Allot Digital Lifestyle Services

ServiceProtector

A System for Network Service Protection

Allot ServiceProtector is part of Allot's portfolio of security services for the digital lifestyle, providing a system for defense against distributed denial of service (DDoS) attacks, prevention of outbound spam, and containment and cleanup of infected botnet hosts.

ServiceProtector Controller

ServiceProtector is built into Allot Service Gateway and NetEnforcer platforms

Features

- ServiceProtector Sensor is embedded in Allot Service Gateway platforms and Allot NetEnforcer devices; activated with a software license key
- The Benefits of adding ServiceProtector to new or existing investments of Allot Service Gateway platforms and NetEnforcer devices:
  - No service interruption or deployment downtime
  - Add network security without adding more hardware into the network
  - More cost effective than separate point solutions
- Performance scales with additional Core Controller blades in Allot Service Gateway or with the number of NetEnforcer devices
- No "flow" sampling – 100% view of packets provides superior detection of DDoS attacks, internal spammers, and botnet-infected hosts
- Behavior-based detection provides accurate, scalable, maintenance-free protection:
  - Host Behavior Anomaly Detection (HBAD) identifies hosts exhibiting symptoms of malware infection or abusive behavior through their abnormal levels of outbound connection activity and further categorized by their match to profiles of malicious connection patterns
  - Network Behavior Anomaly Detection (NBAD) identifies DDoS and other network flooding events by the anomalies they cause in the normally time-invariant behavior of "network ratios" (combinations of Layer 3 and 4 packet rate statistics); filtering rules are obtained dynamically by searching deep into the captured DDoS packets for unique repeating patterns in each event. Optimum filtering accuracy may be achieved by using patterns found in the Layer 2 to 4 headers and payload
- Allot Deep Packet Signatures (ADPS) provide optimum DDoS filtering precision and avoidance of over-blocking; ADPS are created dynamically for each network flooding attack
- Automatic or operator-initiated mitigation
- Management-type PDF reports; user-customized report templates
  - Supports security planning and threat management with subscriber infection analytics, network attack analytics, and trend/distribution reports
  - Comprehensive event reports support operational decisions

Allot communications

Specifications

The Allot ServiceProtector system consists of hardware and software components. The components are: (a) the central management appliance called Allot ServiceProtector Controller, and (b) license-activated functionality embedded in Allot Service Gateway platforms and Allot NetEnforcer devices. Embedded functionality includes detection (ServiceProtector Sensor) and dynamic surgical packet filtering (ServiceProtector NBAD Mitigation). In addition, an appliance-based ServiceProtector Sensor is also available.

General

	DDoS/Network Flood Attack	Infected/Abusive Behavior
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 (evidential captures and manual capture not available for Integrated Sensors (AOS) versions AOS12.x and above)	
Supported Networks	Ethernet, VLAN, MPLS, L2TP, IPv4	
Types of Events	• High packet rate • Small packet size or large packet size • Fan-in or DDoS (many IPs to one IP); Fan-out (one IP to many IPs); Swarms (many IPs to many IPs); DoS (one IP to one IP) • TCP based (SYN, FIN, ACK, RST, invalid flag combinations) • UDP based • ICMP (including echo request, echo reply, unreachable) • Other (non-TCP, UDP or ICMP) • Involving fragmented packets, truncated or malformed packets	• Address scan • Port scan • Flow bomb (bombarding the same target IP and port with a high number of flows) • Mass SMTP (address scanning or flow bombs to 25/TCP) • Mass DNS (address scanning or flow bombs to 53/UDP)
Detection Time (typical)	10–60 seconds	3–5 minutes
Pattern Creation Time (typical)	10–20 seconds	Not applicable
Alert/Notification	Email, syslog, SNMP trap (v2c)	
Enforcement Action		
Approach	• Traffic filtering using Allot Deep Packet Signatures (ADPS) • Filtering occurs in-line and before further policy and bandwidth management	• Notification of subscriber/user via HTTP redirection on Allot NetEnforcer device or Allot Service Gateway platform and/or by triggering existing notification mechanisms (such as email or SMS) • Per-subscriber traffic management by rate-limiting or blocking specific services (such as 25/TCP to prevent propagation of spam) • Per-subscriber solutions require Allot Subscriber Management Platform
Allot Device/Platform Compatibility	Available on Allot Service Gateway platforms and Allot NetEnforcer devices running Allot OS versions AOS10.2 and up	Integrated with Allot SMP for per subscriber traffic enforcement, version SMP9.2.1 and up (see SMP datasheet for device/platform compatibility)
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.	Redback BRAS

ServiceProtector Controller

Capacity per Controller	
Sensors per Controller	16 (maximum)
Sensor-Groups	400 (maximum)
Management Interface	
Interface Media	1 x 10/100/1000BASE-T (RJ-45)
Traffic Encryption and Firewall Requirements	• User to SP-Controller: HTTPS and SSH • SP-Controller to Sensor (Standalone or Embedded): IPSec* **Note:** No NAT traversal except* between SP-Controller and standalone Sensor; No IPSec encryption on NBAD Mitigation traffic when Standalone Sensor is used.* * See Allot ServiceProtector Installation and Admin Guide for firewall configuration requirements.
Management Traffic	100-500kbps (varies according to number of Groups, anomalies and packet size)
Console	VGA/USB and serial
Mechanical and Environmental	
Form Factor/Dimensions	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	675 W (per PSU)
Power Supply	Dual redundant, hot swappable
Certifications and Safety	FCC (Part 15 of FCC rules, Class A), ICES-003 (Issue 4, Class A), UL/IEC 60950-1:2007, CDS C22.2 No. 69950-1-03 2nd Edition, NOM-019

ServiceProtector (Embedded)

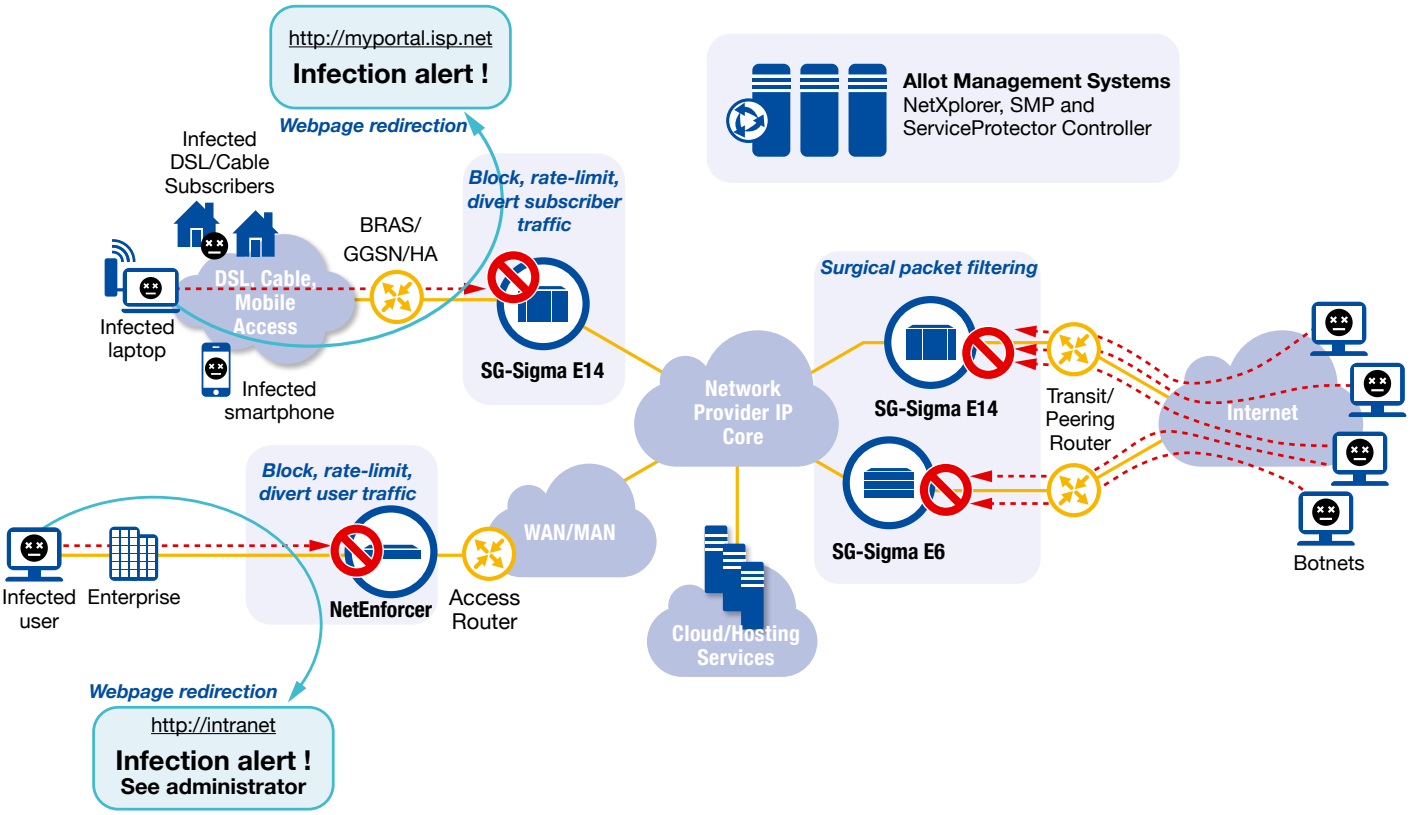
Impact on Legitimate Traffic Flows from Embedded Sensor (NBAD and/or HBAD license) and NBAD Mitigation License	
Bit Rate/Packet Rate	Sensor adds ~15%; NBAD Mitigation adds additional 1-2% on Service Gateway and 5-25% on NetEnforcers (applies only when mitigating)
Latency (relative)	10-20 µsec
CER	Up to 2%
Concurrent Connections/Internal Hosts	No change
Concurrent Suspicious Internal Hosts	1% of Concurrent Internal Hosts (HBAD only)
Max Groups per Sensor	30

ServiceProtector Sensor (Standalone)

	1 GE Sensor Appliance	10GE Sensor Appliance
Capacity (*Aggregated Traffic; **Outbound Connections)		
Max Bit Rate*	4 Gbps (IMIX)	20 Gbps (IMIX)
Max Packet Rate*	5.97 Mpps (60 Byte)	16.6 Mpps (60 Byte)
CER**	~66 kcps	~329 kcps
Concurrent Connections**	9,600,000	
Concurrent Internal Hosts**	2,000,000	
Concurrent Suspicious Internal Hosts**	20,000	
Max Groups per Sensor	30	
Interfaces Options and Connections		
Network Monitoring	4 x 10/100/1000BASE-T (RJ-45) Copper or 4 x 1000BASE-SX/LX (LC)	2 x 10 Gigabit Ethernet SR/LR (LC)
Management	2 x 10/100/1000 BASE-T	
Console	VGA/USB and serial	
Mechanical and Environmental		
Form Factor/Dimensions	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	
Operating Temperature	10–35°C (up to 914.4 m); 10–32°C (914.4–2,133 m)	
Power Consumption	675 W (each PSU)	
Power Supply	Dual redundant, hot swappable	
Certifications and Safety	FCC (Part 15 of FCC rules, Class A), ICES-003 (Issue 4, Class A), UL/IEC 60950-1:2007, CDS C22.2 No. 69950-1-03 2nd Edition, NOM-019	

Deployment

Allot NetEnforcer and Allot Service Gateway are ideally positioned for Allot ServiceProtector to provide visibility and protection.



About Allot Communications

Allot Communications Ltd. (NASDAQ: ALLT) is a leading global provider of intelligent broadband solutions that put mobile, fixed and enterprise networks at the center of the digital lifestyle. Allot's DPI-based solutions identify and leverage the business intelligence in data networks, empowering operators to shape digital lifestyle experiences and to capitalize on the network traffic they generate. Allot's unique blend of innovative technology, proven know-how and collaborative approach to industry standards and partnerships enables service providers worldwide to elevate their role in the digital lifestyle ecosystem and to open the door to a wealth of new business opportunities For more information, please visit www.allot.com.

sales@allot.com

Americas: 300 TradeCenter, Suite 4680, Woburn, MA 01801 USA Tel: +1 (781) 939-9300 Fax: +1 (781) 939-9393 Toll free: 877-255-6826 ● **Europe:** NCI – Les Centres d'A_aires Village d'Entreprises 'Green Side', 400 Avenue Roumanille, BP309, 6906 Sophia Antipolis Cedex, France Tel: +33 (0) 4-93-001160, Fax: +33 (0) 4-93-001165 ● **Asia Pacific:** 25 Tai Seng Avenue, #03-03, Scorpio East Building, Singapore 534104 Tel: +65 67490213 Fax: +65 68481015 ● **Japan:** 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 Tel: +81 (3) 5297-7668 Fax: +81(3) 5297-7669 ● **Middle East and Africa:** 22 Hanagar St., Industrial Zone B, Hod-Hasharon, 45240, Israel, Tel: +972 (9) 761-9200, Fax: +972 (9) 744-3626

www.allot.com **info@allot.com**

P/N D240020 Rev.5