"Commutative Encryption for Privacy preserving in firewall Optimization"

Miss. Priyanka M. Padole
Department of Master of Computer Application, S.R.P.C.E.,Nagpur,Maharashtra,India.
spadole2011@gmail.com

***Abstract* –** The world of internet contains many private networks, and preserving security and privacy of these networks has become a crucial task. Firewall plays a very important role while protecting the internal private network from the outside non-secure network. Firewall stands as a barrier between internal and external networks, checking every incoming and outgoing data traffic against a set of rules or policies. Optimization of firewall policy is required for improving the throughput of the network. In our proposed work, we carry out the interfirewall optimization and provide privacy in two different administrative domains. We propose a privacy-preserving protocol for detecting redundancy in firewall rules of two different domains, without compromising each other's policies. We implemented our work and provided a protocol better than the previous ones.

***Index Terms* –** Privacy, Firewall optimization, Security, Redundancy.

*****

I. INTRODUCTION

In this world of internet, firewall has become a necessity in various organizations, institutions, personal networks, etc. Firewall protects the internal network from any other outside network that poses threat to the internal network. Firewall stands as a barrier between two networks. It secures the internal network by checking every incoming and outgoing network traffic against a set of predefined rules. The performance of a firewall may depend on the rule management[1].

Every incoming and outgoing packet is examined and accepted or declined whether to enter the private network depending upon the policies of the firewall as shown in figure 1.

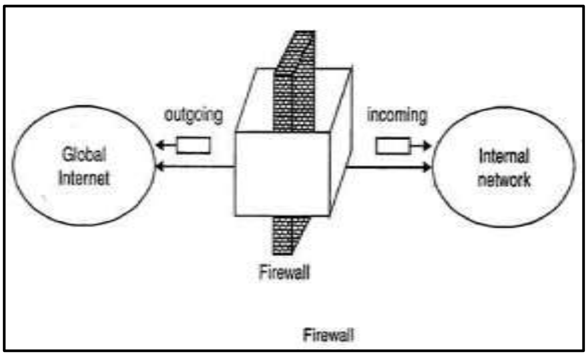


Figure 1: Overview of a firewall

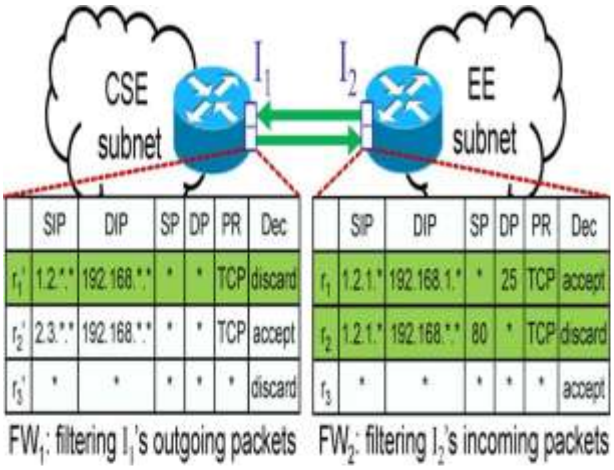
A firewall policy is nothing but a chain of rules and depending on these policies, firewall performs its tasks. The set of rules is called as Access Control List (ACL). Each rule in ACL has a packet header field and a resolution of either accepting or declining the packet. When, packets enter into the system, they are checked according to first-matching rule in the policies. There are two ACLs for checking incoming and outgoing packets respectively. Sometimes the throughput of the network depends upon the number of rules included in the firewall. Due to the growing need for security, the firewall policies are increasing in size. Therefore, optimization of the policies is required to enhance the performance of the network.

Previously, the work on optimizing policies was done on either interfirewall or intrafirewall in a single domain. In such cases, maintaining the privacy of the firewall rules was not of priority. In intrafirewall optimization, the optimization was limited to a single firewall and was done by removing repeated rules or policies. It is a very challenging task to maintain privacy along with optimizing the firewall rules and policies of two different domains.

In this paper we have addressed the issue of privacy preserving with optimization of firewall policies. This paper is organized as follows: In the second section we have surveyed some existing systems proposed for preserving privacy and policy optimization techniques. We have proposed our protocol and described it in the third section with description of the algorithms used. We have also given a graph comparing our system with the previous systems. And then concluded our work in the last section.

II. CROSS-DOMAIN INTERFIREWALL OPTIMIZATION

All preceding works were out of focus on cross-domain privacy preserving interfirewall optimization. Rather our proposed work focuses on eliminating the redundant interfirewall policies by maintaining the privacy. Let us consider this by discussing a scenario, where there are two adjacent firewalls 1 and 2 and are affiliated to two different administrative domains as Net1 and Net2. There are policies attached to each firewall. Let F1 be the policy on first firewall's outgoing interface towards firewall 2, and F2 be the policy on second firewall's incoming interface from firewall 1. In each policy of the firewall, there exists a set of rules. Let r be the rule in F2, and if all the traffic packets that matches r but not any rule over r, then they are discarded by F1. We thus can remove the rule r because the such kind of traffic never comes to F2. Here, rule r is considered as redundant rule with respect to F1 [2, 3]. Figure 2 illustrate an example of inter firewall redundancy, where there are two adjoining routers aligned to two administrative domains CSE and EE.



	SIP	DIP	SP	DP	PR	Dec
r_1'	1.2.*.*	192.168.*.*	*	*	TCP	discard
r_2'	2.3.*.*	192.168.*.*	*	*	TCP	accept
r_3'	*	*	*	*	*	discard

FW_1: filtering I_1's outgoing packets

	SIP	DIP	SP	DP	PR	Dec
r_1	1.2.1.*	192.168.1.*	*	25	TCP	accept
r_2	1.2.1.*	192.168.*.*	80	*	TCP	discard
r_3	*	*	*	*	*	accept

FW_2: filtering I_2's incoming packets

Figure 2: Example interfirewall redundant rules.

III. State Of Art

Various researches have been delineated in this section based on optimization of firewall rules and policies. We shall discuss existing cross-domain firewall optimization systems and also review the literature related to commutative encryption technique.

There are varieties of attacks that can take place in a network. For example in this scenario, in a virtual private network there are roaming users who use tunnel for preserving the privacy of their communications, but these users are not properly scrutinized by the external network firewall. Hence, threatening the privacy of the network. In order to deal with these attacks, a technique is proposed called as VGuard. The author in [4], the author proposes VGuard framework makes a policy owner and a request owner to work together. The protocol known as Xhash is also proposed [4]. The author Liu A. X., proposed a firewall compressor, that reduces the firewall policies while keeping the firewall semantics as it is [5]. The author Alex X. Liu Fei Chen has proposed a technique that removes the redundant rules in an interfirewall without compromising the security of the other firewall's policy [6]. They have proposed a framework, where the firewall policies of two domains are imposed by working together. In [7], the author has presented a general framework for rule-based firewall optimization. The first attempt to solve the first-match problem from an all-match perspective is done by the author in [8]. The proposed work in [8], results prove that the redundancy removal is effective and efficient in terms of reducing TCAM and running time respectively.

IV. Proposed Methodology

A. Limitations of State of Art Methods

Prior research focuses on interfirewall optimization and intrafirewall optimization within single administrative domain. In this privacy of firewall is not considered. In interfirewall it includes two firewalls are of same network and optimization is possible without consideration of privacy preserving. In intrafirewall, it contains only a single firewall where the optimization is done. But no prior work focuses on interfirewall optimization between more than one administrative domains. Policies of firewall are not known to each other so privacy is maintained. In the prior work numbers of rules significantly affects its throughput.

B. System Model

The Proposed System evaluate the effectiveness of firewalls and the efficiency of the firewalls. It shows Commutative Encryption to reduce the redundant rules of intra firewall and inter firewall.

The proposed work divides into various approaches : ***System Initialization* -** This phase will create the application environment and two different administrative domain and will provide firewall admin rights to add or remove incoming and outgoing rules. ***Intra firewall Redundant rules removel* -** In this phase it will allow each firewall admin to remove redundant rules within their own firewall. ***Commutative Encryption* -** This is the main phase where it will implement the algorithm and perform the commutatative encryption with keeping the privacy of user preserved. ***Analysis & Testing*** - This phase will include performance testing and graph analysis the application in order to compare with existing approach.

The research is based on changing the way pohing hellman. It means we can say any value which is being encrypted remains same even after changing the order of encryption key, called as commutative encryption. So making simple calculation based on pohling hellman we can convert any number to equivalent number from which the attacker can not identify the original value and both side can compare the range. The idea of P&H is based on the factors of prime number and it is based on simple calculation.

C= M^ e mod p

Table 1 : Commutative Encryption

1.	*First convert the rage into binary*
2.	*Calculate prefix family for the binary conversion digits*
3.	*Encrypt with hey k1 and then with key k2*

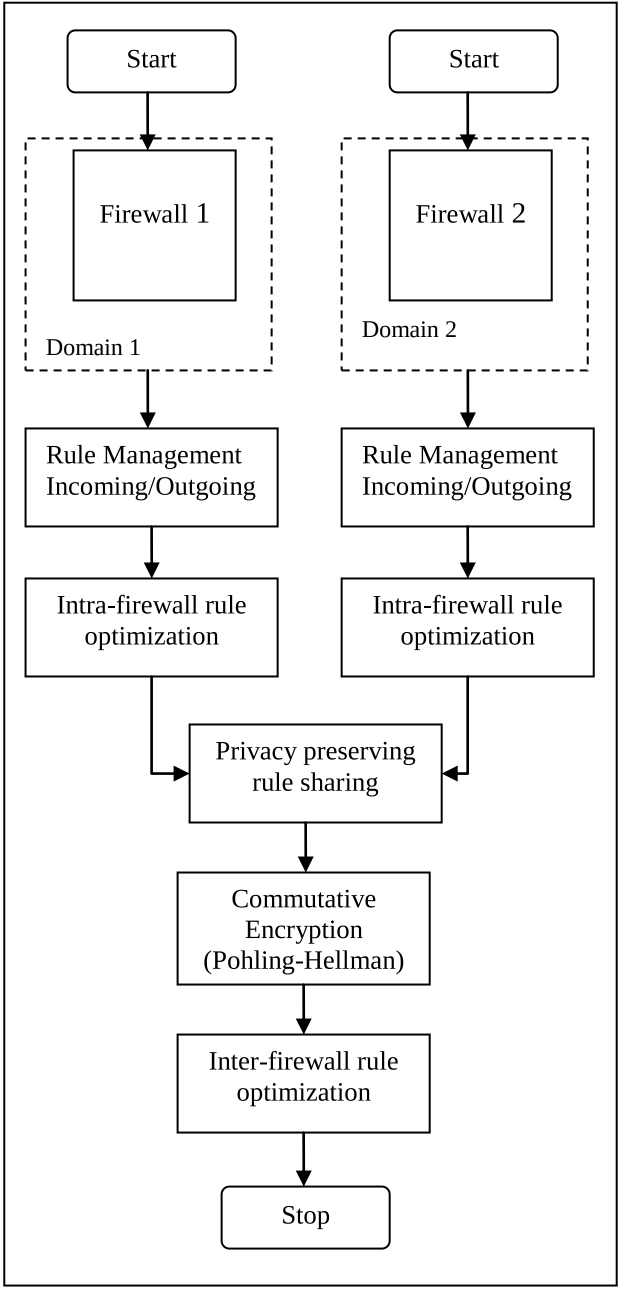
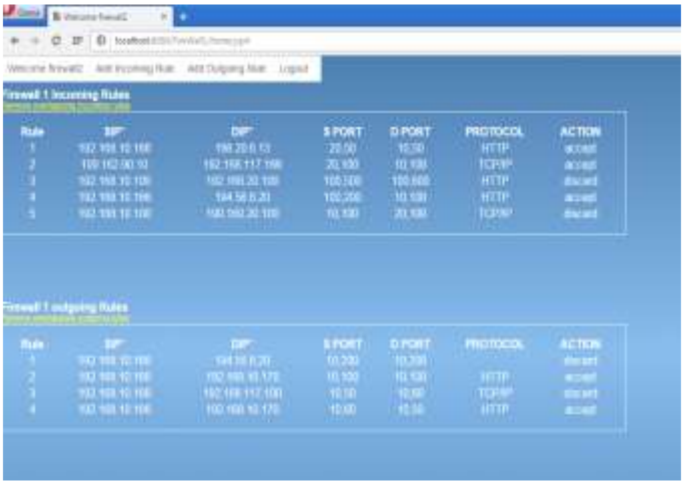

Start
Start
Firewall 1
Firewall 2
Domain 1
Domain 2
Rule Management Incoming/Outgoing
Rule Management Incoming/Outgoing
Intra-firewall rule optimization
Intra-firewall rule optimization
Privacy preserving rule sharing
Commutative Encryption (Pohling-Hellman)
Inter-firewall rule optimization
Stop

Figure 3 : System Architecture

V. IMPLEMENTATION PLAN

The proposed work uses a different method for dealing with removal of redundant rules than used in the existing systems. In the prior existing system, the algorithm included four steps for removing redundant rules, known as: prefix family construction, prefix conversion, prefix numericalization and comparison. But the algorithm takes more processing time for removing the rules. Thus for reducing the processing time, we proposed a method that does not use the four steps and instead benefits the system with the privacy preserving advantage. We use an algorithm, with private keys used for encryption and works similar to the diffie hellman key exchange algorithm.

Following are the screen shots of removal of redundant rules from two firewall administrative domain.



irewall 1 Incoming Rules

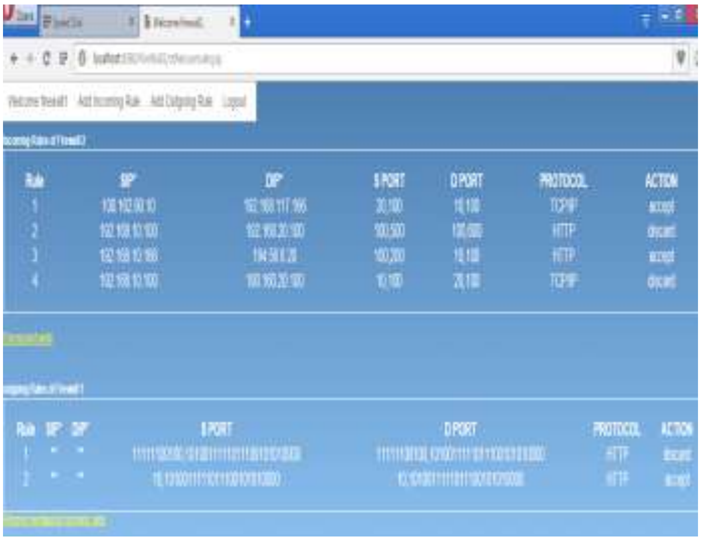
Rule	SIP*	DIP*	S PORT	D PORT	PROTOCOL	ACTION
1	192.168.10.168	198.20.0.13	20,50	10,50	HTTP	accept
2	109.162.90.10	192.168.117.198	20,100	10,100	TCP/IP	accept
3	192.168.10.108	192.168.20.100	100,500	100,600	HTTP	discard
4	192.168.10.196	184.56.8.20	100,200	10,100	HTTP	accept
5	192.168.10.108	190.160.20.100	10,100	20,100	TCP/IP	discard

irewall 1 outgoing Rules

Rule	SIP*	DIP*	S PORT	D PORT	PROTOCOL	ACTION
1	192.168.10.106	184.56.8.20	10,200	10,200		discard
2	192.168.10.106	192.168.10.170	10,100	10,100	HTTP	accept
3	192.168.10.106	192.168.117.100	10,50	10,50	TCP/IP	discard
4	192.168.10.106	192.168.10.170	10,60	10,50	HTTP	accept

Fig.3) Add Incoming and Outgoing Rules in Firewall

In this phase both administrative domain firewall add incoming and outgoing rules. The fields SIP, DIP, SPORT, DPORT and Action are mandatory while the field PROTOCOL is optional.



Welcome firewall1 Add Incoming Rule Add Outgoing Rule Logout

Incoming Rules of Firewall2

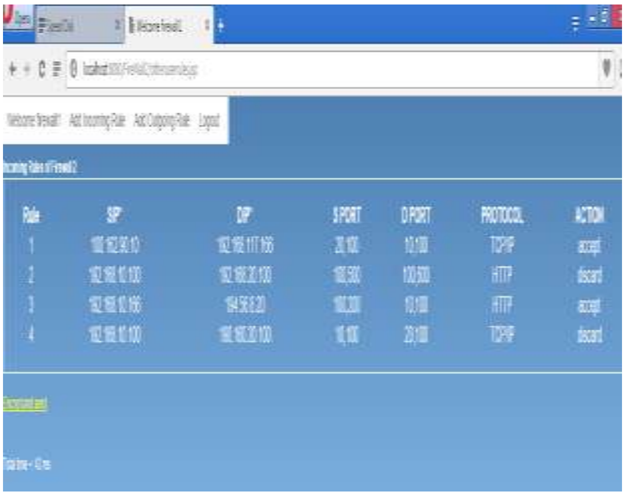
Rule	SIP	DIP	S PORT	D PORT	PROTOCOL	ACTION
1	100.102.90.10	192.168.117.166	20,100	10,100	TCP/IP	accept
2	192.168.10.100	192.168.20.100	100,500	100,600	HTTP	discard
3	192.168.10.166	194.56.8.20	100,200	10,100	HTTP	accept
4	192.168.10.100	100.160.20.100	10,100	20,100	TCP/IP	discard

Outgoing Rules of Firewall1

Rule	SIP	DIP	S PORT	D PORT	PROTOCOL	ACTION
1	*	*	[illegible]	[illegible]	HTTP	discard
2	*	*	[illegible]	[illegible]	HTTP	accept

Fig.4) Encryption of the rules

In this phase the overlapping redundant rules are going to be show in binary form in inter firewall by using Commutative Encryption.



Welcome firewall1 Add Incoming Rule Add Outgoing Rule Logout

Incoming Rules of Firewall2

Rule	SIP	DIP	S PORT	D PORT	PROTOCOL	ACTION
1	100.102.90.10	192.168.117.166	20,100	10,100	TCP/IP	accept
2	192.168.10.100	192.168.20.100	100,500	100,500	HTTP	discard
3	192.168.10.166	194.56.8.20	100,200	10,100	HTTP	accept
4	192.168.10.100	100.160.20.100	10,100	20,100	TCP/IP	discard

Total time - [illegible]

Fig.5) Removal of redundant overlapping rules

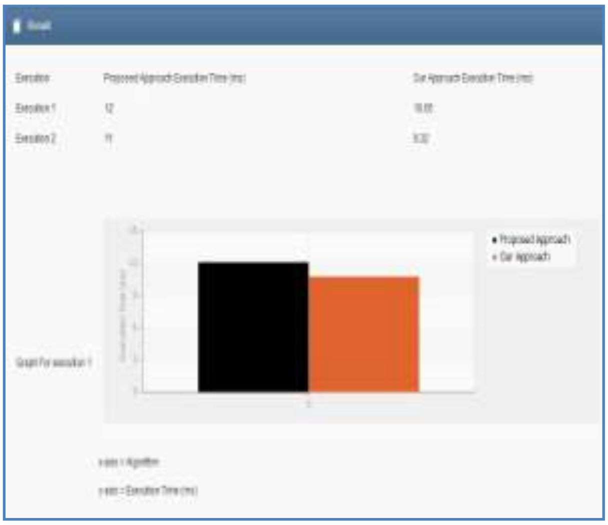
This is the phase where overlapping rules of Firewall2 are removed by Firewall1 i.e. the inter Firewall redundant rules removal is shown.

Possible Outcome: After successful implementation, two machine connected in network simulator will be able to connect with each other even after firewall is on and if they are willing in mutual benefits.

All this can be done without knowing any of the rules or policies of firewall of any machine to each other. That's the beauty of the algorithm.

V. ANALYSIS

With the graph presentation, we carry out the analysis of the system. There are two graphs, that represents the processing time taken by each algorithm. The first estimation describes that more the number of rules more the processing time taken. As the number of rules reduces, processing time taken also reduces in our proposed approach. In our proposed approach, we reduce the number of redundant rule, without revealing the policies and thus, reducing the processing time.



Execution	Proposed Approach Execution Time (ms)	Our Approach Execution Time (ms)
Execution 1	12	[illegible]
Execution 2	11	[illegible]

Figure 4 : Results

EVALUATION PARAMETER

1) Development Cost
2) Execution Time

The development cost is measured on number of temporary variables. As the number of variables increases the development cost decreases. In this project the development cost decreases as compared to prior work. As the number of parameters that are used are less the execution time is also less. So, in our project both development cost and the execution time is less. The result and analysis are shown by calculating the cost and time in the form of graphs.

CONCLUSION

In this paper we deal with the privacy preserving issue in firewall optimization. We have proposed a new and different protocol than before. We present a novel privacy preserving protocol for identifying redundant values in firewall policies without compromising the privacy of the firewall's policies. It in turn improves the performance and throughput of the system. The future scope is to show the firewall optimization between two adjacent firewalls by using hosts or Network Address Translation (NAT) devices.

REFERENCE

[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] 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.

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

[4] A. X. Liu and F. Chen, “Privacy Preserving Collaborative enforcement of firewall policies in virtual private networks”, in Proc. ACM PODC, 2008.

[5] Liu, A.X.; Torng, E.; Meiners, C.R., "Firewall Compressor: An Algorithm for Minimizing Firewall Policies," INFOCOM 2008. The 27th Conference on Computer Communications. IEEE , vol., no., pp.,, 13-18 April 2008.

[6] F. Chen; B. Bruhadeshwar; A. X. Liu, "Cross-Domain Privacy-Preserving Cooperative Firewall Optimization," Networking, IEEE/ACM Transactions on, vol.21, no.3, pp.857,868, June 2013.

[7] Ghassan Misherghi, Lihua Yuan, Zhendong Su, Chen-Nee Chuah, Hao Chen, “A General Framework for Benchmarking Firewall Optimization Techniques“, IEEE Transactions on Network And Service Management, VOL. 5, NO. 4, December 2008.

[8] 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.