

Configureer en controleer NAT op FTD

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Taak 1. Statische NAT op FTD configureren](#)

[Taak 2. Poortadresomzetting \(PAT\) op FTD configureren](#)

[Taak 3. NAT-vrijstelling op FTD configureren](#)

[Taak 4. Object NAT op FTD configureren](#)

[Taak 5. PAT-pool op FTD configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u basisnetwerkadresomzetting (NAT) kunt configureren en verifiëren bij Firepower Threat Defence (FTD).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASA 5506X die FTD-code 6.1.0-26 gebruikt
- FireSIGHT Management Center (FMC) voor gebruik van 6.1.0-226
- 3 Windows 7-hosts
- Cisco IOS® 3925 router die LAN-to-LAN (L2L) VPN uitvoert

Tijd van voltooiing van lab: 1 uur.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

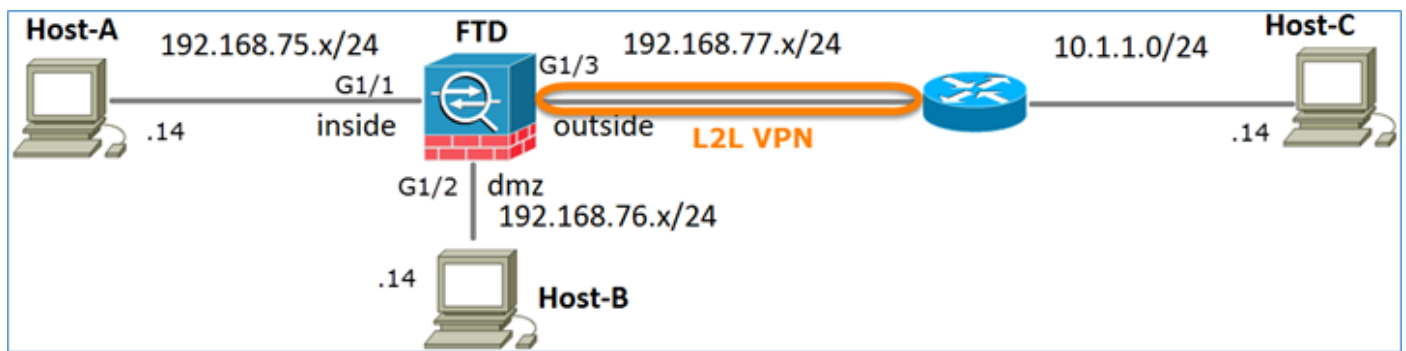
FTD ondersteunt dezelfde NAT-configuratieopties als de klassieke adaptieve security applicatie (ASA):

- NAT-regels voor - Dit is gelijk aan tweemaal NAT (sectie 1) op klassieke ASA
- Auto NAT-regels - Sectie 2 op klassieke ASA
- NAT-regels na - dit is gelijk aan twee NAT (deel 3) op klassieke ASA

Aangezien de FTD-configuratie vanuit het VCC wordt uitgevoerd wat de NAT-configuratie betreft, moet u bekend zijn met de FMC GUI en de verschillende configuratieopties.

Configureren

Netwerkdigram

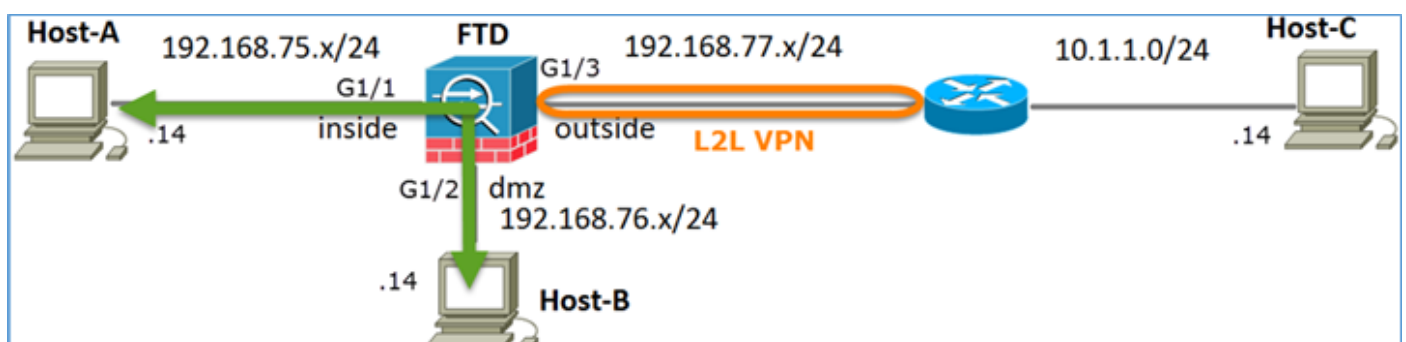


Taak 1. Statische NAT op FTD configureren

NAT configureren volgens deze vereisten:

NAT-beleidsnaam	De naam van het FTD-apparaat
NAT-regel	Handmatige NAT-regel
NAT-type	Statisch
Invoegen	In afdeling 1
Broninterface	binnen*
Doelinterface	DMZ*
Oorspronkelijke bron	192.168.75.14
Vertaalde bron	192.168.76.100

*Gebruik security zones voor de NAT-regel



Statische NAT

Oplossing:

Terwijl op klassieke ASA, moet u nameif in de NAT regels gebruiken. Voor FTD moet u ofwel Security Zones ofwel interfacegroepen gebruiken.

Stap 1. Wijs interfaces toe aan security zones/interfacegroepen.

In deze taak wordt besloten de FTD-interfaces die voor NAT worden gebruikt, aan Security Zones toe te wijzen. U kunt deze ook toewijzen aan interfacegroepen zoals in de afbeelding.

Edit Physical Interface

Mode:
Name: Enabled Management Only
Security Zone:
Description:

General | IPv4 | IPv6 | Advanced | Hardware Configuration

MTU: (64 - 9198)
Interface ID:

Stap 2. Het resultaat is zoals in de afbeelding.

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)

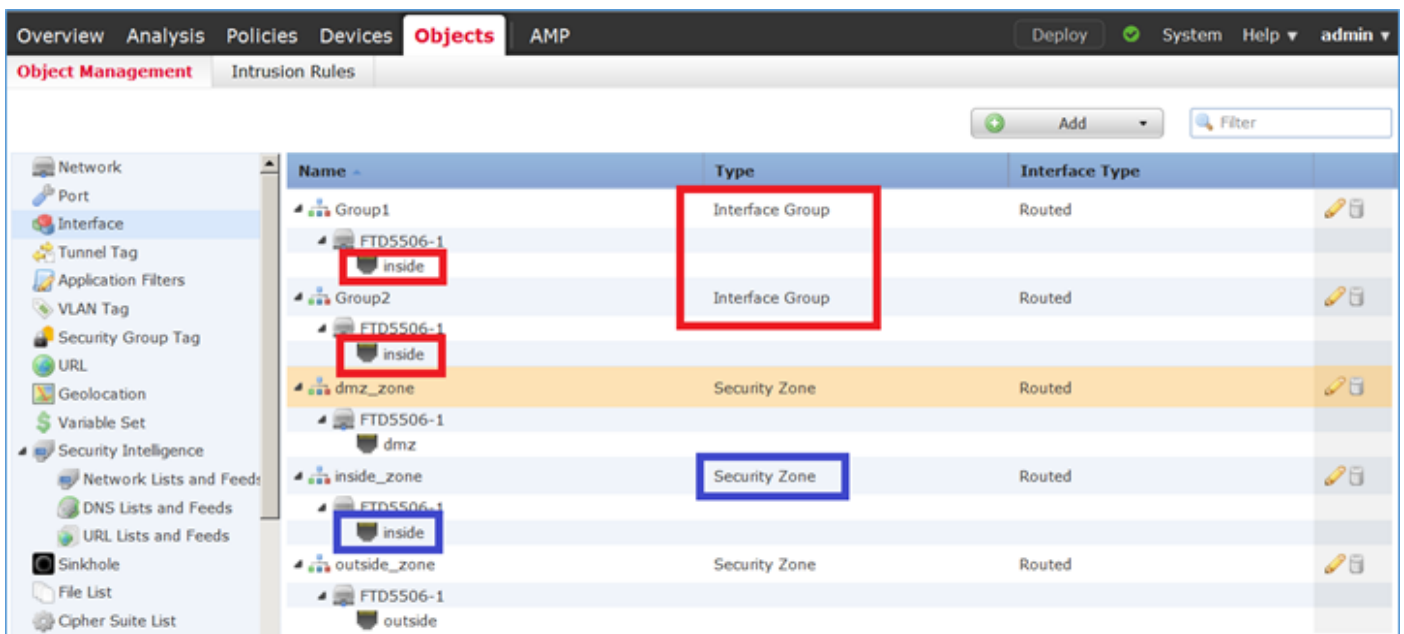
Stap 3. U kunt interfacegroepen en beveiligingszones maken/bewerken vanuit de pagina **Objecten** > **Objectbeheer** zoals in de afbeelding.



Security zones versus interfacegroepen

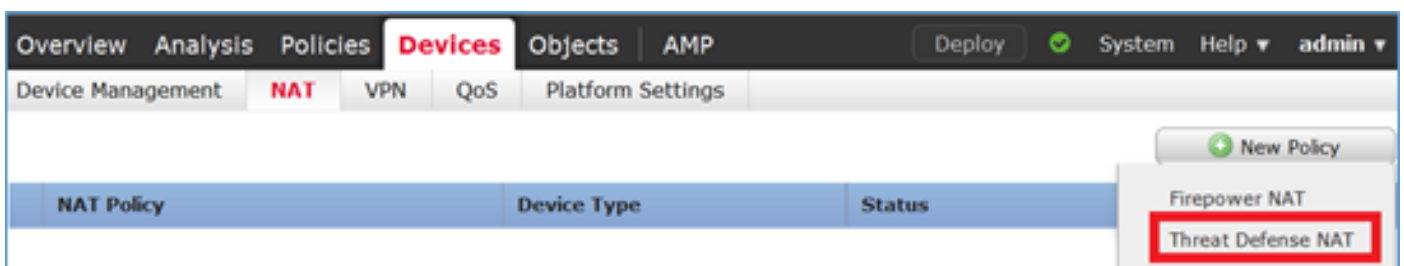
Het belangrijkste verschil tussen Security Zones en Interface Groups is dat een interface kan behoren tot slechts één Security Zone, maar kan behoren tot meerdere Interface Groepen. Praktisch gezien bieden de interfacegroepen dus meer flexibiliteit.

U kunt zien dat de interface **binnen** tot twee verschillende interfacegroepen behoort, maar slechts één Security Zone zoals in het beeld wordt getoond.

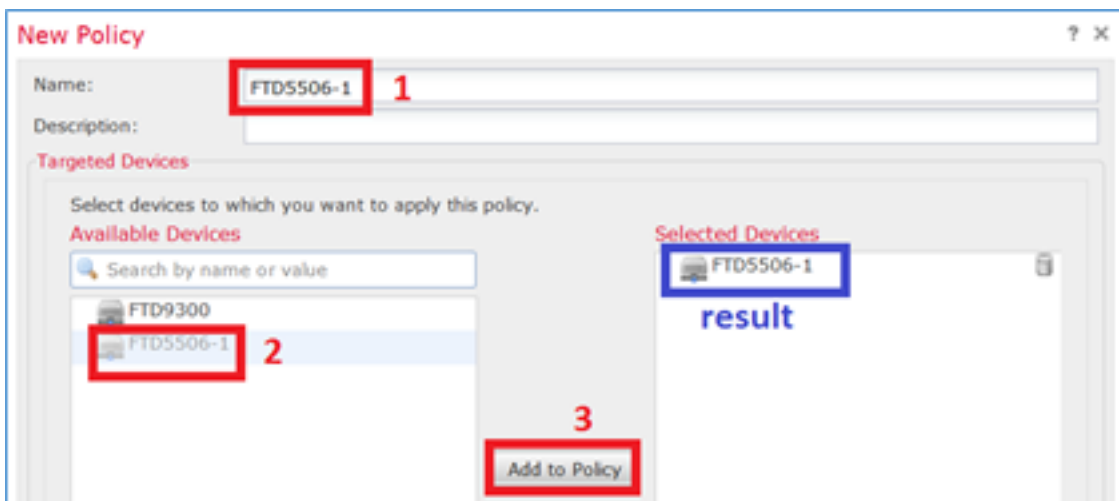


Stap 4. Configureer statische NAT op FTD.

Navigeer naar **Apparaten > NAT** en maak een NAT-beleid. Selecteer **Nieuw beleid > Threat Defense NAT** zoals in de afbeelding.

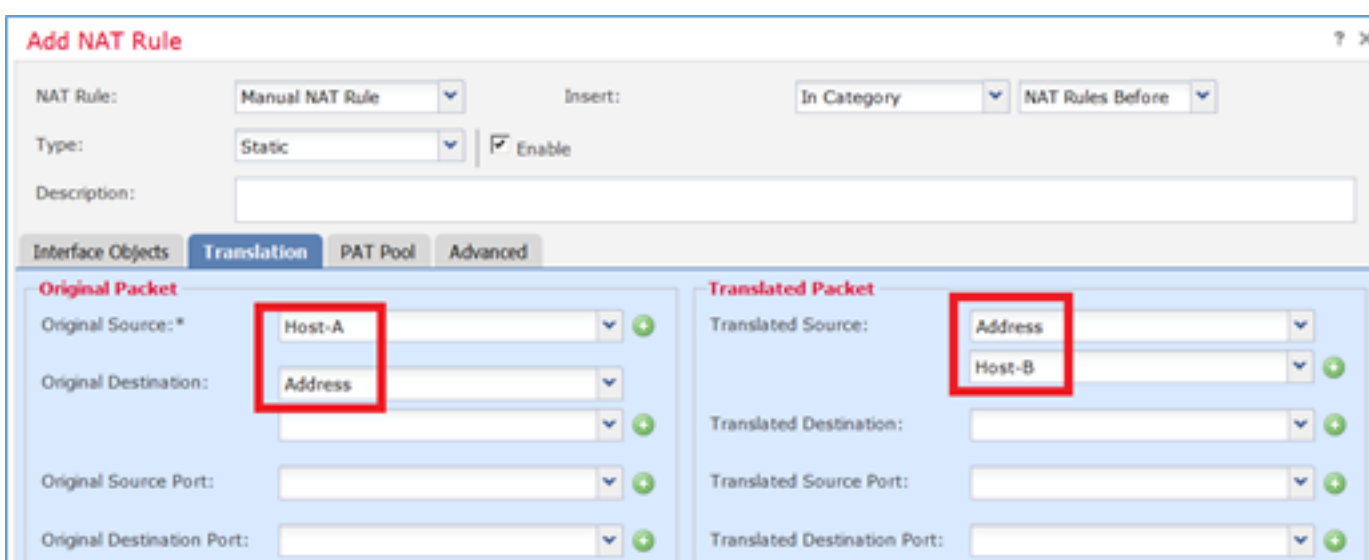
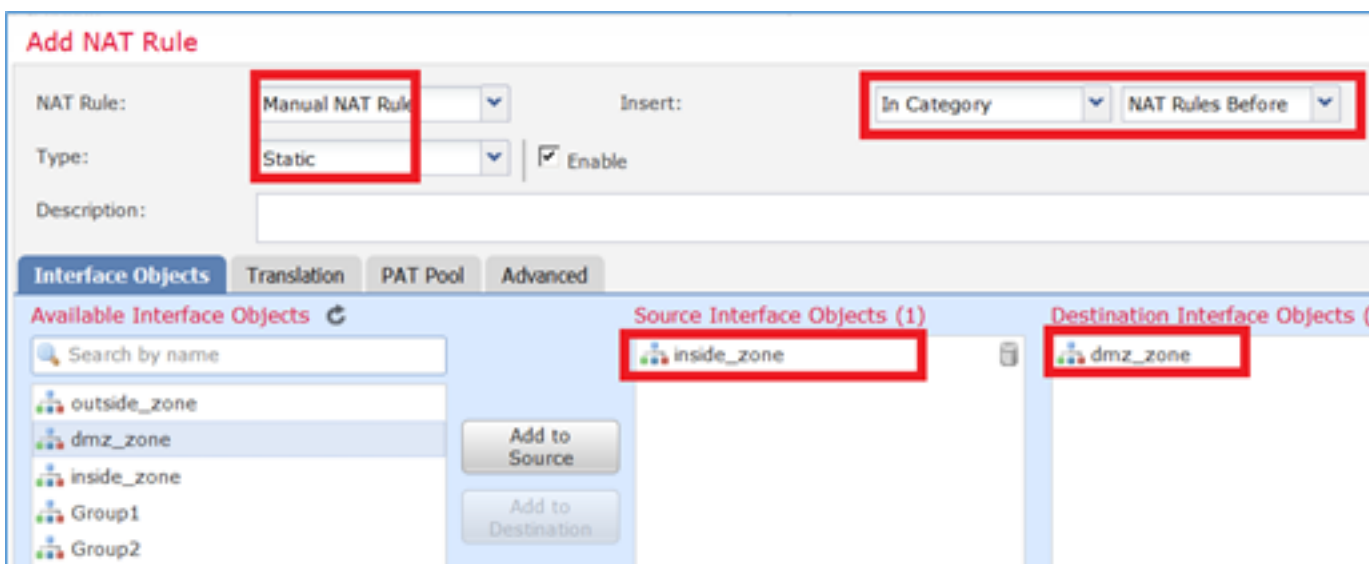


Stap 5. Specificeer de beleidsnaam en wijs deze toe aan een doelapparaat zoals in de afbeelding.



Stap 6. Voeg een NAT-regel toe aan het beleid, klik op **Add Rule**.

Specificeer deze per taak zoals in de afbeeldingen wordt weergegeven.



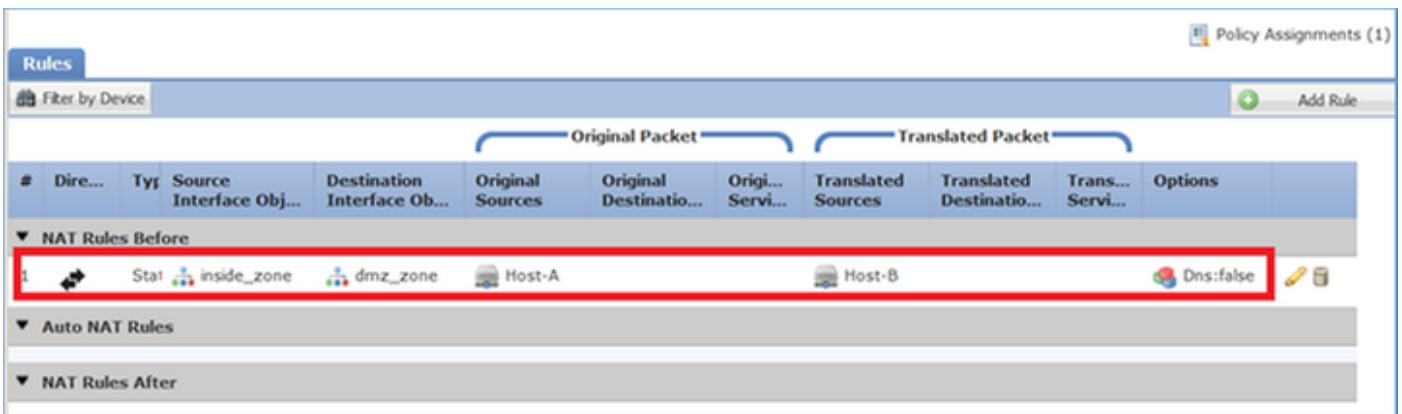
Host-A = 192.168.75.14

Host-B = 192.168.76.100

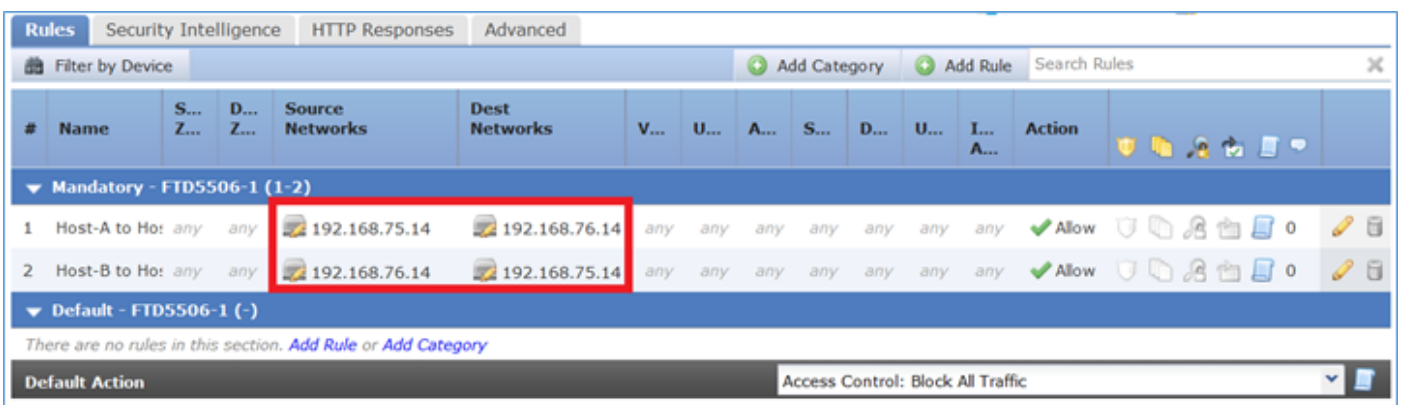
```
firepower# show run object
object network Host-A
  host 192.168.75.14
object network Host-B
  host 192.168.76.100
```

Waarschuwing: Als u Statische NAT configureert en een interface als vertaalde bron opgeeft, wordt al het verkeer dat bestemd is voor het IP-adres van de interface omgeleid. Gebruikers kunnen mogelijk geen toegang krijgen tot services die zijn ingeschakeld op de toegewezen interface. De voorbeelden van dergelijke diensten omvatten het verpletteren van protocollen zoals OSPF en EIGRP.

Stap 7. Het resultaat is zoals in de afbeelding.



Stap 8. Zorg ervoor dat er een Toegangsbeheerbeleid is dat Host-B toegang biedt tot Host-A en vice versa. Herinner dat Statische NAT door gebrek bidirectioneel is. Merk op dat het gebruik van echte IPs. This wordt verwacht aangezien in dit laboratorium, LINA 9.6.1.x code zoals getoond in het beeld in werking stelt.



Verificatie:

VAN LINA CLI:

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

De NAT-regel is zoals verwacht in afdeling 1 ingevoegd:

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

Opmerking: De 2 geeft aan welke op de achtergrond zijn gemaakt.

```
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
```

De ASP NAT-tabellen:

```
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

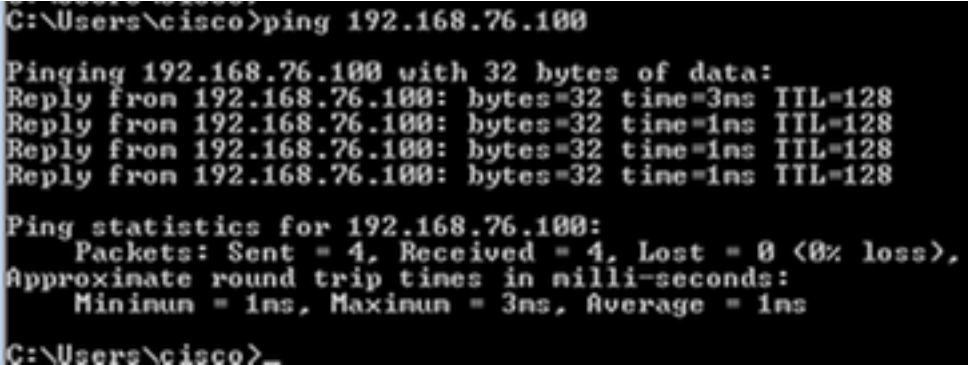
Output Table:

```
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

Schakel opname met overtrek details op FTD in en pingel van host-A naar host-B en zoals in de afbeelding.

```
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>
```

De hit counts staat in de ASP-tabellen:

```
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
```

De pakketopname toont:


```
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
```

Sporen van een pakket (belangrijke punten worden gemarkeerd).

Opmerking: De ID van de NAT-regel en de correlatie ervan met de ASP-tabel:

```
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

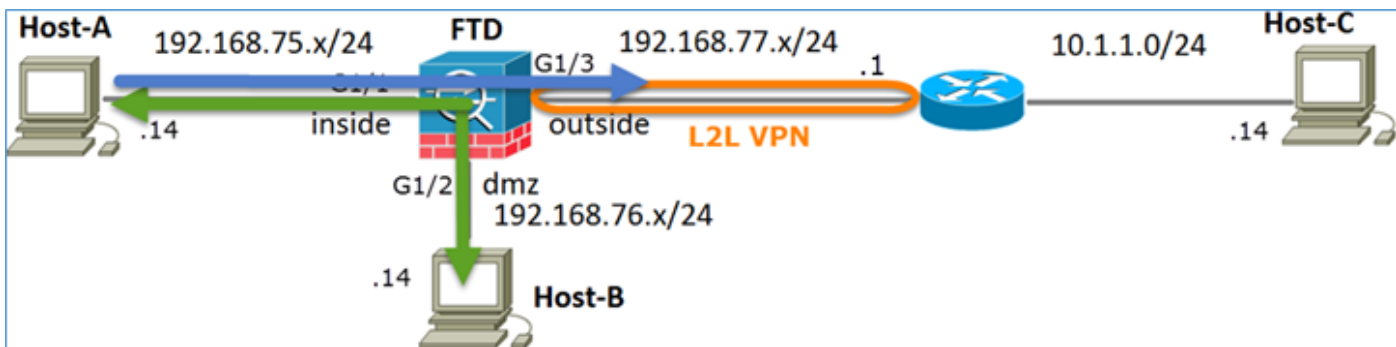
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: inside
output-status: up
output-line-status: up
Action: allow
1 packet shown
```

Taak 2. Poortadresomzetting (PAT) op FTD configureren

NAT configureren volgens deze vereisten:

NAT-regel	Handmatige NAT-regel
NAT-type	Dynamisch
Invoegen	In afdeling 1
Broninterface	binnen*
Doelinterface	buiten*
Oorspronkelijke bron	192.168.75.0/24
Vertaalde bron	Externe interface (PAT)

*Gebruik security zones voor de NAT-regel



Statische NAT

PAT

Oplossing:

Stap 1. Voeg een tweede NAT-regel toe en configureer volgens de taakvereisten zoals in de afbeelding.

Stap 2. Hier is hoe PAT is ingesteld zoals in de afbeelding.

Stap 3. Het resultaat is zoals in de afbeelding.

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

Stap 4. Voor de rest van dit laboratorium, vorm het Beleid van de Toegangscontrole om al verkeer toe te staan om door te gaan.

Verificatie:

NAT-configuratie:

```
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
```

Van LINA CLI noteer het nieuwe bericht:

```
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
```

Schakel opname in binnen- en buiteninterface in. Laat aan de binnenkant sporen toe:

```
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
```

Pingen van host-A (192.168.75.14) naar IP 192.168.77.1 zoals in de afbeelding.

```
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
```

In LINA captures, kunt u de vertaling van het PAT zien:

```
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
```

Sporen van een pakket met belangrijke secties gemarkeerd:

```
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

De dynamische xlate is gemaakt (let op de "ri" vlaggen):

```
firepower# show xlate
4 in use, 19 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
      s - static, T - twice, N - net-to-net
NAT from inside:192.168.75.14 to dmz:192.168.76.100
      flags sT idle 1:16:47 timeout 0:00:00
NAT from dmz:0.0.0.0/0 to inside:0.0.0.0/0
      flags sIT idle 1:16:47 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside:0.0.0.0/0
      flags sIT idle 0:05:35 timeout 0:00:00

ICMP PAT from inside:192.168.75.14/1 to outside:192.168.77.6/1 flags ri idle 0:00:30 timeout 0:00:30
```

In de LINA logboeken zie je:

```
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
```

NAT-secities:

```
firepower# show nat
Manual NAT Policies (Section 1)
1 (inside) to (dmz) source static Host-A Host-B
   translate_hits = 26, untranslate_hits = 26
2 (inside) to (outside) source dynamic Net_192.168.75.0_24bits interface
   translate_hits = 94, untranslate_hits = 138
```

ASP-tabellen tonen:

```
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:

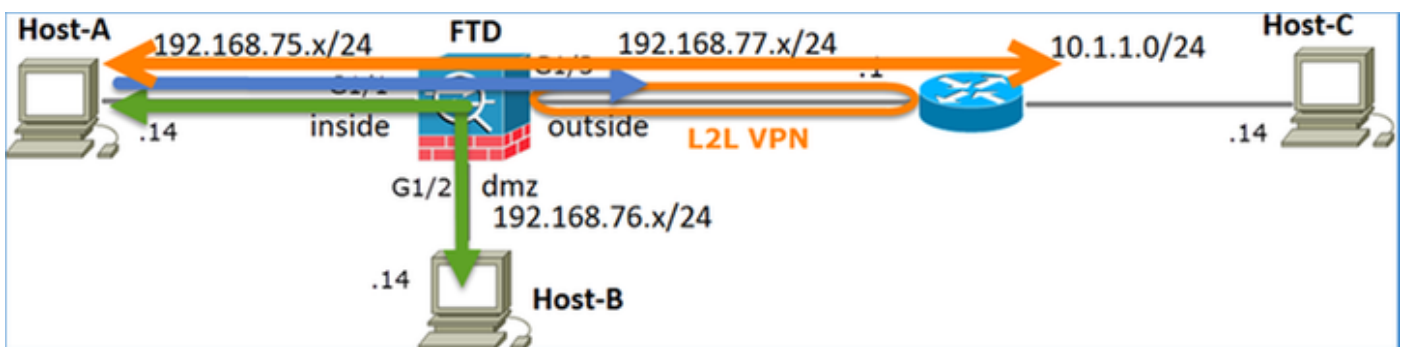
```
out id=0x7ff603685350, priority=6, domain=nat-reverse, deny=false
   hits=4, user_data=0x7ff60314dbf0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
   src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip/id=192.168.75.14, mask=255.255.255.255, port=0, tag=any, dscp=0x0
   input_ifc=dmz, 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
```

Taak 3. NAT-vrijstelling op FTD configureren

NAT configureren volgens deze vereisten:

NAT-regel	Handmatige NAT-regel
NAT-type	Statisch
Invoegen	In deel 1 worden alle bestaande regels binnen*
Broninterface	buiten*
Doelinterface	buiten*
Oorspronkelijke bron	192.168.75.0/24
Vertaalde bron	192.168.75.0/24
Oorspronkelijke bestemming	10.1.1.0/24
Vertaalde bestemming	10.1.1.0/24

*Gebruik security zones voor de NAT-regel



Statische NAT

PAT

NAT-vrijstelling

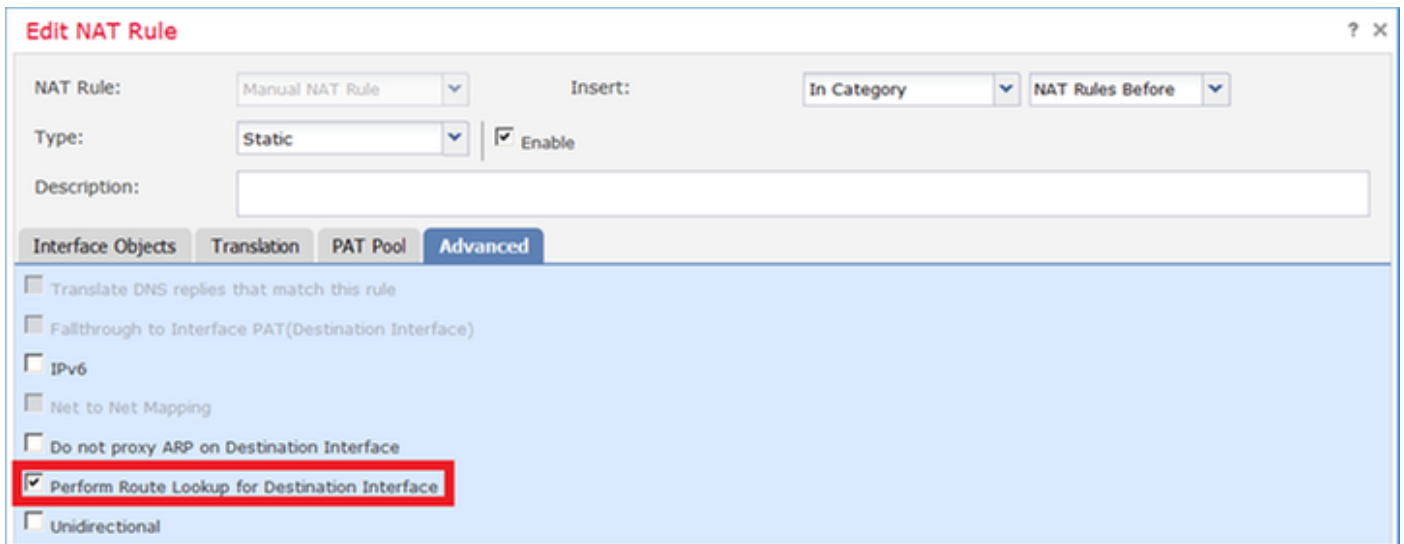
Oplossing:

Stap 1. Voeg een derde NAT-regel toe en configureer per taak zoals in de afbeelding.

Rules										
Filter by Device										
#	Direction	Ty...	Source Interface O...	Destination Interface Obj...	Original Packet			Translated Packet		
					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										

Stap 2. Voer de routeraadpleging uit voor de bepaling van de uitgaande interface.

Opmerking: Voor Identity NAT-regels kunt u, zoals de regels die u hebt toegevoegd, wijzigen hoe de uitgaande interface wordt bepaald en normale routeropzoeking gebruiken zoals in de afbeelding.



Verificatie:

```
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
```

Start pakkettracer voor niet-VPN verkeer via een bron binnen het netwerk. De PAT-regel wordt gebruikt zoals verwacht:

```
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

Laat pakkettracer draaien voor verkeer dat door de VPN-tunnel moet gaan (voer deze twee keer uit sinds de eerste poging de VPN-tunnel omhoog brengt).

Opmerking: U moet de NAT-vrijstellingsregel raken.

Eerste pakkettracer-poging:

```
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

Tweede packet-tracer pinging:

```
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

Verificatie NAT-treffers:

```
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
```

Taak 4. Object NAT op FTD configureren

NAT configureren volgens deze vereisten:

NAT-regel	Auto NAT-regel
NAT-type	Statisch
Invoegen	In afdeling 2
Broninterface	binnen*
Doelinterface	DMZ*
Oorspronkelijke bron	192.168.75.99
Vertaalde bron	192.168.76.99
Vertaal DNS antwoorden die overeenkomen met deze regel	Ingeschakeld

*Gebruik security zones voor de NAT-regel

Oplossing:

Stap 1. Configureer de regel volgens de taakvereisten zoals in de afbeeldingen.

Add NAT Rule

NAT Rule: **Auto NAT Rule** Enable
 Type: **Static** Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- outside_zone
- dmz_zone
- inside_zone
- Group1
- Group2

Source Interface Objects (1): **inside_zone**

Destination Interface Objects (1): **dmz_zone**

Add to Source
Add to Destination

Add NAT Rule

NAT Rule: **Auto NAT Rule** Enable
 Type: **Static** Enable

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source: * **obj-192.168.75.99**

Original Port: TCP

Translated Packet

Translated Source: **obj-192.168.76.99**

Translated Port:

Add NAT Rule

NAT Rule: **Auto NAT Rule** Enable
 Type: **Static** Enable

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Falthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Stap 2. Het resultaat is zoals in de afbeelding.

Rules

Filter by Device

#	Direction	Ty...	Original Packet		Translated Packet					
			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										

Verificatie:

```
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
```

Verificatie met pakkettracer:

```
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

Taak 5. PAT-pool op FTD configureren

NAT configureren volgens deze vereisten:

NAT-regel	Handmatige NAT-regel
NAT-type	Dynamisch
Invoegen	In afdeling 3
Broninterface	binnen*
Doelinterface	DMZ*
Oorspronkelijke bron	192.168.75.0/24
Vertaalde bron	192.168.76.20-22
Gebruik het gehele bereik (1-65535)	Ingeschakeld

*Gebruik security zones voor de NAT-regel

Oplossing:

Stap 1. Configureer de regel per taakvereisten zoals in de afbeeldingen.

Add NAT Rule

NAT Rule: Manual NAT Rule (dropdown) | Insert: In Category (dropdown) | NAT Rules After (dropdown)

Type: Dynamic (dropdown) | Enable

Description: [text area]

Interface Objects | Translation | PAT Pool | Advanced

Available Interface Objects [refresh icon]

Search by name [input field]

- outside_zone
- dmz_zone
- inside_zone
- Group1
- Group2

Source Interface Objects (1): inside_zone

Destination Interface Objects (1): dmz_zone

Add to Source | Add to Destination

Add NAT Rule

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules After

Type: Dynamic Enable

Description:

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:* **Net_192.168.75.0_24bits** +

Original Destination: **Address** +

Original Source Port: +

Original Destination Port: +

Translated Packet

Translated Source: Address +

Translated Destination: +

Translated Source Port: +

Translated Destination Port: +

Stap 2. Schakel **Platte Poortbereik** in met **Reserverpoorten** die het gebruik van het gehele bereik (1-65535) zoals in de afbeelding mogelijk maken.

Add NAT Rule

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules After

Type: Dynamic Enable

Description:

Interface Objects Translation **PAT Pool** Advanced

Enable PAT Pool

PAT: Address **range-192.168.76.20-22** +

Use Round Robin Allocation

Extended PAT Table

Flat Port Range

Include Reserve Ports

Stap 3. Het resultaat is zoals in de afbeelding.

Rules											
#	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

Verificatie:

```
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

```

De regel staat in afdeling 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

```

Packet-tracer verificatie:

```
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

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Verificatie is toegelicht in de afzonderlijke takensecties.

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Open de pagina **Geavanceerde probleemoplossing** op het VCC, voer de pakkettracer uit en voer vervolgens de opdracht **NAT-pool tonen uit**.

Let op het item dat het gehele bereik gebruikt zoals in de afbeelding.

The screenshot shows the Cisco Firepower Management Center (VCC) interface. At the top, there are navigation tabs: Overview, Analysis, Policies, Devices, Objects, and AMP. Below these are sub-tabs: Configuration, Users, Domains, Integration, Updates, Licenses, and Health & Monitor. The main heading is 'Advanced Troubleshooting' for device 'FTD5506-1'. The 'ASA CLI' tab is selected. In the command input area, 'show' is entered in the 'Command' field and 'nat pool' in the 'Parameter' field. A red box highlights the command input area, and a red '1' is next to it. The output area shows the following text:

```
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
```

The 'ICMP PAT pool dmz:range-192.168.76.20-22, address 192.168.76.20, range 1-65535, allocated 1' line is highlighted in blue. At the bottom, the 'Execute' button is highlighted with a red box, and a red '2' is next to it.

Gerelateerde informatie

- Alle versies van de Cisco Firepower Management Center-configuratiehandleiding vindt u hier:
https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html#id_47280
- Cisco Global Technical Assistance Center (TAC) raadt deze visuele gids ten eerste aan voor diepgaande praktische kennis over Cisco Firepower Security Technologies van de volgende generatie, zoals de technologieën die in dit artikel worden vermeld:
<http://www.ciscopress.com/title/9781587144806>
- TechNotes voor alle configuratie en probleemoplossing die betrekking hebben op Firepower-technologieën:
<https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html>

- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.