Guida alla risoluzione dei problemi di configurazione di ZBFW per IOS-XE

Sommario

Introduzione

Questo documento descrive come risolvere al meglio la funzione Zone Based Firewall (ZBFW) su Aggregation Services Router (ASR) 1000, con comandi che vengono usati per interrogare i contatori di rilascio dell'hardware sull'ASR. ASR1000 è una piattaforma di inoltro basata su hardware. La configurazione software dei programmi Cisco IOS-XE® comprende gli ASIC (Quantum Flow Processor), che permettono di eseguire le funzionalità di inoltro delle caratteristiche. Ciò consente un throughput più elevato e prestazioni migliori. Lo svantaggio è che rappresenta una sfida maggiore per la risoluzione dei problemi. I comandi tradizionali di Cisco IOS utilizzati per eseguire il polling delle sessioni correnti e dei contatori di rilascio tramite Zone-Based Firewall (ZBFW) non sono più validi perché le perdite non sono più presenti nel software.

Link e documentazione

Riferimenti per i comandi

- Riferimenti per i comandi di Cisco ASR serie 1000 Aggregation Services Router
- Riferimenti per i comandi Cisco IOS XE 3S

Procedura di risoluzione dei problemi di Datapath

Per risolvere i problemi relativi al percorso dei dati, è necessario identificare se il traffico viene passato correttamente tramite il codice ASR e Cisco IOS-XE. Per risolvere i problemi relativi ai percorsi dei dati specifici delle funzionalità del firewall, procedere come segue:

1. **Verify Configuration** (Verifica configurazione) - Raccogliere la configurazione ed esaminare l'output per verificare la connessione.

2. **Verifica dello stato della connessione** - Se il traffico passa correttamente, Cisco IOS-XE apre una connessione sulla funzione ZBFW. Questa connessione tiene traccia delle informazioni sul traffico e sullo stato tra un client e un server.

3. **Verify Drop Counters** - Quando il traffico non passa correttamente, Cisco IOS-XE registra un contatore di rilascio per tutti i pacchetti ignorati. Controllare questo output per isolare la causa dell'errore di traffico.

4. **Registrazione** - Raccoglie i syslog per fornire informazioni più granulari sulle build di connessione e le perdite di pacchetti.

5. **Packet Trace Dropped Packets**: utilizzare la funzione di traccia dei pacchetti per rilevare i pacchetti ignorati.

6. **Debug** - L'opzione di raccolta dei debug è la più dettagliata. È possibile ottenere i debug in modo condizionale per confermare il percorso esatto di inoltro dei pacchetti.

Verifica configurazione

L'output di **show tech support firewall** è riepilogato qui:

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

Verifica stato connessione

Èpossibile ottenere informazioni sulla connessione in modo da elencare tutte le connessioni su ZBFW. Immettere questo comando:

```
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]
```

Indica una connessione Telnet TCP tra le 14.38.12.250 e le 14.36.1.206.

> **Nota:** Se si esegue questo comando, la presenza di numerose connessioni nel dispositivo richiederà molto tempo. Cisco consiglia di eseguire questo comando con i filtri specifici descritti qui.

La tabella di connessione può essere filtrata in base a un indirizzo di origine o di destinazione specifico. Usa i filtri dopo la modalità secondaria **della piattaforma**. Le opzioni da filtrare sono:

```
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>
```

Questa tabella di connessione è filtrata in modo da visualizzare solo le connessioni originate da 14.38.12.250:

```
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]
```

Una volta filtrata la tabella di connessione, è possibile ottenere informazioni dettagliate sulla connessione per un'analisi più completa. Per visualizzare questo output, usare la parola chiave **detail**.

```
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
```

Controlla contatori di rilascio firewall

L'output del contatore di rilascio è cambiato durante XE 3.9. Prima di XE 3.9, i motivi di rilascio del firewall erano molto generici. Dopo XE 3.9, le cause di caduta del firewall sono state estese per diventare più granulari.

Per verificare i contatori di rilascio, effettuare due operazioni:

1. Confermare i contatori di rilascio globali in Cisco IOS-XE. Questi contatori mostrano la funzionalità che ha interrotto il traffico. Esempi di funzionalità includono Quality of Service (QoS), Network Address Translation (NAT), Firewall e così via.

2. Una volta identificata la sottofunzionalità, eseguire una query sui contatori di rilascio granulari offerti dalla sottofunzionalità. In questa guida, la sottofunzionalità analizzata è la funzionalità Firewall.

Contatori globali di eliminazione su QFP

Il comando di base su cui fare affidamento fornisce tutte le interruzioni in QFP:

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

Questo comando mostra i rilasci generici a livello globale in QFP. Queste gocce possono essere su qualsiasi funzione. Di seguito sono riportati alcuni esempi di funzionalità:

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

Per visualizzare tutte le perdite, includere i contatori con valore zero, utilizzare il comando:

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

Per cancellare i contatori, usare questo comando. Cancella l'output dopo averlo visualizzato sullo

schermo. Questo comando non è impostato durante la lettura, quindi l'output viene reimpostato su zero **dopo** che viene visualizzato sullo schermo.

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

Di seguito è riportato un elenco dei contatori delle perdite del firewall globale QFP e una spiegazione:

Motivo eliminazione globale firewall	Spiegazione
Contropressione firewall	Perdita di pacchetti a causa della contropressione da parte del meccanis di registrazione.
ZonaNonValidaFirewall	Nessuna area di sicurezza configurata per l'interfaccia.
FirewallL4Insp	Errore di controllo criteri L4. Vedere la tabella seguente per motivi di rila più granulari (motivi di rilascio delle funzionalità del firewall).
FirewallNoForwardingZone	Firewall non inizializzato. Traffico non consentito.
Non sessione firewall	Creazione della sessione non riuscita. La causa potrebbe essere il raggiungimento del limite massimo di sessioni o un errore di allocazione della memoria.
CriterioFirewall	Il criterio firewall configurato è stato eliminato.
FirewallL4	Errore di ispezione L4. Vedere la tabella seguente per motivi di rilascio p granulari (motivi di rilascio della funzionalità firewall).
FirewallL7	Perdita del pacchetto a causa dell'ispezione L7. Vedere di seguito per u elenco dei motivi di rilascio più granulari di L7 (motivi di rilascio delle funzionalità del firewall).
NonIniziatoreFirewall	Non è un iniziatore di sessione per TCP, UDP o ICMP. Nessuna sessior creata. Ad esempio, per ICMP il primo pacchetto ricevuto non è ECHO o TIMESTAMP. Per il TCP, non è un SYN. Questo problema si può verificare con la normale elaborazione dei pacc o con l'elaborazione imprecisa dei canali.
FirewallNessunaNuovaSessione	L'alta disponibilità del firewall non consente nuove sessioni.
DstMaxSincronizzazioneFirewall	Al fine di fornire la protezione da flood SYN basata su host, esiste una frequenza SYN per destinazione come limite di flood SYN. Quando il numero di voci di destinazione raggiunge il limite, i nuovi pacchetti SYN vengono scartati.
SincronizzazioneFirewall	Viene attivata la logica SYNCOOLIE. Ciò indica che è stato inviato un SYN/ACK con il cookie SYN e il pacchetto SYN originale viene scartato.
FirewallArsTandby	Il routing asimmetrico non è abilitato e il gruppo di ridondanza non è in s attivo.

Contatori perdite funzionalità firewall su QFP

Il limite del contatore di rilascio globale QFP è che non c'è granularità nei motivi di rilascio, e alcuni dei motivi di rilascio come **FirewallL4** vengono così sovraccaricati al punto che è poco utile per la risoluzione dei problemi. Questa funzionalità è stata migliorata in Cisco IOS-XE 3.9 (15.3(2)S), dove sono stati aggiunti contatori di rilascio delle funzionalità del firewall. Questo fornisce una serie molto più granulare di motivi di caduta:

```
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
....
```

Di seguito è riportato un elenco dei motivi di rilascio delle funzionalità del firewall e le relative spiegazioni:

Motivo eliminazione funzionalità firewall	Spiegazione
Lunghezza intestazione non valida	Le dimensioni del datagramma sono tali da non poter contenere l'intestazione layer 4TCP, UDP o ICMP. Possibili cause: 1. Lunghezza intestazione TCP < 20 2. Lunghezza intestazione UDP/ICMP < 8
Lunghezza dati UDP non valida	La lunghezza del datagramma UDP non corrisponde alla lunghezza specificata nell'intestazione UDP.
Numero ACK non valido	Questo calo potrebbe essere causato da uno dei motivi seguenti: 1. ACK diverso da next_seq# del peer TCP. 2. ACK è maggiore del numero di SEQ più recente inviato dal peer TCP. Negli stati TCP SYNSENT e SYNRCVD, si prevede che il numero ACK sia uguale a ISN+1 ma non lo è.
Flag ACK non valido	Questo calo potrebbe essere causato da uno dei motivi seguenti: 1. Previsto flag ACK ma non impostato in uno stato TCP diverso. 2. Oltre al flag ACK, è impostato anche un altro flag (come RST).
Iniziatore TCP non valido	Ciò si verifica quando: 1. Il primo pacchetto proveniente da un iniziatore TCP non è un SYN (il segmento TCP non iniziale viene ricevuto senza una sessione valida). 2. Per il pacchetto SYN iniziale è impostato il flag ACK.
SYN con dati	Il pacchetto SYN contiene il payload. Operazione non supportata.
Flag TCP non validi	I flag TCP non validi possono essere causati da: 1. Il pacchetto SYN iniziale di TCP ha flag diversi da SYN. 2. Nello stato di ascolto TCP, un peer TCP riceve un RST o un ACK. 3. Il pacchetto dell'altro risponditore viene ricevuto prima di SYN/ACK. 4. SYN/ACK previsto non ricevuto dal risponditore.
Segmento non valido nello stato SYNSENT	Un segmento TCP non valido nello stato SYNSENT è causato da: 1. SYN/ACK con payload. 2. Per SYN/ACK sono impostati altri flag (PSH, URG, FIN). 3. Ricevi un SYN di transito con payload. 4. Ricevere un pacchetto non SYN dall'iniziatore.
Segmento non valido nello stato SYNRCVD	Un segmento TCP non valido nello stato SYNRCVD potrebbe essere causato da: 1. Ricevere un SYN di transito con payload dall'iniziatore. 2. Ricevere un segmento non valido diverso da SYN/ACK, RST o FIN dal responder.
SEQ non valida	Questo si verifica nello stato SYNRCVD quando i segmenti provengono dall'iniziatore. La causa è: 1. Seq# è minore di ISN. 2. Se le dimensioni della finestra di ricezione del ricevitore sono 0 e: Il segmento ha un payload oppure Il segmento non in ordine (seq# è maggiore del LASTACK del ricevitore.

	3. Se le dimensioni della finestra di ricezione del ricevitore sono pari a 0 e il numero di seq supera le dimensioni della finestra. 4. Seq# è uguale a ISN ma non a un pacchetto SYN.
Opzione di ridimensionamento della finestra non valida	L'opzione di ridimensionamento della finestra TCP non valida è causata dalla lunghezza in byte dell'opzione di ridimensionamento della finestra non corretta.
TCP fuori dalla finestra	Il pacchetto è troppo vecchio - una finestra dietro l'altra ACK. Questo problema può verificarsi nello stato DEFINED, CLOSEWAIT e LASTACK.
Payload TCP aggiuntivo dopo invio FIN	Payload ricevuto dopo l'invio di FIN. Questo problema può verificarsi nello stato CLOSEWAIT.
Overflow della finestra TCP	Questo si verifica quando le dimensioni del segmento in ingresso superano la finestra del destinatario. Tuttavia, se vTCP è abilitato, questa condizione è consentita perché il firewall deve inserire il segmento nel buffer per consentirne l'utilizzo in un secondo momento.
Riesegui con flag non validi	Un pacchetto ritrasmesso è già stato riconosciuto dal destinatario.
Segmento TCP non in ordine	Il pacchetto non ordinato sta per essere consegnato a L7 per l'ispezione. Se L7 non consente il segmento OOO, questo pacchetto verrà scartato.
SYN Flood	Sotto un attacco flood TCP SYN. In determinate condizioni, quando le connessioni correnti all'host superano il valore half-open configurato, il firewall rifiuterà per un determinato periodo di tempo qualsiasi nuova connessione a questo indirizzo IP. Di conseguenza, i pacchetti verranno scartati.
Errore interno - allocazione controllo synflood non riuscita	Durante il controllo synflood, l'allocazione dell'hostdb non riesce. Azione consigliata: selezionare "show platform hardware qfp active feature firewall memory" per controllare lo stato della memoria.
Synflood blackout drop	Se vengono configurate connessioni half-open e viene configurato il tempo di blackout, tutte le nuove connessioni a questo indirizzo IP vengono eliminate.
Superato il limite di sessioni aperte	Pacchetto ignorato a causa del superamento del numero massimo di sessioni aperte a metà consentito. Verificare inoltre le impostazioni di "max-complete high/low" e "one-minute high/low" per assicurarsi che il numero di sessioni aperte a metà non sia limitato da queste configurazioni.
Troppi pacchetti per flusso	Èstato superato il numero massimo di pacchetti ispezionabili consentiti per flusso. Il numero massimo è 25.
Troppi pacchetti di errore ICMP per flusso	Èstato superato il numero massimo di pacchetti di errori ICMP consentiti per flusso. Il numero massimo è 3.
Payload TCP imprevisto da Rsp a Init	Nello stato SYNRCVD, il protocollo TCP riceve un pacchetto con payload dal risponditore alla direzione dell'iniziatore.
Errore interno - Direzione non definita	Direzione pacchetto non definita.
SYN nella finestra corrente	Un pacchetto SYN viene visualizzato nella finestra di una connessione TCP già stabilita.
RST nella finestra corrente	Un pacchetto RST viene osservato nella finestra di una connessione TCP già stabilita.
Segmento isolato	Viene ricevuto un segmento TCP che non avrebbe dovuto essere ricevuto tramite la macchina a stati TCP, ad esempio un pacchetto TCP SYN ricevuto nello stato di ascolto dal risponditore.

Errore interno ICMP - Informazioni NAT ICMP mancanti	Il pacchetto ICMP non è disponibile, ma mancano le informazioni NAT interne. Errore interno.
Pacchetto ICMP in stato di chiusura SCB	Ricevuto un pacchetto ICMP in stato SCB CLOSE.
Intestazione IP mancante nel pacchetto ICMP	Intestazione IP mancante nel pacchetto ICMP.
Errore ICMP No IP o ICMP	Pacchetto di errore ICMP senza IP o ICMP nel payload. Probabile causa di un pacchetto non valido o di un attacco.
ICMP Err Pkt troppo breve	Pacchetto di errore ICMP troppo breve.
Limite burst superato da errore ICMP	Il pacchetto di errore ICMP supera il limite di burst di 10.
ICMP Err Unreachable	Il pacchetto di errore ICMP "destinazione irraggiungibile" supera il limite. Solo il 1^{o} pacchetto non raggiungibile può passare.
N. sequenza non valida errore ICMP	Il numero di sequenza del pacchetto incorporato non corrisponde al numero di sequenza del pacchetto da cui proviene l'errore ICMP.
ICMP Err non valido Ack	ACK non valido nel pacchetto incorporato dell'errore ICMP.
ICMP action drop	L'azione ICMP configurata è drop.
Coppia di zone senza mappa dei criteri	Criterio non presente sulla coppia di zone. è possibile che ALG (Application Layer Gateway) non sia configurato per l'apertura del foro per il canale dati dell'applicazione, che ALG non abbia aperto correttamente il foro del canale o che non sia stato aperto alcun foro del foro a causa di problemi di scalabilità.
Sessione Mancante E Criterio Non Presente	Ricerca di sessione non riuscita. Nessun criterio presente per ispezionare il pacchetto.
Errore ICMP e criterio non presenti	Errore ICMP senza criteri configurati sulla coppia di zone.
Classificazione non riuscita	Errore di classificazione in una coppia di zone specificata quando il firewall tenta di determinare se il protocollo è ispezionabile.
Eliminazione azione classificazione	L'azione di classificazione è a caduta.
Configurazione errata dei criteri di sicurezza	Classificazione non riuscita a causa di una configurazione errata dei criteri di sicurezza. Ciò potrebbe anche essere dovuto alla mancanza di un pin pole per il canale dati L7.
Invia RST a risponditore	Invia RST al risponditore nello stato SYNSENT quando ACK# non è uguale a ISN+1.
Eliminazione criteri firewall	L'azione criterio è da eliminare.
Perdita di frammenti	Elimina i frammenti rimanenti quando si elimina il primo frammento.
Rilascio criteri firewall ICMP	L'azione criterio del pacchetto incorporato ICMP è DROP.
L7 ispezione	L7 (ALG) decide di rilasciare il pacchetto. Il motivo può essere trovato da

restituisce DROP Pacchetto	diverse statistiche ALG.
segmento L7 non consentito	Ricevuto pacchetto segmentato quando ALG non lo rispetta.
Frammento L7 Non Consentito	Ricevuti pacchetti frammentati (o VFR) quando ALG non li rispetta.
Tipo di porta L7 sconosciuto	Tipo di protocollo non riconosciuto.

Risoluzione dei problemi relativi alle perdite del firewall

Una volta identificato il motivo della perdita dai contatori delle perdite delle funzionalità globali o firewall sopra indicati, potrebbero essere necessarie ulteriori operazioni di risoluzione dei problemi se tali perdite sono impreviste. Oltre alla convalida della configurazione, per verificare che la configurazione sia corretta per le funzionalità del firewall abilitate, spesso è necessario acquisire i pacchetti per il flusso di traffico in questione per verificare se i pacchetti sono in formato non corretto o se si verificano problemi di implementazione del protocollo o dell'applicazione.

Registrazione

La funzionalità di registrazione ASR genera syslog per registrare i pacchetti ignorati. Questi syslog forniscono ulteriori dettagli sul motivo per cui il pacchetto è stato scartato. Esistono due tipi di syslog:

1. Syslogging nel buffer locale

2. Registrazione remota ad alta velocità

Syslog nel buffer locale

Per isolare la causa delle perdite di dati, potete utilizzare la risoluzione dei problemi generica ZBFW, ad esempio l'attivazione delle perdite di log. Esistono due modi per configurare la registrazione del rilascio dei pacchetti.

Metodo 1: Usare inspect-global parameter-map per registrare tutti i pacchetti scartati.

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

Metodo 2: Utilizzare la mappa dei parametri personalizzata inspect per registrare i pacchetti ignorati solo per una classe specifica.

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

Questi messaggi vengono inviati al registro o alla console a seconda di come l'ASR è configurato per la registrazione. Di seguito è riportato un esempio di messaggio del log di rilascio.

```
*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
```

Limitazioni della registrazione di sistema nel buffer locale

1. La velocità di questi log è limitata a quella indicata dall'ID bug Cisco CSCud09943.

2. Questi registri potrebbero non essere stampati se non viene applicata una configurazione specifica. Ad esempio, i pacchetti eliminati dai pacchetti predefiniti della classe non verranno registrati a meno che non venga specificata la parola chiave **log**:

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

Registrazione ad alta velocità remota

La registrazione ad alta velocità (HSL) genera syslog direttamente da QFP e li invia al collector HSL netflow configurato. Questa è la soluzione di registrazione consigliata per ZBFW su ASR.

Per HSL, utilizzare questa configurazione:

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

Per utilizzare questa configurazione, è necessario un agente di raccolta netflow compatibile con Netflow versione 9. Questo è descritto in

Guida alla configurazione: Policy Firewall basato su zone, Cisco IOS XE release 3S (ASR 1000) Firewall registrazione ad alta velocità

Traccia pacchetti tramite corrispondenza condizionale

Abilitare i debug condizionali per abilitare la traccia dei pacchetti e abilitare quindi la traccia per queste funzionalità:

```
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
```

> **Nota:** La condizione di corrispondenza può utilizzare direttamente l'indirizzo IP, poiché non è necessario un ACL. Corrisponde a come origine o destinazione che consente tracce bidirezionali. È possibile utilizzare questo metodo se non si dispone delle autorizzazioni

necessarie per modificare la configurazione. Ad esempio: debug platform condition ipv4 address 192.168.1.1/32.

Attiva la funzionalità di traccia dei pacchetti:

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

Èpossibile utilizzare questa funzionalità in due modi:

1. Immettere il comando **debug platform packet-trace drop** per tracciare solo i pacchetti scartati.

2. L'esclusione del comando **debug platform packet-trace drop** consentirà di tracciare tutti i pacchetti che soddisfano la condizione, compresi quelli ispezionati/passati dal dispositivo.

Attiva debug condizionali:

```
debug platform condition start
```

Eseguire il test, quindi disattivare i debug:

```
debug platform condition stop
```

A questo punto le informazioni possono essere visualizzate sullo schermo. Nell'esempio, i pacchetti ICMP sono stati scartati a causa di un criterio firewall:

```
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
```

Il comando **show platform packet-trace packet <num>decodifica** le informazioni e il contenuto dell'intestazione del pacchetto. Questa funzionalità è stata introdotta in XE3.11:

```
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

Il supporto Embedded Packet Capture è stato aggiunto in Cisco IOS-XE 3.7 (15.2(4)S). Per ulteriori informazioni, vedere

Esempio di acquisizione integrata dei pacchetti per Cisco IOS e IOS-XE.

Debug

Debug condizionali

In XE3.10 verranno introdotti i debug condizionali. Le istruzioni condizionali possono essere usate per garantire che la funzione ZBFW registri solo i messaggi di debug relativi alla condizione. I debug condizionali usano gli ACL per limitare i log che corrispondono agli elementi ACL. Inoltre, prima di XE3.10, i messaggi di debug erano più difficili da leggere. L'output del comando debug è stato migliorato in XE3.10 per facilitarne la comprensione.

Per abilitare i debug, usare questo comando:

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

```
debug platform condition start
```

Il comando condition deve essere impostato tramite un ACL e la direzionalità. I debug condizionali non verranno implementati finché non vengono avviati con il comando **debug platform condition start**. Per disattivare i debug condizionali, usare il comando **debug platform condition stop**.

```
debug platform condition stop
```

Per disattivare i debug condizionali, **NON** utilizzare il comando **undebug all**. Per disattivare tutti i debug condizionali, utilizzare il comando:

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

Nelle versioni precedenti a XE3.14, i debug di **ha** ed **eventi** non sono condizionali. Di conseguenza, il comando **debug platform condition feature fw dataplane submode** determina **la** creazione di tutti i log, indipendentemente dalla condizione selezionata di seguito. Ciò potrebbe creare ulteriore rumore che rende difficile il debug.

Per impostazione predefinita, il livello di registrazione condizionale è **info**. Per aumentare/diminuire il livello di registrazione, usare il comando:

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

Raccolta e visualizzazione dei debug

I file di debug non verranno stampati sulla console o sul monitor. Tutti i debug vengono scritti sul disco rigido dell'ASR. I debug vengono scritti sul disco rigido sotto la cartella **tracelogs** con il nome **cpp_cp_F0-0.log.<date>**. Per visualizzare il file in cui sono stati scritti i debug, usare l'output:

```
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)
```

Ogni file di debug verrà archiviato come file **cpp_cp_F0-0.log.<date>**. Si tratta di normali file di testo che possono essere copiati dall'ASR con TFTP. Il file di registro massimo sull'ASR è 1 MB. Dopo 1 MB, i debug vengono scritti in un nuovo file di log. Per questo motivo, a ogni file di log viene assegnato un timestamp che indica l'inizio del file.

I file di registro possono essere presenti nei percorsi seguenti:

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

Poiché i file di registro vengono visualizzati solo dopo essere stati ruotati, è possibile ruotarli manualmente con questo comando:

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

Questo crea immediatamente un file di log "cpp_cp" e ne avvia uno nuovo sul QFP. Ad esempio:

```
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)
```

Questo comando consente di unire i file di debug in un unico file per semplificare l'elaborazione. Unisce tutti i file nella directory e li interlaccia in base al tempo. Ciò può essere utile quando i registri sono molto dettagliati e vengono creati su più file:

```
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]
```