عيقوتلا نيوكتو ماحتقالا ةسايس نيوكت يف ةرادإ) ةيطمنلا FirePOWER ةدحو يف (عبرملا

تايوتحملا

<u>ةمدقملا</u> <u>ةىساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>ةىساساً تامولعم</u> نىوكترا <u>للس تالاة سايس نىوكت .1 ةوطخاا</u> <u>ماحتقا ةسايس ءاشنا 1.1 ةوطخلا</u> <u>للستلامية ليدعت 1.2 ةوطخلا</u> <u>ي ساس ألا جەنلا لىدەت .1.3 ةوطخلا</u> <u>حش رملا طيرش رايخ مادختس اب عيق وتلا قيفصت 1.4 ةوطخلا</u> <u>قدعاقلا ةلاح نىوكت .1.5 ةوطخلا</u> ثادحألا ةىفصت لماع نىوكت .1.6 ةوطخلا <u>قىكىمانىدلا قلاحلا نىوكت .1.7 قوطخلا</u> <u>(ىراىتخا) تارىغتملا تاعومجمو (NAP) قكبشلا لىلحت جەن نىوكت .2 قوطخلا</u> <u>ةسايسب ةصاخلا تاريغتملا تاعومجم نيمضتل لوصولا يف مكحتلا نيوكت :3 ةوطخلا</u> <u>/ىنطولا لمعلا جمانرب /ماحتقالا</u> <u>رشن ا ي ل لوص ول اب مكحت ل قس اي س 4. قوط خل ا</u> لفطتلا ثادحاً ةبقارم .5 ةوطخلا <u>ةحصلا نم ققحتلا</u> <u>اهحالصاو ءاطخالا فاشكتسا</u> ةلص تاذ تامولعم

ەمدقملا

ةدحول (IDS) ماحتقالا فاشتكا ماظن/(IPS) للستلا عنم ماظن فئاظو دنتسملا اذه فصي ةدحو يف فاشتكا ةسايس لكشت يتلا ماحتقالا ةسايس رصانع فلتخمو FirePOWER FirePOWER.

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

* (ASDM) ةلدعملا نامألا ةزهجأ ةرادإ جمانربو (ASA) ةلدعملا نامألا ةزهجأ ةيامح رادج ةفرعم (ASDM).

* نامأ زاهج ةفرعم FirePOWER.

ةمدختسملا تانوكملا

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

ةيطمنلاا تادحولا ASA FirePOWER (ASA 5506X/5506H-X/5506W-X، ASA 5508-X، ASA 5516-X) جمانربلا نم ىلعأو 5.4.1 رادصإلا لغشت يتلا.

ا قدحول ASA FirePOWER (ASA 5515-X، ASA 5525-X، ASA 5545-X، ASA 5555-X) يتلا جمانربلا نم ىلعأو 6.0.0 رادصإلا لغشت.

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ 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

نم IPS/تافرعم ميمصت مت FirePOWER نم IPS/تافرعم ميمصت مت يف FirePOWER ةيطمنلا ةدحولا لمعت .ماظن/ةكبش موجه ىلإ ريشت ةراض (تاعيقوت وأ) قبقارملا عضو يف ددحم لكشب ASA ب ةصاخلا ةمدخلا ةسايس نيوكت مت اذإ IDS عضو .نمضملا عضولاا يف لمعت اهنإف ،كلذ فالخب (قطلتخملا)

ىلع مئاق فشك جەن وە FirePOWER زارط ةزەجألاا تافرعم/(IPS) للستلا عنم ماظن قباطتي امدنع ەيبنت ءاشناب IDS عضو يف ةيطمنلا FirePOWER قدحو موقت .عيقوتلا IPS عضو يف ةيطمنلا FirePOWER قدحو موقت امنيب ،ةراضلا رورملا ةكرح عم عيقوتلا .ةراضلا رورملا ةكرح عنمو يات ءاشنإب

، مىرىخرىتىلا نم قىقىحتىلى. تفىيطولدا مذە نىيوكىتىل **Protect** مىرىخرىت ىىلىع يودىتىت نا بىچى تىيىطەنىلا FirePOWER قدىر نىأ نىم دكىاكت :**تىلىچالىم** مىرىن خرىتىلا < ASA FirePOWER Configuration < ئىيوكىتىلا، كەرىتىكە ھىھە تەتەرەپ ھەتھە ھىھە دىيەۋكىتىكا، يىلىقىتىن

نيوكتلا

للستلا ةسايس نيوكت .1 ةوطخلا

ماحتقإ ةسايس ءاشنإ .1.1 ةوطخلا

فيكتلل لباقلا نامألا ةزهجأ ريدم ىلإ لوخدلا ليجستب مق ،ماحتقالا ةسايس نيوكتل (ASDM) تقيلات العاط المكاو (ASDM):

ةسايس < تاسايسلا > ASA FirePOWER Configuration > نيوكتلا ىلإ لقتنا 1. ةوطخلا ماحتقالا ةسايس < ماحتقالا.

.**جەن ءاشنإ** قوف رقنا .2 ةوطخلا

للستلا جەن **مسا** لخدأ .3 ةوطخلا.

(يرايتخإ) للستلا جەن **فصو** لخدأ .4 ةوطخلا.

ا**نمضم نوكي امدنع طاقسإ** رايخ ددح .5 ةوطخلا.

ةلدسنملا ةمئاقلا نم **يساسألا جەنلا** ددح .6 ةوطخلا.

ماحتقالا جەن ءاشنإ لامكإل **جەن ءاشنإ** قوف رقنا .7 ةوطخلا.

File View Tools Wizards Window Help		Type topic to search	io
😽 Home 🦓 Configuration 🔯 Monitoring 🔲 Save ASA Changes	s 🔇 Refresh 🔇 Back 🔘 Forward 💡 Hel	p	CISCO
ASA FirePOWER Configuration 🛛 🗗 🚺 Configuration	n > ASA FirePOWER Configuration > Policies	> Intrusion Policy > Intrusion Policy	
Policies Access Control Policy Sule Editor Files SL Actions Alerts	o policies defined. Click Create Policy to create a polic	Compare Polic 2	Create Policy
Identity Policy DNS Policy Dovice Management Object Management	Policy Information Name * 3 IPS_Policy	7	
System Information Judates Licenses Tools Marcal Information Judates Judates Judates Judates Judates Judates	Description 4 IPS_policy fo Drop when Inline 5 Base Policy 6 Balanced Sec	r LAB	
<u>معمد المعمد المعم المعمد المعمد المعمم المعمم المعمد المعمد المعمد المعمد المعمد المعمم لمعمد المعمد المعمم محمد المعمم المعمد المعمم المعمم المعمد المعمد مدمد المعمد المعممد المعمم محمد المعمد المعمد المعمم محمد المعمد المعمد المعمد </u>	* Required	Create Policy Create and Edit Policy Cancel	
Remote Access VPN			
Site-to-Site VPN			
ASA FirePOWER Configuration			
Device Management			
»			fer.
	<admin> 15</admin>	💽 🌌 🛛 🚹 1/	4/16 1:17:37 AM UTC

زاهج يأ ىلع ەقيبطت متي ال ،كلذ عمو ،جەنلا نيوكت ةظحالم كنكمي.

onfiguration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy □											
			Compare Policies	S Create Policy							
Intrusion Policy	Drop when Inline	Status	Last Modified								
IPS_Policy IPS_policy for LAB	Yes	<u>No access control policies use this policy</u> Policy not applied on device	2016-01-04 07:40:00 Modified by "admin"	🖪 🕞 🥔 🙃							

للستلا جەن ليدعت .1.2 ةوطخلا

ليدعتل ،ماحتقالا ةسايس ليدعتل ASA FirePOWER Configuration < نيوكتلا ماحتقال الماحتقال الماحتي ريرحتلا رايخ ددجو ماحتقالا قسايس < ماحتقالا قسايس < تاسايسلا.



يساسألا جەنلا ليدعت .1.3 ةوطخلا

رايخ دنع ةيساسألا طاقسإلا /ةسايسلا رييغت رايخ ماحتقالا ةسايس ةرادإ ةحفص حنمت لهاجتلاو نيمضتل/ظفحلا.

تاسايس دعت يتلاو ،ماظنلا اهرفوي يتلا تاسايسلا ضعب ىلع يساسألا جەنلا يوتحي ةجمدم.

- جەنلا اذە يوتحي .لاصتالاو نامألا ثيح نم ةيلاثم ةسايس اەنإ :لاصتالاو نامألا نزاوت .1 ضعبلا موقي امنيب طقف ثادحألا ءاشنإب موقي اەضعب ،ةنكمم ةدعاق 7500 يلاوح ىلع رورملا ةكرح طاقسإ ىلإ ةفاضإلاب ثادحألا ءاشنإب رخآلا
- جەن ىلع نيمأتلا رايتخإ كنكميف نيمأتلا كليضفت ناك اذإ:لاصتالا ربع نيمأتلا .2 ةنكمملا دعاوقلا ددع نم ديزي امم ،لاصتالا.
- رايتخإ كنكميف ،نامألاا نم الدب لاصتالا وه كليضفت ناك اذإ :نامألاا ىلع لاصتالاا 3. اهنيكمت مت يتلا دعاوقلاً ددع ليلقت ىلإ يدؤيس يذلا نامألاا جهن نم الدب لاصتالاً.
- .ىصقألا فشكلا ىلع لوصحلل جەنلا اذە ددح ىصقألا فشكلا .4
- دعاوقلا نيكمت بجي .دعاوقلا عيمج ليطعتب رايخلا اذه موقي ةطشن ةدعاق دجوت ال .5 كب صاخلا نامألا جەن يلإ ادانتسا ايودي.

Policy Information	Policy Informa	tion	< Back				
Rules ⊕ Advanced Settings	Name	IPS_Policy					
⊕ Policy Layers	Drop when Inline Base Policy Balanced Se	Manage Base Policy rt)					
	Image: This policy has 7591 enabled rules						
	This policy contain the preprocessors	s enabled preprocessor rules. Please read the rule have the correct settings for these rules Commit Changes Discard Changes	e documentation to ensure				

حشرملا طيرش رايخ مادختساب عيقوتلا ةيفصت .1.4 ةوطخلا

نم فالآلا كانه .دعاوقلا ةرادإ ةحفص رهظتو حفصتلا ةحول يف **دعاوقلا** رايخ ىلإ لقتنا يف ثحبلل ديج ثحب كرحم رايخ ةيفصتلا طيرش رفوي .ةدعاقلا تانايب ةدعاق يف ةدعاقلا لاعف لكشب ةدعاقلا.

اذإ .كب ةصاخلا جئاتنلا ماظنلا فطخيو ةيفصتلا طيرش يف ةيساسأ ةملك يأ جاردإ كنكمي فيزن ةيلباق (SSL) ةنمآلا ليصوتلا ذخآم ةقبط عيقوت نع ثحبلل بلطتم كانه ناك بلجيسو ةيفصتلا طيرش يف ةيساسألا ةملكلا بلق فيزن يف ثحبلا كنكمي ،بلقلا اهب بلقلا فيزن مت يتلا فعضلا طاقنل عيقوتلا

ماظنلا موقي ،حشرملا طيرش يف ةددعتم ةيساساً تاملك مادختساٍ مت اذإ :**حيملت** بكرم ثحب ءاشنإل قطنمو مادختساب مەجمدب.

لال الما الما الحرم (GID) حيق وتال فرعم مادختساب دعاوقال يف ثحبال الال (GID) الدومال فرعمو (SID) عيقوتال فرعم م كالذ ي إ امو DoS :قى الو

/ةئفلاا ىلإ دانتسالا لثم ةددعتم قرط ىلإ لاعف لكشب دعاوقلا ميسقت متي دعاسيو .ددحم يساسأ ماظن /تافينصتلا دعاسي امك ،ةلەس ةقيرطب حيحصلا عيقوتلا ىلع لوصحلا ىلع ليمعلا اذه دعاوقلا نارتقا لاعف لكشب تاعيقوتلا طبض ىلع ليمعلا

Policy Information	Rules		< Back
Rules	Rule Configuration	Filter: heartbleed	× ?
⊕ Advanced Settings	Rule Content	Filter returned 33 results	
Policy Lavers	Category		Policy
Toney Edyers	app-detect	Rule State Event Filtering Dynamic State Alerting Comments	Policy
	blacklist	📃 GID SID Message 🔺	🔿 🔻 🕑 🕕 🖓
	browser-chrome browser-firefox	I 30549 SERVER-OTHER OpenSSL Heartbleed masscan access exploitation attempt	× ^
	browser-ie	SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×
	browser-plugins	SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×
	browser-webkit content-replace	SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×
	decoder exploit-kit	SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×
	file-executable	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×
	file-flash Classifications	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×
	Microsoft Vulnerabilities	SERVER-OTHER OpenSSL TLSv1 large heartbeat response	×
	Microsoft Worms	- possible ssl heartbleed attempt	
	Platform Specific	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×
	Preprocessors	SERVER-OTHER OpenSSL TLSv1.1 large heartbeat	-
	Priority		
	Rule Update	K	

كنكمي .اهيطغت يتلا دعاوقلا ىلع روثعلل CVE مقر مادختساب ثحبلا اضيأ كنكمي. [مادختس] وكلي: CVE: <cve-number>.



ةدعاقلا ةلاح نيوكت .1.5 ةوطخلا

رتخاو دعاوقلا ددح .ةدعاقلا ةرادإ ةحفصو حفصتلا ةحول يف رايخلا رمظي **دعاوقلا** ىلإ لقتنا ةدعاقل اەنيوكت نكمي تالاح ثالث كانە .دعاوقلا ةلاح نيوكتل رايخلا **ةدعاق قلاح**:

رورملا ةكرح ةدعاقلا قباطت امدنع ثادحاً ءاشنإب رايخلا اذه موقي **:ثادحألا ءاشناِ** 1.

2. ةكرح ةدعاقلا قباطت امدنع رورم ةكرح طاقسإو ثادحأ رايخلا اذه جتني **:ثادحألا ديلوتو طاقسإ** رورملا

.ةدعاقلا رايخلا اذه لطعي **:ليطعت** .3

Policy Information	Rules		< Bac	ck
Rules	Rule Configuration	Filter:	×	?
Advanced Settings	Rule Content	Filter returned 33 results		
⊕ Policy Layers	Category app-detect	Rule State Event Filtering Dynamic State Alerting Comments	Policy	•
	blacklist	C Generate Events age 🔺	⇒ 🔻 🕑 🕕 🖓	
	browser-firefox	Drop and Generate Events ER-OTHER OpenSSL Heartbleed masscan access	×	*
	browser-ie	Disable ER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×	
	browser-plugins browser-webkit content-replace decoder evoloit-kit	1 30778 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×	
		1 30785 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×	
		1 30514 SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×	
	file-executable	1 30779 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×	
	file-flash T Classifications	1 30780 SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×	
	Microsoft Vulnerabilities	SERVER-OTHER OpenSSL TLSv1 large heartbeat response	×	
	Microsoft Worms Platform Specific Preprocessors	SERVER-OTHER OpenSSL TLSv1 large heartbeat response possible sel heartbleed attempt	×	
		SERVER-OTHER OpenSSL TLSv1.1 large heartbeat		-
	Priority	1 30781	X	_
	Rule Update	K	(1 of 1))	

ثادحألا ةيفصت لماع نيوكت .1.6 ةوطخلا

.ةەجولاا وأ ردصملل IP ناونع ىلإ وأ ،راركتلا راركت ىلإ ماحتقالاا ثدح ةيمەأ دنتست نأ نكمي نوكت ال دق ،لاثملا ليبس ىلع .تارم ةدع عقي نأ ىلإ ثدحلاب يلابت ال دق ،تالاحلا ضعب يف يفو .تارملا نم نيعم ددع يف لشفي ىتح مداخ ىلإ لوخدلا ليجست ام صخش لواح اذا اقلق ةلكشم دوجو نم دكأتلل دعاوقلا قيبطت تالاح ضعب ةيؤر ىلإ طقف جاتحت دق ،ىرخأ تالاح دراشتنالا قعساو

اذه قيقحت اهلالخ نم كنكمي ناتقيرط كانه

. ثدحلا ةبتع.

.ثدحلا عمق .2

ثدحلا ةبتع

كنكمي .تاراركتلا ددع ىلع ءانب ،ثدحلا ضرع تارم ددع يلمت يتلا دودحلا نييعت كنكمي جەن لكلو ثدح لكل دح نيوكت.

:ثدحلا دح نيوكت تاوطخ

اهل ثدحلا دح نيوكت ديرت يتلا **(دعاوقلا) ةدعاقلا** ددح 1. ةوطخلا.

ثدحلا ةيفصت قوف رقنا .2 ةوطخلا.

- ل**صافلا دحلا** قوف رقنا .3 ةوطخلا.
- امەالك وأ دحلا وأ دحلا) .ةلدسنملا ةمئاقلا نم **عونلا** ددح .4 ةوطخلا.

ةەجولا وأ ردصملا) . **Track By** drop عبرملا نم عبتتلا ديرت فيك ددح .5 ةوطخلا.

ةبتعلاب ءافولل ثادحألا **ددع** لخدأ .6 ةوطخلا.

ددعلا نييعت ةداعإ لبق اهؤاضقنا متيس يتلا **يناوثلا** لخداً .7 ةوطخلا.

لمكتسي نأ **ok** ةقطقط .8 ةوطخلا.

1	GID	SIC	Threshold	d 3				\Rightarrow	9	0	0	9
3	1	280	Suppress	ion	T 360.cn Safe(ess attempt	Guard local HTTP m	anagement	×				-
0	1	280	Remove T	Thresholds	360.cn Safegua	rd runtime outbound	communication	\Rightarrow				
	1	328	Remove S	Suppressions 209.53.113	Absolute Softwa 223	are Computrace outbo	und connection -	\Rightarrow				
0	1	328	46	APP-DETECT absolute.com	[•] Absolute Softwa n	re Computrace outbo	und connection -	⇒				
0	1	328	47	APP-DETECT bh.nameque	Absolute Softwa ry.com	Set Threshold	for 1 rule		?	×		
0	1	328	48	APP-DETECT namequery.	[•] Absolute Softwa nettrace.co.za	4 Type	Limit					
3	1	262	86	APP-DETECT search.dnss	Absolute Softwa earch.org	6 Count	10					
0	1	262	.87	APP-DETECT search.name	Absolute Softwa equery.com	Seconds	60					

لماع ةنوقيأ ةيؤر ىلع ارداق نوكت نأ بجي ،ةدعاق ىلإ ثادحألا ةيفصت لماع ةفاضإ دعب ةدعاقلا هذهل ةنكمم ثادحألا ةيفصت نأ رهظت يتلا ،ةدعاقلا ةراشإ راوجب ةيفصت.

ثدحلا عمق

ةدعاق لكل وأ ةهجولا /ردصملل IP ناونع ساسأ ىلع ةددحملا ثادحألا تاراطخإ عنم نكمي.

ئشني ال ماظنلاا نكل داتعملاك عيقوتلا صحف لمعي .ةدعاقل ثدح عمق ةفاضإ دنع **:ةظحالم** رهظت نلف ،ةنيعم ةهجو/ردصم ديدحتب تمق اذإ .عيقوتلا قباطت رورملا ةكرح تناك اذإ ثادحألا موقي نلف ،ةلماكلا ةدعاقلا عنم ترتخأ اذإ .ةدعاقلا هذهل طقف ةددحملا ةهجولا/ردصملل ثادحألا .ةدعاقلا هذهل شدح يأ ءاشنإب ماظنلا

```
:ثدحلا دح نيوكت تاوطخ
```

اەل ثدحلا دح نيوكت ديرت يتلا **(دعاوقلا) ةدعاقلا** ددح .1 ةوطخلا.

.**ثادحألا ةيفصت** قوف رقنا .2 ةوطخلا

.عمق رقنا .3 ةوطخلا

ةەجولا وأ ردصملا وأ ةدعاقلا) .ةلدسنملا ةمئاقلا نم **عمقلا عون** ددح.4 ةوطخلا.

لمكتسي نأ **ok** ةقطقط .5 ةوطخلا.

⇒ ▼ 2 ▼ ▼ Rule State Event Filtering Dy	▼	Policy	•
GID SID Threshold		⇒	7 🕑 🕕 🖓
1 3 Suppression	T 360.cn SafeGuard local HTTP management ess attempt	^t 🗙	A
Remove Threshold 1 28 Remove Suppressi	360.cn Safeguard runtime outbound ns ^{on}		
1 32845 APP-DET	ECT Absolute Software Computrace outbound on - 209.53.113.223	\Rightarrow	
1 32846 APP-DET connect	ECT Absolute Software Computrace outbound on - absolute.com		▼
Add Suppression for 1 Suppression Type Type Type Suppression Suppression Type Suppression Suppression Type Suppression Type Suppression Type Suppression Type Suppression Suppression Type Suppression Type Suppression Type Suppression Type Suppression Suppression Type Suppression Type Suppression Type Suppression Suppression Type Suppression Type Suppression Type Suppression Type Type Type Suppression Type T	Image: Software uery.cor Add Suppression for 1 Software y.nettra Suppression Type Software ssearch. Network Cancel Software ssearch. Software on - search.namequery 6 CT Absolute Software on - search.us.namequery Add Suppression outbound Add Suppression Type 6 Suppression Software on - search.us.namequery 5 Suppression Software on - search.us.namequery 6 Suppression Type 4 Suppression Software on - search.us.namequery 6 Suppression Type 6 Suppression Type 6 Suppression Type 6 Suppression Type 6	1 rule	? × Cancel

لماع ةنوقيأ ةيؤر ىلع ارداق نوكت نأ بجي ،ةدعاقلا هذه ىلإ ثادحألا ةيفصت لماع ةفاضإ دعب ةنكمم ثادحاً ةيفصت لماوع كانه نأ رهظت يتلا ،ةدعاقلا ةراشإ راوجب "2" دعلا عم ةيفصت ةدعاقلا هذهل.

ةيكيمانيدلا ةلاحلا نيوكت .1.7 ةوطخلا

ددحملا طرشلا تقباطت اذإ ةدعاق ةلاح رييغت اهيف اننكمي ةزيم يه.

ةلواحم نع عيقوتلا فشك اذإ .رورملا ةملك ميطحتل ةوقلاب فينع موجهل ويرانيس ليخت هيبنتلا ءاشنا يف ماظنلا رمتسي .ثدح ءاشنا وه ةدعاقلا ءارجا ناكو رورملا ةملك لشف ثيح **ةيكيمانيدلا ةلاحلا** مادختسا كنكمي ،ةلاحلا هذهل .رورملا ةملك لشف قلواحمب صاخلا .ةمشاغلا ةوقلا موجه رظحل **امتاشناو ثادحاً طاقسا** ىلا **ثادحاً ءاشنا** ءارجا رييغت نكمي

يتلا ةدعاقلا ددح .ةدعاقلا ةرادا ةحفصو حفصتلا ةحول يف رايخلا رهظي **دعاوقلا** ىلإ لقتنا **ةدعاق ةلاح ةفاضاٍ < ةيكيمانيدلا ةلاحل**ا تارايخ رتخاو اهل ةيكيمانيدلا ةلاحلا نيكمت ديرت **ساساً لدعم**.

لدعملا ىلإ ةدنتسملا ةدعاقلا ةلاح نيوكتل:

- اەل ثدحلا دح نيوكت ديرت يتلا **(دعاوقلا) ةدعاقلا** ددح .1.
- 2. **قيكيمانيدلا ةلاحلا** ىلع رقنا.

- . **لدعملا ىل ةدنتسملا ةفاضا ةدعاق ةلاح** قوف رقنا .3
- ةلوصفم ةمئاق وأ ريغتم وأ ناونع ةلتك وأ دحاو IP ناونع ديدحت كنكمي .**ةكبشلا** لخدأ .5 هذه نم بيكرت يأ نم نوكتت يتلاو ةلصافب.
- .يناوثلاب تقولا عباطو ثادحألا **ددع** لخدأ .6
- . ةدعاقلل اەفيرعت ديرت **،ةديدجلا ةلاحل**ا ددح.
- ةدعاقلا ةلاح عاجرا اهدعب متي يتلا <mark>قلەملا</mark> لخدا .8.
- <u>لمكتسي نأ ok ةقطقط .9.</u>

Policy Information	Rules	< Ba
Rules	Rule Configuration	Filter: X
⊕ Advanced Settings	Rule Content	1 selected rule of 33
@ Policy Lowers	Category	
Policy Layers	app-detect	Rule State Event Filtering Dynamic State Alerting Comments
	blacklist	🔲 GID SID M 🗿 Add Rate-Based Rule State 🛛 🔿 🐨 🕑 🔍 🖓
	browser-chrome	SER Remove Rate-Based Rule States ed masscan access
	browser-firefox	explanation and based have stated
	browser-ie	SERVER-OTHER OpenSSL SSLv3 large heartbeat response
	browser-other	Add Rate-Based Rule State for 1 rule
	browser-plugins	1 30778
	browser-webkit	Track By Destination V
	content-replace	1 30785 5 Network 192.168.20.3
	decoder	Rate 10 Count / 5 Seconds
	exploit-kit	New State Drop and Generate Events
	file-executable	1 30779 8 Timeout 30
	file-flash 🔻	
	Classifications	
	Microsoft Vulnerabilities	SERVER-OTHER OpenSSL TLSv1 large heartbeat response
	Microsoft Worms	- possible ssl heartbleed attempt
	Platform Specific	SERVER-OTHER OpenSSL TLSv1 large heartbeat response
	Preprocessors	SERVER-OTHER OpenSSL TLSv1.1 large heartbeat
	Priority	
	Rule Update	K < 1 of 1 > X

(يرايتخإ) تاريغتملا تاعومجمو (NAP) ةكبشلا ليلحت جەن نيوكت .2 ةوطخلا

ةكبشلا ليلحت جەن نيوكت

ةداعإب قبسملاا جلاعملاا موقي .ةقبسملاا تاجلاعملاب اضيأ ةكبشلاا ىلإ لوصولاا جەن فرعي ةقبط لوكوتوربل ذوذشلا ىلع فرعتلا ىلع دعاسي ەنإ .رورملا ةكرح عيبطتو ةمزحلا عيمجت ةمئالملا ريغ سأرلا تارايخ فيرعت يف لقنلا ةقبطو ةكبشلا.

قفدلا عيمجت ةداعإو TCP ةلاح صحف رفوتو ،IP تانايب تاططخم ةئزجت ءاغلإب NAP موقت ،رورملا ةكرح عيبطتب قبسملا جلاعملا موقي .ةيعجرملا غلابملا ةحص نم ققحتلاو ،ەنم ققحتلاو لوكوتوربلا سايقم ةحص نم ققحتلاو

ةطساوب ەليغشت مت يذلا يلوألا جلاعملا لثمي وەو .ەب صاخ GID مقر يلوأ جلاعم لكل ةمزحلا.

ەب ىصوملا لىثمألاا جەنلاا وەو لاصتالاو نزاوتملا نامألا وە يضارتڧالا قكبشلا ليلحت جەن. نم اەديدحت نكمي يتلاو NAP تاسايس لالخ نم اەريڧوت مت ىرخأ ةمظنأ ةثالث كانەو قلدسنملا ةمئاقلا.

صصخم NAP جەن ءاشنإل رايخلل **ةكېشلا ليلحت جەن** ةمئاق ددح.

ASA ASA FIREPOWER Default Allow All Traffic custom policy Status: Policy Up-to-date on device Identity Policy: More Rules Security Intelli Network Analysis and Intrusion Policies Rules Security Intelli Network Analysis and Intrusion Policies Physican Rules Intrusion Policy Variable Set Intrusion Policy Retry URL cache miss to Inspect traffic during po Inspec	Configuration > ASA FirePOV	VER Configuration > Policies > Access	s Control Policy			
Default Allow All Traffic custom policy Identity Policy: None Identity Policy: None Rules SSL Policy: None Intrusion Policy used before Access Control Intrusion Policy Variable Set Intervert Analysis Rules Intervert Analysis	ASA ASA FirePOWE	R				
Default Allow All Traffic custom policy						
Custom poicy	Default Allow All	Traffic				
Identity Policy: None SSL Policy: None Rules Security Intelling Network Analysis and Intrusion Policies ? × General Settings Intrusion Policy used before Access Control Maximum URL character Intrusion Policy Variable Set Intrusion Policy Variable Set Default-Set Allow an Interactive Blog Network Analysis Rules Network Analysis Rules No Custom Rules Default Network Analysis Policy Balanced Security and Connectivity Intrustop Policy Setting Revert to Defaults SSL Policy Settings None SSL Policy to use for inspecting encrypted connections None	custom policy					
Identity Policy: None SSL Policy: None Rules Security Intellit Network Analysis and Intrusion Policies ? × General Settings Intrusion Policy used before Access Control No Rules Active Maximum URL characters Intrusion Policy Variable Set Default-Set Allow an Interactive Bloc Network Analysis Rules No Custom Rules Inspect traffic during policy Default No Custom Rules Identity Policy Settin Revert to Defaults OK SSL Policy Settings None Performance Statistics - Sample Time (seconds) 300 Regular Expression - Limit Default Default Default						
Identity Policy: None SSL Policy: None Rules Security Intellity Rules Security Intellity Maximum URL charactere Intrusion Policy used before Access Control rule is determined No Rules Active Allow an Interactive Blor Network Analysis Rules Default-Set Network Analysis Rules No Custom Rules Intrusion Policy List Default Network Analysis Policy Balanced Security and Connectivity Image: Connectivity Connectivity Intrustion Policy Settin Revert to Defaults No Image: Connectivity Connectivity SSL Policy Settings Image: Connectivity Connectivity Statistics - Sample Time (seconds) 300 Regular Expression - Limit Default Default Default				M 📑 Status: Policy Up-to-date on device		
Rules Security Intellit Network Analysis and Intrusion Policies ? × General Settings Intrusion Policy used before Access Control rule is determined No Rules Active Image: Control rule is determined No Allow an Interactive Bloc Intrusion Policy Variable Set Default-Set Image: Control rule is determined No Inspect traffic during policy Network Analysis Rules No Custom Rules Network Analysis Policy List Disabled Identity Policy Settim Revert to Defaults No Image: Control rule is Control rule is Control rule is Control rule is determined No Image: Control rule is Control rule rule is	Identity Policy: None	SSL Policy: None				
General Settings Intrusion Policy used before Access Control rule is determined No Rules Active Intrusion Policy Used before Access Control rule is determined No Rules Active No Allow an Interactive Blo Intrusion Policy Variable Set Default-Set Intrusion Policy Used Intrusion Policy Used <th>Rules Security Intellic Ne</th> <th>twork Analysis and Intrusion Pol</th> <th>licies</th> <th>? ×</th> <th></th> <th></th>	Rules Security Intellic Ne	twork Analysis and Intrusion Pol	licies	? ×		
Maximum URL characters rule is determined Intrusion Policy Variable Set Default-Set Image: Constraint of the constraint	General Settings	ntrusion Policy used before Access Control	No Rules Active		Ø	
Allow an Interactive Bloc Retry URL cache miss loo Inspect traffic during pol Identity Policy Settin SSL Policy to use for inspecting encrypted connections None N	Maximum URL characters	ule is determined			No	
Retry URL cache miss loo Network Analysis Rules No Custom Rules Network Analysis Policy List Inspect traffic during pol Default Network Analysis Policy Balanced Security and Connectivity Image: Connectivity custom Rules Identity Policy Settin Revert to Defaults OK Cancel yze Per 5 Identity Policy Settings Image: Connectivity custom Rules Performance Statistics - Sample Time (seconds) 300 SSL Policy to use for inspecting encrypted connections None Regular Expression - Limit Default	Allow an Interactive Bloc	ntrusion Policy variable Set	Default-Set		Ø	
Inspect traffic during pol Default OK Cancel Ivze Per 5 Identity Policy None None Performance Statistics - Sample Time (seconds) 300 SSL Policy Settings Image: SSL Policy to use for inspecting encrypted connections None Regular Expression - Limit Default	Retry URL cache miss loo	letwork Analysis Rules Default Network Analysis Policy	No Custom Rules	Network Analysis Policy List	Disabled	
Identity Policy Settin Revert to Defaults OK Cancel Iyze Per 5 Identity Policy None Performance Statistics - Sample Time (seconds) 300 SSL Policy Settings Image: SSL Policy to use for inspecting encrypted connections None None Regular Expression - Limit Default Regular Expression - Recursion Limit Default	Inspect traffic during pol	Count Network Analysis Forey	Dalanceu Security a		Ø	
Identity Policy None SSL Policy Settings Performance Statistics - Sample Time (seconds) 300 SSL Policy to use for inspecting encrypted connections None Regular Expression - Limit Default Regular Expression - Recursion Limit Default	Identity Policy Settine	Revert to Defaults		OK Cancel Iyze Per	5	
SSL Policy Settings Image: Solution of the seturation	Identity Policy		None	Devformance Chatictics - Comple Time (coconds)	200	
SSL Policy to use for inspecting encrypted connections None Regular Expression - Recursion Limit Default	SSL Policy Settings		Ø	Performance Statistics - Sample Thire (seconds)	Default	
Regula Expression Recursion Entre	SSL Policy to use for inspectin	ng encrypted connections	None	Regular Expression - Control Imit	Default	
Network Analysis and Intrusion Policies	Network Analysis and Int	rusion Policies	Ø	Intrusion Event Logging Limits - Max Events Stored Per Packet	8	
Store ASA FirePOWER Changes Cancel				ER-Changes Cancel		

تاريغتملا تاعومجم نيوكت

ردصملا ذفانمو نيوانع ديدحتل لفطتلا دعاوق يف تاريغتملا تاعومجم مادختسإ متي لكشب كيدل ةكبشلا ةئيب تاريغتملا سكعت امدنع ةيلاعف رثكأ دعاوقلا نوكت .ةهجولاو ءادألا طبض يف امهم ارود ريغتملا بعلي .ةقد رثكأ.

مق .(ذفنملا/ةكبشلا) يضارتفالا رايخلا مادختساب لعفلاب تاريغتملا تاعومجم نيوكت مت يضارتفالا نيوكتلا رييغت ديرت تنك اذإ ةديدج تاريغتم تاعومجم ةفاضإب.

< نئاكلا ةراد
 ASA Firepower > نئاكل قراد
 ال قر

ذفنملا مقر لقح يف ذفنملا مقر ددحف ،نيعم ذفنم ىلع لمعي صصخم قيبطت يأ ناك اذإ. ةكبشلا ةملعم نيوكتب مق.

.ةيلخادلا ةكبشلا ددح home_net\$

ةيجراخلا ةكبشلا ددح ecternal_NET.

ASA FirePOWER Configuration	Configuration >	> ASA FirePOWER	Configurati	ion > Obje	ect Management > Variable Set			
Policies Device Management Solutions Monagement Monagement		Add Variable Set						
Port	Name	Name Description						
Application Filters	Default-Set				This Variable Set is system-provided.		0	
URL Geol ocation	New Varia	able Set				? ×	:	
	Name:	Name: Custom_Variable_Set						
Sinkhole	Description	Enter a description	on					
- If FileList						🔘 Add		
⊕	Variable	Variable Name Type Value						
Eccal	Customiz	ed Variables	- 23	24				
Updates	This categ	iory is empty						
Elcenses	Default V	Default Variables						
🗄 🖏 Integration	AIM_SERV	AIM_SERVERS		[64.12.	31.136/32, 205.188.210.203/32, 6]	2 36		
	DNS_SERV	/ERS	Network	HOME_N	NET	2 36		
	EXTERNAL	_NET	Network	any		2 38		
0000	FILE_DATA	PORTS	Port	[HTTP_I	PORTS, 143, 110]	Ø78		
Device Setup	FTP_PORT	S	Port	[21, 21	00, 3535]	2 26		
🚯 Firewall	GTP_PORT	S	Port	[3386,	2123, 2152]	Ø76		
Remote Access VPN	HOME_NE	г	Network	any		Ø28	> C	
Site-to-Site VPN	4					•		
ASA FirePOWER Configuration								
Device Management					Store ASA FirePOWER Change	s Cancel	J	

/NAP /ماحتقالاا تاسايس نيمضتل لوصولا يف مكحتلا نيوكت :3 ةوطخلا تاريغتملا تاعومجم

يف مكحتلا ةسايس < تاسايسلا > ASA Firepower Configuration > نيوكتلا ىل القتنا اذه متي نأ جاتحت تنأ **لوصول**ا

- لفطتلا جەن نييعت ديرت ثيح "لوصولا جەن" ةدعاق ريرحتب مق .1.
- . شيتفتلا بيوبتلا ةمالع رتخأ.
- ةمئاقلاا نم **تاريغتملا تاعومجم** رتخاو ةلدسنملا ةمئاقلاا نم **ماحتقالاً جەن** رتخأ 3. ةلدسنملا

.**ظفح** ۃﻕطﻕط .4

1 Access Boliov Bulo	2014	701/		201/ 20		2014	701/	701/	Allow	
Poot Bulos	any	any a	пу	any an	y any	any	dily	any	Allow	
Root Rules										
Editing Rule - Access	_Policy_R	Rule								? ×
Name Access_Policy_Rul	e			In E	nabled		Move			
Action 🖌 Allow			IPS:	IPS_Policy	Variables: [Default-Set	Files: no	inspection Lo	gging: no la	ogging
Zanas Naturatia	A Users	Applications	Derte			ttributor	2	Increation	Logging	Commonte
Zones Networks	Osers	Applications	Ports	A URLS	A ISE A	ttributes		Inspection	Logging	Comments
Intrusion Policy						Variable	Set			
IPS_Policy					× 0	Default	Set			
Sile Delieu										
News										
None										•
									Care 1	Canad
									Save	Cancel

نوللاب عردلا زمر ةيؤر كنكمي .هذه لوصولا جەن ةدعاق ىلإ ماحتقإ ةسايس ةفاضإ ذنم لفطتلا جەن نيكمت ىلإ ريشي يذلا يبەذلا.

										🖌 📑 Sta	tus: Acces	ss Control policy out-	of-date on devi	ce
Ide	ntity Polic	y: None		SSL Policy: <u>N</u>	one									
Ru	les Sec	urity Inte	elligence	HTTP Responses	Advanced									
									🕜 Add Ca	tegory 📀 A	dd Rule	Search Rules		×
#	Name		Source Zones	Dest Zones	Source Networks	Dest Networks	Users	Applicat	Src Ports	Dest Ports	URLs	Action	V 🕞 🖉 🗸	
Adm	ninistrator	Rules		24		Се	, 	20			20		44	- Cr
Thi	This category is empty													
Sta	ndard Rule	s												
1	Access_Pol	licy_Rule	any	any	any	any	any	any	any	any	any	Allow	0 [] (]	0
Roo	t Rules											/		
Thi	s category i	s empty												
Def	ault Actio	n							Intrusion P	revention: Balan	ced Securi	ity and Connectivity	*	\$ 📕
										Displaying	1 - 1 of 1	1 rules 🛛 🔾 🗸 Page	1 of 1 >	> C
						Store	ASA FirePOW	ER Changes	Cancel					

تارييغتالا ظفحل ASA FirePOWER تارييغت نيزخت قوف رقنا.

رشنلا ىل لوصولاب مكحتلا ةسايس .4 ةوطخلا

مكحتلا جەن ىرتس ،جەنلا قېبطت لبق .لوصولاب مكحتلا جەن رشن كېلع بجي ،نآلا رعشتسملا ىلع تارىيغتلا رشنل .زاەجلا ىلع مېدق ةراشإلىل لوصولاب:

- .**رشن** قوف رقنا .1
- 2. ت**ارييغت رشن** قوف رقنا
- .ةقەثبنملا ةذفانلا يف **رشني** ةقطقط .3

File View Tools Wizards Window	Help
Home 🇠 Configuration 🔯 Monitor	Deploy - 🐼 Refresh 🔇 Back 🔘 Forward 🢡 He
Device List	2 Deploy FirePOWER Changes Ctrl+D
🕈 Add 📋 Delete 🚿 Connect	Save Running Configuration to Flash Ctrl+S
Find: Go	TON NONTHOLOMEN



ASA FirePOWER تاريي غت قي بطت قوف رقن لا كمزلي ، رعشت سمل على لوصول مسايس قي بطت ، 5.4.x رادص إلى يف : قطح الم

.ن يو الختال ري ي غت ق ي بطتال قومها ال المكار نم داكات . تم معها قاراح < ASA FirePOWER مجتى ارم < قبق ارمها عل القتان : تظر الم

لفطتلا ثادحأ ةبقارم .5 ةوطخلا

ة مت يت الفطت الفراك العال المت عال الفطت الترام عال الفطت الترام عال المت عال ال الترام عال ال الترام عال ال ا ASA FirePOWER ، **ي ل عفل اتقول احي حصت (ASA FirePOWER ةبقارم (**

	hitoring > Real Time Ev	<u>entinq</u>			
r & Eventing					
Gaurav_Connection_Eve	ents × All ASA FirePOW	ER Events Connection	Intrusion File	Malware File	Security Intelligen
Filter					
Rule Action=Block * reaso	n=Intrusion Block ×				
10					
Pause Refresh	Rate 5 seconds	• 1/10/16 6:13:	:42 PM (IST)		
Pause Refresh Receive Times	Rate 5 seconds Action	 1/10/16 6:13: Event Type 	:42 PM (IST)	nline Result	Reason
Pause Refresh Receive Times 1/10/16 6:11:50 PM	Rate 5 seconds Action Block	1/10/16 6:13: Event Type ASA FirePOWER Co	:42 PM (IST)	nline Result	Reason Intrusion Bloc
Pause Refresh Receive Times 1/10/16 6:11:50 PM 1/10/16 6:09:52 PM 1/10/16 6:09:52 PM	Rate 5 seconds Action Block Block	1/10/16 6:13: Event Type ASA FirePOWER Co ASA FirePOWER Co	:42 PM (IST) Innection	nline Result	Reason Intrusion Bloc

ةحصلا نم ققحتلا

نيوكتلا اذه ةحص نم ققحتلل ءارجإ اًيلاح دجوي ال.

اهحالصإو ءاطخألا فاشكتسا

جيحص لكشب دعاوقلا ةلاح نيوكت نم دكأت .1 ةوطخلا.

لوصولا دعاوق يف ةحيحصلا IPS ةسايس نيمضت نم دكأت .2 ةوطخلا.

تاعومجم نيوكت متي مل اذإ .حيحص لكشب تاريغتملا تاعومجم نيوكت نم دكأت .3 ةوطخلا رورملا ةكرح عم تاعيقوتلا قباطتت نلف ،حيحص لكشب تاريغتملا.

حاجنب "لوصولاب مكحتلا جەن" رشن لامتكا نم دكأت .4 ةوطخلا.

رورملا ةكرح قفدت ناك اذا امم قرقحتلل لفطتلا ثادحأو لاصتالا ثادحاً ةبقارم .5 ةوطخلا ال مأ ةحيحصلا ةدعاقلا برضي.

ةلص تاذ تامول عم

- توطمناه المحولل عيرساه عدباه اليا المحمد المحمد المحمد المعالي المحمد المحم
- · تادنتسمالاو ينقتلام عدلا

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