Hillstone X-Series
Firewall para Centro de Datos

El Hillstone X7180 Data Center Firewall ofrece un rendimiento excepcional, fiabilidad y escalabilidad, para los proveedores de servicios de alta velocidad, grandes empresas y redes de operadores. Proporciona flexible seguridad de un firewall para entornos de seguridad como servicio multi-inquilino basado en la nube. La plataforma X7180 se basa en la Arquitectura de Seguridad Elástica de Hillstone (ESA), que ofrece firewalls virtuales altamente escalables, de excepcional rendimiento como firewall, sesiones concurrentes masivas y muy altas nuevas sesiones por segundo. El X7180 también es compatible con la inspección profunda de paquetes (DPI), la próxima generación de aplicaciones de control y calidad de servicio (QoS). El sistema ofrece un rendimiento excepcional en un formato pequeño con requisitos de baja potencia.

Detalles del Producto

Arquitectura de Seguridad Elástica

El streaming, aplicaciones basadas en la web, VoIP, el intercambio de archivos P2P, dispositivos móviles, computación en la nube, y la presencia internacional están contribuyendo a acelerar el tráfico de los centros de datos. A medida que crece la red básica, se incrementa el tráfico; la necesidad de interfaces de red de alta velocidad y altas densidades de puerto se vuelven factores críticos. El tráfico de los dispositivos móviles también requiere más énfasis puesto que las soluciones de seguridad de la red pueden degradar significativamente cuando el tráfico se desplaza hacia un gran número de usuarios y tamaños de paquete más pequeños. Como resultado, los servidores de seguridad de los centros de datos deben proporcionar un alto rendimiento, un gran número de sesiones concurrentes y un gran número de nuevas sesiones por segundo. Más importante aún, deben responder a los patrones de uso de sus clientes, que son a menudo altamente impredecibles. En consecuencia, los servidores de seguridad de los centros de datos también deben proporcionar elasticidad rápida y seguridad a la demanda.

El Firewall X7180 para centros de datos se basa en la arquitectura de seguridad elástica de Hillstone. Puede soportar hasta 1000 firewalls virtuales y puede ser aprovisionado como una opción completa de servicio por demanda con los Acuerdos de Servicio (SLAs). Los proveedores de servicios pueden ajustar dinámicamente la asignación de recursos (las CPU, las sesiones, las políticas y los puertos) para cada firewall virtual en respuesta al SLA. El hardware del X7180 de Hillstone se compone de múltiples láminas de seguridad y redes que proporcionan escalabilidad para el crecimiento futuro. Se aprovecha una distribución multi-core arquitectura que permite rendimiento a velocidad de cable hasta 680 Gbps, 240 millones sesiones simultáneas y 4,8 millones de nuevas sesiones por segundo. El chasis soporta hasta 68 puertos 10 GbE o 144 puertos de 1 GbE.

Confiabilidad al Estándar del Operador

El X7180 ofrece fiabilidad al estándar del operador. Es compatible con Alta Disponibilidad (HA) en ambos modos activo/pasivo y activo/activo, asegurando un funcionamiento 24x7. También cuenta con fuentes de alimentación redundantes y reemplazables en caliente, ventiladores, módulos de control del sistema (SMC), módulos de seguridad de Servicio (SSM) y Módulos I/O (IOM). El X7180 también tiene

un multi-modo y el módulo de derivación de fibra monomodo, para asegurar la continuidad del negocio durante los apagones..

IPv6 y NAT

La inevitable marcha hacia el IPv6 está en marcha, pero los proveedores de servicios todavía tienen que implementar Carrier Grade NAT (CGN) y NAT a Gran Escala (LSN) para gestionar el agotamiento de las direcciones IPv4, mientras que la transición está en marcha. El X7180 de Hillstone es compatible con una variedad de tecnologías de transición, incluyendo el Dual Stack, los túneles IPv6/IPv4, DNS64/NAT64, NAT 444, NAT de cono lleno, NAPT, etc. El registro de sesión y la traducción de direcciones permiten que las pistas de auditoría sirvan para el mantenimiento de registros y el análisis forense.

Eficiencia Energética

El X7180 tiene ranuras delanteras y traseras, lo que ahorra espacio en el rack y facilita el enfriamiento. Tiene un factor de forma de 5U y un consumo máximo de energía de 1950W, que es un 50% menos de energía que otros Firewalls para centros de datos.

Seguridad

La X7180 ofrece visibilidad y control para más de 3.000 aplicaciones incluyendo 600 aplicaciones móviles y aplicaciones P2P encriptadas. Permite el control granular de aplicaciones, ancho de banda, de usuarios y de gupos de usuarios. El X7180 evita que los usuarios accedan a aplicaciones maliciosas o inadecuadas y el Sistema de Prevención de Intrusiones (IPS) integrado protege la red de actividades maliciosas. El X7180 admite la inspección profunda de paquetes de VPN IPSec basado en estándares, que utiliza hardware basado en la aceleración criptográfica para proporcionar VPN SSL de tercera generación. Hillstone también ofrece una solución VPN Plug-and-Play única que facilita la implementación de una sucursal VPN.

QoS

La plataforma del X7180 puede manejar el ancho de banda basado en aplicaciones, usuarios y en la hora del día. El sistema proporciona un control de políticas granular incluyendo un ancho de banda garantizado, límites para el ancho de banda, prioridad de tráfico, y FlexQoS, que puede ajustar dinámicamente el ancho de banda basado en la utilización. Estas características, junto con el límite de sesión, su política de enrutamiento y balanceo de carga del enlace permiten la gestión de ancho de banda

Caracteristicas

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

Defensa contra Ataques

- Defensa contra ataques de protocolo anormal
- Anti-DoS/DDoS, incluyendo SYN Flood, defensa contra inundación de consultas tipo 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

Reputación de IP

- Bloqueo del IP del servidor Botnet con base de datos IP de reputación global

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

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

Características

- 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 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

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

HA (Twin-Mode)

- Modo de alta disponibilidad entre múltiples dispositivos
- Múltiples modos de implementación de HA
- Configuración y sincronización de sesión entre múltiples dispositivos

Identidad de Usuarios y Dispositivos

- 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)

Especificaciones del Producto

Escpecificaciones	SG-6000-X7180
FW Throughput (Maximum)[1]	680 Gbps
IPSec Throughput (Maximum)[2]	90 Gbps
IPSec Tunnel (Maximum)	20000
IMIX Throughput[3]	500 Gbps
Concurrent Sessions (Maximum)	240 Million
New Sessions/s [4]	4.8 Million
IPS Throughput (Maximum)[5]	100 Gbps
SSL VPN Users (Default/Max)	128/20000
Management I/O	1 x Console Port, 1 x AUX Port
Fixed I/O Ports	4 x GE Combo slot (1 x M GT+3 x HA)
Availalbe slots for Expansion Modules	10 x Generic Slot, 2 x System Control Modu le Slot, 1 x SD Card Slot, 2 x USB 2.0 Port
Expansion Modules	SCM-100, SSM-100, SSM-200, QSM-100, QSM-200, IOM-16SFP-100, IOM- 2MM-BE, IOM-2SM-BE, IOM-2Q8SFP+
Maximum Power Consumption	2+ 2 redundant, Max.1300W ; 3+1 redundant, Max.1950W
Power Supply	AC 100-240 V (50/60H z), DC -40 ~ -72V
Dimension (W × D × H)	5U 17.3× 23.2× 8.9 in (44 0× 590× 225 mm)
Weight	<116.6 lb (52 KG)
Temperature	32-104 F (0-40oC)
Relative Humidity	10-95%
Compliance and Certificate	CE, CB, FCC, UL/cUL, ROHS, IEC/EN61000-4-5 Proteccion de cambio de voltaje, ISO 9001:2015, ISO 14001:2015, CVE Compatibilidad, IPv6 Ready, ICSA Firewalls

Opciones del Módulo

Especificaciones	IOM-16SFP-100	IOM-2MM-BE	IOM-2SM-BE
			
Name	16SFP Module	2 Port Multi-mode Bypass Module	2 Port Single-mode Bypass Module
Fixed I/O Ports	16 x SFP, SFP module not included	Dual port multi-mode bypass fiber	Dual port multi-mode bypass fiber
Dimension	1 U (Occupies 1 generic slot)	1 U (Occupies 1 generic slot)	1 U (Occupies 1 generic slot)
Weight	2.9 lb (1.3 kg)	2.0 lb (0.9 kg)	2.0 lb (0.9 kg)

Especificaciones	IOM-2Q8SFP+	IOM-8SFP+	IOM-2Q8SFP+-200
			
Name	2xQSFP+ and 8xSFP+ Module	2xQSFP+ and 8xSFP+ Module	2xQSFP+ and 8xSFP+ Module
Fixed I/O Ports	2xQSFP+, 8xSFP+, QSFP+ and SFP+ module not included	2xQSFP+, 8xSFP+, QSFP+ and SFP+ module not included	2xQSFP+, 8xSFP+, QSFP+ and SFP+ module not included
Dimension	1U (Occupies 2 generic slots)	1U (Occupies 2 generic slots)	1U (Occupies 2 generic slots)
Weight	7.72lb (3.50kg)	7.91lb (3.59kg)	7.72lb (3.50kg)

Especificaciones	SCM-100	SSM-100	SSM-200	QSM-100	QSM-200
					
Name	Service Control Management Module	Security Service Module	Security Service Module 200	QoS Service Module	QoS Service Module 200
Dimension	1U (Occupies 1 generic slots)	1U (Occupies 1 generic slots)	1U (Occupies 2 generic slots)	1U (Occupies 1 generic slots)	1U (Occupies 2 generic slots)
Weight	2.4lb (1.1kg)	2.87lb (1.3kg)	7.72lb (3.50kg)	2.87lb (1.3kg)	7.72lb (3.50kg)

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) Las capacidades de trougtput es obtenido de la siguiente manera (68 byte : 512 byte : 1518 byte =5:7:1); (4) las Nuevas Sesiones seobtuvieron en virtud de tráfico TCP; (5) para IPS se obtuvieron los datos de rendimiento bajo de detección de tráfico HTTP bi-direccional con todas las normas de IPS activadas.

Version: EX-08.01-DCFWX7180-5.5R6-0818-SP-01