IOS-XE数据路径数据包踪迹功能

目录

简介

本文描述如何通过数据包踪迹功能执行Cisco IOS XE软件的数据路径包跟踪。

为了识别问题例如误配置，产能超载，甚至普通的软件Bug，当排除故障时，了解是必要的什么发生在系统内的一数据包。Cisco IOS XE数据包踪迹功能针对此需要。它提供使用认为和为了捕获根据用户定义的情况类的每个信息包处理的详细信息的字段SAFE方法。

先决条件

要求

Cisco建议您有是可用的在Cisco IOS XE版本3.10和以上数据包踪迹功能的知识，以及在运行Cisco IOS XE软件的所有平台，例如Cisco 1000系列聚合服务路由器(ASR1K)， Cisco 1000V系列Cloud服务路由器(CSR1000v)和Cisco 4451-X系列集成业务路由器(ISR4451-X)。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS XE软件版本3.10S (15.3(3)S)和以后
- ASR1K

本文档中的信息在特定实验室环境设备上创建。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络实际，请确保您了解使用的所有命令潜在影响。

参考拓扑

此图表说明使用示例在本文描述的拓扑：

包跟踪在使用中

为了说明使用数据包踪迹功能，使用在此部分中的示例描述互联网控制消息协议(ICMP)流量的trace从本地工作站172.16.10.2的(在ASR1K后)到远程主机172.16.20.2 (ASR1K的入口方向在Gig0/0/1接口)。

您能跟踪在ASR1K的数据包与这两个步骤：

1. 使平台有条件调试为了选择您在ASR1K要跟踪的数据包或流量。

2. 启用平台数据包踪迹(路径跟踪或以调用阵列(FIA) trace为特色)。

快速入门指南

这是快速入门指南，如果已经熟悉本文内容，并且想要快速查找的一个部分在CLI。这些是说明使用的仅一些示例工具，参考详细讨论语法的后面的章节，并且保证您使用是适当的对您的需求的配置。

1. 配置平台情况：

```
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)在平台情况配置后，请开始平台条件用此CLI命令：

debug platform condition start

2. 配置数据包踪迹：

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.

3. 其次，请启用平台数据包踪迹：

debug platform packet-trace enable

这是命令清楚缓冲区和重置数据包踪迹：

no debug platform packet-trace enable --> disable the packet trace, this needs to be done before you clear the buffer

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

debug platform packet-trace enable --> reenable the packet trace

命令清除平台调节，并且数据包踪迹配置是：

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

显示命令

验证平台情况，并且数据包踪迹配置，在您适用上一个命令为了保证您后有什么您需要。

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

这是命令检查跟踪的/获取数据包：

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.

Enable (event)平台有条件调试

数据包踪迹功能依靠有条件调试基础设施为了确定将跟踪的数据包。有条件调试基础设施提供能力给基于的过滤数据流：

- 协议
- IP地址和掩码
- 访问控制表(ACL)
- 接口
- 流量方向(入口或出口)

这些情况定义了过滤器何时何地应用到数据包。

对于在本例中使用的流量，请启用在入口方向的平台有条件调试从172.16.10.2的ICMP数据包的到172.16.20.2。换句话说，请选择您要跟踪的流量。有您能使用为了选择此流量的多种选项。

```
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
```

在本例中， access-list使用为了定义情况，如显示此处：

```
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
```

为了开始条件调试，请输入此命令：

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

注意：为了终止或禁用条件调试基础设施，请输入**stop命令调试平台的情况。**

为了查看配置的有条件调试过滤器，输入此命令：

```
ASR1000#show platform conditions

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

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

ASR1000#
```

总之，此配置至今应用：

```
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
```

Enable (event)数据包踪迹

注意：此部分详细描述数据包和复制选项，并且其它选项是描述的以后在本文。

物理和逻辑接口支持数据包踪迹，例如通道或虚拟访问接口。

这是数据包踪迹CLI语法：

```
ASR1000#debug platform packet-trace ?
copy Copy packet data
drop Trace drops only
enable Enable packet trace
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>]
这是此命令关键字的说明：

- **Pkt努姆**-数据包编号指定一次维护的最大信息包的数量。
- **summary-only** -这指定仅概略的数据捕获。默认是获取概略的数据和路径数据。
- **FIA trace** -除路径数据数据信息之外，这或者执行一FIA trace。
- **数据大小**-这允许您指定路径数据数据缓冲区的大小，从2,048个到16,384个字节。默认是2,048个字节。

debug platform packet-trace copy packet {in | out | both} [L2 | L3 | L4]
[size <num-bytes>]
这是此命令关键字的说明：

- **in/out**这指定将复制的数据包流的方向-入口和出口。
- **L2/L3/L4** -这允许您指定数据包的复制开始的位置。Layer2 (L2)是默认位置。
- **大小**-这允许您指定复制八位位组的最大。默认是64个八位位组。

对于此示例，这些是用于的命令为了启用选择与有条件调试基础设施的流量的数据包踪迹：

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

为了查看数据包踪迹配置，请输入此命令：

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

您能也输入**show debugging命令**为了查看平台有条件调试和数据包踪迹配置：

```
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 enable
debug platform packet-trace packet 16 data-size 2048
```

注意：输入**all命令清楚平台的情况**为了清除所有平台调试条件和数据包踪迹配置和数据。

总之，此配置数据至今用于为了启用数据包踪迹：

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

出口与数据包踪迹的情况限制

条件定义了有条件的过滤器，并且，当他们应用到数据包。例如，**调试平台情况接口g0/0/0出口**意味着数据包识别作为匹配，当到达在接口g0/0/0时的输出FIA，那么从入口发生的所有数据包处理，直到该点未命中。

> **注意**：思科强烈建议您使用数据包踪迹的入口条件为了得到可能多数完整和的有意义的数据。可以使用出口条件，但是知道限制。

显示数据包踪迹结果

> **注意**：此部分假设，路径跟踪启用。

数据包踪迹提供三个特定级别检查：

- 核算
- 每个信息包摘要
- 每个信息包路径数据

当五ICMP请求包从172.16.10.2被发送到172.16.20.2时，这些命令可以用于为了查看数据包踪迹结果：

```
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#
```

注意：第三命令提供说明如何查看每数据包的数据包踪迹的一示例。在本例中，跟踪的第一数据包显示。

从这些输出，您能看到五数据包跟踪，并且您能查看输入接口、输出接口、状态和路径跟踪。

状态	**重新标明**
前转	数据包为交付被安排/排队，转发到下一跳通过出口接口。
PUNT	数据包从转发处理器(FP)被踢到路由处理器(RP) (控制层面)。
丢弃	数据包在FP丢弃。运行FIA trace，请使用全局丢弃计数器，或者使用数据路径调试为了查找丢弃原更多详细信息。
缺点	数据包在一数据包进程中被消耗，例如在ICMP Ping请求期间或crypto数据包。

入口和**注入**在输出对应到数据包通过外部接口和数据包分别输入被看到如被注入从控制层面的数据包踪迹统计信息的计数器。

FIA Trace

FIA拿着乘数据包处理器引擎功能的列表(PPE)顺序地执行在Quantum流处理器(QFP)，当数据包是转发的入口或出口时。功能根据在计算机应用的配置数据。因此，当数据包处理， FIA trace帮助了解数据包的流到系统。

您必须运用此配置数据为了启用与FIA的数据包踪迹：

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

显示数据包踪迹结果

注意：此部分假设， FIA trace启用。并且，当您添加或修改当前数据包踪迹命令时，清除缓冲的数据包踪迹详细信息，因此您必须再发送若干流量，以便您能跟踪它。

请发送从172.16.10.2的五ICMP数据包到172.16.20.2，在您输入使用为了启用FIA trace后的命令，正如前面部分所描述。

```
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#
```

检查FIA关联与接口

当您启用平台有条件调试时，被添加到FIA作为功能。根据位置被添加到列表，您也许需要调节您的平台条件，例如，当您跟踪PRE encap和POST encap数据包时。

此输出显示功能的定货在FIA的在入口方向启用的平台条件调试的：

```
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#
```

> **注意**：CBUG_INPUT_FIA和DEBUG_COND_INPUT_PKT对应于在路由器配置的有条件调试功能。

转存跟踪的数据包

您能复制和转存数据包，当他们跟踪，当此部分描述。此示例显示如何复制最多2,048字节的在入口方向(172.16.10.2的数据包到172.16.20.2)。

这是需要的其它命令：

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

> **注意**：复制数据包的大小是在16个到2,048个字节范围内。

输入此命令为了转存复制的数据包：

```
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#
```

下降Trace

丢弃trace是可用的在Cisco IOS XE软件版本3.11和以上。它启用仅数据包踪迹丢弃的数据包的。这是功能的一些优点：

- 它或者允许您指定数据包的挽留一个特定丢弃代码的。
- 它可以用于，不用全局或接口情况为了捕获丢弃事件。
- 丢弃事件捕获意味着仅丢弃跟踪，数据包的不是寿命。然而，它仍然允许您获取概略的数据，元组数据，并且数据包为了帮助完善情况或提供提示向下调试跨步。

这是使用为了启用丢弃类型数据包踪迹的命令语法：

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

丢弃代码是相同的象丢弃ID，如在**显示平台硬件qfp的报告活动统计信息丢弃detail命令**输出：

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

示例丢弃Trace方案

应用在ASR1K的Gig 0/0/0接口的此ACL为了从172.16.10.2降低流量到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
```

使用到位ACL，从本地主机降低流量到远程主机，请运用此丢弃trace配置：

```
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
debug platform packet-trace enable
```

发送从172.16.10.2的五ICMP请求包到172.16.20.2。丢弃trace获取由ACL丢弃的这些数据包，如显示：

```
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#
```

注入并且踢跟踪

注入和平底船数据包踪迹功能在FP接收被踢到控制层面)的Cisco IOS XE软件版本3.12和以上被添加为了跟踪平底船(数据包和注入(被注入对从控制层面的FP)的数据包数据包。

> **注意**：平底船trace能工作，不用全局或建立接口条件，正如丢弃trace。然而，必须定义条件注入trace的能工作。

在这里平底船的示例并且注入数据包踪迹，当您从ASR1K ping到邻接路由器时：

```
 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#debug platform packet-trace enable
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#
```

现在您能验证平底船和注入trace结果：

```
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)
```

数据包踪迹示例

此部分提供数据包踪迹功能是有用的为了实现故障排除目的一些示例。

数据包踪迹示例- NAT

使用此示例，接口源网络地址转换(NAT)在ASR1K (Gig0/0/0)的广域网接口配置本地子网的(172.16.10.0/24)。

这是使用为了跟踪从172.16.10.2的流量到172.16.20.2，变得翻译的平台情况和数据包踪迹配置(NAT)在Gig0/0/0接口：

```
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)
```

当五ICMP数据包从172.16.10.2被发送到与接口来源NAT配置时的172.16.20.2，这些是数据包踪迹结果：

```
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#
```

数据包踪迹示例- VPN

使用此示例，站点到站点VPN通道用于在ASR1K和Cisco IOS路由器之间为了保护流在172.16.10.0/24和172.16.20.0/24之间的流量(本地和远程子网)。

这是使用为了跟踪该的VPN流量从172.16.10.2的流到在Gig 0/0/1接口的172.16.20.2的平台情况和数据包踪迹配置：

```
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#
```

当五ICMP数据包从172.16.10.2被发送到172.16.20.2时，由在ASR1K和Cisco IOS路由器之间的VPN通道加密在本例中，这些是数据包踪迹输出：

注意：数据包踪迹显示使用为了加密数据包，是有用的在trace的QFP安全关联(SA)把柄，当您排除故障IPSec VPN问题为了验证时正确SA使用加密。

```
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#
```

性能影响

数据包踪迹缓冲区消耗QFP DRAM，如此是配置要求是可用的记住内存数量和内存数量。

性能影响变化，从属在启用的数据包踪迹选项。数据包踪迹只影响跟踪数据包的转发性能，例如匹配用户配置的条件的那些数据包。更加粒状和详细信息您配置数据包踪迹捕获，越非常地将影响资源。

当调试情况担保它时，如同所有故障排除，采取一迭代方法和只启用更多详细trace选项是最佳的。

QFP DRAM使用情况可以预计与此公式：

所需的内存= (顶上的stats) +数字pkts * (概略的大小+路径数据大小+复制大小)

> **注意**：那里**stats开销**和**概略的大小**修复在2 KB，并且128 B，分别，**路径数据估量，**并且**复制大小**用户可配置的。

相关信息

- Cisco ASR1000系列聚合系列路由器软件配置指南-数据包踪迹
- 在Cisco ASR1000系列服务路由器的丢包
- 技术支持和文档 - Cisco Systems