

**Tecnología Stream Scanning
de NETGEAR®**

Introducción

La proliferación de las tecnologías Web 2.0 ha incrementado de forma significativa la importancia que supone Internet para las pequeñas y medianas empresas. Sin embargo, también ha alimentado una gran variedad de estrategias de ataques. Los agresores se nutren de las ventajas que ofrece una conectividad masiva asociada a la confianza entre usuarios. Los sites peer-to-peer fomentan el compartir grandes ficheros entre extraños. Una práctica común es aceptar descargarse un plug-in de navegación para poder visualizar una página web específica. Infinidad de páginas populares de la red social han enseñado a muchos usuarios que acceder a los links incluidos en los e-mails es completamente seguro. Este incremento en comportamientos familiares han creado nuevos caminos a explotar por los agresores.

De acuerdo a un reciente estudio Gartner, en el año 2007 el número de amenazas basadas en Web se incrementaron en un 800 por cien y había más de 275 plug-ins de navegación vulnerables. Otro estudio reciente encontró que el 79 por ciento de las amenazas basadas en Web se alojaban en páginas legítimas que habían sido pirateadas por hackers que habían infectado la página. El 21 por ciento restante se encontró en páginas que parecían legítimas pero no lo eran, utilizando el marketing vía email como forma principal de dirigir los ataques a sus usuarios.

El Reto

Internet se ha convertido en la herramienta esencial en las operaciones diarias para pequeñas y medianas empresas. El 90 por ciento de los accesos se realizan por e-mail y Web como principales aplicaciones. Aunque muchas empresas son conscientes de que algunas variedades de software malicioso puede acceder a su red a través del tráfico Web, pocas se dan cuenta de la magnitud del problema.

Las empresas de seguridad reciben un promedio de más de 20.000 ejemplos de programas malignos cada día, y más de la mitad de todas las amenazas a la red que reciben han utilizado como vehículo HTTP. En un gran número de casos el usuario sólo necesita visitar una página Web o visualizar un e-mail para ser infectado con troyanos o softwares espía basados en Web. El e-mail también es una fuente de programas malignos y se usa frecuentemente para enviar a sus usuarios ataques basados en Web.

Este incremento en el número de amenazas basadas en Internet ha suscitado la necesidad de tener una robusta solución de Gateway de Seguridad que escanee tanto el tráfico entrante como el saliente para detectar y eliminar las amenazas antes de que lleguen a cada usuario de la red. Sin embargo una seguridad total y una red informática históricamente siempre se han llevado mal, debido a la relación intrínsecamente inversa entre seguridad y rendimiento. Los usuarios necesitan velocidad, sobre todo cuando se está navegando por Internet. Si una solución Web dota de demasiada latencia a la red, los usuarios serán los primeros en quejarse.

Escaneado tradicional basado en Batch (Lotes) versus la tecnología Stream Scanning

La mayoría de las soluciones de seguridad, desde la seguridad a nivel de puestos hasta los dispositivos Gateway, usan la tecnología de escaneado basada en lotes. Esto quiere decir que el escaneado comienza sólo después de que el archivo se haya recibido completamente, y la salida comienza solo después de que el fichero se haya escaneado completamente (ver imagen 1). Como resultado, los usuarios frecuentemente experimentan retrasos y algunas veces vencimiento del tiempo de espera mientras el fichero es escaneado y transferido.

El escaneado basado en lotes se desarrolló en una época en la que los virus se transmitían a través de un medio intercambiable. Por ello empleaba algoritmos basados en la presunción de que la zona a escanear podría ser accesible de forma aleatoria. Esta tecnología era tremendamente efectiva para este tipo medio. Sin embargo, cuando se aplica a amenazas basadas en Internet con tráfico Web en tiempo real, este tipo de escaneado produce unos niveles de latencia inaceptables.

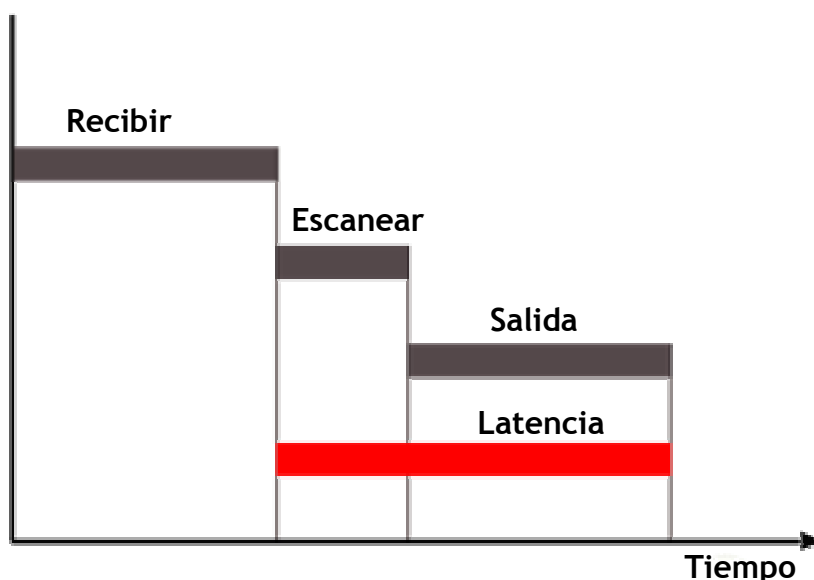


Imagen 1: Escaneado tradicional basado en Lotes

Por el contrario, la tecnología Stream Scanning está basada en la observación de que el tráfico de la red viaja a través de corrientes de información. En vez de esperar a recibir el fichero completamente, el motor de Stream Scanning de NETGEAR comienza a recibir y escanear el tráfico en el momento en que este flujo entra en la red (ver imagen 2). Cuando se recibe un pequeño número de bites, comienza el escaneo. El motor continúa su operación en cuanto recibe más bites, mientras que por otro lado se envían los bites ya escaneados. Esta forma de escaneo permite completar la operación con un impacto mínimo en el rendimiento de la red. El escaneo de un fichero se realiza más rápidamente que utilizando las soluciones de seguridad tradicionales y con un visible incremento en el rendimiento de la red. La tecnología Stream Scanning de NETGEAR es altamente escalable así que el rendimiento irá aumentando a medida que el volumen de tráfico aumente. De este modo las empresas pueden ser capaces de resistir puntos significativos en el tráfico de su red, en caso de que se produzca un brote de amenazas basadas en Internet

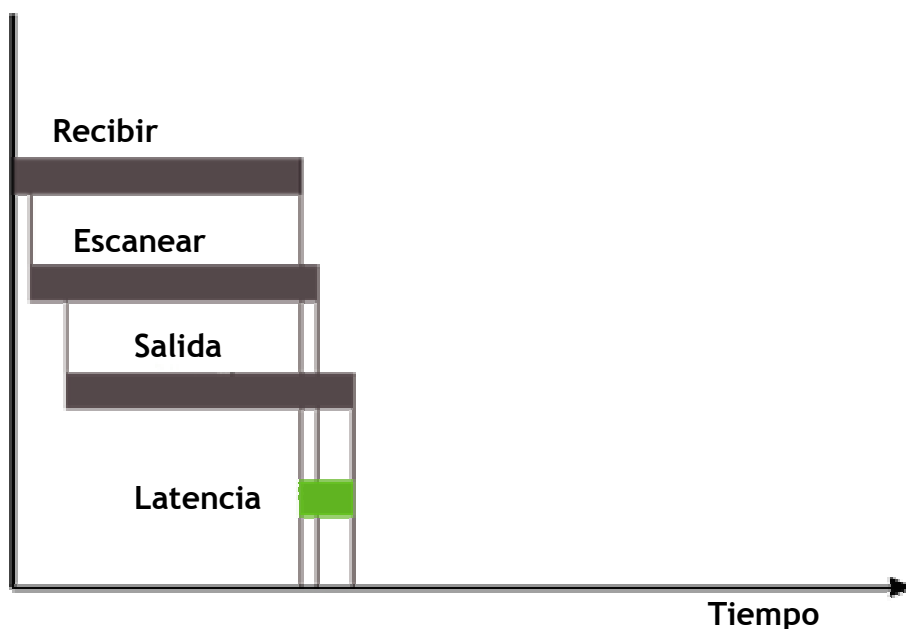


Imagen 2: Tecnología Stream Scanning de NETGEAR®

En una completa prueba de referencia, la tecnología Stream Scanning de NETGEAR trabajó de forma consistente y 5 veces más veloz que las soluciones tradicionales basadas en lotes. Se ha implementado de forma satisfactoria en un gran número de empresas, desde empresas gubernamentales a sanidad o ventas, con implementaciones que van desde pequeñas empresas con menos de 50 usuarios a redes dispersas geográficamente con cientos de usuarios. La tecnología Stream Scanning de NETGEAR ofrece una protección completa y es la solución más completa de su generación contra la amenazas basadas en Web y e-mail con una latencia mínima.

Conclusión

En los actuales entornos de negocio dinámicos, las pequeñas y medianas empresas necesitan un equilibrio entre velocidad de red y seguridad. Las soluciones de seguridad deben mantener a la empresa a salvo del constante aluvión de amenazas basadas en Internet que se producen sin suponer un embotellamiento de las comunicaciones. La arquitectura Stream Scanning de NETGEAR ofrece ese equilibrio. NETGEAR escanea grandes volúmenes de tráfico de la red buscando amenazas de seguridad en tiempo real, sin hacer que las comunicaciones de la empresa se paralicen.

Solución de Gestión ProSecure™ STM contra Amenazas Web y E-mail de NETGEAR®

El dispositivo ProSecure STM utiliza una tecnología única que detecta y bloquea las intrusiones basadas en un comportamiento de distribución rápido y a gran escala. De este modo se puede detectar intrusiones de spam y programas malignos tan pronto como se produzcan y bloquear todos los mensajes asociados en tiempo real.

El dispositivo ProSecure STM con tecnología Stream Scanning, está diseñado para escanear flujos de información a medida que van entrando en la red. NETGEAR STM con la tecnología Stream Scanning es capaz de procesar grandes volúmenes de información en tiempo real, utilizando un simple escáner para identificar spam, programas malignos, brechas de seguridad o aplicaciones innecesarias. Así se asegura que los usuarios de la red reciban su e-mail y los contenidos Web limpios y sin retrasos.

El dispositivo ProSecure STM utiliza un sistema de comportamiento de defensa proactivo que soluciona las vulnerabilidades. La solución NETGEAR utiliza un análisis forense para identificar características sospechosas tanto en el tráfico de entrada como de salida de la red y neutralizarlas hasta que puedan ser examinadas más detenidamente.