Solución de Problemas de Errores de Contador de Sobrecarga de Interfaz ASA

Contenido

Introducción

Este documento describe el contador de errores "desbordamiento" y cómo investigar problemas de rendimiento o de pérdida de paquetes en la red. Un administrador puede detectar errores notificados en el resultado del comando **show interface** en el Adaptive Security Appliance (ASA).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problema

El contador de errores de la interfaz ASA "desbordamiento" hace un seguimiento del número de

veces que se recibió un paquete en la interfaz de red, pero no había espacio disponible en la cola FIFO de la interfaz para almacenar el paquete. Por lo tanto, el paquete se descartó. El valor de este contador se puede ver con el comando **show interface**.

Ejemplo de salida que muestra el problema:

```
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)
```

En el ejemplo anterior, se observaron 2881 desbordamientos en la interfaz desde que el ASA arrancó o desde que el comando **clear interface** se ingresó para borrar los contadores manualmente.

Causas de desbordamientos de interfaz

Los errores de desbordamiento de la interfaz generalmente son causados por una combinación de estos factores:

- Nivel de software: el software ASA no retira los paquetes de la cola FIFO de la interfaz lo suficientemente rápido. Esto hace que la cola FIFO se llene y que se descarten los paquetes nuevos.
- Nivel de hardware: la velocidad a la que los paquetes entran en la interfaz es demasiado rápida, lo que hace que la cola FIFO se llene antes de que el software ASA pueda extraer los paquetes. Por lo general, una ráfaga de paquetes hace que la cola FIFO llene hasta la capacidad máxima en un corto período de tiempo.

Pasos para Resolver la Causa de las Sobrecargas de Interfaz

Los pasos para solucionar y solucionar este problema son:

1. Determine si el ASA experimenta un aumento de la CPU y si contribuye al problema. Trabaje para mitigar cualquier acumulación de CPU larga o frecuente.
2. Comprenda las velocidades de tráfico de la interfaz y determine si el ASA está sobresuscrito debido al perfil de tráfico.
3. Determine si las ráfagas de tráfico intermitentes causan el problema. Si es así, implemente el control de flujo en la interfaz ASA y los puertos de switch adyacentes.

Causas y soluciones potenciales

La CPU en el ASA está periódicamente demasiado ocupada para procesar los paquetes entrantes (intervalos de CPU)

La plataforma ASA procesa todos los paquetes en el software y utiliza los núcleos de CPU principales que manejan todas las funciones del sistema (como syslogs, conectividad Adaptive Security Device Manager e Inspección de aplicaciones) para procesar los paquetes entrantes. Si un proceso de software retiene la CPU durante más tiempo del que debería, el ASA registra esto como un evento de bloqueo de la CPU desde que el proceso "acaparó" la CPU. El umbral de bloqueo de CPU se establece en milisegundos y es diferente para cada modelo de dispositivo de hardware. El umbral se basa en el tiempo que podría tomar llenar la cola FIFO de la interfaz dada la potencia de la CPU de la plataforma de hardware y las tasas de tráfico potenciales que el dispositivo puede manejar.

Las fallas de la CPU a veces causan errores de desbordamiento de la interfaz en los ASA de un solo núcleo, como los 5505, 5510, 5520, 5540 y 5550. Los cerdos largos, que duran 100 milisegundos o más, pueden hacer que se produzcan desbordamientos para niveles de tráfico relativamente bajos y tasas de tráfico sin ráfagas. El problema no afecta tanto a los sistemas de varios núcleos, ya que otros núcleos pueden retirar paquetes de un anillo Rx si uno de los núcleos de CPU se acapara por un proceso.

Un atasco que dura más del umbral del dispositivo hace que se genere un syslog con el id 711004, como se muestra aquí:

```
6 de febrero de 2013 14:40:42: %ASA-4-711004: La tarea se ejecutó durante 60 ms, Proceso = ssh,
PC = 90b0155, Pila de llamadas = 6 de febrero de 2013 14:40:42: %ASA-4-711004: La tarea se
ejecutó durante 60 ms, Proceso = ssh, PC = 90b0155, Pila de llamadas = 0x090b0150x090bf3b6
0x090b3b84 0x090b3f6e 0x090b 4459 0x090b44d6 0x08c46fcc 0x09860ca0 0x080fad6d 0x080efa5a
0x080f0a1c 0x080692 2 quáter
```

El sistema también registra los eventos de bloqueo de CPU. La salida del comando **show proc cpu-hog** muestra estos campos:

- Proceso: el nombre del proceso que acaparó la CPU.
- PROC_PC_TOTAL - el número total de veces que este proceso acaparó la CPU.
- MAXHOG: el tiempo de conexión de CPU más largo observado para ese proceso, en milisegundos.
- LASTHOG - La cantidad de tiempo que el último bloqueo mantuvo la CPU, en milisegundos.
- LASTHOG At: el momento en que ocurrió el bloqueo de la CPU por última vez.
- PC: valor del contador del programa del proceso cuando se produjo el atasco de la CPU. (Información para el Cisco Technical Assistance Center (TAC))
- Pila de llamadas: la pila de llamadas del proceso cuando se produjo el bloqueo de la CPU. (Información para el TAC de Cisco)

Este ejemplo muestra la salida del comando **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#
```

El proceso ASA SSH mantuvo la CPU durante 119 ms el 6 de junio de 2012 a las 12:25:33 EST.

Si los errores de desbordamiento aumentan continuamente en una interfaz, verifique el resultado del comando **show proc cpu-hog** para ver si los eventos de agrupamiento de CPU se correlacionan con un aumento en el contador de desbordamiento de la interfaz. Si encuentra que los cerdos de la CPU contribuyen a que la interfaz sobrecargue errores, es mejor buscar errores con el Bug Toolkit, o plantear un caso con el Cisco TAC. El resultado del comando **show tech-support** también incluye el resultado del comando **show proc cpu-hog**.

El perfil de tráfico procesado se sobresuscribe periódicamente al ASA

En función del perfil de tráfico, el tráfico que fluye a través del ASA podría ser demasiado para que se maneje y podrían producirse desbordamientos.

El perfil de tráfico consta de (entre otros aspectos):

- Tamaño del paquete
- Brecha entre paquetes (velocidad de paquetes)
- Protocolo: algunos paquetes se someten a inspección de aplicaciones en ASA y requieren más procesamiento que otros paquetes

Estas funciones de ASA se pueden utilizar para identificar el perfil de tráfico en el ASA:

- Netflow - el ASA se puede configurar para exportar registros de la versión 9 de NetFlow a un recolector de NetFlow. Estos datos se pueden analizar para comprender mejor el perfil de tráfico.

- SNMP (Protocolo de administración de red simple) - utilice el monitoreo SNMP para realizar el seguimiento de las tasas de tráfico de la interfaz ASA, la CPU, las velocidades de conexión y las tasas de traducción. La información se puede analizar entonces para comprender el patrón de tráfico y cómo cambia con el tiempo. Intente determinar si hay un pico en las velocidades de tráfico que se correlaciona con un aumento en los desbordamientos y la causa de ese pico de tráfico. Ha habido casos en el TAC en los que los dispositivos de la red se comportan de forma incorrecta (debido a una configuración incorrecta o a una infección por virus) y generan una inundación de tráfico periódicamente.

Las ráfagas de paquetes intermitentes sobresuscriben la cola FIFO de la interfaz ASA

Una ráfaga de paquetes que llegan a la NIC podría hacer que la FIFO se llene antes de que la CPU pueda retirar los paquetes de ella. Por lo general, no se puede hacer mucho para resolver este problema, pero se puede mitigar mediante el uso de QoS en la red para suavizar las ráfagas

de tráfico o el control de flujo en el ASA y los puertos de switch adyacentes.

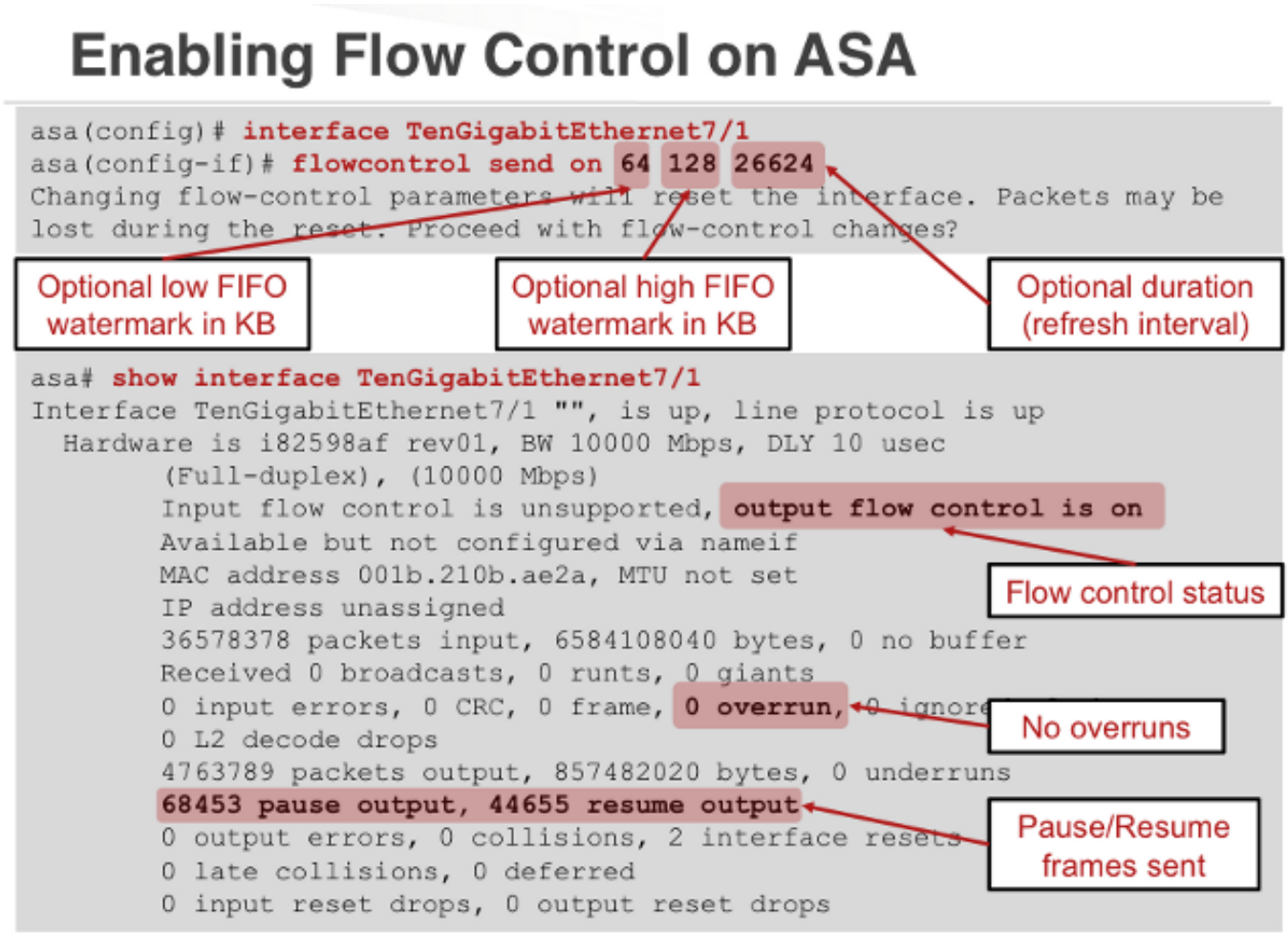
El control de flujo es una función que permite a la interfaz de ASA enviar un mensaje al dispositivo adyacente (por ejemplo, un switchport) para indicarle que deje de enviar tráfico durante un breve período de tiempo. Lo hace cuando la FIFO alcanza una cierta marca de agua alta. Una vez que se ha liberado cierta cantidad de FIFO, el ASA NIC envía una trama de reanudación y el switchport continúa enviando tráfico. Este enfoque funciona bien porque los puertos de switch adyacentes normalmente tienen más espacio de búfer y pueden hacer un mejor trabajo de almacenamiento en búfer de paquetes en la transmisión que el ASA en la dirección de recepción.

Puede intentar habilitar capturas en el ASA para detectar microrráfagas de tráfico, pero normalmente esto no es útil, ya que los paquetes se descartan antes de que el ASA los pueda procesar y agregar a la captura en la memoria. Un sniffer externo se puede utilizar para capturar e identificar la ráfaga de tráfico, pero a veces el sniffer externo también puede ser abrumado por la ráfaga.

Habilitar el control de flujo para mitigar los desbordamientos de interfaz

La función de control de flujo se agregó al ASA en la versión 8.2(2) y posteriores para las interfaces 10GE, y en la versión 8.2(5) y posteriores para las interfaces 1GE. La capacidad de habilitar el control de flujo en las interfaces ASA que experimentan desbordamientos demuestra ser una técnica eficaz para evitar que se produzcan caídas de paquetes.

Refiérase a la [función de control de flujo en la Referencia de Comandos de Cisco ASA 5500 Series, 8.2] para obtener más información.



(Diagrama de la presentación en directo de Andrew Ossipov BRKSEC-3021)

Tenga en cuenta que "control de flujo de salida está activado" significa que el ASA envía tramas de pausa de control de flujo a la interfaz ASA hacia el dispositivo adyacente (el switch). "El control de flujo de entrada no es compatible" significa que el ASA no admite la *recepción* de tramas de control de flujo del dispositivo adyacente.

Configuración de Ejemplo de Control de Flujo:

```
interface GigabitEthernet0/2

flowcontrol send on

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

Información Relacionada

- ASA 8.3 y posterior: Supervisión y resolución de problemas de rendimiento
- Presentación de Cisco Live "Maximizing Firewall Performance" - Esta presentación describe la arquitectura de las diversas plataformas ASA e incluye información sobre el rendimiento y el ajuste. Para acceder a esta presentación, inicie sesión en ¡Ciscolive!365 y busque el número de presentación BRKSEC-3021.
- Episodio del podcast 7 "Monitoring Firewall Performance" - Este podcast presenta una discusión de técnicas y métodos para monitorear el rendimiento del firewall e identificar problemas de rendimiento.
- Soporte Técnico y Documentación - Cisco Systems