

# Hillstone Security Management for SD-WAN

Hillstone Security Management (HSM) for SD-WAN is a powerful management system that provides advanced security and operation efficiency, secure SD-WAN management, and Zero Trust Network Access(ZTNA) control from a single pane of glass. This system enables organizations to efficiently manage and monitor devices, easily orchestrate and manage SD-WAN solution, and implement granular security access with zero trust.

## Product Highlights

### Efficient Security Operation Management

The Hillstone Security Management for SD-WAN(HSM for SD-WAN) simplifies management and streamlines security operations. With centralized device management, which support up to 3,000 devices, this system enables network administration through a single console. It includes an intuitive dashboard to monitor resource usage and supports configuring device settings, firmware upgrades, and signature database upgrades. It also allows administrators to centrally manage global policies while deploying security policies for an individual device.

### Simplified Orchestration with VPN Overlay Automation

By building templates for configurations and policies, HSM for SD-WAN automates establishment of the VPN overlay network with support of numerous transports for IPsec tunnels and a variety of architectures, including hub-and-spoke (single and dual hub) and mesh topology (full mesh and partial mesh). It also allows you to simply orchestrate and deploy the business workflow from a new branch office to the headquarter or to any public cloud with a few simple clicks.

### Intelligent Routing With Application Awareness

Hillstone leverages high network visibility, various supported transports and StoneOS's application awareness capability to enable application performance optimization. HSM for SD-WAN ensures an optimum user experience by intelligently

steering traffic based on the apps or services, the policies enforced, and the dynamic status of transport. It natively supports ECMP with link load balancing and active-passive failover for high availability.

### Zero-Touch Provisioning

HSM for SD-WAN possesses a central management system that allows you to preconfigure settings necessary for zero-touch provisioning to occur, which include upgrading firmware, installing licenses, and deploying policies. It enables quick bring-up of devices in field deployment without introducing any configuration errors, which could significantly reduce configuration overhead, speed up delivery of services and increase reliability, especially in large-scale deployments.

### Deep Network Visibility with Dynamic Health Monitoring

HSM for SD-WAN consolidates dynamic device health status with underlay and overlay network quality such as delay, jitter, packet loss, etc. The iconic full-screen dashboard with a view of global distribution of devices, rich real-time status and alarms, and statistical information, makes daily operation far more efficient. It provides not only real-time alarms through webUI, email or social apps, but also brings enhanced data analytics for transport availability and statistics of historical data for further troubleshooting and optimization.

## Product Highlights (Continued)

### Zero-Trust Network Access

HSM allows you to centrally manage and monitor the ZTNA gateways in real time. This helps improve operational efficiency while providing visibility into the users and endpoints. It also supports the unified distribution of ZTNA policies including policy packages and individual device 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.

### Fully Integrated Security

HSM for SD-WAN brings centralized security policies and consistent network segmentation across the entire infrastructure. It also leverages the advanced Hillstone NGFW that natively integrates intrusion prevention, attack defense, malware protection, and URL filtering capability to provide perimeter protection for organizations of all sizes. It supports Hillstone's A-Series, E-Series, E-Pro Series and X-Series NFGWs as well as Hillstone CloudEdge virtual NGFW as its manageable devices.

## 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 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

### 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 service publishing
- 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 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

### 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 comprehensive device reports
- Support integration with Hillstone iSource XDR, allowing direct access to the HSM homepage and SD-WAN dashboard from iSource

## Specifications

### Recommended Hardware Configuration for vHSM-P

<b>Devices Supported (Default / Max.)</b>	0 / 100	0 / 500	0 / 1000	0 / 3000
<b>vCPU Requirement</b>	8	16	24	16 (Hyper-Threading)
<b>Memory Requirement</b>	16 GB	32 GB	64 GB	128 GB
<b>Port Requirement</b>	2 ports	2 ports	2 ports	2 ports
<b>Hard Disk Requirement (Min.)</b>	250 GB	250 GB	250 GB	250 GB
<b>Virtual Environment Requirement</b>	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			

**NOTES:**

(1) HSM for SD-WAN currently are only available for HSM 5.X release.