

ةيامح رادج) Firepower Firewall تاطقل ليلحت ةكبشلا تالكشم فاشكتسال (Firepower) لأعف لكشب اهالصلإو

تايوتحملإ

[ةمدقملا](#)

[ةيساسألا تابلطتلا](#)

[تابلطتلا](#)

[ةمدختسملاتانوكملا](#)

[ةيساسأ تامولعم](#)

[يلاتلا ليلحلا نم ةيامحلا رادج تاجت نم ةومجم يلعل روص ةيمجت كنكمي فيك
؟اهريصت و \(NGFW\)](#)

[FXOS طاققلا ةيمجت](#)

[FTD Lina طاققلا تايلمع ةيمجت ونيمجت](#)

[FTD ليلحو تاطقل ةيمجت ونيمجت](#)

[اهالصلإو عاقلألا فاشكتسال](#)

[جرخم ةوجاو يلعل TCP SYN دجوي ال 1. ةلاجلإ](#)

[رسل ليلحت](#)

[اهب يصوملا تاعارجلإ](#)

[اهب يصوملا تاعارجلإو ةلمتحملا بابسألا صلخم](#)

[مداخلإ نم TCP RST ليلعملإ نم TCP SYN 2. ةلاجلإ](#)

[رسل ليلحت](#)

[اهب يصوملا تاعارجلإ](#)

[ةدجاو ةياهن ةطقن نم TCP 3-way + RST ةحفاصم 3. ةلاجلإ](#)

[رسل ليلحت](#)

[ليلعملإ نم ةلجفملا TCP 3-way + RST ةحفاصم - 3.1](#)

[اهب يصوملا تاعارجلإ](#)

[RST + ليلعملإ نم ةلجفملا سدكملال ةفن عزلإ TCP ل هاجتاللا ةيثالث ةحفاصملا - 3.2](#)

[مداخلإ نم ةلجفملا](#)

[اهب يصوملا تاعارجلإ](#)

[ليلعملإ نم ةلجفملا TCP 3-way + RST ةحفاصم - 3.3](#)

[اهب يصوملا تاعارجلإ](#)

[مداخلإ نم يروفلا TCP + RST ل هاجتاللا ةيثالث ةحفاصملا - 3.4](#)

[اهب يصوملا تاعارجلإ](#)

[ليلعملإ نم TCP RST 4. ةلاجلإ](#)

[رسل ليلحت](#)

[اهب يصوملا تاعارجلإ](#)

[\(1 ويراني سلا\) ةيطب TCP ل لقتن 5. ةلاجلإ](#)

[ةيطب ل لاقنتنا 1. ويراني سلا](#)

[رسل ليلحت](#)

[اهب يصوملا تاعارجلإ](#)

[ةيرس ل لقتن 2. ويراني سلا](#)

[\(2 ويراني سلا\) ةيطب TCP ل لقتن 6. ةلاجلإ](#)

[رسل ليلحت](#)

[اهب ي صوملا تاعارجالا](#)

[\(قمزجالا فلت\) TCP لاصتا ةلكشم 7. ةلجالا](#)

[رسأ ليلحت](#)

[اهب ي صوملا تاعارجالا](#)

[\(ةدوق فملا مزجالا\) UDP لاصتا ةلكشم 8. ةلجالا](#)

[رسأ ليلحت](#)

[اهب ي صوملا تاعارجالا](#)

[\(1 ويرانيسلا\) HTTPS لاصتا ةلكشم 9. ةلجالا](#)

[رسأ ليلحت](#)

[اهب ي صوملا تاعارجالا](#)

[\(2 ويرانيسلا\) HTTPS لاصتا ةلكشم 10. ةلجالا](#)

[رسأ ليلحت](#)

[اهب ي صوملا تاعارجالا](#)

[IPv6 لاصتا ةلكشم 11. ةلجالا](#)

[رسأ ليلحت](#)

[اهب ي صوملا تاعارجالا](#)

[\(ARP ميسنت\) عطقتملا لى صولتا ةلكشم 12. ةلجالا](#)

[رسأ ليلحت](#)

[اهب ي صوملا تاعارجالا](#)

[ةدو و تاطابترا روه ظيف ببستت يتلا \(SNMP \(OIDs نىاك تا فرعم لىل فرعتلا 13. ةلجالا](#)
[قىزك رمل ا ةجل اعمل](#)

[رسأ ليلحت](#)

[اهب ي صوملا تاعارجالا](#)

[ةلص تا ذتامولعم](#)

ةمدقملا

فاشكتسا ىل فدهت مزجالا طاقتلال ةفلتخم ليلحت تاينقت دنتسمل اذه فصى ةىل عافب اهجال صا ةكبشلال تالكشم

ةيساسال تابلطتملا

تابلطتملا

ةىلاتل عىضاوملاب ةفرعم كىدل نوكت ناب Cisco ى صوت

- Firepower ىساسال ماظنلا ةىنب
- NGFW تالجس
- NGFW Packet-tracer

هذه ةىبلت ةدشب نسحتسمل نم، مزجالا طاقتلال ليلحت ىل فءبلا لبق، كلذ ىل ةفاضلابل تابلطتملا:

- ةىفك مهفت مل اذا ةمزح طاقتلال نم ققحتلال ىل فءبلا - لوكتوربلا ةىلمع فرعت هىل عالىتسالال مت ىل ذلا لوكتوربلا لمع
- انك مم اذه نكى مل اذا. ةىاهن ىل ةىاهن نم لقنلا ةزهجأ فرعت نابجى - طاطخملال فرعت قفدتلال و مءلال نم تانابلا قفدت ةزهجأ ةفرعم لىل ةل عىل عىل فبجى
- ةىنعملال تاهجالل ىه امو، مزجلال كزاهج ةجلعم ةىفك فرعت نابجى - زاهجال لىل فرعت

ة. فلفلخملا طاقنلالا طاقن يه امو، زاهجلا ةينب يه امو، (جورخلا/لوخدلا)

- امي ف زاهجلا ةطساوب ةمزحلا قفدت عم لماعتلا ةيفيك فرعت نا بجي - نيوكتلا فرعت
ب قلعتي:
 - جورخلا/هيجوتلا ةهجاو
 - ةقبطملا تاسايسلا
 - (NAT) ةكبشلا ناو نع ةمحر
- قيبطتل ةزهاج نوكت نا ب صوي، طاقنلالا تاي لمع بناجب - ةحاتملا تاودال يلع فرعت
اهطرب مق، رمال مزلا اذوا (رثال عبتتو ليجستلا لثم) يرخال تاي نقتلاو تاودال
اهطاقنلا مت يتلا مزحلاب

ةمدختسملا تانوكملا

ةيلاللا ةيداملا تانوكملاو جماربلا تارادصا يل دننتملا اذو يف ةدراولا تامولعمل دننست

- 6.5.x رادصال FTD جم انرب لغشي يذال FP4140 يل تاهوي رانيسلا مظعم دننست
- 6.5.x رادصال FMC ليغشت جم انرب

ةصاخ ةيلمعم ةئيبي يف ةدوجوملا ةزهجالا نم دننتملا اذو يف ةدراولا تامولعمل عاشنلا مت
تنالك اذا. (يضارثفا) حوسمم نيوكتب دننتملا اذو يف ةمدختسملا ةزهجالا عيمج تادب
رما يال لمحتملا ريثاتلل كمهف نم دكاتف، ليغشتلا دي قكتكبش

ةيساسا تامولعم

ايموي. مويلا ةرفوتملا الامه رثكالا احوالصوا عاخذالا فاشكتسا تاودا دحا وه ةمزحلا طاقنلا
ةطقتلملا تانايبلا ليحت عم لكاشملا نم ديدعل Cisco نم TAC لحي

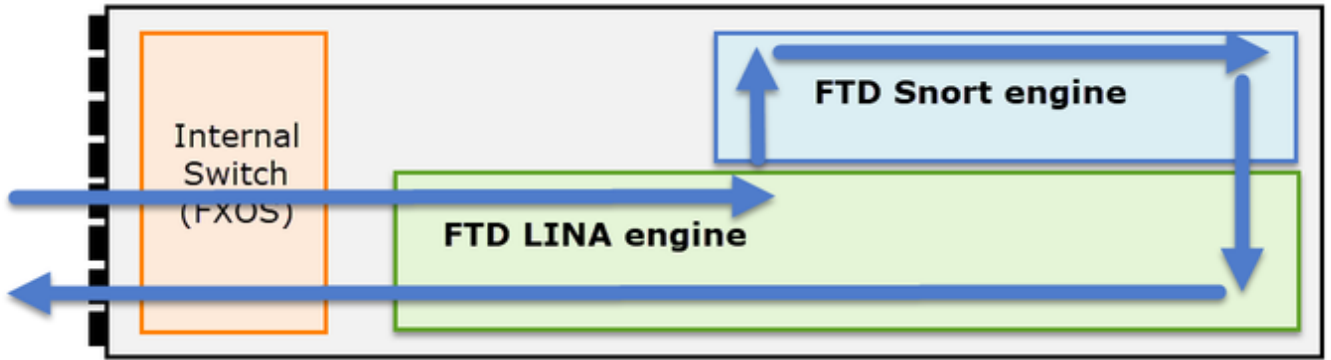
ةكبشلا لكاشم ديدحت يف نامالاو ةكبشلا يس دننتملا ةدعاسم وه دننتملا اذو نم فدهلا
اساسا مزحلا طاقنلا ليحت يل اذانتسا احوالصوا اهئاخذأ فاشكتساو ةعئاشلا

تدهوش يقي قح مدختسم تالاح يل دننتملا اذو يف ةمدقملا تاهوي رانيسلا عيمج دننست
Cisco نم (TAC) ةينقتلا ةدعاسملا زكرم يف

نم (NGFW) يلاتلا ليجلا ةيامح رادج رظن ةهجو نم ةمزحلا طاقنلا تاي لمع دننتملا يطغي
اضا يرخال ةزهجالا عاونأ يلع ميهافل س فن قيبطت متي نكلو، Cisco

ةيامحلا رادج تاجتنم ةعومجم يلع روص عيمجت كنكمي فيك اهري دصتو (NGFW) يلاتلا ليجلا نم

Firepower Threat Defense قيبطتو (1xxx، 21xx، 41xx، 93xx) FirePOWER ناما زاهج ةلاح يف
ةروصل يف حضورم وه امك ةمزحلا ةجالعم ضرع نكمي، (FTD)



1. لكيه ليل خادلا لوجملا ةطساوب اهتجالعم متي و لوخدلا ةهجاو ةمزحلا لخدت.
2. نم ققحتلاب اساساً موقوي يذلا FTD Lina كرحم لىل ةمزحلا لخدت.
3. (يساساً لكشب L7 صحف) snort كرحم ةطساوب ةمزحلا صحف بلطتي جهنلا ناك اذا.
4. ةمزحلل امك ريخشلا كرحم عجري.
5. Snort رارق لىل عانبا اههيجوت ةداعا و ةمزحلا طاقساب LINA كرحم موقوي.
6. يلخادلا لكيه لوجم لالخنم لكيه لبيكرت لىل ةمزحلا لمعت.

في (FTD) ةعرسلا قئاف لاسرالجم انرب" طاقنلا نكمي، ةحضوملا ةينبلا لىل اذانتسا
ةفلتخم نكاماً (3) ةثالث:

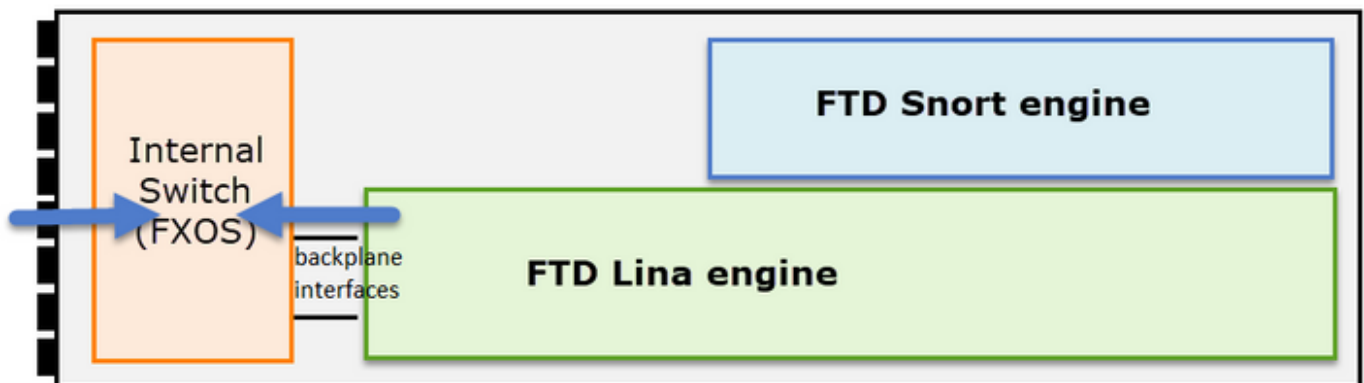
- FXOS
- كرحم FTD Lina
- فتي ريخش كرحم

FXOS طاقنلا عيمجت

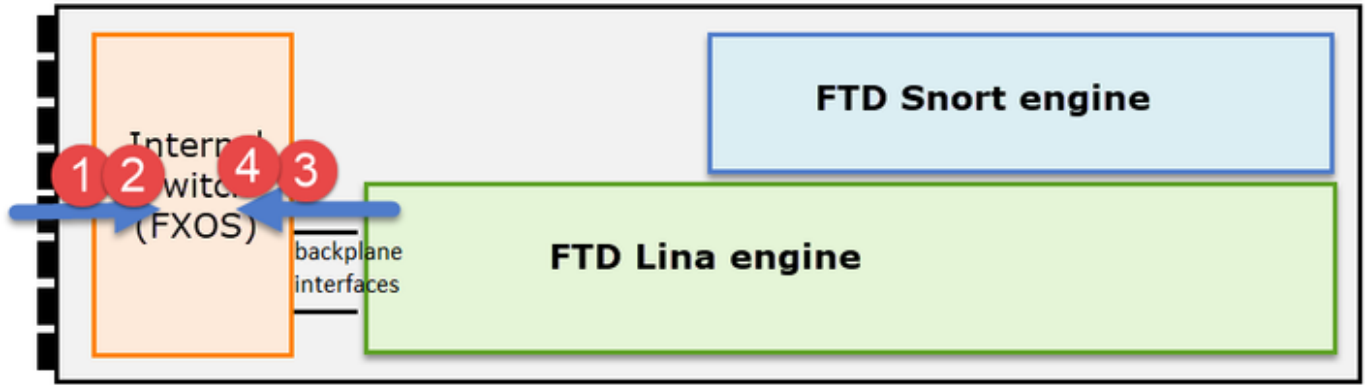
ذنتسمل اذ في ةيلعمل الفصومتي:

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

في رهظت يلخادلا لوجملا ضرع ةطقن نم لخدملا هاجتلا في ذخؤنأ نطقف FXOS طاقنلا نكمي
انه ةروصل.



(يلخادلا لوجملا ةينب ببسب) هاجتلا لكل طاقنلا اطقن اتاه، انه حضوم وه امك



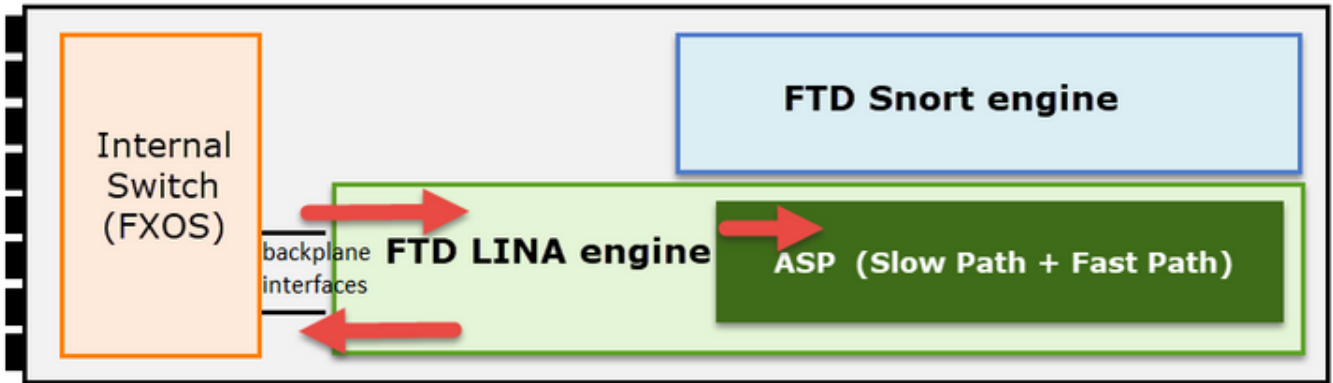
(VNTag) ةيرهاظ ةكبش ةمالع 4 و 3، 2 طاقنل ايف ةطقنل مال مزحل نمضتت

✎ و FP41xx يماظن ايلع ال FXOS ماظن ب لكيله ايو تسم ايلع طاقنل رفوت ال : ةظحال م ةي نك مال هذه FP1xxx و FP21xx رفوت ال . ني ساس ال FP93xx

FTD Lina طاقنل ايلع م عي مجت و ني كمت

ةيسيئرل طاقنل ال طاقن:

- لوخدل ةهجاو
- جورل ةهجاو
- عي رسال نام ال راسم (ASP)



مدختسم ةهجاو) Firepower Management Center ب ةصاخال مدختسم ال ةهجاو مادختس اكنكمي ب ةصاخال طاقنل ال ايلع م عي مجت و ني كمت ال FTD ب ةصاخال (CLI) رماو ال رطس ةهجاو و (FMC) ال FTD Lina.

ةيلخادل ةهجاو ال ايلع CLI نم طاقنل ال ني كمت

<#root>

firepower#

capture CAPI interface INSIDE match icmp host 192.168.103.1 host 192.168.101.1

الك في 192.168.101.1 و 192.168.103.1 IPs نېب رورملا ةكرح عم طاقتلالا اذه قباطتي نيهاجتالا.

FTD Lina: ةطساوب اهطاقسا م ت يتلا مزحلا عيجم ةيؤرل ASP طاقتلا نيكمت

```
<#root>
```

```
firepower#
```

```
capture ASP type asp-drop all
```

FTP: مداخل لىل FTD طخ طاقتلا ريصت

```
<#root>
```

```
firepower#
```

```
copy /pcap capture:CAPI ftp://ftp_username:ftp_password@192.168.78.73/CAPI.pcap
```

TFTP: مداخل لىل FTD طخ طاقتلا ريصت

```
<#root>
```

```
firepower#
```

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

FMC. م دختسم ةهجاو نم FTD Lina تاعومجم عيجمتو نيكمت كنكمي، FMC 6.2.x رادصل نم اءدب

:هوهو، FMC لبق نم هترادا متت ةيماح رادج نم FTD تاطقل عيجمتلا رخأ ةقيرط كانه

1 ةوطخل

FTD. صرق لىل طاقتلالا خسننا طاقتلالا ASP و LINA ةلاح في

```
<#root>
```

```
firepower#
```

```
copy /pcap capture:capin disk0:capin.pcap
```

```
Source capture name [capin]?
```

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

```
!!!!
```

2 ةوطخال

عقوم لى هخسنا م ث ،ظوفحم لاطاقتلالا ناكم ددحو ،ريبخل اعضو لى لقتنا
/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 ةوطخال

لقنتو FTD لوكوتورب ريديت لى (FMC) ةرادل لى ف مكحتل اددحو لى لوخدلا لىجستب مق
اهالصل او اطاخال فاشكتسأ ةنوقى اددحو FTD زاخ عقوم ددح .ةزهال اةرادل > ةزهال لى



4 ةوطخال

Snort: يوتسم طاقتلل نيكت

```
<#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
```

ديعب مداخ ىل FTP لالخ نم هخسنو و capture.pcap مساب فلم ىل طاقتلل اةباتكل:

```
<#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.
```

>

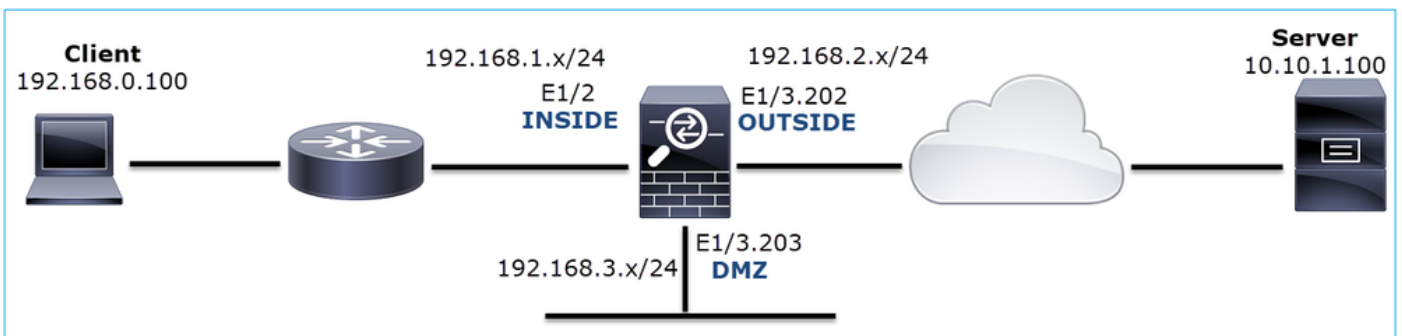
طاقات الة فرصت لم اوع نمضتت يتلاريخشلا يوتسم يلع طاقاتلالا ةلثمأ نم ديزمل
دنتسمللا اذه نم ققحت ةفلتخم:

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

اهحالصإو اءاطخألا فاشككسا

جرخم ةهجاو يلع TCP SYN دجوي ال 1. ةلجال

انه ةروصللا يف حضوم طاطخمللا



لمعي ال HTTP: ةلكشملا فصو

رثأتملا قفدتلا

SRC IP: 192.168.0.100

DST IP: 10.10.1.100

لوكوتوربل: TCP 80

رسأ ليلحت

FTD LINA: كرحم يلع طاقاتلالا نيكمت

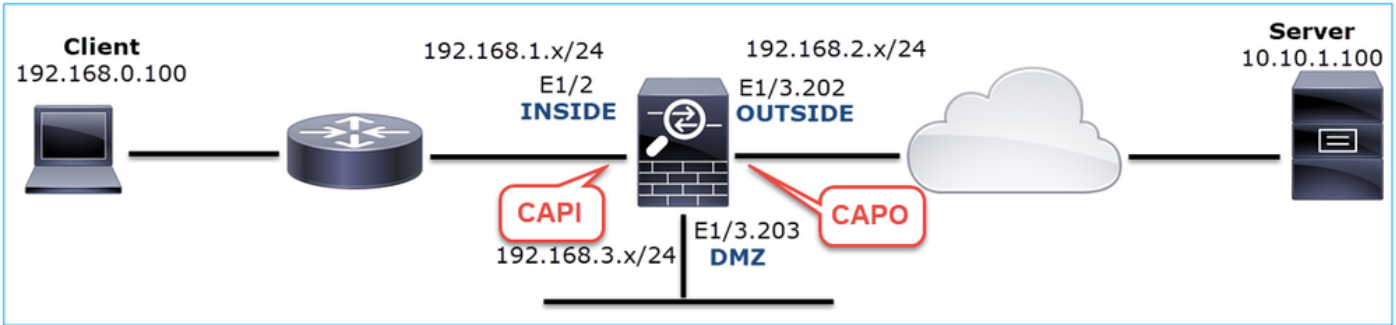
<#root>

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



في طول ويرانيس ال - طاقت ال

في طول ويرانيس نم تاطول لى لصحت نأ امئادج دي فم ال نم ،ساسأ طخك

ةروصل ال في حضور ال وحن ال لى NGFW Inside ةه او طاقت ال متي

CAPI-working.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 1

No.	Time	Source	Destination	Protocol	Length	Info
2	0.250878	192.168.0.100	10.10.1.100	TCP	66	1779 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
3	0.001221	10.10.1.100	192.168.0.100	TCP	66	80 → 1779 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1
4	0.000488	192.168.0.100	10.10.1.100	TCP	54	1779 → 80 [ACK] Seq=1 Ack=1 Win=66240 Len=0
5	0.000290	192.168.0.100	10.10.1.100	HTTP	369	GET / HTTP/1.1
6	0.002182	10.10.1.100	192.168.0.100	HTTP	966	HTTP/1.1 200 OK (text/html)
7	0.066830	192.168.0.100	10.10.1.100	HTTP	331	GET /welcome.png HTTP/1.1
8	0.021727	10.10.1.100	192.168.0.100	TCP	1434	80 → 1779 [ACK] Seq=913 Ack=593 Win=65792 Len=1380 [TCP segment of a reassembled PDU]
9	0.000000	10.10.1.100	192.168.0.100	TCP	1434	80 → 1779 [ACK] Seq=2293 Ack=593 Win=65792 Len=1380 [TCP segment of a reassembled PDU]
10	0.000626	192.168.0.100	10.10.1.100	TCP	54	1779 → 80 [ACK] Seq=593 Ack=3673 Win=66240 Len=0

> Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 > Ethernet II, Src: Cisco_fc:fc:d8 (4c:4e:35: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: 1779, Dst Port: 80, Seq: 0, Len: 0

ةسيس ئر ال طاقت ال

1. TCP 3-way ةح فاصم.
2. هاجت ال ئانث تاناي ال لدابت.
3. مزحل ني ب تقولا قرف لى ادانسا (مزحل ني ب تاريخأت دجوت ال)
4. تاناي ال قف دتل حي حصل ال زاه ال وه ردصم ال MAC.

انه ةروصل ال في ، NGFW ل ةجراخ ال ةه او ال طاقت ال ضرع متي

CAPO-working.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 1

No.	Time	Source	Destination	Protocol	Length	Info
2	0.250787	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_fc: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: 1779, Dst Port: 80, Seq: 0, Len: 0

ةةس ةرل ا طاقنلا:

1. CAPI طاقنلا ة ءو ءوملا ءانا ءا ءسفن.
2. ءءءصلا ءبنملا زا ء ءه ءءول MAC.

لم ءء ال ءءرانا ءس - طاقنلا

ءكشلا اءء رءصلا ءءء، زا ءءلاب ءصا ءلا (CLI) رما ءال رطس ءه ءو ءال ءنم:

<#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

CAPI ءا ءءءم:

<#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

Wireshark في CAPI طاق تلال ةروص هذة:

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	0.250470	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

3

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: Cisco_fc:fc:d8 (4c:4e:35: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

ةس يئرلا طاقنلا:

1. (هاتإلا ةيثالء TCP ءءافاصم ءءوي ال) طقف TCP ماظن مزء ضرع مءي.
2. لمعمل موق ي. امهؤاشن انكم ي ال (3171 و 3172 رءصم ال ءفنم) TCP ل ناء سلء كانه. الءاسرا ءءاء ءمء يءل مزء ال هءه فيءء مءي. TCP syn مزء لءاسرا ءءاء ءءصم ال TCP لءاسرا ءءاء ءاي لمءك Wireshark ءطس اوب.

3. كلكلذى الامو ناوٲ 6 مٲ 3 براقى ام لك TCP لوكوتورب لاسرا ءءاع| تاىلمع ٲءءء.
4. تاناىبل قفءءل ءىءال زاءءل نم MAC ناوع رءصم.

ىل ى ام ءاءءنءسا نكم ى؁ نىلصفل لىل اءانءساو

- راء ءىل (لوكوتوربل او؁ src/dst ءفنمو؁ SRC/dst IP) ءنىعم ءاونق 5 نم ءمزء لصء (لءاءل ىف) ءءقوءملا ءءءاولا لىل ءىامءل (ءىءراءل) ءءقوءملا ءءءاولا لىل ءىامءل راء ءمزءل ءرءء ال.

اهب ىصوملا ءاءاءل

ءلأسملا هءه قاطن قىىىضء ءءاىز وه عرفلا اءه ىف ءءراول ءاءاءل نم ضرءل او

ءىءءم ءمزء ءبءء نم ققءء 1. ءاءل

طاقسا ءلء ىف. ءىامءل راء ءس او ب ءمزء ءءل لعم ءىف ء ءفرءم packet-tracer ءاءمءءسا اءل ءامم ءىءءملا ءمزءل ءبءء وءبى؁ ءىامءل راء لىل لوصول ءهن ءس او ب ءمزءل ءاءل

```
<#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

ةرشابملا مزحلا راثآ نم ققحت 2. ءارجإلا

رارج ةطساوب ةيقيقحلا TCP syn مزح ةجالعم ةيقيقح نم ققحتلل ةمزحلا عبتت نيكم تب مق
طقف لخدم ةمزح 50 لوأ عبتت متي، يضارتفا لكش ب. ةيماحلا

<#root>

firepower#

capture CAPI trace

تقؤملا طاقتلالا نزم حسم:

<#root>

firepower#

clear capture /all

اذهل اهباشم عبتتلا ودبي، ةيماحلا رارج إلا لوصولاهن ةطساوب ةمزحلا طاقتلالا ةلاح ي
جارجإلا

<#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

FTD Lina تالچس نم ققحت 3. ءارجال

دنتسمل اذه نم ققحت، FMC ربع FTD ىلع Syslog نيوكت:

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

مدع ةلاح في FTD Lina تالچسل يجرأخ syslog مداخ نيوكت متي نأ ةدشب نسحتسمل نم ةيامل رادج ىلع ةيحلحمل تقؤملا نزخمل تالچس نيكم تب مق، دعب نع syslog مداخ نيوكت ةيادب ةطقن وه لاثملا اذه في رهاطلا لچسل نيوكت. اهحالصإو ءاطخألا فاشكتسأ ءانثأ ةديج:

```
<#root>
firepower#
show run logging
...
logging enable
logging timestamp
logging buffer-size 1000000
logging buffered informational
```

يفرطال ءادنلا زاھج في مكحتلل ارطس 24 ىلع يفرطال ءادنلا زاھج طبضا:

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

تقؤملا طاقتلال نزخم حسم:

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

متي، لاثملا اذه في ل.لحمل ةيفصت لماع مادختساب تالچسل لصحفو لاصتال ربتخا ةيامل رادج ىلا لوصولا جهن ةطساوب مزحل طاقسا:

```
<#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
```

ةي امحل رادج ASP طاقس ايا لم عم نم ققحت 4. اءال

يتل مزحل عيمج تاداع ةيؤر كنكمي ف، ةي امحل رادج نم تطقس ةمزحل نأ يف كشت تنك اذا
جم انربل يوتسم يل ع ةي امحل رادج اهتطقس ا:

```
<#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
```

ASP: جم انربل يوتسم طاقس ايا لم عم عيمج ضرعل طاقتل ال ايا لم عم ني كم تنك مي

```
<#root>
```

```
firepower#
```

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

 رايخ) طقف ةمزحل س وؤر طاقتل كنكمي ةمزحل ايا وتحمب امتهم نكت مل اذا: حيملت
تقؤملا طاقتل ال نزم يف مزحل نم ديزملا طاقتل كل حيتي اذهو. (طقف س وؤرلا
500 وه يضارتفا لكش ب) تقؤملا طاقتل ال نزم مجح ةدايز كنكمي، كلذ يل ةفاض ال اب
نم اءب، اريخ. (تقؤملا نزملا رايخ) تب اجم 32 يل لصت ةمي ق يل (تيا بولي ك
10 يتح طاقتل فلم نيوكت فلمل مجح رايخ كل حيتي، FTD لوكوتورب نم 6.3 رادص ال
PCAP. قيس ننتب طاقتل ال ايا وتحم ةيؤر طقف كنكمي ةل ال كلت يف. تيا ب اجم

ثحب ال قاطن ق يي ضتل حشرم مادختس كنكمي، طاقتل ال ايا وتحم نم ققحت لل

```
<#root>
```



```
firepower#
capture ASP_NO_ROUTE type asp-drop no-route
firepower#
capture ASP_ACL_DROP type asp-drop acl-drop
```

5. ليغشت) ةي امحل راج لال خ نم اه حال ص او عا ط خ ال فاش كت ساب موقت يذل ق ف دت لال لاس را (راب تخ |

6. دوجوم ريغ راسم ببسب مزحل طاق سا مت ، ة لال 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
```

5. ءارج ال FTD Lina لاصتا لودج نم ققحت .

اهن اف ناك ببسب يأل نكلو ، 'X' ةه جاو ة مزحل ج رخت نأ اه يف ع قوتت تالاح كانه نو كي نأ نكمي
اذه ليغشت لال بيترت لى لى ةي امحل راج ج رخم ةه جاو دي دحت دن تس ي . 'Y' ةه جاو ال ضرعت

1. أشنم لال لاصتا الا ثح ب .
2. لى لى ةي ول و ال (NAT ةي اغ) UN-NAT ة لجرم ذ خأت - (NAT) ة ك ب ش لال نا ونع ةم جرت نع ثح ب ال .
راسم ال ثح ب و PBR .
3. (PBR) ة سا ي س ال لى لى ع مئاق ال لهي جوت ال .
4. هي جوت ال لودج ثح ب .

FTD لاصتا لودج نم ققحت لل

```
<#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:

80

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

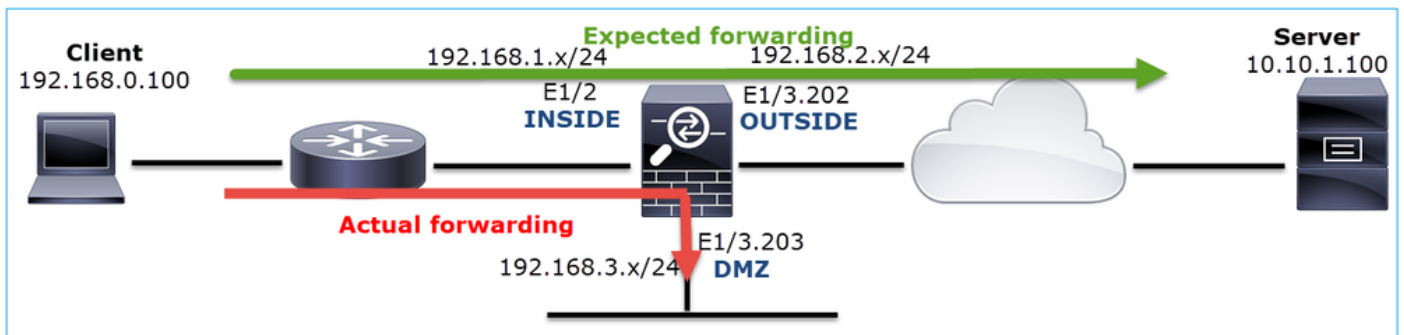
, idle 0:00:01, bytes 0, flags

aA N1

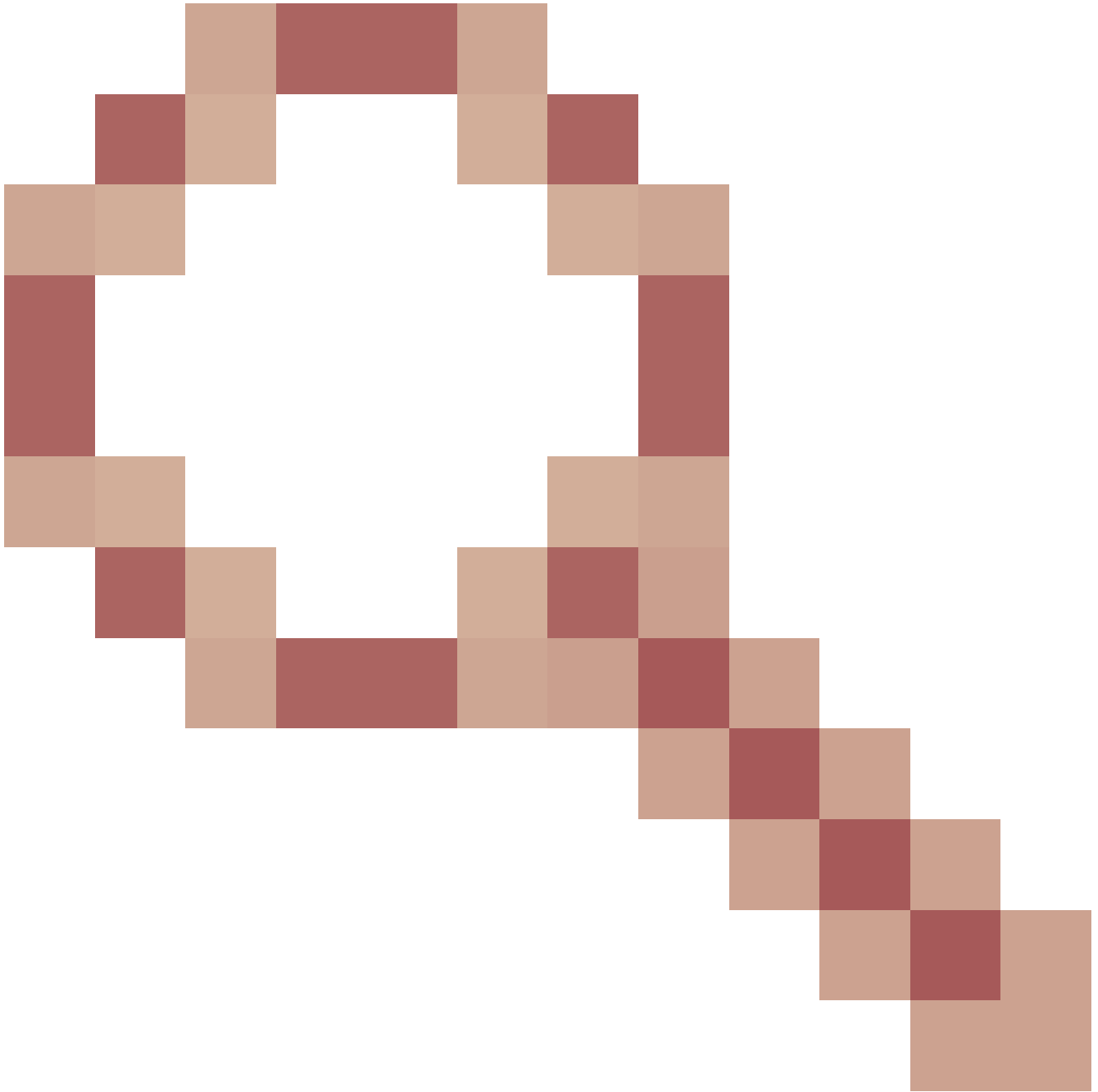
ةيسيرل طاقنل:

- ال رهظي مل - فصن هحتف مت) ينينج لاصتال انإ، زيي متل تامالع ل ا ادانتسا (ةيامحل رادج ةطساوب TCP SYN
- DMZ. وه نراق جرخملا و لخاد نراق لخدملا انيم ةياغل/ردصملا لعل انب.

انه ةروصلال ي ف اذه روصت نكمي:



✍ جارج ي ف ةهاولا رمأ 0 هرادقم نامأ يوتسم لعل يوتحت FTD تاهجاو عيمج نأ امب: ةطخال مقرر تاذه هاولا ديدحت متي، صوصخال هجو لعلو. ةهاولا مقرر ل ا ادانتسا show conn ديدحت متي امنيب ةيلخاد انأ لعل لعلال (VPIF-num) يرهظال ياساسال ماظنل ةهجاو تنأ. ةيجراخ انأ لعل (لقال VPIF-num) يرهظال ياساسال ماظنل ةهجاو مقرر تاذه هاولا ةلصل تاذه تانيسحتل. رمأ ليلصفت نراق ضرعل عم ةميقي vpif نراق ل تيارع يسطسي، نم اطاخال احيصت فرعم Cisco [CSCvi15290](https://www.cisco.com/c/en/us/td/docs/configuration/guide/FTD/CSCvi15290.html)



ENH: FTD 'show conn' جارجخ | فف لاصتالاهاجت | FTD رهظي

```
<#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
```

Interface number is

22

 رڤوي 9.13.x رادصإلإ ASA، 6.5 رادصإلإ FirePOWER ءم انرب رادصإل نم لآلإ وه امك :ةظآالم بئءء سملاو لاصتالآ ئءاب لولء ءامولعم و show conn detail و show conn long رملآل آارآ

1: ءانلآ

```
<#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
```

2: ءانلآ

```
<#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
```

ناونع ءمءرت ءلآ ؤ س اوقأ لآء NATed IPs لئول ؤرءل ؤرءئ، ءلذئ لئل ءفاضلآ بول
ءءبشلآ:

```
<#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), flags
```

Initiator: 192.168.1.100, Responder: 192.168.2.222
Connection lookup keyid: 262895

ARP) راجع اناونع ليلحت لوكوتوربل تقووملا نيزختلا ةركاذ نم ققحت 6. ءارجا

ةيلصألة مزحلا طاقسإب ةيماحلا راج موقى، ةيلاتلا ةلحرملا ل ةيماحلا راج ىلع رذعت اذا
لحب موقى ىتح رارمتساب ARP تابلط لاسراو تاماصل لكشب (ةلاجال هذه في TCP SYN)
ةيلاتلا ةلحرملا.

رمألا مدختسأ، ةيماحلا راجل ARP ل تقووملا نيزختلا ةركاذ ضرعل

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

رمألا مادختسإ كنكمي، نيلحام ريغ نيفيضم دوجو نم ققحتلل، كلذىل إفاضالاب

```
<#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
```

ARP: ب صاخ طاقتلا نيكمت كنكمي في، ARP ةيلعمل صحلل نم ديزم ءارجا ديرت تنك اذا

OUTSIDE 192.168.2.72 4c4e.35fc.fcd8 9

ةرشابملا TCP SYN ةمزحل عبتت رهظي ناكملا في ARP لاخذل دوجو مدع ةلاح في

<#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
```

ةوطخلا نوكت ال امدنع ىتح حامسلا :ءارءالا عبءتلا رهظي ،ءارءالا ي ف هءيؤر نكمي امك ءءالءا هءه ي ف !ءي امءال راءء ءطساوب ءمصب ءمزءال طاقسا مءيول وءول ءلباق ءيلاءال ءاءءن ءءء رءءأ رفوي وه نأ امب ءصءف اضيأ يءبني ءاءا tracer-ءربلا

<#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: ةق بلسلا ةلسرلا نيسحت مت ، ةريخألا ASA/FirePOWER تارادصا يف

<#root>

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

Check ARP table (show arp) has entry for nexthop

., Drop-location: f

اهب يصوملا تاءارجإلاو ةلمتحملا بابسألا صخلم

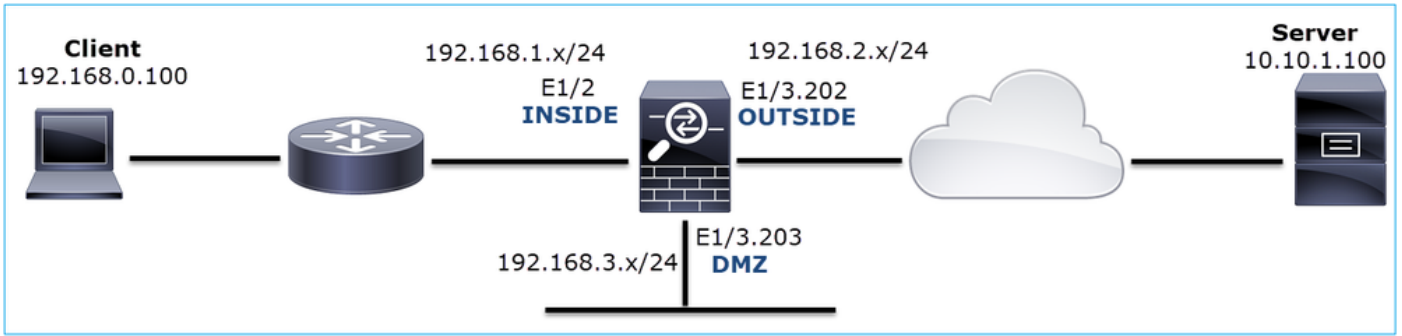
لا نم لسري طبر TCP syn نم ام نأ ريغ ، نراق لخدملا يلع طبر TCP syn طقف تنأ يري نإ
 ببس نكمي ضعب نراق جرخم عقوتي:

لمتحملا ببسلا	اهب يصوملا تاءارجإلا
<p>جهن ةطساوب ةمزحلا طاقسا متي ةيماحلا رادج يلا لوصولا</p>	<ul style="list-style-type: none"> • ةمزحلل ةيماحلا رادج ةجالعم ةيفيك ةفرعمل • ةيماحلا رادج تالجس نم ققحت • ةيماحلا رادج ASP طاقسا تايلمع نم ققحت (show asp drop و capture type asp-drop). • نأ ضررت في اذه FMC لاصتا ثادحأ نم ققحت نكمم ليحست يلع يوتحت ةدعاقلا
<p>جحص ريغ طاقتلاللا ةيفصت لماع</p>	<ul style="list-style-type: none"> • w/trace ضبق يلع و packet-tracer تلمعتسا ل ددعي نأ nat ةمچرت نوكي كانه نإ يري نأ طبضا ، ةلحال كلت في ip. ةيغال و اردصملا طاقتلاللا حشرم • IP نيوانع show conn long رمألا جارخا ضرعي

	NATed ب ةصاخلا
فلتخم جرخم نراق ىلا طبرلا تلسراً	<ul style="list-style-type: none"> • ةمزحلل ةيامحل رادج ةجلاعم ةيفيك ةفرعمل يف عضي يذلا تايلمعل ببيتري ركدت يلاحلا لاصتال او جرخملا ةهجاو ديدحت رابتعالا PBR و UN-NAT و هي جوتلا لودج ثحبو ةيامحل رادج تالجس نم ققحت • ةيامحل رادج لاصتال لودج نم ققحت (show conn). <p>قباطت اهنأل ةئطاخ ةهجاو ىلا ةمزحلل لاسرلا مت اذا clear conn address رمأل مدختساف، يلاح لاصتال ءحسم ديتري ذللا لاصتال نم 5 ةلسلسلا ددحو</p>
ةهجو لا ىلا قيرط دجوي ال	<ul style="list-style-type: none"> • ةمزحلل ةيامحل رادج ةجلاعم ةيفيك ةفرعمل • ةيامحل رادج ASP طاقس تايلمع نم ققحت طاقس ببس ىلع لوصحلل (show asp drop) راسم ال
جرحملا ةهجاو ىلع ARP لاخدا دجوي ال	<ul style="list-style-type: none"> • رادج ARP ل تقؤملا نيزختلا ةركاذ نم ققحت (show arp) ةيامحل • كانه ناك اذا ام ةفرعمل packet-tracer مدختسأ ءلاص رواجت
لطم جرحملا نراق	رادج ىلع show interface ip brief رمأل جارخا نم ققحت ةهجاو لا ةلاح نم ققحتو ةيامحل

مداخل نم TCP RST، ليمعلا نم TCP SYN 2. ةلاحلا

:طاطخملا ةروصلا هذه ضرعت



لمعني ال HTTP: ةل كشم ال ف ص و

رثأتم ال ق ف د ت ال

SRC IP: 192.168.0.100

DST IP: 10.10.1.100

ل و ك و ت و ر ب ال : TCP 80

ر س أ ل ل ح ت

ق م ك ن ي ك م ت ب م ق FTD LINA. ع ل ع ط ا ق ت ل ال ت ا ي ل م ع

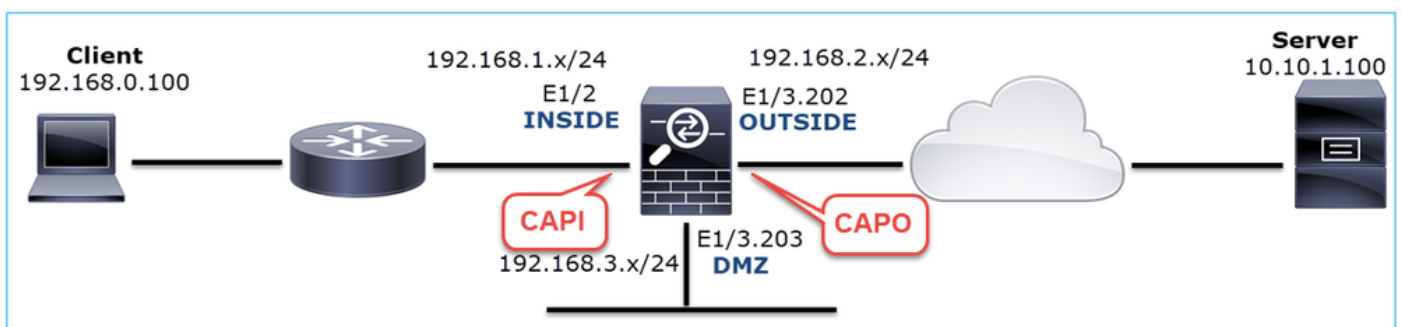
<#root>

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
```



ل م ع ي ال و ي ر ا ن ي س - ط ا ق ت ال

ي ل ي ا م ك ت ا د ي د ح ت ال و د ب ت ، ز ا ه ج ل ا ب ة ص ا خ ال (CLI) ر م ا و ا ل ر ط س ة ه ج ا و ل ل ا خ ن م

<#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
```

CAPI تاي و تحم:

```
<#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>
```

```
...
```

CAPO تاي و تحم:

```
<#root>
```

firepower#

show capture CAPO

```
1: 05:20:36.654507 802.1Q vlan#202 PO 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 PO 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 PO 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 PO 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 PO 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 PO 192.168.0.100.22196 > 10.10.1.100.80:
S
4118617832:4118617832(0) win 8192 <mss 1380,nop,nop,sackOK>
```

Wireshark في CAPI طاقنتل ةروصل ال هذه رهظت.

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	66	[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] 22195 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
9	0.000611	10.10.1.100	192.168.0.100	TCP	54	80 → 22195 [RST, ACK] Seq=1 Ack=1 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:fc:d8 (4c:4e:35: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: 22195, Dst Port: 80, Seq: 0, Len: 0

ةسيئرل ال طاقنل:

1. TCP syn ةمزه ردصم ل لسري.
2. ردصم ل وحن TCP RST ل لسرا متي.
3. TCP syn ةمزه ردصم ل لسري.
4. ثب ل هوم ل ل ردصم ل MAC ناوع يم تني لوخدل مزح ل ع (ةححص MAC ني وان ع ، ةه اول ل خاد ةي امحل راج ل ل ةه وول MAC ناوع يم تني).

Wireshark في CAPI طاقنتل ةروصل ال هذه رهظت:

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
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 07:20:37.914305	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) on interface 0

> Ethernet II, Src: Cisco_fc:fc:d8 (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. TCP syn ةمزح ردصملا لسري.
2. ةجراخللا ةهجاوولا لىل TCP RST لصي.
3. TCP syn مزح ردصملا لسري.
4. هجوم MAC، ردصم وه يجراخللا ةيامحلا راج نوكي جورخللا مزح لىل (ةجحص MAC نيوانع . MAC ةياغللا وه ثبل).

يلي امجاتنتسا نكمي، نيلصفللا لىل اذانتساو:

- مداخللاو لييمعلا نيپ هاجتلا يثالثلا TCP لاصتا ديكأت لامك متي ال
- ةيامحلا راج جرخم ةهجاوولا لىل لصي يذلا TCP RST كانه
- (MAC نيوانع لىل اذانتسا) مداخللا نم تانايبلا قفدت ةزهجا لىل "ثدحتي" ةيامحلا راج

اهب يصوملا تاءارجللا

ةلأسملا هذه قاطن قييضت ةدايز وه عرفلا اذه يف ةدراولا تاءارجللا نم ضرغللاو

TCP RST لسري يذلا MAC ناووع ردصم نم ققحت 1. ءارجللا

دق {upper}mac ردصملا نأ امب هسفنلا لىل TCP syn لىل ف يري {upper}mac ةياغللا نأ تققد
 طبر TCP rst لىل ف يري.

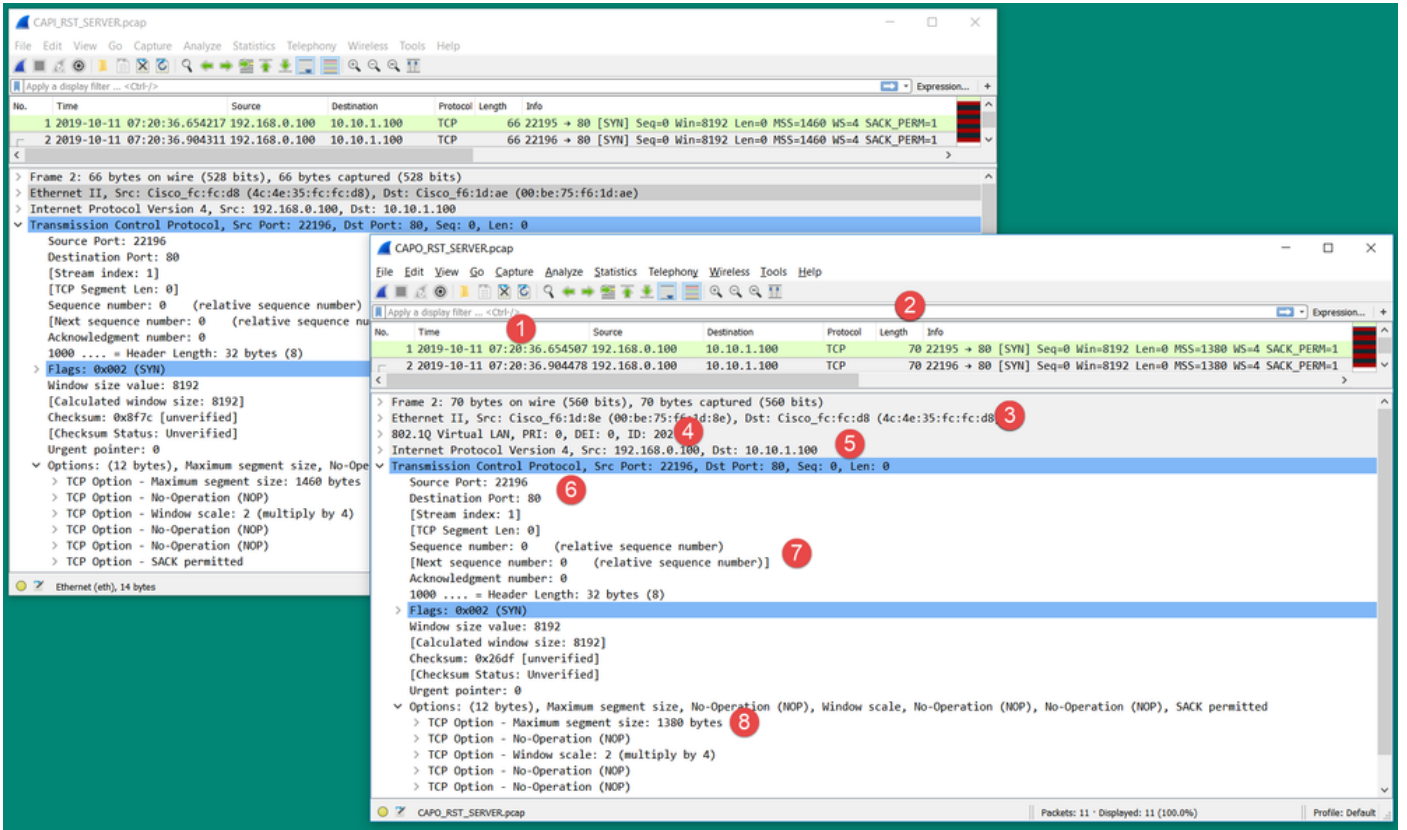
The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows a packet capture for 'CAPO_RST_SERVER.pcap'. The packet list shows two packets: a SYN packet (No. 1) and another SYN packet (No. 2). The packet details for the second packet (No. 2) are expanded, showing the Ethernet II layer with source MAC 'Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8)' and destination MAC 'Cisco_f6:1d:8e (00:be:75:f6:1d:8e)'. The bottom screenshot shows the same capture with a third packet (No. 3) selected, which is an RST, ACK packet. The packet details for this packet are expanded, showing the Ethernet II layer with source MAC 'Cisco_fc:fc:d8 (4c:4e:35:fc:fc:d8)' and destination MAC 'Cisco_f6:1d:8e (00:be:75:f6:1d:8e)'. Two arrows, one green and one orange, point from the source and destination MAC addresses in the top screenshot to the corresponding addresses in the bottom screenshot.

نېرمۇ دېكأت ىلإ صحفلا اذه فدهي:

- رظانتم ريغ قفدت دوجو مدع نم ققحت .
- عقوقتم لانايبال قفدت زاهج ىلإ MAC عامتنا نم ققحت .

جورخلاو لوخدلا مزح نراق 2. عاجلإ

م تي . طببرلا دسفي/لدعي ال ةيامحل راج نأ نم ققحتلل ايرصب Wireshark ىل ع 2 طببرلا نراق . عقوقتملا قورفلا ضعب زاربا



ةيسيئرلا طاقنلا:

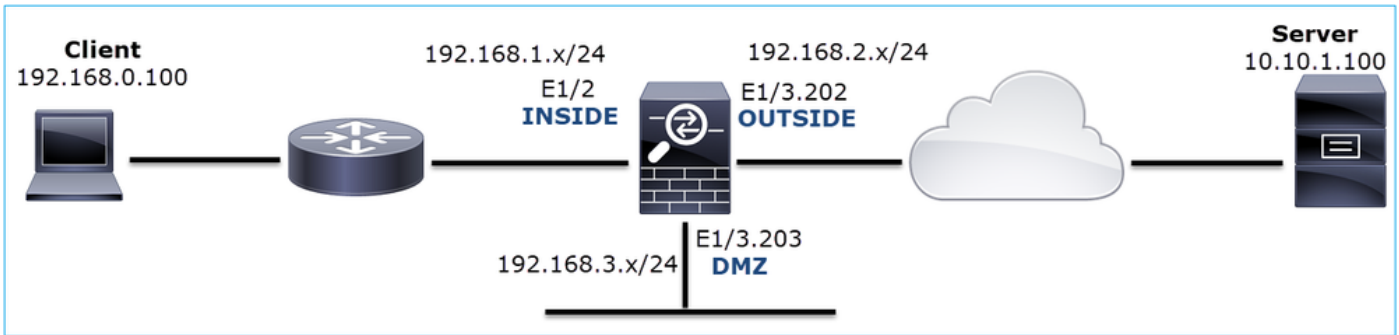
1. الوقعمو الئض قرافال نوئي نا دبال ،رخا ةيحان نمو .ةفلتخم ةينمزلاب واطلا .زاهجال لىل لمحل لثم ةمزلال لىل ةقبطملا ةسايسلا صخفو تازيمل لىل اذه دم تعي راج ةطساوب هتلازاهتفاضلا تمث dot1Q ساركانه ناك اذا ةصاخ مزلال لوط فلتخي دق .طقف دحاو بناج لىل ةيامحل
2. ةفلتخم MAC نيوانع .
3. ةيعرف ةهجاو لىل طاقنلالا مت اذا هنامك يف dot1Q سار نوئي نا نكمي .
4. لىل تقبظ (برض) ةمجرت ناو نع رسي او NAT ةلاحي يف فلتخم (نيوانع) ناو نع ip لىل .طب رلا .
5. طب رلا لىل تقبظ برض او NAT ةلاحي يف ءانيم فلتخم ةياغ او رصملا .
6. ماقرا نا ىرتس ف Wireshark ل ييسننلا لسلسنلا مقرر ايخ لي طعتب تمق اذا .مقرر ةيئاوشع ببسب ةيامحل راج ةطساوب اهلي دعت متي TCP رارقلا ماقرا لسلسنلا (IS) لي وائل لسلسنلا
7. لكشب ةيامحل راج لمعي ،لاثملا لي بس لىل .TCP تاراخي ضع ب قوف ةباتكل نكمي .ةئجت بنجت ل 1380 لىل (MSS) TCP عطقم مجحل لىل صقلا دحل ريغت لىل يضارثفا لىل .لقنلا راسم يف ةمزلال

ةهجولا دنع طاقنلاب مق 3. ءارجلا

نكمي ام برقأ طاقنلا ذخف انكمم اذه نكي مل اذا .اهسفن ةهجولا يف ةروص طقتلا ،نكمم نا زهجال دحاو نم او ةهجولا مداخله) TCP RST لسري يذلل نم نم ققحتلا وه انه فدهلا .ةهجولا لىل (راسملا يف رخالا

ةدحاو ةياهن ةطقن نم TCP 3-way + RST ءحفاصم 3. ةلءال

طءءملا ةروصللا هءه ضرعت



لمعي ال HTTP: ةلكشملا فصول

رءاءملا قفءءال

SRC IP: 192.168.0.100

DST IP: 10.10.1.100

لوكوءوربل: TCP 80

رسل ليلءء

مق FTD LINA ءرءم ىلع طاقءلالءا ءايللمع نءءمءب مق

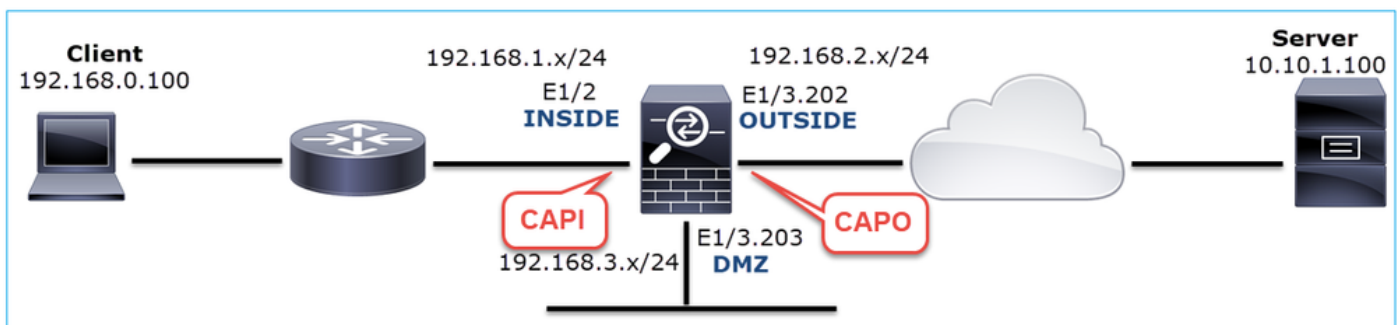
```
<#root>
```

```
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 - طاقءلال

طاقءلالءا ءايللمع يف رهظءا ءلءكشملا هءهل نءمء ناءءفلءءم ناءءقيرط ءانه

3.1 - لي م عمل نم ة لجؤم ال TCP 3-way + RST ة حفاصم -

ةروصلال ي ف حضوم وه امك ،اهسفن مزحل ال عل CAPO و CAPI عل ة ي امحل راج نم لك يوتحي.

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=179631962 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#1] 48295 → 80 [ACK] Seq=179631962 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=179631962 Ack=3838911938 Win=0 Len=0

ة يس يئرل طاقنل:

- ة ي امحل راج ربع TCP 3-way ة حفاصم رمت 1.
- SYN/ACK م داخ ل لسري 2.
- ماع طال نوبزل لسري 3.
- ه ي لسريو TCP RST لو كوتورب نع لي م عمل ال يلختي ،ة يناث 20 ي لاوح دع 4.

اهب ي صومل تاءارال

ة لاسم ال هذه قاطن قي ي ضت ة دايز وه عرفل اذه ي ة دراول تاءارال نم ضرغل او

ة ياهنل ي تطقن ي ل نكمي ام برقأ اروص طقتل 1. ءارال

هذه ي عل ي نبم اذهو . لي م عمل اب صاخ ال ACK ج ل اع ي مل م داخ ل نأ ي ل ة ي امحل راج تاطق ل ري شت قئ اقح ل:

- SYN/ACK م داخ ل لسري
- ماع طال نوبزل لسري
- تاناي ب ي ل بق FIN/ACK و TCP RST لي م عمل لسري

TCP لاصت ا دي كأت نم لي م عمل ال ACK ادبأ لصي مل . ة لك شم ال ي عل طاقن ل ال رهظي ي: ال ثل:

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...

3.2 - لجؤم ال RST + لي م عمل نم لجؤم ال سدك م ال/ة فن عزل ال TCP ل هاجت ال ة ي ثال ة حفاصم ال -

ةروصلال ي ف حضوم وه امك ،اهسفن مزحل ال عل CAPO و CAPI عل ة ي امحل راج نم لك يوتحي.

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	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	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	54	80 → 48299 [RST] Seq=808763520 Win=0 Len=0

ةيسئرلا طاقنلا:

1. ةيامحل راج ربع TCP 3-way ؤحفاصم رمت
2. ACK/ةفنن عز ليمعلا لسري ناوٲ 5 يلاوح دعب
3. هيل لسريو TCP RST عرضو نم مءاخال يهتني ،ةيناث 20 يلاوح دعب

ةيثالث TCP ؤحفاصم ءوؤو نم مءرلا يلع هنأب ؤاتنتسالا نكمي ،طاقنلالا اءه يلع ءانب ريشت) ءءاو ةياهن ةطقن يلع ؤقاواليا يف اهمامتا متي ال هنأ وءبي ،ةيامحل راج ربع ءاؤاإلا (كل ءى لاسرالا ءءاؤاى لملع

اهب يصوملا ءاءارءالا

3.1 ءلاؤال يف ءيشلال سفن

3.3 ليمعلا نم ءلؤؤملا TCP 3-way + RST ؤحفاصم

ءروصلال يف ؤضوم وه امك ،اهسفن مزؤال يلع CAPO و CAPI يلع ةيامحل راج نم لك يوتؤي

No.	Time	Source	Destination	Protocol	Length	Info
129	2019-10-13 17:09:20.513355	192.168.0.100	10.10.1.100	TCP	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	54	80 → 48355 [RST, ACK] Seq=2581697939 Ack=1633018699 Win=0 Len=0

ةيسئرلا طاقنلا:

1. ةيامحل راج ربع TCP 3-way ؤحفاصم رمت
2. هيل لسريو TCP RST لوؤوؤورب نع ليمعلا يلىؤتي ،ةيناث 20 يلاوح دعب

يلى ام ؤاتنتسالا نكمي ،روصلال هءه يلا اءانتساو

- لاصءالا ءاهن ررؤو ءءاو ةياهن ةطقن فقوؤت ،ةيناث 5-20 دعب

اهب يصوملا ءاءارءالا

3.1 ءلاؤال يف ءيشلال سفن

3.4 مءاخال نم يروفلا TCP + RST ل ءاؤاإلا ةيثالث ؤحفاصملا

ءروصلال يف ؤضوم وه امك ،مزؤال هءه يلع CAPO و CAPI يلع ةيامحل راج نم لك يوتؤي

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. ةيامحل راج ربع TCP 3-way ةحفاصم رمت .
2. ةينات ي للم ةعضبب ACK ةمزح دعب مداخل نم TCP RST كانه .

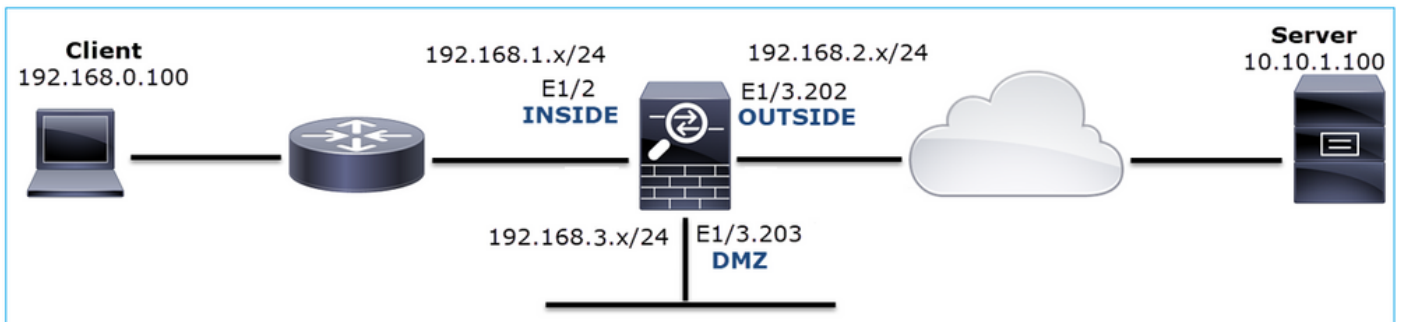
اهب يصوملا تاءارجلال

نالك مال ردق مداخل نم برقلاب روصلا طاقنلا :ءارجلال

TCP لسري يذلا راسملا ي ف زاهج وأ مداح دوجو ىل مداخل نم يروفلا TCP RST ريشي نأ نكمي RST. TCP RST ردصم ددجو هسفن مداخل ىلع طاقنلاب مق .

للمعمل نم TCP RST 4. ةلجال

طاطخملا ةروصولا هذه ضرعت:



HTTP للمعي ال :ةلكشملا فصو

رثأتملا قفدتلا

SRC IP: 192.168.0.100

DST IP: 10.10.1.100

لوكوتوربلا: TCP 80

رسأ ليلحت

FTD LINA كرحم ىلع طاقنلالا تاي للمع نيكم تب مق

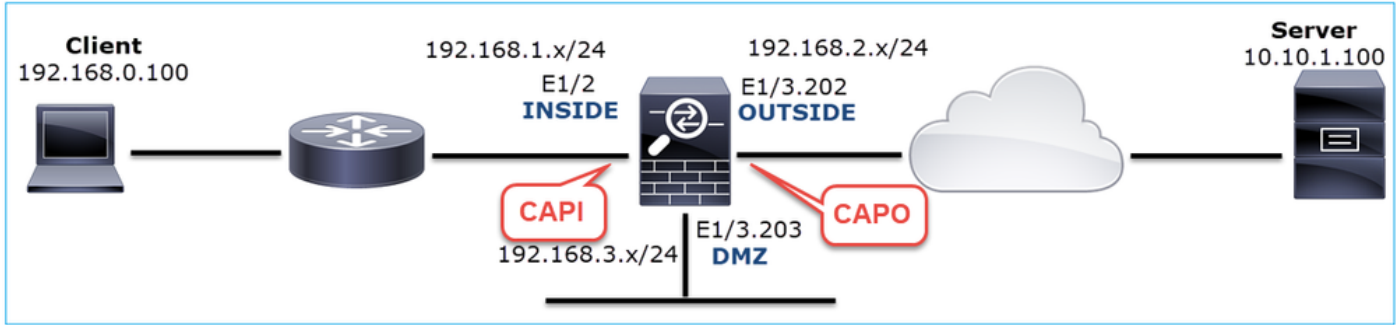
<#root>

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
```



لعمري ال ويراني س - طاقت ل

CAPI تايوت حم يه هذ

<#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

CAPO تايوت حم يه هذ

<#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 1386249852:138624985
2: 12:32:23.111429 802.1Q vlan#202 P0 192.168.0.100.47079 > 10.10.1.100.80: S 3000518857:300051885
3: 12:32:23.112405 802.1Q vlan#202 P0 192.168.0.100.47079 > 10.10.1.100.80: R 3514091874:351409187
4: 12:32:25.858125 802.1Q vlan#202 P0 192.168.0.100.47078 > 10.10.1.100.80: S 1386249852:138624985
5: 12:32:25.868729 802.1Q vlan#202 P0 192.168.0.100.47078 > 10.10.1.100.80: R 2968892337:296889233
6: 12:32:26.108240 802.1Q vlan#202 P0 192.168.0.100.47079 > 10.10.1.100.80: S 3822259745:382225974
7: 12:32:26.109094 802.1Q vlan#202 P0 192.168.0.100.47079 > 10.10.1.100.80: R 40865466:40865466(0)
8: 12:32:31.860062 802.1Q vlan#202 P0 192.168.0.100.47078 > 10.10.1.100.80: S 4294058752:429405875
9: 12:32:31.860917 802.1Q vlan#202 P0 192.168.0.100.47078 > 10.10.1.100.80: R 1581733941:158173394
10: 12:32:32.160102 802.1Q vlan#202 P0 192.168.0.100.47079 > 10.10.1.100.80: S 4284301197:428430119
11: 12:32:32.160971 802.1Q vlan#202 P0 192.168.0.100.47079 > 10.10.1.100.80: R 502906918:502906918(
11 packets shown
```

ةي امحل رادج 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 (
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 (
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 (
Oct 13 2019 13:57:45: %FTD-6-302014: Teardown TCP connection 4871 for INSIDE:192.168.0.100/47741 to OUT
```

ةي لخدال ةي امحل رادج ةه جاو ةل ل صي TCP RST دوجو ةل تالجس ل هذه ريشت

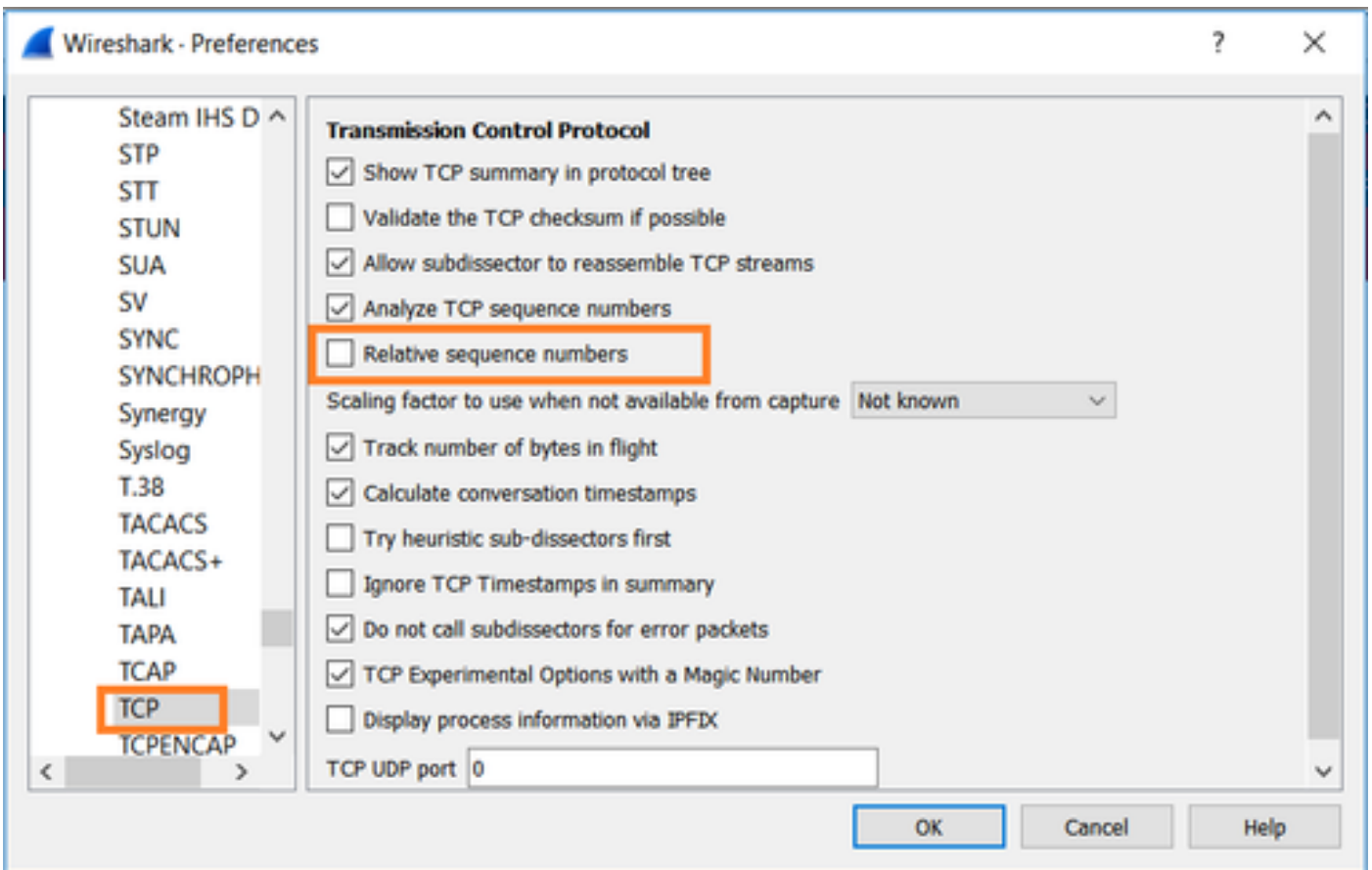
رسأ Wireshark في CAPI

ةروصل في حضورم وه امك، لوال TCP قفدت 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_P...
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_P...
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=1582642485 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=1582642485 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=1582642485 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

- 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
 - UDP Stream
 - SSL Stream
 - HTTP Stream
- Copy
- Protocol Preferences
- Decode As...
- Show Packet in New Window

مقارناً رايخ دي دحت يغل أو TCP > التالوك وتورب > التاليفضفت > ريرحت ىل لقتنا، Wireshark تحت ةروصل ي ف حضورم وه امك ةي بسنن ل لسلسلتا.



CAPI: طاقنن ل ي ف لوالا قفدنن ل تايوتحم ةروصل هذه رهظت

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 14:32:31.860902	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]

```

ةيسيرلرلا طاقنلا:

1. TCP syn ةمزح ليمعلا لسري.
2. TCP RST ةمزح ليمعلا لسري.
3. 4098574664 يواسل لسلسل مقرر ةميقي لىل TCP syn ةمزح يوتحت.

ىل CAPO طاقنلا ي قفدنلا سفن يوتحي:

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


```

> 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

```

ةيسيرلرلا طاقنلا:

1. IS ل ةيئاوشعلا ةيامحل راج TCP syn ةمزح ليمعلا لسري.
2. TCP RST ةمزح ليمعلا لسري.

يلى امجاتنلسا نكمي، نيحتحمللا لىل ادا نساو:

- مداخل او ليمعلا نيح هاجتلا ةيثالث TCP ةحفاصم دجوت ال.
- CAPI طاقنلا ي TCP RST لسلسل مقرر ةميقي. ليمعلا نم يتاى لىل TCP RST كانه ه 1386249853.

اهب ىصوملا تاءارجلال

ةلأسملا هذه قاطن قبيضت ةدايز وه عرفلا اذه يف ةدراولل تاءارجلا نم ضرغل او

ليعملل ام طاقنلاب عتمت 1. ءارجلا

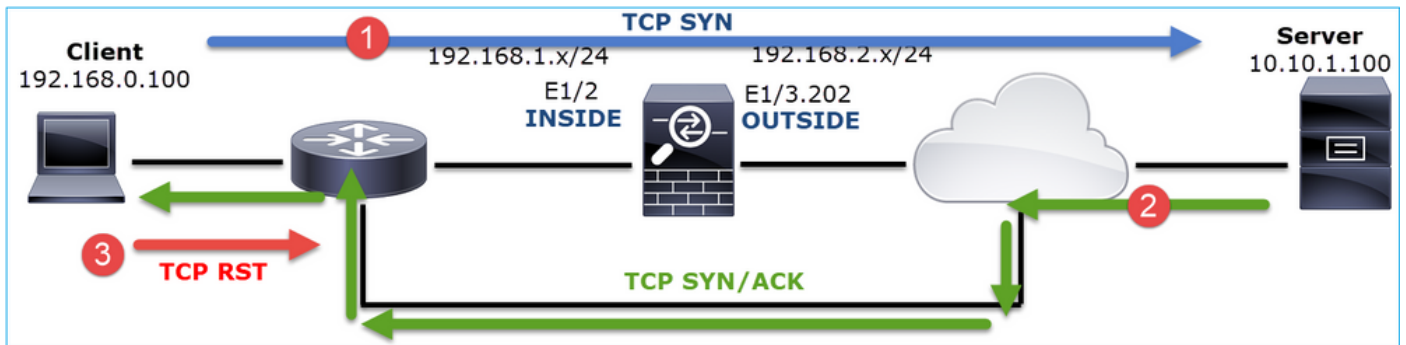
دوجو لىل يوق رشؤم كانه ، ةياملال راج لىل اعجم مت يلى طاقنلال تايلىم لىل اذانتسا
1386249853 ةمبيقب TCP RST لسري لىمعلل نأ ةقبيق لىل اذه دننسي . لثامتم ريغ قفدت
(يئوشعلال IS):

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 192 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=
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 W
31	9.048184	192.168.0.100	10.10.1.100	TCP	54	47078+80 [RST] Seq=1386249853 Win=0 Len=0

ةيسيرللا طاقنلا:

1. يري يذلا هسفن وهو 4098574664 وه لىلسلسنلا مقرلا TCP syn. ةمىح لىمعلل لسري .
ةيلخادلا ةهجالل يف ةياملال راج لىل ع (CAPI)
2. ببسب نوكي نأ عقتولال (ACK 1386249853 مقرب TCP SYN/ACK دجوي
randomization). ةياملال راج طاقنلال يف ةمىحلا هذه ةيؤرمتي مل .
3. هنكلو ، ACK 4098574665 مقرةمبيق عم SYN/ACK عقتو نأ ذنم TCP RST لىمعلل لسري .
1386249853 ةمبيق ملتسا

يلىلال وحننلا لىل كلذ لىلثمت نكميو:

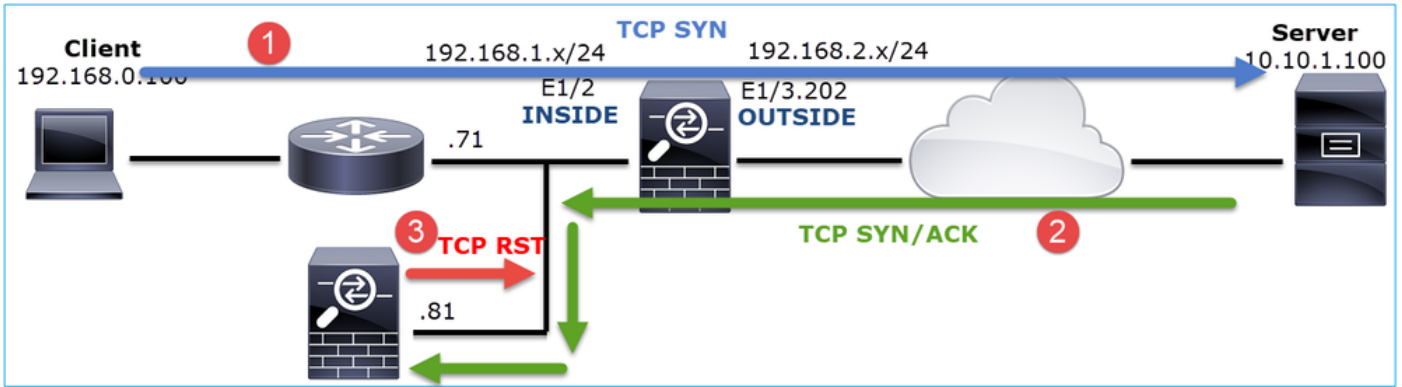


ةياملال راجو لىمعلل نيب هيجوتللا نم ققحت 2. ءارجلا

يلى ام ديكأت:

- ةعقتولال نيوانعلال يه طاقنلال تايلىم لىل اهتايؤرمت يلىل MAC نيوانعل .
- لثامتم لىمعلل ةياملال راج نيب هيجوتللا نأ نم دكأت .

هيجوت دوجو ءانثأ لىمعلل ةياملال راج نيب عقي زاهج نم RST يلىل اذانتسا هيجوتللا نيوانعل
ةروصلال يف ةيجذومن ةلاح رهظت . ةيلخادلا ةكبشلا لىل لثامتم ريغ



ردصم ال MAC ناونع ني ب قرف ال ظ حال . يوت حمل اذه يلع يوتحي طاقت الال اناف ، الال هذه ي في TCP syn/ACK: مزل ة هجول ال MAC ناونعو و TCP RST ب صال ال ردصم ال MAC ناونع لباق م TCP syn

<#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 ويران يسلال) عي طب TCP لقن 5. الال

:الشم ال فصول

دحلنا نم مغرلا ىلع . عيطب 10.77.19.11 و 10.11.4.171 ةفيضملا ةزهجالا نيب SFTP لقن
ناللا ، ةيناثلا يف تباجم 100 وه نيفيضملا نيب (BW) يددرتلا قاطنلا ضرعل ىنداللا
ةيناثلا يف تباجم 5 زواجتتال لقنلا ةعرس.

172.25.18.134 و 10.11.2.124 ةفيضملا ةزهجالا نيب لقنلا ةعرس نإف ، هسفن تقولا يفو
ريثكب كلذ نم ىلعأ.

ةيساسالا ةيرظنلا:

يددرتلا قاطنلا ريخأت جتنم ةطساوب دحاو TCP قفدتل ىوصقلا لقنلا ةعرس ديدحت متي
ةروصللا يف ةمدختسملا ةغيصللا ضرع متي (BDP).

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

انه دراوملا نم ققحت BDP لوح ليصافتلا نم ديزملا:

- [يف تباجم 1 طابترالا ىتح طوق ةيناثلا يف تباجم 10 كقيبطت مدختسي اذامل
ةيناثلا؟](#)
- [ىصقألا دحللا ىللا ةيامحللا رادج اءادأ ةدايز - مدقتم - BRKSEC-3021](#)

عيطب لاقنتا 1. ويرانيسلا

طاطخملا ةروصللا هذه ضرعت



رثأتملا قفدتلا:

SRC IP: 10.11.4.171

DST IP: 10.77.19.11 لوكوتورب

لوكوتوربلا: SFTP (FTP ربع SSH)

رسأ ليلحت

FTD LINA كرحم ىلع طاقتلالا نيكمت


<#root>

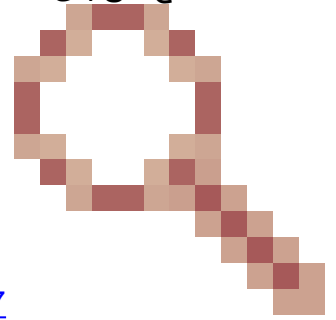
firepower#

```
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
```

 رورم لة كرح لقن لدعم ىلع FP1xxx و FP21xx طاقن لىل لىل LINA طاقن لىل رثؤت :ريذحت
و FP1xxx ةيساسأل ةمظنأل لىل لىل LINA طاقن لىل نيكم تب مقن لىل . FTD ربع رمت يلىل
ك لذنم ال دب . (FTD ربع عي طبل لىل لقن لىل) اهل صا و اءأل اءاخ فاشكتسأ دن ع FP21xxx
لىل ضبق لىل نأ لىل ةفاصل اب ةاأ HW Tap و نىل ماع دن نىل ةحس ف تلمعتسا



ق ب id [CSCvo30697](#) قى رادصل لىل تقو . فىضم ةياغو ردم لىل

<#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.

اهب ىصوم لىل تاءار لىل

ةلأسم لىل هذ قاطن قىيضى ةدايز وه عرف لىل اذ فى ةءاوا لىل تاءار لىل نم ضرغل او

(RTT) ةءو لىل باهذ لىل تقو باسح

ه: عبت او لقن لىل قفدت ددح ،الوأ

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	10.11.4.171	TCP	70	49680
3	0.000168	10.11.4.171	10.77.19.11	TCP	58	49680
4	0.077068	10.77.19.11	10.11.4.171	SSHv2	80	49680
5	0.000152	10.11.4.171	10.77.19.11	TCP	58	49680
6	0.000244	10.11.4.171	10.77.19.11	SSHv2	80	49680
7	0.071545	10.77.19.11	10.11.4.171	TCP	58	49680
8	0.000153	10.11.4.171	10.77.19.11	SSHv2	538	49680
9	0.041288	10.77.19.11	10.11.4.171	SSHv2	738	49680
10	0.000168	10.11.4.171	10.77.19.11	TCP	58	49680
11	0.030165	10.77.19.11	10.11.4.171	TCP	58	49680
12	0.000168	10.11.4.171	10.77.19.11	SSHv2	82	49680

نم اذهو. ةقباسلا ةضورعلم ةمزحل ذنم ين اوثل راهاظال Wireshark ضرع ةقيرط ريغت ب مق RTT باسح لي هس ت ه نأش:

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=0 Len=0
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
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=1737026596 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

ردصملا وحن امهدحاً) مزح لدابت يتي لمع ني ب تقولا ميق ةفاضلا لالخ نم RTT باسح نكمي لسراً يذل زاوجل او ةيامحل راجح ني ب RTT #2 ةمزحل ضرعت ، ةلاجل هذه يف . (ةهوجل وحن رخأل او ACK ةمزح لسراً يذل زاوجل او ةيامحل راجح ني ب RTT #3 ةمزحل ضرعت . (مداخل) SYN/ACK ةمزح لماشل RTT لوح اديج اري دقت ني مق رلا ةفاضل رفوت . (لي م عمل):

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=0 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=1737026596 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

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=1384 WS=1 SACK_PERM=1


```

> Frame 2: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> 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 نلعلأ يذلا صخشلا هنا نم دكأتو، مداخل اللى عروص طاقات لال ةجأ كانه، ةطقن ال هذه دنع (كلذب مايق ال ةيفيك ةفرعمل مداخل قئاتو عجار) هنيوكت دعأو 0 = ةذفان ال سايقم

عيرس لقن 2. ويرانيس ال

(اهسفن ةكبش ال ربع عيرس ال لقن ال) ديال ويرانيس ال صحن انعد نأل:

طاطخم ال:



مامتهال قفدت:

SRC IP: 10.11.2.124

DST IP: 172.25.18.134

لوكوتورب ال: SFTP (FTP ربع SSH)

FTD LINA كرحم اللى طاقات لال نيكتم

```
<#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
```

ة. ينات $RTT \approx 300$ نوكي، ةالال هذ ي: (RTT) ةدوالو باهذلا تقو باسح

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

7. مرق TCP ةذفان سايقم لماع نع مداخل نلعأ: TCP ةذفان مجح باسح

```

> 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]
  
```

تباب ≈ 1600000 مداخل TCP ةذفان مجح:

No.	Time	Source	Destination	Protocol	Length	Window size value	Calculated window size	Info
23...	0.002579	172.25.18.134	10.11.2.124	TCP	70	12854	1645312	22 → 57093 [FIN, ACK]
23...	0.266847	172.25.18.134	10.11.2.124	TCP	70	12854	1645312	22 → 57093 [ACK] Seq=
23...	0.268089	172.25.18.134	10.11.2.124	SSHv2	198	12854	1645312	Server: Encrypted pack
23...	0.000076	172.25.18.134	10.11.2.124	SSHv2	118	12854	1645312	Server: Encrypted pack
23...	0.000351	172.25.18.134	10.11.2.124	SSHv2	118	12854	1645312	Server: Encrypted pack
23...	0.000092	172.25.18.134	10.11.2.124	TCP	70	12854	1645312	22 → 57093 [ACK] Seq=
23...	0.000015	172.25.18.134	10.11.2.124	TCP	70	12854	1645312	22 → 57093 [ACK] Seq=
23...	0.000091	172.25.18.134	10.11.2.124	TCP	70	12854	1645312	22 → 57093 [ACK] Seq=

يل ي ام يددرتال قاطنل ريخأت تاجتنم ةغيص رفوت، ميقل هذه ل اذانتسا

ةيرظنل ل قنل ةرسل ل صقأل دحل ةيناثل ي ف تباچيم $160000 \times 8 / 0.3 = 43$

(2 ويرانيسال) عي طب TCP لقن 6. ةلحال

اى طب ةيامحال راج ربع (ليزنال) FTP فلم لقن نوكي :ةلكشمال فصو

طاطخمال ةروصلال هذه ضرعت



رثأتمال قفدتل

SRC IP: 192.168.2.220

DST IP: 192.168.1.220

لوكوتوربال: FTP

رسأ ليلحت

FTD LINA. كرحم ىلع طاقتلال تايلمع نيكم تب مق

```
<#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) طاقتلال ىلع FTP تانايب ةانق عبتاو FTP-Data ةمزح ددح

75	0.000412	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=1884231612 Ack=2670018383
76	0.000518	192.168.1.220	192.168.2.220	FTP-DATA	(PASV) (RETR file15mb)
77	0.000061	192.168.1.220	192.168.2.220	FTP-DATA	(PASV) (RETR file15mb)
78	0.000046	192.168.1.220	192.168.2.220	FTP-DATA	not captured] FTP Data: 124
79	0.000015	192.168.1.220	192.168.2.220	FTP-DATA	(PASV) (RETR file15mb)
80	0.000107	192.168.2.220	192.168.1.220	TCP	Seq=1884231612 Ack=2670019631
81	0.000092	192.168.2.220	192.168.1.220	TCP	Seq=1884231612 Ack=2670020879
82	0.000091	192.168.2.220	192.168.1.220	TCP	4494 → 2388 [ACK] Seq=188423
83	0.000015	192.168.2.220	192.168.1.220	TCP	4494 → 2388 [ACK] Seq=188423
84	0.000321	192.168.1.220	192.168.2.220	FTP-DATA	(PASV) (RETR file15mb)
85	0.000061	192.168.1.220	192.168.2.220	FTP-DATA	(PASV) (RETR file15mb)
86	0.000153	192.168.2.220	192.168.1.220	TCP	4494 → 2388 [ACK] Seq=188423
87	0.000122	192.168.2.220	192.168.1.220	TCP	4494 → 2388 [ACK] Seq=188423
88	0.918415	192.168.1.220	192.168.2.220	TCP	38 → 54494 [ACK] Seq=2670026
89	0.000397	192.168.2.220	192.168.1.220	TCP	Seq=2670027119
90	0.000869	192.168.1.220	192.168.2.220	FTP-DATA	(RETR file15mb)

FTP تاناي ب ق فدت يوتحم

26	0.000000	192.168.2.220	192.168.1.220	TCP	74 54494 → 2388 [SYN] Seq=1884231611 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSeq=3577289500 TSecr=0 WS=128
28	1.026564	192.168.2.220	192.168.1.220	TCP	74 [TCP Retransmission] 54494 → 2388 [SYN] Seq=1884231611 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSeq=3577289526 TSecr=0 WS=128
29	1.981594	192.168.1.220	192.168.2.220	TCP	74 2388 → 54494 [SYN, ACK] Seq=2669999678 Ack=1884231612 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 TSeq=4264384 TSecr=3577288500
30	0.000488	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=1884231612 Ack=2669999679 Win=29312 Len=0 TSeq=3577291508 TSecr=4264384
34	0.001617	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
35	0.000351	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=1884231612 Ack=2669999927 Win=32128 Len=0 TSeq=3577291510 TSecr=4264384
36	0.000458	192.168.1.220	192.168.2.220	FTP-DATA	1314 [TCP Previous segment not captured] FTP Data: 1248 bytes (PASV) (RETR file15mb)
37	0.000061	192.168.2.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
38	0.000198	192.168.2.220	192.168.1.220	TCP	78 [TCP Window Update] 54494 → 2388 [ACK] Seq=1884231612 Ack=2669999927 Win=35072 Len=0 TSeq=3577291511 TSecr=4264384 SLE=26699993423
39	0.000077	192.168.2.220	192.168.1.220	TCP	78 [TCP Window Update] 54494 → 2388 [ACK] Seq=1884231612 Ack=2669999927 Win=37888 Len=0 TSeq=3577291511 TSecr=4264384 SLE=26699994671
40	0.309906	192.168.1.220	192.168.2.220	TCP	1314 [TCP Out-Of-Order] 2388 → 54494 [ACK] Seq=2669999927 Ack=1884231612 Win=66048 Len=1248 TSeq=4264415 TSecr=3577291511
41	0.000488	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=1884231612 Ack=26699994671 Win=40832 Len=0 TSeq=3577291820 TSecr=4264415
42	0.000489	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
43	0.000045	192.168.1.220	192.168.2.220	FTP-DATA	1314 [TCP Previous segment not captured] FTP Data: 1248 bytes (PASV) (RETR file15mb)
44	0.000077	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
45	0.000244	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=1884231612 Ack=26699995919 Win=43776 Len=0 TSeq=3577291821 TSecr=4264415
46	0.000308	192.168.2.220	192.168.1.220	TCP	78 [TCP Window Update] 54494 → 2388 [ACK] Seq=1884231612 Ack=26699995919 Win=48768 Len=0 TSeq=3577291821 TSecr=4264415 SLE=26699997167 SRE=2669999663
47	0.000504	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
48	0.000259	192.168.2.220	192.168.1.220	TCP	78 [TCP Window Update] 54494 → 2388 [ACK] Seq=1884231612 Ack=26699995919 Win=51584 Len=0 TSeq=3577291822 TSecr=4264415 SLE=26699997167 SRE=2670000911
49	0.918126	192.168.1.220	192.168.2.220	TCP	1314 [TCP Out-Of-Order] 2388 → 54494 [ACK] Seq=26699995919 Ack=1884231612 Win=66048 Len=1248 TSeq=4264507 TSecr=3577291822
50	0.000900	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=1884231612 Ack=2670000911 Win=54528 Len=0 TSeq=3577292741 TSecr=4264507
51	0.000519	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
52	0.000061	192.168.2.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
53	0.000015	192.168.1.220	192.168.2.220	FTP-DATA	1314 [TCP Previous segment not captured] FTP Data: 1248 bytes (PASV) (RETR file15mb)
54	0.000015	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
55	0.000199	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=1884231612 Ack=2670002159 Win=57472 Len=0 TSeq=3577292742 TSecr=4264507
56	0.000229	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=1884231612 Ack=2670003407 Win=60288 Len=0 TSeq=3577292742 TSecr=4264507
57	0.000183	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
58	0.000106	192.168.2.220	192.168.1.220	TCP	78 [TCP Window Update] 54494 → 2388 [ACK] Seq=1884231612 Ack=2670003407 Win=65280 Len=0 TSeq=3577292742 TSecr=4264507 SLE=26700004655 SRE=26700007151
59	0.000168	192.168.2.220	192.168.1.220	TCP	78 [TCP Window Update] 54494 → 2388 [ACK] Seq=1884231612 Ack=2670003407 Win=68224 Len=0 TSeq=3577292743 TSecr=4264507 SLE=26700004655 SRE=26700008399
60	0.000000	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)

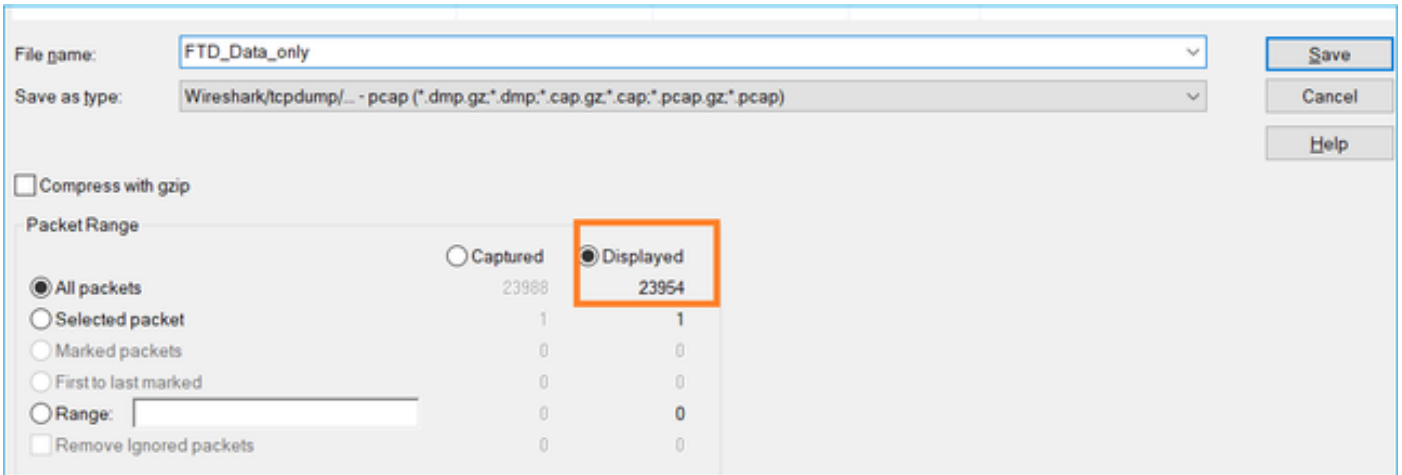
CAPO طاقن لاي يوتحم

31	0.000000	192.168.2.220	192.168.1.220	TCP	74 54494 → 2388 [SYN] Seq=2157030681 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSeq=3577288500 TSecr=0 WS=128
33	1.026534	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 TSeq=3577289526 TSecr=0 WS=128
34	1.981400	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 TSeq=4264384 TSecr=3577288500
35	0.000610	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=2157030682 Ack=2224316912 Win=29312 Len=0 TSeq=3577291508 TSecr=4264384
38	0.001328	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
40	0.000641	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=2157030682 Ack=2224318160 Win=32128 Len=0 TSeq=3577291510 TSecr=4264384
41	0.000381	192.168.1.220	192.168.2.220	FTP-DATA	1314 [TCP Previous segment not captured] FTP Data: 1248 bytes (PASV) (RETR file15mb)
42	0.000046	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
43	0.000290	192.168.2.220	192.168.1.220	TCP	78 [TCP Window Update] 54494 → 2388 [ACK] Seq=2157030682 Ack=2224318160 Win=35072 Len=0 TSeq=3577291511 TSecr=4264384 SLE=2224319408 SRE=2224320656
44	0.000076	192.168.2.220	192.168.1.220	TCP	78 [TCP Window Update] 54494 → 2388 [ACK] Seq=2157030682 Ack=2224318160 Win=37888 Len=0 TSeq=3577291511 TSecr=4264384 SLE=2224319408 SRE=2224321904
45	0.309905	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 TSeq=4264415 TSecr=3577291511
46	0.000590	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=2157030682 Ack=2224321904 Win=40832 Len=0 TSeq=3577291820 TSecr=4264415
47	0.000512	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
48	0.000061	192.168.1.220	192.168.2.220	FTP-DATA	1314 [TCP Previous segment not captured] FTP Data: 1248 bytes (PASV) (RETR file15mb)
49	0.000076	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
50	0.000290	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=2157030682 Ack=2224323152 Win=43776 Len=0 TSeq=3577291821 TSecr=4264415
51	0.000046	192.168.2.220	192.168.1.220	TCP	78 [TCP Window Update] 54494 → 2388 [ACK] Seq=2157030682 Ack=2224323152 Win=48768 Len=0 TSeq=3577291821 TSecr=4264415 SLE=2224324400 SRE=2224326896
52	0.000412	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
53	0.000351	192.168.2.220	192.168.1.220	TCP	78 [TCP Window Update] 54494 → 2388 [ACK] Seq=2157030682 Ack=2224323152 Win=51584 Len=0 TSeq=3577291822 TSecr=4264415 SLE=2224324400 SRE=2224328144
54	0.918019	192.168.1.220	192.168.2.220	TCP	1314 [TCP Out-Of-Order] 2388 → 54494 [ACK] Seq=2224323152 Ack=2157030682 Win=66048 Len=1248 TSeq=4264507 TSecr=3577291822
55	0.001007	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=2157030682 Ack=2224328144 Win=54528 Len=0 TSeq=3577292741 TSecr=4264507
56	0.000457	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
57	0.000061	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
58	0.000016	192.168.1.220	192.168.2.220	FTP-DATA	1314 [TCP Previous segment not captured] FTP Data: 1248 bytes (PASV) (RETR file15mb)
59	0.000000	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
60	0.000274	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=2157030682 Ack=2224329392 Win=57472 Len=0 TSeq=3577292742 TSecr=4264507
61	0.000214	192.168.2.220	192.168.1.220	TCP	66 54494 → 2388 [ACK] Seq=2157030682 Ack=2224330640 Win=60288 Len=0 TSeq=3577292742 TSecr=4264507
62	0.000122	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)
63	0.000168	192.168.2.220	192.168.1.220	TCP	78 [TCP Window Update] 54494 → 2388 [ACK] Seq=2157030682 Ack=2224330640 Win=65280 Len=0 TSeq=3577292742 TSecr=4264507 SLE=2224331888 SRE=2224334384
64	0.000107	192.168.1.220	192.168.2.220	FTP-DATA	1314 FTP Data: 1248 bytes (PASV) (RETR file15mb)

ةيس يئر لاي طاقن لاي

1. (OOO) ب يترت لاي چراخ TCP مزح كانه.
2. TCP لاسر لاي ةدايع كانه.
3. (ةطقس م لاي مزح لاي) ةمزح نادق ف ي لاي ةراش كانه.

طاقن طفاح م. ةددم لاي مزح لاي ري دصت > فلم ي لاي كلقنت ءانثا روص لاي طفاح :ح ي م لاي



اهب ى صوملا تاءارجال

ة. لأسملا هذه قاطن قىيىضت ةدايز وه عرفلا اذه يف ةدراول تاءارجال نم ضرغلاو

ةمزال نادقف ع قوم دىحت 1. اءارجال

قرف ةيجهنم مادختساو ةنمازتم طاقنلا تاي لمع طاقنلا كىل ع بجى ،هذه لثم تالاح يف نم و. ةمزال نادقف يف ببستت يتيلا ةكبشلا (عطاقم) عطقم دىحتل بلغللاو لاصتالا ةسىئر تاهويرانىس ةثالث كانه ةيامحلا راج رطن ةهجو:

1. هسفن ةيامحلا راج ىلا ةمزال دقف ع جري
2. ىلا مداخل نم هاجت) ةيامحلا راج زاهج ىلا تاناي بلا قفدت ةمزال دقف نع جتنى (للمعلا).
3. (مدخال ىلا للمعلا نم هاجت) ةيامحلا راج زاهج ىلا قفدت ةمزال دقف نع جتنى.

ال مأ ةيامحلا راج ببسب ةمزال دقف ناك اذا ام دىحتل :ةيامحلا راج نع مچانلا ةمزال دقف نيتقيرط ةنراقم ل ةريثك قرط كانه .جرحملا طاقنلاب لخدملا طاقنلا ةنراقم ل ةجاج كانه ةمهملا هذبه مايقلل ةدحاو ةقيرط مسقلا اذه حضوي .نيتفلتخم

ةمزال نادقف دىحتل نيتروص ةنراقم اءارجال

نوكت ال بجى هنأ ينعي اذه .ةذفان تقو هسفن ل نم طبر ءاوتح 2 ل نأ تنمض 1. ةوطخلا قرطلا نم لىلق ددع كانه و. رخال طاقنلال دعب وأ لبق هطاقنلا مت دحاو طاقنلا يف مزح كانه :ةيال هذه قىقحتل

- ةمزال ةريخال او ىلوالا (ID) IP فىرعت ميق نم ققحت
- ةريخال او ىلوالا ةمزال ىنمزال ع باطل ميق نم ققحت

IP فرعم ميق سفن اهل طاقنلا لك نم ىلوالا مزال نأ ىرت نأ كنكمى ،لاثملا اذه يف

No.	Time	Source	Destination	Protocol	Length	Identification	Info
1	2019-10-16 16:13:44.169394	192.168.2.220	192.168.1.220	TCP	74	0xb0a34 (2612)	54494 → 2388 [SYN] Seq=1884231611 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3577289526 TSecr=0 WS=128
2	2019-10-16 16:13:45.195958	192.168.2.220	192.168.1.220	TCP	74	0xb0a35 (2613)	[TCP Retransmission] 54494 → 2388 [SYN] Seq=1884231611 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3577289526 TSecr=0 WS=128
3	2019-10-16 16:13:47.177542	192.168.1.220	192.168.2.220	TCP	74	0x151f (5407)	2388 → 54494 [SYN, ACK] Seq=2669989678 Ack=1884231612 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 TSval=4264384 TSecr=3577288500
4	2019-10-16 16:13:47.178030	192.168.2.220	192.168.1.220	TCP	66	0xb0a36 (2614)	54494 → 2388 [ACK] Seq=1884231612 Ack=2669989678 Win=0 Len=0
5	2019-10-16 16:13:47.179647	192.168.1.220	192.168.2.220	TCP	1314	0x1521 (5409)	2388 → 54494 [ACK] Seq=2669989678 Ack=1884231612 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 TSval=4264384 TSecr=3577288500
6	2019-10-16 16:13:47.179998	192.168.2.220	192.168.1.220	TCP	66	0xb0a37 (2615)	54494 → 2388 [ACK] Seq=1884231612 Ack=2669989678 Win=0 Len=0
7	2019-10-16 16:13:47.180456	192.168.1.220	192.168.2.220	TCP	1314	0x1522 (5411)	2388 → 54494 [ACK] Seq=2669989678 Ack=1884231612 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 TSval=4264384 TSecr=3577288500
8	2019-10-16 16:13:47.180957	192.168.1.220	192.168.2.220	TCP	1314	0x1524 (5412)	2388 → 54494 [ACK] Seq=2669989678 Ack=1884231612 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 TSval=4264384 TSecr=3577288500
9	2019-10-16 16:13:47.180715	192.168.2.220	192.168.1.220	TCP	78	0xb0a38 (2616)	54494 → 2388 [ACK] Seq=1884231612 Ack=2669989678 Win=0 Len=0
10	2019-10-16 16:13:47.180792	192.168.2.220	192.168.1.220	TCP	78	0xb0a39 (2617)	54494 → 2388 [ACK] Seq=1884231612 Ack=2669989678 Win=0 Len=0
11	2019-10-16 16:13:47.498988	192.168.1.220	192.168.2.220	TCP	1314	0x1525 (5413)	2388 → 54494 [ACK] Seq=2669989678 Ack=1884231612 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 TSval=4264384 TSecr=3577288500
12	2019-10-16 16:13:47.499076	192.168.2.220	192.168.1.220	TCP	66	0xb0a3a (2618)	54494 → 2388 [ACK] Seq=1884231612 Ack=2669989678 Win=0 Len=0
13	2019-10-16 16:13:47.499065	192.168.1.220	192.168.2.220	TCP	1314	0x1526 (5414)	2388 → 54494 [ACK] Seq=2669989678 Ack=1884231612 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 TSval=4264384 TSecr=3577288500
14	2019-10-16 16:13:47.499210	192.168.2.220	192.168.1.220	TCP	1314	0x1527 (5415)	54494 → 2388 [ACK] Seq=1884231612 Ack=2669989678 Win=0 Len=0
15	2019-10-16 16:13:47.499097	192.168.1.220	192.168.2.220	TCP	1314	0x1529 (5417)	2388 → 54494 [ACK] Seq=2669989678 Ack=1884231612 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 TSval=4264384 TSecr=3577288500
16	2019-10-16 16:13:47.491231	192.168.2.220	192.168.1.220	TCP	66	0xb0a3b (2619)	54494 → 2388 [ACK] Seq=1884231612 Ack=2669989678 Win=0 Len=0
17	2019-10-16 16:13:47.491261	192.168.2.220	192.168.1.220	TCP	78	0xb0a3c (2620)	54494 → 2388 [ACK] Seq=1884231612 Ack=2669989678 Win=0 Len=0
18	2019-10-16 16:13:47.491765	192.168.1.220	192.168.2.220	TCP	1314	0x152a (5418)	2388 → 54494 [ACK] Seq=2669989678 Ack=1884231612 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 TSval=4264384 TSecr=3577288500
19	2019-10-16 16:13:47.492024	192.168.2.220	192.168.1.220	TCP	78	0xb0a3d (2621)	54494 → 2388 [ACK] Seq=1884231612 Ack=2669989678 Win=0 Len=0
20	2019-10-16 16:13:48.410150	192.168.1.220	192.168.2.220	TCP	1314	0x152e (5422)	2388 → 54494 [ACK] Seq=2669989678 Ack=1884231612 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 TSval=4264384 TSecr=3577288500
21	2019-10-16 16:13:48.411050	192.168.2.220	192.168.1.220	TCP	66	0xb0a3e (2622)	54494 → 2388 [ACK] Seq=1884231612 Ack=2669989678 Win=0 Len=0
22	2019-10-16 16:13:48.411569	192.168.1.220	192.168.2.220	TCP	1314	0x152f (5423)	2388 → 54494 [ACK] Seq=2669989678 Ack=1884231612 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 TSval=4264384 TSecr=3577288500
23	2019-10-16 16:13:48.411630	192.168.2.220	192.168.1.220	TCP	1314	0x1530 (5424)	54494 → 2388 [ACK] Seq=1884231612 Ack=2669989678 Win=0 Len=0
24	2019-10-16 16:13:48.411660	192.168.1.220	192.168.2.220	TCP	1314	0x1532 (5426)	2388 → 54494 [ACK] Seq=2669989678 Ack=1884231612 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1 TSval=4264384 TSecr=3577288500
25	2019-10-16 16:13:48.411660	192.168.2.220	192.168.1.220	TCP	1314	0x1533 (5427)	54494 → 2388 [ACK] Seq=1884231612 Ack=2669989678 Win=0 Len=0
26	2019-10-16 16:13:48.411859	192.168.2.220	192.168.1.220	TCP	66	0xb0a3f (2623)	54494 → 2388 [ACK] Seq=1884231612 Ack=2669989678 Win=0 Len=0
27	2019-10-16 16:13:48.412088	192.168.1.220	192.168.2.220	TCP	66	0xb0a40 (2624)	54494 → 2388 [ACK] Seq=1884231612 Ack=2669989678 Win=0 Len=0

نیهباشتم ریغ اوناک اذا ام قلاح یف

1. طاققتالک نم یلوالا ؤمزجال نم ؤینمزل عباوطلال نراق .
2. متخ حشرم ریغت هنم حشرم یلع لوصحلال تقو متخ شذحأ م ادختساب طاققتالال نم .
لاثمل لیبس یلع ، (ؤریخال ؤمزجال) <= و (یلوالا ؤمزجال) >= یل == نم تقولال

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-16 16:13:43.244692	192.168.2.220	192.168.1.220	TCP	74	38400 → 21 [S
2	2019-10-16 16:13:43.245638	192.168.1.220	192.168.2.220	TCP	74	21 → 38400 [S
3	2019-10-16 16:13:43.245867	192.168.2.220	192.168.1.220	TCP	66	38400 → 21 [A

> Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Oct 16, 2019 16:13:43.245638000 Central European Daylight Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1571235223.245638000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.000000000 seconds]

Frame Number: 2

Frame Length: 74 bytes (592 bits)

Capture Length: 74 bytes (592 bits)

(frame.time >= "2019 رپوتكأ 16 2019 16:13:43.244692000") & (frame.time <= "2019 رپوتكأ 16 2019 16:20:21.78513000")

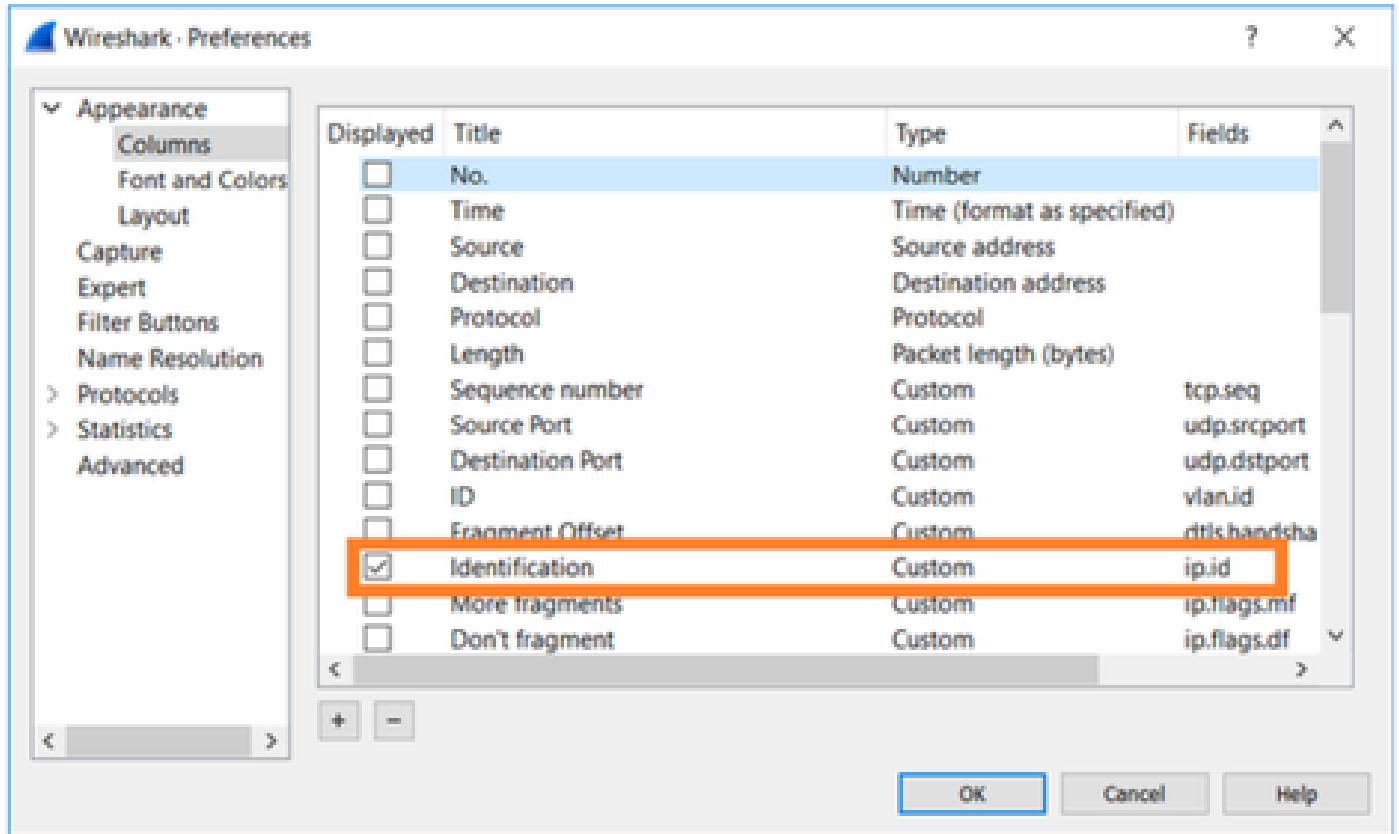
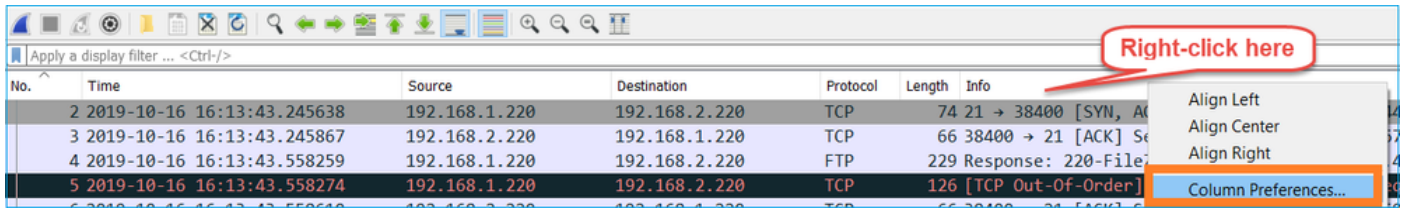
3. مزجال ظفح مٹ ؤدحمال مزجال ریصدت > فلم ددح ، دیج طاققتالال یل ؤدحمال مزجال ریصدت .
ینمزل راطالال یطغت مزح یلع طاققتالال الکی یوتحی نأ بجی ، ؤطقنلال هذہ دنع . ؤضورعمال
نینتطقنلال ؤنراقم ؤدب نآلال کنکم ی . هسفن

لوقجال لاثم . 2. نیتطقنلال لیبس یلع ؤنراقم ل م ادختساب متی یذلا ؤمزجال لوقح ددح . 2. ؤوطخلال
هام ادختساب نکم ی تلال:

- IP فی رعت
- RTP لسلست مقرر
- ICMP ل لسلستال مقررال

یف اهدی دحتب تمق ؤمزح لکل لوقجال یلع یوتحی طاققتالال لکم نم یصن رادصل عاشناب مق
ؤنراقم دیرت تنک اذا ، لاثمال لیبس یلع ، امامتالال دومع طقف کرتأ ، کلذب مایقنلال . 1. ؤوطخلال

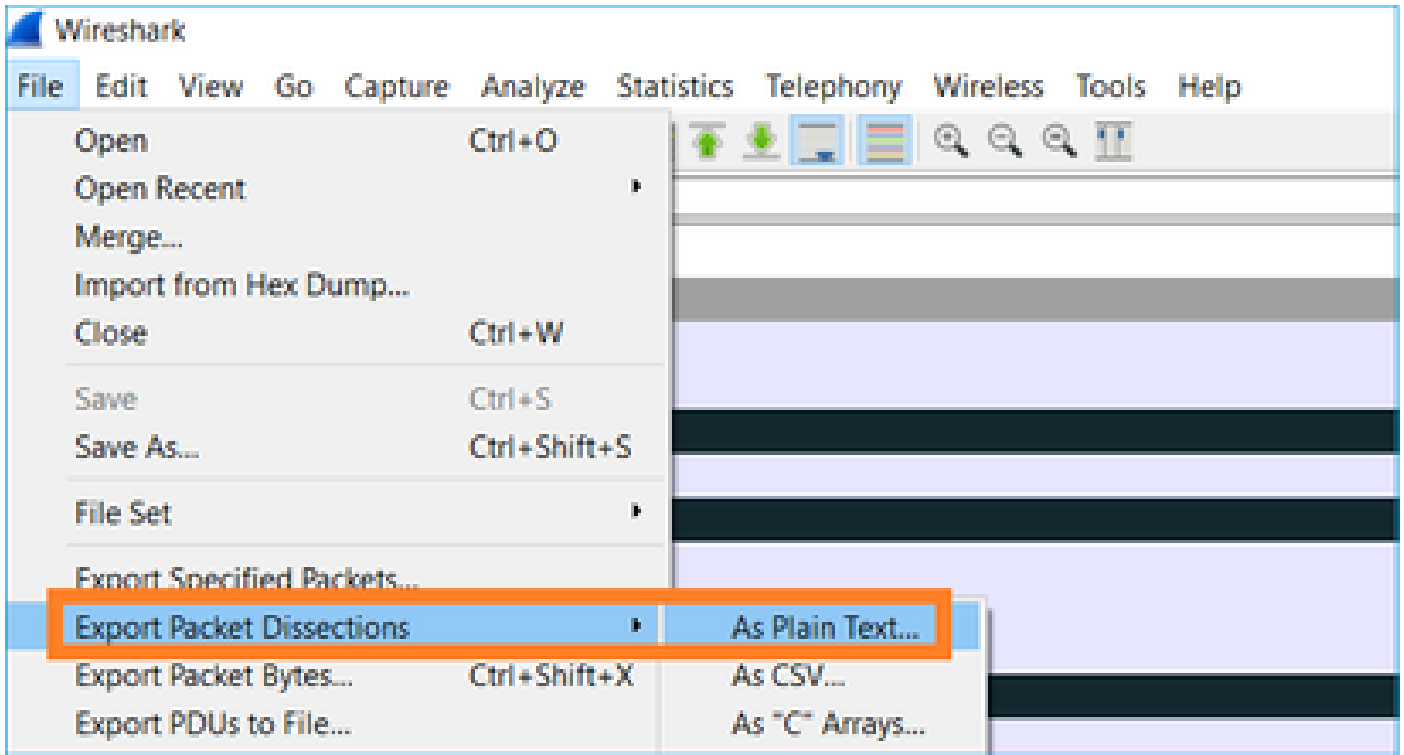
ةروصل اليف حضورم وه امك طاقتلالال ليدعتب مق مث IP فيرعت لىلع اءانب مزحلل



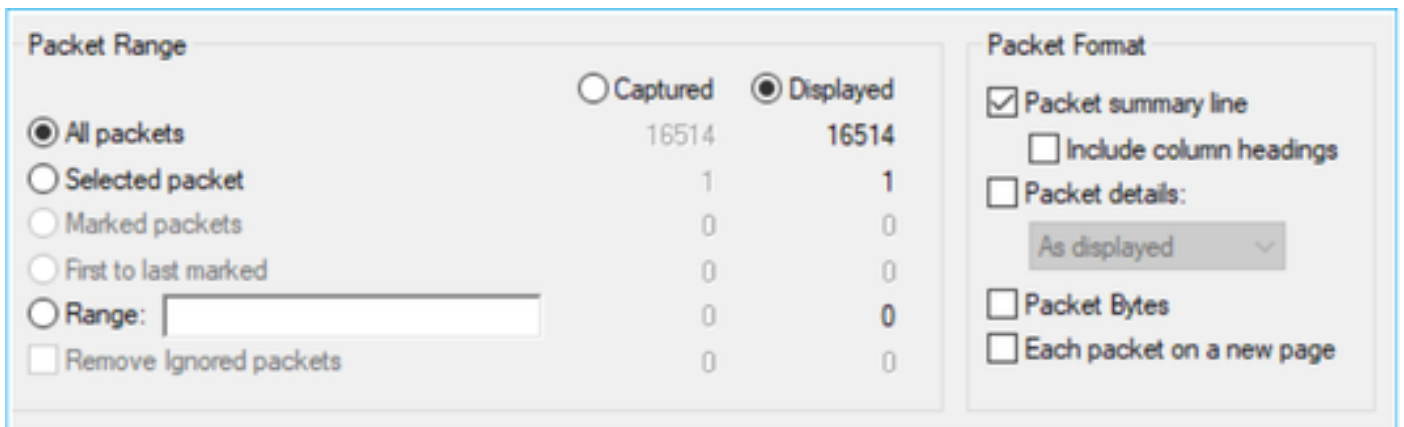
ةحيتلل:

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)
0xfdba (64954)
0x151c (5404)
0xfdbb (64955)
0x151d (5405)
0x0a34 (2612)
0xfdbc (64956)
0x0a35 (2613)
0x151f (5407)
0x0a36 (2614)
<ul style="list-style-type: none"> Frame 23988: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) <ul style="list-style-type: none"> Encapsulation type: Ethernet (1) <ul style="list-style-type: none"> Arrival Time: Oct 16, 2019 16:20:21.785130000 Central European Daylight Time

صنك > مزحل تاميسقت ريصت > فلم) طاقتلالا نم صن رادصا عاشناب مق 3. ةوطخال
ةروصلال يف حضوم وه امك، (...يديع



لحلل ميق ري دصتلة مزحلل لي صافات ودمع ال س وور نيمضت تاريخ دي دجت اعلا اب مق
ة: روصال يف حضورم وه امك ،طقف ضرورع الم



ك: لذب مايقلل سكونيل زرف رم امدختسا كنكمي . اتالمال يف مزحلل بيترت 4. ةوطخل

```
<#root>
```

```
#
```

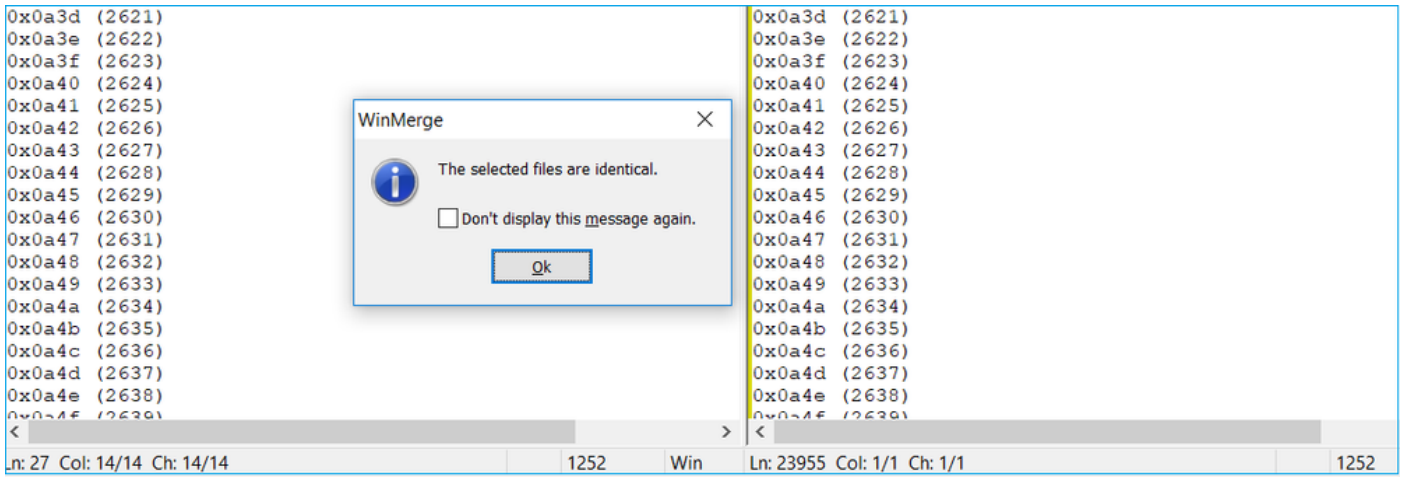
```
sort CAPI_IDs > file1.sorted
```

```
#
```

```
sort CAPO_IDs > file2.sorted
```

روثعلل Linux diff رم أو (WinMerge، لالمال ليبس يلع) صوصن ةنراقم ةادأ مدختسا 5. ةوطخل

2. روصال ني ب قورفال لىل



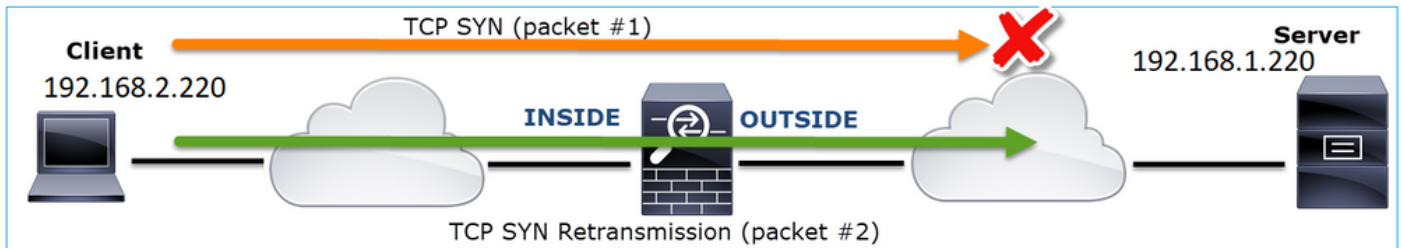
نأ تبثي اذه .ني قباطم FTP تاناي ب رورم ةكحل CAPO و CAPI طاقتلل نوكي ،ةلحال هذه في ةيامحل رادج ببسب نكي مل ةمزلل نادق.

تاناي بلل قفدت/قفت مزح نادق لىل فرعتللا

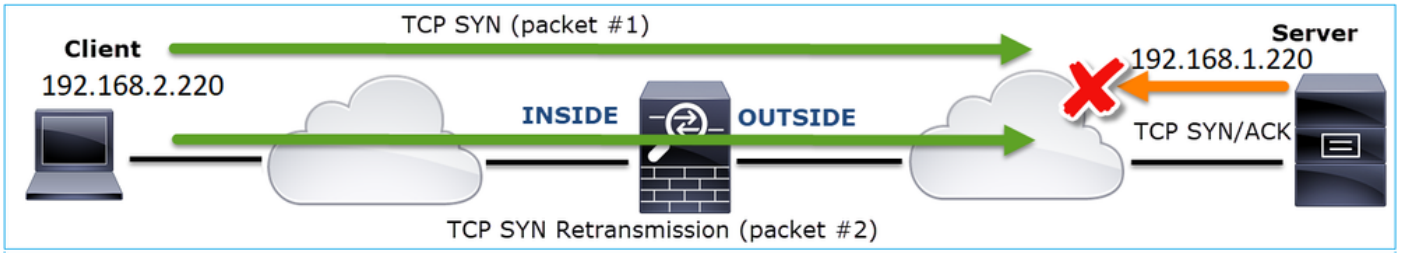
No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-16 16:13:44.169516	192.168.2.220	192.168.1.220	TCP	74	54494 → 2388 [SYN] Seq=2157030681 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3577288500 TSecr=0 WS=1
2	2019-10-16 16:13:45.196090	192.168.2.220	192.168.1.220	TCP	74	[TCP Retransmission] 54494 → 2388 [SYN] Seq=2157030681 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3577288500 TSecr=0 WS=1
3	2019-10-16 16:13:47.177450	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=3577291508 TSecr=3577291508
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 TSecr=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 TSecr=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 TSecr=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=4264415 TSecr=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 TSecr=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 TSecr=4264415
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 TSecr=4264415
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 TSecr=3577291510
12	2019-10-16 16:13:47.490407	192.168.2.220	192.168.1.220	TCP	66	54494 → 2388 [ACK] Seq=2157030682 Ack=2224321904 Win=40832 Len=0 TSval=3577291820 TSecr=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 TSecr=3577291820
14	2019-10-16 16:13:47.490880	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 TSecr=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 TSecr=3577291820
16	2019-10-16 16:13:47.491246	192.168.2.220	192.168.1.220	TCP	66	54494 → 2388 [ACK] Seq=2157030682 Ack=2224323152 Win=43776 Len=0 TSval=3577291821 TSecr=4264415

ةسئللا طاقنلا

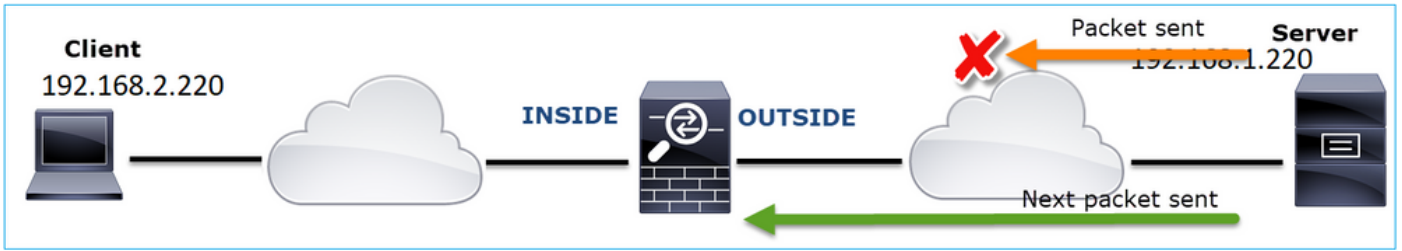
نم اهل اسرا م تي TCP syn ةمزل اهنا ف ،صوصللا هجو لىل و TCP لاسرا ةداعل يه ةمزلل هذه 1. تنأو طبرلا ديعي لىل مزل نأ امب .لملخال عضولا في FTP تاناي بلل مداخل لىل لىل مزل ال ةيامحل رادج لىل مداخل وحن تدق طبرلا (#1 طبر) لىل سىل تىر عىطتسي



دق SYN/ACK ةمزل نكلو ،مداخل لىل تلصو دق SYN ةمزل نوك نأ لامتخا كانه ،ةلحال هذه في عو جزللا قىرط في تدق:



هناك طاقول/هضرع متي مل قبا سلا عطقملا نأ يلى ع Wireshark فرعتو مداخل نم ةمزح كانه 2. في اهتيؤر متي ملو لي معلي الى مداخل نم ةطقملا ريغ ةمزحلا لاسرا مت هنأل ارطن ةياملحلا رادجو مداخل نيب تدقف دق ةمزحلا نأ ينعي اذهف ، ةياملحلا رادج طاقول



ةياملحلا رادجو FTP مداخل نيب مزح نادقف دوجو يلى ريشي اذهو

ةيفاضا روص طاقول 2. عارجلال

ميسقتلا ةقيرط قيبطت لواح . ةياهنلا طاقن دنع تاطول عم ةيفاضا تاطول ذخأ مق ةمزحلا نادقف ببسي يذلا لكاش ملل ريثملا عطقملا نم ديزملا لزلع بلغللاو

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	70	[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..	1314	FTP Data: 1248 bytes (PASV) (RETR file15mb)
164	2019-10-16 16:13:51.751378	192.168.2.220	192.168.1.220	TCP	70	[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	70	[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..	1314	[TCP Fast Retransmission] FTP Data: 1248 bytes (PASV) (RETR file15mb)

> Frame 167: 1314 bytes on wire (10512 bits), 1314 bytes captured (10512 bits) on interface 0
 > Ethernet II, Src: Vmware_30:2b:78 (00:0c:29:30:2b: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: 494, 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)

ةيسيرلا طاقول:

1. ةدراول TCP لسلسلت ماقراً (ةلاجل هذه في FTP لي مع) لبقت سمل عبت تي عاشن اب موقت انه نإف ، (عقوتم لسلسلت مقري طخت مت) اهدقف مت دق ةمزح نأ تفشتك اذم اذ في . هيطخت مت عقوتم لسلسلت مقرب ACK ةمزح لاسرالا ةداع) TCP لوكوت وربل عيرسلا لاسرالا ةداع لي غشتب (ACK) DUP ةركاذ موقت
- 2.

(ACK). رر كم يقلت دع ب ة ناث 20 لال خ

ة رر كم ل تاب ج و ل ا ه ي ن ع ت ي ذ ل ا م

- ن م ه ن ا ل ل ة ل ع ف ل ا س ر ا ة د ا ع ا ت ا ي ل م ع د ج و ت ا ل ن ك ل و ة ر ر ك م ل ا A C K ع ا و ن ا ض ع ب ر ي ش ت م ا ط ن ل ل ج ر ا خ ل ص ت م ز ح ك ا ن ه ن ا ج ر ا ل ا
- م ر د ق د و ج و ل ل ة ل ع ف ل ا ل ا س ر ا ل ا ة د ا ع ا ت ا ي ل م ع ا ه ي ل ت ي ت ل ا ة ر R ك م ل ا A C K ل ل ا س ر ر ي ش ت م ز ح ل ا ن ا د ق ف ن م

ل. ل ق ن ل ل م ز ح ل ة ي ا م ح ل ر ا د ج ة ج ل ا م ت ق و ب ا س ح 3. ا ج ا ل ا

ن ي ت ف ل ت خ م ن ي ت ه ج ا و ل ع ط ا ق ت ل ل ا ل س ف ن ق ي ب ط ت

```
<#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
```

ط ب ر ج ر خ م ل ب ا ق م ل خ د م ن ي ب ت ق و ل ا ق ر ف ن م ق ق ح ت ط ا ق ت ل ل ا ل ر ي د ص ت

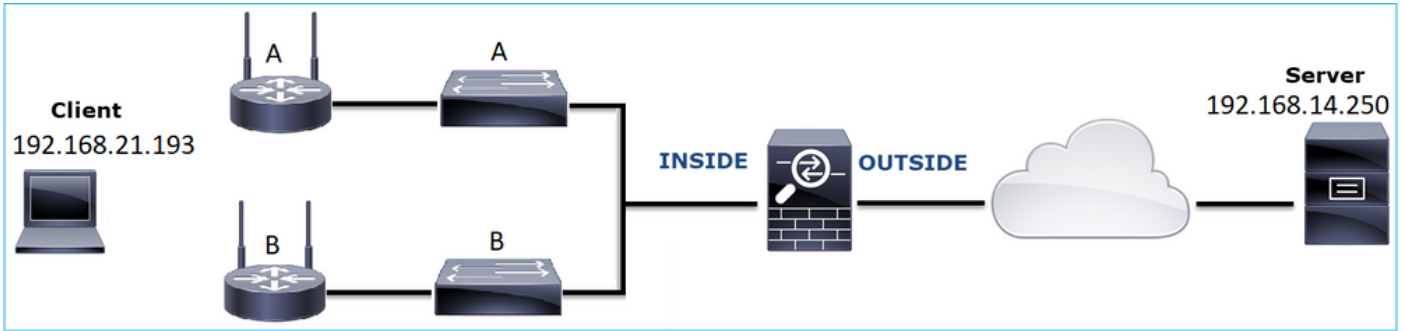
(ة م ز ح ل ا ف ل ت) T C P ل ا ص ت ا ة ل ك ش م 7. ة ل ا ح ل ا

ة ل ك ش م ل ا ف ص و

(HTTP - 192.168.14.250) ة ه ج و م د ا خ ب ل ا ص ت ا ل ا (192.168.21.193) ي ك ل س ا ل ل ا ل ي م ع ل ل ل و ا ح ي ن ا ف ل ت خ م ن ا ه و ي ر ا ن ي س ك ا ن ه و

- HTTP ل ا ص ت ا ل م ع ي ا ل ذ ئ د ن ع 'A' (AP) ل و ص و ل ا ة ط ق ن ب ل ي م ع ل ل ا ل ص ت ي ا م د ن ع
- HTTP ل ا ص ت ا ل م ع ي ا ل ذ ئ د ن ع 'B' (AP) ل و ص و ل ا ة ط ق ن ب ل ي م ع ل ل ا ل ص ت ي ا م د ن ع

ط ا ط خ م ل ا ة ر و ص ل ا ه ذ ه ض ر ع ت



رثأت الما ق ف د لتال:

SRC IP: 192.168.21.193

DST IP: 192.168.14.250

لوكوت و ر ب ل: TCP 80

رسأ ل ل ح ت

FTD LINA ك رح م ى ل ع طاق ت ل ل ال ن ي ك م ت:

<#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
```

ى ف ي ط و ل و ي ر ن ي س ل ل - طاق ت ل ل

ا د ي ج ف و ر ع م و ي ر ن ي س ن م ت ا ط ق ل ى ل ع ل و ص ح ل ا م ئ ا د ج د ي ف م ل ن م ، س ا س ا ط ك

ه ه ج ا و طاق ت ل ل ة ر و ص ل ل ه ذ ه ر ه ط ت NGFW Inside

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=64240 Len=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

ل NGFW ل ة ي ج ر ا خ ل ل ة ه ج ا و ل ل ى ل ع م ت ي ذ ل طاق ت ل ل ال ة ر و ص ل ل ه ذ ه ض ر ع ت

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

ةيسيسئرلا طاقنلا:

1. (ةيسئوشع ال IS ةيلمع يف اولمات) ابيرقت ناتق باطتم نات طقت ال.
2. ةمزلال نادقف ىلع تارشؤم دجوت ال.
3. (OOO) ببيترتل جراخ مزح دجوت ال.
4. يناتل ل لصحي نيح يف ، "دوجوم ريغ" 404 ىلع لولأا لصحي . HTTP GET تابلط 3 كانه . 304 مچح ب "لدعم ريغ" هي جوت ةداعا ةلاسرى لىع ثلثال لصحي و ، "قفاوم" 200 ىلع

أطخالاب فورعلم ويرانيسى ال - طاقنلا:

مخدمال طاقنلا تايوت (CAPI).

No.	Time	Source	Destination	Protocol	Length	Info
1	2013-08-08 15:33:31.909193	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 15:33:31.909849	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=867575960 Win=65535 Len=2 [Malformed Packet]
4	2013-08-08 15:33:31.913649	192.168.14.250	192.168.21.193	HTTP	222	HTTP/1.1 400 Bad Request (text/html)
5	2013-08-08 15:33:31.980326	192.168.21.193	192.168.14.250	TCP	369	[TCP Retransmission] 3072 → 80 [PSH, ACK] Seq=4231766829 Ack=867575960 Win=65535 Len=311
6	2013-08-08 15:33:32.155723	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3072 [ACK] Seq=8675756125 Ack=4231767140 Win=63929 Len=0
7	2013-08-08 15:33:34.871460	192.168.14.250	192.168.21.193	TCP	222	[TCP Retransmission] 80 → 3072 [FIN, PSH, ACK] Seq=867575960 Ack=4231767140 Win=63929 Len=164
8	2013-08-08 15:33:34.894713	192.168.21.193	192.168.14.250	TCP	60	3072 → 80 [ACK] Seq=4231767140 Ack=8675756125 Win=65371 Len=2
9	2013-08-08 15:33:34.933560	192.168.21.193	192.168.14.250	TCP	60	[TCP Retransmission] 3072 → 80 [FIN, ACK] Seq=4231767140 Ack=8675756125 Win=65371 Len=2
10	2013-08-08 15:33:34.933789	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3072 [ACK] Seq=8675756125 Ack=4231767143 Win=63927 Len=0
11	2013-08-08 15:33:35.118234	192.168.21.193	192.168.14.250	TCP	66	3073 → 80 [SYN] Seq=2130836820 Win=65535 Len=0 MSS=1460 SACK_PERM=1
12	2013-08-08 15:33:35.118737	192.168.14.250	192.168.21.193	TCP	66	80 → 3073 [SYN, ACK] Seq=2991287216 Ack=2130836821 Win=64240 Len=0 MSS=1380 SACK_PERM=1
13	2013-08-08 15:33:35.121575	192.168.21.193	192.168.14.250	TCP	60	3073 → 80 [ACK] Seq=2130836821 Ack=2991287217 Win=65535 Len=2 [Malformed Packet]
14	2013-08-08 15:33:35.121621	192.168.21.193	192.168.14.250	TCP	371	[TCP Out-Of-Order] 3073 → 80 [PSH, ACK] Seq=2130836821 Ack=2991287217 Win=65535 Len=313
15	2013-08-08 15:33:35.121896	192.168.14.250	192.168.21.193	HTTP	222	HTTP/1.1 400 Bad Request (text/html)
16	2013-08-08 15:33:35.124657	192.168.21.193	192.168.14.250	TCP	60	3073 → 80 [ACK] Seq=2130837134 Ack=2991287382 Win=65371 Len=2
17	2013-08-08 15:33:35.124840	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3073 [ACK] Seq=2991287382 Ack=2130837136 Win=63925 Len=0
18	2013-08-08 15:33:35.126846	192.168.21.193	192.168.14.250	TCP	60	[TCP Spurious Retransmission] 3073 → 80 [FIN, ACK] Seq=2130837134 Ack=2991287382 Win=65371 Len=2
19	2013-08-08 15:33:35.126244	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3073 [ACK] Seq=2991287382 Ack=2130837137 Win=63925 Len=0

ةيسيسئرلا طاقنلا:

1. هاچتال ةيثالث TCP ءحفاصم كانه .
2. ةمزلال نادقف ىلع تارشؤم و TCP لوكونورب ربع لاسرا ةداعا تايولم كانه .
3. ريغ لكشب ةلكشم اهنأ ىلع Wireshark ةطساوب اهفيرعت مت (TCP ACK) ةمزل كانه . جىحص .

جرخملا طاقنلا تايوتحم ةروصلال هذه رهظت (CAPO).

No.	Time	Source	Destination	Protocol	Length	Info
1	2013-08-08 15:33:31.909514	192.168.21.193	192.168.14.250	TCP	66	3072 → 80 [SYN] Seq=230342488 Win=65535 Len=0 MSS=1380 SACK_PERM=1
2	2013-08-08 15:33:31.909804	192.168.14.250	192.168.21.193	TCP	66	80 → 3072 [SYN, ACK] Seq=268013986 Ack=230342489 Win=64240 Len=0 MSS=1460 SACK_PERM=1
3	2013-08-08 15:33:31.913298	192.168.21.193	192.168.14.250	TCP	60	3072 → 80 [ACK] Seq=230342489 Ack=268013987 Win=65535 Len=2 [Malformed Packet]
4	2013-08-08 15:33:31.913633	192.168.14.250	192.168.21.193	HTTP	222	HTTP/1.1 400 Bad Request (text/html)
5	2013-08-08 15:33:31.980357	192.168.21.193	192.168.14.250	TCP	369	[TCP Retransmission] 3072 → 80 [PSH, ACK] Seq=230342489 Ack=268013987 Win=65535 Len=311
6	2013-08-08 15:33:32.155692	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3072 [ACK] Seq=268014152 Ack=230342800 Win=63929 Len=0
7	2013-08-08 15:33:34.871430	192.168.14.250	192.168.21.193	TCP	222	[TCP Retransmission] 80 → 3072 [FIN, PSH, ACK] Seq=268013987 Ack=230342800 Win=63929 Len=164
8	2013-08-08 15:33:34.894759	192.168.21.193	192.168.14.250	TCP	60	3072 → 80 [ACK] Seq=230342800 Ack=268014152 Win=65371 Len=2
9	2013-08-08 15:33:34.933575	192.168.21.193	192.168.14.250	TCP	60	[TCP Retransmission] 3072 → 80 [FIN, ACK] Seq=230342800 Ack=268014152 Win=65371 Len=2
10	2013-08-08 15:33:34.933774	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3072 [ACK] Seq=268014152 Ack=230342803 Win=63927 Len=0
11	2013-08-08 15:33:35.118524	192.168.21.193	192.168.14.250	TCP	66	3073 → 80 [SYN] Seq=2731219423 Win=65535 Len=0 MSS=1380 SACK_PERM=1
12	2013-08-08 15:33:35.118707	192.168.14.250	192.168.21.193	TCP	66	80 → 3073 [SYN, ACK] Seq=2453407925 Ack=2731219423 Win=64240 Len=0 MSS=1460 SACK_PERM=1
13	2013-08-08 15:33:35.121591	192.168.21.193	192.168.14.250	TCP	60	3073 → 80 [ACK] Seq=2731219423 Ack=2453407926 Win=65535 Len=2 [Malformed Packet]
14	2013-08-08 15:33:35.121652	192.168.21.193	192.168.14.250	TCP	371	[TCP Out-Of-Order] 3073 → 80 [PSH, ACK] Seq=2731219423 Ack=2453407926 Win=65535 Len=313
15	2013-08-08 15:33:35.121865	192.168.14.250	192.168.21.193	HTTP	222	HTTP/1.1 400 Bad Request (text/html)
16	2013-08-08 15:33:35.124673	192.168.21.193	192.168.14.250	TCP	60	3073 → 80 [ACK] Seq=2731219736 Ack=2453408091 Win=65371 Len=2
17	2013-08-08 15:33:35.124810	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3073 [ACK] Seq=2453408091 Ack=2731219738 Win=63925 Len=0
18	2013-08-08 15:33:35.126061	192.168.21.193	192.168.14.250	TCP	60	[TCP Spurious Retransmission] 3073 → 80 [FIN, ACK] Seq=2731219736 Ack=2453408091 Win=65371 Len=2
19	2013-08-08 15:33:35.126229	192.168.14.250	192.168.21.193	TCP	58	[TCP ACKed unseen segment] 80 → 3073 [ACK] Seq=2453408091 Ack=2731219739 Win=63925 Len=0

ةيسيسئرلا طاقنلا:

(ةيئوشع ال IS ةي لمع ي ف اولمأت) ابيرقت ناتقباطم ناتطقتل:

1. هاجتال ةي ثالذ TCP ةحفاصم كانه.
2. ةمزحل نادق ف يلع تارشؤم و TCP لو كوت و رب ربع لاسرا ةداع تايلمع كانه.
3. ريغ لكش ب ةلكشم اهنأ يلع Wireshark ةطساوب اهفيرعت مت (TCP ACK) ةمزح كانه .
ححص

ححص لل ريغ نيوكتلا تاذ ةمزحل نم ققحت:

No.	Time	Source	Destination	Protocol	Length	Info
1	2013-08-08 15:33:31.909193	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 15:33:31.909849	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
v 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)
v [Malformed Packet: Tunnel Socket]
v [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 7d 33 b6  .....P...;...3.
0030 28 98 50 10 ff ff 01 bf 00 00 00 00 00 00 00 00  (.P......:
```

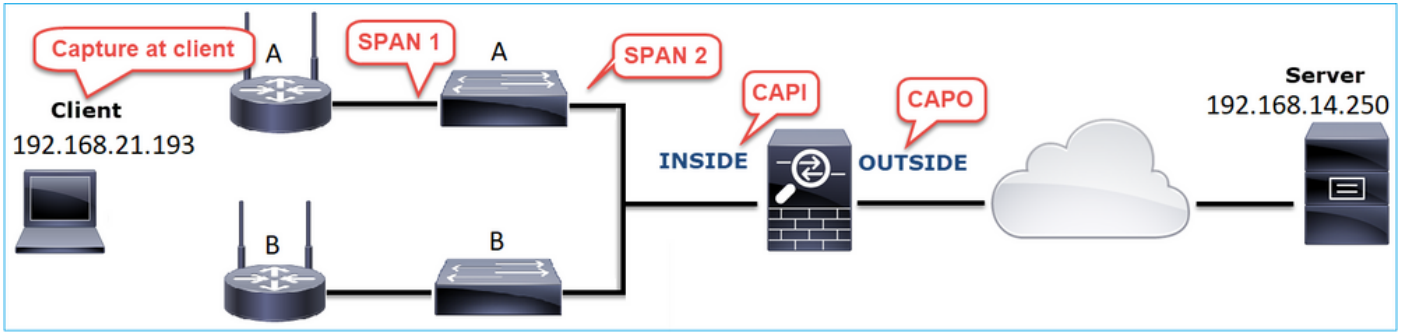
ةيئوشع ال طاقتل:

1. Wireshark لبق نم ححص ريغ لكش ب ةلكشم اهنأ يلع ةمزحل فيرعت متي.
2. تياب 2 هلو ط.
3. تياب 2 رادقم ب TCP ةلومح كانه.
4. ةيفاضا رافصأ 4 يه ةلومحل (00 00).

اهب يصومل تاءارجل

ةلأسملا هذه قاطن قيبيضت ةدايز وه عرفلا اذه في ةدراول تاءارجل نم ضرغلاو

نأ تلواح، نكمأ و اةي اهنال طاقتل في ضربق يلع تنمضت. ةيفاضا روص طاقتل 1. ءارجل الثم، داسف طبرل نم ردمل لزعي نأ ةق طقيرطو تاماسق نال قبطي:

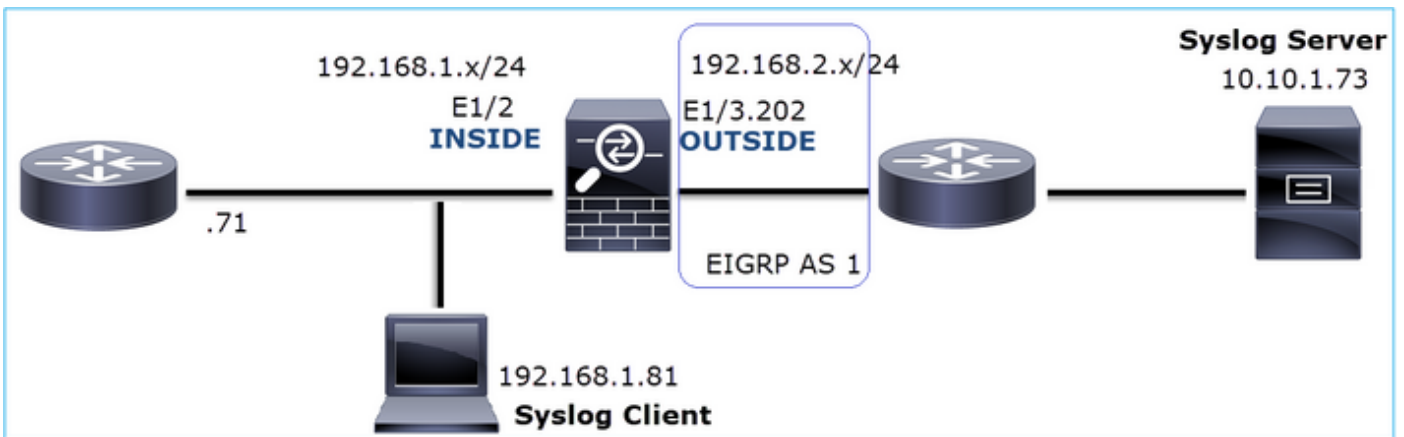


نأ ناك لحل او لى غشت جم ان رب نراق 'A' حات فم ل اب ت فضا ناك ي فاضا تي اب 2 ل، ة ل اح ل هذه ي ف داس فل ب بس ي نأ حات فم ل تل دب ت سا.

(ة دوق فم ل مزح ل) UDP ل اص ت ا ة لك شم 8. ة ل اح ل

ل دان syslog ة ي ا غ ل ل ع ة ل اس ر (UDP 514) Syslog ي ر ي ال : ة لك شم ل ف ص و

ط ا خ م ل ة ر و ص ل ا هذه ض ر ع ت :



ر ث ا ت م ل ا ق ف د ت ل ا :

SRC IP: 192.168.1.81

DST IP: 10.10.1.73

ل و ك و ت و ر ب ل ا : UDP 514

ر س ا ل ي ل ح ت

م ت م ل ا ل ا ل ا ل ا ل ا ل ا : FTD LINA ك ر ح م ل ع ط ا ق ت ل ل ا ل ا ل ا ل ا ل ا ل ا

<#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
```

مزح ي فTD روص 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 ي صوم ال تاءارج ال

ة. ال أسم ال هذه قاطن ق ي ي ضت ة دايز وه عرف ال اذه ي ف ة دراو ال تاءارج ال نم ضرغ ل او

ال فTD لاصت ل و دج نم ق قحت 1. اءارج ال

ة: غ ا ي ص ال هذه مادخت س ا ك ن ك م ي ، د د ح م ل اصت ل نم ق قحت ل ل

```
<#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
```

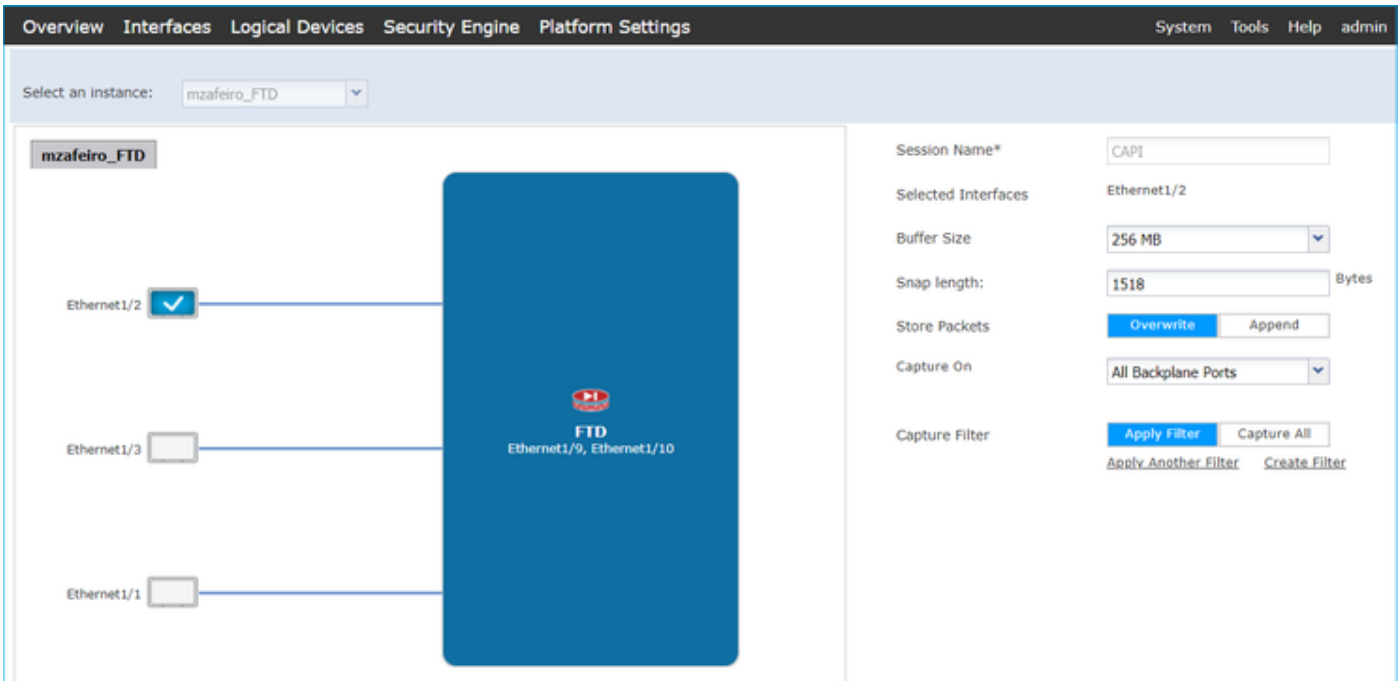
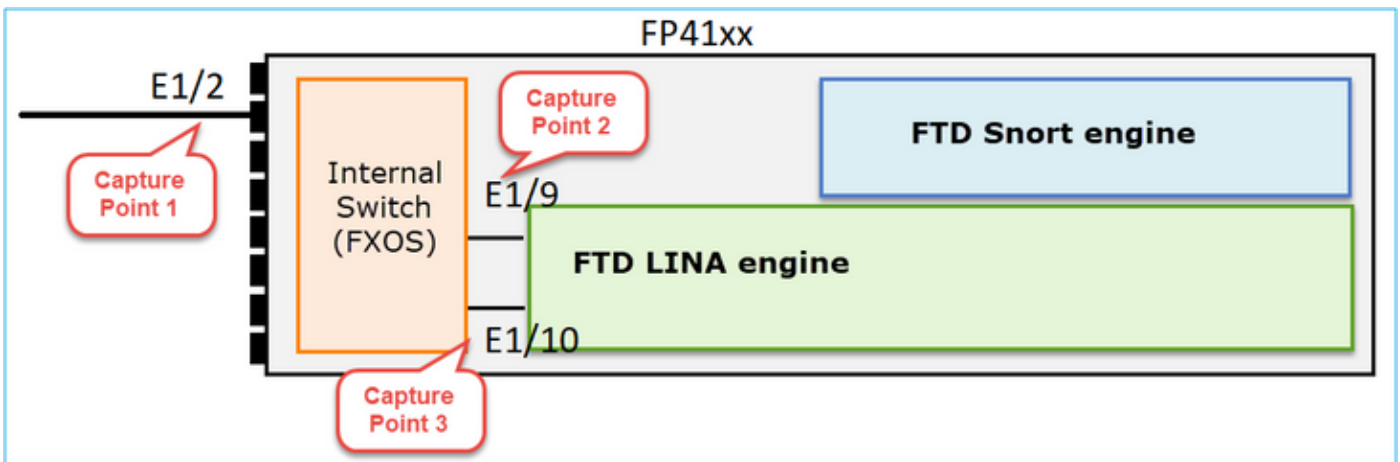
```
N1
```

ةيسيرلا طاقنلا:

1. (نارود) اهسفن يه جورخلاو لوخدلا تاهجاو.
2. (تياپ تياپاغيفغ ~5) ةياغلل ةريبك ةميق ىلع تياپلا تادحو ددع يوتحي.
3. عاروببسلا وه اذه. (عيرسلا HW قفدت) قفدتلا ليحت ءاغلا ىلا "0" ةمالعلا ريشت. ةمظنالا ىلع طقف موعدم قفدتلا ليحت ءاغلا. مزح يا FTD طاقنلا ضرع مدع 41xx وه زاهجا، ةلجال هذه في 41xx و 93xx ةيساسالا.

لكيهلا يوتسم ىلع روصلا طاقنلا عتمت 2. عارجلا

هذه في E1/2) لوخدلا ةهجاو ىلع طاقنلا لانيكمتو FirePOWER لكيه ريديم لاصتالاب مق ةروصلا في حضورم وه امك، (E1/9 و E1/10) ةيفلخلا ةحوللا تاهجاو (ةلجال



ناوٹ عضب دعب:

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

نراقب اللى جودرم طبرللا لى زي نأ طبر VN-tagged لى تي نثتسا Wireshark في فرط يعي بط

لبق:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000	Cisco_61:5a:9c	Spanning-tree-(f...	STP	64	RST. Root = 32768/0/00:11:bc:88:08:c9 Cost = 8 Port = 0x802d
2	0.0000	Cisco_61:5a:9c	Spanning-tree-(f...	STP	64	RST. Root = 32768/0/00:11:bc:88:08:c9 Cost = 8 Port = 0x802d
3	0.0532	Vmware_85:4f:ca	Broadcast	ARP	70	Who has 192.168.103.111? Tell 192.168.103.112
4	0.0000	Vmware_85:4f:ca	Broadcast	ARP	64	Who has 192.168.103.111? Tell 192.168.103.112
5	0.5216	Vmware_85:2f:00	Broadcast	ARP	70	Who has 10.10.10.1? Tell 10.10.10.10
6	0.0000	Vmware_85:2f:00	Broadcast	ARP	64	Who has 10.10.10.1? Tell 10.10.10.10
7	0.5770	Vmware_85:2f:00	Broadcast	ARP	70	Who has 10.10.10.1? Tell 10.10.10.10
8	0.0000	Vmware_85:2f:00	Broadcast	ARP	64	Who has 10.10.10.1? Tell 10.10.10.10
9	0.8479	Cisco_61:5a:9c	Spanning-tree-(f...	STP	64	RST. Root = 32768/0/00:11:bc:88:08:c9 Cost = 8 Port = 0x802d
10	0.0000	Cisco_61:5a:9c	Spanning-tree-(f...	STP	64	RST. Root = 32768/0/00:11:bc:88:08:c9 Cost = 8 Port = 0x802d
11	0.1520	Vmware_85:2f:00	Broadcast	ARP	70	Who has 10.10.10.1? Tell 10.10.10.10
12	0.0000	Vmware_85:2f:00	Broadcast	ARP	64	Who has 10.10.10.1? Tell 10.10.10.10
13	0.8606	Vmware_85:4f:ca	Broadcast	ARP	70	Who has 192.168.103.111? Tell 192.168.103.112
14	0.0000	Vmware_85:4f:ca	Broadcast	ARP	64	Who has 192.168.103.111? Tell 192.168.103.112
15	0.1655	192.168.0.101	173.38.200.100	DNS	91	Standard query 0x4a9f A 2.debian.pool.ntp.org
16	0.0000	192.168.0.101	173.38.200.100	DNS	85	Standard query 0x4a9f A 2.debian.pool.ntp.org
17	0.0000	192.168.0.101	173.38.200.100	DNS	91	Standard query 0x4afd AAAA 2.debian.pool.ntp.org
18	0.0000	192.168.0.101	173.38.200.100	DNS	85	Standard query 0x4afd AAAA 2.debian.pool.ntp.org
19	0.0003	192.168.0.101	173.38.200.100	DNS	91	Standard query 0x4a9f A 2.debian.pool.ntp.org
20	0.0000	192.168.0.101	173.38.200.100	DNS	85	Standard query 0x4a9f A 2.debian.pool.ntp.org

دع ب:

No.	Time	Source	Destination	Protocol	Length	Time to live	Info
1334	0.000000000	192.168.1.81	10.10.1.73	Syslog	147	255	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609002: Teardown local-host identity:192.168.1.81 dur
1336	0.00078873	192.168.1.81	10.10.1.73	Syslog	147	254	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609002: Teardown local-host identity:192.168.1.81 dur
1338	0.00015099	192.168.1.81	10.10.1.73	Syslog	147	253	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609002: Teardown local-host identity:192.168.1.81 dur
1340	0.000128919	192.168.1.81	10.10.1.73	Syslog	131	255	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609001: Built local-host NET_FIREWALL:192.168.1.71\n
1342	0.000002839	192.168.1.81	10.10.1.73	Syslog	147	252	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609002: Teardown local-host identity:192.168.1.81 dur
1344	0.000137974	192.168.1.81	10.10.1.73	Syslog	131	254	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609001: Built local-host NET_FIREWALL:192.168.1.71\n
1346	0.000002758	192.168.1.81	10.10.1.73	Syslog	147	251	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609002: Teardown local-host identity:192.168.1.81 dur
1348	0.000261845	192.168.1.81	10.10.1.73	Syslog	131	253	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609001: Built local-host NET_FIREWALL:192.168.1.71\n
1350	0.000002736	192.168.1.81	10.10.1.73	Syslog	147	250	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609002: Teardown local-host identity:192.168.1.81 dur
1352	0.000798149	192.168.1.81	10.10.1.73	Syslog	200	255	LOCAL4.INFO: Oct 15 2019 07:47:17: %ASA-6-302020: Built inbound ICMP connection for faddr 192.16
1354	0.000498621	192.168.1.81	10.10.1.73	Syslog	131	252	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609001: Built local-host NET_FIREWALL:192.168.1.71\n
1356	0.000002689	192.168.1.81	10.10.1.73	Syslog	147	249	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609002: Teardown local-host identity:192.168.1.81 dur
1358	0.000697783	192.168.1.81	10.10.1.73	Syslog	195	255	LOCAL4.INFO: Oct 15 2019 07:47:17: %ASA-6-302021: Teardown ICMP connection for faddr 192.168.1.7
1360	0.000599702	192.168.1.81	10.10.1.73	Syslog	151	255	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609002: Teardown local-host NET_FIREWALL:192.168.1.71
1362	0.000002728	192.168.1.81	10.10.1.73	Syslog	200	254	LOCAL4.INFO: Oct 15 2019 07:47:17: %ASA-6-302020: Built inbound ICMP connection for faddr 192.16
1364	0.000499914	192.168.1.81	10.10.1.73	Syslog	131	251	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609001: Built local-host NET_FIREWALL:192.168.1.71\n
1366	0.000697761	192.168.1.81	10.10.1.73	Syslog	147	248	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609002: Teardown local-host identity:192.168.1.81 dur
1368	0.000169137	192.168.1.81	10.10.1.73	Syslog	195	254	LOCAL4.INFO: Oct 15 2019 07:47:17: %ASA-6-302021: Teardown ICMP connection for faddr 192.168.1.7
1370	0.000433196	192.168.1.81	10.10.1.73	Syslog	151	254	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609002: Teardown local-host NET_FIREWALL:192.168.1.71
1372	0.000498718	192.168.1.81	10.10.1.73	Syslog	200	253	LOCAL4.INFO: Oct 15 2019 07:47:17: %ASA-6-302020: Built inbound ICMP connection for faddr 192.16
1374	0.000002849	192.168.1.81	10.10.1.73	Syslog	131	250	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609001: Built local-host NET_FIREWALL:192.168.1.71\n
1376	0.000596345	192.168.1.81	10.10.1.73	Syslog	147	247	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609002: Teardown local-host identity:192.168.1.81 dur
1378	0.000600157	192.168.1.81	10.10.1.73	Syslog	195	253	LOCAL4.INFO: Oct 15 2019 07:47:17: %ASA-6-302021: Teardown ICMP connection for faddr 192.168.1.7
1380	0.000002772	192.168.1.81	10.10.1.73	Syslog	151	253	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609002: Teardown local-host NET_FIREWALL:192.168.1.71
1382	0.000600947	192.168.1.81	10.10.1.73	Syslog	200	252	LOCAL4.INFO: Oct 15 2019 07:47:17: %ASA-6-302020: Built inbound ICMP connection for faddr 192.16
1384	0.000498808	192.168.1.81	10.10.1.73	Syslog	131	249	LOCAL4.DEBUG: Oct 15 2019 07:47:17: %ASA-7-609001: Built local-host NET_FIREWALL:192.168.1.71\n

ةيسيرلا طاقنلا:

1. طوق syslog راهظاومزحلا تاراركت ةلازال ضرعلا ةيفصت لماع قيبت متي .
2. مزح لدعم ىلإ ريشي اذهو .ةيناثوركيملا ىوتسم يف مزحلا نيب فالخال نوكي .ةياغلل عفترم .
3. ةطوشنأ ةمزح ىلإ ريشي اذه .رمتسم لكشب (TTL) ةاقبلأ ةدم ةميق ضفخنن .



Packet-tracer قيبطت مادختسا 3. ءارجالا

ضبق ىلع) طشن عبتت متي ال عيطتسي تنأ كرحم LINA ةيامحلا راج ذاتجت ال مزحلا نأ امب w/trace):
 packet-tracer عم يكاخم طبر تعبتت عيطتسي تنأ نأ ريغ:

```
<#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

ة عرس ل قئاف لاس رال ا جم ان رب " هيجوت ديكأت 4. اء اء اء

هيجوت ل ا ف ل كاش م ا كانه تنك اذا ام ة فر عمل ة ا م ح ل ر اء هيجوت ل وء ج نم ق ق ح ت

<#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

ة س س ئ ر ل ا ط ا ق ن ل ا

1. ة ح ص ل ا ج و ر خ ل ا ة ح ا و ل ل ا ر ا س م ل ا ر ي ش ي .

2. ة ل ي ل ق ق ئ ا ق د ل ب ق ق ي ر ط ل ا م ل ع ت م ت (0:02:37).

ل ا ص ت ا ل ا ل ي غ ش ت ت ق و د ي ك أ ت 5. اء اء اء

ل ا ص ت ا ل ا ا ذ ه س س ئ س أ ت ت ق و ة فر عمل ل ا ص ت ا ل ا ل ي غ ش ت ت ق و ن م ق ق ح ت

<#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

ةسيسيئرلا ةطقنلا:

1. لودج يي EIGRP راسم تيبثت لبق اذه) قئاق د 4 يلاوح ذنم لاصتالاءاشنإ مت (هيجوتلل

تباثل لاصتالاءاسم ب مق 6. اءارءالا

اذهو؛ ةءطاخ جرخم ةهءاو لىل اءههيجوت متي و سسؤم لاصتالاءم مزحلل قباطت، ةلءالءه هءه يي
ةياملءالءا ءاى لءم ع بيترت لىل ك لء يي ببس لاء جري. ي ق لء راركت ءوءح يي ببس تي

1. (ماملءهيجوتللاءوءج نع ءحبل لىل ع ةيولوالءا اذه ذءاى) هءاشنإ مت يذلل لاصتالاءءح ب.
2. لىل ع ةيولوالءا (NAT ةياع) UN-NAT ةلءرم ذءأء - (NAT) ةكبشل لاءون ع ةمءرت نع ءحبل لاء.
راسم لاءءح ب و PBR.
3. (PBR) ةساي س لاءىل ع مءاقل لاءهيجوتللاء.
4. ي مومءل لاءهيجوتللاءوءج ءح ب.

لومء ءلءم نوكء ام نيب رارمءساب مزحلل syslog لىل عم لسري) اءبأ يهءني لاء لاصتالاء نأ ام ب
ايوءي لاصتالاءءح لىل ءءا ك لاءه (ءق ي قء د 2 يه UDP

<#root>

firepower#

clear conn address 10.10.1.73 address 192.168.1.81 protocol udp port 514

1 connection(s) deleted.

ءيءج لاصتالاءاشنإ نم ققءء:

<#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

م. ئاعلال لخادتل ةلهم نيوكت 7. ءارجال

UDP تاقفدتل ةصاخو، لثمألا نود هي جوتل بنجت و ةلكشملا ةجالعمل بسانملا لجال وه اذه ةميقلا طبضو تالهم > ياساسألا ماظنلا تاداعل > ةزهجالا لىل لقتنا

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)

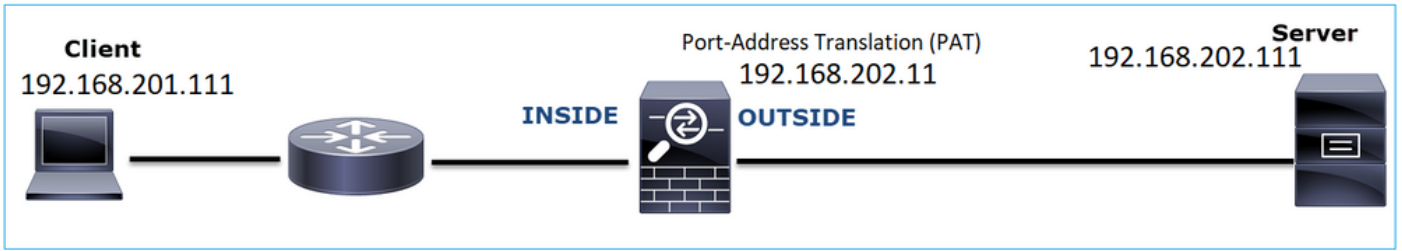
ءجرم رمالا في ةلهم conn ميعوتلا لوح لىصافتلا نم ديزملا تدجوع يعطتسي تأن

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/T-Z/cmdref4/t1.html#pgfld-1649892>

1) ويرانيسلا (HTTPS لاصتا ةلكشم 9. ةلجالا

مدخال او 192.168.201.105 ليعملا نيب HTTPS لاصتا ءاشنل نكمي ال: ةلكشملا فصو 192.168.202.101

طاطخملا ةروصلا هذه ضرعت



رثأت الما قف دت ل:

SRC IP: 192.168.201.111

DST IP: 192.168.202.111

لوكوت ورب: لوكوت ورب ل TCP 443 (HTTPS)

رسأ ل ل لحت

كرحم ىلع طاقتل لال ن ي كمت

ل ل كشت ةم جرت ناونع ل ل بجاو فلل تخم ي جراخل طاقتل لال ي ف لمعت سي ip ل

<#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

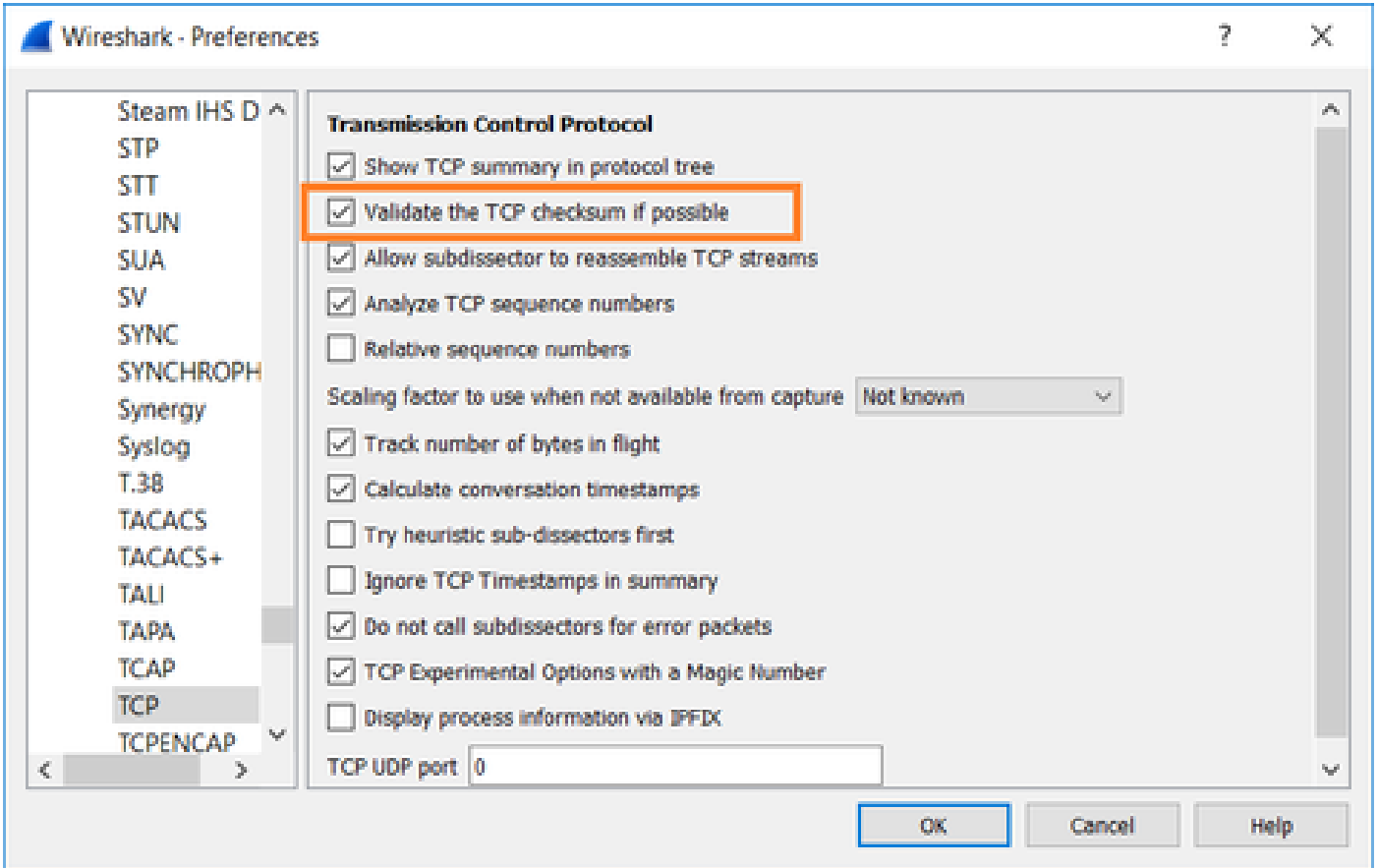
هه جاول ع مت ي ذل طاقتل لال ةروصل ل هذه رهظت

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)	6666 → 443 [SYN] Seq=2034865631 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=192658158 TSecr=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=1380 SACK_PERM=1 TSval=3119
40	2018-02-01 10:39:35.189046	192.168.201.111	192.168.202.111	TCP	70	0x2f32 (12082)	6666 → 443 [ACK] Seq=2034865632 Ack=4086514532 Win=29312 Len=0 TSval=192658158 TSecr=3119615816
41	2018-02-01 10:39:35.251695	192.168.201.111	192.168.202.111	TLSv1	326	0x2f33 (12083)	Client Hello
42	2018-02-01 10:39:35.252352	192.168.201.111	192.168.201.111	TCP	70	0xfcb4 (61364)	443 → 6666 [ACK] Seq=4086514532 Ack=2034865888 Win=8192 Len=0 TSval=3119615816 TSecr=192658174
43	2018-02-01 10:40:05.317320	192.168.202.111	192.168.201.111	TCP	70	0xd8c3 (55491)	443 → 6666 [RST] Seq=4086514532 Win=8192 Len=0 TSval=3119645908 TSecr=0

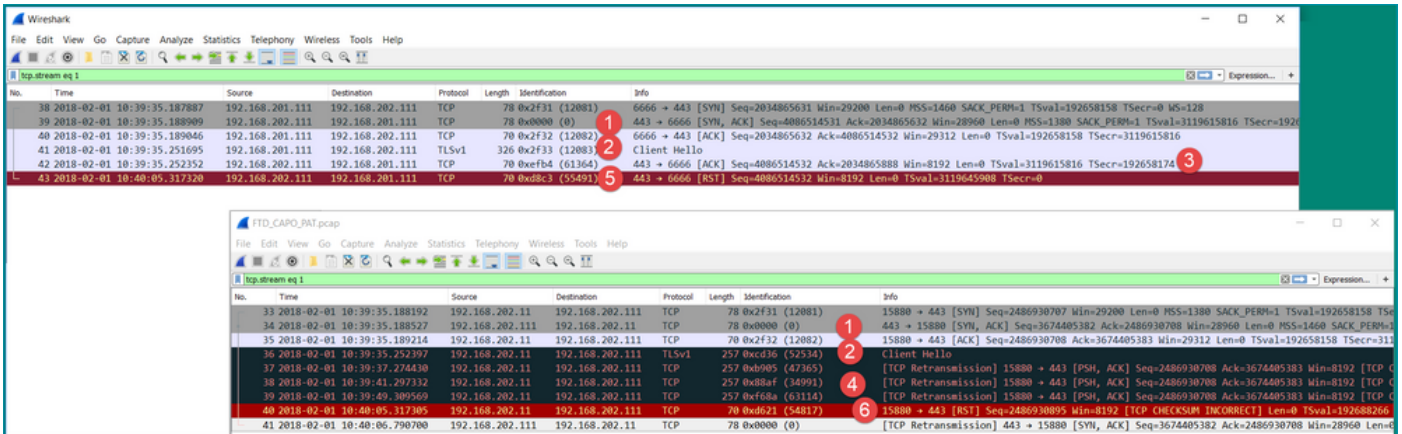
ة سي ل ل طاقن ل:

1. هاجت ال ةي ثالت TCP ةح فاصم كانه.
2. Client Hello ة لاسر ل ل م عمل لسري SSL ضوافت ةب.
3. ل م عمل ل ل لاسر ل م TCP ACK كانه.
4. ل م عمل ل ل لاسر ل م TCP RST كانه.

ل NGFW ل ةي جراخل ةه جاول ل ع مت ي ذل طاقتل لال ةروصل ل هذه ضرعت



ةلماكلا ةروصلا لىل ةلوصلل بئج لىل ابئج تاطاقتل لىل ةرضن نأ ةديفملا نم ،ةلجال هذه يف



ةيسيرلا تاطاقتلا:

1. مل قفدتلا نأ ينعي اذهو .اهسفن يه IP تافرع م .هاتإل ةثالث TCP ةحفاصم كانه .ةيامجال راج ةطساوب هنيوكت متي
2. ةيامجال راج ةطساوب ةمزال لىل لىل م تي . IP 12083 فرعم عم لىل م نم TLS Client Hello متي و (TLS ريفشت كف ةسايس مادختساب ،ةلجال هذه يف ،ةيامجال راج نيوكت مت) TCP ةمزال لىل رابخالال ةومجمل فلتي ،كلذ لىل ةفاضل اب . لىل IP فرعم ريغت (اقحال ةحالصا مت جم انربلا يف بيع ببسب)
3. (مخالل فسني يذل) لىل م عم لىل اب لىل ACK لسري و TCP لىل ةعضوي يف ةيامجال راج بجوي .

```

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 Min=29200 Len=0 MSS=1380 S
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 Min=29
35 2018-02-01 10:39:35.189214 192.168.202.11 192.168.202.111 TCP 70 0x2f32 (12082) 15880 → 443 [ACK] Seq=2486930708 Ack=3674405383 Min=29312 L
36 2018-02-01 10:39:35.252397 192.168.202.11 192.168.202.111 TLSv1 257 0xcd36 (52534) Client Hello

```

```

> Internet Protocol Version 4, Src: 192.168.202.11, Dst: 192.168.202.111
  Transmission Control Protocol, Src Port: 15880, Dst Port: 443, Seq: 2486930708, Ack: 3674405383, Len: 187
    Source Port: 15880
    Destination Port: 443
    [Stream index: 1]
    [TCP Segment Len: 187]
    Sequence number: 2486930708
    [Next sequence number: 2486930895]
    Acknowledgment number: 3674405383
    1000 ... = Header Length: 32 bytes (8)
    > Flags: 0x018 (PSH, ACK)
    Window size value: 64
    [Calculated window size: 8192]
    [Window size scaling factor: 128]
    > Checksum: 0x0c65 incorrect, should be 0x3063(maybe caused by "TCP checksum offload?")
    [Checksum Status: Bad]
    [Calculated Checksum: 0x3063]
    Urgent pointer: 0
    > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
    > [SEQ/ACK analysis]
    > [Timestamps]
    TCP payload (187 bytes)
  > Secure Sockets Layer

```

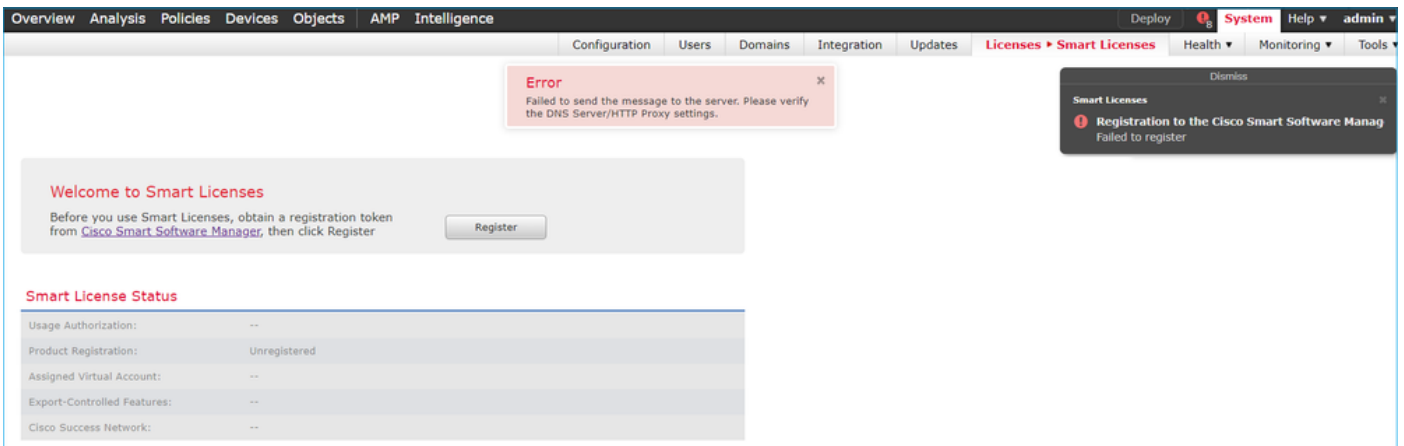
4. TLS Client Hello رسالة لاسر لاسرا دي عي و مداخل نم TCP ACK مزمح ية ايمالح رادج يقبلت ي ال.
- هطيشنتب ايمالح رادج ماق يذلا TCP ليك و عضو بسبب رخأ ارم.
5. ليمعلا وحن TCP RST لسري و ايمالح رادج يهتني ، اةينات 30 يلا و ح دع ب.
6. مداخل وحن TCP RST ايمالح رادج لسري.

هول اوعرلل:

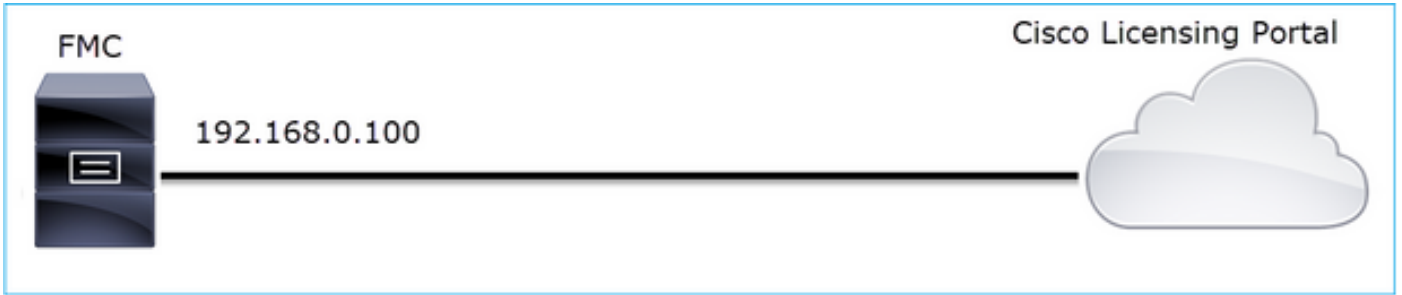
[Firepower TLS/SSL لاصتال اديك اة جلاعم](#)

(2 ويرانيسال) HTTPS لاصتال اة لك شم 10. اة لالحال

FMC ل اديك ذلا صيخرتل ل ايجست ل ش ف : اة لك شم ل ا ف ص و



طاطخ ل ا ا روص ل ا هذ ه ضرعت



رثأت م ل ق ف د ت ل ل :

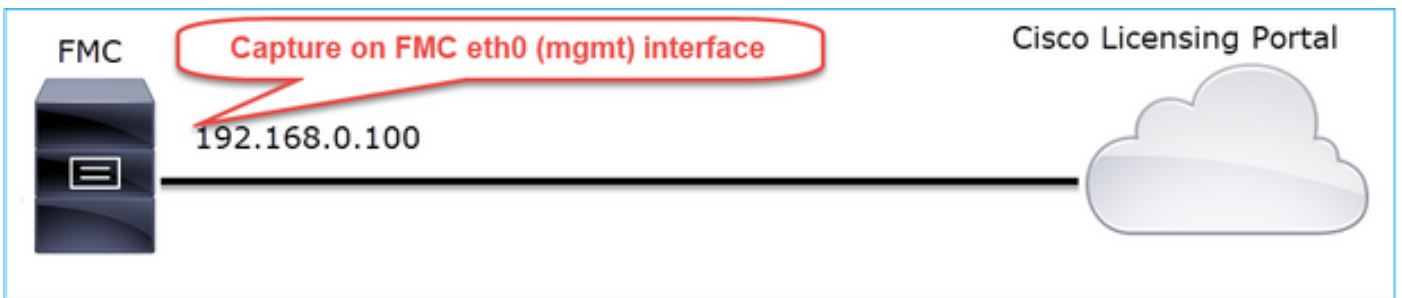
SRC IP: 192.168.0.100

DST: tools.cisco.com

ل و ك و ت و ر ب ل : ل و ك و ت و ر ب : ل و ك و ت و ر ب ل (HTTPS) TCP 443

ر س أ ل ل ح ت

FMC: ة ر ا د ا ة ه ج ا و ل ع ط ا ق ت ل ل ا ل ن ي ك م ت



ط ا ق ت ل ل ا ل ف ا ق ي ا ل C T R L - C ل ع ط غ ض ا ، أ ط خ ل ا ل ا س ر ر و ه ظ د ر ج م ب . ل ر خ أ ة ر م ل ل ل ج س ت ل ل ل و ا ح :

<#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، (System > Health > Monitor) لك يهلا ةرادا يف مكحتلا ةدحو نم طاقنتلالا عمج مق ةروصلال يف حضوم وه امك، (مدقتمل احوال صاوا عاخالأا فاشكتسا ددحو

Wireshark لىل ع فMC طاقنتلالا ةروصلال رهظت:

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 SACK_PERM=1
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

لماع مدختسا، اهطاقنتلالا مت يتلا ةديجال TCP لمع تاسلج عيمج نم ققحتلل: حيملت TCP ماظن مزح عيمج ةيفصتب اذه موقى. Wireshark لىل ع tcp.flags=0x2 ضرع ةيفصت اهطاقنتلالا مت يتلا.

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 07:45:56.468604	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=16169802 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 نم مداخلال مسا لقق قيبطت: حيملت

75 2019-10-23 07:45:14.634091 192.168.0.100 72.163.4.38 TLSv1.2 571 Client Hello

> 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: 517

Secure Sockets Layer

- TLsv1.2 Record Layer: Handshake Protocol
 - 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: 234490a107438c73b595646532
 - Session ID Length: 0
 - Cipher Suites Length: 100
 - Cipher Suites (50 suites)
 - Compression Methods Length: 1
 - Compression Methods (1 method)
 - Extensions Length: 367
 - Extension: server_name (len=20)
 - Type: server_name (0)
 - Length: 20
 - Server Name Indication extension
 - Server Name list length: 18
 - Server Name Type: host_name (0)
 - Server Name length: 15
 - Server Name: tools.cisco.com

Context menu options: Expand Subtrees, Collapse Subtrees, Expand All, Collapse All, Apply as Column, Apply as Filter, Prepare a Filter, Conversation Filter, Colorize with Filter, Follow, Copy, Show Packet Bytes..., Export Packet Bytes..., Wiki Protocol Page, Filter Field Reference, Protocol Preferences, Decode As..., Go to Linked Packet, Show Linked Packet in New Window

🔍 Client Hello ssl.handshake.type لئاسر ةيؤرل اذه ضرعلا ةيفصت لماع قي بطت :حي ملت طوق 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

✍️ (tools.cisco.com) يكدل صيخرتللا ةبواب مدختست ،ريرتللا اذه ةباتك تقوي ف :ةظحالم هذه IP نيوانع 72.163.4.38 و 173.37.145.8

ةروصللا يف حضورم وه امك ،(TCP قفدت > عبتا) TCP تاقفدت دحأ عبتا

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	

Frame 75: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0, 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: 517 Secure 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
- Conversion Filter
- Colorize Conversion
- SCTP
- Follow
 - TCP Stream
 - UDP Stream
 - SSL Stream
 - HTTP 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.co	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	1304		443 → 35752 [PSH, ACK] Seq=2770078981 Ack=2427944049 Win=32768 Len=1330 [TCP segment of a reassembled PDU]
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 07:45:14.966877	72.163.4.38	192.168.0.100	TLSv1.2	155		Certificate
82	2019-10-23 07:45:14.966888	192.168.0.100	72.163.4.38	TCP	54		35752 → 443 [ACK] Seq=2427944049 Ack=2770080421 Win=31920 Len=0
83	2019-10-23 07:45:14.966915	72.163.4.38	192.168.0.100	TLSv1.2	63		Server Hello Done
84	2019-10-23 07:45:14.966925	192.168.0.100	72.163.4.38	TCP	54		35752 → 443 [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		Alert (Level: Fatal, Description: Unknown CA)
86	2019-10-23 07:45:14.967261	192.168.0.100	72.163.4.38	TCP	54		35752 → 443 [RST, ACK] Seq=2427944056 Ack=2770080421 Win=0 Len=0
87	2019-10-23 07:45:14.967382	72.163.4.38	192.168.0.100	TCP	60		443 → 35752 [ACK] Seq=2770080421 Ack=2427944056 Win=32768 Len=0
88	2019-10-23 07:45:14.967398	192.168.0.100	72.163.4.38	TCP	54		35752 → 443 [RST] Seq=2427944056 Win=0 Len=0

> Frame 75: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface 0, 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: 517 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: 234490a107438c73b58564653271c7c09fbb7ac16897184...
Session ID Length: 0
Cipher Suites Length: 100
Cipher Suites (50 suites)

آية سي ئرلا طاقنلا:

1. هاجت إلة آية ثالآ TCP ءء فاصم كانه.
2. يكذلا صيخ رآل لءءم هاجءاب SSL Client Hello ءلاس ر (FMC) ليمع ل لسري.
3. ءفن آءسم ءرود ءسئل انه ن عي اءهو 0. وه SSL ءسلء فرعم.
4. "مءءال آي ف كب ابءرم" و "مءءال آي ف كب ابءرم" ءلاس رب ءهءول مءءال ءري.
5. "فورعم ريع ءءصم عءرم" ب ءلءءي يءل او كلهم SSL هيبنء ليمع ل لسري.
6. ءسلءال ءالءال TCP RST ليمع ل لسري.
7. ءي نآ 0.5 يلاوح (ءالءال إلة آاشن إلة نم) لمءال ب TCP ءسلء ءمءنآ.

مسالال فءكئ ءلءال هءه في. عئاشلال مسالال ءيؤرل رءصم ل لءع عسوو مءءال ءءاهش ءءع (MITM) ليمع ل لءع في رءءب موقئ زاهء نع عئاشلال.

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
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
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-sta
                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_OU)
                        > RDNSSequence item: 1 item (id-at-organizationName=FTD_OU)
                        > RDNSSequence item: 1 item (id-at-organizationalUnitName=FTD_OU)
                        > RDNSSequence item: 1 item (id-at-commonName=FTD4100_MITM)
                  > validity
                  > subject: rdnSequence (0)
                  > subjectPublicKeyInfo
                > extensions: 6 items
  
```

هذه في حضورم اذو

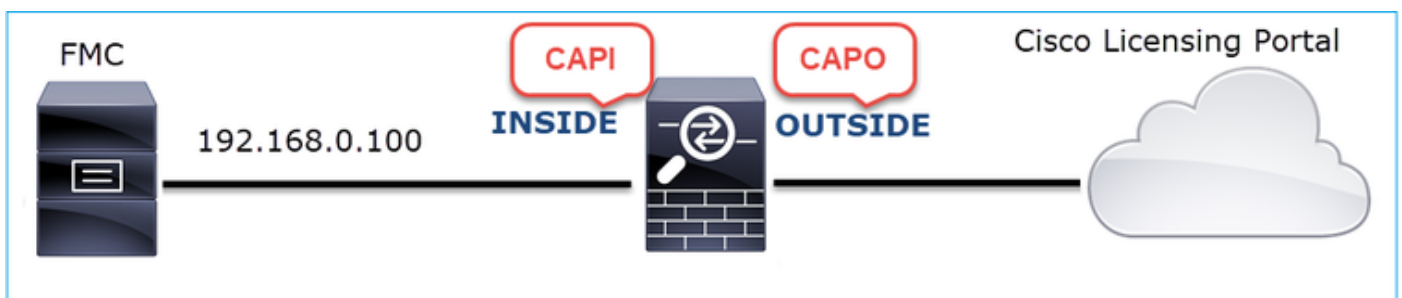


اهب ي صوم ال تاءارج ال

ة. لاسم ال هذه قاطن ق ي ي ضت ةدايز وه عرف ال اذو في ة دراو ال تاءارج ال نم ضرغ لاو

ة. في فاضا روص طاق ال 1. اءارج ال

ل قن ال ة ي امح راج زا هج ل ع طاق ال



رهظت 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=1336
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 Jose)
    signedCertificate
      version: v3 (2)
      serialNumber: 0x00aa23af5d607e00002f423880
      signature (sha256WithRSAEncryption)
      issuer: rdnSequence (0)
        rdnSequence: 3 items (id-at-commonName=FTD4100_MITH,id-at-organizationalUnitName=FTD_OU,id-at-organizationName=FTD_O)
          RDNSSequence item: 1 item (id-at-organizationName=FTD_O)
          RDNSSequence item: 1 item (id-at-organizationalUnitName=FTD_OU)
          RDNSSequence item: 1 item (id-at-commonName=FTD4100_MITH)
      validity
  
```

رہطت CAPO:

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=1169
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=1336
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 17:49:03.709420	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: 6921d084f7a6f6167058f1e2aad8b98b4e6c971ea6ea3b4...
    Certificate Length: 1736
  Certificate: 308206c4308204aca00302010202147517167783d0437eb5... (id-at-commonName=HydrantID SSL ICA G2,id-at-organizationName=HydrantID (Avalanche Cloud Corporation),id-at-localityName=San Jose)
    signedCertificate
      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
  
```

(MITM) مداخل دہاش لدعی لقنلا قیامح راج نأ طاقتلالال هذه تبثت

زاهجال تالجس نم ققحت 2. عارجال

دنتسمل اذه یف حضوم وه امك FMC TS ةمزح عیمرت كنكمی

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

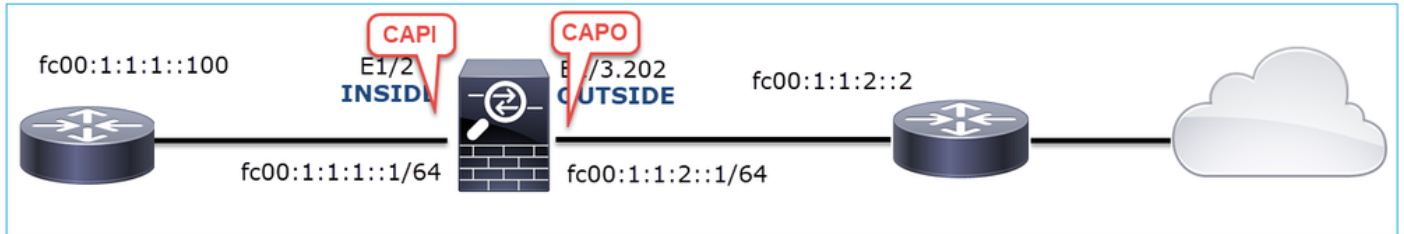
<#root>

firepower#

capture CAPI int INSIDE match ip any6 any6

firepower#

capture CAPO int OUTSIDE match ip any6 any6



لم عي ال وي راني س - طاق تال

لى (هجوم ل ل خاد) IP FC00:1:1:1::100 نم ICMP لاصتا رابتخ عم يزاولاب طاق تال ال هذه ذخا مت (مداخل نم هجوم) IP FC00:1:1:2::2.

ىل ع Capture on Firewall INSIDE وهجاو يوتحي:

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:fef6:1dae	fc00:1:1:1::100	ICMPv6	86	Neighbor Solicitation 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:fef6:1dae	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:fefc:fc:d8	fe80::2be:75ff:fef6:1dae	ICMPv6	86	Neighbor Solicitation for fe80::2be:75ff:fef6:1dae from 4c:4e:35:fc:fc:d8
11	2019-10-24 13:02:17.062862	fe80::2be:75ff:fef6:1dae	fe80::4e4e:35ff:fefc:fc:d8	ICMPv6	78	Neighbor Advertisement fe80::2be:75ff:fef6:1dae (rtr, sol)
12	2019-10-24 13:02:22.059994	fe80::2be:75ff:fef6:1dae	fe80::4e4e:35ff:fefc:fc:d8	ICMPv6	86	Neighbor Solicitation for fe80::4e4e:35ff:fefc:fc:d8 from 00:be:75:f6:1d:ae
13	2019-10-24 13:02:22.063000	fe80::4e4e:35ff:fefc:fc:d8	fe80::2be:75ff:fef6:1dae	ICMPv6	78	Neighbor Advertisement fe80::4e4e:35ff:fefc:fc:d8 (rtr, sol)

ةي سي ئرل ا طاق نال:

1. ثبل زاهب صاخال MAC ناوع بلطيو IPv6 ل ةرواجم بلط بلط ةلاسر هجوم ل لسري (IP FC00:1:1::1).
2. راج نال ع ا مداختساب ةي امحل راج دودر IPv6.
3. ICMP Echo بلط هجوم ل لسري.
4. قفدت زاهب صاخال MAC ناوع بلطيو IPv6 ل ةرواجم بلط ةلاسر ةي امحل راج لسري (مداخل نم تانايبال fc00:1:1::100).
5. راج نال ع ا مداختساب هجوم ل دري IPv6.
6. IPv6 ىصل ةي اضا ICMP ابلط هجوم ل لسري.

ىل ع ةهجاو ل ا جراخ دوجومل ةي امحل راج ل ع طاق تال ال يوتحي:


```
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
```

misconfiguration: لا ليكشنت ةادأ up لا فشكي

```
<#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
```

يفيظو ويراني س - طاقت لا

في CAPI طاقت لا وه اذه . ةلكشم لا (64/ى ل 48/نم) ةيعرف لا ةكبش لا عانق رييغت حلصأ

ي. فيظولا ويراني سل

No.	Time	Source	Destination	Protocol	Length	Info
1	2019-10-24 15:17:20.677775	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 15:17:20.677989	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 15:17:20.678401	fc00:1:1:1::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::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::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	fc00:1:1:1:2::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::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::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::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::2	fc00:1:1:1:1::100	ICMPv6	114	Echo (ping) reply id=0x097e, seq=4, hop limit=64 (request in 9)

ة: سيئرلا طقنلا

1. ثبلا زاهج MAC ناوع بلط يتلا IPv6 ةرواجم بلط بلط ةلاسر هجوملا لسري (IP FC00:1:1::1).
2. راج IPv6 نالعا مادختساب ةيماحلا راج دودر.
3. دودر يلعل لصحيو ICMP ECHO تابلط هجوملا لسري.

م CAPO تايوتحم

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...	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::2	ICMPv6	118	Echo (ping) request id=0x097e, seq=1, hop limit=64 (reply in 6)
4	2019-10-24 15:17:22.677943	fc00:1:1:2:2::2	ff02::1:ff00:1	ICMPv6	90	Neighbor Solicitation for fc00:1:1:2:2::2 from 4c:4e:35:fc:fc:d8
5	2019-10-24 15:17:22.678096	fc00:1:1:2:2::2	fc00:1:1:2:2::2	ICMPv6	90	Neighbor Advertisement fc00:1:1:2:2::2 (rtr, sol, ovr) is at 00:be:75:f6:1d:8e
6	2019-10-24 15:17:22.678462	fc00:1:1:2:2::2	fc00:1:1:1:1::100	ICMPv6	118	Echo (ping) reply id=0x097e, seq=1, 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::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::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::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::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::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::2	fc00:1:1:1:1::100	ICMPv6	118	Echo (ping) reply id=0x097e, seq=4, hop limit=64 (request in 11)

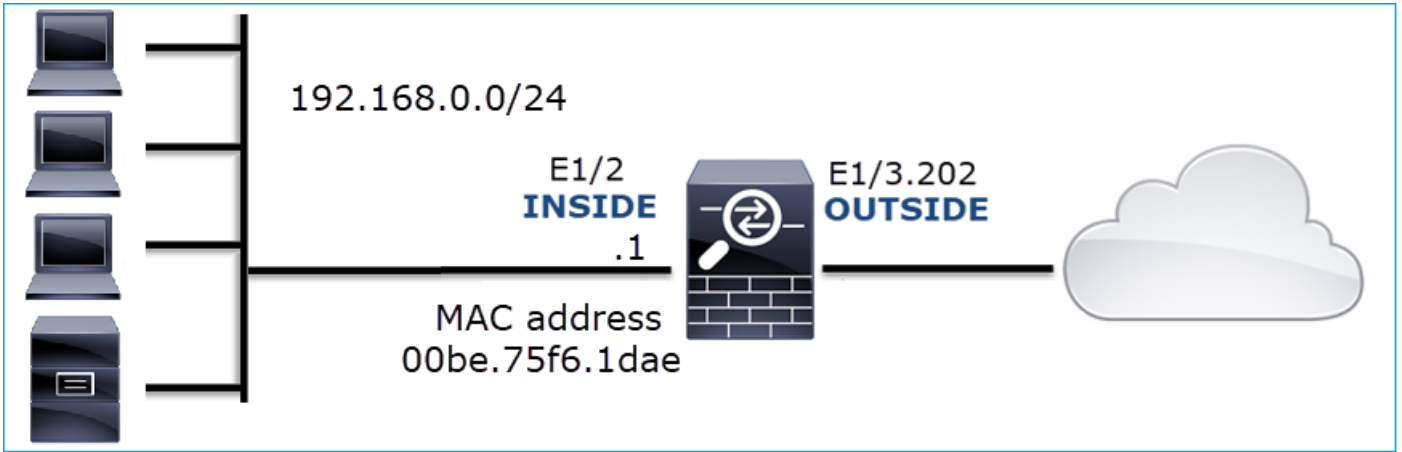
ة: سيئرلا طاقنلا

1. ثبلا زاهج MAC ناوع بلط يتلا IPv6 ةرواجم بلط ةلاسر ةيماحلا راج لسري (IP FC00:1:1:2::2).
2. راج IPv6 نالعا مادختساب ةيماحلا راج دودر.
3. ICMP Echo بلط ةيماحلا راج لسري.
4. قفدت زاهج MAC ناوع بلط يتلا IPv6 ةرواجم بلط بلط ةلاسر هجوملا لسري (IP FC00:1:1:2::2).
5. راج IPv6 نالعا مادختساب ةيماحلا راج دودر.
6. دودر يلعل لصحيو ICMP ECHO تابلط ةيماحلا راج لسري.

12. ةلاجال (ARP ميمست) عطقتملا ليصوتلا ةلكشم

ةعطقتم لاصتا لكاشم (192.168.0.x/24) ةيلخادلا ةفيضملا ةزهجال هجاوت: ةلكشملا فصو اهسفن ةيعرفلا ةكبشلا يف ةفيضملا ةزهجال عم

طاطملا ةروصلا هذه ضرعت



رثأتملأ قفدتلا:

SRC IP: 192.168.0.x/24

DST IP: 192.168.0.x/24 رادصلإا لوكوتورب

يأ: لوكوتوربلا

اهميسست مت دق يلخاد فيضمل تقؤملا ARP نيزخت ةركاذ نأ ودبي:

```

C:\Windows\system32\cmd.exe
C:\Users\mzafeirol>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\mzafeirol>

```

رسأ ليلحت

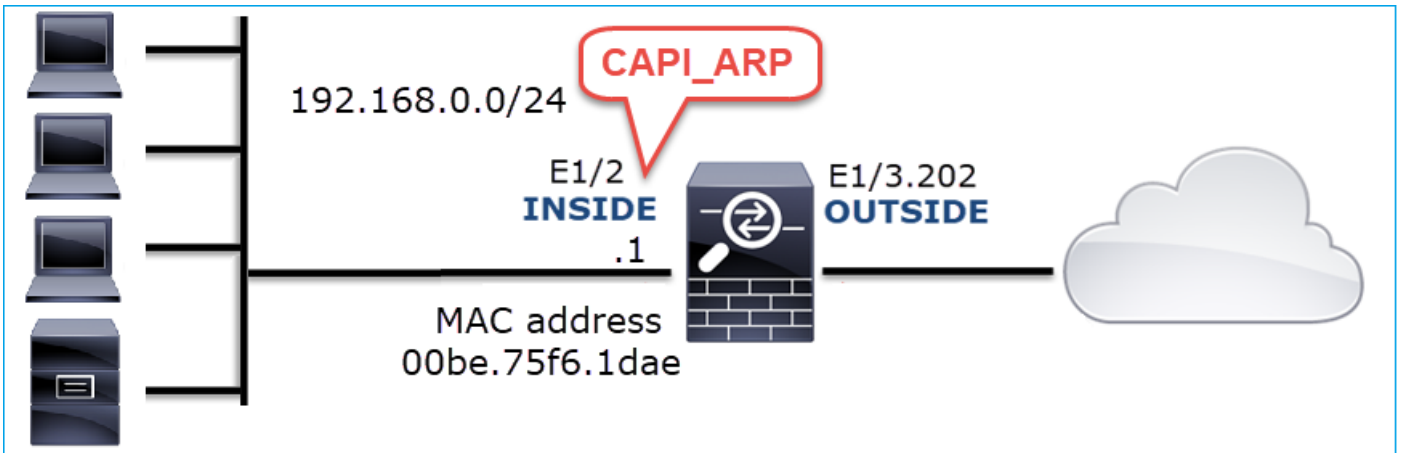
FTD LINA كرحم ىلع طاقتلا نيكمت

ةيلخادلا ةهجاولا ىلع طوقف ARP مزح طاقتلا اذه ضبق ىلع:

<#root>

firepower#

capture CAPI_ARP interface INSIDE ethernet-type arp



لمع ي ال ويراني س - طاقنل

INSIDE. ةامحل راج ةه جاو لى ع طاقنل ال يوتحي

No.	Time	Source	Destination	Protocol	Length	Info
4	2019-10-25 10:01:55.179571	Vmware_2c:9b:a7	Broadcast	ARP	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	42	192.168.0.23 is at 00:be:75:f6:1d:ae
35	2019-10-25 10:02:13.050397	Vmware_2c:9b:a7	Broadcast	ARP	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	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	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	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	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	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	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	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	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	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	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	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	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	42	192.168.0.30 is at 00:be:75:f6:1d:ae

ة:سيئرل طاقنل

1. ةبش نمض IPs لجا نم ةفلتخم ARP تا بل ط ةامحل راج ي قلت ي
2. ب صا ل ال MAC ناوع ما دخت س اب (proxy-arp) ني وانع ال هذه لك لى ةامحل راج بيحت سي

اهب يصومل تا اءار ل

ة. لاسم ال هذه قاطن قي ي ضت ةدايز وه عرف ال اذه ي ةراول تا اءار ل نم ضرغ ل

ل ي كشت nat ل تصح ف 1. اءار ل

ع نم no-proxy-arp ةساس ال ةم لك ل ال اه ي ف نكم ي تا ل اح كانه ، NAT ني وك تب قل ع تي ام ي ف ق باس ل كولس ل

<#root>

firepower#

show run nat

تانايب لاري فشتو 3 رادصل ال SNMP ةقداصل مل دامتعا تانايب هيدل ناك FTD لوؤسم نأ امب
هذه لمعال ةطخ حارتقا مت

1. مزح طاقتل ال SNMP

ديدحتل Wireshark ب صاخ ال SNMP لوكوتورب تاليفضفت مدختساو طاقتل ال لظفا
مادختسا متي 3 رادصل ال SNMP مزح ريفشت كفل SNMP نم 3 رادصل ال دامتعا تانايب
اهعاجرتساو ةيدامل ال SNMP تافرعم ليلحتل اهريفشت كفت مت يتل طاقتل ال تاي لمع

snmp: مداخل فيضم نيوكت في اهمادختسا متي يتل ال ةهجال ال ال ع SNMP مزح طاقتل ال نيوكت

```
<#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 capsnpmp interface management buffer 10000000 match udp host 192.168.10.10 host 192.168.5.254 eq
```

```
firepower#
```

```
show capture capsnpmp
```

```
capture capsnpmp 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	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	0.325	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	560	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	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	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	560	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: 80000009fe1c6dad4930a00ef1fec2301621a4158bfc1f40_
  msgAuthoritativeEngineBoots: 0
  msgAuthoritativeEngineTime: 0
  msgUserName: netmonv3
  msgAuthenticationParameters: ff5176f5973c30b62ffc11b8
  msgPrivacyParameters: 000040e100003196
  > msgData: encryptedPDU (1)
    encryptedPDU: 879a16d23633400a0391c5280d226e0cec844d87101ba703_

```

ةيسيرلر طاقنل:

- ةجولل و SNMP رصم نيوانع/ذفانم.
- Wireshark ل فورعم ريغ privKey نأل SNMP لوكوتورب تانايب ةدحو زيمرت ك ف رذعت.
- ةيلوال EncryptedPDU ةميقي.

اهب يصومل تاءارجلال

ةلأسملل هذه قاطن قيييضت ةدايز وه عرفلل اذه يف ةدراولل تاءارجلال نم ضرغلل او

SNMP طاقنل ريفشت ك فب مق 1. ءارجلال

دامتعا تانايب دي دحتل Wireshark ب صاخلل SNMP لوكوتورب تال ييضفت ررحو طاقنللال ظفحلا مزحلل ريفشت ك فل SNMP نم 3 رادصلال

```
<#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
```

> لوكوتوربالتاليضفت إلىحفصتو SNMP مزمح دح، Wireshark، لى طاقتلالال فلم حتفا
 ةروصلال ي ف حضوم وه امك، نيمدختسملال لودج:

The screenshot shows the Wireshark interface with a list of captured packets. The selected packet (No. 3) is an SNMP report. A context menu is open over the packet, and the 'Users Table...' option is highlighted. The packet details pane shows the following information:

```

    <[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
    
```

ةقداصلال جذومنو SNMP نم 3 رادصلال مدختسم مسا ديدحت مت، SNMP يمدختسم لودج ي ف
 تانايب ضرع متي ال) ةيصوصخالل رورم ةمكلو ةيصوصخالل لوكوتوربو ةقداصلال رورم ةمكلو
 (هاندا ةيلعلال دامتالال

The 'SNMP Users' dialog box is shown with the following table:

Engine ID	Username	Authentication model	Password	Privacy protocol	Privacy password
		MD5		DES	

The dialog also includes a '+' button to add new users, a '-' button to remove users, and a 'Users Table...' button to view the current table. The path to the users file is shown as: `C:\Users\iqasimov\AppData\Roaming\Wireshark\profiles\Profile1\snmp_users`. Buttons for 'OK', 'Copy from', 'Cancel', and 'Help' are at the bottom.

SNMP لوكوتورب تانايب تادحو ضرع ب Wireshark ماق، SNMP يمدختسم تادادعإ قيبطت درجم ب
 اهريفشت ك ف متي الال (PDU):

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	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	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 1.3.6.1.4.1.9.9.221.1.1.1.2.1.1 1.3.6.1.4.1.9.9.221.1.1.1.2.1.2 1.3.6.1.4.1.9.9.221.1.1.1.3.1.8
7	0.490	SNMP	192.168.10.10	65484	161	192.168.5.254	205	getBulkRequest 1.3.6.1.4.1.9.9.221.1.1.1.3.1.8
8	0.490	SNMP	192.168.5.254	161	65484	192.168.10.10	560	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 1.3.6.1.4.1.9.9.221.1.1.1.6.1.8
9	0.675	SNMP	192.168.10.10	65484	161	192.168.5.254	205	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	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 1.3.6.1.4.1.9.9.221.1.1.1.8.1.8
11	0.945	SNMP	192.168.10.10	65484	161	192.168.5.254	205	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	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 1.3.6.1.4.1.9.9.221.1.1.1.18.1.8
13	1.133	SNMP	192.168.10.10	65484	161	192.168.5.254	205	getBulkRequest 1.3.6.1.4.1.9.9.221.1.1.1.18.1.8
14	1.134	SNMP	192.168.5.254	161	65484	192.168.10.10	588	get-response 1.3.6.1.4.1.9.9.221.1.1.1.19.1.1 1.3.6.1.4.1.9.9.221.1.1.1.19.1.2 1.3.6.1.4.1.9.9.221.1.1.1.20.1.8
15	1.317	SNMP	192.168.10.10	65484	161	192.168.5.254	205	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	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 1.3.6.1.4.1.9.9.392.1.1.4.0
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	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	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	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 1.3.6.1.4.1.9.9.221.1.1.1.3.1.8
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 1.3.6.1.4.1.9.9.221.1.1.1.5.1.1 1.3.6.1.4.1.9.9.221.1.1.1.5.1.2 1.3.6.1.4.1.9.9.221.1.1.1.6.1.8
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

```

< msgData: encryptedPDU (1)
  encryptedPDU: 879a16d23633400a0391c5280d226e0cec844d87101ba703...
  Decrypted ScopedPDU: 303b041980000009fec6dad4930a00ef1fec2301621a4158bfc1f40...
    contextEngineID: 80000009fec6dad4930a00ef1fec2301621a4158bfc1f40...
    contextName:
    data: getBulkRequest (5)
      getBulkRequest
        request-id: 5620
        non-repeaters: 0
        max-repetitions: 16
      variable-bindings: 1 item
        1.3.6.1.4.1.9.9.221.1: Value (Null)
          Object Name: 1.3.6.1.4.1.9.9.221.1 (iso.3.6.1.4.1.9.9.221.1)
          Value (Null)
  
```

ةيسيرل طاقنل:

1. ربع لقننل لاولم العتس الل SNMP GetBulkRequest ةبقارم تاودأ مدختست 1.3.6.1.4.1.9.9.221.1 لصلأل ةلصلل تاوذ OID تافرع م و 1.3.6.1.4.1.9.9.221.1 لصلأل.
2. ب ةقلعتم الل OIDs لعل يوتحي يذل get-response عم GetBulkRequest لك فلتس ا. 1.3.6.1.4.1.9.9.221.1.

ةيداملل SNMP تافرع م لعل فرعتل 2. ءارجلل.

(MIB) ةرادلل تامولعم ةدعاق لعل يمتنل 1.3.6.1.4.1.9.221.1 نأ SNMP نئلك حفصتم رهظأ ةروصلل ي فحضم وه امك، Cisco-Enhanced-MEMPOOL-MIB ةامس ملل

Tools & Resources

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

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

Enter OID or object name: 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)
  
```

Wireshark: في ناسنإل لبق نم هتءارق نكمي قيسنتب OIDs ضرعل

- وه امك، اهتاي عبتو Cisco-Enhanced-Mempool-MIB نم (MIB) ةرادإل تامولعم ةءءاق ليزنت 1. ةروصلال في ءضوم:

Tools & Resources

SNMP Object Navigator

HOME | SUPPORT | TOOLS & RESOURCES | **SNMP Object Navigator**

TRANSLATE/BROWSE | SEARCH | DOWNLOAD MIBS | MIB SUPPORT - SW | Help | Feedback

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

List matching MIBs

- 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

Tools & Resources
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 Dependencies
2. SNMPv2-TC	Download	Download	View Dependencies
3. SNMPv2-CONF	Not Required	Download	View Dependencies
4. SNMP-FRAMEWORK-MIB	Download	Download	View Dependencies
5. CISCO-SMI	Download	Download	View Dependencies
6. ENTITY-MIB	Download	Download	View Dependencies
7. HCNUM-TC	Download	Download	View Dependencies
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	

2. مذفان (مسالال ليلحت) > Preferences > Name Resolution (ريلحت) في Wireshark في Edit (م ساراسم) في SMI. اهديدحت متي OID ةقو نيكمت مادختساب دلجملا راطالاددحي (MIB و PIB) في SMI. اهديدحت متي (MIB) ةرادال تامولعم دعواق Cisco-Enhanced-Mempool-MIB ةفاضا مت. ةيظمنلا تادحولا ةمئاق لئلا ايلئاق لئلا CISCO-Enhanced-Mempool-MIB:

The screenshot shows the Wireshark Preferences dialog box with the 'Name Resolution' section expanded. The 'Enable OID resolution' checkbox is checked. The 'SMI Paths' dialog is also open, showing the directory path 'C:/Users/Administrator/Downloads/SNMPMIBS' selected. The 'SMI Modules' dialog is also open, showing the list of modules with 'CISCO-ENHANCED-MEMPOOL-MIB' selected.

3. OID ةقو طيشنت متي، Wireshark، ليلغشت ةداعل درجم 3:

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 SNMP-USER-BASED-SM-MIB::usrStatsUnknownEngineIDs.0
3	0.176	SNMP	192.168.10.10	65484	161	192.168.5.254	197	getBulkRequest CISCO-ENHANCED-MEMPOOL-MIB::cempMIBObjects
4	0.176	SNMP	192.168.5.254	161	65484	192.168.10.10	192	report SNMP-USER-BASED-SM-MIB::usrStatsNotInTimeInWindows.0
5	0.325	SNMP	192.168.10.10	65484	161	192.168.5.254	199	getBulkRequest CISCO-ENHANCED-MEMPOOL-MIB::cempMIBObjects
6	0.326	SNMP	192.168.5.254	161	65484	192.168.10.10	678	get-response CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolType.1.1 CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolType
7	0.490	SNMP	192.168.10.10	65484	161	192.168.5.254	205	getBulkRequest CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolName.1.8
8	0.490	SNMP	192.168.5.254	161	65484	192.168.10.10	560	get-response CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolAlternate.1.1 CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoc
9	0.675	SNMP	192.168.10.10	65484	161	192.168.5.254	205	getBulkRequest CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolValid.1.8
10	0.675	SNMP	192.168.5.254	161	65484	192.168.10.10	610	get-response CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolUsed.1.1 CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolUsed
11	0.945	SNMP	192.168.10.10	65484	161	192.168.5.254	205	getBulkRequest CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolFree.1.8
12	0.946	SNMP	192.168.5.254	161	65484	192.168.10.10	584	get-response CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolUsedOvrflw.1.1 CISCO-ENHANCED-MEMPOOL-MIB::cempMemPc
13	1.133	SNMP	192.168.10.10	65484	161	192.168.5.254	205	getBulkRequest CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolHCUsed.1.8
14	1.134	SNMP	192.168.5.254	161	65484	192.168.10.10	600	get-response CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolFreeQue.1.1 CISCO-ENHANCED-MEMPOOL-MIB::cempMemP


```

CISCO-ENHANCED-MEMPOOL-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-MEMPOOL-MIB::cempMemPoolName.1.1)
CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolName: System memory
CISCO-ENHANCED-MEMPOOL-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-MEMPOOL-MIB::cempMemPoolName.1.2)
CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolName: System memory
CISCO-ENHANCED-MEMPOOL-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-MEMPOOL-MIB::cempMemPoolName.1.3)
CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolName: MEMPOOL_MSGLYR
CISCO-ENHANCED-MEMPOOL-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-MEMPOOL-MIB::cempMemPoolName.1.4)
CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolName: MEMPOOL_HEAPCACHE_1
CISCO-ENHANCED-MEMPOOL-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-MEMPOOL-MIB::cempMemPoolName.1.5)
CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolName: MEMPOOL_HEAPCACHE_0
CISCO-ENHANCED-MEMPOOL-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-MEMPOOL-MIB::cempMemPoolName.1.6)
CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolName: MEMPOOL_DMA_ALT1
CISCO-ENHANCED-MEMPOOL-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-MEMPOOL-MIB::cempMemPoolName.1.7)
CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolName: MEMPOOL_DMA
CISCO-ENHANCED-MEMPOOL-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-MEMPOOL-MIB::cempMemPoolName.1.8)
CISCO-ENHANCED-MEMPOOL-MIB::cempMemPoolName: MEMPOOL_GLOBAL_SHARED

```

موقت SNMP بقارم ةادأ تناك ، طاقنالال ف لمل هري فشت ك ف مت يذلا جارخالال الى اذانتسا وه امك . FTD يلع ةركاذلا تا عمت مادختسا انايب صحفب (ناوٹ 10 ل صاف) يرود لكشب حسمو ، ةركاذلاب ةول عمتل انايب اصلال ASA SNMP عارتقا ناف TechNote ةلاقم يف حضورم ةدحو مادختسا ن عجتني SNMP مادختساب (GSP) يملع الال كرتشم الال عمتل مادختسا حضاولا نم ناك ، (طاقنالال) Capture نم ةالجال هذه يف . ربك لكشب (CPU) ةيزك رملال ةجالع الال GetBulkRequest نم عكج يرود لكشب "يملع الال كرتشم الال عمتل" مادختسا صحف مت دنق هنا ل يلو الال SNMP .

تمت ، SNMP ةي لمع اهيف ببستت يالال (CPU) ةيزك رملال ةجالع الال ةدحو عا طخال ليلقت لجال نم SNMP لوكوتوربل ةيزك رملال ةجالع الال ةدحو عا طخال في فخنال تاو طخال عا بتاب ةي صوتالال نودب . GSP ماظناب ةطب ترملال الال ةفرعم الال طتسا بنجت و ةلاقم الال يف اهيل راشم الال متي مل ، GSP راي عمب طب ترملال (OIDs) دروم الال ةئف فرعمل SNMP لوكوتورب ربع الال طتسا حضفخنا امك ، SNMP لوكوتورب ةي لمع ن عجتان الال ةيزك رملال ةجالع الال ةدحو عا طخال ةي ا ةطخال مل طو حلم لكشب زواجنالال ل ددم .

ةلص تا ذتامول عم

- Cisco ةك رشل عباتلال FireSIGHT ةرادا زك رمل نيوكت ةلدأ
- Firepower Threat جمانرب يلا لوصولال يف مكحتلال ةسايس دعاوق تا اعارجالا حضوت Defense
- مزجالا عبتتو FirePOWER ديدهت دض عاف دلال تا عوم جم عم لمع الال
- مزجالا عبتتو Wireshark

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤتو تامچرتل هذه ةقدنع اهتيلوئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل