Allot Network Security

DDoS Secure

DDoS Protection and Threat Containment for Enterprises

You need to protect your data network against the increasing scale and complexity of inbound and outbound cyber attacks that are designed to flood your network infrastructure and disrupt service availability. Enterprises around the world rely on Allot DDoS Secure to rapidly mitigate volumetric DoS/DDoS attacks and neutralize outbound threats before they affect network service and business continuity.

Benefits

Reduce Business Risk and Network Down Time

- Scale to stop even the biggest attacks at Terabits-per-seconds
- Mitigate in seconds on the fly in seconds without diverting to cloud scrubbing centers
- DPI policies ensure no network element is overwhelmed and QoE is assured throughout attack

Avoid Brand Reputation Damage

- Surgical inline mitigation assures no over-blocking
- Block IoT botnet and spammer activity, to prevent IP blacklisting
- Detect and mitigate outbound DDoS attacks, on the spot, at Terabits/sec

Simplify and Streamline Security Operations

- View and manage your entire network security from a single point of control
- Gain real-time visibility of attackers and their targets in your network
- Use detailed attack forensics and analytics to treat the root cause of misbehaving endpoints and improve your DDoS defense strategy

Reduce CAPEX and OPEX

- Fully automatic, no manual intervention is required
- Drive efficiencies with on-premise, cloud, or hybrid deployment
- Keep even the smallest attacks off the network and defer capacity upgrades

Features

Real-time In-Line DDoS Protection

Detect and block Denial of Service attacks within seconds, before they can threaten or disrupt your network service. Every packet on your network is inspected to ensure no threat goes undetected.

Inbound and Outbound Protection

Automatically detect and block inbound DDoS attacks as well as outbound DDoS attacks, and abusive activity generated by compromised IoT and bot infected end-points.

Scalable Always-On Protection

Defend against the largest volumetric attacks with Tbps scalable platforms that features high-availability, dual power supply and internal bypass to maximize uptime and fault tolerance.

Real-time Threat Intelligence

A Centralized controller allows sharing attack information between inline sensors in real-time to proactively prevent them from happening in all parts of the network..

Comprehensive Attack Forensics

Investigate threats in real-time with detailed attack reporting, event analytics, and full packet analysis. Get notified in real-time on attack detection and mitigation.

Automatic Remote Mitigation

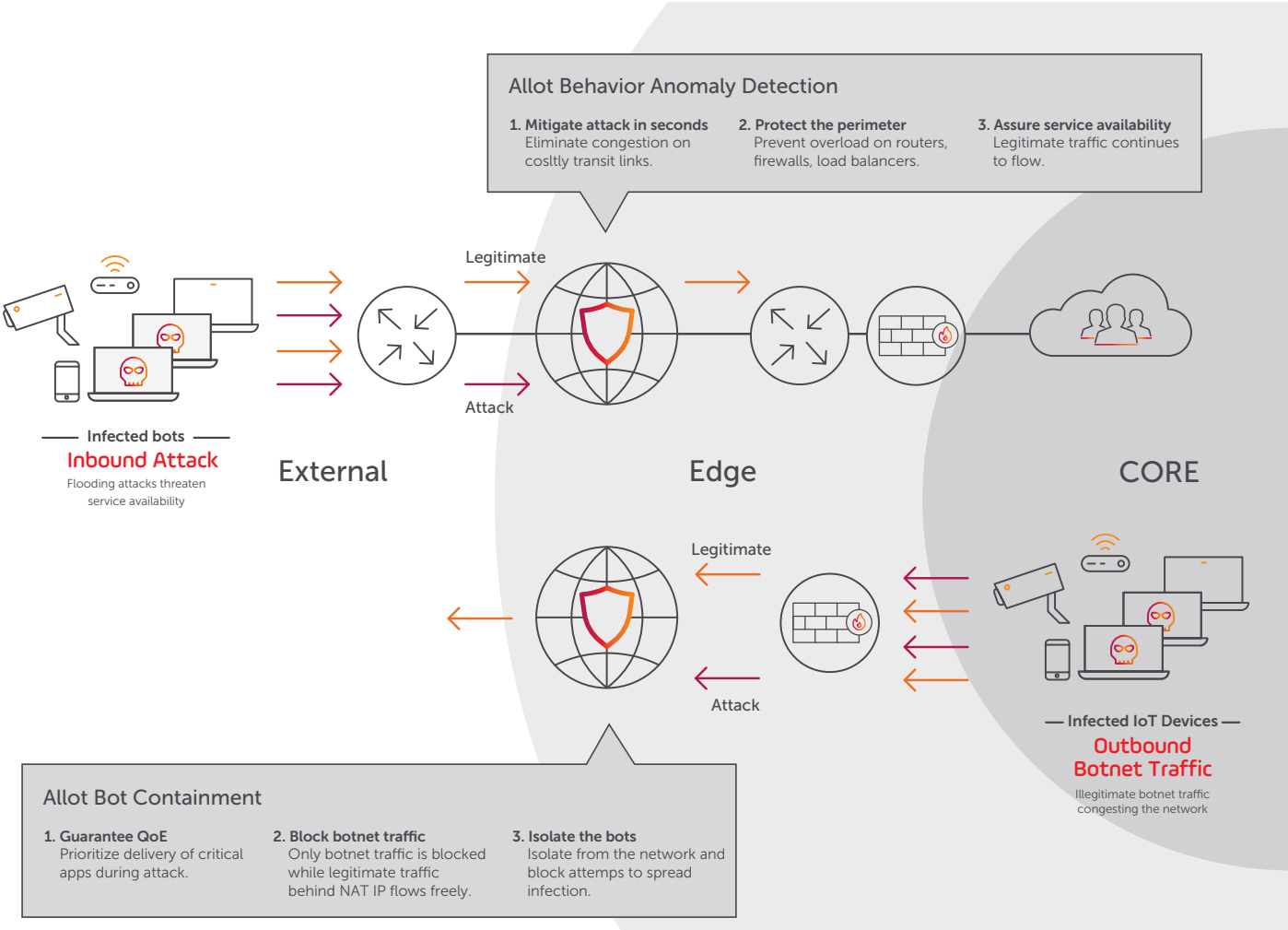
Signal upstream routers/firewalls to stop large attacks that can overwhelm your network infrastructure.

Managed Service Framework

Protect your network and increase your revenues by delivering DDoS Protection services to your customers with a multitenant framework which allows each customer to manage and view their own network.

Flexible Deploymentand Management

Get the solution that best fits your network and efficiency requirements whether on-premise, cloud, hybrid or virtual deployment.



Protect your network and increase your revenues by delivering DDoS Protection services to your customers with a multitenant framework which allows each customer to manage and view their own network.

Specifications

Allot DDoS Secure

Allot DDoS Secure comprises a license-activated Sensor and a central management Controller. Allot Service Gateways provide sensor detection information and surgical network-level mitigation functionality. The Controller assesses the network data it receives from deployed sensors and automatically creates an attack mitigation pattern and propagates it to enforcement platforms. The Controller console dashboard also provides a web GUI for real-time attack visibility, forensics and threat intelligence.

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 Attacks involving fragmented packets, truncated or malformed packets o Slow evolving attacks o Multiple targets attacks o Amplification attacks (DNS NTP, SNMP, LDAP) o Other floods (IGMP, SSDP, CHARGEN, QOTD, BT, Kad)	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
Small Attacks	Yes	
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, SNMP	
Integration with SIEM	Yes	
Network Analytics	Yes	
Mitigation		
Mitigation Time	15 Seconds	
Mitigation Action	Block, according to dynamically generated pattern	Mitigation per individual subscriber/host including: o Block o Rate-limit o Alert o Redirect to cleaning portal
Allot Device/Platform Compatibility	Available on Allot Service Gateway platforms	Integrated with Allot SMP for per subscriber traffic enforcement
Third-party Filtering Rules	SNORT, TCPDUMP, IPTABLES, Cisco ACL (IOS 12.4), Cisco PIX, JUNOS 9.4, Huawei (CX200D), Fortinet 2.80. No device integration.	BRAS
BGP Blackholing (RTBH)	Yes	N/A
IPv6	Yes	No
Session-aware Mitigation	Yes	N/A

Specifications

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 DDoS Secure 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	

Specifications

Allot DDoS Secure

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

*Actual throughput and performance metrics depend on enabled features, policy configuration, traffic mix, and other deployment characteristics.

NOTE: The specified DDoS sensors represent Allot's superior performance in supporting very large deployments.
Additional DDoS sensors for SG and SSG are available. Please contact your local Allot representative for more details.

June 2020