ISSN:0975-9646

Automation of Firewall Management System.

Amit Sulakhe [#1], Ravindra Divekar [*2]

[#1] *MTECH Information Technology*
K.J. Somaiya College of Engineering, Vidyavihar, Mumbai-77
**2 Professor, Dept. Information Technology*
K.J. Somaiya College of Engineering, Vidyavihar, Mumbai-77

***Abstract*— Nowadays in most of the field, there is a trend of automation process which eliminate human error and remove dependency of manual changes. In information security area automation is required to remove human error for the same kind of work, and also there does exist some automation tool but it is mostly up to some restricting privilege level. In network security firewall management existing tool does not change in firewall policy level. In future, Automation tool required blocking or allowing some policy automatically and this makes for the same kind of work. In this project automation tool creates rules in firewall to pass traffic and also do blocking of blacklist IP and services in firewall within a live session because of which cover some level of security in organizations.**

***Keywords*— Automation, Firewall.**

I. INTRODUCTION

When we talk about security of the system always come first with a firewall system which can also says 'great wall of the network system' to secure of internal networks. A network firewall is intended to stop unauthorized users from accessing the network and its services from other external networks [4]. In its simplest form, a firewall is a combination of hardware and software devices, which bifurcates the internal network from the outside networks (Internet) and blocks certain traffic and allows some specific traffic [4]. A firewall is an important factor in network security as it is work according to a defined security policy. Policy installation does by the network administrator as per privilege request got through any system like email system, request incidence system. While installing policy or any updating in the firewall system manually can be difficult to maintain speed of business.

In this paper, we will propose an automation system which automates some task of firewall administration and also do tasks like blocking access of the malicious URL.

Automation of any particular system makes easy doing and continuity of business, make profitable to the organization and curb human error which increases accuracy take good example of self-driving cars which will be safer than human drivers. Due to this reason demand of automation increase in various fields. Automation process has successfully experimented and also deployed in various fields where having repetitive task. In network security system, the administration has lots of work and become difficult to manage and monitoring the network components continuously which raise the requirement of automation tools or system. In information security domain there are various tools or system which automates the process of securing a network system. Automation tools are available which manage the firewall and also monitors continuously firewall system, but these various tools are not doing complete automation process of the firewall. According to article in networkcomputing [2], "It's time to delegate the manual process of firewall policy changes to software intelligence".

In near future there will be require an automation system which makes changes in firewall policy.

In our proposed system will stop access of malicious URLs by blocking IP of corresponding to it, this is done as per input from email or user info or current URL from URL bar of the browser and also do firewall administrator tasks like creating and pushing policy in firewall which is can allow or block the of particular system as per recommended by email.

II. EXISTING SYSTEM

There are various existing system are available to manage the firewall, but these tools offered a comprehensive firewall optimization management solution which verifies changes in firewall. These tools are orchestration tool, not the complete automation tool. The difference between automation and orchestration is Automation is about codifying tasks and orchestration is about codifying processes [3].

Today firewall changes are done manually way. Firewall administrator or network administrator is responsible for making changes by installing or updating any policy on the firewall. These processes are done by referring orchestration tool or request process of organization.

The main drawback of this system makes some impact on the business continuity process when manually changing in firewall gets complicated when there is more number of firewall rules and rate of changes has to come, which makes confusion to administrator and get a rise of complaining from the client side because of slow response or a slow work process.

Depend on manual also create problems when a person has lack good experience and knowledge about firewall system and network structure, these could do damage to network infrastructure and also make an impact on the business continuity process of the organization.

The Main Goal in network security is 'keep business running securely without downtime and protect data'. This can be achieved by automating some task or process which is repetitive, and makes fast process and also new evolution in security field.

III. PROPOSED SYSTEM

In the proposed system, automation process will do on an open source firewall system. In this process policy will be executed on the firewall as mentioned in the email and also examine URL received from email or user input or get current URL from URL bar, this URL will be blocked if it found as malicious URL/IP. In this way network system will secure and also go to one step ahead in automation era.

Below Automation process, classify into Two types-:

A. *TYPE I:*

As shown in fig 1, Automation system gets the URL through an email , User input, and current URL from URL bar. The system will extract the URL from either the mailbox of the network administrator, or through the input provided by the network admin in the textbox provided.

Then the input URL is sent to VirusTotoal for analysis. VirusTotal is a free virus, malware and URL online scanning service. URL checking is done with more than 40 antivirus solutions [1]. Our system can also be integrated with antiphishing, antivirus and other tools which are used to identify malicious URL's.

After getting result from Virustotal, System will analyze multiple output of Virustotal and decide whether a URL is malicious or not malicious. If url is malicious then the URL is sent to extract a list of IP addresses corresponding to the URL. Then the system will take an IP and URL, check in its database wheteher that IP and URL already exist or not. If URL and IP does not exist then system will send the IP to shell script module which executes IP and push policy in the firewall using firewall command and simultaneously updates its own database which is to be used in future. And lastly, our System will send a notification mail to the administrator.

By this process security is increased by not allow accessing the malicious URL.

The advantage of this system makes more secure to internal system by blocking black listed URL, which denied access and block traffic from both outbound and inbound way.

This system can integrate with antiphishing tool, so that an identified phishing website can be blocked in the firewall immediately without interfering of manually processing. Later, after blocking process automation system can alert to administrator about blocked website along with IP corresponding for same.

Similarly, the process can do with other integrated systems like antivirus, advance persistence threat, machine learning system.

A. *TYPE II:*

As shown in fig 2, Automation system gets the email. Extractor extract Source IP, Destination IP, Port no, Service Type from mail body. Then the system will check into database to identify whether extracted data is already existed or not. Because of this there can be prevent from the overlapping rule in the firewall. If extracted data already exist, then send a reply to the user or requester. If not existed then system send data to execute module, in this module execute a shell script to install policy on the firewall. After execution and installation notification mail sends to the administrator.

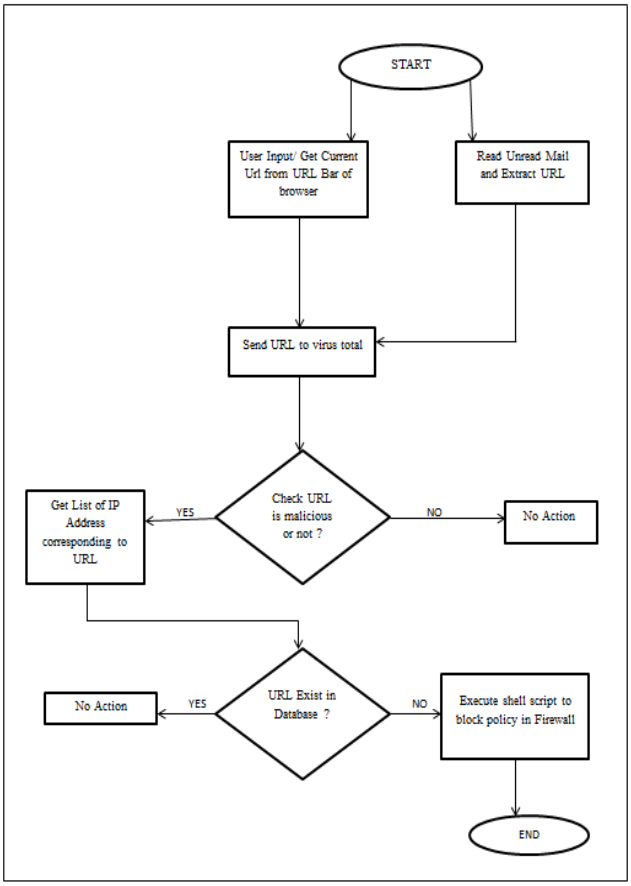

Figure 1. A flowchart for blocking malicious URL

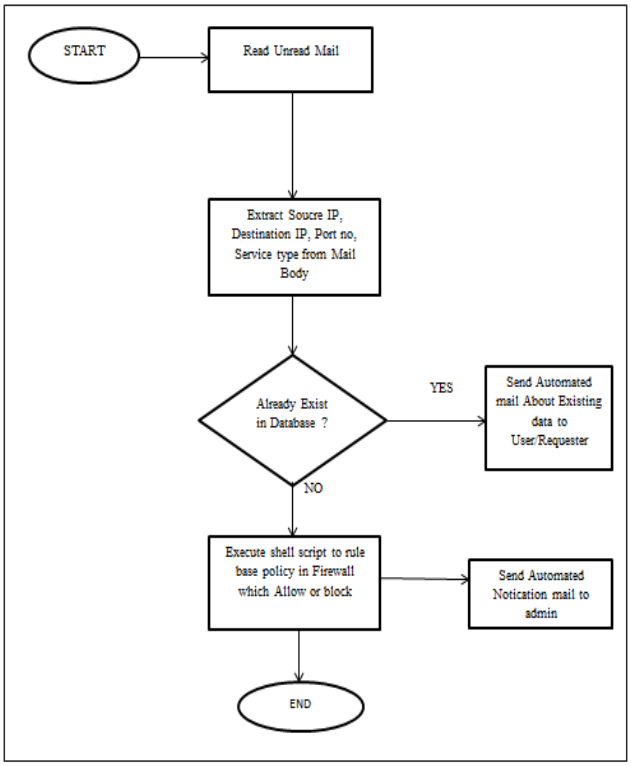

Figure 2. A flowchart of creating rule base policy in firewall.

The advantage of these tools is to make fast process of firewall changes and also positive, effective when number of firewall rule and rate of changes increases.

Secondly, Its eliminate human interaction for the same task because of this increase speed of work and also an administrator can focus on other security work system where they have require to.

IV. FUTURE SCOPE

Currently, our automation system work to make changes in firewall like configuring firewall rule. In future, our system will work with dynamically which manage configuration of the firewall like

- Automation system will automate VPN configuration in firewall,
- It will also can check and update firewall operating system patches regularly.
- Automation system will run penetration tests on the firewall to check how secure your network is from attacks and will maintain schedule regular firewall audits.

V. CONCLUSION

Our system manages firewall policy by configuration in automate process of block malicious URL/IP which help guarding to internal network system from accessing phishing or malicious website. The system also provides security in real time from accessing malicious websites using GETCurrenturl method and detecting unread mail method which forward to block malicious websites immediately at the same moment.

The system manges configuration of firewall change rule base policy by detecting unread mail which eliminates human interaction from repetitive tasks and also curb human error.

This automation system is made beginning step of the automation process in the information security field.

REFERENCES

[1] VirusTotal. Available at: https://www.virustotal.com/
[2] Networkcomputing article Available At https://www.networkcomputing.com/net-security/automating-firewall-administration/
[3] https://devops.com/automation-versus-orchestration/
[4] Umesh Hodeghatta Rao and Umesh Nayak , " The InfoSec Handbook – An Introduction to Information Security" Apress open, 2014.