An Optimized Redundancy Removing Protocol to Minimize the Firewall Policies in Cross Domain Network Architecture

Madhura M.Unde, Simran Khiani

Abstract— **In order to secure the private networks in today's fast-paced business world firewalls are being deployed. Based on the policy adopted, firewall either accepts or rejects the incoming or outgoing network packets by checking them .In this paper the protocol to optimize the cross-domain firewall policies so as to boost the network performance will be explained. The process of protocol optimization involves removal of redundant rules between the two firewalls by extracting the common data. This data will further be encrypted, compressed and sent to other network by compressing the data file. The key technical challenge is to avoid data loss due to compression. The protocol will be developed in Java and is expected to reduce the data transfer rate compared to the previous methods.**

Index Terms— **Cross domain firewall optimization, privacy, protocol optimization, redundancy removal.**

I. INTRODUCTION

A firewall is a conjunction of hardware and software that isolates an organization's internal network from the outside internet majorly, allowing specific connections to pass and obstructing others. Organizations make use of firewalls for one or more of the following reasons:

1. To prevent intruders from interfering with the daily operation of the internal network. SYN flooding is an example of a denial of service attack, in which forged TCP connection-establishment segments are sent to a particular host by the attacker. A separate buffer is assigned for each connection, and within minutes no TCP buffer space is left for "honest" TCP connections.
2. To block the intruders from deleting or modifying data stored in an internal network. Good example can be an attacker can attempt to meddle with an organization's public presence on a Web server -- a successful attack may be seen by thousands of people in a matter of minutes.
3. To block the intruders from obtaining secret data.

Manuscript received Nov, 2014.
***Madhura M.Unde**, Department of Computer Engineering, G.H Raisoni College of Engineering and Management, Pune, India, Pune, India, +919423435018*
***Simran Khiani**, Department of Information Technology, G.H Raisoni College of Engineering and Management, Pune, India, Pune, India, +919326007227*

Many of the organizations have secret information stored on computers which includes product development plans, trade secrets, personal employee records and monetary analysis [1].

The simplest firewall consists of a packet filter. More advanced firewalls consist of combinations of application gateways and packet filters. A firewall safeguards the data's integrity, availability and secrecy. The data needs to be protected from unwanted alterations. It needs to be accessible when needed. Its privacy needs to be secured when applicable. Firewall is a widely deployed mechanism for improving the security of enterprise networks. A firewall system is implemented through a number of mechanisms that collectively achieve the desired functionality.

A. Firewall rules

Various firewalls usually provide different rule logic with different parameters except the common basic elements. All these firewalls empower an action to be defined allowing or banning specific network traffic. Also, all of them allow checking for most important elements in packets like ports, protocol and IP addresses. Software for firewall rule optimization (FIRO) was initially developed for IP Tables firewall command tool. Stateful inspection is one of the most important functionalities of IP Tables firewall [2].It automatically opens only the ports necessary for internal packets for Internet access. It only allows transfer of packets which are defined in firewall rules and which are part of established connections. Specifically a network firewall uses a list of rules for filtering packets from one network to another.

B. Working of firewall

There are two access denial methodologies used by firewalls. A firewall accepts or denies the traffic based upon particular criteria. The type of criteria used to decide whether traffic should be allowed through varies from one type of firewall to another. Firewalls may be apprehensive with the source or destination addresses and ports or with the type of traffic. Complex rule bases that inspect the application data to determine if the traffic should be permitted are used by firewalls [3]. How a firewall determines what traffic to let through depends on which network layer it operates.

The rest of the paper is organized as follows. Section II discusses the related work. Cross domain inter-firewall optimization has been explained in section III. Section IV describes the existing system and its limitations while proposed approach has been explained in section V. Lastly, concluding remarks are drawn in section VI.

ISSN: 2278 – 1323

II. Related Work

Fei Chen, Alex X. Liu and Bezawada Bruhadeshwar, "Cross-Domain Privacy -Preserving Cooperative Firewall Optimization", IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 21, NO. 3, JUNE 2013 state that they have identified an important problem, cross-domain privacy preserving inter-firewall redundancy detection. They have proposed a novel privacy-preserving protocol for detecting such redundancy. The results on real firewall policies show that the protocol can remove as many as 49% of the rules in a firewall whereas the average is 19.4%. The protocol is applicable for identifying the inter-firewall redundancy of firewalls with a few thousands of rules, e.g. 1900 rules. However, it is still expensive to compare two fire- walls with many thousands of rules, e.g. 5000 rules. The protocol is most beneficial if both parties are willing to benefit from it and can collaborate in a mutual manner [4].

A. X. Liu and M. G. Gouda, "Complete redundancy removal for packet classifiers in TCAMs," IEEE Transactions on Parallel Distributed System, vol. 21, no. 4, pp. 424–437, Apr. 2010 state that Packet classification is the core mechanism that enables many networking services on the Internet such as traffic accounting and firewall packet filtering. Using Ternary Content Addressable Memories (TCAMs) to perform high speed packet classification has become the de facto standard in the trade. TCAMs classify packets in constant time by comparing a packet with all classification rules of ternary encoding in parallel. The experiments on real-life classifiers show an average diminution of 58.2 percent in the number of TCAM entries by removing redundant rules. Based on this condition, the researchers categorize redundant rules into upward redundant rules and downward redundant rules. Second, they present two algorithms for detecting and removing the two types of redundant rules, respectively. Third, they formally prove that the resulting classifiers have no redundant rules after running the two algorithms [5].

J. Cheng, H. Yang, S. H.Wong, and S. Lu, "Design and implementation of cross-domain cooperative firewall," in Proceedings IEEE ICNP, 2007, pp. 284– 293 state that security and privacy are two major concerns in supporting roaming users across administrative domains. Ongoing practices show that a roaming user often uses encrypted tunnels, e.g., Virtual Private Networks (VPNs), to protect the secrecy and privacy of her communications. They propose a Cross-Domain Cooperative Firewall (CDCF) that allows two collaborative networks to enforce each other's firewall rules in an oblivious manner. In a Cross-Domain Cooperative Firewall when a roaming user establishes an encrypted tunnel between his home network and the foreign network, the tunnel endpoint (e.g., a VPN server) can regulate the traffic and enforce the foreign network's firewall rules, without knowing these rules. The results show that CDCF can protect the foreign network from encrypted tunnel traffic with minimal overhead [6].

J. Brickell and V. Shmatikov, "Privacy-Preserving Graph Algorithms in the Semi-honest Model", Advances in Cryptology,2005 stated the scenarios in which two alliances, wish to determine some algorithm 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 SSSD (single source shortest distance) and APSD (all pairs shortest distance), and also two new algorithms for privacy-preserving set union. Their algorithms are significantly more efficient than generic constructions [7].

E. Al – Shaer and H. Hamed, "Discovery of policy anomalies in distributed firewalls," in Proceedings IEEE INFOCOM, 2004, pp. 2605–2616 stated that Firewalls are core elements in network security. Firewall filtering rules have to be written, ordered 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 [8].

III. 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 provide security as the firewall policy contains private and confidential information. Fig. 1 illustrates inter-firewall redundancy, where two adjoining routers belong to dissimilar administrative domains CSE and EE.

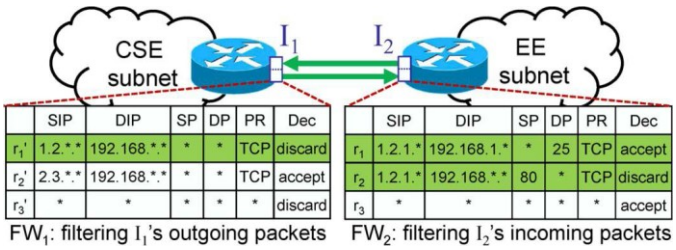

Fig.1. Data flow chart of two administrative domains

Let us consider two firewall policies F1 and F2 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 source IP, destination IP, source and destination ports and protocol type. The protocol type defines the acceptance or denial of the packet. First convert each firewall F1, F2 into non overlapping rules. Validate the equivalent set of non-overlapping rules (nr) with resolving set i.e. M (nr) = R (nr). Here verify if the non-overlapping rule nr in F2 fulfills the non-overlapping discarding rule in F1 and also check for the multiple non overlapping discarding rules. It is also needed to check Privacy-Preserving Range Comparison.

IV. EXISTING SYSTEM

A. Privacy-Preserving Range Comparison

The problem is to check whether a packet's byte code from FW2 is in particular range. Now the aim is to convert the problem of checking if the packet's byte code and the numbers in particular range have some data in common [9].

B. Processing Firewall policy FW1

To detect the redundant rules in FW2, N1 converts its firewall FW1 to a set of non-overlapping rules. To preserve the privacy of FW1, N1 first converts each range of non-overlapping discarding rules from FW1 to a set of prefixes. Second N1 and N2 encrypt these prefixes using commutative encryption.

C. Processing Firewall policy FW2

For comparing the firewall policies in a privacy preserving manner N1, and N2 convert firewall FW2 to b sets of double encrypted numbers, where b is the number of fields.

D. Limitations

1. Can only detect two identical anomalies in firewall rule.
2. Determines all the preceding rules but ignores all subsequent rules while doing the anomaly analysis.
3. 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.

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

Our system will overcome the drawback of existing system. It has advent features which are easily accessing, managing, detecting, rearranging and resolving the firewall rules in the rule engine. It is a beneficial for Administrator and service providers. The existing approach eliminates the redundant rules but at the cost of increased processing and communication time. The configurations for proposed system are shown in the Fig. 2.We thus propose to optimize the protocol using following approach:

1. Encrypt the data sent from home network N1 to other business network N2.
2. Compress the data received from N1 using Huffman data compression algorithm.
3. FW1 will send this data to FW2
4. Data will be decompressed and further decrypted at N2
5. Duplicate rules will be removed in between the two networks.

Encryption and decryption will be done using Pohlig-Hellman algorithm as follows:

$$Enc(M, K) = MK \bmod P \quad (1)$$

Where M is the message, K is the key and P is a large prime modulus.

While compression and decompression will be done through Huffman encoding and decoding mechanism as follows:-

A. Input

1. Packet data in byte format B = $\{b_1, b_2, ..., b_n\}$
2. Set P = $\{p_1, p_2, ..., p_n\}$ which is set of probability of Occurrence of data in a firewall rule i.e. Pi = P (Bi), $1 \leq i \leq n$ where n is the max no of packets

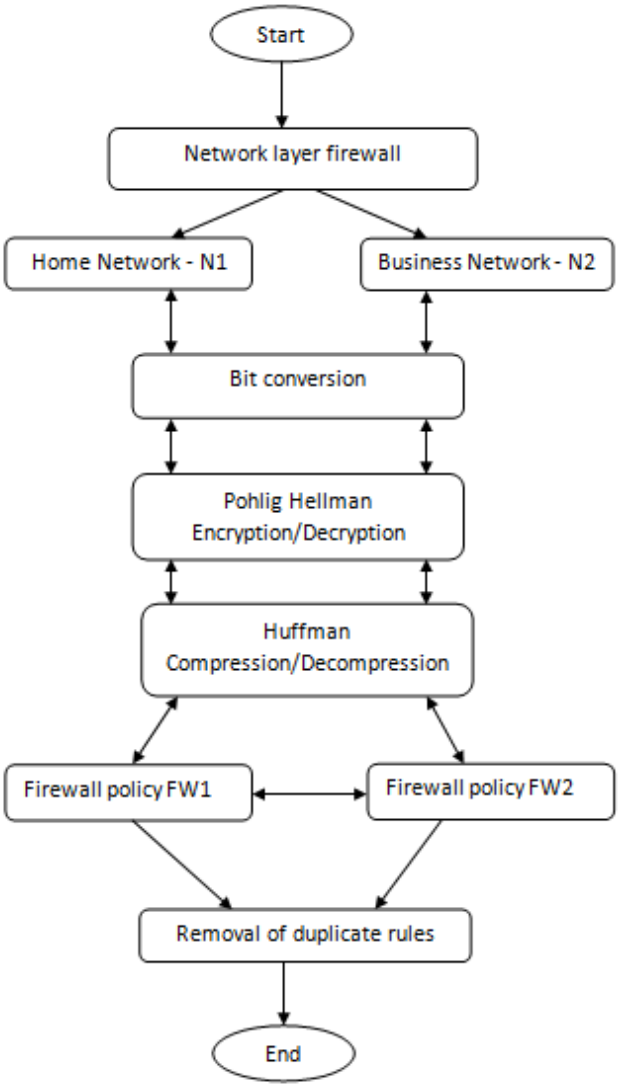

Fig.2. Data flow chart of two administrative domains

B. Output

Code C (B, P) = $\{c_1, c_2, ..., c_n\}$ is binary keyword set of code words where ci is the code word for ai, $1 \leq i \leq n$

C. Goal

Let $L(C) = \sum_{i=1}^{n} P_i \times$ length (Ci) be the weighted path length of code C with condition L(C) <= L(T) for any code T(B,P)

In order to achieve security and increased response and processing time. These data packets in network can either be sent from FW1 to FW2 and vice versa.

VI. CONCLUSION

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 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

ISSN: 2278 – 1323

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 encryption and compression 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.

ACKNOWLEDGMENT

I take immense pleasure in expressing a humble note of gratitude to my project guide **Mrs. Simran Khiani**, Assistant Professor, Department of Information technology, G.H Raisoni College of Engineering and Management, for her useful suggestions, which helped me in completing the paper before deadline.

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, 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,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 AnnualJoint 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

Miss. Madhura M. Unde M.E Computer Engineering Student, G.H Raisoni College of Engineering and Management, Pune, India, +919423435018.

Mrs. **Simran Khiani** Assistant Professor, G.H Raisoni College of Engineering and Management, Pune, India, +919326007227

