

# يـف ةـصـصـخـم ةـيـلـحـم تـاـنـاـيـب دـعـاـوـق نـيـوـكـت Snort2 FTD ىـلـع

## تاـيـوـتـحـمـلـا

[ةـمـدـقـمـلـا](#)

[ةـيـسـاسـأـلـا تـاـبـلـطـتـمـلـا](#)

[تـاـبـلـطـتـمـلـا](#)

[ةـمـدـخـتـسـمـلـا تـاـنـوـكـمـلـا](#)

[ةـيـسـاسـأـتـامـوـلـعـمـ](#)

[نـيـوـكـتـلـا](#)

[ةـلـكـشـلـلـيـطـيـطـخـتـلـا مـسـرـلـا](#)

[نـيـوـكـتـلـا](#)

[رادـصـراـدـيـكـأـ1ـ قـوـطـخـلـا Snort](#)

[يـفـةـصـصـخـمـةـيـلـحـمـتـاـيـرـخـشـ،ـقـدـعـافـ،ـعـاـشـنـاـ2ـ قـوـطـخـلـا Snort 2](#)

[صـصـخـمـلـا ئـيـلـحـمـلـا رـخـشـلـا،ـقـدـعـافـ،ـدـيـكـأـ3ـ قـوـطـخـلـا](#)

[قـدـعـاقـلـا عـاـرـجـاـرـيـغـتـ4ـ قـوـطـخـلـا](#)

[لـوـصـولـا يـفـمـكـحـتـلـا قـسـاسـسـ،ـقـدـعـاقـبـ لـلـسـتـلـا قـسـاسـسـ طـبـرـ5ـ قـوـطـخـلـا](#)

[تـاـرـيـغـتـلـا رـشـنـ6ـ قـوـطـخـلـا](#)

[قـحـصـلـا تـمـ قـرـحـتـلـا](#)

[صـصـخـمـلـا ئـيـلـحـمـلـا رـخـشـلـا قـدـعـاقـلـا لـيـغـشـتـ مـتـيـ مـلـ](#)

[مـدـاخـيـفـ فـيـلـمـلـا تـاـيـوـتـحـمـ طـبـضـ1ـ قـوـطـخـلـا HTTP](#)

[يـلـوـأـلـا HTTP بـلـطـ2ـ قـوـطـخـلـا](#)

[صـصـخـمـلـا ئـيـلـحـمـلـا رـخـشـلـا قـدـعـاقـلـا لـيـغـشـتـ مـتـ](#)

[مـدـاخـيـفـ فـيـلـمـلـا تـاـيـوـتـحـمـ طـبـضـ1ـ قـوـطـخـلـا HTTP](#)

[يـلـوـأـلـا HTTP بـلـطـ2ـ قـوـطـخـلـا](#)

[لـفـطـتـلـا دـيـكـأـثـدـجـ3ـ قـوـطـخـلـا](#)

[اهـالـصـ اوـعـاطـخـأـلـا فـاشـكـتـسـا](#)

## ةـمـدـقـمـلـا

ىـلـعـ SNORT2 يـفـةـصـصـخـمـلـا ئـيـلـحـمـلـا لـاـصـتـالـا دـعـاـوـقـ نـيـوـكـتـ عـاـرـجـاـ دـنـتـسـمـلـا اـذـهـ فـصـيـ

## ةـيـسـاسـأـلـا تـاـبـلـطـتـمـلـا

### تـاـبـلـطـتـمـلـا

ةـيـلـاتـلـا عـيـضـاـوـمـلـابـ ئـفـرـعـمـ كـيـدـلـ نـأـبـ يـصـوتـ:

- Cisco FireSIGHT (FMC) زـكـرمـ
- ئـيـامـحـلـا رـادـجـ دـيـدـهـتـ دـضـ عـافـدـلـا (FTD)

## ةمـدـخـتـسـمـلـا تـانـوـكـمـلـا

ةـيـلـاتـلـا ةـيـدـامـلـا تـانـوـكـمـلـا وجـمـارـبـلـا تـارـادـصـا ئـلـا دـنـتـسـمـلـا اـذـهـ يـفـ ةـدـرـاـوـلـا تـامـوـلـعـمـلـا دـنـتـسـتـ

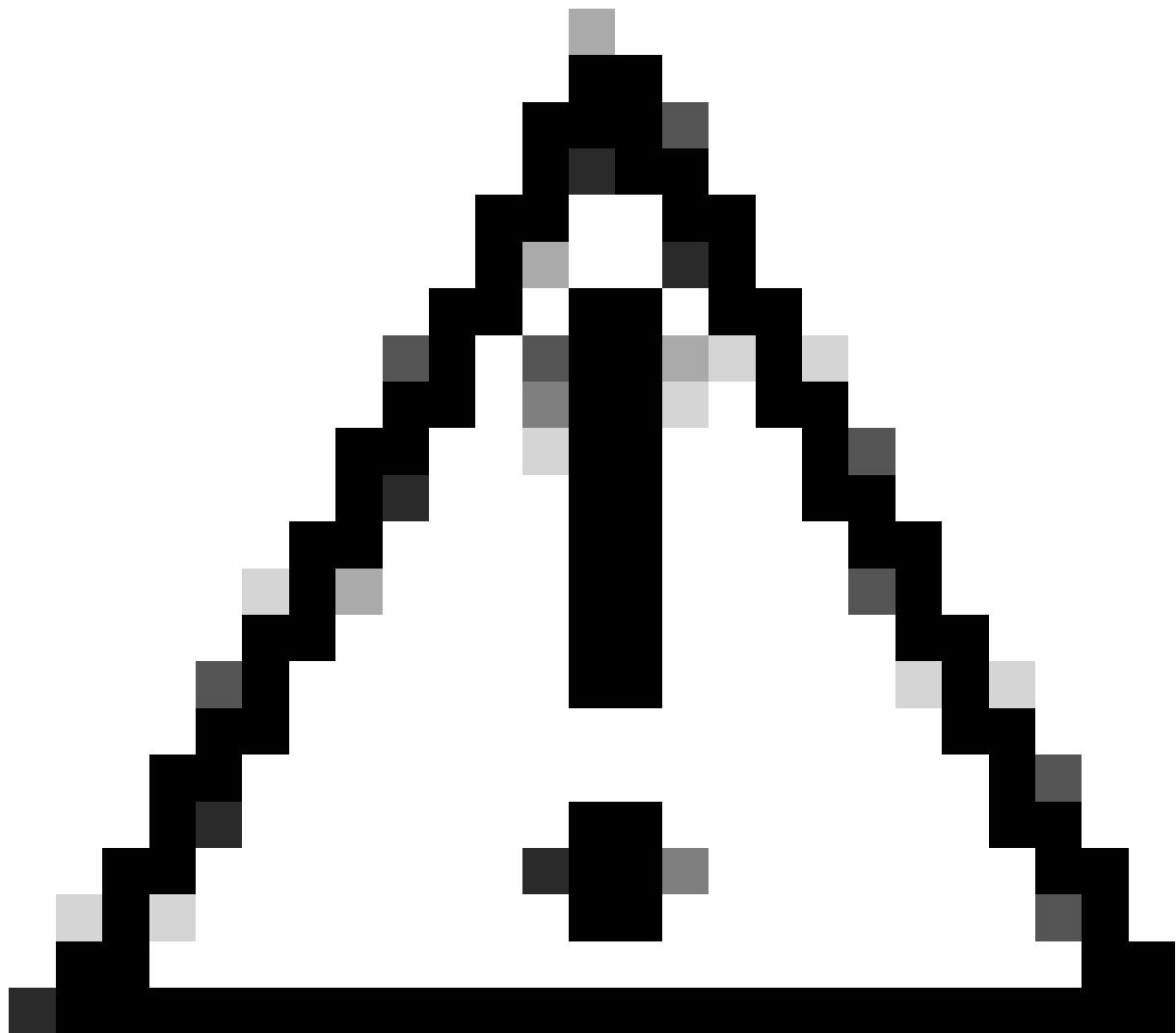
- Cisco Firepower 7.4.1 ل VMWare
- Cisco Firepower 2120 7.4.1

ةـصـاخـ ةـيـلـمـعـمـ ةـيـيـبـ يـفـ ةـدـوـجـوـمـلـا ةـزـهـجـأـلـا نـمـ دـنـتـسـمـلـا اـذـهـ يـفـ ةـدـرـاـوـلـا تـامـوـلـعـمـلـا عـاـشـنـا مـتـ  
تـنـاـكـ اـذـاـ (ـيـضـاـرـتـفـاـ) حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـا اـذـهـ يـفـ ةـمـدـخـتـسـمـلـا ةـزـهـجـأـلـا عـيـمـجـ تـأـدـبـ  
رـمـأـ يـأـلـ لـمـتـحـمـلـا رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ ،ـلـيـغـشـتـلـا دـيـقـ كـتـكـبـشـ.

## ةـيـسـاسـأـ تـامـوـلـعـمـ

كـنـكـمـيـ مـدـخـتـسـمـلـا لـبـقـ نـمـ ةـفـرـعـمـ ةـدـعـاـقـ ئـلـا "ـةـصـصـخـمـلـا ةـيـلـحـمـلـا رـخـشـلـا ةـدـعـاـقـ"ـ رـيـشـتـ  
اـمـدـنـعـ يـفـ جـمـدـمـلـا مـدـاـخـلـا ئـلـعـ لـفـطـتـلـا عـنـمـوـ فـاـشـتـكـاـ مـاـظـنـ لـخـادـ اـهـذـيـفـنـتـوـ اـهـؤـاشـنـا  
فـيـرـعـتـبـ سـاـسـأـلـاـبـ مـوـقـتـ تـنـأـ،ـ يـفـ ةـصـصـخـمـ ةـيـلـحـمـ رـيـخـشـ ةـدـعـاـقـ عـاـشـنـاـبـ مـوـقـتـ  
رـوـرـمـ ةـكـرـحـ تـقـبـاـطـتـ اـذـاـ.ـ اـهـتـبـقـاـرـمـ رـخـشـلـاـ كـرـحـمـلـ نـكـمـيـ يـتـلـاـ طـوـرـشـلـاـ نـمـ ةـعـوـمـجـ وـأـ دـيـدـجـ طـمـنـ  
دـدـحـمـلـاـ عـاـرـجـإـلـاـبـ تـرـوـشـلـاـ مـوـقـيـ نـأـ نـكـمـيـ،ـ ةـصـصـخـمـلـاـ ةـدـعـاـقـلـاـ يـفـ ةـدـدـحـمـلـاـ طـوـرـشـلـاـ عـمـ ةـكـبـشـلـاـ  
حـبـشـلـاـ دـعـاـوـقـ نـوـلـوـفـسـمـلـاـ مـدـخـتـسـيـ.ـ ةـمـزـحـلـاـ طـاـقـسـاـ وـأـ هـيـبـنـتـ عـاـشـنـاـ لـلـثـمـ،ـ ةـدـعـاـقـلـاـ يـفـ  
ةـمـاعـلـاـ دـعـاـوـقـلـاـ تـاعـوـمـجـمـ اـهـيـطـغـتـ الـ يـتـلـاـ ةـدـدـحـمـلـاـ تـادـيـدـهـتـلـاـ ةـجـلـاـعـمـلـ ةـصـصـخـمـلـاـ ةـيـلـحـمـلـاـ

مـتـ اـهـنـمـ قـقـحـتـلـاـوـ ةـصـصـخـمـ ةـيـلـحـمـ مـدـاـخـ ةـدـعـاـقـ نـيـوـكـتـ ةـيـفـيـكـ مـيـدـقـتـ مـتـ،ـ دـنـتـسـمـلـاـ اـذـهـ يـفـ  
(ـمـدـخـتـسـمـلـاـ مـسـاـ)ـ ةـدـدـحـمـ ةـلـسـلـسـ ئـلـعـ يـوـتـحـتـ يـتـلـاـ H~T~P~ ةـبـاجـتـسـاـ مـزـحـ فـاـشـتـكـاـلـ اـهـمـيـمـصـتـ  
اـهـتـالـفـإـوـ



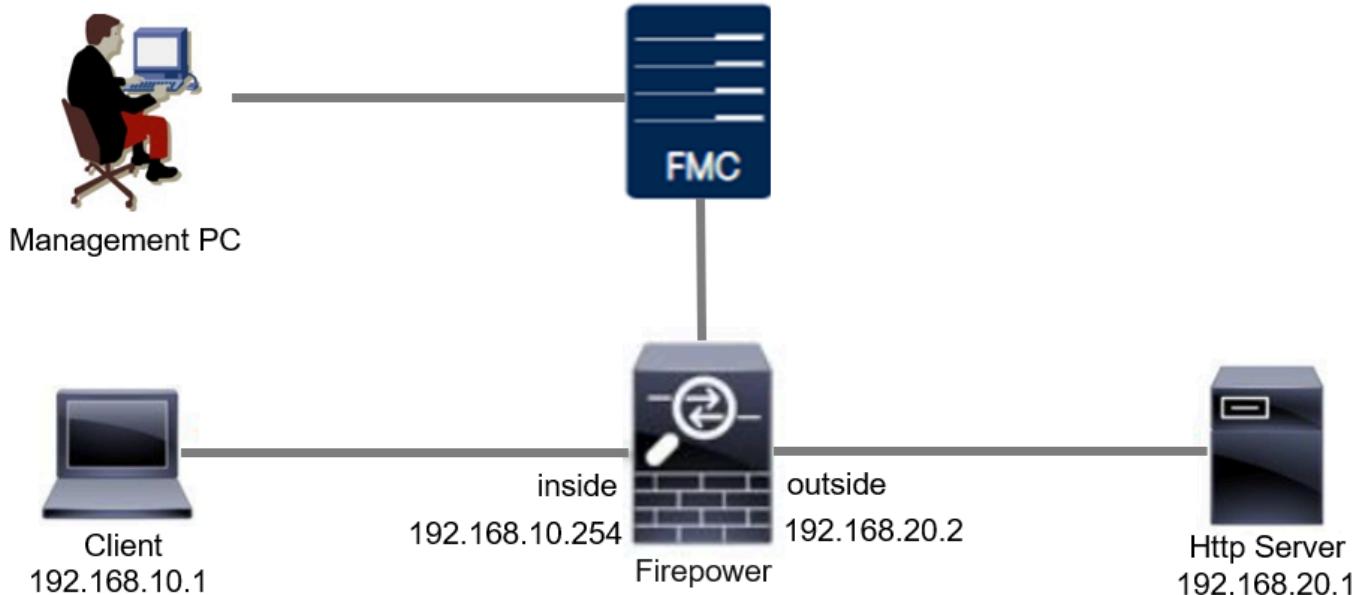
قاطن جراخ اهل معدلاريفوت و ٽصصخم ٽيلحم لاصتا دعاوقي عاشنإ عقي :ريذحت  
كنم بلطتو ، طقف عجرمك دنتسملا اذه مادختسإ نكمي ، كلذل . مععد ٽيطغت  
كتيلوؤسم و كريدىقتل اقفو اهتراداو ٽصصخملا دعاوقيلا هذه عاشنإ.

---

## نيوكتل

### ٽكبشلل يطيطختلا مسرلا

ىلع snort2 يف ٽصصخملا ٽيلحملاتاريخشلا ٽداعقل ققحتلاو نيوكتلا دنتسملا اذه مدقى  
يطيطختلا مسرلا اذه.



## نیوکتلا

یتل ایچ اپ جتسا مزح فاش تکال ۆصص خملا ۆیل حملانیوکتلا ۆدعاق نیوکت وە ادەه طاقس او (مۆدخت سەرەملا مەس) ۆددەم ۆلسلس ىلۇ يوتخت.

رادصى دىكأت 1. ۆوطخىلا Snort

زەھىللا بىۋېتلى ۆمالۇ قوف رقنا، مەكھىتلە ۆدھو يەزەھجىلدا ۆرادى > ۆزەھجىلدا ىلى لقتنە رىخشىلدا رادصى دىكأت.

رادصى Snort

يەزەھجىلە ۆصص خملا ۆیل حملانىوکتلا ۆدعاق ئاشنە 2. ۆوطخىلا

ۆدعاق ئاشنە رز قوف رقنا، قارتىخالا دعاوق > تانئاك ىلى لقتنە.

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

Overview Analysis Policies Devices Objects Integration Deploy admin SECURE

Snort 2 All Rules Snort 3 All Rules

Intrusion Policy

Group Rules By Category (62655)  
app-detect (102)  
browser-chrome (234)

Search Delete Local Rules Import Rules Create Rule

وخصخم ۋە دەعىلەنە

صصخملە يەلەنلە رەشلە دەعىلەنە ئىرورىپەن تامولۇملا لاخداپ مەق.

- قارتىخالا : custom\_http\_sig
- يېبىنت ئارجىلە
- TCP: لوكوتوربىلە
- لىمەعلە تېبىثم: قىفتىلە
- ماخ تانايىب) مەختىسىملا مىسا: يۆتەنەلە

Create New Rule

Message: custom\_http\_sig

Classification: Unknown Traffic

Action: alert

Protocol: tcp

Direction: Bidirectional

Source IPs: any

Destination IPs: any

Source Port: 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

content Add Option Save As New

دەعىلەنە ئىرورىپەن تامولۇملا لاخدا

صصخملە يەلەنلە دەعىلەنە دىكەت. 3. ۋە طەخلى.

2. رادصى رز قوف رقنا، FMC ئىلع لىلسەنلا تاسايىس > تاسايىسلا ئىلەنلىقىتىنە

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

Overview Analysis Policies Devices Objects Integration Deploy admin cisco SECURE

Intrusion Policies Network Analysis Policies

Hide Snort 3 Sync status Search by Intrusion Policy, Description, or Base 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 Snort 2 Version Snort 3 Version

ةصصخملـا ةدعـاقـلـا دـيـكـأـتـ

تـارـيـخـشـلـا ةـدـعـاقـلـا لـيـصـافـتـ نـم دـكـأـتـوـ، يـف ةـيـلـحـمـلـا > ةـيـفـلـا > دـعـاقـلـا لـقـتـنـا ةـصـصـخـمـلـا ةـيـلـحـمـلـا.

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

Overview Analysis Policies Devices Objects Integration Deploy admin cisco SECURE

Intrusion Policies Network Analysis Policies

Policy Information Rules

Cisco Recommendations > Advanced Settings

> Policy Layers

Rule Configuration Rule Content Category file-pdf indicator-compromise indicator-obfuscation indicator-scan indicator-shellcode file-ppt indicator-backdoor malware-cnc malware-other malware-tools netbios os-linux net-mnshare Classifications Microsoft Vulnerabilities Microsoft Worms Platform Specific Preprocessors Priority Rule Update

Rules

Filter: Category:"local"

0 selected rules of 1

Rule State Event Filtering Dynamic State Alerting Comments

GID SID Message

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;)

Add Add SNMP Alert Add

ةصصخـمـلـا ةـدـعـاقـلـا لـيـصـافـتـ

ةـدـعـاقـلـا ءـارـجـا رـيـيـغـتـ 4. وةـوـطـخـلـا

قـفـاـوـمـ رـزـلـا قـوـفـ رـقـنـا مـثـ، ثـادـحـأـلـا ءـاشـنـا وـطـاقـسـا لـلـاحـلـا نـيـيـعـتـ بـمـقـوـ، ؤـلـاحـ قـوـفـ رـقـنـا.

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

Overview Analysis Policies Devices Objects Integration Deploy admin cisco SECURE

Intrusion Policies Network Analysis Policies

Policy Information Rules

Cisco Recommendations > Advanced Settings

> Policy Layers

Rule Configuration Rule Content Category file-pdf indicator-compromise indicator-obfuscation indicator-scan indicator-shellcode file-ppt indicator-backdoor malware-cnc malware-other malware-tools netbios os-linux net-mnshare Classifications Microsoft Vulnerabilities Microsoft Worms Platform Specific Preprocessors Priority Rule Update

Rules

Filter: Category:"local"

0 selected rules of 1

Rule State Event Filtering Dynamic State Alerting Comments

GID SID Message

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;)

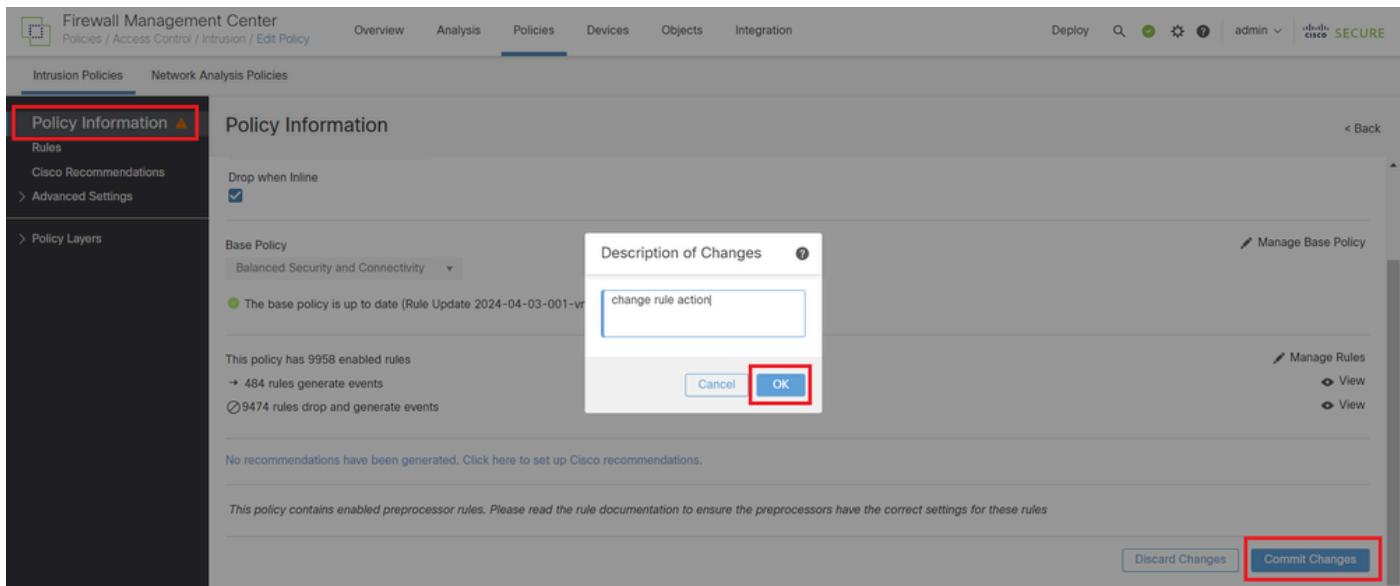
Set rule state for "custom\_http\_sig"

State

Disabled Generate Events Drop and Generate Events Disabled OK Cancel

ةـدـعـاقـلـا ءـارـجـا رـيـيـغـتـ

تارييغتلار ظفحلا ذيفنت رز قوف رقنا مث، جهـنـلـا تـامـولـعـم رـزـلـا قـوـفـ رـقـنـا.

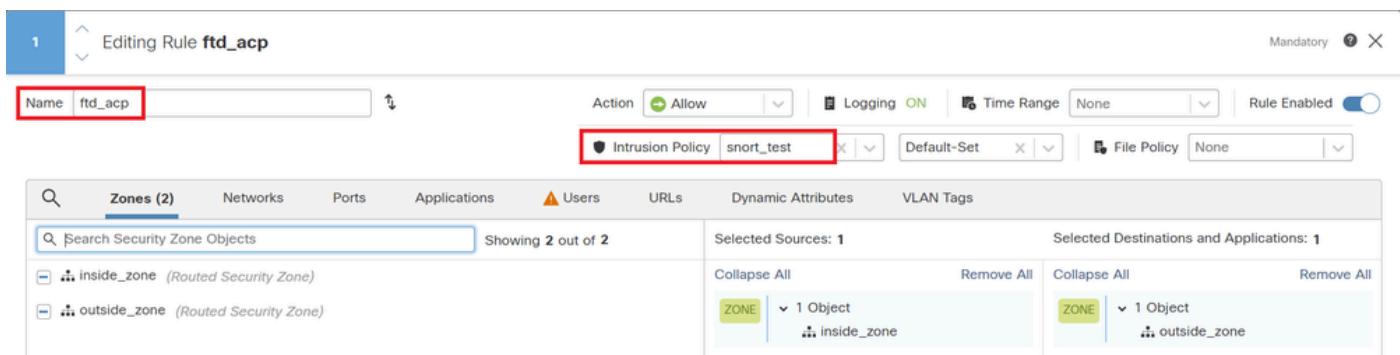


The screenshot shows the 'Policy Information' section of the Cisco FMC interface. On the left, a sidebar lists 'Policy Information', 'Rules', 'Cisco Recommendations', and 'Advanced Settings'. The main area displays policy details: 'Drop when Inline' is checked. Under 'Base Policy', it says 'Balanced Security and Connectivity'. A note states: 'The base policy is up to date (Rule Update 2024-04-03-001-vr)'. It also mentions 'This policy has 9958 enabled rules', '484 rules generate events', and '9474 rules drop and generate events'. A note at the bottom says: 'No recommendations have been generated. Click here to set up Cisco recommendations.' At the bottom right, there are 'Discard Changes' and 'Commit Changes' buttons, with 'Commit Changes' highlighted by a red box.

تارييغتلار ذيفنت

لوصولا يف مكحتلا ئاسايىس ڈعاقب لىلسەتلا ئاسايىس طبر. 5. ۋەطخىلا

ب لىلسەتلا ئاسايىس طبرأو، ئىلع لوصولا يف مكحتلا > تاسايىسلار لىلىقتنى.



The screenshot shows the 'Editing Rule ftd\_acp' screen in the Cisco FMC Policy Editor. The rule has an 'Action' of 'Allow', 'Logging ON', and is 'Rule Enabled'. The 'Intrusion Policy' dropdown is set to 'snort\_test' and is highlighted with a red box. The 'Zones' tab is selected, showing two zones: 'inside\_zone' and 'outside\_zone'. The 'Selected Sources' section shows 'Selected Destinations and Applications: 1' with 'inside\_zone' selected. The 'Selected Destinations' section shows 'Selected Destinations and Applications: 1' with 'outside\_zone' selected. The 'Mandatory' checkbox is checked.

ڈعاقب نارتقا

تارييغتلار رشن. 6. ۋەطخىلا

ئىلع تارييغتلار رشن FTD.



The screenshot shows the 'Policies / Access Control / Policy Editor' screen in the Cisco FMC. A rule named 'FPR2120\_FTD' is selected. The 'Deploy' and 'Deploy All' buttons are highlighted with red boxes. The status bar indicates 'Ready for Deployment' and '1 device'.

تارييغتلار رشن

ۋەھىچىلا نم ققحتلا

صىخىملا يلحىملا رخشىلا ڈعاقلىيغشت مىتى مىل

مدادخ يف فلملاتاي وتحم طبض 1. ۋوطخلما

مدادخ بناجىلىع فلم تاي وتحم طبضا مدخلتسىملل.

يلىوألا HTTP بىلەط 2. ۋوطخلما

دكأتو (192.168.10.1) لىيەرلا ضرۇتسىم نىم (192.168.20.1/test.txt) مدادخ يلىلەنلىپ مۇق لاصتاپ حامىسىلا نىم.



يلىوألا HTTP بىلەط

صصىخملالا يلىحىمىلا رخشىلا ۋەدىعاقلىغىشتىت مەت

مدادخ يف فلملاتاي وتحم طبض 1. ۋوطخلما

مدىختىسىملامساىلىع HTTP مدادخ بناجىلىع test.txt فلم تاي وتحم طبضا.

يلىوألا HTTP بىلەط 2. ۋوطخلما

دكأتو (192.168.10.1) لىيەرلا ضرۇتسىم نىم (192.168.20.1/test.txt) مدادخ يلىلەنلىپ مۇق لاصتا رەظەن نىم.



يلىوألا HTTP بىلەط

لەفەتلىا ثەج دىكأت 3. ۋوطخلما

ماھىتقاالا ثەج ئاشنىمەت ھەنأ نىم دكأتو، FMC ئىلىجەتلىا يلىلەنلىپ تاقارتخالا > تادھالا < لەلەنلىپ.

Firewall Management Center

Analysis / Intrusions / Events

Overview Analysis Policies Devices Objects Integration Deploy Search admin SECURE

Events By Priority and Classification (watch workflow)

Search Constraints (Edit Search Save Search)

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

Jump to...

Time	Priority	Impact	Reason	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Type	SSL Status	VLAN ID	Message	Classification	Generat
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

ماحتقاً ثج

## لـفـطـتـلـاـ ثـجـ لـيـصـافـتـ دـيـكـأـتـلـ ،ـمـزـحـلـاـ بـيـوـبـتـلـاـ ـقـمـالـعـ قـوـفـ رـقـنـاـ

Firewall Management Center

Analysis / Intrusions / Events

Overview Analysis Policies Devices Objects Integration Deploy Search admin SECURE

Events By Priority and Classification (watch workflow)

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.htm
Intrusion Policy	snort_test
Access Control Policy	acp_rule
Access Control Rule	fd_acp
Rule	alert tcp any any > any any {sid:100001; gid:1; flow:established,to_client; content:"username"; rambytes: msg:"custom_http_sig"; classtype:unknown; rev:1; }

Actions

ماحتقاً ثج لـيـصـافـتـ

## اهـحـالـصـ اوـعـاطـخـأـلـاـ فـاشـكـتـسـاـ

هـطـسـاـوبـ رـوـمـ ةـكـرـحـ رـظـحـ مـتـيـ ،ـلـاثـمـلـاـ دـيـكـأـتـلـ رـمـأـلـاـ لـيـغـشـتـبـ مـقـ system support trace FTD. لـيـغـشـتـبـ مـقـ (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
```

## هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ  
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ  
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ  
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ  
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ  
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).