Hillstone S-Series

Network Intrusion Prevention System (NIPS)

As the threat landscape continues to evolve aggressively, an increasing number of network protection technologies have quickly emerged. Among these various technologies, Intrusion Prevention System (IPS) remains one of the most widely deployed solutions, regardless of platform or form factor. Hillstone Network-based IPS (NIPS) appliance operates in-line, and at wire speed, performing deep packet inspection, and assembling inspection of all network traffic. It also applies rules based on several methodologies, including protocol anomaly analysis and signature analysis to block threats. In addition, NIPS leverages AI technology to achieve DDoS protection and encrypted traffic detection without decryption for intelligent and efficient threat protection. Hillstone NIPS can be deployed in the network to inspect traffic left undetected by perimeter solutions, and is an integral part of network security systems for its high-performance, no compromise, best-of- breed protection capability and broad and flexible deployment scenarios.

© 2026 Hillstone Networks All Rights Reserved.

Product Highlights

Unparalleled Threat Protection without Performance Compromise

The Hillstone NIPS platform has the most comprehensive high performance inspection engine, combined with the best- of-breed signature partnering with leading technology partners, providing customers the highest threat detection rate with the lowest total cost of ownership (TCO). Hillstone IPS engine has 99.6% blocking rate of static exploits and 98.325% blocking rate of live exploits (reported by NSS Labs).

The Hillstone NIPS platform provides high throughput, low latency and maximum availability to maintain efficient security operations without compromising network performance. NIPS combines protocol analysis, threat reputation and other features that deliver threat protection from Layer 2 to Layer 7, including ARP attack, Dos/DDoS attack, abnormal protocols, malicious URLs, malwares and web attacks.

Ease of Deployment and Centralized Management

Deploying and managing the Hillstone NIPS is simple, with minimum overhead. It can be deployed in the following modes to meet security requirements and ensure optimal network connectivity:

- Active protection (intrusion prevention mode), real time monitoring and blocking.
- Passive detection (intrusion detection mode), real time monitoring and alert.

The Hillstone NIPS can be managed by the Hillstone Security Management Platform (HSM). Administrators can centrally register, monitor, and upgrade NIPS devices deployed in different branches or locations, with a unified management policy across the network for maximum efficiency.

Granular Reporting with User Targeted Viewpoints

Hillstone NIPS provides comprehensive visibility based on protocol, application, user and content. It can identify more than 7,000 applications, including hundreds of mobile and cloud applications.

Bringing multiple sources together, the system can identify contextual information to make proper blocking decisions. With a granular and robust reporting function, it offers visibility across different views:

- Unique templates, based on whether you are a business system administrator, a security administrator or the CIO or executive.
- Organized Threat Content – whether a security, system risk, network threat or traffic view – in order to help you clearly understand the risk and make the right decision.

© 2026 Hillstone Networks All Rights Reserved.

Features

Intrusion Prevention

- 12,700+ signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia
- IPS Actions: monitor, block, reset (attackers IP or victim IP, incoming interface) with expiry time
- Packet logging option
- Filter based selection and review: severity, target, OS, application or protocol
- IP exemption from specific IPS signatures
- IDS sniffer mode
- IPv4 and IPv6 rate-based DoS protection with threshold settings against TCP Syn flood, TCP/UDP/SCTP port scan, ICMP sweep, TCP/UDP/SCIP/ICMP session flooding (source/destination)
- Active bypass with bypass interfaces
- Predefined prevention configuration
- Support web server protection, including CC attack, external link attack, iframe, cross-site request forgery (CSRF) attack, sensitive file scanning attack, etc.
- Support protection of brute force attack including FTP, MSRPC, POP3, SMTP, SUNRPC, telnet, VNC, RDP, SSH, SMB, LDAP, IMAP and HTTP, SVN, CVS, RSH, Mongodb, Oracle, MSsql, NNTP, REDIS, IRC, RTSP, Casandra, Rlogin, FireBird, Kerberos, SIP, RADIUS, DB2, PGSQL, Sybase, REXEC, SOCKET5 protocols
- Support weak password detection for FTP, POP3, SMTP, Telnet, IMAP, HTTP, Cassandra, DB2, PGSQL, RLOGIN, Sybase, REXEC, SOCKET5, NNTP, REDIS, IRC, RTSP protocols
- Support advanced evasion detection for port remapping, IP/TCP fragmentation, and URL/Unicode encoded malicious payloads
- Support user-defined protocol inspection depth with configurable scan lengths exceeding 4KB
- Support importing/exporting custom weak passwords in the weak password dictionary, with a maximum capacity of 200,000 items
- Support HTTP plaintext password detection
- Threat Details support URI and Attack Data Decoding
- Support MPLS frame inspection
- Support scanning and parsing base64-encoded data
- Detect abnormal encrypted traffic without decryption
- Support global IP whitelist

Threat Correlation Analytics

- Correlation among unknown threats, abnormal behavior and application behavior to discover potential threat or attacks
- Multi-dimension correlation rules, automatic daily update from the cloud

Advanced Threat Detection

- Behavior-based advanced malware detection
- Detection of more than 2000 known and unknown malware families including Virus, Worm, Trojan, Spyware, Overflow etc.
- Real-time, online, malware behavior model database update
- Support mapping detected threats to MITRE ATT&CK tactics
- Support automated Attack Surface Management (ASM)
- Support parsing of X-Forwarded-For (XFF), X-Real-IP, and cdn-src-ip headers

Abnormal Behavior Detection

- Behavior modeling based on L3-L7 baseline traffic to reveal anomalous network behavior, such as HTTP scanning, Spider, SPAM, SSH/FTP weak password, and spyware
- Detection of DDoS including Flood, Sockstress, zip of death, reflect, DNS query, SSL DDos and application DDoS
- Supports inspection of encrypted tunneling traffic for unknown applications
- Real-time, online, abnormal behavior model database update

Antivirus

- Manual, automatic push or pull signature updates
- Flow-based antivirus: protocols include HTTP/HTTPS, SMTP, POP3, IMAP, FTP, SMB, support virus filtering and blocking of files transferred with SMB protocol when resuming from breakpoint
- Compressed file virus scanning
- Intelligent virus detection for PE, ELF, PDF and Microsoft Office files
- Support custom MD5 and URL blocklists/allowlists with external dynamic list integration
- Support compressed file scanning across multiple archive formats including Zip, Rar, 7z, and Tar, with up to 100 recursive decompression layers
- Support dual Antivirus detection engines, including MD5-based detection and AI-powered detection

Attack Defense

- Abnormal protocol attack defense
- Anti-DoS/DDoS, including SYN Flood, DNS Query Flood defense, SIP Flood defense, etc.
- IP scanning and port scanning
- Intelligent DoS/DDoS defense with ML-based baseline establishment
- Attack defense for Internet Control Message Protocol (ICMP) redirection, ARP, and Malformed Packet

URL Filtering

- Flow-based web filtering inspection
- Manually defined web filtering based on URL, web content and MIME header
- Dynamic web filtering with cloud-based real-time categorization database: over 500 million URLs with 64 categories (8 of which are security related)
- Additional web filtering features:
  - Filter Java Applet, ActiveX or cookie
  - Block HTTP Post
  - Log search keywords
  - Exempt scanning encrypted connections on certain categories for privacy
- Web filtering profile override: allows administrator to temporarily assign different profiles to user/group/IP
- Web filter local categories and category rating override
- Support allow/block list
- Customizable alarm

Anti-Spam

- Real-time spam classification and prevention
- Confirmed spam, suspected spam, bulk spam, valid bulk
- Protection regardless of the language, format, or content of the message
- Support both SMTP and POP3 email protocols
- Inbound and outbound detection
- Whitelists to allow emails from trusted domain/email addresses
- User-defined blacklists

Cloud-Sandbox

- Upload malicious files to cloud sandbox for analysis
- Support protocols including HTTP/HTTPS, POP3, IMAP, SMTP and FTP
- Support file types including PE, ZIP, RAR, Office, PDF, APK, JAR and SWF
- File transfer direction and file size control
- Provide complete behavior analysis report for malicious files
- Global threat intelligence sharing, real-time threat blocking
- Support detection only mode without uploading files

Data Security

- Content filtering: file types include doc, docx, xls, xlsx, ppt, pptx, txt; file protocols include FTP, HTTP(S), SMTP(S), POP3(S), IMAP(S), SMB
- Support file filtering with over 100 file formats
- Support network behavior recording

Botnet C&C Prevention

- Discover intranet botnet host by monitoring C&C connections and block further advanced threats such as botnet and ransomware
- Regularly update the botnet server addresses
- Prevention for C&C IP and domain
- Support TCP, HTTP, DNS and TLS protocols detection
- Support Domain Generation Algorithm (DGA) detection
- IP and domain whitelists
- Support manually/automatically imports multiple C2 threat intelligence, and exporting custom threat intelligence

© 2026 Hillstone Networks All Rights Reserved.

Features (Continued)

IP Reputation
- Identify and filter traffic from risky IPs such as botnet hosts, spammers, Tor nodes, breached hosts, and brute force attacks
- Logging, dropping packets, or blocking for different types of risky IP traffic
- Regular IP reputation signature database upgrade

Application Control
- Over 4,000 applications that can be filtered by name, category, subcategory, technology and risk
- Each application contains a description, risk factors, dependencies, typical ports used, and URLs for additional reference
- Actions: block, monitor
- Provide multi-dimensional monitoring and statistics for applications running in the cloud, including risk category and characteristics
- Support encrypted application

Quality of Service (QoS)
- Support encrypted application
- Max/guaranteed bandwidth tunnels or IP/user basis
- Tunnel allocation based on security domain, interface, address, user/user group, server/server group, application/app group, TOS, VLAN
- Bandwidth allocated by time, priority, or equal bandwidth sharing
- Type of Service (TOS) and Differentiated Services (DiffServ) support
- Prioritized allocation of remaining bandwidth
- Maximum concurrent connections per IP
- Bandwidth allocation based on URL category
- Bandwidth limit by delaying access for user or IP

IPv6
- Management over IPv6, IPv6 logging and HA
- IPv6 tunneling, DNS64/NAT64 etc.
- IPv6 routing protocols, static routing, policy routing, ISIS, RIPng, OSPFv3 and BGP4+
- IPS, Application identification, Antivirus, Access control, ND attack defense

VSYS
- System resource allocation to each VSYS
- CPU virtualization
- Non-root VSYS support IPS, URL filtering, Policy, QoS, etc.
- VSYS monitoring and statistics
- Support backup of all VSYS configurations at once

SSL Proxy
- SSL offload: SSL traffic decryption
- SSL require/ exempt: SSL traffic allowed or block based on the policy rules without decryption
- IP and domain whitelists

Flexible Traffic Analysis and Control
- Support 3 operation modes: Route/NAT (layer 3), Transparent (layer 2) with optional bypass interface, and TAP mode (IDS Mode) with Hillstone Firewall Integration
- Traffic analysis and control based on policy rules by source/destination zone, source/destination IP address, users, service or applications

High Availability
- Redundant heartbeat interfaces
- AP and peer mode
- Standalone session synchronization
- HA reserved management interface
- Failover:
  - Port, local & remote link monitoring
  - Stateful failover
  - Sub-second failover
  - Failure notification
- Deployment Options:
  - HA with link aggregation
  - Full mesh HA
  - Geographically dispersed HA

Visible Administration
- Management access: HTTP/HTTPS, SSH, telnet, netconf, console
- Central Management: Hillstone Security Manager (HSM), web service APIs
- Two-factor authentication: username/password, HTTPS certificates file
- System Integration: SNMP, syslog, alliance partnerships
- Upload threat data to iSource for analysis
- Rapid deployment: USB auto-install, local and remote script execution
- Dynamic real-time dashboard status and drill-in monitoring widgets
- Storage device management: storage space threshold customization and alarm, old data overlay, stop recording
- Support packet upload and reply via WebUI
- Language support: English
- Support CLI access from WebUI

Logs and Reporting
- Logging facilities: local storage for up to 6 months, multiple syslog servers and multiple Hillstone Security Audit (HSA) platforms
- Encrypted logging and log integrity with HSA scheduled batch log uploading
- Reliable logging using TCP option (RFC 3195)
- Detailed traffic logs: forwarded, violated sessions, local traffic, invalid packets
- Comprehensive event logs: system and administrative activity audits, routing & networking, VPN, user authentications, WiFi related events
- Support displaying attack result and associated user account in threat logs
- Threat log evidence display and highlighting
- Log aggregation: support aggregation of AV and C&C logs
- IP and service port name resolution option
- Brief traffic log format option
- Granular Reporting with User Targeted Viewpoints
  - HA Management/C-level View
  - Business System Owner View
  - Network Security Administrator View
- Send alert notifications of event logs via SMS, WeCom, Feishu, and Ding Talk; Send alert notifications of threat logs via WeCom, Feishu, and Ding Talk

Statistics and Monitoring
- Application, URL, threat events statistic and monitoring
- Real-time traffic statistic and analytics
- System information such as concurrent session, CPU, Memory and temperature
- iQOS traffic statistic and monitoring, link status monitoring
- Support traffic information collection and forwarding via Netflow (v9.0)
- Cloud-based threat intelligence push service
- Geographical distribution of external network attacks
- Statistical analysis and retrospective analysis of threat events from asset-centric, attacker-centric, and threat-centric perspectives
- Specialized risk monitoring for mining, ransomware, and weak password
- Support threat remediation

Network Configuration
- Support Jumbo Frame forwarding

CloudView
- Cloud-based security monitoring
- 24/7 access from web or mobile application
- Device status, traffic and threat monitoring
- Cloud-based log retention and reporting

© 2026 Hillstone Networks All Rights Reserved.

Specifications

	S1115-IN	S1200-IN	S1215-IN	S1900-IN	S2100-IN
					
IPS Throughput [1]	2 Gbps	3 Gbps	3 Gbps	3 Gbps	5 Gbps
Maximum Concurrent Connections, TCP (Standard/with AEL) [2]	1.2 Million	1.2 Million	1.2 Million	1.2 Million	1.2 Million
New Connections per Second, HTTP [3]	30,000	40,000	40,000	50,000	60,000
Stoneshield	N/A	N/A	N/A	N/A	N/A
Virtual Systems (Default/ Max)	1/5	1/5	1/5	1/5	1/5
Storage [4]	500 GB / 1 TB SSD	500 GB / 1 TB SSD	500 GB / 1 TB SSD	500 GB / 1 TB SSD	500 GB / 1 TB SSD
Form Factor	1U	1U	1U	1U	1U
Management Ports	2 × USB port, 1 × MGT port, 1 × Console port, 1 × HA	2 × USB port, 1 × MGT port, 1 × Console port	2 × USB port, 1 × MGT port, 1 × Console port, 1 × HA	2 × USB Port, 1 × MGT, 1 × Console Port	2 × USB port, 1 × MGT port, 1 × Console port
Fixed I/O Ports	8 × SFP, 8×GE (including 2 pairs Bypass port),	2 ×SFP+, 8 × SFP.8 × GE	8 × GE (including 2 pairs Bypass port), 8 × SFP	8 × GE (including 1 pair Bypass port)	2 ×SFP+, 8 × SFP 8 ×GE
Available Slots for Expansion Modules	1 x Generic Slot	N/A	1 x Generic Slot	N/A	N/A
Expansion Module Option	IOC-S-F-4SFP+-A-IN IOC-S-F-8SFP+-A-IN IOC-S-F-8GE-B-A-IN	N/A	IOC-S-F-4SFP+-A-IN IOC-S-F-8SFP+-A-IN IOC-S-F-8GE-B-A-IN	N/A	N/A
Latency	<300 µs	<300 µs	<300 µs	<70 µs	<350 µs
Bypass Support (Default/Max.)	4/12	N/A	4/12	2/2	N/A
Power Supply	AC 100-240V 50/60 Hz	AC 100~240V 50/60Hz	AC 100-240 V 50/60 Hz	DC-36~-72V AC100-240V50/60Hz	AC 100-240 V 50/60 Hz
Maximum Power Consumption	60W 1 × AC power supply 2 × AC power supply	50W 1 × AC power supply 2 × AC power supply	60W 1 × AC power supply 2 × AC power supply	50W 1 × AC power supply 2 × AC power supply	50W 1 × AC power supply 2 × AC power supply
Dimension (W×D×H, mm)	17.3 × 13.4 × 1.7 in (440 × 340 × 44 mm)	17.3 × 12.6 × 1.7 in (440 × 320 × 44 mm)	17.3 × 13.4 × 1.7 in (440 × 340 × 44 mm)	17.1 × 12.6 × 1.7 in (436 × 320 × 44mm)	17.3 × 12.6 × 1.7 in (440 × 320 × 44mm)
Weight	10.0 lb (4.55 kg)	17 lb (7.7 kg)	10.0 lb (4.55 kg)	14.33 lb (6.5kg)	16.9 lb (7.7kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% (no dew)	10%~95% (no dew)	10-95% (no dew)	10%-95% (no dew)	10%-95% (no dew)

© 2026 Hillstone Networks All Rights Reserved.

Specifications (Continued)

	S2115-IN	S2300-IN	S2700-IN	S3500-IN	S3805-IN
					
IPS Throughput [1]	5 Gbps	9 Gbps	11 Gbps	15 Gbps	20 Gbps
Maximum Concurrent Connections, TCP (Standard/with AEL) [2]	1.2 Million	3 Million	6 Million	8 Million	12 Million
New Connections per Second, HTTP [3]	60,000	60,000	60,000	140,000	250,000
Stoneshield	N/A	N/A	N/A	N/A	N/A
Virtual Systems (Default/ Max)	1/5	1/5	1/50	1/50	1/50
Storage [4]	500 GB / 1 TB SSD	500 GB / 1 TB SSD	500 GB / 1 TB SSD	1 TB SSD	1 TB SSD
Form Factor	1U	1U	1U	1U	1U
Management Ports	2 × USB port, 1 × MGT port, 1 × Console port, 1 × HA port	2 × USB port, 1 × MGT port, 1 × Console port, 1 × HA port	2 × USB port, 1 × MGT port, 1 × Console port, 1 × HA port	2 × USB port, 1 × MGT port, 1 × Console port, 1 × HA port	2 × USB port, 1 × MGT port, 1 × Console port, 1 × HA port
Fixed I/O Ports	8 × SFP, 8 × GE (including 2 pairs Bypass port)	2 × SFP+, 8 × SFP, 16 × GE (including 2 pairs Bypass port)	2 × SFP+, 8 × SFP, 16 × GE (including 2 pairs Bypass port)	2 × SFP+, 8 × SFP, 16 × GE (including 2 pairs Bypass port)	2 × QSFP+, 16 × SFP+, 8 × GE (including 4 pairs Bypass port)
Available Slots for Expansion Modules	1 x Generic Slot	N/A	1 x Generic Slot	1 x Generic Slot	1 x Generic Slot
Expansion Module Option	IOC-S-F-4SFP+-A-IN IOC-S-F-8SFP+-A-IN IOC-S-F-8GE-B-A-IN	N/A	IOC-S-4SFP+-A-IN IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN IOC-S-2QSFP+-A-IN	IOC-S-4SFP+-A-IN IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN IOC-S-2QSFP+-A-IN	IOC-S-4SFP+-A-IN IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN IOC-S-2QSFP+-A-IN
Latency	<300 µs	<300 µs	<300 µs	<300 µs	<300 µs
Bypass Support (Default/Max.)	4/12	4/4	4/4	4/4	8/8
Power Supply	AC 100-240 V 50/60 Hz	AC 100~240V 50/60Hz	AC 100-240 V 50/60 Hz	DC -36~ -72 V AC 100-240 V 50/60 Hz	DC -36~ -72 V AC 100-240 V 50/60 Hz
Maximum Power Consumption	60W 1 × AC power supply 2 × AC power supply	100W 1 × AC power supply 2 × AC power supply	100W 1 × AC power supply 2 × AC power supply	100W 2 × AC power supply 2 × DC power supply	280W 2 × AC power supply 2 × DC power supply
Dimension (WxDxH, mm)	17.3 × 13.4 × 1.7 in (440 × 340 × 44 mm)	17.2 × 17.2 × 1.7 in (436 × 437 × 44mm)	17.1 × 17.2 × 1.7 in (436 × 320 × 44mm. Not include expansion module)	17.1 × 17.2 × 1.7 in (436 × 320 × 44mm, Including power module handle)	17.1 × 21.3 × 1.7 in (436 × 542 × 44mm, Including power module handle)
Weight	10.0 lb (4.55 kg)	20.7 lb (9.4 kg)	20.9 lb (9.5kg, Including accessories and all packages)	26.0 lb (11.8kg, Including accessories and all packages)	32.6 lb (14.8kg, Including accessories and all packages)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% (no dew)	10%~95% (no dew)	10%~95% (no dew)	10%~95% (no dew)	10%~95% (no dew)

© 2026 Hillstone Networks All Rights Reserved.

Specifications (Continued)

	S3900-IN	S3915-IN	S5500-IN
			
IPS Throughput [1]	25/40 Gbps	30 Gbps	45/75 Gbps
Maximum Concurrent Connections, TCP (Standard/with AEL) [2]	12 Million	15 Million	24 Million
New Connections per Second, HTTP [3]	380,000	380,000	550,000
Stoneshield	N/A	N/A	N/A
Virtual Systems (Default/ Max)	1/50	1/50	1/50
Storage [4]	1 TB SSD	1 TB SSD	1 TB SSD
Form Factor	1U	1U	1U
Management Ports	2 × USB port, 1 × MGT port, 1 × Console port, 2 × HA port (SFP+)	2 x USB Port, 1 × MGT port, 1 x Console port, 1 × HA port	2 x USB port, 1 × MGT port, 1 x Console port, 1 × HA port (SFP+)
Fixed I/O Ports	6 × SFP+, 16 × SFP, 8 × GE (including 2 pairs Bypass port)	2 × QSFP+, 16 × SFP+, 8 x GE (including 4 pairs Bypass port)	2 × QSFP+, 16 × SFP+, 8 × GE (including 4 pairs Bypass port)
Available Slots for Expansion Modules	1 x Generic Slot	1 x Generic Slot	1 x Generic Slot
Expansion Module Option	IOC-S-4SFP+-A-IN IOC-S-2QS-FP+-A-IN IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN	IOC-S-4SFP+-A-IN IOC-S-2QSFP+-A-IN IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN	IOC-S-4SFP+-A-IN IOC-S-2QSFP+-A-IN IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN
Latency	<300 µs	<300 µs	<300 µs
Bypass Support (Default/Max.)	4/4	8/8	8/8
Power Supply	DC -36~ -72 V AC 100-240 V 50/60 Hz	DC -36~ -72 V AC 100-240 V 50/60 Hz	DC -36~ -72 V AC 100-240 V 50/60 Hz
Maximum Power Consumption	280W 2 × AC power supply 2 × DC power supply	280W 2 × AC power supply 2 × DC power supply	320W 2 × AC power supply 2 × DC power supply
Dimension (WxDxH, mm)	17.1 × 21.3 × 1.7 in (436 × 542 × 44mm. Including power module handle)	17.1 × 21.3 × 1.7 in (436 × 542 × 44mm. Including power module handle)	17.1 × 21.3 × 1.7 in (436 × 542 × 44mm)
Weight	32.6 lb (14.8kg, Including accessories and all packages)	32.6 lb (14.8kg, Including accessories and all packages)	32.6 lb (14.8kg, Including accessories and all packages)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10%~95% (no dew)	10%~95% (no dew)	10%~95% (no dew)

© 2026 Hillstone Networks All Rights Reserved.

Module Options

Module	IOC-S-F-4SFP+-A-IN	IOC-S-F-8SFP+-A-IN	IOC-S-F-8GE-B-A-IN	IOC-S-4SFP+-A-IN
I/O Ports	4 × SFP+ Ports (for Front Panel)	8 × SFP+ Ports (for Front Panel)	8 × GE, including 4 bypass pairs (for Front Panel)	4 × SFP+, SFP+ module not included
Dimension	1U	1U	1U	1U
Weight	0.55 lb (0.25 kg)	0.62 lb (0.28 kg)	0.6 lb (0.27 kg)	2.09 lb (0.96 kg)

Module	IOC-S-2MM-BE-A-IN	IOC-S-2SM-BE-A-IN	IOC-S-2QSFP+-A-IN
I/O Ports	4 × SFP, MM bypass (2 pairs of bypass ports)	4 × SFP, SM bypass (2 pairs of bypass ports)	2 × QSFP+
Dimension	1U	1U	1U
Weight	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)

NOTES:

(1) IPS throughput data is obtained under HTTP traffic with all IPS rules being turned on. The data for S3900-IN/S5500-IN can be increased to 40/75 Gbps via additional IOC-S-2QSFP+-A-IN expansion module;

(2) Maximum concurrent connections are obtained under TCP traffic; and it can be upgraded with Additional Enhanced License (AEL);

(3) New Connections per Second are obtained under HTTP traffic with all IPS rules being turned off;

(4) 1TB storage for S1115-IN, S1200-IN, S1215-IN, S1900-IN, S2100-IN, S2115-IN, S2300-IN and S2700-IN is only available on devices equipped with dual AC power supplies; The actual available space is smaller and may vary depending on the operating system for management space reservation.

Unless specified otherwise, all performance, capacity and functionality are based on NIPS 6.1. Results may vary based on NIPS version and deployment.

© 2026 Hillstone Networks All Rights Reserved.
Version: EX-08.01-NIPS-V6.1-0326-EN-01

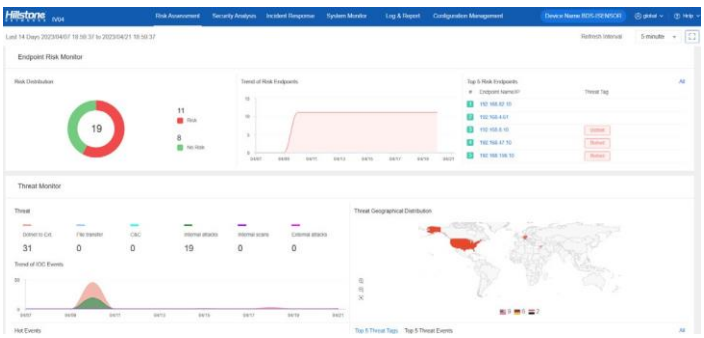
Hillstone Network Detection and Response




Hillstone Network Detection and Response (NDR) provides a robust solution for detecting and responding to sophisticated attacks like ransomware and crypto-mining malware. Hillstone NDR, with its product, the Breach Detection System (BDS), combines proven methods, such as signature- based detection and threat intelligence, with advanced machine learning to analyze user behavior and uncover hidden threats. Once a threat is detected, Hillstone NDR provides deep threat hunting and visibility, helping security administrators quickly identify Indicators of Compromise (IOCs), locate compromised hosts, and reconstruct the entire attack chain. For a complete defense, it integrates with both Hillstone and third-party Next-Generation Firewalls (NGFWs), as well as our iSource XDR system, to automatically mitigate threats and ensure your enterprise assets are comprehensively protected.

Product Highlights

Comprehensive Threat Correlation Analytics for Advanced Threat Detection



Cyber attackers have become ever more sophisticated, using targeted, persistent, stealthy and multi-phased attacks, which can easily evade perimeter detection. Hillstone BDS boasts a diverse range of detection capabilities, including Advanced Threat Detection (ATD), Abnormal Behavior Detection (ABD), deception threat detection, intrusion and attack detection, virus and spam detection, and botnet C&C detection. Hillstone's threat correlation platform analyzes the details of the relationships of each individual suspicious threat event as well as other contextual information within the network, to connect the dots and provide accurate and effective malware and attack detection with high confidence levels.

© 2026 Hillstone Networks All Rights Reserved.

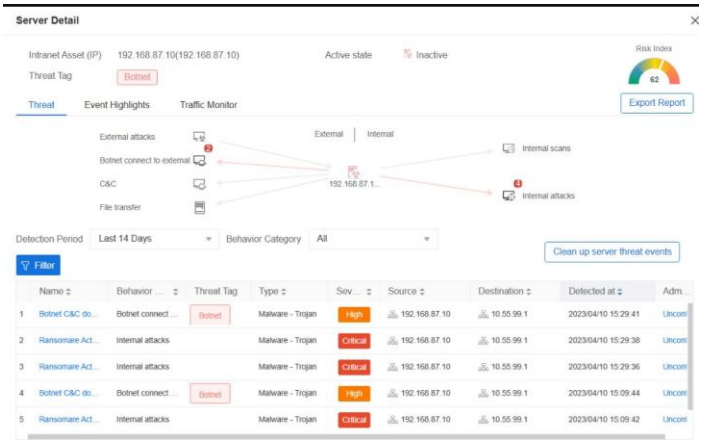
Product Highlights (Continued)

Real-time Threat Monitoring for Critical Servers and Hosts

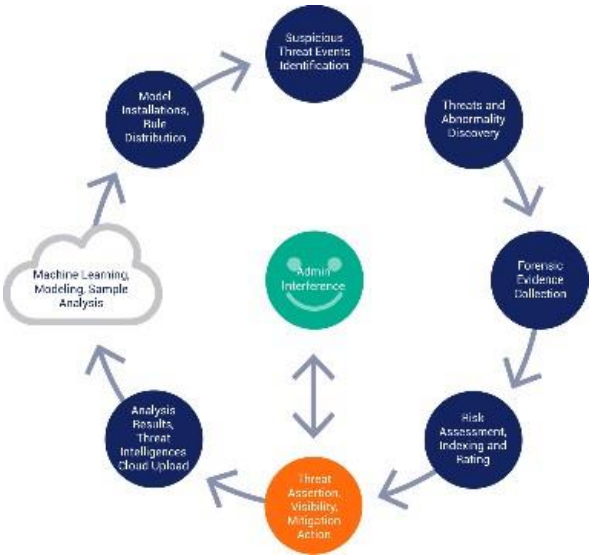
Hillstone NDR focuses on protecting critical servers within the intranet, detecting unknown and 0-day threat attacks and finding abnormal network and application level activities of server and host machines. Once a threat or an abnormal behavior is detected, Hillstone NDR will perform threat or behavioral analysis and use topology-based graphic presentations to provide extensive visibility into the threat details and behavioral abnormalities. This gives security admins unprecedented insights into the attack progress, traffic trending in each direction, as well as the entire network risk assessment.

Complete Indicator of Compromises and Cyber Attack Chain

IOCs events are threat events detected during the post breach attack. They are identified among large numbers of the threat attacks in the network that are directly associated with the protected server or host. IOCs are typically seen as threat activities with higher risk and with a high confidence level that a server or host is being compromised and that poses a potentially bigger threat to the critical assets within the corporate network. To effectively detect IOCs and perform deep threat detection on these IOCs is critical in throttling the goal of stealing important data from critical assets, and preventing a threat attack from further spreading within the network. Hillstone NDR drills down and surfaces more threat analysis and intelligence on these IOC events, reconstructing the attack chain based on these IOCs and correlating other threat events associated with these IOCs within time and space spectrums.



Rich Forensic Information and Preemptive Mitigation



Hillstone NDR conducts threat mitigation with conjunction of Hillstone A-Series NGFW, and X-Series data center NGFW, as well as third-party NGFW devices. After the security admin or network operators analyze and validate threat alerts, they can add threat elements such as IP addresses, type of threats etc., to the blacklist or security policies, and then synchronize them to the firewalls so that future attacks from the same breeds or malware family can be blocked at the network perimeter. This prevents future attacks from spreading to broader network territories.

© 2026 Hillstone Networks All Rights Reserved.

Features

Abnormal Behavior Detection

- Behavior modeling based on L3-L7 baseline traffic to reveal anomalous network behavior, such as HTTP scanning, Spider, SPAM
- Detect DDoS including Flood, Sockstress, zip of death, reflect, DNS query, SSL and application DDoS
- Support inspection of encrypted tunneling traffic for unknown applications
- Real-time, online, abnormal behavior model database update
- Support the detection of RDP/VNC/SMB/SSH/FTP brute force attack, TOR based suspicious HTTP requests
- Support detecting and alerting on remote access software

Advanced Threat Detection

- Behavior-based advanced malware detection
- Detect more than 2,000 known and unknown malware families including Virus, Worm, Trojan, Overflow, etc.
- Real-time, online, malware behavior model database update
- Detect major ransomware and cryptomining malware
- Support threat detection on encrypted traffic without decryption
- Support threat detection for encrypted HTTPS, SMTPS, POP3S, and IMAPS traffic by decryption in TAP mode

Threat Correlation Analytics

- Correlation among unknown threats, abnormal behavior and application behavior to discover potential threat or attacks
- Multi-dimension correlation rules, automatic daily update from the cloud
- Deception Threat Detection
- Local deception engine with regular deception models update
- Simulate to Web, Doc or Database Servers, support protocols including FTP , HTTP, MYSQL, SSH and TELNET

Intrusion Detection

- 35,000+ signatures, protocol anomaly detection and rate-based detection
- Custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia
- Over 20 types of protocols anomaly detection , including HTTP , SMTP , IMAP , POP3, VOIP, NETBIOS, VxLAN, MPLS, etc
- Support for buffer overflow , SQL injection and cross -site scripting attack detection
- Support weak password detection for protocols of FTP/HTTP/SMT/ POP3/IMAP/TELNET/Cassandra/DB2/IRC/NNTP/PGSQL/REDIS/ Rexec/Rlogin/ RTSP/Socket5/Sybase
- Support advanced evasion detection, including port remapping, IP/TCP fragmentation, and URL/Unicode encoding bypass techniques
- Support customizable protocol inspection depth with configurable scan lengths exceeding 4KB
- Support reverse shell detection
- Support capturing complete attack packets
- Support plaintext password detection in HTTP traffic
- Support brute-force detection for over 30 applications/protocols

Antivirus

- Over 15 million virus signature database and online real-time update
- Support compressed file scanning across multiple archive formats including Zip, Rar, 7z, and Tar, with up to 100 recursive decompression layers
- Support custom MD5 and URL blocklists/allowlists with external dynamic list integration
- Support configuring MD5 and URL whitelists
- Support dual Antivirus detection engines, including MD5-based detection and AI -powered detection

Botnet C&C Detection

- Support discovering intranet botnet host by monitoring C&C connections
- Support detecting C&C IP and domain name in TCP, HTTP and DNS traffic
- Support C&C traffic detection over TCP, HTTP, DNS, and TLS encrypted protocols
- Support detecting C & C channels based on Domain Generation Algorithms (DGA)
- Support importing threat intelligence through standardized protocols including STIX, OpenIOC, and JSON
- Support auto-update the botnet C&C defense signature database

Anti-Spam

- Real-time spam classification and prevention• Confirmed Spam, Suspected Spam, Bulk Spam, Valid Bulk
- Protection regardless of the language, format, or content of the message
- Support both SMTP and POP3 email protocols
- Whitelists to allow emails from trusted domain/email addresses

Cloud-Sandbox

- Upload malicious files to cloud sandbox for analysis
- Support protocols including HTTP, SMTP, POP3, IMAP4 and FTP
- Support file types including PE, APK, JAR, MS-Office, PDF, SWF, RAR, ZIP
- Provide complete behavior analysis report for malicious files
- Global threat intelligence sharing, real-time threat blocking
- Multiple static detection engines quickly filter normal files and known threats
- Unknown threat visualization based on logs, reports, monitoring information, file behavior reports

Attack Detection

- Abnormal protocol attack detection
- Support DoS/DDoS detection, including SYN Flood, DNS Query Flood, with intelligent DDoS mitigation based on baseline learning
- ARP attack detection
- Support WEB attack detection based on WAF rules for abnormal HTTP protocol , DDoS attack, injection attack, cross-site attack, special vulnerability attack, information leakage, detection access, malicious software, illegal access to resources
- WEB detection function whitelist

Application Identification

- Over 4,000 applications, including IM, p2p, file transfer, email, online games, media streaming, etc
- Multi-dimension application statistic based on zones, interface, location, user, and IP address
- Support for Android, IOS mobile applications

ARP Spoofing Detection

- Prevent ARP spoofing by IP-MAC binding and APR packet inspection

Monitoring

- Dynamic, real-time dashboard status and drill-in monitoring widgets
- Intranet risk monitoring projection
- Overview of internal network risk status, including TOP5 risk server/ computer list and threat trends, critical assets risk status, host risk status, threat severity and type, external attack geo-locations, etc
- Visual details of threat status for critical assets and other risky hosts, including risk level, risk certainty, attack geo- location, attack chain uncovering and other statistical information
- Support active scanning for assets; scanning results can be uploaded to Hillstone XDR platform iSource
- Support automated attack surface management
- Visual details of network threat events, including threat analysis, knowledge
- base, MITRE ATT&CK® tactic details, MITRE ATT&CK® technique details, history and topology
- Send alert notifications via Email, SMS, WeCom, Feishu, DingTalk and Trap
- Cloud-based threat intelligence push service

Threat Mitigation

© 2026 Hillstone Networks All Rights Reserved.

Features (Continued)

- Admin actions to change threat events status, open, false positive, fixed, ignore, confirmed
- One-click cleanup of server/computer threat and reevaluation of host security
- Threat events whitelist, including threat name, source/destination IP, hit count, etc.
- Support integration with Hillstone and third-party firewalls to block threats
- Sysmon endpoint service integration
- Support global threat detection whitelist for centralized exemption management across all detection policies
- Threat hunting
- Support MITRE ATT&CK® framework mapping
- Support identification of attackers and victims in threat logs

Critical Protection Mode

- Support one-click Critical Protection Mode with built-in global policy template for instant hardening and lossless rollback
- Support signature updates with high-frequency refresh during Critical Protection Mode

Logs & Reporting

- Three predefined reports: Security, Flow and System reports
- Support user defined reporting
- Reports can be exported in PDF, Word and HTML format via Email and FTP
- Logs, including events, networks, threats, and configuration logs
- Logs can be exported via Syslog or Email

Administration

- Monitor internal network hosts and servers: name, OS, browser, type, and network threat statistics
- Management access: HTTP/HTTPS, SSH, telnet, console
- Device condition alerts, including CPU usage, memory usage, disc usage, new session and concurrent sessions, interface bandwidth, chassis temperature and CPU temperature
- Alerts based on application bandwidth and new connection
- Support for three types of alerts: email, text message, trap
- Unknown threat visualization based on logs, reports, monitoring information, file behavior reports
- Seamless integration with 3rd party network management system
- Support High Availlability
- Support web-based CLI access to the device directly through the management GUI
- Support web-based CLI access to the device directly through the management GUI

RESTful APIs

- Support standard RESTful APIs for accessing hardware/system/threat event information

Centralized Management

- Support registering devices to Hillstone Security Management Platform (HSM)
- Support 24/7 monitoring of multiple devices, traffic and threat via Hillstone CloudView (web or mobile)
- Support uploading threat logs, evidential packets, NetFlow, metadata to Hillstone iSource XDR for threat analysis
- Support integration with third- party threat Intelligence to detect malicious files, URLs and IP addresses

Specifications

	I-1870-IN	I-2860-IN
		
Breach Detection Throughput [1]	1 Gbps	2 Gbps
New Sessions/s [2]	25,000	50,000
Maximum Concurrent Sessions [2]	750,000	1.5 Million
Form Factor	1 U	1 U
Storage	1T SSD	1T SSD
Management Ports	2 x USB port 1 x RJ45 port 1 x MGT	2 x USB port 1 x RJ45 port 2 x MGT
Fixed I/O Ports	2 × SFP+ 8 × SFP 8 × GE	2 × SFP+ 8 × SFP 16 × GE
Available Slots for Expansion Modules	N/A	1 x Generic Slot
Expansion Module Option	N/A	IOC-A-BDS-4SFP+-IN
Power Supply	AC 100-240V, 50/60Hz	AC 100-240V, 50/60Hz
Power Specification	50W, Single AC	100W, Dual AC Redundant
Dimension (W×D×H, mm)	17.2 x 12.6 x 1.7 in (436 x 320 x 44mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)
Weight	9 lb (4.1 kg)	18.7 lb (8.5 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% (no dew)	10-95% (no dew)

© 2026 Hillstone Networks All Rights Reserved.

Specifications (Continued)

	I-3860-IN	I-5860-IN
		
Breach Detection Throughput [1]	5 Gbps	10 Gbps
New Sessions/s [2]	120,000	500,000
Maximum Concurrent Sessions [2]	3 Million	6 Million
Form Factor	1 U	1 U
Storage	1T SSD	2T SSD
Management Ports	2 x USB port 1 x RJ45 port 3 x MGT	2 x USB port 1 x RJ45 port 2 x MGT
Fixed I/O Ports	6 ×SFP+ 16 × SFP 8 × GE	2 × QSFP+ 16 × SFP+ 8 × GE
Available Slots for Expansion Modules	1 x Generic Slot	1 x Generic Slot
Expansion Module Option	IOC-A-BDS-4SFP+-IN	IOC-A-BDS-4SFP+-IN
Power Supply	AC 100-240V, 50/60Hz	AC 100-240V, 50/60Hz
Power Specification	289W, Dual AC Redundant	382W, Dual AC Redundant
Dimension (W×D×H, mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)	17.2 x 17.2 x 1.7 in (436 x 437 x 44mm)
Weight	22.5 lb (10.2 kg)	22.5 lb (10.2 kg)
Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% (no dew)	10-95% (no dew)

Specification and Minimum Hardware Configuration

	IV04-IN	IV08-IN
Breach Detection Throughput [3]	Up to 1.5 Gbps	Up to 3 Gbps
CPU Support (Min.)	4 Core	8 Core
Memory (Min.)	8G	16G
Storage (Min.)	100G	100G
System Requirement	KVM / Vmware ESXi version 6.5 or above	KVM / Vmware ESXi version 6.5 or above
Public Cloud Support	Alibaba Cloud / Tencent Cloud	Alibaba Cloud / Tencent Cloud

Network Interface Card Supported

	SR-IOV	All NICs except SR-IOV
KVM	√ (only SR-IOV X710 can be supported)	√
Vmware	×	√

© 2026 Hillstone Networks All Rights Reserved.

Module Options

Module	IOC-A-BDS-4SFP+-IN
I/O Ports	4 x SFP Ports
Dimension	1U (Occupies 1 generic slot)
Weight	0.42 lb (0.19 kg)

Recommended Sysmon Configuration

Specification	Sysmon Server	Sysmon Client
CPU	4 Core	\
Memory	16G	1G
Storage	1T HDD, extendable	40G HDD
Installation Package	OVF Mirror	MSI Service Program
System Requirement	VMware ESXi	Windows 7 / Windows Server 2008 or above

NOTES:

(1) Breach detection throughput is measured under bidirectional HTTP traffic with all threat detection features enabled;
(2) The data reflects performance with web attack detection disabled. Performance may vary if it's enabled;
(3) Breach detection throughput varies based on hardware configuration.
Unless specified otherwise, all performance are based on BDS 5.0. Results may vary based on BDS version and deployment.

© 2026 Hillstone Networks All Rights Reserved.
Version:EX-08.01-BDS-V6.1-0326-EN-01

HAFS
Distributeur à valeur ajoutée WCA

Vous accompagne

www.hafs-networks.com
Visitez notre site web

sales-ci@hafs-networks.com
Envoyez-nous un e-mail

(+225) 07 69 32 13 55
Contact commercial 1

(+225) 07 59 05 85 82
Contact commercial 2

Distributeur à Valeur Ajoutée de Solutions de Cybersécurité | Réseaux | Wi-Fi | HCI/Sauvegarde

Hillstone NETWORKS | Synology | SANGFOR | SECPOINT | Axidian | NEOWAVE | HORNETSECURITY FORMERLY V vade | CyberShield

RUCKUS NETWORKS | Ruijie Reyee | RAY | Wiflyx | SEARCHINFORM | MOBOTIX | EXTRAVIS | HAFS MediVision