Hillstone Networks Serie-S
Sistema de Prevención de Intrusiones (NIPS)

S600 / S1060 / S1560 / S2160 / S2660

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. 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 3000 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

Highlight

informes, que ofrece visibilidad a través de diferentes puntos de vista:

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

Prevención de Intrusiones

- Más de 8,000 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 basada 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.

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

Cloud-Sandbox

- Carga archivos maliciosos a la nube en una sandbox para su análisis, incluyendo el tráfico cifrado HTTPS
- Proporciona un informe completo sobre el análisis del comportamiento de los archivos maliciosos

Anti-Virus

- Más de 13 millones de firmas de AV
- Antivirus basados en flujos: protocolos que incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP
- Escaneo de virus en archivos compreso

Filtrado de URLs

- Inspección de filtrado web basado en el flujo
- 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 las cuales están relacionadas con la seguridad)
- 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 de calificación
- Proxy para prevención de evasión: bloqueo de categorías de sitios proxy, califica tipos de direcciones URL por dominio y por dirección IP, bloquea el redireccionamiento desde el caché y a sitios de traslado, bloquea aplicaciones que evaden los proxy, bloquea comportamiento como servidores proxy (IPS)

Control de Aplicaciones

- Más de 3.000 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

Alta Disponibilidad

- Interfaces heartbeat redundantes
- Activa/Activa y Activa/Pasiva
- 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

- Acceso administrativo: HTTP/HTTPS, SSH, Telnet, 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: memoria y almacenamiento locales, múltiples servidores syslog y varias plataformas Hillstone para Auditoría de Seguridad (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
- 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

Especificaciones del Producto

Módulo	S600	S1060	S1560	S2160	S2660
					
IPS throughput[1]	1 Gbps	2 Gbps	4 Gbps	10 Gbps	14 Gbps
Maximum Concurrent Connections (TCP)[2]	1 M / 2 M	1 M / 2 M	1 M / 2 M	2 M / 4 M	2 M / 4 M
New connections per second (TCP)[3]	9,000	35,000	41,000	92,000	120,000
Stoneshield	N/A	N/A	Yes	N/A	Yes
Storage	1T	1T	1T	1T	1T
Form factor	1 U	1 U	1 U	1 U	1 U
Management Ports	2×USB Port, 1× Consle Port	2×USB Port, 1× Consle Port	2×USB Port, 1× Consle Port	2×USB Port 2×MGT, 1× Consle Port	2×USB Port 2×MGT, 1× Consle Port
Fixed I/O Ports	4×GE	4×GE	4×GE	4×GE	4×GE
Available Slots for Extension Modules	1×Generic Slot	1×Generic Slot	1×Generic Slot	2×Generic Slot	2×Generic Slot
Expansion Module Option	IOC-S-4GE-B-L, IOC-S-4SFP-L	IOC-S-4GE-B-L, IOC-S-4SFP-L	IOC-S-4GE-B-L, IOC-S-4SFP-L	IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-4SFP-B IOC-S-2SFP+, IOC-S-2SFP+-B IOC-S-4SFP+, IOC-S-4SFP+-B	IOC-S-4GE-B, IOC-S-4SFP, IOC-S-8GE-B, IOC-S-8SFP, IOC-S-4GE-4SFP, IOC-S-4SFP-B IOC-S-2SFP+, IOC-S-2SFP+-B IOC-S-4SFP+, IOC-S-4SFP+-B
Bypass Support (Default/ Max.)	4/8	4/8	4/8	4/20	4/20
Power Supply	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz	AC 100-240V 50/60Hz
Maximum Power Consumption	1×60W	1×60W	1×60W	250W Redundancy 1 + 1	250W Redundancy 1 + 1
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)	16.9×11.8×1.7 in (430× 300×44mm)	16.9×14.8×1.7 in (430×375×44mm)	16.9×14.8×1.7 in (430×375×44mm)
Weight	14.3 lb (6.5kg)	14.3 lb (6.5kg)	14.3 lb (6.5kg)	22.0 lb (10kg)	22.0 lb (10kg)
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	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)	5-85% (no dew)

Opciones del Módulo

Módulo	IOC-S-4GE-B-L	IOC-S-4SFP-L	IOC-S-4GE-B	IOC-S-4SFP
I/O Ports	4×GE Bypass Ports	4×SFP Ports	4×GE Bypass Ports	4×SFP Ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.22 lb (0.1kg)	0.22 lb (0.1kg)	0.33 lb (0.15kg)	0.33 lb (0.15kg)

Módulo	IOC-S-8GE-B	IOC-S-8SFP	IOC-S-4GE-4SFP	IOC-S-2SFP+
I/O Ports	8×GE Bypass Ports	8×SFP Ports	4×GE and 4×SFP Ports	2×SFP+ Ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.55 lb (0.25kg)	0.55 lb (0.25kg)	0.55 lb (0.25kg)	0.33 lb (0.15kg)

Módulo	IOC-S-4SFP+	IOC-S-4SFP-B	IOC-S-2SFP+-B	IOC-S-4SFP+-B
I/O Ports	4×SFP+ Ports	4 x SFP Bypass ports	2 x SFP+ Bypass ports	4 x SFP+ Bypass ports
Dimension	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)	1U (Occupies 1 generic slot)
Weight	0.44 lb (0.2kg)	0.88lb (0.4Kg)	0.88lb (0.4Kg)	0.88lb (0.4Kg)

A menos que se especifique lo contrario, todo el rendimiento, la capacidad y funcionalidad se basan en StoneOS 5.5R3. Los resultados pueden variar en función del StoneOS®versión y despliegue.

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; (3) Las nuevas sesiones se obtienen bajo el tráfico TCP.

Version: EX-08.01-NIPS-V2.1-0717-SP-01