



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, page 1](#)

Examples

Access Rule Specifying Individual Networks

ASA configuration:

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

Converts to:

Table 1: 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	True

Access Rule with Network Object Groups

ASA configuration:

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

Converts to:

Table 2: Network Object Groups

Name	Domain	Value (Network)	Type	Override
host1	None	obj1 obj2	Group	False
host2	None	obj3 obj4	Group	False

Table 3: 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 4: 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 5: Port Object

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

Table 6: 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 7: Port Object

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

Table 8: 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 9: 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 legServGroup1_2	False
legServGroup2	Group	None	legServGroup2_1 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 10: 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)	legServGroup1 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 acpl extended permit object-group all-httpz any any
access-group acpl in interface inside
```

Converts to:

Table 11: Port Objects

Name	Type	Domain	Value (Protocol/Port)	Override
http_src	Object	None	TCP(6)/9000-12000	False
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 12: 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 13: Port Objects

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

Name	Type	Domain	Value (Protocol/Port)	Override
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, testOperator_dst_2	False

Table 14: 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 15: 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 16: 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 17: 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 18: 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 19: Port Object

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

Table 20: 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 21: Port Object

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

Table 22: 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	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 acpl extended permit object serviceObj any any
```

Converts to:

Table 23: 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 serviceObj_src_2	False

Table 24: 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	serviceObj	Permit equivalent	True

Access Rule with Extended Service Object (Source and Destination)

ASA configuration:

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

Converts to:

Table 25: 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 26: 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 27: 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 28: 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
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 29: 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 30: Security Zone/Interface Group

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

Table 31: 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 acpl extended permit tcp 3.4.5.0 255.255.255.0 eq 90 any eq 80
access-group acpl out outside
```

Converts to:

Table 32: Security Zone/Interface Group

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

Table 33: Access Control or Prefilter Rule

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

