

# ل قبس ملا ئي فصتل ا لماع تاسايس نيوكت اهليغشت و FTD

## تاي وتحمل

[قىدمىقىملا](#)

[قيس اس الاتابلىطتملا](#)

[تابلىطتملا](#)

[قىمدختسملا تانوكمىلا](#)

[قيس اس ا تامولع](#)

[نيوكتلىا](#)

[1 قبس ملا ئي فصتل ا لماع جەن مادختسەرقلەخ](#)

[قيسىئىزلىا ئەطقىنلىا](#)

[2 قبس ملا ئي فصتل ا لماع جەن مادختسەرقلەخ](#)

[يىضارتفالا ققبس ملا ئي فصتل اجەن نم قىقىحتلىا 1. قەممىلا](#)

[قەممىلا تابلىطتم](#)

[لحللا](#)

[نم قىقىحتلىا CLI \(LINA\)](#)

## قىدمىقىملا

دېدەت نع عافدلل ئىقىمىلا ئي فصتل ا تاسايس نيوكت دنتسىملا اذە فصىي (FTD) اهليغشت و.

## قيس اس الاتابلىطتملا

تابلىطتملا

دنتسىملا اذەل ۋەصالىخ تابلىطتم دجوت ال.

## قىمدختسملا تانوكمىلا

ئىيلاتلا ئىداملا تانوكمىلا وجماربىلا تارادصىلىا دنتسىملا اذە يىف ئەدرالا تامولع ملا دنتسىت:

- ASA5506X زىر 6.1.0-195 لغشى يىذلا FTD
- FireSIGHT Management Center (FMC) رادصىلىا لغشى يىذلا 6.1.0-195
- Cisco IOS® 3925 تاچۈم 15.2 لغشى يىتلىا

ئەصالىخ ئىلمۇم ئىيىب يىف ئەدوچوملا ئەزەجألا نم دنتسىملا اذە يىف ئەدرالا تامولع ملا ئاشنە مەت تىناك اذى. (يىضارتىفا) حوسىمەم نيوكتپ دنتسىملا اذە يىف ئەمدختسملا ئەزەجألا عىمەج تاڭىب رىمأ يىأىل لەمتىحملە كەمەف نم دكأتىف، لىيغشتلىا دىقق كەتكەپش.

# ةيسيئر ضارغأ ةثالث مدخلت 6.1 رادصا يف اهلاخدا مت ةزييم يه ةيفصللا لبقة ام ةسإيس:

ةيجرالخ او ةيلخادلا سوفرلا نم لك ىلإ ادانتسا رورملأا ةكرح ةقباطم.

لكشب ريخشلا كرحم زواجتب قفتلل حمسى يذلا ركبملأا لوصولاب مكحتلا ريفوت لمراك

ةأدأ نم اهليحربت مت ييتلا (ACEs) لوصولأا يف مكحتلا تالاخدا بئان رصنعك لمعلأا (ASA).

## نيوكتل

### 1 قبسملأا ةيفصللا لمع جهن مادختسا ةلاح

ادانتسا ةيفصلاب FTD لحمسى ييتلا قفنلا ةداعق عون مادختسا جهنل نكمي، ءلاقملأا هذه ةباتك تقو. ةيجرالخ او ةيلخادلا وأ/او ةيجرالخ IP سأرل يقفنلا رورملأا ةكرح نم لك ىلإ يقفنلا رورملأا ةكرح ريشت:

- ماعلا هيجوتلا نيمضت (GRE)
- IP-in-IP
- IPv6-in-IP
- ذفنم Teredo 3544

روصلأا يف حضوم وه امك قفن كرابتعا يف عرض.



ةيامحلا راج رباع رورملأا ةكرح رمت، قفن مادختساب R2 ىلإ R1 نم لاصتا رابتخا دنع روصولأا يف حضوم وه امك.

1 2016-05-31 02:15:15.10.0.0.1	10.0.0.2	ICMP	138 Echo (ping) request	id=0x0013, seq=0/0,
2 2016-05-31 02:15:15.10.0.0.2	10.0.0.1	ICMP	138 Echo (ping) reply	id=0x0013, seq=0/0,
Frame 1: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)				
Ethernet II, Src: CiscoInc_8d:49:81 (c8:4c:75:8d:49:81), Dst: CiscoInc_a1:2b:f9 (6c:41:6a:a1:2b:f9)				
# Internet Protocol Version 4, Src: 192.168.75.39 (192.168.75.39), Dst: 192.168.76.39 (192.168.76.39) outer				
# Generic Routing Encapsulation (IP)				
# Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.2 (10.0.0.2) inner				
# Internet Control Message Protocol				

روصلأا يف حضوم وه امك يجرالخ IP سأرنم ققحتي هناف، ASA زاهج ةيامحلا راج ناك اذا.

<b>L2 Header</b>	<b>Outer IP Header</b> src=192.168.75.39 dst=192.168.76.39	<b>GRE Header</b>	<b>Inner IP Header</b> src=10.0.0.1 dst=10.0.0.2	<b>L7</b>
------------------	--	-------------------	--	-----------

```
<#root>
ASA#
show conn
GRE OUTSIDE 192.168.76.39:0 INSIDE 192.168.75.39:0
, idle 0:00:17, bytes 520, flags
```

ي حضوم وه امك يلخادلا IP ناونع نم ققحتي هناف، زاهج ئامحلا رادج ناك اذا روصللا.

<b>L2 Header</b>	<b>Outer IP Header</b> src=192.168.75.39 dst=192.168.76.39	<b>GRE Header</b>	<b>Inner IP Header</b> src=10.0.0.1 dst=10.0.0.2	<b>L7</b>
------------------	--	-------------------	--	-----------

تانيبل رورم ئىچ باطم FTD زاهجل نكمي، قبسملار ئيفصتلار لمعاجھن مادختساب ئىچ راخلاو ئيلخادلا سوئرلا نم لك ىلى ادانتسا.

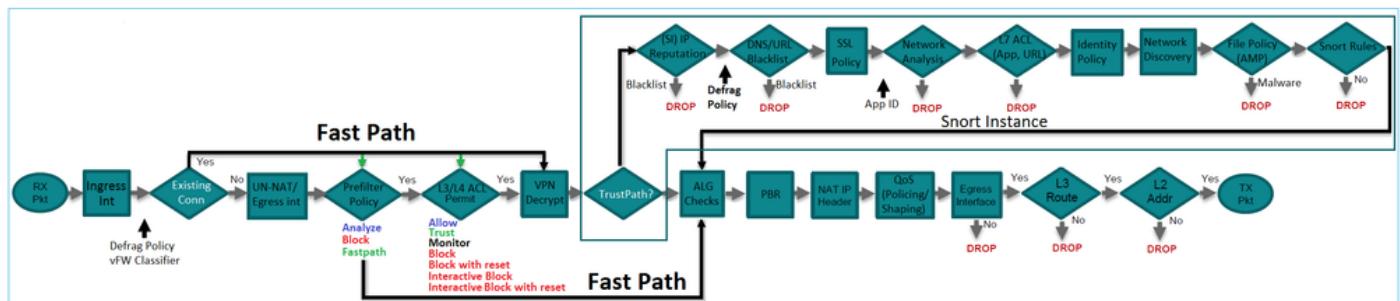
### ئيسىئرلا ئطقنلا

لاثملا يف ييلاتلا	تاكىش
ASA	IP ئىچ راخلا
Snort	ييلخادلا IP
ماظن Firepower Threat Defense	ئاسايىس (Prefilter) + IP ئىچ راخلا (ACP) لوصولا يف مكاحتلا

(FTD)

## 2 قبسملا ةيفرضتلا لماع جهـنـمـاـدـخـتـسـاـةـلـاحـ

لوصولاب مكحـتـلـاـرـيـفـوـتـاهـنـكـمـيـيـتـلـاـPـrـeـFـiـlـeـrـ جـهـنـلـنـكـمـيـةـعـونـمـادـخـتـسـاـةـلـاحـ.ـرـوـصـلـاـيـفـحـضـوـمـوـهـامـكـامـاـتـرـيـخـشـلـاـكـرـحـمـزـوـاجـتـبـقـفـدـتـلـلـحـامـسـلـاوـرـكـبـمـلـاـ.



## يـضـارـتـفـالـاـقـبـسـمـلـاـةـيـفـرـضـتـلـاـجـهـنـنـمـقـقـحـتـلـاـ1ـةـمـمـلـاـ

يـضـارـتـفـالـاـقـبـسـمـلـاـةـيـفـرـضـتـلـاـجـهـنـنـمـقـقـحـتـلـاـ

لـيـضـارـتـفـاـجـهـنـدـجـوـيـ>ـلـوـصـوـلـاـيـفـمـكـحـتـلـاـ>ـتـاسـاـيـسـلـاـىـلـاـلـقـتـنـاـ1ـةـمـمـلـاـ.ـرـوـصـلـاـيـفـحـضـوـمـوـهـامـكـامـاـتـرـيـخـشـلـاـكـرـحـمـزـوـاجـتـبـقـفـدـتـلـلـحـامـسـلـاوـرـكـبـمـلـاـ.

Screenshot of the MikroTik Winbox Policies interface. The top navigation bar shows Overview, Analysis, Policies (highlighted in red), Devices, Objects, and AMP. Below the navigation is a toolbar with Deploy, System, Help, and user info. A sub-menu bar shows Object Management and Access Control. A New Policy button is visible. The main area displays a table for Prefilter Policy. The first row shows "Default Prefilter Policy" with the note "Default Prefilter Policy with default action to allow all tunnels". The second row shows "Domain" as Global and "Last Modified" as 2016-04-22 21:43:25, modified by "admin". Action icons for edit and delete are shown at the end of the row.

ـرـوـصـلـاـيـفـحـضـوـمـوـهـامـكـجـهـنـلـاـتـادـدـعـاـىـرـتـلـرـيـحـتـرـتـخـأـ2ـةـمـمـلـاـ

Overview Analysis Policies Devices Objects AMP Deploy

Access Control > Prefilter Network Discovery Application Detectors Correlation Actions ▾

## Default Prefilter Policy

Default Prefilter Policy with default action to allow all tunnels

Rules

#	Name	Rule T...	Source Interf...	Destin... Interf...	Source Netwo...	Destin... Netwo...	Source Port	Destin... Port	VLAN ...	Action
You cannot add rules to the default Prefilter policy. You can change only default action options.										

Non-tunneled traffic is allowed Default Action: Tunnel Traffic Analyze all tunnel traffic

وە امك لوصولاب مكحتلا جەنب لعفلاب "ةقبس ملا ئىفصىتلار لىماع جەن" قافرا مت. 3. ئوطخلار ۋە روصىلا يىف حضورم.

Overview Analysis **Policies** Devices Objects AMP

Access Control ▶ Access Control Network Discovery Application D

## ACP\_5506-1

Enter Description

Prefilter Policy: [Default Prefilter Policy](#)

Rules Security Intelligence HTTP Responses Advanced

### Prefilter Policy Settings

Prefilter Policy used before access control Default Prefilter Policy

## النماذج المترافقـة (LINA CLI)

<#root>

firepower#

```

show access-list

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
    alert-interval 300
access-list CSM_FW_ACL_; 5 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998:

PREFILTER POLICY:

Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998 (hitcnt=5) 0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any any eq 3544 rule-id 9998 (hitcnt=0) 0xcf6309bc

```

## ةماعل ا مادختساب يقفنلا رورمل ا ةكرح رظح .2

ةمملا تابلطتم

قفن لخاد اهل تاونق عاشنا متي يتلا ICMP رورم ةكرح رظح.

لحلا

ةكرح يرت نأ كنكميـف ،ـذه (ACP) لوصولـا يـف مـكـحتـلـا ةـمـيـاقـ قـيـبـطـتـبـ تـمـقـ اـذـاـ 1ـ.ـ ةـوـطـخـلـاـ رـمـتـ تـنـاكـ اـذـاـ اـمـعـ رـطـنـلـاـ ضـغـبـ ،ـرـوـظـحـمـ (ICMP) تـنـرـتـنـإـلـاـ يـفـ مـكـحتـلـاـ لـئـاسـرـلـوـكـوـتـوـرـبـ رـوـرـمـ عـرـوـصـلـاـ يـفـ حـضـوـمـ وـهـ اـمـكـ ،ـاـلـ مـأـ قـفـنـ رـبـعـ.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Application	Source Po...	Dest Ports	URLs	ISE/SGT Attributes	Action
1	Block ICMP	any	any	any	any	any	any						

<#root>

R1#

ping 192.168.76.39

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.76.39, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

<#root>

R1#

ping 10.0.0.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:

.....  
success rate is 0 percent (0/5)

و ه ان ه قطن مل او . ۋەممەل ا تابىل طتىم ب ئا فولل PreFilter جەن مادختسى كىنكمى ، ئەلا حلا ھ ذە يف يىلاتلار:

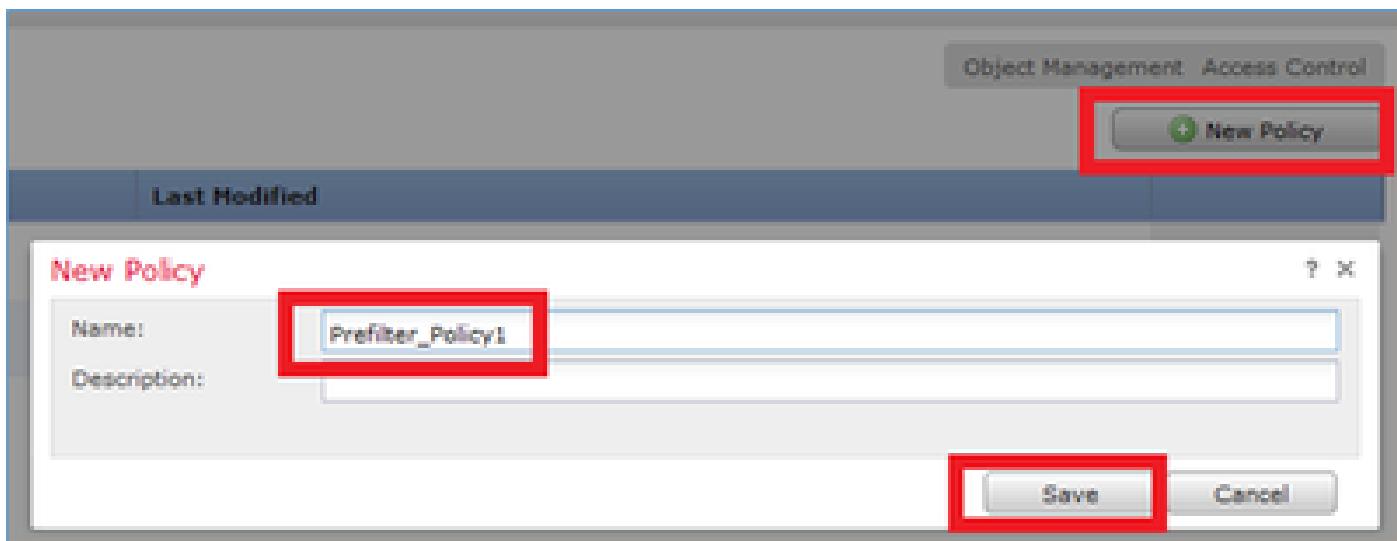
1. لخاد اهن يمىضت مىتى يتلا مزحلا عىمچ زىيىمت.

2. عىنمەت و ئەزمىممەل ا مزحلا قىباطىت يىتلا لوصولار يف مكحتلا ئاسايىس ئاشناب مق.

ۋەممەل ا ئېفصىتلار دعاوق لباقم اھىصف مىتى مزحلا نإف ، ئېرامعەلما ئاسانلىك رظن ئەجۇن مۇقى ارىخأو ، ACP و ئېفصىتلار دعاوق بىطش مىتى Linux (LINA) ، عىم بىسانلىك زاھىج لالخ نەم ئىلۋەل لاصت . طاقسىلل ئەزمىممەل FTD.

يىقىنلار رورمەل ئەكىرەل ئەممالۇ ددھ . 1. ئەوطخلار.

دېدج ئاسايىس ئاشناب مق و > لوصولار يف مكحتلا > تاسايىسلار ئىللىق تىنار ئەرسىلار يف حضۇم وھ امك يىضارىت فالا Prefilter ئەنلىك ئەركىتىنەت ئەنلىك ئەركىتىنەت.



: دعاوقلار نەم نىيۇون دېدھتىب مق ، قېسەملە ئېفصىتلار لىماع جەن يف

1. قىقىنلار ئەدعاق.

2. قېسەملە ئېفصىتلار لىماع ئەدعاق.

يىف اهن يوكت نىكمى امامت ئەفلەت خەتم تازىمەم امەن ئىلۇن ئەتكەنلىك ئەنلىك ئەركىتىنەت ئەنلىك Prefilter.

ئەرسىلار يف حضۇم وھ امك قىقىن ئەدعاق فىيرۇت يىرورپىلار نەم ، ۋەممەل ھ ذەل.

Add Tunnel Rule

Tunnel rules perform early handling of non-encrypted encapsulated traffic, using outer IP headers. Fastpath traffic bypasses access control and QoS.

Name	Tag Tunneled traffic	<input checked="" type="checkbox"/> Enabled	Insert	below rule	1
Action	<input checked="" type="checkbox"/> Analyze		Assign Tunnel Tag	Inside_the_GRE	
2					
<a href="#">Interface Objects</a>   <a href="#">Networks</a>   <a href="#">VLAN Tags</a>   <b>Encapsulation &amp; Ports</b>			<a href="#">Comment</a>   <a href="#">Logging</a>		
Encapsulation Protocols:					
<input checked="" type="checkbox"/> GRE <b>3</b> <input type="checkbox"/> IP-in-IP <input type="checkbox"/> IPv6-in-IP <input type="checkbox"/> Teredo Port (3544)					

تاءاجالاب قلعتي امي في:

عارض إلأ	فصولا
نللخ	نكمي ، اي راي تخا . ريخشلا كرحم ةطساوب قفدتلا نم ققحتلا متي ، دعب لينا . يقفنلا رورملـا ةكرحلـ قـفنـ ةـمالـعـ نـيـيـعـتـ
رـظـحـ	يـجـرـاخـلـاـ سـأـرـلـاـ نـمـ قـقـحـتـلـاـ بـجـيـ . ةـطـسـاـوـبـ قـفـدـتـلـاـ رـظـحـ مـتـ
عيـرسـ رـاسـمـ	كـرحـمـ بـلـاصـتـالـاـ يـلـاـ ةـجـاحـلـاـ نـوـدـ طـقـفـ لـيناـ ةـطـسـاـوـبـ قـفـدـتـلـاـ عـمـ لـمـاعـتـلـاـ مـتـيـ Snortـ

تـامـالـعـلـاـ تـاذـ رـورـمـلـاـ ةـكـرـحـلـ لـوـصـولـاـ يـفـ مـكـحـتـلـاـ ةـسـاـيـسـ دـدـحـ 2ـ وـطـخـلـاـ

ةـمـالـعـ مـادـخـتـسـاـ نـكـمـيـ هـنـأـ إـلـاـ ، ةـيـادـبـلـاـ يـفـ ةـيـاغـلـلـ اـيـهـيـدـبـ نـوـكـيـ نـأـ نـكـمـيـ الـ هـنـأـ نـمـ مـغـرـلـاـ ئـلـعـ > تـاسـاـيـسـلـاـ يـلـاـ لـقـتـنـاـ . رـدـصـمـ ةـقـطـنـمـكـ لـوـصـولـاـ مـكـحـتـلـاـ ةـسـاـيـسـ دـدـعـاـقـ لـبـقـ نـمـ قـفـنـلـاـ وـهـ اـمـكـ زـيـيـمـتـلـاـ تـامـالـعـ تـاذـ رـورـمـلـاـ ةـكـرـحـلـ ICMPـ عـنـمـتـ ةـدـعـاـقـ ئـشـنـأـوـلـوـصـولـاـ يـفـ مـكـحـتـلـاـ .ـرـوـصـلـاـ يـفـ حـضـوـمـ

Policies

ACP\_5506-1

Prefilter Policy: **Prefilter\_Policy1**

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	ISE / SG/T Attributes	Action
1	Block ICMP		any	any	any	any	any	<input checked="" type="checkbox"/> Filter: ICMP	any	any	any	any	
	Default - ACP_5506-1 (-)												

لـوـصـولـاـ يـفـ مـكـحـتـلـاـ جـهـنـبـ دـيـدـجـلـاـ جـهـنـبـ قـافـرـاـ مـتـيـ ؛ـظـحـاـلـمـ

## ققحتل

ىلع طاقتلا CLISH:

```
<#root>
firepower#
show capture

capture CAPI type raw-data trace interface inside [Capturing - 152 bytes]
capture CAPO type raw-data trace interface outside [Capturing - 152 bytes]
```

```
<#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:
```

```
-n
```

لاصتا رابتخا لشف .ديعبلا GRE قفن ئياهن ۋەطقن لاصتا رابتخا لواح، R1 نم:

```
<#root>
```

```
R1#
```

```
ping 10.0.0.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
```

```
.....
```

```
success rate is 0 percent (0/5)
```

هەر ظھمت درلا نأو FTD echo بلىط لوا نأ CLISH طاقتلا رەھظى:

```
<#root>
```

```

Options: -n
18:21:07.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo request
18:21:07.759939 IP 192.168.76.39 > 192.168.75.39: GREv0, length 104: IP 10.0.0.2 > 10.0.0.1: ICMP echo reply
18:21:09.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo request
18:21:11.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo reply
18:21:13.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo request
18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo reply

```

كل ذ طاقتلا دكوفي و:

```

<#root>

>

show capture CAPI | include ip-proto-47

102: 18:21:07.767523 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
107: 18:21:09.763739 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
111: 18:21:11.763769 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
115: 18:21:13.763784 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
120: 18:21:15.763830 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
>
>

show capture CAPO | include ip-proto-47

93: 18:21:07.768133 192.168.75.39 > 192.168.76.39: ip-proto-47, length 104
94: 18:21:07.768438 192.168.76.39 > 192.168.75.39: ip-proto-47, length 104

```

سفن عارج او LINA ASP ل طاقس إلأ تاداع حس و CLISH-engine-debug ةيامح رادج نيكمنتب مق  
ةدعاق ةققاباطمب تمق، Echo-Request، CLISH ايلإ ةبسنلاب هنأ CLISH ءاطخأ حيحصت رهظي. رابتخالا  
دادترالا ئلع درلاب ةصاخلا ACP ةدعاقلو قبسملاءيفصلاتلا لماع

```

<#root>

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0

New session

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0

uses prefilter rule 268434441 with tunnel zone 1

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1 -> -1, 0

icmpType 8, icmpCode 0

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 pending rule order 3, 'Block ICMP', AppId
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0

uses prefilter rule 268434441 with tunnel zone 1

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1 -> -1, 0

icmpType 0, icmpCode 0

```

```

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0
match rule order 3, 'Block ICMP', action Block
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 deny action

```

مزلجا طقس ا Snort نا حضوي:

<#root>

>

show asp drop

Frame drop:

No route to host (no-route)	366
Reverse-path verify failed (rpf-violated)	2
Flow is denied by configured rule (acl-drop)	2

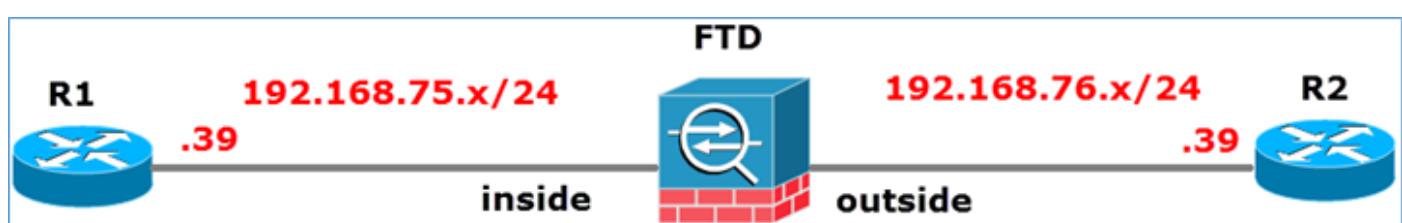
Snort requested to drop the frame (snort-drop)	5
--	---

وهامك اهتقب اطمبا تمق يتلا "Prefilter" سسأوجهن ٽدهاشم كنكمي ، "لاصتا الا ثادحأ" يف ٽروصلالا يف حضوم.

Connection Events (switch workflow)									
Connections with Application Details > Table View of Connection Events									
▶ Search Constraints (Edit Search)									
Jump to... ▾									
First Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Access Control Policy	Access Control Rule	Prefilter Policy	Tunnel/Prefilter Rule
2016-05-21 14:27:54	Block	10.0.0.1	10.0.0.2	8 [Echo Request] / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic
2016-05-21 14:26:51	Block	10.0.0.1	10.0.0.2	8 [Echo Request] / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic
2016-05-21 14:24:52	Block	10.0.0.1	10.0.0.2	8 [Echo Request] / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic
2016-05-21 14:21:07	Block	10.0.0.1	10.0.0.2	8 [Echo Request] / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic
2016-05-21 13:27:04	Block	10.0.0.1	10.0.0.2	8 [Echo Request] / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic
2016-05-21 13:24:36	Block	10.0.0.1	10.0.0.2	8 [Echo Request] / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic
2016-05-21 13:15:26	Block	10.0.0.1	10.0.0.2	8 [Echo Request] / icmp	0 / icmp	ACP_5506-1	Block ICMP	Prefilter_Policy1	Tag Tunneled traffic

## دعاؤق مادختساپ FastPath Prefilter زواجت 3. مهمل

ةكبش للي طي طختلا مسرلا



ةمهملا تابلطتم

1. "لوصولاب مكحتللا جهن" ةدعاق ةفاض او ةيلاحل لوصولاب مكحتللا جهن دعاؤق ةلازاب مق  
لماكلاب رورملا ةكرح عننمت يتلا
  2. يتلا تانايبل رورم ةكرحل Snort Engine زواجتت يتلا Prefilter جهن ةدعاق نويوكتب مق  
192.168.75.0/24.

لحن

وه امك لماكلا ب تانايبل رورم ةكرح عننم يي ذلا لوصولا يف مكحتلا جهن عضومتي . 1. ةوطخلا روصولا يف حضوم.

امك 192.168.75.0/24 ردى ملأ ةكبشل ءاجإك Prefilter عەم ئەدعاق ةفاضاب مق. 2. ئەوطخلاروچىلىكلا يەھىزىمىن وە.

Add Prefilter Rule

Prefilter rules perform early handling of traffic based on simple network characteristics. Fastpathed traffic bypasses access control and QoS.

Name: Fastpath\_src\_192.168.75.0/24    Enabled:

Action:

Interface Objects Networks VLAN Tags Ports Comment Logging

Available Networks: Search by name or value  
any, IPv4-Private-All-RFC1918, any-ipv4, any-ipv6, IPv4-Benchmark-Tests, IPv4-Link-Local, IPv4-Multicast, IPv4-Private-10.0.0.0-8, ...

Source Networks (1): 192.168.75.0/24

Add to Source Add to Destination

Destination Networks (0): any

Enter an IP address Add Enter an IP address Add

روصلایف حضوم وہ امک ۃجیتنلا۔ 3۔ ۃوطخلاء

#	Name	Rule Type	Source Interface Objects	Destination Interface Objects	Source Networks	Destination Networks	Source Port	Destination Port	VLAN 1
1	Fastpath_src_192.168	Prefilter	any	any	192.168.75.0/24	any	any	any	any

Non-tunneled traffic is

رشن و ظفح 4. ۋەتەخلا.

تاھج او نم لىك ىلۇع بېتت مادختساب طاقتلالا نىكىمت:

```
<#root>
firepower#
capture CAPI int inside trace match icmp any any
firepower#
capture CAPO int outside trace match icmp any any
```

لشىف FTD. R1 (192.168.75.39) نم لاصتالا رابتىخا لواح لاصتالا رابتىخا:

```
<#root>
R1#
ping 192.168.76.39
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.76.39, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

حىضوي ئىلخادلا ئەجأولما ىلۇع طاقتلار:

```
<#root>
firepower#
show capture CAPI

5 packets captured
1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: icmp: echo request
```

```
2: 23:35:09.278641 192.168.75.39 > 192.168.76.39: icmp: echo request  
3: 23:35:11.279251 192.168.75.39 > 192.168.76.39: icmp: echo request  
4: 23:35:13.278778 192.168.75.39 > 192.168.76.39: icmp: echo request  
5: 23:35:15.279282 192.168.75.39 > 192.168.76.39: icmp: echo request  
5 packets shown
```

ـ (echo-request) ضورع طاقنلا مهمل ةزيمملا عبـتـتـ

## دس فم (ءارقلا ىلإ زاربإ)

Firepower# show capture CAPI Packet-Number 1

ةمزم 5 طاقتلا مـت

1: 23:35:07.281738 192.168.75.39 > 192.168.76.39: ICMP: ط بـ echo

الرمان: 1

## طاقتل الـا : عونـلـا

## یعرف لا عونل:

## حامسلا: جيتنل

نیوکل

مکالمہ فاضی

اًق مِئَةٍ وَلُوصِيلٍ MAC

الحلقة 2

لوصول اقتصادي: عون

یعرف لا عونل:

حامسلا : جيتنلا

نيوكل

ةيڻمڻ ۽ دعاء

مکالمہ فاضیات

اًق مِئَةٍ وَصَوْلٌ إِلَي MAC

لـ جـ رـ مـ لـ 3

راس ملا ثحب : عونل

## جورخلا ۃج او لح : یعرفلا عونلا

حامسلا: جيتنلا

:نيوكتل

:يفرض اتصالات مولع

جراخ IFC جرخ مدخلتسي 192.168.76.39 ةيلاتل روطخل اىلع روثعلا مت

:ةلحرمل 4

لوصولا ةمهماق: عونلا

لجمسلا: يعرفلا عونلا

حامسلا: جيتنلا

:نيوكتل

access-group CSM\_FW\_ACL\_global

access-list CSM\_FW\_ACL\_Advanced Trust IP 192.168.75.0 255.255.255.0 دعاق يأ id 26843448  
الك ثادحألا لجمس

access-list CSM\_FW\_ACL\_rule-id 26843448: يفرض قناعات لبقة ام جهن prefiler\_policy1

access-list csm\_fw\_acl\_rule-id 26843448: دعاقلا FastPath\_src\_192.168.75.0/24

:يفرض اتصالات مولع

:ةلحرمل 5

عونلا: conn-settings

يعرفلا عونلا:

حامسلا: جيتنلا

:نيوكتل

ةئفل يضارفالا ةطيـخ-ةـئـفـلـا

يأ ئـقـبـاطـم

ةـسـاـيـسـلـاـ\_ـقـمـاعـلـاـ ةـسـاـيـسـلـاـ ةـطـيـخـ

ةـيـضـارـفـالـاـ ةـئـفـلـاـ

ةـمـدـقـتـمـ تـارـايـخـ لـاصـتـالـاـ طـبـصـ UM\_STATIC\_TCP\_MAP

عـيـمـوـمـعـ\_ـp~o~l~i~c~e~\_~s~e~r~v~i~c~e~\_~p~o~l~i~c~y

:يفرض اتصالات مولع

ةلحرملا 6:

عونلا NAT

ةسلج لـ كل يعرفلا عونلا

حامسلا: جيتنلا

: نـيـوكـتـلـا

: ئـيـفـاـضـاـ تـاـمـوـلـعـمـ

ةلحرملا 7:

IP تـارـايـخـ عـونـلـاـ

يـعـرـفـلـاـ عـونـلـاـ

حـامـسـلـاـ: جـيـتـنـلـاـ

: نـيـوكـتـلـا

: ئـيـفـاـضـاـ تـاـمـوـلـعـمـ

ةلحرملـاـ 8:

شيـتـفـتـلـاـ عـونـلـاـ

يـعـرـفـلـاـ np-inspection عـونـلـاـ

حـامـسـلـاـ: جـيـتـنـلـاـ

: نـيـوكـتـلـا

class-map inspection\_default

رورم ةـكـرـحـ يـضـارـتـفـاـ صـحـفـ ةـقـبـاطـمـ

ةـسـاـيـسـلـاـ\_ةـمـاعـلـاـ ةـسـاـيـسـلـاـ ةـطـيـرـخـ

class inspection\_default

صـحـفـ ICMP

يـمـومـعـ policy-service-policy

: ئـيـفـاـضـاـ تـاـمـوـلـعـمـ

ةلحرملـاـ 9:

شيـتـفـتـلـاـ عـونـلـاـ

يـعـرـفـلـاـ np-inspection عـونـلـاـ

حامسلا: جيتنلا

:نيوكتلـا

:ـيـفـاـضـاـ تـاـمـوـلـعـمـ

ـلـحـرـمـلـاـ 10ـ

ـعـونـلـاـ NATـ

ـسـلـجـ لـكـلـ يـعـرـفـلـاـ عـونـلـاـ

حـامـسـلـاـ جـيـتـنـلـاـ

:نيوكتلـاـ

:ـيـفـاـضـاـ تـاـمـوـلـعـمـ

ـلـحـرـمـلـاـ 11ـ

ـتـارـايـخـ عـونـلـاـ IPـ

ـيـعـرـفـلـاـ عـونـلـاـ

حـامـسـلـاـ جـيـتـنـلـاـ

:نيوكتلـاـ

:ـيـفـاـضـاـ تـاـمـوـلـعـمـ

ـلـحـرـمـلـاـ 12ـ

ـقـفـدـتـلـاـ ءـاـشـنـاـ عـونـلـاـ

ـيـعـرـفـلـاـ عـونـلـاـ

حـامـسـلـاـ جـيـتـنـلـاـ

:نيوكتلـاـ

:ـيـفـاـضـاـ تـاـمـوـلـعـمـ

ـيـلـاـتـلـاـ ةـيـطـمـنـلـاـ ةـدـحـوـلـاـ ئـلـاـ ةـمـزـحـلـاـ لـاـسـرـاـ مـتـيـ ،ـ 52ـ فـرـعـمـلـاـ مـاـدـخـتـسـابـ دـيـدـجـ قـفـدـتـ ءـاـشـنـاـ مـتـ

ـلـحـرـمـلـاـ 13ـ

ـلـوـصـوـلـاـ ةـمـئـاقـ عـونـلـاـ

ـلـجـسـلـاـ يـعـرـفـلـاـ عـونـلـاـ

حـامـسـلـاـ جـيـتـنـلـاـ

:نيوكتلـاـ

access-group CSM\_FW\_ACL\_global

access-list CSM\_FW\_ACL\_Advanced Trust IP 192.168.75.0 255.255.255.0 id 26843448 دعاق يأـ لجـسـ اـلـكـ ثـادـحـ أـلـاـ

access-list CSM\_FW\_ACL\_rule-id 26843448 فـصـتـلـاـ لـبـقـ اـمـ جـهـنـ:ـ prefـtـeـrـ\_pـoـlـiـcـyـ1ـ

access-list csm\_fw\_acl\_rule-id 26843448 دـعـاقـلـاـ FastPath\_src\_192.168.75.0/24ـ

فـاـضـاـ تـامـوـلـعـمـ:

ـلـحـرـمـلـاـ 14ـ

ـعـونـلـاـ conn-settingsـ

ـيـعـرـفـلـاـ عـونـلـاـ:

ـحـامـسـلـاـ ـجـيـتـنـلـاـ:

ـنـيـوـكـتـلـاـ:

ـقـفـلـاـ يـضـارـفـالـاـ ـطـيـرـخــقـفـلـاـ

ـيـأـ ـقـبـاطـمـ

ـسـاـيـسـلـاـ ـمـاعـلـاـ ـسـاـيـسـلـاـ ـطـيـرـخــ

ـيـضـارـفـالـاـ ـقـفـلـاـ

ـمـدـقـتـمـ تـارـايـخـ لـاصـتـالـاـ طـبـضـ UM\_STATIC\_TCP\_MAPـ

ـيـمـوـمـ\_p~lic~e~\_service~\_p~lic~e~

ـيـفـاـضـاـ تـامـوـلـعـمـ:

ـلـحـرـمـلـاـ 15ـ

ـعـونـلـاـ NATـ

ـسـلـجـ لـكـلـ يـعـرـفـلـاـ عـونـلـاـ

ـحـامـسـلـاـ ـجـيـتـنـلـاـ:

ـنـيـوـكـتـلـاـ:

ـيـفـاـضـاـ تـامـوـلـعـمـ:

ـلـحـرـمـلـاـ 16ـ

ـعـونـلـاـ IPـ تـارـايـخـ:

ـيـعـرـفـلـاـ عـونـلـاـ

حامسلا :ةجيتنلا

:نيوكتلإا

:ةيفرضإ تامولعم

17 :ةلحرملإا

راسملإا ثحب :عونلإا

جورخلإا ةهجاولج :يعرفلإا عونلإا

حامسلا :ةجيتنلا

:نيوكتلإا

:ةيفرضإ تامولعم

جراخ IFC جرخم مدخلتسى 192.168.76.39 ةيلاتلإا ةوطخلإا ىلع روثعلإا مت

18 :ةلحرملإا

ثحبلا-رواجتلإا :عونلإا

رواجتلإاو ةيلاتلإا ةوطخلإا :يعرفلإا عونلإا

حامسلا :ةجيتنلا

:نيوكتلإا

:ةيفرضإ تامولعم

رواجتلإا طاشن

برضي 140372416161507 ناونع MAC 004.deab.681b ةيلاتلإا ةوطخلل

19 :ةلحرملإا

طاقتلإا :عونلإا

:يعرفلإا عونلإا

حامسلا :ةجيتنلا

:نيوكتلإا

:ةيفرضإ تامولعم

ىلإا لوصولإا ةمئاق MAC

:ةجيتنلا

جراخ: لاخدلإا ةهجاولج

ىلعأـلـ لـاخـ دـالـا ةـلاحـ

ىلـعـأـلـ لـاخـ دـالـا طـخـ ةـلاحـ

جـ رـاخـ جـ اـخـ دـالـا ةـهـجـ اوـ

ىـلـعـأـلـ جـ اـخـ دـالـا ةـلاحـ

ىـلـعـأـلـ جـ اـخـ دـالـا طـخـ ةـلاحـ

حـ اـمـ سـلـاـ عـارـجـ دـالـا

ةـدـحـ اوـ ةـمـزـ حـ ضـرـعـ مـتـ

Firepower#

```
Firepower# show capture capi packet-number 1 trace 5 packet capture 1: 23:35:07.281738
192.168.75.39 > 192.168.76.39: icmp: echo request phase: 1 type: capture subtype: result: allow config: يـفـاضـاـ تـامـولـعـمـ
config: mac access list phase: 2type: access-list subtype: result: allow config: نـعـ ثـحـبـلـ يـعـرـفـلـاـ عـونـلـاـ 3ـ
Implicit rule additional information: mac access phase: 3ـ عـونـلـاـ 3ـ نـعـ ثـحـبـلـ يـعـرـفـلـاـ عـونـلـاـ
config: يـفـاضـاـ تـامـولـعـمـ: نـيـوـكـتـلـاـبـ حـامـسـلـاـ جـوـرـخـلـاـ ةـهـجـ اوـ ةـجـيـتـنـ لـحـ: رـاسـمـلـاـ
config: لـوـصـوـلـاـ ةـمـئـاـقـلـ يـعـرـفـلـاـ عـونـلـاـ 4ـ عـونـلـاـ 4ـ لـحـرـمـلـاـ جـرـاخـ 192.168.76.39ـ ةـيـلـاتـلـاـ
config: نـيـوـكـتـلـاـبـ حـامـسـلـاـ لـجـسـلـاـ ةـجـيـتـنـ
access-group csm_fw_acl_global access-list
csm_fw_acl_advanced trust ip 192.168.75.255.255.55.5 0ـ
جـ هـنـ 268434448ـ ةـدـعـاـقـ ةـظـحـاـلـمـ لـوـصـوـلـاـ ةـمـئـاـقـ نـمـ اـلـكـ
PREFILTER: PreFilter_Policy1 access-list CSM_FW_ACL_LowPriority 268434448ـ
ةـدـعـاـقـلـاـ فـرـعـمـلـ ثـادـحـ لـجـسـ 0ـ 5ـ عـونـلـاـ: CONN-Settings subtype: FastPath_src_192.168.75.0/24ـ
ةـسـايـسـ يـأـ 6ـ قـبـاطـمـ مـدـقـتـمـ لـاصـتـاـ ةـعـوـمـجـمـ
config: class-map class-default options UM_STATIC_TCP_MAP service-policy global_policy
config: تـامـولـعـمـ ةـيـفـاضـاـ تـامـولـعـمـ
config: قـلـحـرـمـلـاـ نـيـوـكـتـلـاـبـ حـامـسـلـاـ ةـجـيـتـنـلـاـ 7ـ عـونـلـاـ: ip-options subtype: قـلـحـرـمـلـاـ ةـيـفـاضـاـ تـامـولـعـمـ
config: قـلـحـرـمـلـاـ نـيـوـكـتـلـاـبـ حـامـسـلـاـ ةـجـيـتـنـلـاـ 8ـ عـونـلـاـ: np-inspection match-class-map_inspection_match
config: يـعـرـفـلـاـ عـونـلـاـ ةـجـيـتـنـ 9ـ عـونـلـاـ: ICMP service-policy
config: يـعـرـفـلـاـ عـونـلـاـ صـحـفـ 10ـ عـونـلـاـ: np-inspection result: Allow config: تـامـولـعـمـ
config: قـلـحـرـمـلـاـ ةـجـيـتـنـلـاـ 11ـ عـونـلـاـ: IP-Options subtype: قـلـحـرـمـلـاـ ةـيـفـاضـاـ تـامـولـعـمـ
config: قـلـحـرـمـلـاـ ةـجـيـتـنـلـاـ 12ـ عـونـلـاـ: قـفـدـتـلـاـ عـاشـنـإـلـ يـعـرـفـلـاـ عـونـلـاـ ةـيـفـاضـاـ تـامـولـعـمـ
config: قـلـحـرـمـلـاـ ةـيـلـاتـلـاـ 13ـ عـونـلـاـ: قـفـدـتـلـاـ عـاشـنـإـلـ يـعـرـفـلـاـ عـونـلـاـ 52ـ فـرـعـمـ مـاـدـخـتـسـابـ دـيـدـجـ قـفـدـتـ عـاشـنـإـ مـتـ
Access-list subtype: log result: allow config: access-group csm_fw_acl_global access-list
csm_fw_acl_advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 268434448 event-log
الـكـ 14ـ عـونـلـاـ: PreFilter_Policy1ـ ةـيـفـصـتـلـاـ لـبـقـ اـمـ جـ هـنــ
access-list CSM_FW_ACL rule-id 268444448ـ ةـدـعـاـقـلـاـ 268434448ـ ةـظـحـاـلـمـ
FastPath_src_192.168.75.0/24ـ
config: نـيـوـكـتـلـاـبـ حـامـسـلـاـ ةـجـيـتـنـلـاـ 15ـ عـونـلـاـ: CONN-Settings subtype: قـلـحـرـمـلـاـ ةـيـفـاضـاـ تـامـولـعـمـ
config: يـعـرـفـ عـونـلـاـ 16ـ عـونـلـاـ: IP-Options subtype: قـلـحـرـمـلـاـ ةـيـفـاضـاـ تـامـولـعـمـ
config: قـلـحـرـمـلـاـ ةـجـيـتـنـلـاـ 17ـ عـونـلـاـ: حـمـسـيـ لـمـعـ ئـسـلـجـ لـكـ لـحـ: لـوـصـوـلـاـ ةـطـقـنـ لـحـ
config: حـمـسـيـ لـحـ: يـعـرـفـلـاـ عـونـلـاـ 18ـ عـونـلـاـ: ةـيـفـاضـاـ تـامـولـعـمـ نـيـوـكـتـلـاـبـ حـمـسـيـ ةـجـيـتـنـ لـوـصـوـلـاـ ةـطـقـنـ
config: ةـلـحـرـمـلـاـ ةـلـعـ روـثـعـلـاـ مـتـ: ةـيـفـاضـاـ تـامـولـعـمـ نـيـوـكـتـلـاـبـ حـمـسـيـ ةـجـيـتـنـ لـوـصـوـلـاـ ةـطـقـنـ
config: يـعـرـفـلـاـ ثـحـبـلـاـ رـواـجـتـلـاـ 192.168.76.39ـ IFCـ جـرـاخـ مـدـخـتـسـيـ 18ـ عـونـلـاـ: ةـلـحـرـمـلـاـ جـرـاخـ
```

## حصوي ةيجرالا ٥٥جاولا لع طاقتلا

<#root>

firepower#

show capture CAPO

10 packets captured

```
1: 23:35:07.282044 192.168.75.39 > 192.168.76.39: icmp: echo request
2: 23:35:07.282227 192.168.76.39 > 192.168.75.39: icmp: echo reply
3: 23:35:09.278717 192.168.75.39 > 192.168.76.39: icmp: echo request
4: 23:35:09.278962 192.168.76.39 > 192.168.75.39: icmp: echo reply
5: 23:35:11.279343 192.168.75.39 > 192.168.76.39: icmp: echo request
6: 23:35:11.279541 192.168.76.39 > 192.168.75.39: icmp: echo reply
7: 23:35:13.278870 192.168.75.39 > 192.168.76.39: icmp: echo request
8: 23:35:13.279023 192.168.76.39 > 192.168.75.39: icmp: echo reply
9: 23:35:15.279373 192.168.75.39 > 192.168.76.39: icmp: echo request
10: 23:35:15.279541 192.168.76.39 > 192.168.75.39: icmp: echo reply
```

10 packets shown

ةطس اوب اهرظح مت نكلو، (52) يلاحلا قفدتلا قباطت اهنأ ةعجترملأا ةمزحلأا عبتت رهظي لوصولأا يف مكحتلا ةممئاق (ACL):

<#root>

firepower#

```
show capture CAPO packet-number 2 trace
```

10 packets captured

2: 23:35:07.282227 192.168.76.39 > 192.168.75.39: icmp: echo reply

## Phase: 1

Type: CAPTURE

**Subtype:**

Result: ALLOW

Result:  
Config:

#### **Additional Information:**

## Additional Info

## Phase: 2

Type: ACCESS-LIST

**Subtype:**

### Result:

Config:  
Implicit Rule  
Additional Information:  
MAC Access List

Phase: 3  
Type: FLOW-LOOKUP  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:

Found flow with id 52, uses current flow

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: DROP

Config:  
access-group CSM\_FW\_ACL\_ global  
access-list CSM\_FW\_ACL\_ advanced deny ip any any rule-id 268434432 event-log flow-start  
access-list CSM\_FW\_ACL\_ remark rule-id 268434432: ACCESS POLICY: ACP\_5506-1 - Default/1  
access-list CSM\_FW\_ACL\_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE  
Additional Information:

Result:  
input-interface: outside  
input-status: up  
input-line-status: up  
Action: drop

Drop-reason: (acl-drop) Flow is denied by configured rule

امك ظجيتنلا .ةدىاعل رورمل ا ةكرحل ئرخأ قبس م ةي فرصت لماع ةدعاق ةفاضاب مق. 5. ةوطخل ا .ةروصل ا يف حضوم و.

#	Name	Role Type	Source Interface Objects	Destination Interface Objects	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action
1	Fastpath_src_192.168. Prefilter	any	any		192.168.75.0/24	any	any	any	any	Fastpath
2	Fastpath_dst_192.168. Prefilter	any	any		any	192.168.75.0/24	any	any	any	Fastpath

زربم ةممهملا طاقنلا) اهارت يتلا ةعجترمل ا ةمزحل ا عبtt نآل ا:

ءارقل ا لىا زارب ا) دس فم)

Firepower# show capture CAPO Packet-2

١٠ طاقتلا مٽ

2: 00:01:38.873123 192.168.76.39 > 192.168.75.39: ICMP echo

:ةلحرملـا 1

طاقتـلا عـونـلـا

يـعـرـفـلـا عـونـلـا

حـامـسـلـا جـيـتـنـلـا

:نـيـوـكـتـلـا

:ةـيـفـاـضـاـ تـاـمـوـلـعـمـ

ىـلـا لـوـصـوـلـا ةـمـئـاـقـ MAC

:ةلحرملـا 2

لـوـصـوـلـا ةـمـئـاـقـ عـونـلـا

يـعـرـفـلـا عـونـلـا

حـامـسـلـا جـيـتـنـلـا

:نـيـوـكـتـلـا

:ةـيـنـمـضـ دـعـاـقـ

:ةـيـفـاـضـاـ تـاـمـوـلـعـمـ

ىـلـا لـوـصـوـلـا ةـمـئـاـقـ MAC

:ةلحرملـا 3

عـونـلـا Flow-lookup

يـعـرـفـلـا عـونـلـا

حـامـسـلـا جـيـتـنـلـا

:نـيـوـكـتـلـا

:ةـيـفـاـضـاـ تـاـمـوـلـعـمـ

يـلـاحـلـا قـفـدـلـا مـدـخـتـسـيـ، 62 فـرـعـمـلـابـ قـفـدـتـ ىـلـعـ رـوـثـعـلـا مـٽـ

:ةلحرملـا 4

لـوـصـوـلـا ةـمـئـاـقـ عـونـلـا

لـجـسـلـا يـعـرـفـلـا عـونـلـا

حامسلا : ةجيتنلا

نيوکٽل

```
access-group CSM_FW_ACL_ global
```

access-list CSM\_FW\_ACL\_ Advanced Trust IP any 192.168.75.0 255.255.255.0 rule-id 26843450  
event-log ایجاد

access-list CSM\_FW\_ACL\_ rule-id 268434450: يفصنلابق ام جن ةظحالم prefiler\_policy1

access-list csm\_fw\_acl\_٥٦٤٣٤٤٥٠ rule-id 268434450: دعاقلٰ: FastPath\_dst\_192.168.75.0/24

مکمل اضافی

لـ ٥

عونل: conn-settings

## يعرف لا عونل:

حاسنلا جيتن

نيوكل

ةيـلـفـلـ يـضـاـرـتـفـالـاـ ةـطـيـخـ-ةـيـلـ

يأٰ قباطم

**ةس اي سلا\_ةم اع لا\_ةس اي سلا\_ة طي رخ**

## ةيضاـرتـفـالـا ةـئـفـلـا

UM\_STATIC\_TCP\_MAP لاصت الا طبض تارايخ دقتم ۆم

عزم\_ي policy-service-policy

مکمل اضافی

الرمان: 6

عونلـا: NAT

## ةسلج لـكـل :يـعـرـفـلـاـعـونـلـا

حاسنلا جيتن

نيوكل

مکالمہ فاضیہ

الحلقة 7

IP تارايخ :عونلما

:يعرفلا عونلما

حامسلما :ةجيتنلما

:نيوكتلما

:ةيفاضا تامولعم

8 :ةلحرملا

راسملما ثحب :عونلما

جورخلا ةهجاولح :يعرفلا عونلما

حامسلما :ةجيتنلما

:نيوكتلما

:ةيفاضا تامولعم

لخادلما نم IFC جرخ مدخلتسن 192.168.75.39 ةيلاتلما ةوطخلما ىلع روثعلما مت

9 :ةلحرملا

ثحبـرواجتلما :عونلما

رواجتلـاو ةيلاتلما ةوطخلما :يعرفلا عونلما

حامسلما :ةجيتنلما

:نيوكتلما

:ةيفاضا تامولعم

رواجتلـا طاشـن

برضـي 140376711128802 نـاونـع MAC ةـيلـاتـلـا ةـوطـخـلـل c84c.758d.4981

10 :ةلحرملا

طاـقـتـلـالـا :عونـلـما

:يـعـرـفـلـا عـونـلـما

حـامـسـلـما :ةـجيـتنـلـما

:نيـوـكـتـلـما

:ةـيفـاضـا تـامـوـلـعم

ىـلـا لـوـصـوـلـا ةـمـئـاـقـ MAC

ةجيتنلا:

لخادل نم :لخادل ٰهجاو

ىلعأ :لخادل ٰلаж

ىلعأ :لخادل طخ ٰلаж

لخادل نم :جارخالا ٰهجاو

ىلعأ :جارخالا ٰلаж

ىلعأ :جارخالا طخ ٰلаж

حامسل :عارجي

```
Firepower# show capture capo packet-number 2 trace 10 packet capture 2: 00:01:38.873123
192.168.76.39 > 192.168.75.39: icmp: echo response phase: 1 type: capture subtype: result: allow
config: mac access list phase: 2 type: access-list subtype: result: allow config:
Implicit rule عونل 3: تامولعم يفاضا: mac access list 3: ةلحرمل 3: Flow-Lookup:
يعرفل عونل 3: ةلحرمل 3: ةلحرمل 3: Allow config: فرعمل امدختساب اهيلع روثعل م: ةيفاضا تامولعم: Access-LIST subtype: log result: allow config: access-group
csm_fw_acl_global access-list csm_fw_acl_advanced trust ip any 192.168.75.0 255.255.255.0
rule-id 2684405 access-list csm_FW_ACL_ rule-id 268434450:
ةداعقل :Prefilter Policy1 access-list CSM_FW_ACL_ rule-id 268434450: ةظحال م
FastPath_dst_192.168.75.0/24: يعرفل عونل 5: CONN-SETTINGS: CLASS-MAP-DEFAULT
يأ قباطم POLICY-MAP_CLASS
JCONFIG: CLASS-MAP-DEFAULT لاصتا لـ ADVANCED-OPTIONS UM_STATIC_TCP_MAP service-policy global_policy
تامولعم حمسى: ةجيتن ةسلج لك: NAT subtype: عون 6: ةلحرمل 6: ةيفاضا تامولعم
تامولعم config: تسلاب حامسل :ةجيتنل 6: IP-OPTIONS: يعرفل عونل 7: ةلحرمل 7: ةيفاضا
حامسل :ةجيتن جورخل ٰهجاو ةلكرشم لح: ROUTE-LOOKUP subtype: عونل 8: ةلحرمل 8: ةيفاضا
مدختسى 192.168.75.39 ةيلاتل ٰوطخل ٰلرع روثعل م: ةيفاضا تامولعم config: تسلاب
ةجيتنو ةيلاتل ٰوطخل ٰرواجتل ٰنفع ثحب ليل يعرفل عونل 9: عونل 9: ةلحرمل لخاد
EGRESS ناونع ةيلاتل ٰوطخل ٰنم طشن رواجتل ٰ: ةيفاضا تامولعم: نيكوتلاب حامسل :رواچتل
ةجيتنل 10: عونل 10: ةلحرمل 10: 14037671128802 برضي c84c.758d.4981
طخ ٰلаж: لخادل ٰهجاو: ةجيتن MAC ىل ٰلوصولا ٰقمي: ةيفاضا تامولعم: نيكوتلاب حامسل
جارخالا طخ عضو: جارخالا طخ عضو: لخادل ٰيف جارخالا ٰلаж: يدعاصتل ٰلخادل ٰطخ عضو: لخادل
حامسل :ىلعأ عارجي
```

## ةحصل نم ققحتل

حيحصل لكشب نيكوتل ٰلمع ديكأتل مسقل ٰاذه مدختسا.

ةلصل ٰا تاذ ماهمل ٰماسقا يف ققحتل ٰفيممع حرش مت دقو.

## اهحالص او عاطخل ٰفاشكتس

نيكوتل ٰاذهل اهحالص او عاطخل ٰفاشكتس ٰال ٰددجم تامولعم ًايلاح رفوتت ال.

## ةلص تاذ تامولعم

انه Cisco Firepower Management Center نيكوت ليلد تارادصا عيمج ىلع روثعلانكمي •

### ن姆 نمآلا ئيامحلا رادج ديدت بع عافدلار قىاثوربعلقىتلىا Cisco

يئرملا ليلدلا اذهب ئاشب Cisco نم (TAC) يملاعلا ئينقتلا ئدعاسملزا زكرم يصوّي •  
نامأ تايىنقت لوح ئقمعتملا ئيلمعلا ئفرعملى Cisco Firepower،  
ئلاقملزا هذه يف ئروكذملاتايىنقتلا نمضتت يتلا او

### FirePOWER (FTD) نم Cisco ديدت دض عافدلار

اھالص او ئينقتلا تاظحالملما ئاطخا فاشكتساو ئئيهتلا تايىلمع عيمج •

### ن姆 نمآلا ئيامحلا رادج قرادا زكرم Cisco

• تادنتسملاو ئينقتلامعدىلا Cisco Systems

## هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ  
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ  
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ  
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ  
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ  
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).