Configure Additional Snort 3 Rule Actions on FMC

Contents

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.

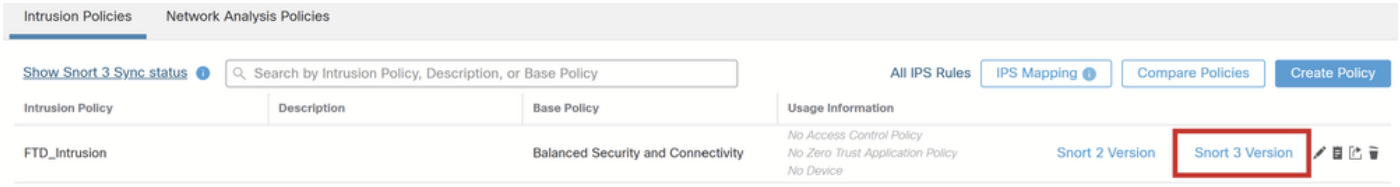
Drop: Generates event, drops matching packet and does not block further traffic in this connection.

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.

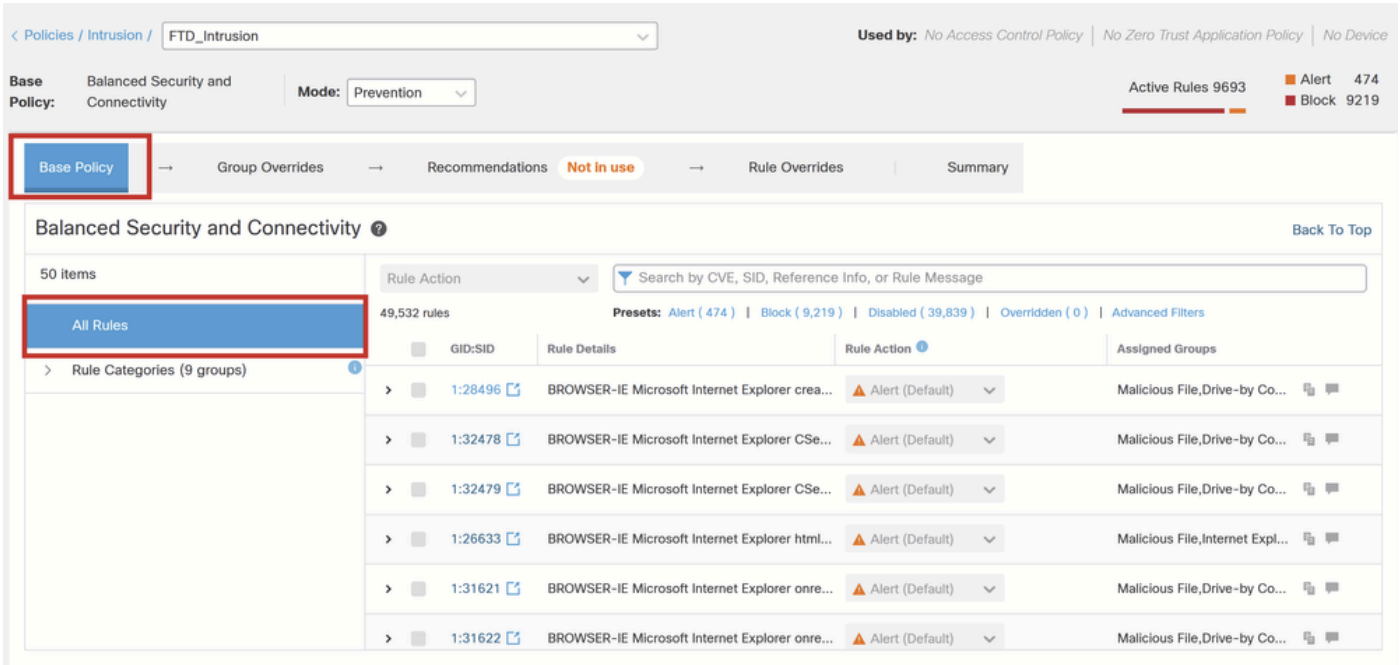
FMC Walkthrough

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:



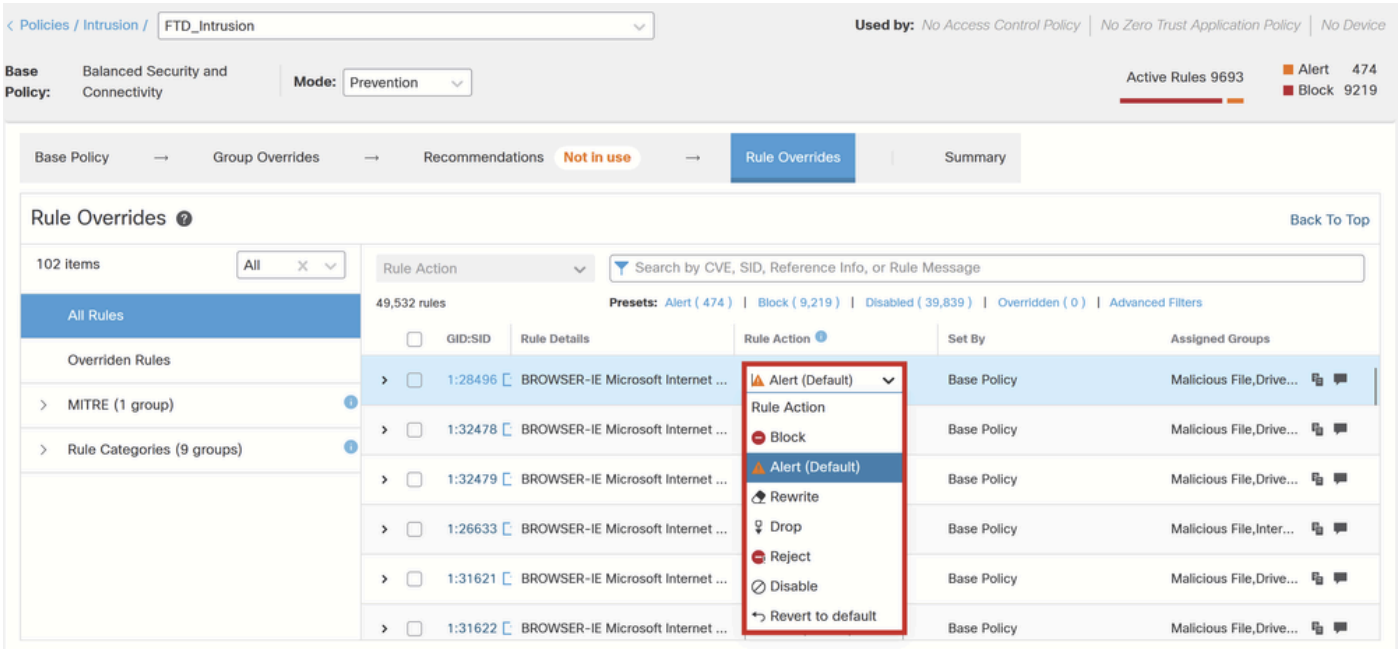
Snort 3 Version

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

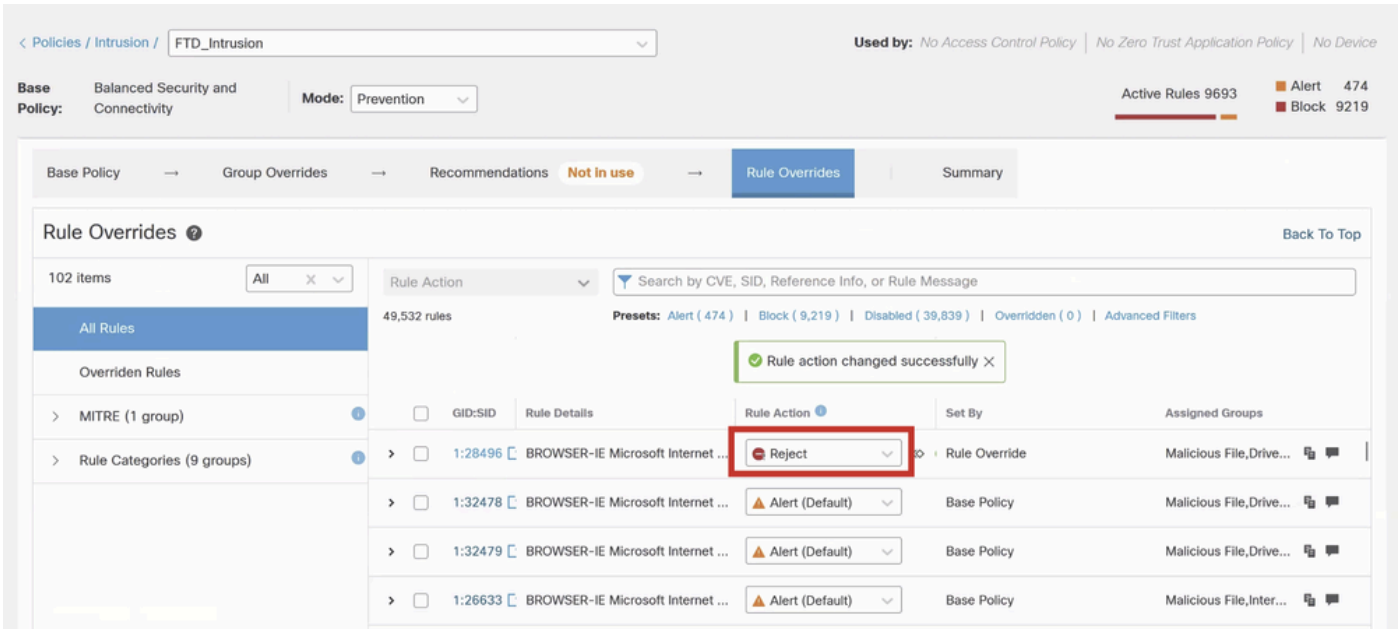


Base Policy

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.

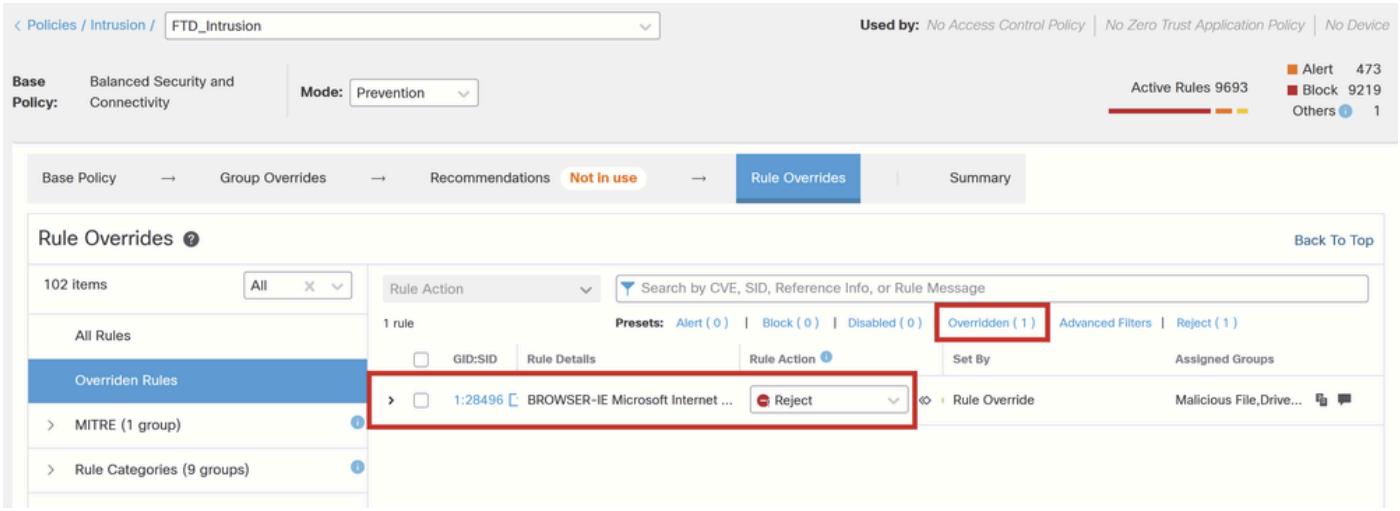


Additional Rule Actions



Changing the Rule Action

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



Overridden Rules