ZBFW for IOS-XE配置故障排除指南

目錄

簡介

本文說明如何使用用於輪詢ASR上硬體丟棄計數器的命令，對Aggregation Services Router(ASR)1000上的基於區域的防火牆(ZBFW)功能進行最佳故障排除。ASR1000是基於硬體的轉發平台。Cisco IOS-XE®的軟體配置會為硬體ASIC（量子流處理器，QFP）程式設計，以便執行功能轉發功能。這樣可以實現更高的吞吐量和更好的效能。缺點是它帶來了更大的故障排除挑戰。用於通過基於區域的防火牆(ZBFW)輪詢當前會話和丟棄計數器的傳統Cisco IOS命令不再有效，因為軟體中不再存在丟包。

連結和文檔

安裝和升級指南

- Cisco ASR 1000系列聚合服務路由器命令參考
- Cisco IOS XE 3S命令參考

Datapath故障排除步驟

為了對資料路徑進行故障排除，您必須確定流量是否正確通過ASR和Cisco IOS-XE代碼。特定於防火牆功能，資料路徑故障排除遵循以下步驟：

1. Verify Configuration — 收集配置並檢查輸出以驗證連線。
2. **驗證連線狀**態 — 如果流量正確通過，Cisco IOS-XE會在ZBFW功能上開啟連線。此連線跟蹤客戶端和伺服器之間的流量和狀態資訊。
3. **驗證捨棄計數**器 — 當流量不能正確傳遞時，Cisco IOS-XE會為所有捨棄的封包記錄捨棄計數器。檢查此輸出以找出流量失敗的原因。
4. **記錄** — 收集系統日誌，以便提供有關連線構建和資料包丟棄的更精細的資訊。
5. Packet Trace Dropped Packets — 使用資料包跟蹤來捕獲丟棄的資料包。
6. **調試** — 收集調試是最詳細的選項。可以有條件地取得偵錯，以便確認封包的準確轉送路徑。

驗證設定

show tech support firewall的輸出總結如下：

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

驗證連線狀態

可以獲取連線資訊，以便列出ZBFW上的所有連線。輸入以下命令：

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

它顯示從14.38.112.250到14.36.1.206的TCP telnet連線。

> **附註**：請注意，如果運行此命令，裝置上有大量連線將需要很長時間。思科建議您使用此處概述的特定過濾器運行此命令。

可將連線表過濾到特定的源地址或目標地址。在platform子模式後使用過濾器。要篩選的選項包括：

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

此連線表經過過濾，因此僅顯示源自14.38.112.250的連線：

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

一旦過濾了連線表，就可以獲得詳細的連線資訊，以便進行更全面的分析。若要顯示此輸出，請使用detail關鍵字。

```
ASR#show policy-firewall sessions platform v4-source-address 14.38.112.250 detail
--show platform hardware qfp active feature firewall datapath scb 14.38.112.250
any any any any all any detail--
[s=session  i=imprecise channel  c=control channel  d=data channel]
 14.38.112.250 41426 14.36.1.206 23 proto 6 (0:0)       [sc]
 pscb : 0x8c5d4f20,  bucket : 64672, fw_flags: 0x204 0x20419441,
       scb state: active, scb debug: 0
 nxt_timeout: 360000, refcnt: 1,  ha nak cnt: 0,  rg: 0, sess id: 117753
 hostdb: 0x0, L7: 0x0, stats: 0x8e118e40, child: 0x0
 l4blk0: 78fae7a7 l4blk1: e36df99c l4blk2: 78fae7ea l4blk3: 39080000
 l4blk4: e36df90e l4blk5: 78fae7ea l4blk6: e36df99c l4blk7: fde0000
 l4blk8: 0 l4blk9: 1
 root scb: 0x0 act_blk: 0x8e1115e0
 ingress/egress intf: GigabitEthernet0/0/2 (1021), GigabitEthernet0/0/0 (131065)
 current time 34004163065573 create tstamp: 33985412599209 last access: 33998256774622
 nat_out_local_addr:port: 0.0.0.0:0 nat_in_global_addr:port: 0.0.0.0:0
 syncookie fixup: 0x0
 halfopen linkage: 0x0 0x0
 cxsc_cft_fid: 0x0
 tw timer: 0x0 0x0 0x372ba 0x1e89c181
 Number of simultaneous packet per session allowed: 25
   bucket 125084 flags 1 func 1 idx 8 wheel 0x8ceb1120
```

檢查防火牆丟棄計數器

在XE 3.9期間，丟棄計數器輸出發生了變化。在XE 3.9之前，防火牆丟棄原因非常普遍。在XE 3.9之後，防火牆的丟棄原因被擴展，變得更加細緻。

若要驗證捨棄計數器，請執行以下步驟：

1. 確認Cisco IOS-XE中的全域性丟棄計數器。這些計數器顯示什麼功能丟棄了流量。功能示例包括服務品質(QoS)、網路地址轉換(NAT)、防火牆等。

2. 識別出子功能後，查詢該子功能提供的粒度丟棄計數器。在本指南中，要分析的子功能是防火牆功能。

QFP上的全域性丟棄計數器

要依賴的基本命令可在QFP上提供所有丟包：

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

此命令向您顯示跨QFP的通用丟棄。這些捨棄可能在任何功能上。一些示例功能包括：

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

若要檢視所有丟包，包括值為零的計數器，請使用命令：

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

若要清除計數器，請使用以下命令。在顯示到螢幕後清除輸出。此命令在讀取時是清除的，因此輸出在顯示到螢幕後**將**重置為零。

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

以下是QFP全域性防火牆丟棄計數器的清單和說明：

防火牆全域性丟棄原因	說明
防火牆背壓	日誌記錄機製造成的背壓導致丟包。
FirewallInvalidZone	沒有為介面配置安全區域。
FirewallL4Insp	L4策略檢查失敗。有關更詳細的丟棄原因（防火牆功能丟棄原因），請參閱下
FirewallNoForwardingZone	防火牆未初始化，並且不允許任何流量通過。
FirewallNonsession	會話建立失敗。這可能是由於已達到最大會話限制或記憶體分配失敗所致。
防火牆策略	已配置的防火牆策略被丟棄。
FirewallL4	L4檢測失敗。有關更詳細的丟棄原因（防火牆功能丟棄原因），請參閱下表。
FirewallL7	由於L7檢測而丟棄的資料包。有關更精細的L7丟棄原因（防火牆功能丟棄原因
FirewallNotInitiator	不是TCP、UDP或ICMP的會話發起程式。未建立任何會話。例如，對於ICMP這種情況可能會發生在正常的資料包處理或不精確的通道處理中。
FirewallNoNewSession	防火牆高可用性不允許新會話。
FirewallSyncookieMaxDst	為了提供基於主機的SYN泛洪保護，有一個目標SYN速率作為SYN泛洪限制。
FirewallSyncookie	SYNCOOLIE邏輯被觸發。這表示已傳送具有SYN cookie的SYN/ACK，且原始
FirewallARStandby	未啟用非對稱路由，並且冗餘組未處於活動狀態。

QFP上的防火牆功能捨棄計數器

QFP全域性丟棄計數器的侷限性在於，丟棄原因沒有粒度，而某些丟棄原因(如**FirewallL4**)會過載，以至於對故障排除幾乎沒有用處。此後在Cisco IOS-XE 3.9(15.3(2)S)中對此進行了增強，其中新增了防火牆功能捨棄計數器。這提供了更精細的丟棄原因集：

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

以下是防火牆功能捨棄原因和說明清單：

防火牆功能丟棄原因	說明
標頭長度無效	資料包過小，不能包含第4層TCP、UDP或ICMP標頭。可能是由以下原因 1. TCP報頭長度< 20 2. UDP/ICMP報頭長度< 8
無效的UDP資料長度	UDP資料包長度與UDP報頭中指定的長度不匹配。
ACK號無效	此下降可能是由於以下原因之一： 1. ACK不等於TCP對等體的next_seq#。 2. ACK大於TCP對等體傳送的最新的SEQ#。
ACK標誌無效	在TCP SYNSENT和SYNRCVD狀態下，預期ACK#等於ISN+1，但不是。 此下降可能是由於以下原因之一： 1. 需要ACK標誌，但未設定為不同的TCP狀態。 2. 除ACK標誌外，還設定了其他標誌（如RST）。
無效的TCP啟動器	發生這種情況時： 1. 來自TCP啟動器的第一個封包不是SYN（收到非初始TCP區段時沒 2. 初始SYN封包已設定ACK旗標。
帶資料的SYN	SYN資料包包含負載。不支援。
無效的TCP標誌	無效的TCP標誌可能是由以下原因造成的： 1. TCP初始SYN封包具有SYN以外的標誌。 2. 在TCP偵聽狀態下，TCP對等體收到RST或ACK。 3. 在SYN/ACK之前收到其他響應方的資料包。 4. 未從響應方收到預期的SYN/ACK。
處於SYNSENT狀態的段無效	處於SYNSENT狀態的無效TCP資料段是由以下原因造成的： 1. SYN/ACK有負載。 2. SYN/ACK設定了其他標誌(PSH、URG、FIN)。 3. 接收具有負載的傳輸SYN。 4. 從啟動器接收非SYN資料包。
處於SYNRCVD狀態的段無效	處於SYNRCVD狀態的無效TCP資料段可能是由以下原因造成的： 1. 從發起方接收具有負載的重傳SYN。 2. 從響應方接收非SYN/ACK、RST或FIN的無效資料段。
無效的SEQ	當資料段來自發起方時，此情況發生在SYNRCVD狀態。其原因是： 1. Seq#小於ISN。 2. 如果接收器rcvd視窗大小為0且： 段有負載，或 亂序段(seq#)大於接收器LASTACK。

	3. 如果接收器rcvd視窗大小為0，並且seq#超出視窗。 4. Seq#等於ISN但不等於SYN資料包。
視窗縮放選項無效	無效的TCP視窗縮放選項是由錯誤的視窗縮放選項位元組長度導致的。
TCP超出視窗	資料包太舊 — 位於另一端ACK後面的一個視窗。這可能發生在ESTABL
傳送FIN之後的TCP額外負載	傳送FIN後收到負載。這可能發生在CLOSEWAIT狀態。
TCP視窗溢位	當傳入段大小溢位接收器的視窗時，會發生這種情況。但是，如果啟用v
具有無效標誌的重傳	重新傳輸的資料包已由接收器確認。
TCP無序區段	無序資料包將傳送到L7進行檢查。如果L7不允許OOO段，此資料包將被
SYN泛洪	在TCP SYN泛洪攻擊下。在某些情況下，當當前與此主機的連線超過配置 被丟棄。
內部錯誤 — synflood檢查分配失敗	在synflood檢查期間， hostdb分配失敗。 建議的操作：檢查「show platform hardware qfp active feature firewall r
Synflood封鎖下降	如果超過已配置的半開放連線且已配置封鎖時間，則會丟棄與此IP地址的
超過半開啟會話限制	由於超出允許的半開啟會話數而丟棄的資料包。 還要檢查「max-incomplete high/low」和「one-minute high/low」的設定
每個流的Pkt太多	超出每個流允許的最大可檢查資料包數。最大值為25。
每個流的ICMP錯誤資料包過多	超出每個流允許的最大ICMP錯誤資料包數。最大值為3。
從Rsp到Init的不期望TCP負載	在SYNRCVD狀態下，TCP從響應方到發起方方向接收具有負載的資料包
內部錯誤 — 未定義方向	未定義資料包方向。
當前視窗中的SYN	在已建立TCP連線的視窗中會看到SYN封包。
當前視窗中的RST	在已建立TCP連線的視窗中觀察到RST封包。
散亂資料段	接收不應通過TCP狀態機接收的TCP資料段，例如以偵聽狀態從響應方接
ICMP內部錯誤 — 丟失的ICMP NAT資訊	ICMP資料包已nat，但內部NAT資訊丟失。這是一個內部錯誤。
處於SCB關閉狀態的ICMP資料包	已收到SCB CLOSE狀態的ICMP封包。
ICMP資料包中的IP報頭丟失	ICMP資料包中缺少IP報頭。
ICMP錯誤無IP或ICMP	負載中沒有IP或ICMP的ICMP錯誤資料包。可能由格式錯誤的資料包或攻
ICMP Err Pkt太短	ICMP錯誤資料包太短。
ICMP錯誤超過突發限制	ICMP錯誤pkt超過了突發限制10。
無法連線的ICMP錯誤	ICMP錯誤pkt無法到達超出限制。僅允許第一個無法到達的封包通過。
ICMP錯誤無效的Seq#	嵌入式資料包的seq#與導致ICMP錯誤的資料包的seq#不匹配。
ICMP錯誤無效Ack	嵌入的ICMP錯誤資料包中的ACK無效。
ICMP操作丟棄	配置的ICMP操作被丟棄。
無策略對映的區域對	區域對上不存在策略。這可能是由於ALG（應用層網關）未配置為開啟應
會話丟失且策略不存在	會話查詢失敗，並且不存在檢查此資料包的策略。
ICMP錯誤和策略不存在	ICMP錯誤，沒有在區域對上配置策略。
分類失敗	當防火牆嘗試確定協定是否可以檢查時，指定區域對中的分類失敗。
分類操作刪除	分類操作已刪除。
安全策略配置錯誤	由於安全策略配置錯誤，分類失敗。這也可能是因為L7資料通道沒有針腳
將RST傳送到響應方	當ACK#不等於ISN+1時，將RST傳送到處於SYNSEND狀態的響應方。
防火牆策略丟棄	策略操作是刪除。
片段捨棄	捨棄第一個片段時捨棄其餘片段。
ICMP防火牆原則捨棄	ICMP嵌入式資料包的策略操作為DROP。
L7檢查返回DROP	L7(ALG)決定捨棄封包。從不同的ALG統計資訊中可以找到原因。
L7段Pkt Not Allow	當ALG不執行分段資料包時，收到該資料包。
L7片段封包不允許	當ALG不執行分段資料包（或VFR）時。
未知的L7原型型別	無法識別的協定型別。

防火牆捨棄疑難排解

從上述全域性或防火牆功能丟棄計數器識別出丟棄原因後，如果出現意外丟棄，可能需要執行其他故障排除步驟。除了配置驗證以確保已啟用的防火牆功能的配置正確之外，通常還需要對有問題的流量進行資料包捕獲，以確定資料包是否格式不正確或者是否存在任何協定或應用程式實施問題。

記錄

ASR日誌記錄功能會生成系統日誌以記錄丟棄的資料包。這些系統日誌提供有關資料包被丟棄原因的更多詳細資訊。系統日誌有兩種型別：

1. 本地緩衝系統日誌

2. 遠端高速日誌記錄

本地緩衝系統日誌

為了找出丟棄的原因，您可以使用通用的ZBFW故障排除，例如啟用日誌丟棄。配置資料包丟棄日誌記錄有兩種方法。

方法1:使用inspect-global parameter-map記錄所有丟棄的資料包。

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

方法2:使用自定義inspect引數對映僅記錄特定類的丟棄資料包。

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

這些消息傳送到日誌或控制檯，具體取決於ASR的日誌配置方式。以下是丟棄日誌消息的示例。

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

本地緩衝系統日誌的侷限性

1. 根據思科錯誤ID CSCud09943，這些日誌的速率受限。

2. 除非應用特定配置，否則可能不會列印這些日誌。例如，除非指定了log關鍵字，否則不會記錄由class-default資料包丟棄的資料包：

```
policy-map type inspect ZBFW_PMAP
```

```
class class-default
drop log
```

遠端高速日誌記錄

高速日誌記錄(HSL)直接從QFP生成系統日誌，並將其傳送到配置的netflow HSL收集器。這是推薦的ASR ZBFW日誌記錄解決方案。

對於HSL，使用以下配置：

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

要使用此配置，需要具備Netflow版本9功能的netflow收集器。詳情見

[配置指南：基於區域的策略防火牆，Cisco IOS XE版本3S(ASR 1000)防火牆高速日誌記錄]

使用條件匹配的資料包跟蹤

開啟條件式偵錯以啟用封包追蹤，然後為這些功能啟用封包追蹤：

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

> **附註**：匹配條件可以直接使用IP地址，因為不需要使用ACL。這將匹配為允許雙向跟蹤的源或目標。如果不允許您更改配置，可以使用此方法。例如：debug platform condition ipv4 address 192.168.1.1/32。

開啟封包追蹤功能：

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

使用此功能的方式有兩種：

1. 輸入**debug platform packet-trace drop**命令以僅跟蹤丟棄的資料包。
2. 排除命令**debug platform packet-trace drop**將跟蹤與條件匹配的任何資料包，包括裝置檢查/通過的資料包。

啟用條件調試：

```
debug platform condition start
```

運行測試，然後關閉調試：

```
debug platform condition stop
```

現在資訊可以顯示在螢幕上。在此範例中，ICMP封包由於防火牆原則而被捨棄：

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

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

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

show platform packet-trace packet <num> decode命令會解碼封包標頭資訊和內容。此功能是在XE3.11中引入的：

```
Router#show platform packet-trace packet all decode
Packet: 0           CBUG ID: 2980
Summary
```

```
 Input     : GigabitEthernet0/0/2
 Output    : GigabitEthernet0/0/0
 State     : DROP 183 (FirewallPolicy)
 Timestamp
   Start   : 1207843476722162 ns (04/15/2014 12:37:01.103864 UTC)
   Stop    : 1207843477247782 ns (04/15/2014 12:37:01.104390 UTC)
Path Trace
 Feature: IPV4
    Source      : 10.1.1.1
    Destination : 192.168.1.1
    Protocol    : 1 (ICMP)
  Feature: ZBFW
    Action  : Drop
    Reason  : ICMP policy drop:classify result
    Zone-pair name  : INSIDE_OUTSIDE_ZP
    Class-map name  : class-default
Packet Copy In
 c89c1d51 5702000c 29f9d528 08004500 00540000 40004001 ac640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
 ARPA
    Destination MAC     : c89c.1d51.5702
    Source MAC          : 000c.29f9.d528
   Type               : 0x0800 (IPV4)
 IPv4
   Version            : 4
   Header Length      : 5
   ToS                : 0x00
   Total Length       : 84
   Identifier         : 0x0000
   IP Flags           : 0x2 (Don't fragment)
   Frag Offset        : 0
   TTL                : 64
   Protocol           : 1 (ICMP)
   Header Checksum    : 0xac64
   Source Address     : 10.1.1.1
   Destination Address : 192.168.1.1
 ICMP
   Type               : 8 (Echo)
   Code               : 0 (No Code)
   Checksum           : 0x172a
   Identifier         : 0x2741
   Sequence           : 0x0001
Packet Copy Out
 c89c1d51 5702000c 29f9d528 08004500 00540000 40003f01 ad640e26 70fa0e24
 01010800 172a2741 00016459 4d5310e4 0c000809 0a0b0c0d 0e0f1011 12131415
 ARPA
   Destination MAC     : c89c.1d51.5702
   Source MAC          : 000c.29f9.d528
   Type               : 0x0800 (IPV4)
 IPv4
   Version            : 4
   Header Length      : 5
   ToS                : 0x00
   Total Length       : 84
   Identifier         : 0x0000
   IP Flags           : 0x2 (Don't fragment)
   Frag Offset        : 0
   TTL                : 63
   Protocol           : 1 (ICMP)
   Header Checksum    : 0xad64
   Source Address     : 10.1.1.1
   Destination Address : 192.168.1.1
 ICMP
   Type               : 8 (Echo)
```

```
Code                : 0 (No Code)
Checksum            : 0x172a
Identifier          : 0x2741
Sequence            : 0x0001
```

內嵌式封包擷取

Cisco IOS-XE 3.7(15.2(4)S)中增加了嵌入式封包擷取支援。 有關詳細資訊，請參閱

適用於Cisco IOS和IOS-XE的嵌入式封包擷取組態範例。

調試

條件調試

在XE3.10中，將引入條件調試。可以使用條件語句來確保ZBFW功能只記錄與條件相關的調試消息。條件式調試使用ACL來限制與ACL元素匹配的日誌。此外，在XE3.10之前，調試消息更難以讀取。在XE3.10中改進了調試輸出，使其更易於理解。

若要啟用這些調試，請發出以下命令：

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

請注意，條件命令必須通過ACL和方向性進行設定。使用命令**debug platform condition start**啟動條件調試之前，不會實現條件調試。要關閉條件調試，請使用**debug platform condition stop**命令。

```
debug platform condition stop
```

要關閉條件調試，**請勿使**用**undebug all**命令。若要關閉所有條件調試，請使用命令：

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

在XE3.14之前，**ha**和**event**調試不是有條件的。因此，命令**debug platform condition**功能fw **dataplane submode all**將導致建立所有日誌，而與下面選擇的條件無關。這可能會產生額外的噪音，使調試變得困難。

預設情況下，條件日誌記錄級別為**info**。要增加/減少日誌記錄級別，請使用命令：

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

收集並檢視調試

調試檔案不會列印到控制檯或監視器。所有調試都寫入到ASR的硬碟中。將調試寫入硬碟中名為**cpp_cp_F0-0.log.<date>**的資料夾**tracelogs**下。若要檢視寫入偵錯的檔案，請使用輸出：

```
ASR# cd harddisk:
ASR# cd tracelogs
```

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

Directory of harddisk:/tracelogs/

3751962 -rwx 1048795 Jun 15 2010 06:31:51 +00:00
cpp_cp_F0-0.log.5375.20100615063151
3751967 -rwx 1048887 Jun 15 2010 02:18:07 +00:00
cpp_cp_F0-0.log.5375.20100615021807
39313059840 bytes total (30680653824 bytes free)
```

每個調試檔案將儲存為cpp_cp_F0-0.log.<date>文件。這些是可通過TFTP從ASR複製的常規文本檔案。ASR上的日誌檔案最大為1Mb。1Mb後，調試將寫入新的日誌檔案。因此，每個日誌檔案都會加上時間戳以指示檔案的開始。

日誌檔案可能存在於以下位置：

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

由於日誌檔案僅在輪替後顯示，因此可以使用以下命令手動輪替日誌檔案：

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

這將立即建立一個「cpp_cp」日誌檔案，並在QFP上啟動一個新的日誌檔案。例如：

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

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

此指令允許將偵錯檔案合併到單一檔案中，以便更容易處理。它合併目錄中的所有檔案，並根據時間進行交錯。當日誌非常冗長並且跨多個檔案建立時，這可以有所幫助：

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

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