International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol. 9, Issue.11, November 2021 E-ISSN: 2347-2693

Protection of Network Devices and Data security using Firewall: A literature Survey

Gayatri Deshmukh[1*], Rachana Kamble[2], Pratap Singh Solanki[3]

[1,2]B.E Students, Department of Electronics and Telecommunication, Sinhgad College of Engineering, Pune, INDIA
[3]Central Water and Power Research Station, Khadakwasla R.S, Pune, Maharashtra, INDIA

**Corresponding Author: gayatrideshmukh@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v9i11.3944 | Available online at: www.ijcseonline.org

Received: 02/Nov/2021, Accepted: 13/Nov/2021, Published: 30/Nov/2021

***Abstract*—** Firewalls play important role in any organization today. Firewall is a layer of security between organization Network and the Internet. A Firewall is programmed with security rules that prevent unregulated access to your internal Network. The rules might control employee access to websites and also prevent files leaving the company over Network. Any number of rules can be used to protect the data. In this literature survey, we studied the work carried out by various researchers about the protection of Network and data security.

***Keywords*—**Firewall, Data Security, Network Protectio,ICT Infrastrcuture,Web Filtering

I. INTRODUCTION

The Internet is one of the fastest growing technologies. Sixty percent of the population (4.80 billion people) around the world use the Internet. The growth in the use of Networked computers in business, especially for e-mail, has also fuelled this interest [1].

Over the past few decades, Firewall deployments have advanced and the functionality as well as the features have increased. Firewalls can now examine individual packets of traffic and test the packets to determine if they are safe.

Before Firewalls, Network security was performed by access control lists receding on routers. ACLs are rules that determine whether Network access should be granted or denied to specific IP address. ACL alone does not have capacity to keep threats out of the Network, hence Firewall was introduced.

The reminder of this paper is organised as follows, how firewall plays an important in data security and also highlights some different techniques and algorithms on how threats can be minimized using firewall (like next generation firewall, Improving Security in Company and IOT Network and etc.).

II. HISTORY OF FIREWALL

We are used to Firewalls in other disciplines, and, in fact, the term did not originate with the Internet. Firewalls are barriers to fire meant to slow down its spread until the fire department can put it out. The same is true for Firewalls in automobiles, segregating the passenger and engine compartments. Cheswick and Bellovin,(1994) in the definitive text on Internet . Firewalls said an Internet Firewall has the following properties: it is a single point between two or more Networks where all traffic must pass (choke point); traffic can be controlled by and may be authenticated through the device, and all traffic is logged. In a talk, Bellovin later stated, "Firewalls are barriers between 'us' and 'them' for arbitrary values of 'them.'" The first Network Firewalls appeared in the late 1980s and were routers used to separate a Network into smaller LANs as stated by Avolio, F. & Ranum, M (1996). In these scenarios and using Cheswick, W. & Bellovin, S. (1994) definition, above "us" might be well, "us." And "them" might be the English Department. Firewalls like this were put in place to limit problems from one LAN spilling over and affecting the whole Network. All this was done so that the English Department could add any applications to its own Network, and manage its Network in any way that the department wanted. The department was put behind a router so that problems due to errors in Network management, or noisy applications, did not spill over to trouble the whole campus Network. The first security Firewalls were used in the early 1990s. They were IP routers with filtering rules. Avolio, F. & Ranum, M (1996) opined that the first security policy was something like the following: allow anyone "in here" to access "out there." Also, keep anyone (or anything I don't like) "out there" from getting "in here." These Firewalls were effective, but limited. It was often very difficult to get the filtering rules right, for example. In some cases, it was difficult to identify all the parts of an application that needed to be restricted. In other cases, people would move around and the rules would have to be changed. The next security Firewalls were more elaborate and more tuneable. There were Firewalls built on so called bastion hosts. Probably the first commercial Firewall of this type, using filters and application gateways (proxies), was from Digital Equipment Corporation, and was based on the DEC

corporate Firewall. Brian Reid and the engineering team at DEC's Network Systems Lab in Palo Alto originally invented the DEC Firewall. The first commercial Firewall was configured for and delivered to the first customer, a large East Coast-based chemical company, on June 13, 1991 Avolio, F. and Ranum, M. (1996). During the next few months, Marcus Ranum at Digital invented security proxies and rewrote much of the rest of the Firewall code. The Firewall product was produced and dubbed DEC SEAL (for Secure External Access Link). The DEC SEAL was made up of an external system, called Gatekeeper, the only system the Internet could talk to, a filtering gateway, called Gate, and an internal Mailhub (see Figure 1). In this same time frame, Cheswick and Bellovin at Bell Labs were experimenting with circuit relay-based Firewalls. Raptor Eagle came out about six months after DEC SEAL was first delivered, followed by the ANS InterLock [2].

III. WHY FIREWALL

A Firewall can help protect your computer and data by managing your Network traffic. It does this by blocking unsolicited and unwanted incoming Network traffic. A Firewall validates access by assessing this incoming traffic for anything malicious like hackers and malware that could infect your computer.

You approve any link to your Network from someone without a Firewall. You wouldn't have any way to identify incoming threats. That could leave malicious users exposed to your computers. If you don't have a Firewall, which could allow anyone to gain control over your computer or Network. Your data could be deleted by cybercriminals. Or to commit identity theft or financial fraud, they may use it.

IV. TYPES OF FIREWALL

Packet filtering Firewall
Circuit-level gateway
Application- level gateway (proxy Firewall)
Stateful inspection Firewall
Next Gen Firewall

V. LITERATURE SURVEY

Sezer YILDIZ, Umut ALTINIŞIK [3]. In the article, methods used in LAN Network are performed. Port security, DHCP security, and ARP control methods have been tested to prevent local Network traffic from being disabled. It has been observed that these methods respond to the need and the method of port security does not respond to DHCP attacks on its own. It is concluded that the port security feature for DHCP starvation attack does not prevent the attack from being performed. Using the port security, the port where the attack occurred was closed so that no DHCP starvation attack could be made from the same port. Therefore, all the protection methods must be applied from Layer-2 attacks. It is seen that the differences in the communication status of two different Networks established for the MAC flood attack are since the MAC address information continues to be kept in the CAM table if there is data flow in the corresponding port. Because of the security vulnerabilities experienced in the local area Networks, the bandwidth of these Networks expires due to heavy traffic and this negatively affects the processor performance of the Network devices. Therefore, it has been determined that the nerve lines that provide the flow of local Network traffic are disabled. In future studies, Network applications need to be secured with an information security program as the applications used on the Network to bring too much load to the Network because of the lack of awareness of the end users and the design of the Network design is complex.

Seny Kamara, Sonia Fahmy, Eugene Schultz, Florian Kerschbaum, and Michael Frantzen[4]. Defined a method to describe Firewall vulnerabilities and relate them to Firewall operations in compact matrices. Researchers reviewed twenty known Firewall vulnerabilities and analyzed the constructed matrices. The matrices not only show vulnerability trends, but also aid in predicting the where and how of new unforeseen vulnerabilities. They are also useful– to both Firewall developers and testers– in making resource allocation decisions. Vulnerability postings on CVE and other sites will eventually appear, but the organization does not necessarily need to be entirely dependent on these postings (which invariably lag behind the discovery of each vulnerability and often also the development of exploitation tools) to maintain a consistent level of security on the Firewall. Knowing that IP/port filtering, legality checks, packet reassembly, and application-level vulnerabilities are most likely to occur, the organization could install an additional packet filter that weeds out the kinds of traffic most likely to exploit these vulnerabilities when the Firewall is installed, thereby reducing the effect of the discovery of any new vulnerabilities related to these processing phases. This approach is proactive rather than reactive– something that most information security practices ardently strive to achieve.

Shunhao Lin, Ding Zhang, Yuqing Fu, Shuxian Wang [5].The purpose of Ethernet Firewall is to segregate the internal and external Network and create a secure communication path. This paper aims at the problems such as High latency, IP address security and system dependency. To resolve the above mentioned problem, this paper proposes design of the Gigabit Ethernet Firewall based on FPGA (Field Pro-grammable Gate Array) runs on Gigabyte Ethernet with low latency and realizes five-tuple binding, static NAPT and packet refactoring. It also introduces the FPGA Program's Frame-work and illustrating an experiment for performance and functionality of the Ethernet Firewall. In Five tuple Binding Detection, the module checks whether the packet meets the ACL in the white-list. Protocol Detection only translates static IP address, to overcome this problem we use SIP (Session Initiation Protocol). FPGA uses FSM

(Finite State Machine) to check whether the IP address matches to the items in white-list. While the second IP address shouldn't be replaced as it is used for authentication. IP address in the application layer is replaced in Data Drainage and Process the Application Layer. Packet Refactoring us-es Frame Header Calculator and NAPT to calculate Frame length, checksum and frame is reassembled and FCS of the Ethernet data is recalculated based on CRC (Cyclic Redundancy Check). ARM management fulfills the white-list configuration and keeps a heartbeat to communicate with the internal Network. The Ethernet Firewall designed in this experiment using FPGA Achieves a throughput of 950Mbps and a delay of 61.266us.

Nastassja Gaudet, Ana E Goulart, Edmond Rogers, Abhijeet Sahu, Kate Davis [6]. Firewall are Network security devices which allow the creation of demilitarized zones (DMZ's) where information about utilities operations can be accessed by outside contract-tors. They monitor and inspect incoming and outgoing traffic. They provide a layer of defence between Networks. A set of rules called access control lists (ACL's), can be established to allow or deny specific packets between Networks. This experiment shows the use of Cisco Adaptive Security Appliances (ASA's). There are many tools to model computer Network and Firewall configuration that allow the user to simulate and test Network architecture that they create using Cisco Packet Tracer. This Firewall only allow certain traffic to pass between specific devices with all other applications. Distributed Network Protocol 3 (DNP3) is a protocol used to control a remote net-work from a central Network which is mainly used in utility Networks with SCADA systems. The next data flow between the substation and UCC is derived from Web-based protocols. UCC can be accessed from an outside node in global Internet DMZ. In Database protocol UCC uses Structured Query Language (SQL) to upload and retrieve data from PI server. To transfer various type of data in form of energy Network, UCC uses Inter-Control Center Protocol (ICCP). Use of discrete DMZ zones allow for various operations to be held at the same type simultaneously without the interference of other operation.

Victor Clincy, Hossain Shahriar [7]. Web applications are developed to serve HTML pages based on server side implementa-tion that can be done in various languages such as PHP and ASP. They normally have a backend database as well such as MySQL. Applications, however, contain bugs that may be exploited by attackers for profit and fun. Application developers have the burden of ensuring input data get validated or sanitized, and code is checked for vulnerabilities. Web Application Firewall (WAF) performs a deep packet inspection of Network traffic that occurs between the client and the server sides. By analyzing the data transferred between the client and the server, WAF can identify possible attacks even if the implementation may be missing such a detection WAF can have two types of security models based on the policy type: positive or negative. A positive security model only allows traffic to pass that matches with the policies. All other traffic is blocked. A negative security model allows all traffic to pass and attempts to block only the traffic represented by malicious rules. Generally, most Firewalls use either positive or negative rules, rarely both. Imperia's web application Firewall works in this manner, it requires a training period or to be manually configured . The downside of manually configuring a WAF is that the security professional responsible for the configuration must know all possible valid and invalid input and output to be processed by applications Nitin Naik and Paul Jenkins [8]. This paper demonstrates a simulation of ICMP flooding, where the created Firewall in-bound and outbound rules are insufficient to monitor ICMP flooding. It is a Fuzzy Reasoning based enhanced version of standard Firewall. It supports further analysis of Firewall logs by embedding a fuzzy rule base system with the Firewall. Windows Fuzzy-Firewall has two main components: Windows Firewall and a fuzzy reasoning system. The Analysis was only focused on two main parameters: ICMP Echo rate called ICMP-ER (average of pack-et/Second) and ICMP packet size called ICMP-PS (average packet size in bytes). Network parameters such as ICMP echo rate and ICMP packet size are passed to the fuzzy reason-ing system. It assists windows Firewall in deciding the ICMP Flooding risk level. The ICMP flooding attack was executed using the Network scanning tools NMAP, Advanced Port Scanner and Ping. Network traffic data was collected in the "pFirewall.log" file and also analyzed in Wireshark. Windows Fuzzy-Firewall generates ICMP flooding risk alerts, which is not possible by using standard Windows Firewall.

Ricardo M. Oliveira Sihyung Lee Hyong S. Kim [9].This paper proposes an application, Prometheus, which implements mechanisms for au-tomatic detection of Firewall configuration problems that are extremely difficult to resolve manually. Prometheus detects two types of misconfiguration inconsistencies and inefficiencies. Inconsistencies arise within a single Firewall when some rules totally or partially mask other rules. These intra-Firewall inconsistencies can be one of the three types: shad-owing Generalization, and correlation. The three types of intra-Firewall inconsistencies can also Occur among the rules in different Firewalls along a path. Cross-path inconsistencies occur when packets that are expected to travel a Network through one path are actually diverted through another path. Prometheus identifies two types of intra-Firewall inefficiencies: redundancies and verbosities. Prometheus identifies a possible route set by using the Depth-Limited Search (DLS) algorithm, a special case of the Depth-First Search where the depth of search is limited. DLS finds a route set, if one exists within a specified depth limit. The use of routing information and the depth limit improves the performance of the DLS algorithm, since it precludes the need for an exhaustive search over an entire Network graph. Another method of performance optimization is to take advantage of what we call Overlapping Path Segments (OPS). An OPS is a path segment where nodes are repeated between two paths. We

reuse the models of Firewalls on an OPS as well as their corresponding re-sults of misconfiguration detection. we analyze the Firewalls on the path in the order they appear along the path. Given a misconfiguration of a Firewall rule Rulei, we determine the rule(s) that caused this misconfiguration using two new sets. The solution to this problem is either to add necessary Firewalls on the violated path or to reroute the traffic through another path that implements the policy. When the rerouting option is chosen, Prome-theus can give information about a set of paths through which the traffic can be rerouted.

Qiumei Cheng∗, Chunming Wu∗, Haifeng Zhou∗, Yuhang Zhang∗, Rui Wang∗, Wei Ruan[10].This paper proposes an artificial intelligence-based software-defined Networks Firewall (AI-SDNF) for solving the above problems. Compared with existing SDN Firewalls, AI-SDNF is able to extract and analyze the payload of data packets based on machine learning technologies rather than simply match with flow tables according to several header fields (e.g., source and destination IP/MAC addresses). We integrate we integrate machine learning technology into SDN architecture, and present an intelligent SDN Firewall with analyzing the payload of a packet to detect malicious traffic. AI-SDNF is a novel architecture that al-lows to timely discard malicious traffic to secure enterprise Networks perimeter with an intelligent SDN Firewall, we combine SDN and artificial intelligence to provide an intelligent and efficient AI-SDNF. With the separation of the control logic and the underlying devices, malicious traffic can be blocked timely and flexibly before matching with flow tables in Open switch, instead of inquiring Open-Daylight controller via Packet-in message. The average training process lasts about 2.5s which may vary with dataset volumes. AI-SDNF achieves the highest detection accuracy of 96.79% with low latency.

Perumalraja Rengaraj, S.Senthil Kumar and Chung-Horng Lung [11].Firewall can be an effective means to Protect the SDN controller from Network security threats. The Firewall rules can be predefined by using either the IP address or the MAC ad-dress filtering. We propose a Firewall implementation for SDN using the MAC filtering. This also describes the proposed SDN Firewall using the MAC filtering technique. The SDN separates the control plane from the data plane by means of centralized controller that control every switch in the data plane. As the Network elements in a SDN Network do not have the control plane to perform certain Network functions, such as routing, firewalling, etc. As the controller is centralized in SDN, a distributed Firewall technique can reduce the workload of the controller as well as the Network. The MAC address of the Network elements is unique and static for wired / wireless Network. In our proposed Firewall technique design, the ACL to add and delete rules for SDN switches is managed by the Network administrator at the SDN controller. The Firewall application at the SDN controller first checks the packet using the deep packet inspection technique. The Firewall mechanism was tested by attaching a learning switch to the Floodlight controller. It uses a simple forwarding algorithm that up-dates the Open Flow Switch by registering the packets' port, MAC, and IP addresses as they entering into the Network. The security performance (packet handling) is pretty much similar to the IP filtering. The unknown MAC address, excess length packet and larger size are similar to the IP filtering rule. The delay performance of the MAC filtering Firewall out-performs the IP filtering Firewall.

Benfano Soewito[12].The aim of this paper is to analyze the effectiveness the Next Generation Firewall that implemented to secure IOT in smart house and company Network. In this paper, two Firewall will be used of which one uses traditional Firewall namely IBM ISS Proventia and other using the next generation Firewall. Therefore several tools are being used in conducting at-tack trials. An attack will be carried out on different zones namely trusted zone and DMZ zone. The server that has been prepared in both zones will be attacked from Internet. At-tacks are carried out from untrusted zones (Internet) that enters the Network. The attack will continue through the Firewall being tested. The Firewall will determine whether the at-tack packet is forwarded or blocked, if the attack packet is forwarded, it will continue to the DMZ zone. The data package will be identified by IPS Sourcefire and if data packet passes, then the data packet sent by the attacker will enter the sever farm. To test the security of two Firewalls DDoS attacks will be carried out with 2 types of attack, DDos UDP flooding and DDos TCP-SYN. The result of Phishing attack and responses of two Firewalls tested in the IB MISS Proventia Firewall test. The last test in this study was the trial of SOL injection attacks in both the Firewall using the SQLMap tool. After testing both Firewalls against DDoS attacks, SQL Injection and Phishing, it can be concluded that the Next Generation Firewall has significantly better performance for protecting smart house and company Network, it can increase security of data communication Networks against threats from the Internet .

Robert Winding, Timothy Wright, and Michael Chapple [13]. This paper proposes an application of data mining and machine learning to discovering Network traffic anomalies in Firewall logs. These system can be improperly configured, operate unexpected services, or fall victim to intrusion attempts. This paper uses data mining techniques to analyze Network traffic, based on Firewall audit logs, to determine if statistical analysis of the logs can be used to identify anomalies. Listed below are the techniques used to apply machine learning to the analysis of Firewall logs.

- •Acquire, prepare, and clean data.
- •Identify methods of aggregating and reducing the data.
- •Select data features.
- •Utilize machine learning techniques such as Clustering and Classification.
- •Analyze and verify results to draw conclusions.

A PERL script was used to extract the following data from the Firewall logs: date and time of connection attempt,

permit/deny, source IP, source port, destination IP, destination port, protocol (ex. TCP/UDP/ICMP), bytes transferred to server, and bytes transferred to client. Below is a sanitized sample of the data records. This raw data and/or its aggregations are used to determine features that, in turn, can detect anomalous patterns. With the log extraction and preparation the data acquisition step is complete. Using SQL, a search for various aggregate relationships was carried out. This proved to be well aligned with the goals of detecting anomalous traffic. The results of these experiments are promising but not entirely conclusive. While more analysis is needed to determine the accuracy and rele-vance of the classifications regarding the flagging of interesting IPs, it seems that there is promise to using this technique.

Michiaki Ito, Hitoshi Iyatomi [14].This paper introduces an efficient machine learning approach that uses Character-level convolutional neural Network (CLCNN) with very large global max-pooling for extracting the feature of HTTP request and identify it into normal or malicious request. Using HTTP DATASET which was produced by the Spanish Research National Council (CSIC). The raw dataset contains raw HTTP requests, URL encoding has already been done for all characters within the request. The architecture A performs convolution and max-pooling twice and is connected to one-dimensional output via the full connect layer. Using architecture A, we compare the discrimination ability when changing the chunk size cut out from the HTTP re-quest character string. Experiment B is aimed at verifying the effect of combining different convolution sizes, in which good results have been obtained in the past research, in a situa-tion where the other conditions are the same. Our system realize fast, accurate and low-cost WAF system by using deep learning approach with an accuracy of 97.5%.

Manoj Chakravati[15]. Since the intension this paper is to give ideas of Next-Gen Firewalls and also that we can contrast UTM Firewalls with Next-Gen Firewalls. Traditionally UTM'S were stateful Firewalls and afterward they developed into UTM Firewalls adding layers of insurance, for example, IPS, AV, web filtering, Anti-spam etc. Presently some UTM sellers have incorporated next generation usefulness with their items. They have now introduced the control of applications, application perceivability and the capacity to make rules based on clients and applications. Next-Gen Firewalls however have been architecture sans preparation to give a totally flushed and upgraded outline with control and perceivability of applications as the centre point. Application recognizable proof and filtering: This is the main normal for NGFWs. They can recognize and channel traffic based upon the particular applications, rather than simply opening ports for any traffic. This keeps noxious applications and movement from using non-standard ports to avoid the Firewall. The most vigorous NGFWs empower administrators to control and oversee both business and non-business-related applications to empower Network and client profitability, and they can filter documents of boundless size over any port and without security or execution corruption. Furthermore, NGFWs can apply all security and application control innovations to SSL encrypted traffic, ensuring this doesn't turn into another malware vector into the Network.

VI. RESULTS AND DISCUSSION

In this literature survey, we studied various Firewall and their functionality. We found that the Firewall is very important device for any Organization to protect the Data and ICT Devices. We learned that some researchers performed Port security, DHCP security, and ARP control methods to prevent local network traffic from being disabled. Some studied revealed about Ethernet firewall to segregate the internal and external network and create a secure communication path. In some experiment, it is observed that the creation of demilitarized zones (DMZ's) where information about utilities operations can be accessed by outside contractors and monitor and inspect incoming and outgoing traffic. We also found about Web Application Firewall (WAF) for deep packet inspection of network traffic that occurs between the client and the server sides. WAF analyses the data transferred between the client and the server and can identify possible attacks. Some experiments proposed firewall implementation for SDN using the MAC filtering and also describes the proposed SDN firewall using the MAC filtering technique. Next Generation Firewall also implemented to secure IOT in smart house and company network. Data Mining and machine learning to discovering network traffic anomalies in firewall logs also used.

VII. CONCLUSION AND FUTURE SCOPE

Firewall is an Integral part of any organization. The Firewall checks all incoming and outgoing data traffic. It protect the network from external threats. Firewall comes with many functions. It may be Hardware or Software based. Web filtering, Customized policy as per Organization need, DMZ, Report generation and Supervision of Quality Control etc. and many more are the major function of Firewall. All major required features are available in the Firewall. If some function pertains to Network Management may be add more in the Firewall.

ACKNOWLEDGMENT

I would like to thank Shri. Akhilesh Kumar Agrawal, Director CWPRS, Pune, for granting us permission for one month internship training. I would like to give my sincere thanks Mr.P.S.Solanki, Scientist-B for their support and valuable guidance that has led this work to its completion.

REFERENCES

[1] Okumoku-Evroro, Oniovosa, "Application of Firewall system to Internet security",International journal of information technology and business management,Vol.**15** No.**1**,pp.**64**,**2015.**

[2] Okumoku-Evroro, Oniovosa, "Application of Firewall system to Internet security",International journal of information technology and business management,Vol.**15** No.**1**,pp.**64**,**2015.**

[3] Sezer YILDIZ , Umut ALTINIŞIK, " Detecting and preventin cyber attacks on local area Networks: A working example", International journal of computer science and engineering, Vol.**6**,Issue**11**,**2018.**

[4] Seny Kamara, Sonia Fahmy, Eugene Schultz, Florian Kerschbaum, and Michael Frantzen, "Analysis of Vulnerabilities in Internet Firewalls"Vol.**22**,No.**3**,pp.**1-19,2003.**

[5] Lin, Ding Zhang, Yuqing Fu, Shuxian Wang, "A Design of the Ethernet Firewall Based on FPGA Shunhao",International Congress on Image and Signal Processing,BioMedical Engineering and Informatics, Shanghai, **China**,pp.**1-5,** ISBN: **978-1-5386-1937-7, 2017.**

[6] Nastassja Gaudet, Ana E Goulart, Edmond Rogers, Abhijeet Sahu, Kate Davis, "Firewall Configuration and Path Analysis for Smart Grid Networks". International Workshop Technical Committee on Communications Quality and Reliability, Stevenson, WA, **USA**, pp.**1-6,** ISBN:**978-1-7281-6627-8, 2020**.

[7] Victor Clincy, Hossain Shahriar "Web Application Firewall: Network Security Models and Configuration",42nd IEEE International Conference on Computer Software & Applications, Tokyo, **Japan**, pp.**1-2,** ISBN:**978-1-5386-2667-2**, **2018**.

[8] Nitin Naik and Paul Jen-kins, "Enhancing Windows Firewall Security Using Fuzzy Reasoning" by 14th Intl Conf on Dependable, Autonomic and Secure Computing, Auckland, **New Zealand** pp.**1-7**, ISBN:**978-1-5090-4065-0**, **2016**.

[9] Ricardo M. Oliveira Sihyung Lee Hyong S. Kim, "Automatic detection of Firewall misconfigurations using Firewall and Network routing policies". pp.**1-6**, **2009**.

[10] Qiumei Cheng, Chunming Wu, Haifeng Zhou, Yuhang Zhang, Rui Wang, Wei Ruan, "Guarding the Perimeter of Cloud-based Enterprise Networks: An Intelligent SDN Firewall". 20th International Conference on High Performance Computing and Communications, Exeter,**UK,** ISBN:**978-1-5386-6614-2, 2018.**

[11] Perumalraja Rengaraj, S.Senthil Kumar and Chung-Horng Lung "Investigation of Security and QoS on SDN Firewall Using MAC Filtering". International Conference on Computer Communication and Informatics, Coimbatore, **INDIA**, ISBN:**978-1-4673-8855-9**. **2017**

[12] Benfano Soewito "Next Generation Firewall for Improving Security in Company and IOT Network". International Seminar on Intelligent Technology and Its Applications, pp.**1-5** ISBN:**978-1-7281-3749-0, 2020**.

[13] Robert Winding, Timothy Wright and Micheal Chappel. " System Anomaly Detection: Mining Firewall Logs",ISBN**:1-4244-0422-3CD:1-4244-0423-1**, **2006.**

[14] Hitoshi Iyatomi, Michiaki Ito, "Web Application Firewall using Character-level Convolutional Neural Network".14th International Colloquium on Signal Processing & its Applications, Penang, Malaysia.pp.**1-4, 2018.**

[15] Manoj Chakravati, "Next Generation Firewall", International Journal of Computer Science and Information Technologies, Vol.**7(3)**, pp.**1-4**, **2016.**

AUTHORS PROFILE

Miss Gayatri Deshmukh is peresently pursuing Bachelor of Engineering(BE) degree from Sinhgad College of Engineering(SCOE), Pune university. She had gone under the internship training for the period of one month under the guidance of Pratap Singh Solanki, Scientist-B, Central Water and Power Research Station, khadakwasla, Pune. This literature survey has been carried out as part of the training

Miss Rachana Kamble is peresently pursuing Bachelor of Engineering(BE) degree from Sinhgad College of Engineering(SCOE), Pune university. She had gone under the internship training for the period of one month under the guidance of Pratap Singh Solanki, Scientist-B, Central Water and Power Research Station, khadakwasla, Pune. This literature survey has been carried out as part of the training

Mr. Pratap Singh Solanki did his Bachelor of Science & Master of Computer Application(MCA) degree from DAVV University Indore(MP). Presently, he is working as Scientist-B in Water and Power Research Station,(Govt. of India,(MoWR,RD&GR) Water and Power Research Station, Khadakwasla, Pune since october 2002, and having more than 20 years of industrial and research experience in the field of software development, Database management, Computer Network, Cyber security, e-Governance activists, System administration. Web development, Hydrology etc. His area of interests of research is Database Management, Data Mining, Cyber security and Intergrated Water Resource Management.

