IOS-XE용 ZBFW 컨피그레이션 트러블슈팅 가이드

목차

[소개](#)
[링크 및 문서](#)
[명령 참조](#)
[데이터 경로 문제 해결 단계](#)
[구성 확인](#)
[연결 상태 확인](#)
[방화벽 삭제 카운터 확인](#)
[QFP의 전역 삭제 카운터](#)
[QFP의 방화벽 기능 삭제 카운터](#)
[방화벽 삭제 문제 해결](#)
[로깅](#)
[로컬 버퍼링된 syslog](#)
[로컬 버퍼링된 syslog의 제한 사항](#)
[원격 고속 로깅](#)
[조건부 일치를 사용한 패킷 추적](#)
[임베디드 패킷 캡처](#)
[디버깅](#)
[조건부 디버깅](#)
[디버깅 수집 및 보기](#)

소개

이 문서에서는 ASR(Aggregation Services Router) 1000에서 ZBFW(Zone Based Firewall) 기능을 트러블슈팅하는 방법과 ASR에서 하드웨어 삭제 카운터를 폴링하는 데 사용되는 명령을 설명합니다.ASR1000은 하드웨어 기반 포워딩 플랫폼입니다.Cisco IOS-XE®의 소프트웨어 구성은 기능 전달 기능을 수행하기 위해 하드웨어 ASIC(quantum flow processor)를 프로그래밍합니다.따라서 처리량이 향상되고 성능이 향상됩니다.문제는 트러블슈팅에 더 큰 과제가 있다는 것입니다 .ZBFW(Zone-Based Firewall)를 통해 현재 세션을 폴링하고 카운터를 삭제하는 데 사용되는 기존의 Cisco IOS 명령은 더 이상 유효하지 않습니다. 삭제는 더 이상 소프트웨어에 존재하지 않습니다.

링크 및 문서

명령 참조

- Cisco ASR 1000 Series Aggregation Services Routers 명령 참조
- Cisco IOS XE 3S 명령 참조

데이터 경로 문제 해결 단계

데이터 경로를 트러블슈팅하려면 트래픽이 ASR 및 Cisco IOS-XE 코드를 통해 올바르게 전달되는지 확인해야 합니다.방화벽 기능에 따라 데이터 경로 문제 해결은 다음 단계를 따릅니다.

1. **Verify Configuration**(컨피그레이션 확인) - 컨피그레이션을 수집하고 출력을 검사하여 연결을 확인합니다.

2. **Verify Connection State**(연결 상태 확인) - 트래픽이 제대로 전달되면 Cisco IOS-XE가 ZBFW 기능에 대한 연결을 엽니다.이 연결은 클라이언트와 서버 간의 트래픽 및 상태 정보를 추적합니다.

3. **Verify Drop Counters(삭제 카운터 확인)** - 트래픽이 제대로 전달되지 않을 경우 Cisco IOS-XE는 삭제된 패킷에 대한 삭제 카운터를 로깅합니다.트래픽 오류의 원인을 격리하려면 이 출력을 확인하십시오.

4. **로깅** - 연결 빌드 및 패킷 삭제에 대한 자세한 정보를 제공하기 위해 syslog를 수집합니다.

5. **Packet Trace Dropped Packets** - 삭제된 패킷을 catch하려면 패킷 추적을 사용합니다.

6. **디버깅** - 디버깅 수집이 가장 자세한 옵션입니다.패킷의 정확한 전달 경로를 확인하기 위해 조건부로 디버그를 얻을 수 있습니다.

구성 확인

show tech support firewall의 출력은 다음과 같습니다.

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

연결 상태 확인

ZBFW의 모든 연결이 나열되도록 연결 정보를 얻을 수 있습니다.다음 명령을 입력합니다.

```
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]
```
14.38.112.250에서 14.36.1.206으로 TCP 텔넷 연결을 표시합니다.

> **참고:**이 명령을 실행하면 디바이스에 많은 연결이 있는 경우 시간이 오래 걸립니다.여기에 설명된 대로 특정 필터와 함께 이 명령을 실행하는 것이 좋습니다.

연결 테이블을 특정 소스 또는 대상 주소로 필터링할 수 있습니다.**플랫폼** 하위 모드 후 필터 사용필터링할 옵션은 다음과 같습니다.

```
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>
```
이 연결 테이블은 필터링되어 14.38.112.250에서 제공된 연결만 표시됩니다.

```
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]
```
연결 테이블을 필터링하면 보다 포괄적인 분석을 위해 자세한 연결 정보를 얻을 수 있습니다.이 출력을 표시하려면 detail 키워드를 사용합니다.

```
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
```

방화벽 삭제 카운터 확인

XE 3.9 동안 드롭 카운터 출력이 변경되었습니다. XE 3.9 이전에는 방화벽 삭제 사유가 매우 일반적이었습니다.XE 3.9 이후 방화벽 삭제 사유가 더욱 세분화되었습니다.

드롭 카운터를 확인하려면 다음 두 단계를 수행하십시오.

1. Cisco IOS-XE에서 전역 삭제 카운터를 확인합니다.이 카운터는 어떤 기능이 트래픽을 삭제했는지 보여줍니다.기능 예로는 QoS(Quality of Service), NAT(Network Address Translation), 방화벽 등이 있습니다.

2. 하위 기능이 식별되면 하위 기능에서 제공하는 세분화된 삭제 카운터를 쿼리합니다.이 설명서에서 분석 중인 하위 기능은 방화벽 기능입니다.

QFP의 전역 삭제 카운터

기본적으로 사용되는 명령은 QFP에서 모든 삭제를 제공합니다.

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

이 명령은 QFP에서 전체적으로 삭제되는 일반적인 항목을 보여줍니다.이러한 삭제는 어떤 기능에서도 가능합니다.일부 기능은 다음과 같습니다.

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

모든 삭제를 보려면 값이 0인 카운터를 포함하려면 다음 명령을 사용합니다.

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

카운터를 지우려면 이 명령을 사용합니다.화면에 표시된 후 출력을 지웁니다.이 명령은 읽기 시 지워지므로 출력이 화면에 표시된 **후** 0으로 재설정됩니다.

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

다음은 QFP 전역 방화벽 삭제 카운터와 설명 목록입니다.

방화벽 전역 삭제 이유	설명
방화벽 후압	로깅 메커니즘으로 인해 패킷이 드롭됩니다.
방화벽유효하지 않은 영역	인터페이스에 대해 구성된 보안 영역이 없습니다.
방화벽L4Insp	L4 정책 확인 실패.보다 세부적인 삭제 이유(방화벽 기능 삭제 이유)는 아래 표를

	하십시오.
방화벽포워딩 영역	방화벽이 초기화되지 않았으며 트래픽을 전달할 수 없습니다.
방화벽 비세션	세션 생성에 실패했습니다.최대 세션 제한에 도달했거나 메모리 할당 오류 때문일 있습니다.
방화벽 정책	구성된 방화벽 정책이 삭제됩니다.
방화벽L4	L4 검사 실패.보다 세부적인 삭제 이유(방화벽 기능 삭제 이유)는 아래 표를 참조 시오.
방화벽L7	L7 검사 때문에 패킷이 삭제됩니다.더욱 세분화된 L7 삭제 이유(방화벽 기능 삭제 유) 목록은 아래를 참조하십시오.
방화벽초기자	TCP, UDP 또는 ICMP에 대한 세션 개시자가 아닙니다.세션이 생성되지 않습니다 를 들어 ICMP의 경우 첫 번째 수신된 패킷은 ECHO 또는 TIMESTAMP가 아닙니 .TCP의 경우 SYN이 아닙니다.
방화벽새세션없음	이는 정상적인 패킷 처리 또는 정확하지 않은 채널 처리에서 발생할 수 있습니다. 방화벽 고가용성은 새 세션을 허용하지 않습니다.
방화벽SyncookieMaxDst	호스트 기반 SYN 플러드 보호를 제공하기 위해 SYN 플러드 제한으로서 대상별 속도가 있습니다.대상 항목 수가 제한에 도달하면 새 SYN 패킷이 삭제됩니다.
방화벽 동기화	SYNCOOLIE 논리가 트리거됩니다.이는 SYN 쿠키가 있는 SYN/ACK가 전송되었 원래 SYN 패킷이 삭제되었음을 나타냅니다.
방화벽ARSandby	비대칭 라우팅이 활성화되지 않았으며 이중화 그룹이 활성 상태가 아닙니다.

QFP의 방화벽 기능 삭제 카운터

QFP 글로벌 드롭 카운터의 제한 사항은 삭제 사유에 세분화된 요소가 없다는 것이며, FirewallL4와 같은 삭제 이유 중 일부는 너무 오버로드되어 트러블슈팅에 거의 사용되지 않는다는 점에 도달합니다.이 기능은 Cisco IOS-XE 3.9(15.3(2)S)에서 개선되었으며, 여기에서 방화벽 기능 삭제 카운터가 추가되었습니다.이렇게 하면 훨씬 더 세분화된 삭제 이유가 제공됩니다.

```
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
....
```

다음은 방화벽 기능 삭제 이유 및 설명 목록입니다.

방화벽 기능 삭제 이유	설명
잘못된 헤더 길이	데이터그램이 너무 작아서 레이어 4TCP, UDP 또는 ICMP 헤더를 포함할 수 없습니다. 이유 때문일 수 있습니다. 1. TCP 헤더 길이 < 20 2. UDP/ICMP 헤더 길이 < 8
잘못된 UDP 데이터 길이	UDP 데이터그램 길이가 UDP 헤더에 지정된 길이와 일치하지 않습니다.
잘못된 ACK 번호	이 삭제는 다음 이유 중 하나로 인해 발생할 수 있습니다. 1. ACK는 TCP 피어의 next_seq#과 같지 않습니다. 2. ACK가 TCP 피어에서 보낸 최신 SEQ#보다 큽니다. TCP SYNSENT 및 SYNRCVD 상태에서는 ACK#이 ISN+1과 같아야 하지만 그렇지 않다.
잘못된 ACK 플래그	이 삭제는 다음 이유 중 하나로 인해 발생할 수 있습니다. 1. ACK 플래그가 필요하지만 다른 TCP 상태로 설정되지 않았습니다.

	2. ACK 플래그 이외의 다른 플래그(예: RST)도 설정됩니다.
잘못된 TCP 개시자	이는 다음과 같은 경우에 발생합니다. 1. TCP 개시자의 첫 번째 패킷은 SYN이 아닙니다(비초기 TCP 세그먼트는 유효한 세 없이 수신됨). 2. 초기 SYN 패킷에는 ACK 플래그가 설정되어 있습니다.
데이터가 있는 SYN	SYN 패킷에 페이로드가 포함되어 있습니다.지원되지 않습니다.
잘못된 TCP 플래그	잘못된 TCP 플래그는 다음과 같은 이유로 인해 발생할 수 있습니다. 1. TCP 초기 SYN 패킷에 SYN 이외의 플래그가 있습니다. 2. TCP 수신 상태에서 TCP 피어는 RST 또는 ACK를 수신합니다. 3. SYN/ACK 전에 다른 응답자의 패킷을 수신합니다. 4. 필요한 SYN/ACK가 응답자로부터 수신되지 않았습니다.
SYNSENT 상태의 잘못된 세그먼트	SYNSENT 상태의 잘못된 TCP 세그먼트는 다음과 같은 원인으로 인해 발생합니다. 1. SYN/ACK에 페이로드가 있습니다. 2. SYN/ACK에는 다른 플래그(PSH, URG, FIN)가 설정되어 있습니다. 3. 페이로드가 있는 전송 SYN을 수신합니다. 4. 개시자로부터 비 SYN 패킷을 수신합니다.
SYNRCVD 상태의 잘못된 세그먼트	SYNRCVD 상태의 잘못된 TCP 세그먼트는 다음과 같은 원인으로 인해 발생할 수 있습 1. 개시자로부터 페이로드를 사용하여 SYN을 다시 전송 받습니다. 2. 응답자로부터 SYN/ACK, RST 또는 FIN이 아닌 잘못된 세그먼트를 받습니다.
잘못된 시퀀스	세그먼트가 이니시에이터에서 오는 경우 SYNRCVD 상태가 됩니다.원인: 1. 시퀀스 번호가 ISN보다 작습니다. 2. 수신자 수신 창 크기가 0이고 다음과 같은 경우: 세그먼트에 페이로드가 있습니다. 또는 순서가 잘못된 세그먼트(seq#이(가) 수신기 LASTACK보다 큽니다. 3. receiver rcvd 창 크기가 0이고 seq#이 창을 벗어나면 됩니다. 4. Seq#은 ISN과 같지만 SYN 패킷은 아닙니다.
잘못된 창 배율 옵션	잘못된 TCP 창 크기 조정 옵션은 잘못된 창 크기 조정 옵션 바이트 길이로 인해 발생합
TCP가 창을 벗어났습니다.	패킷이 너무 오래되었습니다. 다른 쪽의 ACK 뒤에 한 창이 있습니다.이는 ESTABLISH CLOSEWAIT 및 LASTACK 상태에서 발생할 수 있습니다.
FIN이 전송된 후 TCP 추가 페이로드	FIN이 전송된 후 페이로드를 받았습니다.이는 CLOSEWAIT 상태에서 발생할 수 있습니
TCP 창 오버플로	이는 들어오는 세그먼트 크기가 수신기의 창을 오버플로할 때 발생합니다.그러나 vTCP 활성화된 경우 방화벽이 ALG가 나중에 사용하기 위해 세그먼트를 버퍼링해야 하므로 건이 허용됩니다.
플래그가 잘못된 리턴	재전송된 패킷이 수신자가 이미 승인했습니다.
TCP 비주문 세그먼트	Out-of-Order 패킷이 검사를 위해 L7에 전달될 예정입니다.L7에서 OO 세그먼트를 허용 않으면 이 패킷이 삭제됩니다.
SYN 플러드	TCP SYN 플러드 공격에서이 호스트에 대한 현재 연결이 구성된 절반 열기 값을 초과하 특정 조건에서 방화벽은 일정 기간 동안 이 IP 주소에 대한 새 연결을 거부합니다.따라서 킷이 삭제됩니다.
내부 오류 - synflood check alloc 실패	synflood 검사 중 hostdb 할당이 실패합니다. 권장 작업:"show platform hardware qfp active feature firewall memory"를 선택하여 메 상태를 확인합니다.
동기화 중단 삭제	구성된 half-open 연결이 초과되고 일시 중단 시간이 구성된 경우 이 IP 주소에 대한 모 연결이 삭제됩니다.
1/2 열린 세션 제한	허용되는 절반이 열린 세션이 초과되어 패킷이 삭제되었습니다.

초과	또한 "max-incomplete high/low" 및 "1분 high/low"의 설정을 확인하여 절반이 열린 세션 가 이러한 컨피그레이션으로 제한되지 않는지 확인합니다.
플로우당 PKT가 너무 많음	흐름당 허용되는 검사 가능한 최대 패킷 수를 초과했습니다.최대 수는 25입니다.
흐름당 너무 많은 ICMP 오류 패킷	흐름당 허용되는 최대 ICMP 오류 패킷 수를 초과했습니다.최대 수는 3입니다.
RSP에서 초기화(Init)로 TCP 페이로드 예상 안 함	SYNRCVD 상태에서 TCP는 responder에서 initiator 방향으로 페이로드가 있는 패킷을 합니다.
내부 오류 - 정의되지 않은 방향	패킷 방향이 정의되지 않았습니다.
현재 창 내의 SYN	SYN 패킷은 이미 설정된 TCP 연결의 창 내에 표시됩니다.
현재 창 내의 RST	RST 패킷은 이미 설정된 TCP 연결의 창에서 관찰됩니다.
분리 세그먼트	응답자로부터 수신 상태로 수신되는 TCP SYN 패킷과 같은 TCP 상태 시스템을 통해 수 지 않아야 하는 TCP 세그먼트를 수신합니다.
ICMP 내부 오류 - 누락된 ICMP NAT 정보	ICMP 패킷이 nat되었지만 내부 NAT 정보가 없습니다.내부 오류입니다.
SCB 닫기 상태의 ICMP 패킷	SCB CLOSE 상태의 ICMP 패킷을 받았습니다.
ICMP 패킷의 누락된 IP 헤더	ICMP 패킷에 IP 헤더가 없습니다.
ICMP 오류 IP 또는 ICMP 없음	페이로드에서 IP 또는 ICMP가 없는 ICMP 오류 패킷.잘못된 형식의 패킷 또는 공격 때문 수 있습니다.
ICMP 오류 PKT가 너무 짧습니다.	ICMP 오류 패킷이 너무 짧습니다.
ICMP 오류 초과 버스트 제한	ICMP 오류 패킷이 버스트 제한인 10을 초과합니다.
ICMP 오류 도달 불가	ICMP 오류 pkt에 연결할 수 없는 제한이 초과되었습니다.1번째 도달 불가 패킷만 통과하 허용됩니다.
ICMP 오류 잘못된 시퀀스 번호	포함된 패킷의 시퀀스 번호가 ICMP 오류를 시작하는 패킷의 시퀀스 번호와 일치하지 않 니다.
ICMP 오류 잘못된 ACK	ICMP 오류 포함 패킷에 잘못된 ACK가 있습니다.
ICMP 작업 삭제	구성된 ICMP 작업은 삭제됩니다.
정책 맵이 없는 영역 쌍	zone-pair에 정책이 없습니다.ALG(Application Layer Gateway)가 애플리케이션 데이터 에 대한 핀홀을 열도록 구성되지 않았거나, ALG가 핀홀을 제대로 열지 않았거나, 확장 제로 인해 핀홀이 열리지 않았기 때문일 수 있습니다.
세션 누락 및 정책이 없음	세션 조회에 실패했으며 이 패킷을 검사할 정책이 없습니다.
ICMP 오류 및 정책이 없음	영역 쌍에 구성된 정책이 없는 ICMP 오류입니다.
분류 실패	방화벽에서 프로토콜이 검사 가능한지 확인하려고 시도할 때 지정된 영역 쌍의 분류 오 니다.
분류 작업 삭제	분류 작업이 삭제됩니다.
보안 정책 구성 오류	보안 정책 컨피그레이션 오류로 인해 분류하지 못했습니다.L7 데이터 채널에 대한 핀홀 기 때문일 수도 있습니다.
응답자에게 RST 보내기	ACK#이 ISN+1과 같지 않은 경우 SYNSENT 상태의 응답자에게 RST를 보냅니다.
방화벽 정책 삭제	정책 작업은 삭제합니다.
조각 삭제	첫 번째 프래그먼트가 삭제되면 나머지 프래그먼트를 삭제합니다.
ICMP 방화벽 정책	ICMP 임베디드 패킷의 정책 작업은 DROP입니다.

삭제	
L7 검사는 DROP 반환	L7(ALG)은 패킷을 삭제하기로 결정합니다.이유는 다른 ALG 통계에서 찾을 수 있습니
L7 세그먼트 패킷 허용 안 함	ALG가 이를 승인하지 않을 때 세그먼트화된 패킷을 받았습니다.
L7 프래그먼트 PKT 허용 안 함	ALG가 이를 승인하지 않을 때 조각화된(또는 VFR) 패킷을 받았습니다.
알 수 없는 L7 프로토콜 유형	인식할 수 없는 프로토콜 유형입니다.

방화벽 삭제 문제 해결

위의 전역 또는 방화벽 기능 삭제 카운터에서 삭제 이유가 확인되면 이러한 삭제가 예기치 않은 경우 추가 트러블슈팅 단계가 필요할 수 있습니다.활성화된 방화벽 기능에 대한 컨피그레이션이 올바른지 확인하기 위해 컨피그레이션 검증 외에도, 패킷의 형식이 잘못되었거나 프로토콜 또는 애플리케이션 구현 문제가 있는지 확인하기 위해 문제가 있는 트래픽 흐름에 대한 패킷 캡처를 가져와야 하는 경우가 많습니다.

로깅

ASR 로깅 기능은 삭제된 패킷을 기록하기 위해 syslog를 생성합니다.이러한 syslog는 패킷이 삭제된 이유에 대한 자세한 정보를 제공합니다.Syslog에는 두 가지 유형이 있습니다.

1. 로컬 버퍼링된 syslog
2. 원격 고속 로깅

로컬 버퍼링된 syslog

삭제 원인을 격리하기 위해 로그 삭제 활성화와 같은 일반적인 ZBFW 트러블슈팅을 사용할 수 있습니다.패킷 삭제 로깅을 구성하는 방법에는 두 가지가 있습니다.

방법 1:삭제된 모든 패킷을 로깅하려면 inspect-global parameter-map을 사용합니다.

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

방법 2:특정 클래스에 대해서만 삭제된 패킷을 로깅하려면 custom inspect parameter-map을 사용합니다.

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

이러한 메시지는 로깅을 위해 ASR이 구성된 방식에 따라 로그 또는 콘솔로 전송됩니다.다음은 삭제 로그 메시지의 예입니다.

```
*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
```

로컬 버퍼링된 syslog의 제한 사항

1. 이러한 로그는 Cisco 버그 ID CSCud09943에 따라 제한됩니다.
2. 특정 컨피그레이션이 적용되지 않으면 이러한 로그가 인쇄되지 않을 수 있습니다.예를 들어, class-default 패킷에 의해 삭제된 패킷은 **log** 키워드를 지정하지 않으면 로깅되지 않습니다.

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

원격 고속 로깅

HSL(High Speed Logging)은 QFP에서 직접 syslog를 생성하여 구성된 netflow HSL 컬렉터로 전송합니다.이는 ASR의 ZBFW에 권장되는 로깅 솔루션입니다.

HSL의 경우 다음 컨피그레이션을 사용합니다.

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

이 컨피그레이션을 사용하려면 Netflow 버전 9를 지원하는 netflow 컬렉터가 필요합니다.자세한 내용은

구성 가이드:영역 기반 정책 방화벽, Cisco IOS XE Release 3S(ASR 1000) 방화벽 고속 로깅

조건부 일치를 사용한 패킷 추적

패킷 추적을 활성화한 다음 이러한 기능에 대해 패킷 추적을 활성화하려면 조건부 디버그를 활성화합니다.

```
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
```

> **참고:**ACL이 필요하지 않으므로 일치 조건은 IP 주소를 직접 사용할 수 있습니다.이는 양방향 추적을 허용하는 소스 또는 대상으로 매칭됩니다.컨피그레이션을 변경할 수 없는 경우 이 방법을 사용할 수 있습니다.예:디버그 플랫폼 조건 ipv4 주소 192.168.1.1/32.

패킷 추적 기능을 설정합니다.

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

이 기능을 사용하는 방법에는 두 가지가 있습니다.

1. 삭제된 **패킷만 추적하려면 debug platform packet-trace drop** 명령을 입력합니다.

2. 디버그 **플랫폼 packet-trace drop** 명령을 제외하면 디바이스에서 검사/전달한 패킷을 포함하여 조건과 일치하는 모든 패킷을 추적합니다.

조건부 디버깅 사용:

```
debug platform condition start
```

테스트를 실행한 다음 디버그를 끕니다.

```
debug platform condition stop
```

이제 정보를 화면에 표시할 수 있습니다.이 예에서는 방화벽 정책으로 인해 ICMP 패킷이 삭제되었습니다.

```
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** 명령은 패킷 헤더 정보 및 내용을 디코딩합니다 .이 기능은 XE3.11에서 도입되었습니다.

```
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
```

임베디드 패킷 캡처

Embedded Packet Capture 지원이 Cisco IOS-XE 3.7(15.2(4)S)에 추가되었습니다. 자세한 내용은 을/를 참조하십시오.

Embedded Packet Capture for Cisco IOS and IOS-XE Configuration 예

디버깅

조건부 디버깅

XE3.10에서는 조건부 디버그가 도입됩니다.조건문을 사용하여 ZBFW 기능이 조건과 관련된 디버그 메시지만 로깅하도록 할 수 있습니다.조건부 디버깅에서는 ACL을 사용하여 ACL 요소와 일치하는 로그를 제한합니다.또한 XE3.10 이전 버전에서는 디버그 메시지를 읽기 어려웠습니다 .XE3.10에서 디버그 출력이 개선되어 이해하기 쉽습니다.

이러한 디버그를 활성화하려면 다음 명령을 실행합니다.

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

조건 명령은 ACL 및 방향을 통해 설정해야 합니다.조건부 디버그는 **디버그 플랫폼 조건 시작** 명령으로 시작할 때까지 구현되지 않습니다.조건부 디버깅을 끄려면 **디버그 플랫폼 조건 중지** 명령을 사용합니다.

```
debug platform condition stop
```

조건부 디버깅을 끄려면 undebug 명령을 **모두 사용하지 마십시오**.모든 조건부 디버그를 끄려면 다음 명령을 사용합니다.

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

XE3.14 이전에는 ha 및 **이벤트** 디버그가 조건적이지 않습니다.따라서 명령 디버그 **플랫폼 조건 기능 fw**dataplane **하위 모드** 모두**는** 아래에서 선택한 조건과 상관없이 모든 로그를 생성합니다.이렇게 하면 디버깅을 어렵게 하는 추가 노이즈가 발생할 수 있습니다.

기본적으로 조건부 로깅 레벨은 info입니다.로깅 레벨을 높이거나 낮추려면 다음 명령을 사용합니다.

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

디버깅 수집 및 보기

디버그 파일은 콘솔 또는 모니터에 인쇄되지 않습니다.모든 디버그는 ASR의 하드 디스크에 기록됩니다.디버그는 cpp_**cp_F0-0.log**라는 이름**을 사용하여** 폴더 tracelogs 아래의 하드 디스크**에 기록됩니다**.디버그가 작성되는 파일을 보려면 다음 출력을 사용합니다.

```
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)
```

각 디버그 파일은 cpp_**cp_F0-0.log.<date>** 파일**로** 저장됩니다.TFTP를 사용하여 ASR에서 복사할 수 있는 일반 텍스트 파일입니다.ASR의 로그 파일 최대값은 1Mb입니다.1MB 이후에는 디버그가 새 로그 파일에 기록됩니다.따라서 각 로그 파일이 파일의 시작을 나타내기 위해 타임스탬프가 지정됩니다.

로그 파일은 다음 위치에 있을 수 있습니다.

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

로그 파일은 회전된 후에만 표시되므로 이 명령을 사용하여 로그 파일을 수동으로 회전할 수 있습니다.

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

이렇게 하면 "cpp_cp" 로그 파일이 즉시 생성되고 QFP에서 새 로그 파일이 시작됩니다.예:

```
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)
```

이 명령을 사용하면 보다 쉽게 처리할 수 있도록 디버그 파일을 단일 파일로 병합할 수 있습니다.디렉토리의 모든 파일을 병합하고 시간을 기준으로 상호 연결합니다.이렇게 하면 로그가 매우 자세하고 여러 파일에 걸쳐 생성될 때 도움이 됩니다.

```
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]
```