



Service Informatique
ASSURMER
2022

Présentation des fonctionnalités de la solution retenue

Date	Rédacteur	Valideur
30 novembre 2022	LE DOHER Loïc ZAMBON Ronan POISSONNIER Mattéo KENNEDY John-Killian	

Table des matières

Introduction : Proxy et Reverse Proxy, qu'est-ce que c'est ?.....	3
Le Proxy	3
Reverse Proxy	3
Présentation de différentes solutions	5
Haproxy	5
HeartBeat	6
Solution retenue.....	7

Introduction : Proxy et Reverse Proxy, qu'est-ce que c'est ?

Le Proxy

Un serveur Proxy est un intermédiaire entre un client et un serveur distant. Le proxy va aller contacter le destinataire de la requête afin de protéger le client, en effet ce système est utilisé pour fournir un accès à Internet plus sécurisé.

De cette manière le proxy applique un filtrage afin de bloquer certains sites ou un type en particulier.

La mise en cache est une autre fonctionnalité du proxy, cela va permettre de retourner plus rapidement une requête déjà enregistrée.

La compression est une fonctionnalité permettant de réduire le poids des pages afin d'alléger la charge sur le client.

La journalisation (création de logs) permet de garder une trace sur tout ce qui a été fait sur le proxy.

Il permet l'anonymat puisque les pages web ne verront que le proxy.

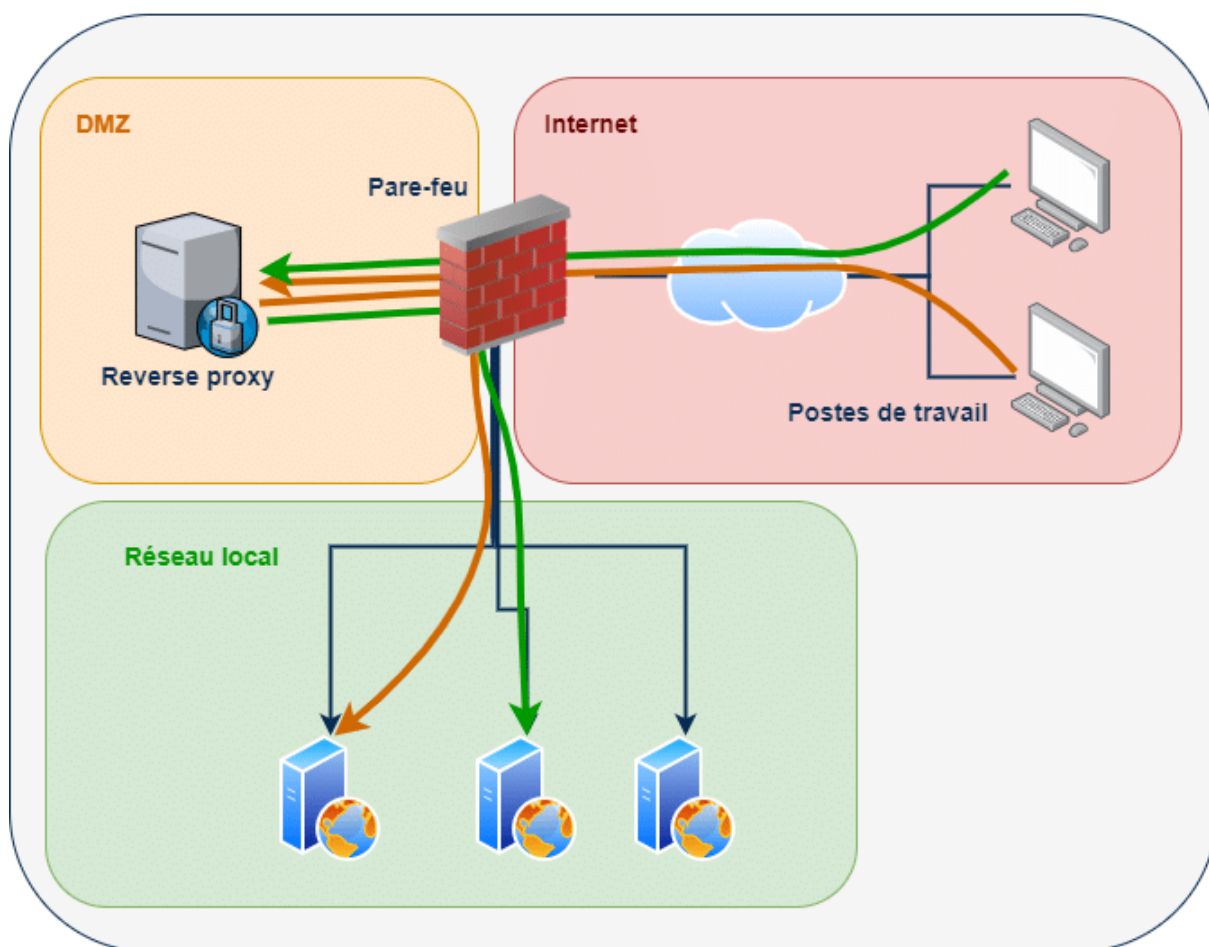
Le serveur Proxy va donc pouvoir contacter Internet à la place du client, filtrer le contenu, mettre en cache le site, intégrer dans les logs la recherche puis le retourner au client, le site quant à lui ne verra que le serveur Proxy.

Reverse Proxy

Un reverse proxy va permettre de sécuriser un serveur interne d'un utilisateur externe, c'est le même fonctionnement que le proxy classique mais pour protéger une infrastructure de l'extérieur.

Un utilisateur externe qui voudrait accéder à des données interne va contacter le proxy, celui-ci va cacher les clients qui sont derrière le proxy, il va aller chercher les informations nécessaires et les afficher à l'utilisateur externe.

Pour illustrer le fonctionnement voici un schéma :



Un utilisateur externe fait une requête au proxy, qui va ensuite aller contacter les serveurs du réseau local pour afficher les ressources de façon sécurisée.

Présentation de différentes solutions

Haproxy

HAProxy est une solution libre, fiable et très performante de répartition de charge de niveau 4 (TCP) et 7 (HTTP). Elle est particulièrement adaptée aux sites web fortement chargés qui nécessitent de la persistance ou du traitement au niveau 7.

La fiabilité est l'un, sinon le point fort d'HAProxy. Il est par exemple utilisé par des sociétés apparaissant au classement Fortune 500 pour servir des millions de pages chaque jour.

Cette fiabilité ne s'est pas faite au détriment des performances : HAProxy requiert peu de ressources, et son architecture évènementielle mono-processus lui permet facilement de gérer plusieurs milliers de connexions simultanées sur plusieurs relais sans effondrer le système.

Enfin, la sécurité est au rendez-vous : pas une seule vulnérabilité en 4 ans. De plus, HAProxy est capable de se chrooter¹ et de diminuer ses privilèges au lancement.

¹chroot (change root) est un appel système qui a également donné son nom à une commande des systèmes d'exploitation Unix permettant de changer le répertoire racine d'un processus de la machine hôte.

Cette commande permet d'isoler l'exécution d'un programme et d'éviter ainsi la compromission complète d'un système lors de l'exploitation d'une faille. Si un pirate utilise une faille présente sur l'application chrootée, il n'aura accès qu'à l'environnement isolé et non pas à l'ensemble du système d'exploitation. Cela permet donc de limiter les dégâts qu'il pourrait causer. Cet environnement est appelé un « chroot jail » en anglais, littéralement une prison.

Il permet également de faire tourner plusieurs instances d'un même ensemble de services ou démons sur la même machine hôte.

Par exemple, il est possible avec chroot d'exécuter des applications 32 bits sur un système 64 bits : il suffit pour cela d'avoir un sous-système qui intègre toutes les bibliothèques logicielles nécessaires ; chroot permet de se connecter à l'intérieur de ce sous-système et d'y exécuter les applications installées.

HeartBeat

HeartBeat ou est un système permettant, sous Linux, la mise en cluster (en groupe) de plusieurs serveurs.

C'est plus clairement un outil de haute disponibilité qui va permettre à plusieurs serveurs d'effectuer entre eux un processus de fail-over².

Le principe du "fail-over" est le fait qu'un serveur appelé "passif" ou "esclave" soit en attente et puisse prendre le relais d'un serveur "actif" ou "maitre" si ce dernier serait amené à tomber en panne ou à ne plus fournir un service.

² *Tolérance de panne*

Solution retenue

Notre choix s'est porté sur Haproxy, car c'est une solution libre et très utilisée. Elle nécessite peu de ressources tout en proposant une haute capacité de connexions simultanées.

De plus, le reverse proxy est réputé pour être sécurisé (aucunes failles découvertes).

Et en plus il est français !!!