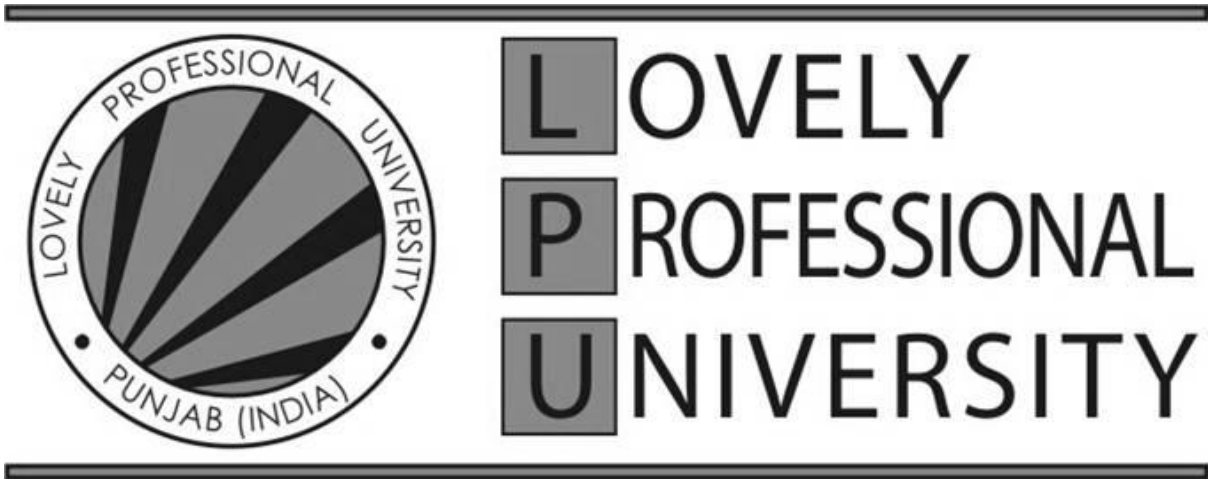


TESTING TO DETECT ANOMALIES IN FIREWALL RULES AND POLICY

A Dissertation Proposal

Submitted by

RAKESH YADAV

Registration Number:-11307683

To

Department of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab, India

In Partial fulfilment of the requirement for the

Award of the Degree of

Master of Technology in Computer Science

Under the guidance of

Mrs. Harjeet Kaur

(April 2015)

PAC FORM

LOVELY PROFESSIONAL UNIVERSITY
Transforming Education, Transforming India

School of: SCIENCE & TECHNOLOGY

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: RAKESH YADAV. Registration No: 11307683

Batch: 2013-15 Roll No: RK2306A12

Session: 14-15 Parent Section: K2306

Details of Supervisor. Designation: AP

Name: Harjeet Kaur Qualification: M.Tech CSE

U.ID: 12887. Research Experience: 9 yrs.

SPECIALIZATION AREA: NETWORK & SECURITY (pick from list of provided specialization areas by DAA)

PROPOSED TOPIC

1. TESTING TO DETECT ANNOMALIES IN FIREWALL POLICY, AND RULES.
2. SURVEY ON FIREWALL POLICY & MANAGEMENT.
3. DISCOVERY OF ANNOMALIES IN FIREWALL POLICY.

12/9/14
Signature of Supervisor

PAC Remarks:

Topic 1 is approved. Publication is expected

APPROVAL OF PAC CHAIRPERSON: Signature: 19/9/14 Date: 19/9/14

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)
*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.
*One copy to be submitted to Supervisor.

ABSTRACT

Firewall security has become necessary because internet usage is high so to avoid the serious attacks through the online, firewall is essential. This paper investigate the study of firewall rules to identify the anomalies in a firewall rule set. Anomalies are generated either when change the position of rules or change the action of the rule. This approach is helpful to improve the efficiency of firewall and maintain the order of firewall rule set in a proper order so that the function of rule would be become well from the previous one. The total function of the firewall is dependent on the rule set and their function.

CERTIFICATE

This is to certify that **Rakesh Yadav,** Registration Number 11307683 has completed M.Tech Dissertation Part 2 proposal titled, **TESTING TO DETECT ANOMALIES IN FIREWALL POLICY & RULES**, under my guidance & supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the dissertation proposal has been submitted for any other degree or diploma.

The dissertation proposal is fit for the submission and the partial fulfilment of the conditions for the award of M.Tech Computer Science & Engg.

Date: ……

Signature of Advisor

Name: Mrs. Harjeet Kaur

UID: 12427

ACKNOWLEDGEMENT

The idea of this research has begun when I was introduced to the subject Network Security & Cryptography during my studies. It looks like very interesting and when I have studied about the Firewall it made me very curious to know about the security and their policies and rules. As Firewall Rule & its Anomalies is a novel idea so it raised my interest after the study of few research papers.

Firewall Rule set requiring the proper maintenance to avoid the anomalies. So my dissertation is "**TESTING TO DETECT ANOMALIES IN FIREWALL POLICY AND RULE**".

I take this opportunity to express my profound gratitude and deep regards to my guide **Mrs. Harjeet Kaur** for her exemplary guidance, monitoring and constant encouragement throughout the course of this thesis. The blessing, help and guidance given by her time to time shall carry me a long way in the journey of life on which I am about to embark.

I also take this opportunity to express a deep sense of gratitude to the teachers of Lovely Professional University for their cordial support, valuable information and guidance, which helped me in completing this task through various stages.

At last, I thank my parent, brother, sister and friends for their constant encouragement without which this assignment would not be possible.

Rakesh Yadav

DECLARATION

I hereby declare that the dissertation proposal entitled, "**TESTING TO DETECT ANOMALIES IN FIREWALL RULES AND POLICY**" submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: MAY 2015 Investigator

RAKESH YADAV

Registration Number: 11307683

Table of Contents

List of Tables:

List of Figures:

List of Screenshots:

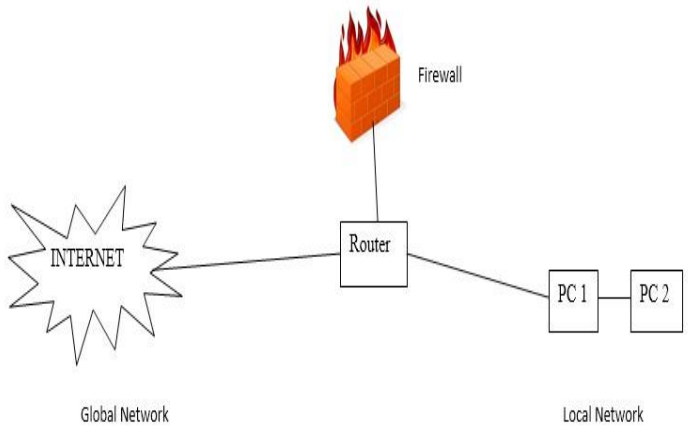
Chapter 1

INTRODUCTION

Now a days, the attacking scenario is increasing day by day either on computer systems or on networks that are helpful to connect to the communication medium. So due to the security concern many security related softwares has been launched in the market for computer system. And for the network security, Firewall is the best core element to provide the security.

Firewall is nothing but the security guard which lies between the system and internet facility, providing the facility that which packet let them pass through the firewall and which to be blocked (Figure 1). This process has been defined by the firewall rules and policies. According to the network administrator or user requirements, the firewall policies and rules are reliable to change it. Firewall not only installed on large networks but also on small arithmetic calculated devices like computer, laptops etc.

Firewall gives all the relevant information to the user or to whom who is operating, about an unauthorised network as well as unauthorised packets passing through the firewall. A hardware firewall means that on Ethernet, firewall is implemented. Whereas software firewall is one that use in computer or network for protection. Firewall helping to protect against computer worms and Trojans as well as unauthorised network whereas it could easily send the packets either authorised or not, firewall can easily pass it. So it means that networks or computer are not be able to sending the packets without passing through the firewall.



INTERNET- Globally Connect the devices and providing communication medium.

ROUTER- Hardware device which helps to connect global facility i.e. internet to local devices i.e. personal systems

FIREWALL- Acts like wall to protect from unauthorised network as well as malicious packets.

PC1, PC2- Local systems

Figure 1: Firewall

A firewall based on a specific security policy across the borders of a secure network that controls a network element of the packet traversal. A firewall security policy based on conditions specific filtering operations performed on network packet is a list of rules that define the order. A rule that such type of protocol, source and destination IP addresses and ports, as well as an action area filtering fields (also called network regions) is composed of a set. A rule that matches this rule to filter fields in the same areas, the possible values represent the actual network traffic. The same value or range of values for each network area can be. Filtering functions to either permit or secure network packets, which to accept, or causes to be blocked packets, which are to deny. Allow packet or packet header information matches the rule to all network segments is blocked by a specific rule. Otherwise, the rule is examined and a matching rule is found or the default policy action is done until the process is repeated.

A firewall is a private network and all incoming and outgoing packets to pass through it such that at the point of entry is placed between the Internet. A firewall function to check every incoming or outgoing packet and decide to accept or to discard it. Such a packet source IP address, destination IP address, source port number, destination port number, and protocol type, with a certain number of fields can be seen as a tuple.

The function of a firewall is conventionally specified as a sequence of rules. Each rule in a firewall is of the form

<predicate> ⟶ <decision>

The <predicate> of a rule is a boolean expression over some packet fields together with the physical network interface on which a packet arrives. For simplicity, it is assume that each packet has a field containing the identification of the network interface on which a packet arrives. The <decision> of a rule can be accept, or discard, or a combination of these decisions with other options such as a logging option. Now it's a rule <decision> that would be easy for either to accept or reject. Only then (iff) packet satisfies predicate rule if a packet matches a rule. A firewall is often in conflict rules. They also overlap and conflict IFF firewall rules in two separate decisions are made. A firewall overlap two rules can match both rules is that at least one packet iff. Due to the conflict between the rules, more than a pack a firewall rule, and a packet matches the rules may be different decisions can match. To resolve the conflict, the decision for each packet that matches the packet (i.e., highest priority) rule decision. As a result, the firewall rules are sensitive to the order. Each packet is a firewall rule that at least one match to ensure a firewall rule predicate past is usually a tautology. A firewall is generally the fundamental rule of the previous regime is called.

Functions of Firewall:

Firewall is the most essential tool while user is connected to the network and making communication on the network with the other remote devices or network devices. So the firewall is having the following functions that make the user free from worms, bugs, malicious files:

1. Firewall scan each & every packets over the network.
2. Modern firewall gives the full specification while connecting to the new network.
3. Flexible to define the rules on the network according to user requirement.
4. Prevents from malicious files e.g. Trojan Horse, etc.

1.1 Rule Format

To create a firewall rule in the firewall following syntax is followed:

<Order><protocol><source ip><source port><destination ip><destination port> <action>

Table 1: Description of firewall rule

ORDER	The number given to the rule at which would be stored in firewall rule and policy.
PROTOCOL	What type of protocol the packet is carrying.
SOURCE IP	From where the packet is coming?
SOURCE PORT	What is the port number for the source?
DESTINATION IP	Where the packet is reaching?
DESTINATION PORT	Port number for the destination
ACTION	Accept or Deny (According to predefined action in the rule set.)

Order is the number given to the rule at which it would be stored in the firewall rule, protocol is for what type of protocol the packet is carrying, source ip having from where the packet is arriving, source port is port number for the source. Destination ip & destination port are related to packet reached and port number for destination respectively (Table 1).

Table 2: Example of Firewall Rule

ORDER	PROTOCOL	SRC_IP	SRC_PORT	DST_IP	DST_PORT	ACTION
1.	TCP	140.14.2.*	Any	*.*.*.*	75	Accept
2.	TCP	*.*.*.*	Any	160.123.1.2	75	Deny
3.	UDP	150.3.4.65	Any	161.23.12.32	ANY	Accept
4.	TCP	140.92.34.*	Any	*.*.*.*	45	Accept
5.	TCP	140.92.34.*	Any	123.42.134.54	80	Accept
6.	UDP	145.13.54.65	Any	161.120.33.40	75	Deny
7.	UDP	*.*.*.*	Any	161.120.33.40	75	Deny

Action is performing according to the defined in the rule set i.e. either accept or deny. Now once the rule set is defined in the rule set for the firewall policy, it doesn't mean that it would not be to change it. Yes the rules of firewall could be change as per the requirements. By changing the rules or just not updating the rules in the firewall rules the anomalies has been created.

1.2 Anomalies in firewall rules

Firewall is the security tool to protect from unauthorised networks, bugs, worms & other malicious files that might be harmful to the user system. The firewall is totally dependent on their defined rules. As much as strong rule is defined according to that the firewall is performing the operations and providing more protection to the user. So hundreds or can say thousands of rules are defined to make an effective firewall system, as result it is very difficult to arrange the rules according to their correct position. It may leads to create erroneous within the set of rules that are responsible to not perform the rule according to their performance. If these errors are occurred then the anomalies are created which have to be detected & removed from the firewall rule set.

By changing rules there are five anomalies has been detected at present named as:

1. Shadowing Anomaly
2. Correlation Anomaly
3. Generalization Anomaly
4. Redundancy Anomaly
5. Irrelevance Anomaly

1.2.1 Shadowing anomaly:

Shadowing anomaly comes when one rule matches all the incoming packets and other rules does not get any chance to match the incoming packets. It means that a big rule matches all the incoming packets and shadowed the adjacent rules to perform their actions.

From the Table 2, if the rule 1 is matched all the packets and do not pass the packets further to rule 2, it means the rule 1 is shadowing to rule 2. And the rule 2 is not activated. From this anomaly the various malicious packets are arrived and it is a critical error in the firewall policy. One more important thing to consider is that if there any inclusive or exclusive match found between the two rules then shadowing anomaly created. The superset rule must be come after

subset rule. It is necessary that if such type of anomalies has been detected then an alarm should be ring to alert the network administrator.

1.2.2 Correlation anomaly:

When the incoming packets has been matched by the two rules and the action performed by them is different then it would be known as correlation anomaly. Lets take the example from the table 2 in which if rule 1 and rule 3 are allowing the HTTP traffic coming from the address 140.14.2.12 and reaching to the address 160.123.1.2 then the packet is discarded but if the order of the rule is reversed then the packet is accepted. So it should be necessary that the order of the rule must be correct order to avoid the anomalies.

1.2.3 Generalization Anomaly:

The action of the rules are different but if the order of the rule is reversed then action is also be changed and the rule would be shadowing to another rule. So the super set is known as the General rule.

It would be easily understandable by the example, from the table it is clearly shown that rule 1 and rule 2, rule 1 is generalization of rule 2, for any reason if the order of the rule is changed then the action is also changed and it effects on firewall policies and its performance. If between the rule there is an inclusive match has been found then the superset rule should be come after the preceding subset rule. This anomaly has been considered as an anomaly warning it makes the defined or specific rule makes an exception of the general rule.

1.2.4 Redundancy Anomaly:

A rule is redundant if and only if there is another rule that matches the same packet and performing the same action then if it remove from the rule set then there is no effect on firewall rule set. Rule 4 is redundant to rule 5 and rule 6 is redundant to rule 7, it means if the rule 6 and rule 4 are deleted from the rule set of firewall then there is no effect on the firewall policies and their performance. But only effect of this anomaly is that taking space and making the time consumable firewall which degrades the performance of the firewall up to some extent.

1.2.5 Irrelevance Anomaly:

At a desired interval of time the rule has not matches any packet then it would be known as irrelevance anomaly.

Anomalies generally occurs when there is updating the rules of the firewall because while updating the position of the rules get disturbed and also either may increase the efficiency or decrease the efficiency. But manually it is very difficult to detect the anomalies and also to resolve it because a firewall is having thousands of rules to check it.

1.3 Tools for detecting firewall anomalies

There are various tools that are helpful to detecting the firewall anomalies. Some common popular tools are as follows:

1. FPA (FIREWALL POLICY ANALYZER)
2. FIRMATTO
3. FAME (FIREWALL ANOMAY MANAGEMENT ENVIRONMENT)
4. GRID
5. FIREMAN

These tools are helpful to detecting the anomalies as well as to resolve them. Some firewall tools are matching the incoming packets according to prototype on packet's header then further matching the source ip and then destination ip. After that the packet has been matched with the rules then the desired action is going to be performed which are predefined in the rule set of firewall.

The firewall tools providing the facilities like Editing, Adding, Deleting, Modification etc. In Editing, it must be compulsory that the order of a rule should be placed on a proper position while editing, so that no anomalies would be created. And in insertion while adding the new rule in the rule set it must be kept in mind that other rules are not getting disturbed so that it is easy to avoid the anomalies. Deleting, by deleting the rule in such a way that firewall policies would not be effected and efficiency as same as before. Modification, make the changes in firewall rules positions that includes the updation to maintain or increase the efficiency of the firewall. Thousands rules are created in a firewall so it would be very difficult to check every rule and make correction. Table 3 presents the comparison of different tools available

1.4 Firewall Anomalies Detection Tools Comparison

Table 3: Comparison of firewall tools on the basis of anomaly detection.

TOOLS → / ↓ ANOMALIES	FIRMATTO	FIREMAN	FANG	FAME	GRID
SHADOWING	YES	YES	YES	YES	YES
CORRELATION	YES	YES	YES	YES	YES
GENERALIZATION	YES	YES	YES	YES	YES
REDUNDANCY	YES	YES	YES	YES	YES
IRRELEVANCE	NO	NO	NO	NO	NO

While designing the firewall rules the major three types of problems occurs and that are:

1. The Consistency Problem
2. Completeness Problem
3. Compactness Problem

Consistency Problem: It is very difficult to order the rules correctly so that the performance will enhanced.

Completeness Problem: It defines about to ensure that thorough consideration for all the incoming packet/outgoing packet or just say the complete traffic.

Compactness Problem: Compactness Problem which states that it is very difficult to keep the rules as a small which means that some rules are may be redundant and some rules are lies on the other rule.

The comparisons have been made according to properties of tools, it is clearly shown in the table:

Tools → / ↓ Properties	Firmatto	Fireman	Fang	Fame	Grid
User interaction	No	Yes	Admin	Admin	Admin
Relationship among the rules	Good	Not good	Good	Good	Not good
Network Topology	Dependent	Independent	Independent	Independent	Independent
Updation of rules	No	Yes	Yes	Yes	No
Processing time of packets	High	Moderate	Moderate	Low	High
Performance	Moderate	Moderate	Low	High	Low
Accuracy	Low	High	Low	High	High

Table 4: Comparison of firewall tools on the basis of their properties

1.5 Firewall Policy Modeling

Firewall rules firewall policy analysis and modelling of relationships such as anomaly detection and policy management techniques to design editing is required. Modeling firewall policy rules define a relationship between creating inconsistencies helps to prevent. Relations between any two rules are the anomaly is created. If the relationship is defined in the section below.

1.5.1 Formalization of Firewall Rule Relations

The model is designed to strengthen the firewall policy, so the proper relationship between the need to make the rules. In the section below, may exist between the rules of filtering all the possible relationships defined, and no other relationship exists. Governance functions of network filtering rules based on the regions as well as the independent determination of these relations.

Definition 1 — Rules R_1 and R_2 are completely disjoint if every field in Rx is not a subset nor a superset nor equal to the corresponding field in Ry.

Formally, $R_1 \Re CD R_2$, if

$$\forall i: R_1[i]\ R_2[i]$$

where $\in \{\subset, \supset, =\}$,

$$i \in \{protocol, s\_ip, s\_port, d\_ip, d\_port\}$$

Definition 2 — Rules R_1 and R_2 are exactly matching if every field in R_1 is equal to the corresponding field in R_2.

Formally, $R_1 \Re EM R_2$ if

$$\forall i: R_1[i] = R_2[i]$$

where $i \in \{protocol, s\_ip, s\_port, d\_ip, d\_port\}$

Definition 3 — Rules R1 and R_2 are inclusively matching if they do not exactly match and if every field in R1 is a subset or equal to the corresponding field in R_2. R_1 is called the subset match while Ry is called the superset match.

Formally, $R_1 \Re IM R_2$ if

$$\forall i : R_1[i] \subseteq R_2[i]$$

and $\exists$ j such that :R_1 [j] $\neq$ R_2[j]

where i, j $\in$ {protocol, s_ip, s_port, d_ip, d_port}

Definition 4 — Rules R_1 and R_2 are partially disjoint (or partially matching) if there is at least one field in R_1 that is a subset or a superset or equal to the corresponding field in R_2, and there is at least one field in R_1 that is not a subset and not a superset and not equal to the corresponding field in R_2.

$R_1 \Re PD R_2$ if

$\exists$ i, j such that R_1 [i] R_2[i] and R_1 [j] R_2[j]

where $\in$ {$\subset$, $\supset$, =},

i, j $\in$ {protocol, s_ip, s_port, d_ip, d_port}, i $\neq$ j

Definition 5 — Rules R_1 and R_2 are correlated if some fields in R_1 are subsets or equal to the corresponding fields in R_2, and the rest of the fields in R_1 are supersets of the corresponding fields in R_2.

$R_1 \Re CR_2$ if

$\forall$i:R_1 [i] R_2 [i] and

$\exists$ j, k such that :R_1 [j] $\subset$ R_2[j] and R_1[k] $\supset$ R_2[k]

where $\in$ {$\subset$, $\supset$, =},

i, j, k $\in$ {protocol, s_ip, s_port, d_ip, d_port}, j $\neq$ k

The following table has been designed to easily understand of anomalies that what relationship has been created to lead or created the defined anomalies.

Anomalies	Firewall Rule Relation
Shadowing Anomaly	Inclusive or Exact Match
Correlation Anomaly	Correlated Match
Redundancy Anomaly	Redundant Match
Generalization Anomaly	Partially Disjoint

Table 5: Anomalies and the relationships among the rules.

Shadowing anomaly is created when the following conditions matches either one or both

$$R_1 \text{ [order]} < R_2 \text{ [order]}, R_1 \Re EM R_2, R_1 \text{ [action]} \neq R_2 \text{ [action]}$$

$$R_1 \text{ [order]} < R_2 \text{ [order]}, R_2 \Re IM R_1, R_1 \text{ [action]} \neq R_2 \text{ [action]}$$

In Redundancy Anomaly the conditions are as:

$$R_1 \text{ [order]} < R_2 \text{ [order]}, R_1 \Re EM R_2, R_1 \text{ [action]} = R_2 \text{ [action]}$$

$$R_1 \text{ [order]} < R_2 \text{ [order]}, R_2 \Re IM R_1, R_1 \text{ [action]} = R_2 \text{ [action]}$$

Whereas rule R1 is redundant to rule R2 if the following condition holds:

$$R_1 \text{ [order]} < R_2 \text{ [order]}, R_1 \Re IM R_2, R_1 \text{ [action]} = R_2 \text{ [action] and}$$

$$R_3 \text{ where } R_1 \text{ [order]} < R_3 \text{ [order]} < R_2 \text{ [order]},$$

$$R_1 \{\Re IM, \Re C\} R3, R_1 \text{ [action]} \neq R_3 \text{ [action]}$$

Now in Correlation Anomaly following condition is to be satisfy:

$$R_1 \Re C R_2, R_1 \text{ [action]} \neq R_2 \text{ [action]}$$

In Generalization Anomaly following condition to be fulfil:

$$R_1 \text{ [order]} < R_2 \text{ [order]}, R_1 \Re IM R_2, R_1 \text{ [action]} \neq R_2 \text{ [action]}$$

Chapter 2

REVIEW OF LITERATURE SURVEY

When inserting or modifying the rule of a firewall requiring the thorough analysis and making a proper space for the new rule to avoiding the anomalies. Al-Shaer S.E., Hamed H. in 2004 presented a set of techniques and algorithms that are helpful to automatic detect the anomalies and also providing the facility of insertion, removal and modification [1]. All this work has been done on Firewall Policy Advisor Tool. Firewall Policy Advisor is helpful to firewall policy without the analysis of the filtering rules. By the help of tree-representation it was helpful to make the relations among rules and policies. Firewall Policy Advisor which are corporating two management tools and that are Policy Analyzer, it is used to identify conflicting, shadowing, correlated and redundant rules. And this analyzer is not be able to automatically fix the rule anomaly instead of that an alarm has been used and second is Policy Editor, in this management tool deals with insertion, modification and deletion. The editor automatically determining the position of rule to insert.

While making the rules for a firewall the basic three main problems are coming forward i.e. consistency problem, completeness problem and compactness problem. The consistency problem deals with the difficulty to ordering the rules in a correct way. The completeness problem defines that get thorough knowledge of all types of traffic. Compactness problem which states that it is very difficult to keep the rules of firewall as a small the reason behind is that some of them are redundant and some may be combined into another one.

Gouda G.M. & Liu X.A. in 2006 developed a structured firewall design to overcome the problem and to increase the efficiency of the firewall rules two algorithms has been used and that are FDD reduction (Firewall Decision Diagram) and FDD marking[2]. The algorithms are extensible to other rule based systems for example IPsec rules.

Mohsen Rezvani and Ramtin Aryan in 2009[3] presented a formal language for specification of security policy in firewalls. Languages, specify the security policy, based on simple inconsistencies and gross anomalies are translated to the functional logic formulas. Also researchers designed and specified to detect anomalies in the policy based on proving the theorem is applied to a device. In addition, the formal model, the two algorithms to resolve inconsistencies in the policy are presented. These algorithms security policy without changing

the minimum number of regulations.

An Internet is providing the communication medium through the network to connect or communicate with other systems globally. Chaure R. & Shandilya K.S. in 2010 showed their concern for security [4]. To providing the protection on to the network, firewall is the best tool which comes on to our mind. As the security threats are increasing then it should also be get compulsory that updating the rules and policies. The rules are placed in a proper manner so that the processing would be fast and error-free. The updation of rule or by change of rule's position it must be kept in mind that the firewall should not be decreased. The rules are written in a proper format. Some rules are defined according to the time parameter within the ruleset. The irrelevance anomaly has not been yet detected and due to that the size of the rule increased. The type of rule and policies have been defined on to firewall, according to that firewall providing services. Hu H., Ahn G.J. & Kulkarni K. in 2010[5] proved that an anomaly management framework is adopting a rule-based segmentation technique which used to identify the anomaly and resolve them is reliable and best. The feasibility and applicability of the framework that has been developed by them, get through the proof-of-concept prototype visualization-based firewall policy analysis tool that is called FAME. The rule-based segmentation has been used get effective and efficient anomaly analysis. FAME deals with the system administrators to enabling an assurable network management.

Hongxin Hu, Gail-Joon Ahn, and Kulkarni K. in 2012 [6] have proposed an innovative policy anomaly management framework for firewalls, adopting a rule-based segmentation technique to identify policy anomalies and derive effective anomaly resolutions. In particular, policy inconsistency about providing an intuitive cognitive sense, vocal technique, a grid-based representation. And also manages firewall anomaly Environment (FAME), a visual analysis tool based firewall policy to discuss the implementation of a proof-of-concept. In addition, researchers also discovered that our approach and firewall policies through rigorous experiments can resolve inconsistencies in how efficiently performed.

The service providing by the firewall depends on rules that are present in policies. Because of lack of systematic analysis mechanisms and the tool it becomes very difficult task rules anomalies. Sriram G.G., SwarnaSri B.I., RamaDevi N., Gouthari K., Arjun Kumar S. in March 2013[7] identified that the detection and resolving firewall anomalies always a challenging job for the researcher. The rule-based segmentation is the best way to find the anomalies and resolve them. The part of the visualization based firewall policy tool called FAME. A novel anomaly management framework algorithm has been designed for detection and resolving of

firewall anomalies. The rule-based segmentation technique is much more reliable to use and easily find the anomalies.

Aubarasan A., Balasubramani G., Madhan C., Naveenkumar. P, Mrs Nithya N.S. in April 2013 [8] have detected the anomalies using rule-based segmentation technique which effectively work. It not only detect the anomalies but also to resolve them. The network space packet is also divided according to firewall policy in the form of disjoint space packets segments. The segment has been divided is associated with unique rule set of firewall. Also proposed a flexible conflict resolution method to keep the firewall rule more efficient and get anomaly free rule set. Moreover, it making the network more protected. First, of all the method has been proposed to a framework that automatically detect the anomalies and also resolve them. After that created a static method to remove inconsistencies, inefficiencies & policy violations. In future, to increase the performance of firewall rules and making to auto healing, to work on cloud based segmentation to resolve the anomalies query through the online to increase security concern.

Lubna K, Robin Cyriac April 2013[9] have studied about the representation of firewall policy anomalies techniques. Generally two types of technology and grid-based representation based on the policy tree representation, which is a rule-based system that are split are discussed. Grid-based representation techniques and approaches in order to overcome the limitations of the policy tree representation has been discussed.

Prof. Chandre R.P., Surve R.R., Badhan R.S., Surve B.A., Mane T.V. March 2014[10] made analysis that the internet access users have increased very rapidly. But the intention of some users are for the fraudulent purpose. So it is very necessary to keep the system updated and using the best security tools for the protection. Attacks are increasing over the network that means if the 60% users perform secure online transaction/operation but 40% get victim of security attacks because of not the complete knowledge or software not updated or no security tools have been used while online operations. So the firewall is the best security tool over the network. It is very difficult to get actual of the user who is using network in an unauthorised manner but it could protect it over the network by the help of firewall from an unauthorised network or even packets. Firewall also helps to identifying normal and abnormal behaviour of the user on the network and prevents from malicious activities. To resolve the conflict occurred on to the network, the firewall is helping to that. The tools i.e. FIREMAN has been used also determines the groups that are correlated. To make the difference between real user and fraud users and also the huge amount of web logs get easily managed. Taking the operation

permission i.e. allow/deny from the user it means that the tool is user-interacted and when the firewall rule detected the malicious code or packet it sends to the block state.

Various Firewall Management Environment Tools has been developed to detect the anomalies among the rules & policies. The tools that are named as FIREMAN, GRID, FAME, FANG & FIRMATTO but still they are having shortcomings either in user interaction or in performance & accuracy. It was clearly notified that no tool is perfect to detect all the anomalies in firewall rules & policies.

Like Firmatto was the first tool to detecting the anomalies, its performance was moderate & overall is good but it's not a user interacted and flexible to change the rules. Another tool is Fireman, which is user based and accuracy was high for detection. But Fireman is not taking responsibility to make better relationship among the rules. Then Fang tool was independent on network topology & it is updated the rules but the performance & accuracy is low. Fame tool is generally designed for administrative based use & updation of rules are required. Performance, accuracy is high but the processing time of packets is high. But overall it is good among all the tools. And Grid was not that much effective to detecting the anomalies.

Designed the algorithm to detecting the most commonly anomalies & also to increase the performance of the firewall. First of all set the rules in an unordered so that to create the anomalies. Then finding the exact position of the rule & then placed the rule according to the protocol, source ip & port as well as for destination. And this happen by reordering of rules. A policy tree is helpful to find the exact position of the rules while inserting a new rule so that to avoid the anomalies in the rule set. First the packet is matches protocol in the policy tree, & then move downwards to matches its source ip & port after that comes to destination ip & port then matches the action(accept or discard) & finding the position of the rule in the rule set. By this it will be helpful to enhance the performance of the firewall.

Chapter 3

PRESENT WORK

3.1 PROBLEM FORMULATION

Anomaly detection tool & also a user friendly tool is Firewall Policy Advisor that helpful to detecting the anomalies in firewall. Firewall Policy Advisor Tool also helping to manage the firewall rules without prior analysis & it requires updating of rules after every transaction (online operation). But this tool or algorithm used is not helpful for detecting the irrelevance anomaly because it requires the complete knowledge of connectivity. The tree paths is to detecting the firewall anomalies, if the path of any rule gets overlap or can say coincides with the another rule there is an anomaly would be detected. And if the paths of any rule are not going to coincide with any other then there is no anomaly. The tool has been applied on small firewall rules, the processing time is average.

Moreover, generally three problems facing while designing the firewall rules i.e. consistency problem, completeness problem and compactness problem. A new method has been discovered and that is structured firewall design. Firewall decision diagram is an algorithm to detecting the anomalies among the rules. To overcome such problems structure firewall design has been used rather than any tool.

The total description have given over the firewall, their rules, format, anomalies, and types of anomalies and tools that are using now a day for detection and resolving the anomalies. How the evolution takes place over the internet and by that how the security concern has been increased. FIRMATTO software to detect the firewall anomaly but its performance is poor on large rules. It does not interacts with the user. One online tool is there to detect the anomalies online i.e. M-CUSUM to detect the firewall anomalies over the high speed network.

FAME is the best tool which is visualization-based firewall policy analysis tool. It is the best tool among all others which is having high performance and updation is required by which keep changes or can say updation helping to improve the efficiency of firewall rule and blocking rate against malicious packet or unauthorised network is much higher. The disadvantage of this tool is that yet it has not discovered irrelevance anomaly because of some limitations.

The firewall anomalies detection tool i.e. FIREMAN is having various limitations and that are:
1. It can only be detect pairwise anomalies.

2. It focuses only on the preceding rules but ignoring subsequent rules.
Because of these limitations generally FAME tool is used in anomaly management environment. The Binary Decision diagram is a data structure based used to detect the anomalies.
Rule Based Segmentation technique used to detecting anomalies and this technique has not been implemented on Firewall Policy Tool. That means rule-based segmentation itself an algorithm, along with that a grid based technique has been applied on a novel static analysis approach to checking the configuration of firewall.
The inbound and outbound rules which are helpful in network segmentation, in modern technology and to detecting the correlated rule and also rearranging the previous rule. The project generally made on the rule-based segmentation technique which is not only more accurate anomaly detection but also their resolution. The main criteria behind this is to control cyber-crimes and provides the security on private as well as public network. But the irrelevance anomaly is not detected by GRID tool and project. The project is containing the greedy algorithm & DES algorithm to detect the anomalies.

3.2 OBJECTIVES

After making complete analysis following objectives have been identified for the research work:

- To identify and compare common firewall anomaly management environment.
- To design algorithm to detect anomalies and to improve the efficiency of detection.
- To identify complete and adequate rule set for a firewall on which proposed algorithm can be applied.
- To implement proposed work for detecting anomalies in efficient way.
- To analyse the performance of proposed tool.

3.3 RESEARCH METHODOLOGY

Research Methodology for the proposed work requires the collection of data related to the research work. In order to meet objectives defined in previous chapter, step wise solution is proposed. Research started from the identification and selection of domain. Comparison of different firewall tools available is made after making the thorough study on them and by analysing their performance. Rest of the design is shown below in the form of chart

1. • Identifying And Selecting Problem
2. • Study about the firewall anomalies and their tools.
3. • To identify and comparing the firewall anomaly management environment.
4. • Alogrithm to detect the anomalies.
5. • To improve the efficiency of firewall.
6. • The alogrithm can be applied on the adequate rule set for a firewall performance.
7. • Implementing proposed algorithm on proposed work.
8. • Analysing the performance of proposed tool.

Chapter 4

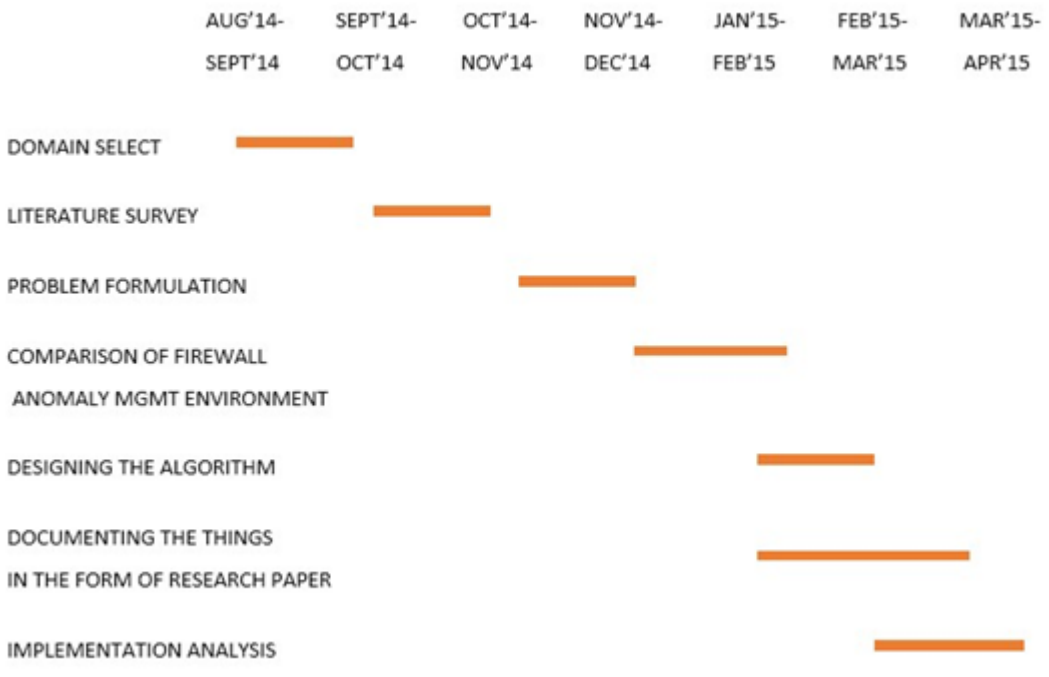
MONTHLY PROGRESS REPORT

4.1 WORKPLAN WITH TIMELINE

TABLE 6: Work plan

TASK	START MONTH	END MONTH
DOMAIN SELECT	AUGUST 2014	SEPTEMBER 2014
LITERATURE SURVEY	SEPTEMBER 2014	OCTOBER 2014
PROBLEM FORMULATION	OCTOBER 2014	NOVEMBER 2014
COMPARISON OF FIREWALL ANOMALY MGMT ENVIRONMENT	NOVEMBER 2014	DECEMBER 2014
DESIGNING THE ALGORITHM	JANUARY 2015	FEBRUARY 2015
DOCUMENTING THE THINGS IN THE FORM OF RESEARCH PAPER	FEBRUARY 2015	MARCH 2015
IMPLEMENTATION ANALYSIS	MARCH 2015	APRIL 2015

4.2 GANTT CHART



According to the timeline thesis work have been done, first selected the problem domain, then literature survey on the problem domain. After selecting the problem domain then designed the problem formulation. There are various tools are available to detecting the anomalies in the firewall rules, so compare them to get the best tools make out the drawbacks among them. After a thorough study design the algorithm by which help to detecting & resolving of anomalies in firewall rules & its policies. Then documenting the materials in the form of research paper so that it is easy to understand the whole research work in proper way & format. Then analysing the implementation by testing on various aspects of packets.

Chapter 5

RESULTS & DISCUSSIONS

Table 7: Firewall Rules & Policies

S.No.	Rule_Name	Protocol	Src_IP	Src_Port	Dest_IP	Dest_Port	Action
1.	R1	UDP	10.*.1.*	35	192.168.*.*	53	ALLOW
2.	R2	UDP	10.1.2.*	*	172.32.1.*	53	DENY
3.	R3	UDP	10.1.*.*	*	172.32.1.*	53	DENY
4.	R4	UDP	10.1.2.*	*	172.32.1.*	53	DENY
5.	R5	ANY	10.1.*.*	*	192.168.*.*	25	ALLOW
6.	R6	ANY	10.*.1.*	*	192.168.2.9	53	ALLOW
7.	R7	ANY	10.1.*.*	*	192.168.1.*	25	ALLOW
8.	R8	ANY	10.1.1.*	*	192.168.*.*	25	DENY
9.	R9	ANY	10.1.1.*	*	192.168.1.*	25	DENY
10.	R10	ANY	10.1.1.*	*	*.*.*.*	*	ALLOW
11.	R11	ANY	10.1.1.*	*	192.168.1.*	*	ALLOW

The figure shows about the firewall policy and the policy is having various rules to perform the operations. The rule name has been given to get identity then which protocol is being used to filter the packets, because on the basis of protocols filtration process is being processed. Source ip is defined, from where it comes from and port number should be given so that it clear that what type of service packet is having. Then define the destination address & port number to providing the services & set the action according to user facility whether to discard the packet or accept it. The following figure shows packet filtration and finding the anomalies and find the appropriate position of the rule to resolve the anomalies.

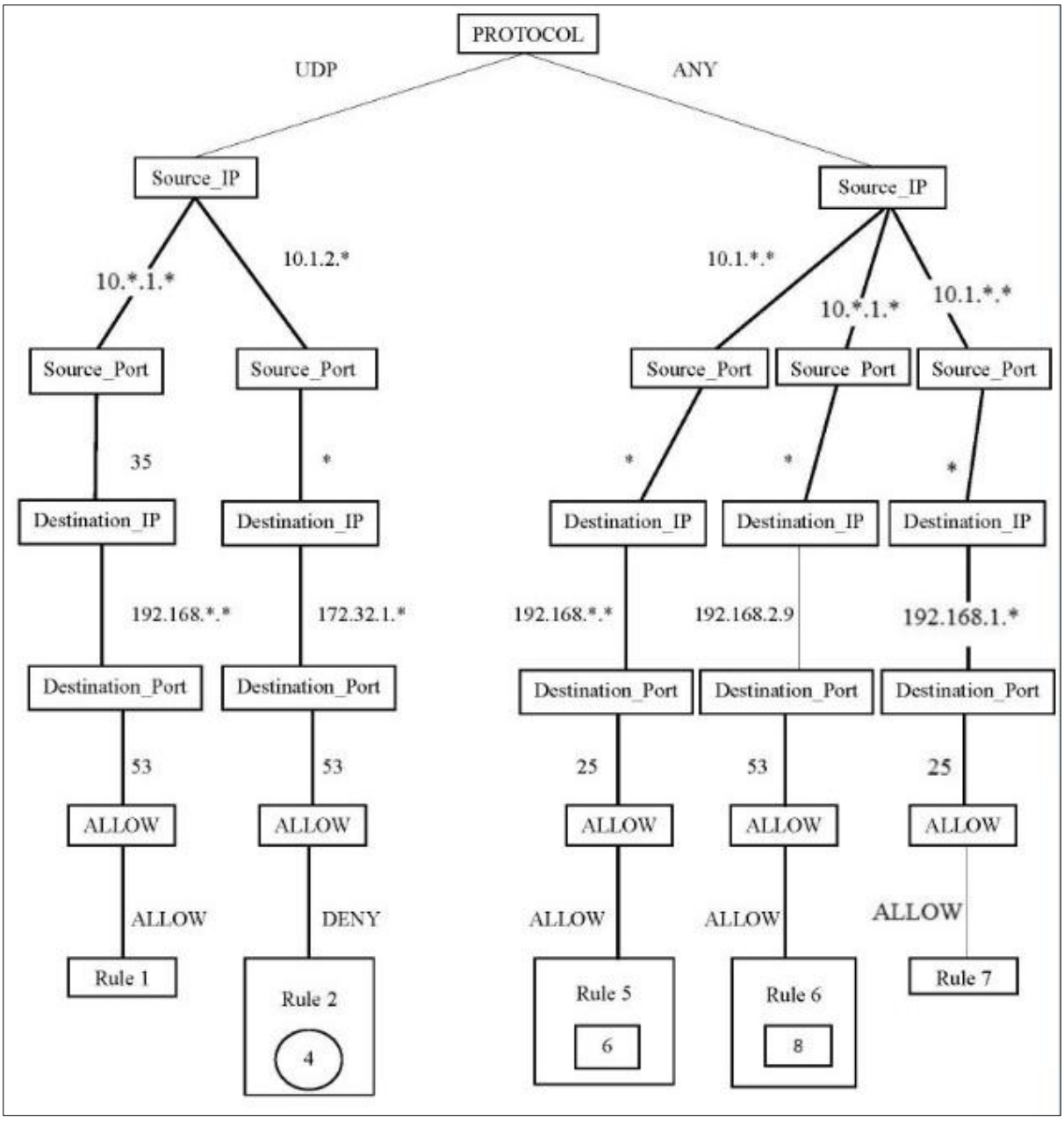


Figure 4: Policy Tree for Firewall Rule Set

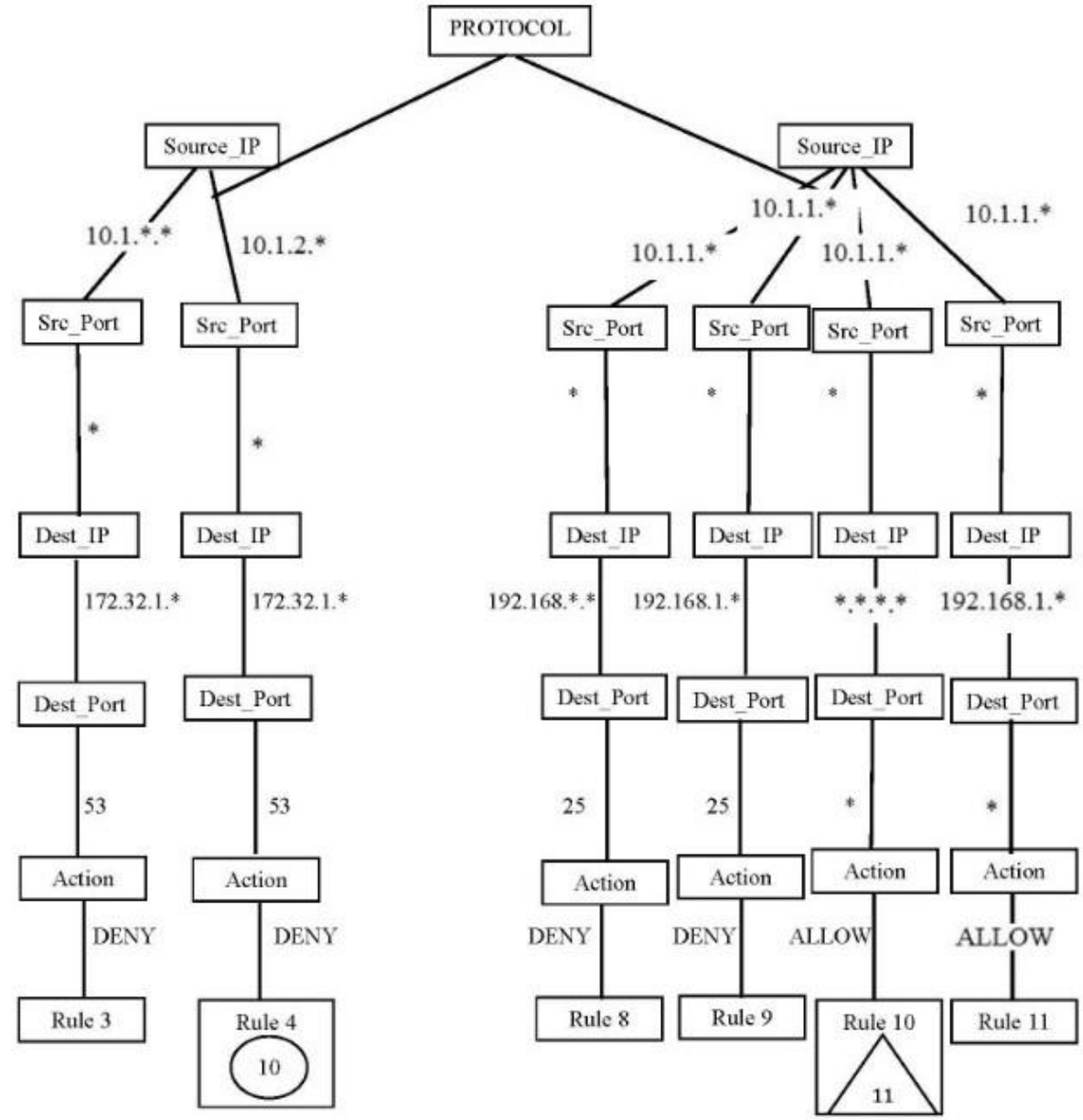


Figure 5: Policy Tree for Firewall Policy

Shadowing Anomaly

Correlation Anomaly

Redundancy Anomaly

From the above two figures (Figure 4 & Figure 5) it is clearly shown that the filtering is occurred on the basis of protocol. On the special protocols the source ip & their port numbers has been defined to more filter out the rules. Then destination ip & port number is liable for further filtration. And at the end action is performing, either to accept the packet or discard the packet. After all process is done, anomalies is generated in the rules. Shadowing anomaly is created between the rules R5-R6 & R6-R8. It means that Rule 5 is shadowing Rule 6, no chance to match the incoming packets to rule 6. And furthermore, Rule 8 is shadowed by the Rule 6. In the Redundancy Anomaly only two rules are get affected i.e. R10 & R11. Rule 11 is redundant to Rule 10 so if Rule 11 is being removed from the rule set & policy then there will be no effect on the firewall performance. Correlation Anomaly is occurring between the rules R2-R4-R10. Rule 2 is correlated to Rule 4 it means that the position of rule 4, some fields of R4 are the subset of R2 & vice-versa. Also R10 is redundant to R4, so the position of rules get changed then the performance might be get affected.

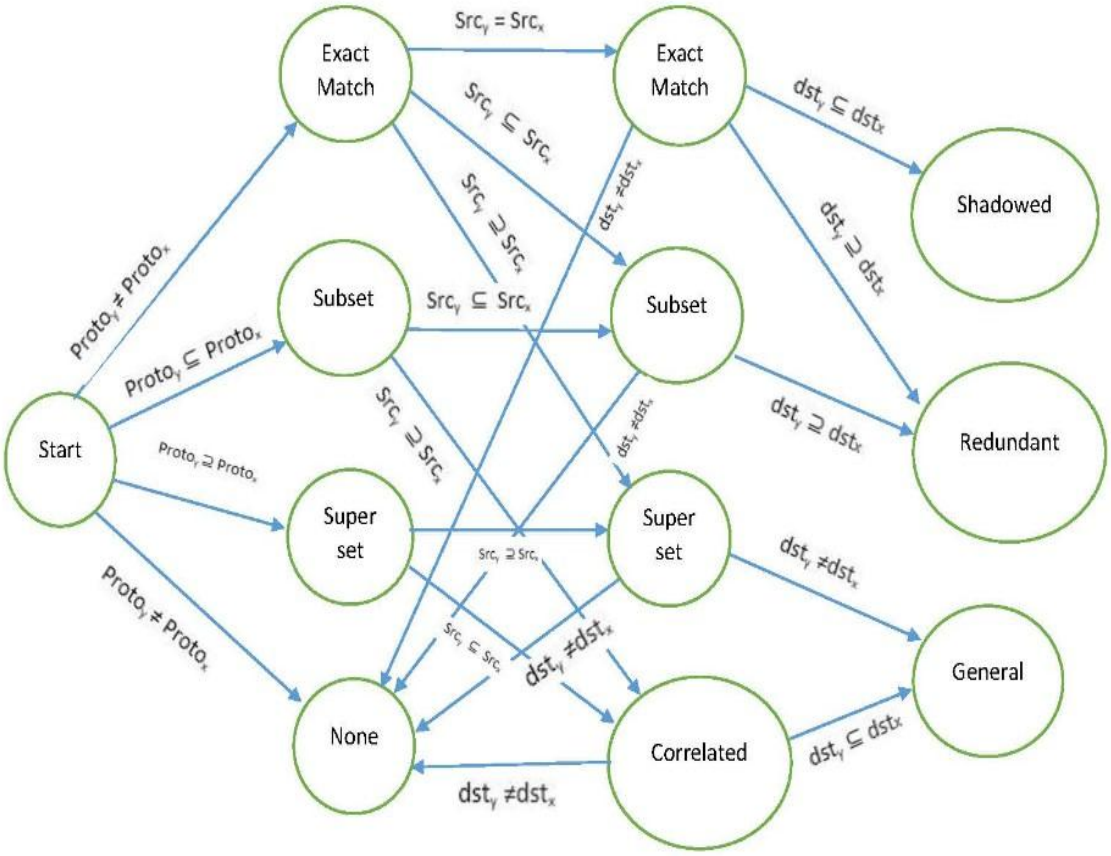
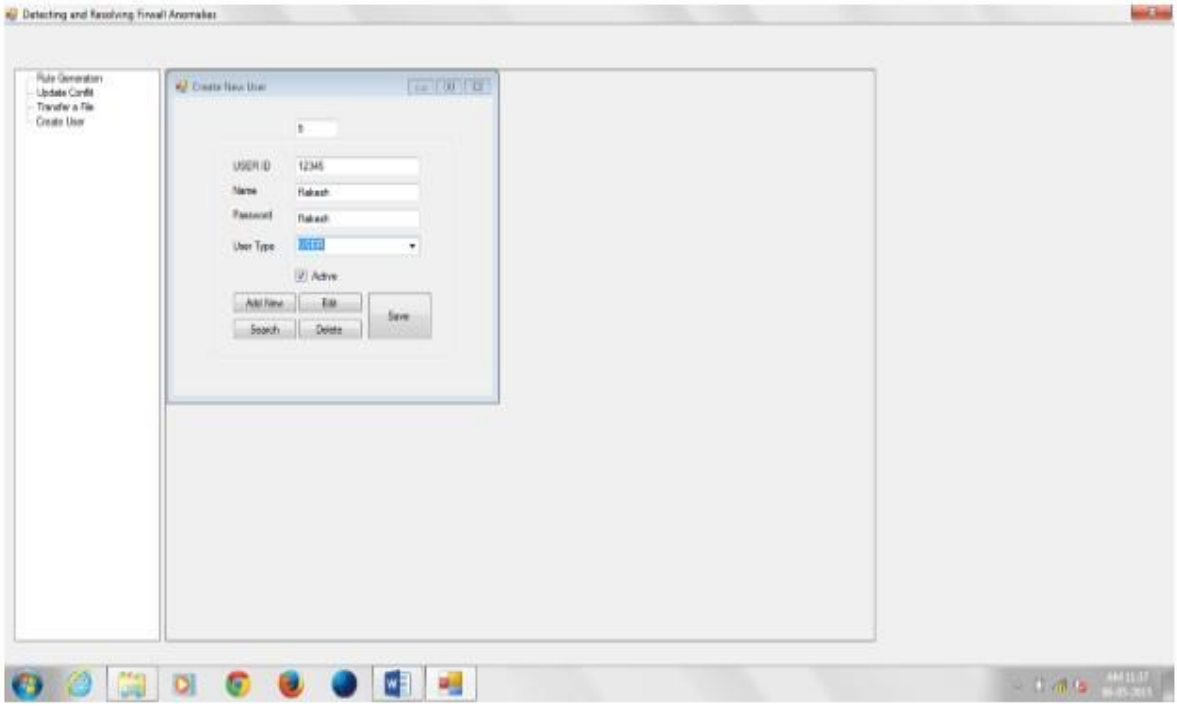


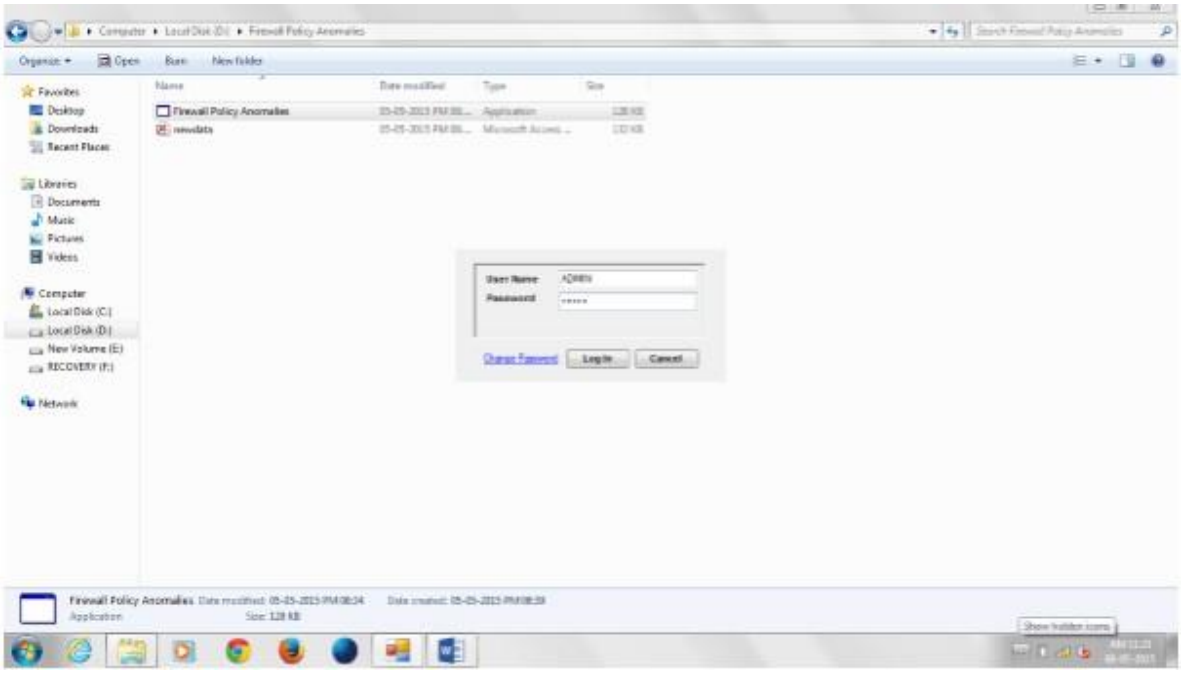
Figure 6: State Diagram to Show Relationships among Rules Responsible For Anomalies Generation

From the above (figure 6) it is clearly shown that when protocols are having the subsets, supersets to filtering of the packets. According to the subset, superset & exactly match Source & destination ip are divided and then action takes place either accept the packet or discard it. Here General is stands for Generalization anomaly. The state diagram gives the straight and brief description about anomaly generation.

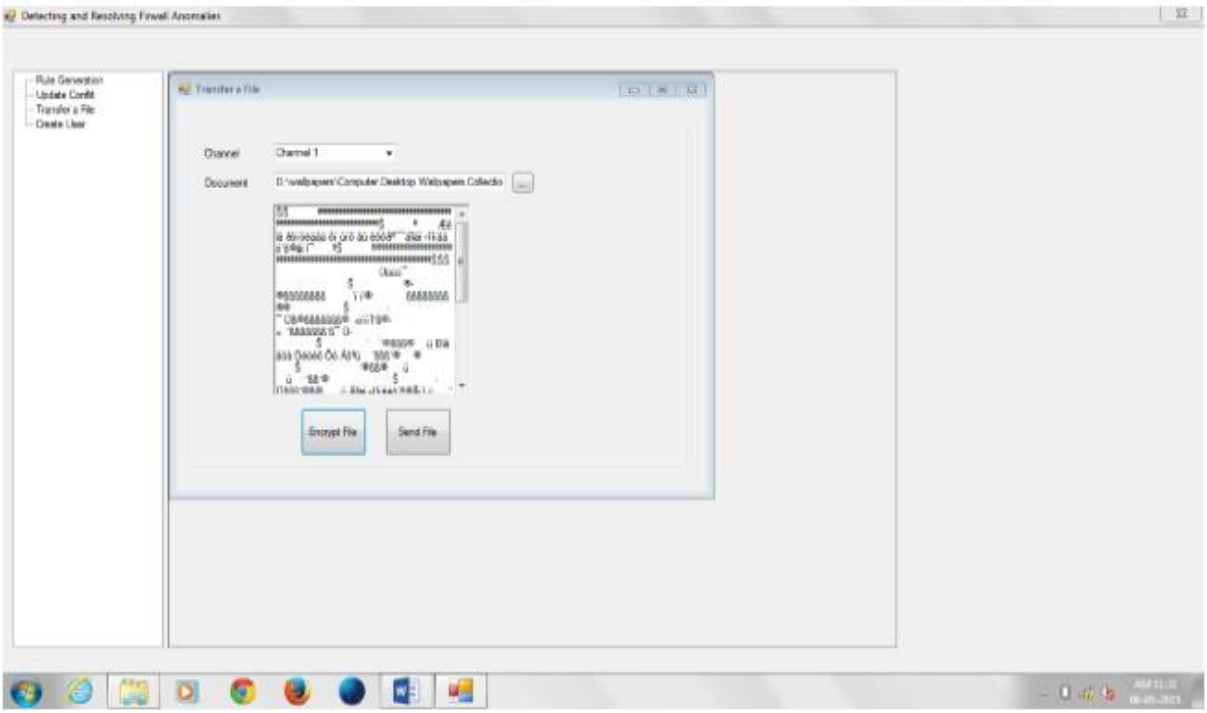
SCREENSHOTS



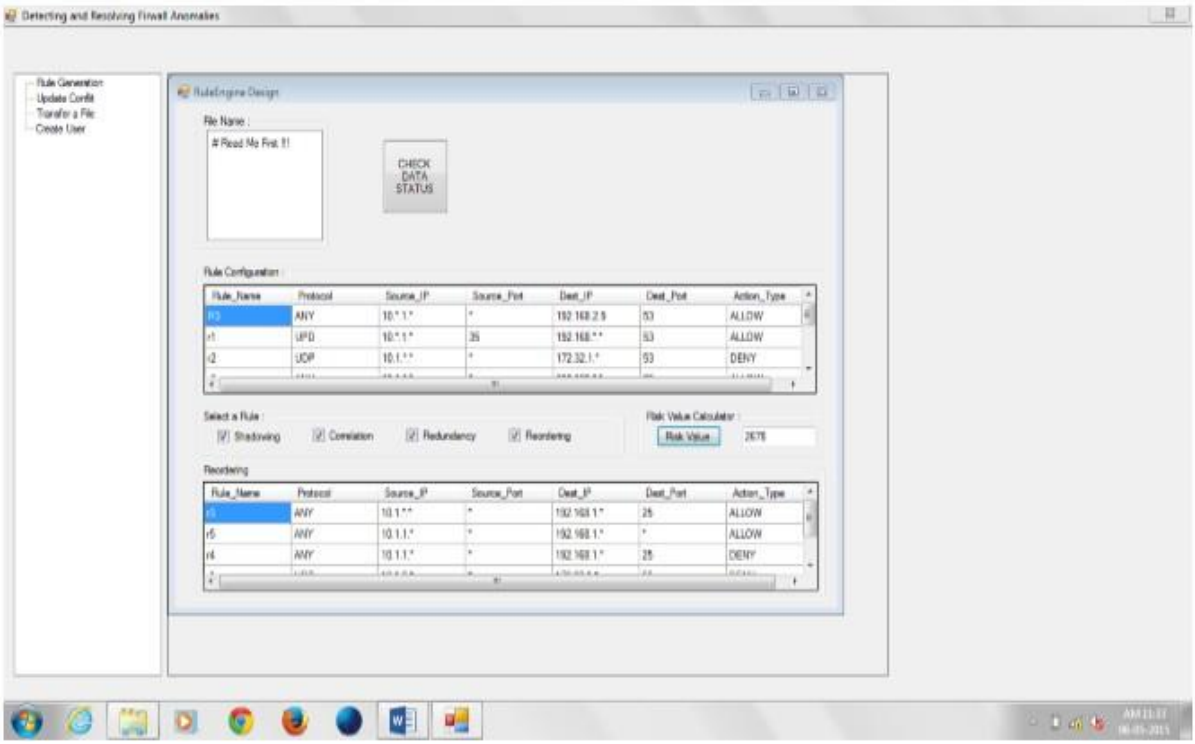
Screenshot 1: User Creation either as a User or Admin



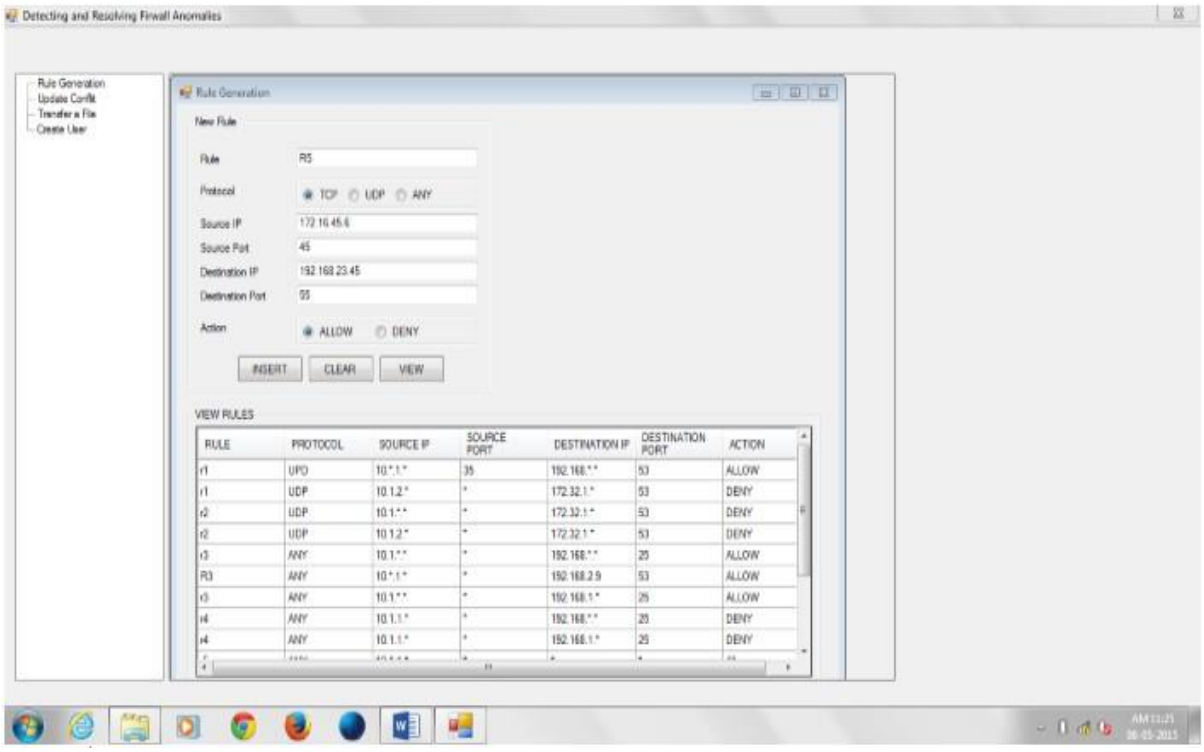
Screenshot 2: Login Page (User)



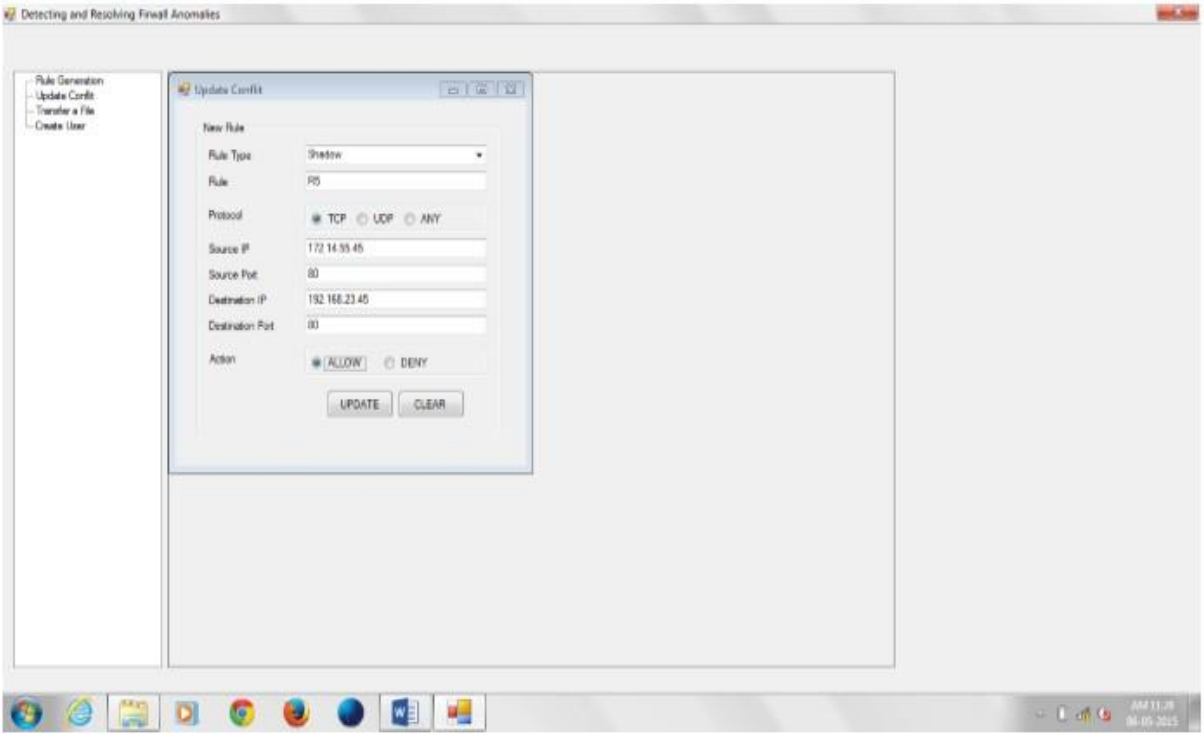
Screenshot 3: Encryption of File



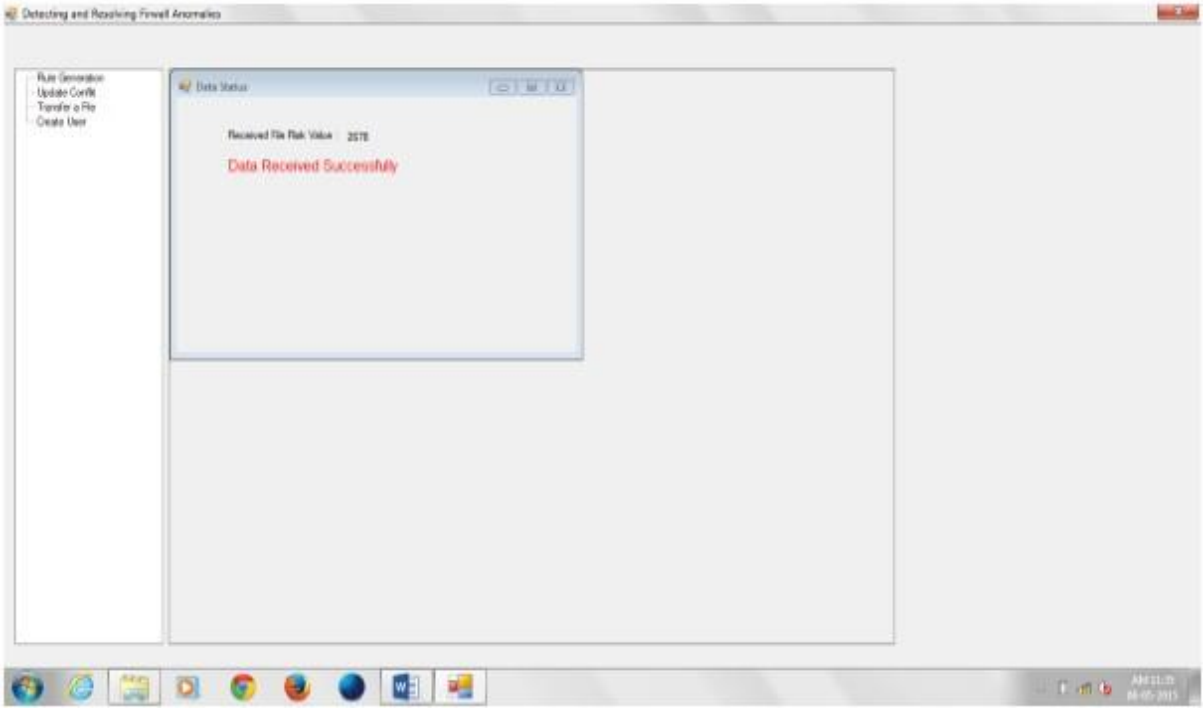
Screenshot 4: Rule Engine Design



Screenshot 5: Rule Generation



Screenshot 6: Update the Conflicted Rules



Screenshot 7: Data Status

Chapter 6

CONCLUSION & FUTURE SCOPE

Firewall protection, like any other technology, to provide appropriate security service requires proper management. Thus, just on the border of a network, the network must be a firewall, but the firewall cannot make it any more secure. One reason the firewall rules and rule because of the conflict is the complexity of managing potential network vulnerabilities. Presented in this paper firewall policy advisor purifying and anomalies to protect the firewall policy that offers a number of user-friendly tools. Administrator's policy analysis of the composition without filtering rules to manage a common firewall security policy advisors can use the firewall policy. Formally, define all possible firewall relations regime and used it to classify the firewall policy inconsistencies. Then by the help of tree, represented the firewall rule modelling information and relationships among the rules. Firewall Rule Engine represented the two tools which are Rule Advisor & Rule Editor.

Rule Advisor is used to identifying the conflicted rules, shadowing, redundant & correlation anomalies. When the user found any anomalies in the rule set then user can perform proper action. It is not automatically to detecting the anomalies among the rules.

Rule Editor is having the facility to rule insertion, modification and deletion. When the new rule is inserted it automatically finds the correct position in the rule set or policy. Any rule is deleted, then it shows the rule set and what the effect changes among the rule set.

Firewall policy adviser network firewall policies for the management of real-life was shown to be very effective. With respect to usability, the tool to discover anomalies in filtering rules written by expert network administrators. Policy analysis algorithm depends parabolically on the number of rules in the firewall policy. The discrepancy is very reasonable for finding practical firewall policies.

Future Scope

Firewall rule has to be assigned in such a way that no desired traffic blocked and no malicious packet is reached to the destination. The proposed tool to handle the distributed firewall policies. The query-based firewall policy analysis to enhance the graphical representation of

the firewall security policy. The tool is also used as an antivirus for the private or individual machine.

Chapter 7

LIST OF REFERENCES

Research Papers

[1] Ehab S. Al-Shaer and Hazem H. Hamed, DePaul University "Modeling and Management of Firewall Policies" 2004 IEEE eTransactions on Network and Service Management• Second Quarter 2004

[2]Mohsen Rezvani and Ramtin Aryan Department of Information Technology and Computer Engineering, Shahrood University of Technology, Shahrood, Iran "Specification, Analysis and Resolution of Anomalies in Firewall Security Policies" World Applied Sciences Journal 7 (Special Issue of Computer & IT): 188-198, 2009 ISSN 1818.4952 © IDOSI Publications, 2009

[3] Mohamed G. Gouda, Alex X. Liu Department of Computer Sciences, The University of Texas at Austin, Austin, TX 78712-0233, United States "Structured firewall design"

[4] Rupali Chaure and Shishir K. Shandilya "Firewall anamolies detection and removal techniques – a survey" International Journal on Emerging Technologies 1(1): 71-74(2010)

[5] Hongxin Hu, Gail-Joon Ahn and Ketan Kulkarni Arizona State University Tempe, AZ 85287, USA "FAME: A Firewall Anomaly Management Environment" SafeConfig'10, October 4, 2010, Chicago, Illinois, USA.

[6]Hongxin Hu, Gail-Joon Ahn & Kulkarni K. Members IEEE, "Detecting and Resolving Firewall Policy Anomalies" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 3, MAY/JUNE 2012

[7] G. Ganesh Sriram, B. I. Swarna Sri, N.Rama Devi, K. Gouthami, S. Arjun Kumar Dept. of CSE, Srinivasa Institute of Engineering & Tech., NH-216, Cheyyeru, AP, India "Anomalies Detection and Recovery in Firewall Policies" IJCST Vol. 4, Issue 1, Jan - March 2013

[8] Anbarasan.A, Balasubramani.G, Madhan.C, Naveenkumar.P, Mrs N.S.Nithya Department Of Computer Science and Engineering, Anna University Chennai, India, Assistant Professor, Department Of Computer Science and Engineering, K.S.R. College Of Engineering, Tiruchengode, India "Detecting and Resolving Firewall Policy Anomalies Using Rule-Based Segmentation " IJCSMC, Vol. 2, Issue. 4, April 2013, pg.134 – 137

[9]Lubna K., Robin Cyriac, Dept. of CSE, Rajagiri School of Engineering and Technology, Kochi, India "A Study on Firewall Policy Anomaly Representation Techniques" International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 4, April 2013

[10] Prof. Pankaj R. Chandre, Rakesh R. Surve, Suraj R. Badhan, Aniket B. Surve, Vikey T. Mane Department of Computer Engineering Sharadchandra Pawar College of Engineering Dumberwadi (Otur), Pune, Maharashtra, India "Anomalies of Firewall Policy Detection and Resolution" Rakesh R. Surve et al Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 3(Version 1), March 2014, pp.696-701

Books:

Cryptography and Network Security Principles and Practices, Fourth Edition By William Stallings (2005) Pg. 621.

Next-Generation Firewalls for Dummies by Lawrence C. Miller, CISSP (2011).

Building Internet Firewalls Elizabeth D. Zwicky, Simon Cooper & D. Brent Chapman Second Edition, June 2000.

Websites:

https://www.en.wikipedia.org/wiki/Firewall_(computing)

https://www.webopedia.com/TERM/F/firewall.html

https://www.searchsecurity.techtarget.com/definition/firewall

https://www.slideshare.net/Alihabeeb/detecting-and-resolving-firewall-policy-anomalies-2

Chapter 8

APPENDIX

8.1 GLOSSARY

1. Action: Performed by the rule set that are defined in the firewall either accept or deny.
2. Anomaly: The error occurring when changing the rule set order or definition.
3. Compactness: While designing the rule set it occurs, the rule set may be redundant or lies on other rules.
4. Completeness: Examining the complete network traffic.
5. Consistency: Difficult to set rule in a proper order to function efficiently.
6. Destination: The reaching point where source wants to send the packet.
7. Firewall: The security guard to protect against the unauthorised network and worms.
8. Firewall Management Environment: It is just tools to help to avoid the anomalies and make the firewall more efficient.
9. HTTP: Http stands for Hyper Text Transfer Protocol for the communication over the web.
10. Internet: Providing the communication medium to connect the remote devices over the network.
11. Policy: The defined rule set in a firewall.
12. Port: Port are important because according to the port number defined with the packet, according to that the services are provided.
13. Protocol: How the packet is going to be transmitted over the network for communication.
14. Router: Hardware device which helps to forward the packet over the network.
15. Rule: The set of source ip, port number, destination ip and its port.
16. Source: From where the packet has been generated.
17. Transaction: Online operation perform over the network.

8.2 ABBREVIATIONS

IM: Implicit Matching

EM: Explicit Matching

PD: Partially Disjoint

CD: Completely Disjoint

C: Correlated