Sangfor IAG vs Allot SSG

Competitive Analysis

www.sangfor.com

This comparison and information document is based on the Sangfor interpretation of publicly available data as of the date of preparing this comparison. This document has been prepared by Sangfor and not the other vendors listed herein. The features or characteristics of the products under comparison, which may have direct impact on the accuracy and/or validity of this comparison, are subject to change. The information contained in this comparison is intended to provide broad understanding and knowledge of factual information of various products and may not be exhaustive. Anyone using the document should make their own decision based on their requirements and should also research original sources of information and not rely only upon this comparison while selecting any product. Sangfor makes no warranty as to the reliability, accuracy, usefulness, or completeness of this document. The information in this document is provided "as is" and without warranties of any kind either expressed or implied. Sangfor retains the right to modify or withdraw this document at any time. This document is confidential and intended for private circulation to Sangfor internal personnel and authorized partners only, and may not be disclosed to unauthorized third parties. Partners may use this comparison only if it is permitted in their jurisdiction and must use the most up-to-date version.

This document is strictly private and confidential. Please do not share.

October 2021

SANGFOR

Competitor Background: Allot Ltd 01

Allot is a provider of security and monetization solutions that enable service providers to analyze and optimize their networks. The company offers security as a service (SECaaS), DOS protection and prevention, network intelligence, traffic management and other related solutions such as service gateway, unified management and etc. The chronology of Allot innovation operates a lot of network intelligence and network security solutions. Allot targeted market is mostly in the telecommunications sector and other areas of network operator providers.

In 2011, it was reported that equipment sold by Allot has illegally reached Iran. In January 2012, Allot was cleared by the Israeli Ministry of Defense of any wrongdoing, as the investigation concluded that the company was unaware that the internet monitoring equipment it sold to the Danish distributor ended up in Iranian hands.

Allot Pros 02

- Enforce QoE-based congestion control aligned to business priorities
- In-line DDoS provides immediate mitigation
- Carrier-grade subscribers' management for ISP and large education sector
- Network analytics
- High port density
- Multi-layer architecture for scalability

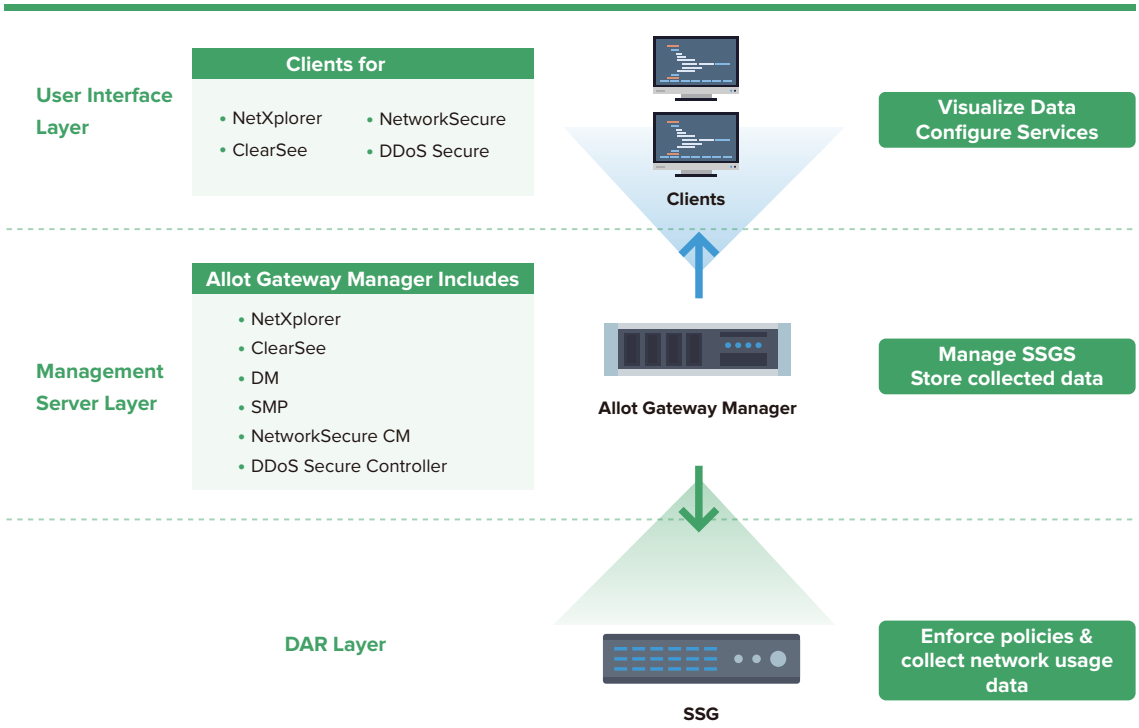
Allot Cons 03

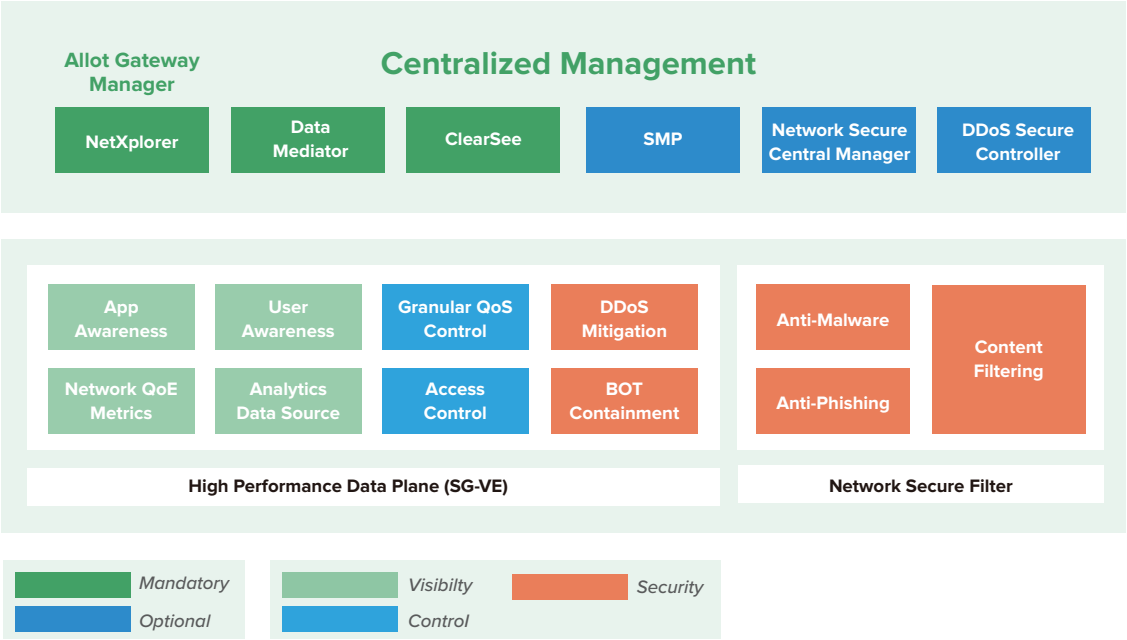
1. Highly depends on OEM Security modules and data structure based on HP Vertica (Data Warehouse), Microstrategy BI (Business Intelligence), Kaspersky Labs/Bitdefender/Sophos (Anti-Malware).
2. SSG200 & SSG400 web security is not supported. NetworkSecure element (content filtering, anti-malware protection) only available on SSG600 & SSG800.
3. Any SSG require to be managed by Allot Gateway Manager and Clients.
3. The Allot Gateway Manager compulsory modules include NX, CS, DM. Optional will be SMP, NS CM and DDOS SC.
4. For client-side, CS client and NX client are compulsory. Optional will be NS Client and DDOS SC if the customer decided to use NS and DDOS.

5. NX client (java-based application) require to be installed in any computer for accessing and managing SSG.
6. SSG requires an external bypass unit (passive optical device) as a compulsory part of the product installation.
7. High availability only supports active-active mode.
8. Localized applications supported are lesser compared to Sangfor application database.
9. For remote server management systems, users are required to use iLO (HP Enterprise), TSM & XCC (Lenovo).
10. Require to use CS for external reporting and there is no in-built reporting within SSG.

Notes 03

- **NX** - NetXplorer
- **CS** – ClearSee
- **DM** – Data Mediator
- **SMP** – Subscriber Management Platform
- **NS CM** – NetworkSecure Central Manager
- **DDOS SC** – DDOS Secure Controller





Complexity with Different Management and Modules 04

- SSG Requires Allot Gateway Manager + Client
- Allot Gateway Manager = NX, CS, DM (Compulsory)/ SMP, NS CM, DDOS CS (Optional)
- Client = NX, CS (Compulsory)/ NS, DDOS (Optional)

Sangfor IAG 05

- Sangfor only need IAG and BI (External and consolidated/independent reporting)

Sangfor approach on IAG involves 4 main focal points

Visibility – To uncover any passing traffic whether this is plain network traffic or encrypted traffic including TLS 1.3. Decryption method includes both gateway decryption and client-based decryption based on customer environment.

(For TLS 1.3, user need to use ingress client to decrypt this encrypted traffic.)

Identity – Ability to detect user identity. Support authentication based on SMS, portal, social media & QR code.

Control – Ability to provide granular control on applications, sanctioned & unsanctioned SaaS applications (Shadow IT), bandwidth management, content audit, anti-malware AI-based engine (Engine Zero), threat intelligence (Neural-X), asset management and endpoint compliance check.

Analytics – Holistic view of logs and reporting. IAG internal reporting provide in-built reporting module by default and can be further extended for further analysis via Sangfor Business Intelligence platform.

Key Differentiator 06

1. Sangfor IAG is an SWG solution and Allot SSG is a traffic intelligence and assurance pure-play platform.
2. Sangfor IAG solution is developed by in-house R&D departments and there is no dependency support from another third-party vendor.
3. Sangfor IAG is not just only bandwidth management and it can be used for network security protection in conjunction with SWG solutions such as secure internet access and two-tier protection with Sangfor NGAF.
4. Sangfor IAG unparalleled visibility on devices with associated users, not just common endpoint devices, including IoT devices.
5. Sangfor IAG is in SWG Gartner Magic Quadrants and Allot is not.

Sangfor IAG vs Allot SSG Model Comparison 07

IAG Model	Throughput	SSG Model	Throughput
M5500	1Gbps	SSG200	1Gbps
M9000	10Gbps	SSG400	8Gbps
M9000	10Gbps	SSG500	8Gbps
M10000	20Gbps	SSG600	20Gbps
M12000	40Gbps	SSG800	40Gbps

Summary Feature Comparison – Sangfor IAG vs Allot SSG

Feature	Description	IAG	SSG
High Availability	Active-Active, Active-Passive	Yes	No, only Active-Active mode
Hardware Bypass - Internal	Hardware bypass - Internal Hardware	Yes	No
Hardware Bypass - External	Hardware bypass - External Hardware	Yes	Yes
SSO Authentication	LDAP, Active Directory, POP3, Proxy, Web Server, Radius	Yes	Yes
User Identity	IP, MAC, IP/MAC binding, hostname, SMS, USB Key	Yes	Yes, except USB key
Guest User Authentication	Social media and QR Code - Facebook, Twitter, Line, WeChat, Gmail	Yes	No
Wireless LAN Integration	Integration with Wi-Fi Controllers	Yes	Yes
Signature Update Frequency	Application signatures are updated every 2 weeks	Yes	Yes, every 2-4 weeks
SSL Inspection	Inspect SSL traffic with TLS 1.3	Yes	Yes, except TLS 1.3
SSL Decryption	SSL Decryption method via gateway and client-based	Yes	No
Web-Based GUI	Access and manage web-based interface via web browser	Yes	Yes, except NetXplorer Client (Java-based)
Anti-Malware	Protection against viruses, worms, trojans, spyware and etc	Yes with AI-based	Yes
URL/Web-Filtering	Protect user against illegal or inappropriate web content	Yes	Yes
Content Audit	Detect and prevent data exposure to the Internet	Yes	Yes, except client-based applications
DDOS/DOS Protection	Protection against suspicious connection for malicious activities	No, only DOS outbound connection	Yes, both inbound and outbound
Endpoint Security Compliance	Detect, identify and access control on endpoint devices within the network	Yes	No

Summary Feature Comparison – Sangfor IAG vs Allot SSG

Feature	Description	IAG	SSG
Asset Discovery	Detect and discover any IoT or onboarding assets within the network	Yes	No
Asset Identification	Identify and classify assets based on passive network scanning profiling	Yes	No
Shadow IT	Support SaaS application discovery grouping for sanctioned and unsanctioned applications	Yes	Yes
Internal Reporting	Support for built-in reporting	Yes	No
External Reporting	Support for external reporting	Yes	Yes
VPN/Proxy Avoidance	Detect and block any VPN/Proxy avoidance applications for bypass Internet access protection	Yes	Yes
Bandwidth Management Channel	Support granular control on bandwidth management with parent, child, line channel	Yes	Yes
Bandwidth Management Objects	Support traffic management based on user, group, application, location and terminal	Yes	Yes
Bandwidth Allocation	Support bandwidth settings on guarantee and restricted channel with customize prioritization	Yes	Yes
Bandwidth Quota-based Control	Configure quota based on traffic, upload/download speed and quota	Yes	Yes
Dynamic Bandwidth Management	Traffic control policies can be automatically enabled or disabled according to the line idleness or the idleness of a specific channel. Avoid competition among users in a single traffic pipe	Yes	Yes
Separate Bandwidth Management	Ability to detect and differentiate between International and domestic internet access line	Yes	No
Application Categorization Rules	Support applications database including 700+ cloud applications, 1000+ mobile applications and 300+ web applications	Yes	Yes,except less supported signature on mobile applications
Anti-Hotspot	Detect and block illegal Wi-Fi hotspot to avoid any information leakage from endpoint devices	Yes	No