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:

Intrusion Policies Network Analysis Policies				
Show Snort 3 Sync status 🚯 🔍	Search by Intrusion Policy, Description, or	Base Policy	All IPS Rules	IPS Mapping Compare Policies Create Policy
Intrusion Policy	Description	Base Policy	Usage Information	
FTD_Intrusion		Balanced Security and Connectivity	No Access Control Policy No Zero Trust Application Policy No Device	Snort 2 Version Snort 3 Version 🖌 🗄 🗈 🗑

Snort 3 Version

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

< Policies / Intrusion / FTD_Intrusion		~	Used by: No Access Control Policy	No Zero Trust Application Policy No Device
Base Balanced Security and Policy: Mode: P	revention V			Active Rules 9693 Alert 474 Block 9219
Base Policy → Group Overrides → Recommendations Not in use → Rule Overrides Summary				
Balanced Security and Connectivity	0			Back To Top
50 items	Rule Action	Search by CVE, SID, Reference	Info, or Rule Message	
All Rules	49,532 rules	Presets: Alert (474) Block (9,219) Disabled (39,839) Overridden (0)	Advanced Filters
	GID:SID	Rule Details	Rule Action 🕕	Assigned Groups
Rule Categories (9 groups)	> 1:28496	BROWSER-IE Microsoft Internet Explorer crea	▲ Alert (Default) ✓	Malicious File,Drive-by Co 🐁 🗯
	> 1:32478	BROWSER-IE Microsoft Internet Explorer CSe	Alert (Default)	Malicious File,Drive-by Co 📲 🗯
	> 1:32479	BROWSER-IE Microsoft Internet Explorer CSe	Alert (Default)	Malicious File,Drive-by Co 📲
	> 1:26633 🖸	BROWSER-IE Microsoft Internet Explorer html	Alert (Default)	Malicious File,Internet Expl 🖷 📕
	> 1:31621	BROWSER-IE Microsoft Internet Explorer onre	▲ Alert (Default) V	Malicious File,Drive-by Co 📲 🗯
	> 1:31622	BROWSER-IE Microsoft Internet Explorer onre	Alert (Default)	Malicious File,Drive-by Co 📲 🗯

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 b	y: No Access Control Policy I	No Zero Trust Application Policy No Device
Base Balanced Security and Mode: Pr Policy: Connectivity Mode: Pr	revention V			Active Rules 9693 Alert 474 Block 9219
Base Policy \rightarrow Group Overrides	→ Recommendations Not In use	→ Rule Overrides	Summary	
Rule Overrides Ø				Back To Top
102 items All $\times \sim$	Rule Action 🗸 🔽 Sea	rch by CVE, SID, Reference Info, or R	ule Message	
All Rules	49,532 rules Presets:	Alert (474) Block (9,219) Disabl	ed (39,839) Overridden (0)	Advanced Filters
Overridee Pulse	GID:SID Rule Details	Rule Action ¹	Set By	Assigned Groups
Overriden Rules	> 1:28496 [BROWSER-IE Microsoft	Internet 🔟 Alert (Default) 🗸	Base Policy	Malicious File, Drive 🔒 🗭
> MITRE (1 group)		Rule Action	Deer Delley	Malaina Dia Daira - B. 🗮
> Rule Categories (9 groups) 0	1:32478 BROWSER-IE Microsoft	Internet OBlock	Base Policy	Malicious File, Drive 📲 🗭
	> 1:32479 E BROWSER-IE Microsoft	Alert (Default)	Base Policy	Malicious File, Drive 📔 🗯
	> 1:26633 BROWSER-IE Microsoft	Internet 💡 Drop	Base Policy	Malicious File,Inter 🖷 🗭
	> 1:31621 E BROWSER-IE Microsoft	Internet Ø Disable	Base Policy	Malicious File,Drive 🔒 🗭
	> 1:31622 E BROWSER-IE Microsoft	Internet	Base Policy	Malicious File,Drive 🔒 🗯

Additional Rule Actions

< Policies / Intrusion / FTD_Intrusion	~	Used by: No Access Control Policy	No Zero Trust Application Policy No Device
Base Balanced Security and Policy: Connectivity	Prevention v		Active Rules 9693 Alert 474 Block 9219
Base Policy \rightarrow Group Overrides	→ Recommendations Not in use →	Rule Overrides Summary	
Rule Overrides Ø			Back To Top
102 items All $\times \sim$	Rule Action V Search by CVE,	SID, Reference Info, or Rule Message	
All Rules 49,532 rules Presets: Alert (474) Block (9,219) Disabled (39,839) Overridden (0) Advanced Filters			
Overriden Rules		${\color{red} { $	
> MITRE (1 group)	GID:SID Rule Details	Rule Action 0 Set By	Assigned Groups
> Rule Categories (9 groups)	A 1:28496 BROWSER-IE Microsoft Internet	Reject V Rule Override	Malicious File,Drîve 🖷 🗯
	> 1:32478 BROWSER-IE Microsoft Internet	Alert (Default) V Base Policy	Malicious File, Drîve 📲 📕
	> 1:32479 E BROWSER-IE Microsoft Internet	Alert (Default) V Base Policy	Malicious File,Drive 🖥 🇯
	> 1:26633 BROWSER-IE Microsoft Internet	Alert (Default) V Base Policy	Malicious File,Inter 🖷 🗯

Changing the Rule Action

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

< Policies / Intrusion / FTD_Intrusion	~	Used by: No Access Control Policy No Zero Trust Application Policy No Device
Base Balanced Security and Mode: F Policy: Connectivity F F	Yrevention	Active Rules 9693 Alert 473 Block 9219 Others 1
Base Policy \rightarrow Group Overrides	→ Recommendations Not in use → Rule Overrides	Summary
Rule Overrides @		Back To Top
102 items All X Y	Rule Action V Search by CVE, SID, Reference In	nfo, or Rule Message
All Rules	1 rule Presets: Alert (0) Block (0) [Disabled (0) Overridden (1) Advanced Filters Reject (1)
	GID:SID Rule Details Rule Action	Set By Assigned Groups
Overriden Rules	> 1:28496 E BROWSER-IE Microsoft Internet	✓ V Rule Override Malicious File, Drive
> MITRE (1 group))	
> Rule Categories (9 groups)		

Overridden Rules