Firewalls offer a protection for private networks against external attacks. However, configuring firewalls is a difficult task. The reason in that the effects of a firewall configuration cannot be easily seen during the configuration time. As a result, errors and loopholes in firewall configurations, if exist are discovered only after they actually happen at the execution time. In this paper, we propose a preliminary yet novel model and its methodology for hardware-based firewalls. Our model offers precise and simple understanding of effects of firewall configurations. Moreover, our methodology offers an analysis of effects of firewall configurations. In particular, it provides reasoning about the correctness of firewall configurations. Also, the redundancy and inconsistency of firewall rules can be reasoned about. As a result, many kinds of errors and loopholes of firewall configurations can be detected during the configuration time.