Migrate an ASA Configuration to a Firepower Threat Defense Configuration

Prepare the ASA for Migration

Step 1 Verify that the ASA device meets the requirements for configuration migration; see ASA Device Requirements.

Step 2 Identify the access control lists (ACLs) and NAT policies you want to export.

Step 3 Determine how many entries are present in the ACL:

```
show access-list acl_name | i elements
```

Step 4 If the configuration contains more than 2000000 elements, prune as many inessential elements as possible.

Install the Migration Tool

Caution Do **not** install the migration tool on a production Firepower Management Center. Use of this tool is *not* supported on production devices. After installing the migration tool, you can uninstall the tool only by reimaging the designated Firepower Management Center.

Step 1 Download one of the following images from Support:

- Firepower Management Center Virtual for VMware
- Firepower Management Center Virtual for KVM

Step 2 Use the image file to install a dedicated Firepower Management Center Virtual, as described in the appropriate guide:

- *Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide*
- *Cisco Firepower Management Center Virtual for KVM Deployment Quick Start Guide*

Step 3 Connect to the Firepower Management Center via `ssh`, using the `admin` username.

Step 4 Log in to the root shell:

```
sudo su -
```

Step 5 Run the following command:

```
enableMigrationTool.pl
```

Note After the process completes, refresh any web interface sessions running on the Firepower Management Center to use the migration tool.

Save the ASA Configuration File

The migration tool can convert ASA configuration files in either the .cfg or .txt format.

Step 1 Save the configuration.
The commands you use to save this configuration may differ depending on the version of your ASA device. For more information, see the version-appropriate ASA configuration guide, as listed in the ASA documentation roadmap at http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html#pgfId-126642.

Step 2 Transfer the saved configuration file to a location accessible from the migration tool (for example, your local computer or a shared drive on your network).

Convert the ASA Configuration File

Follow the steps below to convert the ASA configuration file (.cfg or .txt) to a Firepower configuration file (.sfo).

Caution The migration tool UI is an extension of the Firepower Management Center UI. However, *only* the functionality described in this procedure is viable.

Step 1 In the migration tool, choose **System** > **Tools** > **Import/Export**

Step 2 Click **Upload Package**.

Step 3 Click **Browse**, and choose the configuration file you exported from the ASA.

Step 4 Click **Next**.

Step 5 Choose the policy you want the system to use when converting access rules:

- **Prefilter Policy—**Converts the access rules to prefilter rules.
- **Access Control Policy—**Converts the access rules to access control rules.

Step 6 If you chose **Prefilter Policy**, choose the action you want the system to assign for access rules with a Permit action:

- **Fastpath—**Exempts matching traffic from all further inspection and control, including access control, identity requirements, and rate limiting. Fastpathing a tunnel fastpaths all encapsulated connections.
- **Analyze—**Allows traffic to continue to be analyzed by the rest of access control. If passed by access control and any related deep inspection, this traffic may also be rate limited.

Step 7 If you chose **Access Control Policy**, choose the action you want the system to assign rules with a Permit action:

- **Trust—**Allows traffic to pass without deep inspection or network discovery. Trusted traffic is still subject to authentication requirements imposed by an identity policy, and to rate limiting.
- **Allow—**Allows matching traffic to pass. Allowed traffic is still subject to authentication requirements imposed by an identity policy, to rate limiting, and to deep inspection (if configured).

Step 8 Specify how you want the system to handle unsupported rules:

- **Convert as disabled rules**
- **Do not convert and add to migration report**

Step 9 Choose the action the system should assign when converting access rules with logging enabled:

- **At the start of connection**
- **At the end of connection**
- **Both**

Step 10 Choose **Next**.

The system queues the migration as a task. You can view the status of the task in the Message Center.

Step 11 Click on the System Status icon to display the Message Center.

Step 12 Click on the **Tasks** tab.
The migration task is listed as the top message, because only migration tool tasks can be run on the intermediary Firepower Management Center.

Step 13 If the migration fails, review error messages in the appropriate logs; for more information, see Troubleshoot Conversion Failure, on page 4.

Step 14 If the migration is successful:

- Click **Download .sfo** to copy the converted file to your local computer.
- Click **Migration Report** to view the Migration Report.

Step 15 Review the Migration Report.
The Migration Report summarizes which ASA configurations the migration tool could or could not successfully convert to Firepower Threat Defense configurations. Unsuccessfully converted configurations include:

- ASA configurations that are not supported in the Firepower System
- ASA configurations that are supported in the Firepower System (that have Firepower equivalents) but that the migration tool does not convert

For unsuccessfully converted configurations that have Firepower equivalents, you can manually add them after you import the converted policies onto your production Firepower Management Center.

Troubleshoot Conversion Failure

If the conversion fails on the dedicated Firepower Management Center, the migration tool records error data in troubleshooting files you can download to your local computer.

Step 1 Choose **System** > **Health** > **Monitor**.

Step 2 In the **Appliance** column of the appliance list, click the name of the dedicated Firepower Management Center.

Step 3 Click **Generate Troubleshooting Files**.

Step 4 Check the **All Data** check box.

Step 5 Click **Generate**.
The system queues troubleshooting file generation as a task.

Step 6 Track the task's progress by viewing it in the Message Center.

Step 7 After the system generates the troubleshooting files and the task status changes to `Completed`, click **Click to retrieve generated files**.

Step 8 Follow the directions from TAC to send the troubleshooting files to Cisco.

Import the Converted ASA Configuration

In a multidomain deployment of a Firepower Management Center, the system assigns the converted ASA configuration to the domain where you import it. On import, the system populates the **Domain** fields in the converted objects.

Step 1 On your production Firepower Management Center, choose **System** > **Tools** > **Import/Export**

Step 2 Click **Upload Package**.

Step 3 Click **Choose File**, and use browse to choose the appropriate .sfo file on your local computer.

Step 4 Click **Upload**.

Step 5 Choose which policies you want to import. Policies may include access control policies, prefilter policies, or NAT policies, depending on your earlier migration choices.

Step 6 Click **Import**.
The system analyzes the file and displays the Import Conflict page.

Step 7 On the Import Conflict page:

- Resolve conflicts in the configuration; see Import Conflict Resolution in *Firepower Management Center Configuration Guide*.
- Replicate how rules were grouped by interface in the original ASA configuration, or replace that group association with a new one. To do so, you must assign access control rules to security zones, and prefilter or NAT rules to interface groups, as follows:

Type	Source	Choose This Zone or Group If:
System-generated security zones/interface group	The migration tool automatically creates this security zone/interface group during conversion.	You want to replicate how the rules were grouped by interface in the original ASA configuration.
Security zones/interface group created prior to importing converted ASA configuration	You create this security zone/interface group prior to importing the converted ASA configuration.	You want to associate the rules with a security zone/interface group that already exists on the Firepower Management Center.
Security zone/interface group created on-the-fly during the import process	You create this security zone/interface group by choosing `New...` from the drop-down list next to the rule set.	You want to associate the rules with a new security zone/interface group on the Firepower Management Center.

Tip Use the arrow next to a rule set to expand additional information about the set.

Note The migration tool does not convert interface configurations; you must manually add devices and configure the interfaces on those devices after importing the converted ASA configuration. However, this import step allows you to retain the association between the ACL or NAT policy and a single entity (a security zone or interface group) that you can quickly associate with an interface on the new Firepower Threat Defense device. For more information on associating security zones/interface groups with interfaces, see Configure the Migrated Policies, on page 7.

Step 8 Click **Import**.
When the import is complete, the system displays a message directing you to the Message Center.

Step 9 Click the System Status icon to display the Message Center.

Step 10 Click the **Tasks** tab.

Step 11 Click the link in the import task to download the import report.

Install Firepower Threat Defense

Install Firepower Threat Defense using the appropriate Quick Start Guide, listed in the table below.

Note The Quick Start Guide procedures include installing a new image on the device, so you can use the same procedures whether installing Firepower Threat Defense on a new device or reimaging the original ASA to Firepower Threat Defense.

Platform	Quick Start Guide
Firepower Threat Defense: ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, ASA 5512-X, ASA 5515-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/5500X/ftd-55xx-X-qsg.html
Firepower 4100 Series with Threat Defense: 4110, 4120, and 4140	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp4100/ftd-4100-qsg.html
Firepower 9300 with Threat Defense	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp9300/ftd-9300-qsg.html
Firepower Threat Defense Virtual: VMware	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-qsg.html
Firepower Threat Defense Virtual: AWS Cloud	http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/aws/ftdv-aws-qsg.html

Configure the Migrated Policies

This procedure describes high-level steps for configuring migrated policies on the Firepower Management Center. For more detailed information on each step, see the related procedure in the *Firepower Management Center Configuration Guide*.

Step 1 Assign the interfaces on the Firepower Threat Defense device to the security zones or interface groups created during the conversion process.

Step 2 If you migrated the ASA access rules to an access control policy:

- Optionally, tune the rules in the policy by enabling or editing disabled rules, adding rules, removing rules, and changing rule order. For example, you might want to edit any rules that specify either different source and destination protocols or multiple protocols; see Access Rules that Specify Multiple Protocols.
- Optionally, configure the Firepower equivalents for ASA parameters that tool does not convert:

Access Rule Parameter	Access Control Rule Parameter
User	Selected Users condition
Security Group (Source)	custom SGT condition
Enable Logging	Log at Beginning of Connection and/or Log at End of Connection option
Logging Level	connection event logging
Logging Interval	connection event logging

- Assign the access control policy to the Firepower Threat Defense device.

Step 3 If you migrated the ASA access rules to a prefilter policy:

- Optionally, tune the rules in the policy by enabling or editing disabled rules, adding rules, removing rules, and changing rule order. For example, you might want to edit any rules that specify either different source and destination protocols or multiple protocols; see Access Rules that Specify Multiple Protocols.
- Optionally, configure the Firepower equivalents for ASA parameters that the tool does not convert:

Access Rule Parameter	Prefilter Rule Parameter
Enable Logging	Log at Beginning of Connection and/or Log at End of Connection option
Logging Level	connection event logging
Logging Interval	connection event logging

- Configure the new access control policy that the system created during conversion, or associate the prefilter policy with a different access control policy.
- Assign the associated access control policy to the Firepower Threat Defense device.

Step 4 If you migrated a NAT policy:

- Optionally, tune the rules in the policy by enabling or editing disabled rules, adding rules, removing rules, and changing rule order.
- Assign the NAT policy to the Firepower Threat Defense device.

Step 5 Optionally, configure next-generation firewall features, including application visibility and control, intrusion protection, URL filtering, and Advanced Malware Protection (AMP).

Step 6 Deploy configuration changes; see Deploy Configuration Changes, on page 8.

Deploy Configuration Changes

Use the steps below to deploy the migrated configuration. For more information on the deploy process, see Deploying Configuration Changes in the *Firepower Management Center Configuration Guide*

Step 1 On the Firepower Management Center menu bar, click **Deploy**.
The Deploy Policies dialog lists devices with out-of-date configurations. The **Version** at the top of the dialog specifies when you last made configuration changes. The **Current Version** column in the device table specifies when you last deployed changes to each device.

Step 2 Identify and choose the devices where you want to deploy configuration changes.

- Sort—Sort the device list by clicking a column heading.
- Expand—Click the plus icon (⊞) to expand a device listing to view the configuration changes to be deployed.

  The system marks out-of-date policies with an index (🕘) icon.
- Filter—Filter the device list. Click the arrow in the upper-right corner of any column heading in the display, enter text in the **Filter** text box, and press Enter.

Step 3 Click **Deploy**.

Step 4 If the system identifies errors or warnings in the changes to be deployed, you have the following choices:

- Proceed—Continue deploying without resolving warning conditions.You cannot proceed if the system identifies errors.
- Cancel—Exit without deploying. Resolve the error and warning conditions, and attempt to deploy the configuration again.