Let's Encrypt on Ubuntu 14.04

Prerequisites

In order to complete this guide, you will need:

An Ubuntu 14.04 server with a non-root sudo user, which you can set up by following our Initial Server Setup guide

The Apache web server installed with one or more domain names properly configured

When you are ready to move on, log into your server using your sudo account.

In this lab we will use `netflow.apnictraining.net` as demo domain.

Step 1 — Install the Server Dependencies

The first thing we need to do is to update the package manager cache with:

```
sudo apt-get update
```

We will need git in order to download the Let's Encrypt client. To install git, run:

```
sudo apt-get install git
```

Step 2 — Download the Let's Encrypt Client

```
sudo git clone https://github.com/letsencrypt/letsencrypt /opt/letsencrypt
```

This will create a local copy of the official Let's Encrypt repository under `/opt/letsencrypt`

Step 3 — Set Up the SSL Certificate

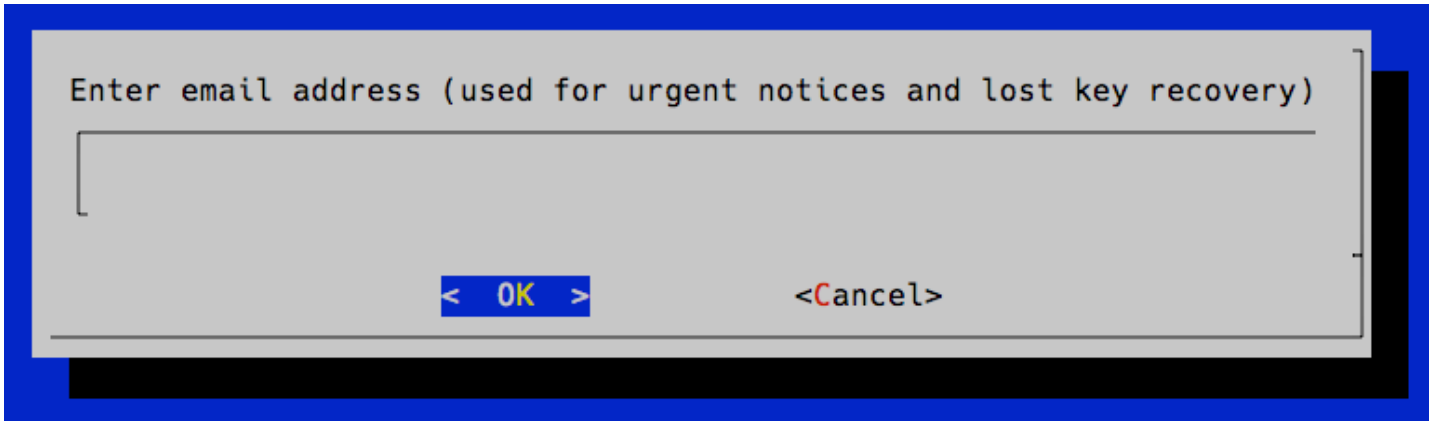
Access the letsencrypt directory:

```
cd /opt/letsencrypt
```

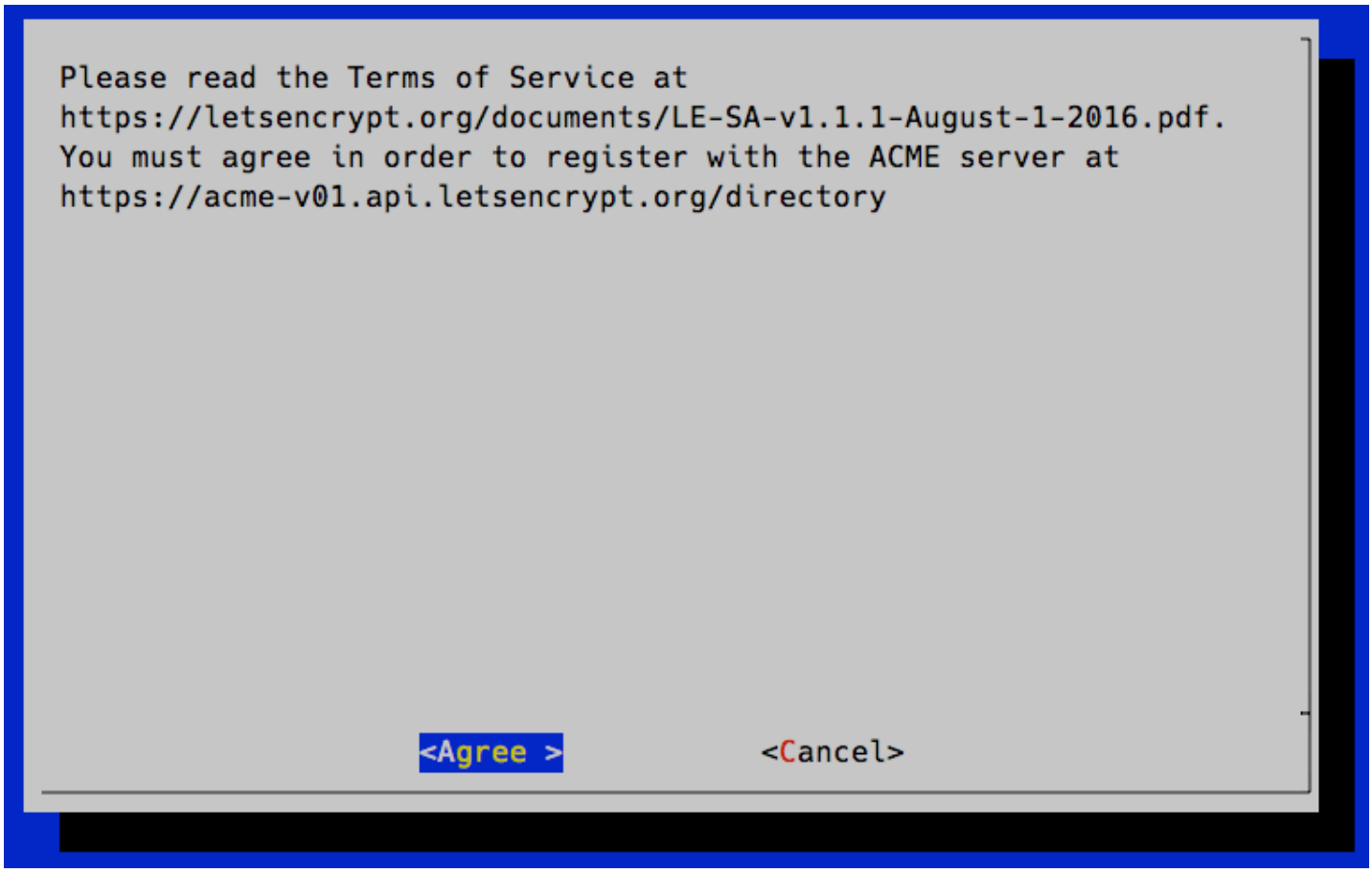
To execute the interactive installation and obtain a certificate that covers only a single domain, run the `letsencrypt-auto` command with:

```
./letsencrypt-auto --apache -d netflow.apnictraining.net
```

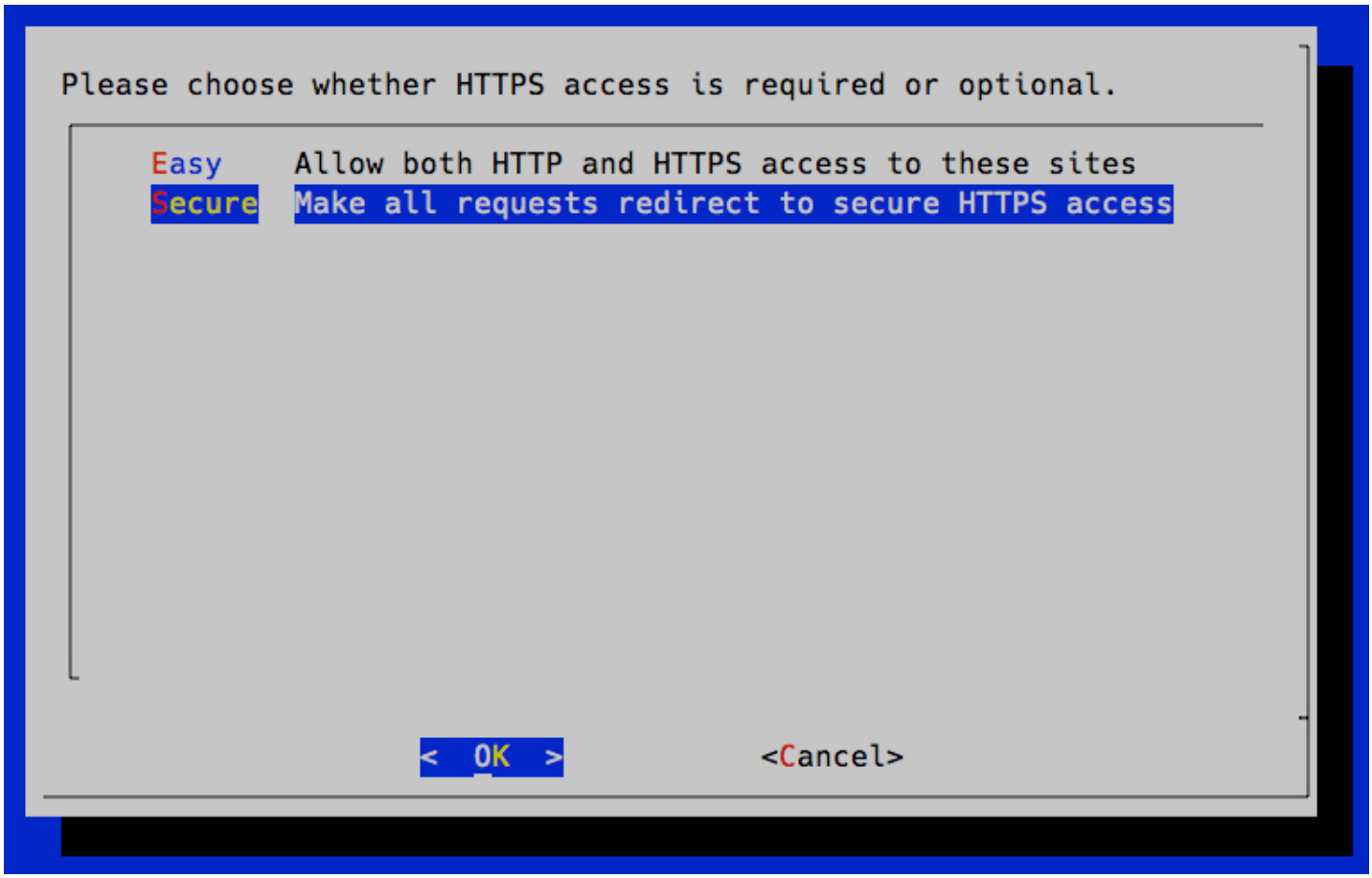
Put your email address for lost key recovery



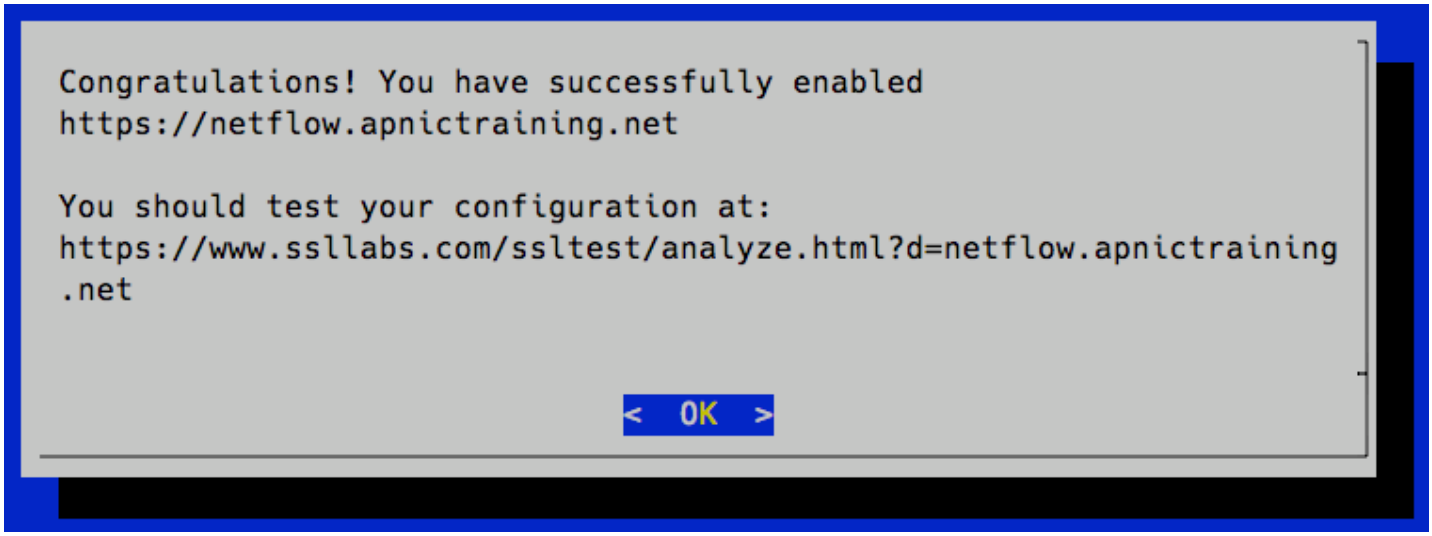
Choose `Agree`



Now you will get two options, one for easy installation where both `HTTP` and `HTTPS` will be allowed. For Secure only `HTTPS` will be allowed.



After successful installation; you will get following notification.



When the installation is finished, you should be able to find the generated certificate files at /etc/letsencrypt/live. You can verify the status of your SSL certificate with the following link (don't forget to replace example.com with your base domain):

```
https://www.ssllabs.com/ssltest/analyze.html?d=netflow.apnictraining.net&latest
```

Step 4 — Set Up Auto Renewal

Let’s Encrypt certificates are valid for 90 days, but it’s recommended that you renew the certificates every 60 days to allow a margin of error. The Let's Encrypt client has a renew command that automatically checks the currently installed certificates and tries to renew them if they are less than 30 days away from the expiration date.

To trigger the renewal process for all installed domains, you should run:

```
./letsencrypt-auto renew
```

Let's edit the crontab to create a new job that will run the renewal command every week. To edit the crontab for the root user, run:

```
sudo crontab -e
```

Include the following content, all in one line:

```
30 2 * * 1 /opt/letsencrypt/letsencrypt-auto renew >> /var/log/le-renew.log
```

Save and exit. This will create a new cron job that will execute the `letsencrypt-auto` renew command every Monday at 2:30 am. The output produced by the command will be piped to a log file located at `/var/log/le-renewal.log` .