Configuración de ASA NAT Y Recomendaciones Para La Implementación De Interfaces De Red Dual De Expressway-E

Contenido

Introducción

Este documento describe cómo implementar la configuración de traducción de direcciones de red (NAT) requerida en el Cisco Adaptive Security Appliance (ASA) para la implementación de interfaces de red duales de Expressway-E.

Sugerencia: Esta implementación es la opción recomendada para la implementación de Expressway-E, en lugar de la implementación de NIC única con reflexión de NAT.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración básica de Cisco ASA y NAT
- Configuración básica de Cisco Expressway-E y Expressway-C

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 8.0 y posteriores.
- Cisco Expressway versión X8.0 y posterior.

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

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

Antecedentes

Por diseño, Cisco Expressway-E se puede colocar en una zona desmilitarizada (DMZ) o con una interfaz orientada a Internet, mientras se puede comunicar con Cisco Expressway-C en una red privada. Cuando Cisco Expressway-E se coloca en una DMZ, estas son las ventajas adicionales:

- En la situación más común, Cisco Expressway-E se gestiona mediante la red privada. Cuando Cisco Expressway-E se encuentra en una DMZ, se puede utilizar un firewall perimetral (externo) para bloquear el acceso no deseado a Expressway desde redes externas mediante solicitudes de protocolo de transferencia de hipertexto Secure (HTTPS) o Secure Shell (SSH).

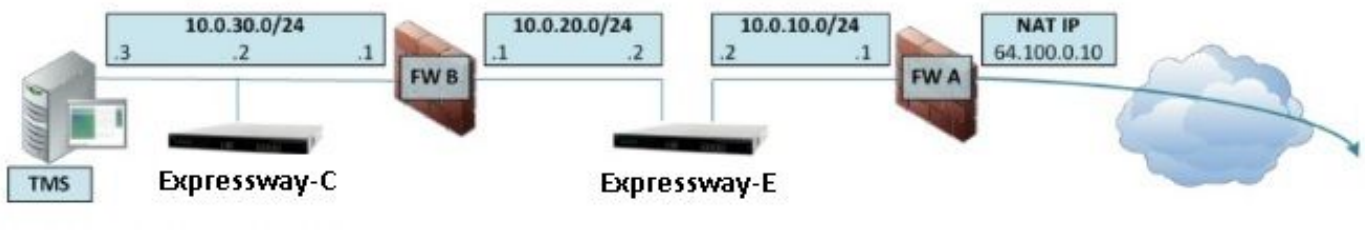
- Si la DMZ no permite conexiones directas entre redes internas y externas, se necesitan servidores dedicados para gestionar el tráfico que atraviesa la DMZ. Cisco Expressway puede actuar como servidor proxy para el tráfico de voz y vídeo de protocolo de inicio de sesión (SIP) o H.323. En este caso, puede utilizar la opción Interfaces de red duales que permite a Cisco Expressway tener dos direcciones IP diferentes, una para el tráfico hacia/desde el firewall externo y otra para el tráfico hacia/desde el firewall interno.

- Esta configuración evita las conexiones directas de la red externa a la red interna. Esto mejora la seguridad de la red interna en general.

Consejo: Para obtener más detalles sobre la implementación de TelePresence, refiérase a Cisco Expressway-E y Expressway-C - Guía de implementación de configuración básica y Colocación de Cisco VCS Expressway en una DMZ en lugar de en Internet pública.

Expressway C y E: interfaces de red duales/implementación de NIC dual

Esta imagen muestra un ejemplo de implementación para Expressway-E con interfaces de red duales y NAT estática. Expressway-C actúa como el cliente transversal. Hay dos firewalls (FW A y FWB). Normalmente, en esta configuración de DMZ, FW A no puede enrutar el tráfico a FW B, y los dispositivos como Expressway-E son necesarios para validar y reenviar el tráfico de la subred de FW A a la subred de FW B (y viceversa).



Esta implementación consta de estos componentes.

Subred DMZ 1 - 10.0.10.0/24

- FW Una interfaz interna - 10.0.10.1
- Interfaz LAN2 de Expressway-E: 10.0.10.2

Subred DMZ 2 - 10.0.20.0/24

- Interfaz externa FW B - 10.0.20.1
- Interfaz LAN1 de Expressway-E: 10.0.20.2

Subred LAN - 10.0.30.0/24

- Interfaz interna FW B - 10.0.30.1
- Interfaz LAN1 de Expressway-C - 10.0.30.2
- Interfaz de red del servidor Cisco TelePresence Management Suite (TMS) - 10.0.30.3

Especificaciones de esta implementación:

- FW A es el firewall externo o perimetral; se configura con IP de NAT (IP pública) de 64.100.0.10 que se traduce estáticamente a 10.0.10.2 (interfaz LAN2 de Expressway-E)
- FW B es el firewall interno
- La LAN1 de Expressway-E tiene el modo NAT estático desactivado
- La LAN2 de Expressway-E tiene el modo NAT estático habilitado con la dirección NAT estática 64.100.0.10
- Expressway-C tiene una zona cliente transversal que apunta a 10.0.20.2 (interfaz LAN1 de Expressway-E)
- No hay ruteo entre las subredes 10.0.20.0/24 y 10.0.10.0/24. Expressway-E une estas

subredes y actúa como proxy para los medios de señalización SIP/H.323 y protocolo de transporte en tiempo real (RTP) / protocolo de control RTP (RTCP).
- Cisco TMS tiene Expressway-E configurado con la dirección IP 10.0.20.2

Requisitos/limitaciones

Subredes no superpuestas

Si Expressway-E está configurado para utilizar ambas interfaces LAN, las interfaces LAN1 y LAN2 deben estar ubicadas en subredes no superpuestas para asegurarse de que el tráfico se envíe a la interfaz correcta.

Agrupación en clústeres

Cuando se agrupan los dispositivos de Expressway con la opción Advanced Networking configurada, cada par de clúster debe configurarse con su propia dirección de interfaz LAN1. Además, la agrupación en clúster se debe configurar en una interfaz que no tenga habilitado el modo NAT estático. Por lo tanto, se recomienda que utilice LAN2 como la interfaz externa, en la cual puede aplicar y configurar NAT estática cuando sea aplicable.

Configuración de la interfaz LAN externa

Los parámetros de configuración de la interfaz LAN externa en la página de configuración IP controlan qué interfaz de red utiliza Transversal Usando relés alrededor de NAT (TURN). En una configuración de interfaz de red dual Expressway-E, esto se configura normalmente en la interfaz LAN externa de Expressway-E.

rutas estáticas

Expressway-E debe configurarse con una dirección de gateway predeterminada de 10.0.10.1 para este escenario. Esto significa que todo el tráfico enviado a través de LAN2 se envía, de forma predeterminada, a la dirección IP 10.0.10.1.

Si FW B traduce el tráfico enviado desde la subred 10.0.30.0/24 a la interfaz LAN1 de Expressway-E (por ejemplo, tráfico de cliente transversal de Expressway-C o tráfico de administración del servidor TMS), este tráfico aparece cuando proviene de la interfaz externa FWB (10.0.20.1) cuando llega a la LAN1 de Expressway-E. Expressway-E puede responder a este tráfico a través de su interfaz LAN1, ya que el origen aparente de ese tráfico se encuentra en la misma subred.

Si NAT está habilitado en FW B, el tráfico enviado desde Expressway-C a Expressway-E LAN1 se muestra a medida que proviene de 10.0.30.2. Si Expressway no tiene una ruta estática agregada para la subred 10.0.30.0/24, envía las respuestas para este tráfico a su gateway predeterminada (10.0.10.1) desde LAN2, ya que no sabe que la subred 10.0.30.0/24 se encuentra detrás del firewall interno (FW B). Por lo tanto, es necesario agregar una ruta estática, ejecute el comando CLI **xCommand RouteAdd** 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 de FW B, a la que se puede acceder a través de la interfaz LAN1. Para lograrlo, ejecute el comando:

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

> **Nota**: SLa configuración de ruta estática se puede aplicar a través de la GUI de Expressway-E, así como en la sección **Sistema/Red > Interfaces/Rutas Estáticas**.

En este ejemplo, el parámetro Interface también se puede establecer en **Auto** ya que la dirección de gateway (10.0.20.1) sólo se puede alcanzar a través de LAN1.

Si la NAT no está habilitada en FW B y Expressway-E necesita comunicarse con dispositivos en subredes (distintas de 10.0.30.0/24) que también se encuentran detrás del FW B, se deben agregar rutas estáticas para estos dispositivos/subredes.

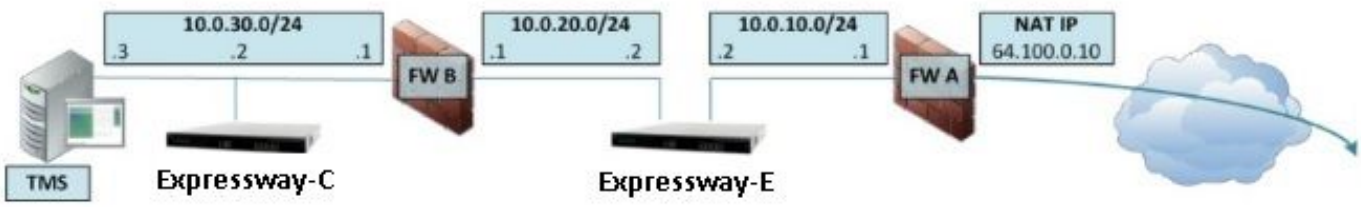
> **Nota:** Esto incluye Conexiones SSH y HTTPS desde estaciones de trabajo de administración de red o para servicios de red como NTP, DNS, LDAP/AD o Syslog.

El comando y la sintaxis **xCommand RouteAdd** se describen con todo detalle en la Guía del administrador de VCS.

Configuración

Esta sección describe cómo configurar la NAT estática necesaria para la implementación de la interfaz de red dual de Expressway-E en el ASA. Se incluyen algunas recomendaciones de configuración adicionales de ASA Modular Policy Framework (MPF) para gestionar el tráfico SIP/H323.

Expressway C y E: interfaces de red duales/implementación NIC dual



En este ejemplo, la asignación de dirección IP es la siguiente.

Dirección IP de Expressway-C: 10.0.30.2/24

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

Direcciones IP de Expressway-E:

- En LAN2: 10.0.10.2/24
- En LAN1: 10.0.20.2/24

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

Dirección IP de TMS: 10.0.30.3/24

Configuración de FW-A

Paso 1. Configuración de NAT estática para Expressway-E.

Como se explica en la sección Información de fondo de este documento, el FW-A tiene una traducción NAT estática para permitir que Expressway-E sea accesible desde Internet con la dirección IP pública 64.100.0.10. Esta última es NATed a la dirección IP LAN2 de Expressway-E 10.0.10.2/24. Dicho esto, esta es la configuración NAT estática FW-A necesaria.

Para las versiones 8.3 y posteriores de ASA:

```
! 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
```

> **Precaución**: Cuando aplica los comandos estáticos PAT, recibe este mensaje de error en la interfaz de línea de comandos ASA, **"ERROR: NAT no puede reservar puertos"**. Después de esto, proceda a borrar las entradas xlate en el ASA, para esto, ejecute el comando **clearxlatelocal x.x.x.x**, desde donde x.x.x.x corresponde a la dirección IP externa de ASA. Este comando borra todas las traducciones asociadas con esta dirección IP y las ejecuta con precaución en entornos de producción.

Para las versiones 8.2 y anteriores de ASA:

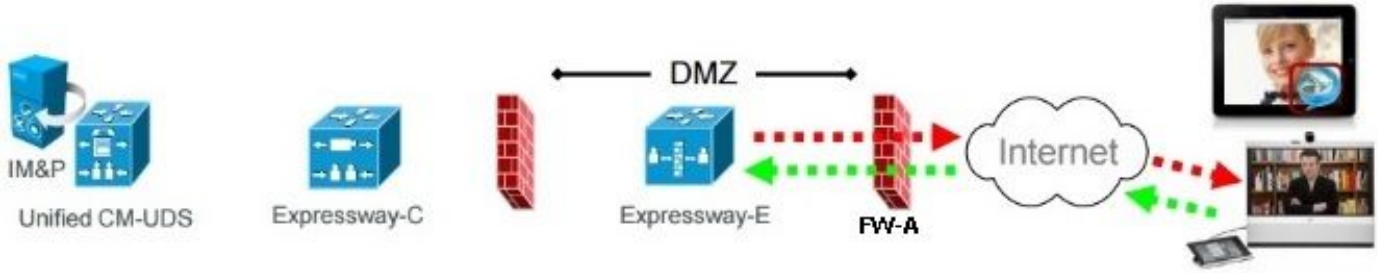
```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

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

Paso 2. La configuración de la lista de control de acceso (ACL) permite que los puertos necesarios de Internet a Expressway-E sean necesarios.

Según Unified Communication: Expressway (DMZ) a la documentación pública de Internet, la lista de puertos TCP y UDP que Expressway-E requiere permitir en FW-A, son como se muestra en la imagen:

Unified Communications: Expressway (DMZ) to public internet



		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 8.3 y posteriores de ASA:

```
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5222
access-list outside-in extended permit tcp any host 10.0.10.2 eq 8443
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
access-list outside-in extended permit udp any host 10.0.10.2 lt 3484
access-list outside-in extended permit udp any host 10.0.10.2 gt 23999
access-list outside-in extended permit udp any host 10.0.10.2 lt 30000
access-list outside-in extended permit udp any host 10.0.10.2 gt 36001
access-list outside-in extended permit udp any host 10.0.10.2 lt 60000
access-list outside-in extended permit udp any host 10.0.10.2 eq 5061
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5061

access-group outside-in in interface outside
```

Para las versiones 8.2 y anteriores de ASA:

```
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5222
access-list outside-in extended permit tcp any host 64.100.0.10 eq 8443
access-list outside-in extended permit udp any host 64.100.0.10 gt 3477
access-list outside-in extended permit udp any host 64.100.0.10 lt 3484
access-list outside-in extended permit udp any host 64.100.0.10 gt 23999
access-list outside-in extended permit udp any host 64.100.0.10 lt 30000
access-list outside-in extended permit udp any host 64.100.0.10 gt 36001
access-list outside-in extended permit udp any host 64.100.0.10 lt 60000
access-list outside-in extended permit udp any host 64.100.0.10 eq 5061
```

```
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5061

access-group outside-in in interface outside
```

Configuración de FW-B

Como se explica en la sección Información de Fondo de este documento, FW B puede requerir una configuración NAT dinámica o PAT para permitir que la subred interna 10.0.30.0/24 se traduzca a la dirección IP 10.0.20.1 cuando vaya a la interfaz exterior del FW B.

Para las versiones 8.3 y posteriores de ASA:

```
object network obj-10.0.30.0
   subnet 10.0.30.0 255.255.255.0
   nat (inside,outside) dynamic interface
```

Para las versiones 8.2 y anteriores de ASA:

```
nat (inside) 1 10.0.30.0 255.255.255.0
global (outside) 1 interface
```

> **Sugerencia**: asegúrese de que todos los puertos TCP y UDP requeridos permitan que Expressway-C funcione correctamente y estén abiertos en el FW B, tal como se especifica en este documento de Cisco: Uso de puertos IP de Cisco Expressway para firewall transversal

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Packet Tracer se puede utilizar en el ASA para confirmar que la traducción NAT estática de Expressway-E funciona según sea necesario.

Packet Tracer to Test 64.100.0.10 en TCP/5222

```
FW-A#packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 5222

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/5222 to 10.0.10.2/5222

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
```

```
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5222
Additional Information:

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

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 13, packet dispatched to next module

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

Packet Tracer to Test 64.100.0.10 en TCP/8443

```
FW-A# packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 8443

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/8443 to 10.0.10.2/8443

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
```

```
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 8443
Additional Information:

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

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 14, packet dispatched to next module

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

Packet Tracer para probar 64.100.0.10 en TCP/5061

```
FW-1# packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 5061

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/5061 to 10.0.10.2/5061

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
```

```
Config:
access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5061
Additional Information:

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

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 15, packet dispatched to next module

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

Packet Tracer a Test 64.100.0.10 en UDP/24000

```
ASA1# packet-tracer input outside udp 4.2.2.2 1234 64.100.0.10 24000

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/24000 to 10.0.10.2/24000

Phase: 2
Type: ACCESS-LIST
Subtype: log
```

```
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
Additional Information:

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

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 16, packet dispatched to next module

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

Packet Tracer a Prueba 64.100.0.10 en UDP/36002

```
ASA1# packet-tracer input outside udp 4.2.2.2 1234 64.100.0.10 36002

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
Additional Information:
NAT divert to egress interface inside
Untranslate 64.100.0.10/36002 to 10.0.10.2/36002

Phase: 2
Type: ACCESS-LIST
```

```
Subtype: log
Result: ALLOW
Config:
access-group outside-in in interface outside
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
Additional Information:

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

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network obj-10.0.10.2
 nat (inside,outside) static interface
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 17, packet dispatched to next module

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

Troubleshoot

Paso 1. Compare Capturas de paquetes.

Las capturas de paquetes se pueden realizar tanto en las interfaces de entrada como de salida de ASA.

```
FW-A# sh cap
capture capout interface outside match ip host 64.100.0.100 host 64.100.0.10
capture capin interface inside match ip host 64.100.0.100 host 10.0.10.2
```

Capturas de paquetes para 64.100.0.10 en TCP/5222:

```
FW-A# sh cap capout

2 packets captured
   1: 21:39:33.646954 64.100.0.100.21144 > 64.100.0.10.5222: S 4178032747:4178032747(0) win 4128
<mss 1460>
   2: 21:39:35.577652 64.100.0.100.21144 > 64.100.0.10.5222: S 4178032747:4178032747(0) win 4128
<mss 1460>
2 packets shown

FW-A# sh cap capin

2 packets captured
   1: 21:39:33.647290 64.100.0.100.21144 > 10.0.10.2.5222: S 646610520:646610520(0) win 4128
<mss 1380>
   2: 21:39:35.577683 64.100.0.100.21144 > 10.0.10.2.5222: S 646610520:646610520(0) win 4128
<mss 1380>
2 packets shown
```

Capturas de paquetes para 64.100.0.10 en TCP/5061:

```
FW-A# sh cap capout
2 packets captured

   1: 21:42:14.920576 64.100.0.100.50820 > 64.100.0.10.5061: S 2023539318:2023539318(0) win 4128
<mss 1460>
   2: 21:42:16.992380 64.100.0.100.50820 > 64.100.0.10.5061: S 2023539318:2023539318(0) win 4128
<mss 1460>
2 packets shown
FW-A# sh cap capin 2 packets captured 1: 21:42:14.920866 64.100.0.100.50820 > 10.0.10.2.5061: S
2082904361:2082904361(0) win 4128 <mss 1380> 2: 21:42:16.992410 64.100.0.100.50820 >
10.0.10.2.5061: S 2082904361:2082904361(0) win 4128 <mss 1380> 2 packets shown
```

Paso 2. Inspeccionar capturas de paquetes descartados de ruta de seguridad acelerada (ASP).

La captura de ASA ASP captura las caídas de paquetes de un ASA. La opción **all**, captura todas las razones posibles por las que ASA descartó un paquete. Esto puede reducirse si hay alguna razón sospechosa. Para obtener una lista de las razones que utiliza un ASA para clasificar estas caídas, ejecute el comando **show asp drop.**

```
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
```

> **Consejo:** La captura de ASA ASP se utiliza en esta situación para confirmar si el ASA descarta paquetes debido a una configuración de ACL o NAT perdida, que requeriría abrir un puerto TCP o UDP específico para Expressway-E.

> **Consejo:** El tamaño predeterminado del búfer para cada captura ASA es de 512 KB. Si el ASA descarta demasiados paquetes, el búfer se llena rápidamente. El tamaño del búfer se

puede aumentar con la opción **buffer**.

Recomendaciones

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
```

Implementación alternativa de VCS Expressway

Una solución alternativa para implementar Expressway-E con interfaces de red duales/NIC duales es implementar Expressway-E pero con una configuración de reflexión de NAT y NIC única en los firewalls. El siguiente enlace muestra más detalles sobre esta implementación Configure NAT Reflection en ASA para dispositivos de VCS Expressway TelePresence.

> **Consejo:** La implementación recomendada para VCS Expressway son las interfaces de red duales/implementación de NIC VCS Expressway dual descritas en este documento.

Información Relacionada

- Configuración de NAT Reflection en ASA para dispositivos VCS Expressway TelePresence
- Soporte Técnico y Documentación - Cisco Systems
- Cisco Expressway-E y Expressway-C: guía de implementación de configuración básica
- Colocación de Cisco VCS Expressway en una DMZ en lugar de en Internet pública
- Uso del puerto IP de Cisco Expressway para firewall transversal