Hillstone X-Series

Data Center Firewall X25803

Front

Rear

El Firewall para Centro de Datos Hillstone X25803 es un DCFW de alto rendimiento que proporciona una protección excepcional y alta disponibilidad. Está perfectamente diseñado para satisfacer las estrictas necesidades de seguridad de grandes empresas, proveedores de servicios y sectores gubernamentales. Con su arquitectura totalmente distribuida, ofrece un alto rendimiento, conexiones concurrentes y nuevas sesiones, lo que le permite mantener su centro de datos funcionando sin problemas. Además, este producto está diseñado para soportar gran cantidad de sistemas virtuales, lo que lo hace ideal para entornos virtualizados.El firewall ofrece una amplia gama de características, incluyendo identificación de aplicaciones, prevención de intrusiones, administración de tráfico y protección avanzada contra comunicaciones de comando y control (C&C), lo que garantiza una seguridad de red completa para los centros de datos.

Aspectos destacados

Alto rendimiento y escalabilidad

A medida que el tráfico de red continúa aumentando, los firewalls del centro de datos necesitan contar con capacidades sólidas para acomodar a un gran número de usuarios y responder rápidamente a picos repentinos en el acceso, incluyendo un alto rendimiento, conexiones concurrentes y nuevas capacidades de procesamiento de sesiones. Hillstone X25803 aborda este desafío a través de su innovadora arquitectura totalmente distribuida que emplea algoritmos inteligentes de distribución de tráfico para implementar el procesamiento de alta velocidad del tráfico en módulos de servicio y entrada/ salida (SIOMs). Con un solo SIOM, puede lograr un impresionante rendimiento de 295 Gbps de firewall y soporte de hasta 60 millones de sesiones simultáneas. La escalabilidad lineal con los SIOM permite que un X25803 totalmente equipado admita un rendimiento de firewall de 880 Gbps, 5 millones de nuevas sesiones por segundo y 180 millones de sesiones simultáneas, todo ello empaquetado en un diseño de 5U que ahorra espacio. La escalabilidad también es soportada por sus extensas interfaces. Con hasta

Aspectos destacados (Continuación)

3 SIOM, el X25803 puede proporcionar hasta 12 puertos de I/O de 100 GE y 60 de 10 GE, con una gama de opciones de conectividad que incluyen 100 GE, 40 GE, 10 GE y 1 GE.

Alta Disponibilidad

Hillstone X25803 incorpora alta disponibilidad en su diseño de hardware y software. Admite esquemas de implementación redundantes en modalidad activos/pasivo y activo/activo, garantizando un negocio ininterrumpido en caso de que falle uno de los dispositivos. También proporciona HA Twin mode para hacer frente al desafío del tráfico asimétrico en centros de datos redundantes. El HA Twin mode es un modo de implementación altamente confiable basado en la copia de seguridad de dispositivos duales, con dos conjuntos de firewalls activos/pasivos en centros de datos separados conectados por un enlace de datos dedicado y un enlace de control. Los firewalls sincronizan la información de sesión y configuración, garantizando la continuidad ininterrumpida del sistema incluso en las condiciones más difíciles.

Todo el sistema adopta un diseño modular, soportando redundancia a nivel de hardware y intercambiabilidad en caliente para componentes clave como SIOMs, módulos de control de sistema (SCMs), módulos de potencia y módulos de ventilador. El Firewall del centro de datos X25803 proporciona un sistema de control dual protección redundante por mediante el soporte de 2 SCMs. También admite 2 fuentes de alimentación y 4 bandejas de ventilador redundantes para mantener una temperatura óptima de la CPU y garantizar la continuidad del sistema.

Tecnología de protección virtual líder

La tecnología de la virtualización es ubicua en centros de datos modernos pues permite la administración segmentada de diversas organizaciones, unidades de negocio, o departamentos dentro de un solo Firewall físico, garantizando la gestión independiente y la seguridad de cada sistema virtual sin interferir con los demás. El Firewall del centro de datos Hillstone X25803 admite la virtualización dividiendo un Firewall físico en 1000 sistemas virtuales, cada uno de los cuales puede asignarse dinámicamente según las necesidades de negocio, como CPU, sesiones, políticas y puertos. Cada sistema virtual se administra de forma independiente, proporcionando paneles de seguridad separados para diferentes servicios o usuarios. Este tráfico de red aislado reduce la superficie de ataque y fortalece la seguridad de la red.

Control granular de aplicaciones y seguridad integral

Hillstone X25803 Data Center Firewall ofrece identificación avanzada en profundidad y control de seguridad flexible para miles de aplicaciones de red, incluyendo cientos de aplicaciones móviles y aplicaciones P2P encriptadas a través de características de protocolo y análisis de comportamiento, y análisis de correlación. Esto mejora la visibilidad de la red y permite un mejor control y optimización del rendimiento de la red. Proporciona un conjunto completo de características de seguridad avanzadas, incluyendo prevención de intrusión, filtrado de URL, antivirus de alto rendimiento, protección de tráfico encriptado por SSL y prevención de C&C de botnet. El firewall también proporciona gestión inteligente del ancho de banda a través de iQoS, lo que permite un control granular, enrutamiento basado en políticas, balanceo de carga LLB y SLB. Estos permiten la protección contra una amplia gama de amenazas y garantizan el uso eficiente de los recursos de la red.

Análisis y detección de amenazas con IA

La creciente prevalencia de ataques avanzados, incluyendo ataques de día cero y amenazas ocultas en el tráfico encriptado, presenta un gran desafío para las organizaciones. El firewall del centro de datos Hillstone X25803 aprovecha la tecnología de IA para proporcionar detección de amenazas basada en el aprendizaje automático (ML) para el tráfico cifrado sin necesidad de descifrado, DDoS inteligente y protección DGA. La detección de amenazas basada en ML y el análisis inteligente ayudan a las organizaciones a mejorar la eficiencia y la precisión de la detección de amenazas y a defenderse mejor contra amenazas conocidas y desconocidas.

Aspectos destacados (Continuación)

Potente adaptabilidad de red

Con el crecimiento explosivo de los dispositivos móviles y servicios de nube, las infraestructuras IPv4 tradicionales están luchando por mantenerse al día. El Firewall del centro de datos Hillstone X25803 aborda este problema ofreciendo preservación IPv4 a través de Carrier Grade NAT (CGNAT) y tecnologías avanzadas de migración IPv6, como double stack, DNS64/ NAT64. Esto le permite adaptarse a su creciente base de suscriptores y demandas de red sin problemas. Además, el firewall del centro de datos X25803 proporciona capacidades VPN IPsec estándar e integra SSL VPN para ofrecer a los usuarios una solución VPN de alto rendimiento, alta capacidad y a gran escala. Su exclusiva VPN plug-and-play simplifica en gran medida la configuración y el mantenimiento, al tiempo que proporciona a los usuarios un acceso seguro cómodo y remoto. Además, el firewall del centro de datos X25803 integra de forma nativa la seguridad para las conexiones SD-WAN, haciendo cumplir las políticas de acceso granulares en todas las ubicaciones. Esto garantiza que los clientes puedan acceder a las funciones SD-WAN manteniendo el más alto nivel de protección

Seguridad ambientalmente sostenible

Hillstone X25803 ofrece un rendimiento ultra-alto mientras minimiza el consumo de energía, todo en una sola plataforma. Esto reduce el número de Firewall de red necesarios para que los clientes puedan cumplir con sus necesidades de negocio, ahorrando consumo de energía a los clientes, a la vez que contribuyen a sus objetivos de sostenibilidad. Además, adopta un diseño de ventilación frontal y trasera para mejorar la eficiencia de disipación de calor. Las bandejas del ventilador se ajustan de forma inteligente en función de la temperatura de las CPU en diferentes áreas para garantizar una disipación de calor equilibrada en todo el dispositivo

Características

Servicios de red

- Enrutamiento dinámico (OSPF, BGP con reinicio elegante, RIPv2)
- Enrutamiento estático y de políticas
- PBR
- DHCP, NTP, servidor DNS y proxy DNS
- Modo Tap - se conecta al puerto SPAN
- Modos de interfaz: sniffer, puerto agregado, loopback, VLANS (802.1Q y Trunking)
- Conmutación y enrutamiento L2/L3
- Multidifusión (PIM-SSM y PIM-SM)
- Implementación en modo transparente -virtual wire (capa 1)

Firewall

- Modos de funcionamiento: NAT/ruta, transparente (bridge) y modo mixto.
- Politicas y objetos: predefinidos, personalizados, agrupación de objetos
- Política de seguridad basada en aplicaciones, roles y geolocalización
- Gateways de nivel de aplicación y soporte de sesión: MSRCP, PPTP, RAS, RSH, SIP, FTP, TFTP, HTTP, dcerpc, dns-tcp, dns-udp, H.245 0, H.245 1, H.323, tcp full proxy
- Soporte NAT y ALG: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, Full Cone NAT (IPv4), STUN
- Configuración NAT: por directiva y tabla NAT central
- VoIP. SIP/H.323/SCCP NAT traversal, RTP pin holing
- Visión global de la gestión de políticas
- Inspección de redundancia de políticas de seguridad, grupo de políticas, reversión de configuración de políticas
- Asistente de políticas para generar políticas basadas en aplicaciones o servicios.
- Análisis de políticas y limpieza de políticas no válidas
- Política integral de DNS
- Horarios: único y recurrente
- Importación y exportación de políticas.

Prevención de intrusiones

- Detección de anomalías en el protocolo, detección basada en tasas, firmas personalizadas, actualizaciones manuales, automáticas de firmas push o pull, enciclopedia de amenazas integrada
- Acciones IPS: por defecto, supervisar, bloquear, restablecer (atacantes IP o víctima IP, interfaz de entrada) con el tiempo de caducidad
- Opción de captura de paquetes
- Selección basada en filtros: severidad, objetivo, sistema operativo, aplicación o protocolo
- Exención de direcciones IP para firmas específicas de IPS
- Modo de detección de IDS
- Protección DoS basada en IPv4 e IPv6 con ajustes de umbral contra inundaciones TCP Syn, exploración de puertos TCP/ UDP/ SCTP, barrido ICMP, inundación de sesiones TCP/ UDP/ SCIP/ ICMP (fuente/ destino)
- Bypass activo con interfaces de bypass
- Perfiles IPS predefinidos
- Admite la protección de ataques de fuerza bruta como VNC, RDP, SSH, LDAP, IMAP, SMB
- Admite la protección de ataques de escaneo de archivos sensibles

Antivirus

- Actualizaciones manuales, automáticas de firma push o pull
- Soporte para la carga de firmas MD5 en el sandbox de la nube, y agregar o eliminar manualmente en la base de datos local
- Antivirus basado en flujo: los protocolos incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP, SMB
- Escaneo de virus de archivos comprimidos

Defensa de Ataque

- Defensa contra anomalía de protocolo
- Anti-DoS/DDoS inteligente con establecimiento

Características (Continuación)

de línea de base basado en ML, incluyendo inundación SYN, inundación UDP, inundación de respuesta DNS, defensa de inundación de consultas DNS, fragmento TCP, fragmento ICMP, inundación SIP, etc.
- Defensa de ataque ARP
- Permite lista para la dirección IP de destino

URL Filtering
- Inspección de filtrado de banda basado en flujo
- Filtrado web definido manualmente basado en URL, contenido web y encabezado MIME
- Filtrado web dinámico con base de datos de categorización en tiempo real basada en la nube: más de 140 millones de URL con 64 categorías (8 de las cuales están relacionadas con la seguridad)
- Características adicionales de filtrado web:
  - Filtro Java Applet, ActiveX o cookie
  - Block HTTP Post
  - Palabras clave de búsqueda de registro
  - Conexiones cifradas de exploración exentas en ciertas categorías para la privacidad
- Anulación de perfil de filtrado web: permite al administrador asignar temporalmente diferentes perfiles al usuario/ grupo/ IP
- Filtro web categorías locales y recategorización de URLs

Cloud-Sandbox
- Subir archivos maliciosos a la nube sandbox para su análisis
- Soporta protocolos como HTTP/HTTPS, POP3, IMAP, SMTP, FTP y SMB
- Admite tipos de archivos como PE, ZIP, RAR, Office, PDF, APK, JAR, SWF y Script
- Soporta transferencia de archivos y control de tamaño de archivo
- Proporciona un informe completo de análisis de comportamiento para archivos maliciosos
- Intercambio global de información sobre amenazas, bloqueo de amenazas en tiempo real
- Admite modo de detección sin cargar archivos
- Admite configurar una lista de URL permitidas/ bloqueadas

Botnet C&C Prevención
- Descubre el host de botnet de intranet mediante el monitoreo de las conexiones de C&C y bloqueo de otras amenazas avanzadas como botnet y ransomware
- Actualiza periódicamente las direcciones del servidor de botnet
- Prevención de IP y dominio de C&C
- Admite la detección de tráfico TCP, HTTP y DNS
- Permitir y bloquear la lista basada en la dirección IP o

nombre de dominio
- Admite la detección de sumideros DNS y túneles DNS
- DGA Detección de dominios

Reputación IP
- Identifica y filtra el tráfico de IP riesgosas, 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
- Actualización periódica de la base de datos de IP por firmas de reputación

Descifrado SSL
- Identificación de aplicaciones para tráfico encriptado SSL
- Habilitación de IPS para tráfico encriptado SSL
- Habilitación de AV para tráfico encriptado SSL
- Filtro de URL para el tráfico HTTPS
- Lista blanca de tráfico encriptado SSL
- Modo de descarga de proxy SSL
- Proxy SSL compatible con la lista blanca de IP y la lista blanca predefinida
- El proxy SSL admite la reutilización de sesiones
- Admite la conexión del servidor AD/ LDAP a través del cifrado SSL
- Soporte TLS v1.2, TLS v1.3
- Permite identificación de aplicaciones, DLP, caja de arena IPS, AV para tráfico descifrado de proxy SSL de SMTPS / POP3S / IMAPS

Identificación del punto final y control de acceso
- Soporte para identificar IP del punto final, cantidad del punto final, tiempo en línea, tiempo fuera de línea y duración en línea
- Admite los principales sistemas operativos, incluidos Windows, iOS, Android, etc.
- Admite consultas basadas en IP, cantidad de terminales, política de control y estado, etc.
- Admite la identificación de la cantidad de puntos finales a los que se accede en capa 3, el registro y la interferencia en IP invadida
- Redirige la visualización de la página después de la operación de interferencia personalizada
- Admite operaciones de bloqueo en IP invadida
- Identificación de usuarios y control de tráfico para servicios de escritorio remoto de Windows Server de escritorio remoto de Windows Server

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

Control de aplicaciones
- Más de 6.000 aplicaciones que pueden filtrarse por nombre, categoría, subcategoría, tecnología y riesgo
- Cada aplicación contiene una descripción, factores de riesgo, dependencias, puertos típicos utilizados, y URL para referencia adicional
- Acciones: bloquear, restablecer sesión, monitorear, perfilado de tráfico
- Identificar y controlar las aplicaciones en la nube
- Proporcionar monitoreo multidimensional y estadísticas para aplicaciones en la nube, incluyendo categoría de riesgo y características

Calidad del servicio (QoS)
- Túneles de ancho de banda máximo/garantizado basado en IP/usuario
- Asignación de túnel basado en el dominio de seguridad, interfaz, dirección, usuario/grupo de usuarios, servidor/grupo de servidores, aplicación/grupo de aplicaciones, TOS
- Ancho de banda asignado por tiempo, prioridad o uso compartido de ancho de banda igual
- Tipo de servicio (TOS) y servicios diferenciados (DiffServ) y soporte de clase de tráfico
- Asignación prioritaria del ancho de banda restante
- Conexiones concurrentes máximas por IP
- Asignación de ancho de banda basada en la categoría URL
- Límite de ancho de banda al retrasar el acceso para el usuario o IP
- SIOM admite la función iQoS

Balanceo de carga del servidor
- Hashing ponderado, conexión menor ponderada y round-robin ponderado
- Protección de la sesión, persistencia de la sesión y seguimiento del estado de la sesión
- Comprobación del estado del servidor, supervisión de sesiones y protección de

Balanceo de carga de enlace
- Balanceo de carga de enlace bidireccional
- Balanceo de carga de enlace saliente: enrutamiento basado en políticas que incluye ECMP, tiempo, ponderado y enrutamiento ISP integrado; Detección activa y pasiva de calidad de enlaces en tiempo real y mejor selección de rutas
- Equilibrio de carga de enlace entrante compatible con SmartDNS y detección dinámica
- Conmutación automática de enlaces basada en ancho de banda, latencia, fluctuación, conectividad, aplicaciones, etc.
- Inspección del enlace con ARP, PING y DNS

VPN
- IPsec VPN
  - Modo IPsec Fase 1: modo de protección agresivo y modo main
  - Opciones de aceptación de pares: cualquier ID, ID específico, ID en el grupo de usuarios de dial-up
  - Soporta IKEv1 e IKEv2 (RFC 4306)
  - Método de autenticación: certificado y clave compartida
  - Soporte de configuración de modo IKE (como servidor o cliente)
  - DHCP over IPSEC
  - Caducidad de la clave de cifrado IKE configurable, la frecuencia de recorrido NAT mantiene activa
  - Fase 1/Fase 2 Cifrado de propuestas: DES, 3DES, AES128, AES192, AES256
  - Fase 1/Fase 2 Autenticación propuesta: MD5, SHA1, SHA256, SHA384, SHA512
  - Soporta IKEv2 Grupo DH 1,2,5,14,15,16,18,19,20,21,24
  - XAuth como modo servidor y para usuarios de acceso telefónico
  - Dead peer detection
  - Detección de repetición
  - Autokey keep-alive para la fase 2 SA
- Compatibilidad con dominios VPN IPsec: permite

Características (Continuación)

múltiples inicios de sesión VPN SSL personalizados asociados con grupos de usuarios (rutas URL, diseño)
- IPsec VPN admite la guía de configuración. Opciones de configuración: basadas en rutas o basadas en políticas
- Modos de implementación de IPSEC VPN: puerta de enlace a puerta de enlace, malla completa, eje y radio, túnel redundante, terminación de VPN en modo transparente
- IPSec VPN admite el modo DPD bajo demanda
- Compatibilidad con LLB y conmutación por error en túneles IPSec
- Soporta VXLAN
- Inicio de sesión único evita accesos concurrentes con el mismo nombre de usuario
- Limitación de usuarios concurrentes del portal SSL
- El módulo de reenvío de puertos VPN SSL cifra los datos del cliente y envía los datos al servidor de aplicaciones
- Admite clientes que ejecutan iOS, Android, Microsoft Windows, MacOS y Linux
- Comprobación de la integridad del host y comprobación del sistema operativo antes de las conexiones del túnel SSL
- Verificación de host MAC por portal
- Opción de limpieza de caché antes de finalizar la sesión VPN SSL
- Modo cliente y servidor L2TP, L2TP sobre IPSEC y GRE sobre IPSEC
- Permite ver y administrar conexiones VPN IPSEC y SSL
- PnPVPN

IPv6
- Gestión sobre IPv6, logging IPv6, HA y HA peermode, twin mode AA y AP
- IPv6 tunneling: DNS64/NAT64, IPv6 ISATAP, IPv6 GRE, IPv6 over IPv4 GRE, 6RD
- Protocolos de enrutamiento IPv6, incluyendo enrutamiento estático, enrutamiento de políticas, ISIS, RIPng, OSPFv3 y BGP4+
- IPS, identificación de aplicaciones, filtrado de URL, control de acceso, defensa de ataque ND, iQoS, SSL VPN
- Compatibilidad con IPv6 Radius
- Compatibilidad con IPv6 en los siguientes ALG: TFTP, FTP, RSH, HTTP, SIP
- Compatibilidad con IPv6 en iQoS distribuido
- Detección de seguimiento de direcciones IPv6

VSYS
- Asignación de recursos del sistema a cada VSYS
- Virtualización de CPU
- Non-root VSYS admiten firewall, IPsec VPN, SSL VPN, IPS, URL filtering, monitoreo de aplicaciones, IP reputation, AV, QoS
- Monitoreo y estadística de VSYS

High Availability
- Interfaces de latido redundantes
- Modo activo/activo y activo/pasivo
- Sincronización de sesión independiente
- Interfaz HA de gestión reservada
- Puertos duales de enlace de datos HA
- Conmutación por error:
  - Monitoreo de enlaces portuarios, locales y remotos
  - Conmutación por error con estado
  - Conmutación por error en una fracción de segundo
  - Notificación de falla
- Opciones de implementación:
  - HA con agregación de enlaces
  - Malla completa HA
  - HA geográficamente dispersa

Twin-mode HA
- Modo de alta disponibilidad entre múltiples dispositivos
- Múltiples modos de implementación de alta disponibilidad
- Configuración y sincronización de sesiones entre múltiples dispositivos
- Twin mode AP compatible con IPv6

Identidad de usuario y dispositivo
- Base de datos de usuarios locales
- Autenticación de usuario remoto: TACACS +, LDAP, Radius, Active Directory
- Inicio de sesión único: Windows AD
- Autenticación de 2 factores: soporte de terceros, servidor token integrado con mensajes físicos y SMS
- Políticas basadas en usuarios y dispositivos
- Sincronización de grupos de usuarios basada en AD y LDAP
- Soporte para 802.1X, SSO Proxy
- WebAuth: personalización de página, prevención de cracks forzados, compatibilidad con IPv6
- Autenticación basada en interfaz
- ADSSO sin agente (AD Polling)
- Uso de 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

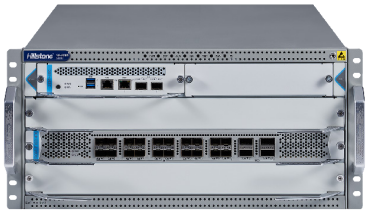
Administración
- Acceso de administración: HTTP / HTTPS, SSH, telnet, consola
- Administración central: Hillstone Security Manager (HSM), API de servicios web
- Integración de sistemas: SNMP, syslog, alianzas
- Implementación rápida: instalación automática de USB, ejecución de scripts locales y remotos
- 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 y reportes
- Instalaciones de registro: memoria local y almacenamiento (si está disponible), múltiples servidores syslog y múltiples plataformas Hillstone Security Audit (HSA)
- Cifrado de registros e integridad de registros con subida programada de lotes HSA
- Registro confiable usando 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, enruta¬miento y networking, VPN, autenticaciones de usuario, eventos relacionados con WiFi
- Opción de IP y servicio de resolución de nombres de puerto
- Opción de formato de registro de tráfico breve
- Tres informes predefinidos: Informes de Seguridad, Flujo y Redes
- Informes definidos por el usuario
- Los informes se pueden exportar en PDF, Word y HTML a través de correo electrónico y FTP

Estadísticas y monitoreo
- Estadísticas y monitoreo de eventos de amenaza, de aplicaciones y de URL
- Estadísticas y análisis de tráfico en tiempo real
- Información del sistema, como sesión concurrente, CPU, memoria y temperatura
- Estadísticas y monitoreo del tráfico iQOS, monitoreo del estado de enlaces
- Admite la recopilación de información de tráfico y expedición vía Netflow (v9.0)

Specifications

X25803-IN



FW Throughput (Maximum) [1]	880 Gbps
IPsec Throughput (Maximum) [2]	280 Gbps
NGFW Throughput [3]	320 Gbps
Threat Protection Throughput [4]	160 Gbps
Concurrent Sessions (Maximum) [5]	180 Million
New Sessions/s [6]	5 Million
IPS Throughput (Maximum) [7]	370 Gbps
SSL VPN Users (Default/Max)	128 / 20,000
Virtual Systems (Default/Max)	1/1000
Module Types	SIOM-P100-400-IN, SCM-400-IN, SCM-D1T-400-IN, SCM-D2T-400-IN
I/O Ports	Maximum 12*100GE+ 60*10GE
Management Ports	1 Console port, 1 MGT port, 2 USB 3.0 ports (single SCM-400 module)
Network Ports	2 Gigabit Ethernet optical ports(HA)(single SCM-400 module)
Expansion Module Slots	3 SIOM expansion slots, 2 System control module expansion slots
Power Consumption	1+1 redundant hot-swappable power supplies, maximum power consumption 2000W, standard power consumption 1100W
Power Supply [8]	AC 90 to 127 V / 180 to 264 V (50/60 Hz) , DC -40 to -72 V
Dimension (W × D × H)	5U, 17.3 x 26.7 x 8.6 in (440 × 680 × 220 mm)
Weight (Without Modules)	65 lb (29.5 Kg)
Compliance and Certificate	CE, CB, FCC, ROHS, IEC/EN61000-4-5 Power Surge Protection, ISO 9001:2015, ISO 14001:2015, ISO 27001:2013, CVE Compatibility, IPv6 Ready

Module Options

SIOM-P100-400-IN

Description	Service and I/O Module
Network Interface	4 QSFP28 100GE interfaces, 20 SFP+ 10GE interfaces
Slot	Occupies 1 universal expansion slot
Weight	15.34 lb (6.90Kg)

Module Options (Continuación)

	SCM-400-IN	SCM-D1T-400-IN	SCM-D2T-400-IN
			
Description	System Control Module	System Control Module	System Control Module
SSD	N/A	1 T	2 T
Slot	Occupies 1 system control module expansion slot	Occupies 1 system control module expansion slot	Occupies 1 system control module expansion slot
Weight	6.63 lb (2.90 Kg)	6.63 lb (2.90 Kg)	6.63 lb (2.90 Kg)

NOTAS:

(1) Los datos de FW Throughput se obtienen con tráfico UDP de pila única con un tamaño de paquete de 1518 bytes;

(2) Los datos de Ipsec Throughput se obtienen con la configuración Preshare Key AES256+SHA256 y un tamaño de paquete de 1400 bytes;

(3) Los datos de NGFW Throughput se obtienen con un tráfico HTTP de 64 Kbytes con control de aplicaciones e IPS habilitados;

(4) Los datos de Threat protection Throughput se obtienen con un tráfico HTTP de 64 Kbytes con el control de aplicaciones, IPS, AV y filtrado de URL habilitados;

(5) Máximo de sesiones concurrentes se obtiene bajo tráfico HTTP;

(6) Se obtienen nuevas sesiones bajo tráfico HTTP;

(7) Los datos de rendimiento de IPS se obtienen bajo la detección de tráfico HTTP bidireccional con todas las reglas de IPS activadas;

(8) Se requieren al menos 1 módulos de alimentación de AC para el funcionamiento a plena carga con alimentación AC y al menos 1 módulos de alimentación de DC para el funcionamiento a plena carga con alimentación de DC. A menos que se especifique lo contrario, todo el rendimiento, la capacidad y la funcionalidad se basan en StoneOS5.5R9. Los resultados pueden variar según la versión y la implementación de StoneOS®.

Version: EX-08.01-DCFW-X25803-5.5R9-0923-SP-01