



SG-6000-X5100

The New Generation Multi-Core Security Appliance

SG-6000-X5100

The SG-6000 series security appliance is a new generation of multi-core security appliance developed by Hillstone Networks. With Multi-core Plus® G2 architecture and role-based, deep application inspection technology, the SG-6000 series can provide network security much beyond the IP and port based defense of traditional firewalls. The modular design of the hardware offers performance extensibility, solves the performance weakness shared by existing UTM products when AV and IPS protections are turned on. SG-6000-G5100 has a performance up to 20Gbps and is suitable for ISPs, large enterprises and government. It can be deployed in network backbone, main point of entry and datacenters. The appliance can provide role and application based security service, including firewall, IPSec/SSL VPN, application and user QoS, AV, IPS and URL filter control.

Characters

The New Generation Firewall – Deep Application Security

With the rapid development of internet, more and more application are now based on protocols such as HTTP/HTTPS. New security threats are becoming application based. Traditional stateful inspection firewall can only enforce security policy based on ports and protocols, without identifying the application that runs through. These devices thus cannot control today's full spectrum of applications. Hillstone's new generation of firewall can identify and control application based on characteristics and behavior of the traffic, even deal with encrypted traffic, allowing these traffic to be managed and controlled.

StoneOS® can identify hundreds of applications, including P2P, IM, games, office software and applications based on protocols such as SIP, H.323 and HTTP. New application can be supported through application signature updated in real-time, without a StoneOS® upgrade.

Comprehensive VPN Solutions

SG-6000 series multi-core security appliance supports multiple types of IPSec VPN deployment. It is fully compatible with standard IPSec VPN. All the SG-6000 series platforms support hardware acceleration of VPN functionality (including SSL VPN). With the combination of hardware acceleration and multi-core processing ability, SG-6000 series products provide you with high-capacity and high-performance VPN solutions.

With patent pending PnPVPN functionality, VPN devices from the remote branches could automatically get the network and security configuration from the headquarter by simply providing a user name and password. This solves the hard-to-configure, hard-to-use, and hard-to-maintain problem shared by traditional IPSec VPN solutions.

SG-6000 security appliance also integrated third generation SSL VPN, providing role-based access control and an easy-to-configure and speedy remote access solution.

Content Security (UTM Plus®)

The UTM Plus® package of SG-6000 series security appliance includes the following functions: AV, IPS, content filter, Website access control, and application traffic shaping. The security appliance can defend against different types of network attacks, both internal and external, from virus, spyware, worms, Trojan, to information leakage and illegal activities. The content filter functionality and Web URL filtering can help administrators easily block inappropriate web sites, to improve working efficiency and control access to harmful material. Virus database, IPS signature database, and URL database can

be updated through the network at real time, ensuring a quickly response to new virus, attacks, and URLs.

Network Visibility – Role and Application Based Management

There is no security with visibility. The application and user identification feature in StoneOS® help customers understand what is happening in their network and establish better security and traffic management policies.

Role based network services (RBNS) gives a fine grain visibility. Different users, even users from different locations or different times can have different access rights and can be managed differently. User activities can be logged and stored locally or in a server, making it easier to audit based on user name.

RBNS can be divided into three parts: access control, network resource allocation and audit log, all based on 'user'. Through authentication and authorization for a user and identifying their security levels, information leakage due to IP spoofing or PC misuse can be avoided.

Fully Parallel Security Architecture (Multi-Core Plus® G2)

StoneOS®, Hillstone's proprietary 64-bit real-time operating system, has powerful parallel processing capability. With a patent pending architecture, StoneOS® realizes the full potential of multi-core processing in application security processing, compares to using multi-core and NP/ASIC only in layer 3 security processing, found in most of today's security appliances. With this StoneOS advantage, SG-6000 series security appliances have an up to 5 times performance advantage in application processing when compared to other appliances with similar hardware configuration. This creates a strong foundation for an integrated security product, solving the performance issue faced by traditional appliances when multiple functionalities are turned on at the same time.

Carrier-class Hardware Design

SG-6000-X5100 is based on carrier-class design with support for high reliability and high redundancy. Modularized power supply is supported with selection of AC/DC. Dual redundant and hot-swappable power supplies keep the system running nonstop.

Except for the fan tray of SG-6000-5100, all other parts of the system are solid state components. This provides the basis for high reliability of the system. The fan tray is hot-swappable with special monitor circuit. Alarm will be generated as soon as a single fan is malfunctioning, without interrupt system function.

Key Index

Index	SG-6000-X5100
Firewall throughput	20Gbps
IPSec throughput ⁽¹⁾	8Gbps
Max. concurrent sessions (standard/can be extended to)	5/10 Million
AV throughput ⁽²⁾	1.5Gbps
IPS throughput ⁽³⁾	3Gbps
Session Rampup per second ⁽⁴⁾	200,000
IPSec tunnels	30,000
Max. SSL VPN users	10,000
Management interfaces	1 CON, 1 AUX, 2 USB 2.0 ports
Internet interfaces	1 GE interface, 12 SFP interfaces, 2 XFP interfaces
Power supplies	Dual redundancy and hot-swappable power supplies, 200W
Input voltage	AC 100-240V 50/60Hz DC -40 ~ -60V
Dimensions (W×D×H,mm)	2U (440 x 520 x 88)
Weight	15kg
Operating temperature	0-40°C
Operating humidity	10-95% (non-condensing)

Function Specification

Application identification

- The new generation of application identification that is based on the application behaviors and characters
- Application database with hundreds of applications
- Real-time updating of application database

Firewall

- The new generation of application based firewall
- Application/Role based security policies
- DNS Query Flood, SYN Flood, DoS/DDoS protection
- Malformed packets protection
- ARP spoofing protection

Traffic management

- Flexible QoS policies based on user/usergroup, role, application, IP address, time, etc
- CoS based traffic control support, compatible with DiffServ
- Flexible QoS, able to assign bandwidth dynamically

High Availability

- A/A mode and A/P mode
- Configuration synchronization
- Session state synchronization

VPN

- All standard IPSec VPN protocols and deployment methods support
- Innovative PnPVPN for fast IPSec VPN deployment
- SSL VPN support (including two-factor authentication with USB key)
- L2TP VPN support

Anti-virus

- Stream based scanning offers low latency, high concurrent sessions, and high performance
- Support scanning of large files
- Real-time virus connection reset and virus event record
- Support HTTP, FTP, SMTP, IMAP, POP3 and popular compression algorithms (RAR, GZIP, etc)
- Virus signature database with more than 400,000 signatures, updated in real time

URL Filter Control

- Web surfing policies based on role/user, time, priority, etc
- Web URL database with more than 20 million domain names, updated in real time
- Category based URL management controls inappropriate Website access
- Support customized web site classification

Intrusion Prevention System (IPS)

- High performance stateful attack inspection and attack defense
- Block attack source and IP in real-time, record attack events
- Support full range of protocols, including HTTP, FTP, SMTP, IMAP, POP3, TELNET, TCP, UDP, DNS, RPC, FINGER, MSSQL, ORACLE, NNTP, DHCP, LDAP, VoIP, NETBIOS, TFTP, etc
- Inspect and defend against over 3,000 attacks

Hillstone Security Management (HSM)

- Centralize management of devices
- Performance, traffic monitor and analysis

Unless otherwise stated, the performance, capacity and characters listed here are based on StoneOS[®] version 4.0. The real results may differ depending on StoneOS[®] version and deployment environment.

NOTES:

- (1) IPSec throughput is benchmarked with Presharekey+AES256+SHA-1, using 1400 byte packets;
- (2) AV throughput is benchmarked using HTTP traffic with attachments;
- (3) IPS throughput is benchmarked using HTTP traffic with all IPS policies enabled and bidirectional inspection;
- (4) Session Rampup is benchmarked using TCP no close.