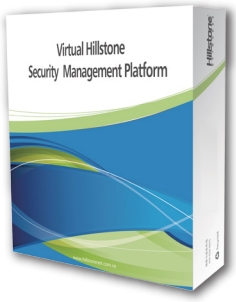
Hillstone Security Management Platform



Hillstone's Security Management Platform enhances network security by allowing businesses to segment their networks into multiple virtual domains. Domains can be based on geography, business unit or security function. It provides the versatility needed to manage Hillstone's infrastructure while simplifying configuration, accelerating deployment cycles, and reducing management overhead.

Product Highlights

Multi-Domain Security

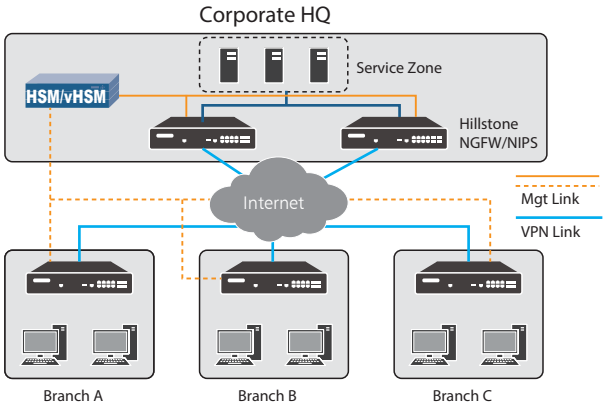
Most companies face security challenges when their business spans offices located in several regions or countries. Multiple security gateways, multiple sites requiring different security policies and multiple administrators can quickly create a complex security environment. Organizations need the tools to manage global security policies while allowing regional administrators to manage devices and users in their geographic location or business division. Hillstone's Security Manager allows the primary administrator to segment security management into multiple virtual domains. It provides the security, visibility, and control required by organizations while reducing management costs, simplifying configuration, and accelerating deployment cycles.

SD-WAN

HSM serves as the centralized Security Manager in Hillstone's SD-WAN solution, offers centralized policy management and global visibility, allowing one-click set-up and deployment of SD-WAN networking from a central console.

Simplified Provisioning and Management

Hillstone's Multi-Domain Security Management simplifies the provisioning of new devices. It allows a primary administrator to create groups of devices for other administrators to monitor and manage. The primary administrator can download global policies, security updates, and policy updates, while local administrators provide policies for local devices, users, and groups. Administrator also can lock the using rules and object configuration to improve the security and reliability of device configuration.



Features

Domain Based Management
- Segregate networks into multiple virtual domains based on location, business unit or security function
- Define global security policy templates and assign them to virtual domains
- Multiple global security policies may be created
- Virtual domains share global security policies and generate separate policies for specific users/groups and devices
- Shared objects can be assigned and used across domains

Role-based Administration
- Administrators assigned to specific domains and devices
- Hierarchical role-based management (administrator, operator, auditor) inherit different privileges
- Multiple administrators can work on separate domains simultaneously

Centralized Management
- Single security console manages multiple domains
- Graphical interface to view, create and manage all domains
- Create groups of devices for administrators to manage
- Assign global policies to multiple management domains
- Create role based administrators to manage policies and devices
- Device registration supported by IP, domain name or template
- Detect redundant policies, useless objects, and policy hits
- Create policy snapshots and rollback policies
- Support policy assistant
- Centralized management of route, NAT and security policies
- Centralized management of IPS/AV/SLB/URL/iQoS policy
- Centralized management of firewall password
- AAA Server, user, role configuration management
- Supports virtual appliance management

Centralized Monitoring
- Monitor all multi-domain system components including Hillstone NGFW, CloudEdge, NIPS, sBDS, ADC and HSA from a central location
- Monitor device availability including CPU, memory, concurrent sessions, and traffic from each domain
- Monitor VPN topography graphs for each registered device
- View network status and VPN link alerts
- Monitor security events from each domain including IP, URLs, applications, and threats
- View trends for device traffic, user traffic, application traffic
- Monitor license and signature update status for devices
- View Top 10 Threats, and Top 10 URLs accessed, last 1 hour threat stats, last 1 hour alarm stats

Log Management
- Logs produced for device traffic, system resource utilization, security events, data security, application usage and device upgrade
- Logs may be filtered by device
- Logs produced for HSM system
- Logs can be exported for historical log queries and backups
- Support log forwarding to third-party syslog server

Configuration Management
- Device IP, domain name, and template registration
- Device software version number
- Device configuration file comparison
- Configuration file backup and recovery
- Support to lock configuration file of device
- IPS, APP, AV, URL signature upgrade configuration centralized management
- Support Firewall HA, including HA cluster management for Hillstone firewalls in Active-Passive/Active-Active/Active-Peer modes, HA groups relationship and status display

VPN Network Monitoring
- VPN topology monitoring
- Network status monitoring
- Link interruption alarm

System Management
- Time zone configuration, support for daylight saving time
- HSM file system automatically fix
- Configuration synchronization prompt
- HSM system password protection

High Availability
- Support HSM HA deployment, Master/Slave roles
- Preemption mode
- Monitor/Log Synchronization
- Automatic Synchronizing and Manual Synchronizing
- Master/Slave Switchover Alarm

Distributed Deployment
- Standalone/Master/Slave modes
- Register up to 16 slave devices on one master device
- Memory alarm, CPU alarm, disk alarm, and slave device offline alarm display on master device

Centralized Reporting
- More than 30 built-in report templates
- Customized reporting: detailed and merged logging report with custom filters by event severity, firewall, protocol, source/destination IP, source/destination port, user, application/service, ingress interface, rule/policy number, action, close reason.
- Reports available in HTML and PDF format

Alerts
- Multiple types of alerts including real-time and threshold-based alerts
- Device security event alerts
- vHSM do not support SMS Alert

IPv6
- IPv6-compliant security policy, NAT, address book configuration & management
- IPv6 log collection and query
- IPv6 monitoring data collection and presentation

Device Inspection
- Manual inspection, regular inspection, intelligent inspection
- Batch inspection

Ticketing System
- Ticket creation, processing, review and deployment
- Ticket batch import and review
- Policy redundancy check
- Device auto identification
- Provide API to connect with other ticketing system

SD-WAN Management
- VPN Star Networking and Mesh Networking
- VPN network management
- Device and link status monitoring
- Support branch device onboarding via ZTP, customizable ZTP template
- Easy SD-WAN business deployment

vHSM
- Support VMware WorkStation, EXSi, KVM
- Support AWS platform

Specifications

HSM Appliance Specification

	HSM-500-D4	HSM-100-D4
Log Performance	5,000 EPS	2,500 EPS
Devices Supported (Default / Max.) (1)	15 / 500	15 / 150
Storage Capacity	4 TB	2 TB
Fixed I/O Ports	2 x GE	2 x GE
RAID Levels	RAID 5	RAID 0
Power Supply	Single/dual 550W	Single 450W
Height	1U	1U

Virtual Appliance (vHSM) Specification

	15/25	15/100	15/500	15/1000
Log Performance	1,000 EPS	2,000 EPS	5,000 EPS	10,000 EPS
vCPU Requirement	4	8	18	24
Memory Requirement	4 GB	16 GB	32 GB	64 GB
Port Requirement	2 ports	2 ports	2 ports	2 ports
Hard Disk Requirement (Min.)	100 GB	2 TB	4 TB	8 TB
Virtual Environment Requirement	VMware Workstation/ESXi or KVM			

NOTES:

(1) The default number of devices that HSM manages is only valid with the HSM platform license. It can be extended to the maximum number with the HSM extension license.

Version: EX-08.01-HSM4.7.0-0221-EN-01