Entender o NAT no Nexus 9300

Contents

Introdução

Este documento descreve o recurso NAT nos switches Nexus 9000 equipados com um Cisco Cloud-Scale ASIC que executa o software NX-OS.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha familiaridade com o Cisco Nexus Operating System (NX-OS) e a arquitetura Nexus básica antes de continuar com as informações descritas neste documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Introduzir o suporte a NAT no N9K

Terminologia

- NAT - NAT é uma técnica usada em redes para modificar o endereço IP origem ou destino de pacotes IP.
- PAT - Port Address Translation, também conhecido como "Overloading NAT", vários endereços IP internos compartilham um único endereço IP externo, diferenciado por números de porta exclusivos.
- NAT sensível a TCP - O suporte a NAT sensível a TCP permite que as entradas de fluxo NAT correspondam ao estado das sessões TCP e sejam criadas e excluídas de acordo.

Recurso NAT TCAM

Por padrão, nenhuma entrada TCAM é alocada para o recurso NAT no Nexus 9000. Você deve alocar o tamanho de TCAM para o recurso NAT reduzindo o tamanho de TCAM de outros recursos.

Há três tipos de TCAM envolvidos nas operações de NAT:

- região NAT

O NAT utiliza a região NAT do TCAM para correspondência de pacotes com base no endereço IP ou na porta.

Cada entrada NAT/PAT para endereços de origem internos ou externos requer duas entradas NAT TCAM.

Por padrão, o modo de atualização atômica da ACL está habilitado; 60% do número de escala não atômica é suportado.

- Região sensível a TCP

Para cada política interna de NAT com "x" aces, é necessário o número "x" de entradas.

Para cada pool NAT configurado, uma entrada é necessária.

O tamanho da TCAM do TCP-NAT deve ser duplicado quando o modo de atualização atômica

estiver habilitado.

- Tabela de regravação de NAT

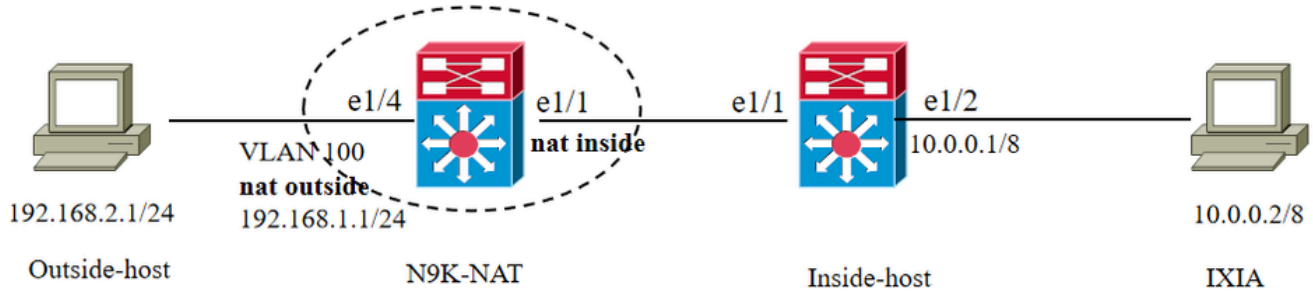
NAT regrava e traduções são armazenado in o "NAT Reescrever Tabela," que existe externa de o NAT TCAM região. O 'NAT Reescrever Tabela' tem a fixed tamanho de 2048 entradas para Nexus 9300-EX/FX/FX2/9300C e 4096 entradas para Nexus 9300-FX3/GX/GX2A/GX2B/H2R/H1. Este tabela é exclusivamente utilizado para NAT traduções.

Cada entrada NAT/PAT estática para endereços de origem internos ou externos requer uma entrada "NAT Rewrite Table".

Para obter mais detalhes sobre TCAM no Nexus 9000, consulte [White paper de classificação TCAM com ASICs Cisco CloudScale para switches Nexus 9000 Series.]

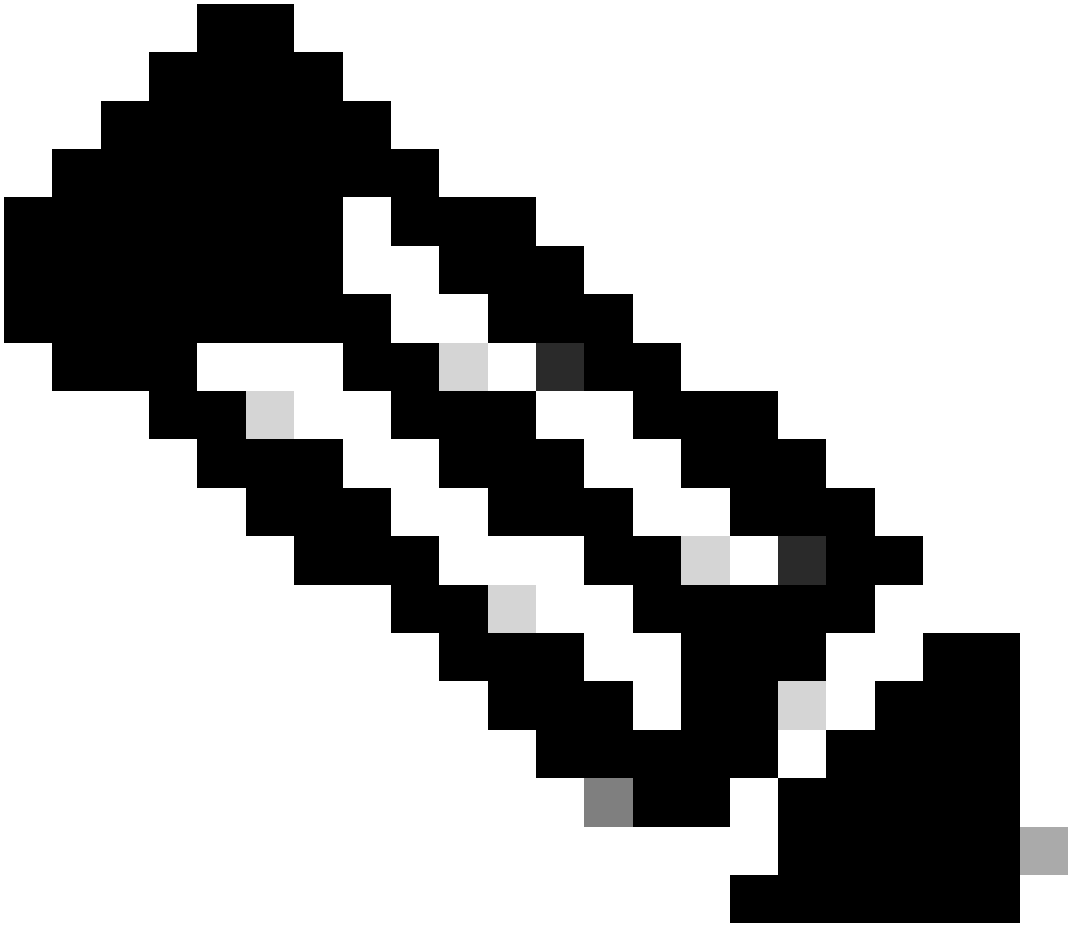
Configuração e verificação

Topologia



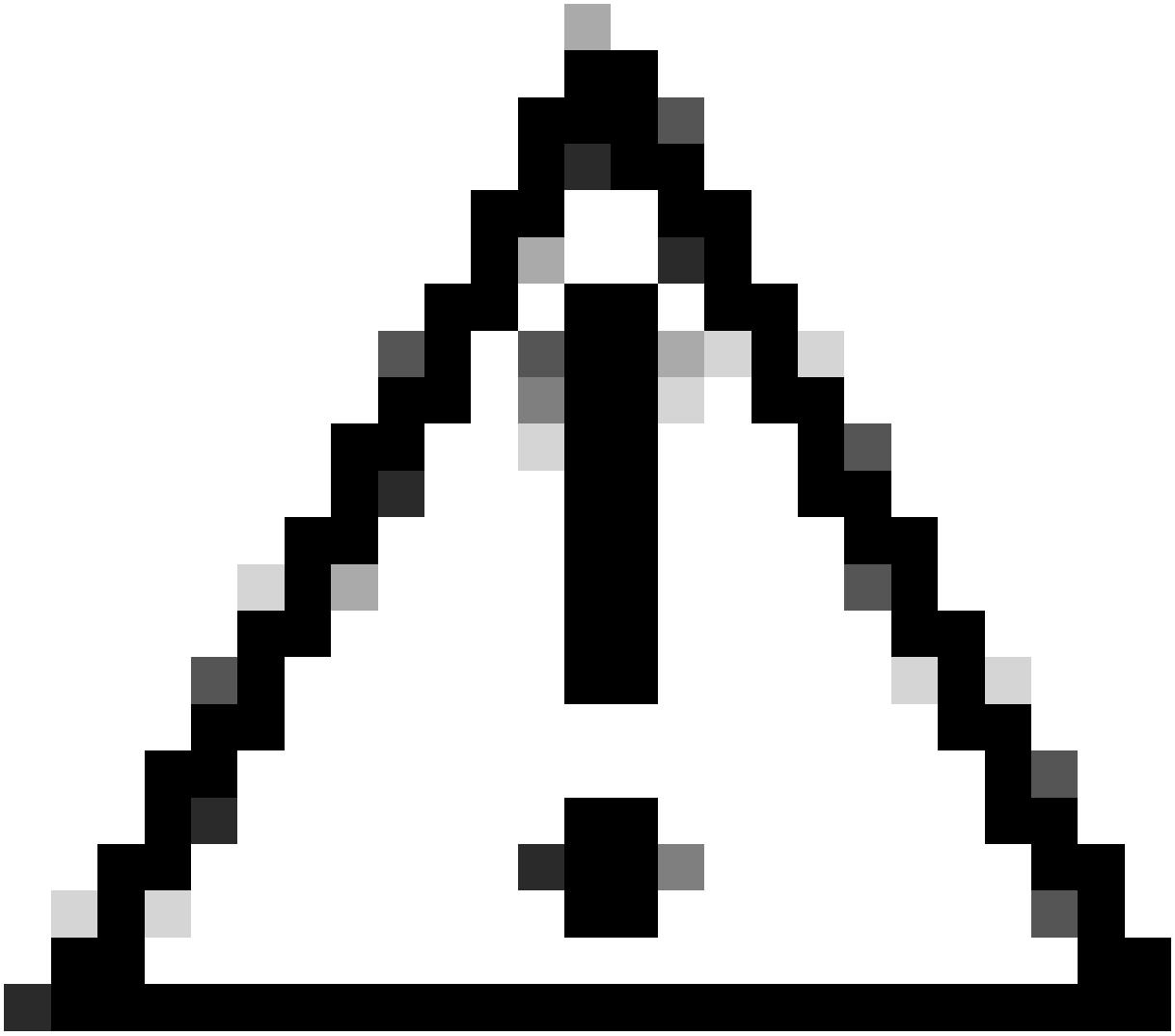
Configuração N9K-NAT

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



Observação: por padrão, a conversão dinâmica nat max-entries é 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



Cuidado: A opção interface overload option for inside policies não é suportada no switch da plataforma Cisco Nexus 9200, 9300-EX, 9300-FX 9300-FX2, 9300-FX3, 9300-FXP e 9300-GX para políticas internas e 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

Verificação

Ping dentro do host

IP de origem do pacote de dados: 10.0.0.1 Convertido em 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

Verificação da tabela de tradução 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

Estatísticas 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

Perguntas mais freqüentes

O que acontece quando a TCAM de NAT se esgota?

Se os recursos TCAM estiverem esgotados, o registro de erros será reportado.

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)

O que acontece quando o número máximo de entradas é atingido?

Por padrão, a conversão de NAT max-entries é 80. Quando as entradas de conversão de NAT dinâmico excederem o limite máximo, o tráfego será direcionado para a CPU, resultando em um log de erros e em um descarte.

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 que alguns pacotes NAT são lançados para a CPU?

Normalmente, há dois cenários nos quais o tráfego deve ser roteado para a CPU.

A primeira ocorre quando as entradas NAT ainda não foram programadas para o hardware, nesse momento o tráfego precisa ser processado pela CPU.

A programação de hardware frequente sobrecarrega a CPU. Para reduzir a frequência de programação de entradas NAT no hardware, o NAT programa conversões em lotes de um segundo. O comando ip nat translation creation-delay atrasa o estabelecimento da sessão.

O segundo cenário envolve pacotes que são enviados à CPU para processamento durante a fase inicial de estabelecimento de uma sessão TCP e durante as interações de término dessa sessão.

Por que o NAT funciona sem proxy-arp no Nexus 9000?

Há um recurso chamado nat-alias adicionado da versão 9.2.X . Esse recurso é ativado por padrão e resolve os problemas do NAT ARP. A menos que o desative manualmente, não é necessário ativar ip proxy-arp ou ip local-proxy-arp.

Os dispositivos NAT possuem endereços Inside Global (IG) e Outside Local (OL) e são responsáveis por responder a qualquer solicitação ARP direcionada a esses endereços. Quando a sub-rede do endereço IG/OL corresponde à sub-rede da interface local, o NAT instala um alias IP e uma entrada ARP. Nesse caso, o dispositivo usa o local-proxy-arp para responder às solicitações ARP.

O recurso sem alias responde às solicitações ARP para todos os IPs convertidos de um determinado intervalo de endereços do pool NAT se o intervalo de endereços estiver na mesma sub-rede da interface externa.

Como o Argumento add-route Funciona no N9K e Por que Ele é Obrigatório?

Nos switches de plataforma Cisco Nexus 9200 e 9300-EX, -FX, -FX2, -FX3, -FXP e -GX, a opção de adicionar rota é necessária para políticas internas e externas devido à limitação de hardware do ASIC. Com esse argumento, o N9K adiciona uma rota de host. O tráfego NAT TCP de fora para dentro é apontado para a CPU e pode ser descartado sem esse 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

Após:

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 que o NAT suporta um máximo de 100 entradas ICMP

Normalmente, o NAT do ICMP flui o tempo limite após a expiração do sampling-timeout e do translation-timeout configurados. No entanto, quando os fluxos de NAT do ICMP presentes no switch se tornam ociosos, eles atingem o tempo limite imediatamente após a expiração do valor de sampling-timeout configurado.

Começando com o Cisco NX-OS versão 7.0(3)I5(2), a programação de hardware é apresentada para ICMP nos switches da plataforma Cisco Nexus 9300. Portanto, as entradas ICMP consomem os recursos TCAM no hardware. Como o ICMP está no hardware, o limite máximo para conversão de NAT em switches da série de plataformas Cisco Nexus é alterado para 1024. É permitido um máximo de 100 entradas ICMP para fazer o melhor uso dos recursos. É fixo e não há opção para ajustar o máximo de entradas ICMP.

Informações Relacionadas

Guia de configuração das interfaces Cisco Nexus 9000 Series NX, versão 10.4(x)

White paper de classificação TCAM com ASICs Cisco CloudScale para switches Nexus 9000 Series

Guia de escalabilidade verificada do NX-OS do Cisco Nexus 9000 Series

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.