International Journal of Communication Networks and Security

Volume 2 | Issue 3 Article 12

January 2014

"FAME": FSPYING & SOLVING FIREWALL ANOMALIES

B LAKSHIMIBHARGAVI
MITS, MADANAPALLE ,A.P,India, 10691f0019@gmail.com

V MARUTI PRASAD
MITS, MADANAPALLE,A.P,India, maruti_vv@yahoo.co.in

Recommended Citation

LAKSHIMIBHARGAVI, B and MARUTI PRASAD, V (2014) ""FAME": FSPYING & SOLVING FIREWALL ANOMALIES," *International Journal of Communication Networks and Security*: Vol. 2 : Iss. 3 , Article 12.
DOI: 10.47893/IJCNS.2014.1098
Available at: https://www.interscience.in/ijcns/vol2/iss3/12

"FAME": ESPYING & SOLVING FIREWALL ANOMALIES

B. LAKSHIMIBHARGAVI[1], V. MARUTHI PRASAD[2]

[1]Final Year, MITS, MADANAPALLE, A.P
[2]Asst. Professor, MITS, Madanapalle, A.P
E-mail:10691f0019@gmail.com, maruthi_vv@yahoo.co.in

Absract- Advent of many emerging computing technologies became very catchy to users. So, usage of technology increasing very rapidly day by day. Security became major issue. People who are working through the internet suffer from unintended security leakages by unauthorised actions in an organization and also problems created by hackers through the malicious codes. To overcome the security issues we have a concept called "firewall" .Network firewalls guard an internal computer network (home, school, business intranet) against malicious access from the outside. Network firewalls may also be configured to limit access to the outside from internal users. In this paper, we elaborate FAME(firewall anomaly management environment) and we will have a glance on firewall anomalies and resolving techniques. In addition we are going explain few concepts practically and also representing diagrammatically.

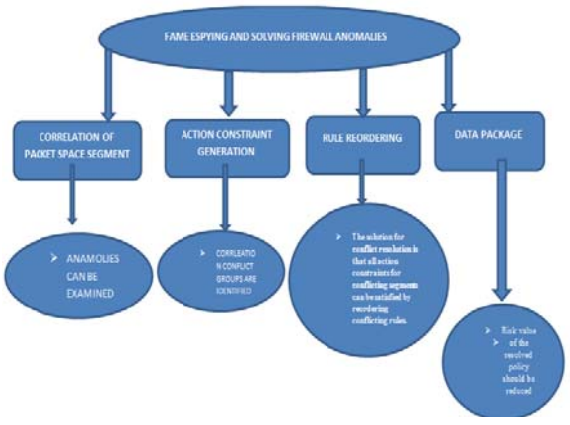
Index Terms- *Fame, firewall,malicious code, internal user,anomalies.*

I. INTRODUCTION

Firewall plays a pivot role in providing security from un authenticated users. Based upon the security rules firewall examines all the incoming and outgoing packets. managing the firewall policy is very crucial due to complexity of policy rules. As we know firewall vendors regularly release new software versions of there products. In addition, more attention is now being paid to firewall rule-set quality, due to regulations such as the Sarbanes-Oxley Act5 and the CobiT framework (www.isaca.org/cobit), the Payment-Card Industry Data Security Standard (www.pcisecuritystandards. org), and the US National Institute of Standards and Technology standard 800-41.6 All these regulations include specific section dealing with firewall configuration, management, and audit.though the firewall policy is recommended it has its own security flaws now in this paper we are going to espy that flaws which are occurred in the firewall policy and trying to resolve them.Hongxin Hu, Student Member, IEEE, Gail-JoonAhn, Senior Member, IEEE, and KetanKulkarni," Detecting and Resolving Firewall Policy Anomalies".Inorder to espying the firewall policy anomalies we have a concept called "fireman" because fireman only examines all preceding rules but ignores all subsequent rules when doing analysis. One more concept called firewall policy advisor only has the capability of detecting pairwise ananomalies. Wecant change the rules as we want.With the global Internet connection, network security hasgained significant attention in research and industrial communities.Due to the increasing threat of network attacks, fireshave becomeimportant elements not only in enterprisenetworks but also in small-size and home networks. Firewalls have been the frontier defence for secure networks againstattacks and unauthorized traffic by filtering out unwantednetwork traffic coming from or going to the secured network.The filteringdecision is based on a set of ordered filtering rulesdefined according to predefined security policy requirements.We can see the firewall setup from the below figure.

Rule	Protocal	Source IP	Dest IP	Desti Port	Action
R1	udp	10.1.2.8	172.32.1.*	53	Deny
R2	Udp	10.1.*.*	172.32.1.*	53	Deny
R3	Tcp	10.1.*.*	192.168.*.*	25	Allow
R4	Tcp	10.1.*	192.168.1.*	25	Deny
R5	Udp	10.1.3.*	182.176.2.*	23	allow

An example for centralized firewall setup.



Overview:

- In the overview of FAME: Espying & Solving Firewall Anomalies we have four modules mainly.
- These four modules are defined for different purposes. Each and every module has its unique identity.

- In the first module i.e correlation of packet space segment all the anomalies can be examined.
- In the second module i.e action constraint generation all the correlation groups are going to be identified. And also risk assessments for conflicts are performed.
- In the third module i.e rule reordering, the solution for conflict resolution is that action constraints for conflicting segments can be satisfied by reordering conflicting rules.
- In the fourth module i.e data package ,risk value for the resolved policy is reduced.

2. ANOMALY REPRESENTATION

1. Correlation of Packet Space Segment
2. Action Constraint Generation
3. Rule Reordering
4. Data Package

2.1 Correlation of Packet Space Segment:
The major benefit of generating correlation groups for the anomaly analysis is that anomalies can be examined within each group independently, because all correlation groups are independent of each other. Especially, the searching space for reordering conflicting rules in conflict resolution can be significantly lessened and the efficiency of resolving conflicts can be greatly improved.

2.2 Action Constraint Generation:
In a firewall policy are discovered and conflict correlation groups are identified, the risk assessment for conflicts is performed. The risk levels of conflicts are in turn utilized for both automated and manual strategy selections. A basic idea of automated strategy selection is that a risk level of a conflicting segment is used to directly determine the expected action taken for the network packets in the conflicting segment. If the risk level is very high, the expected action should deny packets considering the protection of network perimeters

2.3 Rule Reordering:
The solution for conflict resolution is that all action constraints for conflicting segments can be satisfied by reordering conflicting rules. In conflicting rules in order that satisfies all action constraints, this order must be the optimal solution for the conflict resolution.

2.4 Data Package:
When conflicts in a policy are resolved, the risk value of the resolved policy should be reduced and the availability of protected network should be improved comparing with the situation prior to conflict resolution based on the threshold value data will be received in to the server.

3. ANOMALIES IN FIREWALL POLICIES

Two rules in a firewall policy may overlap, which means onepacket may match both rules. Moreover, two rules in a firewall mayconflict, implying that those two rules not only overlap each otherbut also take different actions. Policy conflicts may lead to bothsecurity problems (e.g. allowing malicious traffic) and availabilityproblems (e.g. denying legitimate traffic), and policy redundancieswill affect the performance of a firewall. A comprehensive classificationof policy anomalies (misconfigurations)has been articulatedby several related work [6, 29]. Following existing classification,we summarize policy anomalies as follows:

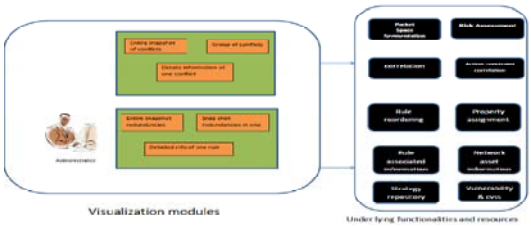
3.1Shadowing: A rule can be shadowed by one or a set of preceding rules that match all the packets which also match the shadowed rule, while they perform a different action. In this case, all the packets that one rule intends to deny (accept) can be accepted (denied) by previous rule(s); thus, the shadowed rule will never be taken effect. In Table 1, r4 is shadowed by r3 because r3 allows every TCP packet coming from any port of 10.1.1._ to the port 25 of 192.168.1._, which is supposed to be denied by r4.

3.2 Generalization: A rule is a generalization of one or a set of previous rules if a subset of the packets matched by this rule is also matched by the preceding rule(s) but taking a different action. Forexample, r5 is a generalization of r4 in Table 1. These two rules indicate that all the packets from 10.1.1._are allowed, except TCP packets from 10.1.1._ to the port 25 of 192.168.1._. Note that, as we discussed earlier, generalization might not be an error.

3.3 Correlation: One rule is correlated with other rules, if arule intersects with others but defines a different action. In this case, the packets matched by the intersection of those rules may be permitted by one rule, but denied by others. In Table 1, r2 correlates with r5, and all UDP packets coming from any port of10.1.1._ to the port 53 of 172.32.1._ match theintersection of these rules. Since r2 is a preceding rule of r5, every packet within the intersection of these rules is denied by r2. However, if their positions are swapped, the same packets will be allowed.

3.4 Redundancy: A rule is redundant if there is another same or more general rule available that has the same effect. For example, r1 is redundant with respect to r2in Table 1, since all UDP packets coming from any port of 10.1.2._ to the port 53 of 172.32.1._ matched with r1 can match r2 as well with the same action.

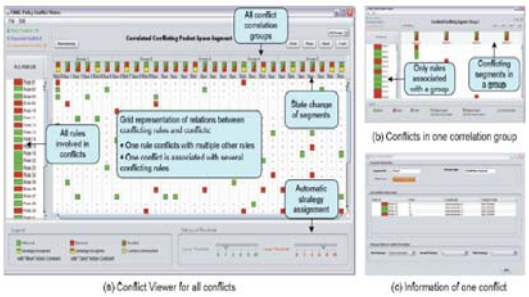
4. IMPLEMENTATION& EVALUATION



Our framework is realized as a proof-of-concept prototype called Firewall Anomaly Management Environment. Fig. 9 shows a high-level architecture of FAME with two levels.The upper level is the visualization layer, which visualizes the results of policy anomaly analysis to system administrators. Two visualization interfaces, policy conflict viewer and policy redundancy viewer, are designed to managepolicy conflicts and redundancies, respectively. The lowerlevel of the architecture provides underlying functionalitiesaddressed in our policy anomaly managementframework and relevant resources including rule information, strategy repository, network asset information, and vulnerability information.

Anomaly Management Framework:
Our policy anomaly management framework is composed oftwo core functionalities: conflict detection and resolution, andredundancy discovery and removal, as depicted in Fig. 3. Bothfunctionalities are based on the rule-based segmentationtechnique. For conflict detection and resolution, conflictingsegments are identified in the first step. Each conflictingsegment associates with a policy conflict and a set ofconflicting rules. Also, the correlation relationships amongconflicting segments are identified and conflict correlationgroups (CG) are derived. Policy conflicts belonging todifferent conflict correlation groups can be resolved separately;thus, the searching space for resolving conflicts isreduced by the correlation process. The second stepgenerates an action constraint for each conflicting segmentby examining the characteristics of each conflicting segment.

4.1.Detecting And Resolving Firewall Policy Anomalies



Evaluation of FAME:For FAME evaluation, we utilized a number of firewall policies and associated information required by our toolfrom different resources. Most of them are from campus networks and some are from major ISPs. Our experiments were performed on Intel Core 2 Duo CPU 3.00 GHz with 3.25 GB RAM running on Linux kernel 2.6.16.

To facilitate the correct interpretation of analysis results, a concise and intuitive representation method is necessary.For the purposes of brevity and understandability, we employ a two-dimensional geometric representation foreach packet space derived from firewall rules. Note that afirewall rule typically utilizes five fields to define the rule condition; thus, a complete representation of packet spaceshould be multidimensional. Fig. 1a gives the two-dimensionalgeometric representation of packet spaces derivedfrom the example policy shown in Table 1. We utilizecolored rectangles to denote two kinds of packet spaces:allowed space (white color) and denied space (graycolor),respectively. In this example, there are two allowed spaces representing rules r3 and r5, and three denied spacesdepicting rules r1, r2, and r4.

5. CONCLUSION

In this paper we find the firewall anomalies and We had given few methods that how to resolve the firewall anomalies, we had explain about "fame"And few techniques involved in it.A rule-based segmentation mechanism and a grid-based representation technique were introduced to achieve the goal of effectiveand efficient anomaly analysis. In addition, we have described a proof-of-concept implementation of our anomaly management environment called FAME and demonstrated that our proposed anomaly analysis methodology is practical and helpful for system administrators to enable an assurable network management.

REFERENCES

[1] IEEE transactions on dependable and secure computing, vol. 9, no. 3, may/june 2012. "Detecting and Resolving Firewall Policy Anomalies".

[2] E. Al-Shaer and H. Hamed, "Discovery of Policy Anomalies in Distributed Firewalls," IEEE INFOCOM '04, vol. 4, pp. 2605-2616, 2004.

[3] A. Wool, "Trends in Firewall Configuration Errors: Measurin the Holes in Swiss Cheese," IEEE Internet Computing, vol. 14, no. 4, pp. 58-65, July/Aug. 2010.

[4] J. Alfaro, N. Boulahia-Cuppens, and F. Cuppens, "Complete Analysis of Configuration Rules to Guarantee Reliable Network Security Policies," Int'l J. Information Security, vol. 7, no. 2, pp. 103- 122, 2008.

[5] F. Baboescu and G. Varghese, "Fast and Scalable Conflict Detection for Packet Classifiers," Computer Networks, vol. 42, no. 6, pp. 717-735, 2003.

[6] L. Yuan, H. Chen, J. Mai, C. Chuah, Z. Su, P. Mohapatra, and C. Davis, "Fireman: A Toolkit for Firewall Modeling and Analysis," Proc. IEEE Symp. Security and Privacy, p. 15, 2006.