

اھالص او ۋەكپىشلە ئاطخاً فاشكىتسال FirePOWER

تايىوت حملە

[قىدەقەملى](#)

[قىساسىلارنى باىلەتتەملى](#)

[باىلەتتەملى](#)

[قىمدىخسەنلىكەنەنوكەملى](#)

[قىساسىاتامولۇم](#)

يىلاتلارلىچىلارنىم قىامىحلى رادج تاجتنىم ۋە مەجمۇلۇ روصۇمىجىت كېنگىمى فىرىك
؟اھرىدىصەت و (NGFW)

[طاقتلى ئىمەجىت FXOS](#)

[طاقتلى تايىلمۇع ئىمەجىت و نىكىمەت FTD Lina](#)

[لېرىۋە ئاطقۇلۇ ئىمەجىت و نىكىمەت FTD](#)

[اھالص او ئاطخاً فاشكىتسا](#)

جورخىلار قەچىۋىلىق TCP SYN دجوىلى 1. قىلاخلى

[رسالىلىخەت](#)

[اھبىصىوەملىكەنەن ئەئارەجىلار](#)

[اھبىصىوەملىكەنەن ئەئارەجىلار بابسىلارنى خىلەم](#)

لەدان نىم TCP RST لېرىمع نىم 2. قىلاخلى

[رسالىلىخەت](#)

[اھبىصىوەملىكەنەن ئەئارەجىلار](#)

فەدەو قىامىن قەطقۇن نىم TCP 3-way + RST 3. قىلاخلى

[رسالىلىخەت](#)

[لېرىمەلەنەن قەلچۈملى ئەفەن ئەۋزىلا - 3.1 - TCP 3-way + RST](#)

[اھبىصىوەملىكەنەن ئەئارەجىلار](#)

[لېرىمەلەنەن قەلچۈملى ئەدەملىكەنەن ئەۋزىلا + TCP + RST لەجاتالا ئەپىتالىڭ ئەفەن ئەۋزىلا - 3.2](#)

[اھبىصىوەملىكەنەن ئەئارەجىلار](#)

[لېرىمەلەنەن قەلچۈملى ئەفەن ئەۋزىلا - 3.3 - TCP 3-way + RST](#)

[اھبىصىوەملىكەنەن ئەئارەجىلار](#)

[مەداخىل ئەنەن ئەرۋەلە ئەپىتالىڭ ئەفەن ئەۋزىلا - 3.4 - TCP + RST](#)

[اھبىصىوەملىكەنەن ئەئارەجىلار](#)

لېرىمەلەنەن 4. TCP RST 4. قىلاخلى

[رسالىلىخەت](#)

[اھبىصىوەملىكەنەن ئەئارەجىلار](#)

(1) وېرەنیسلىك TCP لۆكوتوربىل ئەي طبلىلىقنىلا 5. قىلاخلى

[عېي طبلىلىقنىلا - 1 وېرەنیسلىك](#)

[رسالىلىخەت](#)

[اھبىصىوەملىكەنەن ئەئارەجىلار](#)

[عېيرسلىلىقنىلا - 2 وېرەنیسلىك](#)

(2) وېرەنیسلىك TCP لۆكوتوربىل ئەي طبلىلىقنىلا 6. قىلاخلى

[رسالىلىخەت](#)

[اھبىصىوەملىكەنەن ئەئارەجىلار](#)

لەپەن ئەلەكشىم 7. طېرچىخ لېپاقم لەخەملى ئەنېب تېقلى ئەرقىف نىم قىقىخت طاقتلى ئەرىدىصەت
[قەمۈزىلە فەلتىن](#)

[رسأليحة](#)
[اهبىصومناتاعارجالا](#)

[قدوق فملا مزحلا \(UDP لاصتا قلخش 8. قلاحلا\)](#)

[رسأليحة](#)
[اهبىصومناتاعارجالا](#)
[رسأليحة](#)
[اهبىصومناتاعارجالا](#)

[\(2\) ويرانيسلا \(HTTPS لاصتا قلخش 10. قلاحلا\)](#)

[رسأليحة](#)
[اهبىصومناتاعارجالا](#)
[رسأليحة](#)
[اهبىصومناتاعارجالا](#)

[ميست\) عطقتملا ليصوتلا قلخش 12. قلاحلا \(ARP\)](#)

[رسأليحة](#)
[اهبىصومناتاعارجالا](#)
[قدجو عاطخأ روهوظي في ببس تيبل \(OIDs\) SNMP نياك تافرعم ىلع فرعتلا 13. قلاحلا \(CPU\)](#)
[رسأليحة](#)
[اهبىصومناتاعارجالا](#)

قلص تاذ تامولع

ةمدقملا

فاشكتسا ىلإ فدهت مزحلا طاقتلاا ةفلتخم ليحهت تايونقت دنتسملا اذه فصي
ةيلعافب اهحالص او ةكبشلا تالكشم.

ةيساسألا تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملا ةفرعم كيدل نوكت نأب Cisco يصوت:

- يساسألا ماظنلا ةينب Firepower
- NGFW تالجس
- NGFW Packet-tracer

هذه ةيبلت ةدشب نسحتسملا نم ،مزحلا طاقتلا ليحهت يف عدبلا لباق ،كلذ ىلإ ةفاضيلاب
تابلطتملا:

- ةيفيك مهفت مل اذا ةمزح طاقتلا نم ققحتلا يف أدبت ال - لوكتوربلا ةيلمع فرعت
- هيلع ئاليتسالا مت يذلا لوكتوربلا لمع
- انكمم اذه نكي مل اذا .ةياهن ىلإ ةياهن نم لقنا ةزهجأ فرعت نأ بجي - ططخملا فرعت
- قفتلار مدخل نم تانايبلأا قفت ةزهجأ ةفرعم لقا ىلع كيلع بجي فيف
- ةينعملما تاهجاولا يه امو ،مزحلل كزاهج ةجلام ةيفيك فرعت نأ بجي - زاهجلا ىلع فرعت
- ةفلتخملما طاقتلاا طاقن يه امو ،زاهجلا ةينب يه امو ،(جورخلالوخدلا)
- امي ف زاهجلا ةطساوب ةمزحلا قفت عم لماعتلا ةيفيك فرعت نأ بجي - نيوكتلا فرعت
- بـ قلعيتي

جورخلالا/هيجوتلا ةهجاو

- ۋەقىبى طەملى تاسىسىلار
- ۋەكىبىشلى ناونۇن ۋەمجرىت (NAT)
- ۋېيىبى طەتل ۋەزەج نوكت نأب ئىصو، طاقىتلالا تايىلمۇ بىناجاب - ۋەحاتىملى تاودالا فەرعت اھىطىرىپ مەق، رەمألا مەزلى اذاؤ (رەڭألا عېتتۈلىجىستىلا لىثم) ئىرخألا تايىنقتىلار و تاودالا اھىطاقىتلار مەت يىتىلا مېزىلاب.

ۋەمدىختىسىمىلى تانوكمىلى

ۋەيىلاتلا ۋېيىدالا تانوكمىلار جەنمەرپىلا تارادىصىلى دەنتسىت دەنامولۇمىلى تامىلۇنى دەنتسىت:

- 6.5.x. رادىصىلا FTD جەمانرب لەغىشى يىذلا FP4140 ىلى تاھۇرانىسىلى مۆظۇم دەنتسىت.
- 6.5.x. رادىصىلا FMC لەيغىشىت جەمانرب.

ۋەصالىخ ۋەقىبى ۋەزەج ئەلەن نەم دەنتسىمىلى اذە يىف ۋەدرەوەلە تامىلۇنى ئاشىندا مەت تەنەك اذا. (يىضارتىف) حەسەممە نىيوكىتىپ دەنتسىمىلى اذە يىف ۋەمدىختىسىمىلى ۋەزەج ئەلەن ئەيمەج تأدب رەمأ يىلەنەتتەمەنلا رېيىتەتلىك كەمەف نەم دەكأتىف، لەيغىشىتىلا دېق كەتكەپش.

ۋېيىساساً تامىلۇم

ايىمەي. موپىلى ۋەرفوتىملى الامە رەڭكەنلەنەن اھىالىسى او ئەاطەخەنلەنەن فاشكەتسەن ئەۋەدە دەح و ۋەقىزەلە طاقىتلە.

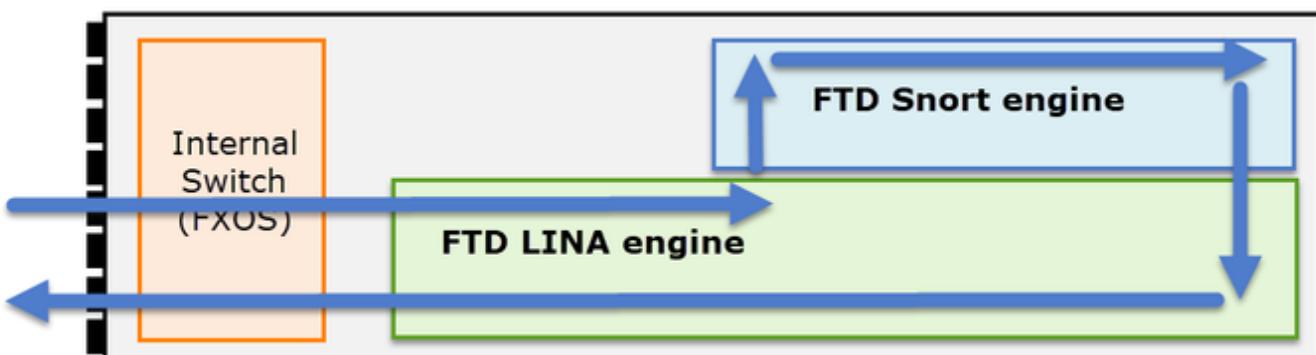
ۋەكىبىشلى لەكاشىم دېدەت يىف ناماملا او ۋەكىبىشلى يىسدنەم ۋەدعاسم و ۋە دەنتسىمىلى اذە نەم فەدەلە. اساساً مېزىلە طاقىتلە لەپەلىخ ىلى ادانىتسا اھىالىسى او اھىئەاطەخەنلەنەن فاشكەتسەن او ۋەعىئەشلى.

تەھۋوش يىقىقىح مەدىختىسىم تالاچ ىلى دەنتسىمىلى اذە يىف ۋەمدەقىملى تاھۇرانىسىلى ئەيمەج دەنتسىت ئەينقىتلە Cisco نەم (TAC).

نەم (NGFW) يىلاتلا لېجىلا ئەيامح رادىج رەظن ۋەجەن نەم ۋەقىزەلە طاقىتلە تايىلمۇ دەنتسىمىلى يىطەغىي ااضىيأ ئىرخألا ۋەزەج ئەلەن ئەۋەنأ ىلىع مېھافىملى سەفن قىيىبەطت مەتى نەكلە، Cisco.

ۋېيىامەلە رادىج تاجىتنەم ۋەعومنەم ىلىع رووصى عەيمەجت كەنکەمەي فېيىك ؟ اھىرىدىصىت و (NGFW) يىلاتلا لېجىلا نەم

ۋەقىبەطت (FirePOWER Threat Defense (FTD) FirePOWER Threat Defense (FTD) نامام زاھىج ۋەلەخ يىف رووصىلا يىف حەضۇم و ۋە امك ۋەقىزەلە ۋەجلەعەم ضرۇنەكمىي،



- لکیهـلـل يـلـخـادـلـا لـوـحـمـلـا ةـطـسـاـوبـ اـهـجـلـاعـمـ مـتـيـوـلـوـخـدـلـا ةـهـجـ اوـ ةـمـزـحـلـا لـخـدـتـ.
2. L3/L4 نـمـ قـقـحـتـلـابـ اـسـاسـأـ مـوـقـيـ يـذـلـا FTD Lina كـرـحـمـ ىـلـا ةـمـزـحـلـا لـخـدـتـ.
 3. (يـسـاسـأـ لـكـشـبـ L7 صـحـفـ) snort كـرـحـمـ ةـطـسـاـوبـ ةـمـزـحـلـا صـحـفـ بـلـطـتـيـ جـهـنـلـا نـاكـ اـذـاـ.
 4. ةـمـزـحـلـلـ اـمـكـ رـيـخـشـلـا كـرـحـمـ عـجـرـيـ.
 5. رـارـقـ ىـلـعـ ئـانـبـ اـهـهـيـجـوـتـ ةـدـاعـاـ وـاـ ةـمـزـحـلـا طـاقـسـاـبـ LINA كـرـحـمـ مـوـقـيـ Snort.
 6. يـلـخـادـلـا لـكـيـهـلـا لـوـحـمـ لـالـخـ نـمـ لـكـيـهـلـا بـيـكـرـتـ ىـلـعـ ةـمـزـحـلـا لـمـعـتـ.

يـفـ "ـعـرـسـلـا قـئـافـ لـاـسـرـالـا جـمـانـرـبـ" طـاقـتـلـا نـكـمـيـ، حـضـوـمـلـا ةـيـنـبـلـا ىـلـا اـدـانـتـسـاـ فـلـتـخـمـ نـكـامـأـ (3) ةـثـالـثـ:

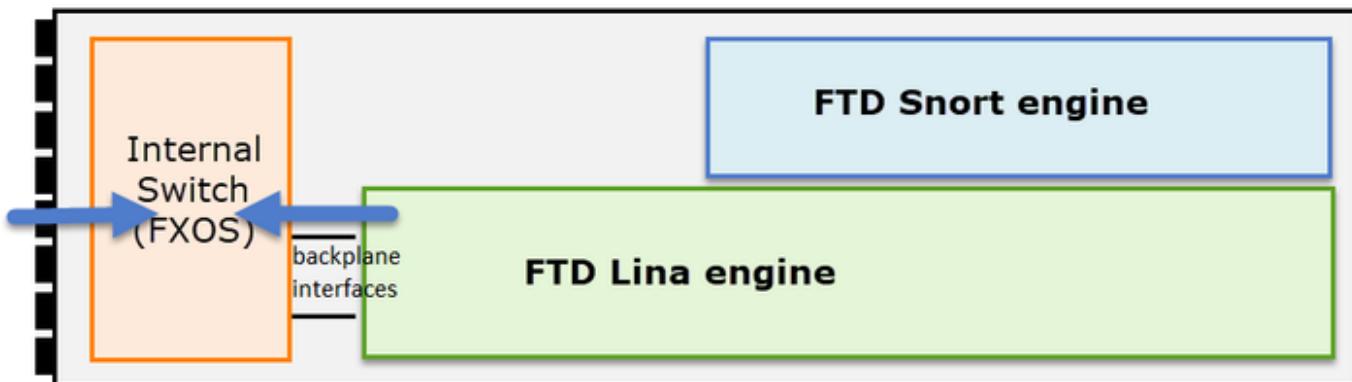
- FXOS
- FTD Lina كـرـحـمـ
- رـيـخـشـ كـرـحـمـ FTD

طـاقـتـلـا FXOS عـيـمـجـتـ

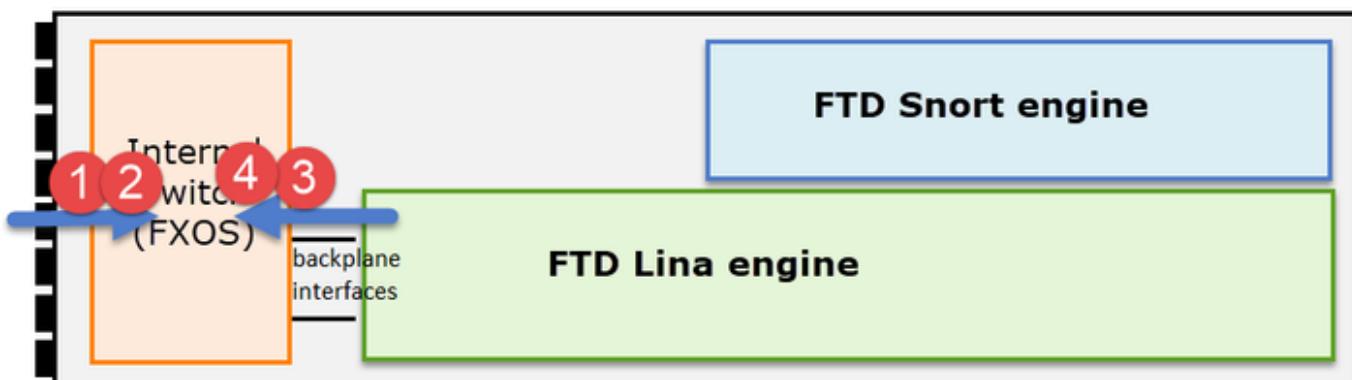
دـنـتـسـمـلـا اـذـهـ يـفـ ةـيـلـمـعـلـا فـصـوـمـتـيـ:

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos271/web-guide/b_GUI_FXOS_ConfigGuide_271/troubleshooting.html#concept_E8823CC63C934A909BBC0DF12F

يـفـ رـهـظـتـ يـلـخـادـلـا لـوـحـمـلـا ضـرـعـ ةـطـقـنـ نـمـ لـخـدـمـلـا هـاجـتـاـ يـفـ ذـخـؤـتـ نـأـ طـقـفـ FXOS طـاقـتـلـا نـكـمـيـ انـهـ ةـرـوـصـلـاـ.



يـلـخـادـلـا لـوـحـمـلـا ةـيـنـبـ بـبـسـبـ) هـاجـتـاـ لـكـلـ طـاقـتـلـا اـتـطـقـنـ نـاتـاهـ، انـهـ حـضـوـمـ وـهـ اـمـكـ.



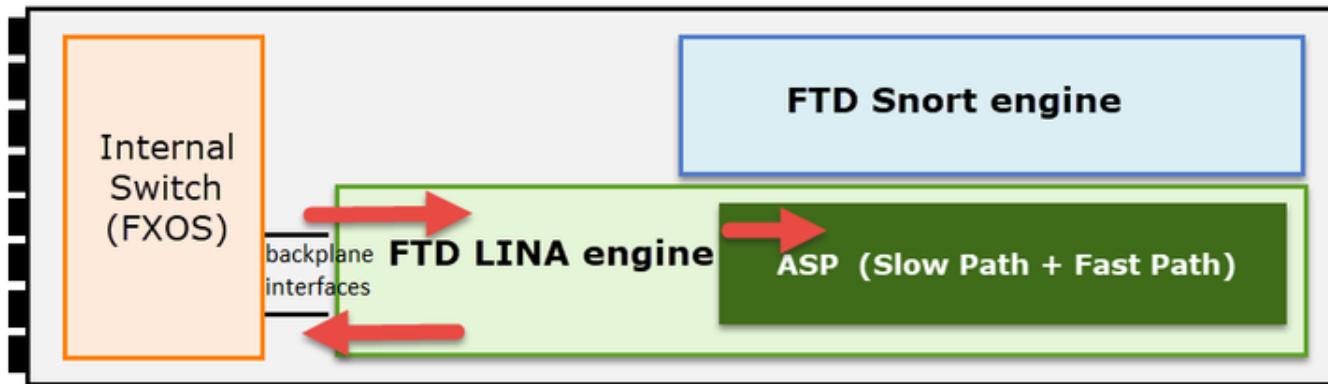
ةيرهاظ ةكبش ۆممالع 4 و 3، 2 طاقنلا يف ۆطقتلملما مزحلا نمضتت (VNTag).

ئياسنالا ۆمظنالا ىلع طقف FXOS ماظنب لکيەلما ىوتسم طاقتلا رفووت: ئەظحالم FP41xx و FP93xx و FP1xxx و FP21xx رفووت ال.

طاقتلا تايىلمۇ عيمجتۇنىكىمت

ةيسىئرلا طاقتلالا طاقن:

- لۇخدلا ۆھجاو
- جورخلا ۆھجاو
- عىرسلا نامالا راسم (ASP)



مدىتسىم ۆھجاو Firepower Management Center (FMC) ب ۆصالخا مدىتسىملا ۆھجاو مادختسى كىنكمىت ب ۆصالخا طاقتلالا تايىلمۇ عيمجتۇنىكىمتل FTD ب ۆصالخا (CLI) رماؤلار طس ۆھجاو وأ FTD Lina.

ئىلىخادلار ۆھجاولارا ىلع CLI نم طاقتلالا نىكىمت:

```
<#root>
firepower#
capture CAPI interface INSIDE match icmp host 192.168.103.1 host 192.168.101.1
```

الك يف 192.168.101.1 و 192.168.103.1 نىب رورملار ئەقاباطتىي نىيەجتالا.

كرح ئەطاقسىمىت يىتلارا مزحلا عيمج ئىۋرىل ASP طاقتلا نىكىمت:

```
<#root>
firepower#
capture ASP type asp-drop all
```

مدادخ لىا FTD طخ طاقتلارا ريدىصت:

```
<#root>
firepower#
copy /pcap capture:CAPI ftp://ftp_username:ftp_password@192.168.78.73/CAPI.pcap
```

مدادخ لىا TFTP طخ طاقتلارا ريدىصت:

```
<#root>
firepower#
copy /pcap capture:CAPI tftp://192.168.78.73
```

FMC مدختسىم ۋەجى او نم FTD Lina تاungomg عىمچتۇنىكىمەت كىنكمى ، FMC 6.2.x رادىصى نم اىدەپ يەو، FMC لېبىق نم ھەترادا مەتت ئىامح رادىج نم FTD تاطقىل عىمچتلىرىخا ۋەقىرەت كانە:

1 ۋەطخىلا

صرق لىا طاقتلالا خسنا طاقتلالا ASP و أ لاح يف FTD.

```
<#root>
firepower#
copy /pcap capture:capin disk0:capin.pcap

Source capture name [capin]?

Destination filename [capin.pcap]?
!!!!
```

2 ۋەطخىلا

عقومىلىا ھەخسنا مىث ، ظوفحەملە طاقتلالا ناكىم دەحۋو، رېبىخلا عضولىا لىقتىنى /ngfw/var/shared:

```
<#root>
firepower#
Console connection detached.

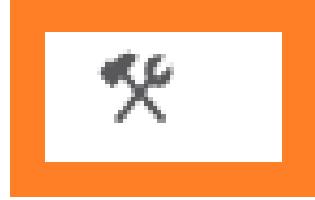
>
```

expert

```
admin@firepower:~$  
sudo su  
Password:  
root@firepower:/home/admin#  
cd /mnt/disk0  
root@firepower:/mnt/disk0#  
ls -al | grep pcap  
-rwxr-xr-x 1 root root    24 Apr 26 18:19 CAPI.pcap  
-rwxr-xr-x 1 root root 30110 Apr  8 14:10  
capin.pcap  
-rwxr-xr-x 1 root root   6123 Apr  8 14:11 capin2.pcap  
root@firepower:/mnt/disk0#  
cp capin.pcap /ngfw/var/common
```

3 ۋەطخىلا

لۇقىت و FTD لوكوت ورب رىدىت يىتلا (FMC) ئارادىلا يې مكحىتلىا دەحۋىلىا لىخدىلا لىجىستېب مۇق اھحالىص او ئاطاخ ئالا فاش كىتسا ئەنۋىقىأ دەحۋى FTD زاھىع قۇم دەح .زەھج ئالا ئارادى > زەھج ئالا لىلإ



4 ۋەطخىلا

مۇدقىت مەللا اھحالىص او ئاطاخ ئالا فاش كىتسا دىدەت:

CISCO Firepower Management Center
System / Health / [Health Monitor Appliance](#)

Overview Analysis Policies

Health Monitor

	Appliance
!	mzafeiro_FP2110-2

[Generate Troubleshooting Files](#)

[Advanced Troubleshooting](#)

لېزنت ددھو طاقتلالا فلم مسما ددھ:

Firepower Management Center
System / Health / AT File Download

Overview Analysis Policies Devices Objects AMP Intelligence

Advanced Troubleshooting

mzafeiro_FP2110-2

File Download Threat Defense CLI Packet Tracer Capture w/Trace

File

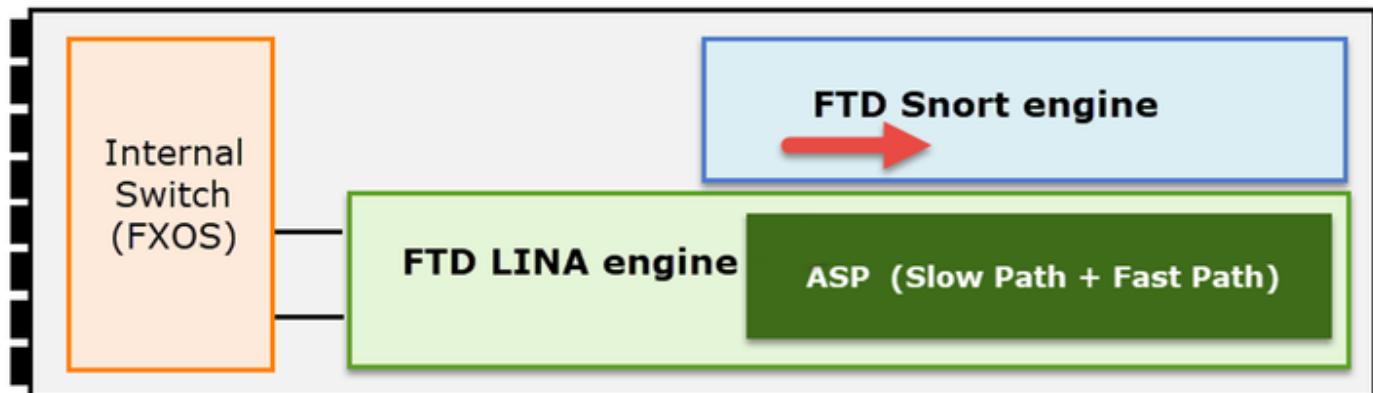
[Back](#) [Download](#)

مدىتسنم ةهجاو نم طاقتلالا عي مجت/نيكمت ةيفيك لوح ئلثممألا نم ديزم ىلع لوصح لىل دنتسملاب اذه نم ققحت،

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html>

ل بيو تاطقل عي مجتو نيكمنت FTD

انه ئروصلاب يف طاقتلالا ئطقن رهظت.



ىوتسم طاقتلا نيكمت:

```
<#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 host 192.168.101.1
```

دىع ب م داخ ىل ا FTP لالخ نم خسنو capture.pcap مساب فلم ىل ا طاقتلا ا ئباتكىل:

```
<#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:
-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.
```

>

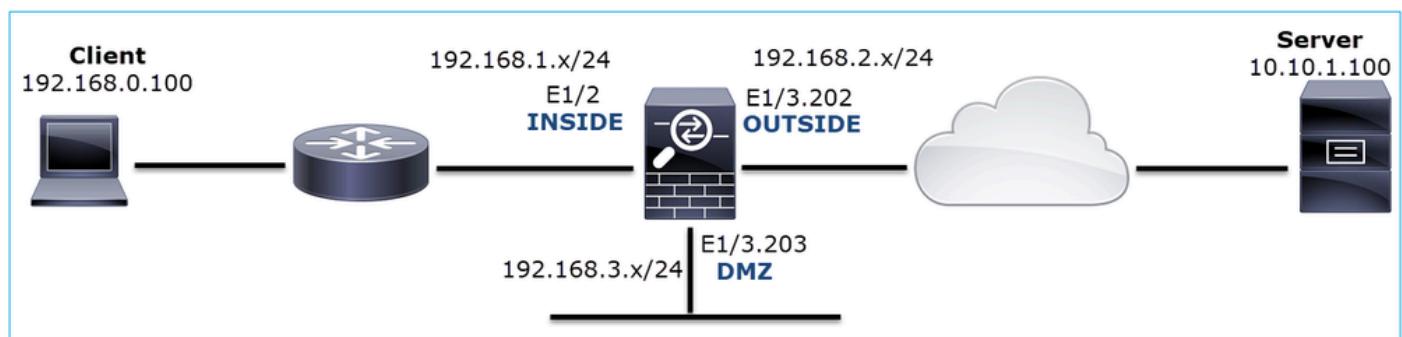
طااقتلا ةيفرضت لمامع نمضتت يتلار ياخشلا ىوتسم ىلع طاقتلala ئلثمأ نم ديزمل دنتسمل اذه نم ققحت ئفلىت خ:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html>

اھالص او ئاطخالا فاشكتسا

جورخلا ئهنج او ىلع TCP SYN دجوی ال 1. ئلاحلا

انه ئروصلا يف حضوم ططخملا:



لمعي ال HTTP ئلکشملا فصو

رثأتملار قفتلار:

SRC IP: 192.168.0.100

لوكوتورب DST IP: 10.10.1.100

لوكوتورب TCP 80 لوكوتوربلا

رسأليلح

لارجم ىلع طاقتلala FTD LINA:

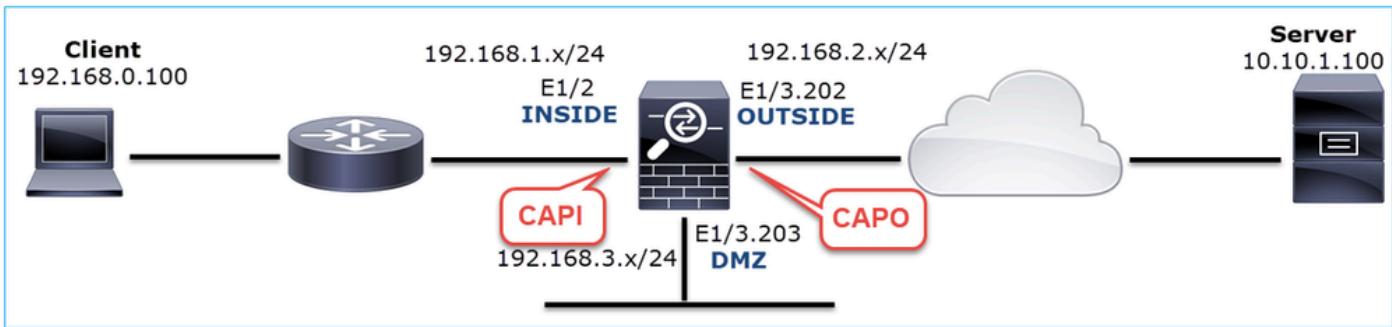
```
<#root>
```

```
firepower#
```

```
capture CAPI int INSIDE match ip host 192.168.0.100 host 10.10.1.100
```

```
firepower#
```

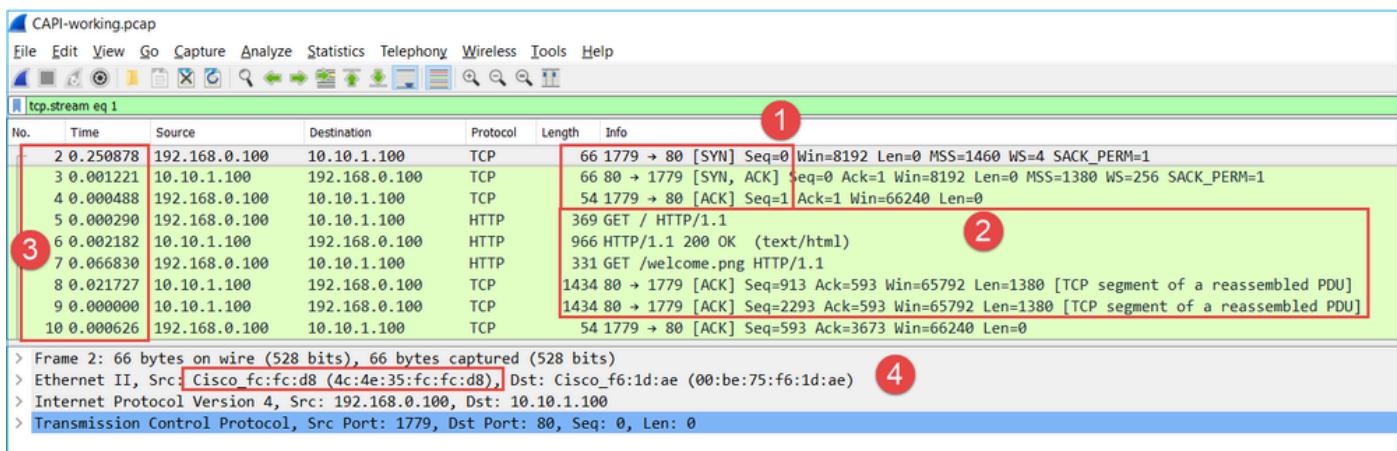
```
capture CAPO int OUTSIDE match ip host 192.168.0.100 host 10.10.1.100
```



يـفـيـظـوـلـا ويـرـانـيـسـلـا - طـاقـتـلـا:

يـفـيـظـوـلـا ويـرـانـيـسـلـا نـم تـاطـقـلـلـا لـعـلـصـحـتـنـا اـمـئـادـدـجـ دـيـفـمـلـا نـم ،سـاسـأـ طـخـكـ.

ةـرـوـصـلـا يـفـ حـضـوـمـلـا وـحـنـلـا لـعـلـهـجـ اوـ طـاقـتـلـا مـتـيـ:



ةـيـسـيـئـرـلـا طـاقـنـلـا:

1. ٤ـهـفـاصـمـ TCP 3-way.
2. ٥ـاـجـتـإـلـا يـئـانـثـ تـانـاـيـبـلـا لـدـابـتـ.
3. (مـزـحـلـا نـيـبـ تـقـوـلـا قـرـفـ إـلـا اـدـانـتـسـا) مـزـحـلـا نـيـبـ تـارـيـخـأـتـ دـجـوتـ الـ).
4. تـانـاـيـبـلـا قـفـدـتـلـ حـيـحـصـلـا زـاهـجـلـا وـهـ رـدـصـمـلـا.

انـهـ ةـرـوـصـلـا يـفـ لـ ةـيـجـرـاخـلـا ةـهـجـاـولـا طـاقـتـلـا ضـرـعـ مـتـيـ:

CAPO-working.pcap

No.	Time	Source	Destination	Protocol	Length	Info
2	0.2500787	192.168.0.100	10.10.1.100	TCP	70	1779 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
3	0.000534	10.10.1.100	192.168.0.100	TCP	70	80 → 1779 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	0.000564	192.168.0.100	10.10.1.100	TCP	58	1779 → 80 [ACK] Seq=1 Ack=1 Win=66240 Len=0
5	0.000534	192.168.0.100	10.10.1.100	HTTP	373	GET / HTTP/1.1
6	0.001663	10.10.1.100	192.168.0.100	HTTP	970	HTTP/1.1 200 OK (text/html)
7	0.067273	192.168.0.100	10.10.1.100	HTTP	335	GET /welcome.png HTTP/1.1
8	0.021422	10.10.1.100	192.168.0.100	TCP	1438	80 → 1779 [ACK] Seq=913 Ack=593 Win=65792 Len=1380 [TCP segment of a reassembled PDU]
9	0.000015	10.10.1.100	192.168.0.100	TCP	1438	80 → 1779 [ACK] Seq=2293 Ack=593 Win=65792 Len=1380 [TCP segment of a reassembled PDU]

```

> Frame 2: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Cisco_f6:1d:8e (00:be:75:f6:1d:8e), Dst: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8) 2
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 202
> Internet Protocol Version 4, Src: 192.168.0.100, Dst: 10.10.1.100
> Transmission Control Protocol, Src Port: 1779, Dst Port: 80, Seq: 0, Len: 0

```

ةيسيئرلا طاقنل:

1. طاقتلا يف ةدوجوملا تانايبل سفن CAPI.
2. MAC حيحصلاب عبنملاب زاهج و هجولا.

لمعی ال ويرانیس - طاقتلا

لکشل اذهب روصلاب دبت، زاهجلاب ةصاخلا (CLI) رمأولاب رطس ةهجاولالخ نم:

```
<#root>
```

```

firepower#
show capture

capture CAPI type raw-data interface INSIDE
[Capturing - 484 bytes]

match ip host 192.168.0.100 host 10.10.1.100
capture CAPO type raw-data interface OUTSIDE

[Capturing - 0 bytes]

match ip host 192.168.0.100 host 10.10.1.100

```

تايويتحم CAPI:

```
<#root>
```

```

firepower#
show capture CAPI

6 packets captured

1: 11:47:46.911482 192.168.0.100.3171 > 10.10.1.100.80:
s

```

```
1089825363:1089825363(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
 2: 11:47:47.161902 192.168.0.100.3172 > 10.10.1.100.80:
```

s

```
3981048763:3981048763(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
 3: 11:47:49.907683 192.168.0.100.3171 > 10.10.1.100.80:
```

s

```
1089825363:1089825363(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
 4: 11:47:50.162757 192.168.0.100.3172 > 10.10.1.100.80:
```

s

```
3981048763:3981048763(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
 5: 11:47:55.914640 192.168.0.100.3171 > 10.10.1.100.80:
```

s

```
1089825363:1089825363(0) win 8192 <mss 1460,nop,nop,sackOK>
 6: 11:47:56.164710 192.168.0.100.3172 > 10.10.1.100.80:
```

s

```
3981048763:3981048763(0) win 8192 <mss 1460,nop,nop,sackOK>
```

<#root>

firepower#

show capture CAPO

0 packet captured

0 packet shown

يەف CAPI طاقتلال ۆروص ھە

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.100	10.10.1.100	TCP	66	3171 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.250420	192.168.0.100	10.10.1.100	TCP	66	3172 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
3	2.745781	192.168.0.100	10.10.1.100	TCP	66	[TCP Retransmission] 3171 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
4	0.255074	192.168.0.100	10.10.1.100	TCP	66	[TCP Retransmission] 3172 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
5	5.751883	192.168.0.100	10.10.1.100	TCP	62	[TCP Retransmission] 3171 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
6	0.250070	192.168.0.100	10.10.1.100	TCP	62	[TCP Retransmission] 3172 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II Src: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8) Dst: Cisco_f6:1d:ae (00:be:75:f6:1d:ae)
Internet Protocol Version 4, Src: 192.168.0.100, Dst: 10.10.1.100
Transmission Control Protocol, Src Port: 3171, Dst Port: 80, Seq: 0, Len: 0

يەسیئرلا طاقنلا:

(هاجتەللا TCP ئىثالت ئەچفاچىم دجويىل) طققىف ماظن مزح ضرع مىتى.

لېمعلە موقۇي. امە واشنە نكەمە ئەل (3172 و 3171 ردىمىلە ذفنەم) TCP ل ناتسلج كانە.

اھلاسرا ئەداعا تىلىا مزحلا ھە فىرىعەت مىتى TCP syn. مزح لاسرا ئەداعا بىردىمىلە اھلاسرا ئەداعا تىلىا مزحلا ھە فىرىعەت مىتى TCP.

- كلذ ىلإ امو ناوث 6 مث 3 براقي ام لك TCP لوكوتورب لاسرا ةداع اتاي لمع ثدحت.
4. تان ايبل ا قفتل حيحصل زاهجلا نم MAC ناونع ردىص.

يلى ام جاتنتس نكمي ،نيلىصفلا ىلإ ادانتس او

- رادج ىلإ (لوكوتوربلاو، src/dst IP، ذفنمو، SRC/dst) ةنيعم تاونق 5 نم ٽمزح لصت .
(لخادل ايف) ةعقولمل ا ٽهج اول ا ىلع ةيامحل ا.
- ةيجراخل ا) ةعقولمل ا ٽهج اول ا ىلع ةيامحل ا راج ٽمزح للا كرتت ال.

اهب ىصوملا تاءارج إلأ

ةلأسمل ا هذه قاطن قييضت ةدایز وھ عرفل ا اذه يف ةدراول ا تاءارج إلأ نم ضرغل او

ةيکاحم ٽمزح عبّت نم ققحت. 1. ئارج إلأ.

طاقس ا ٽلاح يف. ةيامحل ا راج ٽطس اوپ ٽمزح ٽجل اعم ةيفيك ٽفرعمل packet-tracer ٽادأ مدختس ا
اذهل الـثامم ةيکاحملا ٽمزح لاعبّت ودبّي ، ةيامحل ا راج ىلإ لوصول ا جهـن ٽطس اوپ ٽمزح لـا:
جاـخ إـلـا:

```
<#root>
firepower#
packet-tracer input INSIDE tcp 192.168.0.100 11111 10.10.1.100 80

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 192.168.2.72 using egress ifc OUTSIDE

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 268439946 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268439946: ACCESS POLICY: FTD_Policy - Default
access-list CSM_FW_ACL_ remark rule-id 268439946: L4 RULE: DEFAULT ACTION RULE
Additional Information:
```

Result:

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

```
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x00005647a4f4b120 flow
```

رادي حلا مزحلا راثآ نم ققحت 2. ءارج إلأ.

رادج ةطس اوب ةيقيق حلا TCP syn مزح ةجل اعم ةيفيك نم ققحت لـ ةمزحلا عبـتـنـيـكـمـتـبـ مـقـ طـقـفـ لـخـدـمـ ةـمـزـحـ 50ـ لـوـأـ عـبـتـمـتـيـ ،ـيـضـارـتـفـاـ لـكـشـبـ .ـيـامـحـلـاـ

```
<#root>
```

```
firepower#
```

```
capture CAPI trace
```

تـقـؤـمـلـاـ طـاقـتـلـالـاـ نـزـخـمـ حـسـمـ

```
<#root>
```

```
firepower#
```

```
clear capture /all
```

اذـهـلـ اـهـبـ اـشـمـ عـبـتـتـلـاـ وـدـبـيـ ،ـيـامـحـلـاـ رـادـجـ ىـلـاـ لـوـصـوـلـاـ جـهـنـ ةـطـسـ اـوبـ ةـمـزـحـلـاـ طـاقـسـاـ ةـلـاحـ يـفـ جـارـخـإـلـاـ

```
<#root>
```

```
firepower#
```

```
show capture CAPI packet-number 1 trace
```

```
6 packets captured
```

```
1: 12:45:36.279740      192.168.0.100.3630 > 10.10.1.100.80: S 2322685377:2322685377(0) win 8192 <m
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 192.168.2.72 using egress ifc OUTSIDE

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 268439946 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268439946: ACCESS POLICY: FTD_Policy - Default
access-list CSM_FW_ACL_ remark rule-id 268439946: L4 RULE: DEFAULT ACTION RULE
Additional Information:

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

Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x00005647a4f4b120 flow
```

1 packet shown

تالجس نم ققحت 3. ءارجإلا FTD Lina.

دنتسملا اذه نم ققحت FTD FMC، رب ع Syslog ىلع:

<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200479-Configure-Logging->

[on-FTD-via-FMC.html](#)

مدع ۋەلاج يىف FTD Lina. تالجىلى يىچراغ syslog مداخنى يوكت مىتى نأ ئەشىپ نىسحتىمىلا نىم ئىامحىلا رادج ىلىع ئېلىحىملا تىقۇملا نزخىملا تالجىسى ئىكەنلىك مۇق، دىعىب نىع syslog مداخنى يوكت ئىادب ئەطقىن وە لاثمىلا اذه يىف رەاظىلا لجىسىلا نىيۈكت. اەحالىسى او ئاطاخلى فاشكىتسا ئانثأ ئەدىج:

```
<#root>
firepower#
show run logging

...
logging enable
logging timestamp
logging buffer-size 1000000
logging buffered informational
```

يىفرەتلە زاھىج يىف مەكھىتللە ارىطاس 24 ىلىع يىفرەتلە ئادەنلە زاھىج طبضا:

```
<#root>
firepower#
terminal pager 24
```

تىقۇملا طاقىتلەلا نزخىم حىسم:

```
<#root>
firepower#
clear logging buffer
```

مىتى، لاثمىلا اذه يىف لەلەحىملا ئىفۇصىت لەماع مادختىساب تالجىلى صىحفىلەسىنىڭ ئەرپەتىخا: ئىامحىلا رادج ىلىا لۇصۇلما جەن ئەطاساوب مۇزخىلە طاقىسى:

```
<#root>
firepower#
show logging | include 10.10.1.100
```

```
Oct 09 2019 12:55:51: %FTD-4-106023: Deny tcp src INSIDE:192.168.0.100/3696 dst OUTSIDE:10.10.1.100/80
Oct 09 2019 12:55:51: %FTD-4-106023: Deny tcp src INSIDE:192.168.0.100/3697 dst OUTSIDE:10.10.1.100/80
```

```
Oct 09 2019 12:55:54: %FTD-4-106023: Deny tcp src INSIDE:192.168.0.100/3696 dst OUTSIDE:10.10.1.100/80
Oct 09 2019 12:55:54: %FTD-4-106023: Deny tcp src INSIDE:192.168.0.100/3697 dst OUTSIDE:10.10.1.100/80
```

ةيامحلا رادجل ASP طاقس ا تاي لم مع نم ققحت 4. عاجلا.

يـتـلـا مـزـحـلـا عـيـمـجـ تـادـادـعـ ةـيـفـرـ كـنـكـمـيـفـ ، ةـيـامـحـلـا رـادـجـ نـمـ تـطـقـسـ ةـمـزـحـلـا نـأـ يـفـ كـشـتـ تـنـكـ اـذـاـ
جمـانـرـبـلـا ـيـوـتـسـمـ ـىـلـعـ ةـيـامـحـلـا رـادـجـ اـهـتـطـقـسـ اـ:

```
<#root>
```

```
firepower#
```

```
show asp drop
```

Frame drop:

No route to host (no-route)	234
Flow is denied by configured rule (acl-drop)	71

Last clearing: 07:51:52 UTC Oct 10 2019 by enable_15

Flow drop:

Last clearing: 07:51:52 UTC Oct 10 2019 by enable_15

جمـانـرـبـ ـيـوـتـسـمـ طـاقـسـ اـ تـايـ لـمـ عـيـمـجـ ضـرـعـلـ طـاقـتـلـاـ اـ تـايـ لـمـ نـيـكـمـتـ كـنـكـمـيـ:

```
<#root>
```

```
firepower#
```

```
capture ASP type asp-drop all buffer 33554432 headers-only
```

رايـخـ) طـقـفـ ةـمـزـحـلـا سـوـفـرـ طـاقـتـلـا كـنـكـمـيـ ةـمـزـحـلـا تـايـوـتـحـمـبـ اـمـتـهـمـ نـكـتـ مـلـ اـذـاـ جـيـمـلـتـ
تـقـؤـمـلـا طـاقـتـلـا نـزـخـمـ يـفـ مـزـحـلـا نـمـ دـيـزـمـلـا طـاقـتـلـا كـلـ حـيـتـيـ اـذـهـوـ). طـقـفـ سـوـفـرـلـا
500 وـهـ يـصـارـتـفـاـ لـكـشـبـ) تـقـؤـمـلـا طـاقـتـلـا نـزـخـمـ مجـحـ ةـدـاـيـزـ كـنـكـمـيـ ، كـلـذـىـلـا ةـفـاضـإـلـاـبـ
نـمـ اـعـدـ ، اـرـيـخـأـ. (تـقـؤـمـلـا نـزـخـمـلـا رـايـخـ) تـبـاـجـيـمـ 32 ـىـلـاـ لـصـتـ ةـمـيـقـ ـىـلـاـ (ـتـيـابـوـلـيـكـ
10 ـىـتـحـ طـاقـتـلـاـ فـلـمـ نـيـوـكـتـ فـلـمـلـاـ مجـحـ رـايـخـ كـلـ حـيـتـيـ، لـوـكـوـتـورـبـ نـمـ 6.3 رـادـصـاـلـاـ
قـيـسـنـتـبـ طـاقـتـلـاـ اـ تـايـوـتـحـمـ ةـيـفـرـ طـقـفـ كـنـكـمـيـ ةـلـاحـلـاـ كـلـتـ يـفـ. تـيـابـاـجـيـجـ PCAPـ).

ثـحـبـلـاـ قـاـاطـنـ قـيـيـضـتـلـ حـشـرـمـ مـاـدـخـتـسـاـ كـنـكـمـيـ ، طـاقـتـلـاـ اـ تـايـوـتـحـمـ نـمـ قـقـحـتـلـلـ

```
<#root>
```

```
firepower#
```

```
show capture ASP | include 10.10.1.100
```

```

18: 07:51:57.823672 192.168.0.100.12410 > 10.10.1.100.80: S 1870382552:1870382552(0) win 8192 <mss
19: 07:51:58.074291 192.168.0.100.12411 > 10.10.1.100.80: S 2006489005:2006489005(0) win 8192 <mss
26: 07:52:00.830370 192.168.0.100.12410 > 10.10.1.100.80: S 1870382552:1870382552(0) win 8192 <mss
29: 07:52:01.080394 192.168.0.100.12411 > 10.10.1.100.80: S 2006489005:2006489005(0) win 8192 <mss
45: 07:52:06.824282 192.168.0.100.12410 > 10.10.1.100.80: S 1870382552:1870382552(0) win 8192 <mss
46: 07:52:07.074230 192.168.0.100.12411 > 10.10.1.100.80: S 2006489005:2006489005(0) win 8192 <mss

```

ببس ركذ متى الـف، ةـجـاـولـاـىـوـتـسـمـىـلـعـلـعـفـلـابـاـهـبـقـعـتـمـتـيـمـزـحـلـاـنـأـامـبـ، ةـلـاحـلـاـهـذـهـيـفـ
وـأـلـوـخـدـلـاـةـهـجـاـوـ(ـدـحـاـوـنـاـكـمـيـفـطـقـفـةـمـزـحـلـاـبـقـعـتـنـكـمـيـهـنـأـرـكـذـتـ).ـطـاقـتـلـاـيـفـطـاقـسـإـلـاـ
ـطـاقـسـإـبـبـسـنـيـيـعـتـوـةـدـدـعـتـمـASPـطـاقـسـإـتـايـلـمـعـذـخـأـبـيـصـوـيـ، ةـلـاحـلـاـهـذـهـيـفـASPـطـاقـسـإـ
ـهـبـيـصـوـمـلـاـجـهـنـلـاـيـلـيـاـمـيـفـوـ.ـدـدـحـمـ).ـASPـطـاقـسـإـتـادـاـدـعـحـسـمـبـمـقـ:

1. ةـيـلـاحـلـاـASPـطـاقـسـإـتـادـاـدـعـحـسـمـبـمـقـ:

```

<#root>
firepower#
clear asp drop

```

ليغشت) ةـيـاـمـحـلـاـرـاـدـجـلـالـخـنـمـاـهـحـاـلـصـاـوـهـيـاـطـخـأـفـاـشـكـتـسـاـبـمـوـقـتـيـذـلـاـقـفـدـتـلـاـلـاـسـرـاـ.
(ـرـاـبـتـخـاـ).

اهـتـدـاـيـزـثـمـتـدـقـاهـنـأـظـحـاـلـوـASPـطـاقـسـإـتـادـاـدـعـنـمـيـرـأـةـرـمـقـقـحـتـ.

```

<#root>
firepower#
show asp drop
Frame drop:
  No route to host (
no-route
)
Flow is denied by configured rule (
acl-drop
)
```

234

71

اهـتـيـؤـرـمـتـيـيـتـلـاـةـدـدـحـمـلـاـطـاقـسـإـلـاـتـايـلـمـعـلـASPـ(ـطـاقـتـلـاـ)ـطـاقـتـلـاـنـيـكـمـتـ.

```

<#root>
firepower#
capture ASP_NO_ROUTE type asp-drop no-route

```

```

firepower#
capture ASP_ACL_DROP type asp-drop acl-drop

```

لیغشت) ۆيامحلا رادج لالخ نم اهحالص او عاطخاً فاشكتساب موقت يذلا قفدتلا لاسرا (رابتخا).

دوچوم ریغ راسم ببس ب مزحلا طاقس امت، ئالاحلا هذه يف ASP. تاعومجم نم ققحت.

<#root>

```
firepower#
```

```
show capture ASP_NO_ROUTE | include 192.168.0.100.*10.10.1.100
```

```

93: 07:53:52.381663 192.168.0.100.12417 > 10.10.1.100.80: S 3451917925:3451917925(0) win 8192 <mss
95: 07:53:52.632337 192.168.0.100.12418 > 10.10.1.100.80: S 1691844448:1691844448(0) win 8192 <mss
101: 07:53:55.375392 192.168.0.100.12417 > 10.10.1.100.80: S 3451917925:3451917925(0) win 8192 <mss
102: 07:53:55.626386 192.168.0.100.12418 > 10.10.1.100.80: S 1691844448:1691844448(0) win 8192 <mss
116: 07:54:01.376231 192.168.0.100.12417 > 10.10.1.100.80: S 3451917925:3451917925(0) win 8192 <mss
117: 07:54:01.626310 192.168.0.100.12418 > 10.10.1.100.80: S 1691844448:1691844448(0) win 8192 <mss

```

لاصتا لودج نم ققحت 5. ئارجيلا FTD Lina.

اهنإف ناك ببس يأْل نكلى، 'X' ۆهـج او ۆمزـحـلـا جـرـخـتـنـا اـهـيـفـعـقـوـتـتـتـالـاـحـكـانـهـنـوـكـيـنـأـنـكـمـيـيـاـذـهـلـيـغـشـتـلـاـبـيـتـرـتـىـلـاـةـيـامـحـلـاـرـادـجـجـرـخـمـۆـهـجـاوـدـيـدـحـتـدـنـتـسـيـيـ'Y'ـۆـهـجـاـولـاـضـرـعـتـ:

1. أشنـمـلـاـلـاصـتـالـاـثـحـبـ
2. ىـلـعـۆـيـوـلـوـأـلـاـNATـ(ـۆـيـاـغـ)ـUN-NATـ ۆـلـحـرـمـذـخـأـتـ -ـ ۆـكـبـشـلـاـنـاـونـعـۆـمـجـرـتـنـعـثـحـبـلـاـ رـاسـمـلـاـثـحـبـوـ
3. ۆـسـاـيـسـلـاـىـلـعـمـئـاـقـلـاـهـيـجـوـتـلـاـ (PBR)
4. هـيـجـوـتـلـاـلـودـجـثـحـبـ

لاصتا لودج نم ققحتلـلـ:

<#root>

```
firepower#
```

```
show conn
```

```
2 in use, 4 most used
```

```
Inspect Snort:
```

```
preserve-connection: 2 enabled, 0 in effect, 4 most enabled, 0 most in effect
```

TCP

DMZ

10.10.1.100:

INSIDE

```
192.168.0.100:
11694
, idle 0:00:01, bytes 0, flags
```

aa N1

TCP

DMZ

10.10.1.100:80

INSIDE

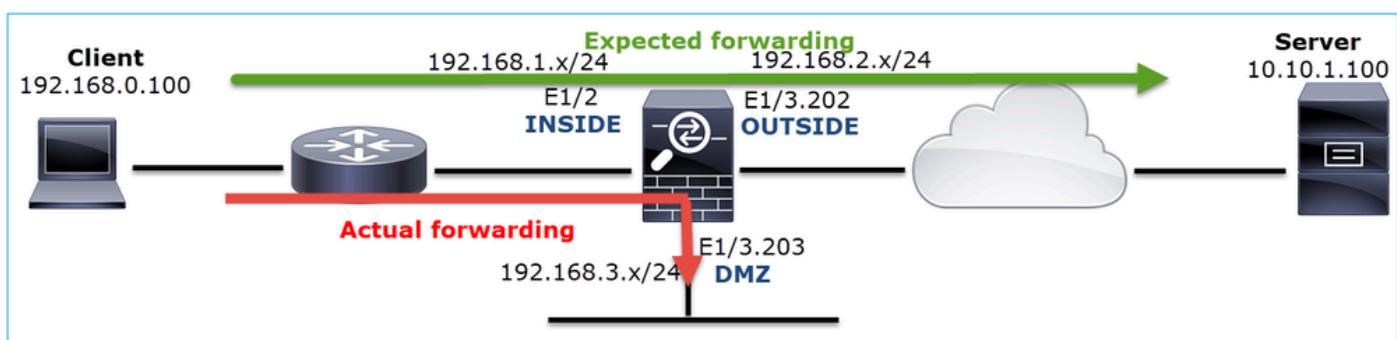
```
192.168.0.100:
11693
, idle 0:00:01, bytes 0, flags
```

aa N1

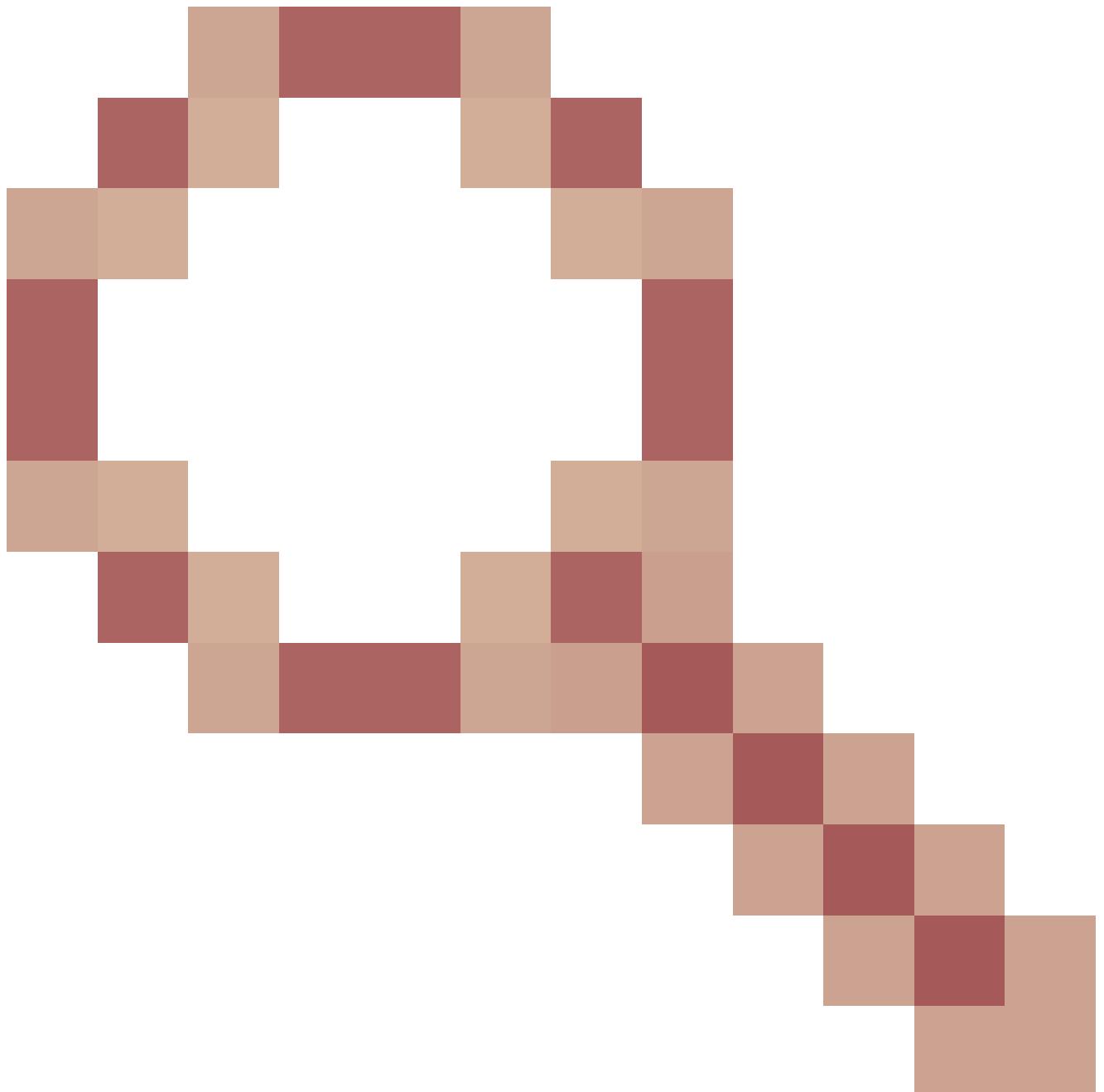
ةيسيئرلا طاقنلا:

- الا رهظي مل - فصن وحتف مت) ينبينج لاصتالا ناف ،(A) زييمتللا تامالع ىلإ ادانتسا ئيامحلا رادج ةطس اوپ TCP SYN.
- وه نراق جرملا ولخاد نراق لخدملا ئانيم ئياغل اردصملا ىلع ئانب DMZ.

انه ۋروصلالا يف اذه روصت نكمي:



show جاخن يف ئەجأولارمأ 0 نم ناماً يوتسم ىلع يوتحت FTD تاهجاو عيجم نأ امب: ظحالم ۆچاو مقر تاذ ئەجأولادىدحت متى، صوصخلالا ھجو ىلعاو. ئەجأولامقر ىلع دمتىعى ۆچأولادىدحت متى امنىيپ ۆيلخاد اهنأ ىلعا ئىلعا (VPIF-num) يرهاظلالي ساسألا ماظننلا تنا. ئېچراخ اهنأ ىلعا (لقلأا VPIF-num) يرهاظلالي ساسألا ماظننلا ئەجأولامقر تاذ، ۆلصلالا تاذ تانيسختلا. رمألىيصفت نراق ضرعلا عم ۆميق vpiif نراقلا تيأرعي طتسى، Cisco CSCvi15290



جاخ! يف لاصتالا هاجت| FTD ضرعی :نن| "show conn" ل FTD

<#root>

```
firepower#  
show interface detail | i Interface number is|Interface [P|E].*is up
```

```
...  
Interface Ethernet1/2 "INSIDE", is up, line protocol is up  
    Interface number is
```

19

```
Interface Ethernet1/3.202 "OUTSIDE", is up, line protocol is up  
    Interface number is
```

20

```
Interface Ethernet1/3.203 "DMZ", is up, line protocol is up
```

نم x 9.13.x رادص إلـا رفوي ، 6.5 رادص إلـا FirePOWER جـمانـرب رادصـا يـف لـاحـلـا وـه اـمـكـ: ظـحـالـمـ
لـاصـتـالـا ئـدـابـ لـوحـ تـامـوـلـعـمـ show conn long وـ show conn detail رـمـأـلـا تـاجـرـخـمـ
بـيـجـتـسـمـلـاوـ

جـتـانـلـا 1:

```
<#root>
firepower#
show conn long
...
TCP OUTSIDE: 192.168.2.200/80 (192.168.2.200/80) INSIDE: 192.168.1.100/46050 (192.168.1.100/46050), flags
Initiator: 192.168.1.100, Responder: 192.168.2.200
Connection lookup keyid: 228982375
```

جـتـانـلـا 2:

```
<#root>
firepower#
show conn detail
...
TCP OUTSIDE: 192.168.2.200/80 INSIDE: 192.168.1.100/46050,
flags aA N1, idle 4s, uptime 11s, timeout 30s, bytes 0
Initiator: 192.168.1.100, Responder: 192.168.2.200
Connection lookup keyid: 228982375
```

نـاـونـعـ ةـمـجـرـتـ ةـلـاحـ يـفـ سـاـوـقـأـ لـخـادـ NATed IPs ليـوطـ ضـرـعـلـاـ ضـرـعـيـ،ـ كـلـذـ ئـلـإـ ةـفـاضـلـاـ بـشـلـاـ:

```
<#root>
firepower#
show conn long
...
```

```
TCP OUTSIDE: 192.168.2.222/80 (192.168.2.222/80) INSIDE: 192.168.1.100/34792 (192.168.2.150/34792), fl
Initiator: 192.168.1.100, Responder: 192.168.2.222
Connection lookup keyid: 262895
```

ةيامحلا رادج ناوونع ليلح لوكوتوربل تقؤملانيزختلا ةركاذ نم ققحت 6. عارج إلأ (ARP).

ةيلصألا ئمزحلا طاقس اب ةيامحلا رادج موقى، ةيلاتلا ئلحرملالا لح ةيامحلا رادج ىلع رذعت اذا لح ب موقى ىتح رارمتسا ب ARP تابلط لاسراو تماص لكشب (ةلاحلا هذه يف TCP SYN) ةيلاتلا ئلحرملالا.

رمألا مدخلتسا، ةيامحلا رادجل ARP ل تقؤملانيزختلا ةركاذ ضرع:

```
<#root>
firepower#
show arp
```

رمألا مدخلتسا كنكمي، نيلاحم ريغ نيفيضم دوجونم ققحتلل، كلذ لـ ئفاض إلاب:

```
<#root>
firepower#
show arp statistics
Number of ARP entries in ASA: 0

Dropped blocks in ARP: 84
Maximum Queued blocks: 3
Queued blocks: 0
Interface collision ARPs Received: 0
ARP-defense Gratuitous ARPS sent: 0
Total ARP retries:
182 < indicates a possible issue for some hosts

Unresolved hosts:
1

< this is the current status
Maximum Unresolved hosts: 2
```

ب صاخ طاقتلا نيكمنت كنكميف ARP، ئيلمعل صحفلا نم ديزم عارجا ديرت تنك اذا

```

<#root>

firepower#

capture ARP ethernet-type arp interface OUTSIDE

firepower#

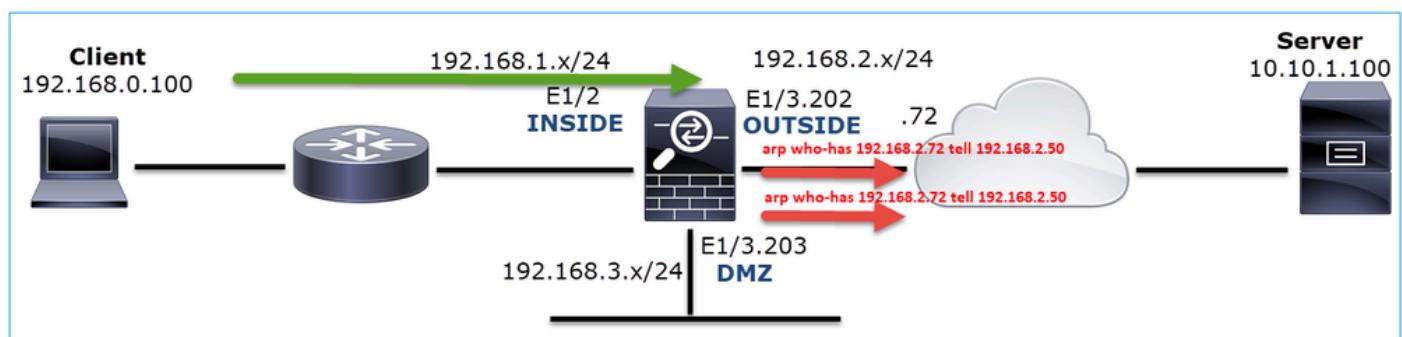
show capture ARP

...
4: 07:15:16.877914      802.1Q vlan#202 P0 arp
who-has 192.168.2.72 tell 192.168.2.50

5: 07:15:18.020033      802.1Q vlan#202 P0 arp who-has 192.168.2.72 tell 192.168.2.50

```

ال نکلو، ئيلاتلا ۋە لەرلە لە (192.168.2.50) ئامحلا رادج لواھى، جارخالا اۇھىف در دجويى ARP



ةبسانملا ARP ۋە ئەنلىك ئەنھە تاجرىخملە ضرعت:

```

<#root>

firepower#

show capture ARP

2 packets captured

1: 07:17:19.495595      802.1Q vlan#202 P0
arp who-has 192.168.2.72 tell 192.168.2.50

2: 07:17:19.495946      802.1Q vlan#202 P0
arp reply 192.168.2.72 is-at 4c:4e:35:fc:fc:d8

2 packets shown

```

```

<#root>

firepower#

show arp

INSIDE 192.168.1.71 4c4e.35fc.fcd8 9

```

OUTSIDE 192.168.2.72 4c4e.35fc.fcd8 9

ةرشابمل ا TCP SYN لاخدا دوجو مدع ةلاح يف ARP رهظي ناكمل اي:

```
<#root>

firepower#

show capture CAPI packet-number 1 trace

6 packets captured

1: 07:03:43.270585

192.168.0.100.11997 > 10.10.1.100.80

: S 4023707145:4023707145(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
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 192.168.2.72 using egress ifc OUTSIDE
...
Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 4814, packet dispatched to next module
...
Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.2.72 using egress ifc OUTSIDE
```

```

Result:
input-interface: INSIDE
input-status: up
input-line-status: up

output-interface: OUTSIDE

output-status: up
output-line-status: up

Action: allow

```

نكمملا نم نوكى ال امدنع يتح حمسى: عارج إلأ رهظي عبّتلا، جاتن إلأ يف يري نأ نكمي امك
هذه يف !ةيامحلا راج ةطساوب تمسىب ّمزلحا طاقس امتي و ئيلاتل ّوطخلالا ىلإ لوصوللا
جاتن| ّقد رثكأ رفوّي و هنأ امب تصحّف اضيأ يغبني ّادأ-tracer، ّلاحلا، ّطبّرلا، ّلاحلا

```

<#root>

firepower#

packet-tracer input INSIDE tcp 192.168.0.100 1111 10.10.1.100 80

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 192.168.2.72 using egress ifc OUTSIDE
...

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 4816, packet dispatched to next module
...
Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface

```

```

Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.2.72 using egress ifc OUTSIDE

```

```

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

```

```
Drop-reason: (no-v4-adjacency) No valid V4 adjacency, Drop-location: frame 0x00005647a4e86109 flow (NA)
```

ل ٰقبا سلـا ٰلاـسـرـلـا نـيـسـحـتـ مـتـ، ٰـرـيـخـأـلـا ASA/FirePOWER تـارـادـصـاـ يـفـ:

<#root>

```

Drop-reason: (no-v4-adjacency) No valid V4 adjacency.

Check ARP table (show arp) has entry for nexthop
., Drop-location: f

```

اهـبـ ىـصـوـمـلـاـ تـاءـاـرـجـاـلـاـ اوـلـمـتـحـمـلـاـ بـابـسـأـلـاـ صـخـلـمـ

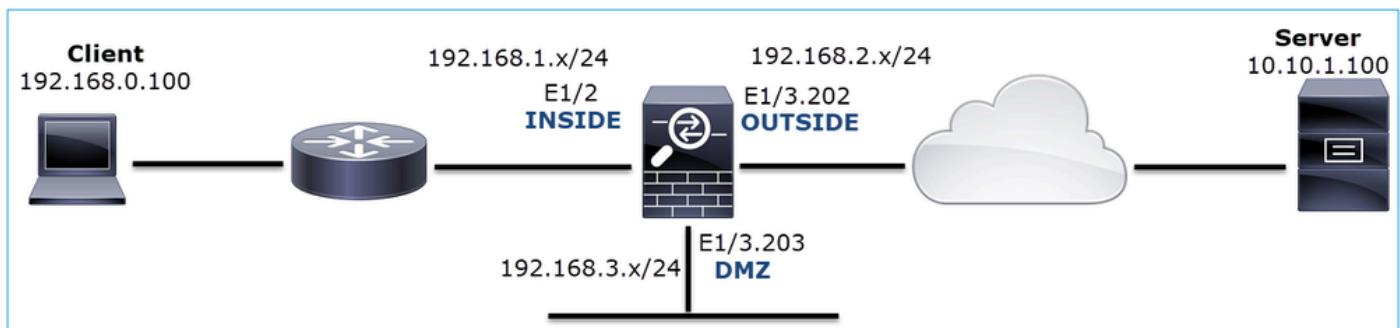
لـاـ نـمـ لـسـرـيـ طـبـرـ TCP syn نـمـ اـمـ نـأـ رـيـغـ، ٰـرـاـقـ لـخـدـمـلـاـ ٰـلـعـ طـبـرـ طـقـفـ تـنـأـ ٰـرـيـ نـاـ
بـبـسـ نـكـمـيـ ضـعـبـ نـرـاـقـ جـخـمـ عـقـوـتـيـ:

لمـتـحـمـلـاـ بـبـسـلـاـ	اهـبـ ىـصـوـمـلـاـ تـاءـاـرـجـاـلـاـ
جهـنـ ٰـطـسـاـوـبـ ٰـمـزـحـلـاـ طـاقـسـاـ مـتـيـ ٰـيـامـحـلـاـ رـاـدـجـ ىـلـاـ لـوـصـوـلـاـ.	<ul style="list-style-type: none"> • ٰـيـامـحـلـاـ رـاـدـجـ ٰـلـاـ ٰـمـدـخـتـسـاـ capture w/trace • ٰـيـامـحـلـاـ رـاـدـجـ تـالـجـسـ نـمـ قـقـحـتـ. • ٰـيـامـحـلـاـ رـاـدـجـ ASP طـاقـسـاـ تـايـلـمـعـ نـمـ قـقـحـتـ (show asp drop أو capture type asp-drop). • نـأـ ضـرـتـفـيـ اـذـهـ FMC. لـاـصـتـاـ ثـادـحـأـ نـمـ قـقـحـتـ • نـكـمـمـ لـيـجـسـتـ ٰـلـعـ يـوـتـحـتـ ٰـدـعـاـقـلـاـ.
حـيـحـصـ رـيـغـ طـاقـتـلـاـ ٰـيـفـصـتـ لـمـاعـ	<ul style="list-style-type: none"> • ٰـضـبـقـ ٰـلـعـ وـأـ packet-tracer تـلـمـعـتـسـاـ w/trace لـدـعـيـ نـأـ ٰـمـجـرـتـ نـوـكـيـ كـانـهـ نـاـ ٰـرـيـ نـأـ طـبـضـاـ، ٰـلـاـحـلـاـ كـلـتـ يـفـ ip. ٰـيـاغـلـاـ وـأـ رـدـصـمـلـاـ طـاقـتـلـاـ حـشـرـمـ. • نـيـوـانـعـ show conn long IP رـمـأـلـاـ جـاـخـاـ ضـرـعـيـ بـ ٰـصـاـخـلـاـ NATed.

<p>فلتخم جرخ نراق ىلا طبرلا تلسرا.</p>	<ul style="list-style-type: none"> • مزح لـ packet-tracer و capture w/trace. • يـ اـ حـ لـ لـ ئـ اـ مـ حـ لـ رـ اـ دـ جـ لـ اـ عـ مـ ئـ فـ يـ كـ ئـ فـ رـ عـ مـ لـ. • يـ اـ حـ لـ لـ اـ لـ اـ صـ تـ اـ لـ اـ وـ جـ خـ مـ لـ اـ ئـ جـ اوـ دـ يـ دـ حـ تـ رـ اـ بـ تـ عـ اـ لـ اـ لـ اـ حـ لـ لـ اـ لـ اـ صـ تـ اـ لـ اـ وـ جـ ثـ حـ بـ وـ. • ئـ اـ حـ لـ لـ رـ اـ دـ جـ تـ الـ جـ سـ نـ مـ قـ قـ حـ تـ. • ئـ اـ حـ لـ لـ رـ اـ دـ جـ لـ اـ صـ تـ اـ لـ اـ وـ جـ نـ مـ قـ قـ حـ تـ (show conn). <p>قباطن اهنأ ئطاخ ئهج او ىلا مزح لـ لـ اـ سـ رـ اـ مـ تـ اـ ذـ اـ دـ دـ حـ وـ clear conn address دـ دـ حـ وـ حـ سـ مـ دـ يـ رـ تـ يـ ذـ لـ اـ لـ اـ صـ تـ اـ نـ مـ 5ـ ئـ لـ سـ لـ سـ لـ اـ.</p>
<p>جـ هـ جـ وـ لـ اـ ىـ لـ اـ قـ يـ رـ طـ دـ جـ وـ يـ اـ لـ.</p>	<ul style="list-style-type: none"> • مزح لـ packet-tracer و capture w/trace. • يـ اـ حـ لـ لـ رـ اـ دـ جـ لـ اـ طـ اـ قـ سـ اـ تـ اـ يـ لـ مـ عـ نـ مـ قـ قـ حـ تـ. • ئـ اـ حـ لـ لـ اـ لـ اـ طـ اـ قـ سـ اـ بـ بـ سـ ىـ لـ عـ لـ وـ صـ حـ لـ لـ رـ اـ سـ مـ.
<p>جـ خـ مـ لـ اـ ئـ هـ جـ اوـ لـ عـ A~R~P~ لـ اـ خـ دـ اـ دـ جـ وـ يـ اـ لـ.</p>	<ul style="list-style-type: none"> • رـ اـ دـ جـ لـ A~R~P~ لـ تـ قـ فـ مـ لـ اـ نـ يـ زـ خـ تـ لـ اـ ئـ رـ كـ اـ ذـ نـ مـ قـ قـ حـ تـ (show arp). • كـ انـ هـ نـ اـ كـ اـ ذـ اـ مـ ئـ فـ رـ عـ مـ لـ مـ دـ خـ تـ سـ اـ حـ لـ اـ صـ رـ وـ اـ جـ تـ.
<p>لـ طـ عـ مـ جـ خـ مـ لـ اـ نـ رـ اـ قـ.</p>	<p>رـ اـ دـ جـ ىـ لـ عـ show interface ip brief رـ مـ اـ لـ اـ جـ اـ خـ اـ نـ مـ قـ قـ حـ تـ.</p> <p>جـ هـ جـ اوـ لـ اـ ىـ لـ اـ قـ قـ حـ تـ وـ ئـ اـ حـ لـ لـ.</p>

لـ دـ اـ نـ مـ 2. 2ـ ئـ لـ اـ حـ

طـ طـ خـ مـ لـ اـ ئـ رـ وـ صـ لـ اـ هـ ذـ هـ ضـ رـ عـ تـ:



للمعی ال هکشمند: HTTP

رثأتهملا قفتل:

SRC IP: 192.168.0.100

لوكوتورب DST IP: 10.10.1.100

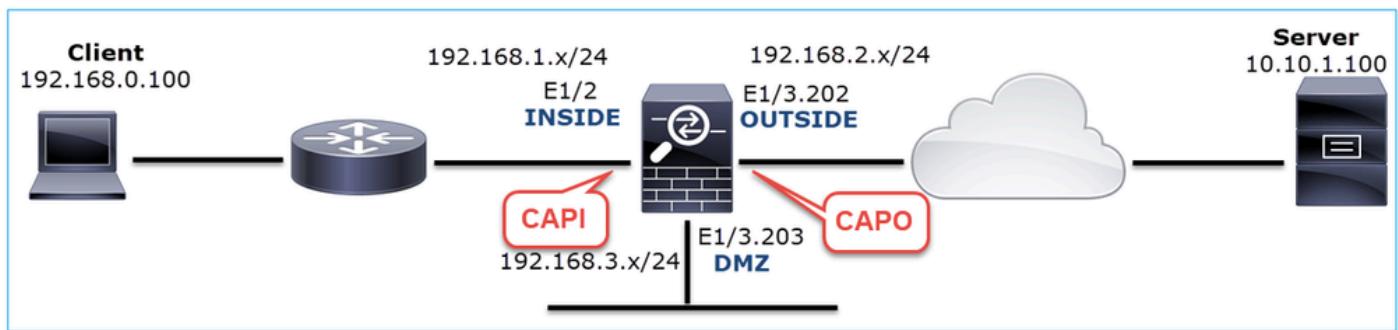
لوكوتورب TCP 80: لوكوتورب

رسأ ليتحت

CRM يلع طاقدلل ا تايـلمـع نـيـكـمـتـبـ مـقـ

<#root>

```
firepower#
capture CAPI int INSIDE match ip host 192.168.0.100 host 10.10.1.100
firepower#
capture CAPO int OUTSIDE match ip host 192.168.0.100 host 10.10.1.100
```



للمعی ال ويـرانـیـسـ - طـاـقـتـلـاـ:

زاهـجلـابـ ـصـاخـلـاـ رـمـأـوـلـاـ رـطـسـ ةـجـاـوـ نـمـ طـاـقـتـلـاـ اـهـ وـدـبـتـ يـتـلـاـ ةـقـيـرـطـلـاـ يـهـ ـذـهـ:

<#root>

```
firepower#
show capture
capture CAPI type raw-data trace interface INSIDE [Capturing -
834 bytes
]
match ip host 192.168.0.100 host 10.10.1.100
capture CAPO type raw-data interface OUTSIDE [Capturing -
878 bytes
```

```
] match ip host 192.168.0.100 host 10.10.1.100
```

م تايوت حم CAPI:

```
<#root>
firepower#
show capture CAPI
1: 05:20:36.654217 192.168.0.100.22195 > 10.10.1.100.80:
s
1397289928:1397289928(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 05:20:36.904311 192.168.0.100.22196 > 10.10.1.100.80:
s
2171673258:2171673258(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
3: 05:20:36.905043 10.10.1.100.80 > 192.168.0.100.22196:
R
1850052503:1850052503(0) ack 2171673259 win 0
4: 05:20:37.414132 192.168.0.100.22196 > 10.10.1.100.80:
s
2171673258:2171673258(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
5: 05:20:37.414803 10.10.1.100.80 > 192.168.0.100.22196:
R
31997177:31997177(0) ack 2171673259 win 0
6: 05:20:37.914183 192.168.0.100.22196 > 10.10.1.100.80:
s
2171673258:2171673258(0) win 8192 <mss 1460,nop,nop,sackOK>
...

```

م تايوت حم CAPO:

```
<#root>
firepower#
show capture CAPO
1: 05:20:36.654507 802.1Q vlan#202 P0 192.168.0.100.22195 > 10.10.1.100.80:
s
2866789268:2866789268(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
2: 05:20:36.904478 802.1Q vlan#202 P0 192.168.0.100.22196 > 10.10.1.100.80:
s
```

4785344:4785344(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
 3: 05:20:36.904997 802.1Q vlan#202 P0 10.10.1.100.80 > 192.168.0.100.22196:

R

0:0(0) ack 4785345 win 0
 4: 05:20:37.414269 802.1Q vlan#202 P0 192.168.0.100.22196 > 10.10.1.100.80:

S

4235354730:4235354730(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
 5: 05:20:37.414758 802.1Q vlan#202 P0 10.10.1.100.80 > 192.168.0.100.22196:

R

0:0(0) ack 4235354731 win 0
 6: 05:20:37.914305 802.1Q vlan#202 P0 192.168.0.100.22196 > 10.10.1.100.80:

S

4118617832:4118617832(0) win 8192 <mss 1380,nop,nop,sackOK>

يەف CAPI طاقەتلا ۆرۆصلە ھەذە رەھەنە.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.100	10.10.1.100	TCP	66	22195 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.250094	192.168.0.100	10.10.1.100	TCP	66	22196 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
3	0.000732	10.10.1.100	192.168.0.100	TCP	54	80 → 22196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4	0.509089	192.168.0.100	10.10.1.100	TCP	54	80 → 22196 [TCP Retransmission] 22196 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
5	0.000671	10.10.1.100	192.168.0.100	TCP	54	80 → 22196 [RST, ACK] Seq=2476911971 Ack=1 Win=0 Len=0
6	0.499380	192.168.0.100	10.10.1.100	TCP	62	[TCP Retransmission] 22196 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
7	0.000625	10.10.1.100	192.168.0.100	TCP	54	80 → 22196 [RST, ACK] Seq=2853655305 Ack=1 Win=0 Len=0
8	1.739729	192.168.0.100	10.10.1.100	TCP	66	[TCP Retransmission] 22196 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
9	0.000611	10.10.1.100	192.168.0.100	TCP	54	80 → 22195 [RST, ACK] Seq=1 Ack=0 Win=0 Len=0
10	0.499385	192.168.0.100	10.10.1.100	TCP	62	[TCP Retransmission] 22195 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
11	0.000671	10.10.1.100	192.168.0.100	TCP	54	80 → 22195 [RST, ACK] Seq=151733665 Ack=1 Win=0 Len=0

```

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: Cisco_fc:fcc:d8 (4c:4e:35:fc:fc:d8), Dst: Cisco_f6:1d:ae (00:be:75:f6:1d:ae) 4
> Internet Protocol Version 4, Src: 192.168.0.100, Dst: 10.10.1.100
> Transmission Control Protocol, Src Port: 22195, Dst Port: 80, Seq: 0, Len: 0

```

يەسیئرلا طاقەنلا:

1. ۋەزىخەنە TCP syn.
2. ۋەزىخەنە TCP RST لاسارا مەتى.
3. ۋەزىخەنە TCP syn.
4. ۋەزىخەنە MAC ناونع يەمتنى لۇخدا مەزىلەنەن (MAC address) نىۋانع، ثېلى ھەجوم ىلە رەدھەنەلەنەن (MAC address) ناونع يەمتنى.

يەف CAPO طاقەتلا ۆرۆصلە ھەذە رەھەنە:

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-11 07:20:36.654507	192.168.0.100	10.10.1.100	TCP	70	22195 → 80 [SYN] 1 0 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
2	2019-10-11 07:20:36.904478	192.168.0.100	10.10.1.100	TCP	70	22196 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
3	2019-10-11 07:20:36.904497	10.10.1.100	192.168.0.100	TCP	58	80 → 22196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 2
4	2019-10-11 07:20:37.414269	192.168.0.100	10.10.1.100	TCP	70	[TCP Port numbers reused] 22196 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
5	2019-10-11 07:20:37.414758	10.10.1.100	192.168.0.100	TCP	58	80 → 22196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	2019-10-11 07:20:37.914395	192.168.0.100	10.10.1.100	TCP	66	[TCP Port numbers reused] 22196 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 SACK_PERM=1
7	2019-10-11 07:20:37.914762	10.10.1.100	192.168.0.100	TCP	58	80 → 22196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8	2019-10-11 07:20:39.654629	192.168.0.100	10.10.1.100	TCP	70	[TCP Retransmission] 22195 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
9	2019-10-11 07:20:39.655102	10.10.1.100	192.168.0.100	TCP	58	80 → 22195 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10	2019-10-11 07:20:40.154700	192.168.0.100	10.10.1.100	TCP	66	[TCP Port numbers reused] 22195 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 SACK_PERM=1
11	2019-10-11 07:20:40.155173	10.10.1.100	192.168.0.100	TCP	58	80 → 22195 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

```

> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Cisco_f6:1d:8e (00:be:75:f6:1d:8e), Dst: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 202
> Internet Protocol Version 4, Src: 192.168.0.100, Dst: 10.10.1.100
> Transmission Control Protocol, Src Port: 22195, Dst Port: 80, Seq: 0, Len: 0

```

ةيسيئرلا طاقنلا:

1. ٩مزمٽ ردقصلما لسرى .TCP syn.
2. ةيجراخلا ٩هوجاولى ىلى لصى .TCP RST
3. ٩مزمٽ ردقصلما لسرى .TCP syn.
4. جوم، ردقصلما و ٩يجراخلا ٩يامحلا رادج نوكى جورخلما مزمٽ ىلعا (٩حىحص MAC نىوانع ٩ياغلا و ٩ثبلما MAC).

يلى ام جاتنتسا نكمى ،نىيلصفلا ىلى ادانتسا و

- مداخل او لىيملعلا نىب هاجتالا يىثاالتلا TCP لاصتا ديكأت لامكى متي ال .
- ٩يامحلا رادج جرخ ٩هوجاولى لصى يذلا TCP RST كانه
- نىوانع ىلى ادانتسا) مداخللا نم تانايبلالا قفت ٩زهجأ ىلى "٩دحتى" ٩يامحلا رادج (MAC)

اهب ىصوصلما تاءارجإلا

ةلأسملما ٩ذه قاطن قىيىضت ٩دايز و ٩عرفلا اذه يف ٩درابولا تاءارجإلا نم ضرغل او.

لسرى يذلا ردقصلما MAC ناونع نم ٩ققحت 1. ٩ارجا TCP RST.

دق {upper}mac نأ امب ٩سفن لـ TCP syn لـ طبر يرى if يف لـ mac ٩ياغلا نأ تقدق طبر لـ TCP rst لـ if يف.

CAPO_RST_SERVER.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No. Time Source Destination Protocol Length Info

1 2019-10-11 07:20:36.654507 192.168.0.100 10.10.1.100 TCP 70 22195 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1

2 2019-10-11 07:20:36.904478 192.168.0.100 10.10.1.100 TCP 70 22196 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1

<

> Frame 2: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Cisco_f6:1d:8e (00:be:75:f6:1d:8e) Dst: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 202
> Internet Protocol Version 4, Src: 192.168.0.100, Dst: 10.10.1.100
> Transmission Control Protocol, Src Port: 22196, Dst Port: 80, Seq: 0, Len: 0

CAPO_RST_SERVER.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No. Time Source Destination Protocol Length Info

1 2019-10-11 07:20:36.654507 192.168.0.100 10.10.1.100 TCP 70 22195 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1

2 2019-10-11 07:20:36.904478 192.168.0.100 10.10.1.100 TCP 70 22196 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1

3 2019-10-11 07:20:36.904997 10.10.1.100 192.168.0.100 TCP 58 80 → 22196 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

<

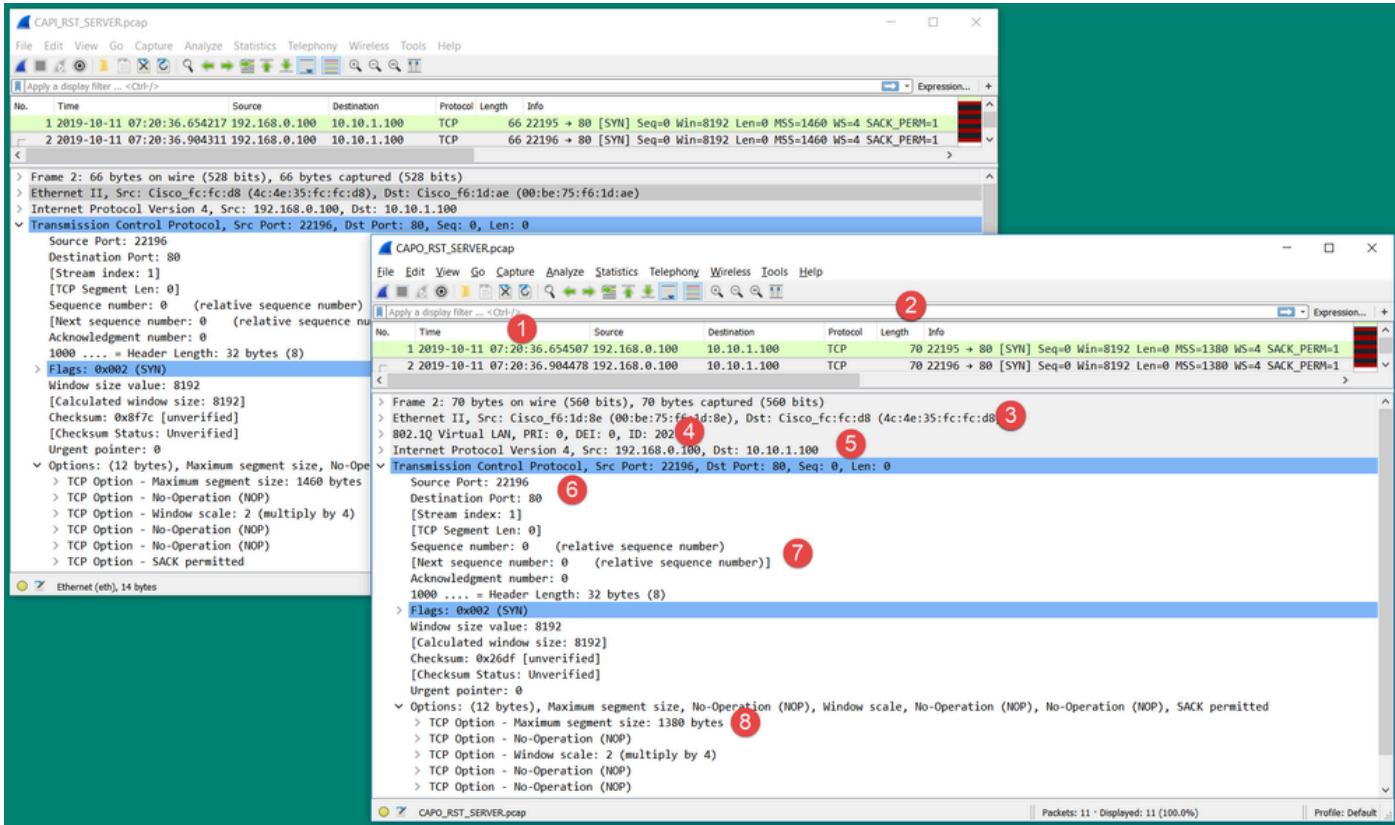
> Frame 3: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
> Ethernet II, Src: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8) Dst: Cisco_f6:1d:8e (00:be:75:f6:1d:8e)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 202
> Internet Protocol Version 4, Src: 10.10.1.100, Dst: 192.168.0.100
> Transmission Control Protocol, Src Port: 80, Dst Port: 22196, Seq: 1, Ack: 1, Len: 0

نیرمأ دیكأت ىلإ صحفلا اذه فدهي:

- رظانتم ریغ قفت دوجو مدع نم ققحت.
- عوقتملا تانایبلا قفت زاهج ىلإ MAC عامتنا نم ققحت.

جورخلاو لوطلا مزح ةنراقم 2. عاجلا.

متی . طبرلا دسفي / لدعی ال ئامحلا رادج نأ نم ققحتلل ايرصب Wireshark ىلع 2 طبرلا نراق . عوقتملا قورفلما ضعب زاربا.



ةيسيئرلا طاقنلا:

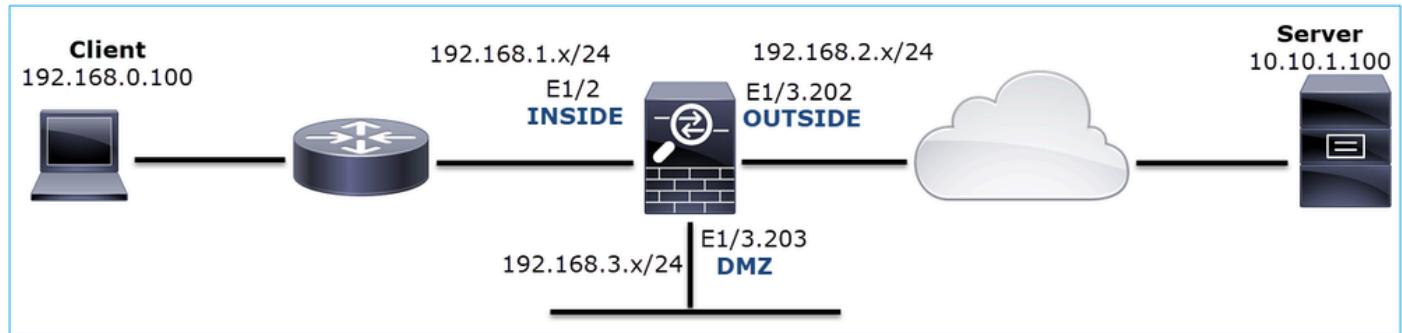
1. الوقعمواليئض قرافللا نوكى نأ دبال، ئرخأ ةيحان نمو. ةفلتخدم ةينمزلا عباوطلا.
2. زاهجلا ىلع لمحللا لثمم مزحلا ىلع ةقبطملا ةسايسللا صحفوتازيملا ىلع اذه دمتعي رادج ةطساوب هتلزا/هتفاضا تمت dot1Q سأركانه ناك اذا ةصاخ مزحلا لوط فلتخي طقف دحاوب بناج ىلع ةيامحللا.
3. ةفلتخدم MAC نيوانع.
4. ةيعرف ةهجاو ىلع طاقتلالا مت اذا هناكم يف dot1Q سأرنوكى نأ نكمي.
5. ىلا تقطب (برض) ومجرت ناونع رسيا وأ ٖ NAT ٖ لاح يف فلتخدم (نيوانع) ناونع ip لـ طبرلا.
6. طبرلا ىلا تقطب برض وأ ٖ NAT ٖ لاح يف عانيم فلتخدم ةياغ وأ ردهصملا.
7. ماقرأ نأ ىرتسف Wireshark، لـ يبسنـلا لـ سـلسـتـلا مـقرـ رـايـخـ لـ يـطـعـتـبـ تـمـقـ اذا مـقرـ ةـيـ اوـشـعـ بـبـسـبـ ةـيـ اـمـحـلـاـ رـادـجـ ةـطـسـاـوـبـ اـهـلـيـدـعـتـ مـتـيـ TCP رـارـقـ إـلـاـ مـاقـرـأـ لـ سـلسـتـ (IS).
8. لكشب ةيامحللا رادج لممعي، لـ اـثـمـلـاـ لـ يـبـسـ ىـلـعـ TCP تـارـاـيـخـ ضـعـبـ قـوـفـ ةـبـاتـكـلـاـ نـكـمـيـ ةـئـزـجـتـ بـنـجـتـلـ 1380 ىـلـاـ (TCP MSS) عـطـقـمـ مجـلـ ىـصـقـأـلـاـ دـحـلـاـ رـيـيـغـتـ ىـلـعـ يـضـارـتـفـاـ لـقـنـلـاـ رـاسـمـلـاـ يـفـ ةـمـزـحـلـاـ.

ةهـجـوـلـاـ يـفـ طـاقـتـلـاـ 3ـ عـارـجـ إـلـاـ

نـكـمـيـ اـمـ بـرـقـأـ طـاقـتـلـاـ ذـخـفـ انـكـمـمـ اـذـهـ نـكـيـ مـلـ اـذـاـ اـهـسـفـنـ ةـهـجـوـلـاـ يـفـ ةـرـوـصـ طـقـتـلـاـ، نـكـمـأـ نـاـ ةـهـجـأـلـاـ دـحـأـ نـمـ وـأـ ةـهـجـوـلـاـ مـدـاخـلـهـ (TCP RST) لـسـريـ يـذـلـاـ نـمـ نـمـ قـقـحـتـلـاـ وـهـ اـنـهـ فـدـهـلـاـ. ةـهـجـوـلـاـ ىـلـاـ (؟ـ رـاسـمـلـاـ يـفـ ةـمـزـحـلـاـ).

ةدح او ةياهن ةطقن نم TCP 3-way + RST 3-للاحلا

ططخملا ۀروصلما هذه ضرعت:



لمعي ال ۀلكشملا فصو

رثأتملما قفدتلا:

SRC IP: 192.168.0.100

لوكوتورب DST IP: 10.10.1.100

لوكوتورب TCP 80

رسأ ليلحت

كرحم ىلع طاقتلا تايلمع نيكمنتب مق FTD LINA.

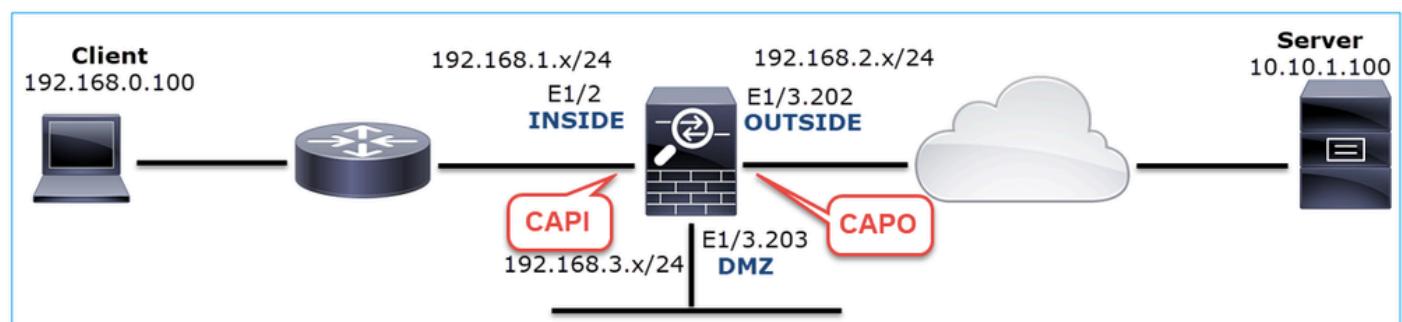
```
<#root>
```

```
firepower#
```

```
capture CAPI int INSIDE match ip host 192.168.0.100 host 10.10.1.100
```

```
firepower#
```

```
capture CAPO int OUTSIDE match ip host 192.168.0.100 host 10.10.1.100
```



لمعي ال ويرانيس - طاقتلا:

طاقتلا تايلمع يف رهظت نأ ۀلكشملا ناتفلتخم ناتقيرط كانه.

لیمعلانوم ڈیلچسپی + RST TCP 3-way

روصلانی فحص وہ امکان ہے کہ CAPWAP میں اس کا علاج کیا جائے گا۔

No.	Time	Source	Destination	Protocol	Length	Info
2	2019-10-13 17:06:27.874085	192.168.0.100	10.10.1.100	TCP	66	48295 → 80 [SYN] Seq=179631561 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
3	2019-10-13 17:06:27.874741	10.10.1.100	192.168.0.100	TCP	66	80 → 48295 [SYN, ACK] Seq=3838911937 Ack=179631562 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
4	2019-10-13 17:06:27.875183	192.168.0.100	10.10.1.100	TCP	54	48295 → 80 [ACK] Seq=179631562 Ack=3838911938 Win=66240 Len=0
8	2019-10-13 17:06:30.882537	10.10.1.100	192.168.0.100	TCP	66	[TCP Retransmission] 80 → 48295 [SYN, ACK] Seq=3838911937 Ack=179631562 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
9	2019-10-13 17:06:30.883056	192.168.0.100	10.10.1.100	TCP	66	[TCP Previous segment not captured] 48295 → 80 [ACK] Seq=179631562 Ack=3838911938 Win=66240 Len=0 SLE=3838911937 SRE=3838911938
13	2019-10-13 17:06:36.889022	10.10.1.100	192.168.0.100	TCP	62	[TCP Retransmission] 80 → 48295 [SYN, ACK] Seq=3838911937 Ack=179631562 Win=65535 Len=0 MSS=1380 SACK_PERM=1
14	2019-10-13 17:06:36.889526	192.168.0.100	10.10.1.100	TCP	66	[TCP Dup ACK 4#] 48295 → 80 [ACK] Seq=179631562 Ack=3838911938 Win=66240 Len=0 SLE=3838911937 SRE=3838911938
17	2019-10-13 17:06:47.943631	192.168.0.100	10.10.1.100	TCP	54	48295 → 80 [RST, ACK] Seq=179631562 Ack=3838911938 Win=0 Len=0

ڈیلچسپی طاقتمندی:

ڈیامحلانوم ڈیلچسپی 4-way TCP راج ربع ہے۔

2. SYN/ACK میں داخلہ کمی

3. نوبزلا کمی

4. ڈیلچسپی RST TCP کو توڑنے کا علاج 20 لامواں دفعہ

اتصالیں اس کا مفاد ہے۔

ڈیلچسپی میں پہلی کمی اسے ادا کرے۔

ڈیلچسپی میں دوسری کمی اسے ادا کرے۔

ڈیلچسپی میں تیسرا شرط ہے کہ یہ لامواں دفعہ تاکہ اسے متعارف کر دیا جائے۔

- SYN/ACK میں داخلہ کمی
- نوبزلا کمی
- ڈیلچسپی RST TCP اور FIN/ACK میں داخلہ کمی

ڈیلچسپی میں اسی سلسلہ کی وجہ سے طاقتمندی کا ساری کامیابی اس کا نتیجہ ہے۔

26	7.636612	192.168.0.100	10.10.1.100	TCP	66	55324→80 [SYN] Seq=433201323 Win=8192 Len=0 MSS=1380 WS=4 SAC...
29	7.637571	10.10.1.100	192.168.0.100	TCP	66	80→55324 [SYN, ACK] Seq=4063222169 Ack=433201324 Win=8192 Len=...
30	7.930152	192.168.0.100	10.10.1.100	TCP	66	55325→80 [SYN] Seq=366197499 Win=8192 Len=0 MSS=1380 WS=4 SAC...
31	7.930221	10.10.1.100	192.168.0.100	TCP	66	80→55325 [SYN, ACK] Seq=2154790336 Ack=366197500 Win=8192 Len=...
41	10.629868	192.168.0.100	10.10.1.100	TCP	66	[TCP Spurious Retransmission] 55324→80 [SYN] Seq=433201323 Wi...
42	10.633208	10.10.1.100	192.168.0.100	TCP	66	[TCP Retransmission] 80→55324 [SYN, ACK] Seq=4063222169 Ack=4...
44	10.945178	10.10.1.100	192.168.0.100	TCP	66	[TCP Retransmission] 80→55325 [SYN, ACK] Seq=2154790336 Ack=3...
60	16.636255	192.168.0.100	10.10.1.100	TCP	62	[TCP Spurious Retransmission] 55324→80 [SYN] Seq=433201323 Wi...
61	16.639145	10.10.1.100	192.168.0.100	TCP	62	[TCP Retransmission] 80→55324 [SYN, ACK] Seq=4063222169 Ack=4...
62	16.951195	10.10.1.100	192.168.0.100	TCP	62	[TCP Retransmission] 80→55325 [SYN, ACK] Seq=2154790336 Ack=3...

RST + TCP 3-way ڈیلچسپی کی وجہ سے مداخلہ کی وجہ سے پہلی طاقتمندی اس کا نتیجہ ہے۔

روصلانی فحص وہ امکان ہے کہ CAPWAP میں اس کا علاج کیا جائے گا۔

25	2019-10-13	17:07:06	853334	192.168.0.100	10.10.1.100	TCP	66	48299 → 80 [SYN] Seq=3239914002 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
29	2019-10-13	17:07:09	852922	192.168.0.100	10.10.1.100	TCP	66	[TCP Retransmission] 48299 → 80 [SYN] Seq=3239914002 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
30	2019-10-13	17:07:09	854844	10.10.1.100	192.168.0.100	TCP	1	66 80 → 48299 [SYN, ACK] Seq=808763519 Ack=3239914003 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
31	2019-10-13	17:07:09	855287	192.168.0.100	10.10.1.100	TCP	54	48299 → 80 [ACK] Seq=3239914003 Ack=808763520 Win=66240 Len=0
34	2019-10-13	17:07:14	856996	192.168.0.100	10.10.1.100	TCP	2	54 48299 → 80 [FIN, ACK] Seq=3239914003 Ack=808763520 Win=66240 Len=0
35	2019-10-13	17:07:15	861451	10.10.1.100	192.168.0.100	TCP	62	[TCP Retransmission] 80 → 48299 [SYN, ACK] Seq=808763519 Ack=3239914003 Win=65535 Len=0 MSS=1380 SACK_PERM=1
36	2019-10-13	17:07:15	861970	192.168.0.100	10.10.1.100	TCP	66	[TCP Dup ACK 31#1] 48299 → 80 [ACK] Seq=3239914004 Ack=808763520 Win=66240 Len=0 SLE=808763519 SRE=808763520
39	2019-10-13	17:07:17	854051	192.168.0.100	10.10.1.100	TCP	54	[TCP Retransmission] 48299 → 80 [FIN, ACK] Seq=3239914003 Ack=808763520 Win=66240 Len=0
40	2019-10-13	17:07:23	855012	192.168.0.100	10.10.1.100	TCP	54	[TCP Retransmission] 48299 → 80 [FIN, ACK] Seq=3239914003 Ack=808763520 Win=66240 Len=0
46	2019-10-13	17:07:27	858949	10.10.1.100	192.168.0.100	TCP	3	54 80 → 48299 [RST] Seq=808763520 Win=0 Len=0

ةيسيئرلا طاقنلا:

1. ةيامحلا رادج رباع TCP 3-way ٥حفاصم رمت.
2. /ةفنع زل يمعلالا لسري ناوث 5 يل اوح دعب.
3. ٥هيلالا لسريو TCP RST عضونم مدخلالا يهتنى، ةيناث 20 يل اوح دعب.

ةيثلاث TCP ٥حفاصم دوجونم مغرلا ىلع هنأب جاتنتسالا نكمي ،طاقتلالا اذه ىلع ءانب (ريشت) ٥دح او ةياهن ٤طقن ىلع عق اولالا يف اهمامتا متى ال هنأ ودبىي ،ةيامحلا رادج رباع هاجت إلالا (كلذ ىلإ لاس رالا ٤داع) تاي لمع.

اهب ىصوملا تاءارج إلأ

3.1 ٤ل احلا يف عيشلا سفن

3.3.1 ليمعلالا نم ٤ل جو فملا TCP 3-way + RST

ةروصلالا يف حضوم وه امك ،اهسفن مزحلالا ىلع ةيامحلا رادج نم لك يوتحي.

No.	Time	Source	Destination	Protocol	Length	Info	
129	2019-10-13	17:09:20.513355	192.168.0.100	10.10.1.100	TCP	1	66 48355 → 80 [SYN] Seq=2581697538 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
130	2019-10-13	17:09:20.514011	10.10.1.100	192.168.0.100	TCP	66	80 → 48355 [SYN, ACK] Seq=1633018698 Ack=2581697539 Win=8192 Len=0 MSS=1
131	2019-10-13	17:09:20.514438	192.168.0.100	10.10.1.100	TCP	54	48355 → 80 [ACK] Seq=2581697539 Ack=1633018699 Win=66240 Len=0
132	2019-10-13	17:09:39.473089	192.168.0.100	10.10.1.100	TCP	2	54 48355 → 80 [RST, ACK] Seq=2581697939 Ack=1633018699 Win=0 Len=0

ةيسيئرلا طاقنلا:

1. ةيامحلا رادج رباع TCP 3-way ٥حفاصم رمت.
2. ٥هيلالا لسريو TCP RST لوك وتر ب نع ليمعلالا ىلختي ،ةيناث 20 يل اوح دعب.

يلى ام جاتنتسالا نكمي ،روصلالا هذه ىلإ ادانتساو:

- لاصتالا عاهن ررقتو ٥دح او ةياهن ٤طقن فقوتت ،ةيناث 20-5 دعب.

اهب ىصوملا تاءارج إلأ

3.1 ٤ل احلا يف عيشلا سفن

3.4.1 مدخلالا نم يروفلا TCP + RST

ةروصلالا يف حضوم وه امك ،مزحلالا هذه ىلع ةيامحلا رادج نم لك يوتحي.

No.	Time	Source	Destination	Protocol	Length	Info
26	2019-10-13 17:07:07.104410	192.168.0.100	10.10.1.100	TCP	66	48300 → 80 [SYN] Seq=2563435279 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
27	2019-10-13 17:07:07.105112	10.10.1.100	192.168.0.100	TCP	66	80 → 48300 [SYN, ACK] Seq=3757137497 Ack=2563435280 Win=8192 Len=0 MSS=1380
28	2019-10-13 17:07:07.105554	192.168.0.100	10.10.1.100	TCP	54	48300 → 80 [ACK] Seq=2563435280 Ack=3757137498 Win=66240 Len=0
41	2019-10-13 17:07:07.106325	10.10.1.100	192.168.0.100	TCP	54	80 → 48300 [RST] Seq=2563435280 Win=0 Len=0

ةيسيئرلا طاقنلا:

1. ةيامحلا رادج رباع TCP 3-way ٰفاصم رمت.
2. ةيناث يللم ٰعصبب ACK ٰمزح دعب مداخلا نم TCP RST كانه.

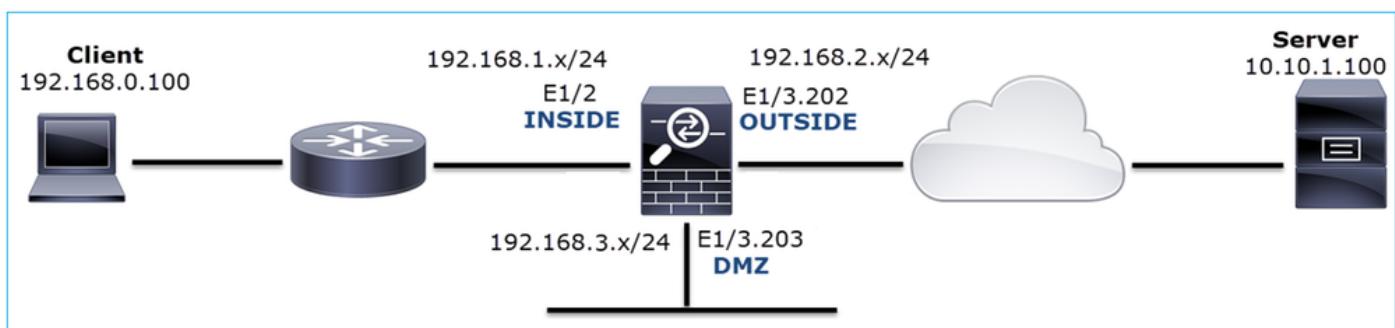
اهب ىصوملا تاءارجإلا

مداخلا ىلإ نكمي ام برقأ روصلا طاقتلا :ءارجإلا.

لسري يذلا راسملأا يف زاهج وأ مداخ دوجو ىلإ مداخلا نم يروفلا TCP RST ريشي نأ نكمي RST. ردصم ددحو هسفن مداخلا ىلع طاقتلا برق TCP RST.

ليمعلأا نم ٰلاحلا 4. TCP RST

طاطخملا ٰروصلأا هذه ضرعت:



لمعي ال ٰلكشملا فصو.

رثأتملأا قفتللا:

SRC IP: 192.168.0.100

DST IP: 10.10.1.100

لوكوتورب: لوكوتورب TCP 80

رسأ ليلحت

كرحم ىلع طاقتلا تايملع نيكمنتب مق FTD LINA.

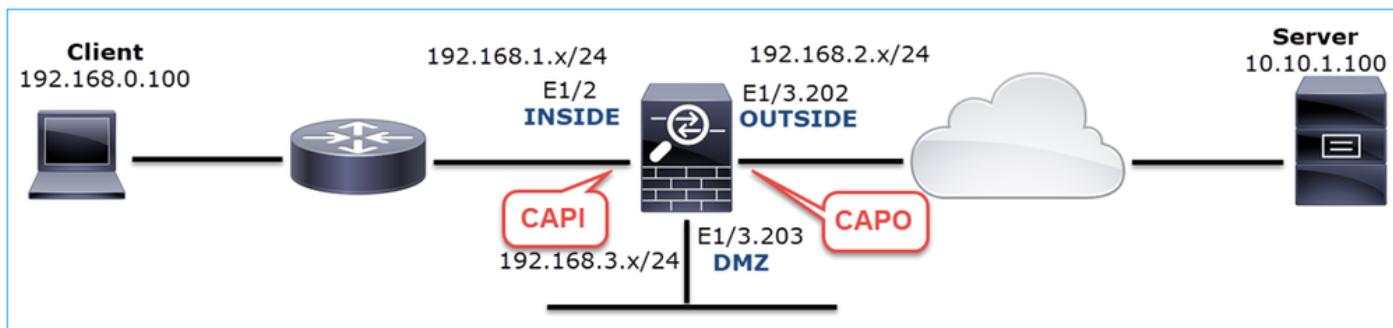
<#root>

```

firepower#
capture CAPI int INSIDE match ip host 192.168.0.100 host 10.10.1.100
firepower#

```

```
capture CAPO int OUTSIDE match ip host 192.168.0.100 host 10.10.1.100
```



لەمۇي اىل ويىرانىي س - طاقىتلە:

تايىوتەم يە ھەذىھ CAPI.

```
<#root>
```

```
firepower#
```

```
show capture CAPI
```

14 packets captured

```
1: 12:32:22.860627 192.168.0.100.47078 > 10.10.1.100.80: S 4098574664:4098574664(0) win 8192 <mss  
2: 12:32:23.111307 192.168.0.100.47079 > 10.10.1.100.80: S 2486945841:2486945841(0) win 8192 <mss  
3: 12:32:23.112390 192.168.0.100.47079 > 10.10.1.100.80: R 3000518858:3000518858(0) win 0  
4: 12:32:25.858109 192.168.0.100.47078 > 10.10.1.100.80: S 4098574664:4098574664(0) win 8192 <mss  
5: 12:32:25.868698 192.168.0.100.47078 > 10.10.1.100.80: R 1386249853:1386249853(0) win 0  
6: 12:32:26.108118 192.168.0.100.47079 > 10.10.1.100.80: S 2486945841:2486945841(0) win 8192 <mss  
7: 12:32:26.109079 192.168.0.100.47079 > 10.10.1.100.80: R 3000518858:3000518858(0) win 0  
8: 12:32:26.118295 192.168.0.100.47079 > 10.10.1.100.80: R 3000518858:3000518858(0) win 0  
9: 12:32:31.859925 192.168.0.100.47078 > 10.10.1.100.80: S 4098574664:4098574664(0) win 8192 <mss  
10: 12:32:31.860902 192.168.0.100.47078 > 10.10.1.100.80: R 1386249853:1386249853(0) win 0  
11: 12:32:31.875229 192.168.0.100.47078 > 10.10.1.100.80: R 1386249853:1386249853(0) win 0  
12: 12:32:32.140632 192.168.0.100.47079 > 10.10.1.100.80: R 3000518858:3000518858(0) win 0  
13: 12:32:32.159995 192.168.0.100.47079 > 10.10.1.100.80: S 2486945841:2486945841(0) win 8192 <mss  
14: 12:32:32.160956 192.168.0.100.47079 > 10.10.1.100.80: R 3000518858:3000518858(0) win 0
```

14 packets shown

تايىوتەم يە ھەذىھ CAPO:

```
<#root>
```

```
firepower#
```

```
show capture CAPO
```

11 packets captured

```
1: 12:32:22.860780 802.1Q vlan#202 P0 192.168.0.100.47078 > 10.10.1.100.80: S 1386249852:1386249852  
2: 12:32:23.111429 802.1Q vlan#202 P0 192.168.0.100.47079 > 10.10.1.100.80: S 3000518857:3000518857
```

```

3: 12:32:23.112405 802.1Q vlan#202 PO 192.168.0.100.47079 > 10.10.1.100.80: R 3514091874:3514091874
4: 12:32:25.858125 802.1Q vlan#202 PO 192.168.0.100.47078 > 10.10.1.100.80: S 1386249852:1386249852
5: 12:32:25.868729 802.1Q vlan#202 PO 192.168.0.100.47078 > 10.10.1.100.80: R 2968892337:2968892337
6: 12:32:26.108240 802.1Q vlan#202 PO 192.168.0.100.47079 > 10.10.1.100.80: S 3822259745:3822259745
7: 12:32:26.109094 802.1Q vlan#202 PO 192.168.0.100.47079 > 10.10.1.100.80: R 40865466:40865466(0)
8: 12:32:31.860062 802.1Q vlan#202 PO 192.168.0.100.47078 > 10.10.1.100.80: S 4294058752:4294058752
9: 12:32:31.860917 802.1Q vlan#202 PO 192.168.0.100.47078 > 10.10.1.100.80: R 1581733941:1581733941
10: 12:32:32.160102 802.1Q vlan#202 PO 192.168.0.100.47079 > 10.10.1.100.80: S 4284301197:4284301197
11: 12:32:32.160971 802.1Q vlan#202 PO 192.168.0.100.47079 > 10.10.1.100.80: R 502906918:502906918(0)

11 packets shown

```

ةيامحلا راجد تالجس رهظت:

<#root>

firepower#

show log | i 47741

```

Oct 13 2019 13:57:36: %FTD-6-302013: Built inbound TCP connection 4869 for INSIDE:192.168.0.100/47741 (0)
Oct 13 2019 13:57:36: %FTD-6-302014: Teardown TCP connection 4869 for INSIDE:192.168.0.100/47741 to OUT

```

TCP Reset-O from INSIDE

```

Oct 13 2019 13:57:39: %FTD-6-302013: Built inbound TCP connection 4870 for INSIDE:192.168.0.100/47741 (0)
Oct 13 2019 13:57:39: %FTD-6-302014: Teardown TCP connection 4870 for INSIDE:192.168.0.100/47741 to OUT

```

TCP Reset-O from INSIDE

```

Oct 13 2019 13:57:45: %FTD-6-302013: Built inbound TCP connection 4871 for INSIDE:192.168.0.100/47741 (0)
Oct 13 2019 13:57:45: %FTD-6-302014: Teardown TCP connection 4871 for INSIDE:192.168.0.100/47741 to OUT

```

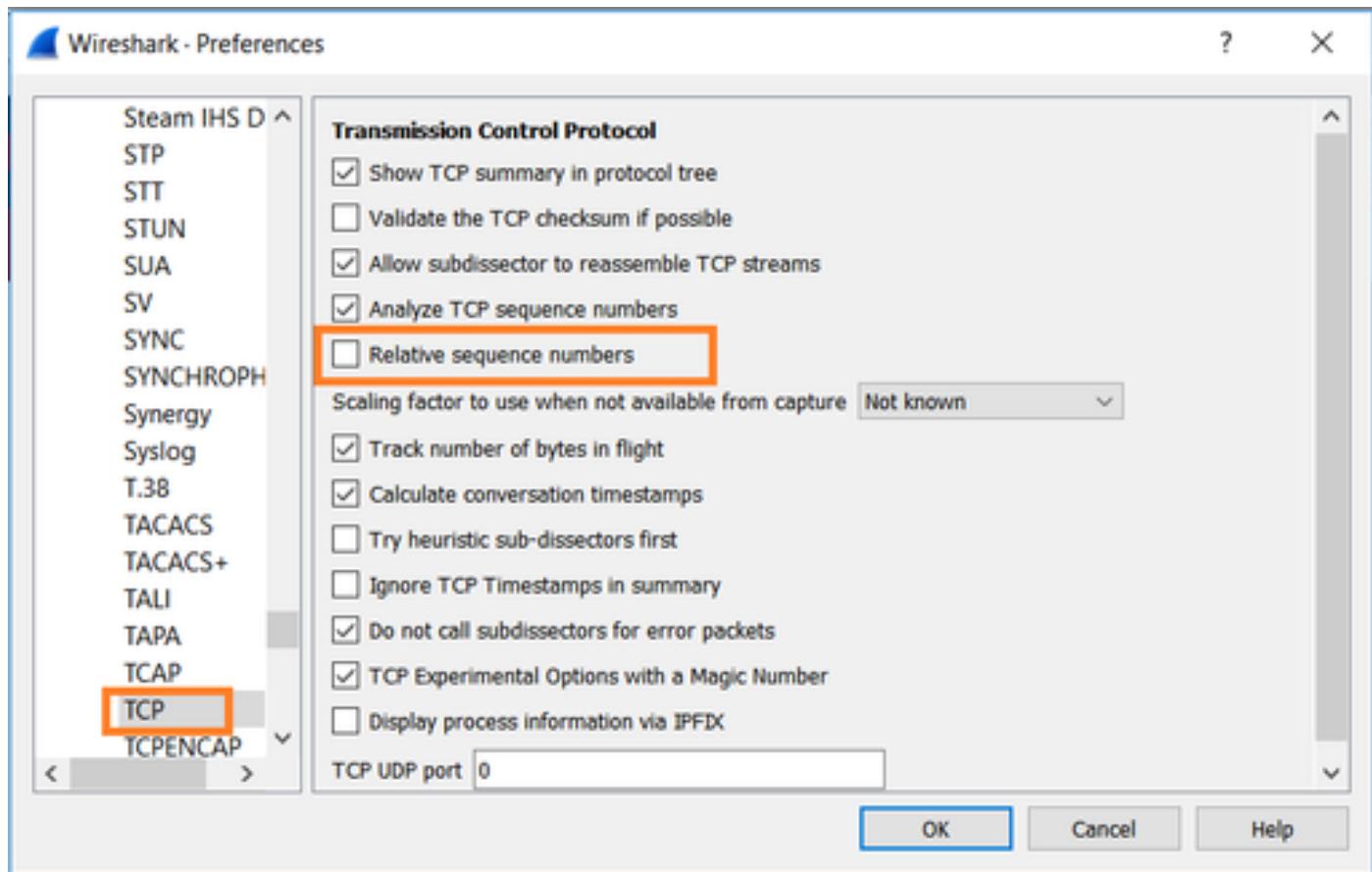
ةيلخادلا ةيامحلا راجد ةهجاولى تالجسلا هذه ريشت

رسأ Wireshark يف CAPI:

ةروصلالا يف حضوم وه امك ،لاؤالا TCP قفت عبتا.

No.	Time	Source	Destination	Protocol	Length	Info	
1	2019-10-13 14:32:22.860627	192.168.0.100	10.10.1.100	TCP	66	47078 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PEE	
2	2019-10-13 14:32:23.111307	192.168.0.100	10.10.1.100	TCP	66	47079 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PEE	
3	2019-10-13 14:32:23.112390	192.168.0.100	10.10.1.100	TCP	54	47079 > 80 [RST] Seq=513573017 Win=0 Len=0	
4	2019-10-13 14:32:25.858109	192.168.0.100	10.10.1.100	TCP	66	[TCP Retransmission] 47078 > 80 [SYN] Seq=0 Win=8192 Len=0	
5	2019-10-13 14:32:25.868698	192.168.0.100	10.10.1.100	TCP	54	47078 > 80 [RST] Seq=5182642485 Win=0 Len=0	
6	2019-10-13 14:32:26.108118	192.168.0.100	10.10.1.100	TCP	66	[TCP Retransmission] 47079 > 80 [SYN] Seq=0 Win=8192 Len=0	
7	2019-10-13 14:32:26.109079	192.168.0.100	10.10.1.100	TCP	54	47079 > 80 [RST] Seq=513573017 Win=0 Len=0	
8	2019-10-13 14:32:26.118295	192.168.0.100	10.10.1.100	TCP	54	47079 > 80 [RST] Seq=513573017 Win=0 Len=0	
9	2019-10-13 14:32:31.859925	192.168.0.100	10.10.1.100	TCP	62	[TCP Retransmission] 47078 > 80 [SYN] Seq=0 Win=8192 Len=0	
10	2019-10-13 14:32:31.860902	192.168.0.100	10.10.1.100	TCP	54	47078 > 80 [RST] Seq=5182642485 Win=0 Len=0	
11	2019-10-13 14:32:31.875229	192.168.0.100	10.10.1.100	TCP	54	47078 > 80 [RST] Seq=5182642485 Win=0 Len=0	
12	2019-10-13 14:32:32.140632	192.168.0.100	10.10.1.100	TCP	54	47079 > 80 [RST] Seq=513573017 Win=0 Len=0	
13	2019-10-13 14:32:32.159995	192.168.0.100	10.10.1.100	TCP	62	[TCP Retransmission] 47079 > 80 [SYN] Seq=0 Win=8192 Len=0	
14	2019-10-13 14:32:32.160956	192.168.0.100	10.10.1.100	TCP	54	47079 > 80 [RST] Seq=513573017 Win=0 Len=0	

ماقراً رايح ديدحت يغلاو TCP > تالوكوتورب > تاليضفت > ريرحت يلى لقتنا، تتحت
ةروصلالا يف حضوم وه امك ةيبسنلا لسلستلا



طاقتلار يف لوألا قفتلار تاي وتحم ئروصلار ھذە رەھەنەت:

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-13 14:32:22.860627	192.168.0.100	10.10.1.100	TCP	66	47078 → 80 [SYN] Seq=4098574664 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
4	2019-10-13 14:32:25.858109	192.168.0.100	10.10.1.100	TCP	66	[TCP Retransmission] 47078 → 80 [SYN] Seq=4098574664 Win=8192 Len=0 MSS=1
5	2019-10-13 14:32:25.868698	192.168.0.100	10.10.1.100	TCP	54	47078 → 80 [RST] Seq=1386249853 Win=0 Len=0
9	2019-10-13 14:32:31.859925	192.168.0.100	10.10.1.100	TCP	62	[TCP Retransmission] 47078 → 80 [SYN] Seq=4098574664 Win=8192 Len=0 MSS=1
10	2019-10-13 14:32:31.860002	192.168.0.100	10.10.1.100	TCP	54	47078 → 80 [RST] Seq=1386249853 Win=0 Len=0
11	2019-10-13 14:32:31.875229	192.168.0.100	10.10.1.100	TCP	54	47078 → 80 [RST] Seq=1386249853 Win=0 Len=0

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8), Dst: Cisco_f6:1d:ae (00:be:75:f6:1d:ae)
> Internet Protocol Version 4, Src: 192.168.0.100, Dst: 10.10.1.100
Transmission Control Protocol, Src Port: 47078, Dst Port: 80, Seq: 4098574664, Len: 0
Source Port: 47078
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 4098574664
[Next sequence number: 4098574664]
Acknowledgment number: 0
1000 = Header Length: 32 bytes (8)
Flags: 0x002 (SYN)
Window size value: 8192
[Calculated window size: 8192]
Checksum: 0x8cd1 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
> [Timestamps]

يسيئرلار طاقنلار:

1. ئەم زىخ لىمعلا لىسلىرى TCP syn.
2. ئەم زىخ لىمعلا لىسلىرى TCP RST.
3. يواست لىسلسىت مقر ئەم يقىلىع 4098574664.

يولع طاقتلا يف قفتلسا سفن يوتحي CAPO:

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-13 14:32:22.860780	192.168.0.100	10.10.1.100	TCP	70	47078 → 80 [SYN] Seq=1386249852 Win=8192 Len=0 MSS=1380 WS=4 SACK_PERM=1
4	2019-10-13 14:32:25.858125	192.168.0.100	10.10.1.100	TCP	70	[TCP Retransmission] 47078 → 80 [SYN] Seq=1386249852 Win=8192 Len=0 MSS=1380
5	2019-10-13 14:32:25.868729	192.168.0.100	10.10.1.100	TCP	58	47078 → 80 [RST] Seq=2968892337 Win=0 Len=0

2

> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Cisco_f6:1d:8e (00:be:75:f6:1d:8e), Dst: Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 202
> Internet Protocol Version 4, Src: 192.168.0.100, Dst: 10.10.1.100
Transmission Control Protocol, Src Port: 47078, Dst Port: 80, Seq: 1386249852, Len: 0

ةيسيئرلا طاقنلا:

1. ل ةيئاوشعلـا ةيامـحـلـا رـادـجـ لـيـمـعـلـا لـسـرـيـ.
2. 2. لـيـمـزـنـهـ لـيـمـعـلـا لـسـرـيـ.

يـلـيـ اـمـ جـاتـنـتـسـ إـنـكـمـيـ ،ـنـيـتـحـمـلـلـاـ إـلـاـ اـدـانـتـسـ اوـ

- مـداـخـلـاـوـ لـيـمـعـلـاـ نـيـبـ هـاجـتـإـلـاـ ةـيـثـالـثـ TCPـ دـجـوـتـ الـ.
- ظـاـقـتـلـاـ يـفـ TCP~ RSTـ لـسـلـسـتـ مـقـرـ ةـمـيـقـ لـيـمـعـلـاـ نـمـ يـتـأـيـ يـذـلـاـ كـانـهـ 1386249853ـ يـهـ.

اهـبـ يـصـوـمـلـاـ تـاءـارـجـ إـلـاـ

ةـلـأـسـمـلـاـ هـذـهـ قـاطـنـ قـيـيـضـتـ ةـدـايـزـ وـهـ عـرـفـلـاـ اـذـهـ يـفـ ةـدـراـوـلـاـ تـاءـارـجـ إـلـاـ نـمـ ضـرـغـلـاوـ

لـيـمـعـلـاـ طـاقـتـلـاـ 1. ءـارـجـ إـلـاـ.

دوـجـوـ يـوـقـ رـشـفـمـ كـانـهـ ،ـةـيـامـحـلـاـ رـادـجـ يـلـعـ اـعـمـجـ مـتـ يـتـلـاـ طـاقـتـلـلـاـ تـايـلـمـعـ إـلـاـ اـدـانـتـسـاـ 1386249853ـ ةـمـيـقـبـ TCP~ RSTـ لـيـمـعـلـاـ نـأـ ةـقـيـقـحـ يـلـاـ اـذـهـ دـنـتـسـيـ لـثـامـتـمـ رـيـغـ قـفـدـتـ (ـيـئـاـوشـعـلـاـ)ـ ISـ:

No.	Time	Source	Destination	Protocol	Length	Info
19	6.040337	192.168.0.100	10.10.1.100	TCP	66	47078>80 [SYN] Seq=4098574664 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
29	9.037499	192.168.0.100	10.10.1.100	TCP	66	[TCP Retransmission] 47078>80 [SYN] Seq=4098574664 Win=8192 Len=0 MSS=1460 WS=4
30	9.048155	10.10.1.100	192.168.0.100	TCP	66	[TCP ACKed unseen segment] 80>47078 [SYN, ACK] Seq=1924342422 Ack=1386249853 Win=0
31	9.048184	192.168.0.100	10.10.1.100	TCP	54	47078>80 [RST] Seq=1386249853 Win=0 Len=0

1

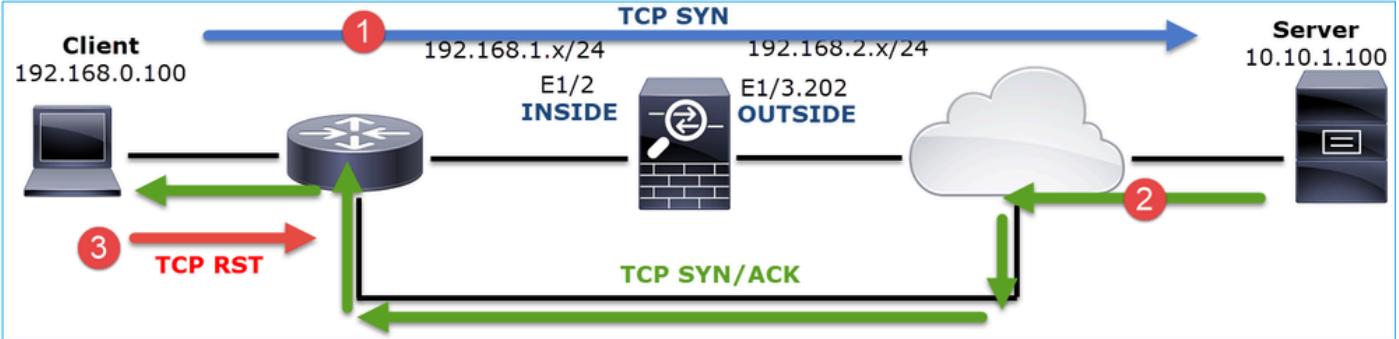
2

3

ةـيـسـيـئـرـلـاـ طـاقـنـلـاـ:

1. ئـرـيـ يـذـلـاـ هـسـفـنـ وـهـ 4098574664ـ وـهـ يـلـسـلـسـلـاـ مـقـرـلـاـ TCP~ synـ ةـيـلـخـادـلـاـ ةـهـجـاـوـلـاـ يـفـ ةـيـامـحـلـاـ رـادـجـ يـلـعـ
2. بـبـسـبـ نـوـكـيـ نـأـ عـقـوـتـمـلـاـ (ـISـNـ randomizationـ).ـ ةـيـامـحـلـاـ رـادـجـ طـاقـتـلـاـ يـفـ ةـمـزـنـهـ 1386249853ـ
3. هـنـكـلـوـ ،ـACKـ 4098574665ـ مـقـرـ ةـمـيـقـ عـقـوـتـ نـأـ ذـنـمـ TCP~ RSTـ لـيـمـعـلـاـ لـسـرـيـ 1386249853ـ

يـلـاتـلـاـ وـحـنـلـاـ يـلـعـ كـلـذـ لـيـثـمـتـ نـكـمـيـ وـ

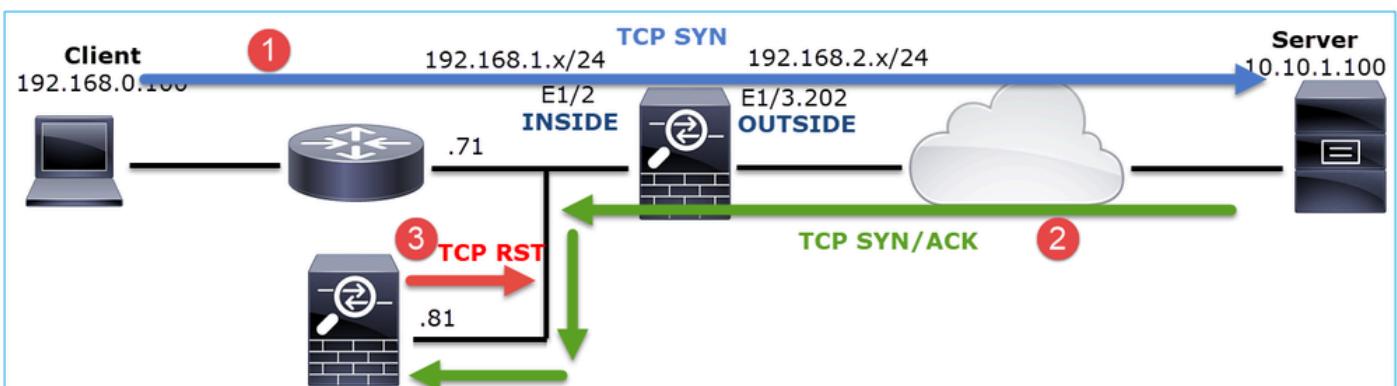


ةيامحلا رادجوليمعلانيب هيجوتلavnم ققحت 2. ءارجلإا.

يلى ام ديكأت:

- عقوتملا نيوانعلا يه طاقتلالا تايملع يف اهتيفرمت يتلا MAC نيوانع .
- لثامتم لميتعلواو ةيامحلا رادج نيب هيجوتلavnأ نم دكأت.

هيجوت دوجو ءانثأ لميتعلواو ةيامحلا رادج نيب عقي زاهج نم RST يتأي ثيحب تاهويرانيس كانه ةروصلالا يف ةيجدومن ةلاح رهظت. ةيلخادلا ةكبشلا يف لثامتم ريع :



ردصملا MAC ناوونع نيب قرفلا ظحال. يوتحملاءهيلع يوتحي طاقتلالا ناف، ةلاحلا هذه يف ردصملا MAC ناوونعو TCP RST ب صالحلا ردصملا MAC ناوونع لباقم TCP syn/ACK:

```
<#root>
```

```
firepower#
```

```
show capture CAPI detail
```

```
1: 13:57:36.730217
```

```
4c4e.35fc.fcd8
```

```
00be.75f6.1dae 0x0800 Length: 66
```

```
192.168.0.100.47740 > 10.10.1.100.80: S [tcp sum ok] 3045001876:3045001876(0) win 8192 <mss 1460,
```

```
2: 13:57:36.981104 4c4e.35fc.fcd8 00be.75f6.1dae 0x0800 Length: 66
```

```
192.168.0.100.47741 > 10.10.1.100.80: S [tcp sum ok] 3809380540:3809380540(0) win 8192 <mss 1460,
```

```
3: 13:57:36.981776 00be.75f6.1dae
```

```
a023.9f92.2a4d
```

```
0x0800 Length: 66
```

```
10.10.1.100.80 > 192.168.0.100.47741: S [tcp sum ok] 1304153587:1304153587(0) ack 3809380541 win
```

4: 13:57:36.982126

a023.9f92.2a4d

00be.75f6.1dae 0x0800 Length: 54
192.168.0.100.47741 > 10.10.1.100.80:

R

[tcp sum ok] 3809380541:3809380541(0) ack 1304153588 win 8192 (ttl 255, id 48501)

...

1) ويرانيسلا (TCP لوكوتوربل عي طبلا لقنا 5. ةلاحلا

ةلكشملا فصو:

دحلا نأ نم مغرا يلع .عي طب 10.77.19.11 و 10.11.4.171 ةفيضملا ۆزهجألا نيب SFTP لقنا نأ إلإ ،ةيناثلا يف تباجيم 100 وه نيفيضملا نيب (BW) يددرتلا قاطنلا ضرع لىندألا .ةيناثلا يف تباجيم 5 زواجتت ال لقنا ۆعرس.

و 10.11.2.124 172.25.18.134 10.11.2.124 و سفن تقولا يفو .ريثكب كلذ نم ىلعأ.

ةيساسألا ةيرظنلا:

يددرتللا قاطنلا ريخأت جتنم ۆتساوب دحاو TCP قفدتلىوصقلا لقنا ۆعرس ديدحت متي (BDP).
ةروصلالا يف ۆمدختسملا ۆغىصلالا ضرع متي:

$$\text{Max Single TCP Flow Throughput [bps]} = \frac{\text{TCP Window (Bytes)}}{\text{RTT (Seconds)}} \times 8 \text{ [bits/Byte]}$$

انه دراوملا نم ققحت BDP لوح ليصافتلا نم دي زمل:

- [يف تباجيج 1 طابترالا ىتح طقف ئيناثلا يف تباجيم 10 كقيبطت مدخلتسي اذامل ئيناثلا؟](#)
- [قيامحلا رادج عادأ نيسحت - مدقتم - BRKSEC-3021](#)

عي طبلا لقنا - 1 ويرانيسلا

ططخملا ةروصلالا هذه ضرعات:



رثأت ملا قفت لـا:

SRC IP: 10.11.4.171

لوكوتورب DST IP: 10.77.19.11

لوكوتورب لـا SFTP (FTP SSH)

رسأ ليتحت

كـرحـمـىـلـعـ طـاقـتـلـاـ نـيـكـمـتـ

```
<#root>
firepower#
capture CAPI int INSIDE buffer 33554432 match ip host 10.11.4.171 host 10.77.19.11
firepower#
capture CAPO int OUTSIDE buffer 33554432 match ip host 10.11.4.171 host 10.77.19.11
```

⚠ رورمـلـاـ ةـكـرحـلـقـنـلـدـعـمـىـلـعـ FP1xxx وـ FP21xx طـاقـتـلـاـ ئـلـعـ LINAـ رـثـفـتـ:ـ رـيـذـحـتـ وـ FP1xxx ةـيـسـاسـأـلـاـ ةـمـظـنـأـلـاـ ئـلـعـ LINAـ طـاقـتـلـاـ نـيـكـمـتـ بـ مـقـتـ الـ FTDـ.ـ رـبـعـ رـمـتـ يـتـلـاـ كلـذـ نـمـ الـ دـبـ FTDـ).ـ رـبـعـ عـيـطـبـلـاـ لـقـنـلـاـ)ـ اـهـحـالـصـ اوـ عـادـأـلـاـ ءـاطـخـأـ فـاشـكـتـسـأـ دـنـعـ فـيـضـمـلـاـ ئـلـعـ ضـبـقـ ئـلـعـ نـأـ ئـلـاـ ةـفـاضـلـاـ بـ قـاـدـأـ HW Tapـ وـأـ نـيـتـمـاعـدـ نـيـبـ ةـحـسـفـ تـلـمـعـتـسـاـ فـيـضـمـلـاـ ئـلـعـ قـبـ cisco id CSCvo30697ـ.

```
<#root>
firepower#
capture CAPI type raw-data trace interface inside match icmp any any
WARNING: Running packet capture can have an adverse impact on performance.
```

اهـبـ ئـصـوـمـلـاـ تـاءـأـجـإـلـاـ

ةـلـأـسـمـلـاـ هـذـهـ قـاطـنـ قـيـيـضـتـ ةـدـايـزـ وـهـ عـرـفـلـاـ اـذـهـ يـفـ ةـدـراـوـلـاـ تـاءـأـجـإـلـاـ نـمـ ضـرـغـلـاـ وـ

ةدعـل او باهـلـا تـقـوـبـاسـح (RTT)

هـعـبـتـاـولـقـنـلـا قـفـدـتـدـجـ، الـوـاـ:

No.	Time	Source	Destination	Protocol	Length	Window size value
1	0.000000	10.11.4.171	10.77.19.11	TCP	70	49640
2	0.072521	10.77.19.11		Mark/Unmark Packet	70	49680
3	0.000168	10.11.4.171		Ignore/Unignore Packet	58	49680
4	0.077068	10.77.19.11		Set/Unset Time Reference	80	49680
5	0.000152	10.11.4.171		Time Shift...	58	49680
6	0.000244	10.11.4.171		Packet Comment...	80	49680
7	0.071545	10.77.19.11		Edit Resolved Name	58	49680
8	0.000153	10.11.4.171		Apply as Filter	738	49680
9	0.041288	10.77.19.11		Prepare a Filter	58	49680
10	0.000168	10.11.4.171		Conversation Filter	58	49680
11	0.030165	10.77.19.11		Colorize Conversation	82	49680
12	0.000168	10.11.4.171		SCTP		
				Follow		TCP Stream
						UDP Stream
						SSL Stream
						HTTP Stream

نم اذهـوـةـقـبـاسـلـا ةـضـورـعـمـلـا ةـمـزـحـلـا ذـنـمـ يـنـاوـثـلـا رـاهـظـاـلـا Wireshark ضـرـعـةـقـيـرـطـ رـيـغـتـبـ مـقـ بـاسـحـ لـيـهـسـتـ هـنـأـشـ:

Protocol	Length	Window size value	Info
TCP	70	49640	39744 → 22 [SYN] Seq=1737026093
TCP	70	49680	22 → 39744 [SYN, ACK] Seq=8351720
TCP	58	49680	39744 → 22 [ACK] Seq=1737026094
SSHv2	80	49680	Server: Protocol (SSH-2.0-Sun_SS
TCP	58	49680	39744 → 22 [ACK] Seq=1737026094

Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+1
 Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
 Time of Day (01:02:03.123456) Ctrl+Alt+2
 Seconds Since 1970-01-01 Ctrl+Alt+3
 Seconds Since Beginning of Capture Ctrl+Alt+4
 Seconds Since Previous Captured Packet Ctrl+Alt+5
 ● Seconds Since Previous Displayed Packet Ctrl+Alt+6

ردصـمـلـا وـنـامـهـدـحـاـ) مـزـحـ لـدـابـتـ يـتـيـلـمـعـ نـيـبـ تـقـوـلـا مـيـقـ ةـفـاضـاـلـا لـالـخـ نـكـمـيـ لـسـرـأـ يـذـلـا زـاهـجـلـا وـةـيـاـمـحـلـا رـادـجـ نـيـبـ #2 RTT ةـمـزـحـلـا ضـرـعـتـ ، ةـلـاحـلـا هـذـهـ يـفـ . ةـهـجـوـلـا وـنـخـآـلـاـوـ ACK ةـمـزـحـ لـسـرـأـ يـذـلـا زـاهـجـلـا وـةـيـاـمـحـلـا رـادـجـ نـيـبـ #3 RTT ةـمـزـحـلـا ضـرـعـتـ . (مـدـاخـلـاـ) SYN/ACK ةـمـزـحـ لـمـاـشـلـا RTT لـوـجـ اـرـيـدـقـتـ نـيـمـقـرـلـا ةـفـاضـاـ رـفـوتـ . (لـيـمـعـلـاـ)

1 0.000000	10.11.4.171	10.77.19.11	TCP	70	49640 39744 → 22 [SYN] Seq=1737026093 Win=49640 Len=0 MSS=1460 WS=1 SACK_PERM=1
2 0.072521	10.77.19.11	10.11.4.171	TCP	70	49680 22 → 39744 [SYN, ACK] Seq=835172681 Ack=1737026094 Win=49680 Len=0 MSS=1380 WS=1 SACK_PERM=1
3 0.000168	10.11.4.171	10.77.19.11	TCP	58	49680 39744 → 22 [ACK] Seq=1737026094 Ack=835172682 Win=49680 Len=0
4 0.077068	10.77.19.11	10.11.4.171	SSHv2	80	49680 Server: Protocol (SSH-2.0-Sun_SSH_1.1.8)
5 0.000152	10.11.4.171	10.77.19.11	TCP	58	49680 39744 → 22 [ACK] Seq=1737026094 Ack=835172704 Win=49680 Len=0
6 0.000244	10.11.4.171	10.77.19.11	SSHv2	80	49680 Client: Protocol (SSH-2.0-Sun_SSH_1.1.4)
7 0.071545	10.77.19.11	10.11.4.171	TCP	58	49680 22 → 39744 [ACK] Seq=835172704 Ack=1737026116 Win=49680 Len=0
8 0.000153	10.11.4.171	10.77.19.11	SSHv2	538	49680 Client: Key Exchange Init
9 0.041288	10.77.19.11	10.11.4.171	SSHv2	738	49680 Server: Key Exchange Init
10 0.000168	10.11.4.171	10.77.19.11	TCP	58	49680 39744 → 22 [ACK] Seq=835173384 Ack=835173384 Win=49680 Len=0
11 0.030165	10.77.19.11	10.11.4.171	TCP	58	49680 22 → 39744 [ACK] Seq=835173384 Ack=1737026596 Win=49680 Len=0
12 0.000168	10.11.4.171	10.77.19.11	SSHv2	82	49680 Client: Diffie-Hellman Group Exchange Request

ةيناث RTT ≈ 80

ةذفان TCP مجح باسح

قيبط ددح و بوسحمل الةذفانلا مجح ديدحتو، TCP سأرعي سوت و سأرعي سوت مدق دومعك:

Transmission Control Protocol, Src Port: 22, Dst Port: 39744, Seq: 835184024, Ack: 1758069308, Len: 32

Source Port: 22
Destination Port: 39744
[Stream index: 0]
[TCP Segment Len: 32]
Sequence number: 835184024
[Next sequence number: 835184056]
Acknowledgment number: 1758069308
0101 = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 49680
[Calculated window size: 49680]
[Window size scaling factor: 1]
Checksum: 0xb49 [unverified]
[Checksum Status: Unverified]

The scaled window size (if scaling has been applied): 49680

Window [Calculated]

Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column

ةذفانلا مجح لىصق ألا دحلا ۆميق يه ام ۆفرعمل بوسحمل الةذفانلا مجح ۆميق دومع نم ققحت ميقلاب يتررت و دومعلا مسا ديدحت اضيأ كنكمي TCP. لمع ۆسلج عانثأ.

اهناع نلعمل ميقلاب نم ققحتلا كيلع بجييف، (ليمع > مداخ) فلم ليزنـت رابـتـخـاب تـمـقـ اـذـاـ ىـصـقـأـ مـداـخـلـاـ لـبـقـ نـمـ اـهـنـاعـ نـلـعـمـلـاـ ۆـذـفـانـلـاـ مجـحـ لـيـوـصـقـلـاـ ۆـمـيـقـلـاـ دـدـحـتـ .ـمـداـخـلـاـ ۆـطـسـ اوـبـ اـهـقـيـقـحـتـ مـتـيـ لـقـنـ ۆـعـرـسـ.

تياب TCP ≈ 50000 ۆذفان مجح غلبي، ۆلاحـلاـ هـذـهـ يـفـ

No.	Time	Source	Destination	Protocol	Length	Calculated window size	Info
24...	0.000091	10.11.4.171	10.77.19.11	TCP	58	49680 39744 → 22 [ACK] Seq=1758069341 Ack=835173384	
24...	0.000077	10.77.19.11	10.11.4.171	TCP	58	49680 22 → 39744 [FIN, ACK] Seq=835184152 Ack=1758069341	
24...	0.071605	10.77.19.11	10.11.4.171	TCP	58	49680 22 → 39744 [ACK] Seq=835184152 Ack=1758069340	
24...	0.000153	10.11.4.171	10.77.19.11	TCP	58	49680 39744 → 22 [FIN, ACK] Seq=1758069340 Ack=835173384	
24...	0.000443	10.11.4.171	10.77.19.11	SSHv2	90	49680 Client: Encrypted packet (len=32)	
24...	0.071666	10.77.19.11	10.11.4.171	SSHv2	154	49680 Server: Encrypted packet (len=96)	
24...	0.044050	10.11.4.171	10.77.19.11	TCP	58	49680 39744 → 22 [ACK] Seq=1758069308 Ack=835173384	
24...	0.073605	10.77.19.11	10.11.4.171	SSHv2	90	49680 Server: Encrypted packet (len=32)	
24...	0.000747	10.11.4.171	10.77.19.11	SSHv2	90	49680 Client: Encrypted packet (len=32)	

ىـلـعـ لـصـحـتـسـ يـدـدـرـتـلـاـ قـاطـنـلـاـ رـيـخـأـتـ جـتـنـمـ ۆـغـيـصـ مـادـخـتـسـاـ عـمـ وـمـيـقـلـاـ هـذـهـ يـلـاـ اـدـانـتـسـاـ تـبـاجـيمـ 50000*8/0.08 = 5: فـورـظـلـاـ هـذـهـ لـظـ يـفـ هـقـيـقـحـتـ نـكـمـيـ يـضـارـتـفـاـ قـاطـنـ ضـرـعـ ۆـصـقـأـ يـرـظـنـلـاـ يـضـارـتـفـاـلـاـ قـاطـنـلـاـ ضـرـعـلـ ۆـصـقـأـلاـ دـحـلـاـ ۆـيـنـاثـلـاـ يـفـ.

ةلحل اه ذه يف ليمعل اه ربختي ام قباطي اذهو.

مداخلا كل ذنم مهألاو، نيبن اجل اهك موقعي. يثالثلا TCP لاصتا ديكتا ذنم بثك نع ققحت رثؤيو. (ذفانل ايف سايق دجوي ال) $1 = 2^{10}$ ينعت يتل او 0 ذفان سايق 0ميق نع نالع ايلاب ليوحتل اه دعم ايلع ابلس اذه:

No.	Time	Source	Destination	Protocol	Length	Window size value	Info
1	0.000000	10.11.4.171	10.77.19.11	TCP	70	49640	39744 → 22 [SYN] Seq=1737026093 Win=49640 Len=0 MSS=1460 WS=1 SACK_PERM=1
2	0.072521	10.77.19.11	10.11.4.171	TCP	70	49680	22 → 39744 [SYN, ACK] Seq=835172681 Ack=1737026094 Win=49680 Len=0 MSS=1386 WS=1 SACK

```

> Frame 2: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: Cisco_1f:72:4e (00:5d:73:1f:72:4e), Dst: Cisco_f8:19:ff (00:22:bd:f8:19:ff)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 102
> Internet Protocol Version 4, Src: 10.77.19.11, Dst: 10.11.4.171
▼ Transmission Control Protocol, Src Port: 22, Dst Port: 39744, Seq: 835172681, Ack: 1737026094, Len: 0
  Source Port: 22
  Destination Port: 39744
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 835172681
  [Next sequence number: 835172681]
  Acknowledgment number: 1737026094
  1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x012 (SYN, ACK)
  Window size value: 49680
  [Calculated window size: 49680]
  Checksum: 0xa91b [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
    > TCP Option - Maximum segment size: 1380 bytes
    > TCP Option - No-Operation (NOP)
      > TCP Option - Window scale: 0 (multiply by 1)
      > TCP Option - No-Operation (NOP)

```

نع نلعأ يذلا صخشلا هنأ ذنم دكتاو، مداخلا اه دفع 0ر0ص طاقتلال اه جاح كانه، اه طقنا هنأ ذنم دفع (كلذب مايقلا ئيفيك ئفرعمل مداخلا قئاثو عجارا) هنـيـوكـتـ دـعـأـوـ 0 = ذـفـانـلـاـ سـايـقـمـ).

عيرسل اه لقـنـلـاـ 2ـ ويـرـانـيـسـلـاـ

(اهـسـفـنـ ئـكـبـشـلـاـ رـبـعـ عـيـرسـلـاـ لـقـنـلـاـ)ـ دـيـجـلـاـ ويـرـانـيـسـلـاـ صـحـفـنـ انـعـدـ نـآـلـاـ:

طـطـخـمـلـاـ:



مامـهـاـلـاـ قـفـدـتـ:

SRC IP: 10.11.2.124

لـوكـوتـورـبـ لـوكـوتـورـبـ لـوكـوتـورـبـ لـوكـوتـورـبـ

لـوكـوتـورـبـ لـوكـوتـورـبـ لـوكـوتـورـبـ لـوكـوتـورـبـ

FTD LINA كـرـحـمـ اـلـعـ طـاقـتـلـاـ نـيـكـمـتـ

<#root>

```

firepower#
capture CAPI int INSIDE buffer 33554432 match ip host 10.11.2.124 host 172.25.18.134
firepower#
capture CAPO int OUTSIDE buffer 33554432 match ip host 10.11.2.124 host 172.25.18.134

```

نوكی، لاحل او باهذلا تقو باسح (RTT) ≈ 300 RTT نانث.

No.	Time	Source	Destination	Protocol	Length
1	0.000000	10.11.2.124	172.25.18.134	TCP	78
2	0.267006	172.25.18.134	10.11.2.124	TCP	78
3	0.000137	10.11.2.124	172.25.18.134	TCP	70
4	0.003784	10.11.2.124	172.25.18.134	SSHv2	91
5	0.266863	172.25.18.134	10.11.2.124	TCP	70
6	0.013580	172.25.18.134	10.11.2.124	SSHv2	91

مقر TCP ڈفان سا یقم لمع نع نالع ایاب مداخلا موقی: 7.

```

> Internet Protocol Version 4, Src: 172.25.18.134, Dst: 10.11.2.124
< Transmission Control Protocol, Src Port: 22, Dst Port: 57093, Seq: 661963571, Ack: 1770516295, Len: 0
    Source Port: 22
    Destination Port: 57093
    [Stream index: 0]
    [TCP Segment Len: 0]
    Sequence number: 661963571
    [Next sequence number: 661963571]
    Acknowledgment number: 1770516295
    1010 .... = Header Length: 40 bytes (10)
    > Flags: 0x012 (SYN, ACK)
        Window size value: 14480
        [Calculated window size: 14480]
        Checksum: 0x6497 [unverified]
        [Checksum Status: Unverified]
        Urgent pointer: 0
    < Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), Window scale
        > TCP Option - Maximum segment size: 1300 bytes
        > TCP Option - SACK permitted
        > TCP Option - Timestamps: TSval 390233290, TSecr 981659424
        > TCP Option - No-Operation (NOP)
        > TCP Option - Window scale: 7 (multiply by 128)
    < [SEQ/ACK analysis]

```

نیاب ≈ مداخلا ڈفان مرح:

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Window size value
23...	0.002579	172.25.18.134	10.11.2.124	TCP	70	12854
23...	0.266847	172.25.18.134	10.11.2.124	TCP	70	12854
23...	0.268089	172.25.18.134	10.11.2.124	SSHv2	198	12854
23...	0.000076	172.25.18.134	10.11.2.124	SSHv2	118	12854
23...	0.000351	172.25.18.134	10.11.2.124	SSHv2	118	12854
23...	0.000092	172.25.18.134	10.11.2.124	TCP	70	12854
23...	0.000015	172.25.18.134	10.11.2.124	TCP	70	12854
23...	0.000091	172.25.18.134	10.11.2.124	TCP	70	12854

يلى ام يددرتلارىخأت تاجتنم ئغىص رفوت، مىقلا ھذە ئىل ادانتسا:

$$160000 * 8 / 0.3 = 43$$
 ئيرظنلارقىلار ئىصقىلار دىل ئىناثلار يىف تباجىم

(2) ويرانىسلار TCP لوكوتوربلىرى طبلىرلارقىلار 6. ئىل احلا:

عيطى ئاماحلا رادج رباع (ليزنت) فلم لقىن: ئىل كىشملا فصىو.

طباطخملار ئروصلار ھذە ضرعىت:



رثأتىملار قىفتىلار:

SRC IP: 192.168.2.220

DST IP: 192.168.1.220

لوكوتوربلىرى: FTP

رسالىلحت

كىچىم ئىل ئاقىتلارلا تايلىم ئەتكەن ئەتكەن ئەتكەن FTD LINA.

<#root>

firepower#

capture CAPI type raw-data buffer 33554432 interface INSIDE match tcp host 192.168.2.220 host 192.168.1.220

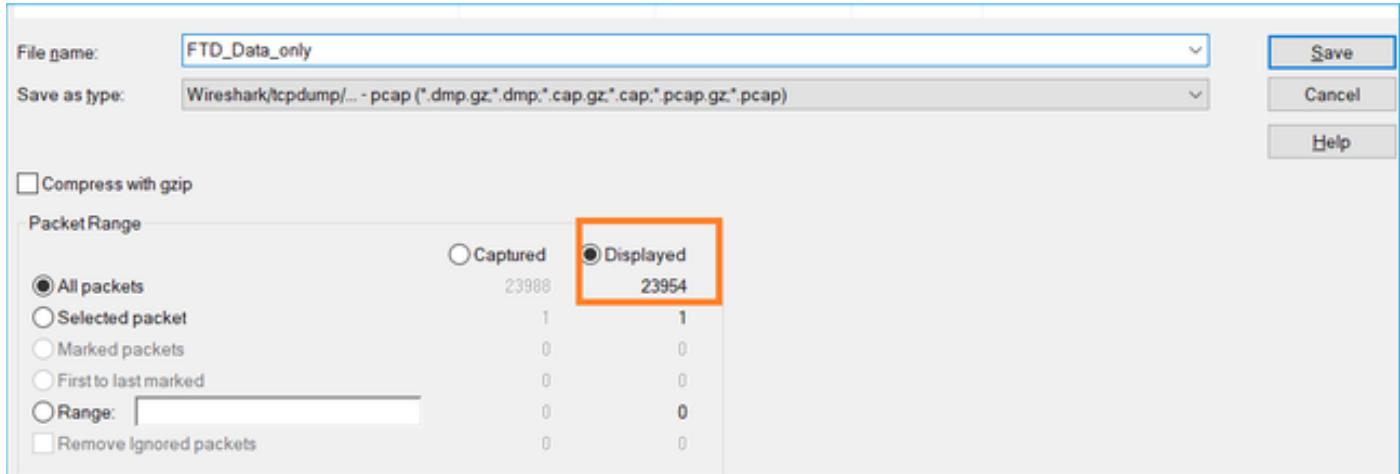
firepower#

cap CAPO type raw-data buffer 33554432 interface OUTSIDE match tcp host 192.168.2.220 host 192.168.1.220

FTD Inside (CAPI):

FTD Data (CAPO):

ةضورعمل ا ٽمزملا قاطن طقف ظفحا



اهب يصوصملات اءاعاج إلأ

ةلأسملالا هذه قاطن قييضت ةدایز وھ عرفلالا اذه يف ةدراولالا تاءاعاج إلأ نم ضرغلار.

ةمزملا نادقف عقوم ديدحت 1. ءاعاج إلأ.

قرف ةيجهنم مادختساو ةنم ازتم طاقتلا تايلىمع طاقتلا كيلع بجي ،هذه لثم تالاح يف نم و. ةمزملا نادقف يف ببسنت يتلا ةكبشلا (عطاوم) عطقم ديدحتل بلغتلار لاصتالا ئيسيلر تاهوي رانيس ةثالث كانه ةيامحلا رادج رظن ةهجو:

1. مسفن ةيامحلا رادج إلأ ةمزملا دقفعجري.

2. ئلإ مدخلالا نم هاجتا) ةيامحلا رادج زاهج إلإ تانايبلالا قفدت ةمزملا دقفع جتنىي (ليمعلالا).

3. (مدخلالا ئلإ ليمعلالا نم هاجتا) ةيامحلا رادج زاهج إلإ قفدت ةمزملا دقفع جتنىي.

ةيامح رادج ببسن نوكىي دقفع طبرلا نإ تنيع in order to: ةيامحلا رادج نع مجانلا ةمزملا نادقف نيتقيرط ةنراقمل ۋەرەپلەك قرط كانه . ضبق جرخملالا ئلإ طاقتلا لخدملا نراقى نأ جاخ كانه ۋەرەپلەك ماسقلالا اذه حضوي . نيتفلت خم:

ةمزملا نادقف ديدحتل نيتروص ةنراقم ءارجا

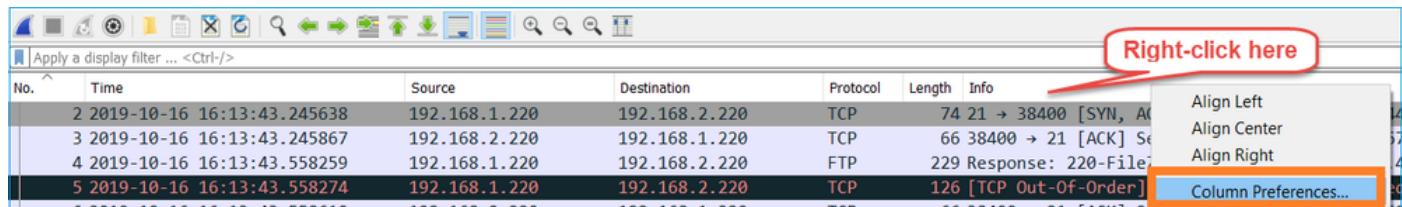
هنأ ينعي اذه . ينمزلالا راطإلا سفن نم مزملا ئىلع يوتحت 2 تاطقتلملا نأ نم دكأت . 1. ۋەوطخلا ددع كانه و. رخآلالا طاقتلالا دعب وأ لباق ھطاقتلا مت دحاو طاقتلا يف مزملا نوكىت الأ بجي ئاغلا اذه قيقتل قرطلا نم ليلق:

• ةمزملا ئىلولالا (ID) فىيعرت ميق نم ققحت .

• ئىلولالا ةمزملا عباتلا ميق نم ققحت .

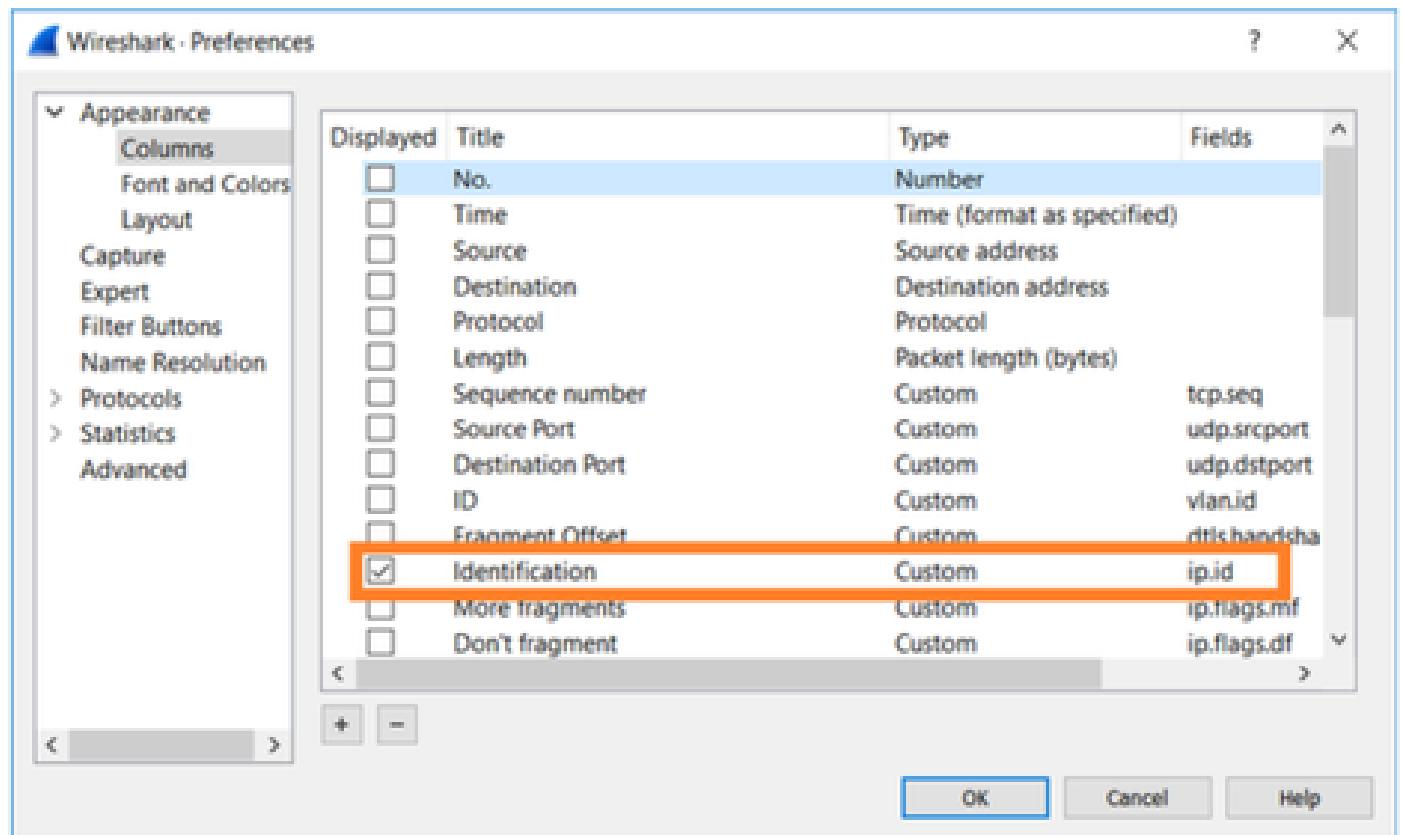
IP فرع ميق سفن اهل طاقتلا لك نم ئىلولالا مزملا نأ يرت نأ كنكمىي ، لاثملالا اذه يف

ة.روصلـا يـف حـضـوم وـه اـمـك طـاقـتـلـا لـيـدـعـتـبـ مـقـمـثـ IPـ فـيـرـعـتـ عـلـعـ ءـانـبـ.



A screenshot of the Wireshark interface showing a list of network packets. A context menu is open over the fifth packet, with a red box highlighting the "Align Right" option under the "Column Preferences..." section.

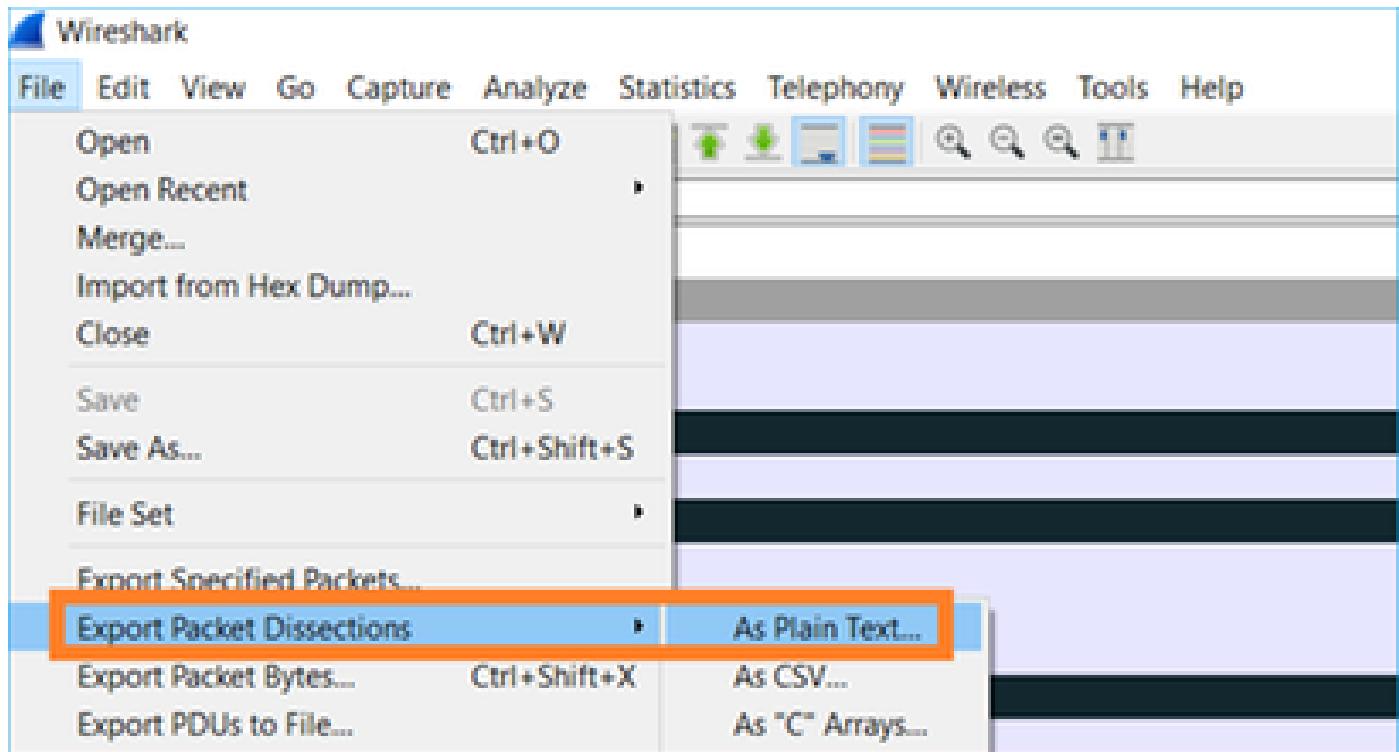
No.	Time	Source	Destination	Protocol	Length	Info	Align Left
2	2019-10-16 16:13:43.245638	192.168.1.220	192.168.2.220	TCP	74	21 → 38400 [SYN, ACK]	Align Center
3	2019-10-16 16:13:43.245867	192.168.2.220	192.168.1.220	TCP	66	38400 → 21 [ACK]	Align Right
4	2019-10-16 16:13:43.558259	192.168.1.220	192.168.2.220	FTP	229	Response: 220-File	
5	2019-10-16 16:13:43.558274	192.168.1.220	192.168.2.220	TCP	126	[TCP Out-Of-Order]	Column Preferences...



ةـجـيـتـنـلـا:

Identification
0x150e (5398)
0xfdb0 (64944)
0x1512 (5394)
0x1510 (5392)
0xfdb1 (64945)
0xfdb2 (64946)
0xfdb3 (64947)
0x1513 (5395)
0xfdb4 (64948)
0xfdb5 (64949)
0x1516 (5398)
0x1515 (5397)
0xfdb6 (64950)
0x1517 (5399)
0xfdb7 (64951)
0x1518 (5400)
0xfdb8 (64952)
0xfdb9 (64953)
0x151b (5403)
0x151a (5402)
0xfdः (64954)
0x151c (5404)
0xfdbb (64955)
0x151d (5405)
0x8a34 (2612)
0xfdbc (64956)
0x8a35 (2613)
0x151f (5407)
0x8a36 (2614)
▼ Frame 23988: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Oct 16, 2019 16:20:21.785130000 Central European Daylight Time

صـنـك > مـزـحـلـا تـامـيـسـقـت رـيـدـصـت < فـلـمـ) طـاقـتـلـالـا نـمـ صـنـ رـادـصـا عـاشـنـابـ مـقـ. 3. ـوـطـخـلـاـ ةـرـوـصـلـاـ يـفـ حـضـوـمـ وـهـ اـمـكـ،ـ...ـيـدـاعـ:



لـ**حـلـا مـيـقـ رـيـدـصـتـلـ ةـمـزـحـلـا لـيـصـافـتـو ةـدـمـعـأـلـا سـوـفـرـنـيـمـضـتـ تـارـايـخـ دـيـدـحـتـ عـاـغـلـابـ مـقـ**
ـةـرـوـصـلـا يـفـ حـضـوـمـ وـهـ اـمـكـ ،ـطـقـفـ ضـوـرـعـمـلـا:

	Captured	Displayed
All packets	16514	16514
Selected packet	1	1
Marked packets	0	0
First to last marked	0	0
Range: []	0	0
Remove Ignored packets	0	0

Packet Format

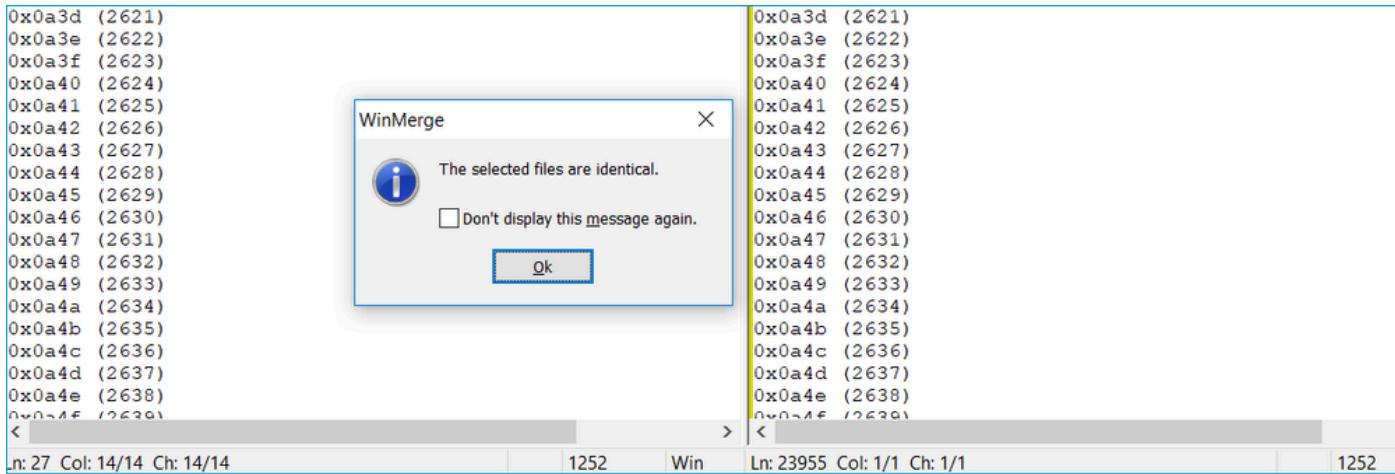
- Packet summary line
- Include column headings
- Packet details:
 - As displayed
- Packet Bytes
- Each packet on a new page

كـلـذـبـ مـاـيـقـلـلـ سـكـونـيـلـ زـرـفـ رـمـأـ مـادـخـتـسـ إـكـنـكـمـيـ .ـتـافـلـمـلـاـ يـفـ مـزـحـلـاـ زـرـفـ 4ـ ةـوـطـخـلـا:

```
<#root>
#
sort CAPI_IDS > file1.sorted
#
sort CAPO_IDS > file2.sorted
```

روـثـعـلـلـ لـمـأـ وـأـ (ـWـi~M~e~r~g~e~) صـوـصـنـ ةـنـرـاقـمـ ةـادـأـ مـدـخـتـسـأـ 5ـ ةـوـطـخـلـا

2. روصلانیب قورفلالىل



نأ تبثي اذه .نيقباتطتم FTP تانايip رورم ةكرحل CAPO و API طاقتلا نوكى، ئلاحلا هذه يف ئامحلا رادج ببس بنكى مل ۋەمىزچىلا نادقىف.

تانايibla قفت/قفت مۇز نادقىف ئىلۇ فرعىتلا.

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-16 16:13:44.169516	192.168.2.220	192.168.1.220	TCP	74	54494 → 2388 [SYN] Seq=2157030681 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3577288500 TSeср=4264384
2	2019-10-16 16:13:45.196050	192.168.2.220	192.168.1.220	TCP	74	[TCP Retransmission] 54494 → 2388 [SYN] Seq=2157030681 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3577291508
3	2019-10-16 16:13:47.177456	192.168.1.220	192.168.2.220	TCP	74	2388 + 54494 [SYN, ACK] Seq=2224316911 Ack=2157030682 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 TSval=3577291510
4	2019-10-16 16:13:47.178060	192.168.2.220	192.168.1.220	TCP	66	54494 → 2388 [ACK] Seq=2157030682 Ack=2224316912 Win=29312 Len=0 TSval=3577291508 TSeср=4264384
5	2019-10-16 16:13:47.179388	192.168.1.220	192.168.2.220	TCP	1314	2388 + 54494 [ACK] Seq=2224316912 Ack=2157030682 Win=66048 Len=1248 TSval=4264384 TSeср=3577291508
6	2019-10-16 16:13:47.180029	192.168.2.220	192.168.1.220	TCP	66	54494 → 2388 [ACK] Seq=2157030682 Ack=2224318160 Win=32128 Len=0 TSval=3577291510 TSeср=4264384
7	2019-10-16 16:13:47.180410	192.168.1.220	192.168.2.220	TCP	1314	[TCP Previous segment not captured] 2388 + 54494 [ACK] Seq=2224319408 Ack=2157030682 Win=66048 Len=1248 TSval=4264384 TSeср=3577291510
8	2019-10-16 16:13:47.180456	192.168.1.220	192.168.2.220	TCP	1314	2388 + 54494 [ACK] Seq=2224320656 Ack=2157030682 Win=66048 Len=1248 TSval=4264384 TSeср=3577291510
9	2019-10-16 16:13:47.180746	192.168.2.220	192.168.1.220	TCP	78	[TCP Window Update] 54494 → 2388 [ACK] Seq=2157030682 Ack=2224318160 Win=35072 Len=0 TSval=3577291510
10	2019-10-16 16:13:47.180822	192.168.2.220	192.168.1.220	TCP	78	[TCP Window Update] 54494 → 2388 [ACK] Seq=2157030682 Ack=2224318160 Win=37888 Len=0 TSval=3577291510
11	2019-10-16 16:13:47.489827	192.168.1.220	192.168.2.220	TCP	1314	[TCP Out-Of-Order] 2388 + 54494 [ACK] Seq=2224318160 Ack=2157030682 Win=66048 Len=1248 TSval=4264415
12	2019-10-16 16:13:47.490807	192.168.2.220	192.168.1.220	TCP	66	54494 → 2388 [ACK] Seq=2157030682 Ack=2224321984 Win=40832 Len=0 TSval=3577291820 TSeср=4264415
13	2019-10-16 16:13:47.490819	192.168.1.220	192.168.2.220	TCP	1314	2388 + 54494 [ACK] Seq=2224321904 Ack=2157030682 Win=66048 Len=1248 TSval=4264415 TSeср=3577291820
14	2019-10-16 16:13:47.490888	192.168.1.220	192.168.2.220	TCP	1314	[TCP Previous segment not captured] 2388 + 54494 [ACK] Seq=2224324400 Ack=2157030682 Win=66048 Len=1248 TSval=4264415 TSeср=3577291820
15	2019-10-16 16:13:47.490956	192.168.1.220	192.168.2.220	TCP	1314	2388 + 54494 [ACK] Seq=2224325648 Ack=2157030682 Win=66048 Len=1248 TSval=4264415 TSeср=3577291820
16	2019-10-16 16:14:47.491246	192.168.2.220	192.168.1.220	TCP	66	54494 → 2388 [ACK] Seq=2157030682 Ack=2224323150 Win=43776 Len=0 TSval=3577291821 TSeср=4264415

ةيسيئرلا طاقنلا:

نم اهلاسرا متي TCP syn ئەنإف ، صوصخلا ھوجو ئىلۇ. لاسرا ۋەمىزچىلا هذه. تىنأو طېرلا دىعىي لىمۇللا نأ امب. لەماخلا عضولالا يف FTP تانايibla مداخىللا ئىلە لىمۇللا. ئامحلا رادج ئىلە مداخىللا وحن تدقىف طېرلا (#1 طېر) يلىۋا syn لە تىيار عىتىسى.



دق ۋەمىزچىلا ئەنإف، مداخىللا ئىلە تلىصو دق SYN ئەنإف نوكىت نأ لامتحا كانه، ئاحلا هذه يف عوجرلا قىرط يف تدقىف:



طاقل اه ضرع متي مل قباسلا عطقملانأى لع Wireshark فرعتو مداخلا نم ڈمزح كانه 2. يف اهتيفور متي ملو لي معلا إلإ مداخلا نم ڈطقتملا ريغ ڈمزحلا لاسرا مت هنأ ارظن ايهامحلا رادجو مداخلا نيب تدقف دق ڈمزحلا نأ ينعي اذهف، ڈيامحلا رادج طاقتلا.



ڈيامحلا رادجو FTP مداخلا نيب مزح نادقف دوجو إلإ ريشي اذهو.

ڈيافاضا روص طاقتلا 2. عاجالا.

مي سقتل اه قيرط قي بطة لواح. ڈيافاضا طاقن دناع تاطقل عم ڈيافاضا تاطقل ذخاب مق مزحلا نادقف ببس ي يذلا لکاش ملل ريثملانم ديزملانم بلغتلار.

No.	Time	Source	Destination	Protocol	Length	Info
155	2019-10-16 16:13:51.749845	192.168.1.220	192.168.2.220	FTP-DA...	1314	FTP Data: 1248 bytes (PASV) (RETR file15mb)
156	2019-10-16 16:13:51.749860	192.168.1.220	192.168.2.220	FTP-DA...	1314	FTP Data: 1248 bytes (PASV) (RETR file15mb)
157	2019-10-16 16:13:51.749872	192.168.1.220	192.168.2.220	FTP-DA...	1314	FTP Data: 1248 bytes (PASV) (RETR file15mb)
158	2019-10-16 16:13:51.750722	192.168.2.220	192.168.1.220	TCP	66	54494 → 2388 [ACK] Seq=2157030682 Ack=2224385552 Win=180480 Len=0 TSv...
159	2019-10-16 16:13:51.750744	192.168.1.220	192.168.2.220	FTP-DA...	1314	FTP Data: 1248 bytes (PASV) (RETR file15mb)
160	2019-10-16 16:13:51.750768	192.168.2.220	192.168.1.220	TCP	66	54494 → 2388 [ACK] Seq=2157030682 Ack=2224386800 Win=183424 Len=0 TSv...
161	2019-10-16 16:13:51.750782	192.168.1.220	192.168.2.220	FTP-DA...	1314	FTP Data: 1248 bytes (PASV) (RETR file15mb)
162	2019-10-16 16:13:51.751001	192.168.2.220	192.168.1.220	TCP	7	[TCP Dup ACK 160#1] 54494 → 2388 [ACK] Seq=2157030682 Ack=2224386800
163	2019-10-16 16:13:51.751024	192.168.1.220	192.168.2.220	FTP-DA...	31	FTP Data: 1248 bytes (PASV) (RETR file15mb)
164	2019-10-16 16:13:51.751378	192.168.2.220	192.168.1.220	TCP	7	[TCP Dup ACK 160#2] 54494 → 2388 [ACK] Seq=2157030682 Ack=2224386800
165	2019-10-16 16:13:51.751402	192.168.1.220	192.168.2.220	FTP-DA...	1314	FTP Data: 1248 bytes (PASV) (RETR file15mb)
166	2019-10-16 16:13:51.751622	192.168.2.220	192.168.1.220	TCP	7	[TCP Dup ACK 160#3] 54494 → 2388 [ACK] Seq=2157030682 Ack=2224386800
167	2019-10-16 16:13:51.751648	192.168.1.220	192.168.2.220	FTP-DA...	31	[TCP Fast Retransmission] 54494 → 2388 [ACK] Seq=2157030682 Ack=2224386800

Frame 167: 1314 bytes on wire (10512 bits), 1314 bytes captured (10512 bits) on interface 0
> Ethernet II, Src: VMware_30:b2:78 (00:0c:29:30:b2:78), Dst: Cisco_9d:89:9b (50:3d:e5:9d:89:9b)
> Internet Protocol Version 4, Src: 192.168.1.220, Dst: 192.168.2.220
> Transmission Control Protocol, Src Port: 2388, Dst Port: 2388, Seq: 2224386800, Ack: 2157030682, Len: 1248
FTP Data (1248 bytes data)
[Setup frame: 33]
[Setup method: PASV]
[Command: RETR file15mb]
[Command frame: 40]
[Current working directory: /]
Line-based text data (1 lines)

ڈيسيرلا طاقنلا:

- اذا. دراول ا TCP لسلست ماقرأ (ةللاحلا هذه يف FTP ليمع) لبقوتس ملا عبtti. عاشناب موقعت اهناف، عقوتم لسلست مقرري طخت مت اهدقف مت دق ڈمزح نأ تفشتكا لالاثم اده يف. هي طخت مت عقوتم لسلست مقرب ACK ڈمزح لاسرالا (DUP ACK) لوكوتوربل عيرسلا لاسرالا ڈاعي ليعشتب.
- لاسرالا (DUP ACK) لوكوتوربل عيرسلا لاسرالا ڈاعي ليعشتب.

ررکم يقلى دعوب ئيناث 20 لالخ ACK).

ةرركملاتابجولاهينعتيذلا ام

- نم هنأ ىلإ ئيلعف لاسرا ئداعا تايىلمع دجوت ال نكلو ةرركملاتا ACK عاونأ ضعب ريشت ماظنلا جراخ لصت مزح كانه نأ حجرألا.
- ام ردق دوجو ىلإ ئيلعفلاتاسرا ئداعا تايىلمع اهيلت يتلا ةرركملاتا ACK لئاسر ريشت مزحلا نادقف نم.

لقدنلا مزحل ئيامحلا رادج ئجلام تقو باسح 3. ئارج إلإ.

نيتفلتخم نيتھج اویلع طاقتلالا سفن قېبىطت:

```
<#root>
```

```
firepower#
```

```
capture CAPI buffer 33554432 interface INSIDE match tcp host 192.168.2.220 host 192.168.1.220
```

```
firepower#
```

```
capture CAPI interface OUTSIDE
```

طبرجرمم لباقيم لخدمنىب تقولا قرف نم ققحت طاقتلالا ريدصت

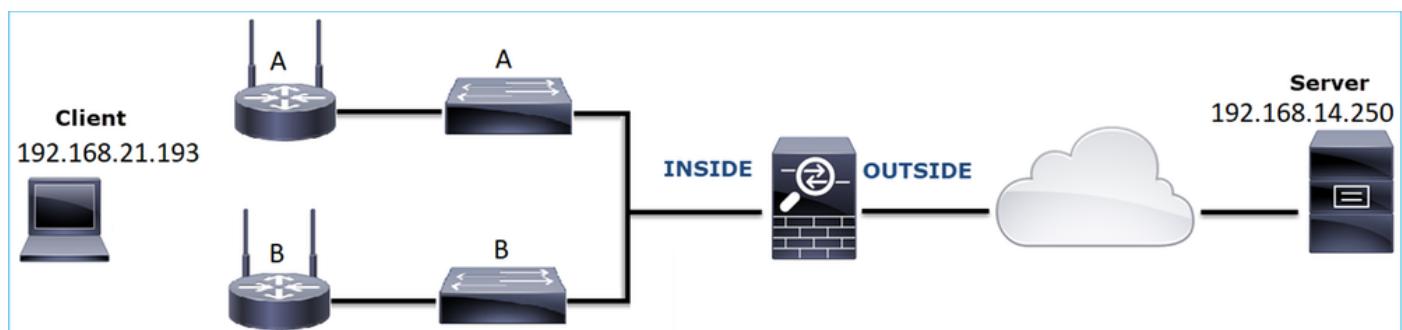
(ةمزحلاتا فلت) TCP لاصتا ئلكشم 7. ئلاحلا

ةلكلشىمىلا فصو:

نافلتخم ناهويرانيس كانه و (192.168.14.250 - HTTP) يكلىساللا لمىمعلا لواحي (192.168.21.193) ئەجومداخب لاصتا (192.168.21.193) ئەجومداخب لاصتا (192.168.21.193) ئەجومداخب لاصتا (192.168.21.193) ئەجومداخب لاصتا (192.168.21.193)

- لاصتا لمىعى ال ذىدىن 'A' (AP) لوصولا ئەطقىنب لمىمعلا لصتى امدىن.
- لاصتا لمىعى ذىدىن 'B' (AP) لوصولا ئەطقىنب لمىمعلا لصتى امدىن.

ططخملاتا ئروصلاتا هذه ضرعات:



رثأتملأا قفتلأا:

SRC IP: 192.168.21.193

DST IP: 192.168.14.250

لوكوتورب TCP 80

رسأليلحـت

كـرحمـىـلـعـ طـاقـتـلـالـاـ نـيـكـمـتـ FTD LINA:

<#root>

firepower#

```
capture CAPI int INSIDE match ip host 192.168.21.193 host 192.168.14.250
```

firepower#

```
capture CAPO int OUTSIDE match ip host 192.168.21.193 host 192.168.14.250
```

يـفـيـظـوـلـاـ وـيـرـانـيـسـلـاـ -ـ طـاقـتـلـاـ:

ادـيجـ فـورـعـمـ وـيـرـانـيـسـ نـمـ تـاطـقـلـىـلـعـ لـوـصـحـلـاـ اـمـئـادـ اـدـجـ دـيـفـمـلـاـ نـمـ ،ـسـاسـأـ طـخـكـ.

نـجـاـوـ طـاقـتـلـاـ ةـرـوـصـلـاـ هـذـهـ رـهـظـتـ

No.	Time	Source	Destination	Protocol	Length	Info
1	2013-08-08 17:03:25.554582	192.168.21.193	192.168.14.250	TCP	66	1055 → 80 [SYN] Seq=1341231 Win=65535 Len=0 MSS=1460 SACK_PERM=1
2	2013-08-08 17:03:25.555238	192.168.14.250	192.168.21.193	TCP	66	80 → 1055 [SYN, ACK] Seq=1015787006 Ack=1341232 Win=0 MSS=1380 SACK_PERM=1
3	2013-08-08 17:03:25.579910	192.168.21.193	192.168.14.250	TCP	58	1055 → 80 [ACK] Seq=1341232 Ack=1015787007 Win=65535 Len=0
4	2013-08-08 17:03:25.841081	192.168.21.193	192.168.14.250	HTTP	370	GET /ttest.html HTTP/1.1
5	2013-08-08 17:03:25.848466	192.168.14.250	192.168.21.193	TCP	1438	80 → 1055 [ACK] Seq=1015787007 Ack=1341544 Win=63928 Len=1380 [TCP segment of a reassembled PDU]
6	2013-08-08 17:03:25.848527	192.168.14.250	192.168.21.193	HTTP	698	HTTP/1.1 404 Not Found (text/html)
7	2013-08-08 17:03:25.858445	192.168.21.193	192.168.14.250	TCP	58	1055 → 80 [ACK] Seq=1341544 Ack=1015789027 Win=65535 Len=0
8	2013-08-08 17:03:34.391749	192.168.21.193	192.168.14.250	HTTP	369	GET /test.html HTTP/1.1
9	2013-08-08 17:03:34.395487	192.168.14.250	192.168.21.193	HTTP	586	HTTP/1.1 200 OK (text/html)
10	2013-08-08 17:03:34.606352	192.168.21.193	192.168.14.250	TCP	58	1055 → 80 [ACK] Seq=1341855 Ack=1015789555 Win=65007 Len=0
11	2013-08-08 17:03:40.739601	192.168.21.193	192.168.14.250	HTTP	483	GET /test.html HTTP/1.1
12	2013-08-08 17:03:40.741538	192.168.14.250	192.168.21.193	HTTP	271	HTTP/1.1 304 Not Modified

نـجـاـوـ طـاقـتـلـاـ ةـرـوـصـلـاـ هـذـهـ ضـرـعـتـ

No.	Time	Source	Destination	Protocol	Length	Info
1	2013-08-08 17:03:25.554872	192.168.21.193	192.168.14.250	TCP	66	1055 → 80 [SYN] Seq=1839800324 Win=65535 Len=0 MSS=1380 SACK_PERM=1
2	2013-08-08 17:03:25.555177	192.168.14.250	192.168.21.193	TCP	66	80 → 1055 [SYN, ACK] Seq=521188628 Ack=1839800325 Win=64240 Len=0 MSS=1460 SACK_PERM=1
3	2013-08-08 17:03:25.579926	192.168.21.193	192.168.14.250	TCP	58	1055 → 80 [ACK] Seq=1839800325 Ack=521188629 Win=65535 Len=0
4	2013-08-08 17:03:25.841112	192.168.21.193	192.168.14.250	HTTP	370	GET /ttest.html HTTP/1.1
5	2013-08-08 17:03:25.848451	192.168.14.250	192.168.21.193	TCP	1438	80 → 1055 [ACK] Seq=521188629 Ack=1839800637 Win=63928 Len=1380 [TCP segment of a reassembled PDU]
6	2013-08-08 17:03:25.848512	192.168.14.250	192.168.21.193	HTTP	698	HTTP/1.1 404 Not Found (text/html)
7	2013-08-08 17:03:25.858476	192.168.21.193	192.168.14.250	TCP	58	1055 → 80 [ACK] Seq=1839800637 Ack=521190649 Win=65535 Len=0
8	2013-08-08 17:03:34.391779	192.168.21.193	192.168.14.250	HTTP	369	GET /test.html HTTP/1.1
9	2013-08-08 17:03:34.395456	192.168.14.250	192.168.21.193	HTTP	586	HTTP/1.1 200 OK (text/html)
10	2013-08-08 17:03:34.606368	192.168.21.193	192.168.14.250	TCP	58	1055 → 80 [ACK] Seq=1839800948 Ack=521191177 Win=65007 Len=0
11	2013-08-08 17:03:40.739646	192.168.21.193	192.168.14.250	HTTP	483	GET /test.html HTTP/1.1
12	2013-08-08 17:03:40.741523	192.168.14.250	192.168.21.193	HTTP	271	HTTP/1.1 304 Not Modified

نـجـاـوـ طـاقـنـلـاـ:

1. (ةـيـاوـشـعـلـاـ ISـ ةـيـلـمـعـ يـفـ اـولـمـأـتـ) اـبـيـرـقـتـ نـاتـقـبـاطـتـمـ نـاتـطـقـتـلـاـ.
2. ـةـمـزـحـلـاـ نـادـقـفـىـلـعـ تـارـشـفـمـ دـجـوـتـ الـ.
3. (OOO) بـيـتـرـتـلـاـ جـراـخـ مـزـحـ دـجـوـتـ الـ.

No.	Time	Source	Destination	Protocol	Length	Info
1	2013-08-08 15:33:31.9099193	192.168.21.193	192.168.14.250	TCP	66	3072 → 80 [SYN] Seq=4231766828 Win=65535 Len=0 MSS=1460 SACK_PERM=1
2	2013-08-08 15:33:31.9099849	192.168.14.250	192.168.21.193	TCP	66	80 → 3072 [SYN, ACK] Seq=867575959 Ack=4231766829 Win=64240 Len=0 MSS=1380 SACK_PERM=1
3	2013-08-08 15:33:31.913267	192.168.21.193	192.168.14.250	TCP	60	3072 → 80 [ACK] Seq=4231766829 Ack=867575960 Win=65535 Len=2 [Malformed Packet]
> Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)						
> Ethernet II, Src: BelkinIn_63:90:f3 (ec:1a:59:63:90:f3), Dst: Cisco_61:cc:9b (58:8d:09:61:cc:9b)						
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 20						
> Internet Protocol Version 4, Src: 192.168.21.193, Dst: 192.168.14.250						
▼ Transmission Control Protocol, Src Port: 3072, Dst Port: 80, Seq: 4231766829, Ack: 867575960, Len: 2						
Source Port: 3072						
Destination Port: 80						
[Stream index: 0]						
[TCP Segment Len: 2]						
Sequence number: 4231766829						
[Next sequence number: 4231766831]						
Acknowledgment number: 867575960						
0101 = Header Length: 20 bytes (5)						
> Flags: 0x010 (ACK)						
Window size value: 65535						
[Calculated window size: 65535]						
[Window size scaling factor: -2 (no window scaling used)]						
Checksum: 0x01bf [unverified]						
[Checksum Status: Unverified]						
Urgent pointer: 0						
> [SEQ/ACK analysis]						
> [Timestamps]						
TCP payload (2 bytes)						
▼ Malformed Packet: Tunnel Socket						
1 [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]						
[Malformed Packet (Exception occurred)]						
[Severity level: Error]						
[Group: Malformed]						
0000	58 8d 09 61 cc 9b ec 1a	59 63 90 f3 81 00 00 14	X- a.... Yc.....			
0010	08 00 45 00 00 2a 7f 1d	40 00 80 06 d5 a4 c0 a8	..E...@.....			
0020	15 c1 c0 a8 0e fa 0c 00	00 50 fc 3b a7 3d 33 b6P;..-3.			
0030	28 98 50 10 ff ff 01 bf	00 00 00 00 00	(.-P.....)			

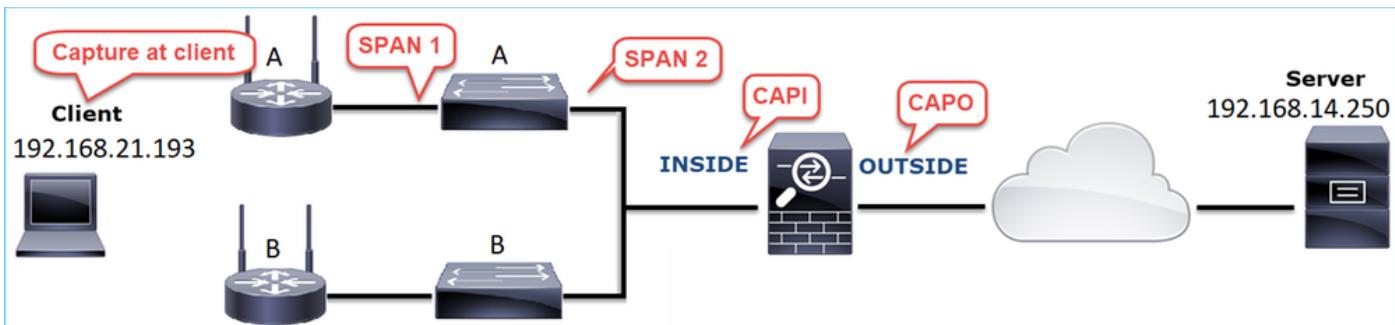
ةيسيئرلا طاقنل:

1. لبق نم حيحص ريع لكشب ۆلکشم اهنأىل عۆمزحلاب فەيەت مەتي.
2. تىياب 2 ھلوط.
3. تىياب 2 رادقمب TCP ۆلۈمۈم كانە.
4. ئەيپاپسا رافصا 4 يە ۆلۈمۈملا (00 00).

اهب ئىصوملا تاءارجىلا

ۆلأسملەملا هذه قاطن قىيىضت ئەدایز وە عرفلىا اذه يە ۆدراولى تاءارجىلا نم ضرغىلە.

نأ تلواح، نكمأ ناوا ئىاهنلە طاقن يە ضبىقىلىع تەنمپىت. ئەيپاپسا روش طاقنلە. 1. ئارجىلا: ئالىم، داسف طېرىلى نم رەصمەلە لىزىي نأ ۆق طقىرطۇ تاماسقنىلا قېبەتى:

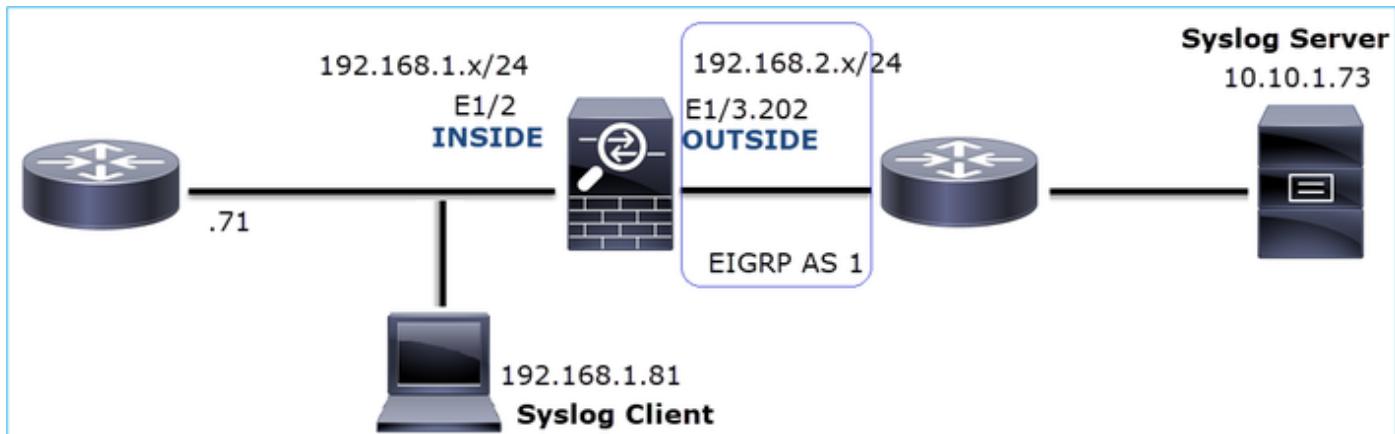


نأ ناك لەلەلەلىغىشت جەمانرب نرافق 'A' حاتفەملاب تەفصىن ناك يە ۆدراولىا تەلەبەتسا.

ۆدوقفەملە UDP لاصتا ۆلکشم 8. ۆلەحلا

لدان ۆياغلا ىلع ۆلاسر syslog (UDP 514) ىري ال: لەكشملا فصو.

طاطخملار ۆروصلانىدا هذه ضرعت:



رئاتملا قىفتلىا:

SRC IP: 192.168.1.81

DST IP: 10.10.1.73

Protocol: UDP 514

رسالىلەت

كىچم ىلع طاقتلالا نىكىمت FTD LINA:

```
<#root>
firepower#
capture CAPI int INSIDE trace match udp host 192.168.1.81 host 10.10.1.73 eq 514
firepower#
capture CAPO int OUTSIDE match udp host 192.168.1.81 host 10.10.1.73 eq 514
```

منج ياروشى رهظت ال:

```
<#root>
firepower#
show capture
capture CAPI type raw-data trace interface INSIDE [Capturing - 0 bytes]
  match udp host 192.168.1.81 host 10.10.1.73 eq syslog
capture CAPO type raw-data interface OUTSIDE [Capturing - 0 bytes]
  match udp host 192.168.1.81 host 10.10.1.73 eq syslog
```

اهب ىصوملات اءارج إلأ

ةلأسملاتا هذه قاطن قييضرت ةدایز وھ عرفلاتا اذه يف ةدراولاتا اءارج إلأ نم ضرغل او.

لاصتا لودج نم ققحت .1. ءارج إلأ FTD.

ةغايصلاتا هذه مادختسإ كنكمي ،ددجم لاصتا نم ققحتلل:

```
<#root>
firepower#
show conn address 192.168.1.81 port 514
10 in use, 3627189 most used
Inspect Snort:
    preserve-connection: 6 enabled, 0 in effect, 74 most enabled, 0 most in effect
UDP
INSIDE
10.10.1.73:514
INSIDE
192.168.1.81:514, idle 0:00:00, bytes
480379697
, flags -
o
N1
```

ةيسئرلا طاقنلا:

1. (u) نارود) اھسفن يھ جورخل او لوخدلاتا هج او.

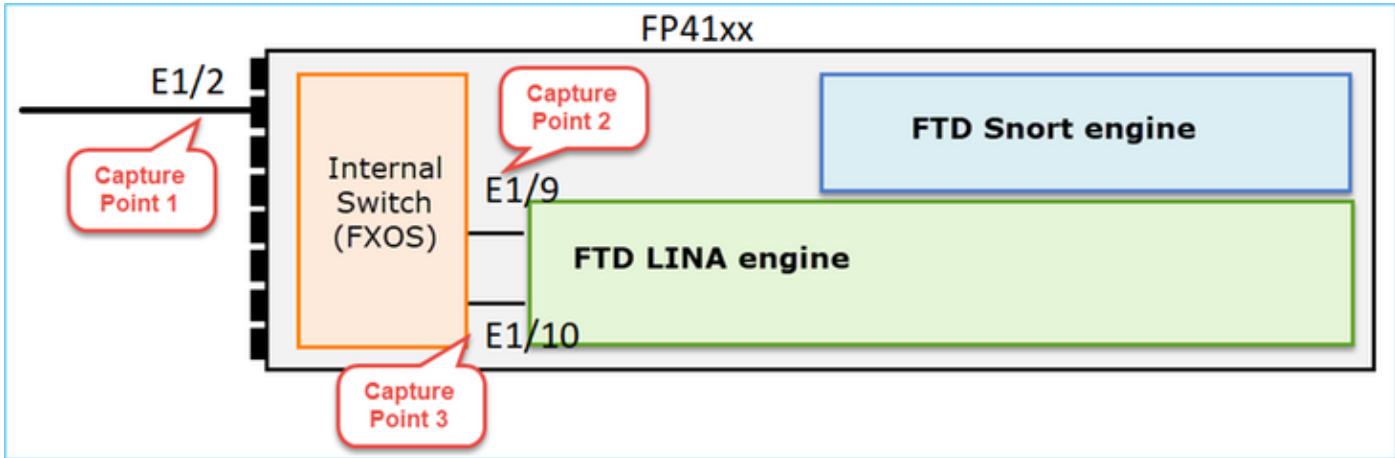
2. (تیاب تیاباغیغ ~5 ئیاغل ئریبک ئمیق ىلع تیابلا تادحو ددع یوتحي).

عارو ببسلا وھ اذه (عیرسلا HW قفتل) قفتل لیمحت ئاغلإ ىلإ "0" ئممالعلا ریشت.

3. ئمظنلأا ىلع طقف موعدم قفتل لیمحت ئاغلإ .مزح يأ FTD طاقتلار ضرع مدع
وھ زاھجلا، ئالاحللا هذھ يف 41xx و 93xx ئاسنلأا 41xx.

لکيھلا یوتسمل ىلع روصلا طاقتلار 2. ءارج إلأ.

هذھ يف (E1/2) لوخدلار ھج او ىلع طاقتلارا نيكمت و FirePOWER لکيھ ريدمب لاصتالاب مق
ةروصلار يف حضوم وھ امك، (E1/10) و (E1/9) ئيفلخلار ھجوللارا (ئالاحلار).



Overview Interfaces Logical Devices Security Engine Platform Settings System Tools Help admin

Select an instance: mzafeiro_FTD

mzafeiro_FTD

Ethernet1/2

Ethernet1/3

Ethernet1/1

FTD
Ethernet1/9, Ethernet1/10

Session Name*: CAPI

Selected Interfaces: Ethernet1/2

Buffer Size: 256 MB

Snap length: 1518 Bytes

Store Packets: Overwrite Append

Capture On: All Backplane Ports

Capture Filter: Apply Filter Capture All
Apply Another Filter Create Filter

ن اوٹ عضب دعب:

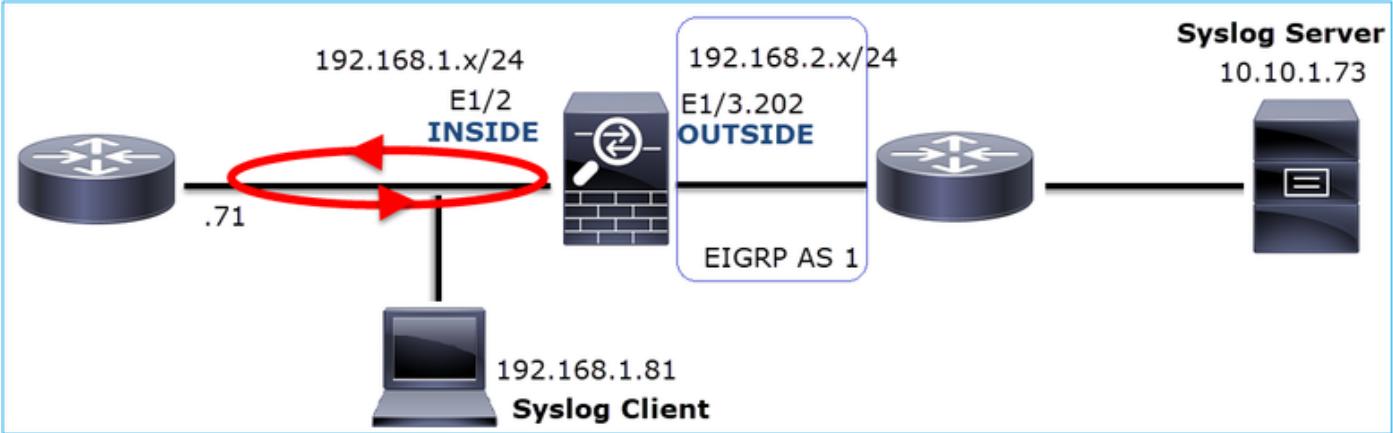
Capture Session Filter List

Drop Count: 40103750 Operational State: DOWN - Memory_Overshoot

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/10	None	276	CAPI-ethernet-1-10-0.pcap	mzafeiro_FTD
Ethernet1/9	None	132276060	CAPI-ethernet-1-9-0.pcap	mzafeiro_FTD
Ethernet1/2	None	136234072	CAPI-ethernet-1-2-0.pcap	mzafeiro_FTD

نراقلا ىلע جودزم طبرلا يغلی نأ طبر VN-tagged Wireshark ا تيـنـثـتـسـا يـفـ حـيـمـلـتـ يـعـيـبـطـ

لـبـقـ



مزحلا عبـت ةادأ مـدخـسـا 3ـ عـاجـإـلـا.

ضـبـقـ لـعـلـ (طـشـنـ عـبـتـتـ مـتـيـ الـعـيـطـتـسـيـ تـنـأـ كـرـحـمـ LINAـ ةـيـامـحـلـاـ رـاـدـجـ زـاتـجـتـ الـمـزـحـلـاـ نـأـ اـمـبـ w~traceـ)، طـبـرـعـمـ يـكـاحـمـ طـبـرـعـتـعـبـتـتـعـيـطـتـسـيـ تـنـأـ رـيـغـ tracerـ:

```
<#root>
firepower#
packet-tracer input INSIDE udp 10.10.1.73 514 192.168.1.81 514

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 25350892, using existing flow

Phase: 4
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (fast-forward) fast forward this flow

Phase: 5
```

```

Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.1.81 using egress ifc  INSIDE

Phase: 6
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address a023.9f92.2a4d hits 1 reference 1

Phase: 7
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: INSIDE

input-status: up
input-line-status: up

output-interface: INSIDE

output-status: up
output-line-status: up
Action: allow

```

هیجوت دیکأت 4. ئارجيلا FTD.

هیجوتلا يف لكاشم يأ كانه تناناڭ اذىام ئەفرۇملىيامحلا رادج ھيچوت لودج نم ققحت:

```

<#root>

firepower#
show route 10.10.1.73

Routing entry for 10.10.1.0 255.255.255.0
Known via "eigrp 1", distance 90, metric 3072, type internal
Redistributing via eigrp 1
Last update from 192.168.2.72 on

OUTSIDE, 0:03:37 ago

  Routing Descriptor Blocks:
    * 192.168.2.72, from 192.168.2.72,

0:02:37 ago, via OUTSIDE

    Route metric is 3072, traffic share count is 1

```

Total delay is 20 microseconds, minimum bandwidth is 1000000 Kbit
Reliability 255/255, minimum MTU 1500 bytes
Loading 29/255, Hops 1

ةيسيئرلا طاقنل:

1. حيچصل جورخلا ڦهنج او لى راسمل ريشي.
2. ڦليلىق ڦئاقد لباق قيرطلا ملعت مت (0:02:37).

لاصتالا ليغشت تقو ديكأت 5. ئارج إلأ.

لاصتالا اذه سيسأت تقو ڦفرعمل لاصتالا ليغشت تقو نم ققحت:

```
<#root>
```

```
firepower#
```

```
show conn address 192.168.1.81 port 514 detail
```

21 in use, 3627189 most used

Inspect Snort:

preserve-connection: 19 enabled, 0 in effect, 74 most enabled, 0 most in effect
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,
b - TCP state-bypass or nailed,
C - CTIQBE media, c - cluster centralized,
D - DNS, d - dump, E - outside back connection, e - semi-distributed,
F - initiator FIN, f - responder FIN,
G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
k - Skinny media, L - decap tunnel, M - SMTP data, m - SIP media
N - inspected by Snort (1 - preserve-connection enabled, 2 - preserve-connection in effect)
n - GUP, O - responder data, o - offloaded,
P - inside back connection, p - passenger flow
q - SQL*Net data, R - initiator acknowledged FIN,
R - UDP SUNRPC, r - responder acknowledged FIN,
T - SIP, t - SIP transient, U - up,
V - VPN orphan, v - M3UA W - WAAS,
w - secondary domain backup,
X - inspected by service module,
x - per session, Y - director stub flow, y - backup stub flow,
Z - Scansafe redirection, z - forwarding stub flow

```
UDP INSIDE: 10.10.1.73/514 INSIDE: 192.168.1.81/514,  
flags -oN1, idle 0s,
```

```
uptime 3m49s
```

```
, timeout 2m0s, bytes 4801148711
```

ةيسيئرلا ڦطقنل:

1. لوچ يف EIGRP راسم تيپٿت لباق اذه) ڦئاقد 4 يل اوچ ذنم لاصتالا ئاشن مت (يچو تل)

ةمئاقلـا ئلـاصـلا حـسـم - 6 ئـارـجـإـلـا.

اـذـهـ ئـطـاخـ جـرـخـ مـهـجـاـوـلـاـ اـهـيـجـوـتـ مـتـيـ وـسـسـفـمـ لـاصـتـاـعـ مـزـحـلـاـ قـبـاطـتـتـ ،ـلـاحـلـاـ هـذـهـ يـفـ ئـيـامـحـلـاـ رـادـجـ تـايـلـمـعـ بـيـتـرـتـ ئـلـاـ كـلـذـيـ فـ بـبـسـلـاـ عـجـرـيـ .ـقـلـحـ بـبـسـيـ

1. (مـاعـلـاـ هـيـجـوـتـلـاـ لـوـدـجـ نـعـ ثـحـبـلـاـ ئـلـعـ ئـيـولـوـأـلـاـ اـذـهـ ذـخـأـيـ)ـ هـؤـاشـنـاـ مـتـ يـذـلـاـ لـاصـتـالـاـ ثـحـبـ.
2. ئـلـعـ ئـيـولـوـأـلـاـ (NATـ ئـيـاغـ)ـ UN-NATـ ئـلـحـرـمـ ذـخـأـتـ -ـ (NATـ ئـكـبـشـلـاـ نـاـونـعـ ئـمـجـرـتـ نـعـ ثـحـبـلـاـ رـاسـمـلـاـ ثـحـبـ وـPBRـ).
3. ئـلـعـ ئـسـاـيـسـلـاـ ئـلـعـ مـئـاـقـلـاـ هـيـجـوـتـلـاـ (PBRـ).
4. ئـمـومـعـلـاـ هـيـجـوـتـلـاـ لـوـدـجـ ثـحـبـ.

لـوـمـخـ ئـلـهـمـ نـوـكـتـ اـمـنـيـبـ رـاـرـمـتـسـابـ مـزـحـلـاـ لـيـمـعـ لـسـرـيـ)ـ اـدـبـأـيـهـتـنـيـ الـلـاصـتـالـاـ نـأـمـبـ اـيـوـدـيـ لـاصـتـالـاـ حـسـمـ ئـلـاـ ئـجـاحـ كـانـهـ (ـقـقـيـقـدـ 2ـ يـهـ UDPـ)

```
<#root>
```

```
firepower#  
  
clear conn address 10.10.1.73 address 192.168.1.81 protocol udp port 514  
1 connection(s) deleted.
```

ديـدـجـ لـاصـتـاـعـشـنـاـ نـمـ قـقـحـتـ:

```
<#root>
```

```
firepower#  
  
show conn address 192.168.1.81 port 514 detail | b 10.10.1.73.*192.168.1.81  
UDP  
  
OUTSIDE  
:  
: 10.10.1.73/514  
  
INSIDE  
:  
: 192.168.1.81/514,  
flags -oN1, idle 1m15s, uptime 1m15s, timeout 2m0s, bytes 408
```

مـئـاـعـلـاـ لـخـادـتـلـاـ ئـلـهـمـ نـيـوـكـتـ.ـ 7ـ ئـارـجـإـلـاـ.

UDPـ تـاقـفـدـتـلـ ئـصـاخـوـ ،ـلـثـمـأـلـاـ نـوـدـ هـيـجـوـتـلـاـ بـنـجـتـوـ ئـلـكـشـمـلـاـ ئـجـلـاعـمـلـ بـسـاـنـمـلـاـ لـحـلـاـ وـهـ اـذـهـ ئـمـيـقـلـاـ طـبـضـوـتـالـمـ >ـ يـسـاـسـأـلـاـ مـاـظـنـلـاـ تـادـدـعـاـ >ـ ئـزـهـجـأـلـاـ ئـلـاـ لـقـتـنـاـ

SMTP Server	H.323	Default	0:05:00	(0:0:0 or 0:0:0 – 1193:0:0)
SNMP	SIP	Default	0:30:00	(0:0:0 or 0:5:0 – 1193:0:0)
SSL	SIP Media	Default	0:02:00	(0:0:0 or 0:1:0 – 1193:0:0)
Syslog	SIP Disconnect:	Default	0:02:00	(0:02:0 or 0:0:1 – 0:10:0)
Timeouts	SIP Invite	Default	0:03:00	(0:1:0 or 0:1:0 – 0:30:0)
Time Synchronization	SIP Provisional Media	Default	0:02:00	(0:2:0 or 0:1:0 – 0:30:0)
UCAPL/CC Compliance	Floating Connection	Custom	0:00:30	(0:0:0 or 0:0:30 – 1193:0:0)
	Xlate-PAT	Default	0:00:30	(0:0:30 or 0:0:30 – 0:5:0)

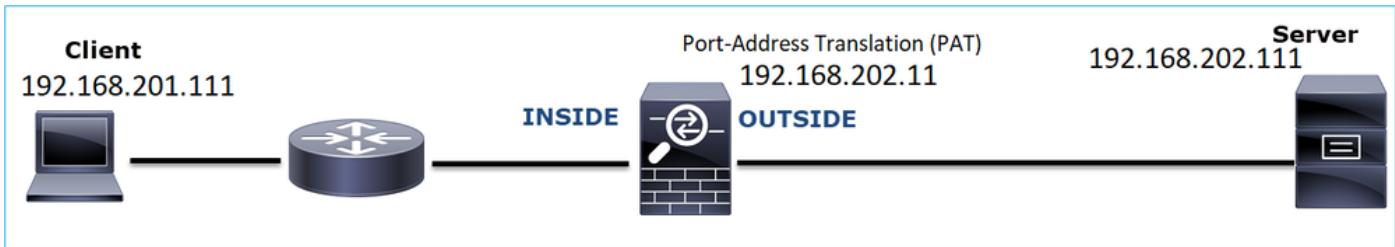
عجرم رمألا يف ۋلەم conn ميوقىتلا لوح ليصافتىلا نم دىزمىلا تدجوع يىطتسىي تنان:

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/T-Z/asa-command-ref-T-Z.html#pgfid-1649892>

ويرانىسىلىا HTTPS لاصتا ۋلەكشم 9. ۋلەحلا

مداخل او 192.168.201.105 لىمۇلا نىب HTTPS لاصتا ئاشنىڭ كىمىي ال: ۋلەكشم لافصىو 192.168.202.101

ططاخملار ۋىزىتەر لە ئەنۋەر:



رثأتىملا قىفتىلا:

SRC IP: 192.168.201.111

DST IP: 192.168.202.111

لوكوتورب TCP 443 (HTTPS)

رسألىلحىت

كىچىم ئىلەن طاقىتلالا FTD LINA:

لېكشت ئەم جىرت ناونۇغا ئىلا بىجا فەلتەخم يىجراخىلا طاقىتلالا يف لەمعتسىي ip لى.

<#root>

firepower#

```
capture CAPI int INSIDE match ip host 192.168.201.111 host 192.168.202.111
firepower#
capture CAPO int OUTSIDE match ip host 192.168.202.11 host 192.168.202.111
```

نەتەنەن ئەم مەت ئىلۇم ئەلا ئەقەل ئەلا ئەرۇصىلا ھەذە رەھەت:

No.	Time	Source	Destination	Protocol	Length	Identification	Info
38	2018-02-01 10:39:35.187887	192.168.201.111	192.168.202.111	TCP	78	0x2f31 (12081)	1 6666 → 443 [SYN] Seq=2034865631 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSeqr=0 WS=128
39	2018-02-01 10:39:35.188909	192.168.202.111	192.168.201.111	TCP	78	0x0000 (0)	443 → 6666 [SYN, ACK] Seq=4086514531 Ack=2034865632 Win=28960 Len=0 MSS=1388 SACK_PERM=1 TSeqr=3119
40	2018-02-01 10:39:35.188946	192.168.201.111	192.168.202.111	TCP	70	0x2f32 (12082)	2 6666 → 443 [ACK] Seq=2034865632 Ack=4086514532 Win=29312 Len=0 TSeqr=3119615816
41	2018-02-01 10:39:35.251695	192.168.201.111	192.168.202.111	TLSv1	326	0x2f33 (12083)	3 Client Hello
42	2018-02-01 10:39:35.252352	192.168.202.111	192.168.201.111	TCP	70	0xerfb4 (61364)	443 → 6666 [ACK] Seq=4086514532 Ack=2034865888 Win=8192 Len=0 TSeqr=3119615816 TSeqr=31196158174
43	2018-02-01 10:40:05.317320	192.168.202.111	192.168.201.111	TCP	70	0xd8c3 (55491)	4 443 → 6666 [RST] Seq=4086514532 Win=8192 Len=0 TSeqr=3119645988 TSeqr=0

ئەس يىرىلا ئەقەل:

1. اجتىلا ئەيىتالىت TCP ۋە حفاصىم كان ھ.
2. ئەلا ئەسلىمىغا لىسىرى. SSL ضوافت عىدب.
3. ئەلا ئەسرا مەت TCP ACK كان ھ.
4. ئەلا ئەسرا مەت TCP RST كان ھ.

نەتەنەن ئەم مەت ئىلۇم ئەلا ئەقەل ئەلا ئەرۇصىلا ھەذە ضرعىت ل ئەچىرخلا ئەجداولا ئەلەن ئەلا ئەقەل ئەلا ئەرۇصىلا ھەذە ضرعىت.

No.	Time	Source	Destination	Protocol	Length	Identification	Info
33	2018-02-01 10:39:35.188192	192.168.202.11	192.168.202.111	TCP	78	0x2f31 (12081)	1 15880 → 443 [SYN] Seq=2486930707 Win=29200 Len=0 MSS=1388 SACK_PERM=1 TSeqr=0 WS=128
34	2018-02-01 10:39:35.188527	192.168.202.111	192.168.202.11	TCP	78	0x0000 (0)	443 → 15880 [SYN, ACK] Seq=3674405382 Ack=2486930708 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSeqr=3119615816
35	2018-02-01 10:39:35.189214	192.168.202.11	192.168.202.111	TCP	70	0x2f32 (12082)	2 15880 → 443 [ACK] Seq=2486930708 Ack=3674405383 Win=29312 Len=0 TSeqr=3119615816 TSeqr=31196158174
36	2018-02-01 10:39:35.252397	192.168.202.11	192.168.202.111	TLSv1	257	0xcd36 (52534)	3 Client Hello
37	2018-02-01 10:39:37.274430	192.168.202.11	192.168.202.111	TCP	257	0xd9b5 (47365)	4 [TCP Retransmission] 15880 → 443 [PSH, ACK] Seq=2486930708 Ack=3674405383 Win=8192 Len=187 TSeqr=192660198 TSeqr=0
38	2018-02-01 10:39:41.297332	192.168.202.11	192.168.202.111	TCP	257	0x88a (34991)	3 [TCP Retransmission] 15880 → 443 [PSH, ACK] Seq=2486930708 Ack=3674405383 Win=8192 Len=187 TSeqr=192664224 TSeqr=0
39	2018-02-01 10:39:49.309569	192.168.202.11	192.168.202.111	TCP	257	0xf68a (63114)	2 [TCP Retransmission] 15880 → 443 [PSH, ACK] Seq=2486930708 Ack=3674405383 Win=8192 Len=187 TSeqr=192672244 TSeqr=0
40	2018-02-01 10:40:05.317305	192.168.202.11	192.168.202.111	TCP	70	0xd621 (54817)	4 15880 → 443 [RST] Seq=2486930895 Win=8192 Len=0 TSeqr=192688266 TSeqr=0
41	2018-02-01 10:40:06.790700	192.168.202.111	192.168.202.11	TCP	78	0x0000 (0)	4 [TCP Retransmission] 443 → 15880 [SYN, ACK] Seq=3674405382 Ack=2486930708 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSeqr=0

ئەس يىرىلا ئەقەل:

1. اجتىلا ئەيىتالىت TCP ۋە حفاصىم كان ھ.
2. ئەلا ئەسلىمىغا لىسىرى. Client Hello.
3. ئەلا ئەسرا ئەمەن ئەپامەنلا رادىج نم ئەلا ئەپامەنلا تايىلمۇم كان ھ.
4. ئەلا ئەسرا مەت TCP RST كان ھ.

اھبىصۇملا تاءارجىلا

ئەلا ئەپامەنلا ئەم قاطن قىيىضت ئەدىز وە عرفلىا اذە يەن ئەلا ئەپامەنلا تاءارجىلا نم ضرغىلار.

ئەيىاضا روش ئەقەل:

يەرابتىخالا عومجمىلا ئەلا ئەپامەنلا زىمر مەلتىسا مەدخىللا نأ مەدخىللا ئەلا ئەپامەنلا ئەلا ئەپامەنلا رەھەتىسىنىڭ (TCP RST) دەرىجىسى ئەلا ئەپامەنلا تەمىصب ھەلاقسەباب مۇقىوفىلات:

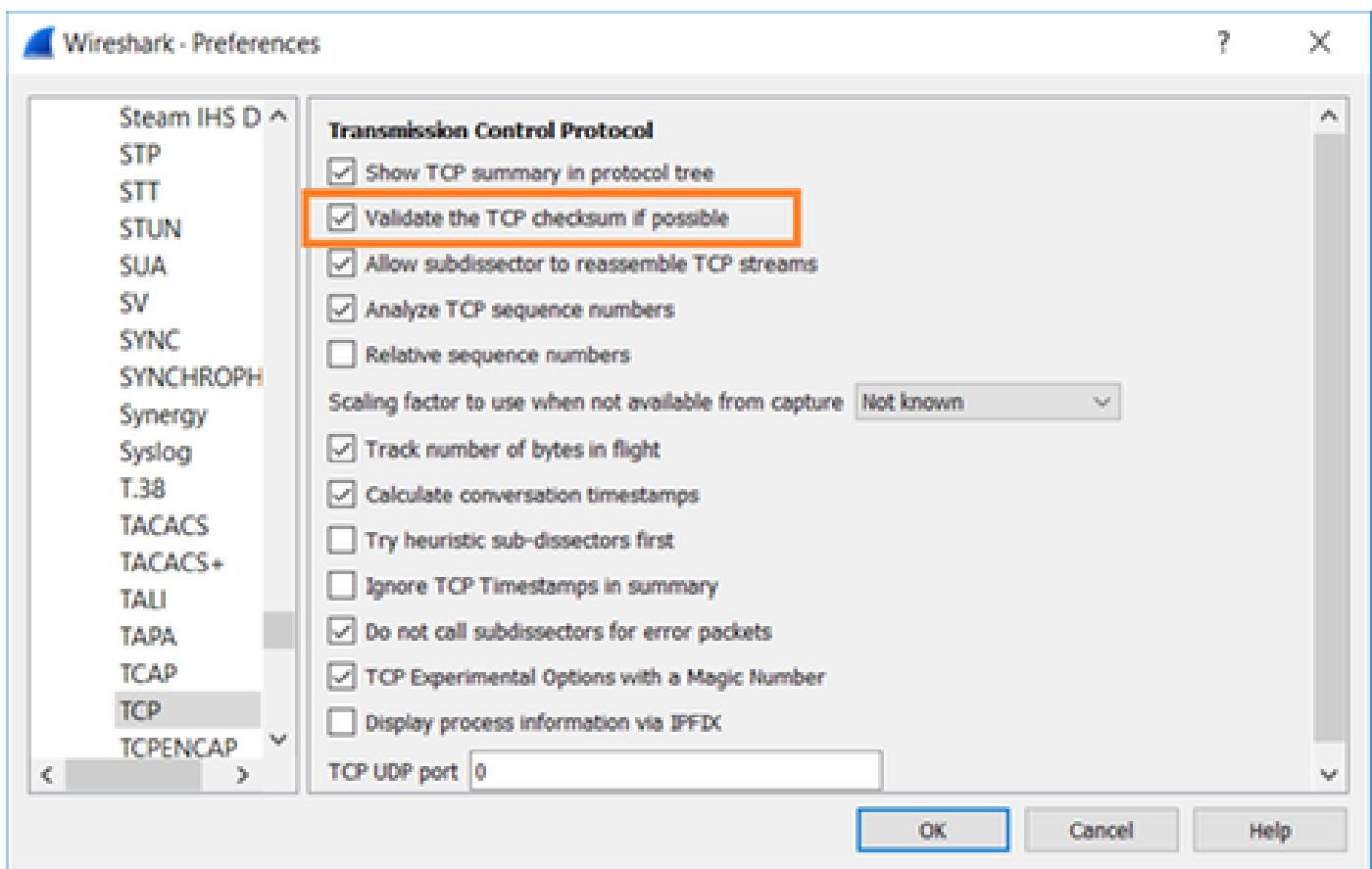
```

21:26:27.133677 IP (tos 0x0, ttl 64, id 52534, offset 0, flags [DF], proto TCP (6), length 239)
    192.168.202.11.15880 > 192.168.202.111.443: Flags [P.], cksum 0xc65 (incorrect -> 0x3063), seq 1:188, ack 1, win 64, options [nop,nop,T]
S val 192658174 ecr 3119615816], length 187
21:26:29.155652 IP (tos 0x0, ttl 64, id 47365, offset 0, flags [DF], proto TCP (6), length 239)
    192.168.202.11.15880 > 192.168.202.111.443: Flags [P.], cksum 0x4db7 (incorrect -> 0x71b5), seq 1:188, ack 1, win 64, options [nop,nop,T]
S val 192660198 ecr 0], length 187
21:26:33.178142 IP (tos 0x0, ttl 64, id 34991, offset 0, flags [DF], proto TCP (6), length 239)
    192.168.202.11.15880 > 192.168.202.111.443: Flags [P.], cksum 0x3d4d (incorrect -> 0x61fb), seq 1:188, ack 1, win 64, options [nop,nop,T]
S val 192664224 ecr 0], length 187
21:26:41.189640 IP (tos 0x0, ttl 64, id 63114, offset 0, flags [DF], proto TCP (6), length 239)
    192.168.202.11.15880 > 192.168.202.111.443: Flags [P.], cksum 0x1e9 (incorrect -> 0x42a7), seq 1:188, ack 1, win 64, options [nop,nop,T]
S val 192672244 ecr 0], length 187
21:26:57.195947 IP (tos 0x0, ttl 64, id 54817, offset 0, flags [DF], proto TCP (6), length 52)
    192.168.202.11.15880 > 192.168.202.111.443: Flags [R], cksum 0x9ee (incorrect -> 0xc2e8), seq 2486930895, win 64, options [nop,nop,TS val 192688266 ecr 0], length 0
21:26:58.668973 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length 60)
    192.168.202.11.15880 > 192.168.202.11.15880: Flags [S.], cksum 0x15fb (incorrect -> 0xffd2), seq 3674405382, ack 2486930708, win 28960, options [mss 1460,sackOK,TS val 3119647415 ecr 192658158,nop,wscale 7], length 0
^C
154 packets captured
154 packets received by filter

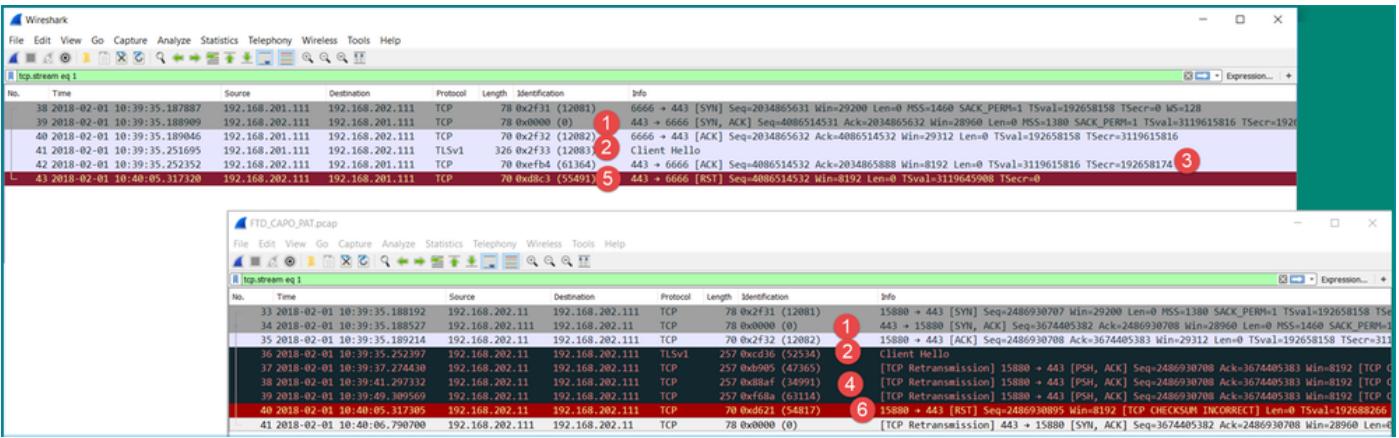
```

اعم عيش لك عضت امدنع:

رایخ ناک اذإ TCP ل يرabitخالا عومجملا نم ققحتلا نيكمتل ٰجاج كانه ،مهفلل ،ٰلاحلا هذه يف وه امك ،TCP > تالوكوتورب > تاليصفت > ريرحت ىلإ لقتنا. Wireshark ىلع انكمم كلذ ٰروصلالا يف حضوم.



ٰلماكلا ٰروصلالا ىلع لوصحلل بنج ىلإ ابنج تاطاقتلا عضن نأ ديفملانم ،ٰلاحلا هذه يف:



ةيسيئرلا طاقنلا:

- مل قفتللا نأ ينعي اذهو. اوسفن يه IP تافرعم .هاجت إلـا ةـيـالـث TCP ـحـفـاصـمـ كـانـهـ ئـامـحـلـا رـادـجـ ظـسـاوـبـ هـنـيـوـكـتـ مـتـيـ.
- رادج ظس او بـ ئـمـزـحـ لـيـثـمـتـ مـتـيـ. IP 12083ـ فـرـعـمـ يـذـلـيـمـعـلـاـ نـمـ TLS Client Helloـ رـيفـشـتـ كـفـ ئـسـاـيـسـ مـاـدـخـتـسـابـ، ئـلـاحـلـاـ هـذـهـ يـفـ، ئـيـامـحـلـاـ رـادـجـ نـيـوـكـتـ مـتـ (TLS)ـ يـرـابـتـخـالـاـ عـوـمـجـمـلـاـ فـالـتـاـ مـتـيـ، كـلـذـىـلـاـ ئـفـاضـإـلـاـبـ 52534ـ ئـلـاـ IPـ فـرـعـمـ رـيـيـغـتـ مـتـ وـ (TCP)ـ ئـمـزـحـ لـلـلـاـ (TCP Retransmission)ـ اـقـحـالـ ـ حـاـلـ اـمـتـ جـمـانـرـبـلـاـ يـفـ لـلـخـ بـبـسـبـ (TCP Retransmission)ـ ـ مـدـاخـلـاـ فـسـنـيـ يـذـلـاـ (TCP checksum incorrect)ـ).
- ـ مـدـاخـلـاـ فـسـنـيـ يـذـلـاـ (TCP ACK)ـ لـيـمـعـلـاـ ئـلـاـ لـسـرـيـوـ (TCP RST)ـ لـيـكـوـعـضـوـيـفـ ئـيـامـحـلـاـ رـادـجـ دـجـوـيـ.

33 2018-02-01 10:39:35.188192	192.168.202.11	192.168.202.111	TCP	78 0x2f31 (12081)	15880 + 443 [SYN] Seq=2486930707 Win=29200 Len=0 MSS=1380 TSval=192658158 TSecr=0
34 2018-02-01 10:39:35.188527	192.168.202.111	192.168.202.111	TCP	78 0x0000 (0)	443 + 15880 [SYN, ACK] Seq=3674405382 Ack=2486930708 Win=28960 Len=0 MSS=1460 SACK_PERM=1
35 2018-02-01 10:39:35.189214	192.168.202.11	192.168.202.111	TCP	78 0x2f32 (12082)	15880 + 443 [ACK] Seq=2486930708 Ack=4086514532 Win=29312 Len=0 TSval=192658158 TSecr=3119615816
36 2018-02-01 10:39:35.189297	192.168.202.11	192.168.202.111	TLSv1	257 0xcd36 (52534)	Client Hello
37 2018-02-01 10:39:37.274430	192.168.202.11	192.168.202.111	TCP	257 0x0000 (0)	[TCP Retransmission] 15880 + 443 [PSH, ACK] Seq=2486930708 Ack=3674405383 Win=8192 [TCP C]
38 2018-02-01 10:39:41.297332	192.168.202.11	192.168.202.111	TCP	257 0x000f (47365)	[TCP Retransmission] 15880 + 443 [PSH, ACK] Seq=2486930708 Ack=3674405383 Win=8192 [TCP C]
39 2018-02-01 10:39:49.309569	192.168.202.11	192.168.202.111	TCP	257 0x00af (34991)	[TCP Retransmission] 15880 + 443 [PSH, ACK] Seq=2486930708 Ack=3674405383 Win=8192 [TCP C]
40 2018-02-01 10:49:05.317395	192.168.202.11	192.168.202.111	TCP	29 0xd621 (54817)	15880 + 443 [RST] Seq=2486930899 Win=8192 [TCP CHECKSUM INCORRECT] Len=0 TSval=1926582466
41 2018-02-01 10:40:06.790708	192.168.202.111	192.168.202.11	TCP	78 0x0000 (0)	[TCP Retransmission] 443 + 15880 [SYN, ACK] Seq=3674405382 Ack=2486930708 Win=28960 Len=0

- ـ ئـلـاسـرـلـاـ دـيـعـيـوـ مـدـاخـلـاـ نـمـ TCP ACKـ يـأـ ئـيـامـحـلـاـ رـادـجـ يـقـلـتـيـ الـ ئـلـاسـرـلـاـ دـيـعـيـوـ مـدـاخـلـاـ نـمـ TLS Client Helloـ .
- ـ ئـطـيـشـنـتـبـ ئـيـامـحـلـاـ رـادـجـ مـاـقـ يـذـلـاـ TCPـ لـيـكـوـعـضـوـيـفـ ئـرـخـأـ ئـرـمـ .
- ـ لـيـمـعـلـاـ وـ حـنـ TCP RSTـ لـسـرـيـوـ ئـيـامـحـلـاـ رـادـجـ يـهـتـنـيـ، ئـيـنـاثـ 30ـ يـلـاـوـحـ دـعـبـ .
- ـ مـدـاخـلـاـ وـ حـنـ TCP RSTـ ئـيـامـحـلـاـ رـادـجـ لـسـرـيـ .

ـ يـلـاـ عـوـجـرـلـلـ

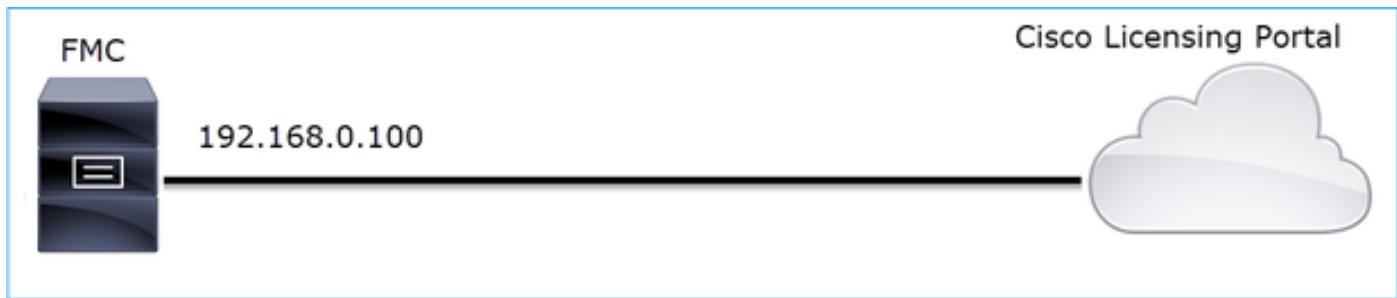
ـ لـاصـتـالـاـ دـيـكـأـتـ ئـجـلـاعـمـ Firepower TLS/SSL

2. ويرانىسلا) HTTPS لاصتا ئلكشىم 10. ئلاحلا

ل يكذلا صىخرتلا ليجست لشىف ئەلكشملا فصو.

The screenshot shows the FMC Smart Licenses interface. At the top, there are two error messages: one in a red box stating "Failed to send the message to the server. Please verify the DNS Server/HTTP Proxy settings." and another in a black box stating "Registration to the Cisco Smart Software Manager Failed to register". Below these, there is a "Welcome to Smart Licenses" message and a "Smart License Status" section with various status fields.

ططخملا ئروصىلا ھذه ضرعت:



رثأتىملار قىفتلى:

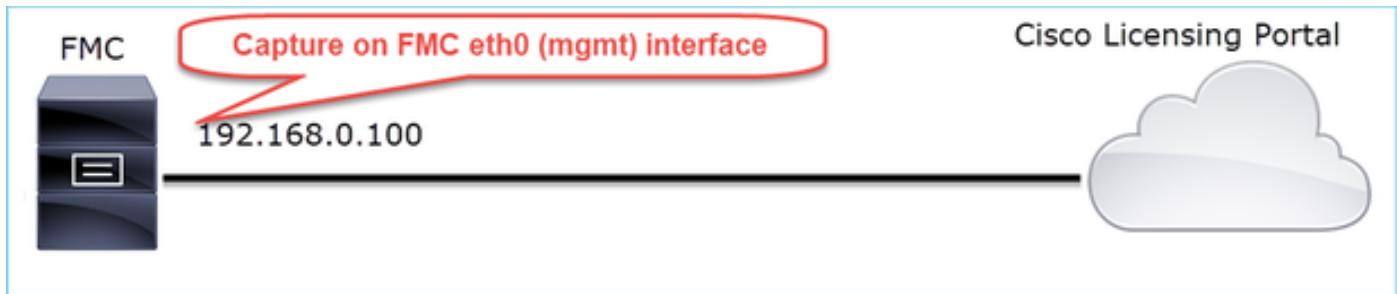
SRC IP: 192.168.0.100

DST: tools.cisco.com

لوكوتورب: TCP 443 (HTTPS)

رسألىلحت

ئەرادا ئەجأولىع طاقتلالا نىكمت:



طاقتلالا فاقىيەل CTRL-C ىلىع طغضا، أطخلا ئىلاسرا روهظ درجمب. يىرخا ئەرم ليجستلا لواح:

```

<#root>

root@firepower:/Volume/home/admin#
tcpdump -i eth0 port 443 -s 0 -w CAP.pcap
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
264 packets captured
-- CTRL-C
264 packets received by filter
0 packets dropped by kernel
root@firepower:/Volume/home/admin#

```

زاهجلا ددحو، مكحتللا ةرادي (System > Health > Monitor، مدقتملا احالصا او عاطخألا فاشكتسأ ددحو، روصلا يف حضوم وه امك، (مدقتملا احالصا او عاطخألا فاشكتسأ ددحو،

The screenshot shows the Firepower Management Center web interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', 'System' (with a red notification badge), 'Help', and 'admin'. Below the navigation is a sub-menu with 'Configuration', 'Users', 'Domains', 'Integration', 'Updates', 'Licenses', 'Health > Monitor' (which is highlighted in red), 'Monitoring', and 'Tools'. The main content area has a red header 'Advanced Troubleshooting'. A 'File Download' dialog box is open, showing the file 'CAP.pcap' and two buttons: 'Download' and 'Back'.

ىلع FMC طاقتللا رهظت روصلا طاقتل:

Wireshark interface showing the 'CAP.pcap' file. The packet list table displays the following information:

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-23 07:44:59.218797	192.168.0.100	10.229.20.96	TLSv1.2	107	Application Data
2	2019-10-23 07:44:59.220929	10.229.20.96	192.168.0.100	TLSv1.2	123	Application Data
3	2019-10-23 07:44:59.220960	192.168.0.100	10.229.20.96	TCP	54	443 → 64722 [ACK] Seq=1380971613 Ack=2615750168 Win=249 Len=0
4	2019-10-23 07:45:02.215376	192.168.0.100	10.229.20.96	TLSv1.2	107	Application Data
5	2019-10-23 07:45:02.217321	10.229.20.96	192.168.0.100	TLSv1.2	123	Application Data
6	2019-10-23 07:45:02.217336	192.168.0.100	10.229.20.96	TCP	54	443 → 64722 [ACK] Seq=1380971666 Ack=2615750237 Win=249 Len=0
7	2019-10-23 07:45:05.215460	192.168.0.100	10.229.20.96	TLSv1.2	107	Application Data
8	2019-10-23 07:45:05.217331	10.229.20.96	192.168.0.100	TLSv1.2	123	Application Data
9	2019-10-23 07:45:05.217345	192.168.0.100	10.229.20.96	TCP	54	443 → 64722 [ACK] Seq=1380971719 Ack=2615750306 Win=249 Len=0
10	2019-10-23 07:45:06.216584	10.229.20.96	192.168.0.100	TCP	66	64784 → 443 [SYN] Seq=4002690284 Win=64240 Len=0 MSS=1380 WS=256 S
11	2019-10-23 07:45:06.216631	192.168.0.100	10.229.20.96	TCP	66	443 → 64784 [SYN, ACK] Seq=3428959426 Ack=4002690285 Win=29200 Len=0
12	2019-10-23 07:45:06.218550	10.229.20.96	192.168.0.100	TCP	60	64784 → 443 [ACK] Seq=4002690285 Ack=3428959427 Win=66048 Len=0
13	2019-10-23 07:45:06.219386	10.229.20.96	192.168.0.100	TLSv1.2	571	Client Hello

لما ع مدخلت سأ، اه طاقت لا مت يتلا ةدي دجلة TCP لمع تاس لجع يموج نم قيقحت لـ حـيـملـت مـاطـنـ مـزـحـ عـيـمـوجـ ةـيـفـصـتـبـ اـذـهـ موـقـيـ ضـرـعـ ةـيـفـصـتـ اـهـ طـاـقـتـ لاـ متـ يـتـلاـ.

No.	Time	Source	Destination	Protocol	Length	Info
10	2019-10-23 07:45:06.216584	10.229.20.96	192.168.0.100	TCP	66	64784 → 443 [SYN] Seq=4002690284 Win=64240 Len=0 MSS=1380 WS=256 SACK_PERM=1
19	2019-10-23 07:45:06.225743	10.229.20.96	192.168.0.100	TCP	66	64785 → 443 [SYN] Seq=3970528579 Win=64240 Len=0 MSS=1380 WS=256 SACK_PERM=1
45	2019-10-23 07:45:12.403280	10.229.20.96	192.168.0.100	TCP	66	64790 → 443 [SYN] Seq=442965162 Win=64240 Len=0 MSS=1380 WS=256 SACK_PERM=1
51	2019-10-23 07:45:12.409842	10.229.20.96	192.168.0.100	TCP	66	64791 → 443 [SYN] Seq=77539654 Win=64240 Len=0 MSS=1380 WS=256 SACK_PERM=1
72	2019-10-23 07:45:14.466836	192.168.0.100	72.163.4.38	TCP	74	35752 → 443 [SYN] Seq=2427943531 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=16127801 TSecr=0 WS=128
108	2019-10-23 07:45:24.969622	192.168.0.100	72.163.4.38	TCP	74	35756 → 443 [SYN] Seq=1993860949 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=16138303 TSecr=0 WS=128
137	2019-10-23 07:45:35.469403	192.168.0.100	173.37.145.8	TCP	74	58326 → 443 [SYN] Seq=723413997 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2040670996 TSecr=0 WS=128
163	2019-10-23 07:45:45.969384	192.168.0.100	173.37.145.8	TCP	74	58330 → 443 [SYN] Seq=2299582550 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2040681496 TSecr=0 WS=128
192	2019-10-23 07:45:56.468664	192.168.0.100	72.163.4.38	TCP	74	35768 → 443 [SYN] Seq=1199682453 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=16169882 TSecr=0 WS=128
227	2019-10-23 07:46:07.218984	10.229.20.96	192.168.0.100	TCP	66	64811 → 443 [SYN] Seq=1496581075 Win=64240 Len=0 MSS=1380 WS=256 SACK_PERM=1
236	2019-10-23 07:46:07.225881	10.229.20.96	192.168.0.100	TCP	66	64812 → 443 [SYN] Seq=563292608 Win=64240 Len=0 MSS=1380 WS=256 SACK_PERM=1

دومعك SSL Client Hello نـمـ مـداـخـلـاـ مـسـاـ لـقـحـ قـيـبـطـ حـيـملـتـ.

طقـفـ لـئـاسـرـ ةـيـفـصـتـ لـمـاعـ قـيـبـطـ حـيـملـتـ ssl.handshake.type == 1

ssl.handshake.type == 1							
No.	Time	Source	Destination	Protocol	Length	Server Name	Info
13	2019-10-23 07:45:06.219386	10.229.20.96	192.168.0.100	TLSv1.2	571		Client Hello
23	2019-10-23 07:45:06.227250	10.229.20.96	192.168.0.100	TLSv1.2	571		Client Hello
48	2019-10-23 07:45:12.406366	10.229.20.96	192.168.0.100	TLSv1.2	571		Client Hello
54	2019-10-23 07:45:12.412199	10.229.20.96	192.168.0.100	TLSv1.2	571		Client Hello
75	2019-10-23 07:45:14.634091	192.168.0.100	72.163.4.38	TLSv1.2	571	tools.cisco.com	Client Hello
111	2019-10-23 07:45:25.136089	192.168.0.100	72.163.4.38	TLSv1.2	571	tools.cisco.com	Client Hello
140	2019-10-23 07:45:35.637252	192.168.0.100	173.37.145.8	TLSv1.2	571	tools.cisco.com	Client Hello
166	2019-10-23 07:45:46.136858	192.168.0.100	173.37.145.8	TLSv1.2	571	tools.cisco.com	Client Hello
195	2019-10-23 07:45:56.635438	192.168.0.100	72.163.4.38	TLSv1.2	571	tools.cisco.com	Client Hello
230	2019-10-23 07:46:07.221567	10.229.20.96	192.168.0.100	TLSv1.2	571		Client Hello
240	2019-10-23 07:46:07.228486	10.229.20.96	192.168.0.100	TLSv1.2	571		Client Hello

يڭىذلا صىخرتلا ئاباوب مىختىست، رىرقىتلا اذه ئباتك تقويف ئەظحالىم (tools.cisco.com) ئېلاتلا IP نىوانع: 72.163.4.38، 173.37.145.8

ئوصىلاي حضوم وە امك، قىفتىت > عېتىا) TCP تاقفدت دەعېتىا.

75	2019-10-23 07:45:14.634091	192.168.0.100	72.163.4.38	TLSv1.2	571	tools.cisco.co
111	2019-10-23 07:45:25.136089	192.168.0.100	72.163.4.38	TLSv1.2	571	tools.cisco.co
140	2019-10-23 07:45:35.637252	192.168.0.100	173.37.145.8	TLSv1.2	571	tools.cisco.co
166	2019-10-23 07:45:46.136858	192.168.0.100	173.37.145.8	TLSv1.2	571	tools.cisco.co
195	2019-10-23 07:45:56.635438	192.168.0.100	72.163.4.38	TLSv1.2	571	tools.cisco.co
230	2019-10-23 07:46:07.221567	10.229.20.96	192.168.0.100	TLSv1.2	571	
240	2019-10-23 07:46:07.228486	10.229.20.96	192.168.0.100	TLSv1.2	571	

rame 75: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits)
thernet II, Src: Vmware_10:d0:a7 (00:0c:29:10:d0:a7), Dst: Cisco_f6:1d:ae (00:be:75:f6:1d:ae)
nternet Protocol Version 4, Src: 192.168.0.100, Dst: 72.163.4.38
transmission Control Protocol, Src Port: 35752, Dst Port: 443, Seq: 2427943532, Ack: 2770078885, Len: 512
ecure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 512

Mark/Unmark Packet
Ignore/Unignore Packet
Set/Unset Time Reference
Time Shift...
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow > TCP Stream
Copy
Protocol Preferences
Decode As...
Show Packet in New Window

No.	Time	Source	Destination	Protocol	Length	Server Name	Info
72	2019-10-23 07:45:14.466836	192.168.0.100	72.163.4.38	TCP	74		35752 → 443 [SYN] Seq=2427943531 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=16127801 TSecr=0 WS=128
73	2019-10-23 07:45:14.632885	72.163.4.38	192.168.0.100	TCP	60		443 → 35752 [SYN, ACK] Seq=2770078884 Ack=2427943532 Win=8190 Len=0 MSS=1330
74	2019-10-23 07:45:14.632935	192.168.0.100	72.163.4.38	TCP	54		35752 → 443 [ACK] Seq=2427943532 Ack=2770078885 Win=29200 Len=0
75	2019-10-23 07:45:14.634091	192.168.0.100	72.163.4.38	TLSv1.2	571	tools.cisco.com	1 Client Hello 2 Server Hello 3 Certificate 4 Server Hello Done 5 Alert (Level: Fatal, Description: Unknown CA)
76	2019-10-23 07:45:14.634796	72.163.4.38	192.168.0.100	TCP	60		443 → 35752 [ACK] Seq=2770078885 Ack=2427944049 Win=32768 Len=0
77	2019-10-23 07:45:14.966729	72.163.4.38	192.168.0.100	TLSv1.2	150		35752 → 443 [ACK] Seq=2427944049 Ack=2770078981 Win=29200 Len=0
78	2019-10-23 07:45:14.966772	192.168.0.100	72.163.4.38	TCP	54		443 → 35752 [PSH, ACK] Seq=2770078981 Ack=2427944049 Win=32768 Len=1330 [TCP segment of a reassembled PDU]
79	2019-10-23 07:45:14.966834	72.163.4.38	192.168.0.100	TCP	1384		35752 → 443 [ACK] Seq=2427944049 Ack=2770080311 Win=31920 Len=0
80	2019-10-23 07:45:14.966850	192.168.0.100	72.163.4.38	TCP	54		443 → 35752 [PSH, ACK] Seq=2427944049 Ack=2770080311 Win=31920 Len=0
81	2019-10-23 07:45:14.966872	72.163.4.38	192.168.0.100	TLSv1.2	155		35752 → 443 [ACK] Seq=2427944049 Ack=2770080412 Win=31920 Len=0
82	2019-10-23 07:45:14.966881	192.168.0.100	72.163.4.38	TCP	54		443 → 35752 [PSH, ACK] Seq=2427944049 Ack=2770080412 Win=31920 Len=0
83	2019-10-23 07:45:14.966915	72.163.4.38	192.168.0.100	TLSv1.2	63		35752 → 443 [ACK] Seq=2427944049 Ack=2770080421 Win=31920 Len=0
84	2019-10-23 07:45:14.966925	192.168.0.100	72.163.4.38	TCP	54		443 → 35752 [ACK] Seq=2427944049 Ack=2770080421 Win=31920 Len=0
85	2019-10-23 07:45:14.967114	192.168.0.100	72.163.4.38	TLSv1.2	61		35752 → 443 [ACK] Seq=2427944049 Ack=2770080421 Win=31920 Len=0
86	2019-10-23 07:45:14.967261	192.168.0.100	72.163.4.38	TCP	54		443 → 35752 [ACK] Seq=2427944049 Ack=2770080421 Win=31920 Len=0
87	2019-10-23 07:45:14.967382	72.163.4.38	192.168.0.100	TCP	60		35752 → 443 [ACK] Seq=2427944049 Ack=2770080421 Win=32768 Len=0
88	2019-10-23 07:45:14.967398	192.168.0.100	72.163.4.38	TCP	54		35752 → 443 [ACK] Seq=2427944049 Ack=2770080421 Win=32768 Len=0

Frame 75: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits)
Ethernet II, Src: Vmware_10:d0:a7 (00:0c:29:10:d0:a7), Dst: Cisco_f6:1d:ae (00:be:75:f6:1d:ae)
Internet Protocol Version 4, Src: 192.168.0.100, Dst: 72.163.4.38
Transmission Control Protocol, Src Port: 35752, Dst Port: 443, Seq: 2427943532, Ack: 2770078885, Len: 512
Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 512
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Random: 234490a187438c73b50564653271c7c09fb7ac16897184...
Session ID Length: 0
Cipher Suites Length: 100
Cipher Suites (50 suites)

يەسەرلە ئاقنلار:

1. چەختىلە ئەپەپلىق (TCP) ۋە ئەپەپلىق (SSL/TLS).

2. يەڭىذلا صىخرتلا لە خەدمەت ئەپەپلىق (FMC) لىمۇعلە لىسىرى.

3. فن أتس م ظسلج تسيل اهنأ ينعي اذه 0. و ه ظسلج فرع م.
4. "مداخلا يف كب ابحرم" و "داهشل" و "مداخلا يف كب ابحرم" ظلاس رب ظهجولا مداخلا دري.
5. "فروع م ريع قدصم عجرم" ب قلعتي يذلوك لم هيبينت ليمعل لسرى.
6. ظسلجلالا قالع إل TCP RST ليمعل لسرى.
7. ئيناث 0.5 يل اوح (قالع إل اىل اعاشنالا نم) لم اكلاب TCP ظسلج ةدم تنانك.

مسالا فشكى ةلاحلا هذه يف .عئاشلا مسالا ئيؤرل ردهصلما لقح عس و مداخلا ئداهش ددح ليخدلا فيرعتب موقى زاهج نع عئاشلا (MITM).

No.	Time	Source	Destination	Protocol	Length	Server Name	Info
72	2019-10-23 07:45:14.466836	192.168.0.100	72.163.4.38	TCP	74		35752 → 443 [SYN] Seq=2427943531 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TStamp=16127801
73	2019-10-23 07:45:14.632885	72.163.4.38	192.168.0.100	TCP	60		443 → 35752 [SYN, ACK] Seq=2770078884 Ack=2427943532 Win=8190 Len=0 MSS=1330
74	2019-10-23 07:45:14.632935	192.168.0.100	72.163.4.38	TCP	54		35752 → 443 [ACK] Seq=2427943532 Ack=2770078885 Win=29200 Len=0
75	2019-10-23 07:45:14.634091	192.168.0.100	72.163.4.38	TLSv1.2	571	tools.cisco.com	Client Hello
76	2019-10-23 07:45:14.634796	72.163.4.38	192.168.0.100	TCP	60		443 → 35752 [ACK] Seq=2770078885 Ack=2427944049 Win=32768 Len=0
77	2019-10-23 07:45:14.966729	72.163.4.38	192.168.0.100	TLSv1.2	150		Server Hello
78	2019-10-23 07:45:14.966772	192.168.0.100	72.163.4.38	TCP	54		35752 → 443 [ACK] Seq=2427944049 Ack=2770078981 Win=29200 Len=0
79	2019-10-23 07:45:14.966834	72.163.4.38	192.168.0.100	TCP	1384		443 → 35752 [PSH, ACK] Seq=2770078981 Ack=2427944049 Win=32768 Len=1330 [TCP segment of a multi-segment message]
80	2019-10-23 07:45:14.966850	192.168.0.100	72.163.4.38	TCP	54		35752 → 443 [ACK] Seq=2427944049 Ack=2770080311 Win=31920 Len=0
81	2019-10-23 07:45:14.966872	72.163.4.38	192.168.0.100	TLSv1.2	155		Certificate

Length: 1426
 Handshake Protocol: Certificate
 Handshake Type: Certificate (11)
 Length: 1422
 Certificates Length: 1419
 Certificates (1419 bytes)
 Certificate Length: 1416
 Certificate: 308205843082046ca003020102020d00aa23af5d607e0000... (id-at-commonName=tools.cisco.com, id-at-organizationName=Cisco Systems, Inc., id-at-localityName=San Jose, id-at-stateOrProvinceName=California, id-at-postalCode=95131, id-at-countryName=US)
 signedCertificate
 version: v3 (2)
 serialNumber: 0x00a23af5d607e00002f423880
 signature (sha256WithRSAEncryption)
 issuer: rdnSequence (0)
 rdnSequence: 3 items (id-at-commonName=FTD4100_MITM, id-at-organizationalUnitName=FTD_OU, id-at-organizationName=FTD_0)
 RDNSequence item: 1 item (id-at-organizationName=FTD_0)
 RDNSequence item: 1 item (id-at-organizationalUnitName=FTD_OU)
 RDNSequence item: 1 item (id-at-commonName=FTD4100_MITM)
 validity
 subject: rdnSequence (0)
 subjectPublicKeyInfo
 extensions: 6 items

ةروصلالا هذه يف حضوم اذهو:

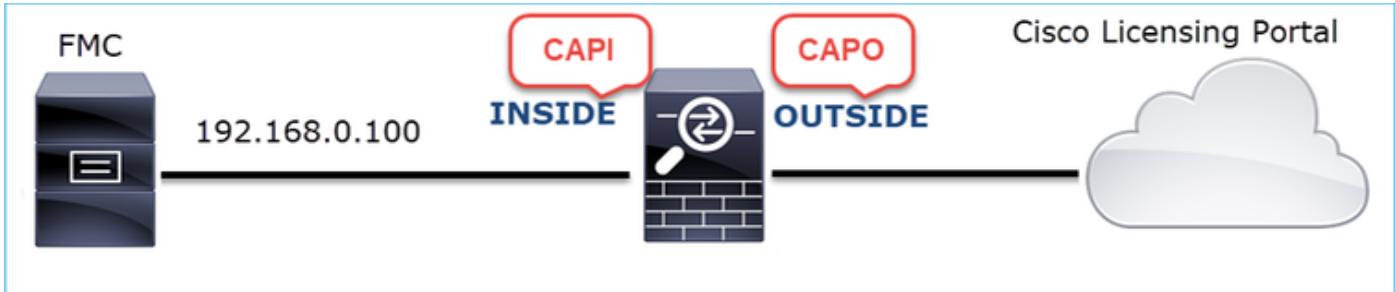


اهب يصوصملات اءارج إلإا

ةلسملالا هذه قاطن قييضرت ئدایز و ه عرفلا اذه يف ئدراولالا تاءارج إلإا نم ضرغل او.

ةيفرضلا روض طاقتلا 1. ئارج إلإا.

لقلالا ئيامح رادج زاهج ئل ع طاقتلا:



رەھەن CAPI:

No.	Time	Source	Destination	Protocol	Length	Server Name	Info
1221	2019-10-22 17:49:03.212681	192.168.0.100	173.37.145.8	TCP	74		39924 → 443 [SYN] Seq=427175838 Win=29200 Len=0 MSS=1460 SACK_PERM=1
1222	2019-10-22 17:49:03.379023	173.37.145.8	192.168.0.100	TCP	58		443 → 39924 [SYN, ACK] Seq=236460465 Ack=427175839 Win=8190 Len=0 MSS
1223	2019-10-22 17:49:03.379298	192.168.0.100	173.37.145.8	TCP	54		39924 → 443 [ACK] Seq=427175839 Ack=236460466 Win=29200 Len=0
1224	2019-10-22 17:49:03.380336	192.168.0.100	173.37.145.8	TLSv1.2	571	tools.cisco.com	Client Hello
1225	2019-10-22 17:49:03.380732	173.37.145.8	192.168.0.100	TCP	54		443 → 39924 [ACK] Seq=236460466 Ack=427176356 Win=32768 Len=0
1226	2019-10-22 17:49:03.710092	173.37.145.8	192.168.0.100	TLSv1.2	150		Server Hello
1227	2019-10-22 17:49:03.710092	173.37.145.8	192.168.0.100	TCP	1384		443 → 39924 [PSH, ACK] Seq=236460562 Ack=427176356 Win=32768 Len=1330
1228	2019-10-22 17:49:03.710092	173.37.145.8	192.168.0.100	TLSv1.2	155		Certificate
1229	2019-10-22 17:49:03.710107	173.37.145.8	192.168.0.100	TLSv1.2	63		Server Hello Done
1230	2019-10-22 17:49:03.710412	192.168.0.100	173.37.145.8	TCP	54		39924 → 443 [ACK] Seq=427176356 Ack=236460562 Win=29200 Len=0
1231	2019-10-22 17:49:03.710519	192.168.0.100	173.37.145.8	TCP	54		39924 → 443 [ACK] Seq=427176356 Ack=236461892 Win=31920 Len=0
1232	2019-10-22 17:49:03.710519	192.168.0.100	173.37.145.8	TCP	54		39924 → 443 [ACK] Seq=427176356 Ack=236461993 Win=31920 Len=0
1233	2019-10-22 17:49:03.710534	192.168.0.100	173.37.145.8	TCP	54		39924 → 443 [ACK] Seq=427176356 Ack=236462002 Win=31920 Len=0
1234	2019-10-22 17:49:03.710626	192.168.0.100	173.37.145.8	TLSv1.2	61		Alert (Level: Fatal, Description: Unknown CA)
1235	2019-10-22 17:49:03.710641	173.37.145.8	192.168.0.100	TCP	54		443 → 39924 [ACK] Seq=236462002 Ack=427176363 Win=32768 Len=0
1236	2019-10-22 17:49:03.710748	192.168.0.100	173.37.145.8	TCP	54		39924 → 443 [RST, ACK] Seq=427176363 Ack=236462002 Win=31920 Len=0
1237	2019-10-22 17:49:03.710870	192.168.0.100	173.37.145.8	TCP	54		39924 → 443 [RST] Seq=427176363 Win=0 Len=0


```

Length: 1426
└ Handshake Protocol: Certificate
  Handshake Type: Certificate (11)
  Length: 1422
  Certificates Length: 1419
  └ Certificates (1419 bytes)
    Certificate Length: 1416
    └ Certificate: 308205843082046ca003020102020d00aa23af5d607e0000... (id-at-commonName=tools.cisco.com,id-at-organizationName=Cisco Systems, Inc.,id-at-localityName=San
      └ signedCertificate
        version: v3 (2)
        serialNumber: 0x00aa23af5d607e00002f423880
        └ signature (sha256WithRSAEncryption)
      └ issuer: rdnSequence (0)
        └ rdnSequence: 3 items (id-at-commonName=FTD4100_MITM,id-at-organizationalUnitName=FTD_OU,id-at-organizationName=FTD_O)
          > RDNSequence item: 1 item (id-at-organizationName=FTD_O)
          > RDNSequence item: 1 item (id-at-organizationalUnitName=FTD_OU)
          > RDNSequence item: 1 item (id-at-commonName=FTD4100_MITM)
      └ validity
  
```

رەھەن CAPO:

tcp.stream eq 57							
No.	Time	Source	Destination	Protocol	Length	Server Name	Info
1169	2019-10-22 17:49:03.212849	192.168.0.100	173.37.145.8	TCP	78		39924 → 443 [SYN] Seq=623942018 Win=29200 Len=0 MSS=1380 SACK_PERM=1 TSval=
1170	2019-10-22 17:49:03.378962	173.37.145.8	192.168.0.100	TCP	62		443 → 39924 [SYN, ACK] Seq=4179450724 Ack=623942019 Win=8190 Len=0 MSS=1380
1171	2019-10-22 17:49:03.379329	192.168.0.100	173.37.145.8	TCP	58		39924 → 443 [ACK] Seq=623942019 Ack=4179450725 Win=29200 Len=0
1172	2019-10-22 17:49:03.380793	192.168.0.100	173.37.145.8	TLSv1.2	512	tools.cisco.com	Client Hello
1173	2019-10-22 17:49:03.545748	173.37.145.8	192.168.0.100	TCP	1388		443 → 39924 [PSH, ACK] Seq=4179450725 Ack=623942473 Win=34780 Len=1330 [TCP]
1174	2019-10-22 17:49:03.545809	173.37.145.8	192.168.0.100	TCP	1388		443 → 39924 [PSH, ACK] Seq=4179452055 Ack=623942473 Win=34780 Len=1330 [TCP]
1175	2019-10-22 17:49:03.545824	192.168.0.100	173.37.145.8	TCP	58		39924 → 443 [ACK] Seq=623942473 Ack=4179453385 Win=65535 Len=0
1176	2019-10-22 17:49:03.545915	173.37.145.8	192.168.0.100	TCP	1388		443 → 39924 [PSH, ACK] Seq=4179453385 Ack=623942473 Win=34780 Len=1330 [TCP]
1177	2019-10-22 17:49:03.545961	173.37.145.8	192.168.0.100	TCP	1388		443 → 39924 [PSH, ACK] Seq=4179454715 Ack=623942473 Win=34780 Len=1330 [TCP]
1178	2019-10-22 17:49:03.545961	192.168.0.100	173.37.145.8	TCP	58		39924 → 443 [ACK] Seq=623942473 Ack=4179456045 Win=65535 Len=0
1179	2019-10-22 17:49:03.709428	173.37.145.8	192.168.0.100	TLSv1.2	82		Server Hello, Certificate, Server Hello Done
1180	2019-10-22 17:49:03.710687	192.168.0.100	173.37.145.8	TLSv1.2	65		Alert (Level: Fatal, Description: Unknown CA)
1181	2019-10-22 17:49:03.710885	192.168.0.100	173.37.145.8	TCP	58		39924 → 443 [FIN, PSH, ACK] Seq=623942480 Ack=4179456069 Win=65535 Len=0
1182	2019-10-22 17:49:03.874542	173.37.145.8	192.168.0.100	TCP	58		443 → 39924 [RST, ACK] Seq=4179456069 Ack=623942480 Win=9952 Len=0

```

Length: 5339
> Handshake Protocol: Server Hello
  ↴ Handshake Protocol: Certificate
    ↴ Handshake Type: Certificate (11)
      Length: 5240
      Certificates Length: 5237
      ↴ Certificates (5237 bytes)
        Certificate Length: 2025
        ↴ Certificate: 308207e5308205cda00302010202143000683b0f7504f7b2... (id-at-commonName=tools.cisco.com,id-at-organizationName=Cisco Systems, Inc.,id-at-localityName=San Jose,
          > signedCertificate
          > algorithmIdentifier (sha256WithRSAEncryption)
          Padding: 0
          encrypted: 6921d084f7a6f6167058f14e2aad8b98b4e6c971ea6ea3b4...
        Certificate Length: 1736
        ↴ Certificate: 308206c4308204aca00302010202147517167783d0437eb5... (id-at-commonName=HydrantID SSL ICA G2,id-at-organizationName=HydrantID (Avalanche Cloud Corporation),id-
          < version: v3 (2)
          < serialNumber: 0x7517167783d0437eb556c357946e4563b8ebd3ac
          < signature (sha256WithRSAEncryption)
          < issuer: rdnSequence (0)
            > rdnSequence: 3 items (id-at-commonName=QuoVadis Root CA 2,id-at-organizationName=QuoVadis Limited,id-at-countryName=BM)
          < validity
    
```

مداخل ا ةداهش لدعی لقنلا ئامح رادج نأ طاقتل الا هذه تببث

زاحلا تالجس نم ققحت. 2. ئارج الـا.

دنتسمـلـا اـذـهـيـفـ حـضـوـمـ وـهـ اـمـكـ FMC TS ةـمزـحـ عـيـمـجـتـ كـنـكـمـيـ

<https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html>

لـثـمـ لـئـاسـرـ /ـفـلـمـلـاـ صـرـعـيـ،ـةـلـاحـلـاـ هـذـهـ يـفـ

<#root>

```

SOUT: 10-23 05:45:14 2019-10-23 05:45:36 sla[10068]: *Wed .967 UTC: CH-LIB-ERROR: ch_pf_curl_send_msg[4
failed to perform, err code 60, err string "SSL peer certificate or SSH remote key was not OK"
...
SOUT: 10-23 05:45:14 2019-10-23 05:45:36 sla[10068]: *Wed .967 UTC: CH-LIB-TRACE: ch_pf_curl_is_cert_is
cert issue checking, ret 60, url "https://tools.cisco.com/its/

```

بـيـصـومـ لـجـ

ةـبـاحـسـىـلـاـ حـاجـنـبـ لـيـجـسـتـلـاـ FMCـ لـنـكـمـيـ ئـتـحـ دـدـحـمـلـاـ قـفـدـتـلـلـ MITMـ

يـكـذـلـاـ صـيـخـرـتـلـاـ.

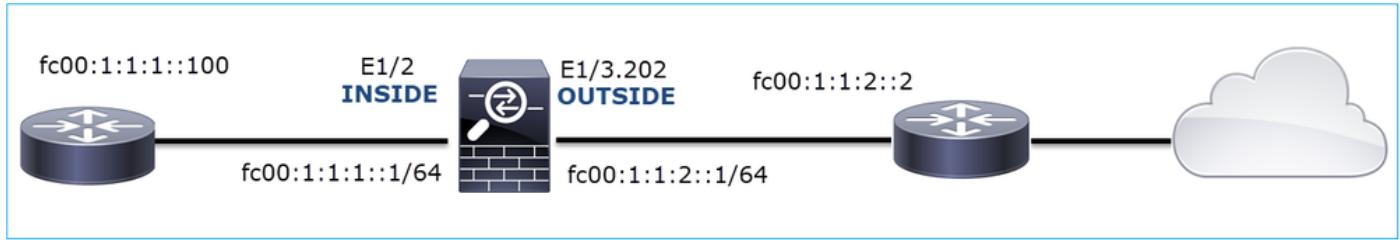
لـاـصـتـاـيـفـ ئـلـكـشـمـ 11. ئـلـاحـلـاـ

ئـيـامـحـلـاـ رـادـجـ ئـهـجـاـوـ فـلـخـ نـيـدـوـجـوـمـلـاـ)ـ نـيـيـلـخـادـلـاـ نـيـفـيـضـمـلـلـ نـكـمـيـ الـ:ـ ئـلـكـشـمـلـاـ فـصـوـ

رـادـجـ ئـهـجـاـوـ فـلـخـ ئـدـوـجـوـمـلـاـ ئـفـيـضـمـلـاـ تـائـيـبـلـاـ)ـ نـيـيـجـرـاخـلـاـ نـيـفـيـضـمـلـاـبـ لـاـصـتـاـلـاـ (ـ ئـلـخـادـلـاـ)

ةيامحلا راخلا ئيجرا.

ضرعت ططخملارا ۋروصلانىدا:



رثأتىملا قىفتىلى:

SRC IP: 00:1:1:1::100 ئيفىللاتاونقلا

DST IP: 00:1:1:2::2 ئيفىللاتاونقلا لوكوتورب

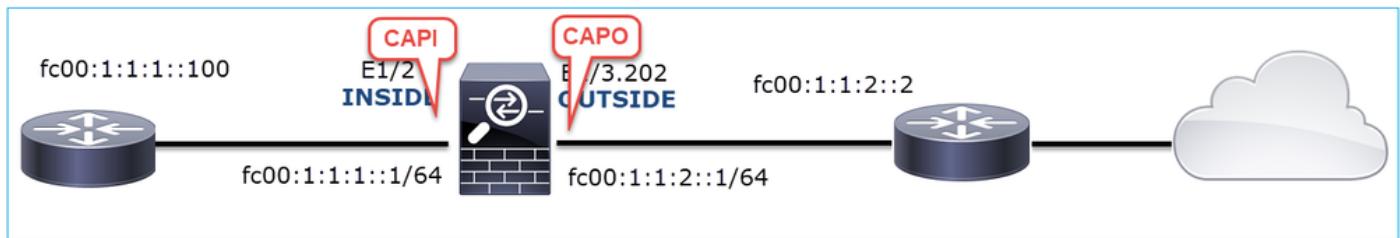
يأ: لوكوتوربلا

رسألىلەت

كەرەمە ئىلۇغ طاقىتلەتايىلمۇن يېكىمتب مق FTD LINA.

```
<#root>
```

```
firepower#  
capture CAPI int INSIDE match ip any6 any6  
firepower#  
capture CAPO int OUTSIDE match ip any6 any6
```



لەمۇي اىل ويرانىس - طاقىتلەت

ىلإ (ھجوملا لخاد) IP FC00:1:1:1::100 نم ICMP رابتخا عازىزلا طاقىتلەتدا ذخا مەت IP FC00:1:1:2::2 نم ھجوم (داخىللا نم).

يەلۇغ ۋەچىجاو يوتحىي Capture on Firewall INSIDE:

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-24 13:02:07.001663	fc00:1:1:1::100	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for fc00:1:1:1::1 from 4c:4e:35:fc:fc:d8
2	2019-10-24 13:02:07.001876	fc00:1:1:1::1	fc00:1:1:1::100	ICMPv6	86	Neighbor Advertisement fc00:1:1:1::1 (rtr, sol, ovr) is at 00:be:75:f6:1d:ae
3	2019-10-24 13:02:07.002273	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x160d, seq=0, hop limit=64 (no response found!)
4	2019-10-24 13:02:08.997918	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x160d, seq=1, hop limit=64 (no response found!)
5	2019-10-24 13:02:10.998056	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x160d, seq=2, hop limit=64 (no response found!)
6	2019-10-24 13:02:11.999917	fe80::2be:75ff:fe:6:1dae	fc00:1:1:1::100	ICMPv6	86	Neighbor Advertisement for fc00:1:1:1::100 from 00:be:75:f6:1d:ae
7	2019-10-24 13:02:12.002075	fc00:1:1:1::100	fe80::2be:75ff:fe:6:1dae	ICMPv6	78	Neighbor Advertisement fc00:1:1:1::100 (rtr, sol)
8	2019-10-24 13:02:12.998346	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x160d, seq=3, hop limit=64 (no response found!)
9	2019-10-24 13:02:14.998483	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x160d, seq=4, hop limit=64 (no response found!)
10	2019-10-24 13:02:17.062725	fe80::4e4e:35ff:fe:fc:cd8	fe80::2be:75ff:fe:6:1dae	ICMPv6	86	Neighbor Solicitation for fe80::2be:75ff:fe:6:1dae from 4c:4e:35:fc:fc:d8
11	2019-10-24 13:02:17.062862	fe80::2be:75ff:fe:6:1dae	fe80::4e4e:35ff:fe:fc:cd8	ICMPv6	78	Neighbor Advertisement fe80::2be:75ff:fe:6:1dae (rtr, sol)
12	2019-10-24 13:02:22.059994	fe80::2be:75ff:fe:6:1dae	fe80::4e4e:35ff:fe:fc:cd8	ICMPv6	86	Neighbor Solicitation for fe80::4e4e:35ff:fe:fc:cd8 from 00:be:75:f6:1d:ae
13	2019-10-24 13:02:22.063000	fe80::4e4e:35ff:fe:fc:cd8	fe80::2be:75ff:fe:6:1dae	ICMPv6	78	Neighbor Advertisement fe80::4e4e:35ff:fe:fc:cd8 (rtr, sol)

لما طاقت ایسیزرا:

1. IP MAC خاچ زابلا (IPv6) ناوون بللطی و ل ةرواجم بللط ةلاسر هجوملا لسري FC00:1:1:1::1).

2. IPv6 راج نالع امادختساب ئامحلا رادج دودر.

3. ICMP Echo بللط هجوملا لسري.

4. IP MAC خاچ زابلا (IPv6) ناوون بللطی و ل ةرواجم بللط ةلاسر ئامحلا رادج لسري (fc00:1:1:1::100). مداخلا نام تانايبلالا.

5. IPv6 راج نالع امادختساب هجوملا دري.

6. ICMP ئىفصلى ئاپلط هجوملا لسري.

لما طاقت ایسیزرا جراخ دوجوملا ئامحلا رادج ىلعلا يوتحي:

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-24 13:02:07.002517	fe80::2be:75ff:fe:6:1d8e	ff02::1:ff00:2	ICMP	90	Neighbor Solicitation for fc00:1:1:2::2 from 00:be:75:f6:1d:8e
2	2019-10-24 13:02:07.005569	fc00:1:1:2::2	fe80::2be:75ff:fe:6:1d8e	ICMP	90	Neighbor Advertisement fc00:1:1:2::2 (rtr, sol, ovr) is at 4c:4e:35:fc:fc:d8
3	2019-10-24 13:02:08.997995	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	18	Echo (ping) request id=0x160d, seq=0, hop limit=64 (no response found!)
4	2019-10-24 13:02:09.001815	fc00:1:1:2::2	ff02::1:ff00:100	ICMPv6	90	Neighbor Solicitation for fc00:1:1:1::100 from 4c:4e:35:fc:fc:d8
5	2019-10-24 13:02:10.025938	fc00:1:1:2::2	ff02::1:ff00:100	ICMPv6	90	Neighbor Solicitation for fc00:1:1:1::100 from 4c:4e:35:fc:fc:d8
6	2019-10-24 13:02:10.998132	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x160d, seq=3, hop limit=64 (no response found!)
7	2019-10-24 13:02:11.050015	fc00:1:1:2::2	ff02::1:ff00:100	ICMPv6	90	Neighbor Solicitation for fc00:1:1:1::100 from 4c:4e:35:fc:fc:d8
8	2019-10-24 13:02:12.066082	fe80::4e4e:35ff:fe:fc:cd8	fe80::2be:75ff:fe:6:1d8e	ICMPv6	90	Neighbor Solicitation for fe80::2be:75ff:fe:6:1d8e from 4c:4e:35:fc:fc:d8
9	2019-10-24 13:02:12.066234	fe80::2be:75ff:fe:6:1d8e	fe80::4e4e:35ff:fe:fc:cd8	ICMPv6	118	Echo (ping) request id=0x160d, seq=0, hop limit=64 (no response found!)
10	2019-10-24 13:02:12.998422	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x160d, seq=3, hop limit=64 (no response found!)
11	2019-10-24 13:02:13.002105	fc00:1:1:2::2	ff02::1:ff00:100	ICMPv6	90	Neighbor Solicitation for fc00:1:1:1::100 from 4c:4e:35:fc:fc:d8
12	2019-10-24 13:02:14.090251	fc00:1:1:2::2	ff02::1:ff00:100	ICMPv6	90	Neighbor Solicitation for fc00:1:1:1::100 from 4c:4e:35:fc:fc:d8
13	2019-10-24 13:02:14.998544	fc00:1:1:1::100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x160d, seq=4, hop limit=64 (no response found!)
14	2019-10-24 13:02:15.178350	fc00:1:1:2::2	ff02::1:ff00:100	ICMPv6	90	Neighbor Solicitation for fc00:1:1:1::100 from 4c:4e:35:fc:fc:d8
15	2019-10-24 13:02:17.059963	fe80::2be:75ff:fe:6:1d8e	fe80::4e4e:35ff:fe:fc:cd8	ICMPv6	90	Neighbor Solicitation for fe80::4e4e:35ff:fe:fc:cd8 from 00:be:75:f6:1d:8e
16	2019-10-24 13:02:17.062512	fe80::4e4e:35ff:fe:fc:cd8	fe80::2be:75ff:fe:6:1d8e	ICMPv6	82	Neighbor Advertisement fe80::4e4e:35ff:fe:fc:cd8 (rtr, sol)

لما طاقت ایسیزرا:

1. IP MAC خاچ زابلا (IPv6) ناوون بللط ئاپل (IPv6) رادج لسري FC00:1:1:2::2).

2. IPv6 راج نالع امادختساب هجوملا دري.

3. ICMP ئىفصلى ئاپلط هجوملا رادج لسري.

4. IP IPv6 ئاپل بللط ةلاسر هجوملا (FC00:1:1:2::2) تانايبلالا قفت زاح لسري.

5. ICMP ئىفصلى ئاپل ئاپل بللط ةلاسر هجوملا (fc00:1:1:1::100) ناوون بللط.

6. ICMP ئىفصلى ئاپل ئاپل بللط ةلاسر ئاپل (IPv6) ناوون عل MAC ناوون عل IPv6 ناوون عل IPv6.

7. IP MAC خاچ زابلا (IPv6) ناوون بللط ئاپل (IPv6) رادج لسري fc00:1:1:1::100.

لما طاقت ایسیزرا رادج بللط ئاپل (IPv6) ناوون عل MAC ناوون عل IPv6 عضوبللطی، كلذ نم الدب نكلو، (FC00:1:1:1:100) يجراخلا ريغنىوكت.

أه بىصوملا تاءارجإلا

لأسملما هذه قاطن قييضت ئاديز وھ عرفلا اذه يف ئادولما تاءارجإلا نم ضرغلما

1. ئارج إلا IPv6 ل رواجملا لودجلانم ققحت.

حى حص لكشب أبعع IPv6 ئيامحلارادجل رواجملا لودجل.

<#root>

```
firepower#
show ipv6 neighbor | i fc00
fc00:1:1:2::2          58 4c4e.35fc.fcd8 STALE OUTSIDE
fc00:1:1:1::100        58 4c4e.35fc.fcd8 STALE INSIDE
```

2. ئارج إلا IPv6 نيوكتنم ققحت.

ةيامحلارادجنيوكتوه اذه.

<#root>

```
firewall#
show run int e1/2
!
interface Ethernet1/2
  nameif INSIDE
  cts manual
    propagate sgt preserve-untag
    policy static sgt disabled trusted
    security-level 0
    ip address 192.168.0.1 255.255.255.0
    ipv6 address

fc00:1:1:1::1/64
  ipv6 enable

firewall#
show run int e1/3.202
!
interface Ethernet1/3.202
  vlan 202
  nameif OUTSIDE
  cts manual
    propagate sgt preserve-untag
    policy static sgt disabled trusted
    security-level 0
    ip address 192.168.103.96 255.255.255.0
    ipv6 address

fc00:1:1:2::1/64
  ipv6 enable
```

لـا لـيـكـشـت ةـادـأ up misconfiguration:

<#root>

Router#

```
show run interface g0/0.202
```

!

```
interface GigabitEthernet0/0.202
encapsulation dot1Q 202
vrf forwarding VRF202
ip address 192.168.2.72 255.255.255.0
ipv6 address FC00:1:1:2::2
```

/48

يـفـيـظـوـ وـيـرـانـيـسـ - طـاقـتـلـا

يـفـ CAPI طـاقـتـلـا وـهـ اـذـهـ . ةـلـكـشـمـلـا (64 /ـلـاـ) ةـيـعـرـفـلـاـ ةـكـبـشـلـاـ عـاـنـقـ رـيـغـتـ حـلـصـاـ . يـفـيـظـوـلـاـ وـيـرـانـيـسـلـاـ

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-24 15:17:20.677775	fc00:1:1:1:1:100	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for fc00:1:1:1:1 from 4c:4e:35:fc:fc:d8
2	2019-10-24 15:17:20.677989	fc00:1:1:1:1:1	fc00:1:1:1:1:100	ICMPv6	86	Neighbor Advertisement fc00:1:1:1:1 (rtr, sol, ovr) is at 00:be:75:f6:1d:ae
3	2019-10-24 15:17:20.678401	fc00:1:1:1:1:100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x097e, seq=0, hop limit=64 (no response found!)
4	2019-10-24 15:17:22.674281	fc00:1:1:1:1:100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x097e, seq=1, hop limit=64 (no response found!)
5	2019-10-24 15:17:24.674403	fc00:1:1:1:1:100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x097e, seq=2, hop limit=64 (reply in 6)
6	2019-10-24 15:17:24.674815	fc00:1:1:2::2	fc00:1:1:1:1:100	ICMPv6	114	Echo (ping) reply id=0x097e, seq=2, hop limit=64 (request in 5)
7	2019-10-24 15:17:24.675242	fc00:1:1:1:1:100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x097e, seq=3, hop limit=64 (reply in 8)
8	2019-10-24 15:17:24.675731	fc00:1:1:2::2	fc00:1:1:1:1:100	ICMPv6	114	Echo (ping) reply id=0x097e, seq=3, hop limit=64 (request in 7)
9	2019-10-24 15:17:24.676356	fc00:1:1:1:1:100	fc00:1:1:2::2	ICMPv6	114	Echo (ping) request id=0x097e, seq=4, hop limit=64 (reply in 10)
10	2019-10-24 15:17:24.676753	fc00:1:1:2::2	fc00:1:1:1:1:100	ICMPv6	114	Echo (ping) reply id=0x097e, seq=4, hop limit=64 (request in 9)

يـسـيـئـرـلـاـ ةـطـقـنـلـاـ:

- ثـبـلـاـ زـاهـجـلـاـ نـاـوـنـعـ بـلـطـتـ يـتـلـاـ IPv6ـ ةـرـوـاجـمـ بـلـطـ ةـلـاسـرـ هـجـوـمـلـاـ لـسـرـيـ (IPـ FC00:1:1:1:1).
- راـجـ نـالـعـ اـمـاـخـتـسـابـ ةـيـامـحـلـاـ رـاـدـجـ دـوـدـرـ IPv6.
- دوـرـىـلـعـ لـصـحـيـوـ ICMP ECHOـ تـابـلـطـ هـجـوـمـلـاـ لـسـرـيـ.

تاـيـوـتـحـ CAPOـ:

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-24 15:17:20.678645	fe80::2be:75ff:fe.. ff02::1:ff00:2	ICMPv6	90	Neighbor Solicitation for fc00:1:1:2::2 from 00:be:75:f6:1d:8e	
2	2019-10-24 15:17:20.681818	fc00:1:1:2::2	fe80::2be:75ff:fe.. fe00:1:1:2::2	ICMPv6	90	Neighbor Advertisement fc00:1:1:2::2 (rtr, sol, ovr) is at 4c:4e:35:fc:fc:d8
3	2019-10-24 15:17:22.674342	fc00:1:1:1:1:100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x097e, seq=1, hop limit=64 (reply in 6)
4	2019-10-24 15:17:22.677943	fc00:1:1:1:2::2	ff02::1:ff00:1	ICMPv6	90	Neighbor Solicitation for fc00:1:1:2::1 from 4c:4e:35:fc:fc:d8
5	2019-10-24 15:17:22.678096	fc00:1:1:2::1	fc00:1:1:2::2	ICMPv6	90	Neighbor Advertisement fc00:1:1:2::1 (rtr, sol, ovr) is at 00:be:75:f6:1d:8e
6	2019-10-24 15:17:22.678462	fc00:1:1:2::2	fc00:1:1:1:1:100	ICMPv6	118	Echo (ping) reply id=0x097e, seq=2, hop limit=64 (request in 3)
7	2019-10-24 15:17:24.674449	fc00:1:1:1:1:100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x097e, seq=2, hop limit=64 (reply in 8)
8	2019-10-24 15:17:24.674785	fc00:1:1:2::2	fc00:1:1:1:1:100	ICMPv6	118	Echo (ping) reply id=0x097e, seq=2, hop limit=64 (request in 7)
9	2019-10-24 15:17:24.675395	fc00:1:1:1:1:100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x097e, seq=3, hop limit=64 (reply in 10)
10	2019-10-24 15:17:24.675700	fc00:1:1:2::2	fc00:1:1:1:1:100	ICMPv6	118	Echo (ping) reply id=0x097e, seq=3, hop limit=64 (request in 9)
11	2019-10-24 15:17:24.676448	fc00:1:1:1:1:100	fc00:1:1:2::2	ICMPv6	118	Echo (ping) request id=0x097e, seq=4, hop limit=64 (reply in 12)
12	2019-10-24 15:17:24.676738	fc00:1:1:2::2	fc00:1:1:1:1:100	ICMPv6	118	Echo (ping) reply id=0x097e, seq=4, hop limit=64 (request in 11)

يـسـيـئـرـلـاـ طـاقـنـلـاـ:

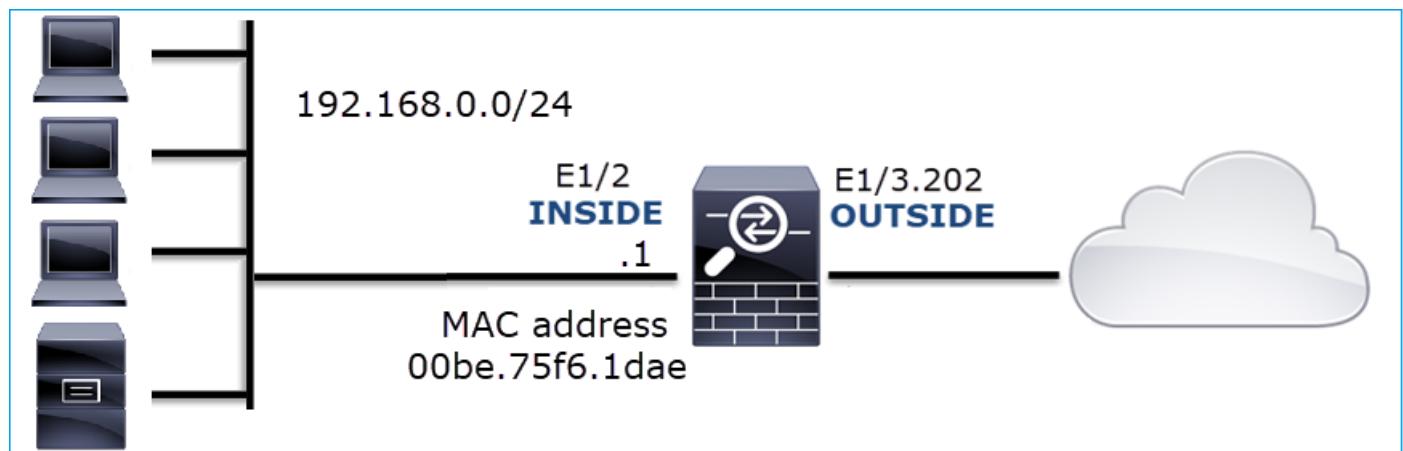
- ثـبـلـاـ زـاهـجـلـاـ نـاـوـنـعـ بـلـطـتـ يـتـلـاـ IPv6ـ ةـرـوـاجـمـ بـلـطـ ةـلـاسـرـ هـجـوـمـلـاـ لـسـرـيـ (IPـ FC00:1:1:2::2).

2. راج نالع امادختساب ئامحلا را داج دودر.
3. ICMP Echo.
4. قفدت زاهج ل MAC ناونع بـلـطـتـيـتـلـا IPv6 ۋـرـاـجـمـ بـلـطـ بـلـطـ ئـامـحـلـا رـاـدـجـ لـسـرـيـ.
5. راج نالع امادختساب ئامحلا را داج دودر.
6. دورىلۇع لـصـحـيـوـ ئـابـلـطـ ئـامـحـلـا رـاـدـجـ لـسـرـيـ ECHO.

12. ۋـلـاحـلـا (ARP مـيـمـسـتـ)

عـطـقـتـمـ لـاصـتـاـ لـكـاشـمـ (192.168.0.x/24) ئـيـلـخـادـلـا ئـفـيـضـمـلـا ئـزـهـجـأـلـا هـجـاـوتـ: ئـلـكـشـمـلـا فـصـوـ اـهـسـفـنـ ئـيـعـرـفـلـا ئـكـبـشـلـا يـفـ ئـفـيـضـمـلـا ئـزـهـجـأـلـا عـمـ

طـطـخـمـلـا ئـرـوـصـلـا ھـذـھـ ضـرـعـتـ:



رـثـأـتـمـلـا قـفـدـتـلـا:

SRC IP: 192.168.0.x/24

DST IP: 192.168.0.x/24

يـأـ: لـوـكـوـتـوـرـبـلـا

اـهـمـيـمـسـتـ مـتـ دقـ يـلـخـادـ فـيـضـمـلـا ARP نـيـزـخـتـ ئـرـكـاـذـ نـأـ وـدـبـيـ:

```
C:\Windows\system32\cmd.exe
C:\Users\mzafeiro1>arp -a
Interface: 192.168.0.55 --- 0xb
  Internet Address      Physical Address          Type
  192.168.0.1            00-be-75-f6-1d-ae    dynamic
  192.168.0.22           00-be-75-f6-1d-ae    dynamic
  192.168.0.23           00-be-75-f6-1d-ae    dynamic
  192.168.0.24           00-be-75-f6-1d-ae    dynamic
  192.168.0.25           00-be-75-f6-1d-ae    dynamic
  192.168.0.26           00-be-75-f6-1d-ae    dynamic
  192.168.0.27           00-be-75-f6-1d-ae    dynamic
  192.168.0.28           00-be-75-f6-1d-ae    dynamic
  192.168.0.29           00-be-75-f6-1d-ae    dynamic
  192.168.0.30           00-be-75-f6-1d-ae    dynamic
  192.168.0.88           00-be-75-f6-1d-ae    dynamic
  192.168.0.255          ff-ff-ff-ff-ff-ff    static
  224.0.0.22              01-00-5e-00-00-16    static
  224.0.0.251             01-00-5e-00-00-fb    static
  224.0.0.252             01-00-5e-00-00-fc    static
  239.255.255.250         01-00-5e-7f-ff-fa    static

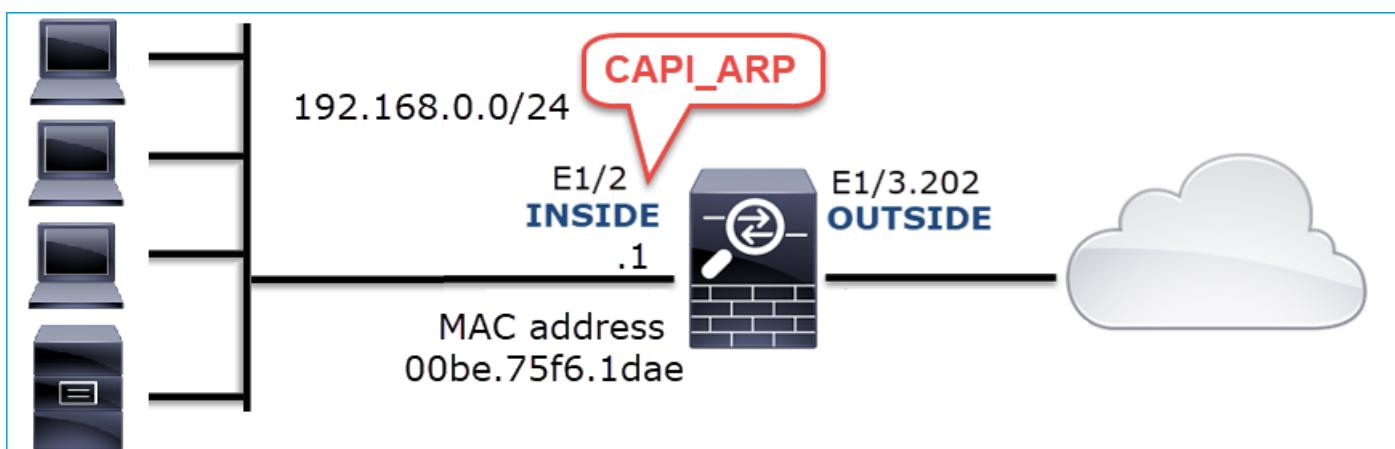
C:\Users\mzafeiro1>
```

رسأ ليلحت

كرحم ىلع طاقتلا نيكمت FTD LINA

: ئيلخادلا ۋە جاولى ىلع طقف ARP مزح طاقتلا اذه ضبق ىلۇ:

```
<#root>
firepower#
capture CAPI_ARP interface INSIDE ethernet-type arp
```



لەمۇي ال ويرانىس - طاقتلا:

ئەيامحلا رادىج ۋە جاولى ىلع طاقتلا يوتحى INSIDE.

No.	Time	Source	Destination	Protocol	Length	Info
4	2019-10-25 10:01:55.179571	Vmware_2c:9b:a7	Broadcast	ARP	1	60 Who has 192.168.0.23? Tell 192.168.0.55
5	2019-10-25 10:01:55.17969	Cisco_f6:1d:ae	Vmware_2c:9b:a7	ARP	2	42 192.168.0.23 is at 00:be:75:f6:1d:ae
35	2019-10-25 10:02:13.058397	Vmware_2c:9b:a7	Broadcast	ARP	1	60 Who has 192.168.0.24? Tell 192.168.0.55
36	2019-10-25 10:02:13.050488	Cisco_f6:1d:ae	Vmware_2c:9b:a7	ARP	2	42 192.168.0.24 is at 00:be:75:f6:1d:ae
47	2019-10-25 10:02:19.284683	Vmware_2c:9b:a7	Broadcast	ARP	1	60 Who has 192.168.0.25? Tell 192.168.0.55
48	2019-10-25 10:02:19.284775	Cisco_f6:1d:ae	Vmware_2c:9b:a7	ARP	2	42 192.168.0.25 is at 00:be:75:f6:1d:ae
61	2019-10-25 10:02:25.779821	Vmware_2c:9b:a7	Broadcast	ARP	1	60 Who has 192.168.0.26? Tell 192.168.0.55
62	2019-10-25 10:02:25.779912	Cisco_f6:1d:ae	Vmware_2c:9b:a7	ARP	2	42 192.168.0.26 is at 00:be:75:f6:1d:ae
76	2019-10-25 10:02:31.978175	Vmware_2c:9b:a7	Broadcast	ARP	1	60 Who has 192.168.0.27? Tell 192.168.0.55
77	2019-10-25 10:02:31.978251	Cisco_f6:1d:ae	Vmware_2c:9b:a7	ARP	2	42 192.168.0.27 is at 00:be:75:f6:1d:ae
97	2019-10-25 10:02:38.666515	Vmware_2c:9b:a7	Broadcast	ARP	1	60 Who has 192.168.0.28? Tell 192.168.0.55
98	2019-10-25 10:02:38.666606	Cisco_f6:1d:ae	Vmware_2c:9b:a7	ARP	2	42 192.168.0.28 is at 00:be:75:f6:1d:ae
121	2019-10-25 10:02:47.384074	Vmware_2c:9b:a7	Broadcast	ARP	1	60 Who has 192.168.0.29? Tell 192.168.0.55
122	2019-10-25 10:02:47.384150	Cisco_f6:1d:ae	Vmware_2c:9b:a7	ARP	2	42 192.168.0.29 is at 00:be:75:f6:1d:ae
137	2019-10-25 10:02:53.539995	Vmware_2c:9b:a7	Broadcast	ARP	1	60 Who has 192.168.0.30? Tell 192.168.0.55
138	2019-10-25 10:02:53.540087	Cisco_f6:1d:ae	Vmware_2c:9b:a7	ARP	2	42 192.168.0.30 is at 00:be:75:f6:1d:ae

ئەسپىئرلارا طاقنلا:

- 192.168.0.x/24 تابلتخ ARP نەم فەلتەن ئەپەپلىقلىتى رادىج.
- 2 MAC ناونع مادختساب (proxy-arp) ئەپەپلىقلىتى رادىج بىجىتسى.

اھبىصۇملا تاءارجىلا

ۋەلأسىملا هذه قاتەن قىيىضت ئەدايىز وە عەرفلا اذە يىف ئەدراولى تاءارجىلا نەم ضرغىلار.

نېوكت نەم قىقىت. 1. ئارجا NAT.

عەنم no-proxy-arp ئەسپاسلا ئەملىكىللى اھىف نەكمىتالاچكانە، NAT نېوكتب قىلۇتىي امىيەت قىباسلى كۈلسىلا:

```
<#root>
firepower#
show run nat
nat (INSIDE,OUTSIDE) source static NET_1.1.1.0 NET_2.2.2.0 destination static NET_192.168.0.0 NET_4.4.4
no-proxy-arp
```

ئەپەپلىقلىتى رادىج ئەھىللى لېكۈلل ARP ئەفيظولى طەمعت. 2. ئارجا.

ئەھىللى لېكۈلل ARP لېطەمعت لواحف، ئەلکىشىملا "no-proxy-arp" ئەسپاسلا ئەملىكىلا لەخت مەل اذىدا ئەپەپلىقلىتى FlexConfig مادختسا ئەباتكىلا هذه تىقۇيىف كىلىع بەجي، دوجو ئەللاج يىف. اەسفن ئەھىللى (بىسانملا ئەھىللى مىسادىيەت) رەمألا رىشنى و.

```
sysopt noproxyarp INSIDE
```

روهظ يف ببستت يتلا SNMP (OIDs) نئاك تافرعم ىلع فرعتلار 13. ٖ لاحلـا ٖ ئـيـزـكـرـمـلـا ٖ ئـجـلـاعـمـلـا ٖ ئـدـحـوـعـاطـخـأـ

اهنأ ىلع ٖ رـكـاـذـلـاـ نـمـ قـقـحـتـلـاـ ئـيـلـمـعـلـاـ SNMPـ تـافـرـعـمـ ضـعـبـ دـيـدـحـتـ ئـيـفـيـكـ ٖ لـاحـلـاـ هـذـهـ حـضـوتـ تـاعـوـمـجـ لـيـلـحـتـ ىـلـاـ اـدـانـتـسـاـ (ـعـادـأـلـاـ رـادـصـاـ)ـ ئـيـزـكـرـمـلـاـ ئـجـلـاعـمـلـاـ ئـدـحـوـعـاطـخـأـلـ يـسـيـئـرـلـاـ بـبـسـلـاـ 3ـ رـادـصـإـلـاـ SNMPv3ـ).

ثـاحـبـأـ تـفـشـكـ اـمـكـ .ـرـمـتـسـمـ لـكـشـبـ تـاـنـاـيـبـلـاـ تـاـهـجـاـوـىـلـعـ تـاـزـوـاجـتـلـاـ ئـدـايـزـ :ـلـكـشـمـلـاـ فـصـوـ بـبـسـلـاـ دـعـتـ يـتـلـاـ SNMPـ (ـئـيـلـمـعـ نـعـ ئـمـجـاـنـلـاـ)ـ ئـيـزـكـرـمـلـاـ ئـجـلـاعـمـلـاـ ئـدـحـوـعـاطـخـأـضـيـأـ دـوـجـوـنـعـ ئـرـخـأـ .ـهـجـاـوـلـاـ تـاـزـوـاجـتـلـ يـسـيـئـرـلـاـ

يرـذـجـلـاـ بـبـسـلـاـ دـيـدـحـتـ يـهـ اـهـحـالـصـ اوـ ئـاطـخـأـلـاـ فـاشـكـتـسـأـ ئـيـلـمـعـ يـفـ ئـلـاتـلـاـ ئـوـطـخـلـاـ تـنـاـكـ هـجـوـىـلـعـوـ،ـ ئـيـلـمـعـ اـهـيـفـ بـبـسـتـتـ يـتـلـاـ (ـC~PU~)ـ ئـيـزـكـرـمـلـاـ ئـجـلـاعـمـلـاـ ئـدـحـوـعـاطـخـأـ جـتـنـيـ نـأـ نـكـمـيـ يـتـلـاـ SNMPـ (ـO~ID~)ـ ئـيـلـمـعـ اـهـيـفـ بـبـسـتـتـ يـتـلـاـ (ـC~PU~)ـ ئـيـزـكـرـمـلـاـ ئـجـلـاعـمـلـاـ ئـدـحـوـعـاطـخـأـ،ـ صـوـصـخـلـاـ .ـهـجـاـوـلـاـ تـاـزـوـاجـتـلـ يـسـيـئـرـلـاـ

تقـولـاـ يـفـ هـحـيـقـلـتـ مـتـيـ يـذـلـاـ SNMP~OIDsـ فـرـعـمـلـ "show~FTD~LINA"ـ كـرـمـ رـفـوـيـ الـ،ـ ايـلـاحـ يـلـعـفـلـاـ

هـذـهـ يـفـ،ـ كـلـذـعـمـوـ،ـ ئـبـقـارـمـ ئـادـأـ نـمـ عـارـتـقـالـابـ ئـصـاخـلـاـ SNMP~OIDsـ ئـمـئـاـقـ دـادـرـتـسـاـ نـكـمـيـ :ـهـيـئـاـقـوـلـاـ لـمـاـعـلـاـ هـذـهـ كـانـهـ تـنـاـكـ،ـ ٖ لـاحـلـاـ

- ئـلـعـ ئـيـصـوـصـخـلـلـ تـاـنـاـيـبـلـاـ رـيـفـشـتـوـ ئـقـدـاصـمـلـاـ عـمـ SNMP~OIDsـ نـمـ 3ـ رـادـصـإـلـاـ نـيـوـكـتـ مـتـ FTD

رسـأـ لـيـلـحـتـ

،ـتـاـنـاـيـبـلـاـ رـيـفـشـتـوـ 3ـ رـادـصـإـلـاـ SNMPـ ئـقـدـاصـمـلـاـ دـامـتـعـاـ تـاـنـاـيـبـ 5ـ يـدـلـ نـاـكـ FTDـ لـوـفـسـمـ نـأـ اـمـبـ ،ـهـذـهـ لـمـعـلـاـ ئـطـخـ حـارـتـقـاـ مـتـ:

1. ئـمـزـحـ طـاقـتـلـاـ SNMP
2. دـيـدـحـتـلـ Wiresharkـ بـ صـاخـلـاـ Lـوـكـوـتـورـبـ تـالـيـضـفـتـ مـدـخـتـسـ اوـ طـاقـتـلـالـاـ ظـفـحـاـ
3. رـادـصـإـلـاـ SNMPـ مـزـحـ رـيـفـشـتـ كـفـلـ SNMP~OIDsـ نـمـ 3ـ رـادـصـإـلـاـ دـامـتـعـاـ تـاـنـاـيـبـ مـادـخـتـسـاـ مـتـيـ .ـهـجـاـوـلـاـ تـاـفـرـعـمـ لـيـلـحـتـلـ اـهـرـيـفـشـتـ كـفـ مـتـ يـتـلـاـ طـاقـتـلـالـاـ تـايـلـمـعـ اـعـاجـرـتـسـ اوـ ئـيـدـامـلـاـ

مـداـخـ فـيـضـمـ نـيـوـكـتـ يـفـ اـهـمـادـخـتـسـاـ مـتـيـ يـتـلـاـ ئـهـجـاـوـلـاـ ىـلـعـ SNMPـ مـزـحـ طـاقـتـلـاـ نـيـوـكـتـ snmp:

```
<#root>
firepower#
show run snmp-server | include host
snmp-server host management 192.168.10.10 version 3 netmonv3

firepower#
show ip address management
```

```

System IP Address:
Interface Name IP address Subnet mask Method
Management0/0 management 192.168.5.254 255.255.255.0 CONFIG

Current IP Address:
Interface Name IP address Subnet mask Method
Management0/0 management 192.168.5.254 255.255.255.0 CONFIG

firepower# capture capsntp interface management buffer 10000000 match udp host 192.168.10.10 host 192.168.5.254 eq snmp

firepower# show capture capsntp

capture capsntp type raw-data buffer 10000000 interface outside [Capturing - 9512 bytes]
match udp host 192.168.10.10 host 192.168.5.254 eq snmp

```

No.	Time	Protocol	Source	Source Port	Destination Port	Destination	Length	Info
1	0.000	SNMP	192.168.10.10	65484	161	192.168.5.254	100	getBulkRequest
2	0.000	SNMP	192.168.5.254	161	65484	192.168.10.10	167	report 1.3.6.1.6.3.15.1.1.4.0
3	0.176	SNMP	192.168.10.10	65484	161	192.168.5.254	197	② encryptedPDU: privKey Unknown
4	0.176	SNMP	192.168.5.254	161	65484	192.168.10.10	192	report 1.3.6.1.6.3.15.1.1.2.0
5	0.325	SNMP	192.168.10.10	65484	161	192.168.5.254	199	encryptedPDU: privKey Unknown
6	0.326	SNMP	192.168.5.254	161	65484	192.168.10.10	678	encryptedPDU: privKey Unknown
7	0.490	SNMP	192.168.10.10	65484	161	192.168.5.254	205	encryptedPDU: privKey Unknown
8	0.490	SNMP	192.168.5.254	161	65484	192.168.10.10	568	encryptedPDU: privKey Unknown
9	0.675	SNMP	192.168.10.10	65484	161	192.168.5.254	205	encryptedPDU: privKey Unknown
10	0.767	SNMP	192.168.5.254	161	65484	192.168.10.10	610	encryptedPDU: privKey Unknown
11	0.945	SNMP	192.168.10.10	65484	161	192.168.5.254	205	encryptedPDU: privKey Unknown
12	0.946	SNMP	192.168.5.254	161	65484	192.168.10.10	584	encryptedPDU: privKey Unknown
13	1.133	SNMP	192.168.10.10	65484	161	192.168.5.254	205	encryptedPDU: privKey Unknown
14	1.134	SNMP	192.168.5.254	161	65484	192.168.10.10	588	encryptedPDU: privKey Unknown
15	1.317	SNMP	192.168.10.10	65484	161	192.168.5.254	205	encryptedPDU: privKey Unknown
16	1.318	SNMP	192.168.5.254	161	65484	192.168.10.10	513	encryptedPDU: privKey Unknown
17	17.595	SNMP	192.168.10.10	62008	161	192.168.5.254	180	getBulkRequest
18	17.595	SNMP	192.168.5.254	161	62008	192.168.10.10	167	report 1.3.6.1.6.3.15.1.1.4.0
19	17.749	SNMP	192.168.10.10	62008	161	192.168.5.254	197	encryptedPDU: privKey Unknown
20	17.749	SNMP	192.168.5.254	161	62008	192.168.10.10	192	report 1.3.6.1.6.3.15.1.1.2.0
21	17.898	SNMP	192.168.10.10	62008	161	192.168.5.254	199	encryptedPDU: privKey Unknown
22	17.899	SNMP	192.168.5.254	161	62008	192.168.10.10	678	encryptedPDU: privKey Unknown
23	18.094	SNMP	192.168.10.10	62008	161	192.168.5.254	205	encryptedPDU: privKey Unknown
24	18.094	SNMP	192.168.5.254	161	62008	192.168.10.10	568	encryptedPDU: privKey Unknown
25	18.290	SNMP	192.168.10.10	62008	161	192.168.5.254	205	encryptedPDU: privKey Unknown

< [Destination Host: 192.168.5.254]
< [Source or Destination Host: 192.168.5.254]>
> User Datagram Protocol, Src Port: 65484, Dst Port: 161
 Simple Network Management Protocol
 msgVersion: snmpv3 (3)
> msgGlobalData
> msgAuthoritativeEngineID: 80000009fe1c6dad4930a00ef1fec2301621a4158bf1cf40...
msgAuthoritativeEngineBoots: 0
msgAuthoritativeEngineTime: 0
msgUserName: netmonv3
msgAuthenticationParameters: ff5176f5973c30b62ffcc11b8
msgPrivacyParameters: 000040e100003196
 msgData: encryptedPDU (1)
③ encryptedPDU: 879a16d23633400a0391c5280d226e0cec844d87101ba703...

يسيئرلا طاقنل:

1. جول او SNMP ردهم نیوانع/ذفانم.
2. ل فورع م ریغ privKey ل وکوت ورب تان ایب ڈھو زیمرت کف رذعت.
3. ڈیل والا EncryptedPDU ڈھمیق.

اہب یصومل ا تاءراج إالا

ۃلس مل ا هذہ قاطن قییضت ڈدایز وہ عرف ل ا اذہ ف ڈراول ا تاءراج إالا نم ضرغل او.

طاقتل ا ریفشت کف 1. عاج إالا SNMP.

دامتغا تان ايپ دي دحـلـا Wireshark بـ صـاخـلـا لـوكـوتـورـبـ تـالـيـضـفـتـ وـرـحـ وـ طـاقـتـلـا ظـفـحـاـ مـزـحـلـاـ رـيـفـشـتـ كـفـلـاـ سـنـمـ نـمـ 3ـ رـادـصـ إـلـاـ.

<#root>

firepower#

copy /pcap capture: tftp:

Source capture name [capsnmp]?

Address or name of remote host []? 192.168.10.253

Destination filename [capsnmp]? capsnmp.pcap

!!!!!!

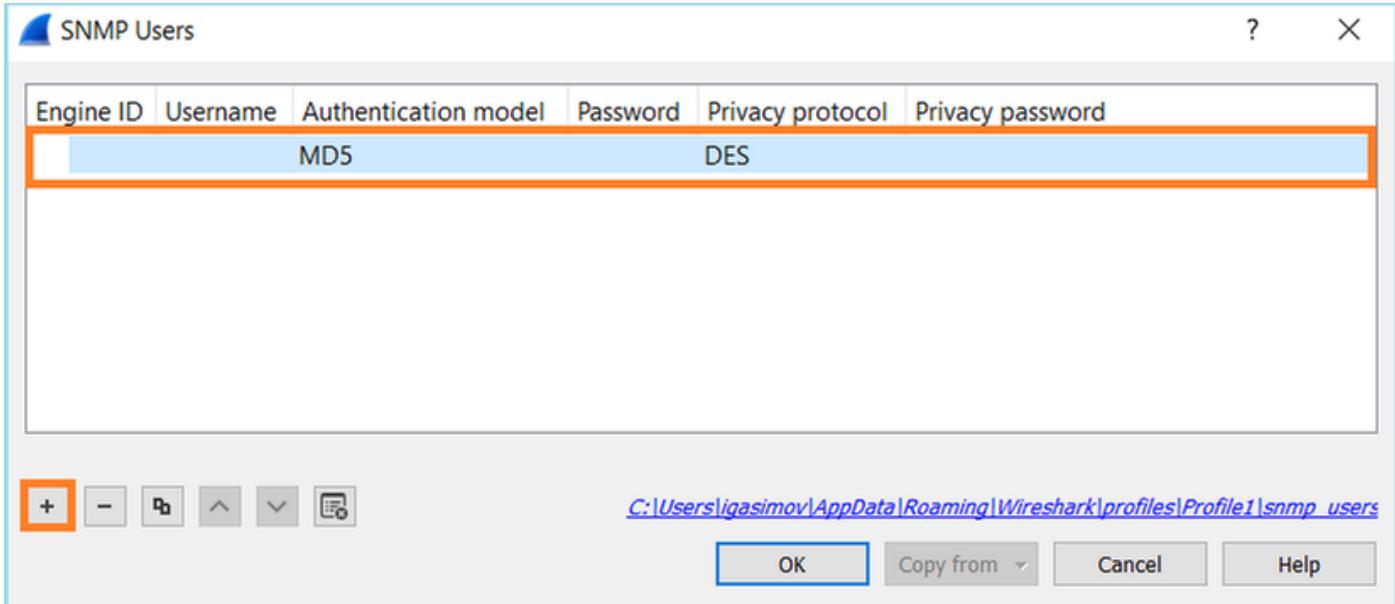
64 packets copied in 0.40 secs

> لـوكـوتـورـبـ لـاـ تـالـيـضـفـتـ ئـلـاـ حـفـصـتـ وـ سـنـمـ ئـلـعـ طـاقـتـلـاـ فـلـمـ حـتـفـاـ رـوـصـلـاـ يـفـ حـضـوـمـ وـهـ اـمـكـ ،ـنـيـمـدـخـتـسـمـلـاـ لـوـجـ

No.	Time	Protocol	Source	Source Port	Destination Port	Destination	Length	Info
1	0.000	SNMP	192.168.10.10	65484	161	192.168.5.254	100	getBulkRequest report 1.3.6.1.6.3.15.1.1.4.0
2	0.000	SNMP	192.168.5.254	161	65484	192.168.10.10	167	encryptedPDU: privKey Unknown report 1.3.6.1.6.3.15.1.1.2.0
3	0.176	SNMP	192.168.10.10	65484				Mark/Unmark Packet Ctrl+M Ignore/Unignore Packet Ctrl+D Set/Unset Time Reference Ctrl+T Time Shift... Ctrl+Shift+T Packet Comment... Ctrl+Alt+C
4	0.176	SNMP	192.168.5.254	161				Edit Resolved Name
5	0.325	SNMP	192.168.10.10	65484				Apply as Filter Prepare a Filter Conversation Filter Colorize Conversation SCTP Follow Copy
6	0.326	SNMP	192.168.5.254	161				Protocol Preferences
7	0.490	SNMP	192.168.10.10	65484				Open Simple Network Management Protocol preferences...
8	0.490	SNMP	192.168.5.254	161				Decode As...
9	0.675	SNMP	192.168.10.10	65484				Show SNMP OID in info column
10	0.767	SNMP	192.168.5.254	161				Reassemble SNMP-over-TCP messages spanning multiple TCP segments
11	0.945	SNMP	192.168.10.10	65484				Display dissected variables inside SNMP tree
12	0.946	SNMP	192.168.5.254	161				Users Table...
13	1.133	SNMP	192.168.10.10	65484				Enterprise Specific Trap Types...
14	1.134	SNMP	192.168.5.254	161				SNMP UDP port: 161...
15	1.317	SNMP	192.168.10.10	65484				SNMP TCP port: 161...
16	1.318	SNMP	192.168.5.254	161				Disable SNMP...
17	17.595	SNMP	192.168.10.10	62008				
18	17.595	SNMP	192.168.5.254	161				
19	17.749	SNMP	192.168.10.10	62008				
20	17.749	SNMP	192.168.5.254	161				
21	17.898	SNMP	192.168.10.10	62008				
22	17.899	SNMP	192.168.5.254	161				
23	18.094	SNMP	192.168.10.10	62008	161	192.168.5.254	205	
24	18.094	SNMP	192.168.5.254	161	62008	192.168.10.10	560	
25	18.290	SNMP	192.168.10.10	62008	161	192.168.5.254	205	

< [Destination Host: 192.168.5.254]>
< [Source or Destination Host: 192.168.5.254]>
> User Datagram Protocol, Src Port: 65484, Dst Port: 161
Simple Network Management Protocol
msgVersion: snmpv3 (3)
> msgGlobalData

وقـدـاصـمـلـاـ جـذـومـنـ وـ سـنـمـ نـمـ 3ـ رـادـصـإـلـاـ مـدـخـتـسـمـ مـسـاـ دـيـدـحـتـ مـتـ،ـ سـنـمـ يـمـدـخـتـسـمـ لـوـجـ يـفـ تـانـايـبـ ضـرـعـ مـتـيـ الـ (ـيـصـوصـخـلـاـ رـوـمـ ـمـلـكـ وـ ـيـصـوصـخـلـاـ لـوـكـوتـورـبـ وـ ـقـدـاصـمـلـاـ رـوـمـ ـمـلـكـ وـ (ـهـانـدـأـ ـيـلـعـفـلـاـ دـامـتـعـالـاـ):ـ



لوكوتورب تان اي ب تادحو ضرعب SNMP ماق، يم دختسنم تادادع اقيب طت درجمب SNMP (PDU) اهري فشت كف مت يتلا:

No.	Time	Protocol	Source	Source Port	Destination Port	Destination	Length	Info
1	0.000	SNMP	192.168.10.10	65484	161	192.168.5.254	100	1 getBulkRequest
2	0.000	SNMP	192.168.5.254	161	65484	192.168.10.10	167	report 1.3.6.1.6.3.15.1.1.4.0
3	0.176	SNMP	192.168.10.10	65484	161	192.168.5.254	197	getBulkRequest 1.3.6.1.4.1.9.9.221.1
4	0.176	SNMP	192.168.5.254	161	65484	192.168.10.10	192	report 1.3.6.1.6.3.15.1.1.2.0
5	0.325	SNMP	192.168.10.10	65484	161	192.168.5.254	199	1 getBulkRequest 1.3.6.1.4.1.9.9.221.1
6	0.326	SNMP	192.168.5.254	161	65484	192.168.10.10	678	get-response 1.3.6.1.4.1.9.9.221.1.1.1.1.2.1.1 1.3.6.1.4.1.9.9.221.1.1.1.2.1.2 1.3.6.1.4.1.9.9.221.1.1
7	0.490	SNMP	192.168.10.10	65484	161	192.168.5.254	205	1 getBulkRequest 1.3.6.1.4.1.9.9.221.1.1.1.1.3.1.8
8	0.490	SNMP	192.168.5.254	161	65484	192.168.10.10	566	2 get-response 1.3.6.1.4.1.9.9.221.1.1.1.5.1.1 1.3.6.1.4.1.9.9.221.1.1.1.5.1.2 1.3.6.1.4.1.9.9.221.1.1
9	0.675	SNMP	192.168.10.10	65484	161	192.168.5.254	205	1 getBulkRequest 1.3.6.1.4.1.9.9.221.1.1.1.6.1.8
10	0.767	SNMP	192.168.5.254	161	65484	192.168.10.10	610	2 get-response 1.3.6.1.4.1.9.9.221.1.1.1.7.1.1 1.3.6.1.4.1.9.9.221.1.1.1.7.1.2 1.3.6.1.4.1.9.9.221.1.1
11	0.945	SNMP	192.168.10.10	65484	161	192.168.5.254	205	1 getBulkRequest 1.3.6.1.4.1.9.9.221.1.1.1.8.1.8
12	0.946	SNMP	192.168.5.254	161	65484	192.168.10.10	584	2 get-response 1.3.6.1.4.1.9.9.221.1.1.1.17.1.1 1.3.6.1.4.1.9.9.221.1.1.1.17.1.2 1.3.6.1.4.1.9.9.221.1.1
13	1.133	SNMP	192.168.10.10	65484	161	192.168.5.254	205	1 getBulkRequest 1.3.6.1.4.1.9.9.221.1.1.1.1.18.1.8
14	1.134	SNMP	192.168.5.254	161	65484	192.168.10.10	588	get-response 1.3.6.1.4.1.9.9.221.1.1.1.1.19.1.1 1.3.6.1.4.1.9.9.221.1.1.1.19.1.2 1.3.6.1.4.1.9.9.221.1.1
15	1.317	SNMP	192.168.10.10	65484	161	192.168.5.254	205	1 getBulkRequest 1.3.6.1.4.1.9.9.221.1.1.1.20.1.8
16	1.318	SNMP	192.168.5.254	161	65484	192.168.10.10	513	2 get-response 1.3.6.1.4.1.9.9.392.1.1.1.0 1.3.6.1.4.1.9.9.392.1.1.2.0 1.3.6.1.4.1.9.9.392.1.1.3.0 1.3.6.1.4.1.9.9.221.1.1
17	17.595	SNMP	192.168.10.10	62008	161	192.168.5.254	100	getBulkRequest
18	17.595	SNMP	192.168.5.254	161	62008	192.168.10.10	167	report 1.3.6.1.6.3.15.1.1.4.0
19	17.749	SNMP	192.168.10.10	62008	161	192.168.5.254	197	1 getBulkRequest 1.3.6.1.4.1.9.9.221.1
20	17.749	SNMP	192.168.5.254	161	62008	192.168.10.10	192	report 1.3.6.1.6.3.15.1.1.2.0
21	17.898	SNMP	192.168.10.10	62008	161	192.168.5.254	199	1 getBulkRequest 1.3.6.1.4.1.9.9.221.1
22	17.899	SNMP	192.168.5.254	161	62008	192.168.10.10	678	2 get-response 1.3.6.1.4.1.9.9.221.1.1.1.2.1.1 1.3.6.1.4.1.9.9.221.1.1.1.2.1.2 1.3.6.1.4.1.9.9.221.1.1
23	18.094	SNMP	192.168.10.10	62008	161	192.168.5.254	205	getBulkRequest 1.3.6.1.4.1.9.9.221.1.1.1.3.1.8
24	18.094	SNMP	192.168.5.254	161	62008	192.168.10.10	560	get-response 1.3.6.1.4.1.9.9.221.1.1.1.5.1.2 1.3.6.1.4.1.9.9.221.1.1.1.6.1.8
25	18.290	SNMP	192.168.10.10	62008	161	192.168.5.254	205	getBulkRequest 1.3.6.1.4.1.9.9.221.1.1.1.6.1.8

يسيز لارلا طاقنلا:

1. SNMP GetBulkRequest تادادع OID رباع لقنتلا او مالعتسالل ظلما تاذ OID 1.3.6.1.4.1.9.9.221.1 تافرع معنى.
2. SNMP GetBulkRequest مع get-response يذلا FTD باجتسا 1.3.6.1.4.1.9.9.221.1.

SNMP OIDس اتافرع معنى فرعتلا 2. عارجي.

(MIB) ةرادالا تامولعم ةدعاق لارلا يمتنى OID 1.3.6.1.4.1.9.9.221.1 نا SNMP نياك حفصتم رهظا: Cisco-Enhanced-MEMPOOL-MIB، امك حضوم وه يف روصلا.

SNMP Object Navigator

HOME
SUPPORT
TOOLS & RESOURCES
SNMP Object Navigator

TRANSLATE/BROWSE **SEARCH** **DOWNLOAD MIBS** **MIB SUPPORT - SW**

[Help](#) | [Feedback](#)

Translate | [Browse The Object Tree](#)

Related Tools
[Support Case Manager](#)
[Cisco Community](#)
[MIB Locator](#)

Translate OID into object name or object name into OID to receive object details

Enter OID or object name: **1.3.6.1.4.1.9.9.221.1** examples -
 OID: 1.3.6.1.4.1.9.9.27
Object Name: ifIndex

Object Information

Specific Object Information

Object	cempMIBObjects
OID	1.3.6.1.4.1.9.9.221.1
MIB	CISCO-ENHANCED-MEMPOOL-MIB - View Supporting Images

OID Tree

You are currently viewing your object with **2** levels of hierarchy above your object.

```
.iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9)
|   |
-- ciscoMgmt(9)
|   |
+- ciscoTcpMIB(6)
```

يـف نـاسـنـاـلـاـ لـبـقـ نـمـ هـتـعـارـقـ نـكـمـيـ قـيـسـنـتـبـ OIDsـ ضـرـعـلـ

وهـ اـمـكـ ،ـاهـتـاـيـعـبـتـوـ وـهـ Cisco-Enhanced-Mempool-MIBـ نـمـ (ـMIBـ)ـ ةـرـادـاـلـاـ تـامـوـلـعـمـ ـدـعـاـقـ لـيـزـنـتـ .ـ

ـرـوـصـلـاـ يـفـ حـضـوـمـ :

SNMP Object Navigator

HOME
SUPPORT
TOOLS & RESOURCES
SNMP Object Navigator

TRANSLATE/BROWSE **SEARCH** **DOWNLOAD MIBS** **MIB SUPPORT - SW**

[Help](#) | [Feedback](#)

Related Tools
[Support Case Manager](#)
[Cisco Community](#)
[MIB Locator](#)

View MIB dependencies and download MIB or view MIB contents

Step 1: Select a MIB name by typing or scrolling and then select a function in step 2 and click Submit
CISCO-ENHANCED-MEMPOOL-MIB

A100-R1-MIB
ACCOUNTING-CONTROL-MIB
ACTONA-ACTASTOR-MIB
ADMIN-AUTH-STATS-MIB
ADSL-DMT-LINE-MIB
ADSL-LINE-MIB
ADSL-TC-MIB
ADSL2-LINE-MIB

Step 2: Select a function:

View MIB dependencies and download MIB
 View MIB contents

SNMP Object Navigator

HOME

SUPPORT

TOOLS & RESOURCES

SNMP Object Navigator

TRANSLATE/BROWSE

SEARCH

DOWNLOAD MIBS

MIB SUPPORT - SW

Help | Feedback

Related Tools

[Support Case Manager](#)[Cisco Community](#)[MIB Locator](#)

CISCO-ENHANCED-MEMPOOL-MIB

View compiling dependencies for other MIBs by [clearing](#) the page and selecting another MIB.

Compile the MIB

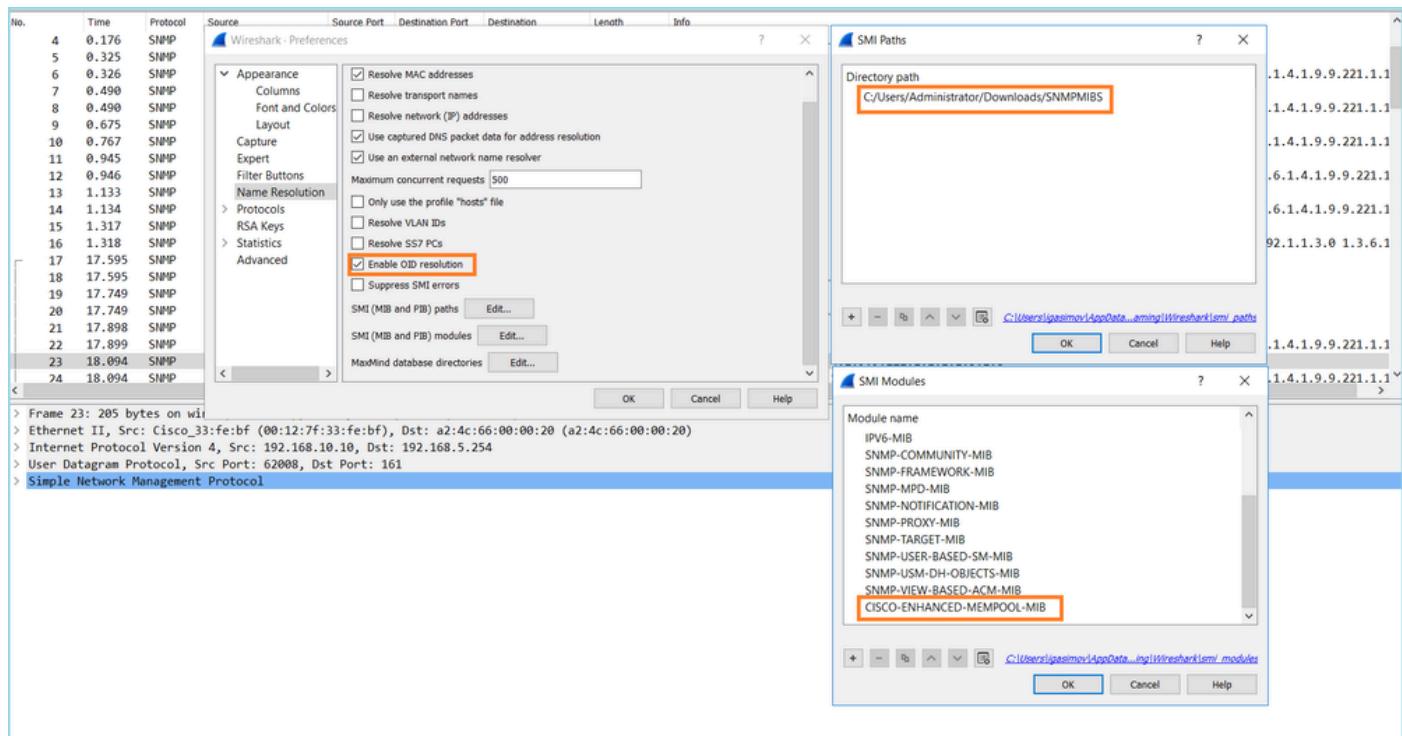
Before you can compile CISCO-ENHANCED-MEMPOOL-MIB, you need to compile the MIBs listed below in the order listed.

Download all of these MIBs (Warning: does not include non-Cisco MIBs) or view details about each MIB below.

If you are using Internet Explorer click [here](#).

MIB Name	Version 1	Version 2	Dependencies
1. SNMPv2-SMI	Download	Download	View
2. SNMPv2-TC	Download	Download	Dependencies
3. SNMPv2-CONF	Not Required	Download	View
4. SNMP-FRAMEWORK-MIB	Download	Download	Dependencies
5. CISCO-SMI	Download	Download	View
6. ENTITY-MIB	Download	Download	Dependencies
7. HCNUM-TC	Download	Download	View
8. RFC1155-SMI	Non-Cisco MIB	Non-Cisco MIB	-
9. RFC-1212	Non-Cisco MIB	Non-Cisco MIB	-
10. RFC-1215	Non-Cisco MIB	Non-Cisco MIB	-
11. SNMPv2-TC-v1	Non-Cisco MIB	Non-Cisco MIB	-
12. CISCO-ENHANCED-MEMPOOL-MIB	Download	Download	View

2. ڈفان (مسالہ لیلحت) If (ریحہت) Edit > Preferences > Name Resolution مادختساب دلجملا راطلا ددھی (PIB و MIB تاراسم) SMI یف. اهديدھت متي OID ڈقدنیکمت ڈفاضاً مٿت SMI و تادھو MIB و PIB). ڈرادإلا تامولعم دعاعو Cisco-Enhanced-Mempool-MIB یطمنلا تادھول اؤمیاًق یلا ایئاقلت:



3. ڈقد طیشنت متي OID لیغشت ڈاعی درجمب:

No.	Time	Protocol	Source	Source Port	Destination Port	Destination	Length	Info
1	0.000	SNMP	192.168.10.10	65484	161	192.168.5.254	100	getBulkRequest report SNMP-USER-BASED-SM-MIB::usmStatsUnknownEngineIDs.0
2	0.000	SNMP	192.168.5.254	161	65484	192.168.10.10	167	getBulkRequest CISCO-ENHANCED-MEMPOLL-MIB::cempMI80Objects
3	0.176	SNMP	192.168.10.10	65484	161	192.168.5.254	197	report SNMP-USER-BASED-SM-MIB::usmStatsNotInTimeWindows.0
4	0.176	SNMP	192.168.5.254	161	65484	192.168.10.10	192	getBulkRequest CISCO-ENHANCED-MEMPOLL-MIB::cempMI80Objects
5	0.325	SNMP	192.168.10.10	65484	161	192.168.5.254	199	getBulkRequest CISCO-ENHANCED-MEMPOLL-MIB::cempMI80Objects
6	0.326	SNMP	192.168.5.254	161	65484	192.168.10.10	678	get-response CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolType.1.1 CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolType
7	0.490	SNMP	192.168.10.10	65484	161	192.168.5.254	205	getBulkRequest CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.8
8	0.490	SNMP	192.168.5.254	161	65484	192.168.10.10	560	get-response CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolAlternate.1.1 CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoc
9	0.675	SNMP	192.168.10.10	65484	161	192.168.5.254	205	getBulkRequest CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolValid.1.8
10	0.767	SNMP	192.168.5.254	161	65484	192.168.10.10	610	get-response CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolUsed.1.1 CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolUsed
11	0.945	SNMP	192.168.10.10	65484	161	192.168.5.254	205	getBulkRequest CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolFree.1.8
12	0.946	SNMP	192.168.5.254	161	65484	192.168.10.10	584	get-response CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolUsedOverFlw.1.1 CISCO-ENHANCED-MEMPOLL-MIB::cempMemP
13	1.133	SNMP	192.168.10.10	65484	161	192.168.5.254	205	getBulkRequest CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolUsedOverFlw.1.8
14	1.134	SMD	192.168.5.254	161	65494	192.168.10.10	599	get-response CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolUsedOverFlw.1.1 CISCO-ENHANCED-MEMPOLL-MIB::cempMemPo

```

▼ CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.1 (1.3.6.1.4.1.9.9.221.1.1.1.3.1.1): System memory
Object Name: 1.3.6.1.4.1.9.9.221.1.1.1.3.1.1 (CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.1)
CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName: System memory
▼ CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.2 (1.3.6.1.4.1.9.9.221.1.1.1.3.1.2): System memory
Object Name: 1.3.6.1.4.1.9.9.221.1.1.1.3.1.2 (CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.2)
CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName: System memory
▼ CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.3 (1.3.6.1.4.1.9.9.221.1.1.1.3.1.3): MEMPOOL_MSGLYR
Object Name: 1.3.6.1.4.1.9.9.221.1.1.1.3.1.3 (CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.3)
CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName: MEMPOOL_MSGLYR
▼ CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.4 (1.3.6.1.4.1.9.9.221.1.1.1.3.1.4): MEMPOOL HEAPCACHE_1
Object Name: 1.3.6.1.4.1.9.9.221.1.1.1.3.1.4 (CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.4)
CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName: MEMPOOL_HEAPCACHE_1
▼ CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.5 (1.3.6.1.4.1.9.9.221.1.1.1.3.1.5): MEMPOOL HEAPCACHE_0
Object Name: 1.3.6.1.4.1.9.9.221.1.1.1.3.1.5 (CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.5)
CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName: MEMPOOL_HEAPCACHE_0
▼ CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.6 (1.3.6.1.4.1.9.9.221.1.1.1.3.1.6): MEMPOOL_DMA_ALT1
Object Name: 1.3.6.1.4.1.9.9.221.1.1.1.3.1.6 (CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.6)
CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName: MEMPOOL_DMA_ALT1
▼ CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.7 (1.3.6.1.4.1.9.9.221.1.1.1.3.1.7): MEMPOOL_DMA
Object Name: 1.3.6.1.4.1.9.9.221.1.1.1.3.1.7 (CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.7)
CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName: MEMPOOL_DMA
▼ CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.8 (1.3.6.1.4.1.9.9.221.1.1.1.3.1.8): MEMPOOL_GLOBAL_SHARED
Object Name: 1.3.6.1.4.1.9.9.221.1.1.1.3.1.8 (CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName.1.8)
CISCO-ENHANCED-MEMPOLL-MIB::cempMemPoolName: MEMPOOL_GLOBAL_SHARED

```

موقت ظبقارم ةادأ تناك ، طاقتل الا فلمل هريفشت كف مت يذلا جارخ الا ئلا ادانتسا وه امك FTD . ىلع ئركاذلا تابع مجت مادختس ا تانايىب صحفب (ناو١٠ لصاف) يرود لكشـب حـسـمـوـ، [قـركـاذـلـابـ ئـقـلـعـتـمـلـاـ تـاـيـىـاـصـحـالـلـ](#) [ASA SNMP عـارـتـقاـنـافـ TechNote](#) ئـلـاقـمـ يـفـ حـضـوـمـ ـةـدـحـوـمـادـخـتـسـاـ هـنـعـ جـتـنـيـ SNMP مـادـخـتـسـاـبـ (GSP) يـمـلـاعـلـاـ كـرـتـشـمـلـاـ عـمـجـتـلـاـ مـادـخـتـسـاـ حـضـاـولـاـ نـمـ نـاـكـ، (طـاقـتـلـاـ) Capture نـمـ ئـلـاحـلـاـ هـذـهـ يـفـ . رـيـبـكـ لـكـشـبـ (CPU) ئـيـزـكـرـمـلـاـ ئـقـلـاعـمـلـاـ ئـلـوكـوتـرـبـ ئـرـجـعـتـسـاـ مـادـخـتـسـاـ GetBulkRequest لـيـلـوـأـلـاـ SNMP.

تمت ، ئـيـلـمـ اـهـيـفـ بـبـسـتـ يـتـلـاـ (CPU) ئـيـزـكـرـمـلـاـ ئـقـلـاعـمـلـاـ ئـدـحـوـ ئـاطـخـأـ لـيـلـقـتـ لـجـأـ نـمـ لـوـكـوتـرـبـ ئـلـوكـوتـرـبـ ئـيـزـكـرـمـلـاـ ئـقـلـاعـمـلـاـ ئـدـحـوـ ئـاطـخـأـ فـيـ فـيـخـتـلـاـ تـاوـطـخـ عـابـتـابـ ئـيـصـوـتـلـاـ نـوـدـبـ GSP . مـاظـنـبـ ئـطـبـتـرـمـلـاـ ئـعـالـمـعـلـاـ تـافـرـعـمـ عـالـطـتـسـاـ بـنـجـتـوـ ئـلـاقـمـلـاـ يـفـ اـهـيـلـاـ رـاشـمـلـاـ مـتـيـ مـلـ GSP ، رـايـعـمـبـ طـبـتـرـمـلـاـ (OIDs) درـومـلـاـ ئـقـيـفـ فـرـعـمـلـاـ لـوـكـوتـرـبـ ئـرـجـعـمـ بـ رـبـ بـ رـبـ عـالـطـتـسـاـ ضـفـخـنـاـ اـمـكـ ، لـوـكـوتـرـبـ ئـرـجـعـمـ بـ ئـلـوكـوتـرـبـ ئـيـلـمـ عـنـ ئـجـتـانـلـاـ ئـيـزـكـرـمـلـاـ ئـقـلـاعـمـلـاـ ئـدـحـوـلـ ئـاطـخـأـ ئـيـأـ ئـظـحـالـمـ ئـظـوحـلـمـ لـكـشـبـ زـواـجـتـلـاـ لـدـعـمـ.

ةـلـصـتـاـذـ تـامـوـلـعـمـ

- [ةـكـرـشـلـ عـبـاتـلـاـ Cisco FireSIGHT](#)
- [جـمـانـرـبـ ئـلـاـ لـوـصـوـلـاـ يـفـ مـكـحـتـلـاـ قـسـاـيـسـ دـعـاوـقـ تـاءـعـاـجـ حـيـضـوـتـ](#)
- [مـنـجـلـاـعـبـتـتـوـ FirePOWER دـيـدـهـتـ دـضـ عـافـدـلـاـ تـاءـعـوـمـجـمـعـمـ لـمـعـلـاـ](#)
- [Wireshark مـلـعـتـ](#)

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).