Hillstone CloudEdge:
Firewall Virtual de Próxima Generación

El Firewall Hillstone Virtual de Próxima Generación, CloudEdge, integrado con el sistema operativo Stonestone de Hillstone Networks, se implementa como una máquina virtual y proporciona servicios de seguridad avanzados para aplicaciones y usuarios en cualquier entorno virtualizado. Proporciona funciones de seguridad integrales que incluyen identificación y control granular de aplicaciones, VPN, prevención de intrusiones, antivirus, defensa contra ataques y un sand-box en la nube para mantener a su empresa completamente segura y operativa. Proporciona soluciones de rendimiento por precio para clientes de nubes públicas y privadas, y se puede aprovisionar y desplegar rápidamente a escala.

Detalles del Producto

Altamente Compatible con Entornos Virtuales

En entornos virtuales, los recursos informáticos, de almacenamiento y de datos se ejecutan en máquinas virtuales. Hillstone CloudEdge admite las principales tecnologías de hipervisor, incluidos los servidores ESXi, KVM, Hyper-V y Xen, y se puede implementar rápidamente en una máquina virtual para proporcionar servicios de seguridad avanzados para redes virtuales o aplicaciones virtualizadas. Implementado como un dispositivo virtual, CloudEdge puede superar la limitación de los firewalls físicos e inspeccionar todo el tráfico dentro de la red virtual, para proteger tanto el tráfico sur-norte como el de este-oeste. Además, los usuarios pueden desplegar y administrar de forma flexible los recursos de red en función de los requisitos de las topologías de red, y así aprovechar al máximo la ventaja de la vitalización.

Gestión de Seguridad Visualizada con Plataforma de Gestión en la Nube

Hillstone CloudEdge proporciona segmentación de seguridad exclusiva y protección de políticas para inquilinos independientes en implementaciones en la nube. Puede realizar una recuperación instantánea basada en el sistema snapshot. Si un dispositivo virtual tiene un problema o interrupción, se puede recuperar a través de un snapshot con una configuración guardada y se puede iniciar un nuevo firewall virtual en la máquina virtual original o nueva. La

Detalles del Producto (Continuación)

interfaz de administración gráfica de CloudEdge tiene múltiples funciones de consulta del registro, que pueden monitorear y seguir eficazmente el estado de la red; y una función de informes que proporciona detalles en tiempo real de los eventos del tráfico y la seguridad. Estas herramientas ayudan a los administradores a visualizar y comprender completamente el estado del funcionamiento de la red y mejorar su eficiencia operativa.

Capacidad Avanzada de Protección Contra Amenazas

CloudEdge comparte su tecnología básica con Hillstone Next-Generation Firewall (NGFW). Puede satisfacer los requisitos de seguridad de la red tanto en una nube pública como para usuarios de una nube privada. Hillstone CloudEdge proporciona un control detallado de las aplicaciones web, independientemente del puerto, protocolo o acción evasiva. Puede identificar y prevenir amenazas potenciales asociadas con las aplicaciones de alto riesgo al tiempo que proporciona un control basado en políticas sobre aplicaciones, usuarios y grupos de usuarios. Además, CloudEdge incorpora un motor unificado de detección de amenazas que comparte detalles de paquetes con múltiples motores de seguridad (AD, IPS, filtrado de URL, antivirus, Cloud-sandbox, etc.), que mejoran significativamente la eficacia de la seguridad y reducen la latencia de la red.

Automatización de Implementación y Orquestación de Servicios

Hillstone CloudEdge proporciona múltiples soluciones integradas para abordar las necesidades y requisitos de las plataformas en la nube y ya se ha implementado en múltiples entornos de prueba y de producción en la nube para servir a diversas industrias y a varios requisitos del cliente. Las funciones de administración de licencias y despliegue de automatización de Hillstone CloudEdge permiten al usuario de la nube la capacidad de autoservicio y autogestión según las necesidades de su negocio sin interrupción por parte de los administradores de la nube. La orquestación garantiza que cada CloudEdge se pueda implementar y configurar automáticamente. La gestión de licencias garantiza que CloudEdge pueda ingresar automáticamente al modo operativo. La API REST de Hillstone CloudEdge admite la configuración del sistema, la configuración de su política de seguridad, las interfaces y las configuraciones de red, para integrarse con las principales plataformas de administración en la nube.

Características

Servicios de Red
- Enrutamiento dinámico (OSPF, BGP, RIPv2)
- Enrutamiento estático y por políticas
- Rutas controladas por la aplicación
- DHCP, NTP, Servidor DNS y proxy DNS incorporados
- Modo Tap - se conecta al puerto SPAN
- Modos de interface: sniffer, puerto agregado, loopback, VLAN (802.1Q y Trunking)
- Conmutación y enrutamiento de L2/L3
- Cable virtual (Capa 1) despliegue transparente en línea

Firewall
- Modos operativos: NAT/ruta, transparente (puente), y modo mixto
- Objetos de política: predefinidos, personalizados y por agrupación de objetos
- Política de seguridad basada en la aplicación, el papel y la geolocalización
- Gateways a nivel de aplicación y soporte de sesiones: MSRCP, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, dcerpc, dns-tcp, dns-udp, H.245 0, H.245 1, H.323
- Soporte NAT y ALG: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT, STUN
- Configuración de NAT: por política y por tabla NAT central
- VoIP: SIP/H.323/SCCP NAT traversal, RTP pin holing
- Vista de gestión de políticas globales
- Inspección de redundancia de la política de seguridad, grupo de política, restauración de la configuración de la política
- Asistente para una implementación fácil y detallada de políticas
- Análisis y limpieza de políticas inválidas
- Política integral de DNS
- Horarios: de una sola vez y recurrente

Prevención de Intrusiones
- Detección de anomalías de protocolo, detección basada en tasas, firmas personalizadas, actualización manual o automática de firmas, enciclopedia de amenazas integrada
- Acciones IPS: por defecto, monitoreo, bloqueado, reinicio (IP de los atacantes o de la víctima, interfaz de entrada) con tiempo de caducidad
- Opción de registro de paquetes
- Selección basada en filtros: gravedad, destino, sistema operativo, aplicación o protocolo
- Exención de IP de firmas específicas de IPS
- Modo rastreo IDS
- Protección DoS basada en tasas IPv4 e IPv6 con configuración de umbral contra inundaciones de TCP Syn, escaneo de puertos TCP/UDP/SCTP, barrido de ICMP, inundación de sesiones TCP/UDP/SCIP/ICMP (origen/destino)
- Bypass activo con interfaces de bypass
- Configuraciones de prevención predefinidas

Antivirus
- Manual, actualización automática de firmas push o pull
- Antivirus basado en flujos: protocolos que incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP
- Escaneo de virus en archivos compreso

Defensa Contra Ataques
- Defensa contra ataques de protocolo anormal
- Anti-DoS/DDoS, incluyendo SYN Flood, defensa contra inundación de consultas DNS
- Defensa contra ataques ARP

Filtrado por URL
- Inspección de filtrado web basado en el flujo
- Filtrado web definido manualmente basado en URL, contenidos web y por cabecera MIME
- Filtrado web dinámico en tiempo real basado en la nube con base de datos categorizadora: más de 140 millones de URLs con 64 categorías (8 de los cuales están relacionados con la seguridad)
- Características adicionales de filtrado web:
  - Filtrado de Applets de Java, ActiveX o de cookies
  - Bloqueo a Posteos HTTP
  - Registro de palabras clave de búsqueda

Características (Continución)

- Por privacidad, conexiones cifradas exentas de exploración en ciertas categorías
- Anulación del perfil web de filtrado: permite que el administrador asigne temporalmente diferentes perfiles de usuario/grupo/IP
- Filtro Web para categorías locales y anulación de categorías calificadas

Cloud Sandbox

- Carga archivos maliciosos a la nube en una sandbox para su análisis, incluyendo el tráfico cifrado HTTPS
- Se incluye el soporte de los siguientes protocolos HTTP/HTTPS, POP3, IMAP, SMTP y FTP
- Se incluye el soporte de los siguientes protocolos PE, ZIP, RAR, Office, PDF, APK, JAR y SWF
- Soporte de Transferencia de Archivos y Control de Tamaño de Archivos
- Proporciona un informe completo sobre el análisis del comportamiento de los archivos maliciosos
- Compartir la inteligencia de amenazas reales. Bloqueo de amenazas en tiempo real
- Único modo de detección de apoyo sin subir archivos

Prevención Botnet C&C

- Descubre botnet en la intranet mediante el control de conexiones C&C y bloquea amenazas avanzadas botnet y ransomware
- Constantemente actualiza direcciones de servidores de botnets.
- prevención para C&C IP y dominio
- Apoyo a la detección de tráfico TCP, HTTP y DNS
- Listas blancas de IP y dominios

Reputación de IP

- Identifica y filtra el tráfico de riesgo IP, como host de botnet, spammers, nodos TOR, host vulnerados y ataques a fuerza bruta
- Registra, caída de paquetes, o bloqueo para los diferentes tipos de riesgo en tráfico IP
- Constante actualización de la base de datos IP por reputación y firmas

Identificación de Puntos Finales

- Soporte e Identificación de Puntos Finales por Dirección IP, Identificación de Puntos Finales por Cantidad , Identificación de Puntos Finales por tiempo de Actividad en línea , Identificación de Puntos Finales por duración en el tiempo de Actividad en línea
- Soporta 10 sistemas operativos incluyendo Windows, iOS, Android, etc.
- Consulta de apoyo basada en IP, cantidad de punto final, política de control y estado etc.
- Apoya la identificación de la cantidad de terminales de acceso en capa 3, registro e interferencia en desbordamiento de IP
- Después de bloquear al usuario, puedes redireccionar al usuario a una página específica
- Soporta bloqueo de operaciones en desbordamiento de IP

Control de Aplicaciones

- Más de 4,000 aplicaciones se pueden filtrar por nombre, categoría, subcategoría, tecnología y por riesgo
- Cada aplicación contiene una descripción, sus factores de riesgo, dependencias, puertos típicos utilizados, y las URL de referencia adicionales
- Acciones: bloqueo, reinicio de la sesión, monitoreo, modulación del tráfico
- Identifica y controla aplicaciones en la nube
- Proporciona monitoreo multidimensional y estadísticas para las aplicaciones en la nube, incluyendo la categoría de los riesgos y sus características

Calidad de Servicio (QoS)

- Número máximo de túneles/ancho de banda garantizados o por IP/usuario
- Asignación de túnel basada en dominio de seguridad, interfaz, dirección, usuario/grupo, servidor/grupo de servidores, app/grupo de apps, TOS, VLAN
- Ancho de banda asignado por hora, prioridad, o reparto equitativo del ancho de banda
- Tipo de Servicio (TOS) y el soporte a servicios diferenciados (DiffServ)
- Asignación de prioridades de ancho de banda restante
- Número máximo de conexiones simultáneas por IP
- Límite de ancho de banda al demorar el acceso por usuario o IP
- Limpieza automática y manual del tráfico expirado utilizado por el usuario

Servidores de Balanceo de Carga

- Hash ponderada, menor conexión ponderada y round-robin ponderado
- Protección de la sesión, persistencia de sesión y estado de la sesión de monitoreo
- Comprueba el estado del servidor, supervisión de sesiones y protección de sesiones

Balanceo de Carga en Enlaces

- Equilibrio de carga del enlace bidireccional
- Equilibrio de carga del enlace de salida que incluye política de enrutamiento, ECMP y ponderada, enrutamiento ISP integrado y detección dinámica
- Equilibrio de carga de enlaces de entrada soporta SmartDNS y detección dinámica
- Cambio de Enlace Automática basada en Anchos de Banda, Latencia, Variación, Conectividad, Aplicación , etc.
- Inspección del enlace con ARP, PING, y DNS

VPN

- VPN IPSec
  - IPSec Fase 1: Modo de protección agresiva y de ID principal
  - Opciones de aceptación de colegas: cualquier ID, ID específica, ID en el grupo usuario de acceso telefónico
  - Soporta IKEv1 e IKEv2 (RFC 4306)
  - Método de autenticación: certificado y una clave pre-compartida
  - Configuración a modo de IKE (como servidor o cliente)
  - DHCP por IPSec
  - Caducidad de clave cifrada IKE configurable, NAT transversal para mantener viva la frecuencia
  - Cifrado propuesto para Fase 1/Fase 2: DES, 3DES, AES128, AES192, AES256
  - Autenticación propuesta para Fase 1/Fase 2: MD5, SHA1, SHA256, SHA384, SHA512
  - Soporte Diffie-Hellman para Fase 1/Fase 2: 1,2,5
  - XAuth como modo de servidor y para usuarios de acceso telefónico
  - Detección de Punto Muerto
  - Detección Replay
  - Autokey para mantener la conexión en la Fase 2 SA
- Apoyo total a IPSEC VPN: permite múltiples inicios de sesión SSL VPN personalizados asociados a grupos de usuarios (rutas de URL, diseño)
- Opciones de configuración IPSEC VPN: por rutas o por políticas
- Modos de implementación de VPN IPSec: puerta de enlace a puerta de enlace, malla completa, hub-and-spoke, túnel redundante, terminación de VPN en modo transparente
- Una entrada de tiempo impide conexiones concurrentes con el mismo nombre de usuario
- Limita usuarios concurrentes en portal SSL
- Módulo VPN SSL para reenvío de puertos encripta los datos del cliente y envía los datos al servidor de aplicaciones
- Permite clientes que ejecutan iOS, Android y Windows XP/Vista, incluyendo el sistema operativo Windows de 64 bits
- Comprueba la integridad del host y del sistema operativo antes de conectar al túnel SSL
- Comprueba equipos MAC por portal
- Opción de limpieza de caché antes de finalizar la sesión SSL VPN
- Modo de servidor y cliente L2TP, L2TP sobre IPSec y GRE sobre IPSec
- Deja ver y administrar conexiones IPSEC y SSL VPN
- PnPVPN

IPv6

- Gestión sobre IPv6, logueo IPv6 y HA
- Túneles IPv6, DNS64/NAT64 etc.
- Protocolos de enrutamiento IPv6, enrutamiento estático, enrutamiento por política, ISIS, RIPng, OSPFv3 y BGP4 +
- IPS, identificación de aplicaciones, control de acceso, defensa contra ataques ND

Alta Disponibilidad

- Interfaces heartbeat redundantes
- Activo/Activo y Activo/Pasivo
- Sincronización de sesión autónoma
- Interfaz HA de gestión reservada
- Conmutación por error:
  - Puerto, monitoreo de vínculos locales y remotos
  - Con estado de conmutación por error
  - Conmutación por error, inferior a un segundo
  - Notificación de fallas
- Opciones de Implementación:
  - HA con agregación de enlaces
  - HA con malla completa
  - HA geográficamente dispersa

"Twin-mode" Alta Disponibilidad

- Modo de alta disponibilidad entre múltiples dispositivos.
- Múltiples modos de despliegue de HA
- Configuración y sincronización de sesiones entre múltiples dispositivos.

Descifrado SSL

- Identificación de la aplicación para el tráfico cifrado SSL
- Habilitación IPS para el tráfico cifrado SSL
- Habilitación AV para el tráfico cifrado SSL
- Filtro URL para tráfico cifrado SSL
- Lista blanca para tráfico cifrado SSL
- Modo proxy por descarga SSL

Identidad de Usuario y Dispositivo

- Base de datos de usuario local
- Autenticación de usuario remoto: TACACS +, LDAP, Radius, Active
- Single-Sign-on: Windows AD
- Autenticación de 2 factores: Apoyo a terceros, servidor de contador integrado con token físico y SMS
- Políticas de usuario y por dispositivo
- Sincronización de grupos de usuarios basada en AD y LDAP
- Soporte para Proxy 802.1X, SSO
- Permite autenticación de usuario basada en MAC

Administración

- Acceso administrativo: HTTP/HTTPS, SSH, Telnet, consola
- Administración Central: Administrador Hillstone de seguridad (HSM), API de servicios web
- Integración de Sistemas: SNMP, Syslog, alianzas
- Despliegue rápido: Instalación automática de USB, ejecución local y remota del script

Características (Continución)

- Estado dinámico, en tiempo real del tablero de instrumentos y widgets de monitoreo drill-in
- Soporte de idiomas: Inglés

Registros e Informes

- Instalaciones para Registros: memoria y almacenamiento locales (si está disponible), múltiples servidores syslog y varias plataformas Hillstone para Auditoría de Seguridad (HSA)
- Cifrado de registros e integridad de registros con subida programada de lotes HSA
- Registro fiable utilizando la opción TCP (RFC 3195)
- Registros detallados del tráfico: reenviados, sesiones violadas, tráfico local, paquetes inválidos, URL, etc.
- Registro detallado de eventos: auditorías del sistema y de la actividad administrativa, enrutamiento y trabajo en red, VPN, autenticaciones de usuario, eventos relacionados con WiFi
- Opción de IP y servicio de resolución de nombres de puerto
- Opción de formato para breves registros del tráfico
- Tres informes predefinidos: Informes de seguridad, de flujo y de red
- Generación de informes definidos por el usuario
- Los informes se pueden exportar en formato PDF, a través de correo electrónico y FTP

Estadísticas y seguimiento

- Aplicación, URL, estadística de eventos de amenaza y control
- Análisis y estadísticas de tráfico en tiempo real
- Información del sistema como la sesión concurrente, CPU, memoria y temperatura
- iQOS estadística de tráfico y seguimiento, enlace monitoreo del estado
- Apoyo a la recopilación de información de tráfico y expedición vía Netflow (v9.0)

Gestión de Licencias

- Activación / desactivación automática de licencias
- Nube pública o usuarios de la nube privada con acceso a Internet
- Movimiento de licencia con un dispositivo

CloudView

- Monitoreo de seguridad basado en la nube
- Acceso 24/7 desde la web o desde una aplicación móvil
- Estado del dispositivo, tráfico y monitoreo de amenazas
- Retención e informes de registros basados en la nube

REST API

- Inicio de sesión, monitoreo de dispositivos
- Libreta de direcciones, libro de servicios, libro de aplicaciones
- Política de aplicaciones, política AV, política IPS, DNAT/SNAT, política de seguridad
- Configuración: Configuración de la interfaz, configuración de enrutamiento, configuración zonal

Virtualización

- Hypervisor: KVM, VMware ESXi, Xen, IAM (AWS), Hyper-V
- Nube Pública AWS, Azure, AliCloud etc.
- Plataforma de Administración de la Nube: Openstack Liberty y versiones anteriores, VMware vCenter 5.5 y versiones anteriores, etc.
- Array AVX Serie de funciones de red de la plataforma

Especificaciones

	VM01	VM02	VM04
Core (Min)	2	2	4
Memory (Min)	2 GB	4 GB	8 GB
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
IMIX Throughput (vNIC/SR-IOV)	550 Mbps / 1.6 Gbps	1.3 Gbps / 2.1 Gbps	1.3 Gbps / 2.6 Gbps
NGFW Throughput (vNIC/SR-IOV)	700 Mbps / 1.5 Gbps	1.4 Gbps / 2.5 Gbps	2.8 Gbps / 3.5 Gbps
Threat Protection Throughput (vNIC/SR-IOV)	400 Mbps / 500 Mbps	800 Mbps / 1 Gbps	1.6 Gbps / 2 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)	20,000 / 30,000	40,000 / 50,000	80,000 / 100,000
Maximum Concurrent Sessions	100,000	500,000	5 Million
IPSec VPN Tunnels (Max.)	100	500	10,000
SSL VPN Users (Max.)	100	500	2,000

NOTA:

El rendimiento anterior se observó utilizando un servidor Dell R720 (Intel (R) Xeon (R) CPU E5-2609 v2 @ 2.50 GHz, 64 GB de memoria, 2x 10 interfaces GE) y StoneOS 5.5R7. El rendimiento real puede variar según la versión de StoneOS y la configuración de red y del sistema.

A menos que se especifique lo contrario, todo el rendimiento, la capacidad y funcionalidad se basan en StoneOS 5.5R7. Los resultados pueden variar en función del StoneOS® Versión y despliegue.

Version: EX-08.01-CloudEdge-5.5R7-0520-SP-01