ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

Distributed Firewall Application for Policy Management and Network Security

Manila Bohra[1], Laghvi Aloria[2], Neha Gupta[3]

B. Tech (6th sem) Student, Rajasthan Technical University, Kota, Rajastan, India[1]

B. Tech (6th sem) Student, Rajasthan Technical University, Kota, Rajastan, India[2]

M.Tech Student, Rajasthan Technical University, Kota, Rajastan, India[3]

Abstract: The extended study of this research leads to the grouping of firewalls which could be capable of providing security at distributed points. Firewall allows separation between frontend and backend entity so as to ensure security. Various other entities like DPFF needs to be protected from outsiders (unauthorized users).To do so firstly, firewall policies needs to be tested because most of the policies have been corrupted or plagued with policy faults which may leads to trafficking. During Firewall working mechanism, DPFF layers themselves act as layers of protection or defence using various policies and algorithms which help in reducing the traffic and making the efficiency in detection and policy updating. The complete frame work signifies a distributed firewall and its testing policies to ensure network security.

Keywords: Distributed packet filtering firewall, Firewall policies, policy faults and policy algorithms.

I.INTRODUCTION

To defend the privacy, reliability and accessibility of outcome packet over the network, in 1990's Firewall was introduced. Nowadays, with the vast use of internet globally there is an increased threat of network attacks and its unauthorized use. Firewalls have been the very first defence for security against such attacks not only in large scale networks but also in small -size networks with its applications such as institutions, enterprisesand various other fields.

Actually, today's firewalls act as a security fence between controlled and managed. To do so appropriate network defense access policies needs to be defined as first defend layer of defence in firewall organization strategy. Firewall implements such policies as for network security.

The firewall technology used must be a segment of typical security strategy which cannot be alone and provides complete secure solution .These technologies needs to be complemented with other security technologies so as to provide the required solution. Rules set policies let the firewall either provide permission or denial to access to the networks .Firewalls are intended to be filtering safeguards in network security. Firewalls role is to focus on security management in single as well as distributed networks.

There are certain limitations for firewalls which prevent them to defend the system from unknown attacks or threats. One of the most important issues is firewall policies faults as these policies can have a huge effect on creating security holes .It can also block the allowed traffic which can also be assumed as a weak feature of firewall. Despite of this firewall is vastly used as an effective tool for controlling the trafficking .As firewall analysis tools is available to overcome such defaults.

In addition; firewalls also propose some models to work as a virus detector or protector to perform in various data packets passing through packet.

II. BACKGROUND

Firewall administrator is located within the network administration to organize and control the services and give the collective effort of policies and rules establishment in an organization. According to various definitions of firewall given by researchers helps us to conclude that firewall is a hardware or software which helps in controlling traffic passing through it .But it can be effective only when the traffic is based on authorized security policy, So as a security measure and protection of firewall itself.

There are many different hot issues about the firewalls since their role is really important in terms of security of the networks. In this section, we are going to clarify motivation and also the scope of this survey paper by introducing the subjects clearly.

Various researchers like M.Hamdi,, N.Boudriga, J.D. Guttman, L. Huang etc have proposed various security policies and protection for internet browser as well as techniques for optimized monitoring of firewall. One of the researchers have proposed research on various types of browsers attacks such as ability of networks to interact with the client, threat scopes, XSS phishing and weak authentication as well as measures to control them by using validate domain, certificates like SSL, HTTP's .

This paper presented in our main research proposed model as the front end layer of the security in collaboration with Distributed Network Detection System which is located behind the Distributed firewalls to be the main components of the main research.

Because of the importance of usable security, we cover some of the latest works in this really interesting field.

III. ANALYSIS OF FIREWALL ACTIVITY

There are several queries of the user about the usage and traffic control in firewall activity. Some of these enquiries are as follows:

∗ Particular source and target and their services which may be accessible by source should be investigated.

∗Comparison between two distributed firewall to check their configuration and to enforce same policy.

∗ Investigation about the active firewall.

∗ The influence of a node compromises to interface the firewall.

∗ Investigation about the conducted policy configuration to meet the organization requirement.

∗ All the open ports that may not to be open to inbound or outbound of the available nodes should be disabled.

∗ The ports according to the organization policy, which require communicating, should be defined in firewall policy.

∗ Correctness of the rules updated on the basis of organization policy should be examined.

With the above examining procedure the firewall policy utilization based on its specification utilized and any similarity or conflict in the policy is indicated to the administrator.

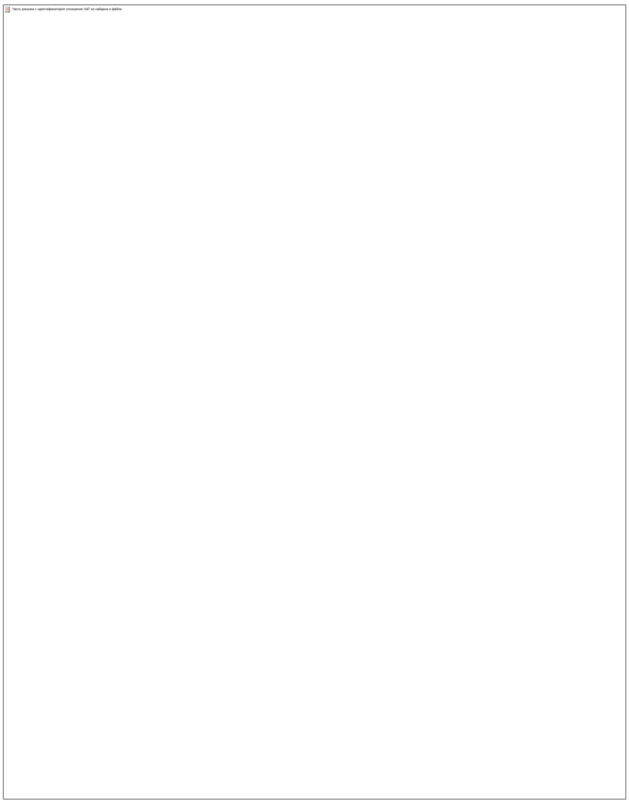
Часть рисунка с идентификатором отношения rId7 не найдена в файле.

Fig- (Firewall Packet Filtering)

As it is shown in firewall connectivity of TCP/IP after receiving the packets (inbound and outbound) firewall performs to open command to receive and initial its investigation. In next firewall is starting to validate the packet based on its policies and somehow updating. In the parallel activity, firewall check for monitoring the network topology and its status. For the first part after monitoring the packet it will check for filtering, relay or update, in the second, the network topology it checks for capability of this topology, and in last, the status for immediate action and response is checked.

IV. FIREWALL POLICY TESTING

The firewall investigates and observes each packer protocol and its IP information and then filters the outgoing and incoming packets based on a set of security configuration policies. The various rules as well as policies which can be updated by the administrator are as follows:

∗It drops all network packets, which may be subject to updating policy or administrator commands.

∗Limitless access to the web-server, which based mostly on port number 80.

∗Limitless access to port number 25 to access mail server through SMTP protocol.

A firewall policy instructs how the network traffic will through the firewall. The appropriate policy illustrates the firewall updating and security measures .To create firewall policy various risk analysis should be carried out on basis of requirement for the execution of the organization. By an overview of this analysis list of applications and how it shall be secure is processed. With the knowledge based of the vulnerabilities, which is associated with each application, the particular method will be used for securing this application. The risk analysis should estimate according to the infrastructure but in the propose model the evaluation has been done the various elements like, vulnerabilities, threat and invader activity and with the impact of sensitive data available on the servers. By this goal, the evaluation of these elements aforementioned to determine the firewall policy is analyzed and the structure of handling applications traffic is processed.

Various steps to create the firewall policy are as follows:

∗ Recognition of vulnerabilities related with applications.

∗Anal**ysis** of the approach model for securing the applications' investigation and protection method to create application traffic

∗Establish of firewall policy is to support the application traffic.

∗Establish of firewall rules based on the IP domicile, ports and protocol.

∗ Identification of the various conducted system vulnerabilities to update the policies.

∗Collaboration with other joint defense layer to completion of the policy.

V. FIREWALL POLICY & SECURITYALGORITM

A very important part in management of firewall policies is to fix the faults. For this goal, first the root of the fault should be defined in the debugging phase of testing.Firewall policy has a common algorithm which consists of a set of rules. Each of the rules has a format as follows: ⟨predicate⟩→⟨decision⟩ (1) A ⟨predicate⟩ defines a collection of packets over a definite number of fields. Fieldsare showed in the format of F1… Fn. On the other hand, ⟨decision⟩ of a rule is related to the evaluation of predicate and it can be true or false. If predicate is evaluated to true, then the decision will be appeared. A packet is basically a tuple (fv1... fvn). As it was mentioned earlier, it is defined over a finite number of *fields* F1... Fn. fvi is a variable whose values of fvi variable are within a D (Fi) domain. It is common to mention values in *fields* to their integer values to make representation format as simple as possible. The predicate itself can be represented: $(F1 \in S1)$ s$\wedge ... \wedge$ $(Fn \in Sn)$ (2) In this representation, Si denotes a part of domain D (Fi). Each of $(Fi \in Si)$ is called a ⟨clause⟩, which should be evaluated to correct or incorrect. It is very important that a firewall policy uses a standard semantic for its functionality which is called the first-match semantic. In this semantic, there is an iteration which continues until the time it reaches the end of the rules. This iteration starts from the first rule by looking for its predicate to see whether it has been evaluated to true or not. If this condition is satisfied then the decision that corresponds to this rule is derived and returned; otherwise it goes to the next rule in the set of policies. There are some other expressions that are technically used in this field for example, conflict or anomaly, overlap, shadowing, generalization, correlation and policy conflicts. Conflict means as follows. When we talk about policy conflict, we are talking about an entity that is associated with a collection of rules. These rules have the ability to derive a packet space which is common among them. The point here is that rules in this collection match all the packets and at least two of the rules have different decisions. Matching of a packet with different rules is called overlap. Shadowing happens when a rule cannot effect on the decision for passing or failing the packet because of the preceding rules that match the packet. Generalization means when a subset of matched packets for this rule is also matched by preceding rules but with different decisions. Correlation happens when there is an intersection between a rule and some other rules but the matched packets by this intersection are not assigned the same decision.

VI. FIREWALL POLICY AND FAULTS

Although automatic correction of firewall policy sounds very useful, it has its own difficulties to be correctly applied on the firewall. These difficulties can be categorized in separate groups as follows:

∗Counting the number of faults and defining types of faults

∗Locating the origin of the fault among torrents of rules in the firewall

∗Correcting the faults without making any side-effects which affects other rules and their functionalities

The act of finding the root of the fault is technically called fault localization. Iftesters and debuggers want toperform it manually, it will take a very long time because of the inherent complexity of fault localization and the huge amount of rules. Thus, efficiency of localizing the faults should be considered as a factor of quality.

VII. CONCLUSION

Firewalls are utilized typically to be the main layer of security in the network framework. The result analysis is that we define the firewall policies and their relations, which assists to identify probable errors and firewall policies weaknesses aforementioned to their development in the framework.Redundancy occurs when there are more than one rule in the policy with same effect. Tools like FPA are not able to do pair wise anomalies using the firewall rules most real-life firewalls have been plagued with policy faults, which either allow malicious traffic.

VIII. FUTURE WORK

In future, it seems to be quite a good job if researchers focus more on qualitative study for usability of the tools that they have already developed. By using the different types of tools we can increase the strength of firewall policies and by using the more protocols in firewall policy mechanism DPFF can give the way of blocking more unprotected data.

REFERENCES

[1] E. Al-Shaer, and H. Hamed, "Firewall Policy Advisor for anomaly discovery and rule editing". Integrated Network Management, IFIP/IEEE Eighth International Symposium on, 2003, pp. 17–30.

[2] AusCERT, "Australian computer crime and security survey", Australian Computer Emergency Response Team. 2005, Technical Report, http://www.auscert.org.au/crime survey.

[3] S. M. Bellovin, "Distributed firewalls. Login: The Magazine of USENIX & SAGE", 1999, pp. 39-47.

[4] M. Bishop, "Early computer security papers, part 1", http://csrc.nist.gov/publications/ history/ index.html. 1998.

[5] WOOL, A. A quantitative study of firewall configuration errors. IEEE Computer 37, 6 (2004), pp. 62–67.

[6] Fei, C., Liu, A.X., Hwang, H., Xie, T. 2010. First Step Towards Automatic Correction of Firewall Policy Faults. In Proceedings of the 24th USENIX Large Installation System Administration Conference (LISA 2010), San Jose, CA, November 2010.

[7] Hwang, J., Xie, T., Chen, F., and Liu, A. X. 2009. Fault localization for firewall policies.In Proceedings of IEEE International Symposium on Reliable Distributed Systems (SRDS).

[8] Hu, H. Ahn, G. AND Kulkarni, K. FAME: A firewall anomaly management environment. SafeConfig '10 Proceedings of the 3rd ACM workshop on Assurable and usable security configuration (New York, NY, USA, 2010), ACM, p. 4.