Firewall para Centros de Datos Hillstone Serie X

X10800

Front

Rear

El Firewall para Centros de Datos Hillstone X10800 ofrece un rendimiento excepcional, fiabilidad y escalabilidad, para los proveedores de servicios de alta velocidad, grandes empresas y redes de operadores. El producto se basa en una arquitectura innovadora totalmente distribuida que implementa completamente firewalls de alto rendimiento, conexiones simultáneas y nuevas sesiones. El Hillstone X10800 también es compatible con firewalls virtuales de gran capacidad, brinda servicios de seguridad flexibles para entornos virtualizados y características tales como identificación de aplicaciones, administración del tráfico, prevención de intrusiones y prevención de ataques para proteger completamente la seguridad de la red del

Product Highlights

Alto rendimiento basado en Arquitectura de Seguridad Elástica

Con el aumento explosivo del tráfico, los firewalls de los centros de datos necesitan poderosas capacidades para manejar el alto tráfico y el acceso masivo simultáneo de los usuarios, así como también la capacidad de hacer frente de manera efectiva a los repentinos estallidos de actividad de los usuarios. Por lo tanto, los firewalls del centro de datos no solo deben tener un alto rendimiento, sino también conexiones concurrentes extremadamente altas y capacidades de procesamiento de nuevas sesiones.

El Firewall para Centros de Datos de Hillstone X10800 adopta una arquitectura innovadora y totalmente distribuida para implementar el procesamiento distribuido de alta velocidad del tráfico de servicio en los Módulos de servicio (SSM) y los Módulos de interfaz (IOM) a través de algoritmos inteligentes de distribución de tráfico. Por medio de algoritmos patentados de administración de recursos, se permite el pleno potencial de las plataformas de procesadores multinúcleo distribuidos, para aumentar aún más el rendimiento de las conexiones concurrentes de los firewalls, nuevas sesiones por segundo y lograr una expansión completamente lineal del rendimiento del sistema. El Firewall para Centros de Datos X10800 puede procesar hasta 1 Tbps, hasta 10 millones de sesiones nuevas por segundo y hasta 480 millones de conexiones simultáneas. El dispositivo puede proporcionar hasta 44 interfaces 100GE, 88 interfaces 10G o 22 interfaz 40GE, 132 capacidades de expansión de interfaz 10G. Además, la demora de reenvío de paquetes es inferior a 10us, lo que puede satisfacer completamente la demanda de un centro de datos

de reenvío de servicios en tiempo real.

Confiabilidad a la Par del Proveedor

El hardware y el software del firewall del centro de datos X10800 ofrece una confiabilidad de nivel de operador del 99.999%. Puede admitir soluciones de implementación redundantes de modo activo/activo o activo/pasivo para garantizar un servicio ininterrumpido durante un solo fallo. Todo el sistema adopta un diseño modular, admite la redundancia del módulo de control redundancia del módulo de servicio, redundancia del módulo de interfaz y redundancia del módulo de conmutación, y todos los módulos son intercambiables en caliente.

El Firewall para Centros de Datos X10800 admite módulos de derivación de puerto óptico multimodo y monomodo. Cuando el dispositivo se está ejecutando en una condición especial, como apagado, el sistema se iniciará en modo de derivación para garantizar el funcionamiento ininterrumpido de la empresa. También proporciona redundancia de alimentación, redundancia de ventiladores y otros componentes clave para garantizar la fiabilidad.

El modo doble AH resuelve eficazmente el problema del tráfico asimétrico en centros de datos redundantes. El modo doble de firewall es un modo de red altamente confiable basado en copias de seguridad de dispositivos dobles. Dos conjuntos de firewalls activos/pasivos en los dos centros de datos están conectados a través de un enlace de datos dedicado y un enlace de control. Los dos conjuntos de dispositivos sincronizan información de sesión e información de configuraciones entre sí.

Líder en Tecnología de Firewalls Virtuales

La tecnología de virtualización se usa cada vez más en los centros de datos. El Firewall para Centros de Datos X10800 puede dividir lógicamente un firewall físico en más de 1000 firewalls virtuales para las necesidades de virtualización del centro de datos, proporcionando capacidades de soporte de firewall virtual para grandes centros de datos. Al mismo tiempo, los usuarios pueden establecer recursos dinámicamente para cada firewall virtual en función de las condiciones reales del negocio, como las CPU, sesiones, número de políticas, puertos, etc., para garantizar cambios flexibles en el tráfico del servicio en un entorno virtualizado. Cada sistema de firewalls virtuales del Firewall para Centros de Datos X10800 no solo tiene recursos de sistema independientes, sino que también se puede gestionar de forma individual y granular para proporcionar planos de gestión de seguridad independientes para diferentes servicios o usuarios.

Control granular de aplicaciones y seguridad integral

El Firewall para Centros de Datos X10800 utiliza una avanzada tecnología de identificación de aplicaciones para identificar con precisión miles de aplicaciones de red basadas en funciones de protocolo, características de comportamiento y análisis de correlación, que incluyen cientos de aplicaciones móviles y aplicaciones P2P cifradas. Proporciona controles de seguridad de aplicaciones sofisticados y flexibles.

El Firewall para Centros de Datos X10800 proporciona tecnología de prevención de intrusiones basada en la identificación profunda de aplicaciones, detección de protocolos y análisis de principios de ataque. Puede detectar amenazas tales como troyanos, gusanos, spyware, ataques de vulnerabilidad y ataques de escape, y proporcionar a los usuarios la seguridad de la red L2-L7. Entre ellos, la función de protección web puede cumplir los requisitos de protección de seguridad profunda del servidor web; La función de filtrado de botnet protege a los hosts internos contra infecciones

El Firewall para Centros de Datos X10800 admite el filtrado por URL para decenas de millones de bibliotecas de firmas URL. Ayuda a los administradores a implementar fácilmente el control de acceso a la navegación web y evitar la infiltración de amenazas de URL maliciosas.

La administración inteligente del ancho de banda del Firewall para Centros de Datos X10800 se basa en la identificación profunda de la aplicación y la identificación del usuario. Combinado con las prioridades de la aplicación de servicio, el Firewall para Centros de Datos X10800 puede implementar control de tráfico detallado, de dos capas y ocho niveles basado en políticas y proporciona funciones de QoS elásticas. Utilizado con funciones tales como restricciones de sesión, políticas, enrutamiento, equilibrio de carga de enlace y equilibrio de carga de servidor, proporciona a los usuarios soluciones de gestión de tráfico más flexibles.

Fuerte adaptabilidad de red

El Firewall para Centros de Datos X10800 es totalmente compatible con las tecnologías de implementación de Internet de próxima generación (incluidas las de doble pila, túnel, DNS64/NAT64 y otras tecnologías en transición). También tiene capacidades maduras NAT444 para admitir el mapeo estático para bloqueo de puerto fijo de direcciones de red externas a direcciones de intranet. Puede generar registros basados en la sesión y el usuario para facilitar la trazabilidad. Funciones NAT mejoradas (NAT de cono completo, multiplexación de puertos, etc.) cumple completamente los requisitos de las redes ISP actuales y reduce el costo de la construcción de redes de usuario.

El Firewall para Centros de Datos X10800 brinda total compatibilidad con las capacidades VPN IPSec estándar e integra la VPN SSL de tercera generación para brindar a los usuarios una solución VPN de

Características

Servicios de red

- Enrutamiento dinámico (OSPF, BGP, RIPv2)
- Enrutamiento estático y por políticas
- Rutas controladas por la aplicación
- DHCP, NTP, Servidor DNS y proxy DNS incorporados
- Modo Tap - se conecta al puerto SPAN
- Modos de interface: sniffer, puerto agregado, loopback, VLAN (802.1Q y Trunking)
- Conmutación y enrutamiento de L2/L3
- Cable virtual (Capa 1) despliegue transparente en línea

Firewall

- Modos de funcionamiento: NAT/ruta, transparente (puente) 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
- Puertas de enlace 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
- Compatibilidad con NAT y ALG: NAT46, NAT64, NAT444, SNAT, DNAT, PAT, NAT de cono completo, 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, actualizaciones de firmas automáticas manuales o automáticas, 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 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 las 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 del 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 ancho de banda según categoría de URL
- Límite de ancho de banda al demorar el acceso por usuario o IP

Equilibrio de Cargas en el Servidor

- Hash ponderada, menor conexión ponderada y round-robin ponderadas
  Planificación Round-Robin
- 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 Cargas

- Equilibrio de carga de enlaces bidireccionales
- 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 automático de enlace basado en ancho de banda, latencia, fluctuación de fase, conectividad, aplicación, etc.
- Inspección del enlace con ARP, PING, y DNS

VPN

- 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
- Encriptación de propuesta Fase 1 / Fase 2: DES, 3DES, AES128, AES192, AES256
- Autenticación de propuesta 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
- 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, 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 fall
- Opciones de Implementación:
  - HA con agregación de enlaces
  - HA con malla completa
  - HA geográficamente dispersa

HA en modo doble

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

Identidad de Usuario y Dispositivo

- Base de datos de usuario local
- Autenticación remota de usuarios: TACACS +, LDAP, Radius, Active
- Single-sign-on (autenticación única): Windows AD
- Autenticación de 2 factores: soporte de terceros, servidor token integrado con mensajes físicos 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 WebAuth
- Autenticación basada en interfaz
- ADSSO sin agente (Encuesta 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: Hillstone Security Manager (HSM), API de servicios web
- Integración del sistema: SNMP, syslog, alianzas de sociedades
- 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

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 networking, 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, Flujo y Redes
- Generación de informes definidos por el usuario
- Los informes se pueden exportar en formato PDF, por correo electrónico y por 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

Especificaciones	SG-6000-X10800
	
Rendimiento de FW (máximo)	1 Tbps
Rendimiento de IPSec (máximo)	300 Gbps
Sesiones Concurrentes (máximo)	480 Millones
Nuevas Sesiones	10 Millones
Rendimiento IPS (máximo)	400 Gbps
Módulos de Expansión	SSM-300, QSM-300, IOM-P40-300, IOM-P100-300, SWM-300, SCM-300
Maximum Interfaces	Maximum 11×2 40GE+11×12 10GE Or Maximum 11×4 100GE+11×8 10GE
Maximum Power Consumption	4400W, N+M(1), redundant hot swap power supply
Fuente de alimentación	AC 100-240 V (50/60H z), DC -40 ~ -72V
Interfaces de Administración	1 puerto de consola, 1 puerto AUX, 1 administración de MGT, 1 puerto USB 2.0
Interfaces de Red	2 interfaces ópticas de Gigabit (2 interfaces HA, módulo SCM-300 único)
Módulos de Expansión	12 ranuras de expansión universales, 2 ranuras de expansión del módulo de control del sistema, 2 ranuras de expansión del módulo de conmutación
Dimensiones (An × La × Al)	18U 17.3× 31.4× 25 in (440× 797× 635 mm)
Peso	253 lb (114.75 KG)
Cumplimiento y Certificados	Protección contra sobretensión de potencia CE, CB, FCC, UL/cUL, ROHS, IE /EN61000-4-5, ISO 9001:2015, ISO 14001:2015, Compatibilidad CVE, preparado para IPv6, firewalls ICSA

Opciones de Módulo

Nombre	IOM-P40-300	IOM-P100-300	SSM-300
			
Descripción	40GE, 10GE módulo interface	100GE, 10GE módulo interface	Módulo de Servicio de Seguridad
Interfaz de red	2 interfaces QSFP+ 40GE, 12 SFP+ 10Gb, no módulos QSFP+ and SFP+	4 interfaces QSFP28 100GE, 8 interfaces SFP+ 10Gb, no módulos QSFP28 and SFP+	N/A
Ranura	Ocupa 1 ranura de expansión universal	Ocupa 1 ranura de expansión universal	Ocupa 1 ranura de expansión universal
Peso	12.45 lb (5.65 kg)	12.67 lb (5.75 kg)	12.56 lb (5.70 kg)

Nombre	SCM-300	SWM-300	QSM-300
			
Descripción	Módulo de gestión de control de servicios	Módulo de conmutación	Módulo de servicio QoS
Ranura	Ocupa 1 ranura de expansión universal	Ocupa 1 ranura de expansión universal	Ocupa 1 ranura de expansión universal
Peso	7.6 lb (3.45 kg)	7.05 lb (3.20 kg)	12.56 lb (5.70 kg)

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.

NOTA: (1) Se requieren al menos 3 módulos de alimentación de CA para la operación de carga completa con alimentación de CA, y se requieren al menos 4 módulos de alimentación de CC para la operación a plena carga con alimentación de CC.

Versión: EX-08.01-DCFWX10800-5.5R6-0818-SP-01