

Ausgangslage und Zielsetzung

Das hier behandelte Szenario basiert auf folgender Infrastruktur:

- Zur Verfügung stehen eine [IPv4](#)-Adresse und ein [IPv6](#)-Subnet (Standard 64-Bit).
Die [IPv4](#)-Adresse ist einem [Proxmox](#)-Server zugewiesen, der diverse virtuelle Maschinen beherbergt, die sich in einem separaten Netzwerk ([Brücke mit NAT](#)) befinden.
Das [IPv6](#)-Subnet wird ebenfalls vom [Proxmox](#)-Server verwaltet und über [geroutete Brücken](#) an die virtuellen Maschinen verteilt.
- Eine dieser virtuellen Maschinen stellt einen Webserver [Apache 2.4](#) als [ReverseProxy](#) zur Verfügung.
Der Traffic, der beim Proxmox-Host auf den Ports 80 (HTTP) und 443 (HTTPS) ankommt, wird direkt zu diesem [ReverseProxy](#) durchgeleitet.
- [Stirling-PDF](#) läuft auf einer weiteren virtuellen Maschinen.
- Die VM mit [Stirling-PDF](#) ist nicht direkt von außen zu erreichen:
Zwar könnte sie über eine IPv6-Adresse aus dem bereit gestellten Subnetz angesprochen werden -
aber damit wären all die Nutzer ausgeschlossen, die nur über eine IPv4-Anbindung verfügen.
Eine weitere (individuelle) IPv4-Adresse (nur für [Stirling-PDF](#)) scheidet aus Ressourcengründen (Kosten und Verfügbarkeit) aus.
[Stirling-PDF](#) wird über Port 8080 bereit gestellt -
dieser ist jedoch aus manchen Netzwerken nicht zu erreichen, weil insbesondere Unternehmensnetzwerke häufig sehr restriktive Firewall-Regeln haben und häufig nur HTTPS via Port 443 erlauben.
Eine Port-Weiterleitung von Port 80 am Host auf Port 8080 zur VM mit [Stirling-PDF](#) scheidet aus, weil Port 80 am Host bereits anderweitig belegt ist.

Ziel ist es, die Anwendung [Stirling-PDF](#) per sicherem HTTPS über den Standard-Port (443) zur Verfügung zu stellen.

Revision #4

Created 11 April 2024 13:40:06 by Rene Schubert

Updated 12 April 2024 06:03:46 by Rene Schubert