Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Interfirewall optimization across various administrative domain for enabling security and privacy preserving

Kalaivani.M[1], Rohini.R[2]
[1,2]*Department of CSE, Vivekanandha College of Engineering for Women,*

Abstract— Network security is usually protected by a firewall, which checks in-out packets against a set of defined policies or rules. Hence, the overall performance of the firewall generally depend on its rule management. For example, the performance can be decreased when there are firewall rule anomalies. The anomalies may happen when two sets of firewall rules are overlapped or their decision parts are both an acceptance and a denial simultaneously. Firewall optimization focuses on either inter-firewall or intra-firewall optimization within one administrative domain where the privacy of firewall policies is not a concern. Explore interfirewall optimization across administrative domain for the first time. The key technical challenge is that firewall policy cannot be shared across domains because a firewall policy contains confidential information and even potential security holes, which can be exploited by attackers. Using interfirewall redundant rule which overcome the prior problem and enable the interfirewall optimization across administrative domains. Also propose the first cross domain cooperative firewall (CDCF) policy optimization protocol. The optimization process involves cooperative computation between the two firewall without any party disclosing its policy to the other.

Keywords- Interfirewall optimization, Redundancy Removal algorithm.

I. INTRODUCTION

Network security is usually protected by a firewall, which checks in-out packets against a set of defined policies or rules. Hence, the overall performance of the firewall generally depends on its rule management. For example, the performance can be decreased when there are firewall rule anomalies. The anomalies may happen when two sets of firewall rules are overlapped or their decision parts are both an acceptance and a denial simultaneously. In this paper, we propose a new paradigm of the firewall design, consisting of two parts:

(1)**Single** Domain Decision firewall (SDD) -a new firewall rule management policy that is certainly not conflicts.

(2)The **Binary** Tree Firewall (BTF) -a data structure and an algorithm to fast check the firewall rules.

Experimental results have indicated that the new design can fix conflicting anomaly and increase the speed of firewall rule checking from $O(N^2)$ to $O(\log_2 N)$.

A firewall is a network security system that controls the incoming and outgoing network traffic based on applied rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the internet) that is assumed not to be secured and trusted. Firewall exist both as a software solution and a hardware appliance.

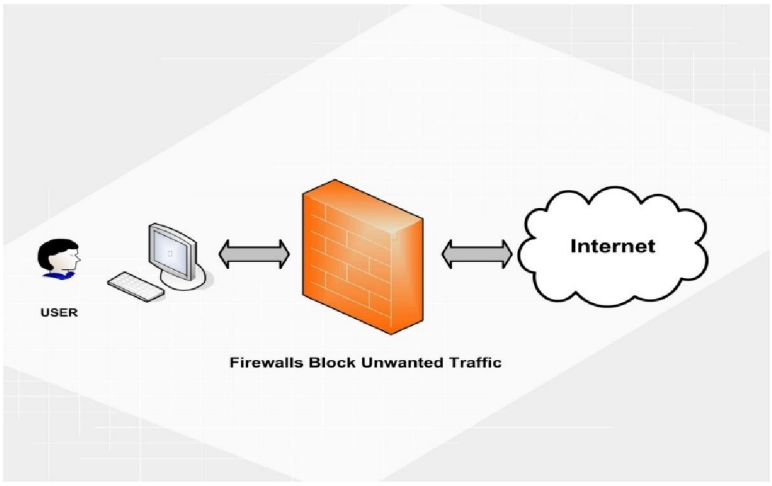

Figure1.Architecture of firewall

Firewalls are critical in securing private network of business, institutions, and home networks. A firewall is often placed at the entrance between a private network and the external network so that it can check each incoming and outgoing packet and decide whether to accept or discard the packet based on its policy. A firewall policy is usually specified as a sequence of rules, called Access Control List (ACL), and each rule has the predicate over multiple packed header fields.

i) Source IP
ii) Destination IP
iii)Source port
iv)Destination port
v) Protocol type

The rule in a firewall policy typically follows the first-match semantics, whether the decision of the packet matches in the policy. Each physical interface of a router/firewall is configured with two ACLs:

1. One for filtering outgoing packets.
2. Other one for filtering incoming packets.

The number of rules in a firewall significantly affects its throughput. Unfortunately, with the explosive growth of services deployed on the internet, firewall policies are growing rapidly in size. Thus, optimizing firewall policy is crucial for improving network performance. The firewall optimization focuses on either inter-firewall or intra-firewall optimization within one administrative domain where the privacy of firewall policy is not a concern. Inter-firewall optimization means optimizing a single firewall. Firewall can protect against some problems (virus and attacks) that come from the internet. That can't protect against viruses that come from infected media (like an infected office documents on an USB flash drive).

II. RELATED WORK

Various researches have been reported in this related work based on optimization of firewall rules and policies.

Managing firewall rules particularly in multi-firewall enterprise network. To identify all anomalies exist in a single and a multi-firewall environment. It automatically discovers the policy

anomalies in centralized and distributed firewall. The tool implements the "interfirewall and intra-firewall anomaly discovery algorithms", as well as the distributed "firewall policy editor"

Oblivious membership verification [2] technique is used for rules in a firewall is redundant. So that they are using "redundancy checking algorithm" that is mainly used for verifying whether the rules in a firewall accept discard an intended set of packets.

"Firewall compressor algorithm" is used for compressing both one-dimensional and multi-dimensional firewall. They uses optimal algorithm such as dynamic programming technique for compressing one-dimensional firewall and systematic approach for multi-dimensional firewall compression.

Digital signature technique is a mathematical technique used to validate the authentication and integrity of a software or digital document. Digital signature is mainly based on public key cryptography also called as asymmetric cryptography. That uses public key algorithm such as RSA, it generates two keys (one private key and one public key) that are mathematically linked.

They propose the VGuard a framework which allows a policy owner and request owner to collaboratively determine whether the request satisfies the policy without the policy owner knowing the request and the request owner knowing the policy. They also use the efficient protocol called as Xhash, that is used for oblivious comparison, for allowing two parties where each party has a number, to compare whether they have same number without disclosing their numbers to each other.

III.PROPOSED ALGORITHM

Firewalls have been commonly implemented over the internet for securing individual network. A firewall checks each and every incoming and outgoing packet to decide whether to accept or discard them based upon its policy. Optimization of firewall policy is essential for improving network performance. It explores interfirewall optimization across various administrative domains for the first and foremost time. The challenge is that firewall policy cannot be disclosed over the different domains, because a firewall policy contains private information and even potential security holes, which can pave way to the attackers to launch attacks. In firewall the similarity join consist of grouping pairs of records whose similarities greater then a threshold, privacy preserving algorithm for similarity join are used to protect the data of two sources from being totally disclosed during the similarity join process.

3.1. Algorithm Overview

My proposed algorithm is "Redundancy Removal algorithm", which is mainly used for reducing the redundant rule in the firewall with multi-rule coverage. This involves semi-honest computation between two firewalls by preserving privacy of the each party firewall policy. To avoid rule overhead and increase efficiency by firewall optimization. The steps involved for identifying the redundant rules are:

3.1.1. Identical Redundancy

The identical rules that is clearly redundant. All matching columns are identical. While the comments are different, the rule number and comments do not affect the behavior of the firewall matching.

3.1.2. Hidden rules

Hidden rules in firewall are the rules that can't be identified in the normal firewall policy or rules. The hidden rules can't check the packets and traffic from the un-trusted network. So initially we have to identify the hidden rules in the firewall.

3.1.3. Redundant rule

An inverse of hidden case is when a lower rule fully includes the higher rule criteria plus more. While the first rule will match some traffic, you can't get rid of the lower rule because the lower rule would not only match what the first rule matches, but will also match additional traffic.

V. ARCHITECTURAL DIAGRAM

Optimization of firewall policy is essential for improving network performance. It explores interfirewall optimization across various administrative domains for the first and foremost time. The challenge is that firewall policy cannot be disclosed over the different domains, because a firewall policy contains private information and even potential security holes, which can pave way to the attackers to launch attacks. In firewall the similarity join consist of grouping pairs of records whose similarities greater then a threshold, privacy preserving algorithm for similarity join are used to protect the data of two sources from being totally disclosed during the similarity join process.

Firewalls have been commonly implemented over the internet for securing individual network. A firewall checks each and every incoming and outgoing packet to decide whether to accept or discard them based upon its policy.

My proposed algorithm is "Redundancy Removal algorithm", which is mainly used for reducing the redundant rule in the firewall with multi-rule coverage. This involves semi-honest computation between two firewalls by preserving privacy of the each party firewall policy. To avoid rule overhead and increase efficiency by firewall optimization.

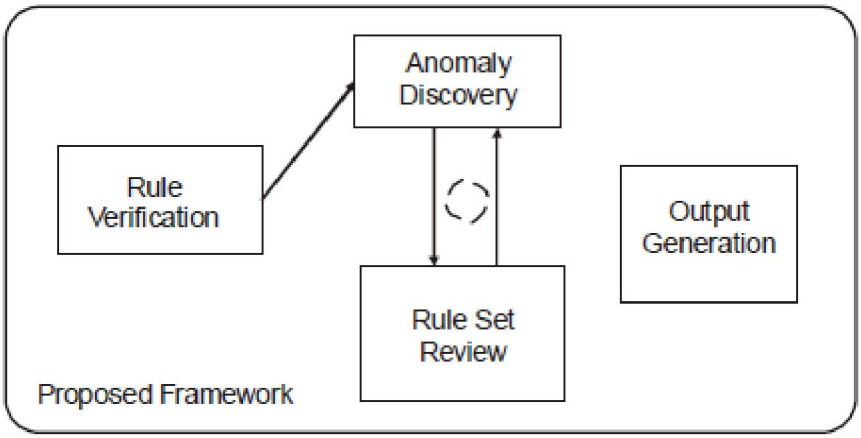

Figure2.Firewall proposed rule set review mechanism

VI. CONCLUSION

To identify an important problem of cross-domain privacy-preserving interfirewall redundancy detection. Implement the protocol in java and conducting extensive evolution. The result of the real firewall policies shows that, the protocol can remove as many of the redundant rules. This protocol is mainly applicable for identifying the interfirewall redundancy of firewall with a few thousands of rules. However it is still expensive to compare two firewall with many thousands of rules. Reducing complexity of the protocol is needs to be further studies. Demonstrate the rule optimization, from FW_1 to FW_2, and note that a similar rule optimization is possible in the opposite direction, i.e., FW_2 to FW_1.

In the first scenario, FW_1 toFW_2, it is FW_1 that is improving the performance load of FW_2, and in return FW_2 is improving the performance of FW_1 in a vice-versa manner. All this is being achieved without FW_1 or FW_2 reveling each other's policies thus allowing for a proper administrative separation. This protocol is most beneficial if both parties are willing to benefit from it and can collaborate in a mutual manner. There are many special cases that could be explored based on the current protocol. For example, there may be host or Network Address Translator (NAT) device between two adjacent firewalls. The current protocol cannot be directly applied to such cases. Extending our protocol to these cases could be an interesting topic and requires further investigation.

REFERENCES

[1] nf-HiPAC, "Firewall throughput test," 2012 [Online]. Available: http:// www.hipac.org/performance_tests/results.html
[2] R. Agrawal, A. Evfimievski, and R. Srikant, "Information sharing across private databases," in*Proc. ACM SIGMOD*, 2003, pp. 86–97.
[3] E.Al-Shaer and H. Hamed, "Discovery of policy anomalies in distributed firewalls," in *Proc. IEEE INFOCOM*, 2004, pp. 2605–2616.
[4] J.Brickell and V. Shmatikov, "Privacy-preserving graph algorithms in the semi-honest model," in *Proc. ASIACRYPT*, 2010, pp. 236–252.
[5] Y.-K. Chang, "Fast binary and multiway prefix searches for packet forwarding," *Comput. Netw.*, vol. 51, no. 3, pp. 588–605, 2007.
[6] 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.
[7] Q. Dong, S. Banerjee, J. Wang, D. Agrawal, and A. Shukla, "Packet classifiers in ternary CAMs can be smaller," in *Proc. ACM SIGMETRICS*, 2006, pp. 311–322.
[8] O.Goldreich, "Secure multi-party computations," Working draft, Ver. 1.4, 2002.
[9] O.Goldreich, *Foundations of Cryptography: Volume II (Basic Applications)*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[10] M. G. Gouda and A. X. Liu, "Firewall design: Consistency, completeness and compactness," in *Proc. IEEE ICDCS*, 2004, pp. 320–327.
[11] M. G. Gouda and A. X. Liu, "Structured firewall design," *Comput. Netw.*, vol. 51, no. 4, pp. 1106–1120, 2007.
[12] P. Gupta, "Algorithms for routing lookups and packet classification," Ph.D. dissertation, Stanford Univ., Stanford, CA, 2000.
[13] A. X. Liu and F. Chen, "Collaborative enforcement of firewall policies in virtual private networks," in *Proc. ACM PODC*, 2008, pp. 95–104.
[14] A. X. Liu and M. G. Gouda, "Diverse firewall design," *IEEE Trans. Parallel Distrib. Syst.*, vol. 19, no. 8, pp. 1237 1251, Sep. 2008.

