# FirePOWER ديدەت نع عافدلا طاقتلا مادختسإ مزحلا عبتتو

## تايوتحملا

<u>ةمدقملا</u> <u>قيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>قيساسأ تامولعم</u> <u>FTD ةمزح ةجااعم</u> <u>نىوكتلا</u> <u>ةكېشلل يطيطختلا مسرلا</u> <u>ريخشال كرجم طاق تال مادخت ساب المعاا</u> <u>قيساسألا تابلطتملا</u> <u>تابلطتملا</u> لحل <u>ريخشال كرجم طاقتال مادختساب المعاا</u> <u>تابلطتملا</u> الحل <u>TCPDUMP ةيفصت لماع ةل ثمأ</u> <u>FTD LINA كرجم طاق تل مادخت ساب لمعلا</u> <u>تابلطتملا</u> الحيا <u>HTTP ربع طاقتال ريدصت - FTD LINA كرجم طاقتال مادختساب لمعلاا</u> <u>تابلطتملا</u> لالحال <u>FTP/TFTP/SCP ربع طاق تلاريد من - FTD LINA كرجم طاق تلارمادخ تس اب لمعلاا</u> <u>تابلطتملا</u> الحل <u>ةيقىقى ورم قكرح قمزح بقرعت - FTD LINA كرجم طاقتالا مادختساب لرمعارا</u> <u>تابلطتملا</u> الحيا <u>6.2 دعب FMC جمارب تارادصا يف طاقتلاالا ةاداً</u> <u>FTD ب ةصاخلا (CLI) رماوألا رطس ةهجاو مادختسا - ليدبلا لحلا</u> <u>6.2 دعب FMC ىلع قېقېقح قمزح عبتت</u> <u>FTD Packet Tracer ةدعاسماا ةادألاا</u> <u>تابلطتملا</u> الحلا <u>6.2 دعب FMC جمارت تارادصا يف Packet Tracer UI تانايټانا مزحل مدختسمانا قوچاو قادأ</u> <u>ةلص تاذ تامولعم</u>

ةمدقملا

تاودألاو "FirePOWER (FTD) ديدهت نع عافدلا" تاطقل مادختسإ ةيفيك دنتسملاا اذه حضوي مزحلا عبتتل ةدعاسملا.

## ةيساسألا تابلطتملا

تابلطتملا

دنتسملا اذهل ةصاخ تابلطتم دجوت ال.

ةمدختسملا تانوكملا

ةيلاتا جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- ASA5515-X جمانربب لمعي يذلا FTD 6.1.0
- FTD 6.2.2 جمانرب لغشي يذلا FPR4110
- FirePOWER (FMC) 6.2.2 ةرادإ زكرم جمانربب لمعت يتلا FS4000

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

FTD ةمزح ةجلاعم

:يلي امك FTD ةمزح ةجلاعم ضرع متي



- 1. كرحم LINA لا ب ةجلاعميو ،نراق لخدملا طبر لخدي.
- .ريخشلا كرحم ةطساوب ةمزحلا صحف بلطتي جەنلا ناك اذا
- .ةمزحلل امكح ريخشلا كرحم عجري .3
- . Snort رارق ىلع ًءانب اەەيجوت ةداعإ وأ ةمزحلا طاقسإب LINA كرحم موقي .4

:نكامألا هذه يف FTD طاقتلا نكمي ،ةيرامعملا ةينبلا ىلإ ادانتسا



## نيوكتلا

ةكبشلل يطيطختلا مسرلا



ريخشلا كرحم طاقتلا مادختساب لمعلا

ةيساسألا تابلطتملا

رورم ةكرحل حمست يتلا FTD ىلع ةقبطم (ACP) لوصولا يف مكحتلا ةسايس كانه اضيأ ةسايسلا هذه قيبطت متيو .رورملاب (ICMP) تنرتنالاا يف مكحتلا لئاسر لوكوتورب لفطتلا جهن ىلع:

Overview Analy	sis Po	licies	Devices	Objects	AMP								Deploy	•	System	Help 🔻	mikis <del>v</del>
Access Control > /	ccess Co	ontrol	Network I	Discovery	Application Det	ectors	Cor	relation	1	Actions 1	,						
FTD5515 🛛 🗍 Save 🛛 😂 Cancel									Cancel								
Enter a description																	
Identity Policy: <u>None</u>	dentity Policy: None SSL Policy: None																
Rules Security	ntelligenc	e HT	TP Response	s Advanc	ed							_					
Filter by Device								0 A	ld Cate	gory	🚺 Ad	ld Rule	Sear	ch Rules			х
e Name	s z	D Z	Source Networks	Des	it works	v	u	A	5r	Dest P	1	u	IS	Action			
▼ Mandatory - FT	5515-(1-	1)													_		
1 Allow ICMP	any	any	<b>2</b> 192.168.	103.0/24 👳	192.168.101.0/24	any	any	any	any	R ICM	ም (1)	any	any	🗸 Allov	V 😳	1	J 🗄
🗢 Default - FTD55	5 (-)																
There are no rules in	this section	n. Add R	ule or Add Cat	regory									lr	ntrus	sion	Polic	:y
Default Action								A	cess C	iontrol: E	lock A	I Traffi	c				× 🗾

```
.ةيفصت لماع نودب FTD ل CLISH عضو ىلع طاقتلالا نيكمت .1
```

.ةطقتلملا تاجرخملا نم ققحتلاو FTD لالخ نم لاصتالا رابتخا

الحل

طاقتلالا نيكمتو BR1 ةەجاو ىلإ SSH وأ FTD مكحت ةدحو ىلإ لوخدلا ليجستب مق 1. ةوطخلا ةيفصت لماع نودب FTD ل CLISH عضو ىلع.

<#root>

>

capture-traffic

```
Please choose domain to capture traffic from:
0 - br1
1 - Router
```

Selection?

1

Please specify tcpdump options desired. (or enter '?' for a list of supported options) Options:

:رمألا FTD 6.0.x يف

<#root>

>

system support

capture-traffic

.طقتلملا جارخإلا نم ققحتلاو FTD لالخ نم لاصتالا رابتخإ .2 ةوطخلا

```
<#root>
>
capture-traffic
Please choose domain to capture traffic from:
    0 - br1
    1 - Router
```

Selection?

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
12:52:34.749945 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 1, least
12:52:34.749945 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 1, least
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 2, least
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 2, least
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 3, least
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 3, least
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 3, least
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo request, id 0, seq 4, least
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 4, least
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 4, least
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 4, least
^C <- to exit press CTRL + C</pre>
```

### ريخشلا كرحم طاقتلا مادختساب لمعلا

### تابلطتملا

- 1. ل ةيفصت لماع مادختساب FTD ل CLISH عضو ىلع طاقتلالا نيكمتب مق 192.168.101.1.
- .طقتلملا جارخإلا نم ققحتلاو FTD لالخ نم لاصتالا رابتخا .2

الحل

ال ةيفصت لماع مادختساب FTD ل CLISH عضو ىلع طاقتلالا نيكمتب مق 1. قوطخلا IP 192.168.101.1.

<#root>

>

```
capture-traffic
```

```
Please choose domain to capture traffic from:
  0 - br1
  1 - Router
```

Selection?

1

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
```

```
host 192.168.101.1
```

:ةطقتلملا تاجرخملا نم ققحتلاو FTD لالخ نم لاصتالا رابتخإ .2 ةوطخلا

1

13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 0, len 13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 1, len 13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 2, len 13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 3, len 13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 3, len

```
ليبس ىلع .يمقر قيسنتب ذفانملا ماقراو فيضملا ةيؤرل N رايخ مادختسإ كنكمي
يلاتلا وحنلا ىلع قباسلا طاقتلالا ضرع متي ،لاثملا:
```

```
<#root>
```

>

```
capture-traffic
```

Please choose domain to capture traffic from: 0 - br1

- 1 Router
- L Router

Selection?

1

Please specify tcpdump options desired. (or enter '?' for a list of supported options) Options:

```
-n host 192.168.101.1
```

13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 0, length 80 13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 1, length 80 13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 2, length 80 13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 3, length 80 13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 4, length 80

```
TCPDUMP ةيفصت لماع ةلثمأ
```

:1 لاثم

تلخد in order to وأ ءانيم src و 192.168.101.1 وأ src ip ضبق ىلع src ip تلخد TCP/UDP = ءانيم dst يرمأ اذه 32. درمأ اذه 23،

#### <#root>

Options:

-n host 192.168.101.1 and port 23

:2 لاثم

:رمأ اذه ،src = TCP/UDP 23 ذفنمو src ip = 192.168.101.1 ضبق ىلع in order to تلخد

<#root>

Options:

```
-n src 192.168.101.1 and src port 23
```

### :3 لاثملا

:رمأ اذه ،src = TCP 23 ذفنمو src ip = 192.168.101.1 ضبق ىلع in order to تلخد

### <#root>

Options:

-n src 192.168.101.1 and tcp and src port 23

:4 لاثم

تفضأ in order to ناونع src ip = 192.168.101.1 إا عجارو src ip = 192.168.101.1 نايخلا طبرلا نم ناونع in crder to زمأ اذه لخدأو:

<#root>

Options:

-ne

src 192.168.101.1

17:57:48.709954

6c:41:6a:a1:2b:f6 > a8:9d:21:93:22:90,

ethertype IPv4 (0x0800), length 58: 192.168.101.1.23 > 192.168.103.1.25420: Flags [S.], seq 3694888749, ack 1562083610, win 8192, options [mss 1380], length 0

:5 لاثم

:رمأ اذه ،طبر 10 تنأ ضبق ىلع نأ دعب تجرخ in order to تلخد

### <#root>

Options:

-n -c 10 src 192.168.101.1

18:03:12.749945 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 3758037348, win 32768, length
18:03:12.749945 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 1, win 32768, length 2
18:03:12.949932 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 1, win 32768, length 10
18:03:13.249971 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 3, win 32768, length 0
18:03:13.249971 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 3, win 32768, length 2
18:03:13.279969 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 3, win 32768, length 0
18:03:13.279969 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 5, win 32768, length 0
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 0
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 1
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 1
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 0
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 1
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 0
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 0
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 0
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 12
18:03:13.349972 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 9, win 32768, length 0

### :6 لاثم

تلخد in order to لالخ نم ەخسنو capture.pcap مسإلا عم دربم ىلإ طاقتلا تبتك TP تلخد رمأ اذه ،ديعب:

### <#root>

Options:

-w capture.pcap host 192.168.101.1
CTRL + C <- to stop the capture
> file copy 10.229.22.136 ftp / capture.pcap

Enter password for ftp@10.229.22.136: Copying capture.pcap

Copy successful.

>

### FTD LINA كرحم طاقتلا مادختساب لمعلا

تابلطتملا

:ةيلاتلا ةيفصتلا لماوع مادختساب FTD ىلع نيطقتلإ نيكمت .1

ردصملا IP	192.168.103.1
ةەجولI P	192.168.101.1
لوكوتوربلا	ICMP
ۃمجاولا	لخاد

ردصملا IP	192.168.103.1
ةەجولا IP	192.168.101.1
لوكوتوربلا	ICMP
ۃەجاولا	جراخ

2. قرقحتلاو (B (192.168.101.1) الحين الم العن ال تاطاقتل إن م.

الحلا

:طاقتلالا نيكمت .1 ةوطخلا

<#root>

> capture CAPI interface INSIDE match icmp host 192.168.103.1 host 192.168.101.1
> capture CAPO interface OUTSIDE match icmp host 192.168.101.1 host 192.168.103.1

.(CLI) رماوألا رطس ةهجاو طاقتلا نم ققحت .2 ةوطخلا

B:فيضملا ىل A-فيضملا نم لاصتالا رابتخاB:

### C:\Users\cisco>ping 192.168.101.1

Pinging 192.168.101.1 with 32 bytes of data: Reply from 192.168.101.1: bytes=32 time=4ms TTL=255 Reply from 192.168.101.1: bytes=32 time=5ms TTL=255 Reply from 192.168.101.1: bytes=32 time=1ms TTL=255 Reply from 192.168.101.1: bytes=32 time=1ms TTL=255

<#root>

> show capture

capture CAPI type raw-data interface INSIDE [Capturing

- 752 bytes

]

match icmp host 192.168.103.1 host 192.168.101.1
capture CAPO type raw-data interface OUTSIDE [Capturing

- 720 bytes

match icmp host 192.168.101.1 host 192.168.103.1

وه امك ،ةيلخادلا ةهجاولا ىلع Dot1Q سأر ببسب ةفلتخم ماجحاً ىلع نافيطقتلا يوتحي اذه جارخإلا لاثم يف حضوم:

<#root>

٦

> show capture CAPI

8 packets captured
 1: 17:24:09.122338

802.1Q vlan#1577

```
P0 192.168.103.1 > 192.168.101.1: icmp: echo request

2: 17:24:09.123071 802.10 vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply

3: 17:24:10.121392 802.10 vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request

4: 17:24:10.122018 802.10 vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply

5: 17:24:11.119714 802.10 vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request

6: 17:24:11.120324 802.10 vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply

7: 17:24:12.133660 802.10 vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo reply

8: 17:24:12.134239 802.10 vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo request

8: 17:24:12.134239 802.10 vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
```

8 packets shown

#### <#root>

> show capture CAPO

```
8 packets captured

1: 17:24:09.122765 192.168.103.1 > 192.168.101.1: icmp: echo request

2: 17:24:09.122994 192.168.101.1 > 192.168.103.1: icmp: echo reply

3: 17:24:10.121728 192.168.103.1 > 192.168.101.1: icmp: echo request

4: 17:24:10.121957 192.168.101.1 > 192.168.103.1: icmp: echo reply

5: 17:24:11.120034 192.168.103.1 > 192.168.101.1: icmp: echo request

6: 17:24:11.12063 192.168.101.1 > 192.168.103.1: icmp: echo reply

7: 17:24:12.133980 192.168.103.1 > 192.168.101.1: icmp: echo request

8: 17:24:12.134194 192.168.101.1 > 192.168.103.1: icmp: echo reply
```

8 packets shown

### HTTP ربع طاقتلاا ريدصت - FTD LINA كرحم طاقتلاا مادختساب لمعلا

تابلطتملا

. ضرعتسم مادختساب قباسلا ويرانيسلا يف اهطاقتلا مت يتلا تاطاقتلالا ريدصت

الحلا

یل جاتحت ،حفصتم مادختساب طاقتلالا ريدصتل:

مداخ نيكمت .1 2. يلإ لوصولاب حامسلا .2

:لوصولاب حامسلا متي الو ،HTTPS مداخ ليطعت متي ،يضارتفا لڬشب

<#root>

>

show running-config http

>

عافدلا تادادعإ رتخاو ،ديدج جەن رقناو ،يساسألا ماظنلا تادادعإ < ةزەجألا ىلإ لقتنا .1 ةوطخلا ديدەتلا نع:

De	vices	Objects	AMP	Deploy	) 📀	System	Help 🔻	mikis 🔻
PN	Platfor	m Settings						
							Object Ma	nagement
							📀 New F	Policy
	Device Type			Status		Firepov	ver Setting	s
	Threat D	efense		Targeting 1 d	levice	Threat	Defense S	ettings

زاهجلا فدهو جەنلا مسا ددح:

New Policy							
Name:	FTD5515-System_Policy						
Description:							
Targeted Devices							
Select devices to v	which you want to apply this policy.						
Available Devices	Selected Devices						
Search by nam	e or value	FTD5515					

زاهج ىلإ لوصولاب كل حامسلا ديرت يتلا ةكبشلا فضأو HTTPS مداخ نيكمتب مق .2 ةوطخلا FTD ربع HTTPS:

Overview Analysis Policie Device Management NAT	IS Devices Objects AN	1P		
FTD5515-System_Po Enter a description	blicy			
ARP Inspection Banner External Authentication	Enable HTTP Server 7 2 Port 443	(Please don't use 80 or 1443)		
HTTP 1     ICMP	Interface		Network	3 🙆 Add
Secure Shell SMTP Server	INSIDE		Net_192.168.103.0_24bits	/ 8

### رشنو ظفح.

:HTTP ةمدخ ةيادب ضرعل debug http نيكمت كنكمي ،جەنلا رشن تقو يف

### <#root>

```
> debug http 255
```

debug http enabled at level 255.

http\_enable: Enabling HTTP server HTTP server starting.

### :يه FTD ل (CLI) رماوألا رطس ةمجاو ىلع ةجيتنلا

### <#root>

> unebug all

> show run http
http server enable
http 192.168.103.0 255.255.255.0 INSIDE

لوألا طاقتلالا ليزنتل اذه URL ناونع مدختساو host-A (192.168.103.1) يلع ضرعتسم حتفا https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap.

Opening CAPI.pcap	
You have chosen to open: CAPL.pcap which is: Wireshark capture file (776 bytes) from: https://192.168.103.62 What should Firefox do with this file?	
Open with Wireshark (default)     Save File     Do this <u>a</u> utomatically for files like this from now on.	
OK Cancel	

ەيلإ عوجرلل:

https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	FTD تانايب ةەجاوب صاخلا IP مداخ نيكمت متي ثيح HTTP
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	FTD طاقتلا مسا
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	ەليزنت مت يذلا فلملا مسا

مدختسأ ،يناثالا <u>https://192.168.103.62/capture/CAPO/pcap/CAPO.pcap</u>.

Mttps://192.168.103.62/capture/CAPO/pcap/CAPO.pcap
Opening CAPO.pcap
You have chosen to open:
CAPO.pcap
which is: Wireshark capture file (744 bytes)
from: https://192.108.103.62
What should Firefox do with this file?
Open with     Wireshark (default)
Save File
Do this automatically for files like this from now on.
OK Cancel

FTP/TFTP/SCP ربع طاقتاا ريدصت - FTD LINA كرحم طاقتال مادختساب لمعال

تابلطتملا

تالوكوتورب مادختساب ةقباسلا تاهويرانيسلا يف ةذوخأملا طاقتلالا ريدصت FTP/TFTP/SCP.

الحل

:FTP مداخ ىلإ طاقتلا ريدصت

<#root>

firepower

# copy /pcap capture:CAPI ftp://ftp\_username:ftp\_password@192.168.78.73/CAPI.pcap

Source capture name [CAPI]?

Address or name of remote host [192.168.78.73]?

Destination username [ftp\_username]?

Destination password [ftp\_password]?

Destination filename [CAPI.pcap]?
!!!!!!

114 packets copied in 0.170 secs

firepower#

:TFTP مداخ ىلإ طاقتلا ريدصت

#### <#root>

firepower

# copy /pcap capture:CAPI tftp://192.168.78.73

Source capture name [CAPI]?

Address or name of remote host [192.168.78.73]?

Destination filename [CAPI]?

346 packets copied in 0.90 secs

firepower#

SCP: مداخ ىلإ طاقتلا ريدصت

#### <#root>

firepower#

copy /pcap capture:CAPI scp://scp\_username:scp\_password@192.168.78.55

Source capture name [CAPI]?

Address or name of remote host [192.168.78.55]?

Destination username [scp\_username]?

Destination filename [CAPI]? The authenticity of host '192.168.78.55 (192.168.78.55)' can't be established. RSA key fingerprint is <cb:ca:9f:e9:3c:ef:e2:4f:20:f5:60:21:81:0a:85:f9:02:0d:0e:98:d0:9b:6c:dc:f9:af:4 Are you sure you want to continue connecting (yes/no)? yes Warning: Permanently added '192.168.78.55' (SHA256) to the list of known hosts.

454 packets copied in 3.950 secs (151 packets/sec)

نم ليمحتلا ءاغلإ طاقتلا FTD نم طاقتلال ليمحت ءاغل على جات المدنع ،ايل FTD. نم ليمحتلا عاغل طاقتل FTD نم طاقت ال تاوطخلا هذه ذيفنت يه ققيرط لهسأ:

1. نم Lina - copy /pcap capture:<cap\_name> disk0:

2. رذج نم FPR - mv /ngfw/mnt/disk0/<cap\_name> /ngfw/var/common/

اهحالصإو ءاطخألا فاشكتسأ < زاهج < ةشاش < ةحص < ماظن - FMC مدختسم ةهجاو نم .3 لخدأو مدقتملا.

ةيقيقح رورم ةكرح ةمزح بقعت - FTD LINA كرحم طاقتلا مادختساب لمعلا

تابلطتملا

:ةيلاتلا ةيفصتلا لماوع مادختساب FTD ىلع طاقتلا نيكمت

ردصملا IP	192.168.103.1
ةەجولا IP	192.168.101.1
لوكوتوربلا	ICMP
ةەجاولا	لخاد
ةمزحلا عبتت	معن
عبتتلا مزح ددع	100

نم ققحتلاو (B (192.168.101.1) -فيضملا (A (192.168.103.1) -فيضملا نم لاصتالا رابتخ<u>ا</u> متي طاقتلالا تايلمع.

لحلا

كل حمسي وهو .اهحالصإو لـاصتالا ءاطخاً فاشكتسال ادج اديفم ةيقيقح ةمزح عبتت دعي ليصافت ثحب تاملك ةفاضإب مق .ةمزحلا اهب رمت يتلا ةيلخادلا تاققحتلا لك ةيؤرب لخدم ةمزح 50 لوأ FTD عبتتي ،يضارتفا لكشب .اهعبتت ديرت يتلا مزحلا ددع ددحو عبتتلا.

يتلا ىلوألا 100 مزحلل عبتتلا ليصافت مادختساب طاقتلالا نيكمتب مق ،ةلاحلا هذه يف

### <#root>

> capture CAPI2 interface INSIDE trace detail trace-count 100 match icmp host 192.168.103.1 host 192.168

:ةجيتنلا صحفو B-فيضملا ىلإ A-فيضملا نم لاصتالا رابتخإ

### C:\Users\cisco>ping 192.168.101.1

Pinging 192.168.101.1 with 32 bytes of data: Reply from 192.168.101.1: bytes=32 time=2ms ITL=255 Reply from 192.168.101.1: bytes=32 time=2ms ITL=255 Reply from 192.168.101.1: bytes=32 time=2ms ITL=255 Reply from 192.168.101.1: bytes=32 time=8ms ITL=255

يه ةطقتلملا مزحلا:

### <#root>

```
> show capture CAPI2
```

```
8 packets captured
```

```
1: 18:08:04.232989 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request

2: 18:08:04.234622 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply

3: 18:08:05.223941 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request

4: 18:08:05.224872 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply

5: 18:08:06.222309 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request

6: 18:08:06.223148 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo request

7: 18:08:07.220752 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request

8: 18:08:07.221561 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo request
```

```
8 packets shown
```

انمەت يتلا ءازجالا .ىلوالا ةمزحلا عبتت جارخإلا اذە ضرعي:

- لاسرا فيفص" وه اذه ."يمامألا قفدتلا" ةيؤر هيف متي يذلا ناكملا يه 12 ةلحرملا ياكرحم LINA" (يلخادلا تايلمعلا بيترت وه ايلعف).
- . snort ليثم ىلإ ةمزحلا FTD هيف لسري يذلا ناكملا يه 13 ةلحرملا
- ريخشلا مكح يف اهيف رظني يتلا يه 14 ةلحرملا.

### <#root>

```
> show capture CAPI2 packet-number 1 trace detail
```

8 packets captured

1: 18:08:04.232989 000c.2998.3fec a89d.2193.2293 0x8100 Length: 78

802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request (ttl 128, id 3346) Phase: 1 Type: CAPTURE

... output omitted ... Phase: 12 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 195, packet dispatched to next module Module information for forward flow ... snp\_fp\_inspect\_ip\_options snp\_fp\_snort snp\_fp\_inspect\_icmp snp\_fp\_adjacency snp\_fp\_fragment snp\_ifc\_stat Module information for reverse flow ... snp\_fp\_inspect\_ip\_options snp\_fp\_inspect\_icmp snp\_fp\_snort snp\_fp\_adjacency snp\_fp\_fragment snp\_ifc\_stat Phase: 13 Type: EXTERNAL-INSPECT Subtype: Result: ALLOW Config: Additional Information: Application: 'SNORT Inspect' Phase: 14 Type: SNORT Subtype: Result: ALLOW Config: Additional Information: Snort Verdict: (pass-packet) allow this packet ... output omitted ... Result: input-interface: OUTSIDE input-status: up input-line-status: up output-interface: OUTSIDE output-status: up output-line-status: up Action: allow 1 packet shown >

## 6.2 دعب FMC جمارب تارادصإ يف طاقتلالا ةادأ

ةرادإ < ةزهجألاا ىلإ لقتنا .ديدج مزح طاقتلا جلاعم ميدقت مت ،FMC نم 6.2.x رادصإلا يف ءاطخألا فاشكتسأ رتخأ مث .اهحالصإو ءاطخألا فاشكتسأ ةنوقيأ قوف رقناو ةزهجألا عاقتلالا اريخأو مدقتملا اهحالصإو w/Trace.

Overview Analysis Policies Devices	Object	s AM	P Inte	lligence				
Device Management NAT VPN <b>v</b> Q	oS Pl	atform S	ettings	FlexCon	fig	Certificates		
By Group								$\bigcirc$
Name	Group	Model	License	Туре	Acc	ess Control Poli		
FTD4110-2 10.48.23.254 - Cisco Firepower 4110 Thread	Cisco	Firepower	411( Bas	e, Threat, M	a	ACP1	ø	6 🔀

:FTD طاقتلا ءاشنإل طاقتلا ةفاضإ رتخأ

Ad FTD4	Advanced Troubleshooting FTD4110-2											
File Download Threat Defense CLI				Packet Tracer Capture w/Trace								
¢	C Auto Refresh Interval (seconds): 10 Enable Auto Refresh											
Na	Interface	Туре	Trace	Buffer Mode	Buffer Size	Packet Length	Buffer Status	Protocol	Source	Destination	Status	

Add Capture				? ×	
Name*:	САРІ	Interface*:	INSIDE		Source interface
Match Criteria:					
Protocol*:	IP 💌	←			IP Protocol
Source Host*:	192.168.0.10	Source Network:	255.255.255.255		
Destination Host*:	192.168.2.10	Destination Network:	255.255.255.255		
SGT number:	0	(0-65535)			Circular buffer
Buffer:					
Packet Size:	1518 14-1522 bytes	Continuous Ca	pture 🕑 Trace		
Buffer Size:	524288 1534-33554432 bytes	Stop when full	Trace Coun	t: 50	

:يە ةيلاحلا FMC مدختسم ةەجاو دويق

- DST و SRC ذفانم ديدحت نكمي ال
- طقف ةيساسألا IP تالوكوتورب ةقباطم نكمي •
- LINA كرحمل ASP طاقسإ تايلمعل طاقتلالا نيكمت نكمي ال

FTD ب ةصاخلا (CLI) رماوألا رطس ةهجاو مادختسإ - ليدبلا لحلا

:طاقتلالا ليغشت متي ،FMC مدختسم ةهجاو نم طاقتلا قيبطت درجمب

File Download Threat Defense CLI Packet Trace		racer	Capture w/Trace			Clear the										
🖒 Auto Refresh Interval (seconds): 10 🗌 Enable Au				to Refresh				capture			0	Add	Captu	ure		
Na	Interface	Туре	Trace	Buffer Mode	Buffer Size	Packet Length	Buffer Status	Protocol	Source	Destination	Status					
CAPI	INSIDE	raw-data	1	M	524288	1518	Capturing	IP	192.168.0.10	192.168.2.10	Running	Ø	6	0		
									_		_					Î
										Pause the capture	Save in po	ə th xap	e fo	cap rm	otui at	re

CLI ل CLI ىلع طاقتلالا

### <#root>

```
> show capture
```

```
capture CAPI%intf=INSIDE% type raw-data trace interface INSIDE [Capturing - 0 bytes]
match ip host 192.168.0.10 host 192.168.2.10
>
```

### 6.2 دعب FMC ىلع ةيقيقح ةمزح عبتت

ىك اهعبتتو ةيقيقحالا مزحلا طاقتال w/Trace طاقتالالا جالعم كل حيتي FMC 6.2.x، ياع اهعبتتو ةيقيقحالا مزحل

Add Capture			? : X	
Name*:	САРІ	Interface*:	INSIDE	
Match Criteria:				
Protocol*:	IP 🗸			
Source Host*:	192.168.16.111	Source Network:	255.255.255.255	
Destination Host*:	192.168.17.1	Destination Network:	255.255.255.255	
SGT number:	0	(0-65533)		
Buffer:				
Packet Size:	1518 14-1522 bytes	O Continuous Cap	oture 🕑 Trace	Trace ingress packets
Buffer Size:	524288 1534-33554432 bytes	Stop when full	Trace Count: 50	

:FMC مدختسم ةەجاو يف اەعبتت مت يتلا ةمزحلا نم ققحتلا كنكمي



## FTD Packet Tracer ةدعاسماا ةادألاا

تابلطتملا

ايلخاد ةمزحلا ةجلاعم ةيفيك صحفو قفدتلا اذهل Packet Tracer ةدعاسملا ةادألا مدختسأ:

لوخدلا ةمجاو	لخاد
لوكوتوربلا	ICMP ىدص بلط
ردصملا IP	192.168.103.1
ةەجولا IP	192.168.101.1

لحلا

ىلا قمزحلا عضخت ،لاثملا اذه يف حضوم وه امك .قيرهاظ قمزح ءاشنإب Packet Tracer موقت ىوتسم ىلع تقولا سفن يف تذخأ طاقتلا قيلمع رهظت .رخشلا صحف ىدص بلط ICMP:

#### <#root>

> packet-tracer input INSIDE icmp 192.168.103.1 8 0 192.168.101.1 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: ROUTE-LOOKUP Subtype: Resolve Egress Interface Result: ALLOW Config: Additional Information: found next-hop 192.168.101.1 using egress ifc OUTSIDE Phase: 4 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM\_FW\_ACL\_ global access-list CSM\_FW\_ACL\_ advanced permit ip 192.168.103.0 255.255.255.0 192.168.101.0 255.255.255.0 rule access-list CSM\_FW\_ACL\_ remark rule-id 268436482: ACCESS POLICY: FTD5515 - Mandatory/1 access-list CSM\_FW\_ACL\_ remark rule-id 268436482: L4 RULE: Allow ICMP Additional Information: This packet is sent to snort for additional processing where a verdict is reached ... output omitted ... Phase: 12 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 203, packet dispatched to next module Phase: 13 Type: SNORT Subtype: Result: ALLOW Confia: Additional Information: Snort Trace: Packet: ICMP AppID: service ICMP (3501), application unknown (0) Firewall: allow rule, id 268440225, allow

NAP id 2, IPS id 0, Verdict PASS Snort Verdict: (pass-packet) allow this packet

```
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

```
>
```

:ةيرهاظلا ةمزحلا packet-tracer رابتخإ تقو يف snort يوتسم طاقتلا رهظي

### <#root>

>

#### capture-traffic

Please choose domain to capture traffic from: 0 - management0 1 - Router

Selection? 1

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
-n
13:27:11.939755 IP 192.168.103.1 > 192.168.101.1: ICMP echo request, id 0, seq 0, length 8
```

```
تانايبلا مزحل مدختسملا ةەجاو ةادأ Packet Tracer UI جمارب تارادصإ يف
6.2 دعب
```

رادصإ يف قادألا ىلإ لوصولا نكمي .مزحلا عبتتل مدختسملا قمجاو قادأ ميدقت مت FMC 6.2.x رادصإ يف Packet ليغشتب كل حمستو طاقتلالا قادأ ىلإ لوصولا امب متي يتلا ققيرطلا سفنب Tracer ليغشتب متوجاو نم FTD يلع FMC:

			C	Configuration	Users	Domains	Integration U	pdates	Licenses <b>•</b>	Health 🕨 M	lonitor
A FTC	dvanced Tro	ubleshooting									
F	ile Download T	hreat Defense CLI	Packe	t Tracer Ca	apture w/	Trace	Ть	2 501	irce int	orface	
	Select the packet ty	/pe and supply the packet pa	aramet	ers. Click start to	o trace the p	acket.		5 30t		enace	
	Packet type:	ТСР	~				Interface*:	INSIDE		~	
	Source*:	IP address (IPv4)	~	192.168.0.10			Source Port*:	1111		~	
	Destination*:	IP address (IPv4)	~	192.168.2.10			Destination Port*	http		~	
	SGT number:	SGT number. (0-65533)		VLAN ID: VLA	N ID (1	-4096)	Destination Mac Address:	XXXXX.XX	00X.3000X		
	Output Format:	summary	~								
	Start	Clear									
•											
	Output					<b>A</b>					Raw
	Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information MAC Access list						The	trace	er outpu	ıt	

## ةلص تاذ تامولعم

- FIREPOWER يرانلا ديدهتلا دض عافدلا قدايقل يعجرملا ليلدلا
- <u>ماظن رادص إلا المجاهجة ماظن رادص الوح تاظحالم</u>
- من المعني ا
- <u>Cisco Systems</u> <u>تادنتسمل او ينقتل امعدل ا</u>

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