# يف صصخم يلحم لقان دعاوق نيوكت Snort3 يلع FTD

# تايوتحملا

<u>قمدق مل</u>
<u>قيساسألاا تابلطتملا</u>
<u>تابلطتملاً</u>
<u>قمدختسمايا تانوكملا</u>
<u>قي،ساسأ تامول.عم</u>
<u>قكېشلىل يىطيىطختالا مسرل</u> ا
<u>ىنى وكەل،</u>
<u>نم داریټسا. 1. ققېرطل Snort 2 انم دارېټسا. 1. ققېرطل Snort 2 ا</u>
<u>Snort رادصا ديكأت .1 ةوطخلا</u>
<u>Snort 2 ي.ف ةصصخم قېلىجم رىخش قدعاق ري،رحت وأ ءاش،نا .2 ةوطخلا</u>
<u>3 قرونشالاا عالاً 2 تارونشالاً نام قصصخماناً قوالحملاً طانشالاً دعاوق دارياتساً 3. قوطخلاً </u>
<u>ةدعاقالا ا ءارچا رېېغت .4 ةوطخلا</u>
<u>قدروتسملاا قصصخملاا قېلحملا تارىخشلا قدعاق دېڭات .5 قوطخلا</u>
(ACP <u>) ل.وصولا يف مكحتانا ةسايس ةدعاقب ل.ل.س.تارا ةس.اي.س طبر .6 ةوطخلاا</u>
<u>تارىيغتا، ارش، ن. 7 قوطخا، ا</u>
<u>ېلىچم فارم ليېمچت .2 ققې،رطارا</u>
<u>Snort رادص ا دېكأت .1 ةوطخل ا</u>
<u>قصصخم قېلحم تايرخش قدعاق ءاشنا .2 قوطخلا</u>
<u>صصخما ا يالحما ا رخشاا قدعاق ليمحت .3 قوطخا ا</u>
<u>قدعاقالاا ءارجا ري.يغت .4 قوطخلاا</u>
<u>اەل.ېمحت مت يېتايا قص.صخمليا قېل.حمليا تياريخشلاا قدعاق ديكأت .5 قوطخليا</u>
(ACP <u>) ل.وص.ول.ا ي.ف مكـحتـل.ا ةس.اي.س ةدعاق.ب ل.ل.س.تـل.ا ةس.اي.س طـبر .6 ةوطخل.ا</u>
<u>تارىيغتا، ارش، .7 قوطخا، ا</u>
<u>قحصلا نم قرقحتلا</u>
<u>HTTP مِداخ يف فالمِلاا تايوتحم طبِض .1 ةوطخلاا</u>
<u>يالوألاا HTTP بالط .2 ةوطخلاا</u>
<u>ل.ف.ط.ت.ا ثدح ديكأت 3 ةوطخلا</u>
(FAQ) قلوادتملا قلء <u>،سأل</u>
<u>امحال صاو ءاطخأل ا فاش كتس ا</u>
عجرمل

# ةمدقملا

ىلع SNORT3 يف ةصصخملا ةيلحملا لاصتالا دعاوق نيوكت ءارجإ دنتسملا اذه فصي (FTD). قيامحلا رادج ديدهت دض عافدلا

```
ةيساسألا تابلطتملا
```

## تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- o Sisco نم (FireSIGHT (FMC) ةرادإ زكرم
- (FTD) ةيامحلا رادج ديدەت دض عافدلا

## ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- کرم VMWare 7.4.1 ل Cisco Firepower کرم
- Cisco Firepower 2120 7.4.1

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا عاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

# ةيساسأ تامولعم

جمانرب معد أدبي Snort 3 رادصإلاا يف ةرادإلاا زكرم عم تاديدهتلاا دض عافدلا يف 3 Snort جمانرب معد أدبي كرحم 3 Snort ربتعي ،ثدحألا تارادصإلاو 7.0 رادصإلا نم ةضوعملاو ةديدجلا ةزهجألل ةبسنلاب يضارتفالاا صحفلا

لانم ىلإ ةفاضإلاب ،3 Snort لرخشلا دعاوق صيصخت ةيفيكل الااثم دنتسملا اذه مدقي ققحتلاو ماحتقإ ةسايس نيوكت ةيفيك ميدقت متي ،صوصخلا هجو ىلعو .يلمع ققحت ةنيعم ةلسلس ىلع يوتحت يتلا HTTP مزح طاقسإل ةصصخم Snort ةدعاق مادختساب اهنم (مدختسملا مسا).



قاطن جراخ اهل معدلا ريفوتو ةصصخم ةيلحم لاصتا دعاوق ءاشنإ عقي :ريذحت كنم بلطتو ،طقف عجرمك دنتسملا اذه مادختسإ نكمي ،كلذل .TAC معد ةيطغت كتيلوؤسمو كريدقتل اقفو اهترادإو ةصصخملا دعاوقلا هذه ءاشنإ.

# ةكبشلل يطيطختلا مسرلا

ىلع Snort3 يف ةصصخملا ةيلحملا ةكوشلا ةدعاقل ققحتلاو نيوكتلا دنتسملا اذه مدقي ططخملا اذه.



ةكبشلل يطيطختلا مسرلا

# نيوكتلا

يتلا HTTP ةباجتسإ مزح فاشتكال ةصصخملا ةيلحملا نيوكتلا ةدعاق نيوكت وه اذه اهطاقسإو (مدختسملا مسا) ةددحم ةلسلس يلع يوتحت.



ةحفص نم ةصصخم ةيلحم تانايب دعاوق ةفاضإ نكمي ال ،نآلا ىتح :ةظحالم All Rules ققيرطلا مادختسإ بجي .FMC ل (GUI) ةيموسرلا مدختسملا ةهجاو يف All Rules دنتسملا اذه يف ةمدقملا.

Snort 3 ىلإ Snort 2 نم داريتسإ .1 ةقيرطلا

ريخشلا رادصإ ديكأت .1 ةوطخلا

ريخشلا رادصإ نأ نم دكأت .DeviceTab ةادأ قوف رقنا ،FMC ىلع ةزهجألا ةرادإ<ةزهجألا ىلإ لقتنا وه Snort3.

Firewall Management Center Overview	Analysis Policies Dev	ices Obje	ects Integration		Deploy Q 💕 🌣	admin v diaba	SECURE
View By: Group		F (0)				Migrate   Deployment H	listory
Collapse All	rmai (1) Ueployment Pen	aing (U)	opgrade (0) Short 3 (1)			Download Device L	List Report
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (1)							
FPR2120_FTI     Snort 3     1.100.0.29 -     Kones	Firepower 2120 with FTD	7.4.1	N/A	Essentials, IPS (1 more)	acp-rule	«ڳ	1

Snort رادصا

### 2 Snort يف ةصصخم ةيلحم ريخش ةدعاق ريرحت وأ ءاشنإ .2 ةوطخلا

ا فطتلا دعاوق < تانځاك ىلإ لقتنا Snort 2 All RuleOn FMC. > الفطتلا دعاوق < تانځاك ىلإ لقتنا لفطتلا دعاوق < تانځاك ىلإ لقتنا وأ ،ةصصخم ةيلحم تانايب ةدعاق ةفاضإل تانايب ةدعاق Snort 2 All Rules > المان ا دعاوقلا حملا دعاوقلا < FMC كام تاناي قدملا مال دعاوقلا = Snort 2 All Rules . قدوجوملا قصصخملا قيلحملا

ىجري ،Snort 2 يف ةصصخم ةيلحم تانايب دعاوق ءاشنا ةيفيك لوح تاميلعت ىلع لوصحلل <u>Snort 2 يف قصصخم قيلحم تانايب دعاوق نيوكت</u> ىل<u>ا</u> عوجرلا .

ةروصلا يف راهظإك ةديدج ةصصخم ةيلحم تايرخش ةدعاق ةفاضإ.

Firewall Management Center Objects / Intrusion Rules / Snort 2 All Rules	Overview Ar	nalysis Policies	Devices	Objects	Deploy Q 🤌 🌣 🖗 admin 🗸 號 SECURE
Snort 2 All Rules Snort 3 All Rules				Object Management	
< Intrusion Policy				Intrusion Rules	Search Delete Local Rules Import Rules Create Rule

ةديدج ةصصخم ةدعاق ةفاضإ

لاثملا اذه يف .ةروصلا يف حضوم وه امك ةدوجوم ةصصخم ةيلحم طبخش ةدعاق ريرحتب مق، ةدوجوم ةصصخم ةدعاق ررحي.

Sond 2 All Rules         Search         Search         Mentod Rules         Cented Rules         Mentod Rules         Cented Rules	Cipects / Intrusion Rul	ement Cer les / Snort 2 All	nter Overview Analysis Rules	Policies	Devices	Objects	Integration			Deploy	Q 📀	° 0	admin $\sim$	disco SECURE
Important         Catego (1990)         Catego	Snort 2 All Rules Snor	rt 3 All Rules												
Group Rules By         • endergon(19:95)           Q. Filter         • booser-detail(10)           • booser-detail(10)         • booser-detail(10)	< Intrusion Policy								Sea	rch Delete	Local Rule	s Im	port Rules	Create Rule
Catagory            Q. Filter         > browser-tenner (23)           > browser-tenner (23)         > browser-tenner (23)           > browser tenner (23)         > browser tenner (23)           > browser tenner (23)         > browser tenner (23)           > browser tenner (23)         > browser tenner (23)           > broberten (21) <t< td=""><td>Group Rules By</td><td></td><td>* Category (62656)</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	Group Rules By		* Category (62656)											
Q. Filter         > browst-fretu (20)           > browst-filt (20)         > browst-filt (20)           > browst-filt (20)	Category		▶ app-detect (162)											
Q. Fibr              • Browne-# (272)            > Browne-# (272)               • Browne-# (272)            • Browe-# (272)	Galogory		<ul> <li>browser-chrome (234)</li> </ul>											
browser-dw(r16)     browser-dw(r2)     browser-dw(r2)     browser-dw(r2)     browser-dw(r2)     browser-dw(r2)     bocoder (153)     content r-splice (2)     odested (2)     bocoder (153)     bocoder (154)     bocoder (154	Q, Filter		<ul> <li>browser-metox (307)</li> <li>browser-in (2022)</li> </ul>											
b browser-webkit (15) b browser-webkit (15) c browser-webkit (15) b rowser-webkit (15) c browser-webkit (15) b rowser-webkit (15) b rowser-webki			<ul> <li>browser-other (166)</li> </ul>											
<ul> <li>b coverse vesket(170)</li> <li>c content vesket(170)</li> <li>c decoder (150)</li> <li>b fore-stace (1200)</li> <li>c fore-stace (1300)</li> <li>c</li></ul>			browser-plugins (2552)											
content register (20)     content regi			<ul> <li>browser-webkit (170)</li> </ul>											
decoder (15)			▶ content-replace (26)											
detector(12005)     detector(12005)     detector(12005)     be-escatable (1207)     be-escatable (1207)     be-escatable (1207)     be-escate (1200)			<ul> <li>decoder (153)</li> </ul>											
			<ul> <li>deleted (12305)</li> </ul>											
<ul> <li>&gt; Net-endo(1201)</li> <li>&gt; Net-endo(1201)</li> <li>&gt; Net-indig(1012)</li> <li>&gt; Net-indig(1012)<!--</td--><td></td><td></td><td><ul> <li>exploit-kit (763)</li> </ul></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></li></ul>			<ul> <li>exploit-kit (763)</li> </ul>											
metamin(2)     metamin(2)     model			<ul> <li>file-executable (397)</li> </ul>											
<ul> <li>televation (1.15%)</li> <li>televation (1.15%</li></ul>			<ul> <li>File-Inden (2225)</li> <li>File-Indentify (1958)</li> </ul>											
Mnt-jose (230)     Mnt-indice (1231)     Mnt-indice (1232)     Mnt-indice (1232)     Mnt-indice (1232)     Mnt-indice (1232)     Mnt-indice (1232)     Mnt-indice (1232)     Mnt-indice (1237)     Mnt-indice (1237)     Mnt-indice (1237)     Mnt-indice (1247)			hie-image (1042)											
<ul> <li>No</li></ul>			► file-java (230)											
<ul> <li>Me-dife(1827)</li> <li>Me-set(1720)</li> <li>Me-set(1720)</li> <li>Micater oftwaren (1827)</li> <li>Micater oftwaren (1827)</li></ul>			► file-multimedia (530)											
Net-obser(2003)     Net-obser(2003)     Net-obser(2003)     Net-obser(2003)     Noticetter - comparative (1512)     Noticetter - comparative (1512)     Noticetter - tradecode (1514)     Noticetter - tradec			► file-office (1821)											
Mile-Bef (1720)     Indicator - other particular (172)     Indicator - other case (142)     Indicator - stane (142)     Indicator - stane (142)     Indicator - stane (142)     Indicator - stane (144)     Indicator - stane			▶ file-other (2003)											
indicator componentie (117)     indicator control (117)     (111000001)-custom_Intp_sig			▶ file-pdf (1730)											
indicator - Section (217)     i			<ul> <li>Indicator-compromise (612)</li> </ul>											
indicator science(12) indicator science(2) indicat			<ul> <li>indicator-obfuscation (247)</li> </ul>											
succurrented on (1%)     - Leas Rules (1)     (1:1000001)-custorm_http_sig			Indicator-scan (42)											
(1:100001) custom_http_sig			<ul> <li>Indicator-sheecode (354)</li> <li>Local Pades (1)</li> </ul>											
(1.100001) coston_mtp_sig			(1.1000001) susteen hits sin											
manware-backboor (1/1)			<ul> <li>nouser-backdoor (I71)</li> </ul>											× •

ةدوجوم ةصصخم ةدعاق ريرحت

مسا) ةددحم ةلسلس ىلع يوتحت يتلا HTTP مزح نع فشكلل عيقوتلا تامولعم لخدأ

مدختسملا).

- تەلاسر: custom\_http\_sig
- هيبنت :ءارجإلا
- TCP :لوكوتوربلا •
- ليمعلل تبثم :قفدتلا
- (ماخ تانايب) مدختسملا مسا :ىوتحملا

Firewall Management Center Objects / Intrusion Rules / Create	ew Analysis	Policies Devi	ces Objec	ts Integration				Deploy	Q 🔮 🌣	admin ~	cisco SECURE
										Search   Upload U	Jpdate   Intrusion
Snort 2 All Rules Snort 3 All Rules											
	Edit Pule 1:10	00000.3				(Rule Comm	nent)				
	Message c	ustom http sig									
	incosoge de	nation_ntp_arg			-						
	Classification Edit C	Nessifications			¥						
	Action al	ert	¥								
	Protocol to	p	•								
	Direction Bi	directional	•								
	Source IPs	NV NV		Source Port	anv						
	Destination IPs			Destination Port	any						
	Detection Opti	iy long		Description For	any						
	flow	ions					×				
	Established	*	To Client		•		<b>*</b> Ĵ				
	content		1				×				
	username						0				
			Case Insens	itive							
			Raw I	Not							
			HTTP	URI							
			HTTP Hea	ader 🗌							
			HTTP Co HTTP Raw	URI							
			HTTP Raw Hea	ader							
			HTTP Raw Co	okie							
			HTTP Met	hod							
		н	TTP Status Mess	age							
			HTTP Status C	ode							
			Dista	ince							
			W	ithin							
			01	ffset							
			De	epth							
		Use I	ast Pattern Mate	cher							
		Fast F	attern Matcher (	Only							
		Fast Pattern Match	er Offset and Ler	ngth							
	ack	<b>.</b>	Add Option			Save	ave As New				
			Can alread	1							

ةدعاقلل ةيرورضلا تامولعملا لاخدإ

3 ةرونشلا ىلإ 2 ترونشلا نم ةصصخملا ةيلحملا طنشلا دعاوق داريتسإ .3 ةوطخلا

لك) All Rules < (لفطتلا دعاوق) Snort 3 All Rules < لفطتلا دعاوق < تانئاك ىلإ لقتنا ماهملا حيرست ةمئاق نم داريتساو 2 Snort دعاوق ليوحت قوف رقناو ،FMC ىلع (دعاوقلا

Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	Overv	iew	Analysis	Policies	Devices	Objects	Integration			Deploy	Q	¢	¢ 0	admin $\vee$	dialia SECURE
Snort 2 All Rules Snort 3 All Rules															
< Intrusion Policy															Back To Top
All Rules		All	Rules												
<ul> <li>Local Rules (1 group)</li> </ul>	0	All ru	iles assigned to	o current intr	rusion policy irre	espective of rul	e group								
All Snort 2 Converted Global	0	Rule 50.0	e Actions 94 rules	~	Y Search by	CVE, SID, Ref	erence Info, or Rul	le Message					Unload	Snort 3 rules	Tasks 🔻
> MITRE (1 group)	0		GID:SID	Inf	fo			Rule Action	As	ligned Groups	5	4	Convert	Snort 2 rules	and import
> Rule Categories (9 groups)	0	,	148:2 🖸	(ci	ip) CIP data is nor	n-conforming to	ODVA standard	🖉 Disable (Default) 🗸	Bu	Itins		N	Convert Add Rul	Snort 2 rules e Groups	and download
		,	133:3 🗹	(d	ce_smb) SMB - b	bad SMB messa	ge type	🖉 Disable (Default) 🗸	Bui	Itins		N	me		¶a ≆

### قفاوم قوف رقناو ريذحتلا ةلاسر 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.



ريذحت ةلاسر

تالوحملا ةفاك قوف رقنا ،FMC ىلع Snort 3 All Rules < لفطتلا دعاوق < تانئاك ىلإ لقتنا اهداريتسإ مت يتلا صصخملا يلحملا رخشلا ةدعاق ديكأتل اهليوحت مت يتلا 2 ةماعلا.

Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	view Analysis Policies Devices Objects	Integration	Deploy Q 💕 🌣 🎯 admin 🗸	cisco SECURE
Snort 2 All Rules Snort 3 All Rules				
< Intrusion Policy				Back To Top
All Rules	Local Rules / All Snort 2 Converted Global			
<ul> <li>Local Rules (1 group)</li> </ul>	Description Group created for custom rules enabled in s	snort 2 version		
All Snort 2 Converted Global 🖍 🗑 🛛	Rule Actions V Y Search by CVE, SID, Re	eference Info, or Rule Message		Tasks 🔻
> MITRE (1 group)			T	
> Rule Categories (9 groups)		The custom rules were successfully imported X		
	GID:SID Info	Rule Action	Assigned Groups Alert Configuration	
	> 2000:1000000 custom_http_sig	🖉 Disable (Default) 🗸	All Snort 2 Converted Glo None	11

ةدروتسملا ةصصخملا ةدعاقلا ديكأت

ةدعاقلا ءارجإ رييغت .4 ةوطخلا

فدهلا ةصصخمانا ةدعاقلاب ةصاخلا ةدعاقلا ءارجإل اقفو لخدت لك جهن قوف رقنا.

þ	Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	Overvi	riew Analysis Policies	Devices Objects Ir	ntegration			Deploy Q 💰	° 0	admin 🗸	cisco SECURE
Sn	ort 2 All Rules Snort 3 All Rules										
< Int	usion Policy										Back To Top
	All Rules		Local Rules / All Snort 2 Co	onverted Global							
~	Local Rules (1 group)	0	Description Group created for	r custom rules enabled in snort	2 version						
	All Sport 2 Converted Global	120	Rule Actions 🗸 🗸	Y Search by CVE, SID, Refere	nce Info, or Rule	Message					Tasks 🔻
	All Short 2 Converted Global		1 rule								
>	MITRE (1 group)	0			The cust	om rules were successful	ly imported X				
>	Rule Categories (9 groups)	0					,				
			GID:SID Info			Rule Action		Assigned Groups	Alert Config	uration	
			>  2000:1000000 custo	om_http_sig		🖉 Disable (Default) 🗸	(Overridden)	All Snort 2 Converted Glo.	None		/1
						Block					
						Alert					
						P Drop					
						Pass					
						C Reject					
						Oisable (Default)					
						<ul> <li>Revert to default</li> </ul>					
						Per Intrusion Policy					

ةدعاقلا ءارجإ رييغت

ةدعاقلاو جەنلا ءارجإ تامولعم لخدأ ،ةدعاقلا ءارجإ ريرحت ةشاش يف.

- snort\_test :جەنUI
- رظح :ةدعاقلاً ءارجإ •



يه ةدعاقلا تاءارجإ :ةظحالم:

اذه يف ةيلاتا مزحلا ةفاكو ةيلاحلا ةقباطملا ةمزحلا رظحو ،ثدح ءاشنإ —رظح لاصتالا.

وأ ةمزحلا طاقسإب موقي الو ةقباطملا ةمزحلل طقف ثادحاً ءاشنإب موقي —هيبنت لاصتالا.

رايخ ىلإ ادانتسا ةمزحلا تايوتحم لدبتسيو ثدح ءاشنإب موقي —ةباتكلا ةداعإ ةدعاقلا يف لادبتسالا.

Pass— مييقتلا نم ديزم ءارجإ نود رورملاب ةمزحلل حمسي ،ثادحا يأ ءاشنإ متي ال دعاوق يأ قطساوب.

ةكرح نم ديزملا عنمي الو ةقباطملا ةمزحلا طقسيو ،ثدحلا ءاشنإب موقي —drop لاصتالا اذه يف رورملا.

ةيفاضإلا رورملا ةكرح عنمو ،ةقباطملا ةمزحلا طاقسإو ،ثدح ءاشنإب موقي —ضفر ردصملا يفيضمل TCP لوكوتورب ناك اذإ TCP نييعت ةداعإ لاسراو لاصتالا اذه يف

### .ةەجولاو

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

ماظنلل يضارتفالا ءارجإلا يلإ عجري—يضارتفالا.

r	
Edit Rule Action	0
2000:100 custom_http_sig	Ĩ
All Policies     Per Intrusion Policy	- 1
Policy Rule Action	- 1
snort_test 🗸 BLOCK v	
Add Another	- 1
Comments (optional)	
Provide a reason to change if applicable	].
Cancel Sav	e

ةدعاقلا ريرحت ءارجإ

### ةدروتسملا ةصصخملا ةيلحملا تاريخشلا ةدعاق ديكأت .5 ةوطخلا

لباقملا 3 Snort رادصإ قوف رقنا ،FMC ىلع ماحتقالاا تاسايس < تاسايسلا ىلإ لقتنا فصلا يف فدهلا ماحتقالاا جەنل.

[	Firewall Management Cer Policies / Access Control / Intrusion /	nter or Intrusion Policies	verview Ar	nalysis	Policies	Devices	Objects	Integration	Deploy	۹	¢	¢ (	admin	cisc	SECURE	
	Intrusion Policies Network Analysis Po	olicies														
	Hide Snort 3 Sync status 🏮 🔍 Search	h by Intrusion Policy, Descri	ption, or Base P	Policy				All IPS Rules	IPS Map	ping 🌘		Comp	are Policies	Crea	ate Policy	
	Intrusion Policy	Description		Base Poli	су		Usage I	nformation								
	snort_test → Snort 3 is in sync with Snort 2. 2024-01-12			Balanced	Security and	Connectivity	1 Acces No Zero 1 Device	s Control Policy Trust Application Policy		Snort	2 Ver	sion	Snort 3 Ve	rsion	1807	

ةدروتسملا ةصصخملا ةدعاقلا ديكأت

نم ققحتلل 2 Snort ل ةلوحملا ةيمومعلا تالوحملا ةفاك < ةيلحملا دعاوقلا قوف رقنا ةصصخملا ةيلحملا ةجنشلا ةدعاق ليصافت.

Firewall Management Center Policies / Access Control / Intrusion / Intrusion Policie	Overview Analysis	Policies Devices	Objects Integration	Deploy	Q 🔮 🌣 🝘 admin	<ul> <li>ababa SECURE</li> </ul>
<pre></pre>	revention v	v	Use	d by: 1 Access Control	Policy No Zero Trust Applicati Active Rules 9811	Alert 478 Block 9333
Base Policy $\rightarrow$ Group Overrides $\rightarrow$	Recommendations Not in us	se → Rule Ov	errides Summ	ary		
Rule Overrides						Back To Top
103 items All X V	Local Rules / All Snort 2 Co Description Group created fo	onverted Global r custom rules enabled in sr	nort 2 version			Include
All Rules	Rule Action 🗸	Y Search by CVE, SID, I	Reference Info, or Rule Messa	ge		
Overriden Rules	1 rule	Presets: Alert (0)   Blo	ock(1)   Disabled(0)   Ove	rridden (1)   Advanced F	ilters	
> MITRE (1 group)	GID:SID Rule Details	R	ule Action 0	Set By	Assigned Groups	
<ul> <li>Local Rules (1 group)</li> </ul>	• 2000:10 custom_http	p_sig	Block v 🗸	Rule Override	All Snort 2 Conver	te 🖊 🗭
All Snort 2 Converted Global	ale	ert tcp any any <> any any ( sg:"custom_http_sig"; class	sid:1000000; gid:2000; flow: type:unknown; rev:3; )	established,to_client; rav	v_data; content:"username";	
> Rule Categories (9 groups)						

ةدروتسملا ةصصخملا ةدعاقلا ديكأت

### (ACP) لوصولا يف مكحتلا ةسايس ةدعاقب للستلا ةسايس طبر .6 ةوطخلا

### .ACP عم ماحتقالاا ةسايس طبرأ ،FMC لالخ نم لوصولاا يف مكحتلاا ةدجو<Policiesىلإ لقتنا

■ Calify Selection Control Co	Mandatory 🛛 🗙
Name [ftd_acp	v 🗸 🖾 Logging ON 🛛 🖪 Time Range None 🔷 Rule Enabled 🇨
Intrusion Polici	$\begin{array}{c c c c c c c c c c c c c c c c c c c $
Q Zones (2) Networks Ports Applications 🔺 Users URLs	Dynamic Attributes VLAN Tags
Q Search Security Zone Objects Showing 2 out of 2	Selected Sources: 1 Selected Destinations and Applications: 1
At inside_zone (Routed Security Zone)	Collapse All Remove All Collapse All Remove All
dutside_zone (Routed Security Zone)	ZONE <ul> <li>1 Object</li> <li>20NE</li> <li>2</li></ul>

ACP ةدعاقب نارتقالا

### تارييغتلا رشن .7 ةوطخلا

### .FTD ىلع تارييغتلا رشن



تارييغتلا رشن

## يلحم فلم ليمحت .2 ةقيرطلا

Snort رادصإ ديكأت .1 ةوطخلا

.1 ةقيرطاا يف 1 ةوطخاا سفن

ةصصخم ةيلحم تايرخش ةدعاق ءاشنإ .2 ةوطخلا

دustom- ىمسي يلحم فلم يف ايودي اەظفحو ةصصخم ةيلحم تانايب ةدعاق ءاشنإب مق customrules.txt.

alert tcp any any <> any any ( sid:1000000; flow:established,to\_client; raw\_data; content:"username"; m

صصخملا يلحملا رخشلا ةدعاق ليمحت .3 ةوطخلا

رقنا ،FMC ىلع دعاوقلا عيمج < دعاوقلا ةفاك 3 Snort < ماحتقالا دعاوق < تانئاك ىلإ لقتنا ماەملا حيرست ةمئاق نم 3 Snort دعاوق ليمحت قوف.

Firewall Management Center Objects / Intrusion Rules / Snort 3 All Rules	Overv	iew	Analysis	Policies	Devices	Objects	Integration			Deploy	Q	e	¢ 0	admin $\checkmark$	cisco SECUI	RE
Snort 2 All Rules																
< Intrusion Policy															Back To	fop
All Rules		All Ru	ules													
<ul> <li>Local Rules (1 group)</li> </ul>	0	All rules	s assigned to	and to current intrusion policy irrespective of rule group												
All Snort 2 Converted Global	0	Rule A	ctions	~	Y Search by	CVE, SID, Re	ference Info, or Rul	e Message							Tasks 🔻	4
		50,054	Tures										Upload s	snort 3 rules		41
MITRE (1 group)			GID:SID	Info				Rule Action	Ass	igned Group	5	A	Convert	Snort 2 rules a	and import	
<ul> <li>ATT&amp;CK Framework (1 group)</li> </ul>	0	• 🗆	148:2 📫	(cip	) CIP data is nor	n-conforming t	to ODVA standard	O Disable (Default)	Buil	tins		N	Convert	Snort 2 rules a	and download	*
> Enterprise (13 groups)	0	<b>&gt;</b> []	133:3 🗹	(dc	e_smb) SMB - b	ad SMB mess	age type	Ø Disable (Default)	Buil	tins		No	00	, circupo	¶a ≆	

ةصصخملا ةدعاقلا ليمحت

ددح ،يلحملا custom-rules.txt فلم تالفإو بحسب مق ،ةصصخم دعاوق ةفاضإ ةشاش يف يلاتا رز رقنا مث ،(لاثملا اذه يف دعاوقلا جمد) بسانملا ءارجإلاو دعاوقلا تاعومجم.

Add Custom Rules	0	Add Custom Rules	9
		File Name	
Drag and drop a file here or click to browse		custom-rules.txt     Replace File	
.rules and .txt files are supported		Associate Rules to Rule Groups 1 Selecte	bd
Cancel	ОК	All Snort 2 Converted Global	
		Create New Custom Rule Group	
		Choose the appropriate action.	
		Merge Rules Merges any extra rules with the existing rules in the rule group.	
		Replace all rules in the group with file contents Replaces the rules which are already present in a custom intrusion rule group with the new rules	0
		Cancel Next	

# Add Custom Rules Summary 1 new rule 2000:1000000 Download the summary file. Back Finish

ليمحتلا ةجيتن ديكأت

عيمج قوف رقنا ،FMC ىلع دعاوقلا ةفاك 3 Snort < لفطتلا دعاوق < تانئاك ىلإ لقتنا اهليمحت مت يتلا صصخملا يلحملا رخشلا ةدعاق ديكأتل 2 ةلوحملا ةماعلا تالوحملا.

Coljects / Intrusion Rules / Snort 3 All Rules	view Analysis Policies	Devices Objects In	ntegration	Deploy Q 💕	admin 🗸	diada SECURE
Snort 2 All Rules Snort 3 All Rules						
< Intrusion Policy						Back To Top
All Rules	Local Rules / All Snort 2	Converted Global				
<ul> <li>Local Rules (1 group)</li> </ul>	Description Group created	d for custom rules enabled in snort	t 2 version			
All Snort 2 Converted Global	Rule Actions V	Y Search by CVE, SID, Refere	ence Info, or Rule Message			Tasks 🔻
V MITRE (1 group)	GID:SID	nfo	Rule Action	Assigned Groups	Alert Configuration	
<ul> <li>ATT&amp;CK Framework (1 group)</li> </ul>	✓ □ 2000:1000000 a	custom_http_sig	🖉 Disable (Default) 🗸	All Snort 2 Converted Glo.	None	11
> Enterprise (13 groups)		alert tcp any any <> any any ( sid	1:1000000; gid:2000; flow:established.to_client; raw_	_data; content:"username"; msj	g:"custom_http_sig";	
> Rule Categories (9 groups)	l	classtype:unknown; rev:3; )				

ةصصخملا ةدعاقلا ليصافت

ةدعاقلا ءارجإ رييغت .4 ةوطخلا

.1 ةقيرطلا يف 4 ةوطخلا سفن

اەليمحت مت يتلا ةصصخملا ةيلحملا تاريخشلا ةدعاق ديكأت .5 ةوطخلا

.1 ةقيرطلا يف 5 ةوطخلا سفن

(ACP) لوصولا يف مكحتلا ةسايس ةدعاقب للستلا ةسايس طبر .6 ةوطخلا

.1 ةقيرطلا يف 6 ةوطخلا سفن

تارييغتلا رشن .7 ةوطخلا

.1 ةقيرطالا يف 7 ةوطخاا سفن

# ةحصلا نم ققحتلا

HTTP مداخ يف فلملا تايوتحم طبض .1 ةوطخلا

.مدختسملا مسا ىلع HTTP مداخ بناج ىلع test.txt فلم تايوتحم طبضا

يلوألا HTTP بلط .2 ةوطخلا

دكأتو (192.168.10.1) ليمعلا ضرعتسم نم HTTP (192.168.20.1/test.txt) مداخ ىلإ لوصولاب مق لاصتا رظح نم HTTP.

) 192.168.20.1 ×	+	-	٥	×
$\leftrightarrow$ $\rightarrow$ X (1) 192.168.20.1/test.	txt	☆	Θ	:

Ľ

يلوألا HTTP بلط

لفطتلا ثدح ديكأت .3 ةوطخلا

ةدعاق ةطساوب ەؤاشنإ مت Intrusion ثدح نأ دكأ ،Analysis>Intrusion>EventSon FMCىلإ لقتنا ةصصخملا قيلحملا قجنشلا.

þ	Fir Ana	ewall Manageme lysis / Intrusions / Even	ent Cen ts	ter <sub>ov</sub>	erview	Analysis	Policies	Devices	Objects li	ntegration				Dep	bloy Q	0 0	admin	<ul> <li>dials sec</li> </ul>	URE
											Bookmark This	Page   Reportir	g   Dashbo	oard   View	Bookmarks	Search Pre	defined	Searches	¥
Even	nts	By Priority an	nd Clas	sification	(switch wor	kflow)									11.2	024-04-06 13	:26:03 - 1	2024-04-06 14:	31:12
No Sea	arch	Constraints (Edit Sear	ch)													021 01 00 10		Expa	nding
Drillde	lown	of Event, Priority, and	Classificat	ion Table \	/iew of Ev	ents Pac	kets												
Jump	to																		
		↓ Time X	Priority X	Impact X	Inline Result ×	Reason X	Source IP X	Source Country ×	Destination IP X	Destination x Country	Source Port / ICMP X Type	Destination Port / ICMP × Code	SSL Status X	VLAN x	Message X			Classification X	General
•		2024-04-06 14:30:48	low	O Unknown	Block		9192.168.20	.1	9 192.168.10.1		80 (http) / tcp	50103 / tcp			custom_http	_sig (2000:100	0000:3)	Unknown Traffic	Standar

ماحتقإ ثدح

.لفطتلا ثدح ليصافت ديكأت ،ClickPacketStab

Firewall Manage Analysis / Intrusions / B	nent Center Overview Analysis Policies Devices Objects Integration Deploy Q 📀 🌣 🚱 admin v 端 SECURE
	Bookmark This Page   Reporting   Dashboard   View Bookmarks   Search Predefined Searches V
Events By Priority	Ind Classification (united another) II 2024-04-06 13:26:03 - 2024-04-06 14:32:46 Exampling
No Search Constraints (Edit S	arch)
Drilldown of Event, Priority,	d Classification Table View of Events Packets
Event Information Message Time Classification Priority	custom_http_sig (2000-1000000-3) 2024-04-05 14:31:26 Unknown Traffic Iow
Ingress Security Zone	UNISING 2000
Egress Security Zone Device	Insue_come EP02120 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 Intrusion Policy	/rest.txt
Access Control Policy	NRGL (1994) Shon Life A
Access Control Rule	Ma ann
Rule	alert tep anv anv 🔿 anv anv ( sids1000000: gids2000: florsestablished.to_client: rar_data: content:"username": msg:"custom_http_gig": classtype:unknown: rev:3; )
<ul> <li>Actions</li> </ul>	

ماحتقالا ثدح ليصافت

# (FAQ) ةلوادتملا ةلئسألا

؟ 3 ترون وأ 2 ترون ، ەب ىصوملا وە ام : س رايخلا ەلعجي امم ،ةديدج تازيمو ةنسحم ةجلاعم تاعرس 3 Snort رفوي ،2 Snor عم ةنراقملاب :أ ربكأ لكشب ەب ىصوملا.

رادصإ نم ةيقرتلا دعب :س FTD رادصإل ال قرار عل 2.0 رادصإل البق FTD رادص ال م تي قرتلا دعب :س 2 رادص ال عل اي اي اي ال عن قرت snort رادص ال عي دحت مادختسال 2 تروش يف ل ازي ال شيتفتلا كرحم ، ال نسحتسمل انم منأو لبقتسمل اي ف 2 Snort رادص المما ططخمل انم منأ ظحال حيرص لكشب .نآل اممادختس انع فقوتل اقدشب

؟ ثلاثلا فصنلا يف ةدوجوم ةصصخم ةدعاق ريرحت نكمملا نم له : س ةداعإو ةلصلا تاذ ةدعاقلا فذح بجي ،ةنيعم ةصصخم ةدعاق ريرحتل .هريرحت كنكمي ال ،ال :أ اهئاشنإ.

# اهحالصإو ءاطخألا فاشكتسا

قطساوب HTTP رورم ةكرح رظح متي ،لاثملا اذه يف FTD ىلع كولسلا ديكأتل رمألاا system support trace **ليغشتب مق** قدعاق 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: blacklist 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: blacklist 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: blacklist 192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist

عجرملا

<u>Cisco Secure Firewall Management Center 3 جمانرب نېوكت لېلد</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما