

Whitepaper

Load Balancing



Moderne Unternehmensanwendungen haben hohe Bandbreitenanforderungen. Immer mehr digitale Anwendungen wie HD-Streaming, die Anbindung von Cloud-Diensten sowie Multimedia- und Sprachanwendungen erfordern Bandbreiten, die heute an vielen Standorten noch nicht verfügbar sind. Und schnelle Glasfaseranschlüsse sind vielerorts noch auf Jahre nicht zu erwarten. Als Lösung bietet sich der Einsatz mehrerer Internetzugänge wie VDSL an. Die Vorteile: Bei Ausfall einer Internetleitung steht ein redundanter Anschluss zur Verfügung (High Availability) und die Last im Netzwerk lässt sich intelligent auf die verschiedenen Internetleitungen verteilen. Die Technologie zur effizienten Nutzung mehrerer WAN-Verbindungen nennt sich Load Balancing. Insbesondere in modernen SD-WAN-Infrastrukturen kommt diese Technologie zum Einsatz, beispielsweise um technisch veraltete MPLS-Leitungen durch mehrere kostengünstige Internetzugänge zu ergänzen oder zu ersetzen.

Das Konzept

Load Balancing dient zur Lastverteilung des Datenaufkommens im Netzwerk. So werden Datenverbindungen ausgeglichen über mindestens zwei Leitungen aufgeteilt und darüber hinaus auch bei Ausfall einer Leitung über die andere Leitung stets abgesichert. Dabei werden TCP-Verbindungen dynamisch auf voneinander unabhängige WAN-Verbindungen verteilt (Dynamisches Load Balancing).

Dem Netzwerk steht damit auch die Summen-Bandbreite der einzelnen Kanäle zur Verfügung, dennoch ist jede einzelne TCP-Verbindung auf die Bandbreite des zugewiesenen WAN-Anschlusses beschränkt. Daher kann es sinnvoll sein, besonders bandbreitenintensive (z. B. HD-Streaming) oder kritische Anwendungen (z. B. Voice over IP) dedizierten WAN-Leitungen zuzuweisen, um eine stets hohe Qualität zu gewährleisten (Statisches Load Balancing).

Paketbasiertes vs. Session-basiertes Load Balancing

Beim paketbasierten Load Balancing kann es zu veränderter Reihenfolge der gesendeten Pakete durch unterschiedliche Laufzeiten kommen. Dadurch ist das paketbasierte Load Balancing für viele Protokolle ungeeignet.

Dieses Problem kann beim Session-basierten Load Balancing nicht auftreten, weshalb dieses zu empfehlen ist. LANCOM verwendet daher auch ausschließlich das Session-basierte Load Balancing.

Empfohlene Geräte

Typischerweise kommen für die Nutzung mehrerer Internetanschlüsse mit Load Balancing auch mehrere Geräte zum Einsatz. Häufig haben Router nur ein Modem integriert, so dass dann zusätzliche Modems zum Einsatz kommen müssen. In solchen

Szenarien müssen also mehrere Geräte betrieben, gewartet und mit Strom versorgt werden. Durch die erhöhte Anzahl der Geräte ergibt sich eine höhere Ausfallrate.

Aus diesem Grund empfiehlt sich der Einsatz von speziell dafür ausgelegten Routern. Diese machen die simultane Nutzung verschiedener Internetanschlusssarten (DSL, Glasfaser, 5G) durch die Integration mehrerer Modems über nur ein Gerät möglich. Das reduziert zum einen den Konfigurationsaufwand, da man nur ein Gerät einrichten muss, und verringert zum anderen die Ausfallwahrscheinlichkeit.

Für den sicheren, standortübergreifenden Datentransfer zum Beispiel in Filialnetzen sollten die zum Einsatz kommenden Geräte zudem die Verschlüsselungstechnologie IPsec-VPN der aktuellen Version IKEv2 unterstützen.

In Kombination dieser Eigenschaften wird von ‚Multi-WAN-VPN-Gateways‘ gesprochen.

Backup vs. Active/Active (Load Balancing)

Beim Backup ist immer nur eine Leitung aktiv, die zweite Leitung wird nur bei Ausfall der Primärverbindung aktiviert. Hierbei kommt z. B. VDSL mit einem LTE-Backup zum Einsatz. Da LTE häufig mit einem Volumentarif verbunden ist, möchte man diese Leitung nicht für eine Lastverteilung nutzen, sondern nur zur Ausfallsicherheit im Hintergrund verfügbar halten.

Im Unterschied dazu sind beim Load Balancing in einem ‚Active/Active‘-Betrieb immer alle Verbindungen gleichzeitig aktiv. Somit wird die vorhandene Bandbreite komplett ausgenutzt und der Datenverkehr kann entsprechend verteilt werden.

Beim Load Balancing hat man somit auch immer ein Backup.

Einsatzszenarien

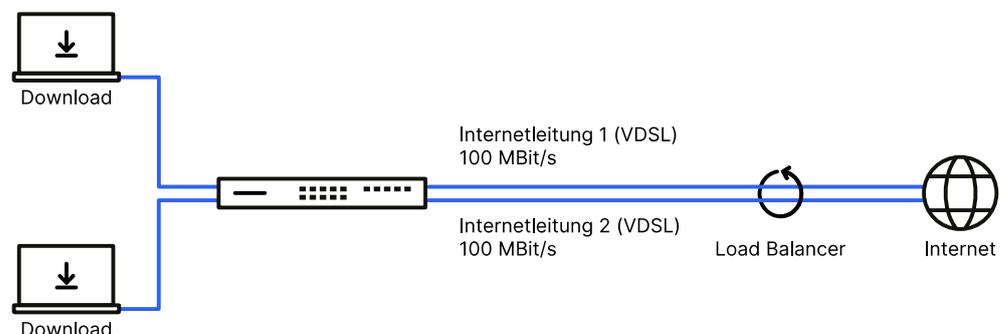


Abbildung 1:
Internet Load Balancing mit
zwei oder mehr Clients

Zwei oder mehr Clients sind über ein Multi-WAN-VPN-Gateway mit dem Internet (2 x VDSL mit je 100 MBit/s) verbunden. Nun können z. B. zwei Clients dank im Gateway integriertem Load Balancer parallel mit jeweils 100 MBit/s Downloadgeschwindigkeit arbeiten, denn dieser ermöglicht die Aufteilung der Datenlast auf beide VDSL-Internetleitungen.

Damit kann eine maximale Auslastung von 200 MBit/s und daraus folgend eine enorme Netzwerk-Effektivitätssteigerung realisiert werden.

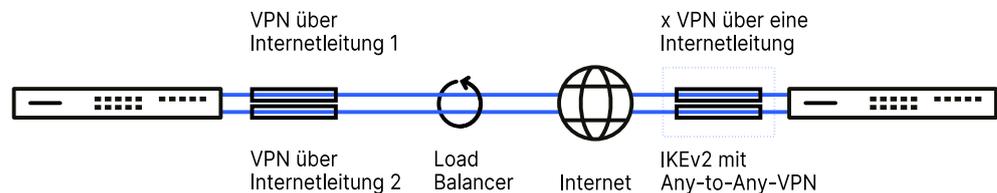
Dieses Szenario funktioniert mit allen Internetverbindungen. Zudem muss nur der lokale Router diese Funktion unterstützen, das heißt, dass kein separates Gateway im Rechenzentrum oder der Zentrale benötigt wird.

Abbildung 2:
Load Balancing und
VDSL-/LTE-Backup von
Internetzugängen



Neben dem Effekt einer effizienten Lastverteilung in einem Load Balancer-Verbund kann bei Ausfall einer Internetleitung die andere den Datentransfer übernehmen. Spezielle Multi-WAN-VPN-Gateways kombinieren neben zwei VDSL-Modems zusätzlich ein LTE-Modem in nur einem Gerät. Dieses zusätzliche LTE-Modem kann für eine Backup-Verbindung genutzt werden, im Fall, dass die VDSL-Leitungen ausfallen – eine ideale Lösung für höchste Verfügbarkeit in geschäftskritischen Umgebungen.

Abbildung 3:
VPN Load Balancing



Auch IKEv2-VPN-Verbindungen lassen sich bequem zu einem Load Balancer-Verbund zusammenfassen. Neben der Lastverteilung und Übernahme des Datenverkehrs, falls eine Verbindung ausfällt, wird durch den Zusammenschluss die VPN-Bandbreite für mehrere Clients deutlich gesteigert.

In diesem Szenario müssen sowohl das Gerät in der Filiale als auch das Gerät in der Zentrale die Load Balancing-Funktion für VPN unterstützen. Dabei muss sichergestellt werden, dass die VPN-Verbindungen, welche sich im Load Balancing-Verbund befinden, immer am gleichen Zielgerät in der Zentrale terminiert werden.

Client Binding

Der Einsatz von Internet Load Balancing kann aufgrund der unterschiedlichen NAT-IP-Adressen bei Servern zu Problemen führen, die zur Identifizierung eines angemeldeten Benutzers dessen IP-Adresse verwenden (z. B. Online-Banking). Wählt der Load Balancer z. B. beim Aufruf einer neuen Webseite eine andere Internetverbindung als die, über die sich der Benutzer am Server angemeldet hat, wertet der Server das als

Verbindungsversuch eines nicht angemeldeten Benutzers. Der Benutzer bekommt bestenfalls erneut einen Anmeldedialog zu sehen, nicht aber die gewünschte Webseite.

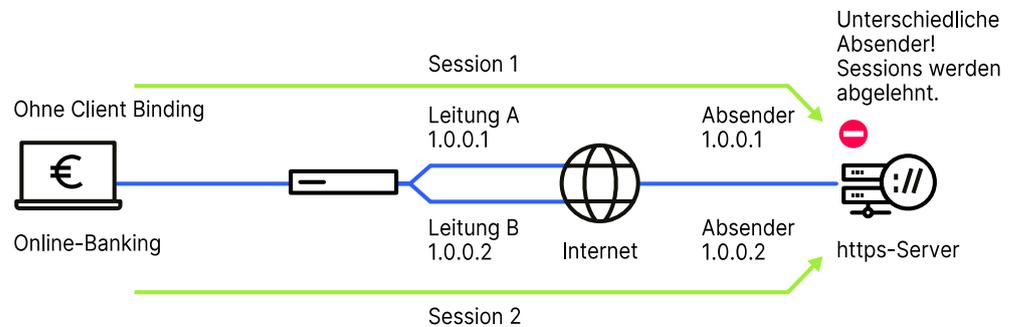


Abbildung 4:
Ohne Client Binding

Eine Möglichkeit zur Abhilfe ist, in den Firewall-Regeln den Datenverkehr mit diesem Server auf eine bestimmte Internetverbindung festzulegen („Policy Based Routing“). Damit ist jedoch der gesamte Datenverkehr aller Clients zu diesem Server auf die Bandbreite dieser einen Verbindung beschränkt.

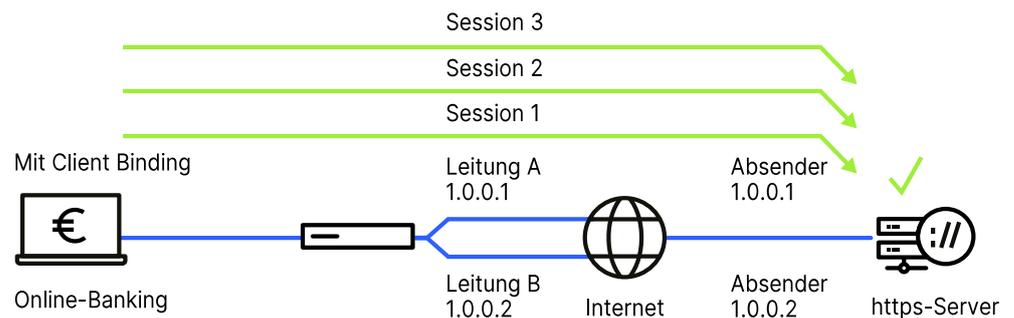


Abbildung 5:
Mit Client Binding

Ein Backup ist darüber hinaus nur mit erhöhtem Konfigurationsaufwand zu erreichen.

Das Client Binding überwacht im Gegensatz dazu nicht die jeweiligen einzelnen TCP/IP-Sessions, sondern orientiert sich am Client, mit dem bei der ersten Session eine Internetverbindung zustande kommt. Es leitet alle nachfolgenden Sessions von diesem Client ebenfalls über diese Internetverbindung, was dem Verhalten nach dem zuvor angesprochenen Policy Based Routing entspricht. Das Client Binding erfolgt protokollabhängig, d. h., es überträgt nur Daten desselben Protokolltyps (z. B. HTTPS) über diese Internetverbindung. Lädt der Client sich zusätzlich Daten über eine HTTP-Verbindung, erfolgt das wahrscheinlich über eine andere Leitung.

Zusammenfassung

In diesem Whitepaper wurde das Load Balancing vorgestellt. Dieses dient insbesondere der Erhöhung der Bandbreite bei gleichzeitiger Verteilung der Last auf die vorhandenen Verbindungen. Gleichzeitig kann es ggfs. als Redundanz dienen, um neben der Lastverteilung auch der Ausfallsicherheit zu dienen und auf Wunsch zusätzlich mit einer Backup-Verbindung abgesichert werden.