Abstract

Due to the rapid growth in the field of Internet, the related security mechanisms are the key area of research. Firewalls serve the solution for secured Internet experience. Latest firewalls are fully-equipped for providing hi-end security to the network. However, due to the continuous growth of security threats, the firewall mechanisms and policies are compulsorily needed to get updated. The manual processing for detecting anomalies in firewall is complex and often error-prone. Any minor change in the rule set of firewall leads to the requirement of rigorous analysis for maintaining the consistency and efficiency of firewall mechanism. Many Data structures have been proposed for detection and removal of anomalies so as to reduce the burden of Network Administrator. In this paper I have shown the results of implementation of a mechanism for the anomalies detection in the centralized and distributed firewall systems. This paper also discusses the design implementation of the irrelevance anomaly for the intra
firewalls. It is developed in VB.Net and SQL Server. The algorithm used in this paper purifies the rule sets of firewall in such a way that makes the rule set optimal and free from all known anomalies.

Reference

- Al-Shaer and H. Hamed, “Conflict classification and Analysis of Distributed Firewall policies”, IEEE J SEL AREA COMM, 2005
- Grout V., Davies J. and McGinn J. “An Argument for simple embedded ACL optimization”, Computer Communications, Volume-30 No-2,
- J. Lane Thames, Randal Abler, David Keeling,” A distributed firewall and active response architecture providing preemptive protection”. In ACM Southeast Regional Conference Proceedings of the 46th Annual Southeast Regional Conference on Network and system security, Auburn, Alabama, 2008.

Index Terms

Computer Science

Network Security
Key words

Anomaly Detection

Distributed Firewalls

firewall

mechanisms