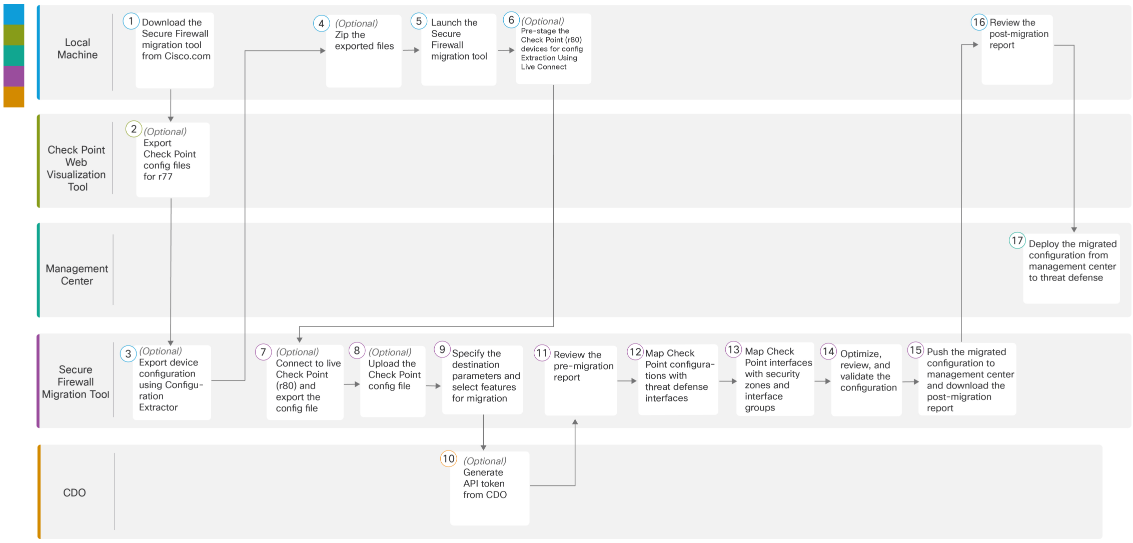
Check Point to Threat Defense Migration Workflow

End-to-End Procedure

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



Local Machine
Check Point Web Visualization Tool
Management Center
Secure Firewall Migration Tool
CDO
1 Download the Secure Firewall migration tool from Cisco.com
2 (Optional) Export Check Point config files for r77
3 (Optional) Export device configuration using Configu-ration Extractor
4 (Optional) Zip the exported files
5 Launch the Secure Firewall migration tool
6 (Optional) Pre-stage the Check Point (r80) devices for config Extraction Using Live Connect
7 (Optional) Connect to live Check Point (r80) and export the config file
8 (Optional) Upload the Check Point config file
9 Specify the destination parameters and select features for migration
10 (Optional) Generate API token from CDO
11 Review the pre-migration report
12 Map Check Point configura-tions with threat defense interfaces
13 Map Check Point interfaces with security zones and interface groups
14 Optimize, review, and validate the configuration
15 Push the migrated configuration to management center and download the post-migration report
16 Review the post-migration report
17 Deploy the migrated configuration from management center to threat defense

	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	Check Point Web Visualization Tool	(Optional) Export the Check Point configuration file for r77: To export the Check Point configuration files for r77, see Export the Check Point Configuration Files for r77, on page 4. If you intend to export configuration files for r80 using Secure Firewall migration tool live connect feature, skip to step 5.
3	Local Machine	Launch the Secure Firewall migration tool on your local machine and select **Check Point (r75–r77)** or **Check Point (r80–r81)** in the **Source Firewall Vendor** drop-down, based on your requirement. See Launch the Secure Firewall Migration Tool for more information.
4	Secure Firewall Migration Tool	(Optional) Export device configuration from Check Point (r75–r77): To export device configuration for r77 using **Configuration Extractor** through a secure gateway connection, see Export Device Configuration Using Configuration Extractor, on page 5.
5	Local Machine	(Optional) Zip the exported files: select all the exported configuration files for r77 and compress them to a zip file. For detailed steps, see Zip the exported files.
6	Local Machine	Pre-stage the Check Point (r80) devices for config Extraction: You must configure the credentials on the Check Point (r80) devices before using Live Connect on the Firewall. For pre-staging credentials on Check Point (r80) devices, see Pre-stage the Check Point (r80) devices for configuration Extraction. This step is only required if you are planning to migrate configuration files for r80 devices. If you have planning to migrate configuration for r77 devices, skip to step 8.
7	Secure Firewall Migration Tool	(Optional) Connect to live Check Point (r80) and export the config file: To export the Check Point configuration files for r80 using live connect feature, see Procedure to Export the Check Point Configuration Files for r80.
8	Secure Firewall Migration Tool	(Optional) Upload the Check Point config file: For detailed steps for uploading Check Point Configuration file, see Upload the Check Point Configuration File.
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.

	Workspace	Steps
12	Secure Firewall Migration Tool	The Secure Firewall migration tool allows you to map the Check Point configuration with threat defense interfaces. For detailed steps, see Map Check Point Configurations with Secure Firewall Device Manager Threat Defense Interfaces.
13	Secure Firewall Migration Tool	To ensure that the Check Point configuration is migrated correctly, map the Check Point interfaces to the appropriate threat defense interface objects, security zones and interface groups. For detailed steps, see Map Check Point 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 Check Point 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

Export the Check Point Configuration Files

Export the Check Point Configuration Files

You can export the Check Point Configuration for the following:

- Export the Check Point Configuration Files for R77
- Export the Check Point Configuration Files for R80

Export the Check Point Configuration Files for r77

To export the Check Point configuration files for r77, perform the following:

- Export the Configuration Using Check Point Web Visualization Tool (WVT)
- Export Device Configuration Using Configuration Extractor, on page 5
- Zip the Exported Files

Export the Configuration Using Check Point Web Visualization Tool (WVT)

Procedure

Step 1 Open the command prompt on the workstation that has access to the Check Point Management Server.

Step 2 Download WVT from the Check Point Portal appropriate for the Check Point Firewall version.

Step 3 Unzip the WVT zip file.

Step 4 Create a new sub folder under the same root folder where the Check Point WVT tool is extracted.

Step 5 Change the directory on the command prompt to the directory where WVT is stored and execute the following commands:

```
C:\Web_Visualisation_Tool> cpdb2web.exe [-s management_server] [-u admin_name | -a certificate_file]
[-p password] [-o output_file_path] [-t table_names] [-c | -m gateway | -l package_names] [-gr] [-go]
[-w Web_Visualization_Tool_installation_directory]
```

For example,

```
C:\Web_Visualisation_Tool> cpdb2web.exe -s 172.16.0.1  -u admin -p admin123 -o  Outputs
```

A total of seven files are created in the *Outputs* directory when these commands are executed, where:

Command	Description
C:\Web_Visualisation_Tool	The root directory for the WVT tool.
172.16.0.1	The IP Address of the Check Point Management Server.
admin	The Check Point Management Server username.
Admin123	The Check Point Management Server password.
Outputs	The relative path to store output files.

Note
The name of the Security Policy and NAT Policy file must be `Security_Policy.xml` and `NAT_Policy.xml` respectively. If the filenames are different, rename them manually.

If there are multiple Security and NAT Policy files, ensure that you select and keep only the `Security_Policy.xml` and `NAT_Policy.xml` files of the Check Point device that you want to migrate.

What to do next

Export Device Configuration Using FMT-CP-Config-Extractor_v2.3.4-5381 Tool

Export Device Configuration Using Configuration Extractor

Procedure

Step 1 In the **Select Source Configuration** page, choose **Check Point (r75–r77)** and click **Start Migration**.

Step 2 On the **Configuration Extractor** pane, click **Connect** to the Check Point Security Gateway for which the policies are to be migrated using the Secure Firewall migration tool.

To connect, you require the following information:

a) IP Address
b) Port
c) Admin Username
d) Admin Password
e) Expert Password
f) (Optional) Virtual ID Number

Step 3 Wait until you see a `networking.txt` file downloaded to your local machine.

The following commands are executed in the background by the configuration extractor and is downloaded as the `networking.txt` file:

- **show hostname**
- **show version product**
- **show interfaces**
- **fw vsx stat**
- **show management interface**
- **show configuration bonding**
- **show configuration bridging**
- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**
- **show configuration ipv6 static-route**
- **netstat -rnv**

For example, 172.16.0.1 is the IP address of Check Point Firewall Gateway for which the policies are to be migrated.

Step 4 If you are trying to export configuration from a Check Point VSX (Virtual System eXtension) version R77 having a virtual ID, the following commands are executed in the background:

- **show hostname**
- **show version product**
- **show interfaces**
- **fw vsx stat**
- **fw vsx stat <vsid>**
- **set virtual system <vsid>**

  Tip
  vsid indicates the virtual system ID.

- **fw getifs**
- **show management interface**
- **show configuration bonding**
- **show configuration bridging**
- **show configuration interface**
- **show configuration static-route**
- **show ipv6-state**

- **show configuration ipv6 static-route**
- **netstat -rnv**

Step 5 Move the .txt file to the `Outputs` folder.

What to do next

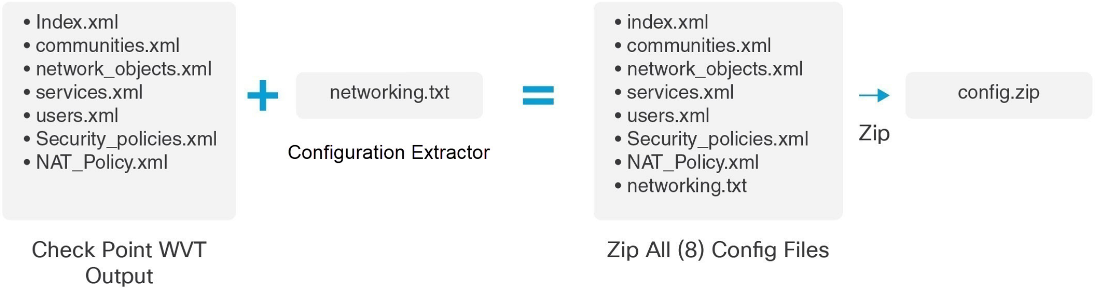
Zip the Exported Files

Zip the Exported Files

Procedure

Select all the eight files (seven from the Web Visualization Tool (WVT) and one .txt file from the Configuration Extractor) and compress them to a zip file.

Note
Before you zip the files for migration, ensure that the `Security_Policy.xml` and `NAT_Policy.xml` files are for the Check Point device that you want to migrate to the threat defense.



Note
.tar or other compressed file types are not supported.

What to do next

Upload the Check Point 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 Security Cloud Control, skip to Upload the Check Point Configuration File .

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 Check Point configuration to your computer, proceed to Upload the Check Point Configuration File.
- If you must extract information from a Check Point (r77) using the Secure Firewall migration tool, proceed to Export the Check Point Configuration Files for r77.
- If you must extract information from a Check Point (r80) using the Secure Firewall migration tool, proceed to Export the Check Point Configuration Files for r80.

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.

Export the Check Point Configuration Files for r80

Note Export of Check Point r80 configuration is supported only with the Live Connect feature on the Secure Firewall migration tool.

To configure on the Check Point device the credentials required for migration and to export the Check Point configuration files, perform the following:

- Pre-stage the Check Point (r80) Devices for Configuration Extraction using Live Connect
- Procedure to export the Check Point Configuration Files for r80

Pre-Stage the Check Point (r80) Devices for Configuration Extraction Using Live Connect

Note Ensure that your Check Point management center command line (CLI) is in CLISH mode. If it is in Expert mode, exit Expert mode and switch to CLISH mode before proceeding with the configuration export via Live Connect.

You can configure the credentials on the Check Point (r80) devices before migration using any one of the following steps:

- Distributed Check Point Deployment—When you have an independent Check Point Security Gateway and a Check Point Security Manager.
- Standalone Check Point Deployment—When you have a Check Point Security Gateway and a Check Point Security Manager as one single device.
- Multi-Domain Check Point Deployment—When you have a Check Point Security Gateway and a Check Point Security Manager with a multi-domain deployment setup.

Export from Distributed Check Point Deployment

You must configure the credentials on the Check Point (r80) devices before using Live Connect on the Secure Firewall migration tool to extract the Check Point configuration.

The procedure for pre-staging credentials on a distributed Check Point deployment includes the following steps:

Procedure

Step 1 Create the following on the Gaia Console Check Point Security Gateway:

a) In the web browser, open the Check Point Gaia Console application through an HTTPS session to connect to the Check Point Security Gateway.

b) Navigate to the **User Management** tab and choose **Users** > **Add**.

c) In the **Add User** window, create a new username and password with the following details:

- From the **Shell** drop-down, choose */etc/cli.sh*.
- From the **Available Roles**, choose *adminRole*.
- Retain the default values for the remaining fields.
- Click **Ok**.

d) SSH into your Check Point Security Gateway and create a new password using the command:

set expert-password <password>

Note

- If you already have the expert password configured on the Check Point device, reuse that.
- You will need these credentials on **Connect to Check Point Security Gateway** page as shown in step 3.

Once you have configured the expert password, the pre-staging of credentials for Check Point r80 Gateway is complete.

For more information, see Figure 3.

Step 2 Create the username and password on the Check Point Security Manager for r80:

a) On the SmartConsole application, perform these steps:

1. Log in to Check Point Security Manager.
2. Navigate to **Manage and Settings** > **Permissions and Administrators** > **Administrators**.

3. Click ***** to create a new username and password, and perform these steps:

    - Choose **Authentication Method** as **Check Point Password**.
    - Click **Set New Password** to set up a new password.

      Note
      Ensure that you do not select the **User Must Change Password on the Next Login** check box.

    - Choose **Permission Profile** as **Super User**.
    - Choose **Expiration** as **Never**.

4. Click **Publish** to save the configuration changes on the Check Point SmartConsole application.

b) On the Gaia Console for Check Point Security Manager, perform these steps:

Note
Ensure that the username and password that you now create is the same as that created in the SmartConsole application in Step 2a.

1. In the web browser, open the Gaia Console application through an HTTPS session to connect to the Check Point Security Manager.
2. Navigate to the **User Management** tab, and choose **Users** > **Add**.
3. Create a username and password that are the same as the username and password created in Step 2a (3) of the SmartConsole application.

    - From the **Shell** drop-down, choose */bin/bash*.
    - From the **Available Roles** drop-down, choose *adminRole*.
    - Retain the default values for the remaining fields.
    - Click **Ok**.

4. SSH into the Check Point Security Manager and create an expert password using the command:

    set expert-password <password>

    Note
    - If you have already configured the expert password, you can use that password.
    - The username and password that are created in Step 2b (3) and Step 2a (3) must be the same.

Pre-staging of credentials on Check Point in a distributed deployment for Check Point Security Manager is complete.

You will need these credentials on **Connect to Check Point Security Manager** page as shown in Step 4.

If you are using a custom API port on the Check Point Smart Manager, see Custom API Port for Check Point r80.

What to do next

Export the Check Point Configuration Files for r80

Export from Standalone Check Point Deployment

You must configure the credentials on the Check Point (r80) devices before using Live Connect on the Secure Firewall migration tool to extract the Check Point configuration.

The procedure for pre-staging credentials on standalone Check Point deployment includes the following steps:

Procedure

Step 1 In the web browser, open the Gaia Console application through an HTTPS session to connect to the standalone Check Point Device that manages both Check Point Security Gateway and Check Point Security Manager.

Step 2 Navigate to the **User Management** tab and choose **Users** > **Add**.

a) In the **Add User** window, create a new username and password with the following details:

- From the **Shell** drop-down, choose */etc/cli.sh*.
- From the **Available Roles** drop-down, choose *adminRole*.
- Retain the default values for the remaining fields.
- Click **Ok**.

You will need these credentials on **Connect to Check Point Security Gateway** page as shown in step 3.

For more information, see Figure 3.

b) In the **Add User** window, create another username and password with the following details:

- From the **Shell** drop-down, choose */bin/bash*.
- From the **Available Roles** drop-down, choose *adminRole*.
- Retain the default values for the remaining fields.
- Click **Ok**.

Step 3 Create the following on the SmartConsole application for r80 on the Check Point device:

Note
Ensure that the username and password that you will now create are the same as those created in the Check Point Gaia Console in the preceding step.

a) Log in to SmartConsole application of the Check Point device.
b) Navigate to **Manage and Settings** > **Permissions and Administrators** > **Administrators**.
c) Click ***** to create a new username and password with the following details:

- Choose the **Authentication Method** as **Check Point Password**.
- Click **Set New Password** to set up a new password.

  Note
  Ensure that you do not select the **User Must Change Password on the Next Login** check box.

- Choose the **Permission Profile** as **Super User**.
- Choose the **Expiration** as **Never.**

The username and password that you created in Step b of Step 2 and Step c of Step 3 must be the same.

You will need these credentials on **Connect to Check Point Security Manager** page as shown in Step 4.

d) Click **Publish** to save the configuration changes on the Check Point SmartConsole application.

Step 4 SSH into the Check Point device and create an expert password using the command:

set expert-password <password>

Note

- If you already have the expert password configured on the Check Point device, reuse that.
- The username and password that were created in Step b of Step 2 and Step c of Step 3 must be the same.

Pre-staging of credentials on Check Point devices in a Standalone deployment is complete.

If you are using a custom API port on the Check Point Smart Manager, see Custom API Port for Check Point r80.

What to do next

Export the Check Point Configuration Files for r80

Export from Multi-Domain Check Point Deployment

You must configure the credentials on the Check Point (r80) devices using Live Connect on the Secure Firewall migration tool to extract the Check Point configuration.

The procedure for pre-staging credentials on a multi-domain Check Point deployment includes the following steps:

Procedure

Step 1 Create the following on the Gaia Console Check Point Security Gateway:

a) In the web browser, open the Gaia Console application through an HTTPS session to connect to the Check Point Security Gateway.

b) Navigate to the **User Management** tab, and choose **Users** > **Add**.

c) In the **Add User** window, create a new username and password with the following details:

- From the **Shell** drop-down, choose */etc/cli.sh*.
- From the **Available Roles** drop-down, choose *adminRole*.
- Retain the default values for the remaining fields.
- Click **Ok**.

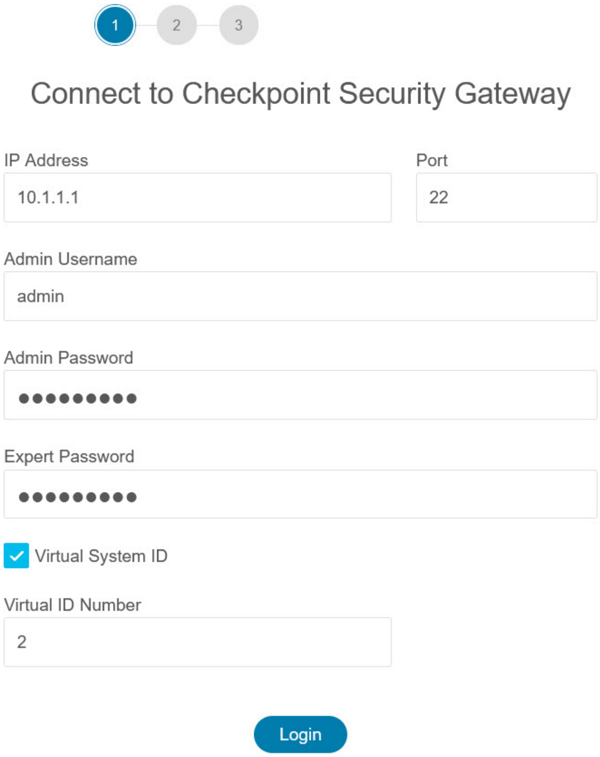
d) SSH into your Check Point Security Gateway and create a new password using the command:

set expert-password <password>

Pre-staging of credentials on the Check Point Security Gateway for a multi-domain deployment is complete.

e) (Optional) When exporting configuration from a Virtual System Extension (VSX) device, check the **Virtual System ID** checkbox to be able to enter the virtual system ID.

Figure 1: Connect to Check Point Security Gateway - Multi-Domain Deployment



Connect to Checkpoint Security Gateway

IP Address: 10.1.1.1

Port: 22

Admin Username: admin

Admin Password: ●●●●●●●●●

Expert Password: ●●●●●●●●●

☑ Virtual System ID

Virtual ID Number: 2

Step 2 Create the username and password on the Check Point Security Manager:

a) On the SmartConsole (mds) application, perform these steps:

1. Log in to Check Point Security Manager.
2. Navigate to **Manage and Settings** > **Permissions and Administrators** > **Administrators**.
3. Click ***** to create a new username and password with the following details:
   - Choose the **Authentication Method** as **Check Point Password**.
   - Click **Set New Password** to set up a new password.

     Note
     Ensure that you do not select the **User Must Change Password on the Next Login** check box.

   - Choose the **Permission Profile** as **Multi-domain Super User**.
   - Choose the **Expiration** as **Never**.
4. Click **Publish** to save the configuration changes on the Check Point SmartConsole application.

   If you are using a custom API port on the Check Point Smart Manager, see Custom API Port for Check Point r80.

b) On the Gaia Console for Check Point Security Manager, perform these steps:

Note
Ensure that the username and password that you will now create is the same as that created in the SmartConsole application Step 2a (3).

1. In the web browser, open the Gaia Console application through an HTTPS session to connect to the Check Point Security Manager.
2. Navigate to the **User Management** tab, and choose **Users** > **Add**.
3. Create a username and password that is the same as that created in Step 2a (3) of the SmartConsole application.
   - From the **Shell** drop-down, choose */bin/bash*.
   - From the **Available Roles** drop-down, choose *adminRole*.
   - Retain the default values for the remaining fields.
   - Click **Ok**.
4. SSH into your Check Point Security Manager and create a new password using the command:

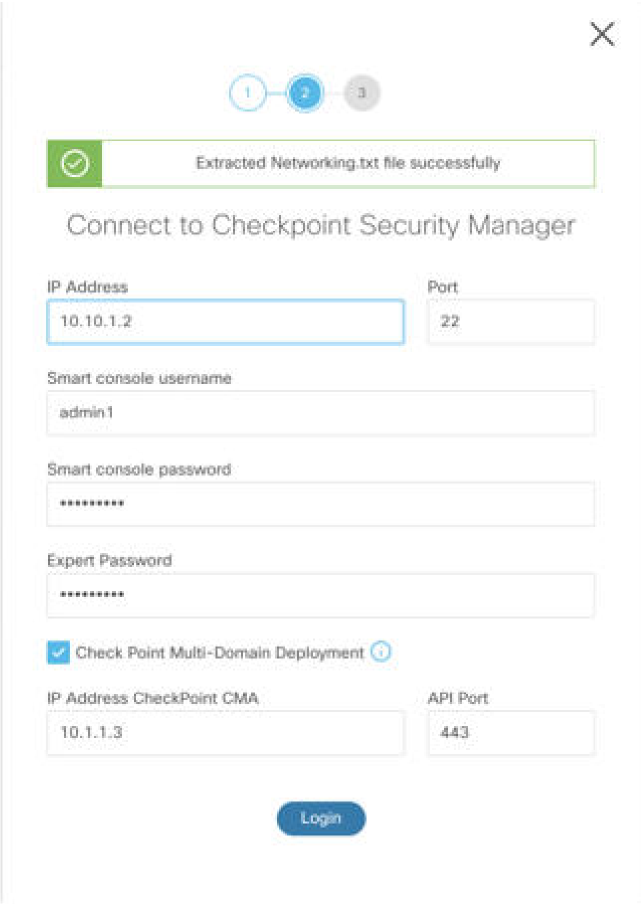
   set expert-password <password>

   Note
   - If you already have the expert password configured on the Check Point device, reuse that.
   - The username and password that are created in Step 2a (3) and Step 2b (3) must be the same.

Pre-staging of credentials on Check Point Security Manager in a Multi-Domain deployment is complete.

You will need the credentials to connect to Live Connect as in Figure 2.

Figure 2: Connect to Check Point Security Manager - Multi-Domain Deployment



Extracted Networking.txt file successfully

Connect to Checkpoint Security Manager

IP Address: 10.10.1.2

Port: 22

Smart console username: admin1

Smart console password: *********

Expert Password: *********

☑ Check Point Multi-Domain Deployment

IP Address CheckPoint CMA: 10.1.1.3

API Port: 443

Note

- If you are using a custom API port on the Check Point Smart Manager, see Custom API Port for Check Point r80.
- Extraction of Global Policy Package for Multi-Domain Deployment is not possible. Hence, the Objects, ACE rules, and NAT rules configured as part of configuration under Check Point CMA are only exported and migrated.

What to do next

Export the Check Point Configuration Files for r80

Use a Custom API Port for Check Point (r80) Security Manager

Note If you are using a custom API port on the Check Point Smart Manager, perform these steps:

- Check the **Check Point Multi-Domain Deployment** check box on the **Check Point Security Manager** page of Live Connect.
- Add the IP Address of Check Point CMA and API port details if using the multi-domain deployment.
- Retain the IP Address of the Check Point Security Manager if it is a general deployment and enter the details of the Custom API Port.

Procedure to Export the Check Point Configuration Files for r80

Before you begin

It is mandatory to pre-stage the Check Point devices. For detailed information on configuring the credentials on the Check Point (r80) devices before migration, see Pre-stage the Check Point (r80) Devices for Configuration Extraction Using Live Connect.

Note

- We recommend that you use Live Connect to extract the Check Point (r80) configurations.
- Using a Check Point (r80) configuration, that is not exported using Live Connect in the Secure Firewall migration tool, results in the configuration getting migrated as unsupported, getting partially migrated, or resulting in a failed migration.

  If the information in the configuration export is incomplete, certain configurations are not migrated and are marked as **unsupported**.

To export the Check Point configuration files for r80, perform the following:

Procedure

Step 1 Select Check Point (r80) from the **Select Source Config** page.

Step 2 Click **Connect**.

Note
Live connect is available for Check Point (r80) only.

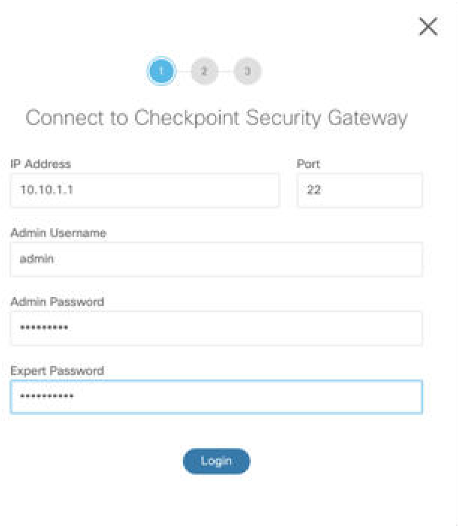
Step 3 Connect to Check Point Security Gateway. Perform the following:

a) Enter the following in the Check Point r80 Security Gateway:

- IP Address
- SSH Port
- Admin Username

- Admin Password
- Expert Password

Figure 3: Connect to Check Point Security Gateway



Connect to Checkpoint Security Gateway

IP Address: 10.10.1.1

Port: 22

Admin Username: admin

Admin Password: *********

Expert Password: **********

b) Click **Login**.

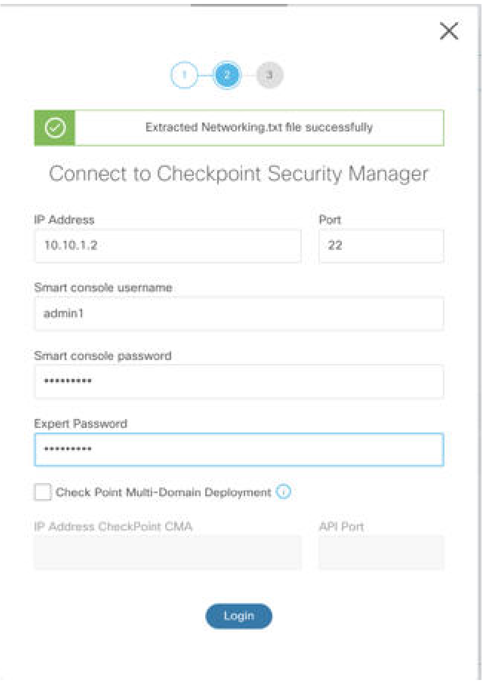
The Secure Firewall migration tool generates the *networking.txt* file that has device-specific configurations such as interface and route configurations. Store the *networking.txt* file in a local directory for the current session of the Secure Firewall migration tool.

Step 4 Connect to Check Point Security Manager. Perform the following:

a) Enter the following in the Check Point r80 Security Manager:

- IP Address
- SSH Port
- Smart Console Username
- Smart Console Password
- Expert Password

Figure 4: Connect to Check Point Security Manager



Extracted Networking.txt file successfully

Connect to Checkpoint Security Manager

IP Address: 10.10.1.2

Port: 22

Smart console username: admin1

Smart console password: •••••••••

Expert Password: •••••••••

□ Check Point Multi-Domain Deployment

IP Address CheckPoint CMA

API Port

b) Click **Login**.

The Secure Firewall migration tool generates the *Extracted-objects.json* file that captures the complete network and service object configuration available in the Check Point Security Manager.

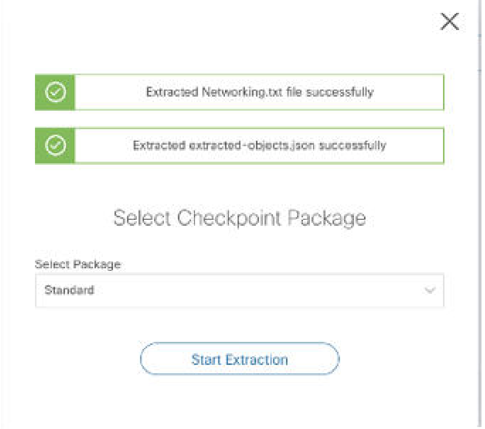
Store the *Extracted-objects.json* in a local directory for the current session of the Secure Firewall migration tool.

Note

If you have connected the Secure Firewall migration tool to the Check Point Security Manager, the list of policy packages available in the Check Point Security Manager is displayed.

Step 5 Select the Check Point Policy Package that you want to migrate from the **Select Check Point Package** list, and click **Start Extraction**.

Figure 5: Extracting the Check Point Policy Package



Extracted Networking.txt file successfully

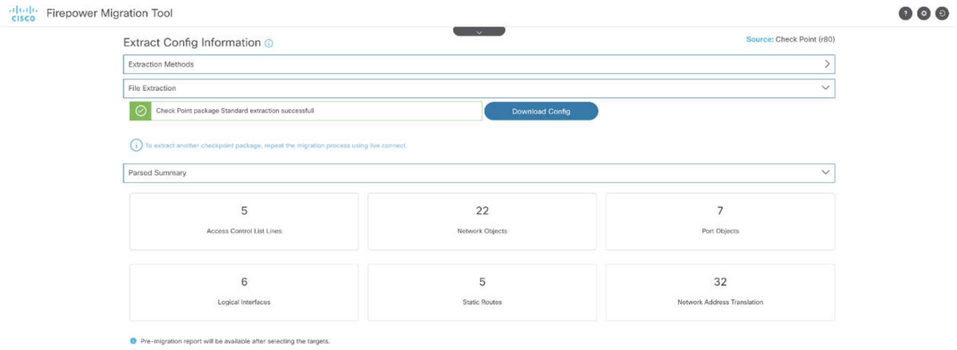
Extracted extracted-objects.json successfully

Select Checkpoint Package

Select Package: Standard

Step 6 Download the configuration and proceed with the migration.

Figure 6: Extraction of the Check Point Configuration Complete for Distributed and Standalone Deployment



Extract Config Information

Source: Check Point (r80)

Check Point package Standard extraction successfull

To extract another checkpoint package, repeat the migration process using live connect.

5 Access Control List Lines	22 Network Objects	7 Port Objects
6 Logical Interfaces	5 Static Routes	32 Network Address Translation

Pre-migration report will be available after selecting the targets.

Step 7 Click **Next** to proceed with Migration of Check Point (r80) configuration.

What to do next

Upload the Check Point Configuration File

Extract Another Configuration File

To extract another configuration file, perform the following steps:

- Click **Back to source selection** to extract a new configuration for a different policy package or to connect to a different Check Point (r80) firewall.
- Download the current configuration if you must migrate the extracted Check Point (r80) configuration later.

Note The current configuration file is downloaded to a default download location set by the browser.

You can use Assembly Line Approach to extract r80 configuration:

- Perform Live Connect to extract the Check Point (r80) configuration file for each package of firewall or for different firewalls.
- Create a repository for multiple configurations.
- Use the **Start Migration later** option using manual upload to proceed with the migration later.

Upload the Check Point Configuration File

Before you begin

Export the configuration file as .zip format.

Procedure

Step 1 On the **Extract Config Information** screen, in the **Manual Upload** section, click **Upload** to upload the Check Point configuration file.

Step 2 Browse to the location where the configuration file is stored. The configuration file is extracted for Check Point (r77) and downloaded using Live Connect for Check Point (r80). Click **Open**.

The Secure Firewall migration tool uploads the configuration file. For large configuration files, this step takes longer time.

The pre-parsing process is now complete.

The Parsed Summary section displays the parsing status.

Step 3 Review the summary of the elements that the Secure Firewall migration tool detected and parsed in the uploaded configuration file.

Step 4 Click **Next** to select the target parameters.

What to do next

Specify Destination Parameters for the Migration Tool

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.

- (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**.

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

- Click the **Select FTD Device** drop-down list and check the device where you want to migrate the Check Point configuration.

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 Check Point 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 Check Point 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.

Check Point firewall migration to Firewall Management Center or Firewall Threat Defense 6.7 or later with the Remote deployment enabled is supported by the Secure Firewall migration tool. Migration of Interface and Routes must be done manually.

- 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.

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 Check Point 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 the Check Point configuration in the **Device Configuration**, **Shared Configuration**, and **Optimization** sections. You can further modify the default selection, according to your requirements.
- For Check Point, under **Shared Configuration**, select the relevant **Access Control** option:
  - Global Policy—When you select this option, the source, and destinations zone for the ACL policy are migrated as **Any**.
  - Zone-Based Policy—When you select this option, source, and destination zones are derived based on the predicative route-lookup through routing mechanism for the source and destination network objects or groups.

    Note

Route-lookup is limited to Static routes and Dynamic routes (PBR and NAT are not considered) and depending on the nature of the source and destination Network Object-Groups, this operation may result in rule explosion.

The routing information is obtained from the `networking.txt` file. This file is the output of the FMT-CP-Config-Extractor_v4.0.1-8248 Tool that uses **netstat -rnv** command to gather the routing table. For more information, see Export Device Configuration Using FMT-CP-Config-Extractor_v4.0.1-8248 Tool.

IPv6 Route-lookup for Zone-Based policies is not supported in this release. Ensure that all the rules of the Global Policy or of the Zone-Based Policy are migrated successfully.

Under **Device Configuration**, choose interfaces, routes, and site-to-site VPN tunnel configurations to be migrated from your Check Point firewall. Note that you can migrate only a policy-based (cryptomap) site-to-site VPN tunnel configuration.

- (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 Check Point 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.

What to do next

Review the Pre-Migration Report, on page 25

Review the Pre-Migration Report

Procedure

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

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.

Note

Each table in the pre-migration report displays 30 entries. For more than 30 entries, you must download the CSV file by clicking the icon on top-right of the table.

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

- **Overall Summary**—Overall summary of the supported Check Point configuration elements that can be successfully migrated to Firepower Threat Defense. For example, Policy Names, Rule Counts etc.
- **Configuration Lines with Errors**—Information about Check Point configuration elements that couldn't be migrated successfully due to parsing issues by the Migration Tool. Rectify these errors in the Check Point device, generate a new configuration file, and upload this file to the Migration Tool before proceeding with the migration.
- **Ignored Configuration**—List of all the Check Point configuration elements that are ignored by FMT during migration and will not be carried forward to the target system.

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

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

Step 4 After your Check Point configuration file is successfully uploaded and parsed, return to the Secure Firewall migration tool and click **Next** to continue the migration.

Map Check Point Firewall 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 Check Point 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 Check Point and the Firewall Threat Defense device according to their interface identities. For example, the 'management-only' interface on the Check Point interface is automatically mapped to the 'management-only' interface on the Firewall Threat Defense device and is unchangeable.

The mapping of Check Point 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 Check Point interfaces or port channel (PC) data interfaces (excluding management-only and subinterfaces in the Check Point 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 Check Point interfaces, physical subinterfaces, port channel, or port channel subinterfaces (excluding management-only in Check Point 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 Check Point 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 22.

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 Check Point interface.

You cannot change the mapping of the management interfaces. If a Firewall Threat Defense interface has already been assigned to an Check Point 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 Check Point configuration.

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

What to do next

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

Map Check Point Interfaces to Security Zones and Interface Groups

To ensure that the Check Point configuration is migrated correctly, map the Check Point interfaces to the appropriate Firewall Threat Defense interface objects, security zones and interface groups. In an Check Point 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.

The Secure Firewall migration tool allows one-to-one mapping of interfaces with security zones and interface groups; 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 and Interface Groups** screen, review the available interfaces, security zones, and interface groups.

Step 2 To map interfaces to security zones and interface groups that exist in Firewall 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 3 To map interfaces to security zones and interface groups that exist in Firewall Management Center, or that is available in Check Point (r80) 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 that interface.
b) In the **Interface Groups** column, choose the interface group for that interface.

Step 4 You can manually map or auto-create the security zones and interface groups.

Step 5 To map the security zones and interface groups manually, perform the following:

a) Click **Add SZ & IG**.
b) In the **Add SZ & IG** dialog box, click **Add** to add a new security zone or Interface Group.
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 Check Point 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 Check Point interface. For example, if the Check Point logical interface is in L3 mode, the security zone and interface group that is created for the interface is also in L3 mode.

Step 6 When you have mapped all interfaces to the appropriate security zones and interface groups, click **Next**.

Optimize, Review and Validate the Configuration

Before you push the migrated Check Point 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.

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 Check Point 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.

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.
- Inconsistent objects—If there are objects with similar names but different content, the object names are modified by the Secure Firewall migration tool before the migration push.

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

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

c) 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 Check Point configuration file. For example, if a Check Point 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**.

   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 3 Click the following tabs and review the configuration items:

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

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 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 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 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 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 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 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 10 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 33.

Push the Migrated Configuration to Firewall Management Center

You cannot push the migrated Check Point 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 Check Point configuration to Firewall 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 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 for Check Point and Complete the Migration

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:

Note
Each table in the pre-migration report displays 30 entries. For more than 30 entries, you must download the CSV file by clicking the icon on top-right of the table.

- **Migration Summary**—A summary of the configuration that was successfully migrated from Check Point to Firepower Threat Defense.

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

- **Selective Policy Migration**—Details of the specific Check Point features selected for migration and Interface Mapping are available.

- **Migration Conversions**—Conversion and push details which includes the following:
  - Network/Service object handling
  - List of partially migrated configurations with reasons
  - List of Unsupported configurations with reason
  - Expanded Access Control Rules

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: Check Point 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 37

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 Check Point Web Visualization Tool and FMT-CP-Config-Extractor_v4.0.1-8248 Tool to collect the Check Point device configurations that you are trying to migrate and save a copy of the Check Point configuration files.

Step 2 Review the Check Point configuration zip 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 Check Point configuration has bond interfaces, 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 22.

Step 8 Map the Check Point interfaces with the Firewall Threat Defense interfaces.

Note

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

For example, you can map a bond interface in Check Point to a physical interface in Firewall Threat Defense.

For more information, see Map the Check Point 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 Check Point logical interfaces to the security zones.

For more information, see Map Check Point 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 for Check Point and Complete the Migration, on page 35.

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 36.

Procedure

Step 1 Connect to the Check Point Security Gateway through the Gaia Console.

Step 2 Shutdown the Check Point interfaces of intended Security Gateway through the Gaia console.

Step 3 (Optional) Access the Firewall Management Center and configure dynamic routing, platform settings, and other features that are not migrated by the Secure Firewall migration tool that are needed manually for the Firepower 2100 series device.

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 Check Point 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.