

# Kỹ thuật sử dụng chứng chỉ SSL với Traefik Proxy, Clouflare và Let's Encrypt

Traefik là một **HTTP reverse proxy** hiện đại, cũng là load balancer để làm cho việc deploy hệ thống microservice được trở lên dễ dàng hơn. Tích hợp rất nhiều các thành phần infrastructure như **Docker, Swarm mode, Kubernetes, Marathon, Consul, Etcd, Rancher, Amazon ECS...** Và tính **tự động** là điểm quan trọng nhất trong các config với traefik. Alt text not found or type unknown

Cách tính năng

Mình liệt kê một số tính năng hiện tại mình đang dùng với traefik.

- Traefik tự động cập nhật cấu hình mà không phải restart
- Hỗ trợ nhiều giải thuật load balancing
- Free HTTPS cho microservice với Let's Encrypt Websocket, HTTP/2, GRPC
- Chống quá tải với Circuit breakers
- Lưu access logs (JSON, CLF)
- Nhanh
- Có Rest API cho bạn sử dụng để update các config.

## Chuẩn bị

Chuẩn bị server Ubuntu 20.04 LTS

- 2 CPU
- 2 GB RAM
- 20 GB HDD

Cài đặt **docker, docker-compose** [Scripts](#)

## Cài đặt

## Tạo thư mục cài đặt và các file cần thiết

```
mkdir /home/ubuntu/docker/traefik
cd /home/ubuntu/docker/traefik
touch acme.json
touch config.yml
```

## Tạo file cấu hình `traefik`

```
nano traefik.yml
```

```
api:
  dashboard: true
  debug: true
entryPoints:
  http:
    address: ":80"
    http:
      redirections:
        entryPoint:
          to: https
          scheme: https
  https:
    address: ":443"
serversTransport:
  insecureSkipVerify: true
providers:
  docker:
    endpoint: "unix:///var/run/docker.sock"
    exposedByDefault: false
  file:
    filename: /config.yml
certificatesResolvers:
  cloudflare:
    acme:
      email: your@email.com #add your email
      storage: acme.json
      dnsChallenge:
        provider: cloudflare
        #disablePropagationCheck: true # uncomment this if you have issues pulling certificates through
```

cloudflare, By setting this flag to true disables the need to wait for the propagation of the TXT record to all authoritative name servers.

resolvers:

- "1.1.1.1:53"
- "1.0.0.1:53"

Tạo file `docker-compose`

nano docker-compose.yml

```
version: '3.5'

services:
  traefik:
    image: traefik:latest
    container_name: traefik
    restart: unless-stopped
    security_opt:
      - no-new-privileges:true
    networks:
      proxy:
    ports:
      - 80:80
      - 443:443
    environment:
      - CF_API_EMAIL=your@email.com
      - CF_DNS_API_TOKEN=your-api-key
      # - CF_API_KEY=YOU_API_KEY
    volumes:
      - /etc/localtime:/etc/localtime:ro
      - /var/run/docker.sock:/var/run/docker.sock:ro
      - /home/ubuntu/docker/traefik/traefik.yml:/traefik.yml:ro
      - /home/ubuntu/docker/traefik/acme.json:/acme.json
      - /home/ubuntu/docker/traefik/config.yml:/config.yml:ro
      - /home/ubuntu/docker/traefik/logs:/var/log/traefik
    labels:
      - "traefik.enable=true"
      - "traefik.http.routers.traefik.entrypoints=http"
      - "traefik.http.routers.traefik.rule=Host(`traefik-dashboard.yourdomain.com`)"
      - "traefik.http.middlewares.traefik-auth.basicauth.users=YOUR_USERNAME_PASSWORD"
```

```
- "traefik.http.middlewares.traefik-https-redirect.redirectscheme.scheme=https"
- "traefik.http.middlewares.sslheader.headers.customrequestheaders.X-Forwarded-Proto=https"
- "traefik.http.routers.traefik.middlewares=traefik-https-redirect"
- "traefik.http.routers.traefik-secure.entrypoints=https"
- "traefik.http.routers.traefik-secure.rule=Host(`traefik-dashboard.yourdomain.com`)"
- "traefik.http.routers.traefik-secure.middlewares=traefik-auth"
- "traefik.http.routers.traefik-secure.tls=true"
- "traefik.http.routers.traefik-secure.tls.certresolver=cloudflare"
- "traefik.http.routers.traefik-secure.tls.domains[0].main=yourdomain.com"
- "traefik.http.routers.traefik-secure.tls.domains[0].sans=*.yourdomain.com"
- "traefik.http.routers.traefik-secure.service=api@internal"
```

networks:

proxy:

name: proxy

external: true

Phần này chú ý:

- **CF\_DNS\_API\_TOKEN=your-api-key** => Tạo token trên Cloudflare và điền ở đây
- **traefik.http.middlewares.traefik-auth.basicauth.users=YOUR\_USERNAME\_PASSWORD** => Tạo user để bảo mật khi vào domain

Cài đặt `htpasswd` nếu chưa có

```
apt install apache2-utils
```

Chạy lệnh sau để tạo `YOUR_USERNAME_PASSWORD`

```
echo $(htpasswd -nb "admin" "admin") | sed -e s/\\$/\\$\\$/g
```

Cài traefik

```
docker-compose up -d
```

Login [https://IP\\_SERVER\\_TRAEFIK](https://IP_SERVER_TRAEFIK) và xem kết quả

# Tham khảo

- <https://traefik.io>

# Mời cà phê

Nếu cảm thấy blog mang đến những thông tin hữu ích cho công việc, cuộc sống, đam mê của bạn, đừng ngại ủng hộ một ly cà phê để mình có thêm động lực chia sẻ thêm nhiều kinh nghiệm, kiến thức nhé.

Bạn có thể ủng hộ mình qua:

## Ví MoMo



[Ví MoMo](#)

## Paypal

[Hỗ trợ qua Paypal](#)

Cám ơn mọi người!

---

Phiên bản #2

Được tạo 16 tháng 3 2024 07:47:10 bởi Kiên Lê

Được cập nhật 16 tháng 3 2024 08:11:20 bởi Kiên Lê