

بقعت ةادأ مادختساب ةمزحلا لئغشت ةداعإ FMC يف مزحلا

تايوتحمل

[ةمدقملا](#)

[ةيساسالاب لطلتملا](#)

[تاب لطلتملا](#)

[ةمدختسملا تانوكملا](#)

[FMC ىلع ةرفوتملا مزحلا بقعت ةادأ مادختساب ةمزحلا لئغشت ةداعإ](#)

[PCAP فلم مادختساب مزحلا لئغشت ةداعإ](#)

[رايخلا اذه مادختسا دويق](#)

[قصلاب تاذ تادنتسملا](#)

ةمدقملا

طبر FMC GUI لمعتسي ةادأ FTD ك يف طبر تدعأ عيطتسي تنأ فيك ةقيثو اذه فصبي
tracer ةادأ.

ةيساسالاب لطلتملا

تاب لطلتملا

ةيلاتل عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت

- FirePOWER ةينقت ةفرعم
- ةيامل راج لالخ نم ةمزحلا قفدت ةفرعم

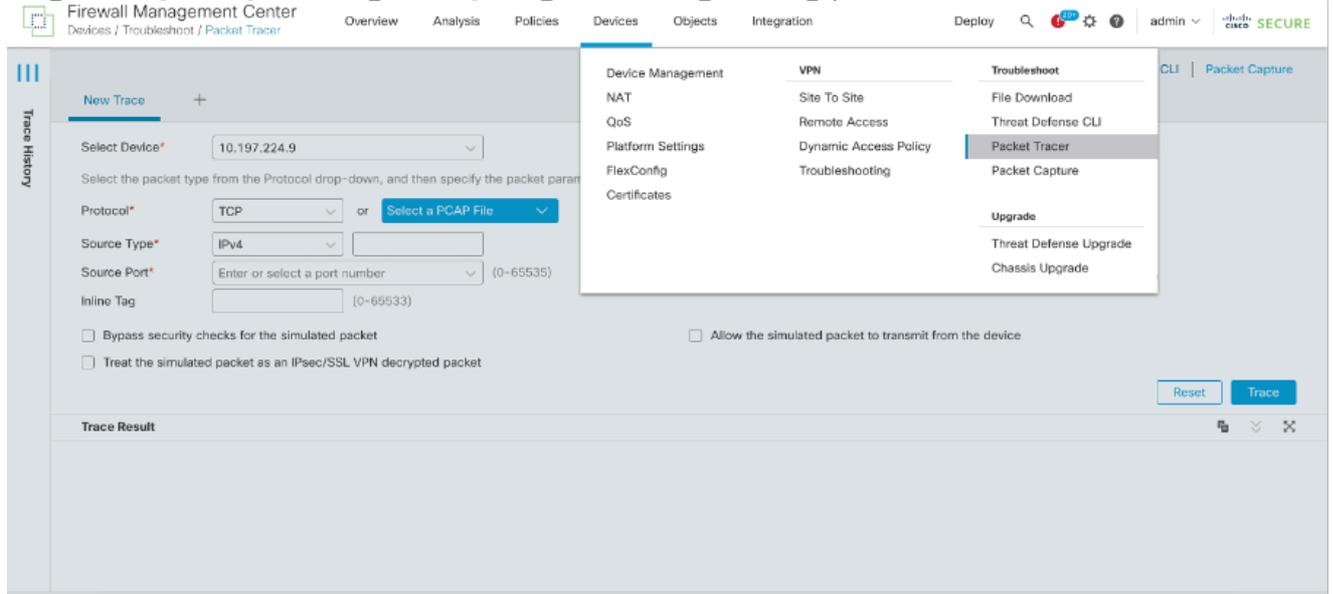
ةمدختسملا تانوكملا

- ديدهت دض عافدلا جم انرب نم 7.1 رادصل او Cisco نم (FMC) نم آلا ةيامل راج ةرادإ زكرم
ثدحأ رادصل أو Cisco نم (FTD) ةيامل راج
- PCAP قيسنتب مزحلا طاقتل تافل م

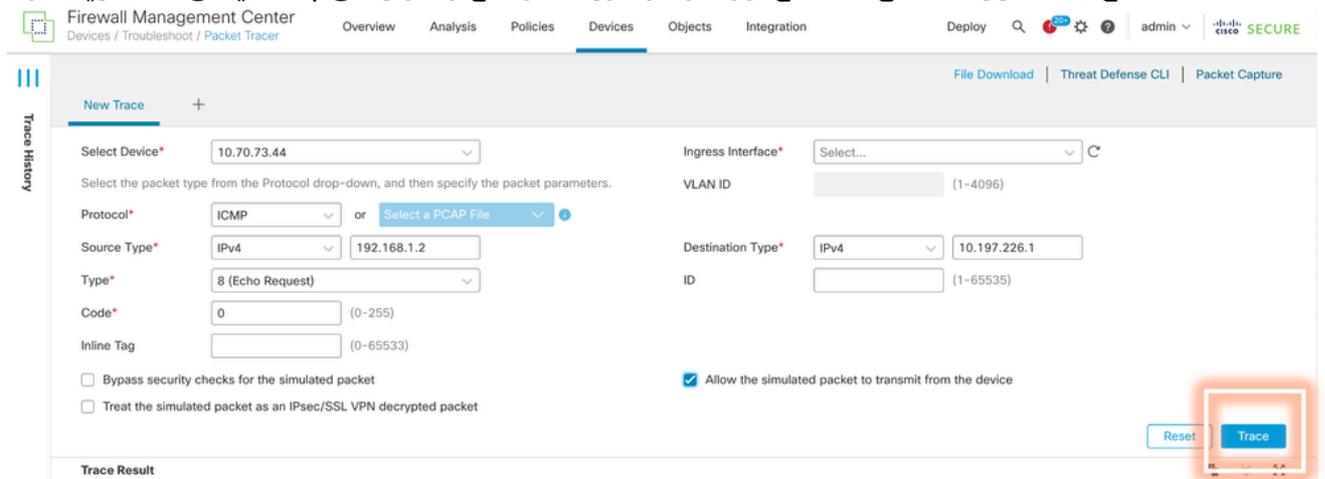
ةصاخ ةي لمعم ةئيبي يف ةدوجوملا ةزهجال نم دنتسملا اذه يف ةدراولا تامولعمل عاشنإ مت
تناك اذإ. (يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجال عي مج تادب
رمأ يال لم تحملا ريثاتلل كم هف نم دكأتف ، لئغشتلا دي ق ك تكبش

ةرفوتملا مزحلا بقعت ةادأ مادختساب ةمزحلا لئغشت ةداعإ FMC ىلع

1. إلى لوقتنا FMC م كحتال ة دحول (GUI) ةي موسرلا مدختسمل ةه جاو إلى لوخدلا لي جست . مزحلل بقعت ةاداً > اه حالصاو عا طخال فاشكتسأ > ةزهجال



2. عبت رقنا . لوخدلا ةه جاوو لوكوت ووربل او ةه جولو او ردصملا لي صافات ريفوت .



3. نم ةمزحلل هذه لي غشت ةداعإل زاهجال نم ثبلاب ةاكاحملا ةمزحلل حامسلا رايلخال مدختسأ . زاهجال

4. في م كحتال ةسايس في اه نيوكت مت ةدعاق دوجو ببسب ةمزحلل طاقسإ مت هنأ ظحال . ICMP مزح طاقسإل لوصول

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 50% ⚙️ ? admin ✓ CISCO SECURE

Reset Trace

Trace Result: DROP

Packet Details: 11:59:51.233 - 192.168.1.2 > 10.106.226.1 ICMP

PC(vrfd:0)

- ACCESS-LIST
- INPUT-ROUTE-LOOKUP | Resolve Egress Interface
- ACCESS-LIST | log
 - Type: ACCESS-LIST
 - Subtype: log
 - Result: **DROP**
 - Config: access-group CSM_FW_ACL_global access-list CSM_FW_ACL_advanced deny object-group ICMP_ALLOW ifc PC any ifc OUT any rule-id 268454920 event-log flow-start access-list CSM_FW_ACL_remark rule-id 268454920: ACCESS POLICY: Port-scan test Mandatory access-list CSM_FW_ACL_remark rule-id 268454920: L4 RULE: block ICMP
 - Additional Information
 - Result: drop
 - Input Interface: PC(vrfd:0)
 - Input Status: up
 - Input Line Status: up
 - Output Interface: OUT(vrfd:0)
 - Output Status: up
 - Output Line Status: up
 - Action: drop
 - Drop Reason: **(acl-drop) Flow is denied by configured rule**
 - Drop Detail: , Drop-location: frame 0x000000aaacd0eb0 flow (NA)/NA
- OUT(vrfd:0)

5. (حضور وه امك) عبت لل ةيئاهن لل ةجيتن لل TCP مزح عم هذه مزحل عبت ةادأ.

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 50% ⚙️ ? admin ✓ CISCO SECURE

File Download Threat Defense CLI Packet Capture

New Trace +

Select Device* 10.70.73.44

Select the packet type from the Protocol drop-down, and then specify the packet parameters.

Protocol* TCP or Select a PCAP File

Source Type* IPv4 192.168.1.2

Source Port* 1234 (0-65535)

Inline Tag (0-65533)

Bypass security checks for the simulated packet

Treat the simulated packet as an IPsec/SSL VPN decrypted packet

Allow the simulated packet to transmit from the device

Ingress Interface* PC - Ethernet1/1

VLAN ID (1-4096)

Destination Type* IPv4 10.197.226.1

Destination Port* 443 (0-65535)

Reset Trace

Trace Result: ALLOW

Packet Details: 12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP

PC(vrfd:0)

- INPUT-ROUTE-LOOKUP | Resolve Egress Interface
- ACCESS-LIST | log
- CONN-SETTINGS

PCAP فلم مادختساب مزحل لئغشت ةداعإ

للع رقناو لوخذلا ةهجاو دح مٲ. PCAP فلم ديدحت رزلا مادختساب PCAP فلم لئمحت كنكمي عبت لل.

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ? admin | **SECURE**

File Download Threat Defense CLI Packet Capture

New Trace 3 +

Select Device* 10.197.224.9

Select the packet type from the Protocol drop-down, and then specify the packet parameters.

Protocol* TCP or Select a PCAP File

Source Type* IPv4

Source Port* Enter or select a port number (0-65535)

Inline Tag (0-65533)

Ingress Interface* outside - GigabitEthernet0/1

VLAN ID (1-4096)

Destination Type* IPv4

Destination Port* Enter or select a port number (0-65535)

Bypass security checks for the simulated packet

Allow the simulated packet to transmit from the device

Treat the simulated packet as an IPsec/SSL VPN decrypted packet

Reset Trace

Trace Result

رايخال اذه مادختسا دويق

1. طبق TCP/UDP مزح ةاكاحم اننكمي.
2. 100 وه PCAP فلم ي ف ةمومدملا مزحلل ددعل ىصقألا دحلا.
3. تياباغي م 1 نم لقا PCAP فلم مزح نوكي نأ بجي.
4. لعل طبق يوتحي نأ بجي و (قحللملا انمضتم) افرح 64 PCAP فلم مسا زواجتي الأ بجي. امهالك وأ ("_" وأ "-" وأ ".") ةصاخ فورح وأ ةي مقر ةي دج بأ.
5. ايلاح ةدحاو قفدت مزح ىوس معد متي ال.

حل اص ريغ IP سارك طاقس إلابس 3 عبتتلا رهظي

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ? admin | **SECURE**

Select the packet type from the Protocol drop-down, and then specify the packet parameters.

Protocol* UDP or single2.pcap

Source Type* IPv4 192.168.29.58

Source Port* 60376 (0-65535)

Inline Tag (0-65533)

VLAN ID (1-4096)

Destination Type* IPv4 192.168.29.160

Destination Port* 161 (0-65535)

Bypass security checks for the simulated packet

Allow the simulated packet to transmit from the device

Treat the simulated packet as an IPsec/SSL VPN decrypted packet

Reset Trace

Trace Result: **Error: Some packets from the PCAP file were not replayed.**

Packet 1: 11:58:21.875534

Packet Details: 11:58:21.875534 192.168.29.58:60376 > 192.168.29.160:161 udp 80

inside(vrfid:0)

Result: drop

Input Interface: inside(vrfid:0)

Input Status: up

Input Line Status: up

Output Interface: NP Identity Ifc

Action: drop

Time Taken: 0 ns

Drop Reason: (invalid-ip-header) Invalid IP header

Drop Detail: Drop-location: frame 0x000055f7c1b1b71b flow (NA)/NA

NP Identity Ifc

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن ت س م ل ا اذ ه Cisco ت مچرت
م ل ا ل ا اء ن ا ع مچ 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 و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ 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 مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
S y s t e m s (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 دن ت س م ل ا