Característica de la traza del paquete IOS-XE Datapath

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Topología de la referencia
El localizar del paquete funcionando
Guía de inicio rápido
Debugs condicionales de la plataforma del permiso
Traza del paquete del permiso
Limitación de la condición de la salida con las trazas del paquete
Visualice los resultados de la traza del paquete
Traza FIA
Visualice los resultados de la traza del paquete
Marque el FIA asociado a una interfaz
Vacie los paquetes localizados
Caiga la traza
Escenario de la traza del descenso del ejemplo
Inyecte y lleve en batea las trazas
Ejemplos de la traza del paquete
Ejemplo de la traza del paquete - NAT
Ejemplo de la traza del paquete - VPN
Impacto en el rendimiento
Información Relacionada

Introducción

Este documento describe cómo realizar el seguimiento del paquete del datapath para el ® del Cisco IOS - software XE vía la característica de la traza del paquete.

Para identificar los problemas tales como misconfiguration, sobrecarga de la capacidad, o aún el bug de software ordinario mientras que resuelve problemas, es necesario entender qué sucede a un paquete dentro de un sistema. La característica de la traza del paquete del Cisco IOS XE dirige esta necesidad. Proporciona un método campo-seguro que se utilice para considerar y para capturar los detalles de proceso por paquete basados en una clase de condiciones definidas por el usario.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de la característica de la traza del paquete que está disponible en las versiones 3.10 del Cisco IOS XE y posterior, así como en todas las Plataformas que funcionen con el Software Cisco IOS XE, tal como el Routers de los servicios de la agregación de las Cisco 1000 Series (ASR1K), las Cisco 1000V Series se nublan el router de los servicios (CSR1000v), y al router de los Servicios integrados de las Cisco 4451-X Series (ISR4451-X).

Componentes Utilizados

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

- Versión 3.10S (15.3(3)S) del Software Cisco IOS XE y posterior
- ASR1K

La información de este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, aseegurese le entender el impacto potencial del comando any usado.

Refiérase a la topología

Este diagrama ilustra la topología que se utiliza para los ejemplos que se describen en este documento:

El localizar del paquete funcionando

Para ilustrar el uso de la característica de la traza del paquete, el ejemplo que se utiliza en esta sección describe una traza del tráfico del Internet Control Message Protocol (ICMP) de la estación de trabajo local 172.16.10.2 (detrás del ASR1K) al host remoto 172.16.20.2 (la dirección de ingreso para el ASR1K en la interfaz Gig0/0/1).

Usted puede localizar los paquetes en el ASR1K con estos dos pasos:

1. Permita a los debugs condicionales de la plataforma para seleccionar los paquetes o traficar que usted quiere localizar en el ASR1K.

2. Habilite la traza del paquete de la plataforma (traza del trayecto o traza del arsenal de la llamada de la característica (FIA)).

Guía de inicio rápido

Aquí está una guía de inicio rápido si usted es ya familiar con el contenido de este documento, y

quiere una sección para un panorama general en el CLI. Éstos son solamente algunos ejemplos para ilustrar el uso de la herramienta. Refiera a las secciones posteriores que discuten los sintaxis detalladamente, y asegúrele el uso la configuración que es apropiada a su requisito.

1. Configure las condiciones de la plataforma:

```
debug platform condition ipv4 10.0.0.1/32 both --> matches in and out packets with source
or destination as 10.0.0.1/32

debug platform condition ipv4 access-list 198 egress --> (Ensure access-list 198 is
defined prior to configuring this command) - matches egress packets corresponding
to access-list 198

debug platform condition interface gig 0/0/0 ingress  --> matches all ingress packets
on interface gig 0/0/0

debug platform condition mpls 10 1 ingress --> matches MPLS packets with top ingress
label 10

debug platform condition ingress --> matches all ingress packets on all interfaces
(use cautiously)
```

   Después de que se configure una condición de la plataforma, comience las condiciones de la plataforma con este comando CLI:

```
debug platform condition start
```

2. Traza del paquete de la configuración:

```
debug platform packet-trace packet 1024  -> basic path-trace, and automatically stops
tracing packets after 1024 packets. You can use "circular" option if needed debug platform
packet-trace packet 1024 fia-trace -> enables detailed fia trace, stops
tracing packets after 1024 packets debug platform packet-trace drop [code <dropcode>]  ->
if you want to trace/capture only
packets that are dropped. Refer to Drop Trace section for more details.
```

   Note: En versiones anteriores del Cisco IOS XE 3.x, el permiso de la traza del paquete de la plataforma del comando debug también se requiere para comenzar la característica de la traza del paquete. Esto se requiere no más en las versiones del Cisco IOS XE 16.x.

Ingrese este comando para borrar el búfer de traza y reajustar la traza del paquete:

```
clear platform packet-trace statistics  --> clear the packet trace buffer
```

El comando de borrar la plataforma condiciona y la configuración de la traza del paquete es:

```
clear platform condition all  --> clears both platform conditions and the packet trace
configuration
```

Comandos show

Verifique la condición de la plataforma y la configuración de la traza del paquete después de que usted aplique los comandos anteriores para asegurarle tiene lo que usted necesita.

```
show platform conditions --> shows the platform conditions configured

show platform packet-trace configuration --> shows the packet-trace configurations

show debugging --> this will show both platform conditions and platform packet-trace configured
```

Aquí están los comandos de marcar los paquetes localizados/capturados:

```
show platform packet-trace statistics --> statistics of packets traced

show platform packet-trace summary  --> summary of all the packets traced, with input and
output interfaces, processing result and reason. show platform packet-trace packet 12 -> Tracing
the 12th packet, with complete path trace
or FIA trace details.
```

Debugs condicionales de la plataforma del permiso

La característica de la traza del paquete confía en la infraestructura condicional del debug para determinar los paquetes que se localizarán. La infraestructura condicional del debug proporciona la capacidad al filtrar tráfico basado encendido:

- Protocolo
- Dirección IP y máscara
- Lista de control de acceso (ACL)
- Interfaz
- Dirección del tráfico (ingreso o salida)

Estas condiciones definen donde y cuando los filtros se aplican a un paquete.

Para el tráfico que se utiliza en este ejemplo, habilite los debugs condicionales de la plataforma en la dirección de ingreso para los paquetes icmp de 172.16.10.2 a 172.16.20.2. Es decir seleccione el tráfico que usted quiere localizar. Hay las diversas opciones que usted puede utilizar para seleccionar este tráfico.

```
ASR1000#debug platform condition ?
egress Egress only debug
feature For a specific feature
ingress Ingress only debug
interface Set interface for conditional debug
ipv4 Debug IPv4 conditions
ipv6 Debug IPv6 conditions
start Start conditional debug
stop Stop conditional debug
```

En este ejemplo, una lista de acceso se utiliza para definir la condición, como se muestra aquí:

```
ASR1000#show access-list 150
Extended IP access list 150
10 permit icmp host 172.16.10.2 host 172.16.20.2
ASR1000#debug platform condition interface gig 0/0/1 ipv4
 access-list 150 ingress
```

Para comenzar el debugging condicional, ingrese este comando:

```
ASR1000#debug platform condition start
```

Note: Para parar o inhabilitar la infraestructura del debugging condicional, ingrese el

comando stop de la condición de la plataforma del debug.

Para ver los filtros condicionales del debug se configuran que, ingrese este comando:

```
ASR1000#show platform conditions

Conditional Debug Global State: Start
Conditions Direction
------------------------------------------------------------------|---------
GigabitEthernet0/0/1 & IPV4 ACL [150] ingress

Feature Condition Format Value
----------------------|----------------------|-------------------------------

ASR1000#
```

En resumen, esta configuración se ha aplicado hasta el momento:

```
access-list 150 permit icmp host 172.16.10.2 host 172.16.20.2
debug platform condition interface gig 0/0/1 ipv4 access-list 150 ingress
debug platform condition start
```

Traza del paquete del permiso

> Note: Esta sección describe el paquete y las opciones Copy (Copiar) detalladamente, y las otras opciones se describen más adelante en el documento.

Las trazas del paquete se soportan en la comprobación y las interfaces lógicas, tales como túnel o interfaces de acceso virtual.

Aquí está la sintaxis CLI de la traza del paquete:

```
ASR1000#debug platform packet-trace ?
copy Copy packet data
drop Trace drops only
inject Trace injects only
packet Packet count
punt Trace punts only

debug platform packet-trace packet <pkt-size/pkt-num> [fia-trace | summary-only]
 [circular] [data-size <data-size>]
```

Aquí están las descripciones para las palabras claves de este comando:

- Pkt-numérico - El número del paquete especifica la cantidad máxima de paquete que se mantiene al mismo tiempo.
- sumario solamente - Esto especifica que solamente los datos de resumen están capturados. El valor por defecto es capturar los datos de resumen y los datos del trayecto de función.
- FIA-traza - Esto realiza opcionalmente una traza FIA además de la información de datos de trayecto.

- **tamaño de los datos** - Esto permite que usted especifique el tamaño del buffer de datos de trayecto, a partir 2,048 a 16,384 bytes. El valor por defecto es **2,048** bytes.

```
debug platform packet-trace copy packet {in | out | both} [L2 | L3 | L4]
 [size <num-bytes>]
```

Aquí están las descripciones para las palabras claves de este comando:

- **in/out** - Esto especifica la dirección del flujo de paquetes que se copiará - ingreso y/o salida.
- **L2/L3/L4** - Esto permite que usted especifique la ubicación que la copia del paquete comienza. La capa 2 (L2) es la ubicación predeterminada.
- **tamaño** - Esto permite que usted especifique al número máximo de octetos se copien que. El valor por defecto es 64 octetos.

Por este ejemplo, éste es el comando usado para habilitar la traza del paquete para el tráfico que se selecciona con la infraestructura condicional del debug:

```
ASR1000#debug platform packet-trace packet 16
```

Para revisar la configuración de la traza del paquete, ingrese este comando:

```
ASR1000#show platform packet-trace configuration
debug platform packet-trace packet 16 data-size 2048
```

Usted puede también ingresar el **comando show debugging** para ver los debugs condicionales de la plataforma y las configuraciones de la traza del paquete:

```
ASR1000# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Start

Conditions
Direction
------------------------------------------------------------------|---------
GigabitEthernet0/0/1 & IPV4 ACL [150] ingress
...
IOSXE Packet Tracing Configs:

Feature Condition Format Value
----------------------|----------------------|--------------------------------

Feature Type Submode Level
-------|--------------|---------------------------------------------|----------

IOSXE Packet Tracing Configs:
debug platform packet-trace packet 16 data-size 2048
```

> **Note**: Ingrese el **comando all claro de la condición de la plataforma** para borrar todas las condiciones del debug de la plataforma y las configuraciones y los datos de la traza del paquete.

En resumen, estos datos de configuración se han utilizado hasta el momento para habilitar la

traza del paquete:

```
debug platform packet-trace packet 16
```

Limitación de la condición de la salida con las trazas del paquete

Las condiciones definen los filtros condicionales y cuando se aplican a un paquete. Por ejemplo, la **salida de la interfaz g0/0/0 de la condición de la plataforma del debug** significa que un paquete está identificado como coincidencia cuando alcanza la salida FIA en la interfaz g0/0/0, tan cualquier proceso del paquete que ocurra del ingreso hasta que se falte esa punta.

> **Note**: El cisco altamente recomienda que usted utiliza las condiciones del ingreso para las trazas del paquete para conseguir la mayoría los datos a completos y significativos posibles. Las condiciones de la salida se pueden utilizar, pero sean conscientes de las limitaciones.

Visualice los resultados de la traza del paquete

> **Note**: Esta sección asume que la traza del trayecto está habilitada.

Tres niveles específicos de examen son proporcionados por la traza del paquete:

- Contabilidad
- Resumen por paquete
- Datos de trayecto por paquete

Cuando cinco paquetes de pedidos ICMP se envían de 172.16.10.2 a 172.16.20.2, estos comandos se pueden utilizar para ver los resultados de la traza del paquete:

```
ASR1000#show platform packet-trace statistics
Packets Traced: 5
Ingress 5
Inject 0
Forward 5
Punt 0
Drop 0
Consume 0

ASR1000#show platform packet-trace summary
Pkt   Input            Output           State  Reason
0     Gi0/0/1          Gi0/0/0          FWD
1 Gi0/0/1 Gi0/0/0 FWD
2 Gi0/0/1 Gi0/0/0 FWD
3 Gi0/0/1 Gi0/0/0 FWD
4 Gi0/0/1 Gi0/0/0 FWD

ASR1000#show platform packet-trace packet 0

Packet: 0           CBUG ID: 4
Summary
Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0
State : FWD
Timestamp
   Start   : 1819281992118 ns (05/17/2014 06:42:01.207240 UTC)
```

```
   Stop    : 1819282095121 ns (05/17/2014 06:42:01.207343 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.20.2
Protocol : 1 (ICMP)

ASR1000#
```

> **Note**: El tercer comando proporciona un ejemplo que ilustre cómo ver la traza del paquete para cada paquete. En este ejemplo, el primer paquete localizado se muestra.

De estas salidas, usted puede ver que cinco paquetes están localizados y que usted puede ver la interfaz de entrada, la interfaz de salida, el estado, y la traza del trayecto.

Estado	Observación
FWD	El paquete se programa/se hace cola para la salida, para ser remitido al salto siguiente vía u interfaz de egreso.
BATEA	El paquete se lleva en batea del Forwarding Processor (FP) al (RP) del Route Processor (av del control).
DESCENSO	El paquete se cae en el FP. Ejecute la traza FIA, utilice a los contadores de caídas globales datapath del uso hace el debug de para encontrar más detalles por las razones del descens
CONS	El paquete se consume durante un proceso del paquete, por ejemplo durante la petición del de ICMP o los paquetes crypto.

El ingreso e **inyecta los** contadores en las estadísticas de la traza del paquete que la salida corresponde a los paquetes que ingresan vía una interfaz externa y los paquetes que se consideren según lo inyectado del avión del control, respectivamente.

Traza FIA

El FIA lleva a cabo la lista de características que sean ejecutadas secuencialmente por los procesadores Engine del paquete (PPE) en el procesador del flujo de Quantum (QFP) cuando un paquete se remite el ingreso o la salida. Las características se basan en los datos de configuración que se aplican en la máquina. Así, una traza FIA ayuda a entender el flujo del paquete a través del sistema mientras que se procesa el paquete.

Usted debe aplicar estos datos de configuración para habilitar la traza del paquete con el FIA:

```
ASR1000#debug platform packet-trace packet 16 fia-trace
```

Visualice los resultados de la traza del paquete

> **Note**: Esta sección asume que la traza FIA está habilitada. También, cuando usted agrega o modifica los comandos trace del paquete actual, se borran los detalles mitigados de la traza del paquete, así que usted debe enviar un cierto tráfico otra vez de modo que usted pueda localizarlo.

Envíe cinco paquetes icmp de 172.16.10.2 a 172.16.20.2 después de que usted ingrese el comando que se utiliza para habilitar la traza FIA, según lo descrito en la sección anterior.

```
ASR1000#show platform packet-trace summary
Pkt   Input            Output           State  Reason
0     Gi0/0/1          Gi0/0/0          FWD
1     Gi0/0/1          Gi0/0/0          FWD
2     Gi0/0/1          Gi0/0/0          FWD
3     Gi0/0/1          Gi0/0/0          FWD
4     Gi0/0/1          Gi0/0/0          FWD

ASR1000#show platform packet-trace packet 0
Packet: 0           CBUG ID: 9
Summary
 Input     : GigabitEthernet0/0/1
 Output    : GigabitEthernet0/0/0
 State     : FWD
 Timestamp
   Start   : 1819281992118 ns (05/17/2014 06:42:01.207240 UTC)
   Stop    : 1819282095121 ns (05/17/2014 06:42:01.207343 UTC)
Path Trace
 Feature: IPV4
   Source      : 172.16.10.2
   Destination : 172.16.20.2
   Protocol    : 1 (ICMP)
 Feature: FIA_TRACE
   Entry     : 0x8059dbe8 - DEBUG_COND_INPUT_PKT
   Timestamp : 3685243309297
 Feature: FIA_TRACE
   Entry     : 0x82011a00 - IPV4_INPUT_DST_LOOKUP_CONSUME
   Timestamp : 3685243311450
 Feature: FIA_TRACE
   Entry     : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
   Timestamp : 3685243312427
 Feature: FIA_TRACE
   Entry     : 0x82004b68 - IPV4_OUTPUT_LOOKUP_PROCESS
   Timestamp : 3685243313230
 Feature: FIA_TRACE
   Entry     : 0x8034f210 - IPV4_INPUT_IPOPTIONS_PROCESS
   Timestamp : 3685243315033
 Feature: FIA_TRACE
   Entry     : 0x82013200 - IPV4_OUTPUT_GOTO_OUTPUT_FEATURE
   Timestamp : 3685243315787
 Feature: FIA_TRACE
   Entry     : 0x80321450 - IPV4_VFR_REFRAG
   Timestamp : 3685243316980
 Feature: FIA_TRACE
   Entry     : 0x82014700 - IPV6_INPUT_L2_REWRITE
   Timestamp : 3685243317713
 Feature: FIA_TRACE
   Entry     : 0x82000080 - IPV4_OUTPUT_FRAG
   Timestamp : 3685243319223
 Feature: FIA_TRACE
   Entry     : 0x8200e500 - IPV4_OUTPUT_DROP_POLICY
   Timestamp : 3685243319950
 Feature: FIA_TRACE
   Entry     : 0x8059aff4 - PACTRAC_OUTPUT_STATS
   Timestamp : 3685243323603
 Feature: FIA_TRACE
   Entry     : 0x82016100 - MARMOT_SPA_D_TRANSMIT_PKT
   Timestamp : 3685243326183

ASR1000#
```

Marque el FIA asociado a una interfaz

Cuando usted habilita los debugs condicionales de la plataforma, se agrega al FIA como característica. Dependiendo de la ubicación que está agregada a la lista, usted puede ser que necesite ajustar sus condiciones de la plataforma, por ejemplo cuando usted localiza el PRE-encap y los paquetes del poste-encap.

Esta salida muestra la pedido de las características en el FIA para el debugging condicional de la plataforma que se habilita en la dirección de ingreso:

```
ASR1000#show platform hardware qfp active interface if-name GigabitEthernet 0/0/1

General interface information
Interface Name: GigabitEthernet0/0/1
Interface state: VALID
Platform interface handle: 10
QFP interface handle: 8
Rx uidb: 1021
Tx uidb: 131064
Channel: 16
Interface Relationships

BGPPA/QPPB interface configuration information
Ingress: BGPPA/QPPB not configured. flags: 0000
Egress : BGPPA not configured. flags: 0000

ipv4_input enabled.
ipv4_output enabled.
layer2_input enabled.
layer2_output enabled.
ess_ac_input enabled.

Features Bound to Interface:
2 GIC FIA state
48 PUNT INJECT DB
39 SPA/Marmot server
40 ethernet
1 IFM
31 icmp_svr
33 ipfrag_svr
34 ipreass_svr
36 ipvfr_svr
37 ipv6vfr_svr
12 CPP IPSEC
Protocol 0 - ipv4_input
FIA handle - CP:0x108d99cc DP:0x8070f400
IPV4_INPUT_DST_LOOKUP_ISSUE (M)
IPV4_INPUT_ARL_SANITY (M)
  CBUG_INPUT_FIA
  DEBUG_COND_INPUT_PKT
IPV4_INPUT_DST_LOOKUP_CONSUME (M)
IPV4_INPUT_FOR_US_MARTIAN (M)
IPV4_INPUT_IPSEC_CLASSIFY
IPV4_INPUT_IPSEC_COPROC_PROCESS
IPV4_INPUT_IPSEC_RERUN_JUMP
IPV4_INPUT_LOOKUP_PROCESS (M)
IPV4_INPUT_IPOPTIONS_PROCESS (M)
IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
FIA handle - CP:0x108d9a34 DP:0x8070eb00
IPV4_OUTPUT_VFR
MC_OUTPUT_GEN_RECYCLE (D)
IPV4_VFR_REFRAG (M)
```

```
IPV4_OUTPUT_IPSEC_CLASSIFY
IPV4_OUTPUT_IPSEC_COPROC_PROCESS
IPV4_OUTPUT_IPSEC_RERUN_JUMP
IPV4_OUTPUT_L2_REWRITE (M)
IPV4_OUTPUT_FRAG (M)
IPV4_OUTPUT_DROP_POLICY (M)
PACTRAC_OUTPUT_STATS
MARMOT_SPA_D_TRANSMIT_PKT
DEF_IF_DROP_FIA (M)
Protocol 8 - layer2_input
FIA handle - CP:0x108d9bd4 DP:0x8070c700
LAYER2_INPUT_SIA (M)
CBUG_INPUT_FIA
DEBUG_COND_INPUT_PKT
LAYER2_INPUT_LOOKUP_PROCESS (M)
LAYER2_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 9 - layer2_output
FIA handle - CP:0x108d9658 DP:0x80714080
LAYER2_OUTPUT_SERVICEWIRE (M)
LAYER2_OUTPUT_DROP_POLICY (M)
PACTRAC_OUTPUT_STATS
MARMOT_SPA_D_TRANSMIT_PKT
DEF_IF_DROP_FIA (M)
Protocol 14 - ess_ac_input
FIA handle - CP:0x108d9ba0 DP:0x8070cb80
PPPOE_GET_SESSION
ESS_ENTER_SWITCHING
PPPOE_HANDLE_UNCLASSIFIED_SESSION
DEF_IF_DROP_FIA (M)

QfpEth Physical Information
DPS Addr: 0x11215eb8
Submap Table Addr: 0x00000000
VLAN Ethertype: 0x8100
QOS Mode: Per Link

ASR1000#
```

> **Note**: Los CBUG_INPUT_FIA y los DEBUG_COND_INPUT_PKT corresponden a las características condicionales del debug que se configuran en el router.

Vacie los paquetes localizados

Usted puede copiar y vaciar los paquetes mientras que se localizan, mientras que esta sección describe. Este ejemplo muestra cómo copiar un máximo de 2,048 bytes de los paquetes en la dirección de ingreso (172.16.10.2 a 172.16.20.2).

Aquí está el comando adicional que es necesario:

```
ASR1000#debug platform packet-trace copy packet input size 2048
```

> **Note**: El tamaño del paquete se copia que está en el rango de 16 a 2,048 bytes.

Ingrese este comando para vaciar los paquetes copiados:

```
ASR1000#show platform packet-trace packet 0
Packet: 0 CBUG ID: 14
```

```
Summary
Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0
State : FWD
Timestamp
    Start   : 1819281992118 ns (05/17/2014 06:40:01.207240 UTC)
    Stop    : 1819282095121 ns (05/17/2014 06:40:01.207343 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.20.2
Protocol : 1 (ICMP)
Feature: FIA_TRACE
Entry : 0x8059dbe8 - DEBUG_COND_INPUT_PKT
Timestamp : 4458180580929

<some content excluded>

Feature: FIA_TRACE
Entry : 0x82016100 - MARMOT_SPA_D_TRANSMIT_PKT
Timestamp : 4458180593896
Packet Copy In
a4934c8e 33020023 33231379 08004500 00640160 0000ff01 5f16ac10 0201ac10
01010800 1fd40024 00000000 000184d0 d980abcd abcdabcd abcdabcd abcdabcd
abcdabcd abcdabcd abcdabcd abcdabcd abcdabcd abcdabcd abcdabcd abcdabcd
abcdabcd abcdabcd abcdabcd abcdabcd abcd

ASR1000#
```

Caiga la traza

La traza del descenso está disponible en la versión 3.11 del Software Cisco IOS XE y posterior. Habilita la traza del paquete solamente para los paquetes perdidos. Aquí están algunos resaltados de la característica:

- Permite opcionalmente que usted especifique la retención de los paquetes para un código específico del descenso.
- Puede ser utilizada sin las condiciones globales o de la interfaz para capturar los eventos del descenso.
- Una captura del evento del descenso significa que solamente el descenso sí mismo está localizado, no la vida del paquete. Sin embargo, todavía permite que usted capture los datos de resumen, los datos del tuple, y el paquete para ayudar a refinar las condiciones o a proporcionar las pistas al debug siguiente camina.

Aquí está la sintaxis de los comandos que se utiliza para habilitar las trazas del paquete del descenso-tipo:

```
debug platform packet-trace drop [code <code-num>]
```

El código del descenso es lo mismo que el descenso ID, como se explica en el **comando detail del descenso de las estadísticas activas del qfp del hardware de plataforma de la demostración** hecho salir:

```
ASR1000#show platform hardware qfp active statistics drop detail
------------------------------------------------------------------------------
```

```
   ID  Global Drop Stats                          Packets                 Octets
-------------------------------------------------------------------------------
   60  IpTtlExceeded                                  3                    126
    8  Ipv4Acl                                       32                   3432
```

Escenario de la traza del descenso del ejemplo

Aplique este ACL en la interfaz del carruaje 0/0/0 del ASR1K para caer el tráfico de 172.16.10.2 a 172.16.20.2:

```
ASR1000#show platform hardware qfp active statistics drop detail
-------------------------------------------------------------------------------
   ID  Global Drop Stats                          Packets                 Octets
-------------------------------------------------------------------------------
   60  IpTtlExceeded                                  3                    126
    8  Ipv4Acl                                       32                   3432
```

Con el ACL en el lugar, que cae el tráfico del host local al host remoto, aplique esta configuración de la descenso-traza:

```
debug platform condition interface Gig 0/0/1 ingress
debug platform condition start
debug platform packet-trace packet 1024 fia-trace
debug platform packet-trace drop
```

Envíe cinco paquetes de pedidos ICMP de 172.16.10.2 a 172.16.20.2. La traza del descenso captura estos paquetes que sean caídos por el ACL, como se muestra:

```
ASR1000#show platform packet-trace statistics
Packets Summary
Matched 5
Traced 5
Packets Received
Ingress 5
Inject 0
Packets Processed
Forward 0
Punt 0
Drop     5
Count Code Cause
5 8 Ipv4Acl
Consume 0
```

```
ASR1000#show platform packet-trace summary
Pkt Input Output State Reason
0 Gi0/0/1 Gi0/0/0 DROP 8 (Ipv4Acl)
1 Gi0/0/1 Gi0/0/0 DROP 8 (Ipv4Acl)
2 Gi0/0/1 Gi0/0/0 DROP 8 (Ipv4Acl)
3 Gi0/0/1 Gi0/0/0 DROP 8 (Ipv4Acl)
4 Gi0/0/1 Gi0/0/0 DROP 8 (Ipv4Acl)
```

```
ASR1K#debug platform condition stop

ASR1K#show platform packet-trace packet 0
Packet: 0 CBUG ID: 140
Summary
Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0
```

```
State     : DROP 8   (Ipv4Acl)
Timestamp
Start : 1819281992118 ns (05/17/2014 06:42:01.207240 UTC)
Stop : 1819282095121 ns (05/17/2014 06:42:01.207343 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.20.2
Protocol : 1 (ICMP)
Feature: FIA_TRACE
Entry : 0x806c7eac - DEBUG_COND_INPUT_PKT
Lapsed time: 1031 ns
Feature: FIA_TRACE
Entry : 0x82011c00 - IPV4_INPUT_DST_LOOKUP_CONSUME
Lapsed time: 657 ns
Feature: FIA_TRACE
Entry : 0x806a2698 - IPV4_INPUT_ACL
Lapsed time: 2773 ns
Feature: FIA_TRACE
Entry : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
Lapsed time: 1013 ns
Feature: FIA_TRACE
Entry : 0x82004500 - IPV4_OUTPUT_LOOKUP_PROCESS
Lapsed time: 2951 ns
Feature: FIA_TRACE
Entry : 0x8041771c - IPV4_INPUT_IPOPTIONS_PROCESS
Lapsed time: 373 ns
Feature: FIA_TRACE
Entry : 0x82013400 - MPLS_INPUT_GOTO_OUTPUT_FEATURE
Lapsed time: 2097 ns
Feature: FIA_TRACE
Entry : 0x803c60b8 - IPV4_MC_OUTPUT_VFR_REFRAG
Lapsed time: 373 ns
Feature: FIA_TRACE
Entry : 0x806db148 - OUTPUT_DROP
Lapsed time: 1297 ns
Feature: FIA_TRACE
Entry : 0x806a0c98 - IPV4_OUTPUT_ACL
Lapsed time: 78382 ns

ASR1000#
```

Inyecte y lleve en batea las trazas

La característica de la traza del paquete de la inyección y de la batea fue agregada en la versión 3.12 del Software Cisco IOS XE y posterior para localizar la batea (los paquetes que se reciben en el FP que se llevan en batea al avión del control) e inyectar (los paquetes que se inyectan al FP del avión del control) los paquetes.

> **Note**: La traza de la batea puede trabajar sin el global o interconecta las condiciones, apenas como una traza del descenso. Sin embargo, las condiciones se deben definir para que una traza de la inyección trabaje.

Aquí está un ejemplo de una batea e inyecta la traza del paquete cuando usted hace ping del ASR1K a un router adyacente:

```
 ASR1000#debug platform condition ipv4 172.16.10.2/32 both
ASR1000#debug platform condition start
ASR1000#debug platform packet-trace punt
```

```
ASR1000#debug platform packet-trace inject
ASR1000#debug platform packet-trace packet 16
ASR1000#
ASR1000#ping 172.16.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 14/14/15 ms
ASR1000#
```

Ahora usted puede verificar la batea e inyectar los resultados de la traza:

```
ASR1000#show platform packet-trace summary
Pkt Input Output State Reason
0 INJ.2 Gi0/0/1 FWD
1 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
2 INJ.2 Gi0/0/1 FWD
3 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
4 INJ.2 Gi0/0/1 FWD
5 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
6 INJ.2 Gi0/0/1 FWD
7 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
8 INJ.2 Gi0/0/1 FWD
9 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)

ASR1000#show platform packet-trace packet 0
Packet: 0 CBUG ID: 120
Summary
Input     : INJ.2
Output : GigabitEthernet0/0/1
State : FWD
Timestamp
Start : 115612780360228 ns (05/29/2014 15:02:55.467987 UTC)
Stop : 115612780380931 ns (05/29/2014 15:02:55.468008 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.1
Destination : 172.16.10.2
Protocol : 1 (ICMP)

ASR1000#
ASR1000#show platform packet-trace packet 1
Packet: 1 CBUG ID: 121
Summary
Input : GigabitEthernet0/0/1
Output : internal0/0/rp:0
State     : PUNT 11  (For-us data)
Timestamp
Start : 115612781060418 ns (05/29/2014 15:02:55.468687 UTC)
Stop : 115612781120041 ns (05/29/2014 15:02:55.468747 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.10.1
Protocol : 1 (ICMP)
```

Ejemplos de la traza del paquete

Esta sección proporciona algunos ejemplos donde está útil la característica de la traza del paquete para los propósitos de Troubleshooting.

Ejemplo de la traza del paquete - NAT

Con este ejemplo, una traducción de la dirección (NAT) de la red de origen de la interfaz se configura en la interfaz de WAN de un ASR1K (Gig0/0/0) para la subred local (172.16.10.0/24).

Aquí está la configuración de la condición y de la traza del paquete de la plataforma que se utiliza para localizar el tráfico de 172.16.10.2 a 172.16.20.2, que se convierte en (NAT) traducido en la interfaz Gig0/0/0:

```
ASR1000#show platform packet-trace summary
Pkt Input Output State Reason
0 INJ.2 Gi0/0/1 FWD
1 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
2 INJ.2 Gi0/0/1 FWD
3 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
4 INJ.2 Gi0/0/1 FWD
5 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
6 INJ.2 Gi0/0/1 FWD
7 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)
8 INJ.2 Gi0/0/1 FWD
9 Gi0/0/1 internal0/0/rp:0 PUNT 11 (For-us data)

ASR1000#show platform packet-trace packet 0
Packet: 0 CBUG ID: 120
Summary
Input     : INJ.2
Output : GigabitEthernet0/0/1
State : FWD
Timestamp
Start : 115612780360228 ns (05/29/2014 15:02:55.467987 UTC)
Stop : 115612780380931 ns (05/29/2014 15:02:55.468008 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.1
Destination : 172.16.10.2
Protocol : 1 (ICMP)

ASR1000#
ASR1000#show platform packet-trace packet 1
Packet: 1 CBUG ID: 121
Summary
Input : GigabitEthernet0/0/1
Output : internal0/0/rp:0
State     : PUNT 11  (For-us data)
Timestamp
Start : 115612781060418 ns (05/29/2014 15:02:55.468687 UTC)
Stop : 115612781120041 ns (05/29/2014 15:02:55.468747 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.10.1
Protocol : 1 (ICMP)
```

Cuando cinco paquetes icmp se envían de 172.16.10.2 a 172.16.20.2 con una configuración del NAT de la fuente de la interfaz, éstos son los resultados de la traza del paquete:

```
ASR1000#show platform packet-trace summary
Pkt Input Output State Reason
0 Gi0/0/1 Gi0/0/0 FWD
```

```
1 Gi0/0/1 Gi0/0/0 FWD
2 Gi0/0/1 Gi0/0/0 FWD
3 Gi0/0/1 Gi0/0/0 FWD
4 Gi0/0/1 Gi0/0/0 FWD

ASR1000#show platform packet-trace statistics
Packets Summary
Matched 5
Traced 5
Packets Received
Ingress 5
Inject 0
Packets Processed
Forward 5
Punt 0
Drop 0
Consume 0

ASR1000#show platform packet-trace packet 0
Packet: 0 CBUG ID: 146
Summary
Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0
State : FWD
Timestamp
Start : 3010217805313 ns (05/17/2014 07:01:52.227836 UTC)
Stop : 3010217892847 ns (05/17/2014 07:01:52.227923 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.20.2
Protocol : 1 (ICMP)
Feature: FIA_TRACE
Entry : 0x806c7eac - DEBUG_COND_INPUT_PKT
Lapsed time: 1031 ns
Feature: FIA_TRACE
Entry : 0x82011c00 - IPV4_INPUT_DST_LOOKUP_CONSUME
Lapsed time: 462 ns
Feature: FIA_TRACE
Entry : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
Lapsed time: 355 ns
Feature: FIA_TRACE
Entry : 0x803c6af4 - IPV4_INPUT_VFR
Lapsed time: 266 ns
Feature: FIA_TRACE
Entry : 0x82004500 - IPV4_OUTPUT_LOOKUP_PROCESS
Lapsed time: 942 ns
Feature: FIA_TRACE
Entry : 0x8041771c - IPV4_INPUT_IPOPTIONS_PROCESS
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry : 0x82013400 - MPLS_INPUT_GOTO_OUTPUT_FEATURE
Lapsed time: 568 ns
Feature: FIA_TRACE
Entry : 0x803c6900 - IPV4_OUTPUT_VFR
Lapsed time: 266 ns
Feature: NAT
Direction : IN to OUT
Action : Translate Source
Old Address : 172.16.10.2 00028
New Address : 192.168.10.1 00002
Feature: FIA_TRACE
Entry : 0x8031c248 - IPV4_NAT_OUTPUT_FIA
Lapsed time: 55697 ns
```

```
Feature: FIA_TRACE
Entry : 0x801424f8 - IPV4_OUTPUT_THREAT_DEFENSE
Lapsed time: 693 ns
Feature: FIA_TRACE
Entry : 0x803c60b8 - IPV4_MC_OUTPUT_VFR_REFRAG
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry : 0x82014900 - IPV6_INPUT_L2_REWRITE
Lapsed time: 444 ns
Feature: FIA_TRACE
Entry : 0x82000080 - IPV4_OUTPUT_FRAG
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry : 0x8200e600 - IPV4_OUTPUT_DROP_POLICY
Lapsed time: 1457 ns
Feature: FIA_TRACE
Entry : 0x82017980 - MARMOT_SPA_D_TRANSMIT_PKT
Lapsed time: 7431 ns
ASR1000#
```

Ejemplo de la traza del paquete - VPN

Con este ejemplo, un túnel del VPN de sitio a sitio se utiliza entre el ASR1K y el router del Cisco IOS para proteger el tráfico que fluye entre 172.16.10.0/24 y 172.16.20.0/24 (local y las subredes remotas).

Aquí está la configuración de la condición y de la traza del paquete de la plataforma que se utiliza para localizar el tráfico VPN que los flujos de 172.16.10.2 a 172.16.20.2 en la interfaz del carruaje 0/0/1:

```
ASR1000#show platform packet-trace summary
Pkt Input Output State Reason
0 Gi0/0/1 Gi0/0/0 FWD
1 Gi0/0/1 Gi0/0/0 FWD
2 Gi0/0/1 Gi0/0/0 FWD
3 Gi0/0/1 Gi0/0/0 FWD
4 Gi0/0/1 Gi0/0/0 FWD

ASR1000#show platform packet-trace statistics
Packets Summary
Matched 5
Traced 5
Packets Received
Ingress 5
Inject 0
Packets Processed
Forward 5
Punt 0
Drop 0
Consume 0

ASR1000#show platform packet-trace packet 0
Packet: 0 CBUG ID: 146
Summary
Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0
State : FWD
Timestamp
Start : 3010217805313 ns (05/17/2014 07:01:52.227836 UTC)
Stop : 3010217892847 ns (05/17/2014 07:01:52.227923 UTC)
Path Trace
```

```
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.20.2
Protocol : 1 (ICMP)
Feature: FIA_TRACE
Entry : 0x806c7eac - DEBUG_COND_INPUT_PKT
Lapsed time: 1031 ns
Feature: FIA_TRACE
Entry : 0x82011c00 - IPV4_INPUT_DST_LOOKUP_CONSUME
Lapsed time: 462 ns
Feature: FIA_TRACE
Entry : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
Lapsed time: 355 ns
Feature: FIA_TRACE
Entry : 0x803c6af4 - IPV4_INPUT_VFR
Lapsed time: 266 ns
Feature: FIA_TRACE
Entry : 0x82004500 - IPV4_OUTPUT_LOOKUP_PROCESS
Lapsed time: 942 ns
Feature: FIA_TRACE
Entry : 0x8041771c - IPV4_INPUT_IPOPTIONS_PROCESS
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry : 0x82013400 - MPLS_INPUT_GOTO_OUTPUT_FEATURE
Lapsed time: 568 ns
Feature: FIA_TRACE
Entry : 0x803c6900 - IPV4_OUTPUT_VFR
Lapsed time: 266 ns
Feature: NAT
Direction : IN to OUT
Action : Translate Source
Old Address : 172.16.10.2 00028
New Address : 192.168.10.1 00002
Feature: FIA_TRACE
Entry : 0x8031c248 - IPV4_NAT_OUTPUT_FIA
Lapsed time: 55697 ns
Feature: FIA_TRACE
Entry : 0x801424f8 - IPV4_OUTPUT_THREAT_DEFENSE
Lapsed time: 693 ns
Feature: FIA_TRACE
Entry : 0x803c60b8 - IPV4_MC_OUTPUT_VFR_REFRAG
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry : 0x82014900 - IPV6_INPUT_L2_REWRITE
Lapsed time: 444 ns
Feature: FIA_TRACE
Entry : 0x82000080 - IPV4_OUTPUT_FRAG
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry : 0x8200e600 - IPV4_OUTPUT_DROP_POLICY
Lapsed time: 1457 ns
Feature: FIA_TRACE
Entry : 0x82017980 - MARMOT_SPA_D_TRANSMIT_PKT
Lapsed time: 7431 ns
ASR1000#
```

Cuando cinco paquetes icmp se envían de 172.16.10.2 a 172.16.20.2, que son cifrados por el túnel VPN entre el ASR1K y el router del Cisco IOS en este ejemplo, éstas son las salidas de la traza del paquete:

> **Note**: Las trazas del paquete muestran la manija de la asociación de seguridad QFP (SA) en la traza que se utiliza para cifrar el paquete, que es útil cuando usted resuelve problemas los problemas del IPSec VPN para verificar que el SA correcto está utilizado para el cifrado.

```
ASR1000#show platform packet-trace summary
Pkt Input Output State Reason
0 Gi0/0/1 Gi0/0/0 FWD
1 Gi0/0/1 Gi0/0/0 FWD
2 Gi0/0/1 Gi0/0/0 FWD
3 Gi0/0/1 Gi0/0/0 FWD
4 Gi0/0/1 Gi0/0/0 FWD

ASR1000#show platform packet-trace packet 0
Packet: 0 CBUG ID: 211
Summary
Input : GigabitEthernet0/0/1
Output : GigabitEthernet0/0/0
State : FWD
Timestamp
Start : 4636921551459 ns (05/17/2014 07:28:59.211375 UTC)
Stop : 4636921668739 ns (05/17/2014 07:28:59.211493 UTC)
Path Trace
Feature: IPV4
Source : 172.16.10.2
Destination : 172.16.20.2
Protocol : 1 (ICMP)
Feature: FIA_TRACE
Entry : 0x806c7eac - DEBUG_COND_INPUT_PKT
Lapsed time: 622 ns
Feature: FIA_TRACE
Entry : 0x82011c00 - IPV4_INPUT_DST_LOOKUP_CONSUME
Lapsed time: 462 ns
Feature: FIA_TRACE
Entry : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
Lapsed time: 320 ns
Feature: FIA_TRACE
Entry : 0x82004500 - IPV4_OUTPUT_LOOKUP_PROCESS
Lapsed time: 1102 ns
Feature: FIA_TRACE
Entry : 0x8041771c - IPV4_INPUT_IPOPTIONS_PROCESS
Lapsed time: 88 ns
Feature: FIA_TRACE
Entry : 0x82013400 - MPLS_INPUT_GOTO_OUTPUT_FEATURE
Lapsed time: 586 ns
Feature: FIA_TRACE
Entry : 0x803c6900 - IPV4_OUTPUT_VFR
Lapsed time: 266 ns
Feature: FIA_TRACE
Entry : 0x80757914 - MC_OUTPUT_GEN_RECYCLE
Lapsed time: 195 ns
Feature: FIA_TRACE
Entry : 0x803c60b8 - IPV4_MC_OUTPUT_VFR_REFRAG
Lapsed time: 88 ns
Feature: IPSec
Result : IPSEC_RESULT_SA
Action : ENCRYPT
SA Handle : 6
Peer Addr : 192.168.20.1
Local Addr: 192.168.10.1
Feature: FIA_TRACE
Entry : 0x8043caec - IPV4_OUTPUT_IPSEC_CLASSIFY
Lapsed time: 9528 ns
Feature: FIA_TRACE
Entry : 0x8043915c - IPV4_OUTPUT_IPSEC_DOUBLE_ACL
Lapsed time: 355 ns
Feature: FIA_TRACE
```

```
Entry : 0x8043b45c - IPV4_IPSEC_FEATURE_RETURN
Lapsed time: 657 ns
Feature: FIA_TRACE
Entry : 0x8043ae28 - IPV4_OUTPUT_IPSEC_RERUN_JUMP
Lapsed time: 888 ns
Feature: FIA_TRACE
Entry : 0x80436f10 - IPV4_OUTPUT_IPSEC_POST_PROCESS
Lapsed time: 2186 ns
Feature: FIA_TRACE
Entry : 0x8043b45c - IPV4_IPSEC_FEATURE_RETURN
Lapsed time: 675 ns
Feature: FIA_TRACE
Entry : 0x82014900 - IPV6_INPUT_L2_REWRITE
Lapsed time: 1902 ns
Feature: FIA_TRACE
Entry : 0x82000080 - IPV4_OUTPUT_FRAG
Lapsed time: 71 ns
Feature: FIA_TRACE
Entry : 0x8200e600 - IPV4_OUTPUT_DROP_POLICY
Lapsed time: 1582 ns
Feature: FIA_TRACE
Entry : 0x82017980 - MARMOT_SPA_D_TRANSMIT_PKT
Lapsed time: 3964 ns
ASR1000#
```

Impacto en el rendimiento

Los buffers de la traza del paquete consumen QFP DRAM, sean tan atentos de la cantidad de memoria que una configuración requiere y de la cantidad de memoria que está disponible.

El impacto del rendimiento varía, dependiente sobre las opciones de la traza del paquete se habilitan que. La traza del paquete afecta solamente al rendimiento de reenvío de los paquetes se localizan que, por ejemplo esos paquetes que hagan juego las condiciones del usuario configurado. El más granular y información detallada que usted configura la traza del paquete para capturar, mayor afectará los recursos.

Como con cualquier troubleshooting, es el mejor tomar un acercamiento iterativo y habilitar solamente las opciones más-detalladas de la traza cuando una situación del debug lo autoriza.

El uso QFP DRAM se puede estimar con esta fórmula:

la memoria necesitó = (los gastos indirectos stats) + numérico del pkts * (tamaño sumario + tamaño de los datos de trayecto + el tamaño de la copia)

> **Note**: Donde los **gastos indirectos stats** y **tamaño sumario** se reparan en 2 KB y 128 B, respectivamente, el **tamaño de los datos de trayecto** y el **tamaño de la copia** son utilizador configurables.

Información Relacionada

- Guía de configuración de software de los routeres de la serie de la agregación de las ASR1000 Series de Cisco - Traza del paquete
- Caídas de paquetes en el Routers del servicio de las ASR1000 Series de Cisco
- Soporte Técnico y Documentación - Cisco Systems