Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv1 with Certificates

September 3, 2019
Table of Contents

Introduction .................................................................................................................................................. 4
Existing ASA Configuration ....................................................................................................................... 4
Verification of VPN Tunnel Status on ASA ............................................................................................... 7
Topology .................................................................................................................................................... 8
Configuration on FTD ............................................................................................................................... 8
  Network Diagram .................................................................................................................................. 8
  License Verification on FMC .................................................................................................................... 9
Configuration Procedure on FTD ............................................................................................................. 10
Configuration on FTD Post Deployment .................................................................................................. 21
Introduction

This document describes the procedure to migrate site-to-site IKEv1 VPN tunnels using certificates (rsa-sig) as a method of authentication from the existing Cisco Adaptive Security Appliance (ASA) to Firepower Threat Defense (FTD), managed by Cisco Firepower Management Center (FMC).

Existing ASA Configuration

The following example illustrates a sample ASA configuration.

```
ASA# show running-config
: Saved

: Serial Number: JAD202407H5
: Hardware: ASA5516, 8192 MB RAM, CPU Atom C2000 series 2416 MHz, 1 CPU (8 cores)
: ASA Version 9.12(1)
!
hostname ASA
enable
!
interface GigabitEthernet1/2 nameif inside
  security-level 100
  ip address 192.168.2.1 255.255.255.0
!
interface GigabitEthernet1/3 nameif outside
  security-level 0
  ip address 10.197.222.163 255.255.255.0
!
interface GigabitEthernet1/4 no nameif
  security-level 0 no ip address
!```
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv1 with Certificates

Existing ASA Configuration

```
----------------- Output Omitted ----------------
!
boot system disk0:/asa9-12-1-1fbbf-k8.SPA ftp mode passive
dns domain lookup outside
same security traffic permit inter-interface same security traffic permit intra-interface

----------------- Output Omitted ----------------
object network LOCAL
subnet 192.168.2.0 255.255.255.0

object network REMOTE
subnet 192.168.1.0 255.255.255.0

----------------- Output Omitted ----------------
access-list cryptoacl extended permit ip object LOCAL object REMOTE

pager lines 24 logging enable logging timestamp
logging monitor debugging logging buffered debugging
----------------- Output Omitted ----------------

nat (inside,outside) source static LOCAL LOCAL destination static REMOTE REMOTE no-proxy-arp route-lookup

route outside 0.0.0.0 0.0.0.0 10.106.67.1 1

----------------- Output Omitted ----------------

service sw reset button

crypto ipsec ikev1 transform set ESP AES SHA esp-aes esp-sha-hmac
crypto ipsec security association pmtu aging infinite

crypto map CMAP 1 match address cryptoacl crypto map CMAP 1 set peer 10.106.52.213

crypto map CMAP 1 set ikev1 transform set ESP AES SHA crypto map CMAP interface outside

crypto ca trustpoint SSL_Trustpoint keypair SSL_Trustpoint
```
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv1 with Certificates

Existing ASA Configuration

crl configure

crypto ca trustpool policy

crypto ca certificate chain SSL_Trustpoint

certificate ca 00e5fa390fac4d43e
30820595 3082037d a0030201 02020900 e54fa390 fac4d43e 300d0609 2a864886 f70d0101 0b050030 61310b30 09060355
04061302 49e310b 30090603 5504080c 024b4131 0c300a06 03550407 0c034247 4c311030 0e060355 040a0c07
4a756e69
70657231 0d300b06 0355040b 0c045443 4f4e3116 30140603 5504030c 0d6b616e
61762e6a 756e6970 6572301e 170d3139 30334309 30393238 35355a17 0d323430
3403830 39323835 355a061 310b3009 06303504 06130249 4e310b30 09060355
04080c02 4b41310c 300a0603 5504070c 0342474c 3110300e 06305504 0a0c074a
756e6970 6572310d 30b0603 55040b0c 0454434f 4e311630 14060355 04030c0d
6b616e61 762e6a75 6e697065 7230802d 22300d06 092a864b 86f70d01 01010500
0382020f 03080202 0a028202 01006b64 b6d7a9c8 e5536625 1c6072a4
b192c6b6 d27b4d98 2e338ede de60d119 648c434c 11ab57ca 4c9427be b13de752 78febc9e cceece00 fe0fedcf 0072c21a
32730cdf 73d9040d 824cde77 39111d44 d8509087 a8f496a8 0face3d9 18bcdce2 f5a22f74 9ce4f7f14 fc087ad9 4c2d7ab9
a94e34c6 f5a8ba07 8b346d7d 31018005 0f410a2e db37a0fe 60664239 97405c86
55d38151 a7197a16 455d1500 5b27a43d e9cecf77 c13dc4cc a9f8e676 6dc09452 7cdcf700 9dc6a757 fb039012 10ab73cf
501d3131 8ce31f87 d52fa025 ed60436 28e51af7 9e658ef9 9a44aae9 adb9dacf 1e0d8521 f08394ff 3f72b6b6 70a8193a
1e4d150e 99c577ec ef220000 02d9d201 a01f8e9f 2726d0dd a57514f5 39fa9a04 4f04466c 573ad712 8ada5006 abb91b2c
525f5930 2fa1da42 34addf3b 8ac018de

Output Omitted

-------- Output Omitted --------

231060c5 46d5ea92 856851cb cee4ff9 771a1859 bcb3710 6abbba3c7 de976d72 64d45c4e 5374f2c7 cf8aae3b d32a0c6f
26234ce9 1347f4cf 6db5751a df892b6a 1fbe00e9 2102b038 4c8ebc8a 84f85f39 f4ca59aa 4e02ff4 3a
quit certificate 01
30820595 30820315 02010130 0d6092a 864886f7 0d01010b 05003061 310b3009
06305504 06130249 4e310b30 09060355 04080c02 4b41310c 300a0603 5504070c
0342474c 3110300e 06305504 0a0c074a 756e6970 6572310d 30b0603 55040b0c
0454434f 4e311630 14060355 04030c0d 6b616e61 762e6a75 6e697065 72301e17
Verification of VPN Tunnel Status on ASA

Use the following command to check the encryption and the hashing algorithms used by the tunnel during Phase 1 negotiation.

```
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication rsa-sig encryption aes-256 hash sha
  group 2
  lifetime 86400

username cisco password **** pbkdf2 privilege 15

tunnel-group 10.106.52.213 type ipsec-l2l

ikev1 trust-point SSL_Trustpoint

! policy-map type inspect dns preset_dns_map parameters
message-length maximum client auto message-length maximum 512
no tcp-inspection

ASA#
```
The above example output shows site-to-site VPN configuration elements for ASA, which depicts the following topology. The example that is shown assumes that the remote peer is a Router.

**Topology**

**Figure 1 - Topology Diagram with ASA**

In *Figure 1* the topology is similar to the current configuration in ASA, then follow the Configuration Steps to migrate the configuration to FTD.

**Note:** Ensure that the required interfaces (Physical/Port-channel/Sub-Interface), Routes, NAT, Access Control Policy (ACP) are migrated properly by the Firepower Migration Tool (FMT).

**Configuration on FTD**

**Network Diagram**
License Verification on FMC

Ensure that the FMC is registered with the Smart Licensing Portal. In addition, ensure that Export-Controlled Features are enabled.

Figure 3 - License Verification on FMC
Configuration Procedure on FTD

Migrate the required certificates or Trustpoint as described in “Migrating ASA to Firepower Threat Defense Using Certificates” document.

Step 1  Navigate to **Devices > VPN > Site To Site**.

**Figure 4 – Create New Site To Site VPN Connection**

Step 2  Click **Add VPN > Firepower Threat Defense Device**.

**Figure 5 – Type of Site to Site VPN**
Step 3  Add the **Topology Name**, **Network Topology (Point to Point)**, the **IKE Version** as **IKEv1**. Click the **Plus (+)** symbol to add a node for the VPN tunnel.

**Figure 6 – Create New VPN Topology**

The configuration that is displayed in Figure 6 uses the following settings:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology Name</td>
<td>S2S-VPN-To-10.106.52.213</td>
</tr>
<tr>
<td>Network Topology</td>
<td>Point to Point</td>
</tr>
<tr>
<td>IKE Version</td>
<td>IKEv1</td>
</tr>
</tbody>
</table>

Step 4  For Node A representing the local endpoint of the VPN tunnel, click the **Plus (+)** symbol to specify the target FTD details and perform the following:

a. Choose **Target FTD** as **Device**.

b. Choose the Interface on which the VPN will terminate.

c. Select **Local Network** from **Protected Networks**.
The configuration that is displayed in Figure 7 uses the following settings:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>FTD-2</td>
</tr>
<tr>
<td>Interface</td>
<td>outside</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.197.222.163</td>
</tr>
<tr>
<td>Protected Network</td>
<td>Subnet / IP Address (Network)</td>
</tr>
</tbody>
</table>

If you require more details on the networks that you must communicate over the VPN tunnel, use the **Access List (Extended)** option and define the access-list that will be used for protected networks. This functionality was added from version 6.2.3 of the FMC.

In case the ACL on the ASA makes use of objects, you can use the option of Subnet/IP Address. In addition, if the ACL is more detailed, make use of the **Access List (Extended)** option on the FMC.
Figure 8 – Add Local Protected Network (Using Access List)

For FMC version 6.2.3 or earlier, use Protected Networks to add the Local and Remote Network Objects displayed in Figure 9.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv1 with Certificates
Configuration on FTD

Figure 9 - Add Local Protected Network (FMC version 6.2.3 or earlier)

Step 5 Select Local Network from Protected Networks, and click OK to save the endpoint configuration.

Figure 10 - Add Remote Endpoint (Using Subnet)

Step 6 For Node B representing the remote endpoint of the VPN tunnel, click the Plus (+) symbol to specify the remote peer details, and perform the following:

a. Choose Extranet as Device.

b. Enter the Device Name and WAN IP Address of the remote endpoint.

c. Select Remote Network from Protected Networks.

d. Click OK to save the endpoint configuration.

Note: If the peer device is managed by the same FMC, see Site-to-Site VPN for FTD managed by the same FMC.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv1 with Certificates

Configuration on FTD

Figure 11 – Add Remote Endpoint

![Figure 11](image)

**Note:** There is no option to configure the tunnel-group name. The FMC will deploy the name of the tunnel-group as the IP address of the peer device.

The configuration that is displayed in **Figure 11** uses the following settings:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Extranet</td>
</tr>
<tr>
<td>Device Name</td>
<td>Router</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.106.52.213</td>
</tr>
<tr>
<td>Protected Network</td>
<td>Subnet / IP Address (Network)</td>
</tr>
</tbody>
</table>

Step 7  Create a New IKEv1 Policy to match the VPN Phase 1 settings existing on the ASA.

To find the IKE policy used by the VPN tunnel, see [Verification of VPN tunnel on ASA](#).

a. Navigate to the **IKE** tab.
b. Click the **Plus (+)** symbol to add a new IKEv1 Policy.
c. Specify the IKE parameters.
d. Click **Save**.
Figure 12 - New IKEv1 Policy

The configuration that is displayed in Figure 12 uses the following settings:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>IKEv1 - AES-256 - SHA</td>
</tr>
<tr>
<td>Encryption</td>
<td>AES-256</td>
</tr>
<tr>
<td>Hash</td>
<td>SHA</td>
</tr>
<tr>
<td>Diffie-Hellman Group</td>
<td>2</td>
</tr>
<tr>
<td>Lifetime</td>
<td>86400 seconds</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Certificate</td>
</tr>
</tbody>
</table>
Step 8  Select **Certificate** as the **Authentication Type** and the required trustpoint from the **Certificate** drop-down option.

**Figure 13 - IKE Settings**

![IKE Settings](image)

Step 9  Create a New IKEv1 IPsec Proposal to match the VPN Phase 2 settings existing on the ASA (you can also edit the default IPsec Proposal to match the parameters).

To create a new IKEv1 IPsec Proposal, perform the following:

a. Navigate to the **IPsec** tab.

b. Click **Edit** to edit the default IKEv1 IPsec Proposal.

c. Click the **Plus (+)** symbol to add a new IKEv1 IPsec Proposal.

d. Specify the IPsec parameters.

e. Click **Save** to save the configuration.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv1 with Certificates
Configuring the ASA using the Firepower Threat Defense platform.

Figure 14 - Create New IKEv1 IPsec Proposal

The configuration that is displayed in Figure 14 uses the following settings:

<table>
<thead>
<tr>
<th>Settings</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>ESP·AES·SHA</td>
</tr>
<tr>
<td>ESP Encryption</td>
<td>AES·128</td>
</tr>
<tr>
<td>ESP Hash</td>
<td>SHA</td>
</tr>
</tbody>
</table>

Step 10 Select the **IPsec Transform Set** from the list of the **Available Transform Sets**.

Figure 15 - Select IKEv1 IPsec Proposal
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv1 with Certificates
Configuration on FTD

Step 11 Confirm that the selected IKEv1 IPsec Proposal is displayed in the **IKEv1 IPsec Proposals**.

**Figure 16 - IPsec Settings**

![IPsec Settings](image)

Step 12 Navigate to **Advanced > Tunnel > Access Control for VPN Traffic**.

The traffic that enters the FTD through a VPN tunnel is subjected to access list checks by default. To bypass the interface ACL check, select the **sysopt connection permit-vpn** check box. Group-policy and per-user authorization access lists still apply to traffic.

**Note:** By default, this setting is enabled on the ASA and is disabled on the FTD.

To get the **sysopt** settings on the ASA, execute the following command on the ASA CLI:

```
ASA# show running-config all
  sysopt no sysopt traffic detailed-statistics no
  sysopt connection timewait
  sysopt connection tcpmss 1380 sysopt connection
tcpmss minimum 0 **sysopt connection permit-vpn**
sysopt connection reclassify-vpn
no sysopt connection preserve-vpn-flows no sysopt
radius ignore-secret

no sysopt noproxyarp inside no sysopt
noproxyarp outside
```
Figure 17 - Advanced VPN Tunnel Settings

This Access Control for VPN Traffic bypasses the check from the WAN to LAN zone. Define access-control policy to allow traffic from the LAN to the WAN zone.

Step 13 Click **Save** to save the VPN tunnel configuration on the FMC.

Figure 18 - Save VPN Settings
Step 14 Select the device to deploy the changes, and click **Deploy**.

**Figure 19 – Deploy Policies**

![Deploy Policies](image)

**Note:** Ensure that the required NAT and Access Control Policy configuration is migrated properly by the Firepower Migration Tool (FMT).

**Configuration on FTD Post Deployment**

```
firepower# show running-config

: Saved
:
: Serial Number: JAD20140353
: Hardware: ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores)
: NGFW Version 6.2.3.12
!
hostname firepower
enable password $sha512$5000$q+ve+AwwZxPmzkSAh+SvTg==$Cizrqb4ziPzWva0kUrf4iw== pbkdf2
names
!
interface GigabitEthernet1/2
```
nameif inside
c
propagate sgt preserve-untag policy static sgt disabled trusted

security-level 100
ip address 192.168.2.1 255.255.254.0

interface GigabitEthernet1/3
nameif outside

c
propagate sgt preserve-untag policy static sgt disabled trusted
security-level 0
ip address 10.197.222.163 255.255.254.0

--- Output Omitted ---
boot system disk0:/os.img ftp mode passive
ngips conn-match vlan-id

object network LOCAL
subnet 192.168.2.0 255.255.255.0

object network REMOTE
subnet 192.168.1.0 255.255.255.0

access-list CSM_FW_ACL record rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL record rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL advanced permit ipinip any any rule-id 9998 access-list CSM_FW_ACL advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL advanced permit gre any any rule-id 9998
access-list CSM_FW_ACL advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL advanced permit udp any any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL remark rule-id 268435458: ACCESS POLICY: FTD-2-ACP - Mandatory
access-list CSM_FW_ACL remark rule-id 268435458: L7 RULE: Inside-Outside-VPN-ACP
access-list CSM_FW_ACL advanced permit ip ifc inside object LOCAL ifc outside object REMOTE rule-id 268435458
access-list CSM_FW_ACL_ remark rule id 268435457: ACCESS POLICY: FTD-2-ACP -

Default

access-list CSM_FW_ACL_ remark rule-id 268435457: L4 RULE: DEFAULT ACTION RULE

access-list CSM_FW_ACL_ extended permit ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0

! 

----------------- Output Omitted -----------------

nat (inside, outside) source static LOCAL LOCAL destination static REMOTE REMOTE no-proxy-arp route-lookup

nat (inside, outside) source dynamic any interface access-group CSM_FW_ACL_ global

route outside 0.0.0.0 0.0.0.0 10.197.222.1 1

----------------- Output Omitted -----------------

crypto ipsec ikev1 transform-set CSM_TS_1 esp-aes esp-sha-hmac

crypto ipsec security-association pmtu-aging infinite

crypto map CSM_Outside_map 1 match address CSM_IPSEC_ACL_1

crypto map CSM_Outside_map 1 set peer 10.106.52.213

crypto map CSM_Outside_map 1 set ikev1 transform-set CSM_TS_1

crypto ca trustpoint SSL_Trustpoint

22rollment terminal

crl configure

crypto ca certificate chain SSL_Trustpoint

certificate ca 00

<table>
<thead>
<tr>
<th>30820400</th>
<th>308202e8</th>
<th>a0030201</th>
<th>02020100</th>
<th>300d0609</th>
<th>2a864886</th>
<th>f70d0101</th>
</tr>
</thead>
<tbody>
<tr>
<td>05050030</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>63310b30</th>
<th>09060355</th>
<th>04061302</th>
<th>55533121</th>
<th>301f0603</th>
<th>55040a13</th>
<th>18546865</th>
</tr>
</thead>
<tbody>
<tr>
<td>20476f20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>44616464</th>
<th>79204772</th>
<th>6f75702c20496e63</th>
<th>2e313130</th>
<th>2f060355</th>
<th>040b1328</th>
</tr>
</thead>
<tbody>
<tr>
<td>476f2044</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>61646479</th>
<th>20436c61</th>
<th>73732032</th>
<th>20436572</th>
<th>74696669</th>
<th>63617469</th>
<th>6f6e2041</th>
</tr>
</thead>
<tbody>
<tr>
<td>7574686f</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv1 with Certificates

Configuration on FTD

<table>
<thead>
<tr>
<th>72697479</th>
<th>301e170d</th>
<th>30343036</th>
<th>32393137</th>
<th>30363230</th>
<th>5a170d33</th>
<th>34303632</th>
</tr>
</thead>
<tbody>
<tr>
<td>39313730</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3632305a</td>
<td>3063310b</td>
<td>30090603</td>
<td>55040613</td>
<td>02555331</td>
<td>21301f06</td>
<td>0355040a</td>
</tr>
<tr>
<td>13185468</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---------------- Output Omitted ----------------

e0ad595 629a0dcf 8882c532 0ce42b9f 45e60d9f 289cb1b9 2a5a57ad 370f3f1d 7f6bbd9f
quit
crypto ca certificate chain **SSL_Trustpoint**
certificate ca 1be715
3082047d 30820365 a0030201 0202031b e715300d 06092a86 4886f70d 01010b05
00306331 0b300906 03550406 13025553 3121301f 06035554 0a131854 68652047
6f204461 64467920 47726f75 702c2049 6e632e31 322043 65727469 66696361 74696f6e 20175468
20446164 64792043 322043 65727469 66696361 74696f6e 20175468
---------------- Output Omitted ----------------
crypto ikev1 enable Outside
crypto ikev1 am- disable
crypto ikev1 policy 1
authentication rsa- sig
encryption aes- 256 hash sha
group 2
lifetime 86400

---------------- Output Omitted ----------------
tunnel- group 10.106.52.213 type ipsec- l2l
tunnel- group 10.106.52.213 general- attributes
default- group- policy .DefaultS2SgroupPolicy
tunnel- group 10.106.52.213 ipsec- attributes
ikev1 trustpoint SSL_Trustpoint

group- policy .DefaultS2SgroupPolicy internal
group- policy .DefaultS2SgroupPolicy attributes
vsys vassl

tunnel interface Site-1

ingress only

vsys vassl

tunnel interface Site-2

ingress only

hostname codec

dynamic access-policy record DfltAccessPolicy

! class-map inspection_default match default inspection traffic

!------------- Output Omitted -------------

Cryptochecksum:b76f6eee4099a9a021b6adb496bee827

: end firepower#