Hillstone NETWORKS

Hillstone CloudEdge:

Virtual Next-Generation Firewall

Businesses have been harnessing the advantages of virtualization for faster and more efficient, on-demand delivery of IT resources, but are still grappling with security in these dynamic virtual environments where virtual machines constantly get added, changed or moved, and visibility and security enforcement remain a challenge. Hillstone CloudEdge addresses this security gap and provides a complete virtual firewall solution available in a software form-factor. Hillstone CloudEdge provides advanced security services across Layer 2-7, in addition to core firewall features. It can be deployed via Cloud Management Platforms (CMPs) as a "Firewall as a Service" for a multi-tenant solution in the virtual environment. CloudEdge is also deployed as a security gateway for Virtual Private Cloud (VPC) in the public cloud.

CloudEdge shares a base technology as the Hillstone Next-Generation Firewall (NGFW), and provides the same robust set of security features offered for physical environments. Security administrators can rapidly provision and deploy CloudEdge at scale, and instantly start protecting virtual deployments. CloudEdge identifies and prevents potential threats associated with high-risk applications while providing policy-based control over applications, users, and user groups. Policies can be defined that guarantee bandwidth to mission-critical applications while restricting or blocking inappropriate or malicious applications. Policy based routing and bandwidth management can also be created for users/groups based on time of day and application attributes.

CloudEdge provides independent management as well as remote security access for each tenant, in multi-tenanted virtual and cloud environment. CloudEdge supports major hypervisor technologies including KVM, Xen, VMware ESXi. It is also tightly integrated and supports cloud management platforms (CMP) such as AWS, Openstack and VMware vCenter.

www.hillstonenet.com
Phone: 1-800-889-9860

Product Highlights

- **Leverages Hillstone NGFW Technology:** CloudEdge delivers the same robust features and benefits of the Hillstone NGFW into virtualized and cloud deployments.
- **Enables Access Control for VPCs:** Virtual Private Clouds provide logical security perimeters to protect virtual data centers. CloudEdge is deployed at the VPC entry to provide independent management, control and protection for each tenant.
- **Secures Data Transmission via VPN:** The CloudEdge VPN feature protects data transmission between VPCs or VPCs to their associated enterprise networks.
- **Achieves Deployment and Management:** CloudEdge can be easily changed or instantiated from templates to address the highly dynamic change operations of virtual machines and virtual environments. Fully integrated with CMPs, administrators can launch, stop and configure firewall policies from the CMP itself; administrators can also configure CloudEdge directly via SecureShell (SSH).
- **Provides Multi-tenant Support:** Tenant-specific configurations and security policies are supported for maximum control and protection.

Product Features

Network Services and Support

- Static and policy routing
- Route controlled by application
- Built-in DHCP, NTP, DNS Server and DNS proxy
- Interface modes: sniffer, port aggregated, loopback

Firewall

- Operating modes: NAT/route, transparent (bridge), and mixed mode
- Schedules: one-time and recurring
- 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 support: SNAT, DNAT, PAT, Full Cone NAT, STUN
- Global policy management view
- Policy objects: predefined, custom, and object grouping

QoS Traffic Shaping

- Tunnel allocation based on security domain, interface, address, user/user group, service/service group, application/application group, TOS, VLAN
- Supports embedded two layers and eight tunnels
- Supports maximum bandwidth cap and minimum bandwidth guarantee on multi-level tunnels or on a per IP/user basis
- Supports differentiated services according to priority and bandwidth average allocation policy
- Flexible allocation of remaining bandwidth according to priority
- Actively restrain inbound traffic from server side

Link Load Balancing

- Outbound functions: Policy based routing (PBR) supports ECMP, time and weighted, supports embedded ISP routing and dynamic detection
- Inbound functions: SmartDNS (supports A-record resolution of DNS) and dynamic detection
- Automatically switches the link according to bandwidth occupancy and network latency
- Link health inspection by ARP, PING and DNS

Server Load Balancing

- Supports server health diagnostic, server session protection and session persistence
- Supports multiple SLB algorithm, including weighted hashing, weighted least-connection and weighted round-robin
- Supports server session status monitoring

VPN

- Supports various standard IPSec VPN protocols and deployment modes
- Supports SSL VPN (USB-key option)
- Supports IKEv2 protocol
- Supports Xauth protocol
- Supports OCSP and SCEP
- Supports clients that run iOS, Android, and Windows XP/Vista including 64-bit Windows OS

User and Device Identity Control

- Local user database
- Remote user authentication: LDAP, Radius, Active Directory
- Single-sign-on: Windows Active Directory
- User-based policies

IPS

- 7,000+ signatures, protocol anomaly detection, custom signatures, manual, automatic 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 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)
- Predefined prevention configuration

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

High Availability

- Redundant heartbeat interfaces
- High availability mode: Active/Passive
- Standalone session synchronization
- Failover:
  - Port, local & remote link monitoring
  - Stateful failover
  - Sub-second failover
  - Failure detection notification
- Deployment Options:
  - HA with link aggregation
  - Full mesh HA

Administration

- Management access: HTTP/HTTPS, SSH, telnet
- Central Management: Hillstone Security Manager (HSM), web service APIs
- System Integration: SNMP, syslog, alliance partnerships
- Rapid deployment: local and remote script execution
- Dynamic real-time dashboard status and drill-in monitoring, widgets
- Language support: English

Logs and Reporting

- Logging facilities: local storage, and third-party multiple syslog servers
- Detailed traffic logs: forwarded, violated sessions, local traffic, invalid packets
- Comprehensive event logs: system and administrative activity audits, routing and networking, VPN, user authentications

Hypervisors Supported

- KVM, VMware ESXi, Xen, AMI (AWS)

Specifications

Model	SG-6000-VM01	SG-6000-VM02
Core (Min/max)	1/1	2/2
Memory	1G	2G
Network Interfaces	10	10
Firewall Throughput (1518 Bytes)	2Gbps	4Gbps
Maximum Concurrent Sessions	100K	500K
New Sessions Per Second	10K	20K
IPS Throughput	1 Gbps	2 Gbps
IPSEC Throughput	200Mbps	400Mbps
IPSEC VPN Tunnels	50	500
SSL VPN Users (Default/max)	5/50	5/250

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS 5.5R1. Results may vary based on StoneOS® version and deployment.