La configuración del NAT y las recomendaciones ASA para Expressway-e se doblan implementación de las interfaces de la red.

Contenido

Introducción

Este documento describe cómo implementar la configuración del Network Address Translation (NAT) requerida en el dispositivo de seguridad adaptante de Cisco (ASA) para Expressway-e y las interfaces de la red duales de Expressway-C/la implementación dual de Network Interface Controller (NIC).

Este despliegue es la opción recomendada para las implementaciones de los dispositivos de Expressway-e y de Expressway-C (bastante que el Solo-NIC con la reflexión NAT).

Contribuido por el cristiano G. Hernández R. y Cesar López Zamarripa, ingenieros de Cisco TAC.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración básica y configuración del NAT de Cisco ASA
- Configuración básica de Cisco Expressway-e y de Expressway-C

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 8.0 y posterior.
- Versión X8.0 de Cisco Expressway 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 su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

> **Note**: A través del documento entero, los dispositivos de Expressway se refieren como Expressway-e y Expressway-C. Sin embargo, la misma configuración se aplica al servidor del comunicación mediante video (VCS) Expressway y los dispositivos de control del VCS.

Antecedentes

Por el diseño, Cisco Expressway-e se puede colocar en una zona desmilitarizada (DMZ) o con una interfaz de los Revestimientos del Internet, mientras que puede comunicar con Cisco Expressway-C en una red privada. Cuando Cisco Expressway-e se coloca en un DMZ, éstos son los beneficios adicionales:

- En la mayoría del escenario frecuente, Cisco Expressway-e se maneja de la red privada. Cuando Cisco Expressway-e está en un DMZ, un Firewall del perímetro (externo) se puede utilizar para bloquear el acceso indeseado a Expressway de las redes externas vía el Protocolo de transporte de hipertexto las peticiones seguras (HTTPS) o del Secure Shell (SSH).

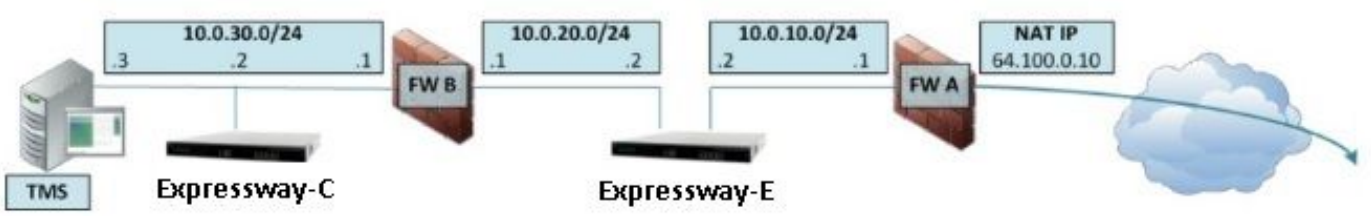
- Si el DMZ no permite las conexiones directas entre interno y las redes externas, requieren a los servidores dedicados manejar el tráfico que atraviesa el DMZ. Cisco Expressway puede actuar como servidor proxy para el Session Initiation Protocol (SIP) y/o Voz y tráfico de video de H.323. En este caso, usted puede utilizar la opción de interfaces de la red dual que permite que Cisco Expressway tenga dos diversos IP Addresses, uno para el tráfico a/desde el firewall externo, y una para el tráfico a/desde el Firewall interno.

- Esta configuración previene las conexiones directas de la red externa a la red interna. Esto mejora el guardapolvo de la Seguridad de la red interna.

  Tip: Para obtener más detalles sobre la implementación del TelePresence, refiera a Cisco Expressway-e y a Expressway-C - Guía de despliegue de la configuración básica y colocación de un VCS Expressway de Cisco en un DMZ bastante que en Internet público.

C de Expressway y E - Implementación dual de las interfaces de la red/del NIC dual

Esta imagen muestra un despliegue de ejemplo para Expressway-e con las interfaces de la red y el NAT estático duales. Expressway-C actúa como el cliente del traversal. Hay dos Firewall (FW A y FWB). Típicamente, en esta configuración de DMZ, el FW A no puede rutear el tráfico a FW B, y los dispositivos tales como Expressway-e se requieren para validar y para remitir el tráfico de la subred FW a la subred FW B (y vice versa).



Este despliegue consiste en estos componentes.

Subred DMZ 1 – 10.0.10.0/24

- Interfaz interna FW A – 10.0.10.1
- Interfaz de Expressway-e LAN2 – 10.0.10.2

Subred DMZ 2 – 10.0.20.0/24

- Interfaz externa FW B – 10.0.20.1
- Interfaz de Expressway-e LAN1 – 10.0.20.2

Subred LAN – 10.0.30.0/24

- Interfaz interna FW B – 10.0.30.1
- Interfaz de Expressway-C LAN1 – 10.0.30.2
- Interfaz de red de servidores del conjunto de administración del Cisco TelePresence (TMS) – 10.0.30.3

Específicos de esta implementación:

- El FW A es el Firewall del externo o del perímetro; se configura con el IP NAT (IP del público) de 64.100.0.10 que se traduce estáticamente a 10.0.10.2 (la interfaz de Expressway-e LAN2)
- El FW B es el Firewall interno
- Expressway-e LAN1 tiene modo NAT estática inhabilitado
- Expressway-e LAN2 tiene modo NAT estática habilitado con el direccionamiento NAT estática 64.100.0.10
- Expressway-C tiene una zona del cliente del traversal que señale a 10.0.20.2 (la interfaz de

Expressway-e LAN1)
- No hay encaminamiento entre 10.0.20.0/24 y 10.0.10.0/24 subredes. Expressway-e interliga estas subredes y actúa como proxy para la señalización SIP/H.323 y los media del Real-Time Transport Protocol (RTP)/RTP Control Protocol (RTCP).
- Cisco TMS tiene Expressway-e configurado con la dirección IP 10.0.20.2

Requisitos/limitaciones

Subredes sin traslapo

Si Expressway-e se configura para utilizar ambas interfaces LAN, las interfaces LAN1 y LAN2 se deben situar en las subredes sin traslapo para asegurarse de que el tráfico está enviado a la interfaz correcta.

El agrupar

Al agrupar los dispositivos de Expressway con la **opción de interconexión de redes avanzada** configurada, cada par del cluster necesita ser configurado con su propio direccionamiento de la interfaz LAN1. Además, el agrupar se debe configurar en una interfaz que no tenga modo NAT estática habilitado. Por lo tanto, se recomienda que usted utiliza el LAN2 como la interfaz externa, en la cual usted puede aplicar y configurar el NAT estático en caso pertinente.

Configuraciones externas de la interfaz LAN

Los ajustes de la configuración externos de la interfaz LAN en la configuración IP paginan el control que la interfaz de la red utiliza transversal usando las retransmisiones alrededor de NAT (VUELTA). En una configuración dual de Expressway-e de la interfaz de la red, esto se fija normalmente a la interfaz LAN del externo de Expressway-e.

Rutas estáticas

Expressway-e se debe configurar con una dirección de gateway predeterminado de 10.0.10.1 para este escenario. Esto significa que todo el tráfico enviado vía el LAN2, por abandono, está enviado a la dirección IP 10.0.10.1.

Si el FW B está traduciendo el tráfico enviado a partir de la subred el 10.0.30.0/24 a la interfaz de Expressway-e LAN1 (por ejemplo, tráfico del cliente del traversal de Expressway-C o tráfico de administración del servidor TMS), este tráfico aparece mientras que viene de la interfaz externa FWB (10.0.20.1) como alcanza Expressway-e LAN1. Expressway-e puede entonces contestar a este tráfico vía su interfaz LAN1 puesto que la fuente evidente de ese tráfico está situada en la misma subred.

Si el NAT se habilita en FW B, el tráfico enviado de Expressway-C a Expressway-e LAN1 muestra mientras que viene de 10.0.30.2. Si Expressway no tiene una Static ruta agregada para la subred 10.0.30.0/24, envía las contestaciones para este tráfico a su default gateway (10.0.10.1) hacia fuera del LAN2, pues no es consciente que la subred 10.0.30.0/24 está situada detrás del Firewall interno (FW B). Por lo tanto, una Static ruta necesita ser agregada, funciona con el comando CLI de **RouteAdd del xCommand** a través de una sesión SSH a Expressway.

En este ejemplo en particular, Expressway-e debe saber que puede alcanzar la subred

10.0.30.0/24 detrás del FW B, que es accesible vía la interfaz LAN1. Para lograr esto, funcione con el comando:

```
xCommand RouteAdd Address: 10.0.30.0 PrefixLength: 24 Gateway: 10.0.20.1 Interface: LAN1
```

> **Note**: La configuración de la Static ruta puede ser aplicada a través del Interfaz gráfica del usuario (GUI) de Expressway-e así como del **/Network del sistema de la** sección **> de las interfaces/de las Static rutas**. ########

En este ejemplo, el parámetro de la interfaz se puede también fijar al **auto** pues la dirección del gateway (10.0.20.1) es solamente accesible vía el LAN1.

Si el NAT no se habilita en FW B y las necesidades de Expressway-e de comunicar con los dispositivos en las subredes (con excepción de 10.0.30.0/24) que también están situadas detrás de FW B, las Static rutas se deben agregar para estos dispositivos/subredes.

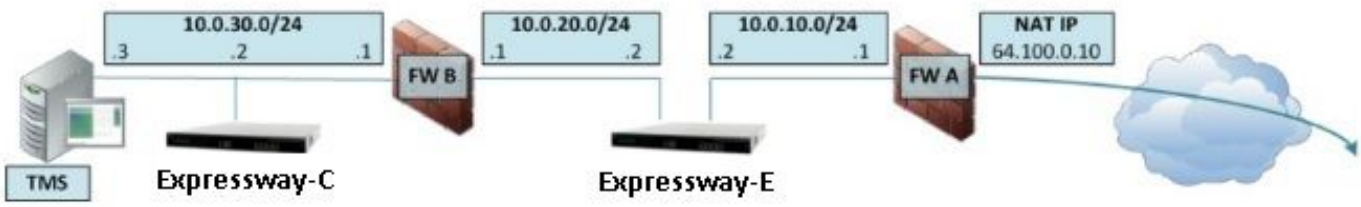
> **Note**: Esto incluye SSH y las conexiones HTTPS de las estaciones de trabajo para administración de red o para los servicios de red como el NTP, el DNS, LDAP/AD, o el Syslog.

El comando y el sintaxis de **RouteAdd del xCommand** se describen en la profundidad total en el *guía del administrador del VCS.*

Configuración

Esta sección describe cómo configurar el NAT estático requerido para las interfaces de la red duales de Expressway-C y de Expressway-e/la implementación del NIC dual en el ASA. Algunas recomendaciones para la configuración modulares adicionales del Marco de políticas ASA (MPF) son incluidas para manejar el tráfico SIP/H323.

C de Expressway y E - Implementación dual de las interfaces de la red/del NIC dual



En este ejemplo, la asignación de la dirección IP es las siguientes.

IP address:10.0.30.2/24 de Expressway-C

Gateway predeterminado de Expressway-C: 10.0.30.1 (FW-B)

IP Addresses de Expressway-e

En el LAN2: 10.0.10.2/24

En el LAN1: 10.0.20.2/24

Gateway predeterminado de Expressway-e: 10.0.10.1 (FW-A)

Dirección IP TMS: 10.0.30.3/24

Configuración FW-A:

Paso 1. Configuración NAT estática para Expressway-e

Como se explica en la sección de **información previa de** este documento, el FW-A tiene una traducción NAT estática para permitir que Expressway-e sea accesible de Internet usando el IP Address público 64.100.0.10. Este último es NATed a la dirección IP 10.0.10.2/24 de Expressway-e LAN2. Que siendo dicho, ésta es la configuración requerida del NAT estático FW-A.

Para las Versiones de ASA 8.3 y posterior:

```
! To use PAT with specific ports range:

object network obj-10.0.10.2
host 10.0.10.2

object service obj-udp_3478-3483 service udp source range 3478 3483 object service obj-
udp_24000-29999 service udp source range 24000 29999 object service obj-udp_36002-59999 service
udp source range 36002 59999 object service obj-tcp_5222 service tcp source eq 5222 object
service obj-tcp_8443 service tcp source eq 8443 object service obj-tcp_5061 service tcp source
eq 5061 object service obj-udp_5061 service udp source eq 5061 nat (inside,outside) source
static obj-10.0.10.2 interface service obj-udp_3478-3483 obj-udp_3478-3483 nat (inside,outside)
source static obj-10.0.10.2 interface service obj-udp_24000-29999 obj-udp_24000-29999 nat
(inside,outside) source static obj-10.0.10.2 interface service obj-udp_36002-59999 obj-
udp_36002-59999 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5222
obj-tcp_5222 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_8443
obj-tcp_8443 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5061
obj-tcp_5061 nat (inside,outside) source static obj-10.0.10.2 interface service obj-udp_5061
obj-udp_5061 OR

! To use with static one-to-one NAT:

object network obj-10.0.10.2
nat (inside,outside) static interface
```

> **Note: Al intentar aplicar el PAT estático le ordena reciben este mensaje de error en la interfaz de la línea de comandos ASA, "ERROR: NAT incapaz de reservar los puertos". Entonces claro las entradas del xlate con el comando clear xlate x.x.x.x local donde x.x.x.x corresponde al IP Address externo ASA. Este comando borra todas las traducciones asociadas a este IP, así que en los entornos de producción, lo ejecuta con cautela.**
> El ### necesita la clarificación

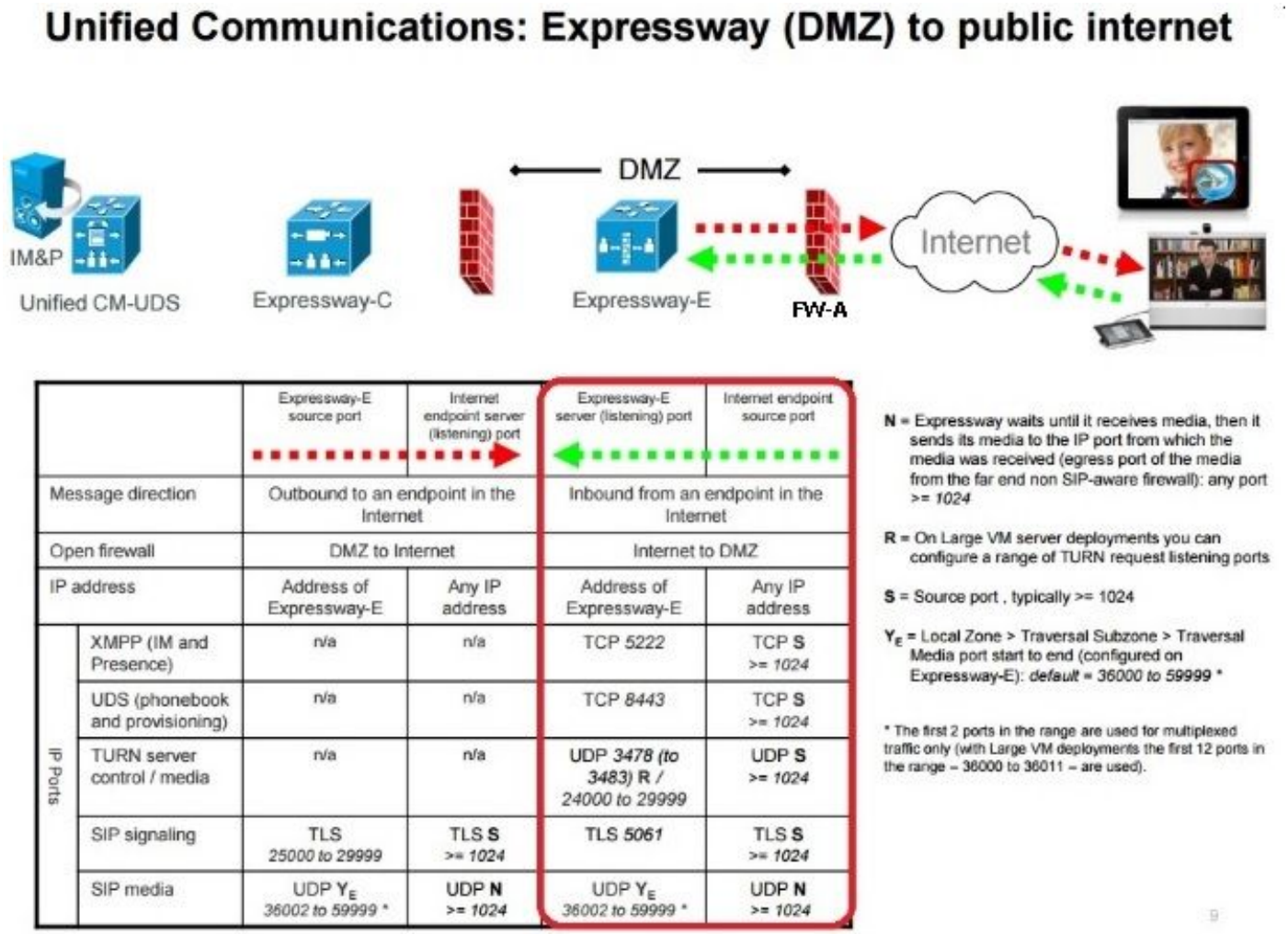
Para las Versiones de ASA 8.2 y anterior:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Paso 2. Configuración de la lista de control de acceso (ACL) para permitir los puertos requeridos de Internet a Expressway-e

Según la comunicación unificada: Expressway (DMZ) a la documentación de Internet público, esto es la lista de puertos TCP y UDP que Expressway-e requiera para ser permitido en FW-A:



		Expressway-E source port	Internet endpoint server (listening) port	Expressway-E server (listening) port	Internet endpoint source port
Message direction		Outbound to an endpoint in the Internet		Inbound from an endpoint in the Internet	
Open firewall		DMZ to Internet		Internet to DMZ	
IP address		Address of Expressway-E	Any IP address	Address of Expressway-E	Any IP address
IP Ports	XMPP (IM and Presence)	n/a	n/a	TCP *5222*	TCP **S** *>= 1024*
	UDS (phonebook and provisioning)	n/a	n/a	TCP *8443*	TCP **S** *>= 1024*
	TURN server control / media	n/a	n/a	UDP *3478 (to 3483)* **R** / *24000 to 29999*	UDP **S** *>= 1024*
	SIP signaling	TLS *25000 to 29999*	TLS **S** *>= 1024*	TLS *5061*	TLS **S** *>= 1024*
	SIP media	UDP Y_E *36002 to 59999* *	UDP **N** *>= 1024*	UDP Y_E *36002 to 59999* *	UDP **N** *>= 1024*

N = Expressway waits until it receives media, then it sends its media to the IP port from which the media was received (egress port of the media from the far end non SIP-aware firewall): any port *>= 1024*

R = On Large VM server deployments you can configure a range of TURN request listening ports

S = Source port , typically >= 1024

Y_E = Local Zone > Traversal Subzone > Traversal Media port start to end (configured on Expressway-E): *default = 36000 to 59999* *

* The first 2 ports in the range are used for multiplexed traffic only (with Large VM deployments the first 12 ports in the range – 36000 to 36011 – are used).

Ésta es la configuración ACL requerida como entrante en la interfaz exterior FW A.

Para las Versiones de ASA 8.3 y posterior.

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Para las Versiones de ASA 8.2 y anterior.

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Note: Se recomienda altamente para inhabilitar el SORBO y los exámenes de H.323 en el tráfico de la red que lleva del Firewall a o desde Expressway-e, como cuando están habilitados, esto se encuentran con frecuencia para afectar negativamente a las funciones incorporadas del traversal de Expressway-e firewall/NAT.

Configuración FW-B

Como se explica en la sección de **información previa de** este documento, el FW B puede requerir una configuración dinámica NAT o de la PALMADITA permitir que la subred interna 10.0.30.0/24 sea traducida a la dirección IP 10.0.20.1 al salir a la interfaz exterior del FW B.

Para las Versiones de ASA 8.3 y posterior:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Para las Versiones de ASA 8.2 y anterior:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

> **Note**: Se recomienda altamente para inhabilitar el SORBO y los exámenes de H.323 en el tráfico de la red que lleva del Firewall a o desde Expressway-e, como cuando está habilitado esto se encuentra con frecuencia para afectar negativamente a las funciones incorporadas del traversal de Expressway-e firewall/NAT.

> **Tip**: Esté seguro que todos los puertos requeridos TCP y UDP para permitir que Expressway-C trabaje correctamente están abiertos en el FW B, apenas como se especifica en este documento de Cisco: Uso del puerto IP de Cisco Expressway para el Traversal del Firewall

Verificación

El trazalíneas del paquete se puede utilizar en el ASA para confirmar que los trabajos de traducción NAT estática de Expressway-e como sea necesario.

Trazalíneas del paquete para probar 64.100.0.10 en TCP/5222:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Trazalíneas del paquete para probar 64.100.0.10 en TCP/8443:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Trazalíneas del paquete para probar 64.100.0.10 en TCP/5061.

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Trazalíneas del paquete para probar 64.100.0.10 en UDP/24000:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Trazalíneas del paquete para probar 64.100.0.10 en UDP/36002:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Troubleshooting

Paso 1. Compare a las capturas de paquetes.

Las capturas de paquetes pueden ser tomadas en el ingreso y las interfaces de egreso ASA

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Capturas de paquetes para 64.100.0.10 en TCP/5222:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Capturas de paquetes para 64.100.0.10 en TCP/5061:

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Paso 2. Examine a las capturas de paquetes aceleradas del descenso de la trayectoria de la Seguridad (ASP).

Las capturas del descenso ASA ASP toman los paquetes que el ASA decidía a caer. La opción **toda** captura todas las razones posibles por las que el ASA cayó un paquete. Esto puede ser estrechada abajo si hay alguna razón sospechosa. Para una lista de razones que un ASA utiliza para clasificar estos descensos, ejecute el **descenso del** comando show **ASP**

El buffer predeterminado para cada captura ASA es 512 KB. Si hay muchos paquetes que son

caídos por este ASA, este buffer será llenado muy rápidamente. Este buffer se puede incrementar usando el **buffer de la** opción.

```
capture asp type asp-drop all

show cap asp

OR

show cap asp | i 64.100.0.10
show cap asp | i 10.0.10.2
```

> **Tip**: Esta captura ASA ASP es muy útil en este escenario para confirmar si el ASA cae los paquetes debido a un ACL o a un NAT que falta (que sea necesario abrir un puerto específico TCP o UDP para Expressway-e).

Recomendaciones

Asegúrese de que el examen SIP/H.323 esté inhabilitado totalmente en los Firewall implicados

Se recomienda altamente para inhabilitar el SORBO y el examen de H.323 en los Firewall que manejan el tráfico de la red a o desde Expressway-e. Cuando está habilitado, el examen SIP/H.323 se encuentra con frecuencia para afectar negativamente a las funciones incorporadas del traversal de Expressway firewall/NAT.

Éste es un ejemplo de cómo inhabilitar el SORBO y los exámenes de H.323 en el ASA:

```
capture asp type asp-drop all

show cap asp

OR

show cap asp | i 64.100.0.10
show cap asp | i 10.0.10.2
```

Solución alternativa

Una solución alternativa a implementar Expressway-e usando las interfaces de la red duales/NIC dual es implementar Expressway-e con un solos NIC y NAT estático usando la configuración de la reflexión NAT en los Firewall. Este link muestra otros detalles sobre este escenario:

> **Note**: Mientras que fue mencionado al principio de este documento, la implementación del NIC dual se recomienda sobre la reflexión NAT.

Documentación relacionada

Cisco Expressway-e y Expressway-C - Guía de despliegue de la configuración básica

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

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