

Техническое описание

ActiveArmor и аппаратный сетевой фильтр NVIDIA Firewall

Надежное сетевое решение

Введение

Компьютеры являются неотъемлемой частью сегодняшней жизни, а широкое распространение высокоскоростных Интернет соединений означает, что многие ПК сегодня подключены к общественным или частным сетям. ПК также содержат очень важную информацию (банковские данные или данные по работе, MP3 и цифровые фильмы), и большая часть этой информации поступает с банковских сайтов или сайтов загрузки музыкальных композиций. Тот факт, что миллионы ПК подсоединены к сети Интернет дает пользователям доступ к данным на сайтах всего мира. Но это также позволяет хакерам подсоединиться к сетевым ПК. Вне зависимости от того, злоумышленно они это делают или для развлечений, хакеры постоянно прощупывают незащищенные ПК. Исследование NVIDIA показало, что хакеры способны найти новый ПК в течение нескольких минут после его подключения к сети. Кроме того, программы-шпионы тайком загружаются на незащищенные ПК и передают информацию несанкционированным пользователям. Вот почему безопасность компьютеров является одной из самых важных проблем на сегодня.

Одна из основных причин, почему ПК страдают от брешей в системе защиты и атак, - это подключение к *совместно используемым сетям* — домашним сетям с большим количеством компьютеров, рабочим окружениям и Интернет, где миллионы ПК подключены одновременно.

В таких окружениях совершаются большинство атак хакеров, и «плохие» пакеты данных приводят к сбою или поломке незащищенного компьютера. Существует множество решений для защиты ПК от атак. Большинство таких решений являются программными. Но они часто потребляют много ресурсов CPU, что сказывается на общей производительности системы и возможностях пользователей. И вопреки распространенному мнению, увеличение циклов процессора не решает эту проблему, потому что многие атаки стали настолько изощренными, что способны легко обходить программную защиту.

В данном документе описываются преимущества решения обеспечения сетевой безопасности NVIDIA®, которое является неотъемлемой частью MCP процессоров nForce™ 4. Оно включает аппаратный сетевой фильтр NVIDIA Firewall 2.0 и технологию NVIDIA ActiveArmor™, первый в индустрии специальный движок сетевой безопасности.

NVIDIA ActiveArmor

Подсистема сетевой безопасности

NVIDIA ActiveArmor – это подсистема сетевой безопасности, встроенная в новое семейство MCP процессоров NVIDIA nForce4. Специальная аппаратная часть, повышающая сетевую защиту при снижении нагрузки на CPU, ActiveArmor обеспечивает более глубокие уровни проверки трафика на

скоростях полнодуплексных гигабитных Ethernet сетей. ActiveArmor гарантирует высочайший уровень производительности, снимая нагрузку с CPU по фильтрации пакетов и обеспечивая пользователям быстрое и безопасное сетевое окружение.

NVIDIA Firewall на базе системы сетевой безопасности ActiveArmor

Компьютерная безопасность имеет три независимых составляющих: сетевой фильтр, определение вторжений и защита от вирусов. (Более подробную информацию по защите компьютерных компонентов смотрите в техническом описании: “Безопасность от NVIDIA– персональный сетевой фильтр и технологии защиты от хакеров,” ТВ-00982-001).

Сетевой фильтр является основным компонентом компьютерной защиты. Он гарантирует, что только те пакеты данных, которые не противоречат гарантийным обязательствам, могут проходить через него. Для осуществления защиты сетевой фильтр анализирует каждый входящий пакет данных и определяет, имеет ли данный пакет допустимые атрибуты; если нет, пакет блокируется. *Этот процесс значительно нагружает CPU, что может сильно сказаться на производительности.*

Использование аппаратного блока решает эту проблему. При работе сетевого фильтра вместе со специальной аппаратной частью падения производительности не происходит.

Первым в индустрии аппаратным сетевым фильтром для ПК является NVIDIA Firewall 2.0, и он теперь работает на базе технологии сетевой защиты NVIDIA ActiveArmor. Сочетание NVIDIA Firewall и ActiveArmor (рис. 1) ускоряет передачу сетевых данных (на скоростях полнодуплексных Gigabit Ethernet), снижает нагрузку на CPU и проводит более глубокую проверку пакетов, улучшая таким образом общую сетевую защиту.

* NVIDIA ActiveArmor вкл.

** NVIDIA ActiveArmor выкл.

Рис. 1. Программные сетевые фильтры увеличивают нагрузку на CPU

Отсутствие нагрузки на CPU

Снижение нагрузки с CPU

В традиционных сетевых окружениях проверка пакетов является трудоемким делом, что сказывается на нагрузке на CPU, полосе пропускания памяти и латентности (рис. 2). Так, пакеты идут от MAC к драйверу, потом к стеку в пределах ядра, и от стека к приложению, что влечет пересечение границы ядерного/пользовательского пространства. Все эти операции копирования ложатся на плечи CPU и занимают много времени, а для обработки драйвера и стека требуется чрезвычайно много циклов CPU.

Рис. 2. Современная обработка пакетов

Система сетевой защиты ActiveArmor отбрасывает «плохие» пакеты даже до того, как CPU видит их. Плюс, проверенные пакеты обходят традиционную обработку стороной, что повышает общую пропускную способность и снижает нагрузку на CPU (рис. 3). Благодаря ActiveArmor все «хорошие» пакеты помещаются прямо в память приложений, что позволяет избежать до трех операций копирования с использованием CPU (из MAC в драйвер; из драйвера в стек в пределах области ядра и затем в приложение, что включает пересечение границы ядерного и пользовательского пространств).

Система сетевой защиты ActiveArmor обрабатывает все соответствующие заголовки протоколов и сверяет их во списке разрешенных соединений и самым последним состоянием соединения, разрешая проходить только надежным пакетам.

Рис. 3. Обработка пакетов с помощью NVIDIA ActiveArmor

Проверяя пакеты на аппаратном уровне и размещая данные пакетов прямо в буферы приложений, ActiveArmor обеспечивает высочайшую производительность и наиболее эффективное решение сетевой защиты, доступное для платформы ПК.

Помимо высокой эффективности по проверке пакетов ActiveArmor имеет еще три возможности: оперативная защита, защита от несанкционированного вмешательства и поддержка архитектуры Microsoft TCP Chimney.

Оперативная защита

Система сетевой безопасности NVIDIA обеспечивает оперативную защиту благодаря тому, что сетевое соединение оказывается под контролем с момента включения ПК. Никакого разрыва по времени между включением компьютера и обеспечением защиты с помощью брандмауэра не существует. Такая оперативная защита гарантируется за счет того, что драйвер и обработка с помощью сетевого фильтра встроены в MCP процессоры NVIDIA nForce.

Напротив, программным решениям требуется время, чтобы загрузиться в память после включения компьютера. А этого времени вполне достаточно хакерам, чтобы найти незащищенные ПК

Повышенная безопасность и защита от несанкционированных вторжений

По сравнению с другими решениями защиты, NVIDIA ActiveArmor гарантирует проверку сетевого трафика на более глубоком уровне для отфильтровывания несанкционированных или подозрительных данных.

Более высокий уровень проверки и фильтрации можно обеспечить только с помощью специального аппаратного движка. Он имеет три преимущества:

- Более высокий уровень безопасности благодаря глубокой проверке пакетов на аппаратном уровне.
- Повышенная безопасность без нагрузки на CPU и без снижения общей производительности системы.
- Защита от несанкционированных вторжений. Любая попытка отключить или воздействовать на работу сетевого фильтра отключает сетевое соединение, защищая ПК от несанкционированного доступа.

Поддержка архитектуры Microsoft TCP Chimney

NVIDIA ActiveArmor полностью поддерживает новую архитектуру Microsoft TCP Chimney, ускоряя работу протоколов TCP/IP. Встроенная политика сетевого фильтра в архитектуру TCP/IP Chimney NVIDIA дает два огромных преимущества— снижение нагрузки на CPU при обработке TCP/IP трафика и поддержка подсистемы обеспечения политики безопасности, которая гарантирует пропуск только санкционированного трафика.

NVIDIA ActiveArmor и семейство NVIDIA nForce4 MCP являются одними из первых продуктов на рынке с поддержкой нового интерфейса Microsoft API, что усиливает лидерские позиции NVIDIA в этой сфере.

Заключение

Современные решения защиты ПК являются программными и потребляют много ресурсов CPU. Данный подход является компромиссом между безопасностью и производительностью.

Однако, когда дело касается безопасности, компромисс должен быть исключен. Пользователи ПК заслуживают высочайшей производительности без какого-либо ущерба безопасности!

Дилемма обеспечения этих двух требований была решена с введением подсистемы сетевой защиты NVIDIA. Аппаратный блок NVIDIA улучшает сетевую безопасность, обеспечивая глубокую аппаратную фильтрацию пакетов и одновременно снимая нагрузку с CPU по обработке сетевых пакетов. В результате вы получаете повышенную безопасность и общую системную производительность.

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

Замечание

ВСЕ СПЕЦИФИКАЦИИ ПРОДУКТОВ NVIDIA, ЭТАЛОННЫЕ ПЛАТЫ, ФАЙЛЫ, ДИАГРАММЫ, ДИАГНОСТИЧЕСКИЕ ДАННЫЕ, СПИСКИ И ДРУГИЕ ДОКУМЕНТЫ (ВСЕ ВМЕСТЕ И ОТДЕЛЬНО НАЗЫВАЕМОЕ "МАТЕРИАЛАМИ") ПРЕДОСТАВЛЯЮТСЯ "КАК ЕСТЬ." NVIDIA НЕ ДАЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ ГАРАНТИИ ТОВАРНОГО СОСТОЯНИЯ, ПРАВОВОГО ТИТУЛА, НАРУШЕНИЯ ПРАВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ И СООТВЕТСТВИЯ ОПРЕДЕЛЕННЫМ ЦЕЛЯМ.

Предоставленная информация является точной и достоверной. Однако корпорация NVIDIA не несет никакой ответственности за последствия использования данной информации и за любые нарушения патентов или других прав третьих сторон, которые могут возникнуть в результате такого использования. Предоставление каких-либо разрешений косвенно либо иначе с использованием патентов или патентных прав корпорации NVIDIA невозможно. Спецификации, упомянутые в данном материале, могут быть изменены без предупреждения. Данный материал заменяет всю ранее предоставленную информацию. Продукция корпорации NVIDIA Corporation не санкционирована для использования в системах жизнеобеспечения без письменного подтверждения корпорации NVIDIA.

Товарные знаки

NVIDIA, логотип NVIDIA, ActiveArmor и NVIDIA nForce являются товарными знаками и/или зарегистрированными товарными знаками корпорации NVIDIA в США и других странах. Названия других компаний и продуктов могут являться товарными знаками соответствующих компаний.

Copyright

© 2004 Корпорация NVIDIA. Все права защищены.