تانايب راسم ءاطخأ فاشكتسأ نم 1 ةلحرملا ةمزحلا لخدم :اهحالصإو Firepower

تايوتحملا

ەمدقملا

يف تانايبلا راسم فاشكتساً ةيفيك حضوت تالاقم ةلسلس نم ءزج يه ةلاقملا هذه رثؤت دق FirePOWER تانوكم تناك اذإ ام ديدحتل يجهنم لكشب اهحالصإو FirePOWER ةمظناً ةينب لوح تامولعم ىلع لوصحلل <u>"قماع قرظن" ةلاقم</u> ىلإ عوجرلا ىجري .رورملا ةكرح ىلع تانايبلا تاراسم ءاطخاً فاشكتساً" تالاقمب اهتاطابتراو FirePOWER ةيساسألا ةمظنالا .ىرخالا "اهحالصإو

تانايب راسم ءاطخأ فاشكتسأ نم ىلوألا ةلحرملا ىلع ةرظن يقلنس ،لاقملا اذه يف FirePOWER .ةمزحلا لوخد ةلحرم يهو ،امحالصإو FirePOWER



تاصنملا ليلد

ةلاقملا هذه اهيطغت يتلا تاصنملا يلاتلا لودجلا فصي.

زمر مسا ماظنلا يساسألا	فصولا	ںٻاق قيٻطتلل ةمظنألا ةزەجألا قىساسأليا	تاظحالم
SFR	ASA ةدحو تيبثت عم FirePOWER Services (SFR) اةيطمنلا.	ASA- ةلسلس 5500-X	رفوتم ريغ

FTD فالخب) SSP و FPR-2100)	ةروص Firepower Threat Defense (FTD) ةروص فيكتلل لباق نامأ زاهج ىلع ةتبثملا يضارتفا يساسأ ماظن وأ (ASA)	ةلسلس ASA- ةمظنأ ،X-5500-X ةيرهاظلا NGFW	رفوتم ريغ
FTD (SSP)	ةعرسلا قئاف لاسرالا جمانرب تيبثت مت ىلع مئاق لكيه ىلع يقطنم زاهجك (FTD) ليغشتلل لباقلا ليغشتلا ماظن (FXOS) Firepower	و FPR-9300 و FPR-4100 FPR-2100	مدختست ال 2100 ةلسلسلا جمانرب FXOS Chassis Manager

اهحالصإو ةمزحلا ىلإ لوخدلا ةلحرم ءاطخأ فاشكتسأ

تايلمع يأ ثودح مدع نم دكأتلاا يه امحالصاو تانايبلا راسم ءاطخأ فاشكتسأ تاوطخ ىلوأ دعب ،لخدت ال امنكلو لخدت ةمزحلا تناك اذإ .ةمزحلا ةجلاعمل جورخلا وأ لوخدلا ةلحرم يف طاقسإ راسم لخاد ام ناكم يف زامجلا نم امطاقسإ متي ةمزحلا نأ نم ادكأتم نوكت نأ كنكمي كلذ (دوقفم ARP لخدم ،لاثملا ليبس ىلع) جورخلا ةمزح ءاشنإ ىلع رداق ريغ زامجلا نأ وأ تانايبلا

ةينعملا رورملا ةكرح ديدحت

يف نمضتي تاهجاولاو قفدتلا لزعي نأ ةلحرم لخدم طبرلا ىرحتي يف ىلوألا ةوطخلا يلي ام كلذ لمشيو .رورم ةكرح ةلكشملا:

ةەجاولا تامولعم قڧدتلا تامولعم

لوكوتوربال لوخدلا ةمجاو ردصملا IP ناونع ردصملا ذفنم جورخلا ةمجاو عانيم ةياغ

:لاثملا ليبس ىلع

TCP inside 172.16.100.101:38974 outside 192.168.1.10:80

يف افلتخم نوكي ام ابلاغ ەنأل ةقدب ردصملا ذفنم ديدحت نم نكمتت ال دق :**حيملت** ايفاك (مداخلا) ةەجولا ذفنم نوكي نأ بجي نكلو ،قفدت لك.

لاصتالا ثادحأ نم ققحتلا

كلذكو ةقباطم رورملا ةكرح نوكت نأ بجي جورخلاو لوخدلا ةمجاو نع ةركف ىلع لوصحلا دعب ققحتلا يه قفدتلا عنمي FirePOWER ناك اذإ ام ديدحتل ىلوألاا ةوطخلاو ،قفدتلا تامولعم قرادإ زكرم يف رصانعلا هذه ضرع نكميو .ةينعملا رورملا ةكرحل لاصتالا ثادحأ نم **ثادحاً < تالااصتا < ليلحتل** عباتلا

جەن دعاوق يف ليجستلا نيكمت نم دكأت ،لاصتالا ثادحاً نم ققحتلا لبق :**قظحالم** لك لخاد "ليجستلا" بيوبتلا ةمالع يف ليجستلا نيوكت متي .لوصولا يف مكحتلا تامولعم" بيوبتلا ةمالع ىلإ ةفاضإلاب لوصولا يف مكحتلا ةسايس دعاوق نم ةدعاق ."ثادحالا ضراع" ىلإ تالجسلا لاسرإل مەب ەبتشملا دعاوق نيوكت نم دكات ."نامالا

Overvi	ew Expl	Analysis Policioner Connectio	ies Devices Obje ns • Events Intro	ects /	AMP Inte Files ▼	Higence Hosts • User	s • Vuln	erabilities • Corr	elation 🔹 🛛	Custorn • Loo	kup • Search			Deploy 2	🦺 System Help 🛪 🤇	ilobal ∖ admin +			
Connect No Sear	Connection Events (residue sociality) Table View of Connection Events																		
Jump	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 0	2	017-05-11 14:54:32	2017-05-11 14:55:02	Allow		192.168.1.200		13.173.197.235	JUSA			60084 / tcp	80 (http) / tcp	HTTP	Web browser	Web Browsing			
4	20	017-05-11 14:54:02	2017-05-11 14:54:32	Allow		192.168.1.200		73.173.197.235	USA			60082 / tcp	80 (http) / tcp	HTTP	Web browser	Web Browsing			
4.0	20	017-05-11 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	Eomao				
1	20	17-05-11 14:52:40	2017-05-11 14:52:55	Allow		192.168.1.200		10.83.181.139				60069 / tcp					-		
1.0	2	17.05.11 14:51:40	2012-05-11 14:51:52	Allow		102 168 1 200		10.83 181 139				60064 / http	Connection Events	8	(unnamed search)		Private	Save Save As New Search	4
	; 60 ; 20	17.05.11.14.51.34	2017-02-11 14-21-24	All series				10000000000000				60050 / http	Sections		Networking				
•		017-05-11 14:51:24	2017-05-11 14:51:24	Allow		M 192.168.1.200		172.217.26.206	<u>USA</u>			500587 tcp	General Information		Initiator IP+	192.168.1.200		192.168.1.0/24, 1192.168.1.3, 2001:08:8	
4 C	2	017-05-11 14:50:40	2017-05-11 14:50:55	Allow		# <u>192.168.1.200</u>		H 10.83.181.139				60056 / tcp	Networking		Responder 1P*			192.168.1.0/24, 1192.168.1.3, 2001:db8:8	
4 0	2	017-05-11 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*		*	192.168.1.0/24, 1192.168.1.3, 2001:db8:8	4.
4	2	017-05-11 14:50:23	2017-05-11 14:50:53	Allow		192.168.1.200		73.173.197.235	USA			60051 / tcp	Stil.		Initiator / Responder IP Initiator / Original Client IP			192.168.1.0/24, 1192.168.1.3, 2001.088.8	4
4	20	17-05-11 14-49-47	2012-05-11 14:49:47	Allow		192 168 1 200		172 217 26 206	IN USA			60043 / tro	Application		Initiator / Responder / Original Cle	rit IP		192.168.1.0/24, 1192.168.1.3, 2001-058-8	4
				CHINE					A REAL PROPERTY			222 12 1 Ske	URL		Ingress Security Zone			My Security Zone	4
•		017-05-11 14:49:40	2017-05-11 14:49:55	Allow		192.168.1.200		10.83.181.139				60046 / tcp	Netflow		Egress Security Zone			Hy Security Zone	J.
4 C	2	017-05-11 14:48:46	2017-05-11 14:51:23	Allow		192.168.1.200		72.246.56.139	M USA			60041 / tcp	Quố		Ingress / Egress Security Zone			My Security Zone	
4 0	23	017-05-11 14:48:46	2017-05-11 14:49:16	Allow		192.168.1.200		1173.197.235	💶 USA			60040 / tcp			Destination Part / ICMP Code*			1-1024, 6000-6011, 180	
4	20	017-05-11 14:48:40	2017-05-11 14:48:55	Allow		192.168.1.200		10.83.181.139				60037 / tcp			Protocol*			tcp, wdp	
		12.05.11 14.48.32	2012-05-11 14-48-32	Allow		102 168 1 200		172 217 26 206	DE LICA			60031 / http	Clobal		DNS Query			suspicious.com, evil*	
	1	117-02-11 14:40.32	2017-02-11 14:40:32	PALIN IN		192.100.1.200		MB 172.217.20.200	<u></u>			200247.00	SuperConnectionTest		DNS Response			NKDOMAEN	
- 4 - C	2	017-05-11 14:48:16	2017-05-11 14:48:46	Allow		H 192.168.1.200		B 73.173.197.235	usa usa			600.34 / tcp	Predefined Searches		DNS Record Type			43200	
- 4 - C	2	017-05-11 14:47:46	2017-05-11 14:48:16	Allow		192.168.1.200		73.173.197.235	SA USA			60030 / tcp	Malicious URLs		DNS Sinkhole Name			Ny Sinkhole	
4	2	017-05-11 14:47:40	2017-05-11 14:47:55	Allow		192.168.1.200		10.83.181.139				60027 / tcp			HTTP Response Code			200	
4.0	2	017-05-11 14:47:15	2017-05-11 14:48:46	Allow		192.168.1.200		72.246.56.169	USA			60022 / tcp	Relevance		VLAN ID			10	
1	20	17-05-11 14:47:15	2017-05-11 14:47:45	Allow		192.168.1.200		73.173.197.235	USA			60021 / tcp	Standard HTTP		Geolocation				
				All of the local division of the local divis								10010 (100			Initiator Country			USA, United States, United*	
•	2	117-05-11 14:46:45	2017-05-11 14:47:15	Allow		192.168.1.200		m /3.1/3.197.235	sau usa			bouly / tcp			Responder Country			USA, United States, United*	
Last look	1 on Tu	esday, 2017-04-25 at 1	12:42:21 PM from rtp-flipk	ev-88111.4	lisco.com										Initiator / Responder Country			USA, United States, United*	
_																			

ئدابلا) ديرف ردصمل IP ةفاضإ متيو "ثحبلا ريرحت" قوف رقنلا متي ،هالعأ لاثملا يف دومع رهظي .FirePOWER ةطساوب اهفاشتكا مت يتلا تاقفدتلا ةدهاشمل ةيفصت لماعك هذه فيضملا رورم ةكرحل "حامسلا" ءارجإلا.

تناك اذإ FirePOWER تفرك يلع ءارجإلا يوتحي ،دصق نع رورملا ةكرح عنمت FirePOWER تناك اذإ لوقحلا ةظحالم نكمي .تانايبلا نم ديزم ريفوت يلإ "لاصتالا ثادحأ لودج ضرع" قوف "رظح" وه ءارجإلا ناك اذإ "لاصتالا ثادحاً" يف ةيلاتلا

ببسلا -

لوصولاب مكحتلا ةدعاق -

يذلا نوكملا قييضت يف ،ينعملا ثدحلا يف ىرخألا لوقحلاب انرتقم ،كلذ دعاسي نأ نكمي رورملا ةكرح قيعي.

اهحالصإو لوصولا يف مكحتلا دعاوق ءاطخأ فاشكتسأ لوح تامولعملا نم ديزم ىلع لوصحل. <u>انه</u> رقنلا كنكمي.

جورخلاو لوخدلا تاهجاو ىلع مزحلا طاقتلا

ثادحاً نأ نم مغرلا ىلع FirePOWER عنم يف هابتشالا رارمتسا وأ ثادحاً دوجو مدع ةلاح يف تانايبلا راسم ءاطخاً فاشكتساً رمتسي ،"ةقثلا" وأ "حامسلا" ةدعاق ءارجاٍ ضرعت لاصتالا اهحالصإو.

ةيساسألاا ةمظنألاا فلتخم ىلع جرخمو لخدم ةمزح طاقتلاا ليغشت ةيفيك لوح تاميلعت انه العاً ةروكذملا:

ASA تاہجاو یلع طاقتلا - SFR

متي نأ لضفألاا نمف ،ASA ةيامح رادج ىلع لمعت ةيطمن ةدحو درجم ةيطمن SFR قدحو نأ امب لخدت يتلا اهسفن مزحلا نأ نم دكأتلل ASA لا نم جورخلاو لوخدلا تاهجاو ىلع الوأ طاقتلالا لخدت اضيأ.

.ASA ىلع طاقتلالاا تايلمع ذيفنت ةيفيك لوح تاميلعت ىلع <u>قلاقملا</u> هذه يوتحت

يف ةيلاتانا ةلحرملا يف رمتسا ،ةجردم ريغ ASA ىلع يوتحت يتلا مزحلا نأ ديدحت مت اذا ملحرم) امحالصاو ءاطخألا فاشكتسأ (DAQ

نم ققحتلا ديفملا نم نوكي دقف ،ASA لخدم ةهجاو ىلع مزحلا ةيؤر مت اذإ :**قظحالم** ةلصتملا ةزهجألا.

جورخلاو لوخدلا تاهجاو ىلع طاقتلا - (FPR-2100 و SSP ريغ) FTD

رماوأ ليغشت كنكمي ،كلذ عمو .ASA ىلع طاقتلالا SSP ريغ FTD زامج ىلع طاقتلالا لثامي ةطقسملا مزحلا ءاطخأ فاشكتسأ دنع .ةيلوألا CLI ةبلاطم ةذفان نم ةرشابم طاقتلالا طاقتلالا ىلإ "عبتتلا" رايخ ةفاضإب ىصوي ،امحالصإو.

:22 ءانيم ىلع رورم ةكرح TCP ل طاقتلاا لخدم لكشي نم لاثم انه

> capture <u>ssh_traffic</u> trace interface inside match <u>tcp</u> any any <u>eq</u> 22 > show capture <u>ssh_traffic</u>
7 packets captured
1: 01:17:38.498906 192.168.62.70.48560 > 10.83.180.173.22: S 4250994241:4250994241(0) win 29200 ⊲ <u>mss.</u>
2: $01:17:38.510898$ 10.83.180.173.22 > 192.168.62.70.48560: S 903999422:903999422(0) ack 4250994242 win
3: 01:17:38.511402 192.168.62.70.48560 > 10.83.180.173.22: . ack 903999423 win 229 < <u>nop.nop.timestamp</u>
4: 01:17:38.511982 192.168.62.70.48560 > 10.83.180.173.22: P 4250994242:4250994283(41) ack 903999423 win
5: 01:17:38.513294 10.83.180.173.22 > 192.168.62.70.48560: . ack 4250994283 win 140 < <u>nop.nop.timestamp</u>
6: 01:17:38.528125 10.83.180.173.22 > 192.168.62.70.48560: P 903999423:903999444(21) ack 4250994283 win
140 <nop.top.timestamp 1045829957="" 513898282=""> 7: 01:17:38.528613 192.168.62.70.48560 > 10.83.180.173.22: . ack 903999444 win 229 <nop.nop.timestamp< td=""></nop.nop.timestamp<></nop.top.timestamp>
140 < <u>nop.nop.timestamp</u> 513898282 1045829957> 7: 01:17:38.528613 192.168.62.70.48560 > 10.83.180.173.22: . <u>ack</u> 903999444 win 229 < <u>nop.nop.timestamp</u> 1045829961 513898282>

ماظنلاا لالخ بقعتلل ةيدرف ةمزح ديدحت ذئدنع كنكميف ،"عبتتلا" رايخ ةفاضإب تمق اذا تاليدعتلا متي نأ نمضي نأ اضيأ دعاسي وهو .يئاهنلا مكحلا ىلإ لوصولا ةيفيك ةفرعمل ترتخأ بسانم جرخملا نأو ليدعت (NAT) ةمجرت ناونع ةكبش لثم طبرلا ىلإ ةبسانملا .نراق > show capture ssh_traffic packet-number 4 trace 7 packets captured 4: 01:17:38.511982 192.168.62.70.48560 > 10.83.180.173.22 4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp 192.168.62.70.48560 > 10.83.180.173.22: P 1045829957 513898266> Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list Phase: 3 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found flow with id 626406, using existing flow Phase: 4 Type: EXTERNAL-INSPECT Subtype: Result: ALLOW Config: Additional Information: pplication: 'SNORT Inspect Phase: 5 Type: SNORT Subtype: Result: ALLOW Config: Additional Information: Snort Trace: Packet: TCP, ACK, seg 4250994242, ack 903999423 AppID: service SSH (846), application unknown (0) Firewall: starting rule matching, zone 1 -> 2, geo 0 -> 0, vlan 0, sgt Firewall: Starting rule materials of a composed of the starting rule material of the start of th trust/fastpath rule, id 268435458, allow IPS id 0, Verdict WHITELIST ict: (fast-forward) fast forward this flow 1, I Verdi esult: nput-interface: inside nput-status: up nput-line-status: up : allow ction

متو حامس مكح اريخاً غلب هنا و رخشلا صحف ىلإ لصويب رورملا نا دهاشن هالعا لااثملا يف نأ نم دكأتف ،نيهاجتالا الك يف اهتيؤر نكمي رورملا ةكرح نأ امب .زاهجلا ربع يلامجالا ريرمت طاقتلا ىلإ ةجاح كانه نوكي ال دق كلذل ،ةسلجلا هذهل زاهجلا لالخ نم قفدتت رورملا ةكرح وه امك حيحص لكشب ءوست رورملا ةكرح نأ نم دكأتلل اضيأ كانه دحاو ذخأ كنكمي نكل ،جرخم .

نكل "حمسي" عبتتلا ءارجإ لظي ،جورخلا ةمزح ءاشنإ ىلع رداق ريغ زاهجلا ناك اذإ :**قظحالم** ةياغلل عئاش ويرانيس اذه .جرخملا ةهجاو طاقتلا ىلع اهتيؤر وأ قمزحلا ءاشنإ متي مل ريخألا اذه ناك اذإ) ةهجولل IP ناونع وأ ةيلاتلا ةوطخلل ARP لاخدا ىلع TD يوتحي ال ثيح (ةرشابم لصتم.

ةيقطنملا FTD تاهجاو ىلع طاقتلا - (SSP) - تاهجاو

ماظن ىلع ەالعأ روكذم وە امك FTD ىلع ةمزح طاقتلاا ءاشنإل اەسفن تاوطخلاا عابتا نكمي قيقطنملا FTD ةەجاوب صاخلا IP ناونع يف SSH مادختساب لاصتالا كنكمي .يساسألا SSP يلاتلا رمألا لاخداو :

```
Firepower-module1> connect ftd
```

مادختساب FXOS رماوأ هجوم نم FTD يف يقطنملا زاهجلا ةقبط ىلإ لاقتنالا اضيأ كنكمي ةيلاتا رماوألا:

connect module 1 console
Firepower-module1> connect ftd
>

نامألا ةدحو بسح ةيطمنلا ةدحولا مقر فلتخي نأ نكمي ،FirePOWER 9300 مادختسإ قلاح يف ةيقطنم ةزهجأ 3 يلإ لصي ام تادحولا هذه معدت نأ نكمي .اهمادختسإ متي يتلا.

رمألا يف ليثملا فرعم نيمضت بجيف ،مادختسالا ديق ةددعتم تاليثم كانه تناك اذإ "سفن يف ةفلتخملا تاليثملاب لاصتالل Telnet جمانرب رما مادختسإ نكمي ."connect". تقولا

connect module 1 telnet
Firepower-module1>connect ftd ftd1
Connecting to container ftd(ftd1) console... enter "exit" to return to Boot CLI
>

ةەجاولا ءاطخأ نم ققحتلا

نوكي نإ ةصاخ اذه ديفي .ةلحرملا هذه ءانثأ ةهجاولا ىوتسم لكاشم نم ققحتلا اضيأ نكمي ديفملا نم نوكي دقف ،ةهجاولا يف ءاطخأ ترهظ اذإ .طاقتلا نراق لخدملا يف دوقفم طبر .ةلصتملا ةزهجألا نم ققحتلا

ASA تاەجاو نم ققرتالا - ASA

نم ققحتلا متي هنإف ،ASA ىلع لمعي يرهاظ زاهج اساساً يه (FirePOWER (SFR قدحو نأ امب نم ققحتلا لوح ةيليصفت تامولعم ىلع لوصحلل .ءاطخاً نع اثحب ةيلعفلا ASA تاهجاو مذه ASA ةلسلسل رماوألا عجرم ليلد <u>مسق</u> عجار ،ASA ىلع ةهجاولا تايئاصحإ.

ةەجاولا ءاطخأ نم ققحتلا - (FPR-2100 و SSP فالخب) FTD

زاربإ متي .يلوألا رمألا هجوم نم show interface < رمألا ليغشت نكمي ،SSP ريغ SSP قزهجأ ىلع رمحألا نوللاب مامتهالل ةريثملا تاجرخملا.



ةەجاولا ءاطخأ نع ثحبلل تانايبلا راسم يف لقنتلا - (SSP) FTD

.الوأ مزحلا جلاعي يلخاد ينيب ينيب لاصتا 4100 و 9300 ةيساسألا SSP ةمظنأ نمضت



متي يتلا رماوألا يه هذه .لخدم يلوأ طبرلا يف رادصإ نراق يأ كانه نإ ققحتي نأ قحتسي تامولعملا هذه ىلع لوصحلل FXOS ماظنل (CLI) رماوألا رطس ةهجاو ىلع اهليغشت.

ssp# scope eth-uplink ssp /et-uplink # show stats تاجرخملل جذومن اذه.

ssp# scope eth-uplink ssp /eth-uplink # show stats Ether Error Stats: Time Collected: 2017-05-15T14:13:46.032 Monitored Object: fabric/lan/A/pc-44/err-stats Suspect: No Rev (errors): 0 Align (errors): 0 Align (errors): 0 Younder Size (errors): 0 Under Size (errors): 0 Under Size (errors): 0 Int Mac Tx (errors): 0 Int Mac Tx (errors): 0 Deferred Tx (errors): 0 Thresholded: Xmit Delta Min Time Collected: 2017-05-15T14:13:46.032 Monitored Object: fabric/lan/A/pc-48/err-stats Suspect: No Rev (errors): 0 Align (errors): 0 Vinder Size (errors): 0 Under Size (errors): 0 Under Size (errors): 0 Int Mac Tx (errors): 0 Under Size (errors): 0 Int Mac Tx (errors): 0 Monitored Tx (errors): 0 Int Mac Tx	Ether Loss Stats: Time Collected: 2017-05-15T14:13:46.032 Monitored Object: fabric/lan/A/pc-44/loss-stats Suspect: No Single Collision (errors): 0 Multi Collision (errors): 0 Carrier Sense (errors): 0 Symbol (errors): 0 SQE Test (errors): 0 Excess Collision (errors): 0 Time Collected: 2017-05-15T14:13:46.032 Monitored Object: fabric/lan/A/pc-48/loss-stats Suspect: No Single Collision (errors): 0 Multi Collision (errors): 0 Carrier Sense (errors): 0 Carrier Sense (errors): 0 Giants (errors): 0 Symbol (errors): 0 SQE Test (errors): 0 Excess Collision (errors): 0 Thresholded: 0

ىلإ كلذ دعب اەلاسرا متي ،لوخدلا دنع ةمزحلا ةجلاعمب ينيبلا ةينبلا لاصتا موقي نأ دعب FTD. زاہج فيضتسي يذلا يقطنملا زاہجلل اەنييعت متي يتلا تاہجاولا

:عجرملل ينايب مسر انه



ةيلاتلا رماوألا لخدأ ،ةەجاولا ىوتسم ىلع لكاشم يأ دوجو نم ققحتلل:

ssp# connect fxos ssp(fxos)# show interface Ethernet 1/7 (رمحألاب ةزربم قلمتحم لكاشم) تاجرخملا ىلع لاثم اذه):

ssp# connect fxos

ssp(fxos)# show interface Ethernet 1/7 Ethernet1/7 is up **Dedicated Interface** Hardware: 1000/10000 Ethernet, address: 5897.bdb9.4080 (bia 5897.bdb9.4080) **Description: U: Uplink** MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec reliability 254/255, txload 1/255, rxload 1/255 [...Omitted for brevity] Last link flapped 14week(s) 4day(s) Last clearing of "show interface" counters never 2 interface resets 30 seconds input rate 1352 bits/sec, 1 packets/sec 30 seconds output rate 776 bits/sec, 1 packets/sec Load-Interval #2: 5 minute (300 seconds) input rate 728 bps, 0 pps; output rate 608 bps, 0 pps RX 3178795 unicast packets 490503 multicast packets 1142652 broadcast packets 4811950 input packets 3354211696 bytes 0 jumbo packets 0 storm suppression bytes 0 runts 0 giants 0 CRC 0 no buffer 44288 input error 0 short frame 44288 overrun 0 underrun 0 ignored 0 watchdog 0 bad etype drop 0 bad proto drop 0 if down drop 0 input with dribble 306404 input discard 0 Rx pause ТΧ 1974109 unicast packets 296078 multicast packets 818 broadcast packets 2271005 output packets 696237525 bytes 0 jumbo packets 0 output errors 0 collision 0 deferred 0 late collision 0 lost carrier 0 no carrier 0 babble 0 output discard 0 Tx pause

.اضيأ ةهجاو ءاطخأ نع اثحب يلعفلا FTD جمانرب نم ققحتلا نكمي ،ءاطخأ يأ ترهظ اذإ



رماوألا رطس ةمجاو رماوأ مجوم ىلإ لاقتنالا الوأ يرورضلا نم FTD، رماوأل مجوم ىلإ لوصولل (CLI) رماوألا رطس قمجاو رماوأ مجوم ىل

connect module 1 console
Firepower-module1> connect ftd
>show interface
:öددعتملا تالىثملل قبس نلاب

connect module 1 telnet Firepower-module1>**connect ftd ftd1** Connecting to container ftd(ftd1) console... enter "exit" to return to Boot CLI > د.تاجرخملا یلع لائم

# connect module 1 console	
Firepower-module1> connect ftd	
> show interface InterfaceGigabitEthernet0/0 "outside", is up, line protocol is up Hardware is i82545EM rev01, BW 1000 Mbps, DLY 10 usec Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps) Input flow control is unsupported, output flow control is off MAC address 000c.2961.f78b, MTU 1500 IPS Interface-Mode: inline, Inline-Set: InlineSet IP address unassigned 20686130 packets input, 8859847035 bytes, 0 no buffer Received 0 broadcasts, 0 runts, 0 giants 2312 input errors, 0 CRC, 0 frame, 12313 overrun, 0 ignored, 0 abort 0 pause input, 0 resume input 0 L2 decode drops 6485096 packets output, 1480276815 bytes, 0 underruns 0 pause output, 0 resume output 1341 output errors, 45635 collisions, 1 interface resets 0 late collisions, 0 deferred 0 input reset drops, 0 output reset drops input queue (blocks free curr/low): hardware (509/362) output queue (blocks free curr/low): hardware (511/415) Traffic Statistics for "outside": 20686131 packets input, 8485139715 bytes 64485096 packets output, 1375761699 bytes 4702172 packets dropped 1 minute input rate 2 pkts/sec, 78 bytes/sec 1 minute output rate 0 pkts/sec	
5 minute output rate 1 pkts/sec, 319 bytes/sec	

ةينقتلا ةدعاسملا زكرم ىلإ اهميدقت متيس يتلا تانايبلا (TAC) نم Cisco

تانايٻلا تاطقل	تاميلعت
ثدح ةشاش لاصتالا	تاميلعت ىلع لوصحلل ةلاقملا ەذە علاط
جارخإ 'show interface'	تاميلعت ىلع لوصحلل ةلاقملا ەذە علاط
طاقتلا مزحلا	يلإ قبسنلاب ASA/LINA: <u>https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-generation-firewalls/1180</u> generation-firewalls/1180 Firepower: <u>http://www.cisco.com/c/en/us/support/docs/security/sourcefire-fire</u> appliances/11777
جرخ ASA "show tech"	ىلإ لوخدلا ليجستب مق ASA CL ىل لوخدلا ليجستب مق ىل قيف تيفرطلا لمعلا تسليج جارخ فل مريفوتب مق مث رمألا اذه مادختساب يجراخ نيزخت ماظن وأ صرقلا ىلع فلملا اذه ظفح نكمي. show tech ميجوت قداع 0:/show_tech.log
فاشكتسأ ءاطخأ فلملا اهحالصإو زامج نم FirePOWER موقي يذلا صحفب	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn

رورملا ةكرح

ب ةصاخلا DAQ ةقبط ءاطخأ فاشكتسأ :ةيلاتلا ةوطخلا FirePOWER اهحالصإو

زامج زواجت نكميف ،ال مأ مزحلا طاقسإب موقي FirePOWER زامج ناك اذإ ام احضاو نكي مل اذإ كلذ نوكيو .تقولاا سفن يف FirePOWER تانوكم عيمج داعبتسال مسفن FirePOWER موقت ةينعملا رورملا ةكرح تناك اذإ ام ةلكشم نم فيفختلا يف صاخ لكشب اديفم كلذب موقت ال امنكلو ةيرانلا اقواطلا زامج بيكرتب

تانايب راسم ءاطخأ فاشكتسأ نم ةيلاتان قلحرما قعجارم ءاجرلا ،ةعباتمل FirePOWER تانايب راسم ءاطخاً فاشكتساً نم قيل . قعباتملل <u>انه</u> رقنا .FirePOWER ب صاخلا DAQ يل قفاضإلاب ،امحالصإو

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