Engineer

VPN

🖧 логічно відокремлена мережа на спільній інфраструктурі

Що це таке

Абревіатура VPN розшифровується як virtual private network, українською — віртуальна приватна мережа. За нею стоїть набір тунелів або позначених шляхів, якими замкнена група машин звертається одна до одної за власними адресами й маршрутами, хоч би через які мережі йшли пакети дорогою. Термінологія IETF наголошує на відокремленні, а не на таємності: групу тримають окремо від інших користувачів, а шифрування згадано лише як можливе доповнення, що лежить поза межами завдань робочих груп. На практиці переважають два різновиди. Site-to-site з'єднує цілі мережі, скажімо офіс і хмарний проєкт, через шлюз на кожному кінці. VPN віддаленого доступу під'єднує один ноутбук чи телефон до мережі, від якої він фізично далеко.

Під однією назвою ховаються дуже різні технології. IPsec захищає IP-пакети всередині мережевого стека хоста або шлюзу безпеки й зазвичай використовує IKEv2 для узгодження ключів; саме цією мовою говорить більшість брандмауерів, маршрутизаторів і керованих хмарних шлюзів. WireGuard — молодший тунель: у системі він виглядає як звичайний мережевий інтерфейс, ходить поверх UDP, упізнає кожного учасника за його відкритим ключем і свідомо пропонує один фіксований набір шифрів замість меню, про яке треба домовлятися. OpenVPN працює як процес у просторі користувача й узгоджує ключі через TLS. Операторські VPN на основі BGP і MPLS розмежовують клієнтів усередині магістралі провайдера і, за власною специфікацією, криптографічної конфіденційності не дають узагалі. Тож коли в договорі, на діаграмі чи в рекламі постачальника брандмауерів написано VPN, варто уточнити, котру з цих речей мають на увазі.

Застосуйте поняття до рішення

Застосуйте «Що таке VPN?» до конкретного рішення. Ми можемо пов'язати поняття із системою, яку ви створюєте або купуєте. Wi-Fi, фаєрволи і віддалений доступ налаштовані так, щоб працювати можна було звідусіль, а заходити — лише своїм.

Переглянути наші послуги Зв'язатися з нами →

Перевірте припущення за терміном

Використайте пояснення та пов'язані роботи, щоб сформулювати запитання для проєкту. Ми можемо перевірити припущення разом до вибору інструмента. Керувала 30 інстансами Ubuntu Linux VPS — 30 серверів Linux під управлінням, із планом відновлення

Керувала 30 інстансами Ubuntu Linux VPS Зв'язатися з нами →

Чому це важливо

Здебільшого VPN відповідає на одне питання: як двом місцям, яким треба обмінюватися даними, робити це, не виставляючи сервіс між ними у відкритий інтернет. База даних, яку читає лише пайплайн в іншій хмарі, внутрішня адмінпанель, сховище для резервних копій — кожне з них може слухати публічно за формою входу або слухати на приватній адресі, до якої веде тільки тунель. Другий варіант зводить усе, що здатен знайти сканер, до одного порту на шлюзі, і для зв’язку між майданчиками це досі найпростіша й найкраще вивчена відповідь.

Далі постає вибір між WireGuard та IPsec, і зазвичай його робить протилежний кінець. Якщо там апаратний брандмауер, керований шлюз хмарного провайдера або мережева команда партнера, IPsec часто виявляється єдиним доступним варіантом, і сумісність важить більше за елегантність. Якщо ж обидва кінці — Linux-машини під вашим власним контролем, WireGuard швидше налаштувати й легше осягнути: по одному короткому файлу конфігурації на кожен бік, по одному відкритому ключу на учасника й перелік адрес, з яких кожному учасникові дозволено надсилати пакети. Стаття з описом його дизайну оцінює реалізацію для Linux у менш ніж 4 000 рядків коду, а такий обсяг реально перевірити рядок за рядком. Налаштування IPsec на Linux натомість поєднує перетворення пакетів у ядрі з окремим демоном обміну ключами та довшим переліком параметрів, про які обидві сторони мають домовитися.

Гроші на експлуатацію рідко йдуть на програмне забезпечення: воно постачається разом із Linux і з більшістю брандмауерів. Платити доводиться увагою. Тунелі падають уночі, оновлення ключів ламається через кілька годин після того, як хтось змінив параметр на іншому боці, а єдиний симптом — тиша: пакети йдуть усередину, а назад не приходить нічого. Тунель

заслуговує того самого ставлення, що й будь-який інший продакшн-сервіс, тобто власної перевірки стану, власного сповіщення і записаної нотатки про те, хто відповідає за кожен його кінець.

Подекуди VPN — взагалі не той інструмент. Якщо кожному віддаленому працівникові видати повний тунель до офісної мережі, людина дістає доступ до цілої підмережі, хоча їй потрібен був один застосунок, а щойно з'єднання встановлено, усе в цій підмережі схильне їй довіряти. Доступ на рівні застосунку, де кожен запит автентифікується окремо і який здебільшого продають під назвою zero trust, краще підходить, коли користувачі — люди, а цілі — вебзастосунки. Споживчі застосунки, що рекламують VPN заради приватності, — це ще третя річ: вони переносять довіру з інтернет-провайдера на VPN-компанію і можуть приховувати початкову IP-адресу джерела від сайтів призначення, але самі по собі не гарантують анонімності.

Як це виглядає на практиці

У 2022–2024 роках захищений трафік між Google Cloud і локальними Linux-системами йшов через вісім тунелів WireGuard та IPsec, які обслуговували як один набір. До того вони були крихкими, діагностувати їх було повільно, а мертвий тунель міг обірвати зв'язок між середовищами. Конфігурацію стандартизували, щоб жоден тунель не лишався особливим випадком, їхній стан почали моніторити, а повторювані проблеми з маршрутизацією та обміном ключами усували в корені, а не знімали перезапуском. Відтоді всі вісім працювали надійно, і повторювані інциденти зі з'єднанням припинилися.

Ті самі роки дали й інший приклад: організації потрібні були дані з віддаленого сховища, що стояло за IPsec VPN. Для шести ETL/ELT-пайплайнів, що наповнювали Google BigQuery, тунель став першою ланкою ланцюга: захищені з'єднання з тим сервером налагодили так, щоб отримання даних ішло без нагляду. Далі заплановані задачі завантажували стиснуті архіви з файлами Parquet, CSV і .bak, відновлювали їх, розкладали по проміжних схемах у MSSQL і PostgreSQL та вантажили результат у BigQuery. Ручна робота тривалістю щонайменше 3 години скоротилася до менш ніж 20 хвилин наскрізно, а синхронізація даних перейшла з щотижневої на щоденну. VPN тут — найменш помітна частина результату і водночас та, на якій тримається все інше: пайплайн, що не може дістатися свого джерела, зупиняється на першому ж кроці, хоч яким би добрим був SQL за ним.

Де виникають проблеми

Великі пакети зникають, а малі проходять. Кожен тунель додає власні заголовки, тож найбільший пакет, що вміщується всередині, менший, ніж дозволяє шлях зовні. Пакет даних WireGuard додає 32 байти сталих накладних витрат ще до зовнішніх заголовків UDP та IP, тобто разом близько 60 байтів поверх IPv4 і 80 поверх IPv6, не враховуючи можливого доповнення пакета. Коли MTU тунелю завищено, а шлях відкидає ICMP-повідомлення, які мали б про це сповістити, ping і вхід по SSH працюють, а передавання файлів і TLS-рукостискання зависають. Перевірте шлях пакетом повного розміру із забороною фрагментації, а тоді зменште MTU інтерфейсу або обмежте розмір TCP-сегмента, щоб пакети вміщалися.

```
# Коли кожен учасник WireGuard востаннє завершив рукостискання, у Unix-часі
wg show wg0 latest-handshakes
# Пакет на 1 420 байтів, який не можна фрагментувати дорогою
ping -M do -s 1392 -c 3 10.0.0.2
# Який інтерфейс і маршрут ядро обирає до віддаленого хоста
ip route get 10.20.0.5
```

Два майданчики обрали однакові адреси. Приватні діапазони на кшталт 10.0.0.0/8 і 192.168.0.0/16 повторно використовують усюди, і якщо з’єднати дві мережі, що обидві займають 10.0.0.0/24, маршрутизатор не зможе визначити, до якого боку прямує пакет. Сплануйте діапазони до першого тунелю або змиріться з трансляцією адрес на одному кінці, яка відтак ускладнює кожен рядок журналу й кожне правило брандмауера.

Тунель піднявся, а маршрут хибний. Учасник може показувати свіже рукостискання, тоді як трафік і далі йде усталеним маршрутом, бо маршруту до віддаленої підмережі немає або бо перелік дозволених адрес WireGuard для цього учасника її не містить. В IPsec відповідником є селектори трафіку (traffic selectors), що різняться на двох кінцях. IKEv2 або звужує їх до перетину, або відхиляє повідомленням TS_UNACCEPTABLE, тож тунель може піднятися й переносити менше, ніж планувала будь-яка зі сторін.

Оновлення ключів дає збій через тривалий час після зміни. Обидва протоколи з часом замінюють активні сеансові ключі, тож розбіжність, внесена на одному кінці, скажімо відредагована пропозиція чи замінений ключ, може проявитися лише тоді, коли поточні ключі замінюють. WireGuard починає нову сесію приблизно кожні дві хвилини, поки йде трафік. Строки дії

ключів в IPsec — локальна політика кожного кінця, і однаковими вони бути не зобов'язані. Для WireGuard вік останнього вдалого рукостискання слід оцінювати разом з очікуваним трафіком або перевірними запитами: саме по собі давнє рукостискання неактивного учасника ще не свідчить про збій. Увімкніть перевірку живучості IKEv2, яку часто називають dead peer detection, щоб шлюз помічав мовчазного учасника, а не надсилав пакети в чорну діру.

Під'єднаний означає довірений. У багатьох схемах віддаленого доступу ноутбук, під'єднаний до VPN, сприймають так, ніби він стоїть в офісі, тож одні викрадені облікові дані відкривають усе в цій підмережі. Фільтруйте на шлюзі, куди може дістатися кожен VPN-клієнт, залишайте автентифікацію на сервісах за ним і свідомо вирішуйте, чи йдуть DNS-запити та інтернет-трафік через тунель чи в обхід нього.

Що почитати далі

- RFC 4026, section 3.10 — загальне визначення VPN від IETF і застереження, що шифрування лежить поза межами завдань робочих груп.
- WireGuard: Next Generation Kernel Network Tunnel — стаття про дизайн: маршрутизація за криптоключами, рукостискання й таймери, що керують оновленням ключів.
- RFC 4301 — архітектура безпеки для IP, на яку спирається кожна реалізація IPsec.
- RFC 7296 — IKEv2, зокрема звуження селекторів трафіку, строки дії як локальна політика і перевірка живучості.
- RFC 4364 — BGP/MPLS IP VPN, операторський різновид з адресними просторами, що перетинаються, і без криптографічної конфіденційності.

Словник

Обирайте за фактичними умовами

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Зробіть термінологію практичною

Запитайте, як «Що таке VPN?» стосується вашої організації. Конкретного прикладу з поточної системи достатньо для початку розмови.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

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

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/glossary/vpn/