

Característica do rastreamento de pacotes IOS-XE Datapath

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Topologia da referência](#)

[Pacote que segue no uso](#)

[Guia de início rápido](#)

[Permita a plataforma condicional debuga](#)

[Permita o rastreamento de pacotes](#)

[Limitação da condição da saída com rastreamentos de pacotes](#)

[Indique os resultados do rastreamento de pacotes](#)

[Traço FIA](#)

[Indique os resultados do rastreamento de pacotes](#)

[Verifique o FIA associado com uma relação](#)

[Despeje os pacotes seguidos](#)

[Deixe cair o traço](#)

[Encenação do traço da gota do exemplo](#)

[Injete e o pontapé segue](#)

[Exemplos do rastreamento de pacotes](#)

[Exemplo do rastreamento de pacotes - NAT](#)

[Exemplo do rastreamento de pacotes - VPN](#)

[Impacto de desempenho](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como executar o pacote do datapath que segue para o software do Cisco IOS[®]-XE através da característica do rastreamento de pacotes.

A fim identificar edições tais como o misconfiguration, sobrecarga da capacidade, ou mesmo o Bug de Software ordinário ao pesquisar defeitos, é necessário compreender o que acontece a um pacote dentro de um sistema. A característica do rastreamento de pacotes do Cisco IOS XE endereça esta necessidade. Fornece um método campo-seguro que seja usado explicando e a fim capturar o pacote per. que processa os detalhes baseados em uma classe de circunstâncias definidas pelo utilizador.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento da característica do rastreamento de pacotes que está disponível em versões 3.10 e mais recente do Cisco IOS XE, assim como em todas as Plataformas que executam o Software Cisco IOS XE, tal como o Roteadores dos serviços da agregação do Cisco 1000 Series (ASR1K), o Cisco 1000V Series nublado o roteador dos serviços (CSR1000v), e o roteador dos Serviços integrados do Cisco 4451-X Series (ISR4451-X).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versões 3.10S do Software Cisco IOS XE (15.3(3)S) e mais tarde
- ASR1K

As informações apresentadas neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, certifique-se de você compreender o impacto potencial do comando any usado.

Proveja a topologia

Este diagrama ilustra a topologia que é usada para os exemplos que são descritos neste documento:



Pacote que segue no uso

A fim ilustrar o uso da característica do rastreamento de pacotes, o exemplo que é usado durante toda esta seção descreve um traço do tráfego do Internet Control Message Protocol (ICMP) da estação de trabalho local 172.16.10.2 (atrás do ASR1K) ao host remoto 172.16.20.2 (a direção de ingresso para o ASR1K na relação Gig0/0/1).

Você pode seguir pacotes no ASR1K com estas duas etapas:

1. Permita a plataforma condicional debug a fim selecionar os pacotes ou tráfego que você quer seguir no ASR1K.
2. Permita o rastreamento de pacotes da plataforma (traço da disposição da invocação do rastreamento de caminho ou da característica (FIA)).

Guia de início rápido

Está aqui um guia de início rápido se você é já familiar com os índices deste documento, e quer uma seção para uma consulta rápida no CLI. Estes são somente alguns exemplos para ilustrar o uso da ferramenta, consultam as seções mais recente que discutem as sintaxes em detalhe, e

asseguram-lhe o uso a configuração que é apropriada a sua exigência.

1. Configurar condições da 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)
```

Depois que uma condição da plataforma é configurada, comece condições da plataforma com este comando CLI:

```
debug platform condition start
```

2. Configurar o rastreamento de pacotes:

```
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. Em seguida, permita o rastreamento de pacotes da plataforma:

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

Estão aqui os comandos cancelar o buffer e restaurar o rastreamento de pacotes:

```
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
```

O comando cancelar a plataforma condicional e a configuração do rastreamento de pacotes é:

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

Comandos show

Verifique que a configuração da condição e do rastreamento de pacotes da plataforma depois que você aplica os comandos precedentes a fim assegurar você tem o que você precisa.

```
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
```

Estão aqui os comandos verificar pacotes seguidos/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.
```

Permita a plataforma condicional debuga

A característica do rastreamento de pacotes confia no condicional debuga a infraestrutura a fim determinar os pacotes a ser seguidos. O condicionais debugam a infraestrutura fornecem a capacidade ao filtrar tráfego baseado sobre:

- Protocolo
- Endereço IP de Um ou Mais Servidores Cisco ICM NT e máscara
- Access Control List (ACL)
- Interface
- Direção de tráfego (ingresso ou saída)

Estas circunstâncias definem onde e quando os filtros estão aplicados a um pacote.

Para o tráfego que é usado neste exemplo, permita a plataforma condicional debuga na direção de ingresso para pacotes ICMP de 172.16.10.2 a 172.16.20.2. Ou seja selecione o tráfego que você quer seguir. Há as várias opções que você pode usar a fim selecionar este tráfego.

```
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
```

Neste exemplo, uma lista de acesso é usada a fim definir a circunstância, como mostrado aqui:

```
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
```

A fim começar o debugging condicional, incorpore este comando:

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

Nota: A fim parar ou desabilitar a infraestrutura do debugging condicional, inscreva o comando stop da condição da plataforma debugar.

A fim ver o condicional debugar os filtros que são configurados, incorporam 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#

Em resumo, esta configuração foi aplicada até aqui:

```
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
```

Permita o rastreamento de pacotes

Nota: Esta seção descreve o pacote e as opções de cópia em detalhe, e as outras opções são descritas mais tarde no documento.

Os rastreamentos de pacotes são apoiados no exame e nas interfaces lógicas, tais como o túnel ou as interfaces de acesso virtual.

Está aqui a sintaxe CLI do rastreamento de pacotes:

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

Estão aqui as descrições para as palavras-chaves deste comando:

- **Pacote-NUM** - O número do pacote especifica o número máximo de pacotes que é mantido ao mesmo tempo.
- **somente resumo** - Isto especifica que somente os dados sumários estão capturados. O padrão é capturar dados sumários e dados do caminho de recurso.
- **FIA-traço** - Isto executa opcionalmente um traço FIA além do que a informação de dados do trajeto.
- **tamanho de dados** - Isto permite que você especifique o tamanho do buffer de dados do trajeto, 2,048 a 16,384 bytes. O padrão é **2,048** bytes.

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

Estão aqui as descrições para as palavras-chaves deste comando:

- **entrada/saída** - Isto especifica o sentido do fluxo de pacote de informação a ser copiado - ingresso e/ou saída.
- **L2/L3/L4** - Isto permite que você especifique o lugar que a cópia do pacote começa. A camada 2 (L2) é o local padrão.
- **tamanho** - Isto permite que você especifique o número máximo de octetos que são copiados.

O padrão é 64 octetos.

Para este exemplo, estes são os comandos usados a fim permitir o rastreamento de pacotes para o tráfego que é selecionado com o condicional debug a infraestrutura:

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

A fim rever a configuração do rastreamento de pacotes, incorpore este comando:

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

Você pode igualmente inscrever o **comando show debugging** a fim ver a plataforma condicional debug e as configurações do rastreamento de pacotes:

```
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
```

Nota: Inscreva o **comando all claro da condição da plataforma** a fim cancelar toda a plataforma debugam condições e as configurações e os dados do rastreamento de pacotes.

Em resumo, estes dados de configuração foram usados até aqui a fim permitir o rastreamento de pacotes:

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

Limitação da condição da saída com rastreamentos de pacotes

As circunstâncias definem os filtros condicionais e quando estiverem aplicadas a um pacote. Por exemplo, **debugar a saída da relação g0/0/0 da condição da plataforma** significa que um pacote está identificado como um fósforo quando alcança a saída FIA na relação g0/0/0, tão todo o processamento do pacote que ocorrer do ingresso até que esse ponto esteja faltado.

Nota: Recomenda Cisco altamente que você usa condições do ingresso para rastreamentos de pacotes a fim obter os dados os mais completos e os mais significativos possíveis. As condições da saída podem ser usadas, mas estejam cientes das limitações.

Indique os resultados do rastreamento de pacotes

Nota: Esta seção supõe que o rastreamento de caminho está permitido.

Três níveis específicos da inspeção são fornecidos pelo rastreamento de pacotes:

- Relatório
- Sumário do pacote per.
- Dados do trajeto do pacote per.

Quando cinco pacotes de requisição ICMP são enviados de 172.16.10.2 a 172.16.20.2, estes comandos podem ser usados a fim ver os resultados do rastreamento de pacotes:

```
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#
```

Nota: O terceiro comando fornece um exemplo que ilustre como ver o rastreamento de pacotes para cada pacote. Neste exemplo, o primeiro pacote seguido é mostrado.

Destas saídas, você pode ver que cinco pacotes estão seguidos e que você pode ver a interface de entrada, a interface de saída, o estado, e o rastreamento de caminho.

Estado Observação

FWD

O pacote é programado/enfileirado para a entrega, para ser enviado ao salto seguinte através uma interface de saída.

PONTAPÉ O pacote punted do Forwarding Processor (FP) ao route processor (RP) (plano do controle).

GOTA	O pacote é deixado cair no FP. Execute o traço FIA, use contadores de queda globais, ou o datapath do uso debuga a fim encontrar mais detalhes para razões da gota.
CONS	O pacote é consumido durante um processo do pacote, como durante o pedido do ping ICMP os pacotes criptos.

O **ingresso** e **injeta** contadores nas estatísticas que do rastreamento de pacotes a saída corresponde aos pacotes que incorporam através de uma interface externa e dos pacotes que sejam considerados como injetados do plano do controle, respectivamente.

Traço FIA

O FIA guarda a lista de características que são executadas sequencialmente pelos Engine de processador do pacote (PPE) no processador do fluxo do quantum (QFP) quando um pacote é enviado o ingresso ou a saída. As características são baseadas nos dados de configuração que são aplicados na máquina. Assim, um traço FIA ajuda a compreender o fluxo do pacote através do sistema enquanto o pacote é processado.

Você deve aplicar estes dados de configuração a fim permitir o rastreamento de pacotes com FIA:

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

Indique os resultados do rastreamento de pacotes

Nota: Esta seção supõe que o traço FIA está permitido. Também, quando você adiciona ou altera os comandos trace do pacote atual, os detalhes protegidos do rastreamento de pacotes são cancelados, assim que você deve enviar algum tráfego outra vez de modo que você possa o seguir.

Envie cinco pacotes ICMP de 172.16.10.2 a 172.16.20.2 depois que você incorpora o comando que está usado a fim permitir o traço FIA, como descrito na seção 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#

Verifique o FIA associado com uma relação

Quando você permite a plataforma condicional debuga, ele está adicionada ao FIA como uma característica. Segundo o lugar que está adicionado à lista, você pôde precisar de ajustar suas condições da plataforma, como quando você segue pacotes do PRE-encap e do cargo-encap.

Esta saída mostra a ordem das características no FIA para o debugging condicional da plataforma que é permitido na direção de ingresso:

```
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#

Nota: Os **CBUG_INPUT_FIA** e os **DEBUG_COND_INPUT_PKT** correspondem ao condicional debugam as características que são configuradas no roteador.

Despeje os pacotes seguidos

Você pode copiar e despejar os pacotes enquanto estão seguidos, enquanto esta seção descreve. Este exemplo mostra como copiar um máximo de 2,048 bytes dos pacotes na direção de ingresso (172.16.10.2 a 172.16.20.2).

Está aqui o comando adicional que é precisado:

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

Nota: O tamanho do pacote que é copiado está na escala de 16 a 2,048 bytes.

Incorpore este comando a fim despejar os pacotes 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#

Deixe cair o traço

O traço da gota está disponível em versões 3.11 e mais recente do Software Cisco IOS XE. Permite o rastreamento de pacotes somente para pacotes descartado. Estão aqui alguns destaques da característica:

- Permite opcionalmente que você especifique a retenção dos pacotes para um código específico da gota.
- Pode ser usada sem condições globais ou da relação a fim capturar eventos da gota.
- Uma captação do evento da gota significa que somente a gota própria está seguida, não a vida do pacote. Contudo, ainda permite que você capture dados sumários, dados da tupla, e o pacote a fim ajudar a refinar circunstâncias ou fornecer indícios ao seguinte debug a etapa.

Está aqui a sintaxe de comando que é usada a fim permitir o gota-tipo rastreamentos de pacotes:

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

O código da gota é o mesmo que a gota ID, como relatado no **comando detail da gota das estatísticas ativas do qfp do hardware da plataforma da mostra** output:

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

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

Encenação do traço da gota do exemplo

Aplique este ACL na relação da atuação 0/0/0 do ASR1K a fim deixar cair o tráfego 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

Com o ACL no lugar, que deixa cair o tráfego do host local ao host remoto, aplique esta configuração do gota-traço:

```
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
```

Envie cinco pacotes de requisição ICMP de 172.16.10.2 a 172.16.20.2. O traço da gota captura estes pacotes que são deixados cair pelo ACL, como mostrado:

```
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#

Injete e o pontapé segue

A característica do rastreamento de pacotes da injeção e do pontapé foi adicionada nas versões 3.12 e mais recente do Software Cisco IOS XE a fim seguir o pontapé (os pacotes que são recebidas no FP que punted ao plano do controle) e injetar (os pacotes que são injetados ao FP do plano do controle) pacotes.

Nota: O traço do pontapé pode trabalhar sem o global ou conecta condições, apenas como um traço da gota. Contudo, as circunstâncias devem ser definidas para que um traço da injeção trabalhe.

Aqui está um exemplo de um pontapé e injeta o rastreamento de pacotes quando você sibila do ASR1K a um roteador adjacente:

```
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#
```

Agora você pode verificar o pontapé e injetar resultados do traço:

```
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)
```

Exemplos do rastreamento de pacotes

Esta seção fornece alguns exemplos onde a característica do rastreamento de pacotes é útil para propósitos de Troubleshooting.

Exemplo do rastreamento de pacotes - NAT

Com este exemplo, uma tradução de endereços da rede da fonte da relação (NAT) é configurada na interface WAN de um ASR1K (Gig0/0/0) para a sub-rede local (172.16.10.0/24).

Está aqui a configuração da condição e do rastreamento de pacotes da plataforma que é usada a fim seguir o tráfego de 172.16.10.2 a 172.16.20.2, que se torna traduzido (NAT) na relação 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)
```

Quando cinco pacotes ICMP são enviados de 172.16.10.2 a 172.16.20.2 com uma configuração de NAT da fonte da relação, estes são os resultados do rastreamento de pacotes:

```
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#

```

Exemplo do rastreamento de pacotes - VPN

Com este exemplo, um túnel do VPN de Site-para-Site é usado entre o ASR1K e o roteador do Cisco IOS a fim proteger o tráfego que flui entre 172.16.10.0/24 e 172.16.20.0/24 (local e sub-redes remotas).

Está aqui a configuração da condição e do rastreamento de pacotes da plataforma que é usada a fim seguir o tráfego VPN que flui de 172.16.10.2 a 172.16.20.2 na relação da atuação 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#
```

Quando cinco pacotes ICMP são enviados de 172.16.10.2 a 172.16.20.2, que estão cifrados pelo túnel VPN entre o ASR1K e o roteador do Cisco IOS neste exemplo, estas são as saídas de rastreamento de pacotes:

Nota: Os rastreamentos de pacotes mostram o punho da associação de segurança QFP (SA) no traço que é usado a fim cifrar o pacote, que é útil quando você pesquisa defeitos edições do IPsec VPN a fim verificar que o SA correto está usado para a criptografia.

```
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 de desempenho

Os buffers do rastreamento de pacotes consomem QFP DRAM, sejam assim conscientes da quantidade de memória que uma configuração exige e da quantidade de memória que está disponível.

O impacto no desempenho varia, dependente das opções do rastreamento de pacotes que são permitidas. O rastreamento de pacotes afeta somente o desempenho de encaminhamento dos pacotes que são seguidos, como aqueles pacotes que combinam as condições do configurado pelo usuário. O mais granulado e informação detalhada que você configura o rastreamento de pacotes para capturar, maior impactará recursos.

Como com todo o Troubleshooting, é o melhor tomar uma aproximação iterativa e permitir somente as opções mais-detalhadas do traço quando uma situação debugar a justifica.

O uso QFP DRAM pode ser calculado com esta fórmula:

a memória precisou = (despesas gerais stats) + número dos pacotes * (tamanho + tamanho de dados do trajeto + o tamanho sumários da cópia)

Nota: Onde as **despesas gerais stats** e **tamanho do sumário** são fixas em 2 KB e 128 B, respectivamente, o **tamanho de dados do trajeto** e o **tamanho da cópia** são configuráveis pelo usuário.

Informações Relacionadas

- [Manual de configuração do software dos Series Router da agregação do ASR1000 Series de Cisco - Rastreamento de pacotes](#)
- [Quedas de pacote de informação no Roteadores do serviço do ASR1000 Series de Cisco](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)