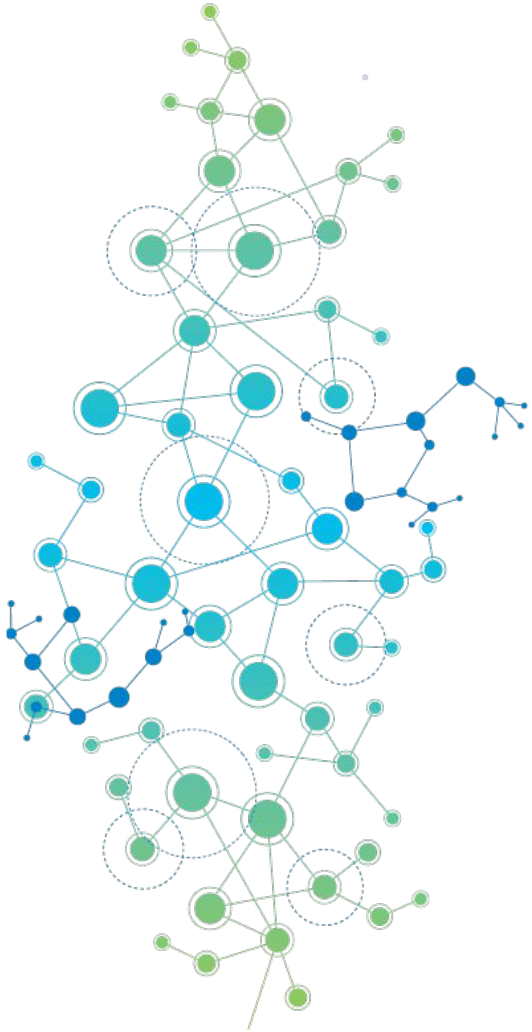


Maison des Ligues

Atelier Professionnel 2

Contexte et Problématiques

M2L, une entreprise possédant un réseau interne, souhaite solutionner deux problématiques actuels.

I. **M2L souhaite protéger et éviter les pénétrations dans ses systèmes**

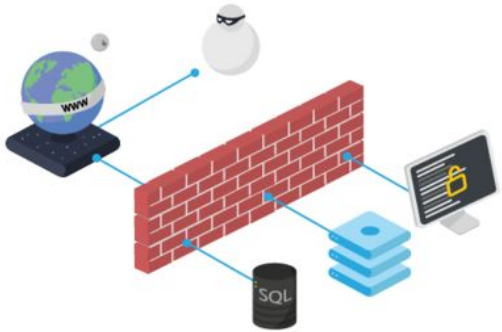
II. **M2L souhaite protéger les données sur ses serveurs**

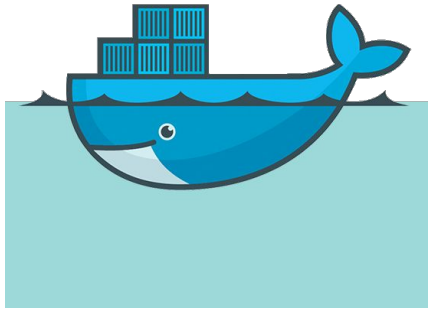
Maison des Ligues

Solutions proposées

Afin de protéger et d'éviter les pénétrations dans ses systèmes, nous proposons à M2L de mettre en place des **firewall**, autrement appelés **pare-feux**.

Et pour protéger leurs données sur leurs serveurs, nous allons leur apporter une solution de hachage et salage de leurs mots de passe, ainsi que de la conteneurisation sur leurs applicatifs et services.





Maison des Ligues

Sommaire

Maison des Ligues

1. Le Firewall

Maison des Ligues

Definition

Un Fortigate 60E, modèle de Firewall de Fortinet

Un firewall est outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau.

Il permet d'assurer la sécurité d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur afin d'empêcher des intrusions externe.

Il est appelle pare-feu, barrière de sécurité ou garde-barrière. Il est doté d’au moins deux interfaces, l'une destinée au réseau interne et l'autre au réseau externe.

Maison des Ligues

Politique de mise en place

Il existe deux grandes politiques de sécurité souvent soumises par l'administrateur :

- La plus sûre consiste à n'autoriser que les communications explicitement admises au nom du principe du moindre privilège.
- Interdire que les échanges explicitement prohibés.

La méthode la plus efficace est la première option, mais demande plus de manipulations. Les trois principales règles sont : accepter la connexion, la bloquer, ou refuser la demande de connexion sans prévenir l'émetteur.

Maison des Ligues

Modèles

Il existe plusieurs modèles de Firewall :

- Le plus ancien étant le **pare-feu sans état** (ou stateless firewall), mis en place sur les routeurs initialement.
  Son but et de comparer les paquet avec une liste de règles préconfigurées.

- Les **pare-feu à états** (ou stateful firewall), ils vérifient la conformité des paquets à une connexion en cours.

Maison des Ligues

Modèles

- Le **pare-feux identifiant** réalise l'identification des connexions passant à travers le filtre IP. L'administrateur peut ainsi définir les règles de filtrage par utilisateur et non plus par adresse IP ou adresse MAC, et ainsi suivre l'activité réseau par utilisateur.

- Le **pare-feux applicatif** est la dernière génération de pare-feu, ils vérifient la complète conformité du paquet à un protocole attendu.
  Par exemple, permet de vérifier que seul le protocole HTTP passe par le port 80.

Maison des Ligues

Utilisation

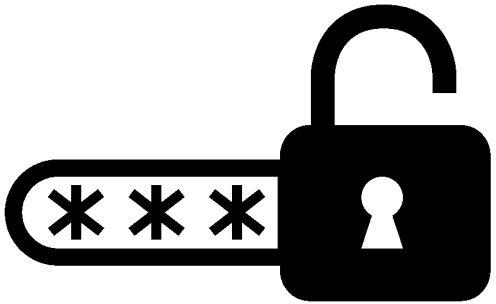
- Il peut être utilisé en entrée de réseau d’une entreprise, et installé sur chaque poste des utilisateurs afin de maximiser la protection.

- Installer 2 pare-feux de constructeur différent à l’entrée du réseau d’une entreprise est conseillé afin d'entourer la zone démilitarisée.

- Une zone démilitarisée est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet (ou d'un autre réseau) par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet, et qui n'ont pas besoin d'accéder au réseau local.

Maison des Ligues

2. Salage et hachage des mots de passe



Maison des Ligues

Définition hachage

Le hachage cryptographique est un type de calcul unidirectionnel.

Il prend une chaîne de données de n'importe quelle taille et donnent toujours une sortie d'une longueur prédéterminée.

Cette sortie est appelée valeur de hachage ou empreinte.

Le résultat pour une entrée donnée est toujours le même.

Maison des Ligues

Hachage

Le hachage des mots de passe apporte une sécurité.

C’est après cette transformation par un algorithme que le mot de passe est enregistré dans la base de données.

Par exemple, voici un mot de passe : **Maison2L2021***
Et voici son hache : **16d32b7cad273c329ee300ad721b0823**

Maison des Ligues

Hachage et avantages

- **Unidirectionnel** : Il n'existe aucun moyen pratique de déterminer quelle était l'entrée d'origine à partir d'une valeur de hachage.

- **Deux entrées n’auront pas la même empreinte**: Les valeurs de hachage sont considérées comme uniques.

- **La même entrée fournit toujours le même résultat :** Si vous mettez les mêmes informations dans une fonction de hachage, elle fournira toujours la même sortie.

- **Le moindre changement donne un résultat différent** : La valeur de hachage diffère au moindre changement.

Maison des Ligues

Salage

Le salage consiste à concaténer le mot de passe avec une chaîne de caractères quelconque, le plus souvent aléatoire, afin d'empêcher que deux informations identiques conduisent à la même empreinte.

Son but est de lutter contre les attaques utilisant des rainbow tables, les attaques par dictionnaire et les attaques par brute-force.

Pour ces deux dernières, le salage est efficace quand le sel utilisé n'est pas connu de l'attaquant ou lorsque l'attaque vise un nombre important de données hachées toutes salées différemment.

Maison des Ligues

Attaques possibles

L’attaque par dictionnaire : dictionnaire de mots de passe couramment utilisé et haché.

L’attaque par force brute, ou brute-force : il va hacher toutes les combinaisons possibles de lettres/chiffres/symboles : a, b, …, aaa, aab…Long mais les fonctions de hachage sont très rapides, efficace pour les mots de passe courts.

Les rainbow tables, ou tables arc-en-ciel : contiennent toutes les combinaisons possibles des mots de passe en fonction des paramètres choisis à la génération. Ils disposent de correspondances directes mot de passe <-> empreinte.

Maison des Ligues

Types de salage

- Statique : chaque mot de passe est salé avec la même chaîne de caractère
- Dynamique : chaque mot de passe est salé aléatoirement.

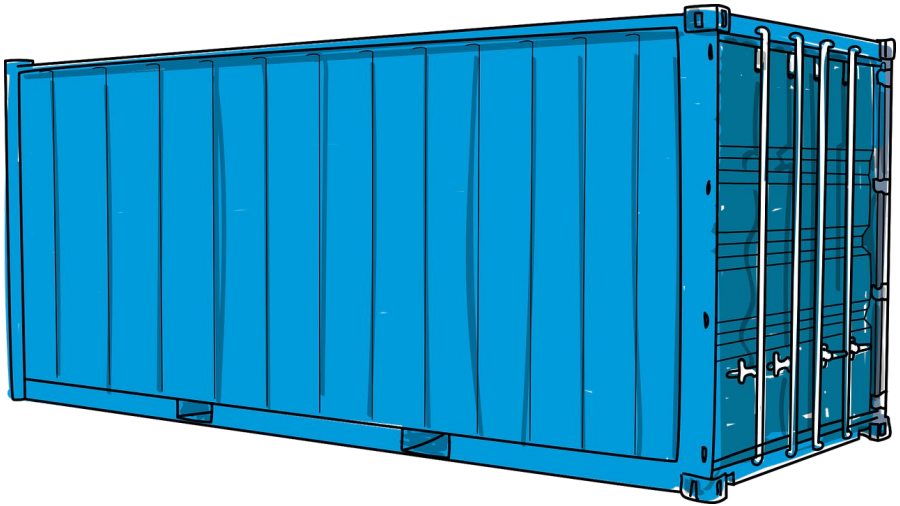
Exemple :

Si l'on veut un salage dynamique sécurisé, chaque enregistrement de la table de mots de passe du système d'authentification peut contenir les informations suivantes :

identifiant | hachage (mot de passe + salage) | salage

Maison des Ligues

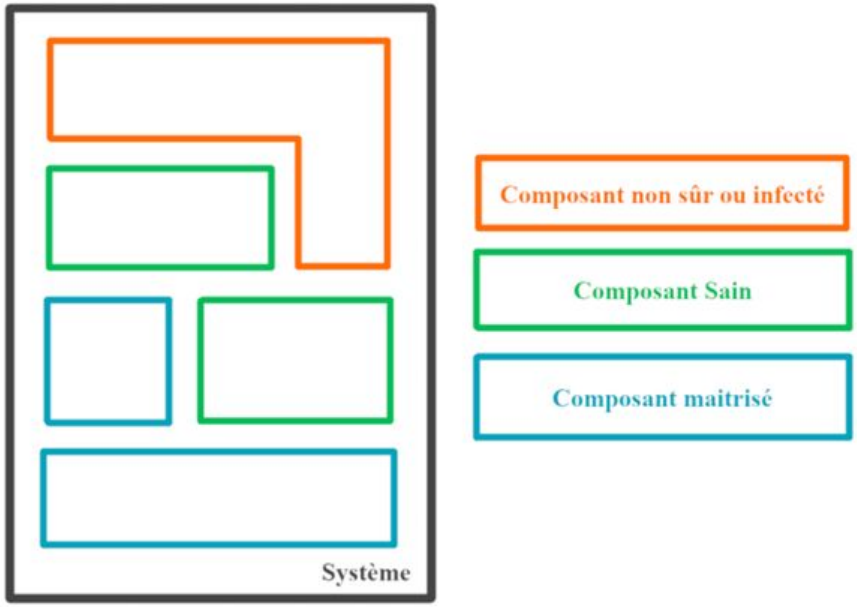
3. La conteneurisation



Maison des Ligues

Notions

Au sein d’un système unique, un certain nombre de composants sont amenés à travailler en parallèle.
Ceux-ci peuvent être développés en interne, sains ou non sûrs.



Maison des Ligues

Point clés de la conteneurisation

- **La portabilité :** il est nécessaire de fournir en plus de la livraison logicielle, une liste très précise de binaires et de librairies avec des versions exactes pour garantir que l'environnement de production sera équivalent à celui de développement.

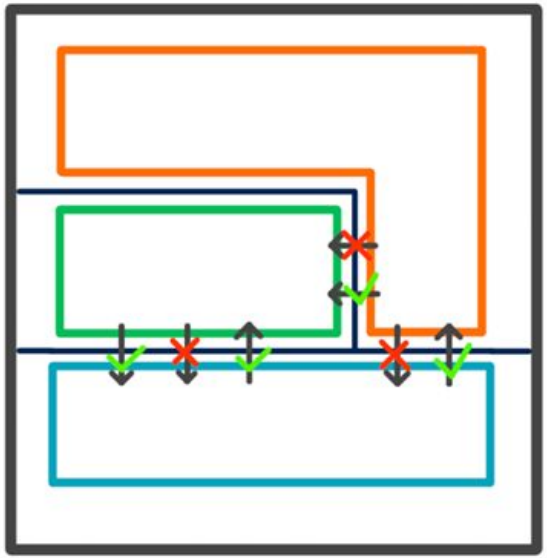
- **L'adhérence système :** sur un système exploité par plusieurs composants distincts, il est compliqué voire impossible d'identifier les librairies et configurations réellement nécessaires à la mise en production d'un composant.

- **La sécurité :** il nous faut une surface d'attaque et un surface de friction

Maison des Ligues

Conteneurisation

Conteneuriser les composant a pour objectif de créer des murs entre les composants afin de les cloisonner et ne permettre que les comportements et interactions autorisés par chaque composant.

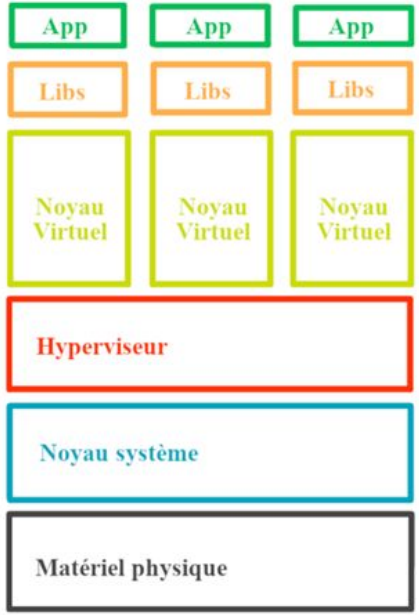


Maison des Ligues

Virtualisation standard

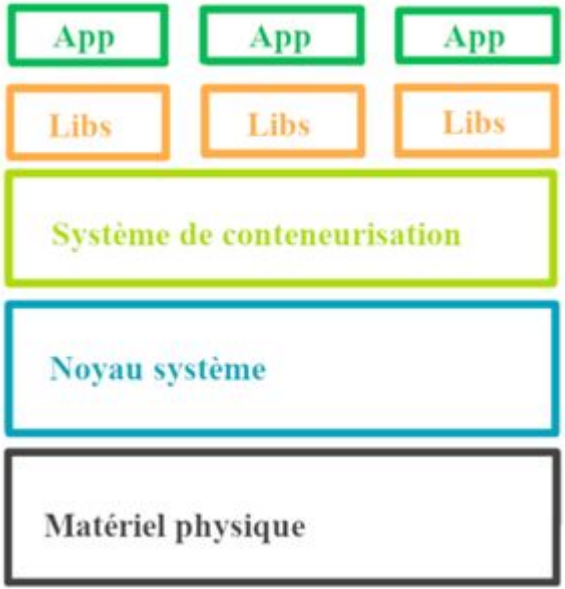
Cela permet de supprimer les problématiques de sécurité mais en amène de nouvelles :

- Consommation de ressource excessive ;
- Aucune flexibilité dans le déploiement ;
- Multiplication des besoins d'administration ;
- Création d'instabilité dans les déploiements ;
- Conservation des problématiques d'adhérence au système.



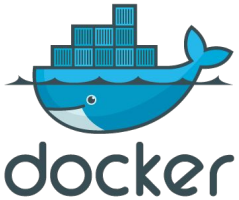
Maison des Ligues

Conteneurisation



La conteneurisation fonctionne sur le principe de partage du noyau hôte.

Le système le plus largement déployé à ce jour est Docker.



Maison des Ligues

Conteneurisation

Les ressources cloisonnées sont les suivantes :

- PID : Il n'accède qu'à son propre processus et n'a pas de vision sur les autres processus existants sur la machine ou dans les autres conteneurs ;
- MNT : Le conteneur n'accède qu'à ses propres points de montages ;
- NET : Le conteneur n'accède qu'à ses propres interfaces réseau ;
- Hostname

Maison des Ligues

Les plus de la conteneurisation

- Possibilité d'allumer et d'éteindre quasi instantanément un environnement car la base le noyau est déjà partagé ;
- Une portabilité qui permet de l'extraire et de le livrer à un client si besoin ;
- Une identifications des librairies utilisés plus claire ;
- Moins de surface d'attaque possible.

Maison des Ligues

Merci de votre attention

ALI Ahmed

CHARPAGNE Prince

KADRI Aurélien

LEGEDZA Thomas

LEMPEREUR Arthur

MERCIER Jeremy

OUDOT Maxime

SIEUDAT Thomas

SIREYZOL Erwan

Maison des Ligues