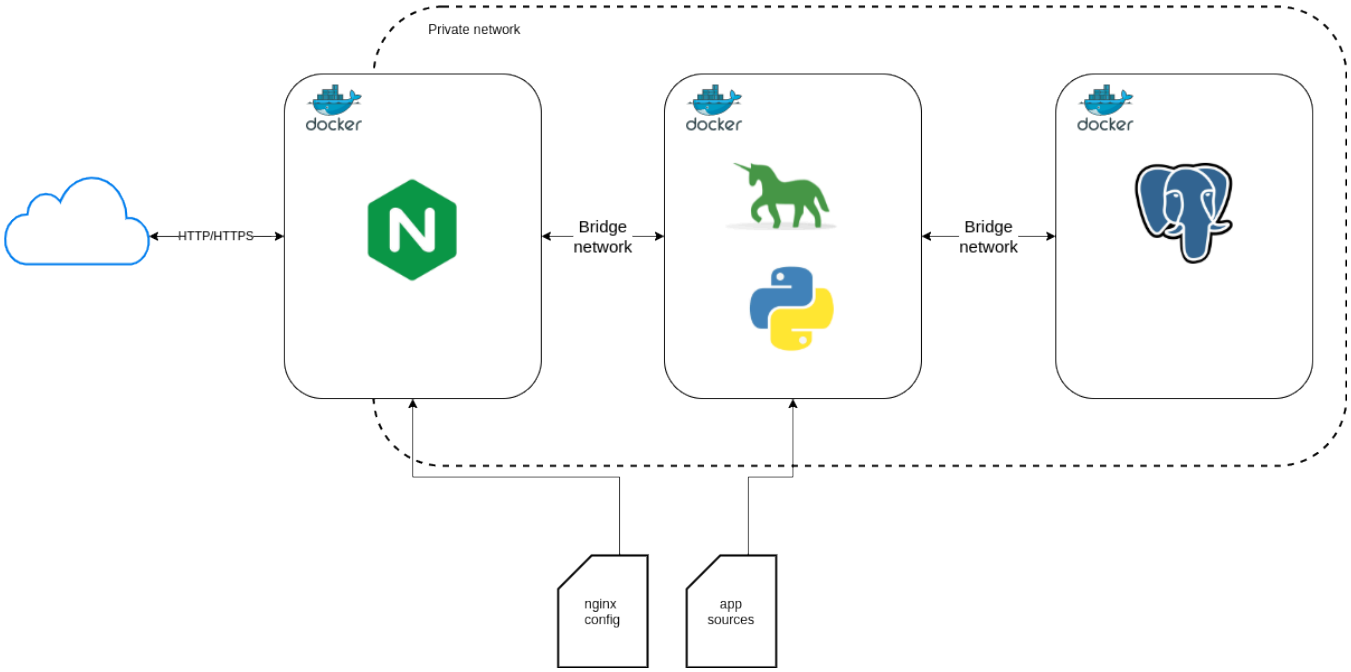
Docker, SSL and other

NGINX and Docker



Мы можем запустить контейнер для nginx, контейнер для нашего приложения и контейнер для БД, они будут в изолированой сети, и наружу будет смотреть только nginx на порту `80`.

Пример конфигурации nginx

```
upstream backend {
    server web:8000;
}

server {
    listen 80;

    server_name localhost;

    location / {
        proxy_pass http://backend;
        proxy_redirect     off;

        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;
    }
}
```

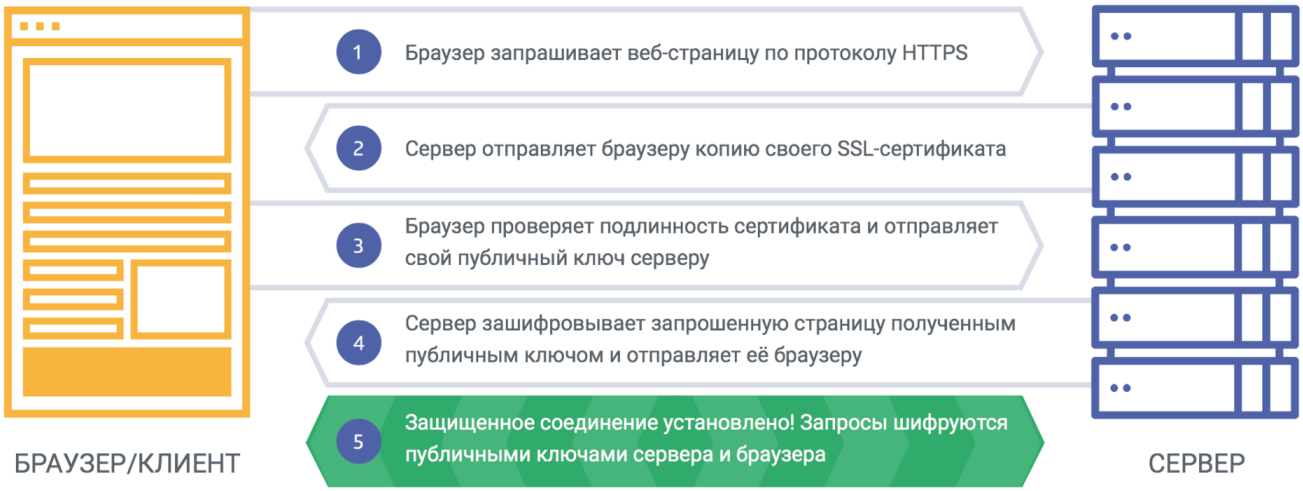
Пример compose файла

```
version: "3.6"

services:
  web:
    build: ./app
    expose:
      - 8000

  nginx:
    build: nginx
    depends_on:
      - web
    ports:
      - 80:80
    volumes:
      - ./nginx:/etc/nginx/conf.d
```

HTTPS

HTTPS (аббр. от англ. HyperText Transfer Protocol Secure) — расширение протокола HTTP для поддержки шифрования в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографических протоколов TLS или устаревшего в 2015 году SSL. В отличие от HTTP с TCP-портом `80`, для HTTPS по умолчанию используется TCP-порт `443`.

HTTPS не является отдельным протоколом. Это обычный HTTP, работающий через шифрованные транспортные механизмы `SSL` и `TLS`. Он обеспечивает защиту от атак, основанных на прослушивании сетевого соединения — от снифферских атак и атак типа man-in-the-middle, при условии, что будут использоваться шифрующие средства и сертификат сервера проверен и ему доверяют.



Полезные ссылки

- "dockerizing flask"
- "Gunicorn with Nginx. WSGI"
- "Знакомство с SSL/TLS"
- "Как защитить сайт с помощью HTTPS"
- "Self signed certificate"
- "Nginx and Certbot" Medium

- "Nginx and Certbot" DigitalOcean