Hillstone CloudEdge: Virtual Next-Generation Firewall

Hillstone Virtual Next-Generation Firewall, CloudEdge, embedded with the Hillstone Networks StoneOS operation system, is deployed as a virtual machine, and provides advanced security services for applications and users in any virtualized environment. It provides comprehensive security features including granular application identification and control, VPN, intrusion prevention, anti-virus, attack defense and cloud-sandbox to fully keep a business secure and operational. It provides price- performance solutions for both public and private cloud customers, and can be rapidly provisioned and deployed at scale.

Product Highlights

Highly Compatible with Virtual Environments

In virtual environments, compute, storage, and data resources run on virtual machines. Hillstone CloudEdge supports major hypervisor technologies including ESXi, KVM, Hyper-V, and Xen server, and can be rapidly deployed on a virtual machine, to provide advanced security services for virtual networks or virtualized applications. Deployed as a virtual appliance, CloudEdge can overcome the limitation of physical firewalls, and inspect all traffic inside the virtual network, to protect both south-north and east-west traffic. In addition, users can flexibly deploy and manage network resources based on the requirements of network topologies, and thereby fully leverage the advantage of vitalization.

Advanced Threat Protection Capability

CloudEdge shares a base technology with Hillstone Next-Generation Firewall (NGFW). It can satisfy the network security requirements of both public cloud and private cloud users. Hillstone CloudEdge provides fine-grained control of web applications regardless of port, protocol, or evasive action. It can identify and prevent potential threats associated with high-risk applications while providing policy-based control over applications, users, and user-groups. In addition, CloudEdge incorporates a unified threat detection engine that shares packet details with multiple security engines (AD, IPS, URL filtering, Anti-Virus, Cloud-sandbox etc.), which significantly enhance security efficiency while reducing network latency.

Visualized Security Management with Cloud Management Platform

Hillstone CloudEdge provide exclusive security segmentation and policy protection for independent tenants in cloud deployments. It can realize instant recovery based on the snapshot system. If a virtual appliance has an issue or outage, it can be recovered via the snapshot of a saved configuration, and start a new virtual firewall on the original or a new virtual machine. The CloudEdge graphical management interface has multiple logging query functions, which can effectively monitor and track the network status; and a reporting function that provides real-time details of traffic and security events. These tools help administrators fully visualize and grasp the network operation status, and improve operational efficiency.

Deployment Automation and Service Orchestration

Hillstone CloudEdge provides multiple integrated solutions to address the needs and requirements of cloud platforms and has already been deployed into multiple test and production cloud environments to serve diverse industries and customer requirements. Hillstone CloudEdge' s automation deployment and license management functions enable the cloud user the capability of self-service and self-management based on their business needs without interruption from cloud administrators. Orchestration ensures each CloudEdge can be deployed and configured automatically. License management ensures CloudEdge can automatically enter operation mode. Hillstone CloudEdge REST API supports system configuration, security policy configuration, interfaces and network configurations, to integrate with major cloud management platforms.

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
- 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

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

Cloud-Sandbox

- Upload malicious files to cloud sandbox for analysis
- Support protocols including HTTP/HTTPS, POP3, IMAP, SMTP and FTP
- Support file types including PE,ZIP, RAR, Office, PDF, APK, JAR and SWF
- File transfer direction and file size control
- Provide complete behavior analysis report for malicious files
- Global threat intelligence sharing, real-time threat blocking
- Support detection only mode without uploading files

Botnet C&C Prevention

- Discover intranet botnet host by monitoring C&C connections and block further advanced threats such as botnet and ransomware

- Regularly update the botnet server addresses
- prevention for C&C IP and domain
- Support TCP, HTTP, and DNS traffic detection
- IP and domain whitelists

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
- 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

Data Security

- File transfer control based on file type
- File protocol identification, including HTTP, FTP, SMTP and POP3
- File signature and suffix identification for over 100 file types
- Content filtering for HTTP-GET, HTTP-POST, FTP and SMTP protocols
- IM identification and network behavior audit

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

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

High Availability

- Redundant heartbeat interfaces
- 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

SSL Decryption

- Application identification for SSL encrypted traffic
- IPS enablement for SSL encrypted traffic
- AV enablement for SSL encrypted traffic
- URL filter for SSL encrypted traffic
- SSL Encrypted traffic whitelist
- SSL proxy offload mode

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
- 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 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)

License Management

- Automatic license activation/deactivation
- Public cloud or private cloud users with internet access
- License movement with device

CloudView

- Cloud-based security monitoring
- 7/24 access from web or mobile application
- Device status, traffic and Threat monitoring
- Cloud-based log retention and reporting

REST API

- Sign-on, device monitoring
- Address book, service book, application book
- Application policy, AV policy, IPS policy, DNAT/SNAT, security policy
- Configuration: Interface configuration, Routing configuration, Zone configuration

Virtualization

- Hypervisor: KVM, VMware ESXi, Xen, AMI (AWS), Hyper-V
- Public Cloud: AWS, Azure, AliCloud etc.
- Cloud Management Platform: Openstack Liberty and above versions, VMware vCenter 5.5 and above versions etc.
- Array AVX Series Network Functions Platform

Specifications

Specification	VM01	VM02	VM04
Core (Min)	2	2	4
Memory (Min)	2G	4G	8G
Storage (Min.)	4 GB	4 GB	4 GB
Network Interfaces	10	10	10
Firewall Throughput (vNIC/SR-IOV)	2 Gbps / 10 Gbps	4 Gbps / 20 Gbps	8 Gbps / 30 Gbps
IPS Throughput (vNIC/SR-IOV)	1 Gbps / 3 Gbps	2 Gbps / 5 Gbps	4 Gbps / 7 Gbps
AV Throughput (vNIC/SR-IOV)	800 Mbps / 1 Gbps	1.6 Gbps / 2 Gbps	3.2 Gbps / 4 Gbps
IPsec VPN Throughput (vNIC/SR-IOV)	200 Mbps / 400 Mbps	400 Mbps / 800 Mbps	800 Mbps / 2 Gbps
New Sessions / Second(vNIC/SR-IOV)	20K / 30K	40K / 50K	80K / 100K
Maximum Concurrent Sessions	100K	500K	5M
IPSec VPN Tunnels (Max.)	100	500	10000
SSL VPN Users (Max.)	100	500	2000

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.5R6. Results may vary based on StoneOS® version and deployment.

Note: The Performance above were observed using a Del R720 Server (Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.70GHz, 64GB memory, 4x 10 GE interfaces) , VMXnet3 under VMware environment. SR-IOV was observed under KVM.

Version: EX-08.01-CloudEdge-5.5R6-0818-EN-01