

FTD ىل ع هتحص نم ققحتل او NAT نيوكت

تايوت حمل

[قمدقم](#)

[قيساس ال تابلطت](#)

[تابلطت](#)

[قمدختس مل تانوك مل](#)

[قيساس ا تامول عم](#)

[نيوكت](#)

[قكبش ليل يطيطختل مسر](#)

[FTD ىل ع تابلطت NAT نيوكت 1. قمه مل](#)

[FTD ىل ع \(PAT\) ذفن مل ناو ن ع قمرت نيوكت 2. قمه مل](#)

[FTD ىل ع NAT ا ن ث س ل نيوكت 3. قمه مل](#)

[FTD ىل ع NAT ن ئ ك ل نيوكت 4. قمه مل](#)

[FTD ىل ع PAT ع مر ت نيوكت 5. قمه مل](#)

[قحص ل نم ققحتل](#)

[اهج الص او ع اط خ ال فاش كتس](#)

[قحص ت اذ تامول عم](#)

قمدقم

FirePOWER ىل ع (NAT) قمرت ناو ن ع قكبش قيساس ا تقق دو ل كشي ن ا فيك ققي ث و اذه فص ي (FTD) ع ا ف د ل ا دي ده ت

قيساس ال تابلطت مل

تابلطت مل

دن تس مل اذه ل ق ص ا خ تابلطت م د ج و ت ال

قمدختس مل تانوك مل

قيل ال ق يد ام ال تانوك مل او ج م ا ر ب ل ا ت ا ر ا د ص ل ا د ن تس مل اذه في ق دراول ا تامول عم ل ا دن تس ت

- ASA5506X ل غ ش ي ي ذ ل ا 6.1.0-226 ز م ر FTD
- FireSIGHT Management Center (FMC) ل غ ش ي ي ذ ل ا 6.1.0-226 ر ا د ص ل ا ل ا ل غ ش ي ي ذ ل ا
- Windows 7 ل غ ش ت ل ا م ا ط ن ل ا ق في ض م ق ز ه ج ا 3
- LAN (L2L) VPN قكبش ل ا ل ا ل غ ش ي ي ذ ل ا Cisco IOS® 3925 ه ج و م ل ا

ق د ح ا و ق ع ا س : ل م ع م ل ا ل ا م ك ا ت ق و

ق ص ا خ ق ي ل م ع م ق ئ ي ب في ق د و ج و م ل ا ق ز ه ج ا ل ا ن م دن تس مل اذه في ق دراول ا تامول عم ل ا ع ا ش ن ا م ت

تتأكد إذا (يضايرتفا) حوسمم نيوكتب دننسسما اذف ةمدختسُما ةزهألا عيمج تأدب رما ألالمحملا ريثألال كمهف نم دكأتف ،ليغشلال ديقتككبش

ةيساسأ تامولعم

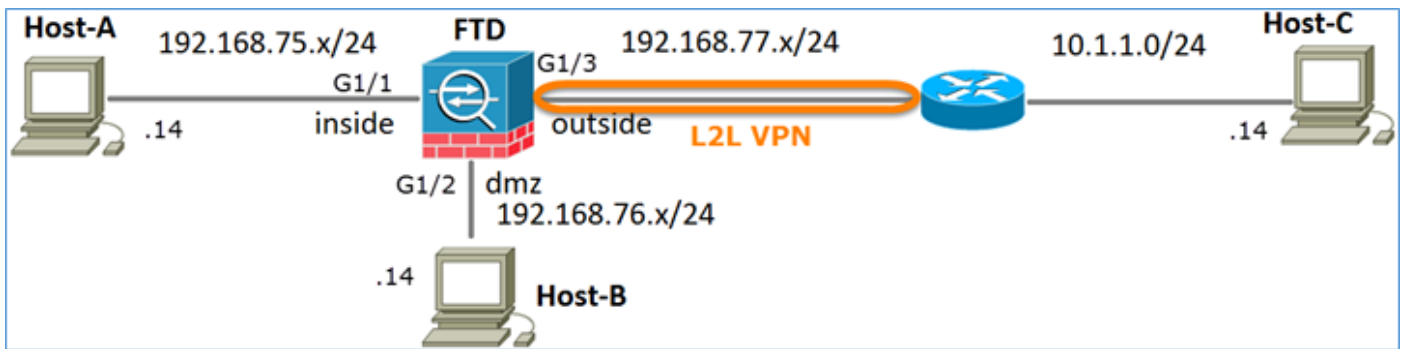
يديلقلال (ASA) فيكتلل لباقلال نامألا زاهج لثم NAT نيوكت تارايف سفن FTD معدف

- يديلقلال ASA لىل (1 مسقلا) NAT نيترم لداعي اذف - لبق نم NAT دعاق
- يديلقلال ASA في 2 مسقلا - ةيئاقللل NAT دعاق
- يديلقلال ASA لىل (3 مسقلا) NAT نيترم لداعي اذف - NAT دعاق دعب

نوكت نأ يرورضلا نمف ، NAT نيوكتب رمالا قلع تي ام دنع FMC ل نم م تي FTD نيوكت نأ ام ن. نيوكتلا تارايف فللخم و FMC ل (GUI) ةيموسرلا مدختسُما ةهجاوب ةيارد لىل

نيوكتلا

ةكبشلل يطيختلا مسرلا



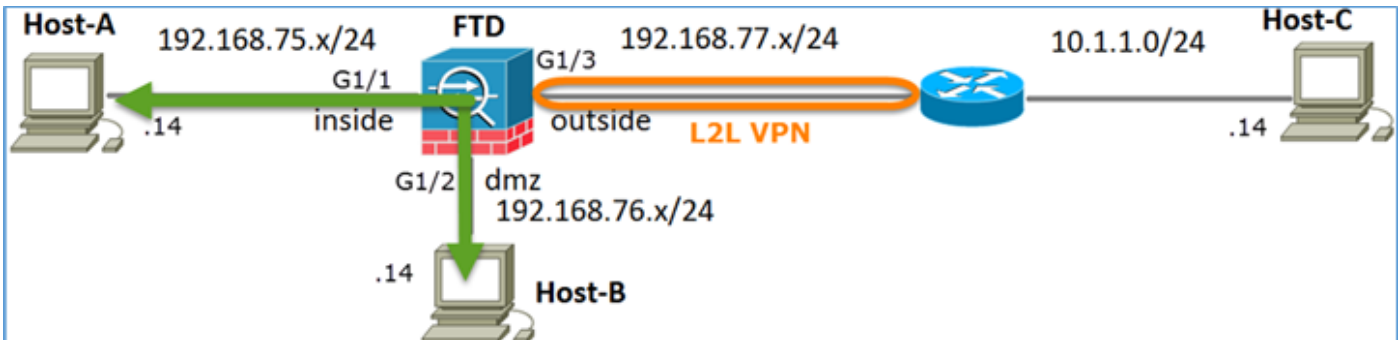
FTD لىل تباثلا NAT نيوكت 1. ةمهمل

تابللتملا هذلل اقبط NAT نيوكت

NAT جهن مسأ	FTD زاهج مسأ
nat دعاق	ةيوديلل NAT دعاق
NAT عون	تباث
چاردا	1 مسقلا في
ردصملا ةهجاو	*لخاد

قوة جولة	DMZ*
يصل الة ردصم	192.168.75.14
مجرتم ردصم	192.168.76.100

*NAT دة اقل نام الة قطانم م ادختسا



تباث الة NAT

لحل:

كمزلي في FTD، في NAT دة اوق في م سا م ادختسا ك ل ع ب ج ي، ي د ل ق ت الة ASA ل ع امن ي بة. قة ج اول تاع وجم و ا نام الة قطانم م ادختسا

ة ج اول تاع وجم/نام الة قطانم ل تاع ج اول ص ي ص خ ت ب م ق 1 ق و ط خ ل

ال د ب. نام الة قطانم ل الة NAT ل اهم ادختسا م ت ي ي ت الة FTD تاع ج اول ن ي ي ع ت ر ر ق ت، قة م ه م الة ه ذ ه في ق ر و ص ل الة في ح ص و م و ه ام ك قة ج اول تاع وجم ل الة م ه ن ي ي ع ت ك ن ك م ي، ك ل ذ ن م

Edit Physical Interface

Mode:

Name: Enabled Management Only

Security Zone:

Description:

General IPv4 IPv6 Advanced Hardware Configuration

MTU: (64 - 9198)

Interface ID:

ةروصلال ي ف حضوم وه امك ةجيتنللا 2. ةوطخللا

Interface	Logical Name	Type	Interface Objects	Mac Address(Active/Standby)	IP Address
GigabitEthernet1/1	inside	Physical	inside_zone		192.168.75.6/24(Static)
GigabitEthernet1/2	dmz	Physical	dmz_zone		192.168.76.6/24(Static)
GigabitEthernet1/3	outside	Physical	outside_zone		192.168.77.6/24(Static)

ةرادا > تانئالكلا ةحفص نم ناما قطانمو ةهجاو تاعومجم ريح/عاشن انك نمكي 3. ةوطخللا ةروصلال ي ف حضوم وه امك تانئالكلا

Name	Type	Interface Type
dmz_zone	Security Zone	
inside_zone	Security Zone	Routed
outside_zone	Security Zone	Routed

ةهجاوالا تاعومجم لباقم نامالا قطانم

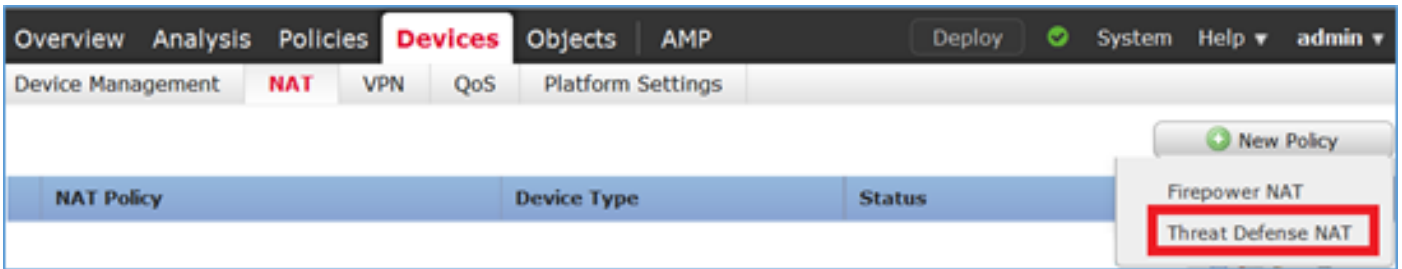
ةهجاوالا عامتنا ةينانكم ي ف ةهجاوالا تاعومجمو نامالا قطانم نيب يسيرلا فالخال نمكي نم كللذل. ةددعتم ةهجاو تاعومجم ىلا يم تنت نأ نمكي نكلو، طقف ةدحاو ناما قطنم ىلا رثكأ ةنورم ةهجاوالا تاعومجم رفوت، ةيلمعلا ةيخانلا

ةقطنم نكلو، نيتفلتخم ةهجاو يتاعومجم ىلا يم تنت ةيلخاللا ةهجاوالا نأ ىرت نأ نمكي ةروصلال ي ف حضوم وه امك طقف ةدحاو ناما

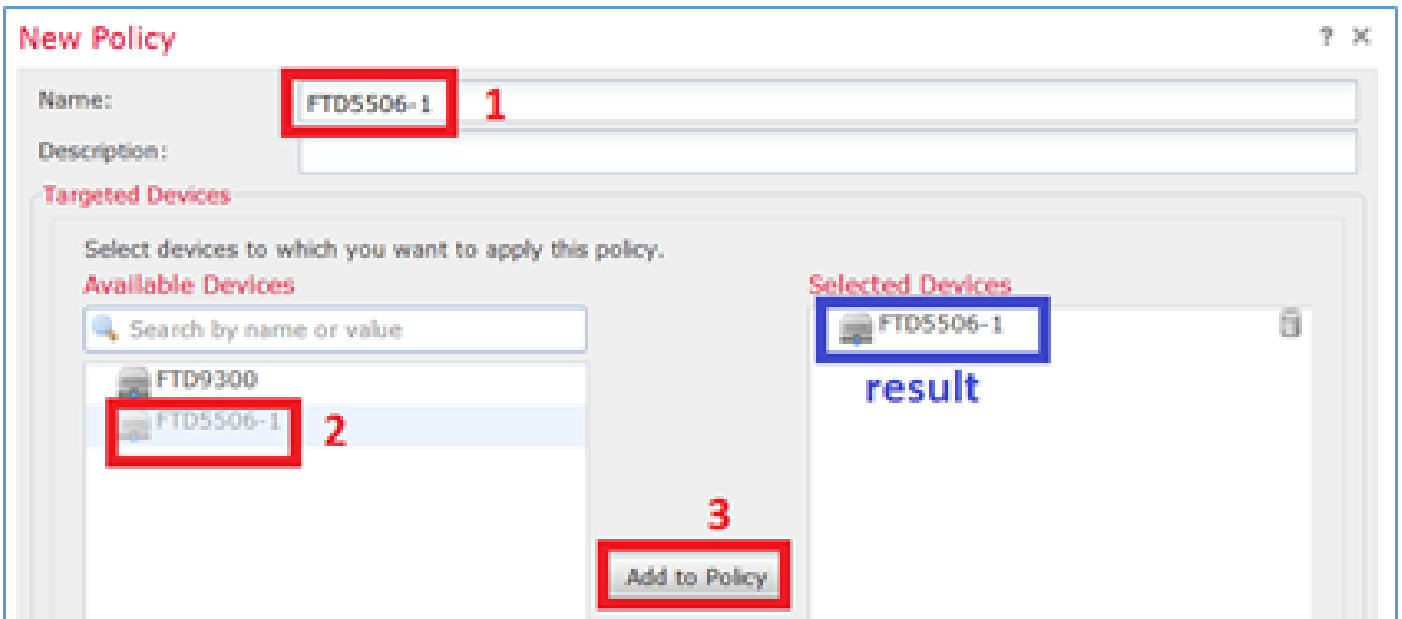
Name	Type	Interface Type
Group1	Interface Group	Routed
FTD5506-1 inside		
Group2	Interface Group	Routed
FTD5506-1 inside		
dmz_zone	Security Zone	Routed
FTD5506-1 dmz		
inside_zone	Security Zone	Routed
FTD5506-1 inside		
outside_zone	Security Zone	Routed
FTD5506-1 outside		

FTD. ىلع يكي تاتاسا نكاس NAT تلكش 4. ةوطخل

ديدهتلا نع عافدلل NAT > ةديج ةسايس دح. nat ةسايس ئشنأو NAT > ةزهألا ىلا لقتنا ةروصلال ي ف حضم وه امك

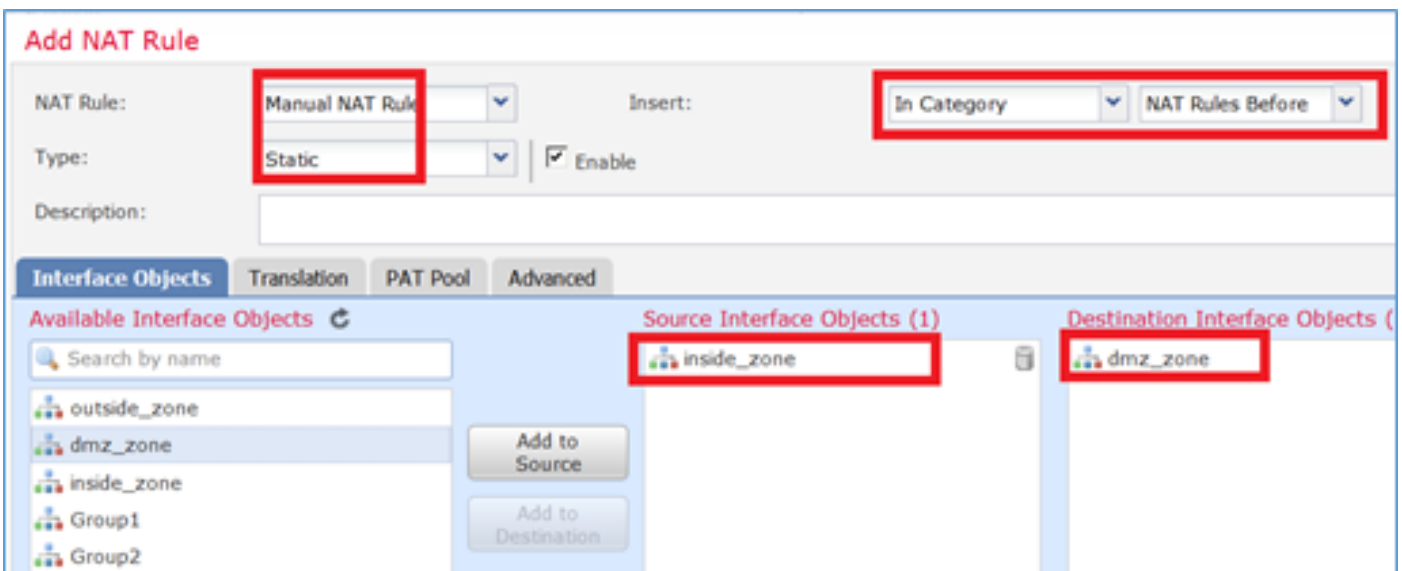


ةروصلال ي ف حضم وه امك فدهتسم زاهج ىلع هنييغتب مقوجهنلا مسادح 5. ةوطخل



ةدعاق ةفاضل قوف رقنا، جهنلا ىلا nat ةدعاق ةفاضل 6. ةوطخل

روصلال ي ف حضم وه امك ةمهمل تابلطتم بسح كلذ دح



Add NAT Rule

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source: * Host-A

Original Destination: Address

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source: Address

Translated Destination: Host-B

Translated Source Port:

Translated Destination Port:

Host-A = 192.168.75.14

host-b = 192.168.76.100

<#root>

firepower#

show run object

```
object network Host-A
 host 192.168.75.14
object network Host-B
 host 192.168.76.100
```

⚠ كل ذ دع ب ، ردصم مجرتي نأ امب نراق ني عوي و nat كي تاتاس نكاس تنأ لك شي نإ : ري ذحت ني مدختسم لا يلع رذعتي . تدعأ نو كي نراق لا نم ناو نعالا لى ل دع م رورم ة ك رح لك تام دخال هذه ة لثمأ نم ضتتو . ة ني عمل ة هجاولا لى ل ة نكمم ة مدخ ة ي لى ل و صولا و OSPF و EIGRP لثم هيجوتل تالوكوتورب .

ة روصلا يف حضوم وه امك ة جيتنلا . 7 ة و طخال

Rules Policy Assignments (1)

Filter by Device Add Rule

#	Dire...	Typ	Original Packet		Translated Packet		Options
			Source Interface Obj...	Destination Interface Ob...	Original Sources	Original Destinatio...	
NAT Rules Before							
1		Static	inside_zone	dmz_zone	Host-A	Host-B	Dns:false
Auto NAT Rules							
NAT Rules After							

ىل لوصول اب B-ف يضم ل حملت لوصولا ي ف م كحت ة سايس دوجو نم دكأت 8. ة وطلال وه امك .ايضارت فا ه اجت ا جودزم nat ي كيتات سا نك اس نأ ت ركذت .حيحص س ك عل او A-ف يضم ل ربت خم ل اذه ي ف LINA نأل عقوتم اذه .ي قيقح ل IPs مادخت سا عجار ،ي ديلقت ل ASA عم ل ا ل ة .وصولا ي ف حضورم وه امك زم ر 9.6.1.x ل غشت

#	Name	S... Z...	D... Z...	Source Networks	Dest Networks	V...	U...	A...	S...	D...	U...	L... A...	Action						
Mandatory - FTD5506-1 (1-2)																			
1	Host-A to Ho:	any	any	192.168.75.14	192.168.76.14	any	any	any	any	any	any	any	Allow						
2	Host-B to Ho:	any	any	192.168.76.14	192.168.75.14	any	any	any	any	any	any	any	Allow						
Default - FTD5506-1 (-)																			
There are no rules in this section. Add Rule or Add Category																			
Default Action													Access Control: Block All Traffic						

ققحت ل:

انيل CLI نم:

```
<#root>
```

```
firepower#
```

```
show run nat
```

```
nat (inside,dmz) source static Host-A Host-B
```

عقوتم وه امك 1 مسقل ي ف NAT ة د عاق جاردا مت:

```
<#root>
```

```
firepower#
```

```
show nat
```

```
Manual NAT Policies
```

```
(Section 1)
```

```
1 (inside) to (dmz) source static Host-A Host-B
```

```
translate_hits = 0, untranslate_hits = 0
```

 ة ف ل ل خ ل ا ي ف ا ه و ا ش ن ا مت ي يت ل ل 2 ل ل ا ل ح ا ر م ل ا : ة ظ ح ا ل م .

```
<#root>
```

```
firepower#
```

show xlate

2 in use, 4 most used

Flags: D - DNS, e - extended,

I - identity

, i - dynamic, r - portmap,

s - static, T - twice

, N - net-to-net

NAT from inside:192.168.75.14 to dmz:192.168.76.100

flags sT idle 0:41:49 timeout 0:00:00

NAT from dmz:0.0.0.0/0 to inside:0.0.0.0/0

flags sIT idle 0:41:49 timeout 0:00:00

جواب ASP NAT:

<#root>

firepower#

show asp table classify domain nat

Input Table

in id=

0x7ff6036a9f50

, priority=6, domain=nat, deny=false

hits=0, user_data=0x7ff60314dbf0, cs_id=0x0, flags=0x0, protocol=0

src ip/id=192.168.75.14

, mask=255.255.255.255, port=0, tag=any

dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0

input_ifc=inside, output_ifc=dmz

in id=

0x7ff603696860

, priority=6, domain=nat, deny=false

hits=0, user_data=0x7ff602be3f80, cs_id=0x0, flags=0x0, protocol=0

src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any

dst ip/id=192.168.76.100

, mask=255.255.255.255, port=0, tag=any, dscp=0x0

input_ifc=dmz, output_ifc=inside

Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never

<#root>

firepower#

show asp table classify domain nat-reverse

Input Table

Output Table:

out id=

0x7ff603685350

, priority=6, domain=nat-reverse, deny=false
hits=0, user_data=0x7ff60314dbf0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any

dst ip/id=192.168.75.14

, mask=255.255.255.255, port=0, tag=any, dscp=0x0
input_ifc=dmz, output_ifc=inside

out id=

0x7ff603638470

, priority=6, domain=nat-reverse, deny=false
hits=0, user_data=0x7ff602be3f80, cs_id=0x0, use_real_addr, flags=0x0, protocol=0

src ip/id=192.168.75.14

, mask=255.255.255.255, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside, output_ifc=dmz

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never

نم لاصتال رابتخاو FTD ىل عبتتال لى صافات مادختساب طاقتلال نى كم تب مق
ةروصلال ىف حضورم وه امك A-ففىضمال ىل B-ففىضمال

<#root>

firepower#

capture DMZ interface dmz trace detail match ip host 192.168.76.14 host 192.168.76.100

firepower#

capture INSIDE interface inside trace detail match ip host 192.168.76.14 host 192.168.75.14

```

C:\Users\cisco>ping 192.168.76.100

Pinging 192.168.76.100 with 32 bytes of data:
Reply from 192.168.76.100: bytes=32 time=3ms TTL=128
Reply from 192.168.76.100: bytes=32 time=1ms TTL=128
Reply from 192.168.76.100: bytes=32 time=1ms TTL=128
Reply from 192.168.76.100: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.76.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\Users\cisco>_

```

ASP: لودج ي ف دوجوم لوصولا تارم ددع

```
<#root>
```

```
firepower#
```

```
show asp table classify domain nat
```

```
Input Table
```

```
in id=0x7ff6036a9f50, priority=6, domain=nat, deny=false
    hits=0, user_data=0x7ff60314dbf0, cs_id=0x0, flags=0x0, protocol=0
    src ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
    input_ifc=inside, output_ifc=dmz
```

```
in id=
```

```
0x7ff603696860
```

```
, priority=6, domain=nat, deny=false
```

```
hits=4
```

```
, user_data=0x7ff602be3f80, cs_id=0x0, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
    dst ip/id=192.168.76.100, mask=255.255.255.255, port=0, tag=any, dscp=0x0
    input_ifc=dmz, output_ifc=inside
```

```
<#root>
```

```
firepower#
```

```
show asp table classify domain nat-reverse
```

```
Input Table
```

```
Output Table:
```

```
out id=
```

```
0x7ff603685350
```

```
, priority=6, domain=nat-reverse, deny=false
```

```
hits=4
```

```
, user_data=0x7ff60314dbf0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
```

```
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
```

```
dst ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any, dscp=0x0
```

```
input_ifc=dmz, output_ifc=inside
```

```
out id=0x7ff603638470, priority=6, domain=nat-reverse, deny=false
```

```
hits=0, user_data=0x7ff602be3f80, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
```

```
src ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any
```

```
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
```

```
input_ifc=inside, output_ifc=dmz
```

ةمزلحلا طاقنللا رهظي:

```
<#root>
```

```
firepower#
```

```
show capture DMZ
```

```
8 packets captured
```

```
1: 17:38:26.324812      192.168.76.14 > 192.168.76.100: icmp: echo request
2: 17:38:26.326505      192.168.76.100 > 192.168.76.14: icmp: echo reply
3: 17:38:27.317991      192.168.76.14 > 192.168.76.100: icmp: echo request
4: 17:38:27.319456      192.168.76.100 > 192.168.76.14: icmp: echo reply
5: 17:38:28.316344      192.168.76.14 > 192.168.76.100: icmp: echo request
6: 17:38:28.317824      192.168.76.100 > 192.168.76.14: icmp: echo reply
7: 17:38:29.330518      192.168.76.14 > 192.168.76.100: icmp: echo request
8: 17:38:29.331983      192.168.76.100 > 192.168.76.14: icmp: echo reply
```

```
8 packets shown
```

آ(اهزاربإ متي ةمهمللا طاقنللا) ةمزلحلا راثآ.



ASP لودجب اهطابتراو NAT ةدعاق فرعم: ةظحالم

```
<#root>
```

```
firepower#
```

```
show capture DMZ packet-number 3 trace detail
```

```
8 packets captured
```

```
3: 17:38:27.317991 000c.2998.3fec d8b1.90b7.32e0 0x0800 Length: 74
   192.168.76.14 > 192.168.76.100: icmp: echo request (ttl 128, id 9975)
```

```
Phase: 1
```

```
Type: CAPTURE
```

```
Subtype:
```

```
Result: ALLOW
```

Config:

Additional Information:

Forward Flow based lookup yields rule:

```
in id=0x7ff602c72be0, priority=13, domain=capture, deny=false
  hits=55, user_data=0x7ff602b74a50, cs_id=0x0, l3_type=0x0
  src mac=0000.0000.0000, mask=0000.0000.0000
  dst mac=0000.0000.0000, mask=0000.0000.0000
  input_ifc=dmz, output_ifc=any
```

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

Forward Flow based lookup yields rule:

```
in id=0x7ff603612200, priority=1, domain=permit, deny=false
  hits=1, user_data=0x0, cs_id=0x0, l3_type=0x8
  src mac=0000.0000.0000, mask=0000.0000.0000
  dst mac=0000.0000.0000, mask=0100.0000.0000
  input_ifc=dmz, output_ifc=any
```

Phase: 3

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

```
nat (inside,dmz) source static Host-A Host-B
```

Additional Information:

```
NAT divert to egress interface inside
Untranslate 192.168.76.100/0 to 192.168.75.14/0
```

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.76.14 host 192.168.75.14 rule-id 268434440
access-list CSM_FW_ACL_ remark rule-id 268434440: ACCESS POLICY: FTD5506-1 - Mandatory/2
access-list CSM_FW_ACL_ remark rule-id 268434440: L4 RULE: Host-B to Host-A
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Forward Flow based lookup yields rule:

```
in id=0x7ff602b72610, priority=12, domain=permit, deny=false
  hits=1, user_data=0x7ff5fa9d0180, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
  src ip/id=192.168.76.14, mask=255.255.255.255, port=0, tag=any, ifc=any
```

```
dst ip/id=192.168.75.14
```

```
, mask=255.255.255.255, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
  input_ifc=any, output_ifc=any
```

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

```
class-map class-default
```

```
match any
policy-map global_policy
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
```

Additional Information:

Forward Flow based lookup yields rule:

```
in id=0x7ff60367cf80, priority=7, domain=conn-set, deny=false
hits=1, user_data=0x7ff603677080, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=dmz, output_ifc=any
```

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

```
nat (inside,dmz) source static Host-A Host-B
```

Additional Information:

Static translate 192.168.76.14/1 to 192.168.76.14/1

Forward Flow based lookup yields rule:

```
in
```

```
id=0x7ff603696860
```

```
, priority=6, domain=nat, deny=false
```

```
hits=1
```

```
, user_data=0x7ff602be3f80, cs_id=0x0, flags=0x0, protocol=0
```

```
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
```

```
dst ip/id=192.168.76.100, mask=255.255.255.255, port=0, tag=any, dscp=0x0
```

```
input_ifc=dmz, output_ifc=inside
```

Phase: 7

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

```
in id=0x7ff602220020, priority=0, domain=nat-per-session, deny=true
```

```
hits=2, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
```

```
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
```

```
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
```

```
input_ifc=any, output_ifc=any
```

Phase: 8

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

```
in id=0x7ff6035c0af0, priority=0, domain=inspect-ip-options, deny=true
```

```
hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
```

```
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
```

```
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
```

```
input_ifc=dmz, output_ifc=any
```

Phase: 9

Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
 inspect icmp
service-policy global_policy global
Additional Information:
Forward Flow based lookup yields rule:
 in id=0x7ff602b5f020, priority=70, domain=inspect-icmp, deny=false
 hits=2, user_data=0x7ff602be7460, cs_id=0x0, use_real_addr, flags=0x0, protocol=1
 src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0, tag=any
 dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, tag=any, dscp=0x0
 input_ifc=dmz, output_ifc=any

Phase: 10
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
 in id=0x7ff602b3a6d0, priority=70, domain=inspect-icmp-error, deny=false
 hits=2, user_data=0x7ff603672ec0, cs_id=0x0, use_real_addr, flags=0x0, protocol=1
 src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0, tag=any
 dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, tag=any, dscp=0x0
 input_ifc=dmz, output_ifc=any

Phase: 11
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,dmz) source static Host-A Host-B
Additional Information:
Forward Flow based lookup yields rule:
 out

id=0x7ff603685350

, priority=6, domain=nat-reverse, deny=false

hits=2

, user_data=0x7ff60314dbf0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
 dst ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any, dscp=0x0
 input_ifc=dmz, output_ifc=inside

Phase: 12
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
 in id=0x7ff602220020, priority=0, domain=nat-per-session, deny=true
 hits=4, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0
 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any

dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 13

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Reverse Flow based lookup yields rule:

in id=0x7ff602c56d10, priority=0, domain=inspect-ip-options, deny=true
hits=2, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside, output_ifc=any

Phase: 14

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 5084, packet dispatched to next module

Module information for forward flow ...

snp_fp_inspect_ip_options

snp_fp_snort

snp_fp_inspect_icmp

snp_fp_translate

snp_fp_adjacency

snp_fp_fragment

snp_ifc_stat

Module information for reverse flow ...

snp_fp_inspect_ip_options

snp_fp_translate

snp_fp_inspect_icmp

snp_fp_snort

snp_fp_adjacency

snp_fp_fragment

snp_ifc_stat

Phase: 15

Type: EXTERNAL-INSPECT

Subtype:

Result: ALLOW

Config:

Additional Information:

Application: 'SNORT Inspect'

Phase: 16

Type: SNORT

Subtype:

Result: ALLOW

Config:

Additional Information:

Snort Verdict: (pass-packet) allow this packet

Phase: 17

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 192.168.75.14 using egress ifc inside

Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address 000c.2930.2b78 hits 140694538708414

Phase: 19
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
out id=0x7ff6036a94e0, priority=13, domain=capture, deny=false
hits=14, user_data=0x7ff6024aff90, cs_id=0x0, l3_type=0x0
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0000.0000.0000
input_ifc=inside, output_ifc=any

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
1 packet shown

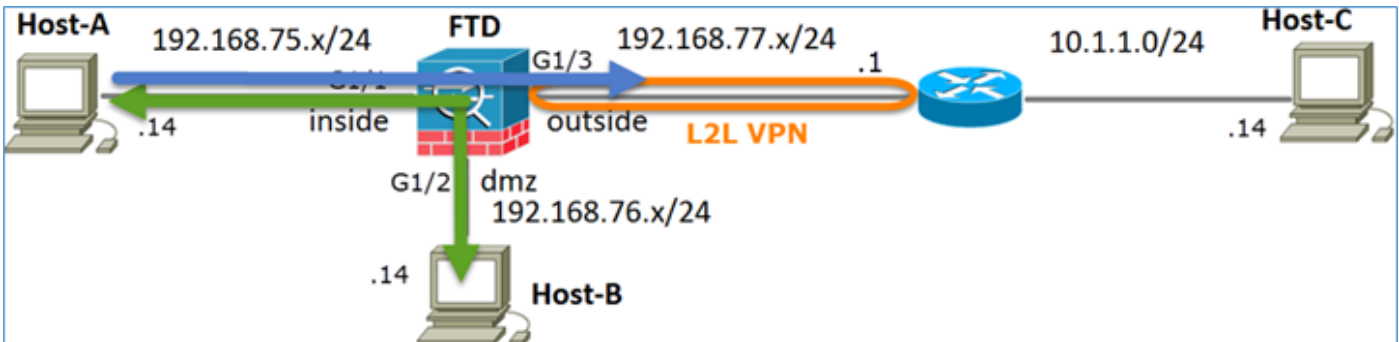
FTD ىل ع (PAT) ذفنم ل ناو ن ع ةم جرت ن ن وكت 2. ةم هم ل

ت: ابل طتم ل هذهل اق ب ط NAT ن وكت

nat ةد اع اق	ة و د ي ل ل NAT ةد اع اق
NAT ع ون	ي م ا ن ي د
ا ر د ا	1 م س ق ل ا ي ف
ر د ص م ل ا ة ه ج ا و	* ل خ ا د

ةهءولا ةهءاوء	ءءاء*
للسألل رءصم الل	192.168.75.0/24
مءءرءم رءصم	ءهءءراءلل ةهءاولل (PAT)

*NAT ةءءاقل نامألل قءانم مءءءس



ءءاءلل NAT

ءاب

لءلل:

وه امك ةمهملل ءابلءممل اءفونل ءلءل اب مءو ةهءءاءل NAT ةءءاقل ءفءاب مء 1 ةوءءلل ءرءوعلل ءفءووم.

ءرءوعلل ءفءووم وه امك ءرء ءلءءش ءلء انه 2 ةوءءلل.

Add NAT Rule ?

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet

Original Source: * +

Original Destination: +

Original Source Port: +

Original Destination Port: +

Translated Packet

Translated Source: +
The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Translated Destination: +

Translated Source Port: +

Translated Destination Port: +

ةروصلال في حضورم وه امك ةچيتنلنل نوكتو 3 ةوطخلل.

Rules

#	Direction	T...	Original Packet			Translated Packet			Options
			Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	
NAT Rules Before									
1	St...		inside_zone	dmz_zone	Host-A		Host-B		Dns:false
2	D...		inside_zone	outside_zone	Net_192.168.75.0_24bits		Interface		Dns:false
Auto NAT Rules									
NAT Rules After									

حامس لل لوصولال في مكحتلال جهن نيوكتب مق ،ربتخملال اذه يقابل ةبس نلاب 4 ةوطخلل رورملاب رورملال ةكرح عيمجل

ققحتلال:

nat ليكشت

<#root>

firepower#

show nat

Manual NAT Policies (Section 1)

1 (inside) to (dmz) source static Host-A Host-B
 translate_hits = 26, untranslate_hits = 26

2 (inside) to (outside) source dynamic Net_192.168.75.0_24bits interface
 translate_hits = 0, untranslate_hits = 0

ديدللا لاخدلال ظحال LINA ب ةصاخلال (CLI) رماوألل رطس ةهچاو نم

<#root>

```
firepower#  
show xlate  
3 in use, 19 most used  
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,  
       s - static, T - twice, N - net-to-net  
NAT from inside:192.168.75.14 to dmz:192.168.76.100  
   flags sT idle 1:15:14 timeout 0:00:00  
NAT from dmz:0.0.0.0/0 to inside:0.0.0.0/0  
   flags sIT idle 1:15:14 timeout 0:00:00  
NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0  
   flags sIT idle 0:04:02 timeout 0:00:00
```

نېكمت ښه ځانگړتيا لري. ښه ځانگړتيا لري او ښه ځانگړتيا لري. ښه ځانگړتيا لري او ښه ځانگړتيا لري. ښه ځانگړتيا لري او ښه ځانگړتيا لري.
ښه ځانگړتيا لري او ښه ځانگړتيا لري.

```
<#root>
```

```
firepower#  
capture CAPI trace interface inside match ip host 192.168.75.14 host 192.168.77.1  
firepower#  
capture CAPO interface outside match ip any host 192.168.77.1
```

ښه ځانگړتيا لري او ښه ځانگړتيا لري. ښه ځانگړتيا لري او ښه ځانگړتيا لري. ښه ځانگړتيا لري او ښه ځانگړتيا لري.
ښه ځانگړتيا لري او ښه ځانگړتيا لري.

```
C:\Windows\system32>ping 192.168.77.1  
Pinging 192.168.77.1 with 32 bytes of data:  
Reply from 192.168.77.1: bytes=32 time=1ms TTL=255  
Reply from 192.168.77.1: bytes=32 time=1ms TTL=255  
Reply from 192.168.77.1: bytes=32 time=1ms TTL=255  
Reply from 192.168.77.1: bytes=32 time=1ms TTL=255  
Ping statistics for 192.168.77.1:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
    Approximate round trip times in milli-seconds:  
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

ښه ځانگړتيا لري او ښه ځانگړتيا لري. ښه ځانگړتيا لري او ښه ځانگړتيا لري. ښه ځانگړتيا لري او ښه ځانگړتيا لري.
ښه ځانگړتيا لري او ښه ځانگړتيا لري.

```
<#root>
```

```
firepower#  
show cap CAPI  
8 packets captured
```

1: 18:54:43.658001

192.168.75.14 > 192.168.77.1

: icmp: echo request

2: 18:54:43.659099	192.168.77.1 > 192.168.75.14: icmp: echo reply
3: 18:54:44.668544	192.168.75.14 > 192.168.77.1: icmp: echo request
4: 18:54:44.669505	192.168.77.1 > 192.168.75.14: icmp: echo reply
5: 18:54:45.682368	192.168.75.14 > 192.168.77.1: icmp: echo request
6: 18:54:45.683421	192.168.77.1 > 192.168.75.14: icmp: echo reply
7: 18:54:46.696436	192.168.75.14 > 192.168.77.1: icmp: echo request
8: 18:54:46.697412	192.168.77.1 > 192.168.75.14: icmp: echo reply

<#root>

firepower#

show cap CAPO

8 packets captured

1: 18:54:43.658672

192.168.77.6 > 192.168.77.1

: icmp: echo request

2: 18:54:43.658962	192.168.77.1 > 192.168.77.6: icmp: echo reply
3: 18:54:44.669109	192.168.77.6 > 192.168.77.1: icmp: echo request
4: 18:54:44.669337	192.168.77.1 > 192.168.77.6: icmp: echo reply
5: 18:54:45.682932	192.168.77.6 > 192.168.77.1: icmp: echo request
6: 18:54:45.683207	192.168.77.1 > 192.168.77.6: icmp: echo reply
7: 18:54:46.697031	192.168.77.6 > 192.168.77.1: icmp: echo request
8: 18:54:46.697275	192.168.77.1 > 192.168.77.6: icmp: echo reply

قزربم عمهم ماسقأ عم عمزحلا راثآ:

<#root>

firepower#

show cap CAPI packet-number 1 trace

8 packets captured

1: 18:54:43.658001 192.168.75.14 > 192.168.77.1: icmp: echo request

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 192.168.77.1 using egress ifc outside

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434434
access-list CSM_FW_ACL_ remark rule-id 268434434: ACCESS POLICY: FTD5506-1 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map class-default
match any
policy-map global_policy
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:

Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
Additional Information:
Dynamic translate 192.168.75.14/1 to 192.168.77.6/1

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
 inspect icmp
service-policy global_policy global
Additional Information:

Phase: 10
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 11
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
Additional Information:

Phase: 12
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 6981, packet dispatched to next module

Phase: 15
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 16
Type: SNORT
Subtype:

Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.77.1 using egress ifc outside

Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: next-hop and adjacency
Result: ALLOW
Config:
Additional Information:
adjacency Active
next-hop mac address c84c.758d.4980 hits 140694538709114

Phase: 19
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
1 packet shown

RI: (تمام ال ع ظ حال) يكي ماني دل xlate ءاشن م ت

<#root>

firepower#

show xlate

4 in use, 19 most used

Flags: D - DNS, e - extended, I - identity,

i - dynamic, r - portmap,

s - static, T - twice, N - net-to-net

NAT from inside:192.168.75.14 to dmz:192.168.76.100

flags sT idle 1:16:47 timeout 0:00:00

NAT from dmz:0.0.0.0/0 to inside:0.0.0.0/0

flags sIT idle 1:16:47 timeout 0:00:00

NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0

```
flags sIT idle 0:05:35 timeout 0:00:00
```

```
ICMP PAT from inside:192.168.75.14/1 to outside:192.168.77.6/1 flags ri idle 0:00:30 timeout 0:00:30
```

ىرت LINA تالچس ي ف:

```
<#root>
```

```
firepower#
```

```
show log
```

```
May 31 2016 18:54:43: %ASA-7-609001: Built local-host inside:192.168.75.14
```

```
May 31 2016 18:54:43: %ASA-6-305011: Built dynamic ICMP translation from inside:192.168.75.14/1 to outside:192.168.77.6/1
```

```
May 31 2016 18:54:43: %ASA-7-609001: Built local-host outside:192.168.77.1
```

```
May 31 2016 18:54:43: %ASA-6-302020: Built inbound ICMP connection for faddr 192.168.75.14/1 gaddr 192.168.77.6/1
```

```
May 31 2016 18:54:43: %ASA-6-302021: Teardown ICMP connection for faddr 192.168.75.14/1 gaddr 192.168.77.6/1
```

```
May 31 2016 18:54:43: %ASA-7-609002: Teardown local-host outside:192.168.77.1 duration 0:00:00
```

```
May 31 2016 18:55:17: %ASA-6-305012: Teardown dynamic ICMP translation from inside:192.168.75.14/1 to outside:192.168.77.6/1
```

مسق nat:

```
<#root>
```

```
firepower#
```

```
show nat
```

```
Manual NAT Policies (Section 1)
```

```
1 (inside) to (dmz) source static Host-A Host-B  
   translate_hits = 26, untranslate_hits = 26
```

```
2 (inside) to (outside) source dynamic Net_192.168.75.0_24bits interface  
   translate_hits = 94, untranslate_hits = 138
```

ضرع ل وادج ASP:

```
<#root>
```

```
firepower#
```

```
show asp table classify domain nat
```

```
Input Table
```

```
in id=0x7ff6036a9f50, priority=6, domain=nat, deny=false  
   hits=0, user_data=0x7ff60314dbf0, cs_id=0x0, flags=0x0, protocol=0  
   src ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any  
   dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0  
   input_ifc=inside, output_ifc=dmz
```



```

in id=0x7ff603696860, priority=6, domain=nat, deny=false
  hits=4, user_data=0x7ff602be3f80, cs_id=0x0, flags=0x0, protocol=0
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
  dst ip/id=192.168.76.100, mask=255.255.255.255, port=0, tag=any, dscp=0x0
  input_ifc=dmz, output_ifc=inside
in id=0x7ff602c75f00, priority=6, domain=nat, deny=false
  hits=94, user_data=0x7ff6036609a0, cs_id=0x0, flags=0x0, protocol=0
  src ip/id=192.168.75.0, mask=255.255.255.0, port=0, tag=any
  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
  input_ifc=inside, output_ifc=outside
in id=0x7ff603681fb0, priority=6, domain=nat, deny=false
  hits=276, user_data=0x7ff60249f370, cs_id=0x0, flags=0x0, protocol=0
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
  dst ip/id=192.168.77.6, mask=255.255.255.255, port=0, tag=any, dscp=0x0
  input_ifc=outside, output_ifc=inside

```

<#root>

firepower#

show asp table classify domain nat-reverse

Input Table

Output Table:

```

out id=0x7ff603685350, priority=6, domain=nat-reverse, deny=false
  hits=4, user_data=0x7ff60314dbf0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
  dst ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any, dscp=0x0
  input_ifc=dmz, output_ifc=inside
out id=0x7ff603638470, priority=6, domain=nat-reverse, deny=false
  hits=0, user_data=0x7ff602be3f80, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
  src ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any
  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
  input_ifc=inside, output_ifc=dmz
out id=0x7ff60361bda0, priority=6, domain=nat-reverse, deny=false
  hits=138, user_data=0x7ff6036609a0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
  dst ip/id=192.168.75.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
  input_ifc=outside, output_ifc=inside
out id=0x7ff60361c180, priority=6, domain=nat-reverse, deny=false
  hits=94, user_data=0x7ff60249f370, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
  src ip/id=192.168.75.0, mask=255.255.255.0, port=0, tag=any
  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
  input_ifc=inside, output_ifc=outside

```

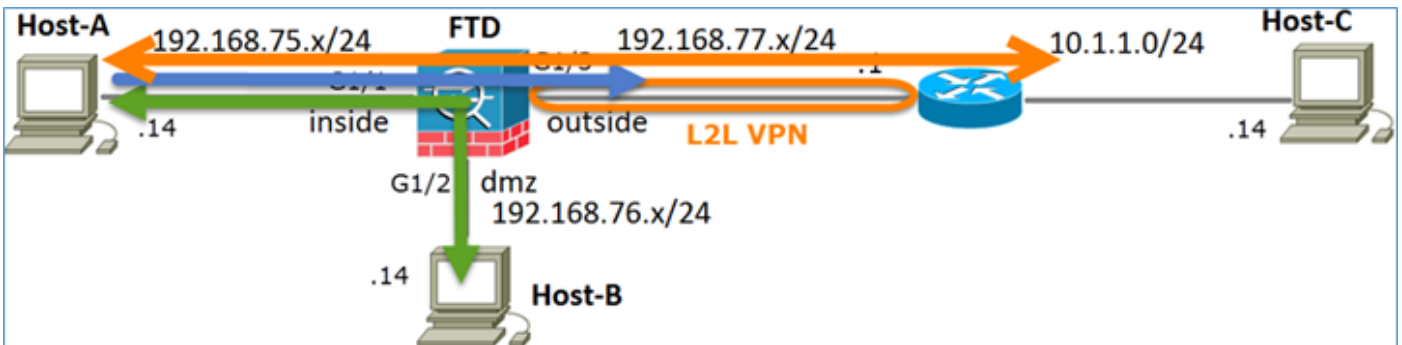
FTD ىلج NAT ءانثتسا نيوكت 3. ةمهمل

تابلطتملا هذهل اقبط NAT نيوكت:

nat ةدءاق	ةيوديلا NAT ةدءاق
-----------	-------------------

تباث	عون NAT
دوجوملا دعاوقلا عي مج 1 مسقلا يف	چاردا
*لخاد	ردصملا ةهجاو
*جراخ	ةهجولا ةهجاو
192.168.75.0/24	يلصلأا ردصملا
192.168.75.0/24	مجرتم ردصم
10.1.1.0/24	ةيلصلأا ةهجولا
10.1.1.0/24	ةمجرتملا ةهجولا

NAT ةدعاوقل نامألا قطانم مادختسا*



تباثلا NAT

تاب

NAT ءانثتسا

لجال:

يف حضورم وه امك ةمهم لك تابللطتم نيوكتب مقو ةثلاث NAT ةدعاوق فضا 1. ةوطخلال ةروصلال.

Rules										
Filter by Device										
					Original Packet			Translated Packet		
#	Direction	Type	Source Interface	Destination Interface	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services
▼ NAT Rules Before										
1	→	Static	inside_zone	outside_zone	Net_192.168.75.0_24bits	net_10.1.1.0_24bits		Net_192.168.75.0_24b	net_10.1.1.0_24bits	
2	→	Static	inside_zone	dmz_zone	Host-A			Host-B		
3	→	Dynamic	inside_zone	outside_zone	Net_192.168.75.0_24bits			Interface		
▼ Auto NAT Rules										
▼ NAT Rules After										

جرحم ةهجاو ديدحتل راسملا ن ع شح ب ءارجاب مق 2. ةوطخل

✎ جرحملا ةهجاو ديدحت ةيفيك ريغت كنكمي، هتفضأ يذلا لثم، nat، ةيوه دعاوقل: ةطخالام ةروصلال يف حضوم وه امك يداعلال راسملا شح ب مادختساو.

Edit NAT Rule

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

ق قحتل:

<#root>

firepower#

show run nat

```
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static ne
```

```
nat (inside,dmz) source static Host-A Host-B
```

```
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
```

<#root>

firepower#

show nat

Manual NAT Policies (Section 1)

```
1 (inside) to (outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static
   translate_hits = 0, untranslate_hits = 0
2 (inside) to (dmz) source static Host-A Host-B
   translate_hits = 26, untranslate_hits = 26
3 (inside) to (outside) source dynamic Net_192.168.75.0_24bits interface
   translate_hits = 96, untranslate_hits = 138
```

م تي تي التال VPN ةكبشبة صاخلا ريغ تانايا بلل رورم ةكرحل packet-tracer لريغش تبة مق
عقوتم وه امك PAT ةدعاق مادختسا متي. ةكبشلا لخاد نم اهليلع لوصحلا

<#root>

firepower#

```
packet-tracer input inside tcp 192.168.75.14 1111 192.168.77.1 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 192.168.77.1 using egress ifc outside
```

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434434
access-list CSM_FW_ACL_ remark rule-id 268434434: ACCESS POLICY: FTD5506-1 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached
```

```
Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
```

```
class-map class-default
  match any
policy-map global_policy
  class class-default
    set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:
```

```
Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
Additional Information:
```

```
Dynamic translate 192.168.75.14/1111 to 192.168.77.6/1111
Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 9
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
Additional Information:
```


```
Phase: 10
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 7227, packet dispatched to next module
```

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow

هلي غشت ب مق VPN ق فن ربع رم ت نأ بجي يتل رورم لة كرحل packet-tracer ل غشت ب مق (ي ل عأل VPN ق فن بلجت يتل ل وأل لة ل واصل م ذنم ني ترم).

 NAT. ءانثت سإ ءءاق رايتخ | بجي : ءظالم

مزل ل ءب ت ل ءل واصل ل و:

<#root>

firepower#

packet-tracer input inside tcp 192.168.75.14 1111 10.1.1.1 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: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static ne
Additional Information:
NAT divert to egress interface outside
Untranslate 10.1.1.1/80 to 10.1.1.1/80

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:

access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434434
access-list CSM_FW_ACL_ remark rule-id 268434434: ACCESS POLICY: FTD5506-1 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map class-default
match any
policy-map global_policy
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:

Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static ne
Additional Information:
Static translate 192.168.75.14/1111 to 192.168.75.14/1111

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: VPN
Subtype: encrypt
Result: DROP
Config:
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

ةيناثلا ةمزحلال بقعت ةلواحم:

<#root>

firepower#

```
packet-tracer input inside tcp 192.168.75.14 1111 10.1.1.1 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: UN-NAT

Subtype: static

Result: ALLOW

Config:

```
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static ne
```

Additional Information:

NAT divert to egress interface outside

Untranslate 10.1.1.1/80 to 10.1.1.1/80

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434434
```

```
access-list CSM_FW_ACL_ remark rule-id 268434434: ACCESS POLICY: FTD5506-1 - Default/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

```
class-map class-default
```

```
match any
```

```
policy-map global_policy
```

```
class class-default
```

```
set connection advanced-options UM_STATIC_TCP_MAP
```

```
service-policy global_policy global
```


Additional Information:

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static n

Additional Information:

Static translate 192.168.75.14/1111 to 192.168.75.14/1111

Phase: 7

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 9

Type: VPN

Subtype: encrypt

Result: ALLOW

Config:

Additional Information:

Phase: 10

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static n

Additional Information:

Phase: 11

Type: VPN

Subtype: ipsec-tunnel-flow

Result: ALLOW

Config:

Additional Information:

Phase: 12

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 13

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 7226, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow

NAT: لوصول و تارم ددع نم ققحتل

<#root>

firepower#

show nat

Manual NAT Policies (Section 1)

1 (inside) to (outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static

translate_hits = 9, untranslate_hits = 9

2 (inside) to (dmz) source static Host-A Host-B

translate_hits = 26, untranslate_hits = 26

3 (inside) to (outside) source dynamic Net_192.168.75.0_24bits interface

translate_hits = 98, untranslate_hits = 138

FTD ىل NAT نئال نيوك ت 4. ةمهمل

تابلطتمل هذهل اقبط NAT نيوك ت:

nat ةدعاق	ةيئاق لئال NAT ةدعاق
NAT عون	تباث
چاردا	2 مسقل ي ف
ردصملا ةهجاو	*لخاد

ةهجولا ةهجاو	DMZ*
يلصلأل رءصملا	192.168.75.99
مءرءم رءصم	192.168.76.99
ةءءاقلل هءه قءاوءل ءل ءل DNS ءوءر ةمءرء	نكمم

*NAT ءءءاقل نامأل قءانم ماءءءسا

لءل:

رءصلل ءل ءءوم وه امك ةمهملا ءابلءم لءق ءو ءءءاقلل نل ءوكءب مق 1. ءوءءل.

Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- outside_zone
- dmz_zone
- inside_zone
- Group1
- Group2

Source Interface Objects (1): inside_zone

Destination Interface Objects (1): dmz_zone

Add to Source

Add to Destination

Add NAT Rule ? x

NAT Rule: Auto NAT Rule

Type: Static Enable

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source: * obj-192.168.75.99

Original Port: TCP

Translated Packet

Translated Source: Address obj-192.168.76.99

Translated Port:

Add NAT Rule

NAT Rule:

Auto NAT Rule

Type:

Static

Enable

Interface Objects

Translation

PAT Pool

Advanced

Translate DNS replies that match this rule

Falthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

ةروصلال ي ف حضوم وه امك يه ةجيتنللا 2. ةوطخللا

Rules										
Filter by Device										
#	Direction	Type	Original Packet				Translated Packet			
			Source Interface	Destination Interface	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services
▼ NAT Rules Before										
1		Static	inside_zone	outside_zone	Net_192.168.75.0_24bits	net_10.1.1.0_24bits		Net_192.168.75.0_24b	net_10.1.1.0_24bits	
2		Static	inside_zone	dmz_zone	Host-A			Host-B		
3		Dynamic	inside_zone	outside_zone	Net_192.168.75.0_24bits			Interface		
▼ Auto NAT Rules										
#		Static	inside_zone	dmz_zone	obj-192.168.75.99			obj-192.168.76.99		
▼ NAT Rules After										

ققحتللا

<#root>

firepower#

show run nat

```
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static n
```

```
nat (inside,dmz) source static Host-A Host-B
```

```
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
```

```
!
```

```
object network obj-192.168.75.99
```

```
nat (inside,dmz) static obj-192.168.76.99 dns
```

<#root>

firepower#

show nat

Manual NAT Policies (Section 1)

```
1 (inside) to (outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static
  translate_hits = 9, untranslate_hits = 9
2 (inside) to (dmz) source static Host-A Host-B
  translate_hits = 26, untranslate_hits = 26
3 (inside) to (outside) source dynamic Net_192.168.75.0_24bits interface
  translate_hits = 98, untranslate_hits = 138
```

Auto NAT Policies (Section 2)

```
1 (inside) to (dmz) source static obj-192.168.75.99 obj-192.168.76.99 dns
  translate_hits = 0, untranslate_hits = 0
```

مزحلل عبتت ةاداً لالخ نم ققحتل:

<#root>

firepower#

packet-tracer input inside tcp 192.168.75.99 1111 192.168.76.100 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 192.168.76.100 using egress ifc dmz

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434434
access-list CSM_FW_ACL_ remark rule-id 268434434: ACCESS POLICY: FTD5506-1 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

class-map class-default

match any

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Additional Information:

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

object network obj-192.168.75.99

nat (inside,dmz) static obj-192.168.76.99 dns

Additional Information:

Static translate 192.168.75.99/1111 to 192.168.76.99/1111

Phase: 7

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 9

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 10

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 11

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 7245, packet dispatched to next module

Result:

input-interface: inside

input-status: up

input-line-status: up

output-interface: dmz

output-status: up

output-line-status: up

Action: allow

FTD على PAT عمجت نيوكت 5. عمهمال

تابلطتمال هذه لاقبب NAT نيوكت:

nat ءءءاق	ءءءاق NAT ءءءاق
NAT عون	ءءءاق
ءءءاق	3 مسءول ءءءاق
ءءءاق ءءءاق	*ءءءاق
ءءءاق ءءءاق	DMZ*
ءءءاق ءءءاق	192.168.75.0/24
ءءءاق ءءءاق	192.168.76.20-22
ءءءاق (1-65535) ءءءاق ءءءاق	ءءءاق

*NAT ءءءاق ءءءاق ءءءاق ءءءاق

ءءءاق:

ءءءاق ءءءاق ءءءاق ءءءاق ءءءاق ءءءاق 1. ءءءاق

Add NAT Rule

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules After

Type: Dynamic Enable

Description:

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- outside_zone
- dmz_zone
- inside_zone
- Group1
- Group2

Source Interface Objects (1): inside_zone

Destination Interface Objects (1): dmz_zone

Add NAT Rule ? X

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules After

Type: Dynamic Enable

Description:

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:* Net_192.168.75.0_24bits

Original Destination: Address

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source: Address

Translated Destination:

Translated Source Port:

Translated Destination Port:

حمست يتي ال ReserveVer ذفانم ني مضت عم تباثل ذف نلما قاطن ني كم تب مق 2. ةوطخل
 ةروصلال ي ف حضورم وه امك (1-65535) لملكالب قاطنل ما دخلتساب.

Add NAT Rule ? X

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules After

Type: Dynamic Enable

Description:

Interface Objects Translation **PAT Pool** Advanced

Enable PAT Pool

PAT: Address ige-192.168.76.20-22

Use Round Robin Allocation

Extended PAT Table

Flat Port Range

Include Reserve Ports

ةروصلال ي ف حضورم وه امك ةچي تنل نوكتو 3. ةوطخل

#	Direction	T...	Source Interface ...	Destination Interface Ob...	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
▼ NAT Rules Before											
1	St...		inside_zone	outside_zone	Net_192.168.75.0_24bits	net_10.1.1.0_24bits		Net_192.168.75.0_24bits	net_10.1.1.0_24bi		Dns:false
2	St...		inside_zone	dmz_zone	Host-A			Host-B			Dns:false
3	Dy...		inside_zone	outside_zone	Net_192.168.75.0_24bits			Interface			Dns:false
▼ Auto NAT Rules											
#	St...		inside_zone	dmz_zone	obj-192.168.75.99			obj-192.168.76.99			Dns:true
▼ NAT Rules After											
4	Dy...		inside_zone	dmz_zone	Net_192.168.75.0_24bits			range-192.168.76.20-22			Dns:false flat include-reserve

قحتال:

<#root>

firepower#

show run nat

```

nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination static n
nat (inside,dmz) source static Host-A Host-B
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
!
object network obj-192.168.75.99
  nat (inside,dmz) static obj-192.168.76.99 dns
!
nat (inside,dmz) after-auto source dynamic Net_192.168.75.0_24bits pat-pool range-192.168.76.20-22 flat

```

3: مسقلا ي ف ةدوجوم ةدعاقلا

<#root>

firepower#

show nat

Manual NAT Policies (Section 1)

```

1 (inside) to (outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination stat
  translate_hits = 9, untranslate_hits = 9
2 (inside) to (dmz) source static Host-A Host-B
  translate_hits = 26, untranslate_hits = 26
3 (inside) to (outside) source dynamic Net_192.168.75.0_24bits interface
  translate_hits = 98, untranslate_hits = 138

```

Auto NAT Policies (Section 2)

```

1 (inside) to (dmz) source static obj-192.168.75.99 obj-192.168.76.99 dns
  translate_hits = 1, untranslate_hits = 0

```

Manual NAT Policies (Section 3)

```

1 (inside) to (dmz) source dynamic Net_192.168.75.0_24bits pat-pool range-192.168.76.20-22 flat include-
  translate_hits = 0, untranslate_hits = 0

```

Packet-tracer نم ققحتلا

<#root>

firepower#

```
packet-tracer input inside icmp 192.168.75.15 8 0 192.168.76.5
```

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 192.168.76.5 using egress ifc dmz

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
```

```
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434434
```

```
access-list CSM_FW_ACL_ remark rule-id 268434434: ACCESS POLICY: FTD5506-1 - Default/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
```

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

```
class-map class-default
```

```
match any
```

```
policy-map global_policy
```

```
class class-default
```

```
set connection advanced-options UM_STATIC_TCP_MAP
```

```
service-policy global_policy global
```

Additional Information:

Phase: 6

Type: NAT

Subtype:

Result: ALLOW

Config:

```
nat (inside,dmz) after-auto source dynamic Net_192.168.75.0_24bits pat-pool range-192.168.76.20-22 flat
```

Additional Information:

```
Dynamic translate 192.168.75.15/0 to 192.168.76.20/11654
```

Phase: 7

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 9

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Config:

```
class-map inspection_default
```

```
  match default-inspection-traffic
```

```
policy-map global_policy
```

```
  class inspection_default
```

```
    inspect icmp
```

```
service-policy global_policy global
```

Additional Information:

Phase: 10

Type: INSPECT

Subtype: np-inspect

Result: ALLOW

Config:

Additional Information:

Phase: 11

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

```
nat (inside,dmz) after-auto source dynamic Net_192.168.75.0_24bits pat-pool range-192.168.76.20-22 flat
```

Additional Information:

Phase: 12

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 13

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 14

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 7289, packet dispatched to next module

Result:

input-interface: inside

input-status: up

input-line-status: up

output-interface: dmz

output-status: up

output-line-status: up

Action: allow

ةحصلا نم ققحتلا

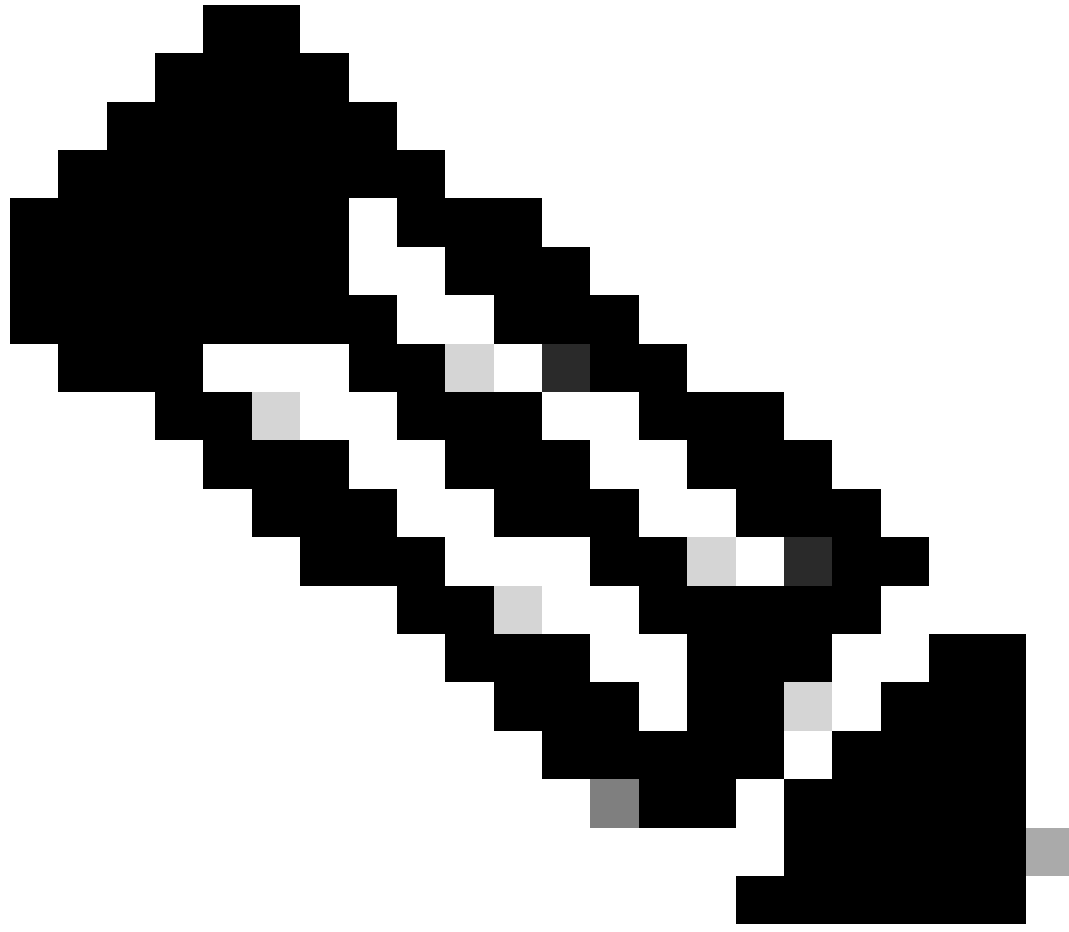
ححص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا

ماهملا ماسقأ نم مسق لك يف ققحتلا حرش مت دقو

اهحالصإو ااطخأل فاشكتسا

اهحالصإو نيوكتلا ااطخأ فاشكتسال اهمادختسا كنكمي تامولعم مسقلا اذه رفوي

packet-tracer ليغشتب مق م ث، FMC لىل عم دقتملا اهلصإو ااطخأل فاشكتسا ةحفص حتفا
show nat pool رمالا ليغشتب مق م ث، tracer



ةروصولا يف حضوم وه امك هلمكأب قاطنلا مدختسي يذلا لخدملا :ةظحالم

Overview Analysis Policies Devices Objects AMP Deploy System

Configuration Users Domains Integration Updates Licenses Health Monitor

Advanced Troubleshooting

FTD5506-1

File Download ASA CLI

Command Parameter **1**

Output

```

UDP PAT pool inside, address 192.168.75.6, range 1-511, allocated 2
UDP PAT pool inside, address 192.168.75.6, range 512-1023, allocated 1
UDP PAT pool inside, address 192.168.75.6, range 1024-65535, allocated 2
ICMP PAT pool dmz:range-192.168.76.20-22, address 192.168.76.20, range 1-65535, allocated 1
UDP PAT pool outside, address 192.168.77.6, range 1-511, allocated 3
UDP PAT pool outside, address 192.168.77.6, range 512-1023, allocated 0
UDP PAT pool outside, address 192.168.77.6, range 1024-65535, allocated 3

```

2

قلمص تاذا تامولعم

- ان: Cisco Firepower Management Center نيوكت ليلد تارادصا عيمج يلع روثلعلا نكمي

[Cisco نم نمآلا ةيماحللا رادج ديدهت نع عافدللا قئاثو ربع لقنلتلا](#)

- ئيرملا ليلدللا اذهب ةدشب Cisco نم (TAC) يملعلا ةينقنلتلا ةدعاسملا زكرم ي صوي Cisco Firepower، نم يلاتلا ليجلا نامأ تاينقنلت لوح ةقمعتملا ةيملعلا ةفرعملل ةلاقملا هذه يف ةروكذملا تاينقنلتلا نمضتت يتلاو:

[ةيرانللا ةقلاطللا ديدهت دض عافدللا - Cisco Press](#)

- تاينقنلتب ةقلعتملا ةينقنلتا تاظالملا ءاطخا فاشكتسا و ةئيهتلا تايلمع ةفاكل ءاحالصا و FirePOWER:

[Cisco نم نمآلا ةيماحللا رادج قرادا زكرم](#)

- [Cisco Systems - تادنتسمللا وينقنلتلا معدلا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نء مء دختسمل معد وء مء مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءء. ةصاأل مء تءل ب
Cisco ةلخت. فرت مء مء مء دقتل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل
ىل ةل
(رفوتم طبارل) ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل ةل