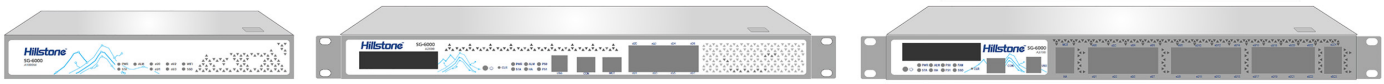
Serie A de Hillstone
de Próxima Generación



El firewall de próxima generación de Hillstone Serie A presenta un alto rendimiento de seguridad, expansión según sea necesario, completa detección y prevención de amenazas avanzadas e inteligente y automatizada operación de políticas. Esta serie NGFW, ya preparada para el futuro, se basa en una nueva arquitectura de hardware que ofrece un rendimiento de capa de aplicaciones líder en la industria para satisfacer las necesidades de seguridad de red del mundo real. Los puertos de alta densidad garantizan una excelente capacidad de acceso y sus grandes opciones de almacenamiento ofrecen mejor visibilidad y análisis. Hillstone Serie A NGFW ofrece defensas completas y avanzadas contra amenazas conocidas y desconocidas, junto con una operación inteligente de políticas, automatizada y eficiente que facilita las operaciones de seguridad.

Detalles del Producto

Protección y detección de amenazas avanzadas

El Hillstone Serie A NGFW incluye un arsenal completo de mecanismos para proporcionar detección y protección en tiempo real durante todo el ciclo de vida de los ataques de red y malware. Antes de que se produzca una infracción, las protecciones proactivas como IPS bloquean la explotación de vulnerabilidades. Los servicios de reputación de IP bloquean las solicitudes de sitios de riesgo potencialmente involucrados en malware y spam. El filtrado de URL evita que los usuarios accedan inadvertidamente a sitios asociados con phishing, descargas de malware y otras vulnerabilidades. El antivirus detecta y bloquea malware conocido a nivel de red con una avanzada base de datos de firmas que se actualiza continuamente. Anti-spam proporciona clasificación y prevención de spam en tiempo real, tanto para el tráfico entrante como para el saliente.

Durante una infracción, el antivirus también juega un papel importante al continuar detectando y bloqueando malware conocido. Una sandbox en la nube proporciona detección y prevención sofisticadas de archivos maliciosos a través del análisis estático y el preprocesamiento, seguido de un análisis de comportamiento que incluye la detección de maniobras evasivas. Luego, la inteligencia de la nube identifica y bloquea los archivos maliciosos, genera registros e informes y comparte la inteligencia de amenazas con la nube.

Al completar las protecciones durante todo el ciclo de vida de las amenazas, la Serie A continúa defendiendo incluso después de que se haya producido una infracción. La función avanzada de prevención Botnet C&C de Hillstone evita la comunicación con el canal de control y también detecta y bloquea bots dentro de la intranet.

Además, el motor de análisis y detección de amenazas

Detalles del Producto (Continuación)

unificado del sistema coordina todos los mecanismos de seguridad integrados para mejorar drásticamente la eficiencia y reducir la latencia en la red.

Arquitectura de hardware de alto rendimiento

La Serie A preparada para el futuro presenta un factor de forma compacto y una base informática poderosa que garantiza un alto rendimiento con una seguridad sin concesiones. Los NGFW de la Serie A ofrecen un rendimiento sólido para el rendimiento del firewall, sesiones nuevas y simultáneas, y un rendimiento increíblemente rápido para la capa de aplicaciones, que es fundamental para satisfacer las necesidades de los actuales entornos de seguridad. También ofrece una ecología de software amigable para la integración de terceros, admitiendo características de seguridad adicionales si se desea. Todos los modelos de montaje en rack cuentan con ventilación delantera y trasera para ayudar en la disipación del calor, que es una preocupación en redes de casi cualquier tamaño.

Excelente capacidad de acceso y expansión de almacenamiento

La Serie A de Hillstone ofrece una alta densidad de puertos de E/S, lo que permite que el NGFW actúe como un switch o enrutador según sea necesario, lo que reduce los costos de implementación y administración. Además, hay ranuras de expansión disponibles para varios modelos de la Serie A para aumentar aún más el rendimiento. Los pares de derivación en la mayoría de los modelos de la Serie A ayudan a garantizar la continuidad del negocio.

Todos los modelos, incluidas las versiones de escritorio, incluyen un gran almacenamiento integrado y muchos de ellos tienen opciones de expansión para un almacenamiento de disco duro más grande de hasta 2 TB. Con más almacenamiento, el sistema puede guardar más registros y datos durante más tiempo, lo que permite un análisis más profundo. Además, el almacenamiento ampliado permite que el sistema proporcione informes más completos con mucha más información, incluidos resultados visualizados y recomendaciones procesables.

Además, con un análisis de amenazas más profundo, WebUI puede mostrar información de detección de amenazas mucho más rica, lo que a su vez brinda a los administradores una mejor visibilidad. La mayor visibilidad permite a los administradores concentrarse rápidamente en anomalías y otros eventos o tráfico de red sospechosos, analizarlos y responder.

Operación Inteligente de Políticas

La Serie A incluye administración y operación inteligente en todo el ciclo de vida de las políticas, desde su implementación hasta la administración, optimización y operación. El sistema cuenta con implementación automatizada de políticas de usuario mediante la autorización dinámica RADIUS.

La gestión de políticas se vuelve mucho más eficiente a través de agrupaciones de políticas basadas en los requisitos comerciales. Además, se pueden agregar políticas para permitir que un conjunto de políticas actúe como una sola política. Un asistente de políticas innovador analiza los patrones de tráfico y recomienda políticas perfeccionadas para una gestión de políticas más rápida, fácil y precisa. La operación de las políticas se vuelve más eficiente y precisa mediante verificaciones de redundancia de políticas, que identifican políticas redundantes para la desactivación o eliminación, y el análisis del recuento de aciertos de políticas, que ayuda a refinar y ajustar las políticas.

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
- Multidifusión (PIM-SSM)
- Cable virtual (Capa 1) despliegue transparente en línea

Firewall
- Modos operativos: NAT/ruta, (puente) transparente, y modo mixto
- Objetos de políticas: política global, personalizada, predefinida, 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 políticas de seguridad, grupo de políticas, políticas agregada con reversión de configuración de políticas
- Asistente para generación de políticas basadas en servicio o aplicación
- Análisis y limpieza de políticas inválidas
- Política integral de DNS
- Agendamiento: de una sola vez y recurrente
- Importación y exportación de políticas de apoyo

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
- Captura de paquetes de amenazas IPS (solo con almacenamiento de expansión)

Antivirus
- Manual, actualización automática de firmas push o pull
- Agregar o eliminar manualmente la firma MD5 a la base de datos AV
- La firma MD5 admite la carga en la caja de arena de la nube y la agregación o eliminación manual en la base de datos local
- Antivirus basados en flujos: protocolos que incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP y SMB
- Escaneo de virus en archivos compreso

Defensa contra Ataques
- Defensa contra ataques de protocolo anormal
- La defensa contra ataques de inundación (flooding) incluye : inundación ICMP, inundación UDP, inundación de consultas DNS, inundación de consultas DNS recursivas, inundación de respuesta DNS, inundación SYN.
- Se incluye defensa contra suplantación de ARP y suplantación de identidad ND
- Defensa contra escaneo y suplantación, incluye la suplantación de direcciones IP, barrido de direcciones IP, escaneo de puertos.
- Defensa DoS / DDoS,incluye ataques de ping de la muerte, ataque teardrop, fragmentación de IP, opción de IP, ataque Smurf , land attack, paquetes ICMP con carga , ataque WinNuke.
- Lista de permisos para la dirección IP de destino

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 basado en la nube para bases de datos con categorización en tiempo real: más de 140 millones de URLs con 64 categorías (8 de los cuales están relacionados con la seguridad)
- Características adicionales del filtrado web:
  - Filtrado de Applets de Java, ActiveX o de cookies
  - Bloqueo a Posteos HTTP
  - Registro de palabras clave de búsqueda
  - 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
- Admite lista de permitidos de URL y lista de bloqueo

Anti-Spam(1)
- Clasificación y prevención del spam en tiempo real
- Spam confirmado, spam sospechoso, spam masivo, volumen válido
- Protección Independientemente del idioma, formato o contenido del mensaje
- Admite protocolos de correo electrónico SMTP y POP3
- Detección entrante y saliente
- Listas blancas para permitir correos electrónicos de dominios confiables

Cloud-Sandbox
- Carga archivos maliciosos a la nube en una sandbox para su análisis
- Se incluye el soporte de los siguientes protocolos HTTP/HTTPS, POP3, IMAP, SMTP, FTP y SMB
- Tipos de archivos soportados, incluye PE, ZIP, RAR, Office, PDF, APK, JAR, SWF y script
- 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
- Configuración de lista de bloqueos / permisos URL

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
- Lista de permitidos y bloqueados según la dirección IP o el nombre de dominio
- Admite detección de sinkhole DNS y túneles DNS
- Admite detección DGA

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

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
- Tráfico cifrado SSL y de lista blanca
- Modo proxy por descarga SSL
- El proxy SSL admite la creación de listas blancas de IP y lista blanca predefinida
- Admite TLS v 1.2, TLS v 1.3
- Admite identificación de aplicaciones, DLP, caja de arena IPS, AV para el tráfico descifrado de proxy SSL de SMTPS/POP3S/IMAPS

Identificación y Control 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
- Identificación de usuarios y control de tráfico para servicios de escritorio remoto de Windows Server

Características (Continuación)

Seguridad de datos
- Control de transferencia de archivos basado en nombre, tamaño y tipo de archivo
- Identificación de protocolo de archivo, incluidos HTTP, FTP, SMTP, POP3 y SMB
- Identificación de firmas y sufijos de archivos para más de 100 tipos de archivos
- Filtrado de contenido para los protocolos HTTP-GET, HTTP-POST, FTP y SMTP
- Filtrado de contenido para palabras clave predefinidas y contenido de archivos
- Identificación de IM y auditoría de comportamiento de la red
- Filtración de archivos transmitidos por HTTPS usando SSL Proxy y SMB

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), Servicios Diferenciados (DiffServ) y soporte de clase de tráfico
- Asignación de prioridades de ancho de banda restante
- Número máximo de conexiones simultáneas por IP
- Asignación de ancho de banda según la categoría de URL
- 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 saliente: enrutamiento basado en políticas que incluye enrutamiento de ISP integrado, ponderado, por tiempo y ECMP; detección de calidad de enlace activo y pasivo en tiempo real y selección de la mejor ruta
- 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 trans versal 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
  - IKEv1 soporte DH para grupos 1,2,5,19,20,21,24
  - IKEv2 soporte DH para grupos 1,2,5,14,15,16,19,20,21,24
  - 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)
- IPsec VPN admite una guía de configuración. Las opciones de configuración incluyen: basado en rutas o basado en 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 sola 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
- Admite clientes que ejecutan iOS, Android, Microsoft Windows, macOS y Linux
- Comprueba la integridad del host y del sistema operativo antes de conectar al túnel SSL
- Comprueba equipos MAC por portal
- Opción de limpieza del caché antes de finalizar la sesión SSL VPN
- Modo de servidor y cliente L2TP, L2TP sobre IPsec y GRE sobre IPsec
- Visualiza y administra conexiones IPsec y SSL VPN
- PnPVPN
- VTEP para túnel de unidifusión estático VxLAN

IPv6
- Gestión sobre IPv6, registro de IPv6, HA y modo HA peer, twin mode AA y AP
- Tuneles IPv6: DNS64/NAT64, IPv6 ISATAP, IPv6 GRE, IPv6 sobre IPv4 GRE
- Protocolos de enrutamiento IPv6, enrutamiento estático, enrutamiento por política, ISIS, RIPng, OSPFv3 y BGP4+
- Compatibilidad con IPv6 en LLB
- IPS, identificación de aplicaciones, filtrado de URL, antivirus, Control de acceso, Attack-Defense, iQoS, SSL VPN
- Soporte de marco jumbo IPv6
- Compatibilidad con IPv6 Radius y SSO-Radius
- IPv6 es compatible con listas blancas de Active Directory
- Compatibilidad con IPv6 en los siguientes protocolos ALG: TFTP, FTP, RSH, HTTP, SORBO, SQLNETv2, RTSP, MSRPC, SUNRPC
- Soporte de IPv6 en iQoS distribuido
- Detección y rastro de direcciones

VSYS (solo disponible en modelos de montaje en rack)
- Asignación de recursos del sistema para cada vSYS
- Virtualización de la CPU
- Firewall de soporte VSYS sin raíz, IPSec VPN, SSL VPN, IPS, filtrado de URL, monitoreo de aplicaciones, reputación de IP, AV, QoS
- Monitoreo vSYS y estadístico, monitoreo de aplicaciones, reputación de IP, AV, QoS

Alta Disponibilidad
- Interfaces heartbeat redundantes
- Activo / pasivo y modo par
- 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
- Puertos de enlace de datos HA duales

"Twin-mode" Alta Disponibilidad (solo disponible en modelos A3000 y superiores)
- Modo de alta disponibilidad entre múltiples dispositivos
- Múltiples modos de despliegue de HA
- Configuración y sincronización de sesiones entre múltiples dispositivos

Identidad de Usuarios y Dispositivos
- Base de datos de usuario local
- Autenticación remota de usuarios: TACACS +, LDAP, Radius, Directorio Activo
- 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
- WebAuth: personalización de la página, prevención cracks forzados, compatibilidad con IPv6
- Autenticación basada en interfaz

Características (Continuación)

- Sin agente ADSSO (Polling AD)
- Usar sincronización de autenticación basada en SSO-monitor
- Admite autenticación de usuario basada en IP y MAC
- El servidor Radius emite la política de seguridad del usuario a través de un mensaje CoA

Administración

- Acceso administrativo: HTTP/HTTPS, SSH, Telnet, consola
- Administración Central: Administrador de seguridad Hillstone (HSM), API de servicios web
- Integración de Sistemas: SNMP, Syslog, alianzas
- Despliegue rápido: Instalación automática de USB, ejecución local y remota del script
- Estado dinámico, en tiempo real del tablero de instrumentos y widgets de monitoreo drill-in
- Soporte de idiomas: Inglés
- Autenticación de administrador: Active Directory y LDAP

Registros e Informes

- Logging facilities: almacenamiento local; hasta 6 meses de almacenamiento de registros con almacenamiento de expansión (disco duro SSD), servidor syslog, Hillstone HSM o 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
- Auditoría de configuración de políticas de soporte

Estadísticas y seguimiento

- Aplicación, URL, estadística de eventos de amenaza y supervisión
- 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)

CloudView

- Monitoreo de seguridad basado en la nube
- Acceso desde la web 24x7 o por medio de Aplicación móvil
- Estado del dispositivo, tráfico y monitoreo de amenazas
- Retención de logs e informes de registros basados en la nube

Seguridad de IoT (Internet de las Cosas)

- Identifique dispositivos IoT, como cámaras IP y grabadores de video en red
- Soporta consulta de resultados de monitoreo basados en condiciones de filtrado, incluyendo tipo de dispositivo, dirección IP, estado, etc.
- Soporta listas blancas personalizadas

Especificaiones del Producto

	SG-6000-A200	SG-6000-A200W	SG-6000-A1000	SG-6000-A1100	SG-6000-A2000	SG-6000-A2600
						
Firewall Throughput [2]	1 Gbps	1 Gbps	4 Gbps	5 Gbps	5 Gbps	5 Gbps
NGFW Throughput [3]	300 Mbps	300 Mbps	1.2 Gbps	1.2 Gbps	1.2 Gbps	1.8 Gbps
Threat Protection Throughput [4]	200 Mbps	200 Mbps	800 Mbps	800 Mbps	800 Mbps	1.6 Gbps
Maximum Concurrent Sessions [5]	300,000	300,000	300,000	300,000	1 Million	1.2 Million
New Sessions/s [6]	15,000	15,000	48,000	48,000	48,000	120,000
IPS Throughput [7]	610 Mbps	610 Mbps	3.4 Gbps	3.7 Gbps	3.2 Gbps	4.5 Gbps
AV Throughput [8]	550 Mbps	550 Mbps	1.8 Gbps	2.0 Gbps	2.0 Gbps	3.7 Gbps
IPsec VPN Throughput [9]	0.62 Gbps	0.62 Gbps	2.5 Gbps	2.7 Gbps	2.7 Gbps	3 Gbps
SSL Proxy Throughput [10]	15 Mbps	15 Mbps	250 Mbps	250 Mbps	250 Mbps	750 Mbps
Virtual Systems (Default/Max)	N/A	N/A	N/A	N/A	1/5	1/5
Firewall Policy Number	4000	4000	4,000	4,000	8,000	12,000
SSL VPN Users (Default/Max)	8/128	8/128	8/128	8/128	8/1,000	8/1,000
IPsec Tunnel Number	512	512	2,000	2,000	4,000	6,000
Management Ports	1 × Console Port, 2 x USB 2.0 Ports	1 × Console Port, 2 x USB 2.0 Ports	1 × Console Port, 2 × USB3.0 Port	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45)
Fixed I/O Ports	1×SFP, 5×GE	1×SFP, 5×GE	4 × GE	8 × GE (including 1 bypass pair)	8 × GE (including 1 bypass pair)	8 × GE (including 1 bypass pair)
Wi-Fi	N/A	IEEE802.11a/b/g/n/ac	N/A	N/A	N/A	N/A
Available Slots for Expansion Modules	N/A	N/A	N/A	N/A	N/A	N/A
Expansion Module Option	N/A	N/A	N/A	N/A	N/A	N/A
Twin-mode HA	N/A	N/A	N/A	N/A	N/A	N/A
Local Storage	4 GB	4 GB	8 GB	8 GB	8 GB	8 GB
Expansion Storage Options	N/A	N/A	256 GB SSD	256 GB SSD	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD
Power Specification	24W, Single AC (default)	24W, Single AC (default)	30W, Single AC	50W, Single AC	50W, Single AC (default), Dual AC (optional)	50W, Single AC (default), Dual AC (optional)
Power Supply	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V
Form Factor	Desktop	Desktop	Desktop	Desktop	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	180 × 110 × 28	180 × 110 × 28	270 × 160 × 44	270 × 160 × 44	436 × 320 × 44	436 × 320 × 44
Dimensions (W × D × H, inches)	7.1 × 4.3 × 1.1	7.1 × 4.3 × 1.1	10.6 × 6.3 × 1.7	10.6 × 6.3 × 1.7	17.2 × 12.6 × 1.7	17.2 × 12.6 × 1.7
Weight	2.2 lb (0.6 kg)	2.2 lb (0.6 kg)	3.1 lb (1.4 kg)	3.1 lb (1.4 kg)	8.6 lb (3.9 kg)	8.6 lb (3.9 kg)
Working Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

Especificaiones del Producto (Continuación)

	SG-6000-A2700	SG-6000-A2800	SG-6000-A3000	SG-6000-A3600	SG-6000-A3700	SG-6000-A3800
						
Firewall Throughput [2]	10 Gbps	16 Gbps	20 Gbps	20 Gbps	20 / 40 Gbps	20 / 40 Gbps
NGFW Throughput [3]	2.59 Gbps	2.6 Gbps	1.8 Gbps	1.8 Gbps	1.8 Gbps	3.7 Gbps
Threat Protection Throughput [4]	1.73 Gbps	1.83 Gbps	1.6 Gbps	1.6 Gbps	1.6 Gbps	2.8 Gbps
Maximum Concurrent Sessions [5]	1,500,000	1,800,000	2 Million	3 Million	6 Million	8 Million
New Sessions/s [6]	130,000	130,000	140,000	140,000	140,000	310,000
IPS Throughput [7]	5 Gbps	5 Gbps	8.3 Gbps	8.5 Gbps	8.6 Gbps	17.5 Gbps
AV Throughput [8]	4.2 Gbps	4.2 Gbps	4.9 Gbps	5.0 Gbps	5.2 Gbps	9.4 Gbps
IPsec VPN Throughput [9]	5 Gbps	5.5 Gbps	6 Gbps	6 Gbps	6.5 Gbps	12 Gbps
SSL Proxy Throughput [10]	800 Mbps	800 Mbps	950 Mbps	950 Mbps	950 Mbps	2 Gbps
Virtual Systems (Default/Max)	5	5	1/5	1/50	1/100	1/100
SSL VPN Users (Default/Max)	8/1,000	8/1,000	8/2,000	8/4,000	8/6,000	8/8,000
IPsec Tunnel Number	6,000	6,000	8,000	10,000	16,000	20,000
Firewall Policy Number	12,000	12,000	20,000	20,000	20,000	40,000
Management Ports	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)	1 × Console Port, 2 × USB3.0 Port, 1 × MGT Port (RJ45), 1 × HA Port (RJ45)
Fixed I/O Ports	2 × SFP+, 8 × SFP, 8 × GE	2 × SFP+, 8 × SFP, 8 × GE	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)	2 × SFP+, 8 × SFP, 16 × GE (including 2 bypass pairs)
Wi-Fi	N/A	N/A	N/A	N/A	N/A	N/A
Available Slots for Expansion Modules	N/A	N/A	N/A	N/A	1	1
Expansion Module Option	N/A	N/A	N/A	N/A	IOC-A-4SFP+, IOC-A-2MM-BE, IOC-A-2SM-BE	IOC-A-4SFP+, IOC-A-2MM-BE, IOC-A-2SM-BE
Twin-mode HA	N/A	N/A	Yes	Yes	Yes	Yes
Local Storage	8 GB	8 GB	8 GB	8 GB	8 GB	8 GB
Expansion Storage Options	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD
Power Specification	50W, Single AC (default), Dual AC (optional)	50W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	100W, Dual AC (default), Dual DC (optional)
Power Supply	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V	AC 100-240 V 50/60 Hz DC -36~-72 V
Form Factor	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	440 x 320 x 44	440 x 320 x 44	436 × 437 × 44	436 × 437 × 44	436 × 437 × 44	436 × 437 × 44
Dimensions (W × D × H, inches)	17.3 x 12.6 x 1.7	17.3 x 12.6 x 1.7	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7
Weight	9 lb (4.1 kg)	9 lb (4.1 kg)	13.2 lb (6 kg)	13.2 lb (6 kg)	13.4 lb (6.1 kg)	15 lb (6.8 kg)
Working Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

Especificaiones del Producto (Continuación)

	SG-6000-A5200	SG-6000-A5500	SG-6000-A5600	SG-6000-A5800
				
Firewall Throughput [2]	32/65 Gbps	40/80 Gbps	60/85 Gbps	80/95 Gbps
NGFW Throughput [3]	15.84 Gbps	17.12 Gbps	30.84 Gbps	31.94 Gbps
Threat Protection Throughput [4]	11.37 Gbps	10.43 Gbps	19.13 Gbps	18.43 Gbps
Maximum Concurrent Sessions [5]	12,000,000	12,000,000	20,000,000	24,000,000
New Sessions/s [6]	400,000	500,000	800,000	930,000
IPS Throughput [7]	20/35 Gbps	25/40 Gbps	35/60 Gbps	45/75 Gbps
AV Throughput [8]	12 Gbps	15 Gbps	20 Gbps	25 Gbps
IPsec VPN Throughput [9]	20 Gbps	28 Gbps	36 Gbps	45 Gbps
SSL Proxy Throughput [10]	5 Gbps	5 Gbps	8.5 Gbps	8.5 Gbps
Virtual Systems (Default/Max)	250	250	500	500
SSL VPN Users (Default/Max)	8/10,000	8/10,000	8/10,000	8/10,000
IPsec Tunnel Number	40,000	40,000	40,000	40,000
Firewall Policy Number	40,000	60,000	60,000	80,000
Management Ports	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 2 × HA ports (SFP+)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 2 × HA ports (SFP+)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA port (SFP)	1 × Console Port, 2 × USB3.0 Ports, 1 × MGT Port (RJ45), 1 × HA port (SFP)
Fixed I/O Ports	6 × SFP+, 16× SFP, 8× GE (including 2 bypass pairs)	6 × SFP+, 16× SFP, 8× GE (including 2 bypass pairs)	2 × QSFP+, 16 × SFP+, 8 × GE (including 4 bypass pairs)	2 × QSFP+, 16 × SFP+, 8 × GE (including 4 bypass pairs)
Wi-Fi	N/A	N/A	N/A	N/A
Available Slots for Expansion Modules	1	1	1	1
Expansion Module Option	IOC-A-4SFP+, IOC-A-2QSFP+, IOC-A-2MM-BE, IOC-A-2SM-BE	IOC-A-4SFP+, IOC-A-2QSFP+, IOC-A-2MM-BE, IOC-A-2SM-BE	IOC-A-4SFP+, IOC-A-2QSFP+, IOC-A-2MM-BE, IOC-A-2SM-BE	IOC-A-4SFP+, IOC-A-2QSFP+, IOC-A-2MM-BE, IOC-A-2SM-BE
Twin-mode HA	Yes	Yes	Yes	Yes
Local Storage	64 GB	64 GB	64 GB	64 GB
Expansion Storage Options	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD	500GB / 1TB / 2TB SSD
Power Specification	289W, Dual AC (default), Dual DC (optional)	289W, Dual AC (default), Dual DC (optional)	382W, Dual AC (default), Dual DC (optional)	382W, Dual AC (default), Dual DC (optional)
Power Supply	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V	AC 100-240V, 50/60 Hz DC -36~-72 V
Form Factor	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U	Rackmount, 1U
Dimensions (W × D × H, mm)	436 × 437 × 44	436 × 437 × 44	436 × 437 × 44	436 × 437 × 44
Dimensions (W × D × H, inches)	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7	17.2 × 17.2 × 1.7
Weight	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)	18.7 lb (8.5 kg)
Working Temperature	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)	32-104°F (0-40°C)
Relative Humidity	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing	10-95% non-condensing

Opciones del Módulo

	IOC-A-4SFP+	IOC-A-2MM-BE	IOC-A-2SM-BE	IOC-A-2QSFP+
				
Names	4SFP+ Expansion Module	4SFP Multi-mode Bypass Expansion Module	4SFP Single-mode Bypass Expansion Module	2QSFP+ Expansion Module
I/O Ports	4 × SFP+, SFP+ module not included	4 × SFP, MM bypass (2 pairs of bypass ports)	4 × SFP, SM bypass (2 pairs of bypass ports)	2 × QSFP+
Dimension	1U	1U	1U	1U
Weight	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)	2.09 lb (0.96 kg)

NOTAS:

(1) La función Anti-Spam no está disponible en el modelo SG-6000-A200 y SG-6000-A200W;
(2) Los datos de rendimiento del firewall se obtienen bajo tráfico UDP de con un tamaño de paquete de 1518 bytes. El rendimiento del firewall para A3700 y A3800 se puede aumentar de 20 Gbps a 40 Gbps a través del módulo de expansión IOC-A-4SFP+ adicional;
(3) Los datos de rendimiento de NGFW se obtienen por debajo de 64 Kbytes de tráfico HTTP con control de aplicaciones e IPS habilitado;
(4) Los datos de rendimiento de protección de amenazas se obtienen por debajo de 64 Kbytes de tráfico HTTP con control de aplicaciones, IPS, AV y filtrado de URL habilitados;
(5) El máximo de sesiones simultáneas se obtiene con tráfico HTTP;
(6) las Nuevas Sesiones se obtuvieron en virtud de tráfico HTTP;
(7) para IPS se obtuvieron los datos de rendimiento bajo de detección de tráfico HTTP bi-direccional con todas las normas de IPS activadas;
(8) datos de rendimiento AV se obtuvieron bajo tráfico HTTP con el archivo adjunto;
(9) se obtuvieron los datos de rendimiento IPSec bajo Preshare configuración AES256 + SHA-1 y paquetes 1400 bytes;
(10) Los datos de rendimiento del proxy SSL se obtienen mediante AES128-GCM-SHA256 con todas las reglas IPS activadas.
A menos que se especifique lo contrario, todo el rendimiento, la capacidad y funcionalidad se basan en StoneOS 5.5R9. Los resultados pueden variar en función del StoneOS® versión y despliegue.

Version: EX-08.01-NGFW-A-Series-5.5R9-0122-SP-01-SR