# SSL certificates and HTTPS – Ubuntu 18.04 servers

## What is SSL?

* Secure socket Layer is a cryptographic protocol
* Provides a secure channel between two machines on the internet
  + Web browser and web server
* It is responsible for
  + Encryption of your data
  + Authentication – to make sure you are connected to the correct server
  + Data integrity – ensures the data that is requested or submitted is what is actually delivered

What is an SSL certificate?

* Small data file that binds a cryptographic key to an organisations details
* Activates padlock on the web browser

Obtaining an SSL certificate:

Step 1

* Install Certbot on your server
  + Certbot is an easy to use client that fetches a certificate from Let Encrypt (an open Certificate authority)
* First we need to add the repository
  + sudo add-apt-repository ppa:certbot/certbot
* Next we need to install certbots ngix package

Step 2

* Certbot needs to be able to find the correct server block in your Nginx configuration for it to be able to automatically configure SSL. Specifically, it does this by looking for a server\_namedirective that matches the domain you request a certificate for.
  + If one is already set up then great if not update the file here
  + sudo nano /etc/nginx/sites-available/example.com
  + To this
  + server\_name example.com [www.example.com](http://www.example.com);
  + check for errors - sudo nginx -t
  + restart ngix - sudo systemctl reload nginx

Step 3

* We need to allow HTTPS through the firewall
* Check the current settings
  + sudo ufw status
* Allow HTTPS
  + sudo ufw allow 'Nginx Full'
* Delete HTTP
  + sudo ufw delete allow 'Nginx HTTP'

Step 4 obtaining SSL certificate

* we are Using the ngix plugin which will take care of reconfiguring ngix and reloading the config whenever necessary
  + sudo certbot --nginx -d example.com -d www.example.com

A screenshot of a newspaper

Description automatically generated

A screenshot of a computer screen

Description automatically generated

Step 5

* Let’s encrypt certificates are only valid for 90 days so we should make sure our certificates are auto renewed every 90 days
* To test this was can do a dry run on Certbot
  + sudo certbot renew --dry-run