Engineer

VPN

🖧 ein logisch getrenntes Netz auf gemeinsamer Infrastruktur

Was es ist

VPN steht für Virtual Private Network, auf Deutsch virtuelles privates Netzwerk. Gemeint ist ein Verbund aus Tunneln oder gekennzeichneten Pfaden, über den eine geschlossene Gruppe von Rechnern einander mit eigenen Adressen und Routen erreicht, unabhängig davon, welche Netze die Pakete unterwegs passieren. Die IETF-Terminologie versteht darunter eine Trennung, keine Geheimhaltung: Die Gruppe wird von anderen Nutzern getrennt; Verschlüsselung wird als mögliche Ergänzung außerhalb des Zuständigkeitsbereichs der Arbeitsgruppen erwähnt. Im Alltag überwiegen zwei Formen. Ein Site-to-Site-VPN verbindet ganze Netze, etwa ein Büro und ein Cloudprojekt, mit je einem Gateway an beiden Enden. Ein Remote-Access-VPN verbindet einen einzelnen Laptop oder ein Smartphone mit einem entfernten Netz.

Unter demselben Namen stehen sehr unterschiedliche Techniken. IPsec schützt IP-Pakete im Netzwerkstack eines Hosts oder eines Sicherheitsgateways und verwendet häufig IKEv2 zur Schlüsselaushandlung. Die meisten Firewalls, Router und verwalteten Cloudgateways sprechen dieses Protokoll. WireGuard ist ein neuerer Tunnel, der als gewöhnliche Netzwerkschnittstelle erscheint, über UDP arbeitet und jeden Peer mit einem öffentlichen Schlüssel identifiziert. Statt eines aushandelbaren Menüs bietet er bewusst einen festen Satz kryptografischer Verfahren an. OpenVPN läuft als Userspace-Prozess und handelt seine Schlüssel mit TLS aus. Auf BGP und MPLS aufgebaute Provider-VPNs trennen Kunden innerhalb des Backbones eines Anbieters und bieten laut eigener Spezifikation keinerlei kryptografische Vertraulichkeit. Steht in einem Vertrag, einem Diagramm oder bei einem Firewallanbieter VPN, lohnt sich die Frage, welche dieser Techniken gemeint ist.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist ein VPN?“ für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. WLAN, Firewalls und Fernzugriff werden so eingerichtet, dass Mitarbeitende von überall arbeiten können und nur Berechtigte Zugang erhalten.

Unsere Leistungen entdecken Kontakt aufnehmen →

Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 30 Ubuntu-Linux-VPS-Instanzen verwaltet — 30 verwaltete Linux-Server mit geplantem Wiederherstellungsweg

30 Ubuntu-Linux-VPS-Instanzen verwaltet Kontakt aufnehmen →

Warum es wichtig ist

Ein VPN beantwortet meist die Frage, wie zwei Standorte miteinander sprechen können, ohne den dazwischen benötigten Dienst ins offene Internet zu stellen. Eine Datenbank, die nur eine Pipeline in einer anderen Cloud liest, eine interne Verwaltungsoberfläche, ein Backupziel: Jeder dieser Dienste kann öffentlich hinter einer Anmeldung lauschen oder an einer privaten Adresse, die nur über den Tunnel erreichbar ist. Die zweite Variante beschränkt das, was ein Scanner findet, auf einen Gatewayport. Für Verbindungen zwischen Standorten bleibt sie eine einfache, gut verstandene Lösung.

Die nächste Frage lautet WireGuard oder IPsec; meist entscheidet die Gegenstelle. Ist sie eine Firewall-Appliance, das verwaltete Gateway eines Cloudanbieters oder das Netzwerkteam eines Partners, steht oft nur IPsec zur Wahl. Interoperabilität wiegt dann schwerer als Eleganz. Sind beide Enden Linux-Rechner unter eigener Kontrolle, lässt sich WireGuard schneller einrichten und leichter überblicken: eine kurze Konfigurationsdatei je Seite, ein öffentlicher Schlüssel je Peer und eine Liste der Adressen, von denen der jeweilige Peer senden darf. Das Entwurfspapier beziffert die Linux-Implementierung auf unter 4.000 Codezeilen, klein genug für ein Audit. Eine IPsec-Konfiguration unter Linux verbindet dagegen die Pakettransformation im Kernel mit einem gesonderten Schlüsselaustausch-Daemon und einer längeren Liste abzustimmender Optionen.

Die Betriebskosten liegen selten in der Software, die mit Linux und den meisten Firewalls geliefert wird. Sie liegen in der Aufmerksamkeit. Tunnel fallen nachts aus, die Schlüsselerneuerung scheitert Stunden nach einer Änderung an der Gegenstelle, und das einzige Symptom ist Stille: Pakete gehen hinein, nichts kommt zurück. Ein Tunnel verdient dieselbe Behandlung wie jeder andere Produktionsdienst: eine eigene Zustandsprüfung, einen eigenen Alarm und eine schriftliche Zuordnung, wer welches Ende betreut.

An manchen Stellen ist ein VPN auch das falsche Werkzeug. Ein vollständiger Tunnel ins Büronetz für jeden Mitarbeiter außerhalb des Büros macht ein ganzes Subnetz erreichbar, obwohl nur eine Anwendung gebraucht wurde. Nach dem Verbindungsaufbau vertraut dieses Subnetz dem verbundenen Rechner häufig pauschal. Anwendungsbezogener Zugang, bei dem jede Anfrage einzeln authentifiziert wird und der meist unter Zero Trust verkauft wird, passt besser, wenn Menschen auf Webanwendungen zugreifen sollen. Verbraucher-Apps, die ein VPN für mehr Privatsphäre bewerben, sind noch einmal etwas anderes. Sie verlagern das Vertrauen vom Internetanbieter zum VPN-Unternehmen und können die ursprüngliche Quell-IP-Adresse vor den Zielwebsites verbergen, garantieren allein aber keine Anonymität.

Wie es in der Praxis aussieht

Zwischen 2022 und 2024 lief geschützter Datenverkehr zwischen Google Cloud und lokalen Linux-Systemen über acht gemeinsam verwaltete und entstörte WireGuard- und IPsec-Tunnel. Die Verbindungen waren instabil gewesen, und ihre Diagnose hatte lange gedauert. Ein ausgefallener Tunnel konnte die Kommunikation zwischen Umgebungen unterbrechen. Ihre Konfiguration wurde vereinheitlicht, sodass kein Tunnel einen Sonderfall mehr bildete. Ihr Zustand wurde überwacht; wiederkehrende Routing- und Schlüsselaustauschprobleme wurden an der Ursache behoben, statt sie mit einem Neustart vorübergehend zu beseitigen. Danach liefen alle acht zuverlässig, und die wiederkehrenden Verbindungsstörungen hörten auf.

In denselben Jahren benötigte eine Organisation Daten aus einem entfernten Data Warehouse hinter einem IPsec-VPN. Für sechs ETL/ELT-Pipelines nach Google BigQuery war der Tunnel das erste Glied der Kette. Geschützte Verbindungen zum abgeschirmten Server wurden so eingerichtet, dass die Abholung ohne Aufsicht laufen konnte. Zeitgesteuerte Jobs luden anschließend komprimierte Archive mit Parquet-, CSV- und .bak-Dateien herunter, stellten sie in MSSQL und PostgreSQL wieder her, bereiteten sie dort auf und luden das Ergebnis in BigQuery. Über einen Tunnel, der nicht mehr auf einen Menschen wartete, dauerte der gesamte Lauf weniger als 20 Minuten statt mindestens drei Stunden Handarbeit. Die Daten wurden täglich statt wöchentlich aktualisiert. Das VPN ist der am wenigsten sichtbare Teil dieses Ergebnisses und der Teil, auf dem alles andere ruht. Eine Pipeline, die ihre Quelle nicht erreicht, bleibt beim ersten Schritt stehen, gleich wie gut das SQL dahinter ist.

Wo es schiefgeht

Große Pakete verschwinden, kleine kommen durch. Jeder Tunnel fügt Header hinzu. Das größte innen übertragbare Paket ist deshalb kleiner, als der äußere Pfad erlaubt. Eine WireGuard-Datennachricht fügt 32 Byte festen Overhead vor den äußeren UDP- und IP-Headern hinzu: insgesamt etwa 60 Byte über IPv4 und 80 über IPv6, zusätzlich zu einer möglichen Paketauffüllung. Ist die Tunnel-MTU zu hoch und verwirft der Pfad die ICMP-Nachrichten, die das melden würden, funktionieren Ping und SSH-Anmeldung, während Dateiübertragungen und TLS-Handshakes hängen. Die Prüfung sollte ein Paket voller Größe verwenden, das unterwegs nicht fragmentiert werden darf. Anschließend wird die Schnittstellen-MTU gesenkt oder die TCP-Segmentgröße passend begrenzt.

```
# 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
```

Zwei Standorte haben dieselben Adressen gewählt. Private Bereiche wie 10.0.0.0/8 und 192.168.0.0/16 werden überall wiederverwendet. Werden zwei Netze verbunden, die beide 10.0.0.0/24 nutzen, kann ein Router nicht erkennen, für welche Seite ein Paket bestimmt ist. Die Bereiche sollten vor dem ersten Tunnel geplant werden. Andernfalls bleibt Adressübersetzung an einem Ende, die jede spätere Protokollzeile und Firewallregel komplizierter macht.

Der Tunnel steht, die Route stimmt nicht. Ein Peer kann einen frischen Handshake anzeigen, während Datenverkehr weiterhin über die Standardroute abfließt: Die Route zum entfernten Subnetz fehlt, oder WireGuards Liste der für diesen Peer erlaubten Adressen enthält es nicht. Das Gegenstück bei IPsec sind abweichende Traffic Selectors an beiden Enden. IKEv2 engt sie auf die Schnittmenge ein oder lehnt sie mit einer Meldung TS_UNACCEPTABLE ab. Ein Tunnel kann daher stehen und weniger Verkehr übertragen, als beide Seiten beabsichtigt hatten.

Die Schlüsselerneuerung scheitert lange nach der Änderung. Beide Protokolle ersetzen aktive Sitzungsschlüssel im Lauf der Zeit. Eine einseitig eingeführte Abweichung, etwa ein geändertes Proposal oder ein ausgetauschter Schlüssel, kann deshalb erst beim Ersetzen der aktuellen Schlüssel auffallen. WireGuard

beginnt bei laufendem Datenverkehr ungefähr alle zwei Minuten eine neue Sitzung. IPsec-Laufzeiten sind lokale Richtlinien an jedem Ende und müssen nicht übereinstimmen. Bei WireGuard ist das Alter des letzten erfolgreichen Handshakes zusammen mit dem erwarteten Datenverkehr oder gezielten Zustandsprüfungen zu beurteilen. Ein alter Handshake eines untätigen Peers beweist allein keinen Ausfall. IKEv2s Erreichbarkeitsprüfung, oft Dead Peer Detection genannt, sollte aktiviert werden, damit ein Gateway einen stummen Peer erkennt, statt weiter ins Leere zu senden.

Verbunden heißt vertrauenswürdig. Bei vielen Remote-Access-Konfigurationen gilt ein Laptop im VPN als Rechner im Büro. Ein gestohlener Zugang reicht dann für alles im Subnetz. Das Gateway sollte filtern, was jeder VPN-Client erreichen darf. Die dahinterliegenden Dienste müssen ihre Authentifizierung behalten. Ob Namensauflösung und Internetverkehr durch den Tunnel oder an ihm vorbeilaufen, ist bewusst festzulegen.

Weiterführende Lektüre

- RFC 4026, Abschnitt 3.10 — die allgemeine VPN-Definition der IETF und der Hinweis, dass Verschlüsselung außerhalb des Auftrags der Arbeitsgruppen liegt.
- WireGuard: Next Generation Kernel Network Tunnel — das Entwurfspapier zu Cryptokey Routing, Handshake und den Timern für die Schlüsselerneuerung.
- RFC 4301 — die Sicherheitsarchitektur für IP, der jede IPsec-Implementierung folgt.
- RFC 7296 — IKEv2 mit eingeengten Traffic Selectors, Laufzeiten als lokaler Richtlinie und Erreichbarkeitsprüfung.
- RFC 4364 — BGP/MPLS-IP-VPNs der Provider, mit überlappenden Adressräumen und ohne kryptografische Vertraulichkeit.

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist ein VPN?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

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

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://engineer.company/de/glossary/vpn/