

# Hillstone High Performance 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 Highlights

### 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 SLA's. 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 360 Gbps throughput, 120 million concurrent sessions and 2.4 million new sessions per second. The chassis supports up to 68 10-GbE ports or 144 1-GbE ports.

### 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 1300W, which is 50-67% 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 guarantee 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 – connect to SPAN port
- IPv6 Support: Mgt. over IPv6, IPv6 routing protocols, IPv6 tunneling, IPv6 logging and HA
- 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
- Application Level Gateways and session support: MSRPC, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, dcerpc, dns-tcp, dns-udp, H.245 0, H.245 1, H.323
- NAT 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
- Schedules: one-time and recurring
- QoS Traffic Shaping:
  - 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
- Virtual Firewall: Up to 1000 vSYS load balanced firewalls
- Load balancing:
  - Weighted hashing, weighted least-connection, and weighted round-robin
  - Session protection, session persistence and session status monitoring

- Bidirectional 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 and latency
- Link health inspection with ARP, PING, and DNS
- Access control based on IP address geolocation
- Repetitive and redundant firewall rule inspection

### 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
- View and manage IPSEC and SSL VPN connections

## 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

## IPS

- 7,000+ signatures, 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

## Threat Protection

- Botnet server IP blocking with global IP reputation database
- Flow-based web filtering inspection
- Manually defined web filtering based on URL, web content and MIME header
- Dynamic web filtering with cloud-based realtime 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

## 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 applications in the

cloud

- Provide multi-dimensional monitoring and statistics for applications running in the cloud, including risk category and characteristics

## 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

## 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
- Comprehensive event logs: system and administrative activity audits, routing & networking, VPN, user authentications
- IP and service port name resolution option
- Brief traffic log format option

## Product Specification

Specification	SG-6000-X7180
FW Throughput (Maximum)	360 Gbps
Maximum Concurrent Sessions	120 million
New Sessions/s	2.4 million per second
IPS Throughput	90 Gbps
Management Ports	1 x Console Port, 1 x AUX Port, 2 x USB 2.0 Port
Fixed I/O Ports	4 x GE Combo slot (1 x MGT + 3 x HA)
Available Slots for Extensible Modules	10 x Generic Slot, 2 x System Control Module Slot, 1 x SD Card Slot
Modules	SCM-100, SSM-100, QSM-100, IOM-16SFP-100, IOM-4XFP-100, IOM-2MM-BE, IOM-2SM-BE, IOM-2Q8SFP+, IOM-8SFP+
Maximum Power Consumption	2+2 redundant power supply, Max.1300W
Power Supply	AC 100-240V 50/60Hz, DC -40 ~ -72V
Dimension (WxDxH)	5U 17.3×23.2×8.9 in (440×590×225 mm)
Weight	<116.6 lb (53 kg)
Temperature	32-104F (0-40 C)
Relative Humidity	10-95%

Specification	IOM-4XFP-100	IOM-16SFP-100	IOM-2MM-BE	IOM-2SM-BE
				
Name	4XFP Module	16SFP Module	2 Port Multi-Mode Bypass Module	2 Port Single-Mode Bypass Module
Fixed I/O Ports	4 x XFP, XFP module not included	16 x SFP, SFP module not included	Dual port multi-mode bypass fiber	Dual port single-mode bypass fiber
Dimension	1U (Occupies 1 generic slots)	1U (Occupies 1 generic slots)	1U (Occupies 1 generic slots)	1U (Occupies 1 generic slots)
Weight	2.6 lb (1.2 kg)	2.9 lb (1.3 kg)	2.0 lb (0.9kg)	2.0 lb (0.9kg)

Specification	IOM-2Q8SFP+	IOM-8SFP+	Specification	SCM-100	SSM-100	QSM-100
						
Name	2xQSFP+ and 8xSFP+ Module	8xSFP+ Module	Name	Service Control Management Module	Security Service Module	QoS Service Module
Fixed I/O Ports	2xQSFP+, 8xSFP+, QSFP+ and SFP+ module not included	8xSFP+, SFP+ module not included	Dimension	1U (Occupies 1 generic slots)	1U (Occupies 1 generic slots)	1U (Occupies 1 generic slots)
Dimension	1U (Occupies 2 generic slots)	1U (Occupies 2 generic slots)	Weight	2.4lb (1.1kg)	2.4lb (1.1kg)	2.4lb (1.1kg)
Weight	8.47lb (3.84kg)	7.91lb (3.59kg)				

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS 5.5R2. Results may vary based on StoneOS® version and deployment.