Hillstone X-Series Data Center Firewall X10800

X10800

Front

Rear

The Hillstone X10800 Data Center Firewall offers outstanding performance, reliability, and scalability, for high-speed service providers, large enterprises and carrier networks. The product is based on an innovative fully distributed architecture that fully implements firewalls with high throughput, concurrent connections, and new sessions. Hillstone X10800 also supports large-capacity virtual firewalls, providing flexible security services for virtualized environments, and features such as application identification, traffic management, intrusion prevention, and attack prevention to fully protect data center network security.

Product Highlights

High performance based on Elastic Security Architecture

With traffic explosively increasing, data center firewalls need powerful capabilities to handle high traffic and massive concurrent user access, as well as the ability to effectively cope with sudden bursts of user activity. Therefore, data center firewalls must not only have high throughput but also extremely high concurrent connections and new session processing capabilities.

The Hillstone X10800 Data Center Firewall adopts an innovative, fully distributed architecture to implement distributed high-speed processing of service traffic on Service Modules (SSMs) and Interface Modules (IOMs) through intelligent traffic distribution algorithms. Through patented resource management algorithms, it allows for the full potential of distributed multi-core processor platforms, to further increase the performance of firewall concurrent connections, new sessions per second, and achieve a fullly linear expansion of system performance. The X10800 data center firewall can process up to 1 Tbps, up to 10 million new sessions per second, and up to 480 million concurrent connections. The device can provide up to 44 100GE interfaces, 88 10G interfaces, or 22 40GE interface, 132 10G interface expansion capabilities. Moreover, the packet forwarding delay is less than 10us, which can fully meet a data center's demand for real-time service forwarding.

Carrier Grade Reliability

The hardware and software of the X10800 data center firewall delivers 99.999% carrier-grade reliability. It can support active/active or active/passive mode redundant deployment solutions to ensure uninterrupted service during single failure. The entire system adopts a modular design, supporting control module redundancy, service module redundancy, interface module redundancy and switching module redundancy, and all modules are hot-swappable.

The X10800 data center firewall supports multi-mode and single-mode optical port bypass modules. When the device is running under a special condition, such as power off, the system will start in Bypass mode to ensure uninterrupted operation of business. It also provides power redundancy, fan redundancy and other key components to guarantee reliability.

Twin-mode HA effectively solves the problem of asymmetric traffic in redundant data centers. The firewall twin-mode is a highly reliable networking mode building on dual-device backup. Two sets of active/passive firewalls in the two data centers are connected via a dedicated data link and control link. The two sets of devices synchronize session information and configuration information with each other.

Leading virtual firewall technology

Virtualization technology is more and more widely used in data centers. The X10800 data center firewall can logically divide a physical firewall into upwards of 1000 virtual firewalls for the data center's virtualization needs, providing virtual firewall support capabilities for large data centers. At the same time, users can dynamically set resource for each virtual firewall based on actual business conditions, such as CPUs, sessions, number of policies, ports, etc., to ensure flexible changes in service traffic in a virtualized environment. Each virtual firewall system of X10800 data center firewalls not only has independent system resources, but also can be individually and granularly managed to provide independent security management planes for different services or users.

Granular application control and comprehensive security

The X10800 data center firewall uses advanced in-depth application identification technology to accurately identify thousands of network applications based on protocol features, behavior characteristics, and correlation analysis, including hundreds of mobile applications and encrypted P2P applications. It provides sophisticated and flexible application security controls.

The X10800 data center firewall provides intrusion prevention technology based on deep application identification, protocol detection, and attack principle analysis. It can effectively detect threats such as Trojans, worms, spyware, vulnerability attacks, and escape attacks, and provide users with L2-L7 network security. Among them, Web protection function can meet the deep security protection requirements of Web server; Botnet filtering function can protect internal hosts from infection.

The X10800 data center firewall supports URL filtering for tens of millions of URL signature library. It can help administrators easily implement web browsing access control and avoid threat infiltration of malicious URLs. It also provides Anti-virus feature that can effectively detect and block malwares with low latency.

The intelligent bandwidth management of X10800 data center firewall is based on deep application identification and user identification. Combined with service application priorities, the X10800 data center firewall can implement fine-grained, two-layer, eight-level traffic control based on policies and provide elastic QoS functions. Used with functions such as session restrictions, policies, routing, link load balancing, and server load balancing, it can provide users with more flexible traffic management solutions.

Strong network adaptability

The X10800 data center firewall fully supports next-generation Internet deployment technologies (including dual-stack, tunnel, DNS64/NAT64 and other transitional technologies). It also has mature NAT444 capabilities to support static mapping of fixed-port block of external network addresses to intranet addresses. It can generate logs based on session and user for easy traceability. Enhanced NAT functions (Full-cone NAT, port multiplexing, etc.) can fully meet the requirements of current ISP networks and reduce the cost of user network construction.

The X10800 data center firewall provides full compliance with standard IPSec VPN capabilities and integrates third-generation SSL VPN to provide users with high-performance, high-capacity, and full-scale VPN solution. At the same time, its unique plug-and-play VPN greatly simplifies configuration and maintenance challenges and provides users with convenient and remote secure access services.

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
- Virtual wire (Layer 1) transparent inline deployment

Firewall

- Operating modes: NAT/route, transparent (bridge), and mixed mode
- Policy objects: predefined, custom, and 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

Anti-Virus
- Manual, automatic push or pull signature updates
- Flow-based Antivirus: protocols include HTTP, SMTP, POP3, IMAP, FTP/SFTP
- Compressed file virus scanning

Attack Defense
- Abnormal protocol attack defense
- Anti-DoS/DDoS, including SYN Flood, DNS Query Flood defense
- ARP attack defense

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

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

Endpoint Identification and Control
- Support to identify endpoint IP, endpoint quantity, on-line time, off-line time, and on-line duration
- Support 10 operation 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

Application Control
- Over 3,000 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
- 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 includes policy based routing, ECMP and weighted, embedded ISP routing and dynamic detection
- 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
  - Phase 1/Phase 2 Diffie-Hellman support: 1,2,5
  - 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

IPv6
- Management over IPv6, IPv6 logging and HA
- IPv6 tunneling, DNS64/NAT64 etc
- IPv6 routing protocols, including static routing, policy routing, ISIS, RIPng, OSPFv3 and BGP4+
- IPS, Application identification, URL filtering, Access control, ND attack defense, 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
- VSYS monitoring and statistic

High Availability
- Redundant heartbeat interfaces
- Active/Active and Active/Passive
- 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
- High availability mode among multiple devices
- Multiple HA deployment modes
- Configuration and session synchronization among multiple devices

User and Device Identity
- Local user database
- Remote user authentication: TACACS+, LDAP, Radius, Active
- 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
- Interface based Authentication
- Agentless ADSSO (AD Polling)
- Use authentication synchronization based on SSO-monitor
- Support 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 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)

Product Specification

Specification	SG-6000-X10800
	 
FW Throughput (Maximum)(1)	1 Tbps
IPSec Throughput (Maximum)(2)	300 Gbps
IMIX Throughput(3)	600 Gbps
NGFW Throughput(4)	280 Gbps
Threat Protection Throughput(5)	200 Gbps
Concurrent Sessions (Maximum)	480 Million
New Sessions/s(6)	10 Million
IPS Throughput (Maximum)(7)	400 Gbps
Virtual Systems (Default/Max)	1/1000
I/O Module	SSM-300, QSM-300, IOM-P40-300, IOM-P100-300, SWM-300, SCM-300
Maximum Interfaces	Maximum 11×2 40GE+11×12 10GE Or Maximum 11×4 100GE+11×8 10GE
Maximum Power Consumption	4400W, N+M(8), redundant hot swap power supply
Power Supply	AC 100-240 V (50/60H z), DC -40 ~ -72V
Management Interfaces	1 Console port, 1 AUX port, 1 MGT management, 1 USB 2.0 port (single SCM-300 module)
Network Interfaces	2 Gigabit optical interfaces (2 HA interfaces, single SCM-300 module)
Expansion Module Slot	12 universal expansion slots, 2 system control module expansion slots, 2 switching module expansion slots
Dimension (W × D × H)	18U 17.3× 31.4× 25 in (440× 797× 635 mm)
Weight	253 lb (114.75 KG)
Compliance and Certificate	CE, CB, FCC, ROHS, IEC/EN61000-4-5 Power Surge Protection, ISO 9001:2015, ISO 14001:2015, CVE Compatibility, IPv6 Ready, ICSA Firewalls

Module Options

Name	IOM-P40-300	IOM-P100-300	SSM-300	QSM-300
				
Description	40GE, 10GE interface module	100GE, 10GE interface module	Security service module	QoS service module
Network interface	2 QSFP+ 40GE interfaces, 12 SFP+ 10Gb interfaces, transceiver not included	4 QSFP28 100GE interfaces, 8 SFP+ 10Gb interfaces, transceiver not included	N/A	N/A
Slot	Occupies 1 universal expansion slot	Occupies 1 universal expansion slot	Occupies 1 universal expansion slot	Occupies 1 universal expansion slot
Weight	12.45 lb (5.65 kg)	12.67 lb (5.75 kg)	12.56 lb (5.70 kg)	12.56 lb (5.70 kg)

Name	SWM-300	SCM-300	IOM-2MM-BE	IOM-2SM-BE
				
Description	Switching module	Security control module	2 Port Multi-mode Bypass Module	2 Port Single-mode Bypass Module
Network interface	N/A	N/A	Dual port multi-mode bypass fiber	Dual port multi-mode bypass fiber
Slot	Occupies 1 universal expansion slot	Occupies 1 universal expansion slot	Occupies 1 universal expansion slot	Occupies 1 universal expansion slot
Weight	7.05 lb (3.20 kg)	7.6 lb (3.45 kg)	2.0 lb (0.9 kg)	2.0 lb (0.9 kg)

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.5R7. Results may vary based on StoneOS® version and deployment.

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 packet; (3) IMIX throughput data is obtained under UDP traffic mix (68 byte : 512 byte : 1518 byte =5:7:1); (4) NGFW throughput data is obtained under 64 Kbytes HTTP traffic with application control and IPS enabled; (5) Threat protection throughput data is obtained under 64 Kbytes HTTP traffic with application control, IPS, AV and URL filtering enabled; (6) New Sessions/s is obtained under TCP traffic; (7) IPS throughput data is obtained under bi-direction HTTP traffic detection with all IPS rules being turned on; (8) At least 3 AC power modules are required for full load operation with AC power, and at least 4 DC power modules are required for full load operation with DC power.

Version: EX-08.01-DCFW10800-5.5R7-0619-EN-01