



Contactos de prensa:

Gerardo Melgoza | SonicWALL | gmelgoza@SonicWALL.com

Francisco Guzmán | SonicWALL | fguzman@SonicWALL.com

Jesús García | SonicWALL | jgarcias@SonicWALL.com

Víctor Ruiz | SHM Consulting | vruiiz.shm@gmail.com

**SONICWALL PROVEE VISIBILIDAD SIN PARALELO,
DENTRO DE LA ACTIVIDAD DE LA RED,
CON EL LANZAMIENTO DE LA NUEVA APPLICATION AWARE
FIREWALLING**

Permite tener un amplio conocimiento y control de las aplicaciones a través de la línea de productos NSA de SonicWALL

SUNNYVALE, CALIF a 15 de diciembre, 2008 – SonicWALL, Inc. (NASDAQ: SNWL), compañía líder en seguridad de infraestructura de red, anunció el lanzamiento y disponibilidad inmediata de Application Aware Firewalling para toda la nueva generación de firewalls NSA de SonicWALL. Este adelanto, llamado aplicación de firewall (Application Firewall), aumenta significativamente la productividad de la red y de la seguridad, mediante la desmitificación del control y acceso de la aplicación, brindando una visibilidad incomparable dentro de la actividad de la red. Application Firewall identifica y clasifica aplicaciones, ofrece visibilidad dentro de aplicaciones específicas y acceso a contenidos por parte de los usuarios y automatiza las respuestas apropiadas contra cualquier riesgo mejorando enormemente el control de políticas y el cumplimiento de las redes actuales.

A diferencia de los firewalls tradicionales que inspeccionan únicamente puertos y protocolos, Application Firewall permite al administrador identificar, clasificar y reforzar, de forma sencilla, las políticas basadas en aplicaciones o el contenido específico de algunas aplicaciones. Estas características le proveen a los administradores de TI un control más detallado de políticas a través de la definición de accesos específicos a contenidos y aplicaciones por tipo de usuario, incluyendo puertos y protocolos. Mientras que la mayoría de los dispositivos de Administración Unificada de Amenazas (Unified Threat Management, UTM) solamente proveen opciones de inicio de sesión y bloqueo, Application Firewall provee a los administradores de TI una lista de acciones personalizadas y predefinidas, permitiendo la ejecución de gestión de ancho de banda y

personalizando los mensajes del soporte a usuario final, además de hacer actualizaciones de firmas comunes.

Las características clave de Application Firewall incluyen:

- **Administración del Ancho de Banda de Aplicaciones:** Permite a los administradores controlar la cantidad de ancho de banda que se asigna sobre la base del uso de cada aplicación. Este control provee la alternativa de bloquear la aplicación, limitar el ancho de banda que la aplicación puede usar o garantizar sólo una cantidad de ancho de banda para determinado cometido. Adicionalmente, pueden ser aplicadas reglas y políticas sobre la administración de ancho de banda en determinados tiempos, fechas, usuarios o grupos. Por ejemplo, se puede limitar el ancho de banda para ver videos en Internet o ejecutar aplicaciones de audio durante la jornada laboral. También se puede garantizar que algunos usuarios específicos, que utilizan aplicaciones de productividad enfocadas al área de ventas y estén basadas en "la nube", puedan obtener la cantidad adecuada de ancho de banda que requieren cada fin de trimestre.
- **Aplicación de identificación, bloqueo y notificación:** Los administradores de TI pueden ahora fácilmente identificar aplicaciones específicas, bloquear su uso y así generar una notificación al usuario diciéndole la razón por la cual la aplicación ha sido bloqueada. Por ejemplo, una organización tal vez desee detectar y tener control sobre una aplicación o un grupo de éstas que operen en una variedad de puertos abiertos a través del firewall. Application Firewall puede detectar las tentativas de uso de estas aplicaciones, bloquearlas y de forma automática crear una notificación apropiada para el usuario final. Esto refuerza el aceptable uso de políticas al mismo tiempo que se incrementa la productividad del empleado y de los recursos de la red. De igual forma, el administrador de TI puede asignar ciertas políticas a un grupo de aplicaciones. Ellos pueden definir sus propios grupos o utilizar algunos de los grupos de aplicaciones definidos por SonicWALL (por ejemplo, las redes Peer-to-Peer), los cuales son constantemente actualizados de forma automática por SonicWALL. Cabe señalar que el uso de los grupos de aplicaciones definidos por SonicWALL permite ahorrar tiempo en la creación y mantenimiento de políticas de identificación y reforzamiento de aplicaciones.
- **Conocimiento y control de información:** Application Firewall además puede analizar los datos, incluyendo la transferencia de archivos FTP, documentos adjuntos a los

correos electrónicos, así como contenido buscado en Internet. Las políticas pueden ser implantadas para identificar contenido específico y tomar la acción adecuada a cada caso. Como ejemplo se encuentra el bloqueo de correos electrónicos empresariales que contengan la frase "documento confidencial" o también la notificación al departamento de TI cuando algunos archivos FTP son transferidos y contienen nombres de proyectos específicos. Las notificaciones al usuario pueden ser generadas automáticamente si así se desea. Las reglas pueden aplicarse basándose en tiempos, fechas, usuarios o grupos, entre muchas opciones más.

"Application Firewall es más que una simple adición para el UTM," dijo Patrick Sweeney, vicepresidente de Seguridad de Red de SonicWALL. "La nueva generación de firewalls ofrece una seguridad de red líder en la industria, en la capa de aplicación, brindando una herramienta de administración que abarca todo, tanto amenazas como aplicaciones. Application Firewall permitirá a los administradores de TI proteger la infraestructura completa contra amenazas y al mismo tiempo administrar aplicaciones y el uso de ancho de banda, lo cual antes habría sido casi imposible."

Application Firewall de SonicWALL, en conjunto con la tecnología UTM y con el desempeño líder de la línea de firewalls NSA permite a los clientes no sólo proteger la totalidad de la red, sino contar con una mejor administración de sus negocios. Además de estas capacidades de gestión de amenazas, la capacidad de firewall para distinguir rápidamente entre aplicaciones seguras o perjudiciales aumenta la productividad a lo largo y ancho de todo el negocio y no sólo la productividad de los departamentos de TI.

Application Firewall está disponible en los sistemas NSA de SonicWALL, desde el NSA-240, líder en desempeño para PyMEs, hasta el NSA E-7500 de clase empresarial, sistema de 16 núcleos con más de 5.6 Gbps en estado de rendimiento.

Para mayor información visite: <http://www.sonicwall.com> en donde encontrará el e-Book: "10 magníficas acciones que su firewall debería hacer" (en inglés).

Para mayor información, por favor contacte a:

Gerardo Melgoza
Regional Manager
Mexico & Central America

gmelgoza@SonicWALL.com

Phone :+52 (55) 28810371

Av. Patriotismo # 229 8° Piso

Col. San Pedro de los Pinos

C.P. 03800 México D.F., México

Visite: www.sonicwall.com

Acerca de SonicWALL

SonicWALL es una empresa comprometida con la mejora del rendimiento y la productividad de los negocios de cualquier tamaño proporcionándoles una ingeniería de seguridad de red sin los costos y la complejidad de antes. Actualmente se han vendido más de un millón de dispositivos SonicWALL a través de la red global de diez mil partners de canal para mantener los datos de más de diez millones de empresas a nivel mundial seguros y bajo control. Entre las soluciones premiadas de SonicWALL se incluyen seguridad de red, acceso remoto seguro, seguridad de contenidos, backup y recuperación y tecnologías de gestión y políticas. Para más información, visite la página web <http://www.sonicwall.com>

NOTA: SonicWALL es una marca registrada de SonicWALL, Inc. Otros productos y nombres de empresas mencionados aquí pueden ser marcas registradas de sus respectivas compañías.