A Survey on Emergent Firewall Techniques in Computer Networks

Bharath.R[1], Mahesh.M[2], Lakshmi Narayan Reddy[3], Dr. Anand Jatti[4]

[1]B.Tech Student, Dept. of Electronics and Instrumentation, RV College of Engineering, Karnataka, India [2]B.Tech Student, Dept. of Electronics and Instrumentation, RV College of Engineering, Karnataka, India [3]B.Tech Student, Dept. of Electronics and Instrumentation, RV College of Engineering, Karnataka, India [4]Associate Professor, Dept. of Electronics and Instrumentation, RV College of Engineering, Karnataka, India

---***---

Abstract - *Network security is a system that is developed to monitor the malicious activities and safeguard the network, which includes the authentication of information access in a network, that is being controlled by the network administrator. A firewall in a network security system is a tool/software that monitors and controls network traffic. The role of a Firewall is most evident inthe huge organizations or a business. For smooth run of any organization, it is very important to protect their data as well as their client's data. The Firewall helps in ensuring the safety of sensitive and confidential data that the businesses is currentlydealing with. In modern-day scenario, there is no better option*

for organizations to protect their data than a robust Firewall. It also aids the network administrators to keep the data virus free andalso prevent any intruders from accessing the data. In this paper we bring out the features that the current firewall techniques isoffering and also analyze the same with respect to different network scenarios.

In this paper, we are comparing and analyzing different firewalltechniques that are of great help by providing useful insights tothe cyber security industry.

.

Key Words: Next-gen firewalls, Software-defied network (SDN) firewall, Cloud based firewall

1. INTRODUCTION

A network consists of various methodologies developedbya network administrator to avoid and prevent misuse of access or alter data in the network.

To safeguard the data and the complete network, various amendments have been developed over the years. These amendments have been considered powerful and an important factor for preventing security breach in any network. Thus, various organizations have started implementing these techniques in their data networks. These technique are robust and redundant in nature. They provide secure streams to send and retrieve data and also provide backup in case one of the security feature fails. Each technique has its ownadvantages and disadvantagesandact differently in different scenarios.

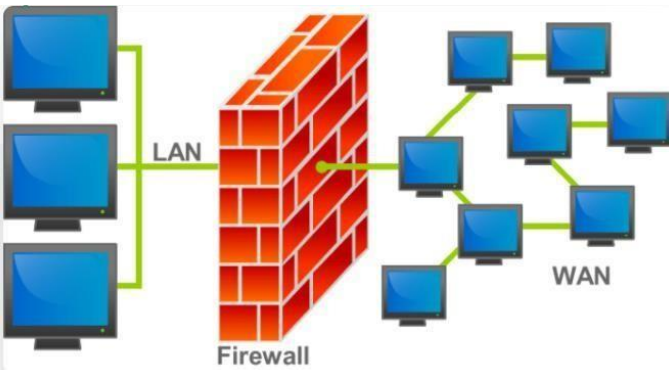


Fig -1: Illustration of firewall

2. THREATS IN A NETWORK

Network threats are getting intense as there is a level of increase in the remote work from past few years. The term "Work from Home" is common term that can be heard numerous number of times. These factors have lead us to be more dependent on the digital devices and their services that are currently being used. Let us look at different types of threats that have been identified at present.

Social engineering: To avoid social engineering scams, organizations can restrict user over the access privileges and lasts only for the time needed for the task to be is granted access privileges for one particular task and lasts only for the time needed to complete it.

Ransomware: Ransomware is a data-encrypting program that requires payment to be made to release the infected data from the user or organization's network.

DDoS attacks: DDos stands for denial of service attack, which is one of the cyber-attacks in which the person/virus is responsible for the malfunction of the network temporarily or indefinitely disrupting services of the host connected to that particular network.

Cloud computing vulnerabilities: Some of the cloud computing vulnerabilities include unauthorized access due

to non-reliable or non-redundant access controls and unauthorized usage of employee credentials.
Unauthorized access and insecure application program interfaces (API) are the important factor responsible for the vulnerability in in cloud computing.

3. FIREWALLS

To prevent or stop such attacks or activities as discussed in the above paragraphs, firewalls have been introduced. They have been one of the main factor that has been rapidly developed and modified over the years. Let us lookatsomeof the current models/techniques that are being implemented as of today.

3.1 Next-gen firewalls

Next-generation firewalls (NGFWs) are one of the updated versions of firewalls which is capable of battling malware assaults that have been increasing day by day. Since the firewall is the front line of resistance against suchassaults, it makes sense that firewallsare being developed rigorously to tackle the threats

A next-generation firewall is a security that is pre-programmed with a set of instructions that can filter malicious activities by implementing different security methodologies at the application level. It is a system comprised of various individual units that have their own specific function. The combine with other system filtering functionalities.

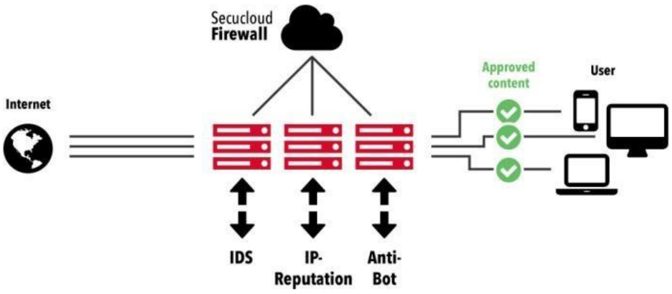


Fig -1: Next gen firewall developed by Secucloud

The insights given by analysis of traffic by next gen firewalls can help in both bandwidth and security aspects. Since they are advanced and give more detailed picture if the activities, it is impossible for a malicious activity to surpass it. They allocate process by providing Quality-of-service (QoS) capacities according to their respective bandwidth. Due to the increase in cloud services and Software as service enterprises, next generation firewalls are in demand due to their features. Next generation firewalls follow unifiedthreat management arrangement

There are few features that the next generation firewalls offer that is central and powerful management, user and or application control, high availability, plug and play deployment, virtualization and enterprise level of VPN.

Advantages:	Disadvantages:
Provides an optimal layer of filtering	Necessity of integration with other security systems
Provides accurate insights of the activities through tracking	Costlier to implement when compared with other firewalls

Table -1: Pros and cons of Next gen firewalls

Cutting edge threats like social engineering, ransomware, denial of service attack and cloud vulnerability are rapidly changing the threat landscape from bad to critical. In fact, greater than 80% of all the new malware are misusing fragility in the applications that are running in the system rather than the fragility in administration services of the system.

3.2 Software-defined network firewalls

The architecture in the software defined network firewall is designed to function as a control point created to label the issues with respect to the other networks that areinterfaced with each other. Software defined network is more of a framework than a mechanism. Its features such as path handling, the flow routes and its topology increase its performance and also reduces the overall cost.

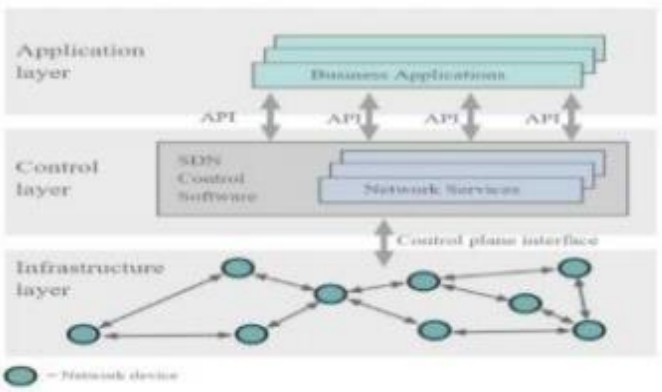


Fig -2: Architecture of SDN

The SDN firewall model or technique is quitepopularinmany enterprises or organizations as of today. It is implemented in various startups in their data networks through their network administrators. The companies can drastically reduce the cost as this technique or model eliminates the need of hardware components in the network. Thisalsohelps us to improve the overallsecurity of the network by reducing the components. Apart from this, the process of replacing firewall is also a tedious procedure as it involves operations such as reconfiguring each and every device in the network and also to troubleshoot the entire network.

Here are few commands used in SDN firewalls:

Add: This command takes in the parameters and adds them to the list consisting of all the rules in a dictionary format.

Delete: This command enables us to take the rule name as an input, and deletes from the rule.

Show: These commands show the name of the rules present in the list.

ShowComplete: This command shows entire list of rules that are present.

SwitchPro: This command takes name and a new priority as its input, and switches the order of the list.

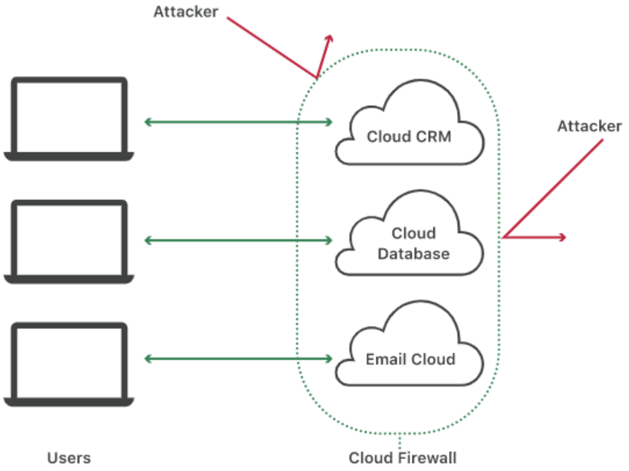
Advantages:	Disadvantages:
Provides better visibility	Prone to distributed denial of attacks
Better security by blocking unauthorized routes	Absence of hardware security(Physical routes and switches)

Table -2: Pros and cons of SDN firewalls

Thearchitectureaims to make networks secureand versatile through programming using different programming languages in the networks. With respect to the functional aspects of the device, we can divide the firewall into two planes. One being the control plane and other being the forwarding plane. In the control plane, SDN controller provides interfaces to the application through API's. Now the packets are being forwarded to the forwarding logic in the form of flow rules to the open flow switches.

3.3 Cloud based firewall

From past few years, firewalls are being run in between a safe internal network and an unsafe network that is in between a private network and a public network such as the internet. Initially, firewalls were physical hardware component in the organization or enterprise's data network. The firewalls allow or stop the network activities according to predefined set of rules. Few firewalls provided access to modify or alter network to their respective network administrators. But on the arrival of cloud computing, the difference that existed between an internal network and the internet is absent. Thus, there is a need of a virtual barrier in between the two and this is being provided by the cloud based firewall.



e

Fig -3: Cloud based firewall

The network perimeter is that divides internal data network and the access network. The internal network is managedby the enterprise or an organization while theaccess networkis is managed by an internet service provider. Thus we can say that the network perimeter is the final element that can be controlled by the enterprise or an organization. It can be used to shut down the internal network if there is any necessity. Earlier, firewalls were designed to control such network perimeter and monitor the activities passing through it.

Advantages:	Disadvantages:
Remote access using a browser	Subscription based services
Managing multiple devices at same time	Not applicable for all enterprises

Table -3: Pros and cons of cloud based firewall

But whenwe talk about cloudcomputing, the term"Network perimeter" can be eleminiated. The physical location or the device that the user is using to access the network doesn't matter. It is impossible to add an extra layer of security at the enterprise or organization's resource, as we cannot predict exactly where the layer should be placed. Few enterprise or organizations do not want to integratesecurity components such as traditional firewalls, networkcontroller, access control as it makes the network more complex for modification and troubleshooting.

4. CONCLUSION

Our main intention behind writing this paper was to provide an insight on the latest firewall techniques that are being developed in recent years. As time progress, we arerealizing that cyber security is one of the main aspect that startups or organizations are focusing on. In this digital era, anything and everything is being carried out online. Thus, protection from security threats such as ransomware, DDoS, data theft can be obtained by implementing one of these firewall models in our networks. While choosing the right firewalls, one has to keep in mind the cost factor, security infrastructure or the framework, update and modification if necessary in future hardware and software requirements and performance of the network. Each of these type has its own requirements from the user end and one can provide his or her the best firewall by considering the above factors and choosing the right firewall technique.

REFERENCES

[1] Manoj R Chakravarthi's, "Next Generation Firewall- AReview", International Journal of Computer Science and Information Technologies, Vol. 7 (3) , 2016, 1212-1215

[2] Sheetal Khodbhaya, Nimit Tiwari, Sachin Mahto, Jishnu Unnikrishnan and Prof. K.S. Charumathi's ,"Centralized Firewall for Software-Defined Networking (SDN)", International Research Journal of Engineering andTechnology (IRJET), Volume: 0 7 Issue: 05 | May 2020

[3] V.Mamatha Reddy. P.Poornima,"COMPUTER NETWORKS AND SECURITY : A REVIEW", International Research Journal of Engineering and Technology (IRJET), Volume: 03 Issue: 10 | Oct -2016

[4] https://www.secucloud.com/next-gen-firewall

[5] https://infosecaddicts.com/meant-firewall-network-security

[6] https://www.secucloud.com/next-gen-firewall

[7] https://comsoft-bh.com

[8] https://www.itcentralstation.com

[9] https://www.cloudflare.com

BIOGRAPHIES

Bharath.R is currently pursuing B.Tech degree in Electronics and Instrumentation from RV College of Engineering, Karnataka. His primary research interestinclude communication systems and security networks.

Lakshmi Narayan Reddy is currently pursuing B.Tech degree in Electronics and Instrumentation from RV College of Engineering, Karnataka. His primary research interestinclude computer communication (CCN) networks.

Mahesh.M is currently pursuing B.Tech degree in Electronics and Instrumentation from RV College of Engineering, Karnataka. His primary research interestinclude computer communication (CCN) networks and signal processing.

Dr. Anand Jatti

Dr. Anand Jatti is an Associate professor in Electronics and Instrumentation department at RV College of Engineering, Karnataka. His primary research interest include image processing and signal processing.