Informazioni su NAT su Nexus 9300

Sommario

Introduzione

Questo documento descrive la funzionalità NAT sugli switch Nexus 9000 dotati di un Cisco Cloud-Scale ASIC con software NX-OS.

Prerequisiti

Requisiti

Cisco consiglia di familiarizzare con il sistema operativo Cisco Nexus (NX-OS) e l'architettura Nexus di base prima di procedere con le informazioni descritte in questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Introduzione del supporto NAT su N9K

Terminologia

- NAT - La tecnica NAT viene usata nelle reti per modificare l'indirizzo IP di origine o di destinazione dei pacchetti IP.
- PAT - Port Address Translation, noto anche come "Overload NAT", consente di condividere più indirizzi IP interni con un unico indirizzo IP esterno, differenziato da numeri di porta univoci.
- NAT compatibile con TCP - Il supporto NAT compatibile con TCP consente alle voci di flusso NAT di corrispondere allo stato delle sessioni TCP e di essere create ed eliminate di conseguenza.

Risorsa NAT TCAM

Per impostazione predefinita, nessuna voce TCAM viene assegnata alla funzione NAT su Nexus 9000. È necessario assegnare le dimensioni TCAM per la funzione NAT riducendo le dimensioni TCAM di altre funzioni.

Esistono tre tipi di TCAM coinvolti nelle operazioni NAT:

- Area NAT

NAT utilizza la regione TCAM NAT per la corrispondenza dei pacchetti in base all'indirizzo IP o alla porta.

Ogni voce NAT/PAT per indirizzi di origine interni o esterni richiede due voci NAT TCAM.

Per impostazione predefinita, la modalità di aggiornamento atomico ACL è attivata, il 60% del numero di scala non atomica è supportato.

- Area compatibile con TCP

Per ciascuna policy NAT inside con "x" assi, è richiesto il numero di voci "x".

Per ogni pool NAT configurato, è necessaria una voce.

Quando è abilitata la modalità di aggiornamento atomico, le dimensioni TCP-NAT TCAM devono

essere raddoppiate.

- Tabella di riscrittura NAT

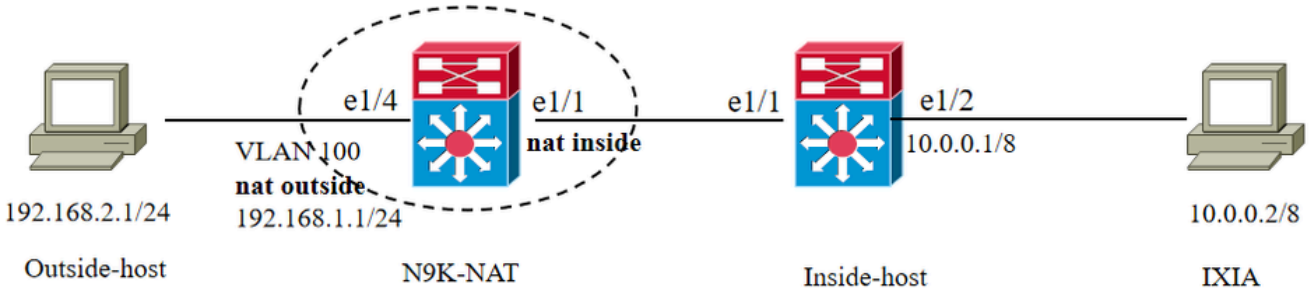
NAT riscrive e traduzioni sono archiviato in OSPF (Open Shortest Path First) "NAT Riscrivi Tabella," che esiste esterno di OSPF (Open Shortest Path First) NAT TCAM regione. OSPF (Open Shortest Path First) 'NAT Riscrivi Tabella' ha a Fixed (Risolto) dimensioni di 2048 voci per Nexus 9300-EX/FX/FX2/9300C e 4096 voci per Nexus 9300-FX3/GX/GX2A/GX2B/H2R/H1. Questo tabella è esclusivamente utilizzato per NAT traduzioni.

Ogni voce NAT/PAT statica per indirizzi di origine interni o esterni richiede una voce "NAT Rewrite Table".

Per ulteriori informazioni su TCAM su Nexus 9000, fare riferimento a White paper sulla classificazione TCAM con Cisco CloudScale ASIC per switch Nexus serie 9000.

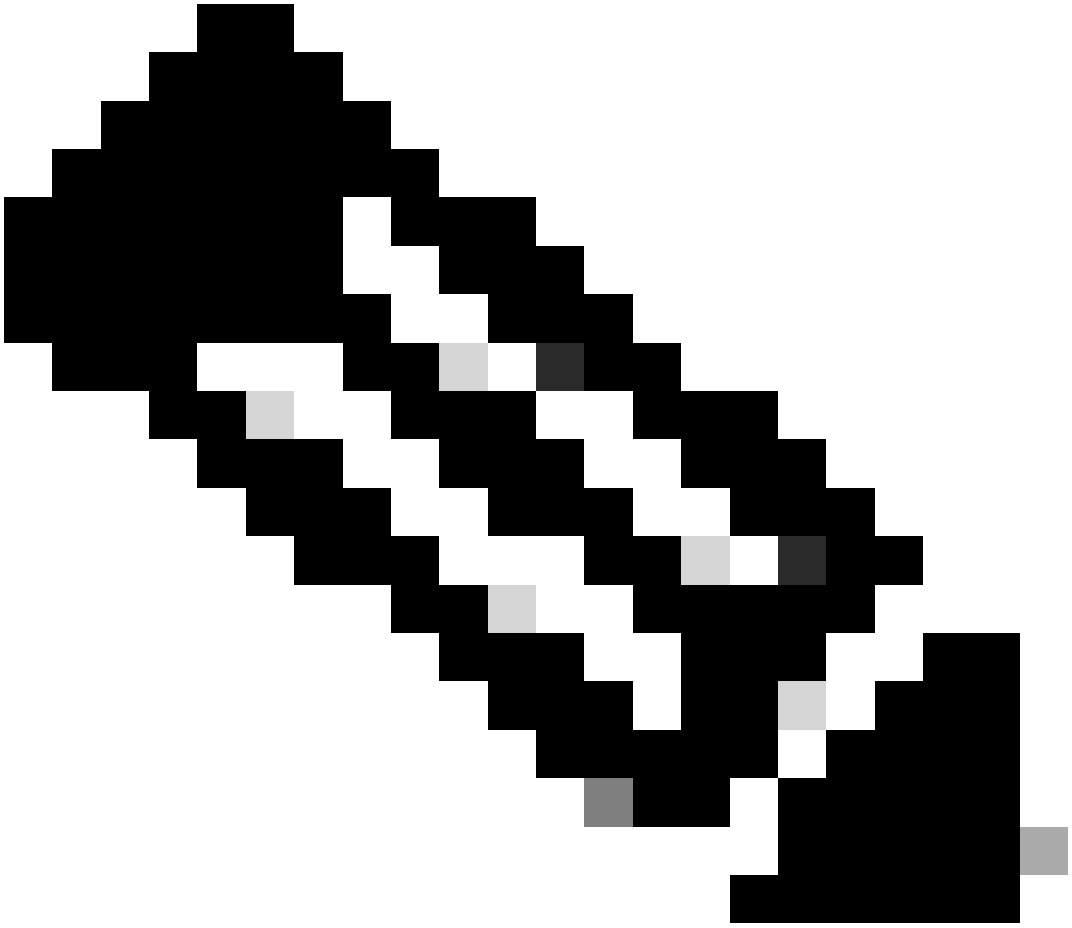
Configurazione e verifica

Topologia



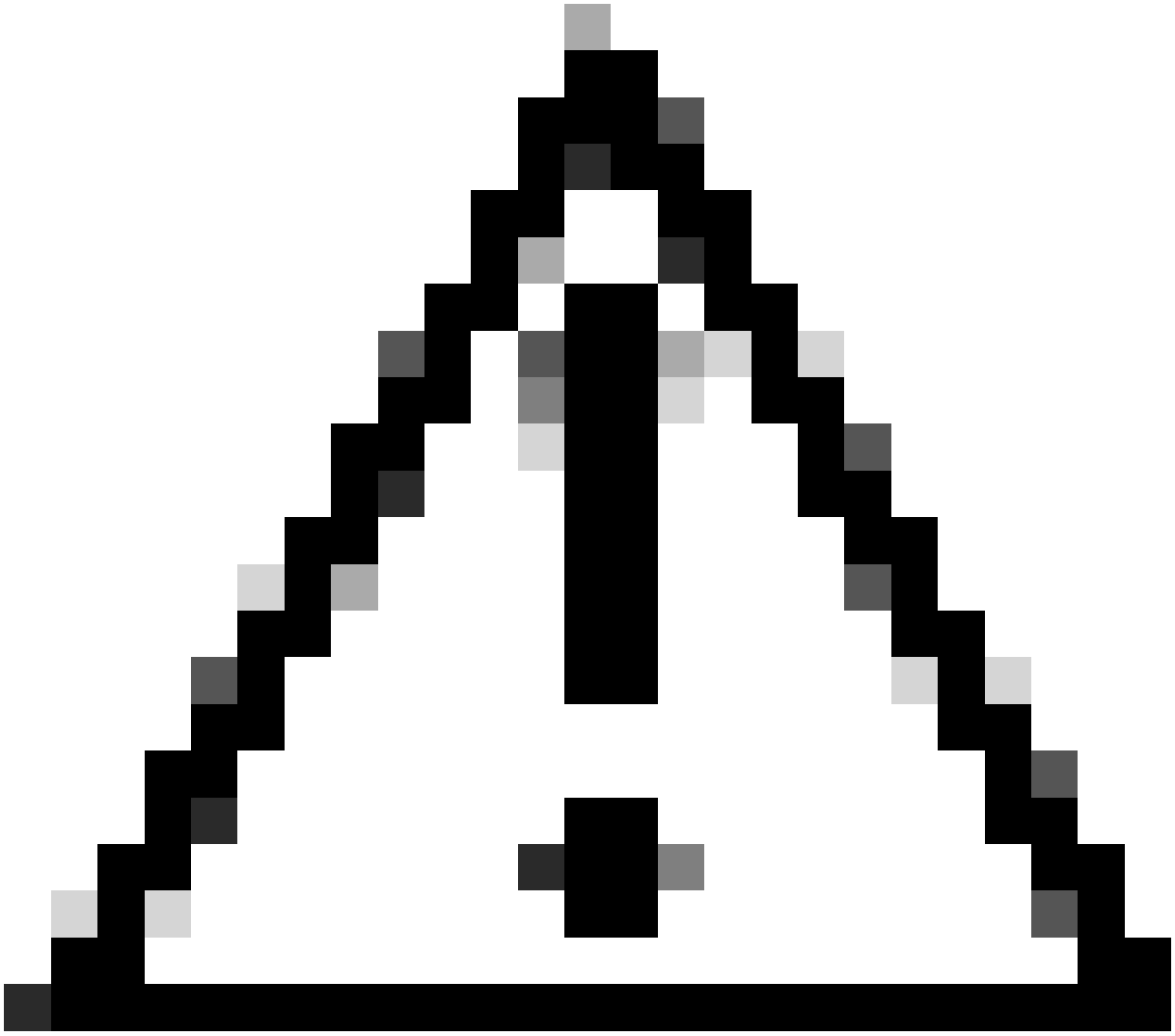
Configurazione N9K-NAT

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



Nota: per impostazione predefinita, il numero massimo di voci per la traduzione nat dinamica è 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



Attenzione: l'opzione di overload dell'interfaccia per le policy interne non è supportata sugli switch con piattaforma Cisco Nexus 9200, 9300-EX, 9300-FX 9300-FX2, 9300-FX3, 9300-FXP e 9300-GX per le policy interne ed esterne

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

Verifica

Ping interno all'host

IP di origine del pacchetto dati: 10.0.0.1 Convertito in IP: 192.168.1.10

IP di destinazione: 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

Verifica tabella di conversione 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

Statistiche 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

Domande frequenti

Cosa succede quando NAT TCAM si esaurisce?

Se le risorse TCAM sono esaurite, viene segnalato il log degli errori.

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)

Che cosa succede quando viene raggiunto il numero massimo di voci?

Per impostazione predefinita, il numero massimo di voci di traduzione NAT è 80. Quando le voci di conversione NAT dinamiche superano il limite massimo, il traffico viene indirizzato alla CPU, generando un log degli errori e il relativo rilascio.

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

Perché alcuni pacchetti NAT sono indirizzati alla CPU?

In genere, esistono due scenari in cui il traffico viene instradato alla CPU.

Il primo si verifica quando le voci NAT non sono ancora state programmate per l'hardware, in questo momento il traffico deve essere elaborato dalla CPU.

Frequenti programmazioni hardware mettono a dura prova la CPU. Per ridurre la frequenza di programmazione delle voci NAT nell'hardware, NAT programma traduzioni in batch di un secondo. Il comando dip nat translation creation-delay ritarda l'impostazione della sessione.

Il secondo scenario riguarda i pacchetti che vengono inviati alla CPU per l'elaborazione durante la fase iniziale di creazione di una sessione TCP e durante le interazioni di terminazione di tale sessione.

Perché NAT funziona senza proxy-arp su Nexus 9000?

È disponibile una funzionalità denominata nat-alias aggiunta dalla versione 9.2.X. Questa funzionalità è abilitata per impostazione predefinita e risolve i problemi ARP NAT. a meno che non venga disabilitato manualmente, non è necessario abilitare ip proxy-arp o ip local-proxy-arp.

I dispositivi NAT possiedono indirizzi globali interni (IG) e locali esterni (OL) e sono responsabili della risposta a qualsiasi richiesta ARP indirizzata a tali indirizzi. Quando la subnet dell'indirizzo IG/OL corrisponde alla subnet dell'interfaccia locale, NAT installa un alias IP e una voce ARP. In questo caso, il dispositivo utilizza local-proxy-arp per rispondere alle richieste ARP.

La funzionalità senza alias risponde alle richieste ARP per tutti gli IP convertiti da un determinato intervallo di indirizzi del pool NAT se l'intervallo di indirizzi si trova nella stessa subnet dell'interfaccia esterna.

Come funziona l'argomento add-route su N9K e perché è obbligatorio?

Sugli switch di piattaforma Cisco Nexus 9200 e 9300-EX, -FX, -FX2, -FX3, -FXP, -GX, l'opzione di aggiunta della route è richiesta sia per le policy interne che per quelle esterne a causa della limitazione dell'hardware ASIC. Con questo argomento, N9K aggiunge una route host. Il traffico TCP NAT dall'esterno all'interno viene puntato alla CPU e può cadere senza questo argomento.

Prima:

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

Dopo:

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

Perché NAT supporta un massimo di 100 voci ICMP

Normalmente, il flusso di dati ICMP NAT scade dopo la scadenza del timeout di campionamento e di conversione configurati. Tuttavia, quando i flussi ICMP NAT presenti nello switch diventano inattivi, scade immediatamente dopo la scadenza del timeout di campionamento configurato.

A partire da Cisco NX-OS versione 7.0(3)I5(2), è stata introdotta la programmazione hardware per ICMP sugli switch di piattaforma Cisco Nexus 9300. Pertanto, le voci ICMP consumano le risorse TCAM nell'hardware. Poiché ICMP è incluso nell'hardware, il limite massimo per la conversione NAT negli switch della serie di piattaforme Cisco Nexus è stato modificato a 1024. Per ottimizzare l'utilizzo delle risorse, è consentito un massimo di 100 voci ICMP. È fisso e non è disponibile alcuna opzione per regolare il numero massimo di voci ICMP.

Informazioni correlate

Guida alla configurazione delle interfacce NX-OS sui Cisco Nexus serie 9000, versione 10.4(x)

White paper sulla classificazione TCAM con Cisco CloudScale ASIC per switch Nexus serie 9000

Guida alla scalabilità Cisco Nexus serie 9000 NX-OS Verified

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).