

# ي ف ة ص ص خ م ة ي ل ح م ت ا ن ا ي ب د ع ا و ق ن ي و ك ت Snort2 ل ع FTD

## ت ا ي و ت ح م ل ا

[ة م د ق م ل ا](#)

[ة ي س ا س ا ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[ة م د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[ة ي س ا س ا ت ا م و ل ع م](#)

[ن ي و ك ت ل ا](#)

[ة ك ب ش ل ل ل ي ط ي ط خ ت ل ا م س ر ل ا](#)

[ن ي و ك ت ل ا](#)

[Snort ر ا د ص ا د ي ك ا ت 1. ة و ط خ ل ا](#)

[Snort 2 ي ف ة ص ص خ م ة ي ل ح م ت ا ي ر خ ش ة د ع ا ق ا ع ا ش ن ا 2. ة و ط خ ل ا](#)

[ص ص خ م ل ا ي ل ح م ل ا ر خ ش ل ا ة د ع ا ق د ي ك ا ت 3. ة و ط خ ل ا](#)

[ة د ع ا ق ل ل ا ع ا ر ج ا ر ي غ ت 4. ة و ط خ ل ا](#)

[\(ACP\) ل و ص و ل ا ي ف م ك ح ت ل ا ة س ا ي س ة د ع ا ق ب ل ل س ت ل ا ة س ا ي س ط ب ر 5. ة و ط خ ل ا](#)

[ت ا ر ي ي غ ت ل ا ر ش ن 6. ة و ط خ ل ا](#)

[ة ح ص ل ل ا ت م ق ق ح ت ل ا](#)

[ص ص خ م ل ا ي ل ح م ل ا ر خ ش ل ا ة د ع ا ق ل ل ي غ ش ت م ت ي م ل](#)

[HTTP م د ا خ ي ف ف ل م ل ا ت ا ي و ت ح م ط ب ص 1. ة و ط خ ل ا](#)

[ي ل و ا ل ا HTTP ب ل ط 2. ة و ط خ ل ا](#)

[ص ص خ م ل ا ي ل ح م ل ا ر خ ش ل ا ة د ع ا ق ل ل ي غ ش ت م ت](#)

[HTTP م د ا خ ي ف ف ل م ل ا ت ا ي و ت ح م ط ب ص 1. ة و ط خ ل ا](#)

[ي ل و ا ل ا HTTP ب ل ط 2. ة و ط خ ل ا](#)

[ل ف ط ت ل ا د ي ك ا ت ت د ح 3. ة و ط خ ل ا](#)

[ا ه ح ا ل ص ا و ا ط خ ا ل ا ف ا ش ك ت س ا](#)

## ة م د ق م ل ا

ل ع SNORT2 ي ف ة ص ص خ م ل ا ة ي ل ح م ل ا ل ا ص ت ا ل ا د ع ا و ق ن ي و ك ت ع ا ر ج ا د ن ت س م ل ا ا ذ ه ف ص ي  
(FTD) ة ي ا م ح ل ا ر ا د ج د ي د ه ت د ص ع ا ف د ل ا

## ة ي س ا س ا ل ا ت ا ب ل ط ت م ل ا

### ت ا ب ل ط ت م ل ا

ة ي ل ل ا ت ل ا ع ي ض ا و م ل ا ب ة ف ر ع م ك ي د ل ن و ك ت ن ا ب Cisco ي ص و ت

- Cisco ن م (FMC) FireSIGHT ة ر ا د ا ز ك ر م
- (FTD) ة ي ا م ح ل ا ر ا د ج د ي د ه ت د ص ع ا ف د ل ا

## ةمدختسمل اتانوكملا

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

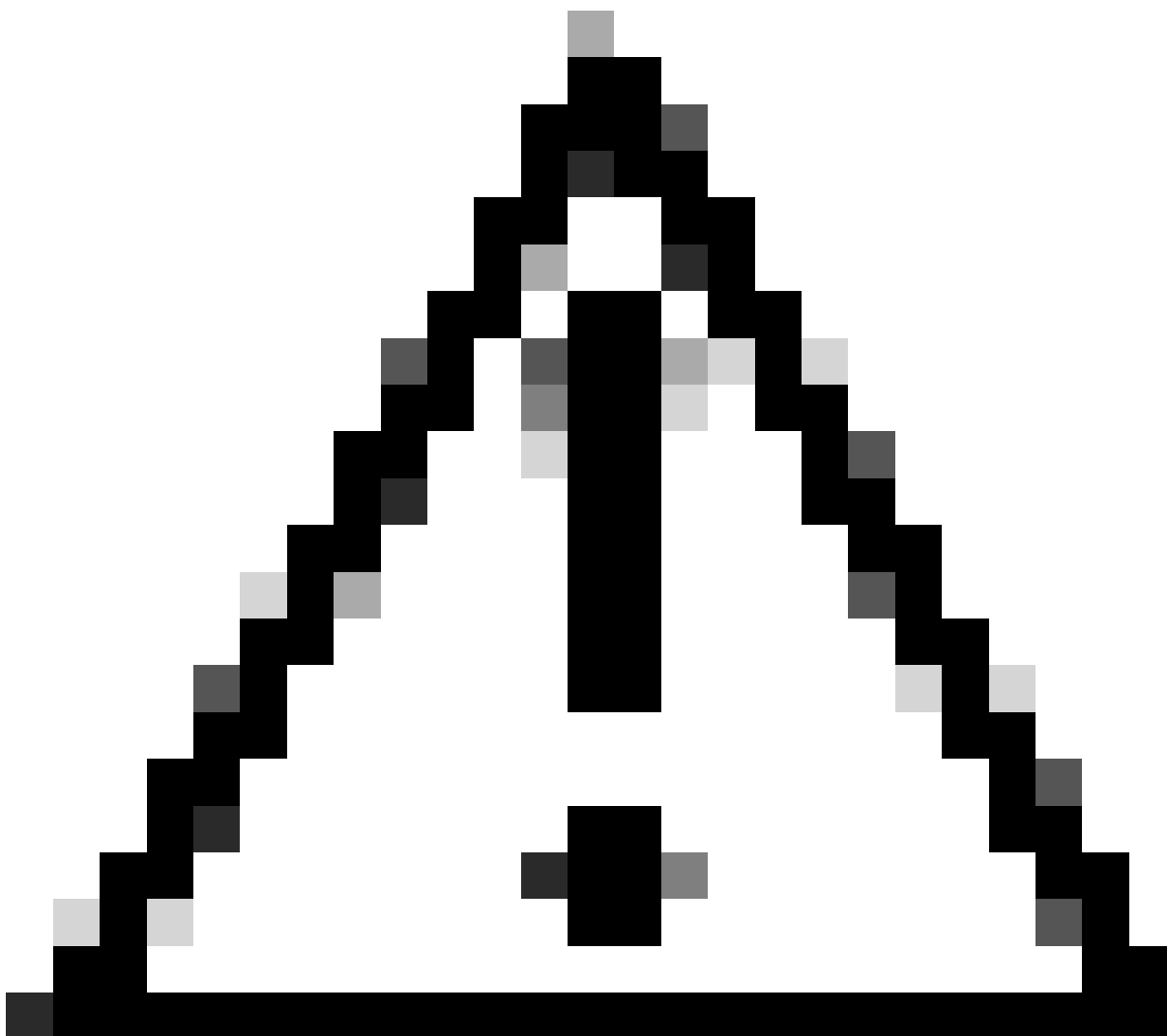
- Cisco Firepower ل VMWare 7.4.1 ةرادل زكرم
- Cisco Firepower 2120 7.4.1

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

## ةيساسل 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 فيرعتب ساسالاب موقت تنل، Cisco FTD يف ةصصخم ةيلحمل ريش ةدعاق عاشنل موقت رورم ةكرح تقباطت اذل. اهتبقارم رخشلا كرحم كنكمي يتل طورشل نم ةعومجم واديدج طمن ددحمل ارجالاب تروشل موقبي نل كنكمي، ةصصخمل ةدعاق لىل يف ةددحمل طورشل عم ةكبشلل حبشلل دعاوق نولوؤسمل مدختسي. ةمزحل طاقسل واهيبنن عاشنل لثم، ةدعاق لىل يف ةماعلل دعاوقل تاعومجم اهيطغت ال يتل ةددحمل تاديدهتلل ةجلاعمل ةصصخمل ةيلحمل

مت اهنم ققحتل او ةصصخم ةيلحمل مدخال ةدعاق نيوكت ةيفيكي ميديقت مت، دننستسمل اذه يف (مدختسمل مسا) ةددحم ةلسلس لىل عيوحتت يتل HTTP ةباجتسل مزح فاشتكال اهميمصت اهتالفاو.



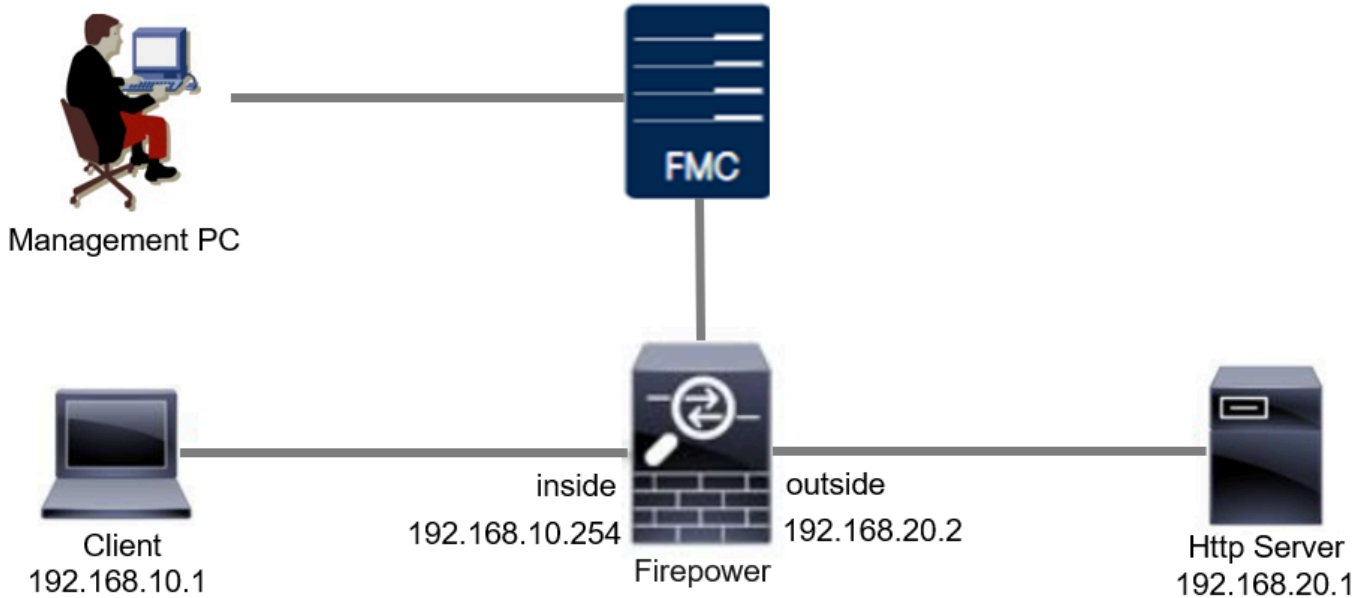
قاطن ج راخ اهل معدل ريفوت و ة ص ص خ م ة ل ح م ل اص ت ا دعاوق عاشن ا ع ق ي : ر ي ذ ح ت  
ك ن م ب ل ط ت و ، ط ق ف ع ج ر م ك د ن ت س م ل ا ا ذ ه م ا د خ ت س ا ن ك م ي ، ك ل ذ ل TAC م ع د ة ي ط غ ت  
ك ت ي ل و و س م و ك ر ي د ق ت ل ا ق ف و ا ه ت ر ا د ا و ة ص ص خ م ل ا دعاوق ل ا ه ذ ه عاشن ا

---

## ن ي و ك ت ل ا

ة ك ب ش ل ل ي ط ي ط خ ت ل ا م س ر ل ا

ل ع snort2 ي ة ص ص خ م ل ا ة ل ح م ل ا ت ا ر ي خ ش ل ا ة دعاوق ل ق ق ح ت ل ا و ن ي و ك ت ل ا د ن ت س م ل ا ا ذ ه م د ق ي  
ي ط ي ط خ ت ل ا م س ر ل ا ا ذ ه



## نيوكتال

يتل HTTP ةباجتسا مزح فاشتكال ةصصخملا ةيلحمل نيوكتال ةدعاق نيوكت وه اذه اهطاقساو (مدختسما مسا) ةدحم ةلسلس ىلع يوتحت

رادصا ديكتأ 1. ةوطخل

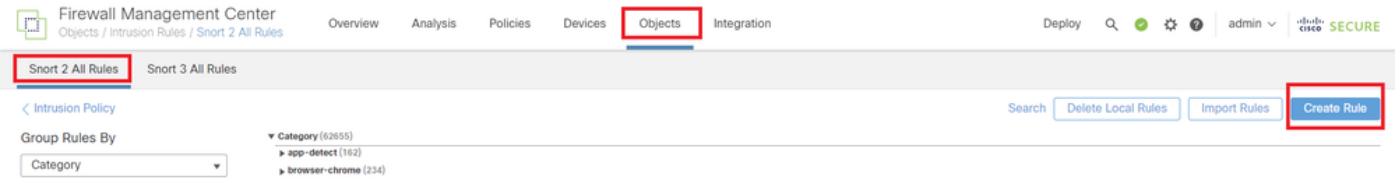
زاهال بيوبتال ةمالع قوف رقنا، FMC مكحتال ةدحو يف ةزهجالا ةرادا > ةزهجالا ىل لقتنا snort2. وه ريخشال رادصا ديكتأ

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The 'Devices' tab is selected, and the 'Device' sub-tab is active. The device name is FPR2120\_FTD. The 'Inspection Engine' is set to Snort 2. The 'License' section shows various features enabled, and the 'System' section shows the device model as Cisco Firepower 2120 Threat Defense.

رادصا Snort

Snort 2 يف ةصصخملا ةيلحمل تايرخش ةدعاق عاشنا 2. ةوطخل

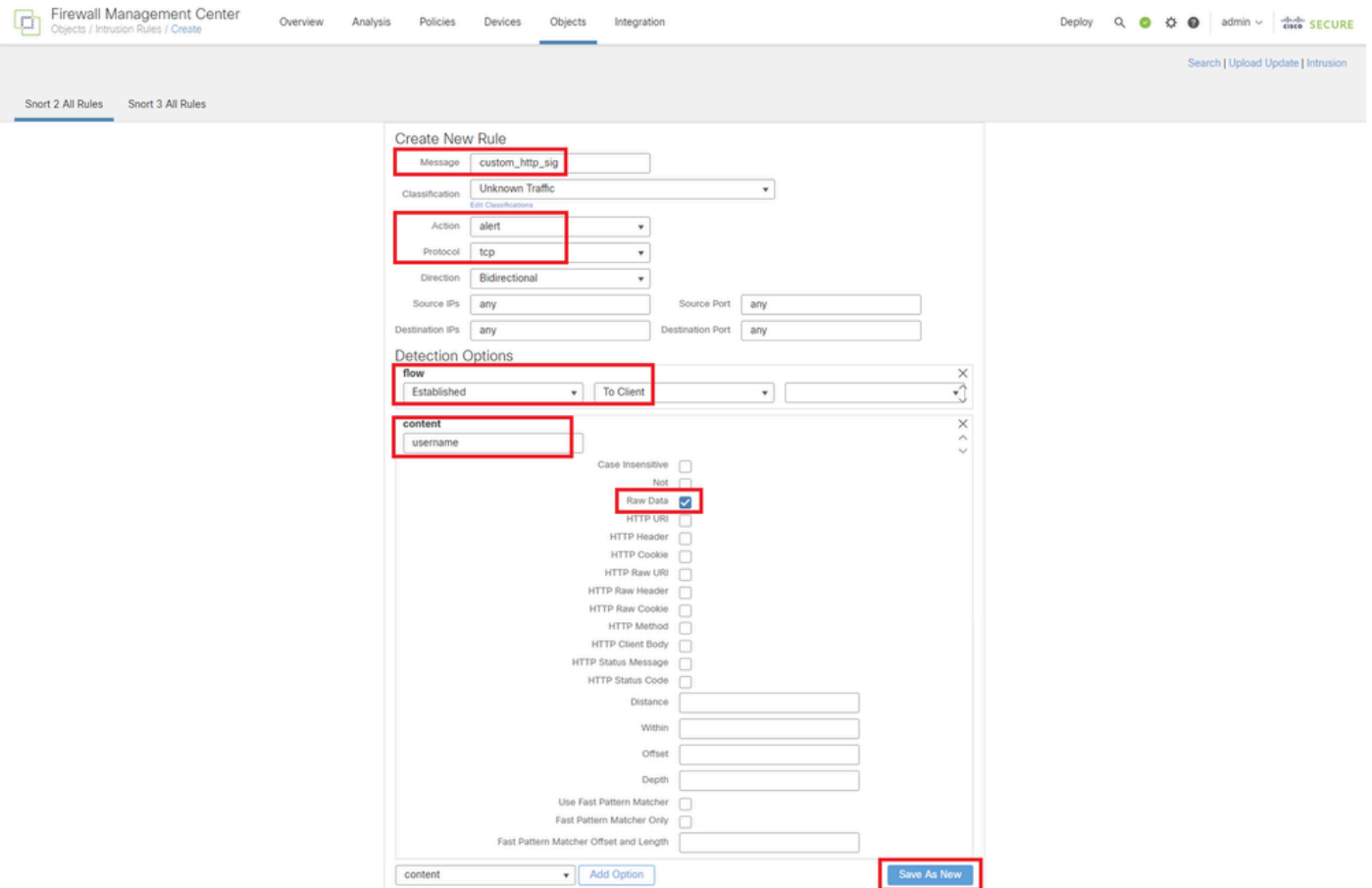
ةدعاق عاشنا رز قوف رقنا، FMC ىلع Snort 2 All Rules > قارتخال دعاقو > تانئاك ىل لقتنا



ةصصخم ةدعاق ءاشنا

صصخملا يلححمل رخشل ةدعاق ل ةرورضل تامولعمل لادبا مق

- قارتخال : custom\_http\_sig
- ءارجال
- لوكوتوربل : TCP
- ليمعمل تبثم : قفدتل
- (ماخ تانايب) مدختسمل مسا : يتوحمل



ةدعاق لل ةرورضل تامولعمل لادبا

صصخملا يلححمل رخشل ةدعاق ديكأت 3 ةوطخل

2. رادصا رز قوف رقنا ، FMC يلعل لستلا تاسايس > تاسايسلا للاقنا

Firewall Management Center  
Policies / Access Control / Intrusion / Intrusion Policies

Overview Analysis **Policies** Devices Objects Integration Deploy

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	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

ةصصخلمل ةدعاقلا ديكتأت

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

Firewall Management Center  
Policies / Access Control / Intrusion / Edit Policy

Overview Analysis **Policies** Devices Objects Integration Deploy

Intrusion Policies Network Analysis Policies

Policy Information Rules

Rule Configuration Rule Content Category: local

0 selected rules of 1

Rule State	Event Filtering	Dynamic State	Alerting	Comments
1				

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;)

ةصصخلمل ةدعاقلا ليصافت

ةدعاقلا ءارج ريغت 4. ةوطخل

قف اوم رزلا قوف رقنا م ث، اءال ءاشن او طاقس يلى ءال ني عتب مقو، ءلا ح قوف رقنا

Firewall Management Center  
Policies / Access Control / Intrusion / Edit Policy

Overview Analysis **Policies** Devices Objects Integration Deploy

Intrusion Policies Network Analysis Policies

Policy Information Rules

Rule Configuration Rule Content Category: local

0 selected rules of 1

Rule State	Event Filtering	Dynamic State	Alerting	Comments
1				

Set rule state for "custom\_http\_sig"

State: Disabled

Generate Events

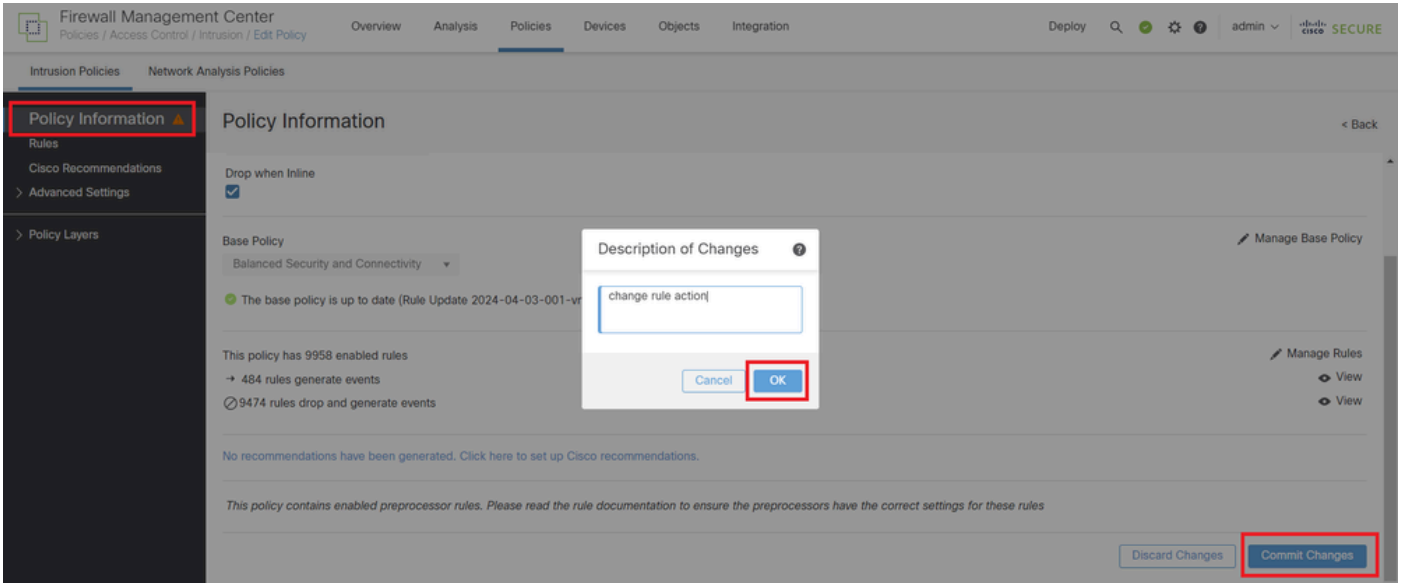
Drop and Generate Events

Disabled

Cancel OK

ةدعاقلا ءارج ريغت

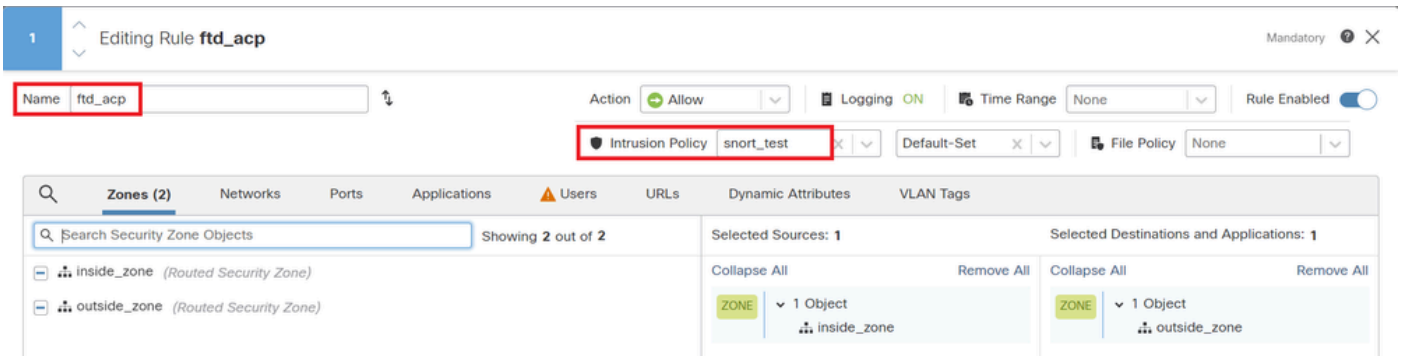
تاريغي غتلا ظفحل تاريغي غتلا ذيفنت رز قوف رقا م ث ، جهنلا تامولعم رزلا قوف رقا



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

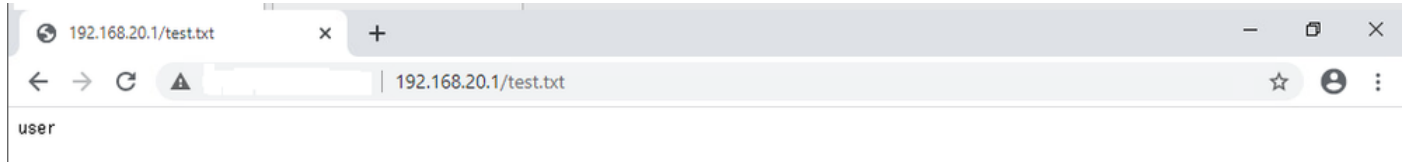
صصخملا يلحمل رخشلا ةدعاق ليغشت متي مل

HTTP مداخل في فيلم التايوتحم طبض 1. ةوطخال

مدختسم لل HTTP مداخل بناج يلع 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 يلى لوصول اب مق HTTP لاصتاب حامس لل نم



يولوال HTTP ب ل ط

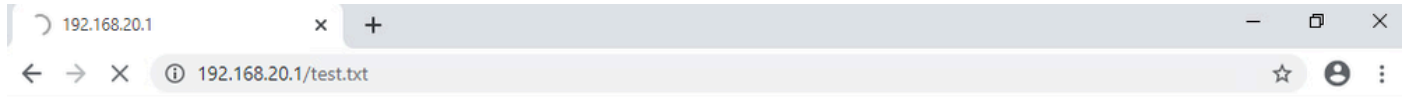
صصخم لل ي ل حم لل رخش لل ةدعاق لي غشت مت

HTTP مداخل في فيلم التايوتحم طبض 1. ةوطخال

مدختسم لل مسا يلع HTTP مداخل بناج يلع 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 يلى لوصول اب مق HTTP لاصتاب رطح نم



يولوال HTTP ب ل ط

ل فطت لل شح ديكأت 3. ةوطخال

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



Firewall Management Center  
Analysis / Intrusions / Events

Overview **Analysis** Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 Cisco 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	<b>Dropped</b>		192.168.20.1		192.168.10.1		80 (http) / tcp	50057 / tcp			custom_http_sig (1:1000001:1)	Unknown Traffic	Standar

ماحتقا ا شح

لفطتلا شح لى صافت دي كأتل ، مزحلا بي وبتلا ةمالع قوف رقنا

Firewall Management Center  
Analysis / Intrusions / Events

Overview **Analysis** Policies Devices Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 Cisco 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:100001; gid:1; flow:established,to\_client; content:"username"; rsnbytes; msz:"custom\_http\_sig"; classtype:unknown; rev:1; )

Actions

ماحتقا الا شح لى صافت

## اهحال صاوا ءاطخال فاشكتسا

ةطساوب HTTP رورم ةكرح رطح متي ، لا ثمل ا اذ ه في . FTD لىع كولسلا دي كأتل رمألا system support trace لىغشتب مق ةطساوب HTTP (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 م ادخت ساب دن تسمل اذة Cisco ت مچرت  
ملاعلاء انء مچ م ف ن م دخت تسمل معد و ت م م دقت ل ة يرش ب ل و  
امك ة ق ق د ن و ك ت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م چ ر ة . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه  
ل ا م ة ا د ع و چ ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ة س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل چ ن إ ل ا دن تسمل ا