

Configure Custom Local Snort Rules in Snort3 on FTD

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Network Diagram](#)

[Configuration](#)

[Method 1. Import from Snort 2 to Snort 3](#)

[Step 1. Confirm Snort Version](#)

[Step 2. Create or Edit a Custom Local Snort Rule in Snort 2](#)

[Step 3. Import Custom Local Snort Rules from Snort 2 to Snort 3](#)

[Step 4. Change Rule Action](#)

[Step 5. Confirm Imported Custom Local Snort Rule](#)

[Step 6. Associate Intrusion Policy with Access Control Policy \(ACP\) Rule](#)

[Step 7. Deploy Changes](#)

[Method 2. Upload a Local File](#)

[Step 1. Confirm Snort version](#)

[Step 2. Create a Custom Local Snort Rule](#)

[Step 3. Upload the Custom Local Snort Rule](#)

[Step 4. Change Rule Action](#)

[Step 5. Confirm Uploaded Custom Local Snort Rule](#)

[Step 6. Associate Intrusion Policy with Access Control Policy \(ACP\) Rule](#)

[Step 7. Deploy Changes](#)

[Verify](#)

[Step 1. Set Contents of File in HTTP Server](#)

[Step 2. Initial HTTP Request](#)

[Step 3. Confirm Intrusion Event](#)

[Frequently Asked Questions \(FAQ\)](#)

[Troubleshoot](#)

[Reference](#)

Introduction

This document describes the procedure to configure Custom Local Snort Rules in Snort3 on Firewall Threat Defense (FTD).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Firepower Management Center (FMC)
- Firewall Threat Defense (FTD)

Components Used

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

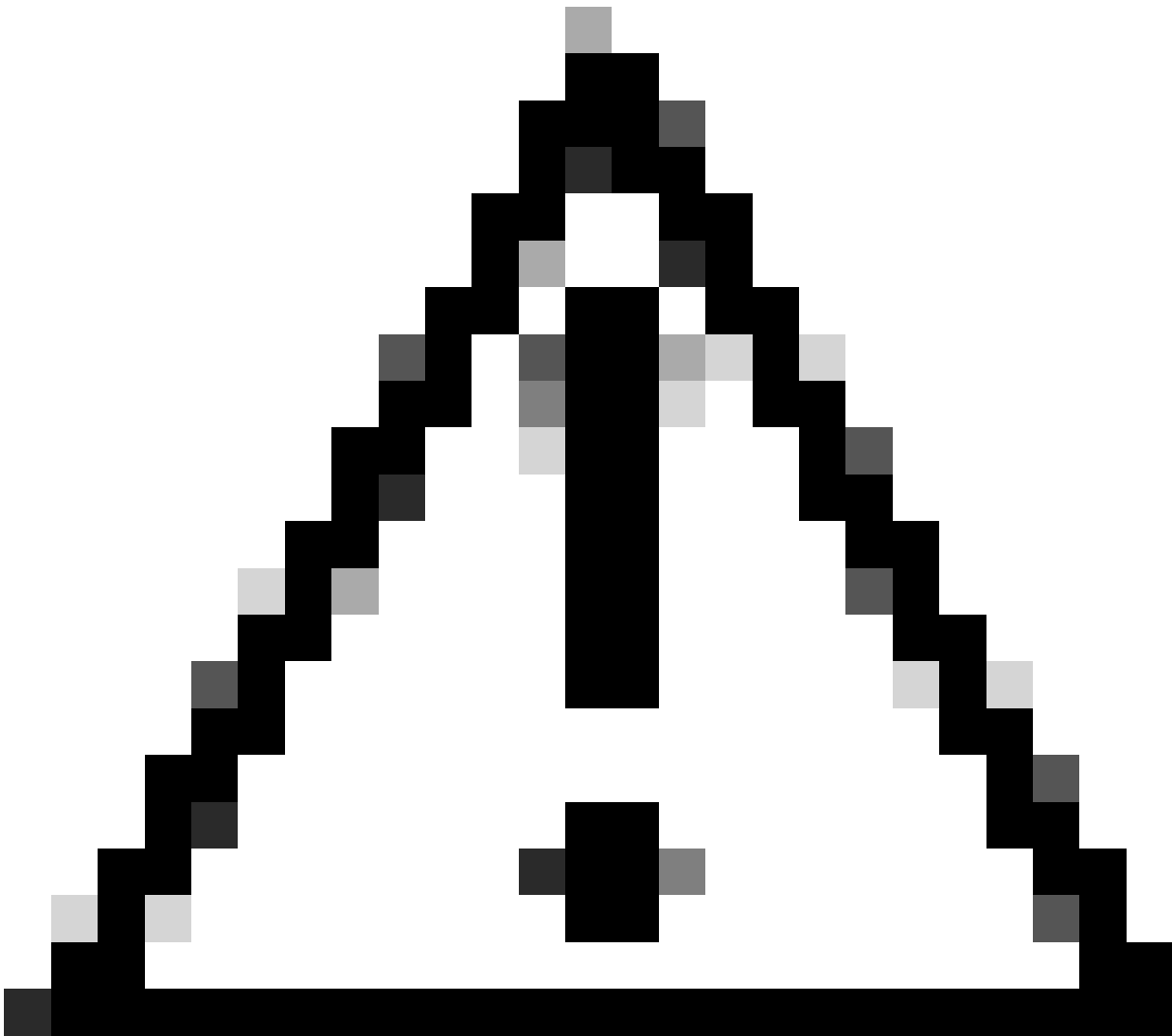
- Cisco Firepower Management Center for VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

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.

Background Information

Support for Snort 3 in threat defense with management center begins in version 7.0. For new and reimaged devices of version 7.0 and later, Snort 3 is the default inspection engine.

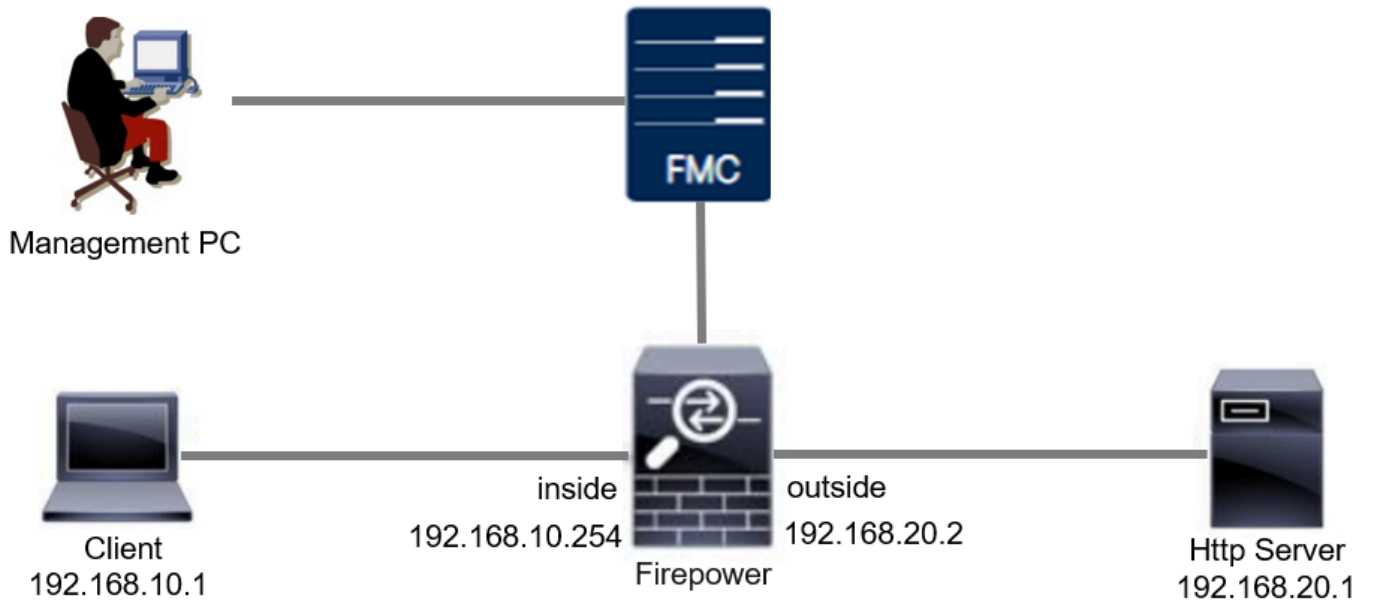
This document provides an example of how to customize Snort rules for Snort 3, as well as a practical verification example. Specifically, you are introduced how to configure and verify an Intrusion Policy with a customized Snort rule to drop HTTP packets that contain a certain string (username).



Caution: Creating Custom Local Snort Rules and providing support for them falls outside of TAC support coverage. Therefore, this document can be used as a reference only, and ask that you create and manage these custom rules at your own discretion and responsibility.

Network Diagram

This document introduces the configuration and verification for Custom Local Snort Rule in Snort3 on this diagram.



Network Diagram

Configuration

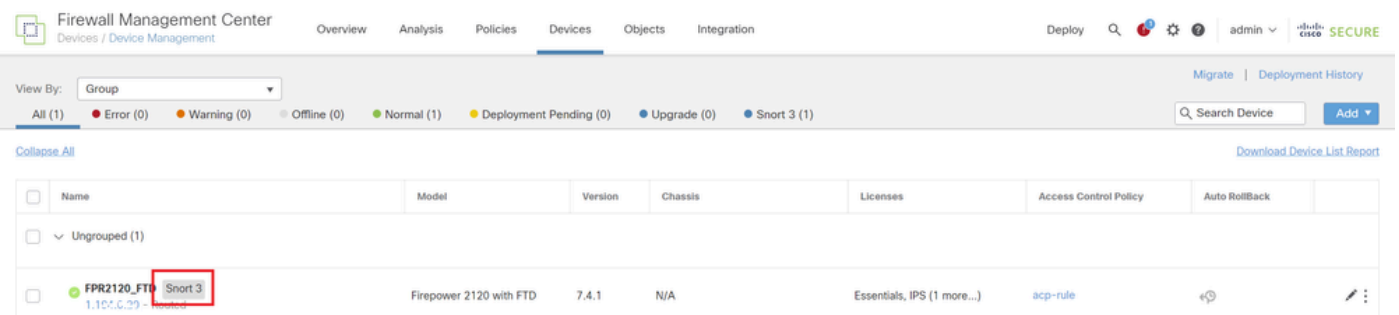
This is the configuration of Custom Local Snort Rule to detect and drop HTTP response packets containing a specific string (username).

Note: As of now, it is not possible to add Custom Local Snort Rules from the Snort 3 All Rules page in the FMC GUI. You must use the method introduced in this document.

Method 1. Import from Snort 2 to Snort 3

Step 1. Confirm Snort Version

Navigate to **Devices > Device Management** on FMC, click **Device** tab. Confirm that the snort version is Snort3.



The screenshot shows the Firepower Management Center (FMC) GUI. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is active. Below the navigation bar, there are filters for 'View By: Group' and a status bar showing 'All (1)', 'Error (0)', 'Warning (0)', 'Offline (0)', 'Normal (1)', 'Deployment Pending (0)', 'Upgrade (0)', and 'Snort 3 (1)'. A search bar and 'Add' button are also present. Below the filters, there is a table with columns: Name, Model, Version, Chassis, Licenses, Access Control Policy, and Auto RollBack. The table contains one entry: 'FPR2120_FTD' with a 'Snort 3' version, which is highlighted with a red box. The table also shows 'Firepower 2120 with FTD', '7.4.1', 'N/A', 'Essentials, IPS (1 more...)', and 'acp-rule'.

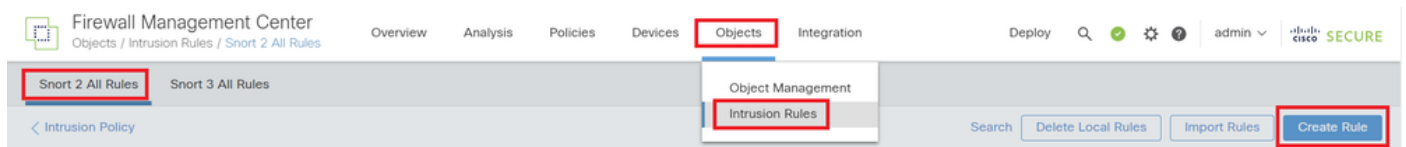
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FPR2120_FTD	Firepower 2120 with FTD	7.4.1	N/A	Essentials, IPS (1 more...)	acp-rule	

Step 2. Create or Edit a Custom Local Snort Rule in Snort 2

Navigate to **Objects > Intrusion Rules > Snort 2 All Rules** on FMC. Click **Create Rule** button to add a Custom Local Snort Rule, or Navigate to **Objects > Intrusion Rules > Snort 2 All Rules > Local Rules** on FMC, click **Edit** button to edit an existing Custom Local Snort Rule.

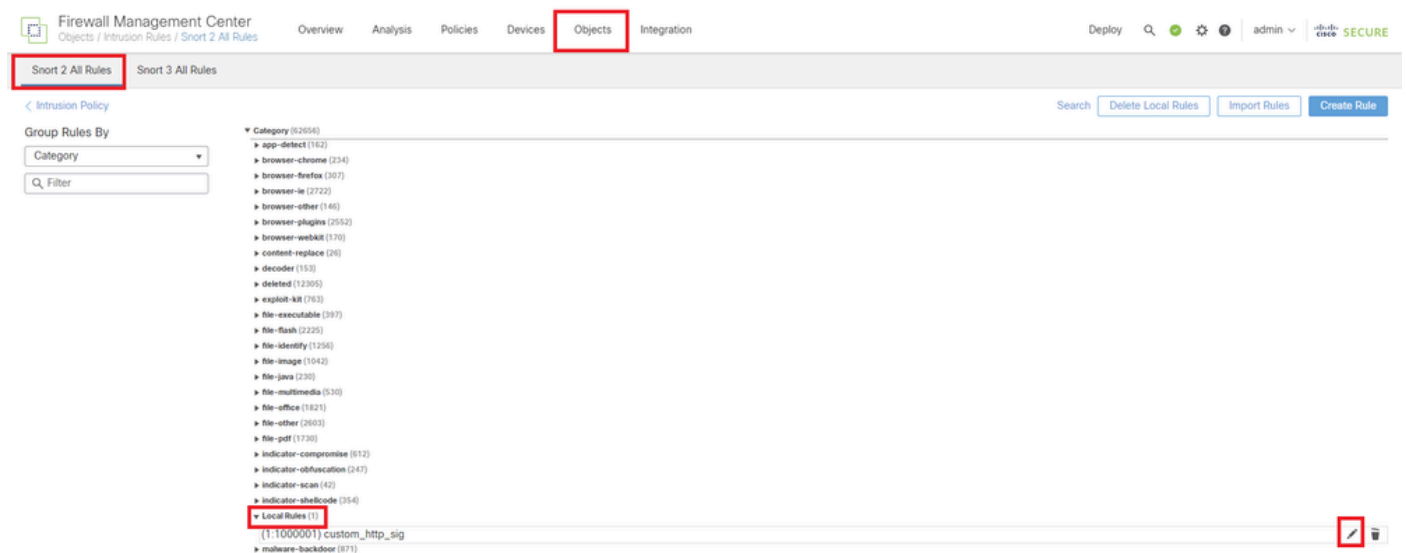
For instructions on how to create Custom Local Snort Rules in Snort 2, please refer to [Configure Custom Local Snort Rules in Snort2 on FTD](#).

Add a new Custom Local Snort Rule as show in the image.



Add a New Custom Rule

Edit an existing Custom Local Snort Rule as show in the image. In this example, edits an existing custom rule.



Edit an Existing Custom Rule

Enter the signature information to detect HTTP packets containing a specific string (username).

- **Message** : custom_http_sig
- **Action** : alert
- **Protocol** : tcp
- **flow** : Established, To Client
- **content** : username (Raw Data)

Firewall Management Center
Objects / Intrusion Rules / Create

Overview Analysis Policies Devices **Objects** Integration

Deploy Search | Upload Update | Intrusion

Snort 2 All Rules Snort 3 All Rules

Edit Rule 1:1000000:3 (Rule Comment)

Message: custom_http_sig

Classification: Unknown Traffic

Action: alert

Protocol: tcp

Direction: Bidirectional

Source IPs: any Source Port: any

Destination IPs: any Destination Port: any

Detection Options

flow: Established To Client

content: username

Case Inensitive: Not: Raw Data:

HTTP URI: HTTP Header: HTTP Cookie: HTTP Raw URI: HTTP Raw Header: HTTP Raw Cookie: HTTP Method: HTTP Client Body: HTTP Status Message: HTTP Status Code:

Distance: Within: Offset: Depth:

Use Fast Pattern Matcher: Fast Pattern Matcher Only: Fast Pattern Matcher Offset and Length:

ack Add Option Save Save As New

Input Necessary Info for Rule

Step 3. Import Custom Local Snort Rules from Snort 2 to Snort 3

Navigate to **Objects > Intrusion Rules > Snort 3 All Rules > All Rules** on FMC, click **Convert Snort 2 rules and Import** from **Tasks** pulldown list.

Firewall Management Center
Objects / Intrusion Rules / Snort 3 All Rules

Overview Analysis Policies Devices **Objects** Integration

Deploy Search | Upload Update | Intrusion

Snort 2 All Rules Snort 3 All Rules

< Intrusion Policy Back To Top

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Actions Search by CVE, SID, Reference Info, or Rule Message Tasks

50,094 rules

<input type="checkbox"/>	OID:SID	Info	Rule Action	Assigned Groups
>	148:2	(cip) CIP data is non-conforming to ODVA standard	Disable (Default)	Builtins
>	133:3	(dce_smb) SMB - bad SMB message type	Disable (Default)	Builtins

Upload Snort 3 rules

Convert Snort 2 rules and Import

Convert Snort 2 rules and download

Add Rule Groups

Import Custom Rule to Snort 3

Check the warning message and click **OK**.

Convert Snort 2 rules and import



The Snort 2 local rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. This action will convert all Snort 2 local rules to Snort 3 rules. All the enabled rules per the Snort 2 version of the policy will be added into different groups and enabled in the corresponding Snort 3 version of the policy.

Cancel

OK

Warning Message

Navigate to **Objects > Intrusion Rules > Snort 3 All Rules** on FMC, click **All Snort 2 Converted Global** to confirm the imported Custom Local Snort Rule.

The screenshot shows the Fire Management Center interface. The breadcrumb path is **Objects / Intrusion Rules / Snort 3 All Rules**. The main content area is titled **Local Rules / All Snort 2 Converted Global**. A notification message states: **The custom rules were successfully imported**. Below this, a table lists the rules:

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups	Alert Configuration
<input checked="" type="checkbox"/>	2000:1000000	custom_http_sig	Disable (Default)	All Snort 2 Converted Glo...	None

Confirm Imported Custom Rule

Step 4. Change Rule Action

Click **Per Intrusion Policy** according to the Rule Action of the target custom rule.

Firewall Management Center
Objects / Intrusion Rules / Snort 3 All Rules

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ admin 🔒 SECURE

Snort 2 All Rules Snort 3 All Rules

< Intrusion Policy Back To Top

All Rules

- Local Rules (1 group)
 - All Snort 2 Converted Global
 - MITRE (1 group)
 - Rule Categories (9 groups)

Local Rules / All Snort 2 Converted Global

Description Group created for custom rules enabled in snort 2 version

Rule Actions Search by CVE, SID, Reference Info, or Rule Message Tasks

1 rule

✔ The custom rules were successfully imported X

GID:SID	Info	Rule Action	Assigned Groups	Alert Configuration
2000:1000000	custom_http_sig	Disable (Default) (Overridden)	All Snort 2 Converted Glo...	None

Block
Alert
Rewrite
Drop
Pass
Reject
Disable (Default)
Revert to default
Per Intrusion Policy

Change Rule Action

In the **Edit Rule Action** screen, enter the information for the **Policy** and **Rule Action**.

- **Policy** : snort_test
- **Rule Action** : BLOCK



Note: Rule actions are:

Block— Generates event, blocks current matching packet and all the subsequent packets in this connection.

Alert— Generates only events for matching packet and does not drop packet or connection.

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

Pass— No events are 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 if it is a TCP protocol to source and destination hosts.

Disable—Does not match traffic against this rule. No events are generated.

Default—Reverts to the system default action.

2000:100... | custom_http_sig

All Policies
 Per Intrusion Policy

Policy:
 Rule Action:

[Add Another](#)

Comments (optional)

[Cancel](#) [Save](#)

Edit Rule Action

Step 5. Confirm Imported Custom Local Snort Rule

Navigate to **Policies > Intrusion Policies** on FMC, click **Snort 3 Version** corresponding to the target Intrusion Policy in the row.

Firewall Management Center

Policies / Access Control / Intrusion / Intrusion Policies

Overview Analysis **Policies** Devices Objects Integration Deploy Search Admin

Intrusion Policies Network Analysis Policies

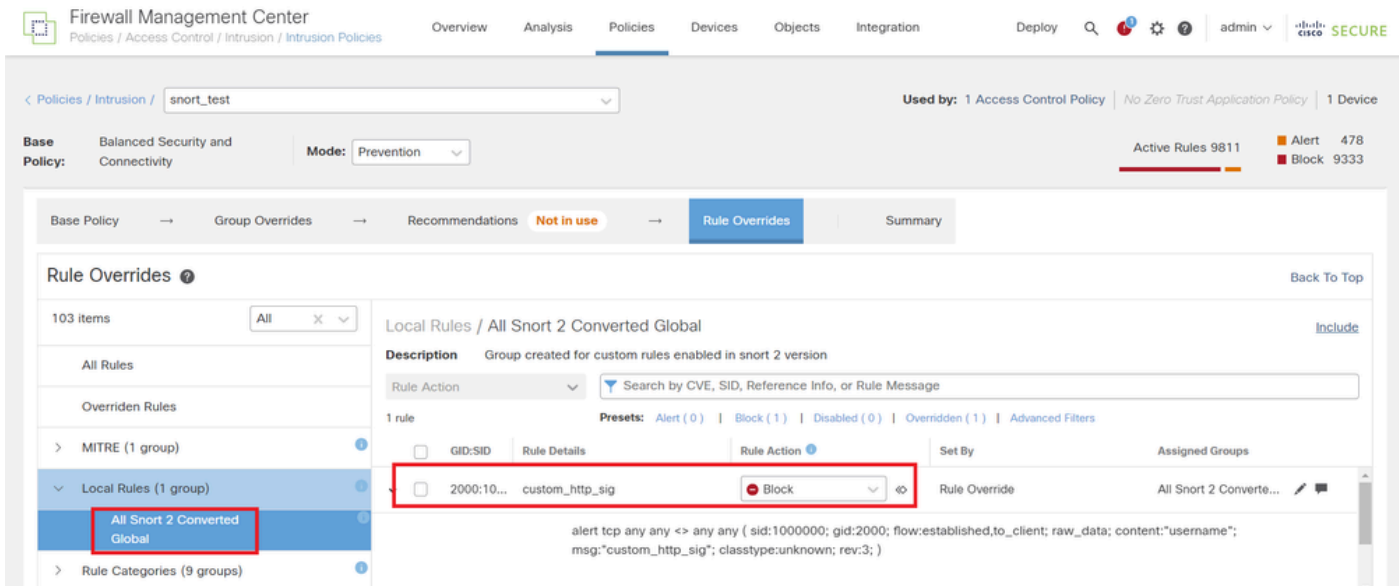
Hide Snort 3 Sync status Search by Intrusion Policy, Description, or Base Policy All IPS Rules IPS Mapping Compare Policies Create Policy

Intrusion Policy	Description	Base Policy	Usage Information
<input checked="" type="checkbox"/> snort_test → Snort 3 is in sync with Snort 2. 2024-01-12	Balanced Security and Connectivity		1 Access Control Policy No Zero Trust Application Policy 1 Device

Snort 2 Version **Snort 3 Version**

Confirm Imported Custom Rule

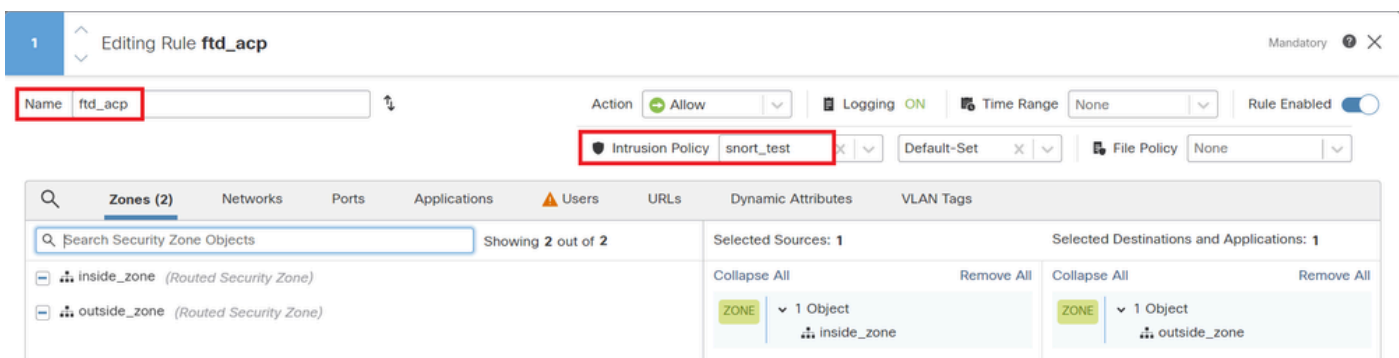
Click **Local Rules > All Snort 2 Converted Global** to check the details of the Custom Local Snort Rule.



Confirm Imported Custom Rule

Step 6. Associate Intrusion Policy with Access Control Policy (ACP) Rule

Navigate to **Policies > Access Control** on FMC, associate Intrusion Policy with ACP.



Associate with ACP Rule

Step 7. Deploy Changes

Deploy the changes to FTD.



Deploy Changes

Method 2. Upload a Local File

Step 1. Confirm Snort version

Same as Step 1 in Method 1.

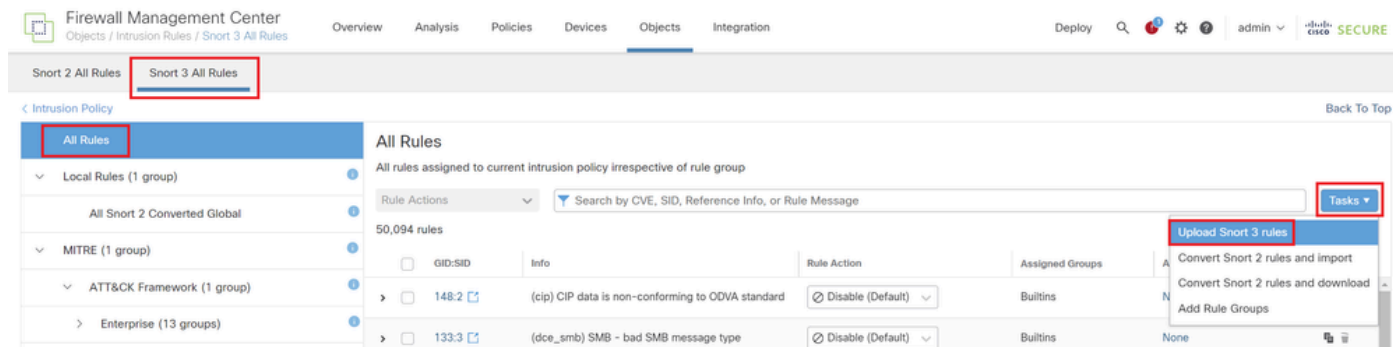
Step 2. Create a Custom Local Snort Rule

Manually create a Custom Local Snort Rule and save it in a local file named custom-rules.txt.

```
alert tcp any any <> any any ( sid:1000000; flow:established,to_client; raw_data; content:"username"; m
```

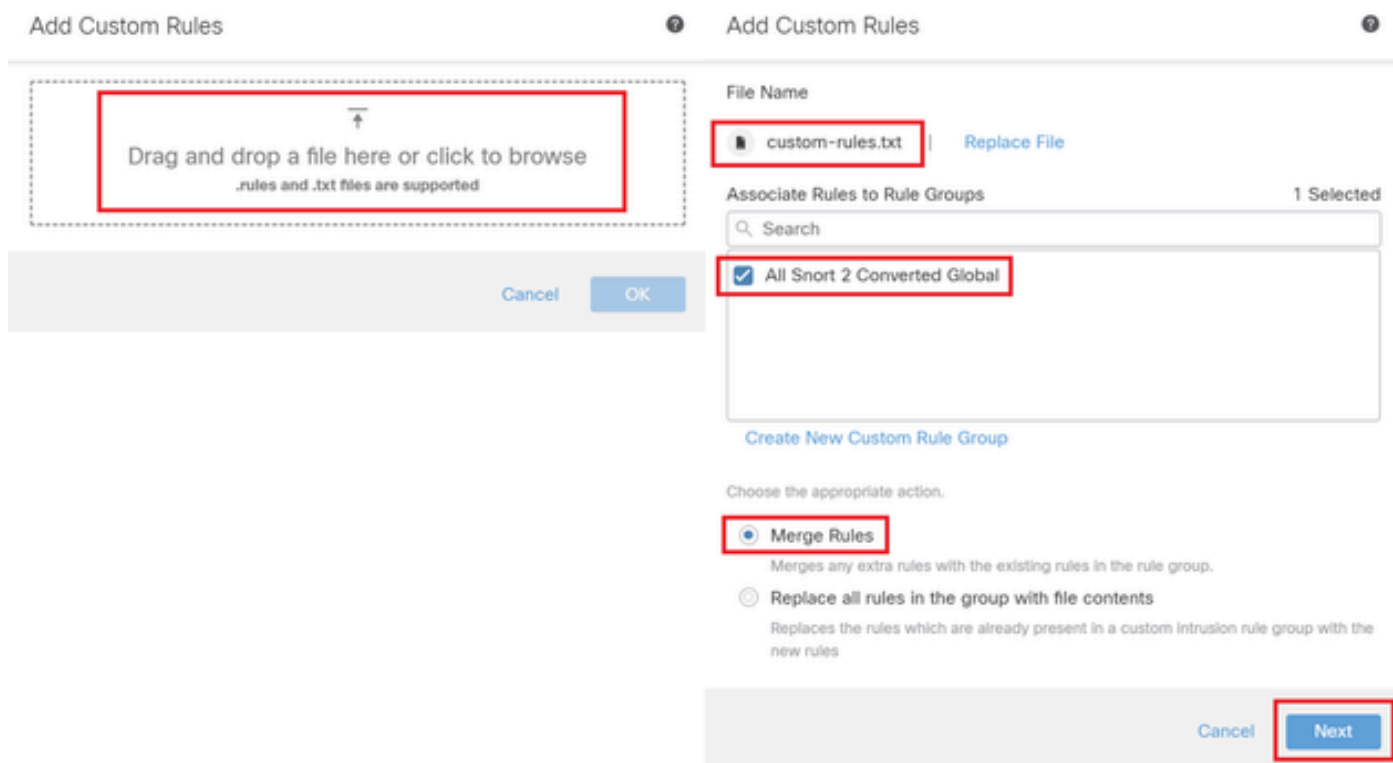
Step 3. Upload the Custom Local Snort Rule

Navigate to **Objects > Intrusion Rules > Snort 3 All Rules > All Rules** on FMC, click **Upload Snort 3 rules** from **Tasks** pulldown list.



Upload Custom Rule

In the Add Custom Rules screen, drag and drop the local custom-rules.txt file, select the **Rule Groups** and the **Appropriate Action** (Merge Rules in this example), and then click the **Next** button.



Add Custom Rule

Confirm that the local rule file has been successfully uploaded.

Add Custom Rules



Summary

✓ 1 new rule

2000:1000000

Download the summary file.

Back

Finish

Confirm Upload Result

Navigate to **Objects > Intrusion Rules > Snort 3 All Rules** on FMC, click **All Snort 2 Converted Global** to confirm the uploaded Custom Local Snort Rule.

The screenshot shows the Firewall Management Center interface. The breadcrumb navigation is **Objects > Intrusion Rules > Snort 3 All Rules**. The page title is **Snort 3 All Rules**. The left sidebar shows a tree view of rule groups, with **All Snort 2 Converted Global** selected. The main content area shows the configuration for this rule group. The **Description** is "Group created for custom rules enabled in snort 2 version". The **Rule Actions** are set to "Disable (Default)". The **Alert Configuration** is set to "None". The **Alert Message** is "alert tcp any any -> any any (sid:1000000; gid:2000; flow.established.to_client; raw_data; content:'username'; msg:'custom_http_sig'; classtype:unknown; rev:3;)".

Detail of Custom Rule

Step 4. Change Rule Action

Same as Step 4 in Method 1.

Step 5. Confirm Uploaded Custom Local Snort Rule

Same as Step 5 in Method 1.

Step 6. Associate Intrusion Policy with Access Control Policy (ACP) Rule

Same as Step 6 in Method 1.

Step 7. Deploy Changes

Same as Step 7 in Method 1.

Verify

Step 1. Set Contents of File in HTTP Server

Set the contents of the test.txt file on HTTP server side to username.

Step 2. Initial HTTP Request

Access the HTTP Server (192.168.20.1/test.txt) from the browser of the client (192.168.10.1) and confirm that the HTTP communication is blocked.



Initial HTTP Request

Step 3. Confirm Intrusion Event

Navigate to **Analysis > Intrusions > Events** on FMC, confirm the Intrusion Event is generated by the Custom Local Snort Rule.

A screenshot of the Cisco Firepower Management Center (FMC) interface. The 'Analysis' tab is selected. The main area shows 'Events By Priority and Classification' for the period 2024-04-06 13:26:03 to 2024-04-06 14:31:12. A table of events is displayed, with one event highlighted. The event details are as follows:

Time	Priority	Impact	Inline Result	Reason	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	VLAN ID	Message	Classification	Generated
2024-04-06 14:30:48	low	Unknown	Block		192.168.20.1		192.168.10.1		80 (http) / tcp	50103 / tcp			custom_http_sig (2000:1000000:3)	Unknown Traffic	Standard

Intrusion Event

Click **Packet** tab, confirm the detail of Intrusion Event.

Detail of Intrusion Event

Frequently Asked Questions (FAQ)

Q : Which is recommended, Snort 2 or Snort 3 ?

A : Compared to Snort 2, Snort 3 offers improved processing speeds and new features, making it the more recommended option.

Q : After upgrading from a version of FTD prior to 7.0 to a version 7.0 or later, does the snort version get automatically updated to Snort 3 ?

A : No, the inspection engine remains on Snort 2. To use Snort 3 after the upgrade, you must explicitly enable it. Note that Snort 2 is planned to be deprecated in a future release and you are strongly recommended to stop using it now.

Q : In Snort 3, is it possible to edit an existing custom rule ?

A : No, you can not edit it. To edit a specific custom rule, you must delete the relevant rule and recreate it.

Troubleshoot

Run `system support trace` command to confirm the behavior on FTD. In this example, the HTTP traffic is blocked by the IPS rule (2000:1000000:3).

```
<#root>
```

```
>
```

```
system support trace
```

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.1
Please specify a client port:
Please specify a server IP address: 192.168.20.1
Please specify a server port:
```

```
192.168.10.1 50104 -> 192.168.20.1 80 6 AS=0 ID=4 GR=1-1 Firewall: allow rule, '
```


ftd_acp

', allow

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1

Event

:

2000:1000000:3

, Action

block

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict Reason:

ips, block

Reference

[Cisco Secure Firewall Management Center Snort 3 Configuration Guide](#)