International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Review: Firewall Privacy Preservation By Packet Filtering Management

Akshay Dattatray Kachare[1], Geeta Atkar[2]

[1]M.E.Computer Network Student, GHRCEM Wagholi, University of Pune, India

[2]Assistant Professor in Computer Engineering Department, GHRCEM Wagholi, University of Pune, India

Abstract: ***Firewalls are fundamental elements in Internet network security. A firewall always identifies every incoming or outgoing packets and takes decision of whether to accept or discard that packet. This decision of firewall is based on its policy. A firewall is nothing but a security protector sited at the point of entry among a private web and also the outdoor network such that entire incoming and outgoing packets must pass through it. Though there is firewall rules management, mainly in multi-firewall enterprise network the management system has become a difficult and complex task. Previous search on firewall optimization concentrates on intra-firewall and inter-firewall optimization within some administrative domain in which the privacy of firewall policies is not a concern. Filtering rules of firewall have to be written, well-ordered and dispersed with care so as to avoid firewall policy anomalies which may cause vulnerability of network. Hence, inserting or updating filtering rules in any firewall needs detailed intra-firewall and inter-firewall analysis to decide the appropriate rule assignment and ordering in the firewalls. Most of firewall rules on the Internet are not well designed and they also have various errors. Hence, in what way one can structure firewall policies appropriately is a significant problem. In the comparison stage, the subsequent multiple versions are compared with each other to detect total functional inconsistencies between them.***

Keywords: Firewall security, Inter-firewall, Intra-firewall optimization.

1. Introduction

1.1. Firewall Optimization

By means of the worldwide Internet connection, security of network has increased vital attention in research study and industrial communities [3]. Because of the increasing threat of the network attacks, the firewalls have come to be significant fundamentals not just in enterprise networks but as well in small-size and household networks. Firewalls have been the limit protection for protected networks in contradiction of attacks and illegal traffic by filtering out network traffic coming from or going to the secured network which might unwanted. The filtering choice is based on ordered filtering rules set which is defined rendering to previously defined security policy necessities [3].

Firewalls are key components in the case of internet security, and it have been extensively deployed in most businesses and enterprises for security of private networks. A firewall is located at the idea of entrance among a private internet network and also outside network such as all incoming and outgoing packets have to permit over it. The firewall functionality is used to observed each and every incoming or outgoing packet and also choose whether to accept or discard that packet. A packet can be observed as a tuple by means of a limited number of fields like source and destination Internet Protocol (IP) address, source and destination port number, and protocol type [1].

Though a firewall policy is a simple order of rules, appropriately designing one is, by not any means, simple. The rules represented in a firewall policy are logically tangled because of conflicts between these rules and the subsequent order sensitivity [25]. Arranging the rules appropriately in a firewall is critical yet problematic. The inference of several rules in a firewall cannot be understood appropriately deprived of observing all the rules scheduled beyond that rule. Moreover, a firewall policy may comprise of an enormous number of rules. A firewall on the network may contain of hundreds or even a few thousand rules in exciting cases. Some can imagine the difficulty of the logic underlying numerous conflicting rules [8].

For the reason that the conflicts and edict sensitivity of firewall rules, firewall designing directly as an order of rules travels from three problems: (1) Consistency problem, (2) Completeness problem, and (3) Compactness problem [6]. These problems can be elaborated as: Firstly, Consistency Problem is problematic to make sequence of the rules in a firewall correctly. The consistency problem mainly originates from conflicts between rules. For the reason that rules often conflict, the rules order in a firewall is complex. The conclusion for each packet is the conclusion of the first rule with which that packet matches. Secondly, Completeness Problem is problematic to guarantee that overall possible packets are take into consideration. To make sure that every single packet has at least single matching rule in a firewall, the mutual preparation is to create the prediction of the last rule a tautology. This sees that it is not a good way to confirm the detailed consideration of overall possible packets. And at last, Compactness Problem: An unwell designed firewall a lot has redundant rules. A rule in firewall called as redundant if eliminating the rule does not change the firewall functionality, which means there is no any impact of rule on firewall for every packet [6].

Firewall is precise only when its policy is correct and a firewall policy is correct only when it satisfies given constraint specification of that policy, which is frequently

inscribed in a natural language [8].

Even though the firewall technology deployment is a significant phase toward securing networks, the complexity of managing firewall policies might limit the effectiveness of firewall security. In a single firewall environment, the local policy of firewall may consist of intra-firewall anomalies, where the matching packet could match extra than one filtering rule. Furthermore, in dispersed firewall environments, firewalls could also have inter-firewall anomalies when distinct firewalls in the similar perform dissimilar filtering actions on the equivalent traffic. Hence, the administrator must need to give much attention not only to total rule relations in the similar firewall so as to determine the precise rule order, nonetheless to all relations between rules in distinct firewalls in order to determine the suitable rule placement in the suitable firewall. The difficulty of addition of a new rule or updating an existing one significantly increases, as the number of filtering rules increases. It is probably same, in this case, to make known to conflicting rules like one common rule following another specific rule, or any other correlated rules whose relative ordering defines various actions for the similar packet. Moreover, a particular large-scale enterprise network may include hundreds of rules that might be inscribed by distinct administrators in many times. This significantly improves the potential regarding occurrence of anomaly in the firewall policy, risking the security of the private network. Thus, the efficiency of firewall security is reliant on provided that policy management methods and tools that can be used by network administrators for purify, analyze and verify the accuracy of inscribed firewall filtering rules.

2. Literature Reviews

2.1 Firewall Optimization

A firewall policy is generally definite as an order of rules, known as Access Control List (ACL), and every rule has a prediction above multiple header fields of packet. These fields like source and destination IP, source and destination port, and type of protocol (TCP, UDP etc.) and accept or reject decision for the packets that equal the predicate. The rules in a firewall policy normally follow the first-match semantics where the choice for a packet is the decision of the principal rule that the packet equals in the policy [base paper]. To kept firewall policies confidential is much important for two causes. (1) A firewall policy could have security holes that might abused by attackers. Quantitative lessons have exposed that utmost firewalls are misconfigured and have security holes [10]. (2) A firewall policy usually consists personal information, e.g., the IP addresses of servers, which can be used by attackers to introduction more precise and targeted attacks.

Various models have been projected for filtering rules. For optimization of packet classification, an ordered binary decision diagram is used as a model from [3]. Additional model by means of tuple space is developed in [3], which combines a collection of filters in one tuple kept in a hash table. The model described in [26] uses bucket filters indexed by search trees. Multi-dimensional binary tries are also used to model filters [27].

Previous research on intra-firewall redundancy elimination objects to identify redundant rules inside an only firewall [11], [9]. Author called Gupta identified forward and backward redundant rules in a firewall policy. Later, Liu et al. addressed that the redundant rules recognized by author Gupta are not complete, and Liu et al. proposed two different methods for identifying all redundant rules [9], [11]. Previous research on inter-firewall redundancy elimination requires the information of two firewall policies and hence is single applicable within single administrative domain [3], [12]. Collaborative firewall implementation in virtual private networks (VPNs) goals to implement firewall policies above encrypted VPN tunnels deprived of leaking the privacy of the policy of remote network, [7]. The issues of collaborative firewall implementation in VPNs and privacy-preserving inter-firewall optimization are basically dissimilar.

2.2 Inter-Firewall Optimization

Previous study on inter-firewall optimization needs two different firewall policies deprived of any privacy protection, and hence can only be used within single administrative domain. Though, in actuality, it is mutual that two firewalls belong to various administrative domains where the firewall policies can't be shared with every other [5], [13], [14], [15], [16], and [17]. A rule is followed when a preceding rule matches all the packets which are match this rule, like as the followed rule will not ever be activated. Following is a critical error in the policy, as the followed rule not ever takes effect. This can cause an accepted traffic to be congested or a denied traffic to be acceptable. Consequently, as overall guideline, if there is a comprehensive or precise match correlation between two rules, the superset (or usual) rule must come after the subsection (or specific) rule. It is very significant to determine followed rules and alert the administrator to precise this error by rearranging or eliminating these rules. In Correlation anomaly the two rules are related to each other if they have distinct filtering actions, and also the first rule matches certain packets that equal the second rule besides the second rule equals some packets that equal the first rule [3]. In generalization anomaly a rule is a generalization of a previous rule if they have dissimilar actions, and if the first rule can equal all the packets that equal the second rule [3]. In Redundancy anomaly a redundant rule does the similar action on the identical packets as additional rule such as if the redundant rule is detached; the security of policy will not be affected. In irrelevance anomaly a filtering rule in a firewall is unrelated if this rule can't match several traffic that may flow over this firewall. This occurs when together the source address and the destination address fields of the rule do not equal any domain reachable over this firewall. In other disputes, the path in between the source address and destination addresses of this rule doesn't pass through the firewall. Therefore, this rule has unaffected on the filtering outcome of this firewall.

2.3 Intra-Firewall Optimization

Intra-firewall optimization is nothing but optimizing an only firewall. It is accomplished by either eliminating redundant rules [15], [17] or modifying rules [5], [13], [14], [15], [16], [17]. An intra-firewall policy anomaly is addressed as the presence of two or more filtering rules that may match the similar packet or the presence of a rule that cannot ever match some packet on the network tracks that cross the firewall [18]. The gathering of filtering rules in a central firewall policy is actual vital in defining the filtering policy in this firewall. This is since the packet filtering process is achieved by successively matching the packet in contradiction of filtering rules till at least one match is found. If filtering rules are separate, the gathering of the rules is unimportant. Though, it is actual common to have filtering rules that are inter-related. In this situation, if the comparative rule ordering is not judiciously assigned, certain rules may be continuously screened by additional rules creating an incorrect policy. Furthermore, when the policy comprises a large number of filtering rules, the likelihood of writing contradictory or redundant rules is comparatively high.

3. Firewall Privacy Preservation

Firewall security, such as any new technology, needs correct management so as to provide correct security services. Thus, just consuming firewalls on the network boundaries or among sub-domains cannot essentially make the network several secure. One purpose of this is the complexity of handling firewall rules and the resultant network vulnerability due to rule anomalies. Authors of paper [4] follows an extended tradition of investigation on privacy-preserving algorithms in the so called Secure Multiparty Computation (SMC) paradigm. Casually, security of a protocol in the SMC paradigm is definite as computational indistinguishability from certain supreme functionality, in which an important third party accepts its inputs and carries out the calculation. Some polynomial-time multi-party calculation can be complete in a privacy preserving way using general techniques [4].

Even though firewall security has been specified strong consideration in the research community, the emphasis was typically on the filtering presentation issues [4]. Instead, rare related study attempt to report solitary one of the conflict issues which is the rule corresponding relationship in filtering policies. Other methods [19], [20], and [21] recommend using a high-level policy linguistic to describe and analyze firewall policies and before plan this language to filtering rules. Though using such high-level languages may avoid rule anomalies, they are not applied for the greatest widely used firewalls that consists low-level filtering rules. The Privacy-preserving algorithms for precise issues such as calculation of estimates, sales, set matching and connection [23], surveys [22], calculation of the k-th ordered element and particularly data mining difficulties such as privacy-preserving calculation of decision trees, classification of consumer data [24], and mining of perpendicularly divided data.

4. Cross-domain Inter-firewall Optimization

Paper [1] emphases on cross-domain privacy-preserving inter-firewall optimization. This paper signifies the first step in discovering this unidentified space. Precisely, the focus is on elimination of inter-firewall policy redundancies in a privacy-preserving method. The crucial challenge is to project a protocol that lets two neighboring firewalls to recognize the inter-firewall redundancy with regard to each other deprived of knowing the policy of the other firewall. Though intra-firewall redundancy elimination is already more complex [11], [9], inter-firewall redundancy elimination with the privacy-preserving need is even problematic. He protocol defined in this paper applies to both stateful and stateless firewalls. The core change between stateful and stateless firewalls is that the stateful firewalls keep a connection table upon acceptance a packet, if it belongs to an established connection; it is automatically accepted without examining against the rules. Consuming the connection table or not does not affect the represented protocol. In this paper authors adopt the semi-honest model which is elaborated. For two neighboring firewalls, assumption is that they are semi-honest, which means, each firewall surveys the protocol properly but every firewall might try to disclose the policy of the supplementary firewall. The semi-honest model is realistic and also well adopted [4].

5. Conclusion

In this survey, overall identification an important problem, privacy-preserving inter-firewall and intra-firewall redundancy detection. In this paper, there officially defined a number of firewall policy anomalies in together centralized and dispersed firewalls. Then presented a set of algorithms are used to detect rule anomalies included a single firewall (intra-firewall anomalies), and in between inter-connected firewalls (inter-firewall anomalies) in the internet network. Once an anomaly is discovered, users are encouraged with appropriate corrective actions. The future research plan comprises implementation optimization of intra-firewall and inter-firewall anomaly detection, online automatic detection and recovery of anomalies created as a consequence of the rule editing.

References

[1] Fei Chen, Bezawada Bruhadeshwar, Alex X. Liu, “A Cross-Domain Privacy-Preserving Protocol for Cooperative Firewall Optimization”, 2011
[2] R. Agrawal, A. Evfimievski, and R. Srikant. Information sharing across private databases”, 2003.
[3] E. Al-Shaer and H. Hamed. Discovery of policy anomalies in distributed firewalls”, 2004.
[4] J. Brickell and V. Shmatikov. Privacy-preserving graph algorithms in the semi-honest model”, 2010.
[5] Q. Dong, S. Banerjee, J. Wang, D. Agrawal, and A. Shukla. Packet classifiers in ternary CAMs can be smaller”, 2006.
[6] M. G. Gouda and A. X. Liu. Structured firewall design”, Computer Networks Journal (Elsevier), 2007.

[7] A. X. Liu and F. Chen. Collaborative enforcement of firewall policies in virtual private networks", 2008.
[8] A. X. Liu and M. G. Gouda. Diverse firewall design", 2008.
[9] A. X. Liu, C. R. Meiners, and Y. Zhou. All-match based complete redundancy removal for packet classifiers in TCAMs", 2008.
[10] A. Wool. A quantitative study of firewall configuration errors", 2004.
[11] A. X. Liu and M. G. Gouda. Complete redundancy removal for packet classifiers in tcams. IEEE TPDS, in press.
[12] L. Yuan, H. Chen, J. Mai, C.-N. Chuah, Z. Su, and P. Mohapatra.cFireman: a toolkit for firewall modeling and analysis", 2006.
[13] A. X. Liu, C. R. Meiners, and E. Torng. Tcam razor: A systematic approach towards minimizing packet classifiers in tcams. IEEE/ACM Trans. on Networking, in press.
[14] A. X. Liu, E. Torng, and C. Meiners. Firewall compressor: An algorithm for minimizing firewall policies", 2008.
[15] C. R. Meiners, A. X. Liu, and E. Torng. TCAM Razor: A systematic approach towards minimizing packet classifiers in TCAMs", 2007.
[16] C. R. Meiners, A. X. Liu, and E. Torng. Bit weaving: A non-prefix approach to compressing packet classifiers in TCAMs", 2009.
[17] C. R. Meiners, A. X. Liu, and E. Torng. Topological transformation approaches to optimizing tcam-based packet processing systems", 2009.
[18] E. Al-Shaer and H. Hamed. "Firewall Policy Advisor for Anomaly Detection and Rule Editing", Integrated Management Conference, 2003.
[19] W. Du, Y. Han, and S. Chen. Privacy-preserving multivariate statistical analysis: linear regression and classification", In Proc. 4th SIAM International Conference on Data Mining (SDM), 2004.
[20] A. Evfimievski, R. Srikant, R. Agrawal, and J. Gehrke. Privacy preserving mining of association rules", Information Systems, 2004.
[21] M. Kantarcioglu, J. Jin, and C. Clifton. When do data mining results violate privacy?", In Proc. 10th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD) , 2004.
[22] J. Feigenbaum, B. Pinkas, R. Ryger, and F. Saint-Jean. Secure computation of surveys", In Proc. EU Workshop on Secure Multiparty Protocols, 2004.
[23] M. Freedman, K. Nissim, and B. Pinkas. Efficient private matching and set intersection", In Proc. Advances in Cryptology, 2004.
[24] Z. Yang, S. Zhong, and R. Wright. Privacy-preserving classification of customer data without loss of accuracy", In Proc. 5th SIAM International Conference on Data Mining (SDM), 2005.
[25] A. Wool, "A Quantitative Study of Firewall Configuration Errors," Computer, 2004.
[26] T. Woo. "A Modular Approach to Packet Classification: Algorithms and Results", 2000.
[27] L. Qiu, G. Varghese, and S. Suri. "Fast Firewall Implementations for Software and Hardware-based Routers." Proceedings of 9th International Conference on Network Protocols, 2001.

Authors Profile

Akshay Kachare received the B.E. degree in Computer Science and Engineering from Satara College of Engineering, Shivaji University and currently student of the second year M.E. in Computer Network from GH Raisoni College of Engineering and Management, Wagholi, University of Pune.

Prof. Geeta Atkar working as Asst. Professor in Computer Engineering department in GH Raisoni College of Engineering and Management, Wagholi, University of Pune.