International Journal of Science Engineering and Advance Technology

To Provide An Innovative Policy Anomaly Management Framework For Firewalls

[1] Subha Sree Mallela, [2] M M Bala Krishna, [3] KTV Subba Rao
1 23 Department of Computer Science And Engineering
Akula Sree Ramulu Institute of Engineering and Technology, Prathipadu, Tadepalligudem, A.P, India
[1]subhasree.mallela@gmail.com, [2] balu_522@yahhoo.co.in, [3]ogidi@rediffmail.com

Abstract- Firewalls have been widely organized on the Internet for securing private networks. A firewall checks each incoming or outgoing packet to choose whether to accept or discard the packet based on its policy. Optimizing firewall policies is vital for improving network performance. In this paper we 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 recognize 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. Firewalls are significant in securing private networks of businesses, institutions and home networks. A firewall is frequently placed at the entry between a private network and the external network so that it can ensure each incoming or outgoing packet and choose whether to accept or abandon the packet based on its policy. A firewall policy is typically specified as a sequence of rules called Access Control List (ACL) and each rule has a predicate over multiple packet header fields i.e., source IP, destination IP, source port, destination port, and protocol type and a decision i.e., accept and discard for the packets that counterpart the predicate. In this paper we recommend the first cross-domain privacy-preserving cooperative firewall policy optimization protocol.

Keywords: Firewall optimization, privacy.

INTRODUCTION:

Purposely for any two adjacent firewalls be in the right place to two different administrative domains our protocol can spot in each firewall the rules that can be removed because of the other firewall. The optimization process engages helpful computation between the two firewalls without any party disclosing its policy to the other. We applied our 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 fewer than a few hundred kilobytes. Our protocol invites no extra online packet processing overhead and the offline processing time is less than a few hundred seconds. The rules in a firewall policy typically follow the first-match semantics where the decision for a packet is the choice of the first rule that the packet matches in the policy. Each physical interface of a router/firewall is configured with two ACLs. One is for filtering outgoing packets and the other one for filtering incoming packets. In this paper we use firewalls, firewall policies and *ACLs* interchangeably. This paper searches inter firewall optimization across administrative domains for the first time. The key technological confront is that firewall policies cannot be shared across domains since a firewall policy surrounds private information and even potential security holes which can be exploited by attackers.

RELATED WORK:

Preceding work on combined firewall enforcement in VPNs enforces firewall policies over encrypted VPN tunnels devoid of leaking the privacy of the remote network's policy. The problems of collaborative firewall enforcement in VPNs and privacy-preserving inter firewall optimization are basically dissimilar. The former focuses on implementing a firewall policy over VPN tunnels in a privacy preserving manner while the latter focuses on removing inter firewall redundant rules with no revealing their policies to each other. The former preserves the privacy of the remote network's policy whereas the latter conserve the privacy of both policies. The semi-honest model is sensible and well adopted. For example this representation is proper for large organizations that have many sovereign branches as well as for insecurely connected agreements composed by multiple parties. While we are secure that all managerial domains follow permission protocols. Also it may be probable for one party to issue a sequence of inputs to try and reveal the other party's policy. For this attack to be successful some

ISSN 2321-6905

suppositions have to be satisfied one of them being that one firewall's policy remain constant.

EXISTING SYSTEM:

Prior work on firewall optimization focuses on either intrafirewall optimization or interfirewall optimization within one organizational 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. Firewall Policy Advisor only has the ability of detecting pair wise anomalies in firewall rules. FIREMAN can detect anomalies among multiple rules by analyzing the relationships between one rule and the collections of packet spaces derived from all preceding rules.

DISADVANTAGES:

The number of rules in a firewall considerably affects its throughput. Fireman can detect anomalies among multiple rules by analyzing the relationships between one rule and the collections of packet spaces derived from all preceding rules. For each firewall rule, FIREMAN only examines all preceding rules but ignores all subsequent rules when performing anomaly analysis.

PROPOSED SYSTEM:

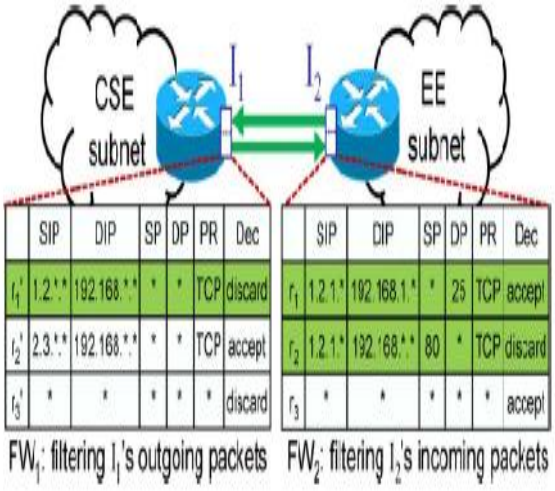
A novel anomaly management framework for firewalls based on a rule-based segmentation technique to ease not only more precise anomaly detection but also effectual anomaly resolution. A network packet space defined by a firewall policy can be divided into a set of disjoint packet space segments. We also introduce a flexible conflict resolution method to allow 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.

ADVANTAGES:

Each conflicting segment links with a policy conflict and a set of conflicting rules. Also the correlation relationships among conflicting segments are recognized and conflict correlation groups are derived. Policy conflicts belonging to different conflict correlation groups can be resolved separately thus the searching space for resolving conflicts is reduced by the correlation process.

INTERFIREWALL REDUNDANT RULES:

The effort confront is to plan a protocol that permit two adjacent firewalls to recognize the inter firewall redundancy with respect to each other without knowing the policy of the other firewall. As intra firewall redundancy removal is compound. Inter firewall severance removal with the privacy-preserving requirement is even harder. Our protocol applies to both statefull and stateless firewalls.



The main dissimilarity between statefull and stateless firewalls is that stateful firewalls uphold a connection table. Upon receiving a packet if it fits in to a recognized connection. It is automatically conventional without checking against the rules. Having the connection table or not does not affect our protocol.

CROSS – DOMAIN INTERFIREWALL OPTIMIZATION:

No previous work focuses on cross-domain privacy-preserving inter firewall optimization. This paper stands for the first step in discover this unknown space. Especially we focus on removing inter firewall policy redundancies in a privacy-preserving manner. Consider two adjacent firewalls 1 and 2 belonging to different managerial domains and NET1 and NET2. For ease we suppose that FW1 and FW2 have no intra firewall redundancy as such redundancy can be removed using the proposed solutions.

SINGLE-RULE COVERAGE REDUNDANCY DETECTION:

NET1 has a series of double encrypted none be related rules obtained from FW1 and d sets of double encrypted numbers obtained from FW2. As there may be manifold rules that please this condition ultimately NET1 connections a set of rule indices with. If no rule satisfies this condition NET1 associates an empty set with a. Upon receiving the sets from NET1, for each prefix family NET2 finds the directory of the rule that overlaps with the prefix family.

FIREWALL UPDATE AFTER OPTIMIZATION:

NET2 modifies the decisions of some rules in FW2. In this case neither party requirements to take actions because the inter firewall redundancy detection does

not think the decisions of the rules in FW2. NET1 adds or removes some rules in FW1. In this case since the decides sets of some rules in FW1 may change a rule in FW2 that used to be inter firewall laid off maybe not redundant any longer. It is significant for NET2 to run our optimization protocol again.

ENHANCEMENT:

- 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.
- Policy-Anomaly-Discovery Algorithm that takes a policy and utilizes the dependency data structure to find and eliminate anomalies returning a list of validated policy.
- algorithm has time complexity *O(n2 log n)*,
- Efficient in detection of anamoloies.
- 92 percent of conflicts can be resolved.
- The proposed system resolves conflicts in each conflict correlation group independently

SEGMENT GENERATION FOR NETWORK PACKET SPACE

Input: A set of rules, R.
Output: A set of packet space segments, S.

```
1  foreach r ∈ R do
2      s_r ⟵ PacketSpace(r);
3      foreach s ∈ S do
4          /* s_r is a subset of s*/
5          if s_r ⊂ s then
6              S.Append(s \ s_r);
7              s ⟵ s_r;
8              Break;
9          /* s_r is a superset of s*/
10         else if s_r ⊃ s then
11             s_r ⟵ s_r \ s;
12         /* s_r partially matches s*/
13         else if s_r ∩ s ≠ ∅ then
14             S.Append(s \ s_r);
15             s ⟵ s_r ∩ s;
16             s_r ⟵ s_r \ s;
17     S.Append(s_r);
18 return S;
```

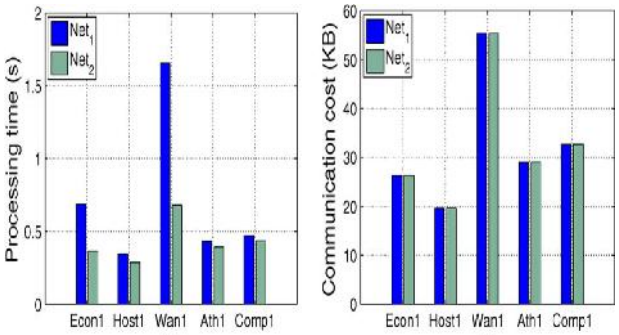
POLICY ANOMALY DISCOVERY

Input: A set P of rules $r_1, r_2, \ldots, r_n$
Output: A set $\grave{P}$ of ordered rules, and P of correlated rules

(* Orders rules according to their dependencies *)

1. construct graphs U and D;
2. set $\grave{P} \leftarrow \emptyset$;
3. **while** D contains terminal nodes
4. **for** every terminal node $v=(i, j) \in D$
5. **do** color v red;
6. **do** color link $e=(i, j) \in U$ red;
7. $\mathcal{C} \leftarrow$ Discover-Connected-Components(U);
8. **if** $\mathcal{C}$ doesn't contain new components
9. return "Rules conflict: ", P;
10. **while** $\mathcal{C} \neq \emptyset$
11. select node u randomly from $\mathcal{C}$;
12. set $\grave{P} \leftarrow \grave{P} \cup \{r_u\}$;
13. set $P \leftarrow P \setminus \{r_u\}$;
14. **return** $\grave{P}$;

EXPERIMENTAL RESULTS:



Processing FW1 on real firewalls. (a) Processing time. (b) Communication cost.

CONCLUSION:

The procedure is appropriate for identifying the inter firewall dismissal of firewalls with a few thousands of rules e.g. 2000 rules. However it is still costly to evaluate two firewalls with many thousands of rules e.g. 5000 rules. Reducing the difficulty of our protocol wants to be further studied. Our procedure is most helpful if both parties are willing to advantage from it and can work together in a mutual manner. There are many special cases that could be explored based on our current protocol. For example there may be hosts or Network Address Translation (NAT) devices between two adjacent firewalls. Our present

protocol cannot be directly applied to such cases. Expanding our protocol to these cases could be an interesting topic and requires further investigation. 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%.

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.

[15] A. X. Liu and M. G. Gouda, "Complete redundancy removal for packet classifiers in TCAMs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 4, pp. 424–437, Apr. 2010.

Authors:

Ms. M. Subha Sree is a student of Akula Sriraamulu Institute of Technology, Tadepalligudem. Presently she is pursuing her M.Tech CSE from this college and she received her B.Tech from DMSSVH College of Engineering, affiliated to Nagarjuna University, Guntur in the year 2008. Her area of interest includes Computer Networks and Object oriented Programming languages and Network Security.

Mr. M M Bala Krishna, excellent teacher Received M.Tech (CSE) and working as an Associate Professor and HOD, Department of CSE, M.Tech Computer science engineering , ASRIT college. He has 7 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences /journals . His area of Interest includes Data Warehouse and Data Mining, information security, flavors of Unix Operating systems and other advances in computer Applications.

Prof. K.T.V Subbarao, well known Author and teacher received M.Tech (CSE) and working as Principal, Akula SreeRamulu institute of Engineering and Technology, He is an active member of ISTE. He has 12 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences/journals. His area of interest includes cryptography and network security, Distributed databases, Operating systems and other advances in computer Applications.