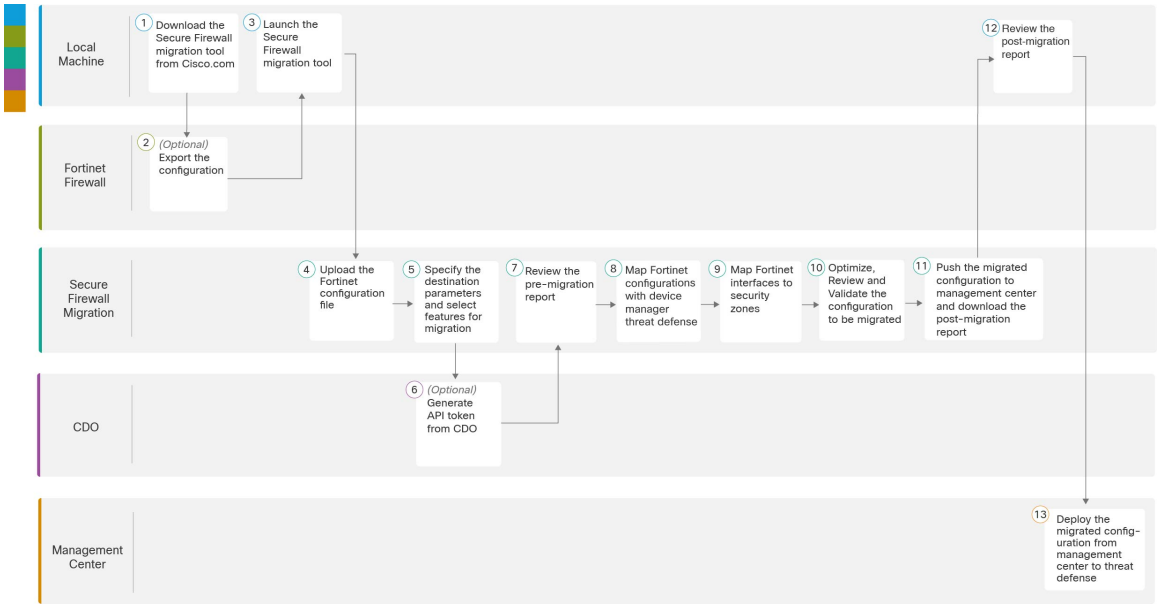
Fortinet Firewall to Threat Defense Migration Workflow

End-to-End Procedure

The following flowchart illustrates the workflow for migrating a Fortinet firewall to threat defense using the Secure Firewall migration tool.



	Workspace	Steps
1	Fortnet Frewall	Export the configuration to the local system, see Download the Secure Firewall Migration Tool from Cisco.com.
2	Fortinet Firewall	Export the Configuration File: To export the configuration from Fortinet firewall, see Export the Configuration from Fortinet Firewall.
3	Local Machine	Launch the Secure Firewall migration tool on your local machine, see Launch the Secure Firewall Migration Tool.
4	Secure Firewall Migration Tool	Upload the Fortinet config file exported from Fortinet firewall, see Upload the Fortinet Configuration File.
5	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. .
6	CDO	(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.
7	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.
8	Secure Firewall Migration Tool	To ensure that the Fortinet configuration is migrated correctly, map the Fortinet interfaces to the appropriate threat defense interface objects, security zones and interface groups. For detailed steps, see Map Fortinet Firewall Configurations with Threat Defense Interfaces
9	Secure Firewall Migration Tool	Map the Fortinet interfaces to the appropriate security zones, see Map Fortinet Interfaces to Security Zones Interface Groups for detailed steps.
10	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.
11	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.
12	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.
13	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 Fortinet 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.

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 threat defense device download areas.

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

Download the appropriate executable of the Secure Firewall migration tool for Windows or macOS machines.

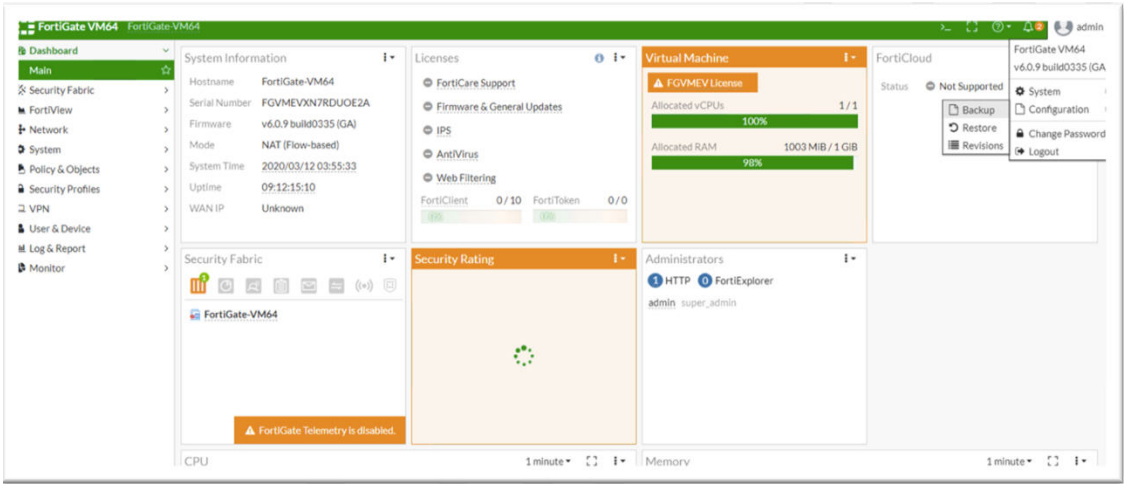
Export the Configuration from Fortinet Firewall

You can export Fortinet firewall configurations in the following ways:

Export Fortinet Firewall Configuration from Fortinet Firewall GUI

Follow these steps to extract the configuration from the Fortinet firewall GUI:

Step 1 From the FortiGate VM64 GUI, choose **Admin** > **Configuration** > **Backup** .



Step 2 Direct the backup to your local PC or to a USB disk.

Note If VDOMs are enabled, indicate whether the scope of the backup is for the entire FortiGate configuration (Global) or only for a specific VDOM configuration (VDOM).

Step 3 Select the VDOM name from the **VDOM** list if the back up is a VDOM configuration.

Note The Secure Firewall migration tool requires an unencrypted file to proceed with the backup process.

Step 4 Select **Ok**.

The web browser prompts you for a location to save the configuration file.

The configuration file has a **.conf** extension.

What to do next

Upload the Fortinet Configuration File

Export Fortinet Firewall Configuration from FortiManager

You can extract the relevant device configuration from FortiManager.

Step 1 Login to FortiManager.

Step 2 Locate the correct Fortigate device for which you must run the backup.

Step 3 Under **Configuration and Installation Status**, choose the icon next to **Total Revision** to get the latest revision.

Step 4 Click **Download** to download the config file.

The downloaded file is a file type with .conf extension.

What to do next

Upload the Fortinet Configuration File

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 CDO, skip to Upload the Fortinet Configuration File.

Note When you launch 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.

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.

  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 pre-migration 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, click the link to verify the version on Cisco.com.

Step 11 Click **Proceed**.

What to do next

You can proceed to the following step:

- If you must extract information from a Fortinet firewall using the Secure Firewall migration tool, proceed to Export the Configuration from Fortinet Firewall.

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 and demo FTD devices.

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 Fortinet Configuration File

Before you begin

Export the configuration file as `.conf` or `.txt` from the source Fortinet 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.

Step 1 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 Fortinet 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 Fortinet.

Step 2 Review the **Context Selection** section and select the Fortinet VDOM that you want to migrate.

Step 3 Click **Start Parsing**.

The **Parsed Summary** section displays the parsing status.

Step 4 Review the summary of the elements in the uploaded configuration file that the Secure Firewall migration tool detected and parsed.

Step 5 Click **Next** to select the target parameters.

What to do next

Specify Destination Parameters for the Secure Firewall Migration Tool, on page 8

Specify Destination Parameters for the Secure Firewall Migration Tool

Before you begin

- Obtain the IP address for the 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.
- (Optional) If you want to migrate device-specific configurations like interfaces and routes, add the target threat defense to the 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 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 access control lists may degrade the performance and may also result in a push failure.

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 threat defense device, you can only migrate to the 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 CDO API token. For generating the API token. from CDO, follow the below steps:

   1. Log in to CDO portal.
   2. Navigate to **Settings** > **General Settings** and copy the API Token.

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 management center and retrieves a list of threat defense devices that are managed by that management center. You can view the progress of this step in the console.

Step 3 Click **Proceed**.

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

- Click the **Select Firewall Threat Defense Device** drop-down list and check the device where you want to migrate the Fortinet configuration.

  The devices in the selected management center domain are listed by **IP Address** and **Name**.

  Note At minimum, the native threat defense device you choose must have the same number of physical or port channel interfaces as the Fortinet configuration that you are migrating. At minimum, the container instance of the 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 Fortinet 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.

  Fortinet firewall migration to management center or threat defense 6.7 or later with the Remote deployment enabled is supported by the Secure Firewall migration tool. However, migration of Interface and Routes must be migrated manually.

- Click **Proceed without FTD** to migrate the configuration to the management center.

  When you proceed without threat defense, the Secure Firewall migration tool will not push any configurations or the policies to threat defense. Thus, interfaces and routes, and site-to-site VPN which are threat defense device-specific configurations will not be migrated and need to be manually configured on 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.

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 threat defense device, the Secure Firewall migration tool automatically selects the features available for migration from the Fortinet 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 management center, the Secure Firewall migration tool automatically selects the features available for migration from the Fortinet configuration in the **Device Configuration**, **Shared Configuration**, and **Optimization** sections. You can further modify the default selection, according to your requirements.

- If you are migrating a configuration from a Fortinet firewall, and if you have VPN configured in your Fortinet firewall, ensure that you do the following on the **Select Features** pane:
  - The migration tool displays your site-to-site VPN features under **Device Configuration**. Select **Policy Based (Crypto Map)** or **Route Based (VTI)**, depending on your requirement.
  - The migration tool displays your remote-access VPN features under **Shared Configuration**.
  - Select **SSL VPN** or both **IPsec VPN** and **SSL VPN**.

    Note You cannot select only **IPsec VPN** because pre-shared key-based (PSK-based) or certificate-based authentication is not supported in management center for remote access VPN configurations.

  If your Fortinet firewall configuration has site-to-site and remote access VPN configured, they are selected by default in the **Select Features** pane. Use the checkboxes to unselect them, if required.
- The Secure Firewall migration tool supports Destination Security Zones that enable mapping of destination zones for the ACL during migration.

  Based on the nature of source and destination network object or groups and service object or groups, this operation may result in ACL rule explosion when migrating from Fortinet to management center.
- (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 Fortinet configuration will not be migrated. This optimizes migration time and cleans out unused objects from the configuration.

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.

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.

Step 1 Navigate to where you downloaded 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.

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

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

- A summary of the supported Fortinet configuration elements that can be successfully migrated to threat defense and specific Fortinet features selected for migration.
- **Configuration Lines with Errors**—Details of Fortinet configuration elements that cannot be successfully migrated because the Secure Firewall migration tool could not parse them. Correct these errors on the Fortinet configuration, export a new configuration file, and then upload the new configuration file to the Secure Firewall migration tool before proceeding.
- **Partially Supported Configuration**—Details of Fortinet configuration elements that can be only partially migrated. These configuration elements include rules and objects with advanced options where the rule or the object can be migrated without the advanced options. Review these lines, verify whether the advanced options are supported in management center, and if so, plan to configure those options manually after you complete the migration with the Secure Firewall migration tool.
- **Unsupported Configuration**—Details of Fortinet configuration elements that cannot be migrated because the Secure Firewall migration tool does not support migration of those features. Review these lines, verify whether each feature is supported in management center, and if so, plan to configure the features manually after you complete the migration with the Secure Firewall migration tool.
- **Ignored Configuration**—Details of Fortinet configuration elements that are ignored because they are not supported by the 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 management center, and if so, plan to configure the features manually.

For more information about supported features in management center and threat defense, see Management Center Configuration Guide.

Step 3 If the **Pre-Migration Report** recommends corrective actions, complete those corrections on the Fortinet interface, export the Fortinet configuration file again and upload the updated configuration file before proceeding.

Step 4 After your Fortinet 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 Fortinet Firewall Configurations with Threat Defense Interfaces

Map Fortinet Firewall Configurations with Threat Defense Interfaces

The threat defense device must have an equal or greater number of physical and port channel interfaces than those used by Fortinet 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 interfaces on the threat defense device. By default, the Secure Firewall migration tool maps the interfaces in Fortinet and the threat defense device according to their interface identities.

The mapping of Fortinet interface to the threat defense interface differs based on the threat defense device type:

- If the target threat defense is of native type:
  - The threat defense must have equal or a greater number of used Fortinet interfaces or port channel (PC) data interfaces (excluding management-only and subinterfaces in the Fortinet configuration). If the number is less, add the required type of interface on the target threat defense.
  - Subinterfaces are created by the secure Firewall migration tool based on physical interface or port channel mapping.
- If the target threat defense is of container type:
  - The threat defense must have equal or a greater number of used Fortinet interfaces, physical subinterfaces, port channel, or port channel subinterfaces (excluding management-only in Fortinet configuration). If the number is less, add the required type of interface on the target threat defense. For example, if the number of physical interfaces and physical subinterface on the target threat defense is 100 less than that of Fortinet then you can create the additional physical or physical subinterfaces on the target 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 management center and chosen the destination as threat defense. For more information, see Specify Destination Parameters for the Secure Firewall Migration Tool, on page 8.

Note This step is not applicable if you are migrating to a management center without a threat defense device.

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 Fortinet interface.

You cannot change the mapping of the management interfaces. If a threat defense interface has already been assigned to an Fortinet 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 threat defense device for all subinterfaces in the Fortinet configuration.

Step 2 When you have mapped each Fortinet interface to a threat defense interface, click **Next**.

What to do next

Map the Fortinet interfaces to the appropriate threat defense interface objects, security zones, and interface groups. For more information, see Map Fortinet Interfaces to Security Zones Interface Groups.

Map Fortinet Interfaces to Security Zones Interface Groups

To ensure that the Fortinet configuration is migrated correctly, map the Fortinet interfaces to the appropriate threat defense interface objects, security zones and interface groups. In an Fortinet configuration, access control policies and NAT policies use interface names (nameif). In management center, those policies use interface objects. In addition, management center policies group interface objects into the following:

- Security zones—An interface can belong to only one security zone.

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

Step 1 To map interfaces to security zones and interface groups that exist in management center, or that is available in 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.

Step 2 To map interfaces to security zones that exist in management center, in the **Security Zones** column, choose the security zone for that interface.

Step 3 You can manually map or auto-create the security zones.

To map the security zones manually, perform the following:

a) Click **Add SZ**.
b) In the **Add SZ** dialog box, click **Add** to add a new security zone.
c) Enter the security zone name in the **Security Zone** column. The maximum characters allowed is 48.
d) Click **Close**.

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

a) Click **Auto-Create**.
b) In the **Auto-Create** dialog box, check **Zone Mapping**.
c) Click **Auto-Create**.

Once you click **Auto-Create**, the source firewall zones are mapped automatically. If the same name zones already exist on management center, then the zone will be re-used. The mapping page will display "(A)" against the re-used zone. For example, **inside** "(A)".

Step 4 When you have mapped all interfaces to the appropriate security zones, click **Next**.

Optimize, Review and Validate the Configuration

Before you push the migrated Fortinet configuration to management center, optimize and review the configuration carefully and validate that it is correct and matches how you want to configure the 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 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.

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.

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

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

- The disabled ACLs are not considered during the optimization process.
- 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 correponding redundant and shadowed ACLs tabulated in an Excel file. Use the **Detailed ACL Information** sheet to view more ACL information. The **Applications** column lists the applications associated with the ACL in your Fortinet firewall.

Step 1 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 policy ID to it to make it easier to map back to the Fortinet configuration file. For example, if a Fortinet 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/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) If you want to apply a 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**.

d) If you want to apply a 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**.

e) 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 management center from the **Syslog** drop-down menu.

f) 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**.

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.

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 2 Click the following tabs and review the configuration items:

- **Access Control**
- **Objects (Network Objects, Port Objects)**
- **NAT**
- **Interfaces**
- **Routes**
- **Site-to-Site VPN Tunnels**
- **Remote Access VPN**

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.

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

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

Step 4 You can view routes from the **Routes** area and select the routes that you do not want to migrate, by selecting an entry and choosing **Actions** > **Do not migrate**.

Step 5 In the **Site-to-Site VPN Tunnels** section, the VPN tunnels from the source firewall configurations are listed. Review the VPN tunnel data such as **Source Interface**, **VPN Type**, and **IKEv1** and **IKEv2** configurations for each row and ensure that you provide the preshared key values for all the rows.

Step 6 In the **Remote Access VPN** section, all objects corresponding to remote access VPN are migrated from Fortinet to the management center, and are displayed:

- **Policy Assignment**: Review and validate your connection profiles, their VPN protocols, targeted devices, and the names of the VPN interfaces. To rename a connection profile, select the corresponding entry and choose **Actions** > **Rename**.
- **IKEV2**: Review and validate your IKEv2 protocol configurations, if any, and the source interfaces mapped with them.
- **Anyconnect Packages**: Retreive the AnyConnect packages and AnyConnect profiles should be retrieved from the source Fortinet 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.
- **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.
- **Connection Profile**—Review all connection profiles/tunnel groups that are displayed here.
- **Trustpoints**—Trustpoint or PKI object migration from the Fortinet firewall 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.

  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 Fortinet firewall, it can be selected under **Override SAML**.

Step 7 (Optional) To download the details for each configuration item in the grid, click **Download**.

Step 8 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 management center, reviews the existing objects, and compares those objects to the list of objects to be migrated. If an object already exists in 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 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 9 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 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 10 When the validation is complete and the **Validation Status** dialog box displays the message **Successfully Validated**, continue with Push the Migrated Configuration to Management Center, on page 18.

Push the Migrated Configuration to Management Center

You cannot push the migrated Fortinet configuration to 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 management center. It does not deploy the configuration to the threat defense device. However, any existing configuration on the 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 management center.

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

Step 2 Click **Push Configuration** to send the migrated Fortinet configuration to management center.

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 management center in the console.

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 14

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.

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 Fortinet configuration was migrated:

- **Migration Summary**—A summary of the configuration that was successfully migrated from Fortinet to threat defense, including information about the Fortinet interface, management center hostname and domain, target threat defense device (if applicable), and the successfully migrated configuration elements.
- **Selective Policy Migration**—Details of the specific Fortinet feature selected for migration are available within three categories - Device Configuration Features, Shared Configuration Features, and Optimization.
- **Fortinet Interface to Threat Defense Interface Mapping**—Details of the successfully migrated interfaces and how you mapped the interfaces on the Fortinet configuration to the interfaces on the threat defense device. Confirm that these mappings match your expectations.

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

- **Source Interface Names to Threat Defense Security Zones**—Details of the successfully migrated Fortinet logical interfaces and name and how you mapped them to security zones in 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 Fortinet objects that were identified as having conflicts with existing objects in management center. If the objects have the same name and configuration, the Secure Firewall migration tool reused the 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 Fortinet 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 management center, and if so, configure these options manually.
- **Unsupported Configuration**—Details of Fortinet 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 threat defense. If so, configure those features manually in management center.
- **Expanded Access Control Policy Rules**—Details of Fortinet access control policy rules that were expanded from a single Fortinet Point rule into multiple threat defense rules during migration.
- **Actions Taken on Access Control Rules**
  - **Access Rules You Chose Not to Migrate**—Details of the Fortinet 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 Fortinet access control policy rules that have IPS Policy applied. Review these rules carefully and determine whether the feature is supported in threat defense.

- **Access Control Rules that have File Policy Applied**—Details of all Fortinet access control policy rules that have File Policy applied. Review these rules carefully and determine whether the feature is supported in threat defense.
- **Access Control Rules that have Rule 'Log' Setting Change**—Details of the Fortinet 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.

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 management center to ensure that this traffic is blocked by 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 management center and threat defense, see Management Center Configuration Guide, Version 6.2.3.

Step 3 Open the **Pre-Migration Report** and make a note of any Fortinet configuration items that you must migrate manually on the threat defense device.

Step 4 In management center, do the following:

a) Review the migrated configuration for the 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

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 management center to the 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 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 Fortinet configuration.

Uninstall the Secure Firewall Migration Tool

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

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: Fortinet 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

Pre-Maintenance Window Tasks

Before you begin

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

Step 1 Save a copy of the Global or per–VDOM configuration from the source Fortinet that you want to migrate.

Step 2 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 3 Register the Firepower 2100 series device to be managed by the management center.

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

Step 4 (Optional) If your source Fortinet configuration has aggregate interfaces, create port channels (EtherChannels) on the target Firepower 2100 series device.

For more information, see Configure EtherChannels and Redundant Interfaces.

Step 5 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 6 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 management center.

For more information, see Specify Destination Parameters for the Secure Firewall Migration Tool, on page 8.

Step 7 Map the Fortinet interfaces with the threat defense interfaces.

Note The Secure Firewall migration tool allows you to map an Fortinet interface type to the threat defense interface type.

For example, you can map an aggregate interfaces in Fortinet to a physical interface in threat defense.

For more information, see Map Fortinet Firewall Configurations with Threat Defense Interfaces.

Step 8 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 Fortinet logical interfaces to the security zones.

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

Step 9 Follow the instructions of this guide to sequentially review and validate the configuration to be migrated, and then push the configuration to the management center.

Step 10 Review the Post Migration report, manually setup and deploy other configurations to the threat defense and complete the migration.

For more information, see .

Step 11 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 22.

Step 1 Clear the Address Resolution Protocol (ARP) cache on the surrounding switching infrastructure.

Step 2 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 3 Perform basic ping tests from devices which require layer 3 routing to Firepower 2100 series device interface IP addresses.

Step 4 If you are assigning a new IP address to the Firepower 2100 series device and not reusing the IP address assigned to the 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 5 Run a comprehensive test plan and monitor logs within the managing management center for your Firepower 2100 device.