

HTTPS with Nginx

The Problem

- We want to use HTTPS
- Prefer not to modify your app code
 - Makes our code more modular and portable
 - Your HTTPS setup can change without changing your app
- Use a reverse proxy

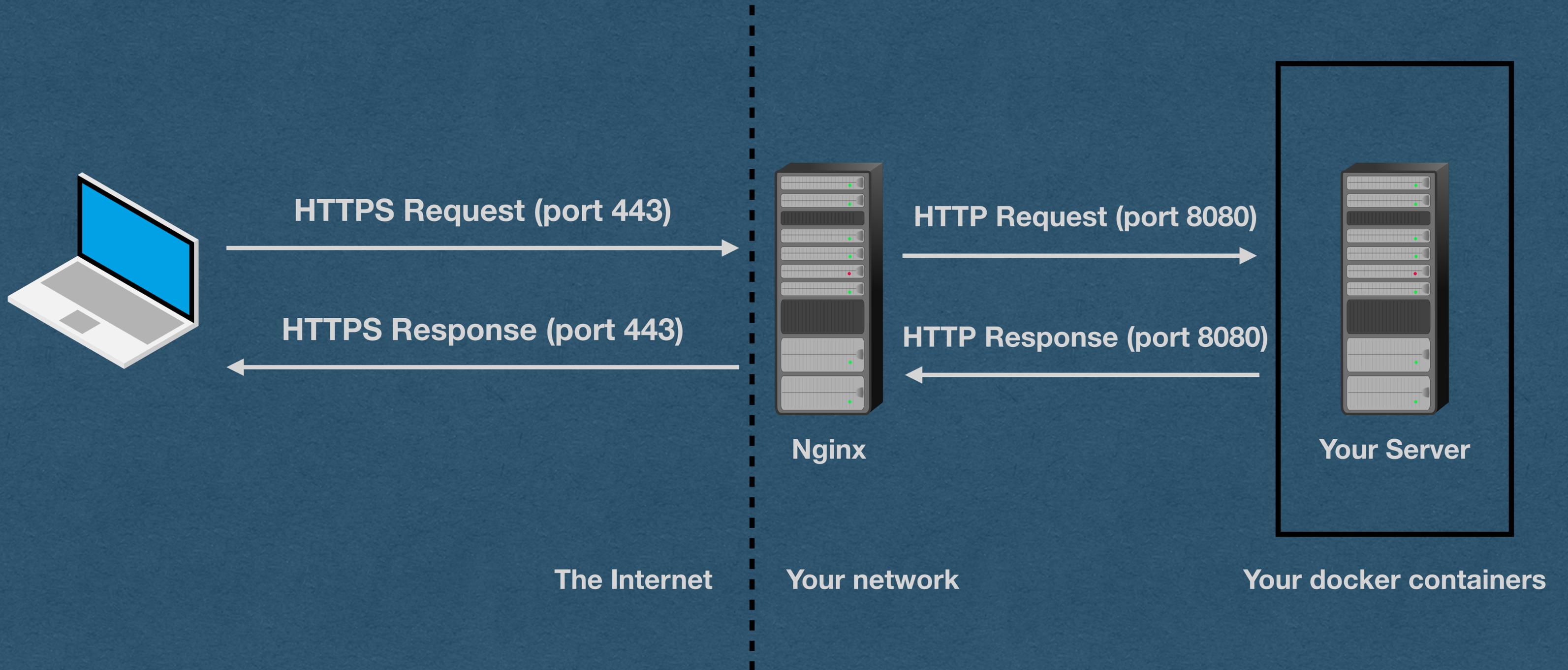
Nginx

- Nginx has many uses and is very powerful software
- We'll use it a reverse proxy with TLS

Nginx Strategy

- Use Nginx to listen for HTTPS requests
 - Nginx needs a cert and private key
- Nginx will decrypt requests and forward them to your server as HTTP requests
 - These unencrypted requests are sent over a local network and never touch the Internet
- Your server sends HTTP responses to Nginx
 - Nginx encrypts and sends the HTTPS response over the Internet
- If Nginx gets an HTTP request (port 80) redirect the user to HTTPS (port 443)

Nginx Strategy



Nginx Strategy

- We'll need:
 - A signed cert and private key
 - Add the cert and private key to the nginx config
 - Run Nginx and listen on ports 80 and 443
 - Redirect port 80 to 443
 - Reconfigure WebSockets to work with the new setup
 - Forward requests to your server

Nginx Strategy

- How we'll do it:
 - Buy a domain name
 - Install nginx
 - Setup nginx as a reverse proxy for your server
 - Tell Certbot to do the rest

Nginx Strategy

Demo