

Reverse Proxy konfigurieren

Prinzipiell lässt sich Netbird hinter verschiedenen Reverse Proxys einsetzen. Es muss also kein eigener Server nur für Netbird eingerichtet werden.

Die offizielle Dokumentation empfiehlt den Reverse Proxy [Traefik](#) und bietet hierfür bereits eine angepasste Docker Compose Konfiguration an.

Aufgrund der Einfachheit, wird im folgenden die notwendige Konfiguration beschrieben, um Netbird hinter dem Reverse Proxy Traefik einzusetzen.

Zuerst sollte Netbird wie in [Server Installation](#) beschrieben eingerichtet werden.

Anschließend liegen im Ordner `infrastructure_files` 2 Docker Compose Dateien. In der Installationsanleitung wird die `docker-compose.yml.tpl` angepasst. Für die Traefik Variante gibt es eine extra Compose Konfiguration, welche `docker-compose.yml.tpl.traefik` heißt. Diese Datei wird einfach in `docker-compose.yml.tpl` umbenannt. Die andere Compose Datei kann bei dem Vorgang einfach überschrieben oder vorher gelöscht werden.

Nun ggf. noch alle anderen Konfigurationsparameter wie beschrieben anpassen und danach das Konfigurationsskript ausführen, was alles in der [Server Installation](#) beschrieben ist.

Bevor die Konfiguration unter *artifacts* direkt gestartet wird, wie in der anderen Anleitung beschrieben, ist ggf. vorher noch die Netzwerke der hinter Traefik zu veröffentlichen Containers anzupassen. Hierfür wird die Docker Compose Konfiguration wie folgt angepasst (einige Bereiche sind ausgelassen, um den Fokus auf die zu ändernden Bereiche zu setzen).

```
version: "3"
services:
  #UI dashboard
  dashboard:
    # [...]
    networks:
      - traefik
  # Signal
  signal:
    # [...]
    networks:
      - traefik
  # Management
```

```
management:
  # [...]
  networks:
    - traefik
# [...]
networks:
  traefik:
    external: true
```

Der Name des Netzwerks muss ggf. angepasst werden und sollte der selbe sein, wie der von Traefik.

Nun kann die Konfiguration einfach gestartet werden.

Da der letzte Container, in der Konfiguration oben nicht gezeigt, keinem Netzwerk angehört, sondern direkt über das Netzwerk des Hosts läuft, müssen hierfür 2 Firewall Regeln erstellt werden. Sofern die Uncomplicated Firewall (ufw) eingesetzt wird, können einfach die beiden folgenden Befehle ausgeführt werden.

```
sudo ufw allow from any to any port 3478
sudo ufw allow 49152:65535/udp
```

Version #3

Erstellt: 2024-03-25 18:46:43 CET von Marcel

Zuletzt aktualisiert: 2024-03-25 19:20:19 CET von Marcel