Engineer

Proxy inverse

← serveur qui reçoit les requêtes pour un service web

Ce que c’est

Un proxy inverse est un serveur qui reçoit les requêtes pour le compte d’un service web. Le navigateur se connecte à l’adresse publique, où le proxy reçoit la requête. Celui-ci la transmet au serveur d’origine, puis renvoie la réponse au navigateur. Le service peut changer de machine, de port ou d’adresse interne sans obliger les visiteurs à modifier leurs liens. La norme HTTP appelle ce rôle une passerelle. Le proxy direct, lui, répond à un besoin du client et contacte des destinations extérieures pour son compte.

Imaginons une application dont la page d’accueil provient d’un service et dont les rapports sont produits par un autre. Le navigateur utilise le même domaine pour consulter la page et demander `/api/rapports/42`. Le proxy peut lire le chemin demandé pour choisir à quel service transmettre la requête. Si plusieurs serveurs sont capables de fournir le même rapport, il peut aussi répartir les demandes entre eux. Cette seconde fonction relève de l’équilibrage de charge. Un proxy inverse devant un seul serveur suffit à dissocier l’adresse publique du réseau interne.

Certains produits savent relayer une connexion TCP chiffrée jusqu’au serveur qui la reçoit. Dans ce mode, le composant dispose des informations de connexion et éventuellement de champs visibles dans la négociation TLS. Pour choisir un service d’après le chemin d’une requête HTTP chiffrée, il lui faut accéder au message déchiffré. Sur un schéma, indiquez le point où la connexion TLS du navigateur prend fin et précisez si une nouvelle connexion chiffrée part de ce point vers le serveur d’origine.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce qu'un proxy inverse ? » 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

Un point d’entrée commun aide à délimiter ce qui est accessible depuis l’extérieur. Le proxy peut gérer le certificat du domaine public, les redirections et les journaux d’accès, pendant que les serveurs d’application restent sur un réseau privé. Les paramètres gagnent à suivre les besoins de chaque chemin. Un téléversement peut exiger une limite de taille plus élevée que la page d’état. Une réponse envoyée en continu doit parfois être transmise dès que les premières données sont disponibles.

Quand le proxy termine TLS, son exploitant peut lire les éléments qu’il transmet. Ceux-ci peuvent inclure des témoins de connexion, des recherches ou le corps d’une requête. Une seconde connexion chiffrée protège les données en transit jusqu’au serveur d’origine. L’exploitant du point où elles sont déchiffrées y conserve un accès. Il faut donc décider qui gère cette entrée, quels éléments sont consignés et qui pourra consulter les journaux avant de prendre des engagements de confidentialité.

L’intermédiaire ajoute une piste à suivre en cas de panne. Une passerelle peut répondre par `502` en recevant une réponse non valable du service en amont. Un `504` indique que la réponse attendue a tardé au-delà du délai autorisé. L’application peut produire ses propres erreurs. Retrouvez la même requête de test dans les journaux des deux composants, puis comparez les heures et les codes d’état. Si le serveur d’origine n’a jamais reçu la requête, examinez aussi la connexion qui le relie au proxy.

À quoi cela ressemble en pratique

Dans son étude de cas sur la réconciliation de la zone DNS sous forme de code, Engineer ApS décrit un proxy CDN mis en service avec succès, puis désactivé. Le réseau du fournisseur aurait traité l'adresse de chaque internaute et l'URL demandée avant l'entreprise. Celle-ci a donné la priorité à la confidentialité par rapport au surcroît de protection contre les attaques que procurait ce service. Elle a conservé une zone DNS versionnée et auditable. Ce choix illustre les deux décisions distinctes que sont la résolution d'un nom et le traitement des requêtes web.

Dans un environnement de test, envoyez une requête à `/health` et une autre à `/api/rapports/42?vue=resume` . Relevez la méthode et le chemin effectivement reçus par l'application. Dans le navigateur, vérifiez le code d'état et l'adresse publique de toute redirection. Déplacez ensuite le service de rapports vers une nouvelle adresse interne et recommencez avec le même nom public. Vous saurez si les liens déjà utilisés restent valides après un changement du serveur d'origine.

Avant d'activer un cache partagé, ouvrez deux sessions avec des comptes de test différents. Donnez à chaque session un marqueur inoffensif et vérifiez que chacune reçoit le contenu qui lui est destiné. Arrêtez ensuite le serveur d'origine dans l'environnement de test et lancez une requête contrôlée. Mesurez le délai et retrouvez l'événement dans les journaux. Vous aurez une trace de référence pour reconnaître ce type de panne en exploitation.

Où les problèmes surviennent

Une requête provenant d'Internet peut déjà contenir un champ `Forwarded` ou `X-Forwarded-For` . L'application doit connaître la liste des intermédiaires dont elle accepte les indications avant d'utiliser l'adresse déclarée. Supprimez ou remplacez les valeurs issues d'une source inconnue et limitez les connexions directes vers l'origine aux pairs prévus. Injectez une fausse adresse dans une requête de test. Comparez celle que l'application consigne et celle qu'elle utilise dans une décision d'accès.

Une boucle de redirections révèle parfois que l'application s'est fondée sur son adresse interne. Le navigateur est entré en HTTPS et l'application a construit un lien de retour en HTTP, ou avec le port interne. Donnez à l'application le nom public et le schéma vérifiés. Parcourez la connexion de bout en bout en

contrôlant les liens de retour et les cookies. Si le proxy retire un préfixe, testez un chemin imbriqué avec des paramètres pour confirmer ce que l'application reçoit.

Un nouvel envoi après un délai dépassé peut répéter une opération déjà exécutée. Le serveur a peut-être enregistré un paiement alors que le proxy attendait encore la réponse. Définissez comment l'application reconnaît les demandes répétées avant d'autoriser leur réémission automatique pour une opération qui change des données. En test, terminez une opération contrôlée, puis retardez sa réponse. Observez quel composant met fin à l'attente et quels indices permettent de retrouver la tentative qui a produit l'effet.

Pour aller plus loin

- RFC 9110 sur les intermédiaires HTTP définit les rôles de proxy, de passerelle et de tunnel.
- RFC 7239 sur Forwarded décrit le champ et ses implications pour la sécurité et la confidentialité.
- Module de proxy HTTP de NGINX détaille les chemins, les en-têtes, les tampons et les délais.
- Directive reverse_proxy de Caddy explique le choix du serveur et la gestion des en-têtes transmis.
- Guide du proxy inverse d'Apache HTTP Server présente une entrée publique qui dessert plusieurs applications.

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 inverse ? » 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/reverse-proxy/