



Informe técnico

ActiveArmor y NVIDIA Firewall
Una solución de seguridad de red
basada en hardware





Introducción

Los ordenadores han entrado a formar parte de nuestra vida cotidiana y la proliferación de conexiones a Internet ha hecho que la gran mayoría de los PC ya estén conectados a redes públicas o privadas. Estos PC contienen información extraordinariamente valiosa (datos financieros, empresariales, archivos MP3 o películas) a la que muchas veces se accede mediante operaciones de banca online o servicios de descarga de música y otros contenidos. Lo cierto es que millones de PC están conectados a Internet y esto da a sus usuarios la oportunidad de acceder a la información distribuida por los sitios web de todo el mundo, pero también abre en una puerta de acceso a los piratas informáticos o *hackers*. Sea por diversión o por malicia, los hackers sondean continuamente la red en busca de PC carentes de protección. Las investigaciones de NVIDIA han desvelado que son capaces de encontrar un nuevo PC en la red pública a los pocos minutos de conectarse. Además, existen programas espía que se cargan furtivamente en los PC desprotegidos y envían información sobre el uso del equipo a usuarios no autorizados. Por este motivo, la seguridad del PC ha pasado a ser una de las grandes preocupaciones de la actualidad.

Una de las principales razones por las que los PC son vulnerables a ataques y brechas de seguridad es que están conectados a redes compartidas: hogares con varios PC, redes empresariales e Internet, donde millones de PC están conectados de forma simultánea. Es en este tipo de entornos donde se producen la mayoría de los ataques informáticos, en los que la llegada de paquetes de datos nocivos produce estragos en el PC.

Existen varias soluciones para proteger los sistemas de estos ataques. Una característica habitual de las opciones de seguridad para PC es que están *basadas en el software*, pero este tipo de soluciones consume elevados recursos de la CPU, lo que afecta al rendimiento del sistema en general y perjudica la experiencia de uso. Y contrariamente a la creencia general, añadir ciclos de reloj a la CPU no resuelve el problema, porque muchos ataques son bastante sofisticados y sortean o desactivan las soluciones de seguridad exclusivamente basadas en software.

En este documento se explican las ventajas de la solución de seguridad para red de NVIDIA, que forma parte de sus procesadores de comunicaciones y contenidos multimedia (MCP) nForce™ 4. Esta solución incluye NVIDIA Firewall 2.0, un cortafuegos basado en hardware, y la tecnología NVIDIA ActiveArmor™, el primer motor de seguridad de red dedicado.

NVIDIA ActiveArmor: motor de seguridad para red

ActiveArmor es un motor de seguridad de red integrado en la nueva familia de procesadores MCP nForce4 de NVIDIA. Se trata de una parte del chip dedicada a mejorar la seguridad del PC y, al mismo tiempo, reducir la carga de trabajo de la CPU, para lo cual comprueba exhaustivamente las conexiones y el tráfico de la red a velocidades Gigabit Ethernet.

Este nuevo motor ofrece el máximo rendimiento del sistema, ya que realiza en el hardware el trabajo de filtrado de paquetes normalmente reservado a la CPU, lo que proporciona un entorno de red a la vez rápido y seguro

NVIDIA Firewall y el motor ActiveArmor

La seguridad de los sistemas depende de tres componentes interdependientes: el cortafuegos (también llamado firewall), la detección de intrusos y los sistemas antivirus (para obtener más información sobre los componentes de seguridad de un PC, consulte el informe técnico: “NVIDIA Firewall– Seguridad del PC y defensa contra intrusos”, TB-01147-001).

El cortafuegos es un componente esencial para cualquier solución de seguridad informática. Sirve para garantizar que sólo entrarán en el sistema los paquetes de datos que cumplan unas normas preestablecidas. Para conseguirlo, el cortafuegos examina cada paquete que intenta atravesarlo y determina si posee los atributos permitidos y, en caso negativo, le impide el paso. *Este proceso consume muchos recursos de la CPU y puede degradar enormemente el rendimiento del sistema.*

La solución para evitar la sobrecarga de la CPU es introducir un motor de hardware en el proceso. Cuando la función de cortafuegos se combina con un motor de hardware dedicado, no se produce ninguna pérdida de rendimiento.

El primer cortafuegos del mercado auténticamente basado en hardware es NVIDIA Firewall 2.0, que ahora utiliza el motor de seguridad ActiveArmor para realizar sus funciones. La combinación del cortafuegos de NVIDIA y el motor ActiveArmor (Figura 1) mejora la velocidad de transferencia del tráfico de red (hasta velocidades Gigabit Ethernet en modo full duplex), reduce el índice de utilización de la CPU y realiza un examen exhaustivo de los paquetes, con lo que mejora la seguridad global del PC en la red.

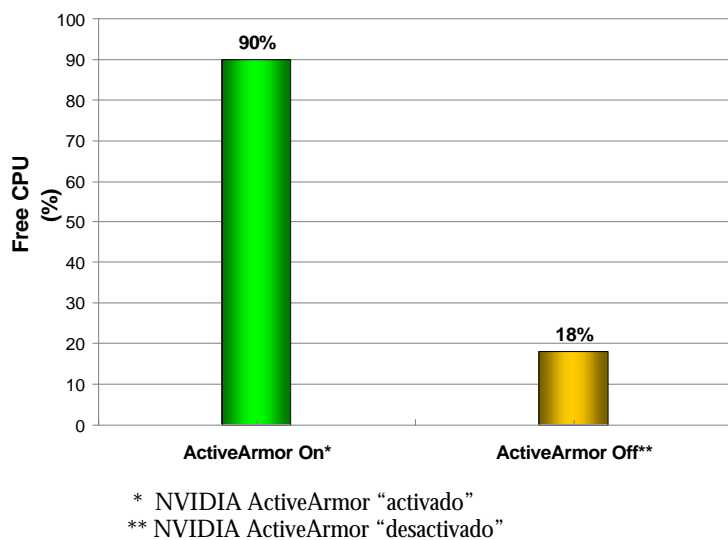


Figura 1. Los cortafuegos basados en software consumen muchos recursos de la CPU

Menor utilización de la CPU

En los entornos de red comunes, la revisión de los paquetes es un proceso laborioso que afecta a la carga de trabajo de la CPU, el ancho de banda de la memoria y la latencia global del sistema (Figura 2). Por ejemplo, los paquetes se trasladan de la conexión MAC al controlador, de aquí a la pila del espacio del kernel y de ahí a la aplicación, lo que implica atravesar la frontera entre el kernel y el espacio de usuario. Todas estas operaciones de copia en memoria consumen mucho tiempo y representan una pesada carga para la CPU, y el procesamiento que se produce en el controlador y la pila entre una copia y otra utiliza un número excesivo de ciclos de la CPU.

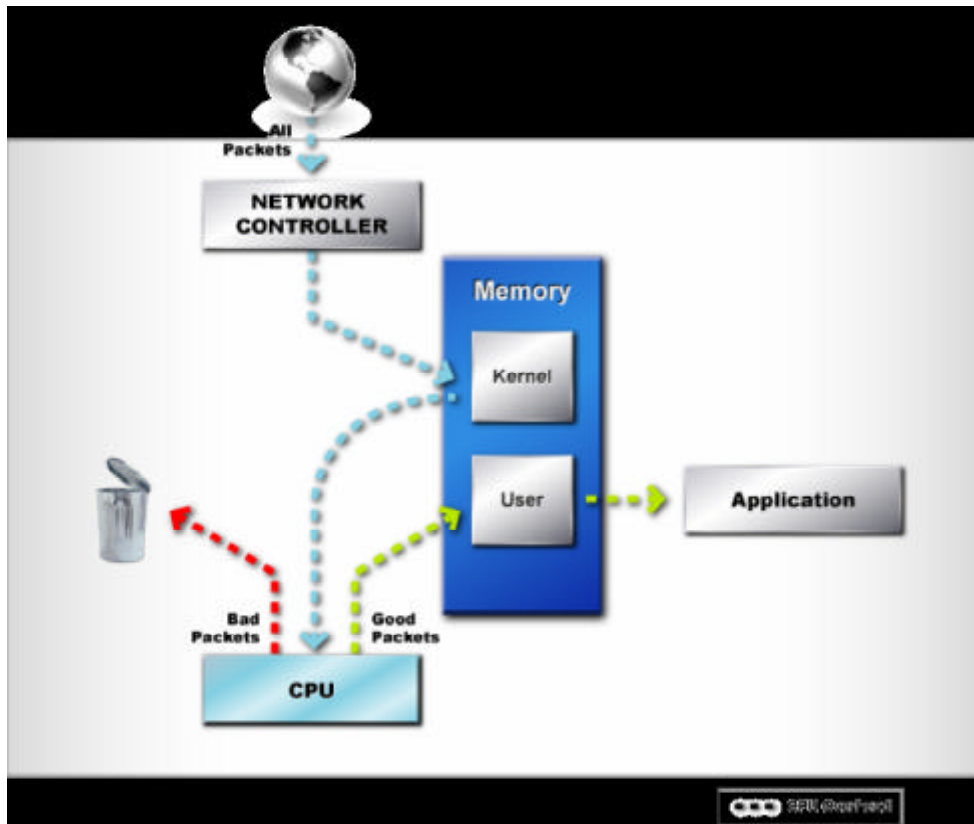


Figura 2. Procesamiento de paquetes en la actualidad

Por el contrario, el motor ActiveArmor descarta los paquetes nocivos antes de que la CPU llegue a verlos. Además, los paquetes seguros utilizan una “vía rápida” y sortean el proceso de la “pila de protocolos de red” habitual, con lo que mejora la velocidad de transferencia global y se reduce el índice de utilización de la CPU (Figura 3). Con ActiveArmor, el trabajo de procesamiento de los paquetes autorizados se traslada directamente a la memoria de la aplicación, lo que evita hasta tres operaciones de copia que sobrecargan bastante a la CPU (de la MAC al controlador, del controlador a la pila del espacio del kernel y de la pila a la aplicación, lo que implica atravesar la frontera entre el kernel y el espacio de usuario).

ActiveArmor procesa todas las cabeceras de los protocolos relevantes y las coteja con la lista de conexiones permitidas y el estado más reciente de la conexión, de forma que únicamente se acepte el paso de paquetes válidos desde (o hacia) la red.

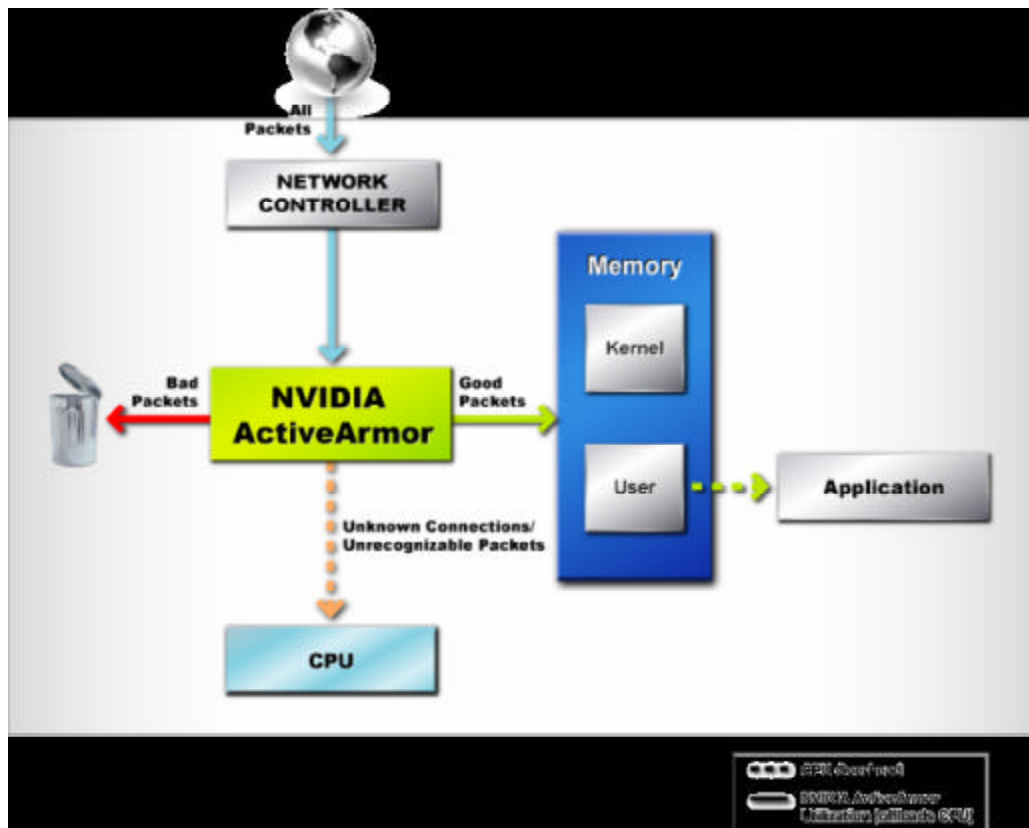


Figura 3. Procesamiento de paquetes con ActiveArmor

Al examinar los paquetes mediante el hardware y transferirlos directamente a los buffers de la aplicación, ActiveArmor proporciona la solución de seguridad más rápida y eficiente disponible para cualquier PC conectado en red.

Pero, además de su eficacia en el filtro de paquetes, el motor de seguridad de NVIDIA proporciona otras tres funciones esenciales: protección instantánea, resistencia a la manipulación y soporte de la arquitectura TCP Chimney de Microsoft.

Protección instantánea

La solución de seguridad de NVIDIA ofrece protección instantánea de la conexión de red desde el momento en que se enciende el PC. No existe ningún espacio de tiempo entre el encendido del sistema y la activación del cortafuegos en el PC. Esta inmediatez se consigue *integrando* el procesamiento del controlador y el cortafuegos directamente en el MCP nForce.

Por el contrario, otras soluciones basadas en software sí introducen un lapso de tiempo entre el encendido del sistema y la carga del software de seguridad en la memoria. Esto basta para que los hackers, que constantemente exploran la red en busca de equipos desprotegidos, inicien su ataque.

Reforzamiento de la seguridad y resistencia a la manipulación

Frente otras soluciones de seguridad, ActiveArmor ofrece una comprobación exhaustiva del tráfico de red que permite filtrar cualquier paquete sospechoso o no autorizado.

Este nivel de examen y filtrado sólo puede conseguirse mediante un motor de hardware dedicado que reporta tres grandes ventajas:

- ❑ Mejora el nivel de seguridad al permitir un examen más profundo de los paquetes mediante el hardware.
- ❑ El aumento de la seguridad se consigue sin perjudicar el rendimiento de la CPU ni el sistema.
- ❑ Es resistente a la falsificación o la manipulación. Cualquier intento de desactivar o manipular las normas del control y filtrado del cortafuegos desactiva la conexión de red para proteger el PC de accesos no autorizados.

Soporte de la arquitectura TCP Chimney de Microsoft

NVIDIA ActiveArmor es totalmente compatible con la nueva arquitectura TCP Chimney de Microsoft, que acelera el procesamiento de los protocolos TCP/IP. Al integrar una norma de filtro del firewall en la arquitectura TCP/IP Chimney, NVIDIA ofrece dos importantes ventajas: menos trabajo de la CPU para procesar el tráfico TCP/IP y el reforzamiento de las normas de seguridad mediante un motor que garantiza el paso (de entrada o salida) únicamente al tráfico autorizado.


ActiveArmor y la familia de MCP nForce4 MCP son unos de los primeros productos de la industria en incorporar soporte para esta nueva API de Microsoft, con lo que consolida su liderazgo en este mercado.

Conclusiones

Las actuales soluciones de seguridad para PC están basadas en software y consumen numerosos recursos de la CPU, con lo que se convierten en una fórmula que trata de buscar un compromiso entre seguridad y rendimiento.

Pero cuando se trata de la seguridad, no debería haber compromisos. Los usuarios de PC necesitan tener el mejor rendimiento del sistema sin perjuicio de la seguridad.

El enigma de cómo compatibilizar ambos aspectos se ha resuelto con la introducción del motor de seguridad de NVIDIA, un motor de hardware dedicado que mejora la seguridad de las conexiones de red porque realiza un examen exhaustivo de los paquetes al tiempo que descarga a la CPU del arduo trabajo de procesar y filtrar el tráfico de red. El resultado es una mejora de la seguridad y del rendimiento global del sistema.



Aviso legal

TODAS LAS ESPECIFICACIONES DE DISEÑO DE NVIDIA, PLACAS DE REFERENCIA, ARCHIVOS, DIBUJOS, DIAGNÓSTICOS, LISTAS Y OTROS DOCUMENTOS (DENOMINADOS CONJUNTAMENTE O POR SEPARADO "MATERIALES") SE ENTREGAN "TAL CUAL". NVIDIA NO OFRECE NINGUNA GARANTÍA EXPRESA, IMPLÍCITA, ESTATUTARIA O DE OTRA NATURALEZA CON RESPECTO A LOS MATERIALES Y RECHAZA EXPRESAMENTE CUALQUIER GARANTÍA IMPLÍCITA DE COMERCIABILIDAD, NO INFRACCIÓN O ADECUACIÓN A ALGÚN PROPÓSITO EN PARTICULAR.

NVIDIA Corporation considera que la información suministrada es exacta y fiable, pero no asume responsabilidad alguna por las posibles consecuencias o infracciones de derechos sobre patentes, u otros derechos de terceras partes, que pudieran derivarse de su uso. NVIDIA no otorga licencia alguna por implicación, ni de ningún otro modo, bajo ninguna patente o derecho de patente de NVIDIA Corporation. Las especificaciones mencionadas en esta publicación son susceptibles de cambios sin previo aviso. El contenido de este documento sustituye y prevalece sobre cualquier otra información anteriormente suministrada por NVIDIA. No se autoriza el uso de los productos de NVIDIA Corporation como componentes esenciales de dispositivos o sistemas de apoyo o sostenimiento de la vida sin el permiso previo y por escrito de NVIDIA Corporation.

Marcas comerciales

NVIDIA, el logotipo de NVIDIA, ActiveArmor y NVIDIA nForce son marcas comerciales y/o marcas registradas de NVIDIA Corporation en los Estados Unidos y en otros países. Otras empresas y productos pueden ser marcas comerciales y/o registradas de sus respectivos propietarios.

Copyright

© 2004 de NVIDIA Corporation. Quedan reservados todos los derechos.



NVIDIA.

NVIDIA Corporation

2701 San Tomas Expressway

Santa Clara, CA 95050

www.nvidia.com