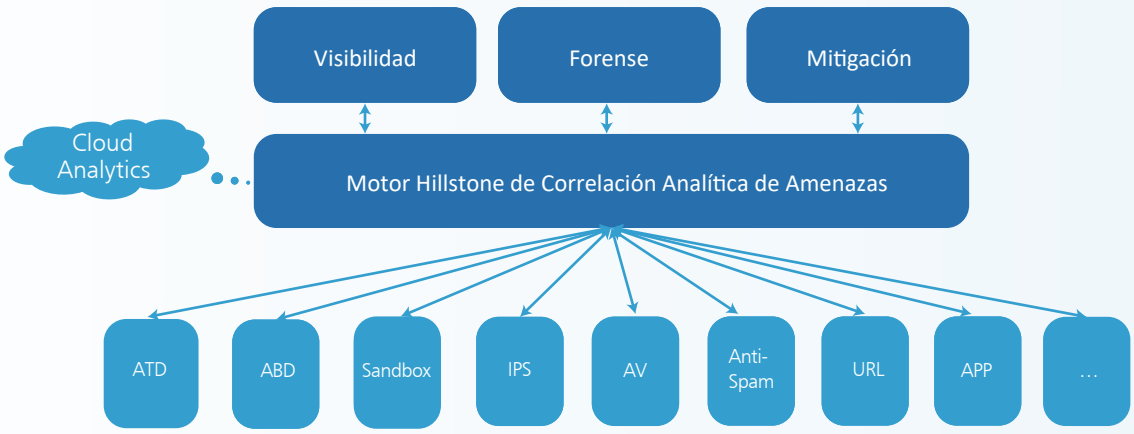
Hillstone Serie-T Firewall Inteligente de Próxima Generación

T1860 / T2860 / T3860 / T5060 / T5860

El Firewall Serie-T inteligente de Hillstone de Próxima Generación (iNGFW) utiliza tres tecnologías clave para detectar ataques avanzados y proporcionar una defensa continua para las redes de hoy en día. En primer lugar, utiliza agrupamiento estadístico para detectar malware desconocido, aprovechando el motor patentado de detección de amenazas Hillstone Advanced Threat Detection Engine (ATD). En segundo lugar, utiliza análisis comportamental para detectar comportamiento anómalo en la red, basado en el motor de detección de Hillstone Advanced Behavior Detection engine (ABD) Por último, apalanca la correlación del motor Hillstone de análisis de amenazas para correlacionar eventos de amenazas detectadas por los motores dispares - incluyendo ATD, ABD, sandbox y otras tecnologías para la detección de amenazas tradicionales basadas en firmas - junto con la información de contexto para identificar las amenazas avanzadas.

Con capacidades de detección y análisis de amenazas profundas, el iNGFW de Hillstone ofrece a los clientes una visibilidad completa de la situación de riesgo en la red, así como los detalles de amenaza para cada huésped. El Hillstone iNGFW proporciona a los administradores la información forense con diferentes herramientas y caminos, con el fin de profundizar en la causa raíz de un ataque. Además, el Hillstone iNGFW faculta al administrador con funciones de mitigación de gran alcance, que pueden ganar tiempo para los administradores al examinar los datos forenses, tomar una decisión informada acerca de la autenticidad del ataque, y reducir al mínimo los daños al negocio.



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

Detalles del Producto

Detección de malware desconocido

Hillstone ha construido un motor propio que ha analizado cerca de un millón de muestras de malware "conocidas." Cada muestra ha sido clasificada y caracterizada basado en múltiples dimensiones que describen sus acciones, activos y atributos. En un entorno de producción, cuando se encuentra un nuevo malware, también se analiza, se caracteriza y se clasifica. Luego, se compara con la base de datos de muestras de malware conocidos que ya han sido analizados. Cuanto más cerca coincida con una muestras conocidas - mayor será la certeza de que se trata de una variante de una muestra de malware conocido. Este proceso se denomina "agrupamiento estadístico" y proporciona un método preciso para la identificación de nuevos programas maliciosos.

Análisis Forense Detallado

Hillstone ofrece una nueva forma de visualizar y analizar los ataques. Cada acción tomada por un código potencialmente malicioso se vincula automáticamente a los pasos dentro de "Kill Chain." Se complementa con información forense rica que permite que el analista determine el origen del ataque, la gravedad de la crisis, y la metodología empleada. Hillstone también proporciona archivos de captura de paquetes, que, cuando se combinan con el registro del sistema y con registros de tráfico, proporcionan al administrador una gran cantidad de información adicional. Además, de los datos del usuario, tales como los sitios web visitados, aplicaciones utilizadas, y el nivel de riesgo de las aplicaciones, para enfocar mejor la explotación. Lo más importante, Hillstone identifica la política de Firewall exacta que le permitió al atacante penetrarlo.

Detección de Comportamiento Anormal

El motor de comportamiento anormal de Hillstone supervisa continuamente la red para aprender como luce el tráfico normal de la red día a día, a cierta hora y en tal mes; proporcionando alertas cuando la actividad de la red supera los umbrales calculados. Se utiliza una matriz dimensional de 50+ para calcular el tráfico normal de la red en la capa L4-L7, llamado "modelado de comportamiento." Además, se ha entrenado con herramientas de piratería reales para asegurar que reconocerá fácilmente la actividad maliciosa. Estas técnicas limitan los falsos positivos y proporcionan al usuario múltiples oportunidades para detener un ataque.

Mitigación Prioritaria

Además de la posibilidad de realizar un cambio de política para prevenir un ataque, Hillstone ha incorporado varias funciones automáticas de mitigación. Estas funciones consisten en plantillas predefinidas que desaceleran automáticamente o bloquean un ataque si se detecta un comportamiento sospechoso. El administrador puede modificar las plantillas para limitar el ancho de banda o el número de sesiones disponibles para el atacante. También puede ajustar las limitaciones que introduce en los recursos de la red según el tipo de ataque y el nivel de gravedad. En los casos en que el ataque es crítico y el nivel de confianza es alto, la mitigación puede incluir un bloqueo completo de todos los recursos de la red. Y, si una plantilla no existe o no está activa, el administrador puede configurar rápidamente una mitigación temporal para ese evento.

Caracteristicas

Análisis de correlación de amenazas

- Correlación entre las amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales
- Reglas de correlación multidimensional, actualización diaria automática en la nube

Detección Avanzada de Amenazas

- Detección avanzada de malware basada en el comportamiento
- Detección de más de 2000 familias de programas maliciosos conocidos y desconocidos, incluyendo virus, desbordamiento, gusanos, troyanos, etc.
- En tiempo real, en línea, comportamiento del malware, actualización de base de datos modelo

Detección de Comportamiento Anormal

- Modelado de comportamiento basado en L3-L7 tráfico de la línea de base para revelar comportamientos anómalos en la red, tales como análisis HTTP, spiders, spam, SSH/FTP contraseña débil
- La detección de ataques DDoS incluyendo por inundación, Sockstress, zip de la muerte, reflexión, consultas DNS, DDos SSL y aplicaciones DDoS
- Apoya la inspección del tráfico de un túnel encriptado para aplicaciones desconocidas
- En tiempo real, en línea, comportamiento anormal de la actualización de la base de datos modelo

Visibilidad y Mitigación de Amenazas

- Indice de riesgo de red, activos críticos y riesgo del estado del anfitrión, gravedad del riesgo de amenaza para la seguridad del anfitrión
- Mapeo del Kill Chain sobre los eventos de amenaza en cada anfitrion
- Amenaza forense que incluye el análisis de las amenazas, base de conocimientos, la historia y los PCAP
- Normas de mitigación predefinidos y personalizados

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, (puente) transparente, 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
- Política integral de DNS
- Agendamiento: 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

Anti-Virus

- 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 con base en datos de categorización en tiempo real, basados en la nube: 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

Anti-Spam

- Clasificación y prevención de spam en tiempo real
- Correo no deseado confirmado, correo no deseado sospechoso, correo no deseado masivo, bulto válido
- Protección Independientemente del idioma, formato o contenido del mensaje
- Admite protocolos de correo electrónico SMTP y POP3
- Detección de entrada y salida
- Listas blancas para permitir correos electrónicos de dominios de confianza

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

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 lista blanca
- Modo proxy por descarga SSL

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
- Soporte de 10 Sistemas Operativos
- 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

Seguridad de datos
- Control de transferencia de archivos basado en el tipo de archivo
- Identificación del protocolo de archivos, incluidos HTTP, FTP, SMTP y POP3
- 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
- Identificación de IM y auditoría de comportamiento de la red

Control de Aplicaciones
- Más de 3.000 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
- Asignación de ancho de banda según la categoría de URL
- Límite de ancho de banda al demorar el acceso por usuario o IP

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 de 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 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
- Acepta 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 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

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, filtrado de URL, antivirus, control de acceso, defensa contra ataques ND

VSYS
- Asignación de recursos del sistema para cada vSYS
- Virtualización de la CPU
- Soporte de Firewall No-root VSYS, IPSec VPN, VPN SSL, IPS, filtrado de URL
- Monitoreo vSYS y estadístico

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

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
- Personalización de la página Web por medio de WebAuth
- Autenticación basada en interfaz
- Sin agente ADSSO (Polling AD)
- Usar sincronización de autenticación basada en SSO-monitor
- Permite autenticación de usuario basada en MAC

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

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)

CloudView
- Monitoreo de seguridad basado en la nube
- Acceso desde la web 7x24 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

Detalles del Producto

Especificaciones	SG-6000-T1860	SG-6000-T2860	SG-6000-T3860	SG-6000-T5060	SG-6000-T5860
					
FW Throughput[1]	8Gbps	10Gbps	20Gbps	25Gbps	40Gbps
IPS Throughput[2]	3Gbps	4Gbps	8Gbps	12Gbps	18Gbps
AV Throughput[3]	1.6Gbps	2Gbps	6Gbps	7Gbps	10Gbps
IPSec Throughput[4]	3Gbps	3.8Gbps	12Gbps	15Gbps	28Gbps
IMIX Throughput[5]	1.6Gbps	2.1Gbps	8.2Gbps	10.9Gbps	17.4Gbps
NGFW Throughput[6]	1Gbps	1.5Gbps	5Gbps	8Gbps	12Gbps
Threat Protection Throughput[7]	600Mbps	900Mbps	2.5Gbps	4Gbps	6Gbps
New Sessions/s [8]	80K	100K	250K	300K	450K
Maximum Concurrent Sessions	1.5M	3M	4M	5M	6M
IPSec Tunnel Number	6,000	10,000	20,000	20,000	20,000
SSL VPN Users (Default/Max)	8/4,000	8/6,000	128/10,000	128/10,000	128/10,000
Integrated I/O	6 × GE, 4 × SFP	6 × GE(1 pair bypass port), 4 × SFP, 2 × SFP+	2 × GE, 4 × SFP	2 × GE, 4 × SFP	2 × GE, 4 × SFP
Maximum I/O	26 × GE	26 × GE, 2 × 10GE	22 × GE, 4 × 10GE	38 × GE, 8 × 10GE	38 × GE, 8 × 10GE
Expansion Modules	2 × Generic Slot	2 × Generic Slot	2 × Generic Slot	4 × Generic Slot	4 × Generic Slot
Expansion Module Option	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M	IOC-4GE-B-M, IOC-8GE-M, IOC-8SFP-M	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-4XFP, IOC-8SFP+, IOC-4SFP+	IOC-8GE-M, IOC-8SFP-M, IOC-4GE-B-M, IOC-4XFP, IOC-8SFP+, IOC-4SFP+
Management Ports	1 × Concole Port, 1 × HA, 1 × MGT, 1 × USB 2.0, 1 × AUX Port	1 × Concole Port, 1 × HA, 1 × MGT, 1 × USB 2.0, 1 × AUX Port	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT	1 × Console Port, 1 × AUX Port, 1 × USB 2.0 Port, 2 × HA, 1 × MGT
Maximum Power Consumption	1 × 150w Redundancy 1 + 1	1 × 150w Redundancy 1 + 1	2 × 450W Redundancy 1 + 1	2 × 450W Redundancy 1 + 1	2 × 450W Redundancy 1 + 1
Storage	480G SSD (960G SSD Optional)	480G SSD (960G SSD Optional)	Dual Storage: 128G (480G or 960G SSD Optional) +480G SSD (960G SSD Optional)	Dual Storage: 128G (480G or 960G SSD Optional) +480G SSD (960G SSD Optional)	Dual Storage: 128G (480G or 960G SSD Optional) +1T HDD (960G SSD Optional)
Power Supply	AC 100~240V 50/60Hz DC -40~-60V	AC 100~240V 50/60Hz DC -40~-60V	AC 100-240V 50/60Hz DC -40 ~ -60V	AC 100-240V 50/60Hz DC -40 ~ -60V	AC 100-240V 50/60Hz DC -40 ~ -60V
Dimension (W × D × H)	1U 17.2 × 14.4 × 1.7 in (436 × 366 × 44 mm)	1U 17.2 × 14.4 × 1.7 in (436 × 366 × 44 mm)	2 U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)	2 U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)	2 U 17.3 × 20.5 × 3.5 in (440 × 520 × 88 mm)
Weight	12.3 lb (5.6KG)	12.3 lb (5.6KG)	34.2 lb (15.5KG)	34.8 lb (15.8 KG)	34.8 lb (15.8 KG)
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)
Relative Humidity	10-95%	10-95%	10-95%	10-95%	10-95%
Compliance and Certificate	CE, CB, FCC, UL/cUL, ROHS, IEC/EN61000-4-5 Power Surge Protection, ISO 9001:2015, ISO 14001:2015, CVE Compatibility, IPv6 Ready, ICSA Firewalls				

Opciones del Módulo

Especificaciones	IOC-8GE-M	IOC-8SFP-M	IOC-4GE-B-M	IOC-4XFP	IOC-8SFP+	IOC-4GE-POE
						
Name	8GE Extension Module	8SFP Extension Module	4GE Bypass Extension Module	4XFP Extension Module	8SFP+ Extension Module	4GE PoE Extension Module
I/O Ports	8 x GE	8 x SFP, SFP module not included	4 x GE Bypass (2 pair bypass ports)	4 x XFP, XFP module not included	8 x SFP+, SFP+ module not included	4 x GE with PoE
Dimension	½U (Occupies 1 generic slots)	½U (Occupies 1 generic slots)	½U(Occupies 1 generic slots)	1 U(Occupies 2 generic slots)	1 U(Occupy 2 generic slots)	1 U(Occupy 2 generic slots)
Weight	1.8 lb (0.8kg)	2.0 lb (0.9kg)	1.8 lb (0.8kg)	2.0 lb (0.9kg)	1.5 lb (0.7kg)	0.9 lb (0.4kg)

A menos que se especifique lo contrario, todo el rendimiento, la capacidad y funcionalidad se basan en StoneOS 5.5R6. Los resultados pueden variar en función del StoneOS® versión y despliegue.

NOTAS: (1) Se obtuvieron datos FW rendimiento bajo tráfico UDP de sola pila con paquetes de 1518 bytes (2) se obtuvieron los datos de rendimiento IPSec bajo Preshare configuración AES256 + SHA-1 y paquetes 1400 bytes; (3) datos de rendimiento AV se obtuvieron bajo tráfico HTTP con el archivo adjunto; (4) para IPS se obtuvieron los datos de rendimiento bajo de detección de tráfico HTTP bi-direccional con todas las normas de IPS activadas; (5) Las capacidades de trougtput es obtenido de la siguiente manera (64 byte : 512 byte : 1518 byte =5:7:1); (6) Los datos de rendimiento de NGFW se obtienen por debajo de 64 Kbytes de tráfico HTTP con control de aplicaciones e IPS habilitado; (7) 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; (8) las Nuevas Sesiones se obtuvieron en virtud de tráfico TCP.