allot
See. Control. Secure.

Network Visibility, Security & Control

Solution Brief

See. Control. Secure.

Contents

1 Introducing Allot Secure Service Gateway

Allot Secure Service Gateway is a platform that combines the functionality of Allot Service Gateway with our powerful web security system, Allot WebSafe Business, to deliver comprehensive network visibility, security and control in a single, scalable appliance. Allot Secure Service Gateway enables enterprises to enhance productivity and protect their networks and users against DDoS attacks and web threats at a significantly lower TCO than what is available today.

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.

1.1 All-in-one Functionality

- Application/User visibility and analytics
- Granular traffic control
- Powerful web security and application control
- DDoS protection
- Bot containment
- High performance and reliability
- Scalability and Lower TCO

1.2 Designed for Businesses

Enterprises operate in a world that is experiencing a continually escalating volume of information and traffic, the increased use of shadow IT, data-sharing through sanctioned and unsanctioned apps, and a massive increase in connectivity, as many enterprises allow users to connect to their networks using their own devices (smartphones, tablets, laptops). Plus, the Internet of Things (IoT) is raising the number of other connected items even more. This impacts upon organizations and drives the need for the integrated visibility, security and control solution that Allot Secure Service Gateway provides.

Allot Secure Service Gateway has been designed specifically with business in mind. It provides the most efficient combination of analytics, policy enforcement and bandwidth management, thereby maximizing cost-efficiency and quality of experience for all network users.

1.3 Lowering TCO

The platform's all-in-one functionality is suitable for all verticals who want to reduce operational and capital cost that a multiple appliance solution incurs. Allot Secure Service Gateway is an integrated solution that is capable of replacing five different appliances. Sized and priced to support a wide range of medium-sized to large organizations, from hundreds to 100,000 employees, such as financial institutions, education, manufacturing, retail and healthcare. Two models, SSG600 and SSG800, both with higher port density than comparable solutions[1], serve the demands of different network deployments, with the SG600's throughput at 12Gbps, and the SG800 handling a throughput of 30Gbps.

[1] For further details, refer to Allot Secure Service Gateway data sheet [note: add link here to datasheet]

2 What's Inside?

Allot Secure Service Gateway creates a more efficient network for your business and the users of your network by optimizing application performance and quality of experience whilst simplifying operations and reducing TCO. It achieves this by offering the following:

2.1 Complete Visibility

Clear visibility of every application and network transaction is critical to pinpointing the causes of risk, and to understanding and managing how well enterprise business applications are supporting employees and helping (or hindering) their productivity. Visibility enables you to plan, see trends and pre-empt issues, so that you can invest wisely where and when you need to. Allot Secure Service Gateway gives you the best insight and the intelligence necessary to control traffic and users' behavior so that you can maintain and enhance the quality of your network.

Allot Secure Service Gateway supplies network business intelligence essential for IP service optimization, providing a clear view of how your IT resources are being consumed. It includes Dynamic Actionable Recognition Technology (DART), Allot's superior brand of deep packet inspection (DPI) technology that is embedded in all Allot platforms to deliver granular visibility of network usage per application, user, quality-of-experience, and any static or dynamic policy element you define. Allot's analytics capabilities gather, consolidate and optimize awareness and visibility of traffic. Allot employs multiple inspection and analytical methods to identify specific applications and protocols, including encrypted applications that are designed to evade detection. Our extensive signature library identifies thousands of web applications and the newest Internet and mobile applications and protocols as well as anonymizers, dark net applications, Peer-to-peer file sharing and conferencing apps. It 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.

Allot Secure Service Gateway monitors network traffic in real time and ensures clear real-time visibility of every application and transaction, with a 5-second refresh. It delivers full Layer 7+ visibility of application QoE, capacity utilization and network health. Integration with Microsoft Active Directory provides traffic intelligence per user and per user group, so you can understand how employees consume cloud applications and bandwidth resources. This granular level of visibility enables you to pinpoint the causes of service degradation and quickly resolve the problems at their source. It also enables you to define traffic management policies that meet your business goals and your users' expectations, thereby enhancing the control that you have over your enterprise network.

With this platform, you can generate real-time and long-term monitoring reports for the most effective viewing, navigation and drill-down. Consequently, Allot Secure Service Gateway facilitates fast diagnosis and resolution of network problems, and it assists in accurate usage analysis and planning of network capacity. This end-to-end

visibility provides easily accessible, actionable information that forms the basis of powerful policy control and security measures that reinforce and protect your network and its users.

Benefits

- Always up-to-date view of application usage for making data-driven decisions
- Measure and improve user QoE
- Real-time view for troubleshooting performance issues
- Long term usage for capacity planning

2.2 Powerful Web Security

The migration to mobility and cloud applications, and the increasing trend of BYOD amongst employees, have introduced Quality of Experience, security, and shadow IT challenges for enterprise networks.

Cyber criminals take advantage of these trends, which provide them lucrative motivation to operate. They monetize their nefarious activities by ransoming data and endpoints using ransomware. Providing robust security is imperative in order to maintain the integrity of any network, meet users' expectations without compromising network and application performance.

Allot Secure Service Gateway includes our powerful DDoS protection and web security system, **Allot WebSafe Business**, combined with security technology powered by **Kaspersky Lab, BitDefender** and **Sophos**. Together, they help you maximize the value of cloud applications by detecting and blocking malware, phishing and other web threats and reduce the enterprise attack surface by enforcing an acceptable use policy that would for example block the use of risky apps. 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 virus, worm, Trojan, phishing, and other malware from damaging endpoints, infiltrating your network and causing loss of business data. Requires no action from users and no resources from their devices.
- **SSL Inspection:** With the growth of SSL encrypted Web traffic, enterprises need to be able to open encrypted connections and apply both anti-malware and content filtering. This has become an essential capability in order to reinforce security while maintaining the capability to selectively bypass health, financial or other private sites so that employee privacy can continue to be assured.

- **Enforce an Acceptable Use Policy:** With the growth of Shadow IT, BYOD and the availability of tools that are intended to conceal identity Enterprises are facing a myriad of risks that are the result of a growing attack surface. This can be reduced by implementing an acceptable use policy that limits shadow IT applications, blocks risky applications and web sites in addition to the traditional block of inappropriate content from the workplace and limit of recreational applications and websites intended to increase productivity.
- **Bot Containment:** Identify infected endpoints by detecting anomalous host behavior and enable automatic quarantine of the host by steering its traffic

Threats from Risky Applications

Heavy use of low priority or recreational applications and websites consumes considerable bandwidth and can congest and impair your network operations. Furthermore, some applications pose high levels of risk that extend beyond operational effectiveness, for example:

Peer-to-peer applications provide a backdoor to host data that can be accessed by anyone on the peer-to-peer network and programs or content downloaded can include malware or violate copyrights.

Anonymizers/VPN Tunnels are typically used to hide a user's identity and are in use by some to access illegal content or purchase illegal goods such as drugs.

Although these applications can be used for the intended purpose of privacy they are also used to hide illegal activities or exploited for cyber-attacks. By nature, they are designed to bypass conventional security controls such as firewalls and IPS/IDS. They achieve concealment through the use of encryption and obfuscation and identifying them is not a trivial effort.

Allot employs advanced mechanisms to detect encrypted applications that enable an enterprise to identify risk and/or malicious apps without having to decrypt them. These methods include the following and apply to encrypted HTTP and non-HTTP traffic:

- Pattern detection
- Certificates analysis
- SSL extensions analysis
- Traffic heuristics
- Traffic statistics
- SNI detection
- Machine learning algorithms

to a remediation vLAN until remediation is achieved, thus containing any potential outbreaks.

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 and superfluous load it puts on your network.

When combined with DPI-based traffic management the SSG behavioral based DDoS mitigation engine makes the network robust by limiting traffic so that no networked resource gets overwhelmed by accidental or intentional traffic anomalies.

Allot Secure Service Gateway provides up to 30Gbps of DDoS mitigation capacity it supports asymmetric traffic for complex datacenter deployments, and provides detailed postmortem analytics.

Benefits

- Real-time protection and mitigation of DDoS attacks directed at your datacenter and DNS servers
- Mitigate inline without diverting massive data volumes to cloud scrubbing centers
- Gain real-time visibility into attackers and their targets in your network
- Treat the root cause of infected endpoints so bots can be stopped without affecting others
- Eliminate spambot abuse and keep port scanning traffic off your network

2.3 Flexible and Dynamic Control

Allot Secure Service Gateway maintains optimal network efficiency and performance while meeting the specific needs and business priorities of your organization by applying acceptable use policy tools for shadow IT, BYOD and resource usage. It safeguards users' quality of experience by controlling, prioritizing and blocking bandwidth availability according to your needs, in order to maximize the bandwidth and responsiveness of applications important to your business.

In order to achieve this, Allot Secure Service Gateway uses access virtualization to manage Internet, LAN and WAN resources to multiple users and applications. It creates virtual instances of Internet and WAN access links that operate and can be controlled completely independently of one another.

Once the Internet and WAN access connections are virtualized, users and applications no longer need to compete with one another for resources.

IT staff are now able to assign appropriate SLA policy to the different applications and users accessing the private or public cloud, taking into account both the inherent requirements of all applications together with their importance to the business. SLA policy may control a number of factors such as bandwidth allocation, QoS, forwarding priority and others. Service Levels may include automatic enforcement triggers such as temporary rate-limiting when utilization reaches a congestion threshold. Furthermore, you can block access to recreational apps, or limit the use of shadow IT that could impact network security and data leakage.

Benefits

Powerful tools for policy creation, traffic management, platform and software configuration and maintenance

- Prioritization of critical applications on your network, expediting business processes regardless of congestion or choke points.
- Easy to use

3 What You Can Do with Allot SSG

Monitor, analyze network usage & behavior of applications/users/endpoints

Industry	Requirement	Solution / Benefit
Retail	Analyze in-store browsing behavior	A retail giant with hundreds of stores used Allot's comprehensive analytics to see if customers were comparing prices to competitors while shopping.

Control & improve application performance and user productivity

Industry	Requirement	Solution / Benefit
Hospitality	Improve guest WiFi experience	A hotel chain differentiated their WiFi service policy based on the type of accommodation each guest had booked, and guest profiles. This greatly improved the Quality of Experience delivered to all customers.
Energy	Prioritize Office 365 business applications and Skype for Business	Allot helped the customer achieve the highest performing detection and control of Office 365 applications and real-time Skype for Business conferencing QoS control.

Block malicious or unauthorized application / user traffic

Industry	Requirement	Solution / Benefit
Retail	Block customers accessing inappropriate web sites from each store	Allot's solutions enable a retail chain to monitor its customers' WiFi usage and prevent them from abusing their free WiFi service. This is achieved by automatically filtering illegal or highly inappropriate website URLs in line with the company's business policy and regulatory guidelines.

Enforce Acceptable Use Policy for shadow IT, BYOD, resource usage

Industry	Requirement	Solution / Benefit
Public Sector & Finance	Stop employees bypassing the Firewall and other security controls through the use of VPN and tunneling apps	Allot solutions provide this customer with the broadest and most accurate detection of anonymizers and other risky applications, so they can be most effectively detected and blocked.

Troubleshoot and resolve issues rapidly

Industry	Requirement	Solution / Benefit
Insurance	Neutralize DDoS attacks against business critical applications and ensure servers run smoothly 24/7	This national insurance provider has deployed Allot to provide a first line of defense that automates the detection and mitigation of DDoS attacks within seconds. It also blocks outbound spam traffic and quarantines users until their endpoint can be cleaned.

Simplify your operations

Industry	Requirement	Solution / Benefit
Food Manufacturing	Manage WAN + data + internet	Allot provides a centralized solution that delivers network intelligence and traffic monitoring and management.

Reduce OPEX and TCO

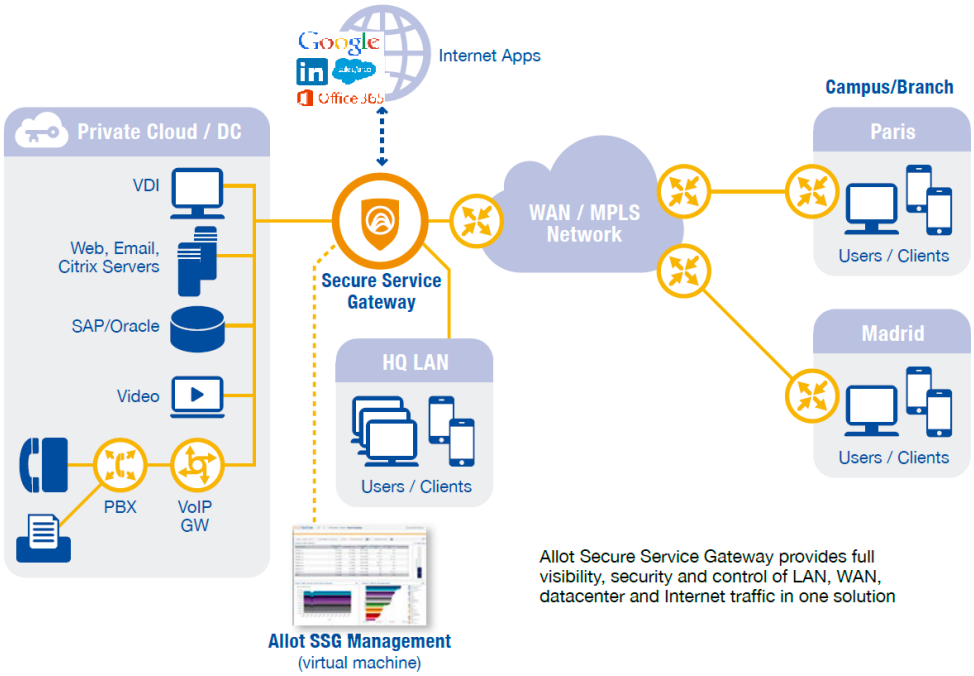
3.1 All-in-one Appliance

- Up to 22 ports
- Up to 30 Gbps
- Up to 600,000 app/user policies
- From 500 to 100,000 employees
- Multiple solutions inside

3.2 How You Benefit

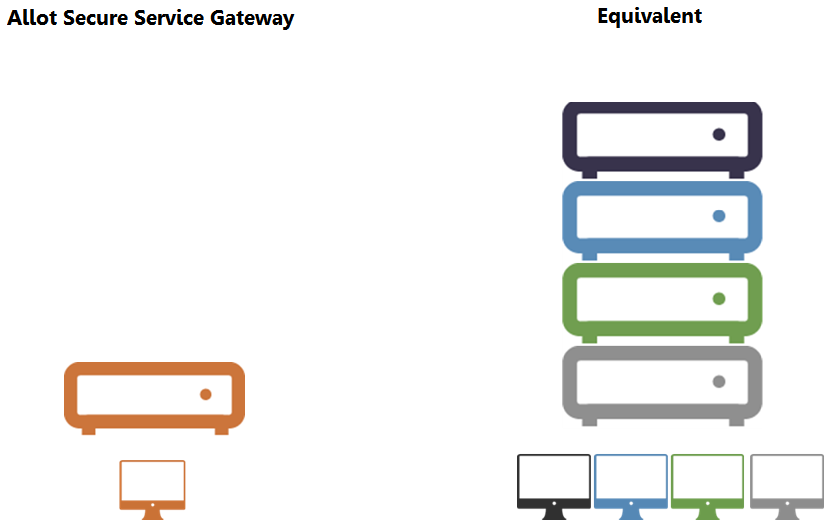
- Deploy one platform instead of many
- Potentially replace five different appliances
- Save rack space

- Save operating costs and reduce support costs
- Easily scalable and flexible to meet the specific needs of your enterprise
- Coordinated version updates from one vendor
- Native interoperability between functions



3.3 Deploy and Manage One Platform, Instead of Many

Without SSG, a typical deployment requires a higher investment in more hardware:



4 Advantages

With the introduction of Allot Secure Service Gateway, Allot has integrated visibility, security and control capabilities within a single, future-ready, cost-effective and highly scalable platform, using standard interfaces to interoperate with other elements in your network as needed. In this way, enterprises reduce the risk and enhance the success of cloud data center implementations. Allot Secure Service Gateway's comprehensive all-in-one solution provides customers with the following 10 advantages over any comparable solutions:

1. More policy options
2. More ports per platform
3. Identifies more mobile apps
4. More QoS control tools
5. Less hardware required
6. Reduces TCO
7. Powered by industry-leading technologies: Intel, Kaspersky, Sophos, BitDefender, HP Vertica, Microstrategy, DART, etc.
8. Interoperability across all deployed appliances
9. Versatile: Scalable and flexible
10. Assured service availability, reliability, scalability and performance

Allot's experience in service integration has been acquired over years of successful implementations with very large carriers and enterprises. We pour this experience back into our product features and into the support we provide to our channels and customers.

P/N Dxxxxxx Rev.1

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: +1 877-255-6826
Europe: NCI–Les Centres d'Affaires Village d'Entreprises, 'Green Side' 400 Avenue Roumanille, BP309 06906 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 6749-0213; Fax: +65 6848-1015
Japan: 4-2-3-301 Kanda Surugadai, Chiyoda-ku, Tokyo 101-0062 - Tel: +81 (3) 5297 7668; Fax: +81 (3) 5297 7669
Middle East & Africa: 22 Hanagar Street, Industrial Zone B, Hod Hasharon, 4501317 Israel - Tel: 972 (9) 761-9200; Fax: 972 (9) 744-3626