Abstract

Firewall (software or hardware device that monitors traffic into and out of the network). It can be classified as stateless or stateful. The existing firewalls are only concerned with filtering packets based on the information contained in the header part of every packet. The most improved stateful inspection firewalls have a state table enabling the storage of header information such as source address, destination address, port, connection status and protocol. Consequently, existing firewalls can be compared to only reading the book tittle and foregoing other essential activities such as evaluating the content of the book. The proposed Deep packet analysis firewall model, not only evaluated the header content of a packet but also open and examines the content in a packet in order to detect and block any threats. In addition, the proposed model will be analyzing the actual content of the traffic that is flowing through packet as opposed to existing firewall which only focuses on analyzing the header content. The model will also locate, detect, categorize, block, or reroute packets having certain data payload and specific codes that are not located, detected, categorized, blocked or redirected by existing firewall. Therefore, deep packet analysis firewall model is a feasible approach to overcome challenges faced in cyberspace today. The proposed Deep packet analysis firewall model will use mixed research method. Quantitative method will include obtaining data from the peer reviewed academic articles in the area of study. Quantitative method will also entail using a simulation by feeding quantitative data into the model to produce quantitative results. Finally, qualitative method will include conducting interviews and use of questionnaires.