Présentation du projet d'auto-hébergement du club Kr[HACK]en

Pierre Coimbra

Contents

1 Préface

Ce document est une documentation non technique qui n'abordera pas ce qu'il y a derrière l'infrastructure (Redondance des services clé, communication entre les deux PC, configuration du cluster...). Une documentation beaucoup plus technique qui part de zéro et détaille la mise en place de l'infrastructure est disponible à cette adresse.

`https://git.elukerio.org/pcoimbra/serveur_proxmox_krkn`

Nous présentons ici les objectifs du projet, l'infrastructure matérielle et logicielle et l'articulation globale des services.

2 Motivation du projet

D'abord, l'idée est d'héberger tous les outils utilisés par le club (Web, NextCloud,Git...) afin d'avoir un contrôle total sur les services que nous utilisons. Ensuite, nous voudrions mettre en place une structure capable d'accueillir des environnements de CTF correctement cloisonnés par rapport aux services permanents du club.

3 Gestion du serveur en interne

Nous sommes conscients que, dans un tel projet le plus dur n'est pas de monter l'infrastructure mais de la maintenir au fil des années. Les responsabilités seront donc gérées de manière extrêmement strictes, avec plusieurs niveaux d'accès. Il faudra en effet différencier le poste de webmestre, qui ne pourra agir que sur la partie applicative, de celui de l'administrateur système qui aura l'accès global. De grands pouvoirs appelant de grandes responsabilités, les adminsys en poste auront la charge de former leur successeurs.

Pour la gestion en interne du serveur, nous nous organiserions de la manière suivante :

- Seules deux personnes du bureau auront le rôle d'administrateur système, soit tous les droits sur le serveur.
- Le responsable technique du club aura le rôle de webmestre, il pourra intervenir sur les services comme le site web, le cloud... Cependant, il ne pourra pas toucher à l'infrastructure autour.
- Tous les membres actifs du club auront accès aux services web.

4 Présentation de l'infrastructure

4.1 Infrastructure matérielle

Du côté infrastructure, nous disposons d'un rack 1U avec deux PC à l'intérieur possédant chacun 24Go de DDR3-ECC et un Xeon x5670 6 Coeurs cadencé à 2.93 GHz. Côté stockage, nous allons mettre en place un RAID1 ZFS avec deux disques par PC (les données du premier disque seront aussi présentes sur le second) ainsi le stockage sera répliqué pour éviter toute perte de données.

4.2 Infrastucture logicielle

Les deux PC accueilleront Proxmox comme hyperviseur ; un hyperviseur permet à plusieurs systèmes virtualisés de travailler sur une seule machine physique en même temps en se partageant les ressources disponibles.

En effet, Proxmox est une solution de virtualisation open source qui propose à la fois des machines virtuelles KVM et des containers LXC. C'est l'équivalent gratuit de VMWare ou de Hyper-V. Grâce à Proxmox, nous pourrons faire de nos deux PC un seul PC virtuel en montant un Cluster. A partir de maintenant, nous parlerons plus que de ce PC virtuel en ignorant toute ce qu'implique une mise en Cluster.

Pour mieux comprendre comment les services seront disposés sur le serveur, il faut se dire que chaque service aura un contenant uniquement pour lui (VM ou container) et qu'il ne pourra communiquer que selon des règles bien précises avec l'hyperviseur (Proxmox) et les autres contenants.

4.3 Les différents services

Nous allons présenter rapidement les services que nous envisageons mais n'aborderons pas ici ce qui permet d'accéder à ces services (Firewall, Proxy...)

N'oublions pas :

1 service = 1 contenant

4.3.1 Les services

Il y aura deux types de services,

- Ceux qui sont directement accessibles depuis Internet derrière le pare-feu, ce sont les services frontend.
- Ceux qui sont accessibles uniquement à travers une frontend, ce sont les services backend.

4.3.2 Services "sensibles"

L'infrastructure du club s'articulait de la manière suivante :

- Le site web du club.
- Le Wiki du club.
- Un serveur mail pour remplacer le service fourni par OVH.

Avec en plus,

- Un annuaire LDAP (slapd), qui permettra d'avoir un compte unique pour chaque utilisateur et de définir différents groupes d'utilisateurs.
- Un cloud (NextCloud) pour mettre en commun des fichiers au sein du club et l'ordre du jour des réunions.
- Un serveur Git (Gitea) sur lequel toutes les sources des challenges du club seront stockées ainsi que la documentation du club.
- Un service de messagerie instantanée du type Mattermost.
- Et d'autres services...

Ce qui permettrait d'auto-héberger tous les services du club.

4.3.3 Services CTF

L'objectif est de remplacer la banque de challenge du club stockée actuellement sur un poste en B141. Celui-ci n'est pas documenté, ce qui réduit les modifications que nous pouvons y apporter.

A partir des sources des challenges actuels, une nouvelle infrastructure CTF prendra forme. Elle s'organisera de la manière suivante :

- Un premier CTFd avec tous les challenges du club utilisés pour les OpenCTF.
- Un autre CTFd que nous utiliserons pour les sessions en externe, comme par exemple pour la session 0.
- Une VM avec différents environnements Docker temporaires pour les challenges système.
- Une VM avec différents environnements Docker pour les challenges Web.

4.4 Articulation globale

Il y aura trois switchs virtuels afin de séparer la partie administration de la partie commune.

Un switch = Une partie

Dans chaque partie, il y aura des sous-parties que l'on appellera ici zones.

Une partie = Plusieurs zones

De même, dans chaque zone, il y aura un type de services.

Une zone = Un type de service

Un switch contiendra donc plusieurs zones qui contiendront elles-mêmes un type de service.

4.4.1 Schéma de l'infrastructure

Ce schéma décrit l'infrastructure réseau, chaque partie est détaillée sommairement ci-dessous.

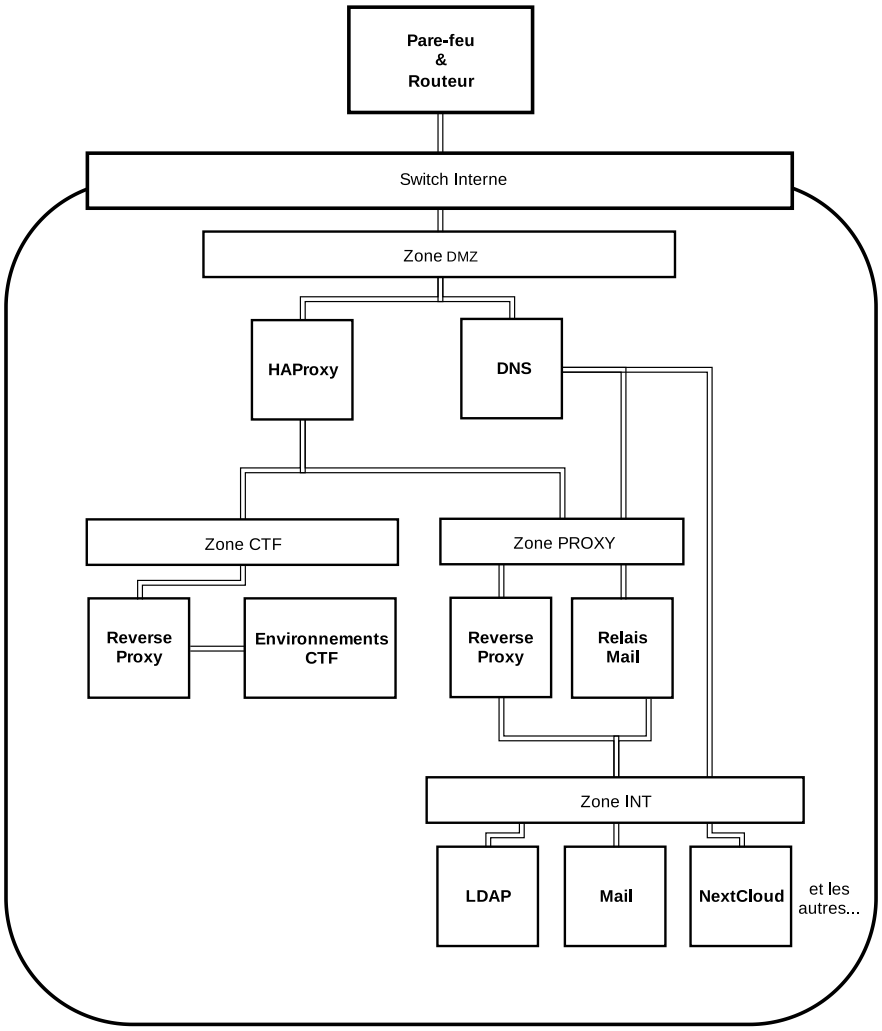

Figure 1: Topologie réseau du switch interne

4.4.2 Les Switchs

- Un switch WAN (extérieur), qui permettra de réaliser le lien entre l'extérieur et les pare-feux et entre les pare-feux et les hyperviseurs.
- Un switch virtuel (partie interne), en séparant le tout en plusieurs zones, gèrera l'accès à Internet des services qui ne sont pas directement derrière le pare-feu (Nextcloud, Git, Serveur Web...) et les services qui sont directement derrière le pare-feu (HAProxy, DNS et Proxy Interne).
- Un switch virtuel (partie administration) pour toutes les tâches d'administration

Pour ce qui est du switch interne, sa topologie est détaillée dans le schéma. Nous avons omis le Proxy Interne et le switch administration (tous les contenants y sont reliés).

4.4.3 Partie Interne

Du côté switch interne, il y aura quatre zones pour les services frontend :

- DMZ sera située juste après le pare-feu ; elle contiendra les loadbalanceurs (HAProxy) et le serveur DNS.
- PROXY sera placée juste après la zone DMZ et contiendra les reverses proxy pour les services autres que les environnements CTF ainsi qu'un relais mail entre l'extérieur et le serveur mail. Ce relais permettra de filtrer les mails.
- INT contiendra les containers des services permanents. La liaison entre INT et PROXY se fera à travers les reverses proxy NGINX et la Mail Gateway.
- CTF sera la zone dédiée au reverse proxy CTF et aux containers/VMs des environnements CTF. Le lien avec l'extérieur se fera directement au niveau de la DMZ via HAProxy.

Par exemple, les requêtes qui arrivent sur le port 80 ou 443 du pare-feu seront retransmises à HAProxy, qui décidera ensuite de transmettre la requête aux reverses proxy de la zone ROUTE ou au reverse proxy de la zone CTF.

4.4.4 Partie Administration

Du côté du switch administration, il y aura plusieurs zones, non détaillées ici, car elles serviront uniquement à l'administration du serveur, ce qui n'est pas l'objet de cette présentation.

4.5 Options pour l'accès au serveur depuis l'extérieur

Dans cette partie, on n'ignore plus le fait que nous avons deux PC distincts dans le serveur.

L'accès au serveur depuis l'extérieur se fera via le pare-feu (une VM pare-feu sur chaque PC).

Plusieurs possibilités on été envisagées pour l'accès au serveur depuis l'extérieur. Elles seront triées par ordre de préférence.

Dans tous les cas, les deux pare-feux seront mis en cluster et accessibles via une seule IP qui passera d'un firewall à l'autre en fonction de la disponibilité de chacun d'eux.

- 3 IP publiques, une sur chaque pare-feux et une entre les deux pare-feux.
- 3 IP publiques, une sur chaque hyperviseur et une entre les deux pare-feux.
- 1 IP publique qui sera entre les deux pare-feu.

5 Pour aller plus loin...

Une documentation plus technique sur la façon de le mettre en place est disponible à cette adresse :

`https://git.elukerio.org/pcoimbra/serveur_proxmox_krkn`