Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

September 3, 2019
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

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 ......................................................................................... 7
Topology ............................................................................................................................................... 9
Configuration on FTD .......................................................................................................................... 9
Network Diagram............................................................................................................................... 9
License Verification on FMC ................................................................................................................. 9
Configuration Procedure on FTD ....................................................................................................... 10
Configuration on FTD Post Deployment .......................................................................................... 20
Exception Cases for Migrating from ASA to FTD ........................................................................... 23
VPN Settings under Group-policy Attributes .................................................................................... 23
Number of IKEv2 Policies More than the Number of Tunnels on the FTD ........................................... 31
Introduction

This document describes the procedure to migrate site-to-site IKEv2 VPN tunnels using pre-shared key (PSK) 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 --------

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 ikev2 ipsec-proposal AES-256
protocol esp encryption aes-256
protocol esp integrity sha-1
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 ikev2 ipsec-proposal AES-256
crypto map CMAP interface outside
crypto ca trustpool policy
crypto ikev2 policy 10
  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

----------- 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
  ikev2 remote-authentication pre-shared-key *****
  ikev2 local-authentication pre-shared-key *****
!
----------- Output Omitted -----------
Cryptoschecksum: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 10.106.52.213
```

```
tunnel-group 10.106.52.213 type ipsec-l2l
  tunnel-group 10.106.52.213 ipsec-attributes
    ikev2 remote-authentication pre-shared-key cisco123
    ikev2 local-authentication pre-shared-key cisco123
```

**Verification of VPN Tunnel Status on ASA**

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

```
ASA# show crypto ikev2 sa detail
```

```
IKEv2 SAs:
  Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                                               Remote                                                  Status  Role
7851179 10.197.222.163/500                                   10.106.52.213/500                                        READY  RESPONDER

  Life/Active Time: 86400/17 sec
  Session-id: 1
  Status Description: Negotiation done
  Local spi: 971C4CC10C9A9C0A       Remote spi: D37FA629892809DD
  Local id: 10.197.222.163
  Remote id: 10.106.52.213
  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
```
Verification of VPN Tunnel Status on ASA

The above sample 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.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Topology

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/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.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Configuration on FTD

Figure 3 – License Verification on FMC

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 (Point to Point), and the IKE Version as IKEv2. Click the Plus (+) symbol to add a node for the VPN tunnel.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Configuration on FTD

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>IKEv2</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**.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Configuration on FTD

Figure 7 – Add Local Endpoint

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>Connection Type</td>
<td>Bidirectional</td>
</tr>
<tr>
<td>Protected Network</td>
<td>Subnet / IP Address (Network)</td>
</tr>
</tbody>
</table>

**Note**: If you require more details on the networks that needs to 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.
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 the Protected Network, and click OK to save the endpoint configuration.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Configuration on FTD

Figure 10 – Add Local Protected Network (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 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:
Create a new IKEv2 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.

To create a new IKEv2 policy, perform the following:

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

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>IKEv2-AES-256-SHA</td>
</tr>
<tr>
<td>Integrity Algorithm</td>
<td>SHA</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>aes-256</td>
</tr>
<tr>
<td>PRF Algorithm</td>
<td>SHA</td>
</tr>
<tr>
<td>Diffie-Hellman-Group</td>
<td>5</td>
</tr>
</tbody>
</table>
### Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

<table>
<thead>
<tr>
<th>Settings</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lifetime</td>
<td>86400</td>
</tr>
</tbody>
</table>

**Step 8**  
Select the policy to be used for the VPN tunnel from the **Policy** drop-down list, and perform the following:  
- a. Choose **Pre-shared Manual Key** from the **Authentication Type** drop-down list.  
- b. Add and confirm the key in the clear text format.

**Figure 13 – IKE Settings**

![IKEV2 Settings](image)

**Step 9**  
Create a **New 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 IKEv2 IPsec proposal, perform the following:  
- a. Navigate to **IPsec** tab.  
- b. Click **Edit** to edit the default IKEv2 IPsec Proposal.  
- c. Click the **Plus (+)** symbol to add a new IKEv2 IPsec Proposal.  
- d. Specify the IPsec parameters.  
- e. Click **Save** to save the configuration.
Figure 14 – Create New IKEv2 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>AES-256</td>
</tr>
<tr>
<td>ESP Hash</td>
<td>SHA-1</td>
</tr>
<tr>
<td>ESP Encryption</td>
<td>AES-256</td>
</tr>
</tbody>
</table>

Step 10 Select the IPsec Transform Set from the list of the Available Transform Sets.
Figure 15 – Select IKEv2 IPsec Proposal

Step 11 Confirm that the selected IKEv2 IPsec Proposal is displayed in the IKEv2 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 the 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:

```plaintext
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
```
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Configuration on FTD

**Figure 17 - Advanced VPN Tunnel Settings**

![Advanced VPN Tunnel Settings](image)

**Note:** The Access Control for VPN traffic check box 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**

![Save VPN Settings](image)

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

no sysopt noproxyarp outside
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Configuration on FTD

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

```plaintext
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+5vTg==$Clzrqb4ziPzva0kLUr4iw== 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 10.197.222.163 255.255.255.254.0

--- 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 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 ikev2 ipsec-proposal CSM_IP_1
protocol esp encryption aes-256
protocol esp integrity sha-1
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 ikev2 ipsec-proposal CSM_IP_1
crypto map CSM_Outside_map interface outside
crypto ikev2 policy 10
encryption aes-256
integrity sha
    group 5
    prf sha
    lifetime seconds 86400
crypto ikev2 enable outside
---------- 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
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
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Exception Cases for Migrating from ASA to FTD

VPN Settings under Group-policy Attributes

a. Changing the `vpn-idle-timeout` in the group-policy.
b. Adding a `VPN filter` in the group-policy.

Configuration on ASA

```plaintext
access-list VPN-Filter-S2S-10.106.52.213 extended permit tcp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0

group-policy Group-Policy-10.106.52.213 internal
group-policy Group-Policy-10.106.52.213 attributes
  vpn-idle-timeout 60
  vpn-filter value VPN-Filter-S2S-10.106.52.213

tunnel-group 10.106.52.213 type ipsec-l2l
tunnel-group 10.106.52.213 general-attributes
default-group-policy Group-Policy-10.106.52.213
tunnel-group 10.106.52.213 ipsec-attributes
  ikev2 remote-authentication pre-shared-key *****
  ikev2 local-authentication pre-shared-key *****
```

Note: The name of the crypto map is a system defined name and cannot be modified. The sequence number of the crypto map cannot be changed from the FMC.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Exception Cases for Migrating from ASA to FTD

To add a configuration similar to the ASA configuration to the FTD, use FlexConfig on the FTD as these options are not currently supported from the FMC GUI.

Configuration on FTD before Deployment

```
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
    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 ikev2
```

FlexConfig Steps

Step 1  Navigate to Objects > Object Management > Access List > Extended. Click the Plus (+) symbol to add a new access list that will be used as the VPN filter.

Figure 20 – Create New Access List

Step 2  Navigate to Network > Add Source and Destination Networks.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Exception Cases for Migrating from ASA to FTD

Figure 21 – Define Access List Network Parameters

Step 3 Navigate to Port > Add the specific ports that need to be allowed, and Click Save.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Exception Cases for Migrating from ASA to FTD

Figure 22 – Define Access List Port Parameters

Step 4 Verify if the ACL entry is valid, and click Save.

Figure 23 - Save Access List

Step 5 Navigate to Devices > FlexConfig. Click Add a new Policy or Edit an existing policy.

Figure 24 - Add New FlexConfig Policy

Step 6 Enter a name for the FlexConfig Policy. Select the FTD to which the FlexConfig Policy must be applied.
Figure 25 – Bind to FTD

Step 7  Click the Plus (+) symbol to add a new FlexConfig Object.

Figure 26 – New FlexConfig object

Step 8  Enter a name for the FlexConfig Object that will refer to the changes in the group-policy settings.
   a. Set the Deployment to Once and Type as Append.
   b. Configure a new Policy.
   c. Navigate to Object > Extended ACL Object.
   d. Choose the ACL created in Step 4.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Exception Cases for Migrating from ASA to FTD

Figure 27 - Define FlexConfig Object

For the configuration example shown in Figure 27, the following content for the group-policy has been used.

```
   group-polic Group-Policy-10.106.52.213 internal
   group-polic Group-Policy-10.106.52.213 attributes
   vpn-idle-timeout 60
   vpn-filter value $test
```

Step 9  Click Save to create the FlexConfig Object.

Figure 28 - Save FlexConfig Object

Step 10  Enter a name for the FlexConfig Object that will refer the binding of the group-policy with the tunnel-group that is created during site-to-site tunnel configuration.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Exception Cases for Migrating from ASA to FTD

a. Set the Deployment to Everytime and Type as Append.

b. Click Save to create the FlexConfig Object.

Figure 29 - Define FlexConfig Object

For the configuration example shown in Figure 29, the following content for the group-policy is used.

tunnel-group 10.106.52.213 general-attribut
default-group-policy Group-Policy-10.106.52.213

Step 11 Select the FlexConfig Objects from the list of Available FlexConfig. Click > to add the objects to be deployed to the FTD.

Figure 30 – Add FlexConfig Object to FlexConfig Policy

Step 12 Click Save to save the FlexConfig Policy on the FMC.
Step 13 Select the device to deploy the changes, and click **Deploy**.

**Figure 32 – Deploy Policies**

Configuration on FTD after Deployment

```
access-list VPN-Filter-S2S-10.106.52.213 extended permit object-group ProxySG_ExtendedACL_12884902577 object REMOTE object LOCAL log

group-policy Group-Policy-10.106.52.213 internal

group-policy Group-Policy-10.106.52.213 attributes

vpn-idle-timeout 60

vpn-filter value VPN-Filter-S2S-10.106.52.213

tunnel-group 10.106.52.213 type ipsec-l2l

tunnel-group 10.106.52.213 general-attributes

default-group-policy Group-Policy-10.106.52.213

tunnel-group 10.106.52.213 ipsec-attributes
```
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 ikev2

Number of IKEv2 Policies More than the Number of Tunnels on the FTD

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

**Configuration on ASA**

```
crypto map CMAP 1 match address cryptoacl  
crypto map CMAP 1 set peer 10.106.52.213  
crypto map CMAP 1 set ikev2 ipsec-proposal AES-256  
crypto map CMAP interface outside

--------- Output Omitted ---------
crypto ikev2 policy 10  
  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
```
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Exception Cases for Migrating from ASA to FTD

---

Due to the default behavior on the FTD, there is only one IKEv2 policy bound to one VPN tunnel.
To check the VPN Phase 1 parameters in use by the VPN tunnel, see Verification of VPN tunnel on ASA.
To configure more number of IKEv2 policies than the number of VPN tunnels on the FTD, use FlexConfig to deploy the additional IKEv2 policies to the FTD CLI.

**Configuration on FTD before Deployment**

```plaintext
crypto ikev2 enable outside

due to the default behavior on the FTD, there is only one IKEv2 policy bound to one VPN tunnel.
to check the VPN Phase 1 parameters in use by the VPN tunnel, see verification of VPN tunnel on ASA.
to configure more number of IKEv2 policies than the number of VPN tunnels on the FTD, use FlexConfig to deploy the additional IKEv2 policies to the FTD CLI.

---

**FlexConfig Steps**

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

**Figure 33 – Add New FlexConfig Policy**

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

**Step 2** Enter a name for the FlexConfig Policy. Select the FTD to which the FlexConfig Policy must be applied.
Figure 34 – Bind to FTD

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

Figure 35 – New FlexConfig Object

FTD-2-FlexConfig

Enter Description

Step 4  Enter a name for the FlexConfig Object that will refer the additional IKEv2 policies.

a.  Set the Deployment to Everytime and Type as Append.

b.  Click Save to create the FlexConfig Object.
Figure 36 - Define FlexConfig Object

For the configuration example shown in Figure 36, the following content for IKEv2 policy has been used.

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

Step 5 Select the FlexConfig Object from the list of Available FlexConfig. Click > to add the object to be deployed to the FTD.
Migrating ASA to Firepower Threat Defense—Site-to-Site VPN Using IKEv2 with Pre-Shared Key Authentication

Exception Cases for Migrating from ASA to FTD

Figure 37 – Add FlexConfig Object to FlexConfig Policy

**FTD-2-FlexConfig**

Enter Description

- Available FlexConfig
- Selected Prepend FlexConfigs
- Selected Append FlexConfigs

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

Figure 38 – Save FlexConfig Policy

Step 7  
Select the device to deploy the changes, and click **Deploy**.
Figure 39 – Deploy Policies

<table>
<thead>
<tr>
<th>Device</th>
<th>Inspect</th>
<th>Signature</th>
<th>Type</th>
<th>Group</th>
<th>Current Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA -</td>
<td>No</td>
<td>No</td>
<td>FTD</td>
<td></td>
<td>2019-09-16 12:05 AM</td>
</tr>
<tr>
<td>ASA</td>
<td>No</td>
<td>No</td>
<td>FTD</td>
<td></td>
<td>2019-09-16 12:05 AM</td>
</tr>
<tr>
<td>ASA</td>
<td>No</td>
<td>No</td>
<td>FTD</td>
<td></td>
<td>2019-09-16 12:05 AM</td>
</tr>
</tbody>
</table>

Configuration on FTD after Deployment

```plaintext
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 ikev2 ipsec-proposal CSM_IP_1
crypto map CSM_Outside_map interface Outside

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

crypto ikev2 policy 10
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
```