Packet-filtering firewalls use a set of rules to decide whether to pass or to drop IP packets which travel, between Internet and a local network at an organization. To identify certain kinds of IP packet filtering, such rules use information about packets, e.g. IP source address, IP destination address and the travelling direction of packets. One rule may mean several ways of filtering. Moreover, the order of the rules has effects on the filtering process.

Therefore, it is often difficult to analyze the correctness of firewall rules. Incorrect firewall rules can create loopholes, which threaten the security of a local network system. In this paper, we aim to develop a model of Firewalls and a methodology to analyze firewall rules using the graph theory. In particular, our methodology can be used to analyze the correctness and the security of firewall rules.