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

September 3, 2019

Table of Contents

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
!
```

```
------------ Output Omitted ------------
!
boot system disk0:/asa9-12-1-lfbff-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
nat (inside,outside) source dynamic any interface
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
```

```
crl configure

crypto ca trustpool policy

crypto ca certificate chain SSL_Trustpoint

certificate ca 00e54fa390fac4d43e

30820595 3082037d a0030201 02020900 e54fa390 fac4d43e 300d0609 2a864886 f70d0101 0b050030 61310b30 09060355
04061302 494e310b 30090603 5504080c 024b4131 0c300a06 03550407 0c034247 4c311030 0e060355 040a0c07
4a756e69

70657231 0d300b06 0355040b 0c045443 4f4e3116 30140603 5504030c 0d6b616e

61762e6a 756e6970 6572301e 170d3139 30343039 30393238 35355a17 0d323430

34303830 39323835 355a3061 310b3009 06035504 06130249 4e310b30 09060355

04080c02 4b41310c 300a0603 5504070c 0342474c 3110300e 06035504 0a0c074a

756e6970 6572310d 300b0603 55040b0c 0454434f 4e311630 14060355 04030c0d

6b616e61 762e6a75 6e697065 72308202 22300d06 092a8648 86f70d01 01010500

0382020f 00308202 0a028202 0100b64b 069ed584 8d7a19c8 e5536625 1c6072a4

b192c6b6 d27b4d98 2e338ede de60d119 64bc434c 11ab57ca 4c9427be b13de752 78febc9e ceecef00 fe0fedcf 0072c21a
32730cdf 73d9040d 824cdf77 39111d44 d8509087 a8f496a8 0face3d9 18bcdce2 f5a22f74 9ce4f714 fc087ad9 4c2d7ab9
a94e34c6 f5a8ba07 8b346d7d 31018005 0f410a2e db37a0fe 60664239 97405c86


55d38151 a7197a16 455d1500 5b27a43d e9cecf77 c13dc4cc a9f8e676 6dc09452 7cdfc700 9dc6a757 fb039012 10ab73cf
50d1d31d 8ce31f87 d52fa025 ed6b0436 28e51af7 9e658efd 9a44aae9 adb9daef 1e0d8521 f08394ff 3f72b6b6 70a8193a
1e4d150e 99c577ec eff22000 02d9d201 a01f8e9f 2726d0dd a57514f5 39fa9a04 4f044d6c 573ad712 8ada5006 abb91bc2
525f5930 2fa1da42 34addfb3 8ac018de


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


231060c5 46d5ea92 856851cb cee44ff9 771a1859 bcdb3710 6abbb3c7 de976d72 64d45c4e 5374f2c7 cf8aaf3b d32a0c6f
26234ce9 1347f4cf 6db5751a df892b6a 1fbe00e9 2102b038 4c8ebcca 84f85f39 f4ca59aa 4e402ff4 3a

quit certificate 01

3082052d 30820315 02010130 0d06092a 864886f7 0d01010b 05003061 310b3009

06035504 06130249 4e310b30 09060355 04080c02 4b41310c 300a0603 5504070c

0342474c 3110300e 06035504 0a0c074a 756e6970 6572310d 300b0603 55040b0c

0454434f 4e311630 14060355 04030c0d 6b616e61 762e6a75 6e697065 72301e17
```

```
0d313930 34303930 39333434 305a170d 32313034 30383039 33343430 5a305831
0b300906 03550406 1302494e 310b3009 06035504 080c024b 41310c30 0a060355
04070c03 42474c31 10300e06 0355040a 0c074a75 6e697065 72310d30 0b060355
040b0c04 54434f4e 310d300b 06035504 030c0469 645f3130 82022230 0d06092a
864886f7 0d010101 05000382 020f0030 82020a02 82020100 9dcaf303 ddc384d5



------------ Output Omitted ------------
crypto ikev1 enable outside crypto ikev1 policy 1
authentication rsa-sig encryption aes-256 hash sha
group 2
lifetime 86400
------------ Output Omitted ------------
username cisco password ***** pbkdf2 privilege 15
tunnel-group 10.106.52.213 type ipsec-l2l
tunnel-group 10.106.52.213 ipsec-attributes
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
------------ Output Omitted ------------
Cryptochecksum:09917190ba126fe882897e8e7975d441
: end
ASA#
```

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.

```
ASA# show crypto ikev1 sa detail

IKEv1 SAs:

Active SA: 1

Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1
```

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

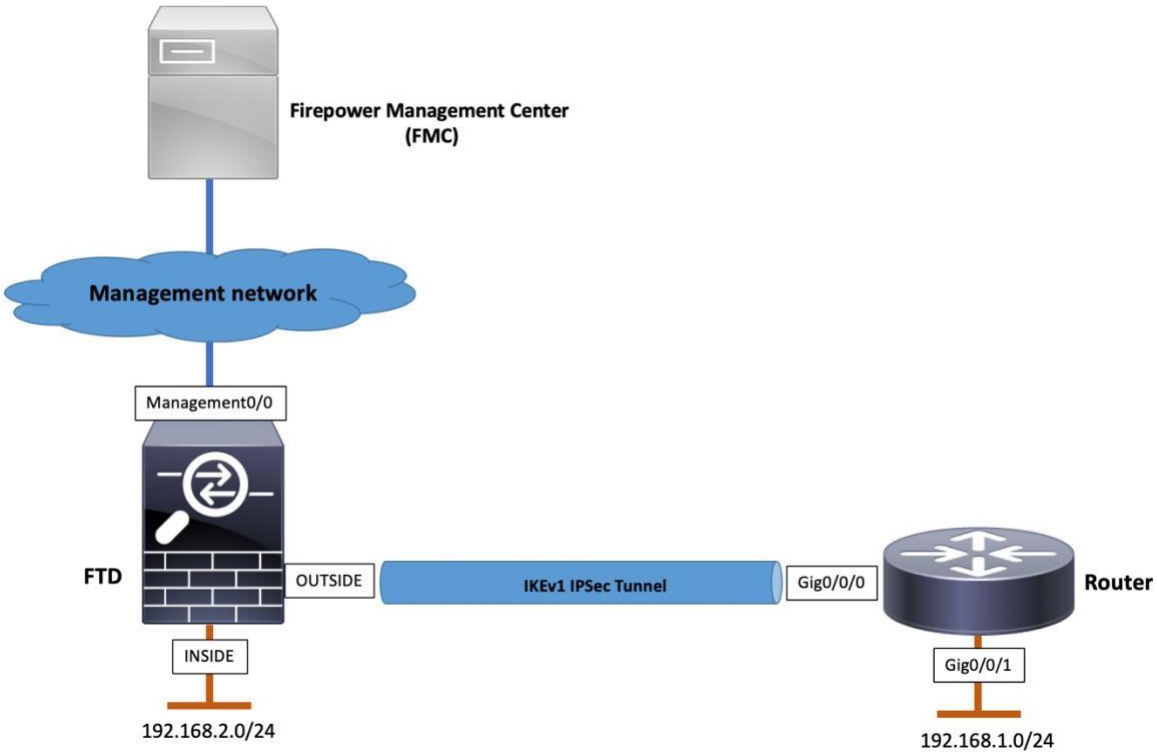
In Figure 1 the topology is similar to the current configuration in ASA, then follow the Configuration Steps to migrate the configuration to FTD.

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

Figure 2 – Network Diagram with FTD



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.

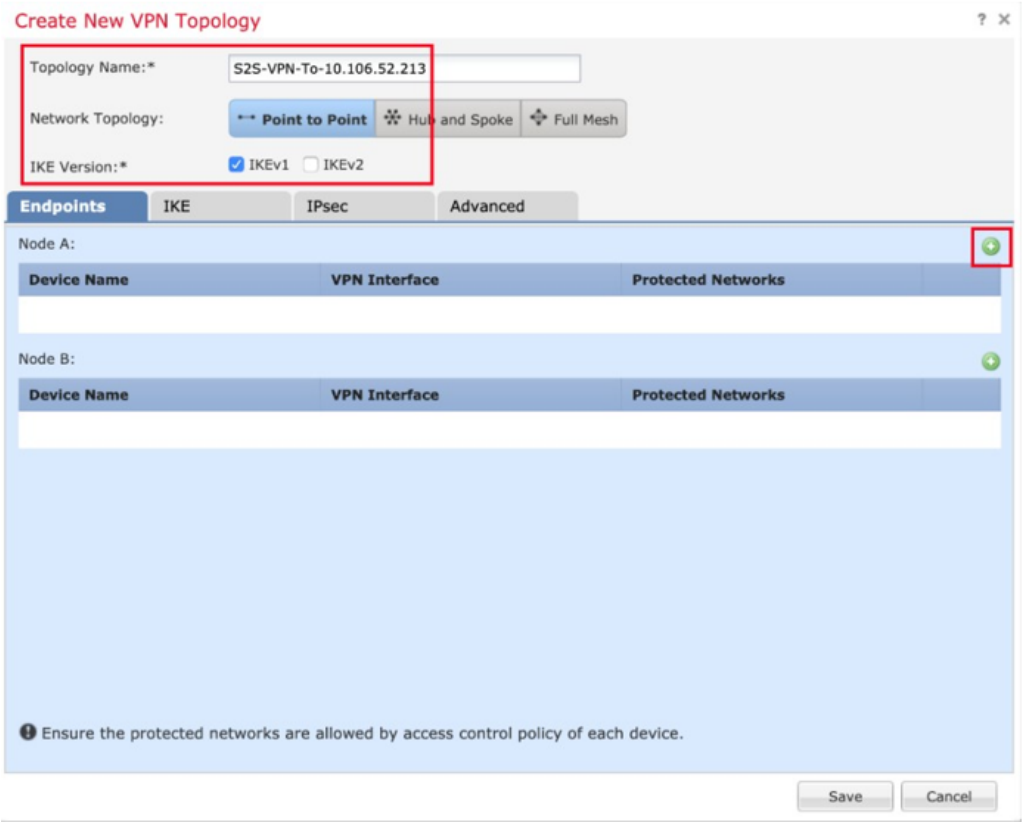
Figure 4 – Create New Site To Site VPN Connection

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:

Settings	Values
Topology Name	S2S-VPN-To-10.106.52.213
Network Topology	Point to Point
IKE Version	IKEv1

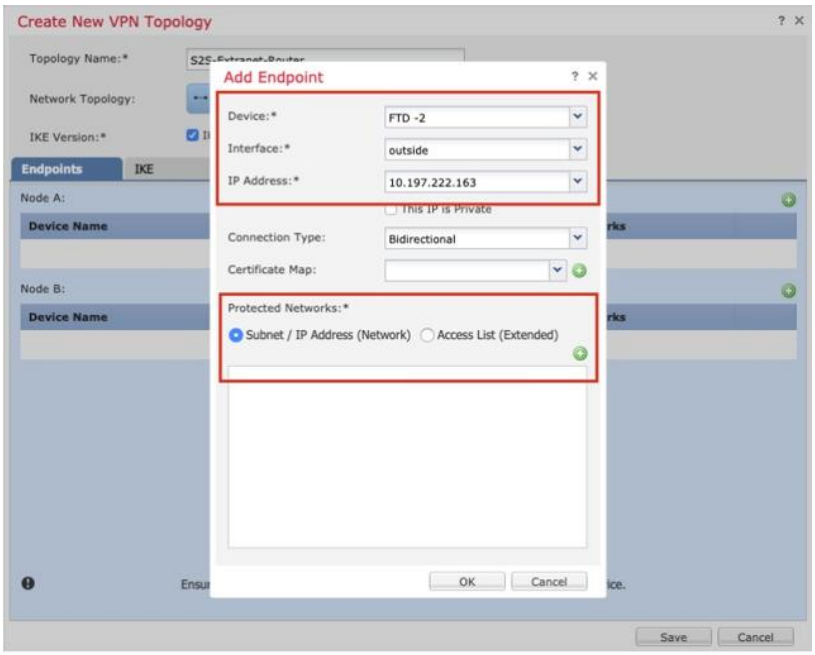
Step 4 For Node A representing the local endpoint of the VPN tunnel, click the Plus (+) symbol to specify the target FTD details and perform the following:

a. Choose Target FTD as Device.

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

c. Select Local Network from Protected Networks.

Figure 7 – Add Local Endpoint



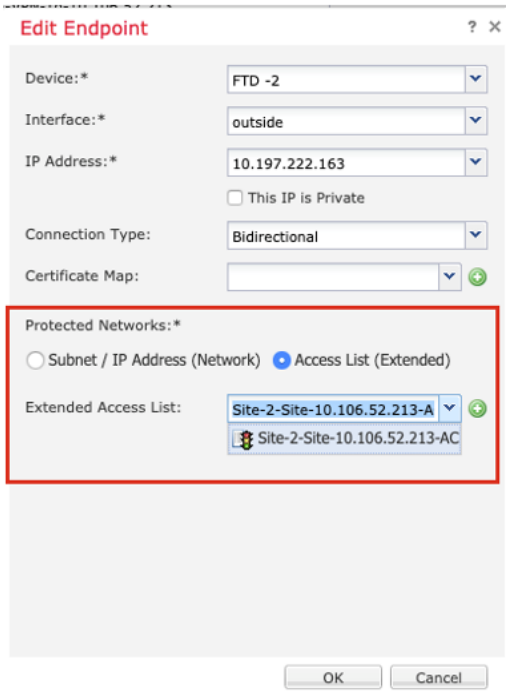
The configuration that is displayed in Figure 7 uses the following settings:

Settings	Values
Device	FTD-2
Interface	outside
IP Address	10.197.222.163
Protected Network	Subnet / IP Address (Network)

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.

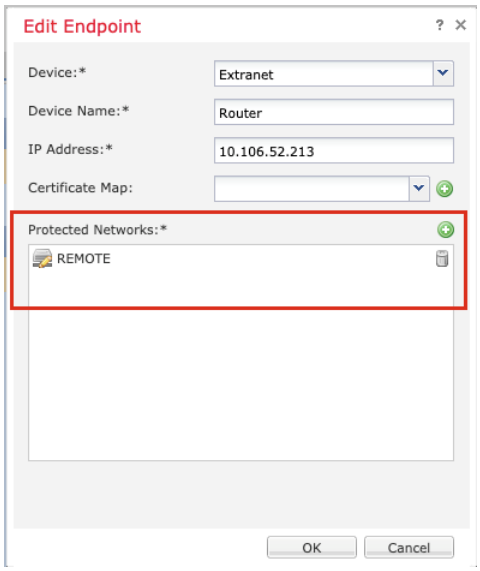
In case the ACL on the ASA makes use of objects, you can use the option of Subnet/IP Address. In addition, if the ACL is more detailed, make use of the Access List (Extended) option on the FMC.

Figure 8 – Add Local Protected Network (Using Access List)



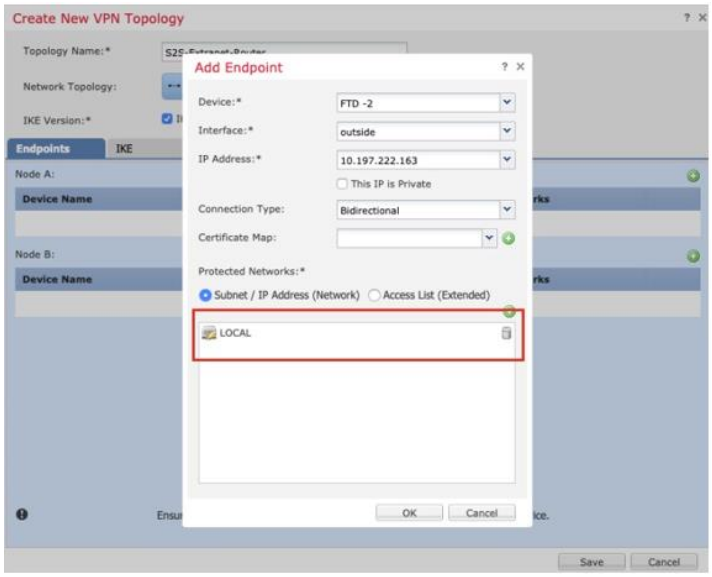
For FMC version 6.2.3 or earlier, use Protected Networks to add the Local and Remote Network Objects displayed in Figure 9.

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.

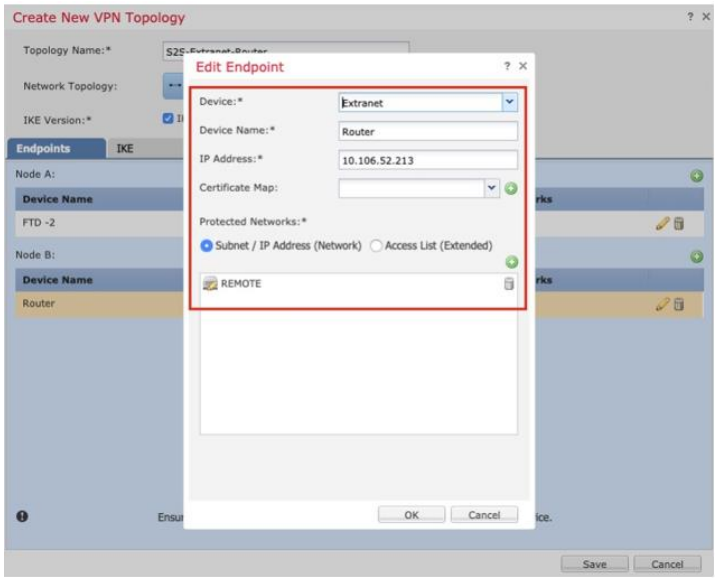
b. Enter the Device Name and WAN IP Address of the remote endpoint.

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.

Figure 11 – Add Remote Endpoint



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:

Settings	Values
Device	Extranet
Device Name	Router
IP Address	10.106.52.213
Protected Network	Subnet / IP Address (Network)

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.

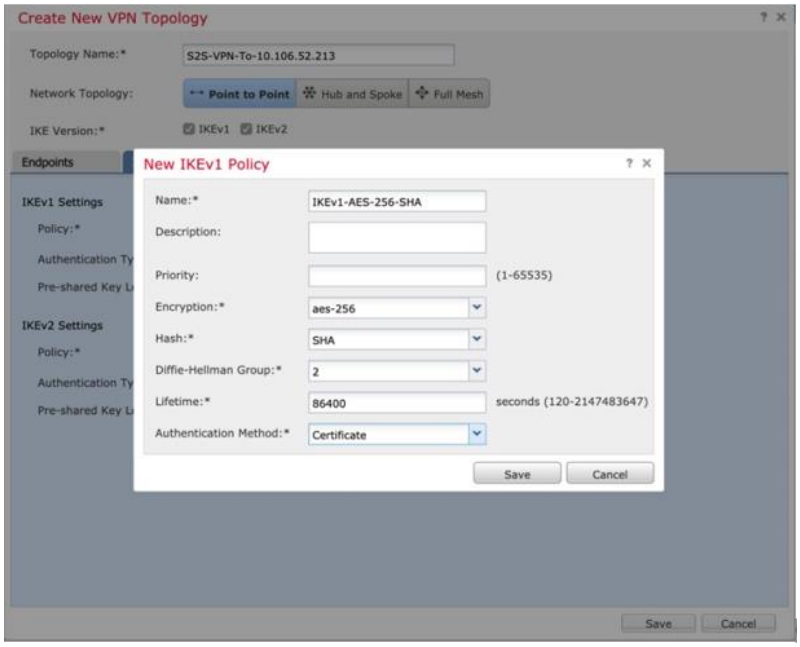
a. Navigate to the IKE tab.

b. Click the Plus (+) symbol to add a new IKEv1 Policy.

c. Specify the IKE parameters.

d. Click Save.

Figure 12 - New IKEv1 Policy

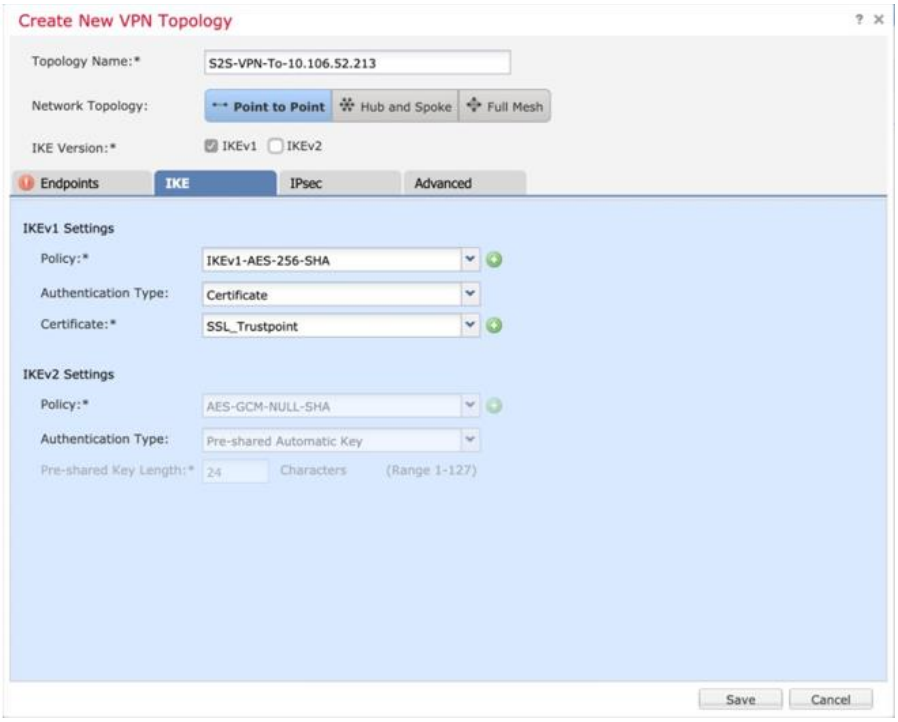


The configuration that is displayed in Figure 12 uses the following settings:

Settings	Values
Name	IKEv1-AES-256-SHA
Encryption	AES-256
Hash	SHA
Diffie-Hellman-Group	2
Lifetime	86400
Authentication Method	Certificate

Step 8 Select Certificate as the Authentication Type and the required trustpoint from the Certificate drop-down option.

Figure 13 - IKE Settings



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.

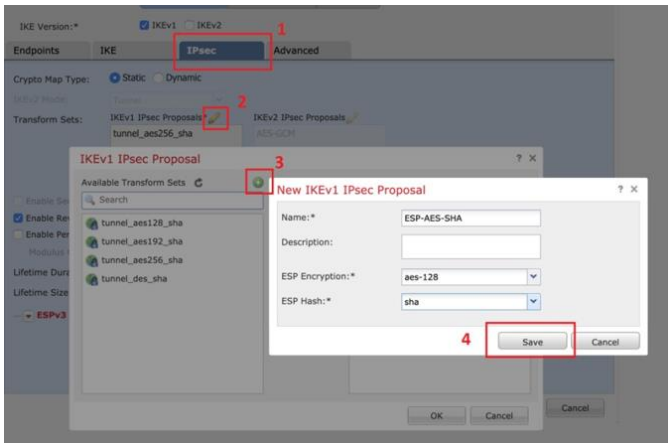
b. Click Edit to edit the default IKEv1 IPsec Proposal.

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

d. Specify the IPsec parameters.

e. Click Save to save the configuration.

Figure 14 - Create New IKEv1 IPsec Proposal

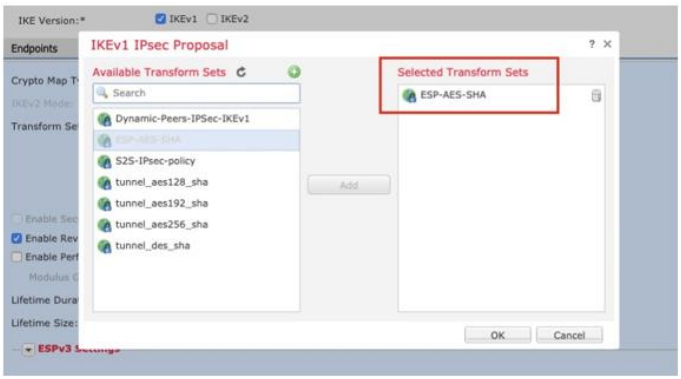


The configuration that is displayed in Figure 14 uses the following settings:

Settings	Values
Name	ESP-AES-SHA
ESP Encryption	AES-128
ESP Hash	SHA

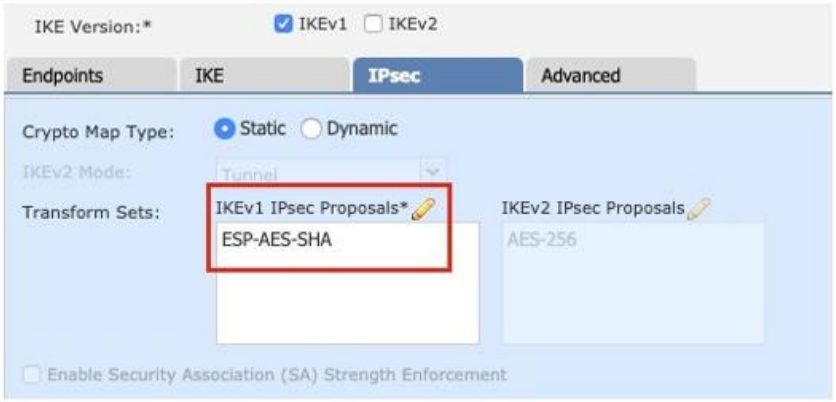
Step 10 Select the IPsec Transform Set from the list of the Available Transform Sets.

Figure 15 - Select IKEv1 IPsec Proposal



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

Figure 16 – IPsec Settings



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.

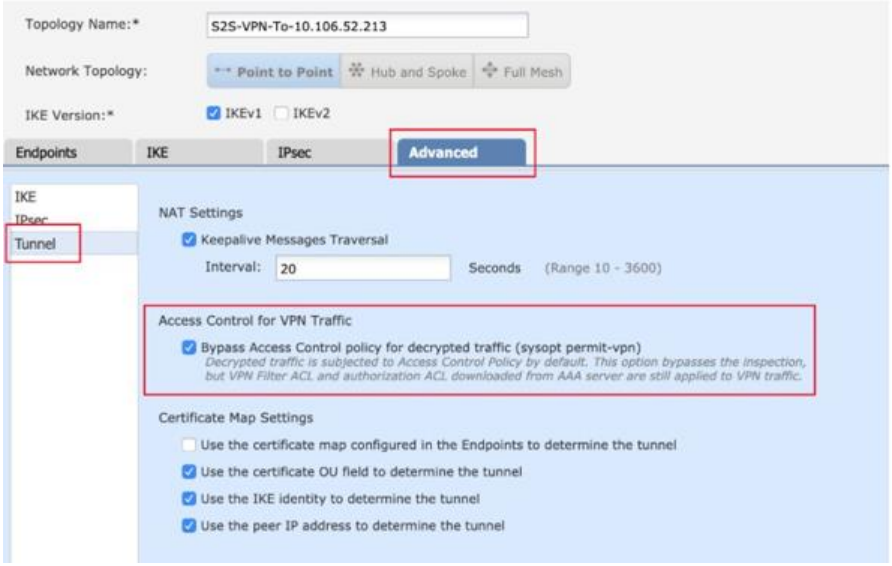
Note: By default, this setting is enabled on the ASA and is disabled on the FTD.

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
```

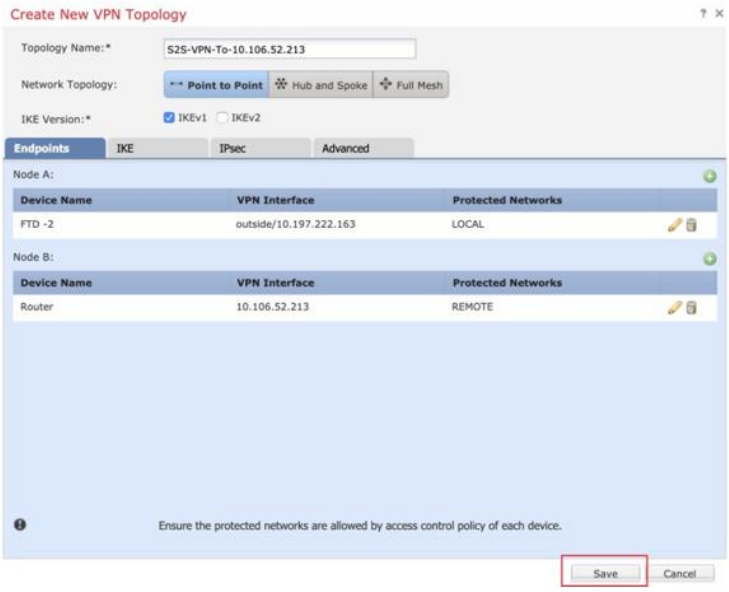
Figure 17 - Advanced VPN Tunnel Settings



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.

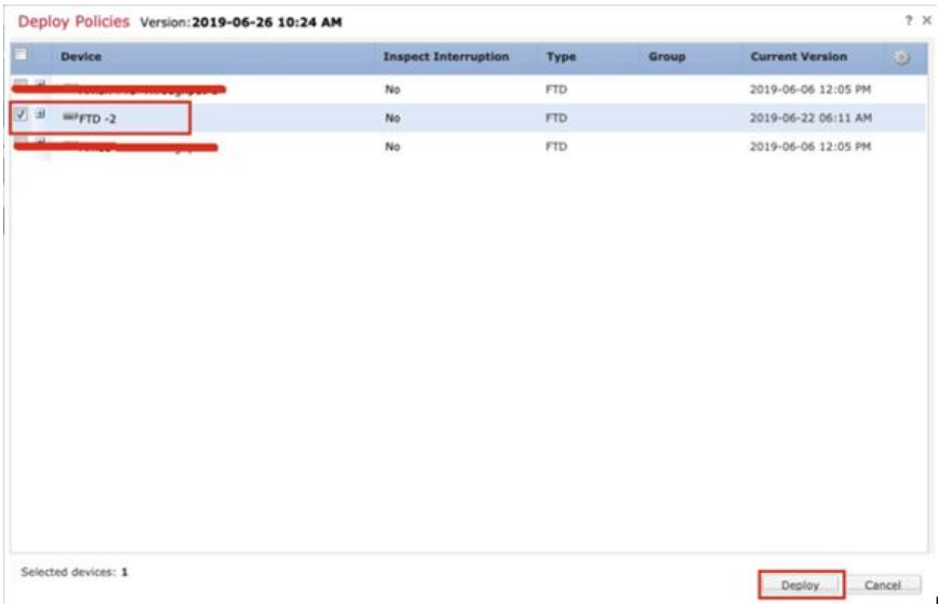
Step 13 Click Save to save the VPN tunnel configuration on the FMC.

Figure 18 - Save VPN Settings



Step 14 Select the device to deploy the changes, and click Deploy.

Figure 19 – Deploy Policies



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==$Cizrqb4ziPzWva0kLUr4iw== pbkdf2
names
!
interface GigabitEthernet1/2
```

```
nameif inside
cts manual
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
cts manual
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_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ remark 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 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_
advanced deny ip any any rule-id 268435457
access-list CSM_IPSEC_ACL_1 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 map CSM_Outside_map interface Outside
crypto ca trustpoint SSL_Trustpoint
22nrolment terminal
crl configure


crypto ca certificate chain SSL_Trustpoint
certificate ca 00


30820400        308202e8        a0030201        02020100        300d0609        2a864886        f70d0101
        05050030
63310b30        09060355        04061302        55533121        301f0603        55040a13        18546865
        20476f20
44616464        79204772        6f75702c20496e63        2e313130        2f060355        040b1328
        476f2044
61646479        20436c61        73732032        20436572        74696669        63617469        6f6e2041
        7574686f
```

```
72697479 301e170d 30343036 32393137 30363230 5a170d33 34303632
        39313730
3632305a 3063310b 30090603 55040613 02555331 21301f06 0355040a
        13185468
------------ Output Omitted ------------
e0ad595 629a0dcf 8882c532 0ce42b9f 45e60d9f 289cb1b9 2a5a57ad 370faf1d 7fdbbd9f
quit
crypto ca certificate chain SSL_Trustpoint
certificate ca 1be715
3082047d 30820365 a0030201 0202031b e715300d 06092a86 4886f70d 01010b05
00306331 0b300906 03550406 13025553 3121301f 06035504 0a131854 68652047
6f204461 64647920 47726f75 702c2049 6e632e31 31302f06 0355040b 1328476f
20446164 64792043 6c617373 20322043 65727469 66696361 74696f6e 20417574
------------ 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
```

```
  vpn-idle-timeout 30
  vpn-idle-timeout alert-interval 1 vpn-session-timeout none
  vpn-session-timeout alert-interval 1
  vpn-filter none
  vpn-tunnel-protocol ikev1


  dynamic-access-policy-record DfltAccessPolicy
  !
  class-map inspection_default match default-inspection-traffic
  !
  ------------ Output Omitted ------------
  Cryptochecksum:b76f6eee4099a9a021b6adb496bee827
: end firepower#
```