ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com

International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

Inter-Firewall Optimization across various Administrative Domains for Enabling Security and Privacy Preserving

[1]G.Suresh, [2]P.C.Rohit Chandar, [3]M.Vinoth Kumar, [4]K.Valliappan
[1]sureshwisdomedu@gmail.com, [2]pcrohitchandar10@gmail.com, [3]jevisus@gmail.com,
[4]valliappankrish94@gmail.com
[1]Assistant Professor, [2,3,4] UG Scholars
[1,2,3,4] Vel Tech High Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai

ABSTRACT: Network securityis usually protected by a firewall, which checks both incoming and outgoing packets against a set of defined policies or rules. Hence, the overall performance of the firewall generally depends on its rule management. The performance can be decreased when there are firewall rule anomalies occurred. 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 intra-firewall or inter-firewall optimization within one administrative domain where the privacy of the firewall policies is not a concern. To explore Inter-firewall optimization across various administrative domains for the first time. The key technical challenge is that firewall policies cannot be shared across domains and the encrypted form of policies can be shared using cooperative encryption technique. Because a firewall policy contains confidential information and even potential security holes, which can be exploited by attackers. Inter-firewall redundant rule overcome the prior problem and enable the Inter-firewall optimization across administrative domains using redundancy removal algorithm. Also propose the first cross-domain cooperative firewall (CDCF) policy optimization protocol. The optimization process involves cooperative computation between the two firewalls without any party disclosing its policy to the other.

Keywords-Interfirewall optimization, different administrative domain, Redundancy Removal algorithm.

I. INTRODUCTION:

Firewalls have been widely deployed on the Internet for securing private networks. A firewall checks each incoming or outgoing packet to decide whether to accept or discard the packet based on its policy. Optimizing firewall policies is crucial for improving network performance. Prior 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.

This concept explores inter-firewall optimization across administrative domains for the first time. The key technical challenge is that firewall policies cannot be shared across domains because a firewall policy contains confidential information and even potential security holes, which can be exploited by attackers. In this concept, propose the first cross-domain privacy-preserving cooperative firewall policy optimization protocol. Specifically, for any two adjacent firewalls belonging to two different administrative domains, this protocol can identify in each firewall the rules that can be removed because of the other firewall.

The optimization process involves cooperative computation to the two firewalls without any party disclosing its policy to the other. This concept implemented that protocol and conducted extensive experiments. The results on real firewall policies show that our protocol can remove as many as 49% of the rules in a firewall whereas the average is 19.4%. The communication cost is less than a few hundred KBs. This protocol incurs no extra online packet processing

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

overhead and the offline processing time is less than a few hundred seconds.

II. RELATED WORK

The prior work on firewall optimization focuses on either intra-firewall optimization, or inter-firewall optimization within one administrative domain where the privacy of firewall policies is not a concern.Firewall policy management is a challenging task due to the complexity and interdependency of policy rules. This is further exacerbated by the continuous evolution of network and system environments.

The process of configuring a firewall is tedious and error prone. Therefore, effective mechanisms and tools for policy management are crucial to the success of firewalls. Existing policy analysis tools, such as Firewall Policy Advisor and FIREMAN, with the goal of detecting policy anomalies have been introduced. Firewall Policy Advisor only has the capability of detecting pair wise anomalies in firewall rules. FIREMAN can detect anomalies among multiple rules by analyzing the relationships concept one rule and the collections of packet spaces derived from all preceding rules.

FIREMAN also has limitations in detecting anomalies. For each firewall rule, FIREMAN only examines all preceding rules but ignores all subsequent rules when performing anomaly analysis. In addition, each analysis result from FIREMAN can only show that there is a misconfiguration concept one rule and its preceding rules, but cannot accurately indicate all rules involved in an anomaly.

Network Firewall is now considered as a first line of defense in the form of a barrier against outside attacks, which is installed on computers connect to internet. In general, Firewall prevents the dangers of Internet from spreading to your internal network. It more like a moat of a medieval castle that a firewall in a modern building. It serves multiple purposes.

In practice, a firewall is a collection of hosts, routers, and other hardware that designed to prevent unauthorized electronic access between two parts of a network. It is also a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria.

2.1. Discovery of Policy Anomalies in Distributed Firewall

Firewalls are core elements in network security. Managing firewall rules, particularly in multi-firewall enterprise networks, has become a complex and error-prone task. Firewall security, like any other technology, requires proper management in order to provide proper security services. Thus, just having firewalls on the network boundaries or Sub-domains may not necessarily make the network any secure. One reason of this is the complexity of managing firewall rules and the resulting network vulnerability due to rule anomalies. The Firewall Policy Advisor presented in this concept provides a number of techniques for purifying and protecting the firewall policy from rule anomalies. The administrator may use the firewall policy advisor to manage legacy firewall policies without prior analysis of filtering rules. In this concept,

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

formally defined a number of firewall policy anomalies in both centralized and distributed firewalls and concept proved that these are the only conflicts that could exist in firewall policies. Concept then presented a set of algorithms to detect rule anomalies within a single firewall (intra-firewall anomalies), and betconcepten inter-connected firewalls (inter-firewall anomalies) in the network. When an anomaly is detected, users are prompted with proper corrective actions. Concept intentionally made the tool not to automatically correct the discovered anomaly but rather alarm the user because concept believes that the administrator should have the final call on policy changes. Finally, concept presented a user-friendly Java-based implementation of Firewall Policy Advisor.With the global Internet connection, network security has gained significant attention in research and industrial communities.Due to the increasing threat of network attacks, firewalls have become important elements not only in enterprise networks but also in small-size and home networks.

2.2.Privacy-Preserving Graph Algorithms in the Semi-honest Model

A related problem is how to construct privacy-preserving protocols for graph comparison. Many of these problems (*e.g.*, comparison of the graphs' respective maximum flow values) reduce to the problem of privacy-preserving comparison of two values, and thus have reasonably efficient generic solutions. For other problems, such as graph isomorphism, there are no known polynomial-time algorithms even if privacy is not a concern. Investigation of other interesting graph algorithms that can be computed in a privacy-preserving manner is a topic of future research.

In this technique, Investigate scenarios with two mutually distrustful parties, each in possession of a graph (representing, *e.g.*, a network topology, a distribution channel map, or a social network). The parties wish to compute some algorithm on their combinedgraph, but do not wish to reveal anything about their private graphs beyond that which will be necessarily revealed by the output of the algorithm in question. For example, consider two Internet providers who are contemplating a merger and wish to see how efficient the resulting joint network would be without revealing the details of their existing networks; or two transportation companies trying to determine who has the greatest capacity to ship goods between a given pair of cities without revealing what that capacity is or which distribution channels contribute to it; or two social networking websites wishing to calculate aggregate statistics such as degrees of separation and average number of acquaintances without compromising privacy of their users, and so on. In this paper, construct privacy-preserving versions of classic graph algorithms for APSD (all pairs shortest distance) and SSSD (single source shortest distance). Our algorithm for APSD is new, while the SSSD algorithm is a privacy preserving transformation of the standard Dijkstra's algorithm show that minimum spanning trees can be easily computed in a privacy-preserving manner. As one of our tools, develop protocols for privacy-preserving set union, which are results of independent interest.

2.3. Design and Implementation of Cross-Domain Cooperative Firewall

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

Cross-Domain Cooperative Firewallarchitecture that can enable the collaborative security in terms of joint traffic filtering without exposing much of the shared information. The novelty of CDCF is the distribution of the firewall primitives of rule matching and verdict enforcement, as concept as the enabling technique of efficient oblivious comparison through commutative cipher and a novel range comparison technique. Our prototype implementation and experimental results have shown that CDCF can readily be deployed to greatly enhance the mobile network security at marginal cost.

Security and privacy are two major concerns in supporting roaming users across administrative domains. Nowadays many organizations have deployed Virtual Private Networks (VPNs) to protect their users when they roam into foreign networks. Once a roaming user establishes a VPN tunnel with her home network, she can access not only the private resources within the home network, but also redirect her Internet traffic through the VPN tunnel, which is typically encrypted to protect the secrecy of the user traffic. While roaming users enjoy the security protection offered by VPNs, little consideration has been given to the impact of such encrypted tunnels on the foreign network. In particular, the foreign network's firewall cannot effectively regulate such tunneled traffic, because it is unable to examine the encrypted connection properties, such as destination IP addresses and ports. As a result, certain connections that are normally prohibited by the foreign network, for either security or policy reasons, can now circumvent the firewall regulation. The existence of such unregulated tunnels not only weakens the security protection for the roaming users, but more importantly leaves the foreign network widely open to various security threats from the public Internet. At first glance, this problem may be alleviated by having the roaming user expose her decrypted traffic to the foreign network. Alternatively, the foreign network could also publish its firewall rules for the roaming user to self-regulate her traffic at the tunnel endpoint. However, neither approach is desirable in practice due to privacy concerns. On one hand, it is unlikely that users are willing to reveal their traffic (or their decryption keys) to the foreign network, which is exactly the motivation for deploying VPNs in the first place. On the other hand, network administrators are also reluctant to publish the firewall rules in use, which can expose sensitive information about the internal network topology and the administrative policies. With these conflicting security and privacy requirements, it is very difficult to regulate the encrypted tunnels using conventional firewall techniques, because they all require a single entity to possess knowledge on both the connection characteristics and he firewall rules.

III. PROBLEM STATEMENT

The prior work on firewall optimization focuses on either intrafirewall or interfirewall optimization within one administrative domain where the privacy of firewall policies is not a concern. This paper explores interfirewall optimization across administrative domains for the first time. The key technical challenge is that firewall policies cannot be shared across domains because a firewall policy

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

contains confidential information and even potential security holes, which can be exploited by attackers. This paper, propose the first cross-domain privacy-preserving cooperative firewall policy optimization protocol. Specifically, for any two adjacent firewalls belonging to two different administrative domains, our protocol can identify in each firewall the rules that can be removed because of the other firewall. The optimization process involves cooperative computation between the two firewalls without any party disclosing its policy to the other.

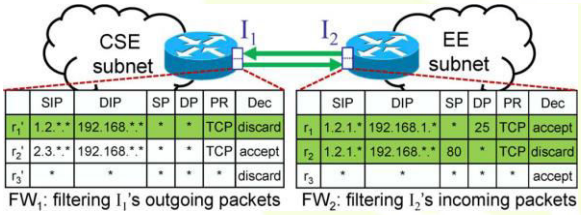

Fig. 3.1. Example interfirewall redundant rules.

IV. PROPOSED WORK

The proposed work is torepresents a novel anomaly management framework for firewalls based on a rule-based segmentation technique to facilitate not only more accurate anomaly detection but also effective anomaly resolution.

Based on this technique, a network packet space defined by a firewall policy can be divided into a set of disjoint packet space segments. Each segment associated with a unique set of firewall rules accurately indicates an overlap relation (either conflicting or redundant) among those rules.

This concept also introduces a flexible conflict resolution method to enable a fine-grained conflict resolution with the help of several effective resolution strategies with respect to the risk assessment of protected networks and the intention of policy definition.

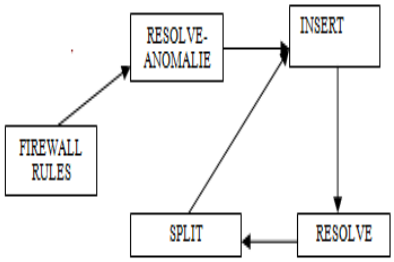

Fig. 4.1.Cooperative firewall optimization architecture

V. CONCLUSION

Identify an important problem of cross-domain privacy-preserving inter firewall redundancy detection. The proposed algorithm is redundancy removal algorithm for detecting such redundancy. This algorithm is implemented in Java and conducted extensive evaluation.An important problem of cross-domain privacy-preserving interfirewall redundancy detection, the concept proposes a novel privacy-preserving protocol for detecting such redundancy. The results on real firewall policies show that this protocol can remove as many of the rules in a firewall. Reducing the complexity of protocol needs to be further studied. In this work, also demonstrated rule optimization from the private network, and note that a similar rule optimization is possible in the opposite direction. The first scenario is to improving the performance of the firewall by removing the redundant rules and also improving the performance of network.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology Ecology Science and Technology (IJARBEST)
Vol. I, Special Issue I, August 2015 in association with VEL TECH HIGH TECH DR. RANGARAJAN DR. SAKUNTHALA ENGINEERING COLLEGE, CHENNAI
National Conference on Recent Technologies for Sustainable Development 2015 [RECHZIG'15] - 28th August 2015

VI. REFERENCE

[1] Alex, X . Liu, Fei Chen," Privacy Preserving Collaborative Enforcement of Firewall Policies in Virtual Private Networks", Issue No.05 - May (2011 vol.22) pp: 887-895.

[2] Alex, X. Liu, E. Torng, and C. Meiners, "Firewall compressor: An algorithm for minimizing firewall policies," in *Proc. IEEE INFOCOM*, 2008.

[3] Alex, X. Liu, E. Torng, and C. Meiners, "Firewall compressor: An algorithm for minimizing firewall policies," in *Proc. IEEE INFOCOM*, 2008.

[4] Al-Shaer and H. Hamed, "Discovery of policy anomalies in distributed firewalls," in *Proc. IEEE INFOCOM*, 2004, pp. 2605–2616.

[5] Brickell and V. Shmatikov, "Privacy-preserving graph algorithms in the semi-honest model," in *Proc. ASIACRYPT*, 2010, pp. 236–252.

[6] 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] 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] Gouda and A. X. Liu, "Firewall design: Consistency, completeness and compactness," in *Proc. IEEE ICDCS*, 2004, pp. 320–327.

[9] P.R.Kadam, V.K. Bhusari ," Review On Redundancy Removal Of Rules For Optimizing Firewall", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308 1 .

[10] Liu A.X and F. Chen, "Collaborative enforcement of firewall policies in virtual networks," in *Proc. ACM PODC*, 2008, pp. 95–104.

[11] Liu, C. R. Meiners, and E. Torng, "TCAM Razor: A systematic approach towards minimizingpacket classifiers in TCAMs," *IEEE/ACM Trans. Netw.*, vol. 18, no. 2, pp.490–500, Apr. 2010.

[12] MungoleMukupa," Firewall Rule set Optimization".

[13] RupaliChaure and Shishir K. Shandilya," Firewall anamolies detection and removal techniques",International Journal on Emerging Technologies 1(1): 71-74(2010) ISSN : 0975-8364.

[14] Simi Mathew and J. Bhavithra," Traffic Aware Privacy Preserving Firewall Policies", Bonfring International Journal of Software Engineering and Soft Computing Online ISSN: 2277-5099.