Comprendre la NAT sur Nexus 9300

Table des matières

Introduction

Ce document décrit la fonction NAT sur les commutateurs Nexus 9000 équipés d'un ASIC Cisco Cloud-Scale qui exécute le logiciel NX-OS.

Conditions préalables

Exigences

Cisco vous recommande de bien connaître le système d'exploitation Cisco Nexus (NX-OS) et l'architecture de base de Nexus avant de poursuivre avec les informations décrites dans ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Introduction de la prise en charge NAT sur N9K

Terminologie

- NAT : la NAT est une technique utilisée dans les réseaux pour modifier l'adresse IP source ou de destination des paquets IP.
- PAT (Port Address Translation) : traduction d'adresses de port, également appelée « surcharge de la NAT », plusieurs adresses IP internes partagent une adresse IP externe unique, différenciée par des numéros de port uniques.
- NAT compatible TCP : la prise en charge NAT compatible TCP permet aux entrées de flux NAT de correspondre à l'état des sessions TCP et d'être créées et supprimées en conséquence.

Ressource NAT TCAM

Par défaut, aucune entrée TCAM n'est allouée pour la fonctionnalité NAT sur Nexus 9000. Vous devez allouer la taille TCAM pour la fonction NAT en réduisant la taille TCAM des autres fonctions.

Il existe trois types de TCAM impliqués dans les opérations NAT :

- région NAT

La fonction NAT utilise la région NAT TCAM pour la mise en correspondance des paquets en fonction de l’adresse IP ou du port.

Chaque entrée NAT/PAT pour les adresses source internes ou externes nécessite deux entrées NAT TCAM.

Par défaut, mode de mise à jour atomique ACL activé, 60 % du numéro d'échelle non atomique est pris en charge.

- Région sensible au protocole TCP

Pour chaque stratégie NAT interne avec « x » as, un nombre « x » d'entrées est requis.

Pour chaque pool NAT configuré, une entrée est requise.

La taille TCAM TCP-NAT doit être doublée lorsque le mode de mise à jour atomique est activé.

- Table de réécriture NAT

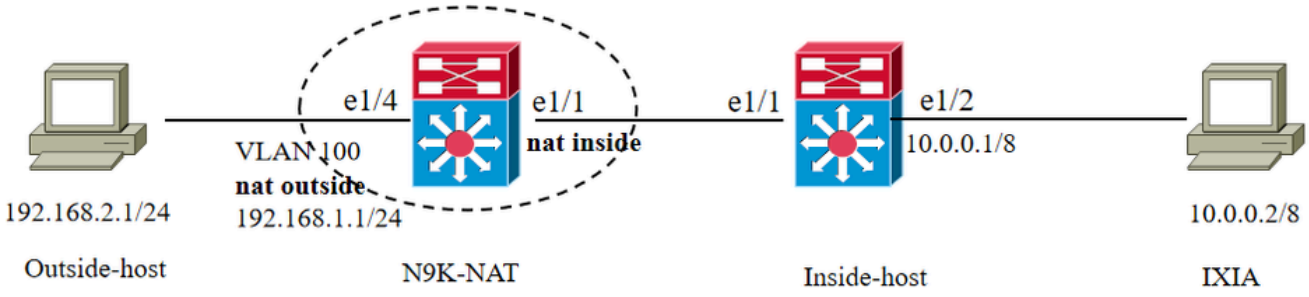
NAT réécritures et traductions sont stocké en les "NAT Réécrire Tableau," qui existe extérieur de les NAT TCAM région. Les 'NAT Réécrire Tableau' a a fixed (corrigé) apprêt de 2048 écritures pour Nexus 9300-EX/FX/FX2/9300C et 4096 écritures pour Nexus 9300-FX3/GX/GX2A/GX2B/H2R/H1. Ceci présenter est exclusivement utilisé pour NAT traductions.

Chaque entrée NAT/PAT statique pour les adresses source internes ou externes nécessite une entrée « Table de réécriture NAT ».

Pour plus d'informations sur la TCAM sur Nexus 9000, vous pouvez consulter Livre blanc sur la classification du TCAM avec les ASIC Cisco CloudScale pour les commutateurs de la gamme Nexus 9000.

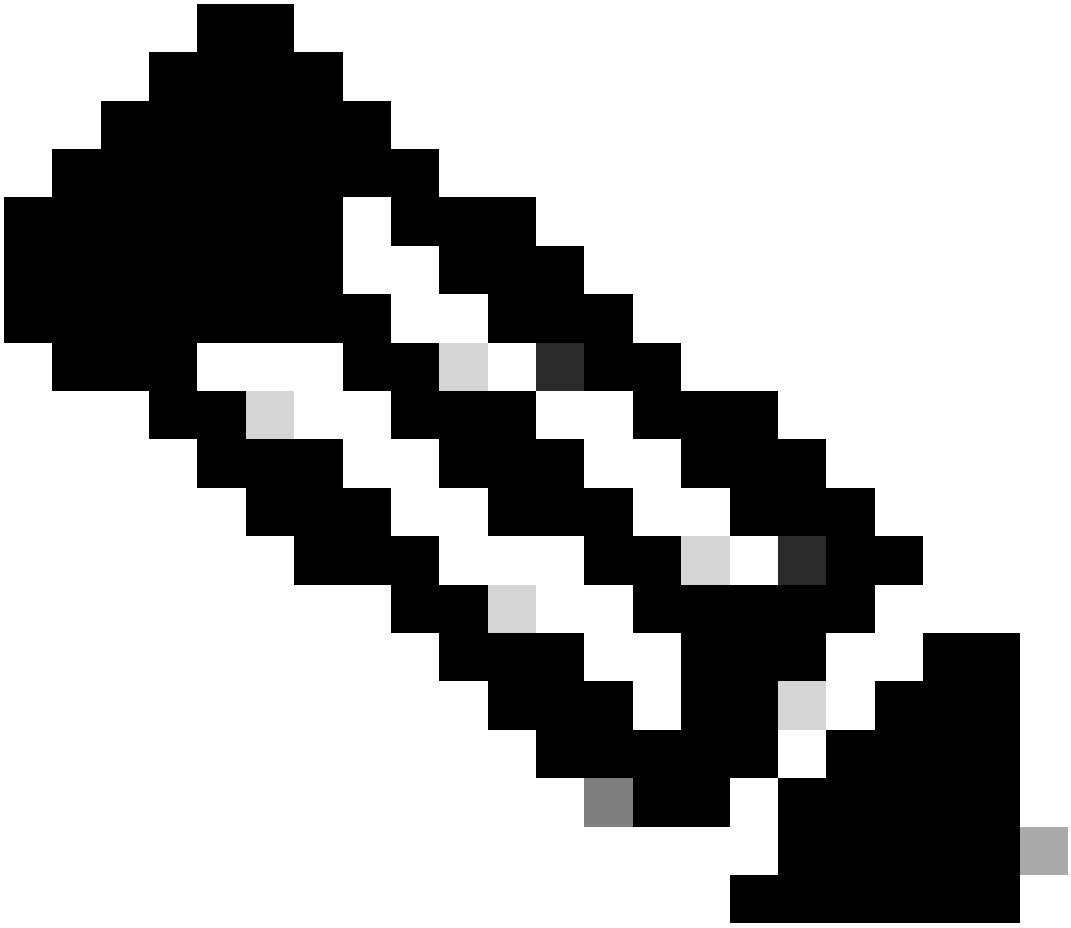
Configuration et vérification

Topologie



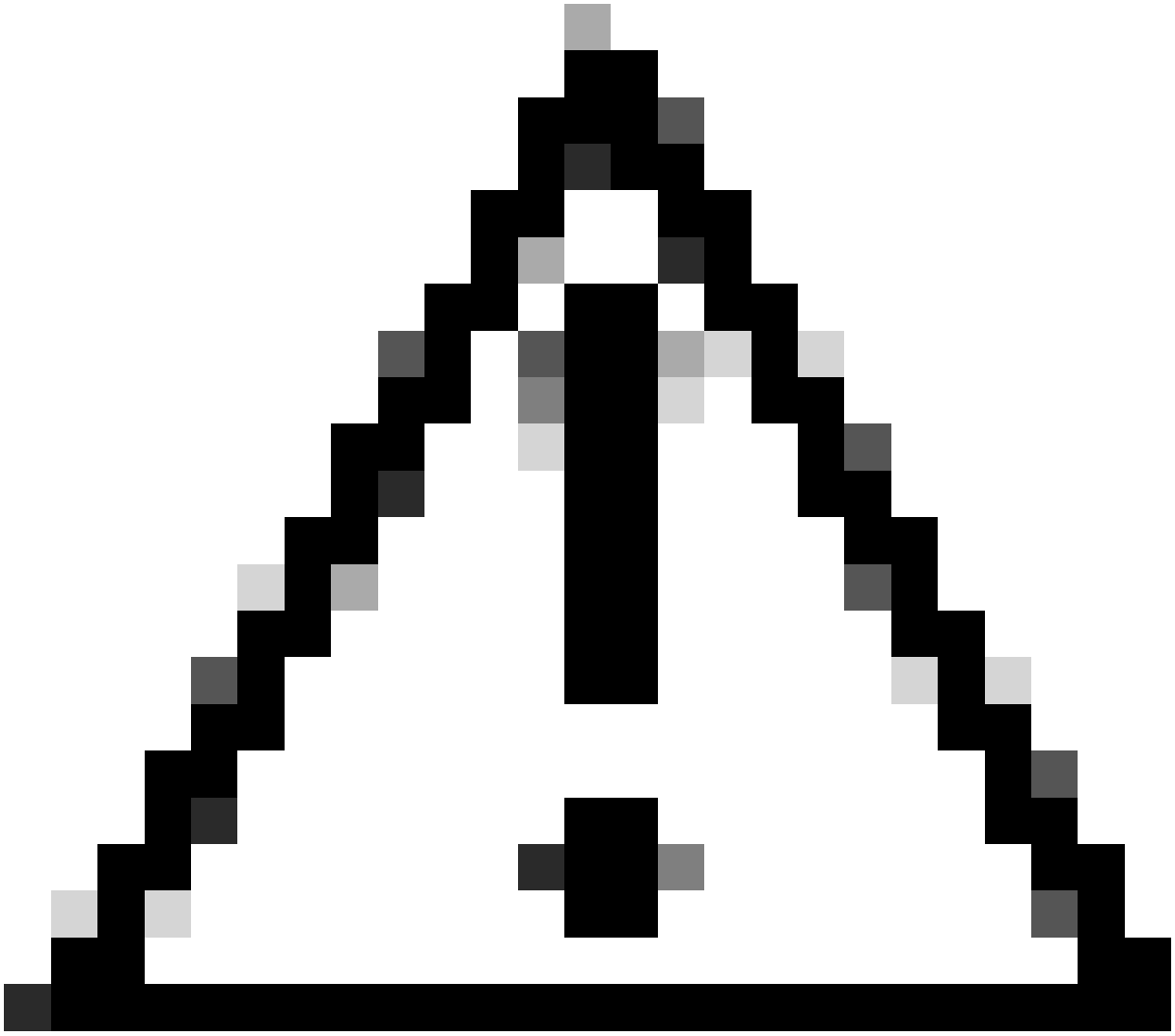
Configuration de N9K-NAT

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



Remarque : par défaut, les entrées max-entries de traduction NAT dynamique sont 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



Attention : l'option de surcharge d'interface pour l'option de politiques internes n'est pas prise en charge sur les commutateurs de plate-forme Cisco Nexus 9200, 9300-EX, 9300-FX 9300-FX2, 9300-FX3, 9300-FXP et 9300-GX pour les politiques internes et externes

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

Vérification

Ping interne à l'hôte

IP source du paquet de données : 10.0.0.1 Converti en IP : 192.168.1.10

Adresse IP de destination : 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

Vérification de la table de traduction NAT

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

Statistiques NAT

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

Forum aux questions

Que se passe-t-il lorsque la TCAM NAT est épuisée ?

Si les ressources TCAM sont épuisées, le journal des erreurs est signalé.

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)

Que se passe-t-il lorsque le nombre maximal d'entrées est atteint ?

Par défaut, la traduction NAT max-entries est 80. Une fois que les entrées de traduction NAT dynamique dépassent la limite maximale, le trafic est dirigé vers le processeur, ce qui entraîne un journal des erreurs et une suppression.

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

Pourquoi certains paquets NAT sont-ils dirigés vers le processeur ?

Normalement, il y a deux scénarios dans lesquels le trafic doit être routé vers le CPU.

La première se produit lorsque les entrées NAT n'ont pas encore été programmées sur le matériel, à ce moment-là le trafic doit être traité par le CPU.

La programmation matérielle fréquente met le processeur à rude épreuve. Pour réduire la fréquence de programmation des entrées NAT dans le matériel, NAT programme les traductions par lots d'une seconde. La commande nat translation creation-delay retarde l'établissement de la session.

Le second scénario implique des paquets qui sont envoyés au CPU pour traitement pendant la phase initiale d'établissement d'une session TCP et pendant les interactions de fin de celle-ci.

Pourquoi NAT fonctionne sans proxy-arp sur Nexus 9000 ?

Une fonctionnalité appelée nat-alias a été ajoutée à partir de la version 9.2.X . Cette fonctionnalité est activée par défaut et résout les problèmes ARP NAT. À moins que vous ne le désactiviez manuellement, vous n'avez pas besoin d'activer ip proxy-arp ou ip local-proxy-arp.

Les périphériques NAT possèdent des adresses globales internes (IG) et locales externes (OL) et sont responsables de répondre à toutes les requêtes ARP dirigées vers ces adresses. Lorsque le sous-réseau d'adresses IG/OL correspond au sous-réseau d'interface local, NAT installe un alias IP et une entrée ARP. Dans ce cas, le périphérique utilise local-proxy-arp pour répondre aux requêtes ARP.

La fonctionnalité no-alias répond aux requêtes ARP pour toutes les adresses IP traduites d'une plage d'adresses de pool NAT donnée si la plage d'adresses se trouve dans le même sous-réseau que l'interface externe.

Comment fonctionne l'argument add-route sur N9K et pourquoi est-il obligatoire ?

Sur les commutateurs de plate-forme Cisco Nexus 9200 et 9300-EX, -FX, -FX2, -FX3, -FXP, -GX, l'option d'ajout de route est requise pour les politiques internes et externes en raison de la limitation matérielle ASIC. Avec cet argument, le N9K ajoute une route hôte. Le trafic NAT TCP de l'extérieur vers l'intérieur est envoyé au processeur et peut être abandonné sans cet argument.

Avant :

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

Après :

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

Pourquoi NAT prend-il en charge un maximum de 100 entrées ICMP ?

Normalement, les flux NAT ICMP expirent après l'expiration des délais d'échantillonnage et de traduction configurés. Cependant, lorsque les flux NAT ICMP présents dans le commutateur deviennent inactifs, ils expirent immédiatement après l'expiration du délai d'échantillonnage configuré.

À partir de la version 7.0(3)I5(2) de Cisco NX-OS, la programmation matérielle est introduite pour ICMP sur les commutateurs de la plate-forme Cisco Nexus 9300. Par conséquent, les entrées ICMP consomment les ressources TCAM dans le matériel. Étant donné que le protocole ICMP se trouve dans le matériel, la limite maximale pour la traduction NAT dans les commutateurs de la gamme de plates-formes Cisco Nexus passe à 1024. Un maximum de 100 entrées ICMP est autorisé pour optimiser l'utilisation des ressources. Elle est fixe et il n'y a pas d'option pour ajuster les entrées ICMP maximales.

Informations connexes

Guide de configuration des interfaces NX-OS de Cisco Nexus série 9000, version 10.4(x)

Livre blanc sur la classification du TCAM avec les ASIC Cisco CloudScale pour les commutateurs de la gamme Nexus 9000

Guide d'évolutivité vérifié du NX-OS de la gamme Cisco Nexus 9000

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.