Hillstone CloudEdge: Virtual Next-Generation Firewall

Hillstone CloudEdge provides advanced security services across Layer 2-7, in addition to core firewall features to public and private cloud users. 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 shares a base technology as the "NSS Labs Recommended" 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, Hyper-V, VMware ESXi etc. It is also tightly integrated and supports CMPs such as Amazon Web Service (AWS), Microsoft Azure, AliCloud, Openstack and VMware vCenter.

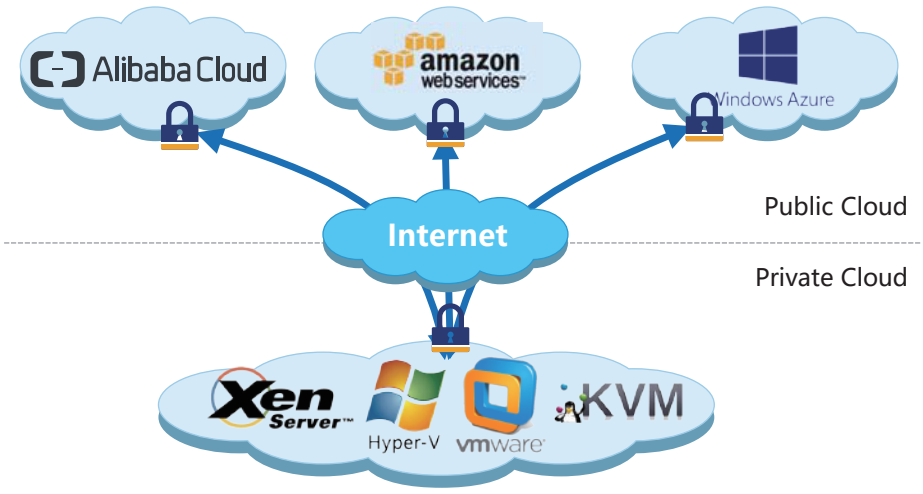

Figure 1. Hillstone CloudEdge Deployment Scenarios

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. It can provide comprehensive security features including granular application identification and control, intrusion prevention, anti-virus, attack defense, etc.

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, VPCs to their associated enterprise networks or VPCs on different cloud platforms.

Easily Deployed and Managed

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.

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
- Schedules: one-time and recurring

Intrusion Prevention

- Up to 8000+ signatures, protocol anomaly detection, rate-based detection, custom signatures, manual, automatic push or pull signature updates, integrated threat encyclopedia (1)
- 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

- 4 million Antivirus signatures, 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

Features

- 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

IP Reputation

- Botnet server IP blocking with global IP reputation database

Endpoint Identification

- 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 and endpoint quantity

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

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
- Server health check, session monitoring and session protection

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

IPv6

- Management over IPv6, IPv6 logging and HA
- IPv6 tunneling, DNS64/NAT64 etc
- IPv6 routing protocols, static routing, policy routing, ISIS, RIPng, OSPFv3 and BGP4+
- IPS, Application identification, Access control, ND attack defense

Features

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

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

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

REST API

- Object: Address book, service book
- 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.

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
AV Throughput	800Mbps	1.6Gbps

Unless specified otherwise, all performance, capacity and functionality are based on StoneOS5.5R4. Results may vary based on StoneOS® version and deployment.
NOTES: (1)The number of IPS signatures supported varies for each platform based on its hardware capability;