Sourcefire IPS™ (Intrusion Prevention System) Best-in-Class Intrusion Detection and Prevention

Las redes son dinámicas. *Las amenazas están* *con stantemente evolucionando y siendo más sofisticadas. Violaciones en las redes de seguridad continuarán ocurriendo ya que las defensas estáticas no pueden protegerse de las también dinámicas amenazas. Entérate porque cada vez más las organizaciones están* ***dependiendo de Snort®*** ***más que ninguna otra tecnología de NIPS*** *y porque miles de empresas confían en Sourcefire's IPS™.*

SOURCEFIRE IPS—EL FUNDAMENTO DEL SOURCEFIRE 3D® SYSTEM

Snort—el IPS estándar “De Facto” para la prevención de intrusos

Basado en Snort, el estándar de facto para la prevención y detección de intrusos (IDS/IPS), Sourcefire IPS™ (Intrusion Prevention System) es el fundamento del reconocido ganador Sourcefire 3D System. El Sourcefire IPS utiliza una potente combinación entre métodos de inspección basados en vulnerabilidades y detección de anomalías—a velocidades de línea de hasta 10Gbps—para analizar tráfico de redes y prevenir amenzas que puedan dañar sus redes. Adicionalmente, cuando el Sourcefire IPS es implementado con el dispositivo Sourcefire SSL, Los beneficios del IPS se extienden a la protección de tráfico encriptado. Ya sea si es implementado en el perímetro, en una DMZ, en el núcleo, o en segmentos críticos de las redes. Los dispositivos de Sourcefire son fáciles de usar, además de que proveen una protección comprensiva a las amenazas.

El IPS de Sourcefire contiene múltiples políticas por defecto para bloqueo pre-configuradas, creadas a partir de una comprensiva librería de reglas abiertas de Snort. Las reglas abiertas permiten a los clientes verificar que las reglas están dirigidas a proteger la cobertura de las vulnerabilidades para las que fueron hechas y crear nuevas reglas o modificar las existentes para proteger aplicaciones y sistemas customizados. El Sourcefire IPS puede ser desplegado en línea bloqueando y/o alertando en modo pasivo, y puede remediar ataques usando equipos externos, tales como, firewalls, routers, sistemas de administración de parches, y más.

Snort, creado por Sourcefire, tiene cerca de 4 millones de descargas y aproximadamente 326,000 usuarios registrados. En todo el mundo cada vez más organizaciones están confiando en Snort más que en ninguna otra tecnología de prevención de intrusos. Durante la década pasada, la comunidad de Snort ha crecido tanto para convertirse en un entero ecosistema., desde grupos de usuarios, libros, así como clases en donde enseñan a miles de colegios y Universidades. Más profesionales del ramo de IT están más familiarizados con Snort que con ninguna otra tecnología de IPS en el mercado. Los clientes de Sourcefire se han beneficiado de este ecosistema desde el primer día.

Protección en contra de Amenazas conocidas y desconocidas

El equipo de Sourcefire Vulnerability Research Team™ (VRT) funciona contra reloj para asegurar que los clientes comerciales de Sourcefire y usuarios de recursos abiertos estén protegidos contra amenazas conocidas y desconocidas.

El VRT lidera la industria de IPS cubriendo las vulnerabilidades del Martes de Microsoft el mismo día que fueron anunciadas.

Es muy común que amenazas desconocidas puedan ser las más dañinas. Es por esto mismo que Sourcefire publica las reglas de Snort basadas en vulnerabilidades. Diferente a los IPS que se concentra primariamente en firmas basadas en “exploits”, las reglas de Snort ofrecen protección en contra de cualquier posible explotación a una vulnerabilidad. Esto fue ilustrado cuando Sourcefire protegió a sus clientes 3D y a los usuarios de fuentes abiertas de Snort del gusano Conficker con más dos años de anticipación.

La herramientas del Sourcefire IPS proveen una comprensiva protección en contra de las siguientes amenazas:

- Gusanos
- Ataques DoS
- Tráfico Malformado
- Troyanos
- Buffer overflows

Amenazas compuestas

Ataques Backdoor

Ataques P2P

Ataques Rate-based

Spyware

Anomalías estadísticas

Amenazas de día cero

Escaneos de puertos

Anomalías de Protocolo

Segmentación de TCP y fragmentación de IP

Ataques a VoIP

Encabezados Inválidos

Ataques a IPv6

Anomalías de aplicaciones

Protección para ambientes físicos virtuales

Dispositivo de propósito específico, certificado por ICSA, los Sourcefire 3D® Sensors están disponibles con IPS capacidades desde 5Mbps hasta 20Gbps. Los 3D Sensors están disponibles con características de tolerancia a fallas, tales como puertos “fail-open” integrados en cobre y fibra, fuentes de poder redundantes, y discos RAID.

El Sensor Sourcefire Virtual 3D™ extiende el Sourcefire 3D System hasta lugares lejanas de las redes donde los recursos de seguridad de IT no existen o el despliegue de los 3D Sensors físicos son poco prácticos. El Virtual 3D Sensor también provee la capacidad de inspeccionar comunicaciones VM-to-VM, y provee la misma protección que su contraparte, el sensor físico. El Virtual 3D Sensor ofrece soporte para la inspección de tráfico de redes a una velocidad hasta de 500Mbps.

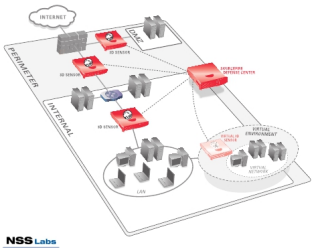

Figure 1. Sourcefire soporta una estrategia de prevención de instrusión Defense-in-Depth, per-mitiendo a los Sourcefire 3D Sensors físicos o virtuales se posesionen en todas las áreas de la red. El Sourcefire Defense Center hace posible agregación de todos los eventos, análisis y la administración de la política IPS.

Agregación y análisis centralizado de eventos

Utilizando la llena de funcionalidades, y además fácil de usar, consola de administración Sourcefire Defense Center™ (DC) de Sourcefire Virtual Defense Center, los clientes pueden analizar eventos, configurar y aplicar políticas a los IPS, descargar y aplicar automáticamente las actualizaciones de las reglas Snort, y más. Enriquecido por la ingeniería de detección de Snort, el Sourcefire IPS es excelente proporcionando paquetes con un nivel forense de detalle, sofisticados y customizados diagramas de flujo para la investigación de eventos de seguridad en el momento que vayan ocurriendo. Para implementaciones mayores, los clientes pueden tomar ventaja de la tecnología del Sourcefire Master Defense Center (MDC) para manejar múltiples CDs y cientos de 3D Sensors físicos y/o virtuales desplegados a través de la entera organización.

Reportes, Alertas y Dashboards

El DC provee a sus clientes con numerosos reportes, alertas y dashboards. Los clientes pueden contar con una variedad de reportes predefinidos o crear reportes customizados que cumplan con las necesidades de cualquier organización. Ellos pueden recibir alertas en formato de entradas de syslog, mensajes de email, o SNMP. Los clientes pueden también crear dashboards totalmente customizadas con docenas de drag-and-drop “widgets” que pueden desplegar información crítica en forma de tablas y gráficas.

SOLUCIÓN DE SEGURIDAD ADAPTATIVA EN TIEMPO REAL DE SOURCEFIRE

Inteligencia de Red en tiempo real

Sourcefire RNA® (Real-time Network Awareness) provee 24x7, inteligencia pasiva 7X24 para redes, almacenando en tiempo real un inventario de sistemas operativos, servicios, aplicaciones, protocolos, y vulnerabilidades potenciales que existen en la red. RNA colecta esta inteligencia en una manera completamente pasiva, mientras discretamente integra la inteligencia con el 3D System. RNA’s base de datos host puede ser incrementada con información reunida por las herramientas activas de descubrimiento para expandir el almacenamiento de inteligencia de la red. Combinar RNA’s visibilidad de redes en tiempo real con Sourcefire RUA® (Real-time User Awareness), es una tecnología que liga la identidad del usuario con eventos de seguridad y su cumplimiento, y organizaciones que tienen iniciativas de inteligencia en sus redes y usuarios dinámicos.

Evaluación de impacto Automático

Los profesionales de Seguridad de IT no tienen el tiempo de examinar a fondo cientos o miles de eventos de seguridad cada día para tratar saber cuales eventos son los más importantes. Apoyándose en Sourcefire RNA's red de inteligencia en tiempo real, los clientes pueden llevar su Sourcefire IPS al siguiente nivel. La inteligencia de amenazas está automáticamente correlacionada en contra del RNA inteligencia objetivo en tiempo real para determinar la relevancia e impacto de un ataque. Con evaluaciones automatizadas de impacto. Los eventos son reducidos hasta en un 99%, permitiendo a los administradores enfocarse en eventos que puedan en realidad afectar sus redes.

Afinación Automatizada del IPS

Los profesionales de seguridad en IT no tienen el tiempo de estar constantemente "afinando" sus IPS a la vez que sus redes cambian. Incorporando RNA inteligencia de redes en tiempo real Sourcefire IPS, el constante proceso de "afinar" el IPS puede también ser automático. A medida que las redes evolucionan, RNA-Reglas recomendadas determinan cuales reglas de Snort habilitar y cuales deshabilitar. RNA recomienda relevantes reglas Snort basándose en la red que se está protegiendo y las reglas Snort pueden ser habilitadas con o sin intervención de humanos.

El uso de la solución de seguridad adaptada en tiempo real Sourcefire da como resultado un menor uso de investigación manual de eventos y el afinar el IPS por el staff de seguridad de IT, menores tiempos muertos de la red, y menores costos de operación. Teniendo el conocimiento en tiempo real de que esta pasando en tu red, el 3D System te ahorra tiempo y esfuerzo y maximiza la protección de tu siempre cambiante red.

TOMA EL SIGUIENTE PASO PARA PROTEGER TU RED

Sourcefire es el único proveedor de IPS en ofrecer defensas dinámicas en contra

de las amenazas objetivo en tu red que constantemente está cambiando. Las

capacidades clave de Sourcefire incluyen:

· **Protección superior de ataques:**

» Snort IPS ingeniería de detección.

» Vulnerabilidad basada en las reglas de Snort.

» Reglas abiertas de lenguaje—vista, edición, y creación de reglas Snort.

» Múltiples default IPS políticas.

» ICSA Labs certificado y NSS Labs examinado.

· **Mayor información contextual acerca de las amenazas:**

» 24x7, inteligencia de la red pasiva

» Rastreo de identidad de usuario

- **El único proveedor en ofrecer soluciones de seguridad adaptadas en tiempo real:**

» Tiempo real, evaluación de impacto automatizada en eventos de intrusión

» Automatizada afinación del IPS basada en las ventajas actuales de la red

- **Sistema integrado de manejo de una consola fácil de usar**

» “Manager of managers” enterprise-class. Escalar a través de la tecnología MDC

- **Excelente análisis forense y de eventos:**

» Poderoso sistema mostrando eventos

» Paquete completo de entradas