Citrix NetScaler

Erste Schritte, Integrationsgrundlagen

Februar, 2012

Dieses Whitepaper beschreibt die Grundlagen zur Integration, unterschiedliche Integrationsvarianten und einige der grundlegenden Funktionen von Citrix NetScaler. Anschließend wird anhand von Beispielen gezeigt, wann der Einsatz welcher Funktionen und welches Vorgehen sinnvoll sind.

Inhalt

NetScaler Grundbegriffe

Citrix NetScaler wird als Application Delivery Controller(ADC) Web-, Application- oder Datenbank-Servern vorgeschaltet und stellt neben einem effektivem Load Balancing und Content-Switching weitere Funktionen auf einer einzigen, umfassenden Plattform bereit: Datenkomprimierung, Caching von Inhalten, SSL-Beschleunigung, Netzwerkoptimierung, Anwendungstransparenz und Anwendungssicherheit. Er stellt in Form von Virtual Servern (VServern) die Gegenstellen bereit, zu denen sich Clients verbinden. Diese Verbindungen werden durch NetScaler in Richtung der Backend Server und Services intelligent verteilt und zudem wahlweise abgesichert, optimiert, inspiziert, authentisiert und modifiziert.

Wichtige Grundbegriffe sind hier:

- **VServer**: Kontaktpunkte, zu denen sich Clients verbinden. Damit assoziiert sind meist „öffentliche“ IP-Adressen, die die Clients ansprechen (VIPs, siehe IP-Adressen von NetScalers).
- **Server**: Ein Backend System, repräsentiert durch eine IP-Adresse. Möglicherweise in einem isolierten Server-Netz.
- **Service**: Ein Dienst auf einem Server, repräsentiert durch einen Port und ein Protokoll und verbunden mit einem Server-Objekt.
- **Monitor**: Prüft periodisch die Funktion des Backend-Services und reicht von einer einfachen Ping-Prüfung bis hin zu komplexen, applikationsnahen und bei Bedarf individuell angepassten Anfragen, die an den Service gestellt werden, um eine definierte Antwort zu erhalten. Je Service-Objekt können ein oder mehrere Monitore zur Überwachung bestimmt werden.

Load Balancing

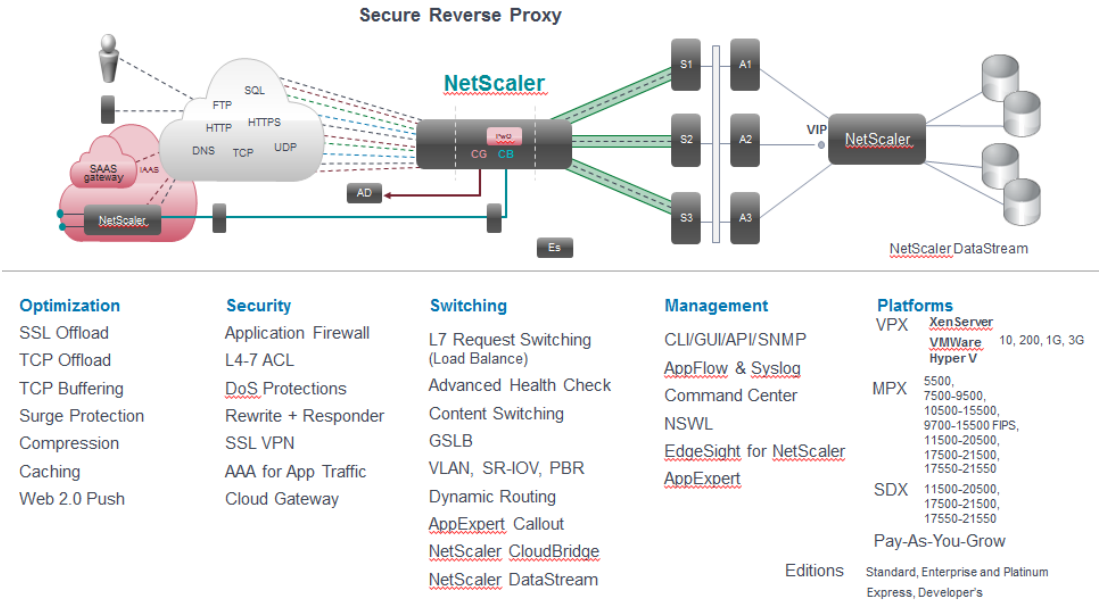
Ein Load Balancing Virtueller Server (LB-VServer) nimmt Anfragen von Clients entgegen und verteilt diese auf Services. Beim Anlegen eines VServers werden zunächst die Services bestimmt, die über diesen VServer angesprochen werden sollen, und im Anschluss um zwei wesentliche Parameter ergänzt:

- **Load Balancing Methode**: Die Methode, nach der je Anfrage (Request) entschieden wird, zu welchem Service diese weitergeleitet werden soll. Beispiele sind Round Robin (reihum je Service eine Anfrage), Least Connection (eine neue Anfrage wird zu dem Service gesendet, zu dem aktuell die wenigsten Verbindungen bestehen) und auch Least Response Time (Anfrage geht zu dem Service, der vorherige Anfragen am schnellsten beantwortet hat).
- **Persistence Methode**: Für viele Services ist es wichtig, dass jede Anfrage (jedes Paket) eines Clients zum gleichen Service geleitet wird. Zu diesem Zweck lässt sich eine „Persistence“ (manchmal auch Stickiness genannt) konfigurieren, die anhand unterschiedlicher Parameter für das gewünschte Ergebnis sorgen kann. Beispiele sind IP-Hash (die erste Anfrage von einer IP-Adresse wird anhand der konfigurierten Load Balancing Methode einem Service zugeordnet, alle weiteren Anfragen von dieser IP landen weiterhin bei diesem Service, solange er verfügbar ist) und Cookie Insert (nur für HTTP; NetScaler fügt in die Server-Antwort ein Cookie ein, anhand dessen er die folgenden Requests des Clients erkennt und wieder zum selben Service leitet).

Weitere wesentliche Funktionen

Der Funktionsumfang von NetScaler inklusive und jenseits der in diesem Dokument beschriebenen Netzwerk-nahen Funktionen gliedert sich in drei Kategorien: **Verfügbarkeit, Performance, Sicherheit.**

Eine Liste der Funktionen mit kurzen Erläuterungen findet sich unter http://blogs.citrix.com/2011/02/08/netscaler-funktionen-kurzfassung und ist in der folgenden Abbildung dargestellt:



[Abbildung: Citrix NetScaler - wesentliche Funktionen]

Vorgehen zur Installation

Für die Installationsvorbereitungen und ein NetScaler Deployment sollten in einem Dokument die ausgewählte Integrationsmethode (siehe folgendes Kapitel), die zugewiesenen IP-Adressen und weitere wesentliche Parameter zusammengefasst werden (aktivierte Modus, Features etc.).

Anschließend kann die Grundkonfiguration der Appliance festgelegt werden. Die Default-IP ist 192.168.100.1. Daraufhin kann die Appliance produktiv verkabelt werden.

Dabei kann die Auswahl von Interfaces zunächst „wahllos“ erfolgen. Alle konfigurierten IP-Adressen werden von NetScaler automatisch auf den Schnittstellen aktiviert, auf denen der zugehörige IP-Verkehr vorgefunden wird ("Layer3-VLAN"). Um diese zwar zuverlässige Automatik später zu unterbinden, respektive die Zuordnung von IP-Adressen zu Interfaces manuell festzulegen, können VLANs definiert und Interfaces diesen VLANs zugeordnet werden (mit oder ohne Tagging, siehe auch Kapitel „Erweiterte Netzwerkfunktionen“). Zusätzlich können IP-Adressen (und damit das zugehörige Subnetz) dann in jeweils einem VLAN aktiviert werden, so dass sie definitiv nur noch dort verfügbar sind.

Nach abgeschlossener Netzwerkkonfiguration lohnt zur Veranschaulichung und Dokumentation ein Blick in den Network Visualizer (Web-GUI direkt unter Punkt „Network“). Vergleichbare Ansichten gibt es übrigens auch für Virtual Server, wo dann alle beteiligten Komponenten und Regeln/Aktionen übersichtlich und im Zusammenhang dargestellt werden. Die Visualizer Darstellung auf dem NetScaler bieten zudem die Möglichkeit der Drag-and-Drop Konfiguration und zudem eine optimale Möglichkeit die Konfigurationen über mehrere Services hinweg zu vereinheitlichen.

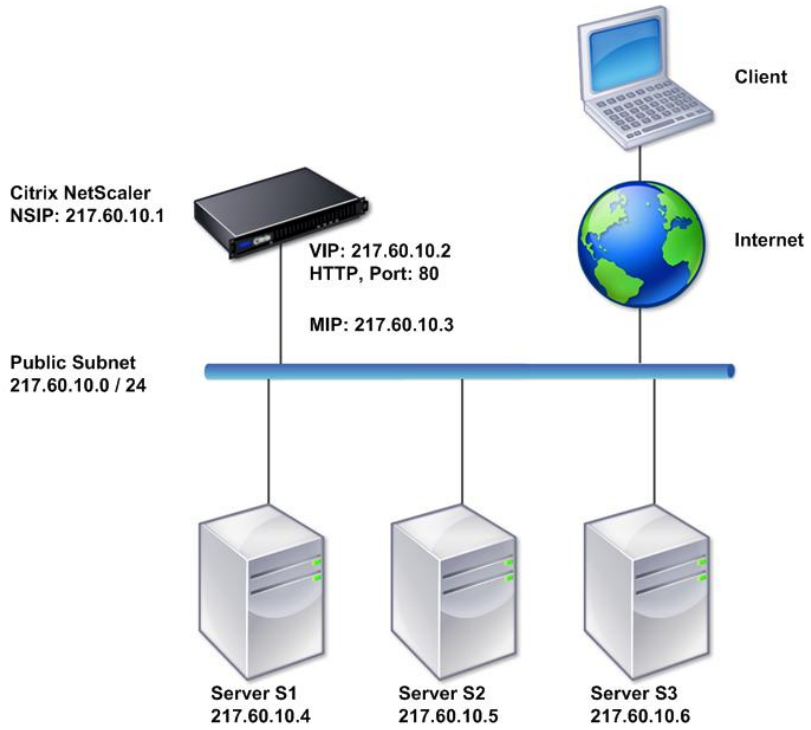
Integrationsvarianten

Für die NetScaler Einbindung in die eigene Infrastruktur stehen unterschiedliche Herangehensweisen zur Verfügung. Angefangen bei der physikalischen Anbindung an die umgebenden Netze bis zur logischen Integration auf Ebene IP-Adressen und Routing.

One-Arm Mode

Soll NetScaler etwa als Reverse Proxy für öffentlich bereitgestellte Services dienen, wird er in einer Demilitarisierten Zone (DMZ) platziert, in der ihn sowohl in Richtung Internet (public) als auch Servernetz (private) eine oder mehrere Firewalls umgeben. Da es sich um einen aus Netzwerksicht sicherheitskritischen Bereich handelt, wird es in der Regel vermieden, dass NetScaler selbst an mehrere Netze mit unterschiedlichen Sicherheitsniveaus angeschlossen wird. Daher wird hier der "One-Arm Mode" gewählt, in dem NetScaler nur an ein Segment angeschlossen ist und daher typischerweise auch nur IP-Adressen aus einem einzigen Subnetz besitzt. Natürlich können davon unabhängig mehrere physikalische Interfaces genutzt werden (siehe Kapitel 3).

Die parallele Anbindung an ein reines Management Segment kann durch strikte Trennung mittels VLANs auf NetScaler erfolgen, ohne dass das Überspringen von Traffic zwischen den Segmenten möglich wird (Layer 3 Modus muss deaktiviert werden!).



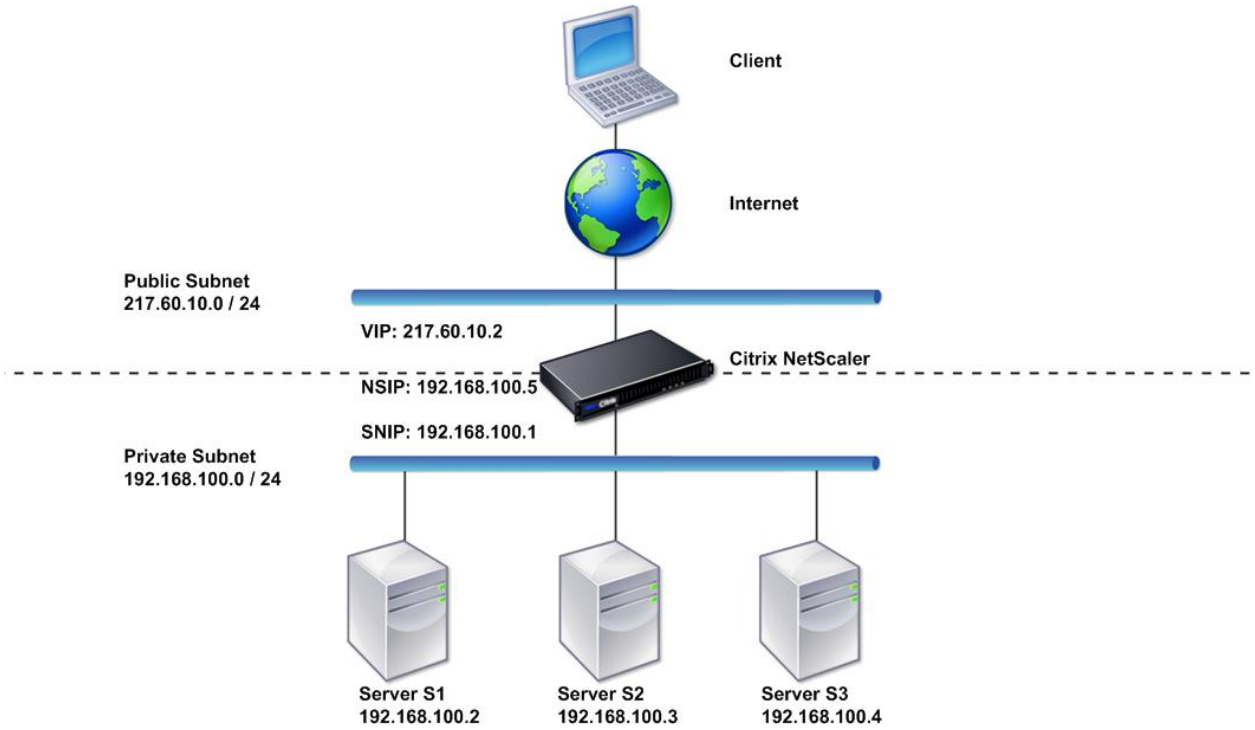
[Abbildung: One-Arm Mode]

Inline (Multi-Arm Mode)

NetScaler stellt bei dieser Integrations-Methode den einzigen Weg für die Clients dar, die Server zu erreichen, d.h. er verbindet die Netzsegmente entweder durch die Virtual Server, die er bereitstellt, oder auch komplett als Layer 3 Router.

Diese "Multi-Arm" Topologie bietet eine höheren Sicherheit, da sie erzwingt, dass jedes Paket zwischen Clients und Servern über NetScaler läuft und damit von ihm inspiziert werden kann. Neben der sauberen Trennung von Public und Private IP-Bereichen erhöht dies den Schutz für die Backends.

Soll zum Beispiel in einer Demilitarisierten Zone eine Trennung von extern und intern gerichtetem Verkehr erfolgen, empfiehlt sich die Integration zwischen zwei DMZ-Segmenten – DMZ-ext für die Annahme der externen User-Anfragen und einer DMZ-int für die Weiterleitung ins Backend.



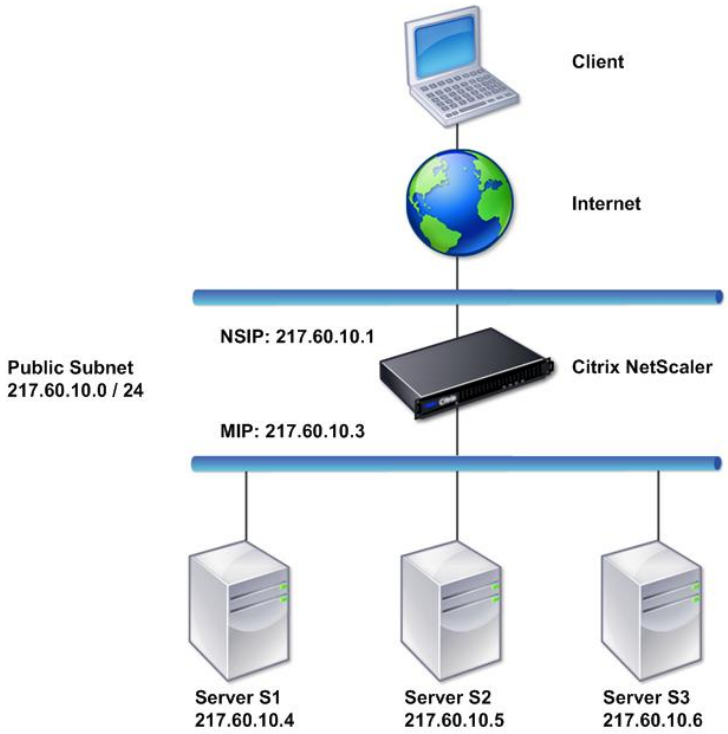
[Abbildung: Inline]

Inline Spezialfall: Transparent (Layer 2 Mode)

Der Vorteil des Inline Mode ist, dass eine NetScaler-Umgehung und der dort implementierten Optimierungs- und vor allem Schutzmaßnahmen verhindert wird. Durch den "Transparent Mode" kann das sogar erreicht werden, ohne eine Segmentierung auf IP-Ebene zu erzwingen. Auch dabei wird NetScaler physikalisch als einziger Weg zwischen der Client- und der Server-Infrastruktur implementiert. Durch die Aktivierung des "Layer 2 Mode" agiert NetScaler als Bridge und Clients können die Server direkt adressieren. Der Netzwerkverkehr aber läuft dennoch durch NetScaler, wo weiterhin annähernd alle Eingriffe in den Traffic möglich sind.

Damit dieses Szenario keinen Single Point of Failure in eine Netzwerkinfrastruktur einführt, sollten mehrere NetScaler eingesetzt werden, die in die bestehenden redundanten Netzwerk-Wege eingebunden werden. NetScaler nimmt nicht am Spanning Tree Protocol teil, er blockiert standardmäßig sogar die Bridge Protocol Data Units (BDPUs), die Switches zur Bestimmung der Baumstruktur austauschen. Je nach Topologie kann es daher erforderlich sein, BDPUs weiterzuleiten. Dazu wird der Modus „Bridge BDPUs“

aktiviert, wodurch NetScaler auch für diese Pakete eine transparente Leitung darstellt.
Für die erforderliche Redundanz sorgt in diesem Fall die den NetScaler umgebende Netzwerk-Infrastruktur durch dynamisches Routing oder Spanning Tree. Zudem erfolgt in diesem Spezialfall keine Konfigurations-Synchronisation zwischen den beiden NetScaler Systemen.



[Abbildung: Transparent]

IP-Adressen des NetScalers

NetScaler hat verschiedene Arten von IP-Adressen für unterschiedliche Aufgaben. Die erste Adresse ist die **NSIP** (NetScaler IP), die als primäre Management IP immer statisch existieren muss. In einem High Availability Paar aus zwei NetScaler-Systemen ist die NSIP die einzige fixe IP, die jedes einzelne System individuell besitzt. Von dieser Adresse gehen standardmäßig administrative Verbindungen wie DNS Requests, NTP Zeitsynchronisation, Authentifizierungsanfragen und die HA Synchronisation aus.

Bei der Erstinstallation muss weiterhin mindestens eine **SNIP** (Subnet IP) konfiguriert werden, die als Ausgangspunkt der Kommunikation zu den Backend Servern verwendet wird. Aus der Historie heraus existiert zudem die MIP (Mapped IP), die die gleiche Funktion wie die SNIP besitzt (Default: USNIP Modus) – nachfolgend wird daher nur noch von der SNIP die Rede sein. Per Default verwendet NetScaler immer die SNIP, die laut Routing Table dem Ziel am nächsten ist. Es sollte in jedem IP-Netz, in das NetScaler direkt kommunizieren kann oder soll, eine SNIP angelegt werden, die für diese Verbindungen genutzt werden kann. Der Weg in andere Netze wird über die Routingtabelle gefunden.

Der Dritte Typ von IP-Adressen sind die **VIP**s (Virtual IPs), die den Clients als Gegenstelle zur Verfügung stehen. Eine VIP wird typischerweise durch das Anlegen eines Virtual Servers erzeugt, der unter dieser IP ansprechbar ist, und muss daher nicht explizit angelegt werden.

Clients verbinden sich also zu VIPs, wo NetScaler die Verbindung terminiert. Dann baut er eine eigene Verbindung zu dem Backend Service auf, ausgehend von der entsprechenden SNIP, über die er die Client-Anfrage weiterleitet. Sollen die Server stattdessen die Client IP selbst als Quelle der Verbindung sehen, muss der USIP Modus (Use Source IP) am Service aktiviert werden. Der USIP Modus lässt sich zwar als globale Voreinstellung setzen, allerdings hat dies keinen Einfluss auf bereits angelegte Services, sondern stellt nur ein Vorgabewert für anschließend neu erstellt Backend-Services dar.

Bei Verwendung des USIP Modus ist zu bedenken, dass die Antwortpakete der Server direkt an die Client IP adressiert werden, was unter Umständen NetScaler umgeht, wenn das System im One-Arm-Modus betrieben wird oder der Server eine andere Route in das Client Netz besitzt, die nicht über NetScaler führt (asymmetrisches Routing).

Die Rücksendung der Pakete direkt zum Client kann allerdings auch ein gewünschtes Verhalten sein, es wird dann von der Funktion Direct Server Return (DRS) auf NetScaler gesprochen. Dazu muss allerdings auch der Backend-Service mit einer Loopback-IP Adresse versehen werden, die der des VServers auf NetScaler entspricht.

Administrative Verbindungen auf SNIP verlagern

Für die von NetScaler selbst ausgehenden administrativen Verbindungen (LDAP, DNS, RADIUS, CRL-Refresh, TACACS usw.) wird die NSIP verwendet. An einer zwischenliegenden Firewall würde somit neben der SNIP für die Client-Backend-Verbindungen auch die NSIP auftauchen. Um das zu vereinfachen, kann der Administrator dafür sorgen, dass auch administrative Verbindungen wie etwa DNS und LDAP (Authentifizierung) von einer SNIP ausgehen. Dazu werden für alle betroffenen Dienste Load Balancing VServer auf NetScaler angelegt, die die eigentlich zu adressierenden Server als load balanced Services ansprechen. Diese Backend Kommunikation geht dann von der entsprechenden SNIP aus, von der auch die sonstigen Verbindungen in das entsprechende Netz initiiert werden.

IP-Adressen im HA Modus

Wie bereits erwähnt, besitzt jeder NetScaler in einem HA-Verbund eine eindeutige NSIP über die er mit seinem HA-Partner kommuniziert. Nur über diese IP-Adresse ist es dem Admin möglich, die NetScaler in einem HA-Verbund für das Management getrennt anzusprechen.
In einem HA Paar ist es sinnvoll, den administrativen Zugriff auf einer SNIP zu aktivieren. Da alle Adressen abgesehen von der NSIP im HA Paar "floating", d.h. immer auf dem primären NetScaler aktiv sind, erreicht man darüber immer das System, auf dem die Konfiguration geändert werden kann.

Sind die an einem HA Setup beteiligten Systeme in unterschiedlichen Subnetzen untergebracht, muss der INC Modus (Independent Networking Configuration) aktiviert werden. Mit INC ist es möglich (und erforderlich), dass die NetScaler eines HA Paares nicht nur unterschiedliche NSIPs, sondern auch individuelle SNIPs besitzen. Die VIPs sind identisch (Public Segment), jedoch unterscheiden sich die IP-Adressen für die Backend Kommunikation entsprechend der unterschiedlichen Subnetze. Der INC-Mode setzt ein dynamisches Routingprotokoll voraus (RIP, OSPF, BGP) über das die VIPs als Hostroute verteilt werden können (RHI – Route Health Injection).

IPv6

Citrix NetScaler unterstützt IPv6 vollständig und insbesondere auch gemischt mit IPv4 Adressen, so dass etwa in einem VServer gleichzeitig IPv4 Backends und IPv6 Backends angesprochen werden können. Dadurch und auch durch die Möglichkeit, als VIP für einen Virtual Server eine IPv6 Adresse zu definieren und auf IPv4 Backends zu verteilen, werden sanfte Migrationen optimal unterstützt.

Erweiterte Netzwerkfunktionen

Um die verfügbare Bandbreite zwischen NetScaler und anderen Komponenten über die Kapazität eines einzelnen Interfaces hinaus zu erhöhen, können Interfaces zu sogenannten Channels zusammengefasst werden. Diese Link Aggregation genannte Konfiguration kann manuell oder durch das Link Aggregation Control Protocol (LACP) gesteuert erfolgen. Neben der Bandbreite wird damit zugleich auch die Ausfallsicherheit verbessert, da die Verbindung auch bei Ausfall eines Interfaces noch verfügbar ist.

Interfaces, die Teil eines Link Aggregate Channels werden, übernehmen die Parameter des Channels, insbesondere dessen VLAN Konfiguration. VLANs können sowohl Port-basiert (ein Interface/Channel in einem VLAN) als auch mit Tagging nach 802.1q (ein Interface/Channel in mehreren VLANs) konfiguriert werden.

Routing oder Bridging von VLANs

Unterschiedliche VLANs sind üblicherweise nur durch Layer 3 Router verbunden, d.h. ein System agiert als IP-Router zwischen ihnen. Diese Funktion kann auch Citrix NetScaler wahrnehmen, indem je ein VLAN mit einem IP-Subnetz assoziiert und der Layer 3 Mode aktiviert wird.

Bei aktiviertem Layer 3 Mode führt NetScaler standardmäßig IP-Forwarding zwischen allen ihm bekannten Netzen aus. Um dieses Routing einzuschränken und nur zwischen definierten Netzen durchzuführen, werden IP-Subnetze an sogenannte Bridge Groups gebunden. Dann werden Pakete nur noch in VLANs (Subnetze) weitergeleitet, die zur selben Bridge Group gehören.

NetScaler ermöglicht es, mehrere VLANs jedoch auch auf Layer 2 zu einer gemeinsamen Broadcast Domain zu verbinden. Sollen zwei oder mehr VLANs zusammengelegt werden, müsste normalerweise auf allen beteiligten Geräten in allen Domains die VLAN Konfiguration geändert werden. Stattdessen können auf NetScaler eine Bridge Group angelegt und die zu verbindenden VLANs dieser Bridge Group zugeordnet werden. Wird dann der Layer 2 Mode aktiviert, leitet NetScaler Broadcast Pakete aus einem VLAN an alle VLANs in derselben Bridge Group weiter und vermittelt auch Unicast Pakete durch das Nachschlagen aller von ihm in der entsprechenden Bridge Table verzeichneten MAC Adressen.

Erweitertes Routing

Neben dem statischen Routing zwischen Netzen, an die NetScaler direkt angebunden ist (durch SNIPs) oder die er über statische Routingeinträge kennt, unterstützt er auch dynamische Routingprotokolle: RIPv2, RIP for IPv6, OSPFv2, OSPFv3 for IPv6 und BGPv4 (RFC4271).

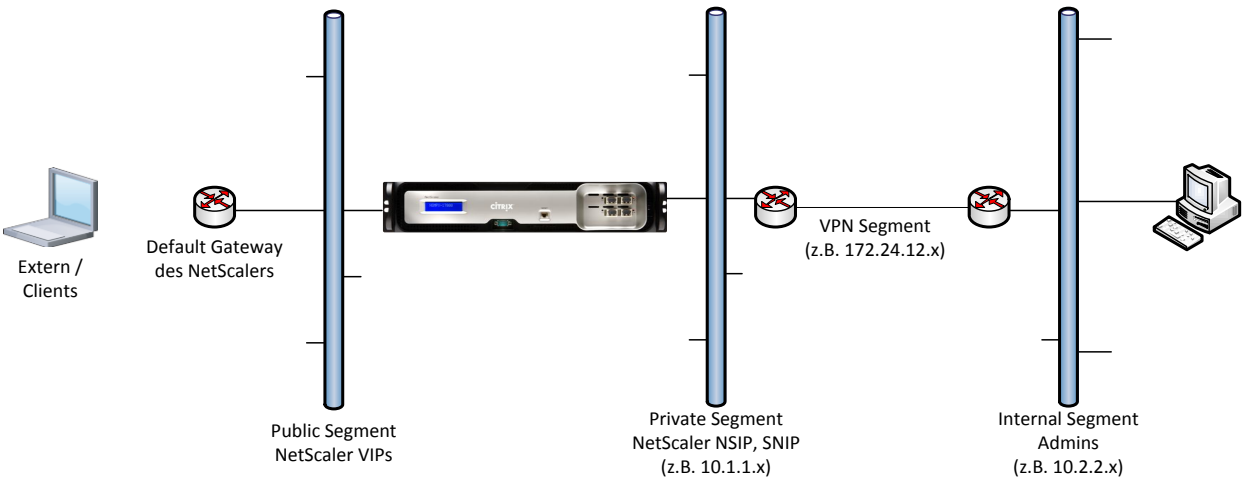
Eine weitere Möglichkeit, das Routingverhalten zu bestimmen, sind Policy Based Routes (PBRs). Mit PBRs kann das System den Next Hop für ein Paket abhängig von verschiedenen Merkmalen wie Quell-/Ziel-IP, Quell-MAC, Ports, Protokoll oder auch VLAN bestimmen. PBRs werden daher in Extended Access Control Lists (ACLs) definiert. NetScaler wertet für ein zu routendes Paket alle aktivierten PBRs aus und wendet die entsprechende Regel auf das Routing an. Trifft keine PBR zu oder ist die definierte Action ein DENY, wird das normale Routing anhand der Ziel-Adresse angewendet.

Das Ziel einer PBR kann auch ein Link Load Balancing (LLB) Virtual Server sein, der wiederum auf mehrere Next Routing Hops als Services weiterleiten kann, so dass beim Ausfall des bevorzugten Routers als Next Hop, was durch das Monitoring festgestellt wird, auf die verbleibenden Hops geschwenkt werden kann. Mittels LLB kann so ausgehender Verkehr auf mehrere Uplinks verteilt werden. Auch die Verteilung von ausgehendem Verkehr über zwei unabhängige Provider-Links ist ein typischer Anwendungsfall für diese Funktion.

MAC Based Forwarding

Vor der Konfiguration der NetScaler-Netzwerkparameter sollte geklärt werden, ob die Installation den MAC Based Forwarding Modus (MBF) nutzen kann oder muss. In dieser Betriebsart merkt sich NetScaler für jedes eingehende Paket, von welcher Absender-MAC dieses angekommen ist. Dazugehörige Antwortpakete sendet er wiederum an diese MAC adressiert zurück - unabhängig von etwaigen Routingentscheidungen auf höheren Schichten.

Auf diese Art erspart sich NetScaler nicht nur das Nachschlagen in seinen Routing- und ARP-Tabellen, sondern er verhindert auch das Entstehen von asymmetrischen Routen. Das ist besonders wichtig, wenn umliegende Systeme statusabhängig agieren, das heißt Pakete nur verarbeiten, die zu einer bekannten, etablierten Verbindung gehören. Typischerweise trifft das für Firewalls zu. Aber auch die Anbindung eines Admin-Netzes per VPN, in dem Adressen auf ein Zwischennetz umgesetzt werden, kann den MBF Modus erfordern, da NetScaler dieses Zwischennetz nicht bekannt ist und kein Gateway darin zur Verfügung steht, das Detault Gateway aber ins Internet führt und daher kein Rückweg in das Admin-Netz existiert.



[Abbildung: Keine ansprechbare Gateway-IP im VPN Segment – MBF erforderlich für Kommunikation mit dem Admin-Netz]

Network Address Translation und Access Control Lists

Um den Traffic zum und über NetScaler zu reglementieren und auf IP-Ebene zu modifizieren, ohne tatsächlich mit VServern einzugreifen, können darüber hinaus auch Access Control Lists sowie Network Address Translation eingesetzt werden.

ACLs sind dabei in einfacher Form (Simple) zum direkten Blockieren von Paketen bestimmter Quellen (IPs) auf bestimmte Ports und in sehr detaillierter Form (Extended) verfügbar. Extended ACLs können sogar „stateful“ agieren, also in Abhängigkeit vom Verbindungszustand.

Weiterhin können Extended ACLs als Filter für NAT verwendet werden: Durch die Definition in der Extended ACL wird spezifiziert, welche Pakete bearbeitet werden sollen. Verändert werden können sowohl die Quell-IP und der Ziel-Port für ausgehenden Verkehr (NetScaler RNAT, sonst auch SNAT und DPAT genannt) als auch die Ziel-IP für eingehenden Traffic (NetScaler INAT, sonst auch DNAT).

Soll etwa ein Server in einem Subnetz A für Clients aus einem anderen Subnetz B erreichbar gemacht werden, ohne dass ein Routing zwischen den Netzen oder ein VServer auf dem NetScaler existiert, kann dies mittels INAT realisiert werden. Voraussetzung ist, dass der NetScaler in beiden Subnetzen verbunden ist. Dann wird eine INAT Route angelegt, deren „Public IP Address“ eine VIP im Client Subnetz A ist (falls diese noch nicht existiert, wird sie neu angelegt) und deren „Private IP Address“ die IP des Servers im Subnetz B ist. Pakete an die Public IP werden dann umadressiert an die Private IP. Je nach Einstellung wird auch noch die Quell-IP verändert auf die nächstgelegene SNIP (Use Subnet IP) oder eine bestimmte SNIP (Proxy IP).

NetScaler High Availability

Eine schon genannte NetScaler Funktion ist der Betrieb in einem Verbund mehrerer Systeme zur Sicherstellung von Hochverfügbarkeit. Durch seine Funktionalität als intelligenter Load Balancer stellt das System Hochverfügbarkeit für die Backend Services sicher und wird damit zugleich zum hochkritischen Punkt der Infrastruktur, von dessen Verfügbarkeit zahlreiche zentrale Dienste abhängig sind.

Active/Standby Modus

Die am häufigsten eingesetzte und angebrachte Variante – der HA Modus ist Active/Standby. In dieser Betriebsart bilden zwei NetScaler Appliances ein HA Paar, in dem lediglich die NSIPs individuell sind, während alle anderen Adressen „floating“ beim Failover vom Standby System übernommen werden. Konfigurationsänderungen sind nur auf dem aktiven Knoten (Primary) möglich bzw. dauerhaft. Solange beide Systeme in Betrieb sind, werden alle auf dem Primary ausgeführten Kommandos (also alle Konfigurationsänderungen) per „Command Propagation“ auch auf dem Secondary Node ausgeführt. Bei einem Reboot zieht sich das startende Standby System die Konfiguration einmal komplett vom Primary Node (HA Synchronization).

Active/Standby mit INC

Eine Möglichkeit des Active/Standby Modus ist die Independent Network Configuration (INC), die dann erforderlich ist, wenn ein HA Paar auf zwei Standorte verteilt ist, in denen unterschiedliche IP-Netze verwendet werden oder zwischen denen gar keine Layer 2 Verbindung existiert. Die INC erlaubt es jedem Knoten im HA Paar, die Backends jederzeit selbst zu überwachen und damit auch ohne Verbindung mit dem HA Partner den Monitor Status zu kennen, da neben der NSIP auch die SNIPs individuell und damit jederzeit aktiv sind. Im Unterschied zu einem Deployment mit Global Server Load Balancing (GSLB), das als nächste Abstraktionsstufe der Hochverfügbarkeit gelten kann, handelt es sich aber immer noch um ein HA Paar, das eine gemeinsame Konfiguration synchronisiert.

Befinden sich die Knoten nicht im selben Layer 2 Segment, müssen die VIPs wiederum per Route Health Injection bekannt gemacht werden, d.h. es muss ein dynamisches Routing Protokoll zum Einsatz kommen. Anderenfalls reicht der normale IP Failover mit anschließender Gratuitious ARP (GARP) Bekanntgabe an alle Teilnehmer des Segmentes aus.

NetScaler Pools, Active/Active

Zu einem HA Deployment können auch mehr als zwei NetScaler verbunden werden, wir sprechen dann von NetScaler Pools. Zwar ist auch ein Deployment mit mehr als einem Standby System möglich (Active/Standby/Standby/…), aber in der Praxis sind NetScaler Pools vor allem interessant in Situationen, wo mehr aktive Leistung benötigt wird, als eine einzelne Appliance liefern kann. In Anbetracht der Leistungsmerkmale der MPX Hardware Appliances mit bis zu 50 Gbit/s Datendurchsatz, sind diese Situationen zwar äußerst selten, aber auch dieser Ansatz zur Skalierung kann gewünscht sein (z.B. sehr hohe Durchsatzanforderung für FIPS-zertifiziertes Deployment). Ein NetScaler Pool mit mehreren aktiven Knoten ist eine Erweiterung eines einfachen Active/Active Paares, um zusätzliche Failover Kapazität (N+1 oder auch N+X) und Leistung.

Bei Active/Active Deployments besteht kein HA Paar im Sinne von gemeinsamer Konfiguration oder gemeinsamen IP Adressen, alle NetScaler laufen standalone. Die Zuordnung von VIPs zu Systemen erfolgt mit Hilfe des Virtual Router Redundancy Protocols (VRRP), indem jedem NetScaler-System für jede VIP eine Priorität zugewiesen wird. Die Systeme regeln dann untereinander, welche VIP zu einem Zeitpunkt auf welchem NetScaler aktiv ist.

Als weitere Konsequenz aus der Tatsache, dass die Systeme in einem NetScaler Pool keine Synchronisationsmöglichkeit haben, müssen zur Sicherstellung von Session Persistence verbindungslose („stateless“) Methoden eingesetzt werden. Beispiele dafür sind Hash-basierte Persistenz und vor allem Cookie Insert, bei dem der Client seine Persistenz-Informationen praktisch selbst besitzt und mitliefert. Zudem erfolgt beim Active/Active Betrieb keine Session-Synchronisation.

VMACs und Firewall Load Balancing

Bei einem IP Failover wird die neue Heimat einer IP-Adresse durch GARP Pakete bekanntgegeben. Sicherheitskritische Systeme beachten diese Pakete unter Umständen nicht weiter, da ihnen damit auch gefälschte ARP Einträge untergeschoben werden könnten, so dass es zu längeren Unterbrechungen im Falle eines Failovers kommen kann. Hier, wie auch speziell im Sonderfall des Firewall Load Balancing, das in der Regel sowieso auf Layer 2 stattfindet, sind virtuelle MAC Adressen (VMACs) hilfreich. Diese können ebenso zwischen NetScaler-Systemen wandern, wie IP-Adressen, so dass keine Neuzuordnung von IP zu MAC mehr erforderlich ist.

Auslöser für ein Failover

Standardmäßig werden alle verbundenen Interfaces überwacht und der Verlust des Links an einem Interface führt zum Failover auf den Standby Node. Die schon beschriebene Link Aggregation zur Erhöhung der verfügbaren Bandbreite, durch die auch die Abhängigkeit von einem einzelnen Interface aufgehoben wird, muss für die HA Konfiguration in Form eines Failover Interface Set (FIS) abgebildet werden. Beim Ausfall eines Interfaces in einem FIS findet daher kein Failover statt, solange noch ein Interface des FIS verfügbar und verbunden ist.

Neben der völligen Unerreichbarkeit des bislang aktiven Partners gibt es weitere Auslöser – oder auch Hinderungsgründe – für ein Failover der Ressourcen auf einen Standby NetScaler. So kann ein Failover auf den HA-Partner abhängig von der Verteilung von dynamischen Routen ausgelöst werden. Dazu können dynamisch via RIP, OSPF, BGP auf NetScaler gelernte Routen mit einem entsprechenden "Route Monitor" versehen werden. Ist diese Route bei dem nächsten Routing-Update nicht mehr enthalten, wir ein Failover ausgelöst.

Failsafe Mode

Diese Einstellung definiert auf dem "Master“ NetScaler, dass dieser auch in dem Fall Master bleiben soll, wenn beide NetScaler gleichzeitig einen Fehler aufweisen und ein System "die Stellung halten muss". Ein Beispiel dafür könnte der Ausfall eines Switches sein, auf dem beide NetScaler mit je einem Interface angeschlossen waren, für das das HA-Monitoring aktiviert war. Diese Einstellung erfolgt pro NetScaler und ist von der Synchronisation ausgenommen – wird also nur auf dem System aktiviert, der in einem solchen Fall Master bleiben soll.

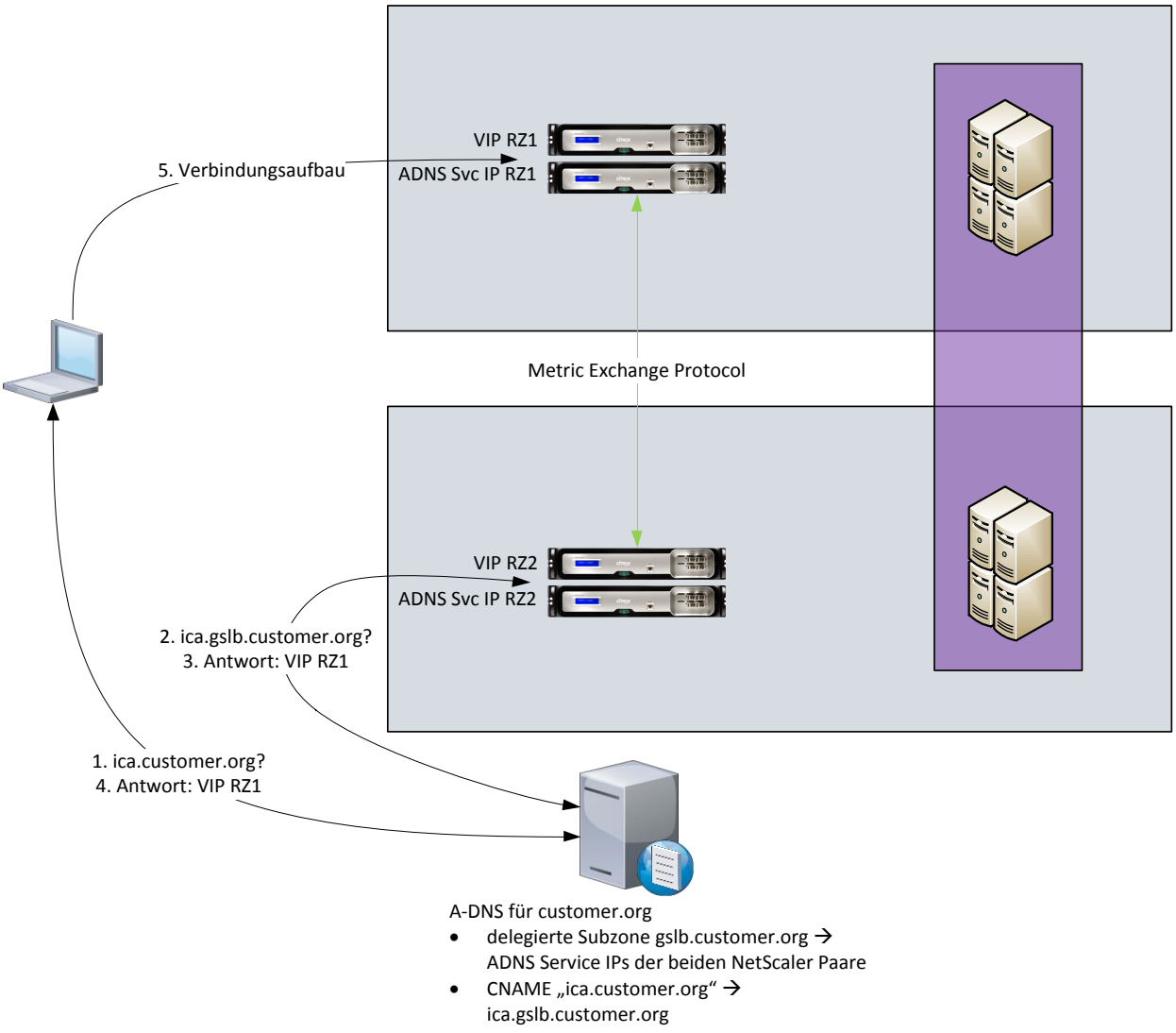
Lastverteilung und Desaster Recovery (DR) über verteilte Rechenzentren

Unternehmen mit hohen Anforderungen an die Verfügbarkeit von Services können eingehende Benutzer-Anfragen über zwei geografisch getrennte Rechenzentren verteilen. Wie beim Load Balancing innerhalb einer lokalen Serverfarm wird durch den einheitlichen Eingangspunkt – hier in Form eines Hostnamens statt einer IP-Adresse – und die Verteilung auf verfügbare Server neben einer höheren Leistungsfähigkeit gleichzeitig eine höhere Verfügbarkeit erreicht.

Um die Verfügbarkeit auch innerhalb jedes einzelnen Rechenzentrums zu gewährleisten, erfordert dieses Szenario ein HA Paar aus zwei NetScaler-Systemen je Rechenzentrum (z.B. in unterschiedlichen Brand-schutzzonen).

Funktion: Global Server Load Balancing (eingehender Verkehr)

„Eingehender Verkehr“ steht dabei für eine User-seitig initiierte Verbindung – dies wird bei NetScaler über die GSLB–Funktion realisiert.



[Abbildung: Global Server Load Balancing (GSLB)]

Die Funktionsweise des GSLB ist wie folgt: Ein Client möchte auf den Service unter „ica.customer.org“ zugreifen und sendet daher eine DNS Anfrage nach diesem Namen. Der autoritative Nameserver für die Zone "customer.org" hat für diesen Namen einen Alias Eintrag (CNAME), der auf „ica.gslb.customer.org“ verweist, sowie eine Subzone „gslb.customer.org“, die an zwei Nameserver delegiert ist, man spricht hier von "Domain Delegation". Diese Nameserver sind die ADNS Service IPs (als solche definierte SNIPs oder MIPs) der beiden NetScaler-Paare.

Die NetScaler-Systeme bestimmen anhand der konfigurierten GSLB Parameter und des Servicestatus die zurück zu liefernde(n) VServer-Adressen (VIPs) und nennen diese als Antwort. Dabei können mehrere Adressen in durch die LB-Präferenz bestimmter Reihenfolge zur Auswahl durch den Client oder auch nur eine einzige zu verwendende IP zurückgeliefert werden. Der Client bekommt diese VIPs als Antwort auf seine DNS Anfrage und baut seine Verbindung dann zur ersten durch die NetScaler gelieferten VIP auf.

Die Entscheidung, welche VIP auf eine bestimmte Anfrage zurückgeliefert wird, basiert auf den eingestellten GSLB Parametern und Methoden (u.a. Round Robin, Least Connection oder Round Trip Time).

Zum Austausch der Statusinformationen, die zur Entscheidung erforderlich sind, sowie von Persistenzinformationen nutzen die NetScaler zwischen den verschiedenen Rechenzentren dabei das Metric Exchange Protocol (MEP). Je Site kommt für diese Kommunikation noch eine weitere IP-Adresse ins Spiel, nämlich die GSLB Site IP, die aber ebenso wie die ADNS Service IP eine bestehende SNIP oder MIP, aber auch ein völlig eigenständige IP sein kann.

Featuring: Link Load Balancing (ausgehender Verkehr)

„Ausgehender Verkehr“ beschreibt eine Server-seitig initiierte Verbindung, diese wird bei NetScaler über die zuvor beschriebene LLB–Funktion realisiert.

Content Switching für Transparente Caches – ein Fallbeispiel

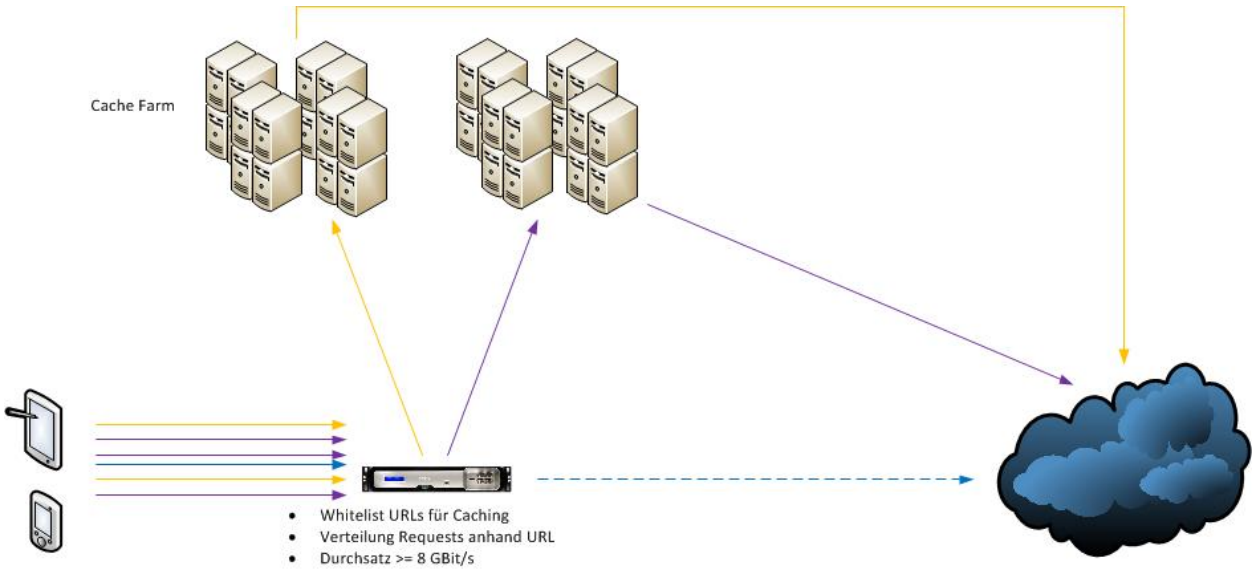
Featuring: Inline, L3 Mode, MAC Based Redirection, Use Source IP

Anforderung: Ein Telekommunikationsanbieter will eine Infrastruktur für transparentes Caching von Inhalten implementieren, die das Datenvolumen in Schach hält und die Zugriffszeiten beschleunigt, die seine Kunden über ihre Mobilfunkgeräte anfordern. Die zu bedienende Bandbreite wird mit 8GBit/s veranschlagt, Luft nach oben sollte natürlich auch noch sein.

Es wird eine Cache-Farm mit einigen Dutzend Cache Servern bereitgestellt, die in Gruppen jeweils für eine definierte Liste von Domains oder URLs zuständig sein sollen. Je Gruppe existiert also eine Liste von URLs, für die diese Gruppe zuständig ist, und deren Gesamtheit ergibt die Liste von URLs für die nur die Cache-Farm angesprochen werden soll. URLs, die nicht auf der Gesamtliste sind, sollen nicht durch die Caches laufen, sondern direkt abgeholt werden (Whitelist-Verfahren). Außerdem soll ein Verbindungslimit pro Cache-Server gesetzt werden, so dass ein Cache, der z.B. 1.000 bestehende Verbindungen bedient, keine weiteren Anfragen mehr bekommt. Gefragt ist nun eine Komponente, die als Content Switch vor den Caches agiert und die Requests entsprechend umleitet oder direkt weitergibt – aber immer ohne etwas an den Paketen ab Layer 3 aufwärts zu ändern. Es dürfen keinerlei Adressumschreibungen oder ähnliche Veränderungen stattfinden, da die Zuordnung von Requests zu Clients jederzeit und dauerhaft möglich sein müssen.

Lösung: Citrix NetScaler MPX 11500. Die MPX 11500 hat genau 8GBit/s als Maximaldurchsatz, ist aber per Lizenzupgrade ("Pay-As-You-Grow") auf bis zu 42Gbit/s (MPX 20500) skalierbar.

Mehr Inforamationen zu Pay-As-You-Grow:
http://www.citrix.com/English/ps2/products/subfeature.asp?contentID=2300447



[Abbildung: NetScaler als Content Switch für eine Transparent Caching-Farm]

Das NetScaler HA Pair wird als L3 Router in den Traffic eingebunden (Inline), d.h. jeglicher Verkehr zwischen Clients (Mobilfunkgeräte) und dem Internet läuft durch die NetScaler-Systeme. Genutzte Funktionen sind: Load Balancing, Content Switching und Cache Redirection. Neben dem Layer 3 Mode wird außerdem der Modus MAC Based Forwarding aktiviert. Die Pakete werden unter Verwendung des Redirection Mode "MAC Based" (Einstellung auf dem VServer) weitergeleitet, ohne an ihren Layer 3 Informationen etwas zu verändern.

Die Cache-Server werden dann als Services für das Load Balancing angelegt, in deren Einstellungen zwei Parameter wichtig sind: Der Cache Type wird auf „TRANSPARENT“ festgelegt und die Option USIP (Use Source IP) aktiviert, falls sie nicht schon global vorgegeben wurde. Darüber hinaus kann die Anforderung, nur maximal 1.000 aktive Verbindungen pro Cache zuzulassen, abgebildet werden, indem für die Services entsprechende Thresholds gesetzt werden. Ein „Max Clients“-Wert von 1.000 stellt sicher, dass ein Service (ein Cache) keine neuen Requests bekommt, sobald er 1.000 aktive Verbindungen hat.

Darauf aufbauend gibt es für jede Cache-Gruppe einen Load Balancing Virtual Server, der auf die entsprechenden Services verteilt. Angesprochen werden die Load Balancing VServer durch den Cache Redirection VServer, der als oberste Instanz angelegt wird. Sein Cache Type muss ebenfalls „TRANSPARENT“ sein, außerdem müssen die Parameter „L2 Connection“ und „Origin USIP“ aktiviert werden. Wichtig sind weiterhin die Einstellungen Redirect = Policy und Redirect To = Cache, durch die festgelegt wird, dass Requests anhand von Policies an Caches zugewiesen werden. Requests, auf die keine Policy zutrifft, werden dann unverändert weitergegeben. Die Policies werden als Content Switching Policies (CSW) angelegt und haben die Load Balancing VServer als Ziel. Die Expressions zur Zuordnung sollten Pattern Sets nutzen, in denen die URL Listen verwaltet werden.

Ergebnis: Ein Cache Redirection Service, der alle Requests transparent weitergibt: abhängig von Policies (URL Listen) an Gruppen von Cache-Servern oder alles außerhalb der Listen direkt ans Ziel bzw. den Next Hop Router in Richtung des Ziels. Trotz des Betriebsmodus als Layer 3 Router werden Verbindungen dieses Service aber anhand von Layer 2 Merkmalen zugeordnet und die Pakete entsprechend vermittelt.