Fehlerbehebung bei Fehlern bei der ASA-Schnittstellenüberlaufanzeige

Inhalt

Einführung

Dieses Dokument beschreibt den Fehlerzähler "overrun" und wie Leistungsprobleme oder Paketverluste im Netzwerk untersucht werden können. Möglicherweise bemerken Administratoren Fehler, die in der Ausgabe des Befehls **show interface** auf der Adaptive Security Appliance (ASA) gemeldet wurden.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

Der Fehlerzähler "overrun" für die ASA-Schnittstelle verfolgt die Anzahl der Aufrufe eines Pakets an der Netzwerkschnittstelle, es war jedoch kein verfügbarer Speicherplatz in der FIFO-Warteschlange für die Speicherung des Pakets vorhanden. Daher wurde das Paket verworfen. Der Wert dieses Zählers wird mit dem Befehl **show interface** angezeigt.

Beispielausgabe, die das Problem anzeigt:

```
ASA# show interface GigabitEthernet0/1
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
Full-Duplex(Full-duplex), 1000 Mbps(1000 Mbps)
Input flow control is unsupported, output flow control is off
MAC address 0026.0b31.0c59, MTU 1500
IP address 10.0.0.113, subnet mask 255.255.0.0
580757 packets input, 86470156 bytes, 0 no buffer
Received 3713 broadcasts, 0 runts, 0 giants
2881 input errors, 0 CRC, 0 frame, 2881 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
905828 packets output, 1131702216 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops, 0 tx hangs
input queue (blocks free curr/low): hardware (255/230)
output queue (blocks free curr/low): hardware (255/202)
```

Im obigen Beispiel wurden auf der Schnittstelle 2881 Überläufe beobachtet, seit die ASA gestartet wurde oder seit die **Clear Interface** (**Klarschnittstelle** des Befehls) eingegeben wurde, um die Zähler manuell zu löschen.

Ursachen für Schnittstellenüberläufe

Schnittstellenüberlauffehler werden in der Regel durch eine Kombination der folgenden Faktoren verursacht:

- Softwareebene - Die ASA-Software löst die Pakete nicht schnell genug aus der FIFO-Warteschlange der Schnittstelle. Dadurch wird die FIFO-Warteschlange gefüllt und neue Pakete werden verworfen.
- Hardware-Ebene - Die Geschwindigkeit, mit der Pakete an die Schnittstelle gesendet werden, ist zu schnell. Das führt dazu, dass die FIFO-Warteschlange gefüllt wird, bevor die ASA-Software die Pakete entfernen kann. In der Regel führt ein plötzliches Anhäufen von Paketen dazu, dass die FIFO-Warteschlange innerhalb kurzer Zeit die maximale Kapazität erreicht.

Schritte zur Fehlerbehebung bei der Ursache von Schnittstellenüberläufen

Zur Behebung dieses Problems gehen Sie wie folgt vor:

1. Stellen Sie fest, ob die ASA CPU-Hogs auftritt und ob diese zum Problem beitragen. Arbeiten, um lange oder häufige CPU-Engpässe zu beseitigen.
2. Informieren Sie sich über die Übertragungsraten der Schnittstellen, und ermitteln Sie, ob die

ASA aufgrund des Datenverkehrsprofils überbelegt ist.
3. Stellen Sie fest, ob das Problem durch zeitweilige Datenverkehrsspitzen verursacht wird. Wenn ja, implementieren Sie die Flusskontrolle auf der ASA-Schnittstelle und den angrenzenden Switch-Ports.

Mögliche Ursachen und Lösungen

CPU auf der ASA ist regelmäßig zu beschäftigt, um eingehende Pakete (CPU-Hogs) zu verarbeiten

Die ASA-Plattform verarbeitet alle Pakete in der Software und verwendet die wichtigsten CPU-Kerne, die alle Systemfunktionen (z. B. Syslogs, Adaptive Security Device Manager-Konnektivität und Application Inspection) verarbeiten, um eingehende Pakete zu verarbeiten. Wenn ein Softwareprozess die CPU länger als vorgesehen hält, zeichnet die ASA dies als CPU-Hog-Ereignis auf, seit der Prozess die CPU "geheftet" hat. Der CPU-Hog-Grenzwert wird in Millisekunden festgelegt und ist für jedes Hardware-Appliance-Modell unterschiedlich. Der Schwellenwert hängt davon ab, wie lange es dauern kann, die FIFO-Warteschlange für die Schnittstelle zu füllen, da die CPU-Leistung der Hardwareplattform und die potenziellen Datenverkehrsraten vom Gerät verarbeitet werden können.

CPU-Hogs führen manchmal zu Schnittstellenüberlauffehlern auf Single-Core-ASAs, z. B. 5505, 5510, 5520, 5540 und 5550. Die langen Hogs, die 100 Millisekunden oder länger dauern, können besonders bei relativ niedrigen Verkehrsaufkommen und bei nicht-bursts zu Überläufen führen. Das Problem betrifft nicht so sehr Multicore-Systeme, da andere Kerne Pakete von einem Rx-Ring abziehen können, wenn einer der CPU-Kerne durch einen Prozess gehostet wird.

Ein Hog, der mehr als den Gerätegrenzwert überschreitet, verursacht, dass ein Syslog mit der ID 711004 generiert wird, wie hier gezeigt:

```
06.02.2013 14:40:42: %ASA-4-711004: Die Aufgabe wurde für 60 ms ausgeführt, Prozess = ssh, PC =
90b0155, Anrufstapel = 06. Februar 2013 14:40:42: %ASA-4-711004: Die Aufgabe wurde für 60 ms
ausgeführt, Prozess = ssh, PC = 90b0155, Anrufstapel = 0x090b0155 0x090bf3b6 0x090b3b84
0x090b3f6e 0x090b0b0009000011110000011000009010000010000100011111111110000001000000000000004459
0x090b44d6 0x08c46fcc 0x09860ca0 0x080fad6d 0x080efa5a 0x080f0a1c 0x08069 22 C
```

CPU-Hog-Ereignisse werden ebenfalls vom System aufgezeichnet. In der Ausgabe des Befehls **show proc cpu-hog** werden folgende Felder angezeigt:

- Prozess: Der Name des Prozesses, der die CPU gehostet hat.
- PROC_PC_TOTAL: Die Gesamtzahl der Zeiten, in denen die CPU durch diesen Prozess gehostet wurde.
- MAXHOG: Die längste für diesen Prozess beobachtete CPU-Hog-Zeit in Millisekunden.
- LASTHOG - Die Zeit, die der letzte Hog die CPU hielt, in Millisekunden.
- LASTHOG At (LASTHOG An): Die Uhrzeit, zu der das CPU-Hog zuletzt auftrat.
- PC: Der Programmindikatorwert des Prozesses, wenn das CPU-Hog auftrat. (Informationen für das Cisco Technical Assistance Center (TAC))
- Call Stack (Anrufliste): Die Aufrufliste des Prozesses, wenn das CPU-Hog auftrat. (Informationen für das Cisco TAC)

Dieses Beispiel zeigt die Befehlsausgabe **show proc cpu-hog**:

```
ASA#

show proc cpu-hog



Process:    ssh, PROC_PC_TOTAL: 1, MAXHOG: 119, LASTHOG: 119
LASTHOG At: 12:25:33 EST Jun 6 2012
PC:         0x08e7b225 (suspend)

Process:    ssh, NUMHOG: 1, MAXHOG: 119, LASTHOG: 119
LASTHOG At: 12:25:33 EST Jun 6 2012
PC:         0x08e7b225 (suspend)
Call stack: 0x08e7b225 0x08e8a106 0x08e7ebf4 0x08e7efde 0x08e7f4c9 0x08e7f546 0x08a7789c
            0x095a3f60 0x080e7e3d 0x080dcfa2 0x080ddf5c 0x0806897c

CPU hog threshold (msec): 10.240
Last cleared: 12:25:28 EST Jun 6 2012
ASA#
```

Der ASA SSH-Prozess hielt die CPU am 6. Juni 2012 um 12:25:33 EST für 119 ms.

Wenn die Anzahl der Überlauffehler an einer Schnittstelle ständig zunimmt, überprüfen Sie die Ausgabe des Befehls **show proc cpu-hog**, um festzustellen, ob CPU-Hog-Ereignisse mit einer Erhöhung des Schnittstellenüberlaufzählers korrelieren. Wenn Sie feststellen, dass die CPU-Hogs zur Schnittstellenüberschreitung beitragen, ist es am besten, nach Fehlern im Bug Toolkit zu suchen oder beim Cisco TAC ein Ticket zu erstellen. Die Ausgabe des Befehls **show tech-support** beinhaltet auch die Befehlsausgabe **show proc cpu-hog**.

Das Datenverkehrsprofil wird regelmäßig über die ASA verarbeitet.

Je nach Datenverkehrsprofil kann der Datenverkehr, der über die ASA fließt, zu groß sein, um ihn zu bewältigen, und es können Überläufe auftreten.

Das Datenverkehrsprofil besteht (unter anderem) aus:

- Paketgröße
- Inter-Packet-Gap (Paketrate)
- Protokoll: Einige Pakete werden auf ASA-Geräten einer Anwendungsüberprüfung unterzogen und erfordern mehr Verarbeitung als andere Pakete.

Diese ASA-Funktionen können zur Identifizierung des Datenverkehrsprofils auf der ASA verwendet werden:

- NetFlow - Die ASA kann so konfiguriert werden, dass NetFlow 9-Datensätze in einen NetFlow Collector exportiert werden. Diese Daten können dann analysiert werden, um mehr über das Datenverkehrsprofil zu erfahren.

- SNMP - SNMP-Überwachung verwenden, um die Datenverkehrsraten der ASA-Schnittstelle, die CPU, die Verbindungsraten und die Übersetzungsraten zu verfolgen. Anschließend können die Informationen analysiert werden, um das Datenverkehrsmuster und dessen Änderungen im Laufe der Zeit zu ermitteln. Versuchen Sie festzustellen, ob die Verkehrsraten in die Höhe schnellen, was mit einem Anstieg der Überläufe und der Ursache für diesen Verkehrsspitzen zusammenhängt. Im TAC gibt es Fälle, in denen Geräte im Netzwerk sich falsch verhalten (aufgrund von Fehlkonfigurationen oder Virusinfektionen) und regelmäßig eine Flut von Datenverkehr erzeugen.

Zwischengeschaltete Paket-Bursts überzeichnen die FIFO-Warteschlange für die

ASA-Schnittstelle

Ein Ausbruch von Paketen, die auf der Netzwerkkarte eintreffen, kann dazu führen, dass die FIFO gefüllt wird, bevor die CPU die Pakete davon abziehen kann. In der Regel kann nicht viel getan werden, um dieses Problem zu beheben, aber es kann durch die Verwendung von QoS im Netzwerk abgefedert werden, um die Datenverkehrsspitzen auszugleichen, oder die Flusskontrolle auf der ASA und den benachbarten Switch-Ports.

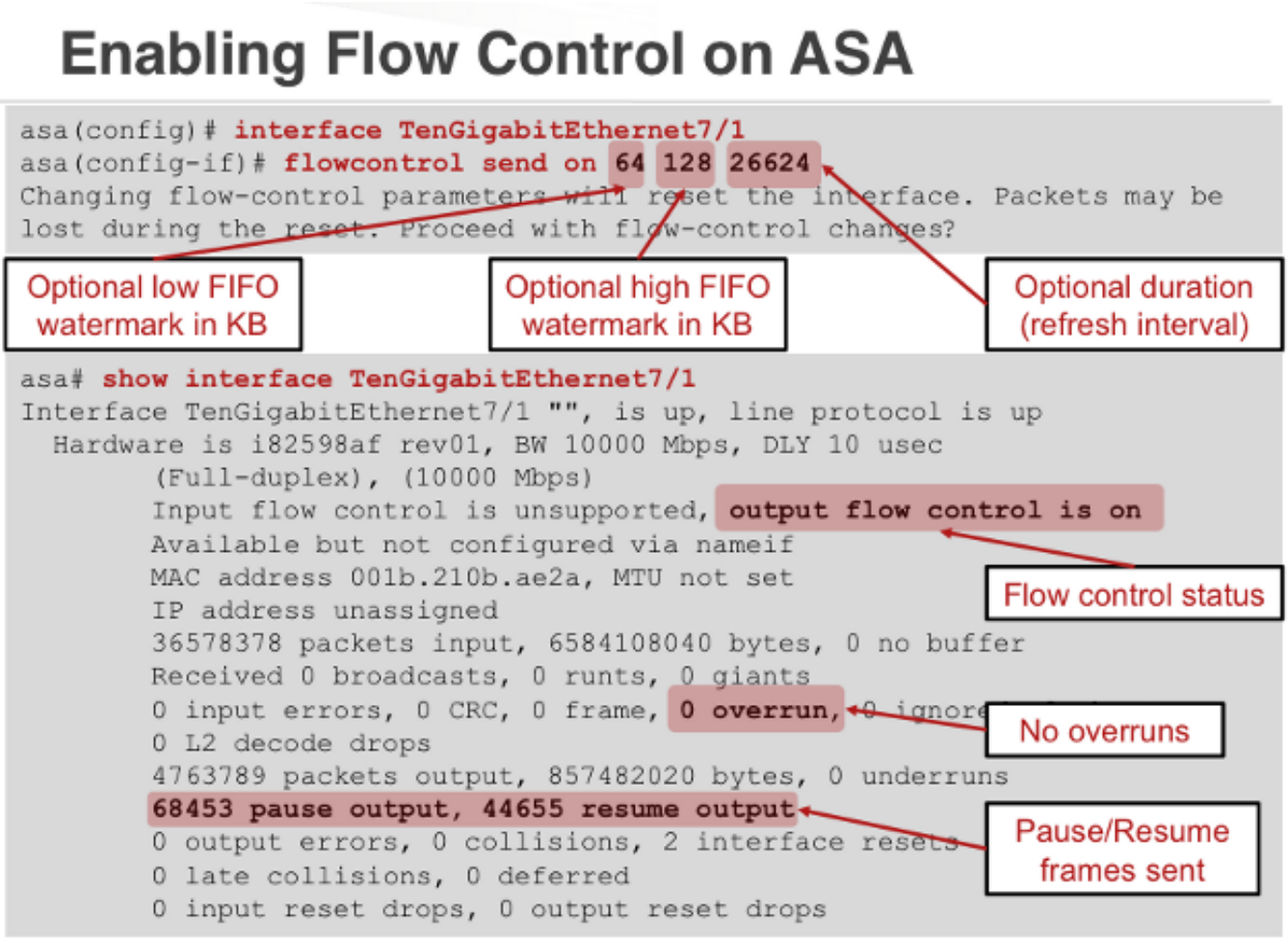
Bei der Flusskontrolle handelt es sich um eine Funktion, mit der die ASA-Schnittstelle eine Nachricht an das benachbarte Gerät (z. B. einen Switch-Port) senden kann, um es anzuweisen, den Datenverkehr für einen kurzen Zeitraum abzubrechen. Dies geschieht, wenn der FIFO eine bestimmte Wassermarke erreicht. Sobald der FIFO-Bereich wieder freigegeben wurde, sendet die ASA-NIC einen Frame für die Wiederaufnahme, und der Switch-Port sendet weiterhin Datenverkehr. Dieser Ansatz funktioniert gut, da die benachbarten Switch-Ports in der Regel über mehr Pufferkapazität verfügen und beim Senden bessere Pufferung für Job-Puffer-Pakete durchführen können als die ASA in Empfangsrichtung.

Sie können versuchen, auf der ASA Captures zu aktivieren, um die Microbursts im Datenverkehr zu erkennen. Dies ist jedoch in der Regel nicht hilfreich, da die Pakete verworfen werden, bevor sie von der ASA verarbeitet und der Erfassung im Speicher hinzugefügt werden können. Ein externer Sniffer kann zum Erfassen und Identifizieren von Datenverkehrsspitzen verwendet werden, aber manchmal kann auch der externe Sniffer vom Burst überwältigt werden.

Aktivieren der Flusssteuerung zur Minimierung von Schnittstellenüberläufen

Die Flow Control-Funktion wurde der ASA in Version 8.2(2) und höher für 10GE-Schnittstellen und Version 8.2(5) und höher für 1GE-Schnittstellen hinzugefügt. Die Möglichkeit zur Flusskontrolle an ASA-Schnittstellen, bei denen es zu Überläufen kommt, erweist sich als effektive Methode zur Vermeidung von Paketverlusten.

Weitere Informationen finden Sie in der Flusskontrollfunktion in der Befehlsreferenz zur Cisco Serie ASA 5500, 8.2.



(Diagramm der Cisco Live-Präsentation von Andrew Ossipov, BRKSEC-3021)

Beachten Sie, dass die "Output Flow Control ist ein" bedeutet, dass die ASA Flow Control Pause-Frames über die ASA-Schnittstelle an das benachbarte Gerät (den Switch) sendet. "Eingangsflusssteuerung wird nicht unterstützt" bedeutet, dass die ASA den *Empfang* von Flusssteuerungs-Frames vom benachbarten Gerät nicht unterstützt.

Beispielkonfiguration für Flusskontrolle:

```
interface GigabitEthernet0/2

flowcontrol send on

 nameif DMZ interface
 security-level 50
 ip address 10.1.3.2 255.255.255.0
!
```

Zugehörige Informationen

- ASA 8.3 und höher: Überwachen und Beheben von Leistungsproblemen
- Cisco Live-Präsentation "Maximale Firewall-Leistung" - Diese Präsentation skizziert die Architektur der verschiedenen ASA-Plattformen und enthält Informationen zur Leistung und zum Tuning. Melden Sie sich an, um Zugriff auf diese Präsentation zu erhalten unter Cisco

Live!365 und suchen Sie nach der Präsentationsnummer BRKSEC-3021.

- Cisco TAC Security Podcast, Folge Nr. 7 "Überwachung der Firewall-Leistung" - In dieser Podcast-Episode werden Techniken und Methoden zur Überwachung der Firewall-Leistung und zur Identifizierung von Leistungsproblemen vorgestellt.
- Technischer Support und Dokumentation - Cisco Systems