

Die drei Elemente eines Application Delivery Networks: Transparenz, Beschleunigung, Sicherheit

„Zunächst muss ein Unternehmen überhaupt sehen können, welche Anwendungen über das WAN laufen“, erklärt Walzer. „Dann kann es entscheiden, welche Applikationen beschleunigt werden und welche gegebenenfalls gar nicht erst in das WAN dürfen.“

Ein ADN sorgt daher zunächst einmal für maximale Transparenz im aktuellen Netzwerkgeschehen. Dazu muss es jedes Datenpaket im WAN bis hinauf zur Anwendungsschicht analysieren und im ersten Schritt die dazugehörige Anwendung identifizieren. Eine simple Zuordnung von Ports zu Anwendungen auf Layer 4 reicht dabei nicht aus. Das zeigt beispielsweise die populäre Nutzung, des in Firewalls in der Regel offenen Port 80, durch zahlreiche andere Anwendungen. Auch ist Webverkehr nicht Webverkehr. So sollte beispielsweise die Kommunikation mit Salesforce.com oder einem internen webbasierten CRM-System einen höheren Stellenwert erhalten als etwa ein Youtube-Video.

Durch eine zuverlässige Identifikation von Anwendungen erhalten Netzwerkmanager einerseits Einblick darin, was in ihrem Weitverkehrsnetzwerk überhaupt abläuft. Andererseits sorgt ein ADN auch für Transparenz im Anwendungsverhalten. Dazu liefern Monitoring-Funktionen Informationen über Verzögerungen (Delay), Laufzeitunterschiede (Jitter), Paketverluste und den Durchsatz jedes einzelnen Datenstroms. Nur so lassen sich Service Level Agreements für die einzelnen Unternehmensapplikationen festlegen, dokumentieren, dauerhaft überprüfen und auch Ursachen für deren Verletzung finden.

Nach Transparenz kommt Beschleunigung

Weiß ein Unternehmen, welche Anwendungen für wie viel Verkehr verantwortlich sind, kann es Entscheidungen über geeignete Maßnahmen zur Beschleunigung der wichtigsten Applikationen treffen. Dies hängt dabei stark von der jeweiligen Situation ab. Nehmen etwa zahlreiche FTP-Sessions oder große E-Mail-Attachments den Citrix-Clients zu viel Bandbreite weg, kann eine entsprechende Priorisierung des ICA- (Intelligent Console Architecture) oder RDP-Verkehrs (Remote Desktop Protocol) für schnellere Reaktionszeiten am Terminalclient sorgen. Telefoniert hingegen die Belegschaft in der Außenstelle privat mit Skype oder betreibt ein Mitarbeiter MP3-Tausch über ein Peer-to-Peer-Netz, so sorgt die Blockade dieser Anwendungen sofort für mehr Platz auf der WAN-Leitung.

Haben alle erwünschten Anwendungen ihre den Unternehmenszielen entsprechende

Anwendungen über das WAN beschleunigen

Von Georg von der Howen

Nicht nur Unternehmen können mithilfe eines Application Delivery Networks (ADN) die Übertragung von Daten zwischen Zentrale und Niederlassung beschleunigen. Auch Carrier und Serviceprovider profitieren von ADN. Sie können zum Beispiel ihren Datenverkehr differenzierter priorisieren als mit MPLS.

■ Typischerweise binden Unternehmen entfernte Niederlassungen per Standleitung oder VPN an ihre Zentrale an. Dieses „Backhaul“ genannte Verfahren ermöglicht Benutzern einerseits, auf einen zentralen Mailserver zuzugreifen. Andererseits können Unternehmen so an zentraler Stelle Richtlinien für die Nutzung des Internets durchsetzen und gleichzeitig den Internetverkehr auf Schadcode prüfen.

Beginnt eine Organisation dann damit, ihre Server in einem zentralen Rechenzentrum zu konsolidieren, muss auch der Verkehr zwischen den entfernten Clients und dem Datenspeicher durch das Nadelöhr WAN. Und dies führt zu einem Phänomen, das viele Anwender frustriert: langsame Anwendungen.

Viel hilft oft nur wenig

Das Problem kennt auch Martin Walzer, Manager Systems Engineering Dach & Eastern Europe bei Blue Coat Systems: „Die erste Reaktion von Unternehmen ist oft der Versuch, langsame Dateizugriffe oder stockende An-

wendungen mit mehr Bandbreite zu beschleunigen – was meist nicht funktioniert. Denn beispielsweise das Cifs-Protokoll (Common Internet File System), das Windows-Server für ihre File-Services nutzen, ist im WAN-Einsatz so ineffizient, dass mehr Bandbreite kaum einen Geschwindigkeitszuwachs beim Öffnen und Speichern von Dateien bringt.“

Abhilfe versprechen so genannte WAN Optimization Controller (WOC), die den kompletten Verkehr von der Zentrale zu den Außenstellen beschleunigen. Doch reine WOCs haben den Nachteil, dass sie im schlimmsten Fall die private Internetnutzung in den Außenstellen oder die Übertragung von Spyware beschleunigen, während die für das Unternehmen wichtigen Anwendungen weiterhin nur zäh reagieren und die Anwender verärgern.

An dieser Stelle kommt ein so genanntes Application Delivery Network (ADN) ins Spiel. Dessen vielfältige Aufgaben lassen sich zu drei großen Gruppen zusammenfassen: Transparenz, Beschleunigung und Sicherheit.

Priorität erhalten und sind unerwünschte Applikationen außen vor, können im nächsten Schritt Beschleunigungstechnologien für schnelleres Anwendungsverhalten sorgen. Den ersten Ansatzpunkt bietet dabei bereits das TCP-Protokoll (Transmission Control Protocol). Neben Standard-Optimierungsfunktionen wie Windows Scaling (RFC 1323) oder TCP Selective Acknowledgements (RFC 2018) bietet auch die Reaktion auf Paketverluste großes Geschwindigkeitspotenzial.

Weitere Ansatzpunkte für anwendungsübergreifende Beschleunigung sind die Kompression der Paketzustand sowie das Caching von Paketdaten auf Byte-Ebene (Byte Caching). Um diese Funktionen ohne Änderungen an Anwendungen zur Verfügung stellen zu können, arbeiten die dafür zuständigen WAN Optimization Controller an beiden Enden einer WAN-Verbindung als transparente Proxies – selbst wenn einige Hersteller diesen Begriff explizit so nicht verwenden.

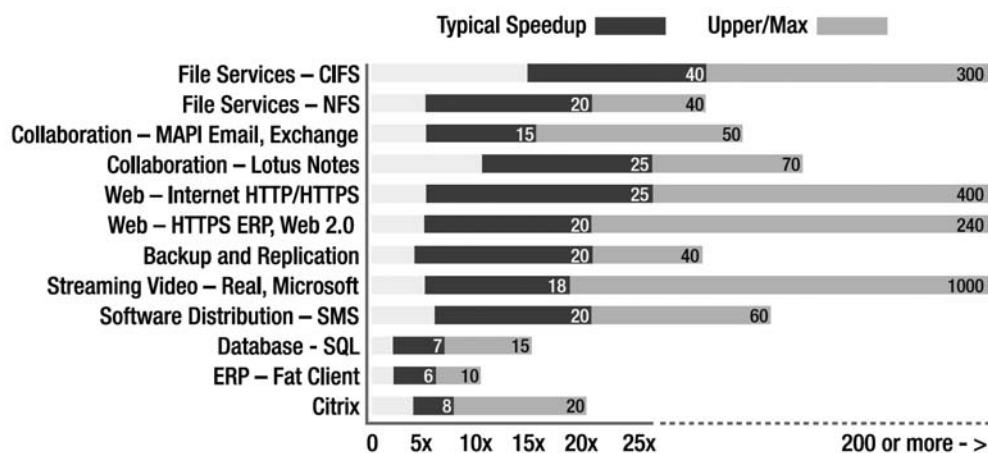
Dedizierte Proxys und Sicherheit

Während transparente Proxies TCP-Verkehr auf Paketebene beschleunigen, gehen dedizierte Proxies für häufig verwendete Protokolle noch einen Schritt weiter: So ist das anfangs erwähnte Cifs ein sehr „geschwätziges“ Protokoll, das durch unzählige Requests und Acknowledgements während des Öffnens und Speicherns einer Datei für enormen Overhead sorgt. Ein Cifs-Proxy kann hier ansetzen und die Gesprächsfreudigkeit auf das notwendige Minimum reduzieren, was der Endanwender direkt durch schnellere Lade- und Speichervorgänge von beispielsweise Office-Dokumenten spürt. Dedizierte Proxies können zudem komplette Dateien zwischenspeichern. Gleichzeitig sorgen sie dafür, dass die lokalen Kopien immer mit dem Original synchron sind und übertragen bei Änderungen an einer Datei nur das jeweilige Delta über das WAN.

Der dritte Funktionsblock eines ADNs ist der Bereich Sicherheit. Viele Unternehmen nutzen inzwischen statt Standleitungen ein VPN (Virtual Private Network), um ihre Außenstellen an die Zentrale anzubinden. Da erscheint es bei genauerer Betrachtungsweise als unlogisch, den legitimen Internetverkehr der Niederlassungen weiterhin über das WAN in die Zentrale zu führen, statt ihn direkt vor Ort in die Weiten des Webs zu entlassen. Voraussetzung dafür ist allerdings, dass in den Außenstellen dieselben Sicherheitsmechanismen greifen wie am zentralen Gateway – zum Beispiel Schutz vor Viren und Spyware. Gleichzeitig sollten auch webbasierte Unternehmensanwendungen wie Webex beschleunigt werden können, selbst wenn die Kommunikation SSL-verschlüsselt ist. Ein ADN stellt alle dazu notwendigen

funkschau Grafik

Mögliche Beschleunigung einzelner Applikationen



Typische und maximale Beschleunigungsfaktoren in einem ADN mit Proxy-SG-Appliances von Blue Coat.

Funktionen für eine zentrale Administration und dezentrale Umsetzung zur Verfügung.

Chancen für Carrier: Mehrwert für MPLS

Entscheidet sich ein Unternehmen dafür, die Vorteile eines Application Delivery Networks zu nutzen, hat es zwei Möglichkeiten: Entweder es baut mit den entsprechenden Geräten sein eigenes ADN auf. Oder es setzt auf einen externen Dienstleister, um dort nicht mehr ein reines „Packet Delivery Network“, sondern ein Netzwerk zur sicheren Auslieferung von Anwendungen zu beziehen. Mithilfe entsprechender Produkte können Anbieter ihr bestehendes MPLS-Netz (Multi Protocol Label Switching) zu einem vollwertigen Application Delivery Network erweitern.

Da MPLS bereits die Definition von Service-Klassen gestattet, kann ein MPLS-Netz die Übertragung bestimmter Anwendungen priorisieren. Dies nutzen Serviceprovider, um verschiedenen Service-Klassen unterschiedliche Bandbreite zuzuweisen und so etwa Voice-over-IP oder Video gegenüber E-Mail oder Webverkehr bevorzugt zu behandeln.

Klassische Router sind jedoch nur in der Lage, etwa auf Basis des verwendeten TCP-Ports Datenpaketen eine Class of Service zuzuweisen. Doch je mehr Datenverkehr über HTTP übertragen wird, desto schwieriger ist es für ein MPLS-Netz, zwischen geschäftsrelevanter und privater Nutzung zu unterscheiden.

„Um MPLS die notwendige Transparenz zu verschaffen, verändern einige Appliances das Type-of-Service-Bit im Header eines Datenpaketes, das wiederum vom MPLS-Router zur Festlegung der Class of Service herangezogen wird“, erklärt Walzer. „Da die Appliances dabei nicht nur zwischen Anwendungen, sondern auch zwischen Benutzern unterscheiden, ermöglicht dies eine viel differenziertere Priorisierung von Datenverkehr im WAN, als MPLS dies allein leisten könnte.“

Letztlich bleibt es eine wirtschaftliche Entscheidung, ob ein Unternehmen lieber ein eigenes ADN aufbaut oder einen entsprechenden Mehrwertdienst eines Carriers nutzt. Doch bei den durch eine ADN erzielbaren Beschleunigungswerte (siehe Grafik) rechnet sich der Einsatz eines ADNs für Unternehmen in den allermeisten Fällen. (CK)

Anbieter in Überblick

| Unternehmen | Produkt | Internet |
|---------------------|------------------|---------------------|
| Blue Coat | Packetshaper | www.bluecoat.de |
| Cisco | WAAS | www.cisco.de |
| Citrix | Branch Repeater | www.citrix.de |
| Expand Networks | Accelerator 6950 | www.expand.com |
| F5 Networks | WAN-Jet | www.f5networks.de |
| Ipanema | WAN Governance | www.ipanematech.com |
| Juniper | WXC-Serie | www.juniper.net |
| Radware | Linkproof | www.radware.com |
| Riverbed Technology | Steelhead | www.riverbed.com |