在FTD上設定和驗證NAT

目錄

簡介

本檔案介紹如何在Firepower威脅防禦(FTD)上設定和驗證基本網路位址翻譯(NAT)。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行FTD代碼6.1.0-226的ASA5506X
- 運行6.1.0-226的FireSIGHT管理中心(FMC)
- 3台Windows 7主機
- 運行LAN到LAN (L2L) VPN的Cisco IOS® 3925路由器

實驗室完成時間：1小時

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

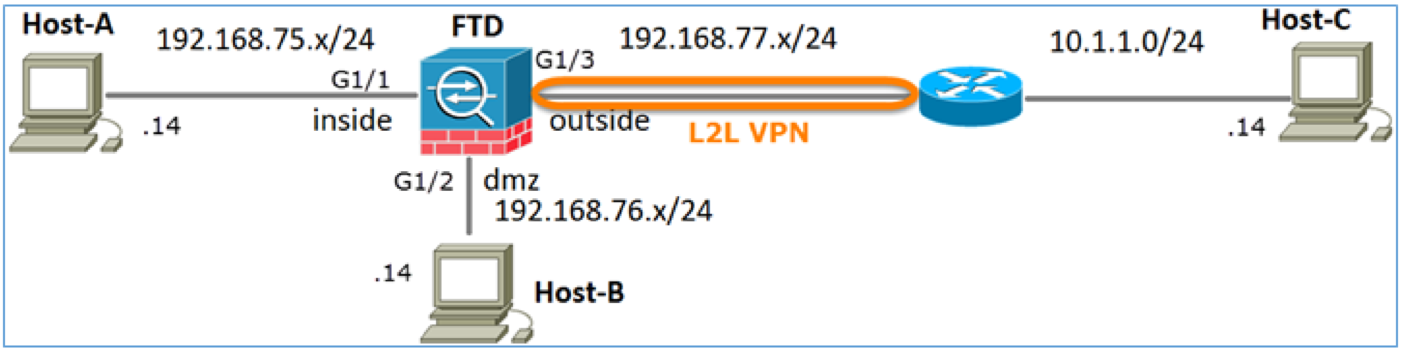
FTD支援與典型調適型安全裝置(ASA)相同的NAT組態選項：

- 之前的NAT規則-這相當於傳統ASA上的兩次NAT（第1部分）。
- 自動NAT規則-傳統ASA第2部分
- NAT Rules After -這相當於傳統ASA上的兩次NAT（第3部分）。

由於FTD配置在NAT配置時從FMC中完成，因此必須熟悉FMC GUI和各種配置選項。

設定

網路圖表



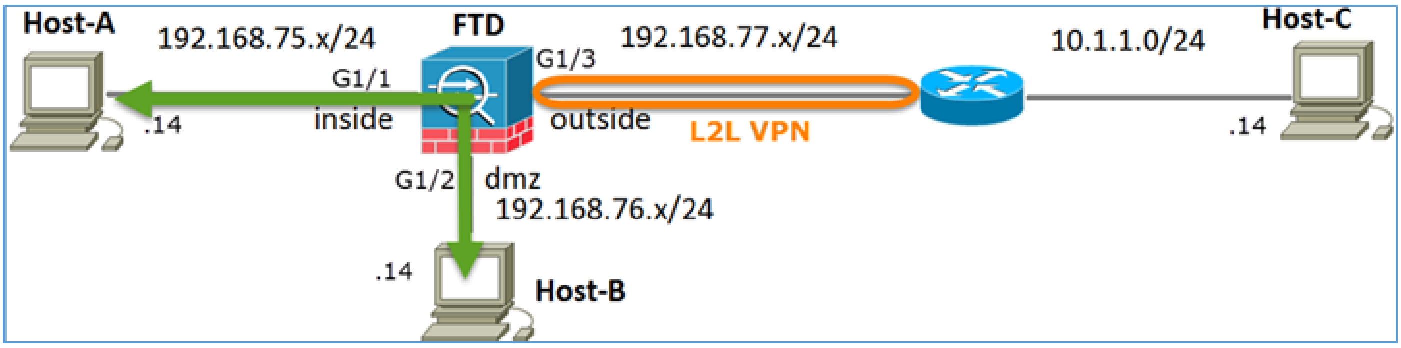
任務1.在FTD上設定靜態NAT

根據以下要求配置NAT：

NAT策略名稱	FTD裝置的名稱
NAT規則	手動NAT規則
NAT型別	靜態
插入	第1部分
源介面	inside*
目標介面	dmz*
原始來源	192.168.75.14

轉換的來源	192.168.76.100

* 對NAT規則使用安全區域



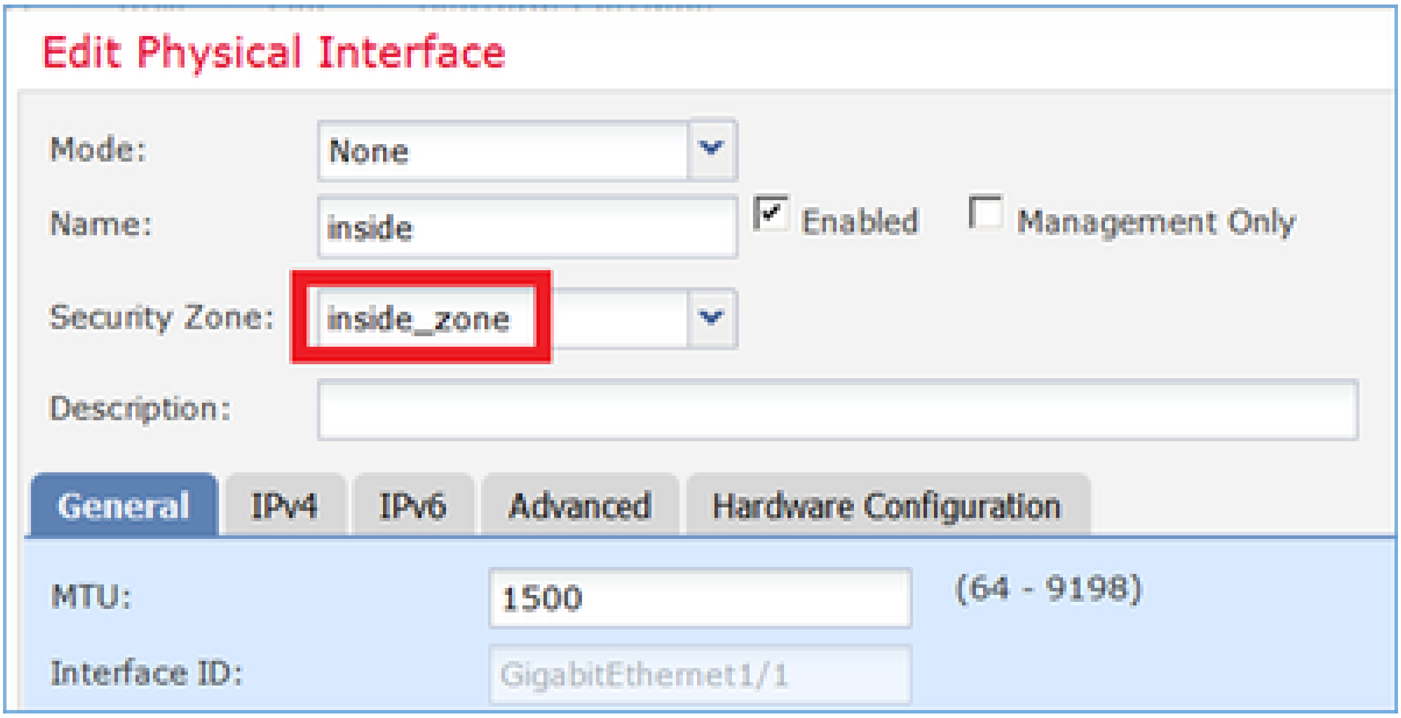
靜態Nat

解決方案：

在傳統ASA上，必須在NAT規則中使用nameif。在FTD上，您需要使用安全區域或介面群組。

步驟 1.將介面分配給安全區域/介面組。

在本任務中，決定將用於NAT的FTD介面分配到安全區域。或者，您可以將其分配到介面組，如圖所示。



Edit Physical Interface

Mode: None

Name: inside ☑ Enabled ☐ Management Only

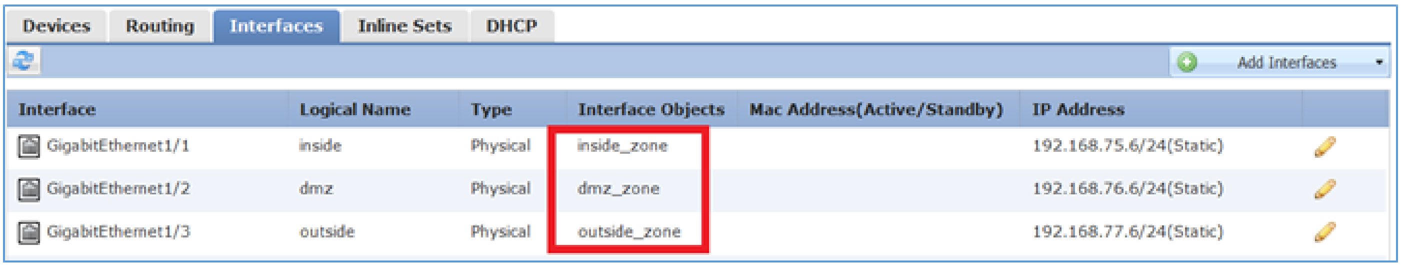
Security Zone: inside_zone

Description:

MTU: 1500 (64 - 9198)

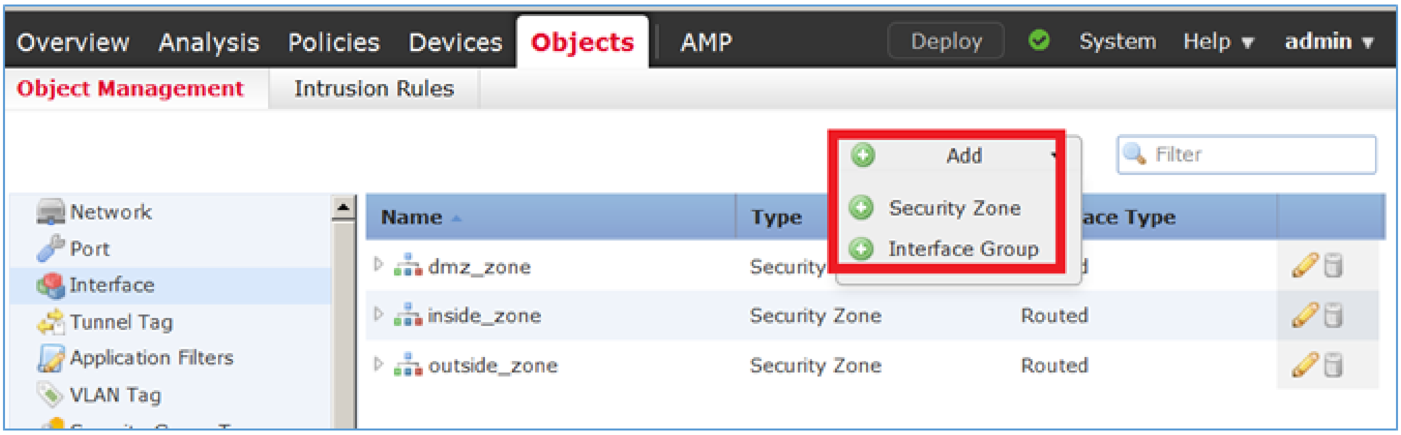
Interface ID: GigabitEthernet1/1

步驟 2.結果如下圖所示。



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)

步驟 3.您可以透過對象>對象管理頁面建立/編輯介面組和安全區域，如下圖所示。

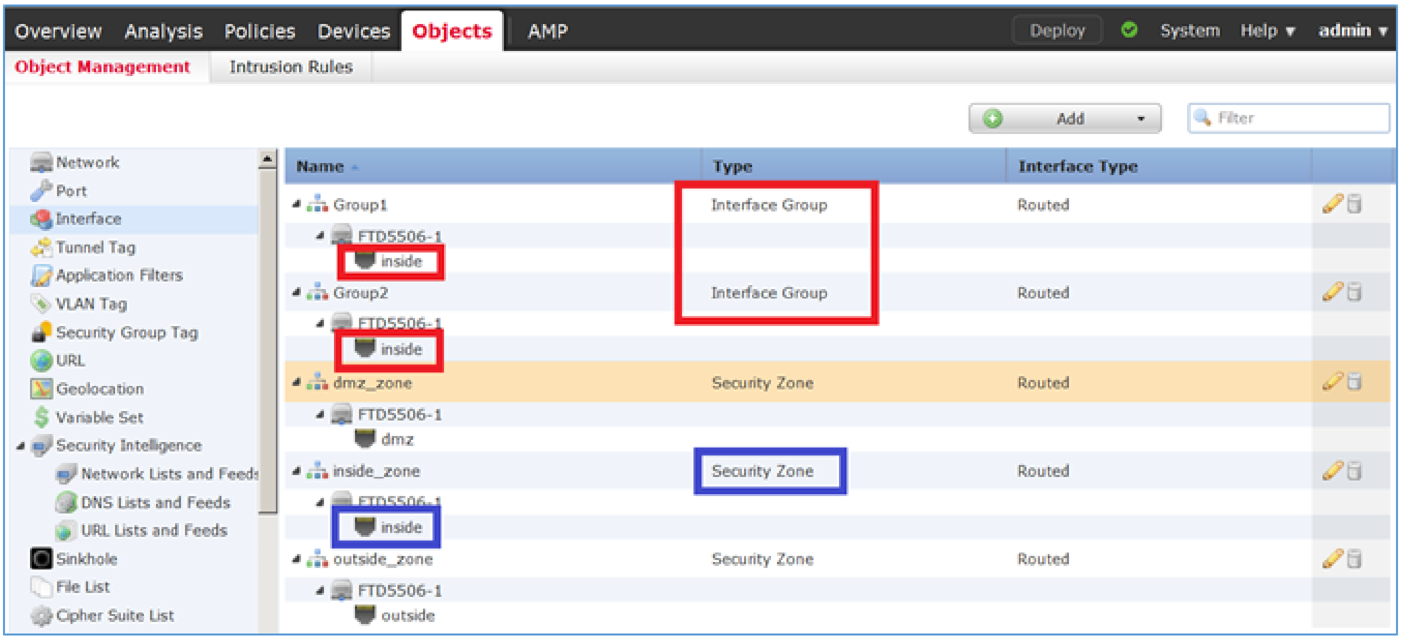


Name	Type	Interface Type
dmz_zone	Security Zone	Routed
inside_zone	Security Zone	Routed
outside_zone	Security Zone	Routed

安全區域與介面組

「安全區域」和「介面組」之間的主要區別在於，一個介面只能屬於一個安全區域，但可以屬於多個介面組。因此，介面組實際上提供了更大的靈活性。

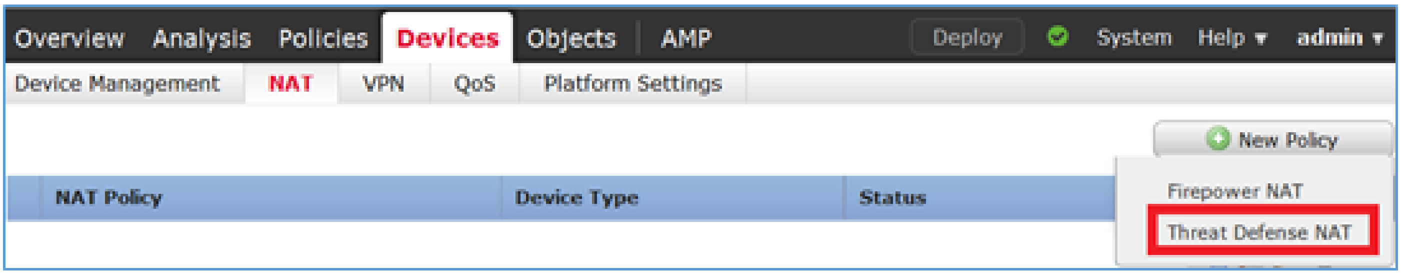
您可以看到內部介面屬於兩個不同的介面組，但只有一個安全區域，如圖所示。



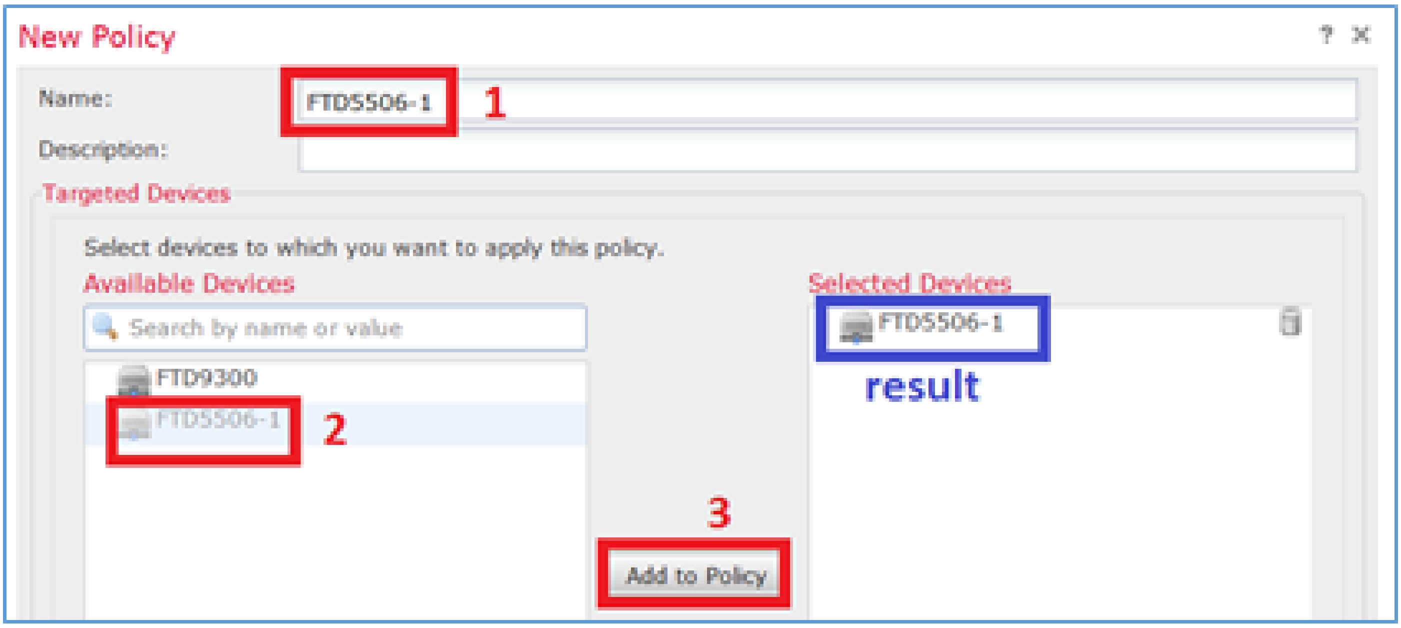
Name	Type	Interface Type
Group1	Interface Group	Routed
FTD5506-1		
inside		
Group2	Interface Group	Routed
FTD5506-1		
inside		
dmz_zone	Security Zone	Routed
FTD5506-1		
dmz		
inside_zone	Security Zone	Routed
FTD5506-1		
inside		
outside_zone	Security Zone	Routed
FTD5506-1		
outside		

步驟 4.在FTD上設定靜態NAT。

導航到裝置> NAT並建立NAT策略。 選擇New Policy > Threat Defense NAT，如圖所示。



步驟 5.指定策略名稱並將其分配給目標裝置，如圖所示。

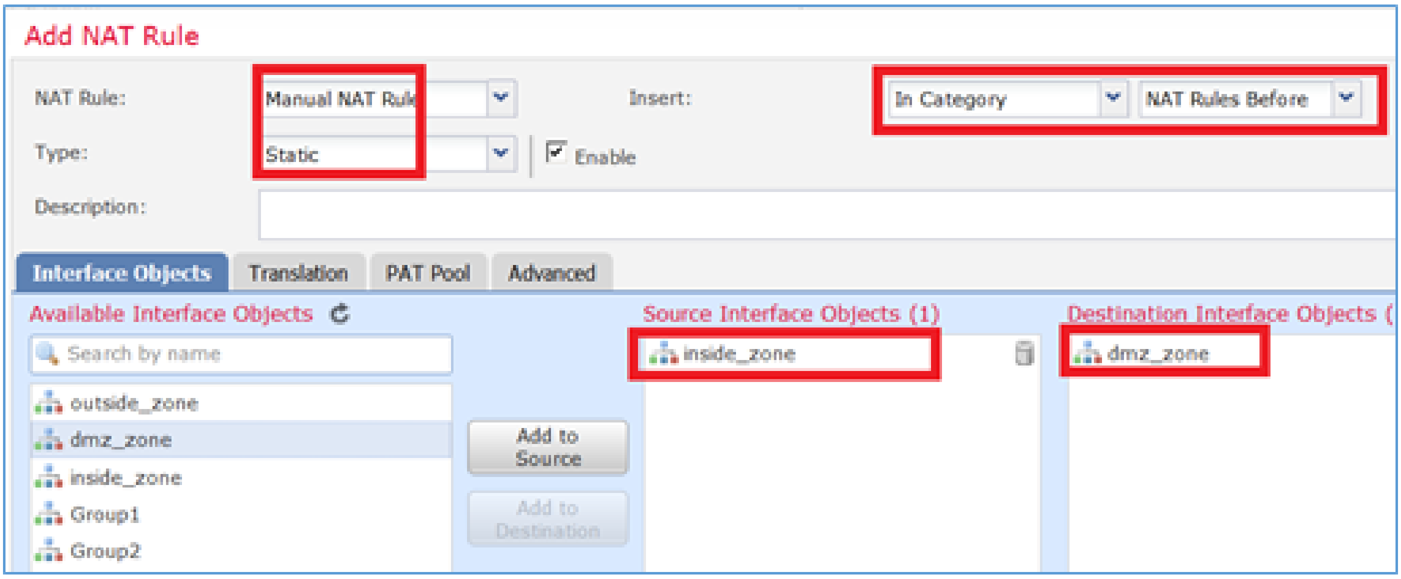


Name: FTD5506-1

Description:

步驟 6.向策略中增加NAT規則，然後按一下Add Rule。

根據任務要求指定這些要求，如圖所示。

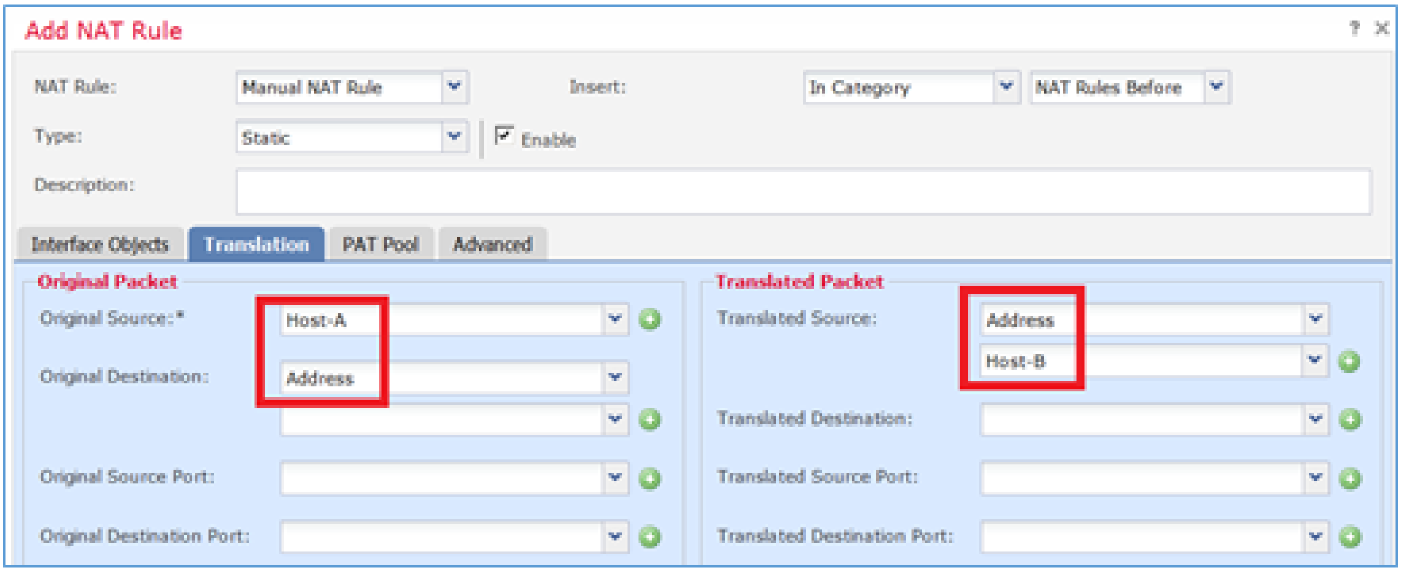


NAT Rule: Manual NAT Rule

Insert: In Category NAT Rules Before

Type: Static ☑ Enable

Description:



Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category | NAT Rules Before

Type: Static

☑ Enable

Description:

Original Packet

Original Source:* Host-A

Original Destination: Address

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source: Address | Host-B

Translated Destination:

Translated Source Port:

Translated Destination Port:

主機A = 192.168.75.14

主機B = 192.168.76.100

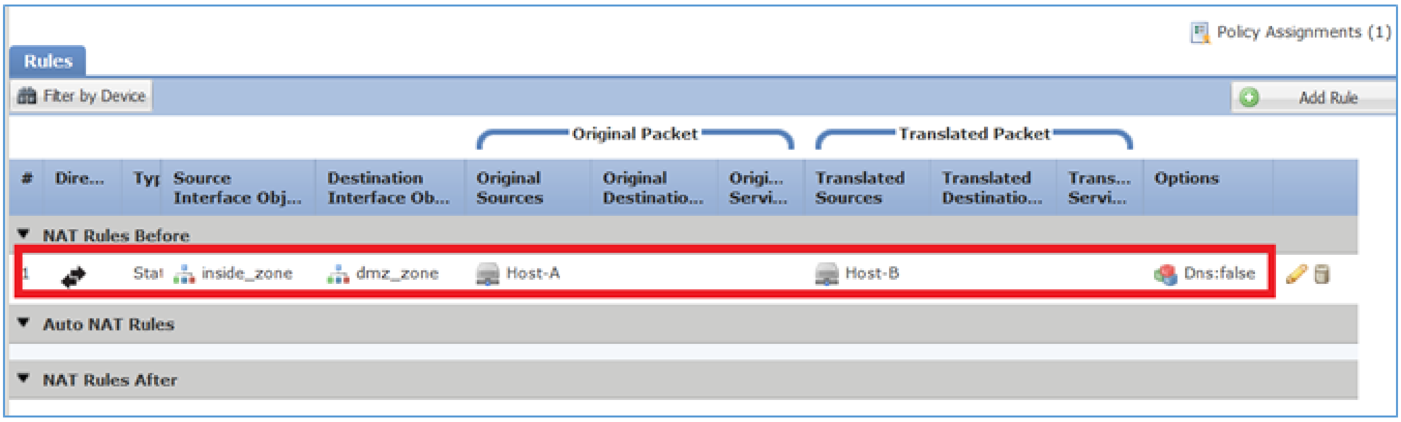
<#root>

```
firepower#
show run object

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

⚠ 警告：如果配置靜態NAT並將某個介面指定為轉換的源，則會重定向發往該介面IP地址的所有流量。使用者無法訪問對映介面上啟用的任何服務。此類服務的示例包括OSPF和EIGRP等路由協定。

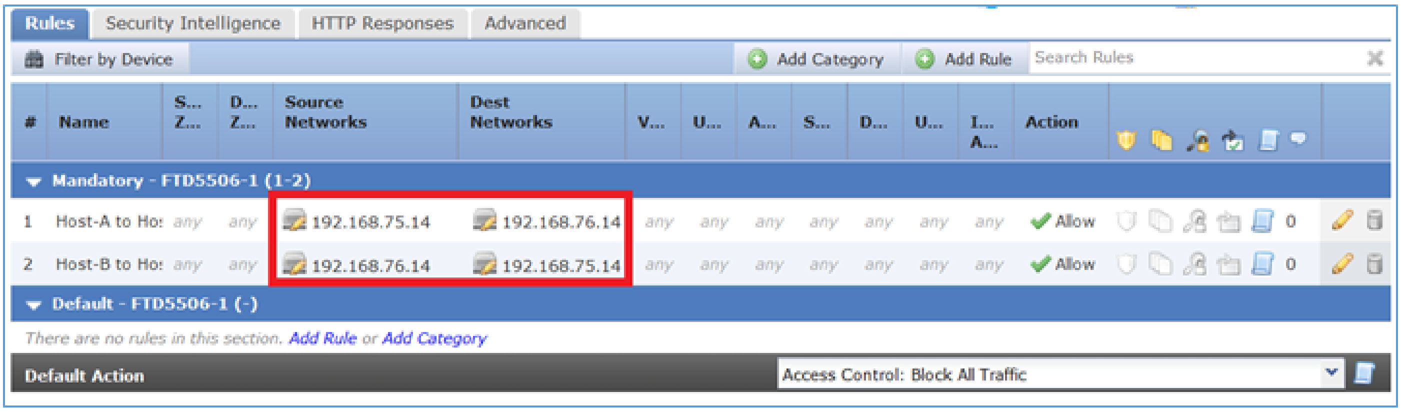
步驟 7.結果如下圖所示。



#	Dire...	Typ	Source Interface Obj...	Destination Interface Ob...	Original Sources	Original Destinatio...	Origi... Servi...	Translated Sources	Translated Destinatio...	Trans... Servi...	Options
▼ NAT Rules Before											
1	⇄	Stat	inside_zone	dmz_zone	Host-A			Host-B			Dns:false
▼ Auto NAT Rules											
▼ NAT Rules After											

步驟 8.確儲存在允許主機B訪問主機A的訪問控制策略，反之亦然。請記住，靜態NAT在預設情況下

是雙向的。與傳統ASA類似，請參閱實際IP的用法。這是預期的，因為在本實驗中，LINA運行9.6.1.x代碼，如圖所示。



#	Name	S... Z...	D... Z...	Source Networks	Dest Networks	V...	U...	A...	S...	D...	U...	I... 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	0
2	Host-B to Ho:	any	any	192.168.76.14	192.168.75.14	any	any	any	any	any	any	any	✓ Allow	0
Default - FTD5506-1 (-)														

There are no rules in this section. Add Rule or Add Category

Default Action | Access Control: Block All Traffic

驗證：

在LINA CLI上：

```
<#root>

firepower#

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

NAT規則已按預期插入到第1部分：

```
<#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
```

附註：在背景中建立的2個xlate。

```
<#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
```

ASP NAT表：

<#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
```

啟用含有FTD上追蹤詳細資訊的擷取，並從主機B ping主機A，如下圖所示。

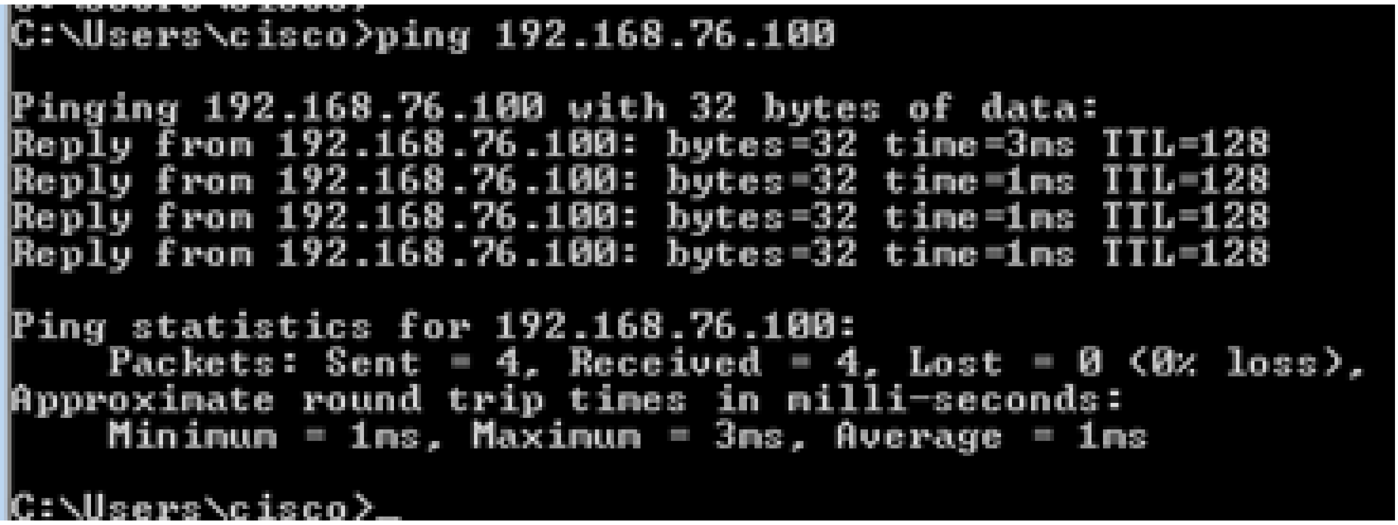
<#root>

```
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>_
```

命中計數在ASP表中：

<#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
```

資料包捕獲顯示：

<#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
```

封包的追蹤（重要點會反白顯示）。

注意：NAT規則的ID及其與ASP表的關聯。

<#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
```

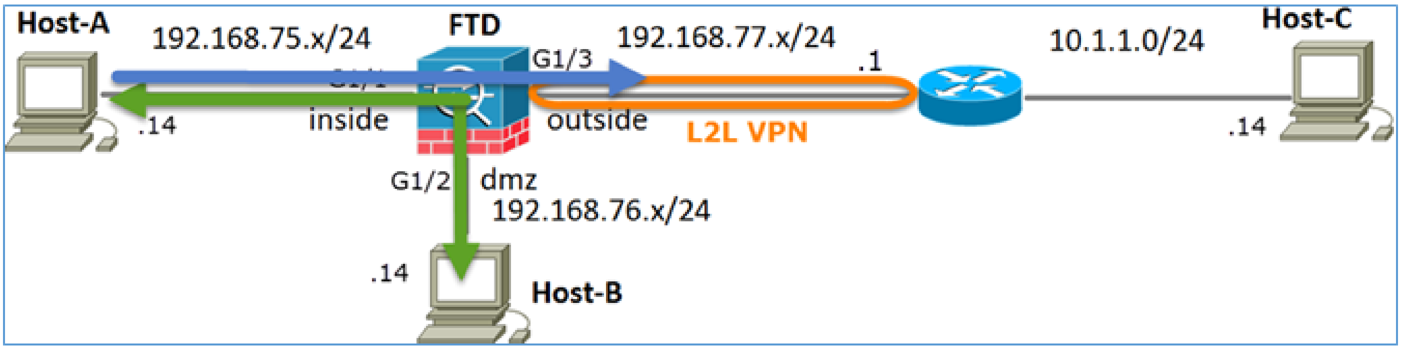
任務2.在FTD上設定連線埠位址翻譯(PAT)

根據以下要求配置NAT：

NAT規則	手動NAT規則
NAT型別	動態
插入	第1部分
源介面	inside*

目標介面	外部*
原始來源	192.168.75.0/24
轉換的來源	外部介面(PAT)

* 對NAT規則使用安全區域

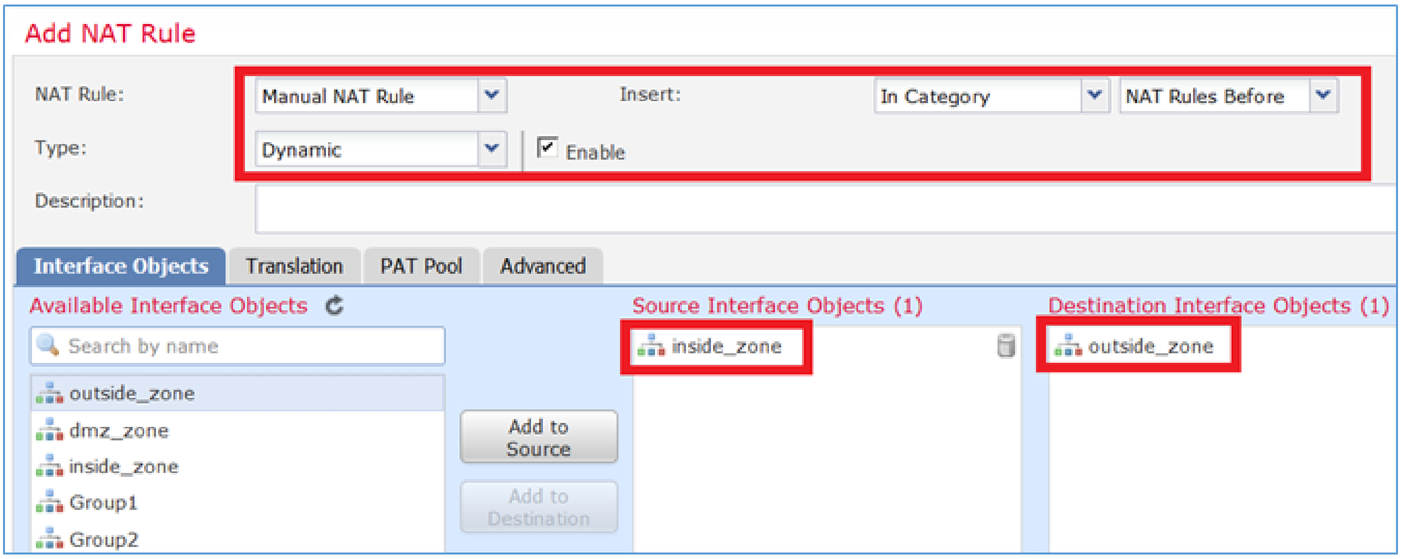


靜態Nat

PAT

解決方案：

步驟 1.增加第二個NAT規則並根據任務要求進行配置，如圖所示。



Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category, NAT Rules Before

Type: Dynamic

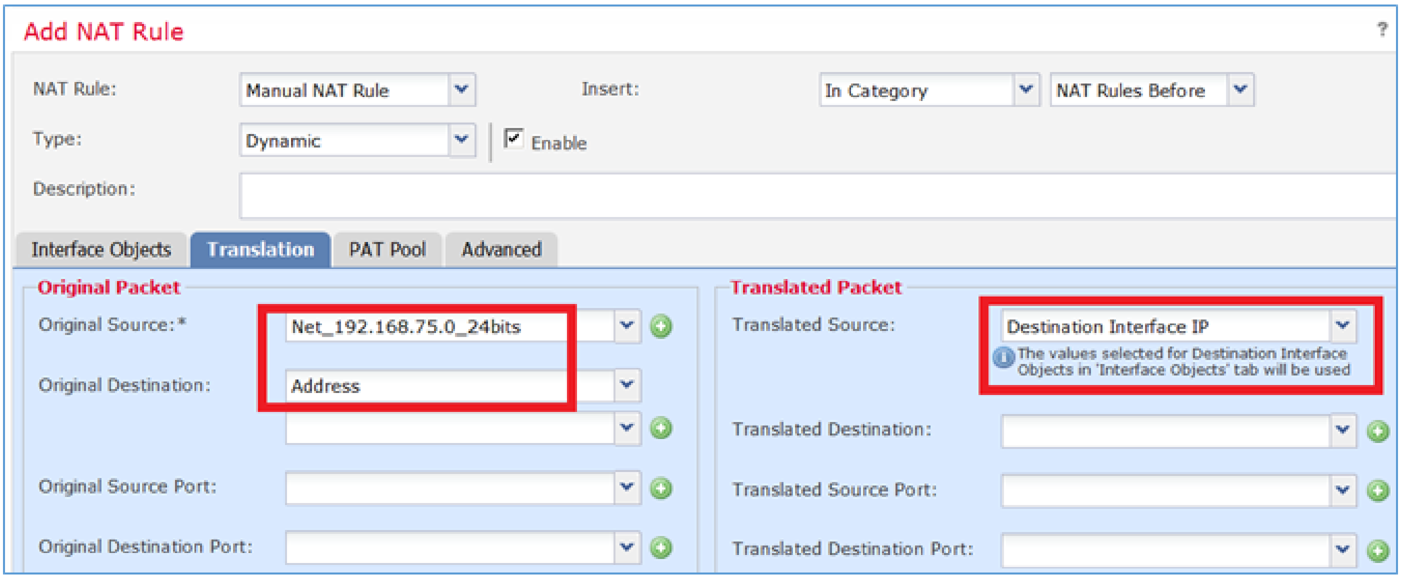
☑ Enable

Description:

Source Interface Objects (1): inside_zone

Destination Interface Objects (1): outside_zone

步驟 2.如下圖所示，PAT是如何配置的。



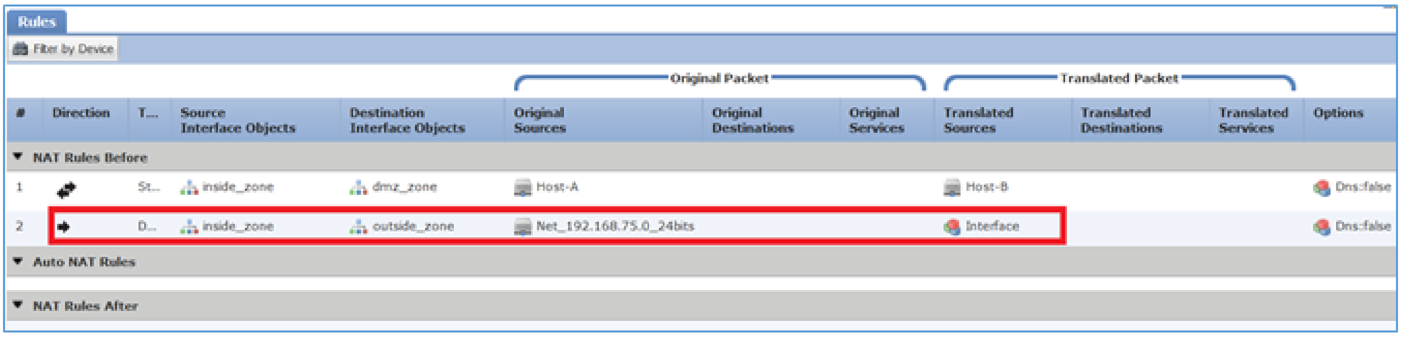
Add NAT Rule

NAT Rule:	Manual NAT Rule	Insert:	In Category / NAT Rules Before
Type:	Dynamic	☑ Enable	
Description:			

Interface Objects | Translation | PAT Pool | Advanced

Original Packet		Translated Packet	
Original Source:*	Net_192.168.75.0_24bits	Translated Source:	Destination Interface IP The values selected for Destination Interface Objects in 'Interface Objects' tab will be used
Original Destination:	Address 	Translated Destination:	
Original Source Port:		Translated Source Port:	
Original Destination Port:		Translated Destination Port:	

步驟 3.結果如下圖所示。



Rules

Filter by Device

					Original Packet			Translated Packet			
#	Direction	T...	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ 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											

步驟 4.在本實驗的其餘部分，配置訪問控制策略以允許所有流量通過。

驗證：

NAT配置：

<#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
```

在LINA CLI中注意新專案：

<#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
```

在內部和外部介面上啟用捕獲。在內部捕獲時，啟用跟蹤：

<#root>

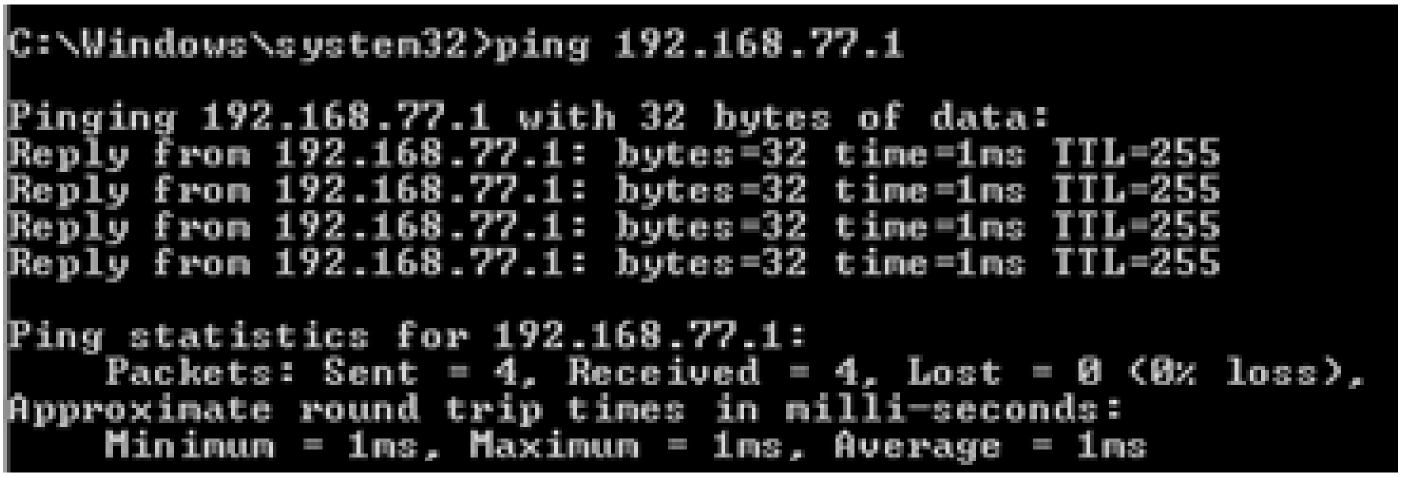
```
firepower#

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
```

從Host-A (192.168.75.14)對IP 192.168.77.1執行ping操作，如下圖所示。



```
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
```

在LINA擷取中，您可以看到PAT翻譯：

<#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
```

突出顯示重要部分的資料包的跟蹤：

<#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
```

動態xlate已建立（請注意ri標誌）：

<#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
```

在LINA記錄中，您會看到：

<#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 outsi

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 192.1
May 31 2016 18:54:43: %ASA-6-302021: Teardown ICMP connection for faddr 192.168.75.14/1 gaddr 192.168.7
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 ou
```

NAT部分：

<#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
```

ASP表格顯示：

<#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
```

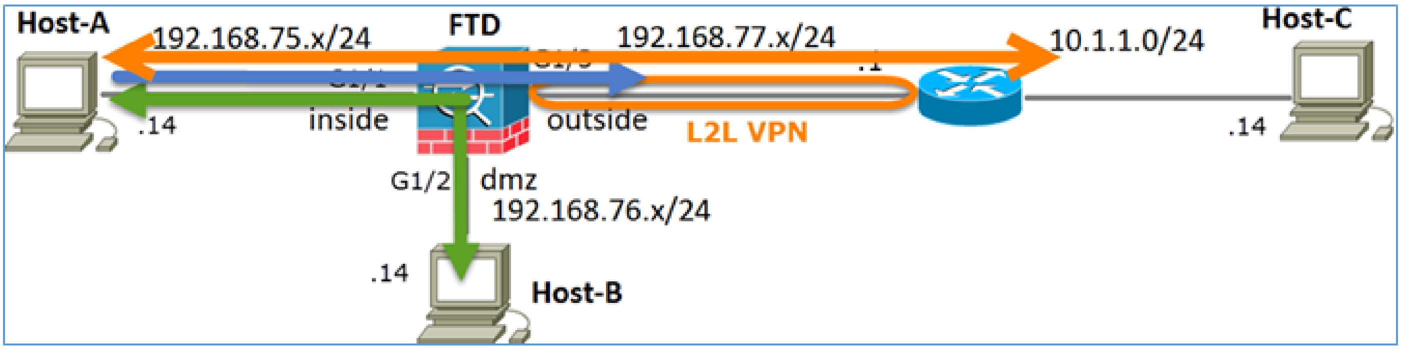
任務3.在FTD上設定NAT豁免

根據以下要求配置NAT：

NAT規則	手動NAT規則
NAT型別	靜態
插入	第1部分中的所有現有規則

源介面	inside*
目標介面	外部*
原始來源	192.168.75.0/24
轉換的來源	192.168.75.0/24
原始目的地	10.1.1.0/24
轉換後的目的地	10.1.1.0/24

* 對NAT規則使用安全區域



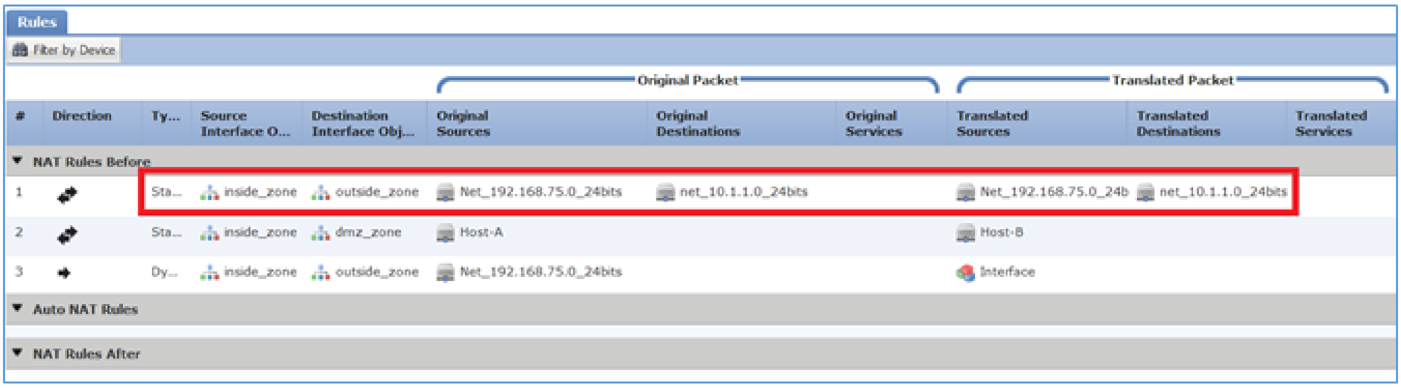
靜態Nat

PAT

NAT免除

解決方案：

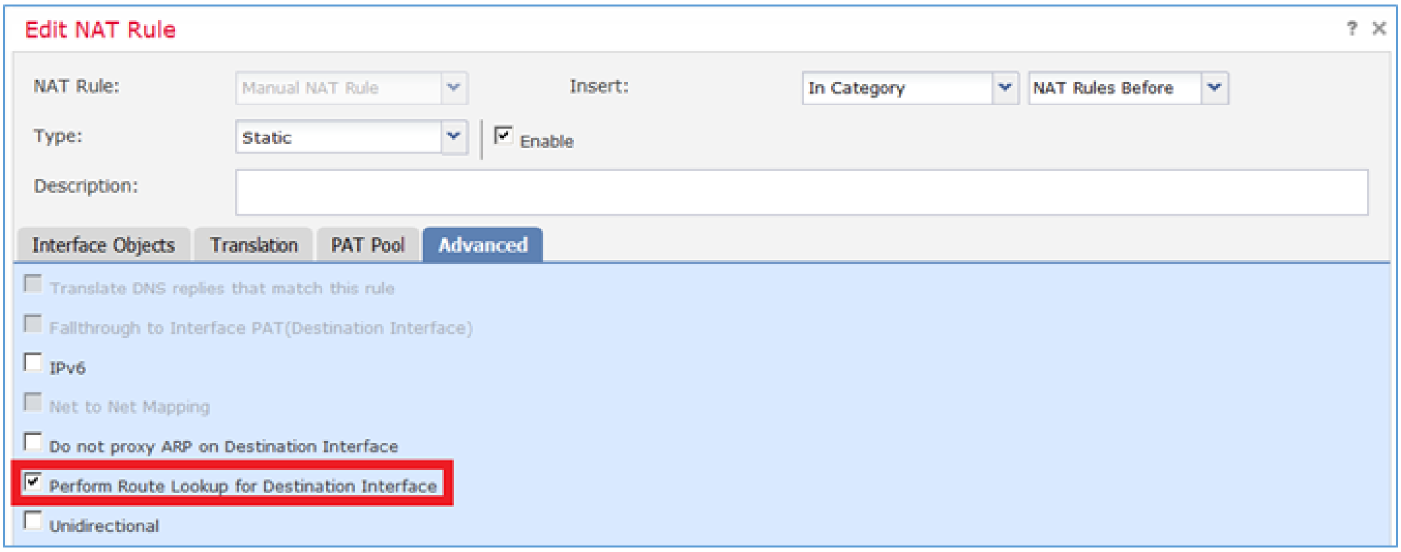
步驟 1.增加第三個NAT規則並根據任務要求進行配置，如圖所示。



					Original Packet			Translated Packet		
#	Direction	Ty...	Source Interface O...	Destination Interface Obj...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services
▼ NAT Rules Before										
1	⇄	Sta...	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	⇄	Sta...	inside_zone	dmz_zone	Host-A			Host-B		
3	→	Dy...	inside_zone	outside_zone	Net_192.168.75.0_24bits			Interface		
▼ Auto NAT Rules										
▼ NAT Rules After										

步驟 2.執行路由查詢以確定出口介面。

注意：對於身份NAT規則（如您增加的規則），您可以更改輸出介面的確定方式並使用常規路由查詢（如圖所示）。



Edit NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category / NAT Rules Before

Type: Static

☑ Enable

Description:

□ 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

驗證：

```
<#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 stati
    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
```

對源自內部網路的非VPN流量運行Packet Tracer。PAT規則按預期使用：

<#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
```

對必須透過VPN隧道的流量運行Packet Tracer（由於第一次嘗試會開啟VPN隧道，請運行兩次）。

註：您必須選擇NAT免除規則。

第一次Packet Tracer嘗試：

<#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
```

第二次Packet Tracer嘗試：

<#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: 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命中計數驗證：

<#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
```

任務4.在FTD上設定物件NAT

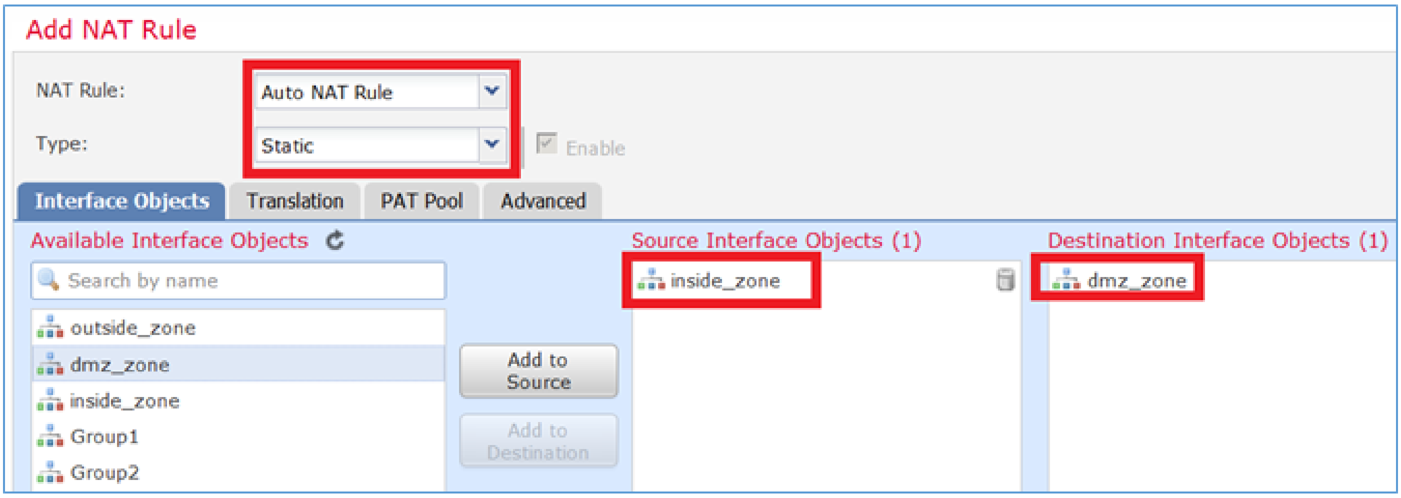
根據以下要求配置NAT：

NAT規則	自動NAT規則
NAT型別	靜態
插入	第2部分
源介面	inside*
目標介面	dmz*
原始來源	192.168.75.99
轉換的來源	192.168.76.99
轉換與此規則匹配的DNS應答	已啟用

* 對NAT規則使用安全區域

解決方案：

步驟 1.根據任務要求配置規則，如圖所示。



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static

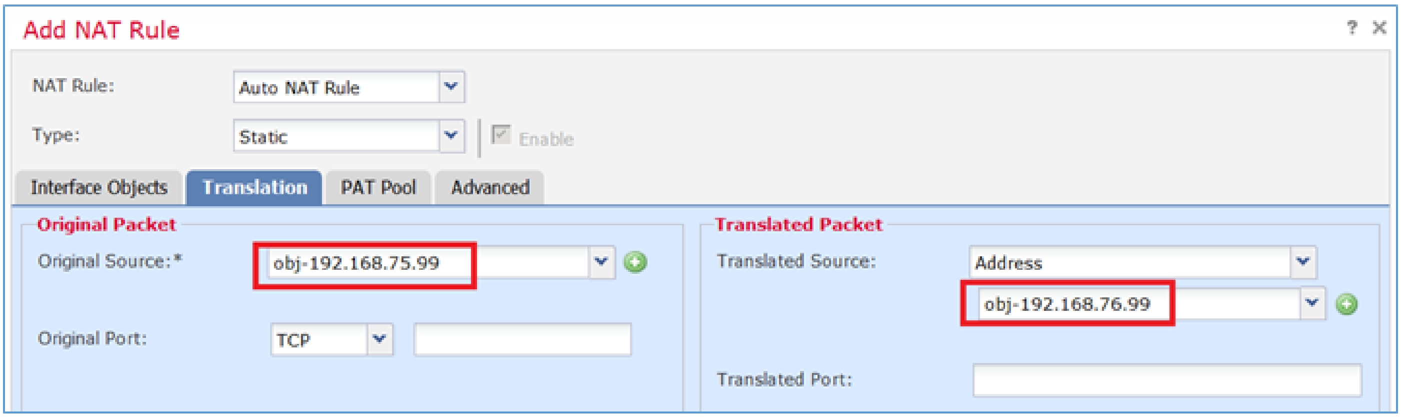
☑ Enable

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

NAT Rule: Auto NAT Rule

Type: Static

☑ Enable

Original Packet

Original Source:* obj-192.168.75.99

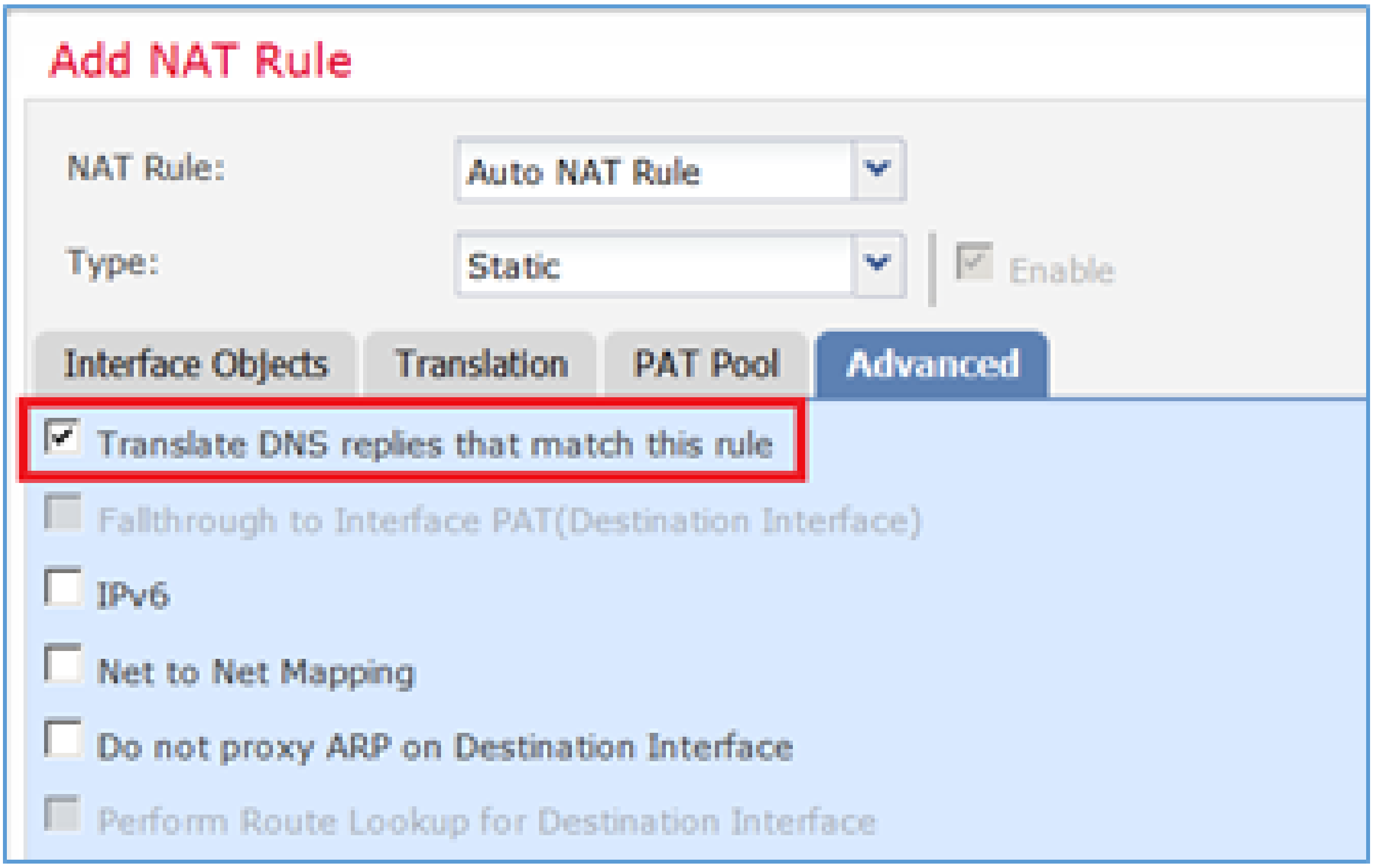
Original Port: TCP

Translated Packet

Translated Source: Address

obj-192.168.76.99

Translated Port:



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static

☑ Enable

☑ Translate DNS replies that match this rule

□ Fallthrough to Interface PAT(Destination Interface)

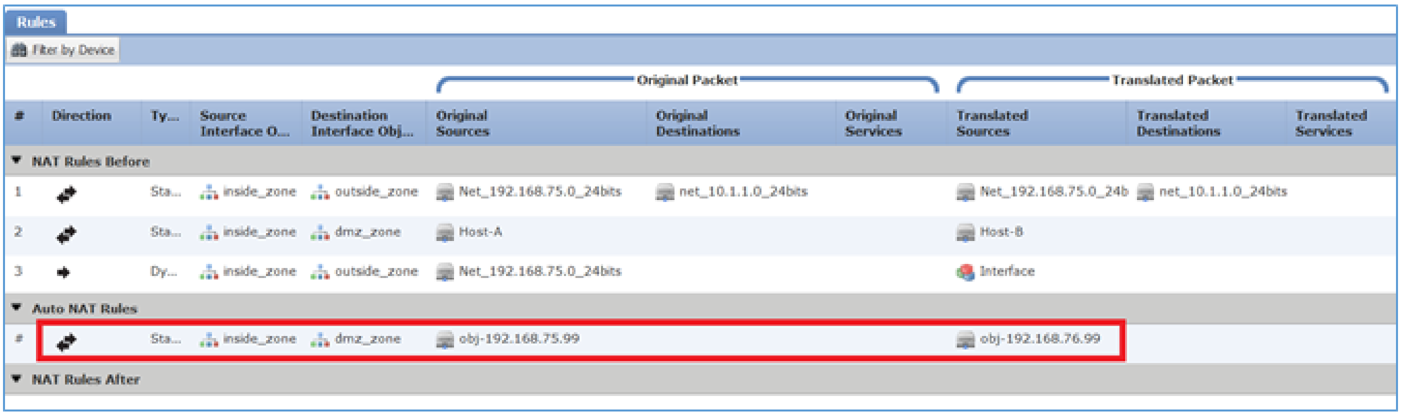
□ IPv6

□ Net to Net Mapping

□ Do not proxy ARP on Destination Interface

□ Perform Route Lookup for Destination Interface

步驟 2.結果如下圖所示。



					Original Packet			Translated Packet		
#	Direction	Ty...	Source Interface O...	Destination Interface Obj...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services
▼ NAT Rules Before										
1	⇄	Sta...	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	⇄	Sta...	inside_zone	dmz_zone	Host-A			Host-B		
3	→	Dy...	inside_zone	outside_zone	Net_192.168.75.0_24bits			Interface		
▼ Auto NAT Rules										
#	⇄	Sta...	inside_zone	dmz_zone	obj-192.168.75.99			obj-192.168.76.99		
▼ NAT Rules After										

驗證：

<#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 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 = 0, untranslate_hits = 0
```

使用Packet Tracer進行驗證：

<#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
```

任務5.在FTD上設定PAT池

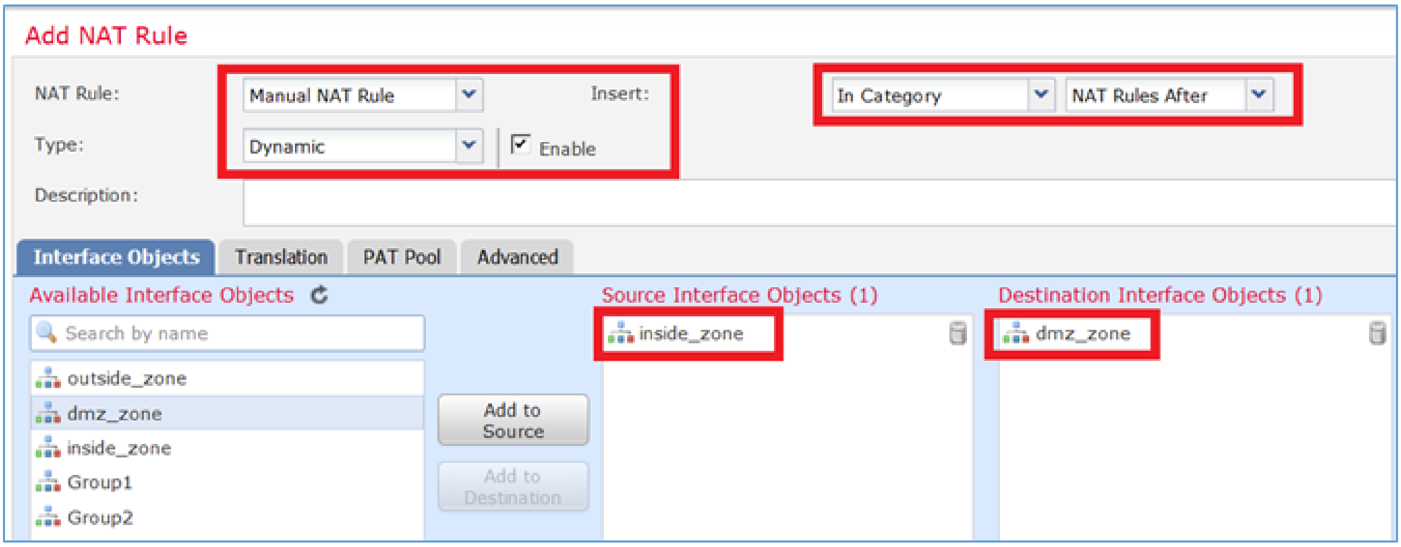
根據以下要求配置NAT：

NAT規則	手動NAT規則
NAT型別	動態
插入	第3部分
源介面	inside*
目標介面	dmz*
原始來源	192.168.75.0/24
轉換的來源	192.168.76.20-22
使用整個範圍(1-65535)	已啟用

* 對NAT規則使用安全區域

解決方案：

步驟 1.根據任務要求配置規則，如圖所示。



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

Search by name

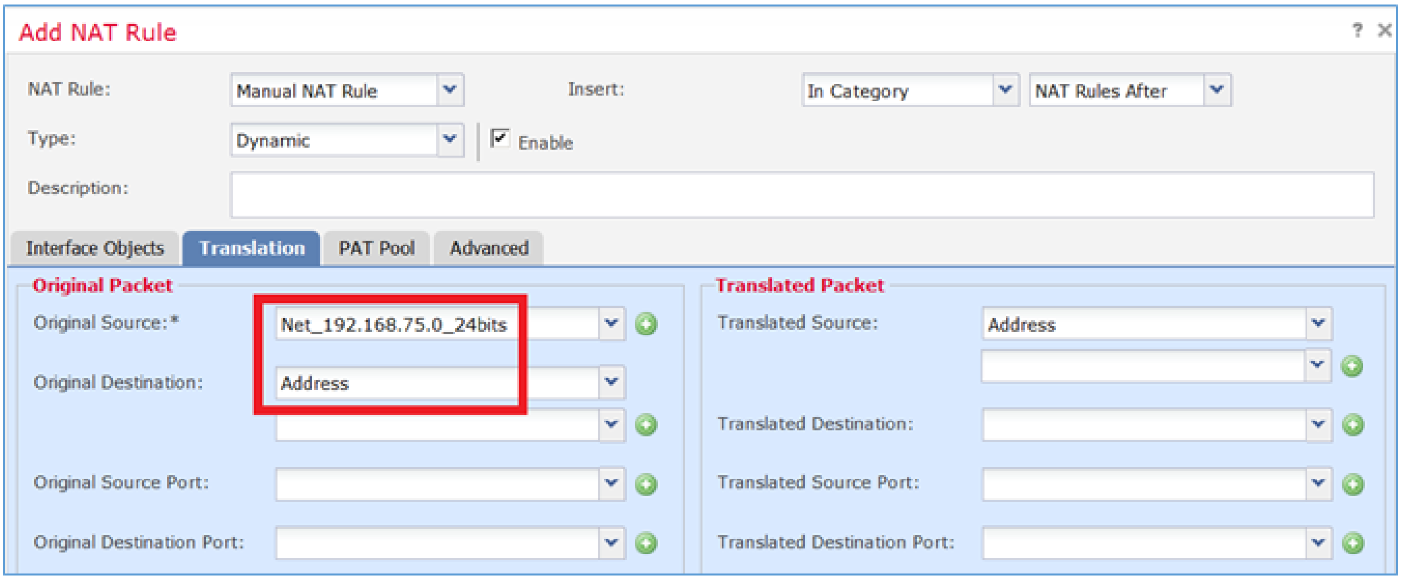
- outside_zone
- dmz_zone
- inside_zone
- Group1
- Group2

Source Interface Objects (1)

- inside_zone

Destination Interface Objects (1)

- dmz_zone



Add NAT Rule

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

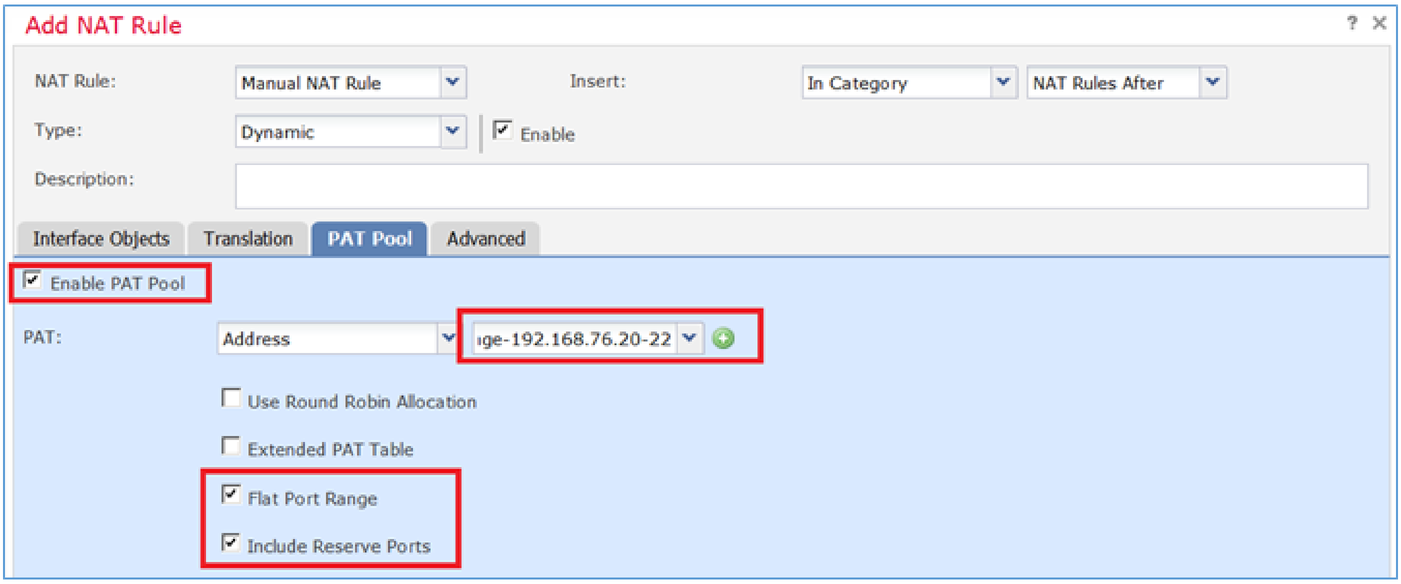
Translated Source: Address

Translated Destination:

Translated Source Port:

Translated Destination Port:

步驟 2.啟用平坦埠範圍和包括預留埠，允許使用整個範圍(1-65535)，如圖所示。



Add NAT Rule

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, ıge-192.168.76.20-22

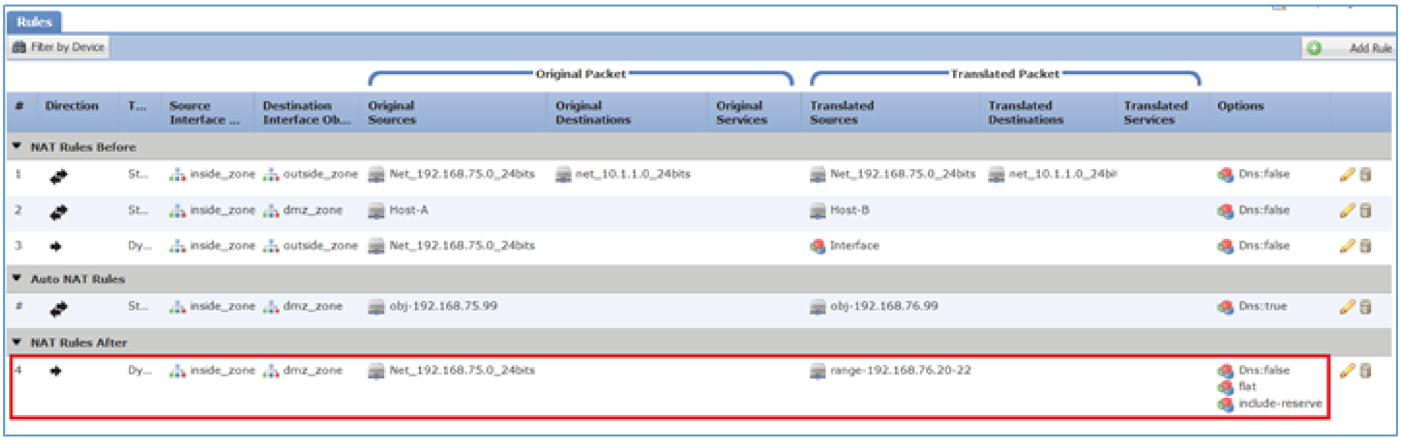
☐ Use Round Robin Allocation

☐ Extended PAT Table

☑ Flat Port Range

☑ Include Reserve Ports

步驟 3.結果如下圖所示。



Rules

Filter by Device

Add Rule

#	Direction	T...	Source Interface ...	Destination Interface Ob...	Original Packet Original Sources	 Original Destinations	 Original Services	Translated Packet Translated Sources	 Translated Destinations	 Translated Services	Options
▼ 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

驗證：

<#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
```

規則在第3部分：

<#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驗證：

<#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
```

驗證

使用本節內容，確認您的組態是否正常運作。

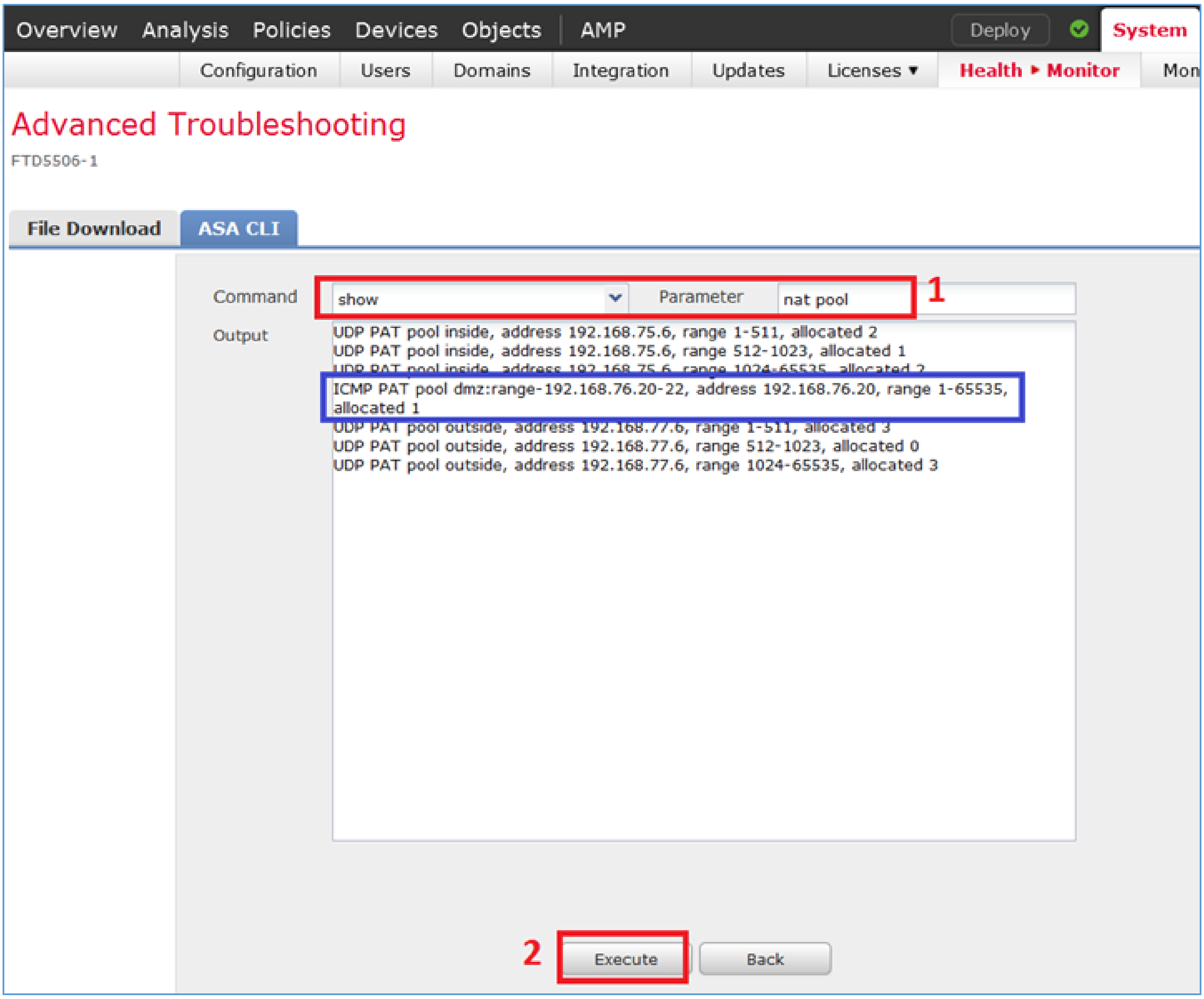
驗證已在個別任務小節中說明。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

打開FMC上的高級故障排除頁，運行Packet Tracer，然後運行show nat pool命令。

附註：使用整個範圍的專案，如下圖所示。



Advanced Troubleshooting

FTD5506-1

1 Command: show Parameter: nat pool

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 Execute

相關資訊

- 所有版本的Cisco Firepower Management Center配置指南都可以在以下位置找到：

導航思科安全防火牆威脅防禦文檔

- 思科全球技術支援中心(TAC)強烈建議使用本視覺指南，以獲得有關Cisco Firepower下一代安全技術的深入實踐知識，其中包括本文中提到的內容：

Cisco新聞- Firepower威脅防禦

- 有關Firepower技術的所有配置和故障排除技術說明：

Cisco安全防火牆管理中心

- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。