Understand the Rule Expansion on FirePOWER Devices

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Understanding Rule Expansion
Expansion of an IP Based Rule
Expansion of an IP Based Rule using Custom URL
Expansion of an IP Based Rule using Ports
Expansion of an IP Based Rule Using VLANs
Expansion of an IP Based Rule with URL Categories
Expansion of an IP based Rule with Zones
General Formula for Rule Expansion
Troubleshooting Deployment Failure due to Rule Expansion
Related Information

Introduction

This document describes the translation of Access Control rules to the sensor when deployed from the Firepower Management Center (FMC).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Firepower technology
- Knowledge on configuring Access control policies on FMC

Components Used

The information in this document is based on these software and hardware versions:

- Firepower Management Center version 6.0.0 and above
- ASA Firepower Defense Image (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) running software version 6.0.1 and above

- ASA Firepower SFR Image (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) running software version 6.0.0 and above

- Firepower 7000/8000 series sensor version 6.0.0 and above

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

An Access control rule is created with the use of one or multiple combinations of these parameters:

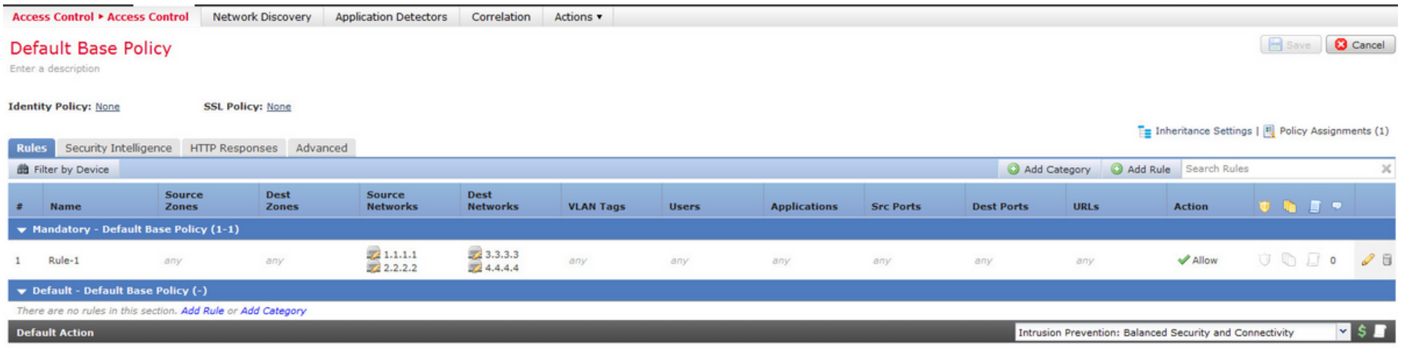
- IP Address (Source and Destination)
- Ports (Source and Destination)
- URL (System provided Categories and Custom URLs)
- Application Detectors
- VLANs
- Zones

Based on the combination of parameters used in the access rule, the rule expansion changes on the sensor. This document highlights various combinations of rules on the FMC and their respective associated expansions on the sensors.

Understanding Rule Expansion

Expansion of an IP Based Rule

Consider the configuration of an access rule from the FMC, as shown in the image:



Default Base Policy

Enter a description

Identity Policy: None SSL Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action				
▾ Mandatory - Default Base Policy (1-1)																
1	Rule-1	any	any	1.1.1.1 2.2.2.2	3.3.3.3 4.4.4.4	any	any	any	any	any	any	✓ Allow				0
▾ Default - Default Base Policy (-)																
There are no rules in this section. Add Rule or Add Category																

Default Action: Intrusion Prevention: Balanced Security and Connectivity

This is a single rule on the Management Center. However, after deploying it to the sensor, it expands into **four** rules as shown in the image:

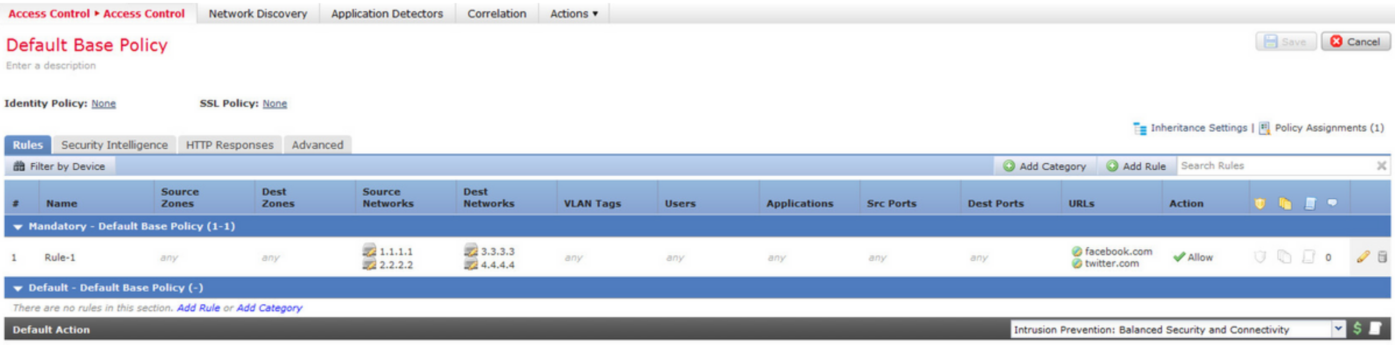
```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

When you deploy a rule with two subnets configured as Source and two hosts configured as destination addresses, this rule is expanded to four rules on the sensor.

> **Note**: If the requirement is to block access based on destination networks, a better way to perform this is to use the feature of Blacklists under Security Intelligence.

Expansion of an IP Based Rule using Custom URL

Consider the configuration of an access rule from the FMC as shown in the image:



Default Base Policy

Enter a description

Identity Policy: None SSL Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action
▾ Mandatory - Default Base Policy (1-1)												
1	Rule-1	any	any	1.1.1.1 2.2.2.2	3.3.3.3 4.4.4.4	any	any	any	any	any	facebook.com twitter.com	✓ Allow
▾ Default - Default Base Policy (-)												
There are no rules in this section. Add Rule or Add Category												

Default Action: Intrusion Prevention: Balanced Security and Connectivity

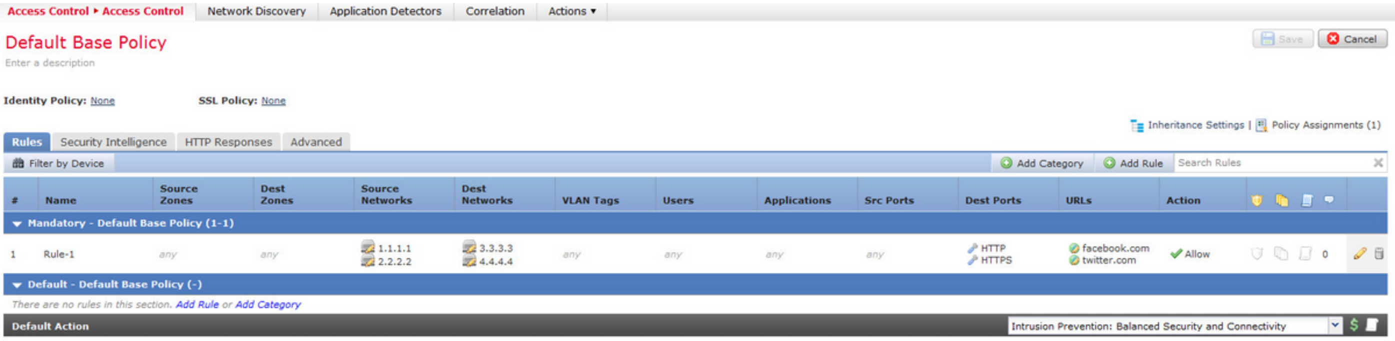
This is a single rule on the Management Center. However, after deploying it to the sensor, it is expanded into eight rules as shown in the image:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url "twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url "twitter.com")
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

When you deploy a rule with two subnets configured as Source, two hosts configured as destination addresses and two custom URL objects in a single rule on the Management Center ,this rule is expanded to eight rules on the sensor. This means that for each custom URL category there is a combination of source and destination IP/port ranges, which are configured and created.

Expansion of an IP Based Rule using Ports

Consider the configuration of an access rule from the FMC as shown in the image:



Default Base Policy

Enter a description

Identity Policy: None   SSL Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action				
▾ Mandatory - Default Base Policy (1-1)																
1	Rule-1	any	any	1.1.1.1 2.2.2.2	3.3.3.3 4.4.4.4	any	any	any	any	HTTP HTTPS	facebook.com twitter.com	✓ Allow				0
▾ Default - Default Base Policy (-)																
There are no rules in this section. Add Rule or Add Category																
Default Action											Intrusion Prevention: Balanced Security and Connectivity					

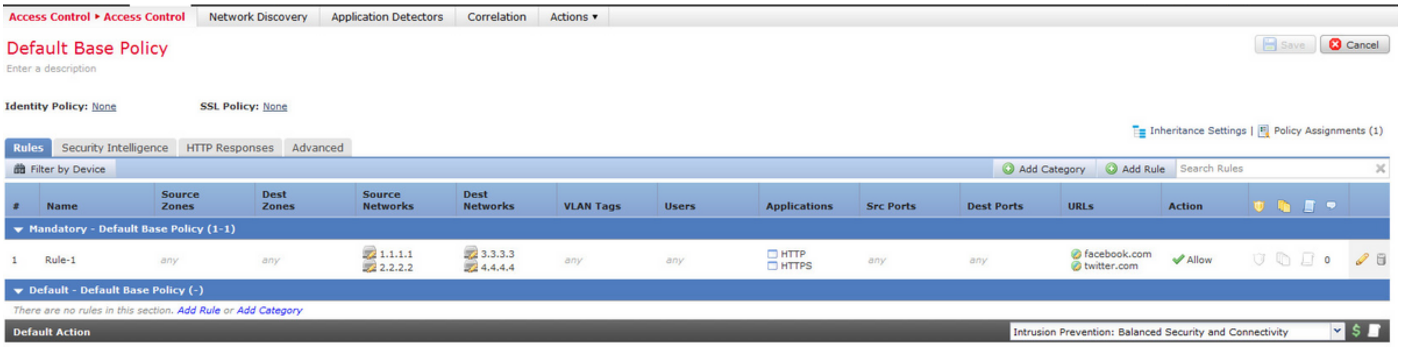
This is a single rule on the Management Center. However, after deploying it to the sensor, it is expanded into sixteen rules as shown in the image:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268435456 allow any any any any any any any any (ipspolicy 2)
```

When you deploy a rule with two subnets configured as Source, two hosts configured as destination addresses and two custom URL objects destined to two ports, this rule expands to sixteen rules on the sensor.

> **Note**: If there is a requirement to use the ports in the access rule, use **application detectors** which are present for standard applications. This helps rule expansion to happen in an efficient way.

Consider the configuration of an access rule from the FMC as shown in the image:



Default Base Policy

Enter a description

Identity Policy: None SSL Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action	
Mandatory - Default Base Policy (1-1)													
1	Rule-1	any	any	1.1.1.1 2.2.2.2	3.3.3.3 4.4.4.4	any	any	HTTP HTTPS	any	any	facebook.com twitter.com	✓ Allow	0
Default - Default Base Policy (-)													
There are no rules in this section. Add Rule or Add Category													

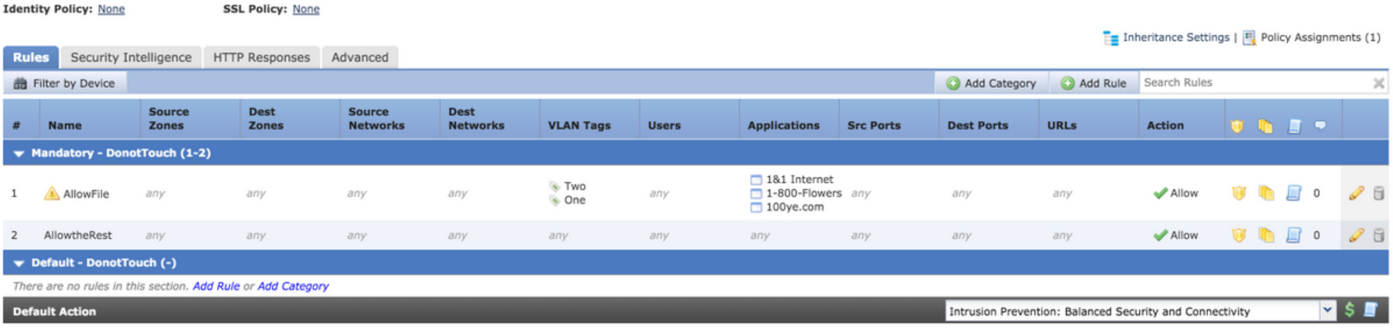
Default Action: Intrusion Prevention: Balanced Security and Connectivity

When you use Application detectors instead of ports, the number of expanded rules reduces from sixteen to eight as shown in the image:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
```

Expansion of an IP Based Rule Using VLANs

Consider the configuration of an access rule from the FMC as shown in the image:



Identity Policy: None SSL Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action	
Mandatory - DonotTouch (1-2)													
1	AllowFile	any	any	any	any	Two One	any	1&1 Internet 1-800-Flowers 100ye.com	any	any	any	✓ Allow	0
2	AllowtheRest	any	any	any	any	any	any	any	any	any	any	✓ Allow	0
Default - DonotTouch (-)													
There are no rules in this section. Add Rule or Add Category													

Default Action: Intrusion Prevention: Balanced Security and Connectivity

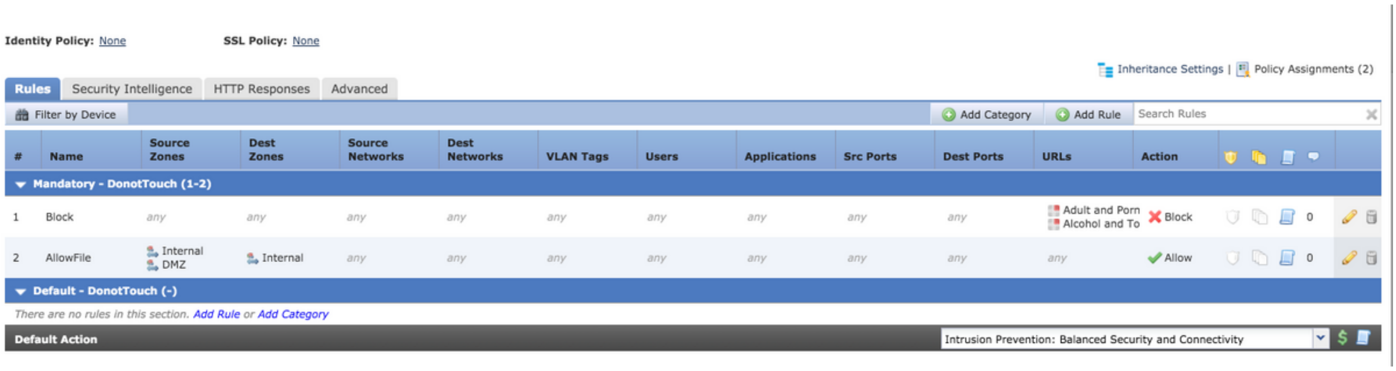
The Rule **AllowFile** has a single line matching two VLAN ids with some Application detectors,Intrusion policies and File policies. The rule AllowFile will expand to two rules.

```
268436480 allow any any any any any any 1 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 enable) (appid 535:4, 1553:4, 3791:4)
268436480 allow any any any any any any 2 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 enable) (appid 535:4, 1553:4, 3791:4)
```

IPS policies and File policies are unique for each Access Control Rule but multiple Application detectors are referred in the same rule and hence do not participate in the expansion. When you consider a rule with two VLAN ids and three application detectors, there are only two rules, one for each VLAN.

Expansion of an IP Based Rule with URL Categories

Consider the configuration of an access rule from the FMC as shown in the image:



Identity Policy: None SSL Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action	
▼ Mandatory - DonotTouch (1-2)													
1	Block	any	any	any	any	any	any	any	any	any	Adult and Porn Alcohol and To	✗ Block	0
2	AllowFile	Internal DMZ	Internal	any	any	any	any	any	any	any	any	✓ Allow	0
▼ Default - DonotTouch (-)													

There are no rules in this section. Add Rule or Add Category

Default Action: Intrusion Prevention: Balanced Security and Connectivity

The Block Rule blocks URL categories for **Adult and pornography Any Reputation** and **Alcohol and Tobacco Reputations 1-3.** This is a single rule on the Management Center but when you deploy it to the sensor it is expanded into two rules as shown in this:

```
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 11)
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 76) (urlrep le 60)
```

When you deploy a single rule with two subnets configured as Source and two hosts configured as destination addresses, along with two custom URL objects destined to two ports with two URL categories, this rule expands to thirty-two rules on the sensor.

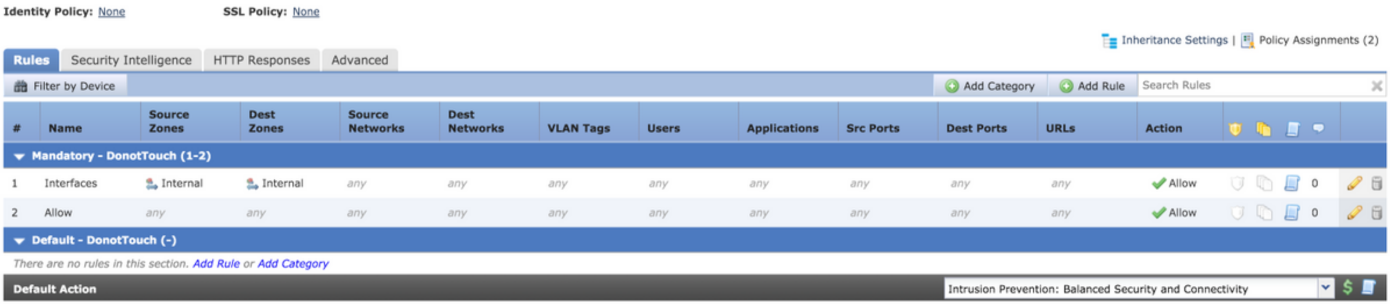
Expansion of an IP based Rule with Zones

Zones are assigned numbers which are referenced in policies.

If a zone is referenced in a policy but that zone is not assigned to any interface on the device to which the policy is being pushed, the zone is considered as an **any** and an **any** does not lead to any expansion of rules.

If the source zone and destination zone are the same in the rule, zone factor is considered as **any** and only one rule is added since ANY does not lead to any expansion of rules.

Consider the configuration of an access rule from the FMC as shown in the image:



Identity Policy: None SSL Policy: None

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action	
▼ Mandatory - DonotTouch (1-2)													
1	Interfaces	Internal	Internal	any	any	any	any	any	any	any	any	✓ Allow	0
2	Allow	any	any	any	any	any	any	any	any	any	any	✓ Allow	0
▼ Default - DonotTouch (-)													

There are no rules in this section. Add Rule or Add Category

Default Action: Intrusion Prevention: Balanced Security and Connectivity

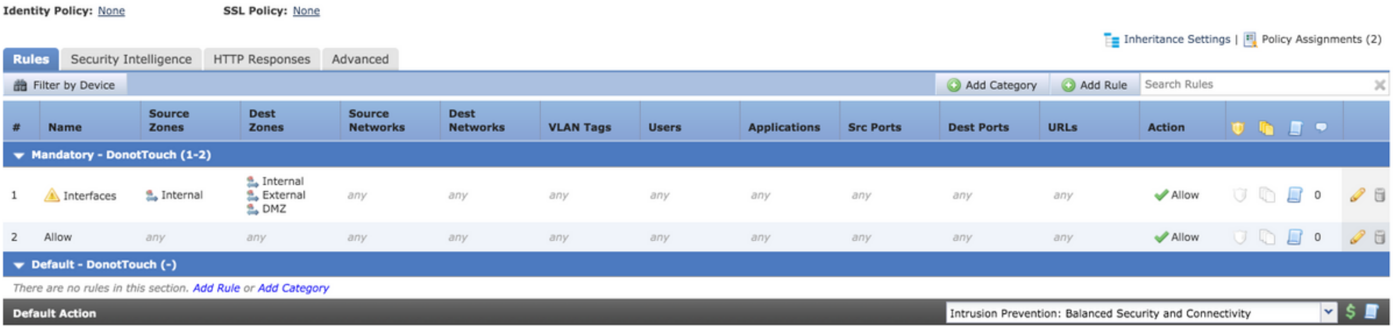
There are two rules. One rule has Zones configured but the source and destination zone is the same. The other rule has no specific configuration. In this example, the **Interfaces** access rule does not translate to a rule.

```
268438531 allow any any any any any any any any (log dcforward flowstart)<-----Allow Access Rule
268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<----------Default Intrusion Prevention Rule
```

On the sensor both the rules appear as the same because zone based control involving the same interfaces does not lead to an expansion.

Expansion of rules for zone based Access Control Rule access occurs when the zone referenced in the rule is assigned to an interface on the device.

Consider the configuration of an access rule from the FMC as shown below:



Identity Policy: None SSL Policy: None

Inheritance Settings | Policy Assignments (2)

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action				
Mandatory - DonotTouch (1-2)																
1	Interfaces	Internal	Internal External DMZ	any	any	any	any	any	any	any	any	Allow				0
2	Allow	any	any	any	any	any	any	any	any	any	any	Allow				0
Default - DonotTouch (-)																

There are no rules in this section. Add Rule or Add Category

Default Action: Intrusion Prevention: Balanced Security and Connectivity

The rule Interfaces involves zone based rules with source zone as Internal and destination zones as Internal, External and DMZ. In this rule Internaland DMZ interface zones are configured on the interfaces and External does not exist on the device.This is the expansion of the same:

```
268436480 allow 0 any any 2 any any any any (log dcforward flowstart) <------Rule for Internal to DMZ)
268438531 allow any any any any any any any any (log dcforward flowstart)<--------Allow Access rule
268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<--------Default Intrusion Prevention: Balanced Security over Connectivity
```

A rule is created for specific interface pair which is **Internal > DMZ** with clear zone specification and an **Internal > Internal** rule is not created.

The number of rules expanded is proportional to the number of zone source and destination pairs that can be created for **valid** associated zones and this include same source and destination zone rules.

> **Note**: Disabled rules from the FMC are not propagated and not expanded to the sensor during the policy deployment.

General Formula for Rule Expansion

Number of rules on sensor = (Number of Source Subnets or hosts) * (Number of Destination S) * (Number of Source Ports) * (Number of Destination Ports) * (Number of Custom URLs)* (Number of VLAN Tags)* (Number of URL Categories)*(Number of valid source and destination zone pairs)

> **Note**: For the calculations, **any** value in the field is substituted by 1.The value **any** in the rule combination is considered as 1 and it does not increase or expand the rule.

Troubleshooting Deployment Failure due to Rule Expansion

When there is a deployment failure after making addition to the access rule, follow the steps mentioned below for the cases where the rule expansion limit has been reached

Check the **/var/log/action.queue.log** for messages with the following keywords :

Error - too many rules - writing rule 28, max rules 9094

The above message indicates that there is a problem with the number of rules that are being expanded. Check the configuration on the FMC to optimize the rules based on the scenario's discussed above.

Related Information

- **Firepower Management Center Configuration Guide, Version 6.0**
- **Technical Support & Documentation - Cisco Systems**