CMX 10.5 SSL certificate installation procedure

Contents

Introduction

This article will give an example on how to get a free SSL certificate and the way to install it on CMX. The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- A domain name which can be resolved externally

- Basic linux skills

- Basic knowledge of PKI (Public Key Infrastracture)

Components Used

The information in this document is based on these software and hardware versions:

- CMX 10.5

Prepare and backup

Web certificate is located in the following folder:

```
[root@cmxtry ssl]# pwd
/opt/haproxy/ssl
```

Backup the old certificate and key:

```
[cmxadmin@cmxtry ssl]$cd /opt/haproxy/ssl/

[cmxadmin@cmxtry ssl]$su root
Password: (enter root password)

[root@cmxtry ssl]# mkdir ./oldcert
[root@cmxtry ssl]# mv host.* ./oldcert/

[root@cmxtry ssl]# ls ./oldcert/
host.key  host.pem
```

In case you are not very familiar with Linux, the above commands can be interpreted in the following way:

```
[cmxadmin@cmxtry ssl]$cd /opt/haproxy/ssl/

[cmxadmin@cmxtry ssl]$su root
Password: (enter root password)

[root@cmxtry ssl]# mkdir ./oldcert
[root@cmxtry ssl]# mv host.* ./oldcert/

[root@cmxtry ssl]# ls ./oldcert/
host.key  host.pem
```

Configure

Generate a private key:

```
[cmxadmin@cmxtry ssl]$cd /opt/haproxy/ssl/

[cmxadmin@cmxtry ssl]$su root
Password: (enter root password)

[root@cmxtry ssl]# mkdir ./oldcert
[root@cmxtry ssl]# mv host.* ./oldcert/

[root@cmxtry ssl]# ls ./oldcert/
host.key  host.pem


[root@cmxtry ssl]# openssl genrsa -out cmxtry.com.key 2048
Generating RSA private key, 2048 bit long modulus
.............
.............
e is 65537 (0x10001)

[root@cmxtry ssl]# ls
cmxtry.com.key  oldcert
```

Generate a CSR (Certificate Sign requests) using the private you key generated in the previous

step.

```
[root@cmxtry ssl]# openssl req -new -sha256 -key cmxtry.com.key -out cmxtry.com.csr

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]:BE
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:DIEGEM
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CMXTRY
Organizational Unit Name (eg, section) []:CMXTRY
Common Name (e.g. server FQDN or YOUR name) []:cmxtry.com
Email Address []:avitosin@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Cisco123
An optional company name []:CMXTRY


[root@cmxtry ssl]# ls
cmxtry.com.csr  cmxtry.com.key  oldcert
```

Display the CSR:

```
[root@cmxtry ssl]# openssl req -new -sha256 -key cmxtry.com.key -out cmxtry.com.csr

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]:BE
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:DIEGEM
Organization Name (eg, company) [Internet Widgits Pty Ltd]:CMXTRY
Organizational Unit Name (eg, section) []:CMXTRY
Common Name (e.g. server FQDN or YOUR name) []:cmxtry.com
Email Address []:avitosin@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:Cisco123
An optional company name []:CMXTRY


[root@cmxtry ssl]# ls
cmxtry.com.csr  cmxtry.com.key  oldcert
```

Copy the CSR (include the beginning of certificate request line and end of certificate request line).

In case of my lab, I was using the free certificate from Comodo (https://www.instantssl.com/)