Engineer

Tor

🕸 мережа, що веде трафік через добровільні вузли

Що це таке

Хто з ким розмовляє — саме це Tor приховує від того, хто стежить за каналом зв'язку. Кожне з'єднання проходить крізь ланцюжок машин, і жодна з них не дізнається водночас, звідки трафік вийшов і куди прямує. Ланцюжок обирає клієнт — програма tor, що працює на комп'ютері самого читача, — і здебільшого він складається з трьох ретрансляторів: вартового (guard), якого клієнт тривалий час використовує як вхід, проміжного та вихідного (exit), що відкриває останнє з'єднання до адресата. Клієнт будує ланцюжок по одному стрибку, домовляється з кожним ретранслятором про окремий ключ і загортає кожен шматок даних в окремий шар шифрування для кожного стрибка. Кожен ретранслятор знімає свій шар і знає лише сусіда перед собою та сусіда після себе. Саме ці вкладені шари й дали цибулю в назві статті про дизайн, The Second-Generation Onion Router. У розмові всі ретранслятори разом називають мережею Tor, tor із малої літери — це програма, а Tor Browser — браузер, зібраний так, щоб нею користуватися.

Дані рухаються комірками (cells) фіксованого розміру, тож ретранслятор бачить потік однакових блоків, а не форму початкових пакетів. Кілька TCP-потоків можуть ділити один ланцюжок, коли їхні вимоги до ізоляції сумісні. Клієнт будує ланцюжки як заздалегідь, так і на вимогу та виводить їх з ужитку залежно від віку й використання; довготривалий потік може лишатися на початковому ланцюжку, а деякі налаштування ізоляції дозволяють використовувати його довше. Застосунки звертаються до клієнта через локальний SOCKS-проксі, і цим шляхом іде тільки TCP; стаття про дизайн прямо каже, що протоколи на кшталт UDP вона не тунелює. Ретранслятори тримають волонтери. Кожен публікує дескриптор зі своїми ключами, адресою, пропускною здатністю та політикою виходу. Невелика група directory authorities голосує, які ретранслятори внести до переліку, і підписує результат як консенсус — документ, який кожен клієнт завантажує, перш ніж вибрати шлях.

Застосуйте поняття до рішення

Застосуйте «Що таке Tor?» 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

Для того, хто тримає публічний вебсайт, Tor передусім — факт про аудиторію. Читач, що прийшов через Tor, виглядає так, ніби звертається з адреси вихідного ретранслятора, а не зі своєї, а перелік ретрансляторів публічний навмисно, бо кожному клієнтові він потрібен, щоб вибрати шлях. Отже, сайт може розпізнати трафік Tor і поводитися з ним інакше. Сам Tor Project вважає, що оператори мають право його блокувати, хоч і сподівається, що вони цього не робитимуть. Лишається вирішити, що робити з такими читачами: обслуговувати їх, як усіх, сповільнювати, ставити перед ними перевірку чи дати їм вхід, який узагалі не виходить за межі мережі Tor. Останнє й робить onion-адреса.

Варто точно знати, що Tor обіцяє, бо стаття про дизайн сама перелічує, чого вона на себе не бере. Вона не стверджує, що встоїть проти спостерігача, який бачить обидва кінці з'єднання й порівнює час та обсяг, а документація проєкту додає, що дослідникам невідомий практичний дизайн із низькою затримкою, який би надійно з цим упорався. Базовий протокол не приховує самого використання Tor; мости з підключуваними транспортами (pluggable transports) додають способи маскування такого трафіку. І Tor не шифрує останній відрізок від вихідного ретранслятора до адресата: для цього стрибка застосунку потрібне власне шифрування.

Поруч із VPN довіра розподілена інакше. Постачальник VPN бачить і користувача, і адресата, і його просто просять не дивитися. У Tor окремий ретранслятор не бачить обох кінців. Для більшості шляхів правила вибору розділяють ретранслятори з однієї оголошеної родини й за замовчуванням уникають спільної підмережі IPv4 /16 або IPv6 /32; є задокументовані винятки, а межі підмереж налаштовуються. Платити доводиться затримкою, адже звичайний вихідний ланцюжок перетинає машини трьох волонтерів, тож читачам Tor найкраще служать легкі сторінки з невеликою кількістю

обмінів. Onion-адреса потребує процесу tor і приватного ключа, який треба берегти, але не відкритого вхідного порту, тому підходить для невеликої інфраструктури.

Як це виглядає на практиці

Сайт компанії можна читати й через Tor. Сторінка про термінал публікує onion-адресу поряд із командою `curl`, що завантажує текст у Markdown через локальний клієнт tor. Адреса навмисно має звичайний `http://`: onion-адреса версії 3 кодує відкритий ключ ідентичності сервісу разом із контрольною сумою та байтом версії. Tor автентифікує сервіс і шифрує ланцюжок ще до обміну HTTP. Публічний вебсертифікат для такої автентифікації onion-адреси не потрібен.

Onion-сервіс потребував місця для процесу tor на хості публічних сервісів компанії у реалізації від вересня 2026 року: одне ядро й близько 464 МБ придатної до використання пам'яті. На цьому хості вже термінувався TLS для семи доменів і працював git-фордж. Місце для цього процесу не обґрунтовували припущеннями, а виміряли за даними вибірок, зафіксованих протягом доби на цьому хості з 512 МБ: найменше спостережене значення доступної пам'яті становило близько 310 МБ із 464, використання підкачування — 2,6%, а процесор 99,7% часу простоював, тож Tor запустили поруч з іншими сервісами.

Сторінка про конфіденційність фіксує вибір компанії щодо підрахунку читачів. Застосунки Gemini та Gopher не ведуть журналу звернень, а їхні щоденні лічильники зберігають лише загальну кількість запитів. Gopher також має журнал з'єднань операційної системи, який містить адресу джерела; строк зберігання цього журналу — 30 днів. Компанія каже, що через Tor не рахує взагалі нічого й не пропонує налаштування, яке вмикало б підрахунок. Це вибір оператора щодо приватності: Tor приховує мережеву адресу читача, але не заважає сервісу рахувати запити. На сторінці сказано, що компанія воліє не знати, ніж мати таку змогу.

Де виникають проблеми

Ім'я з'ясовують поза Tor. Програма, що спрямовує з'єднання до SOCKS-проксі, може все одно спершу сама визначити адресу хоста через звичайний резолвер, і цей запит повідомляє локальній мережі та постачальникові DNS, який сайт відвідують. Далі з'єднання йде крізь Tor, але адресат уже витік. У

`curl` різниця — в одному параметрі: з `--socks5` ім'я розв'язується локально, з `--socks5-hostname` його передають проксі, і адресу визначає вихідний ретранслятор.

```
# Визначає адресу локально, тоді під'єднується через проксі
curl -s --socks5 127.0.0.1:9050 https://example.org/
# Передає ім'я tor; адресу шукає вихідний ретранслятор
curl -s --socks5-hostname 127.0.0.1:9050 https://example.org/
```

Відкритий текст після виходу. Tor шифрує стрибки між ретрансляторами, але не останній. Вихідний ретранслятор відкриває звичайне TCP-з'єднання до адресата й надсилає те, що дав йому застосунок, тож форму входу, надіслану звичайним HTTP, може прочитати оператор цього ретранслятора й будь-хто в мережі за ним. Віддавайте через HTTPS усе, що виходить за межі мережі Tor. Onion-сервіс обходить це питання, бо його трафік мережі не покидає.

Одна адреса за багатьох читачів. Обмеження частоти запитів і блокування, прив'язані до адреси клієнта, сприймають вихідний ретранслятор як одного відвідувача, хоча ним водночас користується багато людей. Ліміт, розрахований на одну людину, відрізає всіх, чий ланцюжок випадково закінчується там, а блокування, яке заслужив один зловмисник, падає на всіх. Вирішіть свідомо, як поводитися з вихідними адресами, а не покладайтеся на загальне правило для кожної адреси.

Особа подорожує всередині ланцюжка. Tor приховує мережеву адресу й нічого не робить із тим, що каже застосунок. Вхід в особистий обліковий запис, характерні налаштування браузера чи документ, що під час відкриття щось завантажує, пов'язують сесію з людиною, хоч би скільки ретрансляторів стояло між ними. Документація проєкту зазначає, що трафік застосунків і далі треба очищати на боці користувача. Цю роботу бере на себе Tor Browser, а звичайний браузер, просто спрямований на проксі, — ні.

Вихідний ретранслятор на домашньому підключенні. На вартові й проміжні ретранслятори скарги на зловживання надходять рідко. Вихідний — це те місце, звідки адресати бачать трафік, тож скарги та зрідка юридичні запити надходять тому, хто його тримає, а посібник Tor Project для операторів радить не запускати такий ретранслятор із дому. Волонтер з

однією домашньою адресою може натомість тримати міст (bridge) — ретранслятор поза публічним переліком, який той самий посібник радить саме для такого випадку.

Очікування, що UDP працюватиме. Голосові дзвінки, багато ігор та інструменти, що надсилають власні DNS-запити, покладаються на UDP, а Tor переносить лише TCP-потоки. Такі програми через нього не працюють, а та, яку не змусили йти через проксі, може просто під'єднатися напряму, в обхід Tor, і ніяк про це не повідомити.

Що почитати далі

- Tor Specifications — специфікації протоколу, вибору шляху, системи каталогів та onion-сервісів в одному місці.
- Tor: The Second-Generation Onion Router — стаття про дизайн: ланцюжки, комірки, політики виходу та прямий перелік того, чого дизайн не намагається робити.
- Tor Path Specification — як клієнт обирає вартовий, проміжний і вихідний ретранслятори та яким ретрансляторам заборонено ділити шлях.
- Types of relays on the Tor network — вартові, проміжні, вихідні ретранслятори й мости та юридичні ризики, які кожен із них несе для свого оператора.
- HTTPS encryption and Tor — інтерактивна схема того, що бачить той, хто підслуховує, з Tor, з HTTPS, з обома й без жодного.

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 Tor?» 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/tor/