ZBFW para la guía del Troubleshooting de la configuración IOS-XE

Contenido

Introducción

Este documento describe cómo el mejor Troubleshooting que la característica basada zona del Firewall (ZBFW) en la agregación mantiene al router (ASR) 1000, con los comandos que se utilizan para sondear a los contadores de caídas del hardware en el ASR. El ASR1000 es una plataforma basado en hardware de la expedición. La configuración del software del ® del Cisco IOS XE programa el ASIC de hardware (procesador del flujo del quántum (QFP) para realizar las funciones de la expedición de la característica. Esto permite el más alto rendimiento y el mejor rendimiento. La desventaja a esto es que presenta un mayor desafío para resolver problemas. Los comandos cisco ios tradicionales usados para sondear las sesiones en curso y a los contadores de caídas vía el Firewall Zona-basado (ZBFW) son no más tan válidos que los descensos son no más en el software.

Links y documentación

Referencias de Comando

- Referencias de comandos del Routers de servicios de agregación Cisco ASR de la serie 1000
- Referencias de comandos del Cisco IOS XE 3S

Pasos del Troubleshooting de Datapath

Para resolver problemas el datapath, usted debe identificar si el tráfico está pasado correctamente con el ASR y el código del Cisco IOS XE. El específico a las características de firewall, el troubleshooting del datapath sigue los siguientes pasos:

1. **Verifique la configuración** - Recolecte la configuración y examine la salida para verificar la conexión.

2. **Verifique al estado de la conexión** - Si el tráfico pasa correctamente, el Cisco IOS XE abre una conexión en la característica ZBFW. Esta conexión sigue el tráfico y la información del estado entre un cliente y servidor.

3. **Verifique a los contadores de caídas** - Cuando el tráfico no pasa correctamente, el Cisco IOS XE registra a un contador de caídas para cualquier paquete perdidos. Marque esta salida para aislar la causa del error del tráfico.

4. **Registración** - Syslog del frunce para proporcionar una información más granular sobre las estructuras y las caídas de paquetes de la conexión.

5. **Paquetes perdidos de la traza del paquete** - Utilice el seguimiento del paquete para coger los paquetes perdidos.

6. **Debugs** - Los debugs del frunce son la mayoría de la opción detallada. Los debugs se pueden obtener condicional para confirmar el trayecto de reenvío exacto para los paquetes.

Verifique la configuración

La salida del **Firewall del soporte técnico de la demostración** 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> --------
```

Verifique al estado de la conexión

La información de conexión puede ser obtenida de modo que todas las conexiones en ZBFW sean mencionadas. 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: Sea consciente que si usted funciona con este comando, tardará un tiempo prolongado si hay porciones de conexiones en el dispositivo. Cisco recomienda que usted funciona con este comando con los filtros específicos según lo delineado aquí.

La tabla de conexiones se puede filtrar abajo a una dirección de origen o de destino específica. Utilice los filtros después del submode de la **plataforma**. Las opciones a 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>
```

Se visualiza esta tabla de conexiones es tan solamente conexiones filtradas originadas de 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 conexiones, la información de conexión detallada se puede obtener para un anlaysis más completo. Para visualizar esta salida, utilice la palabra clave del **detalle**.

```
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
```

Marque a los contadores de caídas del Firewall

La salida del contador de caídas cambiada durante XE 3.9. Antes de XE 3.9, las razones del descenso del Firewall eran muy genéricas. Después de XE 3.9, las razones del descenso del Firewall fueron ampliadas para llegar a ser más granulares.

Para verificar a los contadores de caídas, realice dos pasos:

1. Confirme a los contadores de caídas globales en el Cisco IOS XE. Estos contadores muestran qué característica ha caído el tráfico. Los ejemplos de las características incluyen el Calidad de Servicio (QoS), Network Address Translation (NAT), Firewall, y así sucesivamente.

2. Una vez que se ha identificado el subfeature, pregunte a los contadores de caídas granulares ofrecidos por el subfeature. En esta guía, el subfeature que es analizado es la característica de firewall.

Contadores de caídas globales en QFP

El comando básico de confiar encendido proporciona todos los descensos a través del QFP:

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

Este comando le muestra los descensos genéricos global a través del QFP. Estos descensos pueden estar en cualquier característica. Algunas características del ejemplo son:

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

Para ver todos los descensos, incluya los contadores que tienen un valor de cero, utilizan el comando:

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

Para borrar los contadores, utilice este comando. Borra la salida después de mostrarla a la pantalla. Este comando está claro en leído, así que la salida se reajusta a cero **después de que** se visualice a la pantalla.

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

Abajo está una lista de contadores de caídas y de explicación globales del Firewall QFP:

Razón global del descenso del Firewall	Explicación
FirewallBackpressure	Caída de paquetes debido al backpressure registrando el mecanismo.
FirewallInvalidZone	Ninguna zona de Seguridad configurada para la interfaz.
FirewallL4Insp	Error del control de la directiva L4. Vea la tabla abajo por razones más

	granulares del descenso (razones del descenso de la característica de firewall).
FirewallNoForwardingZone	El Firewall es uninitialized, y no se permite ningún tráfico pasar.
FirewallNonsession	La creación de sesión falla. Podría ser debido a la sesión máxima que el límit ha alcanzado o falla de asignación de memoria.
FirewallPolicy	Las políticas del firewall configuradas son descenso.
FirewallL4	Error del examen L4. Vea la tabla abajo por razones más granulares del descenso (el descenso de la característica de firewall razona).
FirewallL7	Caída de paquetes debido al examen L7. Vea abajo para una lista de razones más granulares del descenso L7 (el descenso de la característica de firewall razona).
FirewallNotInitiator	No un iniciador de la sesión para el TCP, el UDP, o el ICMP. No se crea ninguna sesión. Por ejemplo, porque ICMP el primer paquete recibido no es GENERACIÓN DE ECO o GRUPO FECHA/HORA. Para el TCP, no es un SYN.
FirewallNoNewSession	Esto podía suceder en el paquete normal que procesaba o que procesaba impreciso del canal. La Alta disponibilidad del Firewall no permite las nuevas sesiones.
FirewallSyncookieMaxDst	Para proporcionar la protección contra inundación SYN basada en el host, ha una tarifa del por destino SYN como límite de la inundación SYN. Cuando el número de entradas de destino alcanza el límite, se caen los nuevos paquete SYN.
FirewallSyncookie	Se acciona la lógica SYNCOOLIE. Esto indica que el SYN/ACK con el Cookie SYN fue enviado, y el paquete SYN original está caído.
FirewallARStandby	El Asymmetric Routing no se habilita y el grupo de redundancia no está en e estado activo.

Contadores de caídas de la característica de firewall en QFP

La limitación con el contador de caídas global QFP es que no hay granularity en las razones del descenso, y algunas de las razones del descenso tales como **FirewallL4** consiguen sobrecargadas tan a la punta que son de poco uso para resolver problemas. Esto se ha aumentado desde entonces en el Cisco IOS XE 3.9 (15.3(2)S), donde agregaron a los contadores de caídas de la característica de firewall. Esto da un conjunto mucho más granular de las razones del descenso:

```
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
....
```

Abajo está una lista de razones y de explicaciones del descenso de la característica de firewall:

Razón del descenso de la característica de firewall	Explicación
Longitud del encabezado inválida	El datagrama es tan pequeño que no podría contener la capa 4TCP,UDP, o encabezad ICMP. Podría ser causado por: 1. Longitud de encabezado TCP < 20

	2. Longitud del encabezado UDP/ICMP < 8
Extensión de datos inválida UDP	La longitud del datagrama de UDP no hace juego la longitud especificada en el encabe UDP.
Número inválido ACK	Este descenso se podía causar por una de estas razones: 1. Los iguales ACK no al next_seq# del TCP miran. 2. El ACK es mayor que el SEQ# más reciente enviado por el par TCP. En el estado TCP SYNSENT y SYNRCVD, se espera que el ACK# sea igual a ISN+1 pe es.
Indicador inválido ACK	Este descenso se podía causar por una de estas razones: 1. Contando con el indicador ACK pero no fijado en diverso estado TCP. 2. Con excepción del indicador ACK, el otro indicador (como el RST) también se fija.
Iniciador inválido TCP	Esto sucede cuando: 1. El primer paquete de un iniciador TCP no es un SYN (el segmento NON-inicial TC recibe sin una sesión válida). 2. El paquete SYN inicial tiene el indicador ACK fijado.
SYN con los datos	El paquete SYN contiene el payload. Esto no se soporta.
Indicadores inválidos TCP	Los indicadores inválidos TCP se pueden causar por: 1. El paquete SYN de la inicial TCP tiene indicadores con excepción del SYN. 2. En el TCP escucha el estado, un par TCP recibe un RST o un ACK. 3. El paquete del otro respondedor se recibe antes del SYN/ACK. 4. El SYN/ACK previsto no se recibe del respondedor.
Segmento inválido en el estado SYNSENT	Un segmento inválido TCP en el estado SYNSENT se causa por: 1. El SYN/ACK tiene payload. 2. El SYN/ACK tiene otros indicadores (PSH, URG, FIN) fijados. 3. Reciba un transitar SYN con el payload. 4. Reciba un paquete NON-SYN del iniciador.
Segmento inválido en el estado SYNRCVD	Un segmento inválido TCP en el estado SYNRCVD se podía causar por: 1. Reciba un retransit SYN con el payload del iniciador. 2. Reciba un segmento inválido que no sea SYN/ACK, RST, o FIN del respondedor.
SEQ inválido	Esto ocurre en el estado SYNRCVD cuando los segmentos vienen del iniciador. Se cau por: 1. Seq# es menos que el ISN. 2. Si el tamaño de la ventana del rcvd del receptor es 0 y: El segmento tiene payload, o Segmento fuera de servicio (el seq# es mayor que el receptor LASTACK. 3. Si el tamaño de la ventana del rcvd del receptor es 0 y el seq# cae más allá de la ventana. 4. Iguales de Seq# al ISN pero no a un paquete SYN.
Opción inválida de la escala de la ventana	La opción inválida de la escala de la ventana TCP es causada por la longitud incorrecta byte de opción de la escala de la ventana.
TCP fuera de la ventana	El paquete es demasiado viejo - una ventana detrás del otro ACK del lado. Esto podía suceder en el estado ESTABLECIDO, CLOSEWAIT y LASTACK.
Payload adicional TCP después del FIN	Payload recibido después del FIN enviado. Esto podía suceder en el estado CLOSEWA

enviado	
Desbordamiento de la ventana TCP	Esto ocurre cuando la ventana del segmento del tamaño del receptor entrante de los desbordamientos. Sin embargo, si se habilita el vTCP, se permite esta condición porque Firewall necesita mitigar el segmento para que ALG consuma más adelante.
Retran con los indicadores inválidos	Un paquete retransmitido fue reconocido ya por el receptor.
Segmento fuera de servicio TCP	El paquete defectuoso está a punto de ser entregado al L7 para el examen. Si el L7 no permite el segmento OOO, este paquete será caído.
Inundación SYN	Bajo ataque de inundación SYN TCP. Bajo ciertas condiciones cuando las conexiones actuales a este host exceden el valor medio abierto configurado el Firewall rechazará cualquier nueva conexión a esta dirección IP por un período de tiempo. Como consecue los paquetes serán caídos.
Interno yerra - el alloc del control del synflood fallado	Durante el control del synflood, la asignación del hostdb falla. Acción recomendada: marque “la memoria activa del Firewall de la característica del qfp hardware de plataforma de la demostración” para marcar el estatus de la memoria.
Descenso del apagón de Synflood	Si se exceden las conexiones entreabiertas configuradas y tiempo se configura del apag toda la nueva conexión a esta dirección IP se cae.
El límite de sesión medio abierto se excede	El paquete cayó debido a las sesiones semiabiertas permitidas excedidas. También marque las configuraciones del “max-incomplete alto-bajo” y el “minuto alto-ba aseegurarse # de las sesiones semiabiertas no está siendo estrangulado por estas configuraciones.
Demasiado Pkt por el flujo	El número máximo de paquetes inspectable permitidos por el flujo se excede. El Númer máximo es 25.
Demasiados paquetes del error ICMP por el flujo	El número máximo de paquetes del error ICMP permitidos por el flujo se excede. El núm máximo es 3.
Unexpect carga útil de TCP de Rsp al init	En el estado SYNRCVD, el TCP recibe un paquete con el payload del respondedor a la dirección del iniciador.
Error interno - Dirección indefinida	Dirección del paquete indefinida.
SYN dentro de la ventana actual	Un paquete SYN se ve dentro de la ventana de una conexión TCP ya establecida.
RST dentro de la ventana actual	Un paquete RST se observa dentro de la ventana de una conexión TCP ya establecida.
Segmento perdido	Se recibe un segmento TCP que no se debe haber recibido a través de la máquina de e TCP tal como paquete TCP Syn que es recibido en el estado del escuchar del responde
Error interno ICMP - Información NAT faltada ICMP	Los paquetes icmp nat'ed pero la información NAT interna falta. Esto es un error interno
Paquetes icmp en el estado SCB cercano	Recibió los paquetes icmp en el estado SCB CERCANO.
Encabezado IP	Encabezado IP que falta en los paquetes icmp.

faltado en los paquetes icmp	
Error ICMP ningún IP o ICMP	Paquete del error ICMP sin el IP o el ICMP en el payload. Causado probablemente por u paquete mal formado o un ataque.
El ICMP yerra Pkt demasiado corto	El paquete del error ICMP es demasiado corto.
El ICMP yerra excede el límite de la explosión	El pkt del error ICMP excede el límite de la explosión de 10.
El ICMP yerra inalcanzable	El pkt del error ICMP inalcanzable excede el límite. Solamente el 1r paquete inalcanzab permite pasar a través.
El ICMP yerra Seq# inválido	Seq# del paquete integrado no hace juego el seq# del paquete que origina el error ICMI
El ICMP yerra Ack inválido	ACK inválido en el paquete integrado error ICMP.
Descenso de la acción ICMP	La acción configurada ICMP es descenso.
Zona-pares sin el directiva-mapa	Directiva no presente en los zona-pares. podría ser debido a ALG (gateway de capa de aplicación) que no era configurado para abrir el agujerito para el canal de datos de aplicación, o ALG no abrió el agujerito correctamente, o no hay agujerito abierto debido problemas de ampliación.
Sesión faltada y directiva no presente	Las operaciones de búsqueda de la sesión fallaron y no hay directiva presente examina paquete.
Error ICMP y directiva no presentes	Error ICMP sin la directiva configurada en los zona-pares.
Clasificación fallada	Incidente de la clasificación en un par dado de la zona cuando el Firewall intenta determ si el protocolo es inspectable.
Descenso de la acción de la clasificación	La acción de la clasificación es descenso.
Política de seguridad Misconfig	Clasificación fallada debido al misconfiguration de la política de seguridad. Esto podía también ser debido a ningún pinpole para el canal de datos L7.
Envíe el RST al respondedor	Envíe el RST al respondedor en el estado SYNSENT cuando ACK# no es igual a ISN+1
Descenso de las políticas del firewall	La acción de política es caer.
Descenso del fragmento	Caiga los fragmentos restantes cuando se cae el primer fragmento.
Descenso de la directiva ICMP Firwall	La acción de política del paquete integrado ICMP es DESCENSO.
El examen L7 vuelve el DESCENSO	El L7 (ALG) decide a caer el paquete. La razón se podía encontrar de diversas estadísti ALG.
Pkt del segmento L7 no	Paquete dividido en segmentos recibido cuando ALG no lo honra.

permitir Pkt del fragmento L7 no (O VFR)	paquetes hechos fragmentos recibidos cuando ALG no lo honra.
permitir Tipo Proto desconocido L7	Tipo de protocolo desconocido.

Descensos del Firewall del Troubleshooting

Una vez que la razón del descenso se identifica de los contadores de caídas globales o de la característica de firewall antedichos, los pasos de Troubleshooting adicional pudieron ser necesarios si estos descensos son inesperados. Aparte de la validación de la configuración para asegurar la configuración está correcto para las funciones del Firewall habilitadas, se requiere a menudo para tomar a las capturas de paquetes para el flujo de tráfico en la pregunta para ver si los paquetes son malformados o si hay algunos problemas de la aplicación de protocolo o de la aplicación.

Registro

Las funciones del registro ASR generan los Syslog para registrar los paquetes perdidos. Estos Syslog proporcionan más detalles en porqué el paquete fue caído. Hay dos tipos de sysloggings:

1. Syslogging mitigado Local

2. Registro de alta velocidad remoto

Syslogging mitigado Local

Para aislar la causa de los descensos, usted puede utilizar el troubleshooting genérico ZBFW, tal como habilitar los descensos del registro. Hay dos maneras de configurar el registro de la caída de paquetes.

Método 1: Utilice el parámetro-mapa examinar-global para registrar todos los paquetes perdidos.

```
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
....
```

Método 2: La aduana del uso examina el parámetro-mapa para registrar los paquetes perdidos para solamente la 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 dependiendo de cómo el ASR se configura para registrar. Aquí está un ejemplo de un mensaje del registro del descenso.

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

Limitaciones del syslogging mitigado Local

1. Estos registros son tarifa limitada según el Id. de bug Cisco CSCud09943.

2. Estos registros no pudieron imprimir a menos que la configuración específica sea aplicada. Por ejemplo, los paquetes caídos por los paquetes del class-default no serán registrados a menos que se especifique la palabra clave del **registro**:

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

Registro de alta velocidad remoto

El registro de alta velocidad (HSL) genera los Syslog directamente del QFP y los envía al colector configurado del Netflow HSL. Ésta es la solución de registración recomendada para ZBFW en el ASR.

Para el HSL, utilice esta configuración:

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

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

Guía de configuración: Firewall Zona-basado de la directiva, registro de alta velocidad del Firewall de la versión 3S (ASR 1000) del Cisco IOS XE

Seguimiento del paquete usando corresponder con condicional

Gire los debugs condicionales para habilitar el seguimiento del paquete y después habilitar el seguimiento del paquete para estas características:

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

> Nota: La condición de la coincidencia puede utilizar la dirección IP directamente, pues un ACL no es necesario. Esto hará juego como la fuente o destino que permiten las trazas bidireccionales. Este método puede ser utilizado si a le no se permite alterar la configuración. Por ejemplo: direccionamiento 192.168.1.1/32 de la condición ipv4 de la plataforma del debug.

Gire la característica del paquete-seguimiento:

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

Hay dos maneras de utilizar esta característica:

1. Ingrese el comando del **descenso de la traza del paquete de la plataforma del debug** para localizar solamente los paquetes perdidos.

2. La exclusión del **descenso de la traza del paquete de la plataforma del** comando debug localizará cualquier paquete que haga juego la condición, que incluye unos que sean examinadas/pasadas por el dispositivo.

Gire los debugs condicionales:

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

Funcione con la prueba, después apague los debugs:

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

Ahora la información se puede visualizar a la pantalla. En este ejemplo, los paquetes icmp eran caído debido a las políticas del 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 <num> del paquete de la traza del paquete de la plataforma de la demostración decodifica el comando decodifica la información y el contenido de encabezado de paquete. Esta característica fue introducida 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

El soporte integrado de la captura de paquetes se ha agregado en el Cisco IOS XE 3.7 (15.2(4)S). Para más detalles, vea

Captura de paquetes integrada para el Cisco IOS y el ejemplo de configuración IOS-XE.

Depuraciones

Debugs condicionales

En XE3.10, los debugs condicionales serán introducidos. Las declaraciones condicionales se pueden utilizar para asegurar los mensajes del debug de los registros de la característica ZBFW solamente que son relevantes a la condición. Los debugs condicionales utilizan los ACL para restringir los registros que hacen juego los elementos ACL. También, antes de XE3.10, los mensajes del debug eran más difíciles de leer. Mejoraron a la salida de los debugs en XE3.10 para hacerlo más fácil entender.

Para habilitar estos debugs, publique este comando:

```
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
```

Note que el comando condition debe ser fijado vía un ACL y una direccionalidad. Los debugs condicionales no serán implementados hasta ellos se comienzan con el **comienzo de la condición**

de la plataforma del comando debug. Para apagar los debugs condicionales utilizan la parada de la condición de la plataforma del comando debug.

```
debug platform condition stop
```

Para apagar los debugs condicionales, no utilice el comando undebug all. Para apagar todos los debugs condicionales, utilice el comando:

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

Antes de XE3.14, los debugs ha y del evento no son condicionales. Como consecuencia, el submode todo del dataplane fw de la característica de la condición de la plataforma del comando debug hace todos los registros ser creado, independiente de la condición seleccionada abajo. Esto podría crear el ruido adicional que hace hacer el debug de difícil.

Por abandono, el nivel de registro condicional es información. Para aumentar/disminuya el nivel de registro, utilizan el comando:

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

Recolecte y vea los debugs

Los archivos del debug no imprimirán a la consola o al monitor. Todos los debugs se escriben al disco duro del ASR. Los debugs se escriben al disco duro bajo tracelogs de la carpeta con el nombre cpp_cp_F0-0.log.<date>. Para ver el archivo donde se escriben los debugs, utilice la salida:

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

Cada archivo del debug será salvado como archivo cpp_cp_F0-0.log.<date>. Éstos son los archivos de texto regulares que se pueden copiar del ASR con el TFTP. El máximo del archivo del registro en el ASR es 1Mb. Después de 1Mb, los debugs se escriben a un nuevo archivo del registro. Por eso cada archivo del registro es con impresión horaria para indicar el comienzo del archivo.

Los archivos del registro pudieron existir en estas ubicaciones:

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

Puesto que los archivos del registro se visualizan solamente después de que se giren, el archivo del registro se puede girar manualmente con este comando:

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

Esto crea inmediatamente un archivo del registro del “cpp_cp” y comienza un 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 del debug sean combinados en un archivo único para un

proceso más fácil. Combina todos los archivos en el directorio y los entrelaza basó el tiempo. Esto puede ayudar cuando los registros son muy prolijos y se crean a través de los Archivos múltiples:

```
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]
```