Documentation relative à l'élaboration et la sécurité de l'infrastructure Mangi

Valentine BRAUD PLI3

7 août 2024

1 Introduction

Cette documentation a pour but de regrouper les solutions permettant de répondre aux besoins exprimés lors de l'idéation du projet "Mangî". Elle regroupe les solutions de sécurité concernant toutes les parties de l'infrastructure (Système, réseau, virtualisation).

2 Résumé des besoins

Mangî étant un projet d'étude, le rendu final doit être considéré comme un PoC (Proof of Concept). Il n'est pas destiné à être utilisé en production (multiples connexions de nombreux utilisateurs distants) mais doit cependant s'en rapprocher le plus possible dans sa conception. Nous allons donc pour la totalité du projet utiliser des services Open-source gratuits autant que possible.

les données récupérées au sein des bases de données doivent impérativement être sécurisées et à l'abri des défaillances matérielles ou erreurs de manipulation.

L'environnement de test doit pouvoir être disponible pour l'ensemble du groupe. Pour simuler l'environnement de production au plus proche, le PoC doit pouvoir être disponible publiquement et donc être sécurisé en conséquence.

3 Les solutions proposées

3.1 Sécurité des accès

Il existe ici plusieurs contraintes concernant la sécurité des accès. Les environnements de test et de production ont des contraintes totalement différentes. La nécessité de mettre en place la sécurisation des accès aux services impose la mise en place d'un pare-feu. Le projet étant un PoC, nous allons opter pour le logiciel "Pfsense". Cet OS à part entière, basé sur "FreeBSD" et utilisé en entreprise nous permettra toutes les configurations nécessaire au niveau du réseau pour sécuriser les accès.

3.1.1 Séparation des services et environnements

Pour faciliter l'administration et la sécurisation de l'infrastructure nous allons séparer proprement les différents services et environnements en fonction de leurs contraintes via les VLAN :

- VLAN 30 - L'environnement de test et les divers services de gestion annexe : Accès uniquement aux utilisateurs via le VPN. Tout trafic entrant est bloqué.
- VLAN 31 - L'environnement de production : Seul vlan autorisant les requêtes entrantes via des règles strictes.
- VLAN 32 - Réseau d'administration : Seul réseau ayant accès aux interfaces d'administration des services critiques (Pare-feu, hyperviseur). Accès extrêmement limité (administrateur).
- VLAN 33 - Réseau hébergeant les utilisateurs du VPN. Ceux-ci accèdent au VLAN 30 via celui-ci en respectant des règles strictes.

Chaque VLAN sont isolés les uns des autres. Des règles précises et restreintes permettent la communication inter-vlan.

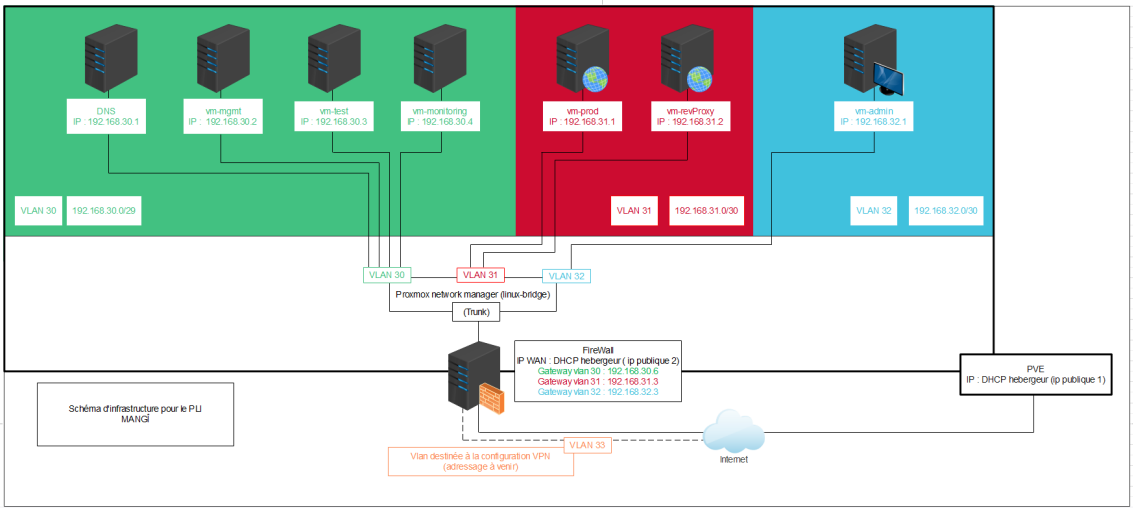

FIGURE 1 – Schéma de l'infrastructure

3.1.2 Restrictions des accès au sein d'un même VLAN

Les communications entre machines virtuelles au sein d'un même vlan sont régies par des règles de pare-feu. Celles-ci doivent être le plus restrictives possible. La dernière règle doit obligatoirement bloquer tout le trafic sur toutes les VM et protocoles.

3.1.3 Mise en place d'une DMZ

La DMZ (pour zone démilitarisé) n'est uniquement destinée pour les services autorisant les requêtes entrantes. Par conséquent, seul ce Vlan autorise les requêtes entrantes venant de l'interface WAN.

3.1.4 Mise en place d'un accès via VPN

Afin de pouvoir accéder de manière sécurisée au VLAN 30, nous allons mettre en place un accès par VPN SSL. Les utilisateurs connectés via celui-ci appartiennent au VLAN 33 et les accès au VLAN 30 sont gérés par des règles de routage inter-vlan. Le routage et le protocole de connexion pour le VPN sont gérés par le pare-feu.

3.1.5 Administration séparée

Le VLAN 32 hébergeant une unique VM doit lui seul avoir les accès aux interfaces d'administration sensible tel que le pare-feu et l'hyperviseur. Les autorisations d'accès à cette VM spécifique seront aussi extrêmement restreints.

3.2 Sécurisation de l'environnement de production

La DMZ est avant tout destinée à protéger les autres Vlan des potentielles menaces extérieurs. La sécurisation de l'environnement de production doit encore être géré. Afin de surveiller le trafic entrant sur celui-ci, nous allons mettre en place un reverse proxy en amont associé à fail2ban. Le reverse proxy permet entre autre l'anonymisation du serveur d'origine et fail2ban une protection contre les attaques bruteforce.

3.3 Sécurisation des données

Les données récupérées sur les bases de données des différents environnement ne sont pas à l'abri de suppressions accidentelles. Il est donc nécessaire de s'en prémunir par différents moyens selon l'origine de la suppression.

3.3.1 Tolérance aux pannes

Afin d'empêcher la perte des données suite à la panne d'un ou plusieurs disques, il est possible de mettre en place un système RAID. Deux RAID peuvent ici être utilisés permettant une tolérance à au moins un disque en défaut :

— Le RAID 1 : Utilisation de N disques redondants. La capacité de stockage est égale à celle du plus petit disque ou groupe de disques.

— Le RAID 5 : Utilisation de N+1 disques, N*capacitéPour1 étant la capacité totale disponible. La capacité de stockage totale est plus importante que le RAID 1. Cependant, la reconstruction des données après une défaillance demande une grande quantité de ressources.

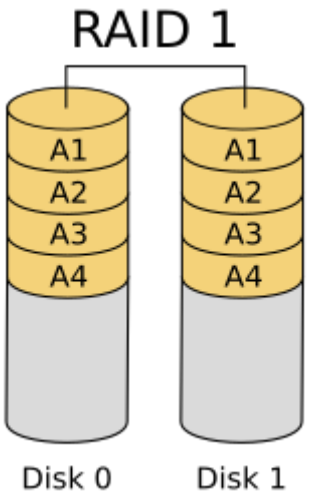

Figure 2 – Principe du RAID 1

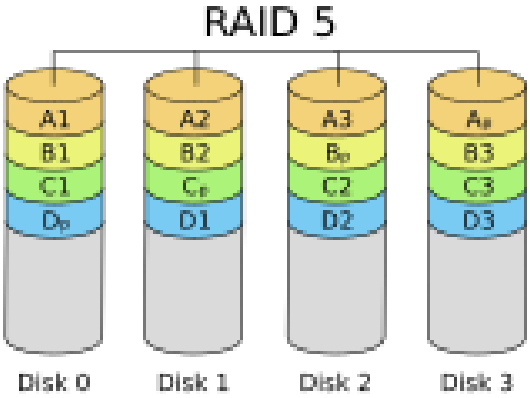

Figure 3 – Principe du RAID 5

3.3.2 Mise en place de sauvegardes des données importantes

Le RAID ne met pas totalement à l'abri les données sensible en cas de nouvelle défaillance avant le remplacement du disque précèdent ou bien d'une erreur humaine. Il est donc important de mettre en place une solution de sauvegarde régulière. Cette sauvegarde sera réalisée sur un disque indépendant à horaires fixes (quotidien). Elle consistera à un dump des bases de données lancé via un script et ordonnancé via cron par exemple.

Une sauvegarde des VM elles même peut aussi être envisagée via un service tel que VEEAM backup.