Reverse Proxy (NGINX)

Ein Reverse Proxy dient dazu einkommende Anfragen zu verwalten und diese an weitere Applikationen weiter zu leiten (Aivaliotis, 2013). Diese Anfragen folgen meist dem HTTP- bzw. HTTPS-Protokoll, aber sind nicht auf diese beschränkt. Im Allgemeinen wird zwischen 2 verschiedenen Reverse Proxy Arten unterschieden. Zum einen dem Protection Reverse Proxy und zum anderen dem Integration Reverse Proxy. Ein Protection Reverse Proxy ermöglicht es Anfragen gezielt zu filtern und nur gewünschte Anfragen durchzulassen. Ein Integration Reverse Proxy ermöglicht es Anfragen auf viele unterschiedliche Systeme zu verteilen. Im Folgenden wird nur der Intergration Reverse Proxy weiter beachtet, da ein Protection Reverse Proxy nicht zu Einsatz kam. (Sommerlad, 2003)

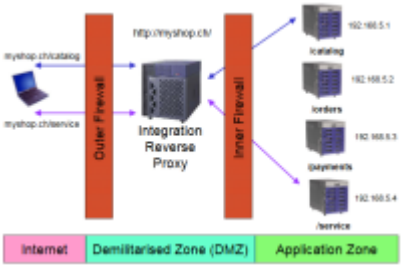
Probleme bei der Bereitstellung von Webapplikationen

Eine Webapplikation besteht meistens nicht nur aus einem Webserver beziehungsweise Webdienst, welcher alle Aufgaben übernimmt, sondern mehreren. Als Entwickler entstehen schwerwiegende Probleme, wenn versucht wird eine Applikation auf lediglich einem Server zu betreiben. Nach Sommerlad gibt es sieben Punkte die es zu beachten gilt:

- Man kann eine Webapplikation nicht auf einem Server implementieren, da dies die Komplexität erhöht, die Performance oder Wiederverwendbarkeit verschlechtert.
- Man möchte die allgemeine Netzwerkstruktur der Webapplikation verstecken, um bei Änderung jener beispielsweise Lesezeichen der Nutzer nicht zu zerstören.
- Das Backend der Webapplikation muss auch funktionieren, wenn sich die Netzwerkstruktur ändert. Wenn eine Applikation des Backends auf eine andere Maschine verschoben wird, darf das die Anderen Applikationen nicht beeinflussen.
- Man muss die Möglichkeit haben Teile der Netzwerkstruktur zu ändern, ohne andere Teile zu beeinflussen.
- Man muss die Möglichkeit haben neue Elemente und somit Funktionalität zur Webapplikation hinzufügen zu können.
- Man muss die Möglichkeit haben Anfragen zwischen mehreren Hosts aufteilen zu können.
- Das ganze System sollte lediglich über ein einziges SSL Zertifikat verfügen, da SSL Zertifikate einen hohen Preis haben und deren Erneurung koordiniert werden muss.

Die von Sommerlad genannten Punkte sind von hoher Relevanz. Jedoch ist ein Punkt mittlerweile nicht mehr aktuell. SSL-Zertifikate können mittlerweile auch kostenlos bezogen und automatisch erneuert werden. Siehe Verschlüsselung mit TLS. Ein weiterer Punkt mit hoher Relevanz ist die Ausfallsicherheit. Sollte eine Webapplikation lediglich auf einem Server betrieben werden und dieser fällt aus, dann ist die komplette Applikation folglich nicht mehr erreichbar.

Lösung für die Probleme



Vorteile der Lösung

Verschlüsselung mit TLS

Load Balancing

Double Reverse Proxy

From:
https://wiki.eolab.de/ - **HSRW EOLab Wiki**

Permanent link:
https://wiki.eolab.de/doku.php?id=user:jan001:ba:reverseproxy&rev=1612801017

Last update: **2021/08/24 17:34**