NAT verstehen auf Nexus 9300

Inhalt

Einleitung

Dieses Dokument beschreibt die NAT-Funktion auf Nexus 9000-Switches, die mit einem Cisco Cloud-Scale ASIC mit NX-OS-Software ausgestattet sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit dem Cisco Nexus-Betriebssystem (NX-OS) und der grundlegenden Nexus-Architektur vertraut zu machen, bevor Sie mit den in diesem Dokument beschriebenen Informationen fortfahren.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-

Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Einführung von NAT-Unterstützung auf N9K

Terminologie

- NAT - NAT ist eine Technik, die in Netzwerken zum Ändern der Quell- oder Ziel-IP-Adresse von IP-Paketen verwendet wird.
- PAT - Port Address Translation, auch als "Overloading NAT" (NAT überlasten) bezeichnet, verwenden mehrere interne IP-Adressen eine gemeinsame externe IP-Adresse, die sich durch eindeutige Portnummern unterscheidet.
- TCP Aware NAT - Dank der TCP-fähigen NAT-Unterstützung können NAT-Flusseinträge dem Status von TCP-Sitzungen entsprechen und entsprechend erstellt und gelöscht werden.

NAT TCAM-Ressource

Standardmäßig werden für die NAT-Funktion auf dem Nexus 9000 keine TCAM-Einträge zugewiesen. Sie müssen die TCAM-Größe für die NAT-Funktion zuweisen, indem Sie die TCAM-Größe anderer Funktionen reduzieren.

Es gibt drei Arten von TCAMs, die an NAT-Vorgängen beteiligt sind:

- NAT-Region

NAT verwendet die TCAM NAT-Region für den Paketvergleich basierend auf der IP-Adresse oder dem Port.

Jeder NAT/PAT-Eintrag für interne oder externe Quelladressen erfordert zwei NAT-TCAM-Einträge.

Standardmäßig ist der atomische ACL-Aktualisierungsmodus aktiviert. Es werden 60 % der nichtatomischen Skalierungszahlen unterstützt.

- TCP-sensitiver Bereich

Für jede NAT-interne Richtlinie mit "x" Asse ist die "x"-Anzahl von Einträgen erforderlich.

Für jeden konfigurierten NAT-Pool ist ein Eintrag erforderlich.

Die TCP-NAT TCAM-Größe muss verdoppelt werden, wenn der atomare Aktualisierungsmodus aktiviert ist.

- NAT-Umschreibtabelle

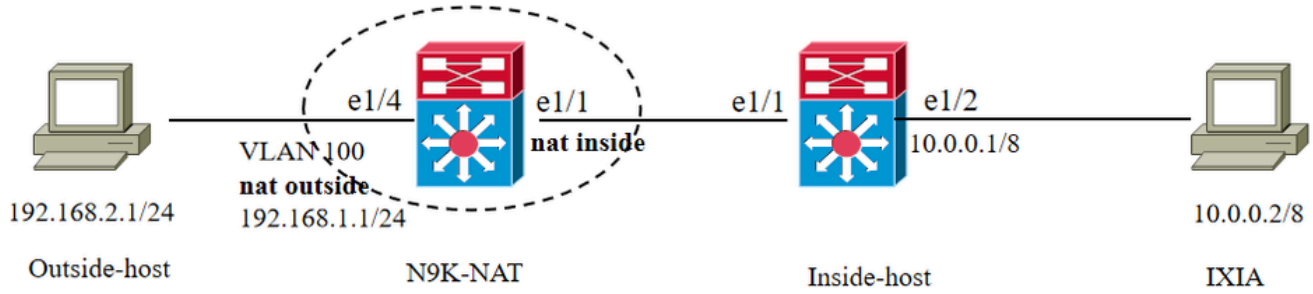
NAT umschreiben und Übersetzungen sind gespeichert in Die Fehlermeldung "NAT Umschreiben Tabelle," die existiert Außen von Die Fehlermeldung NAT TCAM Region. Die Fehlermeldung 'NAT Umschreiben Tabelle' hat a korrigiert Größe von 2048 Einträge für Nexus 9300-EX/FX/FX2/9300C und 4096 Einträge für Nexus 9300-FX3/GX/GX2A/GX2B/H2R/H1 Diese Tisch ist ausschließlich verwendet für NAT Übersetzungen.

Jeder statische NAT/PAT-Eintrag für interne oder externe Quelladressen erfordert einen Eintrag in der "NAT Rewrite Table".

Weitere Informationen zu TCAM auf dem Nexus 9000 finden Sie unter Whitepaper: TCAM-Klassifizierung mit Cisco CloudScale ASICs für Nexus Switches der Serie 9000.

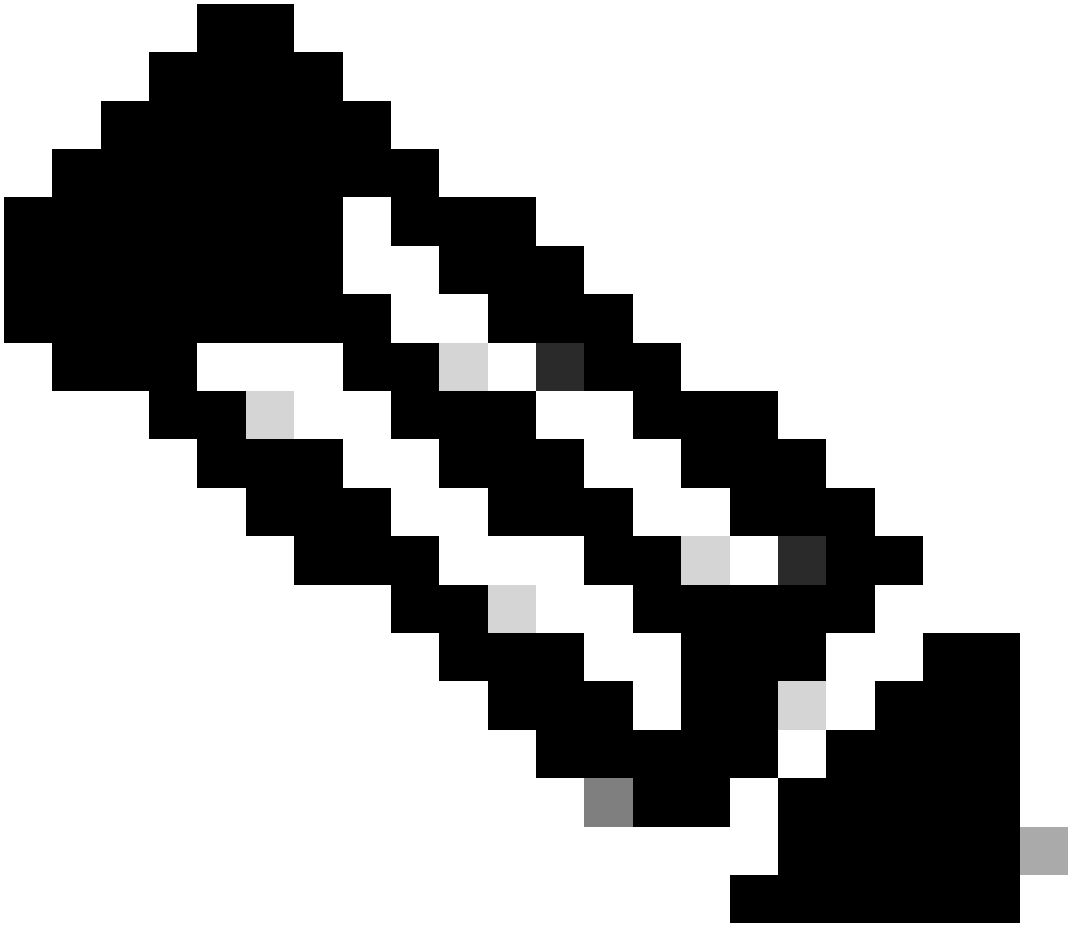
Konfiguration und Verifizierung

Topologie



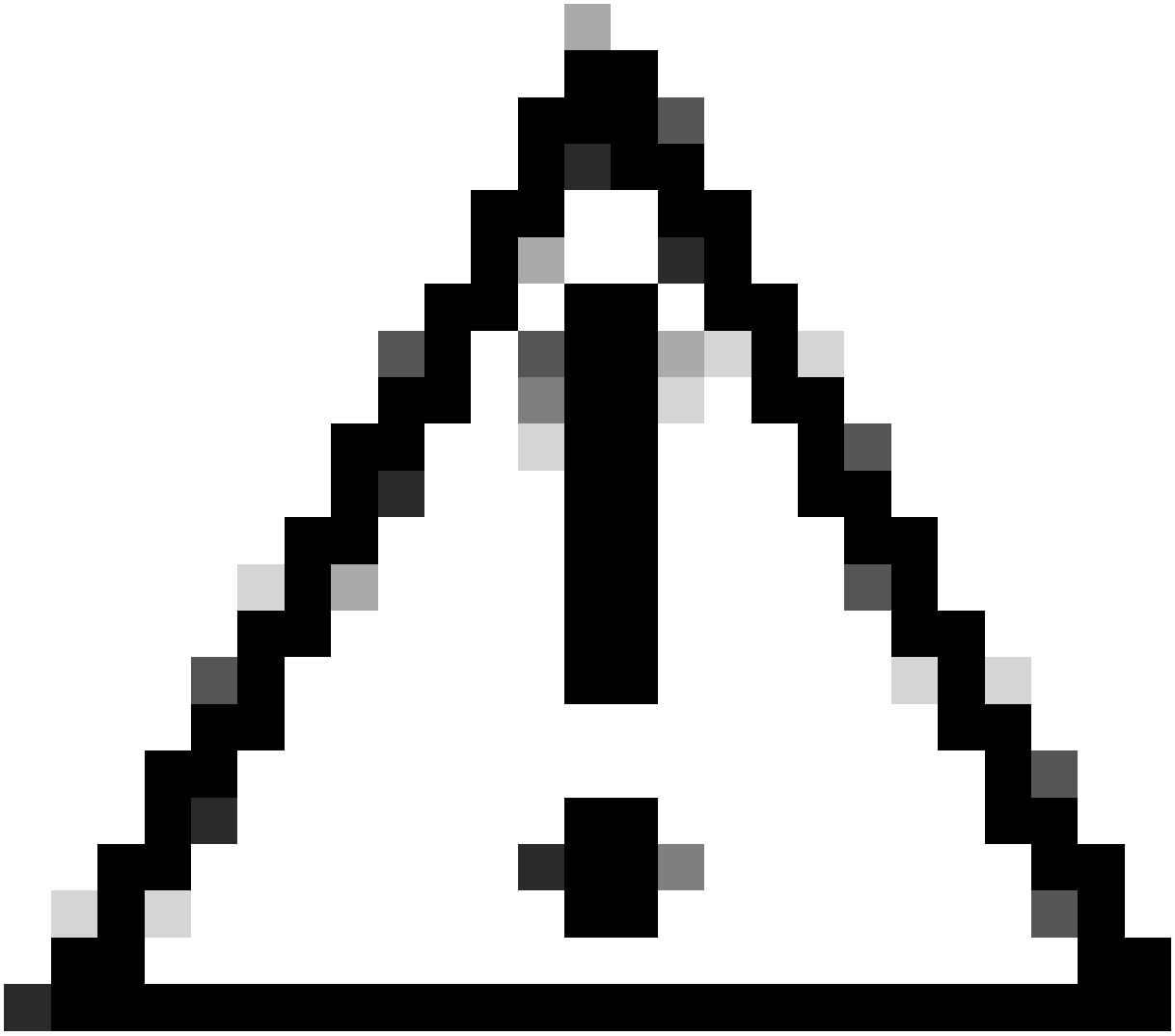
N9K-NAT-Konfiguration

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



Hinweis: Standardmäßig ist die dynamische NAT-Übersetzung "max-entries" 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



Achtung: Die Option zum Überladen der Schnittstelle für interne Richtlinien wird auf dem Cisco Nexus 9200, 9300-EX, 9300-FX 9300-FX2, 9300-FX3, 9300-FXP und 9300-FXP nicht unterstützt. Switches der 300-GX-Plattform für Außen- und Innenrichtlinien

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

Verifizierung

Interner Host-Ping

Quell-IP des Datenpakets: 10.0.0.1 Umwandelt in IP: 192.168.1.10

Ziel-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

Prüfung der NAT-Übersetzungstabelle

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-Statistik

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

Häufig gestellte Fragen

Was geschieht, wenn der NAT TCAM erschöpft ist?

Wenn die TCAM-Ressourcen erschöpft sind, wird das Fehlerprotokoll ausgegeben.

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)

Was passiert, wenn Max-Einträge erreicht werden?

Standardmäßig beträgt die maximale Anzahl von NAT-Einträgen 80. Sobald die Einträge für die dynamische NAT-Übersetzung den maximalen Grenzwert überschreiten, wird der Datenverkehr an die CPU geleitet, wodurch ein Fehlerprotokoll erstellt und gelöscht wird.

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

Warum werden einige NAT-Pakete an die CPU gesendet?

In der Regel gibt es zwei Szenarien, in denen der Datenverkehr an die CPU weitergeleitet wird.

Der erste tritt auf, wenn NAT-Einträge noch nicht auf der Hardware programmiert wurden. Zu diesem Zeitpunkt muss der Datenverkehr von der CPU verarbeitet werden.

Häufige Hardware-Programmierung belastet die CPU. Um die Häufigkeit der Programmierung von NAT-Einträgen in der Hardware zu reduzieren, programmiert NAT die Übersetzungen in Batches mit einer Sekunde. Der Befehl nat translation create-delay verzögert die Sitzungserstellung.

Im zweiten Szenario werden Pakete an die CPU gesendet, die während der Anfangsphase der TCP-Sitzung und während der Terminierungsinteraktionen dieser Sitzung verarbeitet werden.

Warum funktioniert NAT auf Nexus 9000 ohne Proxy-ARP?

Es gibt eine Funktion namens nat-alias, die in Version 9.2.X hinzugefügt wurde. Diese Funktion ist standardmäßig aktiviert und behebt NAT ARP-Probleme. Wenn Sie es nicht manuell deaktivieren, müssen Sie ip proxy-arp oder ip local-proxy-arp nicht aktivieren.

NAT-Geräte besitzen eigene interne globale (IG) und externe lokale (OL) Adressen und sind für die Reaktion auf ARP-Anfragen verantwortlich, die an diese Adressen gerichtet sind. Wenn das IG/OL-Adresssubnetz mit dem Subnetz der lokalen Schnittstelle übereinstimmt, installiert NAT einen IP-Alias und einen ARP-Eintrag. In diesem Fall verwendet das Gerät local-proxy-arp, um auf ARP-Anfragen zu antworten.

Die Funktion ohne Alias reagiert auf ARP-Anfragen für alle übersetzten IPs aus einem bestimmten NAT-Pool-Adressbereich, wenn sich der Adressbereich im gleichen Subnetz befindet wie die externe Schnittstelle.

Wie funktioniert add-route-Argument auf N9K und warum ist es zwingend erforderlich?

Bei den Cisco Nexus Switches der Serien 9200 und 9300-EX, -FX, -FX2, -FX3, -FXP, -GX ist die Add-Routing-Option aufgrund der ASIC-Hardwarebeschränkung sowohl für interne als auch für externe Richtlinien erforderlich. Mit diesem Argument fügt der N9K eine Host-Route hinzu. TCP NAT-Datenverkehr von außen nach innen wird an die CPU gesendet und kann ohne dieses Argument verworfen werden.

Vorher:

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

Nachher:

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

Warum unterstützt NAT maximal 100 ICMP-Einträge?

Normalerweise fließt die ICMP NAT nach Ablauf der konfigurierten Sampling- und Umwandlungs-Zeitüberschreitung eine Zeitüberschreitung. Wenn jedoch die im Switch vorhandenen ICMP NAT-Datenflüsse inaktiv werden, erfolgt unmittelbar nach Ablauf des konfigurierten Sampling-Timeouts eine Zeitüberschreitung.

Ab der Cisco NX-OS-Version 7.0(3)I5(2) wird die Hardwareprogrammierung für ICMP auf Cisco Nexus Switches der Serie 9300 eingeführt. Aus diesem Grund nutzen die ICMP-Einträge die TCAM-Ressourcen in der Hardware. Da sich ICMP in der Hardware befindet, wird der Höchstwert für die NAT-Übersetzung in Switches der Cisco Nexus Plattform in 1024 geändert. Es sind maximal 100 ICMP-Einträge zulässig, um die Ressourcen optimal zu nutzen. Es ist festgelegt, und es gibt keine Option zum Anpassen der maximalen ICMP-Einträge.

Zugehörige Informationen

Konfigurationsleitfaden für die NX-OS-Schnittstellen bei der Cisco Nexus 9000-Serie, Version 10.4(x)

Whitepaper: TCAM-Klassifizierung mit Cisco CloudScale ASICs für Nexus Switches der Serie 9000

Cisco Nexus Serie 9000 - NX-OS - Leitfaden zur verifizierten Skalierbarkeit

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.