Hillstone Security Management Platform

Hillstone Security Management (HSM) is a powerful management system that provides advanced security operation efficiency, secure SD-WAN management, Zero Trust Network Access (ZTNA) control, and more—all from a single pane of glass. This system enables organiz ations to efficiently manage and monitor devices, orchestrate and manage SD-WAN solutions, and implement granular security access with zero trust. Additionally, HSM offers a unified firewall policy analyzer to identify and address abnormal policies across multi-vendor firewalls, and serves as a local signature database server, ensuring seamless, timely updates even in restricted network environments.

Product Highlights

Efficient Security Operations Management

The Hillstone Security Management (HSM) platform offers comprehensive centralized management for Hillstone's NGFW, NIPS, ADC, and WAF, as well as third-party devices via SNMP. With Hillstone HSM, security administrators can efficiently manage and monitor all devices, including device status, resource usage, license management, while streamlining configuration settings, firmware updates, and signature database upgrades. Addtionally, HSM provides centralized security policy management for Hillstone NGF W and NIPS devices, as well as centralized monitoring of application services of all managed ADC devices. For WAF devices, HSM enables seamless site configuration, policy management, and log management. This centralized approach not only simplifies device management but also enhances operational efficiency and visibility, providing improved monitoring and control across the entire security infrastructure.

Secure SD-WAN

HSM also functions as the SD-WAN controller, leveraging Hillstone's advanced NGFW with built-in intrusion prevention, threat defense, malware protection, and URL filtering to deliver secure SD-WAN solutions for organizations of all sizes. With zero-touch provisioning, preconfigured settings enable fast, error-free device deployment, reducing overhead and boosting reliability. HSM automates VPN overlay orchestration, supporting various architectures such as hub-and-spoke and mesh topologies, and enables quick deployment of business workflows from branch offices to headquarters or the cloud with just a few clicks. The HSM SD-WAN dashboard provides dynamic device health status with underlay and overlay network quality such as delay, jitter, packet loss, etc . HSM's intelligent traffic steering, based on applications, policies, and real-time network conditions, optimizes the user experience. HSM empowers organizations to optimize their network infrastructure with confidence by reducing costs, improving operational efficiency, and delivering a highly secure SD-WAN experience.

Zero-Trust Network Access

HSM allows you to centrally manage and monitor the ZT NA gateways in real time. This helps improve operational efficiency while providing visibility into the users and endpoints. It also supports the unified distribution of

Product Highlights (Continued)

ZTNA policies including policy packages and device-specific policies, which enables administrators to enforce fine-grained zero-trust access control with efficiency. With unified ZTNA management, organizations benefit from increased efficiency and a better remote access control solution.

Unifed Firewall Policy Analyzer

HSM serves as a policy analyzer for firewall policy configurations from various vendors, including both Hillstone NGFWs and third-party NGFWs. It identifies redundant, hidden, or empty policies, as well as policies with overly broad addresses or port ranges, and high-risk port usage. HSM generates detailed reports highlighting abnormal policies and provides actionable recommmendations for remediation. This enables organizations to detect and address security vulnerabilities in their firewall policy configurations, ensuring a more secure and optimized security posture.

Local Signature Database Server

HSM functions as a local signature server in environments where network limitations prevent direct access to external signature update services. By managing updates locally, HSM reduces reliance on external connections, ensuring that Hillstone security products receive bulk signature database updates promptly and consistently. This streamlined approach keeps your defenses up-to-date, reducing operational risk and maintaining a strong security posture, even in restricted or private cloud environments.

Features

Security Device Management

- Support displaying device name, device serial number, software version, hardware platform, management IP, unprocessed alarms, signature database version, new connection and session, etc.
- Support graphical display of the CPU utilization, memory utilization, and traffic of the device
- Support custom widgets for device overview monitoring and dashboard display
- Support device information export
- Support firewall image switching
- Support remote WebUI and CLI access management
- Support route and interface management
- Support immediate and scheduled device reboot
- Support centralized management of Hillstone NGFWs
- Support displaying device status and related service
- Support global and individual device policy management
- Support iQoS policy management
- Support policy management for IPv6 environment
- Support individual device source NAT configuration
- Support service and service group configuration
- Support application and application group configuration
- Support schedule configuration
- Support address book configuration
- Support AAA server configuration
- Support application resource and application resource group tag management
- Support local user configuration
- Support management of system template, network template, and device authorization
- Support firmware and signature database upgrade
- Support device replacement with efficient service, configuration, monitoring and log data inheritance
- Support configuration file management
- Support security zone configuration
- Support IPSec VPN configuration and monitoring
- Support configuration for system administrators, trusted hosts, management interfaces, SNMP, DNS servers, mail servers, and NTP servers
- Support centralized management of NIPS

ADC Device Management

- Support ADC device overview
- Support server load balancing overview
- Support device interface and routing management
- Support device license management
- Support device firmware upgrades
- Support configuration file management

WAF Device Management

- Support WAF device and threat overview
- Support WAF resource pools configuration
- Support remote access control for managed WAF devices
- Support WAF log management
- Support WAF device alerts

Third-Party Device Management

- Support third-party device overview, including statistics on online status, device type distribution, alert level distribution, CPU and memory usage
- Support management by device groups
- Support adding, deleting, modifying, and querying managed devices
- Support trend analysis of device CPU and memory usage
- Support alerts for offline/online status and CPU and memory usage thresholds

SD-WAN Management

- Support displaying overview statistics of SD-WAN devices, alarm, traffic and device distribution statistics
- Support monitoring of WAN link, tunnel link, SD-WAN user, SD-WAN application
- Support SD-WAN alarm board display and alarm rule configuration
- Support Star, Mesh and Dedicated Line Networking
- Support networking configuration including domain name, IPSec VPN and custom IKE name
- Support WAN port modification and link change
- Support automatically or manually assigning address pools when networking

- Support application-aware traffic steering
- Support smart routing and tracking
- Support comprehensive SD-WAN report export and display
- Support daily, weekly, monthly and on-demand report generation
- Support SD-WAN device management
- Support branch device onboarding via email-based or USB-based Zero-Touch Provisioning (ZTP), customizable ZTP template

ZTNA Management

- Support displaying statistics of online devices, ZTNA access users, and ZTNA authorization overview
- Support displaying statistics of online users and recent total user
- Support displaying statistics of online endpoints and endpoint tags
- Support endpoint information and endpoint tag configuration
- Support online user list and forced user offline
- Support ZTNA policy package configuration
- Support ZTNA policy configuration of a single device
- Support ZTNA device management

Policy Analysis Management

- Support NGFW policy analysis of multiple third-party vendors
- Support management of the configuration file parsing signature database
- Support policy audit rule configuration

Signature Database Server

- Support offline update of signature databases, including the intrusion prevention database, virus filtering database, botnet database, application signature database, URL signature database, AV intelligent file engine database, IP reputation database, IP geolocation database, WAF rule database, and WAF IP reputation database
- Support offline update of the signature database engine

Alarm Management

- Support general device alarm management
- Support SD-WAN alarm management
- Support ZTNA alarm management
- Support ADC alarm management

System and Task Management

- Support displaying and monitoring of system information
- Support user and role management
- Support contact and contact group management
- Support AAA server management
- Support system upgrade and signature database upgrade
- Support license viewing, application and installation
- Support system operations, diagnostic tools
- Support monitoring process health status at CLI and automatic recovery in case of abnormality
- Support Email / WeCom notifications
- Support network, access IP/Port and trust host management
- Support password policy management
- Support task and specific task log details view
- Support system logo and name customization
- Support alarm and rule configuration of system CPU , memory and HDD utilization
- Support system log query
- Support trusted host management
- Support batch deployment of CLI commands
- Support device inspection
- Support batch deployment of system configurations
- Support log management for Firewall, NIPS, and ADC devices
- Support log forwarding to third-party log servers
- Support comprehensive device reports
- Support integration with Hillstone iSource XDR, allowing direct access to the HSM homepage and SD-WAN dashboard from iSource
- Northbound APIs support for sending security policies, routing, SNAT settings, device configurations, and performance data (CPU, memory, traffic) from the managed HillstoneNGFW and NIPS devices to third-party systems
- Northbound APIs support for sending basic information, status, CPU, and memory usage of the managed third-party devices to third-party systems

Specifications

Recommended Hardware Configuration for vHSM-P

Devices Supported (Default / Max.)	0 / 100	0 / 500	0 / 1000 systems	0 / 3000
vCPU Requirement	8	16	24	16 (Hyper-Threading)
Memory Requirement	16 GB	32 GB	64 GB	128 GB
Port Requirement	2 ports	2 ports	2 ports	2 ports
Hard Disk Requirement (Min.)	250 GB	250 GB	250 GB	250 GB
Virtual Environment Requirement	Vmware Exsi 6.5 or above /VMware Workstation 12 Pro or above /KVM CentOS 7 or above /KVM Ubuntu 14.04 or above /Hyper-V 10.0.19 or above / Amazon AWS /Microsoft Azure / Huawei Cloud /Tianyi Cloud / Alibaba Cloud			