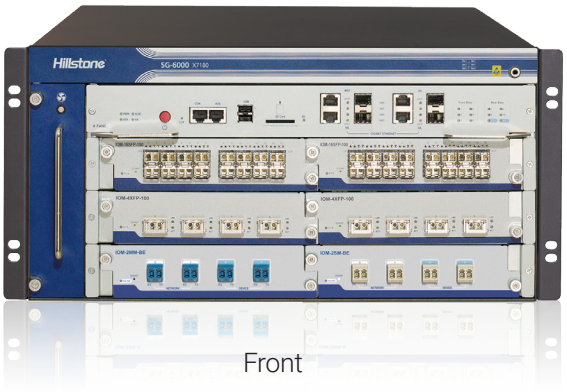
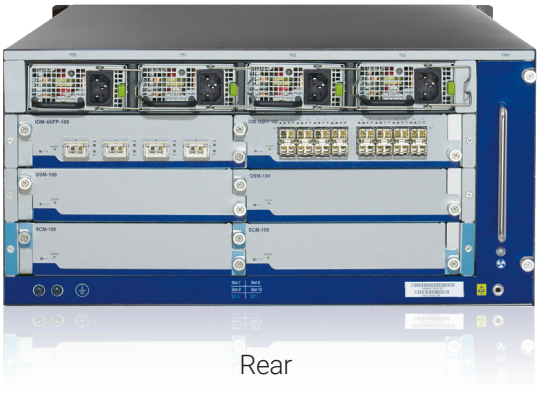
Hillstone X-Series

Data Center Firewall X7180



Front



Rear

The Hillstone X7180 Data Center Firewall offers outstanding performance, reliability, and scalability, for high-speed service providers, large enterprises and carrier networks. It provides flexible firewall security for multi-tenant cloud-based Security-as-a-Service environments. The X7180 platform is based on Hillstone's Elastic Security Architecture (ESA), which offers highly scalable virtual firewalls, exceptional firewall throughput, massive concurrent sessions and very high new sessions per second. The X7180 also supports Deep Packet Inspection (DPI), next generation application control and Quality of Service (QoS). The system delivers exceptional performance in a small form factor with low power requirements.

Product Highlight

Elastic Security Architecture

Streaming media, web-based applications, VoIP, peer-to-peer file sharing, mobile devices, cloud computing, and international presence are all contributing to accelerating datacenter traffic. As core network traffic increases, the need for high-speed network interfaces and high port densities becomes critical. Mobile device traffic also requires more emphasis since network security solutions can degrade significantly when the traffic shifts toward a large number of users and smaller packet size. As a result, data center firewalls must provide high throughput, large numbers of concurrent sessions and high numbers of new sessions per second. More importantly, they must respond to the usage patterns of its customers, which are often highly unpredictable. Consequently, datacenter firewalls must also provide rapid elasticity and on-demand security.

The X7180 data center firewall is built on Hillstone's Elastic Security Architecture. It can support up to 1000 virtual firewalls and it can be provisioned as an on-demand service option complete with service level agreements (SLAs). Service providers can dynamically adjust resource allocation (CPU, sessions, policies and ports) for each virtual firewall in response to SLAs. Hillstone's X7180 hardware is composed of multiple security and networking blades that provide scalability for future growth. It leverages a distributed multi-core architecture enabling wire-speed performance up to 680 Gbps throughput, 240 million concurrent sessions and 4.8 million new sessions per second. The chassis supports up to 68 10-GbE ports or 144 1-GbE ports.

Product Highlight (Continued)

Carrier Grade Reliability

The X7180 provides carrier grade reliability. It supports High Availability (HA) in both Active/Passive and Active/Active modes, ensuring 24x7 operation. It also has redundant and hot swappable power supplies, fans, System Control Modules (SCM), Security Service Modules (SSM) and I/O Modules (IOM). The X7180 also has a multi-mode and single-mode fiber bypass module, to ensure business continuity during power outages.

NAT and IPv6

The inevitable march to IPv6 is underway but service providers still need to deploy Carrier Grade NAT (CGN) and Large Scale NAT (LSN) to manage the IPv4 address shortage while the transition is underway. Hillstone's X7180 supports a variety of transition technologies including Dual Stack, IPv6/IPv4 tunnels, DNS64/NAT64, NAT 444, full cone NAT, NAPT, etc. Session logging and address translation enable audit trails for record keeping and forensics.

Energy Efficiency

The X7180 has slots front and rear, which saves rack space and facilitates cooling. It has a 5U form factor and a maximum power consumption of 1950W, which is 50% less power than other data center firewalls.

Security

The X7180 provides visibility and control of over 3,000 applications including 600 mobile applications and encrypted P2P applications. It allows fine grain control of applications, bandwidth, users, and user/groups. The X7180 prevents users from accessing malicious or inappropriate applications and the embedded Intrusion Prevention System (IPS) protects the network from malicious activity. The X7180 supports deep packet inspection and standard-based IPSec VPN, which uses hardware based crypto acceleration to provide third-generation SSL VPN. Hillstone also offers a unique Plug-and-Play VPN solution that makes branch office VPN deployment a simple task.

QoS

The X7180 platform can manage bandwidth based on applications, users, and time of day. The system provides fine-grained policy control including guaranteed bandwidth, bandwidth limit, traffic priority, and FlexQoS, which can dynamically adjust bandwidth based on utilization. These features, along with session limit, policy routing and link load balancing enable flexible bandwidth management.

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

Features (Continued)

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 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
- 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

Features (Continued)

• 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, Wordl 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-X7180

FW Throughput (Maximum) (1)	680 Gbps
IPSec Throughput (Maximum) (2)	90 Gbps
IPSec Tunnel (Maximum)	20,000
IMIX Throughput (3)	400 Gbps
NGFW Throughput (4)	70 Gbps
Threat Protection Throughput (5)	50 Gbps
Concurrent Sessions (Maximum)	240 Million
New Sessions/s (6)	4.8 Million
IPS Throughput (Maximum) (7)	100 Gbps
SSL VPN Users (Default/Max)	128 / 20,000
Virtual Systems (Default/Max)	1 / 1,000
Management I/O	1 x Console Port, 1 x AUX Port
Fixed I/O Ports	4 x GE Combo slot (1 x M GT+3 x HA)
Availalbe slots for Expansion Modules	10 x Generic Slot, 2 x System Control Modu le Slot, 1 x SD Card Slot, 2 x USB 2.0 Port
Expansion Modules	SCM-100, SSM-100, SSM-200, QSM-100, QSM-200, IOM-16SFP-100, IOM-4XFP-100, IOM- 2MM-BE, IOM-2SM-BE, IOM-2Q8SFP+
Maximum Power Consumption	2+2 redundant, Max.1300W ; 3+1 redundant, Max.1950W
Power Supply	AC 100-240 V (50/60H z), DC -40 ~ -72V
Dimension (W × D × H)	5U 17.3 × 23.2 × 8.9 in (440 × 590 × 225 mm)
Weight	<116.6 lb (52 kg)
Temperature	32-104 F (0-40 ℃)
Relative Humidity	10-95%
Compliance and Certificate	CE, CB, FCC, UL/cUL, ROHS, IEC/EN61000-4-5 Power Surge Protection, ISO 9001:2008, ISO 14001:2004, CVE Compatibility, IPv6 Ready, ICSA Firewalls

Module Options

	IOM-16SFP-100	IOM-2MM-BE	IOM-2SM-BE
			
Name	16SFP Module	2 Port Multi-mode Bypass Module	2 Port Single-mode Bypass Module
Fixed I/O Ports	16 x SFP, transceiver not included	Dual port multi-mode bypass fiber	Dual port multi-mode bypass fiber
Dimension	1 U (Occupies 1 generic slot)	1 U (Occupies 1 generic slot)	1 U (Occupies 1 generic slot)
Weight	2.9 lb (1.3 kg)	2.0 lb (0.9 kg)	2.0 lb (0.9 kg)

	IOM-2Q8SFP+	IOM-8SFP+	IOM-2Q8SFP+-200
			
Name	2xQSFP+ and 8xSFP+ Module	2xQSFP+ and 8xSFP+ Module	2xQSFP+ and 8xSFP+ Module
Fixed I/O Ports	2xQSP+, 8xSFP+, transceiver not included	2xQSP+, 8xSFP+, transceiver not included	2xQSP+, 8xSFP+, transceiver not included
Dimension	1 U (Occupies 2 generic slots)	1 U (Occupies 2 generic slots)	1 U (Occupies 2 generic slots)
Weight	7.7 lb (3.5 kg)	7.9 lb (3.6 kg)	7.7 lb (3.5 kg)

	SCM-100	SSM-100	SSM-200	QSM-100	QSM-200
					
Name	Security Control Module	Security Control Module	Securit Service Module 200	QoS Service Module	QoS Service Module 200
Dimension	1 U (Occupies 1 generic slot)	1 U (Occupies 1 generic slot)	1 U (Occupies 2 generic slots)	1 U (Occupies 1 generic slot)	1 U (Occupies 2 generic slots)
Weight	2.4 lb (1.1 kg)	2.9 lb (1.3 kg)	7.7 lb (3.5 kg)	2.9 lb (1.3 kg)	7.7 lb (3.5 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 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.
Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.5R7. Results may vary based on StoneOS® version and deployment.

Version: EX-08.01-DCFWX7180-5.5R7-0619-EN-01