



Descrizione tecnica

ActiveArmor e il firewall
a base hardware NVIDIA:
una soluzione di networking
sicura



I computer sono una parte integrante della vita di ogni giorno e la proliferazione delle connessioni Internet ad alta velocità implica che la maggior parte dei PC ora sono connessi a reti private o pubbliche. I PC contengono inoltre informazioni straordinariamente preziose (dati bancari o commerciali, MP3 o film digitali) e molte di queste informazioni risultano accessibili da siti bancari online o da servizi di download di brani musicali. Il fatto che oggi milioni di PC siano collegati a Internet offre agli utenti di PC la possibilità di accedere a preziose informazioni situate in siti Web di ogni parte del mondo. Ovviamente, questo offre anche agli hacker la possibilità di accedere a questi PC in rete. Gli hacker, sia quelli con intenti bonari che quelli più nocivi, sono costantemente alla caccia di PC non protetti. Le ricerche condotte da NVIDIA hanno dimostrato che gli hacker sono in grado di individuare un nuovo PC su una rete pubblica entro pochi minuti dalla connessione. Inoltre, i PC non protetti subiscono il caricamento surrettizio di applicazioni spyware, che poi comunicano informazioni sull'uso del PC a intrusi non autorizzati. Questa situazione è il motivo principale per il quale la sicurezza dei computer è diventata uno dei problemi principali degli utenti.

Una delle principali ragioni che rendono vulnerabili alle breche nella sicurezza e agli attacchi i PC è che sono collegati a reti *condivise* — abitazioni con più PC, ambienti di lavoro oppure Internet, dove milioni di PC sono collegati simultaneamente. È proprio all'interno di questi ambienti che si verifica la maggior parte degli attacchi a computer e che pacchetti dati dannosi raggiungono PC non protetti per danneggiarli.

Esistono numerose soluzioni per la protezione dei PC dagli attacchi. Una caratteristica comune della maggior parte delle soluzioni di sicurezza basate su PC è che sono *a base software*. Tuttavia, le soluzioni software sono particolarmente impegnative per la CPU, fatto che ha effetti negativi sulle prestazioni complessive del sistema e rende meno piacevole l'esperienza degli utenti. Inoltre, al contrario di quello che detta la logica comune, l'aggiunta di altri cicli della CPU non risolve il problema, dato che molti attacchi sono ultrasofisticati e ignorano o disattivano le soluzioni di sicurezza a base software.

Questo documento illustra nel dettaglio i vantaggi offerti dalla soluzione di networking sicura NVIDIA®, parte integrante degli MCP (media and communication processors - processori per media e comunicazioni) NVIDIA nForce™ 4. La soluzione di networking sicuro NVIDIA consiste della tecnologia a base hardware NVIDIA Firewall 2.0 nonché di NVIDIA ActiveArmor™, il primo motore di networking sicuro dedicato del settore.

Motore di networking sicuro NVIDIA ActiveArmor

NVIDIA ActiveArmor è un motore di networking sicuro integrato nella nuova famiglia di MCP NVIDIA nForce4. Una porzione dedicata del silicio che aumenta la sicurezza di networking mentre riduce il carico di lavoro della CPU, ActiveArmor offre livelli superiori di ispezione del traffico e di networking alle velocità massime garantite da gigabit Ethernet in full-duplex.

ActiveArmor offre le migliori prestazioni di sistema possibili grazie alla delegazione all'hardware NVIDIA delle impegnative attività di filtraggio dei pacchetti. Questo permette l'implementazione di ambienti di networking PC rapidi e sicuri contemporaneamente.

NVIDIA Firewall fondato sul motore di networking sicuro ActiveArmor

La sicurezza dei computer si articola su tre componenti indipendenti fra loro: un firewall, l'individuazione delle intrusioni e una protezione anti-virus. (Per ulteriori informazioni sui componenti di sicurezza del computer, fare riferimento alla documentazione tecnica: "Sicurezza NVIDIA – firewall personale e funzioni antihacking", TB-00982-001).

Il firewall è il componente portante di tutte le soluzioni di sicurezza per i computer. Questo dispositivo garantisce che solo i pacchetti dati conformi alle politiche definite possano oltrepassarlo. Per conseguire questo risultato, il firewall esamina ogni pacchetto dati che tenta di attraversarlo e determina se il suddetto pacchetto abbia attributi ammissibili. In caso negativo, il pacchetto viene bloccato. *Questa procedura è estremamente impegnativa per la CPU e può ridurre nettamente le prestazioni del sistema.*

La soluzione al problema del carico di lavoro eccessivo per la CPU è proprio l'introduzione di un motore hardware nel procedimento. Quando le funzionalità firewall sono accoppiate a un motore hardware dedicato, non si verifica alcuna riduzione delle prestazioni.

NVIDIA Firewall 2.0 ora si basa sul motore di networking sicuro NVIDIA ActiveArmor, soluzione che lo rende il primo vero firewall per PC a base hardware del settore. La combinazione di NVIDIA Firewall e del motore di networking sicuro NVIDIA ActiveArmor (figura 1) migliora il throughput di rete (a velocità gigabit Ethernet in full-duplex), riduce l'utilizzo della CPU ed esegue ispezioni approfondite dei pacchetti, migliorando pertanto la sicurezza di rete complessiva.

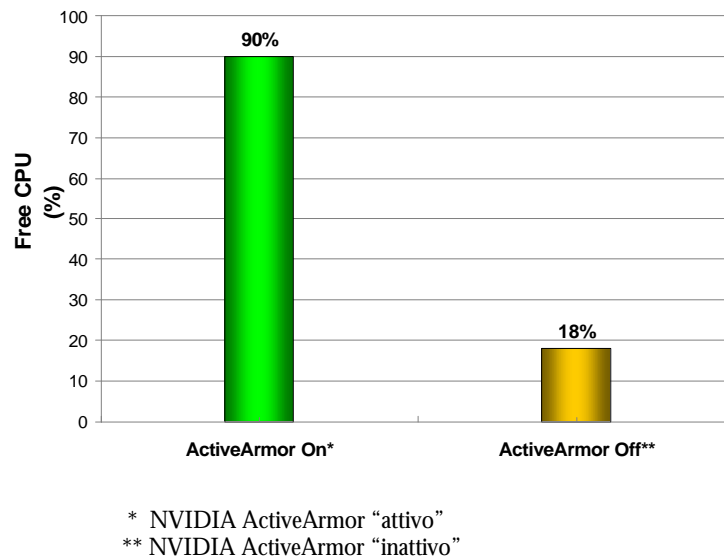


Figura 1. I firewall software sono estremamente impegnativi per la CPU

Utilizzo ridotto della CPU

Negli ambienti di networking tradizionali, l'ispezione dei pacchetti è un compito laborioso che grava sul carico della CPU, sulla banda passante di memoria e sulla latenza complessiva del sistema (figura 2). Per esempio, i pacchetti si spostano dal MAC al driver, quindi dal driver allo stack entro lo spazio del kernel e infine dallo stack all'applicazione, fase che prevede l'attraversamento del confine kernel/spazio utente. Tutte queste operazioni di copia in memoria sono particolarmente impegnative per la CPU e decisamente lente, mentre l'elaborazione di driver e stack che si verifica tra le copie utilizza un numero eccessivo di cicli della CPU.

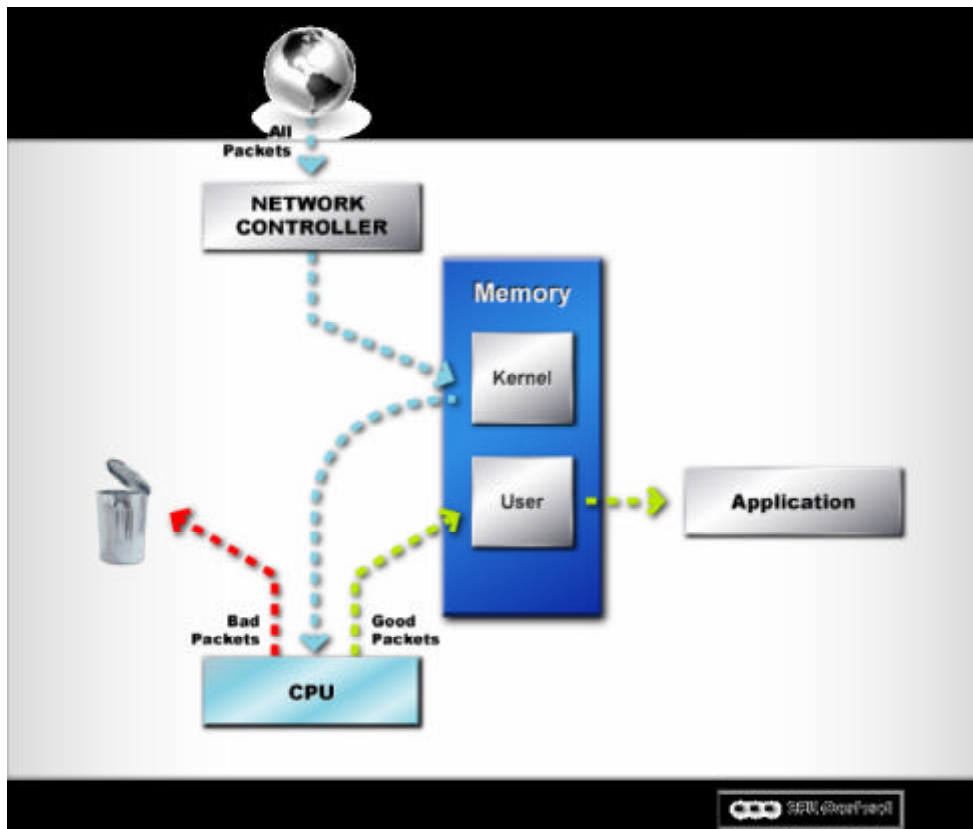


Figura 2. Attuale modello di elaborazione dei pacchetti

Invece, il motore di networking sicuro ActiveArmor scarta i pacchetti errati ancora prima che la CPU li prenda in considerazione. Inoltre, i pacchetti corretti prendono una “corsia espresso” e ignorano il tradizionale processo di “stack di rete”, migliorando il throughput complessivo e riducendo l’utilizzo della CPU (figura 3). Grazie ad ActiveArmor, il payload di tutti i pacchetti corretti viene collocato direttamente nella memoria dell’applicazione, soluzione che permette di evitare sino a tre operazioni di copia impegnative per la CPU (dal MAC al driver, dal driver allo stack entro lo spazio del kernel e dallo stack all’applicazione, fase che prevede l’attraversamento del confine kernel/spazio utente).

Il motore di networking sicuro ActiveArmor processa tutti gli header di protocollo pertinenti e li convalida in base all’elenco delle connessioni consentite e allo stato della connessione più recente in modo che la rete accetti il transito dei soli pacchetti validi.

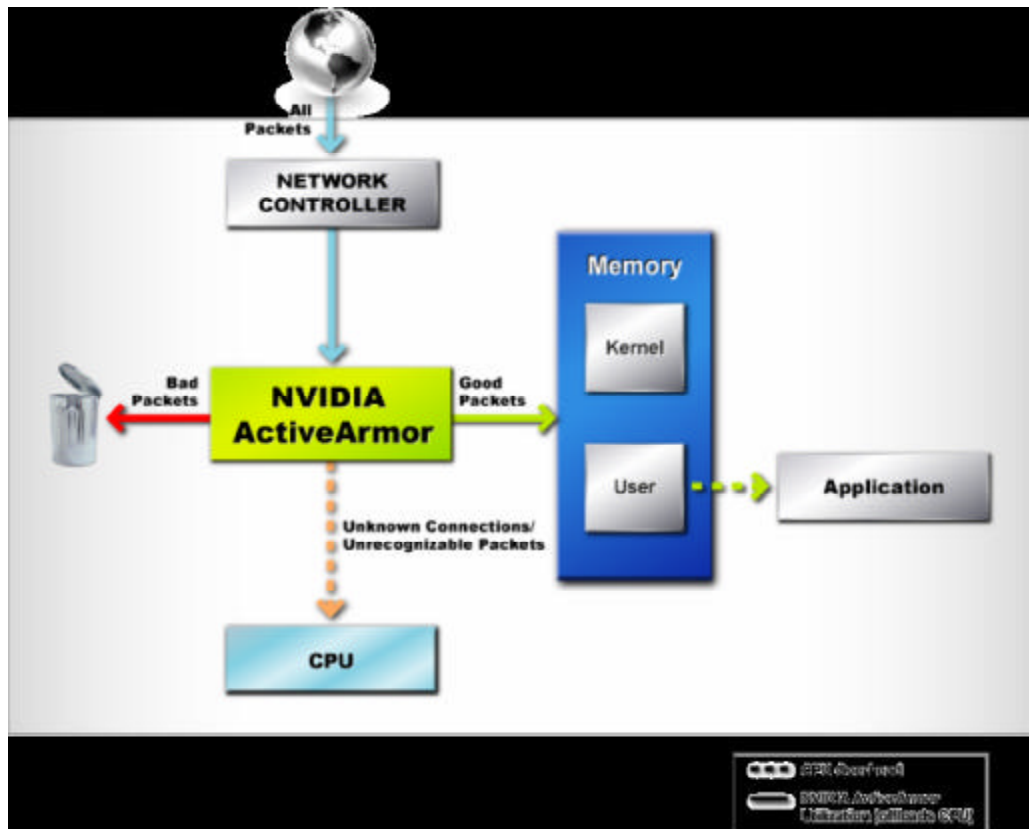


Figura 3. Elaborazione dei pacchetti con NVIDIA ActiveArmor

Grazie all'esame dei pacchetti nell'hardware e alla collocazione dei dati dei pacchetti direttamente nei buffer dell'applicazione, ActiveArmor fornisce le massime prestazioni e la soluzione di sicurezza del networking più efficiente tra quelle disponibili per qualsiasi piattaforma PC.

Oltre all'efficienza della sua procedura di ispezione dei pacchetti, ActiveArmor offre anche altri tre importanti caratteristiche: protezione instant-on, funzionalità antimanomissione e supporto per l'architettura Microsoft TCP Chimney.

Protezione Instant-On

La soluzione di networking sicura di NVIDIA offre una protezione "instant-on" offrendo una connessione di rete per PC sicura sin dall'avvio. Non esiste alcun gap di sicurezza tra il momento dell'avvio del PC e la disponibilità della protezione del firewall. Questa protezione instant-on viene realizzata *integrando* un'elaborazione driver e firewall incorporata negli MCP NVIDIA nForce.

Al contrario, tutte le altre soluzioni software presentano un intervallo tra l'accensione del PC e il momento in cui il software di sicurezza viene caricato in memoria. Questo piccolo intervallo non protetto è tutto ciò di cui hanno bisogno gli

hacker, che effettuano costanti scansioni delle reti per individuare PC non protetti, per fare la propria mossa e attaccare.

Sicurezza perfezionata e funzione antimanomissione

A differenza di altre soluzioni di sicurezza, le impostazioni di sicurezza di NVIDIA ActiveArmor offrono un livello di ispezione più profondo del traffico di rete consentendo una verifica accurata dei dati per filtrare ogni traffico non autorizzato o comunque sospetto.

Questo livello più elevato di ispezione e filtraggio può essere ottenuto solo utilizzando un motore hardware dedicato. I vantaggi derivanti dall'uso di un motore hardware dedicato sono essenzialmente tre:

- ❑ la soluzione presenta un livello di sicurezza superiore grazie all'offerta di un'ispezione più approfondita dei pacchetti eseguita nell'hardware.
- ❑ Questo livello superiore di sicurezza non ha alcun costo supplementare per la CPU e non riduce le prestazioni del sistema.
- ❑ Si tratta di una soluzione antimanomissione. Qualsiasi tentativo di disabilitare o manipolare il controllo delle politiche del firewall e del filtraggio disabilita il collegamento di rete, proteggendo il PC da qualsiasi accesso non autorizzato.

Supporto per l'architettura Microsoft TCP Chimney

NVIDIA ActiveArmor supporta pienamente la nuova architettura Microsoft TCP Chimney, che consente l'accelerazione del protocollo TCP/IP. Grazie all'integrazione di una politica firewall nell'architettura TCP/IP Chimney, NVIDIA offre due importanti vantaggi — una netta riduzione del carico di lavoro della CPU nell'elaborazione del traffico TCP/IP e un motore di attuazione della politica di sicurezza che garantisce il transito nel PC del solo traffico autorizzato.

NVIDIA ActiveArmor e la famiglia di MCP NVIDIA nForce4 sono fra i primi prodotti del settore a incorporare il supporto per la nuova API Microsoft, rafforzando la posizione di leadership detenuta da NVIDIA in quest'area.

Conclusione

Le attuali soluzioni di sicurezza per PC sono basate sul software e assorbono una grande quantità di cicli della CPU. Questo approccio è una sorta di compromesso che tenta di bilanciare sicurezza e prestazioni.

Tuttavia, quando si tratta di sicurezza, non ci dovrebbero essere compromessi. Gli utenti di PC meritano di disporre delle massime prestazioni di sistema senza alcun compromesso in termini di sicurezza!

Il dilemma di come rispondere con efficacia a entrambi questi requisiti in conflitto reciproco è stato risolto dall'introduzione del motore di networking sicuro di

NVIDIA. Il nuovo motore hardware dedicato di NVIDIA perfeziona la sicurezza di rete dato che offre il filtraggio profondo dei pacchetti a base hardware pur demandando all'hardware NVIDIA gli impegnativi calcoli per l'elaborazione del firewall e dei pacchetti di rete. Il risultato è una maggiore sicurezza e prestazioni del sistema nettamente superiori.



Notifica

TUTTE LE SPECIFICHE DI PROGETTAZIONE NVIDIA, LE SCHEDE DI RIFERIMENTO, I FILE, I DISEGNI, LA DIAGNOSTICA, LE LISTE E ALTRI DOCUMENTI (UNITAMENTE E SEPARATAMENTE, DEFINITI "MATERIALI") SONO FORNITI NELLO STATO IN CUI SI TROVANO. NVIDIA NON OFFRE GARANZIE, ESPRESSE, IMPLICITE, STATUTARIE O DI ALTRO TIPO IN RELAZIONE AI MATERIALI, E RIFIUTA ESPRESSAMENTE OGNI GARANZIA IMPLICITA DI NON VIOLAZIONE, COMMERCIALIZZABILITÀ E IDONEITÀ A SCOPI SPECIFICI.

Le informazioni fornite sono ritenute accurate e affidabili. Tuttavia, NVIDIA Corporation non si assume alcuna responsabilità per le eventuali conseguenze derivanti dall'uso di tali informazioni o da qualsiasi violazione di brevetti o altri diritti di terze parti che possono conseguire dal loro uso. Non viene concessa alcuna licenza implicita o in altro modo in base a nessun brevetto o diritto di autore di proprietà di NVIDIA Corporation. Le specifiche tecniche menzionate nella presente pubblicazione sono soggette a modifica senza preavviso. Questa pubblicazione rimpiazza e sostituisce tutte le informazioni precedentemente fornite. Non si autorizza l'impiego dei prodotti di NVIDIA Corporation come componenti cruciali di dispositivi per il supporto vitale o per sistemi che non abbiano ricevuto l'espressa approvazione scritta di NVIDIA Corporation.

Marchi

NVIDIA, il logo NVIDIA, ActiveArmor e NVIDIA nForce sono marchi registrati o marchi di NVIDIA Corporation negli Stati Uniti e in altri paesi. Altri nomi di società e di prodotti possono essere marchi o marchi registrati dei rispettivi detentori.

Copyright

© 2004 NVIDIA Corporation. Tutti i diritti riservati.



NVIDIA.

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