DOSSIER SERVICE GATEWAYS
IN KOOPERATION MIT BOLL ENGINEERING

Ausprobieren statt hadern

jae. Viele Schweizer Unternehmen hadern noch mit der Umstellung auf IPv6. Gerade KMUs fehlt das nötige Know-how und auch die Portion Mut, um sich dem Thema anzunehmen. Dabei ist die Planung und Umsetzung einer Dual-Stack-Implementierung, also eines Parallelbetriebs von IPv4 und IPv6, bei einem KMU ohne weiteres innerhalb einer Woche möglich. Das sagt zumindest Netzwerkspezialist und Firmeninhaber Peter Bruderer von der Bruderer Research GmbH im Interview auf Seite 26.

Bei einer Dual-Stack-Implementierung müssen die verschiedenen Systeme, die entweder auf IPv4 oder IPv6 basieren, miteinander kommunizieren können. Damit dies einwandfrei funktioniert, kommen moderne Unified Application Service Gateways zum Tragen, wie Walter Benz, Product Manager A10 Networks bei Boll Engineering, in seinem Beitrag auf Seite 24 schreibt.

Fest steht: Die IPv4-Adressen sind aufgebraucht. Zwar kann man noch welche beziehen, doch das kostet, und die Provider sind laut Bruderer zurückhaltend mit der Vergabe. Unternehmen werden sich also so oder so mit der Umstellung auf IPv6 auseinandersetzen müssen. Dies nicht zuletzt deshalb, weil die Anzahl (mobiler) Geräte, die aufs Internet zugreifen, stetig zunehmen.

Den Unternehmen, die nicht wissen, wie sie die Umstellung bewerkstelligen sollen, rät Bruderer, sich an ihren Provider zu wenden und sich schrittweise an die Aufgabe heranzutasten. So können sie beispielsweise erste Erfahrungen auf einem Gästenetzwerk sammeln. Denn, wie er treffend sagt: Man kommt nur weiter, wenn man Neues ausprobiert. <

> **Seite 24**
Anwendungen schnell und sicher bereitstellen

> **Seite 26**
Peter Bruderer, Bruderer Research GmbH: «Irgendwann muss sich jedes Unternehmen mit der Umstellung auf IPv6 auseinandersetzen»

Anwendungen schnell und sicher bereitstellen

Die Sicherstellung einer maximalen Verfügbarkeit und Sicherheit unternehmenskritischer Anwendungen ist ein anspruchsvolles Unterfangen. Unified Application Service Gateways (UASGs) leisten dazu einen wichtigen Beitrag für ISPs, Carrier, Grossunternehmen sowie KMUs. Walter Benz

Noch vor wenigen Jahren waren Server Load Balancer (SLB) zur Bereitstellung und Beschleunigung von Applikationen das Mass aller Dinge. Als Schnittstelle zwischen Anwendern und Server-Pool sorgen sie für eine optimierte Lastverteilung zwischen den einzelnen Servern, steigern so die Verfügbarkeit von Anwendungen und minimieren deren Reaktionszeit. Bald schon wurden SLBs mit sogenannten Application Delivery Controllern (ADC) ergänzt. Diese ermöglichen eine intelligente Anwendungsverarbeitung auf Layer 4 bis Layer 7. Sie kommen dann zum Tragen, wenn es gilt, Anwendungen schneller, besser und sicherer bereitzustellen. ADCs haben bei Unternehmen, Cloud-Anbietern und Carriern ihren festen Platz gefunden, sowohl im Datacenter als auch am Netzwerk-Gateway.

Neben ihren Kernfunktionen konsolidieren ADCs diverse zusätzliche Features in einem System. Dazu gehören Datenbank-Load-Balancing ebenso wie die Lastverteilung auf mehrere vorhandene Firewalls. Oft unterstützen ADCs auch ein sogenanntes Application Delivery Partitioning. Dies ermöglicht, unterschiedlichen Benutzergruppen verschiedene Anwendungen und Services auf einer einzigen Plattform mit vollständiger Netz-Separierung zur Verfügung zu stellen. Die Plattform wird somit mandantenfähig.

Sei es als physische oder virtuelle Appliance, Hersteller liefern heute hochleistungsfähige Application Delivery Controller, deren Performance in der Regel durch eine Kombination aus moderner Systemarchitektur, performanter Hardware und optimiertem Betriebssystem ermöglicht wird. Um selbst höchsten Performance-Ansprüchen zu genügen, setzen Hersteller vermehrt hardwarebeschleunigte Plattformen ein. Diese lagern rechenintensive Funktionen an dedizierte FPGAs oder ASICs aus und entlasten so die System-CPU.

Innovative Unified Application Service Gateways (UASG) maximieren die Verfügbarkeit von Applikationen, sorgen für ein hohes Mass an Sicherheit und ermöglichen eine nahtlose IPv6-Migration. Bild: iStock

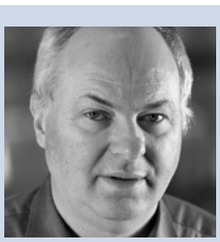
Die Leistungen dieser Anwendungen macht nun einen weiteren Entwicklungsschritt möglich: die Erweiterung von ADCs zu sogenannten Unified Application Service Gateways (UASGs). Diese können, vereinfacht gesagt, als ADC mit markant erweiterten Security- und Networking-Funktionen bezeichnet werden. Ähnlich der Entwicklung im Bereich der IT-Security, bei der sich klassische Firewalls zu hoch integrierten Security-Gateways, sogenannten UTM-Appliances, wandelten, werden klassische ADCs mit einer Vielfalt an Funktionen angereichert. Verfolgt wird dabei das Ziel, wesentliche Security-Funktionen so nahe wie möglich am Perimeter, beziehungsweise am äussersten Punkt des Firmengateways, anzusiedeln. Denn Schadcode, der bereits am Perimeter beziehungsweise vor der Firewall abgewehrt wird, verhindert eine unnötige Belastung und Gefährdung der internen IT- und Netzinfrastruktur. Zu den typischen Security-Features, die UASGs unterstützen, zählen Web und DNS Application Firewall, DDoS-Abwehr und Application-Access-Management beziehungsweise Pre-Authentication. UASGs sind ferner in der Lage, rechenintensive Services wie beispielsweise SSL-Termination auszuführen und somit das interne Netz auch in diesem Bereich zu entlasten. Von zentraler Bedeutung ist ferner die Möglichkeit der nahtlosen Migration von IPv4 auf IPv6.

Security am Firmengateway

Unified Application Service Gateways beinhalten mehrere Security-Funktionen in einem System und ermöglichen somit einen maximalen Perimeterschutz. Zu den wichtigsten Features zählen:

- **Web Application Firewall (WAF) und DNS Application Firewall**

Web Application Firewalls haben zur Aufgabe, Webanwendungen vor Angriffen via HTTP zu schützen, Code-Schwachstellen zu sichern und Datenverluste zu verhindern. UASGs mit WAF-Funktion sind demnach in der Lage, Angriffe auf Webserver zu erkennen und abzuwehren. Dazu untersuchen sie den Datenstrom auf Anwendungsebene und verhindern die Übertragung unerwünschter Daten. DNS Application Firewalls dienen der Absicherung von DNS-



Walter Benz ist Product Manager A10 Networks bei der Boll Engineering AG.

Zu den typischen Security-Features, die UASGs unterstützen, zählen Web und DNS Application Firewall, DDoS-Abwehr und Application-Access-Management beziehungsweise Pre-Authentication. Bild: iStock

Infrastrukturen. Dabei gilt es, selbst massive Attacken ohne Belastung der DNS-Server wirksam abzuwehren. Dadurch ermöglichen DNS Application Firewalls eine Optimierung bestehender Ressourcen beziehungsweise eine Minimierung der Serverkosten.

• Application Access Management (AAM) für Authentifizierung
In einer UASG integrierte Authentifizierungs-Funktionen stellen sicher, dass die Backend-Server keinen unerwünschten oder nicht authentifizierten Datenverkehr erhalten. AAM-Module ermöglichen folglich den Schutz von Rechenzentrumsinfrastrukturen und führen zu einer Effizienzsteigerung von Servern. In der Regel werden die bekanntesten Authentifizierungs- und Speichersysteme wie RADIUS, LDAP, Active Directory und Kerberos ohne weitere Anpassungen an die Webserver oder die Infrastruktur unterstützt.

• Schutz vor mehrschichtigen Distributed-Denial-of-Service-Attacken (DDoS)
Die jüngsten Erfahrungen mehrerer Staaten und Zeitungsverlage zeigen, wie wichtig eine effektive Abwehr von Denial-of-Service-Attacken (DoS) ist. UASGs kombinieren mehrere Technologien zum wirksamen Schutz vor netz- und anwendungsbasierten Angriffen und leisten somit einen entscheidenden Beitrag zur kontinuierlichen Aufrechterhaltung der Dienste. Zu den typischen Abwehrmechanismen gehören SYN-Flood-Protection (SYN-Flood-Angriffe stellen 25 Prozent aller DDoS-Zwischenfälle dar), geografische Filterung, Raten- und Verbindungslimitierung, «Slow HTTP»-Angriffserkennung, aFleX-Kommandos.

Server und Netzwerk ohne Leistungseinbussen

Die Entlastung von Applikationsservern und Netzwerkinfrastrukturen sind weitere Aufgaben, die leistungsfähigen ADCs und UASGs zufallen. Dazu übernehmen die entsprechenden Anwendungen rechenintensive Aufgaben und sorgen mit intelligenten Mechanismen dafür, dass der Datenverkehr reduziert wird. Folgende Funktionen stehen in der Regel zur Verfügung:

• Reduktion der Datenmenge
Mittels Komprimierung des HTTP-Protokolls (HTTP-Komprimierung) lassen sich das Datenvolumen und die benötigte Bandbreite um Faktoren reduzieren. Performancesteigernd wirkt ferner das sogenannte Traffic Caching, bei dem die Anzahl Verbindungen zum Server minimiert wird. Werden zudem mehrere HTTP-Verbindungen zu einer TCP-Sitzung zusammengefasst (TCP-Connection-Reuse), so führt dies zu einer weiteren Entlastung von Server und Netzwerk.

• SSL-Offloading
Die Terminierung verschlüsselter Client-Verbindungen ist – mit den heute angewendeten Schlüssellängen – eine höchst rechenintensive Angelegenheit. Es ist deshalb ratsam, Prozesse zur SSL-Verschlüsselung und -Entschlüsselung nicht dem (Web-)Server zu überlassen, sondern einer vorgelagerten UASG zuzuweisen. Dadurch wird die Leistungsfähigkeit des Servers nachhaltig erhöht und das SSL-Zertifikat effizient ausgeführt. Zu den primären SSL-Offloading-Funktionen zählt die SSL-Terminierung. Diese führt die Entschlüsselungen der Daten durch und sendet diese geschützt an den entsprechenden Server. Unterstützt werden dabei in der Regel alle bekannten TCP-Protokolle.

Mithilfe von SSL-Bridging lassen sich auch verschlüsselte Daten auf fehlerhaften Code überprüfen bevor dieser den Server erreicht. Dazu wird der Code vom Unified Application Service Gateway entschlüsselt, auf Inhaltsebene analysiert, neu verschlüsselt und an den Server weitergereicht. Dieser in beide Richtungen durchlaufende Prozess ist ohne hardwarebeschleunigte UASG kaum denkbar oder hätte markante Leistungseinbussen zur Folge.

• Software Defined Networking (SDN)
Ein noch junger Trend macht von sich reden: Next Generation beziehungsweise Software-defined Networking. Der Wandel von statischen «Gebilden» hin zu dynamischen, skalierbaren, virtuellen und einfach managebaren Netzinfrastrukturen dürfte in naher Zukunft das zentrale (Netzwerk-)Thema sein. Vor diesem Hintergrund ist es nicht erstaunlich, dass innovative Anbieter bereits heute entsprechende Features in ihre UASGs implementieren. Diese verfolgen das Ziel, das Netzwerk auf Basis von Informationen auf Applikationslayer-Ebene zu kontrollieren und auf diesem Weg die Anwendungsperformance zu optimieren.

IPv4/IPv6 – es lebe die Konvergenz

Ein höchst aktuelles Thema, das sich ebenfalls mit Unified Application Service Gateways adressieren lässt, ist die Migration von IPv4 auf IPv6. Die konsequente Einführung von IPv6 ist aufwendig und kostspielig, erfordert hohe Investitionen in IPv6-taugliche Hardware und stellt Unternehmen vor grosse finanzielle und logistische Herausforderungen. Vor diesem Hintergrund setzen Firmen typischerweise auf eine schrittweise Einführung von IPv6, was zur Folge hat, dass beide Protokolle gleichzeitig unterstützt werden müssen. Auf IPv4 und IPv6 basierende Systeme müssen demnach in der Lage sein, nahtlos miteinander zu kommunizieren. Hier kommen moderne UASGs zum Tragen. Als Gateway ermöglichen sie eine nahtlose Kommunikation und Konnektivität zwischen beiden Protokollen und machen mittels Server Load Balancing mit Protocol Translation die eigenen IPv4- und IPv6-basierten Server für alle externen Clients zugänglich – unabhängig davon, ob diese IPv4 oder IPv6 nutzen. Mit NAT64/DNS64 steht zudem eine Lösung für die eigenen IPv6-Clients zur Verfügung, die den Zugang auf IPv4-basierenden Server-Umgebungen sicherstellt. Und im Provider- und Carrier-Umfeld sorgt Carrier Grade NAT (CGN beziehungsweise CGNAT) für eine nahtlose Konvergenz beider Protokolle. <

«Irgendwann muss sich jedes Unternehmen mit der Umstellung auf IPv6 auseinandersetzen»

Netzwerkspezialist Peter Bruderer ist Inhaber und Geschäftsführer der Bruderer Research GmbH in Schaffhausen. Im Interview mit der Netzwoche spricht er über die Umstellung auf IPv6, warum sie primär kleinen Unternehmen Mühe bereitet, und wie man am besten dabei vorgeht. Interview: Janine Aegerter

Herr Bruderer, wie wird man IPv6-Experte, wie Sie einer sind?
(Lacht). Ich habe mich schon mit dem Internet und Firewalls beschäftigt, als alles noch in den Kinderschuhen steckte. 1993 setzte ich mich das erste Mal mit IPv6 auseinander und habe dieses Thema immer weiter verfolgt, auch jetzt, in der Zusammenarbeit mit Boll Engineering.

Wie sieht diese Zusammenarbeit aus?
Ich arbeite mittlerweile seit zehn Jahren mit Boll zusammen. Zuerst war das Unternehmen mein Lieferant. Jetzt gebe ich Firewall-Kurse für Kunden bei Boll Engineering. 2011 stellten wir fest, dass eine grosse Nachfrage nach IPv6-Wissen herrscht. Deshalb begann ich Basiskurse zu diesem Thema zu geben.

Was beinhaltet dieser Basiskurs genau?
Er richtet sich an Vertreter von Unternehmen, die noch nicht viel über IPv6 wissen und sich eine Übersicht über das Thema verschaffen möchten. Es gibt viele Kurse zu IPv6, aber viele davon gehen stark ins Detail oder dauern zwei Tage, was manchen Interessierten zu lang ist.

Wieso sollten sich Unternehmen überhaupt mit IPv6 auseinandersetzen?
Die IPv4-Adressen sind aufgebraucht. Irgendwann muss sich daher jedes Unternehmen mit der Umstellung auf IPv6 auseinandersetzen. Zudem wird das Problem mit der wachsenden Anzahl mobiler Geräte nicht kleiner, im Gegenteil.

Heisst das, dass ich als Unternehmen jetzt keine neuen IPv4-Adressen mehr beziehen kann?
Nein, nicht ganz. Derzeit können wir in Europa zwar noch Adressen beziehen. Heute muss ich aber für IP-Adressen bezahlen und man spürt, dass die Provider zurückhaltend sind mit der Vergabe von IPv4-Adressen. Beziehe ich einen DSL-Aschluss, kosten 32 IPv4-Adressen etwa gleich viel wie der Link selbst. In Asien gehen die Preise bis zu 10 Dollar pro Adresse und Monat.

Netzwerkspezialist Peter Bruderer berät Firmen bei der Umstellung auf IPv6. Bild: Netzmedien

Aber die Schweiz steht doch weltweit mit der Nutzung von IPv6 auf dem ersten Platz?
Ja, das stimmt, wir haben tatsächlich bezüglich IPv6 die prozentual grösste Nutzerzahl weltweit. Aber das sind ja die Enduser, die Dienste von Google, Facebook, und Co. über IPv6 beziehen. Die Firmen selbst sind noch nicht so weit.

Was raten Sie denn Unternehmen, die auf IPv6 umstellen wollen?
Sie müssen sich mit ihrem Provider zusammensetzen, damit er ihnen IPv6 zur Verfügung stellt. Heutzutage ist das mit den meisten Providern kein Problem mehr. Ich muss das Ganze einfach ein wenig planen. Sprich, ich benötige einen Netzwerkplan, muss wissen, wo ich dynamische oder statische Adressen benötige und in welchen Bereichen ich sie benötige. Wenn ich nicht allzu viele alte Hardware habe, muss ich meine Netzwerkinfrastruktur auch nicht komplett ersetzen. Kommt hinzu, dass Unternehmen, wenn sie jetzt damit anfangen, die Umstellung auf IPv6 ohne Zeitdruck durchziehen können.

Wie lange dauert diese Umstellung in etwa?
Eine komplette Umstellung auf eine reine IPv6-Umgebung ist heute eine Illusion. Man richtet deshalb IPv6 parallel zu IPv4 ein, eine sogenannte Dual-Stack-Implementierung. Planung und Umsetzung ist bei einem kleinen bis mittleren Unternehmen ohne weiteres innerhalb einer Woche möglich.

Das klingt sehr einfach. Wieso gibt es denn nicht mehr Firmen, die sich IPv6 auf die Fahne schreiben?
Das grösste Problem für kleine Firmen ist das fehlende Know-how. Sie kämpfen zum Teil schon mit IPv4, und wenn sie jetzt noch IPv6 machen müssen, ist das für sie zu viel. Für den Betrieb von IPv6 in kleinen Firmen reicht aber ein Basiswissen absolut aus.

Wie überzeugen Sie die Leute, sich trotzdem damit auseinanderzusetzen?
Ich bin mit ein paar grossen Unternehmen im Gespräch und versuche sie zu ermuntern, im Kleinen anzufangen und beispielsweise einmal den Mailserver oder das Gästenetzwerk auf IPv6 umzustellen und so erste Erfahrungen zu sammeln. Grundsätzlich sind Firmen, die Angst vor dieser Umstellung haben, auch sonst eher zurückhaltend. Aber man kommt nur weiter, wenn man Neues ausprobiert. Theoretisch gesehen brauche ich zum Überleben ja nur eine Höhle und ein Feuer. Meine Agenda auf Papier zu haben ist auch absolut ausreichend. Aber wenn wir alle so dächten, würden wir uns heute noch mit Pferden fortbewegen und hätten keine Autos.

Wie sieht es im Vergleich zur Schweiz im Ausland mit der Entwicklung von IPv6 aus?
Innerhalb Europas kämpfen alle Provider mit der Tatsache, dass die IPv4-Adressen knapp werden. Deshalb forcieren alle Internet Service Provider die Benutzung von IPv6. In Deutschland wird IPv6 sogar vom Staat gefördert. Die USA sind hingegen sehr zurückhaltend. Sie horten mehr als die Hälfte aller IPv4-Adressen. <