A Novel Technique for Effective Optimization of Cross Domain Network Protocol for Redundancy Removal in Firewall Policies

Madhura M.Unde
ME Student, Department of Computer Engineering
G H R College of Engineering and Management,
Pune, India

Simran Khiani
Asst. Professor, Dept. of Information Technology
G H R College of Engineering and Management,
Pune, India

ABSTRACT

In today's rapidly progressing professional world, internet is being used as a medium for almost every operation. Firewalls are extensively implemented to prevent unauthorized access to concealed networks and secure them. Based upon the applied policies a firewall can approve or decline the data packet by scrutinizing them. The large size and intricacy of modern networks result in big and complex firewall policies. Optimizing these policies is crucial for network performance inflation. Existing system facilitates inter-firewall or intra-firewall optimization within similar sets of administrative domains. They try to achieve optimization but at the cost of decreased network performance. In this paper, a protocol to increase the network performance while the cross domain firewall rules are optimized is explained. Rule optimization is achieved by redundant rule removal between the two firewalls. For boosting the performance and security, the data sent over the network will be encrypted and decrypted over a session key. Two types of rules i.e. network and user rules are supported. User can configure his own rules as per the required configuration in appropriate domain. Network rules will be common for both the domains and can be updated by the network administrator. The key technical experimentation is that firewall policies cannot be involved within similar domain areas because a firewall strategy contains exhaustive information and even potential security holes.

General Terms

Networking, Firewall Optimization.

Keywords

Cross domain firewall optimization; privacy; protocol optimization; redundancy removal.

1. INTRODUCTION

A firewall is integration of software and hardware which secludes company's business (internal) network from the external network. They restrict false connections and enable specific connections to pass. It acts as defensive shield between server and external connections to this server. Many organizations continue to impute a remarkable percentage of their corporate "cyber losses" to inside attacks, signaling the need for more robust firewall filtering throughout the enterprise network segments [1]. Following are the causes due to which organizations deploy the firewalls extensively:

- To prevent the attackers from accessing undisclosed information.
- To prevent the attackers from altering or eradicating the important data hoarded in an internal network. Example can be URL spoofing to make illegal use of user's personal information.
- To block the attacker from hampering the regular network's internal performance.

Firewalls are used extensively as

- They can prevent unwanted network traffic.
- They can deviate the incoming traffic to more reliable internal systems.
- They hide susceptible systems, which can't easily be secured from the Internet.

A common example of such attack is to flood the target server with imitated connections to such an extent that the server is unable to respond to permissible connections, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable leading to a server overload. Organizations have secret information stored on computers which includes trade secrets, monetary analysis, product development plans and personal employee records [1].

Packet filter is a most simple type of firewall while a combination of packet filter and application gateways can act as an advanced firewall. A firewall provides thus protecting the data's integrity, availability and secrecy [2]. The data needs to be protected from unwanted changes to data. It needs to be available when needed. It needs to be secluded and secured when applicable. Firewall is a broadly deployed mechanism for enhancing the security of enterprise networks. To obtain the desired functionality a firewall system is implemented through a number of techniques.

1.1 Firewall rules

A network firewall uses a list of rules for filtering packets from one network to another. Firewall rules accept or reject the network traffic passing via one side of the router to the other. Inbound rules limit access by outsiders to private data precisely permitting only a particular set of outside users to access private data [2]. Outbound rules regulate what outside resources local users have permission to.

A firewall has two default rules, one for outbound network traffic and other for inbound [3]. The default rules of the modem router are :-

- Inbound: Prevent all access from outside excluding the responses to requests from the LAN side.
- Outbound: Permit all access from the LAN side to the outside.

In order to specify exceptions to default rules, additional rules can be defined. Custom rules can be added to reject or accept the access based on application, source or destination IP addresses and ports [9].

1.2 Working of firewall

Firewalls use two access denial methodologies. A firewall allows or blocks the network traffic based upon particular criteria. The type of criteria used to determine whether traffic should be permitted through depends on the type of firewall. Firewalls may be perturbed with the type of traffic and source or destination ports and addresses. In order to decide whether the traffic data should be allowed through complicated rule bases are used [3]. The network layer at which firewall operates decides what type of traffic is allowed.

Further we discuss the paper as follows. Section 2 discusses the related work. Cross domain inter-firewall optimization has been explained in section 3. Section 4 describes the existing system and its limitations while proposed approach has been explained in section 5. Results are shown in section 6 and lastly concluding remarks are drawn in section 7.

2. LITERATURE SURVEY

Alex X. Liu, Fei Chen and Bezawada Bruhadeshwar, “Cross-Domain Privacy -Preserving Cooperative Firewall Optimization”, IEEE/ACM TRANSACTIONS ON NETWORKING, Volume 21, No. 3, JUNE 2013 state that they have recognized a chief problem, cross-domain privacy preserving inter-firewall redundancy detection. The researchers have put forward a novel privacy-preserving protocol for identifying redundancy. The protocol implemented identifies the inter-firewall redundancy with a few thousands of rules, e.g. 2000 rules. It is yet costly to compare two firewalls with thousands of rules, e.g. 5500 rules. The protocol is most favorable only if both the domains are eager to gain profit from it and can collaborate in a reciprocal manner. The system lacks to reorder the rules according to priority; due to which optimization is not achieved on a higher scale. The solution to firewall rule anomaly detection and resolution is not provided. Also, it is unable to provide solution for anomaly resolution [4].

M. G. Gouda and A. X. Liu, “Complete redundancy removal for packet classifiers in TCAMs,” IEEE Transactions on Parallel Distributed System, Volume 21, No. 4, pp. 424–437, April 2010 state that the core mechanism that enables many networking services on the Internet such as traffic accounting and firewall packet filtering is the concept of packet classification . The TCAMs i.e. the Ternary Content Addressable Memories use has actually become the standard in the trade to perform high speed packet classification. The classification of TCAM packets is done by comparing a packet with all classification rules of ternary encoding in parallel. The results show that the packets are classified in constant time. The authors present two algorithms for detecting and removing the two types of redundant rules, respectively. The redundant rules are classified into downward redundant rules and upward redundant rules and they formally conclude that after executing the two algorithms, resulting classifiers have no redundant rules. TCAMs are widely used but they are costly and their power consumption is very high [5].

J. Cheng, S. H.Wong, H. Yang and S. Lu, “Design and implementation of cross-domain cooperative firewall,” in Proceedings IEEE ICNP, 2007, pp. 284– 293 state that across two different administrative domains privacy and security are two major factors supporting roaming users. They further state that a roaming user readily uses encrypted tunnels, e.g. VPNs i.e. Virtual Private Networks, to seclude the secrecy and privacy of communications. They present a Cross-Domain Cooperative Firewall (CDCF) that permits two collaborative networks to enforce each other's firewall rules in an in-cognizant manner. In CDCF when an encrypted tunnel between the home network and the foreign network is established by a roaming user, the tunnel endpoint i.e. the VPN server without knowing these rules can direct the traffic and enforce the foreign network's firewall rules. Though the overhead is less, rules have to be fed manually and linear search takes more time due to slow encryption. [6].

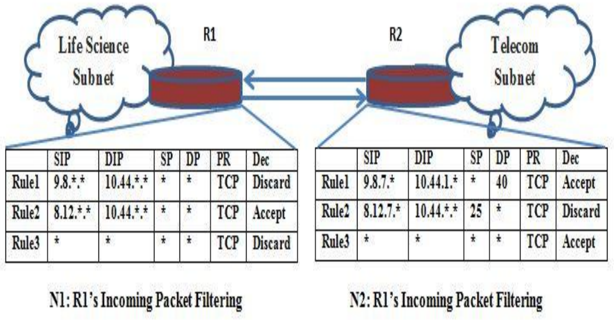
J. Brickell and V. Shmatikov, “Privacy-Preserving Graph Algorithms in the Semi-honest Model”, Advances in Cryptology,2005 presented the scenarios in which two parties, wish to determine some technique through which without leaking any information about their inputs except that revealed by the algorithm’s output. Working in the standard secure multi-party computation paradigm, researcher’s present new algorithms for privacy-preserving computation of single source shortest distance and all pairs shortest distance, and further they also propose two new algorithms for privacy-preserving set union. The algorithms implemented have higher time complexity and they can’t process the discarded traffic. [7].

E. Al – Shaer and H. Hamed, “Discovery of policy anomalies in distributed firewalls,” in Proceedings IEEE INFOCOM, 2004, pp. 2605–2616 explained that the chief elements in network security are Firewalls. Firewall filtering rules have to be ordered, written and distributed correctly in order to avoid firewall policy anomalies that might cause network vulnerability. Hence, modifying or inserting filtering rules in any firewall requires thorough intra- and inter-firewall analysis to determine the proper rule placement and ordering in the firewalls. These techniques are implemented in a software tool called the "Firewall Policy Advisor" that simplifies the management of filtering rules and maintains the security of next-generation firewalls. The advisor detects only pairwise anomalies and forward rules. The anomalies are detected and a warning to resolve them is given but those are not resolved. [8].

3. CROSS DOMAIN INTER-FIREWALL OPTIMIZATION

Firewall works on both inter-firewall and Intra firewall domains [9]. Prior work focuses on both these domains but only within single network. It is necessary to seclude the firewall policy contains private and important reliable information. Fig.1 illustrates inter-firewall redundancy, where in two routers which are next to each other and conjoined belong to dissimilar administrative domains Life Science and Telecom domain in an IT organization.

Let us consider two firewall policies FW1 and FW2 which belong to different administrative domains D1 and D2 and we need to detect inter-firewall redundant rules for these two domains. A firewall policy consists of a collection of rules in which each rule has a predicate and a decision for the packets that are equivalent to the predicate. Based on defined rule r, firewall checks each incoming and outgoing packets among these domains. The protocol contains the protocol type, source



	SIP	DIP	SP	DP	PR	Dec
Rule1	9.8.*.*	10.44.*.*	*	*	TCP	Discard
Rule2	8.12.*.*	10.44.*.*	*	*	TCP	Accept
Rule3	*	*	*	*	TCP	Discard

N1: R1's Incoming Packet Filtering

	SIP	DIP	SP	DP	PR	Dec
Rule1	9.8.7.*	10.44.1.*	*	40	TCP	Accept
Rule2	8.12.7.*	10.44.*.*	25	*	TCP	Discard
Rule3	*	*	*	*	TCP	Accept

N2: R1's Incoming Packet Filtering

Fig 1: Example demonstrating inter-firewall redundant rules

port, destination port and source and destination IP. The protocol type defines whether to allow or deny the packet's entry into the system. Further each of the rules in both firewalls FW1 and FW2 are converted into non-overlapping rules and then the validation of equivalent set of non-overlapping rules (nr) is done using the resolving set i.e. M (nr) = R (nr). Here we verify if the non-overlapping rule nr in FW2 fulfills the non-overlapping discarding rule in FW1 and also check for the multiple non overlapping discarding rules. It is also required to verify Privacy-Preserving Range Comparison.

4. EXISTING SYSTEM

4.1 Comparison of Privacy-Preserving Range

The chief target is to check whether a packet's byte code from FW2 lies in particular range .Now it is necessary to zero-in the problem of checking if the packet's byte code and the numbers in particular range have some data in common. The range comparison is in terms of comparing the source and destination network parameters like IP address, port and protocol. [9]

4.2 Processing Firewall rule FW1

In order to ease the detection of the redundant rules in FW2, Net1 converts its firewall rule FW1 to a set of non-overlapping rules. The network Net1 first converts each range of non-overlapping discarding rules from FW1 to a prefix set to preserve the privacy of FW1 and further the networks Net1 and Net2 encrypt these set of prefixes using commutative encryption techniques.

4.3 Processing Firewall rule FW2

To compare the firewall policies in a privacy preserving manner; Net1, and Net2 convert firewall rules FW2 to f sets of double encrypted numbers, where f is the number of fields.

4.4 Limitations

- It can only detect two identical anomalies in firewall rules.
- Discovers all the preceding rules but disregards all subsequent rules when anomaly analysis is being done.
- It can only show that there is a misconfiguration between one of the rules and its preceding rule, but cannot correctly determine all rules involve in an anomaly.

5. PROPOSED APPROACH TO OPTIMIZE THE PROTOCOL USED TO MINIMIZE THE FIREWALL POLICIES

The system will beat the pitfalls of existing system. It has advent traits which can easily enable the tasks such as accessing, managing, detecting, rearranging and resolving the firewall rules in the rule engine. The system will be valuable for administrators and service providers. The existing approach eliminates the redundant rules but at the cost of increased processing and communication time. The configuration for proposed system is shown in the Fig. 2.

As shown in Fig.2, we propose to optimize the protocol using following approach

- Step 1: Data packet is sent from network Net1 of Life-Science domain towards the network Net2 of Telecom domain.
- Step 2: Network rules and user rules for each domain are inserted into the system. Each time rule is added, an ordering is associated with the rule.
- Step 3: If the rules are redundant, the redundancy is removed by eliminating the duplicate rules.
- Step 4: The applicable rules are applied on the data sent and packet is stored on a server.
- Step 5: A secret key is generated by using the El-Gamal key generation algorithm.
- Step 6: The secret key generated is used in Perfect forward secrecy algorithm as a session key. A separate unique key is maintained for each session.
- Step 7: After the rules are applied on the data packet, the data is encrypted using the generated key through Perfect forward secrecy algorithm.
- Step 8: Lastly the data will be decrypted using Perfect forward secrecy algorithm thus removing the duplicate rules also.
- Step 9: In order to achieve security and increased response and processing time, these data packets in network can either be sent from N1 to N2 and vice-versa.

5.1 Algorithm for Rule Redundancy and Anomaly Removal

5.1.1 Input

Rule set from N1 and N2

5.1.2 Output

Rule set with redundant rules and anomaly removed

5.1.3 Algorithm

```
Initialize all the flags to false
Set anomalyCounter=0

While (each incoming packet $r_{mi}$ from N1)

For each $r_{ni}$ in N2

    Compare (IP of $r_{mi}$ and IP of $r_{ni}$) == 0
        Set IPFlag == true

    Compare ( Port of $r_{mi}$ and Port of $r_{ni}$) == 0
```

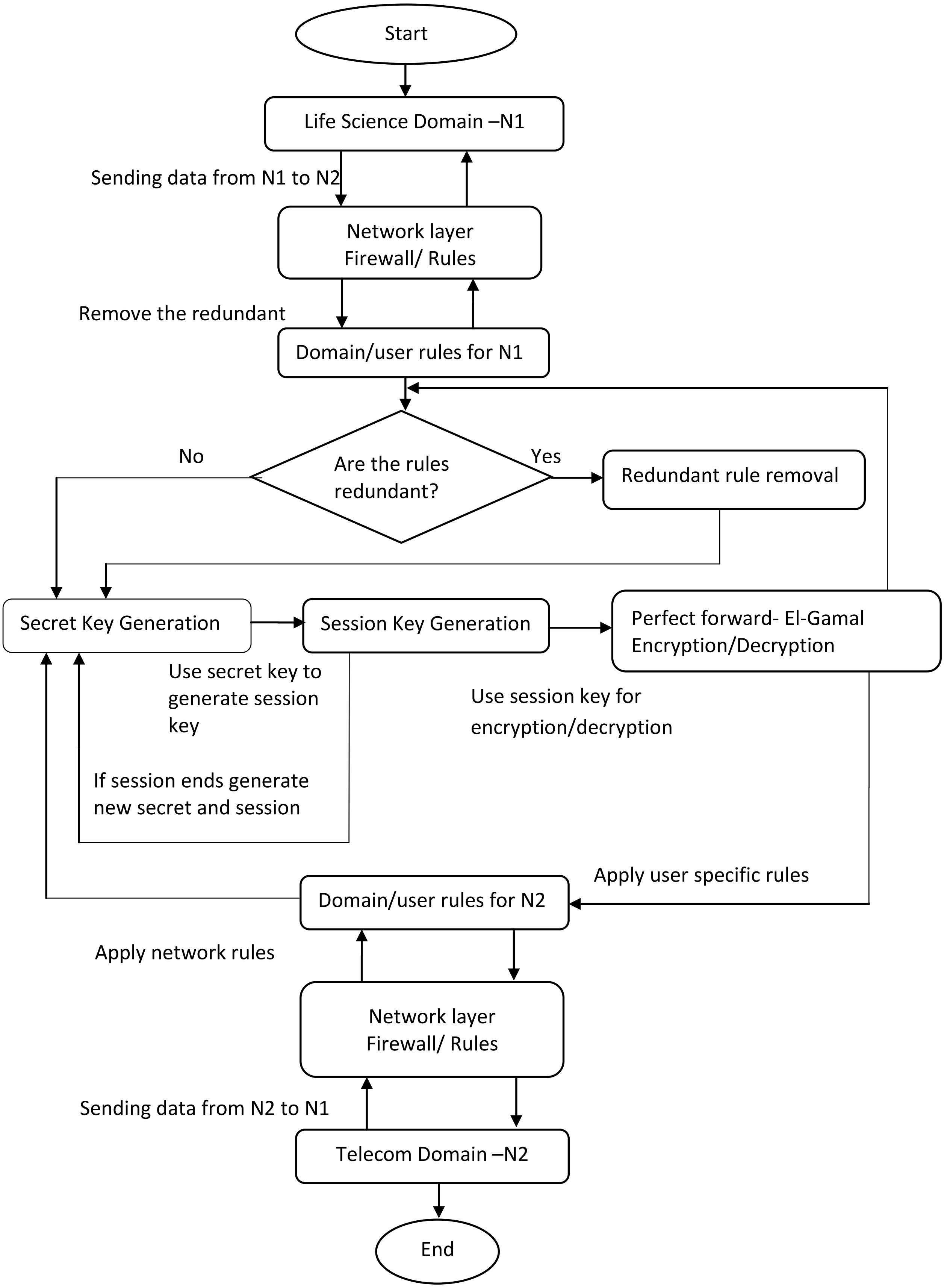


Fig 2: Data flow chart of two Administrative Domains

```
Set Port Flag == true
        Compare ( Protocol of $r_{mi}$ and IP of $r_{ni}$ ) == 0
                Set ProtoFlag == true
        Compare ( Decision of $r_{mi}$ and IP of $r_{ni}$ ) == 0
                Set DecFlag == true

        If( IPFlag == false && PortFlag == true && ProtoFlag == true)
        Compare network identifier of ( $r_{mi}$ and $r_{ni}$ ) ==0
    If host identifier of $r_{ni}$ == any
        AnamalyArr[anomalyCounter] = $r_{ni}$
        Increment AnomalyCounter
                Increment AnomalyCounter
If (IPFlag == true && PortFlag == true && ProtoFlag == true)
        If (DecFlag == false)
                AnamalyArr[anomalyCounter] = $r_{ni}$
                Increment AnomalyCounter
```

5.2 Algorithm for Perfect Forward El-Gamal Encryption/Decryption

Input: - Large Prime number ‘p’, base ‘g’, secret integer ‘a’ and ‘b’, plaintext files from sender

Output: - Secured Plaintext file received after encryption and decryption.

Algorithm:-

1) Sender and receiver agree on a prime number ‘p’ and a base ‘g’.
2) Sender chooses a secret integer ‘a’ and sends A = $g^a \bmod p$
3) Receiver chooses a secret integer ‘b’ and sends B = $g^b \bmod p$
4) Sender computes s = $B^a \bmod p$
5) Receiver computes s = $A^a \bmod p$
6) Sender and receiver share the secret.
7) Receiver at N2 generates a number ‘a’ and a secret integer ‘x’ which is now assigned the value of shared secret session key‘s’.
8) Compute ’d’ as $a^X \bmod p$
9) Determine public key (p, a , d) and private key ‘x’(which is secret key ‘s’)
10) Sender at N1 obtains public key (p , a ,d) from receiver.
11) Choose random integer k such that 1 < k< p-2
12) Compute y= $a^k \bmod p$ and z = $(d^k * m) \bmod p$ where ‘m’ is the plaintext.
13) Obtain cipher text as C = (y, z) and send to receiver at N2.
14) Receiver computes ‘r’ as r = $y^{p-1-x} \bmod \mathrm{p}$
15) Obtain original plaintext as m= (r * z) mod p

6. SIMULATION RESULTS

We examine the potency of our protocol on real firewalls and analyze its effectiveness. Our protocol has been implemented using Java 6.0, MySQL 5.0, and GlassFish Server 3.0 and carried out the experiments on a system with configuration as Windows 7 with 2GB of memory. Firewall converts the packets into format of source and destination IP, source and destination port and prototype type. Firewall evaluates each incoming and outgoing data packets with the rule sets. As shown in the graph from Fig.3, as the no. of rules increase, the throughput i.e. the data transfer productivity decreases. The graph shown in Fig.3 is obtained from the data in Table 1. We address firewall optimization to prevail over the decreasing throughput and communication cost. Hence as seen from the graph in Fig.3 when the no. of rules increases, our approach improves the throughput as compared to the previous approach in Fig.3.As shown in Fig.4 obtained from the data in Table 2, it is clear that comparatively our protocol improves the processing time and security by applying the session key based encryption techniques.

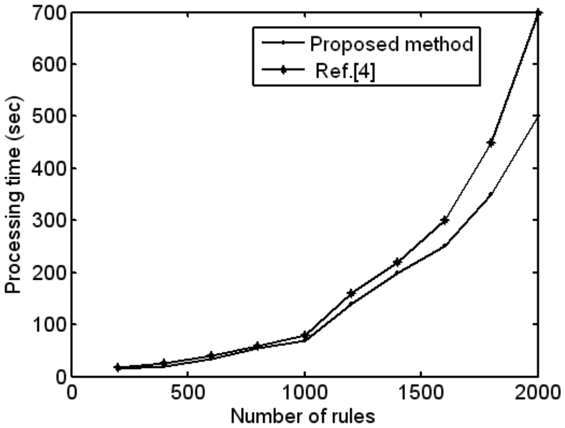


Fig 3: Comparison of processing time in proposed vs existing method

When processing firewall FW1 in the communication cost from Net1 to Net2 and that from Net2 to Net1 are less than 60 KB. Note that the communication cost from Net2 to Net1 and that from Net1 to Net2 are the same because Net1 and Net2 encrypt and decrypt the same no. of data packets and the encrypted values have the same length in our experiments. When processing FW2 in those real firewall groups, the communication cost from Net2 to Net1 is less than 100KB. The total communication cost between two parties is less than 150KB, which can be sent through the current network around 8 seconds.

Table 1. Table showing Processing time for Number of Rules

Number of Rules	Processing Time for Existing method (sec)	Processing Time for Proposed method (sec)
200	23	20
400	31	26
600	42	38
800	66	63
1000	79	67
1200	175	156
1400	218	197
1600	301	258
1800	427	329
2000	698	500

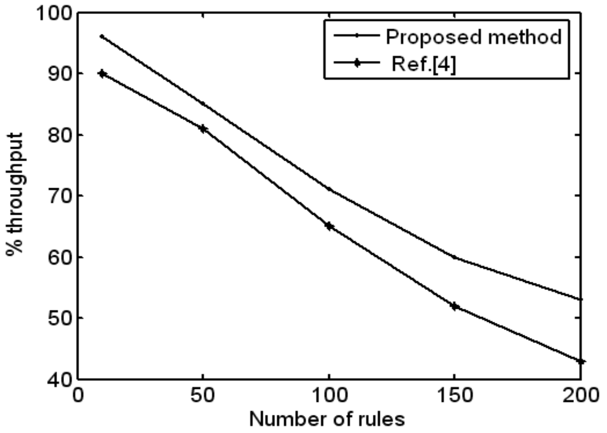


Fig 4: Number of rules vs. Throughput in Proposed and Existing method

Table 2. Table showing Throughput for Number of Rules

Number of Rules	Throughput for Existing method (%)	Throughput for Proposed method (%)
10	96	90
50	85	81
100	71	65
150	60	52
200	53	43

7. CONCLUSION AND FUTURE WORK

Firewall security, requires proper management in order to provide proper security services. In this paper, we recognized a unique privacy-preserving protocol for identifying redundancy in firewall rules. If the rule exists, a cross domain cooperative firewall protocol can be used to increase network performance. But, the network performance slumps down if the rule does not exist. This protocol tries to improve the network performance to safeguard firewall policies but at the cost of loss of security and also large communication and processing time. Hence we have optimized the protocol by applying the session key encryption techniques before sending the data packet over to the other administrative domain. This will provide security along with increase in response time of communication and processing much better when compared with previous methods. There are many notable cases that could be investigated based on our current protocol. A good example may be hosts or Network Address Translation (NAT) devices between two adjoining firewalls.

8. ACKNOWLEDGEMENTS

We are grateful to our project guide Mrs. Simran Khiani for her remarks, suggestions and time. Also the Head of the Department And Principal for providing all the vital facilities like for providing the required facilities, Internet access and important books, which were essential. We are also thankful to all the staff members of the Department of Information Technology of G. H. Raisoni college of Engineering & Management, Pune.

9. REFERENCES

[1] James F. Kurose and Keith W. Ross, "Computer Networking: A Top-Down Approach", Addison-Wesley Publication,6th Edition, pp.641, Copyright 1996-2000

[2] El- Sayed M and El- Alfy, “A Heuristic Approach for Firewall policy optimization”, ICACT Conference: Advanced Communication Technology, vol.3, pp.1782-1787, FEB 2007.

[3] Tihomir Katic and Predrag Pale, “Optimization of Firewall Rules”, Information Technology Interfaces, 29th International Conference, pp.685-690, June 2007

[4] Fei Chen, Bezawada Bruhadeshwar, and Alex X. Liu, “Cross-Domain Privacy – Preserving Cooperative Firewall Optimization”, IEEE/ACM transactions on Networking, vol. 21, Issue no. 3, pp.857-868, June 2013.

[5] A. X. Liu and M. G. Gouda, “Complete redundancy removal for packet classifiers in TCAMs”, IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 4, pp.424–437, April 2010.

[6] J. Cheng, H. Yang, S. H.Wong, and S. Lu, “Design and implementation of Cross-domain cooperative firewall”, IEEE International Conference on Network Protocols, pp.284– 293, Oct.2007

[7] J. Brickell and V. Shmatikov, “Privacy-Preserving Graph Algorithms in the Semi-honest Model”, Proceedings of the 11th international conference on Theory and Application of Cryptology and Information Security, pp.236-252, 2005

[8] E. Al – Shaer and H. Hamed, “Discovery of policy anomalies in Distributed firewalls”, Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, vol.4, pp.2605–2616, 2004

[9] A. X. Liu, C. R. Meiners, and Y. Zhou, "All- match based complete redundancy removal for packet classifiers in TCAMs", The 27th Conference on Computer Communications. IEEE, pp.574–582, 2008