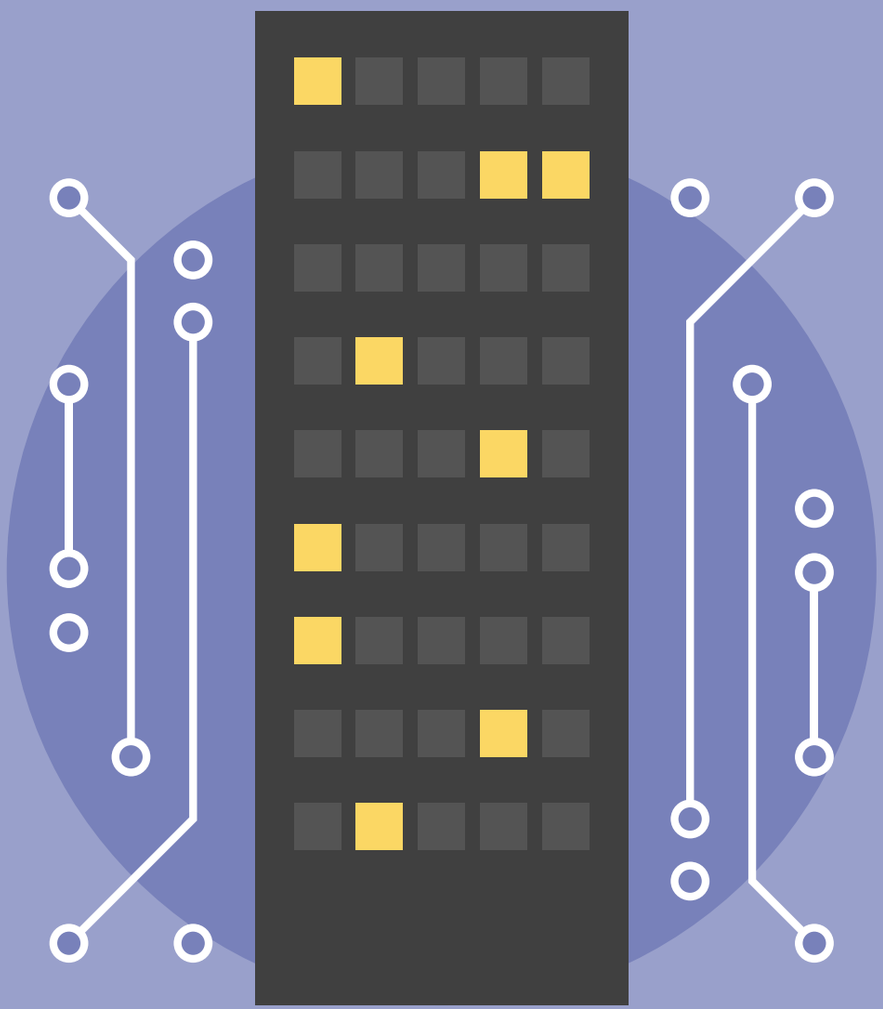


Dossier
Application Delivery Controller

In Kooperation mit **Boll Engineering**

Grosse Datenmengen sicher managen

«Application Delivery Controller» (ADC) sorgen dafür, dass Applikationen und Services sicher bereitgestellt werden können. Bei wachsenden Datenmengen im Cloud Computing und bei der Bewältigung von Big-Data-Anwendungen unterstützen sie die Server Load Balancer, welche die Last allein nicht ausreichend managen können.

ADCs entlasten Applikationsserver und Netzwerkinfrastrukturen, indem sie rechenintensive Aufgaben übernehmen und die Lasten zwischen den einzelnen Servern intelligent verteilen. Besonders bei der Ver- und Entschlüsselung von SSL-geschütztem Datenverkehr, der Migration auf IPv6 oder dem parallelen Betrieb mit IPv4 und Software-Defined Networking entfalten sie ihre volle Wirkung.

Zudem stellen ADCs zahlreiche Sicherheits-Features bereit. Sie helfen zum Beispiel bei DDoS-Angriffen, die Dienste aufrechtzuerhalten, und schützen die DNS-Server vor Überlastungen.

Hohe Verfügbarkeit im Application-Networking

Ob KMU oder Enterprise, ob ISP oder Datacenter: «Server Load Balancer» (SLB) und «Application Delivery Controller» (ADC) sorgen für eine hohe Verfügbarkeit und Sicherheit unternehmenskritischer Anwendungen – und haben einiges mehr zu bieten.

DER AUTOR

Walter Benz, Product Manager für A10 Networks, Boll Engineering

Die schnelle und sichere Bereitstellung von Anwendungen und Ressourcen stellt Firmen und Serviceprovider vor grosse Herausforderungen. Die verstärkte Nutzung mobiler Endgeräte, die ungebrochene Zunahme virtualisierter Umgebungen, der rasante Aufbau von Cloud-Infrastrukturen und Themen wie Big Data, SOA und Web 2.0 haben das Potenzial zur Beeinträchtigung von Qualität, Verfügbarkeit und Sicherheit von Anwendungen. Um eine hohe Verfügbarkeit unternehmenskritischer Applikationen zu gewährleisten, empfiehlt sich der Einsatz intelligenter «Server Load Balancer». Diese agieren als Schnittstelle zwischen Anwendern und Server-Pool, sorgen für eine optimierte Lastverteilung zwischen den einzelnen Servern und steigern dadurch die Verfügbarkeit von Anwendungen bei gleichzeitiger Minimierung der Reaktionszeit.

Doch reine Server Load Balancer reichen nicht aus, um ein performantes und sicheres «Delivery» von Applikationen und Services zu garantieren. Erforderlich sind vielmehr erweiterbare Systeme, die ausgewählte Zusatzfunktionen in einer Plattform beinhalten. Diese mit «Application Delivery Controller» (ADC) bezeichneten Systeme ermöglichen eine intelligente Anwendungsverarbeitung auf Layer-4- bis Layer-7-Ebene und zeichnen sich durch erweiterte Security- und Networking-Funktionen aus. Sie sind bei Unternehmen, Cloud-Anbietern und Carriern gleichermassen bedeutsam – sowohl im (virtualisierten) Datacenter als auch am Perimeter.

Ausser der Kernaufgabe «Load Balancing» verfolgen ADCs das Ziel, wesentliche Security-Funktionen so nahe wie möglich am Firmengateway anzusiedeln. Denn Schadcode, der bereits am Perimeter beziehungsweise im «Nord-Süd-Verkehr» abgewehrt wird, verhindert eine unnötige Belastung und Gefährdung der internen IT- und Netzwerkinfrastruktur. Gleiches gilt für den sogenannten «Ost-West-Verkehr» in (virtualisierten) Datacentern beziehungsweise in Cloud-Infrastrukturen. Durch die tiefe Integration der ADC in die Datacenter-Infrastruktur wird nicht nur eine hochflexible Zuteilung der Ressourcen, sondern auch eine direkte Überwachung von Anwendungen und Daten erreicht.

Zu den typischen Security-Features, die ADCs unterstützen, zählen Web und DNS Application Firewall, DDoS-Abwehr und Application-Access-Management beziehungsweise Pre-Authentication. ADCs sind zudem in der Lage, rechenintensive Services wie beispielsweise SSL-Termination auszuführen und somit das interne Netzwerk zu entlasten. Von zentraler Bedeutung ist ferner die Möglichkeit der nahtlosen Migration von IPv4 auf IPv6.

Integrierte Security

Application Delivery Controller beinhalten mehrere komplementäre Sicherheitsfunktionen in einem System. Sie sind folglich in der Lage, Security-Appliances wie Firewalls oder Systeme zur Abwehr von DDoS-Attacken individuell zu ergänzen. Von Bedeutung ist, dass die Verteilung der Aufgaben flexibel und zentral «orchestriert» erfolgen kann. Zu den wichtigsten ADC-Security-Features zählen:

Schutz vor mehrschichtigen Distributed-Denial-of-Service-(DDoS)-Attacken

Zahlreiche bekanntgewordene Attacken zeigen, wie wichtig eine effektive Abwehr von Distributed-Denial-of-Service-(DDoS-)Attacken ist. ADCs 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, geografische Filterung, Raten- und Verbindungslimitierung, «Slow HTTP»-Angriffserkennung und aFleX-Kommandos.

DNS Application Firewall

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

Deep Packet Inspection (DPS)

DPS ermöglicht die Überwachung und Filterung von Datenpaketen, um Malware, Protokollverletzungen, Spam und unerwünschte Inhalte zu erkennen und abzuwehren. Im Gegensatz zur klassischen «Stateful Packet Inspection», die lediglich den Header der einzelnen Datenpakete überprüft, verschafft DPS einen tiefen Einblick in die Datenströme – selbst dann, wenn die Datenkommunikation verschlüsselt erfolgt (siehe dazu die Erläuterungen zu SSL-Offloading beziehungsweise SSL-Terminierung).

Application Access Management (AAM) für Authentifizierung

Integrierte Authentifizierungsfunktionen 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 bekann-

testen Authentifizierungs- und Speichersysteme wie RADIUS, LDAP, Active Directory und Kerberos ohne weitere Anpassungen an die Web-Server oder die Infrastruktur unterstützt.

Web Application Firewall (WAF)
Web Application Firewalls haben zur Aufgabe, Webanwendungen vor Angriffen via HTTP zu schützen, Code-Schwachstellen zu sichern und Datenverluste zu verhindern. ADCs 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.

Leistungsoptimierung für Server und Netzwerk

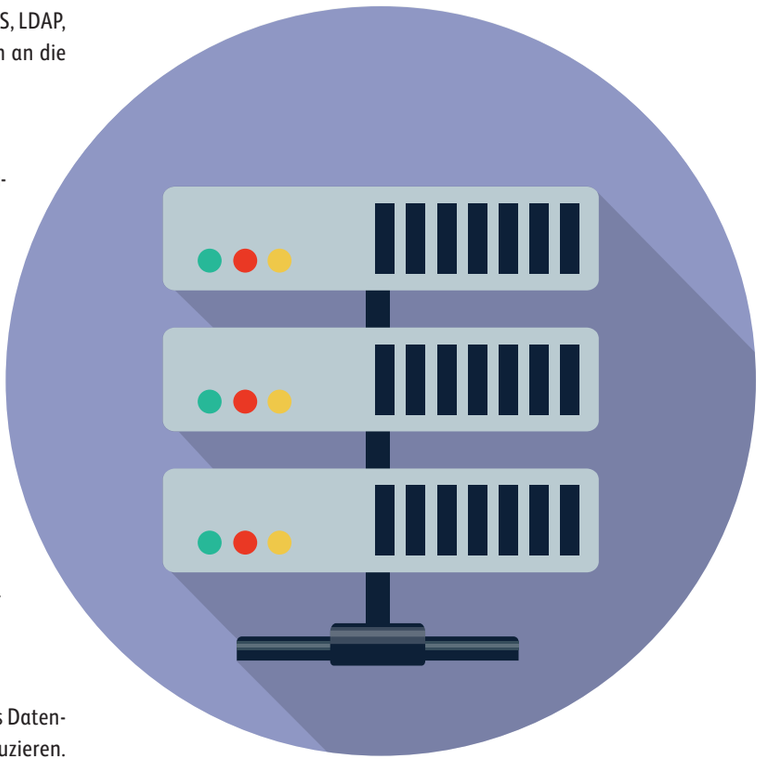
Die Entlastung von Applikationsservern und Netzwerkinfrastrukturen sind weitere zentrale Aufgaben, die leistungsfähigen ADCs zufallen. Dazu übernehmen sie rechenintensive Aufgaben und sorgen mit intelligenten Mechanismen dafür, dass der Datenverkehr reduziert wird. Folgende Funktionen stehen in der Regel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

Reduktion der Datenmenge
Mittels Komprimierung des HTTP-Protokolls 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), führt dies zu einer weiteren Entlastung von Server und Netzwerk.

SSL-Offloading
Die Terminierung verschlüsselter Client-Verbindungen ist, namentlich 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 ADC mit Hardwarebeschleunigung. 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 zudem verschlüsselte Daten auf schadhaften Code überprüfen – bevor dieser den Server erreicht. Dazu wird der Code von der ADC entschlüsselt, auf Inhaltsebene analysiert, neu verschlüsselt und an den Server weitergereicht. Dieser in beide Richtungen durchlaufende Prozess ist ohne Hardwarebeschleunigung kaum denkbar oder hätte markante Leistungseinbussen zur Folge.

IPv4/IPv6-Migration oder Koexistenz
Ein aktuelles Thema, das führende ADCs ebenfalls adressieren, ist die Migration von IPv4 auf IPv6 sowie die Koexistenz beider Protokolle. Als Gateway ermöglichen sie eine nahtlose Kommunikation und Konnektivität zwischen IPv4 und IPv6 und machen mittels



SLB-PT (Server Load Balancing with 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-basierten Serverumgebungen sicherstellt.

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 wie A10 Networks bereits heute entsprechende Features in ihre ADCs implementieren. Diese verfolgen das Ziel, das Netzwerk auf Basis von Informationen auf Applikationslayer-Ebene zu kontrollieren und auf diesem Weg die Anwendungsperformance zu optimieren.

Übergreifende Plattformen

Um die beschriebenen Leistungsmerkmale und Security-Funktionen ganzheitlich zu adressieren, werden an ADC-Hersteller und deren Produkte hohe Anforderungen gestellt. So müssen die Systeme unter anderem in der Lage sein, alle denkbaren Formen der Einbindung zu unterstützen. Sie sollten sich sowohl für den Einsatz am Perimeter eignen als auch die Bedürfnisse von virtualisierten Datacentern und Cloud-Lösungsanbietern adressieren. Zudem müssen sie ein zentrales, übergreifendes Management unterstützen.

«ADCs maximieren die Verfügbarkeit von Daten und Applikationen»

Fritz Steinmann, Head Network & Security Engineering bei SIX, erklärt im Interview, weshalb Server Load Balancer (SLB) beziehungsweise Application Delivery Controller (ADC) für SIX unabdingbar sind. Interview: Marc Landis

Die Anforderungen an die Verfügbarkeit Ihrer IT dürften hoch sein …

Fritz Steinmann: Tagtäglich laufen Millionen von Finanztransaktionen über die Infrastruktur von SIX: Wertpapiere werden gehandelt, verrechnet und abgewickelt, bargeldlose Zahlungen ermöglicht und verarbeitet. Zudem werden Informationen zu Finanzinstrumenten weltweit erfasst, aufbereitet und verteilt. Keine Frage: Verfügbarkeit und Performance der IT sind zentral.

Was wären mögliche Konsequenzen bei einem Systemausfall?

Ein Ausfall der Validierungs- und Clearing-Systeme beispielsweise hätte zur Folge, dass Bargeldbezüge am Bankomaten, der Einkauf von Lebensmitteln und anderen Gütern im Detailhandel oder Onlineshopping nicht mehr möglich wären. Es ist mitunter unsere Aufgabe, derartige Szenarien zu verhindern und einen jederzeit performanten Betrieb zu gewährleisten – auch in Spitzenzeiten.

Wie sorgen Sie dafür?

Wir setzen generell auf den Einsatz hochleistungsfähiger Systeme sowie auf die konsequente Umsetzung weitreichender Security-Policies. Zudem betreiben wir zwei redundant aufgebaute, geografisch getrennte Rechenzentren. Eine wichtige Rolle spielen zudem sogenannte Server Load Balancer beziehungsweise Application Delivery Controller.

Was ist deren Aufgabe?

SLBs und ADCs verteilen die Last dynamisch an die jeweils geeignetsten und verfügbaren Server und sorgen dafür, dass auch beim Ausfall einzelner Systeme oder eines kompletten Rechenzentrums der gesamte Betrieb ohne Performance-Einbussen weitergeführt werden kann.

Sie haben kürzlich neue ADCs evaluiert. Warum?

Die bisher eingesetzten Load Balancer von Cisco – die haben sich übrigens gut bewährt – wurden abgekündigt. Zudem benötigen wir erweiterte Funktionen wie beispielsweise Global Load Balancing. Vor diesem Hintergrund machten wir uns an die Evaluation einer neuen ADC-Lösung, die sowohl unsere aktuellen Bedürfnisse als auch zukünftig benötigte Leistungsmerkmale unterstützt.

Wie sind Sie dabei vorgegangen?

Klassisch. Den Evaluationsprozess – bestehend aus Anforderungsanalyse, detailliertem Konzeptbeschrieb und Systemevaluation – trieben wir zügig voran. Und im Herbst 2014 führten wir im Rahmen eines Proof-of-Concepts (PoC) eine praxisbezogene Ausmarchung durch. In der Folge entschieden wir uns für die Application Delivery Controller von A10 Networks.

Fritz Steinmann, Head Network & Security Engineering, SIX

Welche technischen Anforderungen standen im Vordergrund?

Neben den Standard-SLB- und ADC-Funktionen legten wir Wert auf Funktionen wie Source NAT oder Global-Server-Load-Balancing. Zweitgenannte ermöglicht uns, zum gegebenen Zeitpunkt auch unsere Datacenter im Ausland einzubinden. Zudem waren uns die Unterstützung der Protokolle IPv4 und IPv6 wichtig. Sicherheitsrelevante Funktionen wie Web Application Firewall setzen wir im Moment nicht ein, trotzdem sind wir so bestens für die Zukunft gerüstet. Besonders erwähnen möchte ich das Cisco-ähnliche Command Line Interface und Web-GUI. Diese uns vertraute Umgebung macht das Handling der neuen ADCs sehr einfach.

Gab es ausser den technischen Aspekten weitere Entscheidungskriterien?

Natürlich. Hersteller- und partnerspezifische Faktoren beeinflussten den Entscheidungsprozess stark. Faktoren wie Grösse und Marktanteil spielten dabei eine untergeordnete Rolle. Viel wichtiger waren uns Aspekte wie Engagement, Know-how und Erfahrung – sowohl seitens des Herstellers als auch des lokalen Partners.

Über SIX

SIX betreibt die schweizerische Finanzplatzinfrastruktur und bietet weltweit umfassende Dienstleistungen in den Bereichen Wertschriftenhandel und -abwicklung sowie Finanzinformationen und Zahlungsverkehr an. Das Unternehmen befindet sich im Besitz seiner Nutzer (rund 140 Banken verschiedenster Ausrichtung und Grösse) und erwirtschaftete 2014 mit über 3800 Mitarbeitern und Präsenz in 24 Ländern einen Betriebsertrag von 1,8 Milliarden Franken und ein Konzernergebnis von 247,2 Millionen Franken.
www.six-group.com