ISSN 2320-9984
Volume 3 Issue 1 | March 2015 ISSN: 2320-9984 (Online)
International Journal of Modern Engineering & Management Research
Website: www.ijmemr.org

An Approach for Firewall Optimization in Cross-Domain by Cooperative and Secrecy-Preserving Manner

Neha Asati
M.Tech. Research Scholar
Department of Computer Science & Engineering
Lakshmi Narain College of Technology
Jabalpur (M.P.), [INDIA]
Email: 31asatineha@gmail.com

Sujeet Tiwari
Assistant Professor
Department of Computer Science & Engineering
Lakshmi Narain College of Technology
Jabalpur (M.P.), [INDIA]
Email: sujeet.tiwari08@gmail.com

Raghvendra Kumar Agrawal
Assistant Professor
Department of Computer Science & Engineering
Lakshmi Narain College of Technology
Jabalpur (M.P.), [INDIA]
Email: raghvendraagrawal7@gmail.com

***Abstract*—*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 we are going to explain first cross-domain privacy-preserving cooperative firewall strategy optimization protocol. For any two adjoining firewalls belonging to two dissimilar administrative domains, our protocol can recognize in each firewall the rules that can be removed because of the other firewall.*

***Keywords*:—** *Cross- Domain, Interfirewall Optimization*

1. INTRODUCTION

A firewall is defined as any device used to filter or direct the flow of traffic. Firewalls are typically implemented on the network outer limits and function by defining trusted and untrusted region. Most firewalls will allow traffic from the trusted zone to the untrusted zone, with no any explicit configuration. However, traffic from the untrusted zone to the trusted zone must be clearly permitted. Thus, any traffic that is not explicitly permitted from the untrusted to trusted zone will be absolutely denied (by default on most firewall systems). The vital function of a firewall is to keep unwanted guests from browsing your network [1]. A firewall can be a hardware device or a software application and usually is placed at the boundary of the network to act as the gatekeeper for all incoming and outgoing traffic. There are essentially four mechanisms used by firewalls to limit traffic. One device or application may use more than one of these in combination with each other to give more in-depth protection. The four mechanisms are packet filtering, circuit-level gateway, and proxy server and application gateway. Packet Filtering is one of the core services provided by firewalls. Packets can be filtered (permitted or denied) based on a wide range of criteria:

- Source address
- Destination address

- Protocol Type (IP, TCP, UDP, ICMP, ESP, etc.)
- Destination Port
- Source Port

Packet filtering is implemented as a rule-list. The order of the rule-list is a significant consideration. The rule-list is at all times parsed from top-to-bottom [2]. Each physical interface of a router/firewall is configured with two ACLs: one for filtering outgoing packets and the other one for filtering incoming packets. The number of rules in a firewall considerably affects its throughput. As the number of rules increases firewall performance decreases [3].

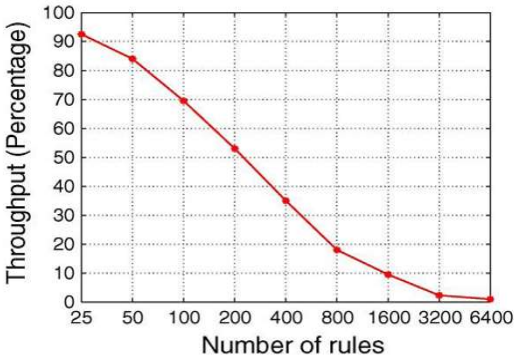

Figure 1: Effect of the number of rules on the throughput

Cross-Domain Interfirewall Optimization

No earlier work focuses on cross-domain privacy preserving interfirewall optimization. We focus on removing interfirewall policy redundancies in a privacy-preserving way. Consider two adjacent firewalls 1 and 2 belonging to dissimilar administrative domains Net1 and Net2. Let F1 indicate the policy on firewall 1's outgoing interface to firewall 2 and F2 indicate the policy on firewall 2's incoming interface from firewall 1. For a rule r in F2, if all the packets that match r but do not match any rule over r in F2 are discarded by F1, rule r can be removed because such packets never come to F2. We call rule r an interfirewall redundant rule with respect to F1 [3, 5]. Fig. 2 illustrates interfirewall redundancy, where two adjoining routers belong to dissimilar administrative domains CSE and EE.

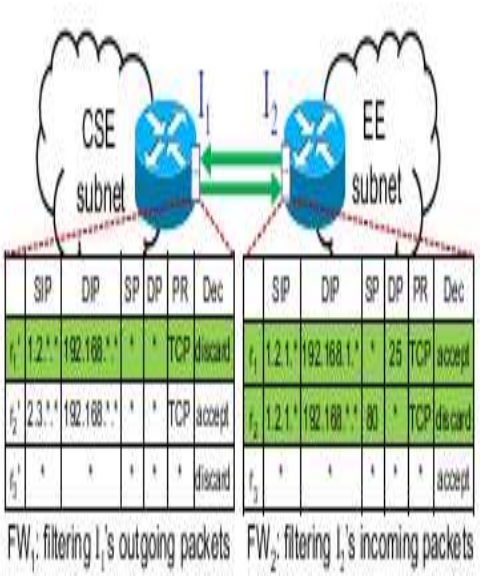

Figure 2: Example interfirewall redundant rules.

2. RELATED WORK

Prior work on firewall optimization did not consider minimizing and maintaining the privacy of firewall policies. Firewall policy management is a difficult chore due to the complexity and interdependency of policy rules. This is further studied by the continuous evolution of network and system environments [8, 10]. The process of configuring a firewall is tedious and error prone. Therefore, efficient mechanisms and tools for policy management are vital to the success of firewalls.

Limitation of Prior Work

Prior work focuses on intrafirewall optimization or interfirewall optimization within one administrative domain, where privacy of firewall policies is not considered. In intrafirewall it contains only the single firewall, where optimization is done and in interfirewall it includes two firewalls but they are in one network and optimization is done without any privacy preserving. But no prior work focuses on interfirewall optimization between more than one administrative domains and major concern is that firewall policies are not known to each other so that privacy is preserved. Also in the previous work numbers of rules in the firewall are not the concern. The number of rules in a firewall significantly affects its throughput.

3. PROPOSED PLAN

In this paper, we have proposed four modules:

Module 1: Login : Window for authentication for administrator.

Module 2:Setting of rules of firewall and redundancy removal in the intrafirewall.

Module 3: Redundancy removal using Pohlig-Hellman commutative encryption algorithm in interfirewall**.**

Module 4:Analysis and Testing. The configuration for proposed system is shown in the figure.

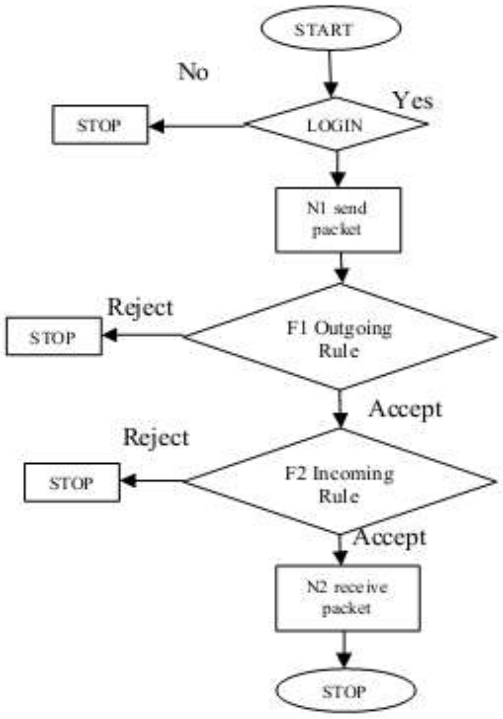

Fig. 3 Data Flow chart of two administrative domains

Terminologies used in the above figure are:

- N1- Network 1(Administrative domain 1)
- N2- Network 2(Administrative domain 2)
- F1- Firewall 1
- F2- Firewall 2

1. In the first module, we have created GUI for authentication of administrator. Also we have created firewall model in which we have made application and added the different parameters for the rules of the firewall i.e. Incoming and outgoing rules.

2. Then we will set the incoming and outgoing rules of firewalls using parameters like source IP, destination IP, source port, destination port, protocol type and action. And then we will remove intrafirewall redundant rules i.e. overlapping rules in individual firewall.

3. In the third module, we will use Pohlig-Hellman Commutative encryption algorithm to remove redundant rules in interfirewall i.e. the rules of firewall 2 with respect to firewall 1. The algorithm works as follows:

   - In Firewall policy, packet may match many rules having dissimilar decisions.
   - To resolve these conflicts, firewalls employ first match semantics where the decision of the packet is the decision of the first rule that packet matches.
   - Input: Sets of rules Output: Few rules which are redundant with respect to FW1

4. In the analysis part we have done the evaluation of proposed system and our approach i.e. the algorithm which we have proposed in this paper which is different than the existing system as it requires minimum processing time than the existing system as the number of rules decreases. We have tested this result on the two synthetic

firewalls i.e. firewall1 of one administrative domain and firewall2 of second administrative domain.

3. IMPLEMENTATION DETAILS

The project is different from the existing system in such a way that, in existing system the algorithm used for removing the rules consists of four steps i.e. prefix conversion, prefix family construction, prefix numericalization and comparison. So, it requires more time to remove rules. So for reducing this processing time we proposed the same algorithm and make changes in that algorithm in such a way that without using the above four steps the privacy is preserved and no firewall can access the rules of other firewall. In this algorithm, we use private keys for encryption in each administrative domains and works like diffiehellman key exchange algorithm. The snapshots of the implementation of the algorithm are as follows:

Figure 4: Outgoing rules of firewall1

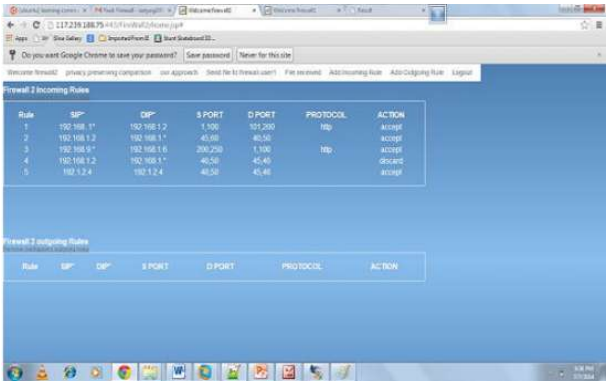

Figure 5: Incoming rules of firewall2

Figure 6: Intrafirewall redundant rule is removed in firewall1 Fi

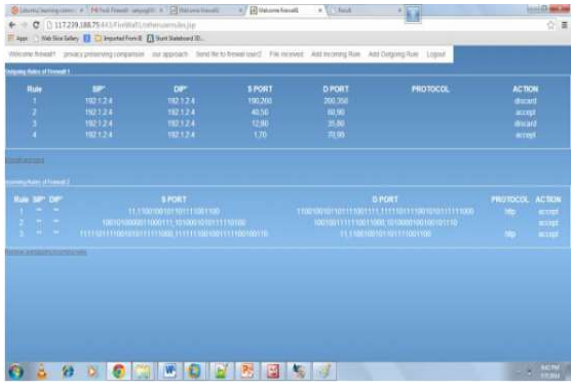

Figure 7: Final output showing removal of redundant rules using PHA algorithm

4. ANALYSIS OF SYSTEM

Now, the analysis is done by showing the graphs, two graphs are shown which shows the processing time of algorithm. In the first evaluation as the number of rules more the processing time is also more in both proposed and our approach. But as the number of rules are minimized the processing time is also minimized in both the cases. And our approach requires less processing time as number of rules are removed without disclosing policies to each other, hence this is the best approach for maintaining privacy as well as removing the redundant rules. The graphs are as follows:

Figure 8: Evaluation 1 when number rules are more

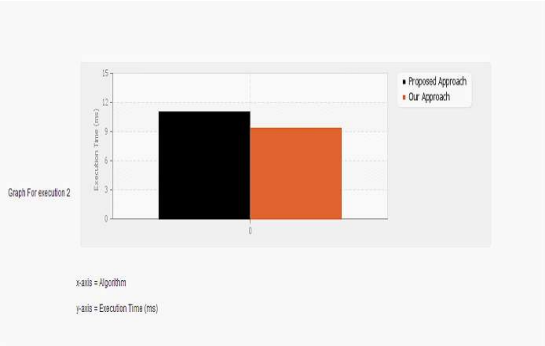

Figure 9: Evaluation 2 when number of rules are less

5. CONCLUSION

Hence by using cross-domain cooperative privacy preserving protocol we have identified and remove the redundant rules in firewall 1 with respect to firewall 2 without disclosing policies to each other. But again we have identified and remove the redundant rules in the same way in firewall 2 with respect to firewall 1. As redundant rules are removed the network performance is improved. The response time is also improved and the communication cost and processing time is reduced.

REFERENCES:

[1] Fei Chen, Bezawada Bruhadeshwar, and Alex X. Liu, "Cross-Domain Privacy - Preserving Cooperative Firewall Optimization", IEEE/ACM Transactions on Networking, Vol. 21, No. 3, June 2013.

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

[3] 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.

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

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

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.