Engineer

NAT

🔀 ルーターを通るパケットのIPアドレスを書き換える仕組み

どのようなものか

NATは、ネットワークアドレス変換の略で、ルーターを通るパケットのIPアドレスを書き換え、一つのアドレス空間でアドレスを割り当てられたホストが、別の空間のホストと通信できるようにします。用語を定めた1999年のRFC 2663は、一つの領域から別の領域へIPアドレスを対応付けることと説明します。目標は、透過的なルーティングです。両側のホストは、変換を知る必要がないはずです。

ほぼ誰もが接する形は、2001年1月公開のRFC 3022が、従来型NATと呼ぶものです。小さい事務所や家庭が、提供元からIPアドレスを一つ受け、ルーターの後ろのマシンは、RFC 1918の10.0.0.0/8、172.16.0.0/12、192.168.0.0/16という私用アドレスを使うのが典型です。これらは、組織間ではルーティングしません。ルーターは、出る各パケットの送信元を、自分の公開アドレスへ書き換え、返答では逆に戻します。基本NATは、アドレスだけを変えるため、同時に外へ出られる内部ホスト数は、保有する公開アドレス数までです。アドレスとポートを変換するNAPTは、TCPやUDPのポート、またはICMPの識別子も書き換え、多数の内部ホストで、一つの公開アドレスを共有できます。RFC 3022は、LinuxがIP masqueradeという名前で提供していたと記し、ファイアウォールのツールは、今もその言葉を使います。

アドレスを変えると、それを使って計算した値もすべて正しくなくなるため、ルーターは、そちらも直します。RFC 3022は、IPヘッダーのチェックサムと、TCP、UDPのチェックサムの調整を求めます。後二つは、送信元と宛先を含む疑似ヘッダーも対象とするからです。正しい内部ホストへ返答するため、ルーターは、一方に内部アドレスとポート、もう一方に外部アドレスとポートを持つ、対応表を保ちます。ネットワークの途中で保つ状態であり、NATの問題の大半は、そこから生まれます。

従来型NATは、一方向です。RFC 3022は、セッションは私用ネットワークから外へ始まり、逆向きは、事前に選んだホスト向けの静的なアドレス対応だけで認めると説明します。現在は、一段上でも同じ考えを使います。2012年4月のRFC 6598は、通信事業者規模のNATのために100.64.0.0/10を予約し、提供元のNATと、顧客の機器との間のリンクに番号を付けます。顧客の機器でも、さらに変換する場合があります。

概念を判断に生かす

「NATとは？」を実際の判断に生かしましょう。その概念を、開発または購入するシステムに結び付けて考えるお手伝いをします。 Wi-Fi、ファイアウォール、リモートアクセスを整え、どこからでも働け、権限のある人だけが接続できるようにします。

サービスを見る お問い合わせ →

用語の背後にある前提を検証する

解説とリンク先の実績を参考に、プロジェクトについての質問を整理してください。ツールを選ぶ前に、前提を一緒に検討できます。 Ubuntu Linux VPSインスタンス30台を管理 — 30 復旧計画とともに管理したLinuxサーバー

Ubuntu Linux VPSインスタンス30台を管理 お問い合わせ →

なぜ重要なのか

RFC 3022は、代償を隠しません。ホストやルーターを変えずに導入できますが、同RFCの言葉では「IPアドレスのエンドツーエンドの意味」を失い、ネットワーク内の状態を増やして補います。実用上のほぼすべての結果は、その一文から導かれます。

サーバーから見た接続の送信元は、一台ではなく、大勢を背後に持つルーターであることがよくあります。一人を狙った遮断やレート制限が、同じアドレスの全員にかかり、不正利用の報告は、犯人でなくルーターを示します。RFC 3022は、内部からも同じことを述べます。私用アドレスの隠蔽を、プライバシー上の利点としつつ、ほかを攻撃したり迷惑メールを送ったりするホストのアドレスも、NATルーターに隠れるため、診断も難しくなると指摘します。

状態を保つことは、タイマーを持つことでもあります。対応は、ルーターが覚えている間だけ存在します。2007年1月のBest Current PracticeであるRFC 4787は、UDPの対応を、少なくとも二分有効にする必要があるとし、五分以上を勧めます。2008年10月のTCP側のRFC 5382は、確立済みで通信のない接続の期限を、2時間4分とします。既定のキープアライブは二時間ごとで、四分は転送中のパケットのためです。文書に従う機器の最低値であり、すべてが従うわけではありません。機器のタイマーより長く静かな接続は、対応を失い、次に外から来るパケットは、行き先を失います。

さらに二つの制約があります。RFC 3022は、セッションの全パケットが同じNATルーターを通ることを必須とし、出口が複数なら、NAT機器が同一の変換表を共有することを不可欠とします。また、ペイロード内にアドレスを持つプロトコルは、NAT機器の助けが必要ですが、内容を読める間しか機能しません。

実際の活用例

Linuxのルーターでは、nftablesが `nat` 型のチェーンでNATを行います。以下は、nft(8)のNAT例を基にした、この記事の説明用ルールです。198.51.100.0/24を内部ネットワーク、203.0.113.5をルーターの公開アドレスとしています。どちらも文書用の範囲で、本当の内部ネットワークには、通常、RFC 1918の範囲を使います。

```
add table nat
add chain nat prerouting { type nat hook prerouting priority dstnat; }
add chain nat postrouting { type nat hook postrouting priority srcnat; }
add rule nat postrouting oif eth0 ip saddr 198.51.100.0/24 snat to 203.0.113.5
add rule nat prerouting iif eth0 tcp dport 443 dnat to 198.51.100.20
```

最初の規則は、日常の使い方です。内部ネットワークからeth0を通って出るパケットは、送信元が203.0.113.5になります。動的な公開アドレスには、送信インターフェースのその時点のアドレスを使う `masquerade` を、マニュアルが用意します。二つ目は、逆向きの静的な対応です。eth0のポート443へ来るTCP接続を、内部の198.51.100.20へ送ります。少ない規則で足りるのは、接続の最初のパケットだけがnatチェーンを通るからです。決定を接続追跡の記録に保存し、以後の全パケットも同じように書き換えます。

もう一方は、自分で制御できないNATの後ろにいるホストです。WireGuardには、まさにそのための設定があります。この記事の二つ目の説明例では、内部ホストから、外側の相手へのトンネルを開いたままにします。

```
[Peer]
PublicKey = <外部ピアの公開鍵>
Endpoint = 192.0.2.44:51820
AllowedIPs = 192.0.2.128/25
PersistentKeepalive = 25
```

wg(8)のマニュアルは、`PersistentKeepalive`を、認証済みの空パケットを送る1から65535秒の間隔と説明します。ステートフルなファイアウォールの状態や、NATの対応を有効に保つためです。自分からはほぼ送らず、いつでも受信する可能性のある、NATの後ろのインターフェースには、25秒を勧めます。既定では無効です。外側の相手に、特別なものは不要です。そのホスト向けの`Endpoint`は、正しく認証したパケットの、最新の送信元アドレスとポートへ更新します。それこそ、NATが割り当てたものです。

NATの問題は、こうしたトンネルで表れがちです。ポートフォリオには、Google CloudとLinuxで、2022年から2024年に管理し、障害を調べた八つのWireGuardとIPsecの接続があります。トンネルは不安定で、落ちると診断しにくかったと記します。繰り返すルーティングと鍵交換の問題を、再起動でなく根本から直し、その後、中断は止まりました。ただし、NATが関係したかは記していません。上の二例は、プロジェクトの実績でなく、この記事の説明例です。

問題が起きるところ

静かな接続が、返答しなくなります。 しばらく何も送らないトンネル、データベース接続、プッシュ通知の経路は、両端が閉じなくても、対応を失って切れます。無通信時間に依存するため、症状は偶然に見えます。`PersistentKeepalive`のように、途中の最短の期限より短い間隔で、内部からキープアライブを送ります。自分で運用するNATでは、タイマーの値をRFC 4787とRFC 5382の最低値以上に保ちます。RFC 4787は、外向きパケットで対応を更新するよう求め、内向きで更新できると、攻撃者が永遠に保てると警告するため、内部から更新すべきです。

外から接続できると思います。 従来型NATは、設計上、外向きです。内部のサービスは、静的な対応を誰かが書くまで、外から届きません。必要なポートだけに`dnat`を加えるか、向きを逆にして、先のキープアライブのように、内部から外へ接続します。

ヘアピンに対応しません。 内部の二ホストが、一方の外部アドレスを使って通信するには、NATがパケットを内部へ折り返す必要があります。RFC 4787は、このヘアピンへの対応と、折り返したパケットの送信元に、外部アドレスとポートを示すことを必須とします。その経路を意図的に試し、対応できない機器では、内部アドレスを使います。

ペイロード内にもアドレスがあります。 典型はFTPで、RFC 2663は、`PORT`コマンドと`PASV`応答に、IPアドレスとポートを文字列として含むと記します。ヘッダーだけを変えるNATでは、その値が誤ったままになります。NAT機器は、アプ

リケーションレベルゲートウェイ、ALGで補い、RFC 3022は、FTP用を最も普及したものとします。ALGは、ペイロードを読む必要があるため、鍵を持たなければ、暗号化で使えなくなります。RFC 3022は、NAT越しのエンドツーエンドIPsecは、当然に使えるとは考えられないとも付け加えます。ペイロードにアドレスを入れないプロトコルを優先します。古いものを自分のNATへ通す必要がある場合は、nft(8)に、FTPの接続追跡ヘルパーがあります。

ログには、ルーターしか残りません。 クライアントがNATの後ろにいると、サーバーのアクセスログには共有アドレスが記録され、それだけでは一台の内部ホストを特定できません。アドレスとともに、送信元ポートと正確な時刻を記録し、時計を同期します。一接続への苦情を、ルーターの変換記録と照合できるようにするためです。

NAPTでフラグメントを扱います。 TCPやUDPのヘッダーは、最初の断片だけにあります。RFC 3022は、NAPTで外向きの断片を変換すると失敗すると警告します。同じ識別子を持つ断片を、内部の二ホストが同じ宛先へ送れば、両セッションを壊す可能性もあります。途中で分割せず通れるほど、パケットを小さく保ちます。

NATをファイアウォールと考えます。 一方向であることを、防御と誤解しがちです。RFC 4787は、安全のために導入することが多いと認めつつ、対応の作り方は安全性に影響せず、どのパケットを入れるかという、フィルタリングだけが決めると明記します。入れてよいものの規則を明示し、各 `dnat` に、意図した通信だけを許すフィルター規則を組み合わせます。

参考資料

- RFC 3022：従来型IPネットワークアドレス変換 — 基本NATとNAPT、その代償を率直に列挙した、2001年の説明です。
- RFC 2663：NATの用語と考慮事項 — アドレス領域から、透過的なルーティング、ALGまでの用語です。
- RFC 4787：ユニキャストUDP向けNATの動作要件 — UDPの対応、期限、ヘアピンの動作です。
- RFC 5382：TCP向けNATの動作要件 — 確立済み、終了中の接続の無通信期限を含む、TCP側の文書です。
- wg(8)：WireGuardインターフェースの設定と取得 — `PersistentKeepalive` と、NATの後ろのホストへの助言を含む、WireGuardのマニュアルです。
- nft(8)：nftablesマニュアル — natチェーンと、 `snat` 、 `dnat` 、 `masquerade` を含む参照資料です。

用語集

実際の制約に合わせて選ぶ

デプロイの流れ、運用上のリスク、緊急対応の担当者をお知らせください。検査、復旧手段、明確な責任の所在を伴う変更の範囲を定められます。

料金を見る お問い合わせ →

用語を実務に結び付ける

「NATとは？」がお客様の組織にどう当てはまるかをご相談ください。現在のシステムの具体例が一つあれば、話を始められます。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く

連絡先カード

心を込めて丁寧に制作： D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://engineer.company/ja/glossary/nat/