

Dossier technique

« Déploiement d'une gateway sécurisée dans le cloud »

Sommaire.

1. Analyse du besoin et enjeux techniques	2
1.1 Contexte	2
1.2 Problématiques Identifiées	2
1.3 Objectifs de la Mission	2
2. Architecture technique	3
2.1 Schéma des Flux	3
2.2 Choix technologiques et justifications	3
3. Mise en Œuvre : Sécurisation et Optimisation	4
3.1 Durcissement du Système (OS Hardening)	4
3.2 La Protection Applicative (WAF/IPS)	4
3.3 Optimisation de la Latence (Kernel Tuning)	4
4. Configuration Avancée Nginx (Snippet DRY)	5
5. Les procédures (Annexes)	6
1. Mise en place de NGINX	6
2. Mise en place de Tailscale	6
4. Mise en place de Crowdsec	6

1. Analyse du besoin et enjeux techniques.

1.1 Contexte

L'infrastructure Loutik héberge des services (GitLab, Site Internet, Blog, Speedtest, Affine et d'autres services) dans un environnement « On-Premise » contraint (Réseau domestique derrière CGNAT/Box opérateur, IP Dynamique).

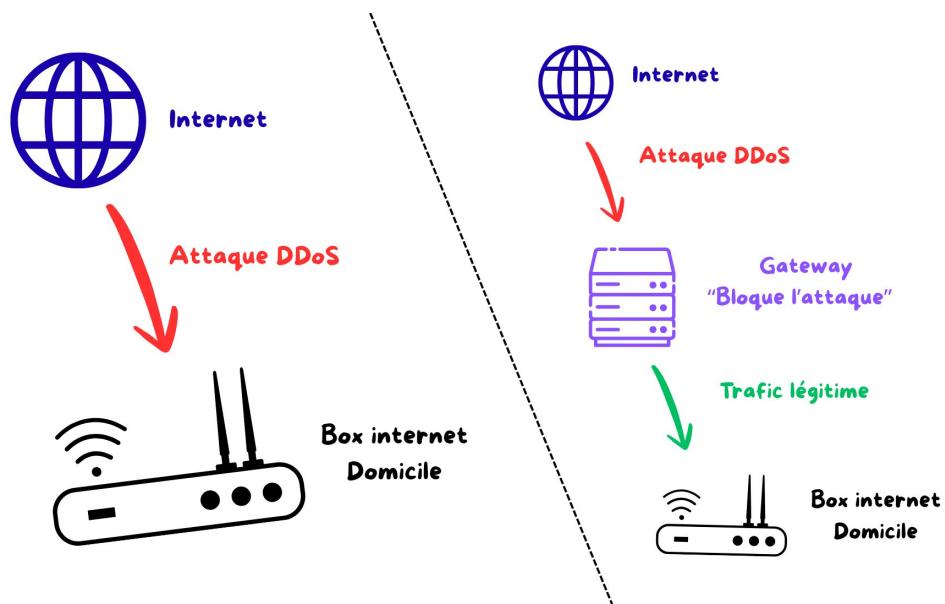
1.2 Problématiques Identifiées

- Surface d'attaque** : l'exposition directe de l'IP résidentielle présente un risque de sécurité majeur (DDoS, Intrusion LAN).
- Disponibilité** : l'absence d'IP fixe publique rend l'accès aux services instable.
- Sécurisé Applicative** : les pare-feux réseau traditionnels (L3/L4) sont inefficaces contre les attaques applicatives (L7) type scans de vulnérabilités ou encore Brute Force lent.

1.3 Objectifs de la Mission

Concevoir et déployer une **Passerelle de Sécurité Déportée (Edge Gateway)** capable de :

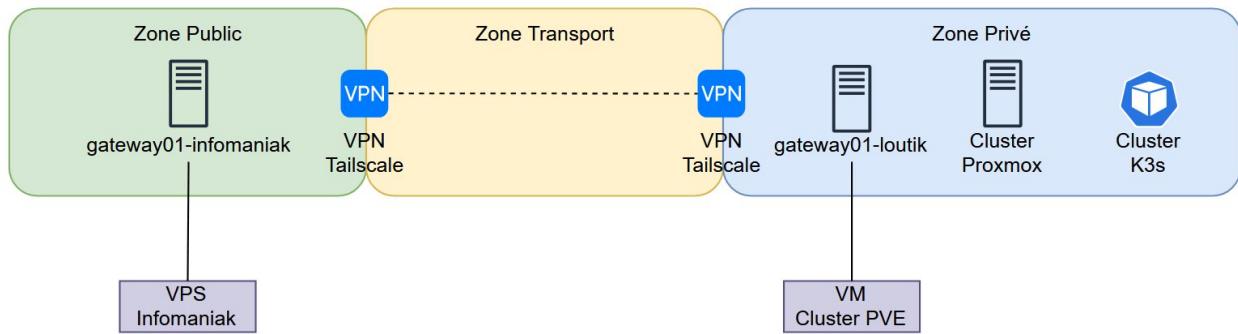
- Masquer** totalement l'infrastructure interne (Architecture Zero Trust).
- Filtrer** le trafic malveillant en amont (Mitigation DDoS & IPS).
- Assurer** la continuité de service via un réseau Overlay résilient.



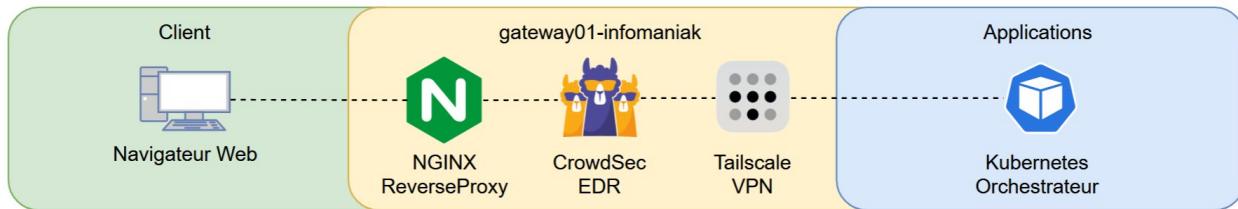
2. Architecture technique.

2.1 Schéma des Flux :

Infrastructure :



Fonctionnement :



2.2 Choix technologiques et justifications

Composant	Solution	Justification technique
Point d'entrée	VPS Cloud (Infomaniak)	Offre une IP fixe, une bande passante (500Mb/s) et isole le risque hors du domicile.
Réseau Overlay	Tailscale (WireGuard)	Protocole UDP performant, chiffrement ChaCha20, et capacité de traversée de NAT (NAT Traversal) sans ouverture de port locale.
Reverse Proxy	Nginx	Gestion asynchrone des connexions, support natif HTTP/2, et terminaison SSL performante.
Sécurité (IPS)	CrowdSec	Approche collaborative (CTI) permettant de bloquer les IPs réputées dangereuses avant même qu'elles n'attaquent.

3. Mise en Œuvre : Sécurisation et Optimisation.

3.1 Durcissement du Système (OS Hardening)

Le VPS étant le seul point exposé publiquement, une politique de sécurité stricte a été appliquée :

- SSH : Changement du port par défaut (22 -> 2045), interdiction de l'authentification par mot de passe (PasswordAuthentication no), usage exclusif de clés cryptographiques.
- Micro-segmentation : Utilisation des ACLs Tailscale pour restreindre les flux. Le VPS ne peut communiquer qu'avec les serveurs applicatifs (192.168.1.200/29) et non avec le reste du LAN (Imprimantes, IoT).

3.2 La Protection Applicative (WAF/IPS)

Mise en place de CrowdSec en mode "Défense en Profondeur" :

1. **Couche Réseau (Firewall Bouncer)** : Interaction directe avec « nftables » pour dropper les paquets des IPs bannies.
2. **Couche Applicative (Nginx Bouncer)** : Inspection des logs HTTP pour détecter les comportements suspects (Scans Nikto, SQL Injection, Bad User-Agent).

Exemple de détection d'attaque « Slow Brute Force » :

ID	Source	Scope:Value	Reason	Action	Country	AS	Events	expiration	Alert ID
30083	crowdsec	Ip:27.79.46.166	crowdsecurity/ssh-slow-bf	ban	VN	7552 Viettel Group	12	3h59m18s	86
30082	crowdsec	Ip:167.99.44.10	crowdsecurity/ssh-slow-bf	ban	NL	14061 DIGITALOCEAN-ASN	14	3h58m22s	85
30080	crowdsec	Ip:45.140.17.124	crowdsecurity/ssh-bf	ban	RU	198953 Proton66 000	6	3h57m59s	83
30072	crowdsec	Ip:45.135.232.92	crowdsecurity/ssh-bf	ban	RU	198953 Proton66 000	6	3h38m10s	75
30068	crowdsec	Ip:91.202.233.33	crowdsecurity/ssh-bf	ban	TM	200593 Prospero 000	6	3h25m30s	71
30053	crowdsec	Ip:193.32.162.157	crowdsecurity/ssh-slow-bf	ban	RO	47890 Unmanaged Ltd	12	2h9m17s	56
15041	crowdsec	Ip:64.225.79.203	crowdsecurity/ssh-slow-bf	ban	NL	14061 DIGITALOCEAN-ASN	14	1h56m6s	43
15040	crowdsec	Ip:20.83.27.149	crowdsecurity/CVE-2022-41082	ban	US	8075 MICROSOFT-CORP-MSN-AS-BLOCK	1	1h55m20s	42
15038	crowdsec	Ip:167.94.138.181	crowdsecurity/http-bad-user-agent	ban	US	398324 CENSYS-ARIN-01	2	1h51m31s	40

3.3 Optimisation de la Latence (Kernel Tuning)

Une problématique de "Timeout" a été détectée lors des pannes backend : le noyau Linux par défaut effectue 6 réessais TCP (env. 63s) avant d'abandonner une connexion.

Action corrective : Modification des paramètres « sysctl » pour améliorer l'expérience utilisateur (UX).

```
# /etc/sysctl.conf
net.ipv4.tcp_syn_retries = 2 # Réduit le délai d'abandon à ~3 secondes
```

4. Configuration Avancée Nginx (Snippet DRY).

Afin de garantir une maintenabilité maximale et de respecter le principe DRY (Don't Repeat Yourself), la configuration a été modularisée via des "Snippets".

Extrait du fichier « /etc/nginx/sites-available/gitlab.loutik.fr.conf » :

```
server {
    listen 443 ssl http2;
    server_name gitlab.loutik.fr;

    # Sécurité SSL & HSTS (Strict-Transport-Security)
    include /etc/nginx/snippets/ssl-loutik.conf;

    # Gestion des erreurs personnalisées & Timeouts
    include /etc/nginx/snippets/error_pages.conf;

    location / {
        proxy_pass [http://192.168.1.209](http://192.168.1.209);
        proxy_set_header X-Forwarded-Proto https;
        # ...
    }
}
```

Expérience utilisateur (UX) : Mise en place de pages d'erreurs 502 personnalisées pour informer l'utilisateur de l'état du service, remplaçant la page par défaut de Nginx.

Capture d'écran de l'erreur 502 :



5. Les procédures (Annexes).

1. Mise en place de NGINX

- [Mise en place de NGINX sur gateway01-infomaniak](#)



2. Mise en place de Tailscale

- [Mise en place de Tailscale sur les gateways](#)



4. Mise en place de Crowdsec.

- [Mise en place de CrowdSec sur gateway01-infomaniak](#)

