ASA-interface voor oplossing van problemen - fouten tegen tellers

Inhoud

Inleiding

Dit document beschrijft de "overschrijding"-foutmelding en hoe u prestatiekwesties of pakketverlies op het netwerk kunt onderzoeken. Een beheerder kan fouten opmerken die zijn gemeld in de opdrachtoutput van de **show** interface op de adaptieve security applicatie (ASA).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Probleem

De ASA interface error teller "overrun" volgt het aantal keren dat een pakket op de netwerkinterface is ontvangen, maar er was geen beschikbare ruimte in de interface-FIFO-wachtrij

om het pakket op te slaan. Dus werd het pakje ingetrokken. De waarde van deze teller kan met de opdracht **showinterface** worden gezien.

Bijvoorbeeld uitvoer die het probleem toont:

```
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)
```

In het bovenstaande voorbeeld werden 2881 overschrijdingen op de interface waargenomen sinds de ASA opstart of sinds de opdracht **duidelijke interface** werd ingevoerd om de tellers handmatig te wissen.

Oorzaken van interfaceoverschrijdingen

De overschrijdingsfouten van de interface worden gewoonlijk veroorzaakt door een combinatie van deze factoren:

- Software niveau - De ASA-software trekt de pakketten niet snel genoeg van de interface-FIFO-wachtrij. Hierdoor wordt de FIFO-wachtrij ingevuld en worden nieuwe pakketten verzonden.
- hardwareniveau - de snelheid waarmee pakketten in de interface komen is te snel, waardoor de FIFO-wachtrij moet worden ingevuld voordat de ASA-software de pakketten kan uitschakelen. Meestal zorgt een uitbarsting van pakketten ervoor dat de FIFO-wachtrij in een korte tijd de maximale capaciteit vult.

Stappen om problemen op te lossen voor het oplossen van interfaceoverschrijdingen

De stappen om problemen op te lossen en dit probleem aan te pakken zijn:

1. Bepaal of de ASA CPU's ervaart en of zij aan het probleem bijdragen. Werk om lange of frequente CPU-slangen te beperken.
2. Begrijp de tarieven van het interfaceverkeer en controleer of de ASA door het verkeersprofiel wordt oversubscript.
3. Bepaal of het probleem veroorzaakt wordt door tussenpozen van het verkeer. Indien dat het

geval is, zorg dan voor stroomcontrole op de ASA-interface en de aangrenzende switchpoorten.

Potentiële oorzaken en oplossingen

CPU's in de ASA zijn periodiek te druk om inkomende pakketten (CPU's) te verwerken

Het ASA-platform verwerkt alle pakketten in de software en gebruikt de belangrijkste CPU-cores die alle systeemfuncties verwerken (zoals syslogs, Adaptieve Security Apparatuur Manager connectiviteit en Application Inspection) om inkomende pakketten te verwerken. Als een softwareproces de CPU langer vasthoudt dan zou moeten, neemt de ASA dit op als een CPU-hoggebeurtenis sinds het proces "opgestapeld" op de CPU. De CPU-drempel wordt ingesteld in milliseconden en is verschillend voor elk model van het hardwareapparaat. De drempel is gebaseerd op hoe lang het kan duren om de interface-FIFO-wachtrij te vullen gezien de CPU-voeding van het hardwareplatform en de potentiële verkeerssnelheden die het apparaat kan verwerken.

CPU's veroorzaken soms fouten die de interface overschrijden bij ASA's met één kern, zoals de telefoons 5505, 5510, 5520, 5540 en 5550. De lange slangen, die 100 milliseconden of meer duren, kunnen vooral leiden tot overschrijdingen bij relatief lage verkeersniveaus en niet-opgebrande verkeerssnelheden. Het probleem heeft niet zo veel invloed op multi-core systemen, omdat andere kernen pakketten van een Rx-ring kunnen verwijderen als een van de CPU-kernen door een proces wordt opgehangen.

Een slang die langer is dan de drempel van het hulpmiddel veroorzaakt een syslog die wordt gegenereerd met id 711004, zoals hier wordt getoond:

```
6 feb. 2013 14:40:42: %ASA-4-7104: Test uitgevoerd voor 60 msec, proces = ssh, PC = 90b0155,
Call stack = Feb 06 2013 14:40:42: %ASA-4-7104: Test uitgevoerd voor 60 msec, proces = ssh, PC =
90b0155, Call stack = 0x090b0155 0x090bf3b6 0x090b3b84 0x090b3f6e 0x090b 4459 0x090b44d6
0x08c46fcc 0x09860ca 00x080fad6d 0x080efa5a 0x080f0a1c 0x08069 22 quater
```

CPU-hostgebeurtenissen worden ook door het systeem geregistreerd. De uitvoer van het **showproces cpu-hog** opdracht toont deze velden:

- Verwerking - de naam van het proces dat de CPU heeft gehost.
- PROC_PC_TOTAL - het totale aantal keren dat dit proces op de CPU heeft gericht.
- MAXHOG - de langste CPU-gijtijd die voor dat proces in milliseconden wordt waargenomen.
- LASTHOG - de hoeveelheid tijd die de vorige centrale verwerkingseenheid in milliseconden had.
- LASTHOG BIJ - op het moment dat de CPU-ingang voor het laatst is gebruikt.
- PC - de tegenwaarde van het proces van het programma toen de CPU-ingang was. (Informatie voor het Cisco Technical Assistance Center (TAC)
- Call Stack - de Call Stack van het proces wanneer de CPU-ingang is. (Informatie voor Cisco TAC)

Dit voorbeeld toont de opdrachtoutput **van het** showproces 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#
```

Het ASA SSH-proces hield de CPU voor 119 ms op 12:25:33 EST 6 juni 2012.

Als overloopfouten op een interface voortdurend toenemen, controleert u de uitvoer van de opdracht **tonen** cpu-**hog** om te zien of de CPU-hoggebeurtenissen correleren met een toename in de interface-overloopteller. Als u vindt dat de CPU-slangen bijdragen aan de fouten bij interfaceoverschrijdingen, is het best om op fouten te zoeken in de bellenwerkset, of om een case te openen met Cisco TAC. De output van de **show tech-support** opdracht omvat ook de **show** proc **cpu-hog** opdrachtoutput.

Verkeersprofiel periodiek wordt overschreden de ASA

Afhankelijk van het verkeersprofiel, zou het verkeer dat door de ASA stroomt te veel kunnen zijn voor het om te gaan en overschrijdingen kunnen voorkomen.

Het verkeersprofiel bestaat onder meer uit:

- Packetsize
- Inter-Packet gap (pakketsnelheid)
- Protocol - sommige pakketten worden op de ASA-website gecontroleerd en vereisen meer verwerking dan andere pakketten

Deze ASA-functies kunnen worden gebruikt om het verkeersprofiel van de ASA te identificeren:

- NetFlow - de ASA kan worden geconfigureerd om NetFlow versie 9 records te exporteren naar een NetFlow Collector. Deze gegevens kunnen vervolgens worden geanalyseerd om meer over het verkeersprofiel te begrijpen.

- SNMP - gebruik SNMP-bewaking om de ASA interface-verkeerssnelheden, CPU's, verbindingssnelheden en vertaalsnelheden te volgen. De informatie kan dan worden geanalyseerd om het verkeerspatroon te begrijpen en hoe het in de loop der tijd verandert. Probeer vast te stellen of er een stijging in verkeerstarieven is die correleert met een stijging in de overschrijdingen, en de oorzaak van die pieken. Er zijn gevallen in de TAC geweest waarin de apparaten op het netwerk zich niet goed gedragen (door verkeerde configuratie of virusinfectie) en regelmatig een stroom verkeer genereren.

Intermitterende pakketkosten voor overabonnement op de ASA-interface-FIFO-wachtrij

Een uitbarsting van pakketten die op de NIC aankomen zou kunnen veroorzaken dat de FIFO

wordt ingevuld voordat de CPU de pakketten van deze computer kan weghalen. Er is meestal niet veel wat er kan worden gedaan om dit probleem op te lossen, maar het kan worden verzacht door het gebruik van QoS in het netwerk om de verkeersopstoppingen te verzachten, of door de controle van de stroom op de ASA en de aangrenzende knooppunten.

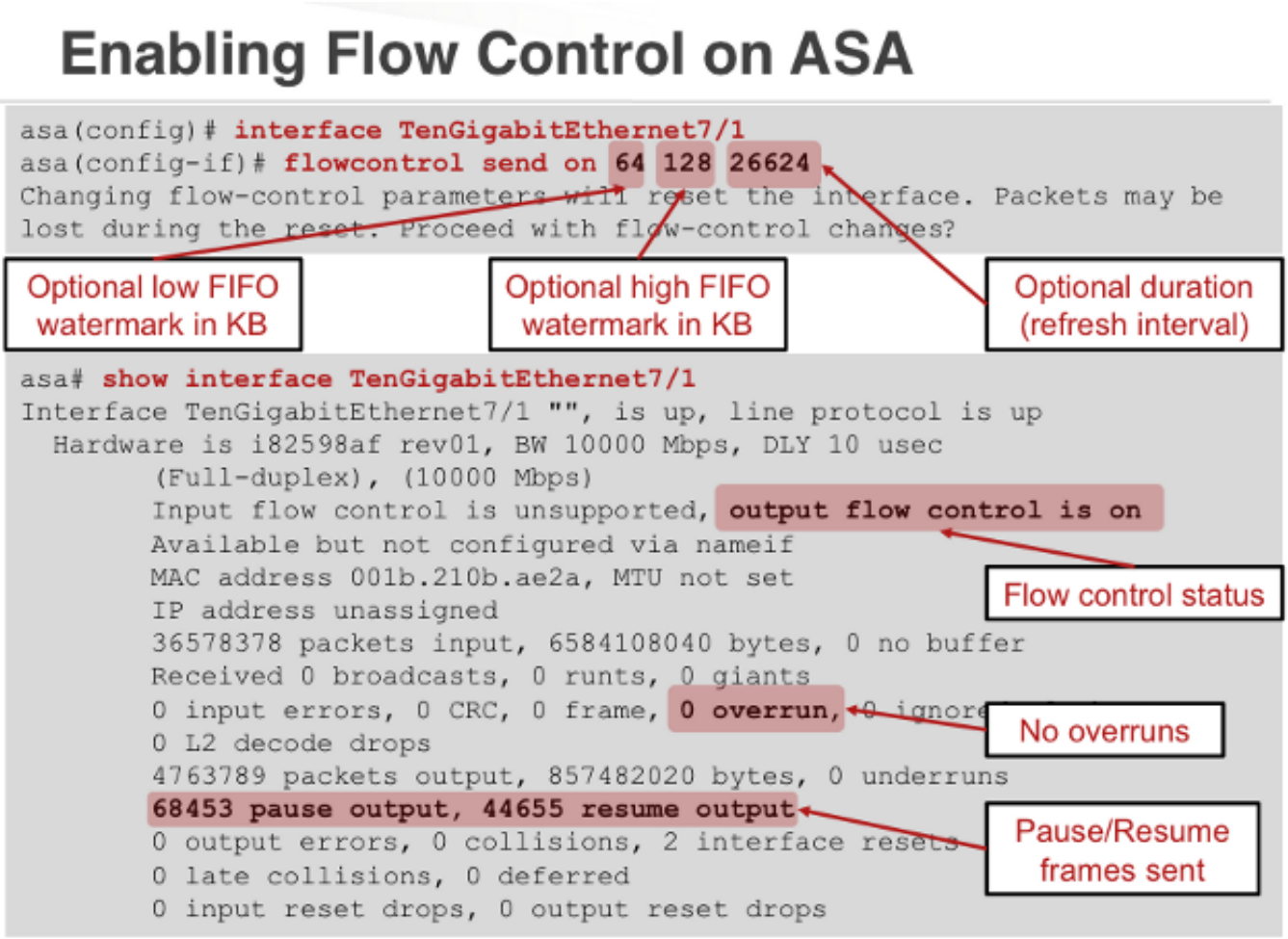
Flow control is een functie die de interface van de ASA toestaat om een bericht naar het aangrenzende apparaat (een switchpoort bijvoorbeeld) te verzenden om het te leren om te stoppen met het verzenden van verkeer voor een korte tijd. Dit gebeurt wanneer de FIFO een bepaald hoogwatermerk bereikt. Zodra de FIFO een bepaald bedrag is vrijgelaten, stuurt de ASA NIC een hervatte frame en blijft de schakelpoort het verkeer versturen. Deze benadering werkt goed omdat de aangrenzende knooppunten meestal meer bufferruimte hebben en een betere job buffering pakketten kunnen doen op verzenden dan de ASA in de ontvangstrichting doet.

U kunt proberen om opnames op de ASA in te schakelen om de micro-bursten van het verkeer te detecteren, maar gewoonlijk is dit niet handig omdat de pakketten worden verzonden voordat ze door de ASA kunnen worden verwerkt en toegevoegd aan de opname in het geheugen. Een externe sluipschutter kan worden gebruikt om de verkeersuitbarsting vast te leggen en te identificeren, maar soms kan de externe sluipschutter ook overweldigd worden door de burst.

Flow Control inschakelen om interfaceoverschrijdingen te verminderen

De functie voor stroomregeling werd aan de ASA toegevoegd in versie 8.2(2) en later voor 10 GE interfaces, en versie 8.2(5) en later voor 1 GE interfaces. Het vermogen om flow control op ASA interfaces mogelijk te maken die overschrijdingen ervaren blijkt een effectieve techniek te zijn om pakketdalingen te voorkomen.

Raadpleeg de stroomregeloptie in de Cisco ASA 5500 Series Opdrachtreferentie, 8.2 voor meer informatie.



(Diagram van de Cisco Live Presentatie BRKSEC-3021 van Andrew Ossipov)

Merk op dat "output flow control is on" betekent dat de ASA flow control pauze frames uit de ASA interface naar het aangrenzende apparaat (de schakelaar) verstuurt. "Invoerstroomregeling wordt niet ondersteund" betekent dat de ASA de *ontvangst* van stroomregelkaders van het aangrenzende apparaat niet ondersteunt.

Configuratie van stroomregelaar:

```
interface GigabitEthernet0/2

flowcontrol send on

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

Gerelateerde informatie

- [ASA 8.3 en later: Prestatieproblemen bij bewaking en probleemoplossing]
- [Cisco Live-presentatie "maximalisatie van de firewallprestaties"] - Deze presentatie schetst de architectuur van de verschillende ASA-platforms en bevat informatie over prestaties en afstemming. Voor toegang tot deze presentatie, log in to [Cisco live!365] en op zoek naar het

presentatienummer BRKSEC-3021.

- Cisco TAC Security Podcast Episode #7 "Monitoring Firewall Performance" - Deze podcast aflevering biedt een discussie over technieken en methoden om firewallprestaties te controleren en prestatieproblemen te identificeren.
- Technische ondersteuning en documentatie – Cisco Systems