Solucionar erros de contador de saturação da interface ASA

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Problema](#)
[Causas de saturação da interface](#)
[Etapas para Solucionar Problemas da Causa de Sobrecargas de Interface](#)
[Possíveis causas e soluções](#)
[A CPU no ASA é periodicamente muito ocupada para processar pacotes de entrada (CPU Hogs)](#)
[Perfil de tráfego processado periodicamente faz excesso de assinaturas no ASA](#)
[Intermitent Packet Bursts Oversubscribe a fila FIFO da interface do ASA](#)
[Habilitar controle de fluxo para mitigar sobrecargas de interface](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve o contador de erros "overrun" e como investigar problemas de desempenho ou problemas de perda de pacotes na rede. Um administrador pode observar erros relatados na saída do comando **show interface** no Adaptive Security Appliance (ASA).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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

O contador de erros da interface ASA "overrun" controla o número de vezes que um pacote foi recebido na interface de rede, mas não havia espaço disponível na fila FIFO da interface para armazenar o pacote. Assim, o pacote foi descartado. O valor desse contador pode ser visto com o

comando **show interface**.

Exemplo de saída que exibe o 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)
```

No exemplo acima, 2881 saturações foram observadas na interface desde que o ASA foi inicializado ou desde que o comando **clear interface** foi inserido para limpar os contadores manualmente.

Causas de saturação da interface

Os erros de saturação da interface são geralmente causados por uma combinação destes fatores:

- Nível de software - O software ASA não retira os pacotes da fila FIFO da interface com rapidez suficiente. Isso faz com que a fila FIFO seja preenchida e que novos pacotes sejam descartados.
- Nível de hardware - A taxa na qual os pacotes entram na interface é muito rápida, o que faz com que a fila FIFO seja preenchida antes que o software ASA possa retirar os pacotes. Geralmente, um burst de pacotes faz com que a fila FIFO preencha até a capacidade máxima em um curto período de tempo.

Etapas para Solucionar Problemas da Causa de Sobrecargas de Interface

As etapas para solucionar e solucionar esse problema são:

1. Determine se o ASA experimenta os porcos da CPU e se eles contribuem para o problema. Trabalhe para atenuar os problemas de CPU longos ou frequentes.
2. Entenda as taxas de tráfego da interface e determine se o ASA está com excesso de assinaturas devido ao perfil de tráfego.
3. Determine se as rajadas intermitentes de tráfego causam o problema. Em caso afirmativo, implemente o controle de fluxo na interface ASA e nas portas de switch adjacentes.

Possíveis causas e soluções

A CPU no ASA é periodicamente muito ocupada para processar pacotes de entrada (CPU Hogs)

A plataforma ASA processa todos os pacotes no software e usa os principais núcleos da CPU que manipulam todas as funções do sistema (como syslogs, conectividade do Adaptive Security Device Manager e Inspeção de Aplicativos) para processar os pacotes de entrada. Se um processo de software retém a CPU por mais tempo do que deveria, o ASA registra isso como um evento de sobrecarga da CPU desde que o processo "interrompeu" a CPU. O limite de suínos da CPU é definido em milissegundos e é diferente para cada modelo de dispositivo de hardware. O limite é baseado no tempo que pode demorar para preencher a fila FIFO da interface, dada a potência da CPU da plataforma de hardware e as taxas de tráfego potenciais que o dispositivo pode lidar.

Os erros de CPU às vezes causam erros de saturação de interface em ASAs de núcleo único, como 5505, 5510, 5520, 5540 e 5550. Os porcos longos, que duram 100 milissegundos ou mais, podem causar derrapagens especialmente para níveis de tráfego relativamente baixos e taxas de tráfego não intermitentes. O problema não afeta tanto os sistemas multi-core, já que outros núcleos podem retirar pacotes de um anel Rx se um dos núcleos da CPU estiver obstruído por um processo.

Um cabo que dura mais que o limite do dispositivo faz com que um syslog seja gerado com o id 711004, como mostrado aqui:

```
06 de fevereiro de 2013 14:40:42: %ASA-4-711004: Tarefa executada para 60 ms, Processo = ssh, PC
= 90b0155, Pilha de chamadas = 06 de fevereiro de 2013 14:40:42: %ASA-4-711004: Tarefa executada
para 60 ms, Processo = ssh, PC = 90b0155, Pilha de chamadas = 0x090b0155 0x090bf3b6 0x090b3b84
0x090b3f6e 0b090b 4459 0x090b44d6 0x08c46fcc 0x09860ca0 0x080fad6d 0x080efa5a 0x080f0a1c 0x08069
22c
```

Os eventos de sobrecarga da CPU também são registrados pelo sistema. A saída do comando **show proc cpu-hog** exibe estes campos:

- Process - o nome do processo que ocultou a CPU.
- PROC_PC_TOTAL - o número total de vezes que esse processo obstruiu a CPU.
- MAXHOG - o maior tempo de sobrecarga de CPU observado para esse processo, em milissegundos.
- LASTHOG - a quantidade de tempo que o último porco manteve a CPU, em milissegundos.
- LASTHOG At - a hora em que o suínos da CPU ocorreu pela última vez.
- PC - o valor do contador de programas do processo quando o suínos da CPU ocorreu. (Informações para o Cisco Technical Assistance Center (TAC))
- Pilha de chamadas - a pilha de chamadas do processo quando ocorreu o bloqueio da CPU. (Informações para o Cisco TAC)

Este exemplo mostra a saída do 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#
```

O processo ASA SSH manteve a CPU por 119 ms em 12:25:33 EST de 6 de junho de 2012.

Se os erros de saturação aumentarem continuamente em uma interface, verifique a saída do comando **show proc cpu-hog** para ver se os eventos de sobrecarga da CPU se correlacionam com um aumento no contador de sobrecarga da interface. Se você descobrir que os porcos da CPU contribuem para os erros de saturação da interface, é melhor pesquisar bugs com o Bug Toolkit ou levantar um caso com o Cisco TAC. A saída do comando **show tech-support** também inclui a saída do comando **show proc cpu-hog**.

Perfil de tráfego processado periodicamente faz excesso de assinaturas no ASA

Dependendo do perfil de tráfego, o tráfego que flui pelo ASA pode ser muito para ele lidar e podem ocorrer derrapagens.

O perfil de tráfego consiste em (entre outros aspectos):

- Tamanho do pacote
- Lacuna entre pacotes (taxa de pacotes)
- Protocolo - alguns pacotes são submetidos à inspeção de aplicativos no ASA e exigem mais processamento do que outros pacotes

Esses recursos do ASA podem ser usados para identificar o perfil de tráfego no ASA:

- Netflow - o ASA pode ser configurado para exportar registros do NetFlow versão 9 para um coletor do NetFlow. Esses dados podem ser analisados para entender mais sobre o perfil de tráfego.

- SNMP - utilize o monitoramento SNMP para rastrear as taxas de tráfego da interface ASA, CPU, taxas de conexão e taxas de conversão. As informações podem ser analisadas para entender o padrão de tráfego e como ele muda com o tempo. Tente determinar se há um pico nas taxas de tráfego que se correlaciona a um aumento nas saturações e a causa desse pico de tráfego. Houve casos no TAC em que os dispositivos na rede se comportam mal (devido a uma configuração incorreta ou infecção de vírus) e geram periodicamente uma inundação de tráfego.

Intermitent Packet Bursts Oversubscribe a fila FIFO da interface do ASA

Uma intermitência de pacotes que chegam à placa de rede pode fazer com que o FIFO seja preenchido antes que a CPU possa retirar os pacotes dela. Geralmente, não há muito que possa ser feito para resolver esse problema, mas pode ser atenuado pelo uso da QoS na rede para suavizar as rajadas de tráfego ou o controle de fluxo no ASA e nas portas de switch adjacentes.

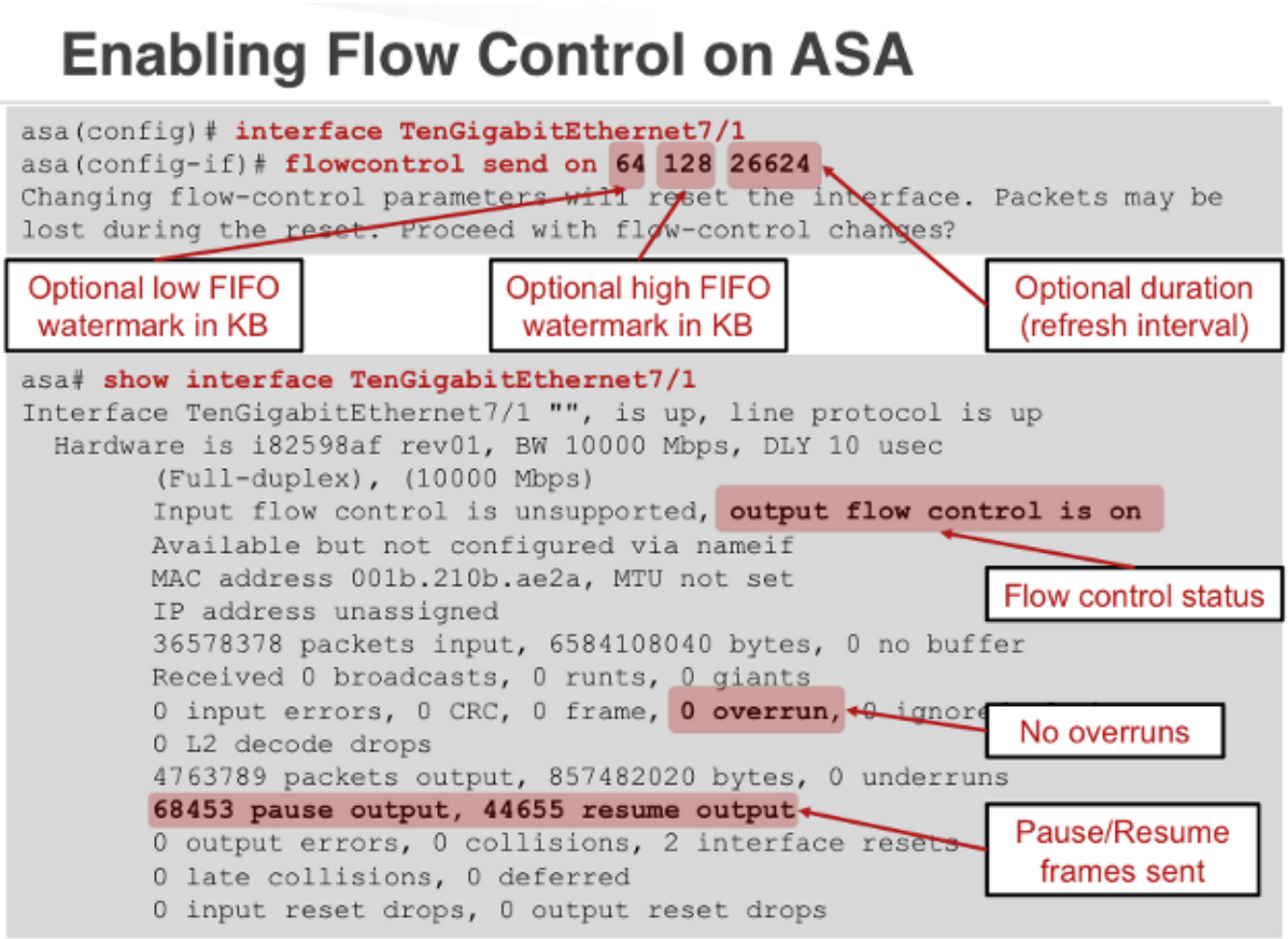
O controle de fluxo é um recurso que permite que a interface do ASA envie uma mensagem ao dispositivo adjacente (uma porta de switch, por exemplo) para instruí-lo a parar de enviar tráfego por um curto período de tempo. Ele faz isso quando o FIFO atinge um certo limite de água. Depois que o FIFO tiver sido liberado, a placa de rede ASA enviará um quadro de retomada e a porta do switch continuará a enviar tráfego. Essa abordagem funciona bem porque as portas de switch adjacentes geralmente têm mais espaço de buffer e podem fazer um melhor trabalho de buffering de pacotes na transmissão do que o ASA na direção de recebimento.

Você pode tentar habilitar capturas no ASA para detectar as microintermitências de tráfego, mas geralmente isso não é útil, pois os pacotes são descartados antes de serem processados pelo ASA e adicionados à captura na memória. Um sniffer externo pode ser usado para capturar e identificar a intermitência de tráfego, mas às vezes o sniffer externo também pode ser sobrecarregado pela intermitência.

Habilitar controle de fluxo para mitigar sobrecargas de interface

O recurso de controle de fluxo foi adicionado ao ASA na versão 8.2(2) e posterior para interfaces 10GE, e na versão 8.2(5) e posterior para interfaces 1GE. A capacidade de ativar o controle de fluxo em interfaces ASA que experimentam saturação prova ser uma técnica eficaz para evitar ocorrências de queda de pacotes.

Consulte o recurso de controle de fluxo na Referência de Comandos do Cisco ASA 5500 Series, 8.2 para obter mais informações.



(Diagrama da apresentação ao vivo BRKSEC-3021 de Andrew Ossipov)

Observe que "o controle de fluxo de saída está ativado" significa que o ASA envia quadros de pausa de controle de fluxo pela interface do ASA em direção ao dispositivo adjacente (o switch). "O controle de fluxo de entrada não é suportado" significa que o ASA não suporta a *recepção* de quadros de controle de fluxo do dispositivo adjacente.

Configuração de exemplo de controle de fluxo:

```
interface GigabitEthernet0/2

flowcontrol send on

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

Informações Relacionadas

- ASA 8.3 e posterior: Monitorar e solucionar problemas de desempenho
- Apresentação ao vivo da Cisco "Maximizando o desempenho do firewall" - Esta apresentação descreve a arquitetura das várias plataformas ASA e inclui informações sobre desempenho e ajuste. Para acessar esta apresentação, faça login no Cisco Live!365 e pesquise o número da apresentação BRKSEC-3021.
- Episódio nº 7 do podcast de segurança do Cisco TAC "Monitorando o desempenho do firewall" - Este episódio de podcast apresenta uma discussão de técnicas e métodos para monitorar o desempenho do firewall e identificar problemas de desempenho.
- Suporte Técnico e Documentação - Cisco Systems