การติดตั้ง Apache24 ให้รองรับ SSL (HTTPS) on FreeBSD 10.2

Secure Sockets Layer (SSL) คือ โพรโทคอลความปลอดภัย ที่ถูกใช้เป็นมาตรฐาน ในการเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ในปัจจุบันเทคโนโลยี SSL ได้ถูกทำการติดตั้งลงบนบราวเซอร์ อาทิ Internet Explorer, Netscape และอื่น ๆ มากมายอยู่เรียบร้อยแล้ว

โพรโทคอล SSL จะใช้ Digital Certificate ในการสร้างท่อสื่อสารที่มีความปลอดภัยสูง สำหรับตรวจสอบ และ เข้ารหัสลับการติดต่อสื่อสารระหว่าง client และ server

1. ขั้นตอนการติดตั้ง

ก่อนทำการติดตั้ง HTTPS บน FreeBSD นั้นจะต้องติดตั้งโปรแกรม Apache24 ให้พร้อมใช้งาน โดยสร้างเว็บเซิร์ฟเวอร์เสมือนแบบ userdir หรือแบบ IP-based (*เว็บเซิร์ฟเวอร์เครื่องเดียวหลายไอพีแอดเดรสและกำหนดให้ 1 ไอพีแอดเดรสต่อ 1 เว็บไซต์*) ก็ได้ ขั้นตอนการติดตั้งมีดังนี้

1.1 เริ่มสร้างคีย์ Key สำหรับ SSL

```
# cd   /root
# pwd
   /root
# mkdir   ssl
# cd   ssl
# pwd
   /root/ssl
# openssl   genrsa   -des3   -out   server.key   1024
```

แล้วพิมพ์ password key ที่ต้องการ 2 ครั้ง (ให้ตรงกัน) ก็จะได้ไฟล์ server.key

```
Generating RSA private key, 1024 bit long modulus
.....................................................................++++++
.....++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
```

กรอกรหัสลับ 2 ครั้ง (ให้ตรงกัน) Enter

```
# cat   server.key
```

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,88C7881E40404824
n7Y5+GPs4Y1sqcz9xbagWrQVzzlfkzd744e42RbnVxYxXg0xx6HLTXIacjg/ff0h
Yx0KQaYl3DcZ6juBPPF2Jd8vvwFQWQDVIlwzSWVmm6QGV8qCAi4RUa8i3kyWYOJ0
```

Ybx0K1Wz3fsNpJ/Z+SBR4SoaNkYqLMrKJQUmw2lYGsc96i2WRG/if2Culpm22QLi
rWtGxzMzWL8tWQnHOAdLb/lG9fT7zAv6Yet1khWsJkUas7lsx90Tkfxg3afyKG1u
JXs0hGw312NedBLCD3zaKLAh31oKHRQMdwBbLzbBeyI3kAt8kwRFhADys+KAAgQb
M7ogZ4f0FDFVgzXn1E2inRY0ldgmYdIelQzEBVxHaLpiITVeU5t+DvAmQ/ewYJuG
DOGl4TTO+9ULwUpaugg5obtiy71gmEzNzqsaSke3942aYzNE0JncC3f0u5+KDCQ3
pw/Cgz56/jedaI2RJf31DI2QTpU1+ll/9hIzvMFs8d+kBLvisNZAGvHiVRnUg+ez
rX3GDpVeQPxHL+I3rS5VCeAJzmoDftA6YBgfcH+N3tX4RWTLI5H/1QnNhOq7cj9S
AlC0N/LhdG2aMdt7QY4zIiViLyMjbj7zjWVVITvMU5Ll+GVe9cbNLp524o/Lbqqn
7OXWIeCQTZ+ZcvYfpsNghO5zLcC1910pA785g/GBAq2eOwHn0CcxiRJLzjK7OV8Z
zIFA0NRUl2+7Niu8xsLS5EsVVeyiFHk/LgGTApsY8oFyOve5TrlgwEqadbACGPfj
SMMa6k/4wqN9aHqQzvgXyGMeifcT83CYJV7ZMletOObrh8+ZSYZFtA==
-----END RSA PRIVATE KEY-----

****** การสร้างไฟล์ server.key ถูกต้อง**

คำสั่งนี้ใช้สำหรับสร้างไฟล์ server.csr โดยนำคีย์จากไฟล์ server.key มาประมวลผลร่วม

 # openssl req -new -key server.key -out server.csr

กรอกรหัสลับให้ตรงกันแล้ว Enter

Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:**TH**
State or Province Name (full name) [Some-State]: **Roi et**
Locality Name (eg, city) []:**selaphum**
Organization Name (eg, company) [Internet Widgits Pty Ltd]:**RERU**
Organizational Unit Name (eg, section) []:**ICT**
Common Name (e.g. server FQDN or YOUR name) []:**ict.reru.ac.th**
Email Address []:**kasam_com@hotmail.com**

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

กรอกรหัสลับให้ตรงกันแล้ว Enter

 # cat server.csr

-----BEGIN CERTIFICATE REQUEST-----
MIIB5DCCAU0CAQAwgY4xCzAJBgNVBAYTAlRIMRAwDgYDVQQIDAcgUm9pIGV0MREw
DwYDVQQHDAhzZWxhcGh1bTENMAsGA1UECgwEUkVSVTEMMAoGA1UECwwDSUNUMRcw
FQYDVQQDDA5pY3QucmVydS5hYy50aDEkMCIGCSqGSIb3DQEJARYVa2FzYW1fY29t

QGhvdG1haWwuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCujyd46syG
ZdmWqEcG3X3HL2PQ1VJD8KtMX1TXrDQLQPeGwxOFRFG+W3mzjqMRHV3v/UPqjl4o
AuZQQ7Ap+zzijF0CYEM0NdmIDxdVXE5brgBu0CeagsI9KBQcp3D4qFX9cKw31tl6
qEf2aLZbfZLtJcPcPOy/Sq93aafGLJ419QIDAQABoBUwEwYJKoZIhvcNAQkHMQYM
BDEyMzQwDQYJKoZIhvcNAQEFBQADgYEAPaL/9GANoy+8A+ii2ETCkf5pTxdWnGXW
1eoPjGkl6yMtWDlG8Z/tvQd067UD13TyoDEsdLr2wMSkiZVTh+jQUe/RGR0rJ4qD
h8Hsm2chtGIFx3U+XqKLKw9PAqjkW+s3nVfvIgfXOkQddWJWVLNiRKeErxONMQzT
Zi0UMga/foY=
-----END CERTIFICATE REQUEST-----

***** การสร้างไฟล์ server.csr ถูกต้อง

จะได้ไฟล์ server.crt

Signature ok

 # openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

Signature ok
subject=/C=TH/ST= Roi
et/L=selaphum/O=RERU/OU=ICT/CN=ict.reru.ac.th/emailAddress=kasam_com@hotma
il.com
Getting Private key
Enter pass phrase for server.key:

กรอกรหัสลับให้ตรงกันแล้ว Enter

 # cat server.crt

-----BEGIN CERTIFICATE-----
MIIClTCCAf4CCQD7u0HeuaNlEDANBgkqhkiG9w0BAQUFADCBjjELMAkGA1UEBhMC
VEgxEDAOBgNVBAgMByBSb2kgZXQxETAPBgNVBAcMCHNlbGFwaHVtMQ0wCwYDVQQK
DARSRVJVMQwwCgYDVQQLDANJQ1QxFzAVBgNVBAMMDmljdC5yZXJ1LmFjLnRoMSQw
IgYJKoZIhvcNAQkBFhVrYXNhbV9jb21AaG90bWFpbC5jb20wHhcNMTYwNDA2MTEx
NTQyWhcNMTcwNDA2MTExNTQyWjCBjjELMAkGA1UEBhMCVEgxEDAOBgNVBAgMByBS
b2kgZXQxETAPBgNVBAcMCHNlbGFwaHVtMQ0wCwYDVQQKDARSRVJVMQwwCgYDVQQL
DANJQ1QxFzAVBgNVBAMMDmljdC5yZXJ1LmFjLnRoMSQwIgYJKoZIhvcNAQkBFhVr
YXNhbV9jb21AaG90bWFpbC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
AK6PJ3jqzlZl2ZaoRwbdfccvY9DVUkPwq0xfVNesNAtA94bDE4VEUb5bebOOoxEd
Xe/9Q+qOXigC5lBDsCn7POKMXQJgQzQ12YgPF1VcTluuAG7QJ5qCwj0oFByncPio
Vf1wrDfW2XqoR/Zotlt9ku0lw9w87L9Kr3dpp8YsnjX1AgMBAAEwDQYJKoZIhvcN
AQEFBQADgYEAUFR9MdzyNTRo+qqaDhZSiy12dXsCiOL5FUpRhR9kYrZ6hTzyn3qB
1beRLQWaMVB0YRb100Bo8HTuFk3jpxd/T3dNo8hl53cMnL8q06DLrZhu59yD/3R6
YpuJr6CZMyAl/Ymawyqeiz5+/liOVMhHioifmYHyck0l0hhEVPyLFK8=
-----END CERTIFICATE-----

***** การสร้างไฟล์ server.crt ถูกต้อง

จะต้องมีรายชื่อไฟล์ครบ ทั้ง 3 ไฟล์ ถ้าไม่ครบให้ เริ่มต้นสร้างคีย์ใหม่

 # ls

server.crt server.csr server.key

1.2 คัดลอกคีย์ไปยังไดเรกทอรีของ Apache24

```
# cd /root/ssl
# cp *.* /usr/local/etc/apache24/.
# cd /usr/local/etc/apache24
# chmod 400 server.crt
# cp server.key server.key.org
# openssl rsa -in server.key.org -out server.key
  Enter pass phrase for server.key.org:
  writing RSA key
# chmod 400 server.key
# ls -l
```

กรอกรหัสลับให้ตรงกันแล้ว Enter

```
-r-------- 1 root wheel 956 Apr 6 18:30 server.crt
-rw-r--r-- 1 root wheel 733 Apr 6 18:30 server.csr
-r-------- 1 root wheel 887 Apr 6 18:39 server.key
-rw-r--r-- 1 root wheel 963 Apr 6 18:37 server.key.org
```

****** การเตรียมไฟล์คีย์ต่าง ๆ ถูกต้อง**

1.3 คอนฟิกโปรแกรม Apache24 ให้รู้จักคีย์

```
# ee /usr/local/etc/apache24/httpd.conf
```

ลบเครื่องหมาย # 3 บรรทัด

```
LoadModule ssl_module libexec/apache24/mod_ssl.so

LoadModule socache_shmcb_module libexec/apache24/mod_socache_shmcb.so

Include etc/apache24/extra/httpd-ssl.conf
```

1.4 แก้ไขไฟล์ /etc/rc.conf โดยเพิ่มข้อความดังนี้

```
Apache24_flags=”-DSSL”
```

1.5 รีสตาร์ทเซิร์ฟเวอร์

 # reboot

ทดลองเปิดเว็บเบราเซอร์ แล้วเรียก URL ดังนี้

https://10.3.210.x
https://10.3.210.x/~username // username ของนักศึกษา

1.6 การคอนฟิกเว็บเซิร์ฟเวอร์เสมือนแบบ IP-Based ให้รองรับ https

1) พิมพ์คำสั่ง ดังนี้

 # ee /usr/local/etc/apache24/extra/httpd-ssl.conf

จากนั้นพิมพ์ข้อมูลต่อท้ายไฟล์ตามที่เราต้องการ ดังนี้

```
<VirtualHost 10.3.210.254:443>
  ServerAdmin kasam_com@hotmail.com
  DocumentRoot /home/student/public_html
  SSLEngine on
  SSLCertificateFile "/usr/local/etc/apache24/server.crt"
  SSLCertificateKeyFile "/usr/local/etc/apache24/server.key"
</VirtualHost>

<VirtualHost 10.3.211.254:443>
  ServerAdmin kasam_com@hotmail.com
  DocumentRoot /home/cheawchan/public_html
  SSLEngine on
  SSLCertificateFile "/usr/local/etc/apache24/server.crt"
  SSLCertificateKeyFile "/usr/local/etc/apache24/server.key"
</VirtualHost>
```

2) reboot เซิร์ฟเวอร์เพื่อให้โปรแกรม Apache รับรู้การแก้ไขไฟล์คอนฟิก **หรือ** ใช้คำสั่งต่อไปนี้โดยไม่ต้องรีสตาร์ทเซิร์ฟเวอร์

```
# service apache24 restart
```

3) ทดลองใช้คอมพิวเตอร์ลูกข่าย เรียก ยูอาร์แอล **https:// 10.3.210.254** และยูอาร์แอล **https:// 10.3.210.253** ซึ่งถ้าการคอนฟิกถูกต้อง แต่ละไอพีแอดเดรส จะให้เว็บไซต์ที่แตกต่างกัน

<u>แบบฝึกหัด</u>

ให้นักศึกษาคอนฟิกเว็บเซิร์ฟเวอร์ให้เรียกใช้งานเว็บไซต์ไอพี หมายเลยที่ 3 แบบ https