Performance of Network Intrusion Detection and Prevention Systems in High-speed Environments

Abstract

Due to the numerous and increasingly malicious attacks on computer networks and systems, current security tools are often not enough to resolve the issues related to illegal users, reliability, and to provide robust network security. Recent research has indicated that although network security has developed, a major concern about an increase in illegal intrusions is still occurring. Addressing security on every occasion or in every place is a really important and sensitive matter for many users, businesses, governments and enterprises. This paper presents an investigation, involving experiments, which shows that current software security i.e. NIDPSs have several shortcomings such as they are incapable to detect or prevent the rising unwanted traffic and threats to high-speed environments, such as flood attacks (UDP, TCP, ICMP and HTTP). The study shows that how embedded technologies (i.e. software and hardware) improve security performance with no extra cost. The study uses free open source NIDPS software along with a layer 3 switch. It shows that NIDPS performance can be weak in the face of high-speed and high-load malicious traffic in terms of packet drops, and outstanding packets without analysis and failing to detect/prevent unwanted traffic. A novel QoS architecture has designed to increase performance of security i.e. analytical, detection, and prevention when deployed in high-speed networks. It has proposed and evaluated a solution using a novel QoS configuration in a multi-layer switch to organise and improve network traffic performance in order to reduce the packets dropped and then uses parallel techniques to increase packet processing speed. The novel architecture was tested under different traffic speeds, types, and tasks. The experimental results show that the novel architecture improves network and security performance which is can cover up to 8 Gbps with 0 packets dropped.