Abstract The objective of this work is to explore the intrusion detection problem and create simple rules for detecting specific intrusions. The intrusions are explored in the realistic CSE-CIC-IDS2018 dataset. First, the dataset is analyzed by computing appropriate statistics and visualizing the data. In the data visualization various dimensionality reduction methods are tested. After analyzing the dataset the data are normalized and prepared for the training. The training process focuses on feature selection and finding the best model for the intrusion detection problem. The feature selection is also used for creating rules. The rules are extracted from an ensemble of Decision Trees. At the end of this work, the rules are compared to the best model. The experiments demonstrate that the simple rules are able to achieve similar results as the best model and can be used in a rule-based intrusion detection system or be deployed as a simple model.