



Nota de Prensa

SONICWALL DA UNA VISIBILIDAD SIN PRECEDENTES EN LA ACTIVIDAD DE RED CON EL NUEVO FIREWALL DE APLICACIÓN

Permite control y conocimiento de aplicación sobre la línea de producto NSA de SonicWALL

Madrid, 2 de diciembre de 2008.- SonicWALL, Inc. (NASDAQ: SNWL), compañía líder en infraestructuras de red seguras, anuncia la disponibilidad inmediata del "*Application Aware Firewalling*" para los firewall NSA de última generación de SonicWALL. Este avance, conocido como **firewall de aplicación**, mejora radicalmente la productividad y la seguridad de las redes mediante la desmitificación del control y del acceso de aplicación, que proporciona una visibilidad sin precedentes en la actividad de la red. El firewall de aplicación identifica y clasifica aplicaciones, proporciona visibilidad en aplicaciones específicas y acceso a los contenidos de usuarios, y automatiza la respuesta apropiada ante cualquier riesgo, mejorando drásticamente el control y el cumplimiento de políticas de las redes actuales.

A diferencia de los firewalls tradicionales que solo inspeccionan puertos y protocolos, el firewall de aplicación permite identificar y clasificar fácilmente así como mejorar las políticas basadas en el contenido específico de la aplicación. Estas características proporcionan un mayor control de la política granular a los administradores, determinando el acceso a contenidos y aplicaciones a usuarios específicos, sin tener en cuenta los puertos y aplicaciones. Mientras la mayoría de dispositivos UTM proporcionan exclusivamente opciones de logging y bloqueo, el firewall de aplicación proporciona a los administradores una lista de acciones predefinidas y a medida que permiten la gestión de aplicación de ancho de banda y soporte para mensajes de usuarios y clientes además de actualizaciones en las firmas de forma regular.

Las principales características del firewall de aplicación incluyen:

- **Aplicación de gestión de ancho de banda:** permite a los administradores controlar en qué se destina el uso del ancho de banda basado en aplicación. Este control proporciona la elección de bloqueo de aplicación, limitando el ancho de banda que la aplicación puede utilizar o garantizando su compromiso de ancho de



banda. Además, las políticas de gestión pueden ser aplicadas en función del tiempo y fecha y por usuario o grupos. Los ejemplos incluyen limitación de ancho de banda para aplicaciones de audio y video streaming durante la jornada laboral o el compromiso de productividad del ancho de banda de usuarios específicos de aplicaciones basadas en ventas por trimestres.

- **Identificación de aplicación, bloqueo y notificación:** los administradores pueden ahora identificar fácilmente aplicaciones específicas, bloquear a sus usuarios, y seguidamente notificar de forma automática al usuario al tiempo que la aplicación es bloqueada. Por ejemplo, una organización tiene que desear detectar y controlar una única aplicación o un grupo de aplicaciones que operan en una variedad de puertos abiertos a través del firewall. El firewall de aplicación puede detectar un intento de uso de estas aplicaciones, bloquear su uso y después notificar automáticamente al usuario final con un mensaje apropiado. Esto mejora el uso de políticas de aceptación mientras se incrementa la productividad de los recursos de red y los empleados. Además, el administrador puede elegir aplicar dichas políticas a un grupo de aplicaciones. Pueden crear su propio grupo o utilizar un grupo definido de aplicaciones SonicWALL (por ejemplo Peer-to-Peer), con las firmas de aplicación de grupos SonicWALL definidos regularmente y actualizados automáticamente por SonicWALL. El uso de grupos definidos ahorra tiempo en la creación y mantenimiento de políticas de mejora e identificación de aplicaciones.
- **Control y concienciación en los datos:** el firewall de aplicación además puede analizar datos, incluyendo transferencia de datos ftp, adjuntos en los emails y contenidos basados en buscadores. Las normas establecidas en las políticas pueden ser implementadas para identificar contenidos específicos y llevar a cabo la acción apropiada. Entre los ejemplos se incluyen bloqueo de tráfico de salida basado en web que contiene la frase "confidencial de la compañía" o notificar a las TI cuando los archivos FTP que son transferidos contienen nombres de proyecto específicos. Las notificaciones al remitente pueden ser generadas automáticamente si se desea y se pueden aplicar normas basadas en datos, tiempo, usuarios/grupos y más.

"El firewall de aplicación es más que simplemente un UTM mejorado," afirma Patrick Sweeney, vicepresidente de seguridad de red de SonicWALL. "El firewall de última generación proporciona la seguridad de red líder del mercado por capa de aplicación, proporcionando una herramienta de gestión de aplicaciones y amenazas todo en uno. El



firewall de aplicación permitirá a los administradores proteger la infraestructura completa contra amenazas y gestionar el uso de aplicaciones y ancho de banda, algo que antes hubiese sido prácticamente imposible."

El firewall de aplicación de SonicWALL, junto con la tecnología UTM, y el rendimiento líder del mercado del firewall NSA, permite a los clientes no solo proteger la red completamente, sino mejorar la gestión de los negocios. Además de la capacidad de gestión de amenazas, la capacidad del firewall de distinguir rápidamente entre aplicaciones seguras y dañinas mejora la productividad del negocio en general – no solamente la productividad dentro de los departamentos de TI.

El firewall de aplicación está disponible en todos los sistemas SonicWALL NSA desde el NSA 240, el rendimiento líder para PYMES, hasta el E-Class NSA E-7500, nuestro sistema 16-core con hasta 5,6 Gbps de rendimiento stateful.

Para más información, por favor visite www.sonicwall.com.

E-Book: "10 Cool Things Your Firewall Should Do"

Acerca de SonicWALL

SonicWALL es una empresa comprometida en la mejora del rendimiento y la productividad de los negocios de cualquier tamaño proporcionándoles una ingeniería de seguridad de red sin los costes y complejidad anteriores. 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/>.

Para más información

BELL COMUNICACIÓN

Silvia Peralta

speralta@bellcomunicacion.com

Tel: 91 742 96 79