Solution Brief:

Hillstone Networks Intelligent Next-Generation Firewall (iNGFW) and Flowmon Anomaly Detection System (ADS)

Overview

Under the backdrop of network security in this dynamic security landscape, cyberattacking technology has to constantly evolve. The junction between attack and defense is constantly escalating. To manage modern cyberattacks comprehensively and stereoscopically, Hillstone Networks and Flowmon have delivered a strategic partnership to help enterprise customers build a complete cybersecurity defense platform. The joint solution consists of the Hillstone Networks Intelligent Next-Generation Firewall (iNGFW) and Flowmon Anomaly Detection System (ADS).

Flowmon ADS is a modern security system for signature-less detection of anomalies and patterns of undesirable network behavior, which is based on an analysis of data flow in the network traffic. The main objective of the solution is to increase the external and internal security of a network. The main advantage over standard Intrusion Detection Systems (IDS) lies in the orientation of the overall behavior of the device on a network, which allows security administrators to respond to yet unknown or specific threats for which the signature is not available. An integrated dashboard displays a quick overview of the latest events and overall statistics of events. This allows for immediate identification of any issues or problematic devices in the network.

With the goal of ensuring granular application security, the next-generation firewall from Hillstone Networks provides users with visualization and elaborate application security management through multi-dimensional business contexts such as application, user, content, as well as geographical location. It delivers a comprehensive threat detection and protection of the L2-L7 layers, using a patented behavioral analysis detection technology, accurate detection of variant malware, and location of the host at risk. It effectively protects network health and server security while providing excellent network performance. It visualizes the risks and cyber-attacks so that they form a closed loop for the security administrator.

www.hillstonenet.com
Phone: 1-800-889-9860

The Joint Solution

The Hillstone Networks iNGFW and Flowmon ADS work in conjunction with each other to support the deployment of linked security policies. The iNGFW of Hillstone Networks is mainly used for threat prevention of external networks in the solution. Flowmon ADS (deployed on Flowmon Collector) mainly detects the internal network threats in the solution and passes the internal threat information to the iNGFW from Hillstone Networks, in order to complete the risk interception of internal threat.

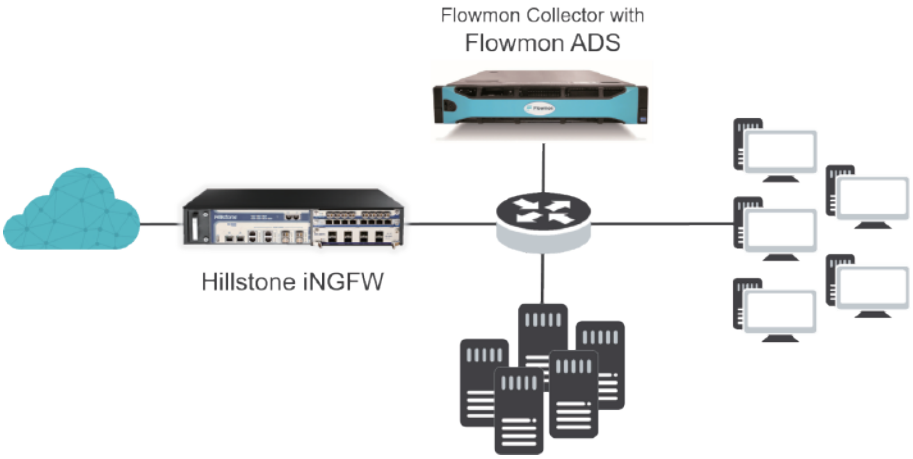

Figure 1. Deployment Scenario

With the easy configurations, the customer can instantly benefit from the Hillstone iNGFW and Flowmon ADS, as well as the joint solution. The detection capability of Flowmon ADS provides Hillstone iNGFW more information and context about the advanced threats, to take more prompt and efficient action to protect the customer critical assets from breach.

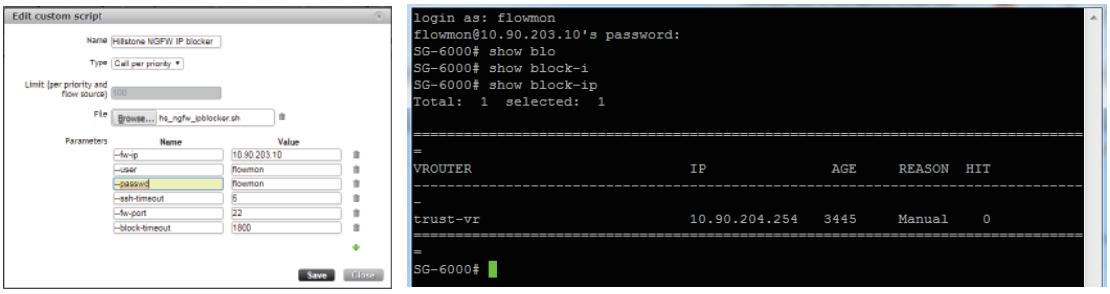

Figure 2. Joint Solution Configurations

Conclusion

Hillstone Networks iNGFW and Flowmon ADS constitute a network security protection solution, which can effectively intercept the threat from the Internet and internal networks, defend against modern network attacks, comprehensively cover the overall network security posture, and make the internal network and external network stable and reliable, as well as secure and credible.