Hillstone™
NETWORKS

Las amenazas avanzadas requieren inteligencia avanzada

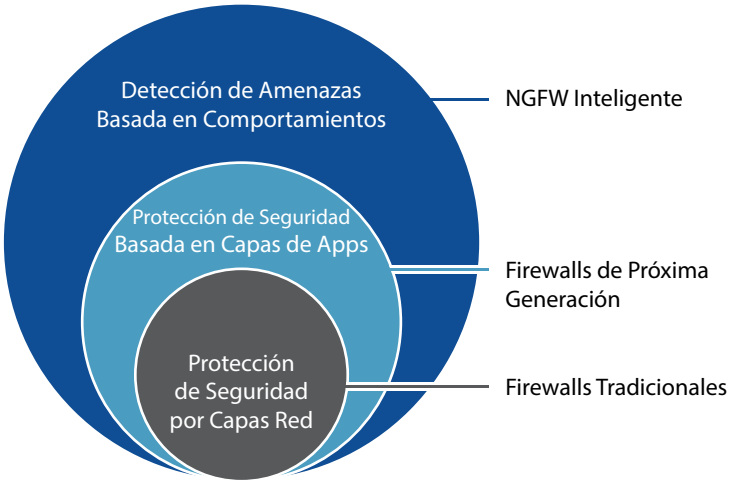
Por qué su organización necesita los firewalls inteligentes de Próxima Generación de Hillstone

La protección de su red nunca ha sido tan crítica como lo es hoy. Si bien los firewalls de próxima generación tradicionales siguen brindando protección, nunca fueron diseñados para abordar las amenazas avanzadas de hoy en día. Los hackers han cambiado su enfoque a amenazas avanzadas como Ransomware u otros tipos de malware que pueden comprometer sus recursos más valiosos y exponer a su organización a pérdidas financieras, comprometer información confidencial o algo peor.

FIREWALL POR FILTRO DE PAQUETES	FIREWALL STATEFUL	GESTIÓN UNIFICADA PARA AMENAZAS	FIREWALL DE PRÓXIMA GENERACIÓN	NGFW Inteligente
1988	1994	2004	2009	NOW!
ACCESO	SESIÓN	FUNCIÓN COMBINADA	USUARIO, APPLICACIÓN, CONTENIDO	ANÁLISIS CONDUCTUAL

NGFW vs. NGFW Inteligente

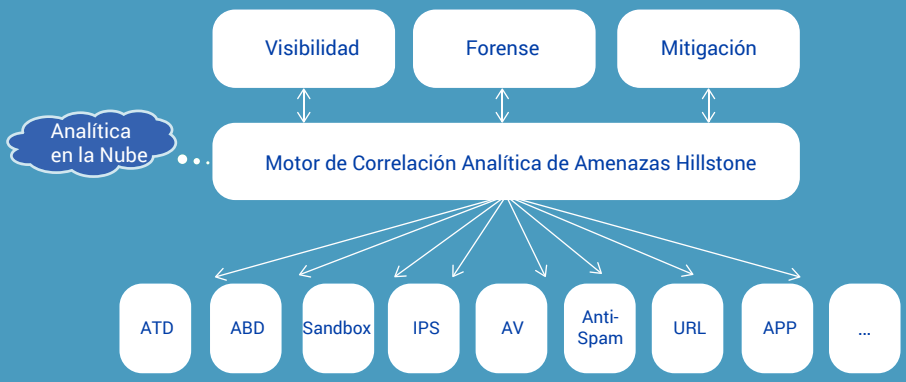
Los firewalls tradicionales proporcionaban seguridad solamente por capa de red básica. Los firewalls de próxima generación actuales agregan protección de seguridad por capas de aplicaciones. Los firewalls inteligentes Next Generation de Hillstone (iNGFW) agregan monitoreo basado en el comportamiento que aumenta significativamente la detección y protección. Utilizan el aprendizaje automático y la inteligencia artificial para examinar de cerca el comportamiento en la red para identificar actividades anómalas que los profesionales de la seguridad deben estudiar o bloquear.



Firewall inteligente de Próxima Generación

El Firewall inteligente de próxima generación (iNGFW) de Hillstone Networks utiliza tres tecnologías clave para detectar ataques avanzados y proporcionar una defensa de amenazas continua para las redes de los clientes:

- El análisis conductual detecta comportamiento anómalo en la red, basado en el motor de Detección Conductual Avanzada de Hillstone (ABD).
- La agrupación estadística ayuda a detectar malware desconocido, aprovechando el motor patentado de Detección de Amenazas Avanzada (ATD) de Hillstone.
- El motor de análisis de correlación de amenazas correlaciona los eventos de amenazas detectados por diferentes motores, incluidos ATD, ABD, Sandbox y otras tecnologías tradicionales de detección de amenazas basadas en firmas, junto con información de contexto para identificar las amenazas avanzadas.



Hillstone iNGFW ofrece 3 beneficios clave para los usuarios finales

Defiende contra las amenazas avanzadas con un análisis de correlación de seguridad en Kill Chain..

Protege los activos críticos por medio de supervisión integral y visibilidad de la red.

Reduce el tiempo entre el compromiso y la detección con múltiples mecanismos de detección y protección, así como el análisis en la nube.

The Difference Between NGFW and iNGFW

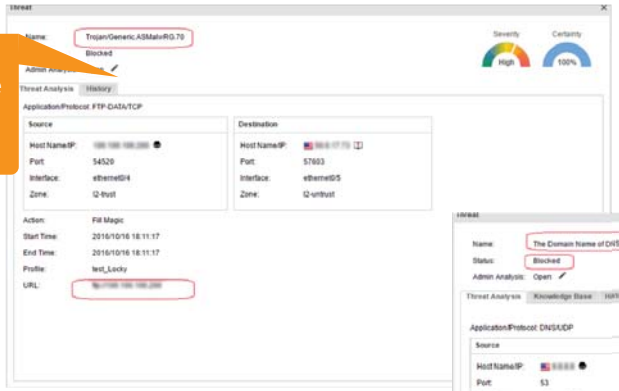
Features	NGFW	iNGFW
Detección Comportamiento Anormal		✔
Detección Avanzada de Amenazas		✔
Kill Chain		✔
Análisis de Correlación de Amenazas		✔
Mitigación Prioritaria		✔
Servicios de Red	✔	✔
Prevención de Intrusiones	✔	✔
Anti-Virus	✔	✔
Defensa contra Ataques	✔	✔
Anti-Spam	✔	✔
Filtrado por URL	✔	✔
Cloud-Sandbox	✔	✔
Reputación de las IP	✔	✔
Descifrado SSL	✔	✔
Identificación de Punto Final	✔	✔
Control Transferencia de Archivos	✔	✔
Control de Aplicaciones	✔	✔
Calidad del Servicio (QoS)	✔	✔
Equilibrio Cargas del Servidor	✔	✔
Balanceo de Cargas Enlaces	✔	✔
VPN	✔	✔
IPv6	✔	✔
VSYS	✔	✔
Alta Disponibilidad	✔	✔
Identidad de Usuario y Dispositivo	✔	✔
Logs e Informes	✔	✔

TRES CASOS DE USO COMÚN

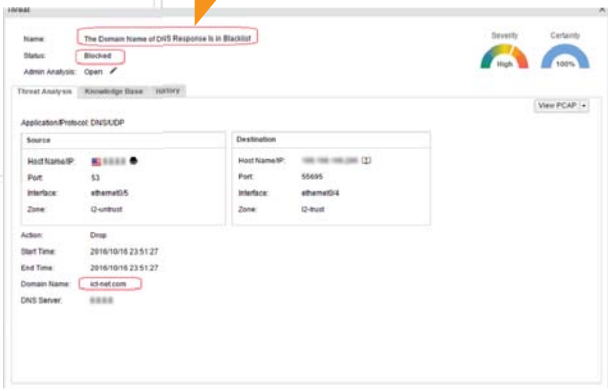
Detectar y Prevenir Ransomware

- El ransomware bloquea los sistemas empresariales mediante la encriptación de sus datos críticos, descifrándolos sólo después de que la víctima pague a los atacantes un rescate monetario. Ahora es la preocupación número uno para la seguridad. El FBI dice que más de US $1.000.000.000 se pagaron debido al ransomware en 2016..
- Hillstone iNGFW aprovecha varios motores de seguridad para proteger contra las amenazas de Ransomware, incluyendo AV, IPS, ATD, ABD y Bases de Datos por Reputación.
- Con una protección de seguridad completa, Hillstone iNGFW puede detectar y mitigar incluso las variantes de ransomware más sofisticadas y en rápida evolución en cualquiera o todas las etapas de ataque tipo Kill Chain.

El motor AV de iNGFW detecta y reconoce la carga útil del ransomware como Trojan/Generic.ASMalwRG.70 y lo pone en cuarentena.



Si el archivo adjunto malicioso se ejecutó e intenta conectarse al servidor C&C, el motor de detección de reputación iNGFW puede reconocer el dominio del servidor C&C aprovechando la base de datos de reputación en la nube y bloquearla.



Protege activos críticos contra ataques DDoS

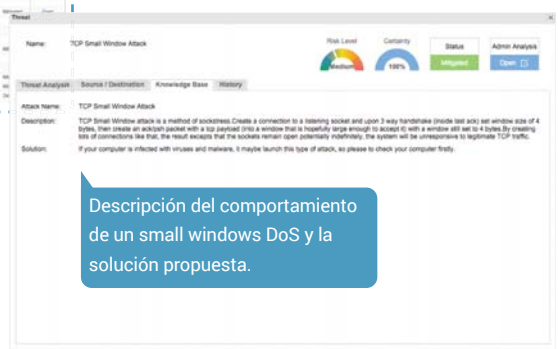
Un ataque de denegación de servicio distribuido (DDoS) es un intento de hacer que un servicio en línea no esté disponible al colmarlo con tráfico de múltiples fuentes. Apuntan a una amplia variedad de recursos importantes, desde bancos hasta sitios web de noticias, y presentan un gran desafío para asegurarse de que las personas puedan publicar y acceder a información importante.

El iNGFW detecta los diferentes comportamientos de un DoS incluyendo los ataques SYN y de TCP

El motor iNGFW ABD puede detectar ataques DDoS de aplicaciones ignorados por las soluciones existentes mediante el modelado de la IP del atacante e identificando el comportamiento anormal de una IP.

El motor ABD rastrea cientos de dimensiones en L4-L7, y puede identificar 6 tipos y más de 50 comportamientos de DoS.

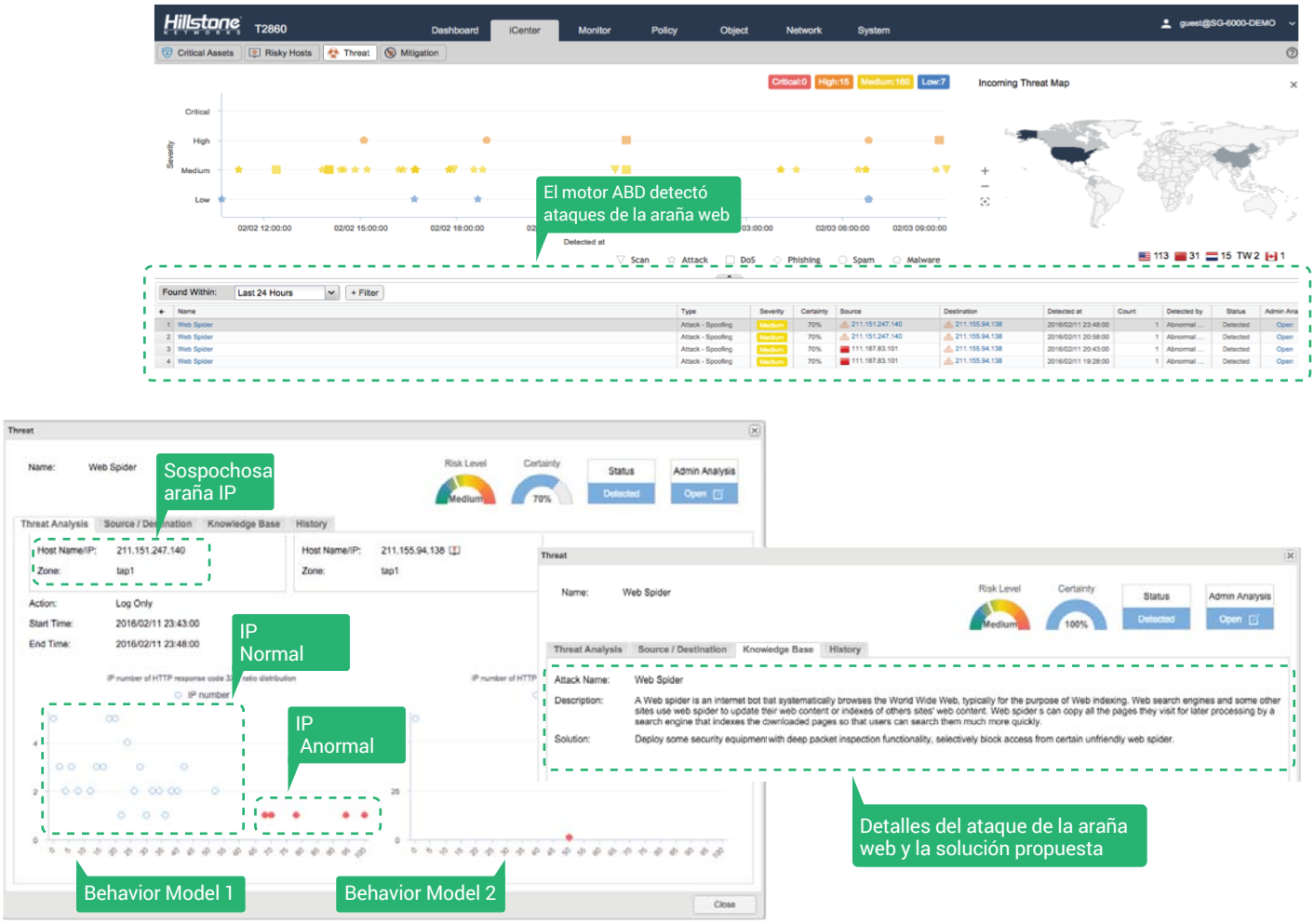
Descripción del comportamiento de un small windows DoS y la solución propuesta.



Detecta una araña web de forma oportuna

Una araña web (también llamada rastreador web, robot web) suele ser una secuencia de comandos o un programa informático que navega por el sitio web objetivo de forma ordenada y automática. Un rastreador web malintencionado o de mal comportamiento puede consumir grandes cantidades de ancho de banda y causar interrupciones, especialmente a las empresas que dependen del tráfico web o contenido para sus negocios.

El Hillstone iNGFW implementado en línea con su función ABD y ATD habilitada. Utilizando el modelo incrustado para comportamiento de la araña y comparación de parámetros, el motor ABD detectó varias direcciones IP que mostraban un comportamiento anormal.



El administrador recibe la advertencia y puede configurar cambios de política para mitigar la amenaza de manera oportuna.

Cómo contactar a Hillstone Networks

www.hillstonenet.com

EMAIL: inquiry@hillstonenet.com