ZBFW voor IOS-XE probleemoplossing voor configuratie

Inhoud

Inleiding

Dit document beschrijft hoe de Zone Based Firewall (ZBFW) het beste kan worden opgelost in de Aggregation Services Router (ASR) 1000, met opdrachten die worden gebruikt om de hardware-valtellers in de ASR te inroepen. ASR1000 is een op hardware gebaseerd transportplatform. De softwareconfiguratie van Cisco IOS-XE® programma's stelt de hardware-ASIC's (Quantum Flow Processor (QFP) in om functies voor het verzenden van functies uit te voeren. Dit maakt een hogere doorvoersnelheid en betere prestaties mogelijk. Het nadeel hiervan is dat het een grotere uitdaging vormt om problemen op te lossen. Traditionele Cisco IOS-opdrachten die worden gebruikt om huidige sessies te inleiden en tellers te laten vallen via Zone-Based Firewall (ZBFW) zijn niet langer geldig omdat de druppels niet langer in software zijn.

Links en documentatie

Opdrachtreferenties

- Cisco ASR 1000 Series referenties voor aggregation services routers
- Cisco IOS XE 3S opdrachtreferenties

Stappen Datapath Troubleshooter

Om de datapath op te lossen, moet u identificeren of het verkeer goed door de ASR en Cisco IOS-XE code wordt doorgegeven. Specifieke aan firewallfuncties, volgt de probleemoplossing bij gegevensbestanden deze stappen:

1. **Controleer de configuratie** - Verzamel de configuratie en controleer de uitvoer om de verbinding te controleren.

2. **Controleer de verbindingsstaat** - Als het verkeer goed verloopt, opent Cisco IOS-XE een verbinding op de ZBFW optie. Deze verbinding volgt de verkeers- en staatsinformatie tussen een client en een server.

3. **Controleer de tellers van de Meld** - wanneer het verkeer niet goed overgaat, registreert Cisco IOS-XE een druppelteller voor om het even welke geworpen pakketten. Controleer deze uitvoer om de oorzaak van de verkeersstoring te isoleren.

4. **Vastlegging** - Verzamel systemen om meer gedetailleerde informatie te verstrekken over verbindingsgebouwen en pakketdruppels.

5. **Packet Trace heeft pakketjes** laten vallen - gebruik het overtrekken van pakketten om geworpen pakketten te vangen.

6. **Debugs** - Gather Debugs is de meest omslachtige optie. Debugs kunnen voorwaardelijk worden verkregen om het exacte verzendpad voor de pakketten te bevestigen.

Controleer de configuratie

De output van **show tech support firewall** wordt hier samengevat:

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

Controleer de verbindingsstaat

Verbinding kan worden verkregen zodat alle verbindingen op ZBFW zijn vermeld. Typ deze opdracht:

```
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]
```

Het toont een TCP-internetverbinding van 14.38.12.250 tot 14.36.1.2006.

> Opmerking: Houd er rekening mee dat als u deze opdracht uitvoert, het lang zal duren als er veel verbindingen op het apparaat zijn. Cisco raadt u aan deze opdracht met specifieke filters te draaien zoals hieronder aangegeven.

De verbindingstabel kan worden gefilterd naar een specifiek bron- of doeladres. Gebruik filters na **platform** submode. De opties om te filteren zijn:

```
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>
```

Deze aansluitingstabel is gefilterd zodat alleen verbindingen die van 14.38.112.250 afkomstig zijn, worden weergegeven:

```
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]
```

Zodra de verbindingstabel is gefilterd, kan de gedetailleerde verbindingsinformatie worden verkregen voor een meer uitgebreide analyse. Om deze uitvoer te tonen, gebruik het **detail** sleutelwoord.

```
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
```

Controleer firewalltellers

De uitvoer van de druppelteller veranderde tijdens XE 3.9. Vóór XE 3.9, waren de redenen voor de daling van de firewall zeer generiek. Na XE 3.9 werden de redenen voor het uitvallen van de firewall uitgebreid om korter te worden.

Voer twee stappen uit om valtellers te controleren:

1. Bevestig de mondiale valtellers in Cisco IOS-XE. Deze tellers tonen welke eigenschap het verkeer heeft laten vallen. Tot de voorbeelden van functies behoren Quality of Service (QoS), Network adresomzetting (NAT), Firewall, enzovoort.

2. Zodra de subfunctie is geïdentificeerd, vraag dan de granulaire druppeltellers die door de suboptie worden aangeboden. In deze handleiding is de 'suboptie' die wordt geanalyseerd de functie Firewall.

Wereldwijde tellers voor QFP's

De basisopdracht om op te bouwen biedt alle druppels in het QFP:

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

Deze opdracht toont aan dat de generieke druppels wereldwijd in het QFP vallen. Deze druppels kunnen op elke functie staan. Sommige voorbeeldfuncties zijn:

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

Om alle druppels te zien, omvat tellers die een waarde van nul hebben, de opdracht:

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

Gebruik deze opdracht om de tellers te verwijderen. De uitvoer wordt gewist nadat deze op het

scherm is weergegeven. Deze opdracht is vrij bij lezen, zodat de uitvoer **nadat** deze op het scherm is weergegeven weer op nul wordt gezet.

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

Hieronder staat een lijst met QFP-tellers voor wereldwijde firewalls en een verklaring:

Firewallalgemene Drop Reden	verklaring
Firewall-backpressie	Verval van pakketten door tegendruk door houtkapmechanisme.
FirewallOngeldigeZone	Geen beveiligingszone ingesteld voor een interface.
FirewallL4Insp	L4-beleidscontrole mislukt. Zie de onderstaande tabel om redenen van korreldruppels (redenen van firewallfunctie).
Firewall/NoForwardingZone	Firewall is niet geïnitialiseerd en er is geen verkeer toegestaan om door te ge
Firewallnonsessie	Sessiecreatie mislukt. Dit kan zijn doordat de maximale sessielimiet is bereik doordat de geheugentoewijzing is mislukt.
Firewallbeleid	Het geconfigureerde firewallbeleid is droog.
FirewallL4	L4-inspectiefout. Zie de onderstaande tabel om redenen van korreldruppels (redenen voor firewallfunctie).
FirewallL7	Daling van de verpakking door L7-inspectie. Zie hieronder voor een lijst met gedetailleerdere L7-uitvalredenen (redenen voor firewalls).
FirewallNotInitiator	Geen sessieinitiator voor TCP, UDP of ICMP. Er wordt geen sessie gemaakt Bijvoorbeeld, voor ICMP is het eerste ontvangen pakket niet ECHO of TIMESTAMP. Voor TCP is het geen SYN. Dit kan gebeuren bij normale pakketverwerking of bij onnauwkeurige kanaalverwerking.
Firewallgeen nieuwe sessie	Firewallhoge beschikbaarheid staat geen nieuwe sessies toe.
FirewallSynthetischMaxDst	Om de door de gastheer gebaseerde SYN-bescherming tegen overstroming bieden, is er een SYN-percentage per bestemming als de SYN-limiet voor de overstromingen. Wanneer het aantal doelitems de grenswaarde bereikt, word er nieuwe SYN-pakketten verzonden.
FirewallSyncie	De SYNCOOLIE-logica wordt geactiveerd. Dit geeft aan dat SYN/ACK met S koekje is verzonden en dat het oorspronkelijke SYN-pakket is gevallen.
Firewallstandaard	Asymmetric Routing is niet ingeschakeld en de groep redundantie is niet in actieve toestand.

Firewallfunctietellers op QFP

De beperking met de wereldwijde QFP-druppelteller is dat er geen granulariteit in de uitvalredenen is en dat sommige uitvalredenen zoals **FirewallL4** zo overbelast zijn dat het van weinig nut is voor het oplossen van problemen. Dit is sindsdien verbeterd in Cisco IOS-XE 3.9 (15.3(2)S), waar de de optie van de de Zet tellers van de Firewall werd toegevoegd. Dit geeft een veel korter aantal drop-redenen:

```
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
....
```

Hieronder staat een lijst met redenen voor firewalls en een verklaring:

Redundantie van firewallfunctie	verklaring
Ongeldige lengte van header	Het datagram is zo klein dat het laag 4TCP-, UDP- of ICMP-header niet kan bevatten. Het zou veroorzaakt kunnen worden door: 1. TCP-headerlengte < 20 2. UDP/ICMP-headerlengte < 8
Ongeldige lengte van UDP-gegevens	De lengte van het UDP-datagram komt niet overeen met de lengte die in de UDP-header is opgegeven.
Ongeldig ACK-nummer	Deze daling kan worden veroorzaakt door een van deze redenen: 1. ACK is niet gelijk aan next_seq# van de TCP peer. 2. ACK is groter dan de meest recente SEQ# die door de TCP peer wordt verzonden.
Ongeldige ACK-markering	In de staat TCP SYNSENT en SYNRCVD wordt verwacht dat ACK# gelijk is aan ISN+1 maar dat is het niet. Deze daling kan worden veroorzaakt door een van deze redenen: 1. Verwacht ACK vlag maar niet ingesteld in verschillende TCP status. 2. Naast de ACK-vlag is ook een andere vlag (zoals RST) ingesteld.
Ongeldige TCP-initiator	Dit gebeurt wanneer: 1. Het eerste pakket van een TCP initiator is geen SYN (het niet-initiële TCP segment wordt ontvangen zonder een geldige sessie). 2. Het eerste SYN-pakket heeft de ACK-markeringsset.
SYN met gegevens	Het SYN-pakket bevat lading. Dit wordt niet ondersteund.
Ongeldige TCP-vlaggen	Ongeldige TCP-vlaggen kunnen worden veroorzaakt door: 1. TCP-beginpakket SYN heeft andere vlaggen dan SYN. 2. In TCP-luisterstaat ontvangt een TCP-peer een RST of een ACK. 3. Het pakket van de andere responder wordt ontvangen vóór SYN/ACK. 4. Verwacht SYN/ACK wordt niet ontvangen van de responder.
Ongeldig segmenteren in SYNSENT-status	Een ongeldig TCP-segment in SYNSENT-status wordt veroorzaakt door: 1. SYN/ACK heeft lading. 2. SYN/ACK heeft andere vlaggen (PSH, URG, FIN) ingesteld. 3. Ontvang een doorvoersysteem met lading. 4. Ontvang een niet-SYN pakket van initiatiefnemer.
Ongeldig segmenteren in de staat SYNRCVD	Een ongeldig TCP-segment in SYNRCVD-status kan worden veroorzaakt door: 1. Ontvang een doorvoerSYN met payload van de initiator. 2. Ontvang een ongeldig segment dat niet SYN/ACK, RST, of FIN van de responder is.
Ongeldige SEQ	Dit gebeurt in de SYNRCVD-status wanneer segmenten van de initiator afkomstig zijn. Het wordt veroorzaakt door: 1. Seq# is minder dan ISN. 2. Als ontvanger de cvd venstergrootte 0 en: Segment een lading heeft, of Uit ordersegment (seq# is groter dan ontvanger LASTACK. 3. Als ontvanger de cvd venstergrootte 0 is en seq# valt voorbij het venster. 4. Seq# is gelijk aan ISN maar geen SYN pakket.

Ongeldige optie voor venstergrootte	De ongeldige optie van de schaal van het TCP venster wordt veroorzaakt door de onjuiste optie van de venster schaal door de lengte.
TCP buiten het venster	Packet is te oud - één venster achter de ACK van de andere kant. Dit zou kunnen gebeuren in VESTIGDE, CLOSEWAIT en LASTACK toestand.
TCP extra lading na verzonden FIN	Loonlading ontvangen na verzending van FIN. Dit zou kunnen gebeuren in CLOSEWAIT-toestand.
TCP-vensteroverflow	Dit gebeurt wanneer de inkomende segmentgrootte het venster van de ontvanger overstroomt. Als vTCP echter is ingeschakeld, is deze voorwaarde toegestaan omdat de firewall het segment moet bufferen zodat ALG later kan consumeren.
Doorlopen met ongeldige vlaggen	Een herverzonden pakket werd reeds door de ontvanger erkend.
TCP op end-of-order segment	Het out-of-order pakket staat op het punt om aan L7 te worden geleverd voor inspectie. Als L7 OO-segment niet toestaat zal dit pakket vallen.
SYN Flood	Onder een TCP SYN-overstroming. Onder bepaalde omstandigheden wanneer de huidige verbindingen met deze host hoger zijn dan de geconfigureerde half-open waarde, wijst de firewall alle nieuwe verbindingen met dit IP-adres voor een bepaalde tijd af. Als resultaat hiervan worden de pakketten verzonden.
Interne fout - controle van synoverstroming mislukt	Tijdens de controle van de synoverstroming faalt de toewijzing van de hostdb. Aanbevolen actie: check "show platform hardware qfp active function firewallgeheugen" om de geheugenstatus te controleren.
Synoverstromingsblokkering	Als de ingestelde halve open verbindingen worden overschreden en de uitstroomtijd is ingesteld, wordt alle nieuwe verbinding met dit IP-adres verbroken.
Half-Open sessie limiet overschreden	Verpakte pakketten vanwege de toegestane halve geopende sessies overschreden. Controleer ook de instellingen van "max-incomplete high/low" en "one-minuut high/low" om er zeker van te zijn dat # van half geopende sessies niet door deze configuraties worden gesloopt.
Te veel pakketsnelheid per stroom	Het maximum aantal controleerbare pakketten dat per stroom wordt toegestaan wordt overschreden. Het maximum aantal is 25.
Te veel ICMP-foutpakketten per flow	Het maximale aantal ICMP-foutpakketten dat per flow is toegestaan, wordt overschreden. Het maximum aantal is 3.
Onverwacht TCP-lading van RSP naar Init	In de staat SYNRCVD ontvangt TCP een pakket met lading van responder naar initiator richting.
Interne fout - niet-gedefinieerde richting	Packet-richting niet gedefinieerd.
SYN binnen venster	Een SYN-pakket wordt gezien in het venster van een reeds bestaande TCP-verbinding.
RST binnen stroomvenster	Een RST-pakket wordt waargenomen binnen het venster van een reeds bestaande TCP-verbinding.
segmenteren	Een TCP-segment wordt ontvangen dat niet via de TCP-staatsmachine had mogen worden ontvangen, zoals een TCP SYN-pakket dat in de luisterstaat is ontvangen vanaf de responder.
ICMP interne fout - gemiste ICMP NAT-informatie	Het ICMP-pakket is leeg maar interne NAT-informatie ontbreekt. Dit is een interne fout.
ICMP-pakje in SCB-status sluiten	Ontvang een ICMP-pakket in de status SCB CLOSE.
Gemiste IP-header in ICMP-	Ontbrekende IP-header in ICMP-pakket.

pakket	
ICMP-fout geen IP of ICMP	ICMP-foutpakket zonder IP of ICMP-lading. Waarschijnlijk veroorzaakt door een misvormd pakje of een aanval.
ICMP Err. te kort	ICMP-foutenpakket is te kort.
ICMP-erf-limiet overschreden	De ICMP-foutenmarkt overschrijdt de barstlimiet van 10.
ICMP fout onbereikbaar	De onbereikbare ICMP-foutmelding overschrijdt de limiet. Alleen het 1ste onbereikbare pakje is toegestaan om door te geven.
ICMP Err Ongeldig Seq#	Seq# ingesloten pakketjes komt niet overeen met het volgende nummer van het pakket dat op de ICMP-fout gebaseerd is.
Ongeldige Actie van ICMP-fout	Ongeldige ACK in het ICMP-fout ingesloten pakket.
ICMP-actie	De geconfigureerde ICMP-actie is droog.
Zone-paar zonder beleidskaart	Geen beleid op zonpaar. Het kan zijn dat ALG (Application Layer Gateway) niet is geconfigureerd om speldengat te openen voor applicatiegegevenskanaal, of dat ALG het speldengat niet correct heeft geopend of dat er geen speldengat is geopend door schaalbaarheidsproblemen.
sessie gemist en beleid niet aanwezig	De raadpleging van de sessie is mislukt en er is geen beleid aanwezig om dit pakket te inspecteren.
ICMP-fout en -beleid niet aanwezig	ICMP-fout zonder beleid ingesteld op zonepaar.
Classificatie mislukt	Classificatie faalt in een gegeven zone paar wanneer Firewall probeert te bepalen of het protocol kan worden geïnspecteerd.
Classificatie	De classificatieactie is droog.
Beveiligingsbeleid	Indeling mislukt vanwege verkeerde configuratie van beveiligingsbeleid. Dit zou ook te wijten kunnen zijn aan geen pinpool voor het L7-gegevenskanaal.
RST naar responder sturen	Verzend RST naar responder in SYNSENT status wanneer ACK# niet gelijk is aan ISN+1.
Firewallbeleid - val	Beleidsmaatregelen moeten vallen.
Fragment Drop	Laat resterende fragmenten vallen wanneer het eerste fragment is gevallen.
ICMP-beleidsdrop	Beleidsactie van het ICMP ingesloten pakket is DROP.
L7 Inspectieaangifte DROP	L7 (ALG) besluit de verpakking te laten vallen. De reden hiervoor is te vinden uit verschillende ALG statistieken.
L7 segmentering is niet toegestaan	Ontvang gesegmenteerd pakje wanneer ALG het niet naleeft.
L7 fragmentatieproduct niet toegestaan	Ontworpen gefragmenteerde (of VFR) pakketten wanneer ALG het niet naleeft.
Onbekend type L7 Proto	Niet-herkend protocoltype.

Firewall voor probleemoplossing:

Als de drop-reden is geïdentificeerd in de hierboven genoemde loketten of firewallfuncties, kunnen extra stappen voor het oplossen van problemen nodig zijn als deze druppels onverwacht zijn. Naast configuratie validatie om er zeker van te zijn dat de configuratie juist is voor de firewallfuncties die ingeschakeld zijn, wordt het vaak vereist om pakketvastlegging voor de verkeersstroom in kwestie te nemen om te zien of de pakketten niet zijn vormgegeven of dat er problemen zijn met de implementatie van een protocol of toepassing.

Vastlegging

ASR-logfunctionaliteit genereert syslogs om gedode pakketten op te nemen. Deze symbolen geven meer informatie over de reden waarom het pakje is gevallen. Er zijn twee soorten syslogings:

1. Plaatselijke gebufferde blokkering

2. Afstandsbediening van hoge snelheid

Plaatselijk gebufferde systeem

Om de oorzaak van de druppels te isoleren, kunt u algemene ZBFW-probleemoplossing gebruiken, zoals het inschakelen van logdruppels. Er zijn twee manieren om pakketblokkering te configureren.

Methode 1: Gebruik parameter-map voor het inspecteren van alle gedeponeerde pakketten.

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

Methode 2: Gebruik aangepaste inspectie parameter-map om geworpen pakketten voor slechts specifieke klasse te registreren.

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

Deze berichten worden naar het logbestand of de console gestuurd, afhankelijk van de manier waarop de ASR voor houtkap is ingesteld. Hier is een voorbeeld van een bericht van het droogrelog.

```
*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
```

Beperkingen van lokaal gebufferd systeem

1. Deze logbestanden zijn in snelheid beperkt volgens Cisco bug-ID CSCud09943.

2. Deze logbestanden kunnen mogelijk niet worden afgedrukt, tenzij er een specifieke configuratie wordt toegepast. Bijvoorbeeld, pakketten die door class-default pakketten worden gedropt zullen niet worden vastgelegd tenzij het **logsleutelwoord** is gespecificeerd:

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

Remote snelle vastlegging

High Speed logging (HSL) genereert systemen rechtstreeks vanuit het QFP en stuurt ze naar de geconfigureerde NetFlow HSL-verzamelaar. Dit is de aanbevolen logoplossing voor ZBFW op ASR.

Gebruik voor HSL deze configuratie:

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

Om deze configuratie te kunnen gebruiken, is een stroomverzamelaar vereist die NetFlow versie 9 kan gebruiken. Dit wordt gedetailleerd in

[Configuratiegids: Firewallgebaseerde beleidsfirewall, Cisco IOS XE release 3S (ASR 1000) snelle vastlegging voor firewall]

Packet Tracing-gebruik van voorwaardelijke matching

Zet voorwaardelijke debugs aan om het pakket overtrekken toe te staan en dan pakket overtrekken voor deze functies mogelijk te maken:

```
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
```

> Opmerking: De matchvoorwaarde kan het IP-adres direct gebruiken, aangezien ACL niet nodig is. Dit komt overeen als bron of bestemming die tweerichtingssporen toelaat. Deze methode kan worden gebruikt als u de configuratie niet kunt wijzigen. Bijvoorbeeld: debug platform conditie ipv4 adres 192.168.1.1/32.

Schakel de functie voor pakkettracering in:

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

Er zijn twee manieren om deze functie te gebruiken:

1. Voer de opdracht **platformoerspoor** in **om** alleen de gedropt pakketten te overtrekken.

2. Uitsluiting van de opdracht **debug platform pakketsporendroger** zal elk pakje dat aan de voorwaarde voldoet, dat ook pakketjes bevat die door het apparaat worden geïnspecteerd/doorgegeven.

Draai voorwaardelijke uitwerpselen open:

```
debug platform condition start
```

Draai de test uit en schakel vervolgens de leidingen uit:

```
debug platform condition stop
```

U kunt de informatie nu op het scherm weergeven. In dit voorbeeld werden ICMP-pakketten verzonden vanwege een firewallbeleid:

```
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
```

Het **pakketsporingspakket <num> decode** van het **platform** toont, decodeert de informatie en

inhoud van de pakketheader. Deze optie is toegevoegd 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
```

Ingesloten pakketvastlegging

Ondersteuning voor ingesloten pakketvastlegging is toegevoegd in Cisco IOS-XE 3.7 (15.2(4)S). Zie voor meer informatie

Configuratievoorbeeld van Embedded Packet Capture voor Cisco IOS en IOS-XE.

Debugs

voorwaartse uitwerpselen

In XE3.10 worden voorwaardelijke deposito's geïntroduceerd. Er kunnen voorwaardelijke verklaringen worden gebruikt om er zeker van te zijn dat de ZBFW optie alleen weblogs bevat die berichten bevatten die relevant zijn voor de aandoening. Voorwaardelijke versies maken gebruik van ACL's om stammen te beperken die overeenkomen met de ACL-elementen. Ook waren de debug-berichten vóór XE3.10 moeilijker te lezen. De debug-uitvoer werd in XE3.10 verbeterd om ze beter te begrijpen.

U geeft deze opdracht als volgt uit:

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

Merk op dat de conditieopdracht via een ACL en directionaliteit moet worden ingesteld. De voorwaardelijke vereisten zullen niet worden geïmplementeerd totdat het begin is begonnen met de opdracht **debug platform conditie**. Om voorwaardelijke insecten uit te schakelen gebruikt de opdracht **debug platform conditie stop**.

```
debug platform condition stop
```

Om voorwaardelijke debugs uit te schakelen, **NIET** gebruikt u de opdracht **undebug all**. Gebruik de opdracht om alle voorwaardelijke signalen uit te schakelen:

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

Vóór XE3.14 zijn **ha** en **gebeurtenissen** onvoorwaardelijk. Als resultaat hiervan **debug** de **functie voor** het **platform conditioneren** van de **volgende dataplane submodus** zorgt **de opdracht** ervoor dat alle logbestanden worden gemaakt, onafhankelijk van de onderstaande conditie. Dit zou extra lawaai kunnen creëren dat het zuiveren moeilijk maakt.

Standaard is het voorwaardelijke houtlogniveau **informatie**. Gebruik de opdracht om het niveau van houtkap te verhogen of te verlagen:

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

Debugs verzamelen en bekijken

Debug bestanden worden niet op de console of monitor afgedrukt. Alle apparaten worden op de harde schijf van de ASR geschreven. Debugs worden op de vaste schijf geschreven onder de map **tracelogs** met de naam **cpp_cp_F0-0.log.<date>**. Gebruik de output om het bestand te bekijken waar debugs worden geschreven:

```
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)
```

Elk debug-bestand wordt opgeslagen als een **cpp_cp_F0-0.log<date>**-bestand. Dit zijn reguliere tekstbestanden die met TFTP kunnen worden gekopieerd van de ASR. Het maximum logbestand in de ASR is 1 MB. Na 1 MB worden de debugs naar een nieuw logbestand geschreven. Dat is waarom elk logbestand is voorzien van een tijdelijke stempel om het begin van het bestand aan te geven.

Logbestanden bestaan mogelijk op deze locaties:

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

Aangezien logbestanden alleen worden weergegeven nadat ze zijn gedraaid, kan het logbestand handmatig met deze opdracht worden gedraaid:

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

Dit maakt meteen een "cpp_cp" logbestand en start een nieuw bestand op het QFP. Bijvoorbeeld:

```
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)
```

Met deze opdracht kunnen de debug-bestanden in één bestand worden samengevoegd zodat ze

gemakkelijker kunnen worden verwerkt. Het combineert alle bestanden in de folder en interlaceert ze op basis van tijd. Dit kan helpen wanneer de logbestanden zeer omslachtig zijn en over meerdere bestanden worden gemaakt:

```
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]
```