Información sobre NAT en Nexus 9300

Contenido

Introducción

Este documento describe la función NAT en los switches Nexus 9000 equipados con un ASIC a escala de nube de Cisco que ejecuta el software NX-OS.

Prerequisites

Requirements

Cisco recomienda que esté familiarizado con el sistema operativo Cisco Nexus (NX-OS) y la arquitectura básica de Nexus antes de continuar con la información que se describe en este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Introducir compatibilidad con NAT en N9K

Terminology

- NAT: técnica utilizada en la conexión en red para modificar la dirección IP de origen o de destino de los paquetes IP.
- PAT: traducción de direcciones de puerto, también conocida como "NAT de sobrecarga", las direcciones IP internas múltiples comparten una sola dirección IP externa, diferenciada por números de puerto únicos.
- NAT con reconocimiento de TCP: la compatibilidad con NAT con reconocimiento de TCP permite que las entradas de flujo de NAT coincidan con el estado de las sesiones de TCP y se creen y eliminen en consecuencia.

Recurso NAT TCAM

De forma predeterminada, no se asignan entradas TCAM para la función NAT en Nexus 9000. Debe asignar el tamaño de TCAM para la función NAT reduciendo el tamaño de TCAM de otras funciones.

Hay tres tipos de TCAM involucrados en las operaciones de NAT:

- región NAT

NAT utiliza la región TCAM NAT para la coincidencia de paquetes basada en la dirección IP o el puerto.

Cada entrada NAT/PAT para direcciones de origen internas o externas requiere dos entradas NAT TCAM.

De forma predeterminada, el modo de actualización atómica de ACL está habilitado, y se admite el 60% del número de escala no atómica.

- región con reconocimiento de TCP

Para cada política interna de NAT con "x" ases, se requiere el número "x" de entradas.

Para cada conjunto NAT configurado, se requiere una entrada.

El tamaño de TCP-NAT TCAM debe duplicarse cuando el modo de actualización atómica está habilitado.

- Tabla de reescritura de NAT

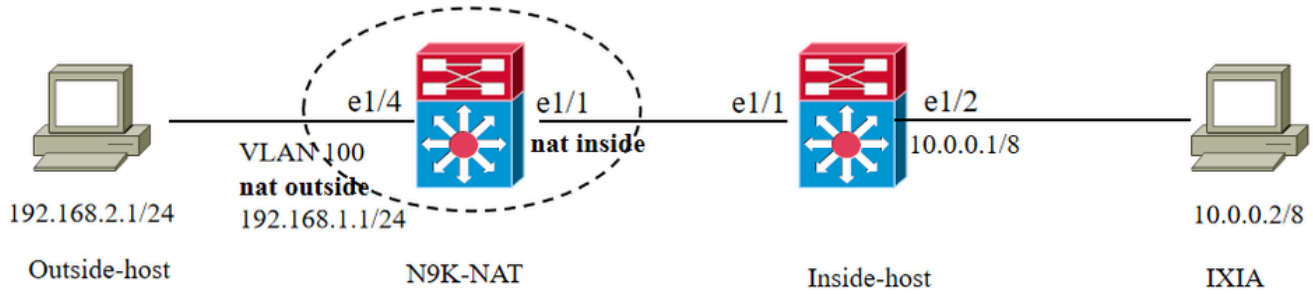
NAT reescribe y traducciones son almacenado in "NAT Reescribir Tabla," que existe fuera de NAT TCAM región. 'NAT Reescribir Tabla' tiene a fijas tamaño de 2048 entradas para Nexus 9300-EX/FX/FX2/9300C y 4096 entradas para Nexus 9300-FX3/GX/GX2A/GX2B/H2R/H1. Esto tabla es exclusivamente usado para NAT traducciones.

Cada entrada NAT/PAT estática para direcciones de origen internas o externas requiere una entrada "Tabla de reescritura de NAT".

Para obtener más información sobre TCAM en Nexus 9000, puede consultar Informe técnico sobre clasificación de TCAM con ASIC de Cisco CloudScale para switches Nexus serie 9000.

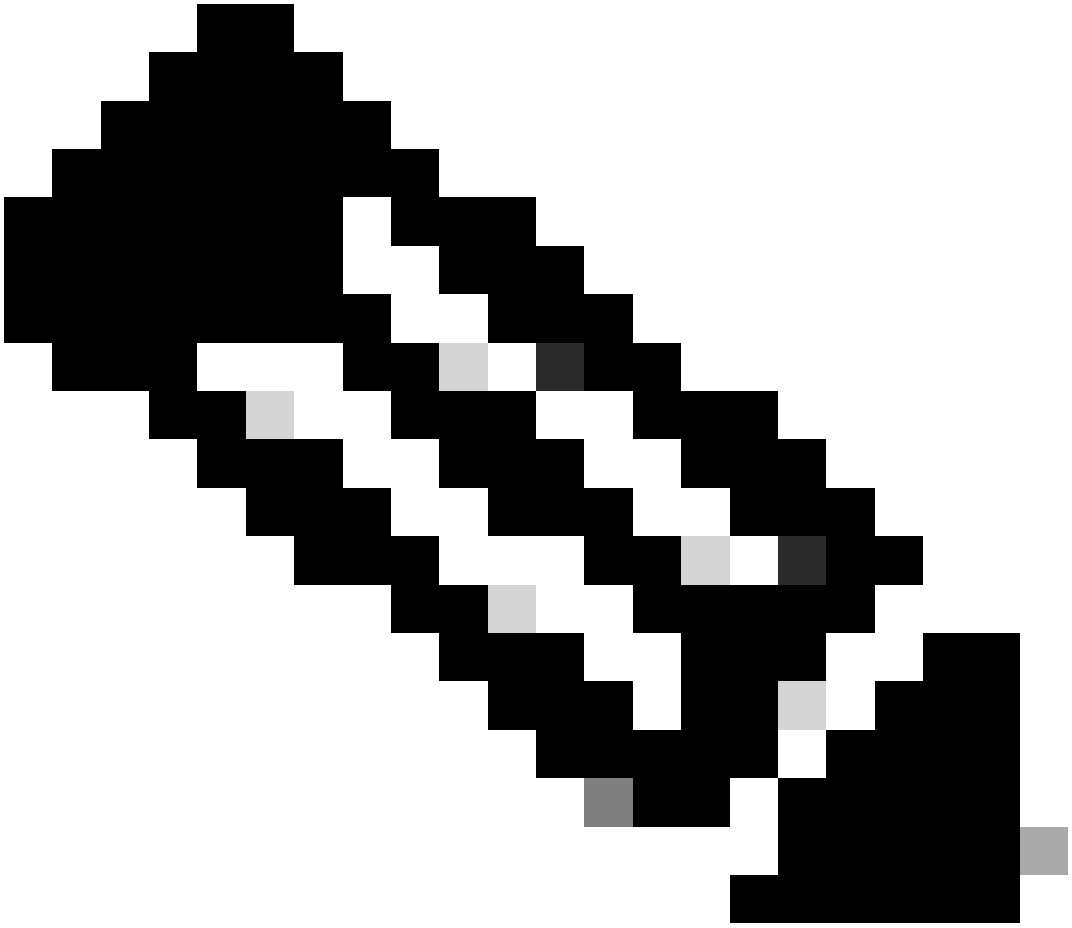
Configuración y verificación

Topología



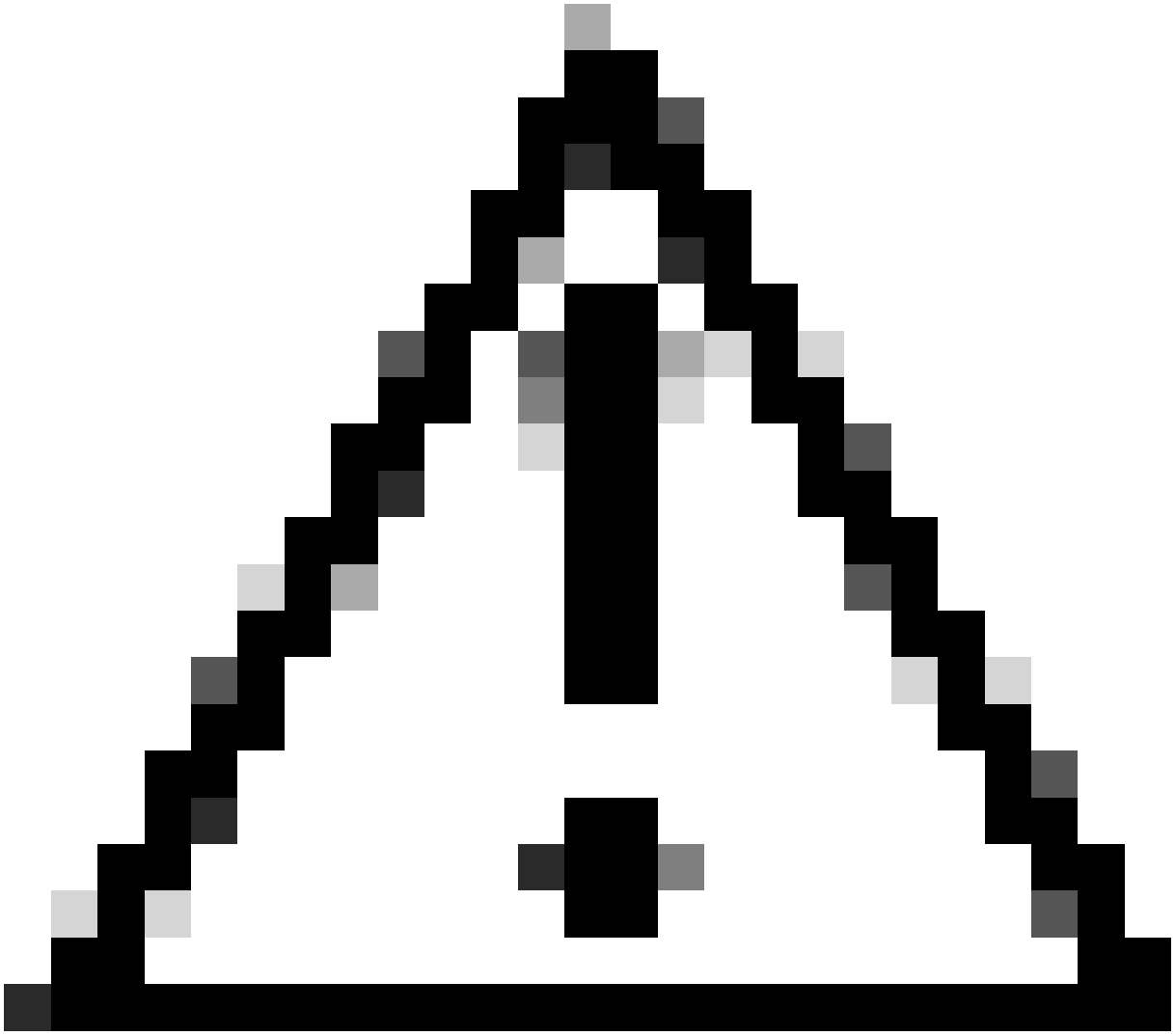
Configuración de N9K-NAT

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



Nota: De forma predeterminada, las entradas máximas de traducción de NAT dinámica son 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



Precaución: La opción interface overload option for inside policies no se admite en los switches de las plataformas Cisco Nexus 9200, 9300-EX, 9300-FX 9300-FX2, 9300-FX3, 9300-FXP y 9300-GX para políticas internas y externas

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

Verificación

Ping de host interno

IP de origen del paquete de datos: 10.0.0.1 Convertido a IP: 192.168.1.10

IP de destino: 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

Verificación de la Tabla de Traducción 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

Estadísticas de 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

Preguntas Frecuentes

¿Qué ocurre cuando se agota el TCAM NAT?

Si se agotan los recursos TCAM, se informa del registro de errores.

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)

¿Qué ocurre cuando se alcanza el número máximo de entradas?

De forma predeterminada, las entradas máximas de traducción NAT son 80. Una vez que las entradas de traducción NAT dinámica exceden el límite máximo, el tráfico se dirige a la CPU, lo que resulta en un registro de errores y una caída.

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

¿Por qué se insertan algunos paquetes NAT en la CPU?

Normalmente, hay dos escenarios en los que el tráfico se rutea a la CPU.

La primera ocurre cuando las entradas de NAT aún no se han programado para el hardware, en este momento el tráfico debe ser procesado por la CPU.

La programación de hardware frecuente ejerce presión sobre la CPU. Para reducir la frecuencia de programación de entradas NAT en el hardware, NAT programa las traducciones en lotes de un segundo. El comando dip nat translation creation-delay retrasa el establecimiento de la sesión.

El segundo escenario involucra paquetes que se envían a la CPU para su procesamiento durante la fase inicial de establecer una sesión TCP y durante las interacciones de terminación de esa sesión.

¿Por qué NAT funciona sin proxy-arp en Nexus 9000?

Hay una función llamada nat-alias agregada desde la versión 9.2.X . Esta función está habilitada de forma predeterminada y resuelve los problemas de NAT ARP. A menos que lo inhabilite manualmente, no necesita habilitar ip proxy-arp o ip local-proxy-arp.

Los dispositivos NAT poseen direcciones globales internas (IG) y locales externas (OL) y son responsables de responder a cualquier solicitud ARP dirigida a estas direcciones. Cuando la subred de direcciones IG/OL coincide con la subred de la interfaz local, NAT instala un alias IP y una entrada ARP. En este caso, el dispositivo utiliza local-proxy-arp para responder a las solicitudes ARP.

La función sin alias responde a las solicitudes ARP para todas las IP traducidas de un rango de direcciones de grupo NAT dado si el rango de direcciones está en la misma subred que la interfaz externa.

¿Cómo funciona el argumento add-route en N9K y por qué es obligatorio?

En los switches de plataforma Cisco Nexus 9200 y 9300-EX, -FX, -FX2, -FX3, -FXP y -GX, se requiere la opción de agregar rutas para las políticas internas y externas debido a la limitación de hardware de ASIC. Con este argumento, el N9K agrega una ruta de host. El tráfico NAT TCP desde el exterior hacia el interior se dirige a la CPU y puede descartarse sin este argumento.

Antes:

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

Después de:

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

¿Por qué NAT admite un máximo de 100 entradas ICMP?

Normalmente, el tiempo de espera de los flujos de NAT ICMP después de la expiración del tiempo de espera de muestreo y del tiempo de espera de traducción configurados. Sin embargo, cuando los flujos de NAT ICMP presentes en el switch se vuelven inactivos, se agota el tiempo de espera inmediatamente después de la expiración del tiempo de espera de muestreo configurado.

A partir de Cisco NX-OS versión 7.0(3)I5(2), se introduce la programación de hardware para ICMP en los switches de la plataforma Cisco Nexus 9300. Por lo tanto, las entradas ICMP consumen los recursos TCAM en el hardware. Debido a que ICMP está en el hardware, el límite máximo para la traducción NAT en los switches de la serie de plataformas Cisco Nexus se cambia a 1024. Se permite un máximo de 100 entradas ICMP para hacer el mejor uso de los recursos. Es fijo, y no hay opción para ajustar las entradas ICMP máximas.

Información Relacionada

Guía de configuración de las interfaces NX-OS de Cisco Nexus 9000 Series, versión 10.4(x)

Informe técnico sobre clasificación de TCAM con ASIC Cisco CloudScale para switches Nexus serie 9000

Guía de escalabilidad verificada de Cisco Nexus serie 9000 NX-OS

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).