RESEARCH ARTICLE OPEN ACCESS

Anomalies of Firewall Policy Detection and Resolution

Prof. Pankaj R. Chandre, Rakesh R. Surve, Suraj R. Badhan, Aniket B. Surve, Vikey T. Mane

Department of Computer EngineeringSharadchandraPawar College of EngineeringDumberwadi(Otur), Pune, Maharashtra, India

{pankajchandre30, Surverakesh12, Badhansuraj177, Surveaniket07, vtmane7 } @gmail.com

Abstract

With the evaluation of internet, user's interaction is rapidly increases. Most of the user's intentions of accessing the websites are special target or someone's are going to turn on fraudulent purpose. Any system expects the well outcome as well as good and secure performance. Most of the users are handle untrusted data over network. If we assume that 60% user's performed secure operations but remaining 40% users are performs the fraudulent activities or untrusted operations.Firewall have the most important role in network security. It's very tedious task to call every user which is interact with their system. So it's not efficient for identifying which users are real among them and which connection is secure in the network which is local or global. It's one of the major and most popular aspect is Firewall. With the help of Firewall we are overcome these drawback and provide proper analyzing of user in private network. This helps in identifying normal and abnormal user behaviors which in turn helps in preventing the malicious activities which are carried out on effectiveness of security protection provided by firewall depends on quality of policy configured in the Firewall. The main aspect is detect and resolve the conflict occurred in a network. This technique can be used to avoid the losses incorrigible from them and enhance the security from business perspective and finally provides the Secure access.

Keywords*:Rule Reordering*, Rule Engine, Shadowing, Rule Generation, Redundancy, Correlation, Policy Conflict, Policy Resolution.

I. INTRODUCTION

As one of essential elements in network and information system security, firewalls have been widely deployed in defending suspicious traffic and unauthorized access to Internet-based enterprises. Sitting on the border between a private network and the public Internet, a firewall examines all incoming and outgoing packets based on security rules.In this paper, we represent a novel anomaly management framework for firewalls based on a rule-based segmentation technique to facilitate not only more accurate anomaly detection but also effective anomaly resolution. Based on this technique, a network packet space defined by a firewall policy can be divided into a set of disjoint packet space segments. Each segment associated with a unique set of firewall rules accurately indicates an overlap relation (either conflicting or redundant) among those rules. We also introduce a flexible conflict resolution method to enable a fine-grained conflict resolution with the help of several effective resolution strategies with respect to the risk assessment of protected networks and the intention of policy definition.

II. EXISTING SYSTEM

The basic security mechanism used for network security is Firewall. Configuring firewall is a hard and error prone. For the success of firewall, effective management of policy is very important. Some of the popular existing policy anomaly detection tools are Firewall policy advisor, FIREMAN, etc. Firewall Policy Advisor only has the capability of detecting pair wise anomalies in firewall rules. FIREMAN can detect anomalies among multiple rules by analyzing the relationships between one rule and the collections of packet spaces derived from all preceding rules. However, FIREMAN also has limitations in detecting anomalies.

Drawbacks:

- Can only detect pairwise anomalies in firewall rules.
- Only examines all preceding rules but ignores all subsequent rules when performing anomaly analysis.
- Can only show that there is a misconfiguration between one rule and it's preceding rule, but cannot accurately indicate all rule involve in an anomaly.

III. PROBLEM STATEMENT

Fraudulent activities involve violating the services in the private network. This involves secure and verified internet protocol address communication in private and public network. Many inventions have been made to make it secure but hackers have to be found to outsmart the developers each time. Obviouslyhuge amount of users' list are made. So maintaining and accessing this type of list, isolating the real users and fraud users list are not efficient for Administrator or database manager and it's a time consuming process.

IV. PROPOSED SYSTEM

In our system, overcomes the drawback of existing system. It has advent features which are easily accessing, managing, detecting, rearranging and resolving the firewall rules in the rule engine. It is a beneficial for Administrator and service providers. It is possible using the modern technology to create own inbound and outbound rules by using network segmentation and detect correlated rule and rearrange the previous rule.Detect user behavior is new powerful technology to restrict the fraudulent activities. These logs are then used to differentiate amongst the genuine user and fraud user. This helps to alert in the administrative authorities about the malicious activity. This project represents a novel anomaly management framework for firewalls based on a rule-based segmentation technique to facilitate not only more accurate anomaly detection but also effective anomaly resolution. Based on this technique, a network packet space defined by a firewall policy can be divided into a set of disjoint packet space segments.

.A. Features:

- 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 rearrang e them.
- Examines both preceding rule And subsequent rule while performing an anomaly analysis.
- Allowing us to create the inbound and outbound rules .

B. Applications:

- To detect the unauthorized user or malicious information through rule engine.
- Firewall policy analysis makes easy to analyse the secure communication over the network.
- Reduce the cyber crimes using the Firewall policy analysis.
- Provides the security for public as well as private network
- Identify the user behaviors.
- Using rule engine we can easily makes the rule reordering and trough this reordering we can easily make our own new rule list.
- Using firewall policy analysis we can easily blocks the unauthorized user.

V. MODULE DESCRIPTION

A. CORRELATION OF PACKET SPACE SEGMENT

In this module, we generate correlated group based on the conflict rules. The major benefit of generating correlation groups for the anomaly analysis is that anomalies can be examined within each group independently, because all correlation groups are independent of each other.

B. ACTION CONSTRAINT GENERATION

To generate action constraints for conflicting segments, we propose a strategy-based conflict resolution method, which generates action constraints with the help of effective resolution strategies based on the minimal interaction with system administrators.

C. RULE REORDERING

The most ideal solution for conflict resolution is that all action constraints for conflicting segments can be satisfied by reordering conflicting rules. In other words, if we can find out conflicting rules in order that satisfies all action constraints, this order must be the optimal solution for the conflict resolution.

D. REDUNDANCY ELIMINATION

In this module, every rule subspace covered by a policy segment is assigned with a property. Four property values,removable (R), strong irremovable (SI), weak irremovable (WI),and correlated (C), are defined to reflect different characteristics of each rule subspace.

VI. PROJECT CONCEPT

A) FIREWALL POLICY ANOMALY CLASSIFICATION

Here, we describe and then define a number of possible firewall policy anomalies. These include errors for definite conflicts that cause some rules to be always pressurized by other rules, or warnings for potential conflicts that may be implied in related rules.

a)FIREWALL POLICY ADVISOR

It is possible to use any field in IP, UDP or TCP headers in the rule filtering part, however, practical experience shows that the most commonly used matching fields are: protocol type, source IP

address, source port, destination IP address and destination port. Some other fields, like TTL and TCP flags, are occasionally used for specific filtering purposes [5]. The following is the common format of packet filtering rules in a firewall policy:
<order><protocol><src_ip><src_port><dst_ip><dst_ port><action>

Firewall Policy Advisor

order	protocol	src_ip	src_port	dst_ip	dst_port	action
1:	tcp,	140.192.37.20,	any,	*.*.*.*,	80,	deny
2:	tcp,	140.192.37.*,	any,	*.*.*.*,	80,	accept
3:	tcp,	*.*.*.*,	any,	161.120.33.40,	80,	accept
4:	tcp,	140.192.37.*,	any,	161.120.33.40,	80,	deny
5:	tcp,	140.192.37.30,	any,	*.*.*.*,	21,	deny
6:	tcp,	140.192.37.*,	any,	*.*.*.*,	21,	accept
7:	tcp,	140.192.37.*,	any,	161.120.33.40,	21,	accept
8:	tcp,	*.*.*.*,	any,	*.*.*.*,	any,	deny
9:	udp,	140.192.37.*,	any,	161.120.33.40,	53,	accept
10:	udp,	*.*.*.*,	any,	161.120.33.40,	53,	accept
11:	udp,	*.*.*.*,	any,	*.*.*.*,	any,	deny

Figure 1. A firewall policy example.

Firewall Policy Advisor

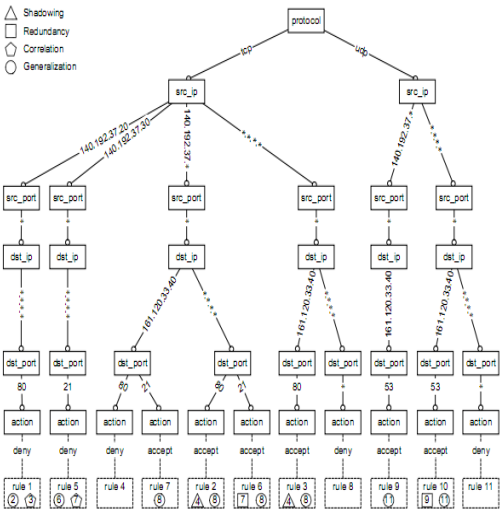

Fig: Policy tree for firewall policy

1. Shadowing anomaly

A rule is shadowed when a previous rule matches all the packets that match this rule, such that the shadowed rule will never be activated. Rule Ry is shadowed by rule Rx if Ry follows Rx in the order, and Ry is a subset match of Rx, and the actions of Rx and Ry are different. As illustrated in the rules in Figure 1, rule 4 is a subset match of rule 3 with a different action. We say that rule 4 is shadowed by rule 3 as rule 4 will never get activated. Shadowing is a critical error in the policy, as the shadowed rule never takes effect. This might cause a permitted traffic to be blocked and vice versa. It is important to discover shadowed rules and alert the administrator who might correct this error by reordering or removing the shadowed rule.

2. Correlation anomaly

Two rules are correlated if the first rule in order matches some packets that match the second rule and the second rule matches some pack- ets that match the first rule. Rule Rx and rule Ry have a correlation anomaly if Rx and Ry are correlated, and the actions of Rx and Ry are different. As illus- trated in the rules in Figure 1, rule 1 is in correlation with rule 3; if the order of the two rules is reversed, the effect of the resulting policy will be different.Correlation is considered an anomaly warning because the correlated rules im- ply an action that is not explicitly handled by the filtering rules. Consider rules 1 and 3 in Figure 1. The two rules with this ordering imply that all HTTP traf- fic coming from address 140.192.37.20 and going to address 161.120.33.40 is denied. However, if their order is reversed, the same traffic will be accepted. Therefore, in order to resolve this conflict, we point out the correlation between the rules and prompt the user to choose the proper order that complies with the security policy requirements.

3. Generalization anomaly

A rule is a generalization of another rule if this gen- eral rule can match all the packets that match a specific rule that precedes it. Rule Ry is a generalization of rule Rx if Ry follows Rx in the order, and Ry is a superset match of Rx, and the actions of Ry and Rx are different. As illus- trated in the rules in Figure 1, rule 2 is a generalization of rule 1; if the order of the two rules is reversed, the effect of the resulting policy will be changed, and rule 1 will not be effective anymore, as it will be shadowed by rule 2. Therefore, as a general guideline, if there is an inclusive match relationship between two rules, the superset (or general) rule should come after the subset (or specific) rule.Generalization is considered only an anomaly warning because the specific rule makes an exception of the general rule, and thus it is important to highlight its action to the administrator for confirmation.

4. Redundancy anomaly

A redundant rule performs the same action on the same packets as another rule such that if the redundant rule is removed, the security policy will not be affected. Rule Ry is redundant to rule Rx if Rx precedes Ry in the order, and Ry is a subset or exact

match of Rx, and the actions of Rx and Ry are similar. If Rx precedes Ry in the order, and Rx is a subset match of Ry, and the actions of Rx and Ry are similar, then Rule Rx is redundant to rule Ry provided that Rx is not involved in any generalization or correlation anomalies with other rules preceding Ry. As illustrated in the rules in Figure 1, rule 7 is redundant to rule 6, and rule 9 is redundant to rule 10, so if rule 7 and rule 9 are removed, the effect of the resulting policy will not be changed.

Redundancy is considered an error. A redundant rule may not contribute in making the filtering decision, however, it adds to the size of the filtering rule table, and might increase the search time and space requirements. It is important to discover redundant rules so that the administrator may modify its filtering action or remove it altogether

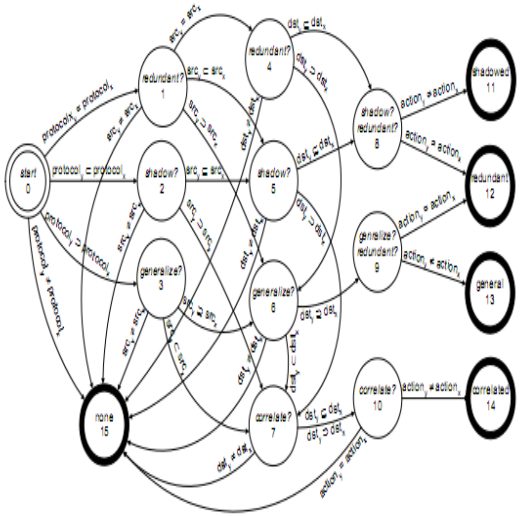

Fig: State diagram for detecting anomalies

VII. PROGRAMMING CONCEPT

A. JAVA

Java is a small, simple, safe, object oriented, interpreted or dynamically optimized, byte coded, architectural, garbage collected, multithreaded programming language with a strongly typed exception-handling for writing distributed and dynamically extensible programs.Java is an object oriented programming language. Java is a high-level, third generation language like C, FORTRAN, Small talk, Pearl and many others. You can use java to write computer applications that crunch numbers, process words, play games, store data or do any of the thousands of other things computer software can do.

- It is simple and object oriented
- It helps to create user friendly interfaces.
- It is very dynamic.
- It supports multithreading.
- It is platform independent
- It is highly secure and robust.
- It supports internet programming

B. MySql

MySQL is a popular choice of database for use in web applications, and is a central component of the widely used LAMP open source web application software stack (and other 'AMP' stacks). LAMP is an acronym for "Linux, Apache, MySQL, Perl/PHP/Python." Free-software-open source projects that require a full-featured database management system often use MySQL.

C. NetBeans

NetBeans IDE is a free, open-source, cross-platform IDE with built-in-support for Java Programming Language.NetBeans is an integrated development environment (IDE) for developing primarily with Java, but also with other languages, in particular PHP, C/C++, and HTML5. It is also an application platform framework for Java desktop applications and others.TheNetBeans IDE is written in Java and can run on Windows, OS X, Linux, Solaris and other platforms supporting a compatible JVM.TheNetBeans Platform allows applications to be developed from a set of modular software components called modules. Applications based on the NetBeans Platform (including the NetBeans IDE itself) can be extended by third party developers.

VIII. ALGORITHM

A. Greedy Algorithm:

In an algorithmic strategy like greedy, decision of solution is taken based on the information available the greedy method is straight forward method. This method is popular for obtaining optimizes solution. In greedy technique, the solution is constructed through a sequence of steps, each expanding a partially constructed solution obtain so far, until a complete solution to the problem is reached. At each step the choice made should be Feasible, Locally Optimal, irrevocable.

Algorithm 1:

1. Greedy(D,n)
2. In greedy approach D is a domain.
3. From which solution is to be obtained of size n
4. Initially assume
5. Solution←0
6. For i←1 to n do
7. {
8. S←select(D)
9. Selection of solution from D
10. If (feasible(solution,s)) then
11. solution←union(solution,s);

12. }
13. Return solution.

B.DES Algorithm:

Data Encyption Standards also called as the Data EncyptionAlgorithm(DEA) by ANSI and DEA-1 by ISO,has been a cryptographic algorithm use for over three decades. Of late, DES has been fount vulnerable against very powerful attacs and therefore, the popularity of DES has been slightly on the decline.

a) Working:

DES is a block cipher. It Encrypts data in blocks of size 64 bits each. That is, 64 bits of plain text goes as input to DES which produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption with minor differences. The key length is 56 bits. The basic idea is shown in figure below

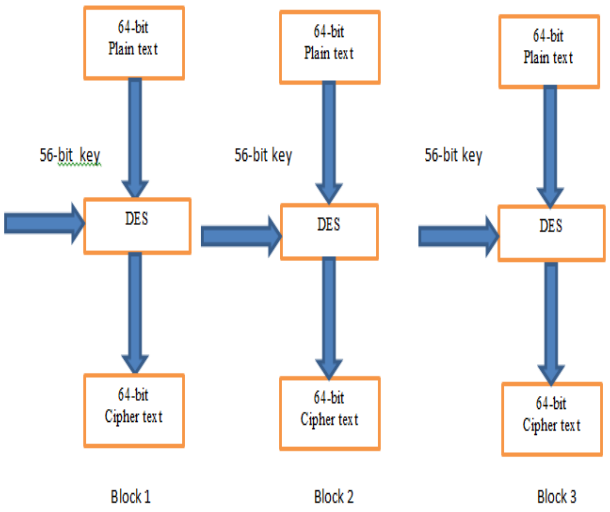

Fig: The conceptual working of DES

IX. TECHNOLOGY USED

A. FIREWALL

The dramatic rise and progress of internet has open possibilities that no one would have thought of. We can connect any computer in the world to any other computer, no matter how far two are located from Each other. This is undoubteldly a great Advantage for indivisual and corporate as well. Most corporations have large amounts of valuable and confidential data in there network. Leaking of this critical information to compititors can be a great set back. This is where a firewall comes into picture. Conceptually, a firewall can be compared with a sentry standing outside an important personshouse.A Firewall acts like a sentry. If implemented, it guards a corporate network by standing between network and the outside world. All traffic between network and internet in either direction must pass thorough the firewall. The firewall desides if the traffic can be allowed to flow or weather it must be stop from proceeding further.

a) Policy Anomaly Detector:

It is for identifying, conflicting, shadowing, correlated and redundant rules. When a rule anomaly is detected, users are prompted with proper corrective actions. We intentially made the tool not to automatically correct the discovered anomaly but rather alarm the user because we believe that the administrator is the one who should do the policy changes.

Algorithm:

1)functionDecideAnomaly(rule, field, node, anomaly)
2)if node has branch_list then
3)branch = node.branch_list.first()
4) if anomaly = CORRELATION then
5) if not rule.action = branch.value then
6) branch.rule.anomaly = CORRELATION
7) report rule rule.id is in correlation with rule branch.rule.id 8) else anomaly = NONE
9)else if anomaly = GENERALIZATION and not rule.action = branch.value then
10)branch.rule.anomaly = SPECIALIZATION
11)report rule rule.id is a generalization of rule branch.rule.id
12) else if anomaly = GENERALIZATION and rule.action = branch.value then
13) ifbranch.rule.anomaly = NONE then
14) anomaly = NONE; branch.rule.anomaly = REDUNDANCY
15) report rule branch.rule.id is redundant to rule rule.id end 16) if else if rule.action = branch.value then
17)anomaly = REDUNDANCY
18)report rule rule.id is redundant to rule branch.rule.id
19)else if not rule.action = branch.value then anomaly = SHADOWING
20)report rule rule.id is shadowed by rule branch.rule.id
21)end if
22)end if
23)rule.anomaly = anomaly
24)end function

b) Policy Editor

For facilitating rules insertion, modification and deletion.The policy editor automatically determines the proper order for any inserted for modified rule.It also gives a preview of the change parts of the policy wheneverrule is removed to show the effect on the policy before and after the removal.

X. LITERATURE SURVEY

Today near about 80-90 % users are interacting with online networking system.E.g. Public network verses private network.In that huge amount

of fraud users are rapidly increases and they share malicious information over the network or in the corresponding system. So it is difficult to know which users are real and which users are frauds among made users list. Hence large number of users list is made and it's tedious task to maintain and isolating the users list and it's time consuming process. To maintaining the huge amount of web traffic over the network are available in Firewall Policy Technique.

Overall survey of the papers concludes that they are uses local Virtual Private Network or Fireman technology for handling incoming and outgoing data in network traffic. But it requires huge time and it only detects the anomalies not resolving it. It can be handled by using Firewall policy analysis which uses Rule Reordering as well as shadowing and correlation to generate new rule.

XI. CONCLUSION

- Detection of Fraud/Sybil user's activities in a network which is control by Firewall Policy Rule Engine.
- Determines the correlated group.
- Huge amount of web logs are easily managed and identifies real users and fraud users.
- Granting permission by performing operation (Allow/Deny) and calculating Threshold value.
- Malicious information is added in a block state.
- Provide finally secure access to or from the private and public network.

XII.FUTURE SCOPE

- It will be used for hacking Prevention.
- It will be used as an Antivirus on individual machine.

REFERENCES

[1] "Teneble Network Security,"http://www.nessus.org ness.2012.
[2] "Tissynbe.py,"http://www.tssci-security.com /projects/Tissynbe_py, 2012.
[3] IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 3, MAY/JUNE 2012.
[4] IEEE Global Internet Symposium (GI) 2011 at IEEE INFOCOM 2011.
[5] P. Hansteen, "Rickrolled? Get Ready for the Hail MaryCloud!,"http://bsdly.blogspot.com/2009/11/rickrolled-get-ready-forhail-mary.html, Feb. 2010
[6] Y. He and Z. Han, "User Authentication with Provable Security against Online Dictionary Attacks," J. Networks, vol. 4, no. 3,pp. 200-207, May 2009.
[7] E. Bursztein, S. Bethard, J.C. Mitchell, D. Jurafsky, and C.Fabry, "How Good Are Humans at Solving CAPTCHAs? ALarge Scale Evaluation," Proc. IEEE Symp. Security and Privacy,May 2010.