International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 4 | ISSN : 2456-3307

Firewall Optimization using Cross-Domain Privacy-Preserving

S. Kiran Kumar
MCA Sri Padmavathi College of Computer Sciences And Technology Tiruchanoor,Tirupati, Andhra Pradesh, India

ABSTRACT

Firewalls are wide deployed on the internet for securing personal networks. A firewall checks every incoming or outgoing packet to make a decision whether or not to accept or discard the packet supported its policy. Optimizing firewall policies is crucial for rising network performance. previous work on firewall improvement focuses on either intrafirewall or interfirewall improvement inside one body domain wherever the privacy of firewall policies isn't a priority. In existing, formally specifies the resource sharing mechanism between 2 totally different tenants within the presence of our projected cloud resource mediation service. The correctness of permission activation and delegation mechanism among totally different tenants using four distinct algorithms (Activation, Delegation,Forward Revocation and Backward Revocation) is additionally incontestable exploitation formal verification. we propose the primary cross-domain privacy-preserving cooperative firewall policy improvement protocol. Specifically, for any 2 adjacent firewalls happiness to 2 totally different body domains, our protocol will determine in every firewall the foundations which will be removed because of the opposite firewall. The optimization method involves cooperative computation between the 2 firewalls with none party revealing its policy to the opposite. we enforced our protocol and conducted in depth experiments. The results on real firewall policies show that our protocol will take away as several as forty ninth of the foundations in a very firewall, whereas the typical is nineteen.4%. The communication value is a smaller amount than many hundred kilobytes. Our protocol incurs no further on-line packet process overhead, and the offline interval is a smaller amount than many hundred seconds.

Keywords: Optimizing firewall, cross-domain privacy-preserving

I. INTRODUCTION

Background and Motivation

Firewalls are critical in securing private networks of businesses, 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 or 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 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 match the predicate. The rules in a firewall policy typically follow the first-match semantics, where the decision for a packet is the decision of the first rule that the packet matches in the policy. Each physical interface of a router/firewall is configured with two ACLs: one for filtering outgoing packets and the other one for filtering incoming packets. In this paper, we use firewalls, firewall policies, and ACLs, interchangeably. The number of rules in a firewall significantly affects its throughput.

II. ALGORITHM

CROSS DOMAIN INTER-FIREWALL OPTIMIZATION

Firewall works on both inter-firewall and Intra firewall domains. Prior work focuses on both these domains but only within single network. It is necessary to provide security as the firewall policy contains private and confidential information.

Let us consider two firewall policies F1 and F2 which belong to different administrative domains D1 and D2 and we need to detect inter-firewall redundant rules for these two domains. A firewall policy consists of a collection of rules in which each rule has a predicate and a decision for the packets that are equivalent to the predicate. Based on defined rule r, firewall checks each incoming and outgoing packets among these domains. The protocol contains source IP, destination IP, source and destination ports and protocol type. The protocol type defines the acceptance or denial of the packet. First convert each firewall F1, F2 into non overlapping rules. Validate the equivalent set of non-overlapping rules (nr) with resolving set i.e. M (nr) = R (nr). Here verify if the non-overlapping rule nr in F2 fulfills the non-overlapping discarding rule in F1 and also check for the multiple non overlapping discarding rules. It is also needed to check Privacy-Preserving Range Comparison.

OPTIMIZE THE PROTOCOL USED TO MINIMIZE THE FIREWALL POLICIES

Our system will overcome the drawback of existing system. It has advent features which are easily accessing, managing, detecting, rearranging and resolving the firewall rules in the rule engine. It is a beneficial for Administrator and service providers. The existing approach eliminates the redundant rules but at the cost of increased processing and communication time. We thus propose to optimize the protocol using following approach:

1. Encrypt the data sent from home network N1 to other business network N2.
2. Compress the data received from N1 using Huffman data compression algorithm.
3. FW1 will send this data to FW2
4. Data will be decompressed and further decrypted at N2
5. Duplicate rules will be removed in between the two networks.

Encryption and decryption will be done using Pohlig-Hellman algorithm as follows:

Enc (M, K) = MK mod P

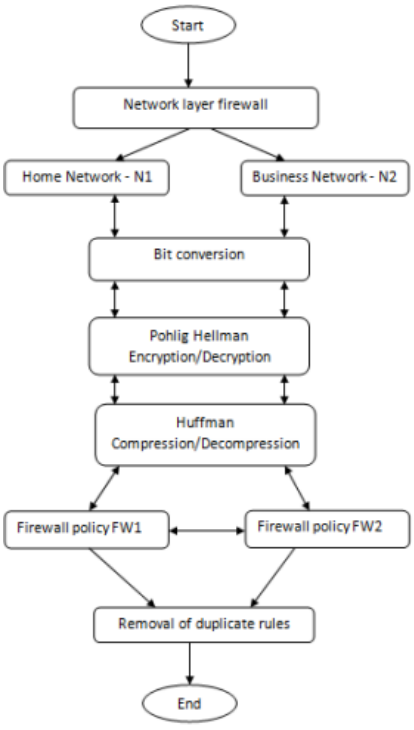
Where M is the message, K is the key and P is a large prime modulus.

While compression and decompression will be done through Huffman encoding and decoding mechanism as follows:-

A. Input

1. Packet data in byte format B ={b1,b2,b3,…bn}

Set P = { p1, p2, ...,pn } which is set of probability of Occurrence of data in a firewall rule i.e. Pi = P (Bi), 1<= i<= n where n is the max no of packets



Fligure 1. Data flow chart of two administrative domains

B. Output

Code C (B, P) = { c1,c2 , ...,cn } is binary keyword set of code words where ci is the code word for ai,1 <=i<= n

C. Goal Let L(C) = $\sum_{i=1}^{n} P_i \times$ length (Ci) be the weighted path length of code C with condition L(C) <= L(T) for any code T(B,P) In order to achieve security and increased response and processing time. These data packets in network can either be sent from FW1 to FW2 and vice versa.

III. CONCLUSION

In this paper, we known a crucial downside, cross domain privacy preserving interfirewall redundancy detection. we propose a completely unique privacy preserving protocol for detective work such redundancy. we enforced our protocol in Java and conducted in depth analysis. The results on real firewall policies show that our protocol will take away as several as forty ninth of the principles during a firewall whereas the common is 19.4%.

IV. REFERENCES

[1]. 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.

[2]. 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.

[3]. O. Goldreich, "Secure multi-party computations," Working draft, Ver. 1.4, 2002.

[4]. O. Goldreich, Foundations of Cryptography: Volume II (Basic Applications). Cambridge, U.K.: Cambridge Univ. Press, 2004.

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

[6]. M. G. Gouda and A. X. Liu, "Structured firewall design," Comput. Netw., vol. 51, no. 4, pp. 1106–1120, 2007.

[7]. P. Gupta, "Algorithms for routing lookups and packet classification," Ph.D. dissertation, Stanford Univ., Stanford, CA, 2000.

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

[9]. A. X. Liu and M. G. Gouda, "Diverse firewall design," IEEE Trans. Parallel Distrib. Syst., vol. 19, no. 8, pp. 1237–1251, Sep. 2008.

[10]. 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.

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

[12]. A. X. Liu, C. R. Meiners, and Y. Zhou, "All-match based complete redundancy removal for packet classifiers in TCAMs," in Proc. IEEE INFOCOM, 2008, pp. 574–582.

[13]. Lin, Y., Malik, S.U., Bilal, K., Yang, Q., Wang, Y. and Khan, S.U., 2016. Designing and Modeling of Covert Channels in Operating Systems. IEEE Transactions on Computers, 65(6), pp.1706-1719.

[14]. Liu, J. K., Au, M. H., Huang, X., Lu, R., and Li, J., 2016. Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services. IEEE Transactions on Information Forensics and Security, 11(3), (pp. 484-497).

[15]. Liu, X., Deng, R. H., Choo, K.-K. R. and Weng, J., 2016. An Efficient Privacy-Preserving Outsourced Calculation Toolkit With Multiple Keys. IEEE Transactions on Information Forensics and Security, 11(11), pp. 2401-2414.

[16]. Ma, K., Zhang, W. and Tang, Z., 2014. Toward Fine-grained Data-level Access Control Model

for Multi-tenant Applications. International Journal of Grid and Distributed Computing, 7(2), pp.79-88.

[17]. Murata, T., 1989. Petri nets: Properties, analysis and applications. Proceedings of the IEEE, 77(4), pp.541-580.

[18]. Sayler, A., Keller, E. and Grunwald, D., 2013. Jobber: Automating inter-tenant trust in the cloud. In Presented as part of the 5th USENIX Workshop on Hot Topics in Cloud Computing.

[19]. C. R. Meiners, A. X. Liu, and E. Torng, "TCAM Razor: A systematic approach towards minimizing packet classifiers in TCAMs," in Proc. IEEE ICNP, 2007, pp. 266–275.

[20]. C. R. Meiners, A. X. Liu, and E. Torng, "Bit weaving: A non-prefix approach to compressing packet classifiers in TCAMs," in Proc. IEEE ICNP, 2009, pp. 93–102.

Author's Profile:

Mr. Sunku Kiran Kumar has received his graduation degree in BSc. Bachelor of Science from Sri Chandra Reddy Degree College, Affiliated to SV University, Tirupati . At Present he is Pursuing Post graduate degree MCA, Master of Computer Applications from Sri Padmavathi College of Computer Sciences and Technology Affiliated to Sri Venkateswara University , Tirupati,AP,India.