Allot Multiservice Platforms

Secure Service Gateway

Meeting Your Need for Network Visibility, Security and Control

The necessity for your employees and customers to connect and work productively with mission-critical applications, from any location and at any time, significantly increases your need for full network visibility, security and control.

The performance and efficiency of your network can be easily compromised by the ever-increasing demand for LAN, WAN and Internet bandwidth driven by cloud, mobile and video applications. Moreover, the growing use of BYOD and shadow IT have opened complex attack vectors for web threats to infect user devices, get into your network, and harm business productivity and viability.

Allot Secure Service Gateway (SSG) supports your demands with a single, scalable solution for your evolving requirements for application and user visibility, performance, and security.

Benefits

Complete Visibility and Control

Allot provides live traffic monitoring and usage reporting according to traffic policies that are mapped to your complex datacenter and cloud applications, giving you full visibility and control of application performance, web access, user quality of experience, shadow IT and web threats.

Powerful Web Security and DDoS Protection

Allot helps you embrace and maximize the business value of cloud (web) applications by detecting and blocking malware, phishing and other web threats before they harm application performance and user productivity. Allot also detects and surgically filters DDoS and bot traffic before it affects your network.

High Performance and Reliability

Allot Secure Service Gateway is built on the same carrier-class performance and reliability that Allot brings to many of the world's largest network operators. Flexible redundancy configurations plus passive bypass with automatic port failover maximize uptime and availability.

Scalability and Lower TCO

Allot Secure Service Gateway integrates multiple functions in an Intel-based platform that protects your investment and lets you scale from 2 to 20 ports of 1GE/10GE network connectivity in a single appliance.

allot See. Control. Secure.

Full Traffic Visibility

Efficient and high performing networks begin with your ability to obtain a 360° view of network traffic and the QoE that your employees, customers, and branches are getting from datacenter and cloud applications. It also sheds light on shadow IT, BYOD, and mobile app usage that might otherwise go unnoticed.
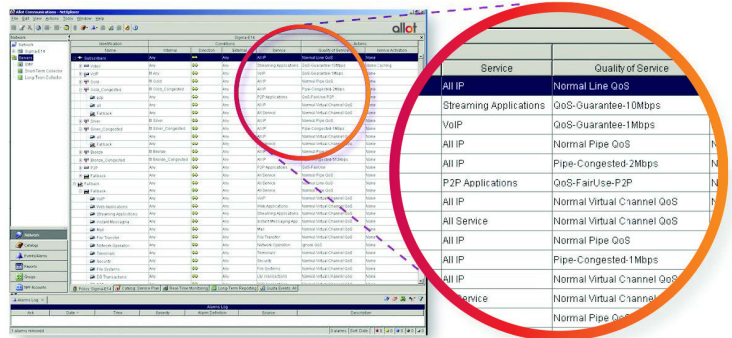
Allot Secure Service Gateway monitors network traffic in real time and delivers full Layer 7+ visibility of application performance, capacity utilization and network health. Integration with Microsoft Active Directory provides traffic intelligence per user and per group, so you can understand how employees consume business applications and network resources. The granular traffic intelligence you get with Allot accelerates root cause analysis so you can pinpoint the cause of service degradation and quickly resolve the problem at its source.

Allot Secure Service Gateway also integrates comprehensive web threat visibility, enabling you to neutralize the impact of malware, phishing, and other web threats as well as inappropriate content that often accompanies recreational web usage and may cause legal or compliance concerns for your business. Key visibility features include:

Enforcement Policy Editor

o   Layer 7 application visibility

o   SSL encrypted traffic visibility

o   Web content and web threat visibility

o   User and endpoint visibility with L4-L7 QoE KPIs

o   Dashboard monitoring and analytics

o   Live, self-refreshing performance metrics reporting in a granularity of seconds

Dynamic Actionable Recognition Technology (DART)

Allot's DART engine, embedded in the platform inspects every single packet and classifies traffic per application, user, IP address, location, and by any static or dynamic policy element you define. Allot's extensive signature library identifies thousands of web applications and protocols and also supports user-defined signatures. Automated DART protocol pack updates from the Allot cloud keep your deployment up to date with the latest application and web developments to ensure accurate traffic classification.

Granular Traffic Control

Allot Secure Service Gateway allows you to virtually partition LAN, WAN and Internet resources so that users and applications no longer compete with one another for bandwidth and Quality of Service (QoS). The highly granular visibility provided by Allot allows you to act with the same level of granularity to maintain optimal network efficiency and high application performance. Powerful policy tools help you define and enforce Acceptable Use Policy and prioritize applications that are critical to your business. For example, to improve user experience, you can dedicate minimum bandwidth to collaboration applications or prioritize real-time point-of-sale and inventory transactions over non-essential traffic. Likewise, you can block access to shadow IT or limit the use of recreational apps that could impact networkand data security. Key control capabilities include:

o   Central and simple QoS policy management

o   Supporting hundreds of thousands of dynamic traffic policies

o   Automated QoS policy propagation to all deployed appliances

o   Asymmetric QoS policy synchronized in real time across multiple datacenters

o   Threshold-based enforcement (e.g., CER, live connections)

o   Actionable alarms
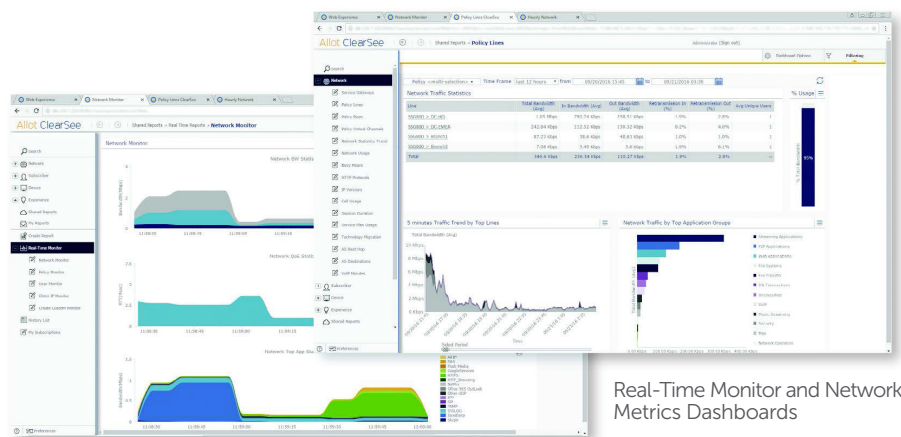
Real-Time Monitor and Network Metrics Dashboards

Web Security

Left unprotected, your business can easily fall victim to malware, ransomware and other web threats. Allot Secure Service Gateway combines superior application visibility and control with SSL inspection and web security powered by Kaspersky Lab, BitDefender and Sophos technologies, so you can prevent malicious attacks from threatening your optimized network while enabling employees and customers to use the Internet and cloud applications safely and productively. Key web security capabilities include:

○ **Internet Threat Visibility:** Get a clear picture of online usage and understand how web security threats are impacting business productivity and viability.

○ **Web Filtering:** Assure safe Internet use and prevent employee exposure to illegal or inappropriate web content in the workplace. Set the URLs and content categories you want to filter; limit access to certain times of the day; enable unblock requests; and receive admin alerts on filtering events.

○ **Anti-Malware:** Prevent viruses, worms, Trojans, spyware, adware, phishing, and other malware from damaging mobile devices, infiltrating your network and causing loss of business data. Requires no action from users and no resources from their devices.

○ **Risky Apps Control:** Block or limit use of risky applications that are often a conduit for malware insertion, data leakage and circumvention of your security measures.

DDoS and Bot Protection

Allot Secure Service Gateway employs carrier-proven anomaly detection technologies to protect your network and data center resources against DDoS and bot attacks that are designed to flood your network and disrupt service availability. Every inbound and outbound packet is inspected to ensure no threat goes undetected. Dynamic creation of filtering rules and surgical filtering of DDoS attack packets avoids over-blocking and allows legitimate traffic to flow unimpeded, keeping your business online and protected at all times. Allot also help you pinpoint host infection and abusive behavior according to abnormal outbound connection activity and malicious connection patterns, so you can treat the root cause of outbound spam, worm propagation and port scanning, and eliminate the additional load it puts on your network.

Scalability and Lower TCO

Modular licensing of capacity and functionality gives you the ability to tailor the security and performance levels of Allot Secure Service Gateway to the evolving needs of your organization. Allot maximizes your investment and dramatically lowers TCO by integrating visibility, security and control in a single appliance, and providing out-of-the-box support for more static and dynamic QoS policies than any comparable solution in the market.
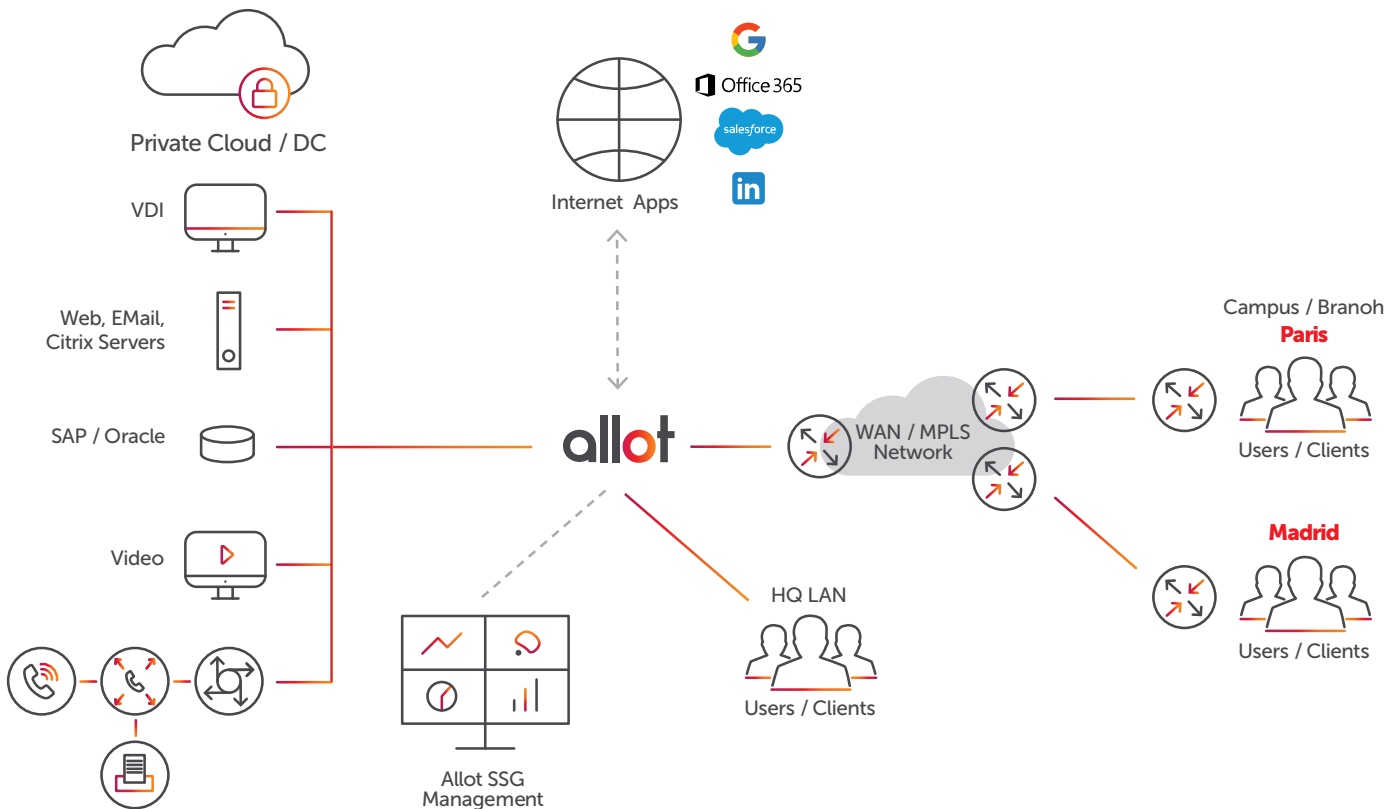
Allot Secure Service Gateway provides full visibility, security and control of
LAN, WAN, Data Center and Internet traffic in one solution

Specifications

	SSG200/400	SSG500/600 V2	SSG800 V2
Maximum Capacity*			
Throughput	1 Gbps (SSG200); 8 Gbps (SSG400)	8 Gbps (SSG500); 20 Gps (SSG600)	35 Gbps
Web Security Throughput	N/A	600 Mbps	1.2 Gbps
IP Flows	4,500,000	24 million	40 million
Traffic Control Policies: Lines / Pipes / Virtual Channels	512/250,000/500,000	512/50,000/200,000	512/150,000/600,000
Employee Count	60,000	60,000	180,000
System Interfaces			
Network I/O ports (with Bypass Capacity)	8 x 1GE Copper (RJ45)	12x1GE/10GE (SFP+) +4 x1GE/10GE (SFP+) for internal steering (can't be used as Network I/O)	20 x 1GE/10GE (SFP+)
Network Interfaces	1GBASE-T (Copper)	10GBASE-SR/LR 1GBASE-LX/SX (Dual rate) Copper	10GBASE-SR/LR 1GBASE-LX/SX (Dual rate) Copper
Management	2 x 1GE Copper	2 x 1GE Copper	2 x 1GE/10GE Copper
Availability			
External Bypass	Independent, passive bypass unit. All units are 1U 19" rack mount.		
HD Multi-Port Bypass Units	8-port unit 2.44kg (5.38lb); 16-port unit 2.64kg (5.82lb); 24-port unit 2.86kg (6.3lb)		
Management	Active-Standby HA on management ports		
System	Redundancy for PSUs and fans		
Dimensions			
Appliance form factor	Standard 1U by 19" rack mount	Standard 2U by 19" rack mount	Standard 2U by 19" rack mount
Size (L x W x H)	429 x 434.6 x 707 mm	Height: 87 mm (3.4 in), width: 445 mm (17.5 in), depth: 720 mm (28.3 in)	87 x 445 x 730 mm without Bezel
Weight (max)	13.04 kg	Approximal 20 kg (44 lb)	Min 32.75 lb (14.9 kg), Max 43 lbs (19.5 kg) per number of NIC interfaces
Power			
Input	100 to 120 VAC ,200 to 240 VAC	Dual Hot Plug, 230/115VAC	Dual Hot Plug, Redundant 100/240VAC or -48VDC, efficiency of up to 94%, Energy star, 80PLUS
Number of PSUs	1	2	2
PSU Redundancy	Optional	Yes	Yes
Total Output Power	500 Watts	750 Watts	800 Watts
Heat Dissipation	1979 BTU/hr (at 100 VAC), 1911 BTU/hr (at 200 VAC), 1965 BTU/hr (at 240 VDC) for China Only	3269 BTU/hour	3207 BTU/hr
Operating Environment			
Temperature	10° to 35°C	10° to 35°C	10°C to 35°C (50°F to 95°F)
Humidity	8% to 90%	Relative humidity (%RH) 8% to 90%	Relative humidity (%RH) 8% to 90%
Management			
Allot SSG Network Management System is available pre-installed on a 1U server appliance, or as software components designed to run on virtual machines: VMWare ESXi (vSphere 5.5 or higher) or KVM (RedHat RHEV 3.5 and above). See Allot SSG Network Management System datasheet for details.			
Standards Compliance			
Safety	UL60950, CE, CB	UL60950, CE, CB	UL60950, CE, CB
EMC (Electromagnetic Compliance)	FCC ,CE , VCCI	FCC ,CE , VCCI	FCC ,CE , VCCI
Environmental	RoHS, China ROHS WEEE REACH	RoHS, China ROHS WEEE REACH	RoHS, China ROHS WEEE REACH

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

Allot Secure Service Gateway Virtual Edition

Allot Secure Service Gateway Virtual Edition supports popular virtualization platforms enabling easy deployment on any public or private cloud. Performance specifications are calculated on the basis of virtual cores and assuming an Intel® Xeon® processor with SR-IOV enabled. Actual throughput performance will be affected by underlying hardware and hypervisor configurations, software licenses, and enabled policies.

Parameters	SSG-VE01	SSG-VE04	SSG-VE08	SSG-VE16	SSG-VE32
vCPU	4	4	8	16	32
RAM	10G	10G	20G	40G	64G
Virtual Storage	100GB	100GB	100GB	100GB	100GB
OS	Linus CentOS 7, 64-bit x86				
Hypervisor VMware ESXi	VMware vSphere 5.5 and above				
Throughput	100Mbps	4Gbps	8Gbps	16Gbps	32Gbps
IP Flows	8M	8M	16M	32M	64M
Traffic Control Policies: Lines / Pipes / Virtual Channels	512/160k/320k	512/160k/320k	512/320k/640k	512/640k/1.3M	512/1.3M/2.6M
Employee Count	500	240k	480k	960k	1.9M

allot See. Control. Secure.