# ل ددعتملا ليثملل يلاعلا رفوتلا نيوكت FTD ىلع Firepower 4100

## تايوتحملا

<u>ةمدقملا</u> <u>قيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسماا تانوكماا</u> <u>ةىساسأ تامولعم</u> <u>ةكېشلل ىطىطختلا مسرلا</u> <u>تانىوكتارا</u> <u>اقبسم تاهجاولا نېوكت .1 ةوطخلا</u> <u>.قېواحا، تالېثمل دروم فېرعت تافلم قفاضا .2 قوطخا، </u> .ةيواجل لييثم تاهجاول يرماظ MAC ناونع نم MAC عمجت ةئداب ةفاض ((يرايتخا) .3 قوطخلا <u>لقتسم ليثم ةفاضا .4 ةوطخلا</u>. <u>تامجاولا نېوكت .5 ةوطخلا</u> <u>ليثم لكل رفوتاا يالاع جوز ةفاضا 6. أقوطخاا.</u> <u>قحصاا نم ققحتاا</u> <u>امحال ص او ءاطخأل ا ف اش ك ت س ا</u> <u>عجرملا</u>

## ةمدقملا

ةددعتم) FTD ةيواح تاليثم يف لشفلا زواجت نيوكت ةيفيك دنتسملا اذه حضوي (تاليثملا).

## ةيساسألا تابلطتملا

تابلطتملا

رادجب ديدهتلا دض عافدلاو FirePOWER ةرادإ زكرمب ةفرعم كيدل نوكت نأب Cisco يصوت ةيامحلا.

### ةمدختسملا تانوكملا

Cisco Firepower Management Center Virtual 7.2.5 نم يلاتا ليجلا نم ةيامحلا رادج زاهج Cisco Firepower 4145 (FTD) 7.2.5 ليغشتلا اليغشتار ماظن (FXOS) Firepower 2.12 (0.498) ليغشتلا ماظن Windows 10

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألا 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 ،ليغشتلا ديق كتكبش.

جمانرب رشن لبق FTD Multi-Instance، ماظنلا عادأ ىلع رثؤي نأ نكمي فيك مەف مەملا نم لثمم ىلإ عجرا وأ Cisco نم ةيمسرلا قئاثولا ىلإ امئاد عجرا .كلذل اقفو طيطختلاو كب صاخلا Cisco .نوتلا تاممل

## ةيساسأ تامولعم

قايسلا عضو لثامت يتلاو (FTD ديدهت دض عافدلا ةزيم وه Multi-Instance دعتملا جمانرب نم ةددعتمو ةلصفنم ةيواح تاليثم ليغشت ةيناكما كل حيتت امك ASA ددعتملا ةتباثلا دراوملا لصف ةيواح ليثم لك حيتي .دجاو زامج ىلع (FTD) ةعرسلا قئاف لاسرإلا جماربلا تاثيدحتو ةلصفنملا ليمحتلا ةداعا تايلمعو ةلصفنملا نيوكتلا ةراداو صاخ لكشب اديفم اذه دعيو .ةلماكلا تاديدهتلا دض ةيامحلا ةزيم معدو قلصفنملا اهنكلو ،ةفلتخملا تاعورشملا وأ تارادالل ةفلتخم ناما تاسايس بلطتت يتلا اتاس مؤملل ايل حيث المالال العامي المالي المالي المالي المالي الماري المالي ال

دنتسملا اذه مدختسي Firepower4145 دنتسملا اذه مدختسي دحلل ةبسنلاب .ىصقأ دحك ةيواح ليثم 14 معدي يذلا Firepower4145 دنتسملا اذه مدختسي <u>ىصقألاا دحلا</u> ىلإ عوجرلا ىجري ،FirePOWER Appliance يف ةموعدملا تاليثملا نم ىصقألا <u>جذومن لكل امدراومو قيواحلا تاليثمل.</u>

## ةكبشلل يطيطختلا مسرلا

.ينايب مسر اذه ىلع multi-instance يف HA ل ققحتلاو ليكشتلا ةقيثو اذه مدقي



يقطنملا نيوكتلل يطيطخت مسر



يداملا نيوكتلل يطيطخت مسر

## تانيوكتلا

اقبسم تاهجاولا نيوكت .1 ةوطخلا

أ. لائملا اذه يف 2 mgmt تاهجاو طبض FCM ىلع تاهجاولا ىل لقتنا. وEthernet1/7.

Overview Interface	s Logical Devices	Security Engine	Platform Settings						Syste	m Tools Help	admin
		CONSOLE MGMT	Network Module 1	5 7	Network Module 2 :	Empty	Network Module 3 : Em	pty			
All Internaces naroware	e bypass								Add No	w • Filter.	×
Interface	Туре	Admin Speed	Operational Speed	Instances	VLAN	Admin Duplex	Auto Negotiation	Operation State	Admin State		
MGMT	Management										
Port-channel48	cluster	10gbps	indeterminate			Full Duplex	no	admin-down	()X)	J 6	
Ethernet1/1	data	1gbps	lgbps			Full Duplex	yes	up		ø	
Ethernet1/2	data	1gbps	lgbps			Full Duplex	yes	up		0	
Ethernet1/3	mgmt	1gbps	lgbps			Full Duplex	yes	up		0	
Ethernet1/4	data	1gbps	lgbps			Full Duplex	yes	up		0	
Ethernet1/5	data	1gbps	lgbps			Full Duplex	yes	up		ø	
Ethernet1/6	data	1gbps	lgbps			Full Duplex	yes	up		ø	
Ethernet1/7	mgmt	1gbps	lgbps			Full Duplex	yes	up		ø	
Ethernet1/8	data	1gbps	lgbps			Full Duplex	yes	up		0	

اقبسم تاهجاولا نيوكت

## ةيواحلا تاليثمل دروم فيرعت تافلم ةفاضإ .2 ةوطخلا.

نييعت .FCM ىلع ةفاضإ < دراوملا فيرعت تافلم < يساسألا ماظنلا تادادعإ ىلإ لقتنا .أ لوألا دروملا فيرعت فلم.

: لاثملا اذه يف 10 ليثملا :مسالا' 10 :ىونلا ددع:



فيرعت فلم تامس سفن مدختسي نأ بجي ،ةيواحلا ليثم جوزل ةبسنلاب :ةظحالم دروملا

فلم مسا رييغت كنكمي ال هنأ ظحال .افرح 64 و 1 نيب صيصختلا فلم مسا طبضا هتفاضإ دعب اذه فيرعتلا.

ىصقألاا دحلاو 6 نيب ،صيصختلا فلمل ىونلا ددع طبضا.

Overvie	w Interfaces l	_ogical	Devices Security Engine	Platform Settings		Syste	em Tools	Help admin	
NTP SSH				0 Ad	d]				
SNMP			Name	Description Cores					
AAA			Default-Small	Auto-created application resource-profile with 6 cpu-cores 6	/ 8				
Syslog									
FIPS an	d Common Criteria								
Access	List			Add Resource Profile					
MAC Po	ol			Name:* Instance01					
Resource	rce Profiles								
Chassis	URL			Description:					
0.0000				Number of Cores:* 10 Range: 6 to 86					
				Specify even value for number of cores.					
				OK Cancel					

### .يناثلا دروملا فيرعت فلم نيوكتل ،2 ةوطخلا يف .a ررك .ب

: لاثملا اذه يف 20 ليثملا :مسالا' 20 :زكارملا ددع'

Overview Interfaces Lo	gical	Devices Security Engine	Platform Settings		System	Tools	Help	admin
NTP SSH			[a	Add				
SNMP		Name	Description Cores					
HTTPS		Default-Small	Auto-created application resource-profile with 6 cpu-cores 6	/ 8				
Syslog		Instance01	10	28				
DNS				<b>•</b> 0				
FIPS and Common Criteria			Add Bessures Brafile					
Access List			Add Resource Profile					
MAC Pool			Name:* Instance02					
<ul> <li>Resource Profiles</li> </ul>			Description					
Network Control Policy								
Chassis URL			Number of Cores:* 20 Range: 6 to 86					
			Specify even value for number of cores.					
			OK Cancel					

يناثلا دروملا فيرعت فلم ةفاضإ

### جاجنب اەتفاضإ تمت دراوم صيصخت تافلم 2 صحف .ج.

0	verview Interfaces Log	cal Devices Security Engine Platform Settings		System Tools Help adr	lmin
	NTP				
	SSH		O Add		
	SNMP	Name Description Cores			
	HTTPS	Default-Small Auto-created application resource-profile with 6 cpu-cores 6	28		
	AAA				
	Syslog	Instance01 10	a 🖉 🗊		
	DNS	Instance02 20	28		
	FIPS and Common Criteria	Industrat KA	ø 0		
	Access List				
	MAC Pool				
	Resource Profiles				
	Network Control Policy				
	Chassis URL				

دروملا فيرعت فلم ديكأت

## ليثم تاهجاول يرهاظ MAC ناونع نم MAC عمجت ةئداب فضأ (يرايتخإ) .3 ةوطخلا ةيواحلا.

نييعت متي مل اذإ .ايودي ةيدنتسملا/ةطشنلا ةمجاولل يرماظلا MAC ناونع نييعت كنكمي ءاشنإب ايئاقلت موقي لكيملا نإف ،ةددعتملا تاليثملا ةيناكمإل ، ةيرماظلا MAC نيوانع ناونع مدختست ليثم لك يف ةكرتشملا ةمجاولا نأ نمضيو ،ليثملا تامجاول MAC نيوانع MAC ديرف

<u>قيواحلا ليثم تامجاول MAC نيوانع ضرعو MAC عمجت ةئداب ةفاضا</u> نم ققحتلا ءاجرلا ناونع لوح ليصافتلا نم ديزم يلع لوصحلل MAC.

لقتسم ليثم ةفاضإ .4 ةوطخلا.

.لوألا ليثملا نييعت .لقتسم ةفاضإ < ةيقطنم ةزهجأ ىلإ لقتنا .أ

: لاثملا اذه يف (المجلا مسا: FTD01



قيبطت ليثمل قبسملا رشنلا يه ةيواح قيبطت رشنل ةديحولا ةقيرطلا :ةظحالم ةيواحلا ديدحت نم دكأت .ةيواحلا ىلع ليثملا عون نييعت عم.

يقطنملا زاهجلا ةفاضإ دعب مسالا اذه رييغت كنكمي ال.

Overview Interfaces Logical Devices Security Engine	Platform Settings	System Tools Help admin
Logical Device List	(0 instances) 100% (86 of 86) Cores Available	C Refresh 🕢 Add 🔹
No logical devices available. Click on Add Device to add a new logical device.		
	Add Standalone	
	Device Name: FTD01	
	Template: Cisco Secure Firewall Threat Defense  Timage Version: 7.2.5.208	
	Instance Type: Container	
	Before you add the first container instance, you must reinitialize the security modulereging so that the disk has the correct formatting. You only need to perform this action once.	
	OK Cancel	

ليثم ةفاضإ

### تاهجاولا نيوكت .5 ةوطخلا

.01ليثملل IP ةرادإ ،ةرادإلا ةهجاو ،دراوملا فيرعت فلم نييعت .أ

: لاثملا اذه يف : '00 ليثملا :دروملا فيرعت فلم 'قرادإلا ةەجاو :Ethernet1/3 'ManagementIP: x.x.1.1

Overview Interfaces Logical Devices Security Engine Platform	Settings	System Tools Help admin
Provisioning - FTD01 Standalone   Cisco Secure Firewall Threat Defense   7.2.5.208	Cisco Secure Firewall Threat Defense - Bootstrap Configuration 🖭	Save Cancel
Data Ports	General Information Settings Agreement	
Ethernet1/1 Ethernet1/2 Ethernet1/4 Ethernet1/6 Ethernet1/8	SH 1 - 66 Cores Available Resource Profile: Instance01 Interface Information Management Interface: Ethernet1/3 Address Type: IPv4 Management IP: 1.552.0 Network Mask: 255.0.0 Network Gateway: 1.^^	
Application Version Resource Profile	rt Status	
G FTD 7.2.5.208		
	OK Cancel	
		•

IP ةرادإ/ةرادإلا ةەجاو/فيرعتلا فلم نيوكت

.تانايبلا تاهجاو نييعت .ب

: لاثملا اذه يف

(لخادلل مدختسي) Ethernet1/1'

(ةيجراخلا ءازجألل مدختسي) 2/Ethernet'

(HA طابترال مدختسي) Ethernet1/4'

o	verview Interfaces	Logical Devices Secu	rity Engine Platform Set	ttings				System Tools Help adm
P S	rovisioning - FTD01 tandalone   Cisco Sec	ure Firewall Threat Defense	e   7.2.5.208					Save Cancel
D	ata Ports Ethernet1/1 Ethernet1/2 Ethernet1/5 Ethernet1/6 Ethernet1/6			Ethern Ethern Ethern	et1/1 et1/2 et1/4	Etbernet1/3 Click to configure	8	
	Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status	
	FTD Interface Name Ethernet1/1 Ethernet1/2 Ethernet1/4	7.2.5.208	Instance01	1.100011 Type data data data	1.0	Ethernet1/3		

تانايٻلا تاهجاو نييعت

### ليثملا ليغشت ءدب راظتنا يف .ةيقطنم ةزهجأ ىلإ لقتنا .ج

	Overview	Interfaces	Logical Devices	Security Engine	Platform Setting	<u>a</u> s				System Tools Help admin
Lo	gical Devic	e List		c	1 Container instanc	e) 100% (86 of 86) Cores	Available			C Refresh 🕢 Add •
	FTD01			Standalone	Status:ok					2 I
	Applicat	tion	Version	Resource P	Profile	Management IP	Gateway	Management Port	Status	
	FTD		7.2.5.208	Instance01		1	1.0-0-000	Ethernet1/3	📌 Installing	C 📧 🎼 C 🕍

01ليثملا ةلاح ديكأت

.هل ليصافتلاا نييعتو يناثلاا ليثملا ةفاضإل c ىلإ 5.a ةوطخلاو 4.a ةوطخلا يف .a ررك .د

: لاثملا اذه يف

:FTD11 :زاهجلا مسا ةيواحلا : ليثملا عون

· دروملا فيرعت فلم : دروملا فيرعت فلم : Ethernet1/7 ·ManagementIP: x.x.10.1

یلخاد = Ethernet1/5-

يجراخ = Ethernet1/6·

HA طابترا = Ethernet1/8

.FCM ىلع ةلصتم ةلاح 2 دوجو نم دكأت .ه

Overview	Interfaces	Logical Devices	Security Engine	Platform Settin	gs				System Tools Help admin
Logical Devic	ce List			2 Container instand	ces) 66% (56 of 86) Core	es Available			C Refresh 🔘 Add •
FTD11			Standalone	Status:ok					
Applica	tion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance02	3	10.1	1/0-0-000	Ethernet1/7	Online	🕶 🕅 c 🖄
FTD01			Standalone	Status:ok					/ I
Applica	tion	Version	Resource I	Profile	Management IP	Gateway	Management Port	Status	
B FTD		7.2.5.208	Instance01	]	C: a1.1	1.0	Ethernet1/3	Online	💌 🕅 Cái

يساسألاا زاهجلا يف ليثملا ةلاح ديكأت

f. (إيرايتخا) scope ssa، scope slot 1 رماوألا رطس ةمجاوب ةلصتم قلاح 2 رادصإلاا ىل show app-Instance رمألاو (CLI) ب قصاخلاا (CLI) ب قصاخلاا (CLI) ب قصاخلاا ا

### <#root>

FPR4145-ASA-K9#

scope ssa

FPR4145-ASA-K9 /ssa #

#### scope slot 1

FPR4145-ASA-K9 /ssa/slot #

#### show app-Instance

Application Instance: App Name Identifier Admin State Oper State Running Version Startup Version Deplo Online

7.2.5 208 7.2.5 208 Container No Instance01 Not Applicable None --> FTD01 Instance is Online ftd FTD11 Online

7.2.5 208 7.2.5 208 Container No Instance02 Not Applicable None --> FTD11 Instance is Online

لصتم ةلاحب نيلاثم دوجو ديكأت .يوناثلا زاهجلا ىلع لثملاب مق .ز

Overvi	ew Interfaces	Logical Devices	Security Engine	Platform Setting	gs				System Tools Help admin
Logical [	evice List			(2 Container instanc	<b>xes)</b> 66% (56 of 86) Cor	res Available			C Refresh 🕢 Add •
FTD	12		Standalone	Status:ok					
Ap	plication	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
· FTC		7.2.5.208	Instance02	]		1.	Ethernet1/7	Online	🚾 🌾 c 🕍
FTD	02		Standalone	Status: ok					1
Ap	plication	Version	Resource	Profile	Management IP	Gateway	Management Port	Status	
B FT	,	7.2.5.208	Instance01	]		1.6	Ethernet1/3	Online	💌 🏹 C 🕍

يوناثلا زاهجلا يف ليثملا ةلاح ديكأت

ليثم لكل رفوتلا يلاع جوز ةفاضإ .6 ةوطخلا.

. FMC ىل| تاليثملا ةفاك ةفاض| .FMC ىلع زامج ففاض! < فَرْمَجَالًا علام لقتنا .أ

: لاثملا اذه يف

·ال FTD1 : FTD1\_FTD01 ل 10لي ثم ل ضرع ل مسا، FTD1 : FTD1\_FTD11 ل 20لي ثم ل ضرع ل مسا، FTD2 : FTD2\_FTD02 ل 10لي ثم ل ضرع ل ا مسا، FTD2 : FTD2\_FTD12 ل 20لي ثم ل ضرع ل ا مسا،

#### .FTD1\_FTD01 دادعإ ةروصلا هذه ضرعت



FMC ىلإ FTD ليثم ةفاضإ

### .ةيداع تاليثملا ةفاك نأ نم دكأت .ب

Firewall Manag Devices / Device Man	ement Center Overview Analysis Po agement	licies Devices Objects I	integration			Deploy	Q 📀 🌣 🚱 admin 🕶	dede SECURE
View By: Group	*						Deploy	ment History
All (4) • Error (0)	<ul> <li>Warning (0)</li> <li>Offline (0)</li> <li>Normal (4)</li> <li>D</li> </ul>	eployment Pending (0)	(0) • Snort 3	(4)			Q, Search Device	Add 👻
Collapse All								
Name		Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)								
FTD1_FTD01     1203.1.1 - R0	Snort 3 Ited	Firepower 4145 with FTD	7.2.5	III FPR4145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	1:
<b>FTD1_FTD11</b>	Short 3 Juited	Firepower 4145 with FTD	7.2.5	IIII Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	1
FTD2_FTD02	Short 3	Firepower 4145 with FTD	7.2.5	IIII Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	1
C FTD2_FTD12	Short 3 suted	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com/443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	(D)	11

*FMC* يف ليثملا ةلاح ديكات

#### . لوألا لشفلا زواجت جوز طبض لاع رفوت مَفاضا < مَرْمَجَالا علام لقتنا .

: لاثملا اذه يف

#### مسالا': FTD01\_FTD02\_HA

FTD1\_FTD01 : يساسألاا ريظنلاا



ةيساسأ ةدحوك ةحيحصلا ةدحولا ديدحت نم دكأت :ظطالم.

Firewall Management Center Overview Analysis Po Devices / Device Management	olicies Devices Objects	Integration		Deploy	Q 📀 🌣 📵 admin 🔹	tiste SECURE
View By: Group					Deploy	ment History
All (4) • Error (0) • Warning (0) • Offline (0) • Normal (4) • D	Deployment Pending (0)	(0) • Snort 3 (4)			Q, Search Device	Add 🔻
Collarse All						
Name	Model	Version Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (4)		Add High Availability Pair				
FTD1_FTD01 Snort 3	Firepower 4145 with FTD	Name:* FTD01_FTD02_H4	Base, Threat (2 more)	acp-rule	49	1
FID1_FID11 Short 3     IO 1 - Booted	Firepower 4145 with FTD	Device Type: Firewall Threat Defense	Base, Threat (2 more)	acp-rule	49	1
FTD2_FTD02_Snort.3	Firepower 4145 with FTD	Primary Peer: FTD1_FTD01 v	Base, Threat (2 more)	acp-rule	49	1
PTD2_FTD12_Snort.3     IO.2 - Rooted	Firepower 4145 with FTD	Secondary Peer: FTD2_FTD02 v	Base, Threat (2 more)	acp-rule	Q+	1
		Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.				
		Cancel Continue				

لوألا لشفلا زواجت جوز ةفاضإ

#### .لوألا لشفلا زواجت جوز يف لشفلا زواجت طابترال IP نييعت .د

: لاثملا اذه يف

1/4 تنرثيا : رفوتلا يلاع طابترا

Ethernet1/4 : قلاح اطابت را

192.168.90.1/24 : يساسألا تنرتن إلى الوكوتورب

#### IP : يون الثال ا

Firewall Management Center Overview Analysis	Policies	Devices Objects Integration		Deploy	Q 🙆 🌣 🔞 admin 🕶	dode SECURE
View By: Group +					Depk	syment History
All (4) • Error (0) • Warning (0) • Offline (0) • Normal (4)	Deployment	Pending (0)   Upgrade (0)  Snort 3 (4)			Q, Search Device	Add 🔻
Collapse.All						
Name	Model			Access Control Policy	Auto RollBack	
		Add High Availability Pair	0			
Ungrouped (4)		High Availability Link	State Link			
FTD1_FTD01 Snort 3	Ereccan	Interface:* Ethernet1/4 +	Interface:* Ethernet1/4 +			
		Logical Name:* ha_link	Logical Name:*		47 <sup>2</sup>	× :
FTD1_FTD11 Snort 3	Firepow	Primary IP:* 192.168.90.1	Primary IP:*	acp-rule	43	1:
		Use IPv6 Address	Use IPv6 Address			
FTD2_FTD02_Snort 3	Firepow	Secondary IP.* 192.168.90.2	Secondary IP:*	acp-rule	«9	11
H 4 - HOURG		Subnet Mask:* 255.255.255.0	Subnet Mask:*			
FTD2_FTD12 Snort 3	Firepow	IPsec Encryption		acp-rule	49	11
		Enabled				
		Key Generation: Auto +				
		LAN failover link is used to sync configuration, stated between poers. Selected interface links and eccentricing	ful failover link is used to sync application content			
		sectors press services interact into and encryption	annenge senning an sinninges men.			
			Cancel Add			

لوألا لشفلا زواجت جوزل IP و HA ةەجاو طبض

لشڧلا زواجت ةلاح ديكأت .ه

طشن ،FTD1\_FTD01: Primay'

دادعتسا ، يونات :FTD2\_FTD02

Fire Devis	ewall Management Center Overview Analysis	Policies Devices Object	ts Integratio	n			Deploy Q	👌 🔅 🕲 admin 🔻	ence SECURE
View By:	Group v							Deploy	ment History
All (4)	• Error (0) • Warning (0) • Offline (0) • Normal (4)	<ul> <li>Deployment Pending (0)</li> </ul>	Jpgrade (0)	<ul> <li>Snort 3 (4)</li> </ul>				Q, Search Device	Add 🔻
Collapse All									
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack		
	V Ungrouped (3)								
	FDD1_FDD2_HA High Availability							,	1
	FTD1_FTD01(Primary, Active) Short 3	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4Q		1
	FTD2_FTD02(Secondary, Standby) Short 3 FTD1.1.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com.443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	¢۹		ı
	FTD1_FTD11 Snort 3     Tri-4.10.1 - Routed	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	4D	,	<b>'</b> :
	C FTD2_FTD12 Snort 3 (	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco com 443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	(Q)	,	<b>'</b> 1

لوألا لشفلا زواجت جوز ةلاح ديكأت

f. تانايبلا ةەجاول طشن IP نييعت .⊐اەجاولا < (لاثملا اذه يف) FTD01\_FTD02\_HA قوف رۇنا < قزەجالا ىل∣ لقتنا.

: لائم يا اذه يف Ethernet1/1 (لخادلا يف): 192.168.10.254/24 ·Ethernet1/2 (جراخ): 192.168.20.254/24 ·Ethernet1/3 (يصيخشت): 192.168.80.1/24

.Ethernet1/1 ل طشنلا IP دادعإ ةروصلا هذه ضرعت

Firewall Management Center Devices / Secure Firewall Interfaces	Overview Analysis I	Policies Devices Objects Integration		Deploy Q 🧬 🌣 🔕 admin 🕶 🐝 SECURE
FTD1_FTD01				You have unsaved changes Save Cancel
Summary High Availability Device Routi	ing Interfaces Inline S	Edit Physical Interface	Edit Physical Interface	e allable for use. X
		General IPv4 IPv6 Path Monitoring Advanced	General IPv6 Path Monitoring Advanced	Add Interfaces 💌
Interface	Logi	inside	Use Static IP v	
Ethernet1/1	inside	Management Only	192.168.10.254/24	
© Ethernet1/2	outside	Description:	- eg. 192.0.2.1/200.200.200.128 0f 192.0.2.1/20	
Ethernet1/3	diagnostic			
Ethernet1/4		Mode:		
		Security Zone:		
		inside_zone *		
		Interface ID:		Cancel OK
		Ethernet1/1		
		MTU:		
		1500		
		(64 - 9184) Diama		
		Phoney:		
		Propagate Security Group Text		
		NVE Only:		
		0		
			Cancel OK	

تانايبلا ةەجاول طشن IP نييعت

g. تانايبلا ةهجاول يطايتحالا IP نييعت قولاعلا قحات الا < (لاشملا اذه يف) FTD01\_FTD02\_HA قوف رقن < قزهجألا يل لقتنا.

: لاثملا اذه يف Ethernet1/1 (لخادلا يف): 192.168.10.253/24 ·Ethernet1/2 (جراخ): 192.168.20.253/24 ·Ethernet1/3 (يصيخشت): 192.168.80.2/24

.1/1 تَنْرِثْيٍ! مَتْبَشْلْ يطايتحالاً IP دادعإ ةروصلاً هذه حضوت

Firewall Management Devices / High Availability	Center Overview Analysis Policies Devices	Objects Inte	gration		Deploy	९ 💕 🕯	🌣 🕜 admin 🔻	cisco SECURE
FTD01_FTD02_HA Cisco Firepower 4145 Threat Defense Summary High Availability	e Device Routing Interfaces Inline Sets DHCP VT	ГЕР						Savo Cancel
IPsec Encryption	Edit inside	0	itics					۹
Monitored Interfaces Interface Name	Monitor this interface for failures IPv6 IPv6			Active Link-Local IPv6	Standby Link-	Local IPv6	Monitori	ing
outside	Interface Name:						٥	1
diagnostic	Active IP Address:						٢	/
inside	192.168.10.254 Mask:						0	1
	24 Standby IP Address:							
Failover Trigger Criteria	192.106.10.233		face MAC Add	resses				+
Failure Limit			cal Interface	Active Mac Ac	Idress	Standby M	ac Address	
Peer Poll Time		Cancel	et1/1	1234.1234.00	01	1234.1234	1.0002	/1
Peer Hold Time								

تانايبلا ةەجاول يطايتحالا *IP* نييعت

.يناثلا لشفلا زواجت جوز ةفاضإل ،g ىلإ 6.c ةوطخلا ررك .ح

: لاثملا اذه يف

·ال : FTD11\_FTD12\_HA : يساسألا ريظنلا: FTD1\_FTD11 : يوناثلار ريظنلان

·لفوتال قئاف طابترا) : Ethernet ا تاران: Ethernet ا خابترا: Ethernet بالا طابترا) : 192.168.91.1/24

Ethernet1/5 (لخاد): 192.168.30.254/24
Ethernet1/6 (طاشنال جراخ): 192.168.40.254/24
Ethernet1/7 (Diagnostic Active): 192.168.81.1/24

Ethernet1/8 (HA\_LINK (دادعتسالا عضو يف): 192.168.91.2/24

·Ethernet1/5 (يلخادلا دادعتسالا عضو يف) 192.168.30.253/24 ·Ethernet1/6 (دادعتسالا عضو جراخ) 192.168.40.253/24 ·Ethernet1/7 (يصيخشتلا دادعتسالا عضو): 192.168.81.2/24

.جراخلا ىلا لخادلا نم رورملا ةكرجب حامسلل ACP ةدعاق نييعت .**لڨتسم تفاض**إ < **ةيڨطنم تزمج**أ ىلإ لقتنا .i

Firewall Management Center Policies / Access Control / Policy Editor	Analysis Policies	Devices	Objects Int	tegration					Deploy	Q 🔮 🕸	🛿 admin 🕶	ideados Cisco S	SECURE
acp-rule     Try New UI Layout () Analyze Hit Counts     Sixe     Cancel													
Rules Security Intelligence HTTP Responses Logging Advanced Prefitter Policy: Default Prefitter Policy: Default Prefitter Policy: Default Prefitter Policy SSL Policy: None Identity Policy: None													
Filter by Device Search Rules								×	Show Rule Con	flicts 🛛 + A	dd Category	+ Ad	dd Rule
II Name Source Zones Dest Zones Source Network	B Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	15 O IS /	8 I I	• •
Mandatory - acp-rule (1-1)													
1 ftd_ha_acp inside_zone outside_zone Any	Any	Any.	Any	Any	Any	Any	Any	Any	Any	Allow	四日日 /	ê 🖂 🖬	0/1
✓ Default - acp-rule (-)	✓ Default - acp-rule (-)												
There are no rules in this section. Add Rule or Add Category													

ACP ةدعاق نييعت

#### j. يف دادعإلا رشن FTD.

CLI يف HA ةلاح ديكأت .ك

.ASA لثامت يتلاو FirePOWER ب ةصاخلا (CLI) رماوألا رطس ةمجاو يف ليثم لكل HA قلاح ديكأت متي امك

.(01 پساسألا ليثملا) FTD1\_FTD01 ب ةصاخلا HA قلاح يلاٍ show failover رمألاو show running-config failover ليغشتب مق

#### <#root>

// confrim HA status of FTD1\_FTD01 (Instance01 of Primary Device) >

#### show running-config failover

failover failover lan unit primary failover lan interface ha\_link Ethernet1/4 failover replication htt

#### show failover

Failover On Failover unit Primary Failover LAN Interface: ha\_link Ethernet1/4 (up) ..... This host: P ..... Other host: Secondary - Standby Ready <---- InstanceO1 of FPRO2 is Standby Interface diagnostic

. (FTD1\_FTD11 (Primay Instance02 ل ةكرتشملا HA قلاح ىل show failover رمألاو show running-config failover ليغشت.

#### <#root>

// confrim HA status of FTD1\_FTD11 (Instance02 of Primary Device) >

#### show running-config failover

failover failover lan unit primary failover lan interface ha\_link Ethernet1/8 failover replication htt

#### show failover

Failover On Failover unit Primary Failover LAN Interface: ha\_link Ethernet1/8 (up) ..... This host: P Other host: Secondary - Standby Ready <---- Instance02 of FPR02 is Standby Interface diagnostic (192.16

.(10 يوناثال ليثملا) 5D2\_FTD2\_FTD0 قاراح ىل show failover رمأل او show running-config failover ليغشت.

#### <#root>

// confrim HA status of FTD2\_FTD02 (Instance01 of Secondary Device) >

#### show running-config failover

failover failover lan unit secondary failover lan interface ha\_link Ethernet1/4 failover replication h

#### show failover

Failover On Failover unit Secondary Failover LAN Interface: ha\_link Ethernet1/4 (up) ..... This host: Other host: Primary - Active <---- InstanceO1 of FPRO1 is Active Active time: 31651 (sec) slot 0: UCSB- .(20 يالا اليثمال) FTD2\_FTD12 قارح ي العالي وصحال show failover رمأل و show running-config failover ليغشت اب مق

#### <#root>

// confrim HA status of FTD2\_FTD12 (Instance02 of Secondary Device) >

#### show running-config failover

failover failover lan unit secondary failover lan interface ha\_link Ethernet1/8 failover replication h Other host: Primary - Active <---- Instance02 of FPR01 is Active Active time: 31275 (sec) slot 0: UCSB-

#### صيخرتلا كالەتسإ ديكأت .ل

.ةيواح ليثم لكل سيلو ،نامأ لكيه/كرحم لكل صيخارتلا عيمج كالهتسإ متي

نامأ لكيه/كرحم لكل ةدحاو :ايئاقلت BaseElite نييعت متي'.

قئاف نامأ لكيه/كرحم لكل طقف دحاو صيخرت كالهتسإ كنكمي نكلو ،ليثم لكل ايودي تازيملا صيخارت صيصخت متي' قمدختسملا تاليثملا ددع نع رظنلا ضغب ،1 يلامجإ صيخرت ىلإ طقف جاتحت ،ددحم قزيم صيخرتل ةبسنلاب .قزيملل.

دنتسملا اذه يف صيخارتلا كالهتسإ ةيفيك لودجلا اذه حضوي.

FPR01	01 ليثملا	،ةراضلا جماربلا، URL ناونع ةيفصت ،ةدعاقلا ديدەتلا
	02 ليثملا	،ةراضلا جماربلا، URL ناونع ةيفصت ،ةدعاقلا ديدەتلا
FPR02	01 ليثملا	،ةراضلا جماربلا، URL ناونع ةيفصت ،ةدعاقلا ديدەتلا
	02 ليثملا	،ةراضلا جماربلا، URL ناونع ةيفصت ،ةدعاقلا ديدەتلا

#### صيخارتلا ددع يلامجإ

ةدعاق	URL ةيفصت	ةثيبخ تايجمرب	ديدەت
2	2	2	2

#### . FMC ل (GUI) ةيموسرلا مدختسملا ةمجاو يف ةكلهتسملا صيخارتلا ددع ديكأت

Smart Licenses			Filter Devices	×	Edit Performance Tier	Edit Licenses
License Type/Device Name	License Status	Device Type		Domain	Group	
V Base (2)	In-Compliance					
> FTD01_FTD02_HA (2) Cisco Frepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 The	eat Defense	Global	N/A	
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thr	eat Defense	Global	N/A	
Mahware (2)	In-Compliance					
FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Th	eat Defense	Global	N/A	
FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thr	eat Defense	Global	N/A	
V Threat (2)	In-Compliance					
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thr	eat Defense	Global	N/A	
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thr	eat Defense	Global	N/A	
✓ URL Filtering (2)	In-Compliance					
> FTD01_FTD02_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thr	at Defense	Global	N/A	
> FTD11_FTD12_HA (2) Cisco Firepower 4145 Threat Defense Threat Defense High Availability	In-Compliance	High Availability - Cisco Firepower 4145 Thr	at Defense	Global	N/A	



#### ةحصلا نم ققحتلا



مطحتلا لبق



لشفلا زواجت ليغشت مت

.00-Win10 ليغشتلا ماظن ىلإ Win10-01 ليغشتلا ماظن نم FTP لاصتا أدبا .1 ةوطخلا Win10-02.

.01 ليثملا نم لك يف كرتشملا FTP لاصتال "ليغشت" رمألاا show conn عاشنا متي .2 ةوطخلا

FPR02

// Confirm the connection in Instance01 of FPR01 >

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:11, bytes 529, flags UIO N1 // Confirm show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:00:42, bytes 530, flags UIO N1

.04-Win10 ليغشتلا ماظن ىلإ Win10-03 ليغشتلا ماظن نم FTP لاصتا أدبا .3 ةوطخلا

.02 ليثملا نم لك يف كرتشملا FTP لاصتال "ليغشت" رمألا show conn عاشناٍ متي .4 ةوطخلا

#### <#root>

// Confirm the connection in Instance02 of FPR01 >

show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:02, bytes 530, flags UIO N1 // Confirm show conn

TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:00:13, bytes 530, flags UIO N1

ليغشتب مق .ASA ل (CLI) رماوألا رطس ةهجاو لاخدال رمألاا ASA ل (CLI) ماوألا رطس تهجاو لاغدال رمأل العن من عن .5 قوطخلا enable **crashinfo force watchdog** داصتلال ليثم ضرفل رمألاو.

#### <#root>

Firepower-module1>

connect ftd FTD01

```
>
```

```
system support diagnostic-cli
```

FTD01>

enable

Password: FTD01# FTD01#

crashinfo force watchdog

reboot. Do you wish to proceed? [confirm]:

ديكأتل رمألا show failover\_show conn ليغشتب مق .FTP لاصتا ةعطاقم متي الو Instance01 يف لشفلا زواجت ثدحي .6 ةوطخلا يف 10 ليثملاا تالااح

#### <#root>

```
>
```

#### show failover

Failover On Failover unit Secondary Failover LAN Interface: ha\_link Ethernet1/4 (up) ..... This host: Other host: Primary - Failed Interface diagnostic (192.168.80.2): Unknown (Monitored) Interface inside

show conn

TCP outside 192.168.20.1:21 inside 192.168.10.1:49723, idle 0:02:25, bytes 533, flags U N1

تالاح ديكأتل رمألاا Instance01 يف لطع ثدح .7 ةوطخلاا يا Show failover show conn يلع ريثأت هل نكي مل Instance01 يف لطع ثدح .7 ةوطخلا 02. لىثملا

#### <#root>

```
>
```

#### show failover

Failover On Failover unit Secondary Failover LAN Interface: ha\_link Ethernet1/8 (up) ..... This host: Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (1

show conn

```
TCP outside 192.168.40.1:21 inside 192.168.30.1:52144, idle 0:01:18, bytes 533, flags UIO N1
```

#### دادعتس ال عضو ، Primay زارطل : FTD1\_FTD01 زارطل ا

#### طشن ، يونات :FTD2\_FTD02:

Fin Dev	ewall Management Center Overview Analysis	Policies Devices Object	s Integration	n			Deploy Q 📀	O admin      Secure			
View By:	w Br. Group										
All (4)	Error (0)     Warning (0)     Offline (0)     Normal (4)	<ul> <li>Deployment Pending (0)</li> </ul>	pgrade (0)	Snort 3 (4)				Q, Search Device Add •			
Collapse All											
	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack				
	<ul> <li>Ungrouped (2)</li> </ul>										
	<ul> <li>FTD01_FTD02_HA</li> <li>High Availability</li> </ul>							1			
	FTD1_FTD01(Primary, Standby) Short 3	Firepower 4145 with FTD	7.2.5	E Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	¢₽	1			
	FTD2_FTD02(Secondary, Active) Soort 3	Firepower 4145 with FTD	7.2.5	Enclose Container (Container)	Base, Threat (2 more)	acp-rule	eQ	1			
	V FTD11_FTD12_HA High Availability							11			
	FTD1_FTD11(Primary, Active) Short 3	Firepower 4145 with FTD	7.2.5	III Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	40	ı			
	FTD2_FTD12(Secondary, Standby) Short 3     T 10.2 - Routed	Firepower 4145 with FTD	7.2.5	Firepower4KHG cisco.com 443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	κβ	:			

*HA* ةلاح ديكأت

ةطساوب كلذ ذيفنت نكمي .ايودي HA قلاح ليدبت كنكمي ،يداع ىل! FPR01 نم 01 ليثملا عجري نأ دعب (يرايتخ|) .9 ةوطخلا

.(CLI) ل (CLI) رماوألا رطس ةهجاو وأ FMC ل (GUI) ةيموسرلا مدختسملا قهجاو

.HA قاراح الحري نأ طشن ريظن حاسف مق مقطقط للكلا < قرّه جألا علام القرين ا FMC، يف HA تراجع الله الحقي المحمد الكلا على المحمد المحم

Firewall Management Center Ov Devices / Device Management	erview Analysis Policies Devices	Objects Integration				Deploy Q 🥝	admin      dede SECURE
View By: Group  All (4)  Error (0)  Warning (0)  Offline	(0)   Normal (4)  Deployment Pending (0)	• Upgrade (0) • Se	nort 3 (4)				Deployment History Q. Search Device Add •
Collapse All							
Name Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (2)							
FTD01_FTD02_HA     High Availability							Switch Active Peer
FTD1_FTD01(Primary, Standby) Snort 3 (111.1 - Routed)	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9-443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	e9	Force refresh node status Delete Revert Upgrade
FTD2_FTD02(Secondary, Active) Snort Control, 1.2 - Routed	3 Firepower 4145 with FTD	7.2.5	Firepower4KHG.cisco.com/443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	ep.	Health Monitor Troubleshoot Files
FTD11_FTD12_HA     High Availability							11
FTD1_FTD11(Primary, Active) Short 3     C.S	Firepower 4145 with FTD	7.2.5	FPR4145-ASA-K9:443 Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	ф	1
FTD2_FTD12(Secondary, Standby) Sec	et 3 Firepower 4145 with FTD	7.2.5	Firepower4040.cisco.com.443 El Security Module - 1 (Container)	Base, Threat (2 more)	acp-rule	49	:

HA ةلاح ليدبت

ىلع FirePOWER CLI، يف لوخدلل رمألار connect ftd FTD01 system support diagnostic-clil ليغشتب مق ASA CLI. يف اليغ enable **failover active** يأل اليدبتلل رمألاو (HA) له (HA) رفوتلا قيل عني لي دبتل رمأل او

#### <#root>

Firepower-module1>

connect ftd FTD01

>

system support diagnostic-cli

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach. Type help or '?' for a list of availab

enable

firepower#

failover active

اهحالصإو ءاطخألا فاشكتسا

.رمألااو show failover\_show failover history ليغشتلاب مق ،لشفلا زواجت ةلاح نم ققحتلل

#### <#root>

>

#### show failover

Failover On Failover unit Secondary Failover LAN Interface: ha\_link Ethernet1/8 (up) ..... This host:

Other host: Primary - Active Interface diagnostic (192.168.81.1): Normal (Monitored) Interface inside (2

show failover history

لشفالا زواجتب صاخلا عاطخألا حيحصت لجس نيكمتل <debug fover <option رمألا ليغشتب مق.

<#root>

>

#### debug fover

auth Failover Cloud authentication cable Failover LAN status cmd-exec Failover EXEC command execution of

عجرملا

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-Instance/multi-Instance solution.html

https://www.cisco.com/c/en/us/support/docs/availability/high-availability/217763-troubleshoot-firepower-threat-defense-hi.html#toc-hId-46641497

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