Migrating ASA to Firepower Threat Defense Platform Settings

November 14, 2019
Migrating ASA to Firepower Threat Defense Platform Settings

Introduction

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  
**Interface Zones/Groups** ............................................................................................................................... 4  
**Network Objects and Port Objects** ............................................................................................................... 10  
**Licensing** .................................................................................................................................................... 17  
**Create Platform Setting Policy on FMC** ....................................................................................................... 18  
**Configure Feature/Parameter in the Platform Setting Policy** ........................................................................ 19  
  - Configure ARP Inspection .......................................................................................................................... 19  
  - Configure Login Banner ............................................................................................................................ 24  
  - Configure DNS ........................................................................................................................................... 26  
  - Configure External Authentication ............................................................................................................. 30  
  - Configure Fragment Handling .................................................................................................................... 34  
  - Configure HTTP ......................................................................................................................................... 38  
  - Configure ICMP .......................................................................................................................................... 41  
  - Configure Secure Shell (SSH) .................................................................................................................... 46  
  - Configure SMTP Server ............................................................................................................................. 50  
  - Configure SNMP ......................................................................................................................................... 52  
  - Configure SSL ........................................................................................................................................... 60  
  - Configure Syslog ......................................................................................................................................... 65  
  - Configure Timeout ..................................................................................................................................... 74  
  - Configure Time Synchronization ................................................................................................................ 76  
  - Configure UCAPL/CC Compliance ............................................................................................................. 79
Introduction

This guide describes the steps to migrate the platform setting configuration of Cisco Adaptive Security Appliance (ASA) to Firepower Threat Defense (FTD) devices.

The following are the set of features that can be defined in the policy for the managed FTD device.

- Configure ARP Solution
- Configure Login Banner
- Configure DNS
- Configure External Authentication
- Configure Fragment Handling
- Configure HTTP
- Configure ICMP
- Configure Secure Shell (SSH)
- Configure SMTP Server
- Configure SNMP
- Configure SSL
- Configure Syslog
- Configure Timeout
- Configure Time Synchronization
- Configure UCAPL/CC Compliance

Interface Zones/Groups

The interface zones/group mapping will be migrated as a part of Firepower migration using the tool.

You can also create new zone/interface manually on new or existing FMC.

a. **Security Zones/Interface Groups** — There are two types of interface objects which help the device to manage the network segments and classify traffic flow in various policies and configuration:
   - Security zones—One or multiple interfaces can belong to one security zone.
   - Interface groups—An interface can belong to multiple interface groups (and to one security zone).

To create security zones:

Step 1 Navigate to **Objects > Object Management > Interface**.

Step 2 Click ![Add](Add_icon) and from the drop-down list choose to add **Security Zone** or **Interface group**.
Interface Zones/Groups

Figure 1 — Add Security Zone/Interface Group

Step 3  Enter the security zone name in the Name field.

**Note**—The object names must be unique on FMC.

In a multidomain deployment, object names should be unique within the domain hierarchy. The system may identify a conflict with the name of an object you cannot view in your current domain.

Step 4  Choose an Interface Type for the zone/group.

Step 5  From the Available Interfaces section, choose a device that contains interfaces you want to add to the zone/group.

**Note**—Only the named interfaces are available in the Available Interfaces.

Step 6  Click Add to add the interfaces to the Security zone or Interface group which reflects under Selected Interfaces.

Figure 2 — Creating Security Zone
Migrating ASA to Firepower Threat Defense Platform Settings

Interface Zones/Groups

Figure 3—Creating Interface Group

Step 7 Click **Save**.

a. **Interfaces**—To create new interface on the managed device:

Step 1 Navigate to **Devices > Device Management** and click **Edit** on your Managed device (Firepower Threat Defense). The **Interfaces** tab is selected by default.

Figure 4—Configuring Interface

Step 2 Click **Edit** for the interface you want to edit. In the **Mode** drop-down list, choose **None**, the Regular firewall interfaces have the mode set to **None**. The other modes are for IPS-only interface types. Assign the security zone for the interface.

You can create a new zone by selecting **New** from drop-down list of **Security Zone** tab.

**Security Zone > New > New Security Zone: Enter the Name**
You can assign the existing security zone available on the FMC or create new zone.

Step 3  Enable the interface by checking the Enabled check box. Assign IP address to the interface under section IPv4 or IPv6.
Step 4  (Optional) Add a description in the **Description** field. The description can be up to 200 characters in a single line, without carriage returns (ASCII value 13, \r).

Figure 8—Add Interface Description

Step 5  (Optional) Set advance fields (MAC address, MTU, static ARP entry, security configuration).

**Note**—The parameters and attributes to be configured differs based on the interface type. See **Interface-Overview** for details on interface types.
Step 5—(Optional) Set the duplex and speed by selecting the **Hardware Configuration** tab.

- **Duplex**—Choose Full, Half, or Auto. **Auto** is selected by default.
- **Speed**—Choose 10, 100, 1000, or Auto. **Auto** is selected by default.

**Note**—Depending on the mode of the interface, the options on the interface are limited.
Network Objects and Port Objects

The network object and port objects in the source configuration will be migrated by the Firepower Migration Tool during the migration.

For any new network or service ports, you can manually create new objects on new or the existing FMC.

i. **Network Objects**—A network object can be of the following types:

   - **Host**—Single IP address
   - **Range**—Range of IP address
   - **Network**—Address block, also known as subnet/netmask
   - **FQDN**—Single fully-qualified domain name (FQDN). FQDN resolution supported is only IPv4 address, only IPv6 addresses, and both IPv4 and IPv6 addresses.
   - **Group**—Group of network objects or other network object groups.

   **Note**—The Firepower System provides default network objects for some commonly used well-known networks like private subnet, multicast, Link local, benchmark test, any network subnet, and others. You cannot modify or delete these default objects. You can create custom network objects in addition to these default objects.

a. **Creating Network Objects**

   Step 1 Navigate to **Objects > Object Management > Network** and click (**Add Network**).

   Step 2 Click **Add Network** and from the drop-down list of object types, choose **Add Object** for Network Object.
**Network Objects and Port Objects**

**Figure 12—Creating Object Network – FMC**

Step 3 Enter a **Name**.

**Note**—In a multidomain deployment, object names must be unique within the domain hierarchy. The system may identify a conflict with the name of an object that you cannot view in your current domain.

Step 4 Enter a **Description**.

Step 5 In the **Network** field, select the required option from **Host**, **Range**, **Network**, **FQDN**, and enter an appropriate value.

**Figure 13—Configuring Network Object - FMC**

Step 6 Manage overrides for the object:

- If you want to allow overrides for this object, check the **Allow Overrides** check box.
- If you want to add override values to this object, expand the **Override** section, and click **Add**.
Migrating ASA to Firepower Threat Defense Platform Settings

Network Objects and Port Objects

Figure 14—Object Override

New Network Object

<table>
<thead>
<tr>
<th>Name</th>
<th>Obj-192.168.0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Host, Range, Network, FQDN</td>
</tr>
<tr>
<td>Allow Overrides</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Override (0)

<table>
<thead>
<tr>
<th>Override On</th>
<th>Content</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No records to display</td>
<td></td>
</tr>
</tbody>
</table>

Step 7  Click Save.

a. Creating Network Objects-Group

Step 1  Navigate to Objects > Object Management > Network and click (Add Network).

Step 2  Click Add Network and from the drop-down list of object types.

Step 3  Choose Add Group to create a Network Object-group.

Figure 15—Creating Network Object-Group

Step 3  Enter a unique Name.

Step 4  Enter a Description.

Step 5  Choose one or more objects from the list in Network Object.

- Use the Filter field to search for the existing objects to include the updates as you type to display the matching items. Click the Reload icon above the Search field or click the Clear (X) icon in the Search field to clear the search string.

- Click ( ) to create objects if no existing objects meet your requirements.

- You can directly add the network providing the literal value under the selected network. Enter the literal value, and then click Add.
Network Objects and Port Objects

Figure 16—Configuring Network Object-group

Step 6 Check the **Allow Overrides** check box to allow overrides for this object group.
Network Objects and Port Objects

Figure 17—Override Network Object-group

Step 7  Click **Save**.

b. Port-Objects—Port objects represent different protocols as follows:

- **TCP and UDP**—A port object represents the transport layer protocol, with the protocol number in parentheses, plus an optional associated port or port range. For example, TCP (6)/22.

- **ICMP and ICMPv6 (IPv6-ICMP)**—A port object represents the Internet layer protocol plus an optional type and code. For example, ICMP (1):3:3. You can restrict an ICMP or IPv6-ICMP port object by type and, if applicable, code.
  - **Other**—A port object can represent other protocols that do not use ports.

**Note**—The Firepower system provides default port objects for well-known ports. You cannot modify or delete these default objects. You can create custom port objects in addition to the default objects.

When using port objects, observe the following guidelines:

- You cannot add any protocol other than TCP or UDP for source port conditions in access control rules. Also, you cannot mix the transport protocols when setting both source and destination port conditions in a rule.

- If you add an unsupported protocol to a port object group used in a source port condition, the rule where it is used does not take effect on the managed device when the configuration is deployed.
Network Objects and Port Objects

- If you create a port object containing both TCP and UDP ports, then add it as a source port condition in a rule. You cannot add a destination port, and vice-versa.

a. Creating Port Objects

Step 1 Navigate to **Objects > Object Management > Port** and click ( ).

Step 2 Choose **Add Object** from the **Port** drop-down list.

**Figure 18—Create Port-object**

Step 3 Enter a unique **Name**.

Step 4 Choose a **Protocol**.

**Note**—Available protocols include TCP, UDP, IP, ICMP, IPv6-ICMP, and any protocol from the **Other** drop-down list (including All protocols).

- If you want to restrict a TCP or UDP object by port or port range, or if you choose All from the **Other** drop-down list, enter a value in the **Port** field. You can specify any port or port range from 1 to 65535, or any to match all ports. Use a hyphen to specify a range of ports.

- You can restrict to an ICMP or IPv6-ICMP port object by **Type** and, if applicable, **Code**. You can set the type to any to match any type or set the code to any to match any code for the specified type.

**Figure 19—Configure Port Object**

Step 5 Manage overrides for the object:

- If you want to allow overrides for this object, check the **Allow Overrides** check box.

- If you want to add override values to this object, expand the **Override** section, and click **Add**.
Network Objects and Port Objects

Figure 20—Port Object Override

### Step 7
Click Save.

**b. Creating Port Objects-group**

**Step 1** Navigate to **Objects > Object Management > Port** and click ( ).

**Step 2** Choose **Add Group** to create Port Object-group.

Figure 21—Create Port Object-group

**Step 3** Enter a Unique **Name**.

**Step 4** Optionally, enter a **Description**.

**Step 5** Choose one or more objects from the list in **Port Object**.

**Note**—Use the **Filter** field (%) to search for existing objects to include, which updates as you type to display matching items. Click the **Reload** icon ( ) above the **Search** field or click the **Clear** ( ) icon in the **search** field to clear the search string.

**Note**—Click **Add** ( ) to create objects if no existing objects meet your needs.
Step 6  Check the **Allow Overrides** check box to allow overrides for this object group.

Step 7  Click **Save**.

**Licensing**

Before proceeding, ensure that the licensing is enabled, and that the device is correctly registered to the smart license portal with export-controlled functionality.

Export-Controlled Functionality is required to enable the following features on the device:
Create Platform Setting Policy on FMC

- Security certifications compliance
- Firepower Threat Defense Remote Access VPN
- Site-to-Site VPN with strong encryption
- SSH platform policy with strong encryption
- SSL policy with strong encryption
- Functionality such as SNMPv3 with strong encryption

See Firepower-Licensing for more details to enable license correctly on firepower device.

Create Platform Setting Policy on FMC

A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be like other managed devices in your deployment, such as time settings and external authentication.

Perform these steps to create policy:

Step 1. Navigate to Devices > Platform Settings > New Policy > Threat Defense Settings.

Figure 24—Navigate Platform Setting

Step 2. Create the policy. Select devices for policy assignment and Save.

Figure 25—Create Platform Setting Policy
Configure Feature/Parameter in the Platform Setting Policy

Configure ARP Inspection

By default, all the ARP packets are allowed through the security appliance. You can control the flow of ARP packets by enabling ARP inspection.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing).

When you enable ARP inspection, the Firepower Threat Defense device compares the MAC address, IP address, and source interface in all the ARP packets to entries in the ARP table, where, if ARP packet does not match any entries in the ARP table, then you can set the Firepower Threat Defense device to either forward the packet out all interfaces (flood), or to drop the packet.

The static ARP entries can be defined in the ARP table for the inspection.

**Note**— Support for FTD in Transparent Mode.

ASA Configuration

---Snippet from ASA running-config ----

```plaintext
interface GigabitEthernet0/2
  bridge-group 10
  nameif Server
  security-level 100

interface GigabitEthernet0/3
  bridge-group 5
  nameif DMZ
  security-level 50

arp DMZ 10.11.1.100 0009.a2c1.b28d
arp DMZ 10.11.1.1 0009.a7b8.a32e
arp DMZ 10.10.1.1 0009.7cbb.21cf

arp-inspection Server enable flood
arp-inspection DMZ enable no-flood
```


Configuration on FMC

To add static entries in the FTD ARP table, perform the following:

Step 1  Navigate to Devices > Device Management and then click Edit (         ) for your FTD device and navigate to the Interfaces Tab.

Step 2  Click edit (         ) on the interfaces on which the static ARP entries are to be added.

Step 3  Click the Advanced tab, and then click the ARP and MAC tab.

Figure 26—Configure ARP and MAC on Interface

Step 4  Click Add ARP Config.

Figure 27—IP Address to MAC Binding

Step 5  Add the IP address and MAC address.
Configure Feature/Parameter in the Platform Setting Policy

Step 6  Click **OK** and **Save** the interface configuration.

Figure 28—ARP Table on Interface

Step 7  Navigate to **Devices > Platform Settings > FTD-Platform_policy**.

Step 8  Choose **ARP Inspection** in the platform setting policy on FMC, and then click **Add** to configure.

Figure 29—Enable ARP Inspection—Platform Setting Policy

Step 9  Configure the parameter with the following options and click **OK**.

- **Inspect Enabled**—To perform ARP inspection on zones.
- **Flood Enabled**—Whether to flood ARP requests that do not match static entries.
- **Security Zone**—The zone/interface on which the inspection is to be enabled.

**Note**—The ARP inspection will be enabled on Interface/Security Zone, before proceeding with selection of security zones, ensure that interfaces created are part of correct security zone.
For more information, see Interface Zones/Groups to create new interface/zones.

- **Security Zone/Interfaces** defined in the policy should match the actual interface of the device. Policies defined with nonmatching interface/security zone will not be deployed.

- **Security Zone/Interfaces** should be defined in the policy, empty **Selected Zones/Interfaces** field cannot be configured.

In the configuration example above, you have interface/nameif **Server** enabled with flood and DMZ with no-flood. The interface nameif **DMZ** is mapped to zone **DMZ_SZ** and interface nameif **Server** is mapped to zone **Server_SZ**.

*Only Switched Security Zones can be configured with ARP Inspection. Only Switched Security Zones will be listed here.*
Configure Feature/Parameter in the Platform Setting Policy

Figure 31—Configure Parameter - ARP Inspection: Without Flood enabled

Step 10  Click Save and deploy to the assigned devices.

Figure 32—ARP Inspection Enabled

Configuration on FTD After Deployment

--- Snippet from FTD running-config---

```
!  icmp unreachable rate-limit 1 burst-size 1
  no asdm history enable
  arp DMZ 10.11.1.100 0009.a2c1.b28d
  arp DMZ 10.11.1.1 0009.a7b8.a32e
  arp DMZ 10.10.1.1 0009.7cbb.21cf
  arp timeout 14400
```
Configure Feature/Parameter in the Platform Setting Policy

no arp permit-nonconnected
arp rate-limit 8192
!
mac-learn flood
arp-inspection Server enable flood
arp-inspection DMZ enable no-flood
dynamic-access-policy-record DfltAccessPolicy
!

Configure Login Banner

ASA supports multiple banner types while on FTD it is collated into a single banner Login Banner. You can use the Login Banner page to specify session, login, or custom message banners for a security appliance.

Login Banner message can be configured on FTD through the platform setting policy to show users when they connect to the device command line interface (CLI).

ASA Configuration

--- Snippet from ASA running-config ----

!  
interface Management0/0  
   management-only  
   shutdown  
   no ip address  
!  
  banner login ** W A R N I N G **  
  banner login Unauthorized access prohibited. All access is  
  banner login monitored, and trespassers shall be prosecuted  
  banner login to the fullest extent of the law.  
  boot system disk0:/asa982-20-lfbff-k8.SPA  
  boot system disk0:/asa992-smp-k8.bin  
  ftp mode passive  
!
**Configure Feature/Parameter in the Platform Setting Policy**

**Configuration on FMC**

**Step 1** Navigate to Devices > Platform Settings > FTD-Platform_policy.

**Step 2** Click Banner in the Platform Setting Policy on FMC.

![Banner - Platform Setting Policy](image1)

**Figure 33—Banner - Platform Setting Policy**

**Step 3** Enter or paste the Banner message for login.

![Configure Banner](image2)

**Figure 34—Configure Banner**

**Step 4** Click Save and deploy the policy to the assigned devices.

The banner file is pushed on the FTD as an issue file. The file is located on FTD in `/ngfw/etc/` directory.

To verify the banner file on FTD, perform these steps:

**Step 1** Login to FTD (Console or SSH).

**Step 2** Log with the Expert Mode on CLI.

**Step 3** Verify the Issue file on FTD.
Configure Feature/Parameter in the Platform Setting Policy

Configure DNS

The DNS resolution settings allow you to configure DNS for the data interfaces and the diagnostic interface. It also allows you to set variables to connect to the DNS server.

ASA Configuration

--- Snippet from ASA running-config ----

```
!  
banner login to the fullest extent of the law.
boot system disk0:/asa982-20-lffk8.SPA
boot system disk0:/asa992-smp-k8.bin
ftp mode passive

clock timezone EST -5

clock summer-time EDT recurring
dns domain-lookup 101_net
dns domain-lookup 100_net
dns server-group Internal-DNS
  name-server 10.1.1.1
  name-server 10.100.1.1
domain-name example.com
  same-security-traffic permit intra-interface
  object network obj1
  host 192.168.100.10
!```
Configure Feature/Parameter in the Platform Setting Policy

Configuration on FMC

Step 1  Navigate to Devices > Platform Settings > FTD-Platform_policy.

Step 2  Click DNS in the Platform Setting Policy on FMC.

Figure 35—DNS - Platform Setting Policy

Step 3  Enable the **Enable DNS name resolution by device** check box.

Figure 36—Enable DNS - Platform Setting Policy

Step 4  Select the **DNS Server Group** or create it.

Step 5  Click **Add** to create the server group, configure, and save it.
Configure Feature/Parameter in the Platform Setting Policy

Figure 37—Configure DNS

![Image of DNS configuration]

Step 6  
(Optional) Enter the **Expiry Entry Timer** and **Poll Timer** values in minutes.

- **Expiry Entry Timer**—Specifies the time limit to remove the IP address of a resolved FQDN from the DNS lookup table after its time-to-live (TTL) expires. Removing an entry requires the table to be recompiled. Frequent removals can increase the processing load on the device. This setting virtually extends the TTL.

- **Poll Timer**—Specifies the time limit after which the device queries the DNS server to resolve the FQDN that was defined in a network object group. An FQDN is resolved periodically either when the poll timer has expired, or when the TTL of the resolved IP entry has expired, whichever occurs first.

Step 7  
Select the **Interface Object** for lookup.

For more information, see *Interface Zones/Groups* to create new interface/zones.

If you do not enable DNS lookup on the diagnostic interface, then the FTD uses the data routing table to determine the interface. If there are no matches, it uses the management routing table.
Configure Feature/Parameter in the Platform Setting Policy

Figure 38—Configure DNS parameters - Platform Setting Policy

Step 8  To enable DNS lookup on diagnostics interface, then select **Enable DNS Lookup via diagnostic interface also** check box.

Step 9  Click **Save** and deploy the policy to the assigned devices.

Configuration on FTD After Deployment

--- Snippet from FTD running-config ----

```
ftp mode passive
ngips conn-match vlan-id
dns domain-lookup 100_net
dns domain-lookup 101_net
dns server-group Internal-DNS
name-server 10.1.1.1
name-server 10.100.1.1
domain-name example.com
dns-group Internal-DNS
access-list CSM_FW_ACL_remark rule-id 268434882: PREFILTER POLICY: testPreFilter
```
Configure External Authentication

You can configure RADIUS or LDAP Server for External Authentication.

ASA Configuration

--- Snippet from ASA running-config ---

```
! timeout igp stale-route 0:01:10
    aaa-server Radius_server protocol radius
    aaa-server Radius_server (inside) host 10.1.1.10
    retry-interval 3
    timeout 30
    key *****
    authentication-port 1812
    aaa-server LDAP-Server protocol ldap
    aaa-server LDAP-Server (inside) host 192.168.1.10
    ldap-base-dn ou=security, dc=example, dc=com
    ldap-login-password *****
    ldap-login-dn ou=admin, dc=example, dc=com
    server-type auto-detect
    user-identity default-domain LOCAL
    aaa authentication ssh console LOCAL
```

Configuration on FMC

Step 1  Navigate to Devices > Platform Settings > FTD-Platform_policy.

Step 2  Click External Authentication in the Platform Setting Policy on FMC and navigate to Manage External Authentication Server.

Figure 39—External Authentication—Platform Setting Policy

Step 3  Click Manage External Authentication Server, that redirects you to the System > Users > External Authentication page as shown in Figure 40.
Configure Feature/Parameter in the Platform Setting Policy

Figure 40—Add External Authentication Object

Step 4 Click **Add External Authentication Object** to add Radius or LDAP server.

Step 5 Configure the parameters for the Server.

- Radius Server

Figure 41—Configure Radius Server

Step 6 **Test** and **Save** the Server Configuration.

- LDAP Server
For LDAP users, set the shell access filter to allow CLI access to FTD. To specify CLI users, choose one of the following methods:

- To use the same filter, you specified when configuring authentication settings, choose **Same as Base Filter**.
- To retrieve administrative user entries based on the attribute value, enter the attribute name, a comparison operator, and the attribute value that you want to use as a filter, enclosed in parentheses. For example, if all the network administrators have a `sysadmin` attribute which has an attribute value of `shell`, you can set a base filter of `(sysadmin=shell)`. 
Configure Feature/Parameter in the Platform Setting Policy

Figure 43—LDAP Server Parameters

Step 7 Test and Save the server configuration.
For more information, see Configuring External authentication Server for more details.

Step 8 Click Save or Save and Apply the server configuration. With Save and Apply, the configuration is saved and applied to your current domain.

Figure 44—External Authentication—Server

Step 9 Navigate to Device > Platform Setting > FTD-Platform_policy. In the platform setting policy, navigate to External Authentication.
Click Refresh and the server details will be populated. Enable the server that will be used for authentication. Save and deploy the policy to assigned devices.
Configure Feature/Parameter in the Platform Setting Policy

Figure 45—External Authentication—Enabled

Step 10   Deploy to assigned devices.

On FTD

- Radius Server

If the user list is given while configuring Radius server object on FMC, then on converged CLI (CLISH prompt “>”), command `show user` should list the users that are configured in the FMC.

If the user list was not given while configuring Radius server object on FMC, then `show user` will not list anything. Only when the radius user successfully logs in for the first time, entry gets added and `show user` starts showing that user (available from FMC 6.4 and later).

- LDAP server

The `show user` command should list all the users mapping to the Shell access filter that has been configured in LDAP server object on FMC.

`show user` Output on FTD

```
> show user
Login  UID  Auth Access  Enabled  Exp Warn  Str Lock Max
admin  1000  Local Config  Enabled  No Never N/A Dis No N/A
dhcp   997   Local  Basic Disabled No 0 0 Dis No N/A
radiusd 995  Local Basic Disabled No 0 0 Dis No N/A
> 
```

Configure Fragment Handling

Configure the Fragment setting to handle the fragmented traffic on your network. By default, the FTD device allows up to 24 fragments per IP packet, and up to 200 fragments awaiting reassembly.

ASA Configuration

--- Snippet from ASA running-config ----

```
snmp-server enable traps nat packet-discard
snmp-server enable traps config
fragment size 200 mgmt
```
Configure Feature/Parameter in the Platform Setting Policy

- fragment chain 24 mgmt
- fragment timeout 5 mgmt
- fragment size 200 inside
- fragment chain 24 inside
- fragment timeout 5 inside
- fragment size 200 dmz
- fragment chain 24 dmz
- fragment timeout 5 dmz
- fragment size 200 Server
- fragment chain 24 Server
- fragment timeout 5 Server
- crypto ipsec security-association pmtu-aging infinite
- crypto ca trustpoint _SmartCallHome_ServerCA

Configuration on FMC

Step 1 Navigate to Devices > Platform Settings > FTD-Platform_policy.
Step 2 Click Fragment Settings in the Platform Setting Policy on FMC.
Step 3 Configure the parameters with the respective values or let the default values remain.

Figure 46—Fragment Parameters—Platform Setting Policy

Step 4 Click Save and deploy to the assigned devices.

These settings establish the defaults for devices assigned with this policy. You can override these settings for specific interfaces on a device by selecting Override Default Fragment Setting in the interface configuration. To configure fragment setting on the interface, perform the following steps:

1. Click Devices > Device Management, click edit () on the FTD device, and then navigate to Interfaces.
2. Click edit ( ) and navigate to Advanced > Security Configuration.

3. Select the Override Default Fragment Setting check box and configure the value for parameter Size, Chain, and Time Out.

Figure 47—Fragment Parameter—Interface

--- Snippet from FTD running-config ----

```bash
!  snmp-server enable
  fragment size 200 diagnostic
  fragment chain 24 diagnostic
  fragment timeout 5 diagnostic
  no fragment reassembly full diagnostic
  fragment size 200 inside
  fragment chain 24 inside
  fragment timeout 5 inside
  no fragment reassembly full inside
  fragment size 200 outside
  fragment chain 24 outside
  fragment timeout 5 outside
  no fragment reassembly full outside
```
Configure Feature/Parameter in the Platform Setting Policy

fragment size 200 DMZ_SZ
fragment chain 24 DMZ_SZ
fragment timeout 5 DMZ_SZ
no fragment reassembly full DMZ_SZ

fragment size 200 dmz
fragment chain 24 dmz
fragment timeout 5 dmz
no fragment reassembly full dmz

fragment size 200 app
fragment chain 24 app
fragment timeout 5 app
no fragment reassembly full app

fragment size 200 100_net
fragment chain 24 100_net
fragment timeout 5 100_net
no fragment reassembly full 100_net

fragment size 200 101_net
fragment chain 24 101_net
fragment timeout 5 101_net
no fragment reassembly full 101_net

fragment size 200 103_net
fragment chain 24 103_net
fragment timeout 5 103_net
no fragment reassembly full 103_net

fragment size 200 105_net
fragment chain 24 105_net
fragment timeout 5 105_net
no fragment reassembly full 105_net

fragment size 200 106_net
fragment chain 24 106_net
fragment timeout 5 106_net
no fragment reassembly full 106_net
### Configure Feature/Parameter in the Platform Setting Policy

<table>
<thead>
<tr>
<th>Feature/Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>fragment size</td>
<td>200 SRV</td>
</tr>
<tr>
<td>fragment chain</td>
<td>24 SRV</td>
</tr>
<tr>
<td>fragment timeout</td>
<td>5 SRV</td>
</tr>
<tr>
<td>no fragment reassembly</td>
<td>full SRV</td>
</tr>
<tr>
<td>no sysopt traffic detailed-statistics</td>
<td></td>
</tr>
<tr>
<td>no sysopt connection timewait</td>
<td></td>
</tr>
<tr>
<td>sysopt connection tcpmss</td>
<td>1380</td>
</tr>
<tr>
<td>sysopt connection tcpmss minimum</td>
<td>0</td>
</tr>
</tbody>
</table>

### Configure HTTP

If you want to allow HTTPS connections to one or more interfaces on the FTD device, configure the HTTPS settings.

**Before you begin:**

- When you manage the FTD using the Firepower Management Center, HTTPS access to the FTD is only for viewing packet capture files. The FTD does not have a web interface for configuration in this management mode.
- The physical management interface is shared between the Diagnostic logical interface and the Management logical interface. This configuration applies only to the Diagnostic logical interface, if used, or to other data interfaces.
- To use HTTPS, you do not need an access rule allowing the host IP address. You only need to configure HTTPS access according to this section.
- You can only use HTTPS to a reachable interface. If your HTTPS host is located on the outside interface, you can only initiate a management connection directly to the outside interface.
- The device allows a maximum of 5 concurrent HTTPS connections.
- You must require the network objects that define the hosts or networks that will allow you to make HTTPS connections to the device.
- You can add objects as part of the procedure. But, if you want to use object-groups to identify a group of IP addresses, ensure that the groups needed in the rules already exist. Select **Objects** > **Object Management** to configure objects.

**ASA Configuration**

--- Snippet from ASA running-config ----

```bash
!  
  aaa authentication serial console LOCAL  
  aaa authentication login-history  
  http server enable 8443  
  http 10.1.1.1 255.255.255.255 100_net  
  http 192.168.0.0 255.255.0.0 101_net
```
Configure Feature/Parameter in the Platform Setting Policy

```
http 202.10.1.1 255.255.255.255 103_net
snmp-server group SNMP-SRV v3 priv
```

Configuration on FMC

Step 1  Navigate to Devices > Platform Settings > FTD-Platform_policy.

Step 2  Click HTTP in the Platform Setting Policy on FMC.

Step 3  Click the Enable HTTP Server check box to enable the server and mention the Port on which the service is to be enabled.

Figure 48—HTTP Server—Platform Setting

Step 4  Click (Add) to configure the network addresses which are allowed for HTTPS service.

For more information, see Network Objects and Port Objects to create network or port objects.

Figure 49—HTTP Server—New Network Object

Add the zones that contain the interfaces to which you allow HTTPS connections. For interfaces not in a zone, you can type the interface name into the field below the Selected Zones/Interfaces list and click Add. These rules will be applied to a device only if the device includes the selected interfaces or zones.
Security Zone/Interface defined in the policy should match the actual interface of the device. You cannot deploy a policy defined with nonmatching interface/security zone.

Security Zone/Interface should be defined in the policy, empty Selected Zones/Interfaces field cannot be configured.

See Interface Zones/Groups to create new interface/zones.

Figure 50—Configure HTTP server Parameter

![Edit HTTP Configuration](image)

Step 5  Add all the network addresses/Objects.

Figure 51—HTTP Server—Enabled

![HTTP Configuration](image)

Step 6  Click Save and deploy the policy to assigned devices.

Configuration on FTD After Deployment

--- Snippet from FTD running-config ----

```bash
!```

---
Configure Feature/Parameter in the Platform Setting Policy

aaa proxy-limit disable
aaa authentication login-history

http server enable 8443
http 10.1.1.1 255.255.255.255 100_net
http 192.168.0.0 255.255.0.0 101_net
http 202.10.1.1 255.255.255.255 103_net

Configure ICMP

You can send the ICMP packets to any interface using either IPv4 or IPv6, with the following exceptions:

- The Firepower Threat Defense device does not respond to the ICMP echo requests directed to a broadcast address.
- The Firepower Threat Defense device responds only to the ICMP traffic sent to the interface on which it is received. You cannot send the ICMP traffic through a far interface.

To protect the device from attacks, you can use ICMP rules to limit the ICMP access to interfaces to particular hosts, networks, or ICMP types.

ASA Configuration

--- Snippet from ASA running-config ----

! failover interface is FO 12.1.1.1 255.255.255.0 standby 12.1.1.2
no monitor-interface service-module
icmp unreachable rate-limit 2 burst-size 2
icmp permit any 101_net
icmp deny host 10.10.1.100 101_net
Migrating ASA to Firepower Threat Defense Platform Settings

**Configure Feature/Parameter in the Platform Setting Policy**

```
icmp permit 100.1.1.0 255.255.255.0 100_net
icmp permit any 103_net
icmp deny 192.16.0.0 255.255.0.0 inside
icmp permit 192.168.0.0 255.255.0.0 inside
icmp deny 100.10.1.0 255.255.255.0 echo-reply outside
icmp deny 100.10.1.0 255.255.255.0 time-exceeded outside
icmp deny 100.10.1.0 255.255.255.0 unreachable outside
icmp permit host 1.1.1.1 echo app
asdm image disk0:/asdm-782-151.bin
```

**Configuration on FMC**

**Step 1** Navigate to Devices > Platform Settings > FTD-Platform_policy.

**Step 2** Click ICMP in the Platform Setting Policy on FMC.

![ICMP in Platform Setting Policy](image)

**Figure 52 — Enable ICMP — Platform Setting**

**Step 3** Set the **Rate Limit** and **Burst size** value for ICMP unreachable.

![ICMP Parameter — Unreachable](image)

**Figure 53 — ICMP Parameter — Unreachable**

**Step 4** Configure the Network addresses/host allowed or denied for the ICMP traffic.

**Step 5** Click (**Add**) to configure the network address/host objects.
Configure Feature/Parameter in the Platform Setting Policy

Figure 54—ICMP Parameters

Step 6  Click ( ) Add and configure objects for the ICMP service and network.

Step 7  Click ( ) Add on the ICMP Service, configure, and Save it.

For more information, see Network Objects and Port Objects to create network or port objects.

Figure 55—Configure ICMP—Service Object - Any

For Any ICMP Service
Migrating ASA to Firepower Threat Defense Platform Settings

Configure Feature/Parameter in the Platform Setting Policy

For ICMP Service Type Defined

Figure 56—Configure ICMP—Service Object—Echo

Add the zones that contain the interfaces to which you will allow or deny ICMP traffic. For interfaces not in a zone, you can type the interface name into the field below the Selected Zone/Interfaces section and click Add. These rules will be applied to a device only if the device includes the selected interfaces or zones.

- Security Zone/Interfaces defined in the policy should match the actual interface of the device. Policies defined with nonmatching interface/security zone will not be deployed.
- Security Zone/Interfaces should be defined in the policy, empty Selected Zones/Interfaces field cannot be configured.

See Interface Zones/Groups to create new interface/zones.
Configure Feature/Parameter in the Platform Setting Policy

Figure 57—Configure ICMP—Network Object

Step 8 Configure the ICMP for other network/host as per the ASA configuration.

Step 9 Click Save.

Figure 58—Configure ICMP—Enabled

Step 10 Deploy the policy to assigned devices.

Configuration on FTD After Deployment

--- Snippet from FTD running-config ----
Configure Secure Shell (SSH)

If you want to allow SSH connections to one or more data or Diagnostic interfaces on the FTD device, configure the Secure Shell settings.

The physical management interface is shared between the Diagnostic logical interface and the Management logical interface. SSH is enabled by default on the Management logical interface; however, this screen does not affect the Management SSH access.

Before you begin, ensure:

- These settings simply enable SSH connections. In addition, you must identify the users who will be allowed to complete SSH connections. Select External Authentication from the platform settings, and define Authentication servers for user authentication.

- On FTD to enhance security, an updated list of supported ciphers and cryptographic algorithms for secure SSH access is available. If your SSH client fails to connect with a Firepower appliance due to a cipher error, update your client to the latest version.

ASA Configuration

--- Snippet from ASA running-config ----

```plaintext
!           
telnet timeout 5
ssh stricthostkeycheck
```

Configure Feature/Parameter in the Platform Setting Policy

```
ssh 206.229.20.0 255.255.255.0 101_net
ssh 184.97.169.216 255.255.255.255 101_net
ssh 0.0.0.0 0.0.0.0 100_net
ssh 172.16.20.0 255.255.255.0 100_net
ssh timeout 5
ssh version 2
ssh cipher encryption all
ssh cipher integrity all
ssh key-exchange group dh-group14-sha1
console timeout 0
vpn load-balancing
```

Note—On FTD, the SSH parameter/attributes like version, ciphers, key are predefined and not configurable. You can verify the attributes/parameter for SSH on FTD at `/ngfw/etc/ssh`.

Configuration on FMC

Step 1 Navigate to Devices > Platform Settings > FTD-Platform_policy.

Step 2 Click Secure Shell in the Platform Setting on FMC.

Figure 59—Configure SSH

Step 3 Configure the Network addresses/host allowed or denied for SSH.

Step 4 Click (Add) to configure and then click OK.

For more information, see Network Objects and Port Objects to create network or port objects.
Select the Zones/Interface on which you want to enable the SSH.

- **Security Zone/Interface** defined in the policy should match the actual interface of the device. You cannot deploy a policy defined with nonmatching interface/security zone.

- **Security Zone/Interface** should be defined in the policy, empty **Selected Zones/Interfaces** field cannot be configured.

For more information, see Interface Zones/Groups to create new interface/zones.
Configure Feature/Parameter in the Platform Setting Policy

Figure 61—Configure SSH - Zone/IG binding

Step 5 Configure the SSH setting for other network/host as per the ASA configuration.

Step 6 Click Save.

Figure 62—Configure SSH—Enabled

Step 7 Deploy the policy to assigned devices.

Configuration on FTD After Deployment

--- Snippet from FTD running-config ----

```bash
! crypto ca trustpool policy
telnet timeout 5
    ssh 0.0.0.0 0.0.0.0 100_net
    ssh 172.16.20.0 255.255.255.0 100_net
```
Configure Feature/Parameter in the Platform Setting Policy

ssh 206.229.20.0 255.255.255.0 101_net
ssh 184.97.169.216 255.255.255.255 101_net
console timeout 0
threat-detection basic-threat

Configure SMTP Server

You can identity an SMTP server if you configure email alerts in the Syslog settings.

ASA Configuration

--- Snippet from ASA running-config ----

! service-policy global_policy global
smtp-server 192.168.1.120 192.168.1.122
prompt hostname context
!

Configuration on FMC

Step 1  Navigate to Devices > Platform Settings > FTD-Platform_policy.
Step 2  Click SMTP Server in the Platform Setting Policy on FMC.
Step 3  Click icon to add Primary Server IP Address and Secondary Server IP Address.
Step 4  Create the object network for the server and Save.
Step 5  Add the created objects to the Primary and Secondary Server IP address Fields.

Figure 63—Configure SMTP—Primary Server
Configure Feature/Parameter in the Platform Setting Policy

Figure 64—Configure SMTP—Secondary Server

Step 6  Click **Save** and deploy the policies to the assigned devices.

Figure 65—Enable SMTP Server

--- Snippet from FTD running-config ----

```plaintext
!  
class class-default  
   set connection advanced-options UM_STATIC_TCP_MAP  
!  
   service-policy global_policy global  
   smtp-server 192.168.1.120 192.168.1.122  
   prompt hostname context  
   call-home  
   profile CiscoTAC-1  
!  
```
Configure SNMP

You can use the SNMP to configure FTD for monitoring by SNMP management stations. Cisco security appliances supports network monitoring using SNMP versions 1, 2c, and 3.

The Simple Network Management Protocol (SNMP) enables monitoring of network devices from a central location. Cisco security appliances support traps and SNMP read access; SNMP write access is not supported. SNMPv3 only supports read-only users and encryption with AES128.

Note—Verify that the license is enabled with export-controlled functionality before configuring SNMPv3. See Licensing for more details.

ASA Configuration

SNMP v1 and 2c

--- Snippet from ASA running-config ----

```bash

!  
aaa authentication serial console LOCAL  
aaa authentication login-history  
http server enable 8443  
http 10.1.1.1 255.255.255.255 mgmt  
http 192.168.0.0 255.255.0.0 mgmt  
http 202.10.1.1 255.255.255.255 mgmt  
snmp-server host Inside 192.168.10.1 community ******  
snmp-server host Inside 192.168.20.1 community ****** version 2c  
snmp-server location US  
snmp-server contact administrator@example.com  
snmp-server community ******  
snmp-server enable traps syslog  
snmp-server enable traps ipsec start stop  
snmp-server enable traps entity config-change fru-insert fru-remove  
snmp-server enable traps memory-threshold  
snmp-server enable traps interface-threshold  
snmp-server enable traps remote-access session-threshold-exceeded  
snmp-server enable traps connection-limit-reached  
snmp-server enable traps cpu threshold rising  
snmp-server enable traps ikcv2 start stop  
snmp-server enable traps nat packet-discard  
snmp-server enable traps config
```


Configure Feature/Parameter in the Platform Setting Policy

- fragment size 200 mgmt
- fragment chain 24 mgmt
- fragment timeout 5 mgmt
- fragment size200 inside

SNMP v3

--- Snippet from ASA running-config -----

```
!  
  aaa authentication serial console LOCAL
  aaa authentication login-history
  http server enable 8443
  http 10.1.1.1 255.255.255.255 mgmt
  http 192.168.0.0 255.255.0.0 mgmt
  http 202.10.1.1 255.255.255.255 mgmt
  snmp-server group SNMP-SRV v3 priv
    snmp-server host Inside 192.168.30.1 version 3 adm-cisco
    snmp-server location US
    snmp-server contact administrator@example.com
    snmp-server enable traps syslog
    snmp-server enable traps ipsec start stop
    snmp-server enable traps entity config-change fru-insert fru-remove
    snmp-server enable traps memory-threshold
    snmp-server enable traps interface-threshold
    snmp-server enable traps remote-access session-threshold-exceeded
    snmp-server enable traps connection-limit-reached
    snmp-server enable traps cpu threshold rising
    snmp-server enable traps ikev2 start stop
    snmp-server enable traps nat packet-discard
    snmp-server enable traps config
```
Configure Feature/Parameter in the Platform Setting Policy

fragment size 200 mgmt
fragment chain 24 mgmt
fragment timeout 5 mgmt
fragment size 200 inside

Note—All the SNMP traps are not supported on FTD like ikev2 start stop, ipsec start stop, memory/interface threshold, cpu threshold rising, remote-access session-threshold-exceeded, and others. FRU traps are not supported on Firepower version 6.5 and later.

Configuration on FMC

Step 1 Navigate to Devices > Platform Settings > FTD-Platform_policy.
Step 2 Click SNMP in the Platform Setting on FMC. Select Enable SNMP Server check box and configure the basic parameters.

Figure 66—Configure SNMP

Step 3 Click Add to add Host, Users, and SNMP Traps.
Step 4 Host (SNMP v1 and 2C)—Configure SNMP v1 and 2c parameters and click Ok.

Note—Configure user for SNMPv3 from the User Tab before configuring the host.

Figure 67—Add SNMP Host

In the IP Address field, either enter a valid IPv6 or IPv4 host or select the network object that defines the SNMP management station host address.

Note—For SNMP host value, FTD supports network object/groups, host, and literals for both IPv4 and IPv6. The range network object is supported for IPv4 only.
Configure Feature/Parameter in the Platform Setting Policy

Figure 68—SNMPv1 Host—Configuration

Select the Zones/Interface from Available Zones, that will be associated to snmp-server.

- **Security Zone/Interface** defined in the policy should match the actual interface of the device. You cannot deploy a policy defined with nonmatching interface/security zone.

- **Security Zone/Interfaces** should be defined in the policy. You cannot configure an empty **Selected Zones/Interfaces** field.

For more information, see Interface Zones/Groups to create new interface/zones.
Configure Feature/Parameter in the Platform Setting Policy

Figure 69—SNMPv2 Host—Configuration

Hosts are added for SNMP v1 and 2c

- User—Click Add to configure.

Figure 70—SNMP v1/2c User
Configure Feature/Parameter in the Platform Setting Policy

Figure 71—Configure User

Step 5  Click OK.

Figure 72—SNMP—User Added

• Host (SNMPv3)—Click Add to configure.

Figure 73—SNMPv3—Add Host
Configure Feature/Parameter in the Platform Setting Policy

Figure 74—SNMPv3—Host Configuration

Step 6  Click OK.

Figure 75—SNMPv3 Host
Configure Feature/Parameter in the Platform Setting Policy

SNMP Traps—Use SNMP Traps tab to configure traps (event notifications) for the FTD device.

Figure 76—SNMP Traps

Figure 77—SNMP Traps Configuration

Step 7 Click Save and deploy the policy to assigned devices.

Configuration on FTD After Deployment

--- Snippet from FTD running-config ----

```
http server enable 8443
http 10.1.1.1 255.255.255.255 100_net
http 192.168.0.0 255.255.0.0 101_net
http 202.10.1.1 255.255.255.255 103_net
snmp-server group Priv v3 priv
  snmp-server host inside 192.168.10.1 community *****
  snmp-server host inside 192.168.20.1 community ***** version 2c
```
Configure Feature/Parameter in the Platform Setting Policy

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp-server host inside 192.168.30.1 version 3 adm-cisco</td>
<td></td>
</tr>
<tr>
<td>snmp-server location US</td>
<td></td>
</tr>
<tr>
<td>snmp-server contact <a href="mailto:administrator@example.com">administrator@example.com</a></td>
<td></td>
</tr>
<tr>
<td>snmp-server community *****</td>
<td></td>
</tr>
<tr>
<td>snmp-server enable traps syslog</td>
<td></td>
</tr>
<tr>
<td>snmp-server enable traps entity config-change</td>
<td></td>
</tr>
<tr>
<td>snmp-server enable traps connection-limit-reached</td>
<td></td>
</tr>
<tr>
<td>snmp-server enable traps nat packet-discard</td>
<td></td>
</tr>
<tr>
<td>crypto ipsec security-association pmtu-aging infinite</td>
<td></td>
</tr>
<tr>
<td>crypto ca trustpool policy</td>
<td></td>
</tr>
<tr>
<td>telnet timeout 5</td>
<td></td>
</tr>
<tr>
<td>ssh 0.0.0.0 0.0.0.0 100_net</td>
<td></td>
</tr>
<tr>
<td>ssh 172.16.20.0 255.255.255.0 100_net</td>
<td></td>
</tr>
</tbody>
</table>

Configure SSL

You can use the SSL to configure the SSL parameters on the FTD.

If you run Firepower Management Center in the evaluation mode, SSL Settings tab will be disabled.

Also, the SSL Settings tab will be disabled when the licensed Firepower Management Center version does not meet the export-compliance criteria. If you are using Remote Access VPN with SSL, your Smart Account must have the strong-crypto features enabled.

ASA Configuration

--- Snippet from ASA running-config ----

```
!  ntp trusted-key 1
  ntp server 202.1.1.10 key 1 source outside
  ssl server-version tlsv1.2
  ssl client-version tlsv1.2
  ssl cipher default custom "AES128-SHA:AES256-SHA:DES-CBC3-SHA"
  ssl cipher tlsv1 custom "AES128-SHA:AES256-SHA:DES-CBC3-SHA"
  ssl cipher tlsv1.1 all
  ssl cipher tlsv1.2 medium
  ssl cipher dtlsv1 custom "AES128-SHA:AES256-SHA:DES-CBC3-SHA"
```
Configure Feature/Parameter in the Platform Setting Policy

- ssl dh-group group24
- ssl ecdh-group group20
- webvpn
- anyconnect enable


Migrating ASA to Firepower Threat Defense Platform Settings

Configure Feature/Parameter in the Platform Setting Policy

Configuration on FMC

Step 1 Navigate to Devices > Platform Settings > FTD-Platform_policy.

Step 2 Click SSL in the Platform Setting Policy on FMC and configure the SSL parameters.

Figure 78—Configure SSL

Step 3 Click Add to configure the Protocol version and Cipher Algorithm/Custom String.

Step 4 Click OK after configuring the version and security level.

Figure 79—Configure SSL Parameter—Medium

Configuration on FMC

Step 1 Navigate to Devices > Platform Settings > FTD-Platform_policy.

Step 2 Click SSL in the Platform Setting Policy on FMC and configure the SSL parameters.

Figure 78—Configure SSL

Step 3 Click Add to configure the Protocol version and Cipher Algorithm/Custom String.

Step 4 Click OK after configuring the version and security level.

Figure 79—Configure SSL Parameter—Medium

Configuration on FMC

Step 1 Navigate to Devices > Platform Settings > FTD-Platform_policy.

Step 2 Click SSL in the Platform Setting Policy on FMC and configure the SSL parameters.

Figure 78—Configure SSL

Step 3 Click Add to configure the Protocol version and Cipher Algorithm/Custom String.

Step 4 Click OK after configuring the version and security level.

Figure 79—Configure SSL Parameter—Medium
Configure Feature/Parameter in the Platform Setting Policy

Figure 80—Configure SSL Parameter—All

![Add SSL Configuration](image)

Note—You can configure custom ciphers as well selecting security Level as Custom.
Migrating ASA to Firepower Threat Defense Platform Settings

Configure Feature/Parameter in the Platform Setting Policy

Figure 81—Configure SSL Parameter—Custom

Add SSL Configuration

- Protocol Version: TLSv1
- Security Level: Custom
- Cipher Suites:
  - Available Algorithms:
    - DHE-RSA-AES256-SHA
    - AES256-SHA
    - DHE-RSA-AES128-SHA
    - AES128-SHA
    - DES-CBC3-SHA
    - NULL-SHA

Figure 82—SSL Enable

- Minimum SSL Version as Server: TLSv1.2
- Diffe-Hellman Group: Group 24 (2048 Bit Modular, 256 Bit prime order sub)
- Elliptic Curve Diffe-Hellman Group: Group 20 (384 Bit)

Configuration on FTD After Deployment

--- Snippet from FTD running-config ----

```bash
! threatsdetection statistics access-list
no threat-detection statistics tcp-intercept
ssl server-version tlsv1.2
ssl cipher tlsv1 custom "AES128-SHA:DES-CBC-SHA"
ssl cipher tlsv1.1 all
```
Configure Feature/Parameter in the Platform Setting Policy

```perl
ssl cipher tlsv1.2 medium
ssl dh-group group24
ssl ecdh-group group20
dynamic-access-policy-record DfltAccessPolicy
```

Configure Syslog

You can enable system logging (syslog) for FTD devices. The information can help you identify and isolate network or device configuration problems.

ASA Configuration

```bash
--- Snippet from ASA running-config ----

access-list acl1 extended permit tcp any object-group obj-server eq www
pager lines 24
logging enable
logging timestamp
logging standby
logging emblem
logging buffer-size 4096
logging monitor informational
logging buffered informational
logging trap informational
logging mail critical
logging from-address asa_alert@example.com
logging recipient-address adm@example.com level critical
logging host Inside 192.168.1.100 format emblem
logging debug-trace
logging ftp-bufferwrap
logging ftp-server 10.10.20.25 /syslogs adm-sys-cisco *****
mtu mgmt 1500
mtu lan 1500
mtu 105_net 150
```
Configuration on FMC

Step 1  Navigate to Devices > Platform Settings > FTD-Platform_policy.
Step 2  Click Syslog in the Platform Setting on FMC, then click Logging Setup.
Step 3  Enable logging and configure basic logging settings.
  - **Enable Logging**—Turns on data plane system logging for the FTD.
    ASA command—logging enable
  - **Enable Logging on Failover Standby Unit**—Turns on logging for standby Unit.
    ASA command—logging standby
  - **Send Logs in EMBLEM format**—Enable emblem logging for all destination.
    ASA command—logging emblem
  - **Send Debug Message syslogs**—Redirect all debug trace output to syslog server.
    ASA command—logging debug-trace
  - **Memory Size of the Internal Buffer**—Internal Buffer size.
    ASA command—logging buffer-size 4096

FMC

**Figure 83—Configure Syslog**

![Syslog Configuration Interface](image)

Step 4  **Configure FTP Server Buffer Wrap** to send the buffer log data to the FTP server.

**ASA Configuration**

```
logging ftp-bufferwrap
logging ftp-server 10.10.20.25 /syslogs adm-sys-cisco ****
```
Configure Feature/Parameter in the Platform Setting Policy

- Create object network for IP address for the server—Object > Object Management > Network > Add Object. See Network Objects and Port Objects to create network or port objects.

- In the Logging Setup on Syslog configuration—Specify the parameters in Specify FTP Server Information.

FMC

Figure 84—Configure Syslog—Setup

Step 5 Specify Flash size if you want to save log buffer contents to flash.

Step 6 In the Logging Destinations dialog box, select a destination and configure the filter to use for a destination.

Step 7 Click Add to configure the following:

- Choose the destination you are enabling in the Logging Destination drop-down list.
- In Event Class, choose the filter that will apply to all classes not listed in the table.
- If you want to create filters per event class, click Add to create a new filter, or edit an existing filter.
- Click OK.

ASA Configuration

```
logging buffered informational
logging trap informational
logging mail critical
```

FMC
Configure Feature/Parameter in the Platform Setting Policy

Figure 85—Configure Syslog—Logging Destination

Step 8  In the **Email Setup**, specify the e-mail address used as the source address for syslog messages sent as e-mail messages.

Step 9  Click **Add** to configure the destination address.

**ASA Configuration**

```
! 
logging from-address asa_alert@example.com
logging recipient-address adm@example.com level critical
! 
```
Configure Feature/Parameter in the Platform Setting Policy

FMC

Figure 86—Syslog—Email Setup

Step 10  Click OK.

Figure 87—Configure Email—Syslog

Step 11  Configure Event List.
- Click Add to add a new list or edit an existing list.
- Enter a name for the event list in the Name field.
- Specify the event class and message ID.
- Click Logging Destinations tab and add or edit the destination that should use the filter.

Step 12  To Rate Limit message generation by severity level, click Add in the Logging Level tab.
For more information, see Rate Limit.

Step 13  Configure Syslog setting to configure the facility and timestamp on syslog messages.

ASA Configuration

```bash
logging timestamp
```

69
Migrating ASA to Firepower Threat Defense Platform Settings

Configure Feature/Parameter in the Platform Setting Policy

FMC

Figure 88—Syslog Settings

For more information, see FTD-Syslog-Messages for supported syslog messages on FTD.

Step 14  Configure Syslog server to specify server details.

Step 15  Click Add.

ASA

```
! logging host Inside 192.168.1.100 format emblem
!
```

FMC

Figure 89—Syslog Server

Step 16  Click Add to add IP address and create the network object.
Configure Feature/Parameter in the Platform Setting Policy

Figure 90—Syslog Server—Network Object

Select the Zones/Interface on which you require to configure for syslog server.

- Security Zone/Interfaces defined in the policy should match the actual interface of the device. Policies defined with nonmatching interface/security zone will not be deployed.

- Security Zone/Interfaces should be defined in the policy, empty Selected Zones/Interfaces field cannot be configured.

To create new interface/zones, see Interface Zones/Groups.

Note—If the syslog server is reachable by Diagnostics interface (Applicable to FTD versions 6.3.0 and later), select Device Management Interface.
Figure 91—Syslog Server—Interface

Step 17  Click **OK**.

Figure 92—Syslog Enable

Step 18  Click **Save** and **Deploy** the policy to assigned devices.

Configuration on FTD After Deployment

--- Snippet from FTD running-config ----

```plaintext
! tcp-map UM_STATIC_TCP_MAP
```
Configure Feature/Parameter in the Platform Setting Policy

tcp-options range 6 7 allow

tcp-options range 9 18 allow

tcp-options range 20 255 allow

urgent-flag allow

!

no pager

logging enable

logging timestamp

logging standby

logging emblem

logging list MANAGER_VPN_EVENT_LIST level errors class auth

logging list MANAGER_VPN_EVENT_LIST level errors class vpn

logging list MANAGER_VPN_EVENT_LIST level errors class vpc

logging list MANAGER_VPN_EVENT_LIST level errors class vpc

logging list MANAGER_VPN_EVENT_LIST level errors class vpnfo

logging list MANAGER_VPN_EVENT_LIST level errors class vpnlb

logging list MANAGER_VPN_EVENT_LIST level errors class webfo

logging list MANAGER_VPN_EVENT_LIST level errors class webvpn

logging list MANAGER_VPN_EVENT_LIST level errors class ca

logging list MANAGER_VPN_EVENT_LIST level errors class svc

logging list MANAGER_VPN_EVENT_LIST level errors class ssl

logging list MANAGER_VPN_EVENT_LIST level errors class dap

logging list MANAGER_VPN_EVENT_LIST level errors class ipaa

logging buffered informational

logging history informational

logging FMC MANAGER_VPN_EVENT_LIST

logging mail critical

logging from-address asa_alert@example.com

logging recipient-address adm@example.com level critical

logging device-id ipaddress inside

logging host inside 192.168.1.100 format emblem

logging debug-trace persistent

logging flash-minimum-free 1024
Configure Feature/Parameter in the Platform Setting Policy

Migrating ASA to Firepower Threat Defense Platform Settings

```plaintext
logging flash-maximum-allocation 3076
logging ftp-bufferwrap
logging ftp-server 10.10.20.25 /syslogs adm-sys-cisco *****
logging permit-hostdown
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
mtu diagnostic 1500
mtu inside 1500
mtu outside 1500
mtu DMZ_SZ 1500
```

Configure Timeout

You can set the global idle timeout durations for the connection and translation slots of various protocols.

ASA Configuration

--- Snippet from ASA running-config ---
Configure Feature/Parameter in the Platform Setting Policy

| ! |
| route app 192.168.100.16 255.255.255.255 30.1.1.10 1 |
| timeout xlate 3:00:00 |
| timeout pat-xlate 0:00:30 |
| timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02 |
| timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 |
| timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 |
| timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute |
| timeout tcp-proxy-reassembly 0:01:00 |
| timeout floating-conn 0:00:00 |
| timeout conn-holddown 0:00:15 |
| timeout igp stale-route 0:01:10 |
| ldap attribute-map ATT-MAP |
| ! |

Configuration on FMC

Step 1 Navigate to Devices > Platform Settings > FTD-Platform_policy.

Step 2 Click Timeouts in the Platform Setting Policy on FMC.

Note—You can configure Console Timeout to modify the timeout setting for management access like SSH.

Figure 93—Configure Timeout

| Console Timeout* | 0 | (0 - 1440 mins) |
| Translation Slot(xlate) | Default | 3:00:00 | (3:00:0 - 3:0:0 - 3:00:0) |
| Connection(Conn) | Default | 1:00:00 | (0:0:0 - 0:30:0 - 1:03:0) |
| Half-Closed | Default | 0:10:00 | (0:0:0 - 0:0:10 - 0:0:0) |
| UDP | Default | 0:02:00 | (0:0:0 - 0:0:10 - 0:0:0) |
| ICMP | Default | 0:00:02 | (0:0:0 - 0:2:0 - 0:02:0) |
| RPC/Num RPC | Default | 0:10:00 | (0:0:0 - 0:0:10 - 0:0:0) |
| H.225 | Default | 1:00:00 | (0:0:0 - 0:0:30 - 1:00:0) |
| H.323 | Default | 0:05:00 | (0:0:0 - 0:0:10 - 0:0:0) |
| SIP | Default | 0:20:00 | (0:0:0 - 0:0:10 - 0:19:0) |
| SIP Media | Default | 0:02:00 | (0:0:0 - 0:0:10 - 0:0:0) |
| SIP Disconnect | Default | 0:02:00 | (0:0:0 - 0:0:10 - 0:0:0) |
| SIP Invite | Default | 0:03:00 | (0:1:0 - 0:1:0 - 0:03:0) |
| SIP Provisional Media | Default | 0:02:00 | (0:0:0 - 0:0:10 - 0:0:0) |
| Floating Connection | Default | 0:00:00 | (0:0:0 - 0:0:30 - 1:19:0) |
The following are the default values:

- Select **Custom** to define your own value.
- Select **Disable** to disable timeout setting.
- Select **Default** to return to the system default value.

Step 3  Click **Save** and deploy the policy to the assigned devices.

**Configuration on FTD After Deployment**

--- Snippet from FTD running-config ----

```

```

--- Snippet from ASA running-config ----

```

```

**Configure Time Synchronization**

Use a Network Time Protocol (NTP) server to synchronize the clock settings on your devices.

By default, the device uses the Firepower Management Center server as the NTP server.

**ASA Configuration**

--- Snippet from ASA running-config ----

```

```

```

```
**Configure Feature/Parameter in the Platform Setting Policy**

```
ntp authenticate
ntp trusted-key 1
ntp server 202.1.1.10 key 1 source outside prefer
ssl server-version tlsv1.2
```

**Note**—The NTP authentication and trusted key parameter are not applicable on FTD.

**Note**—For Firepower 9300 and 4100 platforms that use Firepower Chassis Manager instead to set NTP time synchronization so that Smart Licensing works properly. This also ensures proper timestamps on device registrations. You must use the same NTP server for the Firepower 4100/9300 chassis and the Firepower Management Center.

**Configuration on FMC**

**Step 1** Navigate to Devices > Platform Settings > FTD-Platform_policy.

**Step 2** Click Time Synchronization in the Platform Setting Policy on FMC.

**Figure 94—Time Synchronization**

[Image of Time Synchronization]

**Note**: If selected via NTP from Management Center, then the NTP configured on FMC in System > Configuration > Time Synchronization will be pushed to the managed FTD.

**Step 3** Select the Via NTP from check box and configure the NTP Server IP address.
Configure Feature/Parameter in the Platform Setting Policy

Figure 95 — Configure NTP

**FTD-Platform_policy**
Platform Setting FTD - Internal

---

Step 4  Click **Save** and deploy the policy to assigned devices.

**Configuration on FTD After Deployment**

You can verify NTP configuration on FTD in file **ntp.conf** under directory `/ngfw/etc/` or with command `show ntp` on CLISH mode.

--- Snippet from FTD ---

```
> show ntp
  NTP Server       : 202.1.10.209
  Status           : Unknown
  Offset           : 0.000 (milliseconds)
  Last Update      : - (seconds)

  NTP Server       : 127.0.0.2
  Status           : Being Used
  Offset           : 18.577 (milliseconds)
  Last Update      : - (seconds)

>  
>Expert

root@firepower:/ngfw/etc# cat /ngfw/etc/ntp.conf
# automatically generated by /ngfw/etc/sysconfig/configure-network; do not edit
# Sun Sep 15 20:04:12 UTC 2019
restrict default noquery nomodify notrap nopeer
restrict 127.0.0.1
server 202.1.10.209 iburst
server 127.0.0.2 iburst
```
Configure Feature/Parameter in the Platform Setting Policy

```
logfile /ngfw/var/log/ntp.log
driftfile /ngfw/etc/ntp.drift
tos maxdist 1.5
```

Configure UCAPL/CC Compliance

The Firepower System supports compliance with the following security certifications standards:

- **Common Criteria (CC)**—A global standard established by the international Common Criteria Recognition Arrangement, defining properties for security products
- **Unified Capabilities Approved Products List (UCAPL)**—A list of products meeting security requirements established by the U.S. Defense Information Systems Agency (DISA)

You can enable security certifications compliance in CC mode or UCAPL mode.

**Note**—After you enable this setting, you cannot disable the setting. If you want to take the appliance out of CC or UCAPL mode, you must reimage the appliance.

Before You Begin

- For Firepower Threat Defense devices, ensure that you are not using an evaluation license. You must register the device through a Smart Software Manager account that is enabled with export-controlled functionality.
- You must deploy Firepower Threat Defense device in routed mode to support security certification compliance.

Configuration on FMC

**Step 1** Navigate to Devices > Platform Settings > FTD-Platform_policy.

**Step 2** Click UCAPL/CC Compliance in the Platform Setting Policy on FMC.

**Figure 96—UCAPL/CC Compliance**

**Step 3** To permanently enable security certifications compliance on the appliance, you have two options:

To enable security certifications compliance in Common Criteria mode, choose CC from the Enable UCAPL/CC Compliance drop-down list.
Configure Feature/Parameter in the Platform Setting Policy

- To enable security certifications compliance in Unified Capabilities Approved Products List mode, choose UCAPL from the Enable UCAPL/CC Compliance drop-down list.

Figure 97—Enable Compliance

![Enable UCAPL/CC Compliance](image)

**Note**—Appliances reboot when you enable UCAPL or CC compliance. The Firepower Management Center reboots when you save the system configuration and the managed devices reboot when you deploy configuration changes.

Figure 98—Enable Compliance - Manage Device

![FTD-Platform_policy](image)

**Step 4** Click Yes to enable the Compliance.

**Step 5** Click Save and deploy the policy to assigned devices.