Configuration et vérification de la NAT sur FTD

Contenu

Introduction

Ce document décrit comment configurer et vérifier la traduction d'adresses réseau (NAT) de base sur Firepower Threat Defense (FTD).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASA5506X qui exécute le code FTD 6.1.0-226
- FireSIGHT Management Center (FMC) qui exécute la version 6.1.0-226
- 3 hôtes Windows 7
- Routeur Cisco IOS® 3925 qui exécute un VPN LAN à LAN (L2L)

Durée des travaux pratiques : 1 heure.

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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

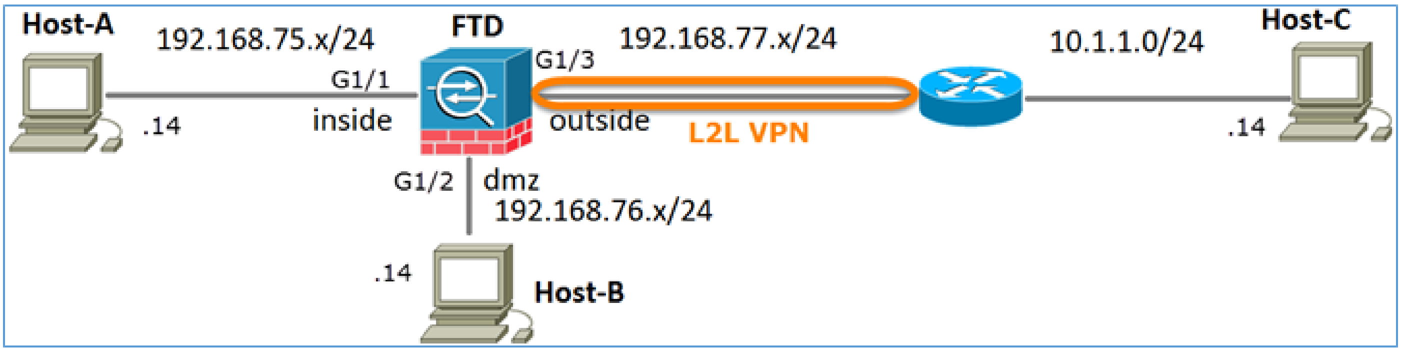
FTD prend en charge les mêmes options de configuration NAT que l'appliance ASA classique :

- Règles NAT antérieures : équivalent à deux fois la NAT (section 1) sur un ASA classique
- Règles NAT automatiques - Section 2 sur ASA classique
- Règles NAT après : équivalent à deux fois la NAT (section 3) sur un ASA classique

Étant donné que la configuration FTD est effectuée à partir du FMC lorsqu'il s'agit de la configuration NAT, il est nécessaire de connaître l'interface utilisateur graphique du FMC et les différentes options de configuration.

Configuration

Diagramme du réseau

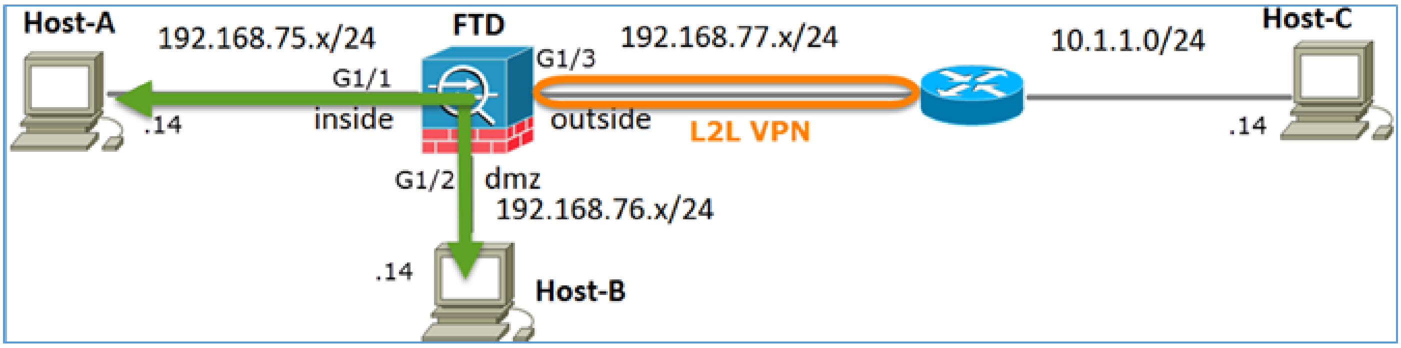


Tâche 1 : configuration de la fonction NAT statique sur FTD

Configurez la fonction NAT conformément à ces exigences :

Nom de stratégie NAT	Le nom du périphérique FTD
Règle NAT	Règle NAT manuelle
Type NAT	static
Insérer	Àla section 1
Interface source	intérieur*
Interface de destination	dmz*
Source initiale	192.168.75.14
Source traduite	192.168.76.100

*Utiliser les zones de sécurité pour la règle NAT



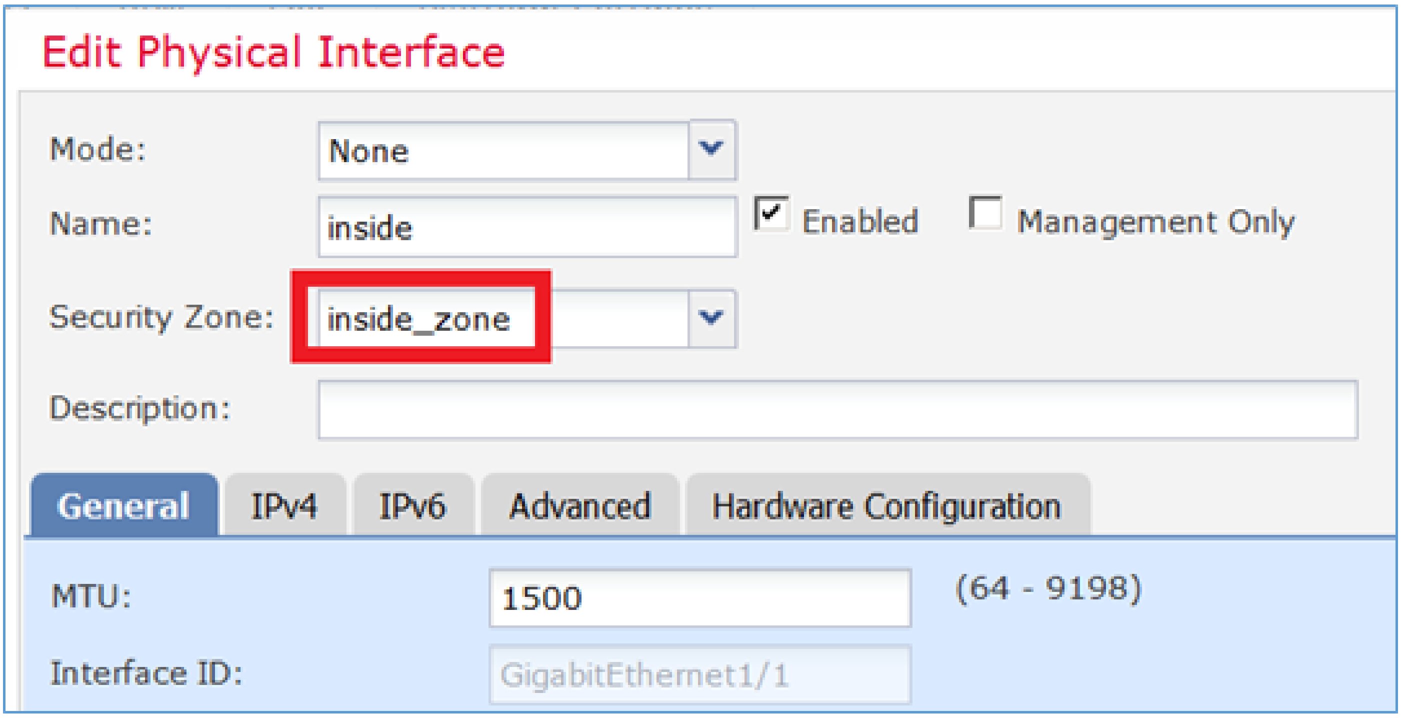
NAT statique

Solution :

Sur un ASA classique, vous devez utiliser nameif dans les règles NAT. Sur FTD, vous devez utiliser des zones de sécurité ou des groupes d'interfaces.

Étape 1. Attribution d’interfaces aux zones de sécurité/groupes d’interfaces

Dans cette tâche, il est décidé d'attribuer les interfaces FTD utilisées pour la NAT aux zones de sécurité. Vous pouvez également les affecter à des groupes d'interfaces, comme illustré dans l'image.



Edit Physical Interface

Mode: None

Name: inside ☑ Enabled □ Management Only

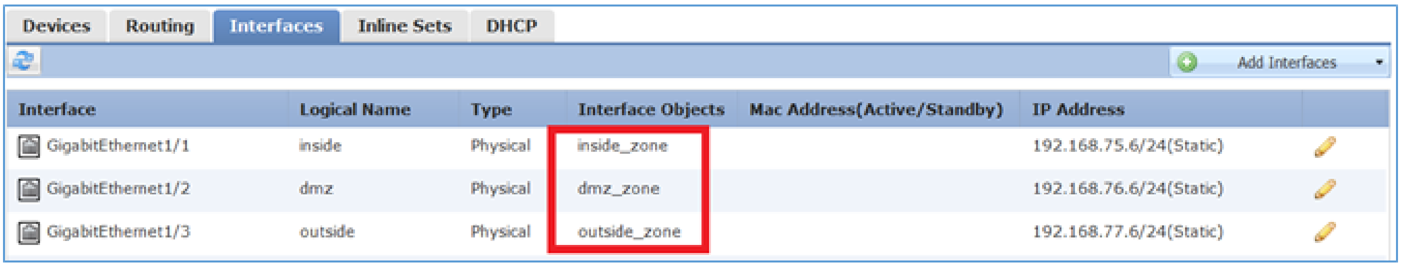
Security Zone: inside_zone

Description:

MTU: 1500 (64 - 9198)

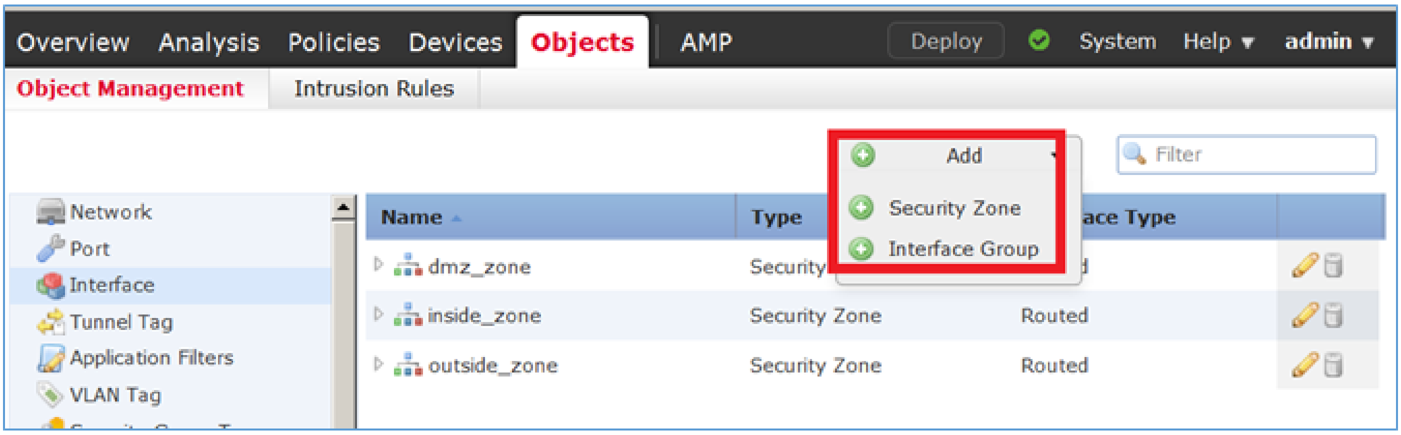
Interface ID: GigabitEthernet1/1

Étape 2. Le résultat est tel qu’illustré dans l’image.



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)

Étape 3. Vous pouvez créer/modifier des groupes d'interfaces et des zones de sécurité à partir de la page **Objets > Gestion des objets**, comme illustré dans l'image.

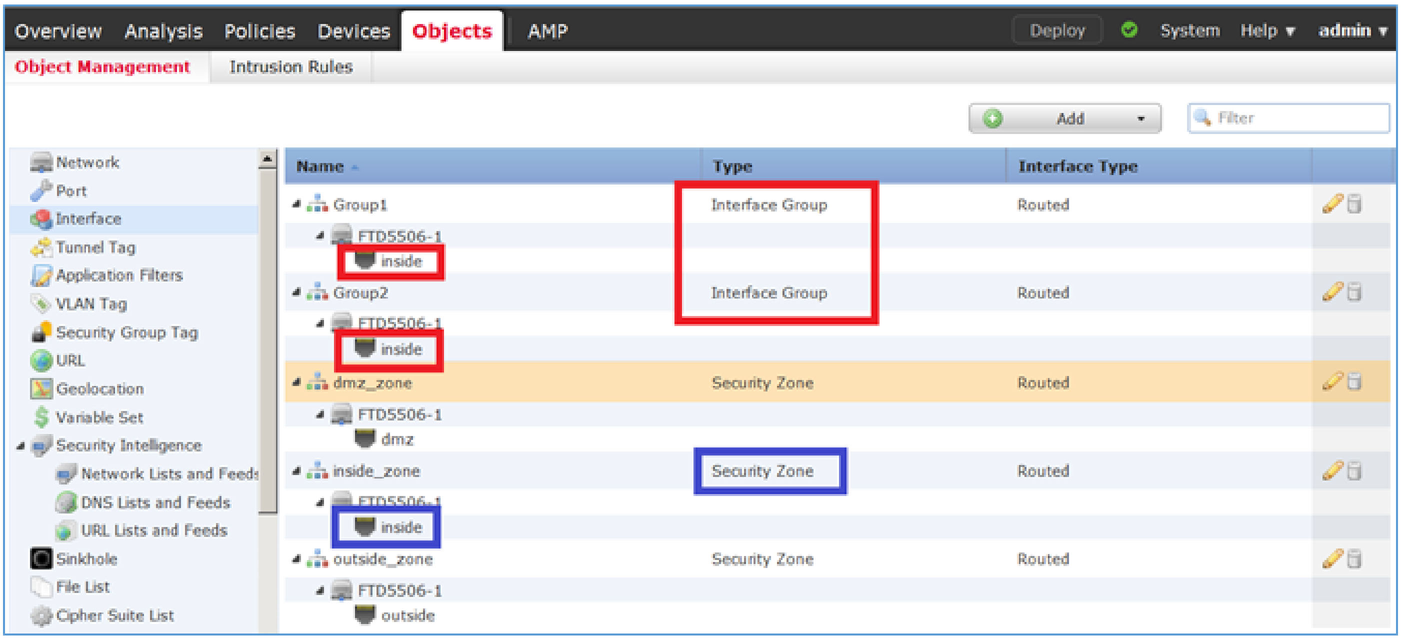


Name	Type	ace Type
dmz_zone	Security	d
inside_zone	Security Zone	Routed
outside_zone	Security Zone	Routed

Zones de sécurité et groupes d'interfaces

La principale différence entre les zones de sécurité et les groupes d'interfaces est qu'une interface peut appartenir à une seule zone de sécurité, mais à plusieurs groupes d'interfaces. Ainsi, les groupes d'interfaces offrent plus de flexibilité.

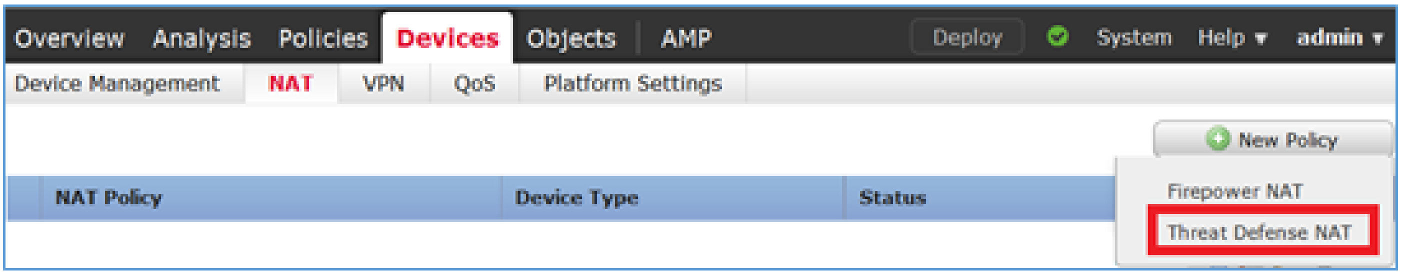
Vous pouvez voir que l'interface **interne** appartient à deux groupes d'interfaces différents, mais à une seule zone de sécurité comme illustré dans l'image.



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		

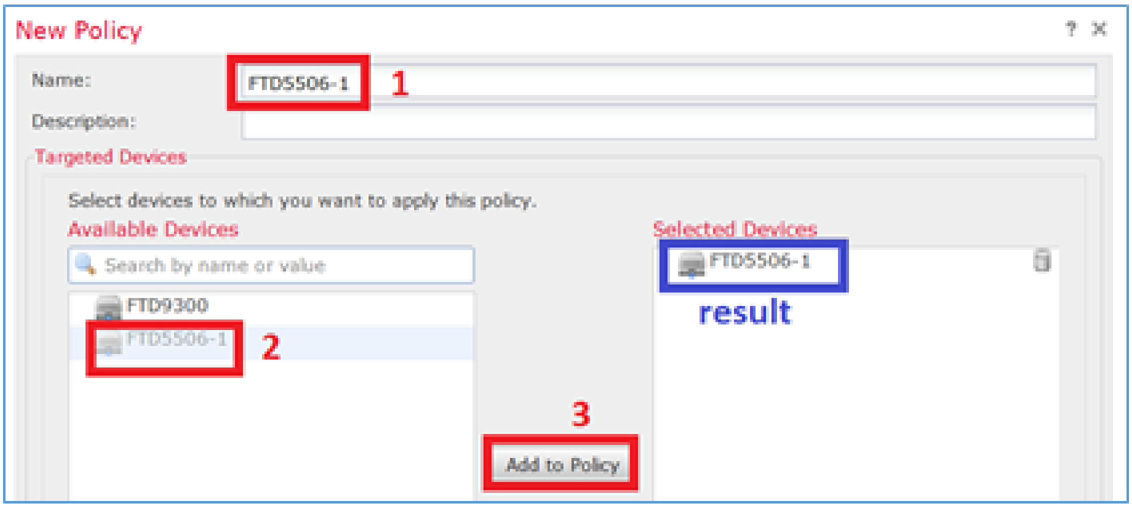
Étape 4 : configuration de la fonction NAT statique sur FTD

Accédez à **Devices > NAT** et créez une stratégie NAT. Sélectionnez **New Policy > Threat Defense NAT** comme indiqué dans l'image.



NAT Policy	Device Type	Status

Étape 5. Spécifiez le nom de la stratégie et attribuez-le à un équipement cible, comme illustré dans l'image.



New Policy

Name: FTD5506-1

Description:

Targeted Devices

Select devices to which you want to apply this policy.

Available Devices

Selected Devices

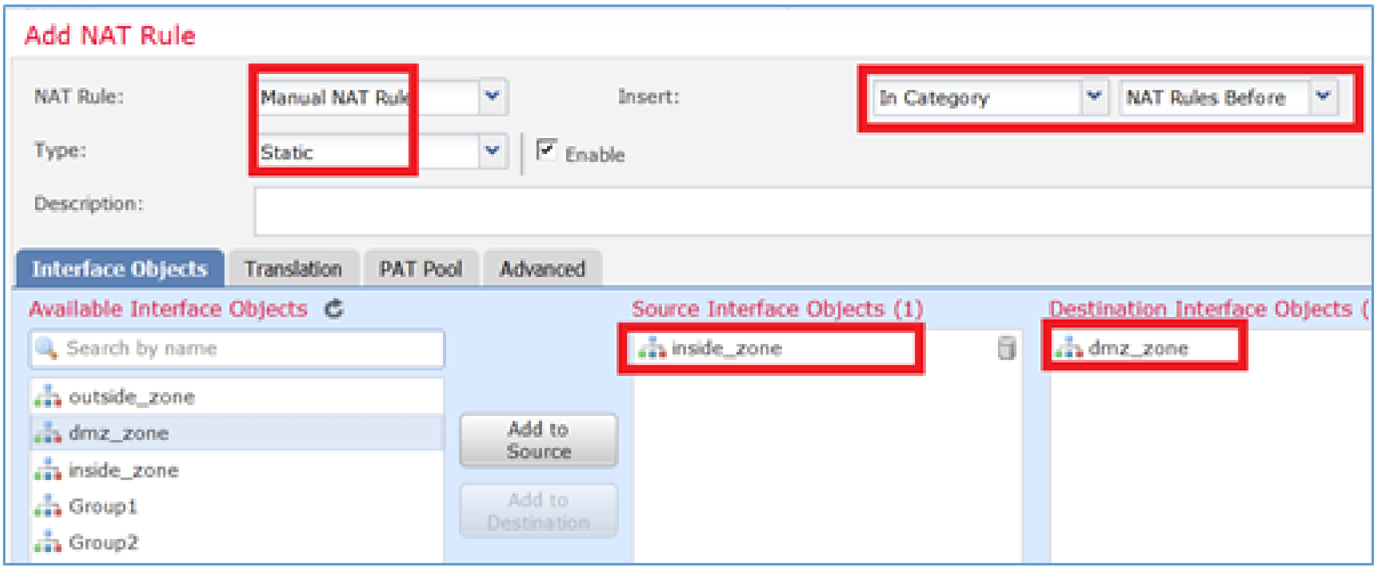
FTD9300

FTD5506-1

FTD5506-1

Étape 6. Ajouter une règle NAT à la stratégie, cliquez sur **Add Rule.**

Spécifiez-les en fonction des exigences des tâches, comme indiqué dans les images.



Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category | NAT Rules Before

Type: Static

☑ Enable

Description:

Available Interface Objects

Source Interface Objects (1)

Destination Interface Objects (

outside_zone

dmz_zone

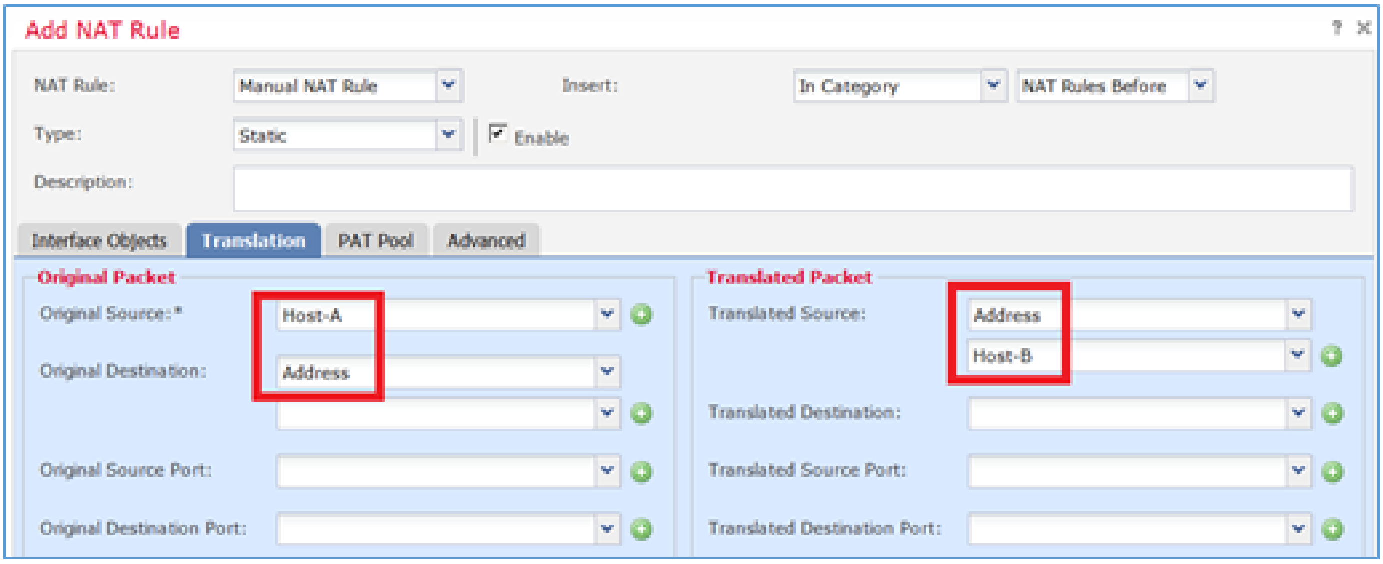
inside_zone

Group1

Group2

Source Interface Objects: 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:

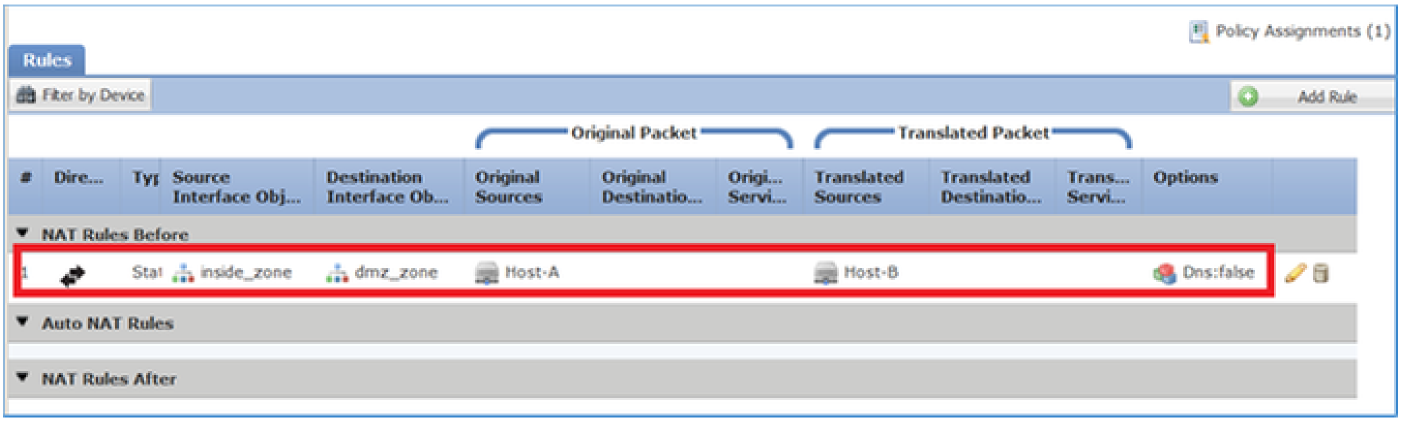
Hôte-A = 192.168.75.14

Hôte-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
```

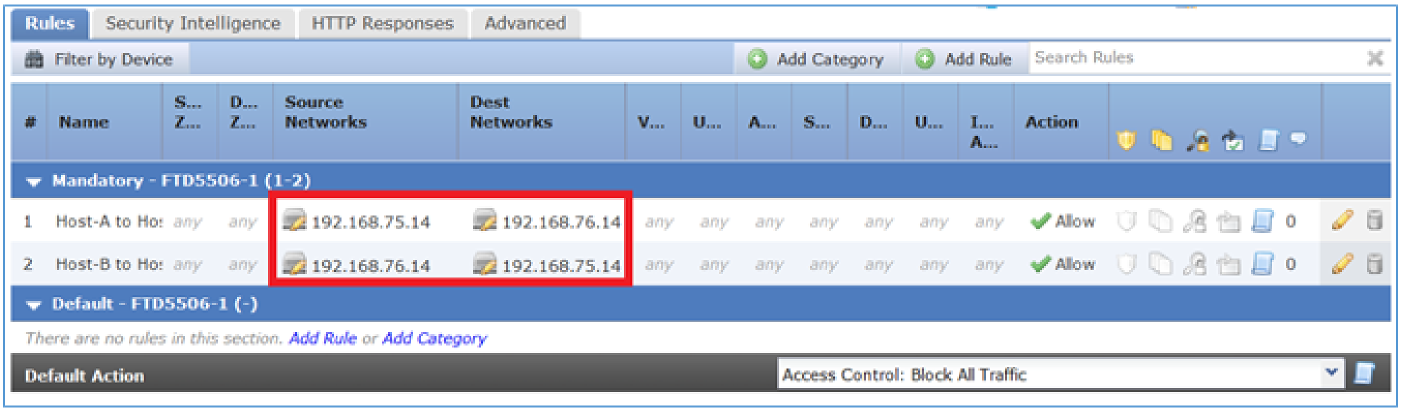
> **Avertissement :** Si vous configurez la NAT statique et spécifiez une interface comme source traduite, alors tout le trafic destiné à l'adresse IP de l'interface est redirigé. Les utilisateurs peuvent ne pas pouvoir accéder à un service activé sur l'interface mappée. Les protocoles de routage tels que OSPF et EIGRP sont des exemples de tels services.

Étape 7. Le résultat est tel qu'illustré dans l'image.



					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											

Étape 8. Assurez-vous qu'une stratégie de contrôle d'accès autorise l'hôte B à accéder à l'hôte A et vice versa. Souvenez-vous que la fonction NAT statique est bidirectionnelle par défaut. Comme pour les ASA classiques, notez l'utilisation d'adresses IP réelles.Ceci est attendu car dans ces travaux pratiques, LINA exécute le code 9.6.1.x comme illustré dans l'image.



#	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					

Vérification :

Àpartir de LINA CLI :

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

La règle NAT a été insérée dans la section 1 comme prévu :

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

Note: Les 2 xlate qui sont créés en arrière-plan.

```
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
```

Les tables NAT ASP :

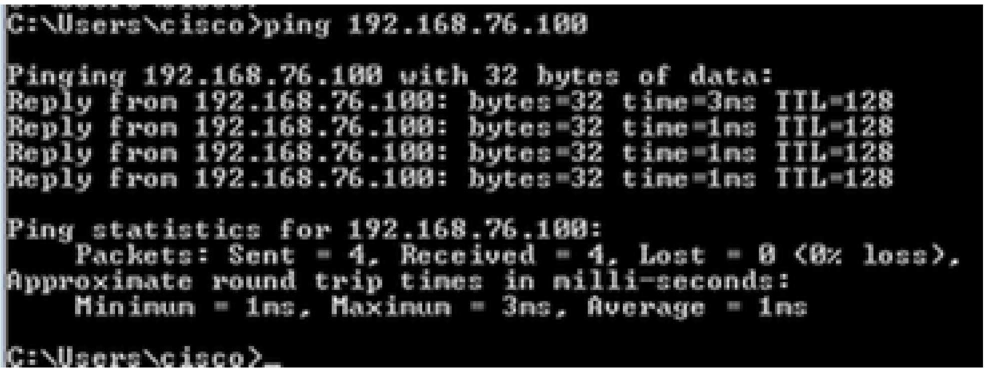
```
firepower# show asp table classify domain nat

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
```

Activez la capture avec les détails de trace sur FTD et envoyez une requête ping de l’hôte A à l’hôte B, comme illustré dans l’image.

```
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>_
```

Le nombre d'occurrences se trouve dans les tables 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 capture de paquets montre :

```
firepower# show capture DMZ
8 packets captured
   1: 17:38:26.324812       192.168.76.14 > 192.168.76.100: icmp: echo request
   2: 17:38:26.326505       192.168.76.100 > 192.168.76.14: icmp: echo reply
   3: 17:38:27.317991       192.168.76.14 > 192.168.76.100: icmp: echo request
   4: 17:38:27.319456       192.168.76.100 > 192.168.76.14: icmp: echo reply
   5: 17:38:28.316344       192.168.76.14 > 192.168.76.100: icmp: echo request
   6: 17:38:28.317824       192.168.76.100 > 192.168.76.14: icmp: echo reply
   7: 17:38:29.330518       192.168.76.14 > 192.168.76.100: icmp: echo request
   8: 17:38:29.331983       192.168.76.100 > 192.168.76.14: icmp: echo reply
8 packets shown
```

Traces d’un paquet (les points importants sont mis en surbrillance).

Note: ID de la règle NAT et sa corrélation avec la table 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
```

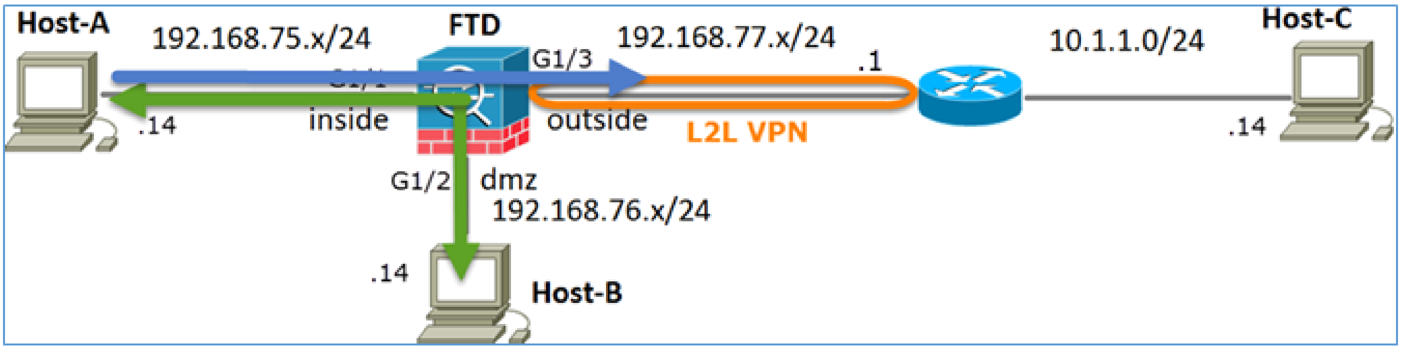
```
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.75.14 using egress ifc  inside

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
```

Tâche 2 : configuration de la traduction d’adresses de port (PAT) sur FTD

Configurez la fonction NAT conformément à ces exigences :

Règle NAT	Règle NAT manuelle
Type NAT	Dynamique
Insérer	Àla section 1
Interface source	intérieur*
Interface de destination	extérieur*
Source initiale	192.168.75.0/24
Source traduite	Interface externe (PAT)

*Utiliser les zones de sécurité pour la règle NAT

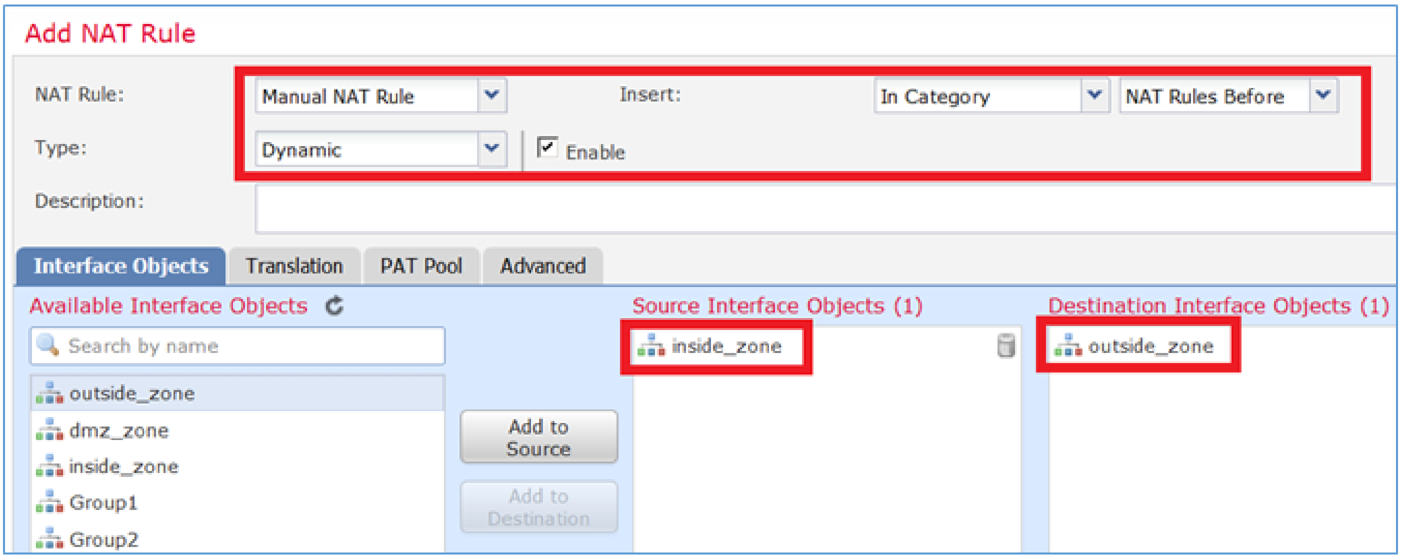


NAT statique

TAPE

Solution :

Étape 1 : ajout d’une deuxième règle NAT et configuration en fonction des exigences de la tâche, comme illustré dans l’image


Add NAT Rule

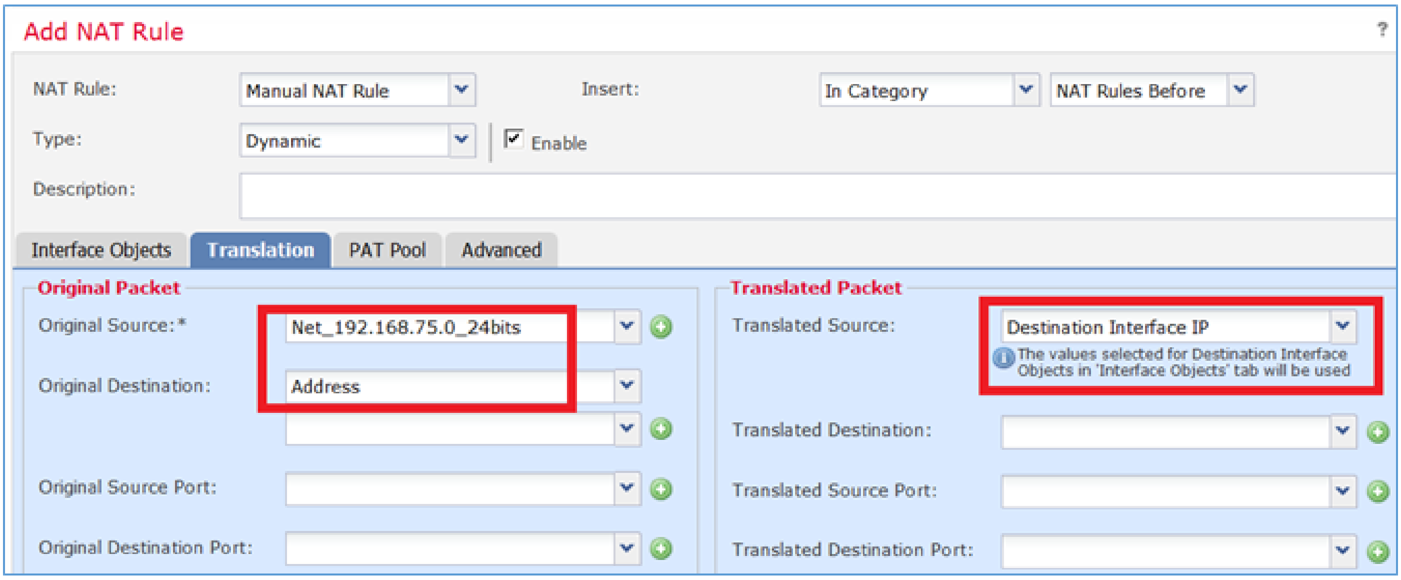
NAT Rule: Manual NAT Rule
Insert: In Category — NAT Rules Before
Type: Dynamic ☑ Enable
Description:

Available Interface Objects

Source Interface Objects (1): inside_zone

Destination Interface Objects (1): outside_zone

Étape 2. Voici comment la fonction PAT est configurée, comme illustré dans l’image.

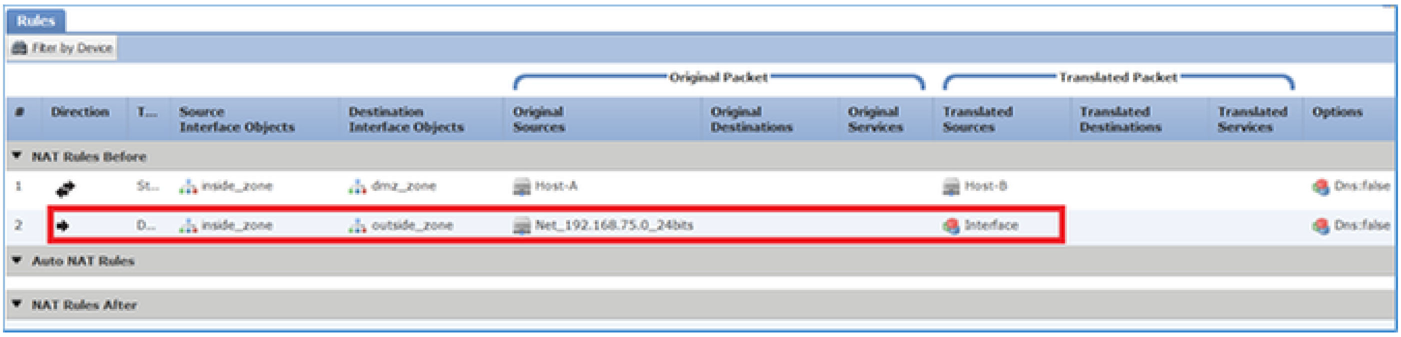

Add NAT Rule

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:

Étape 3. Le résultat est tel qu'illustré dans l'image.



					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											

Étape 4. Pour le reste de ces travaux pratiques, configurez la stratégie de contrôle d'accès pour autoriser l'acheminement de tout le trafic.

Vérification :

Configuration 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
```

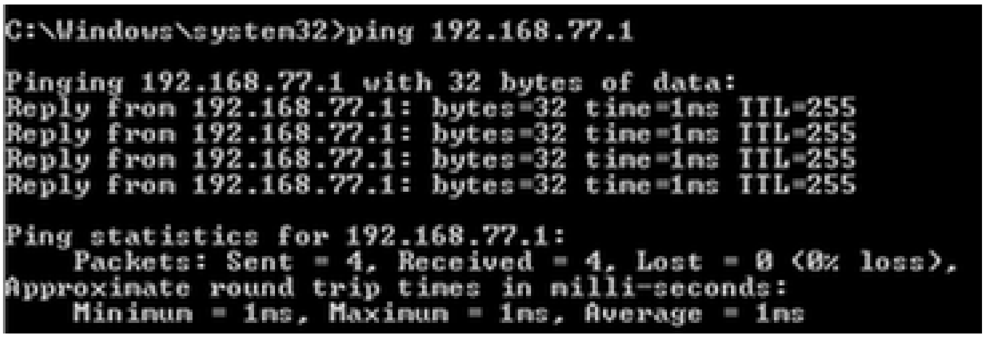
Àpartir de LINA CLI, notez la nouvelle entrée :

```
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
```

Activez la capture sur l'interface interne et externe. Sur la capture interne enable trace :

```
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
```

Envoyez une requête ping à partir de l'hôte A (192.168.75.14) vers l'adresse IP 192.168.77.1, comme indiqué dans l'image.



```
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
```

Dans les captures LINA, vous pouvez voir la traduction 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
```

Les traces d'un paquet avec les sections importantes mises en évidence :

```
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
```

Le xlate dynamique a été créé (notez les indicateurs "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
```

Dans les journaux LINA, vous voyez :

```
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
```

Sections 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
```

Les tableaux ASP montrent :

```
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
```

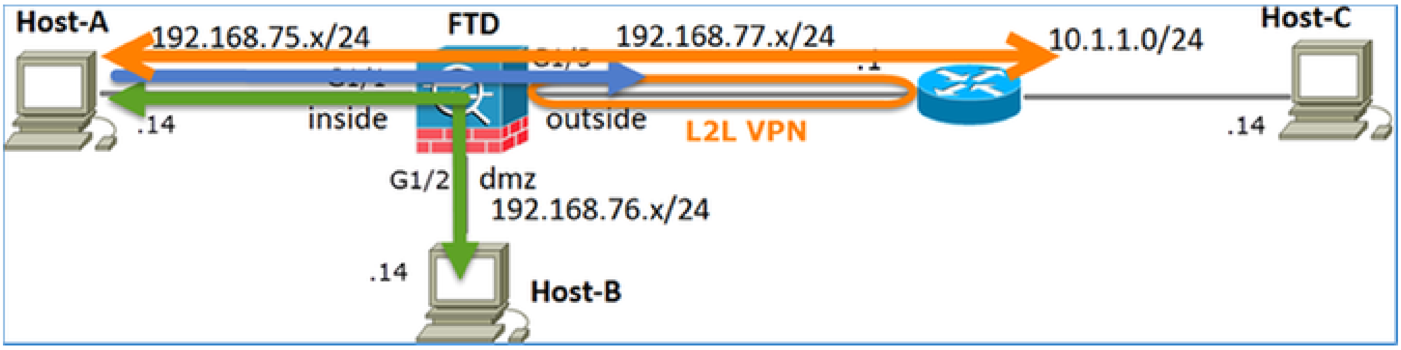
```
firepower# show asp table classify domain nat-reverse

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
```

Tâche 3 : configuration de l'exemption NAT sur FTD

Configurez la fonction NAT conformément à ces exigences :

Règle NAT	Règle NAT manuelle
Type NAT	static
Insérer	Dans la section 1 ci-dessus, toutes les règles existantes
Interface source	intérieur*
Interface de destination	extérieur*
Source initiale	192.168.75.0/24
Source traduite	192.168.75.0/24
Destination initiale	10.1.1.0/24
Destination traduite	10.1.1.0/24

*Utiliser les zones de sécurité pour la règle NAT



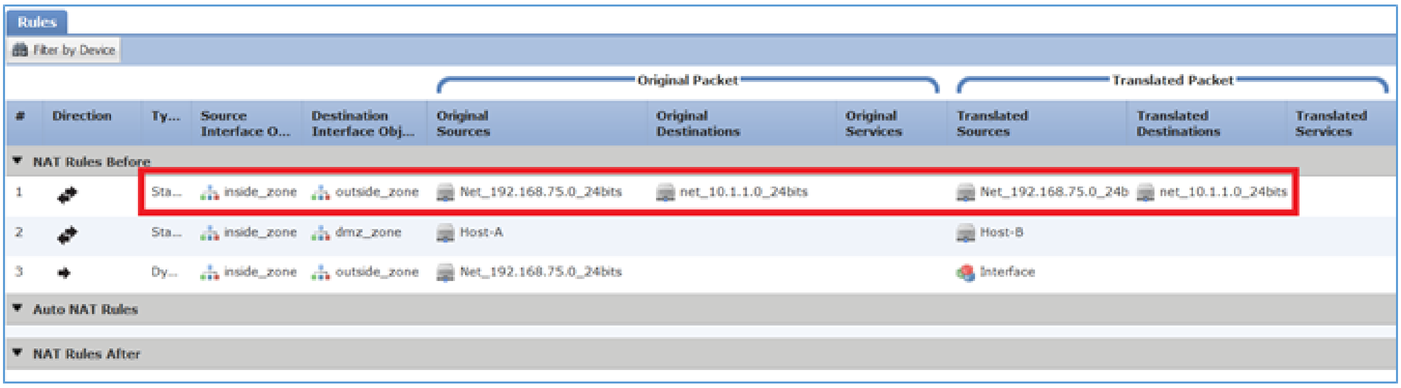
NAT statique

TAPE

Exemption NAT

Solution :

Étape 1 : ajout d'une troisième règle NAT et configuration des exigences par tâche, comme illustré dans l'image.

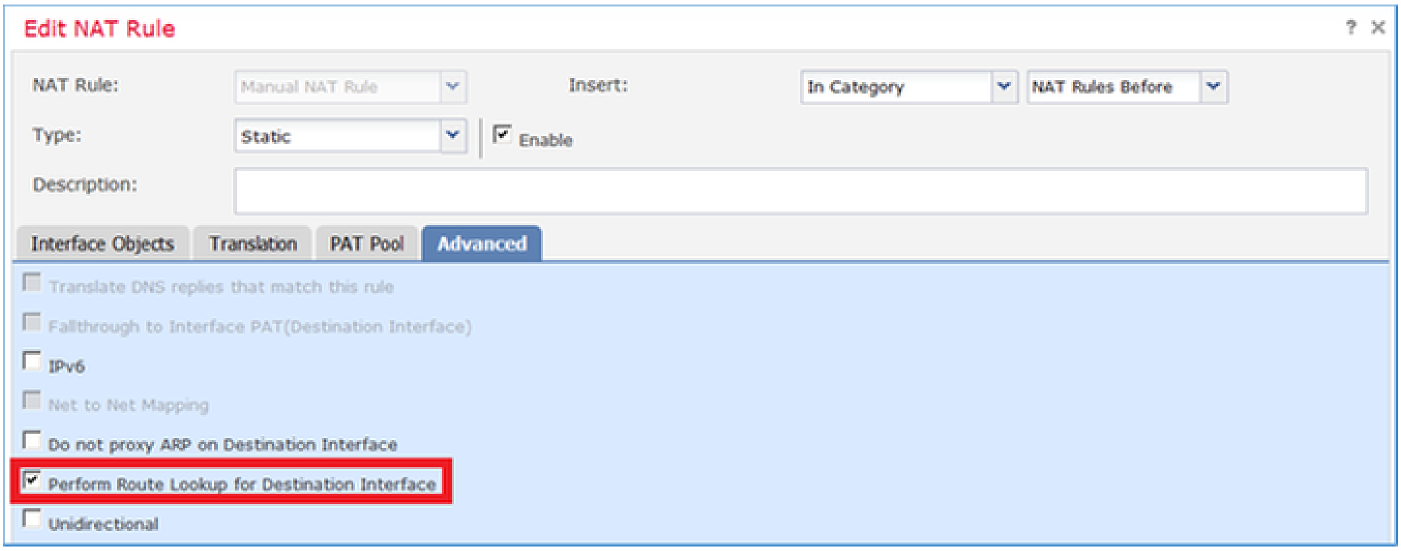


					Original Packet			Translated Packet		
#	Direction	Ty...	Source Interface O...	Destination Interface Obj...	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services
▼ NAT Rules Before										
1	⇄	Sta...	inside_zone	outside_zone	Net_192.168.75.0_24bits	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										

Étape 2 : recherche de route pour déterminer l'interface de sortie

> **Note**: Pour les règles NAT d'identité, comme celle que vous avez ajoutée, vous pouvez modifier la façon dont l'interface de sortie est déterminée et utiliser la recherche de route

normale comme illustré dans l'image.



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

Vérification :

```
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
```

Exécutez Packet Tracer pour le trafic non VPN provenant du réseau interne. La règle PAT est utilisée comme prévu :

```
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
```

Exécutez Packet Tracer pour le trafic qui doit passer par le tunnel VPN (exécutez-le deux fois depuis la première tentative d'activation du tunnel VPN).

> **Note**: Vous devez sélectionner la règle d'exemption NAT.

Première tentative Packet Tracer :

```
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
```

Deuxième tentative Packet Tracer :

```
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
```

Vérification du nombre d'occurrences 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
```

Tâche 4. Configuration de la fonction NAT d’objet sur FTD

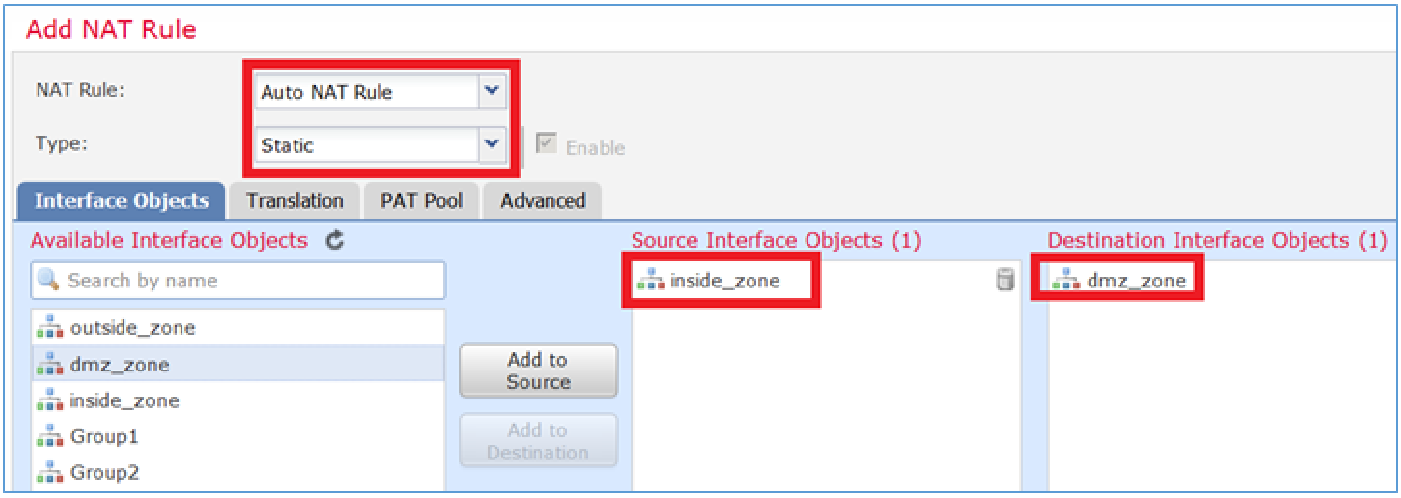
Configurez la fonction NAT conformément à ces exigences :

Règle NAT	Règle NAT automatique
Type NAT	static
Insérer	Àla section 2
Interface source	intérieur*
Interface de destination	dmz*
Source initiale	192.168.75.99
Source traduite	192.168.76.99
Traduire les réponses DNS qui correspondent à cette règle	Activée

*Utiliser les zones de sécurité pour la règle NAT

Solution :

Étape 1 : configuration de la règle en fonction des exigences de la tâche, comme illustré dans les images



Add NAT Rule

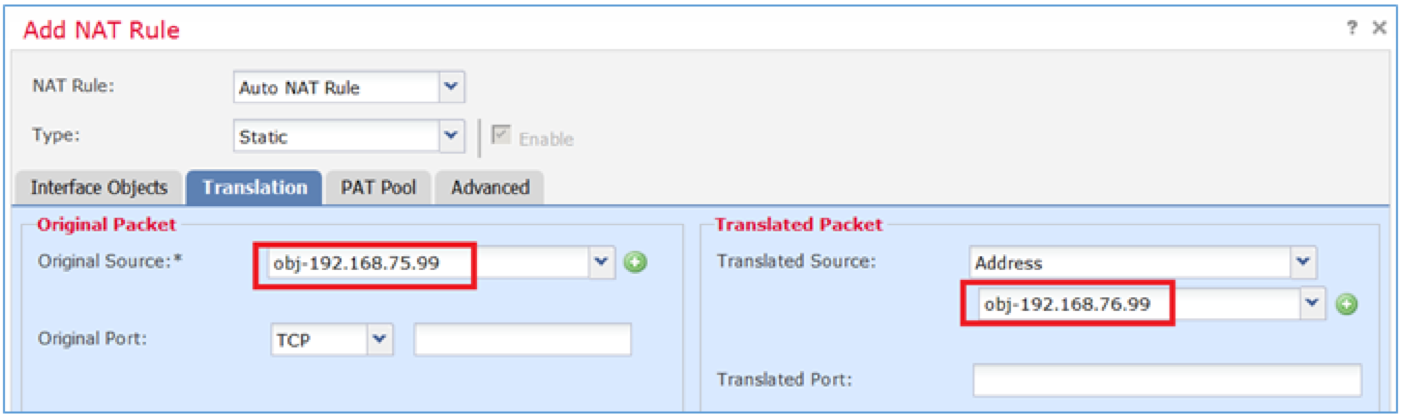
NAT Rule: Auto NAT Rule

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

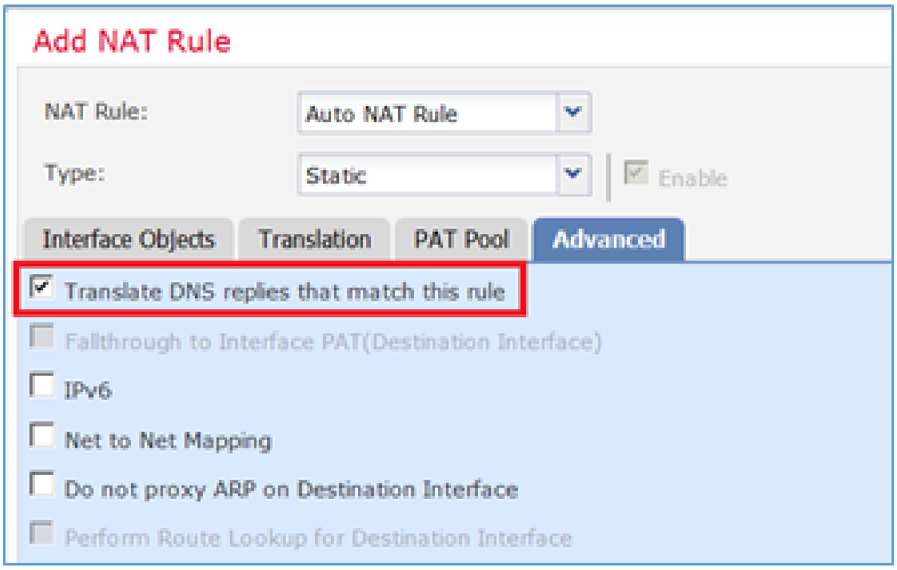
Original Port: TCP

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)

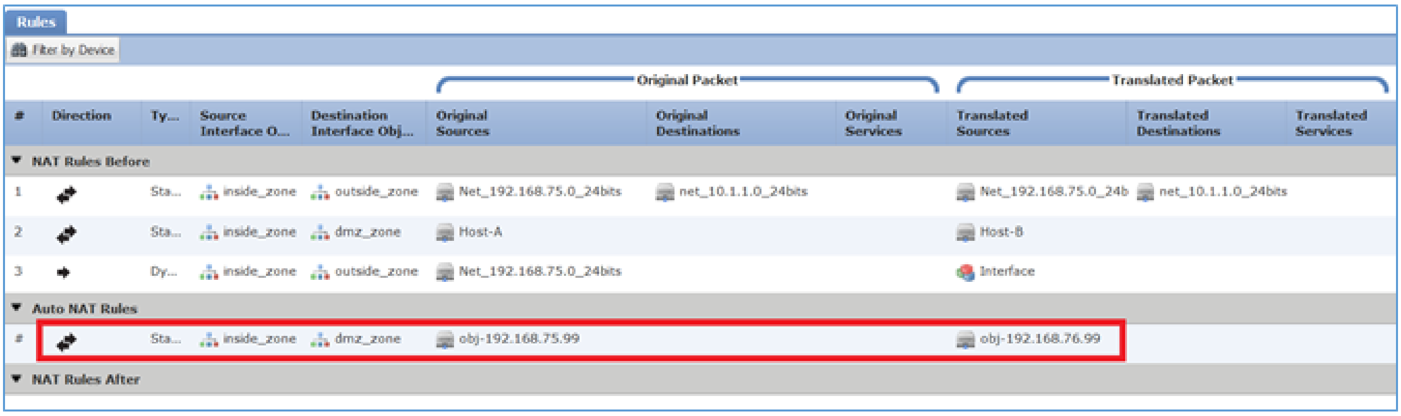
☐ IPv6

☐ Net to Net Mapping

☐ Do not proxy ARP on Destination Interface

☐ Perform Route Lookup for Destination Interface

Étape 2. Le résultat est tel qu'illustré dans l'image.



					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										

Vérification :

```
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
```

Vérification avec 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
```

Tâche 5. Configuration du pool PAT sur FTD

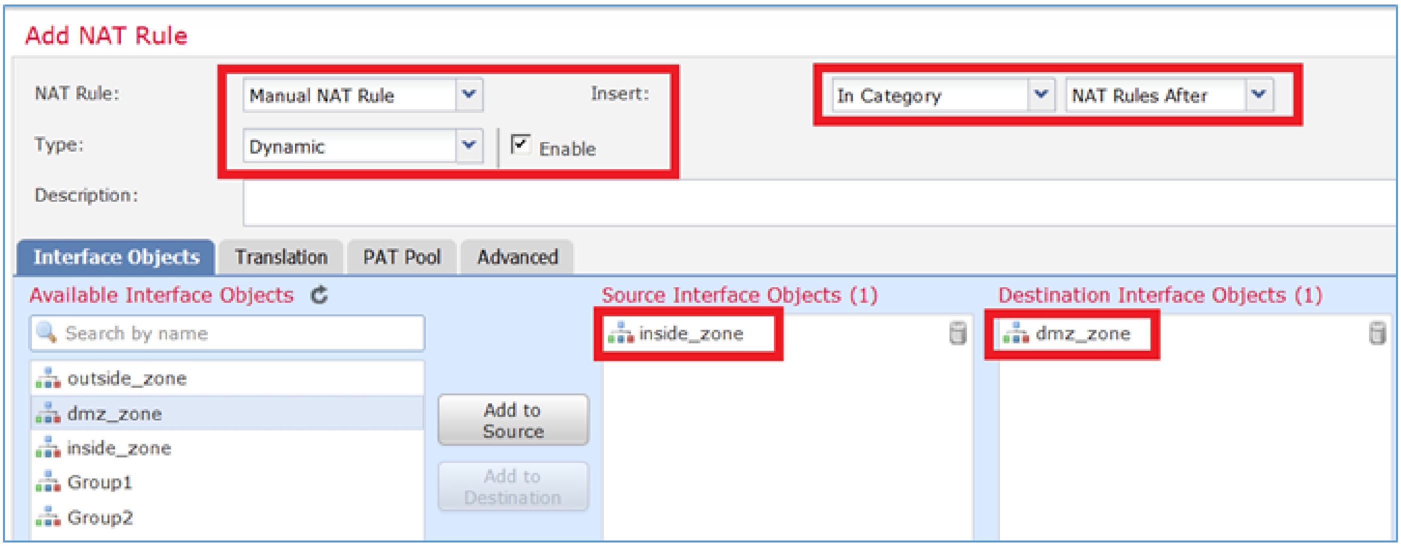
Configurez la fonction NAT conformément à ces exigences :

Règle NAT	Règle NAT manuelle
Type NAT	Dynamique
Insérer	Dans la section 3
Interface source	intérieur*
Interface de destination	dmz*
Source initiale	192.168.75.0/24
Source traduite	192.168.76.20-22
Utiliser la plage complète (1-65535)	Activée

*Utiliser les zones de sécurité pour la règle NAT

Solution :

Étape 1 : configuration de la règle en fonction des exigences des tâches, comme illustré dans les images



Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category | NAT Rules After

Type: Dynamic ☑ Enable

Description:

Available Interface Objects

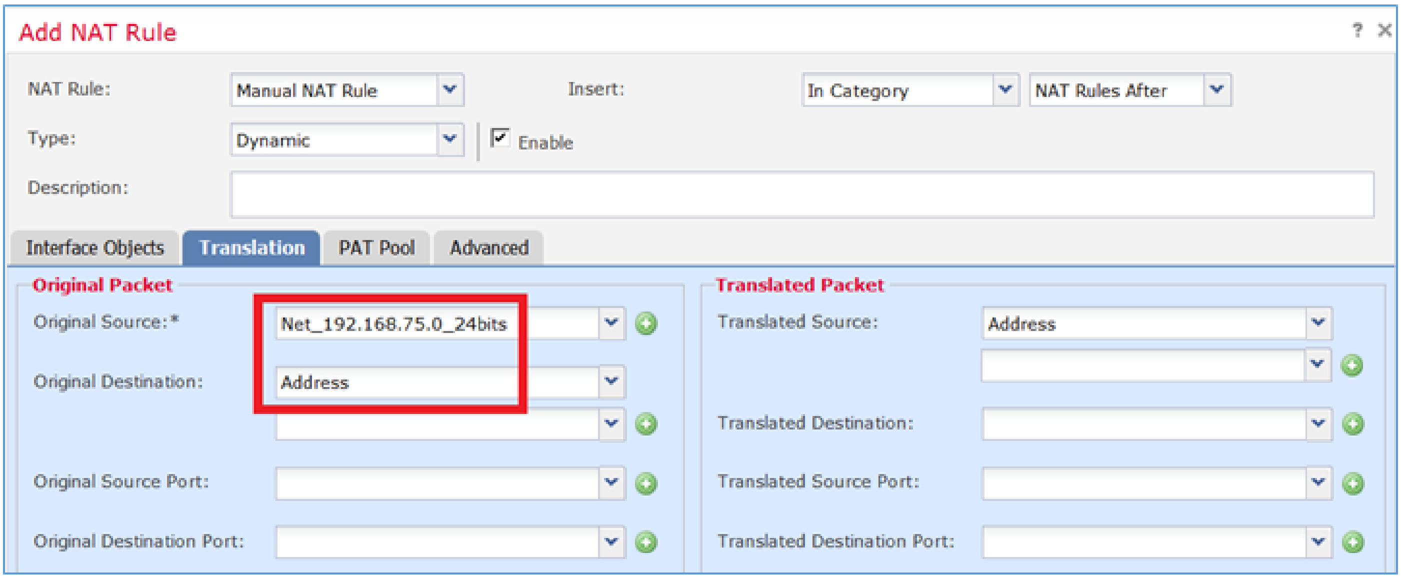
- outside_zone
- dmz_zone
- inside_zone
- Group1
- Group2

Source Interface Objects (1)

- inside_zone

Destination Interface Objects (1)

- dmz_zone



Add NAT Rule

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

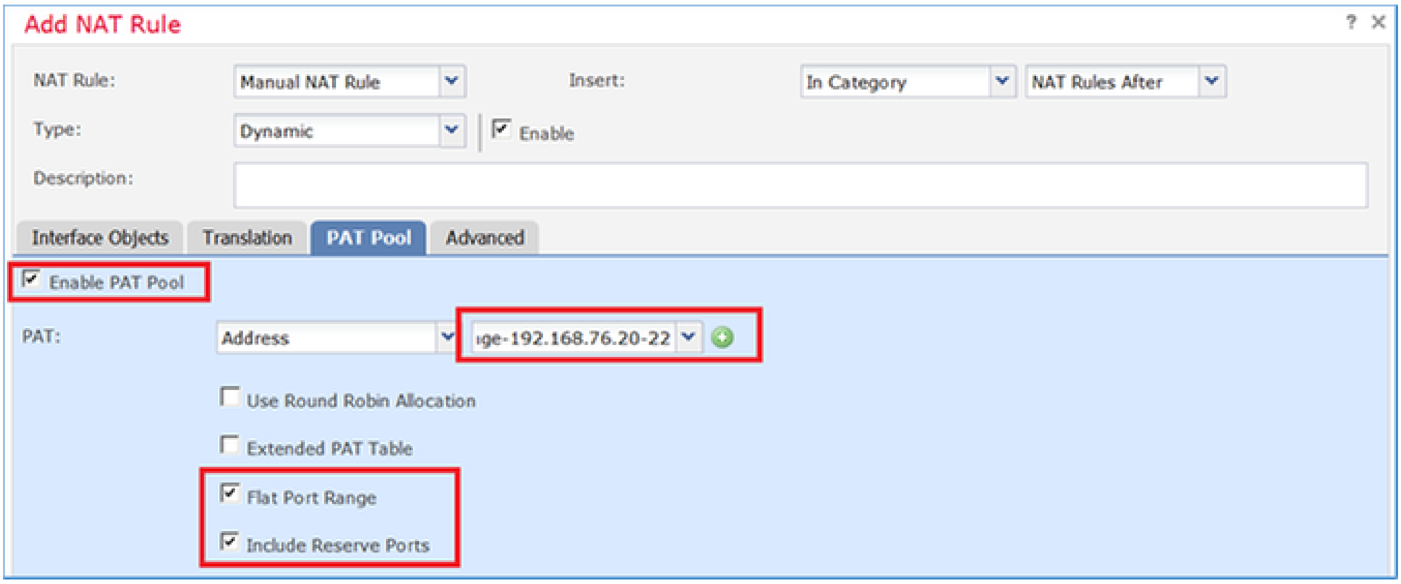
Original Packet

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:	

Étape 2 : activation de la **plage de ports plats** avec **Include Reserver Ports** qui permet d'utiliser la plage complète (1-65535) comme illustré dans l'image



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

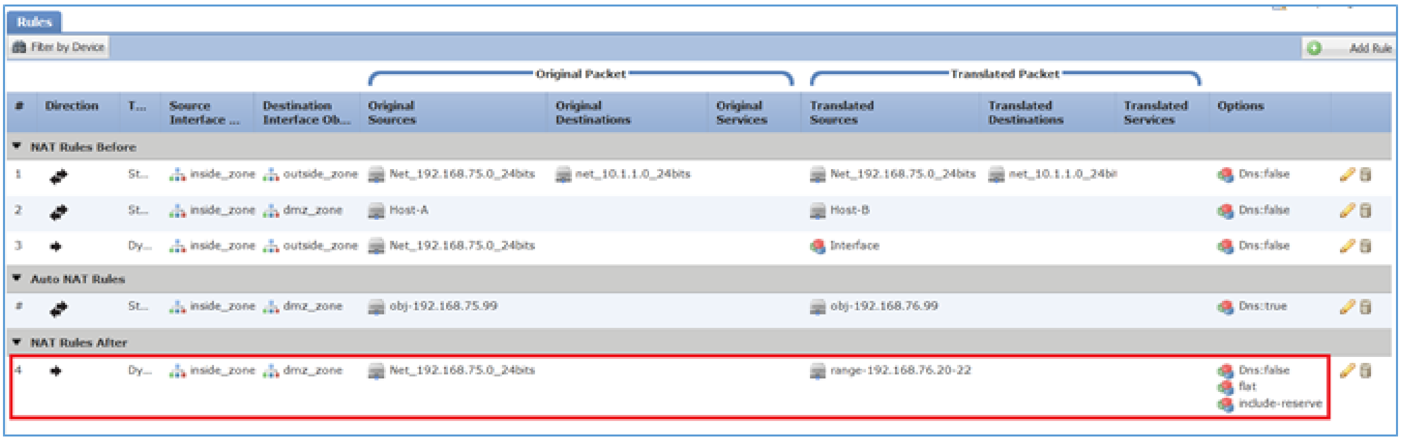
☐ Use Round Robin Allocation

☐ Extended PAT Table

☑ Flat Port Range

☑ Include Reserve Ports

Étape 3. Le résultat est tel qu'illustré dans l'image.



						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

Vérification :

```
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 règle se trouve à la section 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
```

Vérification de Packet-Tracer :

```
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
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

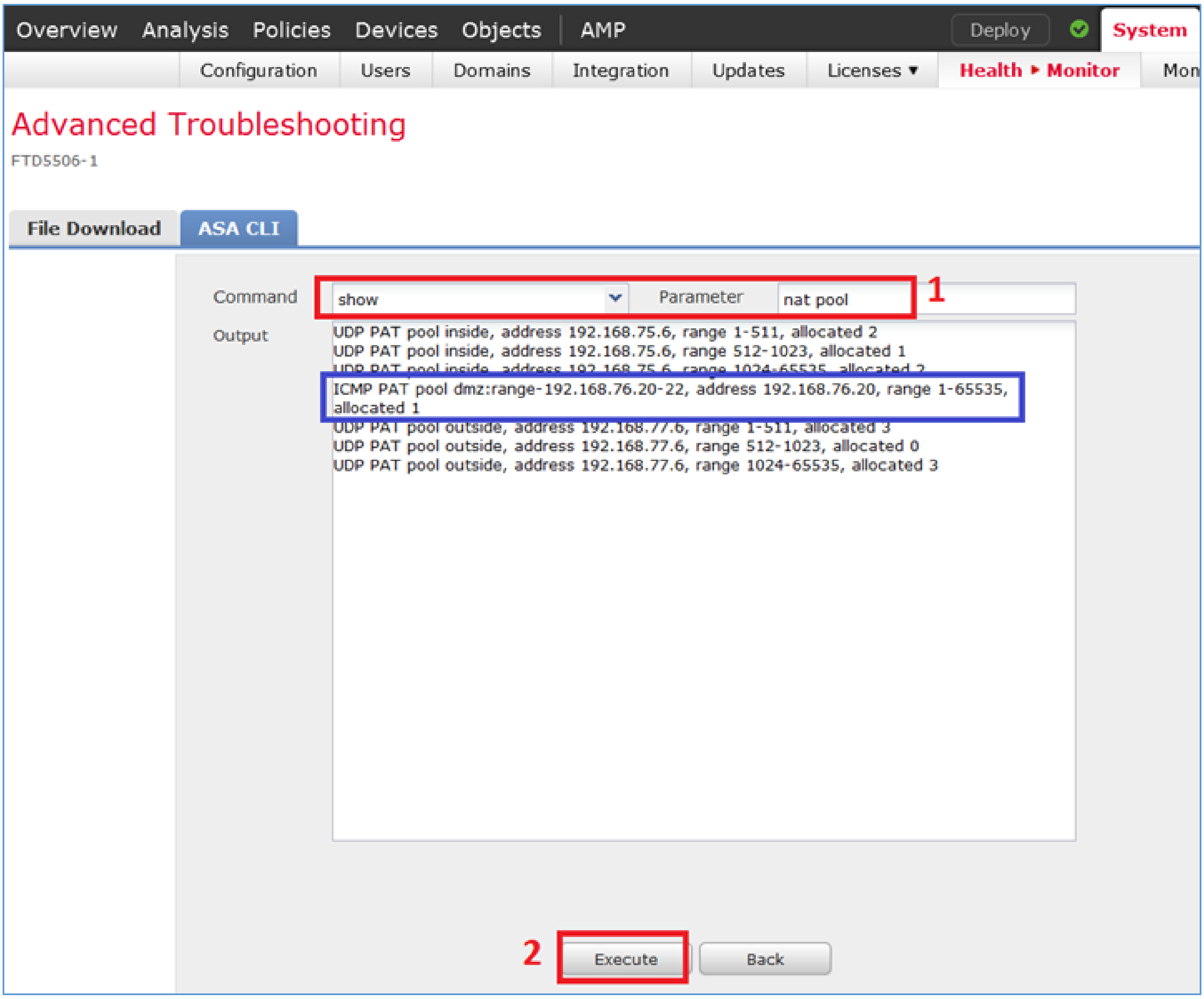
La vérification a été expliquée dans les sections des tâches individuelles.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Ouvrez la page **Advanced Troubleshooting** sur le FMC, exécutez le traceur de paquets, puis exécutez la commande **show nat pool**.

Notez l'entrée qui utilise la plage entière comme illustré dans l'image.



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
```

Informations connexes

- Toutes les versions du guide de configuration de Cisco Firepower Management Center sont disponibles ici :

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

- Le Centre d'assistance technique mondial (TAC) de Cisco recommande vivement ce guide visuel pour des connaissances pratiques approfondies sur les technologies de sécurité de nouvelle génération Cisco Firepower, notamment celles mentionnées dans cet article :

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

- Pour toutes les notes techniques de configuration et de dépannage relatives aux technologies Firepower :

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

home.html

- **Support et documentation techniques - Cisco Systems**