Configure and Verify NAT on FTD

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Network Diagram
- Task 1. Configure Static NAT on FTD
- Task 2. Configure Port Address Translation (PAT) on FTD
- Task 3. Configure NAT Exemption on FTD
- Task 4. Configure Object NAT on FTD
- Task 5. Configure PAT Pool on FTD

Verify

Troubleshoot

Related Information

Introduction

This document describes how to configure and verify basic Network Address Translation (NAT) on Firepower Threat Defense (FTD).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Secure Firewall Threat Defense Virtual running on Version 7.7.0 (Build 89)
- Secure Firewall Management Center Virtual (FMC) running Version 7.7.0 (build 91)
- 3 Windows 7 hosts
- Cisco IOS® 3925 router that runs LAN-to-LAN (L2L) VPN

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

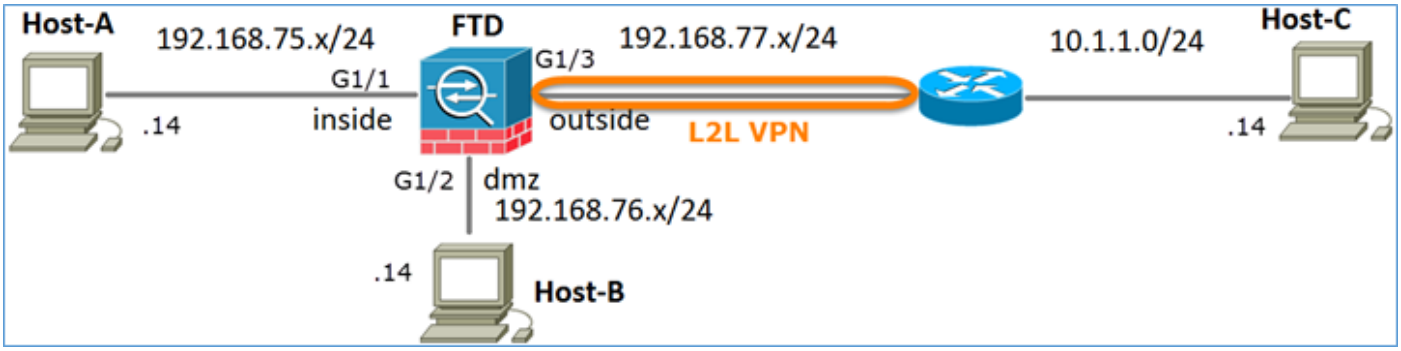
FTD supports the same NAT configuration options as the classic Adaptive Security Appliance (ASA):

- NAT Rules Before – Twice NAT (section 1).
- Auto NAT Rules – Section 2
- NAT Rules After – Twice NAT (section 3) .

Since FTD configuration is done from the FMC when it comes to NAT configuration, it is necessary to be familiar with the FMC GUI and the various configuration options.

Configure

Network Diagram



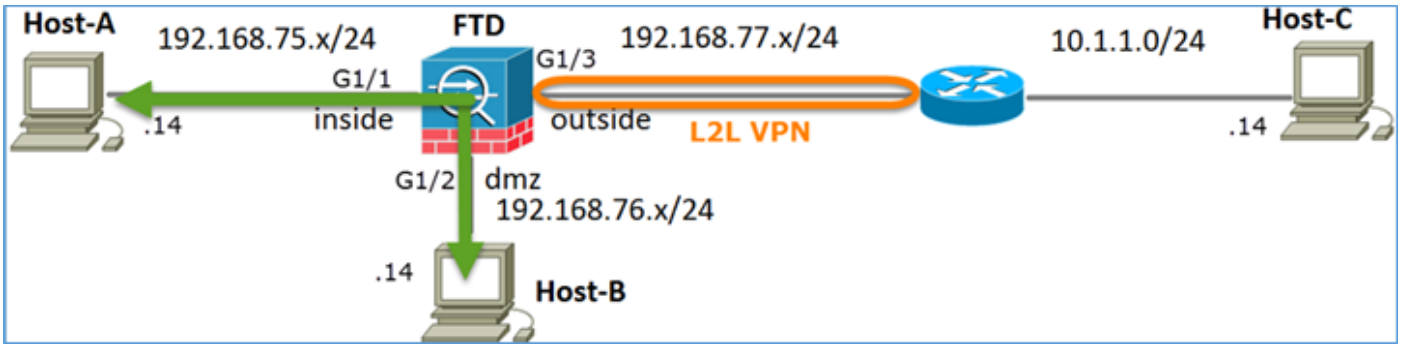
Task 1. Configure Static NAT on FTD

Configure NAT as per these requirements:

NAT Policy Name	Name of the FTD device
NAT Rule	Manual NAT Rule
NAT Type	Static
Insert	In Section 1
Source interface	inside*
Destination interface	dmz*
Original Source	192.168.75.14

Translated Source	192.168.76.100

*Use Security Zones for the NAT Rule

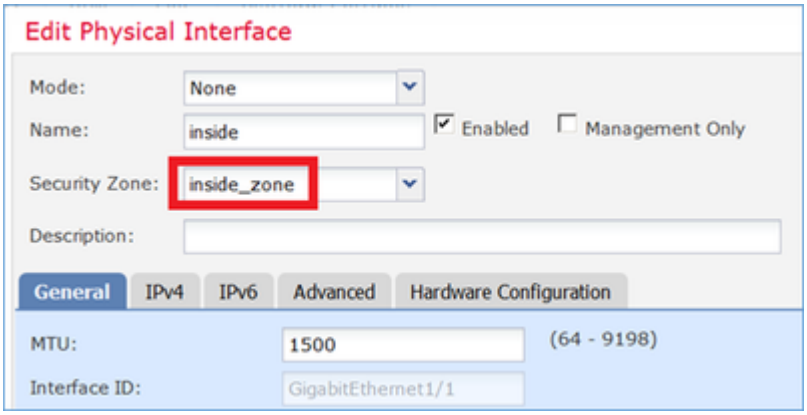


Solution:

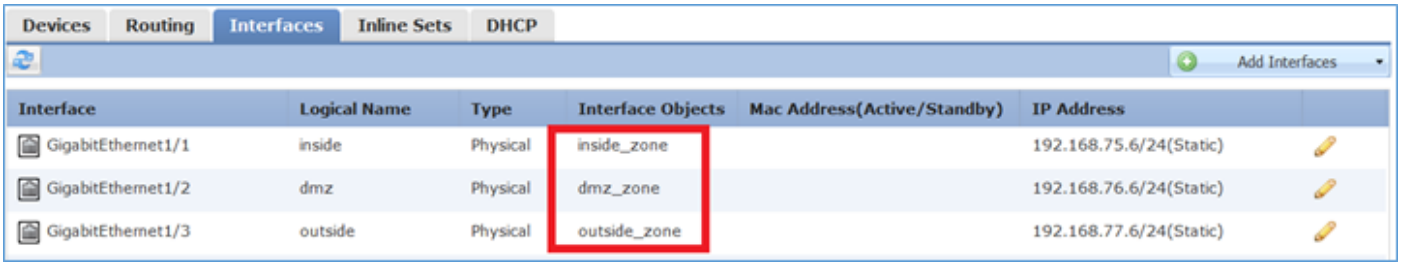
While on classic ASA, you have to use nameif in the NAT rules. On FTD, you need to use either Security Zones or Interface Groups.

Step 1. Assign interfaces to Security Zones/Interface Groups.

In this task, it is decided to assign the FTD interfaces that is used for NAT to Security Zones. Alternatively, you can assign them to Interface Groups as shown in the image.



Step 2. The result is as shown in the image.



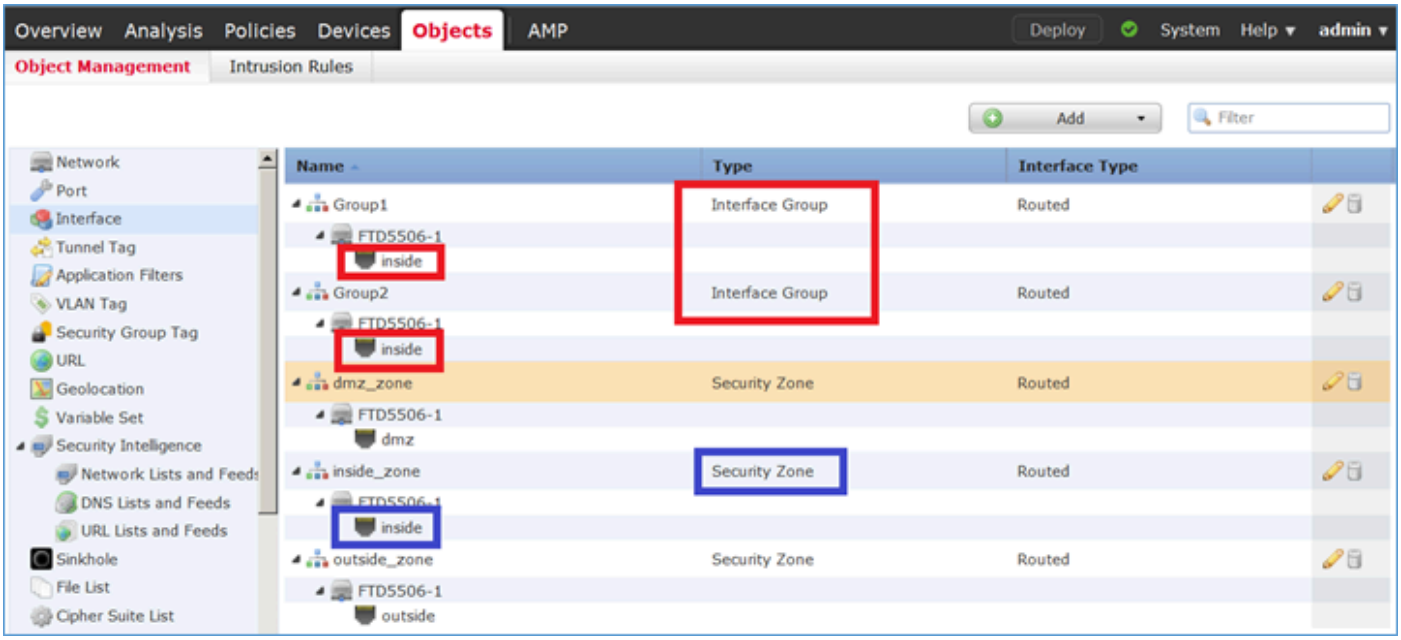
Step 3. You can create/edit Interface Groups and Security Zones from the **Objects > Object Management > Interface** page as shown in the image.



Security Zones vs Interface Groups

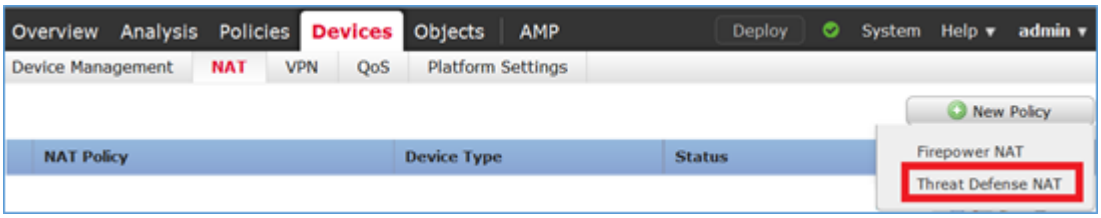
The main difference between Security Zones and Interface Groups is that an interface can belong to only one Security Zone, but can belong to multiple Interface Groups. So practically, the Interface Groups provide more flexibility.

You can see that interface inside belongs to two different Interface Groups, but only one Security Zone as shown in the image.

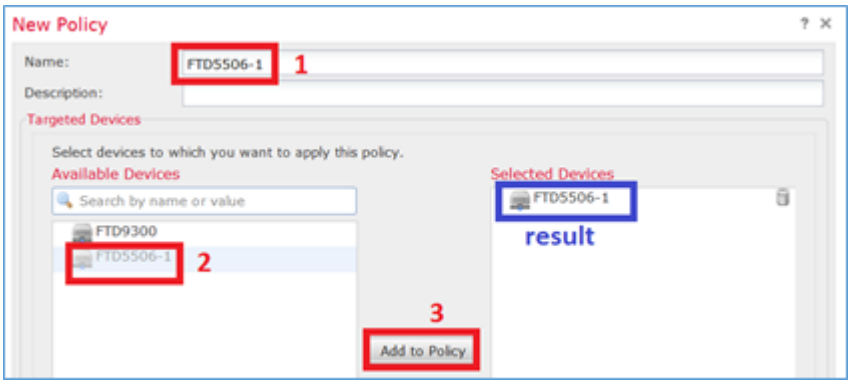


Step 4. Configure Static NAT on FTD.

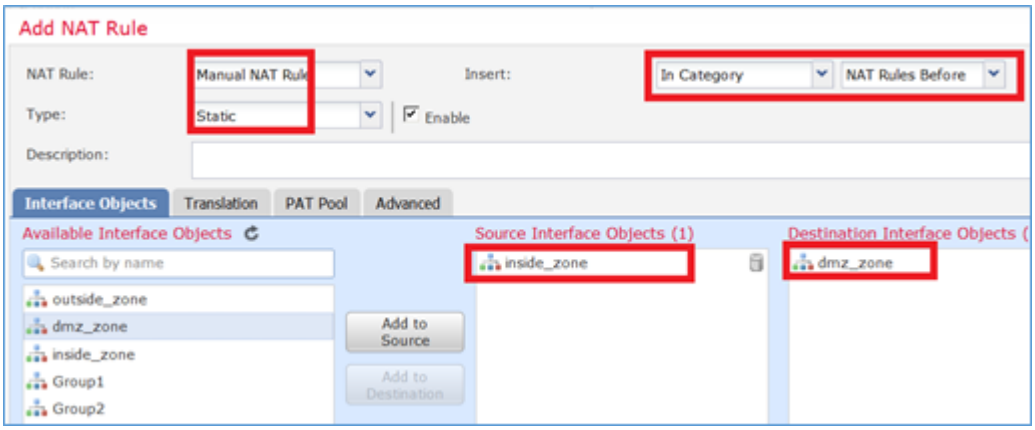
Navigate to **Devices > NAT** and create a NAT Policy. Select **New Policy > Threat Defense NAT** as shown in the image.



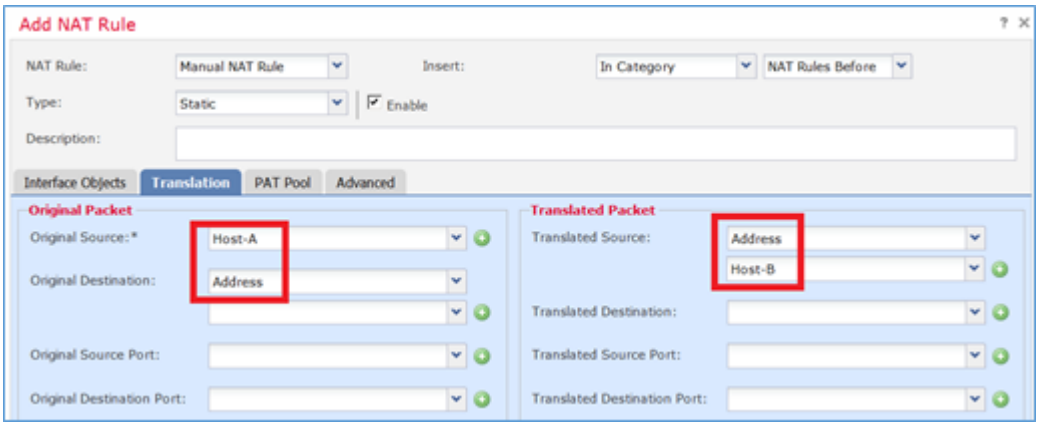
Step 5. Specify the **policy name** and assign it to a **target device** as shown in the image.

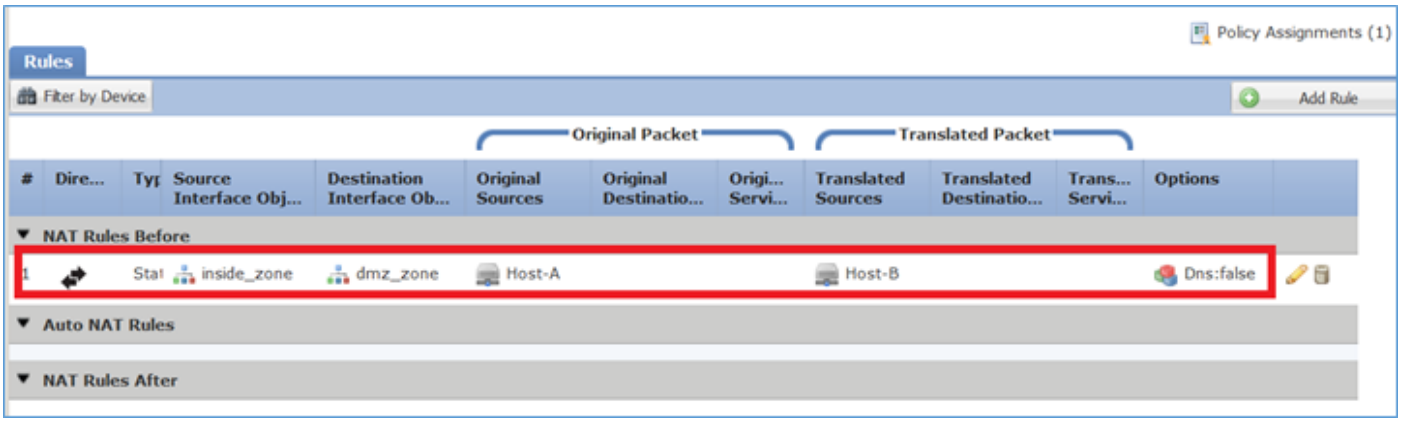


Step 6. Add a NAT Rule to the policy, click **Add Rule**.



Specify these as per task requirements as shown in the images.





Host-A = 192.168.75.14

Host-B = 192.168.76.100

<#root>

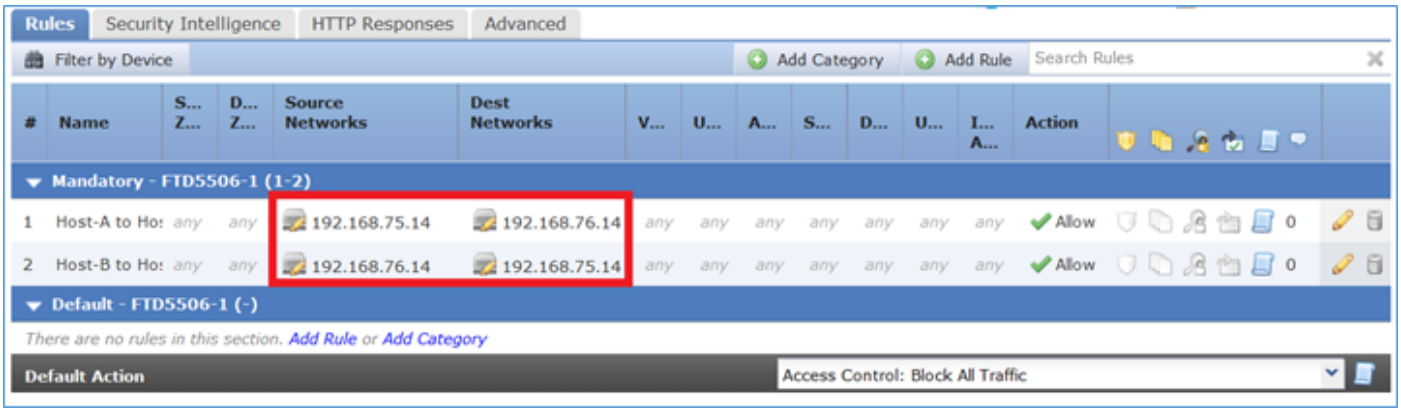
```
firepower#
```

show run object

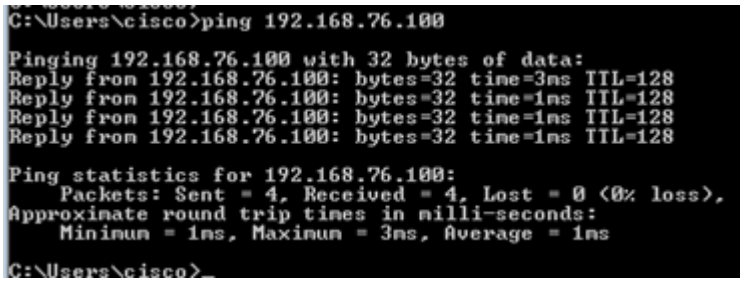
```
object network Host-A
 host 192.168.75.14
object network Host-B
 host 192.168.76.100
```

Warning: If you configure Static NAT and specify an Interface as Translated Source, then all traffic destined to the IP address of the interface is redirected. Users cannot access any service enabled on the mapped interface. Examples of such services include routing protocols like OSPF and EIGRP.

Step 7. The result is as shown in the image.



Step 8. Ensure that there is an Access Control Policy that allows Host-B to access Host-A and vice versa. Remember that Static NAT is bidirectional by default. Similar to classic ASA, see the usage of real IPs.



Verification:

From LINA CLI:

<#root>

firepower#

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

The NAT rule was inserted in Section 1 as expected:

<#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

Note: The 2 xlates that are created in the background.

```
<#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
```

The ASP NAT tables:

```
<#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
```

Enable capture with trace detail on FTD and ping from Host-B to Host-A and as shown in the image.

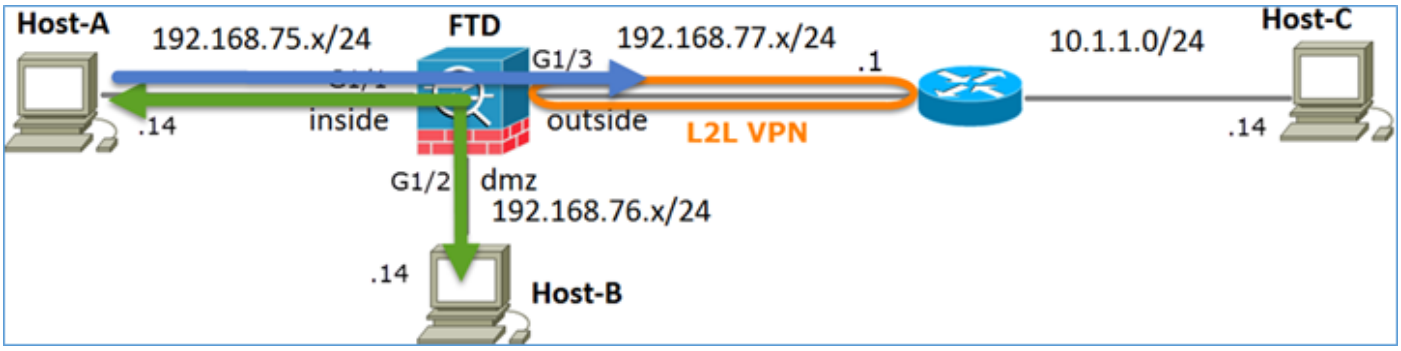
<#root>

```
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



The hit counts is in the ASP tables:

<#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
```

The packet capture shows:

<#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
```

Traces of a packet (important points are highlighted).

Note: The ID of the NAT rule and its correlation with the ASP table.

<#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
```

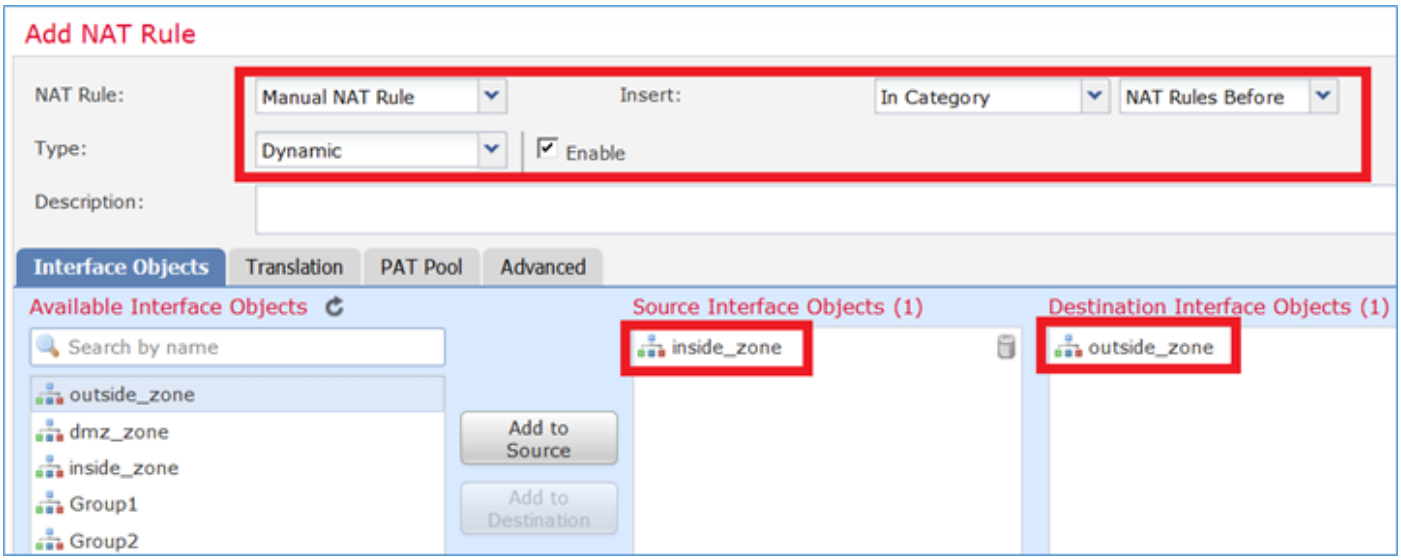
Task 2. Configure Port Address Translation (PAT) on FTD

Configure NAT as per these requirements:

NAT Rule	Manual NAT Rule
NAT Type	Dynamic
Insert	In Section 1
Source interface	inside*
Destination interface	outside*
Original Source	192.168.75.0/24

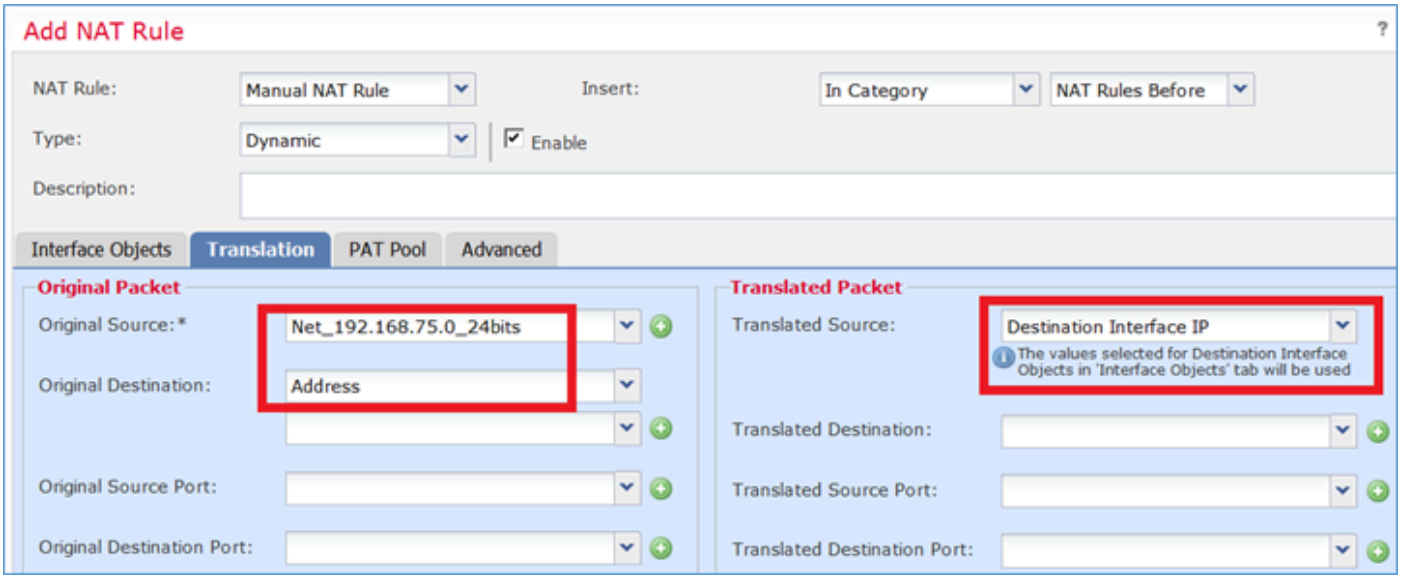
Translated Source	Outside interface (PAT)

*Use Security Zones for the NAT Rule

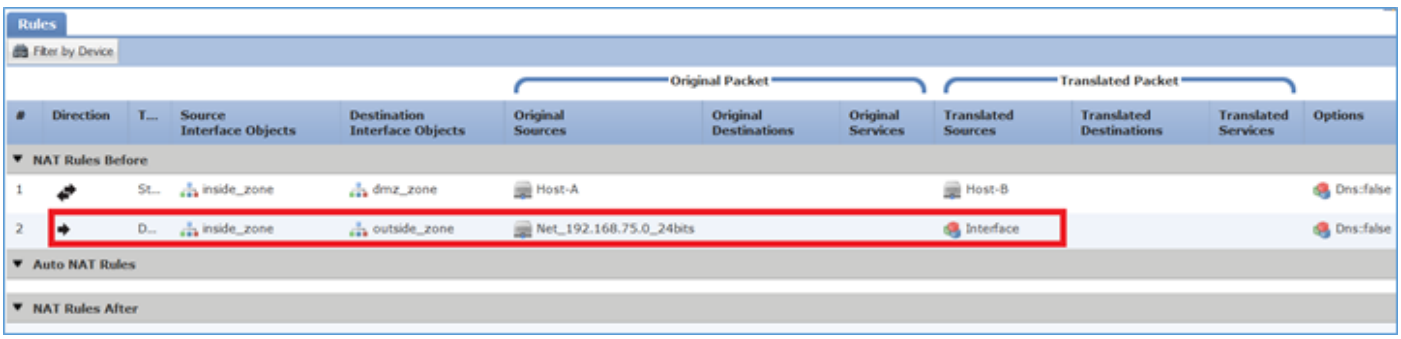


Solution:

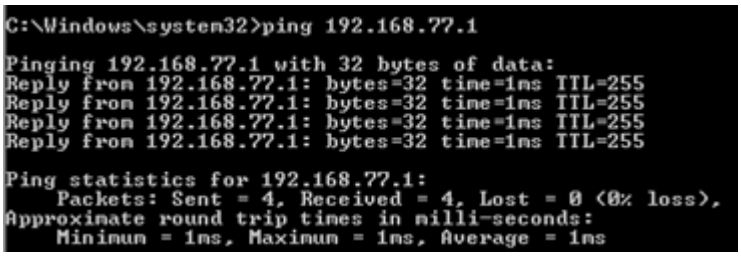
Step 1. Add a second NAT Rule and configure as per the task requirements as shown in the image.



Step 2. Here is how PAT is configured as shown in the image.



Step 3. The result is as shown in the image.



Step 4. For the rest of this lab, configure the Access Control Policy to allow all the traffic to go through.

Verification:

NAT configuration:

```
<#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_24 interface
    translate_hits = 0, untranslate_hits = 0
```

From LINA CLI, note the new entry:

```
<#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
```

Enable capture on inside and outside interface. On inside capture enable trace:

```
<#root>

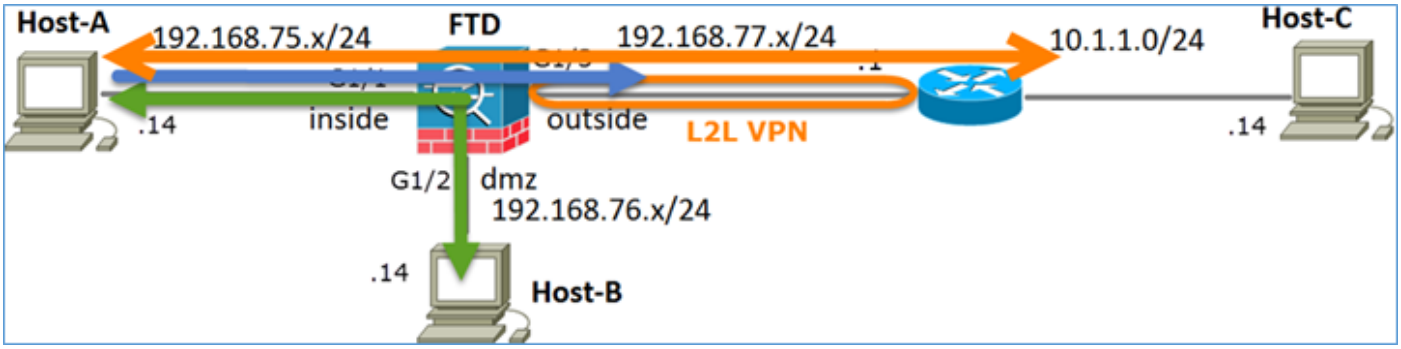
firepower#
```

```
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
```

Ping from Host-A (192.168.75.14) to IP 192.168.77.1 as shown in the image.



In LINA captures, you can see the PAT translation:

<#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
```

Traces of a packet with important sections highlighted:

<#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: ACP - Mandatory
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_24 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_24 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
```

The dynamic xlate was created (note the ri flags):

```
<#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
```

In the LINA logs you see:

```
<#root>

firepower#

show log

Aug 1 2025 18:54:43: %FTD-7-609001: Built local-host inside:192.168.75.14

Aug 1 2025 18:54:43: %FTD-6-305011: Built dynamic ICMP translation from inside:192.168.75.14/1 to outsid

Aug 1 2025 18:54:43: %FTD-7-609001: Built local-host outside:192.168.77.1
Aug 1 2025 18:54:43: %FTD-6-302020: Built inbound ICMP connection for faddr 192.168.75.14/1 gaddr 192.1
Aug 1 2025 18:54:43: %FTD-6-302021: Teardown ICMP connection for faddr 192.168.75.14/1 gaddr 192.168.77
Aug 1 2025 18:54:43: %FTD-7-609002: Teardown local-host outside:192.168.77.1 duration 0:00:00

Aug 1 2025 18:55:17: %FTD-6-305012: Teardown dynamic ICMP translation from inside:192.168.75.14/1 to out
```

NAT sections:

```
<#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_24 interface
**   translate_hits = 94, untranslate_hits = 138**

ASP tables show:

<#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
```

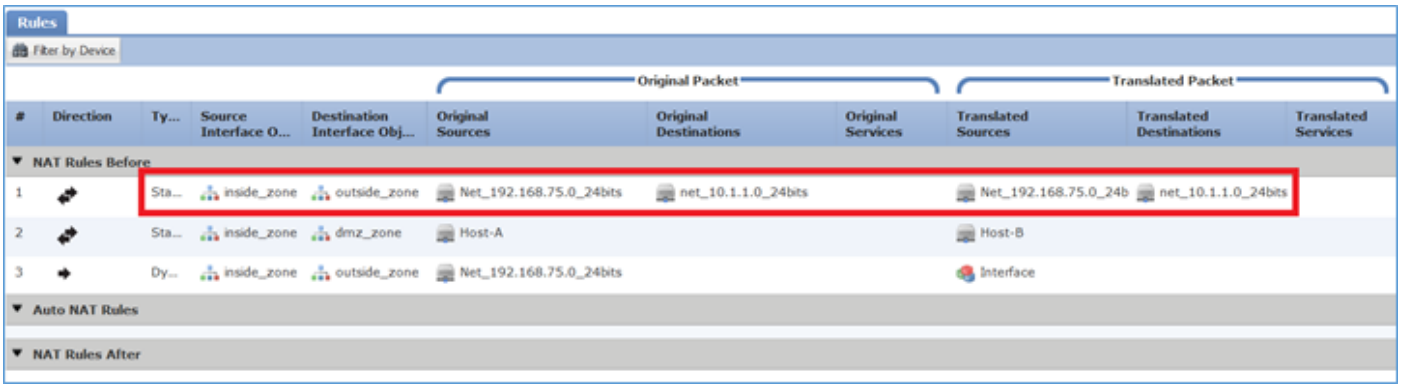
```
        hits=138, user_data=0x7ff6036609a0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip/id=192.168.75.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
        input_ifc=outside, output_ifc=inside
out id=0x7ff60361c180, priority=6, 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
```

Task 3. Configure NAT Exemption on FTD

Configure NAT as per these requirements:

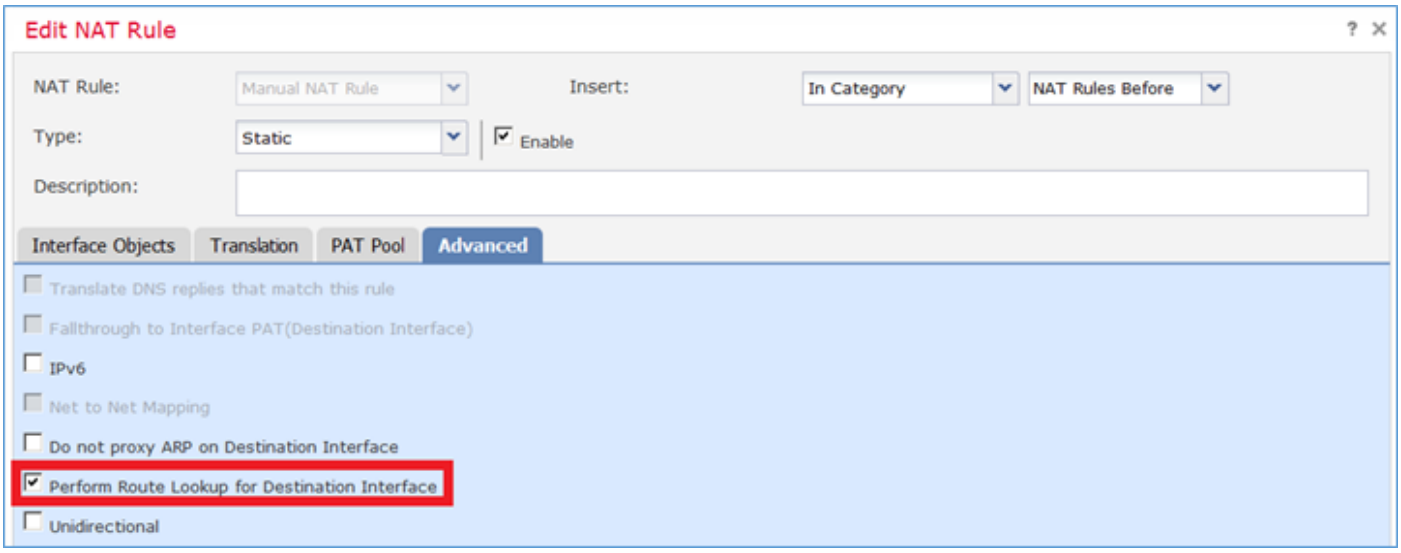
NAT Rule	Manual NAT Rule
NAT Type	Static
Insert	In Section 1 all existing rules
Source interface	inside*
Destination interface	outside*
Original Source	192.168.75.0/24
Translated Source	192.168.75.0/24
Original Destination	10.1.1.0/24
Translated Destination	10.1.1.0/24

*Use Security Zones for the NAT Rule



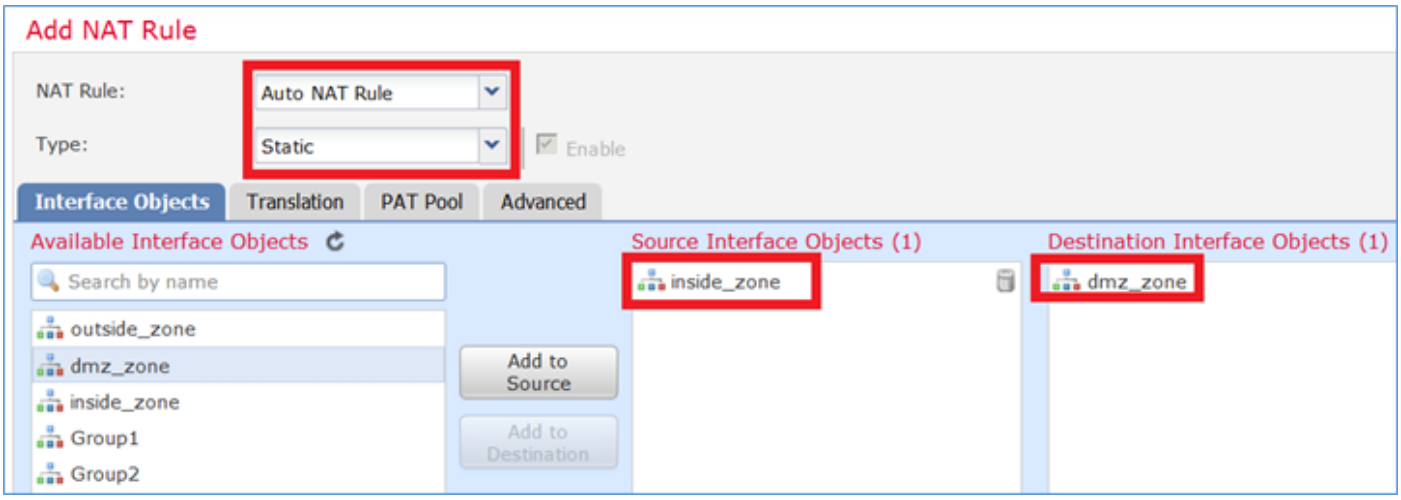
Solution:

Step 1. Add a third NAT Rule and configure per task requirements as shown in the image.



Step 2. Perform Route Lookup for egress interface determination.

Note: For Identity NAT Rules, like the one that you added, you can change how the egress interface is determined and use normal route lookup as shown in the image.



Verification:

<#root>

```
firepower#
show run nat
nat (inside,outside) source static Net_192.168.75.0_24 Net_192.168.75.0_24 destination static net_10.1.1
nat (inside,dmz) source static Host-A Host-B
```

```
nat (inside,outside) source dynamic Net_192.168.75.0_24 interface
```

```
<#root>

firepower#

show nat

Manual NAT Policies (Section 1)

1 (inside) to (outside) source static Net_192.168.75.0_24 Net_192.168.75.0_24  destination static net_10
    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_24 interface
    translate_hits = 96, untranslate_hits = 138
```

Run packet-tracer for non-VPN traffic sourced from inside network. The PAT rule is used as expected:

```
<#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: ACP - Mandatory
```

```
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_24 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_24 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
```

Run packet-tracer for traffic that must go through the VPN tunnel (run it twice since the first try brings the VPN tunnel up).

Note: You must choose the NAT Exemption Rule.

First packet-tracer attempt:

<#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_24 Net_192.168.75.0_24 destination static net_10.1.1
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: ACP - Mandatory
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_24 Net_192.168.75.0_24 destination static net_10.1.1
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
```

Second packet-tracer attempt:

```
<#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_24 Net_192.168.75.0_24 destination static net_10.1.1
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: ACP - Mandatory
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_24 Net_192.168.75.0_24 destination static net_10.1.1
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_24 Net_192.168.75.0_24 destination static net_10.1.1
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 hit count verification:

<#root>

```
firepower#
```

show nat

```
Manual NAT Policies (Section 1)
1 (inside) to (outside) source static Net_192.168.75.0_24 Net_192.168.75.0_24  destination static net_1
    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_24 interface
    translate_hits = 98, untranslate_hits = 138
```

Task 4. Configure Object NAT on FTD

Configure NAT as per these requirements:

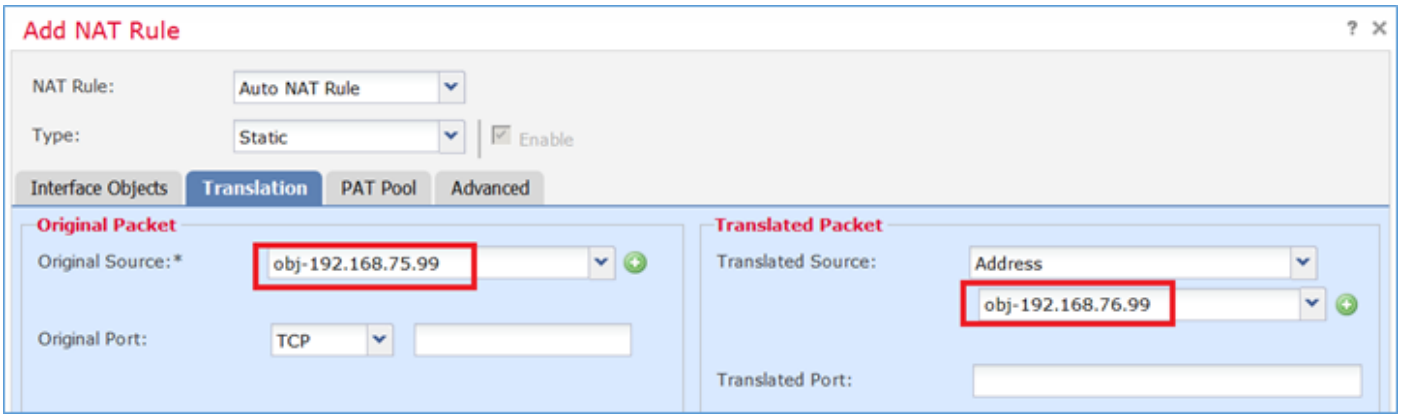
NAT Rule	Auto NAT Rule
NAT Type	Static

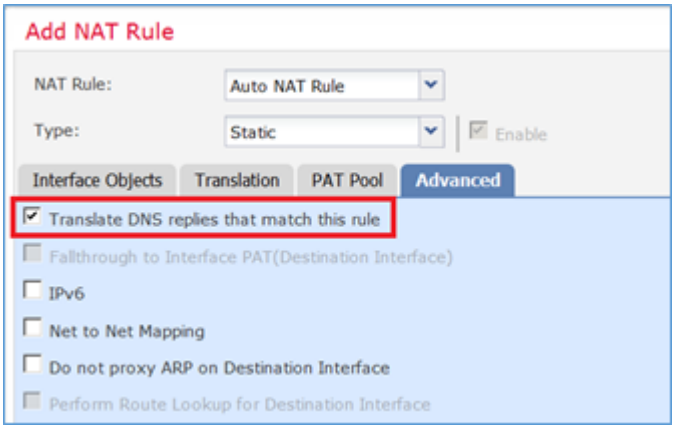
Insert	In Section 2
Source interface	inside*
Destination interface	dmz*
Original Source	192.168.75.99
Translated Source	192.168.76.99
Translate DNS replies that match this rule	Enabled

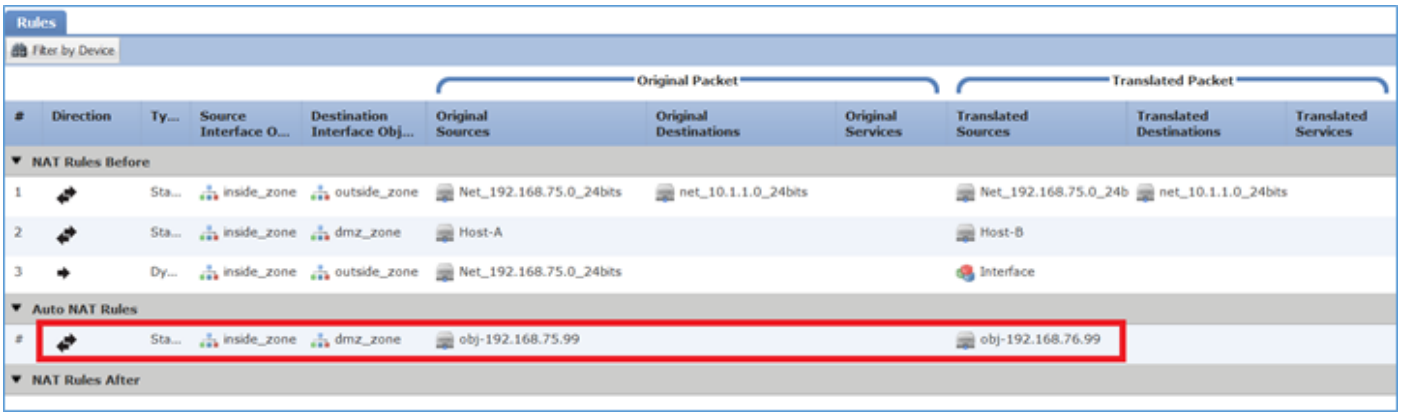
*Use Security Zones for the NAT Rule

Solution:

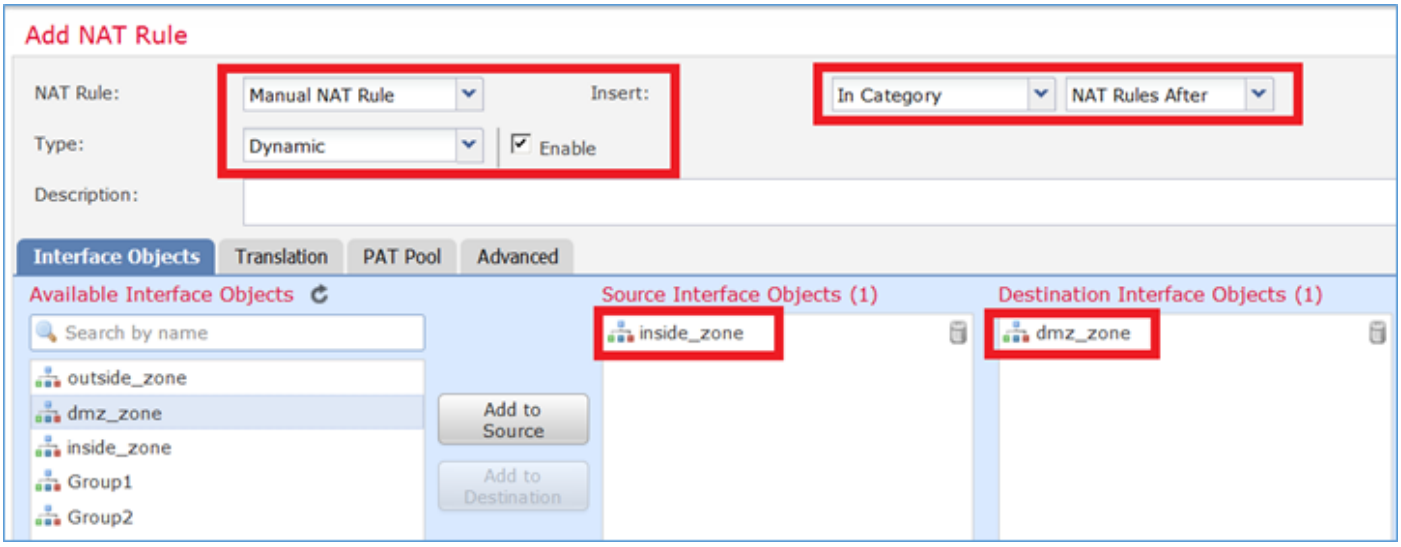
Step 1. Configure the rule as per the task requirements as shown in the images.







Step 2. The result is as shown in the image:



Verification:

<#root>

```
firepower#
```

show run nat

```
nat (inside,outside) source static Net_192.168.75.0_24 Net_192.168.75.0_24 destination static net_10.1.1
nat (inside,dmz) source static Host-A Host-B
nat (inside,outside) source dynamic Net_192.168.75.0_24 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_24 Net_192.168.75.0_24  destination static net_1
    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_24 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
```

Verification with packet-tracer:

<#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: ACP - Mandatory
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
```

Task 5. Configure PAT Pool on FTD

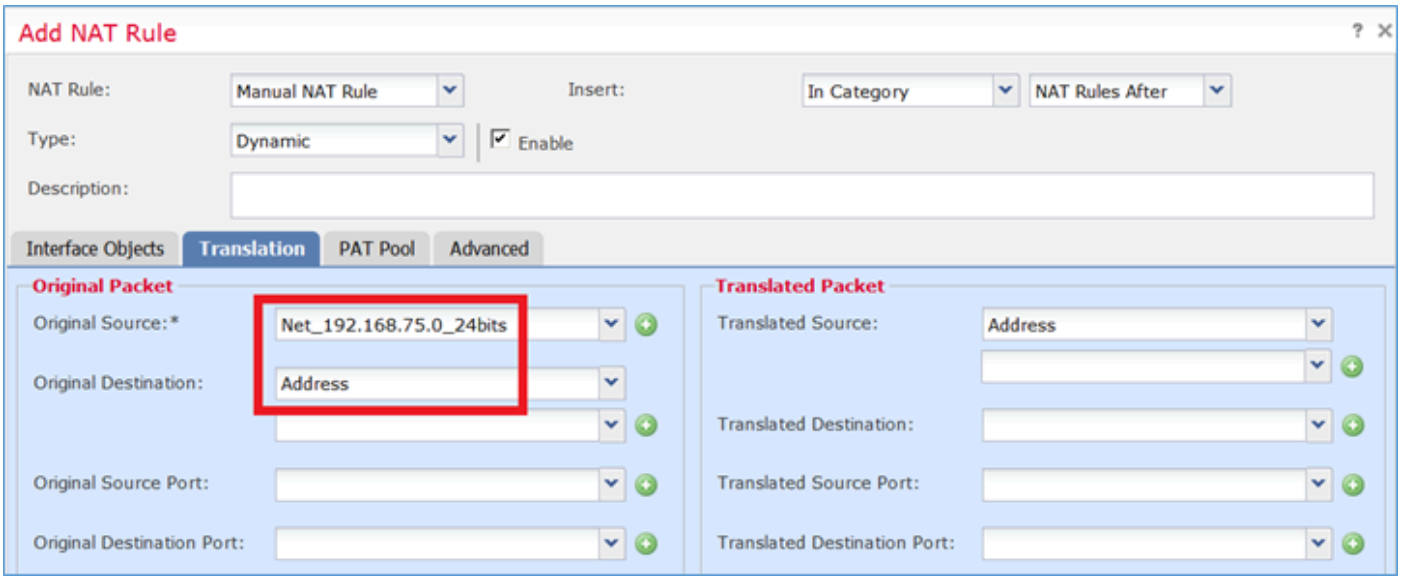
Configure NAT as per these requirements:

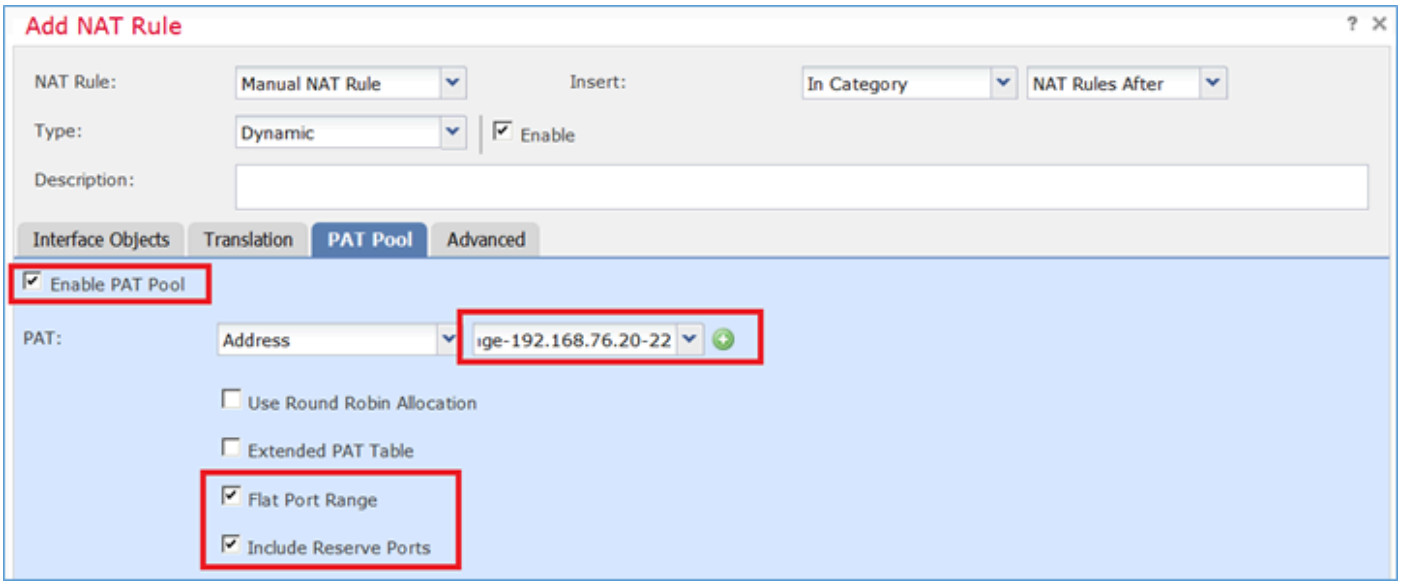
NAT Rule	Manual NAT Rule
NAT Type	Dynamic
Insert	In Section 3
Source interface	inside*
Destination interface	dmz*
Original Source	192.168.75.0/24
Translated Source	192.168.76.20-22
Use the entire range (1-65535)	Enabled

*Use Security Zones for the NAT Rule

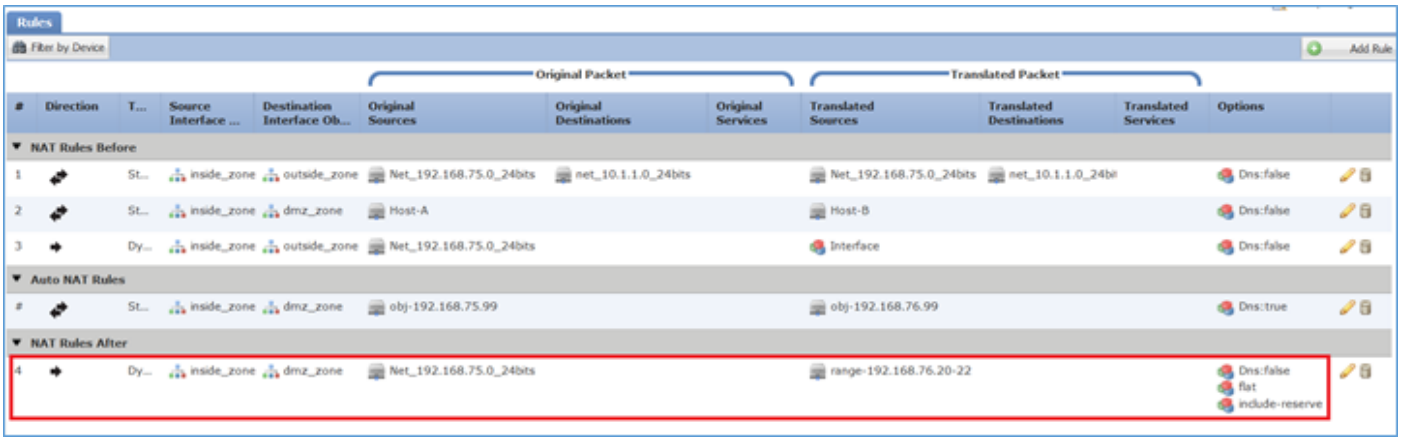
Solution:

Step 1. Configure the rule per task requirements as shown in the images.

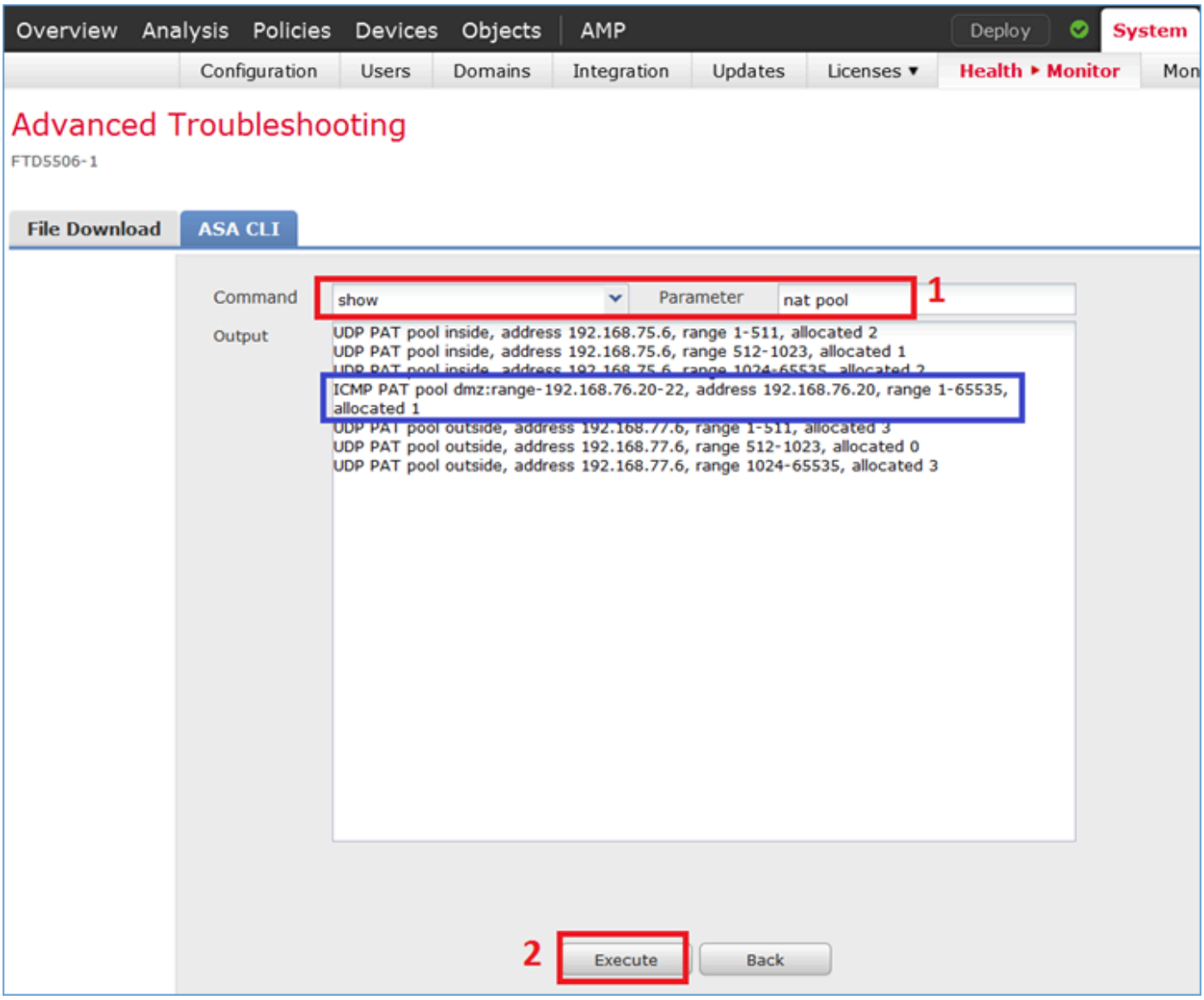




Step 2. Enable **Flat Port Range** with **Include Reserver Ports** which allows the use of the entire range (1-65535) as shown in the image.



Step 3. The result is as shown in the image.



Verification:

<#root>

```
firepower#
```

show run nat

```
nat (inside,outside) source static Net_192.168.75.0_24 Net_192.168.75.0_24 destination static net_10.1.
nat (inside,dmz) source static Host-A Host-B
nat (inside,outside) source dynamic Net_192.168.75.0_24 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_24 pat-pool range-192.168.76.20-22 flat incl

The rule is in Section 3:

<#root>

```
firepower#
```

```
show nat
```

```
Manual NAT Policies (Section 1)
1 (inside) to (outside) source static Net_192.168.75.0_24 Net_192.168.75.0_24  destination static net_1
    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_24 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_24 pat-pool range-192.168.76.20-22 flat include-rese
    translate_hits = 0, untranslate_hits = 0
```

Packet-tracer verification:

<#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: ACP - Mandatory
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_24 pat-pool range-192.168.76.20-22 flat incl
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_24 pat-pool range-192.168.76.20-22 flat inc
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
```

Verify

Use this section in order to confirm that your configuration works properly.

Verification has been explained in the individual task sections.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Open the **Device > Troubleshoot > Packet Tracer** page on the FMC, and run the **packet-tracer**, then run the **show nat pool** command in **Device > Troubleshoot > Threat Defense CLI**.

Sample output:

<#root>

FTDv#

show nat pool

```
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
```

Related Information

- All versions of the Cisco Firepower Management Center configuration guide can be found here:

Navigating the Cisco Secure Firewall Threat Defense Documentation

- Cisco Global Technical Assistance Center (TAC) strongly recommends this visual guide for in-depth practical knowledge on Cisco Firepower Next Generation Security Technologies, which includes the ones mentioned in this article:

  Cisco Press - Firepower Threat Defense

- For all Configuration and Troubleshooting TechNotes that pertain to Firepower technologies:

  Cisco Secure Firewall Management Center

- Technical Support & Documentation - Cisco Systems