تانايب راسم ءاطخأ فاشكتسأ نم 4 ةلحرملا يف مكحتلا ةسايس :اهحالصإو Firepower لوصولا

تايوتحملا

مدق ملا امحال صاو (ACP) لوصول ايف مكحتل اقسايس قل حرم عاطخ أفاش كتس ل اصتال ا ثادح أنم ق ق حتل ا عام ت ق ق حتل ا تاوطخ معي رسل ا فيف ختل ا تاوطخ م<u>تعي رسل ا فيف ختل ا تاوطخ</u> م<u>تعي رسل ا فيف ختل ا تاوطخ</u> م<u>تعي رسل ا فيف حتل ا تاوطخ</u> م<u>تعي رسل ا قكر ح</u> م<u>تعي م</u>اطح ا مقر مط مام ا رورم ل ا قكر ح رظح مت مي ال مقر مط ماوب رورم ل ا قكر ح رظح :3 ويراني س ل م<u>ق</u> محال ا مقر مط ماوج رورم ل ا قكر ح رظح :3 ويراني س ل ام ح ال ص و SSL جهن مق ما عاطخ أفاش كتس أ

ەمدقملا

يف تانايبلا راسم فاشكتسأ ةيفيك حضوت تالاقم ةلسلس نم ءزج يه ةلاقملا هذه رثؤت دق FirePOWER تانوكم تناك اذإ ام ديدحتل يجهنم لكشب اهحالصإو FirePOWER ةمظنأ ةينب لوح تامولعم ىلع لوصحلل <u>"قماع قرظن" قلاقم</u> ىلإ عوجرلا ىجري .رورملا ةكرح ىلع تانايبلا تاراسم ءاطخأ فاشكتسأ" تالاقمب اهتاطابتراو FirePOWER ةيساسألا ةمظنألا .ىرخألا "اهحالصإو

يەو ،اەحالصإو Firepower تانايب راسم ءاطخأ فاشكتسأ نم ةعبارلا ةلحرملا لاقملا اذه يطغي ةيساسألا ةمظنألا عيمج ىلع تامولعملا ەذە قبطنت .(ACP) لوصولا يف مكحتلا ةسايس تارادصإو .



(ACP) لوصولا يف مكحتلا ةسايس ةلحرم ءاطخأ فاشكتسأ اهحالصإو

ىلإ ارشابم ارمأ قفدتلا امعم قفاوتي يتلا ACP ةدعاق ديدحت نوكي نأ بجي ،ماع لكشبو رمظي مل اذإ .مضرف متي يذلا ءارجإلا/ةدعاقلا ةفرعمل "لاصتالا ثادحاً" قعجارم نكمي .مامألا ذيفنت نكمي ،رورملا ةكرح عم (ACP) لوصولا يف مكحتلا ةمئاق مب موقت ام حوضوب كلذ FirePOWER (CLI).

لاصتالا ثادحأ نم ققحتلا

كلذكو ةقباطم رورملا ةكرح نوكت نأ بجي جورخلاو لوخدلا ةمجاو نع ةركف ىلع لوصحلا دعب

ناك اذإ ام ديدحتل ىلوألا ةوطخلا ،قفدتلا تامولعم FirePOWER ناك اذإ ام ديدحتل ىلوألا ةوطخلا ،قفدتلا تامولعم ةرادإ زكرم يف رصانعلا هذه ضرع نكميو .ةينعملا رورملا ةكرحل لاصتالا ثادحأ نم ققحتلل FirePOWER **.ثادحأ < تالاصتإ < ليلحتل** عباتلا

ACP دعاوق يف ليجستلا نيكمت نم دكأت ،لاصتالا ثادحاً نم ققحتلا لبق :**قظحالم** نم ةدعاق لك لخاد "ليجستلا" بيوبتلا ةمالع يف ليجستلا نيوكت متي .كب ةصاخلا "نامألا تامولعم" بيوبتلا ةمالع ىلإ ةفاضإلاب لوصولا يف مكحتلا ةسايس دعاوق. اذه قبطني ."ثادحألا ضراع" ىلإ تالجسلا لاسرال مهب هبتشملا دعاوق نيوكت نم دكأت . يضارتفالا عارجإلا ىلع اضيا

Over	view	Analysis Polic	ies Devices Obj	ects /	AMP Inte	elligence								Deploy	🦺 System Help 🛛	Global \ admin +	
Conte	xt Ex	plorer Connectio	ons + Events Intr	usions •	Files •	Hosts • Use	rs v Vulr	erabilities • Corr	elation •	Custom • Loc	kup • Search						
Con	ne	ction Events	(switch workflow) tails > Table View of Co	innection E	ivents								Bookmark This Pa	ge Report Des	igner Dashboard View B 2017-05-11 13:54:32 - 2	cokmarks Search •	
																Expanding	
No Se	irch C	onstraints (Edit Search)															
Jum	p to	. •															
		• First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	
4		2017-05-11 14:54:32	2017-05-11 14:55:02	Allow		# <u>192.168.1.200</u>		13.173.197.235	SA USA			60084 / tcp	80 (http) / tcp	HTTP	Web browser	Web Browsing	
4		2017-05-11 14:54:02	2017-05-11 14:54:32	Allow		192.168.1.200		73.173.197.235	SA USA			60082 / tcp	80 (http) / tcp	HTTP	Web browser	Web Browsing	
4		2017-05-11 14:53:40	2017-05-11 14:53:55	Allow		192.168.1.200		10.83.181.139				60077 / tcp	135 (loc-srv) / tcp	DCE/RPC	Epmap		
4		2017-05-11 14:52:40	2017-05-11 14:52:55	Allow		192.168.1.200		10.83.181.139				60069 / tcp	Connection Events		(unnamed search)		
4		2017-05-11 14:51:40	2017-05-11 14:51:53	Allow		192.168.1.200		10.83.181.139				60064 / tcp			(annumed search)		
4		2017-05-11 14:51:24	2017-05-11 14:51:24	Allow		192.168.1.200		172.217.26.206	SA USA			60058 / tcp	Sections		Networking		
4		2017-05-11 14:50:40	2017-05-11 14:50:55	Allow		192.168.1.200		10.83.181.139				60056 / tcp	Networking		Responder IP*	192.168.1.200	_
4		2017-05-11 14:50:24	2017-05-11 14:50:24	Allow		192.168.1.200		172.217.26.206	💶 USA			60050 / tcp	Geolocation		Original Client 3P*		
4		2017-05-11 14:50:23	2017-05-11 14:50:53	Allow		192.168.1.200		73.173.197.235	usa 🔜			60051 / tcp	Device Still		Initiator / Responder IP Initiator / Original Clevel IP		
4		2017-05-11 14:49:47	2017-05-11 14:49:47	Allow		192.168.1.200		172.217.26.206	usa 🔜			60043 / tcp	Application		Initiator / Responder / Original	Clert IP	
4		2017-05-11 14:49:40	2017-05-11 14:49:55	Allow		192.168.1.200		10.83.181.139				60046 / tcp	URL		Ingress Security Zone Research Tana		-
4	0	2017-05-11 14:48:46	2017-05-11 14:51:23	Allow		192.168.1.200		# 72.246.56.139	usa 🔜			60041 / tcp	QuS		Ingress / Egress Security Zone		
4		2017-05-11 14:48:46	2017-05-11 14:49:16	Allow		192.168.1.200		73.173.197.235	USA			60040 / tcp			Source Port / ICMP Type		
4		2017-05-11 14:48:40	2017-05-11 14:48:55	Allow		192.168.1.200		10.83.181.139				60037 / tcp	+ New Search		Protocol*		
		2017-05-11 14:48:32	2017-05-11 14:48:32	Allow		192.168.1.200		172.217.26.206	III USA			60031 / tcp	Clobal		DNS Query		
		2017-05-11 14:48:16	2017-05-11 14:48:46	Allow		192.168.1 200		73.173.197.235	USA			60034 / tcp			DNS Response DNS Record Type		
		2017-05-11 14:47:46	2017-05-11 14:48:16	Allow		192 168 1 200		73 173 107 235	A DI LISA			60030 / tro	Predefined Searches		DNS TTL		
		2017 05 11 14:47:40	2012 05 11 14:48:16	Allers		192.100.1.200						40037 / http			DNS Sinkhole Name		
		2017-02-11 14:47:40	2017-02-11 14:47:55	BUILT R					-			927//100	Risky Applications with Lov Belavance	Dusiness .	VLAN ID		
		2017-05-11 14:47:15	2017-05-11 14:48:46	Allow		M 192.168.1.200		TZ.246.56.169	usa			boozz/tep	Standard HTTP		Geolocation		
+		2017-05-11 14:47:15	2017-05-11 14:47:45	Allow		ME 192.168.1.200		B 73.173.197.235	JUSA			60021 / tcp	Standard Hall		Initiator Country		
+		2017-05-11 14:46:45	2017-05-11 14:47:15	Allow		I92.168.1.200		MI 73.173.197.235	usa usa			60017 / tcp			Responder Country		
Last lo	ain on	Tuesday, 2017-04-25 at	12:42:21 PM from rtp-flip	key-88111.4	cisco.com										Initiator / Responder Country		
_																	

ةيؤر كنكمي (ئدابلا) ديرف ردصمل IP فلم ةيفصتو "ثحبلا ريرحت" قوف رقنلاب رورم ةكرحل "حامسلا" "ءارجإلا" دومع رهظي .FirePOWER ةطساوب اهفاشتكا مت يتلا تاقفدتلا فيضملا اذه.

رقنلاا يدؤي ."رظح" ةملك ءارجإلاا نمضتيسف ،ادمع رورملا ةكرح عنمت نارينلا ةوق تناك اذاو ةيلاتلا لوقحلا ةعجارم نكمي .تانايبلا نم ديزم ريفوت ىلإ "لاصتالا ثادحاً لودج ضرع" قوف تقلتك" ءارجإلا ناك اذإ "لاصتالا ثادحاً" يف

- ببسلا -
- لوصولاب مكحتلا ةدعاق -

ةعيرسلا فيفختلا تاوطخ

يلي امب مايقلا نكمي ،ةعرسب ACP دعاوق نع ةمجان اهنأ دقتعي ةلكشم فيفخت لجأ نم:

- ةمئاق ىلعأ يف اهعضوو ةينعملا رورملا ةكرحل "حامسلا" وأ "ةقثلا" ءارجإ عم ةدعاق ءاشنإ مرظحلا دعاوق لك قوف وأ ،ACP
- "رظح" ةمرلك ىلع يوتحي ءارجإ عم اتقؤم دعاوق يأ ليطعت •
- ىلا اتقۇم اەليوحتب مق ،"رورملا ةكرح لك رظح" ىلع يضارتفالا ءارجالا نييعت مت اذا "طقف ةكبشلا فاشتكا"

ةنكمم نوكت ال دق تاسايسلا يف تارييغت عيرسلا فيفختلا هذه بلطتت :**قظحالم** ةدعاقلا ديدحتل ماظنلا معد عبتت مادختسإ ةلواحمب الوأ ىصوي .تائيبلا عيمج يف جەنلا تارىيغت ءارجإ لبق رورملا ةكرح اەعم قباطتت يتلا.

ACP ءاطخأ حيحصت

يف مكحتلا ةمئاق تايلمع لباقم امحالصاو ءاطخألا فاشكتسأ نم ديزملا ذيفنت نكمي ACP) رماوألا رطس ةمجاول ةدعاسملا ةادألا ربع (ACP) رماوأل رطس ةمجاول قدعاسمل قادألا ربع (ACP) لوصول debug.

ةرشقلا ىلإ لوصولا نكمي ،4100 و Firepower 9300 يساسألا ماظنلا يف :**قظحالم** ةيلاتلا رماوألا لالخ نم ةينعملا:

ةيطمنلا ةد<mark>حولا م</mark>كحت قدحو Firepower-module1> **Connect ftd** >

ةصاخلاا (CLI) رماوألاا رطس ةەجاو ىلإ لوصولا نكمي ،ةددعتملا تاليثملل تابيثملل قبسنلاب ةيل مادختساب يقطنملا زامجلاب. # Connect Module 1 telnet Firepower-module1> Connect ftd ftd1 لامكحت قدحوب لامتالا تآلام متي ftd(ftd1) مكحت قدحوب لامتالا تالامتي رطس ةەجاو ىلإ قدوعلل "exit" لخدأ ...ةيواحلل (ftd(ftd1) مكحت قدحوب لامتالا تالامتي ديەمتلاب قصاخلا (CLI) رماوألا

اهمييقت متي ةمزح لكل لاخدا ىلع Firewall-**engine-debug ماظنلا معدل** ةدعاسملا ةادألا يوتحت ال وأ ةدعاقلا قفاوتت اذامل عم ،ةيراجلا ةدعاقلا مييقت ةيلمع رهظت اهنإ ACP. قطساوب قرباطتت.

مدختسي وهو .**ماظنلا معد عبتت** ةادأ ليغشت نكمي ،هدعب امو 6.2 رادصإلا يف :**ةظحالم** اهبلط دنع "y" لاخدا نم دكأت .ليصافتلا نم اديزم نمضتي هنكلو تاملعملا سفن مادختساب .

ةقث ةدعاق قباطت رورملا ةكرح :1 لاثم

رادج-كرحم ءاطخاً حيحصت مادختساب SSH لمع ةسلج ءاشناٍ مييقت متي ،يلاتلا لاثملا يف ماظنلا معد **ةيام**ح.

FirePOWER. زاهج ىلع اەليغشت متي يتلا ACP يە ەذە

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN	Users	Applic	Sourc	Dest P	URLs	ISE/S Attrib	Acti	v h
-	Mandatory - JG AC	(all) (1-6)												
1	Trust ssh for host	Any	Any	👼 192.168.0.7	Any	Any	Any	Any	Any	🥜 SSH	Any	Any	⇒ Tru	ist 🗍 🐚
2	inspect	Any	Any	👳 10.0.0.0/8 🗜	Any	Any	Any	Any	Any	Any	Any	Any	🛹 Allo	ow🤍 🐚
3	trust server backup	Any	Any	👳 192.168.62.3	2 10.123.175.22	Any	Any	Any	Any	Any	Any	Any	⇒ Tru	ıst 🛈 🗈

دعاوق ةثالث اهيدل ئداهلا طيحملاو يبيراكلاو ايقيرفأ لود ةعومجم.

ةمدختسملا ةمجولا ذفانم عم 192.168.0.7 نم رورم ةكرح يأ يف ةقثلا يه ىلوألا ةدعاقلا 1. لبق نم SSH.

- ريياعم قباطتت ثيح 10.0.0/8 نم ةدمتسملا رورملا ةكرح لك ةيناثلا ةدعاقلا صحفت .2 نﺉاك راوجب دوجوملا زمرلا ةطساوب حضوم وه امك) XFF سأر تانايب ىلع ءانب ةكبشلا (ةكبشلا
- 10.123.175.22 ىلإ 192.168.62.3 نم رورملا ةكرح لك يف قثت ةثلاثاا ةدعاقلا .3

ىلا 192.168.62.3 نم SSH لاصتا ليلحت متي ،امحالصإو ءاطخألا فاشكتسأ ويرانيس يف SSH دىل 10.123.175.22.

ة معاق عم لمعلا ةسلج قباطتت نأ عقوتملا نم. له .ةدعاقلا هذه ققباطمل هذه لمعلا قسلج اهقرغتست نأ بجي يتلا مزحلا ددع مك ،وه لاؤسلا اذإو ،ةبولطم ةددعتملا مزحلا وأ AC ةدعاق ديدحتل ىلوألا ةمزحلا يف ةمزاللا تامولعملا عيمج ؟مقرلا وه امف ،كلذك رمألا ناك

ةمئاق ةدعاق مييقت ةيلمع ةيؤرل يلي ام لاخدا مت ،CLI) Firepower (ماوأ رطس ةهجاو ىلع لوصولا يف مكحتلا (ACP).

>system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.3
Please specify a client port:
Please specify a server IP address: 10.123.175.22
Please specify a server port: 22
Monitoring firewall engine debug messages

ءاطخاً حيحصت ليغشت دنع تاملعملا نم نكمم ددع ربكاً ةى بعت لضفألا نم :**حيملت** ىلع طقف ةريثملا ءاطخألا حيحصت لىاسر ةعابط متت ثيحب ،**قيامحلا رادج كرحم** ةشاشلا

ا اهمييقت متي يتلاا ةسلجلا نم ىلوألاا عبرألا مزحلا ىرت ،هاندأ ءاطخألاا حيحصت جارخإ يف

نيس

كآ ،نيس

ةلكآ

(مداخ ىلإ ليمع نم) ىلوألا SSH ةمزح



ربكأ لكشب ءاطخألا حيحصت قطنم حضوي ينايب مسر اذه.

1. SYN 192.168.62.3 → 10.123.175.22

2. SYN,ACK 10.123.175.22 → 192.168.62.3

3. ACK 192.168.62.3 → 10.123.175.22

4. SSH 192.168.62.3 → 10.123.175.22

Starts evaluation at 'inspect' rule

Service identified as SSH No match 'inspect' rule (non-http) Match 'trust server backup' rule and Trust flow

ةدعاقلا ةقباطمل زاهجلل مزح 4 مزلي ،قفدتلا اذهل ةبسنلاب.

ءاطخألاا حيحصت جرخمل يليصفت حرش اذه.

- نأل قباطتت مل "trust ssh for host" ةدعاق نأل "صحف" ةدعاق يف ACP مييقت ةيلمع أدبت تامولعملا عيمج ببسب ةعيرس ةقباطم هذه .تابلطتملا عم قباطتي مل IP ناونع (IPs) ىلوألا ةمزحلا يف ةدوجوم ةدعاقلا هذه قباطتت نأ بجي ناك اذإ ام ديدحتل ةمزاللا (ذفانملاو
- ، قيبطتلا ديدجت متي ىتح "صحف" ةدعاق قباطت رورملا ةكرح تناك اذإ ام ديدجت نكمي ال قيبطتلا نإف ،HTTP قيبطت رورم ةكرح يف X-Forwarding-for (XFF) تامولعم دوجول ارظن راظتنا يف ،2 ةدعاقلل ةقلعم ةلاح يف لمعلا ةسلج عضي اذه نإف كلذل ،دعب فورعم ريغ .قيبطتلا تانايب
- ارظن ،قباطت مدع "صحفلا" ةدعاق نع جتني ،ةعبارلا ةمزحلا يف قيبطتلا ديدحت درجمب HTTP نم الدب ،SSH وه قيبطتلا نأل

IP. نيوانع ىلإ ادانتسا ،"ەب قوثوملا مداخلل يطايتحالا خسنلا" ةدعاق ةقباطم متت مث • ةيامحلا رادج راظتنا ەيلع بجي ەنأل لمعلا ةسلج ةقباطمل مزح 4 لاصتالا بلطتي ،راصتخاب اەيف قيبطت ديق ىلع يوتحت 2 ةدعاقلا نأل ارظن قيبطتلا ديدحتل.

ةمزح كلذ بلطت دق ناكل ،XFF نكت ملو طقف ردصم تاكبش نمضتت 2 ةدعاقلا تناك اذإ ةسلجلا ةقباطمل ةدحاو.

ةلصلا تاذ لوقحلا ىلع يوتحي يذلاو ، firewall-engine-debug رمألا نم عطتقم جارخا يلي اميف فرعملا قيبطتلا مسا ىلع لوصحلل مدختسملا رمألا ظحال .رمحألاب ةزربم.



ةقث ةدعاقل ةقباطملا رورملا ةكرح رظح مت :2 لاثملا

يف ةقث ةدعاق ةقباطم نم مغرلا ىلع رورملا ةكرح رظح نكمي ،تاەويرانيسلا ضعب يف ةزەجألاو لوصولا يف مكحتلا جەن سفن مادختساب رورملا ةكرح يلاتلا لاثملا ميقي ةفيضملا.

ock	Intrusion Block	192.168.62.3	10.123.175.22	55654 / tcp	22 (ssh) / tcp			1	JG AC (all)	trust server backup				
ction >	K <u>Reason</u> X	Initiator IP ×	Responder X IP	Source Port / × ICMP Type	Destination Port / × ICMP Code	Application × Protocol	<u>Client</u> ×	Intrusion × Events	Access Control × Policy	Access Control				
	192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 starting with minimum 0, id 0 and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline sgt tag: 0, ISE sgt id: 0, svc -1, payload -1, client -1, misc -1, user 9999997, icmpType 102, icmpCode 22 192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 3, 'Trust ssh for host', src network and GEO 192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http 192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 5, 'trust server backup', action Trust													
	[!Session was This happened Firewall engine	deleted becaus I before AC rule e will re-evalua	se we hit a drop e was matched te from top of A	IPS rule and b (Intrusion polic) AC policy to find	lacklisted the flow. by before AC rule mains a rule for logging of	atch dropped) decision]								
	192.168.62.3-5 192.168.62.3-5 inline sgt tag: u 192.168.62.3-5 192.168.62.3-5	4650 > 10.123.1 4650 > 10.123.1 ntagged, ISE sg 4650 > 10.123.1 4650 > 10.123.1	75.22-22 6 AS 1 75.22-22 6 AS 1 t id: 0, svc 0, pa 75.22-22 6 AS 1 75.22-22 6 AS 1	I I 0 New sessio I I 0 Starting wit yload 0, client 0, I I 0 pending rul I I 0 Deleting se	n th minimum 4, 'insp misc 0, user 999999 le order 4, 'inspect', ssion	ect', and IPPro 7, icmpType 0, XFF wait for <i>i</i>	oto first with z , icmpCode 0 AppId	cones 1 -> 2,	geo 0 -> 0, vlan (),				

عم قباطتت رورملا ةكرح نأ **ءاطخألا حيحصت-كرحملا-ةيامحلا رادج** جارخا رهظي ،هالعأ رهظي امك "نأل ةددحم) للستلا ةسايس ةدعاق ببسب **رظحلا** ءارجا لاصتالا ثادحاً رهظت نيح يف ،"ةقث لل**لستلا ةلتك** ضرعي ببسلا دومع.

قيبطتلا مقر ةطساوب رورملا ةكرح رظح :3 ويرانيسلا

ةدعاق دجوت ال ەنأ ريغ .cnn.com رظح متي ەنأ نع نومدختسملا غلبي ،ويرانيسلا اذه يف **- ميامحلا رادج** جارخإ عم نارتقالاب ،لاصتالا ثادحأ رەظت .نا نا يسلا عنمت ةددحم - engine-debug، رظحلا ببس.

لوح تامولعم رەظت قىيبطتال لوقح راوچب تامولعم عبرم ىلع "لاصتالا ثادحاً" يوتحت ،الوأ فينصت ةيفيك ىلإ ةفاضإلاب قىبطتال FirePOWER فينصت قيفيك ىلإ ةفاضإلاب قىبطتال

▼ First Pac	<u>ket</u> ×	Last × Packet	Action ×	Initiator IP ×	Responder × IP	Source Port / × ICMP Type	Destination Port / X ICMP Code	Application × Protocol	Web X Application	Application × Risk	Business × Relevance	<u>URL</u> ×
2017-05-19	16:02:29		Block	192.168.62.63	151.101.65.67	54308 / tcp	80 (http) / tcp	п нттр	CNN.com	Medium	Medium	http://cnn.com/
	CN Tur	N.com	sting Syste	m's news website	3.			1				
	тур	e		Web	Application							
	Ris	k		Ver	y Low							
	Bus	siness Rele	vance	High	n							
	Cat	egories		mul	timedia (TV/vide	o), news						
	Тас	IS		disp	lays ads							
		dades Contex	kt Explorer	W Wikipedia	G Google	Y Yahoo!	b Bing					

يف .**ءاطخألا حيحصت-كرحملا-ةيامحلا رادج** ليغشت متي ،رابتعالا يف تامولعملا هذه عضوب قيبطتال قمالع يلإ ادانتسا رورملا ةكرح رظح متي ،ءاطخألا حيحصت جارخإ.

192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 New session
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://cnn.com/") returned 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0(0) -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 1190, client 638, misc 0, user 9999997, url http://cnn.com/, xff
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 match rule order 4, 'block by tag', action Block
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 sending block response of 605 bytes
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Deleting session

ضرعلا تانالعاٍ رظح متي ،<u>http://cnn.com</u> حيرص لكشب عنمت ةدعاق دوجو مدع نم مغرلا ىلع مالع متي ،ACP قدعاقل **تاقيبطت** بيوبتلا ةمالع لخاد اهيلع قمالع عضو مت يتلا

Editing	Rule - block l	by tag												? >
Name	block by tag					🕑 Enabl	led	1	love					
Action	💢 Block with res	et			▼ ∪ ∩ 2 t	- -								
Zone	s Networks	VLAN Tags	🛆 User	rs	Applications	Ports	URLs	SGT/ISE At	tributes			Inspection	Logging	Comments
Applica	tionFilters 🗳	Clear All	Filters 💢		Available Applicat	ions (759	9) C				Selecte	d Applications	and Filters	(1) 🔏 📩 😳
🔍 Sea	rch by name				Search by name	e					Filters			
			19	1	enercogea.			¥ .			🛃 Taos	: displays ads		8
	🛛 💽 blog		53		ClickTale									9
	🔣 bundles softwa	are	7		Clip2Net									
	🔣 business impa	ict	44		Clip2Net Upload	1								
	🛛 💽 Common Indu	strial Protocol	1		CloudFlare									
E	🔣 console gamin	ıg	25		CNBC									
	🔣 content provid	ier	28		CNET									
	🔣 decrypted traf	fic	21		CNET TV									
	🛛 💽 displays ads		759		CNN.com					Rule				
	🔣 eDonkey		2		CNTV			ñ						
E	🛛 🔄 encrypts comr	munications	280		CN77									
E	🛛 💽 evasive		58		Cognitive Match									
E	🛛 💽 Facebook		27											
	🛛 🔝 Facebook gam	ie	23					0						
	🛛 🔝 Facebook post	:	7		Collider			0						
	🔣 file sharing/tra	ansfer	249		Comcast			0						
	🔣 Flash		39		Comedy Centra	1								
E	TP protocol		11		Commission Jur	nction		0 -						
	🗔 Gnutella proto	col	••• •		Viev Viev	wing 101-20	00 of 759							
													Save	Cancel

TAC ىلإ اەمېدقت متېس يتلا تانايبلا

تاناىبلا تامىلعت ءاطخأ فاشكتسأ زامج نم امحاًلصاو فلملًا <u>http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/</u> موقي يذل FirePOWER رورملا ةكرح صحفب **-كرحملا-ةيامحلا رادج** جرخ معدو ءاطخألا حيحصت تاميلعت ىلع لوصحلل ةلاقملا هذه علاط trtrace-ماظنUI ةسايس ريدصت رولا يف مكحتلا ةسايس ددح ،**ريدصت / داريتسإ < تاوداً < ماظن** ىلإ لقتنا لوصولاب مكحتلا

مقف ،SSL ةسايس يلع يوتحت (ACP) لوصولا يف مكحتلا ةمئاق تناك اذإ :**ريذحت** بنجتل ريدصتلاا لبق (ACP) لوصولاا يف مكحتلا ةمئاق نم SSL ةسايس ةلازاب ةساسحلا PKI تامولعم نع فشكلا

اهحالصإو SSL جەن ةقبط ءاطخأ فاشكتسأ :ةيلاتلا ةوطخلا

نع لوصولا يف مكحتلا جهن ءاطخاً فاشكتٍساً فشكي ٍملو مادختسالا ديق SSL جهن ناك اذاٍ .آەحالصاو SSL جەن ءاطخأ فاشكتسا يە ةيلاتلا قوطخلا ناف ،قلكشملا

ةيلاتان القرارية القرارية التراكي الترايية.

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