Engineer

Tor

réseau qui achemine le trafic via des relais bénévoles

Ce que c’est

Tor dissimule qui communique avec qui aux personnes qui observent les échanges sur le réseau : chaque connexion passe par une chaîne de machines dont aucune ne connaît à la fois le départ et l’arrivée du trafic. Le client, un programme appelé tor qui tourne sur l’ordinateur du lecteur, choisit cette chaîne, généralement longue de trois relais : un relais de garde qu’il réutilise comme point d’entrée, un relais intermédiaire et une sortie qui établit la connexion finale vers la destination. Le client construit ce circuit un saut à la fois et convient d’une clé distincte avec chaque relais, puis enveloppe chaque donnée d’une couche de chiffrement par saut. Chaque relais retire sa couche et ne connaît que le voisin précédent et le suivant. Ces couches imbriquées sont l’oignon du titre de l’article de conception, The Second-Generation Onion Router. Dans l’usage courant, l’ensemble des relais est le réseau Tor, tor en minuscules est le programme et Tor Browser est le navigateur préparé pour l’utiliser.

Les données circulent dans des cellules de taille fixe : un relais voit donc un flux de blocs uniformes plutôt que la forme des paquets d’origine. Plusieurs flux TCP peuvent partager un circuit si leurs exigences d’isolation sont compatibles. Le client construit des circuits à l’avance et à la demande, puis les retire selon leur âge et leur utilisation ; un flux de longue durée peut rester sur son circuit d’origine et certains réglages d’isolation permettent une réutilisation prolongée. Les applications atteignent le client par un proxy SOCKS local, et seul TCP emprunte cette voie : l’article de conception précise qu’il ne transporte pas dans un tunnel des protocoles comme UDP. Des bénévoles exploitent les relais, chacun publiant un descripteur avec ses clés, son adresse, sa bande passante et sa politique de sortie. Un petit ensemble d’autorités d’annuaire vote pour déterminer les relais à publier et signe le résultat dans un document de consensus que chaque client récupère avant de choisir un chemin.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce que Tor ? » 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

Pour l’exploitant d’un site public, Tor est d’abord une réalité de son lectorat. Un lecteur arrivant par Tor semble venir de l’adresse d’un relais de sortie plutôt que de la sienne ; la liste des relais est volontairement publique, puisque chaque client en a besoin pour choisir son chemin. Un site peut donc reconnaître le trafic Tor et le traiter différemment. Le Tor Project considère lui-même que les exploitants ont le droit de le bloquer, même s’il espère qu’ils ne le feront pas. Reste à décider comment accueillir ces lecteurs : les servir comme les autres, les ralentir, leur imposer une vérification ou leur donner un accès qui ne quitte jamais le réseau Tor, ce que permet une adresse onion.

Il faut être précis sur les promesses de Tor, car l’article de conception énumère ce qu’il ne couvre pas. Il ne prétend pas résister à un observateur capable de surveiller les deux extrémités d’une connexion et d’en comparer la chronologie et le volume des échanges ; la documentation du projet ajoute que les chercheurs ne connaissent aucune conception pratique à faible latence qui y parvienne de façon fiable. Le protocole de base ne cache pas l’utilisation de Tor elle-même ; des ponts munis de transports enfichables offrent des moyens de déguiser ce trafic. Tor ne chiffre pas non plus le dernier trajet, du relais de sortie à la destination : l’application doit apporter son propre chiffrement pour ce saut.

Par rapport à un VPN, la confiance est répartie autrement. Un fournisseur VPN voit à la fois l’utilisateur et la destination, et on lui demande de détourner le regard. Avec Tor, aucun relais ne voit les deux. Pour la plupart des chemins, les règles de sélection séparent les relais d’une même famille déclarée et évitent par défaut un sous-réseau IPv4 /16 ou IPv6 /32 commun ; des exceptions et des limites de sous-réseau configurables sont documentées. Le prix est la latence, car un circuit de sortie ordinaire traverse trois machines de bénévoles : les pages légères qui demandent peu d’allers-retours servent donc mieux les lecteurs Tor. Proposer une adresse onion exige un processus tor et une clé privée à protéger, mais aucun port entrant ouvert, ce qui convient à une petite infrastructure.

À quoi cela ressemble en pratique

Le site de l'entreprise est accessible par Tor. La page de ligne de commande publie l'adresse onion à côté d'une commande `curl` qui récupère le texte Markdown par un client tor local. L'adresse commence délibérément par `http://` : une adresse onion de version 3 encode la clé publique d'identité du service avec une somme de contrôle et un octet de version. Tor authentifie le service et chiffre le circuit avant que HTTP soit utilisé. Un certificat web public n'est pas nécessaire pour cette authentification par adresse onion.

Un service onion demandait de la place pour un processus tor sur l'hôte des services publics de l'entreprise en septembre 2026 : un cœur avec environ 464 Mo de mémoire utilisable, qui terminait déjà TLS pour sept domaines et hébergeait une forge Git. La place nécessaire a été mesurée plutôt que discutée, sur une journée d'échantillons consignés sur cet hôte de 512 Mo : le minimum de mémoire disponible observé était d'environ 310 Mo sur 464, l'utilisation du swap de 2,6 pour cent et le processeur était inactif 99,7 pour cent du temps. Tor a donc rejoint les autres services sur cet hôte.

La notice de confidentialité consigne le choix de l'entreprise quant au comptage des lecteurs. Les applications Gemini et Gopher ne tiennent aucun journal d'accès, et leurs compteurs quotidiens ne consignent que le nombre total de requêtes. Gopher dispose aussi d'un journal de connexions du système d'exploitation contenant l'adresse source ; ce journal est supprimé au bout de 30 jours. Sur Tor, l'entreprise dit ne rien compter du tout et ne propose aucun réglage pour l'activer. C'est un choix de confidentialité de l'exploitant : Tor cache l'adresse réseau du lecteur, mais n'empêche pas un service de compter les requêtes. La notice précise que l'entreprise préfère ne pas savoir plutôt que de pouvoir le faire.

Où les problèmes surviennent

Le nom est résolu en dehors de Tor. Un programme qui envoie ses connexions à un proxy SOCKS peut encore résoudre lui-même le nom d'hôte, d'abord, par le résolveur habituel. Cette recherche révèle au réseau local et au fournisseur DNS quel site est visité. La connexion passe ensuite par Tor, mais la destination a déjà été divulguée. Avec `curl`, la différence tient à une option : `--socks5` résout le nom localement, tandis que `--socks5-hostname` le transmet au proxy, puis le relais de sortie le résout.

```
# Resolves the name locally, then connects through the proxy
curl -s --socks5 127.0.0.1:9050 https://example.org/
# Hands the name to tor; the exit relay looks it up
curl -s --socks5-hostname 127.0.0.1:9050 https://example.org/
```

Du texte en clair après la sortie. Tor chiffre les sauts entre relais, pas le dernier. La sortie ouvre une connexion TCP ordinaire vers la destination et transmet ce que l'application lui a donné : un formulaire de connexion envoyé en HTTP non chiffré est donc lisible par l'exploitant de cette sortie et par toute personne sur le réseau au-delà. Utilisez HTTPS pour tout ce qui quitte le réseau Tor. Un service onion évite la question, puisque son trafic n'en sort jamais.

Une adresse représente de nombreux lecteurs. Les limites de débit et les interdictions fondées sur l'adresse du client traitent un relais de sortie comme un visiteur unique, alors que beaucoup de personnes l'utilisent en même temps. Une limite prévue pour une personne exclut tous ceux dont le circuit aboutit là, et une interdiction provoquée par un utilisateur malveillant frappe tous les autres. Décidez explicitement du traitement des adresses de sortie au lieu de laisser une règle générique par adresse le déterminer.

L'identité circule dans le circuit. Tor cache l'adresse réseau sans agir sur ce que dit l'application. Se connecter à un compte personnel, utiliser une configuration de navigateur distinctive ou ouvrir un document qui récupère une ressource relie la session à une personne, quel que soit le nombre de relais intermédiaires. La documentation du projet précise que le trafic applicatif demande encore un nettoyage côté utilisateur : c'est le rôle de Tor Browser, qu'un navigateur ordinaire simplement dirigé vers le proxy ne remplit pas.

Un relais de sortie sur une connexion domestique. Les relais de garde et les relais intermédiaires attirent rarement des plaintes pour abus. Les destinations voient le trafic arriver depuis le relais de sortie : les plaintes et, parfois, les demandes juridiques arrivent donc chez son exploitant. Le guide des relais du Tor Project déconseille d'en exploiter un depuis chez soi. Un bénévole disposant d'une seule adresse domestique peut plutôt faire fonctionner un pont, relais non répertorié que le même guide recommande dans ce cas.

S'attendre à faire passer UDP par Tor. Les appels vocaux, de nombreux jeux et les outils qui effectuent leurs propres recherches DNS utilisent UDP, alors que Tor ne transporte que des flux TCP. Ces programmes ne fonctionnent pas par

cette voie ; un programme qui n'est pas forcé de passer par le proxy peut simplement se connecter directement, en dehors de Tor, sans le signaler.

Pour aller plus loin

- Spécifications de Tor — les spécifications du protocole, du choix des chemins, de l'annuaire et des services onion réunies.
- Tor: The Second-Generation Onion Router — l'article de conception : circuits, cellules, politiques de sortie et liste explicite de ce que la conception ne cherche pas à résoudre.
- Spécification des chemins Tor — comment le client choisit son relais de garde, son relais intermédiaire et sa sortie, et quels relais ne peuvent pas partager un chemin.
- Types de relais du réseau Tor — relais de garde, relais intermédiaires, sorties et ponts, avec l'exposition juridique de leurs exploitants.
- Chiffrement HTTPS et Tor — une présentation interactive de ce qu'un observateur voit avec Tor, avec HTTPS, avec les deux ou sans aucun des deux.

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 que Tor ? » 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/tor/