# Introduction to Cisco ASA to Firepower Threat Defense Migration

This guide describes how to use Cisco's migration tool to migrate firewall policy settings from your Cisco ASA to a Firepower Threat Defense device.

The Cisco ASA provides advanced stateful firewall and VPN concentrator functionality. It has long been the industry standard for firewalls. For more information on this product, see http://www.cisco.com/go/asa.

Firepower Threat Defense represents the next step in firewall evolution. It provides unified next-generation firewall and next-generation IPS functionality. In addition to the IPS features available on Firepower Software models, firewall and platform features include Site-to-Site VPN, robust routing, NAT, clustering, and other optimizations in application visibility and access control. Firepower Threat Defense also supports Advanced Malware Protection (AMP) and URL filtering. For more information on this product, see http://www.cisco.com/go/ngfw.

Cisco's migration tool allows you to convert specific features in an ASA configuration to the equivalent features in an Firepower Threat Defense configuration. After this conversion, Cisco recommends that you complete the migration manually by tuning the converted policies and configuring additional Firepower Threat Defense policies.

You can migrate an ASA configuration to a new Firepower Threat Defense device, or to the original ASA device after refreshing it as a Firepower Threat Defense device.

# The Migration Tool

To migrate an ASA configuration to a Firepower Threat Defense configuration Firepower Management Center, use the ASA-to-Firepower Threat Defense migration tool image to prepare a dedicated Firepower Management Center Virtual for VMware. This dedicated Management Center does not communicate with any devices. Instead, the migration tool allows you to convert an ASA configuration file in .cfg or .txt format to a Firepower import file in .sfo format, which you can then import on your production Management Center.

The migration tool can only convert data in the ASA configuration format (that is, a flat file of ASA CLI commands in the appropriate order). When you use the migration tool, the system validates the file's format. For example, the file must contain an ASA version command. If the system cannot validate the file, the conversion fails.

# ASA Device Requirements

The migration tool can migrate configuration data from the following ASA devices:

***Table 1: Supported Platforms and Environments in Version 6.2.1***

| Supported Platforms | Supported Environments |
|---|---|
| Any | ASA Version 9.8/ASDM Version 7.8<br>ASA Version 9.7/ASDM Version 7.7<br>ASA Version 9.6/ASDM Version 7.6<br>ASA Version 9.5/ASDM Version 7.5<br>ASA Version 9.4/ASDM Version 7.4<br>ASA Version 9.3/ASDM Version 7.3<br>ASA Version 9.2/ASDM Version 7.2<br>ASA Version 9.1/ASDM Version 7.1<br>ASA Version 9.0/ASDM Version 7.0<br>ASA Version 8.4/ASDM Version 6.4 |

In addition, the ASA device must be:

- Running in single-context mode.
- The active unit if it is part of a failover pair.
- The Master unit if it is part of a cluster.

The ASA device can be running in transparent or routed mode.

# Firepower Device Requirements

The migration process described in this document requires the following Firepower devices:

- A migration tool running on a dedicated Firepower Management Center Virtual for VMware.
- Your production Firepower Management Center. Must be running a supported environment on a supported platform:

| **Supported Firepower Management Center Platforms** | **Supported Firepower Management Center Environments** |
|---|---|
| Firepower Management Centers: FS750, FS1000, FS1500, FS2000, FS2500, FS3500, FS4000, Virtual | Must be the same version as the migration tool. |

- Your production Firepower Threat Defense device (can be the reimaged ASA device). For a list of supported platforms and environments for Firepower Threat Defense, see theFirepower System Compatibility Guide.

# License Requirements

To use the migrated configurations described in this document, you must have a Base Firepower Threat Defense license. For more information, see http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-licenseroadmap.html.

The migration tool does not migrate license information, because ASA devices require different licenses than Firepower Threat Defense devices. You must purchase new licenses for your Firepower Threat Defense device. For questions about pricing licenses in the context of migration, contact Sales.

# ASA Features Supported for Migration

The migration tool allows you to migrate the following ASA features:

- Extended access rules (can be assigned to interfaces and assigned globally)
- Twice NAT and network object NAT rules
- Any network objects/groups or service objects/groups associated with the extended access rules and NAT rules that the tool converts

For a description of how the tool converts the ASA configurations to Firepower Threat Defense configurations, see Conversion Mapping Overview.

# Migration Limitations

When migrating your ASA configuration, be aware of the following limitations:

### ASA Configuration Only

The migration tool converts only ASA configurations. It does not convert existing ASA FirePOWER configurations. You must manually convert an existing ASA FirePOWER configuration to a Firepower Threat Defense configuration.

### ACL and ACE Limits

There is no specific limit to the size of the ASA configuration file that the migration tool can convert. However, Cisco recommends that you reduce the complexity and size of your ASA configuration as much as possible prior to conversion. Complex policies and rules can command significant resources and negatively affect performance. When you deploy configuration changes in Firepower, the system evaluates all rules together and creates an expanded set of criteria that target devices use to evaluate network traffic. If these criteria exceed the resources (physical memory, processors, and so on) of a target device, you cannot deploy the configuration to that device.

### Applied Rules and Objects Only

The migration tool only converts ACLs that are applied to an interface; that is, the ASA configuration file must contain paired **access-list** and **access-group** commands.

The migration tool only converts objects if they are associated with either actively-applied ACLs or NAT rules; that is, the ASA configuration file must contain appropriately associated **object**, **access-list**, **access-group**, and **nat** commands. You cannot migrate network and service objects alone.

### Unsupported ACL and NAT Configurations

The migration tool supports most ACL and NAT configurations, with certain exceptions. It handles unsupported ACL and NAT configurations as follows:

Converts but Disables—The migration tool cannot fully convert ACEs that use:

- Time range objects
- Fully-qualified domain names (FQDN)
- Local users or user groups
- Security group (SGT) objects
- Nested service groups for both source and destination ports

  It cannot convert certain elements of these rules because there is no Firepower equivalent functionality for the unsupported elements. In these cases, the tool converts rule elements that have Firepower equivalents (for example, source network), excludes rule elements that do not have Firepower equivalents (for example, time range), and disables the rule in the new access control or prefilter policy it creates.

  Egress ACL rules migrated from an ASA configuration are unsupported rules. They appear in a disabled state.

  For each disabled rule, the system also appends `(unsupported)` to the rule name and adds a comment to the rule indicating why the system disabled the rule during migration. After importing the disabled rules on your Firepower Management Center, you can manually edit or replace the rules for successful deployment in the Firepower System.

Excludes—The migration tool excludes the following configurations from policies it creates: EtherType or WebType ACLs, ACEs that use host address name aliases (specified by the **name** command), and ACEs that use predefined (default) service objects. For more information about these excluded configurations, see *CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide* or *ASDM Book 2: Cisco ASA Series Firewall ASDM Configuration Guide*.

### Other Unsupported ASA Configurations

The migration tool does not support migration for ASA features other than those specified in this document. When the tool processes the ASA configuration file, it ignores any configuration data for unsupported features.

# Migration Checklist

Before using the migration tool, verify the following:

- The ASA device meets all requirements for migration; see ASA Device Requirements, on page 2.
- The ASA configuration file is in either .cfg or .txt format.
- The ASA configuration file contains only supported configurations and meets the required limits for migration; see Migration Limitations, on page 3.
- The ASA configuration file contains only valid ASA CLI configurations. Correct any incorrect or incomplete commands before continuing. If the file contains invalid configurations, the migration fails.
- To import a converted ASA configuration file, the Firepower Management Center must be running the same version as the migration tool where you convert the configuration. This restriction is applicable to both major and minor releases. For example, if the migration tool is running Version 6.2.1, but the Firepower Management Center where you want to import the file is running Version 6.1.0.2, you must upgrade to Firepower Management Center 6.2.1 before you can import the converted ASA configuration file.

# Documentation Conventions

This documentation provides examples of ASA configurations converted to Firepower Threat Defense configurations. Most of the columns in these examples map directly to components in the relevant Rule Editor or in the Object Manager on the Firepower Management Center. The table below lists the columns that do not map directly to Firepower UI components.

***Table 2: Columns that Use Indirect Values***

| Column | Value | Description |
|---|---|---|
| Enabled | True/False | Specifies whether the **Enabled** check box is checked or unchecked in the access control or prefilter rule. |
| Action | Permit equivalent | Specifies a value determined by choices you make during conversion, as follows:<br>• If you choose to convert access rules to access control rules, you also choose whether this value is **Allow** or **Trust**.<br>• If you choose to convert access rules to prefilter rules, you also choose whether this value is **Fastpath** or **Analyze**. |

| Column | Value | Description |
|---|---|---|
| Domain | None | At the point of conversion, this field is empty, because the system does not assign the domain until you import it on your production Firepower Management Center. On import, the system assigns the domain based on the domain where you import the converted configuration. |
| Override | True/False | Specifies whether the **Allow Overrides** check box is checked or unchecked in the object. |