NAT-reflectie op de ASA for the VCS Express TelePresence-apparaten configureren

Inhoud

Inleiding

Dit document beschrijft hoe u een NAT-reflectieconfiguratie (Network adresomzetting) kunt implementeren op de Cisco adaptieve security applicaties voor speciale Cisco TelePresence-scenario's waarvoor dit soort NAT-configuratie op de firewall vereist is.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ASA (adaptieve security applicatie) basis-NAT configuratie.
- Cisco TelePresence Video Communication Server (VCS)-controle en VCS-expressbasisconfiguratie.

> Opmerking: Dit document is alleen bedoeld voor gebruik wanneer de aanbevolen implementatiemethode van een VCS-Expressway of Expressway-Edge met beide NIC-interfaces in verschillende DMZ's niet kan worden gebruikt. Raadpleeg voor meer informatie over de aanbevolen implementatie met behulp van dubbele NIC's de volgende link op pagina 60: Cisco TelePresence Video Communication Server Basic Configuration (Control met Expressway) Deployment Guide

Gebruikte componenten

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

- Cisco ASA 5500 en 5500-X Series toestellen die software versie 8.3 en hoger uitvoeren.
- Cisco VCS versie X8.x 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 live is, moet u de potentiële impact van elke opdracht begrijpen.

> **Opmerking**: Via het gehele document worden VCS-apparaten aangeduid als VCS-snelweg en VCS-regeling. Dezelfde configuratie is echter van toepassing op apparatuur met snelwegen-E en snelwegen-C.

Achtergrondinformatie

Volgens de documentatie van Cisco TelePresence, zijn er twee soorten TelePresence-scenario's waarin de NAT-reflectieconfiguratie op de VCS-conversie vereist is om de VCS-controle in staat te stellen met de VCS-sneltoets te communiceren via het openbare IP-adres van de VCS-snelweg.

Het eerste scenario omvat één enkel SUBD DE-Militarized Zone (DMZ) dat één VCS Expressway LAN-interface gebruikt en het tweede scenario heeft een 3-poorts FW DMZ die één VCS expressway LAN-interface gebruikt.

> **Tip**: Raadpleeg de implementatiehandleiding van Cisco TelePresence Video Communication Server Basic Configuration (Controle met expresse) om meer informatie over de TelePresence-implementatie te verkrijgen.

Cisco-technologieën niet aanbevolen voor de VCS C en E-implementatie

Het is belangrijk om op te merken dat de volgende topologieën NIET door Cisco worden aanbevolen. De aanbevolen implementatiemethodiek voor een VCS-snelweg of een snelrand van de snelweg is om twee verschillende DMZ's te gebruiken met de snelweg die een NIC heeft in elk van de DMZ's. Deze handleiding is bedoeld voor gebruik in omgevingen waarin de aanbevolen

implementatiemethode niet kan worden gebruikt.

Enkelvoudig subnetwerk DMZ met één VCS Express LAN-interface

In dit scenario kan FW A verkeer naar FW B (en omgekeerd) leiden. De VCS-snelweg maakt het mogelijk videoverkeer door FW B te laten passeren zonder dat de verkeersstroom op FW B van de buitenzijde naar de binneninterfaces afneemt. Met de VCS-snelweg wordt ook het FW-traject aan de publieke zijde geregeld.

Hier is een voorbeeld van dit scenario:

Deze inzet gebruikt deze componenten:

- Eén enkele Subnet DMZ (10.0.10.0/24) die bevat:
  De interne interface van FW A (10.0.10.1)De externe interface van FW B (10.0.10.2)De LAN1-interface van de VCS Express (10.0.10.3)
- Een LAN SUBSIDIE (10.0.30.0/24) die bevat:
  De interne interface van FW B (10.0.30.1)De LAN1-interface van de VCS-regeling (10.0.30.2)De netwerkinterface van Cisco TelePresence Management Server (TMS) (10.0.30.3)

Een statische één-op-één NAT is geconfigureerd op FW A, die de NAT voor het openbare adres 64.100.0.10 uitvoert naar het LAN1 IP-adres van de VCS-snelweg. De statische NAT-modus is ingeschakeld voor de LAN1-interface in de VCS-snelweg met een statisch NAT IP-adres van 64.100.0.10.

> Opmerking: U moet de Full Qualified Domain Name (FQDN) van de VCS Expressway op de VCS Control Secure Traversal Client Zone (peer address) invoeren zoals het van buiten het netwerk wordt gezien. De reden hiervoor is dat in de statische NAT-modus de VCS-snelweg vraagt om inkomende signalering en mediaverkeer naar zijn externe FQDN te sturen in plaats van naar zijn privé-naam. Dit betekent ook dat de externe FW het verkeer van VCS Control naar VCS Expressway externe FQDN moet toestaan. Dit staat bekend als NAT-reflectie en wordt mogelijk niet ondersteund door alle typen VW's.

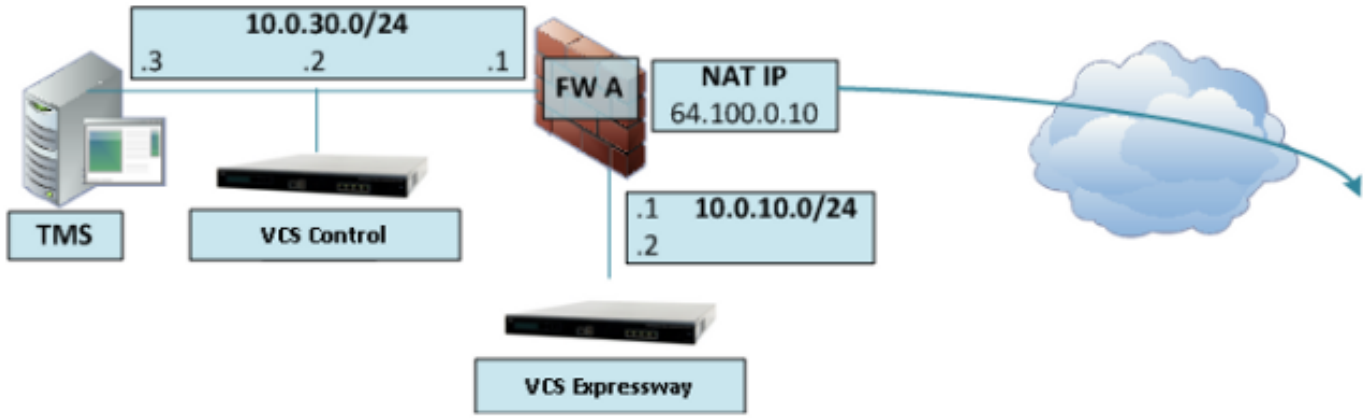
In dit voorbeeld moet FW B de NAT-reflectie van het verkeer mogelijk maken dat afkomstig is van de VCS Control die bestemd is voor het externe IP-adres (64.100.0.10) van de VCS-snelweg. De verplaatsen-zone op de VCS-regeling moet 64.100.0.10 zijn als peer-adres (na FQDN naar IP-conversie).

De VCS-snelweg moet worden geconfigureerd met een standaardgateway van **10.0.10.1**. Of de statische routes in dit scenario nodig zijn, hangt af van de mogelijkheden en instellingen van FW A en FW B. De communicatie van de VCS-controle naar de VCS-snelweg vindt plaats via het IP-adres 64.100.0.10 van de VCS-snelweg; en het retourverkeer van de VCS-snelweg naar de VCS-controle kan via de standaardgateway moeten verlopen.

De VCS Express kan aan Cisco TMS worden toegevoegd met het IP-adres 10.0.10.3 (of met IP-adres 64.100.0.10, als FW B dit toestaat), omdat de Cisco TMS-beheercommunicatie niet wordt beïnvloed door de statische NAT-instellingen op de VCS-snelweg.

3-poorts FW DMZ met één VCS snelle LAN-interface

Hier is een voorbeeld van dit scenario:



In deze plaatsing, wordt een 3-poorts FW gebruikt om:

- Een DMZ-subsysteem (10.0.10.0/24) dat bevat:
  De DMZ-interface van FW A (10.0.10.1)De LAN1-interface van de VCS Express (10.0.10.2)
- Een LAN SUBSIDIE (10.0.30.0/24) die bevat:
  De LAN-interface van FW A (10.0.30.1)De LAN1-interface van de VCS-regeling (10.0.30.2)De netwerkinterface van Cisco TMS (10.0.30.3)

Een statische één-op-één NAT is geconfigureerd op FW A, die de NAT van het openbare IP-adres 64.100.0.10 uitvoert naar het LAN1 IP-adres van de VCS-snelweg. De statische NAT-modus is ingeschakeld voor de LAN1-interface in de VCS-snelweg met een statisch NAT IP-adres van 64.100.0.10.

De VCS-snelweg moet worden geconfigureerd met een standaardgateway van 10.0.10.1. Aangezien deze gateway moet worden gebruikt voor al het verkeer dat de VCS-snelweg verlaat, zijn er geen statische routes vereist in dit soort toepassingen.

De verplaatsen-clientzone op de VCS-regeling moet worden geconfigureerd met een peer-adres dat overeenkomt met het statische NAT-adres van de VCS-snelweg (64.100.0.10 in dit voorbeeld) om dezelfde redenen als die welke in het vorige scenario zijn beschreven.

> Opmerking: Dit betekent dat FW A verkeer van de VCS Control met een IP-adres van de bestemming van 64.100.0.10 moet toestaan. Dit staat ook bekend als NAT-reflectie, en dit wordt niet ondersteund door alle typen VW's.

De VCS Express kan aan Cisco TMS worden toegevoegd met het IP-adres van 10.0.10.2 (of met IP-adres 64.100.0.10, als FW A dit toestaat), omdat de Cisco TMS-beheercommunicatie niet wordt beïnvloed door de statische NAT-instellingen op de VCS-snelweg.

Configureren

In dit deel wordt beschreven hoe de NAT-reflectie in de ASA moet worden configureren voor de twee verschillende VCS C- en E-implementatiescenario's.

Enkelvoudig subnetwerk DMZ met één VCS Express LAN-interface

Voor het eerste scenario moet u deze NAT-reflectieconfiguratie op FW A toepassen om de communicatie van de VCS Control (10.0.30.2) die bestemd is voor het externe IP-adres (64.100.0.10) van de VCS-snelweg mogelijk te maken:

In dit voorbeeld is het IP-adres van VCS Control **10.0.30.2/24** en is het IP-adres van de VCS-snelweg **10.0.10.3/24**.

Als u aanneemt dat het VCS Control IP-adres 10.0.30.2 blijft wanneer deze van de binnenkant naar de externe interface van FW B beweegt wanneer hij naar de VCS Express op zoek is met het IP-adres van de bestemming 64.100.0.10, dan wordt de NAT-reflectie-configuratie die u op FW B moet implementeren in deze voorbeelden getoond.

Voorbeeld voor ASA versies 8.3 en hoger:

```
object network obj-10.0.30.2
host 10.0.30.2

object network obj-10.0.10.3
host 10.0.10.3

object network obj-64.100.0.10
host 64.100.0.10

nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination static
obj-64.100.0.10 obj-10.0.10.3

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.
```

Voorbeeld voor ASA versies 8.2 en eerder:

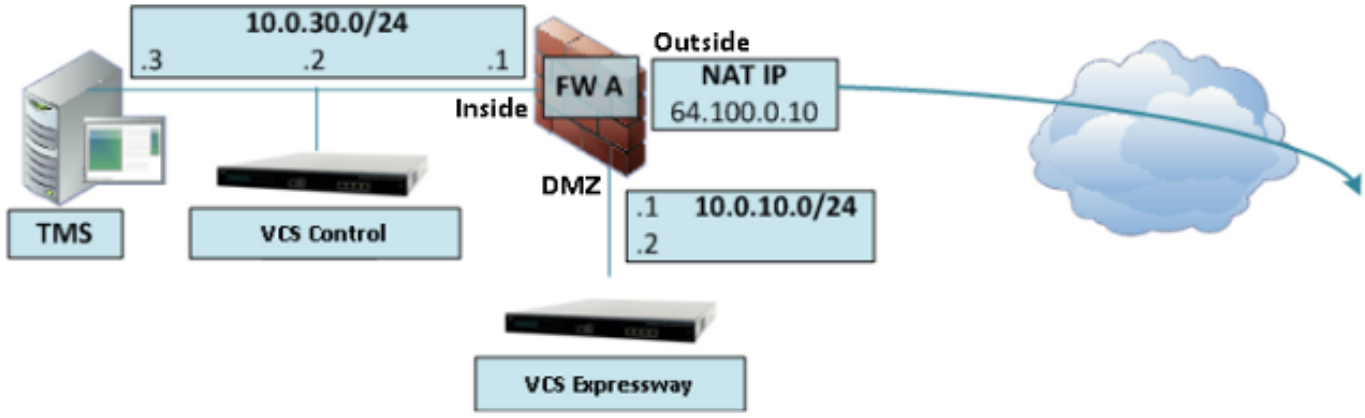
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE

access-list OUT-IN-INTERFACE extended permit ip host 10.0.10.3 host 10.0.30.2
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
```

> Opmerking: Het belangrijkste doel van deze NAT-reflectieconfiguratie is de VCS Control in staat te stellen de VCS-snelweg te bereiken, maar het VCS-snelwegadres te gebruiken in plaats van het particuliere IP-adres. Als het IP-adres van de bron van de VCS-controle tijdens deze NAT-vertaling wordt gewijzigd met een dubbele NAT-configuratie in plaats van

de zojuist getoonde NAT-configuratie, waardoor VCS-expressway verkeer kan zien vanaf zijn eigen openbare IP-adres, dan worden de telefoonservices voor de MRA-apparaten niet gestart. Dit is geen ondersteunde inzet zoals beschreven in paragraaf 3 over de onderstaande aanbevelingen.

3-poorts FW DMZ met één VCS snelle LAN-interface

Voor het tweede scenario moet u deze NAT-reflectieconfiguratie op FW A toepassen om de NAT-reflectie van inkomende verkeer van VCS Controle 10.0.30.2 mogelijk te maken dat bestemd is voor het externe IP-adres (64.100.0.10) van de VCS-snelweg:



In dit voorbeeld is het IP-adres van VCS Control **10.0.30.2/24** en is het IP-adres van de VCS-snelweg **10.0.10.2/24**.

Als u aanneemt dat het VCS Control IP-adres 10.0.30.2 blijft wanneer deze van binnenuit naar de DMZ-interface van FW A beweegt wanneer u naar de VCS Express op zoek gaat met het IP-adres van de bestemming 64.100.0.10, dan wordt de NAT-reflectie-configuratie die u op FW A moet implementeren in deze voorbeelden getoond.

Voorbeeld voor ASA versies 8.3 en hoger:

```
object network obj-10.0.30.2
host 10.0.30.2

object network obj-10.0.10.2
host 10.0.10.2

object network obj-64.100.0.10
host 64.100.0.10

nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination static
obj-64.100.0.10 obj-10.0.10.2

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

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

Voorbeeld voor ASA versies 8.2 en eerder:

```
access-list IN-DMZ-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,DMZ) 10.0.30.2 access-list IN-DMZ-INTERFACE
```

```
access-list DMZ-IN-INTERFACE extended permit ip host 10.0.10.2 host 10.0.30.2
static (DMZ,inside) 64.100.0.10 access-list DMZ-IN-INTERFACE
```

Opmerking: Het belangrijkste doel van deze NAT-reflectieconfiguratie is de VCS Control in staat te stellen de VCS-snelweg te bereiken, maar met het VCS-snelwegadres in plaats van het particuliere IP-adres. Als het IP-bronadres van de VCS-controle tijdens deze NAT-vertaling wordt gewijzigd met een dubbele NAT-configuratie in plaats van de zojuist getoonde NAT-configuratie, resulterend in VCS Expressway (VCS) die verkeer vanaf zijn eigen openbare IP-adres ziet, dan worden de telefoonservices voor de MRA-apparaten niet ter beschikking gesteld. Dit is geen ondersteunde inzet zoals beschreven in paragraaf 3 in de onderstaande aanbevelingen.

Verifiëren

Deze sectie verschaft de pakkettracer outputs die u in de ASA kunt zien om de NAT reflectie configuratie te bevestigen zoals nodig in zowel de VCS C- als E-implementatiescenario's.

Enkelvoudig subnetwerk DMZ met één VCS Express LAN-interface

Hier is de FW B-pakkettracer uitvoer voor ASA versies 8.3 en hoger:

```
FW-B# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.3
Additional Information:
NAT divert to egress interface outside
Untranslate 64.100.0.10/80 to 10.0.10.3/80

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

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.3
Additional Information:
Static translate 10.0.30.2/1234 to 10.0.30.2/1234

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
```

```
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.3
Additional Information:

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

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 2, 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
```

Hier is de FW B-pakkettracer uitvoer voor ASA versies 8.2 en eerder:

```
FW-B# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip outside host 10.0.10.3 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:
NAT divert to egress interface outside
Untranslate 64.100.0.10/0 to 10.0.10.3/0 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,outside) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 outside host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.0.30.2/0 to 10.0.30.2/0 using netmask 255.255.255.255
```

```
Phase: 4
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 outside host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip outside host 10.0.10.3 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 6
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip outside host 10.0.10.3 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
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 1166, 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
```

3-poorts FW DMZ met één VCS snelle LAN-interface

Hier is de FW A-pakkettracer uitvoer voor ASA versies 8.3 en hoger:

```
FW-A# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.2
Additional Information:
NAT divert to egress interface DMZ
Untranslate 64.100.0.10/80 to 10.0.10.2/80

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

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.2
Additional Information:
Static translate 10.0.30.2/1234 to 10.0.30.2/1234

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.2
Additional Information:

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

Phase: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 7, 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
```

Hier is de FW A-pakkettracer uitvoer voor ASA versies 8.2 en eerder:

FW-A# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

```
Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip DMZ host 10.0.10.2 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:
NAT divert to egress interface DMZ
Untranslate 64.100.0.10/0 to 10.0.10.2/0 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) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 DMZ host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.0.30.2/0 to 10.0.30.2/0 using netmask 255.255.255.255

Phase: 4
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,DMZ) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 DMZ host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip DMZ host 10.0.10.2 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 6
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
```

```
match ip DMZ host 10.0.10.2 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
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 1166, 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
```

Problemen oplossen

U kunt pakketvastlegging op de ASA interfaces configureren om de NAT-vertaling te bevestigen wanneer de pakketten de FW interfaces invoeren en verlaten die betrokken zijn.

Packet Capture Application voor de "3-poorts FW DMZ met één VCS Express LAN-interface"-scenario

```
FW-A# sh cap
capture capin type raw-data interface inside [Capturing - 5735 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capdmz type raw-data interface DMZ [Capturing - 5735 bytes]
  match ip host 10.0.10.2 host 10.0.30.2
FW-A# sh cap capin

71 packets captured
   1: 22:21:37.095270 10.0.30.2 > 64.100.0.10: icmp: echo request
   2: 22:21:37.100672 64.100.0.10 > 10.0.30.2: icmp: echo reply
   3: 22:21:37.101313 10.0.30.2 > 64.100.0.10: icmp: echo request
   4: 22:21:37.114373 64.100.0.10 > 10.0.30.2: icmp: echo reply
   5: 22:21:37.157371 10.0.30.2 > 64.100.0.10: icmp: echo request
   6: 22:21:37.174429 64.100.0.10 > 10.0.30.2: icmp: echo reply
   7: 22:21:39.234164 10.0.30.2 > 64.100.0.10: icmp: echo request
   8: 22:21:39.238528 64.100.0.10 > 10.0.30.2: icmp: echo reply
   9: 22:21:39.261110 10.0.30.2 > 64.100.0.10: icmp: echo request
  10: 22:21:39.270234 64.100.0.10 > 10.0.30.2: icmp: echo reply
  11: 22:21:47.170614 10.0.30.2.38953 > 64.100.0.10.23: S 1841210281:1841210281(0)
win 4128 <mss 536> 12: 22:21:47.198933 64.100.0.10.23 > 10.0.30.2.38953: S
3354834096:3354834096(0)
ack 1841210282 win 4128 <mss 536> 13: 22:21:47.235186 10.0.30.2.38953 > 64.100.0.10.23: . ack
3354834097
```

```
win 4128 14: 22:21:47.242815 64.100.0.10.23 > 10.0.30.2.38953: P 3354834097:3354834109(12)
ack 1841210282 win 4128 15: 22:21:47.243014 10.0.30.2.38953 > 64.100.0.10.23: P
1841210282:1841210294(12)
ack 3354834097 win 4128 16: 22:21:47.243258 10.0.30.2.38953 > 64.100.0.10.23: . ack 3354834097
win 4128 17: 22:21:47.261094 64.100.0.10.23 > 10.0.30.2.38953: P 3354834109:3354834151(42)
ack 1841210282 win 4128 18: 22:21:47.280411 64.100.0.10.23 > 10.0.30.2.38953: P
3354834151:3354834154(3)
ack 1841210294 win 4116 19: 22:21:47.280625 64.100.0.10.23 > 10.0.30.2.38953: P
3354834154:3354834157(3)
ack 1841210294 win 4116 20: 22:21:47.280838 64.100.0.10.23 > 10.0.30.2.38953: P
3354834157:3354834163(6)
ack 1841210294 win 4116 21: 22:21:47.281082 10.0.30.2.38953 > 64.100.0.10.23: P
1841210294:1841210297(3)
ack 3354834109 win 4116 22: 22:21:47.281296 10.0.30.2.38953 > 64.100.0.10.23: P
1841210297:1841210300(3)
ack 3354834109 win 4116
FW-A# sh cap capdmz

71 packets captured
   1: 22:21:37.095621 10.0.30.2 > 10.0.10.2: icmp: echo request
   2: 22:21:37.100626 10.0.10.2 > 10.0.30.2: icmp: echo reply
   3: 22:21:37.101343 10.0.30.2 > 10.0.10.2: icmp: echo request
   4: 22:21:37.114297 10.0.10.2 > 10.0.30.2: icmp: echo reply
   5: 22:21:37.157920 10.0.30.2 > 10.0.10.2: icmp: echo request
   6: 22:21:37.174353 10.0.10.2 > 10.0.30.2: icmp: echo reply
   7: 22:21:39.234713 10.0.30.2 > 10.0.10.2: icmp: echo request
   8: 22:21:39.238452 10.0.10.2 > 10.0.30.2: icmp: echo reply
   9: 22:21:39.261659 10.0.30.2 > 10.0.10.2: icmp: echo request
  10: 22:21:39.270158 10.0.10.2 > 10.0.30.2: icmp: echo reply
  11: 22:21:47.170950 10.0.30.2.38953 > 10.0.10.2.23: S 2196345248:2196345248(0)
win 4128 <mss 536> 12: 22:21:47.198903 10.0.10.2.23 > 10.0.30.2.38953: S
1814294604:1814294604(0)
ack 2196345249 win 4128 <mss 536> 13: 22:21:47.235263 10.0.30.2.38953 > 10.0.10.2.23: . ack
1814294605 win 4128 14: 22:21:47.242754 10.0.10.2.23 > 10.0.30.2.38953: P
1814294605:1814294617(12)
ack 2196345249 win 4128 15: 22:21:47.243105 10.0.30.2.38953 > 10.0.10.2.23: P
2196345249:2196345261(12)
ack 1814294605 win 4128 16: 22:21:47.243319 10.0.30.2.38953 > 10.0.10.2.23: . ack 1814294605 win
4128 17: 22:21:47.260988 10.0.10.2.23 > 10.0.30.2.38953: P 1814294617:1814294659(42)
ack 2196345249 win 4128 18: 22:21:47.280335 10.0.10.2.23 > 10.0.30.2.38953: P
1814294659:1814294662(3)
ack 2196345261 win 4116 19: 22:21:47.280564 10.0.10.2.23 > 10.0.30.2.38953: P
1814294662:1814294665(3)
ack 2196345261 win 4116 20: 22:21:47.280777 10.0.10.2.23 > 10.0.30.2.38953: P
1814294665:1814294671(6)
ack 2196345261 win 4116 21: 22:21:47.281143 10.0.30.2.38953 > 10.0.10.2.23: P
2196345261:2196345264(3)
ack 1814294617 win 4116 22: 22:21:47.281357 10.0.30.2.38953 > 10.0.10.2.23: P
2196345264:2196345267(3)
ack 1814294617 win 4116
```

Packet Capture Appliance voor het scenario "Single Subnet DMZ met één VCS Express LAN-interface"

```
FW-B# sh cap
capture capin type raw-data interface inside [Capturing - 5815 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capout type raw-data interface outside [Capturing - 5815 bytes]
  match ip host 10.0.10.3 host 10.0.30.2

FW-B# sh cap capin
```

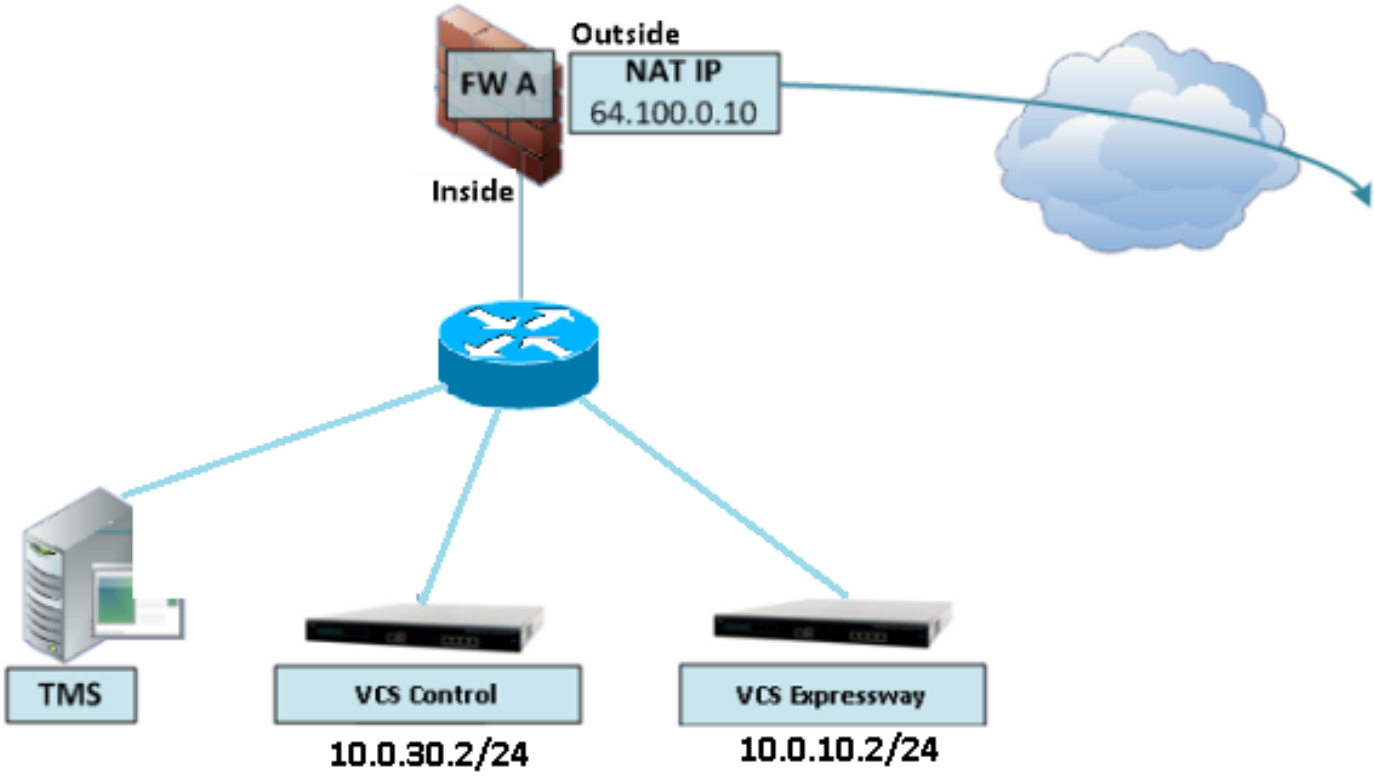
```
72 packets captured
   1: 22:30:06.783681 10.0.30.2 > 64.100.0.10: icmp: echo request
   2: 22:30:06.847856 64.100.0.10 > 10.0.30.2: icmp: echo reply
   3: 22:30:06.877624 10.0.30.2 > 64.100.0.10: icmp: echo request
   4: 22:30:06.900710 64.100.0.10 > 10.0.30.2: icmp: echo reply
   5: 22:30:06.971598 10.0.30.2 > 64.100.0.10: icmp: echo request
   6: 22:30:06.999551 64.100.0.10 > 10.0.30.2: icmp: echo reply
   7: 22:30:07.075649 10.0.30.2 > 64.100.0.10: icmp: echo request
   8: 22:30:07.134499 64.100.0.10 > 10.0.30.2: icmp: echo reply
   9: 22:30:07.156409 10.0.30.2 > 64.100.0.10: icmp: echo request
  10: 22:30:07.177496 64.100.0.10 > 10.0.30.2: icmp: echo reply
  11: 22:30:13.802525 10.0.30.2.41596 > 64.100.0.10.23: S 1119515693:1119515693(0)
win 4128 <mss 536> 12: 22:30:13.861100 64.100.0.10.23 > 10.0.30.2.41596: S
2006020203:2006020203(0)
ack 1119515694 win 4128 <mss 536> 13: 22:30:13.935864 10.0.30.2.41596 > 64.100.0.10.23: . ack
2006020204 win 4128 14: 22:30:13.946804 10.0.30.2.41596 > 64.100.0.10.23: P
1119515694:1119515706(12)
ack 2006020204 win 4128 15: 22:30:13.952679 10.0.30.2.41596 > 64.100.0.10.23: . ack 2006020204
win 4128 16: 22:30:14.013686 64.100.0.10.23 > 10.0.30.2.41596: P 2006020204:2006020216(12)
ack 1119515706 win 4116 17: 22:30:14.035352 64.100.0.10.23 > 10.0.30.2.41596: P
2006020216:2006020256(40)
ack 1119515706 win 4116 18: 22:30:14.045758 64.100.0.10.23 > 10.0.30.2.41596: P
2006020256:2006020259(3)
ack 1119515706 win 4116 19: 22:30:14.046781 64.100.0.10.23 > 10.0.30.2.41596: P
2006020259:2006020262(3)
ack 1119515706 win 4116 20: 22:30:14.047788 64.100.0.10.23 > 10.0.30.2.41596: P
2006020262:2006020268(6)
ack 1119515706 win 4116 21: 22:30:14.052151 10.0.30.2.41596 > 64.100.0.10.23: P
1119515706:1119515709(3)
ack 2006020256 win 4076 22: 22:30:14.089183 10.0.30.2.41596 > 64.100.0.10.23: P
1119515709:1119515712(3)
ack 2006020256 win 4076
ASA1# show cap capout

72 packets captured
   1: 22:30:06.784871 10.0.30.2 > 10.0.10.3: icmp: echo request
   2: 22:30:06.847688 10.0.10.3 > 10.0.30.2: icmp: echo reply
   3: 22:30:06.878769 10.0.30.2 > 10.0.10.3: icmp: echo request
   4: 22:30:06.900557 10.0.10.3 > 10.0.30.2: icmp: echo reply
   5: 22:30:06.972758 10.0.30.2 > 10.0.10.3: icmp: echo request
   6: 22:30:06.999399 10.0.10.3 > 10.0.30.2: icmp: echo reply
   7: 22:30:07.076808 10.0.30.2 > 10.0.10.3: icmp: echo request
   8: 22:30:07.134422 10.0.10.3 > 10.0.30.2: icmp: echo reply
   9: 22:30:07.156959 10.0.30.2 > 10.0.10.3: icmp: echo request
  10: 22:30:07.177420 10.0.10.3 > 10.0.30.2: icmp: echo reply
  11: 22:30:13.803104 10.0.30.2.41596 > 10.0.10.3.23: S 2599614130:2599614130(0)
win 4128 <mss 536> 12: 22:30:13.860947 10.0.10.3.23 > 10.0.30.2.41596: S
4158597009:4158597009(0)
ack 2599614131 win 4128 <mss 536> 13: 22:30:13.936017 10.0.30.2.41596 > 10.0.10.3.23: . ack
4158597010 win 4128 14: 22:30:13.946941 10.0.30.2.41596 > 10.0.10.3.23: P
2599614131:2599614143(12)
ack 4158597010 win 4128 15: 22:30:13.952801 10.0.30.2.41596 > 10.0.10.3.23: . ack 4158597010 win
4128 16: 22:30:14.013488 10.0.10.3.23 > 10.0.30.2.41596: P 4158597010:4158597022(12)
ack 2599614143 win 4116 17: 22:30:14.035108 10.0.10.3.23 > 10.0.30.2.41596: P
4158597022:4158597062(40)
ack 2599614143 win 4116 18: 22:30:14.045377 10.0.10.3.23 > 10.0.30.2.41596: P
4158597062:4158597065(3)
ack 2599614143 win 4116 19: 22:30:14.046384 10.0.10.3.23 > 10.0.30.2.41596: P
4158597065:4158597068(3)
ack 2599614143 win 4116 20: 22:30:14.047406 10.0.10.3.23 > 10.0.30.2.41596: P
4158597068:4158597074(6)
ack 2599614143 win 4116 21: 22:30:14.052395 10.0.30.2.41596 > 10.0.10.3.23: P
2599614143:2599614146(3)
ack 4158597062 win 4076 22: 22:30:14.089427 10.0.30.2.41596 > 10.0.10.3.23: P
```

```
2599614146:2599614149(3)
ack 4158597062 win 4076
```

Aanbevelingen

1. Vermijd de implementatie van niet-ondersteunde topologieën

Als u bijvoorbeeld zowel de VCS Control- als VCS-snelweg achter de ASA-interface hebt aangesloten, zoals in dit scenario wordt aangegeven:



Dit soort implementatie vereist dat het IP-adres van de VCS-controle wordt vertaald naar het binnen-IP-adres van de ASA om het retourverkeer te dwingen terug te keren naar de ASA om asymmetrische routeproblemen voor de NAT-reflectie te voorkomen.

> **Opmerking: Als het IP-bronadres van de VCS-controle tijdens deze NAT-vertaling wordt gewijzigd met een dubbele NAT-configuratie in plaats van de voorgestelde NAT-reflectieconfiguratie, dan ziet de VCS-sneltoets verkeer vanaf zijn eigen openbare IP-adres, dan worden de telefoondiensten voor de MRA-apparaten niet geactiveerd. Dit is geen ondersteunde inzet zoals beschreven in paragraaf 3 in de onderstaande aanbevelingen.**

Dit gezegd hebbende wordt het ten zeerste aanbevolen de VCS-snelweg in te voeren als een implementatie van een E-netwerk met twee interfaces, in plaats van de enige NIC met NAT-reflectie.

2. Zorg ervoor dat de SIP/H.323-inspectie volledig is uitgeschakeld op de betrokken firewalls

Het wordt sterk aanbevolen om SIP en H.323 inspectie op firewalls uit te schakelen die netwerkverkeer naar of van een snelweg-E afhandelen. Als deze optie wordt ingeschakeld, wordt vaak vastgesteld dat SIP/H.323-inspectie een negatieve invloed heeft op de ingebouwde

firewall/NAT-traversale functionaliteit.

Dit is een voorbeeld van hoe te om SIP en H.323 inspecties op de ASA uit te schakelen.

```
policy-map global_policy
 class inspection_default
  no inspect h323 h225
  no inspect h323 ras
  no inspect sip
```

3. Zorg ervoor dat uw huidige implementatie van de snelweg voldoet aan de volgende vereisten die door de Cisco-telepresence-ontwikkelaars worden voorgesteld

- De NAT-configuratie tussen de expressway-C en Expressway-E wordt niet ondersteund.
- Deze wordt niet ondersteund wanneer de snelweg-C en expressway-E NATed op hetzelfde openbare IP-adres krijgen, bijvoorbeeld:
  Expressway-C is ingesteld met IP-adres 10.1.1.1
  Expressway-E is één NIC met IP-adres 10.2.2.1 en een statische NAT is geconfigureerd in de firewall met openbaar IP-adres 64.100.0.10
  Dan kan de Expressway-C niet NATted worden naar hetzelfde openbare adres 64.100.0.10

Aanbevolen implementatie van VCS-sneltoets

De aanbevolen implementatie voor de VCS-snelweg in plaats van de VCS-snelweg met de NAT-reflectieconfiguratie is de dubbele netwerkinterfaces/dubbele NIC VCS-snelimplementatie. Voor meer informatie dient u de volgende link te controleren.

ASA NAT-configuratie en -aanbevelingen voor de implementatie van snelwegen-E met twee netwerken.

Gerelateerde informatie

- ASA NAT-configuratie en -aanbevelingen voor de implementatie van snelwegen-E met twee netwerken
- Cisco TelePresence Video Communication Server Basic Configuration (Controle met sneltoets)
- Cisco IP-poortgebruik voor firewall-trajecten
- Een Cisco VCS-snelweg plaatsen in een DMZ in plaats van op het openbare internet