EriMobile
český bezdrát

Parametry nabídky TMS/IPS systému

Kromě parametrů požadovaných v příloze č.1 – Technická specifikace je součástí nabídky:

- **Gold Support** na dodaný HW přímo od výrobce společnosti Allot communitions po dobu **24 měsíců**
- **Gold Support** na dodaný SW přímo od výrobce společnosti Allot communitions po dobu **24 měsíců** včetně aktualizací
- možnost opakovaného prodloužení Gold supportu a tím i prodloužení FULL záruky,
- vzdálená technická podpora při provozu **Allot SSG- 400** po dobu prvních 6 měsíců s možností rozšíření podpory po dobu až 24 měsíců za ceny a podmínek dle následně uzavřené servisní smlouvy.

Minimální požadavky na server , na kterém běží monitoring aplikace provozu a managamentu **Allot SSG- 400:**

- OVF pro vmware ESXi 5.5 a novější , nebo KVM RHEV 3.5 a novější
- RAM 6GB, HDD 300 GB, procesor CPU Intel 6-ti „jádrový“ a vyšší, 1 x network adapter (vNICs)

Allot High Performance Platforms

Secure Service Gateway

Delivering Network Visibility, Security and Control in a single platform

Your business needs to make sure that employees and customers can connect and work productively with mission-critical applications at all times and from any location. 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 combines the functionality of Allot Service Gateway with our powerful web security and DDoS protection systems, to offer a single, scalable solution to support your evolving requirements for application and user visibility, performance, and security.

Complete Visibility and Control

Allot provides live traffic monitoring and usage reporting according to traffic policies that are mapped to your complex data center 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

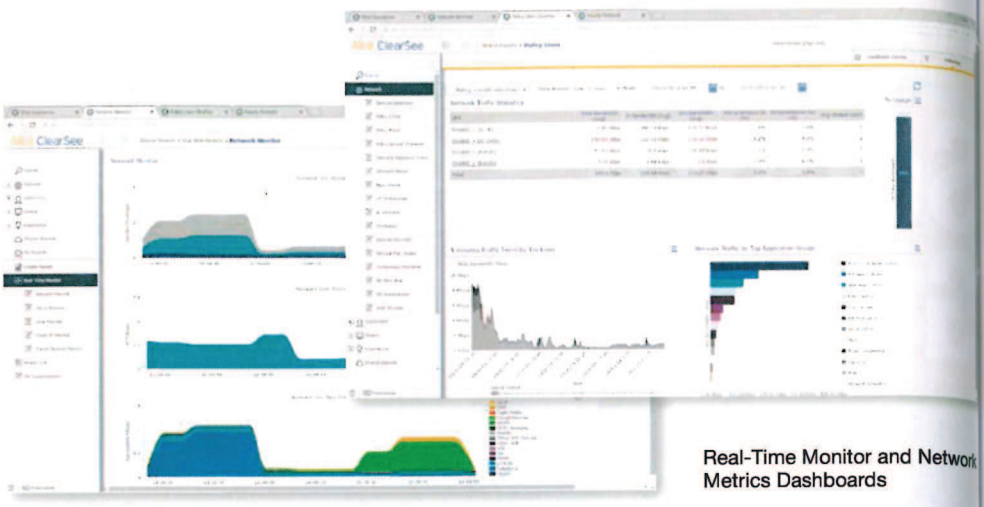
Allot Secure Service Gateway integrates multiple functions in an Intel-based platform that protects your investment and lets you scale from 2 to 20 ports of 1GE/10GE network connectivity in a single appliance.

Allot communications

Features

Full Visibility

Efficient and high performing networks begin with your ability to obtain a 360° view of the QoE that your employees, customers, and branches are getting from your datacenter and cloud applications. It also sheds light on shadow IT, BYOD, and mobile app usage that might otherwise go unnoticed.



Real-Time Monitor and Network Metrics Dashboards

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:

- Layer 7 application visibility
- SSL encrypted traffic visibility
- Web content and web threat visibility
- User and endpoint visibility with L4-L7 QoE KPIs
- Dashboard monitoring and analytics
- Live, self-refreshing performance metrics reporting in a granularity of seconds

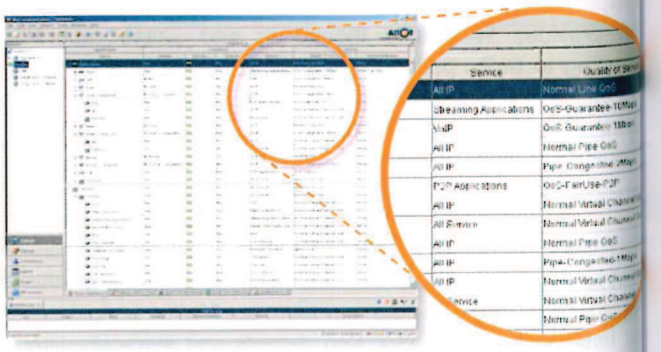
Dynamic Actionable Recognition Technology (DART)

Allot's DART engine, embedded in the platform, provides granular visibility of network usage and quality of experience (QoE) per application, user, IP address, location, and 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 updates from the Allot cloud keep your deployment up to date with the latest application and web developments to ensure accurate traffic classification.

Granular 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 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



Enforcement Policy Editor

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, 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:

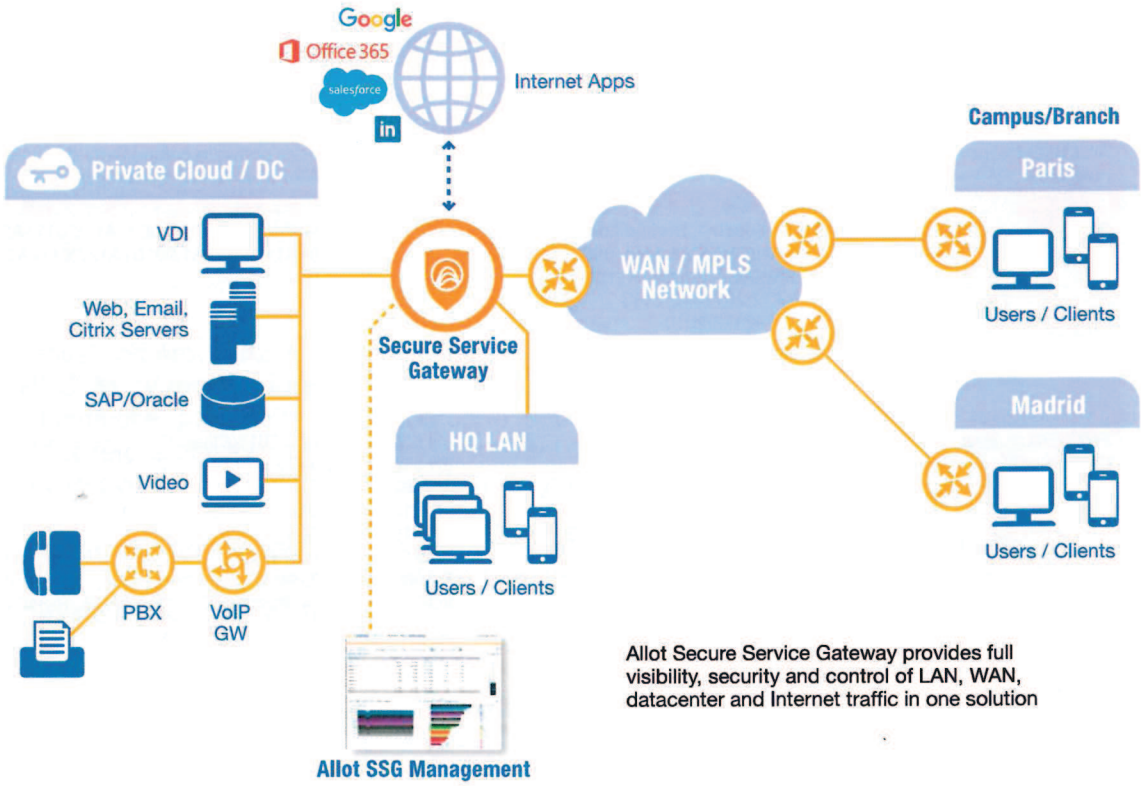
- **Internet Threat Visibility:** Get a clear picture of online usage and understand how web security threats are impacting business productivity and viability.
- **Web Filtering:** Assure safe Internet use and prevent employee exposure to illegal or inappropriate web content in the workplace. Set the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

Specifications

Allot Secure Service Gateway

	Allot SSG400	Allot SSG600	Allot SSG800
Maximum Capacity*			
Throughput	8 Gbps	20 Gbps	35 Gbps
Web Security Throughput	N/A	600 Mbps	1.2 Gbps
IP Flows	6 Million	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)	8 x 1GE/10GE (SFP+)	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 1U by 19" rack mount	Standard 2U by 19" rack mount
Size (L x W x H)	429 x 434.6 x 707 mm	780 mm x 447 mm x 43 mm	783 mm x 482 mm x 97 mm
Weight	13.04 kg	Min: 13.5 kg (29.8 lb) Max: 21.0 kg (46.3 lb)	Min: 16 kg (35.3 lb) Max: 32 kg (70.5 lb)
Power			
Input	100 to 120 VAC ,200 to 240 VAC	100-127 VAC / 200-240 VAC	100-127 VAC / 200-240 VAC
Number of PSUs	1	2	2
PSU Redundancy	Optional	Yes	Yes
Total Output Power	500 Watts	750 Watts	750 Watts
Heat Dissipation	1979 BTU/hr (at 100 VAC), 1911 BTU/hr (at 200 VAC), 1965 BTU/hr (at 240 VDC) for China Only	~2559 BTU/hour	~2559 BTU/hour
Operating Environment			
Temperature	10° to 35°C	10° to 35°C	10° to 35°C
Humidity	8% to 90%	8% to 80%	8% to 80%
Maximum Altitude	3,050 m	3,048 m	3,048 m
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.			
Regukations and Safety			
Safety	UL 60950-1, 2nd Edition, 2014-10-14 CAN/CSA C22.2 No. 60950-1-07 EN60950-1:2006+A11:2009+A1:2010 +A12:2011+A2:2013 EN 62479:2010 CB IEC 60950-1:2005+AMD1:2009+ AMD2:2013 AS/NZS 60950.1: 2015 part 1 BIS IS 13252(PART1):2010	UL 60950-1:2006+A1:2010+A11:2009+A12:2011+A2:2013 EN60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013	
EMC (Electromagnetic Compliance)	EN 55032:2012 Class A EN 55024:2010. EN 61000-3-2:2014 EN 61000-3-3:2013 FCC CFR 47 Part 15 Sub B Canada ICES-003 Issue 6 VCCI -03/2015.04 CISPR 32:2012 TCVN7189:2009 CCC GB17625.1-2012,GB4943.1- 2011,GB/T9254-2008 Class A	EN 55022:2010+AC:2011(Class A) EN 55032:2012/AC:2013 EN 55024:2015. EN 61000-3-2:2014 EN 61000-3-3:2008 FCC CFR 47 Part 15 Sub B Canada ICES-003 Issue 5 VCCI V-3/2013.04 (member ID:1798 [C3775, R-3404, T1630]	
Environmental	RoHS/WEEE compliance ; China ROHS; REACH EU 1907:2006		

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

Contact us: sales@allot.com

www.allot.com info@allot.com

© 2017 Allot Communications Ltd. All rights reserved. Allot Communications, Sigma and NetEnforcer and the Allot logo are trademarks of Allot Communications. All other brand or product names are the trademarks of their respective holders. The information in this document is for reference purpose only and constitutes neither an offer, a commitment nor an acceptance. Allot may change the information at any time without notice.

P/N D240064 Rev.5