Fehlerbehebungsleitfaden für die Konfiguration von ZBFW für IOS-XE

Inhalt

Einführung
Links und Dokumentation
Befehlsreferenzen
Schritte zur Datenpflege
Konfiguration überprüfen
Verbindungsstatus überprüfen
Firewall-Drop-Zähler überprüfen
Globale Drop-Zähler für QFP
Firewall Feature Drop Zähler für QFP
Fehlerbehebung bei Firewall-Ausfällen
Protokollierung
Lokales gepuffertes Syslogging
Einschränkungen bei der lokalen Syslogging-Protokollierung
Remote-Hochgeschwindigkeitsprotokollierung
Ablaufverfolgung von Paketen mithilfe von konditioneller Übereinstimmung
Integrierte Paketerfassung
Debugger
Bedingtes Debuggen
Erfassen und Anzeigen von Debuggern

Einführung

In diesem Dokument wird beschrieben, wie Sie die ZBFW-Funktion (Zone Based Firewall) auf dem Aggregation Services Router (ASR) 1000 am besten beheben können. Hierzu werden Befehle verwendet, mit denen die Hardware-Drop-Zähler auf dem ASR abgefragt werden. Die ASR1000 ist eine hardwarebasierte Weiterleitungsplattform. Die Softwarekonfiguration von Cisco IOS-XE® programmiert die Hardware-ASICs (Quantum Flow Processor (QFP)), um Funktionen zur Funktionsweiterleitung auszuführen. Dies ermöglicht einen höheren Durchsatz und eine bessere Leistung. Der Nachteil dabei ist, dass die Fehlerbehebung eine größere Herausforderung darstellt. Herkömmliche Cisco IOS-Befehle, die zum Abfragen aktueller Sitzungen und zum Ablegen von Zählern über eine zonenbasierte Firewall (ZBFW) verwendet werden, sind nicht mehr gültig, da diese in der Software nicht mehr enthalten sind.

Links und Dokumentation

Befehlsreferenzen

- Cisco Aggregation Services Router der Serie ASR 1000 - Befehlsreferenzen
- Cisco IOS XE 3S-Befehlsreferenzen

Schritte zur Datenpflege

Um eine Fehlerbehebung für den Datenpfad durchzuführen, müssen Sie ermitteln, ob der Datenverkehr ordnungsgemäß über den ASR- und den Cisco IOS-XE-Code geleitet wird. Speziell für Firewall-Funktionen führt die Datenpfadfehlerbehebung die folgenden Schritte aus:

1. **Konfiguration überprüfen** - Ermitteln Sie die Konfiguration, und überprüfen Sie die Ausgabe, um die Verbindung zu überprüfen.

2. **Verbindungsstatus überprüfen**: Wenn der Datenverkehr ordnungsgemäß verläuft, öffnet Cisco IOS-XE eine Verbindung mit der ZBFW-Funktion. Diese Verbindung verfolgt den Datenverkehr und die Statusinformationen zwischen einem Client und Server.

3. **Verifizieren von Drop-Zählern** - Wenn der Datenverkehr nicht ordnungsgemäß verläuft, protokolliert Cisco IOS-XE einen Drop-Zähler für verworfene Pakete. Überprüfen Sie diese Ausgabe, um die Ursache für den Datenverkehrsausfall zu identifizieren.

4. **Protokollierung** - Erfasst Syslogs, um detailliertere Informationen über Verbindungsbuilds und Paketverluste bereitzustellen.

5. **Paketverfolgung verlorene Pakete** - Mithilfe der Paketverfolgung können verlorene Pakete abgefangen werden.

6. **Debugs** - Die ausführlichste Option Debuggen sammeln. Debugger können nur bedingt abgerufen werden, um den genauen Weiterleitungspfad für die Pakete zu bestätigen.

Konfiguration überprüfen

Die Ergebnisse von **show tech support firewall** sind hier zusammengefasst:

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

Verbindungsstatus überprüfen

Verbindungsinformationen können abgerufen werden, sodass alle Verbindungen auf ZBFW aufgelistet sind. Geben Sie den folgenden Befehl ein:

```
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]
```

Es wird eine TCP-Telnet-Verbindung zwischen 14.38.112.250 und 14.36.1.206 angezeigt.

> **Hinweis**: Beachten Sie, dass es bei Ausführung dieses Befehls sehr lange dauert, wenn auf dem Gerät viele Verbindungen vorhanden sind. Cisco empfiehlt die Ausführung dieses Befehls mit speziellen Filtern, wie hier beschrieben.

Die Verbindungstabelle kann bis zu einer bestimmten Quell- oder Zieladresse gefiltert werden. Verwenden Sie Filter nach dem **Plattform-**Submodus. Folgende Filteroptionen stehen zur Verfügung:

```
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>
```

Diese Verbindungstabelle wird gefiltert, sodass nur Verbindungen angezeigt werden, die vom 14.38.112.250 stammen:

```
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]
```

Nach dem Filtern der Verbindungstabelle können die detaillierten Verbindungsinformationen für eine umfassendere Analyse abgerufen werden. Um diese Ausgabe anzuzeigen, verwenden Sie das **detail**-Schlüsselwort.

```
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
```

Firewall-Drop-Zähler überprüfen

Die Ausgabe des Drop-Zählers hat sich während XE 3.9 geändert. Vor XE 3.9 waren die Gründe für einen Firewall-Ausfall sehr allgemein. Nach XE 3.9 wurden die Gründe für den Firewall-Ausfall erweitert, um eine präzisere Handhabung zu ermöglichen.

Führen Sie zwei Schritte aus, um Drop-Zähler zu überprüfen:

1. Bestätigen Sie die globalen Drop-Zähler in Cisco IOS-XE. Diese Zähler zeigen an, welche Funktion den Datenverkehr verworfen hat. Beispiele für Funktionen sind Quality of Service (QoS), Network Address Translation (NAT), Firewall usw.

2. Nachdem die Unterfunktion identifiziert wurde, fragen Sie die detaillierten Ablagezähler ab, die von der Unterfunktion bereitgestellt werden. In diesem Leitfaden ist die zu analysierende Unterfunktion die Firewall-Funktion.

Globale Drop-Zähler für QFP

Der grundlegende Befehl, auf den man sich verlassen muss, enthält alle Dropdown-Menüs im QFP:

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

Dieser Befehl zeigt die globalen Drops im QFP an. Diese Drops können für jede Funktion verwendet werden. Einige Beispielfunktionen sind:

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

Um alle Verwerfen anzuzeigen, schließen Sie Zähler mit dem Wert 0 ein, verwenden Sie den folgenden Befehl:

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

Um die Zähler zu löschen, verwenden Sie diesen Befehl. Die Ausgabe wird gelöscht, nachdem sie auf dem Bildschirm angezeigt wurde. Dieser Befehl ist beim Lesen deutlich sichtbar, sodass die Ausgabe **nach** Anzeige auf dem Bildschirm auf Null zurückgesetzt wird.

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

Nachfolgend finden Sie eine Liste der globalen QFP-Firewall-Drop-Zähler und Erklärungen:

Globale Firewall-Sperrgrund	Erläuterung
Firewall-Backdruck	Paketverlust aufgrund von Rückdruck durch Protokollierungsmechanismus.
FirewallInvalidZone	Keine Sicherheitszone für die Schnittstelle konfiguriert.
FirewallL4insp	Fehler bei der L4-Richtlinienüberprüfung. In der Tabelle unten finden Sie detailliertere Gründe für das Verwerfen von Firewall-Funktionen (Gründe für d Verwerfen von Firewall-Funktionen).
FirewallNoForwardingZone	Die Firewall ist nicht initialisiert, und es darf kein Datenverkehr passieren.
FirewallKeine Sitzung	Die Sitzungserstellung schlägt fehl. Dies kann darauf zurückzuführen sein, da die maximale Sitzungsgrenze erreicht oder ein Speicherzuweisungsfehler aufgetreten ist.
FirewallPolicy	Die konfigurierte Firewall-Richtlinie wird verworfen.
FirewallL4	Fehler bei L4-Prüfung. Die nachfolgende Tabelle enthält detailliertere Gründe einen Ausfall der Firewall-Funktion.
FirewallL7	Paketverlust aufgrund von L7-Prüfung. Im Folgenden finden Sie eine Liste detaillierterer L7-Gründe (Gründe für Firewall-Feature-Drop).
FirewallNotInitiator	Kein Sitzungsinitiator für TCP, UDP oder ICMP. Es wird keine Sitzung erstellt ICMP ist das erste empfangene Paket beispielsweise nicht ECHO oder TIMESTAMP. Bei TCP handelt es sich nicht um ein SYN. Dies kann bei der normalen Paketverarbeitung oder bei der ungenauen Kanalverarbeitung der Fall sein.
FirewallNoNewSession	Die hohe Firewall-Verfügbarkeit lässt keine neuen Sitzungen zu.
FirewallSyncookieMaxDst	Um einen hostbasierten SYN-Flood-Schutz zu bieten, gibt es eine SYN-Rate Ziel als SYN-Flood-Grenzwert. Wenn die Anzahl der Zieleinträge die Grenze erreicht, werden neue SYN-Pakete verworfen.
FirewallSyncookie	SYNCOOLIE-Logik wird ausgelöst. Dies weist darauf hin, dass SYN/ACK mit SYN-Cookie gesendet wurde und das ursprüngliche SYN-Paket verworfen wu
FirewallARStandby	Asymmetric Routing ist nicht aktiviert, und die Redundanzgruppe ist nicht im aktiven Zustand.

Firewall Feature Drop Zähler für QFP

Die Einschränkung beim globalen QFP-Drop-Zähler besteht darin, dass die Drop-Gründe nicht präzise genug sind, und einige Gründe wie **FirewallL4** werden so überlastet, dass sie für die Fehlerbehebung wenig nützlich sind. Dies wurde seither in Cisco IOS-XE 3.9 (15.3(2)S) verbessert, wo die Zähler für die Firewall-Feature-Drop hinzugefügt wurden. Dies führt zu einer sehr viel präziseren Auswahl an Gründen:

```
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
....
```

Im Folgenden finden Sie eine Liste mit Gründen und Erklärungen zu Firewall-Funktionen:

Firewall-Feature-Dropdown-Grund	Erläuterung
Ungültige Headerlänge	Das Datagramm ist so klein, dass es den Layer-4-TCP-, UDP- oder ICMP-Header nicht enthalten konnte. Dies kann durch folgende Faktoren verursacht werden: 1. TCP-Header-Länge < 20 2. UDP-/ICMP-Headerlänge < 8
Ungültige UDP-Datenlänge	Die UDP-Datagrammlänge stimmt nicht mit der im UDP-Header angegebenen Länge überein.
Ungültige ACK-Nummer	Dieser Rückgang könnte auf einen der folgenden Gründe zurückzuführen sein: 1. ACK entspricht nicht dem nächsten_seq# des TCP-Peers. 2. Das ACK ist größer als der letzte vom TCP-Peer gesendete FF#.
Ungültige ACK-Markierung	Im TCP-SYNSENT- und SYNRCVD-Zustand wird erwartet, dass die ACK# gleich ISN+1 ist, dies jedoch nicht. Dieser Rückgang könnte auf einen der folgenden Gründe zurückzuführen sein: 1. ACK-Flag wird erwartet, jedoch nicht in einem anderen TCP-Status festgelegt. 2. Außer dem ACK-Flag wird auch ein anderes Flag (wie RST) gesetzt.
Ungültiger TCP-Initiator	Dies geschieht in folgenden Fällen: 1. Das erste Paket von einem TCP-Initiator ist keine SYN (kein initiales TCP-Segment wird ohne gültige Sitzung empfangen). 2. Für das erste SYN-Paket ist das ACK-Flag festgelegt.
SYN mit Daten	Das SYN-Paket enthält Payload. Dies wird nicht unterstützt.
Ungültige TCP-Flags	Ungültige TCP-Flags können durch Folgendes verursacht werden: 1. Das erste TCP-SYN-Paket enthält andere Flags als SYN. 2. Im TCP-Listen-Zustand empfängt ein TCP-Peer einen RST oder ein ACK. 3. Das Paket des anderen Responders wird vor SYN/ACK empfangen. 4. Die erwartete SYN/ACK-Nummer wird nicht vom Responder empfangen.
Ungültiges Segment im SYNSENT-Status	Ein ungültiges TCP-Segment im SYNSENT-Status wird verursacht durch: 1. SYN/ACK hat Payload. 2. SYN/ACK hat andere Flags (PSH, URG, FIN) gesetzt. 3. Empfangen einer Transit-SYN mit Nutzlast. 4. Empfangen eines Nicht-SYN-Pakets vom Initiator.
Ungültiges Segment im SYNRCVD-Status	Ein ungültiges TCP-Segment im SYNRCVD-Status könnte durch folgende Faktoren verursacht werden: 1. Empfangen einer SYN für die erneute Übertragung mit Payload vom Initiator. 2. Erhalten Sie vom Responder ein ungültiges Segment, das nicht

Ungültiges Format	SYN/ACK, RST oder FIN ist. Dies tritt im SYNRCVD-Zustand auf, wenn Segmente vom Initiator stammen. Sie wird verursacht durch: 1. Seq# ist kleiner als ISN. 2. Wenn die Größe des rcvd-Fensters des Empfängers 0 und ist: Segment hat Nutzlast oder Out of Order Segment (seq# ist größer als Empfänger LASTACK. 3. Wenn der Empfänger rcvd Fenstergröße 0 ist und seq# über das Fenster fällt. 4. Seq# entspricht ISN, aber kein SYN-Paket.
Ungültige Fensterskalierungsoption	Die Option für die TCP-Fensterskalierung ist ungültig, da die Option für die Fenstergröße in Byte-Länge falsch ist.
TCP außerhalb des Fensters	Das Paket ist zu alt - ein Fenster hinter dem ACK der anderen Seite. Dies kann im Status ESTABLISHED, CLOSEWAIT und LASTACK geschehen.
TCP-zusätzliche Payload nach Versand von FIN	Payload, die nach dem Senden der FIN-Nachricht empfangen wurde. Dies könnte im CLOSEWAIT-Staat passieren.
TCP Window Overflow	Dies tritt auf, wenn die Größe eingehender Segmente das Fenster des Empfängers überschreibt. Wenn jedoch vTCP aktiviert ist, ist diese Bedingung zulässig, da die Firewall das Segment puffern muss, damit ALG es später nutzen kann.
Wiederholt mit ungültigen Flags	Ein erneut übertragenes Paket wurde bereits vom Empfänger bestätigt.
TCP-Out-of-Order-Segment	Das Out-of-Order-Paket wird bald zur Prüfung an L7 geliefert. Wenn L7 kein OOO-Segment zulässt, wird dieses Paket verworfen.
SYN Flood	Bei einem TCP SYN Flood-Angriff. Unter bestimmten Bedingungen, wenn die aktuellen Verbindungen zu diesem Host den konfigurierten halb-offenen Wert überschreiten, lehnt die Firewall neue Verbindungen zu dieser IP-Adresse für einen bestimmten Zeitraum ab. Dadurch werden die Pakete verworfen.
Interner Fehler - Synflood-Überprüfung fehlerhaft	Bei der Synflood-Überprüfung schlägt die Zuweisung von hostdb fehl. Empfohlene Aktion: Aktivieren Sie "show platform hardware qfp active feature firewall memory" (Plattform-Hardware-QFP-Firewall-Arbeitsspeicher anzeigen), um den Speicherstatus zu überprüfen.
Synflood Blackout Drop	Wenn konfigurierte Half-Open-Verbindungen überschritten und die Blackout-Zeit konfiguriert wird, werden alle neuen Verbindungen zu dieser IP-Adresse verworfen.
Halboffene Sitzungsbegrenzung überschritten	Das aufgrund der zulässigen halb geöffneten Sitzungen verworfene Paket wurde überschritten. Überprüfen Sie außerdem die Einstellungen für "max-uncomplete high/low" und "one minute high/low", um sicherzustellen, dass die Anzahl der halb geöffneten Sitzungen durch diese Konfigurationen nicht gedrosselt wird.
Zu viele Pkt pro Fluss	Die maximal zulässige Anzahl an überprüfbaren Paketen pro Datenfluss wird überschritten. Die maximale Anzahl beträgt 25.
Zu viele ICMP-Fehlerpakete pro Flow	Die maximal zulässige Anzahl an ICMP-Fehlerpaketen pro Datenfluss wird überschritten. Die maximale Anzahl beträgt 3.
Unerwartete TCP-Payload vom RSP zum Init	Im SYNRCVD-Status empfängt TCP ein Paket mit Payload vom Responder auf die Richtung des Initiators.

Interner Fehler - Nicht definierte Richtung	Paketrichtung nicht definiert.
SYN im aktuellen Fenster	Ein SYN-Paket wird im Fenster einer bereits bestehenden TCP-Verbindung angezeigt.
RST im aktuellen Fenster	Ein RST-Paket wird im Fenster einer bereits bestehenden TCP-Verbindung beobachtet.
Streamsegment	Es wird ein TCP-Segment empfangen, das nicht über den TCP-Statuscomputer empfangen werden sollte, z. B. ein TCP-SYN-Paket, das vom Responder im Listen-Zustand empfangen wurde.
Interner ICMP-Fehler - fehlende ICMP NAT-Informationen	Das ICMP-Paket ist nicht vorhanden, aber interne NAT-Informationen fehlen. Dies ist ein interner Fehler.
ICMP-Paket im SCB-Nahzustand	ICMP-Paket im SCB CLOSE-Status empfangen.
Verpasster IP-Header im ICMP-Paket	IP-Header im ICMP-Paket fehlt.
ICMP-Fehler Keine IP oder ICMP	ICMP-Fehlerpaket ohne IP oder ICMP in Nutzlast. Wird wahrscheinlich durch ein fehlerhaftes Paket oder einen Angriff verursacht.
ICMP-Err-Pkt zu kurz	Das ICMP-Fehlerpaket ist zu kurz.
ICMP-Fehler überschreitet Burst-Grenzwert	ICMP Error Pkt überschreitet die Burst-Grenze von 10.
ICMP-Fehler nicht erreichbar	Der ICMP-Fehler Pkt nicht erreichbar überschreitet den Grenzwert. Nur das 1. nicht erreichbare Paket darf passieren.
ICMP-Fehler ungültiges Suchkennzeichen	Die SEQ# des integrierten Pakets entspricht nicht der seq# des Pakets, das den ICMP-Fehler auslöst.
ICMP-Fehler ungültig	Ungültiges ACK im integrierten ICMP-Fehler-Paket.
ICMP Action Drop	Die konfigurierte ICMP-Aktion wird verworfen.
Zonenpaar ohne Richtlinienzuweisung	Die Richtlinie ist für Zonenpaar nicht vorhanden. Dies kann darauf zurückzuführen sein, dass ALG (Application Layer Gateway) nicht so konfiguriert wurde, dass das Nadelloch für den Anwendungsdatenkanal geöffnet wird, dass ALG das Pinloch nicht richtig geöffnet hat oder dass aufgrund von Skalierbarkeitsproblemen kein Pinloch geöffnet wird.
Sitzung fehlt, Richtlinie nicht vorhanden	Sitzungssuche fehlgeschlagen, und es ist keine Richtlinie vorhanden, um dieses Paket zu überprüfen.
ICMP-Fehler und -Richtlinie nicht vorhanden	ICMP-Fehler ohne Konfiguration einer Richtlinie für Zonenpaar.
Klassifizierung fehlgeschlagen	Klassifizierungsfehler in einem bestimmten Zonenpaar, wenn die Firewall versucht festzustellen, ob das Protokoll inspizierbar ist.
Löschung einer Klassifizierungsaktion	Die Klassifizierungsaktion wird gelöscht.
Misconfig der Sicherheitsrichtlinie	Fehlgeschlagene Klassifizierung aufgrund einer fehlerhaften Konfiguration der Sicherheitsrichtlinien. Dies kann auch darauf zurückzuführen sein, dass für den L7-Datenkanal kein Pinpol vorhanden ist.
RST an Antwort senden	Senden Sie RST an Responder im SYNSENT-Status, wenn ACK# nicht gleich ISN+1 ist.
Firewall-Policy-Drop	Policy Action is to drop.
Fragment-Verlust	Verbleibende Fragmente werden gelöscht, wenn das erste Fragment verworfen wird.
ICMP-Firewall Policy Drop	Die Richtlinienaktion des integrierten ICMP-Pakets lautet DROP.

L7-Inspektionsrücksendungen DROP	L7 (ALG) beschließt, Pakete zu verwerfen. Der Grund hierfür kann aus verschiedenen ALG-Statistiken abgeleitet werden.
L7-Segment-Pkt nicht zulassen	Empfangenes segmentiertes Paket, wenn ALG es nicht einhält.
L7 Fragment-Pkt nicht zulassen	Empfangene fragmentierte (oder VFR-)Pakete, wenn ALG sie nicht einhält.
Unbekannter L7-Prootyp	Nicht erkannter Protokolltyp.

Fehlerbehebung bei Firewall-Ausfällen

Sobald der Grund für den Ausfall anhand der oben genannten globalen oder Firewall-Feature-Drop-Zähler identifiziert wurde, können weitere Schritte zur Fehlerbehebung erforderlich sein, wenn diese Verwerfen unerwartet auftreten. Abgesehen von der Konfigurationsvalidierung muss für den betreffenden Datenverkehrsfluss häufig eine Paketerfassung durchgeführt werden, um sicherzustellen, dass die Konfiguration für die aktivierten Firewall-Funktionen korrekt ist, um festzustellen, ob die Pakete fehlerhaft sind oder ob Probleme mit der Protokoll- oder Anwendungsimplementierung vorliegen.

Protokollierung

Die ASR-Protokollierungsfunktion generiert Syslogs, um verlorene Pakete aufzuzeichnen. Diese Syslogs liefern weitere Details darüber, warum das Paket verworfen wurde. Es gibt zwei Arten von Sysloggings:

1. Lokale gepufferte Syslogging-Protokollierung

2. Remote-Hochgeschwindigkeitsprotokollierung

Lokales gepuffertes Syslogging

Um die Ursache der Verwerfen zu isolieren, können Sie eine generische ZBFW-Fehlerbehebung verwenden, z. B. das Aktivieren von Protokollverwerfen. Die Protokollierung von Paketverlusten kann auf zwei Arten konfiguriert werden.

Methode 1: Verwenden Sie inspect-global parameter-map, um alle verworfenen Pakete zu protokollieren.

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

Methode 2: Verwenden Sie eine benutzerdefinierte inspect parameter-map, um verlorene Pakete nur für eine bestimmte Klasse zu protokollieren.

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

Diese Meldungen werden je nach Konfiguration des ASR für die Protokollierung an das Protokoll oder die Konsole gesendet. Hier sehen Sie ein Beispiel für eine Drop-Log-Meldung.

```
*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
```

Einschränkungen bei der lokalen Syslogging-Protokollierung

1. Diese Protokolle sind gemäß Cisco Bug ID CSCud09943 begrenzt.

2. Diese Protokolle werden möglicherweise nur gedruckt, wenn eine spezifische Konfiguration angewendet wurde. Beispielsweise werden Pakete, die durch Standardpakete der Klasse verworfen wurden, nur protokolliert, wenn das **log-**Schlüsselwort angegeben wurde:

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

Remote-Hochgeschwindigkeitsprotokollierung

Hochgeschwindigkeitsprotokollierung (HSL) erzeugt Syslogs direkt vom QFP und sendet sie an den konfigurierten NetFlow HSL Collector. Dies ist die empfohlene Protokollierungslösung für die ZBFW auf dem ASR.

Verwenden Sie für HSL folgende Konfiguration:

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

Um diese Konfiguration verwenden zu können, ist ein NetFlow Collector erforderlich, der Netflow Version 9 unterstützen kann. Dies wird in detailliert beschrieben.

Konfigurationsanleitung: Zonenbasierte Firewall, Cisco IOS XE Release 3S (ASR 1000), Firewall Hochgeschwindigkeits-Protokollierung

Ablaufverfolgung von Paketen mithilfe von konditioneller Übereinstimmung

Aktivieren Sie bedingtes Debuggen, um die Paketverfolgung zu aktivieren und anschließend die Paketverfolgung für die folgenden Funktionen zu aktivieren:

```
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
```

Hinweis: Die Übereinstimmung-Bedingung kann die IP-Adresse direkt verwenden, da keine ACL erforderlich ist. Dies entspricht als Quelle oder Ziel, das bidirektionale Spuren ermöglicht. Diese Methode kann verwendet werden, wenn Sie die Konfiguration nicht ändern dürfen. Beispiel: debug plattform condition ipv4 address 192.168.1.1/32.

Aktivieren Sie die Funktion zur Paketverfolgung:

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

Es gibt zwei Möglichkeiten, diese Funktion zu verwenden:

1. Geben Sie den Befehl **debug platform packet-trace ein**, um nur die verworfenen Pakete zu verfolgen.

2. Durch den Ausschluss des Befehls **debug platform packet-trace drop** werden alle Pakete verfolgt, die mit der Bedingung übereinstimmen, einschließlich der Pakete, die vom Gerät geprüft/übergeben werden.

Aktivieren von bedingtem Debuggen:

```
debug platform condition start
```

Führen Sie den Test aus, und deaktivieren Sie dann die Debugger:

```
debug platform condition stop
```

Jetzt können die Informationen auf dem Bildschirm angezeigt werden. In diesem Beispiel wurden ICMP-Pakete aufgrund einer Firewall-Richtlinie verworfen:

```
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
```

Der Befehl show platform packet-trace paket <num> decode dekodiert die Informationen und den Inhalt des Paket-Headers. Diese Funktion wurde in XE3.11 eingeführt:

```
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
```

Integrierte Paketerfassung

Die integrierte Paketerfassungs-Unterstützung wurde in Cisco IOS-XE 3.7 (15.2(4)S) hinzugefügt. Weitere Informationen finden Sie unter

Integrierte Paketerfassung für Cisco IOS und IOS-XE - Konfigurationsbeispiel.

Debugger

Bedingtes Debuggen

In XE3.10 werden bedingte Debuggen eingeführt. Bedingte Anweisungen können verwendet werden, um sicherzustellen, dass die ZBFW-Funktion nur Debugmeldungen protokolliert, die für die Bedingung relevant sind. Bei der bedingten Fehlersuche werden ACLs verwendet, um Protokolle zu beschränken, die den ACL-Elementen entsprechen. Vor XE3.10 waren die Debug-Meldungen außerdem schwieriger zu lesen. Die Debug-Ausgabe wurde in XE3.10 verbessert, um sie einfacher zu verstehen.

Führen Sie folgenden Befehl aus, um diese Debugger zu aktivieren:

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

Beachten Sie, dass der Condition-Befehl über eine ACL und eine Direktionalität festgelegt werden muss. Die bedingten Debuggen werden erst implementiert, wenn sie mit dem Befehl **debug platform condition start** gestartet werden. Um bedingte Debuggen zu deaktivieren, verwenden Sie den Befehl **debug platform condition stop**.

```
debug platform condition stop
```

Um bedingte Debuggen zu deaktivieren, verwenden **Sie NICHT** den Befehl **undebug all**. Verwenden Sie den folgenden Befehl, um alle bedingten Debugging-Vorgänge zu deaktivieren:

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

Vor XE3.14 sind **ha-** und **Ereignis-**Debug nicht bedingt. Infolgedessen **ermöglicht** der Befehl **debug platform condition fw dataplane submode all** die Erstellung aller Protokolle, unabhängig von der unten ausgewählten Bedingung. Dies kann zu zusätzlichen Geräuschen führen, die das Debuggen erschweren.

Standardmäßig ist die bedingte Protokollierungsebene **info**. Um die Protokollierungsebene zu erhöhen/zu verringern, verwenden Sie den folgenden Befehl:

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

Erfassen und Anzeigen von Debuggern

Debugdateien werden nicht auf die Konsole oder den Monitor gedruckt. Alle DebuggingInnen werden auf die Festplatte des ASR geschrieben. Debugger werden unter dem Ordner **tracelogs** mit dem Namen **cpp_cp_F0-0.log auf die** Festplatte geschrieben. Um die Datei anzuzeigen, in der Debugger geschrieben sind, verwenden Sie die Ausgabe:

```
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)
```

Jede Debugdatei wird als **cpp_cp_F0-0.log.<date>**-Datei gespeichert. Dabei handelt es sich um reguläre Textdateien, die mit TFTP aus dem ASR kopiert werden können. Die maximale Protokolldatei auf dem ASR beträgt 1 MB. Nach 1 MB werden die Debugger in eine neue Protokolldatei geschrieben. Aus diesem Grund wird jede Protokolldatei mit einem Zeitstempel versehen, um den Start der Datei anzuzeigen.

Protokolldateien können an diesen Speicherorten vorhanden sein:

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

Da Protokolldateien erst nach dem Rotieren angezeigt werden, kann die Protokolldatei mit dem folgenden Befehl manuell rotiert werden:

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

Dadurch wird sofort eine "cpp_cp"-Protokolldatei erstellt und eine neue Datei im QFP gestartet. Beispiel:

```
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)
```

Mit diesem Befehl können die Debugdateien zur Vereinfachung der Verarbeitung in einer einzelnen Datei zusammengeführt werden. Es führt alle Dateien im Verzeichnis zusammen und überschneidet sie je nach Zeit. Dies kann hilfreich sein, wenn die Protokolle sehr ausführlich sind und über mehrere Dateien hinweg erstellt werden:

```
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]
```