Configuración de la Reflexión NAT en el ASA para los dispositivos de VCS Expressway TelePresence

Contenido

Introducción

Este documento describe cómo implementar una configuración de reflexión de traducción de direcciones de red (NAT) en los Cisco Adaptive Security Appliances para escenarios especiales de Cisco TelePresence que requieren este tipo de configuración NAT en el firewall.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración básica de NAT de Cisco ASA (Adaptive Security Appliance).
- Configuración básica de Cisco TelePresence Video Communication Server (VCS) Control y VCS Expressway.

> **Nota:** Este documento está pensado para ser utilizado solamente cuando no se pueda utilizar el método de implementación recomendado de VCS-Expressway o Expressway-Edge con ambas interfaces NIC en diferentes DMZ. Para obtener más información sobre la implementación recomendada mediante NIC duales, consulte el siguiente enlace en la página 60: Guía de implementación de la configuración básica de Cisco TelePresence Video Communication Server (Control con Expressway)

Componentes Utilizados

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

- Dispositivos Cisco ASA serie 5500 y 5500-X que ejecutan la versión de software 8.3 y posteriores.
- Cisco VCS versión X8.x y posteriores.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

> **Nota**: A través de todo el documento, los dispositivos VCS se denominan VCS Expressway y VCS Control. Sin embargo, la misma configuración se aplica a los dispositivos Expressway-E y Expressway-C.

Antecedentes

Según la documentación de Cisco TelePresence, hay dos tipos de escenarios de TelePresence donde se requiere la configuración de reflexión de NAT en los FW para permitir que VCS Control se comunique con VCS Expressway a través de la dirección IP pública de VCS Expressway.

El primer escenario implica una única zona desmilitarizada de subred (DMZ) que utiliza una única interfaz LAN de VCS Expressway, y el segundo escenario implica una DMZ de FW de 3 puertos que utiliza una única interfaz LAN de VCS Expressway.

> **Consejo:** Para obtener más detalles sobre la implementación de TelePresence, refiérase a la guía de implementación Configuración básica de Cisco TelePresence Video Communication Server (Control con Expressway).

Topologías de Cisco no recomendadas para la implementación de VCS C y E

Es importante tener en cuenta que Cisco NO recomienda las siguientes topologías. La

metodología de implementación recomendada para VCS Expressway o Expressway es utilizar dos DMZ diferentes con Expressway que tenga una NIC en cada una de las DMZ. Esta guía se ha diseñado para utilizarse en entornos en los que no se puede utilizar el método de implementación recomendado.

DMZ de subred única con interfaz LAN VCS Expressway

En esta situación, FW A puede enrutar el tráfico al FW B (y viceversa). VCS Expressway permite que el tráfico de vídeo pase a través de FW B sin reducir el flujo de tráfico en FW B desde el exterior a las interfaces interiores. VCS Expressway también gestiona la inversión de FW en su lado público.

Este es un ejemplo de este escenario:

Esta implementación utiliza estos componentes:

- Una única subred DMZ (10.0.10.0/24) que contiene:
  La interfaz interna de FW A (10.0.10.1)La interfaz externa de FW B (10.0.10.2)La interfaz LAN1 de VCS Expressway (10.0.10.3)
- Una subred LAN (10.0.30.0/24) que contiene:
  La interfaz interna de FW B (10.0.30.1)La interfaz LAN1 del VCS Control (10.0.30.2)La interfaz de red del servidor de administración de Cisco TelePresence (TMS) (10.0.30.3)

Se ha configurado una NAT estática uno a uno en FW A, que realiza la NAT para la dirección pública 64.100.0.10 a la dirección IP LAN1 de VCS Expressway. El modo NAT estático se ha habilitado para la interfaz LAN1 en VCS Expressway, con una dirección IP NAT estática de 64.100.0.10.

> **Nota:** Debe introducir el nombre de dominio completo (FQDN) de VCS Expressway en la zona de cliente transversal seguro (dirección de peer) de VCS Control como se ve desde fuera de la red. La razón de esto es que en el modo NAT estático, VCS Expressway solicita que la señalización entrante y el tráfico de medios se envíen a su FQDN externo en lugar de a su nombre privado. Esto también significa que el FW externo debe permitir el tráfico del control VCS al FQDN externo de VCS Expressway. Esto se conoce como reflexión NAT y puede que no sea compatible con todos los tipos de FW.

En este ejemplo, FW B debe permitir la reflexión NAT del tráfico que proviene del control VCS destinado a la dirección IP externa (64.100.0.10) de VCS Expressway. La zona transversal en el control VCS debe tener 64.100.0.10 como dirección de peer (después de la conversión de FQDN a IP).

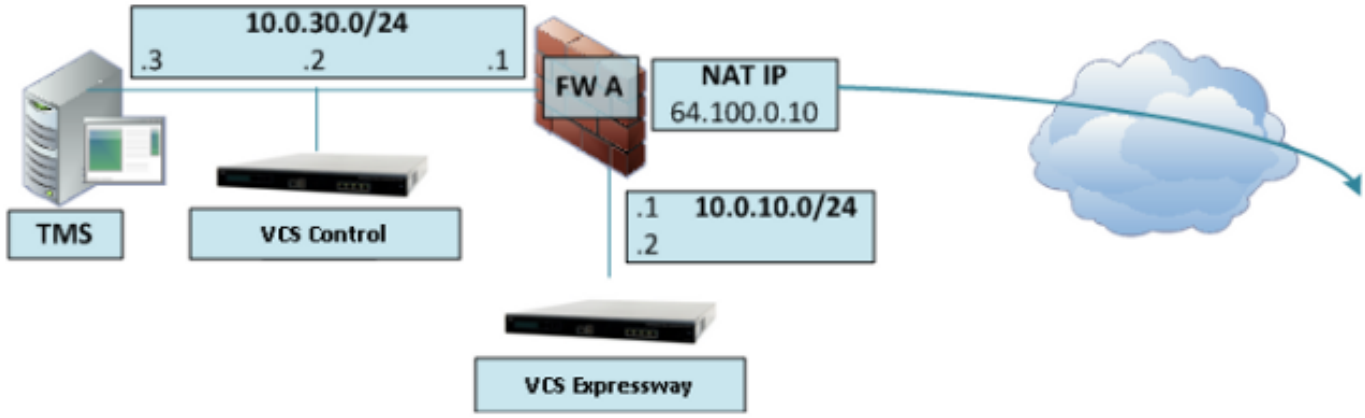
VCS Expressway debe configurarse con un gateway predeterminado de **10.0.10.1**. Si las rutas estáticas son necesarias en este escenario depende de las capacidades y la configuración de FW A y FW B. La comunicación del VCS Control a VCS Expressway se produce a través de la

dirección IP 64.100.0.10 de VCS Expressway; y el tráfico de retorno de VCS Expressway al VCS Control puede tener que pasar a través del gateway predeterminado.

VCS Expressway se puede agregar a Cisco TMS con la dirección IP 10.0.10.3 (o con la dirección IP 64.100.0.10, si FW B lo permite), ya que la comunicación de administración de Cisco TMS no se ve afectada por la configuración de modo NAT estática en VCS Expressway.

DMZ de FW de 3 puertos con interfaz LAN VCS Expressway

Este es un ejemplo de este escenario:



En esta implementación, se utiliza un FW de 3 puertos para crear:

- Subred DMZ (10.0.10.0/24) que contiene:
  Interfaz DMZ de FW A (10.0.10.1)La interfaz LAN1 de VCS Expressway (10.0.10.2)
- Una subred LAN (10.0.30.0/24) que contiene:
  La interfaz LAN de FW A (10.0.30.1)La interfaz LAN1 del VCS Control (10.0.30.2)La interfaz de red de Cisco TMS (10.0.30.3)

Se ha configurado una NAT estática uno a uno en FW A, que realiza la NAT de la dirección IP pública 64.100.0.10 a la dirección IP LAN1 de VCS Expressway. El modo NAT estático se ha habilitado para la interfaz LAN1 en VCS Expressway, con una dirección IP NAT estática de 64.100.0.10.

VCS Expressway debe configurarse con un gateway predeterminado de 10.0.10.1. Dado que este gateway debe utilizarse para todo el tráfico que sale de VCS Expressway, no se requieren rutas estáticas en este tipo de implementación.

La zona de cliente transversal en el control VCS debe configurarse con una dirección de peer que coincida con la dirección NAT estática de VCS Expressway (64.100.0.10 en este ejemplo) por las mismas razones que las descritas en el escenario anterior.

> **Nota:** Esto significa que FW A debe permitir el tráfico del control VCS con una dirección IP de destino de 64.100.0.10. Esto también se conoce como reflexión NAT, y se debe tener en cuenta que esto no es soportado por todos los tipos de FW.

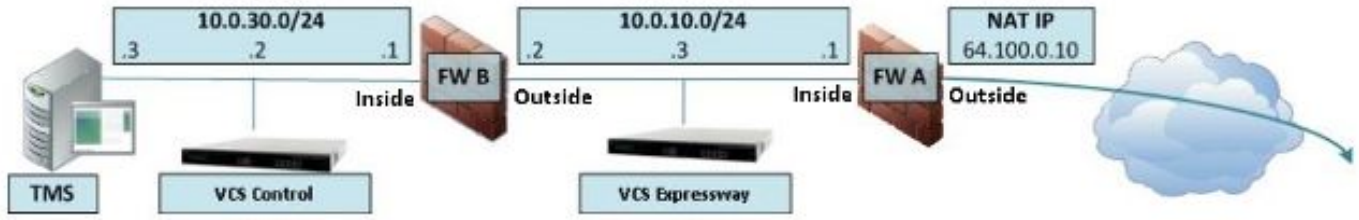
VCS Expressway se puede agregar a Cisco TMS con la dirección IP 10.0.10.2 (o con la dirección IP 64.100.0.10, si FW A lo permite), ya que la comunicación de administración de Cisco TMS no se ve afectada por la configuración de modo NAT estática en VCS Expressway.

Configurar

Esta sección describe cómo configurar la reflexión NAT en el ASA para los dos diferentes escenarios de implementación de VCS C y E.

DMZ de subred única con interfaz LAN VCS Expressway

Para el primer escenario, debe aplicar esta configuración de reflexión de NAT en FW A para permitir la comunicación del VCS Control (10.0.30.2) que está destinado a la dirección IP externa (64.100.0.10) de VCS Expressway:



En este ejemplo, la dirección IP del control de VCS es **10.0.30.2/24**, y la dirección IP de VCS Expressway es **10.0.10.3/24**.

Si se supone que la dirección IP 10.0.30.2 del control de VCS permanece cuando se mueve del interior a la interfaz exterior de FW B cuando se busca VCS Expressway con la dirección IP de destino 64.100.0.10, entonces la configuración de reflexión de NAT que debería implementar en FW B se muestra en estos ejemplos.

Ejemplo para ASA versiones 8.3 y posteriores:

```
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.
```

Ejemplo para ASA versiones 8.2 y anteriores:

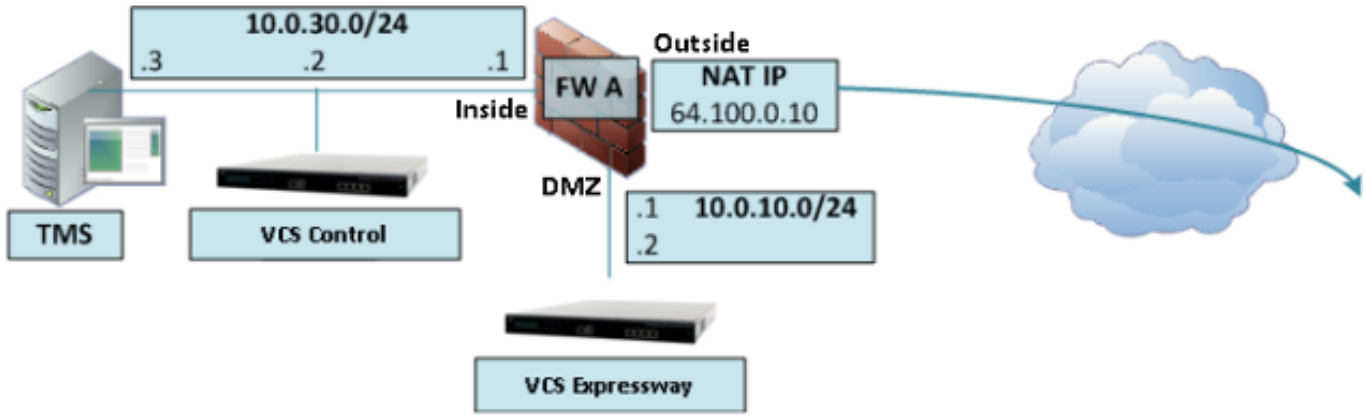
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE

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
```

Nota: El objetivo principal de esta configuración de reflexión de NAT es permitir que VCS

Control pueda alcanzar la expressway de VCS, pero utilizando la dirección IP pública de la expressway de VCS en lugar de su dirección IP privada. Si la dirección IP de origen del control VCS se cambia durante esta traducción NAT con una configuración NAT dos veces en lugar de la configuración NAT sugerida que se muestra, lo que hace que VCS Expressway vea el tráfico de su propia dirección IP pública, entonces los servicios telefónicos para los dispositivos MRA no se activarán. No se trata de una implementación compatible según la sección 3 de la sección de recomendaciones que figura a continuación.

DMZ de FW de 3 puertos con interfaz LAN VCS Expressway

Para el segundo escenario, debe aplicar esta configuración de reflexión de NAT en FW A para permitir el reflejo de NAT del tráfico entrante desde VCS Control 10.0.30.2 que está destinado a la dirección IP externa (64.100.0.10) de VCS Expressway:



En este ejemplo, la dirección IP del control de VCS es **10.0.30.2/24**, y la dirección IP de VCS Expressway es **10.0.10.2/24**.

Si se supone que la dirección IP 10.0.30.2 del control de VCS permanece cuando se mueve del interior a la interfaz DMZ del FW A cuando se busca VCS Expressway con la dirección IP de destino 64.100.0.10, entonces la configuración de reflexión de NAT que debería implementar en el FW A se muestra en estos ejemplos.

Ejemplo para ASA versiones 8.3 y posteriores:

```
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.
```

Ejemplo para ASA versiones 8.2 y anteriores:

```
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
```

> **Nota:** El objetivo principal de esta configuración de reflexión de NAT es permitir que VCS Control pueda alcanzar la expressway de VCS, pero con la dirección IP pública de la expressway de VCS en lugar de su dirección IP privada. Si la dirección IP de origen del control VCS se cambia durante esta traducción NAT con una configuración NAT dos veces en lugar de la configuración NAT sugerida que se muestra, lo que hace que VCS Expressway vea el tráfico de su propia dirección IP pública, entonces los servicios telefónicos para los dispositivos MRA no se activarán. No se trata de una implementación compatible según la sección 3 de la siguiente sección de recomendaciones.

Verificación

Esta sección proporciona los resultados del rastreador de paquetes que puede ver en el ASA para confirmar que la configuración de la reflexión NAT funciona según sea necesario en ambos escenarios de implementación de VCS C y E.

DMZ de subred única con interfaz LAN VCS Expressway

Esta es la salida del rastreador de paquetes FW B para las versiones 8.3 y posteriores de ASA:

```
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
```

Esta es la salida del rastreador de paquetes FW B para las versiones 8.2 y anteriores de ASA:

```
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
```

DMZ de FW de 3 puertos con interfaz LAN VCS Expressway

Esta es la salida del rastreador de paquetes FW A para las versiones 8.3 y posteriores de ASA:

```
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
```

Esta es la salida del rastreador de paquetes FW A para las versiones 8.2 y anteriores de ASA:

```
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
```

Troubleshoot

Puede configurar las capturas de paquetes en las interfaces ASA para confirmar la traducción NAT cuando los paquetes ingresan y dejan las interfaces FW involucradas.

Captura de paquetes aplicada a la situación "DMZ de firewall de 3 puertos con interfaz LAN de VCS Expressway"

```
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
```

Captura de paquetes aplicada para el escenario "DMZ de subred única con interfaz LAN de VCS Expressway"

```
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]
```

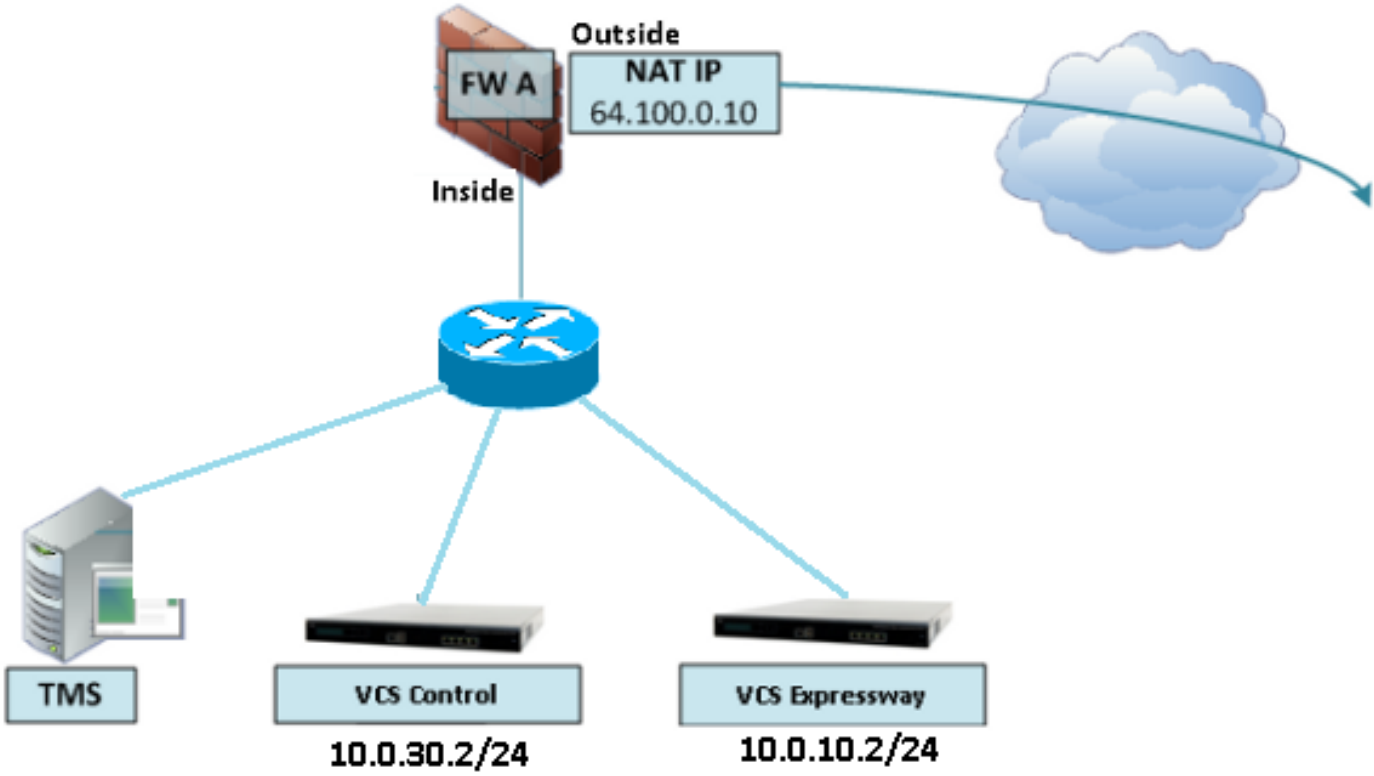
```
  match ip host 10.0.10.3 host 10.0.30.2

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
```

Recomendaciones

1. Evitar la implementación de cualquier topología no admitida

Por ejemplo, si tiene tanto VCS Control como VCS Expressway conectados detrás de la interfaz ASA interna, tal como se muestra en este escenario:



Este tipo de implementación requiere que la dirección IP del control de VCS se traduzca a la dirección IP interna del ASA para obligar al tráfico de retorno a regresar al ASA para evitar problemas de ruta asimétrica para la reflexión de NAT.

> **Nota: Si la dirección IP de origen del control VCS se cambia durante esta traducción NAT con una configuración NAT dos veces en lugar de la configuración de reflexión NAT sugerida, VCS Expressway verá el tráfico de su propia dirección IP pública, entonces los servicios telefónicos para los dispositivos MRA no aparecerán. No se trata de una implementación compatible según la sección 3 de la siguiente sección de recomendaciones.**

Dicho esto, se recomienda implementar VCS Expressway como una implementación de interfaces de red duales de Expressway-E en lugar de la NIC única con reflexión NAT.

2. Asegúrese de que la inspección de SIP/H.323 esté completamente inhabilitada en los firewalls involucrados

Se recomienda inhabilitar la inspección de SIP y H.323 en firewalls que gestionan el tráfico de red hacia o desde Expressway-E. Cuando se activa, la inspección de SIP/H.323 suele afectar negativamente a la funcionalidad transversal NAT/firewall incorporado de Expressway.

Este es un ejemplo de cómo inhabilitar las inspecciones SIP y H.323 en el ASA.

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

3. Asegúrese de que su implementación de Expressway cumple los siguientes requisitos sugeridos por los desarrolladores de Cisco TelePresence

- No se admite la configuración NAT entre Expressway-C y Expressway-E.
- No se admite cuando Expressway-C y Expressway-E, obtienen NATed a la misma dirección IP pública, por ejemplo:
  Expressway-C está configurado con la dirección IP 10.1.1.1
  Expressway-E tiene una única NIC configurada con la dirección IP 10.2.2.1 y una NAT estática configurada en el firewall con la dirección IP pública 64.100.0.10
  A continuación, Expressway-C no se puede NATted a la misma dirección pública 64.100.0.10

Implementación de VCS Expressway recomendada

La implementación recomendada para VCS Expressway en lugar de VCS Expressway con la configuración de reflexión de NAT es la implementación de dos interfaces de red/doble NIC VCS Expressway; para obtener más información, consulte el siguiente enlace.

Configuración de ASA NAT y recomendaciones para la implementación de interfaces de red duales de Expressway-E.

Información Relacionada

- Configuración de ASA NAT y recomendaciones para la implementación de interfaces de red duales de Expressway-E
- Guía de implementación de Cisco TelePresence Video Communication Server Basic Configuration (Control con Expressway)
- Uso del puerto IP de Cisco Expressway para firewall transversal
- Colocación de Cisco VCS Expressway en una DMZ en lugar de en Internet pública