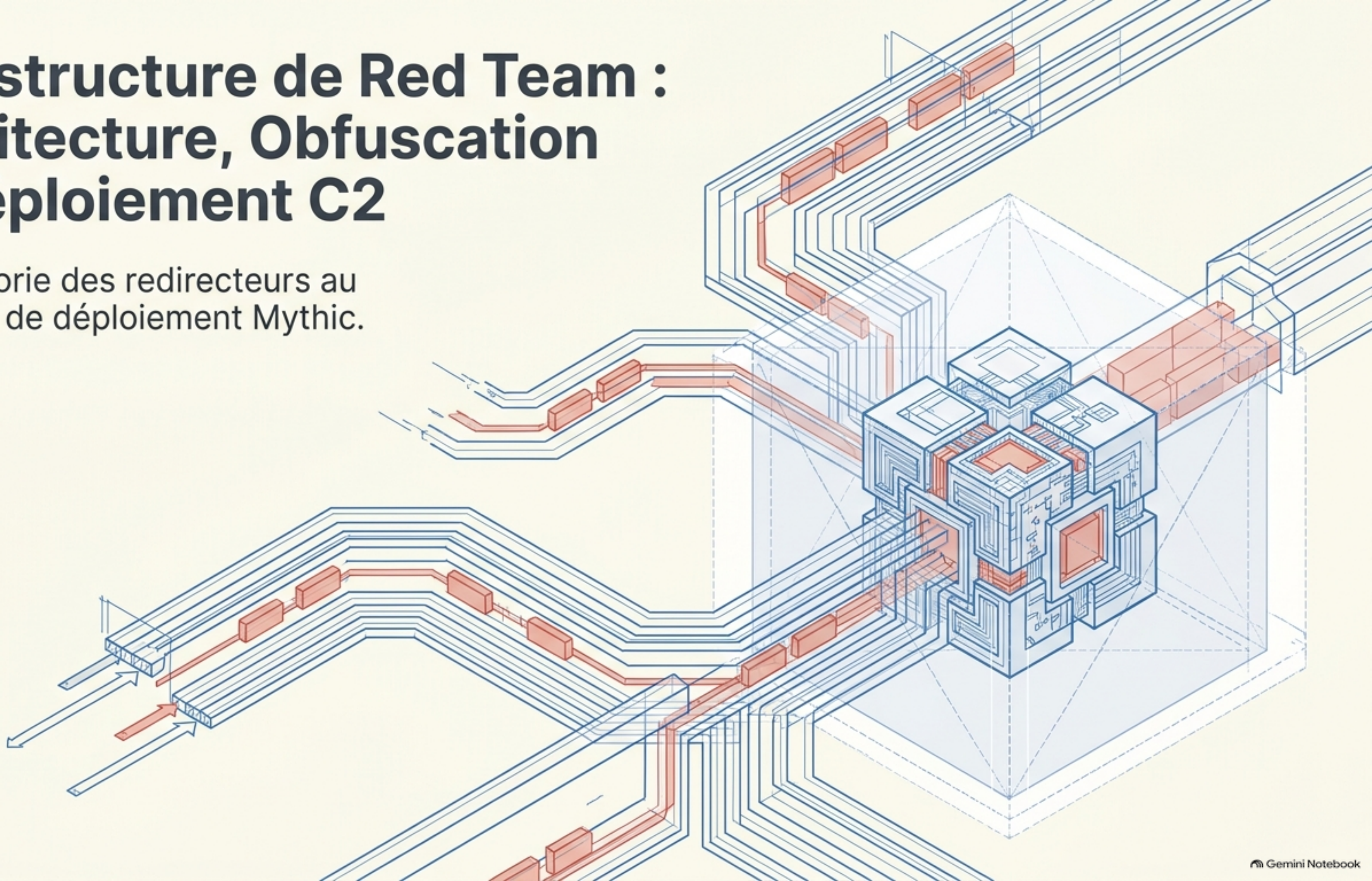


Infrastructure de Red Team : Architecture, Obfuscation et Déploiement C2

De la théorie des redirecteurs au
playbook de déploiement Mythic.



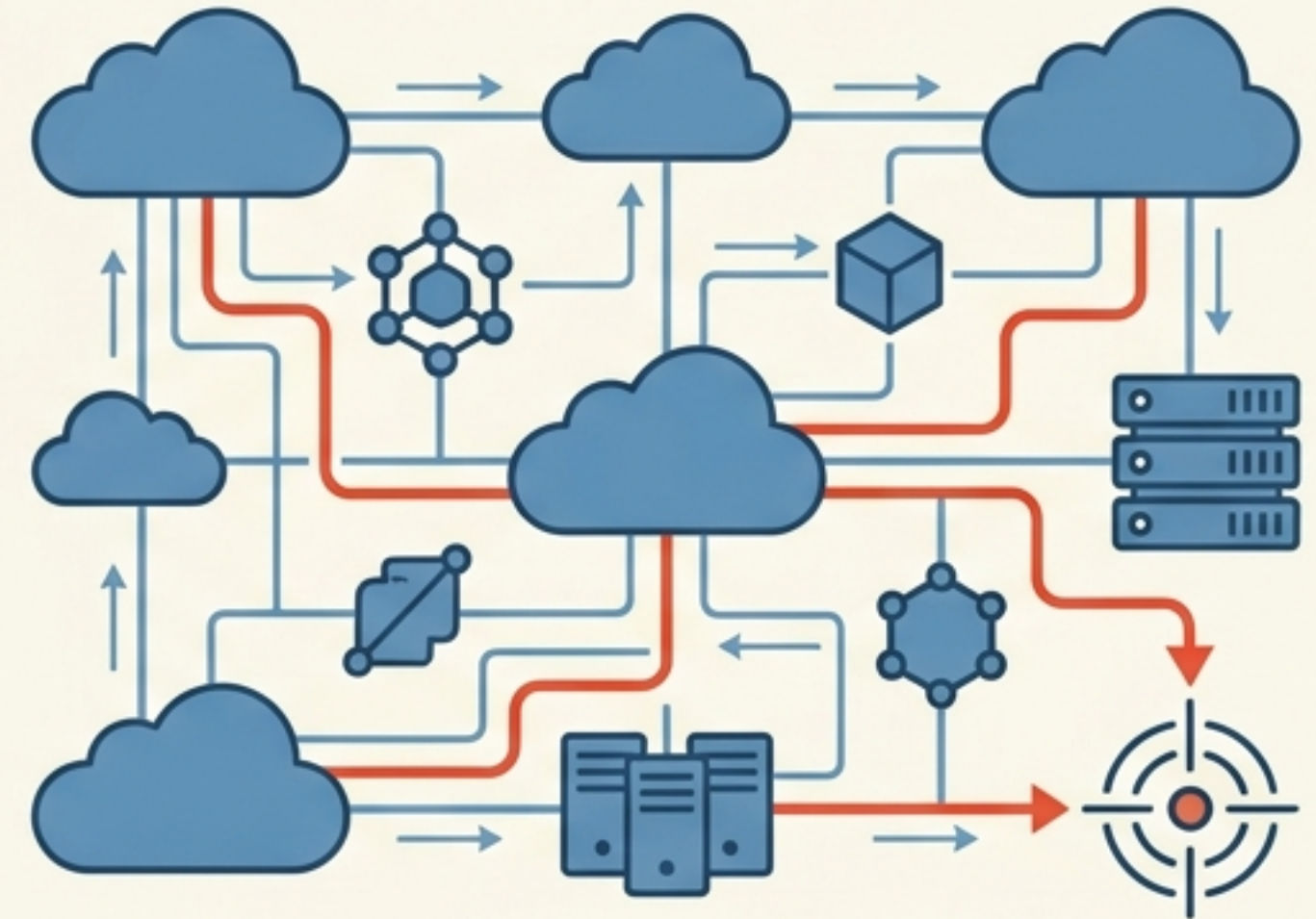
L'obfuscation par l'assimilation : L'évolution de l'infrastructure C2

Avant : Le paradigme rigide



- Serveurs auto-hébergés isolés.
- Charge opérationnelle lourde.
- Infrastructure facilement identifiable par les équipes de défense (Blue Teams).

Aujourd'hui : La résilience Cloud



- Déploiement cloud dynamique et élastique.
- Le trafic d'attaque se fond dans le trafic légitime des fournisseurs réputés (Microsoft, Google).
- Filtrage périmétrique rendu extrêmement complexe pour les défenseurs.

Les canaux de communication : Dissimuler les commandes

Canal 1 : HTTPS (Méthode privilégiée)

La quasi-totalité des réseaux autorise le trafic web HTTPS. Le chiffrement empêche l'inspection du contenu, noyant les commandes C2 dans le bruit de fond.



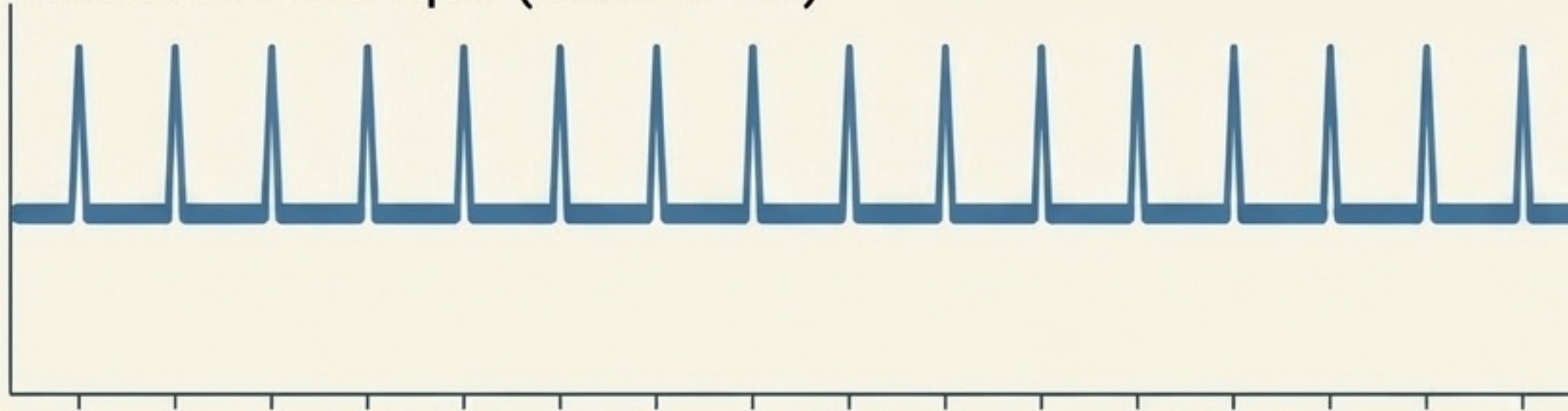
Canal 2 : DNS over HTTPS (DoH)



Encapsule les requêtes de résolution DNS dans un tunnel HTTPS chiffré (ex: pointant vers cloudflare-dns.com). Contourne la surveillance réseau classique, bien que certains réseaux bloquent le DoH non standard.

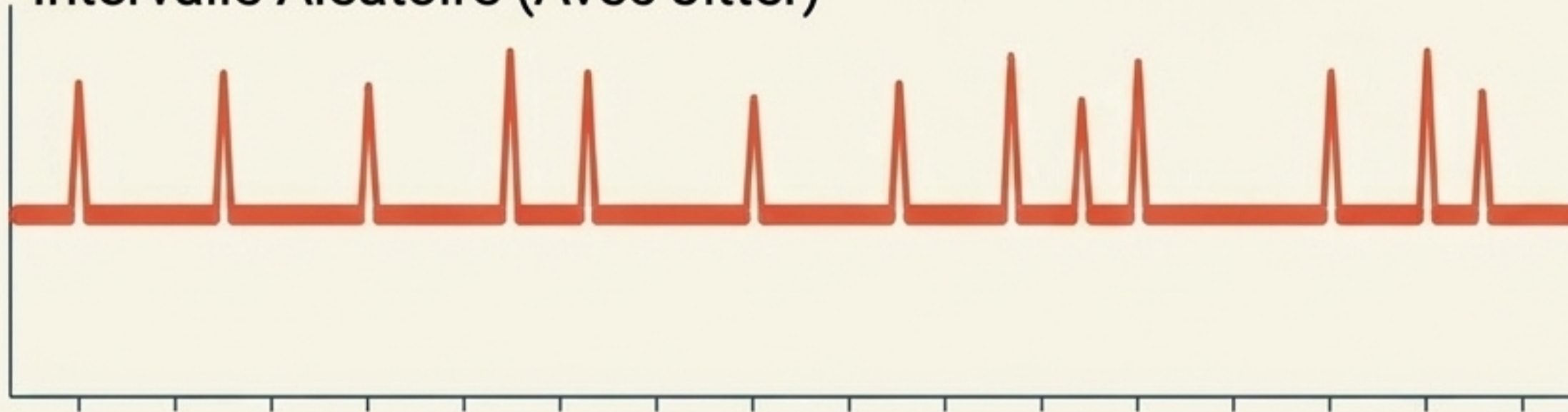
L'art de l'imprévisibilité : L'intégration du « Jitter »

Intervalle Statique (Sans Jitter)



Hautement détectable par l'analyse comportementale du réseau. Les modèles réguliers trahissent une automatisation mécanique.

Intervalle Aléatoire (Avec Jitter)

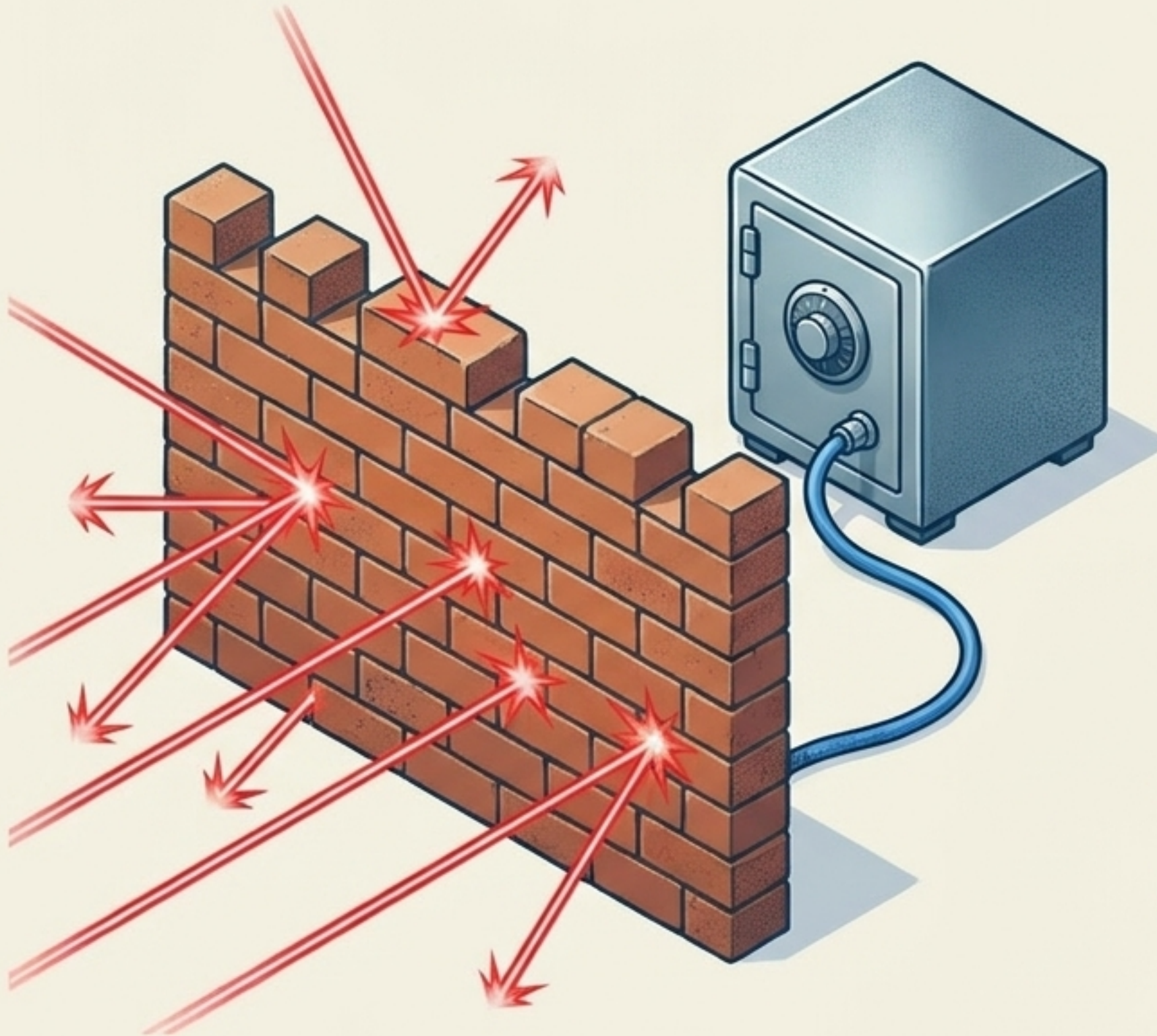


Le « Jitter » (variation aléatoire) applique un pourcentage de déviation à l'intervalle de rappel. La randomisation du signalement de l'agent détruit les modèles prévisibles recherchés par les défenseurs.

Évaluation de l'arsenal : Matrice des Frameworks C2

Solutions Commerciales (Nighthawk, Cobalt Strike)	Solutions Publiques (Mythic, Sliver, Havoc)
✓ • Développées via R&D propriétaire. ✓ • Clés en main, prêtes au déploiement. ✓ • Intégration native des BOF et SOCKS. Risque OPSEC : Détection par signature (EDR) fréquente si les paramètres par défaut sont conservés.	✓ • Architecture plug-and-play (Interface React + Backend Docker pour Mythic). ✓ • Implants multi-plateformes (Linux, macOS, Windows). ✓ • Haute flexibilité de personnalisation en cours d'opération. Avantage tactique : Mappage direct des TTPs avec le framework MITRE ATT&CK.

Le bouclier tactique : Protéger le serveur C2



Niveau 1 : Socat / Iptables

1

Transfert aveugle (Dumb pipe). Toutes les connexions sont relayées. OPSEC très faible.

Niveau 2 : Proxy Inverse (Apache / Nginx)

2

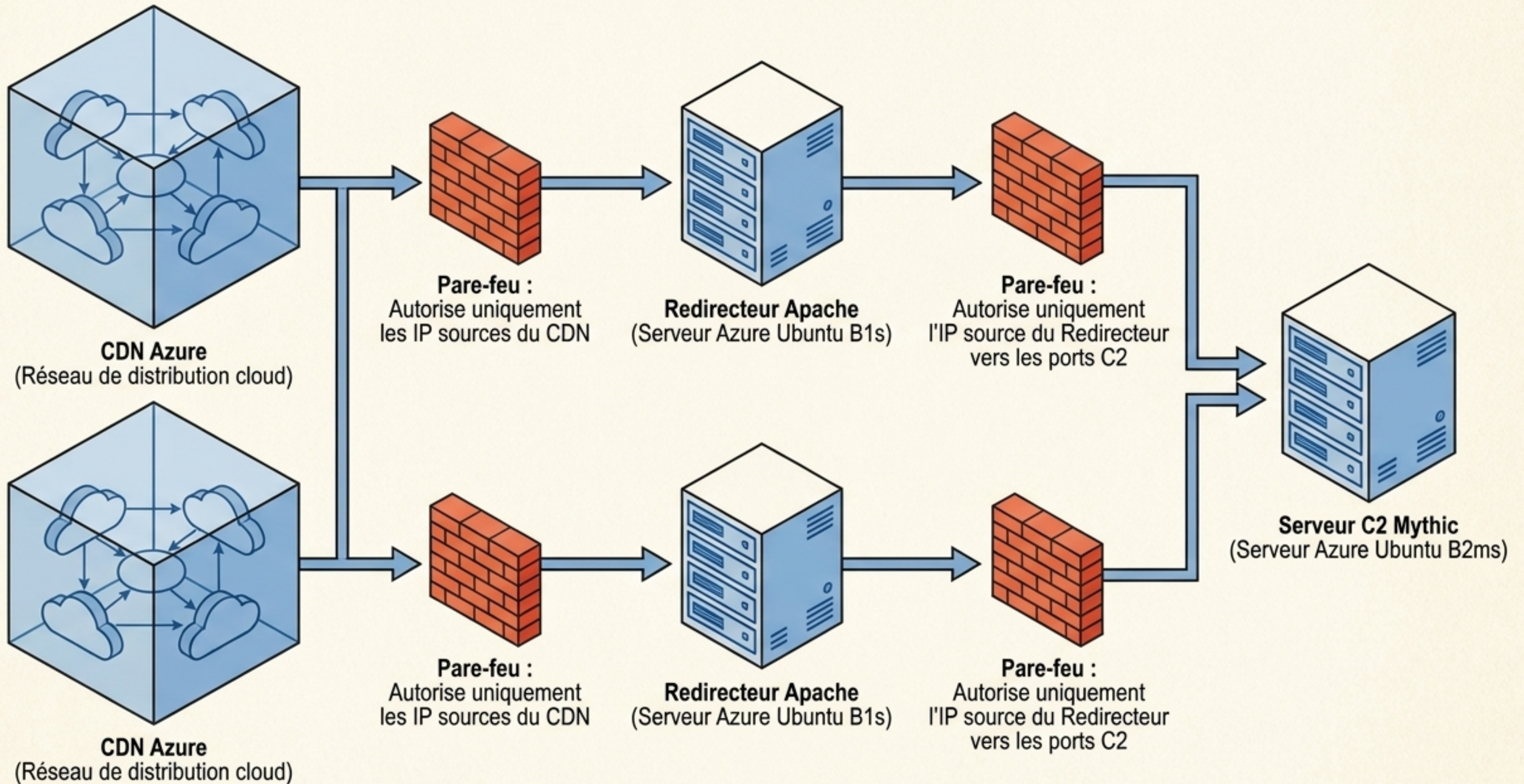
Protection de l'identité backend.
Exploitation de certificats SSL externes.
Filtrage basique par règles (ex: User-Agent).

Niveau 3 : CDN + Réécritures d'URL

3

Distribution géographique. Filtrage réseau strict n'autorisant que les adresses IP sources du CDN.
Manipulation d'URL à la volée. Le standard moderne.

Le Plan d'Architecte : Architecture C2 moderne



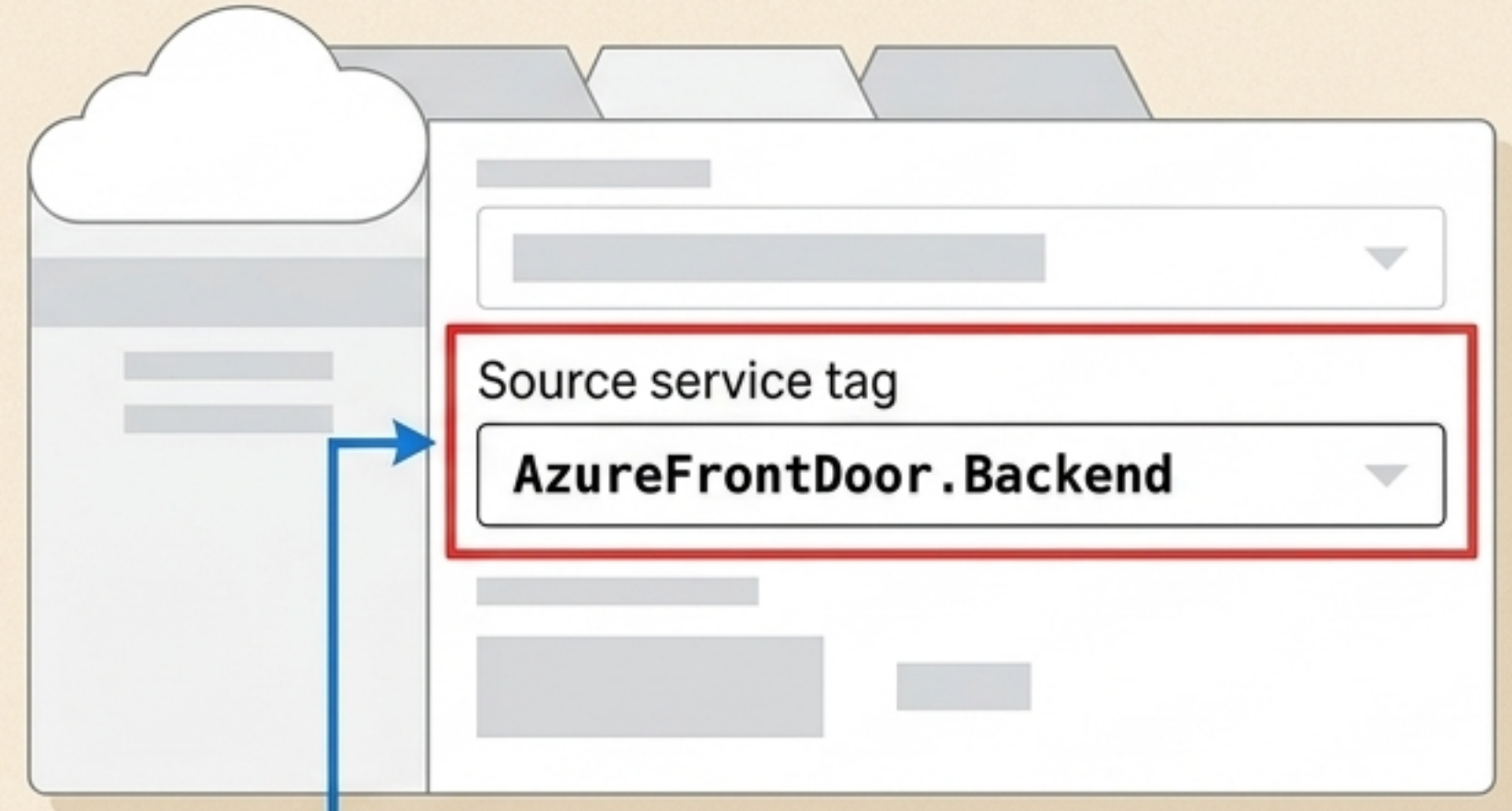
Étape 1 : Déploiement et filtrage du Redirecteur Apache

Configuration Apache

```
sudo apt update  
sudo apt install apache2  
a2enmod ssl proxy remoteip rewrite proxy_http
```

Activation des modules de proxy inverse et de réécriture.

Filtrage Pare-feu Azure



Critique : Le redirecteur doit rejeter tout trafic Internet direct. Seules les requêtes transitant par l'infrastructure du CDN Azure sont autorisées.

Étape 2 : Identité SSL et contournement des altérations CDN

Génération du Certificat

```
certbot certonly --standalone -d domaine.com  
  
cp /etc/letsencrypt/live/domaine.com/privkey.pem $MYTHICDIRECTORY  
cp /etc/letsencrypt/live/domaine.com/fullchain.pem $MYTHICDIRECTORY
```

Les ports 80/443 sont ouverts temporairement pour l'authentification Let's Encrypt, puis refermés pour n'accepter que le CDN.

Désactivation des altérations CDN



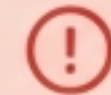
Paramètres CDN

Compression



Caching rules

Bypass caching



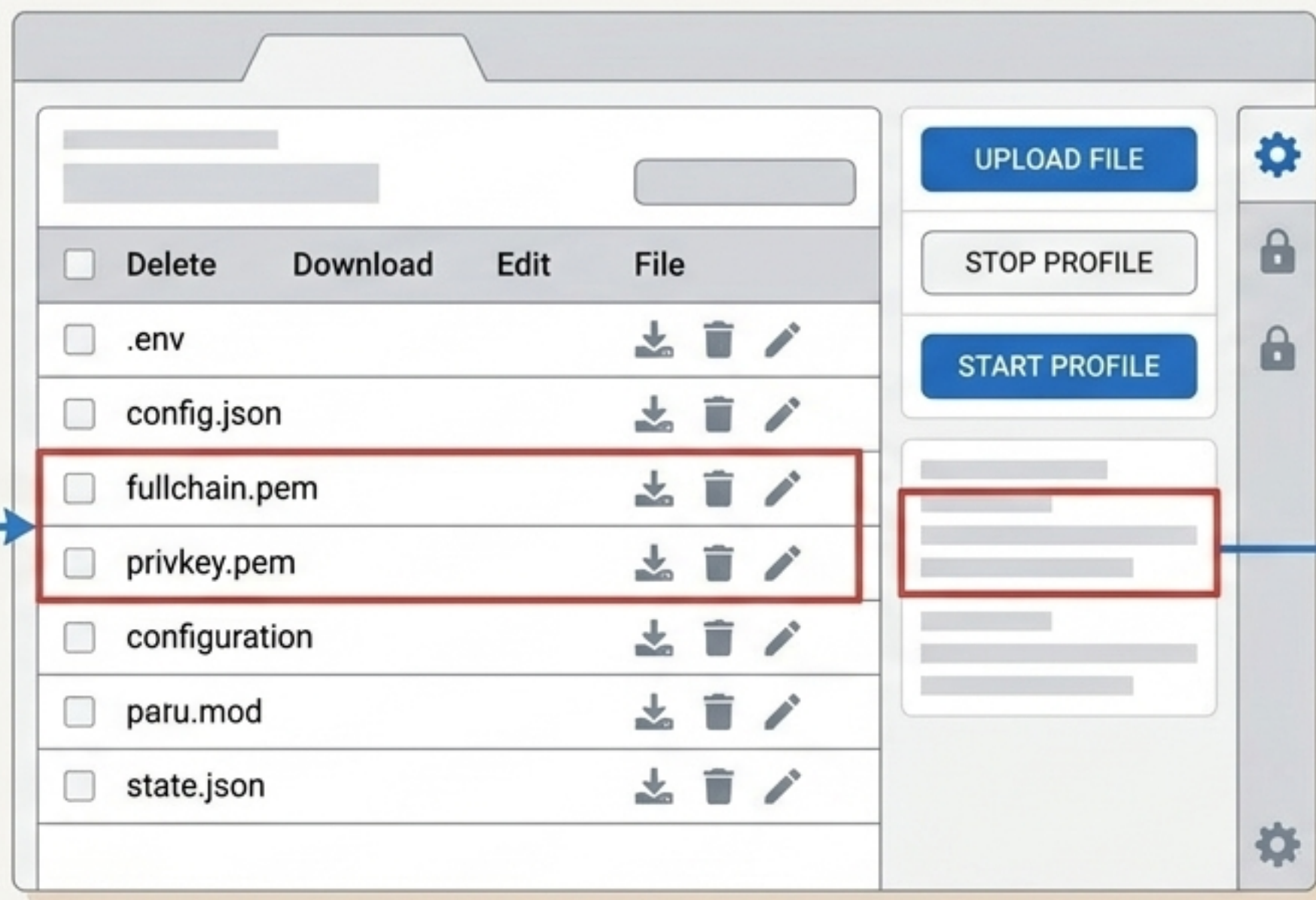
Si le CDN compresse ou met en cache le trafic, il corrompt les communications C2 de l'agent. **Ces paramètres doivent impérativement être désactivés pour maintenir l'intégrité du tunnel.**

Étape 3 : Falsification des en-têtes (Profil C2 Mythic)

1

Intégration SSL manuelle :

Association des certificats *fullchain.pem* et *privkey.pem* générés précédemment.

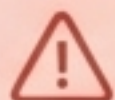


2

Falsification d'identité (Spoofing) :

Modification des requêtes pour imiter le trafic légitime.

```
"Server": "Microsoft-IIS/10.0"
```



Règle d'or : Ne jamais utiliser les profils HTTP par défaut, sous peine de déclencher des alertes basées sur les signatures réseau standards.

Étape 4 : Génération de l'agent Apollo (.NET)

1. Définition de la cible

- Système d'exploitation : Windows.
- Type de charge utile : Apollo.
- Sélectionné pour ses capacités avancées de post-exploitation.

2. Format de sortie

- Format : `WinExe`
- Génération d'un exécutable standard pour valider le flux de bout en bout.

3. Intégration des TTPs

- Sélection des commandes à compiler statiquement dans l'agent.
- Inclut l'exécution de code non managé, communication pair-à-pair et module SOCKS5.
- Objectif : Limiter les téléchargements de modules supplémentaires en cours d'opération.

Validation de l'infrastructure de bout en bout

Phase 1 : Vérification du routage Cloud



```
curl -I https://[cdn-endpoint].azureedge.net
HTTP/2 405 Method Not Allowed
date: Sun, 23 Jun 2024 20:20:25 GMT
content-type: text/plain
content-length: 22
x-azure-ref: <snipped>
x-fd-int-roxy-purgeid: 0
x-cache: TCP_MISS
```

Explication

Un code HTTP 405 confirme que le trafic traverse le CDN, atteint le redirecteur et frappe le backend Mythic sans erreur de routage, même si aucune payload n'est demandée.

Phase 2 : Exécution et Callback



Processus

L'agent est exécuté sur la cible, la connexion traverse l'infrastructure masquée, et le callback apparaît dans l'interface opératoire.

Opérations avancées : Le tunnel Proxy SOCKS5



Principe OPSEC fondamental : L'utilisation du proxy SOCKS permet d'exécuter des outils offensifs massifs à travers le tunnel C2, en opérant directement dans la mémoire de la victime, sans jamais déposer d'exécutable binaire sur son disque dur.

La Checklist OPSEC : Résilience de l'Infrastructure



1. Isolation Stricte (Pare-feu)

Le backend C2 ne communique qu'avec le redirecteur.
Le redirecteur ne communique qu'avec le tag de service `AzureFrontDoor.Backend`.



2. Chiffrement Omniprésent

Aucune communication HTTP en clair autorisée.
Utilisation stricte de certificats TLS/SSL légitimes de bout en bout.



3. Obfuscation Active

Paramétrage systématique du « Jitter » pour casser les modèles temporels d'analyse comportementale.
Falsification des en-têtes HTTP.



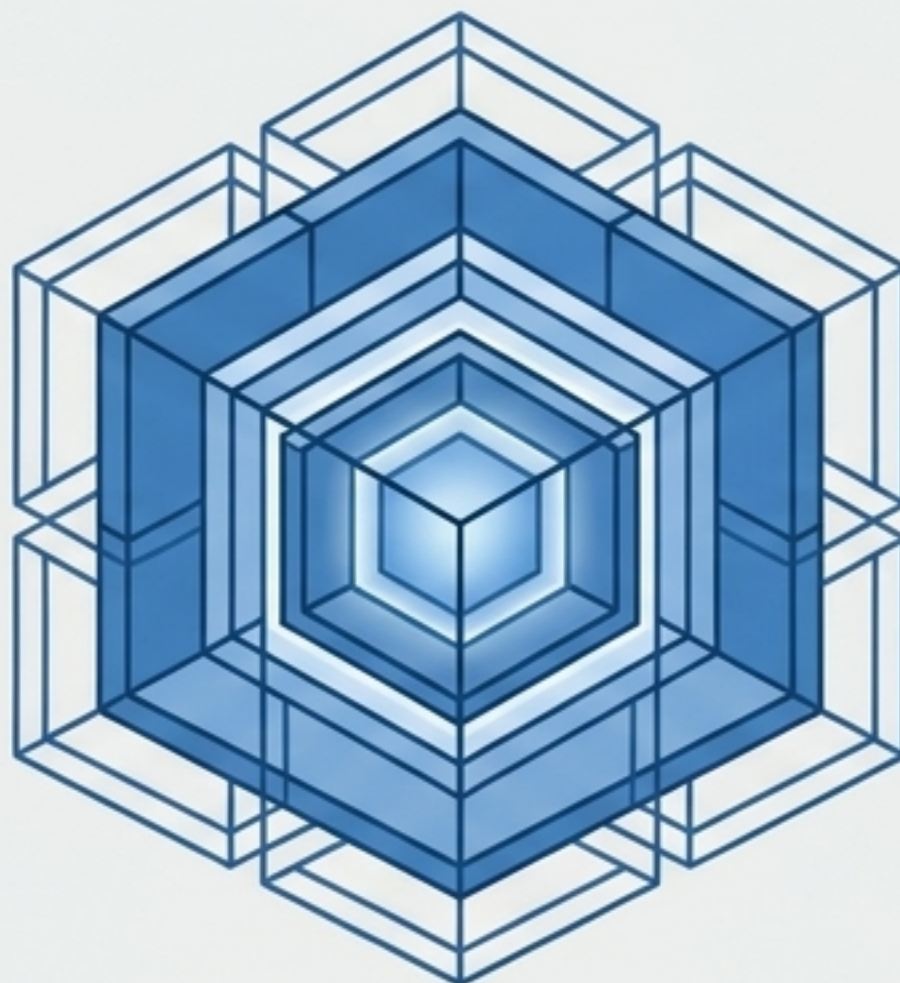
Opérateur

Hôte C2

4. Ségrégation des Rôles

L'opérateur attaque depuis une machine distincte via des tunnels SSH, jamais directement depuis l'interface de l'hôte hébergeant le serveur C2.

L'architecture est votre premier vecteur de réussite



Une sécurité opérationnelle défailante au niveau du canal C2 garantit la détection. Le succès d'une équipe Red Team ne se mesure pas seulement à la sophistication de ses exploits logiciels, mais à sa capacité structurelle à se fondre silencieusement dans le bruit de fond légitime de l'entreprise ciblée.