



Technische Übersicht

NVIDIA Firewall

PC-Sicherheit und Hackerabwehr

PC-Sicherheit und Hackerabwehr

Einführung

Ob bei der Arbeit oder in der Freizeit, Computer sind aus unserem täglichen Leben nicht mehr wegzudenken. Mit ihren teilweise wertvollen Datenbeständen sind sie jedoch auch ein interessantes Angriffsziel für Hacker und andere Cyberkriminelle. Die Computer- und Datensicherheit ist daher mit Recht eines der wichtigsten Themen in der modernen, vernetzten Welt.

Zu einer soliden Sicherheitsstrategie müssen immer drei Komponenten gehören: Eine Firewall, eine Lösung zur Erkennung von Angriffen (ein so genanntes Intrusion-Detection-System) und ein effizienter Virenschutz.

Die Firewall ist dabei das Kernstück einer Sicherheitslösung. Sie garantiert, dass nur Datenpakete passieren können, die genau festgelegten Sicherheitskriterien entsprechen. Zu diesem Zweck prüft sie jedes ankommende Datenpaket anhand eines Regelsatzes und entscheidet dann, ob es weitergeleitet oder verworfen wird. Firewalls können also unbefugten Zugriff auf einen PC durch interne oder externe Angreifer sehr wirkungsvoll eindämmen – besonders dann, wenn sie direkt in die Treibersoftware des PCs integriert sind.

NVIDIA® Firewall ist die erste Firewall, die auf der Security-Engine NVIDIA ActiveArmor™ basiert. Dieses Konzept garantiert maximale Leistung bei sehr geringer CPU-Belastung. Gleichzeitig ermöglicht es hardwarebasierte Packet Inspection, bietet Instant-On-Schutz und verhindert Manipulationen durch unbefugte Programme oder Anwender.

Firewalls

Hintergrund und Einsatzzweck

Netzwerkdaten bestehen aus *Paketen*, die in ihren *Headern* (den Kopfabschnitten) bestimmte Metadaten mit sich führen. Diese Metadaten garantieren, dass das Paket den richtigen Weg durch Heim- und Fremdnetze bis hin zum gewünschten Prozess auf dem Zielhost findet. Für ersteres sind die Angaben in den so genannten Data Link Layer- und Network Layer-Headern zuständig, für letzteres sorgt der Transport Layer-Header. So ist sichergestellt, dass ein Rechner im Internet Datenpakete an einen beliebigen anderen Rechner im Internet schicken kann, solange er nur dessen IP-Adresse kennt.

Die meisten dieser Pakete sind harmlos und legitim. Immer wieder gibt es jedoch Angreifer, die mit besonders geformten Datenpaketen versuchen, Schwächen und Sicherheitslücken in der Protokollsoftware oder dem Betriebssystem eines Rechners auszunutzen. Ziel solcher Attacken ist es, den betreffenden Rechner durch eine Flut von Daten oder Anfragen in die Knie zu zwingen (ein so genannter *Denial-of-Service-Angriff*) oder sich unbefugt Zugang zum Rechner zu verschaffen.

Um die Zahl der möglichen Angriffspunkte zu verringern, ist in den meisten Heim- und Unternehmensnetzwerken der Verbindungsweg ins Internet genau definiert. Nur über eine beschränkte Anzahl von Knotenpunkten (wie zum Beispiel DSL-Modems oder Router) können Pakete aus dem internen Netz ins Internet gelangen und umgekehrt. An diesen Knotenpunkten kann nun mittels einer entsprechenden Hardware- oder Softwarekomponente – der *Firewall* – genau kontrolliert und geregelt werden, welche Pakete diese „unsichtbare Grenze“ überqueren dürfen und welche nicht.

Funktionsweise

Firewalls filtern den Netzwerk-Datenverkehr anhand verschiedener Kriterien. Eine der grundlegendsten Verfahrensweisen hierfür ist sicherlich die Filterung nach Paketart. Die Firewall kann den TCP- bzw. UDP-Port eines Datenpakets ermitteln und dann auf der Grundlage einer zuvor definierten Regeltabelle entscheiden, ob das Paket durchgelassen oder abgewiesen wird.

Beim Einsatz einer solchen Paketfilter-Firewall gibt es zwei grundsätzliche, unterschiedliche Vorgehensweisen:

- ❑ Die Firewall kann entweder prinzipiell den gesamten Datenverkehr zulassen und nur bestimmte Pakete und Ports, die als gefährlich erachtet werden, sperren, oder aber
- ❑ prinzipiell den gesamten Datenverkehr sperren und nur solche Pakete durchlassen, die explizit als ungefährlich definiert worden sind.

Letztendlich wird die Firewall-Strategie somit zu einer Entscheidung über das vertretbare Risiko. Durch eine entsprechende Firewall-Konfiguration kann der externe Datenverkehr ins interne Netzwerk restriktiver gehandhabt werden, womit natürlich auch das damit verbundene Risiko sinkt. In der Regel ist in solchen Situationen für einen Angreifer überdies nicht direkt ersichtlich, welche Arten von Datenverkehr die Firewall zulässt und welche nicht. So stehen ihm wenige Informationen über mögliche Angriffswege und Hintertüren zur Verfügung.

Firewall-Typen

Stateless-Firewall

Die Stateless-Firewall ist ein sehr rudimentäres Firewall-Konzept und existiert in verschiedenen Inkarnationen nun schon seit Beginn der 90er Jahre des vergangenen Jahrhunderts. Eine Stateless-Firewall arbeitet mit einer Liste von Regeln, die Datenverkehr eines bestimmten Typs entweder zulassen oder sperren. Nur Datenpakete, die einem zulässigen Typ angehören, können die Firewall passieren. Die Regeln können sowohl auf ankommenden als auch auf abgehenden Datenverkehr angewendet werden und eine Reihe von Kriterien umfassen:

Ethernet-Typ, IP-Absender- bzw. Zieladresse, IP-Optionen, IP-Protokoll, ICMP-Typ und/oder -Code, TCP-/UCP-Absender-/Zielpport oder TCP-Optionen.

Besteht ein Paket diese Prüfung, so kann es passieren, anderenfalls wird es verworfen. In dieser Prüfung liegt jedoch auch das Hauptproblem dieses Firewall-Ansatzes: Jedes Paket muss in Kombination mit allen Regeln geprüft werden, was sehr schnell zu Grenzen hinsichtlich der Skalierbarkeit führt. Je mehr Regeln hinzugefügt werden, desto aufwändiger wird die Überprüfung eines jeden Pakets – die Leistung in Paketen pro Sekunde sinkt, die CPU-Belastung steigt. Effizient lassen sich Stateless-Firewalls daher eigentlich nur noch für ganz bestimmte Paketarten wie beispielsweise ICMP-Pakete einsetzen, die schon von Natur aus „stateless“ sind.

Auch die NVIDIA Firewall unterstützt dieses Stateless-Inspection-Verfahren und kann den Datenverkehr anhand von Ethernet-Typ, IP-Protokoll und IP-/TCP-Optionen filtern. Soweit möglich werden dabei IPv4 und IPv6 gleichermaßen unterstützt; beispielsweise lassen sich sowohl IPv4-Optionen als auch die Extension-Header von IPv6 als Filterelemente verwenden.

Stateful-Firewall

Die Stateful-Firewall ist eine Variante der Stateless-Firewall. Beim Aufbau einer neuen Datenverbindung ist ihre Arbeitsweise daher auch weitgehend mit einer Stateless-Firewall identisch: Protokoll, Absender- und Empfängeradresse der ersten Pakete müssen den lokal definierten Regeln entsprechen, damit die Verbindung zustande kommt.

Allerdings wird das ursprüngliche Verfahren der Stateless-Firewall bei der Stateful-Firewall insoweit optimiert, als diese detaillierte Prüfung nur beim Verbindungsaufbau, d. h. nur bei den ersten Paketen der Verbindung stattfindet. Wenn die Prüfung ergibt, dass die Verbindung legitim ist, wird diese in eine Verbindungstabelle aufgenommen. Folgepakete werden nun einfach daraufhin überprüft, ob sie einer auf diese Weise überprüften Verbindung angehören; falls ja, können sie ohne eine erneute vollständige Prüfung passieren. Diese Lösung hat den Vorteil, dass eine Stateful-Firewall dasselbe Sicherheitsniveau wie eine Stateless-Firewall bei deutlich niedrigerer CPU-Belastung bietet.

Die NVIDIA Firewall unterstützt dieses sog. Stateful-Inspection-Verfahren sowohl für TCP- und UDP-Verkehr. UDP-States werden durch Beobachtung neu ankommender UDP-Pakete ermittelt; ein State wird nur erzeugt, wenn die Pakete die vom Anwender definierten Regeln erfüllen.

Für den Abgleich der Pakete mit den definierten Regeln kommt ein Hash-Wert aus verschiedenen Feldern des Paket-Headers zum Einsatz. Hierbei kann es sich beispielsweise um die Absender- und Ziel-IP-Adresse, das verwendete IP-Protokoll (TCP, UDP oder ein anderes Transport-Layer-Protokoll) und die Absender-/Zielports handeln. Der Zeitaufwand für die Berechnung eines Hash-Werts aus diesen fünf Werten ist ungleich geringer als bei einer vollständigen Prüfung und bleibt zudem immer konstant.

Aus diesem Grund hängt die Prüfgeschwindigkeit einer Stateful-Firewall auch nicht davon ab, wie komplex das verwendete Regelwerk ist. Eine Stateless-Firewall hingegen muss für jedes Paket alle Regeln (oder zumindest eine für eine definitive Entscheidung ausreichende Anzahl von Regeln) anwenden, um zum gleichen Ergebnis zu kommen. Die zur Paketanalyse erforderliche Zeit steigt daher mit der Anzahl der verwendeten Regeln linear an, während die Leistung entsprechend linear sinkt. Bei Stateful-Firewalls zeigt sich diese Problematik nicht.

Gateways auf Anwendungsebene (Application-Level Gateways)

Die dritte und potenziell sicherste Möglichkeit, eine Firewall zu implementieren, ist die Realisierung als Gateway auf Anwendungsebene (auch als Application-Layer Gateway oder Transport-Layer Bridge bezeichnet). Hierbei kommt ein dediziertes Rechnersystem zum Einsatz, auf dem für jede zulässige Anwendung ein spezieller Proxy-Dienst läuft. Ganz offensichtlich müssen diese Proxy-Server strengste Anforderungen hinsichtlich Sicherheit und Stabilität erfüllen, da sie sonst selber zusätzliche Sicherheitslücken aufreißen.

Eine direkte Weiterleitung von Paketen findet bei einem solchen Gateway nicht statt. Wenn ein Paket beim Gateway ankommt, werden zunächst seine Header entfernt und sein Inhalt wird überprüft. Legitime Pakete werden anschließend mit einem neuen Header versehen in einer neuen Verbindung an den Ziel-Host weitergeschickt.

Für den Endanwender ist ein solches Gateway ebenso transparent wie eine Paketfilter-Firewall, wenn man einmal davon absieht, dass die durch die Prüfung verursachten Verzögerungen eventuell etwas länger ausfallen können. Der Vorteil liegt in der logischen „Luftschleuse“, die zwischen den beiden Netzwerken entsteht.

Der größte Nachteil einer Gateway-Lösung liegt in ihrer Protokollabhängigkeit. Damit Datenverkehr die Firewall passieren kann, muss ein entsprechender Proxy-Server für das jeweils verwendete Protokoll vorhanden sein. Für gängige Protokolle wie SMTP, FTP, HTTP oder Telnet ist dies in aller Regel auch der Fall; exotischere Protokolle können den Anwender jedoch vor gewisse Probleme stellen. Innerhalb dieses eingeschränkten Rahmens sind Gateway-Firewalls jedoch die beste und sicherste Lösung, um sicherzustellen, dass nur legitimer Datenverkehr die Firewall passieren kann.

Gateway-Firewalls benötigen dedizierte Hardware und werden in der Regel nur an den Berührungspunkten zwischen zwei Netzwerken eingesetzt. Als Endpoint-Firewall unterstützt die NVIDIA Firewall daher keine derartige Gateway-Funktionalität.

Firewalls zur Hackerabwehr (Anti-Hacking)

Beim so genannten IP-Spoofing werden IP-Pakete mit gefälschten Absenderadressen versehen, um mit ihrer Hilfe bestimmte Angriffe zu starten. Am bekanntesten (und gängigsten) sind in dieser Hinsicht vermutlich DDoS-Attacken (Distributed Denial-of-Service), bei denen eine Vielzahl „gekaperter“ Rechner gleichzeitig ein bestimmtes Ziel angreift. Solche DDoS-Angriffe sind auf zwei Faktoren angewiesen: 1. an das Internet angebundene Systeme (oft PCs), die der Angreifer ohne Wissen der Besitzer für seine Zwecke nutzt – die so genannten „Zombies“ –, sowie 2. die Möglichkeit, diese Zombie-PCs auf Befehl hin Datenpakete mit gefälschten IP-Absenderadressen verschicken zu lassen.

Für Firewalls stellt es nun natürlich kein Problem dar, Datenverkehr anhand der IP-Adresse zu filtern. Herauszufinden, ob die IP-Adresse möglicherweise gefälscht ist, ist dagegen schon schwieriger. Die Firewall könnte beispielsweise untersuchen, ob es angesichts der ihr bekannten Routing-Regeln plausibel erscheint, dass ein Paket mit einer bestimmten Absenderadresse auf einer bestimmten Netzwerkschnittstelle ankommt. Für Firewalls, die lediglich irgendwo an einer Zwischenstation im Datenstrom sitzen, ist diese Entscheidung jedoch nur schwer zu treffen.

Die beste Strategie gegen IP-Spoofing ist es daher, die gefälschten Pakete schon an der Quelle abzufangen – also noch auf den Zombie-PCs. Wird eine Anti-Spoofing-Lösung direkt in die Netzwerkhardware und -software des PCs integriert, so tragen alle von diesem PC abgehenden Datenpakete immer die korrekte, statisch oder per DHCP zugewiesene Absenderadresse.

Weitere wichtige Sicherheitskomponenten

Für sich betrachtet stellt die Firewall eine wichtige Komponente der gesamten Sicherheitslösung dar – sozusagen das Fundament. Eine vollständige, zuverlässige

Sicherheitslösung verfügt jedoch noch über weitere Schichten, die auf diesem Fundament aufbauen.

Die NVIDIA Firewall beschränkt sich auf ihre Kernfunktionalität und bietet daher keine dieser Zusatzfunktionen. Mit leistungsfähigen Zusatzprodukten lässt sich jedoch eine Komplettlösung zusammenstellen, die den individuellen Anforderungen des Anwenders gerecht wird.

Schutz vor Eindringlingen

So genannte Intrusion-Detection-Lösungen analysieren den gesamten ankommenden Datenverkehr auf Daten- und Verhaltensmuster, die auf einen laufenden oder bevorstehenden Angriff eines bekannten Typs hindeuten. Beispielsweise ist es bei Angreifern gängige Praxis, zunächst alle Ports des Zielsystems abzufragen, um auf diese Weise herauszufinden, ob sich hinter einem der Ports möglicherweise eine Softwarekomponente mit bekannten Sicherheitslücken verbirgt. Wird ein solcher „Portscan“ frühzeitig erkannt, bleibt also eventuell noch genügend Zeit für Abwehrmaßnahmen.

Intrusion-Prevention-Lösungen gehen noch einen Schritt weiter und können eine Reihe bekannter Angriffe direkt erkennen und abwehren, bevor Schaden entsteht.

In beiden Fällen jedoch ist die Abwehrsoftware auf eine möglichst breite Datenbasis mit vorhandenen Referenzmustern für bekannte Angriffe angewiesen. Neue Arten von Angriffen werden von derartigen Produkten in der Regel nicht erkannt, da noch keine entsprechende Signatur vorliegt.

Virenschutz

Antiviren-Software schützt den PC vor bekannten Viren und Trojanern. Wie schon die oben genannte Intrusion-Detection- und Intrusion-Prevention-Software ist auch Antiviren-Software auf vorhandene Definitionen der bekannten Viren und Schädlingsprogramme angewiesen.

Verschiedene Antiviren-Softwarelösungen können den Anwender darüber hinaus auf verdächtige Aktivitäten aufmerksam machen, die möglicherweise von einem noch nicht bekannten Virus stammen.

NVIDIA Firewall

NVIDIA Firewall basiert auf NVIDIAs Security-Netzwerkengine ActiveArmor und ist damit die erste echte hardwarebasierte PC-Firewall auf dem Markt. Dank dieser dedizierten Engine muss die NVIDIA Firewall keine Rechengänge auf den Hauptprozessor auslagern – die CPU-Belastung bleibt also sehr niedrig (s. Abb. 1).

Die Kombination aus NVIDIA Firewall und ActiveArmor bietet Performance auf vollem Gigabit-Ethernet-Niveau, unterstützt Deep Packet Inspection und sorgt insgesamt für bessere Netzwerksicherheit.

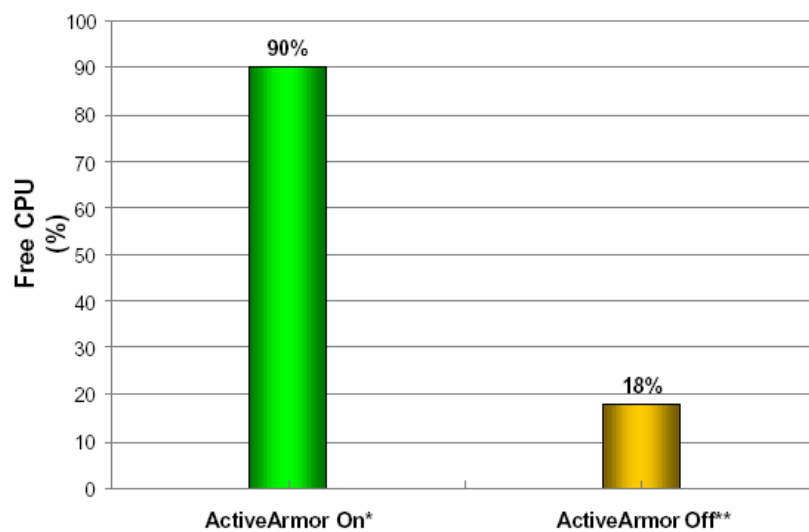


Abb. 1: NVIDIA ActiveArmor: Maximale Performance, minimale CPU-Belastung

Die NVIDIA Firewall integriert sowohl Firewall- als auch Anti-Hacking-Funktionen. Auf der Firewall-Seite unterstützt sie Stateless- und Stateful-Inspection, Web-basiertes Management, vordefinierte Sicherheitsprofile, Portsperrungen/-filter, eine intelligente Anwendungsüberwachung (Intelligent Application Manager), Remote-Verwaltung und stellt zudem einen bedienerfreundlichen Assistenten bereit. Die Antihacking-Funktionen hingegen wirken gezielt gegen IP-Spoofing, Sniffing, ARP-Cache-Poisoning und nicht autorisierte DHCP-Server – Funktionen, die besonders im Unternehmenseinsatz wertvoll sind.

In einer solchen Umgebung können Endpoint-/Desktop-Firewalls mit integrierten Anti-Hacking-Funktionen intern verursachte Sicherheitsattacken deutlich reduzieren, indem sie unbefugten Datenverkehr bereits an der Quelle abfangen. Eine solche Maßnahme steigert das allgemeine Sicherheitsniveau und entlastet das IT-Personal.

Umfassende Managementfunktionen

Die NVIDIA Firewall bietet eine Vielzahl komfortabler Managementfunktionen. Konfiguration und Überwachung lassen sich über eine browserbasierte Oberfläche auch remote erledigen, zudem stehen eine Befehlszeilenschnittstelle und WMI-Skriptmöglichkeiten zur Verfügung. Die Erstkonfiguration wird durch einen benutzerfreundlichen Assistenten erleichtert.

Bei aller Bedienerfreundlichkeit bleibt die NVIDIA Firewall dennoch äußerst flexibel und leistungsfähig.

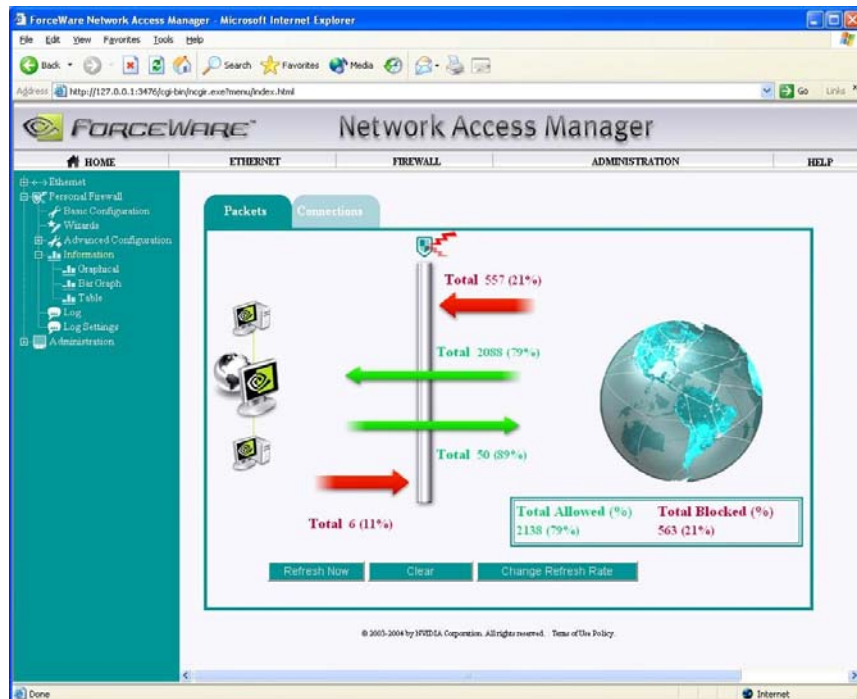


Abb. 2: Einfache Konfiguration über die Web-basierte Browseroberfläche

Intelligent Application Manager (IAM)

Der Intelligent Application Manager erweitert die ohnehin schon umfangreichen Filterfunktionen der NVIDIA Firewall um Filterregeln auf Anwendungsebene. Dabei spielt es keine Rolle, ob die betreffenden Anwendungen als Clients oder Server fungieren. Auf diese Weise kann der Anwender selbst entscheiden, welchen Datenverkehr er zulassen oder sperren will (siehe Abb. 3). Ist der Zugriff für eine bestimmte Anwendung einmal zugelassen, kann diese Anwendung fortan ohne weiteren Konfigurationsaufwand Verbindungen öffnen.

Gleichzeitig wird verhindert, dass eine Anwendung (wie z. B. ein Wurm oder ein anderes Schadprogramm) Daten vom PC aussendet, ohne dass der Benutzer zunächst ausdrücklich Datenverkehr für diese Anwendung zulässt. Dabei kann IAM sogar die auf dem PC vorhandenen Anwendungen überwachen und erkennen, wenn Änderungen daran vorgenommen werden – beispielsweise, wenn eine legitime Anwendung von einem Virus befallen oder von einem Schadprogramm überschrieben wird.

Ebenso kann IAM ankommenden Datenverkehr überwachen. Für Trojaner und Spyware-Programme wird es dadurch deutlich schwieriger, als Server zu agieren und ohne das Wissen des Benutzers Daten von außen zu empfangen. Dabei kann IAM nicht nur nach Ports filtern, sondern auch das Öffnen von Sockets komplett verhindern, um den Empfang von Daten auf der Anwendungsschicht ganz zu unterbinden.

So schützt IAM den PC sowohl gegen Angriffe von außen als auch gegen Schadprogramme, die versuchen, den PC unbemerkt für Angriffe auf andere PCs zu verwenden.

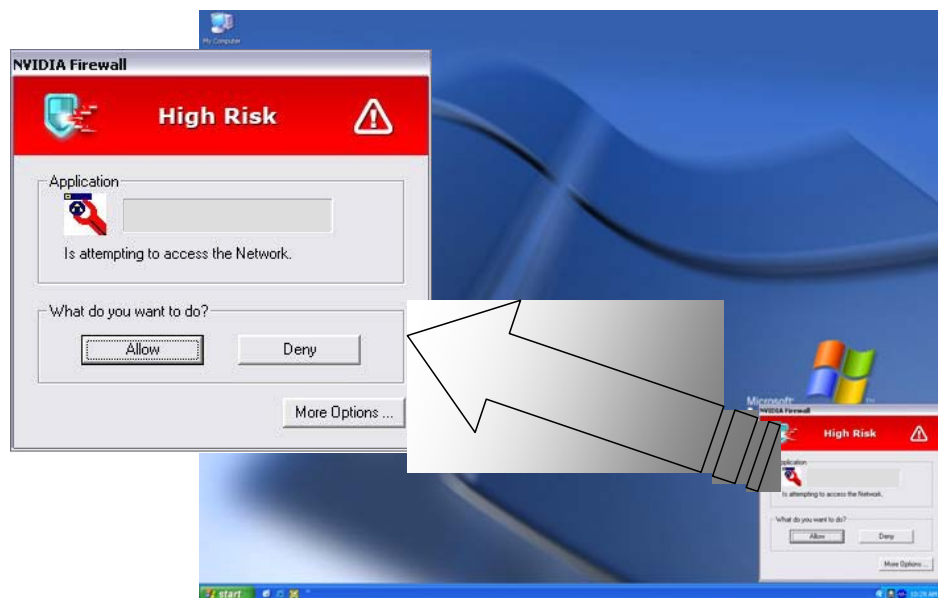



Abb. 3: IAM warnt, wenn unbekannte Anwendungen versuchen, auf das Netzwerk zuzugreifen

Warum NVIDIA Firewall?

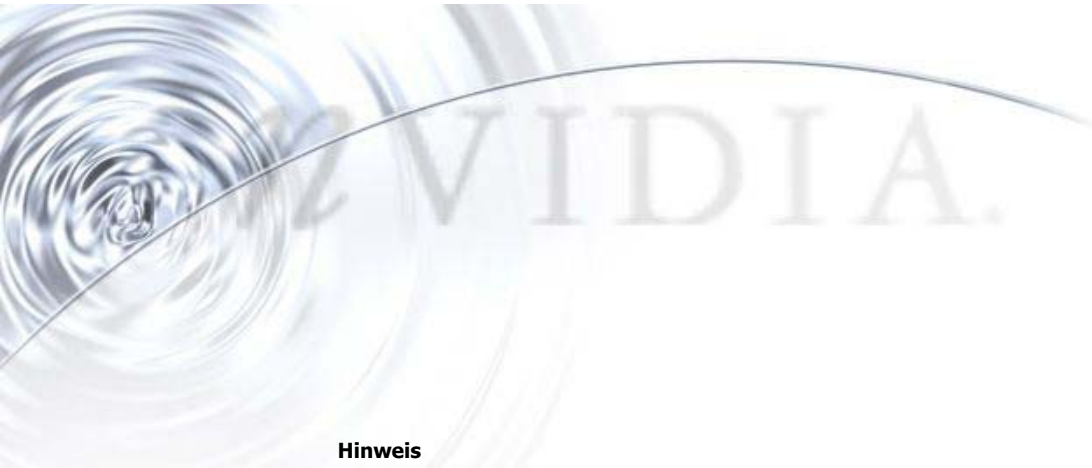
Die meisten derzeit verfügbaren PC-Firewalls sind softwarebasierte Produkte, die lediglich auf das bestehende System aufgesetzt werden. Im Gegensatz dazu ist die NVIDIA Firewall die erste echte hardwarebasierte PC-Firewall auf dem Markt. Mit ihrem NVIDIA ActiveArmor-Konzept bietet sie deutlich verbesserten Schutz gegen Angriffe und Schadprogramme.

Darüber hinaus verfügt die NVIDIA Firewall über umfassende Managementfunktionen wie Remote-Konfiguration und -Überwachung und lässt sich über einen benutzerfreundlichen Assistenten sehr komfortabel einrichten. Der Intelligent Application Manager (IAM) erleichtert dem Benutzer die Arbeit auf Anwendungsebene.



Als Endpoint-Firewall eignet sich die NVIDIA Firewall hervorragend, um in Firmenumgebungen allgemeine Client-Sicherheitsrichtlinien konsequent umzusetzen und die Anwender-Desktops zu schützen. Auch im Privatbereich schützt sie beispielsweise PCs, die über eine Breitbandverbindung ständig ans Internet angebunden sind, vor unbefugtem externen Zugriff.

Für optimalen Rundumschutz lässt sich die NVIDIA Firewall zusätzlich mit geeigneter Antiviren- und Intrusion-Detection-Software kombinieren.



Hinweis

ALLE NVIDIA-DESIGNSPEZIFIKATIONEN, REFERENZPLATINEN, DATEIEN, ZEICHNUNGEN, DIAGNOSEPROGRAMME, LISTEN UND SONSTIGEN DOKUMENTE (EINZELN ODER IM GANZEN ALS „MATERIALIEN“ BEZEICHNET) WERDEN „AS IS“ („WIE BESEHEN“) BEREITGESTELLT. NVIDIA GIBT HINSICHTLICH DER MATERIALIEN KEINERLEI GARANTIE, UNABHÄNGIG DAVON, OB DIESE AUSDRÜCKLICH, KONKLUDENT, GESETZLICH ODER ANDERWEITIG BEGRÜNDET SIND. INSBESONDERE WERDEN AUSDRÜCKLICH KEINERLEI GARANTIE HINSICHTLICH DER NICHTVERLETZUNG VON URHEBERRECHTEN, DER MARKTGÄNGIGKEIT SOWIE DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ÜBERNOMMEN.

Die in diesem Artikel genannten Informationen sind nach bestem Wissen und Gewissen zutreffend und verlässlich. Die NVIDIA Corporation übernimmt jedoch keinerlei Verantwortung für Konsequenzen, die aus der Nutzung dieser Informationen entstehen, bzw. für Patentrechtsverletzungen oder andere Verstöße gegen die Rechte Dritter, die aus einer solchen Nutzung entstehen. Es wird weder konkludent noch anderweitig eine Lizenz im Rahmen eines Patents oder eines Patentanspruchs der NVIDIA Corporation gewährt. Die in diesem Artikel genannten Spezifikationen können sich jederzeit ohne weitere Ankündigung ändern. Dieser Artikel löst alle eventuell vorab bereitgestellten Informationen ab und ersetzt diese. Ohne die ausdrückliche vorherige schriftliche Genehmigung der NVIDIA Corporation dürfen Produkte der NVIDIA Corporation nicht als missionskritische Komponenten in lebenserhaltenden Geräten oder Systemen eingesetzt werden.

Warenzeichen/Marken

NVIDIA, das NVIDIA-Logo und NVIDIA nForce sind Warenzeichen und/oder eingetragene Marken der NVIDIA Corporation. Bei anderen Firmen- und Produktnamen kann es sich um Warenzeichen der jeweils damit verbundenen Unternehmen handeln.

Copyright

© 2004 NVIDIA Corporation. Alle Rechte vorbehalten.



NVIDIA.

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