Nexus 9300でのNATについて

内容

はじめに

このドキュメントでは、NX-OSソフトウェアを実行するCisco Cloud-Scale ASICを搭載したNexus 9000スイッチのNAT機能について説明します。

前提条件

要件

このドキュメントで説明されている情報を使用する前に、Cisco Nexusオペレーティングシステム(NX-OS)と基本的なNexusアーキテクチャに精通しておくことをお勧めします。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- N9K-C93180YC-FX3
- nxos64-cs.10.4.3.F（入手可能）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

N9KでのNATサポートの導入

用語

- NAT:NATは、IPパケットの送信元または宛先のIPアドレスを変更するためにネットワークで使用される技術です。
- PAT:ポートアドレス変換。「オーバーロードNAT」とも呼ばれ、複数の内部IPアドレスが一意のポート番号によって区別され、単一の外部IPアドレスを共有します。
- TCP対応NAT:TCP対応NATのサポートにより、NATフローエントリがTCPセッションの状態に一致し、それに応じて作成および削除されます。

NAT TCAMリソース

デフォルトでは、TCAMエントリはNexus 9000のNAT機能に割り当てられません。他の機能のTCAMサイズを減らして、NAT機能にTCAMサイズを割り当てる必要があります。

NATの動作に関係するTCAMには、次の3つのタイプがあります。

- NAT領域

NATは、IPアドレスまたはポートに基づくパケット照合にTCAM NAT領域を使用します。

内部または外部送信元アドレスの各NAT/PATエントリには、2つのNAT TCAMエントリが必要です。

デフォルトでは、ACLアトミック更新モードが有効になっており、非アトミック尺度番号の60%がサポートされます。

- TCP対応リージョン

「x」個のaceを持つ各NAT内部ポリシーには、「x」個のエントリが必要です。

設定されたNATプールごとに1つのエントリが必要です。

アトミック更新モードが有効な場合、TCP-NAT TCAMサイズを2倍にする必要があります。

- NAT書き換えテーブル

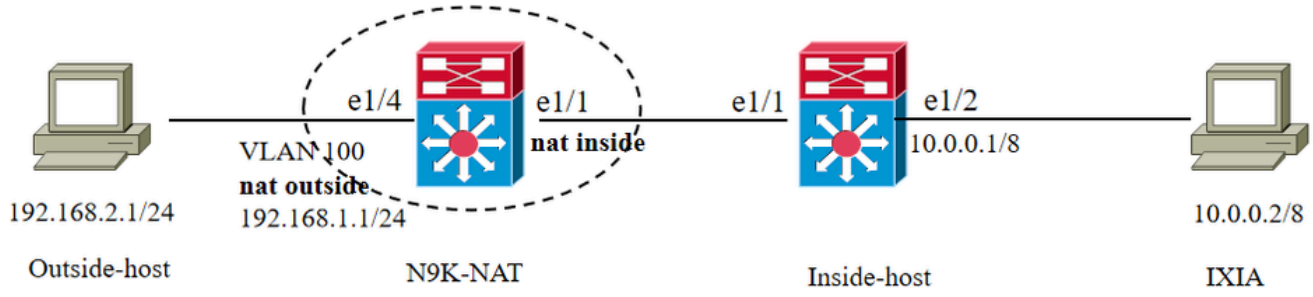
NAT 書き換え と 翻訳 が 保存された イン ページ "NAT 書き換え テーブル," どの 存在する outside（ ページ NAT TCAM リージョン。 「 'NAT 書き換え テーブル' 持つ a fixed サイズ（ 2048 entries を参照 ネクサス 9300-EX/FX/FX2/9300C と 4096 entries を参照 ネクサス 9300-FX3/GX/GX2A/GX2B/H2R/H1。 これは テーブル が もっぱら used を参照 NAT 翻訳。

内部または外部送信元アドレスの各スタティックNAT/PATエントリには、1つの「NAT書き換えテーブル」エントリが必要です。

Nexus 9000でのTCAMの詳細については、 Classification TCAM with Cisco CloudScale ASICs for Nexus 9000 Series Switchesホワイトペーパー。

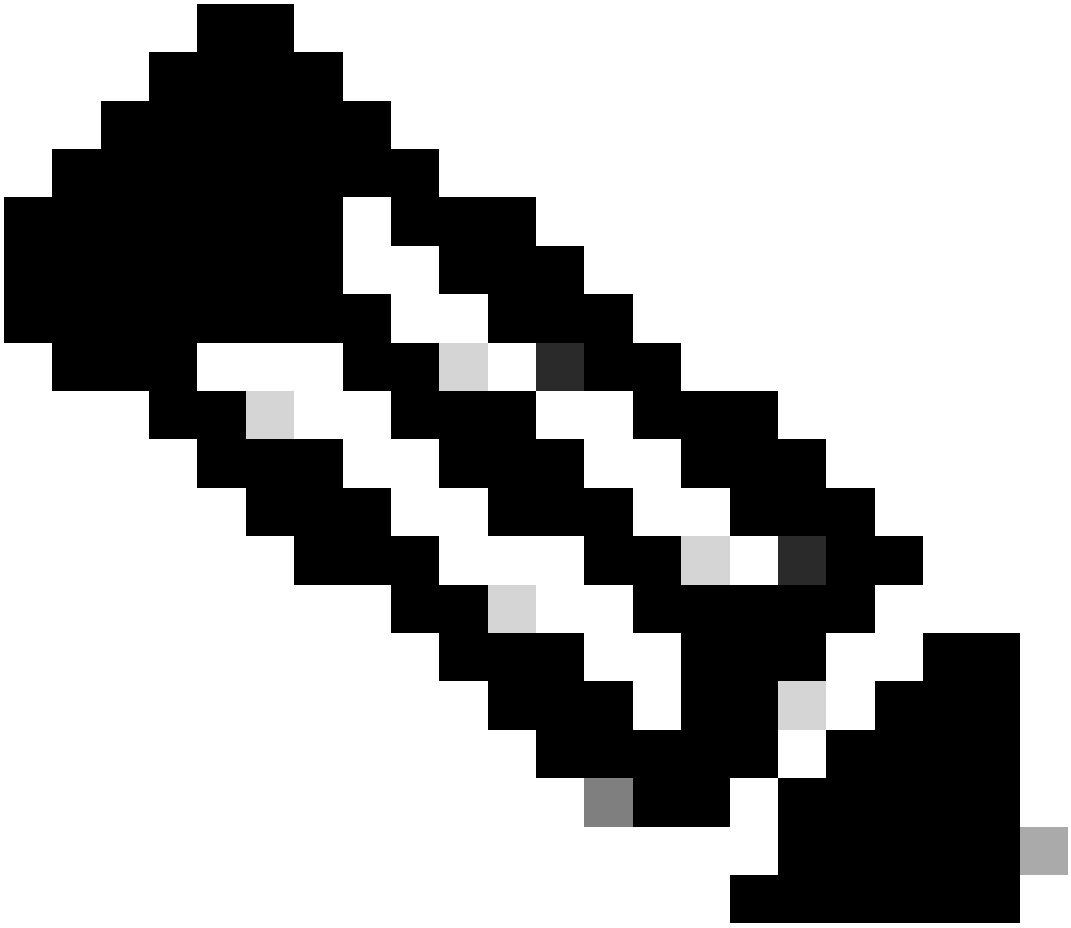
設定と検証

トポロジ



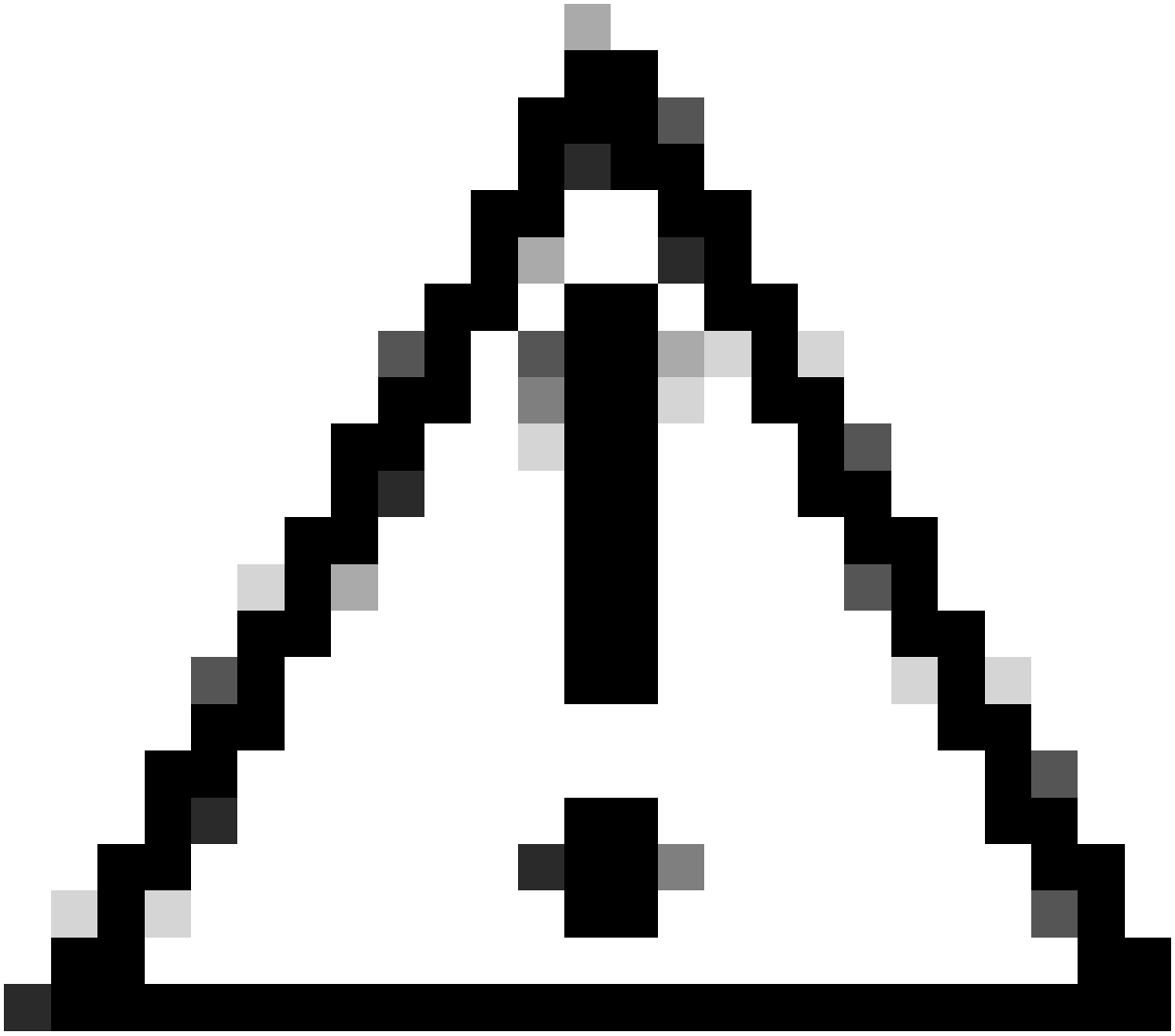
N9K-NATの設定

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



注：デフォルトでは、ダイナミックNAT変換の最大エントリ数は80です。

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



注意: 内部ポリシーのインターフェイスオーバーロードオプションは、外部ポリシーと内部ポリシーの両方について、Cisco Nexus 9200、9300-EX、9300-FX 9300-FX2、9300-FX3、9300-FXP、および9300-GXプラットフォームスイッチではサポートされていません

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

検証

内部ホストのping

データパケットの送信元IP:10.0.0.1をIPに変換：192.168.1.10

宛先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

NAT変換テーブルのチェック

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統計情報

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

よく寄せられる質問（FAQ）

NAT TCAMが枯渇するとどうなりますか。

TCAMリソースが枯渇すると、エラーログが報告されます。

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)

最大エントリ数に達した場合の動作

デフォルトでは、NAT変換の最大エントリ数は80です。 ダイナミックNAT変換エントリが最大制限を超えると、トラフィックはCPUにパントされ、エラーログが生成されて廃棄されます。

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

一部のNATパケットがCPUにパントされる理由

通常、トラフィックがCPUにルーティングされるシナリオは2つあります。

1つ目は、NATエントリがまだハードウェアにプログラムされていない場合に発生し、この時点でトラフィックをCPUで処理する必要があります。

頻繁なハードウェアプログラミングはCPUに負担をかけます。ハードウェアでNATエントリをプログラミングする頻度を減らすために、NATは1秒のバッチで変換をプログラミングします。コマンドip nat translation creation-delayは、セッションの確立を遅延します。

2番目のシナリオでは、TCPセッションを確立する最初のフェーズと、その終了インタラクションの間に処理のためにCPUに送信されるパケットが使用されます。

Nexus 9000でプロキシARPなしでNATが機能する理由

バージョン9.2.Xからnat-aliasという機能が追加されています。この機能はデフォルトで有効になっており、NAT ARPの問題を解決します。手動でディセーブルにしない限り、ip proxy-arpやip local-proxy-arpをイネーブルにする必要はありません。

NATデバイスは、内部グローバル(IG)アドレスと外部ローカル(OL)アドレスを所有し、これらのアドレスに宛てられたARP要求に応答する役割を担います。IG/OLアドレスのサブネットがローカルインターフェイスのサブネットと一致すると、NATはIPエイリアスとARPエントリをインストールします。この場合、デバイスはlocal-proxy-arpを使用してARP要求に応答します。

no-alias機能は、特定のNATプールアドレス範囲が外部インターフェイスと同じサブネットにある場合に、そのNATプールアドレス範囲から変換されたすべてのIPのARP要求に応答します。

add-route引数がN9Kでどのように機能し、なぜ必須なのか

Cisco Nexus 9200および9300-EX、-FX、-FX2、-FX3、-FXP、-GXプラットフォームスイッチでは、ASICハードウェアの制限により、内部ポリシーと外部ポリシーの両方でadd-routeオプションが必要です。この引数により、N9Kはホストルートを追加します。外部から内部へのTCP NATトラフィックはCPUにパントされ、この引数なしでドロップされる可能性があります。

変更前：

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

変更後：

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

NATが最大100のICMPエントリをサポートする理由

通常、ICMP NATフローは、設定されたsampling-timeoutおよびtranslation-timeoutの期限が切れた後にタイムアウトします。ただし、スイッチに存在するICMP NATフローがアイドル状態になると、設定されたサンプリングタイムアウトの満了後すぐにタイムアウトになります。

Cisco NX-OSリリース7.0(3)I5(2)以降では、Cisco Nexus 9300プラットフォームスイッチ上のICMPに対するハードウェアプログラミングが導入されています。したがって、ICMPエントリはハードウェアのTCAMリソースを消費します。ICMPはハードウェア内に存在するため、Cisco Nexusプラットフォームシリーズスイッチの NAT変換の最大制限は1024に変更されます。リソースを最大限に活用するために、最大100個のICMPエントリが許可されます。この問題は修正されており、最大ICMPエントリ数を調整するオプションはありません。

関連情報

『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 10.4(x)』

Classification TCAM with Cisco CloudScale ASICs for Nexus 9000 Series Switchesホワイトペーパー

Cisco Nexus 9000シリーズNX-OS検証済みスケーラビリティガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。