Engineer

VPN

🖧 un réseau logiquement séparé sur une infrastructure partagée

Ce que c’est

Un VPN, abréviation de virtual private network, ou réseau privé virtuel, est un ensemble de tunnels ou de chemins étiquetés permettant à un groupe fermé de machines de communiquer avec leurs propres adresses et routes, quels que soient les réseaux traversés par les paquets. La terminologie de l’IETF en fait une question de séparation plutôt que de secret : le groupe est tenu à l’écart des autres utilisateurs, et le chiffrement est mentionné comme un complément possible, hors du périmètre des groupes de travail. Deux formes dominent l’usage courant. Un VPN de site à site relie des réseaux entiers, par exemple un bureau et un projet cloud, au moyen d’une passerelle à chaque extrémité. Un VPN d’accès distant relie un ordinateur portable ou un téléphone à un réseau dont il est éloigné.

Des technologies très différentes portent ce nom. IPsec protège les paquets IP dans la pile réseau d’un hôte ou d’une passerelle de sécurité et utilise couramment IKEv2 pour négocier ses clés ; c’est ce que prennent en charge la plupart des pare-feu, routeurs et passerelles cloud administrées. WireGuard est un tunnel plus récent qui apparaît comme une interface réseau ordinaire, passe par UDP, identifie chaque pair par une clé publique et propose délibérément une seule suite cryptographique fixe au lieu d’un menu à négocier. OpenVPN fonctionne comme un processus en espace utilisateur et établit ses clés avec TLS. Les VPN d’opérateur fondés sur BGP et MPLS séparent les clients à l’intérieur du réseau dorsal d’un fournisseur et, selon leur propre spécification, n’assurent aucune confidentialité cryptographique. Lorsqu’un contrat, un diagramme ou un fournisseur de pare-feu parle de VPN, mieux vaut demander laquelle de ces technologies est visée.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce qu'un VPN ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Du Wi-Fi, des pare-feu et des accès à distance configurés pour travailler de partout, en laissant entrer uniquement les personnes autorisées.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 30 instances VPS Ubuntu Linux administrées — 30 serveurs Linux gérés, avec récupération prévue

30 instances VPS Ubuntu Linux administrées Contactez-nous →

Pourquoi c’est important

La décision qu’un VPN tranche généralement est de savoir comment deux sites qui doivent communiquer peuvent le faire sans exposer le service qui les relie sur l’Internet public. Une base de données lue uniquement par un pipeline dans un autre cloud, un panneau d’administration interne, une cible de sauvegarde : chacun peut écouter sur une adresse publique derrière une authentification ou sur une adresse privée que seul le tunnel rend accessible. La seconde option réduit ce qu’un scanner peut trouver à un seul port de passerelle. Pour les liaisons entre sites, elle reste la réponse simple et bien comprise.

WireGuard ou IPsec est la question suivante, et l’autre extrémité en décide généralement. S’il s’agit d’un pare-feu matériel, d’une passerelle administrée par un fournisseur cloud ou de l’équipe réseau d’un partenaire, IPsec est souvent la seule option disponible, et l’interopérabilité l’emporte sur l’élégance. Si les deux extrémités sont des machines Linux sous votre contrôle, WireGuard est plus rapide à installer et plus facile à comprendre : un court fichier de configuration par côté, une clé publique par pair et une liste des adresses depuis lesquelles chaque pair est autorisé à émettre. L’article qui présente sa conception décrit une implémentation Linux de moins de 4 000 lignes de code, assez peu pour être auditées. Une configuration IPsec sous Linux associe quant à elle la transformation des paquets dans le noyau à un démon distinct d’échange de clés et à une liste plus longue d’options à mettre en accord.

Le coût d’exploitation est rarement le logiciel, fourni avec Linux et avec la plupart des pare-feu. Le coût, c’est l’attention à y consacrer. Les tunnels tombent la nuit, le renouvellement des clés échoue des heures après une modification à l’autre extrémité, et le seul symptôme est le silence : les paquets entrent et rien ne revient. Un tunnel mérite le même traitement que tout autre service de production, avec son propre contrôle d’état, sa propre alerte et une note écrite indiquant qui est responsable de chaque extrémité.

Un VPN est aussi un mauvais outil dans certains cas. Donner à chaque salarié travaillant à distance un tunnel complet vers le réseau du bureau ouvre l'accès à un sous-réseau entier alors que la personne avait besoin d'une seule application. Une fois la connexion établie, tout ce qui se trouve dans ce sous-réseau a tendance à lui faire confiance. L'accès par application, où chaque appel à l'application est authentifié séparément et qui est généralement vendu sous le nom de zero trust, convient mieux lorsque les utilisateurs sont des personnes et les cibles des applications web. Les applications grand public qui vantent un VPN pour protéger la vie privée constituent encore une troisième catégorie : elles déplacent la confiance du fournisseur d'accès à Internet vers l'entreprise de VPN et peuvent masquer l'adresse IP source d'origine aux sites destinataires, mais ne garantissent pas à elles seules l'anonymat.

À quoi cela ressemble en pratique

Entre 2022 et 2024, le trafic sécurisé entre Google Cloud et des systèmes Linux sur site passait par huit tunnels WireGuard et IPsec administrés et dépannés comme un ensemble. Ils étaient fragiles et longs à diagnostiquer ; un tunnel défaillant pouvait couper la communication entre environnements. Leur configuration a été standardisée pour qu'aucun ne reste un cas particulier, leur état a été supervisé et les problèmes récurrents de routage et d'échange de clés ont été corrigés à la racine au lieu d'être effacés par un redémarrage. Les huit ont ensuite fonctionné de manière fiable, et les incidents de connectivité récurrents ont cessé.

Durant les mêmes années, une organisation avait besoin de données provenant d'un entrepôt de données distant situé derrière un VPN IPsec. Pour six pipelines ETL/ELT alimentant Google BigQuery, le tunnel était le premier maillon de la chaîne : des connexions sécurisées au serveur protégé ont été établies pour permettre une récupération sans surveillance. Des tâches planifiées téléchargeaient ensuite des archives compressées de fichiers Parquet, CSV et .bak, les restauraient et les préparaient dans des zones intermédiaires de MSSQL et PostgreSQL, puis chargeaient le résultat dans BigQuery. Avec un tunnel qui n'attendait plus l'intervention d'une personne, l'exécution complète prenait moins de 20 minutes contre au moins trois heures de travail manuel, et les données étaient actualisées chaque jour au lieu de chaque semaine. Le VPN est la partie la moins visible de ce résultat et celle sur laquelle tout repose : un pipeline qui ne peut atteindre sa source s'arrête à la première étape, quelle que soit la qualité du SQL qui suit.

Où les problèmes surviennent

Les gros paquets disparaissent tandis que les petits passent. Chaque tunnel ajoute des en-têtes : le plus gros paquet pouvant y tenir est donc plus petit que ce que permet le chemin extérieur. Un message de données WireGuard ajoute 32 octets de surcharge fixe avant les en-têtes UDP et IP externes, soit environ 60 octets au total sur IPv4 et 80 sur IPv6, en plus d'un éventuel bourrage du paquet. Lorsque la MTU du tunnel est trop élevée et que le chemin rejette les messages ICMP qui devraient le signaler, ping et une connexion SSH fonctionnent alors que les transferts de fichiers et les négociations TLS se bloquent. Testez avec un paquet de taille maximale interdisant la fragmentation, puis réduisez la MTU de l'interface ou limitez la taille des segments TCP pour qu'ils tiennent.

```
# 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
```

Deux sites ont choisi les mêmes adresses. Les plages privées comme 10.0.0.0/8 et 192.168.0.0/16 sont réutilisées partout. Relier deux réseaux qui utilisent tous deux 10.0.0.0/24 laisse le routeur sans moyen de déterminer de quel côté doit aller un paquet. Prévoyez les plages avant le premier tunnel ou acceptez une traduction d'adresses à une extrémité, ce qui complique ensuite chaque ligne de journal et chaque règle de pare-feu.

Le tunnel est actif et la route est erronée. Un pair peut afficher une négociation récente alors que le trafic continue de sortir par la route utilisée faute de correspondance plus précise, parce que la route vers le sous-réseau distant manque ou que la liste WireGuard des adresses autorisées pour ce pair l'omet. Dans IPsec, l'équivalent est constitué de sélecteurs de trafic différents aux deux extrémités. IKEv2 les réduit à leur intersection ou les refuse par une notification TS_UNACCEPTABLE. Un tunnel peut ainsi s'établir en transportant moins que ce que chacune des parties avait prévu.

Le renouvellement des clés échoue longtemps après la modification. Les deux protocoles remplacent les clés de session actives au fil du temps. Une divergence introduite à une extrémité, telle qu'une proposition modifiée ou une clé remplacée, peut donc ne se révéler qu'au remplacement des clés courantes.

WireGuard démarre une nouvelle session environ toutes les deux minutes tant que du trafic circule. Les durées de vie IPsec relèvent de la politique locale de chaque extrémité et n'ont pas à coïncider. Pour WireGuard, interprétez l'ancienneté de la dernière négociation réussie en fonction du trafic attendu ou des sondes d'état : une ancienne négociation d'un pair inactif ne suffit pas à établir une défaillance. Activez le contrôle de présence d'IKEv2, souvent appelé dead peer detection, pour qu'une passerelle détecte un pair silencieux au lieu d'envoyer les paquets dans un trou noir.

Être connecté devient être digne de confiance. Dans de nombreuses configurations d'accès distant, un ordinateur portable sur le VPN est traité comme s'il se trouvait au bureau. Un seul identifiant volé donne alors accès à tout le sous-réseau. Filtrez sur la passerelle ce que chaque client VPN peut atteindre, conservez l'authentification des services situés derrière et décidez délibérément si les résolutions de noms et le trafic Internet passent par le tunnel ou à côté.

Pour aller plus loin

- RFC 4026, section 3.10 — la définition générique d'un VPN par l'IETF et la remarque plaçant le chiffrement hors du mandat des groupes de travail.
- WireGuard : Next Generation Kernel Network Tunnel — l'article de conception : routage par clés cryptographiques, négociation et temporisateurs du renouvellement des clés.
- RFC 4301 — l'architecture de sécurité IP suivie par chaque implémentation d'IPsec.
- RFC 7296 — IKEv2, avec la réduction des sélecteurs de trafic, les durées de vie comme politique locale et le contrôle de présence.
- RFC 4364 — les VPN IP BGP/MPLS d'opérateur, avec des espaces d'adressage qui se chevauchent et sans confidentialité cryptographique.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu'est-ce qu'un VPN ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

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

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/vpn/