

# Snort3 ي ف ص صخ م يلحم لقان دعاوق نيوكت ىلع FTD

## تايوتحملا

[عمدقملا](#)

[قيساسألا تابلطتملا](#)

[تابلطتملا](#)

[عمدختسملا تانوكملا](#)

[قيساسأ تامولعم](#)

[كك بشلل يطي طختلا مسرلا](#)

[نيوكتلا](#)

[Snort 3 ىلا 2 Snort نم داري ت سا 1. ققير طلا](#)

[Snort رادصا ديكأت 1. ةوطخل](#)

[Snort 2 ي ف ص صخ م يلحم ريخش. دعاوق ريخت وأ عاش بنا 2. ةوطخل](#)

[3. ةرونشلا ىلا 2 ترونشلا نم ةص صخ م يلحم لا طنشلا دعاوق داري ت سا 3. ةوطخل](#)

[دعاوقلا عارجا ريغت 4. ةوطخل](#)

[ةدروتسملا ةص صخ م يلحم لا تاريخشلا دعاوق ديكأت 5. ةوطخل](#)

[\(ACP\) لوصولا ي ف مكحتلا ةساسس. دعاوق ل ل ل س ت لا ةساسس طبر 6. ةوطخل](#)

[تاريخي غتلا رشن 7. ةوطخل](#)

[يلحم فلم لني م ح ت 2. ققير طلا](#)

[Snort رادصا ديكأت 1. ةوطخل](#)

[ةص صخ م يلحم تاي رخش دعاوق عاش بنا 2. ةوطخل](#)

[ص صخ م يلحم لا ريخشلا دعاوق لي م ح ت 3. ةوطخل](#)

[دعاوقلا عارجا ريغت 4. ةوطخل](#)

[اهلي م ح ت مت ي ت لا ةص صخ م يلحم لا تاريخشلا دعاوق ديكأت 5. ةوطخل](#)

[\(ACP\) لوصولا ي ف مكحتلا ةساسس. دعاوق ل ل ل س ت لا ةساسس طبر 6. ةوطخل](#)

[تاريخي غتلا رشن 7. ةوطخل](#)

[ةحصلا نم قق ح ت لا](#)

[HTTP مداخي فلملا تايوتحم طبض 1. ةوطخل](#)

[يولوا HTTP ب ل ط 2. ةوطخل](#)

[ل ف ط ت لا ث د ح ديكأت 3. ةوطخل](#)

[\(FAQ\) ةل واد ت م لا ةلى س أ لا](#)

[اهجالص او اعاطخ أ لا فاشك ت سا](#)

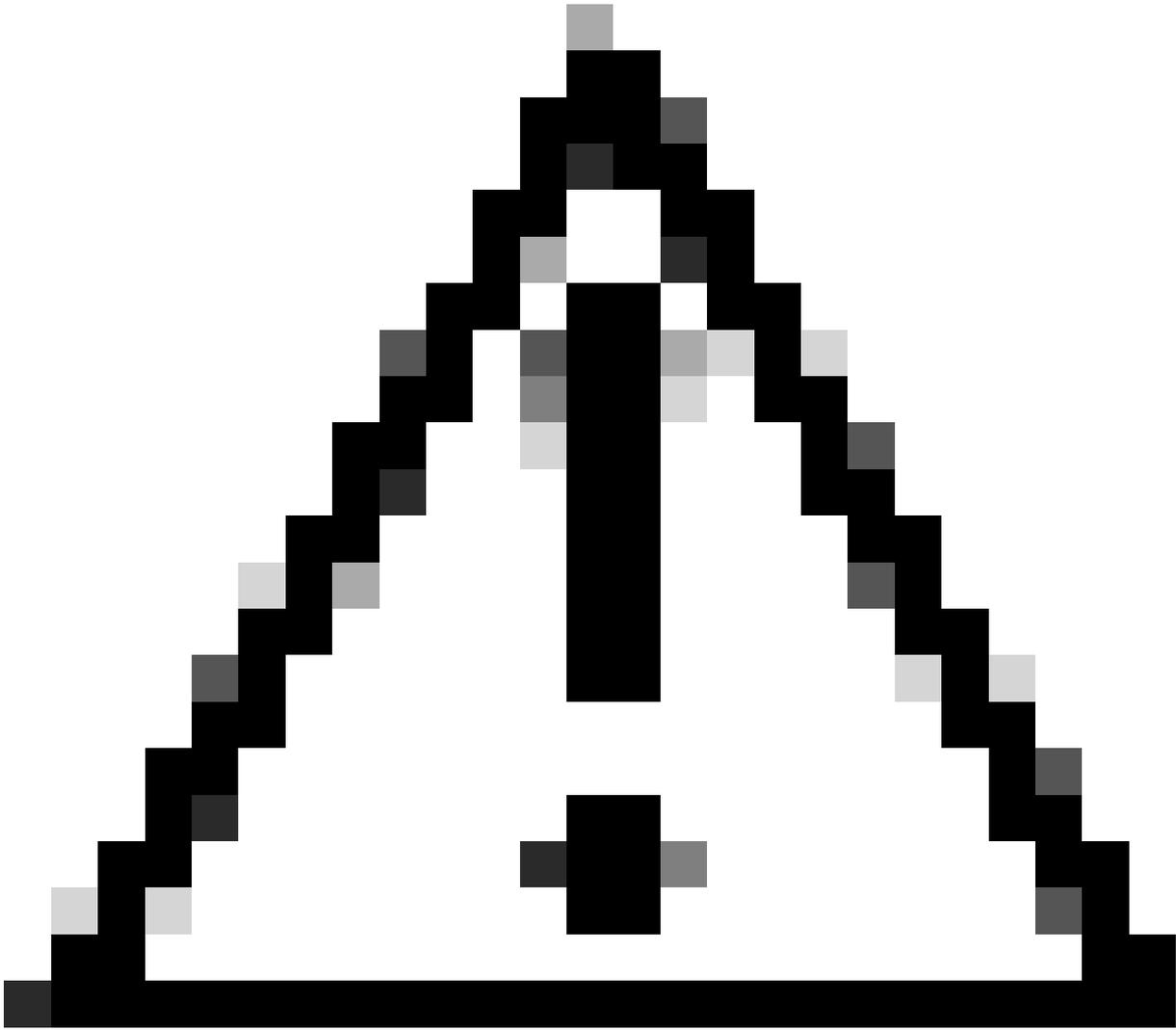
[عجرملا](#)

## عمدقملا

ىلع SNORT3 ي ف ص صخ م يلحم لا لاصتالا دعاوق نيوكت عارجا دن تسملا اذه فص ي  
(FTD). ةي ام ح لا رادج ديدهت دض عافدلا

## ةيساسألا تابلطتملا



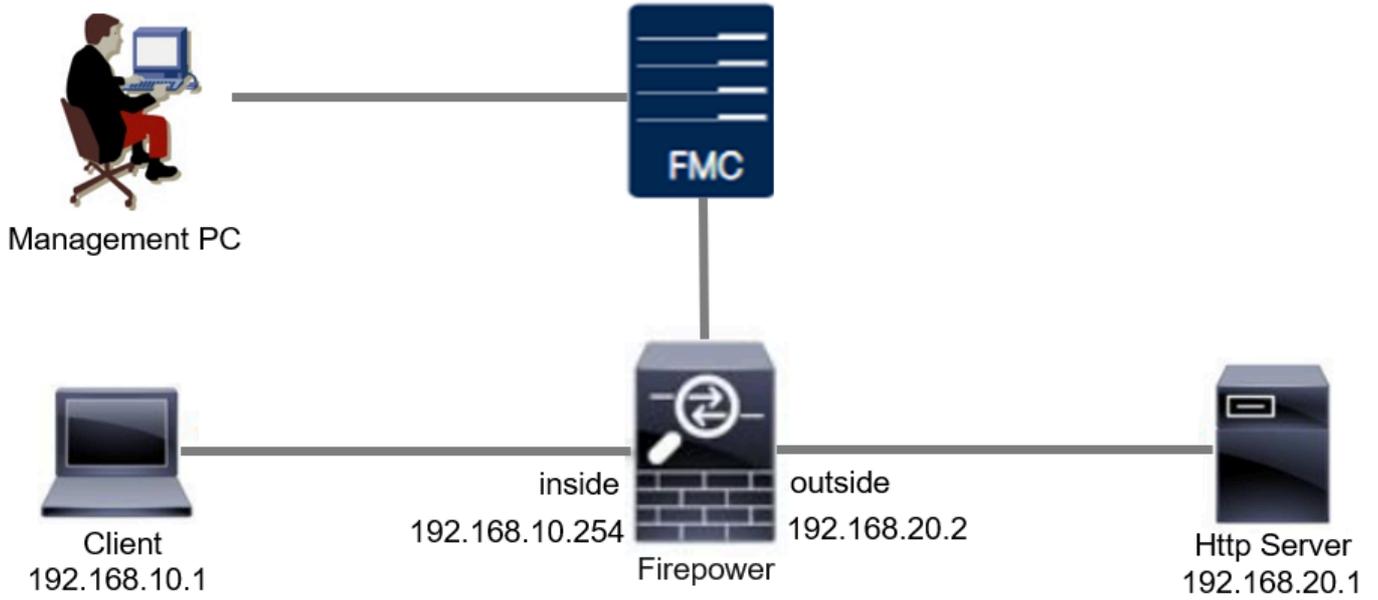


ق اطن ج راخ اهل معدلا ريفوت و ةصصخم ةيلحم لاصتا دعاوق عاشنا عقي :ريذحت  
كنم بلطتو ،طقف عجرمك دنتسملا اذه مادختسا نكمي ،كلذل TAC معد ةي طغت  
كتيلوؤسمو كريدقتل اقفو اهتراداو ةصصخملا دعاوقلا هذه عاشنا

---

## ةكبش لل يطي طختلا مسرلا

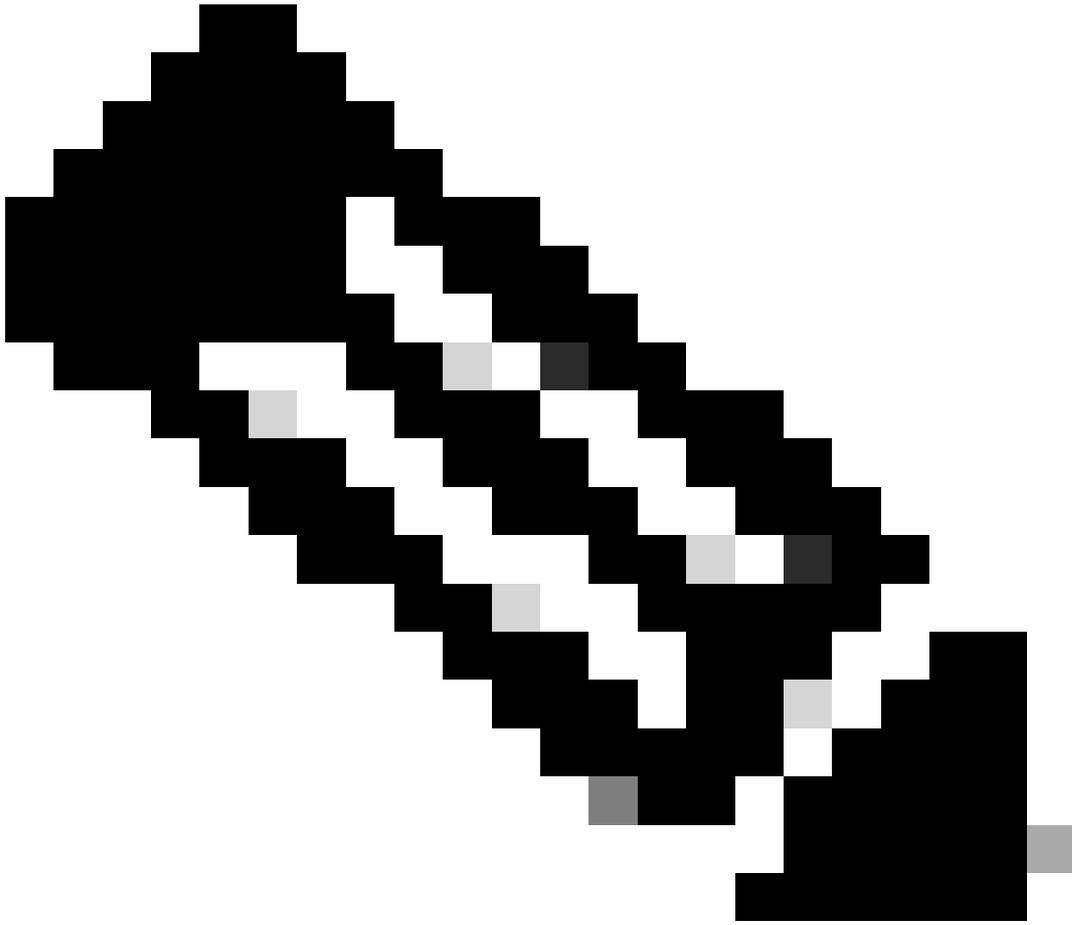
ىلع Snort3 يف ةصصخملا ةيلحملا ةكوشلا دعاوقل ققحتلا او نيوكتلا دنتسملا اذه مدقي  
طاطخملا اذه



ةكبش ل ل يطي طختال مسرلا

## نيوكتلا

يتل HTTP ةباجتسإ مزح فاشتكال ةصصخملا ةيحلحمل نيوكتلا ةدعاق نيوكت وه اذه اهطاقسإو (مدختسمل مسإ) ةدحمةلسلسل ع يوتحت



Snort 3 ةحفص نم ةصصخم ةيلحم تانايب دعاقو ةفاضا نكمي ال ، نألا ىتح : ةظحالم  
ةقيرطالا مادختسا بجي . FMC ل GUI) ةيموسرلا مدختسملا ةهجاوي ف All Rules  
دنتسملا اذه ف ةمدقملا

---

## Snort 3 لىل Snort 2 نم داريتسا . 1 ةقيرطالا

ريخشلا رادصا ديكأت . 1 ةوطخلا

ريخشلا رادصا نأ نم دكأت . DeviceTab ةادا قوف رونا ، FMC لىل ةزهجالا ةرادا ةزهجالا لىل لقتنا  
وه Snort3.



(مدخست مسال).

- رسالة: custom\_http\_sig
- هبنت: اءال
- لوك ووربل: TCP
- لمل ل لبتم: قف دتل
- (ماخ تانا ب) مدخست مسال مسا: ىوت حمل

The screenshot shows the 'Edit Rule' configuration page in the Firewall Management Center. The rule is named '1:1000000:3'. Key configuration details include:

- 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
  - 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:**

ءءاق لل ءرورضال تامول عمل لاء

3 ءرونشال لىل 2 ترونشال نم ءصصمالم ءىل حمل طنشال ءءاق ءارل س. 3 ءوطمالم

ك) All Rules > (لفطال ءءاق) Snort 3 All Rules > لفظال ءءاق > تانئاك لىل لقتنا مالم ءلرسال ءمئاق نم ءارل س او Snort 2 ءءاق لىوحت قوف رقناو، FMC لىل (ءءاق ل)

The screenshot shows the 'All Rules' configuration page in the Firewall Management Center. The page displays a list of rules with columns for Rule Actions, Info, Rule Action, and Assigned Groups. A 'Tasks' dropdown menu is visible, showing options like 'Upload Short 3 rules', 'Convert Snort 2 rules and import', and 'Convert Snort 2 rules and download'.

قف اووم قوف رقناو ريذحت ال ةلاس ر نم ققحت

## 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

ريذحت ةلاس ر

تالوحم ال ةفاك قوف رقنا، FMC إلى ع Snort 3 All Rules > لفطت ال دعاق > تانئاك إلى لقتنا اه اداريتس مت ي ت ال صصم ال يلحم ال رخش ال ةدعاق ديكا ت ال اه ليوت مت ي ت ال 2 ةماع ال

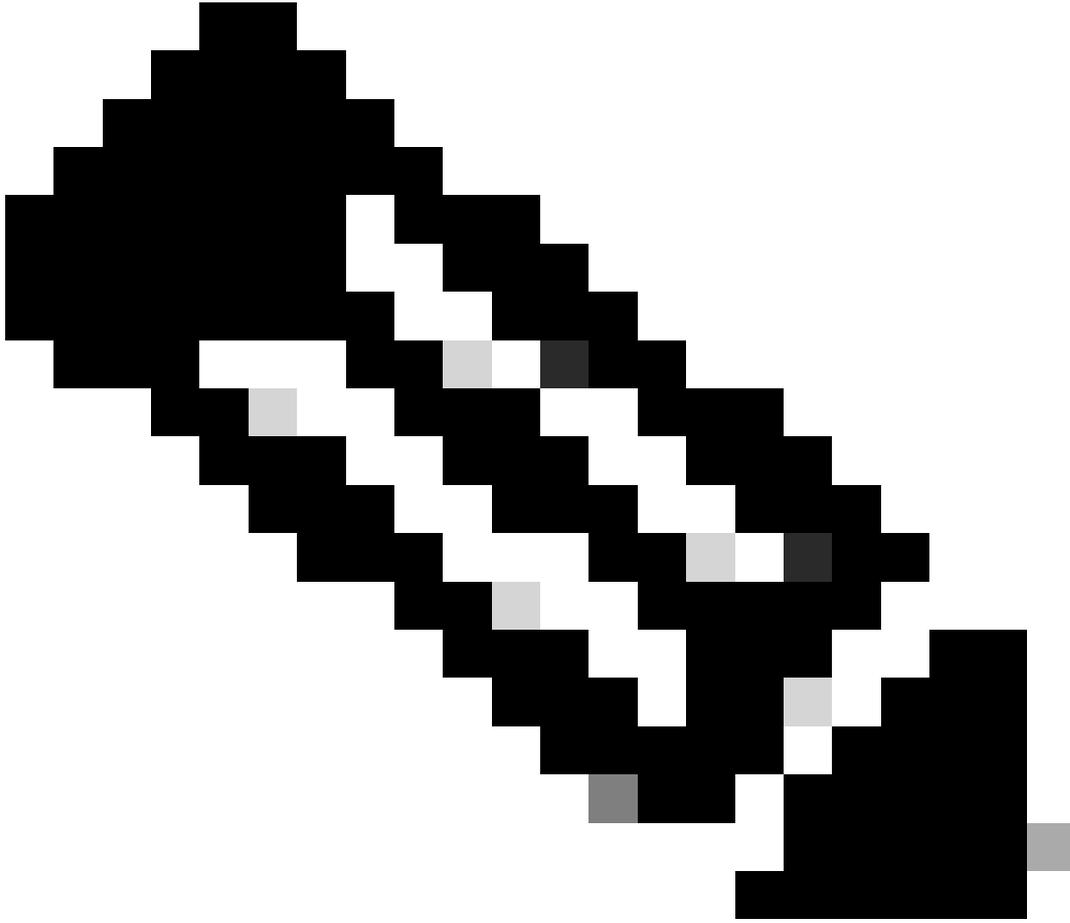
| GID:SID      | Info            | Rule Action       | Assigned Groups              | Alert Configuration |
|--------------|-----------------|-------------------|------------------------------|---------------------|
| 2000:1000000 | custom_http_sig | Disable (Default) | All Snort 2 Converted Glo... |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

ةدروت س م ال ةصصم ال ةدعاق ال ديكا ت

ةدعاق ال ارج ريغت 4. ةوطخ ال

فده ال ةصصم ال ةدعاق ال اب ةصاخ ال ةدعاق ال ارج ال اقو ل خدت لك جهن قوف رقنا





يه ةدعاقلا تاءارجا :ةظحالم

اذه يف ةيلالاتلا مزحلا ةفاكو ةيلالجال ةقباطملا ةمزحلا رطحو، ثدح عاشنإ —رطح  
لاصتالا.

وأ ةمزحلا طاقسإب موقوي الو ةقباطملا ةمزحلل طقف ثادحأ عاشنإب موقوي —هينبنت  
لاصتالا.

رايخ ىلإ ادانتسا ةمزحلا تايوتحم لدبتسيو ثدح عاشنإب موقوي —ةباتكلا ةداع  
ةدعاقلا يف لادبتسالا.

مبيقتلا نم ديزم ءارجا نود رورملا ةمزحلل حمسي، ثادحأ يأ عاشنإ متي ال —Pass  
ةيلالات snort دعاقو يأ ةطساوب.

ةكرح نم ديزملا عنمي الو ةقباطملا ةمزحلا طقسوي، ثدحلا عاشنإب موقوي —drop  
لاصتالا اذه يف رورملا.

ةيفاضالا رورملا ةكرح عنمو، ةقباطملا ةمزحلا طاقسإو، ثدح عاشنإب موقوي —ضفر  
ردصملا يف يضم TCP لوكوتورب ناك اذا TCP نبيعت ةداعا لاسراو لاصتالا اذه يف

ةوجلواو.

ثادحأ يأ عاشنإ متي مل .ةدعاقلا هذه عم تانايبلا رورم ةكرح قباطي ال—disable

م.اظنلل يضا رتفال اءارجإلا يلا عجرى—يضا رتفال

### Edit Rule Action

2000:100... | custom\_http\_sig

All Policies  Per Intrusion Policy

Policy: snort\_test Rule Action: BLOCK

Add Another

Comments (optional)  
Provide a reason to change if applicable

Cancel Save

ةدعاقلا ريرحت اءارج

ةدروت سمل اةص صخمل اةيلحمل ا تاريخشلا ةدعاق ديكأت 5 ةوطخل

لباقملا Snort 3 رادصا قوف رقنا ،FMC يلع ماحتقالا تاسايس > تاسايسلا يلا لقتنا  
فصلا يف فدهلا ماحتقالا جهنل

Firewall Management Center

Policies / Access Control / Intrusion / Intrusion Policies

Overview Analysis Policies Devices Objects Integration Deploy Search admin | Cisco SECURE

Intrusion Policies Network Analysis Policies

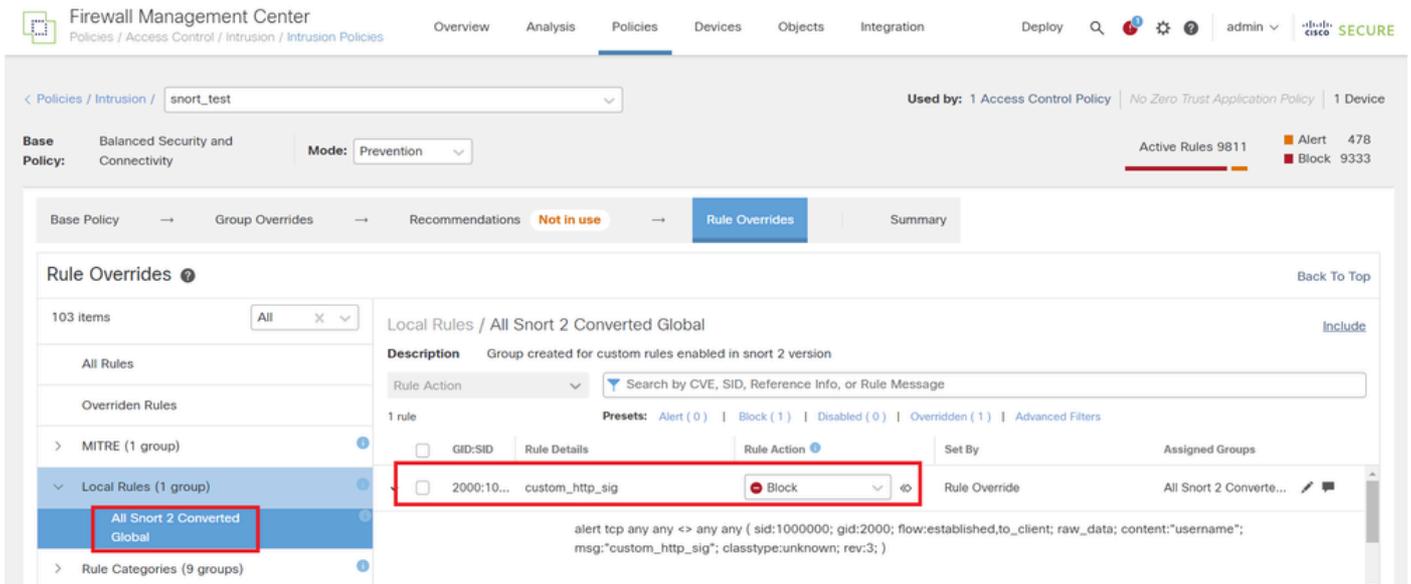
Hide Snort 3 Sync status Search by Intrusion Policy, Description, or Base Policy All IPS Rules IPS Mapping Compare Policies Create Policy

| 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

ةدروت سمل اةص صخمل اةدعاقلا ديكأت

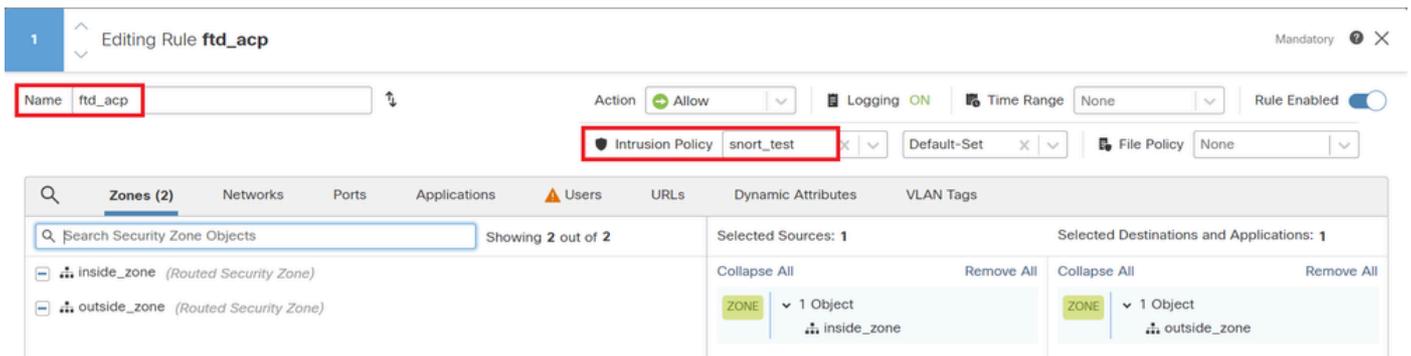
نم ققحتلل Snort 2 ل ةلوحمل اةيمومعلا ةالوحمل اةفاك > ةيلحمل اءاوقلا قوف رقنا  
ةص صخمل اةيلحمل اةجنشلا ةدعاق لياصاف



دروت سمل ءص صخمل ءءءاق لل ءكأت

(ACP) لوصولل ءف مكحتلل ءسائس ءءءاقب للستلل ءسائس طبر 6 ءوطخل

ACP ءم مءحتق الل ءسائس طبرأ ، FMC لالء نم لوصولل ءف مكحتلل ءءءاقب للستلل ءسائس لقتنا



ACP ءءءاقب نارتق الل

تارئفءلل رشن 7 ءوطخل

FTD ءلء تارئفءلل رشن



تارئفءلل رشن

ءلءم فلم لءمءء 2 ءقوءرطالل

Snort راءصا ءكأت 1 ءوطخل

1 ءقوءرطالل ءف 1 ءوطخل لسفن

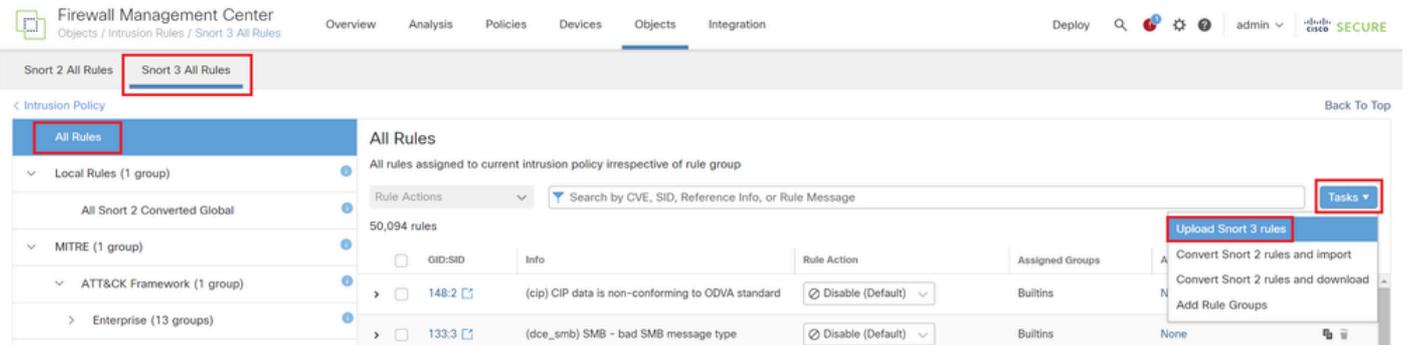
ءص صخمل ءءءاقب للستلل ءسائس طبر 2 ءوطخل

custom-rules.txt. ميسي يلحم فلم ي ف ايودي اهظفحو ةصصخم ةيلحم تاناي ب ةدعاق عاشن اب مق

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

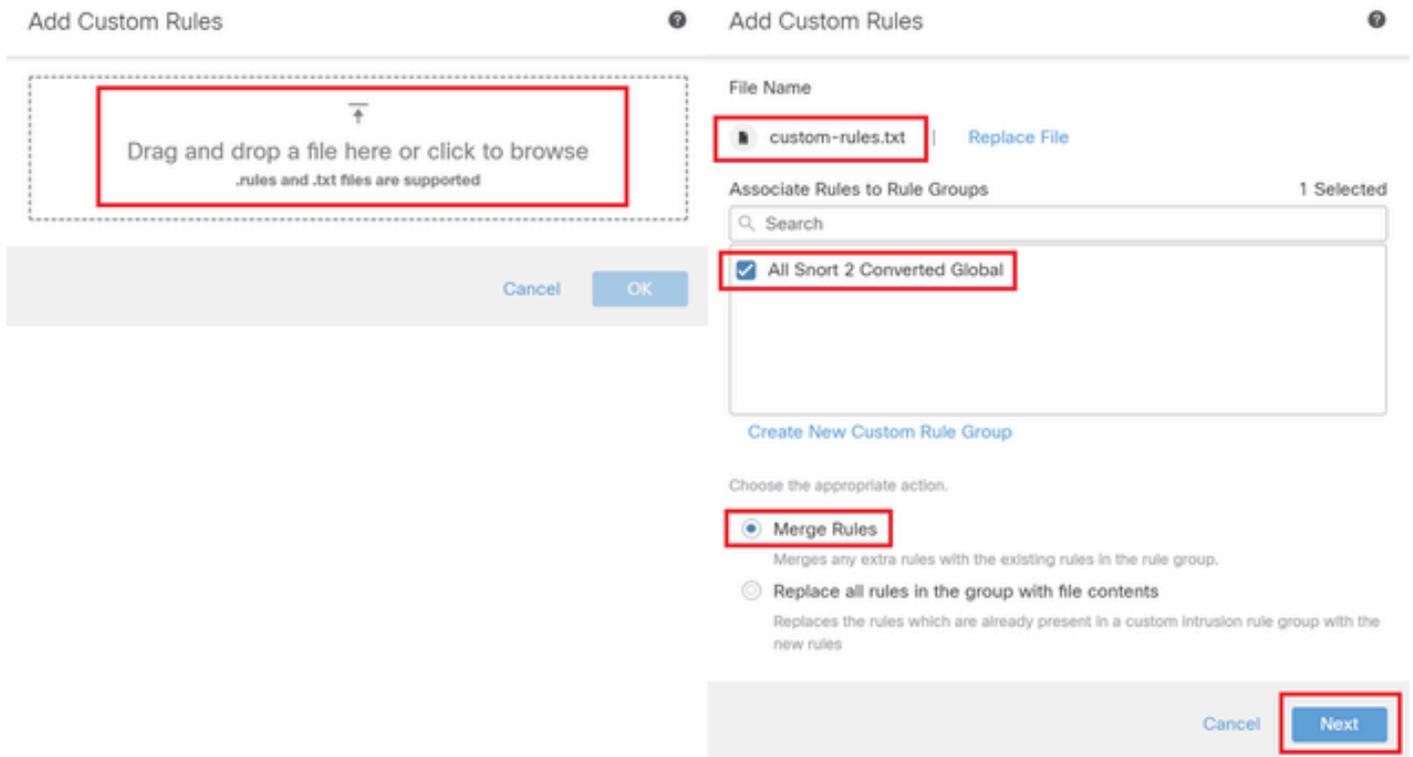
صصخم ل يلحم ل رخشل ةدعاق ليحم ت. 3 ةوطخل

رقنا FMC، لعل دعاق ل عيجم > دعاق ل ةفاك Snort 3 > ماحتقالا دعاق > تانئاك ل ل لقتنا  
ماهمل حيرست ةمئاق نم Snort 3 دعاق ليحم ت قوف



ةصصخم ل دعاق ل ليحم ت

دح، يلحم ل custom-rules.txt فلم تالف او بحسب مق، ةصصخم دعاق ةفاضل ةشاش ي ف  
يلال رزرقنا م ت، (لاثلما اذه ي ف دعاق ل جم د) بسانم ل اءال او دعاق ل اءومجم



ةصصخم ةدعاق ةفاضل



تاريي غتال رشن 7. ةوطخال

1. ةقيرطال ي ف 7 ةوطخال س فن

## ةحصلا نم ققحتلا

HTTP م داخ ي ف فلم ل تايوتحم طبض 1. ةوطخال

م دختسم ل مسا ي ل ع HTTP م داخ بناج ي ل ع test.txt فلم تايوتحم طبضا

ي ل و ال HTTP ب ل ط 2. ةوطخال

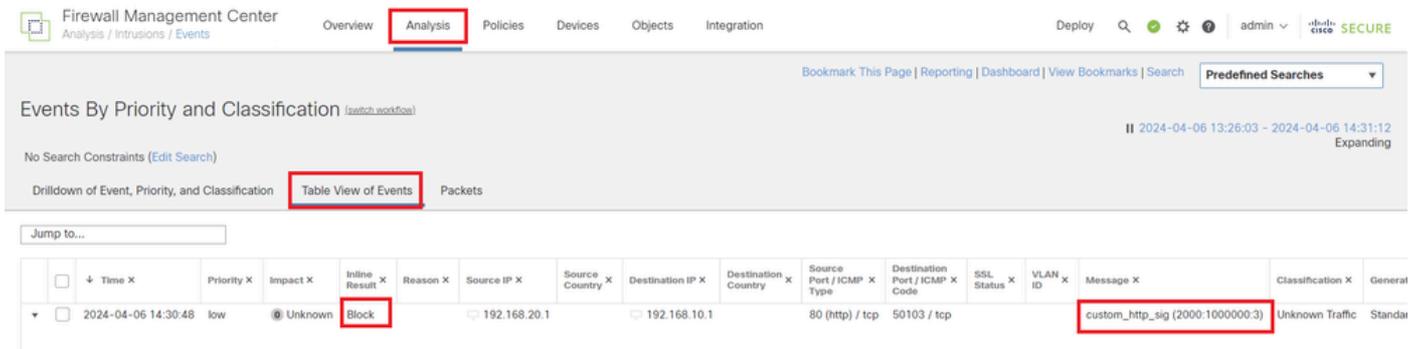
دكأتو (192.168.10.1) ل يم ع ل ضرعتسم نم HTTP (192.168.20.1/test.txt) م داخ ي ل ل و ص و ل اب م ق HTTP ل اص تا ر ط ح نم



ي ل و ال HTTP ب ل ط

ل ف ط ت ل ا ش د ح د ي ك أ ت 3. ةوطخال

ة د ع ا ق ة ط س ا و ب ه و ا ش ن ا م ت Intrusion ش د ح ن ا د ك ا ، Analysis>Intrusion>EventSon FMC ي ل ل ق ت ن ا ة ص ص خ م ل ا ة ي ل ح م ل ا ة ج ن ش ل ا



م ا ح ت ق ا ش د ح

ل ف ط ت ل ا ش د ح ل ي ص ا ف ت د ي ك أ ت ClickPacketStab.

Firewall Management Center Analysis / Intrusions / Events Overview Analysis Policies Devices Objects Integration Deploy Search admin case SECURE

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

Events By Priority and Classification /[/search/2024/04/06](#)

No Search Constraints (Edit Search)

2024-04-06 13:26:03 - 2024-04-06 14:32:46 Expanding

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

Event Information

|                              |                                  |
|------------------------------|----------------------------------|
| Message                      | custom_http_sig (2000:1000000:3) |
| Time                         | 2024-04-06 14:31:26              |
| 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 | 50105 / tcp                      |
| HTTP Hostname                | 192.168.20.1                     |
| HTTP URI                     | /nest.txt                        |
| Intrusion Policy             | snort_test                       |
| Access Control Policy        | acp_rule                         |
| Access Control Rule          | ftd_acp                          |

Rule: alert tcp any any <> any any ( sid:1000000; gid:2000; flow:established,to\_client; rax\_data: content:"username"; msg:"custom\_http\_sig"; classtype:unknown; rev:3; )

Actions

محتوى الـ IDS الذي تم اكتشافه

## FAQ (أسئلة وأجوبة)

3 ترين وأ 2 ترين ، هب يصوملا وه ام : س  
رايخال هل عجي امم ، ةديج تازيمو ةن سحم ةجلا عم تاعرس Snort 3 رفوي ، Snort 2 عم ةنراقم لاب : أ  
ربكأ لكش هب يصوملا

م تي له ، شحأ رادصا وأ 7.0 رادصا إلى 7.0 رادصا لبق FTD رادصا نم ةيقرتلا دعب : س  
3 رادصا إلى ايئاق لت snort رادصا شي دحت ؟  
هنيكمت بجي ، ةيقرتلا دعب Snort 3 مادختس ال 2. تروش يي لازي ال شيتفتلا كرحم ، ال  
نسحتسمل نم هنأو لبق تسمل يي Snort 2 رادصا لامه ططخمل نم هنأ طحال جحيرص لكش ب  
نأل همادختس نع فقوتلا ةدشب

ثلاث الفصنل يي ةدوجوم ةصصخم ةدعاق ريرحت نكمملا نم له : س  
ةدعاق ةلصللا تاذ ةدعاق ل فذح بجي ، ةني عم ةصصخم ةدعاق ريرحتل . هريحت كنكمي ال ، ال : أ  
اهئاشن

## اهحالص او ءاطخال فاشكتسا

ةطساوب HTTP رورم ةكرح رطح م تي ، لاثملا اذه يي FTD. لعل كولسل ديكتل رمأل system support trace ليغشتب مق  
ةدعاق IPS (2000:100000:3).

<#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

عجرجملا

[Cisco Secure Firewall Management Center 3](#) جمانرب نيوكت ليلد

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد ىوتحم مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتحم مچرت مءم دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوءو تاملرتل هذه ةقء نء اهءل ءوئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزىل ءن إل دن تسمل