

# Техническое описание

## NVIDIA Firewall

Безопасность компьютера и  
защита против хакеров

# Безопасность компьютера и защита против хакеров

---

## Введение

Компьютеры являются неотъемлемой частью сегодняшней жизни в сфере бизнеса и развлечений. Они содержат все виды ценной информации, становясь основной целью для хакеров. Вот почему безопасность компьютеров является одной из самых важных проблем на сегодня.

Компьютерная безопасность имеет три независимых составляющих: сетевой фильтр, защита от вторжений и защита от вирусов.

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. Когда функции сетевого фильтра интегрируются в драйверы компьютера, несанкционированный доступ к ПК через Интранет или Интернет значительно снижается.

NVIDIA® Firewall является первым сетевым фильтром на базе надежной сетевой подсистемы NVIDIA ActiveArmor™. В результате, NVIDIA Firewall обеспечивает высочайшую системную производительность при минимальной нагрузке на CPU. В то же время, он улучшает общую защиту, гарантируя аппаратную глубокую проверку пакетов, мгновенно активирующуюся защиту и функциональность с предотвращением несанкционированного вмешательства.

---

## Сетевые фильтры

### Цель

Сетевые данные состоят из пакетов с заголовками, содержащими метаданные. Эта метаданная позволяет передавать пакет по подсети (заголовок канального уровня (Data Link layer)), между сетями (заголовок сетевого уровня (Network Layer)), и в соответствующий процесс хоста (заголовок транспортного уровня (Transport Layer)). Если какой-либо компьютер подключен к сети Интернет, любой другой также подключенный компьютер может послать пакет данных на первый, если удаленный компьютер знает его IP адрес.

Большинство пакетов безопасны, но иногда некоторые пользователи посылают пакеты, вызывающие сбой в программном обеспечении протокола или операционной системе целевого компьютера. Целью таких пакетов является вывод из строя хоста (*отказ от обслуживания*) или получение несанкционированного доступа к хосту.

Большинство корпоративных и домашних сетей имеют четко определенное подключение к Интернет. Соединение состоит из ограниченного числа точек соединения (DSL модем), через которые пакеты с хостов поступают в Интернет, и наоборот. Понятие *сетевого фильтра* и было введено для того, чтобы можно было контролировать, какие пакеты могут проходить через него, а какие нет.

## Как они работают

Сетевые фильтры фильтруют сетевой трафик согласно различным критериям.

Наиболее очевидный способ фильтрации – это по типу пакетов. Сетевой фильтр разрешает или запрещает передачу пакета на основе номеров портов TCP или UDP согласно правилам, хранящихся в таблице контроля доступа.

Существует два возможных сценария фильтрации пакетов:

- ❑ Сетевой фильтр может пропускать все, кроме списка пакетов (согласно номерам портов), которые считаются опасными.
- ❑ Сетевой фильтр может быть запрограммирован на блокирование всей информации по умолчанию, позволяя проходить только определенным безопасным пакетам.

Безопасность тесна связана с управлением рисками. Определяя конфигурацию сетевого фильтра, пользователи ограничивают риск до пакетов, которые могут пройти. В основном, сетевые фильтры могут быть так сконфигурированы, чтобы было «атакующему» было сложно определить, какой трафик разрешен. Такая защита является своеобразной уловкой для поддержания защиты компьютера.

## Типы сетевых фильтров

### Stateless Firewall

Фильтр типа Stateless (без запоминания состояний соединений) является основным типом сетевого фильтра и существует в разных формах с начала 1990х годов. В этом случае список правил разрешения/запрещения определяется таким образом, что пройти могут только те пакеты, которые удовлетворяют разрешающим условиям. Правила диктуют фильтрацию трафика входящих и/или исходящих сообщений на основе типа Ethernet, IP адреса отправителя и получателя, опций IP, протокола IP, ICMP типа и значений кода, порты источника и получателя пакетов по протоколам TCP или UDP, и опций TCP.

Если пакет проходит тест, он может пройти через фильтр; в противном случае он будет сброшен. Однако каждый пакет должен пройти один и тот же набор тестов. Проблема состоит в том, что каждый пакет должен быть проверен по всем правилам. По мере того, как список правил расширяется, требуется все больше и больше ресурсов для обработки каждого пакета, что

негативно сказывается на производительности, - это измеряется в пакетах в секунду или измеряется нагрузка на CPU для обработки данного трафика. Stateless фильтры наиболее подходят для определенных пакетов, таких как ICMP, которые по природе своей являются не запоминают состояние операций.

NVIDIA Firewall поддерживает stateless проверку. Он фильтрует трафик по типу Ethernet, протоколу IP и опциям IP и TCP. IPv4 и IPv6 обрабатываются одинаково, где возможно. Например, опции IPv4 и заголовки IPv6 - оба могут быть использованы в качестве фильтрующих элементов.

## Фильтры, отслеживающие состояние соединений (Stateful Firewall)

Фильтр типа stateful является разновидностью stateless фильтра. Он работает также, как и последний при установке нового соединения, так как он сравнивает новый протокол (а также получателя и отправителя пакета) с локальными правилами.

Оптимизация stateful фильтра заключается в том, что пакеты данного потока подробно исследуются только при начале соединения. Когда новое соединение разрешается, в таблицу отслеживания состояния соединений добавляется запись. Последующие пакеты, которые согласуются с данной записью в таблице, проверяются по таблице разрешенных соединений без необходимости проверки каждого пакета по всему списку правил. Преимущество stateful фильтра заключается в том, что он поддерживает полную защиту пакетной фильтрации, задействуя при этом незначительную часть ресурсов центрального процессора.

NVIDIA Firewall поддерживает stateful проверку TCP и UDP трафика. UDP состояние определяется проверкой новых UDP пакетов и созданием состояний, только если они проходят по правилам сетевого фильтра, установленным пользователем.

Методика заключается в вычислении значения хеш-функции на основе нескольких ключевых полей в заголовке пакета. Ключевые поля могут состоять из IP адресов отправителя и получателя, протокола IP (который указывает, используется ли TCP или UDP, или какой-либо другой протокол транспортного слоя), а также портов транспортного слоя отправителя и получателя. Вычисление хеш-функции на основе этих пяти значений занимает немного времени на каждый пакет.

Сложность правил для фильтра не влияет на скорость принятия пакета фильтром. Stateless фильтр должен применить все правила (или столько правил, чтобы можно было принять решение о разрешении или запрещении прохода) для каждого пакета путем сравнения. Плюс, время анализа пакета линейно возрастает по мере увеличения количества правил, уменьшая скорость пересылки пакетов линейно по мере увеличения числа правил.

## Шлюзы на уровне приложений

Шлюз уровня приложений, или мосты транспортного уровня, - это компьютер специального назначения, который выполняет прокси услуги для каждого разрешенного приложения. Эти прокси-серверы должны быть исключительно стабильны; иначе прокси-сервер будет иметь свои слабые стороны.

Пакеты никогда не проходят прямо через шлюз уровня приложения. После получения пакета все его заголовки убираются, содержание проверяется и создается новая серия пакетов на новом соединении к хосту назначения.

Шлюз уровня приложения прозрачен так же, как и сетевой фильтр пакетов, за исключением того, что задержка при проверке пакетов может быть больше. Преимущество такого подхода заключается в том, что здесь есть логический промежуток между двумя сетями, но только для протоколов, которые шлюз понимает.

Основное ограничение шлюза уровня приложения это то, что для прохождения трафика определенного типа должен существовать прокси-сервер для этого протокола. Прокси-серверы для распространенных протоколов, таких как SMTP, FTP, HTTP и TELNET, легко доступны, но для более экзотических протоколов они не так широко распространены. Хотя для определенного круга приложений эти шлюзы являются лучшей гарантией того, что только санкционированные данные пройдут через фильтр.

Фильтры шлюза уровня приложения обычно находятся на конечной точки сети и требуют специального аппаратного обеспечения. NVIDIA Firewall, сетевой фильтр конечной точки, функционально не поддерживает шлюз уровня приложения.

## Сетевые фильтры как защита против хакеров

Фальсифицированный IP пакет имеет незаконно сгенерированное значение в IP поле адреса отправителя. Используя намеренно неправильный IP адрес, хакер может организовать различные атаки. Наиболее распространенной является атака отказа в обслуживании (DDoS), это также одна из наиболее распространенных типов атак, использующих IP спуфинг. Атаки DDoS зависят от двух факторов: 1) зомби-устройство, подсоединенное к Интернет, часто это ПК, которые было подвергнуто риску; и 2) способность заставить зомбированный ПК отправлять пакеты с фальшивыми IP адресами отправителя.

Сетевые фильтры всегда могли фильтровать данные на основе IP адреса, но определение фальсифицированных пакетов требует более тонкой работы. Например, исходя из IP адреса отправителя конкретного пакета, как можно определить, должен ли он был дойти до получившего его интерфейса, учитывая при этом информацию, известную фильтру о таблице маршрутизации? Промежуточное устройство не может с легкостью определить, что данный пакет фальшивый.

Лучший способ предотвращения спуфинга - это блокирование фальшивых пакетов на отправителе – на зомбированных ПК. Интегрировав анти-спуфинговую функцию в сетевую программно-аппаратную структуру ПК, можно предотвратить использование им IP адресов, кроме его статически присвоенного или DHCP присвоенного адресов.

---

## Другие важные возможности защиты данных

Сетевой фильтр обеспечивает один слой защиты, который называется базовым слоем (*foundation layer*). Но полное решение защиты содержит много слоев.

NVIDIA Firewall не обеспечивает эти дополнительные возможности, но их можно получить вместе с комплектующими в соответствии с требованиями пользователей.

## Защита против вторжений

Защита против вторжений – это способность анализировать весь входящий трафик по поведению на наличие признаков известных атак или предвестников известных атак. Например, чтобы атаковать уязвимую часть сетевого приложения, атакующий может сначала просканировать все возможные порты в поиске известного примера уязвимой части программного обеспечения. Так, обнаружив «сканирование портов», можно предположить, что атака скоро начнется, и необходимо принять защитные меры перед тем, как будет нанесен вред.

Благодаря защите от вторжений можно обнаружить и предотвратить различные известные атаки, не дав им нанести урод системе.

В обоих случаях программное обеспечение, защищающее от вторжений, зависит от библиотеки известных атак. Такие продукты обычно не могут определить новые атаки, потому что ранее такая атака еще «не оставляла своего автографа».

## Защита от вирусов

Антивирусная поддержка защищает пользовательский ПК от исполнения кода, содержащего известные вирусы или трояны. Как и в случае ПО для защиты от вторжений, антивирусная защита основана на библиотеке атак, которые известно как определить.

В дополнение, некоторые программные антивирусные решения могут предупреждать пользователей о подозрительно повышенной деятельности, даже если никакие известные вирусы не были обнаружены.

---

## NVIDIA Firewall

NVIDIA Firewall работает на базе надежной сетевой подсистемы ActiveArmor, благодаря которой мы имеем лучший в индустрии аппаратный сетевой фильтр для ПК. Сетевой подсистема позволяет NVIDIA Firewall обходиться без CPU в случае служебных сигналов.

Надежное сетевое решение NVIDIA ActiveArmor, сочетающее в себе NVIDIA Firewall и подсистему защиты ActiveArmor, повышает сетевую пропускную способность до скоростей Gigabit Ethernet, снижает нагрузку на CPU, проводит глубокую проверку пакетов и улучшает общую сетевую защиту (рис. 1).

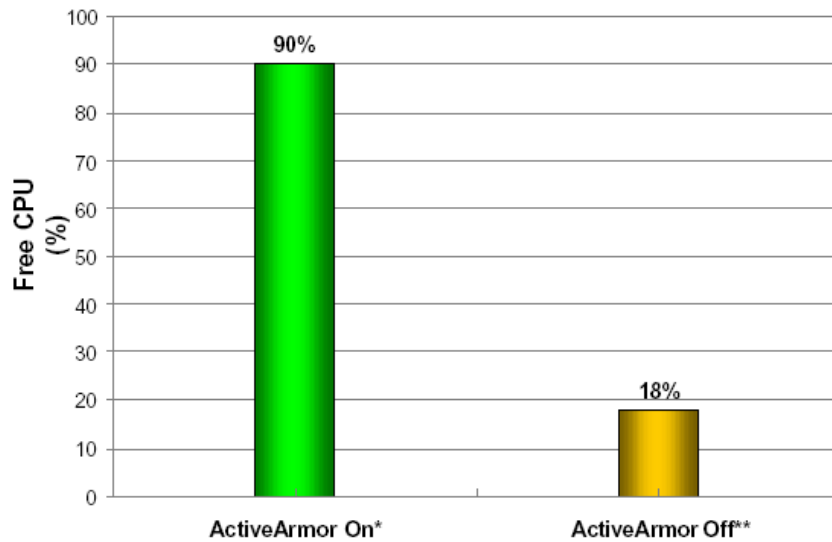


Рис 1. NVIDIA ActiveArmor обеспечивает максимальную производительность при минимальной нагрузке на CPU

К рисунку: Отсутствие нагрузки на CPU (%)

ActiveArmor вкл.

ActiveArmor выкл.

NVIDIA Firewall включает как сетевой фильтр, так и техники защиты от хакеров. NVIDIA Firewall поддерживает stateless и stateful проверку, управление на базе сетевых технологий, предопределенные профили защиты, фильтрацию на основе блокирования портов, удаленное администрирование и простой в использовании помощник. Также, NVIDIA Firewall имеет функции защиты от хакеров, такие как анти-IP-спуфинг, анти-снифинг, функции против отравления ARP кэша и защита против подмены DHCP серверов – важные элементы управления безопасностью для корпоративных сетей.

В корпоративном окружении фильтр конечной точки (как, например, фильтр рабочего стола) с поддержкой функций защиты от хакеров может снизить внутренне нарушение безопасности и предотвратить генерирование несанкционированного доступа рабочим столом. В результате повышается общая защита и снижаются требования, предъявляемые ИТ персоналом.

## Улучшенное управление

NVIDIA Firewall имеет множество продвинутых функций управления, такие как дистанционное управление, конфигурирование, мониторинг, интерфейс командной строки (CLI) и WMI скрипты. И его несложно использовать и устанавливать благодаря удобному помощнику.

Эти продвинутые возможности управления делают NVIDIA Firewall гибким, легким в использовании и мощным решением (рис. 2).

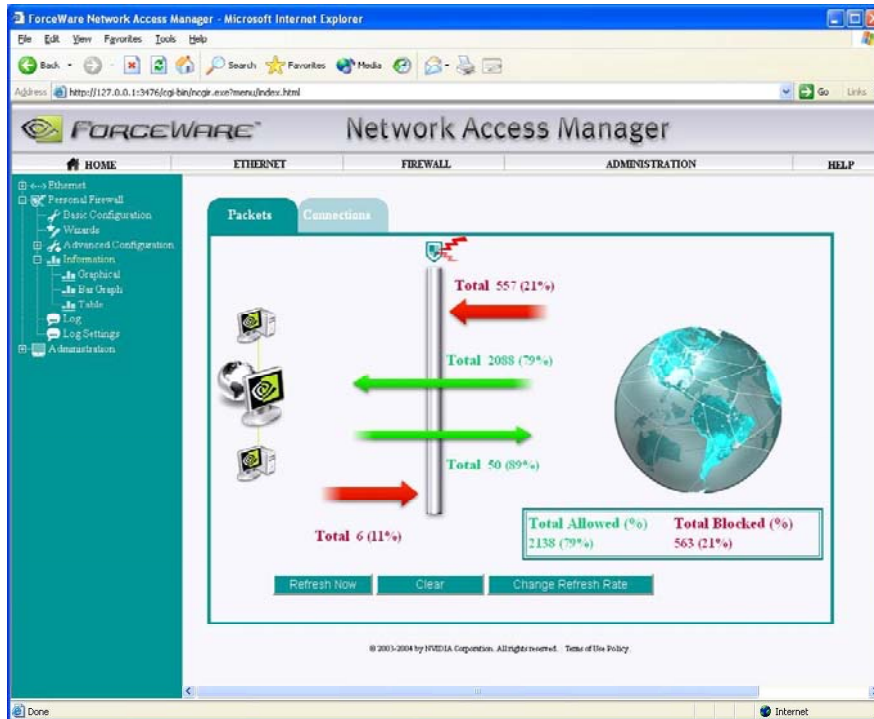


Рис 2. Простая конфигурация с интерфейсом браузера, основанном на сетевых технологиях

## Intelligent Application Manager (IAM)

Программа интеллектуального управления приложениями IAM добавляет фильтрацию на базе приложений к уже существующим возможностям NVIDIA Firewall. IAM расширяет элементы управления политикой NVIDIA Firewall для обеспечения фильтрации на базе приложений вне зависимости, являются они клиентами или серверами. IAM заставляет пользователей решать, какие приложения являются безопасными при взаимодействии с сетью. Если пользователь разрешает приложению обращаться в сеть, оно **может** открывать порты без специфических установок пользователя (рис. 3).

Это предотвращает возможность того, что какое-то неконтролируемое приложение на ПК пользователя отошлет трафик, который прошел через фильтр; исходящий трафик будет санкционирован, только если он поступил от приложения, которое пользователь отметил как безопасное. IAM может также определять изменения в существующих приложениях, например, вызванные вирусом или трояном, присоединившимся к исполняемому файлу, или вызванные приложением, переименованным для имитации какого-либо известного приложения.

IAM также защищает ПК от входящих пакетов. Это ограничивает возможность троянов и другого подобного ПО устанавливаться в качестве серверов на ПК, предотвращая получение ими трафика вне ПК. IAM не только поддерживает фильтрацию на уровне портов, но и не дает серверу

открывать какие-либо каналы, таким образом предотвращая получение трафика на уровне приложения.

IAM предоставляет полную защиту от атак, предотвращая атаку ПК извне или атаку им других компьютеров.

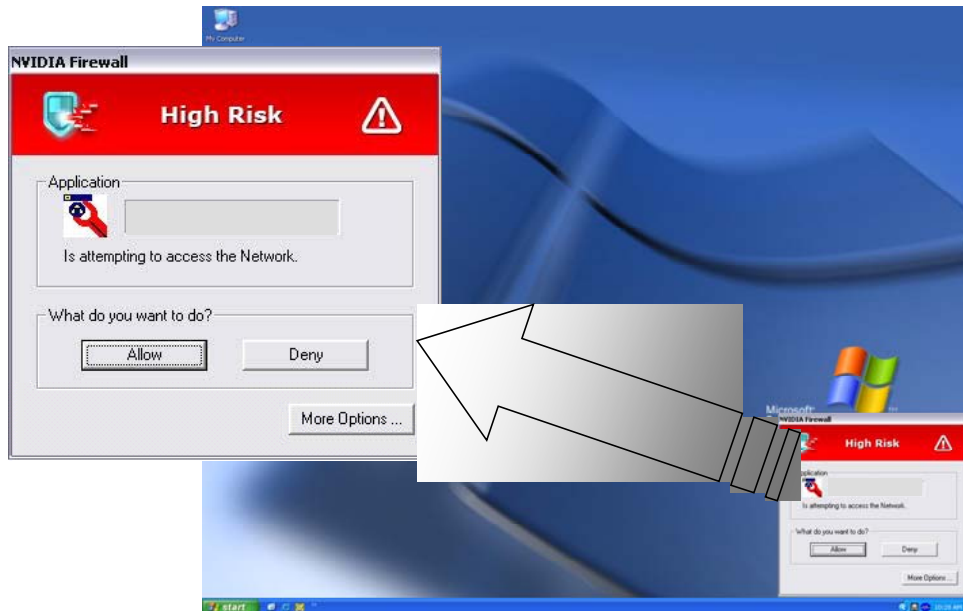


Рис. 3. IAM предупреждает, когда неизвестные приложения пытаются получить доступ в сеть

## Почему следует выбирать NVIDIA Firewall?

Большинство сетевых фильтров для ПК, присутствующие на рынке, являются программными дополнениями. Напротив, NVIDIA Firewall является аппаратно оптимизированным решением. Надежное сетевое решение NVIDIA ActiveArmor, состоящее из NVIDIA Firewall и ActiveArmor, улучшает сетевую безопасность.

NVIDIA Firewall также имеет уникальные функции. Он предоставляет программу управления IAM - удаленное управление, конфигурирование и мониторинг – и его несложно устанавливать и использовать благодаря удобному помощнику.

Плюс, он может использоваться в корпоративных окружениях, включая сетевой фильтр конечной точки (например, фильтр рабочего стола), или в домашних сетях (когда, например, домашний ПК подключен к сети Интернет) для защиты от несанкционированного доступа.

Технология NVIDIA Firewall является мощным полным средством защиты благодаря ведущему программному обеспечению по защите от вирусов и вторжений для лучшей безопасности ПК.

### **Примечание**

ВСЕ ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ НА ПРОЕКТИРОВАНИЕ, ЭТАЛОННЫЕ ПЛАТЫ, ФАЙЛЫ, ЧЕРТЕЖИ, ДИАГНОСТИЧЕСКИЕ ДАННЫЕ, СПИСКИ И ДРУГИЕ ДОКУМЕНТЫ (РАЗДЕЛЬНО И ВМЕСТЕ ИМЕНУЕМЫЕ "МАТЕРИАЛЫ") ПРЕДОСТАВЛЯЮТСЯ КАК ОНИ ЕСТЬ. NVIDIA НЕ ПРЕДОСТАВЛЯЕТ ЯВНЫХ, ПОДРАЗУМЕВАЕМЫХ, СТАТУАРНЫХ ИЛИ ДРУГИХ ГАРАНТИЙ В ОТНОШЕНИИ МАТЕРИАЛОВ И ЯВНЫМ ОБРАЗОМ ОТКАЗЫВАЕТСЯ ОТ ГАРАНТИЙ НЕНАРУШЕНИЯ ПРАВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ, ТОВАРНОГО СОСТОЯНИЯ И СООТВЕТСТВИЯ ОПРЕДЕЛЕННЫМ ЦЕЛЯМ.

Предоставленная информация считается точной и надежной. Однако корпорация NVIDIA не несет ответственности за последствия применения данной информации или за любые нарушения патентов или других прав третьей стороны, которые могут возникнуть в результате ее применения. Не подразумевается предоставление каких-либо лицензий, в том числе патентами или патентными правами корпорации NVIDIA. Спецификации, указанные в данной публикации, могут изменяться без предварительного уведомления. Данная публикация замещает всю информацию, предоставленную прежде. Продукты корпорации NVIDIA не авторизованы для применения в качестве критически важных компонентов в устройствах или системах жизнеобеспечения без специального письменного разрешения NVIDIA Corporation.

NVIDIA, логотип NVIDIA, CineFX и GeForce являются торговыми марками или зарегистрированными товарными знаками NVIDIA Corporation. Названия других компаний и продуктов могут являться товарными знаками соответствующих владельцев.

Авторское право NVIDIA Corporation 2004

NVIDIA Corporation  
2701 San Tomas Expressway  
Santa Clara, CA 95050  
[www.nvidia.com](http://www.nvidia.com)