Novel Design and Implementation of Cross-Domain Privacy-Preserving Firewall Optimization

D.Uma[#1], Dr.G.Venkata Rami Reddy[*2], K.shirisha[#3]

[#1]*M.Tech Computer Science Student School of I.T.JNTU Hyderabad India*

[*2]*Associate Professor of CSE School of I.T.JNTU Hyderabad India*

[#3]*Assistant Professor CSE MGIT Hyderabad India*

***Abstract*— Firewalls are very important in Internet for providing security and privacy. Firewalls checks each incoming and outgoing packets based on its rules set in their policies. As per the vast requirement of services on internet the rule set in firewall policies becomes large, so the increasing number of rules in a firewall policy reduces its throughput. So, optimizing the firewalls is very important for improving the throughput as well as network performance. In this paper we propose a novel privacy preserving protocol that removes the redundant rules present in two adjacent firewalls that belong to two different administrative domains, and reorder those rules, in a privacy preserving way. We implemented our protocol and conducted experiments. As the result our protocol effectively removed the redundant rules and enormously improved the network performance.**

***Keywords*— Cooperative Firewall, Privacy Preservation, Cross domain, Firewall optimization**

I. INTRODUCTION

Firewall is a software or hardware that is designed to prevent unauthorised access to or from a private network. Firewalls control incoming and outgoing network data packets, based on its policy rules set. Firewall is very essential for any networked computer. A firewall can help in preventing the hackers or malicious software from gaining the access from an authorised computer through a network or Internet.

Firewall policy management is a challenging task due to the complexity and interdependency of policy rules. This is further exacerbated by the continuous evolution of network and system environments. The key technical challenge is that the firewall policies cannot be shared across domains, because a firewall policy contains confidential information. Existing policy analysis tools, such as Firewall Policy Advisor and FIREMAN, with the goal of detecting policy anomalies have been introduced. However, Firewall Policy Advisor only has the capability of detecting pair wise anomalies in firewall rules and the Fireman also has limitations in detecting anomalies. For each firewall rule, FIREMAN only examines all preceding rules but ignores all subsequent rules. So, the process of configuring a firewall is monotonous. Therefore effective mechanism and tools for policy management are crucial to the success of firewalls.

Prior Work on Firewall optimization focuses on either intra firewall or inter firewall optimization within one administrative domain only, where the privacy of the firewall is not a concern. But, in this we proposed cross-domain privacy preserving cooperative firewall optimization.

Disadvantages of the existing system are the number of rules in a firewall significantly affects its throughput. Fireman can detect anomalies among multiple rules by analyzing the relationships between one rule and the collections of packet spaces derived from all preceding rules but ignore all subsequent rules when performing anomaly analysis.

The main objective of this paper is to provide an innovative policy anomaly management framework for firewalls, adopting a rule based segmentation technique to identify policy anomalies and derive effective anomaly resolutions. Based on this technique, a network packet space defined by a firewall policy can be divided into a set of disjoint packet space segments. Each segment associated with a unique set of firewall rules accurately indicates an overlap relation (either conflicting or redundant) among those rules.

Advantages of the proposed system are first the conflicting segments are identified in this framework. Each conflicting segment associates with a policy conflict and a set of conflicting rules. Also, the correlation relationships among conflicting segments are identified and conflict correlation groups are derived. Policy conflicts belonging to different conflict correlation groups can be resolved separately, thus the searching space

for resolving conflicts is reduced by the correlation process.

II. Literature Survey

An Approach for Firewall Optimization in Cross-Domain by Cooperative and Secrecy-Preserving Manner AUTHORS : Yogita Nikhare, Prof. Anil Bende: Firewalls are commonly deployed on the Internet for securing private networks. A firewall checks each incoming or outgoing packet to choose whether to accept or reject the packet based on its policy. Optimizing firewall policies is necessary for improving network performance. The optimization process involves cooperative computation between the two firewalls with no any party disclosing its strategy to the other. In this paper they explained cross-domain privacy-preserving cooperative firewall strategy optimization protocol. For any two adjoining firewalls belonging to two dissimilar administrative domains, this protocol can recognize in each firewall the rules that can be removed because of the other firewall.

Discovery of Policy Anomalies in Distributed Firewalls. AUTHORS: E. Al-Shaer and H. Hamed: In this the authors presented a set of techniques and algorithms to automatically discover policy anomalies in centralized and distributed legacy firewalls and the authors aims at the removal of redundant rules in firewalls belonging to single administrative domain, where as the privacy of the firewall policies is not an issue.

Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese AUTHORS: A. Wool: The first quantitative evaluation of the quality of corporate firewall configurations appeared in 2004, based on Check Point Firewall-1 rule sets. In general, that survey indicated that corporate firewalls often enforced poorly written rule sets. This article revisits the first survey. In addition to being larger, the current study includes configurations from two major vendors. It also introduces a firewall complexity. The study's findings validate the 2004 study's main observations: firewalls are (still) poorly configured, and a rule -set's complexity is (still) positively correlated with the number of detected configuration errors.

Complete Analysis of Configuration Rules to Guarantee Reliable Network Security Policies AUTHORS: J. Alfaro, N. Boulahia-Cuppens, and F. Cuppens: In this paper, the authors presented a set of Mechanisms for the managing of anomalies on distributed network security policies. They had given a set of algorithms for the management of anomalies within the configuration of single security components and also a set of algorithms for the management of anomalies between the configuration of different security components implementing a single, but distributed, security policy.

Fast and Scalable Conflict Detection for Packet Classifiers AUTHORS: F. Baboescu and G. Varghese: They described an efficient and scalable conflict detection algorithm for the general case that is significantly faster. In this paper the authors addressed two important new problems: fast packet filter conflict detection and fast rule updates and the results show an order of improvement over the naive algorithm as well as simplistic extensions.

Fireman: A Toolkit for Firewall Modeling and Analysis AUTHORS: L. Yuan, H. Chen, J. Mai, C. Chuah, Z. Su, P. Mohapatra, and C. Davis: In this paper the authors presented a novel static analysis toolkit called FIREMAN, for firewall modeling and analysis and this FIREMAN applies static analysis techniques to check misconfigurations, such as policy violations, inconsistencies, and inefficiencies, in individual firewalls as well as among distributed firewalls. Their technique is based on the symbolic model checking using binary decision diagrams to compactly represent and efficiently process firewall rules.

Firewall Compressor: An algorithm for minimizing firewall policies AUTHORS Alex X. Liu, Eric Torng and Chad R. Meiners: The authors proposed firewall compressor which gives us a framework for compressing firewall rules. They had given an optimal algorithm for compressing one-dimensional firewalls and systematic solution for multi-dimensional firewalls.

Complete redundancy removal for packet classifiers in TCAMS AUTHORS: Alex X. Liu, M. G. Gouda: The authors had given a necessary and sufficient condition for identifying all redundant rules in a classifier and they presented two algorithms for detecting and removing the two types of redundant rules and they provided that the resulting classifiers have no redundant rules after running the two algorithms.

Many other firewall optimization techniques are proposed by researchers in different areas.

III. Design and Implementation

The figure 1 shows the system architecture.

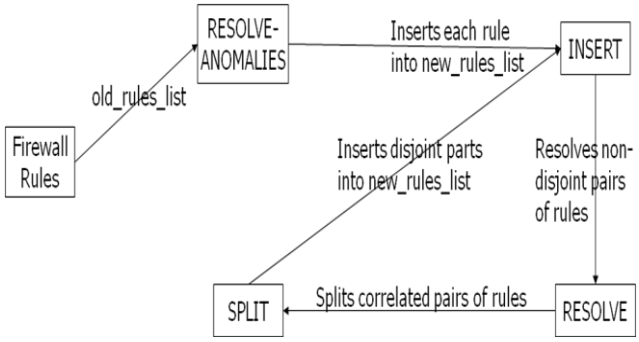

Fig. 1 System Architecture

In this the network packet space defined by the firewall policy can be divided into a set of disjoint packet space segments and each segment associated with a unique set of firewall rules and then generated correlation groups of conflicting segments for the anomaly analysis. The major benefit of generating correlation groups is that anomalies can be examined within each group independently, because all correlation groups are independent of each other. Especially, the searching space for reordering conflicting rules in conflict resolution can be significantly lessened and the efficiency of resolving conflicts can be greatly improved. After generating the correlation groups, risk assessment for the conflicts is performed. The risk level of conflicts are in turn utilized for both automated and manual strategy selections. Then to resolve the conflicts, the rules in the firewalls will be reordered. The order in which the conflicting rules are satisfies all action constraints, that must be the optimal solution for the conflict resolution. When the conflicts in a policy are resolved, the risk value of the resolved policy should be reduced and the availability of protected network should be improved comparing with the situation prior to conflict resolution based on the threshold value data will be received in to the server.

In this, we proposed four modules. The step-by-step procedure is as follows:

1. In the first module, the admin provides the username, password and the user need to register a node in the channel to the server. All user information will be stored in Database.
2. When user enters the username and password then Admin provide a separate session to that particular Node. Here the node inserts various types of files and makes a package, then it converts to XML file and performs encryption on the package for securing the data and sends the package to the rule engine to optimize the firewall policies.
3. The rule engine receives all the data from the various nodes and makes list of all the rules in the particular firewalls through which the data is being sent.
4. Finally the rule engine will perform various operations like shadowing, redundancy and filters the rules thus optimizes the firewalls.

The figure 2 shows the execution screen shot of application for firewall optimization.

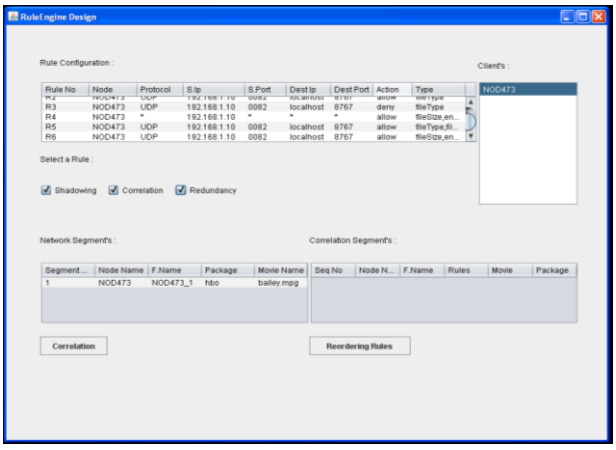

Fig. 2 Execution screen shot of firewall optimization

Figure 3 shows the comparable results of the methodology employed over existing methodology.

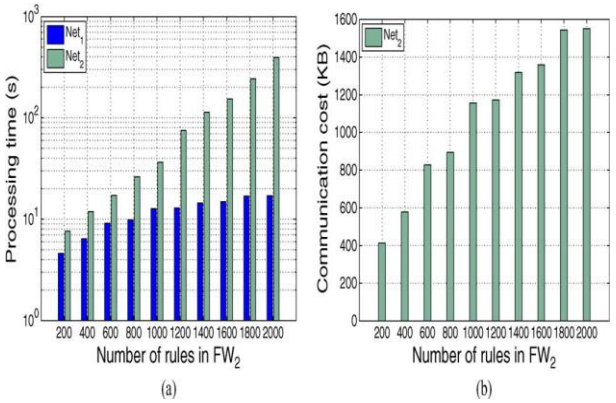

Fig. 3 Comparison of results

IV. CONCLUSIONS

In this, we proposed a novel privacy-preserving protocol for detecting anomalies and redundancies. We implemented our protocol and conducted extensive evaluation. From the results the communication cost is less than a few hundred kilobytes. Our protocol incurs no extra online packet processing overhead. To measure the efficiency, we first processed each synthetic firewall and then measured the processing time and communication cost of two parties and also we measured the comparison time for every two firewalls, where as our protocol effectively removed the redundant rules and significantly improved network performance.

REFERENCES

[1] nf-HiPAC, "Firewall throughput test," 2012 [Online]. Available: http://www.hipac.org/performance_tests/results.html

[2] R. Agrawal, A. Evfimievski, and R. Srikant, "Information sharing across private databases," in Proc. ACM SIGMOD, 2003, pp. 86–97.

[3] E. Al-Shaer and H. Hamed, "Discovery of policy anomalies in distributed firewalls," in Proc. IEEE INFOCOM, 2004, pp. 2605–2616.

[4] J. Brickell and V. Shmatikov, "Privacy-preserving graph algorithms in the semi-honest model," in Proc. ASIACRYPT, 2010, pp. 236–252.

[5] Y.-K. Chang, "Fast binary and multiway prefix searches for packet forwarding," Comput. Netw., vol. 51, no. 3, pp. 588–605, 2007.

[6] J. Cheng, H. Yang, S. H.Wong, and S. Lu, "Design and implementation of cross-domain cooperative firewall," in Proc. IEEE ICNP, 2007, pp. 284–293.

[7] Q. Dong, S. Banerjee, J. Wang, D. Agrawal, and A. Shukla, "Packet classifiers in ternary CAMs can be smaller," in Proc. ACM SIGMETRICS, 2006, pp. 311–322.

[8] O. Goldreich, "Secure multi-party computations," Working draft, Ver. 1.4, 2002.

[9] O. Goldreich, Foundations of Cryptography: Volume II (Basic Applications). Cambridge, U.K.: Cambridge Univ. Press, 2004.

[10] M. G. Gouda and A. X. Liu, "Firewall design: Consistency, completeness and compactness," in Proc. IEEE ICDCS, 2004, pp. 320–327.

[11] M. G. Gouda and A. X. Liu, "Structured firewall design," Comput. Netw., vol. 51, no. 4, pp. 1106–1120, 2007.

[12] P. Gupta, "Algorithms for routing lookups and packet classification," Ph.D. dissertation, Stanford Univ., Stanford, CA, 2000.

[13] A. X. Liu and F. Chen, "Collaborative enforcement of firewall policies in virtual private networks," in Proc. ACM PODC, 2008, pp. 95–104.

[14] A. X. Liu and M. G. Gouda, "Diverse firewall design," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 8, pp. 1237–1251, Sep. 2008.

[15] A. X. Liu and M. G. Gouda, "Complete redundancy removal for packet classifiers in TCAMs," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 4, pp. 424–437, Apr. 2010.

[16] A. X. Liu, C. R. Meiners, and E. Torng, "TCAM Razor: A systematic approach towards minimizing packet classifiers in TCAMs," IEEE/ACM Trans. Netw., vol. 18, no. 2, pp. 490–500, Apr. 2010.

[17] A. X. Liu, C. R. Meiners, and Y. Zhou, "All-match based complete redundancy removal for packet classifiers in TCAMs," in Proc. IEEE INFOCOM, 2008, pp. 574–582.

[18] A. X. Liu, E. Torng, and C. Meiners, "Firewall compressor: An algorithm for minimizing firewall policies," in Proc. IEEE INFOCOM, 2008.

[19] C. R. Meiners, A. X. Liu, and E. Torng, "TCAM Razor: A systematic approach towards minimizing packet classifiers in TCAMs," in Proc. IEEE ICNP, 2007, pp. 266–275.

[20] C. R. Meiners, A. X. Liu, and E. Torng, "Bit weaving: A non-prefix approach to compressing packet classifiers in TCAMs," in Proc. IEEE ICNP, 2009, pp. 93–102.

[21] C. R. Meiners, A. X. Liu, and E. Torng, "Topological transformation approaches to optimizing TCAM-based packet processing systems," in Proc. ACM SIGMETRICS, 2009, pp. 73–84.

[22] S. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," IEEE Trans. Inf. Theory, vol. IT-24, no. 1, pp. 106–110, Jan. 1978.

[23] D. K. H. D. R. Safford and D. L. Schales, "Secure RPC authentication (SRA) for TELNET and FTP," Tech. Rep., 1993.

[24] S. Singh, F. Baboescu, G. Varghese, and J.Wang, "Packet classification using multidimensional cutting," in Proc. ACM SIGCOMM, 2003, pp. 213–224.

[25] A. Wool, "A quantitative study of firewall configuration errors," Computer, vol. 37, no. 6, pp. 62–67, Jun. 2004.

[26] Z.Yang, S. Zhong, and R.N.Wright, "Privacy-preserving classification of customer data without loss of accuracy," in Proc. SIAM SDM, 2005, pp. 21–23.

[27] W. Lee and D. Xiang, "Information-theoretic measures for anomaly detection," in Proc. IEEE S&P, 2001, pp. 130–143.

[28] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, and S. Zhou, "Specification-based anomaly detection: A new approach for detecting network intrusions," in Proc. ACM CCS, 2002, pp. 265–274.

[29] C. Kruegel, T. Toth, and E. Kirda, "Service specific anomaly detection for network intrusion detection," in Proc. ACM SAC, 2002, pp. 201–208.

[30] L. Yuan, H. Chen, J. Mai, C.-N. Chuah, Z. Su, and P. Mohapatra, "Fireman: A toolkit for firewall modeling and analysis," in Proc. IEEE S&P, 2006, pp. 199–213.

[31] Avishai Wool, "Trends in Firewall Configuration errors - Measuring the Holes in Swiss Cheese" in Internet Computing, IEEE, vol 14, pp. 58-65.

[32] J. Alfaro, N. Boulahia-Cuppens and F. Cuppens "Complete Analysis of Configuration Rules to Guarantee Reliable Network Security policies" in Sprinjer, 2007

[33] F. Baboescu and G. Varghese "Fast and Scalable conflict detection for packet classifiers" in Elsevier Computer Networks, 2003.