Hillstone W-Series

Firewall para Aplicaciones Web

El firewall para aplicaciones web (WAF) de la serie W de Hillstone proporciona seguridad integral de clase empresarial para servidores web, aplicaciones y APIs. Defiende contra ataques tanto en la red como en la capa de aplicación, brindando protección contra DDoS, las 10 principales amenazas de OWASP y ataques de bots, por ejemplo. Además, el WAF valida las API con el esquema definido en OpenAPI y genera automáticamente políticas de modelo de seguridad positivas para detectar y defender contra ataques y uso indebido.

Hillstone WAF combina la detección tradicional basada en reglas con un innovador análisis semántico. Este enfoque de motor dual aumenta significativamente la precisión al tiempo que minimiza los falsos positivos. Hillstone WAF también aprovecha la tecnología de aprendizaje automático para ajustar las políticas de seguridad y bloquear amenazas y ataques desconocidos. Además, los registros se pueden agregar automáticamente en múltiples dimensiones para permitir a los administradores identificar fácilmente anomalías sospechosas o localizar falsos positivos, y luego afinar aún más las políticas según sea necesario.

Detalles del Producto

Seguridad Integral para Aplicaciones Web

El firewall para aplicaciones web (WAF) de Hillstone proporciona seguridad completa para las aplicaciones basadas en la web y las API para empresas y otras organizaciones. Detecta y defiende contra ataques tanto en la capa de red (como ataques DDoS, ataques de inundación, escaneo y suplantación de identidad, etc.) como en la capa de aplicación (como los 10 principales riesgos de OWASP, incluidos ataques de inyección, ataques de secuencias de comandos entre sitios (XSS), etc.). Hillstone WAF detecta automáticamente los servidores web y los activos relacionados y los protege. Con esta capacidad, Hillstone WAF cubre todo el espacio web incluso cuando se escala, lo que ayuda a mejorar la eficiencia operativa y ofrece un tiempo de generación de valor más rápido.

Protección API Avanzada

A medida que la transformación digital continúa evolucionando, las API juegan un papel cada vez más importante en el desarrollo y la integración de aplicaciones. La popularidad de las API expone potencialmente superficies de ataque adicionales, como exposición excesiva de datos, falta de recursos y limitación de velocidad, ataques de inyección y XSS entre llamadas a API, etc. Basado en el esquema definido en los archivos de OpenAPI, Hillstone WAF ayuda a validar y generar políticas de modelo de seguridad positivas para detectar esas amenazas en las API.

Detalles del Producto (Continuación)

Precisión y eficiencia de detección mejoradas con motores duales

Hillstone WAF integra el análisis semántico más innovador de la industria con motores de detección WAF tradicionales. Combinado con la detección tradicional basada en reglas, el motor de análisis semántico ayuda a detectar más amenazas como la inyección SQL y la secuencia de comandos entre sitios, y minimiza los falsos positivos. La capacidad de decodificación recursiva de Hillstone WAF también detecta ataques que están oscurecidos por múltiples codificaciones. Este enfoque de motor dual mejora significativamente la precisión de detección y su eficiencia en la operación.

Optimización de reglas de seguridad impulsada por aprendizaje automático y defensa contra ataques desconocidos

Además de la protección general basada en reglas y scripts para ataques conocidos, la capacidad de autoaprendizaje de Hillstone WAF ayuda a mitigar vulnerabilidades nunca antes vistas para proteger aplicaciones específicas de ataques de día cero. Su modelo basado en ML (Machine Learning) aprende de los datos del tráfico normal, como la longitud de los parámetros, las cookies, los métodos HTTP, etc., se ajusta a sí mismo en función de los resultados de las pruebas, así como de las aportaciones de los administradores, y continúa actualizando los modelos de aprendizaje y optimizando las reglas WAF a medida que evolucionan las aplicaciones. Reduce significativamente la sobrecarga operativa al eliminar la resolución de problemas de falsos positivos y el ajuste manual de políticas.

Registros enriquecidos para análisis e informes inteligentes

Hillstone WAF proporciona a los administradores y operadores alta visibilidad e informes completos con análisis de amenazas, análisis de tráfico, desglose de ataques y control de amenazas. Su capacidad para agregar registros permite que los registros se agreguen desde múltiples dimensiones, lo que ayuda a los operadores a identificar fácilmente anomalías sospechosas o encontrar falsos positivos en los registros, y luego ajustar las políticas en consecuencia.

Características

Protección de Aplicaciones Web

- Defensa contra anomalías HTTP
- Proxy transparente SSL
- Soporte para la detección de la integridad de la cadena de certificados en sitios HTTPS
- Defensa contra ataques de inundación rápida HTTP y de inundación lenta
- Defensa contra ataques de inyección, incluida la inyección SQL, inyección LDAP, inyección SSI, inyección Xpath, inyección de comandos, inyección de archivos incluyendo los remotos (RFI), etc.
- Defensa contra los ataques entre sitios, incluidos los ataques XSS y CSRF
- Detección basada en análisis semántico de inyección SQL y ataques XSS
- Prevención de fuga de datos, incluida fuga de errores del servidor, errores en la base de datos, contenido del directorio web, código, palabra clave, etc.
- Evita la fuga de datos personales sensibles. Admite la detección de fugas de identificación personal, número de tarjeta bancaria, tarjeta de crédito y cuenta de correo electrónico. Admite la desensibilización de información confidencial (reemplazada con caracteres especificados)
- Seguridad de las cookies. Apoya en la prevención de manipulación y secuestro de cookies; admite la firma y cifrado de cookies
- Capacidad de control de acceso web, que puede defender el comportamiento de escaneo, rastreo y recorrido de directorios
- Admite un control detallado del acceso HTTP basado en la IP del cliente, al hacer coincidir el método HTTP, el encabezado HTTP, el tipo de contenido HTTP, la versión del protocolo HTTP, la ruta URI, etc.
- Apoya la defensa contra ataques de vulnerabilidad a servidores web, marco web y aplicaciones web
- Defensa contra el acceso ilegal a recursos, incluidas las cargas y descargas ilegales y los ataques de hotlinking; admite el control de descargas ilegales según el tamaño del archivo y el tipo de archivo MIME
- Defensa contra malware, incluidos los ataques WebShell y troyanos, etc.
- Defensa contra ataques de fuerza bruta
- Soporte para detectar y bloquear clientes por su dirección IP de origen (a través de X-forward-for y TCP) cuando se implementa detrás de un balanceador de carga o un proxy
- Admite reglas personalizadas
- Admite plantillas de políticas de protección predefinidas, políticas de protección personalizadas
- Actualización en tiempo real de las bases de datos de las firmas
- Soporte de detección y protección de seguridad API; validación de soporte basada en documentos de especificaciones de OpenAPI
- La solución admite la detección avanzada de tráfico anti-crawler y bot basada en la huella digital del dispositivo, la verificación CAPTCHA para tráfico sospechoso y el bloqueo del tráfico basado en la huella digital del dispositivo
- Soporte para configurar el estado del sitio como "mantenimiento" o "redirección"
- Soporte de operación por lotes de la configuración del sitio

Anti-defacement

- Admite dos modos de funcionamiento: modo de aprendizaje y modo de protección
- Comparación de similitudes de contenidos protegidos
- Admite tipos de páginas web estáticas protegidas personalizadas; admite una lista de URLs de excepción para resistencia a la manipulación;

Características (Continuación)

soporta la duración y ajuste de tiempo para protección.
- Admite la sincronización con servidores y establece una línea base mediante el motor integrado de sincronización.
- Soporte de monitoreo de manipulación y modificación normal.
- Soporte forense de manipulación
- Soporte para desconexión de red con un solo clic para bloquear el acceso al sitio web cuando se detecta manipulación

Protección de Seguridad de Red
- Admite parches virtuales basados en resultados de análisis de vulnerabilidades o informes importados
- Defensa contra ataques DoS, que incluyen: ataques Ping of Death, ataque Teardrop, ataque de fragmentación de IP, ataque Smurf y Fraggle, Land attack, ataque de paquetes grandes ICMP, etc.
- Defensa contra ataques de inundación de consultas de DNS, admite la configuración del nivel de alerta de acuerdo con la dirección de origen y destino
- Protección contra anomalías de TCP
- Protección contra escaneo / suplantación de IP y escaneo de puertos
- Protección contra inundaciones, incluyendo: inundación ICMP, inundación UDP, inundación SYN, etc.
- Soporte de IP Reputation y bloqueo de IP maliciosas
- Soporte de control de políticas basado en el encabezado HTTP, que incluye: host, user-agent, accept, accept-language, accept-encoding, referer, cookie, etc.
- Soporte para HTTP2 en modos transparente, de tracción, one arm y de proxy inverso
- Admite descifrado HTTPS y detección de tráfico IPv6 en modo TAP
- Política de control de acceso con programación horaria

IPv6
- Optimización de políticas de control de acceso
- Admite dual stack (IPv4 e IPv6). Las direcciones IPv4 e IPv6 se pueden agregar como sitios protegidos simultáneamente

Aprendizaje Automático de Políticas
- Soporte para la detección y protección del tráfico IPv4/IPv6
- Aprendizaje inteligente del tráfico al sitio protegido y ajuste de las políticas en función de los resultados del aprendizaje.
- Contenido aprendido que incluye: dirección URL dinámica, parámetro de URL, método de acceso HTTP, cookies e información adcional
- Admite el modo de aprendizaje y modo de protección; admite el cambio automático al modo de protección después de aprender
- Soporte para eximir URL específicas del aprendizaje automático

Defense Response
- Soporta el aprendizaje de URL específica
- Admite alarmas solo si se ejecuta un comportamiento de activación
- Soporte para bloquear el comportamiento que rompa las reglas de seguridad y responder con una página de alerta.
- Admite la personalización de la página de alerta
- Soporte para redirigir la página de alerta a otra URL.
- Soporte para agregar una lista blanca (regla de excepción) a través de registros de seguridad, y soporte para reglas de excepción basadas en URL, dirección IP de origen, encabezado HTTP, parámetro de línea de solicitud y cuerpo de la solicitud, con reglas de excepción tanto a nivel global como específicas del sitio
- Admite agregar atacantes a la lista negra para bloquear su posterior acceso
- Admite lista blanca de direcciones IP y URL
- Apoya la interacción con el firewall para emitir listas negras.
- Soporte de control de acceso basado en GeoIP

Despliegue
- Admite múltiples modos de implementación, incluido el modo proxy transparente, el modo TAP, el modo proxy inverso, el modo proxy inverso one-arm y el modo de tracción
- Soporte para el modo de inspección transparente sin necesidad de cambios en la configuración de red, y soporte para verificación de seguridad en el tráfico MPLS
- Autodescubrimiento de activos web
- Soporte de sitio predeterminado
- Admite la configuración de IP sin interfaz para el sitio y la respuesta ARP en modo proxy inverso one-arm y modo proxy inverso
- Admite asistente de implementación gráfica

Oferta Virtualizada
- Hipervisores compatibles: VMware, KVM, Openstack y Xen
- Admite agente integrado, como VMware Tools y Cloud-init
- Soporte para AWS, Azure, AliCloud, Huawei Cloud, Tinayi Cloud, Tencent Cloud
- Permite la implementación de alta disponibilidad en un entorno de nube pública (AliCloud, AWS)
- Soporta la gestión de licencias a través del sistema LMS
- Soporta Restful API
- Admite NIC intercambiable en caliente, SR-IOV y escalado elástico

Alta Disponibilidad
- Modo activo / pasivo
- Modo activo / activo
- Admite Bypass de software (en modo proxy transparente)
- Soporte para el bypass en varias etapas
- Soporte para el bypass de tiempo de detección del motor
- Soporte para la protección de sobrecarga basada en el bypass de hardware en los modos de proxy transparente e inspección transparente
- Soporte para el bypass de software en caso de falla en los modos transparente, inverso, one arm y de tracción

Aceleración de aplicaciones y balanceo de carga de servidor (SLB)
- Admite caché web, compresión de páginas y multiplexación TCP, descarga SSL, proxy SSL
- Admite aceleración de hardware SSL
- Admite el balanceo de carga de servidor (en modo proxy inverso), incluyendo los métodos: weighted round-robin, least connection e IP Hash algorithm
- Compatibilidad con el balanceo de carga de servidor (SLB) en IPv6
- Soporte de verificación de estado del servidor. Admite la personalización del objeto URL utilizado para la verificación de estado
- Admite el uso de X-header como IP de balanceo de carga
- Soporte para el almacenamiento en caché de respuestas HTTP GET, HEAD, POST y PUT

Configuración de red e interfaz
- Admite enrutamiento estático
- Permite agregar interfaces
- Soporta subinterfaz VLAN
- Admite múltiples conmutadores virtuales, cables virtuales
- Soporte LLDP

Autenticación
- Autorización de varios niveles, roles predefinidos que incluyen administradores del sistema, operadores, auditores, etc.
- Permite autenticación local, Radius y TACAS-C +

Gestión de Dispositivos
- Múltiples métodos de administración que incluyen: HTTP, HTTPS, SSH, consola, etc. Admite la configuración de un host de administración confiable
- Permite la supervisión del estado del dispositivo, que incluye: información resumida y detallada del disco duro, el almacenamiento, la utilización del CPU y la temperatura
- Admite la gestión centralizada y la actualización del firmware a través del sistema de gestión de seguridad de Hillstone (HSM)
- Soporte para herramientas de operación y mantenimiento como ping/tcpdump/curl/dpdump

Registro, Informe y Alarma
- Amplia información de registro, incluidos registros de administración de dispositivos, registros de seguridad de la red, registros de seguridad web, registros a prueba de manipulaciones, registros de control de acceso, registros de estrategias de autoaprendizaje, registros de acceso web, etc.
- Admite el registro de todos los encabezados HTTP en eventos de ataque, incluidos los de URL, UserAgent, contenido POST, cookies, etc.
- Admite alarmas por correo electrónico, SNMP, SYSLOG, SMS, etc.
- Admite la creación de reportes (plantillas de informe compatibles) de múltiples dimensiones, como descripción general de riesgos de seguridad, detalles de riesgo del sitio, detalles del tipo de ataque, análisis de manipulación del sitio, visitas al sitio, resumen del ataque a la capa de red, estado de operación del sistema, cumplimiento de PCI DSS, etc.
- Permite agregar registros según la política o la IP del cliente
- Soporta el análisis de registros inteligente, incluido el análisis de amenazas y el análisis de falsos positivos, y optimización de la política de seguridad basada en los resultados del análisis.
- Admite la reproducción de ataques, lo que puede ayudar a los administradores a analizar y localizar rápidamente las amenazas y los ataques en la red
- El registro de seguridad web admite el registro de tráfico de ataque no web, con acciones de protección codificadas por colores para facilitar la

identificación
- Soporta la investigación manual de alertas sospechosas e informe de falsos positivos a CloudView
- Soporte para borrar el registro de seguridad web
- Permite la transferencia de registros a través de FTP
- Soporta informes definidos por el usuario
- Soporte para informes exportados en formato PDF, DOC, HTML
- Apoya la exportación periódica de informes
- El servidor de correo admite la transmisión encriptada STARTTLS y SSL
- Admite el seguimiento de la sesión del usuario para agregar el nombre de usuario, el identificador de la sesión y el valor de la identidad de la sesión en los registros
- Soporte para el envío de informes a través de FTP y correo electrónico
- Admite la detección de contraseñas débiles

Dashboard:
- Admite la visualización a pantalla completa de información estadística y detallada de amenazas y riesgos
- Soporte para mostrar los principales eventos de amenazas y mostrar últimos eventos de amenazas
- Soporte para mostrar amenazas del sitio por gravedad
- Soporte para mostrar el número total de sitios y sitios de riesgo

Especificaciones del Producto

	W120S-IN	W320S-IN	W620S-IN	W1120S-IN
				
HTTP Throughput	600 Mbps	1 Gbps	1.5 Gbps	3.5Gbps
HTTP New Sessions	1,600	3,500	5,000	8,000
HTTP Maximum Transactions Per Second (TPS)	2400	5,500	7,000	10,000
Storage	480G SSD	480G SSD	480G SSD	480G SSD
RAM	4G	4G	8G	16G
Management Ports	2 x USB Ports, 1 x MGT Port, 1 x Console Port	2 x USB Ports, 1 x MGT Port, 1 x Console Port	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port (SPF)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port (SPF)
Fixed I/O Ports	8 x GE (including 1 bypass pair)	8 x GE (including 1 bypass pair)	2 x SFP+, 8 x SFP, 16 x GE (including 2 bypass pairs)	2 x SFP+, 8 x SFP, 16 x GE (including 2 bypass pairs)
Available Slots for Expansion Modules	N/A	N/A	N/A	1
Expansion Module Option	N/A	N/A	N/A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A
Protected Sites	8	16	32	64
Protected IP/PORT Pairs	64	64	128	512
Power Specification	50W, Single AC (default), Dual AC (optional)	50W, Single AC (default), Dual AC (optional)	100W, Single AC (default), Dual AC (optional)	100W, Dual AC
Power Supply	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz
Form Factor	1U	1U	1U	1U
Dimension(WxDxH)	17.1×12.6×1.7 in (436.0*320.0*44.0mm)	17.1×12.6×1.7 in (436.0*320.0*44.0mm)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)
Weight	14.3 lb (6.5 kg)	14.3 lb (6.5 kg)	20.7 lb (9.4 kg)	26 lb (11.8 kg)
Operating 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)
Relative Humidity	10%-95% non-condensing	10%-95% non-condensing	10%-95% non-condensing	10%-95% non-condensing

Especificaciones del Producto

	W1520S-IN	W3320S-IN	W5602S-IN	W7320S-IN
				
HTTP Throughput	4 Gbps	5 Gbps	7 Gbps	13 Gbps
HTTP New Sessions	10,000	14,000	22,000	45,000
HTTP Maximum Transactions Per Second (TPS)	15,000	22,000	33,500	70,000
Storage	480G SSD	960G SSD	960G SSD	960G SSD
RAM	16G	32G	32G	64G
Management Ports	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port (SPF)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 2 x HA Ports (SFP+)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 2 x HA Ports (SFP+)	2 x USB Ports, 1 x MGT Port, 1 x Console Port, 1 x HA Port (SFP+)
Fixed I/O Ports	2 x SFP+, 8 x SFP, 16 x GE (including 2 bypass pairs)	6 x SFP+, 16 x SFP, 8 x GE (including 2 bypass pairs)	6 x SFP+, 16 x SFP, 8 x GE (including 2 bypass pairs)	2 x QSFP+, 16 x SFP+, 8 x GE (including 4 bypass pairs)
Available Slots for Expansion Modules	1	1	1	1
Expansion Module Option	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A	IOC-W-4SFP+-A IOC-W-2QSFP+-A IOC-W-2MM-BE-A IOC-W-2SM-BE-A
Protected Sites	128	256	512	512
Protected IP/PORT Pairs	512	1024	1024	4096
Power Specification	100W, Dual AC	280W, Dual AC	280W, Dual AC	300W, Dual AC
Power Supply	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz	AC 100-240 V 50/60 Hz
Form Factor	1U	1U	1U	1U
Dimension(WxDxH)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)	17.1×17.2×1.7 in (436.0*437.0*44.0mm)
Weight	26 lb (11.8 kg)	32.6 lb (14.8 kg)	32.6 lb (14.8 kg)	32.6 lb (14.8 kg)
Operating 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)
Relative Humidity	10%-95% non-condensing	10%-95% non-condensing	10%-95% non-condensing	10%-95% non-condensing

Especificaciones: Dispositivo virtual

	SG-6000-WV02-IN	SG-6000-WV04-IN	SG-6000-WV08-IN	SG-6000-WV12-IN
HTTP Throughput	1.2 Gbps	2.5 Gbps	5.5 Gbps	8 Gbps
HTTP New Sessions	2,800	5,800	14,000	20,000
HTTP Maximum Transactions Per Second (TPS)	3,000	6,500	16,000	22,000
vCPU Support	2 Core	4 Core	8 Core	12 Core
Storage (Min/Max)	100 GB/1 TB	100 GB/1 TB	100 GB/1 TB	100 GB/1 TB
RAM	4 GB	8 GB	16 G	24 G
Maximum Network Interface Support	10	10	10	10
Protected Sites	16	32	128	256
Protected IP/PORT Pairs	32	64	1024	1024

Opciones del Módulo

				
Module	IOC-W-4SFP+-A-IN	IOC-W-2QSFP+-A-IN	IOC-W-2MM-BE-A-IN	IOC-W-2SM-BE-A-IN
I/O Ports	4 x SFP+ Ports	2 x QSFP+ Ports	MM Bypass (2 pairs of bypass ports)	SM Bypass (2 pairs of bypass ports)
Dimension	1U	1U	1U	1U
Weight	2.09 lb (0.95 kg)	2.09 lb (0.95 kg)	2.09 lb (0.95 kg)	2.09 lb (0.95 kg)

NOTAS:
Los rendimientos de protección HTTP se obtienen bajo la configuración del sitio de protección y se utiliza la "Estrategia de protección media."

Version: EX-08.01-W-Series-V3.4-1123-SP