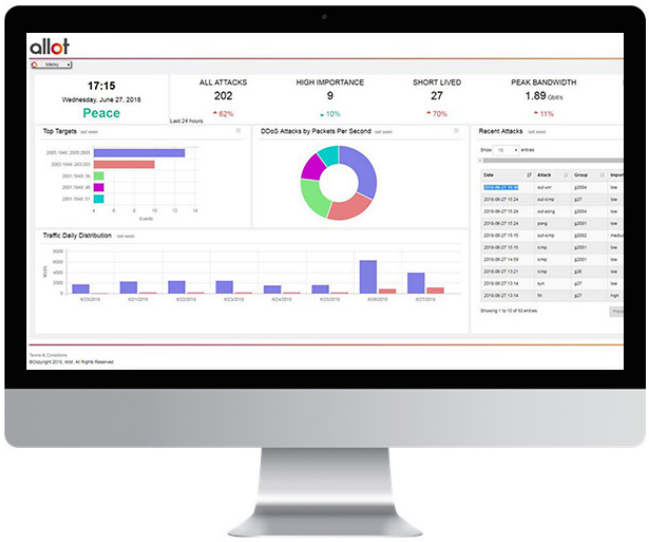
Traffic Intelligence and Assurance Platform

DDoS Secure for Enterprise

DDoS Protection and Threat Containment for Enterprises

Cyberattacks in today's digital world are on the rise, posing a significant risk on business reputation, continuity, and revenue. Enterprises around the world rely on Allot DDoS Secure for Enterprise to rapidly mitigate volumetric DoS/DDoS attacks and neutralize outbound threats before they affect network service and business continuity.



Allot DDoS Secure for Enterprise protects against fast moving, high volume, encrypted attacks or very short duration threats and provides the first line of defense against both inbound and outbound attacks.

Inbound DDoS attacks are automatically mitigated by discarding the DDoS traffic and allowing legitimate traffic to pass through. For outbound attacks, it identifies and then isolates possible threats originating from individual hosts that disrupt the performance and integrity of network infrastructure and services.

Benefits

Reduce Business Risk and Network Down Time

- Scale to stop even the biggest attacks at Terabits-per-seconds
- 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 and any compromised host 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

Multi-Layer Defense Strategy

Integrated with Allot's Secure Service Gateway (SSG) and Application Control Gateway (ACG-2000) platforms, DDoS Secure delivers a powerful multi-layer DDoS defense solution to protect your enterprise network. It combines proactive defense measures of policy-based traffic shaping using machine learning based anomaly detection. It prevents firewalls and routers from being overwhelmed and failing, by providing the required protection under the load of massive DDoS attacks. This is done by controlling the traffic to these network elements making sure they don`t receive more than they can handle. At the same time, it monitors the network to look for anomalies corresponding to DDoS attacks and automatically mitigates them in real time.

Real-time In-Line DDoS Protection

Detects and surgically blocks DoS/DDoS - attacks within seconds before they can threaten or disrupt the network service and applications. DDoS Secure inspects every packet on the network to ensure that no threat goes undetected. Allot advanced Network Behavior Anomaly Detection (NBAD) machine learning based technology accurately identifies zero-day DDOS attacks , detecting the anomalies they cause in the normally time-invariant behavior of Layer 3 and Layer 4 packets. Finally, the solution dynamically creates mitigation rules for surgical filtering of attack packets to enable legitimate traffic to flow through and avoids over-blocking, keeping your business online and protected, always.

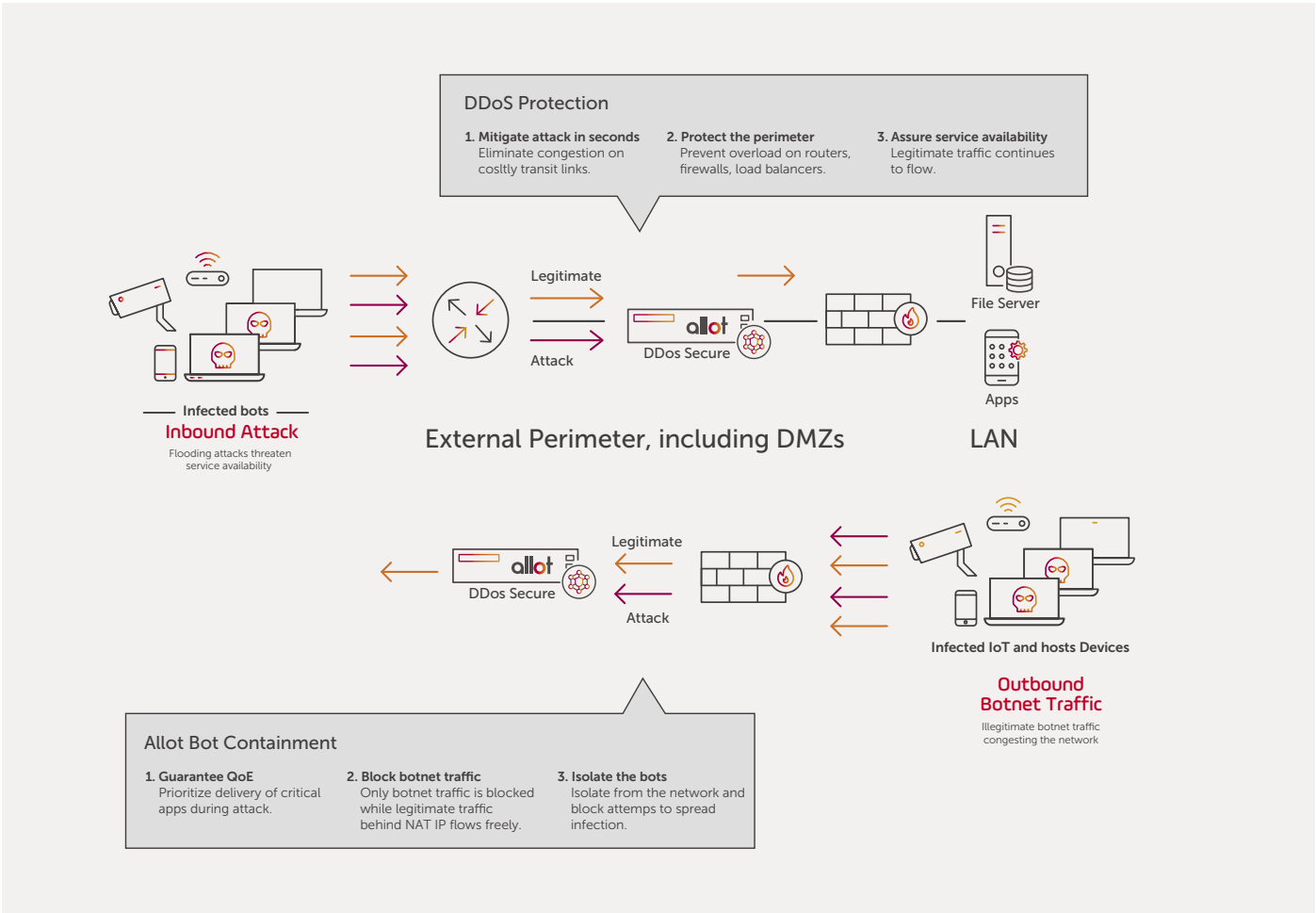
Outbound Threat Containment

Allot DDoS Secure automatically detects and blocks abusive or compromised users/ hosts participating in outbound worm propagation, port scanning as well as IoT traffic generated by bot-infected end points, so enterprises can prevent network blacklisting and eliminate additional traffic load on their network. Allot advanced Host Behavior Anomaly Detection (HBAD) technology identifies host infection and abusive behavior according to abnormal outbound connection activity and malicious connection patterns, enabling enterprises to keep anomalous traffic off the network and treat the root cause of the threat as well as the symptoms.

Real Time Threat Intelligence and Attack Forensics

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.

Graphical dashboards notify, in real-time, on attack detection and mitigation. Trend graphs and history statistics introduce a wide picture of DDoS attacks in your organization, enabling you insightful decision making and corrective action process, if required.



DDoS Secure for Enterprise In-Line Architecture

Specifications

Allot DDoS Secure for Enterprise

Allot DDoS Secure for Enterprise 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	Bot Containment
Detection		
Approach	Inline	
Technologies	Behavior Anomaly Detection and ML	Behavior Anomaly Detection
Depth of Traffic Inspection	Inspects entire packet headers and payload from network traffic collected directly from the network	
Supported Attacks	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 L3/L4 TCP attacks (SYN, FIN, ACK, RST, invalid flag combinations) o L3/L4 UDP attacks o Zero-day attacks o Long persistent attacks (up to 72h) o Pulsed attacks o ICMP (including echo request, echo reply, unreachable) o L7 HTTP floods o L7 SSL Floods o Attacks involving fragmented packets, truncated or malformed packets o Slow evolving attacks o Low-rate attacks (from 1000 pps/10 Gbps) o Multiple targets attacks o Fragmented packet floods (Frag. UDP Flood, Frag. TCP ACK flood, Frag. ICMP Flood) o IP spoofing attacks o Amplification attacks (DNS NTP, SNMP, LDAP) o Amplification attacks o L2/L3 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)
Reporting and Forensics	Attack packet logging, in-depth attack pattern analysis, attack details and statistics, Country and ASN	
Web Based UI	Supported browsers: Chrome, I.E., Firefox, Safari	
Notifications	Email, syslog, SNMP, Script	
Integration with SIEM	Yes	
Network Analytics	Yes	
IP Version	IPv4, IPv6	
Asymmetric Traffic Inspection	Yes	
Protection Groups	300	
Mitigation		
Mitigation Time	25 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
Network Compatibility	Available on Allot Service Gateway platforms	Integrated with Allot service provider subscriber traffic enforcement
BGP Blackholing (RTBH)	Yes	N/A
BGP Flowspec	Yes	N/A
Session-aware Mitigation	Yes	N/A

Specifications

Allot DDoS Secure for Enterprise

Allot DDoS Secure for Enterprise Controller Hardware	Allot DDoS Secure Controller 200	Allot DDoS Secure Controller 1000
Capacity		
Sensors per Controller	Up to 20	Up to 150
Managed Throughput	Up to 10 Tbps	Up to 75 Tbps
Hardware Specification		
Memory	64GB	1TB
Storage	2.8TB	23TB
Processor	Dual Intel Xeon Silver 4214 (12 Cores) 85W 2.2GHz	Dual Intel Xeon Platinum 8280 (28 Cores) 2.7GHz
Management		
Interface Media	4 x 10/100/1000 BASE-T (RJ-45)	1 x 10/100/1000 BASE-T (RJ-45), 2 x 10 Gbit/s SFP+
Traffic Encryption and Firewall Requirements	○ User to DS-Controller: HTTPS and SSH ○ DS-Controller to Sensor: HTTP/HTTPS	○ User to DS-Controller: HTTPS and SSH ○ DS-Controller to Sensor: HTTP/HTTPS
Management Traffic (Varies according to number of Sensors, Groups, anomalies, packet size)	200-1000 Kbps per Sensor	Up to 1.2 Gbit/s
Console	VGA/USB and serial	VGA/USB and serial
Availability		
High Availability modes	Inline failover bypass, active passive cluster, solid-state hard drive RAID 10	Inline failover bypass, active passive cluster, solidstate hard drive RAID 10
Dimensions, Mechanical		
Form Factor	Standard 1U in 19" rack 43 mm x 434 mm x 715 mm (H x W x D)	Standard 1U in 19" rack 43 mm x 434 mm x 715 mm (H x W x D)
Weight	11.9-18.8 kg/26.2-41.4 lb	11.9-18.8 kg/26.2-41.4 lb
Operating Temperature	10°C –35°C (50°F–95°F); (up to 3,000 ft/914.4 m); 10°C –32°C (50°F–90°F); (3,000–7,000 ft/914.4–2,133 m)	10°C –35°C (50°F–95°F); (up to 3,000 ft/914.4 m); 10°C –35°C (50°F–95°F); (3,000–7,000 ft/914.4–2,133 m)
Power Consumption	750 W (per PSU)	1100 W (per PSU)
Power Supply	AC, dual redundant, hot swappable	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	

Allot DDoS Secure for Enterprise Controller Virtual Edition

	Allot DDoS Secure Controller Virtual Edition (DSC-VE)
Virtual Platform	
Supported Hypervisor	VMWare vSphere 6.7+, KVM RHEL 7.6 and above
Minimum Virtual Machine Requirements	vCPU: 8, vRAM: 16GB, vDISK: 200GB

Allot DDoS Secure Sensor

	Allot Service Gateway 9500 (Appliance)	Allot Service Gateway 9700 (Appliance)
Performance		
Max Throughput per unit (PPS)*	20 Million	40 Million
Max Throughput per unit (Gbps)*	125 Gbps	300 Gbps
Max Number of Connections/Flows	24,000,000/48,000,000	72,000,000/144,000,000
Max Number of End-Points	4,000,000	9,000,000
Max SYN Flood Attack Rate	14 Gbps 28 Million SYNs per second	35 Gbps 70 Million SYNs per second
Latency (micro-seconds)	10-20	10-20
Hardware Specification		
Memory	256 GB	384 GB
Processor	Dual Intel Xeon E5-2680 v4 (14 Cores) 3.30 GHz	Dual Intel Xeon-Platinum 8168 (24 Cores) 2.7 GHz
Operating System	Allot Common Platform (ACP)	Allot Common Platform (ACP)
Interfaces		
Ethernet Interfaces	24 x 10 Gigabit Ethernet	40 x 10 Gigabit Ethernet
Management	2 x 10 Gigabit Ethernet or 2 x 1 Gigabit Ethernet	2 x 10 Gigabit Ethernet or 2 x 1 Gigabit Ethernet
Console	SSH, HP iLO	SSH, HP iLO
Availability		
Hardware Bypass	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	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	Active redundancy (1:1, 1+1)	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
Mechanical and Environmental		
Form Factor	2U 19" rack mount	2U 19" rack mount
Dimensions	8.73 x 44 .55 x 73.02 cm (3.44 x 17.54 x 28.75 in), dimensions without Bezel	8.73 x 44 .54 x 67.94 cm (3.44 x 17.54 x 26.75 in), dimensions without Bezel
Weight	Min 32.6 lb (14.759 kg), Max 42 lb (19 kg) per number of NIC interfaces	Min 32.75 lb (14.9 kg), Max 43 lbs (19.5 kg) per number of NIC interfaces
Operating Temperature	10°C to 35°C (50°F to 95°F)	10°C to 35°C (50°F to 95°F)
Operating Humidity	8% to 90% RH	8% to 90% RH
Power Supply	Dual Hot Plug, Redundant 100/240VAC or -48VDC, efficiency of up to 94%, Energy star, 80PLUS	Dual Hot Plug, Redundant 100/240VAC or -48VDC, efficiency of up to 94%, Energy star, 80PLUS
Max Power Consumption	800W	800W
Certifications and Safety	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

Specifications

	Allot Service Gateway Tera (Blade Center)
Performance	**Performance**
Max Throughput per Unit (PPS)*	80 Million
Max Throughput per Unit (Gbps)*	500 Gbps
Max Number of Connections/Flows	360 Million/720 Million
Max Number of End-Points	15,000,000
Max SYN Flood Attack Rate	70 Gbps 135 Million SYNs per second
Latency (micro-seconds)	10-20
Hardware Specification	**Hardware Specification**
Memory	64 GB (per CC-400)
Processor	BROADCOM
Operating System	Allot Operating System (AOS)
Interfaces	**Interfaces**
Ethernet Interfaces	96 x 10 Gigabit Ethernet 8 x 100 Gigabit Ethernet
Management	2 x 1 Gigabit Ethernet or 2 x 10 Gigabit Ethernet (with 1:1 high availability)
Console	Serial, RJ45 Connector
Availability	**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
High Availability	1+1 system-level redundancy N+1 redundancy of Core Controller blades
Management	Active-Standby HA on management ports
System	Redundancy for PSUs and fans
Mechanical and Environmental	**Mechanical and Environmental**
Form Factor	Standard 14U by 19" rack mount
Dimensions	Height 619.5mm (24.3"), width 444mm (17.48"), depth 433.04mm (17.04"), with PEMs
Weight	Up to 87.6 kg (193 lb)
Operating Temperature	5°C to 40°C (41°F to 104°F)
Operating Humidity	5% to 85% 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
Max Power Consumption	2,290W-5,076W
Certifications and Safety	NEBS level 3, CE Conformity, EMC, RoHS, Safety (UL, EN), ISO 9001, ISO/IEC 90003, ISO 14001, SI ISO 27001

	Allot Service Gateway Virtual Edition (SG-VE)
Virtual Platform	
Supported Hypervisor	VMWare vSphere 6.7 and above, KVM RHEL 7.6 and above
Minimum Virtual Machine Requirements	vCPU: 4, vRAM: 10GB, vDISK: 100GB
Performance	
Max Inspection Throughput per Instance	4 Gbps/4 Cores, 12 Gbps/8 Cores, 24Gbps/16 Cores, 48 Gbps/32 Cores
Max DDoS Flood Rate per instance	Line-rate

*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 2021