International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Study of User Behaviour for Firewall Configuration

N. Chiranjeeva Rao*, Shankha De, Chaitali Choudhary
Department of Computer Science Engineering, Bhilai Institute of Technology, Durg, Chhattisgarh, India

ABSTRACT

Configuration of firewalls is a task which every System Administrator need to perform from time to time. Every firewall comes with its own set of default rules which need to be updated from time to time. A thorough analysis of the user behavior in an organization or institution would help the Administrator to understand the needs of the organization in a much better manner. This paper aims at understanding the user behavior of a particular network over a period of time and accordingly redefine the rules. This upgradation of rules helps in efficient utilization of resources in the organization. This also ensures even distribution of resources of organization giving equal usage opportunities to all users.

Keywords: Firewall efficiency, User behavior in Networks, Firewall configuration

I. INTRODUCTION

When two or more computers are connected to each other, they may be located either at the same place or at different corners of the world. In order to connect they need a Computer Network. Using these networks, computers can communicate and exchange information but using these networks also expose the computers to threats. Therefore in order to protect them many of the network security options are used. Some of them are Firewalls, Intrusion Detection System, Honey Pots etc.

In this paper the topic of analysis is firewall. A few characteristics of a firewall are listed below:

1. A firewall is a device used to transfer information securely from an intranet to internet and vice-versa.
2. Only the authorized user or traffic is allowed to pass through the firewall.
3. It is necessary that firewalls must be able to prevent the intranet from attacks from internet as well as the internet from intranet.

There can be three methods of controlling the activities at the firewall. The First one can be done before the packet enters the firewall. Here the number of packets entering the firewall can be reduced by applying some of the techniques such as Random Early Detection etc.

Second method is diverting the traffic by deployment of Bastion Hosts which act as an external DNS Server and the traffic getting diverted directly to Internal DNS Server bypassing the firewall which can be done by defining a set of rules.

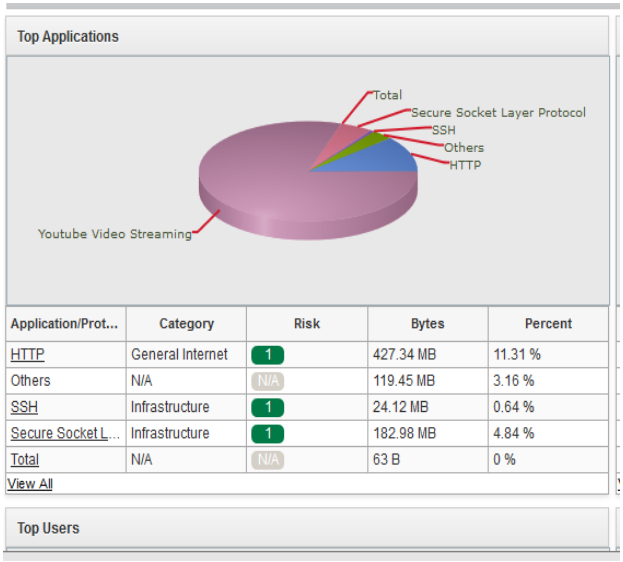
The third method is by studying the user behaviour of the traffic at the firewall and modifying the rules or customizing as per the needs of the organization.

In this paper we are focusing on the third method of improving firewall performance.

II. METHODS AND MATERIAL

For the purpose of experiment, we are taking a firewall installed in an organization with an average of 400 to 500 users. The analysis was done on the users of the organization for a period of two months and the following graphs were obtained. These graphs were analysed and a set of new rules were framed according to the custom necessity of the organization. This customization helped to improve the efficiency of the

network of the organization. The graphs are shown below:-

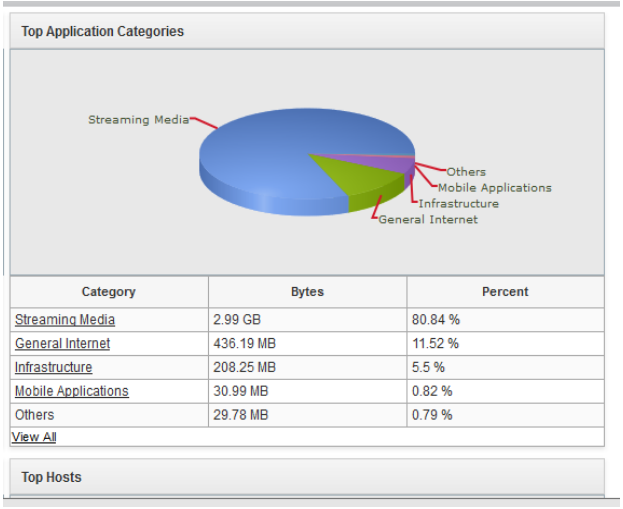


Application/Prot...	Category	Risk	Bytes	Percent
HTTP	General Internet	1	427.34 MB	11.31 %
Others	N/A	N/A	119.45 MB	3.16 %
SSH	Infrastructure	1	24.12 MB	0.64 %
Secure Socket L...	Infrastructure	1	182.98 MB	4.84 %
Total	N/A	N/A	63 B	0 %

View All

Top Users

Figure 1. Graph showing top applications used by the users during the span of two months

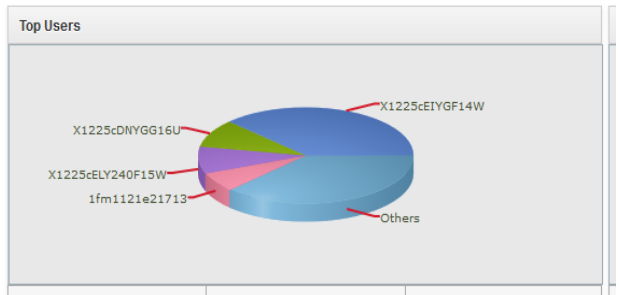


Category	Bytes	Percent
Streaming Media	2.99 GB	80.84 %
General Internet	436.19 MB	11.52 %
Infrastructure	208.25 MB	5.5 %
Mobile Applications	30.99 MB	0.82 %
Others	29.78 MB	0.79 %

View All

Top Hosts

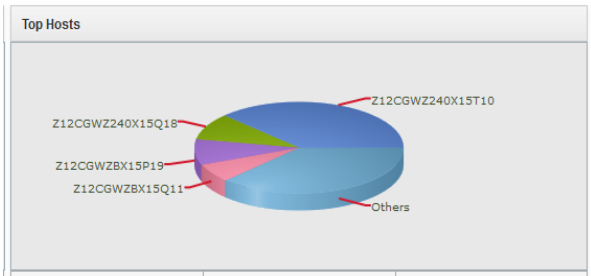
Figure 2. Graph showing top application categories used by the users.



User	Bytes	Percent
X1225cEIYGF14W	1.39 GB	37.8 %
X1225cDNYGG16U	350.27 MB	9.27 %
X1225cELY240F15W	335.73 MB	8.89 %
1fm1121e21713	245.97 MB	6.51 %
Others	1.38 GB	37.53 %

View All

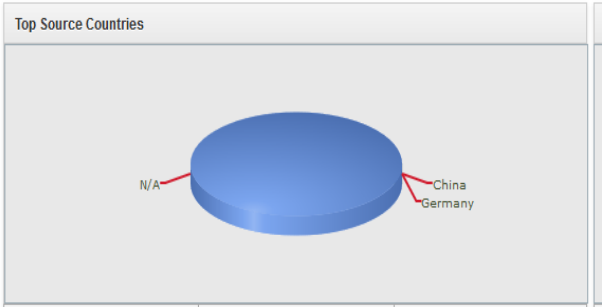
Figure 3. Graph showing top users who used the internet.



Host	Bytes	Percent
Z12CGWZ240X15T10	1.39 GB	37.8 %
Z12CGWZ240X15Q18	350.27 MB	9.27 %
Z12CGWZBX15P19	335.73 MB	8.89 %
Z12CGWZBX15Q11	245.97 MB	6.51 %
Others	1.38 GB	37.53 %

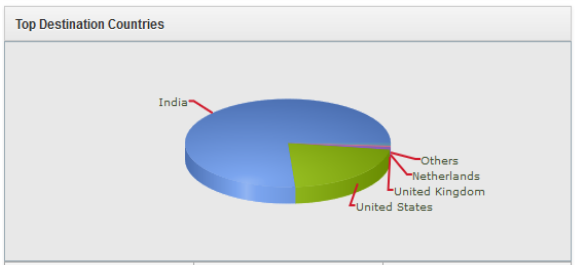
View All

Figure 4. Graph showing top hosts used by the users



Country	Bytes	Percent
N/A	3.69 GB	100 %
Germany	75.22 KB	0 %
China	1.12 KB	0 %

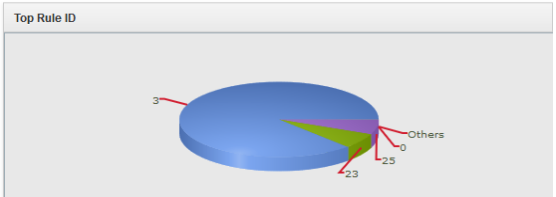
Figure 5. Graph showing top source countries surfed by the users



Country	Bytes	Percent
India	2.81 GB	76.16 %
United States	809.72 MB	21.43 %
United Kingdom	37.59 MB	1 %
Netherlands	18.04 MB	0.48 %
Others	35.27 MB	0.93 %

View All

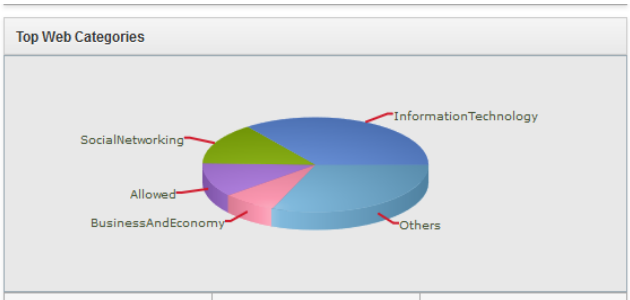
Figure 6. Graph showing top destination countries



Rule ID	Bytes	Percent
3	3.22 GB	87.22 %
23	245.97 MB	6.51 %
25	228.75 MB	6.06 %
0	5.72 MB	0.15 %
Others	2.34 MB	0.06 %

View All

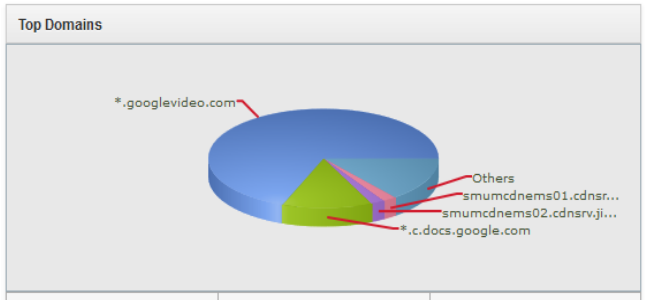
Figure 7. Graph showing top rules encountered by the users.



Category	Hits	Percent
InformationTechnology	4252	35.43 %
SocialNetworking	1689	14.07 %
Allowed	1366	11.38 %
BusinessAndEconomy	929	7.74 %
Others	3766	31.38 %

View All

Figure 8. Graph showing web categories used by the users.



Domain	Bytes	Percent
*.googlevideo.com	2.34 GB	69.08 %
*.c.docs.google.com	447.71 MB	12.89 %
smumcdnems02.cdnsrv.jio.c...	67.43 MB	1.94 %
smumcdnems01.cdnsrv.jio.c...	67.34 MB	1.94 %
Others	491.89 MB	14.16 %

View All

Figure 9. Graph showing top web domains.

III. RESULT AND DISCUSSION

The following results can be drawn from the above figures.

Figure 1 & 2 shows that 81% of the traffic is being used by Streaming media, 11.52%, General Internet and the rest in Infrastructure, mobile & other behavior. Thus by restricting the usage of streaming media at individual user level, the usage can be more smoother for productive purposes.

Figure 3 & 4 shows that the top users of the internet which shows 62% of the traffic used by only four users whereas the rest of the users constitute only 38%. Thus by restricting the usage at individual level to a few Gigabytes per month, more users can avail the network efficiently.

Figure 5 & 6 shows the top Source and Destination countries which shows 76.16% of traffic to Indian Servers, 21.43% to United States and the rest to other countries

Figure 7 & 8 shows the rule IDs which are accepted showing Rule 3 constitutes 87.22%, Rule 23 6.51%, rule 25 6.06% and rest others. Also the web categories show 35.43 constitute IT, 14.07% Social Networking, and the rest others. Thus by specifying Rule 3 at a higher level the traffic can be rejected earlier and do not need to pass up to rule 3.

Figure 9 shows that 80% of traffic is used for google, and the rest by others. Here also rules can be framed to stop misuse of same and a uniform distribution of resources.

IV. CONCLUSION

The result of my analysis will be an improvement in firewall rule specification that will illustrate the distribution of firewall vulnerability causes and effects over firewall operations. The above mentioned scenario is useful in avoiding and detecting unforeseen problems and proper distribution of resources to all the users during firewall implementation and firewall testing. It will help to frame firewall rules that are custom to an organization thus providing higher efficiency and lower vulnerability.

V. REFERENCES

[1] Dr. Ajit Singh, Madhu Pahal & Neeraj Goyat, "A Review Paper on firewall", International Journal for Research in Applied Science & Engineering Technology, Vol. I, Issue II (September 2013)

[2] Sachi Pandey , Vibhore Tyagi, "Performance Analysis of Wired & Wireless Network using NS2 simulator", International Journal of Computer Applications, Vol. 72, No. 21 (June 2013)

[3] Mr. Sachin Taluja, Mr. Pradeep Kumar Verma, Prof. Rajeshwar Dua, "Network Security Using IP firewalls", International Journal of Advanced Research in Computer Science & Software Engineering, Vol. II, Issue 8 (August 2012)

[4] Safaa Zeidan1, Zouheir Trabelsi2, "A Survey on Firewall's Early Packet Rejection Techniques", International Conference on Innovations in Information Technology (2011)

[5] Andrew Lockhart, "Network Security Hacks", O'Reilly Media (2004)

[6] William Stallings, "Network Security Essentials", Pearson Education (2011)