Allot Network Security

Allot DDoS Secure

DDoS Protection and Threat Containment for Service Provider Networks

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. Mobile, fixed and cloud service providers 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

Real-Time Inline DDoS Protection

- Keep firewalls, routers and servers up and running during DDoS attacks
- 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
- Surgical inline mitigation assures no over-blocking

Powerful Outbound Threat Containment

- Automatic detection of IoT botnet/spammer activity, device malfunction
- Automatic isolation of compromised devices assures network availability
- Detect and mitigate outbound DDoS attacks, on the spot, at Terabits/sec
- Avoid IP blacklisting and reputation damage from outbound attacks that originate in your network

Visibility and Root Cause Intelligence

- 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

Flexibility and Cost Savings

- Drive efficiencies with on-premise, cloud, or hybrid deployment
- Protect mobile, fixed and converged networks, including asymmetric traffic flows
- Accelerate ROI through full integration in Allot Service Gateway
- Keep anomalous traffic off the network and defer capacity upgrades

Features

Real-time DDoS Protection

Allot DDoS Secure helps you detect and surgically block Denial of Service (DoS/DDoS) attacks within seconds, before they are able to threaten or disrupt your network service. Our Advanced Network Behavior Anomaly Detection (NBAD) technology identifies volumetric attacks by the anomalies they cause in the normally time-invariant behavior of Layer 3 and Layer 4 packet rate statistics. Allot inspects every packet on your network to ensure that no threat goes undetected. Dynamic creation of mitigation rules and surgical filtering of attack packets helps you avoid over-blocking and allows legitimate traffic to flow unimpeded, keeping . your business online and protected at all times

Outbound Threat Containment

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

Threat Visibility and Reporting

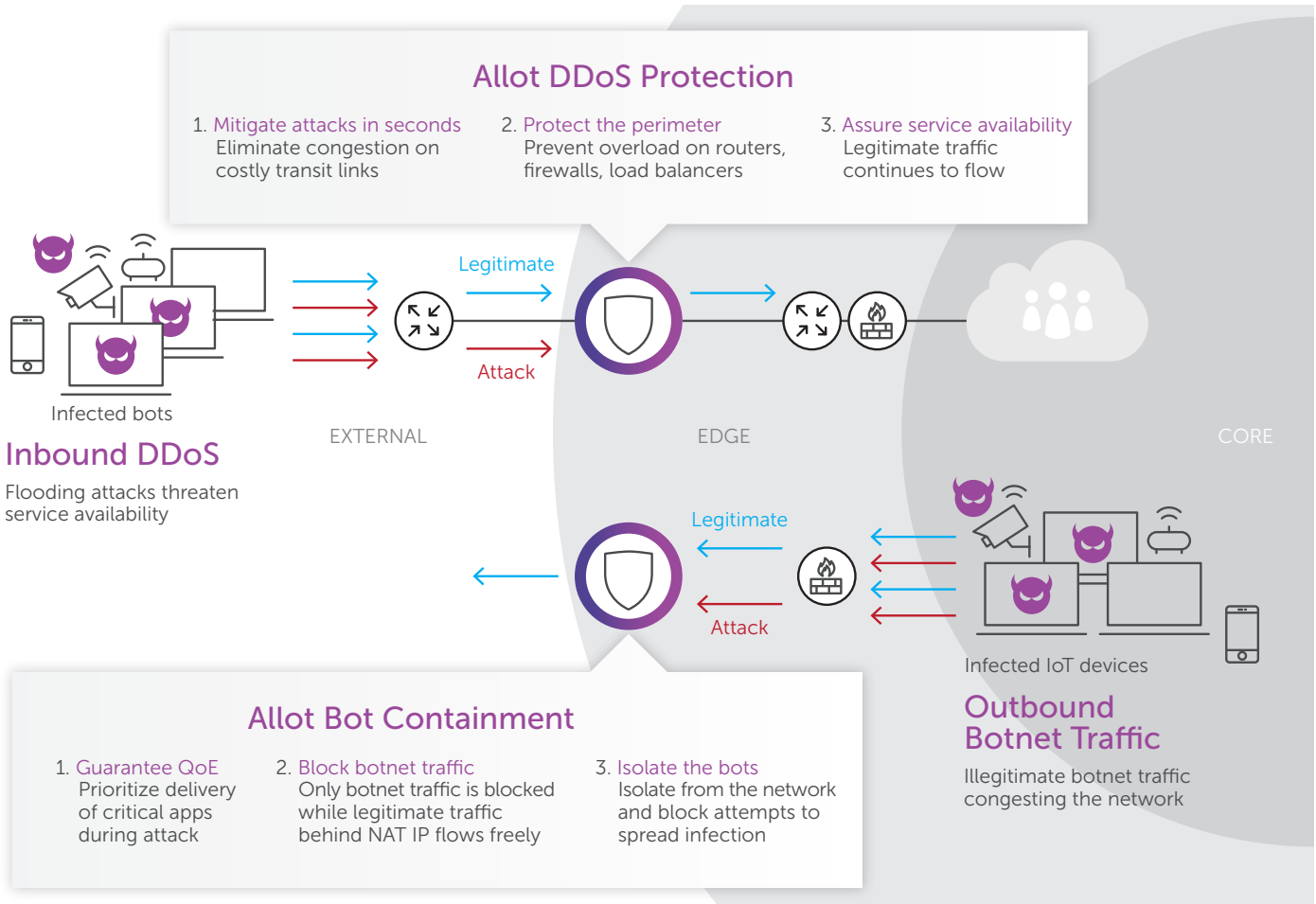
Real-time alerts notify you when a threat is detected and when it has been mitigated. Infected devices may also receive notification. Allot supplies detailed and customizable attack-mitigation logs, event analytics, host infection analytics, and trend/distribution reports to support your security planning, threat management and operational decisions. A unified management controller dashboard monitors network and user activity and manages threat protection across your entire network.

Scalable Always-On Protection

Allot DDoS Secure operates within a unified framework for service delivery, security, and monetization, powered by Allot Service Gateway and providing industry leading performance to defend against the largest volumetric attacks with mitigation bandwidth of Terabits per second. Allot's carrier-grade platform provides built-in high-availability, dual power supply and internal bypass to maximize uptime and fault tolerance. Multiple platforms can be clustered to allow keeping pace .with the proliferating threats

Flexible Deployment, Central Management

Allot DDoS Secure supports on-premise, cloud, hybrid, and virtual deployments with central Controller management so you get the security solution that best fits your network and efficiency requirements Allot also supports accurate DDoS detection and mitigation in NAT and .asymmetric environments



Deployed at critical points in your network, Allot DDoS Secure provides vital insight and effective protection against the ever-growing number of inbound and outbound cyber attacks that threaten your business

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 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	

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 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	

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

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

P/N D240020 Rev.8

sales@allot.com | www.allot.com