IOS-XE 用の ZBFW 設定のトラブルシューティング ガイド

内容

概要

このドキュメントでは、アグリゲーション サービス ルータ（ASR）上のハードウェア ドロップ カウンタをポーリングするコマンドを使用して、ASR 1000 のゾーンベース ファイアウォール（ZBFW）機能をトラブルシューティングするベスト プラクティスについて説明します。ASR 1000 はハードウェアベースの転送プラットフォームです。Cisco IOS-XE® のソフトウェア設定によって、ハードウェア ASIC Quantum Flow Processor（QFP）が機能転送機能を実行するようにプログラムできます。これにより、スループットが増加し、パフォーマンスが向上します。欠点は、トラブルシューティングがやりにくいことです。これまでゾーンベース ファイアウォール（ZBFW）経由で現在のセッションとドロップ カウンタをポーリングするために使用されていた Cisco IOS コマンドは、ソフトウェアでドロップが行われなくなったため、無効になっています。

リンクおよびドキュメント

コマンド リファレンス

- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ コマンド リファレンス
- Cisco IOS XE 3S コマンド リファレンス

データパス トラブルシューティング手順

データパスをトラブルシューティングするには、トラフィックが ASR と Cisco IOS-XE のコードを正しくパス スルーするかどうかを確認する必要があります。ファイアウォール機能に特有のデータパスのトラブルシューティングは次の手順に従います。

1. **設定の確認：設定を収集して、出力を調査し、接続を確認します。**

2. **接続状態の確認：トラフィックが正しく通過する場合は、Cisco IOS-XE が ZBFW 機能の接続を有効にします。**この接続は、クライアントとサーバ間のトラフィックと状態情報を追跡します。

3. **ドロップ カウンタの確認：トラフィックが正しく通過しない場合は、Cisco IOS-XE がドロップされたパケットに関するドロップ カウンタを記録します。**この出力をチェックして、トラフィック障害の原因を特定します。

4. **ロギング：syslog を収集して、接続の構築やパケットのドロップに関するより詳細な情報を調査します。**

5. **パケット トレース ドロップ パケット：パケット トレースを使用して、ドロップされたパケットを収集します。**

6. **デバッグ：デバッグの収集は最も冗長なオプションです。**デバッグは、パケットの正確な転送パスを確認するために、条件付きで入手できます。

設定の確認

show tech support firewall の出力を以下に示します。

```
-------- 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> --------
```

接続状態の確認

接続情報を入手すれば、ZBFW 上のすべての接続を網羅することができます。次のコマンドを入力します。

```
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]
```

これは、14.38.112.250 と 14.36.1.206 間の TCP Telnet 接続を表示します。

> **注**：このコマンドを実行すると、デバイス上の接続数が多い場合に時間がかかることに注意してください。このコマンドは、次のように、特定のフィルタを指定して実行することをお勧めします。

接続テーブルは、特定の送信元アドレスまたは宛先アドレスに絞り込むことができます。**platform サブモードの後でフィルタを使用します。**フィルタリングのオプションを以下に示します。

```
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>
```

この接続テーブルは、14.38.112.250 からの接続だけが表示されるようにフィルタリングされています。

```
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]
```

接続テーブルをフィルタリングすれば、詳細な接続情報を入手してより包括的な分析を行うことができます。この出力を表示するには、**detail キーワードを使用します。**

```
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
```

ファイアウォール ドロップ カウンタのチェック

ドロップカウンタの出力は、XE 3.9で変更されました。XE 3.9より前のバージョンでは、ファイアウォールのドロップの理由は非常に一般的でした。XE 3.9 以降は、ファイアウォール ドロップの理由が拡張され、より詳しくなりました。

ドロップ カウンタを確認するには、次の 2 つのステップを実行します。

1. Cisco IOS-XE でグローバル ドロップ カウンタを確認します。このカウンタは、どの機能がトラフィックをドロップしたかを示します。機能の例として、Quality of Service（QoS）、ネットワーク アドレス変換（NAT）、ファイアウォールなどが挙げられます。

2. サブ機能が特定された場合は、サブ機能によって提供される詳細なドロップ カウンタを照会します。このガイドでは、分析対象のサブ機能がファイアウォール機能です。

QFP 上のグローバル ドロップ カウンタ

基になる基本コマンドは QFP 上のすべてのドロップを提供します。

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

このコマンドは QFP 上のドロップをまとめて表示します。このドロップには任意の機能を含めることができます。機能の例を以下に示します。

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

すべてのドロップを表示するには、値が 0 のカウンタを追加して、次のコマンドを使用します。

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

カウンタをクリアするには、次のコマンドを使用します。これは、画面に表示された出力をクリアします。このコマンドは読み取り時クリアされるため、出力は画面に表示された**後で 0 にリセットされます。**

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

QFP グローバル ファイアウォール ドロップ カウンタと説明のリストを以下に示します。

ファイアウォール グローバル ドロップの理由	説明
FirewallBackpressure	ロギング メカニズムによるバックプレッシャが原因のパケット ドロップ。
FirewallInvalidZone	インターフェイス用に設定されたセキュリティ ゾーンが存在しません。
FirewallL4Insp	L4 ポリシー チェック エラー。より詳細なドロップの理由については、次の表 てください。
FirewallNoForwardingZone	ファイアウォールが初期化されておらず、トラフィックが通過を許可されて
FirewallNonsession	セッションの作成が失敗します。これは、最大セッション制限に到達したか
FirewallPolicy	設定されたファイアウォール ポリシーがドロップになっています。
FirewallL4	L4 検査エラー。より詳細なドロップの理由については、次の表（ファイアウ
FirewallL7	L7 検査が原因のパケット ドロップ。より詳細な L7 ドロップの理由のリスト プの理由）を参照してください。
FirewallNotInitiator	TCP、UDP、または ICMP のセッション イニシエータが存在しません。セッ は、受信された最初のパケットが ECHO でも TIMESTAMP でもありません。 この現象は、通常のパケット処理または不正確なチャネル処理で発生する可
FirewallNoNewSession	ファイアウォール ハイ アベイラビリティで新しいセッションが許可されませ
FirewallSyncookieMaxDst	ホストベースの SYN フラッド保護を提供するために、SYN フラッド制限と トリの数が上限に達すると、新しい SYN パケットがドロップされます。
FirewallSyncookie	SYNCOOLIE ロジックがトリガーされます。これは、SYN Cookie を含む SY されたことを示します。
FirewallARStandby	非対称ルーティングが有効になっておらず、冗長グループがアクティブ状態

QFP 上のファイアウォール機能ドロップ カウンタ

QFP グローバル ドロップ カウンタに伴う制限はドロップの理由が細分化されないことであり、**FirewallL4** などの一部のドロップの理由によって特定の箇所に過負荷が生じ、ほとんどトラブルシューティングに使用できません。これは、ファイアウォール機能ドロップ カウンタが追加された Cisco IOS-XE 3.9（15.3(2)S）以降で改善されています。これにより、ドロップのかなり詳細な理由のセットが提供されます。

```
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
....
```

ファイアウォール機能ドロップの理由と説明のリストを以下に示します。

ファイアウォール機能ドロップの理由	説明
Invalid Header length	データグラムが非常に小さいため、レイヤ4TCP、UDP、またはI 1. TCP ヘッダー長 < 20 2. UDP/ICMP ヘッダー長 < 8
Invalid UDP data length	UDP データグラム長が UDP ヘッダーで指定された長さと一致し このドロップは、次の理由のいずれかで発生する可能性がありま
Invalid ACK Number	1. ACK が TCP ピアの next_seq# と一致しない。 2. ACK が TCP ピアから送信された最新の SEQ# を超えている

Invalid ACK Flag	TCP SYNRCVD 状態と SYNSENT 状態では、ACK# が ISN+1 に このドロップは、次の理由のいずれかで発生する可能性があります 1. ACK フラグが想定されているが、別の TCP 状態でセットさ 2. ACK フラグ以外の他のフラグ（RST など）もセットされる。
Invalid TCP Initiator	この状態が発生するのは、以下の場合です。 1. TCP イニシエータからの最初のパケットが SYN ではない（ 2. 初期 SYN パケットで ACK フラグがセットされている。
SYN with data	SYN パケットにペイロードが含まれています。そのような使用方
Invalid TCP Flags	無効な TCP フラグの原因を以下に示します。 1. TCP 初期 SYN パケットに SYN 以外のフラグが含まれてい 2. TCP リッスン状態で、TCP ピアが RST または ACK を受信 3. 他のレスポンダのパケットが SYN/ACK の前に受信される。 4. 想定された SYN/ACK がレスポンダから受信されない。
Invalid Segment in SYNSENT state	SYNSENT 状態の無効な TCP セグメントの原因を以下に示します 1. SYN/ACK にペイロードが含まれている。 2. SYN/ACK に他のフラグ（PSH、URG、FIN）がセットされ 3. ペイロードを含む通過 SYN を受信する。 4. イニシエータから非 SYN パケットを受信する。
Invalid Segment in SYNRCVD state	SYNRCVD 状態の無効な TCP セグメントの原因を以下に示します 1. イニシエータからペイロードを含む再通過 SYN を受信する。 2. レスポンダから SYN/ACK、RST、または FIN 以外の無効な これは、セグメントがイニシエータから届いたときに SYNRCVD
Invalid SEQ	1. Seq# が ISN 未満である。 2. レシーバの rcvd ウィンドウ サイズが 0 で、 セグメントにペイロードまたは 不正なセグメント（seq# がレシーバ LASTACK を超えてい 3. レシーバの rcvd ウィンドウ サイズが 0 で、seq# がウィンド 4. Seq# が ISN と一致するが、SYN パケットと一致しない。
Invalid Window Scale Option	無効な TCP ウィンドウ スケール オプションは、誤ったウィンド
TCP out of window	パケットが古すぎます。あるウィンドウが相手側の ACK より遅れ 生する可能性があります。
TCP extra payload after FIN sent	ペイロードが FIN の送信後に受信されました。これは、CLOSEW
TCP Window Overflow	これは、入力セグメント サイズがレシーバのウィンドウを超えた されます。これは、ファイアウォールが後で使用する ALG のセク
Retran with Invalid Flags	再通過パケットがすでにレシーバによって確認応答されています。
TCP out-of-order Segment	不正なパケットが検査用に L7 に配信されようとしています。L7
SYN フラッド	TCP SYN フラッド攻撃を受けています。特定の条件下で、このホ ールはこの IP アドレスへの新しい接続を一定期間拒否します。そ
Internal Err - synflood check alloc Failed	synflood チェック中に、hostdb の割り当てに失敗します。 推奨アクション："show platform hardware qfp active feature firew
Synflood blackout drop	設定されたハーフオープン接続数を超過し、ブラックアウト時間 れます。
Half-Open Session Limit Exceed	許容ハーフオープン セッション数を超過したためにパケットがド また、"max-incomplete high/low" と "one-minute high/low" の設定 ことを確認します。
Too Many Pkt per flow	フローごとに許可される検査可能パケットの最大数を超えていま
Too many ICMP error packets per flow	フローごとに許可される ICMP エラー パケットの最大数を超えて
Unexpect TCP payload from Rsp to	SYNRCVD 状態では、TCP がレスポンダからイニシエータの方向

Init	
Internal Error - Undefined Direction	パケット方向が定義されていません。
SYN inside current window	SYN パケットが、すでに確立された TCP 接続のウィンドウ内で
RST inside current window	RST パケットが、すでに確立された TCP 接続のウィンドウ内で
Stray Segment	レスポンダからリッスン状態で受信される TCP SYN パケットな す。
ICMP Internal Error - Missed ICMP NAT info	ICMP パケットが NAT されていますが、内部 NAT 情報が見つか
ICMP packet in SCB close state	SCB CLOSE 状態で ICMP パケットが受信されました。
Missed IP header in ICMP packet	ICMP パケット内に IP ヘッダーがありません。
ICMP Error No IP or ICMP	ペイロード内に IP または ICMP がない ICMP エラー パケット。
ICMP Err Pkt Too Short	ICMP エラー パケットが短すぎます。
ICMP Err Exceed Burst Limit	ICMP エラー パケットが 10 のバースト制限を超えています。
ICMP Err Unreachable	到達不能な ICMP エラー パケットが制限を超えています。最初の
ICMP Err Invalid Seq#	組み込みパケットの seq# が ICMP エラーを引き起こすパケットの
ICMP Err Invalid Ack	ICMP エラー組み込みパケット内の無効な ACK。
ICMP action drop	設定された ICMP アクションがドロップになっています。
Zone-pair without policy-map	ゾーン ペアに対するポリシーが存在しません。アプリケーション トウェイ）が設定されていないか、ALG がピンホールを正しく開 あります。
Session Missed And Policy Not Present	セッション ルックアップが失敗して、このパケットを検査するポ
ICMP Error And Policy Not Present	ゾーン ペアに対するポリシーが設定されていない ICMP エラー。
Classification Failed	プロトコルが検査可能かどうかをファイアウォールが判断しよう
Classification Action Drop	分類アクションがドロップになっています。
Security Policy Misconfig	セキュリティ ポリシーの誤設定によって分類が失敗しました。こ ます。
Send RST to responder	ACK# が ISN+1 と一致しないときに SYNSENT 状態でレスポンダ
Firewall Policy Drop	ポリシー アクションがドロップになっています。
Fragment Drop	最初のフラグメントがドロップされると、残りのフラグメントも
ICMP Firwall Policy Drop	ICMP 組み込みパケットのポリシー アクションがドロップになっ
L7 inspection returns DROP	L7（ALG）がパケットのドロップを決定します。理由は、さまざ
L7 Segment Pkt Not Allow	ALG が受け付けないセグメント化されたパケットが受信されまし
L7 Fragment Pkt Not Allow	ALG が受け付けないフラグメント化されたパケット（または VFR
Unknown L7 Proto Type	認識されないプロトコル タイプです。

ファイアウォール ドロップのトラブルシューティング

前述したグローバルまたはファイアウォール機能ドロップ カウンタからドロップの理由が特定されたが、それらのドロップが想定されていなかった場合は、追加のトラブルシューティング手順が必要になります。有効になっているファイアウォール機能に対して設定が正しいことを保証するための設定検証は別として、大抵の場合は、疑わしいトラフィック フローのパケット キャプチャを取って、パケットが不正かどうか、プロトコルまたはアプリケーションの実装上の問題が発生していないかどうかを確認する必要があります。

Logging

ASR ロギング機能は、ドロップされたパケットを記録する syslog を生成します。この syslog は、パケットがドロップされた理由の詳細を提供します。次の 2 種類の syslog があります。

1. ローカル バッファ syslog

2. リモート高速ロギング

ローカル バッファ syslog

ドロップの原因を特定するには、ログ ドロップの有効化などの一般的な ZBFW トラブルシューティングを使用できます。パケット ドロップ ロギングを設定するには、次の 2 つの方法があります。

方法 1：すべてのドロップされたパケットを記録するためにインスペクト グローバル パラメータ マップを使用します。

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

方法 2：特定のクラスのみのドロップされたパケットを記録するためにカスタム インスペクト パラメータ マップを使用します。

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

ASR がロギング用にどのように設定されているかに応じて、次のメッセージがログまたはコンソールに送信されます。ドロップ ログ メッセージの例を以下に示します。

```
*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
```

ローカル バッファ syslog の制限

1. このログは、Cisco Bug ID CSCud09943 によってレート制限されています。

2. このログは、特定の設定が適用されていない限り、出力されません。たとえば、**log キーワードが指定されなかった場合は、class-default パケットによってドロップされたパケットが記録されません。**

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

リモート高速ロギング

高速ロギング（HSL）は、QFP から直接 syslog を生成し、それを設定された NetFlow HSL コレクタに送信します。これは、ASR 上の ZBFW に対して推奨されているロギング ソリューションです。

HSL では、次の設定を使用します。

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

この設定を使用するには、NetFlow バージョン 9 の NetFlow コレクタ機能が必要です。これについては、以下を参照してください。

『設定ガイド：ゾーンベース ポリシー ファイアウォール Cisco IOS XE Release 3S（ASR 1000）ファイアウォール高速ロギング』

条件一致を使用したパケット トレース

パケット トレースを有効にしてから、次の機能のパケット トレースを有効にするには、条件付きデバッグをオンにします。

```
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
```

> **注：**ACL が必要ないため、照合条件で直接 IP アドレスを使用できます。これは、双方向トレースを許可する送信元または宛先として照合されます。この方法は、設定の変更が許可されていない場合に使用できます。以下に、いくつかの例を示します。debug platform condition ipv4 address 192.168.1.1/32

packet-tracing 機能をオンにします。

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

この機能を使用するには、次の 2 つの方法があります。

1. ドロップされたパケットだけをトレースするには、**debug platform packet-trace drop コマンドを入力します。**
2. **debug platform packet-trace drop コマンドを除外すると、デバイスで検査/転送されるものを含め、条件と一致するパケットが追跡されます。**

条件付きデバッグをオンにします。

```
debug platform condition start
```

テストを実行してから、デバッグをオフにします。

```
debug platform condition stop
```

これで、情報を画面上に表示できます。この例では、ファイアウォール ポリシーが原因で ICMP パケットがドロップされています。

```
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 コマンドは、パケット ヘッダー情報とコンテンツをデコードします。この機能は XE3.11 で導入されました。

```
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
```

Embedded Packet Capture

Embedded Packet Capture のサポートが Cisco IOS XE 3.7 (15.2(4)S) で追加されました。 詳細を参照してください。

『Cisco IOS と IOS XE の組み込みパケット キャプチャの設定例』

デバッグ

条件付きデバッグ

XE3.10 で、条件付きデバッグが導入されます。条件文を使用して、ZBFW 機能が条件に関するデバッグ メッセージのみを記録することを保証することができます。条件付きデバッグは、ACL を使用して、ACL 要素と一致するログを制限します。また、XE3.10 以前は、デバッグ メッセージを読むのが大変でした。XE3.10 では、デバッグ出力が読みやすく改良されています。

このデバッグを有効にするには、次のコマンドを発行します。

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

条件コマンドは ACL と方向性を指定して設定する必要があることに注意してください。条件付きデバッグは、**debug platform condition start** コマンドを使用して開始されるまで実装されません。条件付きデバッグをオフにするには、**debug platform condition stop** コマンドを使用します。

```
debug platform condition stop
```

条件付きデバッグをオフにするために、**undebug all コマンドを使用しない**でください。すべての条件付きデバッグをオフにするには、次のコマンドを使用します。

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

XE3.14 以前は、**ha と event デバッグが条件付きではありませんでした。**そのため、以下で選択される条件に関係なく、**debug platform condition feature fw dataplane submode all コマンドによってすべてのログが作成されます。**これにより、デバッグを困難にする不要な情報が追加される場合があります。

デフォルトで、条件付きロギング レベルは **info** です。ロギング レベルを上げ下げするには、次のコマンドを使用します。

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

デバッグの収集と表示

デバッグ ファイルはコンソールまたはモニタに出力されません。すべてのデバッグが ASR のハードディスクに書き込まれます。デバッグは、ハードディスクのフォルダ **tracelogs の下に、cpp_cp_F0-0.log.<date>** という名前で書き込まれます。デバッグが書き込まれたファイルを確認するには、次の出力を使用します。

```
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)
```

各デバッグ ファイルは **cpp_cp_F0-0.log.<date> ファイルとして保存されます。**これらは、TFTP を使用して ASR をコピー可能な通常のテキスト ファイルです。ASR 上のログ ファイルの上限は 1 MB です。1 MB を超えると、デバッグが新しいログ ファイルに書き込まれます。このために、各ログ ファイルにはファイルの開始を示すタイムスタンプが付けられます。

ログ ファイルは、次の場所に保存することができます。

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

ログ ファイルはローテート後にしか表示されないため、次のコマンドを使用して手動でローテートすることができます。

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

これにより、QFP 上で "cpp_cp" ログ ファイルが即座に作成され、新しいファイルが開始されます。以下に、いくつかの例を示します。

```
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)
```

このコマンドを使用すれば、デバッグ ファイルを処理しやすいように単一のファイルにマージすることができます。このコマンドは、ディレクトリ内のすべてのファイルをマージして時系列に整理します。これは、ログが非常に冗長で、複数のファイルにまたがっている場合に便利です。

```
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]
```