Abstract

Firewall secures a private network from intrusions from other networks. The firewall has ACLs (Access Control List) that contain rules used to allow or deny incoming traffic. These rules form the security policy of the firewall. The large size and complexity of modern networks result in large and complex firewall policies. Designing policies for a network of firewalls is a difficult task as a number of cases have to be taken into consideration for access control. Also, a network administrator may want to update the policies in order to replace them with new ones. The process of updating firewall policies is difficult and error prone. In this paper, we provide a structured and comprehensive overview of various techniques in regards to firewall anomaly
Firewall Anomaly Management: A survey
detection. We briefly describe and compare various known algorithms and tools used to detect
and/or resolve the firewall anomalies.

References

- Sandeep Reddy Pedditi, Du Zhang, and Chung-E Wang, "FIEP: An Initial Design of
  a Firewall Information Exchange Protocol," IEEE 14th International Conference on
  Information Reuse and Integration (IRI), 2013.
- E. Al-Shaer and H. Hamed, "Discovery of Policy Anomalies in Distributed
  Security and Privacy, 2006
- Y. Bartal, A. J. Mayer, K. Nissim, A. Wool, "Firmato: A novel firewall
- Suchart Khummanee, Atipong Khumseela and Somnuk Puangprontitag, "Towards
  a New Design of Firewall: Anomaly Elimination and Fast Verifying of Firewall Rules,
  10th International Joint Conference on Computer Science and Software Engineering (JCSSE),
  2013, pp. 93-98
- Chi-Shih Chao, "A flexible and feasible anomaly diagnosis system for Internet
  (APNOMS), 2011
- A. X. Liu and M. G. Gouda, "Firewall policy queries," IEEE Transactions on
  Parallel and Distributed Systems (TPDS), 20(6), pp. 766-777, 2009
- Hongxin Hu, Gail-Joon Ahn and Ketan Kulkarni, "Detecting and Resolving Firewall
  Policy Anomalies," IEEE Transactions on Dependable and Secure Computing, vol. 9,
  issue 3, pp. 318-331
- Alan Jeffrey and Taghrid Samak, "Model Checking Firewall Policy
  Configurations," IEEE International Symposium on Policies for Distributed Systems and
  Networks, 2009, pp. 60-67
- A. Mayer, A. Wool and E. Ziskind, "Offline firewall analysis," International
- Alex X. Liu, "Firewall policy verification and troubleshooting," The
  pp. 2800-2809
  updated March 31, 2014
- A. X. Liu, "Formal Verification of Firewall Policies," IEEE International
- S. R. Pedditi, "An initial design of firewall information exchange protocol
  (FIEP)," MS Degree Project Report, Department of Computer Science, California State
  University, Sacramento, May 2012.
- Juniper Netscreen Series Security Systems, Juniper Networks Inc., Dec 2011
- Check Point Threat Prevention Appliances, Check Point Software Technologies, Ltd., 2012.

Index Terms

Computer Science
Security

Keywords
firewalls ACL rules anomaly Firewall Policy Policy conflicts