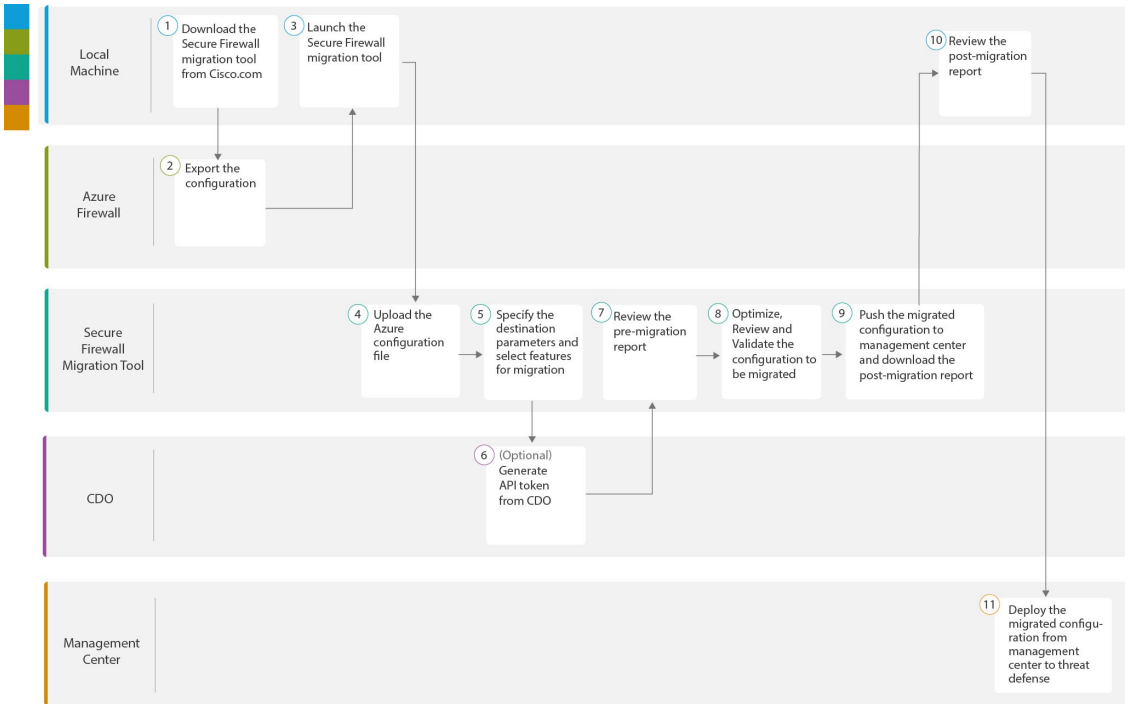
Microsoft Azure Native Firewall to Threat Defense Migration Workflow

End-to-End Procedure

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



	Workspace	Steps
1	Local Machine	Download the latest version of Secure Firewall migration tool from Cisco.com. For detailed steps, see Download the Secure Firewall migration tool from Cisco.com.
2	Azure Firewall	Export the Configuration File: To export the configuration from Azure firewall, see Export the Configuration from Microsoft Azure Native Firewall, on page 3.
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 Azure configuration file exported from Azure firewall, see Upload the Microsoft Azure Configuration File, on page 7.
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, step 1.
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	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.
9	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.
10	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.
11	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 Microsoft Azure 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 CDO, 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 CDO user and want to use the migration tool hosted on it, log in to your CDO tenant and on the left pane, navigate to **Administration** > **Migration** > **Firewall Migration Tool** to create your migration instance.

Export the Configuration from Microsoft Azure Native Firewall

Follow the below procedure to export the Microsoft Azure configuration:

- Export Policy Configuration from Azure Firewall GUI, on page 3
- Export IP Group Configuration, on page 4

Export Policy Configuration from Azure Firewall GUI

Use this procedure to export policy configuration from Microsoft Azure firewall GUI.

Procedure

Step 1 From the Microsoft Azure firewall GUI, choose **Policy**.

Step 2 Select **Export Template** under **Automation** section.

Step 3 Click the download button to download the configuration.

The policy configuration is downloaded in zipped format. Extract the template.json file.

What to do next

Export IP Group Configuration, on page 4

Export IP Group Configuration

Use this procedure to extract IP address group configuration from Microsoft Azure PowerShell

Procedure

Step 1 Open PowerShell and run the command:

```
Get-AzIpGroup -ResourceGroupName "your_ResourceGrp_name"| Select Name,IPAddresses
```

Note
Replace `your_ResourceGrp_name` with resource group name.

Step 2 Copy the output in text file and save it as “IPGroup.txt“.

What to do next

Upload the Microsoft Azure Configuration File, on page 7

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 Microsoft Azure Configuration File, on page 7 .

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

- 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 FDM-managed device configuration to your computer, proceed to Upload the Microsoft Azure Configuration File, on page 7.

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, 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 Microsoft Azure Configuration File

Use this procedure to upload the Microsoft Azure configuration file to the Firewall Migration Tool.

Before you begin

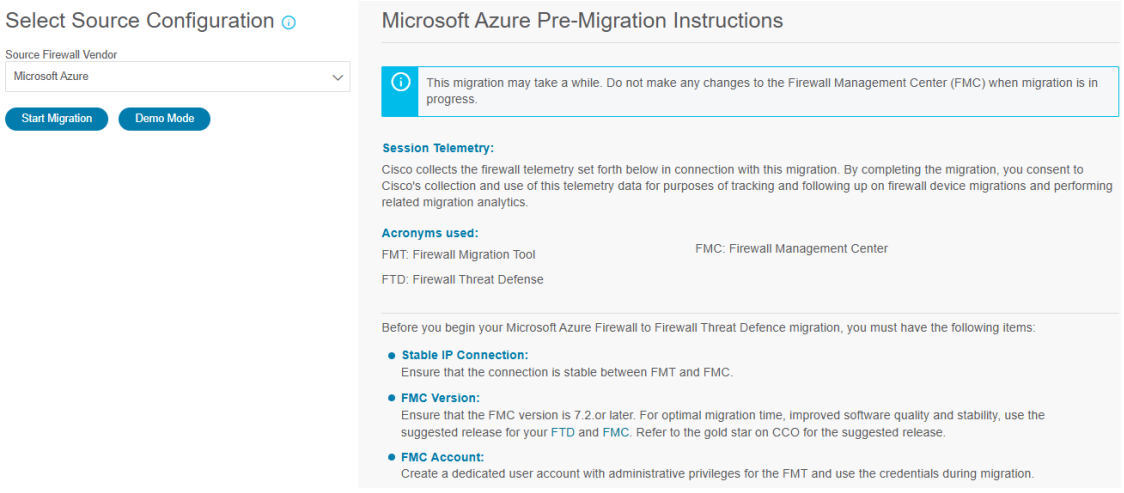
- Export the policy and IP group configuration file from the source Azure device. For more information, see Export the Configuration from Microsoft Azure Native Firewall, on page 3.
- Create a zip file that include the IPGroup.txt and template.json files, which were extracted.

Note If IPGroup is not configured in the Azure environment, use only the template.json file for migration.

Procedure

Step 1 Launch the Secure Firewall Migration Tool.

Step 2 From the drop-down list choose **Microsoft Azure** in **Select Source Configuration** window and click **Start Migration**.



Step 3 Click **Upload** in the **Extract Config Information** window and select the zip file from your local machine.

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.

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 CDO, 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) to the Firewall Management Center. See Adding Devices to the Firewall Management Center

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

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 Azure configuration.

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

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

- 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 Azure 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 theAzure configuration in the **Device Configuration**, **Shared Configuration**, and **Optimization** sections. You can further modify the default selection, according to your requirements.

  Note
  The **Device Configuration** section is not applicable for Azure migration. The migration of Interface and Routes must be done manually.

- (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 Azure 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 10

Review the Pre-Migration Report

Note Review all contents of the Pre-Migration Report carefully. The Unsupported rules are not migrated completely, which might alter the original configuration, restrict traffic, or permit unwanted traffic. We recommend that you update the related rules and policies in Firewall Management Center to handle the traffic appropriately after the configuration is successfully migrated.

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

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

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

Procedure

Step 1 Navigate to 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 Azure configuration elements that can be successfully migrated to Firewall Threat Defense and specific Azure features selected for migration.
- **Configuration Lines with Errors**—Details of Azure configuration elements that cannot be successfully migrated because the Secure Firewall migration tool could not parse them. Correct these errors on the Azure configuration, export a new configuration file, and then upload the new configuration file to the Secure Firewall migration tool before proceeding.

- **Ignored Configuration**—Details of Azure configuration elements that are ignored because they are not supported by the Firewall Management Center or the Secure Firewall migration tool. The Secure Firewall migration tool does not parse these lines. Review these lines, verify whether each feature is supported in Firewall Management Center, and if so, plan to configure the features manually.

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

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

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

Optimize, Review and Validate the Configuration

Before you push the migrated Azure 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.

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.

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 Azure 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

Select the ACL and click download icon at the top-right of the **Optimize, Review and Validate Configuration** window to review the ACL name and the correponding redundant and shadowed ACLs tabulated in an Excel file.

Object Optimization

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

- Network Object
- Port Object
- URL Object

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

Note
You can choose **Actions** > **Edit** to edit any rule.

b) 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.
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, select the row by checking the check box for the policy, and choose **Actions** > **Edit**.

Edit Rule dialog box appears. You can update existing data or add new data in the chosen policy.

To add an object to source or destination:

1. Choose the object from the left pane by checking the check box for it.
2. Click the **Add Source** or **Add Destination** button under **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.

All rules that are not applicable are grayed out in the table.

d) 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.

e) 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**.

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, URL Objects)**
- **NAT**

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

Step 5 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 6 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 7 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 14.

Push the Migrated Configuration to Firewall Management Center

You cannot push the migrated Azure 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 Azure 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 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 11

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

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

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

Procedure

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

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

- **Migration Summary**—A summary of the configuration that was successfully migrated from Azure firewall to Firewall Threat Defense, including information about the source Azure device, target Firewall Threat Defense device, and the successfully migrated configuration elements.

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

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

- **Object Conflict Handling**—Details of the Azure firewall objects identified as having conflicts with the existing objects in Firewall Management Center. If the objects have the same name but a different configuration, you can rename these objects. Review these objects carefully and verify that the conflicts are appropriately resolved.

- **Optimization**—Details of the Azure firewall objects and ACL optimization. If the objects have the same name and configuration, the Migration Tool reuses the management center object. Review these objects carefully and verify that the conflicts are appropriately resolved.

- **ACL Category Conflict Handling**—Details of the ACL Rule categories identified as having conflicts with naming limitation on management center. The category names are trimmed as it exceeded the supported limit on management center. Review these categories carefully.

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

- **Action Taken on Converted Features**—Details of the features that you chose not to migration using the Migration Tool.

  - **Access Rules You Chose Not to Migrate**—Details of the Access Control rules that you chose not to migrate using the Migration Tool. Review these lines and verify that all the rules you chose are listed in this section. If necessary, you can configure these rules manually.

  - **NAT Rules You Chose Not to Migrate**—Details of the Network Address Translation (NAT) rules that you chose not to migrate using the Migration Tool. Review these lines and verify that all the rules you chose are listed in this section. If necessary, you can configure these rules manually.

  - **Access Rules with Rule Action Change**—Details of all the Access Control Policy rules that had ‘Rule Action’ changed using the Migration Tool. The Rule Action values are - Allow, Trust, Monitor, Block, Block with reset. Review these lines and verify that all the rules you chose are listed in this section. If necessary, you can configure these rules manually.

  - **Access Control Rules that have Rule ‘Log’ Setting Change**—Details of the 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 necessary, you can configure these rules manually.

- **Errors/Failure on Migrated Configuration**—Details on error causing the migration failure while pushing the migrated configuration elements. The error reported below could be related to the incorrect migrated configuration or else conflict on management center due to some existing configuration or unsupported feature. Review these errors and verify before proceeding or resuming the configuration push to the target management center.

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

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

Step 4 After you have completed your review, deploy the migrated configuration from Firewall Management Center to the Firewall Threat Defense device.

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

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

Parse Summary

Parse summary displays the number of objects, interfaces, NAT, policy, and application. The summary has three components: Pre-parse Summary, Parse Summary and Pre-push Summary.

- **Pre-parse Summary**—Pre-parse summary is displayed after the configuration is uploaded. At this stage, the Secure Firewall migration tool displays the count of various components. Only custom applications or applications that are used in the group is displayed. If a configuration is multi-vsys, the interface count will be displayed for the complete *vsys*. Pre-parse summary does not show all the applications because, the application that is called directly in policy is not counted. So, application count is different than the Parse summary. Similar behavior is applicable on NAT. Few components of the Pre-parse summary may display zero count but that does not mean that these configurations have zero configurations elements.
- **Parse Summary**—Parse summary is displayed after you click start conversion. At this stage, the Secure Firewall migration tool has taken the action on the configuration and all the unsupported configuration is removed from the summary count. The unsupported policies are part of the count, as unsupported policies are migrated to the Firewall Management Center as disabled. Every component of the configuration is parsed. The count that is displayed at the Parse summary is the exact configuration count that is going to get migrated.
- **Pre-push Summary**—Pre-push summary is displayed before you are prompted to push the configuration to the Firewall Management Center. The Pre-parse summary count may be different from the parse summary as per the action taken by the Secure Firewall migration tool. Directly referenced IP in NAT will be pushed as objects. If applications are mapped to ports, service count increases and the application will go down. If application mapping is left blank, the application count reduces. If the static route has a duplicate entry, that will be removed and the count will decrease.

Migration Failures

The following are the parsing failures during migration:

- **Parse Failure**—Parse failure occurs after the configuration is uploaded to the Secure Firewall migration tool. Due to the misconfiguration of the interface. If multiple IPs are configured or a /32 or /128 IP is assigned to interface, that leads to a parsing failure.

  If an interface has multiple IP assigned or tunneled, loopback, or VLAN interface are part of routing, that leads to a push failure.

  Workaround—Download the **Pre-Migration Report** and refer to **Configuration lines with errors** section of the Migration Report. This section displays the details of the configuration that is causing the issue. You must rectify the issue and reupload the configuration to Secure Firewall migration tool.

  If push failure is caused by tunnel, loopback, or VLAN interface in the routes, you must delete such routes and retry the migration, as such interfaces are not supported on the Firewall Management Center.

- **Push Failure**—Push failure occurs when Secure Firewall migration tool has migrated the configuration and is being pushed to the Firewall Management Center. Push failures are captured in the **Post-Migration Report**.

  Workaround—Download the **Post-Migration Report** and refer to **Error Reporting** section of the Migration Report. This section displays the details of the configuration that causes the issue. You must rectify the issue on the **Review and Validation** page by choosing **do not migrate** option for the section that shows the failure or you can fix the issue in the source configuration and reupload the configuration to Secure Firewall migration tool.

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: Azure 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 20

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 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 2 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 3 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 4 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 8.

Step 5 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 6 Review the Post Migration report, manually setup and deploy other configurations to the Firewall Threat Defense and complete the migration.

For more information, see Review the Post-Migration Report and Complete the Migration, on page 15.

Step 7 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 19.

Procedure

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 Firewall Management Center for your Firepower 2100 device.