

# Application Delivery Networks – mehr Wissen für fundierte Geschäftsentscheidungen

Dietmar Schnabel

**Zukünftig benötigen Unternehmen mehr Einblick in ihren Netzverkehr, um Anwendungen und deren Leistungsfähigkeit zu messen. Sie müssen gezielt geschäftskritische Programme priorisieren und beschleunigen können. Und: Sicherheitsregeln müssen im gesamten Unternehmen und für alle Mitarbeiter gültig und durchsetzbar sein – egal an welchem Ort und zu welcher Zeit. Application Delivery Networks (ADN) setzen genau hier an.**

Die klassischen Netze stehen vor einem Wandel: Genügte es früher, Datenpakete überhaupt von A nach B transportieren zu können, forderten die Nutzer schnell mehr Geschwindigkeit bei der Übertragung der Daten. Auch hier ist zwischenzeitlich eine Grenze erreicht – sowohl bei verfügbarer Bandbreite auf bestimmten Übertragungswegen als auch durch die Architektur der Übertragungsprotokolle. Zusätzlich steigen im Netz die Anforderungen nach Sicherheit und einem Zugriff auf Informationen von überall zu jeder Zeit. Gleichzeitig stehen die IT-Verantwortlichen unter enormem Kostendruck und müssen ihre Ressourcen effizient und sparsam verwenden.

## Neuer Ansatz für künftige Geschäftsanforderungen

Maßnahmen wie die Konsolidierung von Servern oder die Einführung konvergenter Netze für die Übertragung von Sprache, Videos und Daten stellen hohe Anforderungen an bestehende Netze. Mobile Anwendungen und Geräte sind zusätzlich gefährdet durch bösartigen Schadcode oder Datendiebstahl. Und globale IT-Infrastrukturen gleichen oft eher riesigen Datensilos, in denen unzählige Informationen schlummern, die IT-Verantwortliche nur mit Mühe durchforsten und verwalten können. Es fehlt schlicht der Überblick über die gesammelten Informationen. Gleichzeitig steigen die Anforderungen, mittels IT ressourcenschonend, sicher und effizient das Maxi-

mum an Informationen aus dem bestehenden Datenpool herauszufiltern. Eine schier unlösbare Aufgabe vor allem für Netze, die zwar im Laufe der Zeit an Leistung und Intelligenz hinzugewonnen haben, denen aber nach wie vor die klare Einsicht fehlt, welche Pakete sie eigentlich von A nach B befördern.

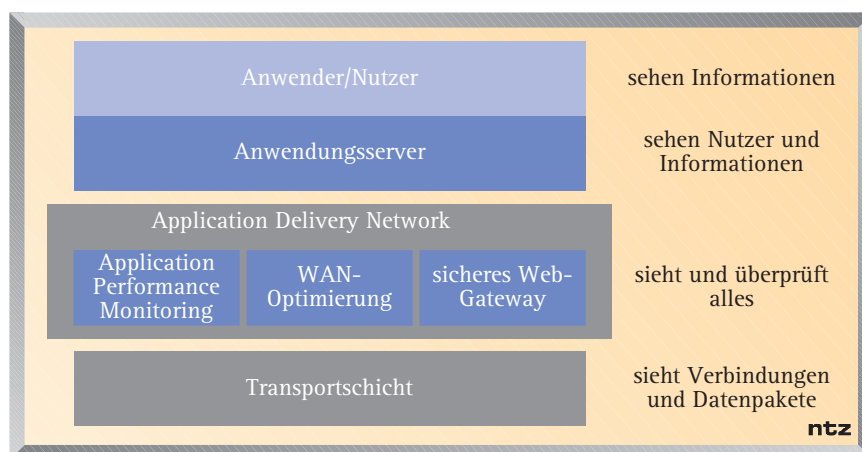
Vor allem die Netzleistung wird zunehmend zur kritischen Größe in Unternehmen. Denn viele Geschäftstrans-

## Auf einen Blick

**Application Delivery Networks (ADN) ermöglichen es Unternehmen, mehr Informationen über ihren Datenverkehr zu erhalten, geschäftskritische Anwendungen gezielt zu beschleunigen sowie ihr gesamtes Netz besser kontrollieren und absichern zu können.**

aktionen hängen bereits in hohem Maß von Software-as-a-Service-Angeboten (SaaS) wie Salesforce.com oder von Unified Communications wie Videokonferenzen oder Instant Messaging ab. Service-orientierte Architekturen (SOA) kombinieren darüber hinaus eine Reihe von Anwendungen und Daten aus vielfältigen Quellen. Für Unternehmen wird es also wichtig, dass ihre IT-Infrastruktur in der Lage ist zu erkennen, welche Art von Datenverkehr und Anwendung geschäftskritisch ist und welche nicht. Es gilt, die Netzleistung so gut wie möglich zu optimieren – d.h. wichtige Anwendungen zu beschleunigen, unerwünschte Anwendungen oder bösartige Inhalte zu stoppen und den übrigen Datenverkehr effizient zu verwalten.

Ein Schritt in diese Richtung ist der Aufbau konvergenter Netze für die Sprach-Daten-Video-Kommunikation. Der Vorteil dieser Netze liegt auf der Hand: Sie sind schnell, verlässlich, er-



Ein Application Delivery Network setzt direkt auf der Transportschicht des Netzes auf und besteht aus den drei Komponenten Application Performance Monitoring, WAN-Optimierung und einem sicheren Web-Gateway

möglichen Echtzeitkommunikation, bieten eine unvergleichliche Mobilität der Informationen und somit erhöhte Flexibilität für die Mitarbeiter. Zudem ermöglichen sie unmittelbar den Austausch einer Vielzahl von Datentypen mit einer ebenso großen Vielzahl von Endgeräten – und das überall auf der Welt. Doch: Unternehmen müssen sich heute auch fragen, wie sie trotz dieser neuen Formen der Kommunikation und des Informationsaustauschs über eine Vielzahl von Anwendungen ihre allgemein gültigen Sicherheitsrichtlinien einhalten und durchsetzen können. Und wie sie Sicherheitsrisiken minimieren und somit die gültigen Compliance-Anforderungen erfüllen können.

## **Neuer Layer für intelligente Steuerung**

Eines der größten Hindernisse für die schnelle, sichere und zuverlässige Bereitstellung von Anwendungen und Informationen liegt derzeit in der Transportschicht (Connectivity) von Netzen. Netze routen und liefern Datenpakete auf dieser Schicht zwar sehr effektiv. Sie können aber keine Auskunft darüber geben, ob die von ihnen transportierten Daten nützlich, schädlich oder gar katastrophal sind. Um Schlüsse für das gesamte Netz zu ziehen, die Aussagen zur Qualität der Netztransaktionen, der Anwendungsleistung sowie der Nutzererfahrung liefern, ist eine neue zusätzliche Steuerungsschicht im Netz nötig. Sie soll helfen, zuverlässig Anwendungen bereitzustellen und nicht nur Pakete von A nach B zu transportieren.

## **Application Delivery Networks (ADN)**

Unternehmen können heute zwar einzelne Belange in Hinblick auf die Leistung von Anwendungen regeln. Doch fehlt ihnen nach wie vor eine Schicht, die mehr liefert als Anwendungen lediglich am Laufen zu halten. Denn in Zukunft müssen Unternehmen die Anwendungen, die über das Netz laufen, erkennen, ihnen Bandbreite im Netz optimal zuteilen und dazu die richtigen Anwendungen priorisieren. Und sie müssen den Nutzern den Zugriff auf geschäftskritische Anwendungen von überall und zu jeder Zeit sicher, effizient und schnell ermöglichen. Eine Aufgabe, bei der sogenannte Application Delivery Networks wertvolle Unterstützung

und somit Wettbewerbsvorteile liefern können. Im Wesentlichen setzt ein ADN direkt auf der Transportschicht des Datennetzes auf und besteht aus den drei Komponenten „Application Performance Monitoring“, WAN-Optimierung und einem sicheren Web-Gateway, Bild.

## **Application Performance Monitoring**

Um diese Aufgabe gut zu erfüllen, kommt es auf mehrere Faktoren an: Das Wichtigste ist es für die IT-Verantwortlichen, den kompletten Verkehr in ihrem Netz zu erkennen. Das bedeutet, Unternehmen benötigen intelligente Instrumente, die mehrere hundert Anwendungen erkennen, die jeden Tag über das Netz laufen. Nur so ist eine Unterscheidung möglich, welche Anwendung geschäftskritisch ist, welche Schadcode enthält und welche eher der Entspannung dient wie beispielsweise iTunes oder Peer-to-Peer-(P2P-)Anwendungen. Zudem ist eine weitere Unterscheidung komplexer Anwendungen wie z. B. Webgestützter Suiten beispielsweise von Oracle oder SAP erforderlich.

Unternehmen müssen erkennen können, welcher Anwender wichtige Aufgaben bearbeitet und dazu entsprechend die höchste Priorität und die meiste Bandbreite erhalten sollte. Dazu benötigen sie Präventivsysteme, die in der Lage sind, Anwendungsverhalten zu messen und frühzeitig Alarmmeldungen abzusetzen, bevor ein Fehler die Anwender bei ihrer Arbeit beeinträchtigt. Ein Beispiel wäre die zu hohe Auslastung der Bandbreite durch P2P-Anwendungen, die dann geschäftskritischen Anwendungen Bandbreite wegnimmt und die Produktivität der Mitarbeiter beeinträchtigt.

Probleme mit der Leistung von Anwendungen können aus einer Vielzahl von Gründen auftreten. Das wiederum bedeutet, dass die IT-Abteilung eine Reihe von Instrumenten zur Hand haben sollte, die eine schnelle Analyse und Auswertung des Problems ermöglichen: Ist es eine Verzögerung zwischen Server und Netz? Bereitet ein bestimmter Host Schwierigkeiten? Welche Anwendungen oder Server bereiten die meisten Geschwindigkeitsprobleme? Und was verursacht das Problem? Ist es eine Lastspitze für eine bestimmte Anwendung? Liegt es am Protokoll? Nur ein effizientes und schnelles Eingrenzen der Ursache

ermöglicht es, das Problem so schnell wie möglich zu beheben.

All diese Aufgaben wurden von vielen IT-Abteilungen bisher mit einer Vielzahl von Produkten und Lösungen unterschiedlicher Hersteller auf der Verbindungsebene des Netzes realisiert. Das kann in der Summe nicht nur zu Kompatibilitätsproblemen führen, sondern es ist langfristig weniger kosteneffektiv und wirkt sich damit auch auf die Rendite (ROI, Return on Invest) und den Aufwand für die Verwaltung der Systeme aus. Es bietet sich also an, in eine integrierte, skalierbare Lösung zu investieren. Diese sollte neben Anwendungsbeschleunigungs- und -steuerungstechniken auch Funktionen für „Service-Level“-Maßnahmen und statistische Berichtsauswertungen bieten, um auftretende Probleme schnell und effizient lokalisieren zu können.

## **Optimierung im Weitverkehrsnetz**

Gerade in Unternehmen mit vielen weltweit verteilten Niederlassungen ist die Leistungsfähigkeit der Anwendungen ein wichtiger Baustein für erfolgreiche Geschäfte. Vor allem Mitarbeiter, die in Außenstellen, im Heimbüro oder auch von unterwegs über ein Weitverkehrsnetz auf Server in der Unternehmenszentrale zugreifen, beklagen sich oft über zu langsame Anwendungen. Diese Wahrnehmung hat in der Praxis mehrere Ursachen: Einerseits konkurriert der interne Verkehr mit dem Internetverkehr auf der WAN-Strecke um Bandbreite. Andererseits beeinflussen externe Anwendungen und ineffiziente Protokolle sowie lange Entfernungen die „gefühlte“ Anwendungsleistung durch hohe Latenzzeiten. Abhilfe schaffen hier Lösungen zur WAN-Optimierung, die durch Kompression, Caching auf Objekt- und Byte-Ebene, Protokolloptimierung und Priorisierung den Datenverkehr zwischen Zentrale und entfernten Mitarbeitern effizient beschleunigen.

Dabei geht es jedoch nicht nur um die reine Beschleunigung. Denn wer einfach seinen gesamten Verkehr beispielsweise auf der Strecke von einer Außenstelle über die Unternehmenszentrale bis in das Internet beschleunigt, spart zwar auf dem gesamten Weg Bandbreite und damit letztlich Leitungskosten. Doch kommen auf dieser Verbindung dann sowohl weniger wichtige Anwendungen

wie E-Mail als auch schädliche Programme wie Spyware und Trojaner in den Genuss einer schnelleren Weiterkehrsstrecke.

Eine neue Herausforderung ist zukünftig auch der richtige Umgang mit bislang klassischen „Freizeitwendungen“ wie YouTube oder Instant Messaging. Denn diese Anwendungen werden zunehmend auch für geschäftsrelevante Zwecke genutzt. Die Herausforderung ist es, zwischen geschäftlichem Zugriff und privaten Aktivitäten zu unterscheiden, dabei die Kontrolle über die Netzressourcen im Unternehmen zu behalten und gleichzeitig mögliche bösartige Inhalte aus dem Netz herauszuhalten, die Huckepack über solche Anwendungen eingeschmuggelt werden können. Echtzeitanwendungen wie z.B. Voice over IP, Videokonferenzen, Kreditkarten- oder Finanztransaktionen sowie Auftragsbearbeitung sind ebenfalls sehr anfällig für Verzögerungen bei der Datenübertragung. Und sie zählen zu den wichtigsten Geschäftsanwendungen überhaupt und müssen jederzeit rund um die Uhr verfügbar sein.

WAN-Optimierungslösungen helfen Unternehmen also, ihre Geschäftsdaten bis hin zum Endgerät optimal zu verwalten und zu schützen. Das wiederum ermöglicht es, Unternehmensrichtlinien wirklich durchzusetzen und Daten vor Diebstahl, Verlust oder schadhafter Massenvermehrung zu schützen.

### Sicheres Web-Gateway schützt das Netz

Man weiß nie, welche neue Form von Malware über den Netzzugang einzubrechen versucht, um dann Finanzdaten zu stehlen oder zu manipulieren, persönliches auszuspähen oder Informationen über Kundenbeziehungen abzugreifen. Daher ist es am besten, mögliche Geschäftsrisiken oder Gefährdungen von vornherein zu erkennen und gleich am Eingang zum Netz abzuwehren.

Gerade für große Unternehmen besteht die Herausforderung darin, ihre

## Anforderungen an ein Application Delivery Network (ADN)

Ein ADN sollte folgende Funktionen bieten:

### Einsicht in den Datenverkehr:

- Automatisch mehrere Hundert Anwendungen erkennen und unterscheiden.
- Freizeitwendungen wie P2P oder Streaming-Anwendungen über jeden Port erkennen.
- Komplexe Anwendungen wie SAP, Oracle, Citrix, Web, CIFS, MAPI und DCOM unterteilen, um dem wichtigsten Arbeitsvorgang Priorität zuzuteilen.
- URL und externe Websites innerhalb eines HTTP-Datenstroms erkennen.
- Identifizieren, welche Hosts, Server oder Anwender Probleme bereiten.

### Beschleunigung:

Ein umfangreiches Set von Beschleunigungstechniken bieten und dabei sowohl interne, externe, verschlüsselte sowie Echtzeitanwendungen erkennen. Zu den Beschleunigungstechniken zählen dabei:

- Objekt- und Byte-Caching.
- Kompression und Basis-Dienstgüteklassifizierungen.
- Beschleunigung für externen Webverkehr und SSL-verschlüsselten Datenverkehr.
- Protokollbeschleunigung für TCP, CIFS/NFS, MAPI, HTTP und andere.
- Moderne Managementfunktionen für Bandbreite und Web-Policies.

### Sicherheit:

- Scannen auf Viren und Malware.
- Filtern von Webinhalten und URL.
- Zentrale Verwaltung auch an verteilten Gateways.
- Granulare Regelverwaltung, u. a. nach einer Vielzahl von Variablen inklusive Nutzer, Nutzergruppen, Anwendungen, Quelle, Art des Dateninhalts und Art der Transaktion.
- Funktionen für Logging, Statistikauswertungen und SNMP-Unterstützung.

globale Sicherheit zu gewährleisten ohne die globale Handlungsfähigkeit zu verlieren. Um das gesamte Unternehmen zu schützen, ist es nötig, jeden Zugangspunkt dazu abzusichern – sowohl die Geräte als auch die Mitarbeiter selbst. Daher sollte jede IT-Strategie die folgenden vier Sicherheitsanforderungen erfüllen:

- **Schutz vor Malware:** Techniken einer Reihe führender Hersteller helfen beim Schutz vor Malware, indem sie ein- und ausgehenden Web-Datenverkehr in Echtzeit kontrollieren.
- **Die Produktivität der Mitarbeiter im Auge behalten:** Nicht alle Freizeitwendungen sind für Unternehmen kontraproduktiv. Unternehmen müssen nur die richtigen Instrumente nutzen, um zu erkennen, wann Freizeitwendungen die Bandbreite beeinträchtigen und die Produktivität der Mitarbeiter leidet, sodass sie die Nutzung entsprechend der Unternehmensrichtlinien und der geschäftlichen Anforderungen steuern können.
- **Informationslecks verhindern:** Unternehmen sollten sicherstellen, dass ihre Mechanismen zum Schutz vor Datenverlust in der Lage sind, den Versuch von Datendiebstahl aus Datenbanken oder anderen wertvollen Unternehmensquellen zu erkennen, einen Alarmierungsprozess anzustoßen und so den Verlust der Daten zu verhindern.

- **Vertrauen bestätigen:** Im Endeffekt müssen sich Unternehmen von innen nach außen absichern, denn geschäftliche Verluste können viele Ursachen haben: Informationsdiebstahl, Ausfallzeiten, gesunkene Produktivität, versehentliche oder absichtliche Datenkorruption und vieles mehr. Bei all diesen Gefahren fragt man sich schnell, ob und wie man es jemals schaffen soll, sein Unternehmen vor all diesen Gefahren abzusichern. Die Integration umfangreicher Funktionen für URL-Filterung, „Data Leakage Prevention“, Malware-Schutz, „Policy Management“ und Identitäts-Authentifizierung in das bestehende Netzmanagement-Arsenal hilft bereits, den gesamten Ansatz in Bezug auf die Unternehmenssicherheit ganz wesentlich zu verbessern.

Application Delivery Networks bilden also eine neue intelligente Schicht im Netz, die es ermöglicht, Anwendungen und Anwender über das gesamte Netz eines Unternehmens hinweg zu identifizieren und zu klassifizieren. So kann sie den ganzen Datenverkehr im Netz erkennen, die Nutzererfahrung mit den Anwendungen beobachten und Leistungsprobleme aufdecken und beheben, bevor sie die Anwender in ihrer Arbeit beeinträchtigen. ■



**Dietmar Schnabel**  
ist Sales Director  
DACH & Eastern Europe  
bei Blue Coat Systems  
in München.