



Cisco ASA to Firepower Threat Defense Migration Guide, Version 6.2.2

First Published: 2017-08-30

Last Modified: 2018-03-09

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Introduction to Cisco ASA to Firepower Threat Defense Migration 1

ASA-to-Firepower Threat Defense Migration Tool 2

ASA Device Requirements 2

Firepower Device Requirements 3

License Requirements 4

ASA Features Supported for Migration 4

Migration Limitations 4

Migration Checklist 5

Documentation Conventions 6

CHAPTER 2

Migrate an ASA Configuration to a Firepower Threat Defense Configuration 7

Prepare the ASA for Migration 7

Install the Migration Tool 7

Save the ASA Configuration File 8

Convert the ASA Configuration File 8

Troubleshoot Conversion Failure 10

Import the Converted ASA Configuration 10

Install Firepower Threat Defense 11

Configure the Migrated Policies 12

Deploy Configuration Changes 13

APPENDIX A

Conversion Mapping 15

Conversion Mapping Overview 15

Naming Conventions for Converted Configurations 16

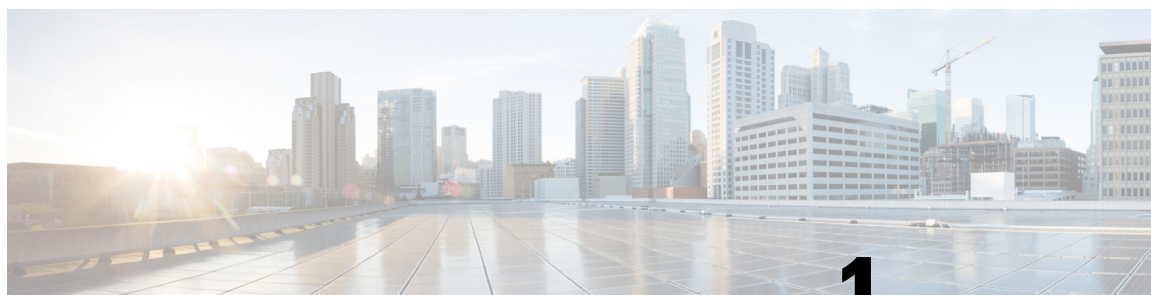
Fields Specific to Firepower Objects and Object Groups 18

Access Rule Conversion 18

| | |
|--|----|
| Access Rule Conversion to Access Control Rules | 18 |
| Access Rule Fields Mapped to Access Control Rule Fields | 19 |
| Fields Specific to Access Control Rules | 20 |
| Access Rule Conversion to Prefilter Rules | 21 |
| Access Rule Fields Mapped to Prefilter Rule Fields | 21 |
| Fields Specific to Firepower Prefilter Rules | 22 |
| Port Argument Operators in Access Rules | 23 |
| Access Rules that Specify Multiple Protocols | 24 |
| NAT Rule Conversion | 25 |
| ASA NAT Rule Fields Mapped to Firepower Threat Defense Rule Fields | 25 |
| Network Object and Network Object Group Conversion | 27 |
| Network Object Conversion | 27 |
| Network Object Group Conversion | 28 |
| Service Object and Service Group Conversion | 29 |
| Service Object Conversion | 29 |
| Port Literal Values in Service Objects | 30 |
| Port Argument Operators in Service Objects | 30 |
| Service Objects with Source and Destination Ports | 31 |
| Example: Protocol Service Object Conversion | 32 |
| Example: TCP/UDP Service Object Conversion | 32 |
| Example: ICMP/ICMPv6 Service Object Conversion | 32 |
| Service Group Conversion | 33 |
| Nested Service Group Conversion | 34 |
| Example: Protocol Service Group Conversion | 35 |
| Example: TCP/UDP Service Group Conversion | 36 |
| Example: ICMP/ICMPv6 Service Group Conversion | 37 |
| Access-Group Conversion | 38 |

APPENDIX B
Conversion Examples 41

| | |
|----------|----|
| Examples | 41 |
|----------|----|



CHAPTER 1

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.

For an overview of the migration process, refer to the video at the following link: <https://www.youtube.com/watch?v=N06xXat59B0>.



Note

Beginning with release 6.5, Firepower Management Center does not support this ASA-to-Firepower Threat Defense Migration Tool. We recommend you to use Cisco's new Firepower Migration Tool.

- You can download the new tool from:
<https://www.cisco.com/c/en/us/products/security/firewalls/firepower-migration-tool.html>.
- For documentation on how to use the new migration tool, see [Migrating ASA to Firepower Threat Defense with the Firepower Migration Tool](#).

You can also use the new tool to migrate ASA devices to Firepower Threat Defense that are supported in Firepower Management Center release 6.2.3 and higher.

Firepower Management Center and Supported Migration Tools

The following table lists the migration tools that are supported in different versions of the Firepower Management Center:

| Firepower Management Center | ASA-to-Firepower Threat Defense Migration Tool | Firepower Migration Tool |
|--------------------------------|--|--------------------------|
| Versions 6.2, 6.2.1, and 6.2.2 | Yes | No |
| Versions 6.2.3 to 6.4 | Yes | Yes |
| Version 6.5 and above | No | Yes |

- [ASA-to-Firepower Threat Defense Migration Tool, on page 2](#)
- [ASA Device Requirements, on page 2](#)
- [Firepower Device Requirements, on page 3](#)
- [License Requirements, on page 4](#)
- [ASA Features Supported for Migration, on page 4](#)
- [Migration Limitations, on page 4](#)
- [Migration Checklist, on page 5](#)
- [Documentation Conventions, on page 6](#)

ASA-to-Firepower Threat Defense 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 FMC 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 FMC.

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 6.2.2

| Supported Platforms | Supported Environments |
|---------------------|---|
| Any | <p>For Version 6.2.1 and 6.2.2 migration tools:</p> <p>ASA Version 9.8/ASDM Version 7.8</p> <p>ASA Version 9.7/ASDM Version 7.7</p> <p>ASA Version 9.6/ASDM Version 7.6</p> <p>ASA Version 9.5/ASDM Version 7.5</p> <p>ASA Version 9.4/ASDM Version 7.4</p> <p>ASA Version 9.3/ASDM Version 7.3</p> <p>ASA Version 9.2/ASDM Version 7.2</p> <p>ASA Version 9.1/ASDM Version 7.1</p> <p>ASA Version 9.0/ASDM Version 7.0</p> <p>ASA Version 8.7/ASDM Version 6.7</p> <p>ASA Version 8.6/ASDM Version 6.6</p> <p>ASA Version 8.5/ASDM Version 6.5</p> <p>ASA Version 8.4/ASDM Version 6.4</p> |

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 the [Cisco Firepower 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, on page 15](#).

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 4](#).
- 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: <ul style="list-style-type: none"> • If you choose to convert access rules to access control rules, you also choose whether this value is Allow or Trust. • If you choose to convert access rules to prefilter rules, you also choose whether this value is Fastpath or Analyze. |
| 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. |



CHAPTER 2

Migrate an ASA Configuration to a Firepower Threat Defense Configuration

- [Prepare the ASA for Migration, on page 7](#)
- [Install the Migration Tool, on page 7](#)
- [Save the ASA Configuration File, on page 8](#)
- [Convert the ASA Configuration File, on page 8](#)
- [Import the Converted ASA Configuration, on page 10](#)
- [Install Firepower Threat Defense, on page 11](#)
- [Configure the Migrated Policies, on page 12](#)

Prepare the ASA for Migration

- Step 1** Verify that the ASA device meets the requirements for configuration migration; see [ASA Device Requirements, on page 2](#).
- Step 2** Identify the access control lists (ACLs) and NAT policies you want to export.
- Step 3** Prune as many inessential rules from the configuration as possible. Cisco recommends that you reduce the complexity and size of your ASA configuration as much as possible prior to conversion. To determine how many entries are present in the ACL:
- ```
show access-list acl_name | i elements
```

## 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#pgfld-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** Direct your browser to `https://hostname/`. The *hostname* element corresponds to the host name of the dedicated Firepower Management Center Virtual where you installed the migration tool.
- Step 2** Log in as the `admin` user.
- Step 3** Choose **System > Tools > Import/Export**
- Step 4** Click **Upload Package**.
- Step 5** Click **Browse**, and choose the configuration file you exported from the ASA.
- Step 6** Click **Next**.
- Step 7** 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 8** 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 9** 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 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 10](#).
- 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** Save the compressed files to your local computer, then unzip the files.
  - Step 9** Review the following files for error messages:
    - `dir-archives/var-log/action_queue.log.#.gz`
    - `dir-archives/var-log/mojo/mojo.log.#`
    - `dir-archives/var-opt-CSCOpX-MDC-log-operation/usmsharedsvcs.log`
    - `dir-archives/var-opt-CSCOpX-MDC-log-operation/vmsbesvcs.log`
    - `dir-archives/var-opt-CSCOpX-MDC-log-operation/vmssharedsvcs.log`
- 

## 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 <small>New . . .</small> 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 12](#).

**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 | <a href="http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/5500X/ftd-55xx-X-qsg.html">http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/5500X/ftd-55xx-X-qsg.html</a>               |
| Firepower 4100 Series with Threat Defense: 4110, 4120, and 4140                                                                                        | <a href="http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp4100/ftd-4100-qsg.html">http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp4100/ftd-4100-qsg.html</a>                 |
| Firepower 9300 with Threat Defense                                                                                                                     | <a href="http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp9300/ftd-9300-qsg.html">http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fp9300/ftd-9300-qsg.html</a>                 |
| Firepower Threat Defense Virtual: VMware                                                                                                               | <a href="http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-qsg.html">http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/vmware/ftdv/ftdv-vmware-qsg.html</a> |
| Firepower Threat Defense Virtual: AWS Cloud                                                                                                            | <a href="http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/aws/ftdv-aws-qsg.html">http://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/aws/ftdv-aws-qsg.html</a>                       |

## 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, on page 24](#).
- 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          |

- 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, on page 24](#).
- Optionally, configure the Firepower equivalents for ASA parameters that the tool does not convert:

| Access Rule Parameter   | Prefilter Rule Parameter |
|-------------------------|--------------------------|
| User                    | Selected Users condition |
| Security Group (Source) | custom SGT condition     |

- Configure the new access control policy that the system created during conversion, or associate the prefilter policy with a different access control policy.

**Warning** The migration tool sets the default action for the migrated access control policy to **Block All Traffic**, which is the equivalent of an implicit deny in an ACL. If you use a different access control policy with your migrated prefilter policy, consider setting its default action to **Block All Traffic**. Otherwise, you may create a security hole.

- 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 13](#).



## 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 **Filters** text box, and press Enter. Check or uncheck the check box to activate or deactivate the filter.
- Arrange—Place the mouse on a column heading to drag and drop the column in your preferred order.

**Step 3** Click **Deploy**.

**Step 4** If the system identifies errors or warnings in the changes to be deployed, it displays the details in the **Errors and Warnings for the Selected Deployment** window.

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.
-



# APPENDIX A

## Conversion Mapping

The following topics describe how the migration tool converts an ASA configuration to a Firepower Threat Defense configuration:

- [Conversion Mapping Overview, on page 15](#)
- [Naming Conventions for Converted Configurations, on page 16](#)
- [Fields Specific to Firepower Objects and Object Groups, on page 18](#)
- [Access Rule Conversion, on page 18](#)
- [NAT Rule Conversion, on page 25](#)
- [Network Object and Network Object Group Conversion, on page 27](#)
- [Service Object and Service Group Conversion, on page 29](#)
- [Access-Group Conversion, on page 38](#)

## Conversion Mapping Overview

The migration tool converts an ASA configuration into a Firepower Threat Defense configuration as follows:

**Table 3: Summary of Conversion Mapping**

| Entity          | ASA Configuration            | Firepower Threat Defense Configuration                                                            |
|-----------------|------------------------------|---------------------------------------------------------------------------------------------------|
| Network objects | Network objects              | Network objects                                                                                   |
|                 | Network object groups        | Network object groups                                                                             |
|                 | Nested network object groups | Nested network object groups                                                                      |
| Service objects | Service objects              | Multiple port objects                                                                             |
|                 | Service object groups        | Multiple port object groups                                                                       |
|                 | Nested service object groups | Multiple or flattened port object groups                                                          |
|                 |                              | For more information, see <a href="#">Service Object and Service Group Conversion, on page 29</a> |

| Entity       | ASA Configuration                           | Firepower Threat Defense Configuration                  |
|--------------|---------------------------------------------|---------------------------------------------------------|
| Access rules | Access rules                                | Access control policy or prefilter policy (as selected) |
| NAT rules    | Twice NAT rules<br>Network object NAT rules | Manual NAT rules<br>Auto NAT rules                      |

## Naming Conventions for Converted Configurations

The migration tool uses the naming conventions described below when converting ASA access rules, NAT rules, and related objects to Firepower Threat Defense equivalents.

### Object and Object Group Names

When converting objects and object groups, the migration tool retains the names of the objects and groups from the ASA configuration file.

For example:

```
object network obj1
 host 1.2.3.4
object network obj2
 range 1.2.3.7 1.2.3.10
 subnet 10.83.0.0 255.255.0.0
object-group network obj_group1
 network-object object obj1
 network-object object obj2
```

The tool converts this configuration to network objects named `obj1` and `obj2` and a network object group named `obj_group1`.

When converting service objects and service groups to port objects and port object groups, the tool can in certain cases append the following extensions to the original object or group name:

**Table 4: Extensions for Converted Service Objects and Groups**

| Extension         | Reason for Appending                                                                                                                                                                                                                                                                                  |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>_dst</code> | Splits a service object with source and destination ports into two port objects. The system appends this extension to the service object used to store the converted destination port data. For more information, see <a href="#">Service Objects with Source and Destination Ports, on page 31</a> . |
| <code>_src</code> | Splits a service object with source and destination ports into two port objects. The system appends this extension to the service object used to store the converted source port data. For more information, see .                                                                                    |
| <code>_#</code>   | Converts a nested service group; see <a href="#">Nested Service Group Conversion, on page 34</a> .                                                                                                                                                                                                    |

## Policy Names

The ASA configuration file contains a `hostname` parameter that specifies the host name for the ASA. The migration tool uses this value to name the policies it creates when converting the file:

- Access control policy—*hostname-AccessPolicy-conversion\_date*
- Prefilter policy—*hostname-PrefilterPolicy-conversion\_date*
- NAT policy—*hostname-NATPolicy-conversion\_date*

## Rule Names

For converted access control, prefilter, and NAT rules, the system names each new rule using the following format:

*ACL\_name-#rule\_index*

where:

- *ACL\_name*—The name of the ACL to which the rule belonged.
- *rule\_index*—A system-generated integer specifying the order in which the rule was converted relative to other rules in the ACL.

For example:

*acl1#1*

If the system must expand a single access rule to multiple rules during service object conversion, the system appends an extension:

*ACL\_name#rule\_index\_sub\_index*

where the appended # represents the position of the new rule in the expanded sequence.

For example:

*acl1#1\_1*

*acl1#1\_2*

If the system determines that the rule name is longer than 30 characters, the system shortens the ACL name and terminates the compressed name with a tilde (~):

*ACL Name~#rule index*

For example, if the original ACL name is `accesslist_for_outbound_traffic`, the system truncates the ACL name to:

*accesslist\_for\_outbound\_tr~#1*

## Security Zone and Interface Group Names

When the migration tool converts `access-group` commands in an ASA configuration file, the tool captures ingress and egress information in the command by creating either security zones or interface groups (depending on choices you make during conversion). It uses the following format to name these new security zones or interface groups:

*ACL\_name\_interface\_name\_direction\_keyword\_zone*

where:

- *ACL\_name*—The name of the ACL from the `access-group` command.
- *interface\_name*—The name of the interface from the `access-group` command.
- *direction\_keyword*—The direction keyword (`in` or `out`) from the `access-group` command.

For example:

```
access-list acpl permit tcp any host 209.165.201.3 eq 80
access-group acpl in interface outside
```

The tool converts this configuration to a security zone or interface group named `acpl_outside_in_zone`.

## Fields Specific to Firepower Objects and Object Groups

Firepower network and port objects/groups contain a small number of fields that are not present in ASA objects and groups. The migration tool populates these Firepower-specific fields in converted network and port objects/groups with the following default values:

**Table 5: Default Values for Fields Specific to Firepower Objects/Groups**

| Field in Firepower Objects/Groups | Default Value for Converted ASA Objects/Groups |
|-----------------------------------|------------------------------------------------|
| Domain                            | None                                           |
| Override                          | False                                          |

For more information on these default values, see [Documentation Conventions](#), on page 6.

## Access Rule Conversion

The migration tool can convert ASA access rules to either access control rules or prefilter rules, depending on choices you make during migration.

### Access Rule Conversion to Access Control Rules

If you choose to convert ASA access rules to Firepower Threat Defense access control rules:

- The system adds the converted rules to the **Default** rule section of the access control policy.
- The system retains Description field contents as an entry in the **Comment History** for the rule.
- The system adds an entry to the **Comment History**, identifying the rule as converted.
- The system sets the access control rule's **Action** as follows:

| Access Rule's Action | Access Control Rule's Action                                                     |
|----------------------|----------------------------------------------------------------------------------|
| <b>Permit</b>        | <b>Allow</b> or <b>Trust</b> , depending on the choice you make during migration |

| Access Rule's Action | Access Control Rule's Action |
|----------------------|------------------------------|
| Deny                 | Block                        |

- The system sets the access control rule's **Source Zones** and **Destination Zones** as follows:

| ACL Type                          | Source Zones                               | Destination Zones |
|-----------------------------------|--------------------------------------------|-------------------|
| Global (applied to Any interface) | Any                                        | Any               |
| Applied to specific interfaces    | The security zone you choose during import | Any               |

- If the access rule is inactive, the tool converts it to a disabled access control rule.

The migration tool assigns the converted rules to an access control policy with the following default parameters:

- The system sets the default action for the new access control policy to **Block All Traffic**.
- The system associates the access control policy with the default prefilter policy.

## Access Rule Fields Mapped to Access Control Rule Fields

The migration tool converts fields in ASA access rules to fields in Firepower Threat Defense access control rules as described in the table below.

Note:

- Field names in Column 1 (ASA Access Rule Field) correspond to field labels in the ASDM interface.
- Field names in Column 2 (Firepower Access Control Rule Field) correspond to field labels in the Firepower Management Center interface.

**Table 6: ASA Access Rule Fields Mapped to Firepower Access Control Rule Fields**

| ASA Access Rule Field        | Firepower Access Control Rule Field                                                    |
|------------------------------|----------------------------------------------------------------------------------------|
| Interface                    | No equivalent field                                                                    |
| Action                       | Action                                                                                 |
| Source                       | Source Networks                                                                        |
| User                         | Does not convert; equivalent to Selected Users condition                               |
| Security Group (Source)      | Does not convert; equivalent to custom SGT condition                                   |
| Destination                  | Destination Networks                                                                   |
| Security Group (Destination) | No equivalent field                                                                    |
| Service                      | Selected Destination Port; if predefined service object is specified, does not convert |

| ASA Access Rule Field        | Firepower Access Control Rule Field                                                                                                                                                                                                                                                                                                                       |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description                  | Comment                                                                                                                                                                                                                                                                                                                                                   |
| Enable Logging/Logging Level | Log at Beginning of Connection/Log at End of Connection. If logging is enabled in the ACE at a non-default logging level, the tool enables connection logging for the converted rule at both the beginning and end of the connection. If logging is enabled in the ACE at the default level, the tool disables connection logging for the converted rule. |
| Logging Interval             | No equivalent field                                                                                                                                                                                                                                                                                                                                       |
| Enable Rule                  | Enabled                                                                                                                                                                                                                                                                                                                                                   |
| Traffic Direction            | No equivalent field                                                                                                                                                                                                                                                                                                                                       |
| Source Service               | Selected Source Port; if predefined service object is specified, does not convert                                                                                                                                                                                                                                                                         |
| Time Range                   | No equivalent field                                                                                                                                                                                                                                                                                                                                       |

**Note**

If the ACE has the log option with a log level assigned, it is enabled. The ACE without a log level is considered as disabled. ACE log level is disabled if it is associated with a default log level.

## Fields Specific to Access Control Rules

Firepower Threat Defense access control rules contain a small number of fields that are not present in ASA access rules. The migration tool populates these Firepower-specific fields in converted access control rules with the following default values:

**Table 7: Default Values for Fields Specific to Access Control Rules**

| Access Control Rules Field | Default Value for Converted Access Rules                                                                                                                                                                |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                       | System-generated (see <a href="#">Naming Conventions for Converted Configurations</a> , on page 16)                                                                                                     |
| Source Zone                | <ul style="list-style-type: none"> <li>If the ACL is applied globally, Any</li> <li>If the ACL is applied to a specific interface, the Security Zone that the tool creates during conversion</li> </ul> |
| Destination Zone           | Any (default for all access control rules)                                                                                                                                                              |
| Selected VLAN Tags         | No default (you can manually add condition after import)                                                                                                                                                |



| Access Control Rules Field        | Default Value for Converted Access Rules                 |
|-----------------------------------|----------------------------------------------------------|
| Selected Applications and Filters | No default (you can manually add condition after import) |
| Selected URLs                     | No default (you can manually add condition after import) |

## Access Rule Conversion to Prefilter Rules

If you choose to convert ASA access rules to Firepower Threat Defense prefilter rules:

- The system retains the Description field contents as an entry in the **Comment History** for the rule.
- Adds an entry to the **Comment History** identifying the rule as converted.
- The system sets the prefilter rule's **Action** as follows:

| Access Rule's Action | Prefilter Rule's Action                                                               |
|----------------------|---------------------------------------------------------------------------------------|
| <b>Permit</b>        | <b>Fastpath</b> or <b>Analyze</b> , depending on the choice you make during migration |
| <b>Deny</b>          | <b>Block</b>                                                                          |

- The system sets the prefilter rule's **Source Interface Objects** and **Destination Interface Objects** as follows:

| ACL Type                                 | Source Interface Objects                     | Destination Interface Objects |
|------------------------------------------|----------------------------------------------|-------------------------------|
| Global (applied to <i>Any</i> interface) | <i>Any</i>                                   | <i>Any</i>                    |
| Applied to specific interfaces           | The interface group you choose during import | <i>Any</i>                    |

- If the access rule is inactive, the tool converts it to a disabled prefilter rule.

The migration tool assigns the converted rules to a prefilter policy with the following default parameters:

- The system sets the default action for the new prefilter policy to **Analyze All Tunnel Traffic**.
- The system creates an access control policy with the same name as the prefilter policy, and then associates the prefilter policy with that access control policy. The system sets the default action for the new access control policy to **Block All Traffic**.

## Access Rule Fields Mapped to Prefilter Rule Fields

The migration tool converts fields in ASA access rules to fields in Firepower Threat Defense prefilter rules as described in the table below.

Note:

- Field names in Column 1 (ASA Access Rule Field) correspond to field labels in the ASDM interface.

- Field names in Column 2 (Firepower Prefilter Rule Field) correspond to field labels in the Firepower Management Center interface.

**Table 8: ASA Access Rule Fields Mapped to Firepower Prefilter Rule Fields**

| ASA Access Rule Field        | Firepower Prefilter Rule Field                                                                                                                                                                                                                                                                                                                            |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface                    | No equivalent field                                                                                                                                                                                                                                                                                                                                       |
| Enable Rule                  | Enabled                                                                                                                                                                                                                                                                                                                                                   |
| Action                       | Action                                                                                                                                                                                                                                                                                                                                                    |
| Source                       | Source Networks                                                                                                                                                                                                                                                                                                                                           |
| User                         | No equivalent field                                                                                                                                                                                                                                                                                                                                       |
| Security Group (Source)      | No equivalent field                                                                                                                                                                                                                                                                                                                                       |
| Destination                  | Destination Networks                                                                                                                                                                                                                                                                                                                                      |
| Security Group (Destination) | No equivalent field                                                                                                                                                                                                                                                                                                                                       |
| Service                      | Selected Source Port<br>Selected Destination Port                                                                                                                                                                                                                                                                                                         |
| Description                  | Comment                                                                                                                                                                                                                                                                                                                                                   |
| Enable Logging/Logging Level | Log at Beginning of Connection/Log at End of Connection. If logging is enabled in the ACE at a non-default logging level, the tool enables connection logging for the converted rule at both the beginning and end of the connection. If logging is enabled in the ACE at the default level, the tool disables connection logging for the converted rule. |
| Logging Interval             | No equivalent field                                                                                                                                                                                                                                                                                                                                       |
| Traffic Direction            | No equivalent field                                                                                                                                                                                                                                                                                                                                       |
| Source Service               | Selected Source Port; if predefined service object is specified, does not convert                                                                                                                                                                                                                                                                         |
| Time Range                   | No equivalent field                                                                                                                                                                                                                                                                                                                                       |

## Fields Specific to Firepower Prefilter Rules

Firepower Threat Defense prefilter rules contain a small number of fields that are not present in ASA access rules. The migration tool populates these Firepower-specific fields in converted prefilter rules with the following default values:

Table 9: Default Values for Fields Specific to Firepower Prefilter Rules

| Prefilter Rule Field          | Default Value for Converted Access Rules                                                                                                                                                                                   |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                          | System-generated (see <a href="#">Naming Conventions for Converted Configurations</a> , on page 16)                                                                                                                        |
| Source Interface Objects      | <ul style="list-style-type: none"> <li>• If the ACL is applied globally, <code>Any</code></li> <li>• If the ACL is applied to a specific interface, the Interface Group that the tool creates during conversion</li> </ul> |
| Destination Interface Objects | <code>Any</code> (default for all prefilter rules)                                                                                                                                                                         |
| Selected VLAN Tags            | No default (you can manually add condition after import)                                                                                                                                                                   |

## Port Argument Operators in Access Rules

An extended access rule can contain a `port_argument` element that uses the same operators used in service objects. The migration tool converts these operators in access rules slightly differently than it does the same operators when it converts service objects, depending on whether the access rule contains a single port argument operator or multiple port argument operators.

The following table lists the possible operators and gives an example of single operator use.

Table 10: Port Argument Operators in Access Rules

| Operator           | Description                                                                                                     | Example                                                                |
|--------------------|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| <code>lt</code>    | Less than.                                                                                                      | <code>access-list acp1 extended permit tcp any lt 300</code>           |
| <code>gt</code>    | Greater than.                                                                                                   | <code>access-list acp2 extended permit tcp any gt 300</code>           |
| <code>eq</code>    | Equal to.                                                                                                       | <code>access-list acp3 extended permit tcp any eq 300</code>           |
| <code>neq</code>   | Not equal to.                                                                                                   | <code>access-list acp4 extended permit tcp any neq 300</code>          |
| <code>range</code> | An inclusive range of values. When you use this operator, specify two port numbers, for example, range 100 200. | <code>access-list acp5 extended permit tcp any range 9000 12000</code> |

If the access rule contains a single port argument operator, the migration tool converts the access rule to a single access control or prefilter rule, as follows:

Table 11: Access Rules with Single Port Argument Operators Converted to Access Control or Prefilter Rules

| Op    | Name   | Src Zone | Dest Zone | Src Network | Dest Network | Src Port            | Dest Port | Action            | Enabled |
|-------|--------|----------|-----------|-------------|--------------|---------------------|-----------|-------------------|---------|
| lt    | acp1#1 | Any      | Any       | Any         | Any          | 1-299               | Any       | Permit equivalent | True    |
| gt    | acp2#1 | Any      | Any       | Any         | Any          | 301-65535           | Any       | Permit equivalent | True    |
| eq    | acp3#1 | Any      | Any       | Any         | Any          | 300                 | Any       | Permit equivalent | True    |
| neq   | acp4#1 | Any      | Any       | Any         | Any          | 1-299,<br>301-65535 | Any       | Permit equivalent | True    |
| range | acp5#1 | Any      | Any       | Any         | Any          | 9000-2000           | Any       | Permit equivalent | True    |

The Original Operator (**Op**) column in this table is provided for clarity; it does not represent a field in the access control rule.

If an access rule contains multiple port operators (for example, `access-list acp6 extended permit tcp any neq 300 any neq 400`), the migration tool converts the single access rule to multiple access control or prefilter rules, as follows:

Table 12: Access Rules with Multiple Port Argument Operators Converted to Access Control Rules

| Op  | Name     | Src Zone | Dest Zone | Src Network | Dest Network | Src Port  | Dest Port | Action            | Enabled |
|-----|----------|----------|-----------|-------------|--------------|-----------|-----------|-------------------|---------|
| neq | acp6#1_1 | Any      | Any       | Any         | Any          | 1-299     | 1-399     | Permit equivalent | True    |
| neq | acp6#1_2 | Any      | Any       | Any         | Any          | 301-65535 | 1-399     | Permit equivalent | True    |
| neq | acp6#1_3 | Any      | Any       | Any         | Any          | 1-299     | 401-65535 | Permit equivalent | True    |
| neq | acp6#1_4 | Any      | Any       | Any         | Any          | 301-65535 | 401-65535 | Permit equivalent | True    |

The Original Operator (**Op**) column in this table is provided for clarity; it does not represent a field in the access control rule.

## Access Rules that Specify Multiple Protocols

In ASA, you can configure source and destination ports in access rules to use protocol service objects that specify multiple protocols (for example, TCP and UDP). For example:

```
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
access-list acp1 extended permit object-group TCPUDP any any
```

In the Firepower System, however, you can only configure access control or prefilter rules as follows:

- Both source and destination ports must specify the same protocol.
- The destination port can specify multiple protocols, but the source port must specify none.

Access rules that contain protocol object groups tcp and udp are migrated as unsupported rules. And therefore the rule is disabled with a comment **Object Group Protocol containing both tcp and udp is not supported.**

## NAT Rule Conversion

NAT for ASA and NAT for Firepower Threat Defense support equivalent functionality, as summarized in the table below.

*Table 13: ASA NAT Policies Mapped to Firepower Threat Defense NAT Policies*

| ASA NAT Policy     | Firepower Threat Defense NAT Policy | Defining Characteristics                                                                                                                                                                                                                                                         |
|--------------------|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Twice NAT          | Manual NAT                          | <ul style="list-style-type: none"> <li>• Specifies both the source and destination address in a single rule.</li> <li>• Configured directly.</li> <li>• Can use network object groups.</li> <li>• Manually ordered in the NAT table (before or after auto NAT rules).</li> </ul> |
| Network object NAT | Auto NAT                            | <ul style="list-style-type: none"> <li>• Specifies either a source or a destination address.</li> <li>• Configured as a parameter of a network object.</li> <li>• Cannot use network object groups.</li> <li>• Automatically ordered in the NAT table.</li> </ul>                |

The migration tool converts ASA NAT configurations to Firepower Threat Defense NAT configurations. However, the tool cannot convert ASA NAT configurations that use unsupported network objects; in such cases, the conversion fails.

## ASA NAT Rule Fields Mapped to Firepower Threat Defense Rule Fields

The migration tool converts fields in ASA NAT rules to fields in Firepower Threat Defense NAT rules as described in the table below.

Note:

- Field names in Column 1 (ASA NAT Rule Field) correspond to field labels in the ASDM interface.
- Field names in Column 2 (Firepower Threat Defense Rule Field) correspond to field labels in the Firepower Management Center interface.

Table 14: ASA NAT Rule Fields Mapped to Firepower Threat Defense NAT Rule Fields

| ASA NAT Rule Field                                                | Firepower Threat Defense Rule Field                                                                       |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Original Packet - Source Interface                                | Interface Objects - Source Interface Objects                                                              |
| Original Packet - Source Address                                  | Original Packet - Original Source                                                                         |
| Original Packet - Destination Interface                           | Interface Objects - Destination Interface Objects                                                         |
| Original Packet - Destination Address                             | Original Packet - Original Destination - Address Type<br>Original Packet - Original Destination - Network |
| Original Packet - Service                                         | Original Packet - Original Source Port<br>Original Packet - Original Destination Port                     |
| Translated Packet - Source NAT Type                               | Type                                                                                                      |
| Translated Packet - Source Address                                | Translated Packet - Translated Source - Address Type<br>Translated Packet - Translated Source - Network   |
| Translated Packet - Destination Address                           | Translated Packet - Translated Destination                                                                |
| Translated Packet - Service                                       | Translated Packet - Translated Source Port<br>Translated Packet - Translated Destination Port             |
| Use one-to-one address translation                                | Advanced - Net to Net Mapping                                                                             |
| PAT Pool Translated Address                                       | PAT Pool - PAT - Address Type<br>PAT Pool - PAT - Network                                                 |
| Round Robin                                                       | PAT Pool - Use Round Robin Allocation                                                                     |
| Extend PAT uniqueness to per destination instead of per interface | PAT Pool - Extended PAT Table                                                                             |
| Translate TCP and UDP ports into flat range 1024-65535            | PAT Pool - Flat Port Range                                                                                |
| Include range 1-1023                                              | PAT Pool - Include Reserve Ports                                                                          |
| Enable Block Allocation                                           | No equivalent                                                                                             |
| Use IPv6 for source interface PAT                                 | No equivalent                                                                                             |
| Use IPv6 for destination interface PAT                            | Advanced - IPv6                                                                                           |
| Enable rule                                                       | Enable                                                                                                    |
| Translate DNS replies that match this rule                        | Advanced - Translate DNS replies that match this rule                                                     |
| Disable Proxy ARP on egress interface                             | Advanced - Do not proxy ARP on Destination Interface                                                      |

| ASA NAT Rule Field                            | Firepower Threat Defense Rule Field |
|-----------------------------------------------|-------------------------------------|
| Lookup route table to locate egress interface | No equivalent                       |
| Direction                                     | Advanced - Unidirectional           |
| Description                                   | Description                         |

## Network Object and Network Object Group Conversion

Network objects and network object groups identify IP addresses or host names. In both ASA and Firepower Threat Defense, these objects and groups can be used in both access and NAT rules.

In ASA, a network object can contain a host, a network IP address, a range of IP addresses, or a fully qualified domain name (FQDN). In the Firepower System, network objects support these same values with the exception of FQDN.

The migration tool converts an ASA network object or group once, regardless of whether the object is used in multiple access or NAT rules.

### Network Object Conversion

For each ASA network object it converts, the migration tool creates a Firepower network object.

The migration tool converts fields in ASA network objects to fields in Firepower network objects as follows:

**Table 15: ASA Network Object Fields Mapped to Firepower Network Object Fields**

| ASA Network Object Field | Firepower Network Object Field                                                                     |
|--------------------------|----------------------------------------------------------------------------------------------------|
| Name                     | System-generated; see <a href="#">Naming Conventions for Converted Configurations</a> , on page 16 |
| Type                     | Type                                                                                               |
| IP Version               | No equivalent field                                                                                |
| IP Address               | Value                                                                                              |
| Netmask                  | Value (included in CIDR notation)                                                                  |
| Description              | Description                                                                                        |
| Object NAT Address       | No equivalent field                                                                                |

#### Example: Network Object in an Access Control List

If the following commands are present in the ASA configuration file:

```
object network obj1
 host 1.2.3.4
object network obj2
 range 1.2.3.7 1.2.3.10
```

```

object network obj3
 subnet 10.83.0.0 255.255.0.0
access-list sample_acl extended permit ip object obj1 object obj2
access-list sample_acl extended permit ip object obj3 object obj1
access-group gigabitethernet_access_in in interface gigabitethernet1/1

```

The system converts these objects as follows:

| Name | Domain | Value (Network)  | Type          | Override |
|------|--------|------------------|---------------|----------|
| obj1 | None   | 1.2.3.4          | Host          | False    |
| obj2 | None   | 1.2.3.7-1.2.3.10 | Address Range | False    |
| obj3 | None   | 10.83.0.0/16     | Network       | False    |

### Example: Network Object in a NAT Rule

If the following command is present in the ASA configuration file:

```

nat (gigabitethernet1/1,gigabitethernet1/2) source static obj1 obj1

```

The system converts object `obj1` in this rule the same way it converts object `obj1` in the access rule example above.

## Network Object Group Conversion

For each ASA network object group it converts, the migration tool creates a Firepower network object group. It also converts the objects contained in the group, if they have not already been converted.

The migration tool converts fields in ASA network object groups to fields in Firepower network object groups as follows:

**Table 16: ASA Network Object Group Fields Mapped to Firepower Network Object Group Fields**

| ASA Network Object Group Field | Firepower Network Object Group Field |
|--------------------------------|--------------------------------------|
| Group Name                     | Name                                 |
| Description                    | Description                          |
| Members in Group               | Value (Selected Networks)            |

### Example: Network Object Group in an Access Control List

If the following commands are present in the ASA configuration file:

```

object network obj1
 host 1.2.3.4
object network obj2
 range 1.2.3.7 1.2.3.10
object network obj3
 subnet 10.83.0.0 255.255.0.0
object-group network obj_group1
 network-object object obj1
 network-object object obj2
 network-object object obj3

```



```
access-list sample_acl extended permit ip object-group obj_group1 any
access-group gigabitethernet_access_in in interface gigabitethernet1/1
```

The system creates the following network group:

| Name       | Domain | Value (Networks)     | Type  | Override |
|------------|--------|----------------------|-------|----------|
| obj_group1 | None   | obj1<br>obj2<br>obj3 | Group | False    |

If the associated objects have not already been converted, the system converts them objects as described in [Network Object Conversion, on page 27](#).

#### Example: Network Object Group in a NAT Rule

If the following command is present in the ASA configuration file:

```
nat (interface1,interface2) source static obj_group1 obj_group1
```

The system converts `obj_group1` in this rule the same way it converts `obj_group1` in the access rule example above.

## Service Object and Service Group Conversion

In ASA, service objects and service groups specify protocols and ports and designate those ports as source or destination ports. Service objects and groups can be used in both access and NAT rules.

In the Firepower System, port objects and port object groups specify protocols and ports, but the system designates those ports as source or destination ports only if you add the objects to access control, prefilter, or NAT rules. To convert service objects to equivalent functionality in the Firepower System, the migration tool converts service objects to port objects or groups and makes specific changes to related access control, prefilter, or NAT rules. As a result, during conversion, the migration tool might expand single service object/service group and related access or NAT rules into multiple port objects/groups and related access control, prefilter, or NAT rules.

## Service Object Conversion

The migration tool converts an ASA service object by creating one or more port objects and one or more access control or prefilter rules that reference those port objects.

The migration tool can convert the following service object types:

- Protocol
- TCP/UDP
- ICMP/ICMPv6

The migration tool converts fields in ASA service objects to fields in Firepower port objects as follows:

Table 17: ASA Service Object Fields Mapped to Firepower Port Object Fields

| ASA Service Object Field | ASA Service Object Type | Firepower Port Object Field                                                                         |
|--------------------------|-------------------------|-----------------------------------------------------------------------------------------------------|
| Name                     | Any                     | System-generated (see <a href="#">Naming Conventions for Converted Configurations, on page 16</a> ) |
| Service Type             | TCP/UDP, ICMP/ICMPv6    | Protocol                                                                                            |
| Protocol                 | Protocol only           | Protocol                                                                                            |
| Description              | Any                     | No equivalent; content is discarded                                                                 |
| Destination Port/Range   | TCP/UDP only            | Port                                                                                                |
| Source Port/Range        | TCP/UDP only            | Port                                                                                                |
| ICMP Type                | ICMP/ICMPv6 only        | Type                                                                                                |
| ICMP Code                | ICMP/ICMPv6 only        | Code                                                                                                |

## Port Literal Values in Service Objects

ASA service objects can specify port literal values, instead of port numbers. For example:

```
object service http
 service tcp destination eq www
```

Because the Firepower System does not support these port literal values, the migration tool converts the port literal values to the port numbers they represent. The tool converts the above example to the following port object:

| Name | Type   | Domain | Value (Protocol/Port) | Override |
|------|--------|--------|-----------------------|----------|
| http | Object | None   | TCP(6)/80             | False    |

For a full list of port literal values and associated port numbers, see TCP and UDP Ports in *CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide*.

## Port Argument Operators in Service Objects

ASA service objects can use the following operators in port arguments:

Table 18: Port Argument Operators in Service Objects

| Operator | Description   | Example                                                  |
|----------|---------------|----------------------------------------------------------|
| lt       | Less than.    | object service testOperator<br>service tcp source lt 100 |
| gt       | Greater than. | object service testOperator<br>service tcp source gt 100 |
| eq       | Equal to.     | object service http-proxy<br>service tcp source eq 8080  |

| Operator | Description                   | Example                                                          |
|----------|-------------------------------|------------------------------------------------------------------|
| neq      | Not equal to.                 | object service testOperator<br>service tcp source neq 200        |
| range    | An inclusive range of values. | object service http-proxy<br>service tcp source range 9000 12000 |

The migration tool converts these operators as follows:

**Table 19: Service Objects with Port Argument Operators Converted to Port Objects/Groups**

| Operator | Converts to                                                                                                                                                                                                                                 | Example Port Object Value (Protocol/Port)                                                                                                                                                     |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lt       | A single port object that specifies a range of port numbers less than the specified number.                                                                                                                                                 | TCP(6)/1-99                                                                                                                                                                                   |
| gt       | A single port object that specifies a range of port numbers greater than the specified number.                                                                                                                                              | TCP(6)/101-65535                                                                                                                                                                              |
| eq       | A single port object that specifies a single port number.                                                                                                                                                                                   | TCP(6)/8080                                                                                                                                                                                   |
| neq      | Two port objects and a port object group. The first port object specifies a range lower than the specified port. The second port object specifies a range higher than the specified port. The port object group includes both port objects. | First object (testOperator_src_1):<br>TCP(6)/1-199<br>Second object (testOperator_src_2):<br>TCP(6)/201-65535<br>Object group (testOperator_src):<br>testOperator_src_1<br>testOperator_src_2 |
| range    | A single port object that specifies an inclusive range of values.                                                                                                                                                                           | TCP(6)/9000-12000                                                                                                                                                                             |

## Service Objects with Source and Destination Ports

In ASA, a single service object can specify ports for both source and destination. In the Firepower System, the port object specifies port values only. The system does not designate the port as source or destination until you use the port object in an access control or prefilter rule.

To accommodate this difference, when the migration tool converts an ASA service object that specifies both source and destination, it expands the single object into two port objects. It appends an extension to the object names to indicate their original designations, *\_src* for source ports and *\_dst* for destination ports.

### Example

```
object service http-proxy
service tcp source range 9000 12000 destination eq 8080
```

The tool converts this service object into the following port objects:

| Name           | Type   | Domain | Value (Protocol/Port) | Override |
|----------------|--------|--------|-----------------------|----------|
| http-proxy_src | Object | None   | TCP(6)/9000-12000     | False    |

| Name           | Type   | Domain | Value (Protocol/Port) | Override |
|----------------|--------|--------|-----------------------|----------|
| http-proxy_dst | Object | None   | TCP(6)/8080           | False    |

## Example: Protocol Service Object Conversion

ASA Configuration:

```
object service protocolObj1
 service snp
 description simple routing
```

Converts to:

**Table 20: Port Object**

| Name         | Type   | Domain | Value (Protocol) | Override |
|--------------|--------|--------|------------------|----------|
| protocolObj1 | Object | None   | SNP (109)        | False    |

## Example: TCP/UDP Service Object Conversion

ASA configuration:

```
object service servObj1
 service tcp destination eq ssh
```

Converts to:

**Table 21: Port Object**

| Name     | Type   | Domain | Value (Protocol/Port) | Override |
|----------|--------|--------|-----------------------|----------|
| servObj1 | Object | None   | TCP(6)/22             | False    |

## Example: ICMP/ICMPv6 Service Object Conversion

### ICMP

ASA configuration:

```
object service servObj1
 service icmp alternate-address 0
```

Converts to:

Table 22: Port Object

| Name     | Type   | Domain | Value (Protocol/Type:Code)                                    | Override |
|----------|--------|--------|---------------------------------------------------------------|----------|
| servObj1 | Object | None   | ICMP(1)/Alternate Host Address:<br>Alternate Address for Host | False    |

**ICMPv6**

ASA configuration:

```
object service servObj1
 service icmp6 unreachable 0
```

Converts to:

Table 23: Port Object

| Name     | Type   | Domain | Value (Protocol/Type:Code)                                     | Override |
|----------|--------|--------|----------------------------------------------------------------|----------|
| servObj1 | Object | None   | IPV6-ICMP (58)/Destination Unreachable:no route to destination | False    |

## Service Group Conversion

The migration tool converts an ASA service group by creating port object groups and associating those port object groups with the related access control or prefilter rules.

The migration tool can convert the following service group types:

- Protocol
- TCP/UDP
- ICMP/ICMPv6

The migration tool converts fields in ASA service objects to fields in Firepower port objects as follows:

Table 24: ASA Service Group Fields Mapped to Firepower Port Object Fields

| ASA Service Group Field | Port Object Group Field                                                                             |
|-------------------------|-----------------------------------------------------------------------------------------------------|
| Name                    | System-generated (see <a href="#">Naming Conventions for Converted Configurations</a> , on page 16) |
| Description             | Description                                                                                         |
| Members in Group        | Selected Ports                                                                                      |

## Nested Service Group Conversion

ASA supports nested service groups (that is, service groups that contain other service groups). The Firepower System does not support nested port object groups; however, you can achieve equivalent functionality by associating multiple groups with a single access control or prefilter rule. When converting nested service groups, the migration tool "flattens" the group structure, converting the innermost service objects and groups to port objects and port object groups, and associating those converted groups with access control or prefilter rules.

You can associate up to 50 port objects with a single access control or prefilter rule. If the number of new port objects exceeds 50, the tool creates duplicate access control or prefilter rules until it has associated all of the new port objects with a rule.

The Firepower system rules containing nested service objects that are used as both source and destination services are not supported.

### Example

```
object-group service http-8081 tcp
 port-object eq 80
 port-object eq 81

object-group service http-proxy tcp
 port-object eq 8080

object-group service all-http tcp
 group-object http-8081
 group-object http-proxy

access-list FMC_inside extended permit tcp host 33.33.33.33 object-group all-http host
33.33.33.33 object-group all-http
```

In the example above, service objects *http-8081* and *http-proxy* are nested within the *all-http* service group.

In such a scenario, the rules pertaining to the port objects are ignored. The system imports the objects but disables the related access control or prefilter rule, and adds the following comment to the rule: **Nested service groups at both Source and Destination are not supported.**

For a description of the naming conventions the tool uses for converted service objects, service groups, and any duplicate rules the system might create during their conversion, see [Naming Conventions for Converted Configurations, on page 16](#)

### Example

ASA configuration:

```
object-group service legServGroup1 tcp
 port-object eq 78
 port-object eq 79
object-group service legServGroup2 tcp
 port-object eq 80
 port-object eq 81
object-group service legacyServiceNestedGrp tcp
 group-object legServGroup1
 group-object legServGroup2
access-list acpl extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0
object-group legacyServiceNestedGrp
access-group acpl global
```

Converts to:

Table 25: Port Object Groups

| Name            | Type   | Domain | Value (Protocol/Port)              | Override |
|-----------------|--------|--------|------------------------------------|----------|
| legServGroup1_1 | Object | None   | TCP(6)/78                          | False    |
| legServGroup1_2 | Object | None   | TCP(6)/79                          | False    |
| legServGroup2_1 | Object | None   | TCP(6)/80                          | False    |
| legServGroup2_2 | Object | None   | TCP(6)/81                          | False    |
| legServGroup1   | Group  | None   | legServGroup1_1<br>legServGroup1_2 | False    |
| legServGroup2   | Group  | None   | legServGroup2_1<br>legServGroup2_2 | False    |

Table 26: Access Control or Prefilter Rule

| Name   | Src Zone | Dest Zone | Src Network | Dest Network | Src Port | Dest Port                      | Action            | Enabled |
|--------|----------|-----------|-------------|--------------|----------|--------------------------------|-------------------|---------|
| acp1#1 | Any      | Any       | 3.4.5.0/24  | 5.6.7.0/24   | TCP(6)   | legServGroup1<br>legServGroup2 | Permit equivalent | True    |

## Example: Protocol Service Group Conversion

ASA configuration:

```
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
```

Converts to:

Table 27: Port Objects and Groups

| Name     | Type   | Domain | Value (Protocol/Port) | Override |
|----------|--------|--------|-----------------------|----------|
| TCPUDP_1 | Object | None   | TCP(6)                | False    |
| TCPUDP_2 | Object | None   | UDP(17)               | False    |
| TCPUDP   | Group  | None   | TCPUDP_1<br>TCPUDP_2  | False    |

## Example: TCP/UDP Service Group Conversion

### Objects Created During Group Creation

In ASA, you can create objects on-the-fly during service group creation. These objects are categorized as service objects, but the entry in the ASA configuration file uses `port-object` instead of `object service`. Because these objects are not independently created, the migration tool uses a slightly different naming convention than it does for objects created independently of group creation.

ASA configuration:

```
object-group service servGrp5 tcp-udp
 port-object eq 50
 port-object eq 55
```

Converts to:

**Table 28: Port Objects and Groups**

| Name       | Type   | Domain | Value (Protocol/Port)    | Override |
|------------|--------|--------|--------------------------|----------|
| servGrp5_1 | Object | None   | TCP(6)/50                | False    |
| servGrp5_2 | Object | None   | TCP(6)/55                | False    |
| servGrp5   | Group  | None   | servGrp5_1<br>servGrp5_2 | False    |

### Objects Created Independently from Group

ASA configuration:

```
object service servObj1
 service tcp destination eq ssh
object service servObj2
 service udp destination eq 22
object service servObj3
 service tcp destination eq telnet
object-group service servGrp1
 service-object object servObj1
 service-object object servObj2
 service-object object servObj3
```

Converts to:

**Table 29: Port Objects and Groups**

| Name     | Type   | Domain | Value (Protocol/Port) | Override |
|----------|--------|--------|-----------------------|----------|
| servObj1 | Object | None   | TCP(6)/22             | False    |
| servObj2 | Object | None   | UDP(17)/22            | False    |
| servObj3 | Object | None   | TCP(6)/23             | False    |



| Name     | Type  | Domain | Value (Protocol/Port)            | Override |
|----------|-------|--------|----------------------------------|----------|
| servGrp1 | Group | None   | servObj1<br>servObj2<br>servObj3 | False    |

## Example: ICMP/ICMPv6 Service Group Conversion

### ICMP

ASA configuration:

```
object-group icmp-type servGrp4
 icmp-object echo-reply
```

Converts to:

**Table 30: Port Objects and Groups**

| Name       | Type   | Domain | Value (Protocol/Port) | Override |
|------------|--------|--------|-----------------------|----------|
| servGrp4_1 | Object | None   | ICMP(1)/Echo Reply    | False    |
| servGrp4   | Group  | None   | servGrp4_1            | False    |

### ICMPv6

ASA configuration:

```
object-group service servObjGrp3
 service-object icmp6 packet-too-big
 service-object icmp6 parameter-problem
```

Converts to:

**Table 31: Port Objects and Groups**

| Name          | Type   | Domain | Value (Protocol/Port)          | Override |
|---------------|--------|--------|--------------------------------|----------|
| servObjGrp3_1 | Object | None   | IPV6-ICMP(58)/2                | False    |
| servObjGrp3_2 | Object | None   | IPV6-ICMP(58)/4                | False    |
| servObjGrp3   | Group  | None   | servObjGrp3_1<br>servObjGrp3_2 | False    |

# Access-Group Conversion

In ASA, to apply an ACL, you enter the `access-group` command in the CLI, or you choose **Apply** in the ASDM access rule editor. Both of these actions result in an `access-group` entry in the ASA configuration file (see example below).

The `access-group` command specifies the interface where the system applies the ACL and whether the system applies the ACL to inbound (ingress) or outbound (egress) traffic on that interface.

In the Firepower System, to configure equivalent functionality, you:

- Create a security zone, associate the security zone with an interface, and add the security zone to access control rules as either a Source Zone condition (for inbound traffic) or a Destination Zone condition (for outbound traffic).
- Create an interface group, associate the interface group with an interface, and add the interface group to prefilter rules as either a Source Interface Group condition (for inbound traffic) or a Destination Interface Group condition (for outbound traffic).

When converting the `access-group` command, the migration tool captures ingress and egress information by creating either security zones or interface groups and adding the security zones and interface groups as conditions in the related access control or prefilter rules. However, the migration tool retains the interface information in the name of the security zone or interface group, but it does not convert any related interface or device configurations, which you must add manually after importing the converted policies. After importing the converted policies, you must associate the policies manually with devices, and security zones or interface groups with interfaces.

When converting ACLs, the system positions globally-applied rules *after* rules applied to specific interfaces.

## Special Cases

If the ASA configuration applies a single ACL to both ingress and egress interfaces, the tool converts the ACL to two sets of access control or prefilter rules:

- a set of ingress rules (enabled)
- a set of egress rules (disabled)

If the ASA configuration applies a single ACL both globally and to a specific interface, the tool converts the ACL to two sets of access control or prefilter rules:

- a set of rules associated with the specific interface (enabled)
- a set of rules with source and destination zone set to `Any` (enabled)

## Example: ACL Applied Globally

ASA configuration:

```
access-list global_access extended permit ip any any
access-group global_access global
```

The migration tool converts this configuration to:

Table 32: Access Control or Prefilter Rule

| Name            | Src Zone/Int Grp | Dest Zone/Int Grp | Src Network | Dest Network | Src Port | Dest Port | Action            | Enabled |
|-----------------|------------------|-------------------|-------------|--------------|----------|-----------|-------------------|---------|
| global_access#1 | Any              | Any               | Any         | Any          | Any      | Any       | Permit equivalent | True    |

**Example: ACL Applied to Specific Interface**

ASA configuration:

```
access-list acpl permit tcp any host 209.165.201.3 eq 80
access-group acpl in interface outside
```

In this example, the `access-group` command applies the ACL named `acpl` to inbound traffic on the interface named `outside`.

The migration tool converts this configuration to:

Table 33: Security Zone/Interface Group

| Name                 | Interface Type                                                                                                                                                          | Domain | Selected Interfaces |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---------------------|
| acpl_outside_in_zone | <ul style="list-style-type: none"> <li>• Routed (if ASA device is running in routed mode)</li> <li>• Switched (if ASA device is running in transparent mode)</li> </ul> | None   | Any                 |

Table 34: Access Control or Prefilter Rule

| Name   | Src Zone/Int Grp     | Dest Zone/Int Grp | Src Network | Dest Network  | Src Port | Dest Port | Action            | Enabled |
|--------|----------------------|-------------------|-------------|---------------|----------|-----------|-------------------|---------|
| acpl#1 | acpl_outside_in_zone | Any               | Any         | 209.165.201.3 | Any      | TCP(6)/80 | Permit equivalent | True    |





## APPENDIX B

# Conversion Examples

This section contains examples of ASA configurations and the Firepower Threat Defense rules and objects to which the migration tool converts them.

- [Examples, on page 41](#)

## Examples

### Access Rule Specifying Individual Networks

ASA configuration:

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0
access-group acp1 global
```

Converts to:

**Table 35: Access Control or Prefilter Rule**

| Name   | Source Zone | Destination Zone | Source Network | Destination Network | Source Port | Destination Port | Action            | Enabled |
|--------|-------------|------------------|----------------|---------------------|-------------|------------------|-------------------|---------|
| acp1#1 | Any         | Any              | 3.4.5.0/24     | 5.6.7.0/24          | TCP(6)      | Any              | Permit equivalent | True    |

### Access Rule with Network Object Groups

ASA configuration:

```
access-list acp1 extended permit ip object-group host1 object-group host2
access-group acp1 global
```

Converts to:

**Table 36: Network Object Groups**

| Name  | Domain | Value (Network) | Type  | Override |
|-------|--------|-----------------|-------|----------|
| host1 | None   | obj1<br>obj2    | Group | False    |

| Name  | Domain | Value (Network) | Type  | Override |
|-------|--------|-----------------|-------|----------|
| host2 | None   | obj3<br>obj4    | Group | False    |

Table 37: Access Rule Using Network Object Groups

| Name   | Source Zone | Destination Zone | Source Network | Destination Network | Source Port | Destination Port | Action            | Enabled |
|--------|-------------|------------------|----------------|---------------------|-------------|------------------|-------------------|---------|
| acpl#1 | Any         | Any              | host1          | host2               | Any         | Any              | Permit equivalent | True    |

### Access Rule Specifying Individual Networks and Ports

ASA access rule:

```
access-list acpl extended permit tcp 3.4.5.0 255.255.255.0 eq 90 5.6.7.0 255.255.255.0 eq 80
access-group acpl global
```

Converts to:

Table 38: Access Control or Prefilter Rule

| Name   | Source Zone | Destination Zone | Source Network | Destination Network | Source Port | Destination Port | Action            | Enabled |
|--------|-------------|------------------|----------------|---------------------|-------------|------------------|-------------------|---------|
| acpl#1 | Any         | Any              | 3.4.5.0/32     | 5.6.7.0/32          | TCP(6)/90   | TCP(6)/80        | Permit equivalent | True    |

### Access Rule with Service Object

ASA configuration:

```
object service servObj1
 service tcp destination eq 78
access-list acpl extended permit object servObj1 any any
access-group acpl in interface outside
```

Converts to:

Table 39: Port Object

| Name     | Type   | Domain | Value (Protocol/Port) | Override |
|----------|--------|--------|-----------------------|----------|
| servObj1 | Object | None   | TCP(6)/78             | False    |

Table 40: Access Control or Prefilter Rule

| Name   | Source Zone | Destination Zone | Source Network | Destination Network | Source Port | Destination Port | Action            | Enabled |
|--------|-------------|------------------|----------------|---------------------|-------------|------------------|-------------------|---------|
| acpl#1 | Any         | Any              | Any            | Any                 | Any         | servObj1         | Permit equivalent | True    |

### Access Rule with Service Object Group

ASA configuration:

```
object-group service legServGroup tcp
 port-object eq 78
access-list acpl extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0
object-group legServGroup
access-group acpl global
```

Converts to:

Table 41: Port Object

| Name         | Type   | Domain | Value (Protocol/Port) | Override |
|--------------|--------|--------|-----------------------|----------|
| legServGroup | Object | None   | TCP(6)/78             | False    |

Table 42: Access Control or Prefilter Rule

| Name   | Source Zone | Destination Zone | Source Network | Destination Network | Source Port | Destination Port | Action            | Enabled |
|--------|-------------|------------------|----------------|---------------------|-------------|------------------|-------------------|---------|
| acpl#1 | Any         | Any              | 3.4.5.0/24     | 5.6.7.0/24          | TCP(6)      | legServGroup     | Permit equivalent | True    |

### Access Rule with Nested Service Object Group

ASA configuration:

```
object-group service legServGroup1 tcp
 port-object eq 78
 port-object eq 79
object-group service legServGroup2 tcp
 port-object eq 80
 port-object eq 81
object-group service legacyServiceNestedGrp tcp
 group-object legServGroup1
 group-object legServGroup2
access-list acpl extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0
object-group legacyServiceNestedGrp
access-group acpl global
```

Converts to:

Table 43: Port Objects and Groups

| Name            | Type   | Domain | Value (Protocol/Port)              | Override |
|-----------------|--------|--------|------------------------------------|----------|
| legServGroup1_1 | Object | None   | TCP(6)/78                          | False    |
| legServGroup1_2 | Object | None   | TCP(6)/79                          | False    |
| legServGroup2_1 | Object | None   | TCP(6)/80                          | False    |
| legServGroup2_2 | Object | None   | TCP(6)/81                          | False    |
| legServGroup1   | Group  | None   | legServGroup1_1<br>legServGroup1_2 | False    |
| legServGroup2   | Group  | None   | legServGroup2_1<br>legServGroup2_2 | False    |

Note that the converted configuration does *not* contain an equivalent for the nested group, legacyServiceNestedGrp, because that group has been flattened.

Table 44: Access Control or Prefilter Rule

| Name   | Source Zone | Destination Zone | Source Network | Destination Network | Source Port | Destination Port               | Action            | Enabled |
|--------|-------------|------------------|----------------|---------------------|-------------|--------------------------------|-------------------|---------|
| acp1#1 | Any         | Any              | 3.4.5.0/24     | 5.6.7.0/24          | TCP(6)      | legServGroup1<br>legServGroup2 | Permit equivalent | True    |

### Access Rule with Nested Extended Service Object Group

ASA configuration:

```
object service http
 service tcp source range 9000 12000 destination eq www
object service http-proxy
 service tcp source range 9000 12000 destination eq 8080
object-group service all-http
 service-object object http
 service-object object http-proxy
object-group service all-httpz
 group-object all-http
 service-object tcp destination eq 443
access-list acp1 extended permit object-group all-httpz any any
access-group acp1 in interface inside
```

Converts to:

Table 45: Port Objects

| Name     | Type   | Domain | Value (Protocol/Port) | Override |
|----------|--------|--------|-----------------------|----------|
| http_src | Object | None   | TCP(6)/9000-12000     | False    |



| Name           | Type   | Domain | Value (Protocol/Port) | Override |
|----------------|--------|--------|-----------------------|----------|
| http_dst       | Object | None   | TCP(6)/80             | False    |
| http-proxy_src | Object | None   | TCP(6)/9000-12000     | False    |
| http-proxy_dst | Object | None   | TCP(6)/8080           | False    |
| all-httpz-dst  | Group  | None   | TCP(6)/443            | False    |

Note that the converted configuration does *not* contain an equivalent for the nested group, all-httpz, because that group has been flattened.

**Table 46: Access Control or Prefilter Rules**

| Name     | Source Zone | Dest Zone | Source Network | Destination Network | Source Port    | Destination Port | Action            | Enabled |
|----------|-------------|-----------|----------------|---------------------|----------------|------------------|-------------------|---------|
| acpl#1_1 | Any         | Any       | Any            | Any                 | http_src       | http_dst         | Permit equivalent | True    |
| acpl#1_2 | Any         | Any       | Any            | Any                 | http-proxy_src | http-proxy_dst   | Permit equivalent | True    |
| acpl#1_3 | Any         | Any       | Any            | Any                 | Any            | all-httpz-dst    | Permit equivalent | True    |

### Access Rule with Service Object Using "gt" and "neq" Operators

ASA configuration:

```
object service testOperator
 service tcp source gt 100 destination neq 200
access-list acpl extended permit object testOperator any any
```

Converts to:

**Table 47: Port Objects**

| Name               | Type   | Domain | Value (Protocol/Port)                     | Override |
|--------------------|--------|--------|-------------------------------------------|----------|
| testOperator_src   | Object | None   | TCP(6)/101-65535                          | False    |
| testOperator_dst_1 | Object | None   | TCP(6)/1-199                              | False    |
| testOperator_dst_2 | Object | None   | TCP(6)/201-65535                          | False    |
| testOperator_dst   | Group  | None   | testOperator_dst_1,<br>testOperator_dst_2 | False    |

Table 48: Access Control or Prefilter Rule

| Name   | Source Zone | Dest Zone | Source Network | Dest Network | Source Port      | Destination Port | Action            | Enabled |
|--------|-------------|-----------|----------------|--------------|------------------|------------------|-------------------|---------|
| acpl#1 | Any         | Any       | Any            | Any          | testOperator_src | testOperator_dst | Permit equivalent | True    |

### Access Rule with Security Objects Using "lt" and "gt" Operators

ASA configuration:

```
object service testOperator
 service tcp source gt 100 destination lt 200
access-list acpl extended permit object testOperator any any
```

Converts to:

Table 49: Port Objects

| Name             | Type   | Domain | Value (Protocol/Port) | Override |
|------------------|--------|--------|-----------------------|----------|
| testOperator_src | Object | None   | TCP(6)/101-65535      | False    |
| testOperator_dst | Object | None   | TCP(6)/1-199          | False    |

Table 50: Access Control or Prefilter Rule

| Name   | Source Zone | Dest Zone | Source Network | Dest Network | Source Port      | Destination Port | Action            | Enabled |
|--------|-------------|-----------|----------------|--------------|------------------|------------------|-------------------|---------|
| acpl#1 | Any         | Any       | Any            | Any          | testOperator_src | testOperator_dst | Permit equivalent | True    |

### Access Rule with TCP Service Object Using "eq" Operator and Port Literal Values

ASA configuration:

```
object service svcObj1
 service tcp source eq telnet destination eq ssh
access-list acpl extended permit object testOperator any any
```

Converts to:

Table 51: Port Objects

| Name        | Type   | Domain | Value (Protocol/Port) | Override |
|-------------|--------|--------|-----------------------|----------|
| svcObj1_src | Object | None   | TCP(6)/21             | False    |
| svcObj1_dst | Object | None   | TCP(6)/22             | False    |

Table 52: Access Control or Prefilter Rule

| Name   | Source Zone | Dest Zone | Source Network | Dest Network | Source Port | Destination Port | Action            | Enabled |
|--------|-------------|-----------|----------------|--------------|-------------|------------------|-------------------|---------|
| acpl#1 | Any         | Any       | Any            | Any          | svcObj1_src | svcObj1_dst      | Permit equivalent | True    |

**Access Rule with ICMP Service Object**

ASA configuration:

```
object-group service icmpObj
 service-object icmp echo-reply 8
 access-list acpl extended permit object icmpObj any any
```

Converts to:

Table 53: Port Object

| Name    | Type   | Domain | Value (Protocol/Port) | Override |
|---------|--------|--------|-----------------------|----------|
| icmpObj | Object | None   | ICMP(1)/Echo reply    | False    |

Table 54: Access Control or Prefilter Rule

| Name   | Source Zone | Destination Zone | Source Network | Destination Network | Source Port | Destination Port | Action            | Enabled |
|--------|-------------|------------------|----------------|---------------------|-------------|------------------|-------------------|---------|
| acpl#1 | Any         | Any              | Any            | Any                 | Any         | icmpObj          | Permit equivalent | True    |

**Access Rule with protocol Service Object**

ASA configuration:

```
object-group protocol testProtocol
 protocol-object tcp
 access-list acpl extended permit object testProtocol any any
```

Converts to:

Table 55: Port Object

| Name         | Type   | Domain | Value (Protocol/Port) | Override |
|--------------|--------|--------|-----------------------|----------|
| testProtocol | Object | None   | TCP(6)                | False    |

Table 56: Access Control or Prefilter Rule

| Name   | Source Zone | Dest Zone | Source Network | Dest Network | Source Port | Destination Port | Action            | Enabled |
|--------|-------------|-----------|----------------|--------------|-------------|------------------|-------------------|---------|
| acp1#1 | Any         | Any       | Any            | Any          | Any         | testProtocol     | Permit equivalent | True    |

**Access Rule with Extended Service Object (Source Only)**

ASA configuration:

```
object service serviceObj
 service tcp source eq 300
 service tcp source eq 800
access-list acp1 extended permit object serviceObj any any
```

Converts to:

Table 57: Port Objects

| Name             | Type   | Domain | Value (Protocol/Port)                | Override |
|------------------|--------|--------|--------------------------------------|----------|
| serviceObj_src_1 | Object | None   | TCP(6)/300                           | False    |
| serviceObj_src_2 | Object | None   | TCP(6)/800                           | False    |
| serviceObj       | Group  | None   | serviceObj_src_1<br>serviceObj_src_2 | False    |

Table 58: Access Control or Prefilter Rule

| Name   | Source Zone | Destination Zone | Source Network | Destination Network | Source Port | Destination Port | Action            | Enabled |
|--------|-------------|------------------|----------------|---------------------|-------------|------------------|-------------------|---------|
| acp1#1 | Any         | Any              | Any            | Any                 | Any         | serviceObj       | Permit equivalent | True    |

**Access Rule with Extended Service Object (Source and Destination)**

ASA configuration:

```
object service serviceObj
 service tcp source eq 300 destination eq 400
access-list acp1 extended permit tcp object serviceObj any any
```

Converts to:

Table 59: Port Objects

| Name           | Type   | Domain | Value (Protocol/Port) | Override |
|----------------|--------|--------|-----------------------|----------|
| serviceObj_src | Object | None   | TCP(6)/300            | False    |
| serviceObj_dst | Object | None   | TCP(6)/400            | False    |

Table 60: Access Control or Prefilter Rule

| Name   | Source Zone | Dest Zone | Source Network | Dest Network | Source Port    | Destination Port | Action            | Enabled |
|--------|-------------|-----------|----------------|--------------|----------------|------------------|-------------------|---------|
| acpl#1 | Any         | Any       | Any            | Any          | serviceObj_src | serviceObj_dst   | Permit equivalent | True    |

**Access Rule with Port Argument Operator "neq" in Source Port**

ASA configuration:

```
access-list acpl extended permit tcp any neq 300
```

Converts to:

Table 61: Access Control or Prefilter Rule

| Name   | Source Zone | Destination Zone | Source Network | Destination Network | Source Port      | Destination Port | Action            | Enabled |
|--------|-------------|------------------|----------------|---------------------|------------------|------------------|-------------------|---------|
| acpl#1 | Any         | Any              | Any            | Any                 | 1-299, 301-65535 | Any              | Permit equivalent | True    |

**Access Rule with Port Argument Operator "neq" in Source and Destination Ports**

ASA configuration:

```
access-list acpl extended permit tcp any neq 300 any neq 400
```

Converts to:

Table 62: Access Control or Prefilter Rules

| Name     | Source Zone | Destination Zone | Source Network | Destination Network | Source Port | Destination Port | Action            | Enabled |
|----------|-------------|------------------|----------------|---------------------|-------------|------------------|-------------------|---------|
| acpl#1_1 | Any         | Any              | Any            | Any                 | 1-299       | 1-399            | Permit equivalent | True    |
| acpl#1_2 | Any         | Any              | Any            | Any                 | 301-65535   | 1-399            | Permit equivalent | True    |
| acpl#1_3 | Any         | Any              | Any            | Any                 | 1-299       | 401-65535        | Permit equivalent | True    |

| Name     | Source Zone | Destination Zone | Source Network | Destination Network | Source Port | Destination Port | Action            | Enabled |
|----------|-------------|------------------|----------------|---------------------|-------------|------------------|-------------------|---------|
| acpl#1_4 | Any         | Any              | Any            | Any                 | 301-65535   | 401-65535        | Permit equivalent | True    |

### Inactive Access Rule

ASA configuration:

```
access-list acpl extended permit tcp 3.4.5.0 255.255.255.0 5.6.7.0 255.255.255.0 inactive
access-group acpl global
```

Converts to:

**Table 63: Access Control or Prefilter Rule**

| Name   | Source Zone | Destination Zone | Source Network | Destination Network | Source Port | Destination Port | Action            | Enabled |
|--------|-------------|------------------|----------------|---------------------|-------------|------------------|-------------------|---------|
| acpl#1 | Any         | Any              | 3.4.5.0/24     | 5.6.7.0/24          | TCP(6)      | Any              | Permit equivalent | False   |

### Access Control List Applied to Inbound Traffic

ASA configuration:

```
access-list acpl extended permit tcp 3.4.5.0 255.255.255.0 eq 90 any eq 80
access-group acpl in inside
```

Converts to:

**Table 64: Security Zone/Interface Group**

| Name                | Interface Type                                                                                                                                                          | Domain | Selected Interfaces |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---------------------|
| acpl_inside_in_zone | <ul style="list-style-type: none"> <li>• Routed (if ASA device is running in routed mode)</li> <li>• Switched (if ASA device is running in transparent mode)</li> </ul> | None   | Any                 |

**Table 65: Access Control or Prefilter Rule**

| Name   | Source Zone         | Dest Zone | Source Network | Dest Network | Source Port | Destination Port | Action            | Enabled |
|--------|---------------------|-----------|----------------|--------------|-------------|------------------|-------------------|---------|
| acpl#1 | acpl_inside_in_zone | Any       | 3.4.5.0/24     | Any          | TCP(6)/90   | TCP(6)/80        | Permit equivalent | True    |

### Access Control List Applied to Outbound Traffic

ASA configuration:

```
access-list acp1 extended permit tcp 3.4.5.0 255.255.255.0 eq 90 any eq 80
access-group acp1 out outside
```

Converts to:

**Table 66: Security Zone/Interface Group**

| Name                  | Interface Type                                                                                                                                                          | Domain | Selected Interfaces |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|---------------------|
| acp1_outside_out_zone | <ul style="list-style-type: none"> <li>• Routed (if ASA device is running in routed mode)</li> <li>• Switched (if ASA device is running in transparent mode)</li> </ul> | None   | Any                 |

**Table 67: Access Control or Prefilter Rule**

| Name   | Source Zone           | Dest Zone | Source Network | Dest Network | Source Port | Destination Port | Action            | Enabled |
|--------|-----------------------|-----------|----------------|--------------|-------------|------------------|-------------------|---------|
| acp1#1 | acp1_outside_out_zone | Any       | 3.4.5.0/24     | Any          | TCP(6)/90   | TCP(6)/80        | Permit equivalent | True    |

