Errores contrarios del overrun de la interfaz del Troubleshooting ASA

Contenido

Introducción

Este documento describe al contador de errores del “overrun” y cómo investigar los problemas de rendimiento o los problemas de la pérdida del paquete en la red. Un administrador pudo notar los errores señalados en el **comando show interface** hecho salir en el dispositivo de seguridad adaptante (ASA).

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Problema

El contador de error de interfaz ASA “sobra” sigue la cantidad de veces que un paquete fue recibido en la interfaz de la red, pero no había espacio disponible en la cola primero en entrar, primero en salir de la interfaz para salvar el paquete. Así, el paquete fue caído. El valor de este contador se puede considerar con el **comando show interface**.

Salida de ejemplo que visualiza 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, 2881 sobrantes fueron observados en la interfaz puesto que el ASA arrancado o puesto que ingresaron al comando clear interface para borrar los contadores manualmente.

Causas de los sobrantes de la interfaz

Los errores del overrun de la interfaz se causan generalmente por una combinación de estos factores:

- Nivel de software - El software ASA no arranca los paquetes de la cola primero en entrar, primero en salir de la interfaz rápidamente bastante. Esto hace la cola primero en entrar, primero en salir llenarse y los nuevos paquetes que se caerán.
- Nivel del hardware - La tarifa en la cual los paquetes entran en la interfaz es demasiado rápida, que hace la cola primero en entrar, primero en salir llenar antes de que el software ASA pueda arrancar los paquetes. Generalmente, una explosión de los paquetes hace la cola primero en entrar, primero en salir llenar hasta la capacidad máxima en una pequeña cantidad de hora.

Los pasos para resolver problemas la causa de la interfaz sobran

Los pasos para resolver problemas y para abordar este problema son:

1. Determine si el ASA experimenta los cerdos CPU y si contribuyen al problema. Trabaje para atenuar cualquier cerdo largo o frecuente CPU.

2. Entienda las relaciones del tráfico de la interfaz y determinelas si el ASA es oversubscribed debido al perfil del tráfico.
3. Determine si las ráfagas de tráfico intermitentes causan el problema. Si es así implemente el control de flujo en la interfaz y los puertos del switch adyacente ASA.

Causas y soluciones del potencial

El CPU en el ASA está periódicamente demasiado ocupado procesar los paquetes entrantes (los cerdos CPU)

La plataforma ASA procesa todos los paquetes en el software y utiliza las memorias de la CPU principal que manejan todas las funciones de sistema (tales como Syslog, Conectividad adaptante del Administrador de dispositivos de seguridad, y Inspección de la aplicación) para procesar los paquetes entrantes. Si un proceso del software celebra el CPU para más de largo que debe, el ASA registra esto como evento de la CPU HOG puesto que el proceso “hogged” el CPU. El umbral de la CPU HOG se fija en los milisegundos, y es diferente para cada modelo del dispositivo de hardware. El umbral se basa en cuánto tiempo podría tomar para llenar la cola primero en entrar, primero en salir de la interfaz dada las energías en la CPU de la plataforma de hardware y el tráfico potencial valora el dispositivo puede dirigir.

La interfaz de la causa de los cerdos CPU sobra a veces los errores en la solo-memoria ASA, tales como los 5505, los 5510, los 5520, los 5540, y los 5550. Los cerdos largos, esos duran por 100 milisegundos o más, pueden hacer especialmente los sobrantes ocurrir para los niveles relativamente con poco tráfico y las relaciones del tráfico NON-bursty. El problema no afecta los sistemas multifilares tanto, puesto que otras memorias pueden arrancar los paquetes de un timbre del rx si una de las memorias CPU hogged por un proceso.

Un cerdo que dura más que el umbral del dispositivo hace un Syslog ser generado con la identificación 711004, como se muestra aquí:

```
6 de febrero de 2013 14:40:42: %ASA-4-711004: La tarea se ejecutó para 60 milisegundos, proceso
= ssh, PC = 90b0155, pila de llamadas = el 6 de febrero de 2013 14:40:42: %ASA-4-711004: La
tarea se ejecutó para 60 milisegundos, proceso = ssh, PC = 90b0155, pila de llamadas =
0x090b0155 0x090bf3b6 0x090b3b84 0x090b3f6e 0x090b4459 0x090b44d6 0x08c46fcc 0x09860ca0
0x080fad6d 0x080efa5a 0x080f0a1c 0x0806922c
```

Los eventos de la CPU HOG también son registrados por el sistema. La salida del comando de la **CPU HOG del proc de la demostración** visualiza estos campos:

- Proceso - el nombre del proceso que hogged el CPU.
- PROC_PC_TOTAL - el número total de épocas que este proceso hogged el CPU.
- MAXHOG - el tiempo más largo de la CPU HOG observado para ese proceso, en los milisegundos.
- LASTHOG - la cantidad de tiempo el cerdo más reciente sostuvo el CPU, en los milisegundos.
- LASTHOG cuando ocurrió el último de la CPU HOG.
- PC - el valor de contador del programa del proceso cuando ocurrió la CPU HOG. (Información para el Centro de Asistencia Técnica de Cisco (TAC))
- Pila de llamadas - la pila de llamadas del proceso cuando ocurrió la CPU HOG. (Información para el TAC de Cisco)

Este ejemplo muestra la salida de comando de la **CPU HOG del proc de la demostración**:

```
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 celebró el CPU para 119ms en 12:25:33 EST de junio el 6 de 2012.

Si los errores del overrun aumentan continuamente en una interfaz, marque la salida del comando de la **CPU HOG del proc de la demostración** para ver si los eventos de la CPU HOG correlacionan con un aumento en el contador del overrun de la interfaz. Si usted encuentra que los cerdos CPU contribuyen a la interfaz sobra los errores, es el mejor buscar para los bug con el Bug Toolkit, o plantee un caso con el TAC de Cisco. La salida del **comando show tech-support** también incluye la salida de comando de la **CPU HOG del proc de la demostración**.

Periódicamente Oversubscribes procesado perfil del tráfico el ASA

El dependiente sobre en el perfil del tráfico, el tráfico que atraviesa el ASA pudo ser demasiado para que dirija y los sobrantes pudo ocurrir.

El perfil del tráfico consiste en (entre otros aspectos):

- Tamaño de paquetes
- Brecha entre paquetes (velocidad de paquetes)
- Protocolo - algunos paquetes se sujetan a la Inspección de la aplicación en el ASA y requieren el proceso que otros paquetes

Estas características ASA se pueden utilizar para identificar el perfil del tráfico en el ASA:

- Netflow - el ASA se puede configurar para exportar los expedientes de la versión 9 del Netflow a un colector NetFlow. Estos datos se pueden entonces analizar para entender más sobre el perfil del tráfico.

- SNMP - utilice la supervisión SNMP para seguir las relaciones del tráfico de la interfaz ASA, CPU, las velocidades de conexión, y las tarifas de la traducción. La información se puede entonces analizar para entender al patrón de tráfico y cómo cambia en un cierto plazo. Intente determinar si hay un punto en las relaciones del tráfico que correlaciona a un aumento en los sobrantes, y la causa de ese pico de tráfico. Ha habido casos en TAC donde los dispositivos en la red se comportan mal (debido al misconfiguration o a la infección del virus) y generan una inundación del tráfico periódicamente.

Ráfagas de paquetes intermitentes Oversubscribe la cola primero en entrar, primero en salir de la interfaz ASA

Una explosión de los paquetes que llegan en el NIC podría hacer el (Primero en Entrar, Primero

en Salir FIFO) llenarse antes de que el CPU pueda arrancar los paquetes de él. No hay generalmente mucho que se puede hacer para solucionar este problema, pero puede ser atenuado por el uso de QoS en la red de allanar las ráfagas de tráfico, o el control de flujo en el ASA y los puertos del switch adyacente.

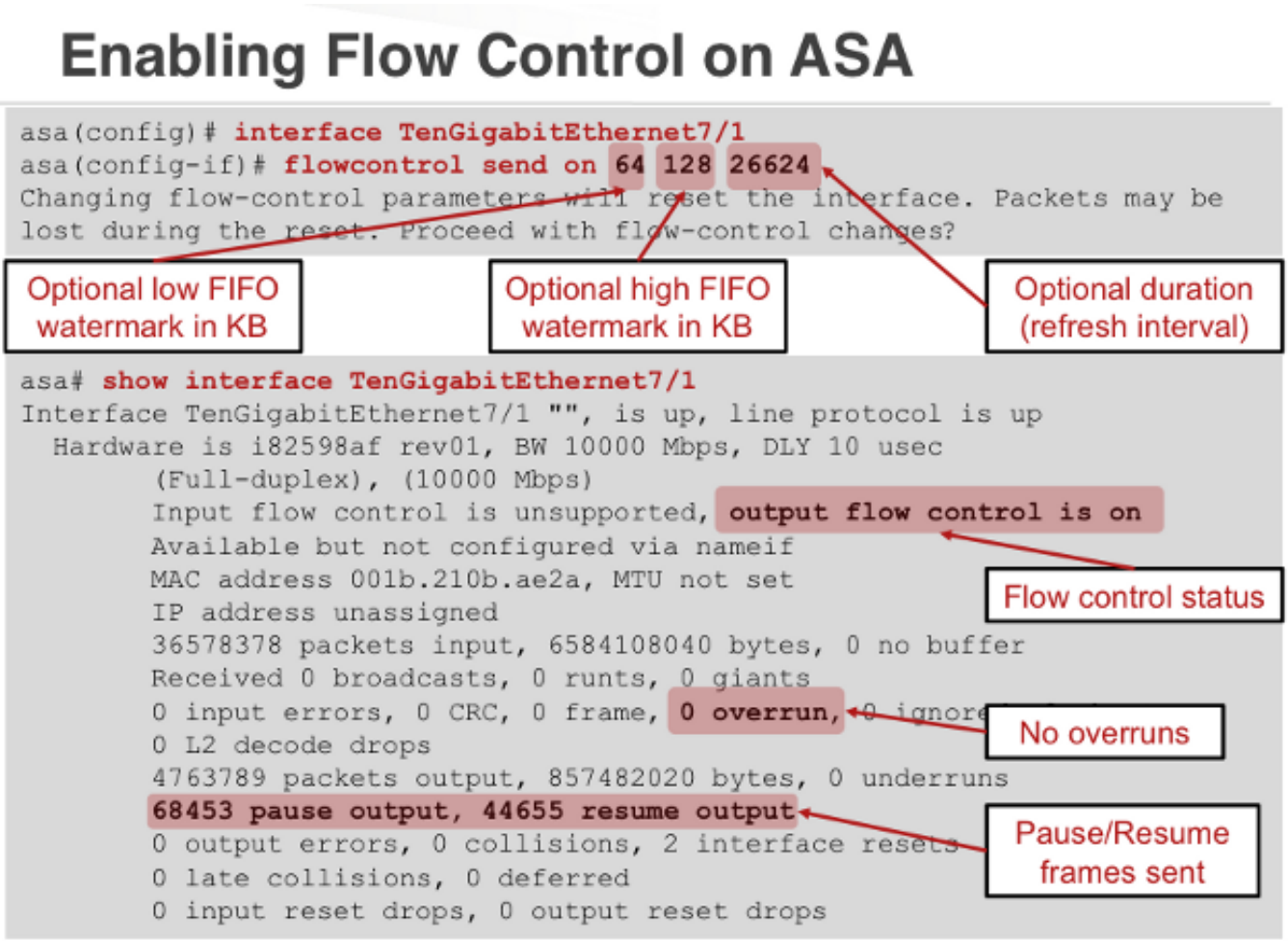
El control de flujo es una característica que permite que la interfaz ASA envíe un mensaje al dispositivo adyacente (un switchport por ejemplo) para darlo instrucciones para parar el enviar del tráfico por una pequeña cantidad de hora. Hace esto cuando el (Primero en Entrar, Primero en Salir FIFO) alcanza cierto punto más alto. Una vez que el (Primero en Entrar, Primero en Salir FIFO) se ha liberado encima de un cierto periodo, el ASA NIC envía una trama del curriculum vitae, y el switchport continúa enviando el tráfico. Este acercamiento trabaja bien porque los puertos del switch adyacente tienen más espacio del búfer y pueden generalmente hacer un mejor trabajo que mitiga los paquetes encendido transmiten que el ASA hace en la dirección receptora.

Usted puede intentar permitir a las capturas en el ASA para detectar las micro-explosiones del tráfico, pero esto no es generalmente útil puesto que se caen los paquetes antes de que puedan conseguir procesados por el ASA y agregados a la captura en la memoria. Un sniffer externo se puede utilizar para capturar y para identificar la ráfaga de tráfico, pero el sniffer externo se puede abrumar a veces por la explosión también.

Control de flujo del permiso para atenuar los sobrantes de la interfaz

La característica del control de flujo fue agregada al ASA en la versión 8.2(2) y posterior para las interfaces 10GE, y a la versión 8.2(5) y posterior para las interfaces 1GE. La capacidad de habilitar el control de flujo en las interfaces ASA que experimentan los sobrantes demuestra ser una técnica eficaz para prevenir los acontecimientos de la caída de paquetes.

Refiera a la característica del control de flujo en la referencia de comandos de las 5500 Series de Cisco ASA, 8.2 para más información.



(Diagrama de la presentación BRKSEC-3021 del cisco live de Andrew Ossipov)

Observe que el “control de flujo de la salida está en” significa que el ASA manda las tramas de pausa del control de flujo la interfaz ASA hacia el dispositivo adyacente (el Switch). El “control de flujo de la entrada está sin apoyo” significa que el ASA no soporta la *recepción de los* bastidores del control de flujo del dispositivo adyacente.

Configuración de muestra del 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: Problemas de rendimiento del monitor y del Troubleshooting
- Presentación del cisco live el “que maximiza funcionamiento del Firewall” - esta presentación delinea la arquitectura de las diversas Plataformas ASA, e incluye la información sobre el funcionamiento y ajustar. Para el acceso a esta presentación, inicie sesión a Ciscolive!365 y busque para el número BRKSEC-3021 de la presentación.
- La Seguridad del TAC de Cisco hace un podcast el episodio #7 “funcionamiento del Firewall de la supervisión” - ésta episodio hecho un podcast ofrece una descripción de las técnicas y los métodos para monitorear el funcionamiento del Firewall y para identificar los problemas de

rendimiento.

- Soporte Técnico y Documentación - Cisco Systems