Hillstone E-Pro Series

Next-Generation Firewall

The Hillstone E-Pro Series Next Generation Firewall (NGFW) is designed for comprehensive security with superior price performance. It provides granular visibility and control of applications. Advanced system architecture and dedicated hardware acceleration capabilities allow the E-Pro Series to secure all traffic with fine-grained control without compromising performance. The Hillstone E-Pro Series NGFW incorporates advanced firewall features, offers excellent energy efficiency, and a flexible, affordable and easy-to-manage solution that delivers comprehensive threat protection and improved security posture.

Product Highlights

Multi-Dimensional Granular Control

Hillstone's E-Pro Series provides admins with rich security features and flexible controls. The E-Pro Series provides precise identification and application-aware control through deep application inspection to intelligently and accurately identify thousands of applications and help admins identify security risks across multiple dimensions. It supports a rich set of user authentication methods, including local, TACACS+, RADIUS, LDAP, and authentication based on password, SMS, certificates, token or email. It allows fine-grained user control such as access control, application limits, and bandwidth guarantees. The E-Pro Series NGFW can accurately identify the geographic location of the source/destination IP of an attack, which enables access control to block attacks. The E-Pro Series provides granular control of data in transit, protecting organizations from the leakage of critical, sensitive, or confidential data and files.

Comprehensive Threat Detection and Prevention

Hillstone's E-Pro Series NGFW provides intrusion prevention based on analysis of attacks and deep inspection of applications and protocols, which secures Layers 2-7 of the network by effectively filtering security threats such as viruses, Trojan horses, worms, spyware, vulnerability attacks, and evasion attacks. The E-Pro Series uses an optimized attack identification algorithm to mitigate DoS/DDoS , which ensures the security of the network and the availability of business applications. Hillstone's NGFW offers advanced web attack protection, which not only prevents web attacks such as SQL injection and cross-site scripting, but also defends against web page tampering and similar exploits. The stream scanning based virus detection engine enables low-latency and high-performance filtering in HTTP/HTTPS, FTP, SMB, various mail transfer protocols and compressed files. URL filtering can help network administrators easily control browsing of malicious URLs. A variety of management and

Product Highlights (Continued)

controls can prevent malicious activities concealed in SSL-encrypted traffic including email. Cloud Sandbox, an advanced threat detection engine, can emulate the execution environment and analyze all activities related to malicious files, identify advanced threats and provide comprehensive threat reports as well as rapid remediation.

Advanced Networking Capabilities

Hillstone's E-Pro Series NGFW integrates advanced network adaptability with consistent security enforcement across diverse network environments. Dynamic detection and inbound SmartDNS functions intelligently load balance traffic across multiple links. It significantly improves link utilization and delivers an improved user experience without compromising security. The routing table can be dynamically adjusted according to the network conditions with support of protocols such as RIP, OSPF and BGP. The E-Pro Series also enables high VPN performance through the built-in hardware acceleration capability for large-scale IPsec/SSL VPN deployments.

Full-concurrence and High-performance Architecture

Hillstone's E-Pro Series NGFW delivers high performance with a unique approach, allowing organizations to take advantage of its high throughput, low latency, and high concurrency. Full-concurrence packet processing technology performs all security checks and analysis in a single pass, which reduces processing overhead for complex security features, while delivering consistently high performance. The best-of-breed architecture and proprietary algorithms of Hillstone's StoneOS optimize the session load across all CPU cores to take full advantage of multiple cores.

Unified and Centralized Management

Hillstone's E-Pro Series NGFW supports centralized management via the Hillstone Security Management Platform (HSM). Unified policy management, device configuration management, and real-time security monitoring simplifies deployment, reduces response time for security incidents, improves operational efficiency and reduces TCO. Hillstone's E-Pro Series NGFW also supports the cloud-based Hillstone CloudView security management and analytics platform, which provides real-time monitoring, analysis and alarming of hardware, traffic trends, ranking of apps and users, as well as threat information via a unified web portal or mobile app.

Features

Network Services
- Dynamic routing (OSPF, BGP, RIPv2)
- Static and policy routing
- Route controlled by application
- Built-in DHCP, NTP, DNS Server and DNS proxy
- Tap mode – connects to SPAN port
- Interface modes: sniffer, port aggregated, loopback, VLANS (802.1Q and Trunking)
- L2/L3 switching & routing
- Multicast(PIM-SSM)
- Virtual wire (Layer 1) transparent inline deployment

Firewall
- Operating modes: NAT/route, transparent (bridge), and mixed mode
- Policy objects: predefined, custom, aggregate policy, object grouping
- Security policy based on application, role and geo-location
- Application Level Gateways and session support: MSRCP, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, dcerpc, dns-tcp, dns-udp, H.245 0, H.245 1, H.323
- NAT and ALG support: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN
- NAT configuration: per policy and central NAT table
- VoIP: SIP/H.323/SCCP NAT traversal, RTP pin holing
- Global policy management view
- Security policy redundancy inspection, policy group, policy configuration rollback
- Policy Assistant for easy detailed policy deployment
- Policy analyzing and invalid policy cleanup
- Comprehensive DNS policy
- Schedules: one-time and recurring

Intrusion Prevention
- Protocol anomaly detection, rate-based detection, custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia
- IPS Actions: default, monitor, block, reset (attackers IP or victim IP, incoming interface) with expiry time
- Packet logging option
- Filter Based Selection: 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

Antivirus
- Manual, automatic push or pull signature updates
- Manually add or delete MD5 signature to the AV database
- MD5 signature support uploading to cloud sandbox, and manually add or delete on local database
- Flow-based antivirus: protocols include HTTP, SMTP, POP3, IMAP, FTP/SFTP, SMB
- Compressed file virus scanning

Attack Defense
- Abnormal protocol attack defense
- Anti-DoS/DDoS, including SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment, etc.
- ARP attack defense
- Allow list for destination IP address

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 140 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 multi-language

Cloud-Sandbox
- Upload malicious files to cloud sandbox for analysis
- Support protocols including HTTP/HTTPS, POP3, IMAP, SMTP, FTP and SMB
- Support file types including PE, ZIP, RAR, Office, PDF, APK, JAR, SWF and Script
- 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
- URL allow / block list configuration

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, and DNS traffic detection
- Allow and block list based on IP address or domain name
- Support DNS sinkhole and DNS tunneling detection

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
- Periodical IP reputation signature database upgrade

SSL Decryption
- Application identification for SSL encrypted traffic
- IPS enablement for SSL encrypted traffic
- AV enablement for SSL encrypted traffic
- URL filter for SSL encrypted traffic
- SSL encrypted traffic whitelist
- SSL proxy offload mode
- Support application identification, DLP, IPS sandbox, AV for SSL proxy decrypted traffic of SMTPS/POP3S/IMAPS

Endpoint Identification and Control
- Support to identify endpoint IP, endpoint quantity, on-line time, off-line time, and on-line duration
- Support 10 operating systems including Windows, iOS, Android, etc.
- Support query based on IP, endpoint quantity, control policy and status etc.
- Support the identification of accessed endpoints quantity across layer 3, logging and interference on overrun IP
- Redirect page display after custom interference operation
- Supports blocking operations on overrun IP
- User identification and traffic control for remote desktop services of Windows Server

Data Security
- File transfer control based on file type, size and name
- File protocol identification, including HTTP, FTP, SMTP, POP3 and SMB
- File signature and suffix identification for over 100 file types
- Content filtering for HTTP-GET, HTTP-POST, FTP and SMTP protocols
- IM identification and network behavior audit
- Filter files transmitted by HTTPS using SSL Proxy and SMB

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, reset session, monitor, traffic shaping
- Identify and control cloud applications in the cloud
- Provide multi-dimensional monitoring and statistics for cloud applications, including risk category and characteristics

Quality of Service (QoS)
- 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
- Automatic expiration cleanup and manual cleanup of user used traffic

Server Load Balancing
- Weighted hashing, weighted least-connection, and weighted round-robin

Features (Continued)

- Session protection, session persistence and session status monitoring
- Server health check, session monitoring and session protection

Link Load Balancing

- Bi-directional link load balancing
- Outbound link load balancing: policy based routing including ECMP, time, weighted, and embedded ISP routing; Active and passive real-time link quality detection and best path selection
- Inbound link load balancing supports SmartDNS and dynamic detection
- Automatic link switching based on bandwidth, latency, jitter, connectivity, application etc.
- Link health inspection with ARP, PING, and DNS

VPN

- IPsec VPN
  - IPsec Phase 1 mode: aggressive and main ID protection mode
  - Peer acceptance options: any ID, specific ID, ID in dialup user group
  - Supports IKEv1 and IKEv2 (RFC 4306)
  - Authentication method: certificate and pre-shared key
  - IKE mode configuration support (as server or client)
  - DHCP over IPsec
  - Configurable IKE encryption key expiry, NAT traversal keep alive frequency
  - Phase 1/Phase 2 Proposal encryption: DES, 3DES, AES128, AES192, AES256
  - Phase 1/Phase 2 Proposal authentication: MD5, SHA1, SHA256, SHA384, SHA512
  - IKEv1 support DH group 1,2,5,19,20,21,24
  - IKEv2 support DH group 1,2,5,14,15,16,19,20,21,24
  - XAuth as server mode and for dialup users
  - Dead peer detection
  - Replay detection
  - Autokey keep-alive for Phase 2 SA
- IPsec VPN realm support: allows multiple custom SSL VPN logins associated with user groups (URL paths, design)
- IPsec VPN configuration options: route-based or policy based
- IPsec VPN deployment modes: gateway-to-gateway, full mesh, hub-and-spoke, redundant tunnel, VPN termination in transparent mode
- One time login prevents concurrent logins with the same username
- SSL portal concurrent users limiting
- SSL VPN port forwarding module encrypts client data and sends the data to the application server
- Supports clients that run iOS, Android, and Windows XP/Vista including 64-bit Windows OS
- Host integrity checking and OS checking prior to SSL tunnel connections
- MAC host check per portal
- Cache cleaning option prior to ending SSL VPN session
- L2TP client and server mode, L2TP over IPsec, and GRE over IPsec
- View and manage IPsec and SSL VPN connections
- PnPVPN
- VTEP for VxLAN static unicast tunnel

IPv6

- Management over IPv6, IPv6 logging and HA
- IPv6 tunneling: DNS64/NAT64, IPv6 ISATAP, IPv6 GRE, IPv6 over IPv4 GRE
- IPv6 routing including static routing, policy routing, ISIS, RIPng, OSPFv3 and BGP4+
- IPS, Application identification, URL filtering, Antivirus, Access control, ND attack defense, iQoS
- IPv6 jumbo frame support
- IPv6 Radius support
- IPv6 support on the following ALGs: TFTP, FTP, RSH, HTTP, SIP
- IPv6 support on distributed iQoS
- Track address detection

VSYS

- System resource allocation to each VSYS
- CPU virtualization
- Non-root VSYS support firewall, IPsec VPN, SSL VPN, IPS, URL filtering, app monitoring, IP reputation, QoS
- VSYS monitoring and statistic, app monitoring, IP reputation, AV, QoS

High Availability

- Redundant heartbeat interfaces
- Active/Active and Active/Passive 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

Twin-mode HA (only available on E3960P and above models)

- High availability mode among multiple devices
- Multiple HA deployment modes
- Configuration and session synchronization among multiple devices
- Dual HA data link ports

User and Device Identity

- Local user database
- Remote user authentication: TACACS+, LDAP, Radius, Active Directory
- Single-sign-on: Windows AD
- 2-factor authentication: 3rd party support, integrated token server with physical and SMS
- User and device-based policies
- User group synchronization based on AD and LDAP
- Support for 802.1X, SSO Proxy
- WebAuth: page customization, force crack prevention, IPv6 support
- Interface based authentication
- Agentless ADSSO (AD Polling)
- Use authentication synchronization based on SSO-monitor
- Support IP-based and MAC-based user authentication

Administration

- Management access: HTTP/HTTPS, SSH, telnet, console
- Central Management: Hillstone Security Manager (HSM), web service APIs
- System Integration: SNMP, syslog, alliance partnerships
- Rapid deployment: USB auto-install, local and remote script execution
- Dynamic real-time dashboard status and drill-in monitoring widgets
- Language support: English

Logs & Reporting

- Logging facilities: local log storage with storage models 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, URL etc.
- Comprehensive event logs: system and administrative activity audits, routing & networking, VPN, user authentications, WiFi related events
- IP and service port name resolution option
- Brief traffic log format option
- Three predefined reports: Security, Flow and Network reports
- User defined reporting
- Reports can be exported in PDF, Word and HTML via Email and FTP

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)

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

IoT Security

- Identify IoT devices such as IP Cameras and Network Video Recorders
- Support query of monitoring results based on filtering conditions, including device type, IP address, status, etc.
- Support customized whitelists

Wireless

- Multi-SSID and wireless traffic control (only on E1600WP)

Specifications

	SG-6000-E1600P	SG-6000-E1600WP	SG-6000-E1700P	SG-6000-E2800P	SG-6000-E3662P	SG-6000-E3668P	SG-6000-E3960P	SG-6000-E3968P
								
FW Throughput [1]	4.7 Gbps	4.7 Gbps	4.75 Gbps	8 Gbps	10 Gbps	10 Gbps	10 Gbps	10 Gbps
IPsec Throughput [2]	850 Mbps	850 Mbps	850 Mbps	3 Gbps	3 Gbps	3 Gbps	4 Gbps	4 Gbps
AV Throughput [3]	890 Mbps	890 Mbps	890 Mbps	2.1 Gbps	2.1 Gbps	2.1 Gbps	2.2 Gbps	2.2 Gbps
IPS Throughput [4]	1.2 Gbps	1.2 Gbps	1.2 Gbps	3.3 Gbps	3.3 Gbps	3.3 Gbps	3.9 Gbps	3.9 Gbps
IMIX Throughput [5]	1.7 Gbps	1.7 Gbps	1.7 Gbps	5.3 Gbps	5.3 Gbps	5.3 Gbps	7 Gbps	7 Gbps
NGFW Throughput [6]	470 Mbps	470 Mbps	470 Mbps	1.25 Gbps	1.25 Gbps	1.25 Gbps	1.5 Gbps	1.5 Gbps
Threat Protection Throughput [7]	360 Mbps	360 Mbps	400 Mbps	860 Mbps	900 Mbps	900 Mbps	1.1 Gbps	1.1 Gbps
New Sessions/s [8]	27,000	27,000	28,000	80,000	120,000	120,000	150,000	150,000
Maximum Concurrent Sessions [9]	0.2M	0.2M	0.6M	1M	3M	3M	3.2M	3.2M
IPsec Tunnel Number	512	512	2000	2000	6000	6000	6000	6000
SSL VPN Users (Default/Max)	8 / 128	8 / 128	8 / 500	8 / 1000	8 / 4000	8 / 4000	8 / 6000	8 / 6000
Virtual Systems (Default/Max)	N/A	N/A	1 / 5	1 / 5	1/ 50	1/ 50	1/ 100	1/ 100
Storage	N/A	N/A	N/A	N/A	N/A	256G SSD	N/A	256G SSD
Management Ports	1 x Console Port, 1 x USB Port	1 x Console Port, 1 x USB Port	1 x Console Port, 1 x USB Port	1 x Console Port, 1×USB port	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1x MGT	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1x MGT	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1x MGT	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1x MGT
Fixed I/O Ports	9 x GE	9 x GE	9 x GE	5 x GE, 4 x Combo	6 x GE, 4 x SFP	6 x GE, 4 x SFP	6 x GE (1 bypass pair), 4 x SFP, 2 x SFP+	6 x GE (1 bypass pair), 4 xSFP, 2 x SFP+
Available Slots for Expansion Modules	N/A	N/A	N/A	N/A	2 x Generic Slot	2 x Generic Slot	2 x Generic Slot	2 x Generic Slot
Expansion Module Option	N/A	N/A	N/A	N/A	IOC-4GE-B-P, IOC-8GE-P, IOC-8SFP-P	IOC-4GE-B-P, IOC-8GE-P, IOC-8SFP-P	IOC-4GE-B-P, IOC-8GE-P, IOC-8SFP-P	IOC-4GE-B-P, IOC-8GE-P, IOC-8SFP-P
Twin-mode HA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes
Power Specification	30W, Single AC AC 100-240 V 50/60 Hz	30W, Single AC AC 100-240 V 50/60 Hz	45W, Single AC AC 100-240 V 50/60 Hz	45W, Dual AC Redundant AC 100-240 V 50/60 Hz	150W, Dual AC Redundant AC 100-240 V 50/60 Hz	150W, Dual AC Redundant AC 100-240 V 50/60 Hz	150W, Dual AC Redundant AC 100-240 V 50/60 Hz	150W, Dual AC Redundant AC 100-240 V 50/60 Hz
Dimension (W×D×H, mm)	desktop 12.6×5.91×1.7 in (320×150×44 mm)	desktop 12.6×5.91×1.7 in (320×150×44 mm)	1U 17.4x9.5x1.7 in (442x241x44 mm)	1U 17.4x9.5x1.7 in (442x241x44 mm)	1U 17.2x14.4x1.7 in (436x366x44 mm)	1U 17.2x14.4x1.7 in (436x366x44 mm)	1U 17.2x14.4x1.7 in (436x366x44 mm)	1U 17.2x14.4x1.7 in (436x366x44 mm)
Weight	3.3 lb (1.5 kg)	3.3 lb (1.5 kg)	5.5 lb (2.5 kg)	5.5 lb (2.5 kg)	12.3 lb (5.6 kg)	12.3 lb (5.6 kg)	12.3 lb (5.6 kg)	27.1 lb (11.8 kg)
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)	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)	10-95% (no dew)	10-95% (no dew)	10-95% (no dew)

Module Options

	IOC-8GE-P	IOC-8SFP-P	IOC-4GE-B-P
Names	8GE Expansion Module	8SFP Expansion Module	4GE Bypass Expansion Module
I/O Ports	8 x GE	8 x SFP, SFP module not included	4 x GE Bypass (2 pair bypass ports)
Dimension	½U (Occupies 1 generic slot)	½U (Occupies 1 generic slot)	½U (Occupies 1 generic slot)
Weight	1.8 lb (0.8 kg)	2.0 lb (0.9 kg)	1.8 lb (0.8 kg)

Specifications

	SG-6000-E5260P	SG-6000-E5268P	SG-6000-E5560P	SG-6000-E5568P	SG-6000-E5760P	SG-6000-E5960P	SG-6000-E6368P
							
FW Throughput (1)	20 Gbps	20 Gbps	20 Gbps	20 Gbps	40 Gbps	40 Gbps	90 Gbps
IPsec Throughput (2)	8.4 Gbps	8.4 Gbps	12 Gbps	12 Gbps	18.8 Gbps	25.6 Gbps	64 Gbps
AV Throughput (3)	3.8 Gbps	3.8 Gbps	4.9 Gbps	4.9 Gbps	7.9 Gbps	14 Gbps	28 Gbps
IPS Throughput (4)	8.9 Gbps	8.9 Gbps	9.3 Gbps	9.3 Gbps	18.5 Gbps	18.8 Gbps	37 Gbps
IMIX Throughput (5)	15.5 Gbps	15.5 Gbps	20 Gbps	20 Gbps	36.5 Gbps	40 Gbps	90 Gbps
NGFW Throughput (6)	3.9 Gbps	3.9 Gbps	5.6 Gbps	5.6 Gbps	8.9 Gbps	14 Gbps	26 Gbps
Threat Protection Throughput (7)	2.2 Gbps	2.2 Gbps	3.1 Gbps	3.1 Gbps	5.2 Gbps	8.2 Gbps	18 Gbps
New Sessions/s (8)	200,000	200,000	300,000	300,000	500,000	600,000	1,100,000
Maximum Concurrent Sessions (9)	6M	6M	10M	10M	12M	15M	30M
IPsec Tunnel Number	20,000	20,000	20,000	20,000	20,000	20,000	20,000
SSL VPN Users (Default/Max)	8 / 10,000	8 / 10,000	8 / 10,000	8 / 10,000	8 / 10,000	8 / 10,000	8 / 10,000
Virtual Systems (Default/Max)	1 / 250	1 / 250	1 / 250	1 / 250	1 / 250	1 / 250	1 / 500
Storage	N/A	256G SSD	N/A	256G SSD	N/A	N/A	512G SSD
Management Ports	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1x MGT	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1x MGT	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1x MGT	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1x MGT	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1x MGT	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1x MGT	1 x Console Port, 1 x AUX Port, 1 x USB Port, 1 x HA, 1x MGT
Fixed I/O Ports	4 x GE (1 bypass pair), 4 x SFP, 2 x SFP+	4x GE (1 bypass pair), 4 x SFP, 2 x SFP+	4 x GE (1 bypass pair), 4 x SFP, 2 x SFP+	4 x GE (1 bypass pair), 4 x SFP, 2 x SFP+	4 x GE, 4x SFP	4 x GE, 4x SFP	2 x GE, 8 x SFP+, 2×QSFP+
Available Slots for Expansion Modules	4 x Generic Slot	4 x Generic Slot	4 x Generic Slot	4 x Generic Slot	4 x Generic Slot	4 x Generic Slot	2 x Generic Slot 1 x Bypass Slot
Expansion Module Option	IOC-4GE-B-P IOC-8GE-P IOC-8SFP-P IOC-4SFP+-P IOC-8SFP+-P IOC-2SFP+-Lite-P	IOC-4GE-B-P IOC-8GE-P IOC-8SFP-P IOC-4SFP+-P IOC-8SFP+-P IOC-2SFP+-Lite-P	IOC-4GE-B-P IOC-8GE-P IOC-8SFP-P IOC-4SFP+-P IOC-8SFP+-P IOC-2SFP+-Lite-P	IOC-4GE-B-P IOC-8GE-P IOC-8SFP-P IOC-4SFP+-P IOC-8SFP+-P IOC-2SFP+-Lite-P	IOC-4GE-B-P IOC-8GE-P IOC-8SFP-P IOC-4SFP+-P IOC-8SFP+-P IOC-2SFP+-Lite-P	IOC-4GE-B-P IOC-8GE-P IOC-8SFP-P IOC-4SFP+-P IOC-8SFP+-P IOC-2SFP+-Lite-P	IOC-8GE-P, IOC-8SFP-P
Twin-mode HA	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Power Specification	450W, Dual AC Redundant, AC 100-240 V 50/60 Hz	450W, Dual AC Redundant, AC 100-240 V 50/60 Hz	450W, Dual AC Redundant, AC 100-240 V 50/60 Hz	450W, Dual AC Redundant, AC 100-240 V 50/60 Hz	450W, Dual AC Redundant, AC 100-240 V 50/60 Hz	450W, Dual AC Redundant, AC 100-240 V 50/60 Hz	450W, Dual AC Redundant, AC 100-240 V 50/60 Hz
Dimension (W×D×H, mm)	2U 17.3x20.9x3.5 in (440x530x88 mm)	2U 17.3x20.9x3.5 in (440x530x88 mm)	2U 17.3x20.9x3.5 in (440x530x88 mm)	2U 17.3x20.9x3.5 in (440x530x88 mm)	2U 17.3x20.9x3.5 in (440x530x88 mm)	2U 17.3x20.9x3.5 in (440x530x88 mm)	2.5U 17.3×18.1×4.3 in (440×460×110 mm)
Weight	26.0 lb (11.8 kg)	26.0 lb (11.8 kg)	27.1 lb (12.3 kg)	27.1 lb (12.3 kg)	27.1 lb (12.3 kg)	27.1 lb (12.3 kg)	30.4 lb (13.8 kg)
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)	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)	10-95% (no dew)	10-95% (no dew)

Module Options

	IOC-4GE-B-P	IOC-8GE-P	IOC-8SFP-P	IOC-2SFP+-Lite-P	IOC-4SFP+-P	IOC-8SFP+-P
Names	4GE Bypass Expansion Module	8GE Expansion Module	8SFP Expansion Module	2SFP+ Expansion Module	4SFP+ Expansion Module	8SFP+ Expansion Module
I/O Ports	4 x GE Bypass (2 pair bypass ports)	8 x GE	8 x SFP, SFP module not included	2 x SFP+, SFP+ module not included	4 x SFP+, SFP+ module not included	8 x SFP+, SFP+ module not included
Dimension	½U (Occupies 1 generic slot)	½U (Occupies 1 generic slot)	½U (Occupies 1 generic slot)	½U (Occupies 1 generic slot)	1U (Occupies 2 generic slot)	1U (Occupies 2 generic slot)
Weight	1.8 lbs (0.8 kg)	1.8 lbs (0.8 kg)	2.0 lbs (0.9 kg)	0.7 lbs (0.3 kg)	1.5lbs (0.9 kg)	1.5lbs (0.9 kg)

NOTES:
(1) FW throughput data is obtained under single-stack UDP traffic with 1518-byte packet size;
(2) IPsec throughput data is obtained under Preshare Key AES256+SHA-1 configuration and 1400-byte packet size;
(3) AV throughput data is obtained under HTTP traffic with file attachment;
(4) IPS throughput data is obtained under bi-direction HTTP traffic detection with all IPS rules being turned on;
(5) IMIX throughput data is obtained under UDP traffic mix (64 byte : 512 byte : 1518 byte =5:7:1);
(6) NGFW throughput data is obtained under 64 Kbytes HTTP traffic with application control and IPS enabled;
(7) Threat protection throughput data is obtained under 64 Kbytes HTTP traffic with application control, IPS, AV and URL filtering enabled;
(8) New sessions/s is obtained under TCP traffic;
(9) Maximum concurrent sessions is obtained under HTTP traffic.
Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.5R8. Results may vary based on StoneOS® version and deployment.

Version: EX-08.01-NGFW-E-Pro-Series-5.5R8-0421-EN-01