Engineer

Proxy

serveur qui transmet une requête pour votre compte

Ce que c’est

Un proxy est un programme placé entre un client et le serveur qu’il souhaite joindre. Il accepte la requête du client, en émet une à son tour vers la machine suivante et transmet la réponse au client. Le client communique avec le proxy et le proxy avec le serveur : les deux extrémités ne partagent donc jamais une connexion. Il existe plusieurs sortes de proxys ; pour chacun, la question utile est de savoir qui l’a mis en place.

La spécification HTTP elle-même, la RFC 9110, nomme trois intermédiaires courants. Un proxy au sens strict est choisi par le client, généralement au moyen d’une configuration locale, comme un réglage du navigateur ou une variable d’environnement. Une passerelle, également appelée proxy inverse dans la RFC, se place du côté du serveur : elle se comporte comme le serveur d’origine pour quiconque s’y connecte, tout en transmettant chaque requête vers un ou plusieurs serveurs derrière elle. Un tunnel relaie aveuglément les octets entre deux connexions et cesse de participer à la conversation une fois ouvert. Un client le demande avec la méthode CONNECT, en indiquant un hôte et un port, puis y fait passer TLS de bout en bout. La RFC ajoute une quatrième sorte que personne n’a choisie : le proxy d’interception, souvent appelé proxy transparent, qui redirige le trafic sortant sur le port 80 à la périphérie d’un réseau, comme le font les points d’accès publics et les pare-feu d’entreprise.

Chaque liaison entre deux machines est une connexion distincte. Le schéma de la RFC place trois intermédiaires entre un navigateur et un serveur d’origine, soit quatre connexions. Les paramètres comme le maintien de connexion (keep-alive) ou un délai d’expiration s’appliquent à une seule de ces connexions à la fois. HTTP demande aussi au proxy de signaler sa présence : il doit ajouter un champ d’en-tête Via à chaque message transmis. C’est ainsi qu’une boucle ou un intermédiaire inattendu apparaît dans une trace.

HTTP n’est qu’une couche. Un proxy SOCKS, dont la version 5 est définie dans la RFC 1928 de mars 1996, relaie les connexions TCP et les datagrammes UDP sans lire leur contenu : tout protocole peut donc l’utiliser. Tor en est un exemple connu : par défaut, il écoute sur le port 9050 les connexions SOCKS des applications locales.

Utilisez le concept pour prendre une décision

Utilisez « Qu’est-ce qu’un proxy ? » 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

L’exploitant du proxy peut lire le trafic. En HTTP non chiffré, cela signifie chaque en-tête et chaque corps de message. Dans un tunnel CONNECT, il voit le nom d’hôte et le port ; le reste est une communication TLS du client au serveur. Un proxy inverse qui termine TLS voit tout en clair, et c’est son rôle, puisqu’il doit lire une requête pour l’acheminer. Placer le proxy inverse d’une autre entreprise devant un site, ce que fait un réseau de diffusion de contenu, donne donc à cette entreprise l’adresse de chaque visiteur et chaque URL avant que le site ne les voie lui-même. Le compromis peut être justifié pour une boutique attaquée. Il reste un choix en matière de confidentialité, que la page consacrée à celle-ci devrait expliquer.

La deuxième conséquence concerne ce que le serveur apprend. La RFC 7239 décrit clairement la perte d’information : derrière un proxy, les requêtes semblent provenir de l’adresse de celui-ci. Un journal, une limitation de débit, une liste de blocage ou une liste d’autorisation fondée sur l’adresse du client voit alors une seule adresse pour tout le monde. La solution habituelle est un en-tête qui transmet l’adresse d’origine : le champ standard Forwarded de la RFC 7239 ou l’ancien X-Forwarded-For. La plupart des problèmes commencent lorsqu’il faut choisir à quelle copie de cet en-tête se fier.

Troisièmement, un proxy change le sens d'une erreur. Une erreur 502 Bad Gateway ou 504 Gateway Timeout est produite par un intermédiaire à propos du serveur placé derrière lui : le proxy a reçu une réponse invalide ou aucune réponse dans le délai imparti. Une erreur 407 signifie que le proxy lui-même exige des identifiants avant de transmettre quoi que ce soit. Savoir quelle machine a produit l'erreur, c'est déjà la moitié du diagnostic.

Quatrièmement, de nombreux proxys mettent les réponses en cache. La RFC 9111 appelle cache partagé un cache qui conserve des réponses pour plusieurs utilisateurs, généralement au sein d'un intermédiaire. Il rend un site plus rapide et moins coûteux à servir. C'est aussi l'endroit où une réponse destinée à une personne peut parvenir à une autre.

À quoi cela ressemble en pratique

En août 2026, l'entreprise a placé sa zone DNS d'une vingtaine d'enregistrements dans le dépôt et l'a mise en cohérence avec l'API Cloudflare. Faire passer le trafic web par le CDN du fournisseur comme proxy inverse faisait partie du travail, puis un proxy CDN fonctionnel placé devant le site a été démantelé pour préserver la confidentialité. L'objection tenait à sa position : l'adresse de chaque lecteur et chaque chemin demandé seraient d'abord parvenus à un tiers. Pour une entreprise qui dit à ses lecteurs que personne ne les observe, cela pesait davantage que la protection contre les attaques ainsi obtenue.

Compter les lecteurs à partir du journal d'accès que le serveur web conserve déjà a demandé, le mois suivant, de tenir compte des proxys que l'entreprise n'exploite pas. Le journal d'accès élimine sept en-têtes qui transmettent l'adresse d'un client avant d'écrire une ligne. L'encodeur du journal copie les en-têtes tels quels : sans cette étape, l'adresse non masquée d'un lecteur passant par un proxy d'entreprise aurait été enregistrée sous un nom d'en-tête non couvert par la règle de masquage.

Lorsque le site a reçu un miroir onion sur Tor le même mois, le port proxy du démon Tor destiné au trafic sortant a été désactivé dans sa configuration. Le service onion est accessible par des circuits que le démon établit vers l'extérieur : publier ce miroir ne nécessite donc aucun port Internet entrant supplémentaire. Son point d'écoute SOCKS étant désactivé, ce démon Tor ne propose aucun proxy sortant aux applications locales.

Où les problèmes surviennent

Toutes les requêtes du journal proviennent de la même adresse. L'application se trouve derrière un proxy inverse et enregistre l'adresse de la connexion reçue, celle du proxy. Une limitation de débit restreint alors tout le monde à la fois, et un blocage effectué par un outil de détection d'intrusion bloque le proxy, donc tout le public. Faites transmettre l'adresse du client dans un en-tête par le proxy et configurez l'application pour ne lire cet en-tête que sur les connexions provenant de l'adresse du proxy. Dans nginx, c'est la directive set_real_ip_from du module realip ; la plupart des frameworks web disposent d'un réglage équivalent pour les proxys de confiance.

Un client choisit sa propre adresse en envoyant un en-tête. L'application lit X-Forwarded-For sur chaque requête, y compris celles qui lui sont parvenues directement et celles qui contenaient déjà une valeur falsifiée. La RFC 7239 précise que le champ peut être modifié par n'importe quel nœud du trajet, client compris. Ne faites confiance qu'aux entrées ajoutées par votre propre proxy, en comptant à partir de la droite, et faites écouter l'application sur l'interface de bouclage ou un réseau privé pour que le proxy soit la seule voie d'accès.

Le journal que vous vouliez anonymiser conserve les adresses complètes. L'adresse du client est masquée dans le champ vérifié, mais elle circule aussi dans Forwarded, X-Forwarded-For, X-Real-IP et d'autres en-têtes. Un système de journalisation qui écrit leur ensemble tel qu'il l'a reçu les conserve intégralement. Répertoriez chaque en-tête susceptible de contenir une adresse, éliminez-le ou masquez-le au moment de l'écriture de la ligne, puis envoyez une requête de test et lisez la ligne sur disque.

Les pages renvoient 502 ou 504 alors que le journal du backend ne signale rien. L'erreur a été produite par le proxy. Une erreur 502 signifie qu'il a reçu une réponse invalide : le backend était arrêté, écoutait sur un autre port ou parlait HTTP non chiffré là où le proxy attendait TLS, ou l'inverse. Une erreur 504 signifie que le backend a dépassé le délai de lecture du proxy, fixé par défaut à 60 secondes dans nginx. Commencez par lire le journal d'erreurs du proxy, qui nomme l'adresse amont essayée, et n'augmentez un délai que pour les routes connues pour être lentes.

Un utilisateur voit la page d'un autre. Un cache partagé dans un proxy ou un réseau de diffusion a conservé une réponse personnelle, comme une page de compte renvoyée avec un cookie de session, puis l'a servie à la personne suivante

qui a demandé la même URL. Marquez chaque réponse propre à un utilisateur avec Cache-Control: private : la RFC 9111 interdit à un cache partagé de conserver une telle réponse. Utilisez no-store si aucune copie ne doit être gardée où que ce soit. Vérifiez les en-têtes effectivement renvoyés par le proxy.

Pour aller plus loin

- RFC 9110, section 3.7 : intermédiaires — Les définitions de proxy, de passerelle, de tunnel et de proxy d'interception.
- RFC 9110, section 9.3.6 : CONNECT — Comment un client demande à un proxy d'ouvrir un tunnel vers un hôte et un port.
- RFC 7239 : extension HTTP Forwarded — L'en-tête standard de transmission de l'adresse d'origine du client, avec ses limites.
- RFC 9111 : mise en cache HTTP — Les caches partagés et privés et les directives qui les séparent.
- RFC 1928 : protocole SOCKS version 5 — Le proxy indépendant du protocole qui relaie TCP et UDP.

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 proxy ? » 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/proxy/