Hillstone X-Series

Data Center Firewall X8180

Front

Rear

The Hillstone X8180 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 implements firewalls with high throughput, concurrent connections, and new sessions. Hillstone X8180 also supports large-capacity virtual firewalls, providing flexible security services for virtualized environments, and features such as application identification, traffic management, intrusion prevention, Botnet C&C prevention and attack prevention to fully protect modern data centers. Further, as part of the ZTNA solution, it granularly controls the application access with eliminated implicit trust and continuous verification.

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 X8180 Data Center Firewall adopts an innovative, fully distributed architecture to implement distributed high-speed processing of service traffic on Service and IO Modules (SIOMs) 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 fully linear expansion of system performance. The X8180 data center firewall can process up to 450 Gbps, up to 2.5 million new sessions per second, and up to 130 million concurrent connections. Moreover, the packet forwarding delay is less than 10us, which can fully meet a data center's demand for real-time service forwarding.

Product Highlights (Continued)

Carrier Grade Reliability

The hardware and software of the X8180 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. It also provides power redundancy, fan redundancy 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 X8180 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 X8180 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 X8180 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 X8180 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 X8180 data center firewall supports URL filtering for tens of millions of URLs. It can help administrators easily implement web browsing access control and avoid threat infiltration of malicious URLs. It also provides an antivirus feature that can effectively detect and block malwares with low latency.

The intelligent bandwidth management of X8180 data center firewall is based on deep application identification and user identification. Combined with service application priorities, the X8180 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.

Complete Botnet C&C Prevention

One of the more damaging battles when fighting against polymorphic malware is the defense against notorious Command and Control (also known as C&C, or C2) attacks, often executed over DNS with the goal of helping the attacker gain a foothold into the network to steal sensitive data or even to obtain full control of the network. The X8180 data center firewall supports complete Botnet C&C prevention features, which protect the data center from any potential threat-through the monitoring of C&C connections from L3 to L7.

Product Highlights (Continued)

• DGA detection: DGA, domain generation algorithms, on infected hosts generate pseudo domain names randomly, including C&C server domain names. The DGA detection feature detects and prevents these traffic types and generate threat log.

• DNS sinkhole detection: Protection for hosts and the network by supplying the admins with a detailed report of DNS access requests with false results, automatically redirecting systems to prevent connection to potentially malicious destinations.

• DNS tunneling detection: Detection of traffic over the DNS protocol which couldbe exploited by any suspicious, non-DNS protocols for C&C callbacks and data exfiltration.

• Botnet C&C customized access list: The ability to dynamically adjust and customize the access list to allow or block based on the IP address or domain name.

Strong Network Adaptability

The X8180 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 X8180 data center firewall provides full compliance with standard IPSec VPN capabilities and integrates third-generation SSL VPN to provide users with a 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
- 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
- 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 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 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
- 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
- URL allow list configuration

Features (Continued)

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
- 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
- Support 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 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) 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
- Automatic expiration cleanup and manual cleanup of user used traffic
- 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
  - 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 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
- 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 an 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
- IPv6 routing protocols, including static routing, policy routing, ISIS, RIPng, OSPFv3 and BGP4+
- IPv6 support on LLB
- 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,

Features (Continued)

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 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
  - 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
- 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 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 auto-install, local and remote script execution
- Dynamic real-time dashboard status and drill-in monitoring widgets
- Language support: English
- Administrator authentication: Active Directory and LDAP

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)

Specifications

	SG-6000-X8180
	 
FW Throughput (Maximum) (1)	450 Gbps
NGFW Throughput (2)	75 Gbps
Threat Protection Throughput (3)	70 Gbps
Concurrent Sessions (Maximum) (4)	130 Million
New Sessions/s (5)	2.5 Million
IPS Throughput (Maximum) (6)	180 Gbps
SSL VPN Users (Default/Max)	128 / 20,000
Virtual Systems (Default / Max)	1 / 1,000
Expansion Modules	SCM-260, SIOM-P100-260
Maximum Interfaces	Maximum 6*100GE + 48*10GE
Maximum Power Consumption	Max. 1300W, 1+1 redundant
Power Supply	AC 100-127 V / 200-240 V (50/60 Hz), DC -48 ~ -60 V
Management Interfaces	1 Console port, 1 MGT management, 1 USB 2.0 port (single SCM-260 module)
Network Interfaces	2 Gigabit optical interfaces (2 HA interfaces, single SCM-260 module)
Expansion Module Slot	3 universal expansion slots, 2 system control module expansion slots
Dimension (W × D × H)	3U W 17.3 in × D 21.7 in × H 5.2 in (W 440 mm × D 552 mm × H 132 mm)
Weight	44.5 lb (20.2 kg)
Compliance and Certificate	CE, FCC, ROHS, IEC/EN61000-4-5 Power Surge Protection, ISO 9001:2015, ISO 14001:2015, CVE Compatibility, IPv6 Ready, ICSA Firewalls

Module Options

	SCM-260	SIOM-P100-260
		
Description	System Control Module	Service and IO Module
Network Interface	2 Gigabit Optical Interfaces (2 HA interfaces)	2 QSFP28 100GE interfaces, 16 SFP+ 10GE interfaces
Slot	Occupies 1 universal expansion slot	Occupies 1 universal expansion slot
Weight	2.4 lb (1.10 kg)	12.3 lb (5.60 kg)

NOTES:

(1) FW throughput data is obtained under single-stack UDP traffic with 1518-byte packet size;
(2) NGFW throughput data is obtained under 64 Kbytes HTTP traffic with application control and IPS enabled;
(3) Threat protection throughput data is obtained under 64 Kbytes HTTP traffic with application control, IPS, AV and URL filtering enabled;
(4) Maximum concurrent sessions is obtained under HTTP traffic;
(5) New sessions/s is obtained under HTTP traffic;
(6) IPS throughput data is obtained under bi-direction HTTP traffic detection with all IPS rules being turned on.
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-X8180-5.5R9-0622-EN-01