



# Condensé technique

**NVIDIA Firewall**  
Sécurité PC et anti-piratage

# Sécurité PC et anti-piratage

---

## Introduction

Travail ou loisirs, les ordinateurs font désormais partie de notre quotidien. Nous leur confions toutes sortes de données capitales qui en font une cible de rêve pour les pirates. Voilà pourquoi la sécurité des ordinateurs est un problème qui nous concerne tous.

La sécurité d'un ordinateur repose sur trois éléments indépendants : le pare-feu, la détection des intrusions et la protection anti-virus.

Le pare-feu est l'élément clé de cette sécurité. En effet, il ne laisse passer que les paquets de données qui répondent à des critères bien définis. Pour assurer cette protection, le pare-feu examine chaque paquet de données qui tente de passer, détermine s'il est conforme aux critères établis et, dans la négative, le bloque. En intégrant la fonctionnalité de pare-feu au logiciel pilote d'un PC, les possibilités d'accès au PC par des intrus via un intranet ou Internet diminuent considérablement.

NVIDIA® Firewall est le premier pare-feu boosté par le moteur de gestion sécurisée de réseau NVIDIA ActiveArmor™. Le NVIDIA Firewall qui en résulte est le plus performant du marché pour une utilisation très basse de l'UC. En même temps, il augmente la sécurité générale en assurant une inspection matérielle minutieuse des paquets de données, une protection instantanée et une fonctionnalité résistante aux agressions.

---

## Les pare-feux

### Leur raison d'être

Les données circulent sur les réseaux sous la forme de *paquets* dont les en-têtes contiennent des méta-informations. Ce sont ces méta-informations qui permettent l'acheminement du paquet sur un sous-réseau (en-tête de la couche Liaison de données), un inter-réseau (en-tête de la couche Réseau) et dans le juste processus d'un hôte (en-tête de la couche Transport). Quand un ordinateur est connecté à

Internet, tout autre ordinateur également connecté peut lui envoyer un paquet à la simple condition d'en connaître l'adresse IP.

La plupart des paquets sont inoffensifs, mais il arrive que des personnes mal-intentionnées tentent d'envoyer des paquets qui exploitent les failles du logiciel de protocole ou du système d'exploitation de l'ordinateur cible. L'objectif de ces paquets est de paralyser l'ordinateur cible (on parle alors d'attaque par « denial of service », en français « déni de service ») ou d'y accéder sans autorisation. La plupart des réseaux d'entreprise et personnels ont une connexion Internet bien définie. Cette connexion consiste en un nombre limité de points d'accès (modem DSL) par l'intermédiaire desquels les ordinateurs envoient les paquets sur Internet ou les reçoivent d'Internet. Et pour contrôler les paquets qui traversent cette ligne de démarcation, les pare-feux (en anglais firewalls) sont nés.

## Leur mode de fonctionnement

Les pare-feux permettent de filtrer le trafic sur les réseaux en fonction de nombreux critères. Le critère le plus évident est le filtrage par type de paquet : le pare-feu utilise les numéros de port TCP ou UDP contenus dans un paquet pour en autoriser ou interdire le passage, sur la base de règles stockées dans une table de contrôle d'accès.

Deux cas de figure peuvent se présenter :

- ❑ Le pare-feu laisse tout passer à l'exception d'une liste de paquets (identifiés par leurs numéros de port) considérés comme nuisibles et auxquels l'accès est refusé.
- ❑ Le pare-feu est programmé pour tout bloquer par défaut et ne laisser passer que certains paquets considérés comme sûrs.

La sécurité est une affaire de gestion des risques. En définissant la configuration d'un pare-feu, les utilisateurs limitent les risques aux paquets autorisés sur leur réseau. Par ailleurs, les pare-feux étant en général configurables, un pirate aura du mal à déterminer le type de trafic autorisé par un pare-feu donné. Cette protection contribue à garantir un certain degré d'indétectabilité à l'ordinateur protégé.

## Types de pare-feux

### Les pare-feux statiques

Les pare-feux statiques (*stateless* en anglais) sont les plus élémentaires et existent sous une forme ou une autre depuis le début des années 1990. Dans ce type de pare-feux, une liste de règles d'acceptation/rejet est établie afin que seuls les paquets qui remplissent certaines conditions ne soient autorisés à traverser le barrage. Ces règles permettent de filtrer le trafic entrant ou sortant en fonction du type Ethernet, de l'adresse source IP ou de l'adresse de destination, des options IP, du protocole IP, du type ICMP et/ou des valeurs de code, du port source ou de destination TCP ou UDP, et des options TCP.

Si le paquet passe le test avec succès, il traverse, sinon il est bloqué. Tous les paquets sont ainsi soumis aux mêmes tests. L'inconvénient majeur de cette solution est que

chaque paquet doit être contrôlé à la lueur de toutes les règles. Par conséquent, plus les règles sont nombreuses, plus le temps nécessaire au traitement de chaque paquet augmente. Cet effort supplémentaire réduit donc la performance (mesurée en paquets/seconde ou en CPU utilisé pour traiter une quantité donnée de trafic)? Les pare-feux statiques conviennent mieux pour certains paquets, tels que les paquets ICMP, qui sont statiques par nature.

NVIDIA Firewall assure l'inspection statique. Ce produit est en mesure de filtrer le trafic en fonction du type d'Ethernet, du protocole IP et de règles relatives aux options IP et TCP. IPv4 et IPv6 sont gérés de façon similaire, chaque fois que possible. Par exemple, les options IPv4 comme les en-têtes d'extension IPv6 peuvent être utilisés comme éléments de filtrage.

## Les pare-feux dynamiques

Les pare-feux dynamiques (*stateful* en anglais) sont une variante des pare-feux statiques. Ils en reprennent plus ou moins le principe à chaque nouvelle connexion en ce qu'ils comparent le nouveau protocole (et la source et la destination du paquet) à certaines règles locales.

L'avantage des pare-feux dynamiques tient dans le fait que les paquets d'un flux donné ne sont examinés en détail qu'à l'ouverture d'une connexion. À chaque nouvelle connexion autorisée, une entrée est ajoutée dans une table des connexions ouvertes. Les paquets suivants qui correspondront à cette entrée de la table pourront être vérifiés en fonction de la table des connexions autorisées sans besoin de confronter chaque paquet à l'intégralité des règles. Les pare-feux dynamiques offrent donc toute la sécurité des pare-feux de filtrage de paquets pour une fraction des cycles de CPU consommés.

NVIDIA Firewall permet l'inspection dynamique du trafic TCP et UDP. Un « état » UDP est déterminé en observant les nouveaux paquets UDP et en créant des états uniquement s'ils dépassent les critères définis par l'utilisateur.

La technique de recherche et de confrontation repose sur une valeur de hachage basée sur plusieurs champs clés des en-têtes des paquets. Ces champs clés peuvent inclure les adresses IP de la source et du destinataire, le protocole IP (qui indique si TCP, UDP ou un autre protocole de couche de transport est utilisé), et les ports de couche de transport de la source et du destinataire. Calculer une fonction de hachage sur ces cinq valeurs prend un laps de temps fixe (limité) par paquet.

La complexité des critères n'affecte pas la vitesse de validation des pare-feux dynamiques. Par comparaison, le pare-feu statique doit appliquer toutes les règles (ou suffisamment de règles pour pouvoir prendre une décision quant à l'acceptation et le rejet) pour chaque paquet. Sans compter que le temps nécessaire à l'analyse des paquets augmente proportionnellement au nombre des règles, ce qui se traduit par une performance de transmission de paquets qui diminue proportionnellement à l'augmentation du nombre des règles.

## Les passerelles applicatives

Une passerelle de la couche application ou un pont de la couche transport est un ordinateur dédié qui exécute les services proxy pour chaque application dont le passage est autorisé. Ces serveurs proxy doivent être exceptionnellement stables et à toute épreuve, sinon ils seraient eux mêmes vulnérables. Les paquets ne traversent jamais directement une passerelle applicative. Lorsqu'un paquet est reçu par un pare-feu de ce type, l'ensemble de ses en-têtes sont éliminés, son contenu est examiné et une nouvelle série de paquets est créée sur une nouvelle connexion à l'hôte de destination.

Une passerelle applicative est aussi transparente que les pare-feux à filtrage de paquets, sauf que l'examen peut être plus long. L'avantage de cette solution réside dans la création d'un véritable « sas » logique entre les deux réseaux (mais uniquement pour les protocoles que la passerelle comprend).

Le principal inconvénient des passerelles applicatives est que pour qu'un certain type de trafic passe, il faut un serveur proxy pour ce protocole. Des proxies sont actuellement disponibles pour les protocoles courants, tels que SMTP, FTP, HTTP et TELNET, mais pas ce n'est pas toujours le cas pour les protocoles moins répandus. Pour un petit nombre d'applications, ces passerelles sont cependant la meilleure solution pour ne laisser passer que les données valides à travers le pare-feu.

Les pare-feux applicatifs se trouvent en général sur le bord du réseau et nécessitent un matériel dédié. Étant un pare-feu d'extrémité, NVIDIA Firewall n'assure pas la fonctionnalité de passerelle applicative.

## Les pare-feux pour se défendre contre les pirates (anti-piratage)

Un paquet IP « spoofé » est un paquet dont l'adresse source IP contient une valeur générée illégalement. L'usurpation intentionnelle d'une adresse IP peut permettre au pirate de tromper un système pour le rendre perméable à plusieurs types d'attaques. Le type d'attaque le plus célèbre est le DDoS (distributed denial-of-service ou déni de service distribué), qui est aussi l'un des plus courants utilisant le spoofing IP. Ces attaques DDoS reposent sur deux facteurs : 1) une machine « zombie » connectée à Internet, qui est en général un PC compromis ; et 2) la capacité de commander ce PC zombie afin d'envoyer des paquets avec des adresses IP source usurpées.

Les pare-feux ont toujours été en mesure de filtrer les paquets sur la base d'une adresse IP, mais la détection des paquets spoofés implique une distinction plus subtile. Par exemple, en se basant sur son adresse IP de provenance, un paquet devrait-il être arrivé sur l'interface qui l'a reçu, compte tenu de ce que le pare-feu sait de la table de routage ? Une machine intermédiaire ne peut pas détecter facilement qu'un paquet donné est spoofé.

La meilleure méthode pour lutter contre le spoofing consiste à bloquer les paquets spoofés à la source : les PC zombies. En intégrant la fonctionnalité anti-spoofing directement dans l'infrastructure matérielle/logicielle réseau du PC, ce dernier n'est plus en mesure d'utiliser une adresse IP autre que celle qui lui a été attribuée de manière statique ou que celle attribuée par DHCP.

---

## Autres fonctions de sécurité importantes

Le pare-feu fournit une « couche » de protection, qui est en général considérée comme la couche de fondation. Mais, pour être complète, une solution de sécurité devra comporter plusieurs couches.

NVIDIA Firewall n'incorpore pas ces fonctionnalités, mais l'utilisateur pourra se les procurer en choisissant les composants répondant le mieux à ses besoins.

## Protection contre les intrusions

La détection des intrusions est la capacité d'analyser tout le trafic entrant pour identifier des modèles de comportement, qui correspondent à des attaques connues ou à des signes précurseurs d'attaques connues. Par exemple, pour attaquer une partie vulnérable d'un logiciel d'application réseau, un attaquant commencera par balayer les ports disponibles à la recherche d'une faille connue de ce logiciel. Ainsi, la détection d'un « balayage de ports » pourra être le signe d'une attaque imminente et permettre de prendre des mesures défensives avant l'intrusion.

Avec la prévention des intrusions, de nombreuses attaques connues sont directement détectées et contrecarrées avant de pouvoir endommager un système.

Dans les deux cas, le logiciel anti-intrusion ne réagit qu'aux attaques connues répertoriées dans une bibliothèque. Ces produits ne sont en général pas en mesure de détecter de nouvelles attaques pour lesquelles aucune « signature » n'a encore été définie.

## Protection anti-virus

Un anti-virus empêche le PC d'un utilisateur d'exécuter du code contenant des virus ou des chevaux de Troie connus. Similairement aux produits anti-intrusion, les anti-virus agissent à partir d'une bibliothèque d'attaques connues contre lesquelles le produit sait se défendre.

De plus, certains produits anti-virus peuvent avertir les utilisateurs lorsqu'ils détectent des activités suspectes, même si celles-ci ne sont dues à un virus connu.

---

## NVIDIA Firewall

NVIDIA Firewall est maintenant boosté par ActiveArmor, un puissant moteur de gestion de réseau sécurisée, qui en fait le premier véritable pare-feu de l'industrie pour PC. Grâce au moteur de gestion de réseau sécurisée, NVIDIA Firewall n'est plus tributaire de la surcharge de l'UC.

La solution de gestion de réseau sécurisé NVIDIA ActiveArmor (une combinaison entre NVIDIA Firewall et le moteur de sécurisation ActiveArmor) permet d'atteindre des débits plus élevés en plein Gigabit Ethernet, de réduire l'utilisation de l'UC, d'inspecter en profondeur les paquets et d'améliorer la sécurité générale du réseau (Figure 1).

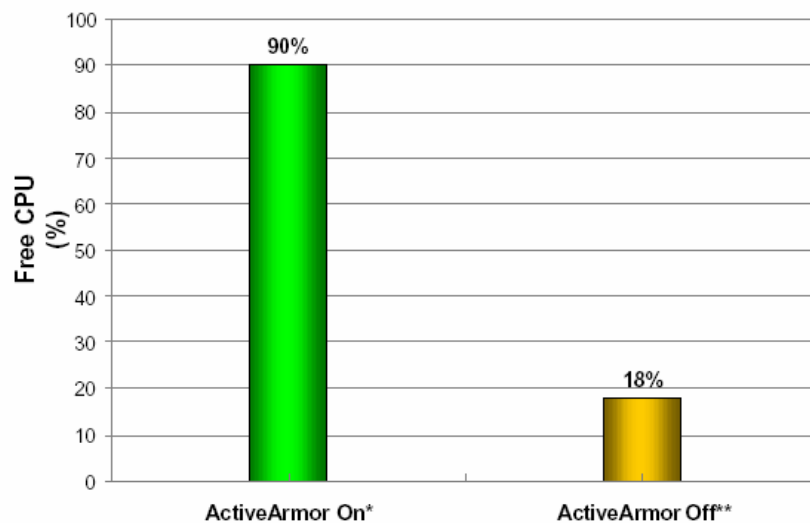


Figure 1. NVIDIA ActiveArmor offre la performance maximale pour un usage minimal de l'UC

**Remarques :**

NVIDIA Firewall incorpore à la fois les technologies de pare-feu et d'anti-piratage. Cette solution prend en charge l'inspection statique et dynamique, la gestion via Internet, les profils de sécurité prédéfinis, le filtrage/blocage des ports et l'administration à distance et un assistant intuitif. Elle comprend par ailleurs des fonctions d'anti-piratage, telles que l'anti-spoofing IP, l'anti-sniffing, une fonction d'anti-empoisonnement de cache ARP et une autre dite anti-serveur DHCP, des sécurités qui revêtent toutes une importance capitale pour les réseaux d'entreprises.

Dans le cadre d'une entreprise, un pare-feu situé en un point de sortie (comme un ordinateur de bureau) et doté de fonctions anti-piratage peut contribuer à réduire les attaques qui proviennent de l'intérieur et peut empêcher les ordinateurs de bureau de générer un trafic non autorisé. La sécurité globale est ainsi accrue tout en libérant le personnel informatique de certaines tâches.

## Fonctions de gestion avancées

NVIDIA Firewall offre de nombreuses fonctions de gestion avancées, telles que l'accès, la configuration et le monitoring à distance, une interface de ligne de commande (ILC) et des scripts WMI. Il est également facile à utiliser et à configurer grâce à un assistant très convivial.

Ces fonctions de gestion avancées rendent NVIDIA Firewall particulièrement flexible, intuitif et puissant (Figure 2).

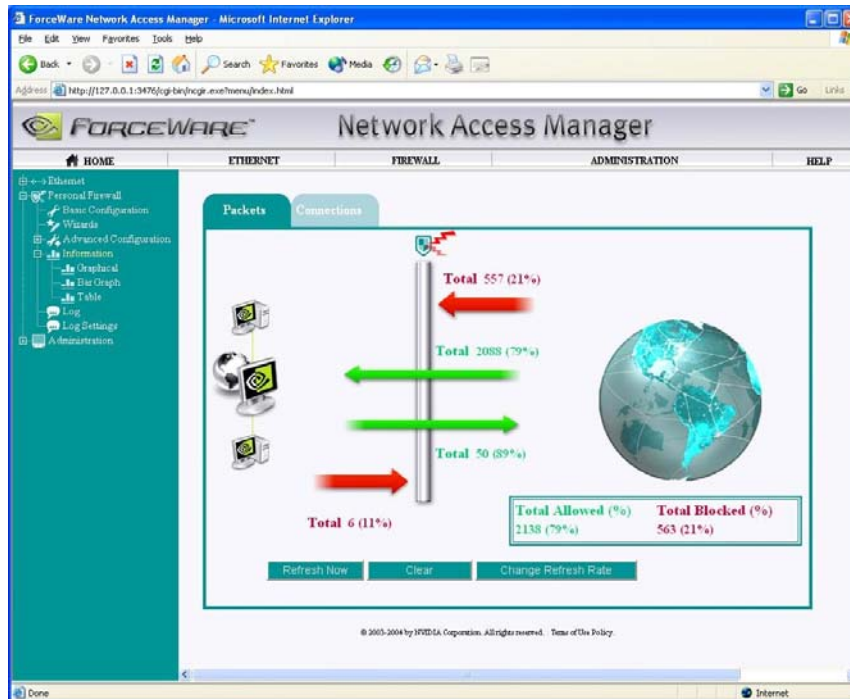


Figure 2 Facilité de configuration avec l'interface de navigation sur le web

## Gestionnaire applicatif intelligent IAM (Intelligent Application Manager)

Le gestionnaire applicatif intelligent complète NVIDIA Firewall en ajoutant un filtrage applicatif aux fonctionnalités de filtrage déjà étendues du pare-feu. L'IAM élargit les critères de gestion de NVIDIA Firewall et permet d'obtenir un filtrage basé sur les applications, indépendamment du fait qu'elles soient client ou serveur. L'IAM permet aux utilisateurs de décider ce qui peut entrer ou sortir de leur ordinateur en toute sécurité. Lorsque qu'une application a été autorisée, elle peut ouvrir des ports sans besoin de configuration spécifique par l'utilisateur (Figure 3).

L'IAM élimine la possibilité qu'une application illégale sur le PC de l'utilisateur ne puisse envoyer des données qui auraient traversé le pare-feu ; le trafic sortant n'est autorisé que s'il provient d'une application que l'utilisateur estime sûre. L'IAM peut même détecter les applications existantes et déterminer si elles ont été altérées (par exemple, par un virus ou un cheval de Troie attaché à l'exécutable ou par une application qui se serait renommée elle-même afin de se faire passer pour une application connue).

L'IAM est également utile pour la protection du PC contre les paquets entrants. Il limite la capacité des Chevaux de Troie ou autres logiciels espions de se configurer comme des serveurs sur le PC et évite qu'ils ne reçoivent du trafic provenant de l'extérieur du PC. Il n'est pas seulement à même d'effectuer un filtrage basé sur les ports, mais il peut également interdire au serveur d'ouvrir des connexions, en empêchant efficacement tout trafic sur la couche applicative.

Il assure une protection totale contre les attaques, en protégeant non seulement votre PC des attaques extérieures, mais également en empêchant votre PC d'attaquer d'autres PC.

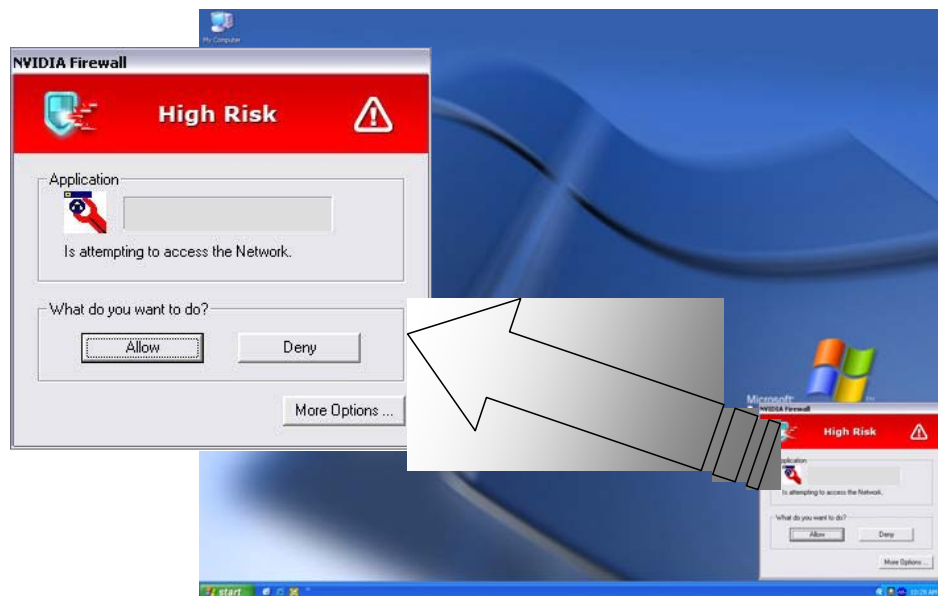


Figure 3. IAM vous avertit quand des applications inconnues tentent d'accéder au réseau

---

## Pourquoi choisir NVIDIA Firewall ?

La plupart des pare-feux pour PC sur le marché se présentent sous forme de logiciels complémentaires, tandis que NVIDIA Firewall est le premier pare-feu de l'industrie véritablement « natif ». Et la solution de gestion sécurisée de réseau ActiveArmor de NVIDIA, qui allie NVIDIA Firewall et le moteur ActiveArmor, augmente encore la sécurité globale des réseaux.

NVIDIA Firewall offre en outre des fonctionnalités exclusives, telles que le gestionnaire applicatif intelligent (IAM)— accès, configuration et monitoring à distance—qui viennent se greffer sur une extrême facilité d'emploi et de configuration grâce à l'assistant très convivial et intuitif fourni. Il peut être déployé au sein d'entreprises dotées d'un pare-feu d'extrémité, tel qu'un pare-feu de bureau. Ou il peut être utilisé chez les particuliers, par exemple quand leur PC dispose d'une connexion Internet à large bande, pour protéger l'ordinateur contre les accès non autorisés.

La technologie NVIDIA Firewall est un allié de taille pour la mise en œuvre de politiques de sécurité. Pour bénéficier d'une solution de sécurité PC totale, les utilisateurs sont toutefois invités à compléter la protection offerte par leur pare-feu NVIDIA Firewall par des logiciels de détection des intrusions et anti-virus de la dernière génération.



#### **Avis**

L'ENSEMBLE DES SPÉCIFICATIONS DE CONCEPTION, CARTES DE RÉFÉRENCE, FICHIERS, DESSINS, DIAGNOSTICS, LISTES ET AUTRES DOCUMENTS NVIDIA (DÉSIGNÉS ENSEMBLE ET SÉPARÉMENT COMME LES « MATÉRIAUX ») SONT FOURNIS « EN L'ÉTAT ». NVIDIA NE FOURNIT AUCUNE GARANTIE, QU'ELLE SOIT EXPRESSE, TACITE, LÉGALE OU AUTRE, CONCERNANT LES MATÉRIAUX, ET EXCLUT EXPRESSÉMENT TOUTE GARANTIE IMPLICITE DE CONTREFAÇON, DE QUALITÉ MARCHANDE ET D'APTITUDE À UN USAGE PARTICULIER.

Les informations ci-incluses sont censées être précises et fiables. Toutefois, NVIDIA Corporation décline toute responsabilité quant aux conséquences de l'utilisation qui pourrait en être faite ou de la contrefaçon de brevets ou autres droits de tierces parties pouvant résulter de leur utilisation. Aucune licence n'est octroyée implicitement ou de quelque autre manière sous quelque brevet ou droit de brevet de NVIDIA Corporation. Les caractéristiques techniques mentionnées dans ce document peuvent être modifiées sans préavis. Cette publication annule et remplace toute information diffusée antérieurement. **Les produits de NVIDIA Corporation ne peuvent en aucun cas être utilisés en tant que composants critiques pour des systèmes de survie sans l'accord préalable écrit de NVIDIA Corporation.**

#### **Marques commerciales**

NVIDIA, le logo NVIDIA et ActiveArmor sont des marques commerciales des marques déposées de NVIDIA Corporation aux États-Unis et dans d'autres pays. Les autres noms de sociétés et de produits cités sont des marques commerciales de leurs sociétés respectives ou des sociétés auxquelles ils sont associés.

#### **Droits d'auteur**

© 2004 by NVIDIA Corporation. Tous droits réservés.



**NVIDIA.**

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