Hillstone Virtual Firewall

The Hillstone virtual Firewall (vFW) allows you to provision firewall security whenever and wherever it is needed. It features most of the networking services common to Hillstone's hardware based appliances and is an ideal solution for protecting network resources within the cloud and virtualized infrastructure. With the addition of the virtual firewall Hillstone offers greater choice and flexibility by providing the ability to deploy a mix of hardware and virtual appliances operating together and managed from a centralized management platform.

Highlights

Inter-VM Traffic Inspection

Physical security lacks the flexibility to inspect inter-VM traffic. It requires traffic to be routed to the physical appliance and back again into the virtualized environment. This complicates network topology and impacts performance. With Hillstone's vFW performance is increased because network traffic is inspected inside the virtualized environment, which eliminates the rerouting of traffic.

Granular Application Control

Hillstone's vFW provides fine-grained control of web applications. It can identify and prevent 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. In addition, selected features within an application (e.g., games, file sharing) can be blocked or bandwidth managed by user/group, time of day and other criteria.

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

Features

Network Services

- Static and Policy routing
- Route controlled by application
- Built-in DHCP, NTP, DNS Server and DNS proxy
- 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
- 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
- NAT configuration: per policy and central NAT table
- VoIP: SIP/H.323/SCCP NAT traversal, RTP pin holing
- Global policy management view
- Schedules: one-time and recurring
- QoS Traffic Shaping:
  - 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
  - Load balancing:
  - Weighted hashing, weighted least-connection, and weighted round-robin
  - Session protection, session persistence and session status monitoring
  - Bidirectional 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 and latency
  - 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
- SSL VPN tunnel mode 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
- View and manage IPSEC and SSL VPN connections

User and Device Identity

- Local user database
- Remote user authentication: LDAP, Radius, Active Directory
- Single-sign-on: Windows AD
- 2-factor authentication: 3rd party support, integrated token server with physical and SMS
- User and device-based policies

IPS

- 7,000+ signatures, 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

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
- Active/Passive
- Standalone session synchronization
- 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

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 & Reporting

- Logging facilities: local memory and storage (if available), multiple syslog servers
- Reliable logging using TCP option (RFC 3195)
- Detailed traffic logs: forwarded, violated sessions, local traffic, invalid packets
- 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

Hypervisors Supported

- VMware, KVM, 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.