

## Hillstone High Performance Data Center Firewall SG-6000-X6150



The Hillstone SG-6000-X6150 Firewall is the latest high performance carrier-grade firewall solution. Modular in design, it combines the Hillstone Multi-Core Plus™ G2 hardware architecture with a proprietary fully parallelized security engine to deliver robust firewall protection. The SG-6000-X6150 platform provides enhanced scalability and adaptability through a complete solution set of firewall and application controls. Designed specifically for Internet Service Providers (ISPs), data centers and large enterprises, the SG-6000-X6150 integrates high performance and high capacity in a reliable platform that centralizes network management while minimizing complexity and cost of ownership and operations.

### Carrier-Grade Design

The SG-6000-X6150 adopts a carrier-grade redundant design. Both System Control module and Security Service modules are redundant and hot-swappable. Leveraging the StoneOS® 64 bit real-time security operating system, the platform delivers High Availability (HA) at the device level (A/P and A/A), and module level (network management and security services), ensuring 7x24 continuous and uninterrupted performance. The SG-6000-X6150 comes with modular and hot-swappable redundant power supplies supporting both AC and DC power input.

### High Performance/High Capacity Firewall

The industry-leading Hillstone Multi-Core Plus™ G2 platform provides up to 100Gbps in firewall throughput at a ramp-up rate of 1 million new sessions per second. The system can support up to 50 million sessions concurrently. The SG-6000-X6150 provides near linear performance extensibility through Security Service Modules (SSMs), and versatile scalability that meets the firewall demands of ISPs, data centers and large enterprises for high performance connectivity and critical assets protection.

### Adaptive Distribution of Security Processing

The use of data center virtualization provides a flexible method to increase system capacity. This method however may lead to uneven loads across the network servers resulting in performance degradation. Leveraging high performance parallel processing with multi-core hardware architecture, the SG-6000-X6150 addresses this issue by analyzing changes in trends and dynamically redistributing the processing load evenly across servers to maximize system availability and efficiency.

### Deep Application Inspection and Network Visibility

The state-of-the-art SG-6000-X6150 application identification engine provides real-time detection and analysis of network traffic and message contents. The identification of applications is based on both application signature and behavior in addition to routine port monitoring. With its sophisticated network usage visualization and

analysis capabilities in a user friendly package, the SG-6000-X6150 empowers network administrators with complete control over network traffic. The QoS functionality enables easy optimization of the network quality of service and timely detection and control of traffic anomalies to ensure network reliability and a stable firewall.

### Extensibility and Scalability

SG-6000-X6150 supports the following extensibility and scalability add-on modules:



- IO Module (IOM): The combination of IOM-16SFP and IOM-4XFP can provide a maximum of 144 SFP or 36 XFP.
- Security Service Module (SSM): Security processing performance scales almost linearly with the addition of SSMs, to deliver up to 100Gbps firewall performance.
- QoS Service Module (QSM): Customers who demand superior quality of service can use QoS Service modules to upgrade firewall functionality and performance.
- System Control Module (SCM): Maximizes the redundancy and stability of devices.

### Key Specifications


Specifications	SG-6000-X6150
Firewall Throughput	100Gbps
IPSec Throughput <sup>(1)</sup>	42Gbps
Maximum Concurrent Sessions	50 million
New Connections/s (Max) <sup>(2)</sup>	1,000,000/sec
Management	1 Console, 1 Aux, 2 USB 2.0
Fixed Ports	4 Combo ports (1 Management, 3 HA)
Expansion Slots	10 General Purpose Slots, 2 Management Module Slots, SD Slot
Expansion Module Types	SCM-20, SSM-20, QSM-20, IOM-16SFP, IOM-4XFP
Power Supply	2+2 Redundant Hot-swappable Power Supplies, Max Output 1300W
Power Input	AC: 100-240V 50/60Hz DC: -40 ~ -72V
Dimensions(W×D×H)	5U (440×590×225mm)
Weight	<53kg (114lb)
Operating Temperature	0-40°C (32- 104°F)
Humidity	10-95% (Noncondensing)

### Expansion Modules


#### IO Module (IOM)

Specifications	IOM-4XFP	IOM-16SFP
		
Firewall Throughput	20Gbps	20Gbps
Maximum Concurrent Sessions	12,500,000	12,500,000
Port	4-port XFP	16-port SFP
Dimensions	1U, occupies 1 general purpose expansion slot	1U, occupies 1 general purpose expansion slot
Weight	1.2kg (2.6lb)	1.3kg (2.8lb)
Operating Temperature	0-40°C (32-104°F)	0-40°C (32-104°F)
Humidity	10-95% (Noncondensing)	10-95% (Noncondensing)
Supported Platforms	SG-6000-X6150	SG-6000-X6150


## System Control Module (SCM)

Specifications	SCM-20
	
Dimensions	1U, occupies 1 general purpose expansion slot
Weight	1.1 kg (2.4lb)
Operating Temperature	0-40°C (32-104°F)
Humidity	10-95% (Noncondensing)
Supported Platforms	SG-6000-X6150

## Security Service Module (SSM)

Specifications	SSM-20
	
Firewall Throughput	20Gbps
Maximum Concurrent Sessions	8,500,000
Dimensions	1U, occupies 1 general purpose expansion slot
Weight	1.1 kg (2.4lb)
Operating Temperature	0-40°C (32-104°F)
Humidity	10-95% (Noncondensing)
Supported Platforms	SG-6000-X6150

## QoS Service Module (QSM)

Specifications	QSM-20
	
QoS Throughput	20Gbps
Dimensions	1U, occupies 1 general purpose expansion slot
Weight	1.1 kg (2.4lb)
Operating Temperature	0-40°C (32-104°F)
Humidity	10-95% (Noncondensing)
Supported Platforms	SG-6000-X6150

### Features

#### Deployment Mode

- Transparent mode
- Route/NAT mode
- L2/L3 mixed mode

#### High Availability (HA)

- Redundancy of key components
- Active-Active (A/A) and Active-Passive (A/P)

- Configuration synchronization
- Session state synchronization

#### Firewall

- Firewall based on application identification and control
- Role-based access control (RBAC)

### Destination NAT (DNAT)

- IP address translation
- IP address/port translation
- IP address range translation
- Server load balancing based on DNAT

### Protection Against Attacks

- ICMP flood
- UDP flood
- ARP spoofing
- SYN flood
- WinNuke
- IP spoofing
- IP address scanning
- Port scanning
- Ping of Death
- Teardrop
- IP fragment
- IP option anomalies
- Smurf and Fraggle
- Land attack
- Huge ICMP attack
- SYN proxy
- SYN cookie
- TCP option anomalies
- DNS query flood
- DNS recursive query flood

### IPSec VPN

- Standard-based implementation, tested for interoperability with major 3rd party vendors
- Encryption algorithms: DES, 3DES and AES (up to AES256), Diffie-Hellman Group 1, 2 and 5 and Hash algorithms SHA-1 and MD5.
- Preshared key and PKI
- Route-based VPN and policy-based VPN
- VPN quick deployment (PnPVPN)
- Dead Peer Detection (DPD)
- NAT Traversal
- Static IP, dynamic IP and dial-up VPN support
- Anti-Replay
- Responder set COMMIT bit
- QoS over VPN tunnel
- Application control over VPN tunnel
- Routing protocol over VPN tunnel
- GRE and GRE-over-IPSec
- Routing protocol over VPN/GRE/GRE-over-IPSec

### IPv6

- Dual stack IPv4/IPv6 firewall

### Source NAT (SNAT)

- Interface IP or IP pool
- NAT/NAPT
- Sticky NAT
- Translation source and destination IP/port at the same time

### Traffic Management Quality of Service (QoS)

- QoS based on IP, role, application or mixed attributes
- DSCP
- Class of Service (CoS)
- Priority-based QoS
- Support bandwidth limit, bandwidth guarantee, flexible QoS
- Bandwidth limit based on physical port
- Session limit based on source and destination

### ALG Support

- H.323
- SIP
- FTP
- TFTP
- RSH
- RTSP
- SQL Net
- MS-RPC

### Routing

- Dynamic routing RIP v1/v2, OSPF, BGP
- Static routes
- Source-based routing
- Policy-based routing
- Role-based routing
- Equal-Cost Multi-Path (ECMP)

### Centralized Monitoring and Auditing

- Centralized device monitoring
- Bulk device firmware upgrade
- Device CPU/Memory/Session real-time monitoring
- Application visibility and monitoring
- User visibility and monitoring
- Real-time monitoring of various attacks (virus, intrusion)
- Periodic reporting

Unless specified otherwise, all performance, capacity and functionalities are based on StoneOS® 4.0. Results may vary based on StoneOS® version and deployment scenarios.

Notes: (1) IPSec throughput is measured using Preshared Key AES256 +SHA-1, with 1400 byte packets.

(2) New connections/s rate is measured using TCP no close.