

مكحتللة دحوب ةصاخلا لفطتلا ثادحأ ضرعت (FMC) ةيلارديفلا تالاصتالا ةرادإ يف لئاسرلا؛ ةماع تانايب

تايوتحملا

ةلأسم

• مدختسملا ةهجاو يف ةيفصولا لفطتلا ةدعاق لئاسر ضرعت لفطتلا ثادحأ دعت مل رثؤتو ذي فننلل ةلباقلا هيبنتلا تامولعم دقف اهنع جتنتو FMC ل (GUI) ةيموسرلا نامألا ةبقارم تاناكمإ ىلع

• اذه لثم يجذومن لكشب Echo دودرب ةصاخلا قارتخالا ثدح ةلاسرهظت

• ICMP Echo Response (1:408:8) لوكوتوربلا

هيبنت" لك ةيمومع رثكأ لكشب ريخشلا لئاسر روهظ يف ةلكشملا ببستت، كلذعمو
":ريخشلا

Snort Alert (1:408:8)

• لثم طقف ةماع تالاخدا نع ةرابع يه ةضورعلملا فاصولأاو ةيلعفلا ةدعاقلا عامسأ
Snort (gid:sid:"rev). هيبنت

Overview Analysis Policies Devices Objects Integration				
Context Explorer	Unified Events	Connections ▼	Intrusions ► Events	Files ▼ Hosts ▼ Users ▼ Correlation ▼ Advanced ▼ Search

Events By Priority and Classification [\(switch workflow\)](#)

[Drilldown of Event, Priority, and Classification](#) > [Table View of Events](#) > [Packets](#)

No Search Constraints ([Edit Search](#))

Jump to... ▼

☐	Message	▼ Priority	Classification
☐	Snort Alert (1:51390:2)	medium	Attempted Information Leak
☐	Snort Alert (1:1000074:6)	low	Generic ICMP Event
☐	Snort Alert (1:1000087:5)	high	Web Application Attack
☐	Snort Alert (1:41421:2)	high	Web Application Attack
☐	Snort Alert (1:63309:1)	high	Web Application Attack
☐	Snort Alert (1:16431:6)	high	Web Application Attack
☐	Snort Alert (1:58726:7)	high	Attempted User Privilege Gain
☐	Snort Alert (1:58737:5)	high	Attempted User Privilege Gain
☐	Snort Alert (1:58723:6)	high	Attempted User Privilege Gain
☐	Snort Alert (1:58743:6)	high	Attempted User Privilege Gain
☐	Snort Alert (1:58742:8)	high	Attempted User Privilege Gain
☐	Snort Alert (1:65554:1)	high	Attempted User Privilege Gain
☐	Snort Alert (1:58744:6)	high	Attempted User Privilege Gain
☐	Snort Alert (1:58722:5)	high	Attempted User Privilege Gain
☐	Snort Alert (3:58806:4)	high	Attempted User Privilege Gain

• ثدحل تامولعم يف ةدعاقلا رفوت مدع عم ةلاس رلا عون سفن رهظي ، ةمزل ضرع يف

Overview Analysis Policies Devices Objects Integration				
Context Explorer	Unified Events	Connections ▼	Intrusions ► Events	

Events By Priority and Classification [\(switch workflow\)](#)

[Drilldown of Event, Priority, and Classification](#) > [Table View of Events](#) > [Packets](#)

► Search Constraints ([Edit Search](#) [Save Search](#))

Event Information ▼

Message	Snort Alert (1:51390:2)
Time	2026-05-05 15:37:39
Classification	Attempted Information Leak
Priority	medium
Ingress Security Zone	
Device	
Ingress Interface	
Source IP	
Source Port / ICMP Type	60402 / tcp
Source Country	USA
Destination IP	
Destination Port / ICMP Code	80 (http) / tcp
Destination Country	USA
HTTP Hostname	
HTTP URI	
Intrusion Policy	
Access Control Policy	
Access Control Rule	
Rule	Rule Unavailable

• SIEM ةمظنأ إىل FMC نم اهرى دصت مت يتل syslog ثادحأ يتوتحت ، كلذى إىل ةفاضلإابو لوقحل هذهل ةغراف ميقي لىل

• sig_فرعم

• signature_msg

- ثدحل لئاسرب قلعتت ةددعت ماحتقإ ثادحأل ةرركتم عاطخأ FMC لئاسر لجس رهظي

Apr 10 23:28:56 FMC SF-IMS[21500]: [21500] EventStreamer child(192.X.X.210):sfestreamer [WARN] Unable to

- ةحولل ةرادإ يف مكحتل ةدحو ىلإ ةدراول قارتخال ثادحأ عيمج ىلع ةلكشملا رثؤتو نارينل ردصم ةدعاق ثاثيردحت ربع رمتستو ةرادملا راعشتسال ةزهجأ نم ةيساسأل FMC. نم ةيداعل (LSP) ةيلحمل نامأل ةمزحو (SRU)

ةئيبلا

- (313 ةينب) FMC 7.2.11 ضكري 2600 ةرادإ زكرم ةيامح رادج نمأي cisco يف ةرم لوا دهوش (HA) لاج رفوت يف
- مل اهنكلو VDB و GeoDB و sru/LSP ةدحول ةمظتنم ثاثيردحت تايلمع قيبطت متي امك ةلكشملا لحت

رارق

Sourcefire (SRU) ةدعاق ثاثيردحت ةمزحل يرابجإ تيبتت ةداعإ ءارجإ لالخ نم ةلكشملا لحت مت جىحص لكشب Snort عيقوت لئاسر تانايب ةدعاق ءاشنإ ةداعإل

ةمزح ثدحأ نم ققحتل او FMC مكحتل ةدحوب ةصاخلا (CLI) رماوأل رطس ةهجاو ىلإ لوصولا 1.-
ةتبتلم SRU

<#root>

```
> expert
admin@FMC:~$ sudo su
root@FMC:/Volume/home/admin# ls -halts /var/sf/SRU/ | grep SRU-2026-05
```

```
43M -rw-r--r-- 1 www www 43M May 27 04:02 Cisco_Firepower_SRU-2026-05-26-001-vrt.sh.REL.tar
```

```
43M -rw-r--r-- 1 www www 43M May 22 04:02 Cisco_Firepower_SRU-2026-05-20-001-vrt.sh.REL.tar
43M -rw-r--r-- 1 www www 43M May 20 04:02 Cisco_Firepower_SRU-2026-05-19-001-vrt.sh.REL.tar
43M -rw-r--r-- 1 www www 43M May 13 04:03 Cisco_Firepower_SRU-2026-05-12-001-vrt.sh.REL.tar
```

```
43M -rw-r--r-- 1 www www 43M May 8 04:03 Cisco_Firepower_SRU-2026-05-06-001-vrt.sh.REL.tar
43M -rw-r--r-- 1 www www 43M May 6 04:03 Cisco_Firepower_SRU-2026-05-04-001-vrt.sh.REL.tar
```

2.- sru: ةدحو ةمزل يرابجلال تيبتل ةداعل ذي فنن

<#root>

root@FMC:/Volume/home/admin#

```
install_update.pl --detach /var/sf/SRU/Cisco_Firepower_SRU-2026-05-26-001-vrt.sh.REL.tar --force
```

3.- رمال اذه مادختساب تيبتل مدقت بقعت

<#root>

root@FMC:/Volume/home/admin#

```
tail -f /var/log/sf/sru-2026-05-26-001-vrt/status.log & tail -f /var/log/sf/sru-2026-05-26-001-vrt/sru.
```

```
[260528 12:43:34] *****
[260528 12:43:34] [260528 12:43:34] **** Finish POST phase
[260528 12:43:34] [260528 12:43:34] COMPLETED post/999_finish.sh
[260528 12:43:34] [260528 12:43:34]
[260528 12:43:34] Lock //tmp/sru.lock for force install removed successfully.
[260528 12:43:34] [260528 12:43:34] Pruning logs and old installs
[260528 12:43:34] [260528 12:43:34]
[260528 12:43:34] [260528 12:43:34] #####
[260528 12:43:34] [260528 12:43:34] # FORCE COMPLETE
[260528 12:43:34] [260528 12:43:34] #####
ui:[63%] Running script installer/602_log_package.pl...
ui:[68%] Running script installer/900_update_version.sh...
ui:[74%] Running script installer/999_finish.sh...
ui:[79%] Running script post/000_start.sh...
ui:[84%] Running script post/500_copy_contents.sh...
ui:[89%] Running script post/900_iiru_log_finish.pl...
ui:[95%] Running script post/999_finish.sh...
ui:[100%] The force install completed successfully.
ui:The force install has completed.
state:finished
```

نأ نكمي امك ،لامنكالل ةقيقد 20 ىلإ لصي ام sru ةدحو تيبتل قرغتسي دق :ةطحال م
يعيبط لولس اذه .قئاقد ةدعل ةنيعم بسن دنع تبات هنا ىلع رهظي

4: حاجنب ةيرابجلال SRU تيبتل ةداعل ةيلمع لامنكال دعب

- ةدي دجل شادحألل FMC ةيرادلإل مكحتل ةدحو ىلع ل فطتل شادحأ ةحفص ةبقارم
- نم الدب ةبسانملا رخشل ةدعاق لئاسر ضرعت ةدي دجل ل فطتل شادحأ نأ نم ققحت "رخشل هيبنت" ةماعلا تالاخلإل
- ةلوهأم عي قوت لوقح ىلع نألل يوتحت SIEM ةمظنأ ىلإ syslog تارداص نأ نم دكأت

نودب أقبسّم اهؤاشنا مت يتلثادحأل لظت. يعجر رثأب سيل حالصإلا اذه: حيملت لئاسر ةديجل لفطتلثادحأ عيمج ضرعت نأ بجي نكلو، ريغت نودب ءحيحص ءلاسر ءحيحص لكشب syslog لوقح رشن ءو ءحيحصلل Snort ءءاق

پ پ س ل ا

عنم امم Snort، عي قوت لئ اسرر تانا ي ب ة د عاق ن مازت ا غل ا و/و فلت ي ف FMC ي ب ع ب ب س ت
اذه ب ق ع ت م ت ي . اه ت ب ع ت و ق ا ر ت خ ا ل ا ث ا د ح ا ي ف Snort ة د عاق ف ي ر ع ت ت ا ن ا ي ب ل ح ن م FMC
Cisco CSCwu63768. ن م ا ط خ ا ل ا ح ي ح ص ت ف ر ع م ت ح ت ك و ل س ل ا

sru/LSP، ةدحول قباس شيدحتل حيحصلا ريغ تيبتتلال نع تجتن دق ةلكشملا هذه نأ دقتعيو
 يلع ةدوجوم عيقتولال فيرعت تانايب نأ ةلدألا ترهظأ. تيبتتال حاجنة يناملا يلع
 FMC ةطساوب اهلح رذعت نكلو (GID:SID:REV ةطساوب ةدحملال شادحال) رعشتسملال يوتسم
 تانايبلا ةدعاق فلت بابسب syslog ريصت وأ حيحص لكشب لئاسرلا ضرعل

ةلصللا يذى وتحمللا

- [Cisco Bug ID CSCwu63768](#)
- [Sourcefire ةدعاق شيدحت تاليزنت](#)
- [Cisco نم تاليزنت لاو ينفلإ معدلا](#)

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا