

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

تايوتحملا

[عمدقملا](#)

[قيساسألا تابلطتملا](#)

[تابلطتملا](#)

[عمدختسملا تانوكملا](#)

[قيساسأ تامولعم](#)

[كش ليل يطي طختلا مسرلا](#)

[نيوكتلا](#)

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

[Snort رادصا ديكأت 1. ةوطخللا](#)

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

[3. ةرونش للا ىللا 2. ترونش للا نم ةص صخ م يلحم لطنش للا دعاوق داري ت سا 3. ةوطخللا](#)

[دعاوق للا عارجا ريغت 4. ةوطخللا](#)

[ةدروت س م لا ةص صخ م يلحم لطنش للا دعاوق ديكأت 5. ةوطخللا](#)

[\(ACP\) لوصولا ي ف مكحت للا ةساسيس. دعاوق ل ل ل س ت ل لا ةساسيس طبر 6. ةوطخللا](#)

[تاري ي غ ت ل لا ر ش ت 7. ةوطخللا](#)

[يلحم فلم لني م ح ت 2. ققير طلا](#)

[Snort رادصا ديكأت 1. ةوطخللا](#)

[ةص صخ م يلحم تاري خ ش دعاوق عاش بنا 2. ةوطخللا](#)

[ص صخ م يلحم لطنش للا دعاوق لني م ح ت 3. ةوطخللا](#)

[دعاوق للا عارجا ريغت 4. ةوطخللا](#)

[اهلي م ح ت م ت ي ت ل لا ةص صخ م يلحم لطنش للا دعاوق ديكأت 5. ةوطخللا](#)

[\(ACP\) لوصولا ي ف مكحت للا ةساسيس. دعاوق ل ل ل س ت ل لا ةساسيس طبر 6. ةوطخللا](#)

[تاري ي غ ت ل لا ر ش ت 7. ةوطخللا](#)

[ةحصلا نم ققحتلا](#)

[HTTP مداخ ي ف فلم ل تايوتحم ط ب ص 1. ةوطخللا](#)

[ي ل و ل لا HTTP ب ل ط 2. ةوطخللا](#)

[ل ف ط ت ل لا ش د ح د ي ك أ ت 3. ةوطخللا](#)

[\(FAQ\) ةل و اد ت م ل ا ةل ي س أ ل ا](#)

[اهجالص او اعطخ أ ل ا فاش ك ت س ا](#)

[عجرملا](#)

عمدقملا

ىلع SNORT3 ي ف ص صخ م يلحم لطنش للا دعاوق نيوكت عارجا دن ت س م ل ا اذ ه ف ص ي (FTD). ةي ام ح ل ا ر ا د ج د ي د ه ت د ص ع ا ف د ل ا

ةساسألا تابلطتملا

تاب لطلت مل

ة لالتل عيضاوم لابل ة فرعم كيدل نوكت نأب Cisco ي صوت

- Cisco نم FireSIGHT (FMC) ةرادإ زكرم
- (FTD) ةيامحل رادج ديدهت دض عافدلا

ةمدختس مل تانوك مل

ة لالتل ةيدام ل تانوك مل او جماربل تارادصل ل دن تسمل اذ ه ي ة دراو ل تامولعمل دن تست

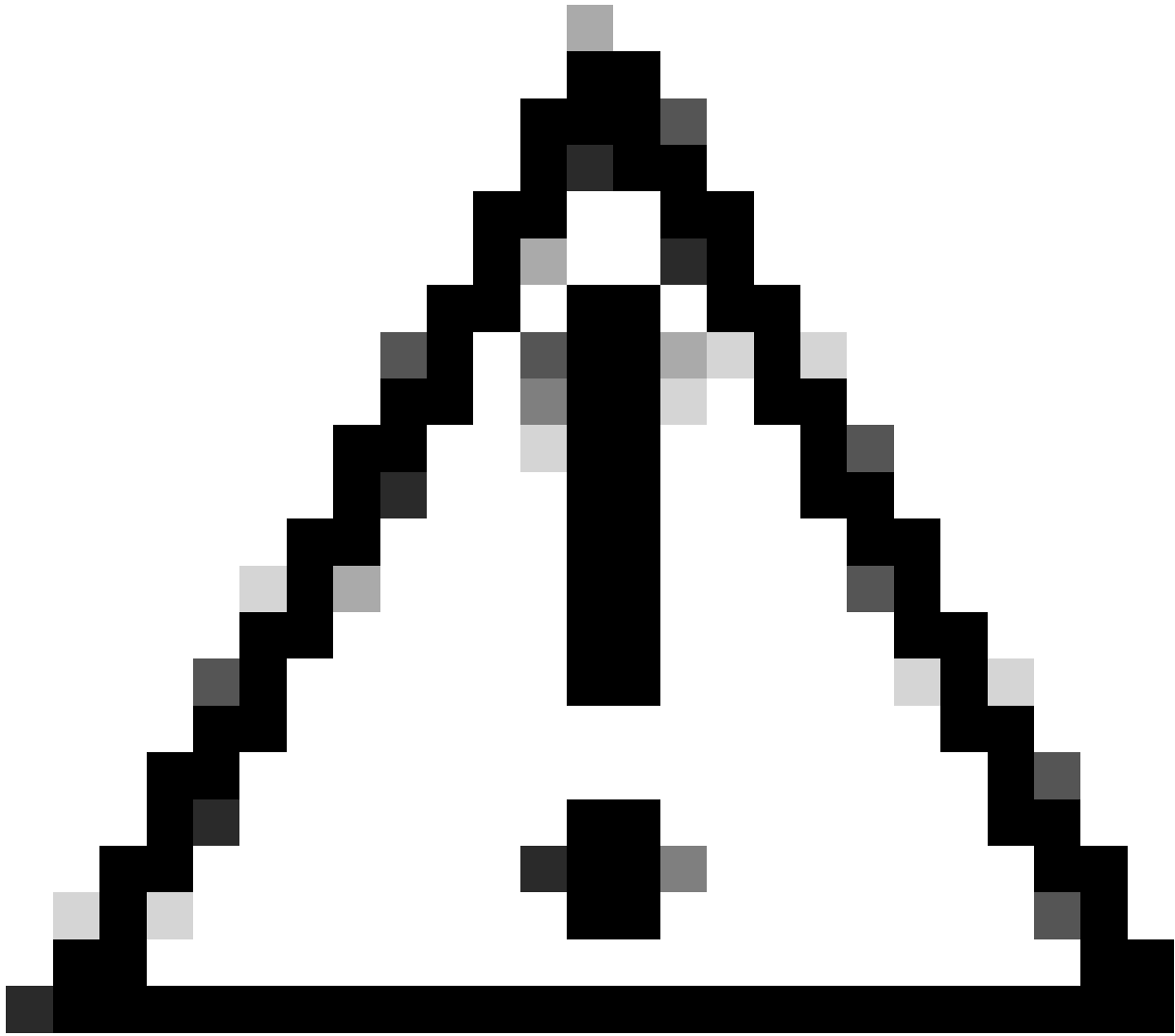
- Cisco Firepower ل VMWare 7.4.1 ةرادإ زكرم
- Cisco Firepower 2120 7.4.1

ة صاخ ةيلمعم ةئيب ي ةدوجوم ل ةزهجال نم دن تسمل اذ ه ي ة دراو ل تامولعمل عاشنإ مت تناك اذإ. (يضا رتفا) حوسمم نيوكتب دن تسمل اذ ه ي ةمدختس مل ةزهجال عيمج تادب رمأ يال لم تحمل ريثأ ل لك م ه ف نم دكأ ت ف، ليغشتل دي ق ك تكبش

ةيساسأ تامولعمل

7. 0 رادصل ل ي ةرادإ ل زكرم عم تاديدهت ل دض عافدلا ي ف Snort 3 جم انرب معد أدبي كرحم Snort 3 ربت عي، ثدجال تارادصل ل او 7.0 رادصل ل نم ةضوعمل او ةديجل ةزهجال ةبس ن لابل يضا رتفا ل ص ح فل

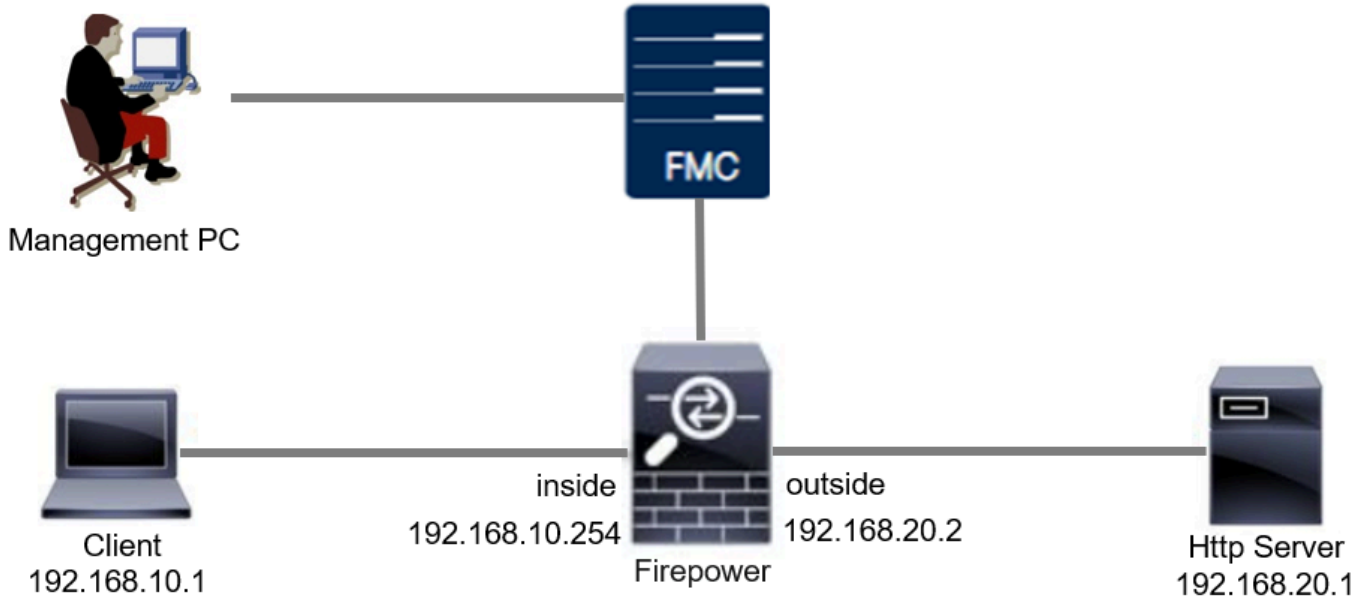
لا ثم ل ةفاض لابل، Snort 3 ل رخشل دعاق صي صخت ةيفيكل الا ثم دن تسمل اذ ه مدقي ققحتل او محتق ةساي س نيوكت ةيفيكل مي دقت متي، صوصخ ل هج و ل عو. يلمع ققحت ةنيعم ةلسلس ل ع يوتحت ي ل HTTP مزح طاقس ل ةص صخم Snort ةدعاق مادختساب انم (مدختس مل م سا).



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

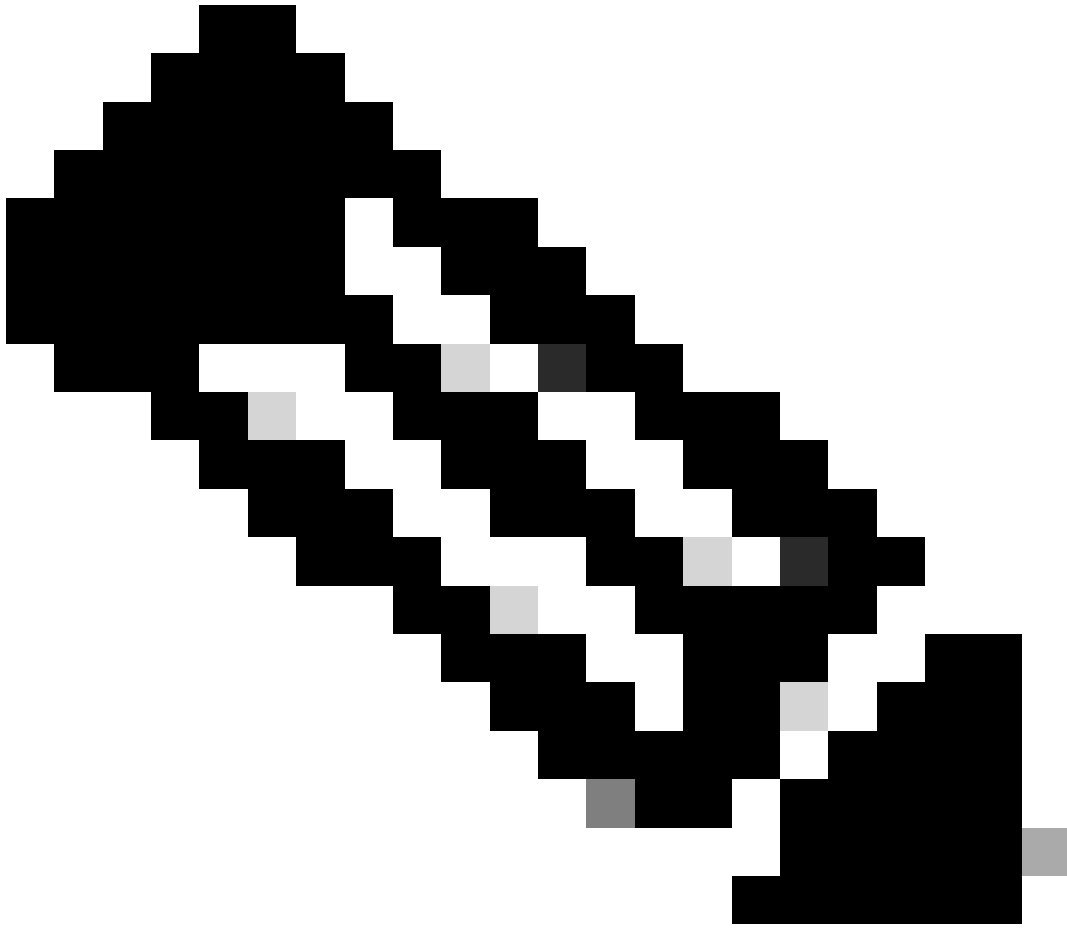
يلع Snort3 يف ةصصخملا ةكوشلا دعاوقل ققحتلاو نيوكتلا دنتسملا اذه مدقي
طاطخملا اذه



ةكبش ل ل يطي طختال مسرلا

نيوكتلا

يتل HTTP ةباجتسإ مزح فاشتكال ةصصخملا ةيلحمل نيوكتلا ةدعاق نيوكت وه اذه اهطاقسإو (مدختسمل مسإ) ةددحم ةلسلس يلع 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.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
FPR2120_FTD	Firepower 2120 with FTD	7.4.1	N/A	Essentials, IPS (1 more...)	acp-rule	

رأى Snort

Snort 2 في صرخم ةي لحم ريخش ةدعاق ريحت وأ عاشنإ 2. ةوطخلإ

عاشنإ رز عاشنإ قوف رونا Snort 2 All Rule On FMC > لفطتلا دعاق > تانئاك ىلإ لقتنا لفطتلا دعاق > تانئاك ىلإ لقتنا وأ، ةص صرخم ةي لحم تانايب ةدعاق ةفاضل تانايب ةدعاق ةطنشلل ةدعاق ريحتل ريحت رز قوف رونا، FMC ىل ع ةي لحم ل دعاقول > Snort 2 All Rules > ةدعاق ةفاضل ةص صرخم ل ةي لحم ل.

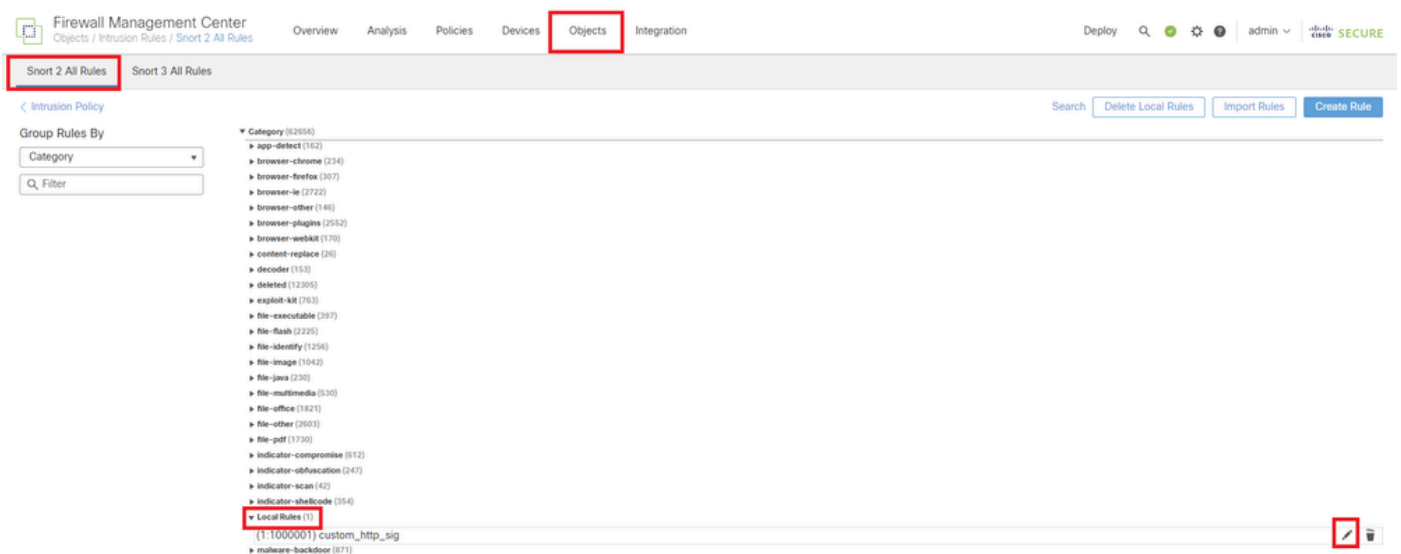
ىجري Snort 2 في صرخم ةي لحم تانايب دعاق عاشنإ ةي فيك لوح تاميلعت ىل ع لوصحلل FTDC Snort2 في صرخم ةي لحم تانايب دعاق نيوك ىل ع وجرلا

ةروصلال في راهظاك ةديج ةص صرخم ةي لحم تانايب ةدعاق ةفاضل.



ةديج ةص صرخم ةدعاق ةفاضل

لا ثمل اذه في ةروصلال في حضورم وه امك ةدوجوم ةص صرخم ةي لحم طبخش ةدعاق ريحتب مق ةدوجوم ةص صرخم ةدعاق رري.



ةدوجوم ةص صرخم ةدعاق ريحت

مسا) ةددم ةلسلس ىل ع يوتحت يتل HTTP مزح نع فشك لل عي قوتل تامولعم لخدأ

(مدخست مسال).

- رسالة: custom_http_sig
- هبنت: اءال
- لوكوتوربل: TCP
- ليملل تبثم: قفدتل
- (ماخ تانايب) مدخست مسال مسا: ىوتحمل

Firewall Management Center
Objects / Intrusion Rules / Create

Overview Analysis Policies Devices **Objects** Integration

Deploy Search Upload Update Intrusion

Snort 2 All Rules Snort 3 All Rules

Edit Rule 1:1000000:3 (Rule Comment)

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

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:

ack Add Option Save Save As New

ءءاق لل ءرورضال تامولءملا لاءا

3 ءرونشل ال ىل 2 ترونشل ال نم ءصصءملا ءىلءملا طنشال ءءاق ءارىتسا 3 ءوطءال

ك) All Rules > (لفطال ءءاق) Snort 3 All Rules > لفظال ءءاق > تانءاك ىل لقتنا مءملا ءىرست ءمءاق نم ءارىتسا او Snort 2 ءءاق لىوت قوف رءناو، FMC ىلء (ءءاقال)

Firewall Management Center
Objects / Intrusion Rules / Snort 3 All Rules

Overview Analysis Policies Devices **Objects** Integration

Deploy Search Upload Update Intrusion

Snort 2 All Rules Snort 3 All Rules

Intrusion Policy

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Actions Search by CVE, SID, Reference Info, or Rule Message Tasks

50,094 rules

Info	Rule Action	Assigned Groups
<input type="checkbox"/> 148:2 (cip) CIP data is non-conforming to ODVA standard	Disable (Default)	Builtins
<input type="checkbox"/> 133:3 (dce_smb) SMB - bad SMB message type	Disable (Default)	Builtins

Upload Short 3 rules

Convert Snort 2 rules and import

Convert Snort 2 rules and download

Add Rule Groups

قفءوم قوف رقنءو ريزءءءل ءلءس ر نم ققءء.

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

ريءءء ءلءس ر

ءالءءم ءلء ءلء قوف رقنءا، FMC ءلء Snort 3 All Rules > لفظءءل ءءءق > ءءءءء ءلء لققءءءا ءءءءرءس ءم ءلء صصمخ م ءلء رءءءء ءءءءء ءم ءلء 2 ءءءءلء.

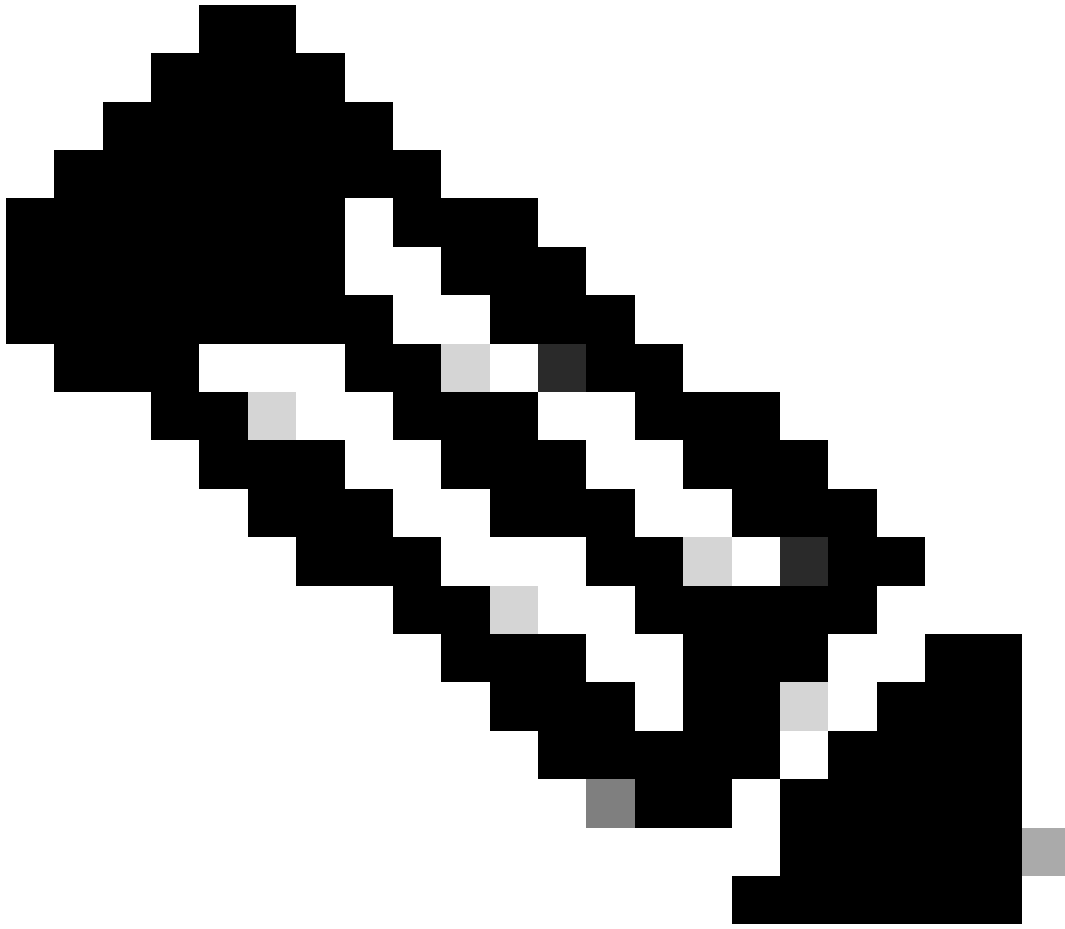
The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The main content area is titled 'Snort 3 All Rules' and shows a list of rule groups on the left. The 'All Snort 2 Converted Global' group is selected. The main panel displays the details for this group, including a description, search filters, and a table of rules. A red box highlights a success message: 'The custom rules were successfully imported'. Below this, a table lists the imported rules.

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

ءءرءس م ءلء صصمخ م ءءءءء ءلء ءلء ءءءءء

ءءءءء ءلء ءءءءء ريزءءء 4. ءءءءءلء

فءءءلء ءلء صصمخ م ءءءءء ءلء ءءءءء ءءءءء ءءءءء ءلء ءءءءء ءلء قوف رقنءا.



يه ةدع اقل تا ارج: ةظح الم

اذه يف ةيلالت المرحل ةفاكو ةيلال ال ةقباطم الم ةمزلال رطحو، ثدح ءاشن ا— رطح
لاصتالال.

وأ ةمزلال طاقس اب موقوي الو ةقباطم الم ةمزلال طقف اءا ءاشن اب موقوي— هـ يـ بنت
لاصتالال.

رايخ ال اءانتسا ةمزلال تاوتحم لءبتسيو ثدح ءاشن اب موقوي— ةباتكل ةءاع
ةءع اقل يف لاءبتسالال.

مـ يـ قـ تـ لـ نـ مـ ءـ يـ مـ ءـ اـ رـ جـ نـ وـ دـ رـ وـ رـ مـ لـ اـ بـ ةـ مـ زـ لـ لـ حـ مـ سـ يـ ، ثـ اـ ءـ اـ يـ ءـ اـ شـ نـ اـ مـ تـ يـ ال — Pass
ةـ يـ لـ a snort ءـ اـ وـ قـ يـ ءـ ءـ طـ سـ اـ وـ بـ .

ءـ كـ رـ حـ نـ مـ ءـ يـ مـ ال ءـ وـ ءـ قـ بـ اـ طـ مـ ال ءـ مـ زـ لـ لـ طـ قـ سـ يـ و ، ثـ دـ حـ ال ءـ اـ شـ نـ اـ بـ مـ وـ قـ يـ — drop
لاصتالال اذه يف رورم ال.

ةـ يـ فـ اـ ضـ الـ رـ وـ رـ مـ ال ءـ كـ رـ حـ نـ مـ و ، ءـ قـ بـ اـ طـ مـ ال ءـ مـ زـ لـ لـ طـ اـ قـ سـ اـ و ، ثـ دـ حـ ءـ a snort مـ وـ قـ يـ — ضـ فـ ر
رءصم ال يف يضم ال TCP لوكو تورب ناك اذا TCP نـ يـ عـ تـ ءـ اـ لـ لـ سـ رـ a لـ لـ صـ تـ الـ اذه يف

ةوجلواو.

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

م.اظنلل يضايرتفال اءارجإلا يلا عجرى—يضايرتفال

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

ةدروتسمللا ةصصخمللا ةيلحمللا تاريخشللا ةدعاق ديكأت 5. ةوطخللا

لباقملا Snort 3 رادصا قوف رقنا ،FMC يلع ماحتقالا تاسايس > تاسايسلا يلا لقتنا
فصللا يف فدهللا 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

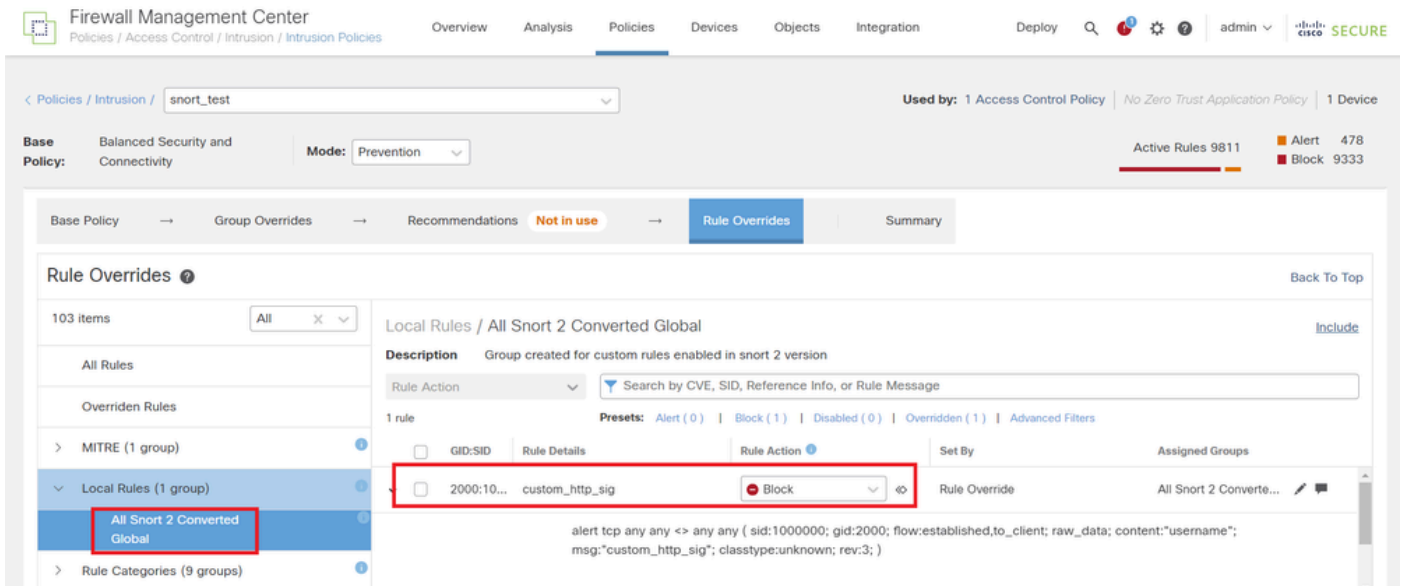
Hide Snort 3 Sync status Search by Intrusion Policy, Description, or Base Policy All IPS Rules IPS Mapping Compare Policies Create Policy

Intrusion Policy	Description	Base Policy	Usage Information
snort_test → 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

ةدروتسمللا ةصصخمللا ةدعاقلا ديكأت

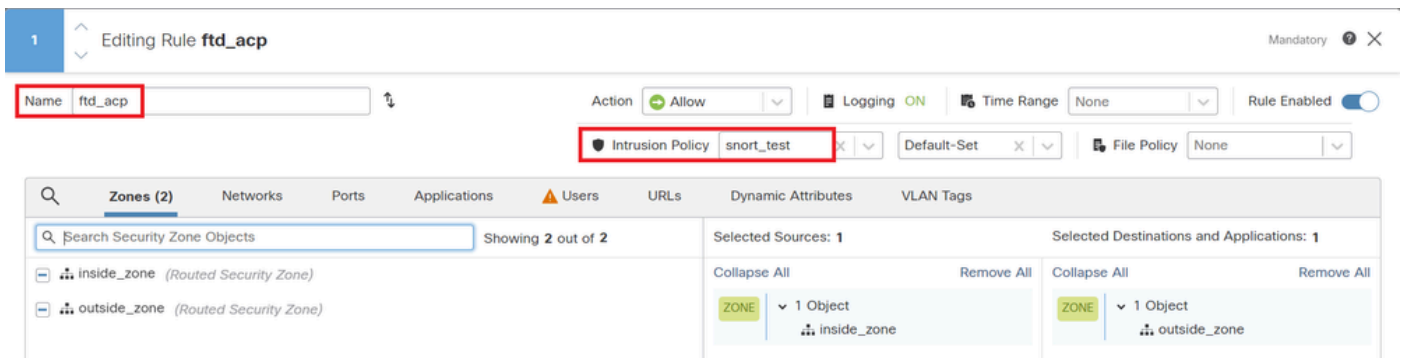
نم ققحتلل Snort 2 ل ةلوحمللا ةيمومعللا ةلوحمللا ةفاك > ةيلحمللا دعاقلا قوف رقنا
ةصصخمللا ةيلحمللا ةجنشللا ةدعاق ليصافت



دروت سمل ةصصخمل ةدءاق ل دي كأت

(ACP) لوصول ي ف مكحتل ةسايس ةءاقب للستل ةسايس طبر 6 ةوطخل

ACP عم مءحتق ال ةسايس طبرأ ، FMC لال خ نم لوصول ي ف مكحتل ةءحو >Policies ل لقتنا



ACP ةءاقب نارتق ال

تاريغتل رشن 7 ةوطخل

FTD لعل تاريغتل رشن



تاريغتل رشن

يلحم فلم ليمحت 2 ةقيرطال

Snort رادصا دي كأت 1 ةوطخل

1 ةقيرطال ي ف 1 ةوطخل س فن

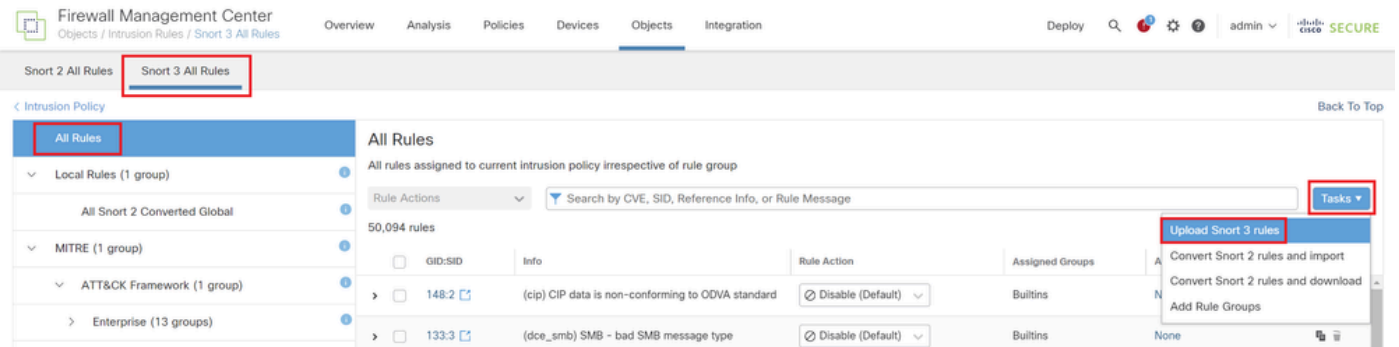
ةصصخم ةيلحم تايخش ةءاق ءاشن 2 ةوطخل

custom-rules.txt. ميسي يلحم فلم ي ف ايودي اهظفحو ةصصخم ةيلحم تانايب ةدعاق عاشناب مق

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

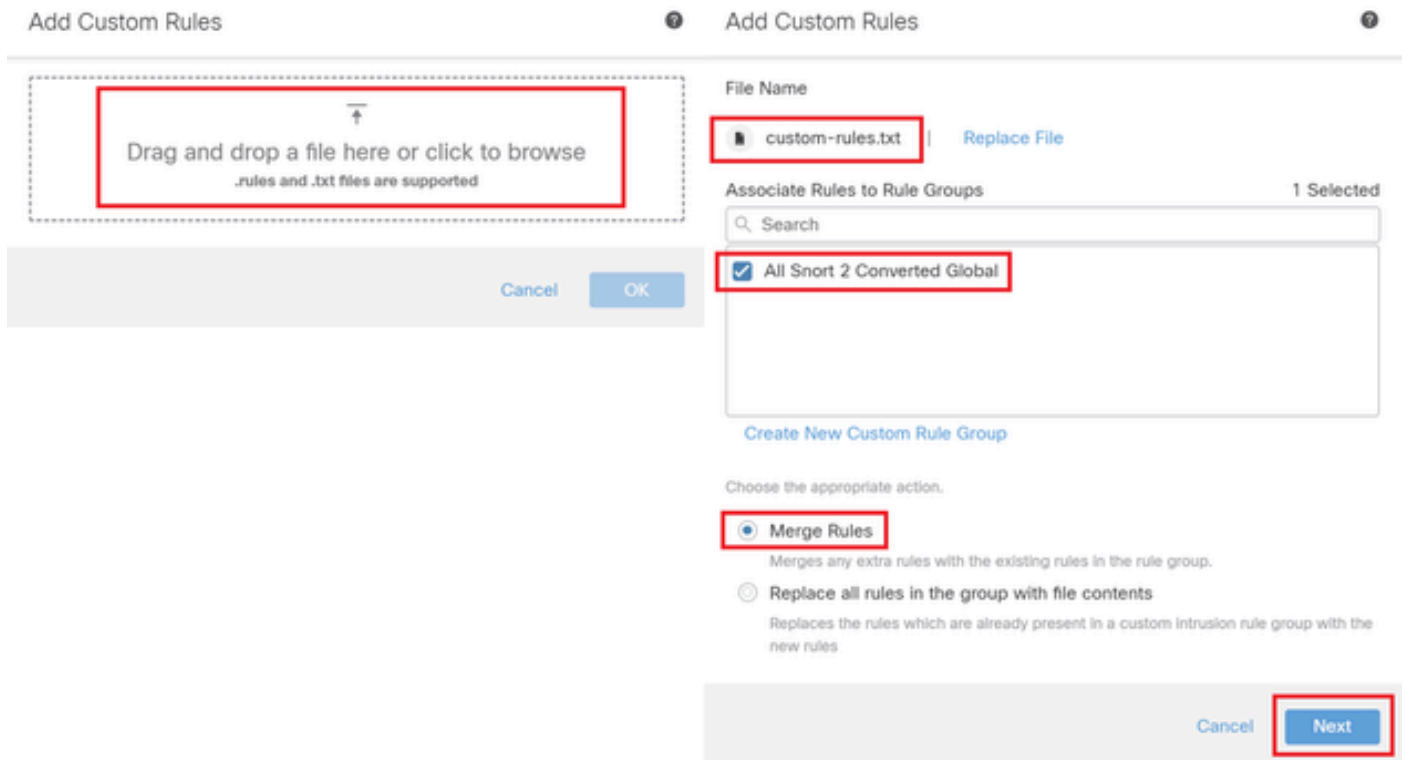
صصخملا يلحملا رخشلا ةدعاق ليحمحت 3. ةوطخل

رقنا FMC، يلع دعاوقلا عيجم > دعاوقلا ةفاك Snort 3 > محتقالا دعاوق > تانئاك يلى لقتنا
ماهمل حيرست ةمئاق نم Snort 3 دعاوق ليحمحت قوف



ةصصخملا ةدعاقلا ليحمحت

دح، يلحملا custom-rules.txt فلم تالف او بحسب مق، ةصصخم دعاوق ةفاضل ةشاش ي
يللاتل رزرقنا م، (لائملا اذه ي دعاوقلا جم د) بسانملا ءارجال او دعاوقلا تاعومجم



ةصصخم ةدعاق ةفاضل

تاريخي غتال رشن 7. ةوطخال

1. ةقيرطال ي ف 7 ةوطخال س فن

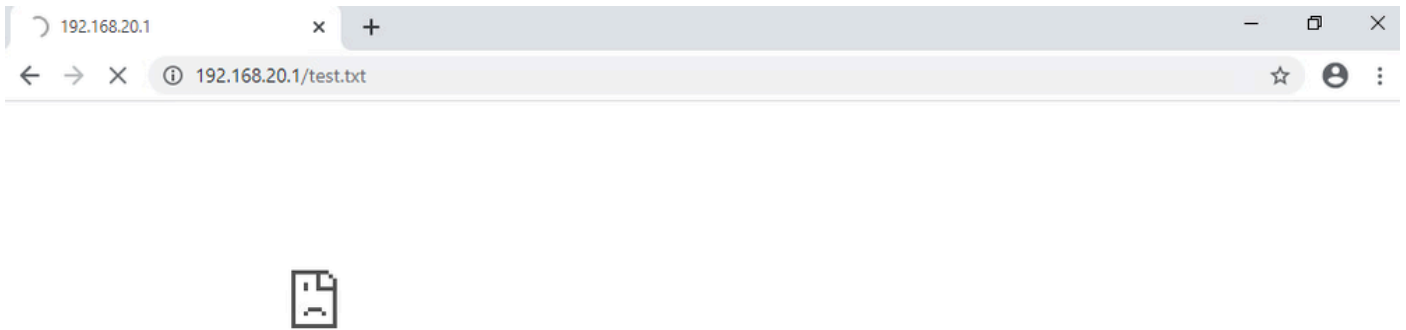
ةحصلا نم ققحتلا

HTTP م داخ ي ف فلملا تايوتحم طبض 1. ةوطخال

م دختسملا مسا يلع HTTP م داخ بناج يلع test.txt فلم تايوتحم طبضا

ي لوألا HTTP ب ل ط 2. ةوطخال

دكأتو (192.168.10.1) لي م عالا ضرعتسم نم HTTP (192.168.20.1/test.txt) م داخ يلع لوصولاب مق HTTP لاصتا رطح نم



ي لوألا HTTP ب ل ط

ل فطتلا شح ديكأت 3. ةوطخال

ةدعاق ةطساوب هؤاشنإ مت Intrusion شح نأ دكأ، Analysis>Intrusion>EventSon FMC يلع لقتنا ةصصخملا ةيحلحمل ةجنشلا

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	Generat
2024-04-06 14:30:48	low	Unknown	Block		192.168.20.1		192.168.10.1		80 (http) / tcp	50103 / tcp			custom_http_sig (2000:1000000:3)	Unknown Traffic	Standar

ماحتقا شح

ل فطتلا شح لي صافات ديكأت، 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_1003105a](#)

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

No Search Constraints (Edit Search)

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 ترحيل لي صافات

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 ب هب يصوملا

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

ثلاث لفصنلا يي ةدوجوم ةصصخم ةدعاق ريحت نكمملا نم له : س
 ةدعاقو ةلصللا تاذ ةدعاقول فذح بجي ، ةني عم ةصصخم ةدعاق ريحتل . هريحت كنكمي ال ، ال : أ
 اهئاشن

اهحالص او عا طخال فاشكتسا

ةطساوب HTTP رورم ةكرح رطح م تي ، لاثملا اذه يي FTD. لىع كولسلا ديكاتل 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 ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ان أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح 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 ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج 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 ئ س م Cisco
Systems (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا