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
<u>Verify</u>
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.

Firewall Management Center Overview	Analysis Policies Dev	vices Obje	ects Integration		Deploy Q 💕 🌣	admin v dubb	SECURE
View By: Group • All (1) • Error (0) • Warning (0) • Offline (0) • No	rmal (1) • Deployment Per	nding (0)	Upgrade (0) Snort 3 (1)		٥	Migrate Deployment	History Add 🔻
Collapse All						Download Device	List Report
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (1)							
FPR2120_FT1 Snort 3 1.104.6.29 - Rooted	Firepower 2120 with FTD	7.4.1	N/A	Essentials, IPS (1 more)	acp-rule	«Ø	1

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 <u>Configure Custom</u> <u>Local Snort Rules in Snort2 on FTD</u>.

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.

Cipiects / Intrusion Rules / Snort	Center Overview Analysis Policies Devices Objects Integration	Deploy Q 📀 🌣 🚱 admin 🗸 📫 SECURE
Snort 2 All Rules Snort 3 All Rule	5	
< Intrusion Policy		Search Delete Local Rules Import Rules Create Rule
Group Rules By Category Category C, Filter	<pre> Cathgory(1006) Sepondet(1102) Soroase-cherme(230) Soroase-cherme(230) Soroase-cherme(230) Soroase-cherme(240) Soroas</pre>	
	indicate-components (012) indicate-oblyscation (247) indicate-oblyscation (247) indicate-shetcode (354) kodicate-shetcode (354) kodicate-shetcode (354) kodicate-shetcode (354) mathrare-backdoor ((71))	∠ ¥

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)

Chief Strewall Management Center Overview	w Analysis Policies Devices Objects Integration	Deploy Q 💕 🌣 🍘 admin 🗸 🕬 SECURE
		Search Upload Update Intrusion
Snort 2 All Rules Snort 3 All Rules		
	Edit Pule 1:1000000:2 (Rule Comment)	
	Message custom http sig	
	Lakeeure Troffe	
	Classification 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	Ç.
	Case Insensitive	
	Raw Data	
	HTTP Header	
	HTTP Cookie	
	HTTP Raw Header	
	HTTP Raw Cookle	
	HTTP Method	
	HTTP Client Body	
	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 I	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	Iverview Analysis Polici	es Devices Objects Integration		Deploy Q	🚱 🌣 🔕 admin 🗸 👘 SEC	CURE
Snort 2 All Rules Snort 3 All Rules						
< Intrusion Policy					Back	То Тор
All Rules	All Rules					
 Local Rules (1 group) 	 All rules assigned to current 	t intrusion policy irrespective of rule group				_
All Snort 2 Converted Global	Rule Actions	 Search by CVE, SID, Reference Info, 	or Rule Message		Tasks	s v
	50,094 rules				Upload Snort 3 rules	_
> MITRE (1 group)	GID:SID	Info	Rule Action	Assigned Groups	Convert Snort 2 rules and import	
> Rule Categories (9 groups)	• 148:2 [1	(cip) CIP data is non-conforming to ODVA stand	ard Ø Disable (Default)	Builtins	Convert Snort 2 rules and downloa	~ bec
					Add Rule Groups	
) 133:3 1	(dce_smb) SMB - bad SMB message type	Ø Disable (Default) 🗸	Builtins	None 🖬 🗑	

Import Custom Rule to Snort 3

Check the warning message and click OK.

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	ОК

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.

Cipiects / Intrusion Rules / Snort 3 All Rules	erview Analysis Policies Devices Objects	Integration	Deploy Q 💕 🌣 🍘 admin 🗸	cisco SECURE
Snort 2 All Rules Snort 3 All Rules				
< Intrusion Policy				Back To Top
All Rules	Local Rules / All Snort 2 Converted Global			
 Local Rules (1 group) 	Description Group created for custom rules enabled in sno	ort 2 version		
All Snort 2 Converted Global	Rule Actions V Search by CVE, SID, Refe	rence Info, or Rule Message		Tasks 🔻
> MITRE (1 group)	0			
> Rule Categories (9 groups)	0	The custom rules were successfully imported X		
	GID:SID Info	Rule Action	Assigned Groups Alert Configuration	
	> 2000:1000000 custom_http_sig	O Disable (Default)	All Snort 2 Converted Glo None	/1

Confirm Imported Custom Rule

Step 4. Change Rule Action

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

0

Ę	Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	Overvi	ew Analysis Policies	Devices Obje	ects Integration			Deploy Q 💰	° 0	admin \lor	cisco SECURE
Sno	rt 2 All Rules Snort 3 All Rules										
< Intr	usion Policy										Back To Top
	All Rules		Local Rules / All Snort 2	Converted Global							
~	Local Rules (1 group)	0	Description Group created	for custom rules enab	led in snort 2 version						
	All Coast 2 Converted Clobal	120	Rule Actions 🗸 🗸	Y Search by CVE,	SID, Reference Info, or Rule	Message					Tasks 🔻
	All Short 2 Converted Global		1 rule								
>	MITRE (1 group)	0					. Income the state of the				
>	Rule Categories (9 groups)	0			Ine custo	m rules were successful	iy imported X				
			GID:SID In	fo		Rule Action		Assigned Groups	Alert Config	guration	
			> 2000:1000000 cr	ustom_http_sig		🖉 Disable (Default) 🗸	(Overridden)	All Snort 2 Converted Glo.	None		11
						O Block					
						Alert					
						▲ Rewrite					
						C Drop					
						C Reject					
						Oisable (Default)					
						Cevert 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.

Edit Rule Action	0
2000:100 custom_http_sig	Î
All Policies Per Intrusion Policy	- 1
Policy snort_test Add Another Rule Action BLOCK	
Comments (optional)	
Provide a reason to change if applicable	
Cancel Sav	e

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 C	bjects Integration	Deploy	९ 🚱	° 0	admin \sim	cisco SECURE
Intrusion Policies Network Analysis Policies									
Hide Snort 3 Sync status 🜒 🔍 Search by Intrusion Policy,		All II	PS Rules IPS Map	ping 📵	Compare	e Policies	Create Policy		
Intrusion Policy Description	Base	Policy		Usage Information					
snort_test → Snort 3 is in pync with Snort 2. 2024-01-12	Balar	Balanced Security and Connectivity		1 Access Control Policy No Zero Trust Application Pol 1 Device	icy	Snort 2 Ver	sion	Snort 3 Versio	n 🖊 🗄 🖒 🗑

Confirm Imported Custom Rule

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

Firewall Management Center Policies / Access Control / Intrusion / Intrusion Policie	es Overview Analysis Pol	icies Devices Objects	Integration Deploy	Q 🔮 🌣 🙆 admin 🗸 🕬 SECURE
A Policies / Intrusion / snort_test Base Balanced Security and Policy: Connectivity Mode: Pr	v)		Used by: 1 Access Contro	Active Rules 9811
Base Policy \rightarrow Group Overrides \rightarrow	Recommendations Not in use	→ Rule Overrides	Summary	
Rule Overrides @				Back To Top
103 items All X 🗸	Local Rules / All Snort 2 Convert Description Group created for custor	ed Global m rules enabled in snort 2 version		Include
All Rules	Rule Action	Search by CVE, SID, Reference Info,	or Rule Message	
Overriden Rules	1 rule Prese	ts: Alert (0) Block (1) Disal	oled (0) Overridden (1) Advanced	Filters
> MITRE (1 group)	GID:SID Rule Details	Rule Action	Set By	Assigned Groups
✓ Local Rules (1 group)	2000:10 custom_http_sig	Block	✓ «> Rule Override	All Snort 2 Converte 💉 💻
All Snort 2 Converted Global > Rule Categories (9 groups)	alert top a msg:"cus	any any <> any any (sid:1000000; c tom_http_sig"; classtype:unknown;	id:2000; flow:established,to_client; ra rev:3;)	aw_data; content:"username";

Confirm Imported Custom Rule

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

Navigate to Policies>Access Controlon FMC, associate Intrusion Policy with ACP.

1 Citing Rule ftd_acp						Mandatory 🛛 🗙
Name ftd_acp	ţ	Action 🔤 Allo	w 🗸 🕹 Logging	ON 🐻 Time Ran	ge None V	ule Enabled 💽
		Intrusion Poli	cy snort_test × v	Default-Set X	V File Policy None	
Q Zones (2) Networks	Ports Application	ons 🛕 Users URLs	Dynamic Attributes	VLAN Tags		
Q Bearch Security Zone Objects		Showing 2 out of 2	Selected Sources: 1		Selected Destinations and Applic	ations: 1
E inside_zone (Routed Security Zone	»)		Collapse All	Remove All	Collapse All	Remove All
detaile_zone (Routed Security Zon	ne)		ZONE V 1 Object		ZONE v 1 Object	
Associate with ACP Rule						

Step 7. Deploy Changes

Deploy the changes to FTD.

Firewall Management Center Overview Analysis Policies Devices Objects Integration		Deploy Q 🤌 🏟 admin 🗸 🚽	SECURE
★> Return to Access Control Policy Management acp+rule	٩	Advanced Deploy	Legacy UI Savo
Packets • O Prefiter Rules O Decryption • O Security Intelligence O Identity O Access Control O More	FPR2120_FTD	Ready for Deployment	1 device

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.

Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	view Analysis Policie	es Devices Objects Integration		Deploy Q 🎸	admin 🗸 🖓 admin V	ECURE
Snort 2 All Rules Snort 3 All Rules						
< Intrusion Policy					Bac	к То Тор
All Rules	All Rules					
 Local Rules (1 group) 	All rules assigned to current	intrusion policy irrespective of rule group				_
All Snort 2 Converted Global	Rule Actions	Search by CVE, SID, Reference Info, or F	Rule Message		Tas	iks 🔻
 MITRE (1 group) 	GID:SID	Info	Rule Action	Assigned Groups	Upload Snort 3 rules A Convert Snort 2 rules and import	rt
 ATT&CK Framework (1 group) 	→ 148:2 [™]	(cip) CIP data is non-conforming to ODVA standard	🖉 Disable (Default) 🗸	Builtins	Convert Snort 2 rules and down	nload .
> Enterprise (13 groups)	> 133:3 1	(dce_smb) SMB - bad SMB message type	Ø Disable (Default)	Builtins	None Ta i	i i

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 Rules	0	Add Custom Rules	0
) OK	File Name Custom-rules.txt Associate Rules to Rule Groups Search All Snort 2 Converted Global Create New Custom Rule Group Choose the appropriate action. Merge Rules Merges any extra rules with the existing rules in the rule group. Choose the rules which are already present in a custom intrusion or new rules	1 Selected
		Cance	Next

Add Custom Rule

Confirm that the local rule file has been successfully uploaded.



```
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.

Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	rview Analysis Policie:	Devices Objects Integr	ation	Deploy Q 💕	🔅 🚱 🛛 admin 🗸	cisco SECURE
Snort 2 All Rules						
< Intrusion Policy						Back To Top
All Rules	Local Rules / All Snort	2 Converted Global				
 Local Rules (1 group) 	Description Group creat	ed for custom rules enabled in snort 2 ve	rsion			
All Snort 2 Converted Global	Rule Actions V	Search by CVE, SID, Reference I	info, or Rule Message			Tasks 🔻
 MITRE (1 group) 	GID:SID	Info	Rule Action	Assigned Groups	Alert Configuration	
 ATT&CK Framework (1 group) 	♥ □ 2000:1000000	custom_http_sig	🖉 Disable (Default) 🗸	All Snort 2 Converted Glo	None	11
> Enterprise (13 groups)	D	alert tcp any any <> any any (sid:100	0000; gid:2000; flow:established,to_client; raw_	data; content:"username"; msg	g:"custom_http_sig";	
> Rule Categories (9 groups)		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

2

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.

Fi An	rewall Managem alysis / Intrusions / Even	ent Cente	er ov	erview	Analysis	Policies	Devices	Objects I	integration				Dep	oloy Q	0 0	e 🕜 ad	min ~ dualto SE	CURE
										Bookmark This	Page Reportin	g Dashbo	oard View	Bookmark	Search	Predefine	ed Searches	Y
Events	s By Priority ar	nd Class	sification	(switch wor	kflow)										2024-04	-06 13:26:03	- 2024-04-06 14	:31:12
No Searc	h Constraints (Edit Sear	ch)															Exp	anding
Drilldow	n of Event, Priority, and	Classificatio	on Table V	/iew of Ev	ents Pac	kets												
Jump to	L																	
	↓ Time ×	Priority X	Impact X	Inline Result X	Reason X	Source IP X	Source x	Destination IP X	Destination x Country	Source Port / ICMP X Type	Destination Port / ICMP X Code	SSL Status ×	VLAN X	Message 3	¢.		Classification X	General
•	2024-04-06 14:30:48	low	O Unknown	Block		9 192.168.20.1		9 192.168.10.	1	80 (http) / tcp	50103 / tcp			custom_h	ttp_sig (20	000:1000000:3	3) Unknown Traffic	Standa

Intrusion Event

ClickPacketstab, confirm the detail of Intrusion Event.

Firewall Manage Analysis / Intrusions / E	gement Center Overview Analysis Policies Devices Objects Integration Deploy Q 📀 🌣 🚱 i	admin ~ secure secure
	Bookmark This Page Reporting Dashboard View Bookmarks Search Predet	fined Searches 👻
Events By Priority	y and Classification (seator). Very and	:03 - 2024-04-06 14:32:46
No Search Constraints (Edit S	i Search)	Coperionity
Drilldown of Event, Priority, a	r, and Classification Table View of Events Packets	
 ✓ Event Information Message Time 	je custom_http_sig (2000:1000000:3) ∞ 2024-04-06 14:31:26	
Classification	n Unknown Traffic	
Priority	y low postile zone	
Foress Security Zone	e ousoe_oue	
Device	* FPR2120. FTD	
Ingress Interface	e outside	
Egress Interface	ie inside	
Source IP	P 192.168.20.1	
Source Port / ICMP Type	e 80 (http) / tcp	
Destination IP	P 192.168.10.1	
Destination Port / ICMP Code	ie 50105 / tcp	
HTTP Hostname	e 192.168.20.1	
HTTP URI	3 /test.txt	
Intrusion Policy	y snort_test	
Access Control Policy	y ap-rue	
Access Control Rule	e na acp	
Rule	e arert tçe any any √ any any t sid:iuuuuu; gid:zuuuu; rio#:estabiisheq.to_ciient; ram_pata; content; username i msg; custom_http_ig ; classtype:unknown; rev:3;)	
 Actions 		

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