Abstract

In today’s rapidly progressing professional world, internet is being used as a medium for almost every operation. Firewalls are extensively implemented to prevent unauthorized access to concealed networks and secure them. Based upon the applied policies a firewall can approve or decline the data packet by scrutinizing them. The large size and intricacy of modern networks result in big and complex firewall policies. Optimizing these policies is crucial for network performance inflation. Existing system facilitates inter-firewall or intra-firewall optimization within similar sets of administrative domains. They try to achieve optimization but at the cost of decreased network performance. In this paper, a protocol to increase the network performance while the cross domain firewall rules are optimized is explained. Rule optimization is achieved by redundant rule removal between the two firewalls. For boosting the performance and security, the data sent over the network will be encrypted and decrypted over a session key. Two types of rules i.e. network and user rules are supported. User can configure his own rules as per the required configuration in appropriate domain. Network rules will be common for both the domains and can be updated by the network administrator. The key technical experimentation is that firewall policies cannot be involved within similar domain areas because a firewall strategy contains exhaustive information and even potential security holes.
References


Index Terms

Computer Science

Networks

Keywords

Cross domain firewall optimization; privacy; protocol optimization; redundancy removal.