# **1.Etude de l’existant**

* **Contexte**

La sécurité des systèmes d'information fait face à des menaces de plus en plus complexes, variées et automatisées. Dans ce contexte, les pare-feux jouent un rôle essentiel en protégeant les réseaux informatiques. Ils contrôlent les flux de données en filtrant les connexions, qu’elles soient autorisées ou interdites. Chaque action du pare-feu génère des journaux d’événements (logs) détaillés, contenant des informations techniques telles que les adresses IP, les ports utilisés, les protocoles, ainsi que les décisions de filtrage (acceptation ou rejet).

Cependant, avec l’explosion du volume de trafic réseau et la sophistication croissante des cyberattaques, ces logs deviennent extrêmement volumineux et complexes. Leur analyse manuelle devient alors non seulement fastidieuse mais aussi inefficace face à l’ampleur des données.

L’intelligence artificielle, et plus particulièrement l’apprentissage automatique (machine learning), constitue une réponse prometteuse à cette problématique. Elle permettrait d’automatiser la détection d’anomalies au sein des logs, de s’adapter dynamiquement au comportement réel du réseau et de réduire significativement les faux positifs, tout en améliorant la réactivité face aux menaces émergentes.

* **Architecture réseau**