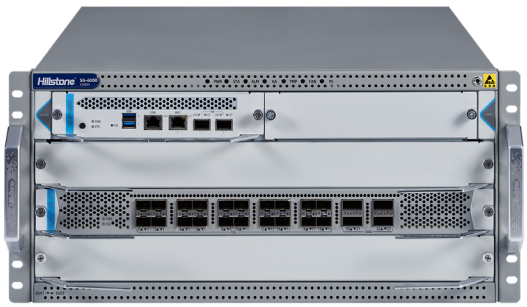
Hillstone X-Series

Data Center Firewall X25803



Front

Rear

The Hillstone X25803 Data Center Firewall is a high-performance DCFW that provides exceptional protection and high availability. It is perfectly crafted to meet the stringent security needs of large enterprises, service providers, and government sectors. With its fully distributed architecture, it delivers high throughput, concurrent connections, and new sessions, allowing you to keep your data center running smoothly. In addition, this product is designed to support large-capacity virtual systems, making it ideal for virtualized environments. The firewall offers a wide range of features, including application identification, intrusion prevention, traffic management and advanced protection against command and control (C&C) communications, ensuring comprehensive network security for data centers.

Product Highlights

High Performance and Scalability

As network traffic continues to surge, data center firewalls need to have robust capabilities that can accommodate a large number of users and respond promptly to sudden spikes in access, including high throughput, concurrent connections and new session processing capabilities. Hillstone X25803 Data Center Firewall addresses this challenge through its innovative, fully distributed architecture that employs intelligent traffic distribution algorithms to implement high-speed processing of traffic on Service and Input/Output Modules (SIOMs). With a single SIOM, it can achieve an impressive 295 Gbps of firewall throughput and support up to 60 million concurrent sessions. The linear scalability with the SIOMs enables a fully equipped X25803 to suppport 880 Gbps firewall throughput, 5 million new sessions per second, and 180 million concurrent sessions, all packed into a space-efficient 5U design. The scalability is also supported by its extensive interfaces. With up to 3 SIOMs, X25803 can provide up to 12 100GE and 60 10GE I/O ports, with a range of connectivity options including 100GE, 40GE, 10GE, and 1GE.

High Availability

Hillstone X25803 data center firewall incorporates high availability into its hardware and software design. It supports

Product Highlights (Continued)

redundant deployment schemes for active/passive and active/active peer modes, ensuring uninterrupted business in the event of a single device failure. It also provides Twin-mode HA to address the challenge of asymmetric traffic in redundant data centers. The twin-mode HA is a highly reliable deployment mode building on dual-device backup, with two sets of active/passive firewalls in separate data centers connected by a dedicated data link and control link. The firewalls synchronize session and configuration information, ensuring uninterrupted system continuity even under the most challenging conditions.

The entire system adopts a modular design, supporting hardware-level redundancy and hot-swappability for key components such as SIOMs, system control modules (SCMs), power modules, and fan modules. The X25803 data center firewall provides dual system control redundancy protection by supporting 2 SCMs. It also supports 2 power supplies and 4 redundant fan trays to maintain an optimal CPU temperature and ensure system continuity.

Leading Virtual Protection Technology

Virtualization technology is ubiquitous in modern data centers as it allows segmented administration of different organizations, business units, or departments within a single physical firewall, ensuring independent management and security of each virtual system without interfering with others. Hillstone X25803 data center firewall supports virtualization by dividing a physical firewall into 1000 virtual systems, each of which can be dynamically allocated resources based on business needs such as CPUs, sessions, policies, and ports. Each virtual system is independently managed, providing separate security panels for different services or users. This isolated network traffic reduces the attack surface and strengthens network security.

Granular Application Control and Comprehensive Security

Hillstone X25803 data center firewall offers advanced in-depth identification and flexible security control for thousands of network applications, including hundreds of mobile applications and encrypted P2P applications through protocol features and behavior analysis, and correlation analysis. This improves network visibility and allows for better control and optimization of network performance. It provides a comprehensive suite of advanced security features, including intrusion prevention, URL filtering, high-performance antivirus, SSL-encrypted traffic protection, and botnet C&C prevention. The firewall also provides intelligent bandwidth management through iQoS, enabling fine-grained, policy-based traffic control, as well as session and policy routing, link, and server load balancing. These enable protection against a wide range of threats and ensure efficient use of network resources.

AI-powered Threat Detection and Analytics

The increasing prevalence of advanced attacks, including zero-day attacks and threats hidden in encrypted traffic, presents a major challenge for organizations. Hillstone X25803 data center firewall leverages AI technology to provide Machine Learning (ML) based threat detection for encrypted traffic without the need for decryption, intelligent DDoS, and DGA protection. ML-based threat detection and intelligent analysis help organizations improve the efficiency and accuracy of threat detection and better defend against known and unknown threats.

Powerful Network Adaptability

With the explosive growth of mobile devices and cloud services, traditional IPv4 infrastructures are struggling to keep up. Hillstone X25803 data center firewall addresses this issue by offering IPv4 preservation through Carrier-Grade Network Address Translation (CGNAT) and advanced IPv6 migration technologies, such as dual-stack, tunneling, and DNS64/NAT64. This enables you to accommodate your growing subscriber base and network demands seamlessly. Additionally, the X25803 data center firewall provides standard IPsec VPN capabilities and integrates SSL VPN to offer users a high-performance, high-capacity, and full-scale VPN solution. Its unique plug-and-play VPN greatly simplifies configuration

Product Highlights (Continued)

and maintenance while providing users with convenient and remote secure access. Moreover, the X25803 data center firewall natively integrates security for SD -WAN connections, enforcing fine-grained access policies across all locations. This ensures that customers can access SD-WAN features while maintaining the highest level of protection.

Environmentally Sustainable Security

Hillstone X25803 data center firewall delivers high performance while minimizing power consumption, all on a single platform. This reduces the number of network firewalls required for customers to accomplish their business needs, saving customers power consumption, while also contributing to their sustainability goals. Additionally, it adopts a front and rear ventilation design to improve heat dissipation efficiency. The fan trays are intelligently adjustable based on the temperature of the CPUs in different areas to ensure balanced heat dissipation across the device.

Features

Network Services

- Dynamic routing (OSPF, BGP with graceful restart, RIPv2)
- Static and Policy routing
- Route controlled by application
- Support Service Level Agreement (SLA)-based WAN path control
- 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 and PIM-SM)
- 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, tcp full proxy
- NAT and ALG support: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT (IPv4), 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 service based or application based police recommendation
- Policy analyzing and invalid policy cleanup
- Comprehensive DNS policy
- Schedules: one-time and recurring
- Support policy import and export

Intrusion Prevention

- Protocol anomaly detection, rate-based detection, custom signatures, manual, automatic push or pull signature updates, integrated threat encyclo-pedia
- 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
- Support protection of brute force attacks including VNC, RDP, SSH, LDAP, IMAP, SMB
- Support protection of sensitive file scanning attack

Antivirus

- Manual, automatic push or pull signature updates
- 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
- Intelligent Anti-DoS/DDoS with ML-based baseline establishment, including SYN flood, UDP flood, DNS reply flood, DNS query flood defense, TCP fragment, ICMP fragment, SIP flood, 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
- URL allow list configuration

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

Features (Continued)

- 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
- DGA Domain 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
- Regular 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 HTTPS traffic
- SSL encrypted traffic whitelist
- SSL proxy offload mode
- SSL proxy supports IP whitelist and predefined whitelist
- SSL proxy supports session re-use
- Support AD/LDAP server connection via SSL encryption
- Support TLS v1.0, TLS v1.2, TLS v1.3
- Support application identification, DLP, IPS sandbox, AV for SSL proxy decrypted traffic of SMTPS/POP3S/IMAPS

Endpoint Identification and Access Control

- Support to identify endpoint IP, endpoint quantity, on-line time, off-line time, and on-line duration
- Support major 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
- Support customized redirect page
- 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
- Content filtering for predefined keywords and file contents
- IM identification and network behavior audit
- Filter files transmitted by HTTPS using SSL Proxy and SMB

Application Control

- Over 6,000 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
- Bandwidth allocated by time, priority, or equal bandwidth sharing
- Type of Service (TOS) and Differentiated Services (DiffServ) and traffic-class 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
- SIOM support full iQoS function

Server Load Balancing

- Weighted hashing, weighted least-connection, and weighted round-robin
- 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
  - IKEv2 support DH group 1,2,5,14,15,16,18,19,20,21,24
  - 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 supports configuration guide. 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
- IPSec VPN supports DPD On-Demand mode
- LLB and failover support over IPSec tunnels
- Support VXLAN
- 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, Microsoft Windows, MacOS and Linux
- 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

IPv6

- Management over IPv6, IPv6 logging and HA and HA peermode, twin-mode AA and AP
- IPv6 tunneling: DNS64/NAT64, IPv6 ISATAP, IPv6 GRE, IPv6 over IPv4 GRE, 6RD
- IPv6 routing protocols, including static routing, policy routing, ISIS, RIPng, OSPFv3 and BGP4+
- IPS, Application identification, URL filtering, Access control, ND attack defense, iQoS, SSL VPN
- Track address detection
- IPv6 Radius and SSO-radius support
- IPv6 is supported in Active Directory whitelist
- IPv6 support on the following ALGs: TFTP, FTP, RSH, HTTP, SIP, SQLNETv2, RTSP, MSRPC, SUNRPC
- IPv6 support on distributed iQoS

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, AV, QoS
- VSYS monitoring and statistic

High Availability

- Redundant heartbeat interfaces
- Active/Active peer mode with Hillstone Virtual Redundancy Protocol (HSVRP) support, and Active/Passive mode
- Standalone session synchronization
- HA reserved management interface
- Dual HA data link ports
- Failover:
  - Port, local & remote link monitoring
  - Stateful failover
  - Sub-second failover

Features (Continued)

  - Failure notification
- Deployment options:
  - HA with link aggregation
  - Full mesh HA
  - Geographically dispersed HA

Twin-mode HA

- High availability mode among multiple devices
- Multiple HA deployment modes
- Configuration and session synchronization among multiple devices
- Twin-mode AP supports IPv6

User and Device Identity

- Local user database
- Remote user authentication: TACACS+, LDAP, Radius, Active Directory
- Single-sign-on: Windows AD
- 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
- SSL VPN, ZTNA, WebAuth support Azure Active Directory(AD) authentication
- Interface based authentication
- Agentless ADSSO (AD Polling)
- Use authentication synchronization based on SSO-monitor
- Support MAC-based user authentication
- Radius server issues user security policy via CoA message

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 and email-based zero-touch provisioning(ZTP), local and remote script execution
- Dynamic real-time dashboard status and drill-in monitoring widgets
- Language support: English
- Administrator authentication: Active Directory and LDAP
- Support CLI access from WebUI

Logs & Reporting

- Logging facilities: local memory and storage (if available), 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

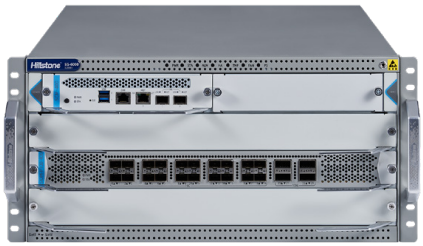
- Application, URL, threat events statistic and monitoring
- Real-time traffic statistic and analytics
- System information such as concurrent session, CPU, Memory and temperature
- iQoS traffic statistic and monitoring, link status monitoring
- Support traffic information collection and forwarding via Netflow (v9.0)

Zero Trust Network Access (ZTNA)

- Support intranet access
- Support end-user access with a Zero-Trust principle
- ZTNA tags support account password and terminal status
- Support Zero-Trust policy configuration based on ZTNA tags and application resources, with optional security protection and data security
- Support application resource management
- Support application resource configuration based on domain name
- Support dynamic adjustment of authorization in policy when the endpoint state changes
- Support application publishing, and displaying authorized applications to end-users over ZTNA portal
- Support single packet authentication (SPA)
- Support domain name level permission management
- Support auto-selection of the optimal gateway
- Support smooth transition from current SSL VPN to ZTNA solution
- Support operating systems including iOS, Android, Microsoft Windows, MacOS and Linux
- Support centralized ZTNA management by HSM, including upload monitoring data and statistics, and accept the configuration delivered
- Support Resftful APIs

Specifications

X25803-IN



FW Throughput (Maximum) (1)	880 Gbps
IPsec Throughput (Maximum) (2)	280 Gbps
NGFW Throughput (3)	320 Gbps
Threat Protection Throughput (4)	160 Gbps
Concurrent Sessions (Maximum) (5)	180 Million
New Sessions/s (6)	5 Million
IPS Throughput (Maximum) (7)	370 Gbps
SSL VPN Users (Default/Max)	128 / 20,000
Virtual Systems (Default/Max)	1/1000
Module Types	SIOM-P100-400-IN, SCM-400-IN, SCM-D1T-400-IN, SCM-D2T-400-IN
I/O Ports	Maximum 12*100GE+ 60*10GE
Management Ports	1 Console port, 1 MGT port, 2 USB 3.0 ports (single SCM-400 module)
Network Ports	2 Gigabit Ethernet optical ports(HA)(single SCM-400 module)
Expansion Module Slots	3 SIOM expansion slots, 2 System control module expansion slots
Power Consumption	1+1 redundant hot-swappable power supplies, maximum power consumption 2000W, standard power consumption 1100W
Power Supply (8)	AC 90 to 127 V / 180 to 264 V (50/60 Hz) , DC -40 to -72 V
Dimension (W × D × H)	5U, 17.3 x 26.7 x 8.6 in (440 × 680 × 220 mm)
Weight (Without Modules)	65 lb (29.5 Kg)
Compliance and Certificate	CE, CB, FCC, ROHS, IEC/EN61000-4-5 Power Surge Protection, ISO 9001:2015, ISO 14001:2015, ISO 27001:2013, CVE Compatibility, IPv6 Ready

Module Options

SIOM-P100-400-IN

Description	Service and I/O Module
Network Interface	4 QSFP28 100GE interfaces, 20 SFP+ 10GE interfaces
Slot	Occupies 1 universal expansion slot
Weight	15.34 lb (6.90Kg)

	SCM-400-IN	SCM-D1T-400-IN	SCM-D2T-400-IN
			
Description	System Control Module	System Control Module	System Control Module
SSD	N/A	1 T	2 T
Slot	Occupies 1 system control module expansion slot	Occupies 1 system control module expansion slot	Occupies 1 system control module expansion slot
Weight	6.63 lb (2.90 Kg)	6.63 lb (2.90 Kg)	6.63 lb (2.90 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+SHA256 configuration and 1400-byte packet size;

(3) NGFW throughput data is obtained under 64 Kbytes HTTP traffic with application control and IPS enabled;

(4) Threat protection throughput data is obtained under 64 Kbytes HTTP traffic with application control, IPS, AV and URL filtering enabled;

(5) Maximum concurrent sessions is obtained under HTTP traffic;

(6) New Sessions/s is obtained under HTTP traffic;

(7) IPS throughput data is obtained under bi-direction HTTP traffic detection with all IPS rules being turned on;

(8) At least 1 AC power modules are required for full load operation with AC power, and at least 1 DC power modules are required for full load operation with DC power. Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.5R9. Results may vary based on StoneOS® version and deployment.

Version: EX-08.01-DCFW-X25803-5.5R11-0824-EN-01