CHAPTER 2: PROBLEM DEFINITION

Traditional firewall systems are inadequate in the face of the growing sophistication and complexity of intrusions. Using rule-based engines, these systems filter network traffic and prevent unauthorized or malicious access to the internal network. Nonetheless, rule-based algorithms have the following limitations:

- They cannot recognize new and emergent threats that do not match any predefined criteria.
- They can generate false positives, which can impede legitimate traffic and cause user dissatisfaction and decreased productivity.
- They can be circumvented by attackers employing encryption, obfuscation, or other evasion techniques.

Therefore, organizations must implement firewalls with a higher level of sophistication that provide enhanced protection against intrusions. These systems should be able to:

- Examine network traffic at a finer level, such as the application layer or the payload layer, to identify malicious behaviour and content.
- Utilize machine learning, artificial intelligence, or other techniques to glean intelligence from network data and adapt to evolving threats.
- Integrate with additional security solutions, such as antivirus, intrusion detection and prevention, or security information and event management (SIEM), to provide a comprehensive defense.