Cross-Domain Search for Policy Anomalies in Firewall

G.Vanikalyani
M.Tech (CSE)
Gudlavalleru Engg college
Gudlavalleru

P.Avinash
Assistant Professor (CSE)
Gudlavalleru Engg College
Gudlavalleru

P.Pandarinath, PhD
Professor (CSE)
AKRG Engineering College
Tadepalligudem

ABSTRACT
Most of the business services have been performing very effectively by using some of the evolving technologies like cloud computing and other architectures etc. But still they have been suffering from security problems due to the undesired actions in their services. So, in this situation firewalls can plays a vital role. Firewalls can ensure the security of private networks in organizations by providing some of the security related mechanisms. So, in this paper major and latest developments have been made in anomaly management framework which works on a rule-based segmentation technique for correct detection of anomalies [1] and for the effective anomaly resolution and this can also be extended to the other types of policies

Keywords: Anomalies, Firewall Policy, Security

1. INTRODUCTION
The migration of security threats had become a necessary action for networks. The increasing trend of target network attacks has not been decreasing down. Most of the company networks are especially in danger. This malicious breach of security may be a serious business problem. Internet usage has been increasing now-a-days and its attention drawn towards the research and business communities'. Generally to provide security to the internet is a challenging task to the most of the administrators. Firewalls can act like barriers for the most of the enterprise and business networks from the any type of attacks. A Firewall is a software device which is used to filter and to control the traffic as shown in the Figure 1. The firewall decision is based on a set of filtering rules which can be specified in the form of Access control policies (ACP). However the designing and managing of these policies can be crucial due to the improper policy management techniques and the tools. However the managing of these policy rules especially in the single and multifirewall environments is also crucial. So, properly configuring the firewall policies based on technique for the anomaly problem may have an idea to develop the correct algorithm to reconfigure the firewalls. The goal is to have an algorithm which can withstand with any type of attack.

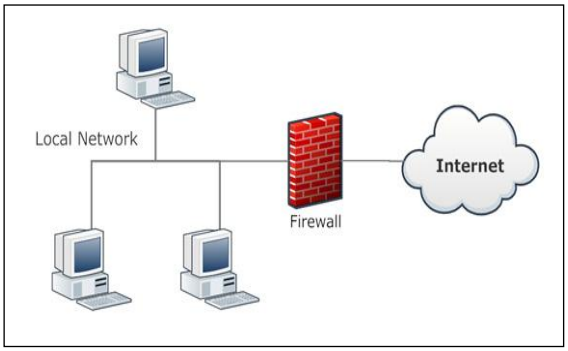


Figure 1. An Example Firewall

A firewall is software or a hardware system that prevents malicious and unauthorized access from a network. Firewalls are used to filter and to control the traffic from the unwanted Internet users from accessing their networks connected to the Internet. The firewall can check each and every data of its criteria that have been set by the specified firewall. Another use of the firewall is to protect against unauthenticated logins from the outside world. This helps to prevent the threats on our network. Most of the firewalls can permit only the limited number of users from the outside world. A firewall is a part of a network that has been designed to block undesired access while providing permission to the authenticated users.

2. BASICS OF FIREWALL RULES

2.1 Firewall rule set
The Firewall filtering decision is based on set of specified rules. Each rule has a <predicate>over a multiple packet header fields and a <decision>where <predicate> is a Boolean value consisting of certain variables which it assign to each packet as true or false and <decision> specifies whether to "accept or deny". Eha [6] mention the packet header fields as (Source IP address, Destination IP address, Source port, Destination port, protocol type) as shown in Table 1.

Rule	Protocol	Source IP	Source Port	Dest. IP	Dest Port	Action
r1	TCP	162.11.1*	*	162.32.1.*	80	allow
r2	TCP	162.11.*.*	80	162.32.1.*	80	deny
r3	UDP	142.11.2.*	*	192.168.*.*	53	allow
r4	UDP	100.11.1.*	*	192.168.1.*	53	allow

Table 1: Example of firewall rule set

2.2 Filtering rule format

The most commonly used fields in a firewall policy are the multiple packet header fields [7, 8]. The format of the policy are rules in each and every <rule> <protocol> <source_IP> <source_port> <destination_ip> <destination_port> <Action>. The rule specifies the name of the rule. Port can be a specific port number and IP address can be host or a network. Firewalls use the first match mechanism to decide which should be applied first to which packet. The important characteristics of a firewall is to first maintain the orderness of their rule-base because each firewall has to check the packets in the sequence for each and every new session i.e. the rule that its matches first. The deny option is mainly used to support some of the errors due to some of the conflicts.

3. EXISTING SYSTEM

In the existing system the main focus is on intrafirewall optimization in a single firewall environment by removing the redundant rules but the privacy is not at all concerned. As a result conflict detection [4] will be more complex and this may occur due to the overlaps i.e. the same rule matching more than one filtering rule can occur. To solve these conflicts, the first matching strategy mechanism is used in which each packet to be processed by a firewall is mapped to the decision of rule with highest priority. So to overcome this type of conflicts we approach the goal by" how to decrease the errors when a firewall policy rules have been designed".

Drawbacks:

- Detection of anomalies is incomplete and not accurate.
- Misconfiguration will be more between the rules and it cannot accurately identify the anomalies.
- The increase in number of rules can significantly effects its throughput.

4. PROPOSED SYSTEM

In existing approach, they can detect only conflicts and other type of anomalies but it can't able to resolve them accurately. So in this proposed system using a novel anomaly management framework to accurately identify the anomalies and to effectively resolve them using a rule-based segmentation technique. This technique can easily identify the relationships among the rules as subset, superset or overlap, partially match, exactly match Policy Anomaly algorithm can be used to find out the anomalies from the rules and eliminate these anomalies which has a time complexity of $O(n^2 \log n)$. In this system Cross-domain search [2] has been used to overcome the drawback of existing system. This proposed system can provide evidence to the administrator about the malicious activity.

4.1 Firewall policies and anomalies

Generally when a data packet has been entering into a network, the packet has to satisfy the criteria of the firewalls. The criterion in which it consists of multiple packet header field and decision. Every firewall policy has an important characteristic is the adoption of correct policy and correct ordering of filtering rules. Anomalies in firewall policy may occur due to existence of two or more policy filtering rules that may match the same packet. The main aim of discovering anomalies is to determine if any two rules coincide with each other in a policy. Based on the comparison of each field with the other fields in a firewall, the classification of anomalies are of five types as shadowing anomaly, Correlation anomaly, Redundancy anomaly, Generalization and Irrelevance anomaly[3][5].

- **Shadowing Anomaly —**Suppose when a rule which is positioned after the first rule matches all the packets in which it match this rule then he rule is shadowed by the before rule and it never be active.
- **Correlation Anomaly —**Suppose when the first rule matches some packets and second rule also the packets that have been matched by the first rule and performing the different type of actions, then these rules are correlated.
- **Redundancy Anomaly —** If two rules perform same type of actions such that removing one rule does not affect the the other rule and security policy will not be affected.
- **Generalization Anomaly —** Suppose the first rule match the packets that have been matched by the second rule and at same time performing different types of actions then there are generalized.
- **Irrelevance Anomaly —** A rule in a firewall is irrelevant if this rule does match any rule in the given time interval due to some network connectivity. This may happens when both the source and the destination address fields of the rule do not match any domain.

4.2 Advantages

- Easy to understand policy anomalies with the help of grid like representation.
- Can accurately indicate all rule involve in policy anomaly.
- Firewall makes secure and trusted access.
- Easy to detect predefined rule and rearrange them.
- Examines both preceding rule and subsequent rule while performing an anomaly analysis.
- Allowing us to create the inbound and outbound rules.

5. METHODOLOGY

In the proposed work, rules and actions are generated or modified according to the changes in the requirements of the dynamic environment. When a client sends a data packet to network, firewall checks the packet characteristics and decides to allow/deny the packet flow into the network. The firewall rule anomalies are identified using packet space segmentation technique, and then the risk of anomalies is assessed, based upon the risk, the firewall rules are re-ordered. Risk assessment is measured using an upper bound and lower bound threshold values as shown in Figure 2.

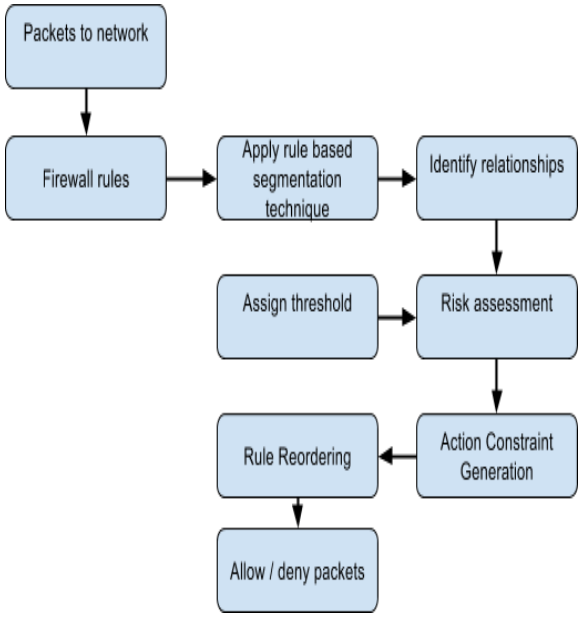


Figure 2. Architecture of proposed system

5.1 Modules

- Rule generation
- Correlation of Packet Space Segment
- Action Constraint Generation
- Rule Reordering
- Data Package

5.1.1 Rule generation

When we want to send the data packets to a network, the packets have satisfy the rules of a firewall. Here the rules can be generated by taking some of the specifications and constraints. The rules can be generated in rule engine, action can happen when data packet has been sent to rule engine.

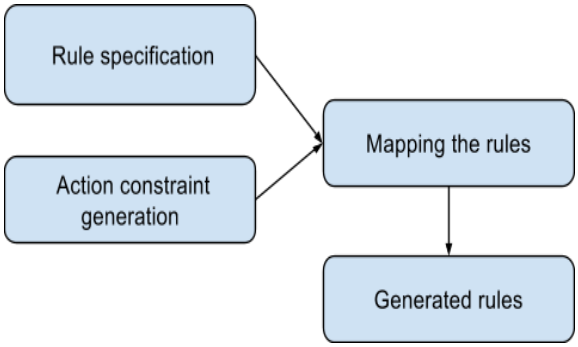


Figure 3. Generation of rules

5.1.2 Correlation of packet space segment

Here we use the rule-based segmentation technique to identify the correlation groups for the analysis of anomalies with each independently based on the conflicting rules. Correlated rules can also be generated independently. The searching space can also significantly decrease as shown in Figure 4.

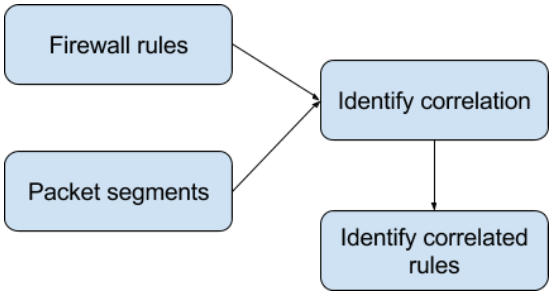
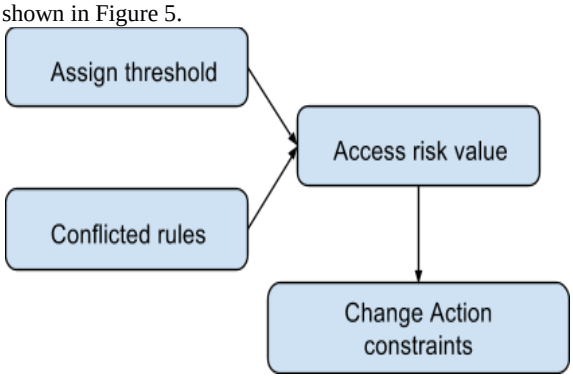


Figure 4. Packet space segments

5.1.3 Action constraint generation

Here we first identify the correlated groups and we assess the risk value of each conflict. Each conflict risk value can be utilized for automated and manual selection and here we set the threshold valued be on different situations. The system administrator can set a threshold value based on different situations. If the risk value is low, the expected action will be taken. If risk is high then we generate action constraints based on resolution strategies considering the protection of network perimeter. The basic idea can be as shown in Figure 5.



. **Figure 5. Generation of constraints**

5.1.4 Rule reordering

To resolve conflicts, every conflict has to satisfy the action constraints that have been generated for the Reordering conflicting rules and this provides a minimal solution for the conflict resolution.

5.1.5 Data package

When all the conflicts in a policy has been resolved, the risk value can be compared with the original polices based on the threshold value when data has been received in to a server as shown in Figure 6.

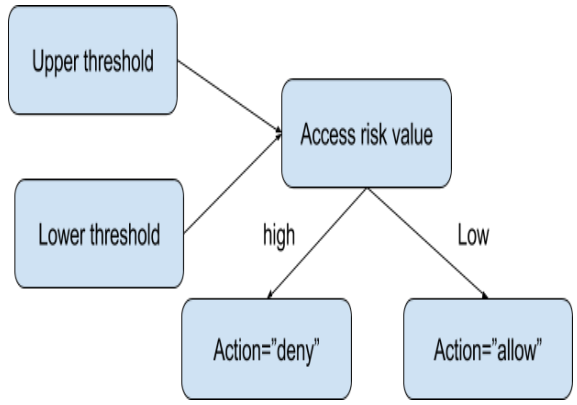


Figure 6. Data Package

5.2 Algorithm

Policy Anomaly detection is mainly used to identify the anomalies and conflicts that may exists in the firewall rules. These algorithms not only detect the anomalies but it also provides effective resolutions for the identified anomalies by considering the protection of network perimeter. Generally each policy in a firewall follows he first-match semantic mechanism in which it has to match the packets to which it first applies.

Algorthim.1.Firewall anomaly discovery algorithm

Input: rule, field, node

Output: anomaly

1. **FunctionDecideAnomaly**(rule,field,node,anomaly)
2. **if** each feld,node has branch_list **then**
3. branch=node.branch_list.first()
4. **if** anomaly←CORRELATION then
5. **if** rule.action≠branch.value **then**
6. branch.rule.anomaly←CORRELATION
7. report rule rule.id←Correlation←branch.rule.id
8. **else** anomaly=NONE
9. **else if** rule.action≠branch.value **then**
10. anomaly←SHADOWING
11. report rule rule.id←shadowed←branch.rule.id
12. **if** branch.rule.anomaly=NONE **then**
13. anomaly←NONE
14. **if** branch.rule.anomaly←REDUNDANCY
15. rule branchrule.id←redundant←rule rule.id
16. **end**
17. **if** else if rule.action=branch. value **then**
18. anomaly←REDUNDANCY
19. **else** anomaly←NONE
20. **else if** anomaly←GENERALIZATION and rule.action≠branch.value then
21. .branch.rule.anomaly=SPECIALIZATION
22. **end if**
23. **end if**
24. **rule. anomaly=anomaly**
25. **end function**

Algorthim1 is mainly used for identifying the anomalies, to determine if any two rules coincide in their paths. Suppose if a rule coincides with the path of another rule, there is an anomaly that can be discovered. If a rule does not coincide, then we conclude that they have no anomalies. First we start with no relationship between the rules. Each field in one rule is compared to the corresponding fields to identify the relationships. Suppose if some fields in one rule are subset to the corresponding fields and performing same type of actions then these rules are redundant. At the same time when their actions are completely different then the rules shadowed to one another. If some fields are supersets and some fields are subsets while performing different types of actions then the rules are correlated to each other to identify the rules that are irrelevant, we require the knowledge of network connections.

5.3 Result analysis

For any project to evaluate the effectiveness we need to consider three metrics as availability, their resolution rates and risks for the quality of resolving the policies using the proposed approach. First we start with the strategy mechanism and by obtaining the results we compared this with the proposed system approach. As from the results seen in Figure 7 only 63 percent of conflicts have been resolved using the first match strategy but by using the interfirewall optimization an average of 92 percent of conflicts have been resolved in our experiments.

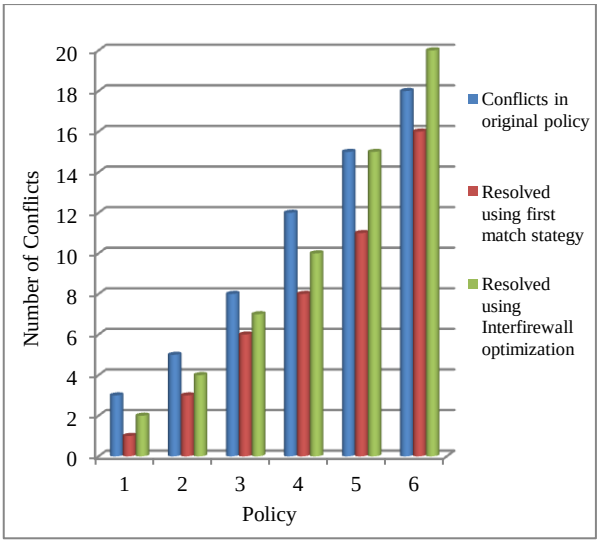


Figure.7 Resolution rate for policy anomalies

6. CONCLUSION

Network security made many developments in the areas of research, industrial communities' etc. Generally, firewall may require some proper management of tools and techniques to provide security for such type of services. One of the major challenge tasks with the firewalls is the managing and designing of the firewall rules. This technique can help the system administrators to have some evidence about the anomaly. So we have proposed a anomaly management framework which can handle this type of tasks and provide a effective anomaly resolution. This proposed system helps in the real and fraud users and provide the secure access to both the public and private network.

7. FUTURE ENHANCEMENT

In future, our work can be extended to evaluate the functionalities of policy approaches. It includes extending our anomaly analysis to handle distributed firewalls and for the other types of access control policies and it can be used for hacking prevention on individual machine.

8. REFERENCES

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

[2] Fei Chen, Bezwada Bruhadeshwar, and Alex X. Liu," Cross-Domain Privacy-Preserving Cooperative Firewall Optimization" IEEE/ACM Transactions on Networking vol.21,, no. 3, June 2013.

[3] L. Qiu, G. Varghese, and S. Suri, "Fast Firewall Implementations for Soft-ware and Hardware-Based Routers," Proc. 9th Int'l. Conf. Network Protocols (ICNP 2001), Nov. 2001.

[4] Wool, "Trends in Firewall Configuration Errors" IEEE Internet Computing, vol. 14, no. 4, pp. 58-65, July/Aug. 2010.

[5] Hari et al. (2000); Epstein and Muthukrishnan (2001); Moffett and Sloman (1994); "conflict detection and resolution "Baboescu and Varghese (2002).

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

[7] Subana Thanasegaran, Yuichiro Tateiwa, Yoshiaki Katayama, Naohisa Takahashi, "Simultaneous Analysis of Time and Space for Conflict Detection in Time-Based Firewall Policies", 978-0-7695-4108-2/10 $26.00 © 2010 IEEE

[8] S. Cobb, "ICSA Firewall Policy Guide v2.0," NCSA Security White Paper Series, 1997.

[9] J. Wack, K. Cutler, and J. Pole, "Guidelines on Firewalls and Firewall Policy," NIST Recommendations, SP 800-41, Jan. 2002.

[10] Proc 2000 IEEE Symp. "Security and Privacy for protecting the firewall policies: May 2000.

[11] Yuan, C. Chua, and P. Mohapatra,"ProgME: Towards Programmable Network.

[12] G. Misherghi, L. Yuan, Z. Su, C.-N. Chuah, and H. Chen, "A General Framework for Benchmarking Firewall Optimization Techniques," IEEE Trans. Network and Service Management, vol. 5,no. 4, pp. 227-238, Dec. 2008

[13] Mohamed Taibah, Ehab Al-Shaer and Hazem Hamed School of Computer Science, Telecommunications and Information Systems DePaul University, Chicago, USA "Dynamic Response in Distributed Firewall Systems"

[14] Frederic Cuppens, Nora Cuppens-Boulahia†, and Joaqu´ınGarc´ıa-Alfaro "Detection of Network Security Component Misconfiguration by Rewriting and Correlation"