ASA 인터페이스 오버런 카운터 오류 문제 해결

목차

소개

이 문서에서는 "오버런" 오류 카운터와 네트워크에서 성능 문제 또는 패킷 손실 문제를 조사하는 방법에 대해 설명합니다.관리자는 ASA(Adaptive Security Appliance)의 **show interface** 명령 출력에 보고된 오류를 확인할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

ASA 인터페이스 오류 카운터 "overrun"은 네트워크 인터페이스에서 패킷을 받은 횟수를 추적하지만, 패킷을 저장할 수 있는 인터페이스 FIFO 큐에 사용 가능한 공간이 없습니다.따라서 패킷이 삭제되었습니다.이 카운터의 값은 **show interface** 명령과 함께 볼 수 있습니다.

문제를 표시하는 출력의 예:

```
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)
```

위의 예에서, ASA가 부팅된 이후 또는 카운터를 수동으로 지우기 위해 명령 **clear interface**를 입력한 이후 인터페이스에서 2881 오버런이 관찰되었습니다.

인터페이스 오버런의 원인

인터페이스 오버런 오류는 일반적으로 다음 요소의 조합으로 인해 발생합니다.

- 소프트웨어 레벨 - ASA 소프트웨어가 인터페이스 FIFO 대기열에서 패킷을 충분히 빠르게 제거하지 않습니다.그러면 FIFO 대기열이 채워지고 새 패킷이 삭제됩니다.
- 하드웨어 레벨 - 패킷이 인터페이스로 들어오는 속도가 너무 빠릅니다. 따라서 ASA 소프트웨어가 패킷을 풀 수 있기 전에 FIFO 대기열이 채워집니다.일반적으로 패킷의 버스트는 FIFO 대기열이 짧은 시간 내에 최대 용량을 채우도록 합니다.

인터페이스 오버런의 원인 해결 단계

이 문제를 해결하고 해결하는 단계는 다음과 같습니다.

1. ASA에서 CPU 돼지를 경험하는지, CPU가 문제에 기여하는지 확인합니다.길고 자주 사용하는 CPU 마침을 완화시키는 작업
2. 인터페이스 트래픽 속도를 파악하고 트래픽 프로필로 인해 ASA가 초과 가입되어 있는지 확인합니다.
3. 간헐적인 트래픽 버스트가 문제를 일으키는지 확인합니다.이 경우 ASA 인터페이스 및 인접 스위치 포트에 흐름 제어를 구현합니다.

잠재적 원인 및 솔루션

ASA의 CPU가 주기적으로 너무 바빠서 수신 패킷(CPU TINES)을 처리할 수 없음

ASA 플랫폼은 소프트웨어에서 모든 패킷을 처리하고 모든 시스템 기능(예: syslog, Adaptive Security Device Manager 연결, 애플리케이션 검사)을 처리하는 기본 CPU 코어를 사용하여 수신 패킷을 처리합니다.소프트웨어 프로세스에서 CPU를 필요한 시간보다 오래 보관할 경우 프로세스

가 CPU를 "과다"한 후 ASA는 이를 CPU 과다 사용 이벤트로 기록합니다.CPU 호그 임계값은 밀리초 단위로 설정되며 각 하드웨어 어플라이언스 모델에 따라 다릅니다.임계값은 하드웨어 플랫폼의 CPU 전력 및 디바이스가 처리할 수 있는 잠재적 트래픽 속도를 고려하여 인터페이스 FIFO 대기열을 채우는 데 걸리는 시간을 기반으로 합니다.

CPU Thins는 때때로 5505, 5510, 5520, 5540 및 5550과 같은 싱글 코어 ASA에서 인터페이스 오버런 오류를 발생시킵니다.100밀리초 이상 지속되는 긴 돼지, 특히 상대적으로 낮은 트래픽 수준과 비버스트 트래픽 속도에서 오버런이 발생할 수 있습니다.CPU 코어 중 하나가 프로세스에 의해 호스팅되는 경우 다른 코어가 Rx 링에서 패킷을 꺼낼 수 있으므로 이 문제는 멀티코어 시스템만큼 큰 영향을 미치지 않습니다.

디바이스 임계값보다 오래 지속되는 과다 사용은 다음과 같이 ID 711004로 syslog를 생성합니다.

```
2013 2 6 14:40:42:%ASA-4-711004:60msec   ,  = ssh, PC = 90b0155,   = 2013 2 6 14:40:42:%ASA-4-
711004:60msec   ,  = ssh, PC = 90b0155,   = 0x090b0155 0x090bf3b6 0x090b3b84 0x090b3f6e
0x090b4590x094b4d4d4d 0x08c46fcc 0x09860ca0 0x080fad6d 0x080efa5a 0x080f0a1c 0x0806922c
```

CPU 호그 이벤트도 시스템에 의해 기록됩니다.**show proc cpu-hog** 명령의 출력에는 다음 필드가 표시됩니다.

- Process(프로세스) - CPU를 고정한 프로세스의 이름입니다.
- PROC_PC_TOTAL - 이 프로세스에서 CPU를 홀딩한 총 횟수입니다.
- MAXHOG - 해당 프로세스에 대해 관찰된 가장 긴 CPU 호그 시간(밀리초)입니다.
- LASTHOG - 마지막 과다 사용 시 CPU가 걸린 시간(밀리초)입니다.
- LASTHOG At - CPU 과다 사용이 마지막으로 발생한 시간입니다.
- PC - CPU 과다 사용이 발생한 프로세스의 프로그램 카운터 값입니다.(Cisco TAC(Technical Assistance Center) 정보)
- 통화 스택 - CPU 과다 사용이 발생한 프로세스의 통화 스택입니다.(Cisco TAC에 대한 정보)

다음 예에서는 show proc cpu-**hog** 명령 출력을 보여 줍니다.

```
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#
```

ASA SSH 프로세스는 2012년 6월 6일, 12:25:33에 119ms의 CPU를 보유했습니다.

인터페이스에서 오버런 오류가 계속 증가하면 **show proc cpu-hog** 명령의 출력을 확인하여 CPU 과다 처리 카운터의 증가와 상관관계가 있는지 확인합니다.CPU 돼지를 인터페이스 오버런 오류로 간주할 경우 버그 툴킷으로 버그를 검색하거나 Cisco TAC에서 케이스를 제기하는 것이 좋습니다

.**show tech-support** 명령의 출력에는 **show proc cpu-hog** 명령 출력도 포함됩니다.

ASA를 정기적으로 오버서브스크립션하는 트래픽 프로필

트래픽 프로필에 따라 ASA를 통과하는 트래픽이 너무 많아 처리할 수 없으며 오버런이 발생할 수 있습니다.

트래픽 프로필은 (기타 여러 측면) 로 구성됩니다.

- 패킷 크기
- 패킷 간 간격(패킷 속도)
- 프로토콜 - 일부 패킷은 ASA에서 애플리케이션 검사를 받고 다른 패킷보다 더 많은 처리가 필요합니다.

다음 ASA 기능을 사용하여 ASA에서 트래픽 프로필을 식별할 수 있습니다.

- Netflow - NetFlow 버전 9 레코드를 NetFlow 컬렉터로 내보내도록 ASA를 구성할 수 있습니다.그런 다음 이 데이터를 분석하여 트래픽 프로필에 대해 자세히 이해할 수 있습니다.

- SNMP - ASA 인터페이스 트래픽 속도, CPU, 연결 속도 및 변환 속도를 추적하기 위해 SNMP 모니터링을 활용합니다.그런 다음 트래픽 패턴과 시간의 경과에 따른 변경 방법을 파악하기 위해 정보를 분석할 수 있습니다.초과 실행 증가 및 트래픽 급등의 원인과 관련된 트래픽 비율이 높은지 확인합니다.TAC에서는 컨피그레이션 오류 또는 바이러스 감염으로 인해 네트워크의 디바이스가 잘못 동작하고 주기적으로 트래픽이 플러딩되는 경우가 있었습니다.

간헐적인 패킷 버스트 ASA 인터페이스 FIFO 대기열 초과 가입

NIC에 도착하는 패킷의 버스트로 인해 CPU에서 패킷을 빼내기 전에 FIFO가 채워질 수 있습니다.이 문제를 해결하기 위해 할 수 있는 일은 많지 않지만, 트래픽 버스트를 원활하게 하기 위해 네트워크에서 QoS를 사용하거나 ASA와 인접 스위치 포트에 대한 흐름 제어를 통해 완화될 수 있습니다.

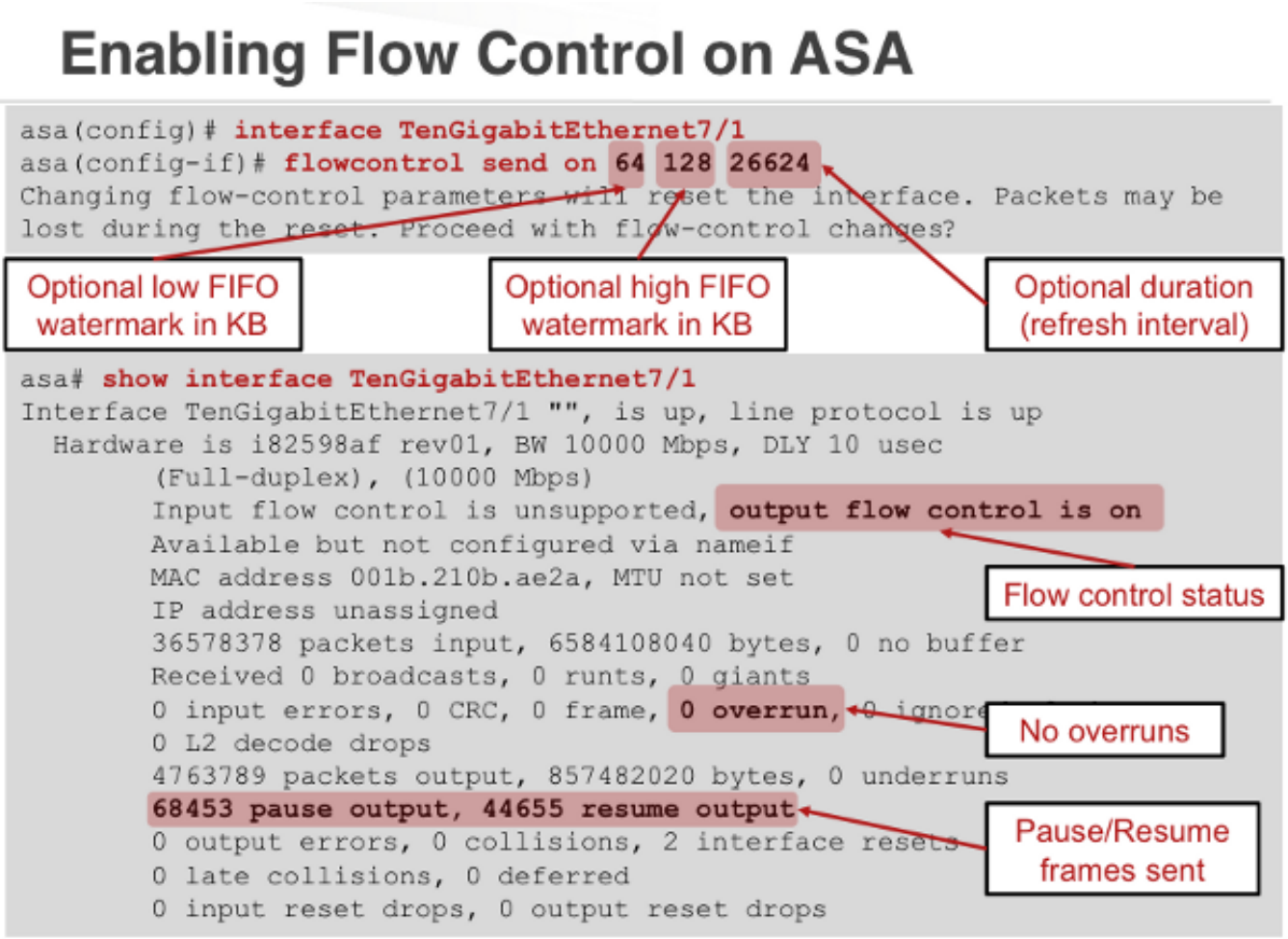
흐름 제어는 ASA의 인터페이스가 짧은 시간 동안 트래픽 전송을 중지하도록 지시하기 위해 인접 디바이스(예: switchport)로 메시지를 보낼 수 있도록 하는 기능입니다.이것은 FIFO가 특정 높은 수위 점에 도달할 때 그렇게 합니다.FIFO가 어느 정도 여유 있게 되면 ASA NIC는 재개 프레임을 전송하고 스위치 포트는 트래픽을 계속 전송합니다.이러한 접근 방식은 인접 스위치 포트가 일반적으로 버퍼 공간을 더 많이 가지며 ASA가 수신 방향에서 하는 것보다 전송 시 패킷을 더 잘 버퍼링할 수 있기 때문에 효과적입니다.

ASA에서 캡처를 활성화하여 트래픽 마이크로 버스트를 탐지할 수 있지만, 일반적으로 패킷이 삭제되기 전에 ASA에서 처리되어 메모리의 캡처에 추가되므로 유용하지 않습니다.외부 스니퍼를 사용하여 트래픽 버스트를 캡처하고 식별할 수 있지만, 외부 스니퍼는 버스트로 인해 압도될 수도 있습니다.

Flow Control을 활성화하여 인터페이스 오버런 완화

10GE 인터페이스의 경우 버전 8.2(2) 이상, 1GE 인터페이스의 경우 버전 8.2(5) 이상에서 흐름 제어 기능이 ASA에 추가되었습니다.오버런이 발생하는 ASA 인터페이스에서 흐름 제어를 활성화하는 기능은 패킷 삭제 발생을 방지하는 효과적인 기법입니다.

자세한 내용은 Cisco ASA 5500 Series 명령 참조, 8.2의 흐름 제어 기능을 참조하십시오.



(Andrew Ossipov의 Cisco Live Presentation BRKSEC-3021 다이어그램)

"출력 흐름 제어가 켜져 있음"은 ASA가 흐름 제어 일시 중지 프레임을 ASA 인터페이스에서 인접 디바이스(스위치)로 전송함을 의미합니다."입력 흐름 제어가 지원되지 않음"은 ASA가 인접 디바이스에서 흐름 제어 프레임의 수신을 지원하지 않음을 의미합니다.

플로우 제어 샘플 컨피그레이션:

```
interface GigabitEthernet0/2

flowcontrol send on

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

관련 정보

- [ASA 8.3 이상:성능 문제 모니터링 및 문제 해결]
- [Cisco Live Presentation "방화벽 성능 극대화"] - 이 프레젠테이션은 다양한 ASA 플랫폼의 아키텍처를 요약하고 성능 및 튜닝에 대한 정보를 포함합니다. 이 프레젠테이션에 액세스하려면 Cisco!365 프레젠테이션 번호 BRKSEC-3021을 검색합니다.
- [Cisco TAC 보안 팟캐스트 에피소드 #7 "방화벽 성능 모니터링"] - 이 팟캐스트 에피소드는 방화

벽 성능을 모니터링하고 성능 문제를 식별하는 기술 및 방법에 대해 설명합니다.

- 기술 지원 및 문서 – Cisco Systems