ءانثأ ءادوسلا ةمئاقلا يف IP جاردإ نيوكت لا عاكذ مادختسإ ASDM لالخ نم Cisco المألا عاكذ مادختس عبرملا لخاد ةرادإلا)

تايوتحملا

قمدق مليا قمدة من الماليات تابل طتمل تابل طتمل تابل طتمل قمدة تسمل التابولعر قمدة تسمل التابولعر قمين الماليات مولع مراع تام اللا تامول ع مراع تام اللا تامول ع مرعاق تام اللا تامول ع مرعال م المالي قام اللا مالي المالي م المالي م المالي تام اللا مالي المالي م المالي م المالي تام اللا مالي المالي م المالي م المالي تام اللا مالي المالي م المالي م المالي م المالي تام اللا مالي م المالي م الما

ةمدقملا

IP ل ءادوسلا ةمئاقلا نيوكتو Cisco نم نامألاا تامولعم/IP ناونع ةعمس دنتسملا اذه فصي ةعمسلا ضفخنم IP ناونعل يئاقلت/صصخم بيو زجوم مادختسإ ءانثأ (رظحلا).

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- لباقلا نامألا ةزهجأ ريدم) ASDM و (ASA) فيكتلل لباقلا نامألا زاهج ةيامح رادج ةفرعم (فيكتلل
- FirePOWER نامأ زاهج ةفرعم •

. قيام حسي خرت نامأل اتامول عم ةيف صت بلطتت : قظ حالم

ةمدختسملا تانوكملا

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

• اتادحول من ا اتادحول ASA FirePOWER (ASA 5506X/5506H-X/5506W-X، ASA 5508-X، ASA مي طمن ا

ىلعأو 5.4.1 رادصإلا لغشت يتلا (X-5516-X

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

ةيساسأ تامولعم

مت IP نيوانعل مظتنم لكشب ةثدحم تاعومجم ةدع نم Cisco نم نامألا تارباخم فلأتت قيرف قطساوب ةئيس قعمس تاذ اهنأ نم ققحتلا جماربلاو IP مزح لثم هذه IP نيوانع نم راض طاشن يأ ءاشنإ مت اذإ ةضفخنملا ةعمسلا كلذ يلإ امو عادخلا تامجهو قراضلا.

و Bogon و نيمجاهملا تانايب ةدعاق Cisco IP Security Intelligence نامأ تامولعم زجوم عبتتي و Bogo و ExploitKit و Open_proxy و Open_relay و DGA و Suspicious و Suspicious و Suspicious و IP ناونعل صصخم بيو زجوم ءاشنإ رايخ FirePOWER ةيطمنلا ةدحولا رفوت . قعمسلا ضفخنم.

نامألا تامولعم زجوم ىلع ةماع ةرظن

اهفينصت نكمي يتلاا IP نيوانع تاعومجم عون لوح ةيفاضإلا تامولعملا ضعب يلي اميف نامألا ءاكذ يف ةفلتخم تائفك.

ةلواحم وأ فعضلا طاقن نع اثحب رارمتساب اهحسم متي يتلا IP نيوانع ةعومجم :نيمجاهملا يرخأ ةمظنأ لالغتسإ.

يأ ةمجاهمب موقت وأ ةراضلا جماربلا رشن لواحت يتلا IP نيوانع ةعومجم :ةراضلا جماربلا طشن لكشب اهترايزب موقي صخش.

عادخ طشن لكشب لواحت يتلا ةفيضملا تائيبلا نم ةعومجم :يلايتحالا ديصتلا رورملا تاملكو نيمدختسملا ءامسأ لثم ةيرس تامولعم لاخدال نييئاەنلا نيمدختسملا.

لﺉاسر لاسرال ردصمك اەدىدحت مت يﺕﻝﺍ ﻗﻑيۻﻣﻞﺍ ﺕﺍﺉيﺏﻝﺍ ﻥﻡ ﻗﻉﻭﻣﺞﻢ **:ﻱﺉﺍﻭﺷﻉﻝﺍ ﺩﻱﺭﺏﻝﺍ** .يﺉﺍﻭﺷﻉﻝﺍ يﻥﻭﺭﺕﻙﻝﺍﻝﺍ ﺩﻱﺭﺏﻝﺍ

زاهج اهيف مكحتيو ،ام ةكبش يف طاشنب كراشت يتلا ةفيضملا ةزهجألا نم ةعومجم **:توب** فورعم توب ةكبشب مكحت.

CNc: ةكبشل مكحت مداوخك اهديدحت مت يتلا ةفيضملا تائيبلا نم ةعومجم BOTNET ةكبشل مكحت مداوخك المديدحت مت يتلا

OpenProxy: بيولاا تايسكورب" ليغشتب ةفورعملا ةفيضملا تائيبلا نم ةعومجم قلوهجم بيو ضارعتساٍ تامدخ ميدقتو "قحوتفملا.

كيربال ليحرت تامدخ ميدقتب ةفورعمال ةفيضمال تائيبال نم ةعومجم OpenRelay: ديربال ليحرت تامدخ ميدقتب ةفورعمال قفيضمال تائيبال المي عادخان ويثاوشعال ديربال ومجاهم اهمدختسي يتال لوهجمال ينورتكالال

ةكبشل جورخلا دقع تامدخ ميدقتب ةفورعملا ةفيضملا تائيبلا نم ةعومجم **:TorExitNode**

.Tor ةيوەلا لوحم

.رورم ةكرح لسرت اەنكلو ةصصخملا ريغ IP نيوانع ةعومجم Bogon: رورم ةكرح ل

طشنلا ثحبلا ديق يتلاو ابيرم اطاشن رهظت يتلا IP نيوانع ةعومجم **:بيرم**

كولسلاب مايقلاا ءانثأ رركتم لكشب اهتظحالم مت يتلا IP نيوانع نم ةعومجم **:ةباجتسإلا** راضلا وأ بيرملا

ةيملاعلا ءادوسلا ةمئاقلا ىلإ ايودي IP نيوانع ةفاضإ ةيملاعلا ءاضيبلا مداوخلاو

امدنع ةيملاعلا عادوسلا ةمئاقلا ىل قنيعم IP نيوانع ةفاضإب FirePOWER قدحو كل حمست تنك اذإ ،Global-Whitelist ىل IP نيوانع ةفاضإ اضيأ نكمي .راض طاشن نم ءزج اهنأ فرعت قمئاقلل IP نيوانع قطساوب اهرظح متي ةنيعم IP نيوانع ىل رورملا قكرحب حامسلا ديرت زيح لخدي هنإف ،Global-BlackList/Global-Whitelist ىل IP ناونع يأ قفاضإب تمق اذإ .ءادوسلا قربطات يل IP ناونع يأ قفاض

ىل IP ياونع ةفاضإ لجأ نم Global-BlackList/ Global-Whitelist، اناونع ةفاض الجأ ددحو لاصتال ثادحأ يف سوامل كيرحتب مق BirePOWER Monitoring > Real Time Eventing، ددحو لاصتال ثادحأ يف سوامل عرف ليصافتل ضرع.

قوف رقنا. IP ناونع امإ ةفاضإ كنكمي global-blackList/ global-whitelist. قوف رقنا العن العن العن العن العن العن ا وه امك ،ةلباقملا ةمئاقلا ىل IP ناونع ةفاضإل WhiteList Now/BlackList ددحو رزلا **ريرحت** ةروصلا يف حضوم.

All ASA FirePOV	VER Events Con	nection Intrusion	n File Malwa	re File Security Intel	ligence
Filter					
Rule Action=Allow	¢				
·					
Pause	Defrech Date 5	seconds	* 1/25/16	0-11-25 AM (IST)	
	venean kate 5	seconds	- 1/23/10	5.11.25 AH (151)	
Receive Times	AC	tion	First Packet	Last Packe	t Reaso
1/25/16 9:09:50 AM	All	ow	1/25/16 9:09:4	8 AM 1/25/16 9:09	9:49 AM
1/25/16 9:07:36 AM	All	ow 🖑	1/25/16 9:07:0	View details	7:03 AM
1/25/16 9:07:07 AM	All	ow	1/25/16 9:07:0	06 AM 1/25/16 9:07	7:06 AM
toring > ASA FirePOW	/FR Monitoring 5	Real Time Even	tina		
Time Eventing		- Real Fine Even	ung		
			Respond	er E	dit
Initiator			Deserved	- ID 10 10	445
Initiator Initiator IP	192.168.2	20.3 /	Responde	10.100	ATT 0 /
Initiator Initiator IP Initiator Country a Continent	192.168.2 and <i>not availa</i>	20.3 A Whitelist Now	Responde	r Country and not av	ailable

ةمئاقلا /ةيملاعلا ءادوسلا ةمئاقلا ىلإ ةمجولا وأ ردصملل IP ناونع ةفاضإ نم ققحتلل < **نئاكلا ةرادا > ASA FirePOWER Configuration > نيوكتلا** ىلإ لقتنا ،ةيملاعلا ءاضيبلا **ةمئاقلا /ةيملاعلا ءادوسلا ةمئاقلا** ريرحتو **بيولا تازجومو تاكبشلا مئاوق < نامألا ءاكذ** ةمئاقلا نم IP ناونع يأ ةلازال فذحلا رز مادختسإ اضيأ كنكمي .<mark>ةيملاعلا ءاضيبل</mark>ا

ءادوسلا ةمئاقلل IP ناونعل ةصصخم ةمئاق ءاشنإ

اهمادختسإ نكمي يتلا ةصصخملا ةكبشلاP/ا نيوانع ةمئاق ءاشنإب Firepower كل حمسي كلذب مايقلل تارايخ ةثالث كانه .(رظحلا) ءادوسلا ةمئاقلا يف

- ليمحت كنكميو (رطس لكل دحاو IP ناونع) يصن فلم ىلإ IP نيوانع ةباتك كنكمي .1 ASA < نيوكتلا ىلإ لقتنا ،فلملا ليمحتل .FirePOWER قيطمنلا ةدحولا ىلإ فلملا مث **بيولا زجومو ةكبشلا مئاوق < نامألا ءاكذ < نئاكلا ةرادإ < FirePOWER Configuration** ةمئاقلا مسا ددح **:مسالاً بيولاً زجومو ةكبشلاً مئاوق ةفاضاٍ** ىلع رقنا رتخأ **:ليمحتلا ةمئاق** .قلدسنملاً ةمئاقلاً نم **ةمئاقلاً** ديدت **:عونلاً** .قصصخملاً .فلملا ليمحتل عوم داريخ ددح .كماظن يف يصنا افلملاً عقوم ديدتا .
- ل صتت يتلا ةصصخملا ةمئاقلل ةيجراخ ةهجل IP ل تانايب ةدعاق يأ مادختسإ كنكمي .2 نيوكت لجأ نمو .IP نيوانع ةمئاق بلجل ةيجراخ ةهج مداخب ةيطمنلا FirePOWER قدحو اهب **نيوكت الجأ نمو ASA FirePOWER Configuration > Object Management (نيوكت) مئاوق < (نامألاا ءاكذ) Security Intelligence (نئاكلا قرادا) مئاوق < (نامألاا ءاكذ) Security Intelligence (نئاكل قرادا) ميولا زجومو ةكبشلا مئاوق ةفاضا** قوف رقنا مث **بيول زجوم و ةكبشلا** .صريخملا بيو زجوم مسا ددح :

ةلدسنملا ةمئاقلا نم رايخلل **ٻيو زجوم** ددح **:عونلا**.

ةدحو ەب لصتت نأ بجي يذلا مداخلاب صاخلا URL ناونع ددح **:بيولا زجوم URL** .ەيلإ بيولا زجوم ليزنتتو ةيطمنلا FirePOWER

زجوملل URL ناونع راسم نم ققحتلل ةئزجتلا ةميق ددح :URL ناونع .

URL. بيو زجوم مداخب ماظنلا هيف لصتي يذلا ينمزلا لصافلا ددح **:ثيدحتا راركت**

	U	Ipdate Feeds O Add Network Lists and Feed
Name	Security Intellig	gence for Network List / Feed ?
Cisco-Intelligence-Feed <i>Last Updated: 2016-01-22 05:56</i> Custom_Feed	Name: Type:	Custom_Feed List
Global-Blacklist Global-Whitelist	Upload	Store ASA FirePOWER Changes Cancel
guration > ASA FirePOWER Configurat	tion > Object Management	t > SecurityIntelligence > Network Lists and Feeds
guration > ASA FirePOWER Configurat	tion > Object Management	t > SecurityIntelligence > Network Lists and Feeds pdate Feeds Add Network Lists and Feed pence for Network List / Feed ?
guration > ASA FirePOWER Configurat Name Cisco-Intelligence-Feed	tion > Object Management U Security Intellig Name:	t > SecurityIntelligence > Network Lists and Feeds pdate Feeds O Add Network Lists and Feed gence for Network List / Feed ? Custom_Network_Feed
iguration > ASA FirePOWER Configurat Name Cisco-Intelligence-Feed Last Updated: 2016-01-22 05:56: Custom_Feed	tion > Object Management U Security Intellig Name: Type: Feed URL:	t > SecurityIntelligence > Network Lists and Feeds pdate Feeds O Add Network Lists and Feed gence for Network List / Feed ? Custom_Network_Feed Feed http://192.168.30.1/blacklist-IP.txt
iguration > ASA FirePOWER Configurat Name Cisco-Intelligence-Feed Last Updated: 2016-01-22 05:56: Custom_Feed Global-Blacklist	tion > Object Management U Security Intellig Name: Type: Feed URL: MD5 URL:	t > SecurityIntelligence > Network Lists and Feeds pdate Feeds ③ Add Network Lists and Feed gence for Network List / Feed ? Custom_Network_Feed Feed http://192.168.30.1/blacklist-IP.txt (optional)

نامألا تامولعم نيوكت

ح تاسايسلا < ASA Firepower Configuration < نيوكتلا ىل ل ق ت ا ، ن ام أل ا ءاكذ ن يوك ت ل
 درج ،لوصول يف مكحتل قسايس

رظح/حامسلل Whitelist/ BlackList دومع ىلإ لقتناو ،حاتملا ةكبشلا نئاك نم بيولا زجوم رتخأ راضلا IP ناونعب لاصتالا.

ةروصلا يف ددحم وه امك ليجستلا نيكمتو ةنوقيألا رقن كنكمي.

نميألا سواملا رزب رقنا ،لاصتالا رظح نم الدب ةراضلا IP تالاصتال ثدح ءاشناٍ ديرت تنك اذاٍ ةروصلا يف حضوم وه امك ،**(رظحلا مدع) طقف ةبقارملا عضو** رتخاو ،بيولا زجوم قوف:

Configuration > ASA FirePOWER Config	uration > Policies > Access Control Po	icy	6
ASA ASA FirePOWER			
Default Allow All Tra Enter a description	ffic	Status: Policy Un-to-date	You have unsaved changes
Identity Policy: <u>None</u> Rules Security Intelligence	SSL Policy: Default SSL Policy HTTP Responses Advanced		
Available Objects C C Search for a Network Networks URLs Attackers Bogon Bots CnC Malware Open_proxy Open_relay Phishing	Available Zones C	Add to Whitelist Add to Blacklist	S Policy Blacklist (7) Enable logging Networks S Global-Blacklist (Any Zone) URL (Any Bots (Any Zone) Block Block Monitor-only (do not block) Cogging Options Select All Delete
4	Store 650	FirePOWER Channes Cancel	•

.ددرتملا رايتلا ةسايس تارييغت ظفحل ASA FirePOWER تارييغت نيزخت رايخ رتخاً

رشنلا ىلإ لوصولاب مكحتلا ةسايس

قيبطت لبق .لوصولاب مكحتاا جەن رشن بجي ،لوعفملا ةيراس تارييغتال حبصت يكل ال مأ زامجلا ىلع ثدحم ريغ لوصولا يف مكحتال جەن ناك اذإ ام ىلإ ةراشإلا عجار ،جەنالا.

مث **FirePOWER تارييغت رشن** رتخاو **رشن** قوف رقناج ،رعشتسملا ىلع تارييغتلا رشنل تارييغتلا رشنل ةقثبنملا ةذفانلا يف **رشن** ددح.

File View Tools Wizards Window	Help
Device List □ ♣ Add	2 Deploy FirePOWER Changes Ctrl+D Save Running Configuration to Flash Ctrl+S
Deploy FirePOWER Changes	
Deploy Policies Version:2016-01	1-05 09:09 AM ?
System Policy: Default Sensor Policy: firepower	
 Access Control Policy: Default Allow A Intrusion Policy: Balanced Security 	All Traffic and Connectivity
 Intrusion Policy: IPS_Policy DNS Policy: Default DNS Policy 	
	Teploy Cancel

ASA FirePOWER تارىي غت قى يبطت قى وف رقن ا كمزلى ، رعشت سما على علو صول المسايس قى يبطت ل ، 5.4.x راد ص إلى ايف : قطح الم

ين يو كتل ات اري يغت ق يبطت لقمهم ال المكا بجي من أن مدكات . قم ممل اقل اح < ASA FirePOWER قبق ارم ما عل إلق تن ا : قطح الم

ينمألا ءاكذلا ثادحأ ةبقارم

ةدحو ةطساوب نامألاا ءاكذ ةدهاشمل FirePOWER، قدحو ةطساوب نامألاا ءاكذ ةدهاشمل ASA **قبقارم < ةبقارملا** ىل إلقتنا كلذ يدؤيس .**نامألاا تامولعم** بيوبتلاا ةمالع ددح .**يلعفلا تقولا يف قيقدتلاا < FirePOWER** قروصلا يف حضوم وه امك ثادحألاا راهظإ ىلإ

Monitor	onitoring > ASA FirePOWER Monitoring > Real Time Eventing						
-Real Tim	al Time Eventing						
	All All A FirePOWER Events	Connection Intrusion	File Malware File	Security Intelligence			
F	Filter						
ſ	Enter filter criteria						
	Pause Refresh Rate 5 seconds 2/9/16 1:03:31 PM (IST)						
	Receive Times	Action	First Packet	Last Packet	Reason	Initiator IP	Responder IP
	2/9/16 1:01:48 PM	Block	2/9/16 1:01:47 PM		IP Block	192.168.20.3	184.26.162.43

ةحصلا نم ققحتلا

نيوكتلا اذه ةحص نم ققحتلل ءارجإ أَيلاح دجوي ال.

اهحالصإو ءاطخألا فاشكتسا

ASA **نيوكت < نيوكتل**ا ىلإ لقتنا ،ةثدحم ةيكذلاا نامألاا تامولعم تاميقلت نأ نامضل مت يذلا تقولاا ددحو **بيولا زجومو ةكبشلا مئاوق < نامألاا ءاكذ < نئاكلاا قرادإ < FirePOWER** .بيولا زجوم ثيدحت راركت طبضل ريرحت رز رايتخإ كنكمي .قرم رخآ هيف بيولاا زجوم ثيدحت

nfiguration > ASA FirePOWER Configuration >	<u>Object Management > SecurityIntelligence > Network Lists a</u>	nd Feeds			
Update Feeds 🕢 Add Network Lists and Feeds 🔍 Filter					
Name	Туре				
Cisco-Intelligence-Feed Last Updated: 2016-02-08 10:03:14	Feed	0			
Custom_Feed	Feed	0			
Global-Blacklist	List	Ø 🖯			
Global-Whitelist	List	08			

حاجنب لوصولاب مكحتلا جەن رشن لامتكا نم دكأت.

ال مأ ةلطعم رورملا ةكرح تناك اذإ ام ةفرعمل ةينمألا ةيتارابختسإلا تامولعملا بقار.

ةلص تاذ تامول عم

- درولل عيرسال اعدبال اليال متحول عيرسال المحدبال المياد المعدبال المعاد المع
- · تادنتسمال وين ق تارا معدل ا

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