LAN-communicatie tussen hosts die op zoek zijn naar hun openbare IP-adressen achter een ASA

Inhoud

Inleiding

Dit document beschrijft verschillende netwerkimplementaties van de plaats waar deze nodig zijn om LAN-communicatie (Local Area Network) tussen hosts mogelijk te maken die op zoek zijn naar hun openbare IP-adressen achter een adaptieve security applicatie (ASA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco basis ASA NAT-configuratie, versie 8.3 en hoger.
- Cisco basis ASA NAT-configuratie, versie 8.2 en ouder.

Gebruikte componenten

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

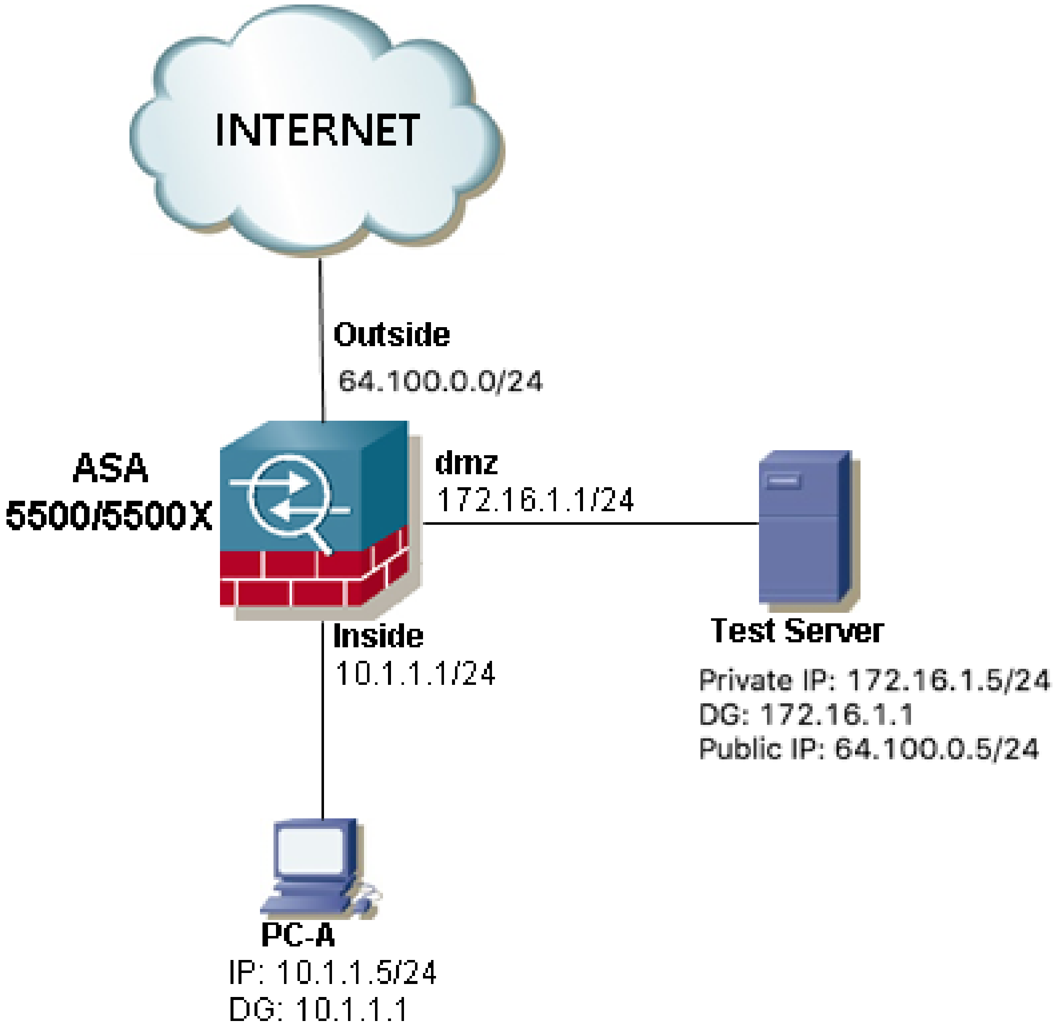
- ASA 5500 en ASA 5500-X Series.
- Cisco ASA versie 8.3 en hoger.
- Cisco ASA versie 8.2 en hoger.

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

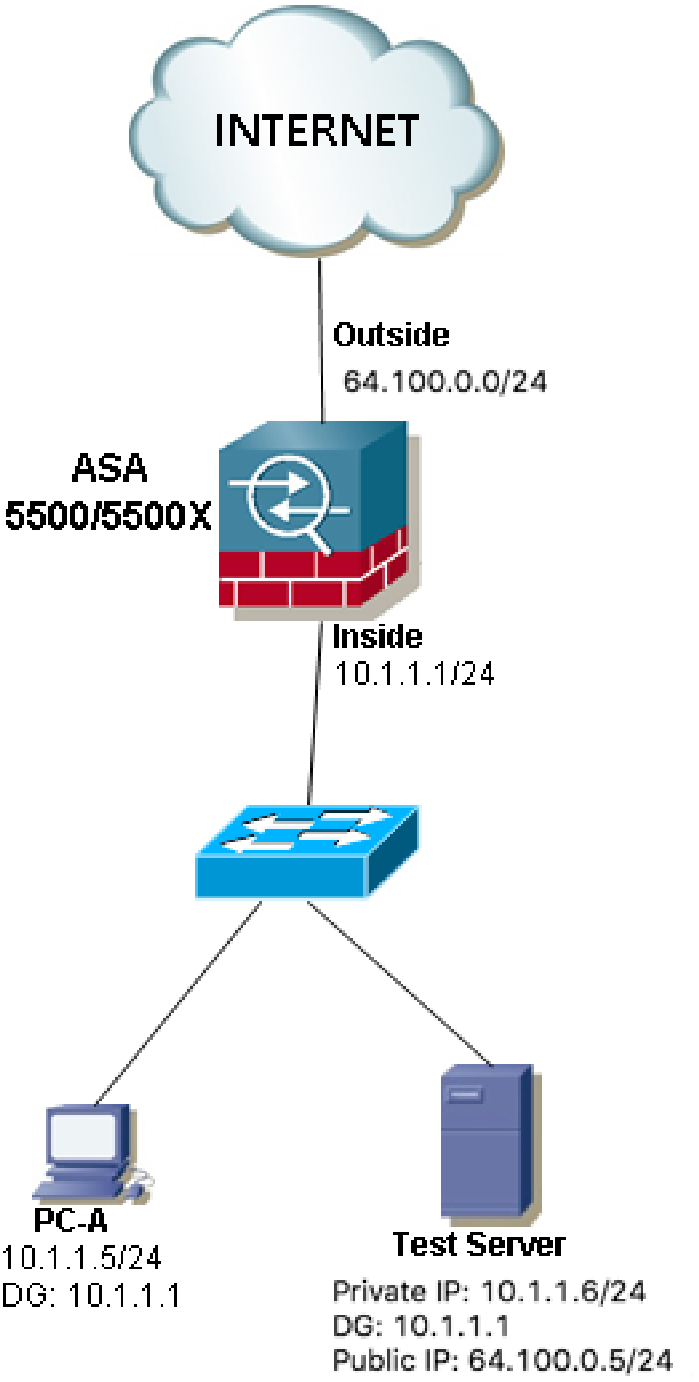
Probleem: LAN-communicatie tussen hosts die op zoek zijn naar hun openbare IP-adressen achter een ASA

In de volgende sectie, kunt u drie topologie voorbeelden zien die deze communicatie vereiste tonen om LAN communicatie tussen gastheren toe te staan die hun openbare IP adressen achter een ASA zoeken.

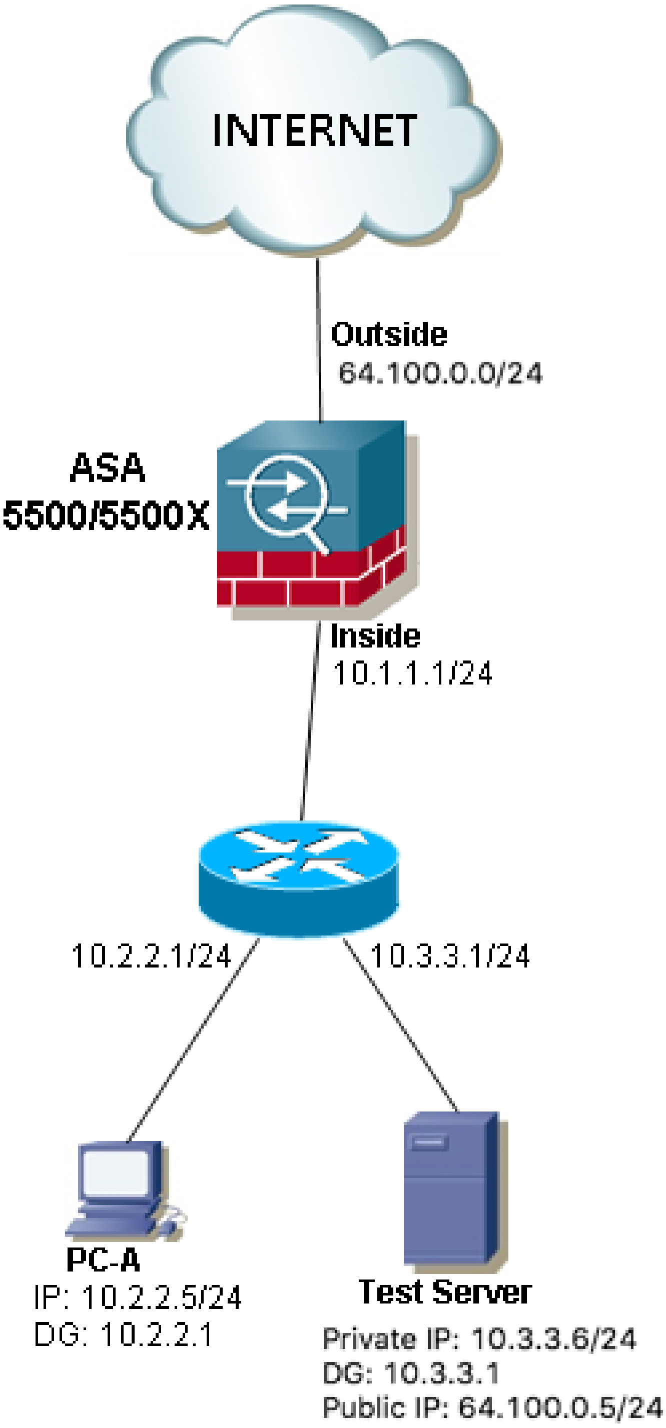
Voorbeeld 1. De PC-A van de bronhost wordt aangesloten op de interne ASA-interface terwijl de doelhost host Test Server is verbonden met de DMZ-interface.



Voorbeeld 2. De bron- en doelgastheren PC-A en Test Server worden verbonden met de zelfde binnen ASA interface.



Voorbeeld 3. De bron- en doelgastheren PC-A en Test Server worden verbonden met de binnen-ASA interface, maar achter een ander laag 3 apparaat (het kan een router of een meerlaagse switch zijn).



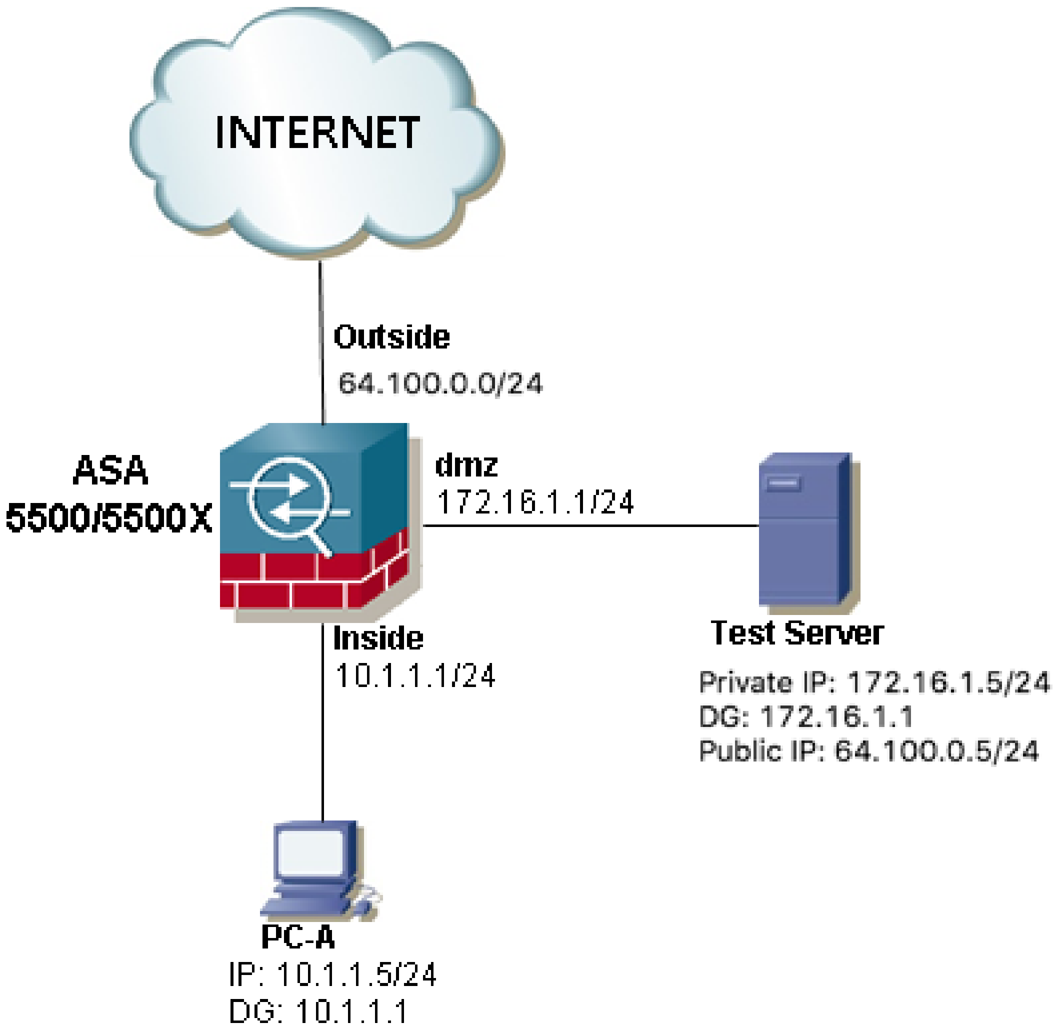
Opmerking: De **Test Server** in de drie beelden heeft een statische Netwerkadresomzetting (NAT) in de ASA, deze statische NAT-vertaling wordt van buitenaf op de corresponderende interne interface toegepast om de **Test Server** van buitenaf bereikbaar te maken met het openbare IP-adres 64.100.0.5. Vervolgens wordt dit vertaald naar het interne IP-adres van **Test Server**.

Oplossing

Om de PC-A van de bronhost in staat te stellen de doelserver met zijn openbare IP-adres te bereiken in plaats van het privé-adres, moeten we een dubbele NAT-configuratie toepassen. De twee NAT configuratie helpt ons om zowel de bron- als de doeladressen van de pakketten te vertalen wanneer het verkeer door de ASA passeert.

Hier zijn de details van de twee nat configuratie vereist voor elke topologie:

Voorbeeld 1. De PC-A van de bronhost wordt aangesloten op de interne ASA-interface terwijl de doelhost host Test Server is verbonden met de DMZ-interface.



Configuratie

Twice NAT voor ASA versies 8.3 en later:

```
object network obj-10.1.1.5
host 10.1.1.5

object network obj-172.16.1.5
host 172.16.1.5

object network obj-64.100.0.5
host 64.100.0.5

nat (inside,dmz) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-
172.16.1.5
```

NOTE: After this NAT is applied in the ASA you will receive a warning message as the following:

```
WARNING: All traffic destined to the IP address of the outside interface is being redirected.
```

```
WARNING: Users may not be able to access any service enabled on the outside interface.
```

Twice NAT voor ASA versies 8.2 en ouder:

```
access-list IN-DMZ-INTERFACE extended permit ip host 10.1.1.5 host 64.100.0.5
static (inside,dmz) interface access-list IN-DMZ-INTERFACE

access-list DMZ-IN-INTERFACE extended permit ip host 172.16.1.5 host 172.16.1.1
static (dmz,inside) 64.100.0.5 access-list DMZ-IN-INTERFACE
```

Problemen oplossen

Packet Tracer uitvoer versies 8.3 en later:

```
ASA# packet-tracer input inside tcp 10.1.1.5 123 64.100.0.5 80

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,dmz) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-
172.16.1.5
Additional Information:
NAT divert to egress interface dmz
Untranslate 64.100.0.5/80 to 172.16.1.5/80

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,dmz) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-
172.16.1.5
Additional Information:
Static translate 10.1.1.5/123 to 172.16.1.1/123

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
```

```
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,dmz) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-
172.16.1.5
Additional Information:

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: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 167632, 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
```

Packet Tracer uitvoer versies 8.2 en ouder:

```
ASA#packet-tracer input inside tcp 10.1.1.5 123 64.100.0.5 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (dmz,inside) 64.100.0.5 access-list DMZ-IN-INTERFACE
match ip dmz host 172.16.1.5 inside host 172.16.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
Additional Information:
NAT divert to egress interface dmz
Untranslate 64.100.0.5/0 to 172.16.1.5/0 using netmask 255.255.255.255

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

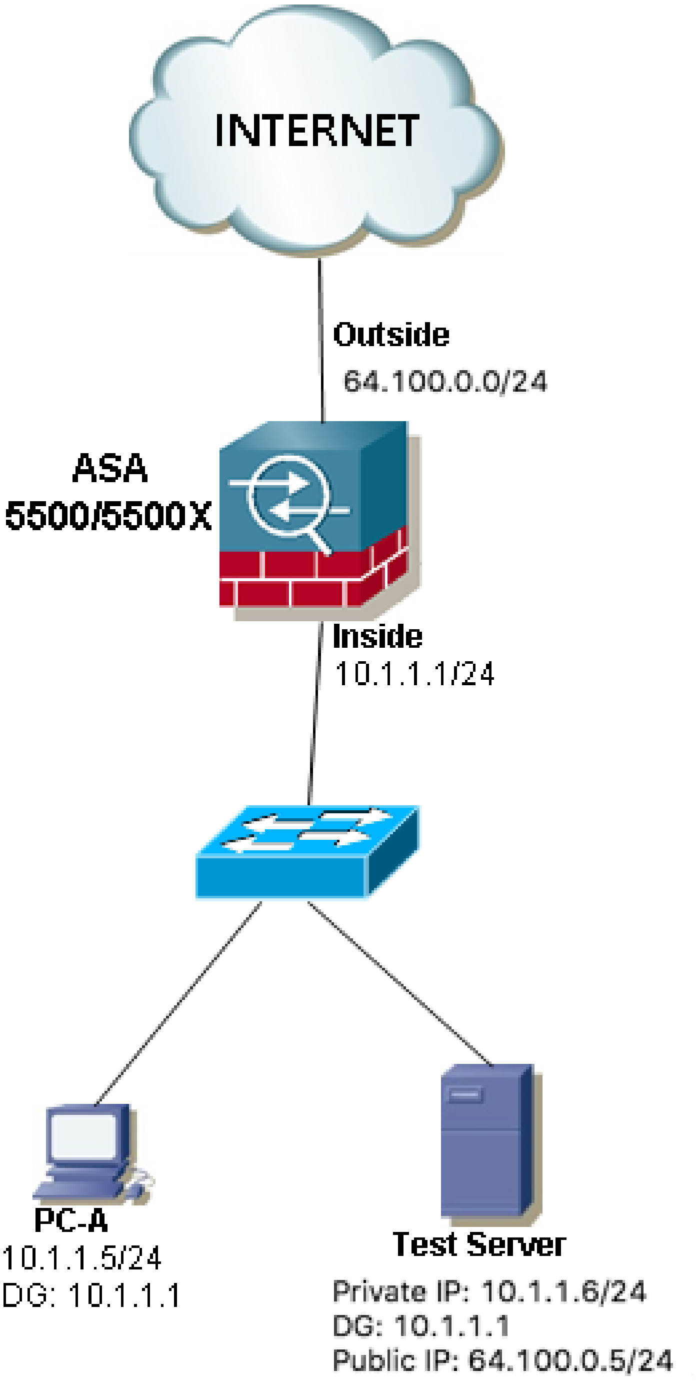
```
Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
static (inside,dmz) interface access-list IN-DMZ-INTERFACE
match ip inside host 10.1.1.5 dmz host 64.100.0.5
static translation to 172.16.1.1
translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.1.1.5/0 to 172.16.1.1/0 using netmask 255.255.255.255

Phase: 4
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,dmz) interface access-list IN-DMZ-INTERFACE
match ip inside host 10.1.1.5 dmz host 64.100.0.5
static translation to 172.16.1.1
translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
static (dmz,inside) 64.100.0.5 access-list DMZ-IN-INTERFACE
match ip dmz host 172.16.1.5 inside host 172.16.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
Additional Information:

Phase: 6
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (dmz,inside) 64.100.0.5 access-list DMZ-IN-INTERFACE
match ip dmz host 172.16.1.5 inside host 172.16.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 503, 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
```

Packet Capture:

```
ASA# sh cap
capture capin type raw-data interface inside [Capturing - 1300 bytes]
match ip host 10.1.1.5 host 64.100.0.5
capture capout type raw-data interface dmz [Capturing - 1300 bytes]
match ip host 172.16.1.1 host 172.16.1.5

ASA# sh cap capin

10 packets captured
1: 12:36:28.245455 10.1.1.5 > 64.100.0.5: icmp: echo request
2: 12:36:28.269441 64.100.0.5 > 10.1.1.5: icmp: echo reply
3: 12:36:28.303451 10.1.1.5 > 64.100.0.5: icmp: echo request
4: 12:36:28.333692 64.100.0.5 > 10.1.1.5: icmp: echo reply
5: 12:36:28.372478 10.1.1.5 > 64.100.0.5: icmp: echo request
6: 12:36:28.395563 64.100.0.5 > 10.1.1.5: icmp: echo reply
7: 12:36:28.422402 10.1.1.5 > 64.100.0.5: icmp: echo request
8: 12:36:28.449241 64.100.0.5 > 10.1.1.5: icmp: echo reply
9: 12:36:28.481420 10.1.1.5 > 64.100.0.5: icmp: echo request
10: 12:36:28.507435 64.100.0.5 > 10.1.1.5: icmp: echo reply
10 packets shown

ASA1# sh cap capout

10 packets captured
1: 12:36:28.245730 172.16.1.1 > 172.16.1.5: icmp: echo request
2: 12:36:28.269395 172.16.1.5 > 172.16.1.1: icmp: echo reply
3: 12:36:28.303725 172.16.1.1 > 172.16.1.5: icmp: echo request
4: 12:36:28.333646 172.16.1.5 > 172.16.1.1: icmp: echo reply
5: 12:36:28.372737 172.16.1.1 > 172.16.1.5: icmp: echo request
6: 12:36:28.395533 172.16.1.5 > 172.16.1.1: icmp: echo reply
7: 12:36:28.422661 172.16.1.1 > 172.16.1.5: icmp: echo request
8: 12:36:28.449195 172.16.1.5 > 172.16.1.1: icmp: echo reply
9: 12:36:28.481695 172.16.1.1 > 172.16.1.5: icmp: echo request
10: 12:36:28.507404 172.16.1.5 > 172.16.1.1: icmp: echo reply
10 packets shown
```

Voorbeeld 2. De bron- en doelgastheren PC-A en Test Server worden verbonden met de zelfde binnen ASA interface.



Configuratie

Twice NAT voor ASA versies 8.3 en later:

```
object network obj-10.1.1.5
host 10.1.1.5

object network obj-10.1.1.6
host 10.1.1.6

object network obj-64.100.0.5
host 64.100.0.5

nat (inside,inside) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-
10.1.1.6
```

```
NOTE: After this NAT is applied in the ASA you will receive a warning message as the following:

WARNING: All traffic destined to the IP address of the outside interface is being redirected.
WARNING: Users may not be able to access any service enabled on the outside interface.
```

Twice NAT voor ASA versies 8.2 en ouder:

```
access-list IN-OUT-INTERFACE extended permit ip host 10.1.1.5 host 64.100.0.5
static (inside,inside) interface access-list IN-OUT-INTERFACE

access-list OUT-IN-INTERFACE extended permit ip host 10.1.1.6 host 10.1.1.1
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
```

> Opmerking: De belangrijkste bedoeling van de NAT-vertaling voor het bron-IP-adres van 10.1.1.5 naar het ASA-binneninterface-adres 10.1.1.1 is om de antwoorden van host 10.1.1.6 te dwingen naar de ASA terug te keren. Dit is dringend nodig om asymmetrische routing te voorkomen en om de ASA in staat te stellen alle verkeer tussen de geïnteresseerde hosts te verwerken, indien we niet vertalen Bewaar het IP-adres van de bron zoals we dat deden in dit voorbeeld, dan blokkeert de ASA het geïnteresseerde verkeer vanwege asymmetrische routing.

Problemen oplossen

Packet Tracer uitvoer versies 8.3 en later:

```
ASA# packet-tracer input inside tcp 10.1.1.5 123 64.100.0.5 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,inside) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-
10.1.1.6
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.5/80 to 10.1.1.6/80

Phase: 2
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,inside) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-
10.1.1.6
Additional Information:
Static translate 10.1.1.5/123 to 10.1.1.1/123

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 4
Type: NAT
```

```
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,inside) source static obj-10.1.1.5 interface destination static obj-64.100.0.5 obj-
10.1.1.6
Additional Information:

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: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 167839, packet dispatched to next module

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

Packet Tracer uitvoer versies 8.2 en ouder:

```
ASA# packet-tracer input inside tcp 10.1.1.5 123 64.100.0.5 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
match ip inside host 10.1.1.6 inside host 10.1.1.1
```

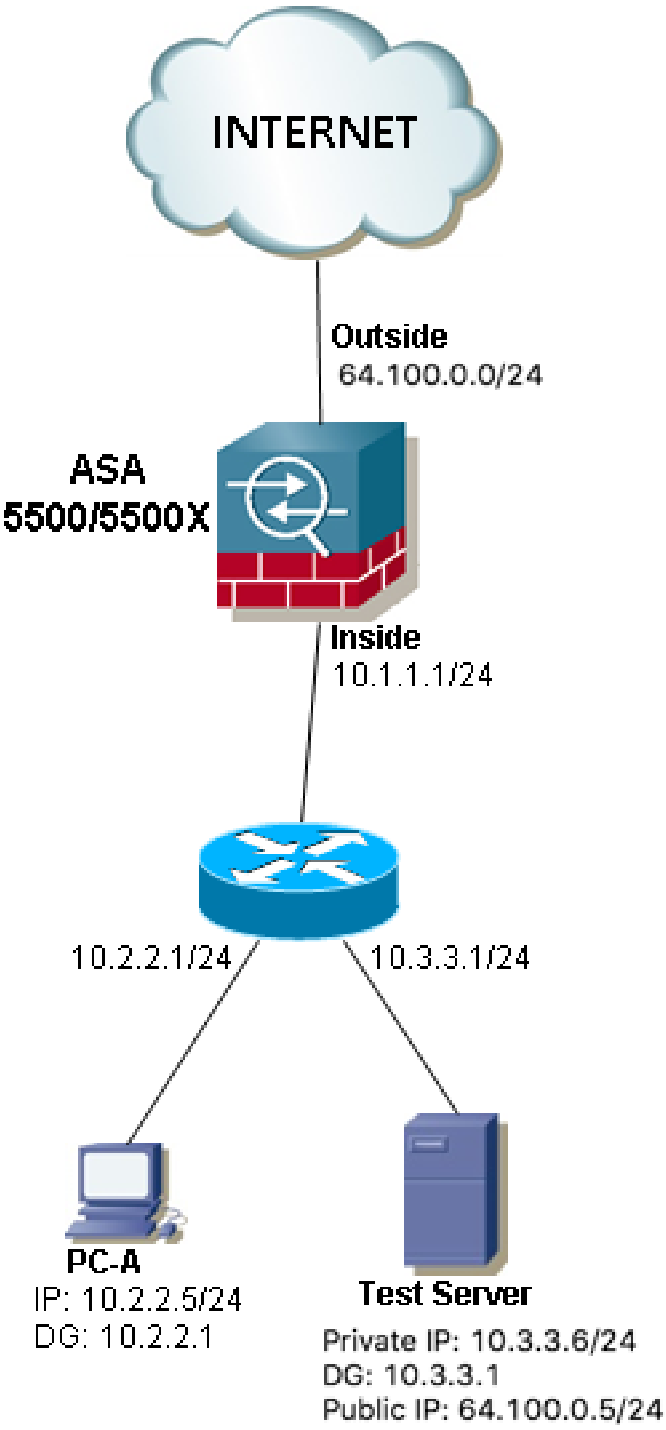
```
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.5/0 to 10.1.1.6/0 using netmask 255.255.255.255

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
static (inside,inside) interface access-list IN-OUT-INTERFACE
match ip inside host 10.1.1.5 inside host 64.100.0.5
static translation to 10.1.1.1
translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.1.1.5/0 to 10.1.1.1/0 using netmask 255.255.255.255

Phase: 5
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,inside) interface access-list IN-OUT-INTERFACE
match ip inside host 10.1.1.5 inside host 64.100.0.5
static translation to 10.1.1.1
translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
match ip inside host 10.1.1.6 inside host 10.1.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
Additional Information:

Phase: 7
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
match ip inside host 10.1.1.6 inside host 10.1.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
```

```
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 727, packet dispatched to next module

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

Packet Capture:

```
ASA# sh cap
capture capin type raw-data interface inside [Capturing - 1300 bytes]
match ip host 10.1.1.5 host 64.100.0.5
capture capout type raw-data interface inside [Capturing - 1300 bytes]
match ip host 10.1.1.1 host 10.1.1.6

ASA# sh cap capin

10 packets captured
1: 12:50:39.304748 10.1.1.5 > 64.100.0.5: icmp: echo request
2: 12:50:39.335431 64.100.0.5 > 10.1.1.5: icmp: echo reply
3: 12:50:39.368389 10.1.1.5 > 64.100.0.5: icmp: echo request
4: 12:50:39.389368 64.100.0.5 > 10.1.1.5: icmp: echo reply
5: 12:50:39.398432 10.1.1.5 > 64.100.0.5: icmp: echo request
6: 12:50:39.418176 64.100.0.5 > 10.1.1.5: icmp: echo reply
7: 12:50:39.419732 10.1.1.5 > 64.100.0.5: icmp: echo request
8: 12:50:39.425103 64.100.0.5 > 10.1.1.5: icmp: echo reply
9: 12:50:39.434395 10.1.1.5 > 64.100.0.5: icmp: echo request
10: 12:50:39.438423 64.100.0.5 > 10.1.1.5: icmp: echo reply
10 packets shown

ASA2# sh cap capout

10 packets captured
1: 12:50:39.305282 10.1.1.1 > 10.1.1.6: icmp: echo request
2: 12:50:39.335386 10.1.1.6 > 10.1.1.1: icmp: echo reply
3: 12:50:39.368663 10.1.1.1 > 10.1.1.6: icmp: echo request
4: 12:50:39.389307 10.1.1.6 > 10.1.1.1: icmp: echo reply
5: 12:50:39.398706 10.1.1.1 > 10.1.1.6: icmp: echo request
6: 12:50:39.418130 10.1.1.6 > 10.1.1.1: icmp: echo reply
7: 12:50:39.419762 10.1.1.1 > 10.1.1.6: icmp: echo request
8: 12:50:39.425072 10.1.1.6 > 10.1.1.1: icmp: echo reply
9: 12:50:39.434669 10.1.1.1 > 10.1.1.6: icmp: echo request
10: 12:50:39.438392 10.1.1.6 > 10.1.1.1: icmp: echo reply
10 packets shown
```

Voorbeeld 3. De bron- en doelgastheren PC-A en Test Server worden verbonden met de binnen-ASA interface, maar achter een ander laag 3 apparaat (het kan een router of een meerlaagse switch zijn).



Configuratie

Twice NAT voor ASA versies 8.3 en later:

```
object network obj-10.2.2.5
host 10.2.2.5

object network obj-10.3.3.6
```

```
host 10.3.3.6

object network obj-64.100.0.5
host 64.100.0.5

nat (inside,inside) source static obj-10.2.2.5 interface destination static obj-64.100.0.5 obj-
10.3.3.6
```

NOTE: After this NAT is applied in the ASA you will receive a warning message as the following:

```
WARNING: All traffic destined to the IP address of the outside interface is being redirected.
WARNING: Users may not be able to access any service enabled on the outside interface.
```

Twice NAT voor ASA versies 8.2 en ouder:

```
access-list IN-OUT-INTERFACE extended permit ip host 10.2.2.5 host 64.100.0.5
static (inside,inside) interface access-list IN-OUT-INTERFACE

access-list OUT-IN-INTERFACE extended permit ip host 10.3.3.6 host 10.1.1.1
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
```

> **Opmerking**: De belangrijkste bedoeling van de NAT-vertaling voor het bron-IP-adres van 10.1.1.5 naar het ASA-binneninterface-IP-adres (10.1.1.1) is om de antwoorden van host 10.1.1.6 te dwingen terug te keren naar de ASA. Dit is dringend nodig om asymmetrische routing te voorkomen en om de ASA in staat te stellen alle verkeer tussen de ASA Als we het IP-adres van de bron niet vertalen zoals we in dit voorbeeld deden, dan blokkeert de ASA het geïnteresseerde verkeer door asymmetrische routing.

Problemen oplossen

Packet Tracer uitvoer versies 8.3 en later:

```
ASA# packet-tracer input inside tcp 10.2.2.5 123 64.100.0.5 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,inside) source static obj-10.2.2.5 interface destination static obj-64.100.0.5 obj-
10.3.3.6
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.5/80 to 10.3.3.6/80

Phase: 2
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,inside) source static obj-10.2.2.5 interface destination static obj-64.100.0.5 obj-
10.3.3.6
Additional Information:
Static translate 10.2.2.5/123 to 10.1.1.1/123

Phase: 3
Type: ACCESS-LIST
Subtype:
```

```
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,inside) source static obj-10.2.2.5 interface destination static obj-64.100.0.5 obj-
10.3.3.6
Additional Information:

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: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 167945, packet dispatched to next module

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

Packet Tracer uitvoer versies 8.2 en ouder:

```
ASA# packet-tracer input inside tcp 10.2.2.5 123 64.100.0.5 80
```

```
Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
match ip inside host 10.3.3.6 inside host 10.1.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.5/0 to 10.3.3.6/0 using netmask 255.255.255.255

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 3
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
static (inside,inside) interface access-list IN-OUT-INTERFACE
match ip inside host 10.2.2.5 inside host 64.100.0.5
static translation to 10.1.1.1
translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.2.2.5/0 to 10.1.1.1/0 using netmask 255.255.255.255

Phase: 5
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,inside) interface access-list IN-OUT-INTERFACE
match ip inside host 10.2.2.5 inside host 64.100.0.5
static translation to 10.1.1.1
translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
match ip inside host 10.3.3.6 inside host 10.1.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
Additional Information:

Phase: 7
Type: NAT
```

```
Subtype: host-limits
Result: ALLOW
Config:
static (inside,inside) 64.100.0.5 access-list OUT-IN-INTERFACE
match ip inside host 10.3.3.6 inside host 10.1.1.1
static translation to 64.100.0.5
translate_hits = 0, untranslate_hits = 1
Additional Information:

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 908, packet dispatched to next module

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

Packet Capture:

```
ASA# sh cap
capture capin type raw-data interface inside [Capturing - 1300 bytes]
match ip host 10.2.2.5 host 64.100.0.5
capture capout type raw-data interface inside [Capturing - 1300 bytes]
match ip host 10.1.1.1 host 10.3.3.6

ASA# sh cap capin

10 packets captured
1: 13:06:09.302047 10.2.2.5 > 64.100.0.5: icmp: echo request
2: 13:06:09.315276 64.100.0.5 > 10.2.2.5: icmp: echo reply
3: 13:06:09.342221 10.2.2.5 > 64.100.0.5: icmp: echo request
4: 13:06:09.381266 64.100.0.5 > 10.2.2.5: icmp: echo reply
5: 13:06:09.421227 10.2.2.5 > 64.100.0.5: icmp: echo request
6: 13:06:09.459204 64.100.0.5 > 10.2.2.5: icmp: echo reply
7: 13:06:09.494939 10.2.2.5 > 64.100.0.5: icmp: echo request
8: 13:06:09.534258 64.100.0.5 > 10.2.2.5: icmp: echo reply
9: 13:06:09.564210 10.2.2.5 > 64.100.0.5: icmp: echo request
10: 13:06:09.593261 64.100.0.5 > 10.2.2.5: icmp: echo reply
10 packets shown

ASA# sh cap capout

10 packets captured
1: 13:06:09.302367 10.1.1.1 > 10.3.3.6: icmp: echo request
2: 13:06:09.315230 10.3.3.6 > 10.1.1.1: icmp: echo reply
3: 13:06:09.342526 10.1.1.1 > 10.3.3.6: icmp: echo request
4: 13:06:09.381221 10.3.3.6 > 10.1.1.1: icmp: echo reply
```

```
5: 13:06:09.421517 10.1.1.1 > 10.3.3.6: icmp: echo request
6: 13:06:09.459174 10.3.3.6 > 10.1.1.1: icmp: echo reply
7: 13:06:09.495244 10.1.1.1 > 10.3.3.6: icmp: echo request
8: 13:06:09.534213 10.3.3.6 > 10.1.1.1: icmp: echo reply
9: 13:06:09.564500 10.1.1.1 > 10.3.3.6: icmp: echo request
10: 13:06:09.593215 10.3.3.6 > 10.1.1.1: icmp: echo reply
10 packets shown
```

Gerelateerde informatie

- ASA 8.3 Configuratie-gids: Voorwaarden voor Twice NAT
- ASA 8.4 Configuratie-gids: DNS en NAT
- ASA Pre-8.3 tot 8.3 NAT-configuratievoorbeelden