



Condensé technique

Pare-feu matériel
NVIDIA et **ActiveArmor**
Une solution de gestion
réseau sécurisée





Introduction

Les ordinateurs font désormais partie de notre quotidien et la prolifération des connexions Internet haut débit implique que la plupart des ordinateurs sont désormais reliés à des réseaux publics ou privés. Par ailleurs, les ordinateurs renferment de précieuses informations (données bancaires ou professionnelles, MP3 ou films numériques), dont la majeure partie est accessible à partir de sites bancaires en ligne ou de services de téléchargement musical. Comme des millions de PC sont à présent connectés à Internet, les utilisateurs disposent d'un accès fabuleux à des informations stockées sur des sites Web du monde entier. À l'inverse, cette situation offre également aux pirates informatiques la possibilité d'accéder à ces PC en réseau. Que leurs intentions soient malveillantes ou d'ordre purement récréatif, les pirates sont constamment à la recherche d'ordinateurs vulnérables. D'après l'unité de recherche de NVIDIA, les pirates détectent un nouveau PC connecté à un réseau public après simplement quelques minutes de connexion. Et ce n'est pas tout : les PC non protégés doivent également faire face aux applications espions qui y sont chargées à leur insu, et qui permettent de communiquer des informations sur l'utilisation du PC à des personnes non autorisées. C'est pour cela que la sécurité des ordinateurs est l'un des problèmes les plus préoccupants pour les utilisateurs d'aujourd'hui.

L'une des raisons principales pour lesquelles les PC sont si vulnérables aux failles et attaques visant leur système de sécurité est le fait qu'ils soient reliés à des réseaux *partagés*, qu'il s'agisse de particuliers possédant plusieurs ordinateurs, d'environnements professionnels ou d'Internet, point auquel sont connectés des millions de PC en même temps. La plupart des attaques se produisent dans le cadre de ces environnements. Conséquence : des paquets de données nuisibles sont transmis à des PC non protégés afin de causer le maximum de dégâts.

C'est pour cela que de nombreuses solutions de protection de PC ont été mises en place pour lutter contre ces attaques. Une caractéristique commune à la plupart des solutions de protection pour PC est leur base : *logicielle*. Cependant, les solutions de type logiciel sont gourmandes en UC, ce qui affecte négativement les performances système globales et l'expérience de l'utilisateur. Et, contrairement à la croyance populaire, l'ajout de cycles d'UC supplémentaires ne résout pas le problème, car de nombreuses attaques sont sophistiquées et contournent ou désactivent les solutions de sécurité logicielles.

Ce document décrit en détail les avantages que présente la solution de gestion réseau de NVIDIA®, qui fait partie intégrante des processeurs multimédia et de communication MCP NVIDIA nForce™ 4. Cette solution intègre la technologie matérielle NVIDIA Firewall 2.0 ainsi que NVIDIA ActiveArmor™, le premier moteur de gestion réseau sécurisé dédié du secteur.

Le moteur de gestion réseau sécurisé NVIDIA ActiveArmor

NVIDIA ActiveArmor est un moteur de gestion réseau sécurisé intégré à la nouvelle famille de processeurs MCP NVIDIA nForce4. Petite portion dédiée de silicium visant à améliorer la sécurité réseau tout en réduisant la surcharge de l'UC, ActiveArmor offre des niveaux d'analyse du réseau et du trafic plus fins, à des vitesses Gigabit Ethernet en duplex intégral.

ActiveArmor fournit les meilleures performances système en déchargeant l'UC du filtrage de paquets au niveau matériel, tâche très mobilisatrice. Les utilisateurs bénéficient ainsi d'un environnement réseau PC à la fois rapide et sécurisé.

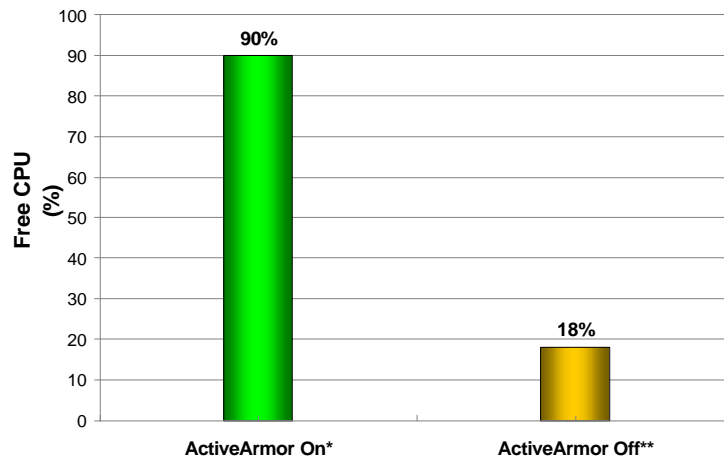
NVIDIA Firewall boosté par le moteur de gestion réseau sécurisé ActiveArmor

La sécurité d'un ordinateur repose sur trois composants indépendants les uns des autres : un pare-feu, la détection des intrusions et la protection antivirus. (Pour plus d'informations sur les composants de la sécurité informatique, reportez-vous au condensé technique relatif à la sécurité, aux pare-feux et à la technologies anti-piratage de NVIDIA.)

Le pare-feu est l'élément clé de cette sécurité. C'est lui qui, en effet, garantit que seuls les paquets de données conformes aux stratégies établies soient admis. Pour ce faire, le pare-feu analyse chaque paquet de données qui tente de passer, détermine s'il présente les attributs requis et, dans la négative, le bloque. *Il s'agit d'un processus qui mobilise énormément l'UC et qui, de ce fait, peut diminuer considérablement les performances système.*

Pour remédier au problème de l'utilisation trop intensive de l'UC, NVIDIA a introduit un moteur matériel dans ce processus. En effet, lorsque la fonctionnalité du pare-feu est associée à un moteur matériel dédié, les performances ne se détériorent pas.

NVIDIA Firewall 2.0 est le premier véritable pare-feu pour PC basé sur du matériel du secteur ; il est désormais boosté par le moteur de gestion réseau sécurisé NVIDIA ActiveArmor. La combinaison de NVIDIA Firewall et du moteur de gestion réseau sécurisé ActiveArmor (voir Figure 1) permet d'améliorer le débit réseau (à des vitesses Gigabit Ethernet en duplex intégral), de ménager l'UC et d'analyser en profondeur les paquets de données, ce qui renforce la sécurité globale sur le réseau.



* NVIDIA ActiveArmor activé
** NVIDIA ActiveArmor désactivé

Figure 1 : Les pare-feux logiciels sont gourmands en UC

Une utilisation réduite de l'UC

Dans les environnements réseau traditionnels, l'analyse des paquets est une procédure fastidieuse qui surcharge l'UC, affecte la bande passante mémoire et le temps de latence global du système (voir Figure 2). Par exemple, les paquets transitent du périphérique réseau MAC au pilote, du pilote à la pile au sein de l'espace noyau, et de la pile à l'application, ce qui implique la traversée de la frontière espace noyau/utilisateur. Ces opérations de copie mémoire mobilisent énormément l'unité centrale et nécessitent un temps de traitement relativement long. De plus, les opérations au niveau du pilote et de la pile qui surviennent entre les copies utilisent un nombre élevé de cycles d'UC.

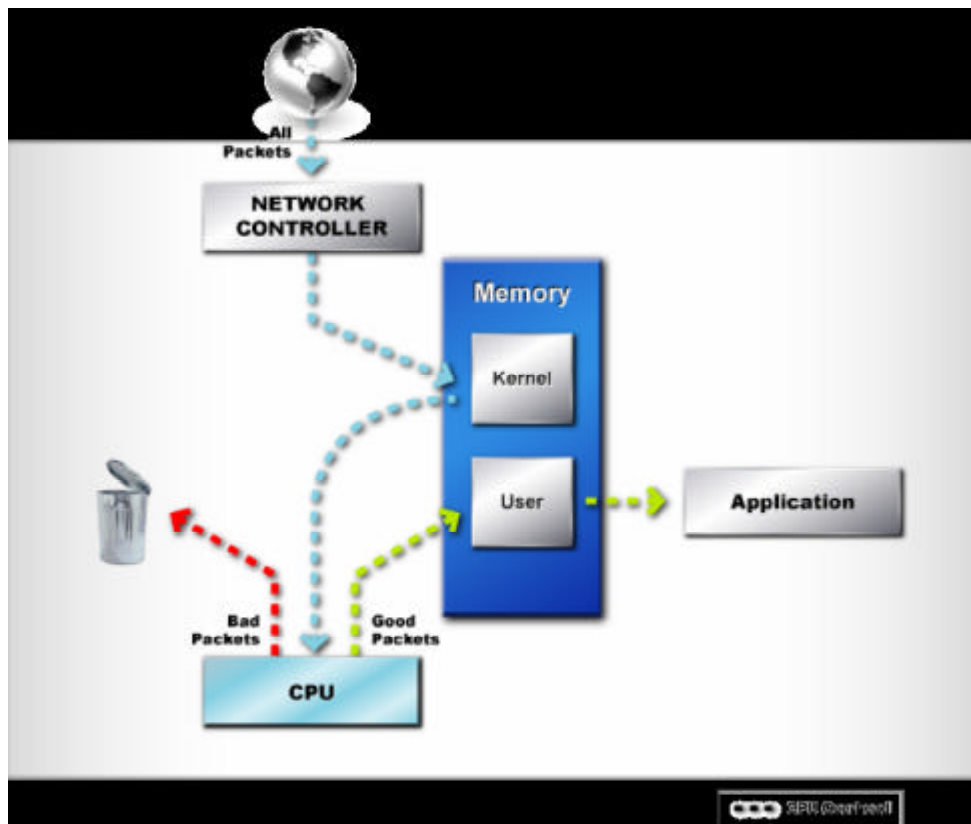


Figure 2 : Traitement des paquets actuel

Par comparaison, le moteur ActiveArmor écarte les mauvais paquets avant même que l'UC les détecte. En outre, les bons paquets sont mis sur une " voie expresse " et contournent le traditionnel processus de " pile réseau ", ce qui accélère le débit global et économise l'UC (voit Figure 3). Avec ActiveArmor, les bons paquets sont chargés directement dans la mémoire de l'application, ce qui évite à l'UC de traiter jusqu'à trois opérations lourdes de copie (du périphérique MAC au pilote, du pilote à la pile au sein de l'espace noyau et de la pile à l'application, ce qui implique la traversée de la frontière espace noyau/utilisateur).

Le moteur de gestion réseau sécurisé ActiveArmor traite tous les en-têtes de protocole pertinents et les valide par rapport à la liste de connexions autorisées et à l'état de connexion le plus récent de façon à garantir que seuls les paquets valides sont acceptés (ou autorisés) à transiter sur le réseau.

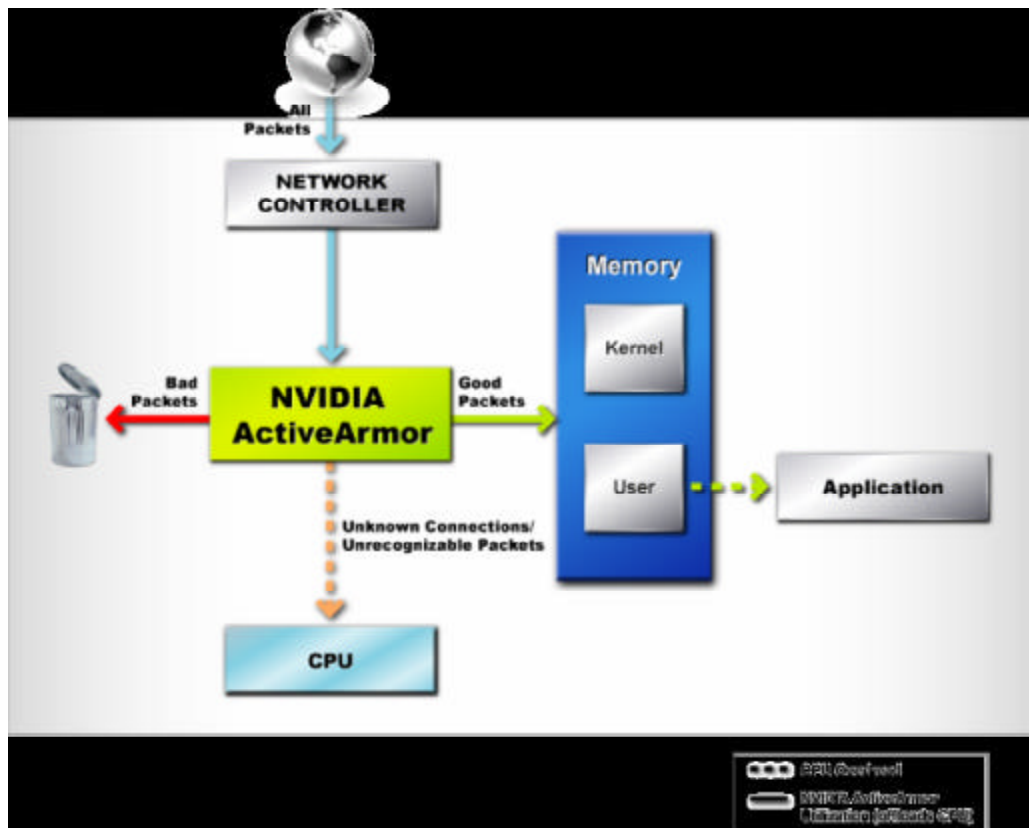


Figure 3 : Traitement des paquets effectué par NVIDIA ActiveArmor

En analysant les paquets au niveau du matériel et en plaçant les données qu'ils contiennent directement dans les tampons de l'application, ActiveArmor offre des performances optimales et la solution de sécurité réseau la plus efficace disponible sur toute plate-forme PC.

Outre son efficacité au niveau de l'analyse des paquets, ActiveArmor comprend trois autres fonctions majeures : une protection instantanée (*instant-on*), une fonctionnalité de résistance au sabotage et la prise en charge de l'architecture Microsoft TCP Chimney.

Protection *instant-on*

La solution de gestion réseau sécurisé NVIDIA offre une protection instantanée (*instant-on*) en protégeant la connexion réseau du PC dès l'instant où ce dernier est mis sous tension. Le PC est protégé en permanence, entre le moment où il est allumé et celui où il dispose de la protection par pare-feu. Cette protection instantanée est rendue possible par l'*intégration* d'un pilote incorporé et d'un traitement pare-feu dans le MCP NVIDIA nForce.

Les autres solutions logicielles, en revanche, accusent un manque de sécurité entre le moment où le PC est mis sous tension et celui où le logiciel de sécurité est chargé dans la mémoire. Ce laps de temps suffit aux pirates informatiques, qui parcourent constamment les réseaux à la recherche de PC non protégés, pour agir et attaquer l'ordinateur.

Sécurité renforcée et résistance au sabotage

Contrairement aux autres solutions de protection, les paramètres de sécurité de NVIDIA ActiveArmor comprennent un niveau d'analyse du trafic réseau extrêmement fin. Il permet de vérifier vos données en profondeur afin d'éliminer par filtrage tout trafic non autorisé ou suspect.

Ce niveau supérieur d'analyse et de filtrage est uniquement possible grâce à l'utilisation d'un moteur matériel dédié à ces tâches. Un moteur matériel dédié offre trois types d'avantages :

- ❑ Il renforce la sécurité en analysant les paquets en profondeur au niveau du matériel.
- ❑ Le niveau de sécurité maximal est atteint sans pour autant mobiliser l'UC et détériorer les performances système.
- ❑ Il résiste au sabotage. Toute tentative de désactivation ou de manipulation du contrôle et du filtrage des stratégies de pare-feu existantes a pour conséquence de désactiver la connexion réseau, ce qui protège le PC contre les accès non autorisés.

Prise en charge de l'architecture Microsoft TCP Chimney

NVIDIA ActiveArmor prend entièrement en charge la nouvelle architecture Microsoft TCP Chimney, autorisant l'accélération du protocole TCP/IP. En intégrant une stratégie de pare-feu dans l'architecture TCP/IP Chimney, NVIDIA bénéficie de deux avantages non négligeables : la réduction de la surcharge de l'UC due au traitement du trafic TCP/IP et un moteur d'application de la stratégie de sécurité qui garantit l'entrée et la sortie exclusives du trafic autorisé sur le PC.

NVIDIA ActiveArmor et la famille de MCP NVIDIA nForce4 comptent parmi les précurseurs sur le marché à intégrer la prise en charge de la nouvelle API Microsoft, consolidant ainsi la position de leader de NVIDIA dans ce domaine.

Conclusion

Les solutions de sécurité pour PC actuelles sont de type logiciel et consomment un grand nombre de cycles d'UC. Cette approche constitue un compromis entre la sécurité et la performance.

Mais quand il s'agit de sécurité, il ne devrait jamais y avoir de compromis. Les utilisateurs de PC sont en droit d'exiger les meilleures performances système sans pour autant compromettre la sécurité de leur système informatique !

Ce dilemme entre deux exigences concurrentes a été résolu grâce à l'introduction du moteur de gestion réseau sécurisé de NVIDIA. Ce moteur matériel dédié renforce la

sécurité du réseau en offrant un filtrage affiné des paquets au niveau du matériel tout en libérant l'UC du traitement des paquets transitant sur le réseau et via le pare-feu.
Résultat : l'utilisateur bénéficie à la fois d'une sécurité accrue et de performances système globale supérieures.



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

NVIDIA, le logo NVIDIA, ActiveArmor et NVIDIA nForce sont des marques ou 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 elles sont associées.

Droits d'auteur

© 2004 NVIDIA Corporation. Tous droits réservés.



NVIDIA.

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