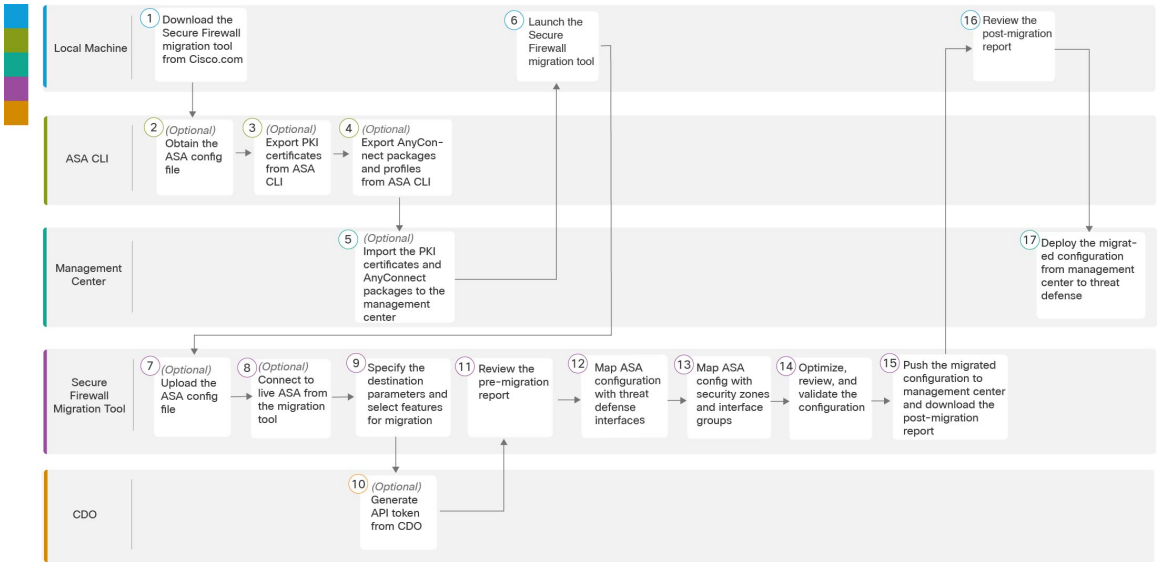


ASA to Threat Defense Migration Workflow

- End-to-End Procedure, on page 1
- Prerequisites for Migration, on page 3
- Run the Migration, on page 6
- Uninstall the Secure Firewall Migration Tool, on page 45
- Sample Migration: ASA to Threat Defense 2100 , on page 45

End-to-End Procedure

The following flowchart illustrates the workflow for migrating an ASA to threat defense using the Secure Firewall migration tool.



	Workspace	Steps
1	Local Machine	Download the latest version of Secure Firewall migration tool from Cisco.com. For detailed steps, see Download the Secure Firewall migration tool from Cisco.com.

	Workspace	Steps
2	ASA CLI	(Optional) Obtain the ASA configuration file: To obtain the ASA config file from ASA CLI, see Obtain the ASA configuration file. If you intend to connect the ASA from Secure Firewall migration tool, skip to step 3.
3	ASA CLI	(Optional) Export PKI certificates from ASA CLI: This step is required only if you are planning to migrate site-to site VPN, RA VPN, or WebVPN configurations from ASA to threat defense. To export the PKI certificates from ASA CLI, see Export PKI Certificate from and Import into Firewall Management Center, step 1. If you are not planning to migrate site-to-site VPN, RA VPN, or WebVPN configurations, skip to step 7.
4	ASA CLI	(Optional) Export AnyConnect packages and profiles from ASA CLI: This step is required only if you are planning to migrate RA VPN features from ASA to threat defense. To export AnyConnect packages and profiles from ASA CLI, see Retrieve AnyConnect Packages and Profiles, step 1. If you are not planning to migrate site-to-site VPN and RA VPN, skip to step 7.
5	Management Center	(Optional) Import the PKI certificates and AnyConnect packages to management center: To import the PKI certificates to management center, see Export PKI Certificate from and Import into Firewall Management Center, step 2 and Retrieve AnyConnect Packages and Profiles, step 2.
6	Local Machine	Launch the Secure Firewall migration tool on your local machine, see Launch the Secure Firewall Migration Tool.
7	Secure Firewall Migration Tool	(Optional) Upload the ASA config file obtained from ASA CLI, see Upload the ASA Configuration File. If you are planning to connect to live ASA, skip to step 8.
8	Secure Firewall Migration Tool	You can connect to live ASA directly from the Secure Firewall migration tool. For more information, see Connect to the ASA from the Secure Firewall Migration Tool.
9	Secure Firewall Migration Tool	During this step, you can specify the destination parameters for the migration. For detailed steps, see Specify Destination Parameters for the Secure Firewall Migration Tool.
10	Security Cloud Control	(Optional) This step is optional and only required if you have selected cloud-delivered Firewall Management Center as destination management center. For detailed steps, see Specify Destination Parameters for the Secure Firewall Migration Tool, step 1.
11	Secure Firewall Migration Tool	Navigate to where you downloaded the pre migration report and review the report. For detailed steps, see Review the Pre-Migration Report.
12	Secure Firewall Migration Tool	The Secure Firewall migration tool allows you to map the ASA configuration with threat defense interfaces. For detailed steps, see Map ASA Configurations with Secure Firewall Device Manager Threat Defense Interfaces.

	Workspace	Steps
13	Secure Firewall Migration Tool	To ensure that the ASA configuration is migrated correctly, map the ASA interfaces to the appropriate threat defense interface objects, security zones and interface groups. For detailed steps, see Map ASA Interfaces to Security Zones and Interface Groups.
14	Secure Firewall Migration Tool	Optimize and review the configuration carefully and validate that it is correct and matches how you want to configure the threat defense device. For detailed steps, see Optimize, Review and Validate the Configuration to be Migrated.
15	Secure Firewall Migration Tool	This step in the migration process sends the migrated configuration to management center and allows you to download the post-migration report. For detailed steps, see Push the Migrated Configuration to Management Center.
16	Local Machine	Navigate to where you downloaded the post migration report and review the report. For detailed steps, see Review the Post-Migration Report and Complete the Migration.
17	Management Center	Deploy the migrated configuration from the management center to threat defense. For detailed steps, see Review the Post-Migration Report and Complete the Migration.

Prerequisites for Migration

Before you migrate your ASA configuration, execute the following activities.

Download the Secure Firewall Migration Tool from Cisco.com

Before you begin

You must have a Windows 10 64-bit or macOS version 10.13 or higher machine with an internet connectivity to Cisco.com.

If you want to use the cloud version of the Secure Firewall migration tool hosted on Security Cloud Control, skip to step 4.

Procedure

Step 1 On your computer, create a folder for the Secure Firewall migration tool.

We recommend that you do not store any other files in this folder. When you launch the Secure Firewall migration tool, it places the logs, resources, and all other files in this folder.

Note
Whenever you download the latest version of the Secure Firewall migration tool, ensure, you create a new folder and not use the existing folder.

Step 2 Browse to https://software.cisco.com/download/home/286306503/type and click **Firewall Migration Tool**.

The above link takes you to the Secure Firewall migration tool under Firewall NGFW Virtual. You can also download the Secure Firewall migration tool from the Firewall Threat Defense device download areas.

Step 3 Download the most recent version of the Secure Firewall migration tool into the folder that you created.

Ensure that you download the appropriate executable of the Secure Firewall migration tool for Windows or macOS machines.

Step 4 If you are a Security Cloud Control user and want to use the migration tool hosted on it, log in to your Security Cloud Control tenant and on the left pane, navigate to **Administration** > **Migration** > **Firewall Migration Tool** to create your migration instance.

What to do next

Obtain the ASA Configuration File

Obtain the Configuration File

You can use one of the following methods to obtain an configuration file:

- Export the Configuration File, on page 4
- Connect to the ASA from the Secure Firewall Migration Tool, on page 10

Export the Configuration File

This task is required only if you want to manually upload an configuration file. If you want to connect to an from the Secure Firewall migration tool, skip to Connect to the ASA from the Secure Firewall Migration Tool, on page 10.

Note Do not hand code or make changes to the configuration after you export the file. These changes will not be migrated, and they create errors in the migration or cause the migration to fail. For example, opening and saving the configuration file in terminal can add white space or blank lines that the Secure Firewall migration tool cannot parse.

Ensure that the exported configuration file does not contain the **--More--** keyword as text, because this can cause the migration to fail.

Procedure

Step 1 Use the **show running-config** command for the ASA device or context that you are migrating and copy the configuration from there. See View the Running Configuration.

Alternately, use Adaptive Security Device Manager (ASDM) for the ASA device or context that you want to migrate and choose **File** > **Show Running Configuration in New Window** to obtain the configuration file.

Note

For a multi context , you can use the **show tech-support** command to obtain the configuration for all the contexts in a single file.

Step 2 Save the configuration as either `.cfg` or `.txt`.

You cannot upload the configuration to the Secure Firewall migration tool if it has a different extension.

Step 3 Transfer the configuration file to your computer where you downloaded the Secure Firewall migration tool.

Export PKI Certificate from ASA and Import into Management Center

Before you begin

The Secure Firewall migration tool supports migration of certificate-based VPN into the management center.

ASA uses the trustpoint model for storing certificates in the configuration. A trustpoint is a container in which certificates are stored. ASA trustpoint can store up to two certificates.

The ASA trustpoint or certificates in the ASA configuration file contains hash values. Hence, you cannot directly import them into a management center.

In the destination management center, migrate the ASA trustpoint or the VPN certificates manually as PKI objects as part of the pre-migration activity.

Procedure

Step 1 Use the following command to export the PKI certificate through the CLI from the source ASA config with the keys to a PKCS12 file:

```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```

Step 2 Import the PKI certificate into a management center (**Object Management PKI Objects)**.

For more information, see PKI Objects in the *Firepower Management Center Configuration Guide*.

The manually created PKI objects can now be used in the Secure Firewall migration tool under the **Trustpoint** section in **Remote Access VPN** tab in the **Optimize, Review, and Validate** page.

Retrieve AnyConnect Packages and Profiles

AnyConnect profiles are optional and can be uploaded through the management center or Secure Firewall migration tool.

Before you begin

- Remote Access VPN on the management center requires at least one AnyConnect package.
- If the configuration consists of Hostscan and External Browser package, you must upload these packages.

- All packages must be added to the management center as part of the pre-migration activity.
- Dap.xml and Data.xml must be added through the Secure Firewall migration tool.

Procedure

Step 1 Use the following command to copy the required package from the source ASA to an FTP or TFTP server:

```
Copy <source file location:/source file name> <destination>
ASA# copy disk0:/anyconnect-win-4.10.02086-webdeploy-k9.pkg tftp://1.1.1.1 <----- Example
of copying Anyconnect Package.
ASA# copy disk0:/ external-sso- 4.10.04071-webdeploy-k9.zip tftp://1.1.1.1 <----- Example
of copying External Browser Package.
ASA# copy disk0:/ hostscan_4.10.04071-k9.pkg tftp://1.1.1.1 <----- Example of copying
Hostscan Package.
ASA# copy disk0:/ dap.xml tftp://1.1.1.1. <----- Example of copying Dap.xml
ASA# copy disk0:/ sdesktop/data.xml tftp://1.1.1.1 <----- Example of copying Data.xml
ASA# copy disk0:/ VPN_Profile.xml tftp://1.1.1.1 <----- Example of copying Anyconnect
Profile.
```

Step 2 Import the downloaded packages to management center (**Object Management** > **VPN** > **AnyConnect File**).

a. Dap.xml and Data.xml must be uploaded to the management center from the Secure Firewall migration tool in the **Review and Validate** > **Remote Access VPN** > **AnyConnect File** section.

b. AnyConnect profiles can be uploaded directly to the management center or through the Secure Firewall migration tool in the **Review and Validate** > **Remote Access VPN** > **AnyConnect File** section.

The manually uploaded files can now be used in the Secure Firewall migration tool.

Run the Migration

Launch the Secure Firewall Migration Tool

This task is applicable only if you are using the desktop version of the Secure Firewall migration tool. If you are using the cloud version of the migration tool hosted on Security Cloud Control, skip to Upload the ASA Configuration File, on page 9 .



Note When you launch the desktop version of the Secure Firewall migration tool a console opens in a separate window. As you go through the migration, the console displays the progress of the current step in the Secure Firewall migration tool. If you do not see the console on your screen, it is most likely to be behind the Secure Firewall migration tool.

Before you begin

- Download the Secure Firewall Migration Tool from Cisco.com
- Review and verify the requirements in the Supported Target Management Center for Migration section.

- Ensure that your computer has a recent version of the Google Chrome browser to run the Secure Firewall migration tool. For information on how to set Google Chrome as your default browser, see Set Chrome as your default web browser.
- If you are planning to migrate a large configuration file, configure sleep settings so the system doesn't go to sleep during a migration push.

Procedure

Step 1 On your computer, navigate to the folder where you downloaded the Secure Firewall migration tool.

Step 2 Do one of the following:

- On your Windows machine, double-click the Secure Firewall migration tool executable to launch it in a Google Chrome browser.

  If prompted, click **Yes** to allow the Secure Firewall migration tool to make changes to your system.

  Note
  Ensure you disable any popup blockers in your browser because they might hinder login popus from appearing.

  The Secure Firewall migration tool creates and stores all related files in the folder where it resides, including the log and resources folders.

- On your Mac move, the Secure Firewall migration tool `*.command` file to the desired folder, launch the Terminal application, browse to the folder where the Secure Firewall migration tool is installed and run the following commands:

  ```
  # chmod 750 Firewall_Migration_Tool-version_number.command
  # ./Firewall_Migration_Tool-version_number.command
  ```

  The Secure Firewall migration tool creates and stores all related files in the folder where it resides, including the log and resources folders.

  Tip
  When you try to open the Secure Firewall migration tool, you get a warning dialog because the Secure Firewall migration tool is not registered with Apple by an identified developer. For information on opening an application from an unidentified developer, see Open an app from an unidentified developer.

  Note
  Use MAC terminal zip method.

Step 3 On the **End User License Agreement** page, click **I agree to share data with Cisco Success Network** if you want to share telemetry information with Cisco, else click **I'll do later**.

When you agree to send statistics to Cisco Success Network, you are prompted to log in using your Cisco.com account. Local credentials are used to log in to the Secure Firewall migration tool if you choose not to send statistics to Cisco Success Network.

Step 4 On the Secure Firewall migration tool's login page, do one of the following:

- To share statistics with Cisco Success Network, click the **Login with CCO** link to log in to your Cisco.com account using your single sign-on credentials. If you do not have a Cisco.com account, create it on the Cisco.com login page.

  Proceed to step 8, if you have used your Cisco.com account to log in.

- If you have deployed your firewall in an air-gapped network that does not have internet access, contact Cisco TAC to receive a build that works with administrator credentials. Note that this build does not send usage statistics to Cisco, and TAC can provide you the credentials.

Step 5 On the **Reset Password** page, enter the old password, your new password, and confirm the new password.

The new password must have 8 characters or more and must include upper and lowercase letters, numbers, and special characters.

Step 6 Click **Reset**.

Step 7 Log in with the new password.

Note
If you have forgotten the password, delete all the existing data from the <*migration_tool_folder*> and reinstall the Secure Firewall migration tool.

Step 8 Review the premigration checklist and make sure you have completed all the items listed.

If you have not completed one or more of the items in the checklist, do not continue until you have done so.

Step 9 Click **New Migration**.

Step 10 On the **Software Update Check** screen, if you are not sure you are running the most recent version of the Secure Firewall migration tool, verify the version on Cisco.com.

Step 11 Click **Proceed**.

What to do next

You can proceed to the following step:

- If you have exported configuration to your computer, proceed to Upload the Configuration File.
- If you want to extract information from an using the Secure Firewall migration tool, proceed to Connect to the ASA from the Secure Firewall Migration Tool, on page 10

Using the Demo Mode in the Secure Firewall Migration Tool

When you launch the Secure Firewall Migration tool and are on the **Select Source Configuration** page, you can choose to start performing a migration using **Start Migration** or enter the **Demo Mode**.

The demo mode provides an opportunity to perform a demo migration using dummy devices and visualize how an actual migration flow would look like. The migration tool triggers the demo mode based on the selection you make in the **Source Firewall Vendor** drop-down; you can also upload a configuration file or connect to a live device and continue with the migration. You can proceed performing the demo migration by selecting demo source and target devices such as demo FMC, demo FTD devices, or Multicloud Defense.

Caution Choosing **Demo Mode** erases existing migration workflows, if any. If you use the demo mode while you have an active migration in **Resume Migration**, your active migration is lost and needs to be restarted from first, after you use the demo mode.

You can also download and verify the pre-migration report, map interfaces, map security zones, map interface groups, and perform all other actions like you would in an actual migration workflow. However, you can only perform a demo migration up to validation of the configurations. You cannot push the configurations to the demo target devices you selected because this is only a demo mode. You can verify the validation status and the summary and click **Exit Demo Mode** to go the **Select Source Configuration** page again to start your actual migration.

Note The demo mode lets you leverage the whole feature set of the Secure Firewall Migration Tool, except pushing of configurations, and do a trial run of the end-to-end migration procedure before performing your actual migration.

Upload the ASA Configuration File

Before you begin

Export the configuration file as `.cfg` or `.txt` from the source ASA device.

Note Do not upload a hand-coded or manually altered configuration file. Text editors add blank lines and other issues to the file that can cause the migration to fail.

Procedure

Step 1 On the **Extract ASA Information** page, in the **Manual Upload** section, click **Upload** to upload an ASA configuration file.

Step 2 Browse to where the configuration file is located and click **Open**.

The Secure Firewall migration tool uploads the configuration file. For large configuration files, this step takes a longer time. The console provides a line by line log view of the progress, including the ASA configuration line that is being parsed. If you do not see the console, you can find it in a separate window behind the Secure Firewall migration tool.

The **Context Selection** section identifies if the uploaded configuration corresponds to the multi-context ASA.

Step 3 Review the **Context Selection** section and select the context that you want to migrate.

What to do next

Specify Destination Parameters for the Secure Firewall Migration Tool, on page 12

Connect to the ASA from the Secure Firewall Migration Tool

The Secure Firewall migration tool can connect to an ASA device that you want to migrate and extract the required configuration information.

Before you begin

- Download and launch the Secure Firewall migration tool.
- For single context ASA, obtain the management IP address, administrator credentials, and the enable password.
- For multi-context mode ASA, obtain the IP address of the **admin** context, administrator credentials, and the enable password.

Note If ASA is not configured with **Enable Password**, you can leave the field blank on the Secure Firewall migration tool.

Procedure

Step 1 On the **Extract ASA Information** screen, in the **Connect to ASA** section, click **Connect** to connect to the ASA device that you want to migrate.

Step 2 On the **ASA Login** screen, enter the following information:

a. In the **ASA IP Address/Hostname** field, enter the management IP address or hostname (for single context ASA) or IP address of the admin context or hostname (for a multi-context ASA).

b. In the **Username**, **Password**, and **Enable Password** fields enter the appropriate administrator login credentials.

Note
If ASA is not configured with an **Enable password**, you can leave the field blank on the Secure Firewall migration tool.

c. Click **Login**.

When the Secure Firewall migration tool connects to the ASA, it displays a successfully connected to the ASA message.

For a multi-context ASA, the Secure Firewall migration tool identifies and lists the contexts.

Step 3 Select the ASA context that you want to migrate from the **Context** drop-down list.

Step 4 (Optional) Select **Collect Hitcounts**.

When checked, this tool computes the number of times an ASA rule was used and the last time the rule was used since ASA uptime or last ASA restart and displays this information on the **Review and Validate** page. This allows you to evaluate the efficacy and relevance of the rule before migration.

Step 5 Click **Start Extraction**.

The Secure Firewall migration tool connects to the ASA and starts extracting configuration information. When the extraction completes successfully, the **Context Selection** section identifies if the uploaded configuration corresponds to a single-context or multi-context ASA.

Select the ASA Security Context

Before you begin

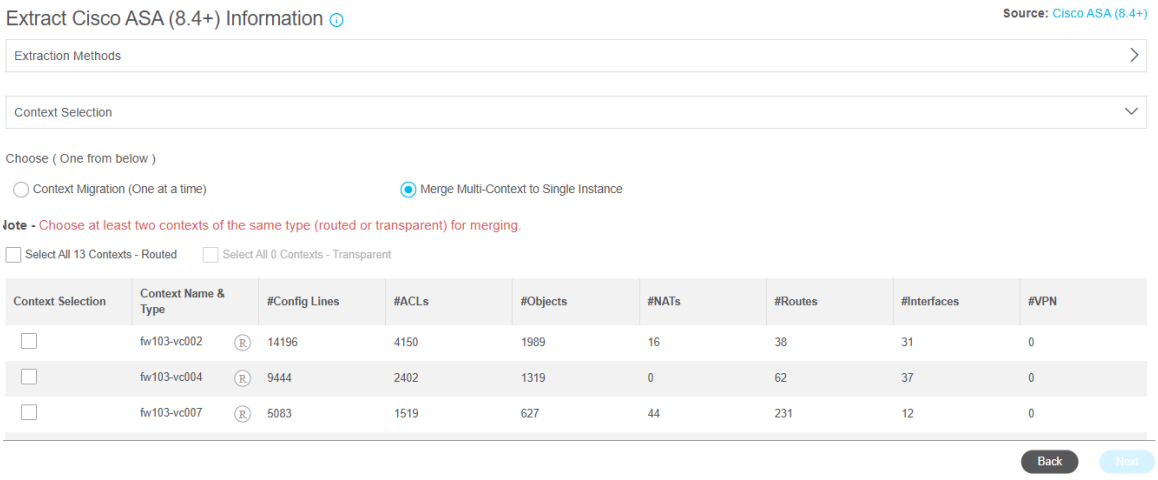
You can partition a single ASA device into multiple virtual devices, and these partitions are known as security contexts. Each security context acts as an independent device, with its own security policies, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices, while you actually have only one device. To know more about security contexts, see Common Uses for Security Contexts in the *Cisco ASA Series General Operations CLI Configuration Guide*.

This task procedure is applicable to you if you have configured two or more security contexts on your Cisco Secure Firewall ASA. When you upload your ASA configuration, the Secure Firewall migration tool detects security contexts on your device, parses all the configuration information pertaining to the contexts, and displays them on the **Context Selection** page.

Procedure

Step 1 Upload your ASA configuration file; if your configuration file contains contexts, the migration tool displays the names of all the security contexts.

Figure 1: Extract Cisco ASA (8.4+) Information window



Step 2 (Optional) To migrate configurations from one of your contexts, click the **Context Migration (One at a time)** radio button and choose a context to proceed with migration.

Step 3 (Optional) To merge configurations from multiple contexts into a single instance and migrate them, do the following:

Note
Make sure that you read these prerequisites before attempting to merge multiple contexts:

- If you have port channels configured on your ASA, ensure they are configured in your target Firewall Threat Defense device also.
- If two interfaces have the same VLAN ID and subinterface ID, the migration tool automatically adds new VLAN and subinterface IDs to a new interface. Information about these IDs is part of the premigration report. Ensure that you configure these new interfaces created by the migration tool to the trunk port objects of the corresponding devices. This is because Firewall Threat Defense devices do not allow two interfaces with the same VLAN and subinterface IDs.
- The AS path objects must be unique across all the contexts that are being migrated. Duplicates are not migrated.

a) Click the **Merge Multi-Context to Single Instance** radio button. When you opt for multicontext merging, you can see context information such as the number of configuration lines, ACLs, objects, routes including static routes, PBR, and ECMP, and interfaces.
b) If you want to merge all routed-mode firewall contexts, check the **Select All Context - Routed** check box, to merge all transparent-mode firewall contexts, check the **Select All Context - Transparent** check box.

Note
When merging multiple contexts, if two or more of the contexts that you have chosen to merge have VPN configured, the migration tool prompts you to select one of the contexts with VPN configuration. Only the VPN configuration in the selected context is migrated and those from the other contexts are ignored. However, note that all the other configurations, such as objects, extended ACLs, NAT rules, and unreferenced VPN objects in the unselected contexts are still migrated.

Step 4 Click **Start Parsing**. Once you select a context and start to parse, the migration tool merges the configurations from all the contexts, parses them, and displays the **Parsed Summary**. If you are performing a merged-context migration, note that the number of contexts you selected to migrate is the same as the number of VRFs in the parsed summary. However, if you have a context with VPN configuration, the parsed summary displays one VRF less, because the VRF that has the VPN configuration gets pushed to the global router directly.

Note
If you have clicked **Start Parsing** and you wish to select a different context, you cannot go back and select a different context. You can click **Back** and start from uploading your configuration file, selecting a different context this time.

Step 5 Review the summary of the elements in the uploaded configuration file that the Secure Firewall migration tool detected and parsed.

Step 6 Click **Next** to select the target parameters.

Specify Destination Parameters for the Secure Firewall Migration Tool

Before you begin

If you are using the cloud version of the migration tool hosted on Security Cloud Control, skip to Step 3.

- Obtain the IP address for the Firewall Management Center for On-Prem Firewall Management Center.

- From Secure Firewall Migration Tool 3.0 onwards, you can select between On-Prem Firewall Management Center or Cloud-delivered Firewall Management Center.
- For Cloud-delivered Firewall Management Center, region and API token have to be provided. For more information, see Supported Target Management Center for Migration.
- Create a dedicated account for the Secure Firewall migration tool in the Firewall Management Center with sufficient privileges to access the REST API, as described in User Accounts for Management Access.
- (Optional) If you want to migrate device-specific configurations like interfaces and routes, add the target Firewall Threat Defense to the Firewall Management Center. See Adding Devices to the Firewall Management Center
- If it requires you to apply IPS or file policy to ACL in the **Review and Validate** page, we highly recommend you create a policy on the Firewall Management Center before migration. Use the same policy, as the Secure Firewall migration tool fetches the policy from the connected Firewall Management Center. Creating a new policy and assigning it to multiple access control lists may degrade the performance and may also result in a push failure.

Procedure

Step 1 On the **Select Target** screen, in the **Firewall Management** section, do the following: you can choose to migrate to an On-Prem Firewall Management Center or Cloud-delivered Firewall Management Center:

- For migrating to an On-Prem Firewall Management Center, do the following:

a) Click the **On-Prem FMC** radio button.
b) Enter the IP address or Fully-Qualified Domain Name (FQDN) for the management center.
c) In the **Domain** drop-down list, select the domain to which you are migrating.

   If you want to migrate to a Firewall Threat Defense device, you can only migrate to the Firewall Threat Defense devices available in the selected domain.

d) Click **Connect** and proceed to **Step 2**.

- For migrating to a Cloud-delivered Firewall Management Center, do the following:

a) Click the **Cloud-delivered FMC** radio button.
b) Choose the region and paste the Security Cloud Control API token. For generating the API token. from Security Cloud Control, follow the below steps:

   1. Log in to Security Cloud Control.
   2. From the top-right corner, navigate to **Preferences** > **General Preferences** and copy the API Token from **My Tokens** section.

c) Click **Connect** and proceed to **Step 2**.

Step 2 In the **Firewall Management Center Login** dialog box, enter the username and password of the dedicated account for the Secure Firewall migration tool, and click **Login**.

The Secure Firewall migration tool logs in to the Firewall Management Center and retrieves a list of Firewall Threat Defense devices that are managed by that Firewall Management Center. You can view the progress of this step in the console.

Step 3 Click **Proceed**.

In the **Choose Threat Defense** section, you can either select a Firewall Threat Defense device that you want to migrate to, or if you do not have a Firewall Threat Defense device, you can migrate the shared policies (Access Control Lists, NAT, and Objects) of the ASA configuration to the Firewall Management Center.

Step 4 In the **Choose FTD** section, do one of the following:

- Click the **Select FTD DeviceSelect FTD Device (Includes FTD - Standalone/HA Pair)** drop-down list and check the device where you want to migrate the ASA configuration.

  Note
  This list includes both standalone threat defense devices and devices that are part of a high availability (HA) pair on the target Firewall Management Center.

  The devices in the selected Firewall Management Center domain are listed by **IP Address**, **Name**, **Device Model**, and **Mode** (routed or transparent).

  Note
  At minimum, the native Firewall Threat Defense device you choose must have the same number of physical or port channel interfaces as the ASA configuration that you are migrating. At minimum, the container instance of the Firewall Threat Defense device must have the same number of physical or port channel interfaces and subinterfaces. You must configure the device with the same firewall mode as the ASA configuration. However, these interfaces do not have to have the same names on both devices.

  Note
  Only when the supported target threat defense platform is Firewall 1010 with management center version 6.5 or later.6.5, FDM 5505 migration support is applicable for shared policies and not for device specific policies. When you proceed without threat defense, the Secure Firewall migration tool will not push any configurations or the policies to the threat defense. Thus, interfaces and routes, and site-to-site VPN which are threat defense device-specific configurations will not be migrated. However, all the other supported configurations (shared policies and objects) such as NAT, ACLs, and port objects will be migrated. Remote Access VPN is a shared policy and can be migrated even without threat defense.

Table 1: ASA Firewall Features and Supported Firewall Management Center or Firewall Threat Defense Versions

Firewall Features	Supported Management Center or Threat Defense Version
with remote deployment	6.7 or later
Crypto Map Site-to-Site VPN	6.6 or later
Virtual Tunnel Interface (VTI) and Route-based (VTI)	6.7 or later
Dynamic-Route Objects and BGP	7.1 or later
Remote Access VPN	• Management Center 7.2 or later • Threat Defense 7.0 or later.
EIGRP	• Management Center 7.2 or later • Threat Defense 7.0 or later.

Firewall Features	Supported Management Center or Threat Defense Version
PBR	• Management Center 7.3 or later • Threat Defense 7.3 or later.
ECMP	• Management Center 7.1 or later • Threat Defense 6.5 or later.
WebVPN	• Management Center 7.4 or later • Threat Defense 7.4 or later
SNMP	• Management Center 7.4 or later • Threat Defense 7.4 or later
DHCP Relay, Server, and DDNS	• Management Center 7.4 or later • Threat Defense 7.4 or later

Note
To migrate Site-to-Site VPN, VTI, and Route-based (VTI) interfaces, Firewall Threat Defense must be configured on Firewall Management Center.

- For ASA 5505, the device-specific configs (Interface and routes) and shared policies (NAT, ACLs, and Objects) can be migrated only when the supported target Firewall Threat Defense platform is Firewall 1010 with Firewall Management Center version 6.5 or later.

  Note
  - If the target Firewall Threat Defense is not FPR-1010 or the target Firewall Management Center is earlier than 6.5, ASA 5505 migration support is applicable for shared policies only. Device specifics will not be migrated.
  - You can select only FPR-1010 in the **Select Device** drop-down list as the source config is ASA 5505.
  - ASA-SM migration support is for shared policies only. Device specifics will not be migrated.

- Click **Proceed without FTD** to migrate the configuration to the Firewall Management Center.

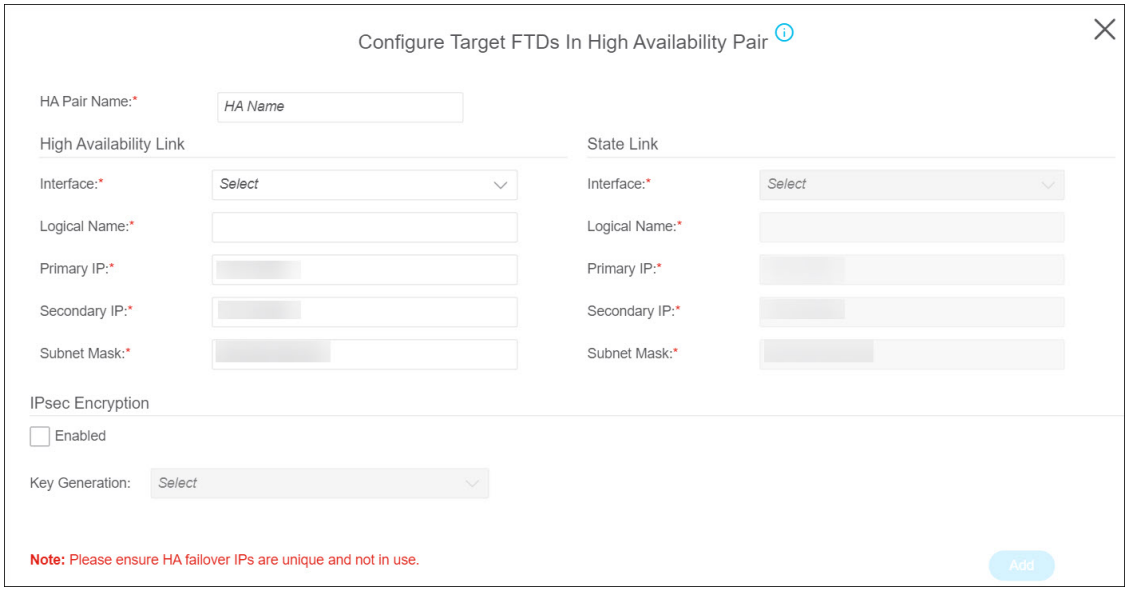
  When you proceed without Firewall Threat Defense, the Secure Firewall migration tool will not push any configurations or the policies to Firewall Threat Defense. Thus, interfaces and routes, and site-to-site VPN which are Firewall Threat Defense device-specific configurations will not be migrated and need to be manually configured on Firewall Management Center. However, all the other supported configurations (shared policies and objects) such as NAT, ACLs, and port objects will be migrated. Remote Access VPN is a shared policy and can be migrated even without threat defense.

- This option displays only if the source ASA device is in an HA pair.

  Click **Proceed with FTD HA Pair Configuration** to select active and standby threat defense devices for your HA pair. When you select the active device, ensure that there is an identical device on the target

Firewall Management Center for FMT to be able to show up the idential device as the standby device option and the HA pair creation to be successful.

Note
You cannot proceed to the further steps of migration if there is no identical device on the target Firewall Management Center to be selected as the standby device or if you do not select a standby threat defense device.



Click **Setup FTD HA Pair** and configure the following on the **Configure Target FTDs in High Availability Pair** window:

a. Specify a name for the HA pair in the **HA Pair Name** filed.

b. Under **High Availability Link**, choose an **Interface** which has enough bandwidth to reserve when failover communications need to happen.

Note
The **Interface** drop-down lists only the interfaces which do not have a logical name and are not part of any security zones.

c. Specify a **Logical Name** for the interface.

d. Specify a **Primary IP** address for the high availability link on the active device unit. Ensure that the IP address is on an unused subnet.

e. Specify a **Secondary IP** address for the high availability link on the standby device unit. Ensure that the secondary IP address is on the same subnet as the primary IP address.

f. Specify a **Subnet Mask** that applies to both the primary and secondary IP addresses.

g. Under **State Link**, choose **Same as LAN Failover Link** or a different **Interface**. Selecting the **Same as LAN Failover Link** populates the data from the failover link that you just configured.

h. Check the **Enabled** checkbox under **IPsec Encryption** to enable encryption between the failover links and choose a **Key Generation** method.

i. Click **Add** to start setting up the HA pair.

Note that the **Notifications Center** icon keeps blinking until the creation of HA pair is in progress. In cases where the creation of HA pair fails for some reason, FMT notifies you by showing a **Blocked** error message. In such cases, because the migration tool attempted to create the HA pair and failed, the Firewall Management Center will have the HA pair created but not successful.

Log in to the Firewall Management Center and break the HA manually and select **Click Here** in the error message in the migration tool to start to configure the HA pair again. For more information on how to break an HA pair, see:

- Break a High Availability Pair if the target Firewall Management Center is On-Premises Firewall Management Center
- Break a High Availability Pair if the target Firewall Management Center is Cloud-delivered Firewall Management Center

Note
The values entered or populated as part of the other migration steps are retained even if the HA setup fails and is to be re-configured.

Step 5 Click **Proceed**.

Depending on the destination that you are migrating to, the Secure Firewall migration tool allows you to select the features that you want to migrate.

Step 6 Click the **Select Features** section to review and select the features that you want to migrate to the destination.

- If you are migrating to a destination Firewall Threat Defense device, the Secure Firewall migration tool automatically selects the features available for migration from the ASA configuration in the **Device Configuration** and **Shared Configuration** sections. You can further modify the default selection, according to your requirements.
- If you are migrating to a Firewall Management Center, the Secure Firewall migration tool automatically selects the features available for migration from theASA configuration in the **Device Configuration**, **Shared Configuration**, and **Optimization** sections. You can further modify the default selection, according to your requirements.
- The Secure Firewall migration tool supports the following for access control during migration:
  - Populate Destination Security Zones—Enables mapping of destination zones for the ACL during migration.

    Route-lookup logic is limited to Static Routes and Connected Routes, whereas PBR, Dynamic Routes, and NAT are not considered. Interface network configuration is used to derive the connected route information.

    Based on the nature of Source and Destination network object-groups, this operation may result in rule explosion.

  - Migrate Tunneled rules as Prefilter—Mapping of ASA encapsulated tunnel protocol rule to Prefilter tunnel rules has the following advantages:
    - Tailor Deep Inspection—For encapsulated traffic and to improve performance with fastpathing.
    - Improve Performance—You can fastpath or block any other connections that benefit from early handling.

The Secure Firewall migration tool identifies the encapsulated tunnel traffic rules in source configuration and migrates them as Prefilter tunnel rules. You can verify the migrated tunnel rule under the Prefilter policy. The Prefilter policy is associated with the migrated access control policy on Firewall Management Center.

The protocols which are migrated as Prefilter tunnel rules are following:

- GRE (47)
- IPv4 encapsulation (4)
- IPv6 encapsulation (41)
- Teredo Tunneling (UDP:3544)

Note
If you do not opt to select the prefilter option, all the tunneled traffic rules will be migrated as unsupported rules.

The ACL tunnel rules (GRE and IPnIP) in the ASA configuration are currently migrated as bidirectional by default. You can now specify the Rule direction for the destination as bidirectional or unidirectional in the access control state option.

- The Secure Firewall migration tool supports the following interfaces and objects for VPN Tunnel migration:
  - Policy-based (Crypto Map)—If the target Firewall Management Center and Firewall Threat Defense is version 6.6 or later.
  - Route-based (VTI)—If the target Firewall Management Center and Firewall Threat Defense is version 6.7 or later.
- The Secure Firewall migration tool supports migration of Remote Access VPN if the target management center is 7.2 or later. Remote Access VPN is a shared policy that can be migrated without threat defense. If migration is selected with threat defense, the threat defense version should be 7.0 or later.
- (Optional) In the **Optimization** section, select **Migrate only referenced objects** to migrate only those objects that are referenced in an access control policy and a NAT policy.

  Note
  When you select this option, unreferenced objects in the ASA configuration will not be migrated. This optimizes migration time and cleans out unused objects from the configuration.
- (Optional) In the **Optimization** section, select **Object group search** for optimal memory utilization by access policy on Firewall Threat Defense.
- (Optional) In the **Inline Grouping** section, the Secure Firewall migration tool allows you to clear the access rules of the pre-defined network and service object names that start with CSM or DM. If you uncheck this option, the pre-defined object names will be retained during migration. For more information, see Inline Grouping.

  Note
  By default, the option of Inline Grouping is enabled.
- If you have **SNMP** and **DHCP Server**, **Relay**, and **DDNS** configurations on your source ASA device, the corresponding checkboxes are checked by default. Manually uncheck them if you do not want to migrate these configurations. Note that when DHCP is selected, you can either check **Server** or both **Relay** and **DDNS**.

- If you have group policies with SSL clientless VPN tunnel protocol configurations and tunnel groups with group policies that use SAML authentication, the migration tool checks the **WebVPN** checkbox by default. Ensure you manually uncheck this if you do not want to migrate these configurations.

Step 7 Click **Proceed**.

Step 8 In the **Rule Conversion/ Process Config** section, click **Start Conversion** to initiate the conversion.

Step 9 Review the summary of the elements that the Secure Firewall migration tool converted.

To check whether your configuration file is successfully uploaded and parsed, download and verify the **Pre-Migration Report** before you continue with the migration.

Step 10 Click **Download Report** and save the **Pre-Migration Report**.

A copy of the **Pre-Migration Report** is also saved in the `Resources` folder in the same location as the Secure Firewall migration tool.

What to do next

Review the Pre-Migration Report, on page 20

Inline Grouping

Object Grouping by ASDM and CSM Managed ASA

When you enter more than one item (object or inline values) in the source or destination address, or source or destination service, CSM or ASDM automatically creates an object group. The naming conventions for these object groups that are used by CSM and ASDM are CSM_INLINE and DM_INLINE respectively while deploying the configuration on to respective ASA device.

Note To change the behavior of the object grouping from **Tools** > **Preferences**, choose **Auto-expand network and service objects with specified prefix** rule table preference.

The following is the configuration snippet extracted using the **show run** command on ASA managed by ASDM.

```
object network host1
 host 10.1.1.100
object network fqdn_obj1
 fqdn abc.cisco.com
object-group network DM_INLINE_NETWORK_1
 network-object 10.21.44.189 255.255.255.255
 network-object 10.21.44.190 255.255.255.255
object-group network DM_INLINE_NETWORK_2
 network-object 10.21.44.191 255.255.255.255
 network-object object host1
 network-object object fqdn_obj1


access-list CSM_DM_ACL extended permit tcp object-group DM_INLINE_NETWORK_1 object-group
DM_INLINE_NETWORK_2
```

In the above example, access-list CSM_DM_ACL on ASDM UI does not show DM_INLINE group as rule's Source and Destination network instead displays contents of DM_INLINE group.

Inline Grouping—ASDM/CSM

The Inline Grouping functionality of the Secure Firewall migration tool allows you to parse **show running-configuration** of ASDM or CSM managed ASA devices. It provides an option to preserve the same UI representation of the access-list rules as on ASDM or CSM. If opted out, migrated rules will refer to DM_INLINE groups as recorded in ASA **show running-configuration**.

Note The source ASA configuration file input to the Secure Firewall migration tool would still be **show run** or **show tech** collected from ASA or via live connection to ASA device (SSH). The Secure Firewall migration tool does not support any other form of configuration files or methods.

The following figures show how the Source and Destination Network fields of ACE or RULE change based on the enabling or disabling the inline grouping option respectively.

Figure 2: With Inline Grouping—ASDM/CSM Enabled

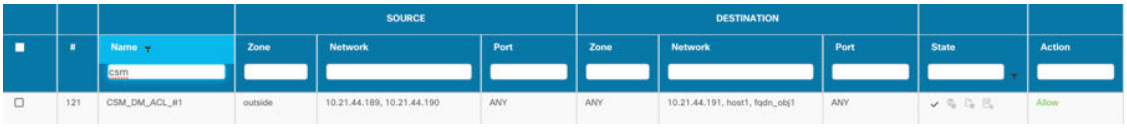


Figure 3: With Inline Grouping—ASDM/CSM Disabled



Review the Pre-Migration Report

If you have missed to download the Pre-Migration Reports during migration, use the following link to download:

Pre-Migration Report Download Endpoint—http://localhost:8888/api/downloads/pre_migration_summary_html_format

Note You can download the reports only when the Secure Firewall Migration Tool is running.

Procedure

Step 1 Navigate to the location where you downloaded the **Pre-Migration Report**.

Note
A copy of the **Pre-Migration Report** is also saved in the `Resources` folder in the same location as the Secure Firewall Migration Tool.

Step 2 Open the **Pre-Migration Report** and carefully review its contents to identify issues, if any, that may cause the migration to fail.

The **Pre-Migration Report** includes the following information:

- **Overall Summary**—The method used to extract the ASA configuration information or connecting to a live ASA configuration.

  If connecting to a live ASA, the firewall mode detected on the ASA, and for multiple context mode, the context you chose for migration.

  A summary of the supported ASA configuration elements that can be successfully migrated to Firewall Threat Defense or Multicloud Defense and specific ASA features selected for migration.

  While connecting to a live ASA, the summary includes the hit count information- the number of times an ASA rule was encountered and its time-stamp information.

- **Configuration Lines with Errors**—Details of ASA configuration elements that cannot be successfully migrated because the Secure Firewall Migration Tool could not parse them. Correct these errors in the ASA configuration, export a new configuration file, and then upload the new configuration file to the Secure Firewall Migration Tool before proceeding.

- **Object and Object Groups Conflict Resolution**—Details of ASA network and service objects and object, service, and protocol object groups that have conflicts across the contexts you are trying to migrate. To view detailed information about these object conflicts, click the **Link for Conflict Count**; you can check the reason for the conflicts and also know how the migration tool is handling the conflicts.

- **Ignored Configuration**—Details of ASA configuration elements that are ignored because they are not supported by the Firewall Management Center or the Secure Firewall Migration Tool. The Secure Firewall Migration Tool does not parse these lines. Review these lines, verify whether each feature is supported in Firewall Management Center, and if not supported, plan to configure the features manually. Click **Link for the ignored configuration lines** to view all the ignored lines.

For more information about the supported features in Firewall Management Center and Firewall Threat Defense, see the Cisco Secure Firewall Management Center Device Configuration Guide.

Step 3 (Optional) If the **Pre-Migration Report** recommends corrective actions, complete the corrections in the ASA interface, export the ASA configuration file again, and upload the updated configuration file before proceeding.

Step 4 After your ASA configuration file is successfully uploaded and parsed, return to the Secure Firewall Migration Tool, and click **Next** to continue the migration.

What to do next

Map ASA Interfaces with Firepower Threat Defense Interfaces

Map ASA Configurations with Firewall Threat Defense Interfaces

The Firewall Threat Defense device must have an equal or greater number of physical and port channel interfaces than those used by ASA configuration. These interfaces do not have to have the same names on both devices. You can choose how you want to map the interfaces.

On the **Map FTD Interface** screen, the Secure Firewall migration tool retrieves a list of the interfaces on the Firewall Threat Defense device. By default, the Secure Firewall migration tool maps the interfaces in ASA and the Firewall Threat Defense device according to their interface identities. For example, the 'management-only' interface on the ASA interface is automatically mapped to the 'management-only' interface on the Firewall Threat Defense device and is unchangeable.

The mapping of ASA interface to the Firewall Threat Defense interface differs based on the Firewall Threat Defense device type:

- If the target Firewall Threat Defense is of native type:
  - The Firewall Threat Defense must have equal or a greater number of used ASA interfaces or port channel (PC) data interfaces (excluding management-only and subinterfaces in the ASA configuration). If the number is less, add the required type of interface on the target Firewall Threat Defense.
  - Subinterfaces are created by the secure Firewall migration tool based on physical interface or port channel mapping.
- If the target Firewall Threat Defense is of container type:
  - The Firewall Threat Defense must have equal or a greater number of used ASA interfaces, physical subinterfaces, port channel, or port channel subinterfaces (excluding management-only in ASA configuration). If the number is less, add the required type of interface on the target Firewall Threat Defense. For example, if the number of physical interfaces and physical subinterface on the target Firewall Threat Defense is 100 less than that of ASA then you can create the additional physical or physical subinterfaces on the target Firewall Threat Defense.
  - Subinterfaces are not created by the Secure Firewall migration tool. Only interface mapping is allowed between physical interfaces, port channel, or subinterfaces.

Before you begin

Make sure you have connected to the Firewall Management Center and chosen the destination as Firewall Threat Defense. For more information, see Specify Destination Parameters for the Secure Firewall Migration Tool, on page 12.

Note This step is not applicable if you are migrating to a Firewall Management Center without a Firewall Threat Defense device.

Procedure

Step 1 If you want to change an interface mapping, click the drop-down list in the **FTD Interface Name** and choose the interface that you want to map to that ASA interface.

You cannot change the mapping of the management interfaces. If a Firewall Threat Defense interface has already been assigned to an ASA interface, you cannot choose that interface from the drop-down list. All assigned interfaces are greyed out and unavailable.

You do not need to map subinterfaces. The Secure Firewall migration tool maps subinterfaces on the Firewall Threat Defense device for all subinterfaces in the ASA configuration.

Step 2 When you have mapped each ASA interface to a Firewall Threat Defense interface, click **Next**.

What to do next

Map the ASA interfaces to the appropriate Firewall Threat Defense interface objects, security zones, and interface groups. For more information, see Map Interfaces to Security Zones and Interface Groups.

Map ASA Interfaces to Security Zones, Interface Groups, and VRFs

Note If your ASA configuration does not include Access Lists and NAT rules or if you choose not to migrate these policies, you can skip this step and proceed to Optimize, Review and Validate the Configuration, on page 24.

To ensure that the ASA configuration is migrated correctly, map the ASA interfaces to the appropriate Firewall Threat Defense interface objects, security zones and interface groups, and VRFs. In an ASA configuration, access control policies and NAT policies use interface names (nameif). In Firewall Management Center, those policies use interface objects. In addition, Firewall Management Center policies group interface objects into the following:

- Security zones—An interface can belong to only one security zone.
- Interface groups—An interface can belong to multiple interface groups.
- VRFs—An interface can belong to only one VRF configuration.

The Secure Firewall migration tool allows one-to-one mapping of interfaces with security zones, interface groups, and VRFs; when a security zone or interface group is mapped to an interface, it is not available for mapping to other interfaces although the Firewall Management Center allows it. For more information about security zones and interface groups in Firewall Management Center, see Security Zones and Interface Groups in *Cisco Secure Firewall Management Center Device Configuration Guide*.

Procedure

Step 1 On the **Map Security Zones, Interface Groups and VRFs** screen, review the available interfaces, security zones, interface groups, and VRF configurations.

Step 2 To map interfaces to security zones and interface groups that exist in Firewall Management Center, or that is available in ASA configuration files as Security Zone type objects and is available in the drop-down list, do the following:

a) In the **Security Zones** column, choose the security zone for the interface.
b) In the **Interface Groups** column, choose the interface group for the interface.
c) In the **VRF** column, choose the VRF configurations for the interface.

Note
If you are setting up a threat defense HA pair as part of the migration, you can add or autocreate security zones and interface groups for both primary and secondary peers. Note that the security zones and interface groups of the secondary peer are same as those of the primary peer.

Step 3 You can manually map or auto-create the security zones, interface groups, and VRFs.

Step 4 To map the security zones, interface groups, and VRFs manually, perform the following:

a) Click **Add SZ, IG & VRF**.

b) In the **Add SZ, IG & VRF** dialog box, click the edit icon, enter the name you want to give to the VRF, and click the green check mark. You can also edit the VRF name by clicking on the edit icon again.

Note
If you are performing a merged-configuration migration and one of your contexts had VPN configuration, it does not get displayed here to be mapped to an interface, because it gets migrated to the global router directly.

c) Enter the security zone name in the **Security Zone** column. The maximum characters allowed is 48. Similarly, you can add an interface group.
d) Click **Close**.

To map the security zones and interface groups through auto-creation, perform the following:

a) Click **Auto-Create**.
b) In the **Auto-Create** dialog box, check one or both of **Interface Groups** and **Zone Mapping**.
c) Click **Auto-Create**.

The Secure Firewall migration tool gives these security zones the same name as the ASA interface, such as **outside** or **inside**, and displays an "(A)" after the name to indicate that it was created by the Secure Firewall migration tool. The interface groups have an `_ig` suffix added, such as **outside_ig** or **inside_ig**. In addition, the security zones and interface groups have the same mode as the ASA interface. For example, if the ASA logical interface is in L3 mode, the security zone and interface group that is created for the interface is also in L3 mode.

Step 5 When you have mapped all interfaces to the appropriate security zones, interface groups, and VRFs, click **Next**.

Optimize, Review and Validate the Configuration

Before you push the migrated ASA configuration to Firewall Management Center, optimize and review the configuration carefully and validate that it is correct and matches how you want to configure the Firewall Threat Defense device. A flashing tab indicates that you must take the next course of action.



Note If you close the Secure Firewall migration tool at the **Optimize, Review and Validate Configuration** screen, it saves your progress and allows you to resume the migration later. If you close the Secure Firewall migration tool before this screen, your progress is not saved. If there is a failure after parsing, relaunching the Secure Firewall migration tool resumes from the **Interface Mapping** screen.

Here, the Secure Firewall migration tool fetches the Intrusion Prevention System (IPS) policies and file policies, which are already present on the Firewall Management Center and allows you to associate those to the access control rules you are migrating.

A file policy is a set of configurations that the system uses to perform Advanced Malware Protection for networks and file control, as part of your overall access control configuration. This association ensures that before the system passes a file in traffic that matches the conditions of the access control rule, it first inspects the file.

Similarly, you can use an IPS policy as the system's last line of defense before traffic is allowed to proceed to its destination. Intrusion policies govern how the system inspects traffic for security violations and, in inline

deployments, can block or alter malicious traffic. Whenever the system uses an intrusion policy to evaluate traffic, it uses an associated variable set. Most variables in a set represent values commonly used in intrusion rules to identify source and destination IP addresses and ports. You can also use variables in intrusion policies to represent IP addresses in rule suppression and dynamic rule states.

To search for specific configuration items on a tab, enter the item name in the field at the top of the column. The table rows are filtered to display only items that match the search term.

The source ASA device may be managed by CSM or ASDM. When you enter more than one item (object or inline values) in the source or destination address, or source or destination service, CSM or ASDM automatically creates an object group. The naming conventions for these object groups that are used by CSM and ASDM are CSM_INLINE and DM_INLINE respectively.

When you opt to clear the inline grouping CSM or ASDM managed configurations, the predefined objects are replaced with the actual object or member name. If you do not clear the CSM or ASDM managed configurations, the predefined object names will be retained for migration.

For example, 10.21.44.189 and 10.21.44.190 are members of an object group and are renamed with the predefined names such as object-group DM_INLINE_NETWORK_1 and object-group DM_INLINE_NETWORK_2.



Note By default, the Inline Grouping option is enabled.

If you close the Secure Firewall migration tool at the **Optimize, Review and Validate Configuration** screen, it saves your progress and allows you to resume the migration later. If you close the before this screen, your progress is not saved. If there is a failure after parsing, relaunching the Secure Firewall migration tool resumes from the **Interface Mapping** screen.

Secure Firewall Migration Tool ACL Optimization Overview

The Secure Firewall migration tool provides support to identify and segregate ACLs that can be optimized (disabled or deleted) from the firewall rule base without impacting the network functionality.

The ACL optimization supports the following ACL types:

- Redundant ACL—When two ACLs have the same set of configurations and rules, then removing the non-base ACL will not impact the network. For example, if any two rule allows FTP and IP traffic on the same network with no rules that are defined for denying access, the first rule can be deleted.
- Shadow ACL—The first ACL completely shadows the configurations of the second ACL. If two rules have similar traffic, the second rule is not applied to any traffic as it appears later in the access list. If the two rules specify different actions for traffic, you can either move the shadowed rule or edit any one of the rules to implement the required policy. For example, the base rule may deny the IP traffic, and the shadowed rule may allow FTP traffic for a given source or destination.
- Disable ACL—The ACL that has been explicitly turned off in the firewall's configuration. The rules exist in the configuration file, but the Secure Firewall Migration Tool ignores them when processing traffic.

The Secure Firewall migration tool uses the following parameters while comparing rules for ACL optimization:



Note Optimization is available for the ASA only for ACP rule action.

- The source ACLs are expanded into the corresponding ACEs (inline values), and then compared for the following parameters:
  - Source and Destination Zones
  - Source and Destination Network
  - Source and Destination Port

Click **Download Report** to review the ACL name and the corresponding redundant, shadowed and disabled ACLs tabulated in an Excel file. Use the **Detailed ACL Information** sheet to view more ACL information.

Object Optimization

The following objects are considered for object optimization during the migration process:

- Unreferenced objects—You can choose not to migrate unreferenced objects at the beginning of the migration.
- Duplicate objects—If an object already exists on Firewall Management Center, instead of creating a duplicate object, the policy is reused.

Procedure

Step 1 (Optional) On the **Optimize, Review and Validate Configuration** screen, click **Optimize ACL** in **Access Control** > **ACP** to run the optimization code, and perform the following:

a) Click **Proceed** to proceed with the ACL optimization, where the identified Redundant ACLs, Shadow ACLs and Disable ACLs rules for migration are displayed.

The time taken for analyzing the ACL optimization depends on the source configuration file size. The estimation time is displayed.

A report with the summary of total ACL rules considered for optimization is displayed. For more information on optimization report and its components, see Reporting for ACL Optimization, on page 38.

The **Redundant ACLs**, **Shadow ACLs** and **Disable ACLs** tabs appears only if there is data in the ACL optimization report.

The ACLs are displayed in both Redundant, Shadow and Disable ACLs under different base rules.

Note
An ACL entry that is displayed under the Redundant, shadow or disable ACL, the same is not considered as the base ACL.

b) To download the identified ACL optimization rules, click **Download Report**.

c) Select rules and choose **Actions** > **Migrate as disabled** or **Do not migrate** and apply one of the actions.

d) Click **Save**.
The migration operation changes from **Do not migrate** to **disabled** or vice-versa.

You can perform bulk selection of rules, using the following options

- Migrate—To migrate with default state.
- Do not Migrate—To ignore the migration of ACLs.

- Migrate as disabled—To migrate ACLs with ***State*** field set to ***Disable***.
- Migrate as enabled—To migrate ACLs will with ***State*** field set to ***Enable***.

Step 2 On the **Optimize, Review and Validate Configuration** screen, click **Access Control Rules** and do the following:

a) For each entry in the table, review the mappings and verify that they are correct.

A migrated Access Policy Rule uses the ACL name as prefix and appends the ACL rule number to it to make it easier to map back to the ASA configuration file. For example, if an ASA ACL is named "inside_access," then the first rule (or ACE) line in the ACL will be named as "inside_access_#1." If a rule must be expanded because of TCP or UDP combinations, an extended service object, or some other reason, the Secure Firewall migration tool adds a numbered suffix to the name. For example, if the allow rule is expanded into two rules for migration, they are named "inside_access _#1-1" and " inside_access_#1-2".

For any rule that includes an unsupported object, the Secure Firewall migration tool appends an "_UNSUPPORTED" suffix to the name.

b) If you do not want to migrate one or more access control list policies, choose the rows by checking the box against the policy, choose **Actions** > **Do not migrate** and then click **Save**.

All rules that you choose not to migrate are grayed out in the table.

c) To edit an access control list policy, check the check box adjacent to the corresponding policy, and choose **Actions** > **Edit**.

d) In the **Edit Rule** dialog box, update the existing data or add new data.

To add an object to source or destination:

1. Check the check box adjacent to the object in the left pane.
2. Click the **Add Source** or **Add Destination** button under the **Selected Sources** or **Selected Destination and Applications** column to move the object to the respective location.

You can also delete the existing object from the source or destination by clicking the delete icon.

Note
Rules that are not applicable are grayed out in the table.

e) If you want to apply a Firewall Management Center file policy to one or more access control policies, check the box for the appropriate rows, choose **Actions** > **File Policy**.

In the **File Policy** dialog, select the appropriate file policy and apply it to the selected access control policies and click **Save**.

f) If you want to apply a Firewall Management Center IPS policy to one or more access control policies, check the box for the appropriate rows, choose **Actions** > **IPS Policy**.

In the **IPS Policy** dialog, select the appropriate IPS policy and its corresponding variable set and apply it to the selected access control policies and click **Save**.

g) If you want to change the logging options for an access control rule which has logging enabled, check the box for the appropriate row and choose **Actions** > **Log**.

In the **Log** dialog, you can enable logging events either at the beginning or end of a connection or both. If you enable logging, you must opt to send the connection events either to the **Event Viewer** or to the

Syslog or both. When you opt to send connection events to a syslog server, you can choose the syslog policies that are already configured on the Firewall Management Center from the **Syslog** drop-down menu.

h) If you want to change the actions for the migrated access control rules in the Access Control table, check the box for the appropriate row and choose **Actions** > **Rule Action**.

In the **Rule Action** dialog from the **Actions** drop-down, you can either choose **ACP** or **Prefilter** tabs:

- ACP—Every access control rule has an action that determines how the system handles and logs matching traffic. You can either perform an allow, trust, monitor, block, or block with reset action on an access control rule.
- Prefilter—A rule's action determines how the system handles and logs matching traffic. You can either perform a fastpath and block.

Tip
The IPS and file policies that are attached to an access control rule are automatically removed for all rule actions except for the **Allow** option.

ACL Rule Category—The Secure Firewall migration tool preserves the Rule sections in the CSM managed ASA configuration and migrates them as ACL categories on Firewall Management Center.

Policy capacity and limit warning—The Secure Firewall migration tool compares the total ACE count for the migrated rules with the supported ACE limit on the target platform.

Based on the comparison result, the Secure Firewall migration tool displays a visible indicator and a warning message if the total count of migrated ACE exceeds threshold or if it approaches the threshold of the supported limit of target device.

You can optimize or decide not to migrate if the rules exceed the ACE Count column. You can also complete the migration and use this information to optimize the rules after a push on the Firewall Management Center before deployment.

Note
The Secure Firewall migration tool does not block any migration despite the warning.

You can filter the ACE counts in the ascending, descending, equal, greater than, and lesser than filtering order sequence.

To clear the existing filter criteria, and to load a new search, click **Clear Filter**.

Note
The order that you sort the ACL based on ACE is for viewing only. The ACLs are pushed based on the chronological order in which they occur.

Step 3 To edit the source and destination zones of NAT rules, click **NAT** and do the following:

a) Select the NAT rule you want to edit.
b) From the **Actions** drop-down list, choose **Edit**.
c) On the **Security Zone Update** dialog box, select the **Source Zone** and **Destination Zone** from the drop-down list, and click **Update**.

You can also do a bulk update by selecting multiple NAT rules.

Step 4 Click the following tabs and review the configuration items:

- **Access Control**

- **Objects (Access List Objects, Network Objects, Port Objects, VPN Objects, Security Group Tag Objects, and Dynamic-Route Objects)**
- **NAT**
- **Interfaces**
- **Routes**
- **DHCP**
- **SNMP**
- **Site-to-Site VPN Tunnels**
- **Remote Access VPN**
- **WebVPN**

Note
For site-to-site and remote access VPN configurations, VPN filter configurations and extended access list objects pertaining to them are migrated and can be reviewed under the respective tabs.

Access List objects displays Standard and Extended ACL used in BGP, EIGRP, and RA VPN.

If you do not want to migrate one or more NAT rules or route interfaces, check the box for the appropriate rows, choose **Actions** > **Do not migrate**, and then click **Save**.

All rules that you choose not to migrate are grayed out in the table.

Step 5 (Optional) On the **Network Objects** and the **Port Objects** tabs, review all the network objects, network groups, port objects, port groups, and their values. To rename an object or object group, select the object and choose **Actions** > **Rename**.

- Click **Optimize Objects and Groups** to optimize your list of objects before migrating them to the target management center. The migration tool identifies objects and groups that have the same value and prompts you to choose which to retain.
- Click  to move objects from **Conflict Detected** column to **Objects/Groups Retained** column and click  to move them back. Note that the ones that are referenced in most configurations are displayed in bolded text.
- Click **Auto Select** to automatically select all the objects and groups with most number of referenes. However, you can still manually override the autoselection and move objects between columns because manual selection takes higher priority.
- Click **Optimize**. The migration tool performs the optimization and displays an optimization summary with optimization data including retained and duplicate objects. For a detailed version of the optimization report, refer to the postmigration report.
- Click **Proceed** and **Validate**.

  Note
  The objects and groups which are not chosen to be retained are not migrated and are replaced with the retained objects in the configurations they were used, such as in ACL and NAT configurations. This ensures the list of objects being migrated is fully optimized and there are no duplicate objects migrated.

Step 6 (Optional) While reviewing your configuration, you can rename one or more network, port, or VPN objects in the **Network Objects** tab or **Port Objects** tab, or the **VPN Objects** by choosing **Actions** > **Rename**.

Access rules and NAT policies that reference the renamed objects are also updated with new object names.

Step 7 On the **Security Group Tag Objects** tab, review all the values. To rename an object or object group, select the object and choose **Actions** > **Rename**.

SGT objects support multi-context configuration. The tag value must range from 0 to 65535.

Note
To migrate the SGT objects configuration, ensure that the management center and threat defense version are 7.0 or later.

Step 8 In the **Dynamic-Route Objects** section, all the supported objects that are migrated are displayed:

- Policy-List
- Prefix-List
- Route-Map
- Community List
- AS-Path
- Access-List

Step 9 In the **Routes** section, the following routes are displayed:

- Static—Displays all IPv4 and IPv6 static routes.
- BGP—Displays all the BGP routes.
- EIGRP—Displays all the EIGRP routes.

  For EIGRP, authentication keys are obtained if the `more system:running` configuration is uploaded and the keys are unencrypted. If the key is encrypted in the source configuration, you can manually provide the key under the interface section in EIGRP. You can select the authentication type (encrypted, unencrypted, auth, or none) and provide the key accordingly.
- ECMP—Displays all the ECMP zones and associated VRFs.

  Note
  The only action which can be performed in this section is renaming the ECMP zones.
- PBR—Displays all the PBR routes.

Step 10 Under the **DHCP** tab, you can review and validate the following tabs:

- **DHCP Server**: Review all the IP address pools and the corresponding interfaces.
- **DHCP Relay**: Review the DHCP Relay server IP addresses, interfaces to which the DHCP server is associated with, and the Relay-enabled interfaces.
- **DDNS**: Under **DDNS Update Methods** tab, review the DDNS method names, types, the DDNS update intervals, and which records are configured to be updated by the DHCP Server (A or PTR records).

Note

In the **Select Features** page, you can select either DHCP Server only or Relay and DDNS together. Therefore, if you see configurations in the **DHCP Server** tab in the **Optimize, Review and Validate Configuration** page, the **DHCP Relay** and **DDNS** tabs are empty.

Step 11 Under the **SNMP** tab, you can review, validate, and work with the following tabs:

Based on whether you have SNMPV1/V2 or SNMPV3 configurations on your ASA device, the configurations gets displayed in **SNMPV1/V2** tab or **SNMPV3** tab.

SNMPV1/V2:

- **Host Server Name**: The hostname of the SNMP host
- **IP Address**: The IP address of the SNMP host
- **Community String**: The SNMP community string that must be provided manually. Select the host and navigate **Actions** > **Update Community String** to provide the community string. This must be the same as the community or username that is configured for the SNMP service.
- **Validation State**: The host server's validation state that will be created in the target management center

SNMPV3:

- **User Name**: The username for SNMP host
- **Authentication Password**: Click **Actions** to provide the authentication password for the user
- **Encryption Password**: Click **Actions** to provide the privacy password for the user
- **Validation State**: The user's validation state that will be created in the target management center

Step 12 In the **Site-to-Site VPN Tunnels** section, all the supported VPN tunnels that are migrated from ASA to Firewall Management Center are displayed, and includes the following lists.

- Both crypto map and route-based (VTI) based VPN tunnels.
- VPN tunnels of authentication type preshared key and certificate-based authentication.

  You must enter the values for preshared key and the PKI object for each VPN topology for validation for all the rows. Failure to update will be marked as incomplete and the Secure Firewall migration tool will not allow to proceed to validation.

  Note
  For a live connect ASA, the preshared keys are retrieved automatically by the migration tool; for a manually uploaded configuration, use the **more system: running-config** to retrieve the hidden keys and provide them manually in the **preshared Key** column.

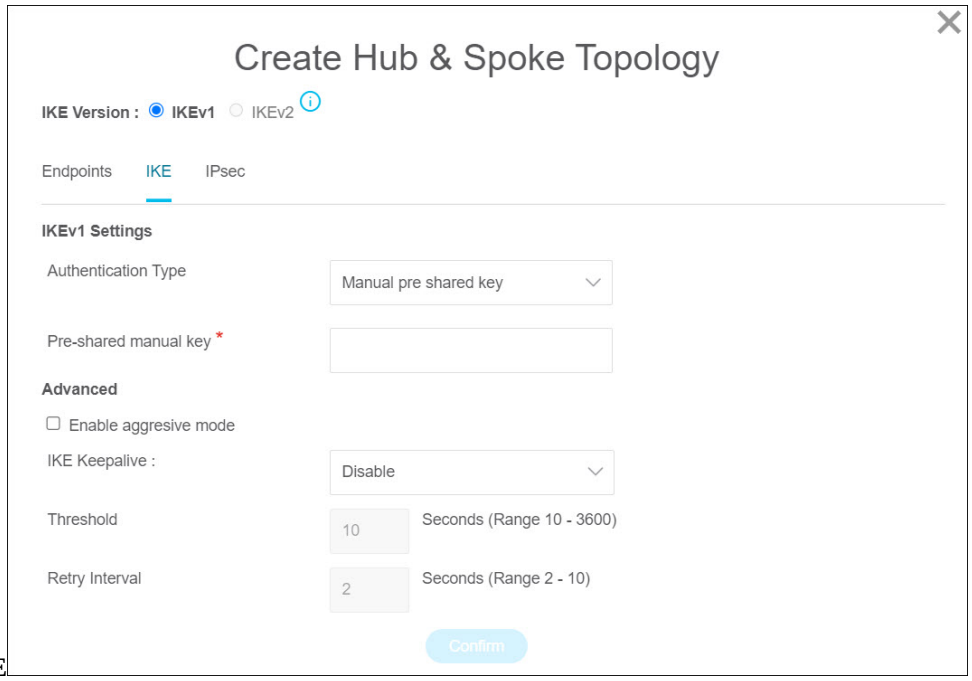
Note
Trustpoint or PKI object migration from ASA to Firewall Management Center is part of the pre-migration activity and is required for successful migration of certificate-based VPN migration.

Step 13 (Optional) Click **Add Hub & Spoke Topology** to configure a hub and spoke VPN topology using the target threat defense as the hub node and selecting one or more ASA peer interfaces as the spoke nodes.

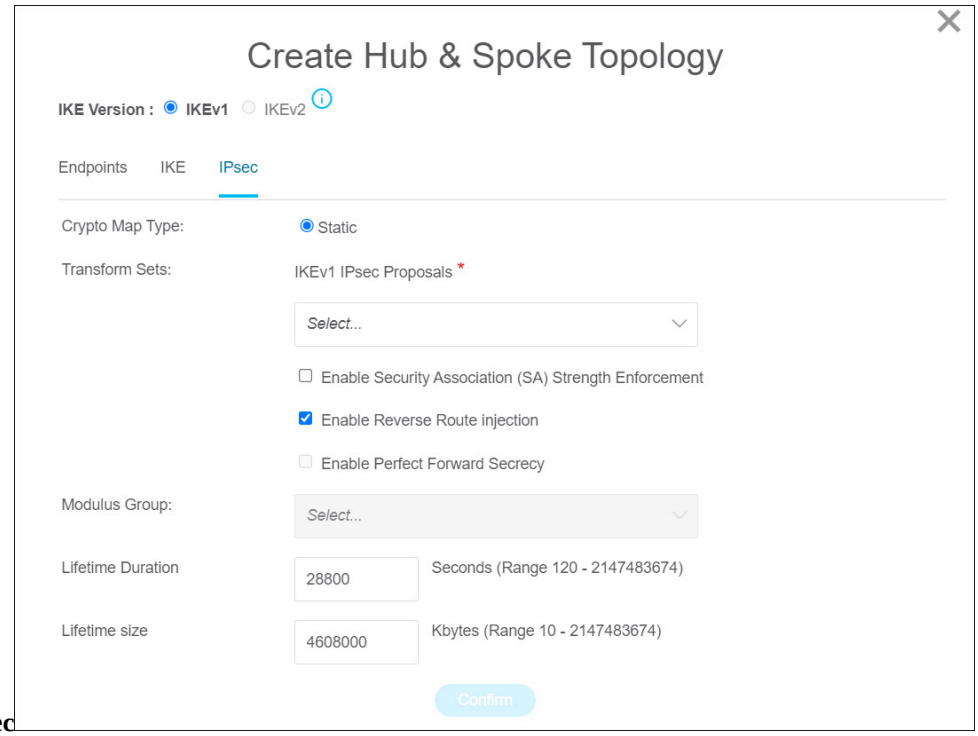
Note
You can select spoke nodes of the same IKE versions only. For instance, you cannot choose one spoke node of IKEv1 and another spoke node of IKEv2 IKE version.

Based on the IKE version of the selected spoke nodes, configure or verify the following:

- **IKE Version**—Verify that the IKE version of the selected nodes is checked.
- **Endpoints**—Verify that the target threat defense device is by default selected as the hub node, the spoke nodes you selected from the list, and their VPN interfaces and protected source and remote networks.



- **IKE**
  - **IKEv1 Settings** or **IKEv2 Settings**
    - **Authentication Type**—The two supported authentication methods are preshared key and certificate. See Deciding Which Authentication Method to Use in the *Cisco Secure Firewall Management Center Device Configuration Guide*.
  - **Advanced**
    - **Enable Aggressive Mode**—Select this negotiation method for exchanging key information if the IP address is not known and DNS resolution might not be available on the devices.
    - **IKE Keepalive**—Enable or disable this for the keepalive monitoring.
    - **Threshold**—Specify the IKE keep alive confidence interval. This interval is the number of seconds allowing a peer to idle before beginning keepalive monitoring. The minimum and default interval is 10 seconds; the maximum interval is 3600 seconds.
    - **Retry Interval**—Specify number of seconds to wait before the IKE keep alive retries. The default is 2 seconds, the maximum is 10 seconds.



- **IPsec**
  - **Crypto Map Type**—A crypto map combines all the components required to set up IPsec security associations (SA). When two peers try to establish an SA, they must each have at least one compatible crypto map entry. The IPsec security negotiation uses the proposals defined in the crypto map entry to protect the data flows specified by that crypto map's IPsec rules. Choose static or dynamic for this deployment's crypto map.
  - **Transform Sets**—Select the IPsec proposal that you want to use for the IKE version nodes you selected.
    - **Enable Security Association (SA) Strength Enforcement**—Check this checkbox to ensure that the encryption algorithm used by the child IPsec SA is not stronger (in terms of the number of bits in the key) than the parent IKE SA.
    - **Enable Reverse Route Injection**—Check this checkbox to enable reverse route injection which automatically inserts static routes into routing for networks and hosts, which are protected by a remote tunnel group list.
    - **Enable Perfect Forward Secrecy**—Check this checkbox to generate and use a unique session key for each encrypted exchange. The unique session key protects the exchange from subsequent decryption, even if the entire exchange was recorded and the attacker has obtained the preshared or private keys used by the endpoint devices.
  - **Modulus Group**—Choose the Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. See Deciding Which Diffie-Hellman Modulus Group to Use in the *Cisco Secure Firewall Management Center Device Configuration Guide* for more information.
  - **Lifetime Duration**—The number of seconds you want a security association to exist before expiring. The default is 28,800 seconds.

- **Lifetime Size**—The volume of traffic (in kilobytes) that can pass between IPsec peers using a given security association before it expires. The default is 4,608,000 kilobytes. Infinite data is not allowed.

If you have an existing site-to-site hub and spoke VPN configuration on one of the devices in the management center, you can choose to add your target threat defense device as one of the spokes to it. Choose **Add to existing Hub & Spoke Topology**, select the topology to which you want to add your device, and select **Interface** and **Protected Networks**.

Step 14 For configurations containing several site-to-site VPN tunnel configurations, to update the preshared keys for multiple entries at once, follow the steps below:

- Select the site-to-site VPN configuration entries for which you want to update the preshared keys.
- Click download () to export the table to an editable Excel sheet.
- Enter the preshared keys in the respective columns against each VPN configuration and save the file. For VPN configurations containing both IKEv1 and IKEv2 versions of IKE, ensure you enter two values in the column separated by a comma.
- Click upload (). The migration tool reads the entries in the Excel and automatically adds them to the corresponding preshared key columns of the VPN configurations.

  Note
  To update a preshared key that was missed to be updated as part of the bulk update, use the default method of selecting the entry and choosing **Actions** > **Update Pre-Shared Key** or export the Excel, update the key, and import it.

If the target threat defense device already has a site-to-site VPN topology configured, the migration tool detects it and prompts you to choose if you want to delete it. If you choose to delete it, the migration tool deletes it for you, without you having to log in to the management center to manually delete it. If you choose **No**, you need to manually delete any existing VPN configurations on the target threat defense device to continue the migration.

Step 15 In the **Remote Access VPN** section, all objects corresponding to remote access VPN are migrated from ASA to the management center, and are displayed:

- **Anyconnect Packages**: Retreive the AnyConnect packages, Hostscan Files (Dap.xml, Data.xml, Hostscan Package), External Browser package, and AnyConnect profiles should be retrieved from the source ASA device for migration.

  As part of the premigration activity, upload all the AnyConnect packages to the management center. You can upload AnyConnect profiles either directly to the management center or from the Secure Firewall migration tool.

  Select pre-existing AnyConnect, Hostscan, or external browser packages retrieved from the management center. You must select atleast one AnyConnect package. You must also select the Hostscan, dap.xml, data.xml, or external browser, if they are available in the source configuration. AnyConnect profiles are optional.

Ensure that the correct Dap.xml file is retrieved from the source firewall. Validations are performed on the dap.xml file that are available in the configuration file. You must select all the files that are required for validation and upload them. Failure to update marks as incomplete and the Secure Firewall migration tool does not proceed with validation.

- **AAA**—Authentication servers of Radius, LDAP, AD, LDAP, SAML, and Local Realm type are displayed. Update the keys for all AAA servers. From Secure Firewall migration tool 3.0, the preshared keys are retrieved automatically for a Live Connect ASA. You can also upload the source configuration with the hidden keys using **more system: running-config** file. To retrieve the AAA authentication key in clear text format, follow the below steps:

  Note
  These steps should be performed outside the Secure Firewall migration tool.

  a. Connect to the ASA through the SSH console.

  b. Enter the *more system:running-config* command.

  c. Go to the **aaa-server and local user** section to find all the AAA config and the respective key values in clear text format.

  ```
  ciscoASA#more system:running-config

  !

  aaa-server Test-RADIUS (inside) host 2.2.2.2

   key <key in clear text>     <-----The radius key is now displayed in clear text
  format.

  aaa-server Test-LDAP (inside) host 3.3.3.3

  ldap-login-password <Password in clear text> <-----TheLDAP/AD/LDAPS password is now
  displayed in clear text format.

  username Test_User password <Password in clear text> <-----The Local user
          password is shown in clear text.
  ```

  Note
  If the password for the local user is encrypted, you can internally check for the password or configure a new one on the Secure Firewall migration tool.

- LDAPS requires domain on management center. You must update domain for encryption type LDAPS.
- Unique AD Primary Domain is required on Firewall Management Center for an AD server. If a unique domain is identified, it will be displayed on the Secure Firewall migration tool. If conflict is found, you must enter a unique AD primary domain to push the objects successfully.

  For AAA server with encryption set to LDAPS, ASA supports IP and hostname or domain but the management center supports only hostname or domain. If ASA config contains hostname or domain, it is retrieved and displayed. If ASA config contains the IP address for LDAPS, enter a domain in the **AAA** section under **Remote Access VPN**. You must enter the domain that can be resolved to the IP address of the AAA server.

  For AAA server with type AD (server-type is Microsoft in ASA config), **AD Primary Domain** is a mandatory field to be configured on a management center. This field is not configured separately on ASA and extracted from the LDAP-base-dn config on ASA.

  ```
  If the ldap-base-dn is: ou=Test-Ou,dc=gcevpn,dc=com
  ```

The **AD Primary Domain** is the field starting with dc, with dc=gcevpn, and dc=com that forms the primary domain. The AD primary domain would be gcevpn.com.

LDAP-base-dn example file:

```
cn=asa,OU=ServiceAccounts,OU=abc,dc=abc,dc=com:
```

Here, dc=abc, and dc=com will be combined as abc.com to form the AD Primary Domain.

```
cn=admin, cn=users, dc=fwsecurity, dc=cisco, dc=com:
```

AD Primary Domain is fwsecurity.cisco.com.

AD Primary Domain is retrieved automatically and displayed on the Secure Firewall migration tool.

Note
AD Primary Domain value needs to be unique for each Realm object. In case a conflict is detected or if the Firewall Migration Tool is unable to find the value in the ASA config, you are requested to enter an AD Primary Domain for the specific server. Enter the AD Primary Domain to validate the configuration.

- **Address Pool**—Review all the IPv4 and IPv6 pools that are displayed here.
- **Group-Policy**—Select or remove the user profile, management profile, and client module profile from this area, which displays group policies with client profiles, management profiles, client modules, and group policies without profiles. If a profile was added in the AnyConnect file area, it is displayed as preselected. You can select or remove the user profile, management profile, and client module profile.

  The custom attribute related to the specific group-policy is displayed in the **AnyConnect Custom Attribute** tab. You can select the custom attribute and validate it.
- **Connection Profile**—Review all connection profiles/tunnel groups that are displayed here.
- **Trustpoints**—Trustpoint or PKI object migration from the ASA to the management center is part of the premigration activity and is required for successful migration of remote access VPN. Map the trustpoint for Global SSL, IKEv2, and interfaces in the **Remote Access Interface** section to proceed with the migration. Global SSL and IKEv2 Trustpoint are mandatory if the LDAPS protocol is enabled.

  If a Security Assertion Markup Language (SAML) object exists, the trustpoint for the SAML IDP and SP can be mapped in the SAML section. SP certificate upload is optional. Trustpoints can be overridden for a specific tunnel group. If the overriden SAML trustpoint configuration is available in the source ASA, it can be selected under **Override SAML**.

  For information on exporting PKI certificates from ASA, see Export PKI Certificate from ASA and Import into Management Center.
- **Certificate Maps**—Certificate maps are displayed here.
- **VPN Load Balancing**—VPN load balancing Configurations are displayed here.

  For VPN load balancing, the Secure Firewall migration tool will fetch the encryption key if **more system: running-config** configuration is uploaded. You can manually update the encryption key using **Actions** > **Update Keys**.

- Under the **WebVPN** tab, the migration tool lists all the WebVPN policies that it detected in the source ASA device. WebVPN policies include any ASA group policy with SSL clientless VPN tunnel protocol configurations and tunnel groups that are referenced to policies using SAML authentication. Ensure you review the tabs associated with your WebVPN configurations before proceeding:

- **Zero Trust Application Policy**: Provide a different value by selecting the policy and navigating **Actions** > **Update Zero Trust Policy fields**
  - **Policy Name**: The policy's name that will get migrated.
  - **Domain Name**: User-defined domain name that must be manually provided. This domain name resolves to the threat defense interface from where the private applications are accessed. The domain name is used to generate the ACS URL for all private applications in an Application Group.
  - **Identity Certificate**: The identity certificate that you imported into the target management center before migration. This must be done as part of the premigration tasks.
  - **Security Zones**: The corresponding security zones associated with the policy.
  - **Global Port Pool**: The port range for the policy. A unique port from this pool is assigned to each application.
- **Application Group**
  - **Application Group**: Review the **Application Group Settings** including application group name, re-authentication interval, and security zones.

    Under the **SAML IdP Metadata** tab, you can choose to manually configure application group name, entity ID for the service provider, single sign-on URL for the SAML identity provider (IdP), and IdP certificate or choose **Configure Later**

    The **Applications** tab lets you review or configure application-specific settings such as application name, external URL, application URL, application certificate, and application group.
- **Standalone Applications**: Review or configure **Application Settings** for standalone applications, including application name, external URL, application URL, application certificate, re-authentication interval, and security zones. The **SAML IdP Metadata** tab lets you manually configure IdP metadata settings for standalone applications or configure later. The tabs include application group name, entity ID, single sign-on URL, and IdP certificate.

To update the fields, click **Actions** and choose to update the various fields.

After the migration is successful, ensure you do a thorough review of the configurations that you migrated to the management center and when ready, deploy it to your threat defense device.

Step 16 (Optional) To download the details for each configuration item in the grid, click **Download**.

Step 17 After you have completed your review, click **Validate**. Note that the mandatory fields that need your attention keeps flickering until you enter values in them. The **Validate** button gets enabled only after all the mandatory fields are filled.

During validation, the Secure Firewall migration tool connects to Firewall Management Center, reviews the existing objects, and compares those objects to the list of objects to be migrated. If an object already exists in Firewall Management Center, the Secure Firewall migration tool does the following:

- If the object has the same name and configuration, the Secure Firewall migration tool reuses the existing object and does not create a new object in Firewall Management Center.
- If the object has the same name but a different configuration, the Secure Firewall migration tool reports an object conflict.

You can view the validation progress in the console.

Step 18 When the validation is complete, if the **Validation Status** dialog box shows one or more object conflicts, do the following:

a) Click **Resolve Conflicts**.

The Secure Firewall migration tool displays a warning icon on either or both of the **Network Objects** or **Port Objects** tab, depending upon where the object conflicts were reported.

b) Click the tab and review the objects.
c) Check the entry for each object that has a conflict and choose **Actions** > **Resolve Conflicts**.
d) In the **Resolve Conflicts** window, complete the recommended action.

For example, you might be prompted to add a suffix to the object name to avoid a conflict with the existing Firewall Management Center object. You can accept the default suffix or replace it with one of your own.

e) Click **Resolve**.
f) When you have resolved all object conflicts on a tab, click **Save**.
g) Click **Validate** to revalidate the configuration and confirm that you have resolved all object conflicts.

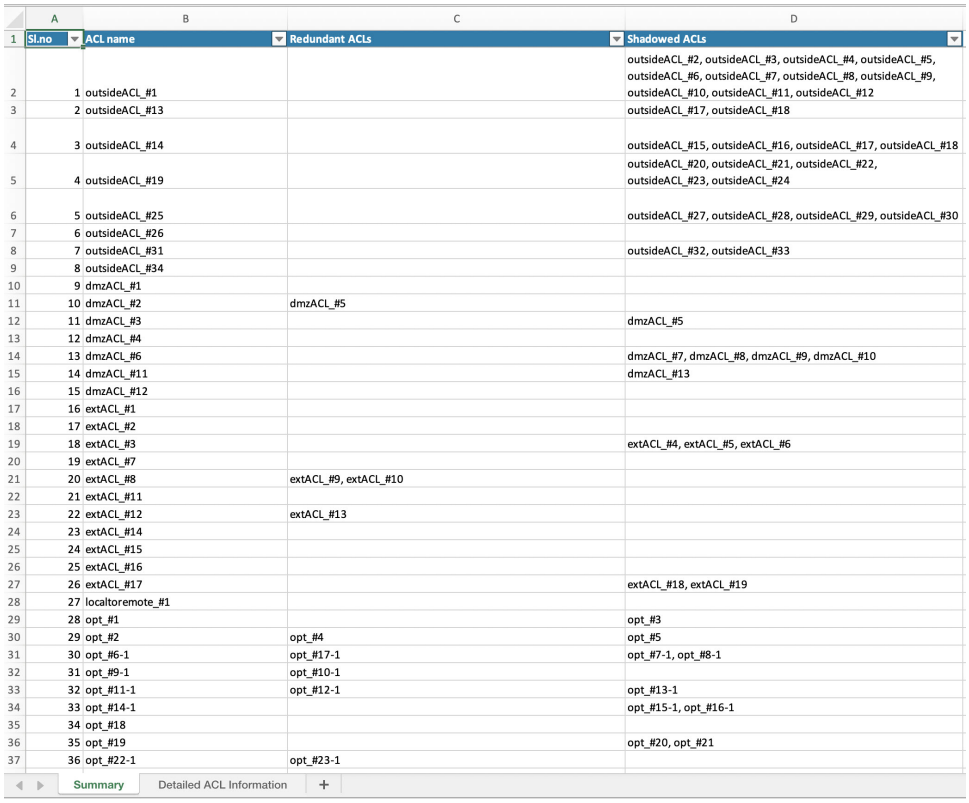
Step 19 The **Optimize Your Configuration** dialog box displays a check mark next to each optimized attribute and identifies attributes that need optimization. Click **Proceed** to start the optimization. You can skip optimization, but it is recommended to optimize the attributes before proceeding with migration.

Step 20 When the validation is complete and the **Validation Status** dialog box displays the message **Successfully Validated**, continue with Push the Migrated Configuration to Firewall Management Center, on page 39.

Reporting for ACL Optimization

The ACL optimization report displays the following information:

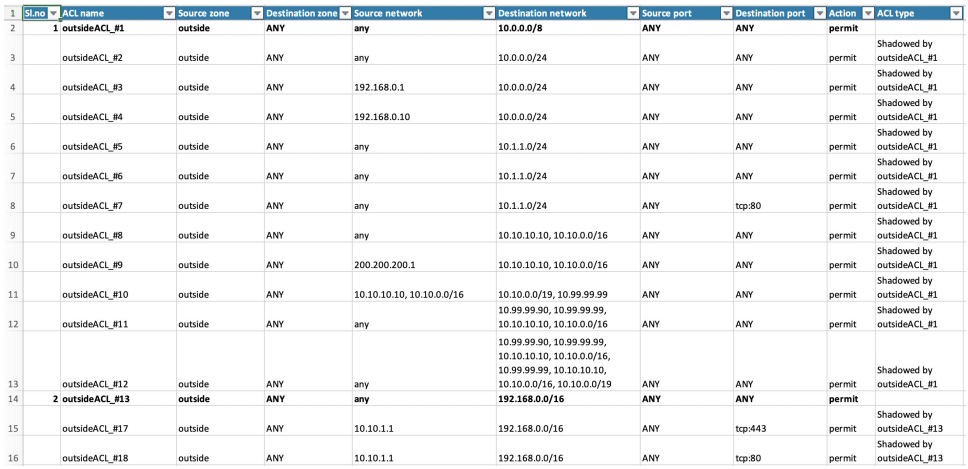
- Summary Sheet—Displays the summary of the ACL optimization.



Sl.no	ACL name	Redundant ACLs	Shadowed ACLs
1	outsideACL_#1		outsideACL_#2, outsideACL_#3, outsideACL_#4, outsideACL_#5, outsideACL_#6, outsideACL_#7, outsideACL_#8, outsideACL_#9, outsideACL_#10, outsideACL_#11, outsideACL_#12
2	outsideACL_#13		outsideACL_#17, outsideACL_#18
3	outsideACL_#14		outsideACL_#15, outsideACL_#16, outsideACL_#17, outsideACL_#18
4	outsideACL_#19		outsideACL_#20, outsideACL_#21, outsideACL_#22, outsideACL_#23, outsideACL_#24
5	outsideACL_#25		outsideACL_#27, outsideACL_#28, outsideACL_#29, outsideACL_#30
6	outsideACL_#26		
7	outsideACL_#31		outsideACL_#32, outsideACL_#33
8	outsideACL_#34		
9	dmzACL_#1		
10	dmzACL_#2	dmzACL_#5	
11	dmzACL_#3		dmzACL_#5
12	dmzACL_#4		
13	dmzACL_#6		dmzACL_#7, dmzACL_#8, dmzACL_#9, dmzACL_#10
14	dmzACL_#11		dmzACL_#13
15	dmzACL_#12		
16	extACL_#1		
17	extACL_#2		
18	extACL_#3		extACL_#4, extACL_#5, extACL_#6
19	extACL_#7		
20	extACL_#8	extACL_#9, extACL_#10	
21	extACL_#11		
22	extACL_#12	extACL_#13	
23	extACL_#14		
24	extACL_#15		
25	extACL_#16		
26	extACL_#17		extACL_#18, extACL_#19
27	localtoremote_#1		
28	opt_#1		opt_#3
29	opt_#2	opt_#4	opt_#5
30	opt_#6-1	opt_#17-1	opt_#7-1, opt_#8-1
31	opt_#9-1	opt_#10-1	
32	opt_#11-1	opt_#12-1	opt_#13-1
33	opt_#14-1		opt_#15-1, opt_#16-1
34	opt_#18		
35	opt_#19		opt_#20, opt_#21
36	opt_#22-1	opt_#23-1	

Summary | Detailed ACL Information | +

- Detailed ACL Information—Displays the details of base ACL. Each ACL comes with a ACL type (Shadow or Redundant) tag to identify the base ACL for comparison and its association with the optimization category.



Sl.no	ACL name	Source zone	Destination zone	Source network	Destination network	Source port	Destination port	Action	ACL type
1	**outsideACL_#1**	**outside**	**ANY**	**any**	**10.0.0.0/8**	**ANY**	**ANY**	**permit**	
	outsideACL_#2	outside	ANY	any	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#3	outside	ANY	192.168.0.1	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#4	outside	ANY	192.168.0.10	10.0.0.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#5	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#6	outside	ANY	any	10.1.1.0/24	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#7	outside	ANY	any	10.1.1.0/24	ANY	tcp:80	permit	Shadowed by outsideACL_#1
	outsideACL_#8	outside	ANY	any	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#9	outside	ANY	200.200.200.1	10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#10	outside	ANY	10.10.10.10, 10.10.0.0/16	10.10.0.0/19, 10.99.99.99	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#11	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16	ANY	ANY	permit	Shadowed by outsideACL_#1
	outsideACL_#12	outside	ANY	any	10.99.99.90, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.99.99.99, 10.10.10.10, 10.10.0.0/16, 10.10.0.0/19	ANY	ANY	permit	Shadowed by outsideACL_#1
2	**outsideACL_#13**	**outside**	**ANY**	**any**	**192.168.0.0/16**	**ANY**	**ANY**	**permit**	
	outsideACL_#17	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:443	permit	Shadowed by outsideACL_#13
	outsideACL_#18	outside	ANY	10.10.1.1	192.168.0.0/16	ANY	tcp:80	permit	Shadowed by outsideACL_#13

Push the Migrated Configuration to Firewall Management Center

You cannot push the migrated ASA configuration to Firewall Management Center if you have not successfully validated the configuration and resolved all object conflicts.

This step in the migration process sends the migrated configuration to Firewall Management Center. It does not deploy the configuration to the Firewall Threat Defense device. However, any existing configuration on the Firewall Threat Defense is erased during this step.



Note Do not make any configuration changes or deploy to any device while the Secure Firewall migration tool is sending the migrated configuration to Firewall Management Center.

Procedure

Step 1 In the **Validation Status** dialog box, review the validation summary.

Step 2 Click **Push Configuration** to send the migrated ASA configuration to Firewall Management Center.

The new optimization functionality in the Secure Firewall migration tool allows you to fetch the migration results quickly using the Search filters.

The Secure Firewall migration tool also provides support to optimize CSV download and to apply the actions per page view or on all rules.

Note
When the Secure Firewall Migration tool identifies duplicate object attributes, a dialog box appears and prompts you to correct the duplicate values. You can proceed with migration only after renaming the duplicate attributes.

The Secure Firewall migration tool displays a summary of the progress of the migration. You can view detailed, line-by-line progress of which the components that are being pushed to Firewall Management Center in the console.

Note
If there are configurations with errors when a bulk configuration push is being done, the migration tool throws a warning, prompting you to abort the migration to fix the error manually or to continue the migration leaving out the incorrect configurations. You can choose to view the configurations that have errors and then select **Continue with migration** or **Abort**. If you abort the migration, you can download the troubleshooting bundle and share it with Cisco TAC for analysis.

If you continue the migration, the migration tool will treat the migration as a partial success migration. You can download the postmigration report to view the list of configurations that were not migrated because of the push error.

Step 3 After the migration is complete, click **Download Report** to download and save the post-migration report.

Copy of the **Post-Migration Report** is also saved in the `Resources` folder in the same location as the Secure Firewall migration tool.

Step 4 If your migration failed, review the post-migration report, log file, and unparsed file carefully to understand what caused the failure.

You can also contact the support team for troubleshooting.

Migration Failure Support

If the migration is unsuccessful, contact Support.

a. On the **Complete Migration** screen, click the **Support** button.

The Help support page appears.

b. Check the **Support Bundle** check box and then select the configuration files to download.

Note
The Log and dB files are selected for download by default.

c. Click **Download**.

The support bundle file is downloaded as a .zip to your local path. Extract the Zip folder to view the log files, DB, and the Configuration files.

d. Click **Email us** to email the failure details for the technical team.

You can also attach the downloaded support files to your email.

e. Click **Visit TAC page** to create a TAC case in the Cisco support page.

Note
You can open a TAC case at any time during the migration from the support page.

Review the Post-Migration Report and Complete the Migration

The Post-migration report provides details on ACL count under various categories, ACL optimization, and the overall view of optimization performed on the configuration file. For more information, see Optimize, Review and Validate the Configuration, on page 24

Review and verify the objects:

- **Category**
  - Total ACL rules (Source Configuration)
  - Total ACL rules considered for Optimization. For example, Redundant, Shadow, and so on.
- ACL Count for optimization gives the total number of ACL rules counted before and after Optimization.

If you have missed to download the Post-Migration Reports during migration, use the following link to download:

Post-Migration Report Download Endpoint—http://localhost:8888/api/downloads/post_migration_summary_html_format

Note You can download the reports only when the Secure Firewall migration tool is running.

Procedure

Step 1 Navigate to where you downloaded the **Post-Migration Report**.

Step 2 Open the post-migration report and carefully review its contents to understand how your ASA configuration was migrated:

- **Migration Summary**—A summary of the configuration that was successfully migrated from ASA to Firewall Threat Defense, including information about the ASA interface, Firewall Management Center hostname and domain, target Firewall Threat Defense device (if applicable), and the successfully migrated configuration elements.

  You can also view a comparison chart that illustrates the difference between the count of pre-migration and post-migration states.

- **Selective Policy Migration**—Details of the specific ASA feature selected for migration are available within three categories - Device Configuration Features, Shared Configuration Features, and Optimization.

- **ASA Interface to Threat Defense Interface Mapping**—Details of the successfully migrated interfaces and how you mapped the interfaces on the ASA configuration to the interfaces on the Firewall Threat Defense device. Confirm that these mappings match your expectations.

  Note
  This section is not applicable for migrations without a destination Firewall Threat Defense device or if **Interfaces** are **not** selected for migration.

- **Source Interface Names to Threat Defense Security Zones and Interface Groups**—Details of the successfully migrated ASA logical interfaces and name and how you mapped them to security zones and interface groups in Firewall Threat Defense. Confirm that these mappings match your expectations.

  Note
  This section is not applicable if **Access Control Lists** and **NAT** are **not** selected for migration.

- **Object Conflict Handling**—Details of the ASA objects that were identified as having conflicts with existing objects in Firewall Management Center. If the objects have the same name and configuration, the Secure Firewall migration tool reused the Firewall Management Center object. If the objects have the same name but a different configuration, you renamed those objects. Review these objects carefully and verify that the conflicts were appropriately resolved.

- **Access Control Rules, NAT, and Routes You Chose Not to Migrate**—Details of the rules that you choose not to migrate with the Secure Firewall migration tool. Review these rules that were disabled by the Secure Firewall migration tool and were not migrated. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.

- **Partially Migrated Configuration**—Details of the ASA rules that were only partially migrated, including rules with advanced options where the rule could be migrated without the advanced options. Review these lines, verify whether the advanced options are supported in Firewall Management Center, and if so, configure these options manually.

- **Unsupported Configuration**—Details of ASA configuration elements that were not migrated because the Secure Firewall migration tool does not support migration of those features. Review these lines, verify whether each feature is supported in Firewall Threat Defense. If so, configure those features manually in Firewall Management Center.

- **Expanded Access Control Policy Rules**—Details of ASA access control policy rules that were expanded from a single ASA Point rule into multiple Firewall Threat Defense rules during migration.

- **Actions Taken on Access Control Rules**

- **Access Rules You Chose Not to Migrate**—Details of the ASA access control rules that you choose not to migrate with the Secure Firewall migration tool. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.
- **Access Rules with Rule Action Change**—Details of all Access Control Policy Rules that had 'Rule Action' changed using the Secure Firewall migration tool. The Rule Action values are - Allow, Trust, Monitor, Block, Block with reset. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.
- **Access Control Rules that have IPS Policy and Variable Set Applied**—Details of all ASA access control policy rules that have IPS Policy applied. Review these rules carefully and determine whether the feature is supported in Firewall Threat Defense.
- **Access Control Rules that have File Policy Applied**—Details of all ASA access control policy rules that have File Policy applied. Review these rules carefully and determine whether the feature is supported in Firewall Threat Defense.
- **Access Control Rules that have Rule 'Log' Setting Change**—Details of the ASA access control rules that had 'Log setting' changed using the Secure Firewall migration tool. The Log Setting values are - False, Event Viewer, Syslog. Review these lines and verify that all the rules you choose are listed in this section. If desired, you can configure these rules manually.
- **Access Control Rules that have failed Zone-lookup**—Details of the ASA access control rules that fail the Route-lookup operation and that is populated in the **Post-Migration Report**. The Secure Firewall migration tool performs the route-lookup operation based on the route (static and connected) information in the source configuration to populate the destination security zones in the access rules.
- **Access Control Rules for Tunneled Protocols**—Details of Tunnel rules that are migrated as a prefilter tunnel rule during migration.
- **Errors/Failure on Migrated Configuration**—Details on error causing the migration failure while pushing the migrated configuration elements. The error reported below could be related to the incorrect migrated configuration or else conflict on management center due to some existing configuration or unsupported feature. Review these errors and verify before proceeding or resuming the configuration push to the target management center.

Note
An unsupported rule that was not migrated causes issues with unwanted traffic getting through your firewall. We recommend that you configure a rule in Firewall Management Center to ensure that this traffic is blocked by Firewall Threat Defense.

Note
If it requires you to apply IPS or file policy to ACL in the **Review and Validate** page, you are highly recommended to create a policy on the management center before migration. Use the same policy, as the Secure Firewall migration tool fetches the policy from the connected management center. Creating a new policy and assigning it to multiple policies may degrade the performance and may also result in a push failure.

For more information about supported features in Firewall Management Center and Firewall Threat Defense, see Management Center Configuration Guide, Version 6.2.3.

Step 3 Open the **Pre-Migration Report** and make a note of any ASA configuration items that you must migrate manually on the Firewall Threat Defense device.

Step 4 In Firewall Management Center, do the following:

a) Review the migrated configuration for the Firewall Threat Defense device to confirm that all expected rules and other configuration items, including the following, were migrated:

- Access control lists (ACL)
- Network Address Translation rules
- Port and network objects
- Routes
- Interfaces
- IP SLA objects
- Object Group Search
- Time-based objects
- VPN objects
- Site-to-Site VPN Tunnels
- Dynamic Route objects

b) Configure all partially supported, unsupported, ignored, and disabled configuration items and rules that were not migrated.

For information on how to configure these items and rules, see the Management Center Configuration Guide. The following are examples of configuration items that require manual configuration:

- Platform settings, including SSH and HTTPS access, as described in Platform Settings for Threat Defense
- Syslog settings, as described in Configure Syslog
- Dynamic routing, as described in Routing Overview for Threat Defense
- Service policies, as described in FlexConfig Policies
- VPN configuration, as described in Threat Defense VPN
- Connection log settings, as described in Connection Logging

Step 5 After you have completed your review, deploy the migrated configuration from Firewall Management Center to the Firewall Threat Defense device.

Verify that the data is reflected correctly in the **Post-Migration Report** for unsupported and partially supported rules.

The Secure Firewall migration tool assigns the policies to the Firewall Threat Defense device. Verify that the changes are reflected in the running configuration. To help you to identify the policies that are migrated, the description of those policies includes the hostname of the ASA configuration.

Uninstall the Secure Firewall Migration Tool

All components are stored in the same folder as the Secure Firewall migration tool.

Before you begin

This procedure is applicable to you only if you are using the desktop version of the Secure Firewall migration tool.

Procedure

Step 1 Navigate to the folder where you placed the Secure Firewall migration tool.

Step 2 If you want to save the logs, cut or copy and paste the `log` folder to a different location.

Step 3 If you want to save the pre-migration reports and the post-migration reports, cut or copy and paste the `resources` folder to a different location.

Step 4 Delete the folder where you placed the Secure Firewall migration tool.

Tip
The log file is associated with the console window. If the console window for the Secure Firewall migration tool is open, the log file and the folder cannot be deleted.

Sample Migration: ASA to Threat Defense 2100



Note Create a test plan that you can run on the target device after you complete the migration.

- Pre-Maintenance Window Tasks
- Maintenance Window Tasks, on page 47

Pre-Maintenance Window Tasks

Before you begin

Make sure you have installed and deployed a Firewall Management Center. For more information, see the appropriate Management Center Hardware Installation Guide and the appropriate Management Center Getting Started Guide.

Procedure

Step 1 Use the **show running-config** command for the device or context that you are migrating and save a copy of the configuration. See View the Running Configuration.

Alternately, use Adaptive Security Device Manager (ASDM) for the device or context that you want to migrate and choose **File > Show Running Configuration in New Window** to obtain the configuration file.

Note
For a multi context , you can use the **show tech-support** command to obtain the configuration for all the contexts in a single file.

Step 2 Review the configuration file.

Step 3 Deploy the Firepower 2100 series device in your network, connect the interfaces and power on the appliance.

For more information, see Cisco Threat Defense for the 2100 Series Using Management Center Quick Start Guide.

Step 4 Register the Firepower 2100 series device to be managed by the Firewall Management Center.

For more information, see Add Devices to the Management Center.

Step 5 (Optional) If your source configuration has port channels, create port channels (EtherChannels) on the target Firepower 2100 series device.

For more information, see Configure EtherChannels and Redundant Interfaces.

Step 6 Download and run the most recent version of the Secure Firewall migration tool from https://software.cisco.com/download/home/286306503/type.

For more information, see Download the Secure Firewall Migration Tool from Cisco.com, on page 3.

Step 7 When you launch the Secure Firewall migration tool, and specify destination parameters, make sure that you select the Firepower 2100 series device that you registered to the Firewall Management Center.

For more information, see Specify Destination Parameters for the Secure Firewall Migration Tool, on page 12.

Step 8 Map the ASA interfaces with the Firewall Threat Defense interfaces.

Note
The Secure Firewall migration tool allows you to map an ASA interface type to the Firewall Threat Defense interface type.

For example, you can map a port channel in to a physical interface in Firewall Threat Defense.

For more information, see Map the ASA Interfaces with Threat Defense Interfaces.

Step 9 While mapping logical interfaces to security zones, click **Auto-Create** to allow the Secure Firewall migration tool to create new security zones. To use existing security zones, manually map the ASA logical interfaces to the security zones.

For more information, see Map Logical Interfaces to Security Zones and Interface Groups.

Step 10 Follow the instructions of this guide to sequentially review and validate the configuration to be migrated, and then push the configuration to the Firewall Management Center.

Step 11 Review the Post Migration report, manually setup and deploy other configurations to the Firewall Threat Defense and complete the migration.

For more information, see Review the Post-Migration Report and Complete the Migration, on page 41.

Step 12 Test the Firepower 2100 series device using the test plan that you would have created while planning for migration.

Maintenance Window Tasks

Before you begin

Make sure you have completed all the tasks that must be performed before the maintenance window. See Pre-Maintenance Window Tasks, on page 45.

Procedure

Step 1 Connect to the through the SSH console and switch to the interface configuration mode.

Step 2 Shutdown the interfaces using the **shutdown** command.

Step 3 (Optional) Access the Firewall Management Center and configure dynamic routing for the Firepower 2100 series device.

For more information, see Dynamic Routing.

Step 4 Clear the Address Resolution Protocol (ARP) cache on the surrounding switching infrastructure.

Step 5 Perform basic ping tests from surrounding switching infrastructure to the Firepower 2100 series device interface IP addresses, to make sure that they are accessible.

Step 6 Perform basic ping tests from devices which require layer 3 routing to Firepower 2100 series device interface IP addresses.

Step 7 If you are assigning a new IP address to the Firepower 2100 series device and not reusing the IP address assigned to the ASA perform the following steps:

a. Update any static routes which refer to the IP address, so that they now point to the Firepower 2100 series device IP address.

b. If you are using routing protocols, ensure that neighbors see the Firepower 2100 series device IP address as the next hop for expected destinations.

Step 8 Run a comprehensive test plan and monitor logs within the managing Firewall Management Center for your Firepower 2100 device.