ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

A Survey On: Privacy Ensuring Optimization Protocol for Cross-Domain Firewalls to Improve the Network Performance

Trupti V Inamdar, Prof R. M. Goudar

Student, MITAOE, Pune University, India.

Associate Professor, MITAOE, Pune University, India.

ABSTRACT: Firewalls have become the most essential part that is deployed on the Internet for protecting the private networks. Optimizing firewall rules is very critical for enhancing the performance of a network. The early work on firewall optimization focuses on either intra-firewall or inter-firewall optimization within one administrative domain where the privacy of firewall policies is not a concern. The main technical challenge to focused on is that firewall policies cannot be disclosed across domains because a firewall policy contains secret information and even potential security holes, which can be easily utilized by attackers. Proposed work involves first the protocol for preserving firewall policies and optimizing them. Particularly, for any two adjacent firewalls that belongs to two different administrative domains, this protocol can identify the rules in each firewall that can be removed because of the other firewall. This process of optimization involves computation between the two firewalls without any party disclosing their policies to the other. The communication cost is reduced by the optimization process. This protocol sustains no extra online packet processing overhead, and also the offline processing time is less.

KEYWORDS: Firewall optimization, Privacy, Redundancy, Security, IP Networks

I.INTRODUCTION

Firewalls are widely used by various institutions, organizations, personal network etc. So, securing firewalls has become a need which will in turn provide the security to the network. In this world of internet, firewalls are settled at the entry point of a private network which provides a secure access to and from the network. This means that it will check each and every packet coming to the network or packet which is going from the network. According to the policies designed network will accept or discard the packets. Designing the policies means designing the sequence of rules and based on this rules firewall will perform its functions. We call these set of rules as access control list(ACL). This list is organized in rule table. Each rule has condition on packet header fields and has decision whether to accept or deny the packet. When packet comes to system according to first match of rule in the policies decision will be taken. The number of rules in the firewall significantly affects the throughput of the network. Also with the drastic growth of various services that are deployed on the internet, the size of the firewall policies growing rapidly. Therefore, it is the need to optimize the firewall policies to improve the network performance.

Previous work on firewall optimization shows only the intra-firewall optimization [2], [3] or inter-firewall optimization. And this was observed within one administrative domain where the secracy of firewall policies is not taken into consideration. Intra-firewall optimization means optimizing a single firewall for minimizing the policies. It is achieved by either removing the redundant rules[3], or rewriting the rules[2], [4], [5]. Previous work on inter-firewall optimization needs two firewall policies without any protection provided for privacy and therefore it can only be used within a single administrative domain. But in real, it is common that two firewalls belonging to separate administrative domains cannot share their policies with each other. Keeping the confidentiality of such a firewall policies is important because a firewall policy may be associated with the security holes that are easily utilized by the attackers. This is happened for a reason that most of the firewalls are misconfigured. Another reason why confidentiality is important is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

that, a firewall policy often contain a secret information e.g. IP address of server which can be misused by attackers to launch more precise attacks.

II. SURVEY ON FIREWALL OPTIMIZATION

A. Cross-Domain Firewall Optimization

Roaming user uses tunnels for keeping privacy of communication for example virtual private networks, but this traffic is not properly checked and controlled by foreign network firewall due to its encrypted nature. Because of this various attacks may happen. To prevent these two methods can be used in first, users release their network to foreign network and in second case this network may release firewall rules to tunnel end. But practical implementation of these two methods is not possible. The Proposed solution gives us a cross domain co-operative firewall in virtual private networks applies firewall policies to virtual private networks tunnel which is encrypted with keeping security of remote network's firewall policies. They actually distribute firewall's primitive rules across network and their result shows that this technique protects outside network from ciphered tunnels. By using same techniques as above Alex X. Liu Fei Chen, proposed us a new technique to remove redundant rules present in interfirewall without knowing each other's policies. They proposed a type of protection framework in which they work collaboratively and enforce the firewall policies. This solution is better than proposed Cross Domain Cooperative Firewall (CDCF) because, the encryption technique used in CDFC is slower than three magnitude order proposed by Alex X. Liu Fei,Linear searching of packet processing takes more time than using firewall decision diagrams. So this technique is better than previous one.

As all previous work give focus on optimizing inter-firewall or optimizing intra-firewall in one administrative domain without considering privacy metrics of the policies. Intra firewall optimization works on single firewall in which we can achieve firewall optimization either by redundancy removal or by rewriting of these redundant rules. But working on this basis requires one firewall reveal its policies with others or one firewall should know another firewall's policies. But in practical it is not possible firewall present in different domains not share anything. As firewall contains security hole keeping firewall policies confident is very important. So, Fei Chen, BezawadaBruhadeshwar, and Alex X. Liu [1] proposed a cross domain optimization technique with privacy preserving in cooperative environment. To achieve this two techniques are proposed in first they gave a novel approach and designed a protocol which detect inter-firewall redundancy removal in one firewall, and in second part they focused on removing of redundant rules. But while designing this protocol they consider threat model that they consider two firewalls are semi honest. They first convert each firewall into non overlapping rule sequence. After this they work on range comparison for privacy preservation. In next step they detect single rule redundancy and multi rule redundancy detection and at last they remove the redundancy in firewall. This technique is applicable to few thousands of rules up to 2000 rules redundancy get removed and preserving the firewall privacy is the main issue because none of the two firewalls need to tell the policies. In this research they show the firewall optimization from one firewall to second firewall and reverse direction is also possible. Fei Chen, BezawadaBruhadeshwar, and Alex X. Liu, got the tremendous results after evaluating this protocol. They evaluate this Protocol to get good efficiency on real and synthetic firewall. They conducted evaluation on five group of firewall. Each will examine the five important fields like source IP address, destination IP address, source and destination port address, source and destination protocol. The number of rules ranges from one to many and for to do encryption they have used Pohling-Hellman algorithm [1]. The Protocol proposed is efficient for processing and comparing real and synthetic firewall. Also it is efficient for communication cost happen between real and synthetic firewall. In this way the privacy of rules is preseved and also optimization of firewall in two different administrative domains is to be done.

III. PROPOSED WORK

A. Firewall Redundancy Removal

The previous work on removal of intrafirewall redundancy focused on detecting redundant rules withing a single firewall [3]. The knowledge of two firewall policies is required for removing redundancies, therefore that is applicable to only single administrative domain. The proposed system focuses on the optimization of firewalls from different domains.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

B. System Model

A Firewall is an ordered list of rules, each has the predicate over the fields and decision for the packetthat matches the predicate. Usually five fields are checked by the firewall, source IP address, destination IP address, source port address, destination port address and protocol type. The firewall decisions typically include accept, discard, accept with logging and discard with logging. The proposed work focuses on accept and discard rules of firewall.

C. Privacy-Preserving Inter-firewall Redundancy Removal

The proposed privacy preserving protocol for detecting inter-firewall redundant rules in firewall two with respect to the firewall one. For doing this the conversion of each firewall to an equivalent sequence of non-overlapping rules, because non-overlapping rules set equal to the matching rule set.

PROPOSED SYSTEM ARCHITECTURE

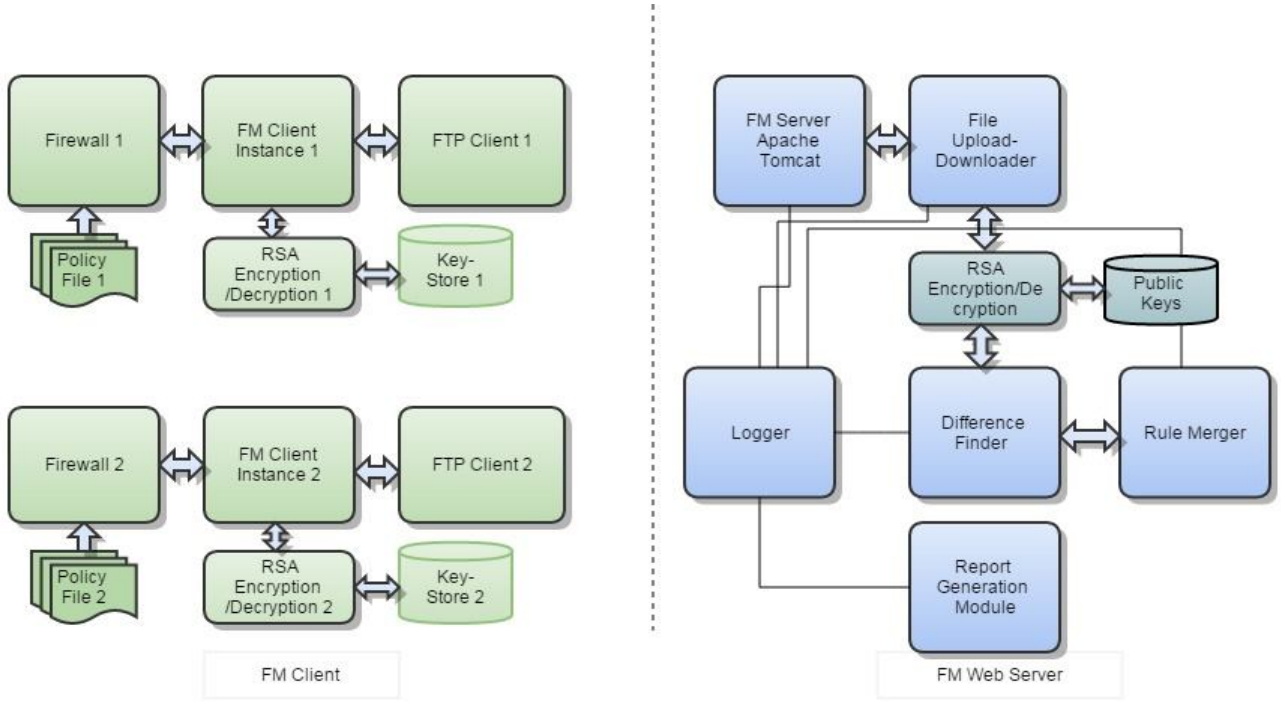

Fig.Architecture of Firewall Optimization

Fig. shows the system architecture for proposed work. The firewall policy file which contains various rules for accepting the packets is identified and security is provided by using the encryption techniques for secure transmission[6]. Redundant rules are identified and updated. This processing of firewalls is done for both the firewalls from different domains. And updated firewall policies are defined by optimizing them.

V.CONCLUSION AND FUTURE SCOPE

In this paper, we identified and studied the problems occurred while detecting the redundancies for preserving the firewall policies. The proposed protocol preserves the privacy by detecting and removing such a redundancies. To keep secrecy of private rules encryption technique is used in both one administrative domain and in two different administrative domains. Optimization of firewall can be done by using removing redundancies in rule or by rewriting the rules. In the proposed work rule optimization is demonstrated from one firewall to another and vice-versa, that improves the load performance of both the firewalls. The proposed system reduces the communication cost and processing overhead.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

REFERENCES

1. Fei Chen; Bruhadeshwar, B.; Liu, A.X., "Cross-Domain Privacy-Preserving Cooperative Firewall Optimization," *Networking, IEEE/ACM Transactions on* , vol.21, no.3, pp.857,868, June 2013.
2. Q. Dong, S. Banerjee, J. Wang, D. Agrawal, and A. Shukla. Packet classifiers in ternary CAMs can be smaller. In *ACM SIGMETRICS*,pages 311–322, 2006.
3. Liu, A.X.; Gouda, M.G., "Complete Redundancy Removal for Packet Classifiers in TCAMs," *Parallel and Distributed Systems, IEEE Transactions on* , vol.21, no.4, pp.424,437, April 2010.
4. Meiners, C.R.; Liu, A.X.; Torng, E., "TCAM Razor: A Systematic Approach Towards Minimizing Packet Classifiers in TCAMs," *Network Protocols, 2007. ICNP 2007. IEEE International Conference on* , vol., no., pp.266,275, 16-19 Oct. 2007.
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. K. H. D. R. Safford and D. L. Schales. Secure RPC authentication(SRA) for TELNET and FTP. Techn. Rep., 1993.
7. S. Singh, F. Baboescu, G. Varghese, and J. Wang. Packet classification using multidimensional cutting. In *ACM SIGCOMM*, 2003.
8. Acharya, S.; Wang, J.; ZihuiGe; Znati, T.F.; Greenberg, Albert, "Traffic-Aware Firewall Optimization Strategies," *Communications, 2006. ICC '06. IEEE International Conference on* , vol.5, no., pp.2225,2230, June 2006.
9. Shaer and H. Hamed, "Firewall policy advisor for anomaly detection and rule editing," in Proc. Integrated Management (IM), 2003.
10. Jerry Cheng, Hao Yang, Starsky H.Y. Wong, PetrosZergos, Songwu Lu, “Design and Implementation of Cross-Domain Firewalls.”,2007, IEEE.
11. Shaer and H. Hamed, "Discovery of policy anomalies in distributed firewalls," in Proc. IEEE INFOCOM, 2004.
12. S. loannidis, A. Keromytis, S. Bellovin, and J. Smith, "Implementing adistributed firewall," in Proc. ACM CCS, 2000.
13. J. Lee, J. Jeon, and K. Yoo, "A security scheme for protecting securitypolicies in firewall," SIGOPS Operating System Review, vol. 38, no. 2,pp. 69-72, 2004.
14. P. Gupta and N. McKeown, "Algorithms for packet classification," IEEENetwork, vol. 15, no. 2, pp. 24-32, 2001.
15. B. Hore, S. Mehrotra, and G. Tsudik, "A privacy-preserving index forrange queries," in Proc. VLDB, 2004.