Engineer

VPN

共通の通信基盤上で論理的に分離したネットワーク

どのようなものか

VPNはvirtual private networkの略で、トンネルやラベル付き経路を組み合わせ、限定されたマシン群が、それぞれのアドレスと経路で互いに到達できるようにするものです。途中でパケットがどのネットワークを通るかは問いません。IETFの用語では、機密性よりも分離の問題として扱います。そのグループを他の利用者から分離し、暗号化は作業部会の対象外にある追加機能として挙げています。日常的によく使われる形は2つです。拠点間VPNは、両端のゲートウェイを通じ、事務所とクラウドプロジェクトなどのネットワーク全体を結びます。リモートアクセスVPNは、離れた場所のノートPCやスマートフォン1台をネットワークへ接続します。

VPNという名前は、仕組みの大きく異なる技術にも使われています。IPsecはホストやセキュリティゲートウェイのネットワークスタック内でIPパケットを保護し、鍵の交渉には一般にIKEv2を使います。多くのファイアウォール、ルーター、マネージドクラウドゲートウェイが使う方式です。より新しいWireGuardは通常のネットワークインターフェースとして現れるトンネルで、UDPを使い、公開鍵で各ピアを識別します。交渉する暗号方式の一覧を持たず、意図的に固定の組み合わせを1組だけ提供します。OpenVPNはユーザー空間のプロセスとして動き、TLSで鍵を確立します。BGPとMPLSによる通信事業者のVPNは、事業者のバックボーン内で顧客を分離しますが、その仕様自体が暗号による機密性を一切提供しないと定めています。契約、構成図、ファイアウォールのベンダーがVPNと言うときは、どの方式を指すか確認する価値があります。

概念を判断に生かす

「VPN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

VPNが通常解決するのは、互いに通信する必要のある2か所を、両者間のサービスを公開インターネットに置かずに接続する方法です。別のクラウドのパイプラインだけが読むデータベース、社内の管理画面、バックアップ先は、ログインを設けて公開アドレスで待ち受けることも、トンネル経由でしか届かないプライベートアドレスで待ち受けることもできます。後者なら、スキャナーが見つけられるものをゲートウェイの1ポートに絞れます。拠点間の接続では、依然として単純でよく理解された選択肢です。

次はWireGuardかIPsecかですが、通常は接続先によって決まります。相手がファイアウォール装置、クラウド事業者のマネージドゲートウェイ、取引先のネットワークチームなら、IPsecしか選べないことも多く、設計の簡潔さより相互運用性が優先します。両端が自分で管理するLinuxマシンなら、WireGuardの方が導入も仕組みの把握も容易です。各側に短い設定ファイル1つ、各ピアに公開鍵1つ、そして各ピアが送信元として使えるアドレスの一覧を用意します。設計論文によると、Linux実装は監査可能な規模の4,000行未満です。一方、LinuxのIPsec構成はカーネルのパケット変換処理と別個の鍵交換デーモンを組み合わせ、合意すべき設定も多くなります。

運用費用の中心は、Linuxや多くのファイアウォールに含まれるソフトウェアそのものではありません。注意を払い続ける手間です。夜間にトンネルが切れ、相手側の設定変更から何時間も後に鍵更新が失敗します。その兆候は、パケットを送っても何も戻らないという沈黙だけです。トンネルにも他の本番サービスと同じ扱いが必要です。専用のヘルスチェックとアラートを設け、両端の管理責任者を書き残します。

VPNが不適切な場面もあります。リモート勤務者全員に事務所のネットワークへの完全なトンネルを与えると、必要なのは1つのアプリケーションなのに、サブネット全体へ到達できてしまいます。接続後は、そのサブネットのすべてから信頼されがちです。通常ゼロトラストとして販売される、要求ごとに個別に認証するアプリケーション単位のアクセスは、利用者が人で、接続先がウェブアプリケーションなら適しています。プライバシーのためのVPNをうたう一般消費者向けアプリは、さらに別のものです。インターネット接続事業者に置く信頼をVPN会社へ移し、接続先のサイトから元の送信元IPアドレスを隠せる場合はありますが、それだけで匿名性を保証するものではありません。

実際の活用例

2022年から2024年にかけて、Google Cloudとオンプレミスの Linuxシステム間の安全な通信は、一組として管理し、障害を調べた8本のWireGuardとIPsecのトンネルを通っていました。それまでは不安定で原因の特定に時間がかかり、1本の停止で環境間の通信が切れることもありました。各トンネルが特別扱いにならないよう構成を標準化し、状態を監視し、繰り返す経路設定や鍵交換の問題を再起動で一時的に解消するのではなく根本から修正しました。その後は8本すべてが安定して動き、繰り返していた接続障害も止まりました。

同じ時期、ある組織はIPsec VPNの先にある遠隔データウェアハウスからデータを取得する必要がありました。Google BigQueryへ送る6本のETL/ELTパイプラインでは、トンネルが一連の処理の最初の接続を担いました。保護されたサーバーへの安全な接続を設け、取得を無人で実行できるようにしました。その後、定期ジョブがParquet、CSV、.bakファイルの圧縮アーカイブをダウンロードし、MSSQLとPostgreSQLへ復元してステージング領域に入れ、結果をBigQueryへ読み込みました。人の操作を待たないトンネルを通じ、以前は手作業で少なくとも3時間かかった処理全体が20分未満になり、週1回ではなく毎日データを更新できるようになりました。VPNは成果の中で最も目立たない部分でありながら、他のすべての土台です。取得元へ届かないパイプラインは、後段のSQLがどれほど優秀でも最初の工程で止まります。

問題が起きるところ

小さなパケットは通るのに、大きなパケットが消える。 どのトンネルもヘッダーを加えるため、内部で運べる最大パケットは外側の経路が許す大きさより小さくなります。WireGuardのデータメッセージは、外側のUDPとIPヘッダーの前に固定で32バイトを加えます。パケットのパディングは別として、合計ではIPv4で約60バイト、IPv6で約80バイトです。トンネルのMTUが高すぎ、経路がそれを知らせるICMPメッセージを破棄すると、pingやSSHログインは動くのに、ファイル転送やTLSハンドシェイクは止まります。断片化を禁止したフルサイズのパケットで試し、インターフェースのMTUを下げるか、TCPセグメントサイズを収まるよう制限します。

```
# When each WireGuard peer last completed a handshake, as Unix time
wg show wg0 latest-handshakes
# A 1,420-byte packet that may not be fragmented on the way
ping -M do -s 1392 -c 3 10.0.0.2
# Which interface and route the kernel picks for a remote host
ip route get 10.20.0.5
```

2拠点が同じアドレスを選んでいた。 10.0.0.0/8や192.168.0.0/16といったプライベート範囲は各所で再利用されます。両方が10.0.0.0/24を使うネットワークを接続すると、ルーターはパケットがどちら向けか区別できません。最初のトンネルを作る前に範囲を計画するか、片側でアドレス変換を受け入れます。ただし変換すると、それ以降のすべてのログ行とファイアウォール規則が複雑になります。

トンネルは接続しているのに経路が違う。 ピアに新しいハンドシェイクが表示されても、遠隔サブネットへの経路がない場合や、WireGuardのそのピア向けの許可アドレス一覧に範囲がない場合、通信は既定経路から出ていきます。IPsecでこれに当たるのは、両端でトラフィックセレクターが異なる場合です。IKEv2は両者を重なり合う範囲へ絞るか、TS_UNACCEPTABLE通知で拒否します。そのためトンネル自体は接続できても、どちらかが意図した範囲より狭い通信しか運べないことがあります。

変更から長い時間がたって鍵更新に失敗する。 両プロトコルは使用中のセッション鍵を時間と共に交換するため、プロポーザルの編集や鍵のローテーションなど、片側で加わった不一致が、現在の鍵を交換するまで現れない場合があります。WireGuardは通信が続く間、およそ2分ごとに新しいセッションを開始します。IPsecの有効期間は各端点のローカルポリシーで、両端が一致する必要はありません。WireGuardでは、最後に成功したハンドシェイクからの経過時間を、想定する通信やヘルスチェックと併せて判断します。通信していないピアの古いハンドシェイクだけで障害とは言えません。一般にdead peer detectionと呼ばれるIKEv2の生存確認を有効にし、ゲートウェイが無応答の相手へ送り続けるのではなく、その沈黙を検知できるようにします。

接続できることが信頼の根拠になる。 多くのリモートアクセス構成は、VPN上のノートPCを事務所内にあるかのように扱います。そのため、認証情報が1つ盗まれるだけでサブネット全体に届いてしまいます。各VPNクライアントが到達できる範囲をゲートウェイで制限し、背後のサービス側でも認証を維持します。また、名前解決とインターネット向け通信をトンネルに通すか、外へ直接出すかを意図して決めます。

参考資料

- RFC 4026の3.10節 — IETFによるVPNの一般的な定義と、暗号化が作業部会の活動範囲外であるという注記。
- WireGuard: Next Generation Kernel Network Tunnel — 設計論文。暗号鍵による経路制御、ハンドシェイク、鍵更新を支えるタイマー。
- RFC 4301 — すべてのIPsec実装が従うIPのセキュリティアーキテクチャー。

- RFC 7296 — IKEv2。トラフィックセレクターの絞り込み、ローカルポリシーとしての有効期間、生存確認を含みます。
- RFC 4364 — 通信事業者が使うBGP/MPLS IP VPN。重複するアドレス空間を扱い、暗号による機密性は提供しません。

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

「VPN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/vpn/