La Sécurité du réseau avec Allot

Allot DDoS Secure

Protection DDoS et Mitigation des cyberattaques pour les clients des réseaux d'opérateurs (MPLS, Internet, …)

Vous devez protéger votre réseau de données contre l'ampleur et la complexité croissantes des cyberattaques entrantes et sortantes qui sont conçues pour inonder votre infrastructure réseau et perturber la disponibilité des services. Les fournisseurs de services mobiles, fixes et Cloud du monde entier s'appuient sur Allot DDoS Secure pour assurer la mitigation ou endiguer rapidement les attaques volumétriques DoS/DDoS et neutraliser les attaques sortantes avant qu'elles n'affectent les services réseau et la continuité des activités.

Bénéfices

Protection DDoS en ligne et en temps réel

- Protéger les pare-feux, les routeurs et les serveurs opérationnels pendant les attaques DDoS
- Se préparer à arrêter même les plus grosses attaques en térabits par seconde
- Endiguer les attaques en quelques secondes et en temps réel sans passer par les centres de nettoyage Cloud
- La mitigation chirurgicale en ligne assure que seul le trafic non professionnel est touché et pas le trafic professionnel.

Puissante mitigation des menaces sortantes

- Détection automatique de l'activité des botnets/spammeurs IoT, dysfonctionnement des équipements
- L'isolation automatique des équipements infectés garantit la disponibilité du réseau
- Détectez et endiguez les attaques DDoS sortantes, sur place, jusqu'à des vitesses de plusieurs Térabits/seconde
- Évitez les listes noires IP et les dommages de réputation liés aux attaques sortantes émanant de votre réseau

Visibilité et Détection intelligente des causes

- Obtenez une visibilité temps réel des attaquants et des cibles sur votre réseau.
- Utilisez la criminalistique et des analyses d'attaques détaillées pour traiter la cause source des équipements infectés et améliorez votre stratégie de défense DDoS

Flexibilité et économies de coûts

- Améliorez votre efficacité grâce au déploiement sur Site, dans le Cloud ou en Hybride
- Protégez les réseaux mobiles, fixes et convergents, y compris les flux de trafics asymétriques
- Accélérez le retour sur investissement grâce à une intégration totale dans Allot Service Gateway
- Éliminez le trafic non conforme du réseau et différez les mises à niveau de l'infrastructure réseau

allot See. Control. Secure.

Caractéristiques

Protection DDoS en temps réel

Allot DDoS Secure vous aide à détecter et bloquer chirurgicalement les attaques par déni de service (DoS/DDoS) en quelques secondes, et avant qu'elles ne puissent menacer ou perturber votre service réseau. Notre technologie NBAD (Advanced Network Behavior Anomaly Detection) identifie les attaques volumétriques par les anomalies qu'elles provoquent dans le comportement, normalement invariable, des statistiques au cours du temps relatives au taux de paquets de couche 3 et de couche 4. Allot inspecte chaque paquet de votre réseau pour vous assurer qu'aucune menace n'est présente. La création dynamique de règles de mitigation et de filtrage chirurgical des paquets d'attaques vous aide à éviter des blocages inutiles et permet au trafic légitime de circuler librement, en gardant votre réseau d'entreprise accessible et protégé à tout moment.

Confinement des menaces sortantes

DDoS Secure d'Allot détecte et bloque automatiquement la propagation des vers sortants, l'analyse des ports et le trafic IoT généré par les points terminaux infectés par des bots, afin que vous puissiez empêcher la mise sur liste noire du réseau et éliminer la charge de trafic supplémentaire sur votre réseau. Notre technologie HBAD (Advanced Host Behavior Anomaly Detection) identifie l'infection de l'hôte et les comportements abusifs en fonction de l'activité de connexion sortante anormale et malveillante et des modèles de connexion, ce qui vous permet de maintenir le trafic anormal hors du réseau et de traiter la cause première de la menace ainsi que le symptôme.

Visibilité des menaces et rapports

Les alertes en temps réel vous informent lorsqu'une menace est détectée et lorsqu'elle a été atténuée. Les appareils infectés peuvent également recevoir une notification. Allot fournit des journaux détaillés et personnalisables d'atténuation des attaques, des analyses d'événements, des analyses d'infection d'hôte et des rapports de tendance/distribution pour prendre en charge votre planification de la sécurité, la gestion des menaces et les décisions opérationnelles. Un tableau de bord unique du contrôleur de gestion surveille l'activité du réseau et des utilisateurs et gère la protection contre les menaces sur l'ensemble de votre réseau.

Protection évolutive permanente

DDoS Secure d'Allot fonctionne dans un cadre unifié pour la délivrance de services, la sécurité et la monétisation, optimisées par Allot Service Gateway et offrant des performances de pointe pour se défendre contre les plus grandes attaques volumétriques pouvant atteindre plusieurs térabits par seconde. La plate-forme de classe opérateur d'Allot offre une haute disponibilité intégrée, une double alimentation et un bypass interne pour maximiser la disponibilité et la tolérance aux pannes. Plusieurs plates-formes peuvent être groupées pour suivre une prolifération éventuelle des menaces.

Déploiement flexible et Gestion centralisée

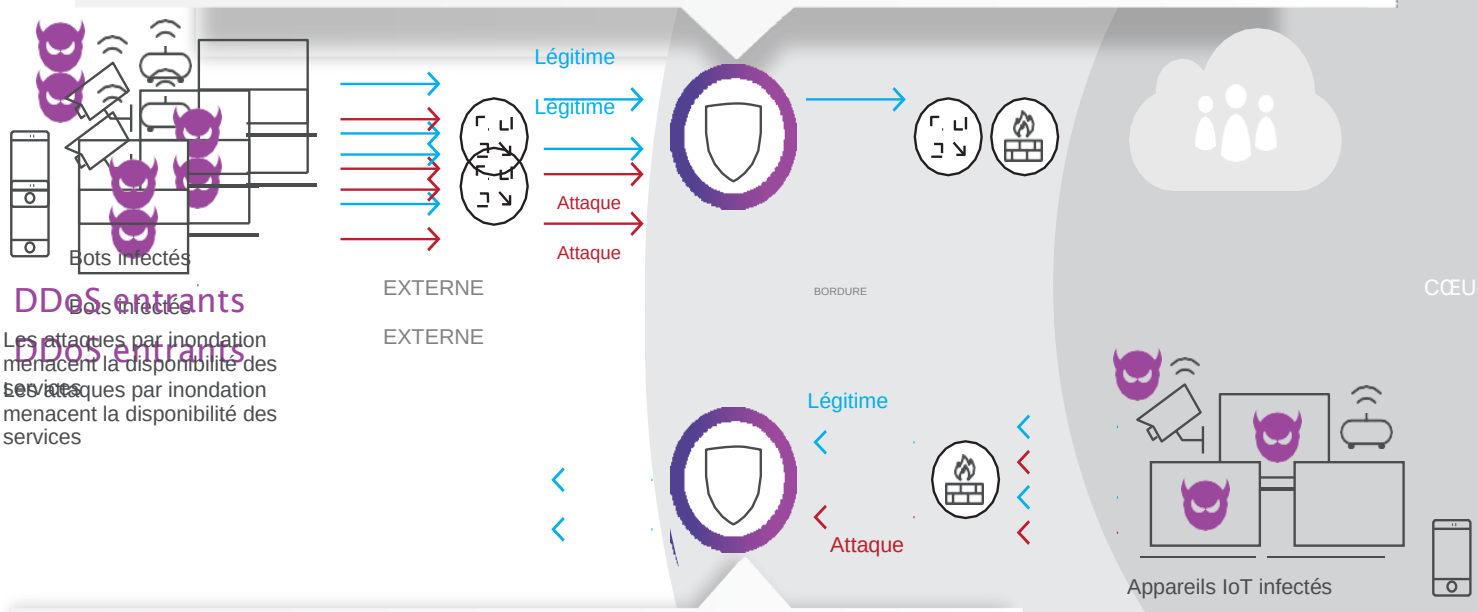
Allot DDoS Secure prend en charge les déploiements sur site, Cloud, hybrides et virtuels avec une gestion centrale des contrôleurs afin que vous obteniez la solution de sécurité qui répond de manière la plus efficace à votre besoin réseau. Allot prend également en charge la détection et la mitigation précises des attaques DDoS en mode NAT

Allot Protection DDoS

1. Endiguer les attaques en quelques secondes
Éliminer les congestions sur liaisons WAN coûteuses

2. Protéger le périmètre
Préviens les surcharges routeurs, Firewall, …

3. Assurer la disponibilité des services
Permet au trafic légitime de circuler librement



DDoS entrants

Les attaques par inondation menacent la disponibilité des services

DDoS entrants

Les attaques par inondation menacent la disponibilité des services

Trafic de botnets sortant ?

Trafic illégitime des botnets qui congestionne le réseau

Allot assure aussi la mitigation des bots

1. Garantie QoE
Prioriser les applications critiques pendant les attaques DDoS

2. Bloquer le trafic des Botnets
Seul le trafic du Botnet est bloqué alors que le trafic légitime, derrière l'IP NAT, circule librement

3. Isoler les bots
Isoler les bots du reste du réseau et bloquer les tentatives de propagation de l'infection

Traitement des environnements asymétriques

Déployé aux points critiques de votre réseau, Allot DDoS Secure fournit des informations cruciales et une protection efficace contre le nombre toujours croissant des cyberattaques entrantes et sortantes qui menacent votre entreprise

Spécifications

DDoS Secure d'Allot

Allot DDoS Secure comprend un capteur activé par licence et un contrôleur de gestion central. Allot Service Gateway fournit des informations sur la détection des capteurs et des fonctionnalités de mitigation de manière chirurgicale. Le contrôleur analyse les données qu'il reçoit des capteurs déployés sur le réseau et crée automatiquement un modèle de mitigation des attaques et le propage aux plates-formes Allot. Le tableau de bord de la console du contrôleur fournit également une interface graphique web pour la visibilité des attaques en temps réel, la criminalistique et des informations sur les menaces.

Security Coverage	Network-level DDoS Protection	Abusive Host Containment
Detection		
Approach	Network-based monitoring; traffic meta data collected directly from the network	
Technologies	Network Behavior Anomaly Detection (NBAD)	Host Behavior Anomaly Detection (HBAD)
Depth of Traffic Inspection	Modeling: Layer 3 and 4 packet headers are inspected to build HBAD flow data or NBAD network statistics Evidence/Analysis: Entire packet header and payload; 500 packets per automatic capture; Maximum of 25,000 packets for manual captures	
Supported Networks	Ethernet, VLAN, MPLS, L2TP, IPv4	
Types of Events	o High packet rate o Small packet size or large packet size o Fan-in or DDoS (many IPs to one IP); o Fan-out (one IP to many IPs); o Swarms (many IPs to many IPs); o DoS (one IP to one IP) o TCP based (SYN, FIN, ACK, RST, invalid flag combinations) o UDP based o ICMP (including echo request, echo reply, unreachable) o HTTP floods o Non-TCP floods (UDP, ICMP) o Attacks involving fragmented packets, truncated or malformed packets o Slow evolving attacks o Multiple targets attacks o Amplification attacks (DNS NTP, SNMPv2, LDAP)	o Address scan o Port scan o Flow bomb (bombarding the same target IP and port with a high number of flows) o Mass SMTP (address scanning or flow bombs to 25/TCP) o Mass DNS (address scanning or flow bombs to 53/UDP)
Detection Time	10-60 seconds	3 minutes
Reporting and Forensics	Attack packet logging, in-depth attack pattern analysis, attack details and statistics	
Web Based UI	Supported browsers: Chrome, I.E., Firefox, Safari	
Notifications	Email, syslog	
Enforcement Action		
Approach	o Traffic filtering using Allot dynamic packet signatures o Filtering occurs in-line and before further policy and bandwidth management	o Notification of subscriber/user via HTTP redirection on Allot Service Gateway platform and/or by triggering existing notification mechanisms (i.e. Email) o Per-subscriber traffic management by rate-limiting or blocking specific services (such as 25/TCP to prevent propagation of spam) o Per-subscriber solutions require Allot Subscriber Management Platform (SMP)
Allot Device/Platform Compatibility	Available on Allot Service Gateway platforms	Integrated with Allot SMP for per subscriber traffic enforcement
Third-party Compatibility	Filter recommendations provided in the following formats: SNORT, TCPDUMP, IPTABLES, Cisco ACL (IOS 12.4), Cisco PIX, JUNOS 9.4, Huawei (CX200D), Fortinet 2.80. No device integration.	BRAS
BGP Blackholing	10-60 seconds	

Spécifications

Allot DDoS Secure

Allot DDoS Secure Controller Virtual Edition	(Virtual DDoS Secure Controller (SPC-VE
Virtual Platform	
Virtual Network Function Orchestration	Openstack Neutron, VMWare vCloud Director 8.2, Nokia CIBAM, ECOMP/ONAP
Supported Hypervisor	VMWare EXXi 5.5+, RedHat RHEL 6.7 and above
Minimum Virtual Machine Requirements	vCPU: 32, vRAM: 64GB, vDISK: 1.2 TB

Allot DDoS Secure Sensor Virtual Edition	Allot Service Gateway Virtual Edition (SG-VE 32)
Virtual Platform	
Virtual Network Function Orchestration	Openstack Neutron, VMWare vCloud Director 8.2, Nokia CIBAM, ECOMP/ONAP
Supported Hypervisor	VMWare EXXi 5.5+, RedHat RHEL 6.7 and above
Minimum Virtual Machine Requirements	vCPU: 32, vRAM: 64GB, vDISK: 100GB
Performance	
Max Inspection Throughput per Instance	40 Gbps per instance (1.25Gbps per vCPU)
Max DDoS Flood Rate per instance	Line-rate

Allot DDoS Secure Controller Hardware	SPC 80	SPC 200
Capacity		
Sensors per Controller	Unlimited (per sizing)	
Hardware Specification		
Memory	32GB	64 GB
Storage	300 GB	1.2 TB
Processor	Intel Xeon E5-2620 v4 (8 Cores) 2.1 GHz	Dual Intel Xeon E5-2620 v4 (8 Cores) 2.1 GHz
Management		
Interface Media	8 x 10/100/1000 BASE-T (RJ-45)	
Traffic Encryption and Firewall Requirements	o User to SP-Controller: HTTPS and SSH o SP-Controller to Sensor: HTTP/HTTPS	
Management Traffic	100-500 Kbps Varies according to number of Groups, anomalies, packet size	
Console	VGA/USB and serial	
Availability		
High Availability modes	Inline failover bypass, , active passive cluster, solid-state hard drive RAID 10	
Dimensions, Mechanical		
Form Factor	Standard 1U in 19" rack; 43 mm x 440 mm x 711.4 mm (H x W x D)	
Weight	12.7–15.6 kg/28–34.5 lb	
Operating Temperature	50–95°F; 10–35°C (up to 3,000 ft/914.4 m); 50–90°F; 10–32°C (3,000–7,000 ft/914.4–2,133 m)	
Power Consumption	750 W (per PSU)	
Power Supply	AC , dual redundant, hot swappable	
Standards		
Certifications and Safety	FCC (Part 15 of the FCC Rules, Class A), ICES-003 (issue 5, Class A), UL/IEC 60950-1 CSA C22.2 No. 60950-1, NOM-019, Argentina IEC60950-1, Japan VCCI, Class A, Australia/New Zealand AS/NZS CISPR 22, Class A; AS/NZS 60950.1, China CCC GB4943.1, GB9254 Class A, GB17625.1, Taiwan BSMI CNS13438, Class A; CNS14336-1, Korea KN22, Class A; KN24, Russia, Belorussia and Kazakhstan, TR CU 020/2011 (for EMC) and TR CU 004/2011 (for safety), IEC 60950-1 (CB Certificate and CB Test Report), CE Mark (EN55022 Class A, EN60950-1, EN55024, EN61000-3- 2, EN61000-3-3), CISPR 22, Class A, TUV-GS (EN60950-1/IEC60950-1,EK1-ITB2000), RoHS Directive, Energy Star 2.0	

Spécifications

Allot DDoS Secure

Allot DDoS Secure Sensor Hardware	Allot Service Gateway (Blade Center)	Allot Service Gateway 9500 (Appliance)
Performance		
Max Throughput per unit (PPS)	80 Million	20 Million
Max Throughput per unit (Gbps)	500 Gbps	125 Gbps
Max Number of Connections/Flows	360 Million/720 Million	24,000,000/48,000,000
Max Number of End-Points	15,000,000	4,000,000
Max SYN Flood Attack Rate	70 Gbps 135 Million SYNs per second	14 Gbps 28 Million SYNs per second
Latency (micro-seconds)	10-20	10-20
Hardware Specification		
Memory	64 GB (per CC-400)	256 GB
Processor	BROADCOM	Dual Intel Xeon E5-2680 v4 (14 Cores) 3.30 GHz
Operating System	Allot Operating System (AOS)	Allot Operating System (AOS)
Interfaces		
Ethernet Interfaces	96 x 10 Gigabit Ethernet 8 x 100 Gigabit Ethernet	24 x 10 Gigabit Ethernet
Management	2 x 1 Gigabit Ethernet or 2 x 10 Gigabit Ethernet (with 1:1 high availability)	2 x 10 Gigabit Ethernet or 2 x 1 Gigabit Ethernet
Console	Serial, RJ45 Connector	SSH, HP iLO
Availability		
Hardware Bypass	Up to 4 independent, passive bypass units, supporting either 8 fiber-optic ports (4 links), or 16 fiber-optic ports (8 links), or 24 fiber-optic ports (12 links) per unit	Up to 2 independent, passive bypass units, supporting either 8 fiber-optic ports (4 links), or 16 fiber-optic ports (8 links), or 24 fiber-optic ports (12 links) per unit
High Availability	1+1 system-level redundancy N+1 redundancy of Core Controller blades	Active redundancy (1:1, 1+1)
Management	Active-Standby HA on management ports	Active-Standby HA on management ports
System	Redundancy for PSUs and fans	Redundancy for PSUs and fans
Max Groups per Sensor	30	30
Mechanical and Environmental		
Form Factor	Standard 14U by 19" rack mount	2U 19" rack mount
Dimensions	Height 619.5mm (24.3"), width 444mm (17.48"), depth 433.04mm (17.04"), with PEMs	8.73 x 44 .55 x 73.02 cm (3.44 x 17.54 x 28.75 in) , dimensions without Bezel
Weight	Up to 87.6 kg (193 lb)	Min 32.6 lb (14.759 kg), Max 42 lb (19 kg) per number of NIC interfaces
Operating Temperature	5°C to 40°C (41°F to 104°F)	10°C to 35°C (50°F to 95°F)
Operating Humidity	5% to 85% RH	8% to 90% RH
Power Supply	Dual Hot Plug, Redundant 200-240VAC, 50/60Hz, 4 x 12A/240V Max 4 x 15A/100V Max or -48V DC (-40V to -60V DC), 2 x 190A Max	Dual Hot Plug, Redundant 100/240VAC or -48VDC, efficiency of up to 94%, Energy star, 80PLUS
Max Power Consumption	2,290W-5,076W	800W
Certifications and Safety	NEBS level 3, CE Conformity, EMC, RoHS, Safety (UL, EN), ISO 9001, ISO/IEC 90003, ISO 14001, SI ISO 27001	CE Conformity, EMC, RoHS, Safety (UL, EN), ISO 9001, ISO/IEC 90003, ISO 14001, SI ISO 27001

* Les mesures de débit et de performances réelles dépendent des fonctionnalités activées, de la configuration des stratégies, de la composition du trafic et d'autres caractéristiques de déploiement.

P/N D240020 Rév.8

sales@allot.com | www.allot.com