Propuesta Técnica
NIPS S600

Realizado por: IT Sistemas

Modelo: S600

Fecha: Julio del 2020

Contenidos

T&GSIMPLECOM CIA LTDA
RUC: 1792613523001
Telf: (02) 2523981
Email: info@itsistemas.com.ec
Orellana y 6 de Diciembre edificio La Viña oficina 204, MZ

Antecedentes

El presente documento tiene por objeto detallar todas las funcionalidades detalladas de los equipos **"HILLSTONE NIPS SERIE S-600".** Cada una de sus características y bondades, así como los módulos que contienen.

Hillstone NIPS S600

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.

A continuación, se presentan las características y funcionalidades que contiene dicho equipo dentro de esta propuesta técnica:

Componente Especificaciones Técnicas

DESCRIPCIÓN	CUMPLE
La solución tiene un puerto de consola dedicado, y dos puertos USB	SI
La solución tiene 4 puertos Gigabit Ethernet fijos	SI
La solución posee una ranura para los módulos de IO de extensión, para crecimiento de la infraestructura tecnológica.	SI
La solución admite un máximo de 4 puertos Gigabit Ethernet, o un máximo de 4 puertos SFP, con el módulo IO opcional en las ranuras de extensión.	SI
La solución es compatible con la fuente de alimentación de CA	SI
La solución tiene un factor de forma 1-U.	SI
La solución propuesta admite IPS Throughput de 1Gpbs	SI
La solución soporte 2M sesiones concurrentes.	SI
La solución admite 9,000 nuevas sesiones por segundo bajo tráfico TCP.	SI
La solución admite un par de Gigabit Ethernet Bypass como una opción de actualización futura.	SI

T&GSIMPLECOM CIA LTDA
RUC: 1792613523001
Telf: (02) 2523981
Email: info@itsistemas.com.ec
Orellana y 6 de Diciembre edificio La Viña oficina 204, MZ

La solución posee un espacio de almacenamiento de 1T	SI

Componente Prevención de Intrusiones

DESCRIPCIÓN	CUMPLE
La solución tiene 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	SI
La solución tiene como acciones de IPS: Monitoreo, bloqueo, reinicio (IP de los atacantes o de la víctima, interfaz de entrada) con tiempo de caducidad	SI
La solución es compatible con el registro de paquetes	SI
La solución es compatible con la selección basada en filtros: gravedad, destino, sistema operativo, aplicación o protocolo	SI
La solución es compatible con la exención de IP de firmas específicas de IP	SI
La solución soporta el Modo de husmeo IDS	SI
La solución es compatible con 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)	SI
La solución es compatible con Bypass activo con interfaces de bypass	SI
La solución propuesta admite la prevención de configuración predefinida	SI

Componente Detección y Amenazas

DESCRIPCIÓN	CUMPLE
La solución admite correlación entre las amenazas desconocidas, comportamiento anormal y comportamiento de la aplicación para descubrir amenazas o ataques potenciales	SI
La solución es compatible con reglas de correlación multidimensional, actualización diaria automática en la nube	SI

T&GSIMPLECOM CIA LTDA
RUC: 1792613523001
Telf: (02) 2523981
Email: info@itsistemas.com.ec
Orellana y 6 de Diciembre edificio La Viña oficina 204, MZ

La solución es compatible con Detección avanzada de malware basada en el comportamiento	SI
La solución admite la detección de más de 2000 familias de programas maliciosos conocidos y desconocidos, incluyendo virus, desbordamiento, gusanos, troyanos, etc.	SI
La solución es compatible con la detección en tiempo real, en línea, comportamiento del malware, actualización de base de datos modelo	SI
La solución es compatible con el 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	SI
La solución permite la detección de ataques DDoS incluyendo por inundación, Sockstress, zip de la muerte, reflexión, consultas DNS, DDoS SSL y aplicaciones DDoS	SI
La solución permite el apoyo a la inspección del tráfico de un túnel encriptado para aplicaciones desconocida	SI
La solución admite la detección de comportamiento anormal en tiempo real, en línea, comportamiento anormal de la actualización de la base de datos modelo	SI

Componente Antivirus y Defensa contra Ataques

DESCRIPCIÓN	CUMPLE
La solución soporta más de 13 millones de firmas de AV	SI
La solución es compatible con Antivirus basados en flujos: protocolos que incluyen HTTP, SMTP, POP3, IMAP, FTP/SFTP.	SI
La solución es compatible con el escaneo de virus en archivos compreso	SI
La solución es compatible con la defensa contra ataques de protocolo anormal	SI
La solución es compatible con la defensa Anti-DoS/DDoS, incluyendo SYN Flood, defensa contra inundación de consultas DNS	SI
La solución es compatible con la defensa contra ataques AR	SI

T&GSIMPLECOM CIA LTDA
RUC: 1792613523001
Telf: (02) 2523981
Email: info@itsistemas.com.ec
Orellana y 6 de Diciembre edificio La Viña oficina 204, MZ

Componente Filtrado URL

DESCRIPCIÓN	CUMPLE
La solución admite la inspección de filtrado web basado en el flujo	SI
La solución es compatible con el Filtrado web definido manualmente basado en URL, contenidos web y por cabecera MIME	SI
La solución admite el 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)	SI
La solución soporta las siguientes 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	SI
La solución admite la anulación del perfil web de filtrado: permite que el administrador asigne temporalmente diferentes perfiles de usuario/grupo/IP	SI
La solución admite el Filtro Web para categorías locales y anulación de categorías calificadas	SI

Componente Anti-Spam

DESCRIPCIÓN	CUMPLE
La solución es compatible con la Clasificación y prevención del spam en tiempo real	SI
La solución soporta spam confirmado, spam sospechoso, spam masivo, volumen válido	SI
La solución admite la protección Independientemente del idioma, formato o contenido del mensaje	SI
La solución admite protocolos de correo electrónico SMTP y POP3	SI
La solución admite la detección entrante y saliente	SI

T&GSIMPLECOM CIA LTDA
RUC: 1792613523001
Telf: (02) 2523981
Email: info@itsistemas.com.ec
Orellana y 6 de Diciembre edificio La Viña oficina 204, MZ

La solución es compatible con listas blancas permiten correos electrónicos de dominios / direcciones de correo electrónico confiables	SI
La solución admite listas negras definidas por el usuario	SI

Componente Sandbox

DESCRIPCIÓN	CUMPLE
La solución es compatible con la carga archivos maliciosos a la nube en una sandbox para su análisis, incluyendo el tráfico cifrado HTTPS	SI
La solución admite la carga de archivos maliciosos desde protocolos que incluyen HTTP / HTTPS, POP3, IMAP, SMTP y FTP.	SI
La solución admite tipos de archivos que incluyen PE, ZIP, RAR, Office, PDF, APK, JAR y SWF	SI
La solución admite la dirección de transferencia de archivos y el control del tamaño del archivo.	SI
La solución proporciona un informe completo de análisis de comportamiento para archivos maliciosos	SI
La solución es compatible con el intercambio global de inteligencia de amenazas y bloqueo de amenazas en tiempo real.	SI

Componente Botnet

DESCRIPCIÓN	CUMPLE
La solución descubre intranet botnet host mediante el control de CyC conexiones y el bloque más avanzaron amenazas como botnet y ransomware	SI
La solución es compatible con las actualizaciones regulares de la dirección del servidor Botnet.	SI
La solución admite dos tipos de base de datos de direcciones C&C: la base de datos de direcciones IP (excluyendo las direcciones IPv6) y la base de datos del dominio.	SI
La solución admite la detección de los protocolos TCP, HTTP y DNS.	SI
La solución es compatible con la lista blanca para C&C IP y dominio	SI

T&GSIMPLECOM CIA LTDA
RUC: 1792613523001
Telf: (02) 2523981
Email: info@itsistemas.com.ec
Orellana y 6 de Diciembre edificio La Viña oficina 204, MZ

Componente IP Reputation

DESCRIPCIÓN	CUMPLE
Identifica y filtra el tráfico del riesgo IP, como host de botnet, spammers, nodos TOR, host vulnerados y ataques a fuerza bruta	SI
Soporta los registros, caída de paquetes, o bloqueo para los diferentes tipos de riesgo en tráfico	SI
Soporta la constante actualización de la base de datos IP por reputación y firmas	SI

Componente Control de Aplicaciones

DESCRIPCIÓN	CUMPLE
La solución soporta más de 3.000 aplicaciones que se pueden filtrar por nombre, categoría, subcategoría, tecnología y por riesgo	SI
La solución permite que cada aplicación contenga una descripción, sus factores de riesgo, dependencias, puertos típicos utilizados, y las URL de referencia adicional	SI
La solución admite Acciones de bloqueo y monitoreo	SI
Proporciona monitoreo multidimensional y estadísticas para las aplicaciones que se ejecutan en la nube, incluyendo la categoría de los riesgos y sus características	SI

Componente Alta Disponibilidad

DESCRIPCIÓN	CUMPLE
La solución soporta interfaces heartbeats redundantes	SI
La solución admite el Modo activo / pasivo y de pares	SI
La solución admite la sincronización de sesión autónoma	SI
La solución soporta interfaz HA de gestión reservada	SI
La solución soporta la conmutación por error (failover): ▪ Puerto, monitoreo de vínculos locales y remotos	SI

T&GSIMPLECOM CIA LTDA
RUC: 1792613523001
Telf: (02) 2523981
Email: info@itsistemas.com.ec
Orellana y 6 de Diciembre edificio La Viña oficina 204, MZ

▪ Con estado de conmutación por error ▪ Conmutación por error, inferior a un segundo ▪ Notificación de fallas	
La solución soporta las siguientes Opciones de Implementación: ▪ HA con agregación de enlaces ▪ HA con malla completa ▪ HA geográficamente dispersa	SI

Componente QoS

DESCRIPCIÓN	CUMPLE
La solución es compatible con el control de ancho de banda máximo o garantizado, en una dirección IP o usuario.	SI
La solución admite la asignación de túneles en función del dominio de seguridad, la interfaz, la dirección, el grupo de usuarios / usuarios, el grupo de servidores / servidores, el grupo de aplicaciones / aplicaciones, los TOS, las VLAN.	SI
La solución admite el ancho de banda asignado por tiempo, prioridad o el mismo ancho de banda compartido.	SI
La solución es compatible con TOS y DiffServ.	SI
La solución admite la asignación flexible y priorizada del ancho de banda restante no utilizado.	SI
La solución admite la asignación de ancho de banda según la categoría de URL	SI
La solución soporta un número máximo de conexiones simultáneas por IP	SI
La solución controla el límite de ancho de banda al demorar el acceso por usuario o IP	SI

Componente Administración

DESCRIPCIÓN	CUMPLE
La solución soporta acceso administrativo: HTTP/HTTPS, SSH, Telnet, consola	SI
La solución soportal la administración Central: Administrador Hillstone de seguridad (HSM), API de servicios web	SI

T&GSIMPLECOM CIA LTDA
RUC: 1792613523001
Telf: (02) 2523981
Email: info@itsistemas.com.ec
Orellana y 6 de Diciembre edificio La Viña oficina 204, MZ

La solución soporta la autenticación de dos factores: archivo de nombre de usuario/contraseña, certificados HTTPS	SI
La solución es compatible con la integración de Sistemas: SNMP, Syslog, alianzas	SI
La solución admite administración de dispositivos de almacenamiento: personalización del umbral y alarmas sobre el espacio almacenamiento, superposición de datos antiguos, detención de la grabación.	SI

Componente IPv6

DESCRIPCIÓN	CUMPLE
La solución es compatible con la administración de dispositivos a través de IPv6, el registro de IPv6 y HA en IPV6.	SI
La solución es compatible con túneles IPv6, DNS64 / NAT64, etc.	SI
La solución es compatible con los protocolos de enrutamiento IPv6 de enrutamiento estático, enrutamiento de políticas, ISIS, RIPng, OSPFv3 y BGP4 +	SI
La solución es compatible con IPv6 IPS, identificación de la aplicación, filtrado de URL, antivirus, control de acceso, defensa de ataque ND	SI

Componente Logs y Reportes

DESCRIPCIÓN	CUMPLE
La solución admite las instalaciones para registros: memoria y almacenamiento locales, múltiples servidores syslog y varias plataformas Hillstone para Auditoría de Seguridad (HSA)	SI
La solución soporta el cifrado de registros e integridad de registros con subida de lotes HSA programados	SI
La solución soporta registros fiables utilizando la opción TCP (RFC 3195)	SI
La solución soporta registros de tráfico detallados: reenviados, sesiones violadas, tráfico local, paquetes inválidos	SI
La solución soporta registros detallados de eventos: auditorías del sistema y de la actividad administrativa, enrutamiento y	SI

T&GSIMPLECOM CIA LTDA
RUC: 1792613523001
Telf: (02) 2523981
Email: info@itsistemas.com.ec
Orellana y 6 de Diciembre edificio La Viña oficina 204, MZ

trabajo de la red, VPN, autenticaciones de usuario, eventos relacionados con Wifi	
La solución admite el registro por opción de IP y servicio de resolución de nombres de puerto	SI
La solución admite informes Granulares con Puntos de Vista Orientados a los Usuario: ▪ Administración de HA/Visualización a nivel C ▪ Visualización para el Dueño Sistema Empresarial ▪ Visualización para el Administrador de Seguridad	SI

Componente Monitoreo

DESCRIPCIÓN	CUMPLE
Soporta las estadísticas de eventos de amenaza y monitoreo de aplicaciones y URL	SI
La solución es compatible con el análisis y estadísticas de tráfico en tiempo real	SI
Brinda información del sistema como la sesión concurrente, CPU, memoria y temperatura	SI
Estadísticas y monitoreo del tráfico iQOS, monitoreo del estado de enlaces	SI
Servicio de inteligencia de amenazas basado en la nube	SI

T&GSIMPLECOM CIA LTDA
RUC: 1792613523001
Telf: (02) 2523981
Email: info@itsistemas.com.ec
Orellana y 6 de Diciembre edificio La Viña oficina 204, MZ