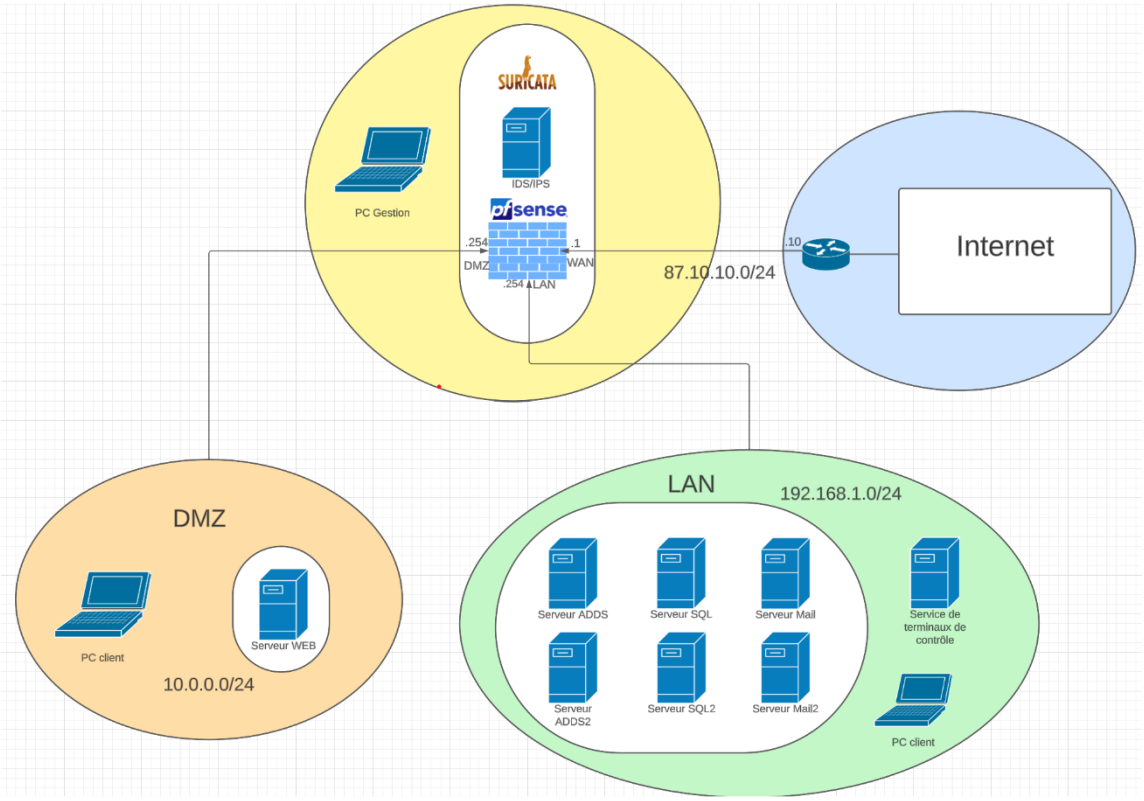
Ilyas TUNAY

Ibrahim DBOUK

Rapport de test

Pour rappeler le contexte, nous sommes des Ingénieurs en réseaux et sécurité, nous devons mettre en place une architecture sécurisé pour un réseau d'hôpital, avec la mise en place de différents services. Toutes les communications passe par un Pare-feu, qui est pour notre cas, Pfsense, un logiciel gratuit que nous allons mettre en place dans votre hôpital. Les communications sont filtrées via ce Pare-feu en fonction de l'architecture que nous proposons.

Premièrement, voici l'architecture réseau et sécurisé que nous avons mis en place :



Nous avons la mise en place de 4 cloisonnements avec différentes configurations :

- Une partie qui provient de l'extérieur, soit Internet, avec un routeur que nous avons mis en place via le logiciel gns3 qui peut être branché via un cloud directement sur notre réseau, donc pour notre part sur le port Wan de notre Pare-feu.

- Le deuxième cloisonnement contient principalement un PC de gestionnaire de notre IDS/IPS(Suricata) et notre firewall. Nous avons cloisonné cela car depuis notre logiciel de pare feu Pfsense nous pouvons installé un plugin de notre Suricata qui fera donc un lien entre nos deux logiciels. Suricata agira en plus du filtrage firewall en cas d'attaque ou d'anomalie détecté sur le réseau. Notre Pare-feu comprend donc un autre port Lan, puis un port DMZ.

- Le troisième cloisonnement comprend la DMZ (zone démilitarisée) de notre Pare-feu, dans lequel les machines sont accessibles depuis le réseau Internet. Ici, dans notre cas, nous avons mis en place dans la DMZ, le Serveur WEB. La DMZ héberge des machines du réseau interne qui doivent être accessibles depuis l'extérieur.

- Le quatrième cloisonnement comprend le port LAN du pare-feu, qui est un réseau local privé. Dans notre architecture, nous avons mis en place les serveurs d'authentification, de bases de données ainsi que de mails à cet endroit. Nous avons dupliqué ces serveurs pour avoir une architecture plus sécurisés et favorisés la redondance.

En effet, le côté LAN est la partie qui est sécurisés où sont hébergés les serveurs sensibles (avec des informations plus confidentielles), contrairement à la DMZ qui contient un serveur qui n'est pas autant sensible (serveur WEB), cela représente une stratégie visant à minimiser les risques d'attaque, en gardant un réseau fonctionnel.

De plus, en créant la DMZ, nous augmentons notre champ de test de contrôle pour les trafics que nous effectuons entre la DMZ, le réseau interne et Internet. Voici les règles que nous avons mis en place :

Pour le cloisonnement Internet :

- Les pings depuis Internet peuvent accéder uniquement au Pare-feu ainsi qu'à la DMZ.
- Aucun ping ne peut passer d'Internet vers le réseau local privé.

Pour le cloisonnement du Pare-feu :

• Toutes les trames passent par le Pare-feu, c'est à cet endroit que la décision est prise en fonction des règles pour déterminer si une trame peut passer d'un endroit à un autre.

Pour le cloisonnement de la DMZ :

• Les trames provenant de la DMZ peuvent aller vers Internet mais non vers le réseau privé.

Pour le cloisonnement du réseau privé local :

• Le réseau privé local peut discuter avec la DMZ ainsi qu'avec le réseau WAN (Internet), mais aucun des deux ne peut discuter directement avec l'autre.

Les différents équipements peuvent communiquer en temps normal, mais suite à la mise en place et la configuration du Pare-feu dans l'architecture, certains sont bloqués et d'autres autorisés.

Pour l'instant les tests de trafics sont réalisés à 70%, nous finalisons correctement les détails de la mise en place pour avoir la meilleure architecture de réseau sécurisés possibles.

Remarques :

- Il faut limitée autant que possible les communications non nécessaires depuis la DMZ vers Internet.
- Des mises à jour régulières doivent être mis en place.
- En pleine réflexion là-dessus, nous allons peut-être mettre en place des graphes MRTG pour les serveurs de terminaux de contrôle pour avoir un aperçu des informations. (En pleine réflexion)