ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Redundancy Removing Protocol to Minimize the Firewall Policies in Cross Domain

Kamarasa V D S Santhosh
M.Tech Student,
Department of ComputerScience & Engineering,
School of Technology,
Gitam University, Hyderabad.

G Sri Sowmya, M.Tech
Assistant professor,
Department of Computer Science & Engineering,
School of Technology,
Gitam University, Hyderabad.

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.

I. 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.)
Source Port
Destination 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].

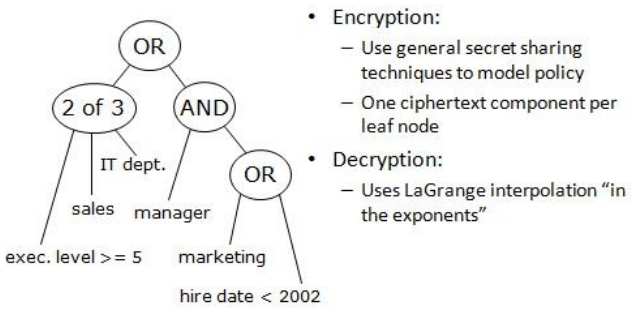

Fig. 1 Effect of the number of rules on the throughput

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

II. 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.

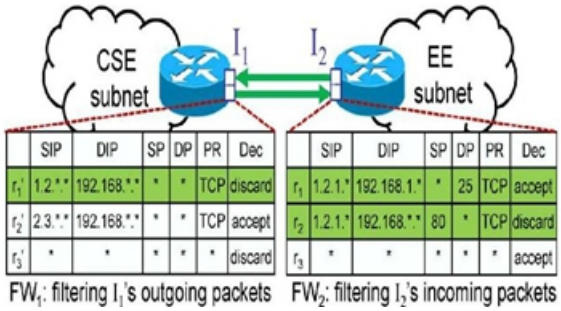

Fig. 2 Example interfirewall redundant rules.

III. 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.

A. 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.

IV. PROPOSED SYSTEM:

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 3.

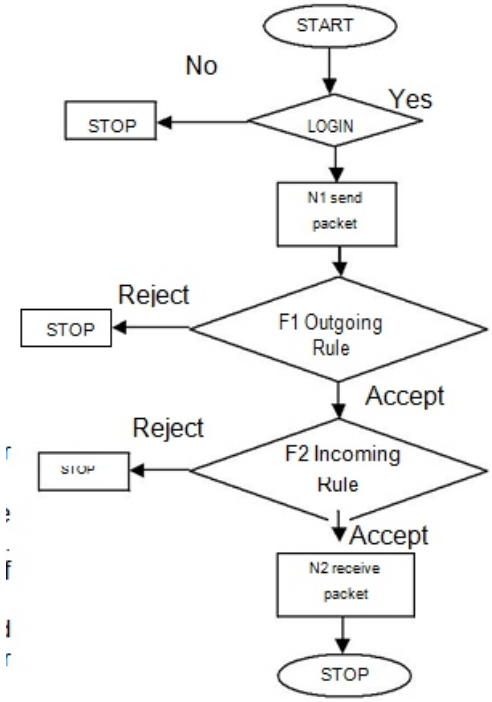

Fig. 3 Data Flow chart of two administrative domains

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

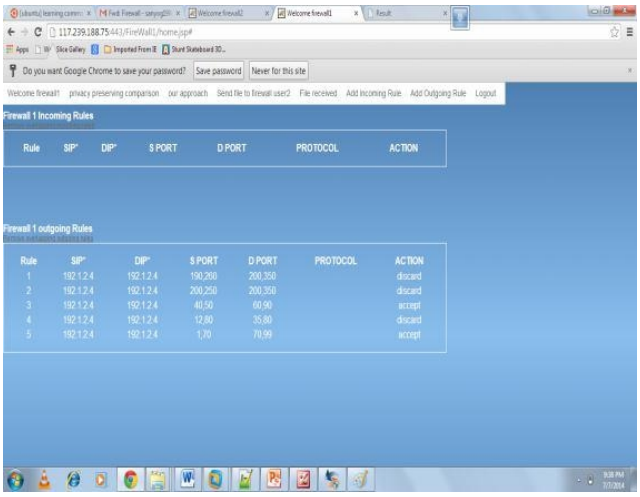

Fig. 4 Outgoing rules of firewall1

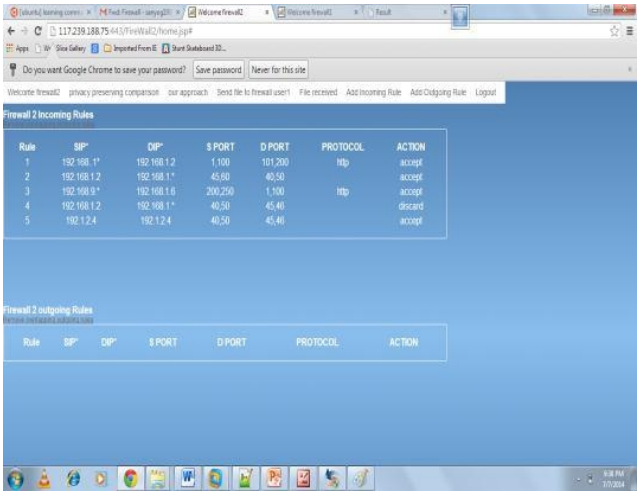

Fig. 5 Incoming rules of firewall2

Fig. 6 Intrafirewall redundant rule is removed in firewall1

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

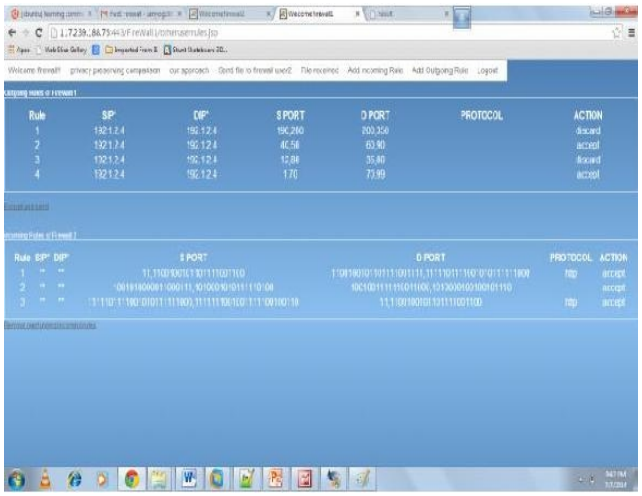

Fig. 7: Final output showing removal of redundant rules using PHA algorithm

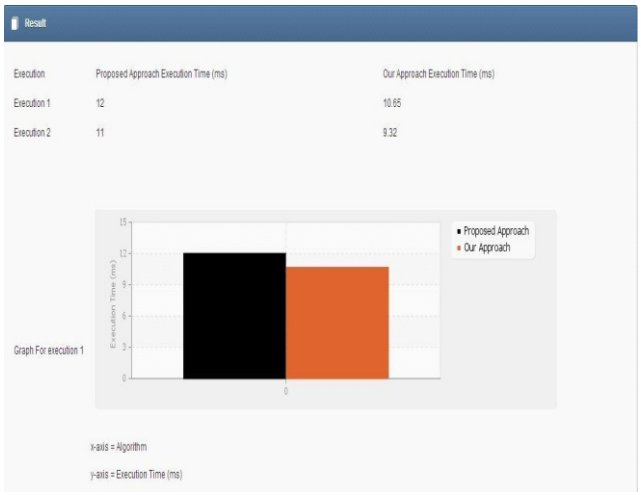

Fig. 8 Evaluation 1 when number rules are more.

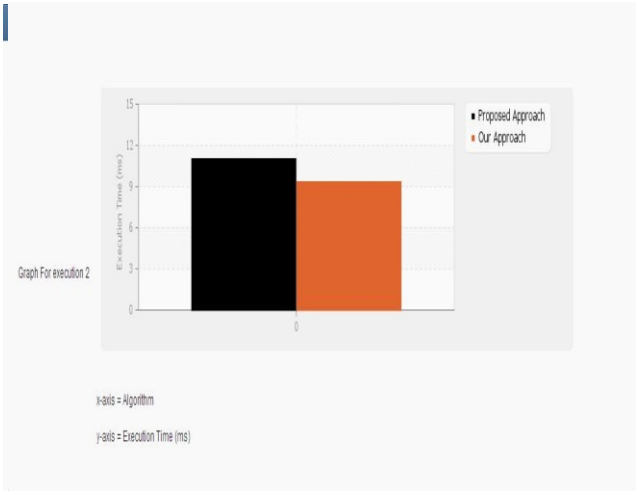

Fig. 9 Evaluation 2 when number of rules are less

II. LITERETURE SURVEY:

A. FIREWALL REDUNDANCY REMOVAL:

Preceding work on intrafirewall severance removal aims to sense redundant rules within aonly firewall Gupta recognized backward and onward redundant instructions in a firewall [12]. Later, Liu etal. pointed out that the fired. rules identified by Gupta are imperfect and planned twoapproaches for detecting all jobless rules Prior work on interfirewall joblessness removal requires the information of two firewall strategies and therefore is only appropriate within one directorial domain.

B.COLLABORATIVE FIREWALLENFORCEMENT IN VIRTUAL PRIVATE NETWORKS (VPNS):

Given research work on collaborative firewall implementation in VPNs imposes firewall policies finishedencoded VPN tunnels deprived of leaking the confidentiality of the remote network's rule [6], 13]. The difficulties of collaborative firewall execution in VPNs and confidentialitypreserving entombfirewall optimization are fundamentally dissimilar.

First, their resolves are different. The previous focuses on imposing a firewall policy over VPN tunnels in a confidentialitypreserving method, whereas the latter emphases on removing interfirewall dismissed rules without unveiling their guidelines to each further. Second, their necessities are different. The former conserves the privacy of the isolated network's procedure, whereas the latter conserves the privacy of both strategies.

C.PRIVACY-PRESERVINGINTERFIREWALL REDUNDACYREMOVAL:

wecontemporary our privacy-preserving protocol for perceivingentombfirewall terminated rules in FW1 with deference to FW2 To do this,we first adapt each firewall to an correspondingorder of nonoverlappingrubrics. We first convert every firewall to ancorrespondingarrangement of nonoverlapping rules.Lastly, afterterminated nonoverlapping rules produced from fw2 are recognized we map them back to innovative rules in fw2 and then classify theterminated ones.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A.PRIVACY-PRESERVING RANGE COMPARISON:

To crisscross whether a number after is in a variety from FW2, we use a technique similar to FW1 the precede membership corroborationsystem in [13]. The basic idea is to renovate the delinquent of examination whether to the problem of inspection whether two arrangements converted from and require a common component.

III. RELATED WORK:

Given work base on firewall optimization did not reflect minimizing and preserving the isolation of firewall strategies. Firewall strategy management is a challenging chore due to the difficulty and interdependency of strategy rules. This is supplementary studied by the unceasing evolution of network and classification environments [8, 10].The progression of constructing a firewall is tedious and miscalculation prone. Therefore, effectual mechanisms and tools for strategy management are energetic to the achievement of firewalls.

VII.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, BezawadaBruhadeshwar, 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," Comput.Netw., 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