IJCSN - International Journal of Computer Science and Network, Volume 6, Issue 4, August 2017
ISSN (Online): 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Tuning Firewall Based on User's Usage Statistics

[1] V. Valli Kumari; [2] K.V. Kalyan Chakravarthy

[1] Dept. of Computer Science and Systems Engineering. AU College of Engineering (A)
Visakhapatnam – 530003, Andhra Pradesh, India

[2] Dept. of Computer Science and Systems Engineering. AU College of Engineering (A)
Visakhapatnam – 530003, Andhra Pradesh, India

Abstract -The number of Internet users worldwide has skyrocketed since the birth of the World Wide Web. Users access different internet websites includes social networking websites, peer to peer or other categories which affects internet bandwidth of the organization. Internet service provider (ISP) will send warning mails forcing administrator to identify the user who is accessing or misusing internet service. Monitoring of network data gives overall network flow in organization. Monitoring can be done within the firewall or redirecting the logs that are received to external server. External log server can be deployed, if organization is large in size as the traffic flowing through the firewall will be more. So internal storage for storing of such huge data can't be done. This paper proposed a new deployment technique which helps the administrator to automate by using predefined policies of the organization user behavior and bandwidth are monitored. To conserve this system automated operation, every step is recorded in log server and evaluated. Tests are developed and analyzed on proposed system resulting in good result.

Keywords - Logs, RMON, SNMP, MIB, Access list

1. Introduction

Internet traffic monitoring is a process of observing data flow between two end user devices in network through network devices for communication. Each data that is sent or received from the network is monitored by firewall. Alerts are generated based on the unauthorized access in network by log server. Administrator will take action on user based on alert severity. There are two different techniques, Router based and Non router based [1]. Router based techniques have a built-in functionality that supports software and hardware. Non-router based techniques require additional software and hardware to be integrated into the system. Simple Network Management Protocol (SNMP) is the basis for network monitoring and analysis. It can be defined as a set of protocols that manage and monitor the network [2]. These protocols are supported by routers, firewall and bridges. All these devices are connected to the network, which needs to be monitored for detecting the conditions. The Remote Monitoring (RMON) protocol helps various network monitors and console systems to exchange network monitoring data [3]. RMON is typically implemented in a client-server model. It supports continuous off-line monitoring in the presence of failures It is primarily used for analysing network traffic and determining incoming and outgoing traffic, as well as the amount of traffic being generated. Goal of this paper is to automate by intercepting the user behavior and bandwidth, if that user goes against the policies of organization

1.1 Existing System

In an organization, as number of users increases, use of internet access will also increase, hence there is rapid increase in log data which contains all types of data. In previous work of authors [4], a system which collects the logs and saves them in the database. Administrator gets an alert message based on functionality of user in network. Based on the policies administrator of the organization, will take action on the user and is known as passive monitoring. It is defined as devices are polled periodically and information is collected using SNMP protocol, the data is extracted from Management Information Bases (MIB) to assess network performance and status, there may be delay in analysis or the data may be overwritten due to less storage in devices. So external log servers are used in order to overcome this problem. External log server can save raw data until the storage gets exhausted. Mails are sent by ISP to administrator to identify the user who is tries unauthorized access to remote web server. To identify such intranet users external log server plays important role. As this is passive monitoring the data is stored in database, based on time-stamp, IP address and port number users are identified in campus. Major disadvantage of this type is user may pretend as if user didn't access the internet. In new proposed system this problem is overcome by automatically blocking the user if he tries to bypass the policies of the organization. Existing system is shown below.

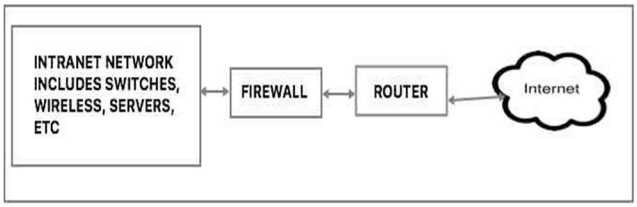

Fig: 1 Existing system in an organisation

2. Proposed System

In the proposed system when an entry hits the router or firewall the entry data is sent to the log server. Each hit or entry is taken as 'e'. In the log server preprocessor is present which is responsible for processing the raw data into predefined values and these values are sent to the database for storing.

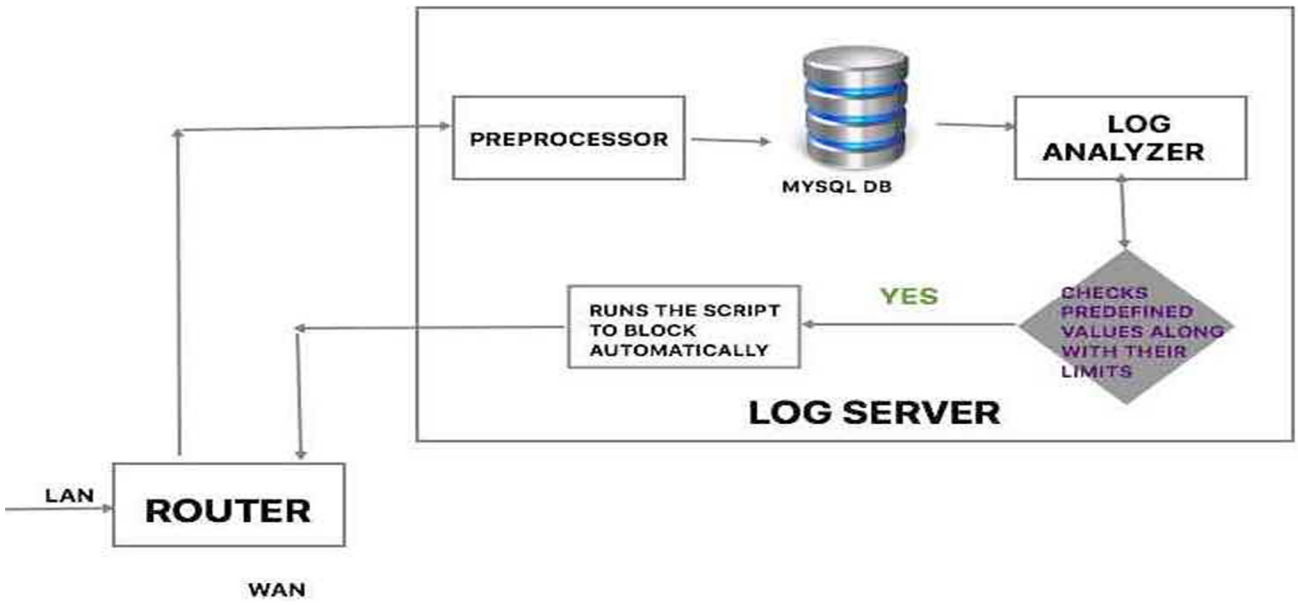

Fig: 2 Proposed system in an organisation

Once the preprocessed data is stored in the database, data is ready for analysis. For every organization there will be a set of rules which are predefined policies. For example, in an organization the user should not access torrents, proxies and malware sites or software. These rules will be defined in analyzer so that once user tries to access any one of the above said websites it will check number of hits, user or the ip address that is being accessed that website / application. If the default value of the threshold is 'x', then For experimentation we have considered seven days' raw data and categorized based on category of the hit or the website it belongs. Here we considered four main categories which include social networking, Peer to peer, proxies and Virus. These categories are divided based on the total number of hits in a day. Suppose 'totalhits' is the total number of hits in a day and snlnw, p2p, virus and proxy are the social networking, peer to peer, virus and proxy respectively.

If **e >x = True** ; blocks user from access the internet for t seconds

= False: Denies user to access webpage, displays access denied page

Now, the number of hits of category are analyzed from the given total number of hits. An sql query is executed for extracting the total number of category hits from the total hits is given by

*Select * from hits where ctgy="x";* ---------- (1)

where x denotes which category of the information to be extracted from the total information. The details of the above daily hits are shown below.

Date	Total Hits	Social Networking (snlnw)	Peer to Peer (p2p)	Virus (virus)	Proxy (proxy)
11th Feb 2017	25,000	1,236	3,487	345	1,324
12th Feb 2017	24,573	3,345	1,286	175	1,422
13th Feb 2017	29,843	2,635	3,485	635	1,108
14th Feb 2017	34,790	5,326	2,754	1135	1,529
15th Feb 2017	42,746	3,983	4,111	1573	1,632
16th Feb 2017	39,279	4,290	5,634	986	1,212
17th Feb 2017	31,674	2,345	2,255	1643	1,274
Total	2,27,905	23,160	23,012	6,492	9,501

Table 1: Daily total hits and category wise hits

"snlnws" is taken into consideration, as total number of selected hits of social networking category and given as

$$snlnws = \sum_{i=1}^{7} \text{snlnw(i)} \quad \text{----------} \quad (2)$$

Similarly, other categories and their total sums is shown in the table 1. Total percentage of hits for individual categories to the total number of hits for one week can be calculated based on the following equation 3. totalhits is total number of hits for one week. snlnws, p2ps, viruss and proxys are the total number of category wise hits for one week. TH is the percentage of unauthorized hits by the user in organization.

$$TotalHits\% = [\{\sum(\text{snlnws} + \text{p2ps} + \text{viruss} + \text{proxys})\}/\text{th}] * 100 \quad \text{----------} \quad (3)$$

Based on equation 2, lets consider Facebook as our social network category for blocking the user in the network. So equation 4 can be rewritten as

*Select * from hits where ctgy = "snlnw"; ------ (4)*

Based on the equation 4, data is saved in temporary table for further analysis is shown below.

Time Stamp	IP address	Category
11-02-2017,11:45:20	10.2.5.11	Facebook
12-02-2017,17:00:20	10.1.55.212	Facebook
13-02-2017,12:46:20	192.168.11.54	Facebook
14-02-2017,10:33:20	10.5.32.14	Facebook
15-02-2017,19:54:20	172.16.111.21	Facebook
16-02-2017,15:12:20	10.11.4.2	Facebook
17-02-2017,11:26:20	10.12.11.123	Facebook

Table 2 table showing ip address and category for one week

Total number of hits of user who tries to hit the above mentioned category by using the query as shown in below syntax.

Select (count ipa) from hits where ctgy= "snlnw"; ---------- (5)

Top five output of above syntax is shown in table 3

IP address	Number of hits
10.2.5.11	942
10.1.55.212	862
192.168.11.54	640
10.5.32.14	449
172.16.111.21	245

Table 3 IP address Vs total number of hits for one week

In table the analysis of top five users and their hits are shown. based on the above scenario one might know whether the network is misused rather than using for informative purpose

Select count (ts) from hits where ip = "10.2.45.11"; ---------- (6)

The above equation selects the average number of hits for every 24 hours for a particular selected ip address.

Time stamp	Number of hits
11-02-2017,11:45:20	442
12-02-2017,17:00:20	382
13-02-2017,12:46:20	250
14-02-2017,10:33:20	637
15-02-2017,19:54:20	501
16-02-2017,15:12:20	658
17-02-2017,11:26:20	596

Table 4: Timestamp and number of hits of an ip address

Blocking of user can be done using shell script programming here, python is used, that is IP address of the user is saved in one of files where all list of ip address are saved which are to be blocked and named as toblock.txt. Blocked list of ip address along with timestamp is saved in another text file named as blocked.txt. Implementation is done in operating system is Centos 6.8. In every device SSH should be enabled along with SNMP [5] protocol. Script that needs to run the command is saved in script.py. Administrator set the timer in the crontab, where after timer becomes zero automatically the script runs without the help of any network engineer or administrator. Address which are listed in the text file (toblock.txt), based on the timer that admin has set in crontab, script will start executing. It takes the ip address from toblock.txt file and executes deny rule and appends the blocked.txt with this ip address and time stamp are recorded for further allowing the user to access internet after a particular period of time. Deny rule is shown below

Object host b1
Ip address 10.1.15.11
access-list 123 deny host b1 any.

Once this access list[6] is executed, user will be blocked. In order to revoke back access list based on the timer that is set by admin. Revoke.py program is used to revoke the blocked set of ip addresses from the blocked.txt.

After the ip address is revoked the ip address is cleared from blocked.txt file and saved in ublock.txt. ublock.txt file contains all the ip addresses that are revoked in past one week. Along with this a table is maintained in the database that records all the user information includes username, ip address and number of times it is blocked. Syntax to revoke the access list and access to internet is shown below.

Object host b1
Ip address 10.1.15.11
no access-list 123 deny host b1 any.

Based on these access list the administrator able to block or unblock the user so that there is no intervention of admin. If this has to be done manually, admin needs to block and unblock each and every ip address and may have user influence on the administrator. But in proposed scenario there is no intervention of any user. Time gap between the block and unblock time can be decided based on the policies of organization. For example, let consider 10.1.15.123 is an ip address that is being accessed continuously to torrentz2.eu website. Once the request is received from the user to firewall LAN port it stores the data in the database and also forwards it to the log analyzer to check whether the user has tried to access the same website before. Log analyzer check the number of entries user tries to access. Once the user exceeds the threshold immediately log analyzer sends and appends ip address to toblock.txt after a particular time once the timer becomes zero the code execution starts. In this IP address from the toblock.txt is taken and sends to the router to execute the block of internet for some duration of time. This duration can vary based on organization to organization.

Object host b2
Ip address 10.1.15.21
access-list 123 deny host b2 any.

Access list is deployed to server the ip address in the toblock.txt will be removed and gets appended in blocked.txt along with timestamp. Here 60 mins duration is taken for unblocking of user. Once timer in crontab becomes zero, ip address from the blocked.txt is retrieved by comparing the timestamp of IP address with the current timestamp. Difference between two timestamp exceeds the value of 60 mins then automatically unblock script will execute in order to remove the entry in the router or firewall

Object host b2
Ip address 10.1.15.21
Access-list 123 deny host b2 any.

After unblocking of the ip address count in the table of ip address will increase by one to this ip address 10.1.15.123. Data related to this ip address will be removed from all the text file except in the database. In this paper, the network was monitored continuously and it is active monitoring.

On the other hand, this paper also discusses about the restriction of bandwidth for unauthorized access of any application that leads to downfall of the organization. Let's consider social networking websites, which user is updating his / her information in social websites. If admin wants to block the access of that particular user or he can block access of that website or any application after exceeding the bandwidth limit of that user or to overall organization.

Suppose if admin wants to block access to website like facebook after exceeding the bandwidth limit of 1GB per day, we can block manually by denying rule in firewall. Then admin needs continuous monitor of all the websites which users are accessing internet. Because of automation of firewall, admin can write his/her own rules based on policies of organization.

In order to make network automated, organization should have authentication authorization and accounting (AAA) server where all user related information resides. In this server, admin can write his /her own rules so that user bandwidth can be monitored. But admin needs to block the user if he tries to misbehave or unauthorized access to internet. In the proposed system blocking of user is automated. Below figure shows us the manual blocking of user from a AAA server like 24online [7].

Next>>

Account Id	User Name	Package Name	FAP Name	FAP Limit(MB)	Current FAP Cycle Usage(MB)	Datatransfer Type	Cycle Type	Next Reset Date	Switch Over Bandwidth Pol
A000001946	151fa17024	Unlimited Usage	stdnt	10240.0	10680.87	Total	1 x Monthly	30/04/2017 23:59:59	students crossed
A000001883	151fa05135	Unlimited Usage	stdnt	10240.0	12501.61	Total	1 x Monthly	30/04/2017 23:59:59	students crossed
A000001981	151fa04241	Unlimited Usage	stdnt	10240.0	11454.5	Total	1 x Monthly	30/04/2017 23:59:59	students crossed
A000001603	151fa05283	Unlimited Usage	stdnt	10240.0	10291.3	Total	1 x Monthly	30/04/2017 23:59:59	students crossed
A000001628	151fa05153	Unlimited Usage	stdnt	10240.0	10253.93	Total	1 x Monthly	30/04/2017 23:59:59	students crossed
A000001878	151fa05289	Unlimited Usage	stdnt	10240.0	12846.91	Total	1 x Monthly	30/04/2017 23:59:59	students crossed
A000001593	151fa08091	Unlimited Usage	stdnt	10240.0	15306.65	Total	1 x Monthly	30/04/2017 23:59:59	students crossed
A000001889	151fa11005	Unlimited Usage	stdnt	10240.0	10746.25	Total	1 x Monthly	30/04/2017 23:59:59	students crossed
A000002010	15fe1a05c9	Unlimited Usage	stdnt	10240.0	11249.55	Total	1 x Monthly	30/04/2017 23:59:59	students crossed
A000002005	151fa08114	Unlimited Usage	stdnt	10240.0	14117.49	Total	1 x Monthly	30/04/2017 23:59:59	students crossed
A000002062	141fa08079	Unlimited Usage	stdnt	10240.0	12783.38	Total	1 x Monthly	30/04/2017 23:59:59	students crossed
A000001567	141fa12032	Unlimited Usage	stdnt	10240.0	11371.59	Total	1 x Monthly	30/04/2017 23:59:59	students crossed
A000002056	13fe1a0499	Unlimited Usage	stdnt	10240.0	15428.25	Total	1 x Monthly	30/04/2017 23:59:59	students crossed
A000001907	151fa07039	Unlimited Usage	stdnt	10240.0	10595.29	Total	1 x Monthly	30/04/2017 23:59:59	students crossed

Fig: 3 Users exceeds the bandwidth limit

Above figure shows the user has crossed the bandwidth. So internet access will be blocked. In our proposed system if total bandwidth used by all the users for an application exceeds FUP limit then user can access all websites or application except this application.

4. Conclusions

Based on the tests which we performed, proposed system had shown good results. Without any intervention of the administrator, the system could be implemented in small and big organizations. In small organization admin can restrict the bandwidth so that other users who require access to internet can be used. In big organizations, system can automatically monitor and block user immediately so that organization reputation with not be defamed because the system has been automated. In future the system can be extended to servers so that we can restrict unauthorized access and reduce attacks to the server.

References

[1] Pries, R., et al. Traffic Measurement and Analysis of a Broadband Wireless Internet Access. in Vehicular Technology Conference, 2009. VTC Spring 2009. IEEE 69th. 2009.

[2] Xinyu, X. and S. Mishra. Where is the tight link in a home wireless broadband environment? in Modeling, Analysis & Simulation of Computer and Telecommunication Systems, 2009. MASCOTS '09. IEEE International Symposium on. 2009.

[3] Alisha Cecil. A Summary of Network Traffic Monitoring and Analysis Techniques. Available from: http://www.cse.wustl.edu/~jain/cse567-06/ftp/net_monitoring.pdf.

[4] Prof. V Valli Kumari, K V Kalyan Chakravarthy. Analysis of user's behavior in the network using log data. IRACST- International Journal of Computer Networks and AWireless Communications (IJCNWC), Vol. 7 No.2 Mar 2017. Under printing

[5] Jianxin, L. and B.J. Leon. A formal approach to model SNMP network management systems. in Computer Communications and Networks, 1995. Proceedings., Fourth International Conference on. 1995.

[6] Prakash Chandrasekaran, Access Control Lists, ISEA, IMSc, 22 May 2006.

[7] http://www.24onlinebilling.com/telecom-internet-billing-software-solution.html

[8] www.cisco.com.