الجمهورية الشعبية الديمقراطية الجزائرية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
المدرسة العليا للإعلام الآلي بسيدي بلعباس
École Supérieure en Informatique
-08 Mai 1945- Sidi Bel Abbès

THESIS

To obtain the diploma of **Engineer**
Field: **Computer Science**
Specialty: **Ingénierie des Systèmes Informatiques (ISI)**

Theme

Modern Firewall System and AI-Driven Intrusion Detection: Implementation and Evaluation

---

Presented by:

Bouaziz Imene

Submission Date: **[Exact Date]**
In front of the jury composed of:

Mr. Khaldi Miloud	President
Ms. Hanae Naoum	Supervisor
Mr. Baraka Younes	Co-Supervisor
Ms. Baba Ahmed Manel	Examiner

Academic Year: 2023/2024

Abstract

This project is proposed by SOCARAM SPA, a company specialized in various technical services and solutions.It starts by an understanding of the company's infrastructure and integrating a new firewall to enhance security. It consists as well of conducting a study on how machine learning can enhance intrusion detection systems by analyzing firewall logs. We focus on logs from the Sophos XG firewall, which offer a comprehensive view of network activity. Our goal is to successfully update the infrastructure and identify patterns and anomalies that signal security threats using various machine learning models.

We start with an overview of firewall technologies, discussing their types, methodologies, and policies. We then detail the features and deployment options of the Sophos XG firewall. Next, we explore key concepts in machine learning and deep learning, emphasizing their relevance to network security.

Through our experiments, we evaluate the performance of different machine learning models in detecting intrusions. We assess these models using metrics such as accuracy, precision, recall, and silhouette score. Our results demonstrate the potential of machine learning to enhance classical firewall systems, making them more effective at identifying and responding to security threats.

Keywords: Cybersecurity, Next-Generation Firewalls (NGFWs), Sophos, Intrusion Detection, Artificial Intelligence (AI), Machine Learning, Deep Learning.