Engineer

Service onion

Adresse qui ne fonctionne qu'à travers le réseau Tor

Ce que c'est

Un service onion est un serveur que les lecteurs atteignent dans le réseau Tor par un nom construit à partir de sa propre clé publique, au lieu d'un nom DNS pointant vers une adresse IP. On parle souvent simplement d'onion ; un démon tor peut héberger plusieurs services onion côte à côte et la spécification emploie encore l'ancien nom, service caché.

Le nom contient 56 caractères en base32 suivis de `.onion`. Décodé, il représente 35 octets : clé d'identité ed25519 de 32 octets, somme de contrôle de deux octets tirée d'un hachage SHA3-256 de cette clé et octet de version fixé à 3. Comme cet octet est le dernier, toutes les adresses actuelles se terminent par la lettre d. Personne ne choisit le libellé : c'est la clé transcrite sous forme de texte. Les anciens noms de version 2 comptaient 16 caractères tirés du hachage SHA-1 d'une clé RSA-1024 ; tor les a supprimés dans la version 0.4.6.1-alpha, en 2021.

Joindre le service demande deux lieux de rencontre. Le service choisit quelques relais comme points d'introduction, garde des circuits ouverts vers eux et publie sur des relais d'annuaire un descripteur signé les énumérant. Celui-ci est enregistré sous une clé aveuglée qui change à chaque période et son corps est chiffré : un relais qui le stocke sans connaître l'adresse ne peut lire la liste. Le client connaissant l'adresse récupère le descripteur, vérifie la signature avec la clé du nom, choisit un relais comme point de rendez-vous et demande au service, par un point d'introduction, de l'y rejoindre. Le service construit son propre circuit vers ce relais et termine la négociation ; le relais joint les deux circuits. Le trajet traverse six relais, trois choisis de chaque côté, et aucune extrémité n'apprend l'adresse IP de l'autre. Un mode facultatif, appelé découverte restreinte et auparavant autorisation des clients, chiffre aussi le descripteur pour la clé de chaque client autorisé : seuls ceux-ci découvrent les points d'introduction.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce qu'un service onion ? » 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

Le nom remplit le rôle partagé entre DNS et autorité de certification sur un site ordinaire, sans nécessiter l'un ni l'autre. Vérifier le descripteur puis terminer la négociation confirme au client qu'il parle au détenteur de la clé privée correspondant à l'adresse. La RFC 7686, qui réserve `.onion` comme domaine à usage spécial, décrit ces noms comme combinant localisation et authentification et en tire cette conséquence : un nom onion ne peut être enregistré, attribué, transféré ou révoqué. Le posséder signifie contrôler la paire de clés, rien de plus.

Le chiffrement vient de la même conception. Le trafic vers un service onion ne quitte jamais le réseau Tor : il n'y a donc ni relais de sortie au bout, ni dernier tronçon en clair. Un simple `http://` sur un onion transporte ainsi une page chiffrée de bout en bout, vers un hôte dont le client a vérifié l'identité avec le nom saisi.

Le service n'établit que des connexions sortantes, vers ses points d'introduction et chaque point de rendez-vous : il n'a besoin d'aucun port entrant ouvert et fonctionne derrière un NAT. Ajouter un onion ne change pas la liste des ports ouverts de l'hôte.

Les lecteurs doivent encore découvrir l'adresse. Un site peut l'annoncer par l'en-tête de réponse `Onion-Location` ; Tor Browser affiche alors une pastille violette dans la barre d'adresse menant à la copie onion de la page. Le projet Tor fixe trois conditions : valeur constituée d'une URL `http:` ou `https:` avec un hôte onion, page émettrice reçue en HTTPS et n'étant pas elle-même sur un onion. Une balise meta peut porter la même annonce quand on ne peut pas définir les en-têtes, mais sans le chemin : toutes les pages pointent alors vers une URL fixe.

À quoi cela ressemble en pratique

La publication du miroir onion de l'entreprise sous une adresse lisible est décrite pas à pas. Le démon vient du paquet de la distribution, avec son port de proxy sortant désactivé. La clé privée correspondant à l'adresse a été générée hors de l'hôte et n'a jamais été présente dans le dépôt ni sur un portable ; le rôle refuse d'écraser une identité qu'il n'a pas générée, donc une clé placée à la main est utilisée telle quelle. L'adresse est une valeur déclarée dans l'inventaire ; chaque convergence vérifie que le fichier d'identité de l'hôte lui correspond, si bien qu'une clé remplacée avec une déclaration périmée arrête l'exécution. Les deux contrôles de secrets détectent le fichier de clé, après qu'une mesure a montré que le motif de recherche le plus évident pour les fichiers de clé détectait une clé de déploiement, mais pas celle-ci.

Un préfixe lisible peut être trouvé, jamais choisi. Chaque caractère supplémentaire multiplie l'effort de recherche attendu par 32 : les huit lettres de `engineer` demandent donc en moyenne environ 1 100 milliards de paires de clés. Le retrait de l'adresse aléatoire utilisée lors de la première publication du miroir a suivi une bascule par étapes, gardant l'adresse publiée joignable tout du long. Une étape semblait finale et ne l'était pas : la clé était en place, la convergence ne signalait aucun changement, mais la nouvelle adresse restait non publiée, car rien ne nommait son répertoire. Le rôle échoue désormais sur toute identité présente sur disque qu'aucun service ne nomme.

La page des crédits affiche l'adresse complète, `engineer2ezpeji52ipphljcflzyhetvy5r6tnqubtq45nzlxxv6rsqd.onion`, à côté de celles de Gemini et Gopher. Les quatre portes d'entrée partagent un dossier de fichiers et un déploiement : aucune ne peut diverger des autres. Le site ordinaire envoie `Onion-Location` et Tor Browser propose ainsi l'onion spontanément. Ce que voit le réseau du lecteur dépend de la porte : avec Gopher, la page lue ; avec Gemini, l'adresse demandée ; avec l'onion, ni l'une ni l'autre. Le préfixe lisible est une commodité, pas une preuve : c'est l'adresse entière qu'il faut comparer.

La structure de l'adresse se vérifie hors ligne. Ces lignes la décodent et recalculent la somme de contrôle ; les deux comparaisons affichent `True` :

```
import base64
import hashlib

label = "engineer2ezpeji52ipphljcflzyhetvy5r6tnqubtq45nzlxxv6rsqd"
raw = base64.b32decode(label.upper())
```

```
key, checksum, version = raw[:32], raw[32:34], raw[34:]
digest = hashlib.sha3_256(b".onion checksum" + key + version).digest()
print(version == b"\x03", digest[:2] == checksum)
```

Une somme de contrôle valide indique que l'adresse est bien formée, pas à qui elle appartient. Cette information vient de sa lecture sur les pages HTTPS de l'entreprise elle-même.

Où les problèmes surviennent

La clé est le seul titre de propriété. Sans bureau d'enregistrement derrière le nom, perdre la clé privée revient à perdre l'adresse ; une copie permet à quelqu'un d'autre d'y répondre. Le guide d'installation de Tor demande de garder les fichiers de clé privés et de sauvegarder la clé si le service doit durer. Traitez-la comme une clé de signature, pas comme de la configuration.

Seules les premières lettres sont lues. La RFC 7686 avertit qu'un attaquant peut trouver des clés dont les noms ressemblent à celui visé ; le risque augmente car ces noms ne signifient rien pour une personne. Elle cite comme remède les noms lisibles obtenus avec beaucoup de calcul, mais un préfixe de huit caractères laisse les 48 autres aussi opaques. Comparez l'adresse entière ou utilisez un favori ou un lien sur les pages HTTPS du site lui-même.

Le serveur révèle son nom. Tor masque l'emplacement du service, mais le logiciel derrière peut encore le révéler. La RFC 7686 cite parmi les échecs de protection un serveur divulguant son identité dans un message applicatif ; une page d'erreur affichant le vrai nom de l'hôte en est un exemple. Le guide conseille aussi d'acheminer le trafic vers le serveur web par socket Unix plutôt que TCP, pour ne pas exposer le service sur le réseau local :

```
HiddenServiceDir /var/lib/tor/my-website/
HiddenServicePort 80 unix:/var/run/tor/my-website.sock
```

Cela compte surtout lorsque l'emplacement lui-même est secret.

Le nom part vers DNS. Un logiciel ne parlant pas Tor interroge le résolveur ordinaire sur le nom onion, révélant au réseau local et au fournisseur DNS l'onion recherché. La RFC 7686 demande à ce logiciel d'échouer sans interrogation, et

aux serveurs DNS de répondre que le nom n'existe pas. Transmettez plutôt le nom au client Tor.

La pastille `Onion-Location` n'apparaît jamais. Un en-tête placé seulement sur la redirection HTTP en clair ne remplit pas la condition HTTPS ; une adresse mal saisie ne mène nulle part. Vérifiez l'en-tête de la réponse HTTPS finale.

Pour aller plus loin

- Spécification de rendez-vous Tor, version 3 — protocole complet : identité et clés aveuglées, descripteurs, introduction et rendez-vous.
- Encodage des adresses onion — formule transformant une clé publique en nom de 56 caractères, avec exemples d'adresses.
- Fonctionnement des services onion — points d'introduction, descripteurs et rendez-vous, pas à pas.
- Installer un service onion — lignes de torrc, fichiers créés par tor et conseils sur les clés et les fuites d'emplacement.
- Onion-Location — en-têtes et balises meta pour Apache, Nginx et Caddy, et conditions imposées à l'en-tête.
- RFC 7686 — réservation de `.onion` et obligations des résolveurs, opérateurs DNS et bureaux d'enregistrement.

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 service onion ? » 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/onion/