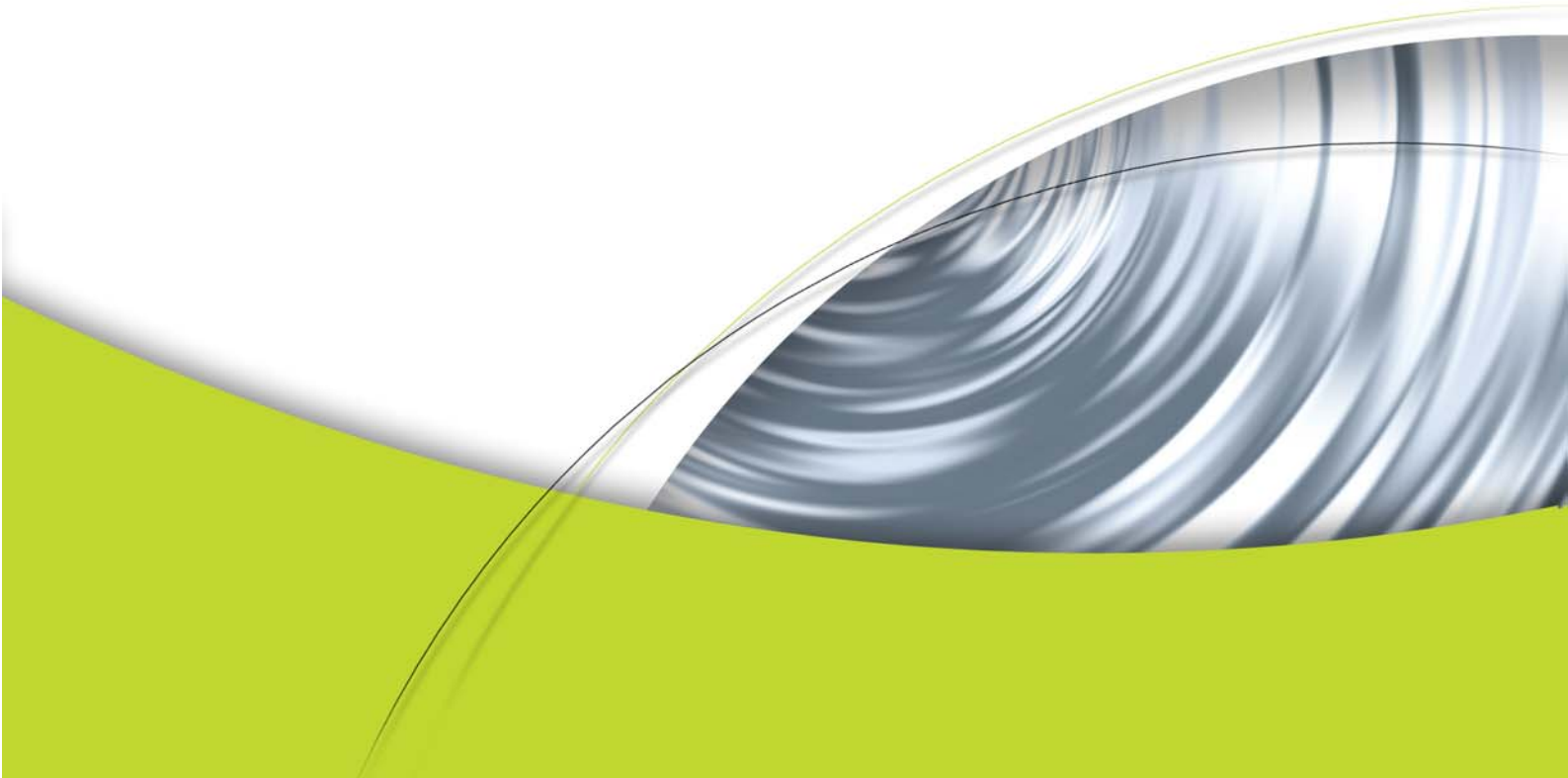




# Informe técnico

## NVIDIA Firewall

Seguridad del PC y defensa  
contra intrusos



# Seguridad del PC y defensa contra intrusos

---

## Introducción

Los ordenadores han entrado a formar parte de nuestra vida cotidiana y pueden contener información importante que se ha convertido en uno de los primeros objetivos de los piratas informáticos o hackers. Por este motivo, la seguridad de los ordenadores ha pasado a ser uno de los principales retos de la actualidad.

La seguridad de los sistemas depende de tres componentes interdependientes: el cortafuegos (también llamado firewall), la detección de intrusos y los sistemas antivirus.

El cortafuegos es el 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. Cuando los controladores del PC incluyen funciones de cortafuegos, se reduce drásticamente el acceso no autorizado al sistema por parte de intrusos procedentes de la intranet o Internet.

El de NVIDIA es el primer cortafuegos basado en el motor de seguridad de red NVIDIA ActiveArmor™, lo que proporciona el máximo rendimiento con el índice más bajo de utilización de la CPU. Al mismo tiempo mejora la seguridad global del sistema porque ofrece un cuidadoso filtro de paquetes basado en hardware, protección instantánea y funciones para combatir la falsificación y manipulación de paquetes.

---

## Cortafuegos

### Para qué sirven

Los datos que atraviesan las redes se componen de paquetes cuyas cabeceras contienen información sobre los propios paquetes, es decir, metadatos. Los metadatos proporcionan la información necesaria para enviar el paquete a una subred (cabecera de la capa de enlace), a otra red (cabecera de la capa de red) y al proceso correcto dentro de un sistema (cabecera de la capa de transporte). Cuando una máquina está conectada a Internet, cualquier otra máquina también a conectada a esta red puede enviarle paquetes si conoce la dirección IP de la máquina de destino.

La mayoría de los paquetes son inocuos, pero, en ocasiones, alguien envía paquetes que tratan de aprovechar posibles defectos del sistema operativo o el software del sistema de destino para, por ejemplo, desactivar ese sistema (lo que se conoce como “ataque de denegación de servicio”) o simplemente acceder a él sin autorización.

La mayoría de las redes empresariales y domésticas tienen una conexión a Internet bien definida que consiste en un número limitado de puntos de conexión (módem DSL) a través de los cuales los sistemas internos pueden enviar y recibir paquetes de Internet. Para controlar qué tipo de paquetes cruzan esta frontera se ha creado el concepto de cortafuegos.

## Cómo funcionan

Los cortafuegos filtran el tráfico de la red utilizando una gran variedad de criterios. El modo más obvio de filtrar el tráfico es por tipo de paquete. El cortafuegos utiliza los números de puerto TCP o UDP de los paquetes para permitirles o denegarles el paso basándose en ciertas normas guardadas en una tabla de control de acceso.

He aquí dos posibles casos de filtro de paquetes:

- ❑ El cortafuegos permite el paso a todos los paquetes excepto los incluidos en una lista (identificados por los números de puerto), que se consideran dañinos y se rechazan.
- ❑ El cortafuegos se programa para bloquear el paso a todos los paquetes de forma predeterminada y dejar pasar únicamente los que se consideran seguros.

La seguridad consiste en saber gestionar el riesgo. Al configurar un cortafuegos, los usuarios limitan el riesgo de que ciertos paquetes entren en su red. Los cortafuegos suelen ser configurables, por lo que resulta difícil para los atacantes averiguar qué tráfico puede traspasarlos. Este sistema ayuda a mantener el grado de privacidad del ordenador al que protege.

## Tipos de cortafuegos

### Sin estado

El cortafuegos sin estado o stateless es el tipo más básico de cortafuegos y ha existido, de una forma u otra, desde principios de los 90. En esta modalidad se definen una serie de normas de permiso/rechazo, de tal manera que sólo pasen los paquetes que cumplan las condiciones adecuadas. Estas normas permiten filtrar el tráfico de entrada o salida en función del tipo de paquete Ethernet, la dirección IP de origen o destino, las opciones IP, el protocolo IP, los valores de tipo y código de ICMP, el puerto TCP o UDP de origen o destino y las opciones TCP.

Si el paquete cumple los criterios, puede atravesar el filtro, de lo contrario, se rechaza. El problema de este enfoque es que todos los paquetes se someten a la misma serie de pruebas, por lo que es necesario comprobar el cumplimiento de las normas con cada paquete. Cuantas más normas se añaden, más trabajo cuesta procesar cada paquete y, por tanto, menor es el rendimiento del sistema en términos de paquetes por segundo o de utilización de la CPU para procesar una determinada cantidad de tráfico. Los cortafuegos sin estado son más adecuados para ciertos tipos de paquetes como los del protocolo ICMP, que son paquetes sin estado.

NVIDIA Firewall puede funcionar con este tipo de enfoque. Es capaz de filtrar el tráfico en función del tipo de paquete Ethernet, el protocolo IP y las opciones de IP y TCP. Cuando es aplicable, IPv4 e IPv6 se tratan de la misma manera. Por ejemplo las opciones de IPv4 y las cabeceras de extensión IPv6 pueden utilizarse como elementos de filtro.

## Con estado

El cortafuegos con estado (stateful) es una variante del cortafuegos sin estado. Se comporta de forma muy parecida a este último cuando se establece una nueva conexión porque compara el nuevo protocolo (además del origen y el destino del paquete) con las normas de acceso establecidas localmente.

La novedad del cortafuegos con estado reside en que los paquetes de un determinado flujo sólo se examinan con detalle cuando se establece la conexión. Cada vez que se permite una conexión nueva, se agrega una entrada a una tabla de seguimiento del estado de las conexiones. Los futuros paquetes que coincidan con esa entrada de la tabla podrán verificarse a través de la tabla de conexiones permitidas, lo que evitará la necesidad de comparar cada paquete con todo el conjunto de normas. La ventaja de este tipo de cortafuegos es que ofrece toda la seguridad del filtro de paquetes pero con un índice de utilización de la CPU muy inferior.

La tecnología Firewall de NVIDIA admite esta modalidad de filtro del tráfico TCP y UDP con estado. El “estado” de UDP se determina observando los nuevos paquetes UDP y creando estados únicamente si cumplen las normas definidas por el usuario en el cortafuegos.

La técnica de comprobación implica el cálculo de un valor hash basado en varios campos clave de la cabecera del paquete. Los campos clave pueden incluir las direcciones IP de origen y destino, el protocolo IP (que indica si se está utilizando TCP, UDP o cualquier otro protocolo de la capa de transporte) y los puertos de origen y destino de la capa de transporte. El cálculo de una función basada en estos cinco valores exige una pequeña cantidad (fija) de tiempo por paquete.

La complejidad de las normas establecidas para el filtro no afecta a la velocidad de validación de los paquetes en el cortafuegos. Por el contrario, el cortafuegos sin estado debe aplicar todas sus normas (o un número suficiente de normas para tomar la decisión de permitir/no permitir el paso) para cada paquete. Además, el tiempo de análisis de los paquetes aumenta linealmente a medida que se incrementan las normas de filtrado, lo que da como resultado una velocidad de transmisión de paquetes que también disminuye linealmente con el aumento de dichas normas.

## Gateways de la capa de aplicación

Un gateway (puerta de acceso) de la capa de aplicación, o puente de la capa de transporte, es un sistema especial que ejecuta servicios proxy para cada aplicación a la que se permite el paso. Estos servidores proxy deben ser excepcionalmente estables y a prueba de ataques, de lo contrario, tendrán sus propias vulnerabilidades. Ningún paquete atraviesa directamente el gateway de la capa de aplicación. Cuando se recibe un paquete, todas sus cabeceras se descomponen, el contenido se examina y se crea una serie de paquetes nueva dentro de otra conexión dirigida al sistema de destino.

El gateway es tan transparente como el cortafuegos de filtro de paquetes, excepto por el hecho de que puede producir más retrasos en el proceso de examen. La ventaja de este enfoque es que existe una “pared” lógica entre las dos redes, pero sólo para los protocolos que el gateway entiende.

La mayor limitación de este gateway es que, para que pueda pasar cierto tipo de tráfico, debe existir un servidor proxy para ese protocolo. Los proxies para

protocolos habituales como SMTP, FTP, HTTP y TELNET son muy frecuentes, pero no es tan fácil encontrar proxies para otros protocolos menos comunes. En cualquier caso, si se utiliza un número limitado de aplicaciones, estos gateways son la mejor opción para garantizar exclusivamente el paso de datos válidos a través del cortafuegos.

Los cortafuegos basados en un gateway de la capa de aplicación se sitúan normalmente en el extremo de la red y requieren el uso de un hardware dedicado. NVIDIA Firewall, como cortafuegos para PC, no incluye funciones de gateway.

## El cortafuegos como defensa antipiratero

Un paquete IP manipulado de forma ilegal ha generado un valor en el campo de dirección IP de origen. Mediante el uso de direcciones IP intencionadamente incorrectas, un hacker puede originar ciertos tipos de ataques. El más conocido es el de denegación de servicio distribuida (DDoS), que también es uno de los tipos más comunes de ataque basado en la falsificación (spoofing) de direcciones IP. Los ataques de denegación de servicio dependen de dos factores: 1) la existencia de un dispositivo “zombi” conectado a Internet, a menudo un PC que ha sido infectado; y 2) la capacidad de ordenar al PC zombi que envíe paquetes con direcciones IP de origen falsas.

Los cortafuegos siempre han sido capaces de filtrar paquetes basados en la dirección IP, pero la detección de paquetes falsos implica un nivel más sutil de discriminación. Por ejemplo, si nos basamos en la dirección IP de origen de un determinado paquete, ¿es posible que ese paquete llegue a una determinada interfaz teniendo en cuenta lo que el cortafuegos sabe sobre la tabla de encaminamiento? Un dispositivo intermedio no puede detectar fácilmente si un paquete ha sido manipulado.

El mejor método para impedir la entrada de paquetes falsificados es bloquearlos en su origen, el PC zombi. Al incorporar la función antispoofing directamente en el hardware y el software de red del PC, se impide que éste utilice cualquier dirección IP que no sea su dirección asignada estáticamente o la dirección asignada por el servidor DHCP.

---

## Otras funciones de seguridad importantes

El cortafuegos proporciona una “capa” de protección que normalmente se considera la capa básica, pero una solución de seguridad completa debe ser multicapa.

La solución Firewall de NVIDIA no proporciona estas capacidades adicionales, pero pueden obtenerse seleccionando los productos del mercado que mejor se adapten a las necesidades del usuario.

## Protección contra intrusos

La detección de intrusos es la capacidad de analizar todo el tráfico entrante para buscar patrones de comportamiento que coincidan con ataques conocidos o con

precursores de ataques conocidos. Por ejemplo, para atacar un componente vulnerable de un software de red, el atacante debe explorar primero todos los puertos posibles para encontrar un ejemplo conocido de componente de software vulnerable. Por tanto, si se detecta una “exploración de puertos”, puede indicar que se va a producir un ataque, lo que permite adoptar medidas de defensa antes de que se produzcan daños.

Pero las técnicas de protección contra intrusos también pueden detectar directamente algunos ataques conocidos y neutralizarlos antes de que afecten a los sistemas.

En ambos casos, los productos de software de detección de intrusos dependen del acceso a una biblioteca de ataques conocidos y normalmente no pueden detectar nuevos ataques porque aún no se ha establecido ninguna “seña” para identificarlos.

## Protección antivirus

Las funciones antivirus evitan que el PC ejecute código que contiene virus conocidos o troyanos. Como en el caso del software contra intrusos, los antivirus se basan en una biblioteca de virus conocidos que el producto sabe cómo contrarrestar.

Además, ciertos antivirus pueden avisar de la presencia de actividades sospechosas, aunque no correspondan exactamente a un virus conocido.

---

## NVIDIA Firewall

El cortafuegos de NVIDIA ahora se basa en el motor de seguridad de red ActiveArmor, lo que lo convierte en el primer firewall de PC del mercado basado en hardware. Gracias a este motor, NVIDIA Firewall no necesita utilizar la CPU para las operaciones.

La solución NVIDIA ActiveArmor Secure Networking (una combinación del cortafuegos de NVIDIA y su motor de seguridad Active Armor) acelera la transferencia de paquetes a velocidades gigabit Ethernet, reduce la utilización de la CPU, realiza un profundo examen de los paquetes y mejora la seguridad global de la red (Figura 1).

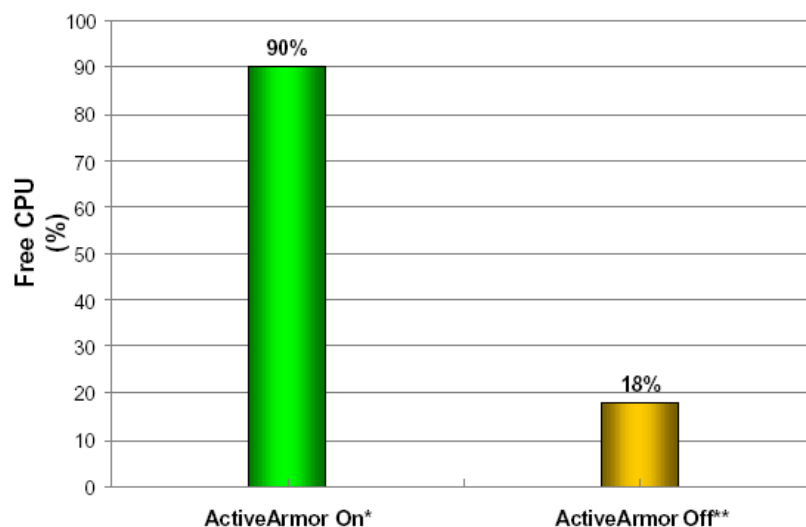


Figura 1. NVIDIA ActiveArmor ofrece máximo rendimiento con mínima utilización de la CPU

**Notas:**

El cortafuegos de NVIDIA incluye funciones de filtro y antipiratero. Asimismo, proporciona filtro de paquetes con y sin estado, gestión basada en navegador, perfiles de seguridad predefinidos, filtro/bloqueo de puertos, un administrador de aplicaciones inteligente (Intelligent Application Manager), administración remota y un asistente de configuración muy sencillo. A esto se añade funciones antipiratero para evitar diferentes tipos de ataques como son la falsificación de direcciones IP (spoofing), la interceptación de contraseñas (sniffing), la manipulación de la caché de ARP y la suplantación de servidores DHCP, todas ellas medidas de seguridad esenciales para las redes corporativas.

En un entorno empresarial, un cortafuegos de PC con funciones antipiratero puede reducir las brechas de seguridad originadas internamente e impedir que los PC generen tráfico no autorizado. El resultado es una mejora global de la seguridad con menos intervención del personal técnico.

## Funciones de gestión avanzadas

La solución Firewall de NVIDIA ofrece numerosas funciones de gestión avanzada que incluyen: acceso remoto, configuración, monitorización, interfaz de línea de comandos (CLI) y scripts WMI. Además, un sencillo asistente facilita su configuración.

Estas funciones de gestión convierten al cortafuegos de NVIDIA en un producto flexible, manejable y muy funcional (Figura 2).

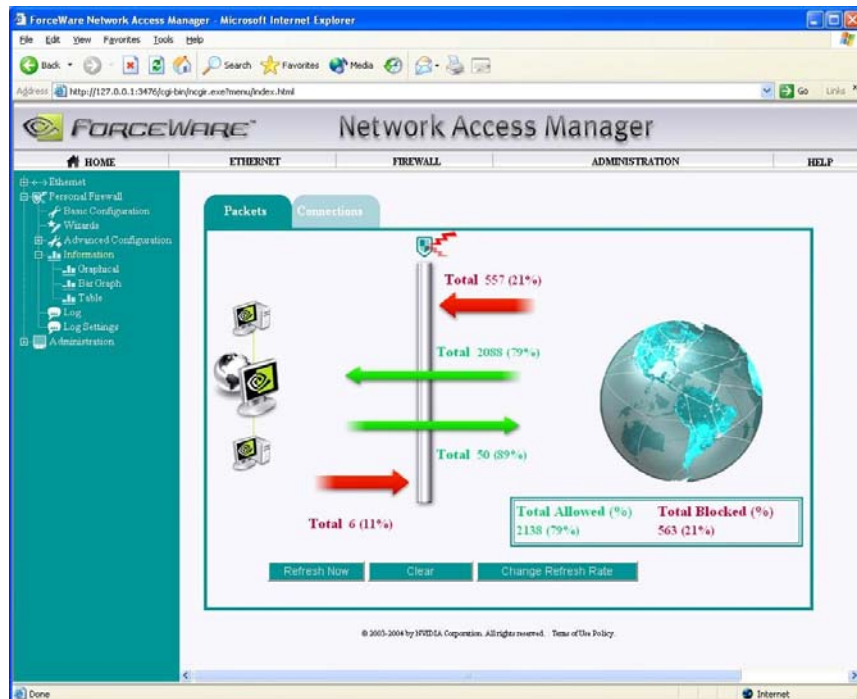


Figura 2. Fácil configuración mediante una interfaz de navegador

## Intelligent Application Manager (IAM)

Intelligent Application Manager (administrador de aplicaciones inteligente) es una nueva función incorporada al cortafuegos de NVIDIA que suma a las completas funciones de filtro del firewall la función de filtro de aplicaciones. IAM amplía los elementos de administración de normas de NVIDIA Firewall para proporcionar filtro basado en aplicaciones, ya sean de tipo cliente o servidor. Además, permite intervenir al usuario, ya que le deja decidir qué aplicaciones pueden acceder o salir del PC con seguridad. Cuando una aplicación se considera segura, puede abrir puertos sin ninguna configuración específica por parte del usuario (Figura 3).

IAM elimina la posibilidad de que una aplicación nociva instalada en el PC del usuario pueda enviar tráfico que ha conseguido atravesar el cortafuegos. El tráfico de salida sólo se permite si procede de una aplicación que el usuario considera segura. Este administrador puede incluso hacer el seguimiento de aplicaciones existentes y determinar si han sido alteradas de alguna forma, por ejemplo, por un

virus, un troyano o una aplicación que haya cambiado su propio nombre para imitar a otra aplicación conocida.

También resulta útil para proteger el PC contra paquetes entrantes, ya que limita la capacidad de los troyanos y otras aplicaciones espía para instalarse automáticamente como servidores en el PC, lo que les impide recibir tráfico externo al sistema. IAM no sólo puede realizar el filtro por puertos, también puede prohibir al servidor que abra puntos de conexión (sockets) para impedir que reciban tráfico en la capa de aplicaciones.

IAM ofrece protección completa del PC contra ataques procedentes de agentes externos y, a su vez, impide que el PC pueda atacar a otros PC.

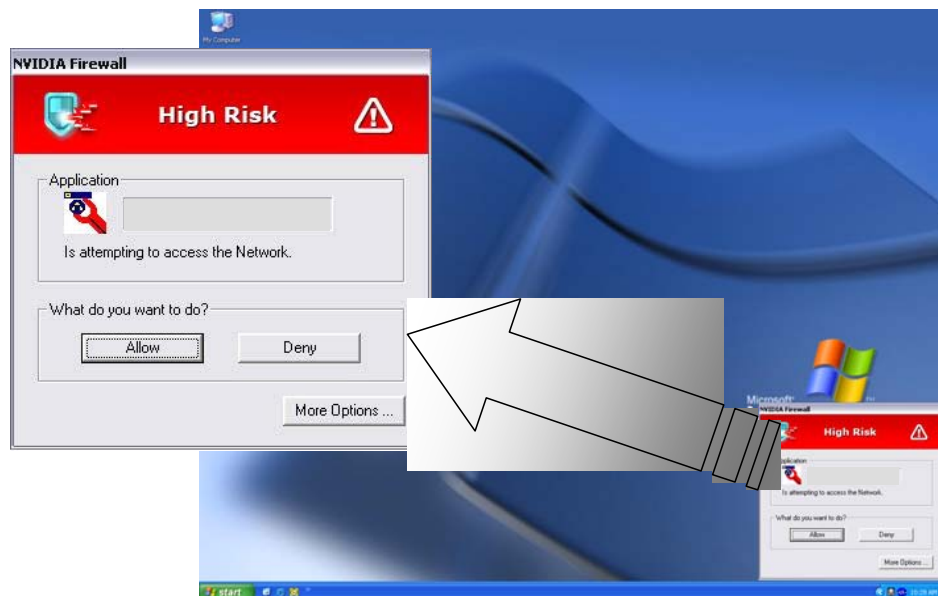


Figura 3. IAM avisa cuando aplicaciones desconocidas tratan de acceder a la red

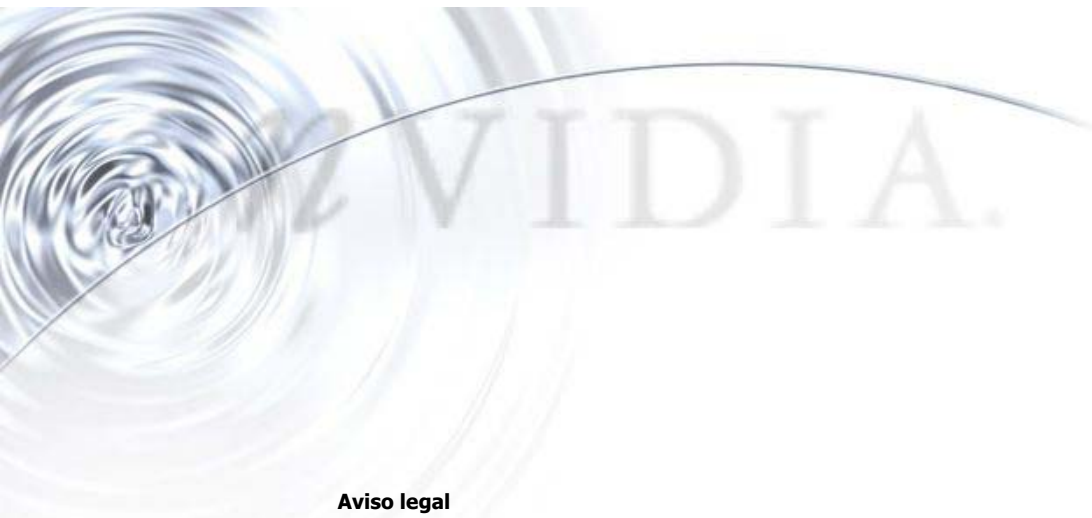
## Por qué elegir NVIDIA Firewall

La mayoría de los cortafuegos de PC del mercado son módulos de software, pero la solución de NVIDIA es el primero auténticamente basado en hardware. La solución de seguridad ActiveArmor de NVIDIA, que consta de NVIDIA Firewall y el motor Active Armor, mejora la seguridad global de la red.

Además, NVIDIA Firewall posee funciones únicas. Incluye la función Intelligent Application Manager (IAM), funciones de gestión avanzadas (configuración, monitorización y acceso remoto) y un asistente que facilita su configuración y

manejo. Puede implantarse en entornos corporativos, como último filtro de protección en los PC de sobremesa, o en PC domésticos con conexión de banda ancha a Internet para proteger el sistema contra accesos no autorizados.

La tecnología NVIDIA Firewall puede ser una poderosa herramienta para utilizarla como barrera básica de acceso, aunque, para obtener una protección total, los usuarios necesitarán complementar las funciones de cortafuegos de NVIDIA con un buen software antivirus y un producto de detección de intrusos que proporcionen una solución de seguridad completa para el PC.



#### **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 y ActiveArmor son marcas comerciales y/o marcas registradas de NVIDIA Corporation en los Estados Unidos y en otros países. Otros nombres de 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](http://www.nvidia.com)