Configuración y verificación de NAT en FTD

Contenido

Introducción

Este documento describe cómo configurar y verificar la traducción de direcciones de red (NAT) básica en Firepower Threat Defence (FTD).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA5506X que ejecuta el código FTD 6.1.0-226
- FireSIGHT Management Center (FMC) que ejecuta 6.1.0-226
- 3 hosts de Windows 7
- Router Cisco IOS® 3925 que ejecuta VPN de LAN a LAN (L2L)

Hora de finalización del laboratorio: 1 hora.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

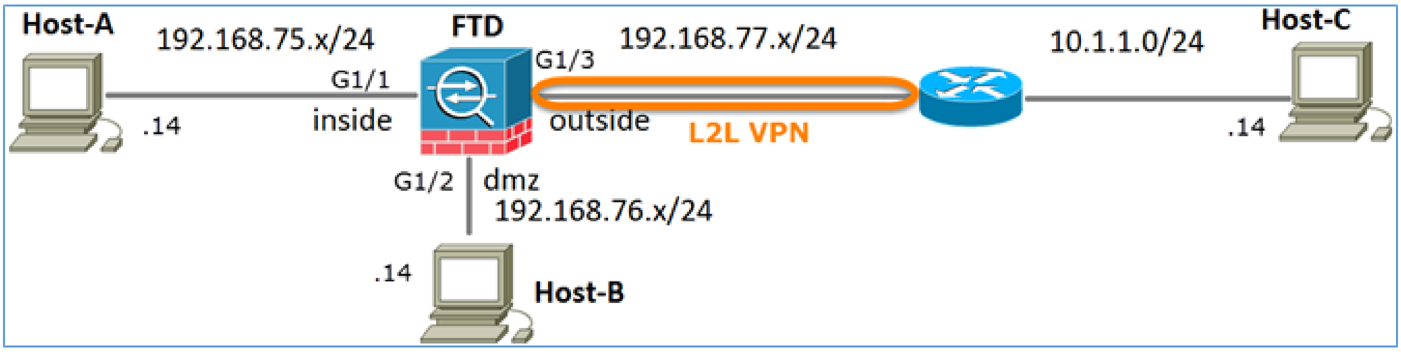
FTD admite las mismas opciones de configuración de NAT que el dispositivo de seguridad adaptable (ASA) clásico:

- Reglas NAT anteriores: equivalen a NAT doble (sección 1) en ASA clásico
- Reglas NAT automáticas - Sección 2 en ASA clásico
- Reglas NAT después de: equivalen a NAT doble (sección 3) en ASA clásico

Dado que la configuración FTD se realiza desde el FMC cuando se trata de la configuración NAT, es necesario estar familiarizado con la GUI de FMC y las diversas opciones de configuración.

Configurar

Diagrama de la red

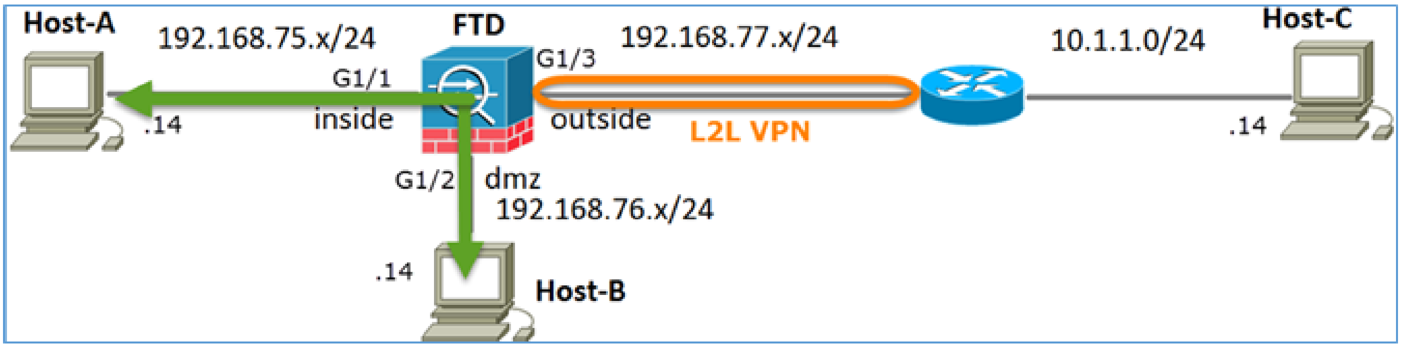


Tarea 1. Configuración de NAT estática en FTD

Configure NAT según estos requisitos:

Nombre de política NAT	El nombre del dispositivo FTD
Regla NAT	Regla NAT manual
Tipo de NAT	Estática
Insertar	En la sección 1
Interfaz de origen	interior*
Interfaz de destino	dmz*
Origen original	192.168.75.14
Origen traducido	192.168.76.100

*Usar zonas de seguridad para la regla NAT



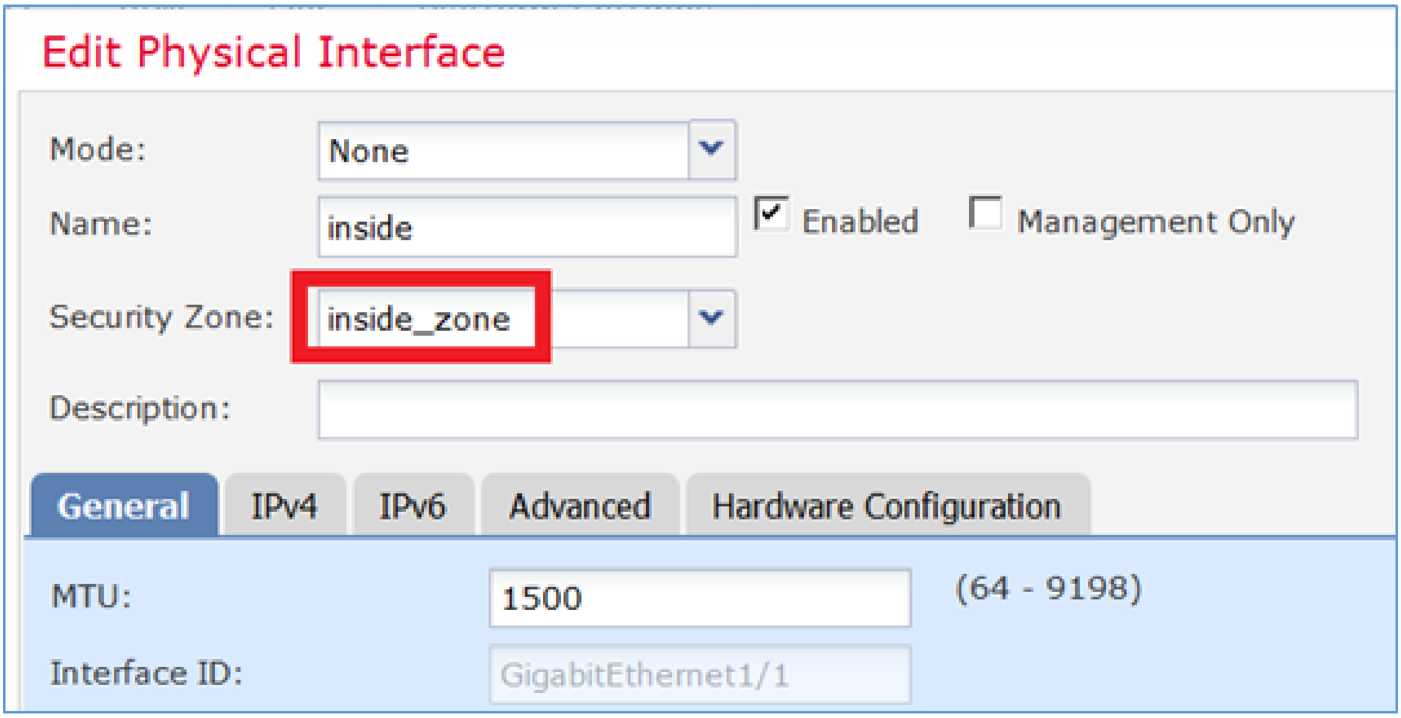
NAT estática

Solución:

Mientras que en el ASA clásico, debe utilizar nameif en las reglas NAT. En FTD, debe utilizar zonas de seguridad o grupos de interfaces.

Paso 1. Asignar interfaces a zonas de seguridad/grupos de interfaces.

En esta tarea, se decide asignar las interfaces FTD que se utilizan para NAT a las zonas de seguridad. Alternativamente, puede asignarlos a los grupos de interfaz como se muestra en la imagen.



Edit Physical Interface

Mode: None

Name: inside ☑ Enabled □ Management Only

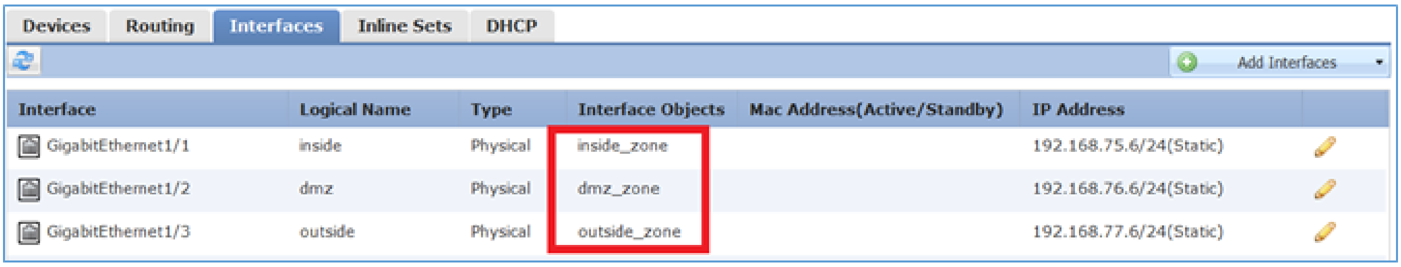
Security Zone: inside_zone

Description:

MTU: 1500 (64 - 9198)

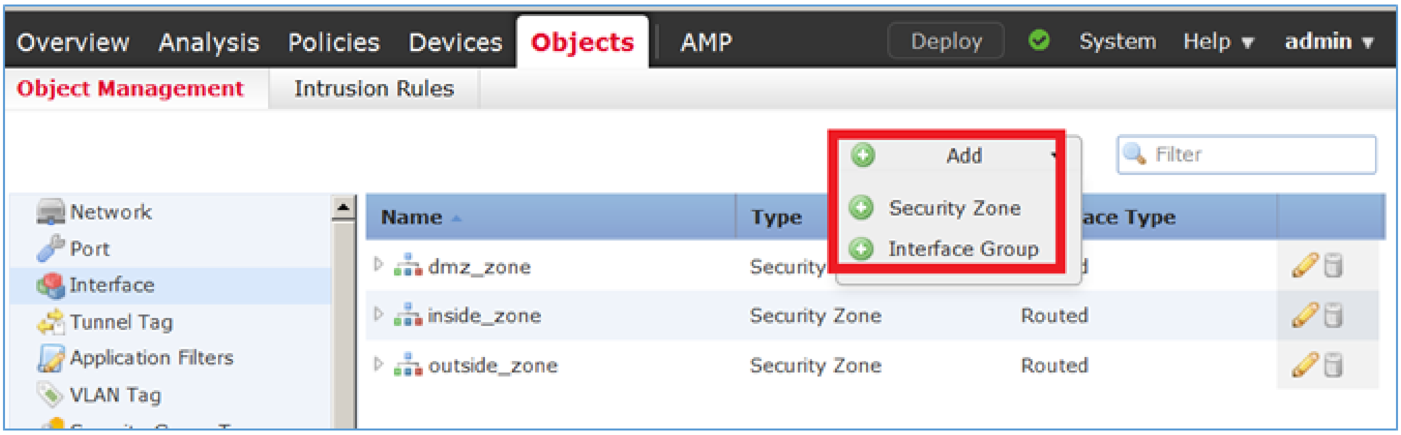
Interface ID: GigabitEthernet1/1

Paso 2. El resultado es como se muestra en la imagen.



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)

Paso 3. Puede crear/editar grupos de interfaz y zonas de seguridad desde la página **Objetos > Gestión de Objetos** como se muestra en la imagen.

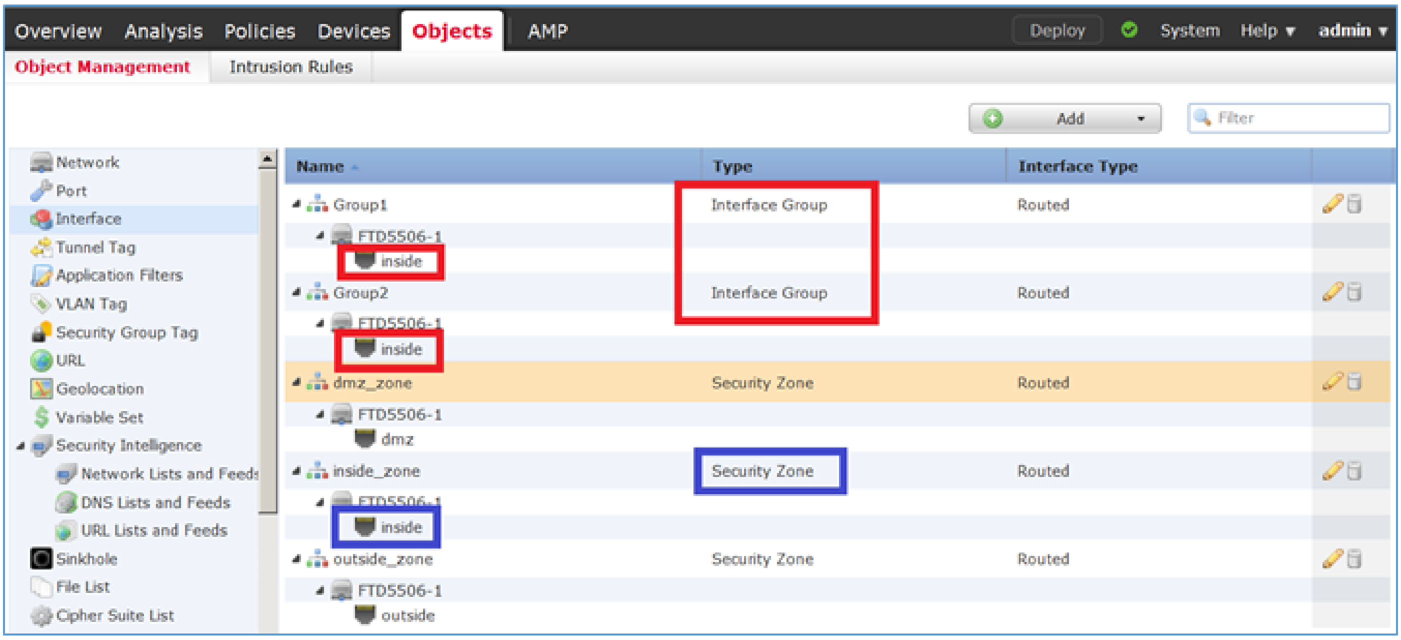


Name	Type	ace Type
dmz_zone	Security	d
inside_zone	Security Zone	Routed
outside_zone	Security Zone	Routed

Zonas de seguridad frente a grupos de interfaces

La diferencia principal entre las zonas de seguridad y los grupos de interfaz es que una interfaz puede pertenecer a una sola zona de seguridad, pero puede pertenecer a varios grupos de interfaz. Así que prácticamente, los grupos de interfaz proporcionan más flexibilidad.

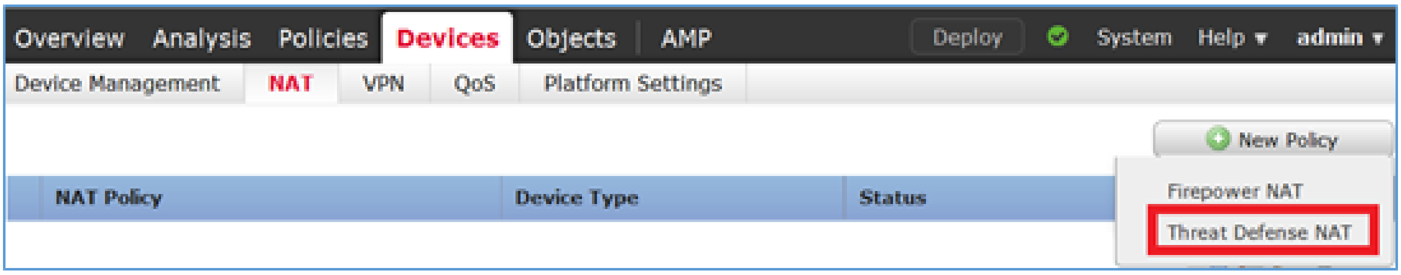
Puede ver que la interfaz **interna** pertenece a dos grupos de interfaz diferentes, pero sólo a una zona de seguridad como se muestra en la imagen.



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		

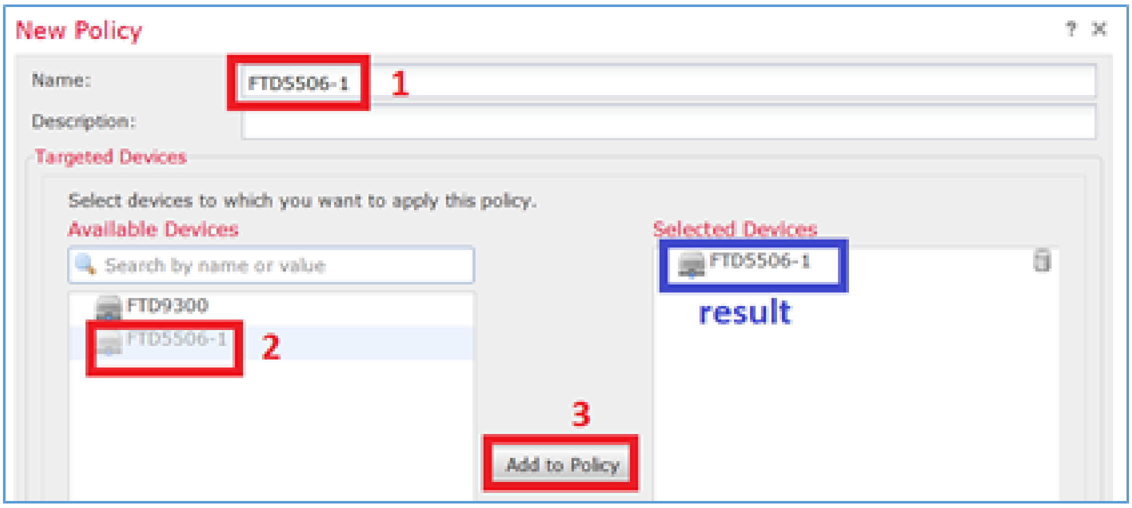
Paso 4. Configuración de NAT estática en FTD.

Navegue hasta **Devices > NAT** y cree una política NAT. Seleccione **New Policy > Threat Defence NAT** como se muestra en la imagen.



NAT Policy	Device Type	Status

Paso 5. Especifique el nombre de política y asígnelo a un dispositivo de destino como se muestra en la imagen.



New Policy

Name: FTD5506-1

Description:

Targeted Devices

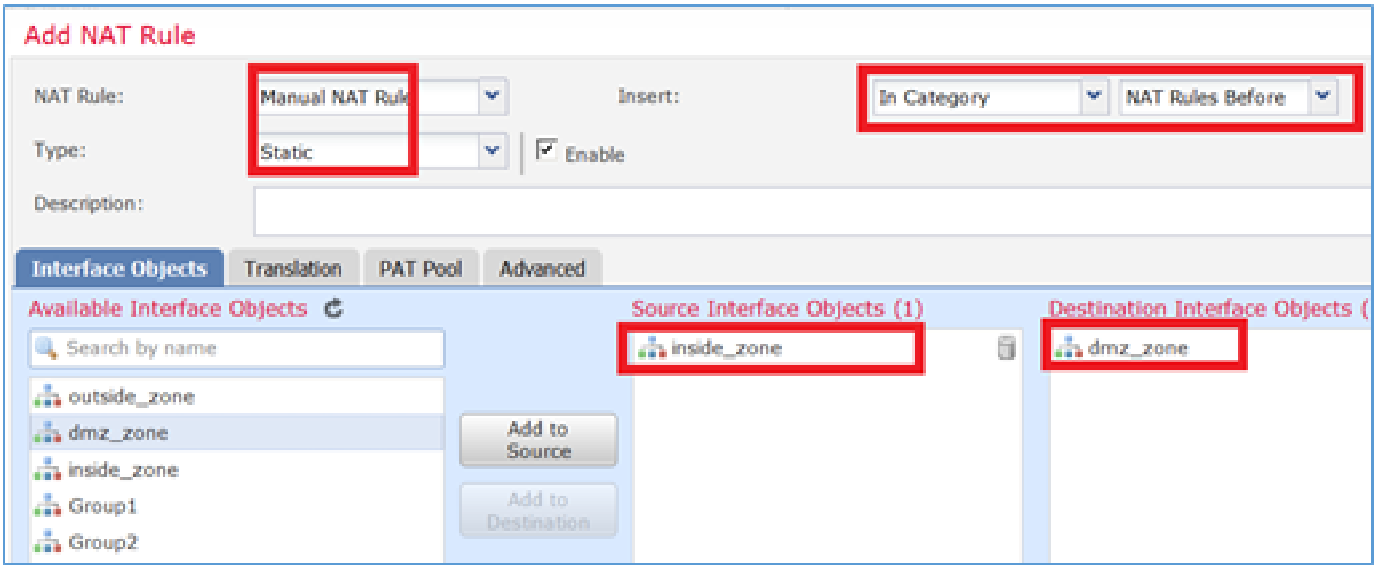
Select devices to which you want to apply this policy.

Available Devices: FTD9300, FTD5506-1

Selected Devices: FTD5506-1

Paso 6. Agregue una regla NAT a la política, haga clic en **Add Rule** .

Especifique estos según los requisitos de la tarea como se muestra en las imágenes.



Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category / NAT Rules Before

Type: Static

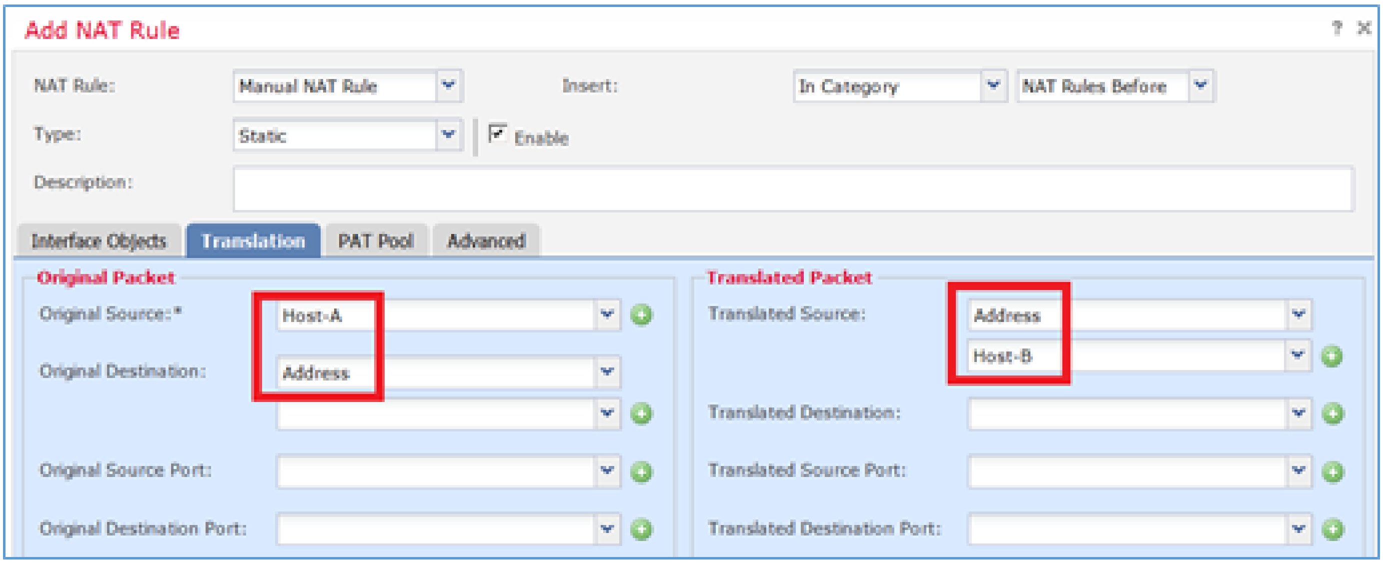
☑ Enable

Description:

Available Interface Objects: outside_zone, dmz_zone, inside_zone, Group1, Group2

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:

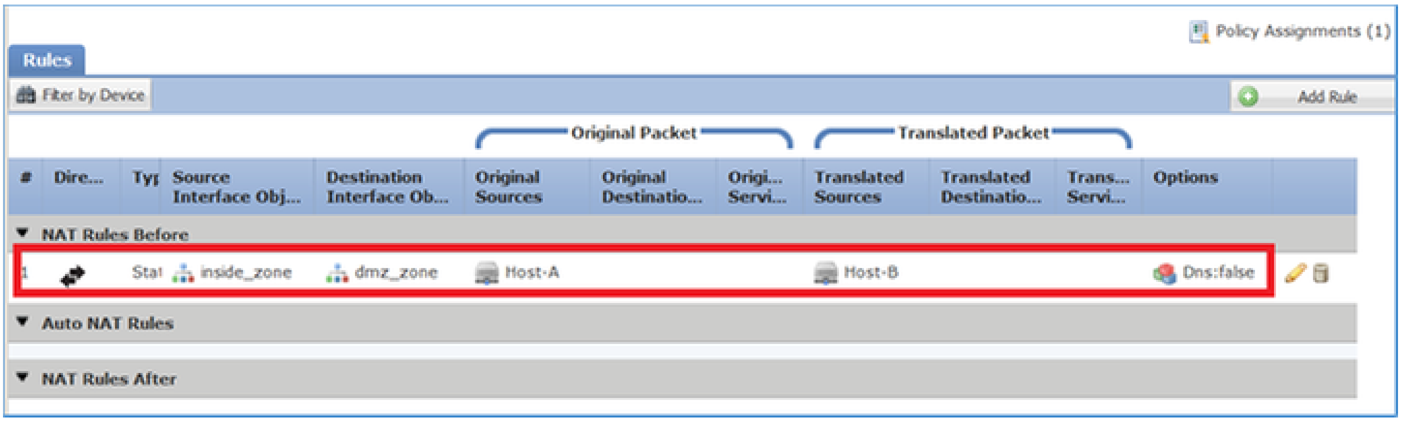
Host-A = 192.168.75.14

Host-B = 192.168.76.100

```
firepower# show run object
object network Host-A
 host 192.168.75.14
object network Host-B
 host 192.168.76.100
```

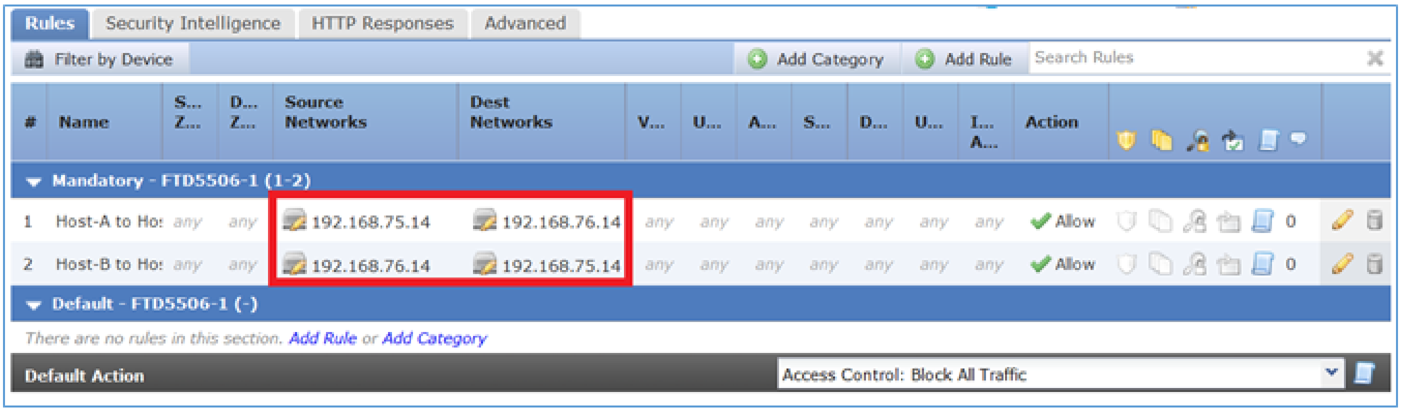
> **Advertencia:** Si configura la NAT estática y especifica una interfaz como origen traducido, todo el tráfico destinado a la dirección IP de la interfaz se redirige. Es posible que los usuarios no puedan acceder a ningún servicio habilitado en la interfaz asignada. Algunos ejemplos de estos servicios incluyen protocolos de ruteo como OSPF y EIGRP.

Paso 7. El resultado es como se muestra en la imagen.



#	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											

Paso 8. Asegúrese de que existe una política de control de acceso que permite al Host-B acceder al Host-A y viceversa. Recuerde que la NAT estática es bidireccional de forma predeterminada. Similar a los ASA clásicos, observe el uso de IP reales.Esto se espera ya que en este laboratorio, LINA ejecuta el código 9.6.1.x como se muestra en la imagen.



#	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

Verificación:

Desde LINA CLI:

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

La regla NAT se insertó en la Sección 1 como se esperaba:

```
firepower# show nat
Manual NAT Policies (Section 1)
1 (inside) to (dmz) source static Host-A Host-B
    translate_hits = 0, untranslate_hits = 0
```

Nota: Las 2 xlates que se crean en segundo plano.

```
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
```

Las tablas NAT de ASP:

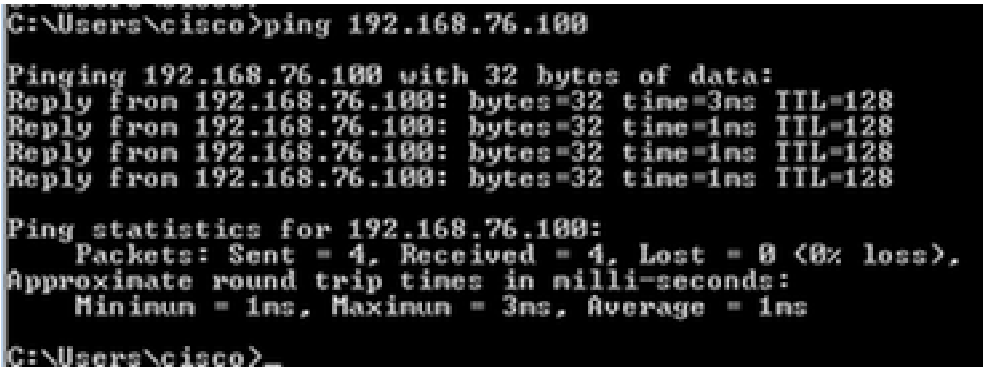
```
firepower# show asp table classify domain nat

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
```

```
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
```

Habilite la captura con detalles de seguimiento en FTD y haga ping del Host A al Host B y como se muestra en la imagen.

```
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>_
```

El número de visitas se encuentra en las tablas ASP:

```
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
```

```
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
```

La captura de paquetes muestra:

```
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
```

Rastros de un paquete (los puntos importantes están resaltados).

> **Nota:** El ID de la regla NAT y su correlación con la tabla ASP:

```
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
```

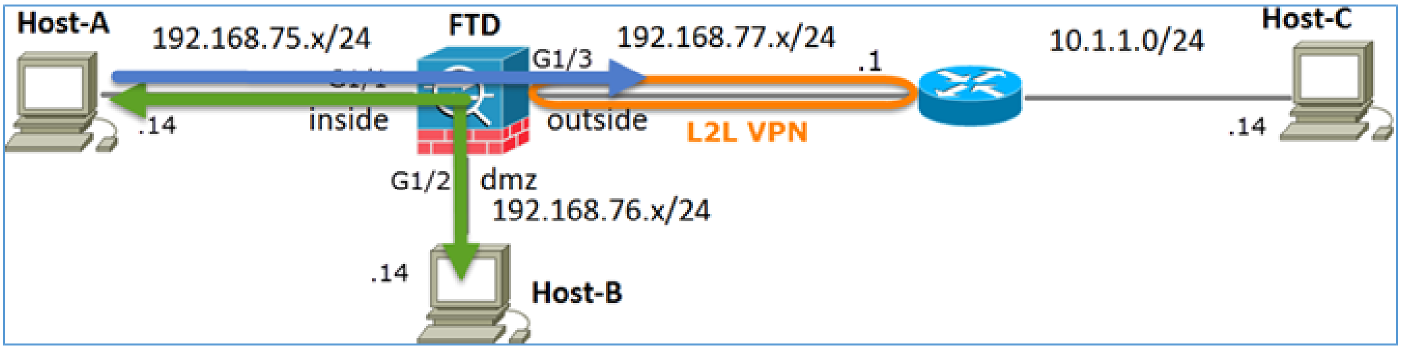
```
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.75.14 using egress ifc  inside

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
```

Tarea 2. Configuración de la traducción de direcciones de puerto (PAT) en FTD

Configure NAT según estos requisitos:

Regla NAT	Regla NAT manual
Tipo de NAT	Dinámico
Insertar	En la sección 1
Interfaz de origen	interior*
Interfaz de destino	exterior*
Origen original	192.168.75.0/24
Origen traducido	Interfaz externa (PAT)

*Usar zonas de seguridad para la regla NAT

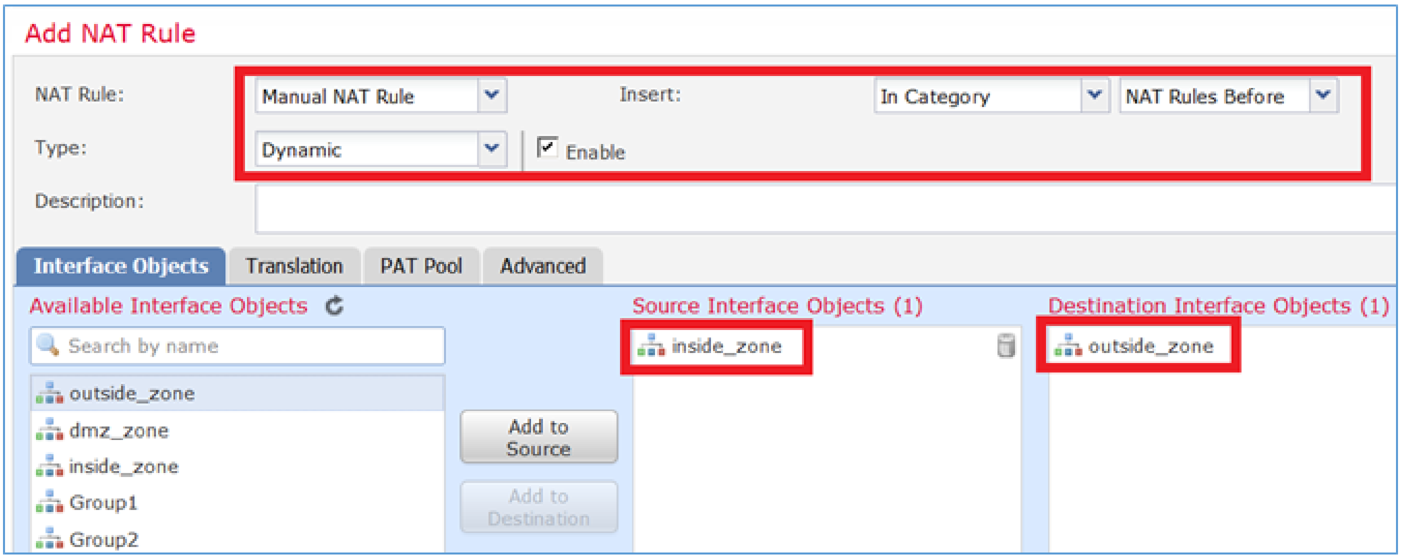


NAT estática

PAT

Solución:

Paso 1. Agregue una segunda regla NAT y configúrela según los requisitos de la tarea, como se muestra en la imagen.

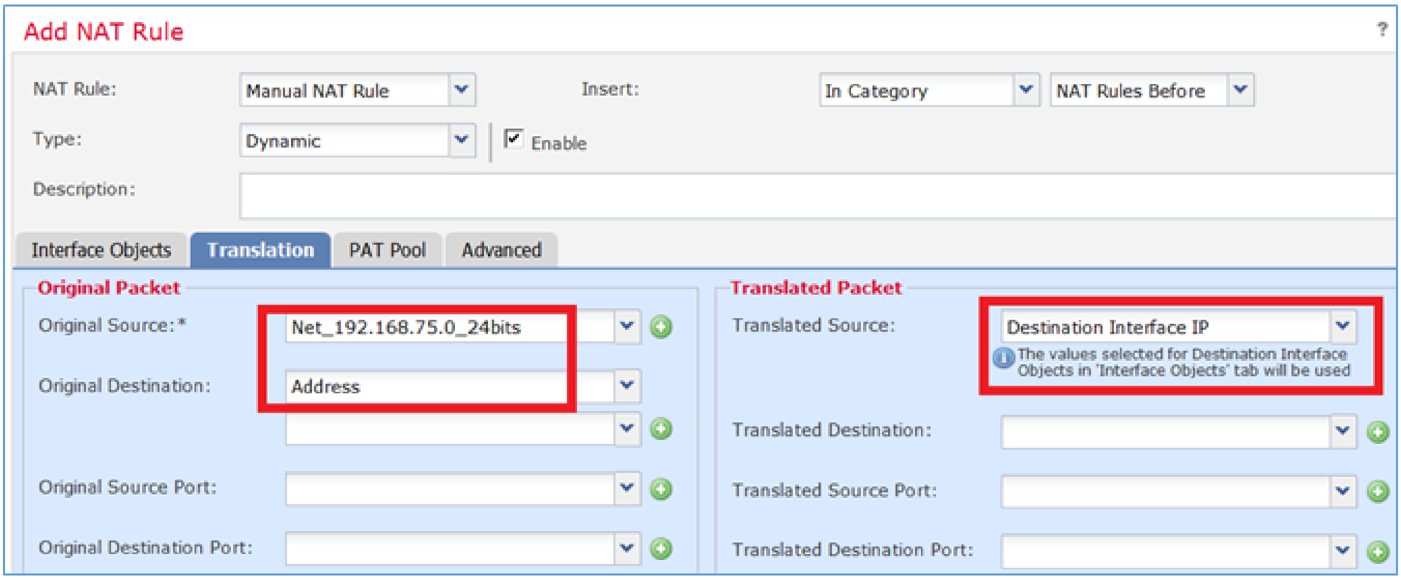


Add NAT Rule

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

Paso 2. Aquí está cómo se configura PAT como se muestra en la imagen.



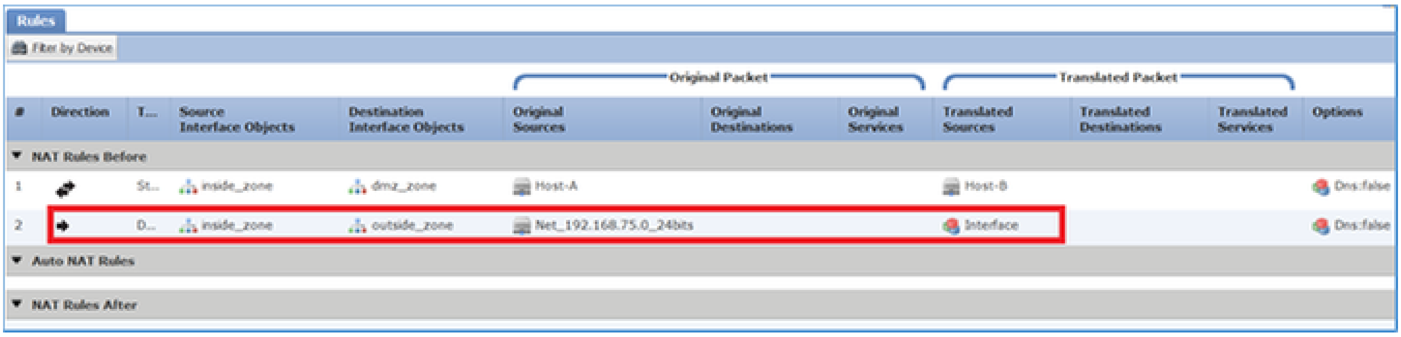
Add NAT Rule

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:

Paso 3. El resultado es como se muestra en la imagen.



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											

Paso 4. Para el resto de este laboratorio, configure la política de control de acceso para permitir que todo el tráfico pase.

Verificación:

Configuración de NAT:

```
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
```

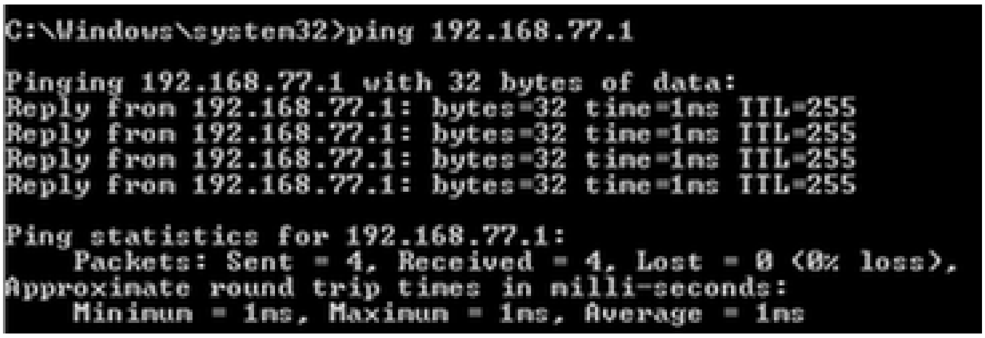
En LINA CLI, observe la nueva entrada:

```
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
```

Habilite la captura en la interfaz interna y externa. En la captura interna, habilite el seguimiento:

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

Ping desde Host-A (192.168.75.14) a IP 192.168.77.1 como se muestra en la imagen.



```
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
```

En las capturas LINA, puede ver la traducción PAT:

```
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
```

```
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
```

Rastros de un paquete con secciones importantes resaltadas:

```
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
```

Se creó la xlate dinámica (observe los indicadores "ri"):

```
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
```

En los registros de LINA verá:

```
firepower# show log
May 31 2016 18:54:43: %ASA-7-609001: Built local-host inside:192.168.75.14
May 31 2016 18:54:43: %ASA-6-305011: Built dynamic ICMP translation from inside:192.168.75.14/1
to outside:192.168.77.6/1
May 31 2016 18:54:43: %ASA-7-609001: Built local-host outside:192.168.77.1
May 31 2016 18:54:43: %ASA-6-302020: Built inbound ICMP connection for faddr 192.168.75.14/1
gaddr 192.168.77.1/0 laddr 192.168.77.1/0
May 31 2016 18:54:43: %ASA-6-302021: Teardown ICMP connection for faddr 192.168.75.14/1 gaddr
192.168.77.1/0 laddr 192.168.77.1/0
May 31 2016 18:54:43: %ASA-7-609002: Teardown local-host outside:192.168.77.1 duration 0:00:00
May 31 2016 18:55:17: %ASA-6-305012: Teardown dynamic ICMP translation from
inside:192.168.75.14/1 to outside:192.168.77.6/1 duration 0:00:34
```

Secciones de NAT:

```
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
```

Las tablas ASP muestran:

```
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
```

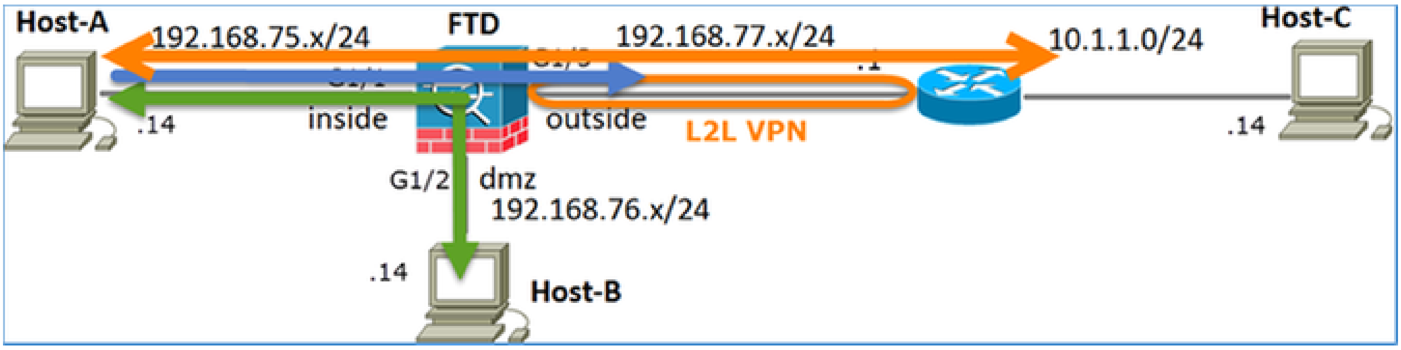
```
firepower# show asp table classify domain nat-reverse

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
```

Tarea 3. Configuración de la exención de NAT en FTD

Configure NAT según estos requisitos:

Regla NAT	Regla NAT manual
Tipo de NAT	Estática
Insertar	En la sección 1 anterior todas las normas existentes
Interfaz de origen	interior*
Interfaz de destino	exterior*
Origen original	192.168.75.0/24
Origen traducido	192.168.75.0/24
Destino original	10.1.1.0/24
Destino traducido	10.1.1.0/24

*Usar zonas de seguridad para la regla NAT



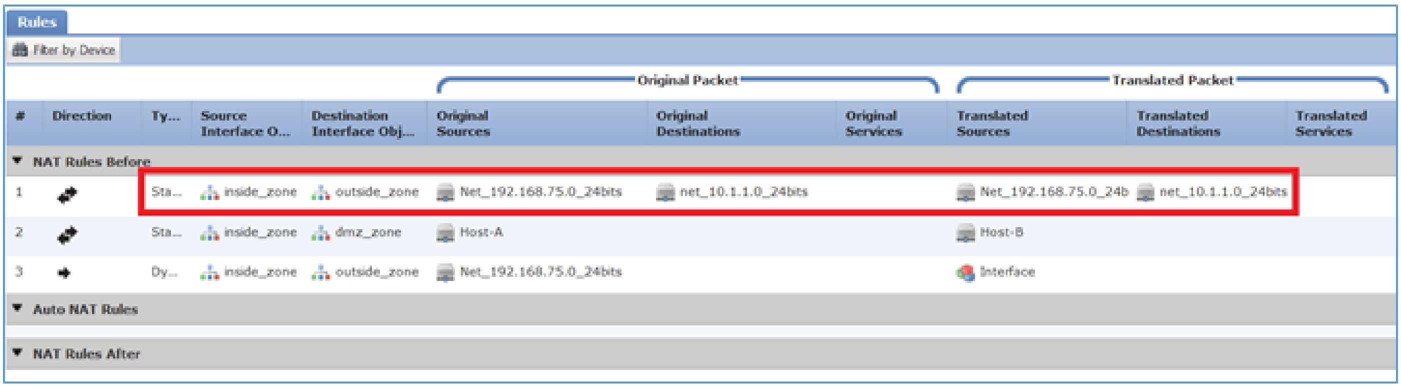
NAT estática

PAT

Exención de NAT

Solución:

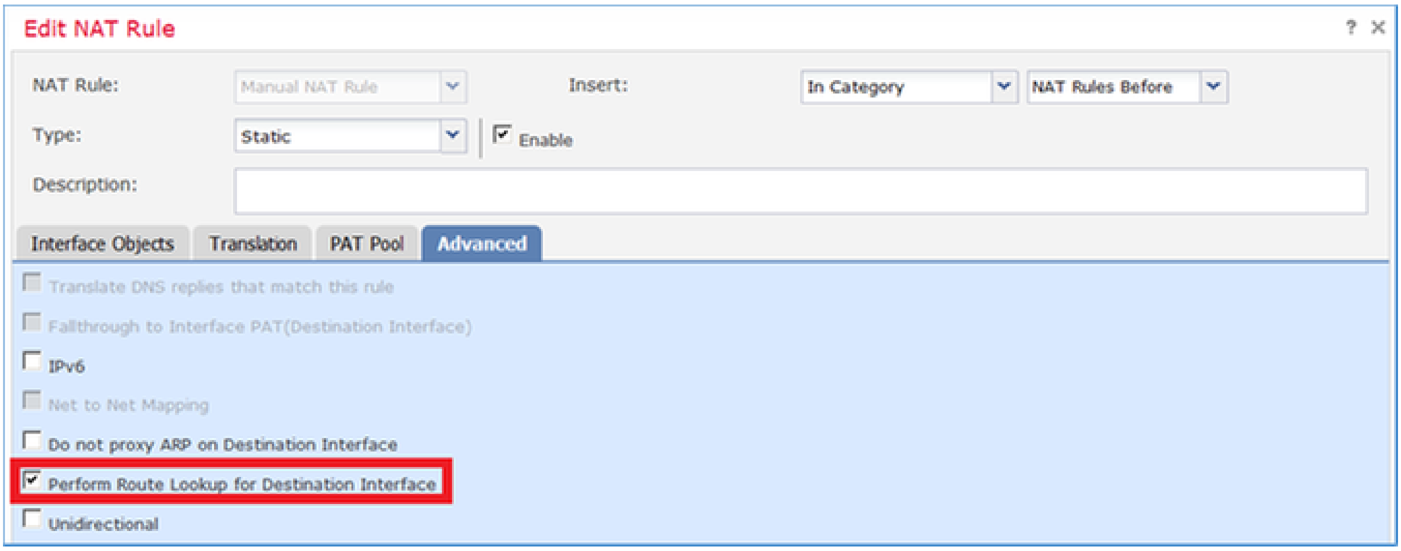
Paso 1. Agregue una tercera regla NAT y configure los requisitos por tarea como se muestra en la imagen.



#	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										

Paso 2. Realice la búsqueda de ruta para determinar la interfaz de salida.

> **Nota:** Para las reglas NAT de identidad, como la que agregó, puede cambiar cómo se determina la interfaz de salida y utilizar la búsqueda de ruta normal como se muestra en la imagen.



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

Verificación:

```
firepower# show run nat
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination
static net_10.1.1.0_24bits net_10.1.1.0_24bits
nat (inside,dmz) source static Host-A Host-B
nat (inside,outside) source dynamic Net_192.168.75.0_24bits interface
```

```
firepower# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits
destination static net_10.1.1.0_24bits net_10.1.1.0_24bits
    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
```

Ejecute packet-tracer para el tráfico no VPN originado en la red interna. La regla PAT se utiliza según lo esperado:

```
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
```

Ejecute packet-tracer para el tráfico que debe pasar a través del túnel VPN (ejecútelo dos veces desde que el primer intento activa el túnel VPN).

> **Nota:** Debe presionar la regla de exención de NAT.

Primer intento de rastreo de paquetes:

```
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 net_10.1.1.0_24bits net_10.1.1.0_24bits
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 net_10.1.1.0_24bits net_10.1.1.0_24bits
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
```

Segundo intento de rastreo de paquetes:

```
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 net_10.1.1.0_24bits net_10.1.1.0_24bits
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 net_10.1.1.0_24bits net_10.1.1.0_24bits
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 net_10.1.1.0_24bits net_10.1.1.0_24bits
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
```

Verificación de conteo de aciertos NAT:

```
firepower# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits
destination static net_10.1.1.0_24bits net_10.1.1.0_24bits
    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
```

Tarea 4. Configurar NAT de objetos en FTD

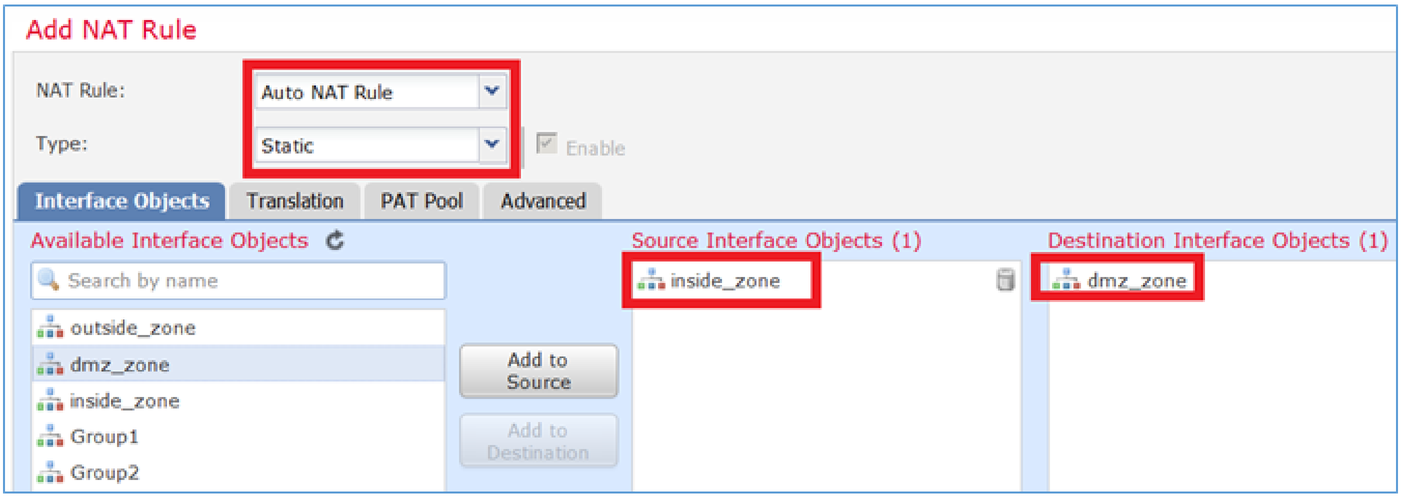
Configure NAT según estos requisitos:

Regla NAT	Regla NAT automática
Tipo de NAT	Estática
Insertar	En la sección 2
Interfaz de origen	interior*
Interfaz de destino	dmz*
Origen original	192.168.75.99
Origen traducido	192.168.76.99
Traducir respuestas DNS que coincidan con esta regla	Habilitado

*Usar zonas de seguridad para la regla NAT

Solución:

Paso 1. Configure la regla según los requisitos de la tarea como se muestra en las imágenes.



Add NAT Rule

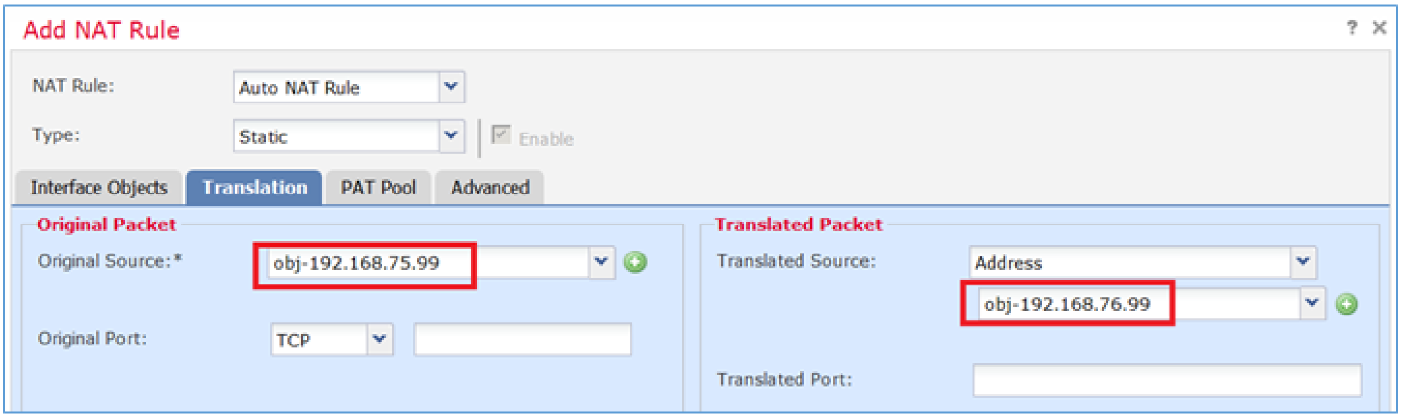
NAT Rule: Auto NAT Rule

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 Packet

Original Source:* obj-192.168.75.99

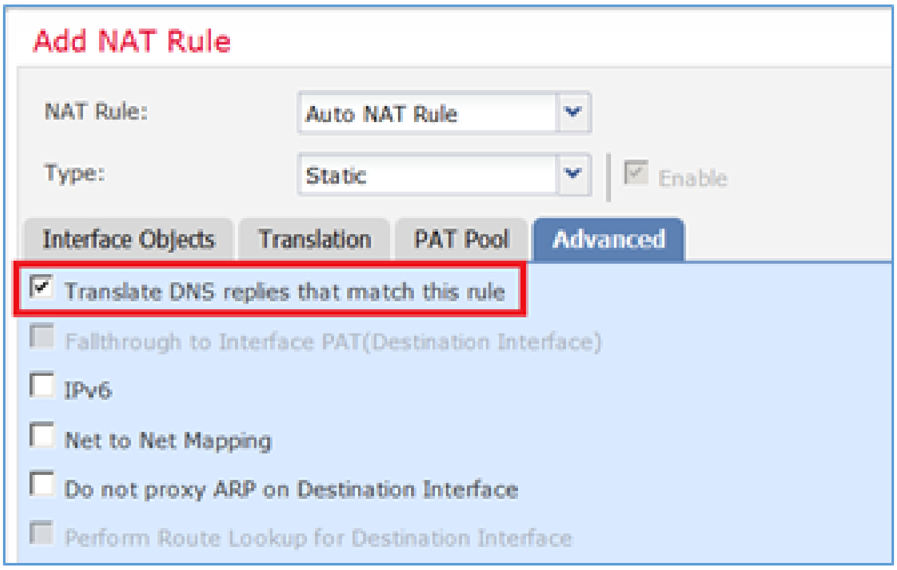
Original Port: TCP

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)

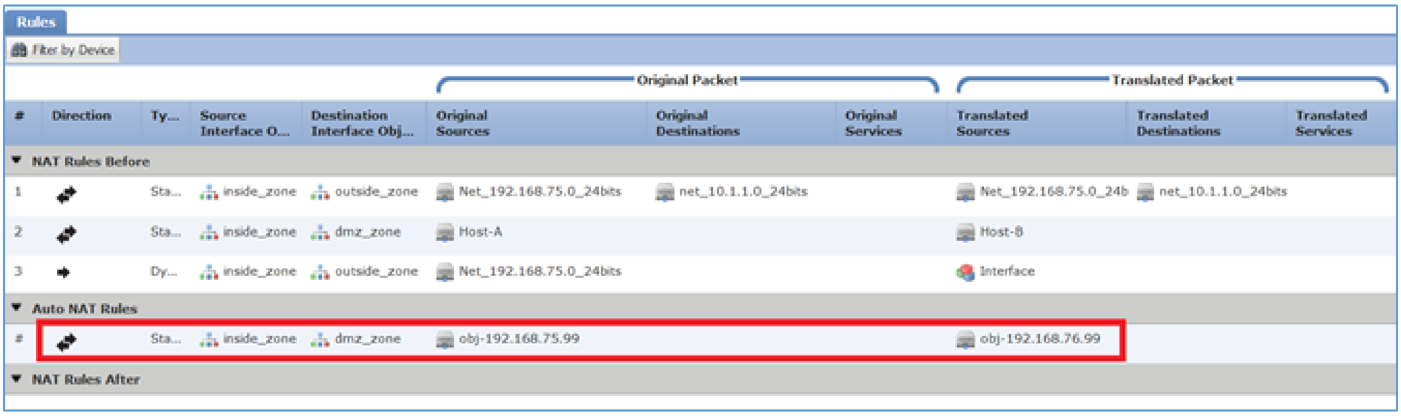
□ IPv6

□ Net to Net Mapping

□ Do not proxy ARP on Destination Interface

□ Perform Route Lookup for Destination Interface

Paso 2. El resultado es como se muestra en la imagen.



					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										

Verificación:

```
firepower# show run nat
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination
static net_10.1.1.0_24bits net_10.1.1.0_24bits
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
```

```
firepower# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits
destination static net_10.1.1.0_24bits net_10.1.1.0_24bits
    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
```

Verificación con packet-tracer:

```
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
```

Tarea 5. Configuración del conjunto PAT en FTD

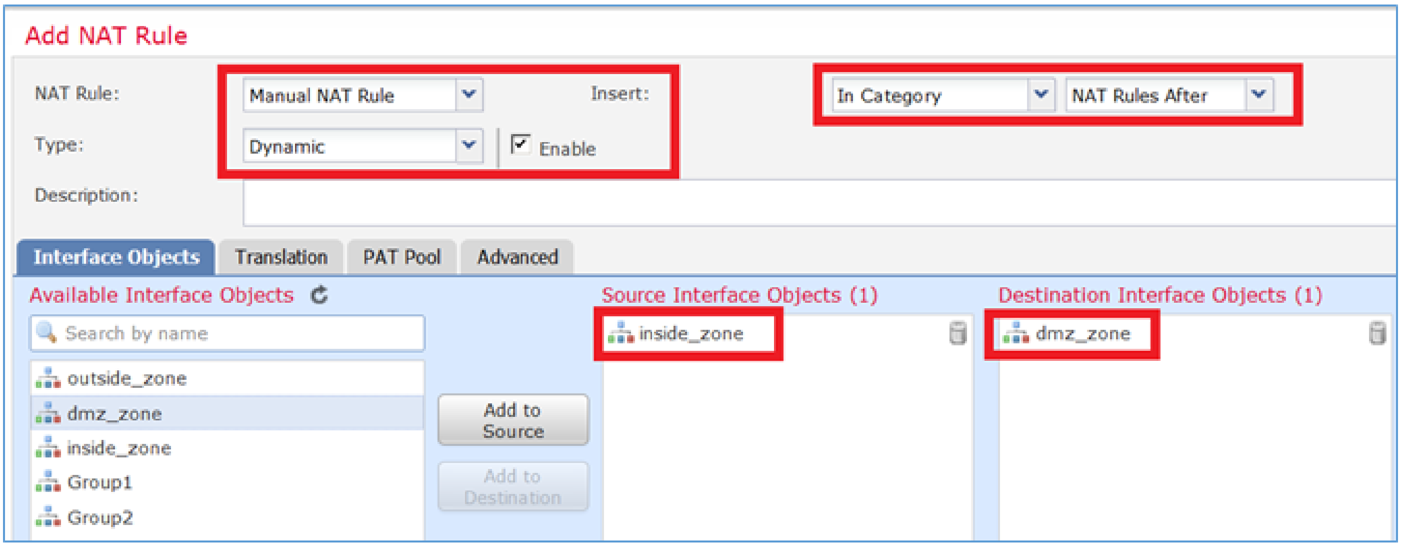
Configure NAT según estos requisitos:

Regla NAT	Regla NAT manual
Tipo de NAT	Dinámico
Insertar	En la sección 3
Interfaz de origen	interior*
Interfaz de destino	dmz*
Origen original	192.168.75.0/24
Origen traducido	192.168.76.20-22
Utilizar toda la gama (1-65535)	Habilitado

*Usar zonas de seguridad para la regla NAT

Solución:

Paso 1. Configure la regla según los requisitos de la tarea como se muestra en las imágenes.



Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category, NAT Rules After

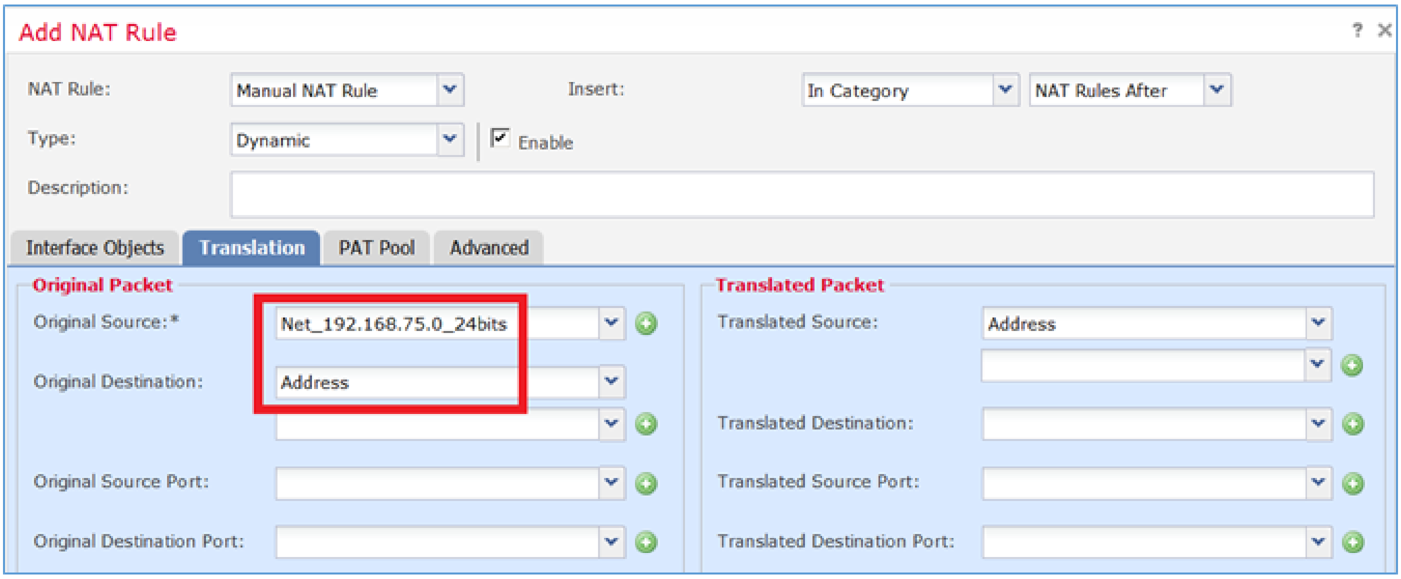
Type: Dynamic

☑ Enable

Description:

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:

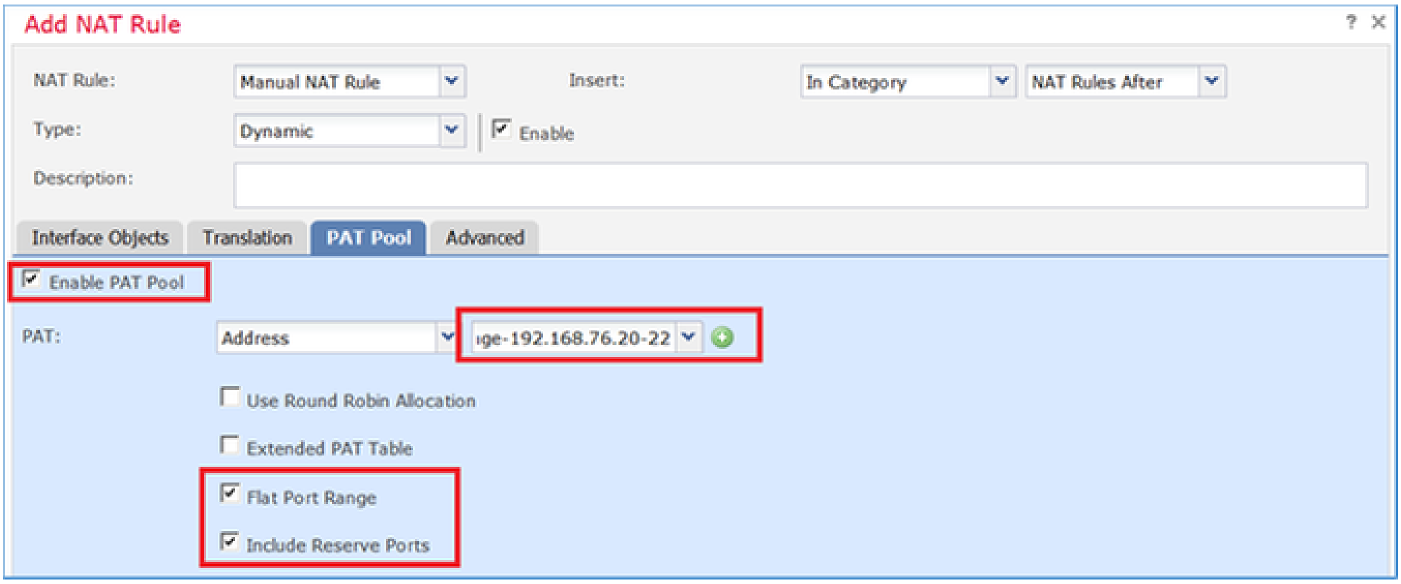
Original Packet

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:

Paso 2. Habilite **Flat Port Range** con **Include Reserver Ports** que permite el uso del rango completo (1-65535) como se muestra en la imagen.



Add NAT Rule

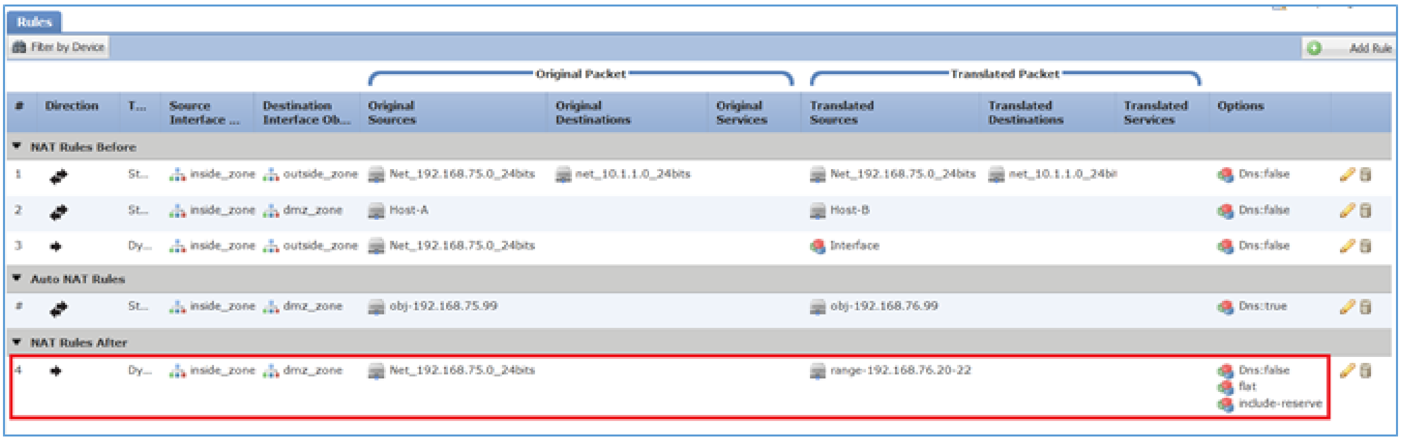
NAT Rule: Manual NAT Rule
Insert: In Category / NAT Rules After
Type: Dynamic ☑ Enable
Description:

☑ Enable PAT Pool

PAT: Address ıge-192.168.76.20-22

☐ Use Round Robin Allocation
☐ Extended PAT Table
☑ Flat Port Range
☑ Include Reserve Ports

Paso 3. El resultado es como se muestra en la imagen.



					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

Verificación:

```
firepower# show run nat
nat (inside,outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits destination
```

```
static net_10.1.1.0_24bits net_10.1.1.0_24bits
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 include-reserve
```

La regla está en la Sección 3:

```
firepower# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source static Net_192.168.75.0_24bits Net_192.168.75.0_24bits
destination static net_10.1.1.0_24bits net_10.1.1.0_24bits
    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-reserve
    translate_hits = 0, untranslate_hits = 0
```

Verificación del trazador de paquetes:

```
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 include-reserve
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 include-reserve
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
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

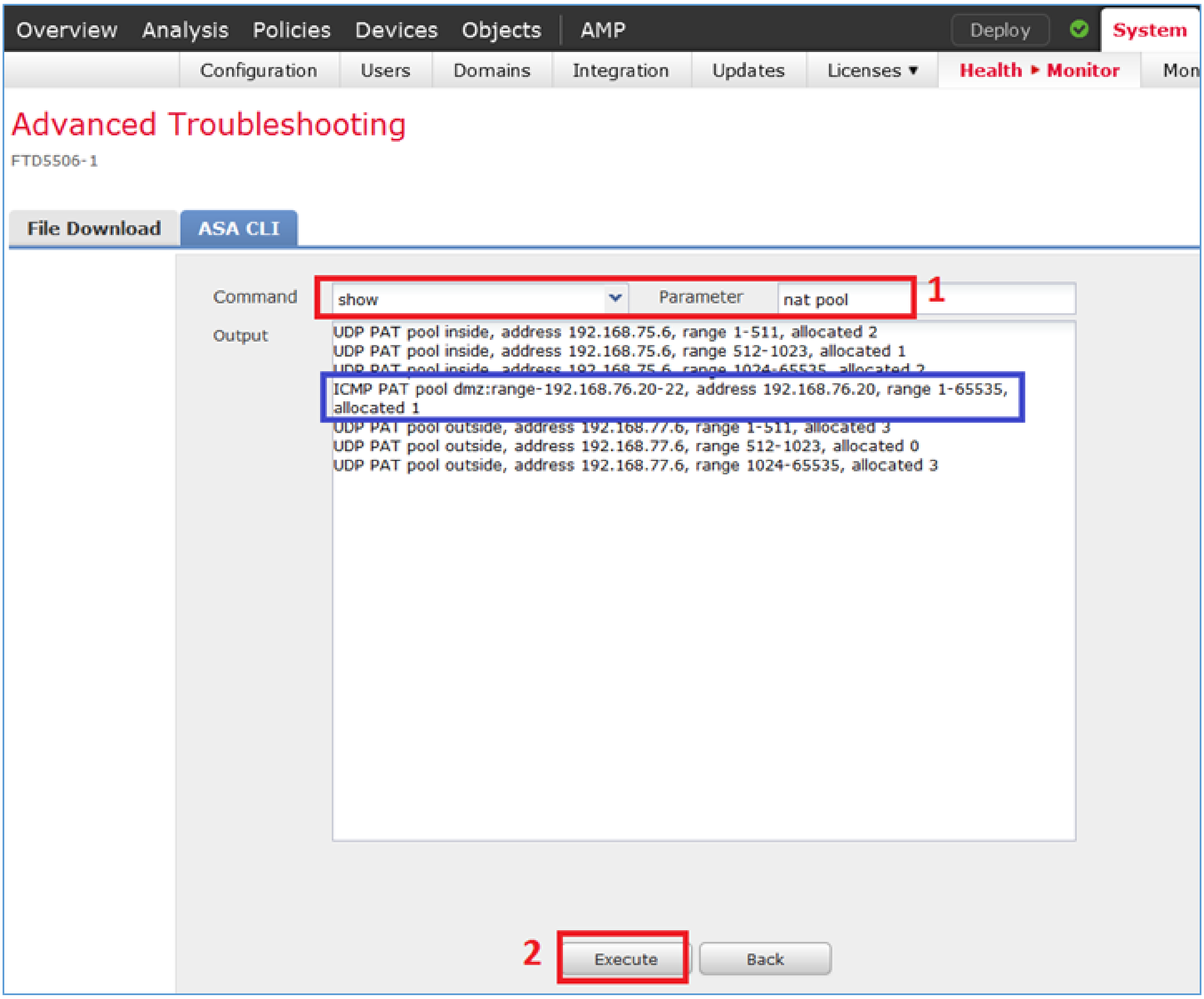
La verificación se ha explicado en las secciones de tareas individuales.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Abra la página **Advanced Troubleshooting** en el FMC, ejecute el packet-tracer y luego ejecute el comando **show nat pool**.

Observe la entrada que utiliza todo el rango como se muestra en la imagen.



Command: show
Parameter: nat pool

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

Información Relacionada

- Todas las versiones de la guía de configuración de Cisco Firepower Management Center se pueden encontrar aquí:

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html#id_47280

- Cisco Global Technical Assistance Center (TAC) recomienda encarecidamente esta guía visual para obtener un conocimiento práctico en profundidad de las tecnologías de seguridad de última generación de Cisco Firepower, que incluye las mencionadas en este artículo:

http://www.ciscopress.com/title/9781587144806

- Para todas las notas técnicas sobre configuración y resolución de problemas relacionadas con las tecnologías Firepower:

https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-

home.html

- **Soporte Técnico y Documentación - Cisco Systems**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).