NAT op Nexus 9300 begrijpen

Inhoud

Inleiding

Dit document beschrijft NAT-functie op Nexus 9000 switches die zijn uitgerust met een Cisco Cloud-Scale ASIC die NX-OS-software uitvoert.

Voorwaarden

Vereisten

Cisco raadt u aan bekend te zijn met het Cisco Nexus Operating System (NX-OS) en de basis Nexus-architectuur voordat u doorgaat met de informatie die in dit document wordt beschreven.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- N9K-C93180YC-FX3
- nxos 64-cs.10.4.3.f

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Introduceer NAT-ondersteuning op N9K

Terminologie

- NAT - NAT is een techniek die wordt gebruikt in netwerken om het IP-adres van de bron of de bestemming van IP-pakketten aan te passen.
- PAT - Poortadresomzetting, ook bekend als "Overloading NAT", meerdere interne IP-adressen delen één extern IP-adres, gedifferentieerd naar unieke poortnummers.
- Dankzij TCP Aware NAT - TCP-bewuste NAT-ondersteuning kunnen NAT-flowvermeldingen overeenkomen met de status van TCP-sessies en dienovereenkomstig worden gemaakt en verwijderd.

NAT TCAM-bron

Standaard worden er geen TCAM-vermeldingen toegewezen voor de NAT-functie op Nexus 9000. U moet de grootte TCAM voor de NAT eigenschap toewijzen door de grootte TCAM van andere eigenschappen te verminderen.

Er zijn drie types van TCAM betrokken bij NAT verrichtingen:

- NAT-regio

NAT gebruikt de TCAM NAT-regio voor pakketmatching op basis van IP-adres of poort.

Elke NAT/PAT-ingang voor binnen- of buitenbronadressen vereist twee NAT TCAM-vermeldingen.

Standaard wordt de automatische updatemodus van ACL ingeschakeld en wordt 60% van het aantal niet-atomaire schalen ondersteund.

- TCP-bewuste regio

Voor elke NAT inside policy met "x" azen, is "x" aantal waarden vereist.

Voor elke geconfigureerde NAT-pool is één ingang vereist.

De TCP-NAT TCAM-grootte moet worden verdubbeld wanneer de atomaire update modus is ingeschakeld.

- NAT-herschrijftabel

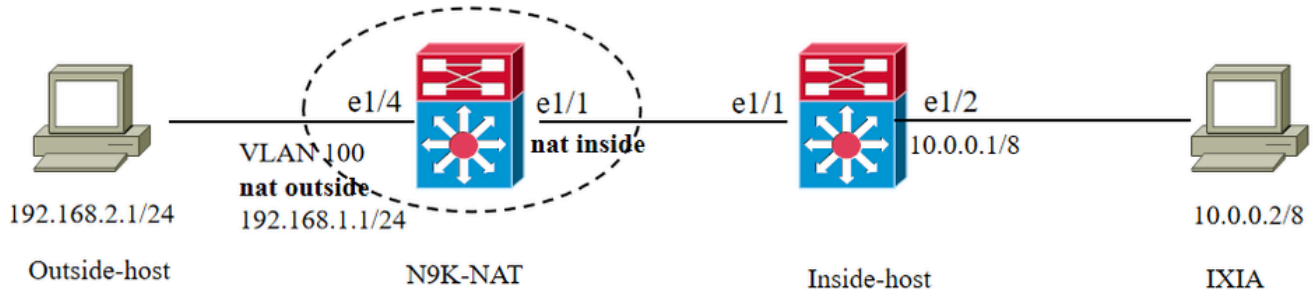
NAT herschrijft en vertalingen zijn opgeslagen in het "NAT Herschrijven Tabel," die bestaat buiten van het NAT TCAM regio. Het "NAT Herschrijven Tabel" heeft a Fixed (Verholpen) grootte van 2048 inzendingen voor Nexus Catalyst 9300-EX/FX2/9300C switch en 4096 inzendingen voor Nexus Nexus 9300-FX3/GX/GX2A/GX2B/H2R/H1. Dit tabel is uitsluitend gebruikt voor NAT vertalingen.

Elke statische NAT/PAT-ingang voor binnen- of buitenbronadressen vereist één "NAT-herschrijftabel"-ingang.

Voor meer informatie over TCAM op Nexus 9000, kunt u verwijzen naar TCAM-classificatie met Cisco CloudScale-ASIC's voor Nexus 9000 Series Switches - Whitepaper.

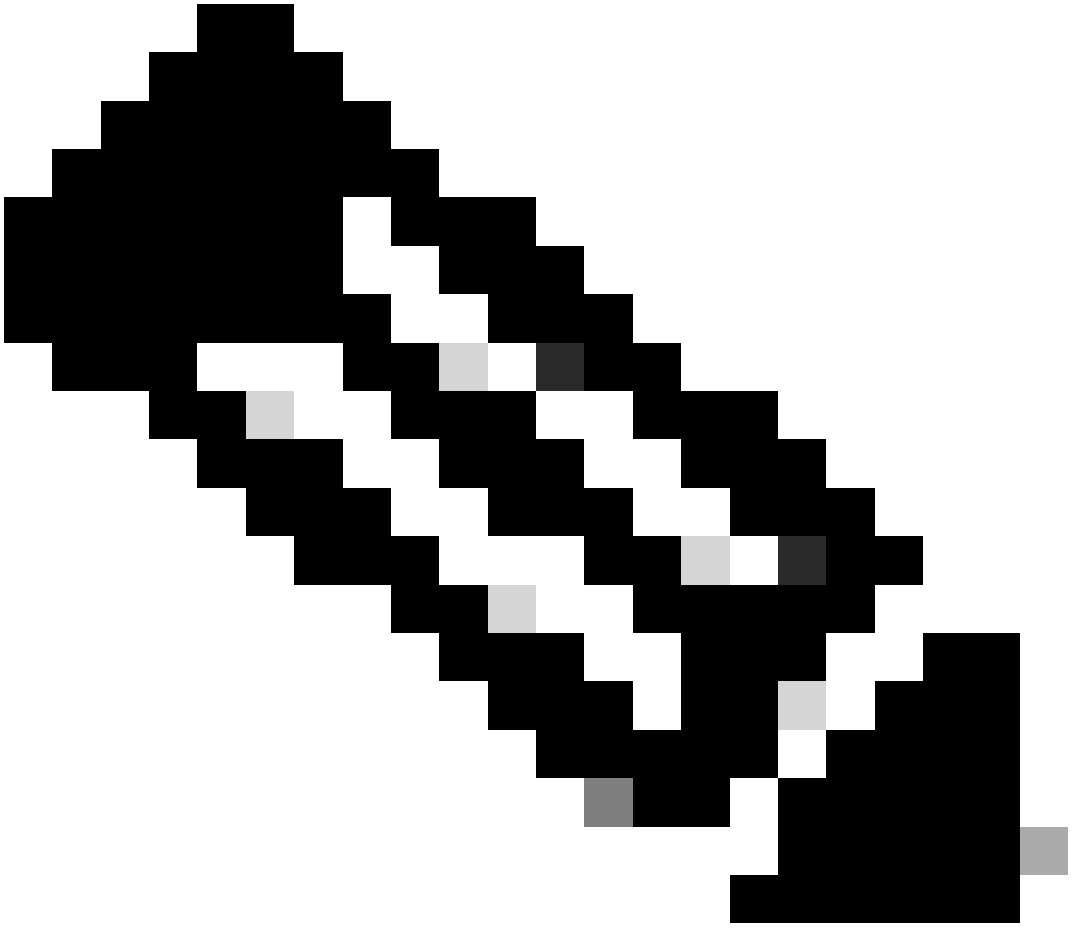
Configuratie en verificatie

Topologie



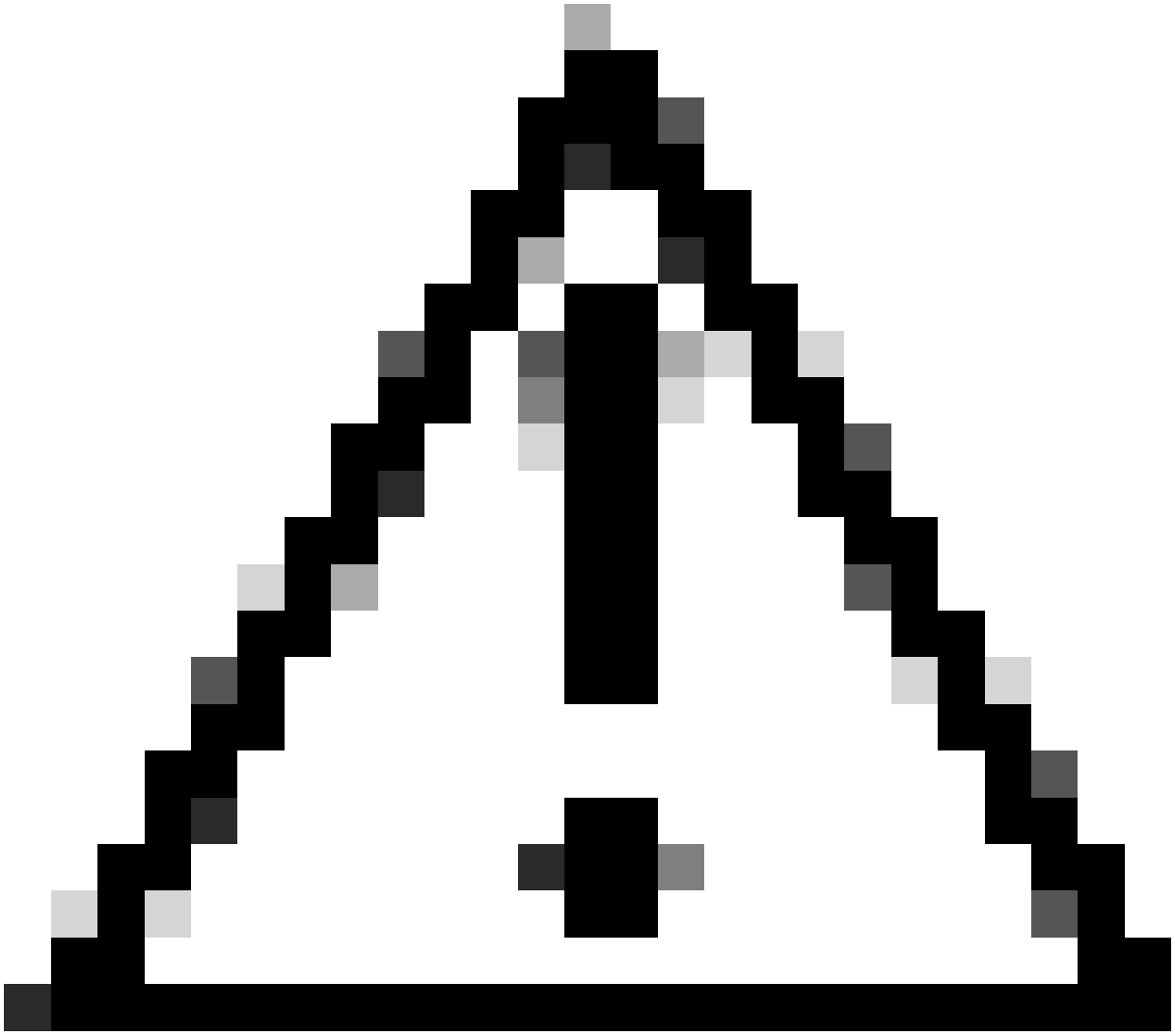
Configuratie N9K-NAT

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



Opmerking: standaard zijn de max-waarden voor dynamische nat-omzetting 80.

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



Let op: de optie voor interfaceoverbelasting voor de optie inside policies wordt niet ondersteund op de Cisco Nexus 9200, 9300-EX, 9300-FX 9300-FX2, 9300-FX3, 9300-FXP en 9300-GX platform switches voor zowel buiten- als binnenkant beleid

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

Verificatie

Inside-host ping

Bron IP van het gegevenspakket: 10.0.0.1 geconverteerd naar IP: 192.168.1.10

IP-bestemming: 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-tabelcontrole voor vertaling

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-statistieken

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

Veelgestelde vragen

Wat gebeurt er als NAT TCAM is uitgeput?

Als de TCAM-bronnen uitgeput zijn, wordt het foutenlogboek weergegeven.

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)

Wat gebeurt er als Max-inzendingen wordt bereikt?

Standaard zijn de max-waarden voor NAT-omzetting 80. Als de dynamische NAT-vertaalvermeldingen de maximumwaarde overschrijden, wordt het verkeer naar de CPU gestraft, wat resulteert in een foutenlogboek en een foutenval.

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

Waarom worden sommige NAT-pakketten gekopieerd naar de CPU?

Normaal gesproken zijn er twee scenario's waarin verkeer naar de CPU wordt geleid.

De eerste gebeurtenis doet zich voor wanneer NAT-items nog niet zijn geprogrammeerd op de hardware, op dit moment moet het verkeer worden verwerkt door de CPU.

Frequente hardwareprogrammering zet de CPU onder druk. Om de frequentie van het programmeren van NAT-vermeldingen in de hardware te verminderen, programmeert NAT vertalingen in batches van één seconde. De opdrachtregel voor het aanmaken van een NAT-vertaling vertraagt het instellen van de sessie.

Het tweede scenario betreft pakketten die naar de CPU worden verzonden voor verwerking tijdens de eerste fase van het instellen van een TCP-sessie en tijdens de beëindiging interacties van die sessie.

Waarom NAT werkt zonder proxy-arp op Nexus 9000?

Er is een functie genaamd nat-alias toegevoegd van versie 9.2.X . Deze eigenschap wordt toegelaten door gebrek en lost NAT ARP kwesties op. Tenzij u het handmatig uitschakelt, hoeft u geen ip proxy-arp of ip local-proxy-arp in te schakelen.

NAT-apparaten hebben Inside Global (IG)- en Outside Local (OL)-adressen en zijn verantwoordelijk voor het reageren op ARP-verzoeken die naar deze adressen worden gestuurd. Wanneer het IG/OL-adressubnet overeenkomt met het lokale interfacesubnet, installeert NAT een IP-alias en een ARP-ingang. In dit geval gebruikt het apparaat een lokale proxy-arp om te reageren op ARP-verzoeken.

De no-alias-functie reageert op ARP-verzoeken voor alle vertaalde IP's uit een gegeven NAT-pooladresbereik als het adresbereik in dezelfde subnetinterface ligt als de buiteninterface.

Hoe werkt add-route Argument op N9K en Waarom is het verplicht?

Op Cisco Nexus 9200 en 9300-EX, -FX, -FX2, -FX3, -FXP, -GX platform switches is de add-route optie vereist voor zowel binnen als buiten beleid vanwege de ASIC-hardwarebeperking. Met dit argument voegt de N9K een hostroute toe. TCP NAT verkeer van buiten naar binnen wordt gestraft naar de CPU en kan zonder dit argument vallen.

Voor:

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

Na:

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

Waarom ondersteunt NAT maximaal 100 ICMP-vermeldingen

Normaal gesproken laat ICMP NAT de tijd uitstromen na het verlopen van de geconfigureerde sampling-time-out en translatietime-out. Als ICMP NAT-stromen in de switch echter inactief worden, wordt de tijd onmiddellijk na het verstrijken van de geconfigureerde bemonsteringstijd uitgezet.

Beginnend met Cisco NX-OS release 7.0(3)I5(2), wordt hardwareprogrammering geïntroduceerd voor ICMP op Cisco Nexus 9300 platform switches. Daarom verbruiken de ICMP-vermeldingen de TCAM-bronnen in de hardware. Omdat ICMP zich in de hardware bevindt, wordt de maximale limiet voor NAT-vertaling in Cisco Nexus platform Series switches gewijzigd in 1024. Maximum aantal 100 ICMP-vermeldingen is toegestaan om de bronnen zo goed mogelijk te gebruiken. Het is vast en er is geen optie om de maximale ICMP-items aan te passen.

Gerelateerde informatie

Configuratiehandleiding voor Cisco Nexus 9000 Series NX-OS-interfaces, release 10.4(x)

TCAM-classificatie met Cisco CloudScale-versterkers voor Nexus 9000 Series Switches - witboek

Cisco Nexus 9000 Series NX-OS geverifieerde schaalbaarheidsgids

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.