

ال يتل FTD ن Traceroute ءاطخأ فاشكتسأ لاصتا رابتخإ مغر ةلقنلا تامولعم ضرعت حجانل ICMP

ةلأسم

رهظت ضارعالا هذه لك

- زاهج نم ةرشابم اهليغشت عدب متي يتل traceroute رم اوأ دوعت ال Traceroute لشف
تالقتل اعيمجل * * * ال تباث لكشب Cisco نم (FTD) ةيامحل رادج ديدت نع عافدل
ةجراخل IP نيوانع فادهتسإ دنع

- متيو، ءحجان اهسفن ءهجولا ل ICMP لاصتا تارابتخإ نوكت: ءحجان لاصتا ءينام
لوصولي فمكتل ءسايس في حيرص لكشب ICMP رورم ءكرب حامسلا

FTD، زاهج نم أشنت يتل رورملا ءكرحل راسملا تالقن في ءيؤرلا ءينام لكولسلا اذع نمي
اهالصال ءكبشلا راسم ءاطخأ فاشكتسأ دوهج ل ع رثؤي امم

لاثم

لمعي ءهجولا ل لاصتال رابتخإ

<#root>

firepower#

ping 192.168.203.89

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.203.89, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

سي ل traceroute نكلو

<#root>

firepower#

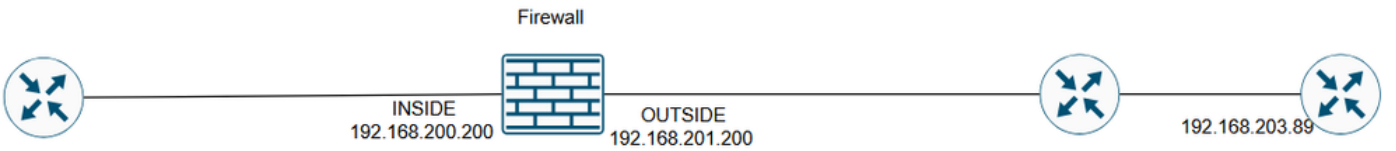
traceroute 192.168.203.89

```
Type escape sequence to abort.  
Tracing the route to 192.168.203.89  
 1*  *  *  
 2*  *  *  
 3*  *  *  
   ....  
30*  *  *  
firepower#
```

ةئبلا

- Cisco نم (FTD) ةئبلا راج ديهت نع نم آلا عافدلا
- ىرخأ خسن اضيأ رثأتت نأ نكميو، 7-6-2 و 7-4-2-3 و 7-4: يف ةرم لوأ طحولو
- ةرادلا ل Cisco (FMC / CDfmc / FDM) نم نم آلا ةئبلا راج ةرادا زكرم
- هاجت إلا ةئبلا تانويكتلا كذا يف امب، مادختسالا ديق ةتباثلا NAT دعاقو
- (Lina عضو) FTD CLI نم traceroute رماوأ ذيفنت مت
- لوصولا يف مكحتلا ةسايس يف هب حومسمل ICMP

طاطملا



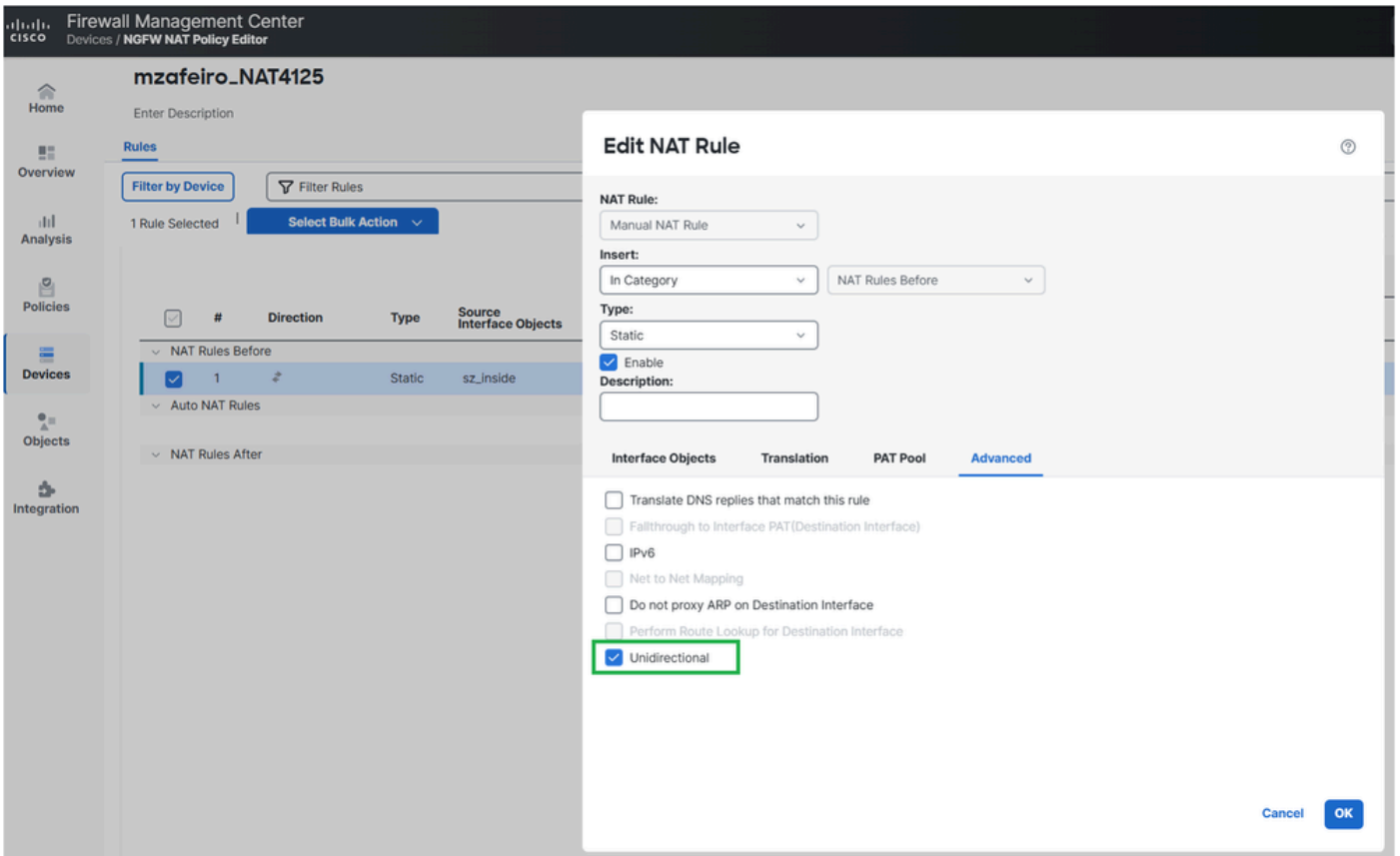
inline_image_0.png

راق

انويكت مت يتلا NAT دعاقو نم ضرغلا ىلع نكمملا لولحلا دمتعت

دعاق nat ل تلكش عي طتسي تنأ جراخ لوصول طقف ip لدان يخلخال مجرتي نأ فدهل انك نإ هاجت إيداح نأ أمب

NAT: دعاقول عم دقتمل تاراخيال نم كلذب مايقولل نكمي، FMC ىلع



inline_image_0.png

روش نمل NAT نيوكت

<#root>

firepower#

show run nat

```
nat (INSIDE,OUTSIDE) source static server_host interface unidirectional
firepower#
```

قحت ل

<#root>

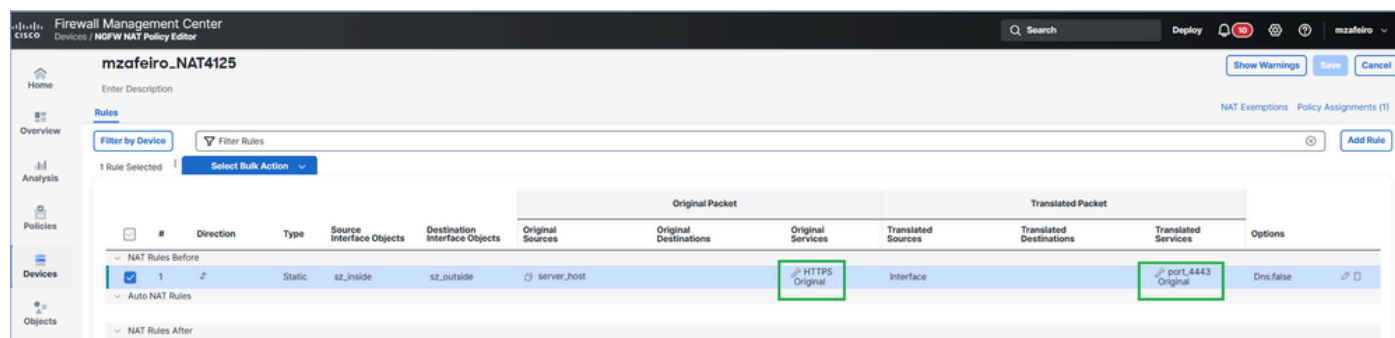
firepower#

traceroute 192.168.203.89

Type escape sequence to abort.
Tracing the route to 192.168.203.89
1 192.168.201.88 2 msec 2 msec 2 msec
2 192.168.203.89 1 msec * 1 msec

ل 2

nat ل تل ع عي طت سي تنأ كل ذ دع ب ج را خ ل ا نم reachable نو كي نأ ي ل خ ا د ل دان ل ف ده ل ا نو كي ن ا forwarding: ء ان يم ل ك شي ب ا دي د ح ت ر ث ك أ ة دع اق



inline_image_0.png

روش نم ل NAT ني وكت:

<#root>

firepower#

show run nat

nat (INSIDE,OUTSIDE) source static server_host interface service SVC_25769850586 SVC_25769850587

<#root>

firepower#

traceroute 192.168.203.89

Type escape sequence to abort.
Tracing the route to 192.168.203.89
1 192.168.201.88 2 msec 2 msec 2 msec
2 192.168.203.89 1 msec * 1 msec

لمعي فيك

لمعي فيك

غنيب

1. (0 زمرلا 8 عونل ICMP) يدص بلط ةلاسرة فيامحل راج لسري
2. ICMP ل ديدج ةيامح راج لاصتا ءاشنإ متي
3. (0 عونل نم ICMP زمر) دادترالا يلع در ةلاسرة فيامحل راج ملتسي
4. 2. ةوطخلل في هؤاشنإ متي ذللا لاصتالا ةلاسرلا قباطت
5. ةيامحل راج ةطساوب ةكلهتسم دادترالا يلع درلا ةلاسر

traceroute

1. ةهجو لا وحن 33436 و 33435 و 33434 ، ذفانم لا نم اءب UDP مزح ثالث ةيامحل راج لسري
1. TTL عم
2. UDP ل ديدج ةيامح راج لاصتا ءاشنإ متي

3. وأ (0 زمرلا 11 عونلا) لقنلا ءانثأ هزواجت مت يذلا ICMP TTL ام ةيماحلا راج لبق تسي (3 زمرلا 3 عونلا) هيلا لوصول رذعتي يذلا ICMP ذفنم

4. UDP مزح نع ةفلتخم تالاصتاك اهتجالعم متي ،ةيماحلا راج ىلا ICMP مزح لوصول درجم 2. ةوطخل نم

كراشيري و ي ف اذه ىرن نأ انعسوبو

No.	Time	Delta	Source	Destination	Protocol	Length	Total Length	Identification	Source Port	Destination Port	Info
1	2026/03 13:08:35.429177	0.000000	192.168.201.200	192.168.203.89	ICMP	118	100	0x4f8d (20365)			Echo (ping) request id=0xf825, seq=39095/47000, ttl=255 (reply in 2)
2	2026/03 13:08:35.429680	0.000503	192.168.203.89	192.168.201.200	ICMP	118	100	0x4f8d (20365)			Echo (ping) reply id=0xf825, seq=39095/47000, ttl=254 (request in 1)
3	2026/03 13:08:35.429989	0.000229	192.168.201.200	192.168.203.89	ICMP	118	100	0x0542 (1346)			Echo (ping) request id=0xf826, seq=39095/47000, ttl=255 (reply in 4)
4	2026/03 13:08:35.430275	0.000366	192.168.203.89	192.168.201.200	ICMP	118	100	0x0542 (1346)			Echo (ping) reply id=0xf826, seq=39095/47000, ttl=254 (request in 3)
5	2026/03 13:08:35.430489	0.000214	192.168.201.200	192.168.203.89	ICMP	118	100	0x0953 (2387)			Echo (ping) request id=0xf827, seq=39095/47000, ttl=255 (reply in 6)
6	2026/03 13:08:35.430840	0.000351	192.168.203.89	192.168.201.200	ICMP	118	100	0x0953 (2387)			Echo (ping) reply id=0xf827, seq=39095/47000, ttl=254 (request in 5)
7	2026/03 13:08:35.431038	0.000198	192.168.201.200	192.168.203.89	ICMP	118	100	0x7290 (29328)			Echo (ping) request id=0xf828, seq=39095/47000, ttl=255 (reply in 8)
8	2026/03 13:08:35.431389	0.000351	192.168.203.89	192.168.201.200	ICMP	118	100	0x7290 (29328)			Echo (ping) reply id=0xf828, seq=39095/47000, ttl=254 (request in 7)
9	2026/03 13:08:35.431587	0.000198	192.168.201.200	192.168.203.89	ICMP	118	100	0x5789 (22409)			Echo (ping) request id=0xf829, seq=39095/47000, ttl=255 (reply in 10)
10	2026/03 13:08:35.431938	0.000351	192.168.203.89	192.168.201.200	ICMP	118	100	0x5789 (22409)			Echo (ping) reply id=0xf829, seq=39095/47000, ttl=254 (request in 9)
11	2026/03 13:08:41.221317	5.789379	192.168.201.200	192.168.203.89	UDP	46	28	0x338e (13198)	49166	33434	49166 → 33434 Len=0
12	2026/03 13:08:41.224002	0.002685	192.168.201.88	192.168.201.200	ICMP	74	56,28	0x00c2 (194),0x...	49166	33434	Time-to-live exceeded (Time to live exceeded in transit) Reply from transit device
13	2026/03 13:08:44.210331	2.986329	192.168.201.200	192.168.203.89	UDP	46	28	0x67af (26543)	49166	33435	49166 → 33435 Len=0
14	2026/03 13:08:44.212711	0.002380	192.168.201.88	192.168.201.200	ICMP	74	56,28	0x00c3 (195),0x...	49166	33435	Time-to-live exceeded (Time to live exceeded in transit) Reply from transit device
15	2026/03 13:08:47.210224	2.997513	192.168.201.200	192.168.203.89	UDP	46	28	0x27bc (10172)	49166	33436	49166 → 33436 Len=0
16	2026/03 13:08:47.212620	0.002396	192.168.201.88	192.168.201.200	ICMP	74	56,28	0x00c4 (196),0x...	49166	33436	Time-to-live exceeded (Time to live exceeded in transit)
17	2026/03 13:08:50.210224	2.997684	192.168.201.200	192.168.203.89	UDP	46	28	0x6345 (25413)	49166	33437	49166 → 33437 Len=0
18	2026/03 13:08:50.210728	0.000504	192.168.203.89	192.168.201.200	ICMP	74	56,28	0x00f5 (95),0x6...	49166	33437	Destination unreachable (Port unreachable)
19	2026/03 13:08:53.210331	2.999603	192.168.201.200	192.168.203.89	UDP	46	28	0x4fcb (20427)	49166	33438	49166 → 33438 Len=0
20	2026/03 13:08:53.210819	0.000488	192.168.203.89	192.168.201.200	ICMP	74	56,28	0x0060 (96),0x4...	49166	33438	Destination unreachable (Port unreachable) Traceroute test
21	2026/03 13:08:56.210224	2.999485	192.168.201.200	192.168.203.89	UDP	46	28	0x03a8 (936)	49166	33439	49166 → 33439 Len=0
22	2026/03 13:08:56.210712	0.000488	192.168.203.89	192.168.201.200	ICMP	74	56,28	0x0061 (97),0x0...	49166	33439	Destination unreachable (Port unreachable)
23	2026/03 13:08:59.210209	2.999497	192.168.201.200	192.168.203.89	UDP	46	28	0x6ec1 (28353)	49166	33440	49166 → 33440 Len=0
24	2026/03 13:08:59.210667	0.000458	192.168.203.89	192.168.201.200	ICMP	74	56,28	0x0062 (98),0x6...	49166	33440	Destination unreachable (Port unreachable) Reply from the destination
25	2026/03 13:09:02.210331	2.999664	192.168.201.200	192.168.203.89	UDP	46	28	0x2666 (9830)	49166	33441	49166 → 33441 Len=0
26	2026/03 13:09:02.225497	0.015166	192.168.203.89	192.168.201.200	ICMP	74	56,28	0x0063 (99),0x2...	49166	33441	Destination unreachable (Port unreachable)
27	2026/03 13:09:05.210224	2.984727	192.168.201.200	192.168.203.89	UDP	46	28	0x1da7 (7591)	49166	33442	49166 → 33442 Len=0
28	2026/03 13:09:05.210728	0.000504	192.168.203.89	192.168.201.200	ICMP	74	56,28	0x0064 (100),0x...	49166	33442	Destination unreachable (Port unreachable)
29	2026/03 13:09:08.210209	2.999481	192.168.201.200	192.168.203.89	UDP	46	28	0x3254 (12884)	49166	33443	49166 → 33443 Len=0
30	2026/03 13:09:08.210712	0.000503	192.168.203.89	192.168.201.200	ICMP	74	56,28	0x0065 (101),0x...	49166	33443	Destination unreachable (Port unreachable)

inline_image_0.png

اهحالص او ءاطخال افاشكتسا

1 ةوطخل

لخدملا جلاعي ةيماحلا راج فيك ىري نأ عبتت عم نراق جرخم قيحلل عنام راج ىلع طبرت نكم طبر:

<#root>

fi repower#

capture CAPI trace interface OUTSIDE match ip host 192.168.203.89 host 192.168.201.100

2 ةوطخال

لصتال را بتخا م ادخت ساب را بتخال:

<#root>

```
firepower#
```

```
ping 192.168.203.89
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.203.89, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ع م رب تخا م ث traceroute:

<#root>

```
firepower#
```

```
traceroute 192.168.203.89
```

```
Type escape sequence to abort.  
Tracing the route to 192.168.203.89  
 1* * *  
 2* * *  
 3* * *  
 4* * *  
 5* * *  
 6* * *  
 7* * *  
 ...
```

3 ةوطخال

طاقت لال تا يوتحم نم ق قحت:

- ICMP لاصت را بتخا را بتخاب 1-10 مزحل لاصت
- لوال ةوطخال نم دودرل traceroute. ب ةط برم 11-16 طبرل

• ةطقن ةياهن ةياغلل نم دودرلا. traceroute اضيا 17-28 طبر ت طبر

<#root>

firepower#

show capture CAPI

```
190 packets captured
1: 13:50:27.345471      802.1Q vlan#201 PO 192.168.201.200 > 192.168.203.89 icmp: echo request
2: 13:50:27.345975      802.1Q vlan#201 PO 192.168.203.89 > 192.168.201.200 icmp: echo reply
3: 13:50:27.346219      802.1Q vlan#201 PO 192.168.201.200 > 192.168.203.89 icmp: echo request
4: 13:50:27.346600      802.1Q vlan#201 PO 192.168.203.89 > 192.168.201.200 icmp: echo reply
5: 13:50:27.346814      802.1Q vlan#201 PO 192.168.201.200 > 192.168.203.89 icmp: echo request
6: 13:50:27.347165      802.1Q vlan#201 PO 192.168.203.89 > 192.168.201.200 icmp: echo reply
7: 13:50:27.347378      802.1Q vlan#201 PO 192.168.201.200 > 192.168.203.89 icmp: echo request
8: 13:50:27.347714      802.1Q vlan#201 PO 192.168.203.89 > 192.168.201.200 icmp: echo reply
9: 13:50:27.347928      802.1Q vlan#201 PO 192.168.201.200 > 192.168.203.89 icmp: echo request
10: 13:50:27.348279     802.1Q vlan#201 PO 192.168.203.89 > 192.168.201.200 icmp: echo reply
11: 13:50:33.229724     802.1Q vlan#201 PO 192.168.201.200.49168 > 192.168.203.89.33434: udp 0
12: 13:50:33.232562     802.1Q vlan#201 PO 192.168.201.88 > 192.168.201.200 icmp: time exceeded in-tr
13: 13:50:36.220279     802.1Q vlan#201 PO 192.168.201.200.49168 > 192.168.203.89.33435: udp 0
14: 13:50:36.222827     802.1Q vlan#201 PO 192.168.201.88 > 192.168.201.200 icmp: time exceeded in-tr
15: 13:50:39.220172     802.1Q vlan#201 PO 192.168.201.200.49168 > 192.168.203.89.33436: udp 0
16: 13:50:39.222675     802.1Q vlan#201 PO 192.168.201.88 > 192.168.201.200 icmp: time exceeded in-tr
17: 13:50:42.220157     802.1Q vlan#201 PO 192.168.201.200.49168 > 192.168.203.89.33437: udp 0
18: 13:50:42.220737     802.1Q vlan#201 PO 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
19: 13:50:45.220264     802.1Q vlan#201 PO 192.168.201.200.49168 > 192.168.203.89.33438: udp 0
20: 13:50:45.220752     802.1Q vlan#201 PO 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
21: 13:50:48.220157     802.1Q vlan#201 PO 192.168.201.200.49168 > 192.168.203.89.33439: udp 0
22: 13:50:48.220645     802.1Q vlan#201 PO 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
23: 13:50:51.220157     802.1Q vlan#201 PO 192.168.201.200.49168 > 192.168.203.89.33440: udp 0
24: 13:50:51.220645     802.1Q vlan#201 PO 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
25: 13:50:54.220264     802.1Q vlan#201 PO 192.168.201.200.49168 > 192.168.203.89.33441: udp 0
26: 13:50:54.220752     802.1Q vlan#201 PO 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
27: 13:50:57.220157     802.1Q vlan#201 PO 192.168.201.200.49168 > 192.168.203.89.33442: udp 0
28: 13:50:57.220645     802.1Q vlan#201 PO 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
```

4 ةوطخلال

للاصتال رابتخل نم لخدملاب ةصاخال ICMP مزح عبتت ب مق

#1 ةمزحلالي ف لسرملال ICMP للاصتال رابتخل بلط يلعل درلا يه #2 ةمزحلالي

<#root>

firepower#

show capture CAPI packet-number 2 trace

```

2: 13:50:27.345975      802.1Q vlan#201 PO 192.168.203.89 > 192.168.201.200 icmp: echo reply
                                                                    ...
                                                                    Phase: 4
                                                                    Type: FLOW-LOOKUP
                                                                    Subtype:
                                                                    Result: ALLOW
                                                                    Elapsed time: 488 ns
                                                                    Config:
                                                                    Additional Information:
                                                                    Found flow with id 143799, using existing flow
                                                                    ...
                                                                    Phase: 6
                                                                    Type: ADJACENCY-LOOKUP
                                                                    Subtype: Resolve Nexthop IP address to MAC
                                                                    Result: ALLOW
                                                                    Elapsed time: 1952 ns
                                                                    Config:
                                                                    Additional Information:
                                                                    Found adjacency entry for Next-hop 0.0.0.0 on interface identity
                                                                    Adjacency :Active
                                                                    MAC address 0000.0000.0000 hits 483359 reference 2
                                                                    Result:
                                                                    input-interface: OUTSIDE(vrfid:0)
                                                                    input-status: up
                                                                    input-line-status: up
                                                                    output-interface: NP Identity Ifc
                                                                    Action: allow
                                                                    Time Taken: 18056 ns
                                                                    1 packet shown

```

• یہ عبتت لل ةيسئرلا طاقنلا

• دوجوم قفدت ةمزحل تقباط

• (ةيوهلا ةهجاو) هسفن ةيامحل رادج يه جارخال ةهجاو

5 ةوطخال

tracertool رابتخا نم لخدملاب ةصاخلا ICMP مزح عبتت بمق

لقنلا فيضم نم درلا يه #12 ةمزحل

<#root>

firepower#

show capture CAPI packet-number 12 trace

```

12: 13:50:33.232562      802.1Q vlan#201 P0 192.168.201.88 > 192.168.201.200 icmp: time exceeded in-tr
190 packets captured
Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 6344 ns
Config:
nat (INSIDE,OUTSIDE) source static server_host interface
Additional Information:
NAT divert to egress interface INSIDE(vrfid:0)
Untranslate 192.168.201.200/49168 to 192.168.200.50/49168
Phase: 7
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 97 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268436480
access-list CSM_FW_ACL_ remark rule-id 268436480: ACCESS POLICY: mzafeiro_empty - Default
access-list CSM_FW_ACL_ remark rule-id 268436480: L4 RULE: DEFAULT ACTION RULE
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 18
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 16104 ns
Config:
Additional Information:
New flow created with id 143805, packet dispatched to next module
...
Phase: 20
Type: SNORT
Subtype: identity
Result: ALLOW
Elapsed time: 39496 ns
Config:
Additional Information:
user id: no auth, realm id: 0, device type: 0, auth type: invalid, auth proto: basic, username: none, A
src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, abp src: none, abp dst: none, loc
Result:
input-interface: OUTSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: INSIDE(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 158341 ns

```

- (دوجوم قفدت عم قباطت مل) ديدج لى صوت نم عزج ةمزلال
- (NAT ةياغ ينعي UN-NAT، ديدحتلال هجولىع) ةكبشلال ناوع ةمچرتل ةمزلال عرضت

- يف مكحتللا جهنل عضختو ةياملال رادجل روبع رورم ةكرحك ةمزلال عم لماعتللا متي اياطشللا صحتو (ACP) لوصوللا
- ةمحررت nat لىللا عجرى اذه .يلخاد نراق (جرخم) جاتنللا

ببسلا

ةدعاق nat كيتاتسلا نكاس اذه اببس ةلكشملا ،ةلالا هذه يف

<#root>

```
firepower#
```

```
show run nat
```

```
nat (INSIDE,OUTSIDE) source static server_host interface
```

ةلصللا يذى وتحمللا

- [\(FTD\) ةيرانللا ةقاطلا ديدهت دض عافدللا لالخ نم Traceroute ب حامسلا](#)
- [Cisco نم تاليزنتلا او ينفلا معدلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال 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 ال ا ة مچرت 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 مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
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 دن ت س م ل ا