Migrating Certificates from ASA to Firepower Threat Defense

September 3, 2019
Table of Contents

Introduction ......................................................................................................................... 4
Pre-Requisites ...................................................................................................................... 4
Components Used ............................................................................................................... 4
Prepare the ASA for Migration .......................................................................................... 4
Export ID Certificates or Trustpoint(s) from Source ASA .................................................. 4
  Using Command Line Interface ....................................................................................... 5
  Using Adaptive Security Device Manager ....................................................................... 5
Import Exported Certificate(s) to Target FTD ................................................................. 6
  Verify the Identity and CA Certificate ............................................................................. 9
Export Trustpoint which have Only CA Certificate from the Source ASA .......................... 9
  Verify Certificate Object Status ..................................................................................... 12
Introduction

This document describes the procedure to migrate Identity (ID) and Certificate Authority (CA) Certificates from Cisco Adaptive Security Appliance (ASA) to Firepower Threat Defense (FTD) device.

**Note:** This document does not cover migration of CA server feature of ASA.

**Note:** For more information on creating and applying certificates on FTD, see [Managing FTD Certificates](#).

Pre-Requisites

- Presence of Identity (ID) Certificate on Cisco ASA.
  
  **Note:** In this document, Cisco ASA means that the source ASA firewall which has the ID certificate that you want to migrate to your FTD device.

- When you migrate the ID certificate from source ASA to target FTD, the **PKCS#12** format of the certificate is migrated. This format has private and public RSA keys with certificate information.

- Migration of trustpoint which only contains a CA.

Components Used

<table>
<thead>
<tr>
<th>Components</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source ASA</td>
<td>Version 9.x</td>
</tr>
<tr>
<td>Target FMC</td>
<td>Version 6.2.3 or later</td>
</tr>
<tr>
<td>Target FTD</td>
<td>Version 6.2.3 or later</td>
</tr>
</tbody>
</table>

Prepare the ASA for Migration

**Step 1** Identify the **trustpoint** that you want to migrate from the ASA device.

```bash
ASA# show crypto ca trustpoints
crypto ca trustpoint SSL-Trustpoint
  enrollment terminal fqdn vpn.remoteasa.com
  subject-name CN=vpn.remoteasa.com,O=Company Inc,C=US,St=California,L=San Jose
  keypair SSL-Keypair
```

**Step 2** Note down the name of the **trustpoint**.

The trustpoint name is highlighted in bold in the above configuration sample output.

Export ID Certificates or Trustpoint(s) from Source ASA
Using Command Line Interface

Use the following command to export your ID certificate along with CA certificate using the CLI:

```
ASA(config)#crypto ca export <trustpoint-name> pkcs12 <passphrase>
```

**Note:** Passphrase protects the **PKCS#12** file and is required while importing the certificate in FTD.

Using Adaptive Security Device Manager

**Step 1** Navigate to **Configuration > Remote Access VPN > Certificate Management > Identity Certificates.**

**Figure 1 – Exporting trustpoint from ASDM**

Step 2 In the **Destination** screen, you can choose the certificate that you want to migrate, and click **Export.**

Step 3 Browse the location where you want to save the certificate and perform the following:

a. Choose **PKCS#12 Format (Certificate(s) + Private Key)** option.

b. Enter the passphrase for the file as shown in **Figure 2.**
Migrating Certificates from ASA to Firepower Threat Defense

Import Exported Certificate(s) to Target FTD

You must now have a .p12 file in your possession. This is the certificate bundle with all its associated keys that allows you to import to the FMC by performing the following steps:

**Step 1** Navigate to Devices > Certificates, and click Add to open a New Certificate dialog box.

**Figure 3 - Add Certificate Object on FMC**

**Step 2** Choose the appropriate Target FTD device from the Device drop-down list, and in the Add New Certificate screen, perform the following:

   a. Choose the appropriate Target FTD device from the Device drop-down list.
   b. Click the Plus (+) symbol to add the certificate enrollment object.
   c. Click Add to add the object or click Cancel to cancel the operation.
In the Add Cert Enrollment screen, perform the following:

a. Enter the trustpoint name.

b. (Optional) Enter the trustpoint description.

c. In the CA Information tab, associate a certificate enrollment object with target FTD by selecting PKCS#12 format from the Enrollment Type drop-down list.

d. Browse the .p12 file.

e. Enter the Passphrase key.

f. Click Save.
Figure 5 – PKCS#12 File Selection

Add Cert Enrollment

Name: Ssl_Trustpoint
Description:

CA Information

Enrollment Type: PKCS12 File
PKCS12 File: Ssl_trustpoint_pkcs12.p12
Passphrase: ********

Allow Overrides

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device: FTD
Cert Enrollment: Ssl_Trustpoint

Cert Enrollment Details:

Name: Ssl_Trustpoint
Enrollment Type: PKCS12 file
SCEP URL: NA

Save Cancel
To add a new certificate, click **Add**. The **CA certificate and Identity certificate** status changes from **In Progress** to **Available** as it installs the PKSC#12 file on the device.

**Figure 6 – Certificate Installation on FMC**

Verify the Identity and CA Certificate

Once the certificate status turns to **Available**, click the magnifying glass to view the Identity and CA certificate for the target FTD.

**Figure 7 - Verify Certificate Installation**

Export Trustpoint which have Only CA Certificate from the Source ASA

**Step 1** Execute the **show run** command to copy the **hexdump** of the certificate of the source ASA.

```
ciscoasa# sh run
: Saved
:
: Serial Number: FCH1549777C
: Hardware: ASA5512, 4096 MB RAM, CPU Clarkdale 2792 MHz, 1 CPU (2 cores)
:
:----------- omitted output ----------- crypto ca certificate chain SSL_Trustpoint_CA certificate ca 00e54fa390fac4d43e
30820595 3082037d a0030201 02020900 e54fa390 fac4d43e 300d0609 2a864886 f70d0101 0b050030 61310b30 06035504061302494e310b300906035504080c024b41310c300a06035504070c034247 4c3110300e060355040a0c074a756e69706572310d300b060355040b0c045443 4f4e3116301406035504030c0d6b616e6a756e69706572301e170d313930393238355a
70657231 0d300b060355040b0c045443 4f4e3116301406035504030c0d6b616e6a756e69706572301e170d313930393238355a
61762e617669706572301e170d313930393238355a170d23430
3430830 39323835 355a3061 310b3009 06035504 06130249 4e310b30 09060355
:----------- omitted output -----------
```
Export Trustpoint which have Only CA Certificate from the Source ASA

```
8919f0da c967f291 81f293d5 d9ea86da 4a993d59 4f0e28bb 22d6f865 06bdcc78 231060c5 46d5ea92 856851cb cee44ff9
771a1859 bcd83710 6abbb3c7 de976df7 64d45c4e 5374f2c7 cf8aaaf3b d32a0c6f 26234ce9 1347f4cf 6db5751a df892b6a
1fbe00e9 2102b038 4c8ebcca 84f85f39 f4ca59aa 4e402ff4 3a
```

Step 2  Convert the hexdump to base64 format.

**Note:** You can use the readily available online conversion tools.

Step 3  Navigate to Devices > Certificates, and click Add to open the New Certificate dialog box.

**Figure 8 – Add Certificate Object on FMC**

Step 4  Choose the appropriate Target FTD device from the Device drop-down list and click the Plus (+) symbol, to add the certificate enrollment object.

**Figure 9 - Cert Enrollment Object on FMC**

Step 5  In the Cert Enrollment screen, perform the following:
   a.  Enter the trustpoint name.
   b.  (Optional) Enter the trustpoint description.
   c.  In the CA Information tab, associate a certificate enrollment object with target FTD by selecting Manual from the Enrollment Type drop-down list.
   d.  Enter the base64 format of the CA certificate in the CA certificate field.
   e.  Click Save.
Migrating Certificates from ASA to Firepower Threat Defense

Export Trustpoint which have Only CA Certificate from the Source ASA

**Figure 10 - Manual Enrollment Selection**

### Add Cert Enrollment

| Name:* | SSL_Trustpoint_CA |
| Description: | |

#### CA Information

| Enrollment Type: | Manual |
| CA Certificate:* | -----BEGIN CERTIFICATE-----MUFTI7CCAp8IqIAgIAGYqTaOgvPo556xNQ+MA0GCSqGSIb3OPQFBCyAMGExC2AIBgNV | 
| | BAYTAkMOMQswcQYDVQQIDAJLQTEMMAoGA1UEBwwQOkydMMR | 
| | AwDgYDVQQKDAgKdW5p | 
| | cGMS0MQwCwYDVQQQLDARUQ0F0MRYwFAYDVQQDA1rW5hd | 
| | SodW5pcGWMB4XDTE5 | 
| | MDQwOTASMjI1NVoXTIowMDQwODASMjI1NVoYTLMMAkGA1UE | 
| | EBhMC2UJ4x3CzA9BbNV | 
| | BAgMAkt8M0wwCgYDVQQHDANCROwxEDAQBgNVBAoMBp1bm | 
| | hwZXJxdTA2BgNVBAAsM | 
| | BFRD704xFJAU8BnvBnMMDWthbmF2Lmp1bmlwZXIwggIlMA0GCS | 
| | SqcSib3OPQFBAOQA | 
| | A=3C4RwAwgiKQkCAOQC2Swae1YSNehn15VNm1RtqgoSxksa20nt | 
| | NmC4j27LqeYNEZ | 
| | ZLxDTBGvV8pMSiCe+sT3hUnj+v17O708A/g/tzwBwhoywxcwfr9kEO | 
| | DYJM33c5ER1E | 
| | 2FCQe6J0lqPPrPZGlc4vWiL3ScSCPcU/An62LuwtempTJTG9a6B4 | 
| | e0X6AVAF |

#### Allow Overrides:

Step 6  Click **Save**. Click **Add** to add the certificate enrollment object.
Migrating Certificates from ASA to Firepower Threat Defense

Export Trustpoint which have Only CA Certificate from the Source ASA

Figure 11 - Add Certificate on FMC

Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: 10.106.45.233

Cert Enrollment*: SSL_Trustpoint_CA

Cert Enrollment Details:
Name: SSL_Trustpoint_CA
Enrollment Type: Manual
SCEP URL: NA

Add Cancel

Verify Certificate Object Status

You can see the status when the certificate object is complete. The trustpoint with the CA certificate is now complete.

Figure 12 - Verify Certificate on FMC