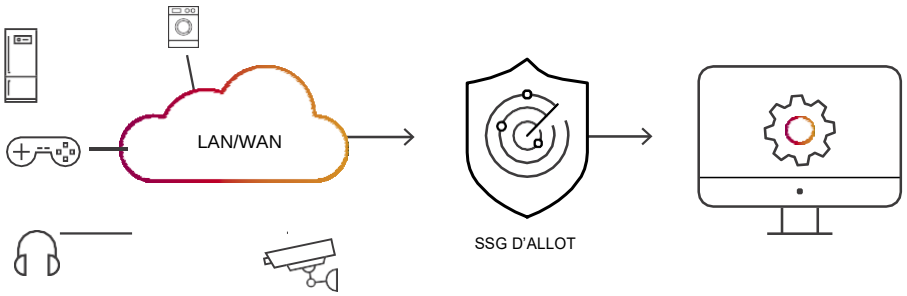


ENSEIGNEMENT SUPÉRIEUR

L'INTELLIGENCE INTERNET DES OBJETS (IOT)

Les appareils 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'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 IoT, les performances et l'intégrité du réseau. Les solutions de sécurité Allot surveillent les taux d'établissement de connexion et d'autres symptômes de comportement anormal 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 ASSURE LA VISIBILITÉ, LA SÉCURITÉ ET LE CONTRÔLE IOT



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 – 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), 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

Atouts majeurs

- Permet d'accepter un large éventail de charges de travail d'étudiants et d'enseignants
- Aligne l'accès à Internet et l'allocation des ressources aux priorités éducatives
- Contrôle les coûts d'accès au cloud

Gère la migration vers le cloud

- Priorise les applications Cloud et limite le trafic Internet non lié à l'enseignement
- Applique un contrôle dynamique de congestion du tarfic 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

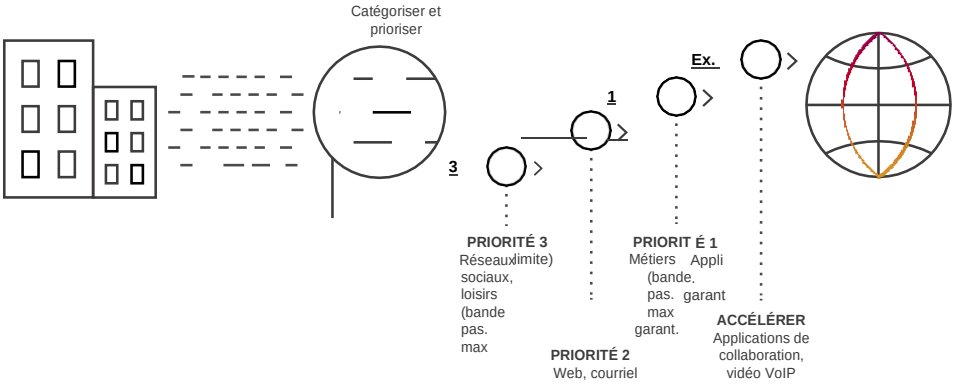
Généré par Secure Service Gateway (SSG) d'Allot

- Gestionnaire de passerelle Allot
- ClearSee Analytics d'Allot

ENSEIGNEMENT SUPÉRIEUR
GÉRER LA MIGRATION VERS LE CLOUD

De nombreux établissements d'enseignement migrent les applications de leurs centres de données privés vers des applications basées sur le Cloud. Par exemple, les serveurs d'échanges et de collaboration sont remplacés par Office 365 et CRM sur site avec Salesforce. Les avantages de la migration vers le Cloud sont d'un coût réduit, un accès universel et une maintenance zéro, et pourtant de nombreuses entreprises ont eu la mauvaise surprise de recevoir une facture élevée en raison d'utilisations inattendues. 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 établissements éducatifs de surveiller l'utilisation et le comportement des applications basées sur le Cloud et d'appliquer au contenu personnel les priorités et les engagements de SLA, notamment, en terme de débit de données (bande passante Internet) valable pour les applications de l'enseignement supérieur. 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 perçue et celle reçue par l'utilisateur final. Grâce à des rapports d'utilisation granulaires, des mises à niveau effectuées à bon escient vont pouvoir apporter leur concours aux établissements d'enseignement supérieur.

MIGRATION VERS LE CLOUD ET LES APPLICATIONS MÉTIERS

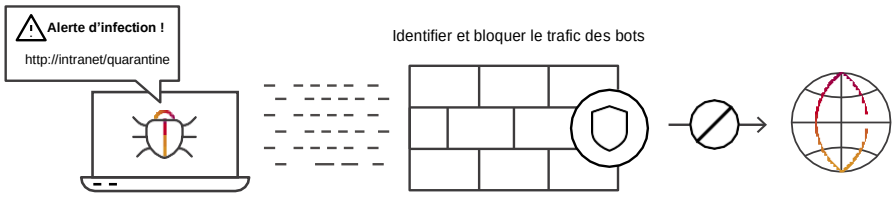


ENSEIGNEMENT SUPÉRIEUR

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 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 AUX INFECTIONS



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

- Détection d'un comportement anormal de l'hôte liée aux 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

- 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

Mitigation des attaques DDoS en temps réel

- Détection et mitigation en ligne en quelques secondes. Fournit une correction immédiate pour les attaques de courte durée
- Détecte les anomalies de trafic compatibles avec les 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'attaques
- 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

ENSEIGNEMENT SUPÉRIEUR

MITIGATION DES ATTAQUES DDOS EN TEMPS RÉEL

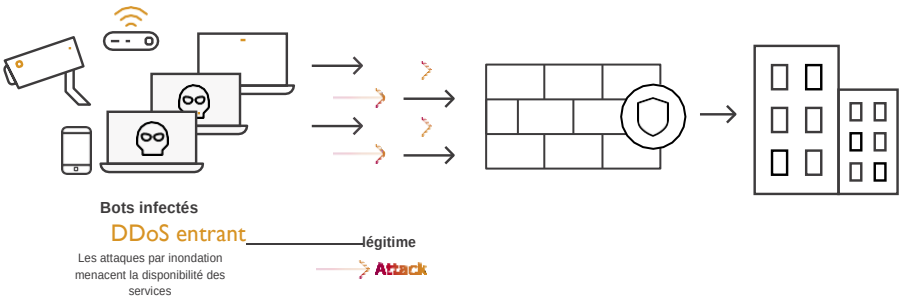
Les attaques DDoS gagnent en intensité et en sophistication chaque année, comme les attaques « memcached » et les attaques de courte durée qui se confondent avec les solutions de mitigation DDoS basées sur le Cloud. Alors que les centres de données sont au cœur du fonctionnement des organisations modernes, 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 grâce contre des applications métiers critiques. La protection DoS/DDoS en ligne neutralise les attaques par inondation dans les secondes qui suivent l'émergence en détectant, identifiant et filtrant rapidement les paquets DDoS, tout en permettant au trafic légitime de circuler librement.

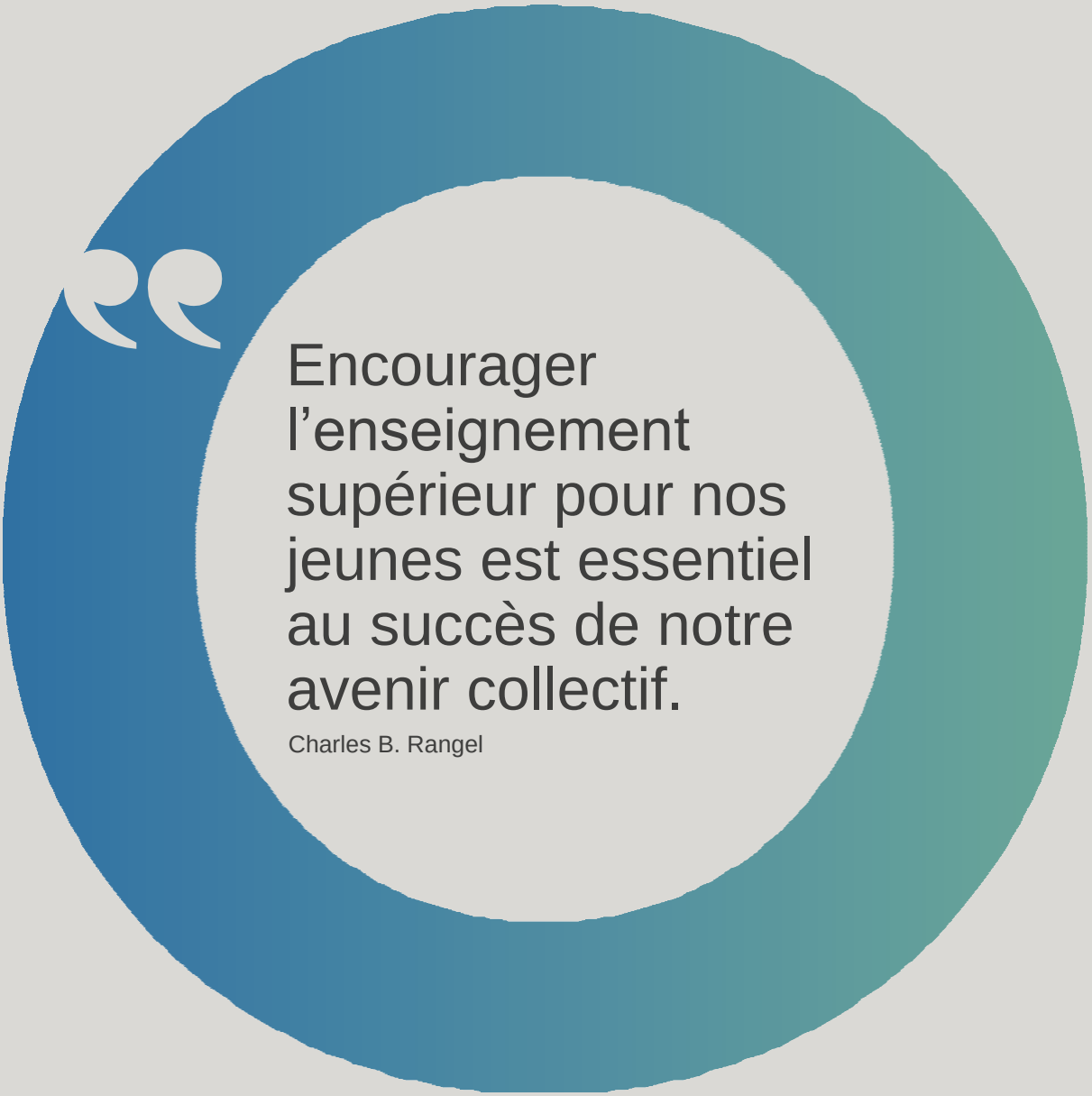
PROTECTION ANTI-DDoS

La détection et mitigation en ligne bloquent les attaques en quelques secondes

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

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




Encourager l'enseignement supérieur pour nos jeunes est essentiel au succès de notre avenir collectif.
Charles B. Rangel

Atouts majeurs

- Empêche la congestion du trafic du réseau Wi-Fi
- Assure la disponibilité du service Wi-Fi à tous les utilisateurs
- Amélioration de la satisfaction client

Optimisation Wi-Fi en action

- Alignement des conditions de congestion de trafic aux règles de politique de QoS
- Le seuil d'utilisation déclenche automatiquement l'application de la politique d'utilisation équitable
- Limite le débit de tous les utilisateurs ou uniquement des utilisateurs excessifs
- Restaure automatiquement la politique régulière lorsque la congestion de trafic diminue

Généré par Secure Service Gateway (SSG) d'Allot

- DDoS Secure d'Allot

ENSEIGNEMENT SUPÉRIEUR
OPTIMISATION WI-FI

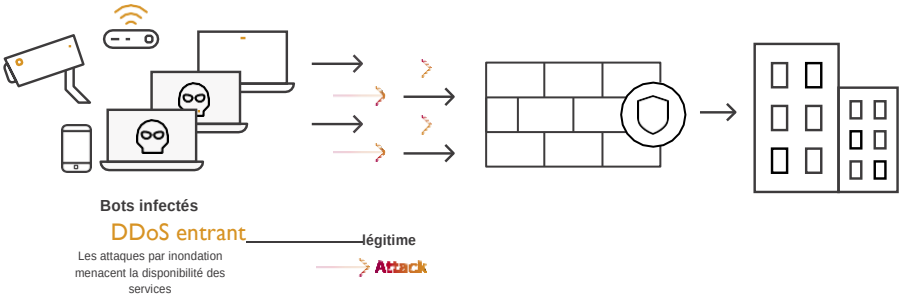
Un nombre croissant d'établissements d'enseignement supérieur offrent un service Wi-Fi pour fournir des services Internet à leur personnel et à leurs étudiants afin d'améliorer leur expérience éducative sur le campus. Ce service peut être facilement monopolisé par quelques gros utilisateurs et nécessite donc une gestion équitable des ressources réseau. Par exemple, un établissement d'enseignement supérieur ne peut pas permettre à ses étudiants de monopoliser sa bande passante Internet en regardant ou en téléchargeant des vidéos haute définition aux heures de cours. Les solutions basées sur le DPI permettent à ces établissements de surveiller l'utilisation du Wi-Fi en temps réel et d'appliquer la QoS en fonction des conditions dynamiques du réseau.

PROTECTION ANTI-DDoS

La détection et l'atténuation 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



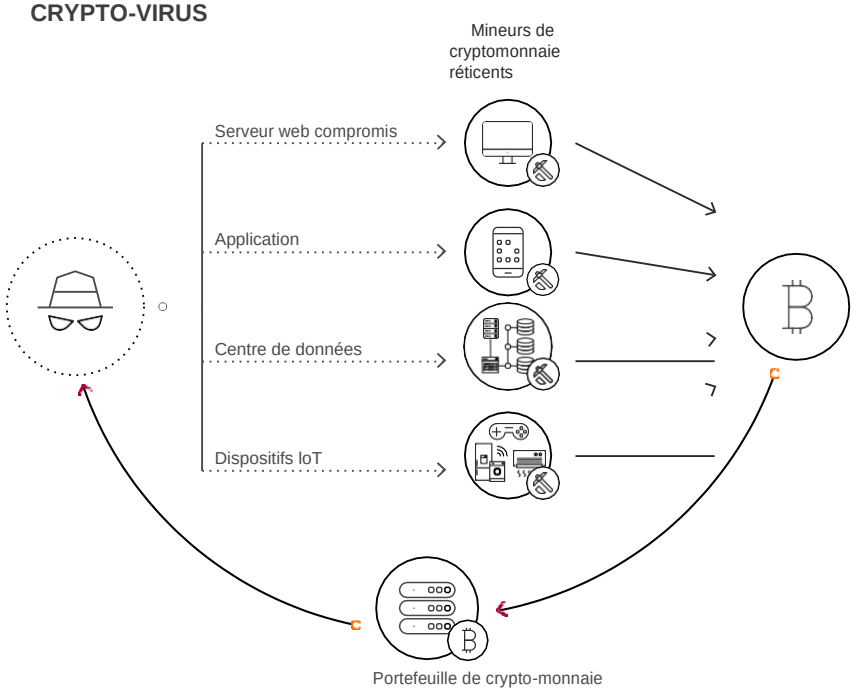
ENSEIGNEMENT SUPÉRIEUR

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'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 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 cryptomonnaie Monero
- Large reconnaissance et application des politiques de protocoles et d'applications de minage de cryptomonnaie
- Empêche le piratage des ressources du serveur 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 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 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 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