Guía de Troubleshooting de Configuración de ZBFW para IOS-XE

Contenido

Introducción

Este documento describe cómo resolver mejor los problemas de la función de firewall basado en zonas (ZBFW) en el router de servicios de agregación (ASR) 1000, con comandos que se utilizan para sondear los contadores de caídas de hardware en el ASR. ASR1000 es una plataforma de reenvío basada en hardware. La configuración de software de Cisco IOS-XE® programa los ASIC de hardware (procesador de flujo cuántico (QFP) para realizar funciones de reenvío de funciones. Esto permite un mayor rendimiento y un mejor rendimiento. La desventaja de esto es que presenta un mayor desafío para resolver problemas. Los comandos tradicionales de Cisco IOS utilizados para sondear las sesiones actuales y los contadores de caídas mediante el firewall basado en zonas (ZBFW) ya no son válidos, ya que las caídas ya no se encuentran en el software.

Enlaces y documentación

Referencias de Comando

- Referencias de Comandos de Routers de Servicios de Agregación de la Serie ASR 1000 de Cisco
- Referencias de Comandos de Cisco IOS XE 3S

Pasos de Troubleshooting de Datapath

Para resolver problemas de la ruta de datos, debe identificar si el tráfico pasa correctamente a través del código ASR y Cisco IOS-XE. Específicamente para las funciones de firewall, la resolución de problemas de la ruta de datos sigue estos pasos:

1. **Verificar configuración**: recopile la configuración y examine el resultado para verificar la conexión.

2. **Verifique el estado de la conexión**: si el tráfico pasa correctamente, Cisco IOS-XE abre una conexión en la función ZBFW. Esta conexión realiza un seguimiento del tráfico y la información de estado entre un cliente y un servidor.

3. **Verificar contadores de caídas**: cuando el tráfico no pasa correctamente, Cisco IOS-XE registra un contador de caídas para cualquier paquete descartado. Verifique esta salida para aislar la causa de la falla de tráfico.

4. **Registro**: recopile los registros del sistema para proporcionar información más granular sobre las generaciones de conexiones y las caídas de paquetes.

5. **Packet Trace Dropped Packets** - Use el seguimiento de paquetes para capturar paquetes perdidos.

6. **Depuraciones**: la opción más detallada es Recopilar depuraciones. Las depuraciones se pueden obtener condicionalmente para confirmar el trayecto de reenvío exacto para los paquetes.

Verificar configuración

El resultado de **show tech support firewall** se resume aquí:

```
-------- show clock --------
-------- show version -------
-------- show running-config --------
-------- show parameter-map type inspect --------
-------- show policy-map type inspect -------
-------- show class-map type inspect --------
-------- show zone security --------
-------- show zone-pair security --------
-------- show policy-firewall stats global --------
-------- show policy-firewall stats zone --------
-------- show platform hardware qfp active feature firewall datapath <submode> --------
-------- show platform software firewall RP <submode> --------
```

Verificar estado de conexión

La información de conexión se puede obtener para que se muestren todas las conexiones en ZBFW. Ingrese este comando:

```
ASR#show policy-firewall sessions platform
--show platform hardware qfp active feature firewall datapath scb any any any any any all any --
[s=session  i=imprecise channel  c=control channel  d=data channel]
 14.38.112.250 41392 14.36.1.206 23 proto 6 (0:0)    [sc]
```

Muestra una conexión Telnet TCP de 14.38.112.250 a 14.36.1.206.

> **Nota:** Tenga en cuenta que si ejecuta este comando, tomará mucho tiempo si hay muchas conexiones en el dispositivo. Cisco recomienda ejecutar este comando con filtros específicos, tal y como se describe aquí.

La tabla de conexión se puede filtrar a una dirección de origen o de destino específica. Utilice filtros después del submodo **de plataforma**. Las opciones para filtrar son:

```
radar-ZBFW1#show policy-firewall sessions platform ?
 all                     detailed information
 destination-port        Destination Port Number
 detail                  detail on or off
 icmp                    Protocol Type ICMP
 imprecise               imprecise information
 session                 session information
 source-port             Source Port
 source-vrf              Source Vrf ID
 standby                 standby information
 tcp                     Protocol Type TCP
 udp                     Protocol Type UDP
 v4-destination-address  IPv4 Desination Address
 v4-source-address       IPv4 Source Address
 v6-destination-address  IPv6 Desination Address
 v6-source-address       IPv6 Source Address
 |                       Output modifiers
 <cr>
```

Esta tabla de conexión se filtra para mostrar solamente las conexiones que se originan en 14.38.112.250:

```
ASR#show policy-firewall sessions platform v4-source-address 14.38.112.250
--show platform hardware qfp active feature firewall datapath scb 14.38.112.250
any any any any all any --
[s=session  i=imprecise channel  c=control channel  d=data channel]
 14.38.112.250 41392 14.36.1.206 23 proto 6 (0:0)    [sc]
```

Una vez que se filtra la tabla de conexión, se puede obtener la información de conexión detallada para un análisis más completo. Para mostrar este resultado, utilice la palabra clave **detail**.

```
ASR#show policy-firewall sessions platform v4-source-address 14.38.112.250 detail
--show platform hardware qfp active feature firewall datapath scb 14.38.112.250
any any any any all any detail--
[s=session  i=imprecise channel  c=control channel  d=data channel]
 14.38.112.250 41426 14.36.1.206 23 proto 6 (0:0)       [sc]
```

```
pscb : 0x8c5d4f20,  bucket : 64672, fw_flags: 0x204 0x20419441,
      scb state: active, scb debug: 0
nxt_timeout: 360000, refcnt: 1,  ha nak cnt: 0,  rg: 0, sess id: 117753
hostdb: 0x0, L7: 0x0, stats: 0x8e118e40, child: 0x0
l4blk0: 78fae7a7 l4blk1: e36df99c l4blk2: 78fae7ea l4blk3: 39080000
l4blk4: e36df90e l4blk5: 78fae7ea l4blk6: e36df99c l4blk7: fde0000
l4blk8: 0 l4blk9: 1
root scb: 0x0 act_blk: 0x8e1115e0
ingress/egress intf: GigabitEthernet0/0/2 (1021), GigabitEthernet0/0/0 (131065)
current time 34004163065573 create tstamp: 33985412599209 last access: 33998256774622
nat_out_local_addr:port: 0.0.0.0:0 nat_in_global_addr:port: 0.0.0.0:0
syncookie fixup: 0x0
halfopen linkage: 0x0 0x0
cxsc_cft_fid: 0x0
tw timer: 0x0 0x0 0x372ba 0x1e89c181
Number of simultaneous packet per session allowed: 25
  bucket 125084 flags 1 func 1 idx 8 wheel 0x8ceb1120
```

Comprobar contadores de caídas de firewall

La salida del contador de caídas cambió durante XE 3.9. Antes de XE 3.9, las razones de caída del firewall eran muy genéricas. Después de XE 3.9, las razones de caída del firewall se ampliaron para ser más granulares.

Para verificar los contadores de caídas, realice dos pasos:

1. Confirme los contadores de caídas globales en Cisco IOS-XE. Estos contadores muestran qué función ha descartado el tráfico. Algunos ejemplos de funciones son Calidad de servicio (QoS), Traducción de direcciones de red (NAT), Firewall, etc.

2. Una vez identificada la subcaracterística, consulte los contadores de caídas granulares que ofrece la subcaracterística. En esta guía, la subcaracterística que se analiza es la función Firewall.

Contadores de caídas globales en QFP

El comando básico en el que confiar proporciona todas las caídas a través de QFP:

```
Router#show platform hardware qfp active statistics drop
```

Este comando muestra las caídas genéricas globalmente en el QFP. Estas caídas pueden estar en cualquier función. Algunas características de ejemplo son:

```
Ipv4Acl
Ipv4NoRoute
Ipv6Acl
Ipv6NoRoute
NatIn2out
VfrErr
...etc
```

Para ver todas las caídas, incluya los contadores que tienen un valor de cero, utilice el comando:

```
show platform hardware qfp active statistics drop all
```

Para borrar los contadores, utilice este comando. Borra la salida después de mostrarla en la pantalla. Este comando está claro al leer, por lo que el resultado se restablece a cero **después de** que se muestre en la pantalla.

```
show platform hardware qfp active statistics drop clear
```

A continuación se ofrece una lista de los contadores de caídas de firewall globales de QFP y una explicación:

Motivo de caída global del firewall	Explicación
FirewallRepresión	Caída de paquetes debido a contrapresión por el mecanismo de registro.
ZonaNoVálidaFirewall	No hay ninguna zona de seguridad configurada para la interfaz.
FirewallL4Insp	Falla de verificación de política L4. Consulte la tabla siguiente para obtener información más detallada sobre los motivos de las caídas (motivos de las caíd de las funciones del firewall).
ZonaSinReenvíoFirewall	El firewall no se inicializa y no se permite el paso de tráfico.
FirewallNoSesión	La creación de la sesión falla. Podría deberse a que se ha alcanzado el límite máximo de sesiones o a una falla en la asignación de memoria.
Política de firewall	Se descarta la política de firewall configurada.
FirewallL4	Falla de inspección L4. Consulte la tabla siguiente para obtener información m detallada sobre los motivos de las caídas (Motivos de descarte de la función d firewall).
FirewallL7	Caída de paquetes debido a inspección L7. Consulte a continuación una lista d motivos de caída L7 más granulares (motivos de descarte de la función Firewa
FirewallNotInitiator	No es un iniciador de sesión para TCP, UDP o ICMP. No se ha creado ninguna sesión. Por ejemplo, para ICMP, el primer paquete recibido no es ECHO ni TIMESTAMP. Para TCP, no es un SYN.
FirewallNoNewSession	Esto podría ocurrir en el procesamiento normal de paquetes o en el procesamiento impreciso del canal. Firewall High Availability no permite nuevas sesiones.
FirewallSyncookieMaxDst	Para proporcionar protección contra inundación SYN basada en host, existe un velocidad SYN por destino como límite de inundación SYN. Cuando el número entradas de destino alcanza el límite, se descartan los paquetes SYN nuevos.
FirewallSyncookie	Se activa la lógica SYNCOOLIE. Esto indica que se envió SYN/ACK con la cookie SYN y se descartó el paquete SYN original.
FirewallARStandby	El enrutamiento asimétrico no está habilitado y el grupo de redundancia no es en estado activo.

Contadores de caídas de funciones de firewall en QFP

La limitación con el contador de caídas global de QFP es que no hay granularidad en las razones de caída, y algunas de las razones de caída como **FirewallL4** se sobrecargan tanto que es de poca utilidad para la resolución de problemas. Esto se ha mejorado desde entonces en Cisco IOS-XE 3.9 (15.3(2)S), donde se agregaron los contadores de caídas de funciones del firewall. Esto proporciona un conjunto mucho más granular de razones de caída:

```
ASR#show platform hardware qfp active feature firewall drop all
-----------------------------------------------------------------------------
Drop Reason Packets
-----------------------------------------------------------------------------
Invalid L4 header 0
```

```
Invalid ACK flag 0
Invalid ACK number 0
....
```

A continuación se ofrece una lista de las razones y explicaciones de las caídas de funciones del firewall:

Motivo de la caída de la función de firewall	Explicación
Longitud de encabezado no válida	El datagrama es tan pequeño que no puede contener el encabezado ICMP, TCP o TCP capa 4. Podría deberse a: 1. longitud del encabezado TCP < 20 2. Longitud del encabezado UDP/ICMP < 8
Longitud de datos UDP no válida	La longitud del datagrama UDP no coincide con la longitud especificada en el encabez UDP.
Número ACK no válido	Esta caída podría deberse a una de estas razones: 1. ACK no es igual al siguiente_seq# del par TCP. 2. ACK es mayor que el número SEQ más reciente enviado por el peer TCP. En el estado TCP SYNSENT y SYNRCVD, se espera que el ACK# sea igual a ISN+1 p no lo es.
Indicador ACK no válido	Esta caída podría deberse a una de estas razones: 1. Se espera el indicador ACK pero no se establece en un estado TCP diferente. 2. Aparte del indicador ACK, también se establece otro indicador (como RST).
Iniciador TCP no válido	Esto sucede cuando: 1. El primer paquete de un iniciador TCP no es un SYN (el segmento TCP no inicial s recibe sin una sesión válida). 2. El paquete SYN inicial tiene el indicador ACK configurado.
SYN con datos	El paquete SYN contiene carga útil. Esto no se admite.
Indicadores TCP no válidos	Los indicadores TCP no válidos pueden ser causados por: 1. El paquete SYN inicial de TCP tiene indicadores distintos de SYN. 2. En el estado de escucha TCP, un peer TCP recibe un RST o un ACK. 3. El paquete de otro respondedor se recibe antes de SYN/ACK. 4. SYN/ACK esperado no se recibe del respondedor.
Segmento no válido en estado SYNSENT	Un segmento TCP no válido en estado SYNSENT es causado por: 1. SYN/ACK tiene carga útil. 2. SYN/ACK tiene otros indicadores (PSH, URG, FIN) configurados. 3. Reciba un SYN de tránsito con carga útil. 4. Reciba un paquete no SYN del iniciador.
Segmento no válido en estado SYNRCVD	Un segmento TCP no válido en estado SYNRCVD podría ser causado por: 1. Reciba un SYN de retránsito con carga útil del iniciador. 2. Reciba un segmento no válido que no sea SYN/ACK, RST o FIN del respondedor. Esto ocurre en el estado SYNRCVD cuando los segmentos provienen del iniciador. Se a:
SEQ no válida	1. Seq# es menor que ISN. 2. Si el tamaño de la ventana rcvd del receptor es 0 y: El segmento tiene carga o Segmento fuera de orden (el número de cola es mayor que el receptor LASTACK. 3. Si el tamaño de la ventana rcvd del receptor es 0 y seq# cae más allá de la ventar

	4. Seq# es igual a ISN pero no a un paquete SYN.
Opción de ampliación de ventana no válida	La opción de escala de ventana TCP no válida se debe a una longitud de byte incorrec la opción de escala de ventana.
TCP fuera de la ventana	El paquete es demasiado viejo: una ventana detrás del ACK del otro lado. Esto podría o en el estado ESTABLECIDO, CERRADO y LASTACK.
Carga útil adicional de TCP después de que se envió FIN	Carga recibida después de enviar FIN. Esto podría suceder en el estado de CLOSEWA
Desbordamiento de ventana TCP	Esto ocurre cuando el tamaño del segmento entrante desborda la ventana del receptor. embargo, si se habilita vTCP, esta condición se permite porque el firewall necesita almacenar en búfer el segmento para que el ALG lo consuma más tarde.
Volver con etiquetas no válidas	El receptor ya reconoció un paquete retransmitido.
Segmento fuera de pedido TCP	El paquete Out-Of-Order está a punto de ser entregado a L7 para su inspección. Si L7 permite el segmento OOO, este paquete se descartará.
Inundación SYN	Bajo un ataque de inundación TCP SYN. Bajo ciertas condiciones cuando las conexion actuales a este host exceden el valor semirabierto configurado, el firewall rechazará cualquier nueva conexión a esta dirección IP durante un período de tiempo. Como resu se descartarán los paquetes.
Error interno: error al asignar comprobación de la sininundación	Durante la verificación de la sininundación, la asignación de hostdb falla. Acción Recomendada: marque "show platform hardware qfp active feature firewall mem para verificar el estado de la memoria.
Desconexión de sininundación	Si se exceden las conexiones semirabiertas configuradas y se configura el tiempo de apagón, se descartan todas las conexiones nuevas a esta dirección IP.
Límite de sesiones semirabiertas excedido	El paquete se descartó debido a que se excedieron las sesiones semirabiertas permitid También verifique las configuraciones de "max-complete high/low" y "one-minute high/l para asegurarse de que el número de sesiones semirabiertas no esté siendo reducido p estas configuraciones.
Demasiados paquetes por flujo	Se supera el número máximo de paquetes inspeccionables permitidos por flujo. El núm máximo es 25.
Demasiados paquetes de error ICMP por flujo	Se supera el número máximo de paquetes de error ICMP permitidos por flujo. El númer máximo es 3.
Carga útil TCP no esperada de Rsp a Init	En el estado SYNRCVD, TCP recibe un paquete con carga útil del respondedor a la dirección del iniciador.
Error interno - Dirección no definida	Dirección del paquete no definida.
SYN dentro de la ventana actual	Se ve un paquete SYN dentro de la ventana de una conexión TCP ya establecida.
RST dentro de la ventana	Se observa un paquete RST dentro de la ventana de una conexión TCP ya establecida

actual	
Segmento inactivo	Se recibe un segmento TCP que no debería haberse recibido a través de la máquina de estado TCP, como un paquete TCP SYN que se recibe en el estado de escucha del respondedor.
Error interno de ICMP: información de NAT de ICMP perdida	El paquete ICMP no está activado pero falta la información NAT interna. Este es un erro interno.
Paquete ICMP en estado de cierre SCB	Recibió un paquete ICMP en el estado SCB CLOSE.
Encabezado IP perdido en paquete ICMP	Falta el encabezado IP en el paquete ICMP.
Error ICMP sin IP ni ICMP	Paquete de error ICMP sin IP o ICMP en carga útil. Probablemente causado por un pac mal formado o un ataque.
Pkt ICMP Err Demasiado Corto	El paquete de error ICMP es demasiado corto.
Límite de ráfaga de error ICMP excedido	El paquete de error ICMP supera el límite de ráfaga de 10.
Error ICMP inalcanzable	El paquete de error ICMP no se puede alcanzar excede el límite. Sólo se permite pasar primer paquete inalcanzable.
Nº De Seq No Válido De ICMP Err	Seq# de paquete incrustado no coincide con el seq# del paquete que origina el error IC
ICMP Err Invalid Ack	ACK no válido en el paquete de error ICMP incrustado.
Descarte de acción ICMP	La acción ICMP configurada es drop.
Par de zonas sin mapa de políticas	La política no está presente en el par de zonas. podría deberse a que el ALG (Applicati Layer Gateway) no se ha configurado para abrir el orificio de entrada para el canal de d de la aplicación, o al ALG no se ha abierto correctamente el orificio de entrada o no se abierto ningún orificio de entrada debido a problemas de escalabilidad.
Sesión Perdida Y Política No Presente	Error en la búsqueda de sesión y no hay ninguna política presente para inspeccionar es paquete.
Error ICMP Y Política No Presente	Error ICMP sin política configurada en el par de zonas.
Error de clasificación	Falla de clasificación en un par de zonas dado cuando el firewall intenta determinar si e protocolo es inspeccionable.
Descarte de acción de clasificación	La acción de clasificación es descartada.
Configuración errónea de la política de seguridad	Error en la clasificación debido a una configuración incorrecta de la política de seguridad Esto también podría deberse a que no hay una clavija para el canal de datos L7.
Enviar RST al	Enviar RST al respondedor en estado SYNSENT cuando ACK# no es igual a ISN+1.

respondedor	
Descarte de política de firewall	La acción de la política es caer.
Descarte de fragmentos	Descartar los fragmentos restantes cuando se descarta el primer fragmento.
Descarte de política de firewall ICMP	La acción de política del paquete integrado ICMP es DROP.
La inspección L7 devuelve DROP	L7 (ALG) decide descartar el paquete. La razón se puede encontrar en diferentes estadísticas de ALG.
Pkt De Segmento L7 No Permitido	Paquete segmentado recibido cuando ALG no lo honra.
L7 Fragmento Pkt No Permitido	Se recibieron paquetes fragmentados (o VFR) cuando ALG no los cumple.
Tipo de prueba L7 desconocido	Tipo de protocolo no reconocido.

Resolución de problemas de caídas de firewall

Una vez identificado el motivo de la caída desde los contadores de caídas de funciones globales o de firewall anteriores, podrían ser necesarios pasos adicionales para la resolución de problemas si estas caídas son inesperadas. Aparte de la validación de la configuración para asegurarse de que la configuración es correcta para las funcionalidades de firewall habilitadas, a menudo se requiere tomar capturas de paquetes para el flujo de tráfico en cuestión para ver si los paquetes están mal formados o si hay algún problema de implementación de protocolo o aplicación.

Registro

La funcionalidad de registro ASR genera syslogs para registrar los paquetes perdidos. Estos syslogs proporcionan más detalles sobre por qué se descartó el paquete. Hay dos tipos de sysloggings:

1. syslogging almacenado en búfer local

2. Registro remoto de alta velocidad

Syslogging en búfer local

Para aislar la causa de las caídas, puede utilizar la resolución de problemas genérica de ZBFW, como habilitar las caídas de registro. Hay dos maneras de configurar el registro de descarte de paquetes.

Método 1: Utilice inspect-global parámetro-map para registrar todos los paquetes perdidos.

```
parameter-map type inspect-global     log dropped-packets
```

Método 2: Utilice el mapa de parámetro de inspección personalizado para registrar los paquetes

perdidos sólo para una clase específica.

```
parameter-map type inspect LOG_PARAM
log dropped-packets
!
policy-map type inspect ZBFW_PMAP
class type inspect ZBFW_CMAP
inspect LOG_PARAM
```

Estos mensajes se envían al registro o a la consola en función de la configuración del ASR para el registro. Este es un ejemplo de un mensaje de registro de caídas.

```
*Apr  8 13:20:39.075: %IOSXE-6-PLATFORM: F0: cpp_cp: QFP:0.0 Thread:103
TS:00000605668054540031 %FW-6-DROP_PKT: Dropping tcp pkt from GigabitEthernet0/0/2
14.38.112.250:41433 => 14.36.1.206:23(target:class)-(INSIDE_OUTSIDE_ZP:class-default)
due to Policy drop:classify result with ip ident 11579 tcp flag 0x2, seq 2014580963,
ack 0
```

Limitaciones del Syslogging en Búfer Local

1. Estos registros se limitan a la velocidad según el ID de bug de Cisco CSCud09943.

2. Es posible que estos registros no se impriman a menos que se aplique una configuración específica. Por ejemplo, los paquetes descartados por paquetes class-default no se registrarán a menos que se especifique la palabra clave **log**:

```
policy-map type inspect ZBFW_PMAP
class class-default
drop log
```

Registro remoto de alta velocidad

El registro de alta velocidad (HSL) genera registros del sistema directamente desde QFP y los envía al colector HSL de NetFlow configurado. Esta es la solución de registro recomendada para ZBFW en ASR.

Para HSL, utilice esta configuración:

```
parameter-map type inspect inspect-global
  log template timeout-rate 1
  log flow-export v9 udp destination 1.1.1.1 5555
```

Para utilizar esta configuración, se requiere un colector de NetFlow capaz de la versión 9 de Netflow. Esto se detalla en

Guía de configuración: Firewall de políticas basado en zonas, firewall Cisco IOS XE versión 3S (ASR 1000) Registro de alta velocidad

Seguimiento de paquetes mediante coincidencia condicional

Active las depuraciones condicionales para habilitar el seguimiento de paquetes y después habilitar el seguimiento de paquetes para estas funciones:

```
ip access-list extended CONDITIONAL_ACL
 permit ip host 10.1.1.1 host 192.168.1.1
 permit ip host 192.168.1.1 host 10.1.1.1
!
debug platform condition feature fw dataplane submode all level info
debug platform condition ipv4 access-list CONDITIONAL_ACL both
```

> **Nota:** La condición de coincidencia puede utilizar la dirección IP directamente, ya que no es necesaria una ACL. Esto coincidirá como origen o destino que permite rastros bidireccionales. Este método se puede utilizar si no se le permite modificar la configuración. Por ejemplo: debug platform condition ipv4 address 192.168.1.1/32.

Active la función de seguimiento de paquetes:

```
debug platform packet-trace copy packet both
debug platform packet-trace packet 16
debug platform packet-trace drop
debug platform packet-trace enable
```

Hay dos formas de utilizar esta función:

1. Ingrese el comando **debug platform packet-trace drop** para rastrear solamente los paquetes perdidos.

2. La exclusión del comando **debug platform packet-trace drop** rastreará cualquier paquete que coincida con la condición, que incluye aquellos que son inspeccionados/pasados por el dispositivo.

Activar depuraciones condicionales:

```
debug platform condition start
```

Ejecute la prueba y, a continuación, desactive las depuraciones:

```
debug platform condition stop
```

Ahora la información se puede mostrar en la pantalla. En este ejemplo, los paquetes ICMP se descartaron debido a una política de firewall:

```
Router#show platform packet-trace statistics
Packets Summary
 Matched  2
 Traced   2
Packets Received
 Ingress  2
 Inject   0
Packets Processed
 Forward  0
 Punt     0
 Drop     2
   Count       Code  Cause
   2           183   FirewallPolicy
```

```
 Consume  0
```

```
Router#show platform packet-trace summary
Pkt   Input            Output           State  Reason
0     Gi0/0/2          Gi0/0/0          DROP   183 (FirewallPolicy)
1     Gi0/0/2          Gi0/0/0          DROP   183 (FirewallPolicy)
```

```
Router#show platform packet-trace packet 0
Packet: 0           CBUG ID: 2980
Summary
 Input     : GigabitEthernet0/0/2
 Output    : GigabitEthernet0/0/0
 State     : DROP 183 (FirewallPolicy)
 Timestamp
   Start   : 1207843476722162 ns (04/15/2014 12:37:01.103864 UTC)
   Stop    : 1207843477247782 ns (04/15/2014 12:37:01.104390 UTC)
Path Trace
 Feature: IPV4
   Source      : 10.1.1.1
   Destination : 192.168.1.1
   Protocol    : 1 (ICMP)
 Feature: ZBFW
   Action  : Drop
   Reason  : ICMP policy drop:classify result
   Zone-pair name  : INSIDE_OUTSIDE_ZP
   Class-map name  : class-default
Packet Copy In
 c89c1d51 5702000c 29f9d528 08004500 00540000 40004001 ac640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
Packet Copy Out
 c89c1d51 5702000c 29f9d528 08004500 00540000 40003f01 ad640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
```

El comando **show platform packet-trace packet <num> decode** decodifica la información y el contenido del encabezado del paquete. Esta función se introdujo en XE3.11:

```
Router#show platform packet-trace packet all decode
Packet: 0           CBUG ID: 2980
Summary
 Input     : GigabitEthernet0/0/2
 Output    : GigabitEthernet0/0/0
 State     : DROP 183 (FirewallPolicy)
 Timestamp
   Start   : 1207843476722162 ns (04/15/2014 12:37:01.103864 UTC)
   Stop    : 1207843477247782 ns (04/15/2014 12:37:01.104390 UTC)
Path Trace
 Feature: IPV4
    Source      : 10.1.1.1
    Destination : 192.168.1.1
    Protocol    : 1 (ICMP)
  Feature: ZBFW
    Action  : Drop
    Reason  : ICMP policy drop:classify result
    Zone-pair name  : INSIDE_OUTSIDE_ZP
    Class-map name  : class-default
Packet Copy In
 c89c1d51 5702000c 29f9d528 08004500 00540000 40004001 ac640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
```

```
 ARPA
    Destination MAC     : c89c.1d51.5702
    Source MAC          : 000c.29f9.d528
    Type                : 0x0800 (IPV4)
 IPv4
    Version             : 4
    Header Length       : 5
    ToS                 : 0x00
    Total Length        : 84
    Identifier          : 0x0000
    IP Flags            : 0x2 (Don't fragment)
    Frag Offset         : 0
    TTL                 : 64
    Protocol            : 1 (ICMP)
    Header Checksum     : 0xac64
    Source Address      : 10.1.1.1
    Destination Address : 192.168.1.1
 ICMP
    Type                : 8 (Echo)
    Code                : 0 (No Code)
    Checksum            : 0x172a
    Identifier          : 0x2741
    Sequence            : 0x0001
Packet Copy Out
 c89c1d51 5702000c 29f9d528 08004500 00540000 40003f01 ad640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
 ARPA
    Destination MAC     : c89c.1d51.5702
    Source MAC          : 000c.29f9.d528
    Type                : 0x0800 (IPV4)
 IPv4
    Version             : 4
    Header Length       : 5
    ToS                 : 0x00
    Total Length        : 84
    Identifier          : 0x0000
    IP Flags            : 0x2 (Don't fragment)
    Frag Offset         : 0
    TTL                 : 63
    Protocol            : 1 (ICMP)
    Header Checksum     : 0xad64
    Source Address      : 10.1.1.1
    Destination Address : 192.168.1.1
 ICMP
    Type                : 8 (Echo)
    Code                : 0 (No Code)
    Checksum            : 0x172a
    Identifier          : 0x2741
    Sequence            : 0x0001
```

Captura de paquetes integrada

La compatibilidad con la captura de paquetes integrada se ha agregado en Cisco IOS-XE 3.7 (15.2(4)S). Para obtener más información, consulte

Ejemplo de Configuración de Captura de Paquetes Incrustada para Cisco IOS e IOS-XE.

Depuraciones

Depuraciones condicionales

En XE3.10, se introducirán depuraciones condicionales. Las sentencias condicionales se pueden utilizar para asegurar que la función ZBFW sólo registre los mensajes de depuración que sean relevantes para la condición. Los debugs condicionales utilizan ACL para restringir los registros que coinciden con los elementos ACL. Además, antes de XE3.10, los mensajes de depuración eran más difíciles de leer. El resultado de la depuración se mejoró en XE3.10 para facilitar su comprensión.

Para habilitar estos debugs, ejecute este comando:

```
debug platform condition feature fw dataplane submode [detail | policy | layer4 | drop]
debug platform condition ipv4 access-list <ACL_name> both
debug platform condition start
```

Observe que el comando condition debe configurarse a través de una ACL y una direccionalidad. Los debugs condicionales no se implementarán hasta que se inicien con el comando **debug platform condition start**. Para desactivar las depuraciones condicionales, utilice el comando **debug platform condition stop**.

```
debug platform condition stop
```

Para desactivar las depuraciones condicionales, **NO** utilice el comando **undebug all**. Para desactivar todas las depuraciones condicionales, utilice el comando:

```
ASR#clear platform condition all
```

Antes de XE3.14, las depuraciones **ha** y **event** no son condicionales. Como resultado, el comando **debug platform condition fw dataplane submode all** hace que se creen todos los registros, independientemente de la condición seleccionada a continuación. Esto podría crear ruido adicional que dificulta la depuración.

De forma predeterminada, el nivel de registro condicional es **info**. Para aumentar/disminuir el nivel de registro, utilice el comando:

```
debug platform condition feature fw dataplane submode all [verbose | warning]
```

Recopilar y ver depuraciones

Los archivos de depuración no se imprimirán en la consola ni en el monitor. Todas las depuraciones se escriben en el disco duro del ASR. Las depuraciones se escriben en el disco duro debajo de la carpeta **tracelogs** con el nombre **cpp_cp_F0-0.log.<date>**. Para ver el archivo donde se escriben las depuraciones, utilice el resultado:

```
ASR# cd harddisk:
ASR# cd tracelogs
ASR# dir cpp_cp_F0*Directory of harddisk:/tracelogs/cpp_cp_F0*

Directory of harddisk:/tracelogs/

3751962 -rwx 1048795 Jun 15 2010 06:31:51 +00:00
cpp_cp_F0-0.log.5375.20100615063151
```

```
3751967 -rwx 1048887 Jun 15 2010 02:18:07 +00:00
cpp_cp_F0-0.log.5375.20100615021807
39313059840 bytes total (30680653824 bytes free)
```

Cada archivo de depuración se almacenará como un archivo **cpp_cp_F0-0.log.<date>**. Estos son archivos de texto normales que se pueden copiar del ASR con TFTP. El máximo del archivo de registro en el ASR es de 1 Mb. Después de 1Mb, las depuraciones se escriben en un nuevo archivo de registro. Es por eso que cada archivo de registro se marca con el tiempo para indicar el inicio del archivo.

Los archivos de registro pueden existir en estas ubicaciones:

```
harddisk:/tracelogs/
bootflash:/tracelogs/
```

Dado que los archivos de registro sólo se muestran después de rotar, el archivo de registro se puede rotar manualmente con este comando:

```
ASR# test platform software trace slot f0 cpp-control-process rotate
```

Esto crea inmediatamente un archivo de registro "cpp_cp" e inicia uno nuevo en el QFP. Por ejemplo:

```
ASR#test platform software trace slot f0 cpp-control-process rotate
 Rotated file from: /tmp/fp/trace/stage/cpp_cp_F0-0.log.7311.20140408134406,
Bytes: 82407, Messages: 431

ASR#more tracelogs/cpp_cp_F0-0.log.7311.20140408134406
04/02 10:22:54.462 : btrace continued for process ID 7311 with 159 modules
04/07 16:52:41.164 [cpp-dp-fw]: (info): QFP:0.0 Thread:110 TS:00000531990811543397
:FW_DEBUG_FLG_HA:[]: HA[1]: Changing HA state to 9
04/07 16:55:23.503 [cpp-dp-fw]: (info): QFP:0.0 Thread:120 TS:00000532153153672298
:FW_DEBUG_FLG_HA:[]: HA[1]: Changing HA state to 10
04/07 16:55:23.617 [buginf]: (debug): [system] Svr HA bulk sync CPP(0) complex(0)
epoch(0) trans_id(26214421) rg_num(1)
```

Este comando permite que los archivos de depuración se combinen en un solo archivo para facilitar el procesamiento. Combina todos los archivos del directorio y los entrelaza en función del tiempo. Esto puede ayudar cuando los registros son muy detallados y se crean en varios archivos:

```
ASR#request platform software trace slot rp active merge target bootflash:MERGED_OUTPUT.log
Creating the merged trace file: [bootflash:MERGED_OUTPUT.log]
 including all messages

Done with creation of the merged trace file: [bootflash:MERGED_OUTPUT.log]
```