Table Of Contents

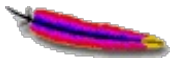
nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

CentOS / Redhat Apache mod_ssl Configuration

Posted by Vivek Gite <vivek@nixcraft.com>


[1]

The mod_ssl module provides strong cryptography for the Apache Web server via the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. How do I install and configure mod_ssl under CentOS / Fedora / Redhat Enterprise Linux?


[2]

mod_ssl is the SSL/TLS module for the Apache HTTP server. You can use self signed certificate or 3rd party SSL certificate. This module provides SSL v2/v3 and TLS v1 support for the Apache HTTP Server. It was contributed by Ralf S. Engeschall based on his mod_ssl project and originally derived from work by Ben Laurie. This module relies on OpenSSL to provide the cryptography engine.

Step #1: Install mod_ssl


[3]

Type the following command as the root user to install mod_ssl [4], enter:

```
# yum install mod ssl
```

Step #2: Create an SSL Certificate

Type the following commands:

```
# cd /etc/pki/tls/certs
# openssl genrsa -des3 -out apachekey.pem 2048
```

Sample outputs:

```
Generating RSA private key, 2048 bit long modulus
...................+++
.....................................+++
e is 65537 (0x10001)
Enter pass phrase for apachekey.pem:
Verifying - Enter pass phrase for apachekey.pem:
```

Note enter a strong, passphrase to protect the Apache web server key pair.

Generate a Certificate Signing Request (CSR)

Type the following command:

```
# openssl req -new -key apachekey.pem -out apachekey.csr
```

Sample outputs:

```
Enter pass phrase for apachekey.pem:
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) [GB]:IN
State or Province Name (full name) [Berkshire]:MH
Locality Name (eg, city) [Newbury]:Poona
Organization Name (eg, company) [My Company Ltd]:nixCraft LTD
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:www.nixcraft.com
```

```
Email Address []:vivek@nixcraft.com

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

You need to provide the information fill or hit [Enter] key to accept defaults, but the Common Name field is very important. You must match the fullyqualified domain name of your server exactly (e.g. www.nixcraft.com) or the certificate will not work. No need to enter the challenge password.

Create the Web Server Certificate

You must signed the CSR to create the web server certificate, enter (you can send it to your CA to sign the same). To sign httpserver.csr using your CA:

```
# openssl ca -in apachekey.csr -out apachecert.pem
```

Install SSL Certificate

Copy server key and certificates files /etc/pki/tls/http/, enter:

```
# cp apachecert.pem /etc/pki/tls/http/
# cp apachekey.pem /etc/pki/tls/http/
```

Edit /etc/httpd/conf.d/ssl.conf, enter:

```
# vi /etc/httpd/conf.d/ssl.conf
```

Listen to the the HTTPS port, enter:

```
Listen 10.10.29.68:443
```

Update it as follows to seed appropriately, enteR:

```
SSLRandomSeed startup file:/dev/urandom 1024
SSLRandomSeed connect file:/dev/urandom 1024
```

Update VirtualHost as follows:

```
<VirtualHost www.nixcraft.com:443>
    SSLEngine On
    SSLCertificateFile /etc/pki/tls/http/apachecert.pem
    SSLCertificateKeyFile /etc/pki/tls/http/apachekey.pem
    SSLProtocol All -SSLv2
    SSLCipherSuite HIGH:MEDIUM:!aNULL:+MD5
    DocumentRoot "/var/www/html/ssl"
    ServerName www.nixcraft.com:443
</VirtualHost>
```

Save and close the file. Make sure /var/www/html/ssl exits, enter:

```
# mkdir -p /var/www/html/ssl
```

Edit /etc/httpd/conf/httpd.conf, enter:

```
# vi /etc/httpd/conf/httpd.conf
```

Make sure SSL is used for /var/www/html/ssl and set other options for the same, enter:

```
<Directory /var/www/html/ssl>
```

```
        SSLRequireSSL
        SSLOptions +StrictRequire
        SSLRequire %{HTTP_HOST} eq "www.nixcraft.com"
        ErrorDocument 403 https://www.nixcraft.com/sslerror.html
</Directory>
```

Now, you can upload ssl specific php or html pages in /var/www/html/ssl directory and can access them by visiting https://www.nixcraft.com/ url. Do not forgot to restart Apache:

```
# service httpd restart
```

Firewall Configuration

Edit /etc/sysconfig/iptables [5]. Add the following lines, ensuring that they appear before the final DROP lines:

```
-A RH-Firewall-1-INPUT -m state --state NEW -p tcp --dport 443 -j ACCEPT
```

Save and close the file. Restart the [6] firewall:

```
# service iptables restart
```

References:

- Apache Module [7] mod_ssl.
- OpenSSL [8] project.
- Apache SSL/TLS Encryption [9].
- CentOS / Redhat Iptables Firewall [5] Configuration Tutorial
- Redhat [10] apache documentation.