IOS-XE NAT 간헐적 오류 트러블슈팅으로 일부 패킷 변환

목차

[소개](#)

[배경 정보](#)

[영향을 받는 플랫폼](#)

[우회되는 NAT 데모](#)

- [비 NAT-ed 목적지로 트래픽 흐름](#)
- [NAT 기반 대상을 전송하려는 동일한 소스의 트래픽](#)
- [NAT-ed 트래픽 복원](#)

[문제의 예](#)

[해결 방법/수정](#)

- [해결 방법 1](#)
- [해결 방법 2](#)
- [해결 방법 3](#)

[요약](#)

[참조](#)

소개

이 문서에서는 Cisco IOS XE Router에서 NAT를 우회하여 잠재적으로 트래픽 장애를 유발하는 변환되지 않은 패킷에 대해 설명합니다.

배경 정보

소프트웨어 버전 12.2(33)XND에서는 NAT(Network Address Translation) 게이트키퍼라는 기능이 기본적으로 도입되어 활성화되어 있습니다. NAT 게이트키퍼는 비 NAT 대상 플로우가 과도한 CPU를 사용하여 NAT 변환을 생성하는 것을 방지하도록 설계되었습니다. 이를 위해 소스 주소를 기반으로 두 개의 소형 캐시(in2out 방향용 캐시 하나와 out2in 방향용 캐시 하나)가 생성됩니다. 각 캐시 엔트리는 소스 주소, VRF(virtual routing and forwarding) ID, 타이머 값(10초 후 엔트리를 무효화하는 데 사용됨) 및 프레임 카운터로 구성됩니다. 테이블에 캐시를 구성하는 256개의 항목이 있습니다. 일부 패킷에는 NAT가 필요하고 일부는 필요하지 않은 동일한 소스 주소에서 여러 트래픽 흐름이 발생하는 경우 패킷이 NAT-ed 상태가 되지 않고 라우터를 통해 변환되지 않을 수 있습니다. Cisco에서는 가능한 한 동일한 인터페이스에서 NAT-ed 및 비-NAT-ed 플로우를 사용하지 않는 것이 좋습니다.

✎ 참고: 이 기능은 H.323과 무관합니다.

영향을 받는 플랫폼

- ISR1K
- ISR4K
- C8200
- C830
- C850

우회되는 NAT 데모

이 섹션에서는 NAT 게이트키퍼 기능으로 인해 NAT를 우회하는 방법에 대해 설명합니다. 다이어그램을 자세히 검토합니다. 소스 라우터, ASA(Adaptive Security Appliance) 방화벽, ASR1K 및 대상 라우터가 있습니다.

비 NAT-ed 목적지로 트래픽 흐름

1. Ping은 소스에서 시작됩니다. 소스: 172.17.250.201 대상: 198.51.100.11.
2. 패킷이 소스 주소 변환을 수행하는 ASA의 내부 인터페이스에 도착합니다. 이제 패킷에 Source(소스): 203.0.113.231 Destination(대상): 198.51.100.11이 있습니다.
3. 패킷이 NAT 외부-내부 인터페이스의 ASR1K에 도착합니다. NAT 변환은 목적지 주소에 대한 변환을 찾지 않으므로 게이트키퍼 "out" 캐시가 소스 주소 203.0.113.231로 채워집니다.
4. 패킷이 대상에 도착합니다. 목적지는 ICMP(Internet Control Message Protocol) 패킷을 수락하고 ICMP ECHO Reply를 반환하여 ping에 성공합니다.

NAT 기반 대상을 전송하려는 동일한 소스의 트래픽

1. .Ping은 소스: 172.17.250.201 대상: 198.51.100.9에서 시작됩니다.
2. 패킷이 소스 주소 변환을 수행하는 ASA의 내부 인터페이스에 도착합니다. 이제 패킷에 Source(소스): 203.0.113.231 Destination(대상): 198.51.100.9가 있습니다.
3. 패킷이 NAT 외부-내부 인터페이스의 ASR1K에 도착합니다. NAT는 먼저 소스 및 목적지에 대한 변환을 찾습니다. 검색되지 않으므로 게이트키퍼 "out" 캐시를 확인하고 소스 주소 203.0.113.231을 찾습니다. (잘못) 패킷이 변환이 필요하지 않다고 가정하고 대상에 대한 경로가 있거나 패킷을 삭제하는 경우 패킷을 전달합니다. 어느 쪽이든 패킷이 원하는 대상에 도달하지 않습니다.

NAT-ed 트래픽 복원

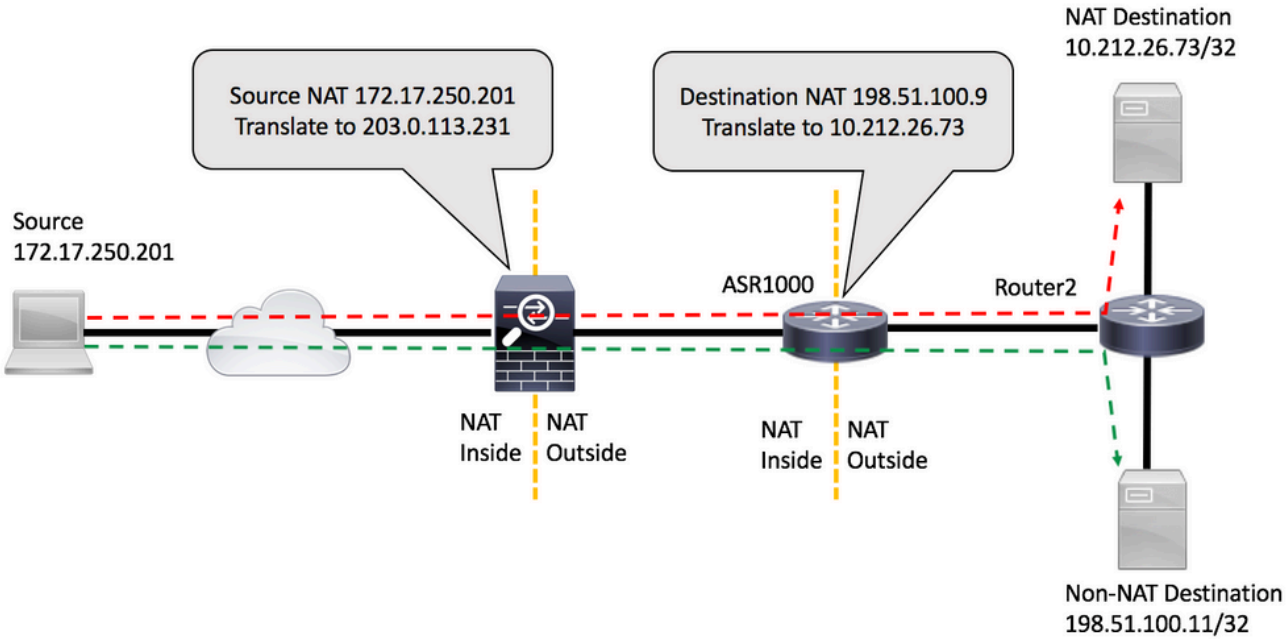
1. 10초 후 소스 주소 203.0.113.231의 항목이 게이트키퍼 출력 캐시에서 시간 초과됩니다.

   참고: 이 항목은 캐시에 여전히 물리적으로 존재하지만 만료되었으므로 사용되지 않습니다.

2. 동일한 소스 172.17.250.201이 NAT 지원 대상 198.51.100.9로 전송하는 경우 패킷이 ASR1K의 out2in 인터페이스에 도착하면 변환을 찾을 수 없습니다. 게이트키퍼 아웃 캐시를 선택하면 활성 항목을 찾을 수 없으므로 대상에 대한 변환을 생성하고 패킷이 예상대로 흐름

니다.

3. 비활성화로 인해 변환이 시간 초과되지 않는 한 이 흐름의 트래픽은 계속 진행됩니다. 그 동안 소스가 비 NAT 기반 대상으로 트래픽을 다시 전송하면 캐시에서 다른 항목이 게이트키퍼에 채워집니다. 그러면 설정된 세션에 영향을 주지 않지만, 동일한 소스에서 NAT 기반 대상으로의 새 세션이 실패하는 10초 기간이 있습니다.



문제의 예

1. Ping은 소스 라우터에서 시작됩니다. 소스: 172.17.250.201 대상: 198.51.100.9. Ping은 2회 반복 횟수[FLOW1]로 실행됩니다.
2. 그런 다음 ASR1K에서 NAT를 지원하지 않는 다른 대상을 ping합니다. 소스: 172.17.250.201 Destination:198.51.100.11 [FLOW2].
3. 그런 다음 198.51.100.9 [FLOW1]에 더 많은 패킷을 보냅니다. 이 흐름의 처음 몇 패킷은 대상 라우터의 액세스 목록 일치에서 볼 수 있는 것처럼 NAT를 우회합니다.

<#root>

```
source#
```

ping 198.51.100.9 source lo1 rep 2

```
Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
source#ping 198.51.100.9 source lo1 rep 2

Type escape sequence to abort.
Sending 2, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
```

```
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 1/1/1 ms
source#ping 198.51.100.11 source lo1 rep 200000

Type escape sequence to abort.
Sending 200000, 100-byte ICMP Echos to 198.51.100.11, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.
Success rate is 99 percent (3007/3008), round-trip min/avg/max = 1/1/16 ms
source#
```

ping 198.51.100.9 source lo1 rep 10

```
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 198.51.100.9, timeout is 2 seconds:
Packet sent with a source address of 172.17.250.201
...!!!!!!!
Success rate is 70 percent (7/10), round-trip min/avg/max = 1/1/1 ms
source#
```

대상 라우터의 ACL 일치는 변환되지 않은 3개의 패킷을 표시합니다.

<#root>

Router2#

show access-list 199

```
Extended IP access list 199
    10 permit udp host 172.17.250.201 host 198.51.100.9
    20 permit udp host 172.17.250.201 host 10.212.26.73
    30 permit udp host 203.0.113.231 host 198.51.100.9
    40 permit udp host 203.0.113.231 host 10.212.26.73 (4 matches)
    50 permit icmp host 172.17.250.201 host 198.51.100.9
    60 permit icmp host 172.17.250.201 host 10.212.26.73
```

70 permit icmp host 203.0.113.231 host 198.51.100.9 (3 matches) <<<<<<<

```
    80 permit icmp host 203.0.113.231 host 10.212.26.73 (42 matches)
    90 permit udp any any log (2 matches)
    100 permit icmp any any log (4193 matches)
    110 permit ip any any (5 matches)
Router2#
```

ASR1K에서 게이트키퍼 캐시 항목을 확인할 수 있습니다.

<#root>

PRIMARY#

show platform hardware qfp active feature nat datapath gatein

Gatekeeper on
sip 203.0.113.231 vrf 0 cnt 1 ts 0x17ba3f idx 74
sip 10.203.249.226 vrf 0 cnt 0 ts 0x36bab6 idx 218
sip 10.203.249.221 vrf 0 cnt 1 ts 0x367ab4 idx 229

PRIMARY#

show platform hardware qfp active feature nat datapath gateout

Gatekeeper on
sip 198.51.100.11 vrf 0 cnt 1 ts 0x36db07 idx 60
sip 10.203.249.225 vrf 0 cnt 0 ts 0x36bb7a idx 217
sip 10.203.249.222 vrf 0 cnt 1 ts 0x367b7c idx 230

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

기본 옵션은 Cisco IOS® XE를 게이트키퍼 개선 사항이 포함된 버전으로 업그레이드하는 것입니다.

Cisco 버그 ID CSCun06260 XE3.13 게이트키퍼 강화

이러한 개선을 통해 NAT 게이트키퍼는 소스 및 목적지 주소를 캐시할 수 있으며 캐시 크기를 구성할 수 있습니다. 확장 모드를 켜려면 이러한 명령으로 캐시 크기를 늘려야 합니다. 또한 캐시를 모니터링하여 크기를 늘려야 하는지 확인할 수 있습니다.

<#root>

PRIMARY(config)#

ip nat settings gatekeeper-size 1024

PRIMARY(config)#

end

확장 모드는 다음 명령을 확인하여 확인할 수 있습니다.

<#root>

PRIMARY#

show platform hardware qfp active feature nat datapath gatein

Gatekeeper on

sip 10.203.249.221 dip 10.203.249.222 vrf 0 ts 0x5c437 idx 631

PRIMARY#

show platform hardware qfp active feature nat datapath gateout

Gatekeeper on

sip 10.203.249.225 dip 10.203.249.226 vrf 0 ts 0x5eddf idx 631

PRIMARY#

show platform hardware qfp active feature nat datapath gatein active

Gatekeeper on

ext mode Size 1024

, Hits 2, Miss 4, Aged 0 Added 4 Active 1

PRIMARY#

show platform hardware qfp active feature nat datapath gateout active

Gatekeeper on

ext mode Size 1024

, Hits 0, Miss 1, Aged 1 Added 2 Active 0

해결 방법 2

Cisco 버그 ID CSCun06260에 대한 수정 사항이 없는 릴리스의 경우, 유일한 옵션은 게이트키퍼 기능을 끄는 것입니다. 유일한 부정적 영향은 비 NAT 기반 트래픽의 성능이 약간 저하되고 QFP(Quantum Flow Processor)의 CPU 사용률이 높아지는 것입니다.

<#root>

PRIMARY(config)#

no ip nat service gatekeeper

PRIMARY(config)#

```
end

PRIMARY#PRIMARY#
Sh platform hardware qfp active feature nat datapath gatein

Gatekeeper off
PRIMARY#
```

다음 명령을 사용하여 QFP 활용률을 모니터링할 수 있습니다.

<#root>

```
show platform hardware qfp active data utilization summary

show platform hardware qfp active data utilization qfp 0
```

해결 방법 3

NAT 패킷과 비 NAT 패킷이 동일한 인터페이스에 도착하지 않도록 트래픽 흐름을 구분합니다.

요약

NAT 게이트키퍼 명령을 도입하여 NAT가 아닌 플로우에 대한 라우터의 성능을 향상했습니다. 일부 조건에서 이 기능은 NAT 패킷과 비 NAT 패킷이 동일한 소스에서 수신될 때 문제를 일으킬 수 있습니다. 향상된 게이트키퍼 기능을 사용하거나, 사용할 수 없는 경우 게이트키퍼 기능을 비활성화하는 것이 해결책입니다.

참조

게이트키퍼를 끌 수 있는 소프트웨어 변경 사항:
Cisco 버그 ID CSCty67184 ASR1k NAT CLI - 게이트키퍼 On/Off
Cisco 버그 ID CSCth23984 nat 게이트키퍼 기능을 설정/해제하기 위한 cli 기능 추가

NAT 게이트키퍼 개선
Cisco 버그 ID CSCun06260 XE3.13 게이트키퍼 강화

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.