Intrusion Prevention System (IPS) has two functions which are monitoring network traffic scanning for threats and take suitable automatic actions in case it detects any threat or suspicious traffic (Jeyashankar, 2021). According to (Rao & Nayak, 2014) IPS monitors traffic to detect ant malicious activities then it takes decisions such as dropping the packet, blocking the connection, and resetting the connection to prevent intrusions to protect the network, IPS also sends alarms for the network administrator about the detected intrusion.

In real-time and high-speed networks, monitoring or scanning every packet and all traffic for an accurate classifier will cause a series of bottlenecks by queuing the traffic (Seo & Pak,2021). (IBM, 2020) mentioned that performing deep packet inspection such as Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) cause slow down the network and traffic and with bandwidth limitation, can cause degrade in network performance.

References

IBM. (2021) Identifying and understanding performance bottlenecks with Aspera Transfers. Available from: https://www.ibm.com/support/pages/identifying-and-understanding-performance-bottlenecks-aspera-transfers [Accessed 25 September 2021].

Jeyashankar, A. (2021) IDS vs IPS : Key Differences , Rule Structure , Pros and Cons. *Security Investigation*. Available from: https://www.socinvestigation.com/ids-vs-ips-key-differences-rule-structure-pros-and-cons/ [Accessed 25 September 2021].

Rao, U.H. & Nayak, U. (2021) ‘Intrusion Detection and Prevention Systems‘, In: *The InfoSec Handbook*. Apress, Berkeley, CA. Available from: https://doi.org/10.1007/978-1-4302-6383-8\_11 [Accessed 25 September 2021].

Seo, W. & Pak, W. (2021) Real-Time Network Intrusion Prevention System Based on Hybrid Machine Learning. *IEEE Access*, 9: 46386-46397. Available from: https://ieeexplore.ieee.org/document/9380395 [Accessed 25 September 2021].