International Journal of Computer Networks and Communications Security

VOL. 5, NO. 2, FEBRUARY 2017, 20–27
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Case Study on Firewall Rules Analysis for CWN

MANIKRAO L DHORE[1] and RADHWAN ALDHAHERI[2]

[1, 2] Computer Engineering Department, Vishwakarma Institute of Technology, Savitribai Phule Pune University, Pune, India

[1]*manikrao.dhore@vit.edu*, [2]*radhwannn@gmail.com*

ABSTRACT

In this paper authors proposed a software based system which carry out the analysis of rules implemented in the firewall to find hidden anomalies if any as well as any address conflicts for the Campus Wide Network (CWN) of Vishwakarma Institute of Technology, Pune, India. This information can be very useful for the administrator to modify the existing policies as well as to add the new policies with fewer complexities. Institute has the CWN consisting the seven Ethernet Segments for seven major departments in the institute. The proposed system control the flow of Local Area Network (LAN) segments communication which is a part of CWN by using a method that analyzes the firewall polices or rule-set, Relational Algebra and One Way 2D Road proposed Model. It can discover all the types of anomalies in the firewall rule-set in the format that is usually used by many firewall products. The most of the existing analyzing methods consider the anomalies between any two rules and very few consider more than two rules together at the same time to discover the anomalies. In this paper we have adopted the combination of both these methods to detect the anomalies effectively. With the proposed system, it is possible to discover most of the hidden anomalies in the firewall rule-set and to reduce the size of rule set by eliminating redundant rules without changing the existing policies. This software based system is developed, implemented and tested over the CWN.

Keywords: *Firewall Policies, Shadowing Anomaly, Correlation Anomaly, Generalization Anomaly, Redundancy Anomaly.*

1 INTRODUCTION

Firewall is a device either hardware-based or software-based used to protect a LAN or CWN from unauthorized access to the users within as well as outside the organization as depending on the policies of organization.

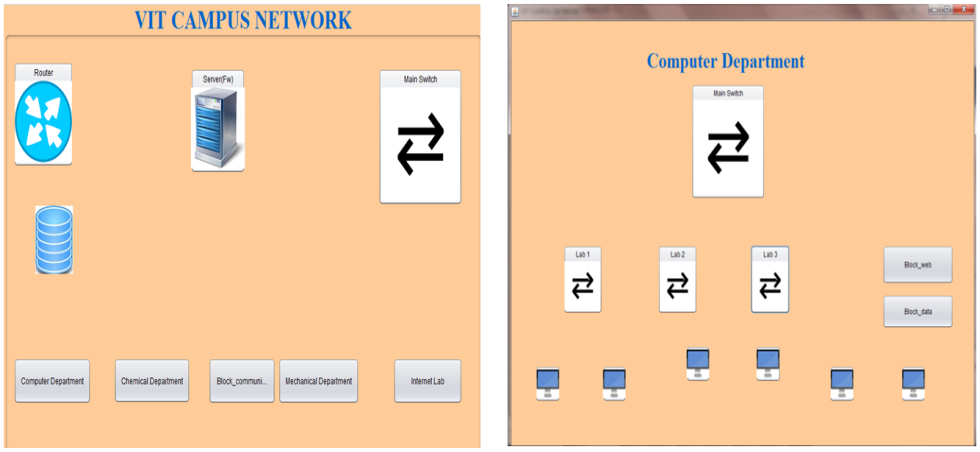

Fig. 1. Campus Network as a Case Study

For our case study we selected the CWN of our institute having 1500 plus nodes as depicted in figure 1 and figure 2 as a part of our case study. We collected the network access policies implemented for the different departments and students for the purpose of analysis in order to find out the anomalies if any.

Within all higher educational campuses the connectivity of Internet has more or less become the mandatory. As Internet connection is provided in all the classrooms and laboratories, it increases more chances of misusing the networks. Nowadays network security has become the prime concern due to cyber attacks and many other such reasons. A prime solution to apply the security is the deployment of software-based or Hardware-based firewall at the edge of Local area networks (LAN) and Campus Wide Networks (CWN). Network security policies often includes the rules intended to preserve and protect valuable ,confidential, or proprietary information from the unauthorized access or disclose, to limit or eliminate potential legal liability from employees or third parties and most important is to prevent waste or inappropriate use of organization resources.

Among these policies few of the important polices implemented for our campus are given below.

- Face book access is permitted only in common Internet Lab and restricted in classrooms and all other laboratories.
- Audio/Video downloading access is permitted only in common Internet Lab and restricted in classrooms and all other laboratories.
- Downloading of any necessary open source software more than 80 MB in size is permitted only in common Internet Lab and restricted in classrooms and all other laboratories.
- Access to open source and legal licensed software available on Institute Application Server is permitted all laboratories except the common Internet lab.
- And many more policies…

In this paper, authors presented the detection of various anomalies in the rule set of firewall and on the fly modifications in the policies with little bit human intervention of network administrator.

2 BACKGROUND

In most of the cases, network grows gradually and keeps on changing the policies for the firewall. After few years it starts having the address conflicts and incorrect sequence of rules in the rule set of firewall. This results in improper functioning of the firewall and users tend to take the advantage of it. Many researchers have worked on these issues and few of them are included as a part of literature survey which we have referred for our work. Thawatchai Chomsiri proposed a method for analyzing rule-set of firewall by using relational algebra operations and proposed a model named as raining 2D-Box model. It can detect all the types of anomalies in the firewall rule-set and also presented the theorems to eliminate and combine rules without making any major changes in the present policies [1]. Ehab Al-Shader presented an algorithm to discover the anomalies by using SET theory. Their method detects few mistakes within rule-set and cannot find all anomalies when it requires more than two rules to detect it at the same time [2]. Pasi Eronen proposed an expert system based on constraint logic programming (CLP). This system allows the user to write advance operations to discover the common configuration errors in the firewall rule-set [3]. Scott Hazelhurst proposed Binary Decision Diagrams (BDDs) to present and analyze rule-set. It can discover the entire hidden anomalies when considering more two rules together [4]. We propose the firewalls rule-set to manage the network flow, internet connection flow and application server flow by using Relational Algebra and one way 2D Road model. We proposed an alternative approach using Relational Algebra and one way 2D model for finding anomalies within the rule-set. The paper is organized as follows. Section 3 presents how to map the firewall rules-set into Relation using Cartesian product [5]. Section 4 presents how classify and define firewall policy anomalies. It extends anomaly detection if any and describes how to remove anomaly. It also tries to minimize the rule-set's size by combining some rules together. Application of the proposed method on our VIT college network is presented in each section and subsection as and when required.

3 RELATIONAL ALGEBRA FOR FIREWALL RULE-SET

More or less there is common format to specify the rules for firewall and routing policies. Mostly, it contains Rule Order, Source Address/Mask, Destination Address/Mask, Destination Port, Protocol and Action. Table 1 is the example for specifying the rules in general for the bigger size networks for firewall and routers [8].

Table 1: Format for Rule Set -I

Rule	Source Address/Mask	Destination Address/Mask	Destination Port	Protocol	Action
1	201.15.17.21/32	201.15.75.4/32	<1024	*	Deny
2	201.18.20.25/24	201.15.100.10/32	=80	TCP	Permit
3	201.15.20.25/24	201.15.100.10/32	<1024	UDP	Permit

For LAN and CWN, mostly format shown in Table is used for specifying the firewall rules.

Table 2:Format for Rule Set-II

R	Source Address	Destination Address	Dest Port	Action
1	201.15.17.21	201.15.75.4	23	Deny
2	201.18.20.25	201.15.100.10	25	Permit
3	201.15.20.25	201.15.100.10	110	Permit

Relational Algebra is used to specify the conditions in the firewall and it helps to classify the nature of data flow as the port numbers are unique for most of the standard Internet based applications. It works on a relation which is subset of Cartesian product [5]. It is a procedural query language which consists ofa set of operations either over the single relation(R) or group of relations depending on the situation. Relational Algebra consists of unary and binary operations. Unary operations are SELECT, PROJECT and RENAME while UNION, INTERSECTION and DIFFERENCE are binary operations. Our implementation requires five operations SELECT, PROJECT, UNION INTERSECTION and DIFFERENCE. Working of these relational algebra operations is explained by considering two relations R1 and R2 depicted in Table 3.

Table 3: Relation R1 and R2

Relation R1					Relation R2				
Source IP	Dest. IP	Dest. Port	Proto	Action	Source IP	Dest. IP	Dest. Port	Proto	Action
172.21.0.0	172.22.0.1	25	TCP	Deny	172.21.0.0	172.22.0.1	25	TCP	Permit
172.21.0.1	172.22.0.1	25	TCP	Deny	172.21.0.0	172.22.0.1	23	TCP	Permit
172.21.0.2	172.22.0.1	25	TCP	Deny	172.21.0.1	172.22.0.1	25	TCP	Permit
172.21.0.3	172.22.0.1	25	TCP	Deny	172.21.0.1	172.22.0.1	23	TCP	Permit

PROJECT operation is used to select a set of columns for given number of attributes. It returns the argument relation with certain attribute left out. Since a relation is set, any duplicate rows are eliminated [5].Table 4 shows the relations R3 and R4 after applying PROJECT operation on relations R1 and R2 for first three attributes respectively.

Table 4: Relations R3 and R4

R3	Source IP	Dest. IP	Dest. Port	R4	Source IP	Dest. IP	Dest. Port
	172.21.0.0	172.22.0.1	25		172.21.0.0	172.22.0.1	25
	172.21.0.1	172.22.0.1	25		172.21.0.0	172.22.0.1	23
	172.21.0.2	172.22.0.1	25		172.21.0.1	172.22.0.1	25
	172.21.0.3	172.22.0.1	25		172.21.0.1	172.22.0.1	23

Table 5: Relations R5, R6 and R7

R5			R6			R7		
Source IP	Dest. IP	Dest Port	Source IP	Dest. IP	Dest. Port	Source IP	Dest. IP	Dest Port
172.21.0.0	172.22.0.1	25	172.21.0.0	172.22.0.1	25	172.21.0.2	172.22.0.1	25
172.21.0.1	172.22.0.1	25	172.21.0.1	172.22.0.1	25	172.21.0.3	172.22.0.1	25

Table 5 shows the relations R5, R6, R7 for SELECT, INTERSECTION and DIFFERENCE operations respectively on relations R3 and R4 respectively.

4 RULE-SET AND TYPES OF ANOMALY

For the case study we have selected the nodes from the major departments of our institute and they are Mechanical, Chemical and Computer Engineering Department. Table 6 shows few rules from the real set of selected 198 rules from the rule-set created for firewall configuration. For the detection of anomalies, in our case study we are considering only File Transfer Protocol (FTP) protocol which is being used by most of the faculties as well as students. FTP protocol is the protocol at application layer and uses TCP protocol from host to host layer of TCP/IP model. It runs by using two ports 20 and 21 respectively where one port is used as a control port while other one is used delicately for data transfer.

Table 6: Selected Rule-Set for Anomaly Testing

Rule	Source Address/Mask	Destination Address/Mask	Destination Port	Protocol	Action
R1	172.21.0.0/30	172.22.0.0/30	20-21	TCP	Deny
R2	172.21.0.1	172.22.0.1	21-22	TCP	Permit
R3	172.21.0.1	172.22.0.1	23-26	TCP	Deny
R4	172.21.0.1	172.22.0.1	22-23	TCP	Permit
---	---	---	---	---	----
R6	172.21.0.0/30	172.22.0.0/30	20	TCP	Deny
R7	172.21.0.7	172.22.0.7	20-25	TCP	Permit
R8	172.21.0.7	172.22.0.7	20	TCP	Deny
---	---	---	---	---	----
R19	172.21.0.21	172.22.0.20	20-21	TCP	Permit
R20	172.21.0.21	172.22.0.20/30	20-21	TCP	Permit
R21	172.21.0.20/30	172.22.0.20/30	20-21	TCP	Deny
---	---	---	---	---	----
R27	172.21.0.35/30	172.22.0.35	21-22	TCP	Deny
---	---	---	---	---	----
R31	172.21.0.31/30	172.22.0.31	20-21	TCP	Deny
R32	172.21.0.31/30	172.22.0.30/30	20-21	TCP	Deny
---	---	---	---	---	----
R35	172.21.0.35/30	172.22.0.35	20-21	TCP	Deny
R36	172.21.0.36	172.22.0.0/30	20-21	TCP	Permit
R37	172.21.0.35/30	172.22.0.34/30	20-21	TCP	Deny
---	---	---	---	---	----
R100	172.21.0.100	172.22.0.100	20-21	TCP	Deny
---	---	---	---	---	----
R150	172.21.0.150	172.22.0.151	20-21	TCP	Deny
---	---	---	---	---	----
R198	172.21.0.197	173.22.0.208	20-21	TCP	Deny

4.1 Shadowing Anomaly

This anomaly occurs when the one (say Rx) or more rules (say Rx and Ry) are already matched and executed and there is a rule (Say Rz) which is the subset of either of the above rules, then Rz will never be executed [6][7]. Only solution is to check, is there any kind of anomaly like this in the given rule-set and if it is present, then remove it as no action will be happen for it. In our rule set

Rule R4 is shadowed by Rule R3 U R2.
Rule R35 is shadowed by Rule R27

Figure 2 depicts the screen shot for shadowing anomaly for our case study.

We proposed ***One Way 2D Road model*** to simulate the flow of the packets and the sequence of the rule-set. We proposed the packets like cars and the check points like rule-set. This model will make easy to understand the flow of packets and the sequence of rule-set. Figure 3 depicts the

shadowing anomaly using ***One Way 2D Road model.***

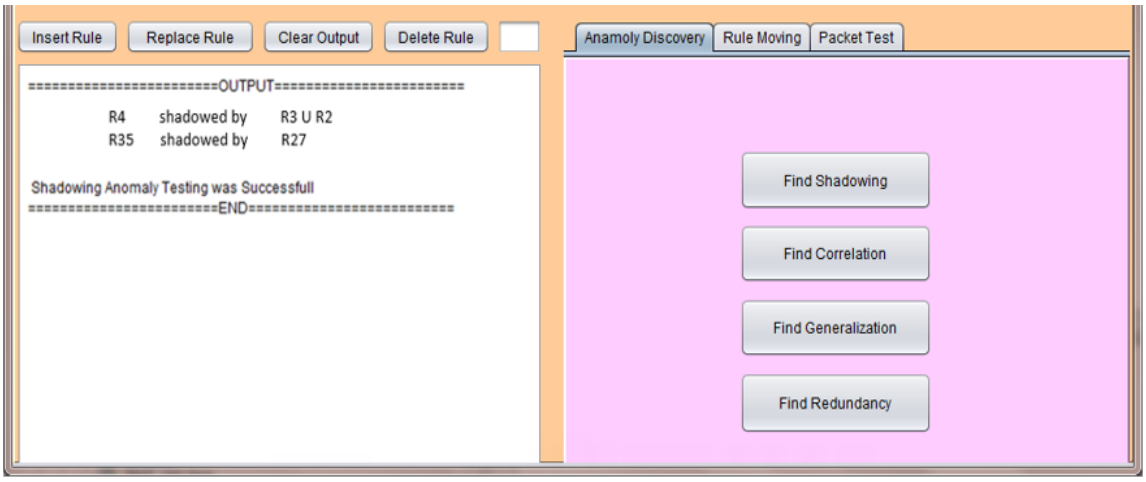

Fig. 1.Shadowing Anomaly Detection

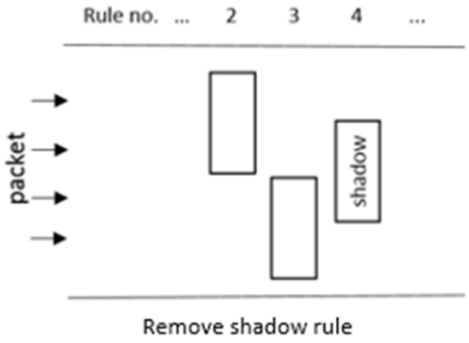

Fig. 2. Shadowing Anomaly

4.2 Correlation Anomaly

This anomaly occurs when first rule matches some packets which also have match in second rule and vice-versa. These two rule having different actions but having match for few packets are called correlated rule and they creates the correlation anomaly. The part of (Ry) matches the some packets that match in the previous rule (Rx) will never be executed [6][7]. The solution is only to report such kind of anomaly to network administrator. Sometime first rule shadows the one or more further rules in sequence. In this case if next two rules are shadowed by previous rule then we can swap these two rules without changing the policy of the system. In our rule-set

R4 is correlated with R3
R8 is correlated with R7 and both are shadowed by R6, then we can swap R7 with R8.

Figure 4 depicts the screen shot for correlation anomaly for our case study. Figure 5 depicts the correlation anomaly using ***One Way 2D Road model.***

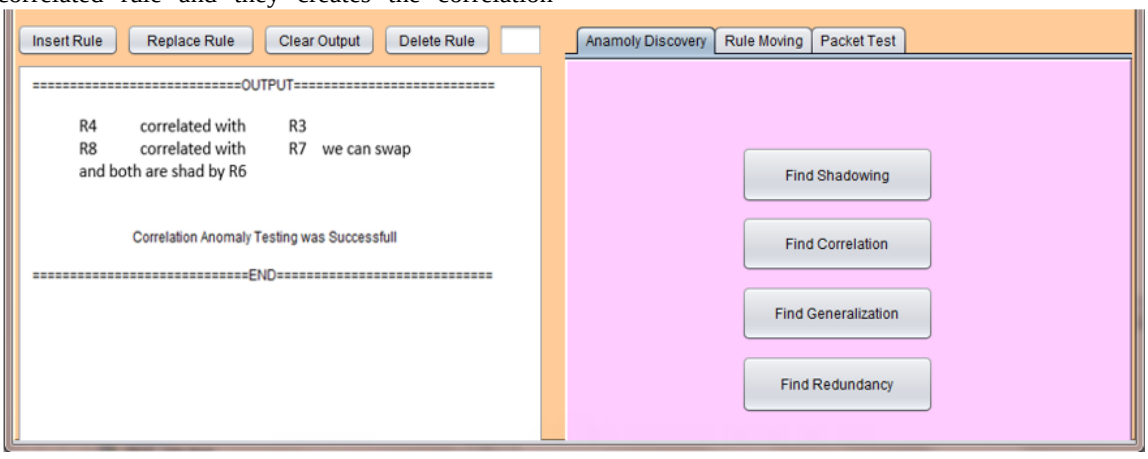

Fig. 3. Correlation Anomaly Detection

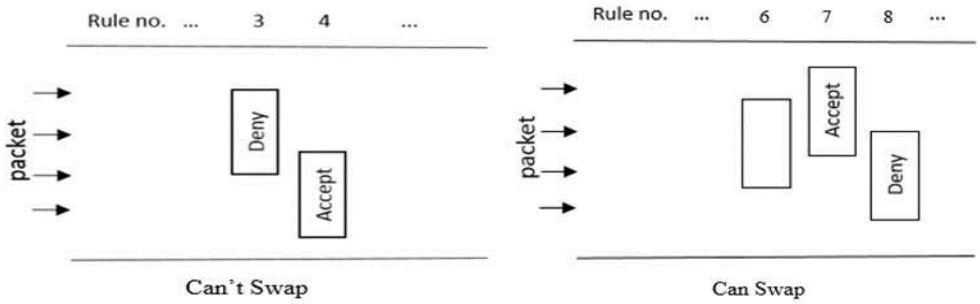

Fig. 4.Correlation Anomaly

4.3 Generalization Anomaly

This anomaly occurs when there is one rule (say Rx) is a subset of another rule (say Ry) and the action of two rules are different. In this case we can say (Ry) is generalization of (Rx). Only solution to this anomaly is to report it to network administrator. In second case if same two rules (Rx, Ry) are shadowed by previous rules then we can swap rules (Rx, Ry) and the swap of two rules will happen without changing the policy of the system [6][7]. In our rule-set

R21 is generalization of R19
R21 is generalization of R20

Figure 6 depicts the screen shot for Generalization anomaly for our case study. Figure 7 depicts the correlation anomaly using ***One Way 2D Road model.***

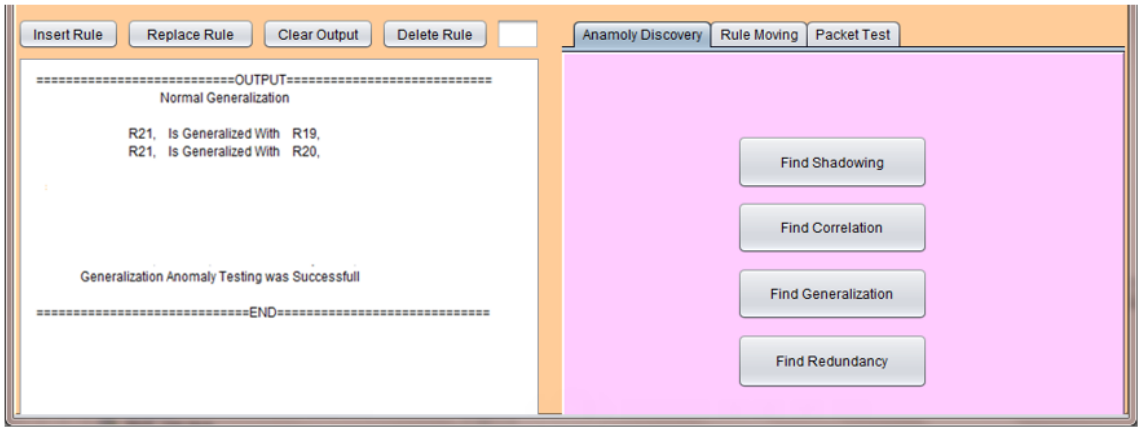

Fig. 5.Generalization Anomaly Detection

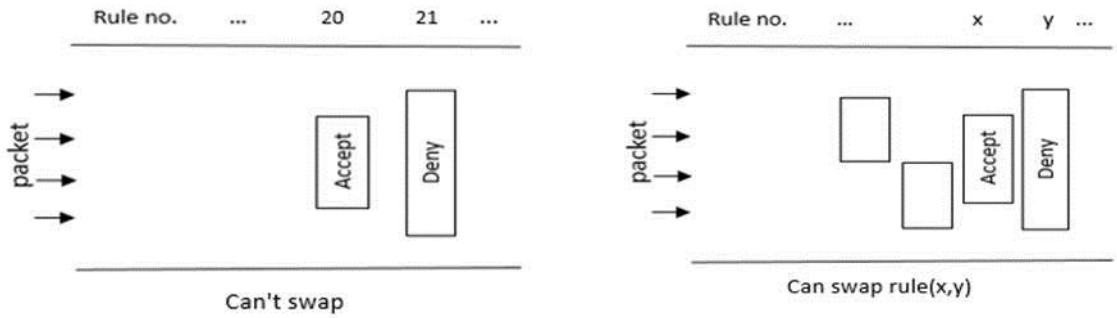

Fig. 6.Generalization Anomaly

4.4 *Redundancy Anomaly*

This anomaly occurs when there is one rule (say Rx) are subset of another rule (say Rz) and the action of two rules are same then we say (Rx) is redundant to (Rz). The solution is removing this type of anomaly (Rx). In second case if there is one rule (say Ry) between these two rules (Rx, Rz), then we cannot remove redundant rule (Rx), if we remove then the policy of system will change [6][7]. In our rule-set

R19 is redundant to R20
R31 is redundant to R32
R35 is redundant to R37 we can't remove R35 because of there is one rule (R36) between these two rules(R35, R37) with different action.

Figure 8 depicts the screen shot for redundancy anomaly for our case study. Figure 9 depicts the redundancy on anomaly using ***One Way 2D Road model.***

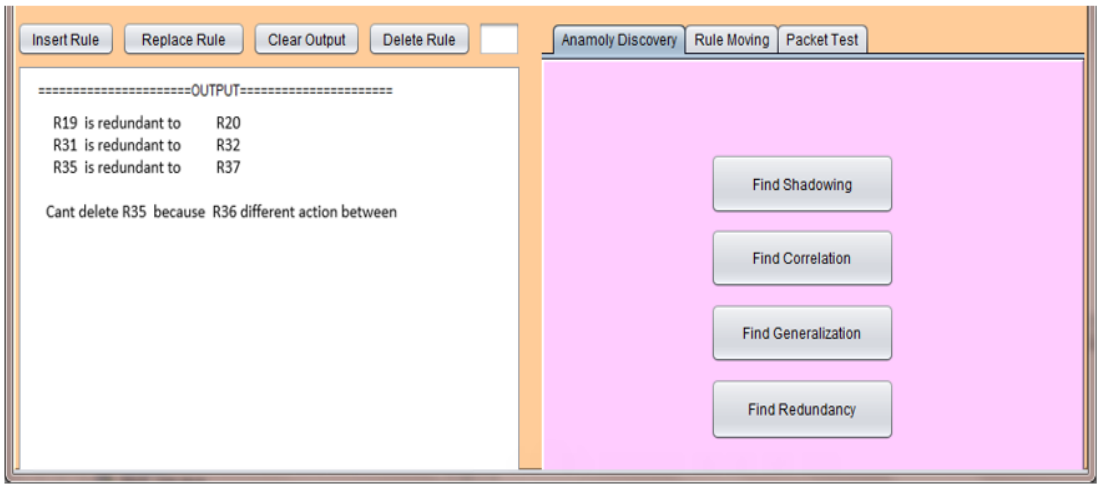

Fig. 7.Redundancy Anomaly Detection

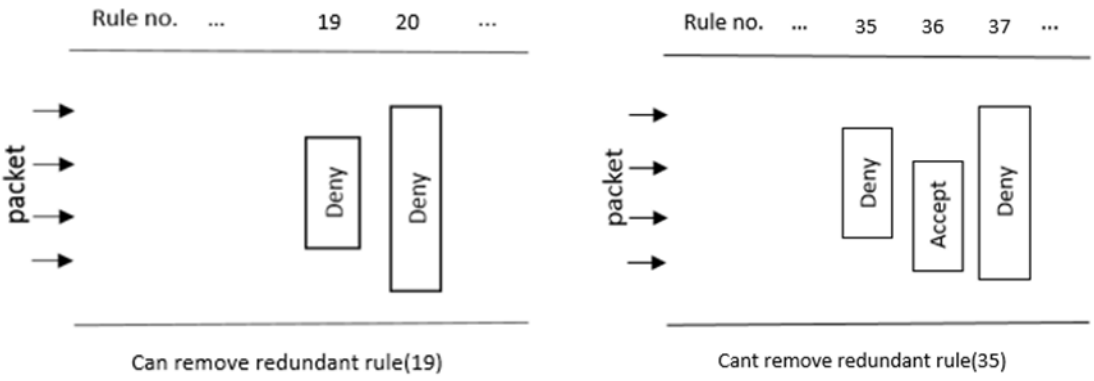

Fig. 8.Redundancy Anomaly

5 CONCLUSION

Authors proposed a software based system to carry out the analysis of rules implemented in the firewall to find hidden anomalies if any for the Campus Wide Network (CWN) of Vishwakarma Institute of Technology, Pune, India. This information can be very useful for the administrator to modify the existing policies as well as to add the new policies with fewer complexities. The proposed system control the flow of Local Area Network (LAN) segments communication which is a part of CWN by using a method that analyzes the firewall polices or rule-set, Relational Algebra and One Way 2D Road proposed Model. It can discover all the types of anomalies in the firewall rule-set in the format that is usually used by many firewall products. With the proposed system, it is possible to discover most of the hidden anomalies in the firewall rule-set and to reduce the size of rule set by eliminating

redundant rules without changing the existing policies.

6 REFERENCES

[1] Thawatchai Chomsiri and Chotipat Pornavalai. "Firewall rules analysis", International Conference on Security and Management (SAM06), January 2006

[2] Ehab Al-Shaer and Hazem Hamed. "Firewall Policy Advisor for anomaly Detection and Rule Editing". IEEE/IFIP Integrated Management IM'2003, March 2003.

[3] P. Eronen and J. Zitting. "An Expert System for Analyzing Firewall Rules". Proceedings of 6th Nordic Workshop onSecure IT-Systems (NordSec 2001), November 2001

[4] S. Hazelhusrt. "Algorithms for Analyzing Firewall and Router Access Lists". Technical Report TR-WitsCS-1999 Department of Computer Science, University of the Witwatersrand, July1999

[5] Abraham Silberschatz. Henry F. Korth, Sudharsan S. "Database System Concepts, 3rd Edition". Tata McGraw-Hill,1997.

[6] Chotipat Pornavalai and Thawatchai Chomsiri. "Firewall Policy Analyzing by Relational Algebra". The 2004 International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2004), JULY 2004.

[7] Chotipat Pornavalai and Thawatchai Chomsiri. "Firewall Policy Analyzing by Relational Algebra". Draft TechnicalReport, Faculty of Information Technology, King Mongkut's Institute of Technology Ladkrabang, Thailand, January2004.

[8] George Varghese, University of California, San Diego, Amsterdam, Network Algorithmic Fast Networked Devices , An Interdisciplinary Approach to Designing, 2005 by Elsevier Inc.