



Technical Brief

ActiveArmor
A Secure Networking Solution



Computers are an integral part of everyday life for business and pleasure. They contain all sorts of valuable information, making them prime targets for hackers. This reality is why computer security is one of the most important issues facing users today.

One of the main reasons PCs are vulnerable to security breaches and attacks is that they are connected to *shared* networks—either homes with multiple PCs; workplace environments; or the Internet, where millions of PCs are simultaneously connected. Most computer attacks occur within these environments, allowing harmful data packets to reach unprotected PCs and wreck havoc.

Many solutions exist for protecting PCs from attacks. A common characteristic of most PC-based security solutions is that they are *software-based*. However, software solutions are very CPU intensive, which affects overall system performance and degrades the user experience. And contrary to popular belief, adding more CPU cycles does not solve the problem, because many attacks are sophisticated and bypass or disable software-only security solutions.

The NVIDIA® ActiveArmor™ secure networking solutions include two components:

- ❑ The ActiveArmor Secure Networking Engine (SNE), the industry's first dedicated processor for accelerating firewall processing
- ❑ The hardware-optimized ActiveArmor Firewall 2.0

This paper details the benefits of the ActiveArmor secure networking solutions integrated into the latest NVIDIA nForce™ media and communication processors (MCPs).

ActiveArmor Secure Networking Engine (SNE)

The NVIDIA ActiveArmor Secure Networking Engine is integrated into the new NVIDIA nForce4 SLI™ and NVIDIA nForce4 Ultra families. A dedicated portion of the silicon that enhances networking security while reducing CPU overhead, the ActiveArmor Secure Networking Engine accelerates ActiveArmor Firewall and provides deep levels of networking and traffic inspections at full-duplex gigabit Ethernet speeds.

ActiveArmor SNE delivers the highest system performance by offloading CPU-intensive packet filtering tasks in hardware, providing users with a PC networking environment that is both fast and secure.

ActiveArmor Firewall 2.0

Computer security has three independent components: a firewall, intrusion detection, and antivirus protection. (For more information on the computer security components, please refer to “ActiveArmor Firewall: PC Security and Hacker Defenses,” TB-01147-001_v04).

A firewall is the core component of a computer security solution. It ensures that only data packets that comply with the defined policies get through. To provide this protection, the firewall examines each data packet that attempts to pass through and determines if the packet has permissible attributes; if it doesn't, the firewall blocks the packet. *This is a very CPU-intensive process and can dramatically degrade system performance.*

To solve the CPU-intensive problem, we introduced a hardware engine into the process. Why? Because when firewall functionality is coupled with a dedicated hardware engine, there is little performance degradation. The industry's first true hardware-optimized PC firewall is NVIDIA ActiveArmor Firewall 2.0, which is now powered by the NVIDIA ActiveArmor secure networking engine.

The combination of the ActiveArmor Firewall and the ActiveArmor secure networking engine improves network throughput (at full-duplex gigabit Ethernet speeds), lowers CPU utilization, and performs deep packet inspection, thereby improving overall network security.

Reduced CPU Utilization

In traditional networking environments, inspecting packets is laborious and affects CPU overhead, memory bandwidth, and overall system latency (Figure 1). For example, packets move from MAC to driver; from driver to stack within kernel space; and from stack to application, crossing the kernel-space/user-space boundary. All those memory copy operations are CPU intensive and time consuming, and the driver and stack processing that occurs between the copies uses an excessive number of CPU cycles.

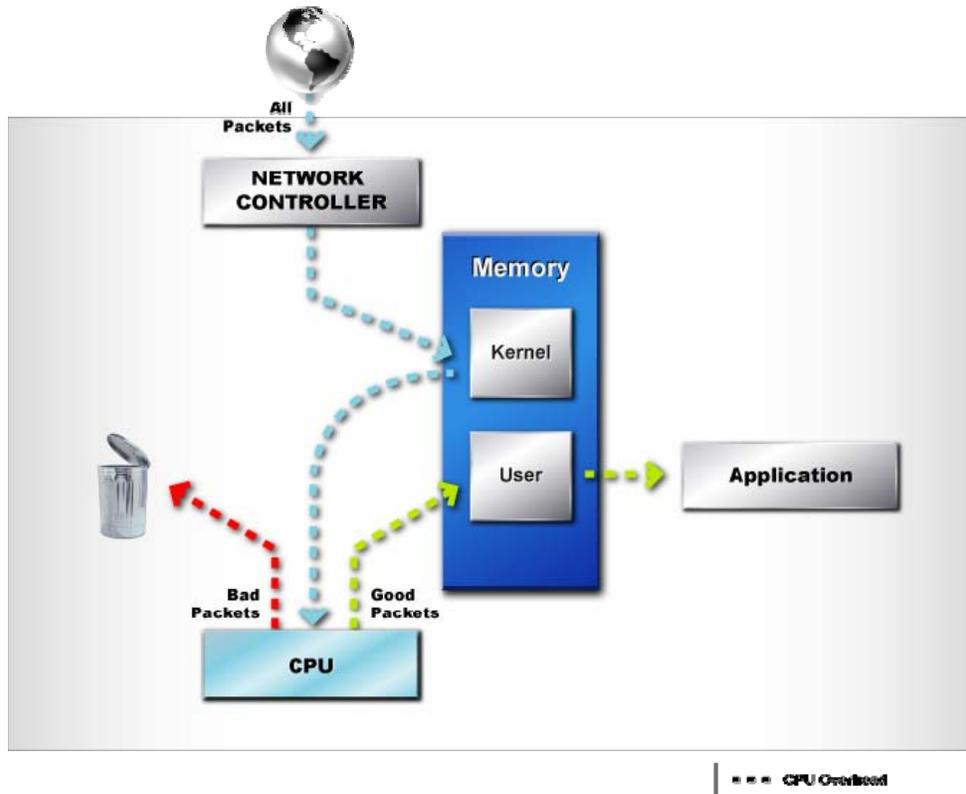


Figure 1. Current Packet Processing

In comparison, the ActiveArmor secure networking engine discards bad packets before the CPU sees them. Plus, good packets take an “express lane” and bypass the traditional “network stack” process, improving overall throughput and lowering CPU utilization (Figure 2). With ActiveArmor, the payload of all good packets is placed directly into application memory, which avoids up to three CPU-intensive copy operations (from MAC to driver; from driver to stack within kernel space; and from stack to application, which involves crossing the kernel-space/user-space boundary).

The ActiveArmor secure networking engine processes all the relevant protocol headers and validates them against the list of allowed connections and the most recent connection state so that only valid packets are accepted from (or allowed onto) the network.

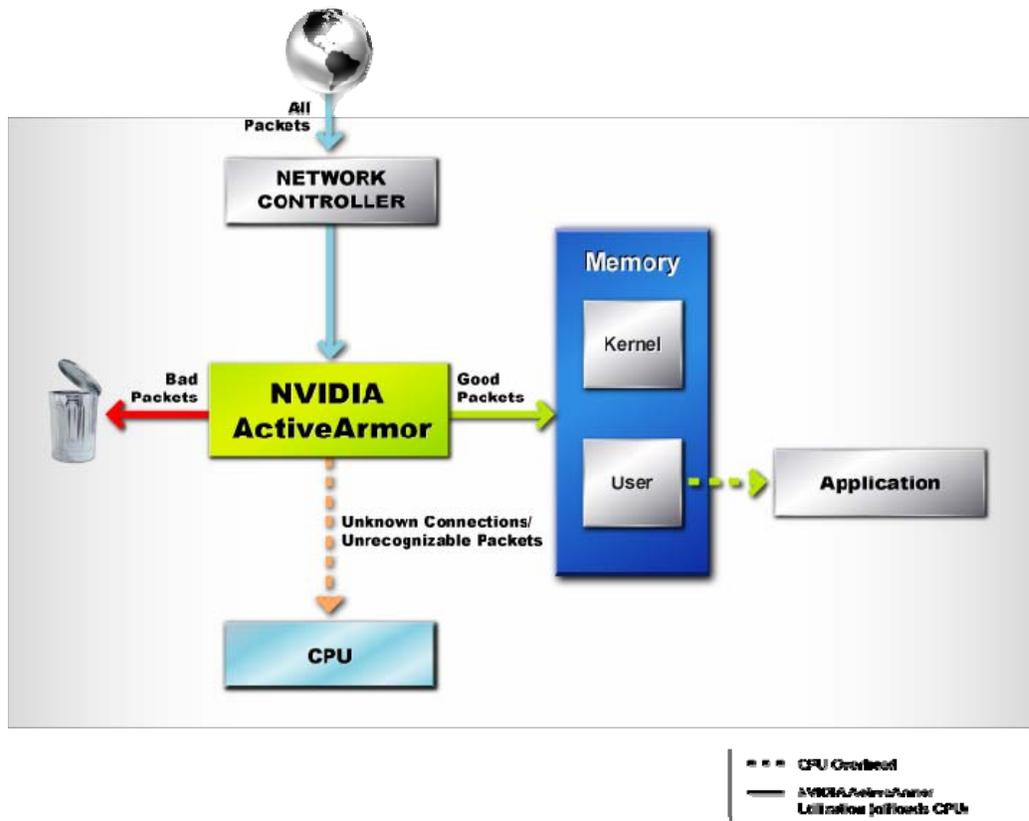


Figure 2. NVIDIA ActiveArmor Packet Processing

By examining the packets in hardware and placing the packet data directly into the application's buffers, ActiveArmor provides the highest performance and most efficient networking security solution available for any PC platform.

In addition to its packet inspection efficiencies, ActiveArmor provides three other major features: instant-on protection, enhanced security and tamper resistance, and support for Microsoft TCP Chimney Architecture.

Instant-On Protection

NVIDIA's secure networking solution provides "instant-on" protection by delivering a PC network connection that is secure the moment your PC is powered on. No security gap exists between the moment the PC is turned on and the availability of firewall protection on that PC. This instant-on protection is achieved by *integrating* an embedded driver and firewall processing into the NVIDIA nForce MCP.

In contrast, all other software solutions have a time gap between when the PC is turned on and when the security software is loaded into memory. This time gap is all that hackers, who constantly scan the networks for unprotected PCs, need to make their move and attack.

Enhanced Security and Tamper Resistance

Unlike other security solutions, NVIDIA ActiveArmor security settings deliver a deep level of inspection to your networking traffic. ActiveArmor accomplishes this by allowing your data to be closely checked to filter out any unauthorized or suspicious traffic.

This higher level of inspection and filtering can only be achieved by using a dedicated hardware engine, which offers these advantages:

- ❑ An enhanced level of security, achieved by offering deep packet inspection in hardware
- ❑ A higher level of security, which comes at no cost to the CPU and does not degrade system performance
- ❑ Tamper resistance (any attempt to disable or manipulate firewall policy control and filtering disables the network connection, protecting the PC from any unauthorized access)

Support for Microsoft TCP Chimney Architecture

ActiveArmor fully supports the new Microsoft TCP Chimney Architecture, allowing for protocol acceleration of TCP/IP. By integrating a firewall policy into the TCP/IP Chimney architecture, NVIDIA creates two powerful advantages—reduced CPU overhead in processing TCP/IP traffic, and a security policy enforcement engine that only allows authorized traffic into (or out of) the PC.

ActiveArmor and the NVIDIA nForce4 MCP family are one of the first products in the industry to incorporate support for the new Microsoft API, solidifying NVIDIA's leadership position in this area.

Conclusion

Current PC security solutions are software-based and consume a lot of CPU cycles. This approach is a compromise that tries to balance security and performance.

When it comes to security, however, there should be no compromise. PC users deserve to have the highest system performance without any security compromise!

The dilemma of how to address these two competing requirements has been resolved by the introduction of the NVIDIA secure networking engine. NVIDIA's dedicated hardware engine enhances network security because it provides hardware-based deep packet filtering while offloading CPU-intensive firewall and networking packet processing. As a result, NVIDIA ActiveArmor delivers better security and overall system performance.



Notice

ALL NVIDIA DESIGN SPECIFICATIONS, REFERENCE BOARDS, FILES, DRAWINGS, DIAGNOSTICS, LISTS, AND OTHER DOCUMENTS (TOGETHER AND SEPARATELY, "MATERIALS") ARE BEING PROVIDED "AS IS." NVIDIA MAKES NO WARRANTIES, EXPRESSED, IMPLIED, STATUTORY, OR OTHERWISE WITH RESPECT TO THE MATERIALS, AND EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE.

Information furnished is believed to be accurate and reliable. However, NVIDIA Corporation assumes no responsibility for the consequences of use of such information or for any infringement of patents or other rights of third parties that may result from its use. No license is granted by implication or otherwise under any patent or patent rights of NVIDIA Corporation. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied. NVIDIA Corporation products are not authorized for use as critical components in life support devices or systems without express written approval of NVIDIA Corporation.

Trademarks

NVIDIA, the NVIDIA logo, ActiveArmor, NVIDIA nForce, and SLI are trademarks or registered trademarks of NVIDIA Corporation in the United States and other countries. Other company and product may be trademarks of the respective companies with which they are associated

Copyright

© 2005 NVIDIA Corporation. All rights reserved.



NVIDIA.

NVIDIA Corporation
2701 San Tomas Expressway
Santa Clara, CA 95050
www.nvidia.com