# Configure Custom Local Snort Rules in Snort2 on FTD

## Contents

## Introduction

This document describes the procedure to configure Custom Local Snort Rules in Snort2 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

Custom Local Snort Rule refers to a user-defined rule that you can create and implement within the Snort intrusion detection and prevention system that is integrated into the FTD. When you create a custom local Snort rule in Cisco FTD, you are essentially defining a new pattern or set of conditions that the Snort engine can watch for. If network traffic matches the conditions specified in your custom rule, Snort can take the action defined in the rule, such as generating an alert or dropping the packet. Administrators use custom local Snort rules to address specific threats that are not covered by the general rule sets.

In this document, you are introduced how to configure and verify a Custom Local Snort Rule designed to detect and drop HTTP response packets containing a specific string (username).

---

**Caution**: Creating Custom Local Snort Rules and providing support for them falls outside of TAC

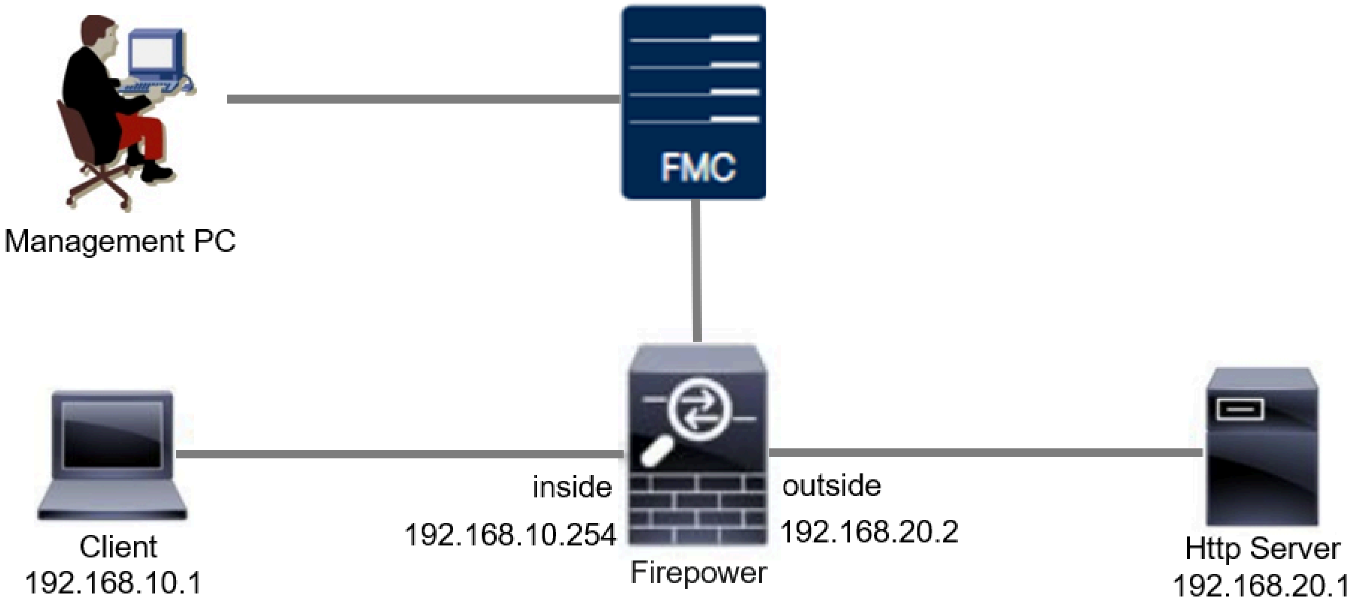
---

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.

# Configure

## Network Diagram

This document introduces the configuration and verification for Custom Local Snort Rule in Snort2 on this diagram.

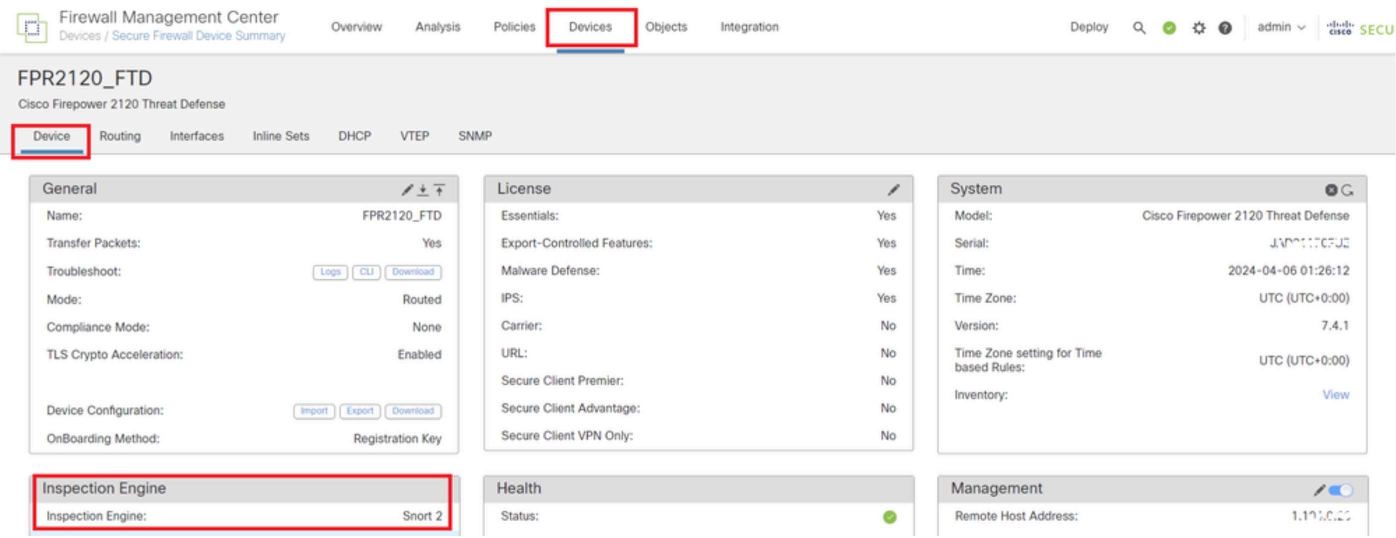


## Configuration

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

### Step 1. Confirm Snort Version

Navigate to **Devices** > **Device Management** on FMC, click **Device** tab. Confirming the snort version is Snort2.



Firewall Management Center
Devices / Secure Firewall Device Summary

FPR2120_FTD
Cisco Firepower 2120 Threat Defense

| General | |
|---|---|
| Name: | FPR2120_FTD |
| Transfer Packets: | Yes |
| Troubleshoot: | Logs CLI Download |
| Mode: | Routed |
| Compliance Mode: | None |
| TLS Crypto Acceleration: | Enabled |
| Device Configuration: | Import Export Download |
| OnBoarding Method: | Registration Key |

| License | |
|---|---|
| Essentials: | Yes |
| Export-Controlled Features: | Yes |
| Malware Defense: | Yes |
| IPS: | Yes |
| Carrier: | No |
| URL: | No |
| Secure Client Premier: | No |
| Secure Client Advantage: | No |
| Secure Client VPN Only: | No |

| System | |
|---|---|
| Model: | Cisco Firepower 2120 Threat Defense |
| Serial: | [redacted] |
| Time: | 2024-04-06 01:26:12 |
| Time Zone: | UTC (UTC+0:00) |
| Version: | 7.4.1 |
| Time Zone setting for Time based Rules: | UTC (UTC+0:00) |
| Inventory: | View |

| Inspection Engine | |
|---|---|
| Inspection Engine: | Snort 2 |

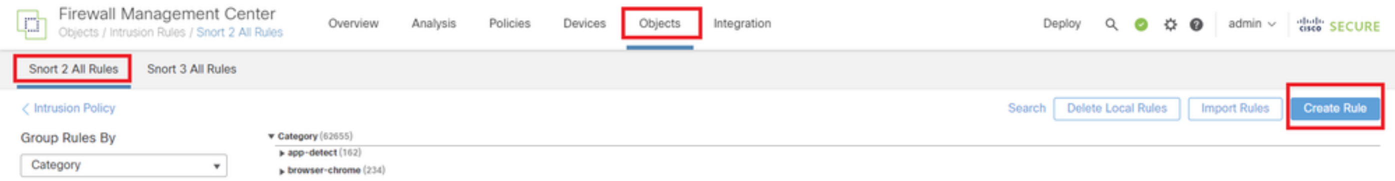
| Health | |
|---|---|
| Status: | ● |

| Management | |
|---|---|
| Remote Host Address: | [redacted] |

*Snort Version*

## Step 2. Create a Custom Local Snort Rule in Snort 2

Navigate to **Objects** > **Intrusion Rules** > **Snort 2 All Rules** on FMC, click **Create Rule** button.



Firewall Management Center
Objects / Intrusion Rules / Snort 2 All Rules

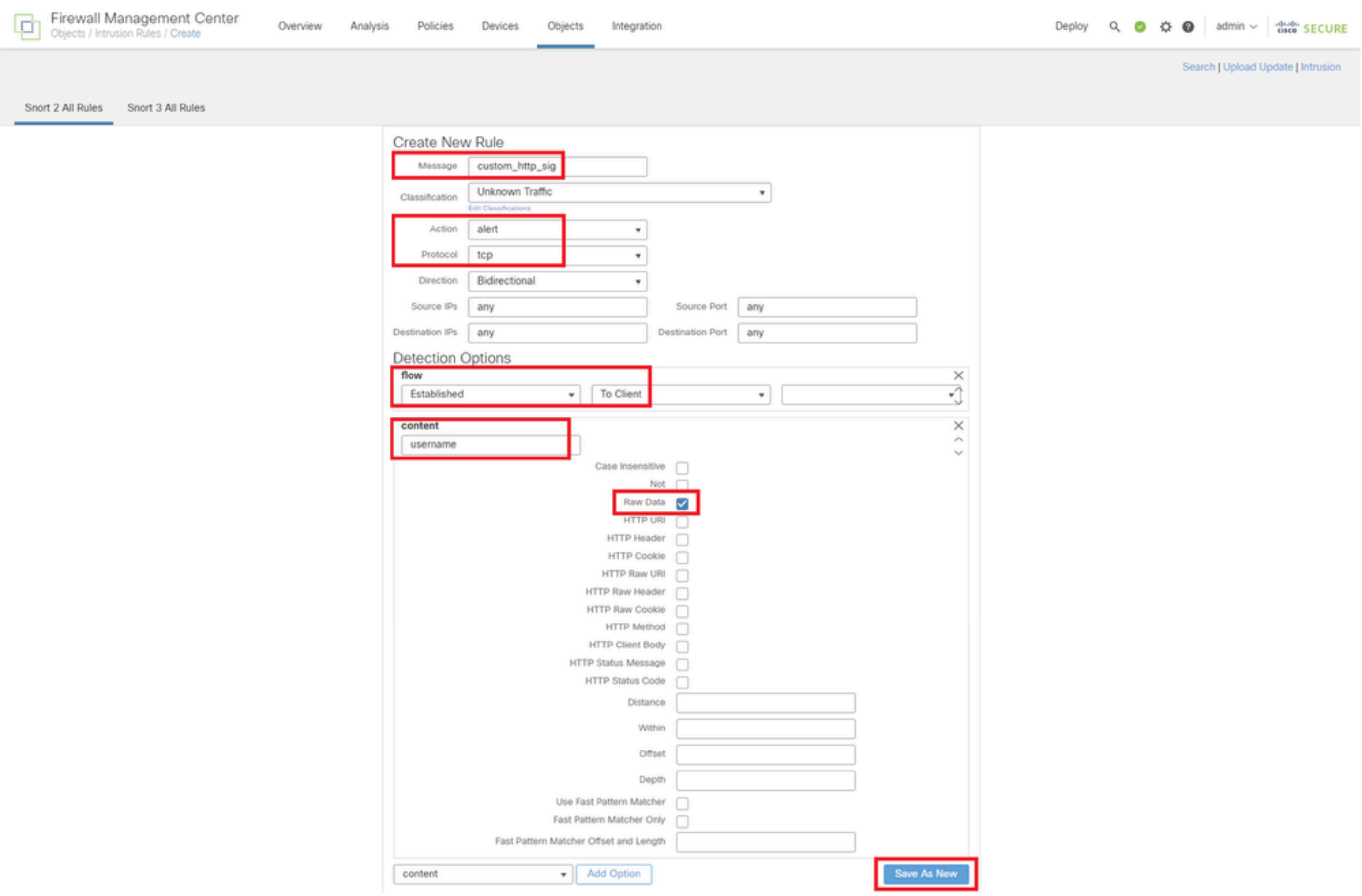
▾ Category (62655)
▸ app-detect (162)
▸ browser-chrome (234)

*Create Custom Rule*

Input necessary info for Custom Local Snort Rule.

- **Intrusion** : custom_http_sig
- **Action** : alert
- **Protocol** : tcp
- **flow** : Established, To Client

- **content** : username (Raw Data)



Create New Rule

Message: custom_http_sig

Classification: Unknown Traffic

Edit Classifications

Action: alert

Protocol: tcp

Direction: Bidirectional

Source IPs: any

Source Port: any

Destination IPs: any

Destination Port: any

Detection Options

flow: Established, To Client

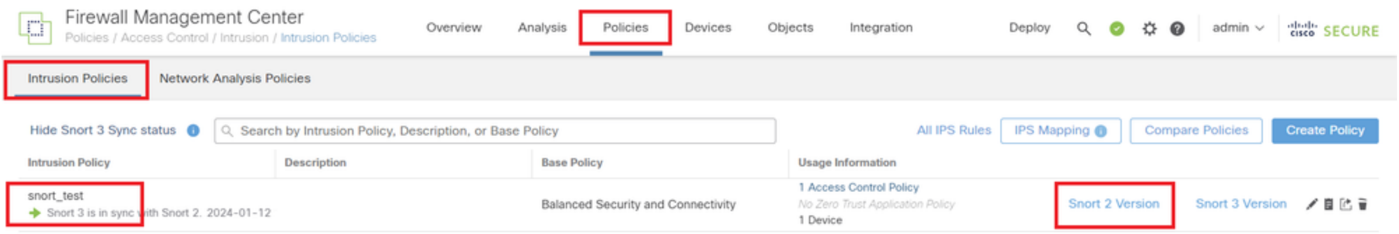
content: username

- Case Insensitive □
- 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

*Input Necessary Info for Rule*

## Step 3. Confirm Custom Local Snort Rule

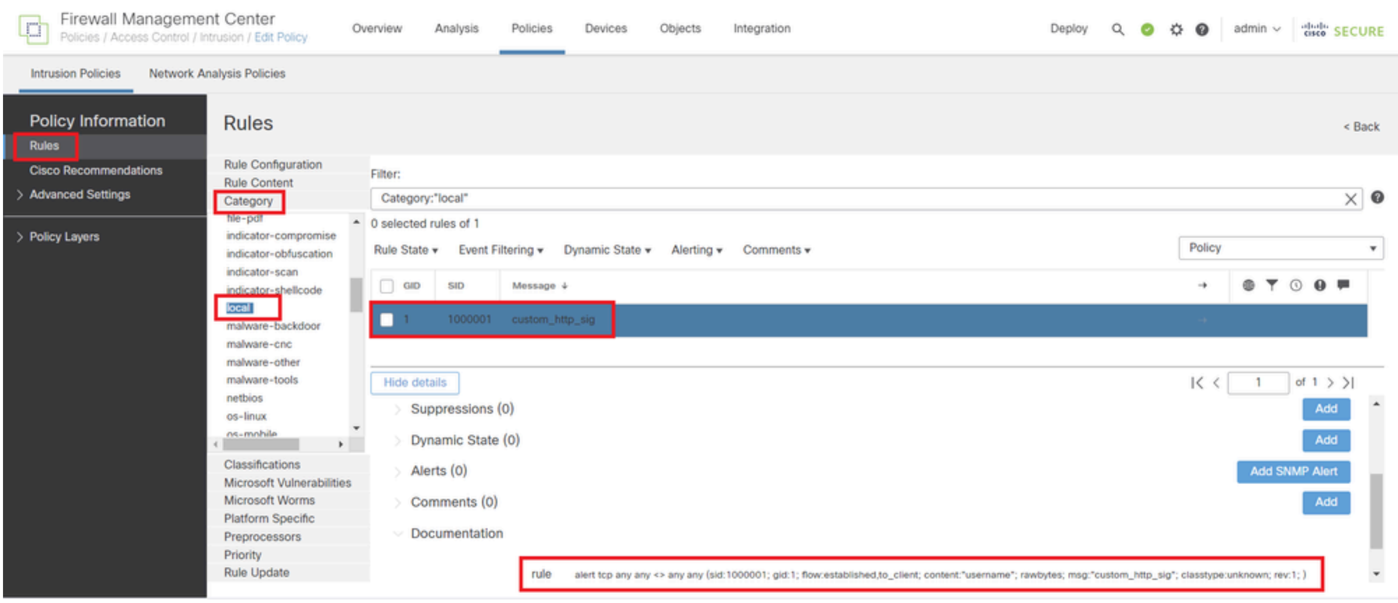
Navigate to **Policies > Intrusion Policies** on FMC, click **Snort 2 Version** button.


Firewall Management Center
Policies / Access Control / Intrusion / Intrusion Policies
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE
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 | | |
|---|---|---|---|---|---|
| snort_test<br>Snort 3 is in sync with Snort 2. 2024-01-12 | | Balanced Security and Connectivity | 1 Access Control Policy<br>No Zero Trust Application Policy<br>1 Device | Snort 2 Version | Snort 3 Version |

*Confirm Custom Rule*

Navigate to **Rules > Category > local** on FMC, confirm the detail of Custom Local Snort Rule.



Filter: Category:"local"

0 selected rules of 1

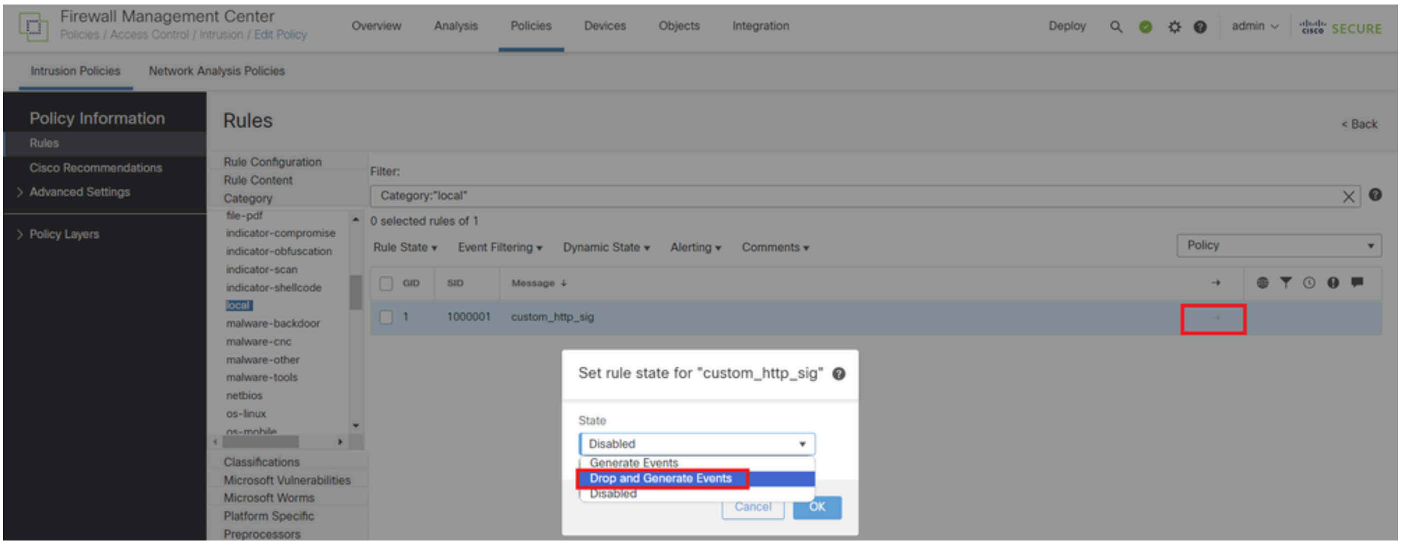
| GID | SID | Message |
|---|---|---|
| 1 | 1000001 | custom_http_sig |

rule alert tcp any any <> any any (sid:1000001; gid:1; flow:established,to_client; content:"username"; rawbytes; msg:"custom_http_sig"; classtype:unknown; rev:1; )

*Detail of Custom Rule*

## Step 4. Change Rule Action

Click **State** button, set the State to **Drop and Generate Events** and click **OK** button.



Filter: Category:"local"

0 selected rules of 1

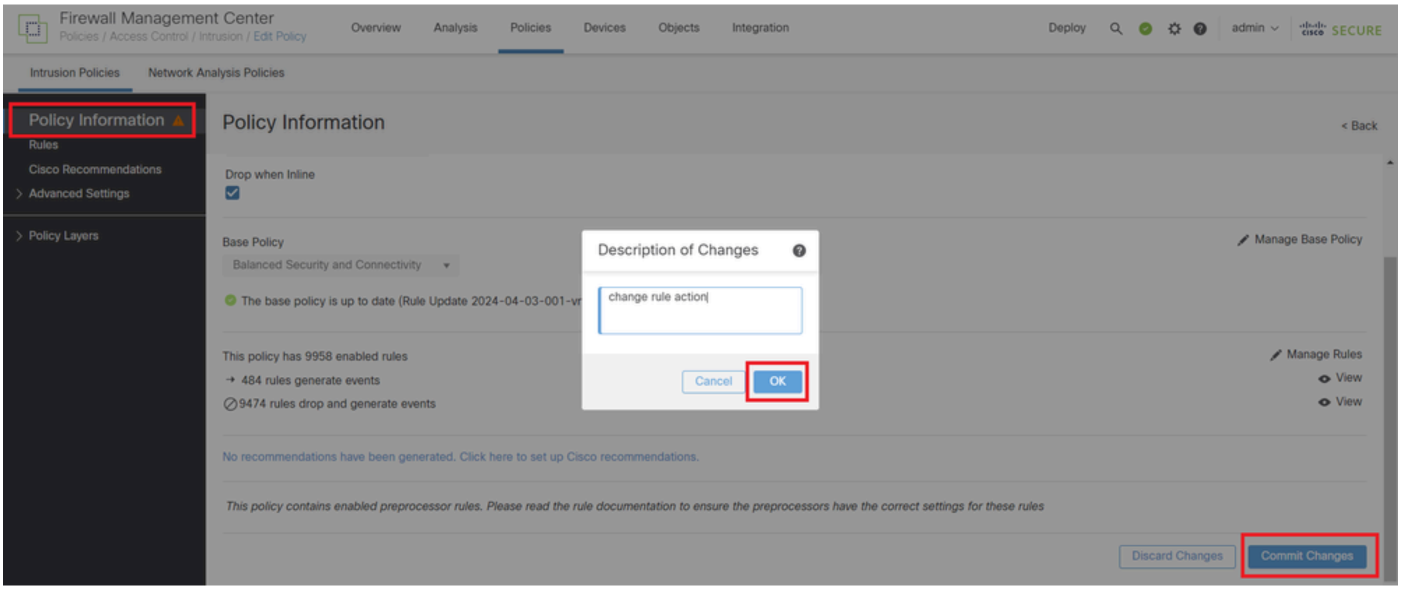
| GID | SID | Message |
|---|---|---|
| 1 | 1000001 | custom_http_sig |

Set rule state for "custom_http_sig"

State: Disabled

*Change the Rule Action*

Click **Policy Information** button, click **Commit Changes** button to save changes.



Policy Information

Drop when Inline ☑

Base Policy: Balanced Security and Connectivity

The base policy is up to date (Rule Update 2024-04-03-001-vr

This policy has 9958 enabled rules
484 rules generate events
9474 rules drop and generate events

No recommendations have been generated. Click here to set up Cisco recommendations.

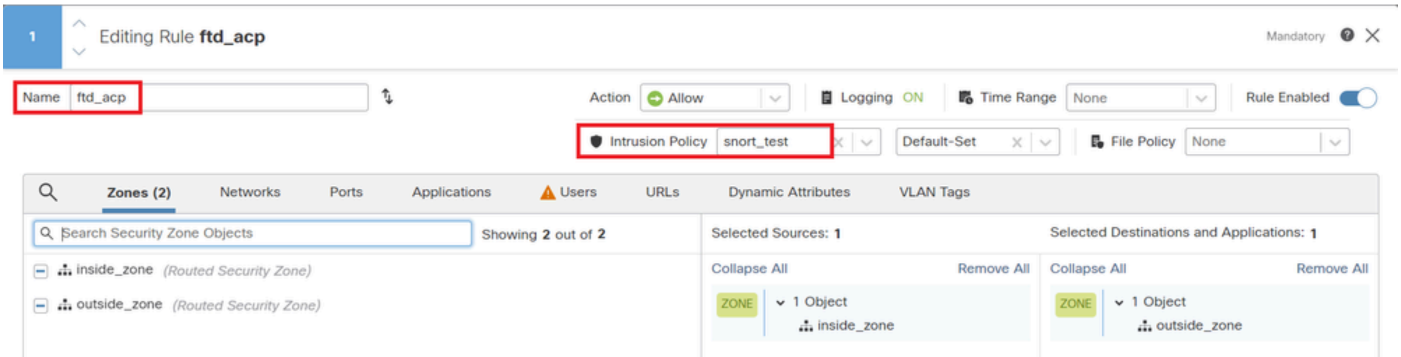
This policy contains enabled preprocessor rules. Please read the rule documentation to ensure the preprocessors have the correct settings for these rules

Description of Changes: change rule action

*Commit Changes*

### Step 5. Associate Intrusion Policy with Access Control Policy (ACP) Rule

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



Editing Rule **ftd_acp**

Name: ftd_acp
Action: Allow
Logging: ON
Time Range: None
Rule Enabled
Intrusion Policy: snort_test
Default-Set
File Policy: None

Showing 2 out of 2
inside_zone (Routed Security Zone)
outside_zone (Routed Security Zone)

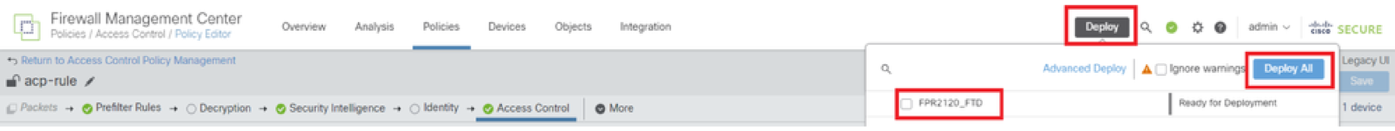
Selected Sources: 1
1 Object
inside_zone

Selected Destinations and Applications: 1
1 Object
outside_zone

*Associate with ACP Rule*

### Step 6. Deploy Changes

Deploy the changes to FTD.



acp-rule

□ FPR2120_FTD — Ready for Deployment

1 device

*Deploy Changes*

# Verify

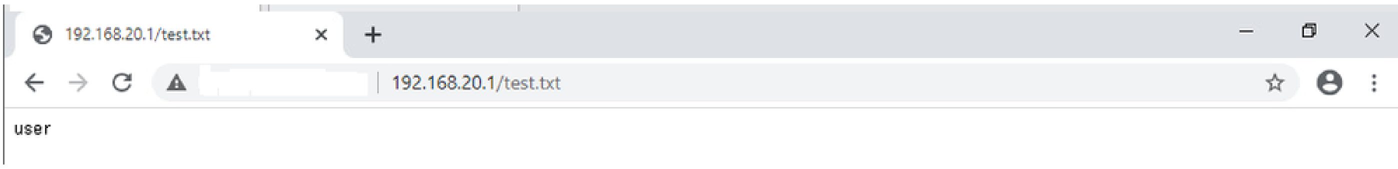
## Custom Local Snort Rule is Not Triggered

### Step 1. Set Contents of File in HTTP Server

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

### 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 permitted.



192.168.20.1/test.txt

192.168.20.1/test.txt

```
user
```

*Initial HTTP Request*

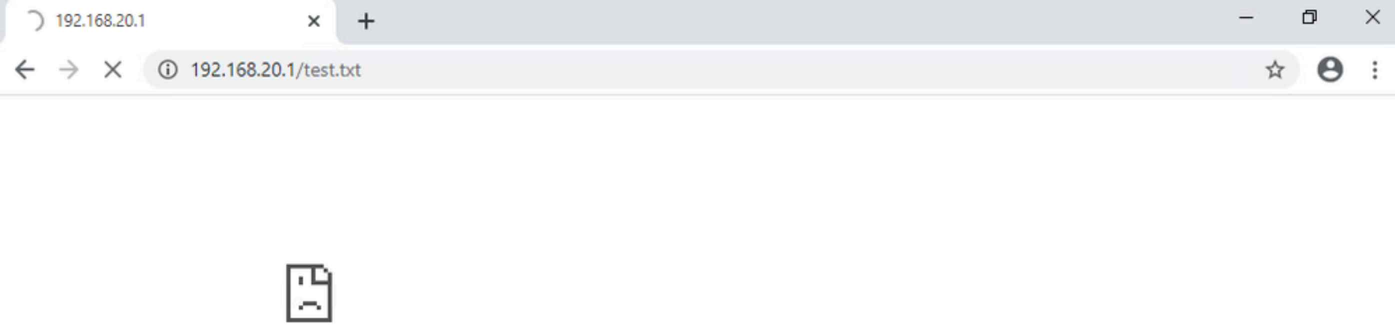
## Custom Local Snort Rule is Triggered

### 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.



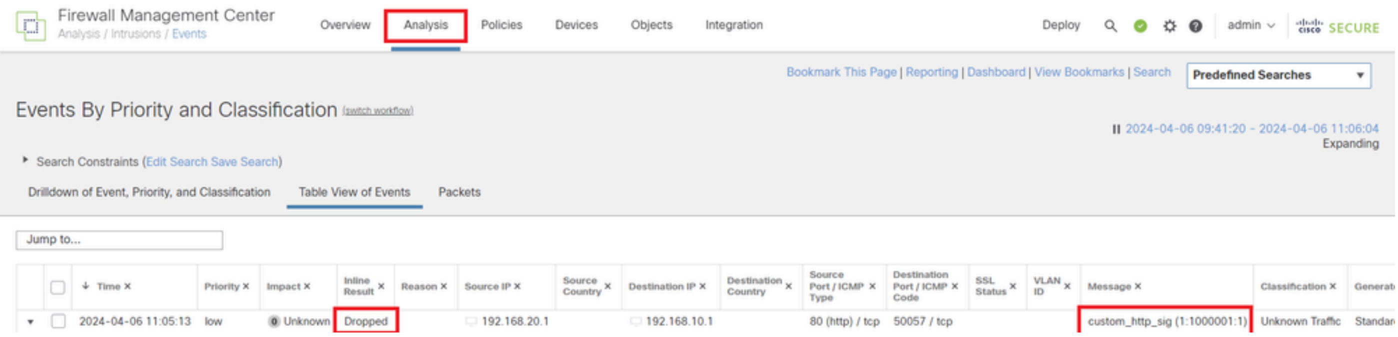
192.168.20.1

192.168.20.1/test.txt

*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.



Firewall Management Center
Analysis / Intrusions / Events
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE
Bookmark This Page | Reporting | Dashboard | View Bookmarks | Search
Predefined Searches
(switch workflow)
Search Constraints (Edit Search Save Search)
Drilldown of Event, Priority, and Classification
Table View of Events
Packets
Jump to...

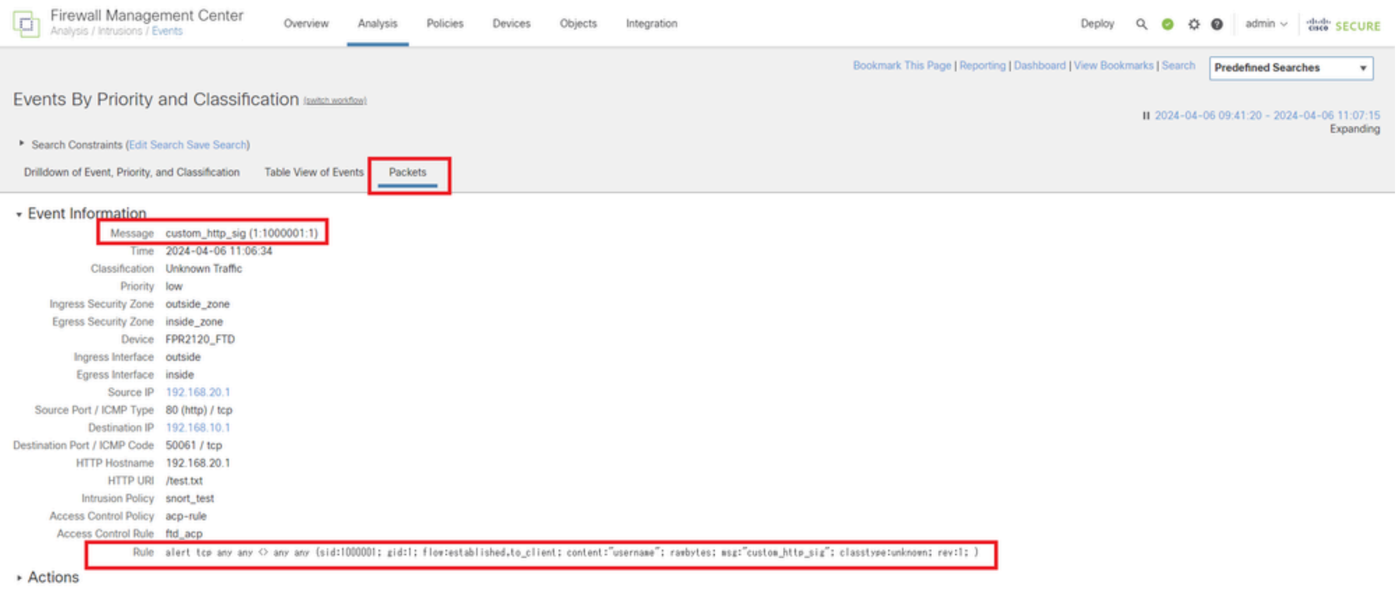
Events By Priority and Classification

2024-04-06 09:41:20 - 2024-04-06 11:06:04
Expanding

| | | 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 | Generat |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ▾ | □ | 2024-04-06 11:05:13 | low | 0 Unknown | Dropped | | 192.168.20.1 | | 192.168.10.1 | | 80 (http) / tcp | 50057 / tcp | | | custom_http_sig (1:1000001:1) | Unknown Traffic | Standar |

*Intrusion Event*

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


Firewall Management Center
Analysis / Intrusions / Events
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE
Bookmark This Page | Reporting | Dashboard | View Bookmarks | Search
Predefined Searches
Search Constraints (Edit Search Save Search)
Drilldown of Event, Priority, and Classification
Table View of Events
Packets
Actions

Events By Priority and Classification (switch workflow)

2024-04-06 09:41:20 - 2024-04-06 11:07:15
Expanding

Event Information

Message custom_http_sig (1:1000001:1)
Time 2024-04-06 11:06:34
Classification Unknown Traffic
Priority low
Ingress Security Zone outside_zone
Egress Security Zone inside_zone
Device FPR2120_FTD
Ingress Interface outside
Egress Interface inside
Source IP 192.168.20.1
Source Port / ICMP Type 80 (http) / tcp
Destination IP 192.168.10.1
Destination Port / ICMP Code 50061 / tcp
HTTP Hostname 192.168.20.1
HTTP URI /test.txt
Intrusion Policy snort_test
Access Control Policy acp-rule
Access Control Rule ftd_acp
Rule alert tcp any any <> any any (sid:1000001; gid:1; flow:established,to_client; content:"username"; rawbytes; msg:"custom_http_sig"; classtype:unknown; rev:1; )

*Detail of Intrusion Event*

# Troubleshoot

Run `system support trace` command to confirm the behavior on FTD. In this example, the HTTP traffic is blocked by the IPS rule (gid 1, sid 1000001).

<#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:

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Firewall: allow rule, '

ftd_acp

', allow
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0

IPS Event

:

gid 1

,

sid 1000001

, drop

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Snort id 3, NAP id 2, IPS id 1, Verdict BLOCKFLOW
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 ===>
```

Blocked by IPS