FTD에서 NAT 구성 및 확인

목차

소개

이 문서에서는 FTD(Firepower Threat Defense)에서 기본 NAT(Network Address Translation)를 구성하고 확인하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FTD 코드 6.1.0-226을 실행하는 ASA5506X
- 6.1.0-226을 실행하는 FMC(FireSIGHT Management Center)
- Windows 7 호스트 3개
- L2L(LAN-to-LAN) VPN을 실행하는 Cisco IOS® 3925 라우터

실습 완료 시간: 1시간

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

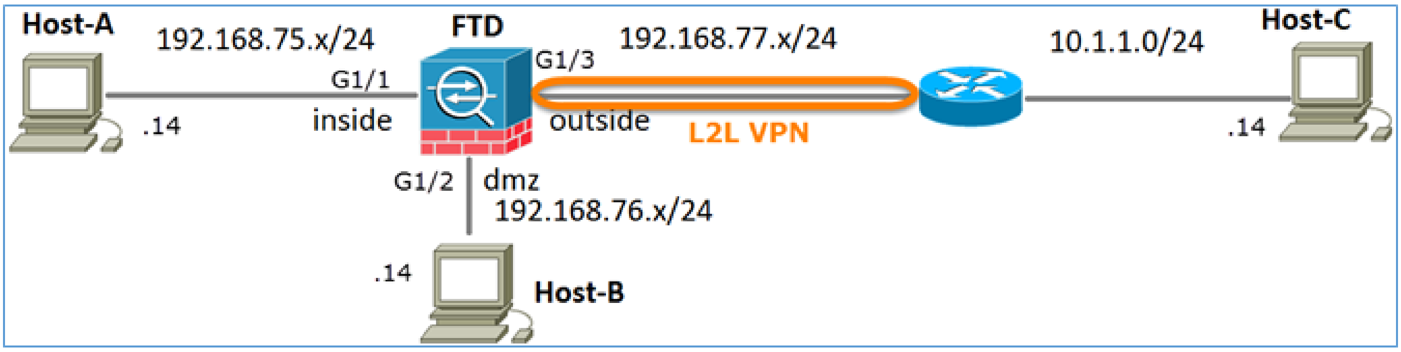
FTD는 기존 ASA(Adaptive Security Appliance)와 동일한 NAT 컨피그레이션 옵션을 지원합니다.

- NAT Rules Before(이전 NAT 규칙) - 기존 ASA의 Twice NAT(섹션 1)와 동일합니다.
- 자동 NAT 규칙 - 기존 ASA의 섹션 2
- NAT Rules After - 기존 ASA의 Twice NAT(섹션 3)와 동일합니다.

FTD 컨피그레이션은 NAT 컨피그레이션에 대해 FMC에서 수행되므로 FMC GUI 및 다양한 컨피그레이션 옵션을 숙지해야 합니다.

구성

네트워크 다이어그램



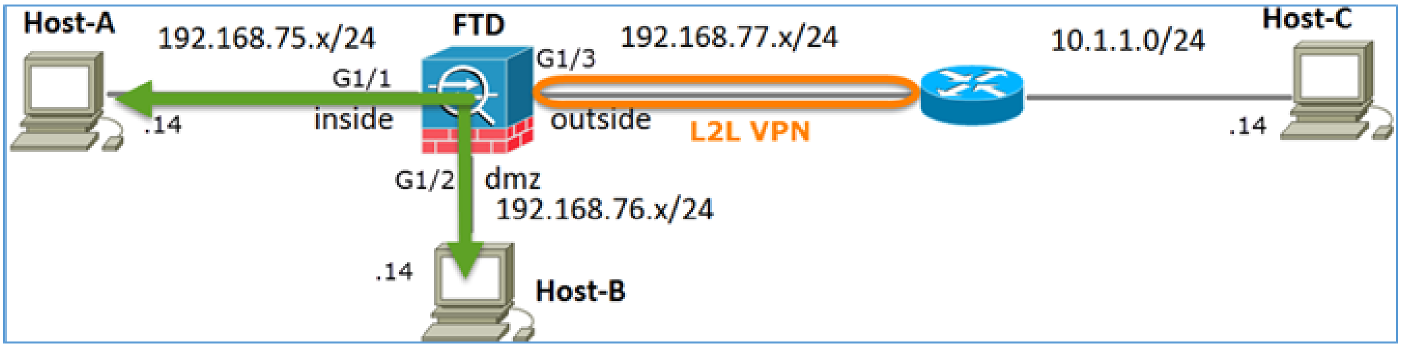
작업 1. FTD에서 고정 NAT 구성

다음 요구 사항에 따라 NAT를 구성합니다.

NAT 정책 이름	FTD 디바이스의 이름
NAT 규칙	수동 NAT 규칙
NAT 유형	고정
삽입	섹션 1
소스 인터페이스	내부*

대상 인터페이스	DMZ*
원본	192.168.75.14
변환된 소스	192.168.76.100

*NAT 규칙에 보안 영역 사용



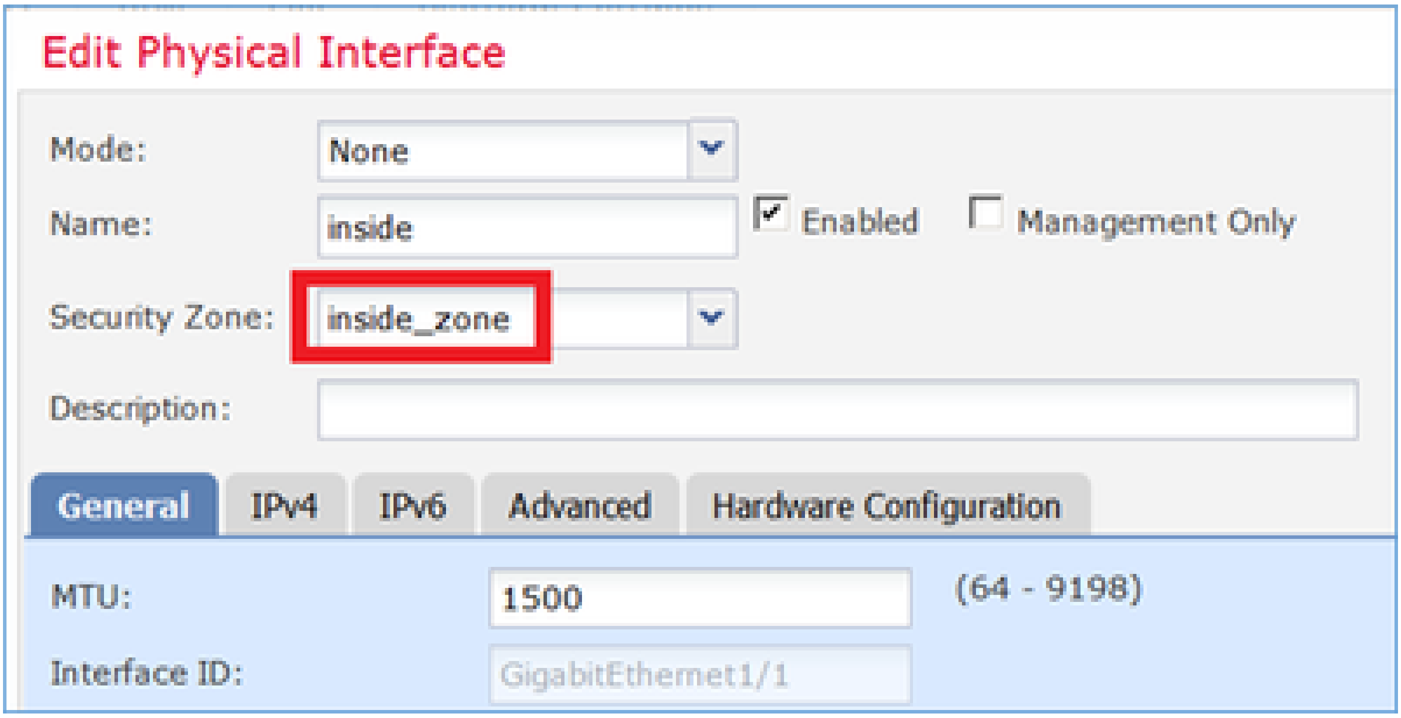
고정 NAT

해결책:

기존 ASA에서는 NAT 규칙에서 nameif를 사용해야 합니다. FTD에서는 보안 영역 또는 인터페이스 그룹을 사용해야 합니다.

1단계. 보안 영역/인터페이스 그룹에 인터페이스를 할당합니다.

이 작업에서는 NAT에 사용되는 FTD 인터페이스를 보안 영역에 할당하기로 결정합니다. 또는 이미지에 표시된 대로 인터페이스 그룹에 지정할 수 있습니다.



Edit Physical Interface

Mode: None

Name: inside ☑ Enabled □ Management Only

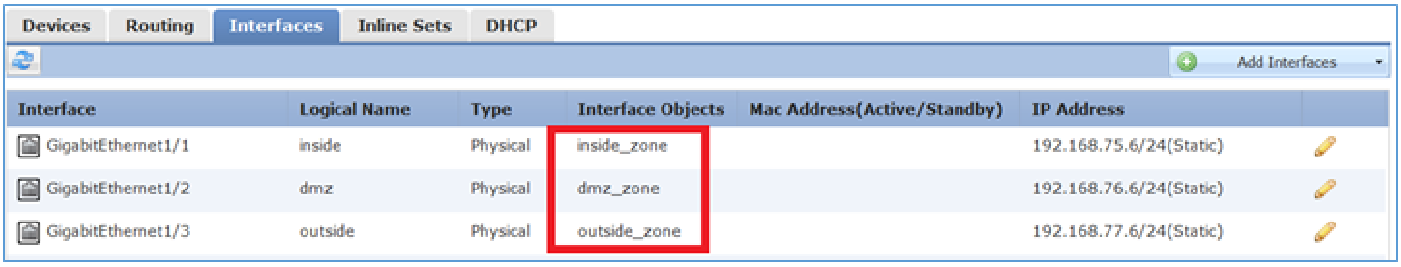
Security Zone: inside_zone

Description:

MTU: 1500 (64 - 9198)

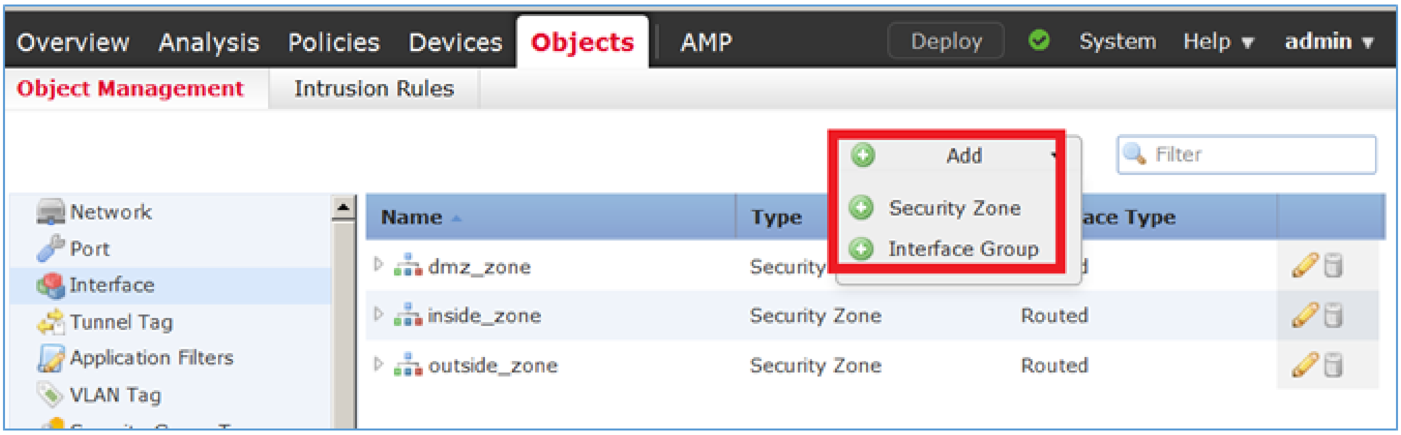
Interface ID: GigabitEthernet1/1

2단계. 결과는 이미지에 표시된 것과 같습니다.



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)

3단계. 이미지에 표시된 대로 Objects(개체) > Object Management(개체 관리) 페이지에서 Interface Groups and Security Zones(인터페이스 그룹 및 보안 영역)를 생성/수정할 수 있습니다.

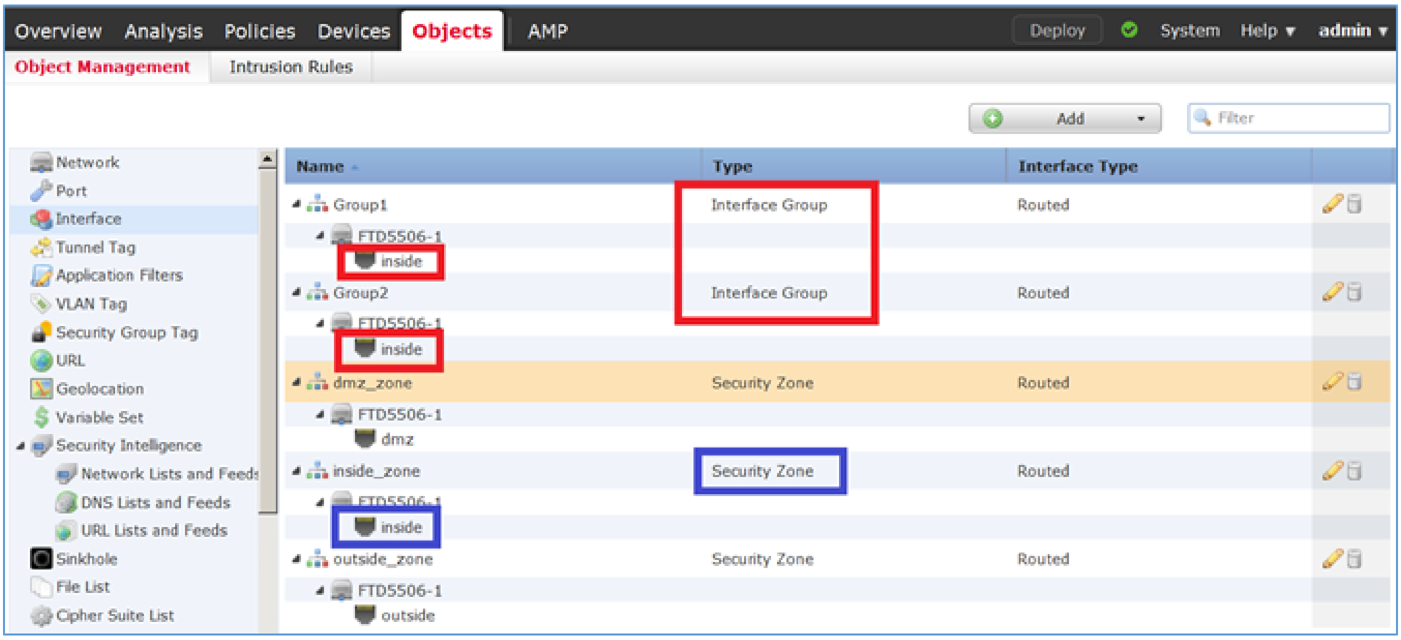


Name	Type	Interface Type
dmz_zone	Security Zone	Routed
inside_zone	Security Zone	Routed
outside_zone	Security Zone	Routed

보안 영역 대 인터페이스 그룹

보안 영역과 인터페이스 그룹의 주요 차이점은 인터페이스가 하나의 보안 영역에만 속할 수 있지만 여러 인터페이스 그룹에 속할 수 있다는 것입니다. 실제로 인터페이스 그룹은 더 많은 유연성을 제공합니다.

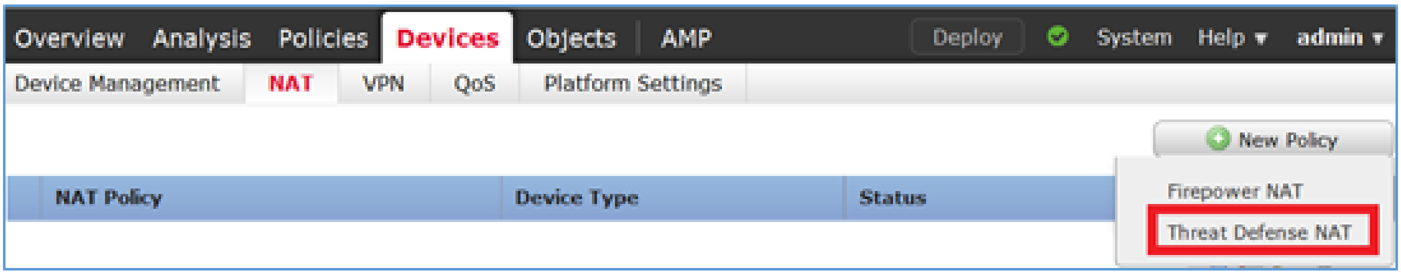
내부 인터페이스가 두 개의 서로 다른 인터페이스 그룹에 속하지만 그림과 같이 하나의 보안 영역에만 속하는 것을 볼 수 있습니다.



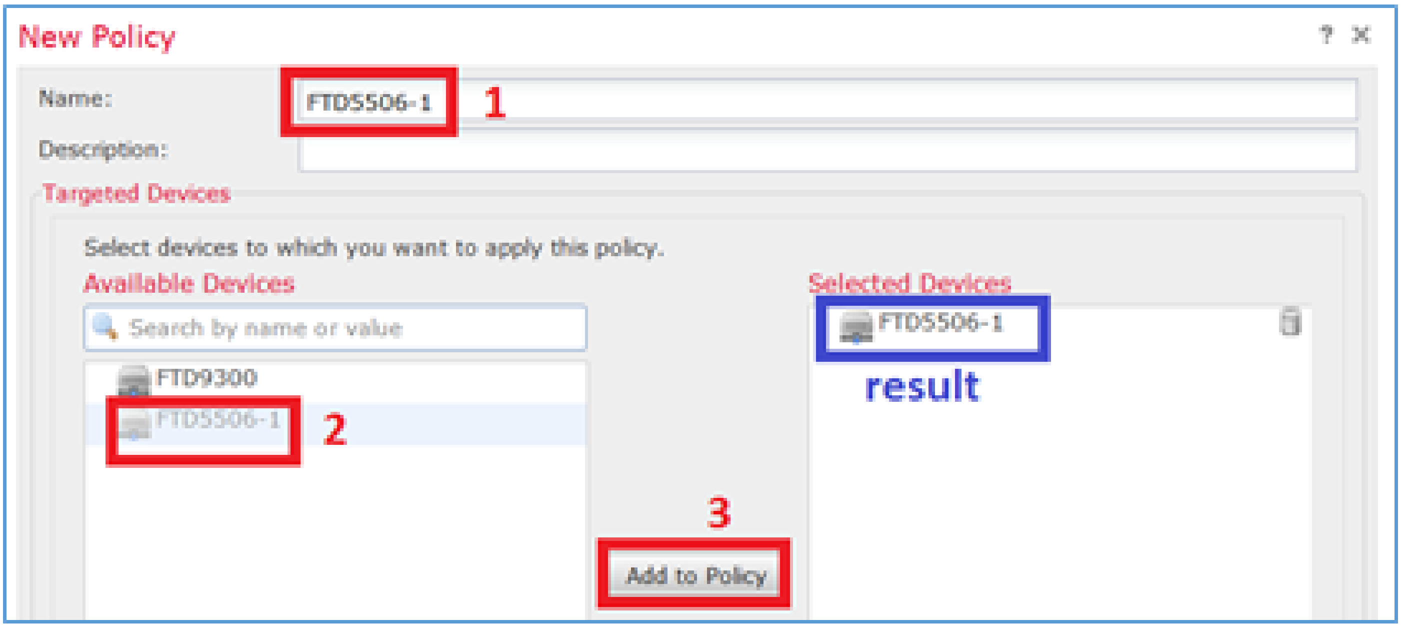
Name	Type	Interface Type
Group1	Interface Group	Routed
FTD5506-1		
inside		
Group2	Interface Group	Routed
FTD5506-1		
inside		
dmz_zone	Security Zone	Routed
FTD5506-1		
dmz		
inside_zone	Security Zone	Routed
FTD5506-1		
inside		
outside_zone	Security Zone	Routed
FTD5506-1		
outside		

4단계. FTD에서 고정 NAT를 구성합니다.

Devices(디바이스) > NAT로 이동하여 NAT 정책을 생성합니다. 이미지에 표시된 대로 New Policy(새 정책) > Threat Defense NAT를 선택합니다.



5단계. 이미지에 표시된 대로 정책 이름을 지정하고 대상 디바이스에 할당합니다.


New Policy

Name: FTD5506-1

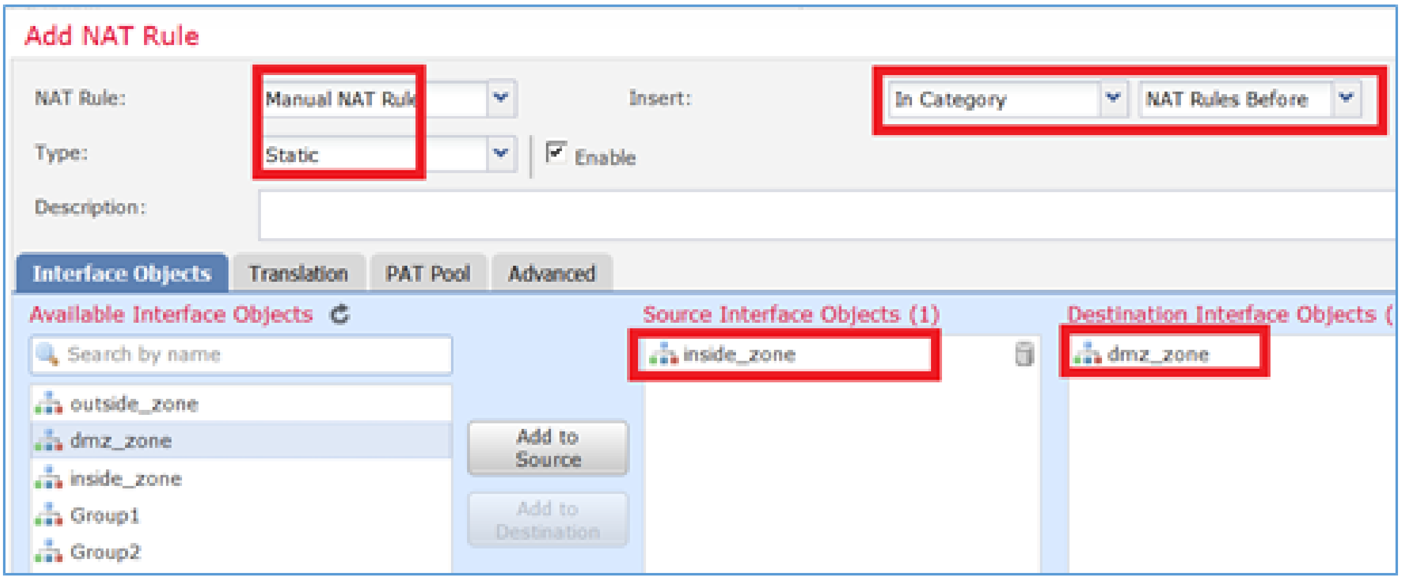
Description:

Targeted Devices

Select devices to which you want to apply this policy.

6단계. NAT 규칙을 정책에 추가하고 Add Rule을 클릭합니다.

이미지에 표시된 대로 작업 요구 사항에 따라 이를 지정합니다.


Add NAT Rule

NAT Rule: Manual NAT Rule

Type: Static

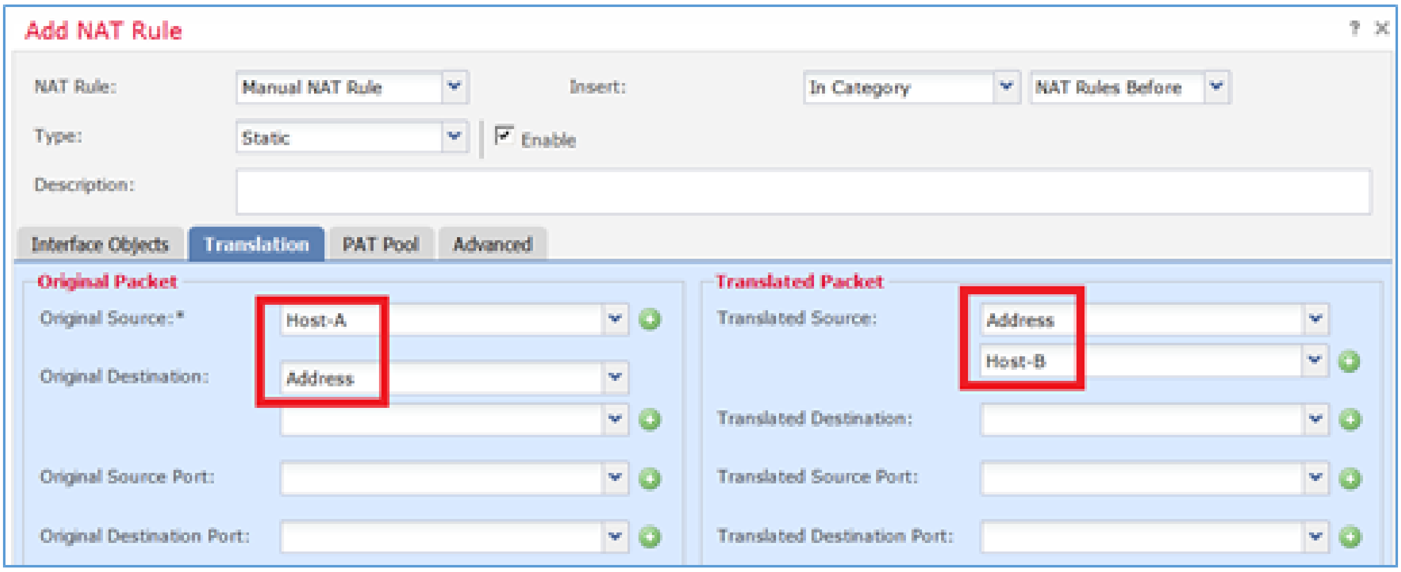
☑ Enable

Insert: In Category | NAT Rules Before

Description:

Source Interface Objects (1): inside_zone

Destination Interface Objects (: dmz_zone



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:

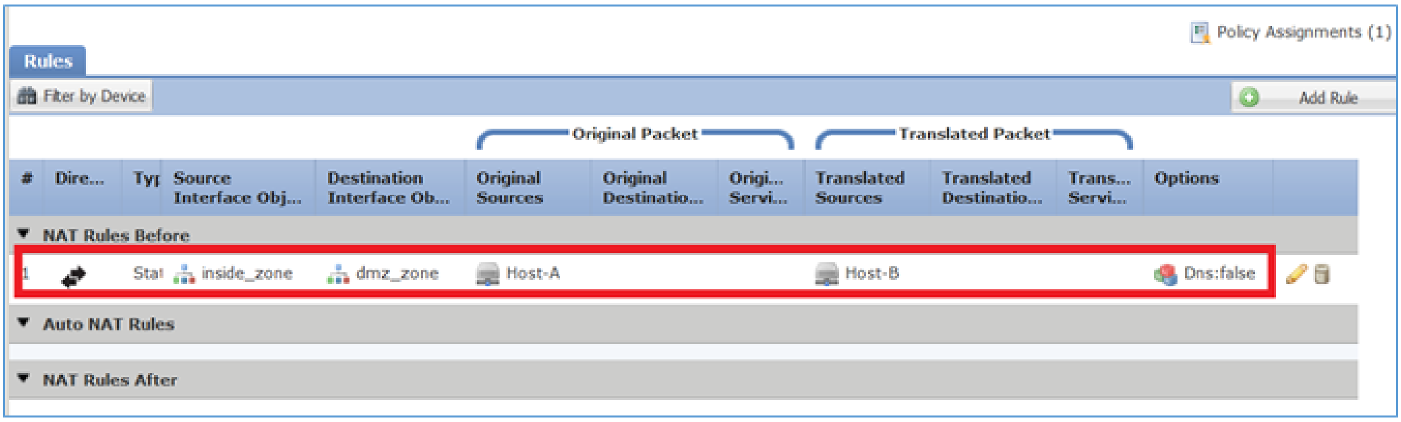
Host-A = 192.168.75.14

호스트 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
```

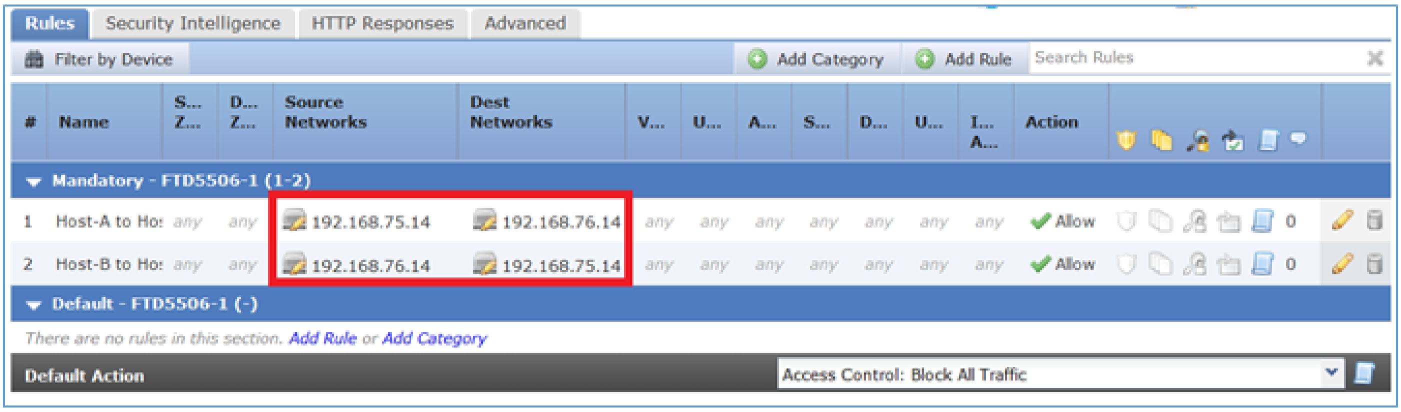
경고: Static NAT를 구성하고 인터페이스를 Translated Source로 지정하면 인터페이스의 IP 주소로 향하는 모든 트래픽이 리디렉션됩니다. 사용자는 매핑된 인터페이스에서 활성화된 서비스에 액세스할 수 없습니다. 이러한 서비스의 예로는 OSPF 및 EIGRP와 같은 라우팅 프로토콜이 있습니다.

7단계. 결과는 이미지에 표시된 것과 같습니다.



					Original Packet			Translated Packet			
#	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											

8단계. Host-B가 Host-A에 액세스하거나 Host-B가 Host-A에 액세스하도록 허용하는 액세스 제어 정책이 있는지 확인합니다. 고정 NAT는 기본적으로 양방향입니다. 기존 ASA와 마찬가지로 실제 IP의 사용법을 참조하십시오. 이 실습에서는 이미지에 표시된 대로 LINA가 9.6.1.x 코드를 실행하므로 이는 예상된 결과입니다.



Rules | Security Intelligence | HTTP Responses | Advanced

Filter by Device | Add Category | Add Rule | Search Rules

#	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

확인:

LINA CLI에서:

<#root>

```
firepower#

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

NAT 규칙이 예상대로 섹션 1에 삽입되었습니다.

<#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
```

참고: 백그라운드에서 생성되는 2개의 xlate입니다.

<#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 테이블:

<#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
```

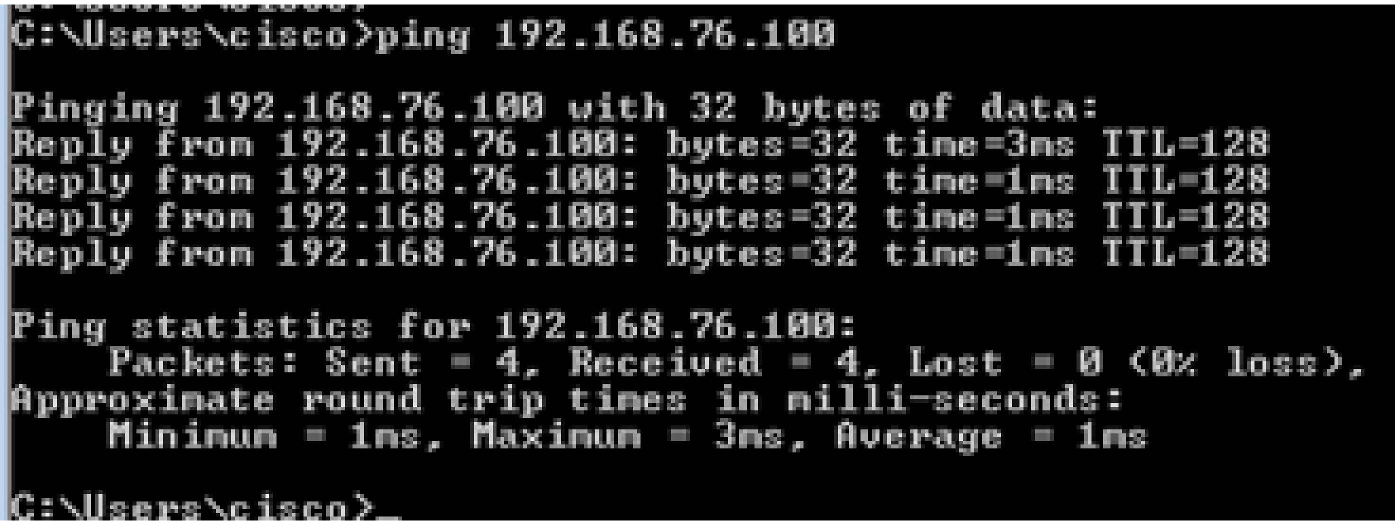
<#root>

```
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
```

그림과 같이 FTD에 대한 추적 세부사항을 사용하여 캡처를 활성화하고 Host-B에서 Host-A로 ping합니다.

<#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>_
```

적중 횟수는 ASP 테이블에 있습니다.

<#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
```

패킷 캡처에는 다음이 표시됩니다.

<#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
```

패킷의 추적(중요 포인트가 강조 표시됨)

참고: NAT 규칙의 ID 및 ASP 테이블과의 상관관계.

<#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
```

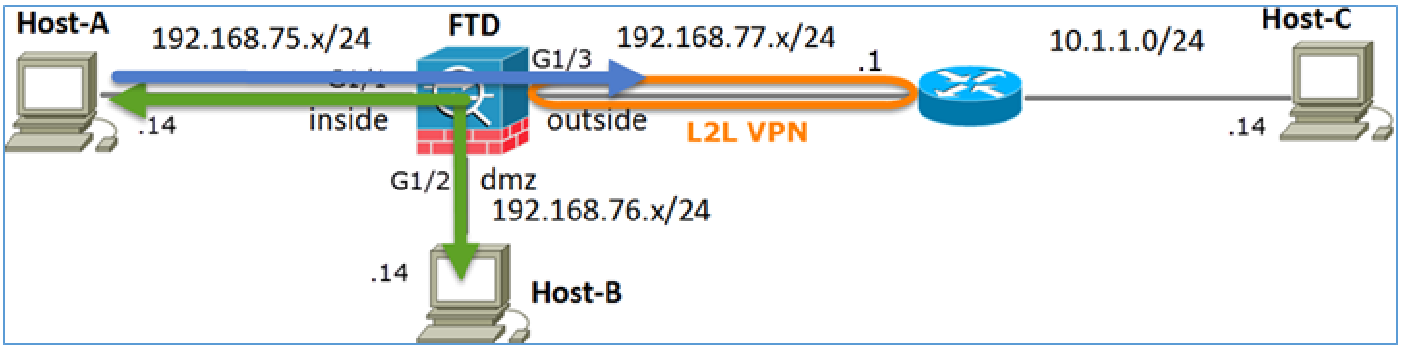
작업 2. FTD에서 PAT(Port Address Translation) 구성

다음 요구 사항에 따라 NAT를 구성합니다.

NAT 규칙	수동 NAT 규칙
NAT 유형	동적
삽입	섹션 1
소스 인터페이스	내부*

대상 인터페이스	외부*
원본	192.168.75.0/24
변환된 소스	외부 인터페이스(PAT)

*NAT 규칙에 보안 영역 사용

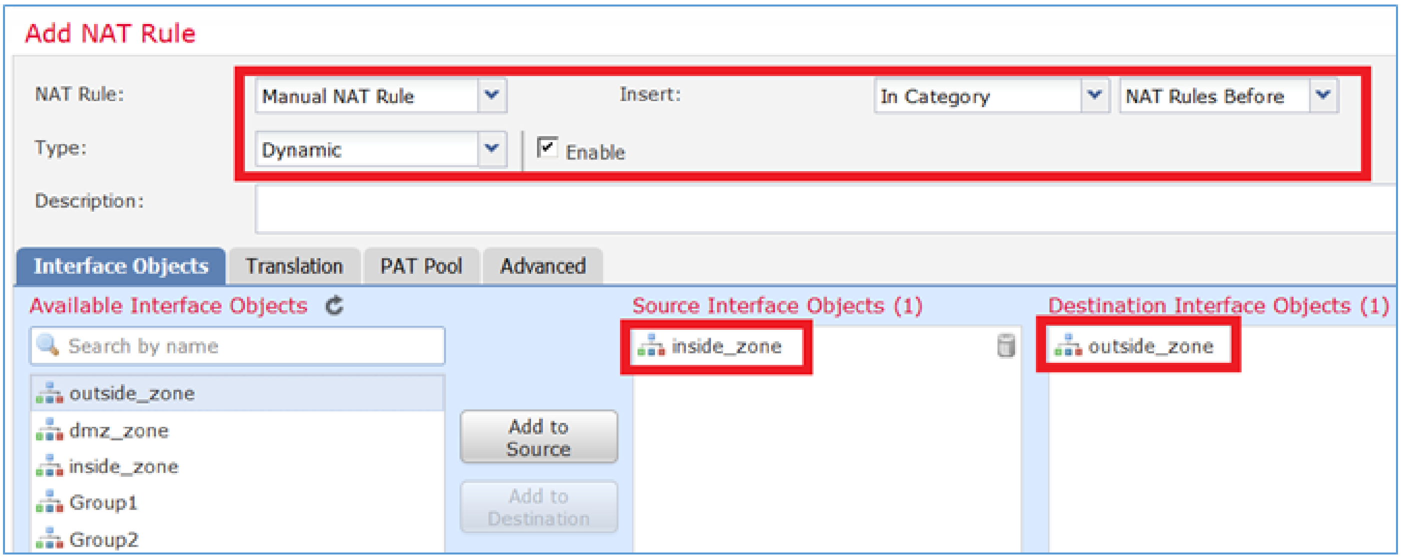


고정 NAT

가볍게 침

해결책:

1단계. 이미지에 표시된 대로 두 번째 NAT 규칙을 추가하고 작업 요건에 따라 구성합니다.



Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category | NAT Rules Before

Type: Dynamic

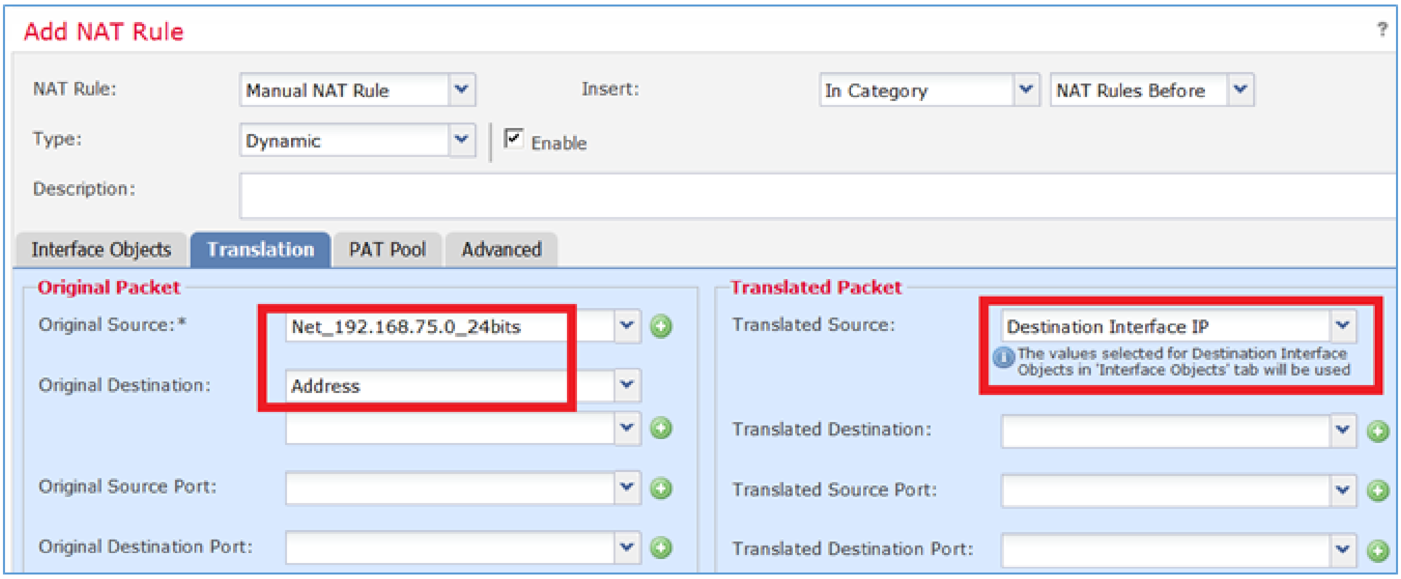
☑ Enable

Description:

Source Interface Objects (1): inside_zone

Destination Interface Objects (1): outside_zone

2단계. 다음은 이미지에 표시된 대로 PAT를 구성하는 방법입니다.



Add NAT Rule

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

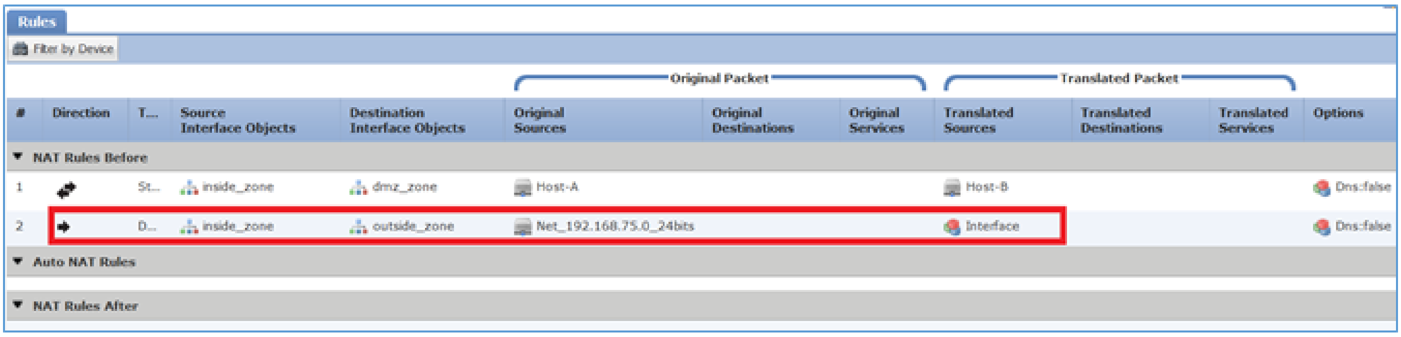
Original Packet

Original Source:* Net_192.168.75.0_24bits
Original Destination: Address
Original Source Port:
Original Destination Port:

Translated Packet

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

3단계. 결과는 그림과 같습니다.



Rules

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

4단계. 이 실습의 나머지 부분에서는 모든 트래픽이 통과할 수 있도록 액세스 제어 정책을 구성합니다.

확인:

NAT 구성:

<#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
```

LINA CLI에서 새 항목을 확인합니다.

<#root>

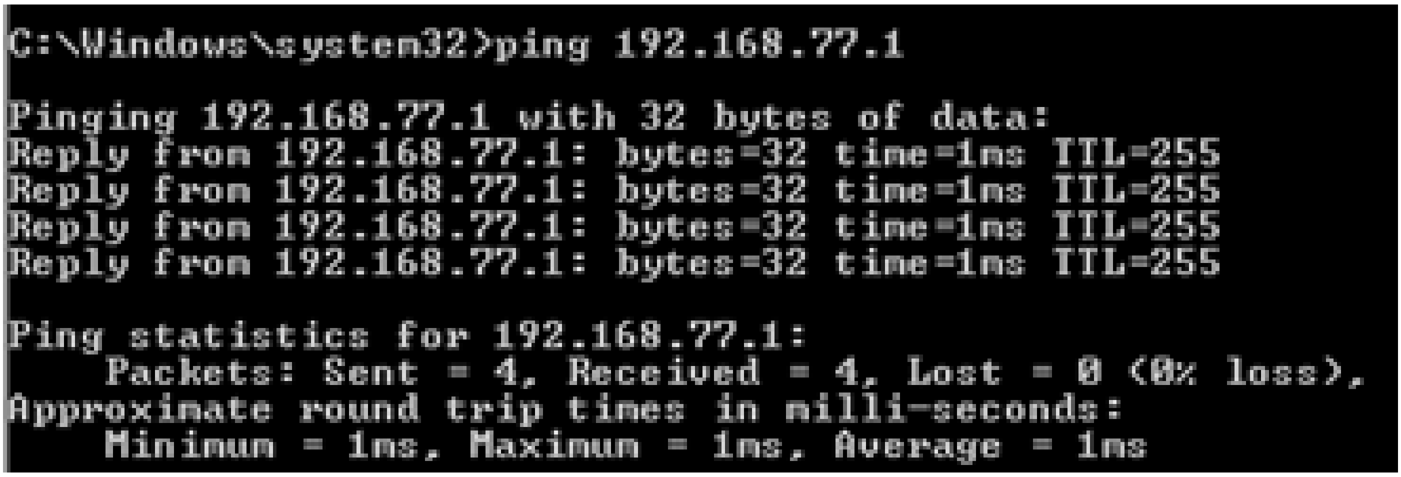
```
firepower#

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
```

내부 및 외부 인터페이스에서 캡처를 활성화합니다. 내부 캡처에서 추적을 활성화합니다.

<#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
```

그림과 같이 Host-A(192.168.75.14)에서 IP 192.168.77.1로 ping합니다.



```
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
```

LINA 캡처에서는 PAT 변환을 볼 수 있습니다.

<#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
```

중요 섹션이 강조 표시된 패킷의 추적:

<#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
```

동적 xlate가 생성되었습니다(ri 플래그 참고).

<#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
```

LINA 로그에는 다음이 표시됩니다.

<#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 섹션:

<#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 표에는 다음이 표시됩니다.

<#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
```

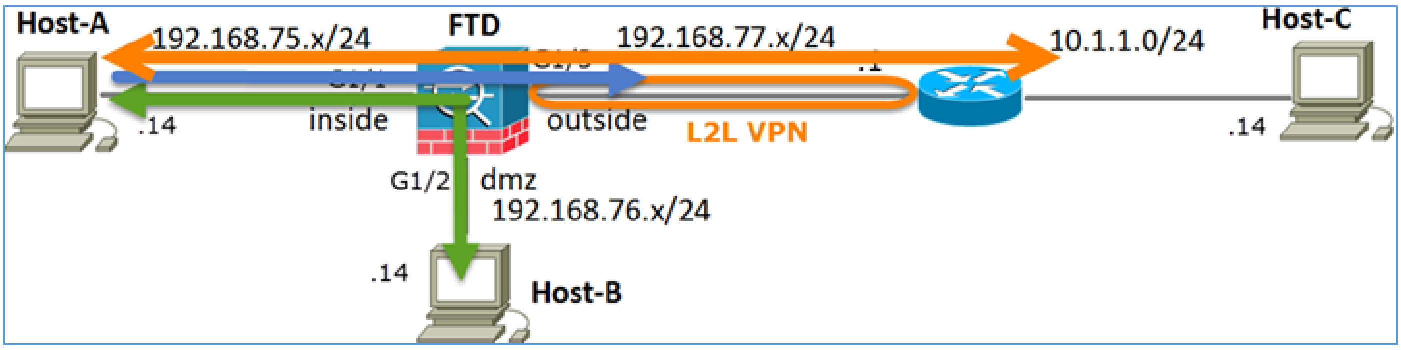
작업 3. FTD에서 NAT 예외 구성

다음 요구 사항에 따라 NAT를 구성합니다.

NAT 규칙	수동 NAT 규칙
NAT 유형	고정
삽입	섹션 1에서 모든 기존 규칙

소스 인터페이스	내부*
대상 인터페이스	외부*
원본	192.168.75.0/24
변환된 소스	192.168.75.0/24
원래 대상	10.1.1.0/24
변환된 대상	10.1.1.0/24

*NAT 규칙에 보안 영역 사용



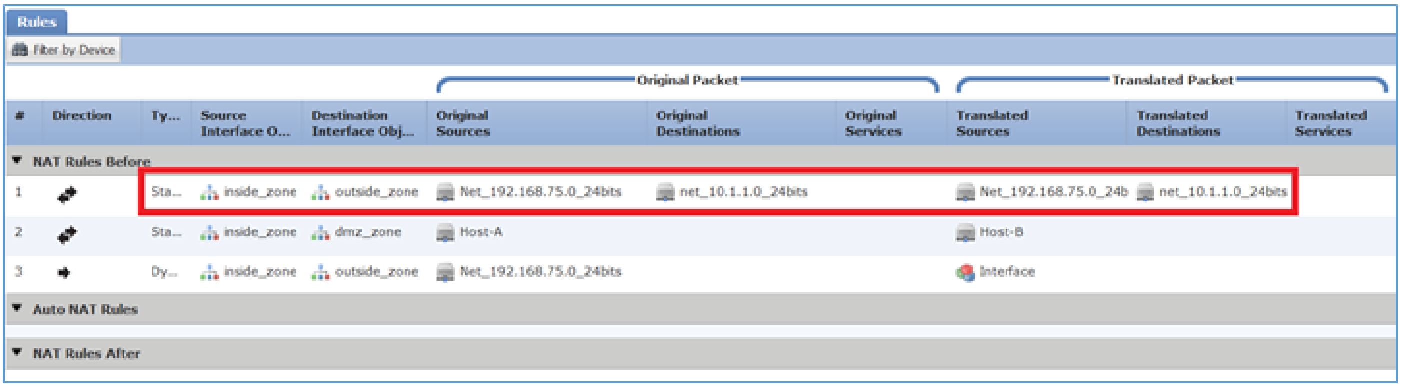
고정 NAT

가변게 침

NAT 예외

해결책:

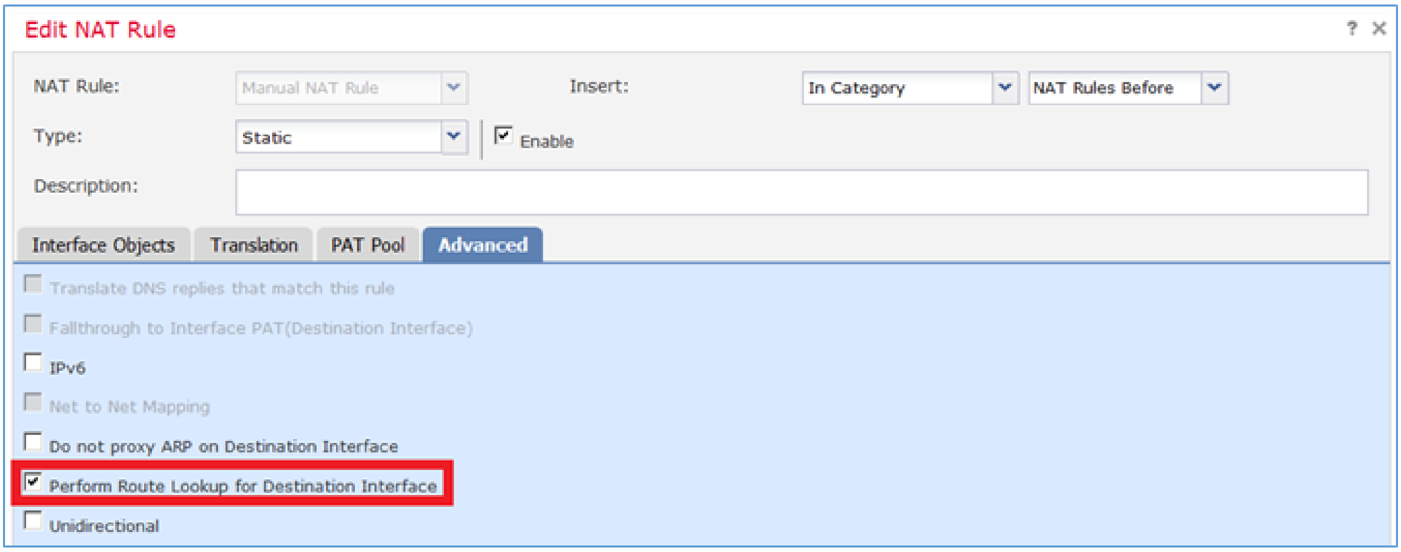
1단계. 이미지에 표시된 대로 세 번째 NAT 규칙을 추가하고 작업별 요건을 구성합니다.



					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										

2단계. 이그레스 인터페이스 확인을 위해 경로 조회를 수행합니다.

참고: 추가한 것과 같은 ID NAT 규칙의 경우 이그레스 인터페이스가 결정되는 방법을 변경하고 이미지에 표시된 대로 일반 경로 조회를 사용할 수 있습니다.



Edit NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category | NAT Rules Before

Type: Static

☑ Enable

Description:

Interface Objects | Translation | PAT Pool | Advanced

□ Translate DNS replies that match this rule

□ Fallthrough to Interface PAT(Destination Interface)

□ IPv6

□ Net to Net Mapping

□ Do not proxy ARP on Destination Interface

☑ Perform Route Lookup for Destination Interface

□ Unidirectional

확인:

<#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
```

내부 네트워크에서 소싱된 비 VPN 트래픽에 대해 packet-tracer를 실행합니다. PAT 규칙이 예상대로 사용됩니다.

<#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
```

VPN 터널을 통과해야 하는 트래픽에 대해 packet-tracer를 실행합니다(첫 번째 시도에서 VPN 터널을 가져온 후 두 번 실행).

참고: NAT 예외 규칙을 선택해야 합니다.

첫 번째 패킷 추적기 시도:

<#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
```

두 번째 패킷 추적기 시도:

<#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 적중 횟수 확인:

<#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
```

작업 4. FTD에서 개체 NAT 구성

다음 요구 사항에 따라 NAT를 구성합니다.

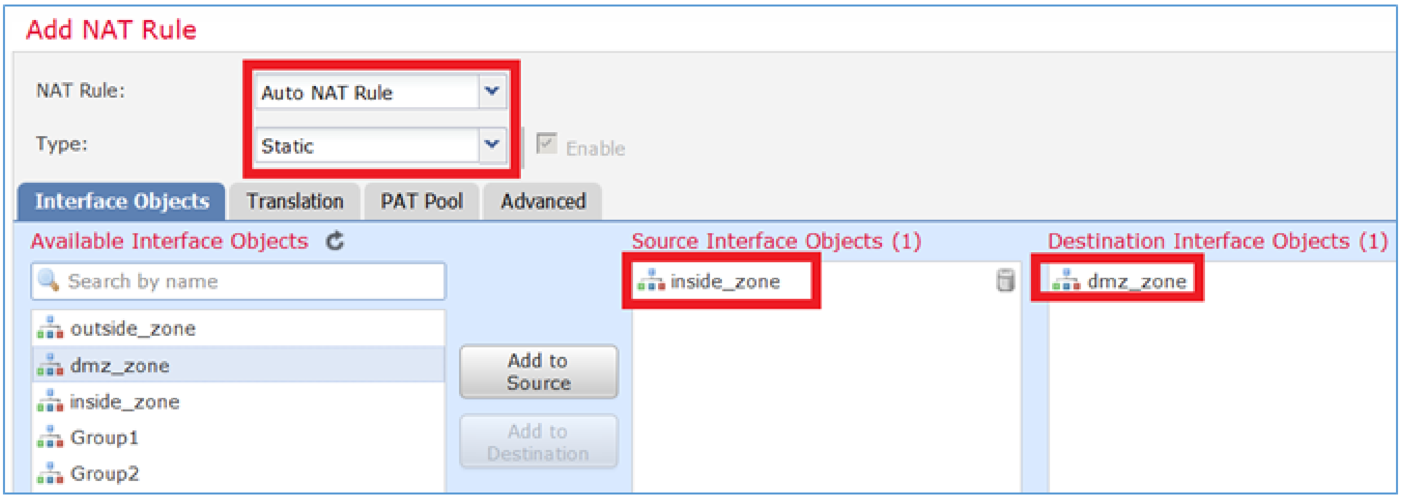
NAT 규칙	자동 NAT 규칙
NAT 유형	고정
삽입	섹션 2
소스 인터페이스	내부*
대상 인터페이스	DMZ*
원본	192.168.75.99
변환된 소스	192.168.76.99

이 규칙과 일치하는 DNS 회신 변환	사용

*NAT 규칙에 보안 영역 사용

해결책:

1단계. 이미지에 표시된 대로 작업 요구 사항에 따라 규칙을 구성합니다.



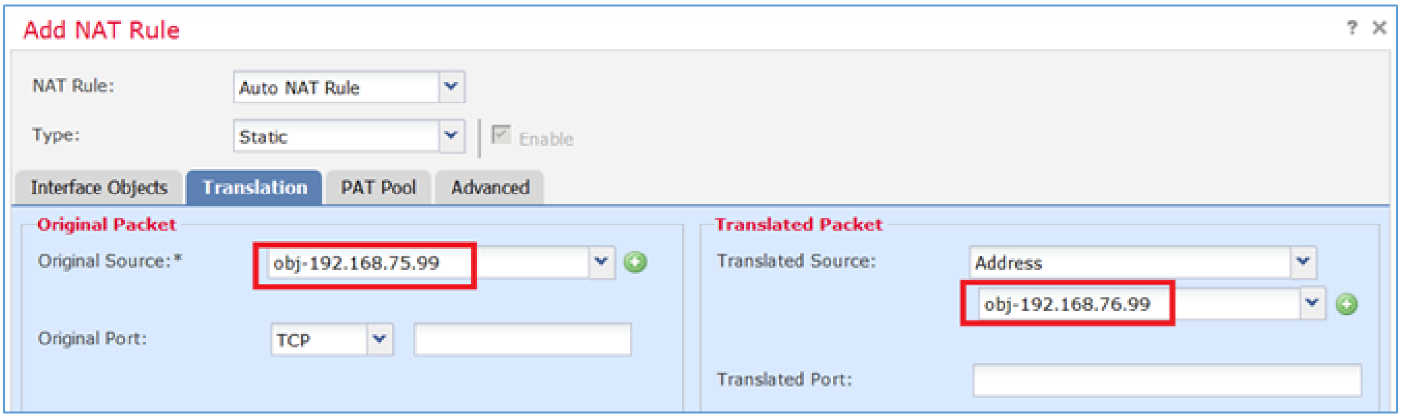
Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static ☑ Enable

Source Interface Objects (1): inside_zone

Destination Interface Objects (1): dmz_zone



Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Static ☑ Enable

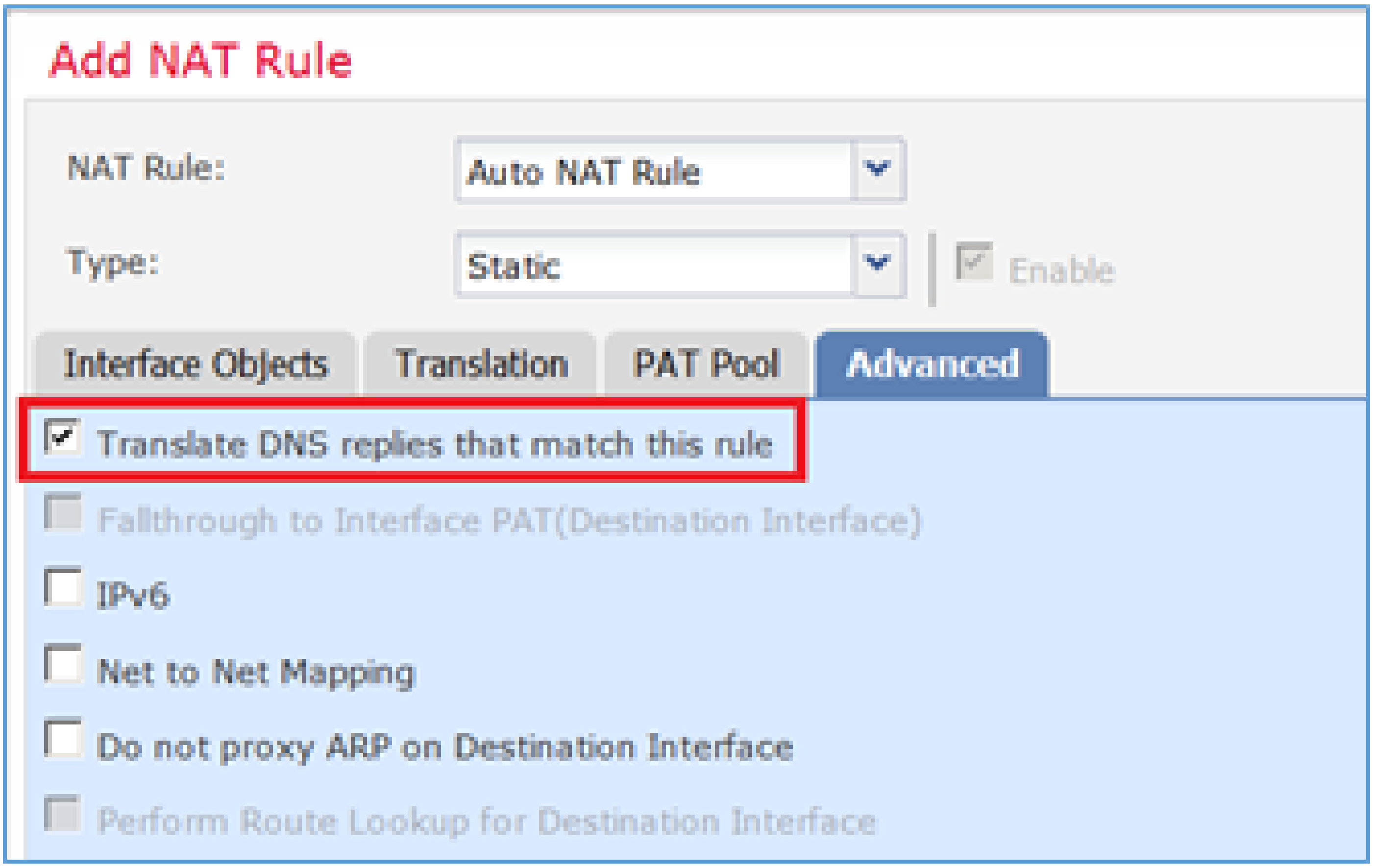
Original Source:* obj-192.168.75.99

Original Port: TCP

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)

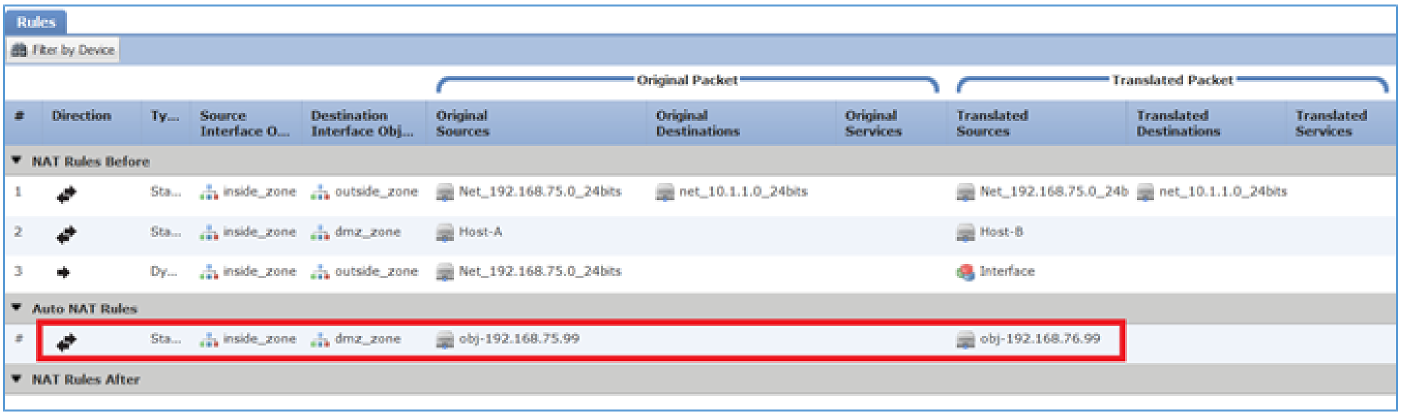
□ IPv6

□ Net to Net Mapping

□ Do not proxy ARP on Destination Interface

□ Perform Route Lookup for Destination Interface

2단계. 결과는 그림과 같습니다.



					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										

확인:

<#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
```

패킷 추적기를 통한 확인:

<#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
```

작업 5. FTD에서 PAT 풀 구성

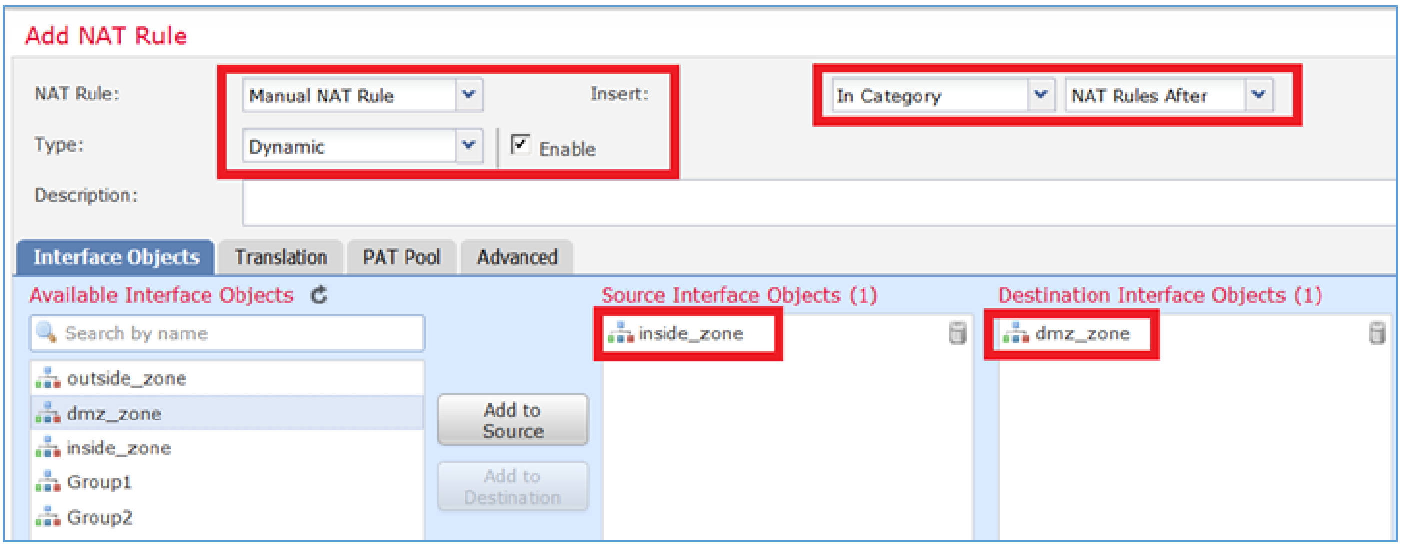
다음 요구 사항에 따라 NAT를 구성합니다.

NAT 규칙	수동 NAT 규칙
NAT 유형	동적
삽입	섹션 3
소스 인터페이스	내부*
대상 인터페이스	DMZ*
원본	192.168.75.0/24
변환된 소스	192.168.76.20-22
전체 범위 사용(1~65535)	사용

*NAT 규칙에 보안 영역 사용

해결책:

1단계. 이미지에 표시된 대로 작업 요구 사항별로 규칙을 구성합니다.



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

Add to Source

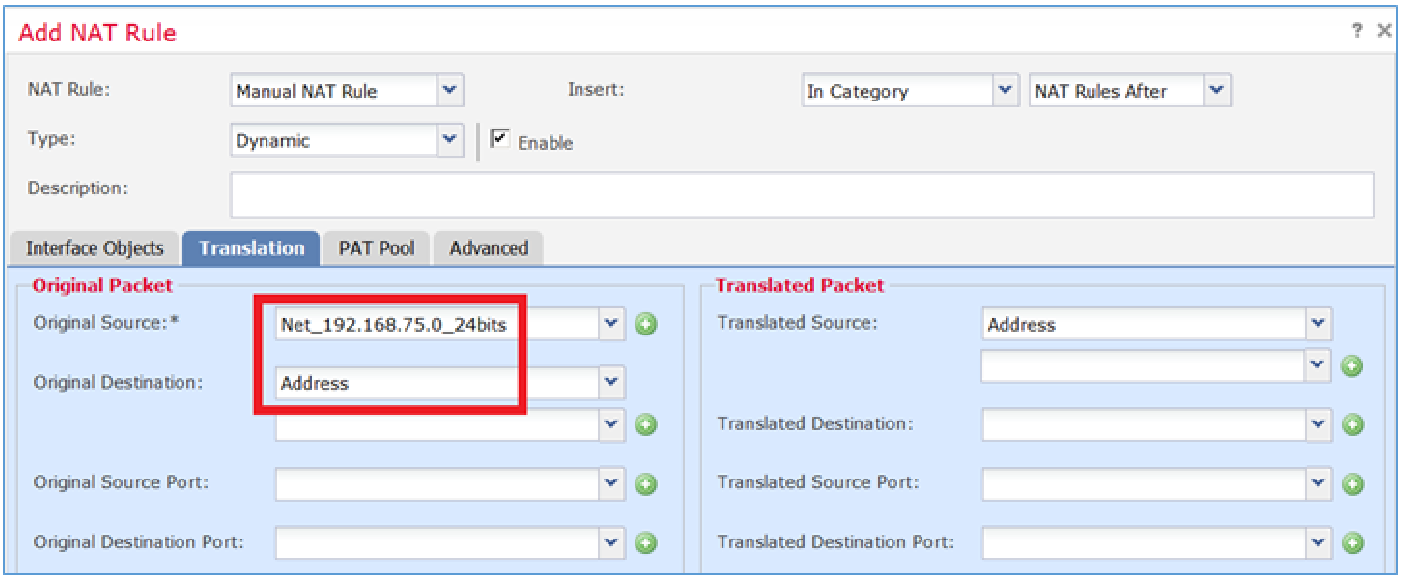
Add to Destination

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

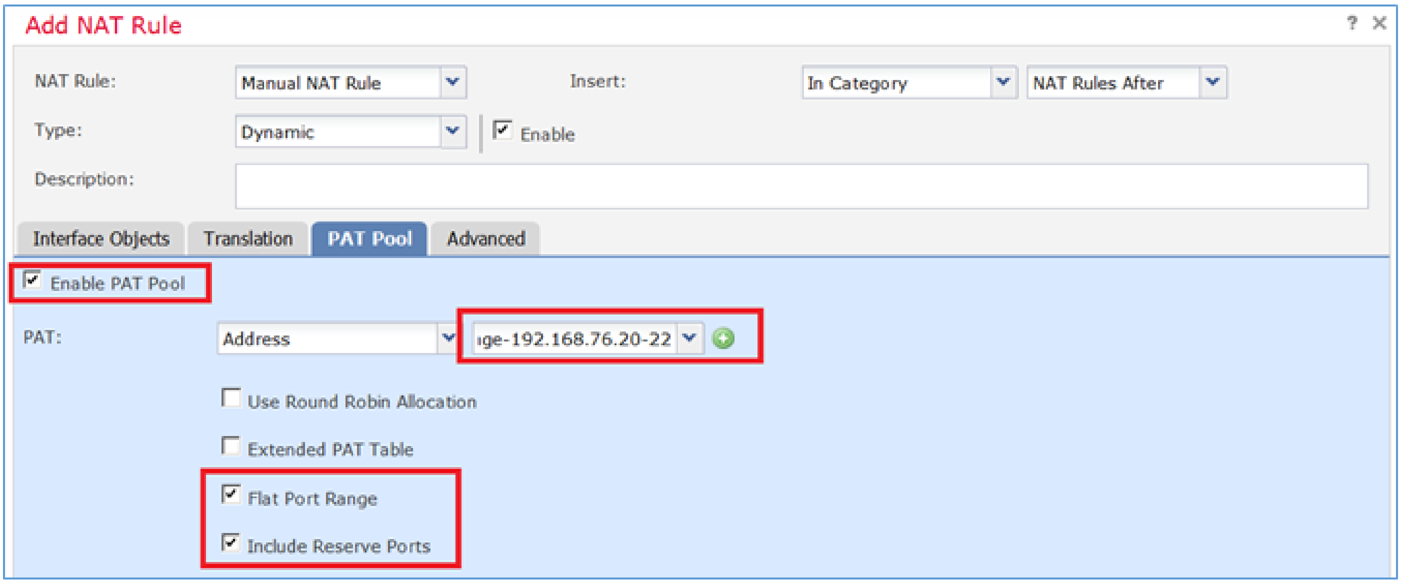
Translated Source: Address

Translated Destination:

Translated Source Port:

Translated Destination Port:

2단계. 이미지에 표시된 대로 전체 범위(1-65535)를 사용할 수 있도록 하는 Include Reserver Ports(Reserver 포트 포함)를 사용하여 Flat Port Range(플랫 포트 범위)를 활성화합니다.



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

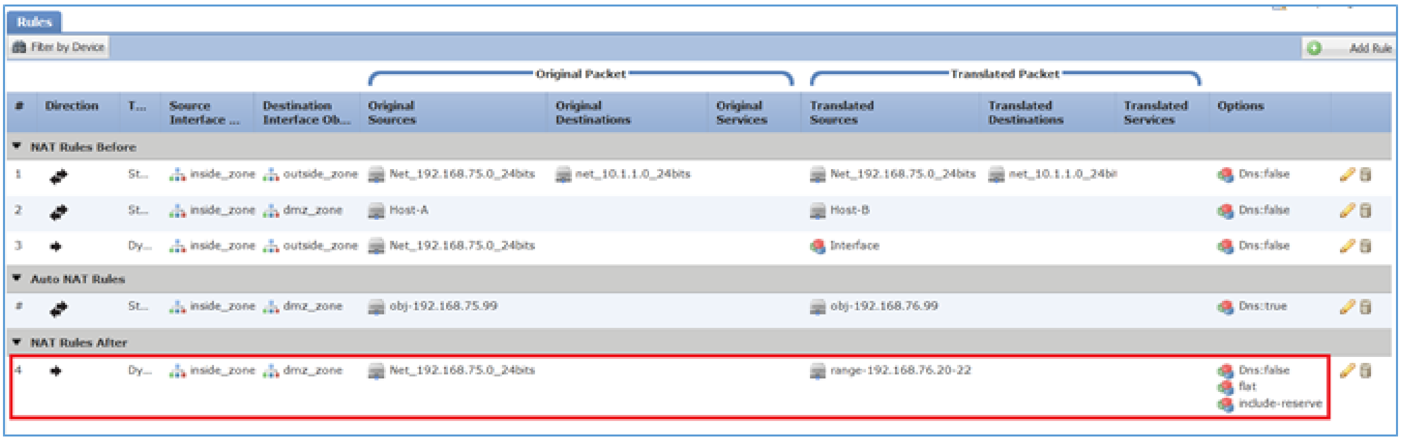
□ Use Round Robin Allocation

□ Extended PAT Table

☑ Flat Port Range

☑ Include Reserve Ports

3단계. 결과는 그림과 같습니다.



Rules

Filter by Device

Add Rule

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

확인:

<#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
```

규칙은 섹션 3에 있습니다.

<#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
```

패킷 추적기 확인:

<#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
```

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

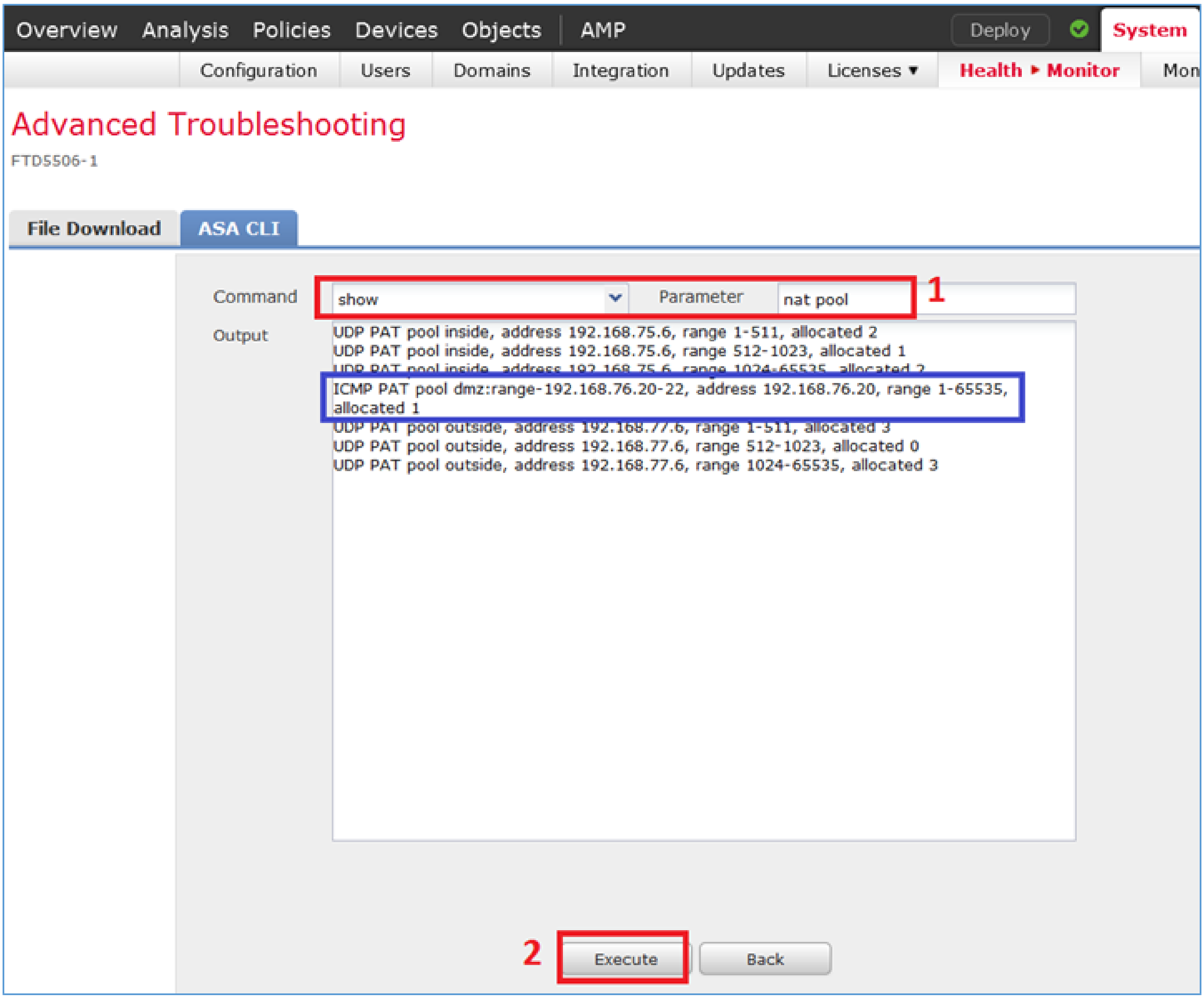
검증은 개별 작업 섹션에서 설명했습니다.

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

FMC에서 Advanced Troubleshooting(고급 트러블슈팅) 페이지를 열고, packet-tracer를 실행한 다음, show nat pool 명령을 실행합니다.

참고: 이미지에 표시된 대로 전체 범위를 사용하는 항목입니다.



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
```

관련 정보

- 모든 버전의 Cisco Firepower Management Center 컨피그레이션 가이드는 여기에서 찾을 수 있습니다.

Cisco Secure Firewall Threat Defense 설명서 탐색

- Cisco Global Technical Assistance Center(TAC)는 이 문서에 언급된 기술을 포함하여 Cisco Firepower Next Generation Security 기술에 대한 심층적인 실무 지식을 얻기 위해 이 시각적 가이드를 적극 권장합니다.

Cisco Press - Firepower 위협 방어

- firepower 기술과 관련된 모든 컨피그레이션 및 트러블슈팅 TechNote:

Cisco Secure Firewall 관리 센터

- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여