Traefik

From certbot to traefik

1. Get public IP address of server

```
curl ifconfig.me
8.8.8.8
```

2. Setup a DNS entry that points to that server

2.1. Check DNS name

```
dig @8.8.8.8 test.javilegido.com +short
8.8.8.8
```

3. Make sure ports TCP 80 and 443 are open

WARNING: if behind LAN router remember to setup NAT

4. Generate certificate

```
mkdir etc_letsencrypt
docker run -it \
  --rm \
  --name certbot \
  -v `pwd`/etc_letsencrypt:/etc/letsencrypt \
  -p 80:80 \
  certbot/certbot certonly
```

```
1
javi@example.com
Y
N
test.javilegido.com
```

```
Requesting a certificate for test.javilegido.com
Successfully received certificate.
Certificate is saved at:
/etc/letsencrypt/live/test.javilegido.com/fullchain.pem
Key is saved at:
/etc/letsencrypt/live/test.javilegido.com/privkey.pem
This certificate expires on 2022-08-24.
These files will be updated when the certificate renews.

NEXT STEPS:
- The certificate will need to be renewed before it expires. Certbot can
automatically renew the certificate in the background, but you may need to
take steps to enable that functionality. See
https://certbot.org/renewal-setup for instructions.
```

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
 * Donating to EFF:                    https://eff.org/donate-le
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
```

5.

```
tree
```

```
etc_letsencrypt/
├── accounts
│   └── acme-v02.api.letsencrypt.org
│       └── directory
│           └── 77fcea9a20707993ed3e5d65f5960a8f
│               ├── meta.json
│               ├── private_key.json
│               └── regr.json
├── archive
│   └── test.javilegido.com
│       ├── cert1.pem
│       ├── chain1.pem
│       ├── fullchain1.pem
│       └── privkey1.pem
├── csr
│   └── 0000_csr-certbot.pem
├── keys
│   └── 0000_key-certbot.pem
├── live
│   ├── README
│   └── test.javilegido.com
│       ├── cert.pem -> ../../archive/test.javilegido.com/cert1.pem
│       ├── chain.pem -> ../../archive/test.javilegido.com/chain1.pem
│       ├── fullchain.pem ->
../../archive/test.javilegido.com/fullchain1.pem
│       ├── privkey.pem -> ../../archive/test.javilegido.com/privkey1.pem
│       └── README
├── renewal
│   └── test.javilegido.com.conf
└── renewal-hooks
    ├── deploy
    ├── post
    └── pre

    certbot
```

```
fullchain.pem   =>    certificate
privkey.pem =>    key
```

```
chain.pem   =>    CA public certificate
```

```
acme.json
```

```
    "Certificates": [
      {
        "domain": {
          "main": "ranura.d.kedu.coop"
        },
        "certificate": "CONTENT_OF_fullchain.pem",
        "key": "CONTENT_OF_privkey.pem",
        "Store": "default"
      },
```

6. Deploy traefik with one example

https://doc.traefik.io/traefik/user-guides/docker-compose/acme-tls/

6.1.

```
vim docker-compose.yml
```

Adjust:

```
--certificatesresolvers.myresolver.acme.email
traefik.http.routers.whoami.rule
```

NOTE: the challenge is listening in port 8080, so don't change it

```
version: "3.3"

services:

  traefik:
    image: "traefik:v2.7"
    container_name: "traefik"
    command:
      - "--log.level=DEBUG"
      - "--api.insecure=true"
      - "--providers.docker=true"
      - "--providers.docker.exposedbydefault=false"
      - "--entrypoints.websecure.address=:443"
      - "--certificatesresolvers.myresolver.acme.tlschallenge=true"
      #- "--
certificatesresolvers.myresolver.acme.caserver=https://acme-staging-v02.api.
letsencrypt.org/directory"
      - "--certificatesresolvers.myresolver.acme.email=javi@example.com"
      - "--
certificatesresolvers.myresolver.acme.storage=/letsencrypt/acme.json"
    ports:
      - "443:443"
```

```
      - "8080:8080"
    volumes:
      - "./letsencrypt:/letsencrypt"
      - "/var/run/docker.sock:/var/run/docker.sock:ro"

  whoami:
    image: "traefik/whoami"
    container_name: "simple-service"
    labels:
      - "traefik.enable=true"
      - "traefik.http.routers.whoami.rule=Host(`test.javilegido.com`)"
      - "traefik.http.routers.whoami.entrypoints=websecure"
      - "traefik.http.routers.whoami.tls.certresolver=myresolver"
```

6.2. Start

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

```
docker logs -f traefik
```

```
...
time="2022-06-03T18:15:00Z" level=debug msg="Certificates obtained for
domains [test.javilegido.com]" providerName=myresolver.acme
routerName=whoami@docker rule="Host(`test.javilegido.com`)" ACME
CA="https://acme-v02.api.letsencrypt.org/directory"
time="2022-06-03T18:15:00Z" level=debug msg="Configuration received:
{\"http\":{},\"tcp\":{},\"udp\":{},\"tls\":{}}" providerName=myresolver.acme
...
```

6.3.

(From another host)

```
wget https://test.javilegido.com
```

6.4. Stop

```
sudo docker-compose down
```

6.5. Backup

```
sudo cp letsencrypt/acme.json ./acme.json.bak
```

7. Replace certs

7.1. Transform certbot certificates in strings

```
sudo chown -R `whoami`:`whoami` etc_letsencrypt*
```

```
_IN=etc_letsencrypt/live/test.javilegido.com/fullchain.pem
```

```
_OUT=traefik_certificate
cat $_IN | base64 | tr '\n' ' ' | sed --expression='s/\ //g' > $_OUT
```

```
_IN=etc_letsencrypt/live/test.javilegido.com/privkey.pem
_OUT=traefik_key
cat $_IN | base64 | tr '\n' ' ' | sed --expression='s/\ //g' > $_OUT
```

7.2. Edit:

```
sudo vim letsencrypt/acme.json
```

And replace:

```
certificate:    Content of file 'traefik_certificate'
key:        Content of file 'traefik_key'
```

WARNING: both files content differ, “letsencrypt/acme.json” and “acme.json.bak”

8. Test

8.1. Take MD5 of acme.json

```
sudo md5sum letsencrypt/acme.json
```

```
ec151c804d1776d898b62b1b30691aeb  letsencrypt/acme.json
```

8.2. Make file “acme.json” readonly

```
vim docker-compose.yml
```

And leave change only below line:

```
      #- "./letsencrypt:/letsencrypt"
      - "./letsencrypt:/letsencrypt:ro"
```

8.3. Recreate

```
sudo docker-compose up -d --force-recreate
```

8.4. Check MD5 of the file:

```
sudo md5sum letsencrypt/acme.json
```

```
ec151c804d1776d898b62b1b30691aeb  letsencrypt/acme.json
```

Should be the same than step 8.1.

8.5. Test

```
wget https://test.javilegido.com
```