

في فة صصخم ةي لحم تانايب دعاوق نيوكت Snort2 لىل فTD

تايوتحملا

[ةمدقملا](#)

[ةيساسأل تابلطتلا](#)

[تابلطتلا](#)

[ةمدختسمل تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[ةكبش ليل طي طختلا مسرلا](#)

[نيوكتلا](#)

[Snort رادصا ديكأت 1. ةوطخلا](#)

[Snort 2 في فة صصخم ةي لحم تاي رخش ةدعاوق عاشنا 2. ةوطخلا](#)

[صصخملا يلحملا رخشلا ةدعاوق ديكأت 3. ةوطخلا](#)

[ةدعاوقلا عارجا ريغت 4. ةوطخلا](#)

[\(ACP\) لوصولا في فة مكنحتلا ةيساس ةدعاوق ليل سئلا ةيساس طبر 5. ةوطخلا](#)

[تاري ريغتلا رشن 6. ةوطخلا](#)

[ةحصلا نم ققحتلا](#)

[صصخملا يلحملا رخشلا ةدعاوق لي غشت متي مل](#)

[HTTP مداخ في فة ملما تايوتحم طبض 1. ةوطخلا](#)

[يلوالا HTTP بلط 2. ةوطخلا](#)

[صصخملا يلحملا رخشلا ةدعاوق لي غشت مت](#)

[HTTP مداخ في فة ملما تايوتحم طبض 1. ةوطخلا](#)

[يلوالا HTTP بلط 2. ةوطخلا](#)

[لفطتلا ديكأت ثدح 3. ةوطخلا](#)

[اهحالص او عاطحأل افاشكتسا](#)

ةمدقملا

لىل SNORT2 في فة صصخملا ةي لحملا لاصتالا دعاوق نيوكت عارجا دن تسملا اذه فصبي
(FTD) ةي امحل رادج ديدهت دض عافدلا

ةيساسأل تابلطتلا

تابلطتلا

ةيلاتلا عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت:

- Cisco نم (FMC) FireSIGHT ةرادا زكرم
- (FTD) ةي امحل رادج ديدهت دض عافدلا

ةمدختسمل اتانوكملا

ةيلالتل ةيدامل اتانوكملا وجماربل اتارادصل لىل دننستسمل اذه يف ةدراول تامولعمل دننستس:

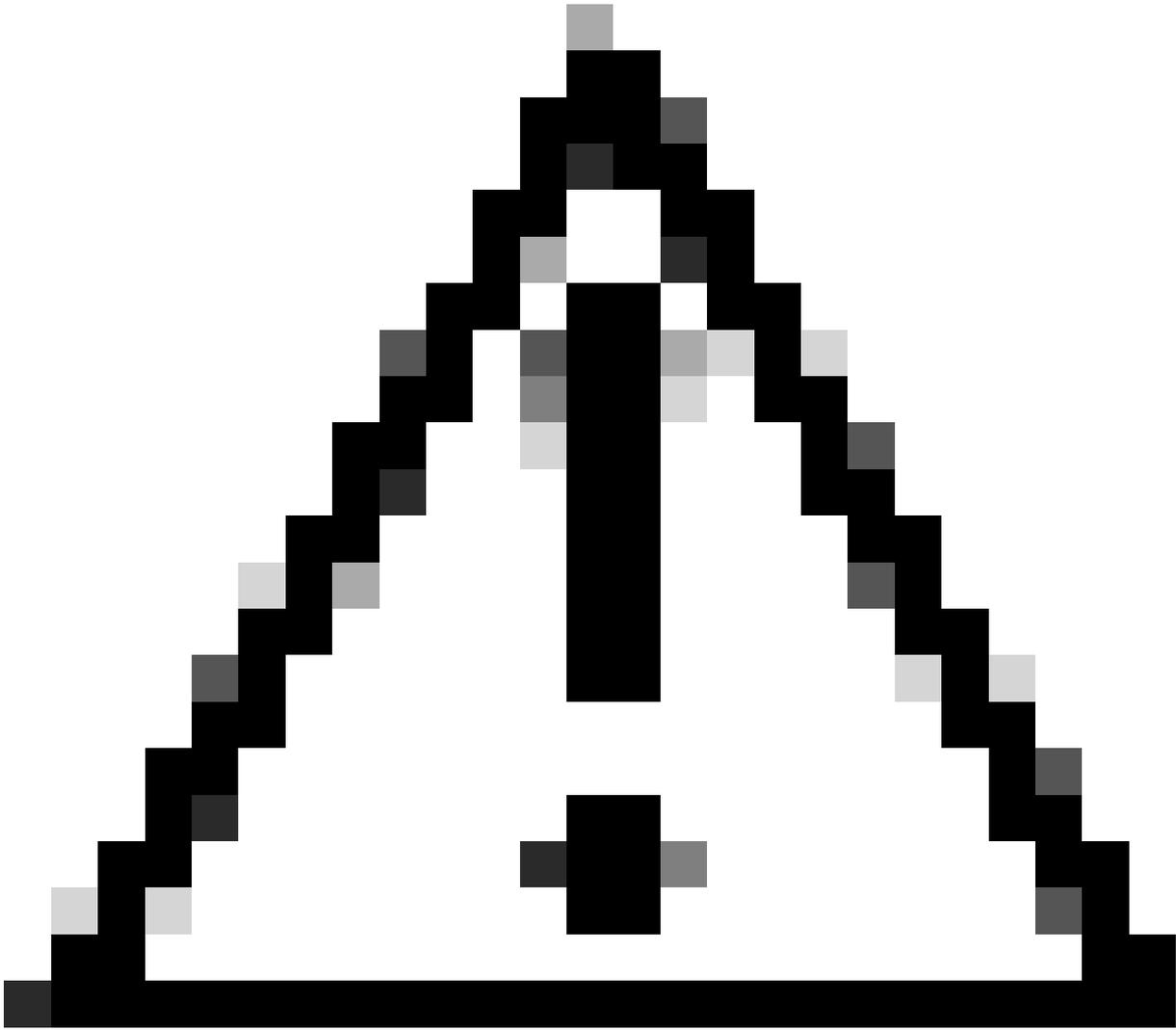
- Cisco Firepower ل VMWare 7.4.1 ةرادل زكرم
- Cisco Firepower 2120 7.4.1

ةصاخ ةيلعمل ةئيبل يف ةدوجوملا ةزهجال نم دننستسمل اذه يف ةدراول تامولعمل عاشنل مت تناك اذل. (يضارتفا) حوسم نيوكتب دننستسمل اذه يف ةمدختسمل ةزهجال عيمج تادب رمل لمتحمل ريثاتلل كمهف نم دكاتف، ليغشتل ديقتككباش

ةيساسا تامولعمل

كنكمي مدختسمل لبق نم ةفرعم ةدعاق لىل "ةصصخمل ةيلحمل رخشلا ةدعاق" ريشت ام دنع. FTD يف جمدملا مدخال لىل علفطتلل عنمو فاشتكما ماظن لخاد اهذيفنت واهواشنل يف رعتب ساسالاب موقت تنأ، Cisco FTD يف ةصصخم ةيلحمل ريش ةدعاق عاشنل موقت رورم ةكرح تقباطت اذل. اهتبقارم رخشلا كرحم كنكمي يتل طورشل نم ةعومجم وأ ديدج طمن ددحمل ارجالاب تروشل موقبي نأ كنكمي، ةصصخمل ةدعاق لىل يف ةددحمل طورشل عم ةكبشلل حبشلل دعاوق نولوؤسمل مدختسي. ةمزحل طاقس وأ هيبنت عاشنل لثم، ةدعاق لىل يف ةماعل دعاوقل تاعومجم اهيطغت ال يتل ةددحمل تاديدهتلل ةجلاعمل ةصصخمل ةيلحمل

مت اهنم ققحتل ةصصخم ةيلحمل مدخال ةدعاق نيوكت ةيفي كمي دقت مت، دننستسمل اذه يف (مدختسمل مسا) ةددحم ةلسلس لىل عيوحت يتل HTTP ةباجتسإ مزح فاشتكال اهميمصت اهتالفاو.

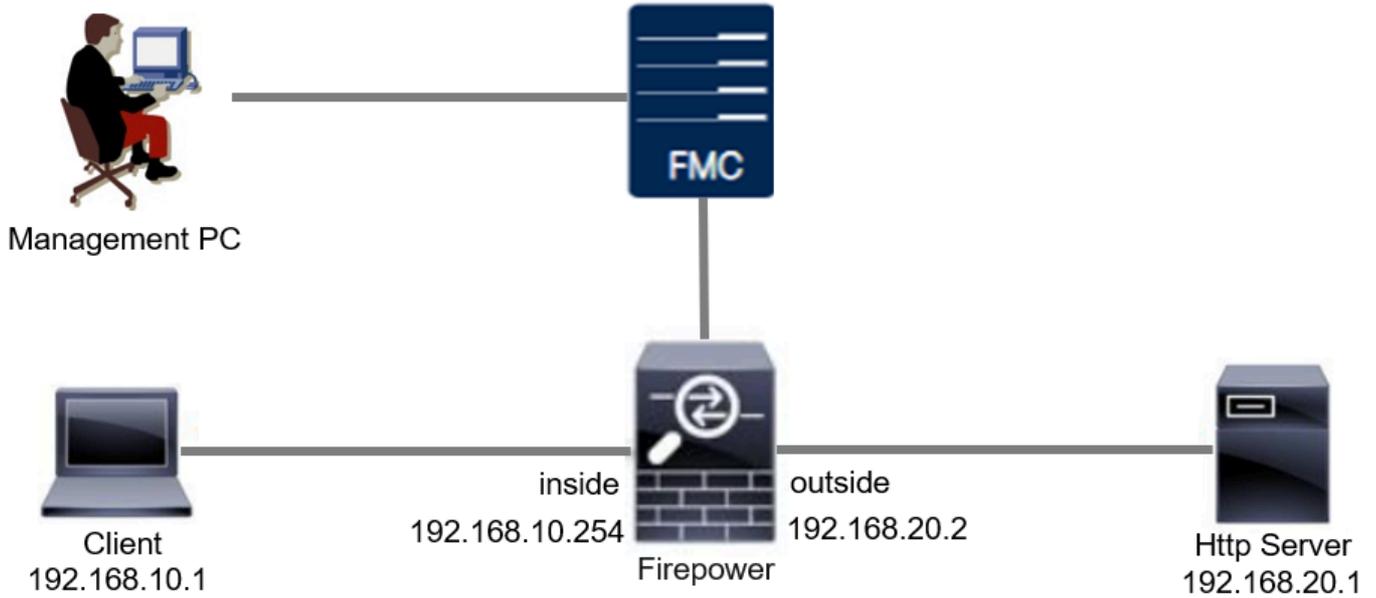


قاطن ج راخ اهل معدلا ريفوت و ةصصخم ةيلحم لاصتا دعاوق عاشنا عقي :ريذحت
كنم بلطتو ، طقف عجرمك دنتسملا اذه مادختسا نكمي ، كلذل TAC معد ةيطغت
كتيلوؤسمو كريدقتل اقفو اهتراداو ةصصخملا دعاوقلا هذه عاشنا

نيوكتلا

ةكبش لل يطيختلا مسرلا

ىلع snort2 ف ةصصخملا ةيلحملا تاريخشلا دعاوقل ققحتلاو نيوكتلا دنتسملا اذه مدقي
يطيختلا مسرلا اذه



نيوكتال

يتل HTTP ةباجتسإ مزح فاشتكال ةصصخملا ةيلحمل نيوكتال ةدعاق نيوكت وه اذه اهطاقسإو (مدختسمل مسا) ةدحم ةلسلس ىلع يوتحت

رادصإ ديكتأ 1. ةوطخل

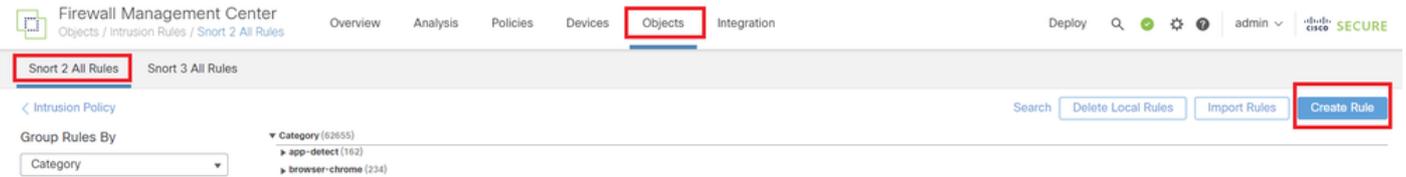
زاهجل بيوبتل ةمالع قوف رقنا، FMC مكحتل ةدحو يف ةزهجال ةرادإ > ةزهجال ىل لقتنا snort2. وه ريخشلا رادصإ ديكتأ

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The 'Devices' tab is selected, and the 'Device' sub-tab is active. The device configuration for FPR2120_FTD is displayed. The 'Inspection Engine' is set to Snort 2. Other configuration details include: Name: FPR2120_FTD, Transfer Packets: Yes, Troubleshoot: Logs, CLI, Download, Mode: Routed, Compliance Mode: None, TLS Crypto Acceleration: Enabled, 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: J4N111111111, 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, Health: Status: Green, Management: Remote Host Address: 1.1.1.1

رادصإ Snort

Snort 2 يف ةصصخملا ةيلحمل تايرخش ةدعاق عاشنإ 2. ةوطخل

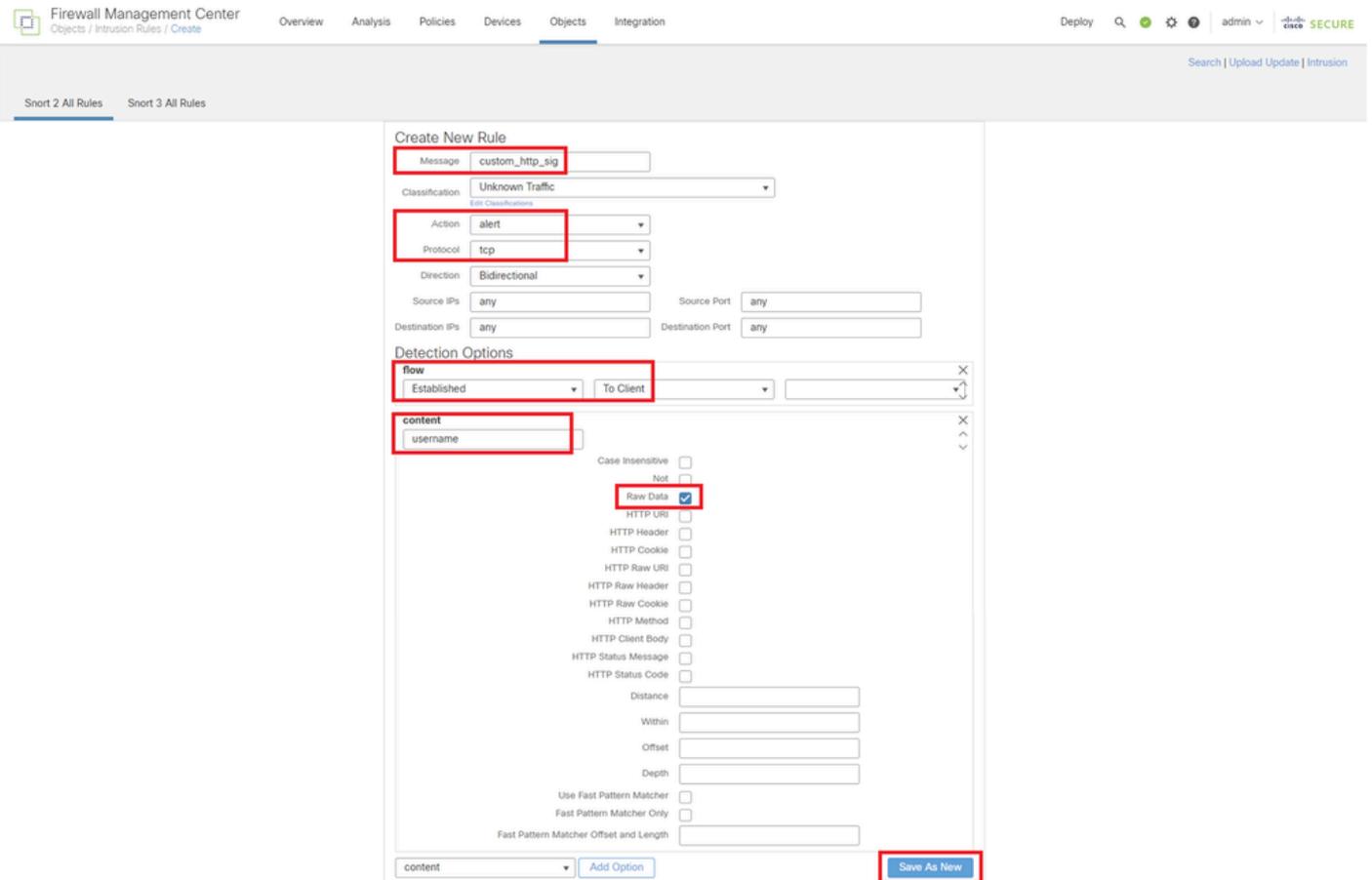
ةدعاق عاشنإ رز قوف رقنا، FMC ىلع Snort 2 All Rules > قارتخال دعاقو > تانئاك ىل لقتنا



ةصصخم ةدعاق عاشنا

صصخملا يلححمل رخشلل ةدعاق ل ةيرورضل تامولعمل لاخدا ب مق

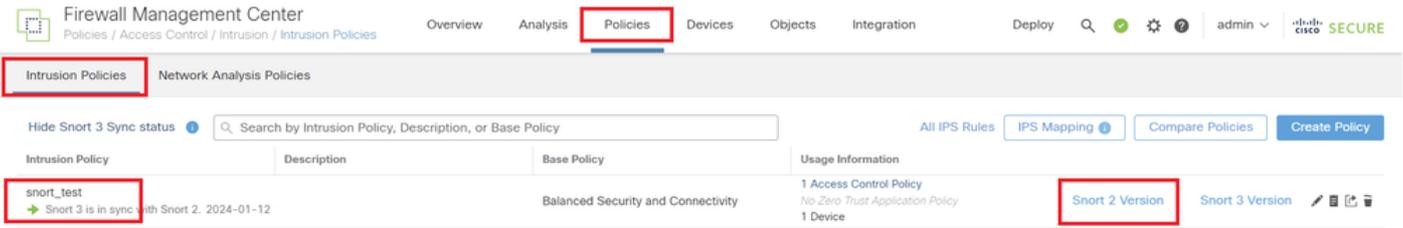
- قارتخال : custom_http_sig
- ءارجال
- لوكوتوربل : TCP
- ليمعمل تبثم : قفدتل
- (ماخ تانايب) مدختسمل مسا : يوتحمل



ةدعاق ل ةيرورضل تامولعمل لاخدا

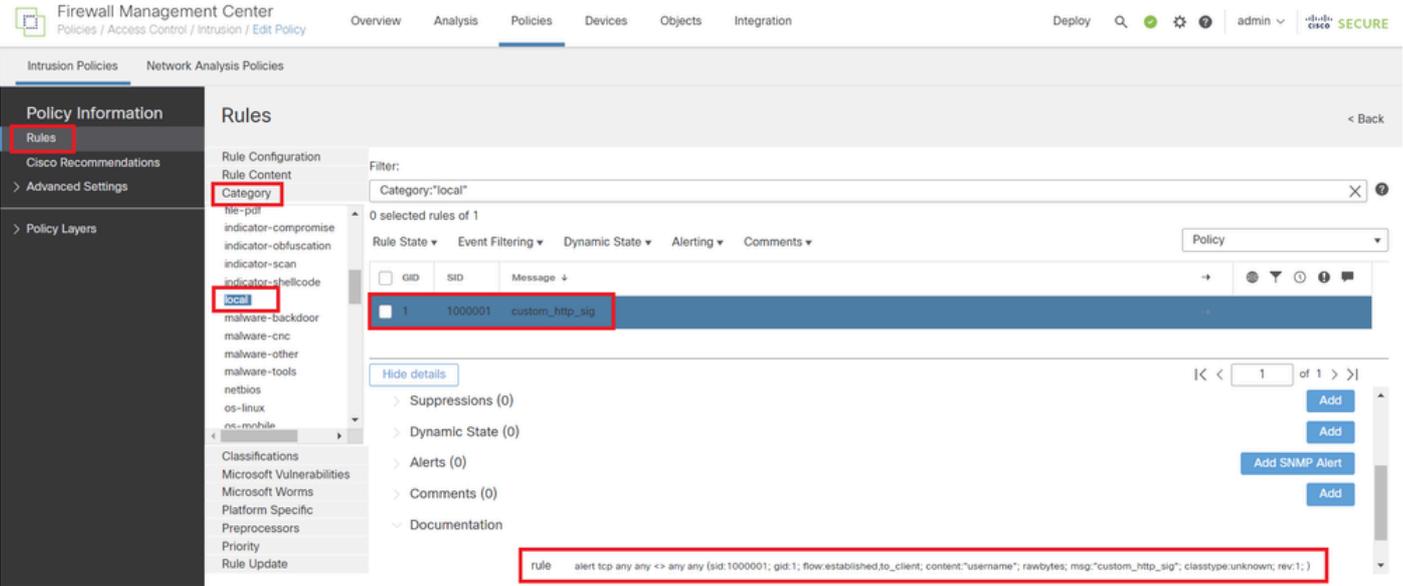
صصخملا يلححمل رخشلل ةدعاق ديكأت 3 ةوطخل

2. رادصا رز قوف رقنا ، FMC يلعل لس تال تاسايس > تاسايسلا ل لقتنا



ةصصخلمل ةدعاقلا ديكت

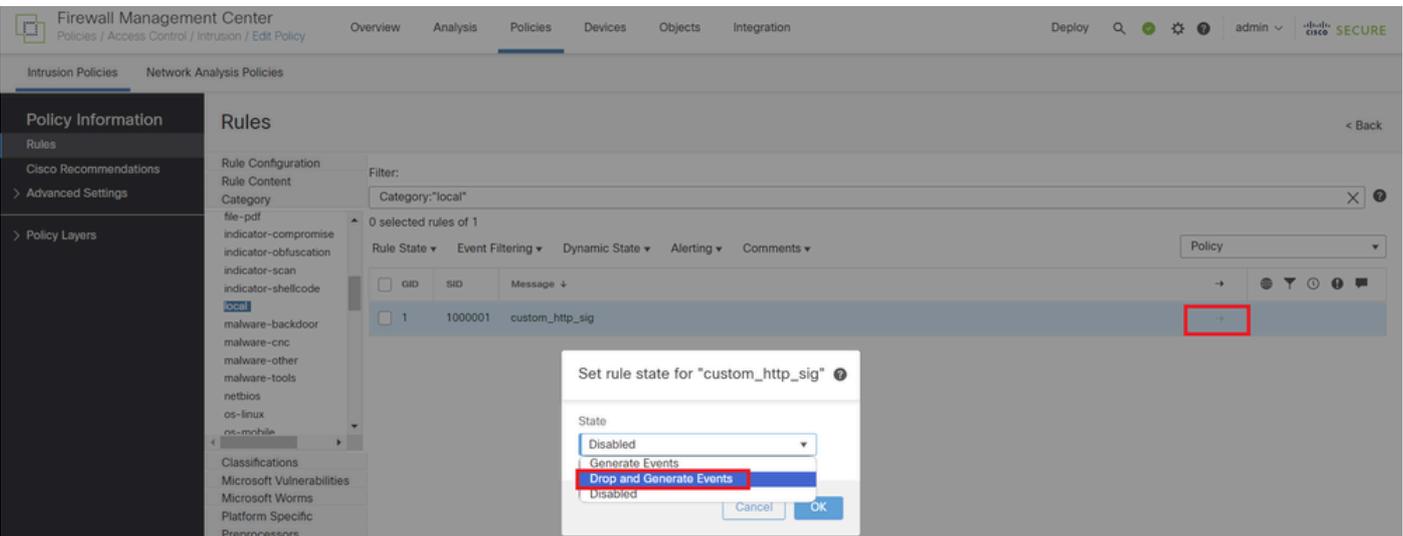
تاريخشلا ةدعاق ليصافت نم دكأتو، FMC يف ةيحلحمل > ةئفل > دعاوقلا يلى لقتنا ةصصخلمل ةيحلحمل.



ةصصخلمل ةدعاقلا ليصافت

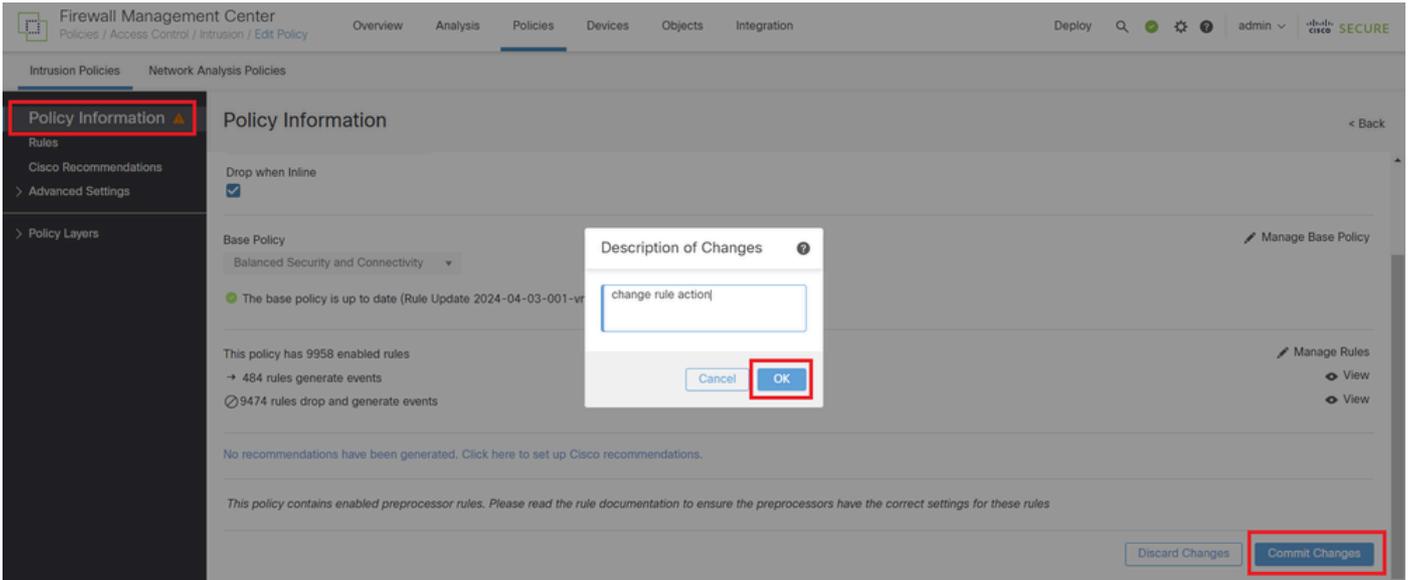
ةدعاقلا ءارج ريغت 4. ةوطخل

قف اوم رزلا قوف رقنا م ث، ثادجال ءاشن او طاقس يلى ةلاجل نيغت ب مقو، ةلاح قوف رقنا.



ةدعاقلا ءارج ريغت

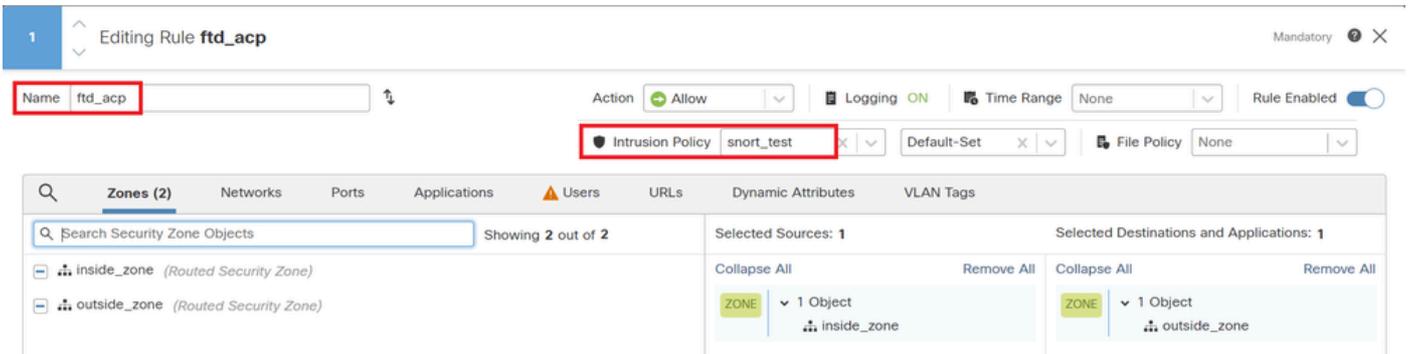
تاريغي غتلا ظفحل تاريغي غتلا ذيفنت رز قوف رقا م ث ، جهنلا تامولعم رزلا قوف رقا



تاريغي غتلا ذيفنت

لوصولا ي ف مكحتلا ةسايس ةدعاقب للستلا ةسايس طبر 5 ةوطخلا

ACP ب للستلا ةسايس طبرأو ، FMC لوصولا ي ف مكحتلا > تاسايسلا ل لقتنا



ACP ةدعاقب نارقتالا

تاريغي غتلا رشن 6 ةوطخلا

FTD لعل تاريغي غتلا رشن



تاريغي غتلا رشن

ةحصللا نم ققحتلا

صصخملا يلحمل رشنلا ةدعاق ليغشت متي مل

HTTP مداخل في فيلم التايوتحم طبض 1. ةوطخال

مدختسم لل HTTP مداخل بناج ىلع test.txt فلم تايوتحم طبضا

يولوال HTTP ب ل ط 2. ةوطخال

دكأتو (192.168.10.1) لي م عمل ضرعتسم نم (192.168.20.1/test.txt) مداخل ىل لوصولاب مق HTTP لاصتاب حامس لل نم



يولوال HTTP ب ل ط

صصخم لل ي ل حم لل رخش لل ةدعاق لي غشت مت

HTTP مداخل في فيلم التايوتحم طبض 1. ةوطخال

مدختسم لل مسا ىلع HTTP مداخل بناج ىلع test.txt فلم تايوتحم طبضا

يولوال HTTP ب ل ط 2. ةوطخال

دكأتو (192.168.10.1) لي م عمل ضرعتسم نم (192.168.20.1/test.txt) مداخل ىل لوصولاب مق HTTP لاصتابا رطح نم



يولوال HTTP ب ل ط

ل فطت لل شح ديكأت 3. ةوطخال

ماحتقالا شح عاشنإ مت هنا نم دكأتو، FMC ىلع شادخال > تاقارخال > لي لحت لل ىل لقتنا صصخم لل ي ل حم لل رخش لل ةدعاق ةطساوب

Firewall Management Center Overview **Analysis** Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Bookmark This Page | Reporting | Dashboard | View Bookmarks | Search **Predefined Searches**

Events By Priority and Classification [\[switch workflow\]](#) || 2024-04-06 09:41:20 - 2024-04-06 11:06:04 Expanding

Search Constraints [\[Edit Search\]](#) [\[Save Search\]](#)

Drilldown of Event, Priority, and Classification **Table View of Events** Packets

Jump to...

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 11:05:13	low	Unknown	Dropped		192.168.20.1		192.168.10.1		80 (http) / tcp	50057 / tcp			custom_http_sig (1:1000001:1)	Unknown Traffic	Standar

ماحتقا ا شذح

لفطتلل شذح لى صافت دى كأتل ، مزحلل بى وبتلل ةمالع قوف رقنل .

Firewall Management Center Overview **Analysis** Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Bookmark This Page | Reporting | Dashboard | View Bookmarks | Search **Predefined Searches**

Events By Priority and Classification [\[switch workflow\]](#) || 2024-04-06 09:41:20 - 2024-04-06 11:07:15 Expanding

Search Constraints [\[Edit Search\]](#) [\[Save Search\]](#)

Drilldown of Event, Priority, and Classification **Table View of Events** **Packets**

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"; rsnbytes; msz:"custom_http_sig"; classtype:unknown; rev:1;)

Actions

ماحتقالل شذح لى صافت

اهحال صاوا ءاطخالل فاشك تسلا

ةطساوب HTTP رورم ةكرح رطح متي ، لاثلما اذف يف . FTD لىل ءكولسلل دى كأتل رمالل system support trace لى غشتب مق ةطساوب IPS (GID 1, sid 100001).

<#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

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل