

# Configure Additional Snort 3 Rule Actions on FMC

## Contents

---

[Introduction](#)

[Background Information](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Feature Details](#)

[FMC Walkthrough](#)

---

## Introduction

This document describes the Firepower Management Center (FMC) support for additional Snort 3 rule actions feature added in 7.1 release.

## Background Information

Although the Firepower Threat Defense (FTD) supports Seven Intrusion Policy rule actions Alert/Disable/Block/Reject/Rewrite/Pass/Drop in 7.0, FMC supported only three Snort 3 rule actions: 'Alert', 'Disable', and 'Block'.

From Firepower 7.1.0, FMC supports to configure new rule actions.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of open-source Snort
- Firepower Management Center (FMC) 7.1.0+
- Firepower Threat Defense (FTD) 7.0.0+

### Components Used

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

- This document applies to all Firepower platforms running Snort 3
- Cisco Firepower Threat Defense Virtual (FTD) which runs software version 7.4.2
- Firepower Management Center Virtual (FMC) which runs software version 7.4.2

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, ensure that you understand the potential impact of any command.

# Feature Details

The new Snort 3 rule actions added and their descriptions are as follows:

**Pass:** No event generated, allows packet to pass without further evaluation by any subsequent Snort rules.

**Drop:** Generates event, drops matching packet and does not block further traffic in this connection.

**Reject:** Generates event, drops matching packet, blocks further traffic in this connection and sends TCP reset or ICMP port unreachable to source and destination hosts.

**Rewrite:** Generates event and overwrites packet contents based on the replace option in the rule.

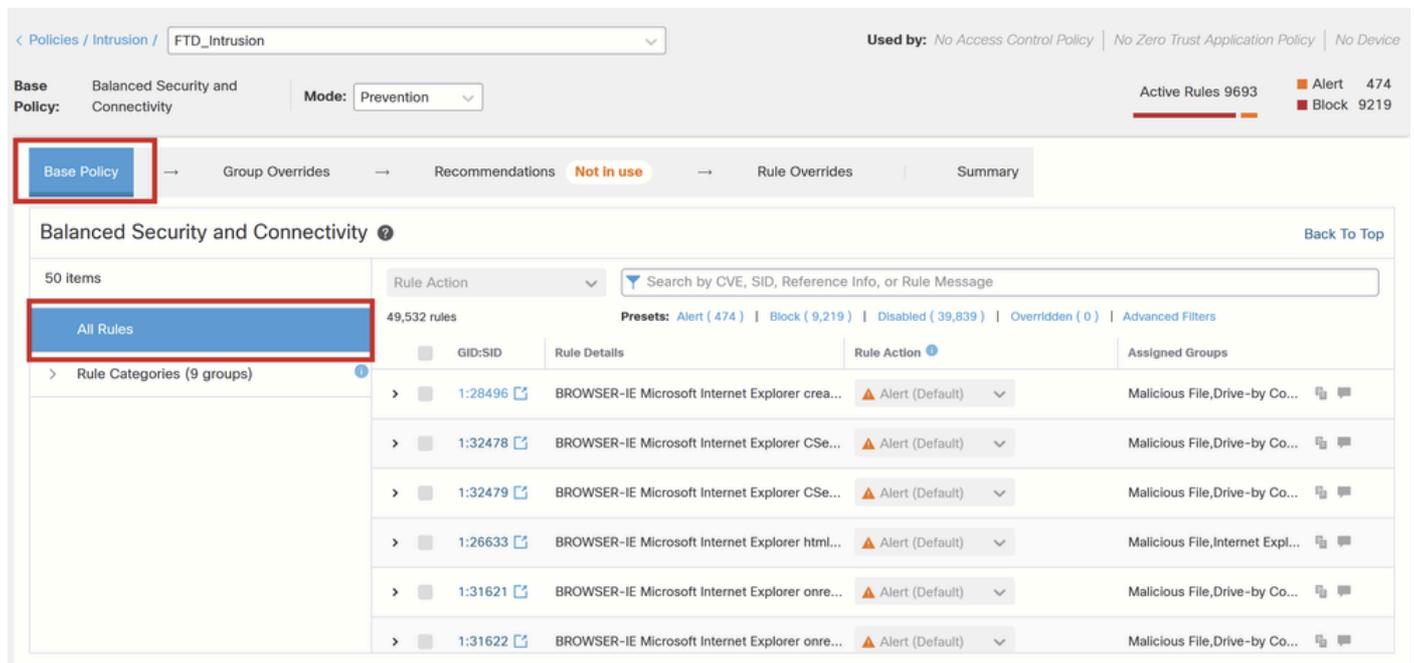
# FMC Walkthrough

To view the Snort 3 rules in an intrusion policy, navigate to FMC Policies > Access Control > Intrusion, thereafter click **Snort 3 Version** option in the top right corner of the policy, as shown in the image:



*Snort 3 Version*

Click **Base Policy > All Rules**, you can see the default actions of all the system defined Snort 3 rules.



*Base Policy*

To change the rule action to any of these new rule actions, navigate to **Rule Overrides > All Rules** and select the rule action from the drop-down for the selected rule.

< Policies / Intrusion / FTD\_Intrusion Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention Active Rules 9693 ■ Alert 474 ■ Block 9219

Base Policy → Group Overrides → Recommendations Not in use → **Rule Overrides** | Summary

### Rule Overrides Back To Top

102 items All X Rule Action Search by CVE, SID, Reference Info, or Rule Message

49,532 rules Presets: Alert (474) | Block (9,219) | Disabled (39,839) | Overridden (0) | Advanced Filters

	GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
	<input type="checkbox"/> 1:28496	BROWSER-IE Microsoft Internet ...	Alert (Default) <span style="border: 1px solid red; padding: 2px;">▼</span>	Base Policy	Malicious File,Drive... <span style="float: right;">🔗 🗨</span>
	<input type="checkbox"/> 1:32478	BROWSER-IE Microsoft Internet ...	Block	Base Policy	Malicious File,Drive... <span style="float: right;">🔗 🗨</span>
	<input type="checkbox"/> 1:32479	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File,Drive... <span style="float: right;">🔗 🗨</span>
	<input type="checkbox"/> 1:26633	BROWSER-IE Microsoft Internet ...	Rewrite	Base Policy	Malicious File,Inter... <span style="float: right;">🔗 🗨</span>
	<input type="checkbox"/> 1:31621	BROWSER-IE Microsoft Internet ...	Drop	Base Policy	Malicious File,Drive... <span style="float: right;">🔗 🗨</span>
	<input type="checkbox"/> 1:31622	BROWSER-IE Microsoft Internet ...	Reject	Base Policy	Malicious File,Drive... <span style="float: right;">🔗 🗨</span>
	<input type="checkbox"/> 1:31622	BROWSER-IE Microsoft Internet ...	Disable	Base Policy	Malicious File,Drive... <span style="float: right;">🔗 🗨</span>
	<input type="checkbox"/> 1:31622	BROWSER-IE Microsoft Internet ...	Revert to default	Base Policy	Malicious File,Drive... <span style="float: right;">🔗 🗨</span>

*Additional Rule Actions*

< Policies / Intrusion / FTD\_Intrusion Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention Active Rules 9693 ■ Alert 474 ■ Block 9219

Base Policy → Group Overrides → Recommendations Not in use → **Rule Overrides** | Summary

### Rule Overrides Back To Top

102 items All X Rule Action Search by CVE, SID, Reference Info, or Rule Message

49,532 rules Presets: Alert (474) | Block (9,219) | Disabled (39,839) | Overridden (0) | Advanced Filters

✔ Rule action changed successfully ✕

	GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
	<input type="checkbox"/> 1:28496	BROWSER-IE Microsoft Internet ...	<span style="border: 1px solid red; padding: 2px;">Reject</span>	Rule Override	Malicious File,Drive... <span style="float: right;">🔗 🗨</span>
	<input type="checkbox"/> 1:32478	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File,Drive... <span style="float: right;">🔗 🗨</span>
	<input type="checkbox"/> 1:32479	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File,Drive... <span style="float: right;">🔗 🗨</span>
	<input type="checkbox"/> 1:26633	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File,Inter... <span style="float: right;">🔗 🗨</span>

*Changing the Rule Action*

The overridden rules can be found under **Rule Overrides > Overridden Rules**.

< Policies / Intrusion / FTD\_Intrusion Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention Active Rules 9693   
 Alert 473   
 Block 9219   
 Others 1

Base Policy → Group Overrides → Recommendations **Not in use** → **Rule Overrides** | Summary

### Rule Overrides Back To Top

102 items All x

Rule Action Search by CVE, SID, Reference Info, or Rule Message

1 rule Presets: Alert (0) | Block (0) | Disabled (0) | **Overridden (1)** | Advanced Filters | Reject (1)

<input type="checkbox"/>	GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
> <input type="checkbox"/>	1:28496	BROWSER-IE Microsoft Internet ...	<b>Reject</b>		Malicious File, Drive...

*Overridden Rules*