Hillstone Networks Series-S

Sistema de Prevención de Intrusiones (NIPS)

A medida que el panorama de las amenazas sigue evolucionando de manera agresiva, un número cada vez mayor de tecnologías de protección para la red ha surgido rápidamente. Entre estas diversas tecnologías, el Sistema de Prevención de Intrusiones (IPS por su sigla en inglés) sigue siendo una de las soluciones más ampliamente desplegadas, independientemente de la plataforma o del factor de forma.

El dispositivo Hillstone IPS (NIPS) basado en redes, opera en línea, y a la velocidad de cable, realizando una inspección profunda de paquetes y haciendo un montaje de inspección a todo el tráfico de la red. También aplican reglas basadas en varias metodologías, incluyendo el análisis de anomalías de protocolo y el análisis de firmas para bloquear las amenazas. Además, el NIPS aprovecha la tecnología de inteligencia artificial para lograr protección DDoS y detección de tráfico cifrado sin descifrarlo para una protección inteligente y eficiente contra amenazas. El Hillstone NIPS se puede implementar en la red para inspeccionar el tráfico y yace sin ser detectado por soluciones perimetrales, siendo una parte integral de los sistemas de seguridad de red por su alto rendimiento, sin comprometer recursos, con la mejor capacidad de protección en su clase y sus amplios y flexibles escenarios de despliegue.

Detalles del Producto

Protección contra amenazas sin precedentes y sin comprometer el rendimiento

La plataforma Hillstone NIPS cuenta con el más completo motor de inspección de alto rendimiento, combinado con la mejor asociación de firmas de su clase, compaginando con los principales socios tecnológicos, proporcionando a los clientes la tasa de detección de amenazas más alta con el menor coste total de propiedad (TCO por su sigla en inglés). El motor Hillstone IPS tiene una tasa de bloqueo del 99,6% de las gestas estáticas y una tasa de bloqueo del 98,325% de gestas en vivo (reportadas por NSS Labs). La plataforma Hillstone NIPS proporciona un alto desempeño. NIPS combina el análisis de protocolo, reputación de amenazas y otras funcionalidades que entregan protección de amenazas desde la Capa 2 hasta la 7, incluyendo ataques ARP, Dos/DDoS, protocolos anormales, URLs maliciosas, malwares y ataques web.

Informes Granulares con Puntos de Vista Orientados a los Usuarios

Hillstone NIPS proporciona una visibilidad completa basada en protocolos, aplicaciones, usuarios y contenidos. Se pueden identificar más de 4,000 aplicaciones, incluyendo cientos de aplicaciones móviles y en la nube.

Uniendo múltiples fuentes, el sistema puede identificar la información contextual para tomar decisiones de bloqueo adecuadas. Con una función granular y robusta para informes, que ofrece visibilidad a través de diferentes puntos de vista:

- Plantillas únicas, en función de si usted es un administrador

Detalles del Producto (Continuación)

del sistema de negocios, un administrador de seguridad, CIO o ejecutivo.

- Contenidos Organizados contra Amenazas - sea un riesgo de seguridad, del sistema, amenaza de red o visualización de tráfico - con el fin de ayudarle a entender claramente el riesgo y tomar la decisión correcta.

Facilidad de Implementación y Gestión Centralizada

El despliegue y administración del Hillstone NIPS es simple, con una sobrecarga mínima. Se puede desplegar de la siguiente manera para satisfacer los requisitos de seguridad y garantizar la óptima conectividad:

- Protección activa (modo de prevención de intrusiones), monitoreo en tiempo real y bloqueo.
- Detección pasiva (modo de detección de intrusos), control en tiempo real y alertas.

El Hillstone NIPS puede ser gestionado por la Plataforma Hillstone de Gestión de Seguridad (HSM). Los administradores pueden inscribir, monitorear y actualizar centralmente los dispositivos NIPS desplegados en diferentes sucursales o ubicaciones, con una política de gestión unificada en la red para la máxima eficiencia.

Características

Prevención de Intrusiones

- Más de 12,700+ firmas, detección de anomalías de protocolo, detección basada en tasas, firmas personalizadas, actualización manual o automática de firmas, enciclopedia de amenazas integrada (1)
- Acciones IPS: Monitoreo, bloqueo, reinicio (IP de los atacantes o de la víctima, interfaz de entrada) con tiempo de caducidad
- Opción de registro de paquetes
- Selección y revisión basadas en filtros: gravedad, destino, sistema operativo, aplicación o protocolo
- Exención de IP de firmas específicas de IPS
- Modo de husmeo IDS
- Protección DoS basado 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
- Prevención de configuración predefinida
- Admite protección contra ataques de fuerza bruta, incluidos los protocolos FTP, MSRPC, POP3, SMTP, SUNRPC, telnet, VNC, RDP, SSH, SMB, LDAP, IMAP y HTTP.
- Admite la detección de contraseñas débiles para los protocolos FTP, POP3, SMTP, Telnet, IMAP y HTTP
- Admite la detección de contraseñas en texto plano HTTP
- Threat Details admite URI y decodificación de datos de ataque
- Soporta inspección de tramas MPLS
- Admite escanear y analizar datos codificados en base64
- Detectar tráfico cifrado anormal sin descifrarlo
- Admite la lista blanca de IP global

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
- Admite mapear amenazas detectadas a las tácticas de MITRE ATT&CK

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 HTTPS, spiders, spam, SSH/FTP contraseña débil y spyware
- 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

Antivirus

- Más de 13 millones de firmas de AV
- Antivirus basados en flujos: protocolos que incluyen HTTP/HTTPS, SMTP, POP3, IMAP, FTP/SFTP, SMB, admite el filtrado de virus y el bloqueo de archivos transferidos con el protocolo SMB al reanudarlo desde un punto de interrupción
- Escaneo de virus en archivos compreso
- Detección inteligente de virus para archivos PE, ELF, PDF y Microsoft Office sin escanear archivos completos

Defensa contra Ataques

- Defensa contra ataques de protocolo anormal
- Anti-DoS/DDoS, incluyendo SYN Flood, DNS Query Flood, defensa SIP Flood, etc
- Defensa contra ataques ARP
- Defensa inteligente DoS/DDoS con establecimiento de línea base basado en ML
- Defensa contra ataques para redirección del Protocolo de mensajes de control de Internet (ICMP), ARP y paquetes con formato incorrecto

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
- Soporte de lista de permitidos / bloqueados
- Alarma personalizable

Anti-Spam

- 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
- Las listas blancas permiten correos electrónicos de dominios / direcciones de correo electrónico confiables
- Las listas negras son definidas por el usuario

Cloud-Sandbox

- Carga archivos maliciosos a la nube en una sandbox para su análisis, incluyendo el tráfico cifrado HTTPS
- Protocolos de soporte que incluyen HTTP/HTTPS, POP3, IMAP, SMTP y FTP
- Tipos de archivos soportados, incluye PE, ZIP, RAR, Office, PDF, APK, JAR y SWF
- Dirección de transferencia de archivos y control de tamaño de archivo
- Proporciona un informe completo sobre el análisis del comportamiento de los archivos maliciosos
- Intercambio global de inteligencia sobre amenazas, bloqueo de amenazas en tiempo real

Características (Continuación)

Seguridad de datos
- Filtrado de contenido: los tipos de archivos incluyen doc, docx, xls, xlsx, ppt, pptx, txt; Los protocolos de archivos incluyen FTP, HTTP(S), SMTP(S), POP3(S), IMAP(S), SMB
- Soporta filtrado de archivos con más de 100 formatos de archivo
- Soporte de grabación de comportamiento de red

Botnet con prevención CyC
- Descubre intranet botnet host mediante el control de CyC conexiones y el bloque más avanzaron amenazas como botnet y ransomware
- Actualizan con regularidad las direcciones del servidor del botnet
- Prevención para CyC IP y dominios
- Apoyo a la detección de tráfico TCP, HTTP y DNS
- Listas blancas de IP y dominios
- Admite la importación manual/automática de múltiples inteligencia sobre amenazas C2 y la exportación de inteligencia sobre amenazas personalizada

Reputación de las IP
- Identifica y filtra el tráfico del riesgo IP, como host de botnet, spammers, nodos TOR, host vulnerados y ataques a fuerza bruta
- Registros, 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

Control de Aplicaciones
- Más de 4,000 aplicaciones que 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, monitoreo
- Proporcionar monitoreo multidimensional y estadísticas para las aplicaciones que se ejecutan en la nube, incluyendo la categoría de los riesgos y sus características
- Compatible con aplicaciones encriptadas

Calidad del Servicio (QoS)
- Soporte de aplicaciones cifradas
- 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

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

VSYS
- Asignación de recursos del sistema a cada VSYS
- Virtualización de CPU
- VSYS no root admite IPS, filtrado de URL, políticas, QoS, etc.
- Seguimiento y estadísticas de VSYS
- Admite la copia de seguridad de todas las configuraciones de VSYS a la vez

Proxy SSL
- Descarga SSL: descifrado del tráfico SSL
- SSL requerido / exento: tráfico SSL permitido o bloqueado según las reglas de la política sin descifrado

Análisis y Control de Tráfico Flexible
- Admite 3 modos de operación: Ruta / NAT (capa 3), Transparente (capa 2) con interfaz de bypass opcional y modo TAP (modo IDS) con integración con Firewalls de Hillstone
- Análisis y control del tráfico basado en reglas de política por zona de origen / destino, dirección IP de origen / destino, usuarios, servicio o aplicaciones

Alta Disponibilidad
- Interfaces heartbeat redundantes
- Modo activo / pasivo y de pares
- Sincronización de sesión autónoma
- Interfaz HA de gestión reservada
- Conmutación por error (failover):
  - 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

Administración Visible
- Protocolos para administración: HTTP/HTTPS, SSH, telnet, netconf, consola
- Administración Central: Administrador Hillstone de seguridad (HSM), API de servicios web
- Autenticación de dos factores: archivo de nombre de usuario/contraseña, certificados HTTPS
- 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
- Administración de dispositivos de almacenamiento: personalización del umbral y alarmas sobre el espacio almacenamiento, superposición de datos antiguos, detención de la grabación.

Registros e Informes
- Instalaciones para registros: múltiples servidores syslog y múltiples plataformas Hillstone Security Audit (HSA)
- Cifrado de registros e integridad de registros con subida de lotes HSA programados
- Registros fiables utilizando la opción TCP (RFC 3195)
- Registros de tráfico detallados: reenviados, sesiones violadas, tráfico local, paquetes inválidos
- Registros detallados de eventos: auditorías del sistema y de la actividad administrativa, enrutamiento y trabajo de la red, VPN, autenticaciones de usuario, eventos relacionados con WiFi
- Soporte para mostrar el resultado del ataque y la cuenta de usuario asociada en los registros de amenazas
- Agregación de registros: La solución admite la agregación de registros de AV y C&C
- Opción de IP y servicio de resolución de nombres de puerto
- Opción de formato para breves registros del tráfico
- Informes Granulares con Puntos de Vista Orientados a los Usuarios
  - Administración de HA/Visualización a nivel C
  - Visualización para el Dueño Sistema Empresarial
  - Visualización para el Administrador de Seguridad

Estadísticas y monitoreo
- Estadística de eventos de amenaza y monitoreo de aplicaciones y URL
- Análisis y estadísticas de tráfico en tiempo real
- Información del sistema como la sesión concurrente, CPU, memoria y temperatura
- Estadísticas y monitoreo del tráfico iQOS, monitoreo del estado de enlaces
- Apoyo a la recopilación de información de tráfico y expedición vía Netflow (v9.0)
- Servicio de inteligencia de amenazas basado en la nube
- Distribución geográfica de ataques a redes externas

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

Especificaciones del Producto

	S600-IN	S1060-IN	S1200-IN	S1560-IN	S1900-IN	S2100-IN
						
IPS Throughput [1]	1 Gbps	3 Gbps	3 Gbps	4 Gbps	3.8 Gbps	5 Gbps
Maximum Concurrent Connections, TCP (Standard/with AEL) [2]	1 Million / 2 Million	1 Million / 2 Million	1.2 Million	1 Million / 2 Million	1.2 Million	2 Million
New Connections per Second, TCP [3]	17,800	31,000	40,000	32,000	49,000	64,000
Stoneshield	N/A	N/A	N/A	Yes	N/A	N/A
Virtual Systems (Default/Max)	0/5	0/5	0/5	0/5	0/5	0/5
Storage	1T	1T	500 GB	1T	500 GB	500 GB
Form Factor	1U	1U	1U	1U	1U	1U
Management Ports	2 x USB Port, 1 x Console Port	2 x USB Port, 1 x Console Port	2 x USB port, 1 × MGT port, 1 x Console port	2 x USB Port, 1 x Console Port	2 x USB Port, 1 × MGT, 1 x Console Port	2 x USB port, 1 × MGT port, 1 x Console port
Fixed I/O Ports	4 x GE (including 2 pairs Bypass port)	4 x GE (including 2 pairs Bypass port)	2× SFP+, 8 × SFP, 8 × GE	4 x GE (including 2 pairs Bypass port)	8 x GE (including 1 pair Bypass port)	2× SFP+, 8 × SFP, 8 × GE
Available Slots for Expansion Modules	1 x Generic Slot	1 x Generic Slot	N/A	1 x Generic Slot	N/A	N/A
Expansion Module Option	IOC-S-4SFP-L-IN IOC-S-4GE-B-IN	IOC-S-4SFP-L-IN IOC-S-4GE-B-IN	N/A	IOC-S-4SFP-L-IN IOC-S-4GE-B-IN	N/A	N/A
Latency	<100 µs	<100 µs	<300µs	<100 µs	<70µs	<350 µs
Bypass Support (Default/Max.)	4/8	4/8	N/A	4/8	2/2	N/A
Power Supply	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100~240V 50/60Hz	AC 100-240 V 50/60 Hz	DC -36~ -72 V AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz
Maximum Power Consumption	1 x 60W	1 x 60W	50W 1 x AC power supply (default) 2 x AC power supply (optional)	1 x 60W	50W 1 x AC power supply (default) 2 x AC power supply (optional)	50W 1 x AC power supply (default) 2 x AC power supply (optional)
Dimension (W×D×H, mm)	16.9 × 11.8 × 1.7 in (430×300×44mm)	16.9 × 11.8 × 1.7 in (430×300×44mm)	17.3 × 12.6 × 1.7 in (440x 320x 44mm)	16.9 × 11.8 × 1.7 in (430×300×44mm)	17.1×12.6×1.7 in (436x 320x 44mm)	17.3×12.6×1.7 in (440x320x44mm)
Weight	14.3 lb (6.5 kg)	14.3 lb (6.5 kg)	17 lb (7.7 kg)	14.3 lb (6.5 kg)	14.33 lb (6.5kg)	16.9 lb (7.7kg)
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	5-85% (no dew)	5-85% (no dew)	10%~95%(no dew)	5-85% (no dew)	10%~95% (no dew)	10%~95% (no dew)

Especificaciones del Producto

	S2300-IN	S2700-IN	S3500-IN	S3900-IN	S5500-IN	S5560-IN
						
IPS Throughput [1]	9 Gbps	12 Gbps	17 Gbps	25 Gbps	45 Gbps	50 Gbps
Maximum Concurrent Connections, TCP (Standard/with AEL) [2]	3 Million	6 Million	8 Million	12 Million	24 Million	8 Million / 10 Million
New Connections per Second, TCP [3]	61,000	65,000	135,000	320,000	652,000	664,000
Stoneshield	N/A	N/A	N/A	N/A	N/A	Yes
Virtual Systems (Default/Max)	0/5	0/50	0/50	0/50	0/50	0/100
Storage	500 GB	500 GB	1T	1T	1T	1T
Form Factor	1U	1U	1U	1U	1U	2U
Management Ports	2 x USB Port, 1 × MGT port, 1 x Console Port , 1 HA port	2 x USB Port, 1 × MGT port, 1 x Console Port , 1 HA port	2 x USB Port, 1 × MGT port, 1 x Console Port , 1 HA port	2 x USB port, 1 × MGT port, 1 x Console port , 2 HA port (SFP+)	2 x USB port, 1 × MGT port, 1 x Console port , 1 HA port (SFP+)	2 × USB Port, 2 × MGT, 1 × Console Port
Fixed I/O Ports	2 × SFP+,8 × SFP, 16 × GE (including 2 pairs Bypass port)	2 × SFP+,8 × SFP, 16 x GE (including 2 pairs Bypass port)	2 × SFP+,8 × SFP,16 x GE (including 2 pairs Bypass port)	6 × SFP+, 16 × SFP, 8 × GE (including 2 pairs Bypass port)	2 × QSFP+, 16 × SFP+, 8 × GE (including 4 pairs Bypass port)	N/A
Available Slots for Expansion Modules	N/A	1 x Generic Slot	1 x Generic Slot	1 x Generic Slot	1 x Generic Slot	4 x Generic Slot
Expansion Module Option	N/A	IOC-S-4SFP+-A-IN IOC-S-2MM-BE-A-IN IOC-S-2SM-BE-A-IN IOC-S-2QSFP+-A-IN	IOC-S-4SFP+-A-IN, IOC-S-2MM-BE-A-IN, IOC-S-2SM-BE-A-IN, IOC-S-2QSFP+-A-IN	IOC-S-4SFP+-A-IN, IOC-S-2QSFP+-A-IN, IOC-S-2MM-BE-A-IN, IOC-S-2SM-BE-A-IN	IOC-S-4SFP+-A-IN, IOC-S-2QSFP+-A-IN, IOC-S-2MM-BE-A-IN, IOC-S-2SM-BE-A-IN	IOC-S-4GE-B-H-IN, IOC-S-4SFP-H-IN, IOC-S-8GE-B-H-IN, IOC-S-8SFP-H-IN, IOC-S-4SFP-B-H-IN, IOC-S-2SFP+-H-IN, IOC-S-4SFP+-H-IN, IOC-S-2SFP+-B-H-IN, IOC-S-4GE-4SFP-H-IN
Latency	<300µs	<300 µs	<300µs	<300 µs	<300 µs	<100 µs
Bypass Support (Default/Max.)	4/4	4/4	4/4	4/4	8/8	0/32
Power Supply	AC 100~240V 50/60Hz	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	AC 100-240 V 50/60 Hz
Maximum Power Consumption	100W 1 x AC power supply (default) 2 x AC power supply (optional)	100W 1 x AC power supply (default) 2 x AC power supply (optional)	100W 2 x AC power supply (default) 2 x DC power supply (optional)	280W 2 x AC power supply (default) 2 x DC power supply (optional)	320W 2 x AC power supply (default) 2 x DC power supply (optional)	350W Redundancy 1 + 1
Dimension (W×D×H, mm)	17.2 × 17.2 × 1.7 in (436x 437x 44mm)	17.1×17.2×1.7 in (436x 320x 44mm, No including expansion module)	17.1×17.2×1.7 in (436x 320x 44mm, Including power module handle)	17.1×21.3×1.7 in (436x542x44mm)	17.1×21.3×1.7 in (436x542x44mm)	16.9 × 19.7 × 3.5 in (430×500×88mm)
Weight	20.7 lb (9.4 kg)	20.9 lb (9.5kg, Including accessories and all packages)	26.0 lb (11.8kg, Including accessories and all packages)	32.6 lb (14.8kg)	32.6 lb (14.8kg)	35.3 lb (16 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)	32-104°F (0-40°C)
Relative Humidity	10%~95%(no dew)	10%~95% (no dew)	10%~95% (no dew)	10%~95% (no dew)	10%~95% (no dew)	5-85% (no dew)

Opciones del Módulo

Module	IOC-S-4SFP-L-IN	IOC-S-4GE-B-IN	IOC-S-4GE-B-H-IN	IOC-S-4GE-4SFP-H-IN	IOC-S-8GE-B-H-IN
I/O Ports	4 x SFP Ports	4 × GE Bypass Ports	4 × GE Bypass Ports	4 × GE and 4 × SFP Ports	8 × GE Bypass Ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.22 lb (0.1 kg)	0.33 lb (0.15 kg)	0.33 lb (0.15 kg)	0.55 lb (0.25 kg)	0.55 lb (0.25 kg)

Module	IOC-S-8SFP-H-IN	IOC-S-4SFP-H-IN	IOC-S-2SFP+-H-IN	IOC-S-4SFP+-H-IN	IOC-S-4SFP-B-H-IN
I/O Ports	8 × SFP Ports	4 × SFP Ports	2 × SFP+ Ports	4 × SFP+ Ports	4 × SFP Bypass Ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.55 lb (0.25 kg)	0.33 lb (0.15 kg)	0.33 lb (0.15 kg)	0.44 lb (0.2 kg)	0.88 lb (0.4 kg)

Module	IOC-S-2SFP+-B-H-IN	IOC-S-4SFP+-A-IN	IOC-S-2MM-BE-A-IN	IOC-S-2SM-BE-A-IN	IOC-S-2QSFP+-A-IN
I/O Ports	2 × SFP+ Bypass 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 (Occupies 1 generic slot)	1U	1U	1U	1U
Weight	0.88 lb (0.4 kg)	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)Los datos del throughput del IPS se obtienen bajo la detección de tráfico bidireccional HTTP con todas las reglas IPS activadas;

(2) Las Conexiones Concurrentes Máximas se obtienen bajo tráfico TCP; y se puede actualizar con Licencia Adicional Mejorada (AEL);

(3) Nuevas conexiones por segundo son obtenidas bajo tráfico TCP con todas las reglas IPS activadas.

A menos que se especifique lo contrario, todo el rendimiento, la capacidad y funcionalidad se basan en StoneOS 5.5R8. Los resultados pueden variar en función del StoneOS® versión y despliegue.

Version: EX-08.01-NIPS-V5.0-1123-SP-01