Allot Traffic Intelligence and Assurance Platform

Secure Service Gateway (SSG)

Assuring excellent Digital Experience for your employees and customers

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, control and security.

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

- **Increase IT efficiency through rapid root cause analysis to network and applications issues**

  Thanks to its complete visibility and control of business applications performance, web access, user Quality of Experience, shadow IT and web threats, Allot SSG enables enterprise's IT to quickly identify network and applications quality of Digital Experience issues.

- **Assure business continuity through powerful Anti-DDoS protection**

  Allot SSG delivers inline, zero-day detection and mitigation for both inbound and outbound volumetric DDoS attacks, safeguarding your network infrastructure and customer services at all times. It also identifies and isolates botnet-infected hosts, preventing malicious outbound traffic from impacting your network or external organizations.

- **Assure employees productivity and minimize revenue loss, due to network down time**

  Real Time troubleshooting of network and applications issues and rapid identification of behavioral anomalies in your network and servers in seconds.

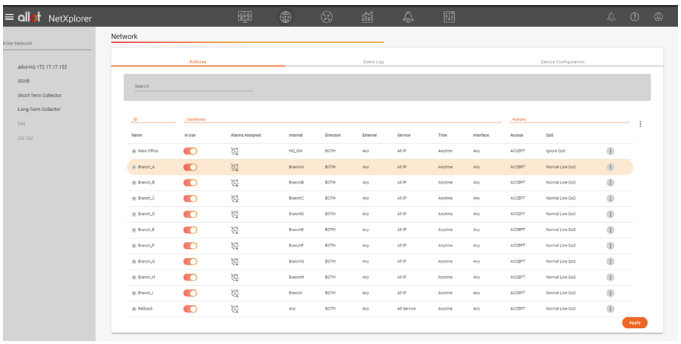
Complete Traffic Visibility

Efficient and high performing networks begin with your ability to obtain a 360° view of network traffic and the quality of Digital Experience 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 organizational unit, 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 key visibility features include:

- Layer 7 application visibility
- In-line SSL encrypted traffic visibility with no SSL decryption
- User and endpoint visibility with L4-L7 quality of Digital Experience KPIs
- Dashboard monitoring and analytics
- Live, self-refreshing performance metrics reporting
- in a granularity of seconds



Enforcement Policy Editor

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 andenforce Acceptable Use Policy and prioritize applications that are criticalto your business. For example, to improve user experience, you candedicate minimum bandwidth to collaboration applications or prioritizereal-time point-of-sale and inventory transactions over non-essentialtraffic. Likewise, you can block access to shadow IT or limit the use of recreational apps that could impact network and data security.

Key control capabilities include:

Central and simple QoS policy management

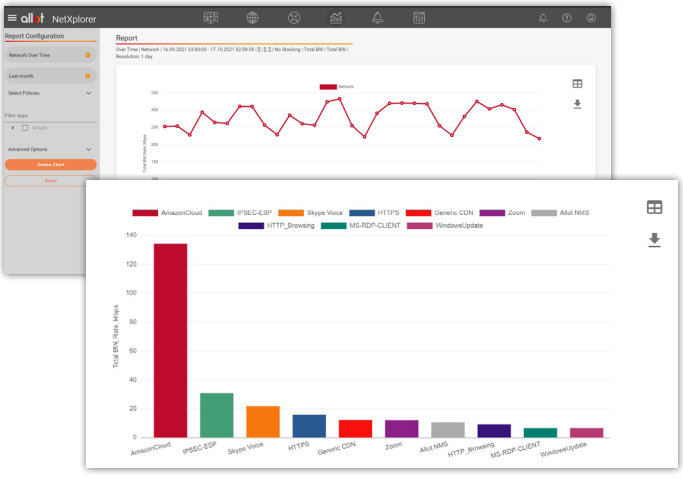
- Supporting hundreds of thousands of dynamic traffic policies
- Automated QoS policy propagation to all deployed appliances
- Asymmetric QoS policy synchronized in real time across multiple datacenters
- Threshold-based enforcement (e.g., CER, live connections)
- Actionable alarms

Dynamic Actionable Recognition Technology (DART)

Allot's Dynamic Application Recognition Technology (DART), an AI-powered engine embedded in the platform, provides granular visibility into application, user, device, quality-of-experience (QoE), and network topology traffic, even with fully encrypted traffic (ECH).

Allot's extensive signature library accurately identifies thousands of Internet applications and protocols and supports user-defined signatures. Frequent and automated updates to the signature library keep Allot SSG up to date with the latest applications and Internet developments, ensuring accurate traffic detection and classification.

Moreover, Allot's flexible and powerful Policy Editor makes it easy for you to provision and enforce real-time Quality of Service (QoS), steering, metering and charging policy with equal granularity.



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 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:

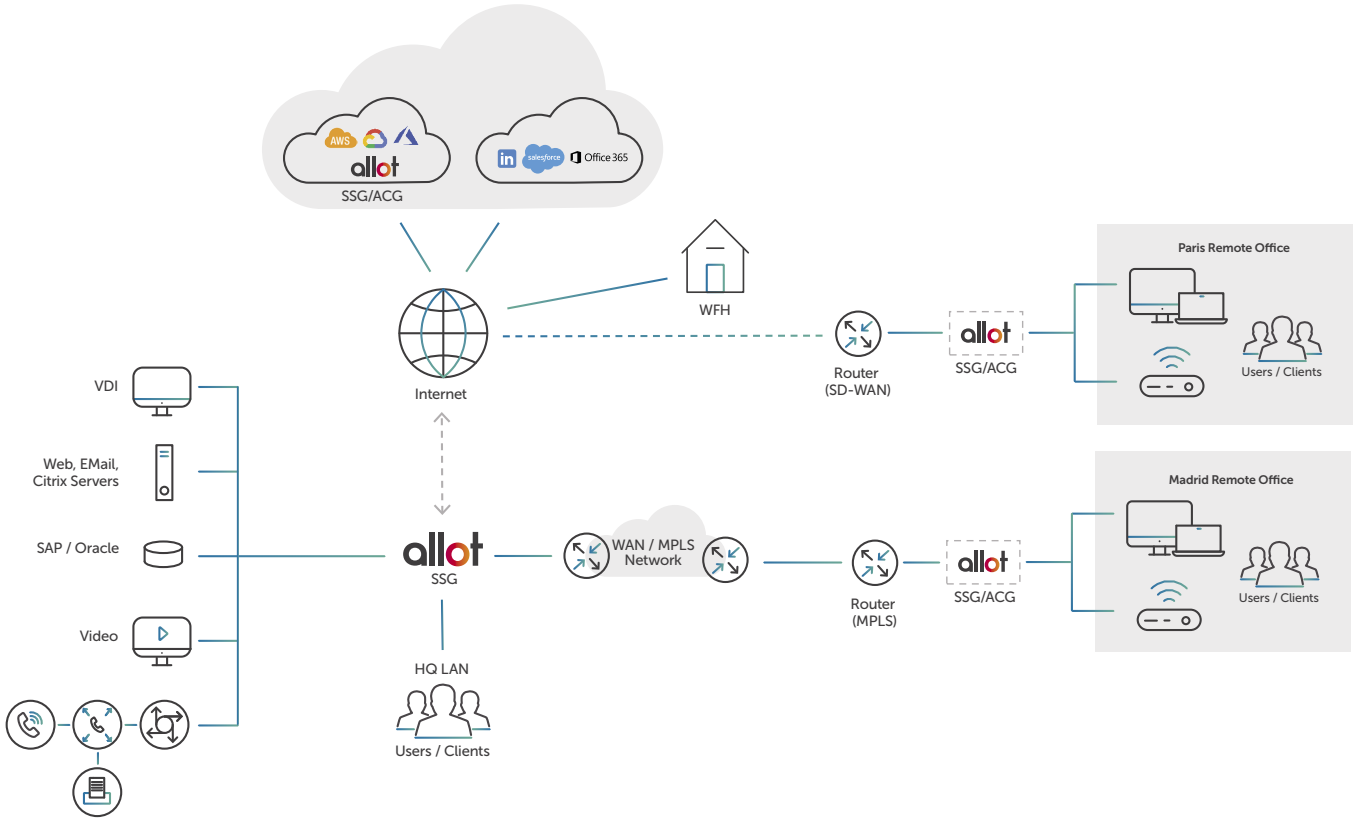
- **Internet Threat Visibility:** Get a clear picture of online usage and understand how web security threats are impacting business productivity and viability.
- **Web Filtering:** Assure safe Internet use and prevent employee exposure to illegal or inappropriate web content in the workplace. Set the 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.
- **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.

Anti DDoS Protection

Allot Secure Service Gateway employs large enterprises anti DDoS solution 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 overblocking 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-thebox support for more static and dynamic QoS policies than any comparable solution in the market.



Allot SSG Architecture - assures excellent Digital Experience, available on-premise or on a cloud based virtual edition

Specifications

	SSG-400E Copper	SSG-400E Fiber
Maximum Capacity*		
Throughput	10 Gbps / 8 Gbps	10 Gbps / 8 Gbps
IP Flows	4.5 million	4.5 million
Number of Traffic Control Policies: Lines / Pipes / Virtual Channels	512 / 250K / 500K	512 / 250K / 500K
Employee Count Number	60,000	60,000
System Interfaces		
Ethernet Interfaces	8 x 1GbE (RJ-45)	4 x 1GbE/10GbE (SFP+)
Ethernet Interface Types	1GbE RJ-45 Copper	10GbE SR/LR 1GbE SX/LX
Management	2 x 1GbE (RJ-45)	2 x 1GbE (RJ-45)
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 1U by 19" rack mount
Dimensions	Height – 42.8 mm (1.68 inches) Width – 482.0 mm (18.97 inches) Depth – 585.3 mm (23.04 inches) without bezel Depth — 598.9 mm (23.57 inches) with bezel	Height – 42.8 mm (1.68 inches) Width – 482.0 mm (18.97 inches) Depth – 585.3 mm (23.04 inches) without bezel Depth — 598.9 mm (23.57 inches) with bezel
Weight (max)	13.04 kg	13.04 kg
Power		
Input	100 to 120 VAC ,200 to 240 VAC	100 to 120 VAC ,200 to 240 VAC
Number of PSUs	1	1
PSU Redundancy	Optional	Optional
Total Output Power	500 Watts	500 Watts
Heat Dissipation	1979 BTU/hr (at 100 VAC), 1911 BTU/hr (at 200 VAC), 1965 BTU/hr (at 240 VDC) for China Only	1979 BTU/hr (at 100 VAC), 1911 BTU/hr (at 200 VAC), 1965 BTU/hr (at 240 VDC) for China Only
Operating Environment		
Temperature	10° to 35°C	10° to 35°C
Humidity	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 6.5 or higher) or KVM (RedHat RHEL 7.6 and above). See Allot SSG Network Management System datasheet for details.		
Security Capabilities		
Allot NetworkSecure is available either embedded in the SSG appliance, standalone appliance or virtual edition, per ordering option. Please refer to NetworkSecure data sheet for more details (https://www.allot.com/resources/DS-NetworkSecure.pdf)		
Standards Compliance		
Safety	UL60950, CE, CB	UL60950, CE, CB
EMC (Electromagnetic Compliance)	FCC, CE, VCCI	FCC, CE, VCCI
Environmental	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-VE04	SSG-VE08	SSG-VE16	SSG-VE32	SSG-VE48
vCPU	4	8	16	32	48
RAM	10GB	20GB	40GB	80GB	135GB
Virtual Storage	100GB	100GB	100GB	100GB	100GB
OS	Linus CentOS 7, 64-bit x86				
Hypervisor VMWare ESXi / KVM	VMware vSphere 6.5 and above KVM RHEL version 7.6				
Throughput	4Gbps	8Gbps	16Gbps	32Gbps	72Gbps
IP Flows	8M	16M	32M	64M	52M
Number of Traffic Control Policies: Lines / Pipes / Virtual Channels	512 / 40k /80k	512 / 320k / 640k	512 /640k / 1.3M	512 / 1.3M / 2.6M	512/1.92M/3.84M
Employee Count	240k	480k	960k	1.9M	2.88M

June 2026