Seminararbeit

Verteilte und parallele Systeme

Thema: Web Switching

Autoren: Birkner, Marcel
Morick, Sebastian

Datum: Dez. 2004
Ort: Sankt Augustin

1 Inhaltsverzeichnis

2 Einleitung

Webseiten werden schon lange nicht mehr nur auf einem Webserver abgespeichert. Stark frequentierter Web-Inhalt wird zunehmend auf mehreren Webservern gespeichert, die sogar weltweit verteilt sein können. Diese Server bilden eine Gruppe, die mit nur einer IP-Adresse erreichbar sein muss und als verteilter Webserver angesehen werden kann. Die technische Umsetzung dieser Thematik wird als **Web-Switching** bezeichnet. Diese Seminararbeit wird einen Einblick in die verschiedenen Arten und Prinzipien des Web-Switchings geben. Eine Betrachtung der Abwehr von Angriffsversuchen auf einen Webserver sowie eine Marktübersicht der Web-Switches runden die Arbeit ab.

3 Motivation

Die Definition eines Web-Switches ist sicher noch nicht jedem sehr geläufig. Hier [Sie] wird dieses folgendermaßen definiert: „Web-Switches, auch Layer-7-Switches oder Content-Switches genannt, haben die Aufgabe, Web-Anfragen ohne große Verzögerungen bedienen zu können und den Datenverkehr mittels eines optimalen Lastausgleichs an die entsprechenden Server zu leiten. Die Web-Switches untersuchen die TCP/IP-Daten und werten die URL-Informationen und Cookies aus, um daraufhin ein optimales Load-Balancing vorzunehmen. Sie verteilen den Datenverkehr in Abhängigkeit von den übertragenen Inhalten und erkennen anhand eines Datenpakets, ob es sich um einfaches Web-Surfen, eine zeitkritische SAP-Transaktion oder um eine Online-Bestellung handelt. Web-Switches unterstützen mehrere Load-Balancing-Verfahren“.

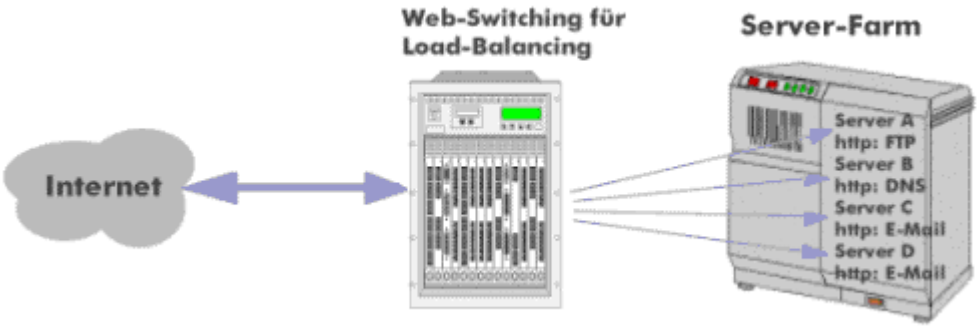


Abbildung 1: [Sie] Load-Balancing über einen Web-Switch

Eine genauere Betrachtung des Themas Web-Switching ist die Intention dieser Seminararbeit.

4 Grundlagen des Web-Switching

Das Web-Switching richtet sich vor allem an Web-Inhalte, die stark frequentiert sind. Die Verteilung dieser Web-Inhalte auf verschiedene Server bezeichnet man als Web-Switching. Hierbei ist das lokale- und globale Web-Switching zu unterscheiden. Von lokalen Web-Switching spricht man, wenn eine Gruppe von Webserver an einem Standort in einem Cluster organisiert ist. Ziel dabei ist es eine optimale Verteilung der Anfragen aus dem Internet an die verschiedenen Server zu erreichen, um Web-Inhalte performant wiederzugeben. Deshalb spricht man auch von Server Load Balancing (SLB).
Von globalen Web-Switching wird im Kontext einer weltweiten Verteilung der Webserver gesprochen. Ziel dieser Variante ist es ebenfalls die Lastverteilung auf die Webserver zu steuern, aber auch eine minimale Antwortzeit der Webserver zum Benutzer zu erreichen. Dieses kann durch die globale Verteilung der Webserver umgesetzt werden. Die zweite Art des Web-Switching wird auch als Global Server Load Balancing (GSLB) bezeichnet.
Da die URL einer Webseite nur über einen eindeutigen Namen angesprochen werden kann, entstehen bei einer weltweiten Verteilung der Webserver Probleme, die es mit den Mitteln des Web-Switching zu lösen gilt.

4.1 Clusterbasiertes Web-Switching

Wenn mehrere Web Server an einem Standort installiert sind, können diese zu einem Cluster zusammengefasst werden. Es wird in diesem Fall ein Web-Switch zur Seite des Internets dem Cluster vorgelagert, um den Cluster nach außen hin als nur ein System erkennbar zu machen. (vgl. Abb. 2) Dieser kann dann natürlich auch mit einer einzigen IP-Adresse angesprochen werden. Der Web-Switch hat die Aufgabe die ankommenden Anfragen aus dem Internet an die Webserver innerhalb des Clusters zu verteilen. Die einzelnen Webserver des Clusters müssen von dem Web-Switch angesprochen werden können, und benötigen so eine eigene IP-Adresse. Da es sich hierbei um eine IP-Adresse handelt, die nicht im Internet sichtbar gemacht wird, kann man eine individuelle IP für die Adressierung benutzten. Bei der IP des Web-Switches selbst spricht man auch von einer virtuellen IP-Adresse (VIP). Anhand dieser VIP wird der Web-Switch die Anfragen aus dem Internet an die Webserver innerhalb des Clusters weiterleiten, und dient somit als Vertretung der Webserver-Gruppe nach außen hin. Die VIP wird also auch genutzt, um die Webservernamen innerhalb des Clusters per DNS auflösen zu können. Die Funktionsweise der Namensauflösung per DNS ist nicht Teil dieser Seminararbeit.
Damit der Web-Switch eine Anfrage an einen Webserver auch richtig weiterleiten kann, muss dieser den HTTP-Request eines Web-Clients interpretieren. Um dieses zu leisten gibt es zwei verschiedene Ansätze.

- Der TCP-Header wird ausgewertet. D.h. die Schicht 4 (Layer 4) wird ausgewertet.
- Der TCP-Header und die Angaben des HTTP Protokolls werden ausgewertet. D.h. die Schicht 4 und 7 (Layer 4 and 7) werden ausgewertet.

Bei der ersten Variante nennt man den Web-Switch auch Layer-4 Switch oder kurz L4-Switch. Bei der zweiten Variante wird der Web-Switch dann analog Layer-7 Switch oder kurz L7-Switch genannt.
Ein Layer-4 Switch leitet eine Webanfrage aufgrund der Port-Nummer 80 im TCP-Header weiter. Diese Art von Web-Switches kennt den geforderten Web-Inhalt einer Anfrage nicht. HTTP-Requests werden an einzelne Web-Server also ohne Kenntnis des Inhalts weitergeleitet und werden deshalb auch als Content-Blind oder contentunabhängiges Web-Switching bezeichnet.
Der L7-Switch wertet nicht nur die Zieladresse der HTTP-Anfrage aus (Layer-4) sondern auch den Inhalt (Layer-7). Bei dieser Technik nennt man den Web-Switch auch Content-Aware-Switch oder die Art des Web-Switching wird als contentabhängiges Web-Switching bezeichnet.

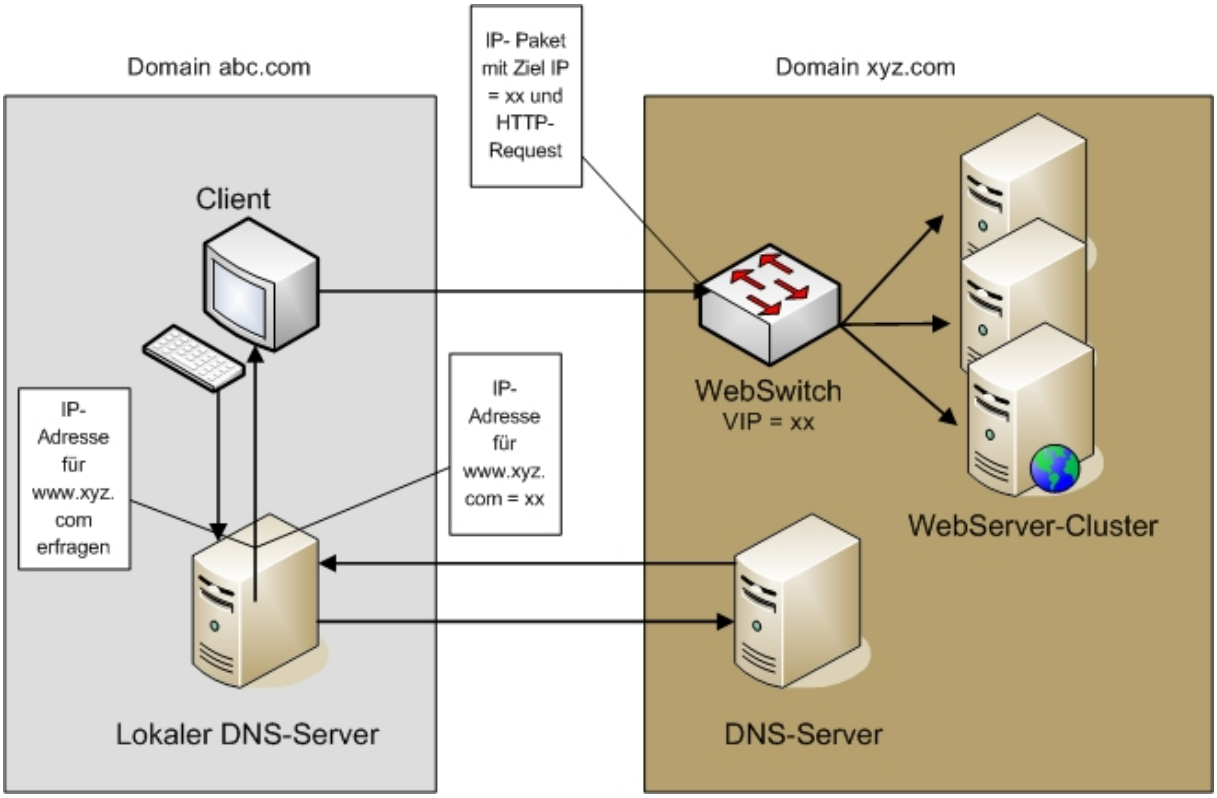


Abbildung 2: Beispiel für ein clusterbasiertes Web-Switching-System

4.2 Verteiltes Web-Switching

Im Gegensatz zum clusterbasierten Web-Switching befinden sich beim verteilten Web-Switching die Webserver einer Internet-Domain nicht an einem Standort sondern sind räumlich verteilt. (vgl. Abb. 3) Dieses kann innerhalb eines Gebäudes wie auch weltweit sein. Da die Webserver alle den gleichen Web-Kontext zur Verfügung stellen, aber nur über eine URL angesprochen werden sollen, entstehen hier gewisse Probleme mit der Adressierung der verteilten Webserver. Die Webserver sind in einer weltweit verteilten Struktur alle in verschiedenen lokalen Netzwerken mit verschiedenen Subnetzen installiert. Somit hat auch jeder Webserver eine andere IP-Adresse. Um dieses Problem lösen zu können, werden einige Ansätze des clusterbasierten Web-Switching übernommen.
Ein globaler Web-Switch nimmt alle Anfragen an die verteilten Webserver entgegen und leitet diese an den jeweils „günstigsten“ Webserver weiter. Unter günstig versteht man in diesem Kontext die Übermittlungszeit und die Belastung eines Webservers, der den Web-Inhalt zum Web-Client (Nachfrager) schicken soll. Es ist also vom Web-Switch die Lokation des Webservers auf der Erdkugel zu berücksichtigen, aber auch z.B. die Sprache in der der Web-Inhalt angefordert wird. Um dieses leisten zu können muss man hier einen L7-Switch einsetzen, da dieser über Content-Kenntnisse der Anfrage aus dem Internet verfügt. Beim globalen Web-Switching spricht man in diesem Zusammenhang von Content-Aware-Routing oder Request-Routing.

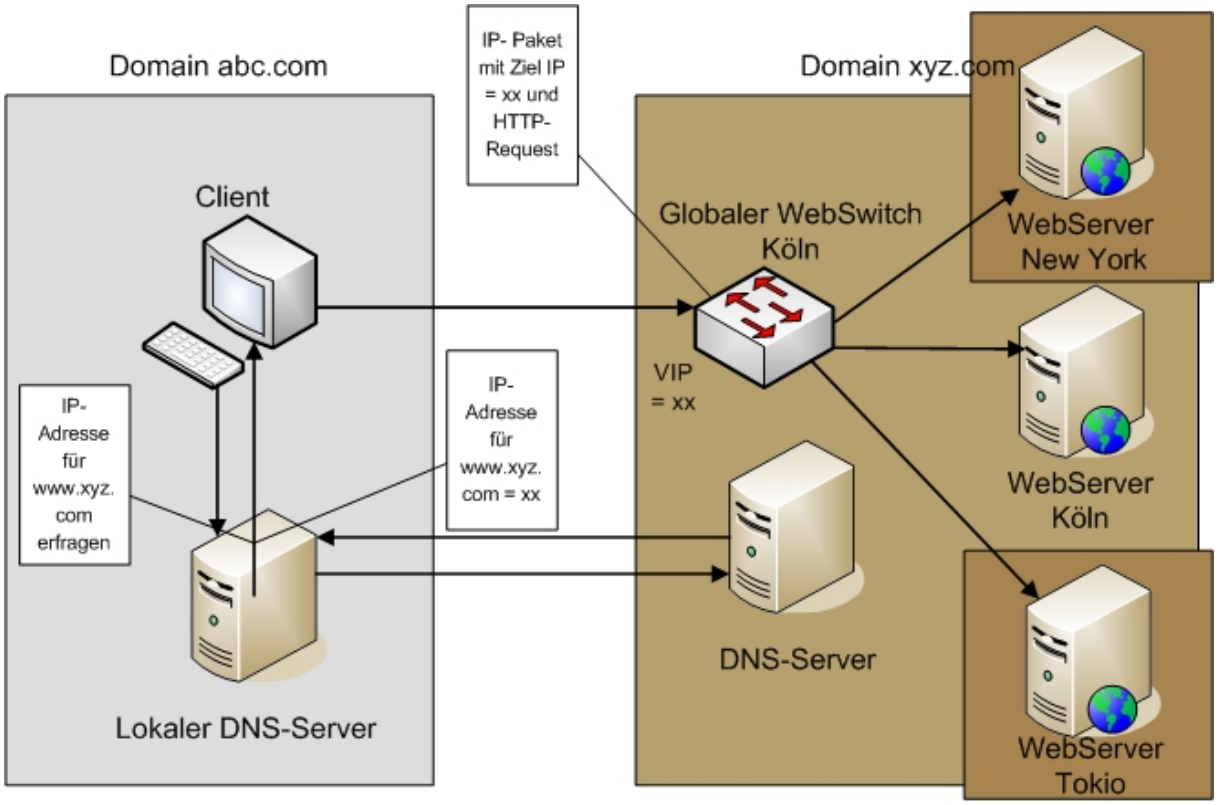


Abbildung 3: Beispiel eines verteilten Web-Switching-System

4.3 Ziele des Web-Switching

Das Web-Switching bringt eine Menge von Vorteilen für den Betreiber. Durch den Einsatz von clusterbasierten Webservern steigt durch die physikalischen Präsents mehrerer Webserver an einem Ort die Verfügbarkeit des Web-Contents. Wartungsarbeiten können flexibler gestaltet werden. Dynamische Inhalte auf Webservern sind dabei eher problematisch als statischer Content, da die Webserver sich untereinander abgleichen müssen. Ein weiter Pluspunkt für die Benutzung eines Web-Switches ist die schnellere Antwortzeit auf eine Anfrage. Dieses resultiert aus dem Gebrauch des oben erwähnten Server Load Balancing, das die Webserver gleichmäßig belasten soll. Der Einsatz von spezialisierten Webservern kann ebenfalls durch den Einsatz von Content-Aware-Web-Switches ermöglicht werden. Da der Web-Switch den Inhalt der Anfrage kennt, können z.B. rechenintensive Anfragen auf andere Webserver geroutet werden als statische Web-Anfragen.
Als weitere Vorteile der Web-Switching Technologie sind noch die Bildung von Benutzerklassen für benutzerabhängige Web-Anfragen und den Einsatz von verschiedenen Software- und Hardwareplattformen auf den Webservern zu nennen.

4.4 Struktur clusterbasierter Web-Systeme

Die Umsetzung des clusterbasierten Web-Switching kann generell in vier verschiedenen Strukturen passieren:

1. eine Domain und ein Webserver (klassischer Fall)
2. eine Domain und mehrere Webserver (SLB Lösung)
3. mehrere Domains und ein Webserver (virtueller Webserver)
4. mehrere Domains und mehrere Webserver (Lastverteilung bei virtuellen Webservern)

Im ersten und dritten Fall wird kein Webswitching benötigt, da die HTTP-Anfragen nur an einen Webserver direkt gestellt werden. Der zweite Fall ist ein typischer Server Load Balancing (SLB) Fall, da mehrere Server zu einer Domain gehören und in der Regel den gleichen Web-Content haben. Es wird eine Lastverteilung und Erhöhung der Verfügbarkeit der Webserver erreicht.
Im dritten und vierten Fall befindet sich der Web-Switch gleichzeitig in mehren Domänen und benötigt eine VIP um die Anfragen an den bzw. die Webserver weitergeben zu können. Hier können nur Layer-7 Web-Switches zum Einsatz kommen, da der Web-Switch die Port-Nummer im TCP-Header auswerten und den Datenstrom an einen virtuellen Webserver weiterschicken muss. Variante vier ist ein Lösungsansatz wie Variante drei, nur mit einer redundanten Auslegung von virtuellen Webservern.

5 Web-Switching mit Layer 4 Switches

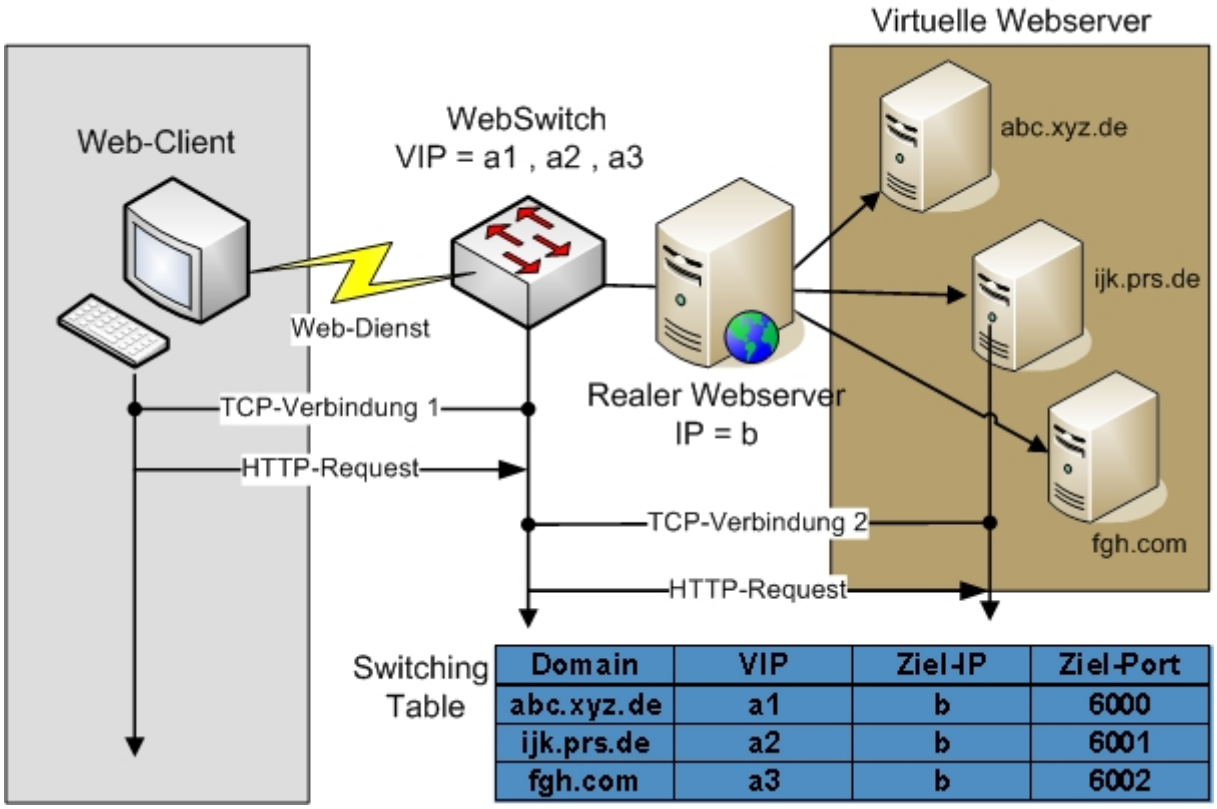
Das Web Protokoll HTTP nutzt das verbindungsorientierte Protokoll TCP um eine Verbindung zwischen Client und Webserver aufbauen zu können. Im Header des TCP Protokolls wird der Zielport (80) mitgeschickt. Hierdurch kann ein Zielsystem erkennen, dass es sich um ein eingebettetes HTTP- Protokoll handelt. Andere Dienste des Internets wie z.B. FTP, SMTP etc. nutzen verschiedene Standardports. Diese Ports sind für einen L4-Switch ebenfalls von Bedeutung.
Der Verbindungsaufbau bei einer Webserver Anfrage läuft folgendermaßen ab: Ein Web-Client initiiert zuerst den Aufbau einer TCP Verbindung. Hierzu sendet er ein IP-Paket an die VIP des Web-Switches und dem TCP-Segment <SYN>. Im Header steht der Zielport 80, anhand dessen der Web-Switch die Anfrage an einen der Webserver des Clusters weiterleitet. Die TCP-Verbindung wird nach dem Three-Way-Handshake Verfahren aufgebaut, auf die hier nicht weiter eingegangen wird. Der L4-Switch kann also keine Angaben des HTTP-Protokolls auswerten, was ihn wie oben erwähnt als Content-Blind bezeichnen lässt.
Für einige E-Commerce-Anwendungen ist es nötig, dass der Web-Switch eine aufgebaute Verbindung zu einem bestimmten Webserver unbedingt beibehält, und nicht einen anderen Webserver adressiert. Dabei handelt es sich meistens um Web-Transaktionen, die vollständig abgeschlossen sein müssen. Um dieses zu erreichen führt der Web-Switch eine interne Switching-Tabelle die auch Binding Table genannt wird. Hier trägt der Web-Switch die jeweiligen Quell- und Zieladressen mit Portnummer ein. Der L4-Web-Switch verhält sich hierbei wie ein transparentes Zwischensystem zwischen Client und Webserver.
Die bisherige Betrachtungsweise reduzierte sich bis jetzt hauptsächlich auf die Kommunikation zwischen Client und Web-Switch. Die Übermittlung der IP-Pakete vom L4-Switch zum Webserver selbst ist im Allgemeinen von der Art der Anbindung des Webservers an den Web-Switch abhängig. Ein Ansatz ist die Umsetzung von IP-Adressen. Hierbei tauscht der Web-Switch die Ziel-IP-Adresse (seine VIP) des ankommenden Paketes mit der des Webservers aus. Die Quell-IP-Adresse des Rück-Paketes wird dann analog mit der VIP überschrieben. Um eine nach der Spezifikation gemäße TCP/IP Verbindung zu garantieren, muss der Web-Switch bei diesem Verfahren auch die Prüfsummen der jeweiligen Pakete neu berechnen. Dieses Vorgehen ermöglicht es die Webserver und den Web-Switch in unterschiedlichen IP-Subnetzen zu installieren, da sie durch die IP-Umsetzung nicht direkt physikalisch verbunden sein müssen.
Ein weiteres Verfahren ist die Umsetzung auf MAC-Adressen Basis. Hierbei müssen die Webserver und der Web-Switch zwingend zu einem Subnetz gehören. Einem Webserver werden dabei zwei IP-Adressen zugewiesen. Eine Adresse für Management- und Konfigurationszwecke und eine zweite Adresse, die mit der VIP des Web-Switches identisch ist. Der L4-Switch wertet nun die MAC-Frames in denen seine IP-Adresse eingebettet ist aus und generiert einen neuen MAC-Frame mit der MAC-Adresse des

Webservers. Mit Hilfe des ARP-Protokolls wird das ankommende IP-Paket so als MAC-Frame zum Webserver weitergeleitet. Dieser Ansatz ist in der Literatur auch als MAC Address Translation bekannt.
Die letzte und dritte Variante des Anschließens eines Web-Switches an einen Webserver ist das IP-Tunneling. Hierbei wird das ankommende IP-Paket in ein weiteres IP-Paket eingebettet. Der Webserver wird so konfiguriert, dass er nur das „innere“ IP-Paket auswertet. Diese Technik macht es auch möglich ein Webserver-Cluster über ein VPN weltweit zu verteilen.

6 Web-Switching mit Layer 7 Switches

Das Content Aware Switching mit einem L7-Web-Switch läuft in den unteren Schichten des OSI-7-Schichten Modells im Wesentlichen wie beim L4-Web-Switching ab. Die TCP-Verbindungen werden im Three-Way-Handshake Verfahren aufgebaut. Anders ist das der L7-Web-Switch nun in der Anfrage eines Web-Clients den HTTP-Request auswerten kann. Der L7-Web-Switch wählt nach der Client-Anfrage einen Webserver aus und baut eine weitere TCP Verbindung zu diesem auf. Der HTTP-Request wird nun auf dieser zweiten TCP-Verbindung zum Webserver geschickt. Der L7-Web-Switch hat also im Ganzen die Aufgabe die zwei TCP-Verbindungen zwischen Web-Client und –Server für den Benutzer transparent zusammenzuführen. Diese Technik wird auch als TCP-Splicing bezeichnet.

Eine Form des Content Aware Switching ist das URL-Switching. Hierbei werden nur die URL Angaben aus den HTTP-Requests vom L7-Web-Switch ausgewertet. Anhand dieser Informationen kann der Web-Switch einen Webserver auswählen, der den passenden Content gespeichert hat. Webserver können so mit unterschiedlichen Inhalten eingerichtet werden. Dieses ermöglicht eine Spezialisierung der Webserver auf bestimmte Funktionen, die gerade bei E-Commerce Sinn machen.
Ein weitergehender Ansatz ist der Multi-Domain-Web-Server. Da jede URL einen Domainnamen beinhaltet, ist es möglich auf einem physikalischen Webserver mehrere virtuelle Webserver laufen zu lassen. (vgl. Abb. 4) Hierbei werden in dem physikalischen Webserver Bereiche so konfiguriert, dass sie als virtuelle Webserver interpretiert werden können. Der Web-Switch bekommt als VIP nicht nur eine IP zugewiesen, sondern mehrere VIPs. Wenn der Web-Switch einen HTTP-Request von einem Web-Client bekommt mit z.B. VIP = a3 und Domain-Name = fgh.com in der URL, dann setzt der Web-Switch nach der internen Switching-Tabelle die IP-Adresse auf den realen Webserver z.B. = b und den Zielport auf den Port, mit dem der virtuelle Webserver angesprochen werden kann. In diesem Beispiel wäre das Port 6002. Es wird eine zweite TCP-Verbindung zum virtuellen Webserver aufgebaut, und mit der ersten TCP-Verbindung des Web-Clients gespleißt. Die Kommunikation läuft wie oben erwähnt transparent über den Web-Switch.



Domain	VIP	Ziel-IP	Ziel-Port
abc.xyz.de	a1	b	6000
ijk.prs.de	a2	b	6001
fgh.com	a3	b	6002

Abbildung 4: Virtuelle Webserver mit Hilfe von URL-Switching

7 Server Auswahl bei lokalem Web-Switching

Die Auslastung eines Webservers soll möglichst gleichmäßig passieren. Hierzu wird das schon erwähnt Server Load Balancing eingesetzt. Es gibt eine Reihe von Verfahren, mit denen die Webserver die Anfragen vom Web-Switch weitergeleitet bekommen.

Im Round-Robin-Verfahren (RR-Verfahren) werden die Anfragen der Reihe um an die Webserver geschickt. Hierbei ist das ungewichtete- und gewichtete Round-Robin Verfahren zu unterscheiden. Beim ungewichteten RR-Verfahren wird die aktuelle Belastung und Reaktionszeit der Webserver nicht beachtet. Dieses eignet sich z.B. bei Webservern der gleichen Leistungsklasse. Das gewichtete RR-Verfahren wiederum kann unterschiedlich leistungsstarke Webserver verschiedene Menge von Anfragen je nach Auslastung zusenden. Ein weiteres Server Load Balancing Verfahren basiert auf der Anzahl der TCP-Verbindungen zu den Webservern. Im Least-Connection Verfahren wird ähnlich dem RR-Verfahren durch ein ungewichtetes- oder gewichtetes Verfahren die Auslastung der Webserver entweder unbewertet oder bewertet. Der Einsatz dieser Verfahren orientiert sich ebenfalls an der Leistungsklasse der Webserver. Ein letztes Verfahren ist das Response Time Verfahren. Hier wird die Reaktionszeit der Webserver geschätzt, und so aktuelle Web-Anfragen an den Webserver mit der schnellsten Antwortzeit übergeben. Ein weit verbreiterter Algorithmus ist der Arrowpoint Content Awareness Algorithm von Cisco Systems [Cis].

8 Web-Switching mittels DNS

Eine relativ einfache Form des Web-Switching kann mittels DNS realisiert werden. (vgl. Abb. 5) Der Vorteil hierbei ist, dass kein extra Web-Switch angeschafft werden muss, sondern der DNS-Server das Web-Switching anhand der URL übernimmt. Jedem Webserver wird im DNS-Server eine eindeutige IP-Adresse zugeordnet. Startet der Web-Client eine Anfrage an eine Web-Ressource, dann fragt dieser nach der IP-Adresse des Webservers beim DNS-Server nach. Der DNS-Server kann nun verschiedene IP-Adressen der Webserver zurückliefern, um eine Lastverteilung auf Webserver mit den gleichen Inhalten zu realisieren. Bei diesem Verfahren gibt es zwei Möglichkeiten mit der der DNS-Server die IP-Adressen auswählen kann. Einmal im Round-Robin Verfahren also reihum oder zufällig im Random Verfahren. In der Abbildung 5 wird das Round-Robin Verfahren verdeutlicht. Der Client macht eine Anfrage an den DNS-Server der Domain xyz.de. Der DNS-Server antwortet auf diese erste Anfrage mit der IP-Adresse des Webserver1. Bei der zweiten Anfrage des Clients antwortet der DNS-Server jedoch mit der IP-Adresse des nächsten Webservers also Webserver2. Wie aus der Abbildung 5 ersichtlich wird nicht nur eine einzelne IP-Adresse vom DNS-Server zum Client geschickt, sondern eine Liste der möglichen IP-Adressen der Webserver. Dieses ermöglicht dem Client bei Ausfall eines Webservers automatisch einen anderen Webserver zu adressieren.
In dem RFC 1794, das hier [Faq] zu finden ist, wird das Verfahren für die Lastverteilung mittels DNS beschrieben.

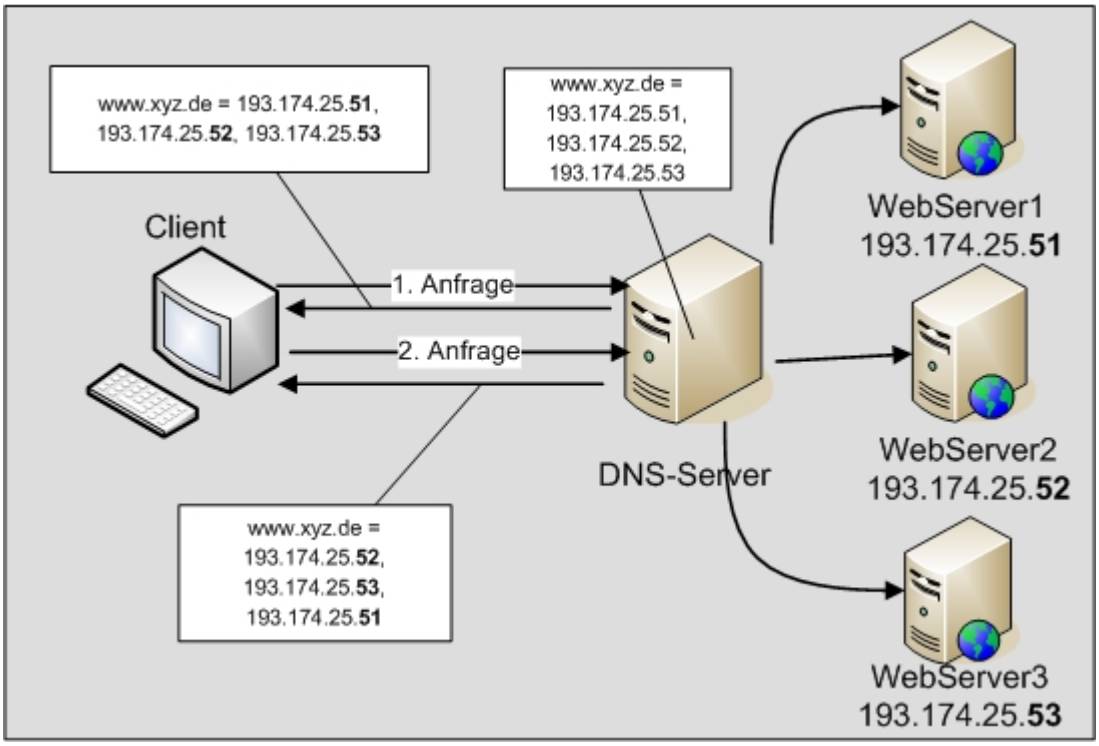


Abbildung 5: Lastverteilung mit DNS-Hilfe

9 Web-Switching und Transaktionen

Um eine Transaktion im Web durchführen zu können müssen Web-Switche folgende Punkte leisten:

- Auswahl des richtigen Webservers
- Herstellung der Transaktion
- Aufrechterhaltung der Verbindung innerhalb der Transaktion zu einem bestimmten Webserver
- Identifizierung der jeweiligen Transaktion

Für die Identifizierung von webbasierten Transaktionen werden in der Regel Cookies vergeben. Dabei kann sowohl der Web-Switch wie auch der Webserver diese vergeben. Eine TCP-Verbindung zwischen Client und Webserver setzt sich wieder aus zwei einzelnen TCP-Teilverbindungen zusammen. Nachdem Empfangen der ersten Response auf eine Web-Anfrage des Clients vom Webserver, wird ein Cookie, das der Webserver mitliefert, vom Web-Switch an die beiden Enden der TCP-Verbindung „geklebt“. Dieses wird auch als Cookie Sticky genannt. Danach sendet der der Web-Switch die Response an den Client weiter. Anhand dieser Technik kann der Web-Switch nun die TCP Zuordnungen zwischen Switch und Server sowie Client und Switch speichern. Kommt ein HTTP-Request vom Client oder ein HTTP-Response vom Server erkennt der Web-Switch anhand des Cookies, das mitgeschickt wird, um welche TCP-Verbindung es sich handelt. Die gesamte Kommunikation läuft also wieder auf einer gespleißten TCP-Verbindung nur diesmal mit einem Cookie ab. Der Nachteil beim Einsatz von Cookies ist, dass der Benutzer sie im Browser deaktivieren kann. Dieses bedeutet dass mehrere Transaktionen zwischen Web-Client und Webserver nicht realisierbar sind. Bei Erlauben des Anlegens von Cookies ist jedoch auch der Missbrauch des E-Commerce Anbieters nicht auszuschließen, da die Transaktionen des Benutzers auf diese Cookies abgebildet werden.

10 Web-Switching mit unidirektionalem Datenverkehr

Die bisher dargestellten Web-Switching Systeme benutzen einen bidirektionalen Datenverkehr zwischen Web-Client und Webserver. Dabei kann es bei Web-Anforderungen mit hoher Übertragungsbandbreite, wie z.B. Videos, schnell zu einem Engpass am Web-Switch kommen. Eine Lösung dieses Problems ist der Einsatz eines Web-Switching Systems mit unidirektionalem Datenverkehr. (vgl. Abb. 6) Bei diesem Ansatz nimmt der Web-Switch die Web-Anfragen entgegen und verteilt diese auf die Webserver wie gehabt. Die Webserver antworten nun jedoch nicht über den Web-Switch, sondern schicken den HTTP-Response direkt über einen leistungsfähigen Multi-Layer-Switch direkt an den Web-Client zurück. Der Datenverkehr im Web-Switch verläuft somit nur in eine Richtung und entlastet diesen. Das Verfahren wird auch als Switch-Back-Verfahren bezeichnet. Die technische Realisierung nennt man analog dazu TCP Handoff. Dabei überträgt der Web-Switch den Endpunkt und den Zustand der vom Web-Client an ihn aufgebauten TCP-Verbindung an den ausgewählten Webserver. Diese Nachbildung des Sockets auf dem Webserver wird auch als Klonen des Sockets (TCP-Verbindung) bezeichnet.
Das Web-Switching mit unidirektionalem Datenverkehr ist eine neue Generation des Web-Switchings.

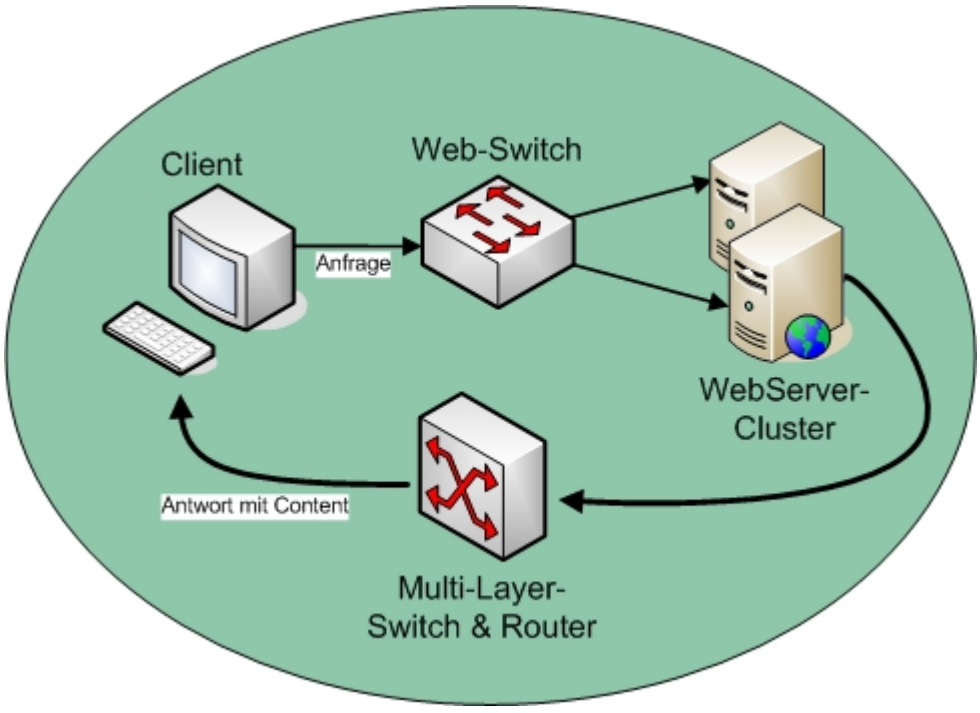


Abbildung 6: Web-Switching mit Unidirektionalem Datenverkehr

11 Angriffsversuche abwehren

Die Redaktion tecCHANNEL [Tec] untersuchte die Abwehrmöglichkeiten gegen eine Denial-of-Service Attacke anhand des Einsatzes von Web-Switches. Für viele E-Commerce Anbieter ist es von bedeutender Wichtigkeit, das ihre Webserver im Internet jederzeit erreichbar sind. Denial-of-Service Attacken versuchen genau dieses zu unterbinden, und können bei erfolgreichen Einsatz den Unternehmer in den Ruin treiben. Es gibt fünf Schlüsselfaktoren weshalb die Attacken aus dem Internet nur schwer abzuwehren sind:

1. fehlerhafte Software
2. allgemeine Standards
3. Anonymität der Internet-Nutzer
4. Schwächen von Internet-Protokollen
5. Missbrauch von Unbeteiligten zum Angriff

Fehlerhafte Software ist ein Hauptgrund der erfolgreichen Attacken aus dem Internet. Viele Programme und Betriebsysteme werden erst nach der Veröffentlichung durch die Hersteller mit Sicherheitsupdates gegen Angriffe resistent gemacht. Wegen der geringen Anzahl von verschiedenen Betriebsystemen und Protokollen im Internet lassen sich von Hackern gefundene Sicherheitslücken schnell auf vielen Systemen anwenden. Die Zurückverfolgung dieser Angriffe ist aufgrund von IP-Adressänderungen (IP-Spoofing) selten erfolgreich. Das Internet baut auf eine verbindungslose Übertragungsstruktur auf. Das TCP/IP-Protokoll benötigt jedoch eine verlässliche Punkt-zu-Punkt Verbindung für den Aufbau einer Kommunikation. Dieses passiert über einen Synchronisierungsprozess zwischen Sender und Empfänger. Der Sender sendet dem Empfänger einen Synchronization Request und wartet darauf, dass der Empfänger reagiert. In dieser Phase findet sich die TCP Kommunikation in einem „embryonalen“ Zustand, da es zwar eine Verbindung zwischen Sender und Empfänger gibt, aber beide Seite noch warten, ob eine Sitzung zustande kommt. Dieser Zustand lässt sich zum lahm legen des Webservers missbrauchen, indem man in kürzester Zeit viele solche „embryonale“ Sitzungen startet. Ein weiter Grund warum sich Attacken gegen Webserver nur schlecht verhindern lassen, ist der Missbrauch von unbeteiligten Dritten an den Angriffsversuchen. Da immer mehr Rechner permanent online im Internet sind, lassen sich diese Rechner nach einer erfolgreichen Kompromittierung gleichzeitig gegen einen Webserver richten.

Eine Möglichkeit die Angriffe gegen einen Webserver abzuwehren ist die „Härtung“ des TCP/IP-Stacks. Das bedeutet dass man alle unnötigen Services und Daemons deaktivieren, Patches und Updates einspielen und den eingehenden Datenverkehr filtern sollte. Dieses lässt sich auf eine Firewall oder einen Web-Switch auslagern. Ein Web-Switch ist z.B. in der Lage die eingehenden Pakete nach unzulässigen Adressen und Integrität zu überprüfen. Diese Switche können außerdem tausende von TCP-Verbindungen aufbauen und stoßen nicht so schnell an ihre Kapazitätsgrenzen wie ein einzelner Webserver. Weiter lassen sich mit Web-Switches auch die Eigenschaften der TCP-Kommunikation so umkonfigurieren, dass eine „embryonale“ Verbindung schon nach wenigen Sekunden für „tot“ erklärt wird. Dieses verhindert das minutenlange warten auf den Aufbau einer Verbindung und somit der unnötigen Belastung des Webservers. In der Praxis hat sich gezeigt, dass Internet-Nutzer nicht länger als 5-8 Sek. auf den Aufbau einer Webseite warten wollen.
Große Attacken auf Webserver lassen sich mit einer gut ausgebauten Hardware des Webservers sicher auch abwehren. Da dieses aber sehr teuer ist, kann man sich besser mit dem oben erklärten Global Web-Switching gegen solche Attacken schützen. Durch den Einsatz eines DNS basierten Web-Switching wird die Angriffslast auf mehrere Webserver mit dem gleichen Dienst gleichmäßig verteilt.

12 Marktübersicht

Eine Übersicht der Web-Switches im Markt hat das von der AWi - Aktuelles Wissen Verlagsgesellschaft mbH herausgegebene Online Magazin LanLine [Lan] zusammengestellt. Nortel Networks ist in diesem Segment Marktführer (Stand Nov. 2000). Es werden Web-Switche von fast allen großen Netzwerk-Komponenten Herstellern wie Cisco, 3com und Extreme Networks angeboten. Ausschlaggebend bei der Auswahl eines Web-Switches sind der Datendurchsatz und die Anzahl der Sessions die der Switch ermöglichen kann. Der Datendurchsatz liegt hier bei 50 Mbit/s bei einfachen Switches und geht bis 256.000 Mbit/s bei Hochleistungs-switches. Die Anzahl der simultanen TCP-Sessions liegt bei günstigen Web-Switches bei 5000 und bei teuren Web-Switches bis zu 16 Millionen.

Marktübersicht: Web-Switches

Hersteller	Produktname	Netzwerkschnittstellen: 10Base-TX	100Base-TX	1000Base-T	1000Base-LX	1000Base-SX	1000Base-FX	Zahl der LAN-Schnittstellen (max. Ausbaustufe)	Sessions/Durchsatz: max. simultane TCP-Session	max. simultane HTTP-Session	max. TCP-Flow-Setups/Sekunde	max. HTTP-Flow-Setups/Sekunde	max. Durchsatz (Pakete/Sekunde)	max. Durchsatz (MBit/Sekunde)
3Com	Superstack 3 Server Load Balancer	●	●	●	●	●		14	128.000				2.000.000	2200
Cisco Systems	Catalyst 6000/6500 mit Content Switching Modul	●	●		●	●		576	1.000.000	1.000.000	200.000	80.000	15.000.000	256.000
	CSS 11050 Content Service Switch	●	●			●		9	64.000	64.000		19.500	5.359.680	5000
	CSS 11150 Content Service Switch	●	●			●		16	112.000	112.000		19.500	9.528.320	5000
	CSS 11800 Content Service Switch	●	●			●		64	1.000.000	1.000.000		130.000	11.904.000	20.000
Clickarray Networks	Array 500	●	●					2	5000	1000	1000			50
	Array 500 i	●	●					2	20.000	2000	2000			50
	Array1000 SX					●		2	250.000	20.000	20.000			500
	Array 1000 SXi					●		2	1.000.000	20.000	20.000			500
	Array1000 TX	●	●	●				2	250.000	20.000	20.000			500
	Array 1000 TXi	●	●	●				2	1.000.000	20.000	20.000			500
Extreme Networks	Summit Px1		●	●	●	●		1	2.000.000	524.000	235.000	120.000	2.880.000	2000
F5 Networks	Big-IP 5000 Application Switch	●	●			●		28	1.000.000	1.000.000		25.000		1500
Foundry Networks	Server Iron 400	●	●	●	●	●	●	72	16.000.000	16.000.000	600.000	160.000	48.000.000	24.000
	Server Iron 800	●	●	●	●	●	●	168	16.000.000	16.000.000	600.000	160.000	84.000.000	56.000
	Server Iron XL	●	●	●	●	●	●	26	1.000.000	1.000.000	80.000	20.000	3.000.000	2000
	Server Iron XL/G				●	●	●	8	1.000.000	1.000.000	80.000	20.000	12.000.000	8000
Nortel Networks/ Alteon	ACEdirector 3	●	●			●		9	336.000	336.000	296.000			8000
	ACEdirector 4	●	●			●		10	512.000	512.000	296.000			8000
	ACEswitch 180E	●	●			●		9	336.000	336.000	296.000			8000
	ACEswitch 184	●	●			●		9	512.000	512.000	296.000			8000
	Passwort 8600 mit Web Switch Module	●	●	●	●	●		340	4.000.000	4.000.000	2.400.000			128.000
Radware	Web Server Director +Application Switch II	●	●			●		21	unbegrenzt	unbegrenzt	38.000	38.000	300.000	4000
	WSD-Pro 8FE	●	●					8	unbegrenzt	unbegrenzt		5600	200.000	950
	WSD-Pro 2GE					●		2	unbegrenzt	unbegrenzt		5600	200.000	950
	WSD-Pro 8FE+2GE	●	●			●		10	unbegrenzt	unbegrenzt		5600	200.000	950

Hersteller	Produktname	Sicherheitsfunktionen: Abwehr von Denial of Service	Firewall	Radius	SSH	URL-Filtering	Auswahl des lokalen Servers: URL	Cookie	Datei-Typ	Host-Tag	Direct Server Return	Inbound NAT	MAC Address Translation	Outbound NAT	Multi-Site Auswahlverfahren: DNS-Redirection	HTTP-Redirection	Triangulation
3Com	Superstack 3 Server Load Balancer	●										●		●	●	●	
Cisco Systems	Catalyst 6000/6500 mit Content Switching Modul	●	●	●	●	●	●	●	●		●	●		●			
	CSS 11050 Content Service Switch	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	CSS 11150 Content Service Switch	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	CSS 11800 Content Service Switch	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Clickarray Networks	Array 500	●	●		●	●	●	●		●	●	●		●	●	●	
	Array 500 i	●	●		●	●	●	●		●	●	●		●	●	●	
	Array1000 SX	●	●		●	●	●	●		●	●	●		●	●	●	
	Array 1000 SXi	●	●		●	●	●	●		●	●	●		●			
	Array1000 TX	●	●		●	●	●	●		●	●	●		●	●	●	
	Array 1000 TXi	●	●		●	●	●	●		●	●	●		●	●	●	
Extreme Networks	Summit Px1	●			●	●	●	●	●	●		●			●	●	
F5 Networks	Big-IP 5000 Application Switch	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	
Foundry Networks	Server Iron 400	●		●	●		●	●	●		●	●	●	●	●	●	●
	Server Iron 800	●		●	●		●	●	●		●	●	●	●	●	●	●
	Server Iron XL	●		●	●		●	●	●		●	●	●	●	●	●	●
	Server Iron XL/G	●		●	●		●	●	●		●	●	●	●	●	●	●
Nortel Networks/ Alteon	ACEdirector 3	●		●	●	●	●	●	●	●	●	●	●	●	●	●	
	ACEdirector 4	●		●	●	●	●	●	●	●	●	●	●	●	●	●	
	ACEswitch 180E	●		●	●	●	●	●	●	●	●	●	●	●	●	●	
	ACEswitch 184	●		●	●	●	●	●	●	●	●	●	●	●	●	●	
	Passwort 8600 mit Web Switch Module	●		●	●	●	●	●	●	●	●	●	●	●	●	●	
Radware	Web Server Director +Application Switch II	●			●	●	●	●	●	●	●			●	●	●	●
	WSD-Pro 8FE	●					●	●	●		●	●		●	●	●	●
	WSD-Pro 2GE	●					●	●	●		●	●		●	●	●	●
	WSD-Pro 8FE+2GE	●					●	●	●		●	●		●	●	●	●

Hersteller	Produktname	Load Balancing Algorithmen: Least Connections	Predictive	Antwortzeit	Round Robin	Server-Auslastung	Weighted Distribution	Weighted Round Robin	Protokollunterstützung: TCP	UDP	HTTP	FTP	DNS	POP3	SMTP	IMAP4	NNTP	LDAP	Telnet	TFTP	SHTTP	SSL	SNMP	ICMP
3Com	Superstack 3 Server Load Balancer	●		●	●	●	●	●	●		●	●			●				●	●		●	●	●
Cisco Systems	Catalyst 6000/6500 mit Content Switching Modul	●			●	●	●	●	●	●	●	●	●		●				●	●		●	●	●
	CSS 11050 Content Service Switch	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	CSS 11150 Content Service Switch	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	CSS 11800 Content Service Switch	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Clickarray Networks	Array 500	●		●	●		●	●	●	●	●		●									●	●	
	Array 500 i	●		●	●		●	●	●	●	●		●									●	●	
	Array1000 SX	●		●	●		●	●	●	●	●		●									●	●	
	Array 1000 SXi	●		●	●		●	●	●	●	●		●									●	●	
	Array1000 TX	●		●	●		●	●	●	●	●		●									●	●	
	Array 1000 TXi	●		●	●		●	●	●	●	●		●									●	●	
Extreme Networks	Summit Px1	●			●		●	●	●	●	●	●		●	●	●	●	●	●	●	●	●	●	●
F5 Networks	Big-IP 5000 Application Switch	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Foundry Networks	Server Iron 400	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	Server Iron 800	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	Server Iron XL	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	Server Iron XL/G	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Nortel Networks/ Alteon	ACEdirector 3	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	ACEdirector 4	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	ACEswitch 180E	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	ACEswitch 184	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	Passwort 8600 mit Web Switch Module	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Radware	Web Server Director +Application Switch II	●			●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	WSD-Pro 8FE	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	WSD-Pro 2GE	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	WSD-Pro 8FE+2GE	●		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Abbildung 7: Marktübersicht Web-Switches (Stand Nov. 2000)

13 Zusammenfassung

Web-Switche gibt es grundlegend in zwei verschiedenen Ausführungen. Einmal als Layer-4 sowie als Layer-7 Web-Switch. Die Unterschiede liegen in der Auswertung der Schichten des OSI-7-Schichten Modells durch den Web-Switch. Man kann mehrere Webserver entweder in einem Cluster zentral anordnen oder global verteilen. Ein Web-Switch übernimmt die Lastverteilung auf diese Webserver durch Verfahren wie IP-Translation, MAC Address Translation und IP-Tunneling bei L4- und URL-Switching bei L7-Web-Switches. Die Webserver werden von den Web-Switches im Round-Robin-Verfahren oder im Least-Connection-Verfahren angesprochen. Eine Alternative des Web-Switching ohne Web-Switch bietet das DNS-basierte Web-Switching, bei dem die Webserver durch den lokalen DNS-Server adressiert werden. Als Cookie Sticky wird das Spleißen von zwei TCP-Verbindungen mittels eines Cookies genannt, das man im E-Commerce zur Speicherung von Benutzer-Transaktionen benötigt. Für ein hohes Datenvolumen im Rückkanal der Kommunikation zwischen Webserver und Web-Client werden häufig Web-Switching-Architekturen mit einem unidirektionalen Datenverkehr bevorzugt. Dieses wird anhand eines hochperformen Switches über den die Antworten der HTTP-Anfragen laufen realisiert. Web-Switche können die Verfügbarkeit der Webserver durch die Lastverteilung auf verschiedene Server erhöhen, um so Denial-of-Service Angriffe aus dem Internet abzuschwächen. Die handelsüblichen Web-Switche gehen in Sachen Datendurchsatz und TCP-Verbindungshandling weit auseinander.

14 Literaturverzeichnis

[Cis] Cisco Systems. http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_tech_note09186a0080093de5.shtml
Configuring ACA on the CSS 11000 and 11500.

[Faq] Internet RFC/STD/FYI/BCP Archives. http://www.faqs.org/rfcs/rfc1794.html
RFC 1794 - DNS Support for Load Balancing.

[Lan] Lanline, Magazin für Netze-, Daten- und Telekommunikation. http://www.lanline.de/O/148/Y/82690/default.aspx. Online-Marktübersichten. Grasbrunn, 12/2001.

[Sie] Siemens AG. http://www.networks.siemens.de/solutionprovider/_online_lexikon/
Das Siemens Online Lexikon.

[Tec] IDG Interactive GmbH, Redaktion tecCHANNEL, Bernd Reder. http://www.tecchannel.de/netzwerk/networkworld/technologyupdate/586/
Schadensbegrenzung durch Web-Switching, München, 2000.

[Web] Badach/Rieger/Schmauch. Web-Technologien - Architekturen, Konzepte, Trends. 1. Auflage. Hanser Verlag, München, 2003.