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

Contenido

Introducción

Este documento describe cómo implementar una configuración de la reflexión del Network Address Translation (NAT) en los dispositivos de seguridad adaptantes de Cisco para los escenarios especiales del Cisco TelePresence que requieren esta clase de configuración del NAT en el Firewall.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración del NAT básica de Cisco ASA (dispositivo de seguridad adaptante)
- Control del servidor del comunicación mediante video del Cisco TelePresence (VCS) y configuración básica de Expressway del VCS

> **Note**: Este documento se piensa para ser utilizado solamente cuando el método de implementación recomendado de VCS-Expressway o de un Expressway-borde con ambas interfaces NIC en diversos DMZ no puede ser utilizado. Para más información sobre el despliegue recomendado usando los NIC duales satisfaga marcan el siguiente enlace en la página 60: Guía de despliegue de la configuración básica del servidor del comunicación mediante video del Cisco TelePresence (control con Expressway)

Componentes Utilizados

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

- Dispositivos de las 5500 y 5500-X Series de Cisco ASA que funcionan con la versión de software 8.3 y posterior.
- Versión X8.x del VCS de Cisco y posterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

> **Note**: A través del documento entero, los dispositivos del VCS se refieren como control del VCS Expressway y del VCS. Sin embargo, la misma configuración se aplica a los dispositivos de Expressway-e y de Expressway-C.

Antecedentes

Según la documentación del Cisco TelePresence, hay dos clases de escenarios del TelePresence donde la configuración de la reflexión NAT se requiere en los FW para permitir que el control del VCS comunique con el VCS Expressway vía el IP Address público de Expressway del VCS.

El primer escenario implica un De-Militarized Zone de la subred única (DMZ) ese las aplicaciones una sola interfaz LAN de Expressway del VCS, y el segundo escenario implica un 3-port FW DMZ que utilice una sola interfaz LAN de Expressway del VCS.

> **Tip**: Para obtener más detalles sobre la implementación del TelePresence, refiera al Guía de despliegue de la configuración básica del servidor del comunicación mediante video del Cisco TelePresence (control con Expressway).

Topologías de Cisco NON-recomendadas para el C del VCS y la implementación E

Es importante observar que las topologías siguientes no son recomendadas por Cisco. La metodología recomendada del despliegue para un VCS Expressway o el borde de Expressway es utilizar dos diversos DMZ con Expressway que tiene un NIC en cada uno de los DMZ. Esta guía se significa para ser utilizada en los entornos donde el método de implementación recomendado no puede ser utilizado.

Subred única DMZ con la sola interfaz LAN de Expressway del VCS

En este escenario, el FW *A* puede rutear el tráfico a FW *B* (y vice versa). El VCS Expressway permite que el tráfico de video sea pasado con FW B sin una reducción en el flujo de tráfico en FW B del exterior a las interfaces interiores. El VCS Expressway también maneja el traversal FW en su lado público.

Aquí está un ejemplo de este escenario:

Este despliegue utiliza estos componentes:

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

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

> **Note**: Usted debe ingresar el Nombre de dominio totalmente calificado (FQDN) (FQDN) del VCS Expressway en la zona segura del cliente del traversal del control del VCS (dirección de peer) como cómo se ve desde fuera de la red. La razón de esto, es ésa en el modo NAT estática, el VCS Expressway pide que la señalización entrante y los media trafiquen estén enviados a su externo FQDN bastante que su nombre privado. Esto también significa que el externo FW debe permitir el tráfico del control del VCS al externo FQDN de Expressway del VCS. Esto se conoce como reflexión NAT, y no se pudo soportar por todos los tipos de FW.

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

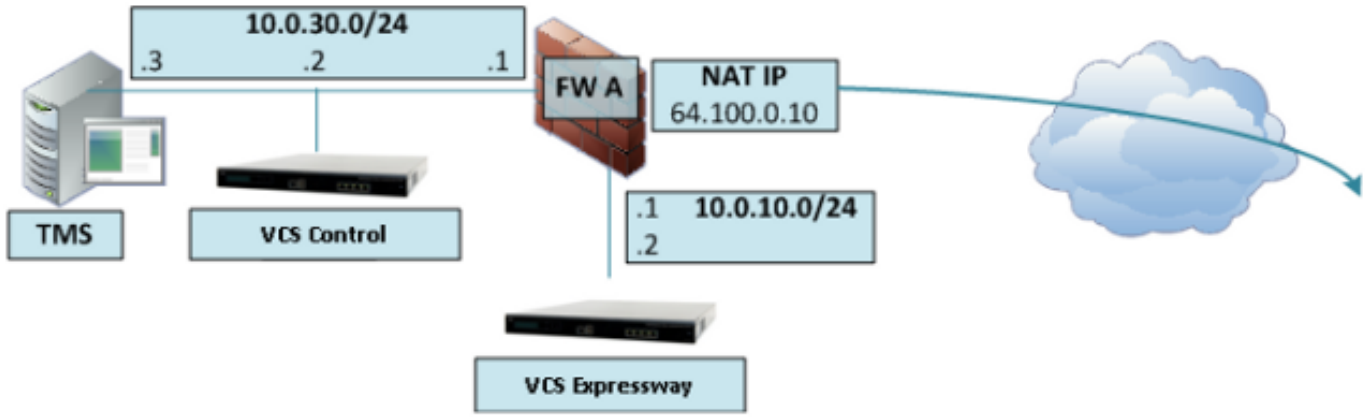
El VCS Expressway se debe configurar con un default gateway de **10.0.10.1**. Si las Static rutas están requeridas en este escenario depende de las capacidades y de las configuraciones de FW

A y de FW B. La comunicación del control del VCS al VCS Expressway ocurre vía la dirección IP 64.100.0.10 del VCS Expressway; y el tráfico de retorno del VCS Expressway al control del VCS pudo tener que pasar vía el default gateway.

El 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 el FW B permite esto), puesto que la comunicación de Administración de Cisco TMS no es afectada por las configuraciones de modo NAT estáticas en el VCS Expressway.

3-Port FW DMZ con la sola interfaz LAN de Expressway del VCS

Aquí está un ejemplo de este escenario:



En este despliegue, un 3-port FW se utiliza para crear:

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

Un NAT uno por estático se ha configurado en el FW A, que realiza el NAT del IP Address público 64.100.0.10 a la dirección IP LAN1 del VCS Expressway. El modo NAT estática se ha habilitado para la interfaz LAN1 en el VCS Expressway, con una dirección IP NAT estática de 64.100.0.10.

El VCS Expressway se debe configurar con un default gateway de 10.0.10.1. Puesto que este gateway se debe utilizar para todo el tráfico que salga del VCS Expressway, no se requiere ningunas Static rutas en este tipo de despliegue.

La zona del cliente del traversal en el control del VCS se debe configurar con una dirección de peer que haga juego el direccionamiento NAT estática del VCS Expressway (64.100.0.10 en este ejemplo) por las mismas razones que ésos descritos en el escenario previó.

> **Note**: Esto significa que el FW A debe permitir el tráfico del control del VCS con un IP Address de destino de 64.100.0.10. Esto también se conoce como reflexión NAT, y debe ser observado que esto no es soportada por todos los tipos de FW.

El VCS Expressway se puede agregar a Cisco TMS con la dirección IP de 10.0.10.2 (o con la dirección IP 64.100.0.10, si el FW A permite esto), puesto que la comunicación de Administración

de Cisco TMS no es afectada por las configuraciones de modo NAT estáticas en el VCS Expressway.

Configurar

Esta sección describe cómo configurar la reflexión NAT en el ASA para las dos diversas situaciones de implementación del C y E del VCS.

Subred única DMZ con la sola interfaz LAN de Expressway del VCS

Para el primer escenario, usted debe aplicar esta configuración de la reflexión NAT en FW A para permitir la comunicación del control del VCS (10.0.30.2) que se destina al IP Address externo (64.100.0.10) del VCS Expressway:

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

Si usted supone que sigue habiendo la dirección IP 10.0.30.2 del control del VCS cuando se mueve desde el interior a la interfaz exterior de FW B cuando busca el VCS Expressway con el IP Address de destino 64.100.0.10, después la configuración de la reflexión NAT que usted debe implementar en FW B se muestra en estos ejemplos.

Exmpla para las Versiones de ASA 8.3 y posterior:

```
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 las Versiones de ASA 8.2 y anterior:

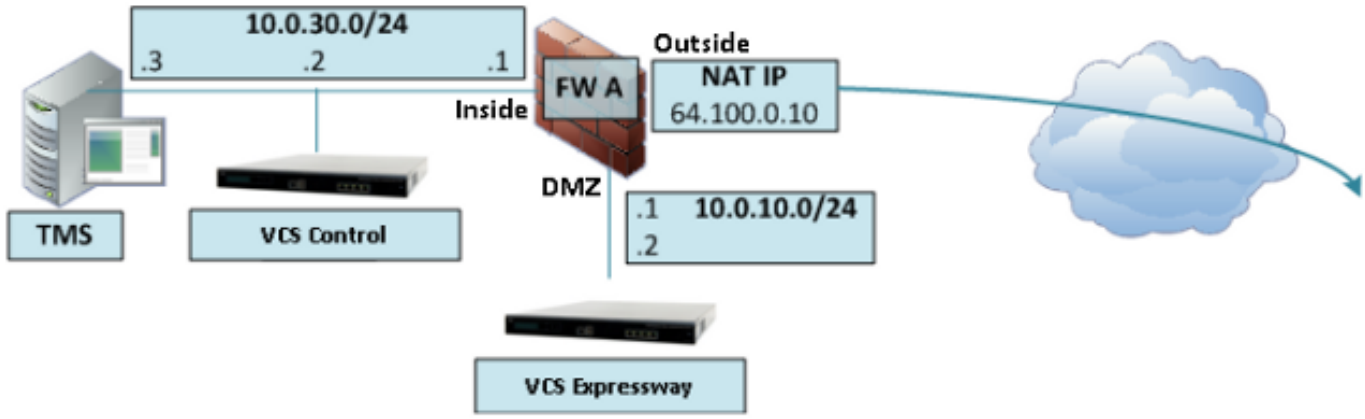
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE

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
```

Note: El objetivo principal de esta configuración de la reflexión NAT es permitir que el control del VCS pueda alcanzar la autopista del VCS, pero usar al IP Address público de la autopista del VCS en vez de su IP Address privado. Si la dirección IP de origen del control del VCS se cambia durante esta traducción de NAT con dos veces una configuración del NAT en vez de la configuración del NAT sugerida apenas mostrada, dando por resultado el VCS Expressway ver el tráfico de su propio IP Address público, después de los servicios telefónicos para los dispositivos MRA no subirá. Esto no es un despliegue soportado según la sección 3 en la sección de las recomendaciones abajo.

3-Port FW DMZ con la sola interfaz LAN de Expressway del VCS

Para el segundo escenario, usted debe aplicar esta configuración de la reflexión NAT en FW A para permitir la reflexión NAT del tráfico entrante del control 10.0.30.2 del VCS que se destina al IP Address externo (64.100.0.10) del VCS Expressway:



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

Si usted supone que sigue habiendo la dirección IP 10.0.30.2 del control del VCS cuando se mueve desde el interior a la interfaz DMZ de FW A cuando busca el VCS Expressway con el IP Address de destino 64.100.0.10, después la configuración de la reflexión NAT que usted debe implementar en FW A se muestra en estos ejemplos.

Ejemplo para las Versiones de ASA 8.3 y posterior:

```
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 las Versiones de ASA 8.2 y anterior:

```
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
```

Note: El objetivo principal de esta configuración de la reflexión NAT es permitir que el control del VCS pueda alcanzar la autopista del VCS, pero con el IP Address público de la autopista del VCS en vez de su IP Address privado. Si la dirección IP de origen del control del VCS se cambia durante esta traducción de NAT con dos veces una configuración del NAT en vez de la configuración del NAT sugerida apenas mostrada, dando por resultado el VCS Expressway ver el tráfico de su propio IP Address público, después de los servicios telefónicos para los dispositivos MRA no subirá. Esto no es un despliegue soportado según la sección 3 en la sección de las recomendaciones abajo.

Verificación

Esta sección proporciona las salidas del trazalíneas del paquete que usted puede ver en el ASA para confirmar los trabajos de la configuración de la reflexión NAT según las necesidades en ambas situaciones de implementación del C y E del VCS.

Subred única DMZ con la sola interfaz LAN de Expressway del VCS

Aquí está el trazalíneas del paquete FW B hecho salir para las Versiones de ASA 8.3 y posterior:

```
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
```

Aquí está el trazalíneas del paquete FW B hecho salir para las Versiones de ASA 8.2 y anterior:

```
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-Port FW DMZ con la sola interfaz LAN de Expressway del VCS

Aquí está el trazalíneas del paquete FW A hecho salir para las Versiones de ASA 8.3 y posterior:

```
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
```

Aquí está el trazalíneas del paquete FW A hecho salir para las Versiones de ASA 8.2 y anterior:

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
```

Troubleshooting

Usted puede configurar a las capturas de paquetes en las interfaces ASA para confirmar la traducción de NAT cuando los paquetes ingresan y salen de las interfaces FW que están implicadas.

Captura de paquetes solicitada el "3-Port FW DMZ con escenario de la sola del VCS interfaz LAN de Expressway el"

```
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 solicitada “subred única DMZ con el escenario de la sola del VCS interfaz LAN de 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
```

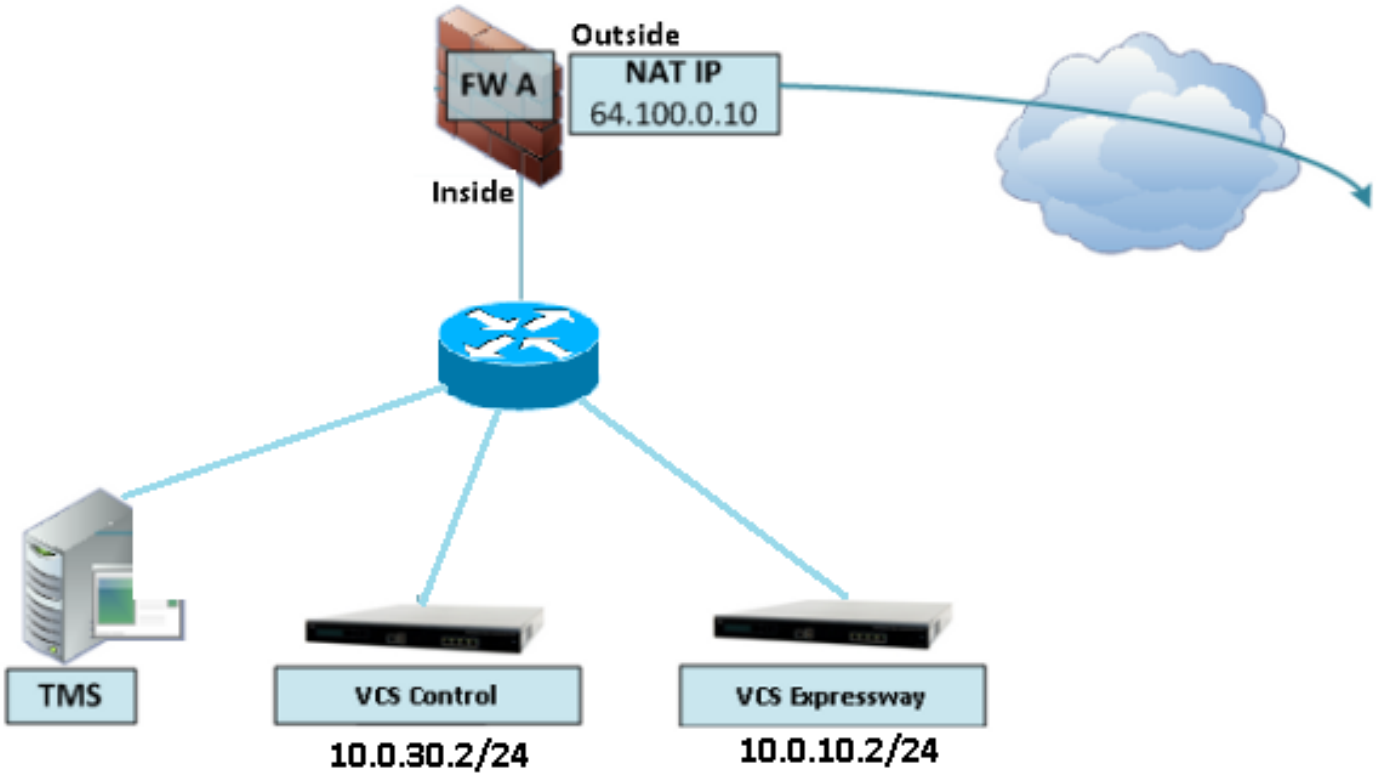
```
   4: 22:30:06.900710 64.100.0.10 > 10.0.30.2: icmp: echo reply
   5: 22:30:06.971598 10.0.30.2 > 64.100.0.10: icmp: echo request
   6: 22:30:06.999551 64.100.0.10 > 10.0.30.2: icmp: echo reply
   7: 22:30:07.075649 10.0.30.2 > 64.100.0.10: icmp: echo request
   8: 22:30:07.134499 64.100.0.10 > 10.0.30.2: 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

Evite la implementación de cualquier topología sin apoyo

Por ejemplo, teniendo el control y VCS Expressway del VCS detrás de la interfaz interior ASA, apenas tal y como se muestra en de este escenario:



Esta clase de implementación requiere la dirección IP del control del VCS ser traducida a la dirección IP interior del ASA para forzar el tráfico de retorno para volver al ASA para evitar los problemas del Asymmetric Routing durante la reflexión NAT.

> Nota importante: Si la dirección IP de origen del control del VCS se cambia durante esta traducción de NAT con dos veces una configuración del NAT en vez de la configuración del NAT sugerida apenas mostrada, dando por resultado el VCS Expressway ver el tráfico de su propio IP Address público, después de los servicios telefónicos para los dispositivos MRA no subirá. Esto no es un despliegue soportado según la sección 3 en la sección de las recomendaciones abajo.

Que dicho, está recomendado altamente para implementar el VCS Expresswy/el borde de Expressway usando dos interfaces - que estén en los DMZ separados.

Esté seguro que el examen SIP/H323 está inhabilitado totalmente en el Firewall

Se requiere inhabilitar el SORBO y H.323 ALGs en el Routers/los Firewall que llevan el tráfico de la red a o desde un VCS Expressway, as, cuando está habilitado esto se encuentra con frecuencia para afectar negativamente a las funciones del VCS Expressway sí mismo del traversal del accesorio firewall/NAT.

Para inhabilitar el examen del valor por defecto SIP/H323 en Cisco los ASA satisfacen aplican la configuración siguiente:

```
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
```

Asegúrese que su implementación real de Expressway cumpla con los requisitos siguientes, confirmados por los desarrolladores del TelePresence

- Soportamos el NAT entre Expressway-C y Expressway-e
- Pero no soportamos la situación específica de donde Expressway-C consigue NATted a la dirección IP que se configura como NAT estático en Expressway-e, ejemplo:
  Expressway-C se configura con el IP1
  Expressway-e tiene solo NIC con IP2 configurado y el NAT estático IP3
  Entonces Expressway-C no puede ser NATted a IP3

Solución recomendada

La solución recomendada en vez de implementar el VCS Expressway usando la configuración de la reflexión NAT es implementarlo usando las interfaces de la red/la implementación duales de Expressway del VCS del NIC dual, para más información satisface marca el link siguiente:

Información Relacionada

Guía de despliegue de la configuración básica del servidor del comunicación mediante video del Cisco TelePresence (control con Expressway)

Uso del puerto IP de Cisco Expressway para el Traversal del Firewall

Colocando un VCS Expressway de Cisco en un DMZ bastante que en Internet público