Pesquise defeitos erros contrários do overrun da relação ASA

Índice

Introdução

Este documento descreve o contador de erros do “overrun” e como investigar problemas de desempenho ou problemas da perda de pacotes na rede. Um administrador pôde observar os erros relatados no **comando show interface** output na ferramenta de segurança adaptável (ASA).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Problema

O contador de erro de interface ASA “passa” segue o número de vezes que um pacote esteve

recebido na interface de rede, mas não havia nenhum espaço disponível na fila de FIFO da relação para armazenar o pacote. Assim, o pacote foi deixado cair. O valor deste contador pode ser considerado com o **comando show interface**.

Saídas de exemplo que indicam 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 excedentes foram observadas na relação desde que o ASA carreg acima ou desde que o comando clear interface foi inscrito a fim cancelar manualmente os contadores.

Causas de excedentes da relação

Os erros do overrun da relação são causados geralmente por uma combinação destes fatores:

- Nível de software - O software ASA não retira os pacotes da fila de FIFO da relação rapidamente bastante. Isto faz com que a fila de FIFO encham-se acima e os pacotes novos a ser deixados cair.
- Nível de hardware - A taxa em que os pacotes entram a relação é demasiado rápida, que faz com que a fila de FIFO se encha antes que o software ASA possa retirar os pacotes. Geralmente, uma explosão dos pacotes faz com que a fila de FIFO encha-se até a capacidade máxima em uma quantidade de tempo curta.

As etapas para pesquisar defeitos a causa da relação passam

As etapas para pesquisar defeitos e endereçar este problema são:

1. Determine se o ASA experimenta CPU hog e se contribuem ao problema. Trabalhe para abrandar todos os CPU hog longos ou frequentes.
2. Compreenda as taxas de tráfego da relação e determine se o ASA é oversubscribed devido ao perfil de tráfego.
3. Determine se as intermitências de tráfego intermitentes causam o problema. Em caso afirmativo, execute o controle de fluxo na relação e em portas de switch adjacente ASA.

Causas e soluções do potencial

O CPU no ASA é periodicamente demasiado ocupado processar pacotes recebidos (os CPU hog)

A plataforma ASA processa todos os pacotes no software e usa os núcleos do CPU principal que seguram todas as funções de sistema (tais como Syslog, a Conectividade adaptável do Security Device Manager, e a inspeção de aplicativo) a fim processar pacotes recebidos. Se um processo de software guarda o CPU para mais por muito tempo do que deve, o ASA grava este como um evento do CPU hog desde que o processo “hogged” o CPU. O ponto inicial do CPU hog é ajustado nos milissegundos, e sido diferente para cada modelo da ferramenta de hardware. O ponto inicial é baseado em quanto tempo poderia tomar para encher a fila de FIFO da relação dada a potência de CPU da plataforma de hardware e o tráfego potencial avalia o dispositivo pode segurar.

A relação da causa dos CPU hog às vezes passa erros no único-núcleo ASA, tais como os 5505, os 5510, os 5520, os 5540, e os 5550. Os porcos longos, isso duram por 100 milissegundos ou mais, podem especialmente fazer com que as excedentes ocorram para relativamente níveis do tráfego baixo e taxas de tráfego da NON-intermitência. O problema não impacta sistemas do multi-núcleo tanto quanto, desde que outros núcleos podem retirar pacotes de um anel RX se um dos núcleos CPU hogged por um processo.

Um porco que dure mais do que o ponto inicial do dispositivo faz com que um Syslog seja gerado com identificação 711004, como mostrado aqui:

```
6 de fevereiro de 2013 14:40:42: %ASA-4-711004: A tarefa foi executado para 60 milissegundos,
processo = ssh, PC = 90b0155, pilha de atendimento = 6 de fevereiro de 2013 14:40:42: %ASA-4-
711004: A tarefa foi executado para 60 milissegundos, processo = ssh, PC = 90b0155, pilha de
atendimento = 0x090b0155 0x090bf3b6 0x090b3b84 0x090b3f6e 0x090b4459 0x090b44d6 0x08c46fcc
0x09860ca0 0x080fad6d 0x080efa5a 0x080f0a1c 0x0806922c
```

Os eventos do CPU hog são gravados igualmente pelo sistema. A saída do comando do **CPU hog do proc da mostra** indica estes campos:

- Processo - o nome do processo que hogged o CPU.
- PROC_PC_TOTAL - o número total de épocas que este processo hogged o CPU.
- MAXHOG - o tempo o mais longo do CPU hog observado para esse processo, nos milissegundos.
- LASTHOG - a quantidade de tempo o último porco guardou o CPU, nos milissegundos.
- LASTHOG então o CPU hog ocorreu por último.
- PC - o valor do contador de programa do processo quando o CPU hog ocorreu. (Informação para o centro de assistência técnica da Cisco (TAC))
- Pilha de atendimento - a pilha de atendimento do processo quando o CPU hog ocorreu. (Informação para o tac Cisco)

Este exemplo mostra o comando do **CPU hog do proc da mostra** output:

```
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 guardou o CPU para 119ms em 12:25:33 EST junho 6o 2012.

Se os erros do overrun aumentam continuamente em uma relação, verifique a saída do comando do **CPU hog do proc da mostra** a fim ver se os eventos do CPU hog correlacionam com um aumento no contador do overrun da relação. Se você encontra que os CPU hog contribuem à relação passa erros, é o melhor procurar por erros com o Bug Toolkit, ou aumente um caso com o tac Cisco. A saída do **comando show tech-support** igualmente inclui a saída do comando do **CPU hog do proc da mostra**.

Oversubscribes periodicamente processado perfil de tráfego o ASA

O dependente em cima no perfil de tráfego, do tráfego que corre através do ASA pôde ser demasiado para que segure e das excedentes pôde ocorrer.

O perfil de tráfego consiste (entre outros aspectos):

- Tamanho do pacote
- Lacuna inter-pacote (taxa de pacote de informação)
- Protocolo - alguns pacotes são sujeitados à inspeção de aplicativo no ASA e exigem o processamento do que outros pacotes

Estas características ASA podem ser usadas a fim identificar o perfil de tráfego no ASA:

- Netflow - o ASA pode ser configurado para exportar registros da versão 9 do Netflow para um coletor de Netflow. Estes dados podem então ser analisados para compreender mais sobre o perfil de tráfego.

- SNMP - utilize a monitoração SNMP a fim seguir as taxas de tráfego da relação ASA, CPU, taxas de conexão, e taxas da tradução. A informação pode então ser analisada a fim compreender o teste padrão de tráfego e como muda ao longo do tempo. Tente determinar se há um ponto nas taxas de tráfego que correlacione a um aumento nas excedentes, e na causa desse aumento de tráfego. Houve uns casos no TAC onde os dispositivos na rede se portam mal (devido ao misconfiguration ou à infecção do vírus) e se gerenciem uma inundação do tráfego periodicamente.

Intermitências de pacote de informação intermitentes Oversubscribe a fila de FIFO da relação ASA

Uma explosão dos pacotes que chegam no NIC poderia fazer com que o FIFO torne-se enchido antes que o CPU possa retirar os pacotes dele. Não há geralmente muito que pode ser feito a fim resolver este problema, mas pode ser abrandado pelo uso de QoS na rede alisar para fora as intermitências de tráfego, ou pelo controle de fluxo no ASA e nas portas de switch adjacente.

O controle de fluxo é uma característica que permita que a relação do ASA envie uma mensagem ao dispositivo adjacente (um switchport por exemplo) a fim o instruir para parar de enviar o tráfego para uma quantidade de tempo curta. Faz este quando o FIFO alcança uma determinada

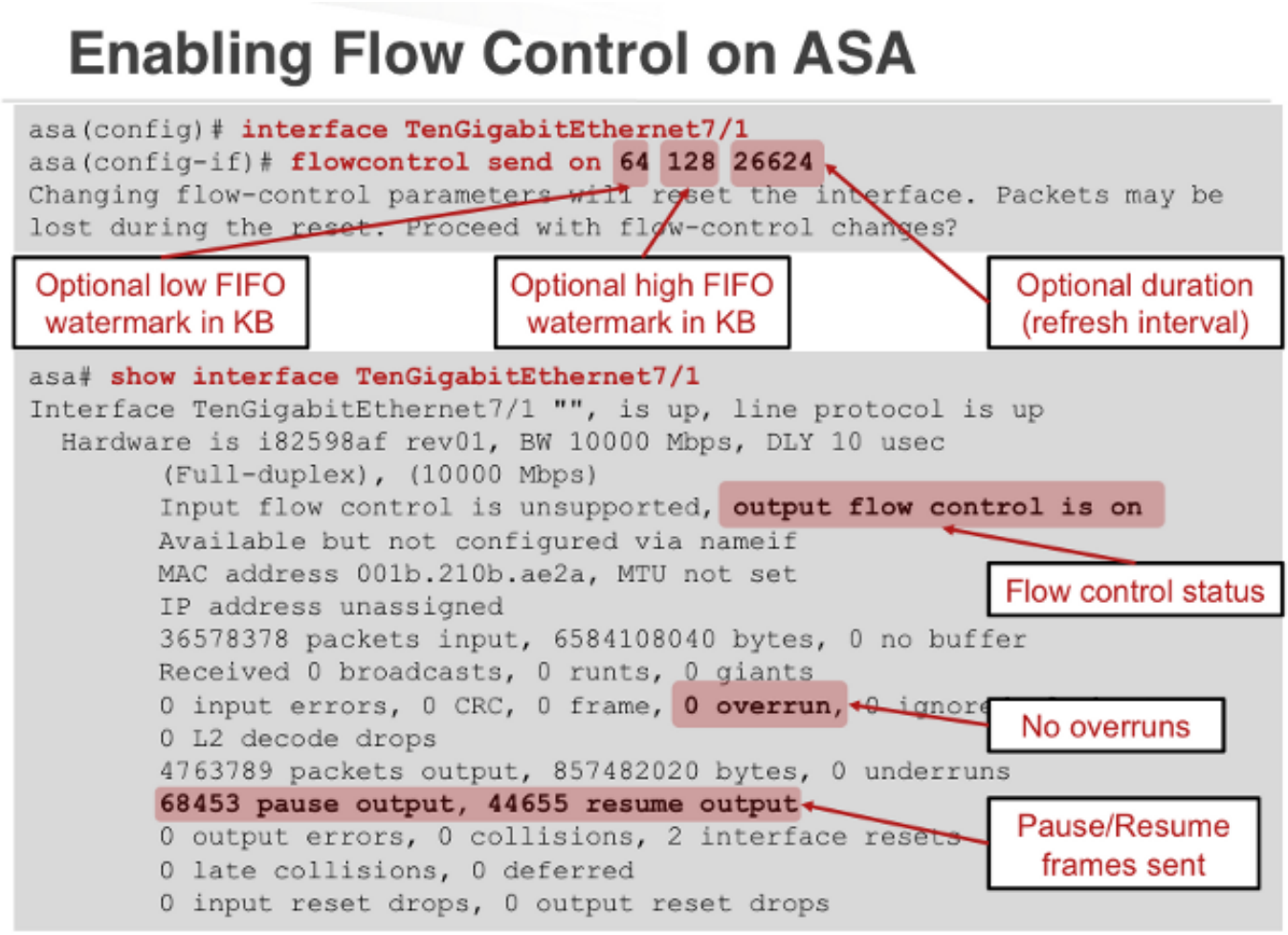
marca d'água alta. Uma vez que o FIFO foi livrado acima de alguma quantidade, o ASA NIC envia um quadro do resumo, e o switchport continua a enviar o tráfego. Esta aproximação trabalha bem porque as portas de switch adjacente geralmente têm mais espaço de buffer e podem fazer pacotes melhores de uma proteção do trabalho transmitem sobre do que o ASA faz na rota de recepção.

Você pode tentar permitir captações no ASA de detectar as micro-explosões do tráfego, mas geralmente este não é útil desde que os pacotes são deixados cair antes que possam obter processados pelo ASA e adicionados à captação na memória. Um sniffer externo pode ser usado para capturar e identificar a intermitência de tráfego, mas às vezes o sniffer externo pode ser oprimido pela explosão também.

Permita o controle de fluxo de abrandar excedentes da relação

A característica do controle de fluxo foi adicionada ao ASA na versão 8.2(2) e mais recente para as relações 10GE, e à versão 8.2(5) e mais recente para as relações 1GE. A capacidade para permitir o controle de fluxo nas relações ASA que a experiência passa prova ser uma técnica eficaz para impedir ocorrências da queda de pacote de informação.

Refira a característica do controle de fluxo na referência de comandos do 5500 Series de Cisco ASA, 8.2 para mais informação.



(Diagrama da apresentação BRKSEC-3021 do cisco live de Andrew Ossipov)

Note que da “o controle de fluxo saída está em” significa que o ASA envia a frames de pausa do controle de fluxo para fora a relação ASA para o dispositivo adjacente (o interruptor). Da “o

controle de fluxo entrada é unsupported” significa que o ASA não apoia a *recepção de* quadros do controle de fluxo do dispositivo adjacente.

Configuração de exemplo do 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 mais atrasado: Monitore e pesquise defeitos problemas de desempenho
- Apresentação do cisco live “que maximiza o desempenho do Firewall” - esta apresentação esboça a arquitetura das várias Plataformas ASA, e inclui a informação sobre o desempenho e o ajustamento. Para o acesso a esta apresentação, entre a Ciscolive!365 e procure pelo número BRKSEC-3021 da apresentação.
- A Segurança do tac Cisco Podcast o episódio #7 da “desempenho do Firewall monitoração” - este episódio do podcast caracteriza uma discussão de técnicas e métodos para monitorar o desempenho do Firewall e para identificar problemas de desempenho.
- Suporte Técnico e Documentação - Cisco Systems