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 1
- Naming Conventions for Converted Configurations, on page 2
- Fields Specific to Firepower Objects and Object Groups, on page 4
- Access Rule Conversion, on page 4
- NAT Rule Conversion, on page 11
- Network Object and Network Object Group Conversion, on page 13
- Service Object and Service Group Conversion, on page 15
- Access-Group Conversion, on page 24

Conversion Mapping Overview

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

Table 1: Summary of Conversion Mapping

Entity	ASA Configuration	Firepower Threat Defense Configuration
Network objects	Network objects Network object groups Nested network object groups	Network objects Network object groups Nested network object groups
Service objects	Service objects Service object groups Nested service object groups	Multiple port objects Multiple port object groups Multiple or flattened port object groups For more information, see Service Object and Service Group Conversion, on page 15

Entity	ASA Configuration	Firepower Threat Defense Configuration
Access rules	Access rules	Access control policy or prefilter policy (as selected)
NAT rules	Twice NAT rules Network object NAT rules	Manual NAT rules 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 2: Extensions for Converted Service Objects and Groups

Extension	Reason for Appending
`_dst`	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 Service Objects with Source and Destination Ports, on page 17.
`_src`	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 .
`_#`	Converts a nested service group; see Nested Service Group Conversion, on page 20.

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 converstion). 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 acp1 permit tcp any host 209.165.201.3 eq 80
access-group acp1 in interface outside
```

The tool converts this configuration to a security zone or interface group named `acp1_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 3: 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.

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
Permit	**Allow** or **Trust**, 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 4: 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 5: Default Values for Fields Specific to Access Control Rules

Access Control Rules Field	Default Value for Converted Access Rules
Name	System-generated (see Naming Conventions for Converted Configurations, on page 2)
Source Zone	• If the ACL is applied globally, `Any` • If the ACL is applied to a specific interface, the Security Zone that the tool creates during conversion
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
Permit	**Fastpath** or **Analyze**, depending on the choice you make during migration
Deny	**Block**

- 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 `Any` interface)	`Any`	`Any`
Applied to specific interfaces	The interface group you choose during import	`Any`

- 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 6: 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 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 7: Default Values for Fields Specific to Firepower Prefilter Rules

Prefilter Rule Field	Default Value for Converted Access Rules
Name	System-generated (see Naming Conventions for Converted Configurations, on page 2)
Source Interface Objects	• If the ACL is applied globally, `Any` • If the ACL is applied to a specific interface, the Interface Group that the tool creates during conversion
Destination Interface Objects	`Any` (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 8: Port Argument Operators in Access Rules

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

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 9: 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, 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 10: 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 11: ASA NAT Policies Mapped to Firepower Threat Defense NAT Policies

ASA NAT Policy	Firepower Threat Defense NAT Policy	Defining Characteristics
Twice NAT	Manual NAT	• Specifies both the source and destination address in a single rule. • Configured directly. • Can use network object groups. • Manually ordered in the NAT table (before or after auto NAT rules).
Network object NAT	Auto NAT	• Specifies either a source or a destination address. • Configured as a parameter of a network object. • Cannot use network object groups. • Automatically ordered in the NAT table.

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 12: 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 Original Packet - Original Destination - Network
Original Packet - Service	Original Packet - Original Source Port Original Packet - Original Destination Port
Translated Packet - Source NAT Type	Type
Translated Packet - Source Address	Translated Packet - Translated Source - Address Type Translated Packet - Translated Source - Network
Translated Packet - Destination Address	Translated Packet - Translated Destination
Translated Packet - Service	Translated Packet - Translated Source Port 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 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 13: ASA Network Object Fields Mapped to Firepower Network Object Fields

ASA Network Object Field	Firepower Network Object Field
Name	System-generated; see Naming Conventions for Converted Configurations, on page 2
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 14: 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 obj2 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 13.

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 15: 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 Naming Conventions for Converted Configurations, on page 2)
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 16: Port Argument Operators in Service Objects

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

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

The migration tool converts these operators as follows:

Table 17: 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`):
		`TCP(6)/1-199`
		Second object (`testOperator_src_2`):
		`TCP(6)/201-65535`
		Object group (`testOperator_src`):
		`testOperator_src_1`
		`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 18: 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 19: 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 20: Port Object

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

ICMPv6

ASA configuration:

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

Converts to:

Table 21: 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 22: ASA Service Group Fields Mapped to Firepower Port Object Fields

ASA Service Group Field	Port Object Group Field
Name	System-generated (see Naming Conventions for Converted Configurations, on page 2)
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 2

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

Converts to:

Table 23: 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 legServGroup1_2	False
legServGroup2	Group	None	legServGroup2_1 legServGroup2_2	False

Table 24: 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 legServGroup2	Permit equivalent	True

Example: Protocol Service Group Conversion

ASA configuration:

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

Converts to:

Table 25: 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 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 26: 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 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 27: 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 servObj2 servObj3	False

Example: ICMP/ICMPv6 Service Group Conversion

ICMP

ASA configuration:

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

Converts to:

Table 28: 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 29: 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 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 30: 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 acp1 permit tcp any host 209.165.201.3 eq 80
access-group acp1 in interface outside
```

In this example, the `access-group` command applies the ACL named `acp1` to inbound traffic on the interface named `outside`.

The migration tool converts this configuration to:

Table 31: Security Zone/Interface Group

Name	Interface Type	Domain	Selected Interfaces
acp1_outside_in_zone	• Routed (if ASA device is running in routed mode) • Switched (if ASA device is running in transparent mode)	None	Any

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
acp1#1	acp1_outside_in_zone	Any	Any	209.165.201.3	Any	TCP(6)/80	Permit equivalent	True