



Migrating ASA to Firepower Threat Defense—Dynamic Crypto Map Based Site-to-Site Tunnel on FTD

September 3, 2019

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2019 Cisco Systems, Inc. All rights reserved.

Table of Contents

Introduction	4
Existing ASA Configuration	4
Verification of VPN Tunnel Status on ASA	8
Topology	9
Configuration on FTD	10
Network Diagram	10
License Verification on FMC	10
Configuration Procedure on FTD	11
Configuration on FTD Post Deployment	24
Exception Cases for Migrating from ASA to FTD	29
VPN Settings Under Group-policy Attributes	29
Number of IKE Policies More than the number of Tunnels on the FTD	34

Introduction

This document describes the procedure to migrate Dynamic Crypto Map based site-to-site VPN tunnels (with IKEv1 or IKEv2) using pre-shared key and certificate 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

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 password ***** pbkdf2

no mac-address auto

!

interface GigabitEthernet1/1

no nameif

security-level 0

no ip address

!

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 -----

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 ikev2 ipsec-proposal AES
```

```
protocol esp encryption aes-256
protocol esp integrity sha-1
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map DMAP 1 set ikev1 transform-set ESP-AES-SHA
crypto dynamic-map DMAP 1 set ikev2 ipsec-proposal AES
crypto dynamic-map DMAP 1 set reverse-route
crypto map CMAP 65535 ipsec-isakmp dynamic DMAP
crypto map CMAP interface outside
crypto ca trustpool policy
crypto ikev2 policy 1
  encryption aes-256
  integrity sha
  group 5
  prf sha
  lifetime seconds 86400
crypto ikev2 policy 20
  encryption aes
  integrity sha256
  group 2
  prf sha
  lifetime seconds 86400
crypto ikev2 enable outside
crypto ikev1 enable outside
crypto ikev1 policy 1
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 86400
crypto ikev1 policy 2
  authentication pre-share
  encryption 3des
  hash sha
  group 2
```

```
lifetime 86400

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

username cisco password ***** pbkdf2 privilege 15

tunnel-group DefaultL2LGroup ipsec-attributes

ikev1 pre-shared-key *****

ikev2 remote-authentication pre-shared-key *****

ikev2 local-authentication pre-shared-key *****

!

policy-map type inspect dns preset_dns_map

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

Cryptochecksum:09917190ba126fe882897e8e7975d441

: end

ASA#
```

To get the clear text form of the pre-shared key used for the VPN tunnel, execute the following command in the ASA CLI:

```
ASA# more system:running-config | begin tunnel-group DefaultL2LGroup
```

```
tunnel-group DefaultL2LGroup ipsec-attributes
```

```
ikev1 pre-shared-key cisco123
```

```
ikev2 remote-authentication pre-shared-key cisco123
```

```
ikev2 local-authentication pre-shared-key cisco123
```

Verification of VPN Tunnel Status on ASA

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

```
ASA# show crypto isakmp sa detail
```

```
There are no IKEv1 SAs
```

```
IKEv2 SAs:
```

```
Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

Tunnel-id	Local	Remote	Status	Role
10514185	10.197.222.163/500	10.106.52.213/500	READY	RESPONDER

```
Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:5, Auth sign: PSK, Auth verify: PSK
```

```
Life/Active Time: 86400/18 sec
```

```
Session-id: 2
```

```
Status Description: Negotiation done
```

```
Local spi: 104CBBE0FBBBAFFD Remote spi: 05DBC67E9F85AEDD
```

```
Local id: 10.197.222.163
```

```
Remote id: 10.106.52.224
```

```
Local req mess id: 1 Remote req mess id: 2
```

```
Local next mess id: 1 Remote next mess id: 2
```

```
Local req queued: 1 Remote req queued: 2
```

```
Local window: 1 Remote window: 5
```

```
DPD configured for 10 seconds, retry 2
```

```
NAT-T is not detected
```

```
IKEv2 Fragmentation Configured MTU: 576 bytes, Overhead: 28 bytes, Effective MTU: 548 bytes
```

```
Child sa: local selector 192.168.2.0/0 - 192.168.2.255/65535
```

```
remote selector 192.168.1.0/0 - 192.168.1.255/65535
```

```
ESP spi in/out: 0xd71be66b/0xcf7bbd1d
```

```
AH spi in/out: 0x0/0x0
```


Topology

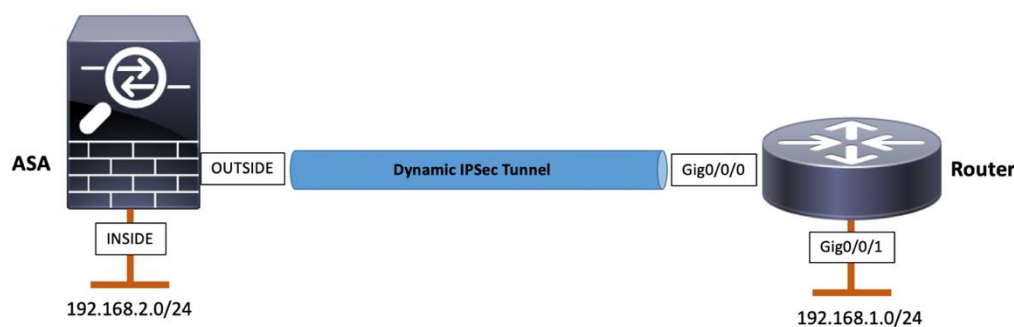
```
CPI in/out: 0x0/0x0  
Encr: AES-CBC, keysize: 256, esp_hmac: SHA96  
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel  
Parent SA Extended Status:  
Delete in progress: FALSE  
Marked for delete: FALSE
```

The above sample output shows site-to-site VPN configuration elements for ASA.

Topology

Figure 1 displays the site-to-site VPN configuration when the remote peer is a Router.

Figure 1 - Topology Diagram with ASA



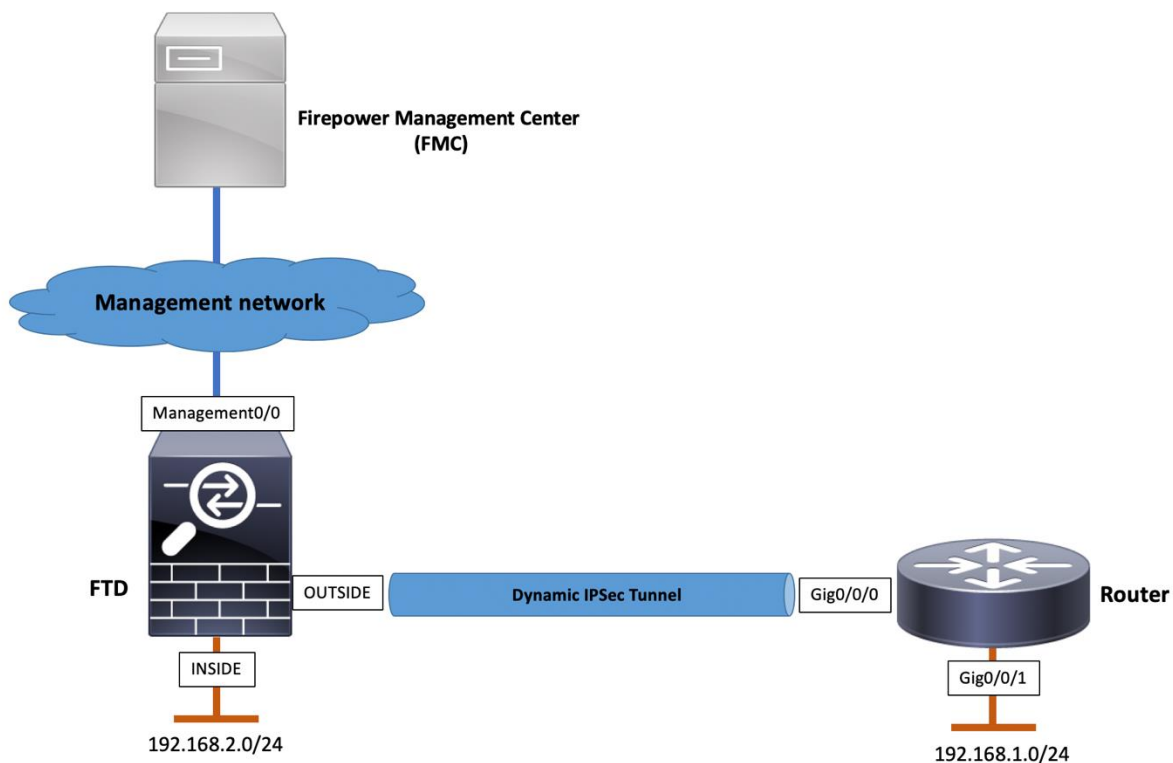
If Figure 1 is similar to the current configuration in ASA, then follow the [Configuration Steps](#) to migrate the configuration to FTD.

Note: Ensure that the required interfaces (Physical or Port-channel or Subinterface), Routes, NAT, Access Control Policies (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 [Smart Licensing Portal](#). In addition, ensure that Export-Controlled features are enabled.

Figure 3 – License Verification on FMC

Smart License Status

Usage Authorization: Authorized (Last Synchronized On Sep 10 2018)

Product Registration: Registered (Last Renewed On Jul 16 2018)

Assigned Virtual Account: JPT 63 Account

Expert-Controlled Features: Enabled

Cisco Success Network: Enabled

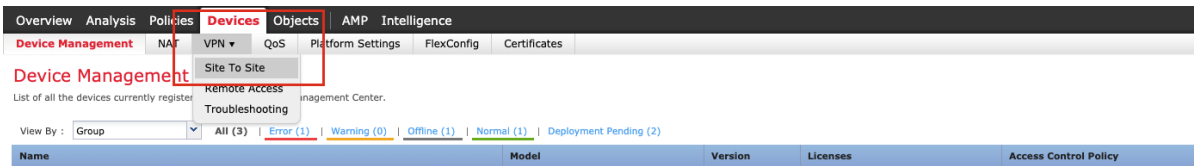
Smart Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
Firepower Management Center Virtual (1)	✓			
Base (1)	✓			
Malware (1)	✓			
Threat (1)	✓			
URL Filtering (1)	✓			
AnyConnect Apex (0)				
AnyConnect Plus (0)				
AnyConnect VPN Only (0)				

Configuration Procedure on FTD

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 (Hub and Spoke)**, the **IKE Version** as **IKEv1** and **IKEv2**. Click the **Plus (+)** icon to add a node for the VPN tunnel.

Figure 6 – Create New VPN Topology

Create New VPN Topology

Topology Name:*

Dynamic-Peers

Network Topology:

Point to Point

Hub and Spoke

Full Mesh

IKE Version:*

☒ IKEv1
☒ IKEv2

Endpoints

IKE

IPsec

Advanced

Hub Nodes:

Device Name	VPN Interface	Protected Networks

+

Spoke Nodes:

Device Name	VPN Interface	Protected Networks

+

ⓘ

Ensure the protected networks are allowed by access control policy of each device.

Save

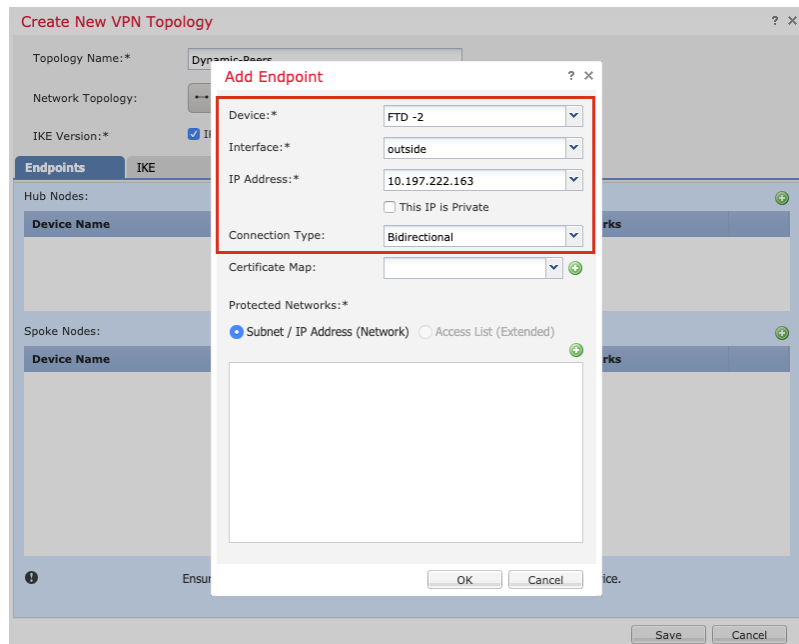
Cancel

The configuration that is displayed in [Figure 6](#) uses the following settings:

Settings	Values
Topology Name	Dynamic-Peers
Network Topology	Hub and Spoke
IKE Version	IKEv1 and IKEv2
Topology Name	Dynamic-Peers

- Step 4 For **Node A** representing the local endpoint of the VPN tunnel, click the **Plus (+)** icon to specify the target FTD details and do the following:
- Choose the **Target FTD** as **Device**.
 - Choose the interface on which the VPN terminates.
 - Select a **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
Connection Type	Bidirectional
Type of Protected Network	Subnet / IP Address (Network)

For FMC version 6.2.3 or earlier, use **Protected Networks** to add the **Local and Remote Network Objects** as displayed in [Figure 8](#).

Figure 8 – Add Local Protected Network (FMC version 6.2.3 or earlier)

The 'Edit Endpoint' dialog box is shown with the following fields:

- Device: * (Extranet)
- Device Name: * (Router)
- IP Address: * (10.106.52.213)
- Certificate Map: (empty)
- Protected Networks: * (REMOTE)

Buttons at the bottom: OK, Cancel.

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

Note: Set the **Local Network** to **any-ipv4** as you have created the dynamic crypto map.

Figure 9 – Add Local Protected Network (FMC version 6.2.3 or later)

The 'Create New VPN Topology' dialog box is shown with the following fields:

- Topology Name: * (Dynamic-Base)
- Network Topology: (empty)
- IKE Version: * (1)
- Endpoints: (selected)
- Hub Nodes: (empty)
- Spoke Nodes: (empty)
- Device Name: (empty)
- Protected Networks: * (any-ipv4)

Buttons at the bottom: OK, Cancel.

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

- Choose **Extranet** as **Device**.
- Enter the **Device Name** and **WAN IP Address** of the remote endpoint.
- Select **Remote Network** from **Protected Networks**.

- d. Click **OK** to save the endpoint configuration.

For FMC version 6.4.0 or later:

- You can choose Dynamic peer.
- As the **Remote Network** is unknown in a dynamic site-to-site tunnel, it is selected as **any-ipv4**. For more information, see [Figure 10](#).

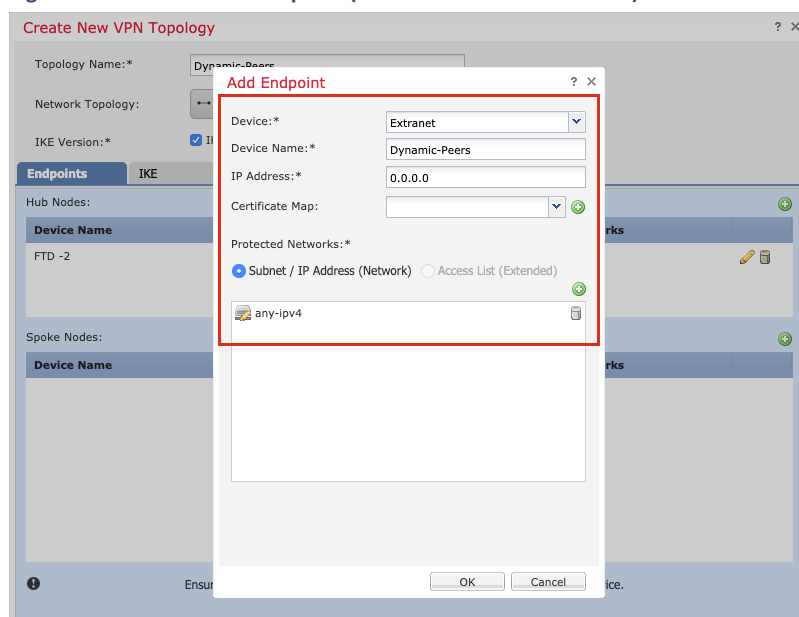
Figure 10 – Add Remote Endpoint (FMC version 6.4.0 or later)

The screenshot shows the 'Add Endpoint' dialog box. The 'Device:*' dropdown is set to 'Extranet'. The 'Device Name:*' text field contains 'Router'. The 'IP Address:*' section has two radio buttons: 'Static' and 'Dynamic', with 'Dynamic' selected. Below this is an 'IP address' text field. The 'Certificate Map:' dropdown is empty. The 'Protected Networks:*' section has two radio buttons: 'Subnet / IP Address (Network)' (selected) and 'Access List (Extended)'. Below this is a list box containing 'any-ipv4'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

For FMC version 6.4.0 or later:

- Use the IP address of the **remote end point** as **0.0.0.0** to create a dynamic crypto map on the FTD, as this is a dynamic site-to-site VPN tunnel.
- As the **Remote Network** is not known in a dynamic site-to-site tunnel, it is selected as **any-ipv4**.

Figure 11 – Add Remote Endpoint (FMC version 6.4.0 or earlier)



Note: There is no option to configure the tunnel-group name. The FMC deploys 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	Dynamic-Peers
IP Address	0.0.0.0

Step 7 Create a **New IKEv1 and IKEv2 Policy** to match the VPN Phase 1 settings existing on the ASA.

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

To create a new IKEv1 policy, do the following:

- Navigate to the **IKE** tab.
- Click the **Plus (+)** icon to add a new IKEv1 Policy.
- Specify the IKE parameters.
- Click **Save**.

Figure 12 - New IKEv1 Policy

The screenshot shows the 'New IKEv1 Policy' dialog box. The 'Name' field is set to 'IKEv1-AES-256-SHA'. The 'Encryption' dropdown is set to 'aes-256'. The 'Hash' dropdown is set to 'SHA'. The 'Diffie-Hellman Group' dropdown is set to '2'. The 'Lifetime' field is set to '86400' seconds. The 'Authentication Method' dropdown is set to 'Preshared Key'. The 'Priority' field is empty, with a default value of '(1-65535)' shown. The 'Description' field is empty. The 'Save' and 'Cancel' buttons are at the bottom right.

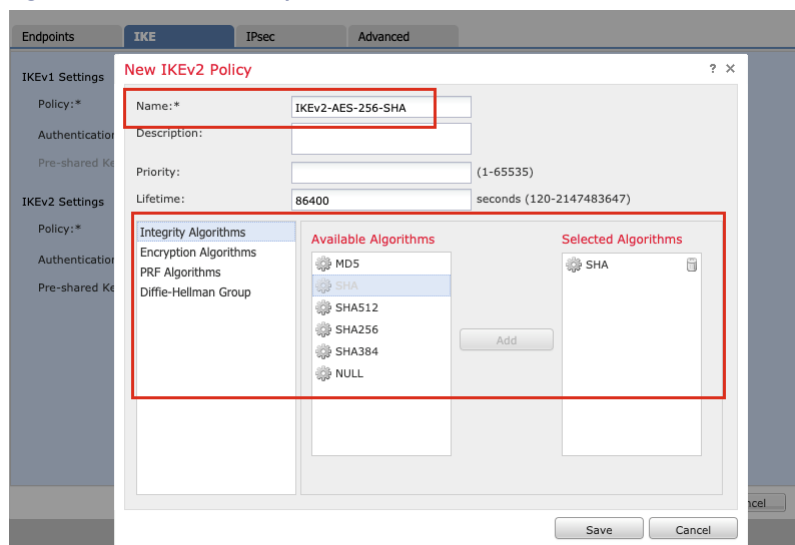
The configuration that is displayed in [Figure 12](#) uses the following settings:

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

To create a new IKEv2 policy, perform the following:

- Navigate to the **IKE** tab.
- Click the **Plus (+)** icon to add a new IKEv2 Policy.
- Specify the IKE parameters.
- Click **Save**.

Figure 13 – New IKEv2 Policy



The configuration that is displayed in [Figure 13](#) uses the following settings:

Settings	Values
Name	IKEv2-AES-256-SHA
Integrity Algorithm	SHA
Encryption Algorithm	AES-256
PRF Algorithm	SHA
Diffie-Hellman-Group	5

Step 8 Select the policy to be used for the VPN tunnel from the **Policy** drop-down list, and perform the following:

- Choose **Pre-shared Manual Key** from the **Authentication Type** drop-down list.
- Add and confirm the key in the clear text format.

Figure 14 – IKE Settings

Step 9 Create a new IKEv1 and IKEv2 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 **IPsec** tab.
- b. Click **Edit** to edit the default IKEv1 IPsec Proposal.
- c. Click the **Plus (+)** icon to add a new IKEv1 IPsec Proposal.
- d. Specify the IPsec parameters.
- e. Click **Save** to save the configuration.

Figure 15 – Create New IKEv1 IPsec Proposal

The configuration that is displayed in Figure 15 uses the following settings:

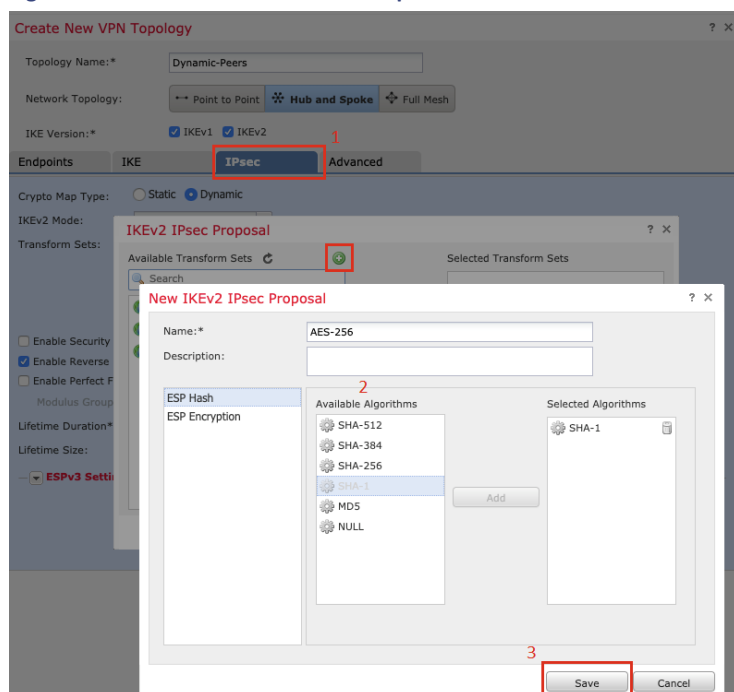
Settings	Values
Name	ESP-AES-SHA

Settings	Values
ESP Hash	SHA-1
ESP Encryption	AES-256

To create a new IKEv2 IPsec Proposal, perform the following:

- Navigate to **IPsec** tab.
- Click **Edit** to edit the default IKEv2 IPsec Proposal.
- Click the **Plus (+)** icon to add a new IKEv2 IPsec Proposal.
- Specify the IPsec parameters.
- Click **Save** to save the configuration.

Figure 16 – Create New IKEv2 IPsec Proposal



The configuration that is displayed in [Figure 16](#) uses the following settings:

Settings	Values
Name	AES-256
ESP Hash	SHA-1
ESP Encryption	AES-256

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

Figure 17 – Select IKEv1 IPsec Proposal

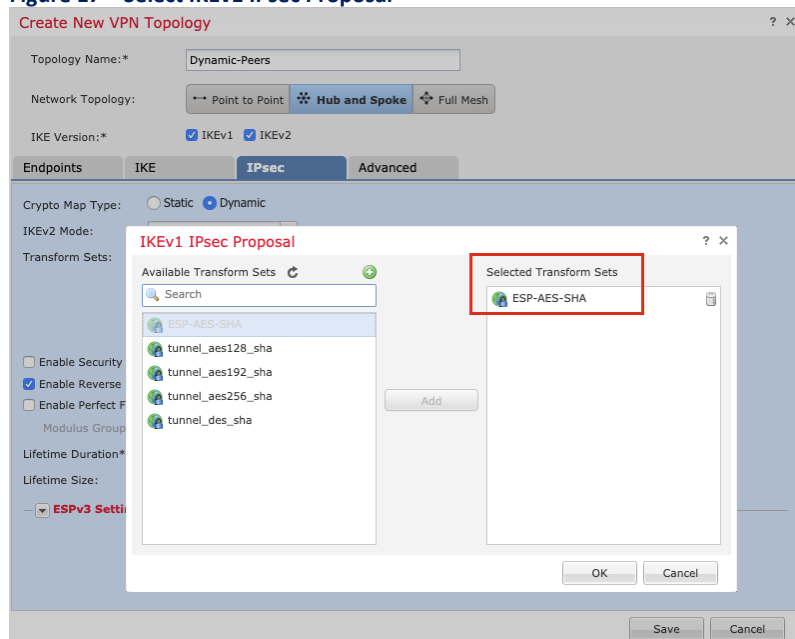
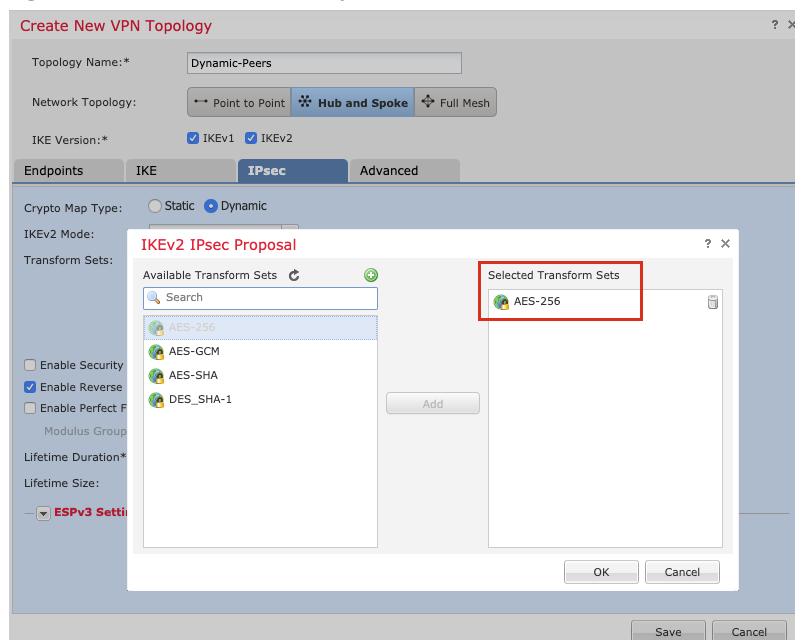


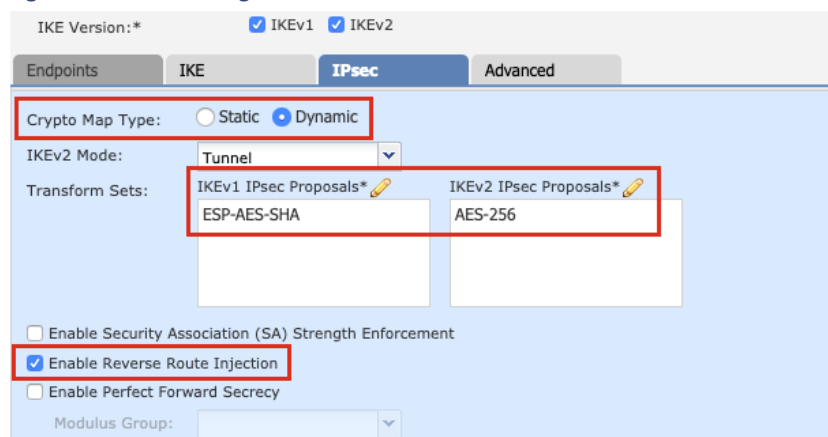
Figure 18 – Select IKEv2 IPsec Proposal



Step 11 Confirm that the selected IKEv1 and IKEv2 IPsec Proposal is displayed in the **Transform Sets**, and configure the IPsec settings by doing the following:

- Select **Crypto Map Type** as **Dynamic**.
- Check **Enable Reverse Route Injection** check box.

Figure 19 – 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 ACL 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 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 20 – Advanced VPN Tunnel Settings

Create New VPN Topology ? X

Topology Name:* Dynamic-Peers

Network Topology: ** Point to Point **Hub and Spoke** Full Mesh

IKE Version:* ☒ IKEv1 ☒ IKEv2

Endpoints IKE IPsec **Tunnel**

Advanced

Tunnel Options

☐ Enable Spoke to Spoke Connectivity through Hub
For spokes with dynamic IP addresses, "both" the spokes need to create "interesting" traffic to bring up the tunnels to the hub in order to have effective spoke-to-spoke traffic connectivity.

NAT Settings

☒ Keepalive Messages Traversal
Interval: 20 Seconds (Range 10 - 3600)

Access Control for VPN Traffic

☒ Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
Decrypted traffic is subjected to Access Control Policy by default. This option bypasses the inspection, but VPN Filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Certificate Map Settings

☐ Use the certificate map configured in the Endpoints to determine the tunnel

☒ Use the certificate OU field to determine the tunnel

☒ Use the IKE identity to determine the tunnel

☒ Use the peer IP address to determine the tunnel

Note: The **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 21 – Save VPN Settings

Create New VPN Topology

Topology Name: *

Network Topology: ☐ Point to Point ☒ Hub and Spoke ☐ Full Mesh

IKE Version: * ☒ IKEv1 ☒ IKEv2

Endpoints | IKE | IPsec | Advanced

Hub Nodes:

Device Name	VPN Interface	Protected Networks
FTD -2	outside/10.197.222.163	any-ipv4

Spoke Nodes:

Device Name	VPN Interface	Protected Networks
Dynamic-Peers	0.0.0.0	any-ipv4

Ensure the protected networks are allowed by access control policy of each device.

Save **Cancel**

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

Figure 22 – Deploy Policies

Deploy Policies Version: 2019-06-26 10:24 AM

Device	Inspect Interruption	Type	Group	Current Version
FTD -2	No	FTD		2019-06-06 12:05 PM
FTD -2	No	FTD		2019-06-22 06:11 AM
FTD -2	No	FTD		2019-06-06 12:05 PM

Selected devices: 1

Deploy **Cancel**

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==$Clzrb4ziPzWva0kLUr4iw== 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 any4 any4

----- 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 ikev2 ipsec-proposal CSM_IP_1

protocol esp encryption aes-256

protocol esp integrity sha-1

crypto ipsec security-association pmtu-aging infinite

crypto dynamic-map CSM_Outside_map_dynamic 1 match address CSM_IPSEC_ACL_1

crypto dynamic-map CSM_Outside_map_dynamic 1 set ikev1 transform-set CSM_TS_1

crypto dynamic-map CSM_Outside_map_dynamic 1 set ikev2 ipsec-proposal CSM_IP_1

crypto dynamic-map CSM_Outside_map_dynamic 1 set reverse-route

```
crypto map CSM_Outside_map 30000 ipsec-isakmp dynamic CSM_Outside_map_dynamic
```

```
crypto map CSM_Outside_map interface Outside
```

```
crypto ikev2 policy 1
```

```
encryption aes-256
```

```
integrity sha
```

```
group 5
```

```
prf sha
```

```
lifetime seconds 86400
```

```
crypto ikev2 enable Outside
```

```
crypto ikev1 enable Outside
```

```
crypto ikev1 am-disable
```

```
crypto ikev1 policy 1
```

```
authentication pre-share
```

```
encryption aes-256
```

```
hash sha
```

```
group 2
```

```
lifetime 86400
```

```
----- Output Omitted -----
```

```
tunnel-group DefaultL2LGroup type ipsec-l2l
```

```
tunnel-group DefaultL2LGroup general-attributes
```

```
default-group-policy .DefaultS2SGroupPolicy
```

```
tunnel-group DefaultL2LGroup ipsec-attributes
```

```
ikev1 pre-shared-key *****
```

```
ikev2 remote-authentication pre-shared-key *****
```

```
ikev2 local-authentication pre-shared-key *****
```

```
!
```

```
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 ikev2
!
dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
  match default-inspection-traffic
!
----- Output Omitted -----
Cryptochecksum:b76f6eee4099a9a021b6adb496bee827
: end
firepower#
```

Note: You cannot perform the following:

- Modify the name of the dynamic crypto map because it is a system-defined name.
- Change the sequence number of the dynamic crypto map from the FMC.

Exception Cases for Migrating from ASA to FTD

VPN Settings Under Group-policy Attributes

- Changing the **vpn-idle-timeout** in the group-policy
- Configuration on ASA

```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
  vpn-idle-timeout 60
!
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup ipsec-attributes
  ikev1 pre-shared-key *****
  ikev2 remote-authentication pre-shared-key *****
  ikev2 local-authentication pre-shared-key *****
```

Note:

- Any setting in the **DfltGrpPolicy** affects all the VPN tunnels on the device (unless there is another group-policy that is bound to the tunnel-group overriding this setting).
- Use **FlexConfig** on the FTD to add a configuration similar to the ASA configuration to the FTD, as these options are not currently supported from the FMC GUI.
- Any change made to the **DefaultS2SGroupPolicy** affects all the VPN tunnels on the FTD and to any tunnel created eventually.

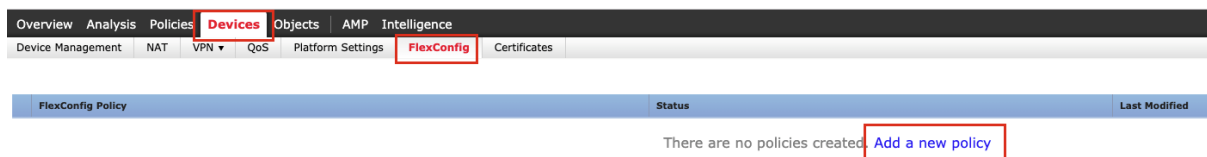
Configuration on FTD before Deployment

```
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
default-group-policy .DefaultS2SGroupPolicy
tunnel-group DefaultL2LGroup ipsec-attributes
ikev1 pre-shared-key *****
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
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
```

FlexConfig Steps

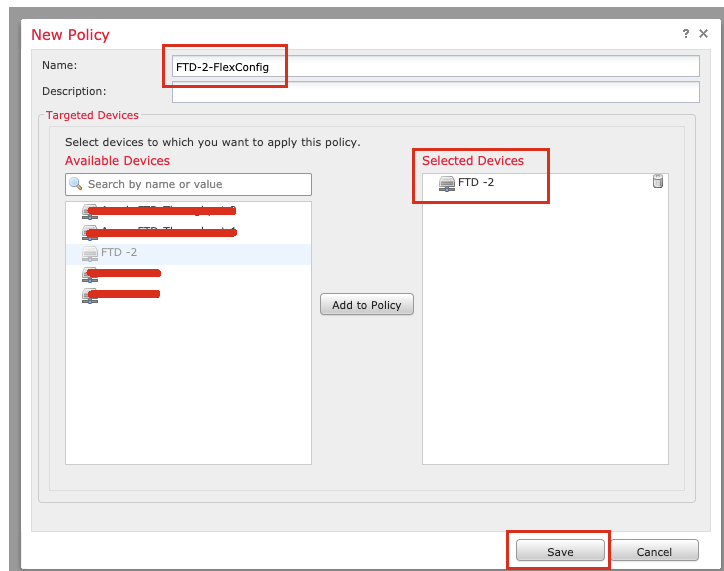
Step 1 Navigate to **Devices > FlexConfig**. Click **Add a new policy** or **Edit an existing policy**.

Figure 23 - Add New FlexConfig Policy



Step 2 Enter a name for the **FlexConfig Policy**. Select the **FTD** to which the **FlexConfig Policy** must be applied.

Figure 24 – Bind to FTD

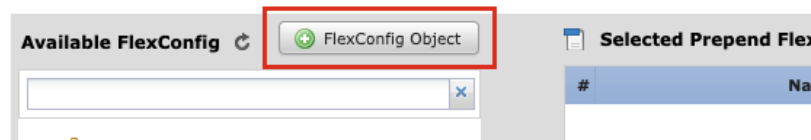


Step 3 Click the **Plus (+)** icon to add a new **FlexConfig Object**.

Figure 25 – New FlexConfig Object

FTD-2-FlexConfig

Enter Description



- Step 4 Enter a name for the **FlexConfig Object** that refers the changes in the group-policy settings, and then do the following.
- Set the **Deployment** to **Everytime** and **Type** as **Append**.
 - Click **Save** to create the **FlexConfig Object**.

Figure 26 – Define FlexConfig Object

Add FlexConfig Object

Name: VPN-Settings-Group-Policy

Description:

Insert: [icon] [icon]

Deployment: Everytime Type: Append

```
group-policy .DefaultS2SGroupPolicy attributes
vpn-idle-timeout 60
```

Variables

Name	Dimension	Default Value	Property (Ty...	Override	Description
No records to display					

Save Cancel

Use the following content for the group-policy for the configuration example shown in Figure 26.

```
group-policy .DefaultS2SGroupPolicy attributes
vpn-idle-timeout 60
```

Step 5 Select the **FlexConfig Object** from the list of **Available FlexConfig**. Click > to add the object to be deployed to the FTD.

Figure 27 - Add FlexConfig Object to FlexConfig Policy

Available FlexConfig FlexConfig Object

User Defined

- VPN-Settings-Group-Policy

System Defined

- Default_DNS_Configure
- Default_Inspection_Protocol_Disable
- Default_Inspection_Protocol_Enable
- DHCPv6_Prefix_Delegation_Configure
- DHCPv6_Prefix_Delegation_UnConfigure
- DNS_Configure
- DNS_UnConfigure
- Eigrp_Configure
- Eigrp_Interface_Configure
- Eigrp_UnConfigure
- Eigrp_UnConfigure_All
- Inspect_IPv6_Configure
- Inspect_IPv6_UnConfigure

>

Selected Prepend FlexConfigs

#	Name
---	------

Selected Append FlexConfigs

#	Name
---	------

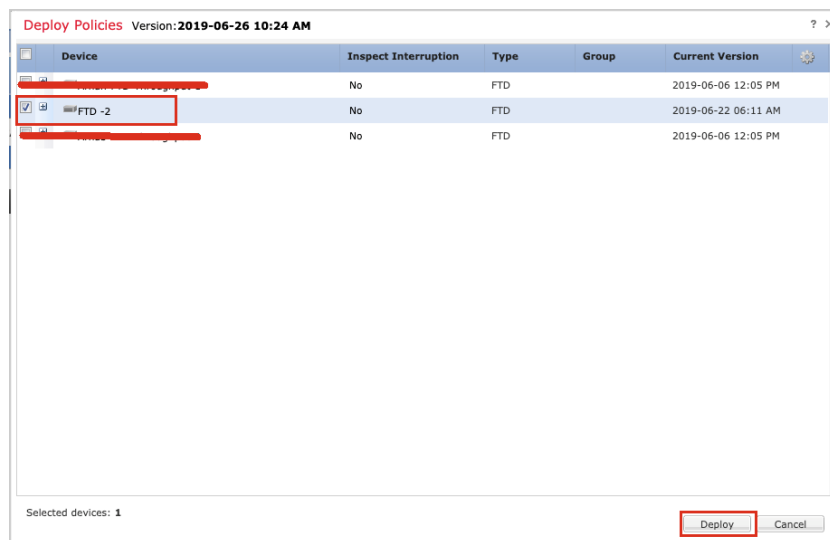
Step 6 Click **Save** to save the **FlexConfig Policy** on the FMC.

Figure 28 - Save FlexConfig Policy



Step 7 Select the device to deploy the changes, and click **Deploy**.

Figure 29 – Deploy Policies



Configuration on FTD after Deployment

```
tunnel-group DefaultL2LGroup type ipsec-l2l
tunnel-group DefaultL2LGroup general-attributes
default-group-policy .DefaultS2SGroupPolicy
tunnel-group DefaultL2LGroup ipsec-attributes
ikev1 pre-shared-key *****
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
group-policy .DefaultS2SGroupPolicy internal
group-policy .DefaultS2SGroupPolicy attributes
vpn-idle-timeout 60
vpn-idle-timeout alert-interval 1
```

```
vpn-session-timeout none

vpn-session-timeout alert-interval 1

vpn-filter none

vpn-tunnel-protocol ikev1
```

Number of IKE Policies More than the number of Tunnels on the FTD

The following example provides the configuration sample, when there are two IKEv1 and IKEv2 policies, but only one VPN tunnel is available on the ASA.

Configuration on ASA

```
crypto dynamic-map DMAP 1 set ikev1 transform-set ESP-AES-SHA

crypto dynamic-map DMAP 1 set ikev2 ipsec-proposal AES

crypto dynamic-map DMAP 1 set reverse-route

crypto map CMAP 65535 ipsec-isakmp dynamic DMAP

crypto map CMAP interface outside

crypto ca trustpool policy

crypto ikev2 policy 1

  encryption aes-256

  integrity sha

  group 5

  prf sha

  lifetime seconds 86400

crypto ikev2 policy 20

  encryption aes

  integrity sha256

  group 2

  prf sha

  lifetime seconds 86400

crypto ikev2 enable outside

crypto ikev1 enable outside

crypto ikev1 policy 1

  authentication pre-share

  encryption aes-256
```

```

hash sha
group 2
lifetime 86400

crypto ikev1 policy 2
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

```

Due to the default behavior on the FTD, there is only one IKEv1 and IKEv2 policy that is bound to one VPN tunnel.

To check the VPN Phase 1 parameters in use by the VPN tunnel, see [Verification of VPN Tunnel Status on ASA](#).

To configure more number of IKEv1 and IKEv2 policies than the number of VPN tunnels on the FTD, use FlexConfig to deploy the additional IKEv1 and IKEv2 policies to the FTD CLI.

Configuration on FTD before Deployment

```

crypto dynamic-map CSM_Outside_map_dynamic 1 match address CSM_IPSEC_ACL_1

crypto dynamic-map CSM_Outside_map_dynamic 1 set ikev1 transform-set CSM_TS_1

crypto dynamic-map CSM_Outside_map_dynamic 1 set ikev2 ipsec-proposal CSM_IP_1

crypto dynamic-map CSM_Outside_map_dynamic 1 set reverse-route

crypto map CSM_Outside_map 30000 ipsec-isakmp dynamic CSM_Outside_map_dynamic

crypto map CSM_Outside_map interface Outside

crypto ikev2 policy 1
encryption aes-256
integrity sha
group 5
prf sha
lifetime seconds 86400

crypto ikev2 enable Outside

crypto ikev1 enable Outside

crypto ikev1 am-disable

crypto ikev1 policy 1
authentication pre-share
encryption aes-256
hash sha

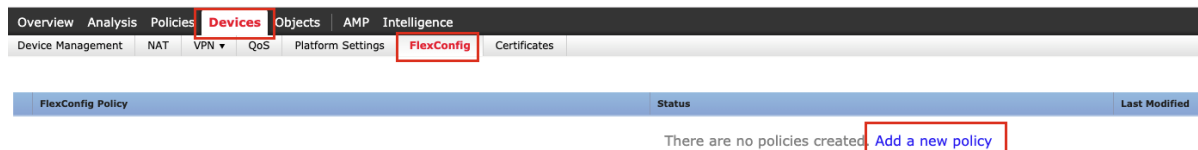
```

group 2
lifetime 86400

FlexConfig Steps

Step 1 Navigate to **Devices > FlexConfig**. Click **Add a new policy** or **Edit an existing policy**.

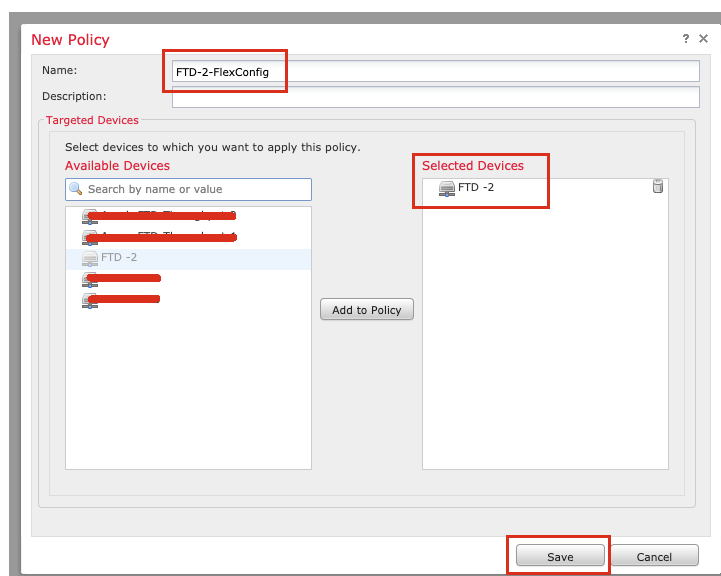
Figure 30 – Add new FlexConfig Policy



Step 2 Enter a name for the **FlexConfig Policy**.

Step 3 Select the **FTD** to which the **FlexConfig Policy** must be applied.

Figure 31 – Bind to FTD

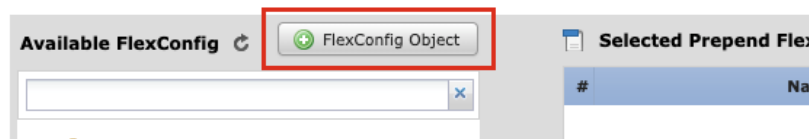


Step 4 Click the **Plus (+)** icon to add a new **FlexConfig Object**.

Figure 32 – New FlexConfig Object

FTD-2-FlexConfig

Enter Description



- Step 5 Enter a name for the **FlexConfig Object** that refers the additional IKEv1 policies.
- Set the **Deployment** to **Everytime** and **Type** as **Append**.
 - Click **Save** to create the **FlexConfig Object**.

Figure 33 - Define FlexConfig Object

Name:

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert

```
crypt ikev1 policy 2
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
```

Variables

Name	Dimension	Default Value	Property (Typ...	Override	Description
No records to display					

Use the following content for IKEv1 policy for the configuration example shown in [Figure 33](#).

```
crypt ikev1 policy 2
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
```

- Step 6 Enter a name for the **FlexConfig Object** that refers the additional IKEv2 policies.
- Set the **Deployment** to **Everytime** and **Type** as **Append**.
 - Click **Save** to create the **FlexConfig Object**.

Figure 34 – Define FlexConfig Object

Name: IKEv2-policy-2

Description:

⚠ Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert: [Icons] Deployment: Everytime Type: Append

```
crypt ikev2 policy 20
encryption aes
integrity sha256
group 2
prf sha
lifetime seconds 86400
```

Name	Dimension	Default Value	Property (Typ...	Override	Description
No records to display					

Save Cancel

Use the following content for IKEv2 policy for the configuration example shown in [Figure 34](#).

```
crypt ikev2 policy 20

encryption aes

integrity sha256

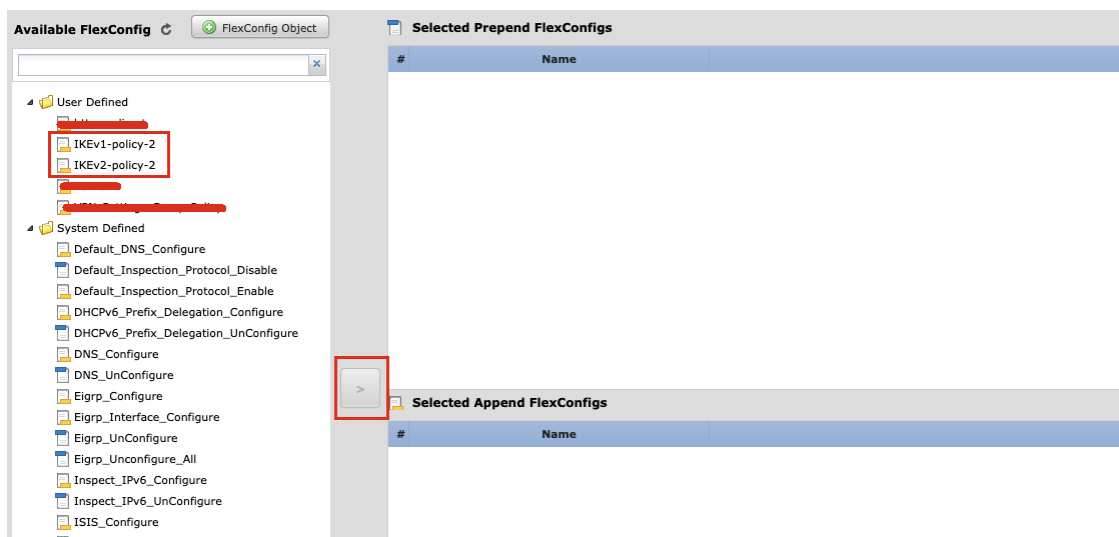
group 2

prf sha

lifetime seconds 86400
```

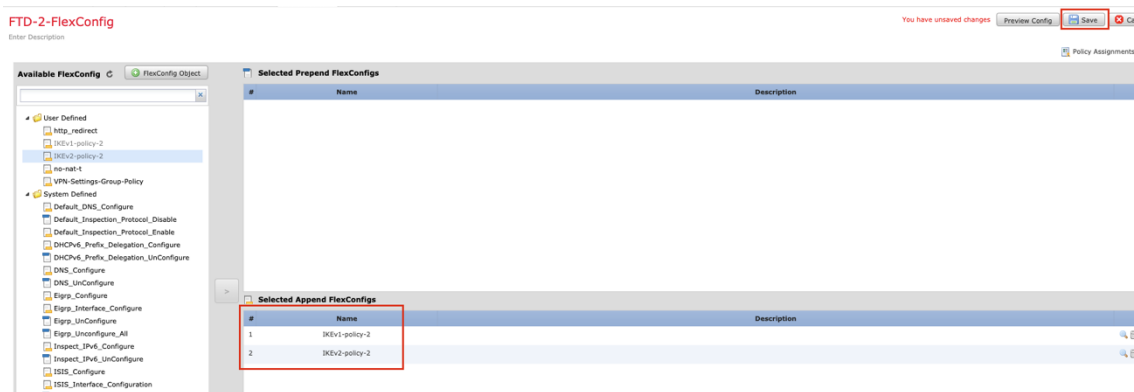
Step 7 Select the **FlexConfig Objects** from the list of **Available FlexConfig**. Click the > icon to add the objects to be deployed to the FTD.

Figure 35 – Add FlexConfig Object to FlexConfig Policy



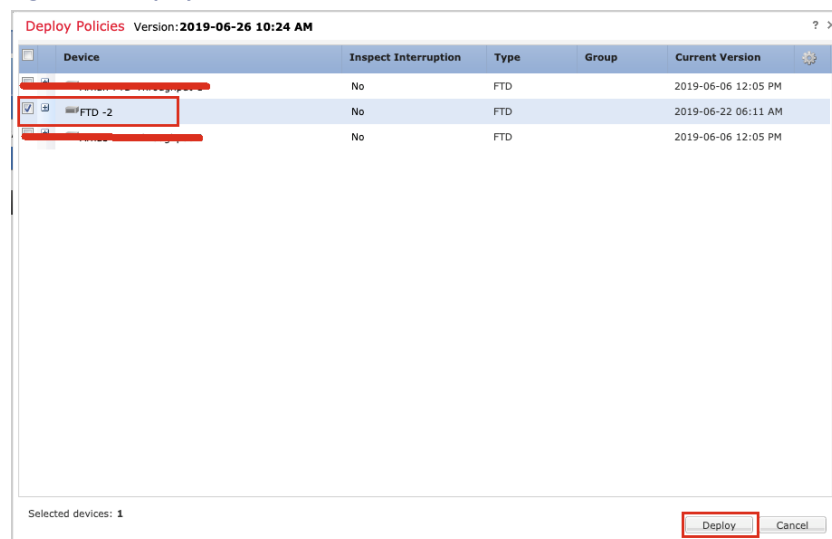
Step 8 Click **Save** to save the **FlexConfig Policy** on the FMC.

Figure 36 – Save FlexConfig Policy



Step 9 Select the device to deploy the changes, and click **Deploy**.

Figure 37 – Deploy Policies



Configuration on FTD after Deployment

```
crypto dynamic-map CSM_Outside_map_dynamic 1 match address CSM_IPSEC_ACL_1
crypto dynamic-map CSM_Outside_map_dynamic 1 set ikev1 transform-set CSM_TS_1
crypto dynamic-map CSM_Outside_map_dynamic 1 set ikev2 ipsec-proposal CSM_IP_1
crypto dynamic-map CSM_Outside_map_dynamic 1 set reverse-route
crypto map CSM_Outside_map 30000 ipsec-isakmp dynamic CSM_Outside_map_dynamic
crypto map CSM_Outside_map interface Outside

crypto ikev2 policy 1
  encryption aes-256
  integrity sha
  group 5
  prf sha
  lifetime seconds 86400

crypto ikev2 policy 20
  encryption aes
  integrity sha256
  group 2
  prf sha
  lifetime seconds 86400

crypto ikev2 enable Outside
crypto ikev1 enable Outside
```


Exception Cases for Migrating from ASA to FTD

```
crypto ikev1 am-disable
```

```
crypto ikev1 policy 1
```

```
authentication pre-share
```

```
encryption aes-256
```

```
hash sha
```

```
group 2
```

```
lifetime 86400
```

```
crypto ikev1 policy 2
```

```
authentication pre-share
```

```
encryption 3des
```

```
hash sha
```

```
group 2
```

```
lifetime 86400
```