Nexus 9300의 NAT 이해

목차

소개

이 문서에서는 NX-OS 소프트웨어를 실행하는 Cisco Cloud-Scale ASIC가 장착된 Nexus 9000 스위치의 NAT 기능에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 설명된 정보를 계속 진행하기 전에 Cisco Nexus 운영 체제(NX-OS) 및 기본 Nexus 아키텍처에 대해 잘 아는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- N9K-C93180YC-FX3
- nxos64-cs.10.4.3.F

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.

N9K에서 NAT 지원 소개

용어

- NAT - NAT는 네트워킹에서 IP 패킷의 소스 또는 목적지 IP 주소를 수정하는 데 사용되는 기술입니다.
- PAT - "Overloading NAT"라고도 하는 포트 주소 변환, 여러 내부 IP 주소가 단일 외부 IP 주소를 공유하며 고유한 포트 번호로 구분됩니다.
- TCP 인식 NAT - TCP 인식 NAT 지원을 통해 NAT 흐름 항목이 TCP 세션의 상태와 일치하고 그에 따라 생성 및 삭제됩니다.

NAT TCAM 리소스

기본적으로 Nexus 9000의 NAT 기능에는 TCAM 항목이 할당되지 않습니다. 다른 기능의 TCAM 크기를 줄여 NAT 기능의 TCAM 크기를 할당해야 합니다.

NAT 작업에는 세 가지 유형의 TCAM이 포함됩니다.

- NAT 영역

NAT는 IP 주소 또는 포트를 기반으로 패킷 일치를 위해 TCAM NAT 영역을 활용합니다.

내부 또는 외부 소스 주소에 대한 각 NAT/PAT 항목에는 2개의 NAT TCAM 항목이 필요합니다.

기본적으로 ACL atomic 업데이트 모드가 활성화되며, Non-Atomic 스케일 번호의 60%가 지원됩니다.

- TCP 인식 영역

"x" ace가 있는 각 NAT 내부 정책에는 "x" 개수의 항목이 필요합니다.

구성된 각 NAT 풀에는 하나의 엔트리가 필요합니다.

atomic 업데이트 모드가 활성화된 경우 TCP-NAT TCAM 크기를 두 배로 늘려야 합니다.

- NAT 재작성 테이블

NAT 재작성 및 번역 현재 저장됨 에서 이 "NAT 재작성 표," 어떤 있음 외부 의 이 NAT TCAM 지역입니다. 이 'NAT 재작성 표' 이(가) a 고정 크기 의 2048 항목 대상: 넥서스 9300-EX/FX/FX2/9300C

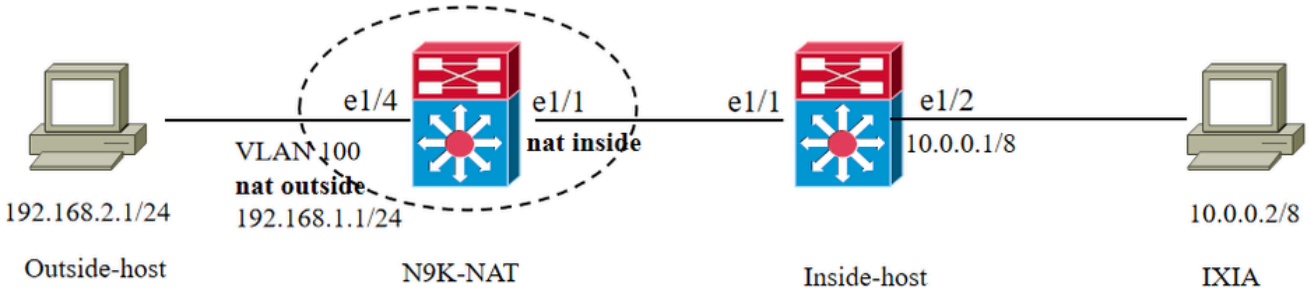
및 4096 항목 대상: 넥서스 9300-FX3/GX/GX2A/GX2B/H2R/H1. 이 테이블 이(가) 독점적으로 used 대상: NAT 번역.

내부 또는 외부 소스 주소에 대한 각 고정 NAT/PAT 항목에는 하나의 "NAT 재작성 테이블" 항목이 필요합니다.

Nexus 9000의 TCAM에 대한 자세한 내용은 Classification TCAM with Cisco CloudScale ASICs for Nexus 9000 Series Switches 백서

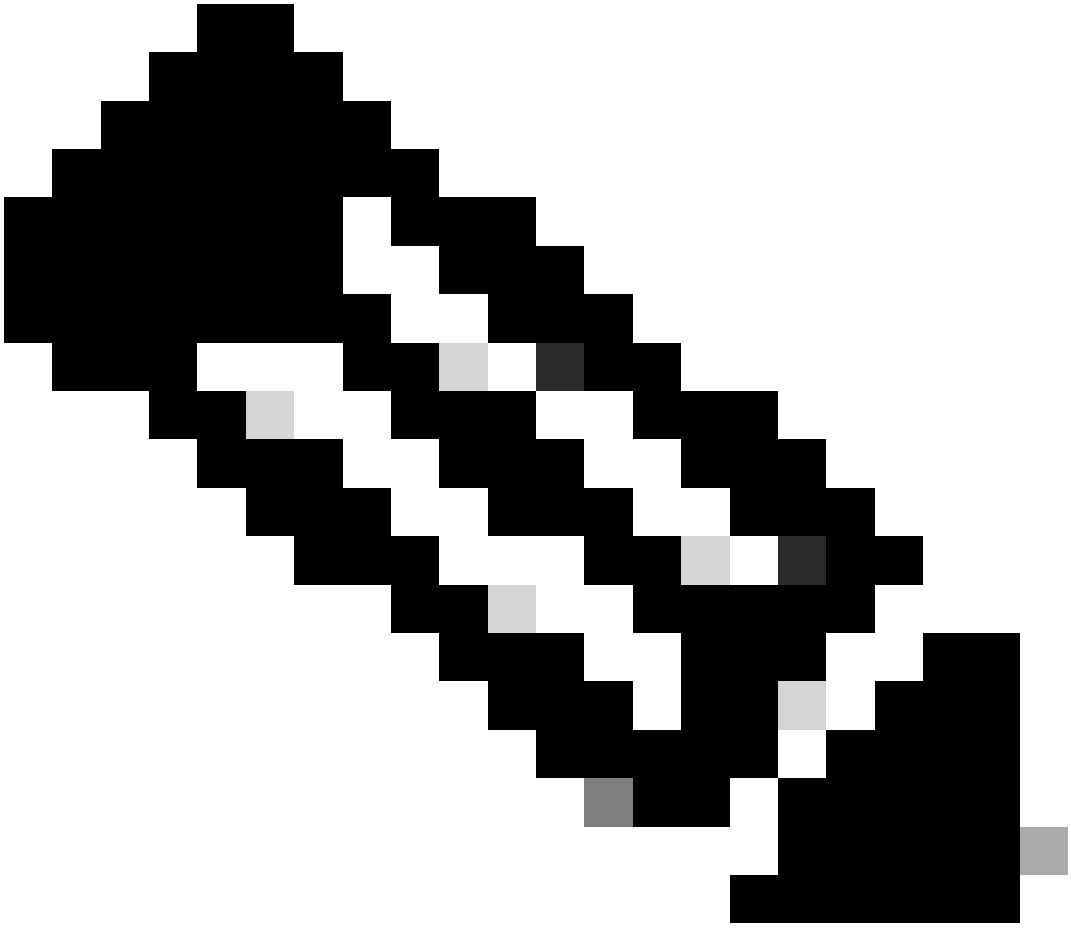
구성 및 확인

토폴로지



N9K-NAT 컨피그레이션

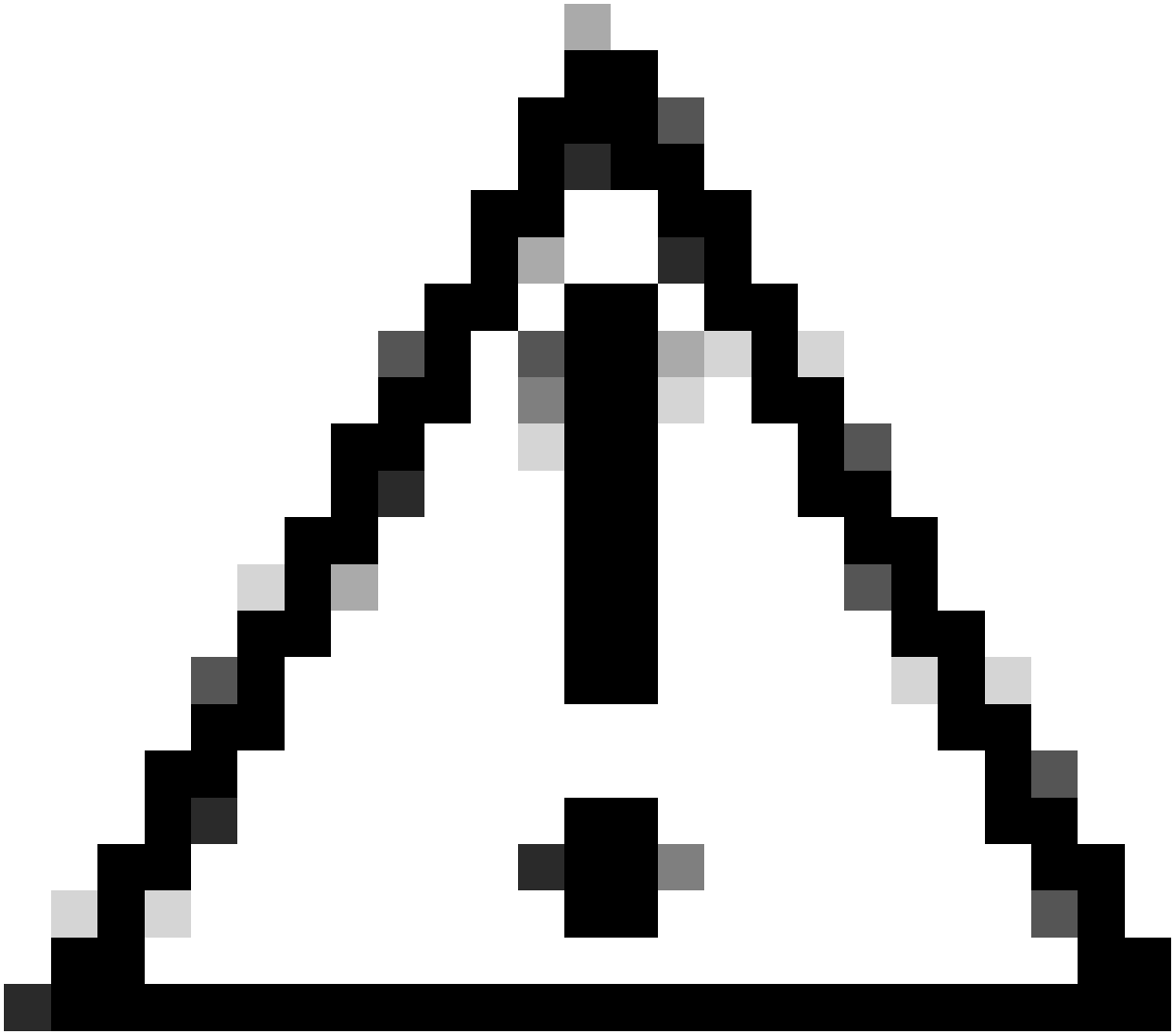
hardware access-list tcam region nat 1024 hardware access-list tcam region tcp-nat 100 ip nat translation max-entries 80



참고: 기본적으로 dynamic nat translation max-entries는 80입니다.

---

ip access-list TEST-NAT 10 permit ip 10.0.0.1/8 192.168.2.1/24 ip nat pool TEST 192.168.1.10 192.168.1.10 netmask 255.255.255.0 ip nat inside source list TEST-NAT pool TEST overload



주의: 내부 정책에 대한 인터페이스 오버로드 옵션은 외부 및 내부 정책에 대한 Cisco Nexus 9200, 9300-EX, 9300-FX 9300-FX2, 9300-FX3, 9300-FXP 및 9300-GX 플랫폼 스위치에서 지원되지 않습니다

interface Vlan100 no shutdown ip address 192.168.1.1/24 ip nat outside

interface Vlan100 no shutdown ip address 192.168.1.1/24 ip nat outside

확인

내부 호스트 Ping

데이터 패킷의 소스 IP: 10.0.0.1 IP로 변환: 192.168.1.10

대상 IP: 192.168.2.1

Inside-host# ping 192.168.2.1 source 10.0.0.1 PING 192.168.2.1 (192.168.2.1): 56 data bytes 64 bytes from 192.168.2.1: icmp_seq=0 ttl=63 time=0.784 ms 64 bytes from 192.168.2.1: icmp_seq=1 ttl=63 time=0.595 m

NAT 변환 테이블 확인

N9K-NAT# show ip nat translations icmp 192.168.1.10:60538 10.0.0.1:48940 192.168.2.1:0 192.168.2.1:0 icmp 192.168.1.10:60539 10.0.0.1:0 192.168.2.1:0 192.168.2.1:0

NAT 통계

N9K-NAT# show ip nat statistics IP NAT Statistics == Stats Collected since: Tue Sep 3 14:33:01 2024 ---------- Total active translations: 82 / Number of translations active in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or times out. No.Static: 0 / Total number of static translations present in the system. No.Dyn: 82 / Total number of dynamic translations present in the system. No.Dyn-ICMP: 2 ---------- Total expired Translations: 2 SYN timer expired: 0 FIN-RST timer expired: 0 Inactive timer expired: 2 ---------- Total Hits: 10475 / Total number of times the software does a translations table lookup and finds an entry. Total Misses: 184884 / Total number of packet the software dropped Packet. In-Out Hits: 10474 In-Out Misses: 184884 Out-In Hits: 1 Out-In Misses: 0 ---------- Total SW Translated Packets: 10559 / Total number of packets software does the translation. In-Out SW Translated: 10558 Out-In SW Translated: 1 ---------- Total SW Dropped Packets: 184800 / Total number of packet the software dropped Packet. In-Out SW Dropped: 184800 Out-In SW Dropped: 0 Address alloc. failure drop: 0 Port alloc. failure drop: 0 Dyn. Translation max limit drop: 184800 / Total number of packets dropped due to configured maximum number of dynamic translation entry limit reached. (ip nat translation max-entries <1-1023>) ICMP max limit drop: 0 Allhost max limit drop: 0 ---------- Total TCP session established: 0 Total TCP session closed: 0 ---------- NAT Inside Interfaces: 1 Ethernet1/1 NAT Outside Interfaces: 1 Vlan100 ---------- Inside source list: ++++++++++++++++++++ Access list: TEST-NAT RefCount: 82 / Number of current references to this access list. Pool: TEST Overload Total addresses: 1 / Number of addresses in the pool available for translation. Allocated: 1 percentage: 100% Missed: 0

자주 묻는 질문(FAQ)

NAT TCAM이 모두 소진되면 어떻게 됩니까?

TCAM 리소스가 모두 사용되면 오류 로그가 보고됩니다.

2024 Aug 28 13:26:56 N9K-NAT %ACLQOS-SLOT1-2-ACLQOS_OOTR: Tcam resource exhausted: Feature NAT outside [nat-outside] 2024 Aug 28 13:26:56 N9K-NAT %NAT-2-HW_PROG_FAILED: Hardware programming for NAT failed:Sufficient free entries are not available in TCAM bank(3)

최대 항목에 도달하면 어떻게 됩니까?

기본적으로 NAT 변환 max-entries는 80입니다. 동적 NAT 변환 엔트리가 최대 제한을 초과하면 트래픽이 CPU에 펀트되어 오류 로그 및 드롭이 발생합니다.

Ping test failure: Inside-host# ping 192.168.2.1 source 10.0.0.1 count unlimited interval 1 PING 192.168.2.1 (192.168.2.1): 56 data bytes Request 0 timed out N9K-NAT Error log: 2024 Sep 5 15:31:33 N9K-NAT %NETSTACK-2-NAT_MAX_LIMIT: netstack [15386] NAT: Can't create dynamic translations, max limit reached - src:10.0.0.1 dst:192.168.2.1 sport:110 dport:110 Capture file from CPU: N9K-NAT# ethanalyzer local interface inband limit-captured-frames 0 Capturing on 'ps-inb' 15 2024-09-05 15:32:44.899885527 10.0.0.1 → 192.168.2.1 UDP 60 110 → 110 Len=18

일부 NAT 패킷이 CPU에 Punt되는 이유는 무엇입니까?

일반적으로 트래픽이 CPU로 라우팅되는 두 가지 시나리오가 있습니다.

첫 번째는 NAT 항목이 아직 하드웨어에 프로그래밍되지 않은 경우 발생하며, 이때 트래픽은 CPU에서 처리해야 합니다.

빈번한 하드웨어 프로그래밍은 CPU에 부담을 줍니다. 하드웨어에서 NAT 항목을 프로그래밍하는 빈도를 줄이기 위해 NAT는 1초 단위로 변환을 프로그래밍합니다. commandip nat 변환 생성 지연 세션 설정을 지연합니다.

두 번째 시나리오는 TCP 세션 설정의 초기 단계 및 그 종료 상호 작용 중에 처리를 위해 CPU로 전송되는 패킷을 포함합니다.

Nexus 9000에서 프록시 arp 없이 NAT가 작동하는 이유

버전 9.2.X에서 추가된 nat-alias라는 기능이 있습니다. 이 기능은 기본적으로 활성화되어 있으며 NAT ARP 문제를 해결합니다. 수동으로 비활성화하지 않는 한 ip proxy-arp 또는 ip local-proxy-arp를 활성화할 필요가 없습니다.

NAT 디바이스는 IG(Inside Global) 및 OL(Outside Local) 주소를 소유하며, 이러한 주소로 전달되는 ARP 요청에 응답해야 합니다. IG/OL 주소 서브넷이 로컬 인터페이스 서브넷과 일치하면 NAT는 IP 별칭 및 ARP 항목을 설치합니다. 이 경우 디바이스는 ARP 요청에 응답하기 위해 local-proxy-arp를 사용합니다.

주소 범위가 외부 인터페이스와 동일한 서브넷에 있는 경우, 비 별칭 기능은 지정된 NAT 풀 주소 범위에서 모든 변환된 IP에 대한 ARP 요청에 응답합니다.

N9K에서 add-route 인수가 작동하는 방식 및 필수 이유

Cisco Nexus 9200 및 9300-EX, -FX, -FX2, -FX3, -FXP, -GX 플랫폼 스위치에서는 ASIC 하드웨어 제한으로 인해 내부 및 외부 정책 모두에 add-route 옵션이 필요합니다. 이 인수를 사용하여 N9K는 호스트 경로를 추가합니다. 외부에서 내부로 들어오는 TCP NAT 트래픽은 CPU에 punt되며 이 인수 없이 삭제할 수 있습니다.

공격 전:

192.168.1.0/24, ubest/mbest: 1/0, attached *via 192.168.1.1, Vlan100, [0/0], 10:23:08, direct 192.168.1.0/32, ubest/mbest: 1/0, attached *via 192.168.1.0, Null0, [0/0], 10:23:08, broadcast 192.168.1.1/32, ubest/mbest: 1/0, attached *via 192.168.1.1, Vlan100, [0/0],10:23:08, local

이후:

192.168.1.2/32, ubest/mbest: 1/0 *via 10.0.0.2, [1/0], 00:02:48, nat >>route created by NAT feature 10.0.0.2/32, ubest/mbest: 1/0 *via 192.168.100.2, [200/0], 06:06:58, bgp-64700, internal, tag 64710 192.168.1.0/24, ubest/mbest: 1/0, attached *via 192.168.1.1, Vlan100, [0/0], 20:43:08, direct

NAT가 최대 100개의 ICMP 엔트리를 지원하는 이유

일반적으로 ICMP NAT는 구성된 샘플링 시간 제한 및 변환 시간 제한이 만료된 후 시간 초과로 흐릅니다. 그러나 스위치에 있는 ICMP NAT 흐름이 유휴 상태가 되면 구성된 샘플링 시간 초과가 만료되는 즉시 시간 초과됩니다.

Cisco NX-OS Release 7.0(3)I5(2)부터 Cisco Nexus 9300 플랫폼 스위치의 ICMP에 대한 하드웨어 프로그래밍이 도입되었습니다. 따라서 ICMP 항목은 하드웨어에서 TCAM 리소스를 소비합니다. ICMP는 하드웨어에 있으므로 Cisco Nexus 플랫폼 시리즈 스위치의 NAT 변환 최대 한도가 1024로 변경됩니다. 최대 100개의 ICMP 항목은 리소스를 가장 잘 사용할 수 있도록 허용됩니다. 이는 고정되어 있으며 최대 ICMP 엔트리를 조정할 수 있는 옵션이 없습니다.

관련 정보

Cisco Nexus 9000 시리즈 NX-OS 인터페이스 설정 가이드, 릴리스 10.4(x)

Classification TCAM with Cisco CloudScale ASICs for Nexus 9000 Series Switches 백서

Cisco Nexus 9000 Series NX-OS 검증 확장성 가이드

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.