Firewall's Best Practices in an Organization

Vijender Kumar Solanki
Research Scholar
Anna University, Chennai, TN
Nammakal, TN

Kumar Pal Singh
Faculty
Institute of Technology & Science
Ghaziabad, UP

M. Venkatesan
Principal
KSRIET, Trichungode,
Nammakal, TN

ABSTRACT

The network security always remains attraction for the IT security professionals due to the availability of various solutions for the single problem such as opting single layered security approached e.g., Software Based Firewall or Either select for High Range Firewalls or go for mixed solution which include the deployment of firewall including the NIDPS and Optional Monitoring Tools. However it is always tough for them to select which solution is the best one due to managerial as well as technical issues which suits to their organization's problem in current scenario [1]. In this paper we are discussing about the network security issues in the context of firewalls, how to opt an appropriate solution in view of present problem if any. The administrators options varies from the theoretical approach as they do not follow the security standards and their policies as mentioned in security books however in the organization instead of that they just tuned up most demanding protocols and handle the most immediate problem in context of security.

Keywords

Keywords Network Security, Internet Protocol, Firewall, Security Management.

1. INTRODUCTION

Internet has been emerged as a foremost communication medium with inhabitants who are available at different geographical location. It takes just a click and the communication reaches to the recipient's machines that are also connected with the internet. While addressing the security issues in the network due to internet communications, [1-5] we have seen that in majority organization's management believes that they are secure because they have installed the security firewalls whose job actually is to filter the authorized and unauthorized information towards the organization [8]. While this silent question always remain a threat for technical teams that is it really secure and now onwards will there be no problem in order to securing Client-Server Architecture hereafter referred as CSA by External Unauthorized traffic. In the Fig. 1 a Layout of firewall is shown where the firewall is placed between the internal network and external network i.e. Internet [6]. Our effort is to secure the network from the outsider in such a way that all the authorized traffic should be allowed in the CSA network, and rest should be dropped outside the CSA network.

The paper is distributed into seven sections viz., Section 1 is introduction, and basics of firewalls to use in client server architecture. Section 2 is describing about the firewall impact on client server architecture. Section 3 is describing about to improve the existing firewalls for better use in existing scenario. Section 4 is basically given to conclude the attempt made by authors in this paper. Section 5 is to portray the future work. Section 6 is about acknowledgement and Section 7 is about the list of references and books.

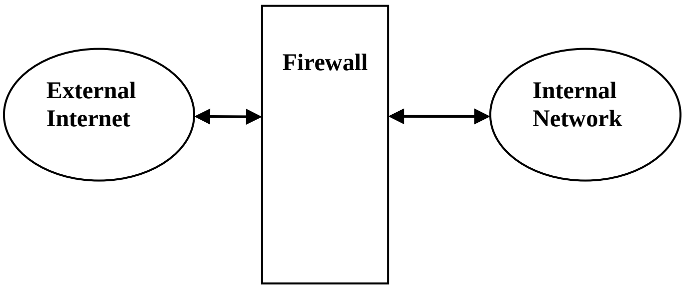

Fig. 1: A layout of Firewall

1.1 Firewall Classification

Firewalls is the first defense of network which is placed outside the network to monitor the traffic in such a way that only authorized data can flow inside the network and rest should be dropped by firewalls outside as the configuration rules is given in the firewalls by administrators [7]. The firewalls can be broadly categorized as of three types' viz., Packets Filters, Proxy Servers, and Stateful Packets Filters [Fig. 2]. Though there are some other schemes also for firewalls but we have given here basic and simple one which is mostly used by organizations. The packets filter firewalls is mainly stand on the packet allow rules e.g., what we want to allow and deny we mention it in the firewall configuration. So it checks only that whatever we have blocked should be dropped outside or whatever we permit should be allowed in the network. The big benefit of this firewall is it's easy to configure and work on it as whereas the drawback is that it drop and allow the packets but not provide the log file facility so it's tough to know the threat point. Proxy Server is like a sharing (Virtual) machine which is having capacity to read the security instruction what to allow and deny and accordingly it provide the service to the client. The advantage of this firewall is it's easy to use in small networks where the number of clients is less but the bypass is always a big threat to proxy firewalls. It has two flavors' Application and Server Level Gateway, which respectively give the control in context of application and server level but it leads to the problem of slowing down the data traffic in coming/going channels. The Stateful Packet filtering also causes security by passing through network layer [3]. It maintains the status for each session also but it is not a complete solution in term of firewalls

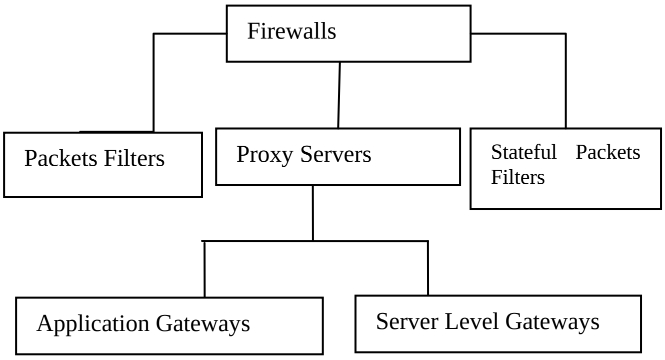

Fig. 2: A Firewall Classification

2. STUDY ANALYSIS OF FIREWALL

In this section we are writing about the functioning of firewall. It is having multiple options and every computer network has some pros and cons [2]. The study shows that firewall is used to enforce security policy which is initially pre-identified by the network security analyst. The firewall security policy is the set of rules which is first listed down on the paper and then analyzed with the management. The outcome of this discussion is that after the policy build up it would not be possible to give every service to every client due to security constraint [10]. Another important function is to maintain the log of activities which enables the network administrators to updates the rules in firewalls if it's not enlisted earlier in the list. It is obvious that due to enormous growth and data availability on the Internet, it remain a question that what is suitable to us and what is not suitable to us is our concerns. Apart from that the firewall is also used to provide different services to different groups as per their accountability of work in the organization. It can provide the varied permissions to different services for selected users. There are numbers of methods in context of firewall to make different security environments as per the demand of organizations. It provides flexibility to focus on the decision which play quiet important role in the organization.

2.1 Firewall Limitations

After a brief discussion on the capacity of firewall here a little discussion on firewall limitations is given. The major one is that firewalls are not fully capable to protect malicious threat in CSA. The antivirus and intruder detection and intruder prevention systems (IPD/IDS) are comparatively stronger solution for that. Though the intruders initially entered as authorized users but after that the vulnerability is a big concern for the system security analyst. By passing firewalls are big challenges as different mode of firewalls installation leads to different impact on CSA [4]. So the constant monitoring of the CSA becomes a daily routine for the technical team members. The other important part where it stands fail is it is unable to protect any new threats because it's not having that details in security policy and hence it harm to the security of the CSA by raising new vulnerability issues.

2.2 Strategies

We are working with firewall and as its functions for Internet and able to find the traffic which is required to be allowed or blocked, but in majority we are to work out our strategies by Firewalls with the major Internet services as HTTP, SMTP, FTP, SSH, DNS [9]. If we are capable to get in details with these protocols at certain level we can get better framework then the present because mostly faults likely to be arisen due to the unbalanced protocol tuning as mentioned above.

2.3 Issues Emerged

The network security team feels that there is no such a data in the network so no need for monitoring on day-by day basis. Many Application runs with Admin Panels Permission only so it's quite tough at that time to refrains other to get that service. The Zones are defined in the local area network hereafter called as LAN but the trust level is always a confusing and conflicting one. It has been seen at various places that the administrator is using his/here computer with all the permission granted which surely leads to the intrusion of various threats in the networks. So we should sketch a system design which could provide us the compact solutions of these issues. Although these are valid to the administration tuning level but our effort is to sketch the architecture where these could be analyzed in better than present ways.

2.4 Challenges

We feel that the majority of attacks are happens due to the traffic bypass from the firewall's access control lists and thus they are no longer come in the perimeter for the CSA security[11]. Due to bypassing traffic the network also suffer the cause of vulnerability which causes the emergence of threats whose improved version leads to the successful attacks in the CSA. The CSA is known for its services to clients but bypassing of the traffic further leads to the performances issues [12]. It provides the services slower than it actually supposed to do so. If the vulnerability get pointed in a single machine gradually it infect the trusted zones which leads to failure of network services in spite of having the capacity to serve well to clients.

3. OUR OBSERVATIONS

The discussion with the various Network Administrators comes up with the different opinions as we surveyed nearly 15 organizations in the duration of three months from May 2012 to July 2012 to know the basic information, that what is the arrangements and management they are doing to secure their network from the unauthorized vulnerabilities [see Table 1] from outside as well as inside of the network. The most of the questions asked during the discussion belong to the network security in the context of Firewalls. The concerned persons responded that the number of terminals they were controlling range from minimum 480 to the maximum 1200. The responders were basically working in a capacity of system administrators and senior security administrators. The survey was conducted purely on the basis of questionnaires to know the awareness of network security product available in the markets in the terms of software and hardware based tools. The surprising result we receive from their side was that, they are totally confident that their network is fully secure in spite of having some deficiency as per our research point of view. They never receive any problem regarding security instead of few basic one which we feel that it nowhere belong to our research objective. The big loopholes we have sensed in many sites was that they are merely a mute device controller for the name, if any problem comes, then the troubleshooting is done remotely by the outsourcing firm who is managing their firewalls. This condition is valid for configuration updating and even for replacement of device also.

Table 1. Result of survey conducted with responders

Topics	**0-25%**	**26-50%**	**51- 75%**	**76- 100%**
Firewalls Knowledge	7	3	3	2
Software Firewalls	8	4	2	1
Hardware Firewalls	4	3	6	2
Policies	7	3	2	3
Log Inspection	9	2	3	1
Updates in Markets	8	4	2	1
Exclusive For Firewalls	1	2	1	1

3.1 Our Proposed Solutions

In this paper we have concluded four points which we want to highlight:

a). If the organization is going to deploy firewall as a fresh in network then it should be done in such way that it gives feasible solution in future also. It should not be deployed for just present scenario solution only.

b) The administrator should be skilled in order to understand the updates what's going across the globe in context of Firewalls developments.

c) Due to managerial reason if not possible to go for firewalls equipments then it is not a bad idea to harden the CSA and provide controlled services to avoid the vulnerability in the networks.

d) The use of open source based Firewalls are also a key idea to start something innovative as it requires little more technical skill but it may offer better solution than existing ones in down costs.

4. CONCLUSION

In this effort we have made an attempt firstly to assess the traditional belief of majority of management of organization in context of firewall deployment and its operations. Then the functioning and limitations of the firewall are discussed. The authors brought out the emerging issues and challenges in the applications of firewall. All through the survey followed by analysis it was the major point that there is lack of expertise about the functioning of firewall. And not only it is supervised offhand but the majority of responsible workforce believe that their network become secure once they install the firewall but in reality this not factual. The authors also proposed the suitable solution which is based on observations come out with study, survey and analysis.

5. FUTURE WORK

Our future work plan in this research line is to work out the framework where we can utilize the maximum capacity of firewalls without disturbing other policies with other network components. And to study how the rules harden the Client Server Architecture and will give comparison of various same strength firewalls given by various vendors with their pros and cons.

6. ACKNOWLEDGEMENTS

Practicality always gives different taste than theory, so at this juncture we give sincere thanks to various technical members who as a capacity of system administrators/security consultant spared their valuable time during discussion and due to their co-operation a lot of facts became core part of our knowledge base.

7. REFERENCES

[1] Charles C. Zhang, Marianne Winslett, Carl A. Günter, On the Safety and Efficiency of Firewall Policy Deployment,2007 IEEE Symposium on Security and Privacy (SP'07).

[2] Cisco Firewall Services Module http://www.cisco.com/en/US/products/hw/modules /ps2706/ps4452. html.

[3] Patrick W. Dowd, John T. McHenry, Network Security: It's Time to Take it Seriously, Computers, IEEE Sept, 1998.

[4] Jan L. Harrington, Network Security: A Practical Approach, Elsevier, Edition 2011.

[5] Gunnar Peterson, Security Architecture Blueprint, Arctec Group, LLC.

[6] IBM Service Management Series White Paper, March 2008, Take a Holistic Approach to Business-Driven Security.

[7] Eric Seagren, Wesley J. Noonan, Secure Your Network For Free, Elsevier Professional and Trade Series Edition 2007.

[8] Alain Mayer, Avinashi Wool, Elisha Ziskind, FANG: A Firewall Engine, 2000 IEEE.

[9] Alex X. Liu, Mohamed G, Gouda, Diverse Firewall Design, IEEE Transaction on Parallel and Distributed System, Vol 19, No 9, September 2008.

[10] P.Bera, S.K.Gosh, Pallabh dasgupta, Policy Based Security Analysis in Enterprise networks: A Formal Approach, IEEE Transaction of Network and Service Management Vol 7, No 4, December 2010.

[11] Ehab Al-Shaer, Adel El-Atway, and Taghrid Samak, Automated Pseudo-Live Testing of Firewall Configuration Enforcement, IEEE Journal on Selected Area in Communications, Vol 27, No 03, April 2009.

[12] Kevin.W.Helman,Vishwath,Mohan,M.M.Masud,L,K han,B.Thuraisingam, Exloiting An Antivirus Inteface,Computer Standard and Interface 31(2009),1182-1189.