Exgate : Une infrastructure de réseau souverain pair-à-pair (Peer-to-Peer)

Version 1.0

Résumé. L'architecture Internet contemporaine souffre d'une centralisation structurelle, d'une surveillance omniprésente et de dépendances de confiance inhérentes envers les opérateurs intermédiaires. Nous proposons Exgate, une infrastructure de réseau distribuée qui élimine la nécessité de faire confiance aux fournisseurs d'accès Internet (FAI) et aux autorités centrales grâce à des preuves cryptographiques et à la propriété physique du matériel. Le système utilise une architecture de routage à double relais "oblivious" (inconscient) pour découpler mathématiquement l'identité de l'utilisateur de l'activité réseau, tout en mettant en œuvre une mise en cache centrée sur le contenu pour atteindre la résilience du réseau et réduire la latence. La garde physique des nœuds du réseau par les utilisateurs finaux établit une souveraineté matérielle sur le transit et le stockage des données. Le réseau maintient sa sécurité tant que les nœuds relais fonctionnent indépendamment et que les chemins de routage sont diversifiés à travers le maillage pair-à-pair.

---

1. Introduction

L'architecture originale d'Internet mettait l'accent sur la décentralisation et la résilience grâce au routage distribué des paquets. L'infrastructure Internet contemporaine s'est fondamentalement écartée de cette philosophie de conception, consolidant le contrôle au sein des FAI, des fournisseurs de cloud et des appareils de surveillance. Les utilisateurs transmettent des métadonnées non chiffrées aux FAI, s'appuient sur des autorités DNS centralisées pour la résolution des noms et stockent des données sur des serveurs tiers sans garanties cryptographiques de confidentialité ou de disponibilité.

Les réseaux privés virtuels (VPN) tentent de répondre aux problèmes de confidentialité mais introduisent un problème de confiance critique : l'opérateur VPN observe à la fois l'identité de l'utilisateur (adresse IP source) et l'activité de l'utilisateur (trafic de destination). Cela représente un point de défaillance unique où une entité possède une capacité de surveillance complète. De plus, les protocoles VPN présentent des signatures de trafic distinctives qui permettent aux systèmes d'inspection approfondie des paquets (DPI) d'identifier et de bloquer ces connexions, en particulier dans les régimes de censure.

La diffusion de contenu repose sur des serveurs centralisés, créant des points de défaillance uniques vulnérables à la censure, aux interruptions de service et aux attaques d'infrastructure. Lorsque du contenu populaire est consulté par plusieurs utilisateurs à proximité géographique, chaque demande traverse tout le chemin vers les serveurs d'origine, gaspillant la bande passante et augmentant

inutilement la latence.

Ce qu'il faut, c'est une infrastructure réseau basée sur la séparation cryptographique des connaissances plutôt que sur la confiance, permettant aux utilisateurs d'acheminer le trafic sans qu'aucune entité unique n'observe à la fois l'identité et l'activité. Un système où la propriété du matériel établit la souveraineté des données, et où la disponibilité du contenu ne dépend pas de l'accessibilité du serveur d'origine.

Dans ce document, nous proposons une solution utilisant un réseau pair-à-pair avec des nœuds matériels appartenant aux utilisateurs qui mettent en œuvre un routage relais inconscient, une mise en cache centrée sur le contenu et une gestion d'identité cryptographique. Le système assure la confidentialité par la conception architecturale plutôt que par des promesses de politique. Tant que les nœuds relais fonctionnent indépendamment et que les utilisateurs conservent la garde physique de leur matériel réseau, l'infrastructure résiste à la surveillance, à la censure et au contrôle centralisé.

---

2. Infrastructure Physique : Le Nœud Exgate

2.1 Principe de Souveraineté Matérielle

Nous définissons l'axiome de sécurité fondamental : Si vous ne possédez pas le matériel, vous ne contrôlez pas les données. Les services VPN basés sur le cloud et les infrastructures virtuelles nécessitent de faire confiance aux opérateurs ayant un accès en texte clair au trafic et aux métadonnées. Exgate inverse ce modèle en exigeant que les utilisateurs conservent la garde physique d'un matériel réseau dédié.

Un nœud Exgate est un appareil spécialement conçu positionné entre le routeur fourni par le FAI et le réseau local de l'utilisateur, fonctionnant en mode pont (bridge). Du point de vue du FAI, le nœud ne présente que du trafic tunnel chiffré sans indicateurs en texte clair distinguables de l'activité de l'utilisateur.

2.2 Spécifications Techniques

Pour prendre en charge les opérations cryptographiques en temps réel et la mise en cache de contenu, un nœud Exgate nécessite: * **Processeur :** Architecture ARM64 (par exemple, Rockchip RK3588) avec accélération cryptographique matérielle (équivalent AES-NI) pour minimiser la surcharge de chiffrement. * **Stockage :** SSD NVMe de 2 à 4 To pour la mise en cache de contenu à grande vitesse et le stockage d'index DHT avec une latence d'accès inférieure à la milliseconde. * **Réseau :** Deux ports Ethernet 2,5 GbE (WAN/LAN) pour éviter les goulots d'étranglement des connexions fibre. * **Module de Sécurité :** Trusted Platform Module (TPM 2.0) ou Enclave Sécurisée pour le stockage de clés privées inviolable. * **Mémoire :** 8 Go de RAM minimum pour les tables de routage DHT et la gestion des connexions simultanées.

2.3 Rôle Fonctionnel

Contrairement aux routeurs passifs, les nœuds Exgate participent activement au réseau distribué en tant que: 1. **Cache de Contenu :** Stockage de fragments de contenu chiffrés récupérés par le réseau local ou les nœuds voisins. 2. **Nœud Relais :** Transfert du trafic chiffré pour d'autres participants du réseau. 3. **Nœud de Sortie (Optionnel) :** Fourniture d'une sortie à large bande passante vers le "clearnet" pour les pairs autorisés. 4. **Fournisseur de Stockage :** Contribution de la capacité de stockage inutilisée au système de sauvegarde distribué.

Le micrologiciel du nœud applique la réciprocité : pour consommer des ressources réseau (bande passante, stockage, capacité de relais), un nœud doit contribuer proportionnellement. Cela n'est pas encouragé par des jetons spéculatifs mais par un bridage de la qualité de service (QoS) des nœuds non contributeurs.

---

3. Architecture de Relais Inconscient (Oblivious Relay)

3.1 Le problème de confiance dans les VPN traditionnels

Les architectures VPN traditionnelles ne parviennent pas à éliminer les exigences de confiance. Considérez un utilisateur U se connectant à la destination D via le fournisseur VPN V:

$$U \xrightarrow{\text{chiffré}} V \xrightarrow{\text{texte clair}} D$$

Le fournisseur V observe: * **Source :** IP_U (identité) * **Destination :** IP_D et SNI_D (activité) * **Temps :** Horodatages et durée de connexion * **Volume :** Octets transmis

Cela donne à V une capacité de surveillance complète, réduisant la confidentialité de l'utilisateur à une promesse légale ou politique plutôt qu'à une garantie cryptographique.

3.2 Séparation des connaissances à double relais

Exgate met en œuvre un système de relais à deux parties où aucune entité unique ne possède à la fois les informations d'identité et d'activité. Le trafic de l'utilisateur U vers la destination D traverse deux nœuds indépendants:

$$U \xrightarrow{\text{chiffré E2E}} R1 \xrightarrow{\text{chiffré E2E}} R2 \xrightarrow{\text{texte clair}} D$$

Où : * R_1 = Nœud Relais (premier saut, généralement un autre nœud Exgate) * R_2 = Nœud de Sortie (deuxième saut, serveur de sortie haute capacité)

Informations disponibles pour chaque partie :

Entité	Connaît l'identité	Connaît l'activité	Capacité de surveillance
FAI	IP_U	Trafic chiffré vers R_1	Non
R_1 (Relais)	IP_U	Charge utile chiffrée	Non
R_2 (Sortie)	IP_{R_1}	IP_D, SNI_D	Non
Destination D	IP_{R_2}	Contenu de la demande	Non

Garantie cryptographique : Aucune entité unique dans le chemin de relais ne peut construire la correspondance $U \to D$. Même si R_1 et R_2 complotent, ils doivent corréler le temps et les modèles de volume de trafic à travers des tunnels chiffrés, une attaque coûteuse en calcul atténuée par le remplissage de trafic (padding) et la sélection aléatoire de relais.

3.3 Tunnels chiffrés imbriqués

L'utilisateur établit deux tunnels cryptographiques: 1. $T_1 : U \leftrightarrow R_2$ (Tunnel WireGuard de bout en bout) 2. $T_2 : U \to R_1$ (Transport QUIC externe)

Flux de trafic: 1. L'utilisateur U chiffre la charge utile avec les clés T_1 (destination : R_2). 2. Le paquet chiffré est encapsulé dans le transport T_2 (destination : R_1). 3. R_1 reçoit un blob chiffré opaque, le transfère à R_2 sans capacité de déchiffrement. 4. R_2 déchiffre le tunnel T_1, récupère le texte clair, transmet à la destination D.

R_1 ne possède jamais les clés cryptographiques pour T_1, assurant une séparation mathématique des connaissances.

3.4 Sélection de relais et diversité de chemin

Pour empêcher l'analyse du trafic à long terme, les chemins de relais sont tournés périodiquement: * **Nœud Relais (R_1) :** Sélectionné aléatoirement parmi les nœuds Exgate avec des scores de réputation de bande passante suffisants, tourné toutes les 6 à 12 heures. * **Nœud de Sortie (R_2) :** Sélectionné parmi des nœuds haute capacité de confiance (partenaires commerciaux, supernœuds communautaires), tourné toutes les 24 heures.

La diversité de chemin est appliquée de manière algorithmique: * Pas de sélection consécutive du même R_1 pendant 7 jours. * Distribution géographique : Éviter de sélectionner R_1 et R_2 dans des juridictions ayant des traités d'assistance judiciaire mutuelle lorsque cela est possible. * Diversité de chemin AS : Sélectionner des relais à travers différents systèmes autonomes pour empêcher la corrélation du trafic par un seul FAI.

4. Pile de Protocoles : WireGuard sur QUIC

4.1 Le problème de l'effondrement TCP (TCP Meltdown)

L'encapsulation de protocoles VPN basés sur TCP (OpenVPN, IPsec/mode TCP) dans un transport TCP crée une dégradation catastrophique des performances. Lorsque la perte de paquets se produit, les couches TCP internes et externes déclenchent indépendamment le contrôle de congestion et la retransmission, provoquant un "effondrement TCP":

$$\text{Latence} \approx (RTT_{externe} + RTT_{interne}) \times k^2$$

Où k est le nombre de tentatives de retransmission. Cela s'aggrave de manière exponentielle dans des conditions de réseau avec pertes.

4.2 Conception de WireGuard sur QUIC

Exgate utilise WireGuard encapsulé dans des datagrammes non fiables QUIC (RFC 9221). Cette conception offre :

Avantages de performance : * **Contrôle de congestion monocouche :** QUIC gère la congestion au niveau de la couche transport ; WireGuard fonctionne en mode datagramme sans retransmission. * **Surcharge réduite :** WireGuard n'ajoute que 32 octets par paquet (contre 57+ octets pour IPsec). * **Handshake rapide :** L'établissement de connexion QUIC 0-RTT réduit les pics de latence lors des changements de relais.

Résistance à la censure : QUIC est la base de HTTP/3 et constitue un pourcentage significatif du trafic Internet mondial. Bloquer QUIC perturberait des services majeurs (YouTube, Google, Cloudflare). Le trafic Exgate est indiscernable des flux QUIC standards pour les systèmes DPI: * Utilise des ID de connexion et une négociation de version QUIC standard. * Charges utiles chiffrées avec une distribution de taille identique à HTTP/3. * Server Name Indication (SNI) chiffré via les paramètres de transport QUIC.

Les censeurs observant le trafic Exgate ne voient que : `Connexion QUIC FAI → Un serveur Internet` Cela fournit une liberté collatérale : bloquer ce modèle nécessite de bloquer des services légitimes.

4.3 Propriétés cryptographiques

Sécurité WireGuard : * Framework de protocole Noise (modèle de handshake Noise_IK). * Chiffrement authentifié ChaCha20-Poly1305. * Curve25519 pour l'échange de clés, BLAKE2s pour le hachage. * Confidentialité persistante (Forward secrecy) grâce à des clés éphémères tournées toutes les 2 minutes.

Sécurité QUIC : * Handshake TLS 1.3 pour l'établissement de connexion. * Chiffrement de l'ID de connexion pour empêcher le suivi. * Validation de chemin pour empêcher les attaques de routage.

Le chiffrement imbriqué garantit que même si le transport QUIC est compromis, la charge utile WireGuard reste sécurisée.

---

5. Réseautage Centré sur le Contenu (Content-Centric Networking)

5.1 Principes de réseautage de données nommées

Le réseautage IP traditionnel route les paquets en fonction du *où* (emplacement de l'hôte). Le réseautage centré sur le contenu route en fonction du *quoi* (identité du contenu). Exgate implémente cela pour le contenu statique (pages web, fichiers multimédias, paquets logiciels).

5.2 Adressage de contenu et mise en cache

Lorsqu'un utilisateur demande du contenu (par exemple, https://example.com/page.html): 1. Le contenu est récupéré via un relais inconscient (Section 3). 2. Le contenu est haché : $H = \text{SHA3-256}(\text{contenu})$. 3. Le contenu est chiffré avec une clé symétrique : $C = \text{AES-256}(\text{contenu, K})$. 4. Le contenu chiffré C et la clé K sont stockés sur le nœud Exgate local. 5. Le mappage (H, K, URL) est publié dans la Table de Hachage Distribuée (DHT).

Demandes ultérieures pour un contenu identique: 1. L'utilisateur interroge la DHT pour H. 2. La DHT renvoie la liste des nœuds stockant C et la clé K. 3. L'utilisateur récupère C depuis le nœud géographiquement le plus proche (souvent un voisin sur le même FAI). 4. L'utilisateur déchiffre C en utilisant K.

Avantages : * **Réduction de la latence :** Le contenu servi depuis le cache local élimine l'aller-retour vers le serveur d'origine. * **Efficacité de la bande passante :** Le contenu populaire (Wikipedia, articles d'actualité) est téléchargé une fois par quartier. * **Résistance à la censure :** Le blocage du serveur d'origine n'empêche pas la récupération du contenu depuis le cache distribué. * **Résilience :** Le contenu reste accessible pendant les temps d'arrêt du serveur d'origine ou une partition Internet.

5.3 Politique d'éviction de cache

Le stockage est fini. Exgate met en œuvre une politique d'éviction "Moins Fréquemment Utilisé (LFU) avec décroissance temporelle":

$$Score(C) = FreqCount(C) \times e^{-\lambda \cdot (t_{now} - t_{last})}$$

Où : * $FreqCount(C)$: Nombre de fois que le contenu C a été demandé localement. * $t_{now} - t_{last}$: Temps écoulé depuis le dernier accès. * λ : Constante de décroissance (ajustée pour une demi-vie d'environ 30 jours).

Le contenu avec le score le plus bas est expulsé lorsque la capacité de stockage dépasse 85%. Cela équilibre popularité et récence, assurant que le contenu

fréquemment consulté reste en cache tout en empêchant les données obsolètes de consommer trop de stockage.

---

6. Implémentation de la Table de Hachage Distribuée (DHT)

6.1 Routage basé sur Kademlia

Exgate utilise une DHT Kademlia modifiée pour le stockage décentralisé clé-valeur. Chaque nœud maintient : * **ID de Nœud :** Identifiant 256 bits dérivé de la clé publique du nœud : $ID = \text{SHA3-256}(\text{PubKey})$. * **Table de Routage :** 256 k-buckets ($k = 20$), chacun stockant jusqu'à 20 nœuds à une distance de 2^i à 2^{i+1}. * **Magasin de Données :** Paires clé-valeur où distance (Clé, ID) $<$ seuil.

Métrique de distance : $d(A, B) = A \oplus B$ (distance XOR).

6.2 Protocole de découverte de contenu

Pour trouver du contenu avec le hachage H: 1. Interroger la table de routage locale pour les $k = 20$ nœuds les plus proches de H. 2. Envoyer `FIND_NODE(H)` à ces nœuds en parallèle. 3. Chaque nœud répond avec k nœuds de sa table de routage plus proches de H. 4. Interroger itérativement les nœuds plus proches jusqu'à trouver les nœuds stockant (H, K, URL). 5. Temps de recherche attendu : $O(\log N)$ où $N =$ nombre total de nœuds du réseau.

Redondance : Chaque paire clé-valeur est répliquée sur les 20 nœuds les plus proches de H, offrant une tolérance aux pannes contre la rotation des nœuds (churn).

6.3 Résistance aux attaques Sybil

Les réseaux DHT sont vulnérables aux attaques Sybil où un adversaire génère de nombreux faux ID de nœuds pour contrôler le routage. Exgate atténue cela par:

Preuve de Matériel (PoH) : 1. En rejoignant le réseau, le nœud génère une preuve cryptographique démontrant la possession d'un TPM/Enclave Sécurisée. 2. La preuve inclut la signature d'attestation TPM et les registres de configuration de plateforme (PCRs). 3. Les nœuds existants vérifient l'attestation à l'aide des clés publiques du fabricant. 4. Les ID de nœuds dérivés de clés adossées au TPM sont marqués comme "matériel vérifié".

Notation de Réputation : * Les nœuds suivent les interactions réussies/échouées avec les pairs. * Score de réputation $R = \frac{\text{Réponses réussies}}{\text{Total des requêtes}} \times$ Fraction de temps de disponibilité . * Les tables de routage priorisent les nœuds avec $R > 0.95$ et un matériel vérifié.

Cela empêche un attaquant de générer à bas coût des milliers de nœuds virtuels pour manipuler le routage.

---

7. Identité Auto-Souveraine

7.1 Fondation d'identité cryptographique

Exgate rejette les systèmes d'identité traditionnels (noms d'utilisateur, e-mail, authentification tierce). Chaque utilisateur est identifié exclusivement par sa paire de clés cryptographiques : $(sk, pk) \leftarrow \text{KeyGen}(\text{entropie})$. * sk : Clé privée Ed25519 (256 bits), stockée dans le TPM/Enclave Sécurisée. * pk : Clé publique Ed25519 (256 bits), sert d'identifiant global de l'utilisateur.

Représentation de l'identité : $UserID = \text{Base58}(pk)$. Exemple : `ExG7K9pQrS...`.

7.2 Le principe "Game Over"

Il n'y a pas de récupération de compte. Si un utilisateur perd sa clé privée sk, son identité et toutes les autorisations d'accès associées sont définitivement irrécupérables. Ce n'est pas un défaut mais une propriété de sécurité fondamentale : * **Pas de tiers de confiance :** Aucune autorité de "réinitialisation de mot de passe" ne peut compromettre la sécurité. * **Authentification indéniable :** Les signatures prouvent le contrôle exclusif de sk. * **Élimine l'ingénierie sociale :** Pas de support client à manipuler pour la prise de contrôle de compte.

Les utilisateurs sont invités à générer et stocker en toute sécurité une phrase de récupération (mnémonique BIP-39) à partir de laquelle (sk, pk) sont dérivés de manière déterministe.

7.3 Authentification Challenge-Response

Lorsque l'utilisateur U se connecte à la ressource R, l'authentification se déroule sans mot de passe: 1. R envoie un défi : $c \leftarrow \text{RandomBytes}(32)$. 2. U signe le défi : $\sigma \leftarrow \text{Sign}(sk_U, c)$. 3. R vérifie : $\text{Verify}(pk_U, c, \sigma) == \text{True}$.

Si la vérification réussit, U est authentifié. Le défi empêche les attaques par rejeu ; la signature prouve le contrôle exclusif de sk_U.

---

8. Système de Nommage Décentralisé (ExDNS)

8.1 Le problème de l'ICANN

Le DNS traditionnel centralise l'autorité de nommage sous l'ICANN et les registres nationaux. Les gouvernements peuvent saisir des domaines ; les bureaux d'enregistrement peuvent censurer le contenu ; les frais de renouvellement créent une dépendance perpétuelle.

8.2 Propriété cryptographique des noms

ExDNS élimine les autorités centralisées. Pour enregistrer le nom `mysite.exg`: 1. L'utilisateur génère un message d'enregistrement : $M = (\text{name}, pk_{owner}, \text{content\_hash}, \text{timestamp})$. 2. L'utilisateur signe le message : $\sigma = \text{Sign}(sk_{owner}, M)$. 3. L'utilisateur publie (M, σ) dans la DHT à la clé $K = \text{SHA3-256}(\text{name})$.

Vérification de propriété : Tout nœud peut vérifier la propriété du nom : $\text{Verify}(pk_{owner}, M, \sigma) == \text{True}$. Si la signature est valide et que l'horodatage est le plus ancien pour ce nom, la propriété est établie.

8.3 Allocation "Premier arrivé, premier servi"

Les collisions de noms sont résolues par priorité d'horodatage. Pas de frais de renouvellement. La propriété est permanente tant que le propriétaire publie périodiquement une signature "heartbeat" (battement de cœur) prouvant le contrôle continu de sk.

8.4 Clause de caducité

Pour empêcher la pollution de l'espace de noms par des noms abandonnés: * Tous les 180 jours, le propriétaire doit publier un heartbeat. * Si aucun heartbeat n'est publié pendant 730 jours (2 ans), le nom devient disponible pour un réenregistrement.

---

9. Stockage Redondant Distribué (ExCloud)

9.1 Le problème du point de défaillance unique

Le stockage local est performant mais vulnérable à la destruction physique. Exgate met en œuvre un système de sauvegarde distribué avec chiffrement à connaissance nulle.

9.2 Codage d'effacement et partage (Sharding)

Les données utilisateur D sont protégées par un codage d'effacement Reed-Solomon: 1. D est divisé en k morceaux : $D = \{C_1, ..., C_k\}$. 2. Le codage génère $n - k$ morceaux de redondance. 3. k morceaux quelconques parmi les n totaux peuvent reconstruire D (Paramètres typiques : $k = 10, n = 20$).

Chiffrement : Avant distribution, chaque morceau C_i est chiffré : $E_i = \text{AES-256}(C_i, K_{user})$.

9.3 Protocole de stockage distribué

L'utilisateur télécharge chaque fragment E_i vers un nœud cible N_i trouvé via la DHT. Pour la récupération, l'utilisateur télécharge $k = 10$ fragments disponibles,

les déchiffre et reconstruit D .

9.4 Mécanisme d'incitation

Les nœuds fournissant du stockage sont priorisés dans la sélection des relais et reçoivent des allocations de bande passante plus élevées. Les nœuds demandant du stockage sans contribuer sont limités en débit (anti-leech).

---

10. Isolation au Niveau du Réseau (Quarantaine IoT)

10.1 Le problème de sécurité IoT

Les appareils IoT présentent fréquemment des vulnérabilités (identifiants par défaut, manque de chiffrement) et sont utilisés pour des botnets.

10.2 Classification automatique des appareils

Les nœuds Exgate effectuent une empreinte passive des appareils (recherche MAC OUI, analyse des modèles de trafic, empreinte DHCP) . Les appareils à haut risque sont automatiquement assignés à un VLAN IoT dédié.

10.3 Politique de ségrégation

Le VLAN IoT applique une isolation stricte:

Type d'accès	Autorisé	Bloqué
Appareil IoT → Internet (direct)	Oui	
Appareil IoT → Appareils utilisateur		Oui
Appareil IoT → NAS/serveur de fichiers		Oui
Appareil utilisateur → Appareil IoT (contrôle)	Oui*	

**nécessite une autorisation explicite de l'utilisateur.*

10.4 Réponse dynamique aux menaces

Si un appareil IoT présente un comportement malveillant, le nœud bloque immédiatement toutes les connexions sortantes de l'appareil et alerte l'utilisateur .

---

11. Contrôle d'Accès au Maillage par Permission

11.1 Le problème du mot de passe

Les services traditionnels exposent des ports à Internet et reposent sur des mots de passe, vulnérables au bourrage d'identifiants et aux attaques par force brute .

11.2 Listes de contrôle d'accès cryptographiques

Les services Exgate sont invisibles par défaut. Pour exposer un service, le propriétaire crée une liste de contrôle d'accès (ACL) : $ACL_{service} = \{pk_1, pk_2, ..., pk_m\}$.

Port Knocking avec signatures : 1. Le client envoie une demande signée. 2. Le nœud Exgate vérifie si $pk_{client} \in ACL_{service}$ et valide la signature . 3. Si valide, le nœud ouvre un tunnel éphémère ; sinon, la connexion est silencieusement abandonnée.

Du point de vue de l'attaquant, le port semble fermé.

---

12. Analyse de Sécurité

12.1 Modèle de menace

Nous considérons un adversaire capable de surveillance réseau, de compromission de relais, d'analyse de trafic et d'attaques Sybil . Nous supposons que l'adversaire ne peut pas casser les primitives cryptographiques ou compromettre le matériel physique de l'utilisateur (TPM) .

12.2 Résistance à l'analyse de trafic

Pour atténuer les attaques par corrélation temporelle, Exgate utilise le remplissage de trafic, l'envoi à taux constant et la diversité de chemin . La probabilité de corrélation devient statistiquement irréalisable avec la diversité de chemin ($P_{correlation} \approx 10^{-7}$).

12.3 Résistance à l'attaque Sybil

La Preuve de Matériel (PoH) rend la création de faux nœuds économiquement prohibitive. Pour créer $N = 1000$ nœuds Sybil avec matériel vérifié, le coût d'attaque dépasse 150 000 $, contre un coût quasi nul pour les attaques virtuelles.

12.4 Résistance à la censure

Le trafic Exgate utilise le protocole QUIC standard, indiscernable de HTTP/3. Les nœuds de sortie peuvent être déployés sur une infrastructure CDN (Cloud-

flare, AWS), rendant le blocage difficile sans dommages collatéraux.

---

13. Analyse de Performance

13.1 Surcharge de latence

Latence Exgate ≈ 2x à 3x la latence directe, acceptable pour la navigation et le streaming. Pour le contenu mis en cache, la latence est de 1 à 10 ms, souvent plus rapide que la connexion directe.

13.2 Efficacité de la bande passante

Surcharge totale par paquet ≈ 6%. La mise en cache de contenu permet d'économiser une bande passante significative pour le contenu populaire (ex: 9,9 Go économisés pour 100 utilisateurs regardant la même vidéo).

13.3 Utilisation du stockage

Le stockage est utilisé efficacement avec 80-90% d'occupation sous fonctionnement normal (Cache de contenu + Fragments ExCloud + DHT).

---

14. Modèle Économique et Gouvernance

14.1 Philosophie "Zéro Tokénomique"

Exgate rejette explicitement les jetons de crypto-monnaie spéculatifs. La contribution est imposée par l'architecture via la réciprocité au niveau du micrologiciel et les politiques QoS.

14.2 Modèle de financement

- **Ventes de matériel :** Prix cible de 250 600 selon le modèle .
- **Services d'abonnement optionnels :** Accès à des nœuds de sortie commerciaux à large bande passante (5-10 $/mois).
- **Fondation et dons :** Partenariats avec des organisations de droits numériques pour parrainer des nœuds de sortie dans les régions censurées.

14.3 Structure de gouvernance

Le développement est guidé par un code open-source, un développement transparent et une absence de contrôle centralisé . Les changements de protocole critiques nécessitent un consensus, une période d'examen et un déploiement sur testnet .

---

15. Stratégie de Déploiement et d'Adoption

15.1 Problème de démarrage (Bootstrap)

Pour résoudre le problème de démarrage, Exgate utilise des "nœuds graines" (Seed Nodes) financés publiquement et des partenariats avec des FAI axés sur la confidentialité . L'incitation à la mise en cache de contenu favorise l'adoption même avant les effets de réseau complets.

15.2 Phases d'adoption

- **Phase 1 (0-10k nœuds) :** Fonctionnalité type VPN via les nœuds graines.
- **Phase 2 (10k-100k nœuds) :** Le maillage pair-à-pair devient autonome.
- **Phase 3 (100k+ nœuds) :** Exgate devient l'infrastructure par défaut pour les utilisateurs soucieux de leur vie privée.

---

16. Comparaison avec les Systèmes Existants

Propriété	Exgate	VPN	Tor	I2P	IPFS
Pas de point de confiance unique		X			
Propriété du matériel		X	X	X	X
Mise en cache de contenu		X	X	X	
Résistant à la censure		Δ			Δ
Faible latence (< 100 ms)			X	X	Δ
Haute bande passante (> 50 Mbps)			X	X	Δ
Isolation IoT		X	X	X	X
Identité auto-souveraine		X	Δ		Δ

(Légende : ✓ = oui, X = non, Δ = partiel)

Exgate synthétise les meilleures propriétés des systèmes existants tout en remédiant à leurs limites fondamentales.

---

17. Travaux Futurs

17.1 Cryptographie Post-Quantique

Transition vers des algorithmes post-quantiques (Kyber pour l'échange de clés, Dilithium pour les signatures) pour contrer la menace de l'algorithme de Shor .

17.2 Calcul Vérifiable

Mise en œuvre de calculs vérifiables pour empêcher les nœuds relais malveillants de falsifier le contenu mis en cache (signatures du serveur d'origine).

17.3 Marché Décentralisé de Nœuds de Sortie

Permettre aux utilisateurs de mettre aux enchères la bande passante des nœuds de sortie via des canaux de paiement préservant la confidentialité (Lightning Network).

17.4 Support Client Mobile

Développement de clients mobiles légers (Android, iOS) se connectant aux nœuds Exgate domestiques via WireGuard.

---

18. Conclusion

Nous avons proposé Exgate, une infrastructure réseau pair-à-pair qui élimine les dépendances de confiance grâce à la séparation cryptographique des connaissances et à la propriété physique du matériel. Le système atteint la confidentialité, la résistance à la censure et la performance grâce à l'architecture de relais inconscient, la souveraineté matérielle et la mise en cache centrée sur le contenu
.

Contrairement aux services VPN existants, Exgate fournit une preuve cryptographique de confidentialité. Exgate représente une refonte fondamentale de l'architecture Internet : de la confiance centralisée à la preuve cryptographique, du centrage sur le serveur au centrage sur le contenu, et de l'infrastructure d'entreprise au matériel appartenant à l'utilisateur.

Références

[1] Baran, P. (1964). On Distributed Communications Networks. IEEE Transactions on Communications Systems. [2] Perta, V. C., et al. (2015). A glance through the VPN looking glass… Proceedings on Privacy Enhancing Technologies. [3] Schmitt, P., et al. (2019). Oblivious DNS… Proceedings on Privacy Enhancing Technologies. [4] Honda, M., et al. (2005). Is it still possible to extend TCP? ACM SIGCOMM. [5] Iyengar, J., & Thomson, M. (2021). QUIC: A UDP-Based Multiplexed and Secure Transport. RFC 9000. [6] Rüth, J., et al. (2018). A first look at QUIC in the wild. [7] Feamster, N., et al. (2002). Infranet: Circumventing web censorship… USENIX. [8] Perrin, T. (2018). The Noise Protocol Framework. [9] Jacobson, V., et al. (2009). Networking named content. [10] Maymounkov, P., & Mazières, D. (2002). Kademlia… [11] Douceur,

J. R. (2002). The Sybil attack. [12] Reed, I. S., & Solomon, G. (1960). Polynomial codes over certain finite fields. [13] Antonakakis, M., et al. (2017). Understanding the Mirai botnet. [14] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization… SIAM Journal on Computing.