NAT 게이트키퍼 기본 컨피그레이션으로 인한 높은 QFP 사용률 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[배경 정보](#)

[증상](#)

[패킷 추적 기능](#)

- [기본 패킷 추적 컨피그레이션](#)

[NAT 게이트키퍼란?](#)

[NAT 게이트키퍼 확인](#)

[해결 방법/수정](#)

- [해결 방법 1](#)
- [해결 방법 2](#)

[요약](#)

[관련 정보](#)

소개

이 문서에서는 NATed 트래픽과 비 NATed 트래픽이 혼합되어 발생하는 라우팅 플랫폼의 QFP(High Quantum Flow Processor) 활용을 식별하고 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS® XE 패킷 포워딩 아키텍처에 대한 기본 지식
- 패킷 추적 기능을 통한 기본 환경

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다. ASR1000, ISR4000, ISR1000, Cat8000 또는 Cat8000v와 같은 물리적/가상 QFP가 포함된 모든 라우팅 Cisco IOS XE 플랫폼에 적용됩니다.

이 문서는 자동 모드의 Cisco IOS XE 디바이스, SDWAN(컨트롤러) 또는 SD-routing을 기반으로 하

며 유사한 논리를 따를 수 있지만 세부 사항은 다를 수 있습니다.

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

배경 정보

Cisco QFP(Quantum Flow Processor)의 높은 사용률 및 성능 문제는 동일한 인터페이스에 NAT된 트래픽 흐름과 비 NAT 트래픽 흐름이 혼합된 경우 Cisco 라우터에서 관찰될 수 있습니다. 이는 또한 인터페이스 오류 또는 느림과 같은 다른 성능 문제를 야기할 수 있습니다.

참고: QFP는 ESP(Embedded Services Processor)에 위치하며, 모든 인바운드 및 아웃바운드 트래픽 흐름에 대한 데이터 플레인 및 패킷 처리를 담당합니다. 이는 플랫폼에 따라 물리적 또는 가상화될 수 있습니다.

증상

이 동작을 식별하려면 라우터에서 이러한 증상을 검증하고 확인하는 것이 중요합니다.

1. HIgh QFP 로드 경고. 이러한 경고는 로드가 임계값 80%를 초과할 때 나타납니다.

```
Feb 8 08:02:25.147 mst: %IOSXE_QFP-2-LOAD_EXCEED: Slot: 0, QFP:0, Load 81% exceeds the setting threshol
Feb 8 08:04:15.149 mst: %IOSXE_QFP-2-LOAD_RECOVER: Slot: 0, QFP:0, Load 59% recovered.
```

참고: 또한 QFP의 로드와 트래픽 속도를 나타내기 위해 show platform hardware qfp active datapath utilization summary 명령을 실행할 수 있습니다.

```
Router# show platform hardware qfp active datapath utilization summary
  CPP 0: Subdev 0            5 secs        1 min        5 min       60 min
Input:  Priority (pps)            0            0            0            0
                 (bps)           96           32           32           32
    Non-Priority (pps)       327503       526605       552898       594269
                 (bps)   1225600520   2664222472   2867573720   2960588728
           Total (pps)       327503       526605       552898       594269
                 (bps)   1225600616   2664222504   2867573752   2960588760
Output: Priority (pps)            6            7            7            7
                 (bps)         8576         9992         9320         9344
    Non-Priority (pps)       327715       526839       553128       594506
                 (bps)   1257522072   2714335584   2920005904   3016943800
           Total (pps)       327721       526846       553135       594513
                 (bps)   1257530648   2714345576   2920015224   3016953144
Processing: Load (pct)           99           72           34           19
```

2. 인터페이스 오류 QFP 사용률이 높은 경우 역압으로 인해 패킷이 삭제될 수 있습니다. 이러한 경우, 인터페이스에서 오버런 및 입력 드랍이 일반적으로 관찰됩니다. 이 정보를 표시하려면 show interfaces 명령을 실행할 수 있습니다.

```
Router# show interface gigabitEthernet 0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is ISR4351-3x1GE, address is e41f.7b59.cba1 (bia e41f.7b59.cba1)
  Description: ### LAN Interface ###
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 2/255
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is force-up, media type is LX
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:02, output 00:06:47, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  30 second input rate 9390000 bits/sec, 2551 packets/sec
  30 second output rate 1402000 bits/sec, 1323 packets/sec
     368345166434 packets input, 199203081647360 bytes, 0 no buffer
     Received 159964 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     2884115457 input errors, 0 CRC, 0 frame, 2884115457 overrun, 0 ignored
     0 watchdog, 3691484 multicast, 0 pause input
     220286824008 packets output, 32398293188401 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     3682606 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     21 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

3. 일부 시나리오에서는 사용자가 네트워크의 느림을 호소할 수 있습니다.

패킷 추적 기능

- 패킷 추적은 Cisco IOS XE 플랫폼에서 데이터 패킷을 처리하는 방법에 대한 자세한 정보를 제공하는 툴입니다.
- 여기에는 계정 관리, 요약 및 데이터 경로인 세 가지 검사 레벨이 있습니다. 검사 레벨은 디버그 플랫폼 조건 상태를 기반으로 합니다.
- 다음과 같은 정보를 얻을 수 있습니다.
    - 입출력 인터페이스
    - 패킷 상태
    - 타임스탬프
    - 패킷 추적

참고: 데이터 경로 구성은 더 많은 패킷 처리 리소스를 소비하며, 이는 필터 조건과 일치하는 패킷에만 반영됩니다.

Cisco IOS XE Datapath 패킷 추적 기능 트러블슈팅의 패킷 추적에 대한 자세한 정보

기본 패킷 추적 컨피그레이션

데이터 경로 레벨 검사가 포함된 기본 패킷 추적 구성의 예입니다. 8192개의 패킷을 순환 방식으로 수집하고(기존 패킷을 덮어쓰기), 레이어 3에서 각 패킷의 복사본을 생성하며, 이 사본은 인터페이스 GigabitEthernet 0/0/1에 도달하고 그대로 남습니다.

```
Router# debug platform packet-trace packet 8192 circular fia-trace data-size 2048
Router# debug platform packet-trace copy packet both L3 size 64
Router# debug platform condition interface gigabitEthernet 0/0/1 both
Router# debug platform condition start
Router# debug platform condition stop
```

이러한 명령을 사용하여 패킷 추적의 결과를 확인할 수 있습니다.

```
Router# show platform packet-trace summary
Router# show platform packet-trace packet all
```

패킷 추적 캡처에서 NAT 기능이 예상보다 많은 리소스를 소비하는지 확인할 수 있습니다. 다음 예에서는 IPV4_NAT_INPUT_FIA 기능의 경과된 시간이 다른 기능의 경과된 시간보다 상당히 크다는 것을 알 수 있습니다. 이 동작은 일반적으로 QFP가 이 기능을 처리하는 데 더 많은 시간이 소요되며, 그 결과 NAT에 QFP의 더 많은 리소스가 사용됨을 나타냅니다.

```
Packet: 161         CBUG ID: 161
Summary
  Input     : GigabitEthernet0/0/1
  Output    : GigabitEthernet0/0/2.1730
  State     : FWD
  Timestamp
    Start   : 25136781447706429 ns (02/10/2024 00:25:49.584050 UTC)
    Stop    : 25136781447993237 ns (02/10/2024 00:25:49.584337 UTC)



  Feature: IPV4_NAT_INPUT_FIA   <<<<<<<<<<<<
    Entry       : Input - 0x700162ac
    Input       : GigabitEthernet0/0/1
    Output      :
```

```
    Lapsed time : 1873376 ns     <<<<<<<<<<<<
```

```
  Feature: IPV4_INPUT_IPOPTIONS_PROCESS
    Entry       : Input - 0x70016344
    Input       : GigabitEthernet0/0/1
    Output      : GigabitEthernet0/0/2.1730
    Lapsed time : 64 ns
```

NAT 게이트키퍼란?

Cisco IOS XE 라우팅 플랫폼에서는 NAT(Network Address Translation) 게이트키퍼 기능이 기본적으로 활성화되어 있습니다. NAT 게이트키퍼는 원래 NAT 변환을 생성하기 위해 과도한 처리 리소스를 사용하는 비 NAT 처리 흐름을 방지하기 위해 만들어졌습니다. NAT 게이트키퍼는 소스 주소를 기반으로 내부-외부 방향 및 다른 방향에 대해 2개의 작은 캐시를 생성합니다. 각 캐시 엔트리는 소스 주소, VRF(virtual routing and forwarding) ID, 타이머 값(엔트리를 무효화하는 데 사용됨) 및 프레임 카운터로 구성됩니다.

NATed 인터페이스의 많은 양의 비 NATed 트래픽은 많은 양의 리소스를 소비하고 QFP 사용률을 급상승시킵니다. Cisco는 고객이 가능한 한 동일한 인터페이스에서 NAT-ed 및 비 NAT-ed 플로우를 갖지 않도록 권장합니다.

NAT 게이트키퍼 확인

NAT 게이트키퍼 통계는 show platform hardware qfp active feature nat datapath { gatein 명령을 사용하여 확인할 수 있습니다 | 게이트아웃 }활동. 캐시의 크기, 적중 횟수, 누락 횟수, 시간 초과 횟수, 추가된 활성 항목 수를 표시합니다.일반적으로 누락 횟수가 많고 짧은 시간 내에 이 숫자가 급격하게 증가하는 경우 많은 수의 Not-Natted 플로우가 캐시에 추가되지 않음을 나타냅니다. 이러한 동작으로 인해 이러한 흐름은 NAT 워크플로 내의 QFP에 의해 처리되며 높은 QFP 사용률로 증가할 수 있습니다.

```
Router# show platform hardware qfp active feature nat datapath gatein activity
Gatekeeper on
def mode Size 8192, Hits 191540578459, Miss 3196566091, Aged 1365537 Added 9 Active 7

Router# show platform hardware qfp active feature nat datapath gateout activity
Gatekeeper on
def mode Size 8192, Hits 448492109001, Miss 53295038401, Aged 149941327 Added 603614728 Active 1899
```

해결 방법/수정

대부분의 환경에서 NAT 게이트키퍼 기능은 제대로 작동하며 문제를 일으키지 않습니다. 그러나 이 문제가 발생하면 몇 가지 방법으로 해결할 수 있습니다.

해결 방법 1

이러한 유형의 문제에 대해서는 NATed 트래픽과 비 NATed 트래픽을 동일한 인터페이스에서 분리하는 것이 좋습니다. 서로 다른 인터페이스 또는 네트워크 디바이스에서 사용할 수 있습니다.

해결 방법 2

게이트키퍼에서 누락되는 수를 줄이기 위해 NAT 게이트키퍼 기능의 캐시 크기를 늘립니다.

다음 예는 Cisco 라우터에서 게이트키퍼를 조정하는 방법을 보여줍니다. 이 값은 2의 거듭제곱으로 표시되어야 합니다. 그렇지 않으면 값이 자동으로 다음으로 낮은 크기로 설정됩니다.

```
Router(config)# ip nat service gatekeeper
Router(config)# ip nat settings gatekeeper-size 65536
```

참고: 캐시 크기를 조정하면 QFP 내의 메모리 비용이 발생할 수 있으므로 사용을 최적화합니다. 이 값을 점진적으로 조정하여 기본 설정에 가장 가까운 값으로 시작합니다.

설명된 솔루션 중 하나를 수행한 후에는 문제가 해결되었는지 확인하기 위해 다음 두 매개변수를 모니터링하는 것이 좋습니다.

1. QFP 사용률이 감소했는지 확인합니다.
2. 누락 수가 계속 증가하지 않는지 확인합니다.

요약

NAT 게이트키퍼 기능은 NATed 인터페이스에 비 NATed 흐름이 있을 때 라우터의 성능을 향상시킬 수 있습니다. 이는 일반적으로 비 NAT된 흐름이 동일한 인터페이스를 통과하는 동시에 NAT가 일부 NAT된 흐름을 변환할 때 발생합니다. 대부분의 환경에서 NAT 게이트키퍼 기능은 라우터에 영향을 미치지 않습니다. 그러나 부작용을 피하기 위해 필요하다면 이 기능을 신중하게 조정하는 것이 중요합니다.

관련 정보

- ASR1K NAT가 간헐적으로 일부 패킷을 변환하지 못함
- Cisco IOS XE Datapath 패킷 추적 기능으로 문제 해결
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.