

HTTPS Reverse Proxy mit Nginx konfigurieren

Einleitung

Sobald wir **Lokal Webdienste** erstellen, möchten wir diese vielleicht auch über ein **TLS Zertifikat** verschlüsseln. Dazu verwenden wir **selbst signierte Zertifikate** und einen **Nginx Webserver**. Dadurch ist es möglich, dass wir unsere **Web-Dienste** über **HTTPS** erreichbar machen können.

Wie wir **TLS Zertifikate** erstellen können, wird [hier](#) genauer erklärt.

Nginx installieren

Im ersten Schritt müssen wir auf unserem **Debian Server** das Paket **Nginx** installieren. Dazu verwenden wir folgenden Befehl:

```
apt update && apt upgrade -y && apt install nginx -y
```

Nginx Konfiguration anpassen

Jetzt erstellen wir die **Nginx Konfigurationsdatei** einmal neu. Im Anschluss öffnen wir die **Konfigurationsdatei** und fügen den nachstehenden Inhalt in die Datei ein.

```
rm /etc/nginx/sites-enabled/default
nano /etc/nginx/sites-enabled/default
```

```
server {
    listen 80;
    server_name host.name;
    return 301 https://die.domain$request_uri;
}

server {
    listen 443 ssl;
    server_name host.name;
    ssl_certificate /pfad/zum/zertifikat.csr;
    ssl_certificate_key /pfad/zum/zertifikat.key;
```

```
ssl_prefer_server_ciphers on;

location / {
    proxy_pass http://localhost:<port>;

    proxy_set_header    Host $host;
    proxy_set_header    X-Real-IP $remote_addr;
    proxy_set_header    X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header    X-Forwarded-Proto $scheme;
}
}
```

Sobald wir diesen Inhalt in die Datei eingefügt haben, brauchen wir jetzt nur noch einmal den **Nginx Dienst** neu zu starten.

```
systemctl restart nginx
```

Sobald der Dienst neu gestartet ist, überprüfen wir, ob der Dienst ordnungsgemäß gestartet ist. Dies können wir mit dem nachstehenden Befehl überprüfen.

```
systemctl status nginx
```

[nginx_reverse_proxy_1.JPG](#)

Revision #3

Created 27 October 2022 07:49:44 by Phillip U.

Updated 16 May 2024 14:12:57 by Phillip U.