Matrik: Jurnal Manajemen, Teknik Informatika, dan Rekayasa Komputer
Vol. 20, No. 2, Mei 2021, pp. 427~434
ISSN: 2476-9843, accredited by Kemenristekdikti, Decree No: 200/M/KPT/2020
DOI: 10.30812/matrik.v20i2.410

Developing Application in Anticipating DDoS Attacks on Server Computer Machines

Anthony Anggrawan[1], Raisul Azhar[2], Bambang Krismono[3], Mayadi[4]

Universitas Bumigora, Indonesia

Article Info

Article history:

Received, 31 Maret 2021
Revised, 15 Mei 2021
Accepted, 28 Mei 2021

Keywords:

DDos
Firewall
Computer Server
Security threat
Network applications
Web hosting

ABSTRACT

The use of server computer machines in companies is primarily a web hosting server that is very easy to experience threats, especially external security threats such as attempts to infiltrate, hacking, viruses, and other malicious attacks. Having a secure server is indispensable for working online and especially if involved in business-related network transactions. The Server's realization to be safe from threats is to protect the server machine's security on the hardware and software side and pay attention to network security that goes to the server machine. Generally, firewall applications on router devices have configuration limitations in securing the network, namely non-integrated applications. In other words, it is necessary to manage the perfect firewall configuration to anticipate Distributed Daniel attacks of Service (DDoS) attacks. Therefore, this study aims to integrate existing firewall applications for router devices into an integrated program to secure the network. The methodology used is the Network Development Life Cycle (NDLC). The research results on this developed application program can overcome DDoS attacks without setting up a firewall on the router device and can automatically monitor DDoS attack activities from outside the Server. Securing servers from DDoS attacks without setting up a firewall on the router device and automating the monitoring of DDoS attack activity from outside the Server are the novelties of this study that have not been available in previous studies.

Corresponding Author:

Anthony Anggrawan,
Department of Engineering And Design,
Universitas Bumigora,
Email: anthony.anggrawan@universitasbumigora.ac.id

1. INTRODUCTION

The Internet of Things (IoT) has made millions of computer devices connected via the internet network, thereby increasing security threats, including DDoS attacks [1][2], and is the most noticed and most important attack on the Internet network today [3]. One such attack is the Simple Network Management Protocol (SNMP), a UDP protocol commonly used for network management so that a request sent to an SNMP server returns a larger response than an incoming request [4]. However, DDOS is one of the most prominent attacking behaviors over the network, which interrupts and blocks legitimate users from using network resources [5][6]. This research is a solution in overcoming server security problems experienced by business companies engaged in web hosting and Internet Service Providers (ISPs). In the study, the network connection system used is a wireless network using Grid antenna devices, Omni antennas, two outdoor access points, a server machine that functions as a proxy server. This study uses Mikrotik RouterOS as a router on its network system and all forms of network security policies. Computer servers running web hosting operate with the Linux Operating System with Ubuntu Server 11.04 distributions with default application packages such as Squid packages for Proxy Servers, BIND as DNS, and SAMBA function as file sharing. Research observations are on corporate customers, namely customers who rent web hosting services and internet services such as internet cafes and educational institutions with an average bandwidth rental of 512 Kbps to 2 Mbps.

Based on the results of observations directly to customers, customers often experience disruptions to their networks, such as sudden disconnection of internet services; remote access to remote access with SSH (Secure Shell) that does not run usually; and activities for the file or file sharing and access web hosting have experienced a sudden downturn caused by damage to the computer network that goes to the center of the company's web hosting server machine. Besides, the server computer and Mikrotik RouterOS often hang and crash, the cause of which is unknown to the customer. Based on observations made on the disturbances that usually occur on the network by looking at the server cache, back errors, server system configuration, and policies applied to network routers, the primary cause attacks from outside the network segment indicated by using DDoS. DDoS attacks that occur are attacks on server computers in the internet network by consuming the server computer's resources not to carry out its functions properly. Attacks on server computers so that the server computer cannot perform its functions indirectly preventing other users from gaining access to services from the attacked computer. Based on the observations made in this study provides clues that there are several types of attacks on the server computer, such as Buffer Overflow attacks by sending data that exceeds system capacity, for example, sending a very large ICMP packet; SYN attack sends TCP SYN data using a fake address; Teardrop attacks, sending IP packets with confusing offset values; and Smurf attack, sending a large volume ICMP packet with another host address. These all attack disturbances occur in the company where this research has an average frequency of 3 to 6 times in 1 month. It results in customers at these companies often being dissatisfied with the web hosting and internet services they rent.

DDOS is one of the most prominent attacking behaviors over the network, which interrupts and blocks legitimate users from using network resources [2]. DDoS attacks that occur are attacks on server computers in the internet network by consuming the server computer's resources not to carry out its functions properly. Server computers cannot handle DDoS attacks, which rely solely on configuring or managing the router devices t; this is because the router devices do not explicitly receive DDoS attacks. Therefore, this research aims to integrate the router firewall application to secure the network. To realize this research's objectives, the researchers built an application capable of handling these attacks by managing a firewall on the network to anticipate Distributed Denial of Service DDoS attacks. A firewall management application will integrate with the Mikrotik router device connected to the server computer. So that with the Application, network administrators who manage company servers can quickly minimize security disturbances on networks and servers. Besides, network administrators can create policies such as opening or closing specific ports, limiting the number of connectivity to servers, making policies accessed by specific IPs, and monitoring DDoS attack activity.

Two types or forms of attacks occur on server machines, namely DDos and Thick Flood Network (TFN). The most common and simple form of attack on the system is Denial of Service (DoS). This type of attack will not try to get sensitive information. The purpose of this attack only prevents users who have access rights from being able to access usually [7]. DoS is relatively simple to do. In principle, requires only a minimum of technical skills; what's more, every device has operational limitations, and every computer system, web server, or network also has limitations [8]. The TFN known as the Tribal Flood Network is an application used to carry out DoS attacks (peer-to-peer attacks). While TFN2K is a tool used to do DoS or attacks using multiple computers. Both TFN and TFN2K can carry out some attacks, both UDP, ICMP, and TCP SYN flood attacks. The workings of the TFN2K are: The master will instruct his agents (zombies) to attack the designated target list; and Agents (zombies) respond by flooding the target with a series of packets sent [9]. Stacheldraht is a type of DDoS attack that incorporates the Trinoo DDoS features. Stacheldrahta can deliver on attacks including UDP, ICMP, TCP SYN, and Smurf flood attacks. [7]. TCP SYN Flood Attacks is a form of attack by connecting to the Server [10] when activity between the client and the server takes place on the network using the TCP protocol. Packages are sent to the Server with a 1-bit flag called the SYN flag [11]. SYN is a server synchronization and then allocates resources to the client and sends SYN (synchronizes) and ACK (acknowledges). The client machine must then work with an ACK state which signals the process of the handshake activity [12].

Smurf IP attack is a popular type of DoS attack. ICMP packets are distributed to internet protocol addresses, In carrying out this type of attack is to use some software such as a Trojan horse virus. During the Smurf attack, there are three parties involved, namely the attacker, the intermediary (who can also become a victim), and the victim. The attacker first sends an

ICMP to ask message to the intermediary. Because this is sent to the broadcast IP address, the ICMP echo request packet is also sent to all intermediate machines. When all the intermediary devices begin to reply to echo requests, the reply will flood the victim. Smurf attacks are examples of attacks using several other parties [12]. Ping of Death (PoD) is a common attack that that happens a lot. This attack is launched with the ping utility on the operating system. Ping usually acts to check for the host's presence or the IP address of a website. Data transmission is sent at 32 bytes, but this application program can send data up to 65kb. Currently, these attacks are no longer effective because most systems have equipped themselves with previous weaknesses. Moreover, with increasingly advanced technology and wider available bandwidth, this type of attack no longer affects the system [7]. Based on the description above, a single attacker or hacker who uses DoS techniques can almost certainly be captured by the Administrator or network security manager. [7].

A firewall is a device that filters traffic between internal networks and external networks. Usually, the Firewall runs on special devices [10]. Besides, the Firewall is also a barrier between internal networks and external networks. Some devices that can be used as firewalls are servers, routers, and software that runs on computer machines [7]. A firewall is a unique device or software that filters and acts as a barrier between internal and external networks. Whatever type of Firewall is used a firewall is a tool to block certain traffic from a computer network [13]. Firewalls are an important part of security strategies. Firewalls can be a good way to stop attacks, denial of service, or prevent hackers from scanning details from internal networks. However, firewalls have various capabilities, including Packet Filtering Gateway and Stateful Inspection Firewall [10]. Packet Filtering Gateway or Screening is the most uncomplicated Firewall, and in some situations, the most effective type of Firewall. Packet Filtering Gateway controls packet access based on packet address (source or destination) or transportation of certain types of protocols (such as HTTP web traffic). Allows HTTP and Bloc Telnet Protocols, as shown in figure 1 below: [14]

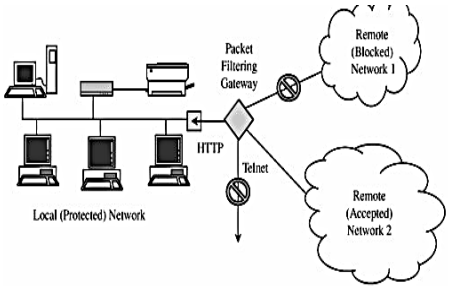

Figure 1. Packet Filter Blocking Address and Protocols

Attackers use one approach to break attacks on multiple packets by forcing several packets to have very short lengths. So that the Firewall cannot detect the signature of the second or more packages. So Stateful Inspection Firewall will track package sequences and conditions from one package to another to thwart attacks [12]. Personal Firewall is an application program that works on workstations to block unwanted traffic on the network. A personal Firewall can compensate for the shortcomings of ordinary firewalls. Implementing this personal Firewall is like Norton Personal Firewall from Symantec, McAfee Personal Firewall, and Zone Alarm from Zona Labs [15]. Advance Policy Firewall is an iptables based firewall that is designed for current internet needs and is run on Linux. There are three parts of filtering carried out by APF, including [13]: First, Static Rule Base Policies are the most traditional Firewall rule a fixed firewall rule responsible for handling traffic in normal conditions. An example of a Static Rule Base Policies is an allow/deny setting for an address to access the Server by allowing active ports through the conf.apf file. which is the rules don't change much or don't change when the Firewall is run. Second, Connection Based Stateful Policies mean differentiating data packages for various types of connections. Only packages that are connected are permitted by the Firewall, while other packages will be rejected. An example is FTP data transfer, with connection-based stateful policies filtering, the Firewall can know that the address has connected to port 21. Then connect the address to the data transfer portion and dynamically change the Firewall to allow that traffic [11]. This paper is structured as follows. After the Introduction section, Part two provides a research methodology. Section three presents the results and discussion. Finally, the fourth section contains the conclusions.

2. METHODOLOGY

This study's first thing was to produce a firewall management application program to anticipate DDoS attacks. Built-in applications are also used to manage network security from DDoS attacks on companies. The methodology used in this study is the NDLC. The methodology used in this study is the Network Development Life Cycle (NDLC). According to Goldan and Rawles (2001), NDLC is a model behind the key to designing computer networks. NDLC is a model that defines the process cycle of designing or developing a computer network system. NDLC consists of 6 stages, namely analysis, design, simulation prototyping, implementation, monitoring, and management [16].

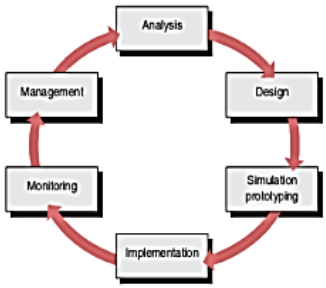

Figure 2. Methodology NDLC

This study's research method only adopted part of the NDLC methodology stages, namely planning, analysis, design, and implementation. Data collection is carried out with two methods, namely observation and documentation.

2.1. Observation

2.1.1. Security Policy

From the observations made in this study and referring to the documentation results, an observation analysis was obtained based on the policies applied to the company's network, where when this research was carried out applying a policy of security system policy or the Application of a firewall.

2.1.2. Static Rule Base Policies

Applied Static Rule Base Policies are the most traditional security or Firewall methods, a fixed firewall rule tasked with handling traffic in normal conditions. An example of a Static Rule Base Policies applied is an allow/deny access setting for an address that will access the Server by allowing active ports through the conf.apf file, where the rules don't change much or change when the Firewall is run.

2.1.3. Sanity Based Policies

Sanity Based Policies are defined, namely firewalls to recognize various traffic patterns to find out the attacker's method or study traffic to fit the internet standards. An example that is done is: if there is an attack by disguising the source of the IP address when sending data to the Server, the APF can easily reject the traffic or optionally record it to the lock file then leave the traffic.

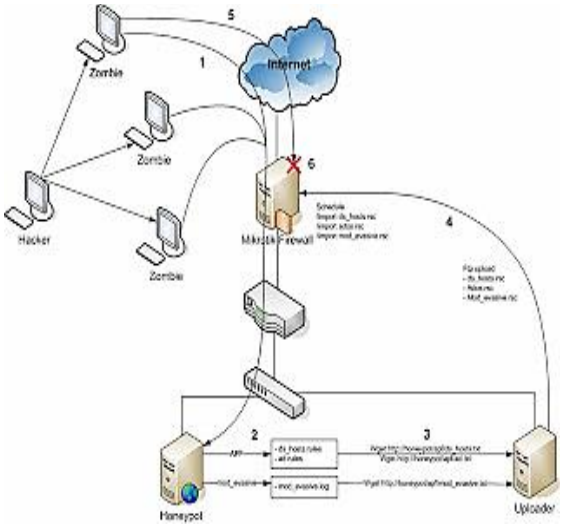

Figure 3. DDos Defense Mechanism

2.1.4. Application of Deflate DDos

Applied DDoS Deflate is a shell bash script that will help block attacks. DDoS Deflate works by monitoring the IP Address that sends packets and establishes a connection TCP (smtp, http) or ICMP ping. When this script sees too many connections that exceed the specified threshold, the script will order the APF firewall to block the corresponding IP Address and then unblocking if needed.

2.1.5. Network Conditions

Used proxy server engine with Ubuntu Server 11.04 Operating System, equipped with Microtech RouterOS, Omni Antenna as Bridge as a customer Hotspot service and uses Switch devices for local internet services and Grid Antenna for Point-to-point services on the network. Some observations of network conditions are as follows: Users or clients who rent bandwidth either through Point-to-point, Hotspot, or internet cafe rely on one Server located in the company.

1. Network security Network administrators still use firewalls that are on RouterOS and the configuration contents function to do limited virus removal.
2. The disadvantage of any DoS attack is that a flood of packets must be sustainable from the attacker's point of view. When a hacker carries out a distributed attack, and once the Administrator or owner realizes that the machine is infected, steps are taken to remove the virus and ensure the attack doesn't continue. When a hacker tries to carry out an attack, the hacker should realize that the packet sent can be traced to the source. In other words, hackers who carry out a DoS attack can be said to be arrested by the authorities for their crimes.
3. There is no sure way to guarantee the prevention of all DoS attacks. However, some steps can be taken to minimize the danger. Some steps can be taken to prevent DoS attacks. One of the first things to consider is how the attack is carried out. Via ICMP packets, its implementation can be carried out over the internet to send error messages, as well as by ping and traceroute utilities. If a person has a firewall, then it is enough to configure ICMP packets from outside networks. DoS / DDoS attacks can be carried out through various protocols, so someone can configure the firewall to shut down incoming traffic. This step is just the safest frontal method [7].

3. RESULTS AND ANALYSIS

The study in this section was done by collecting data on the company's network design under study, namely the design of the RouterOS Mikrotik network security configuration. Data obtained from this documentation is used to make Firewall Management Applications anticipate DDoS attacks. Based on the company's network configuration documentation, it was found that network security uses firewalls in RouterOS with configuration designs as shown in Figure 4.

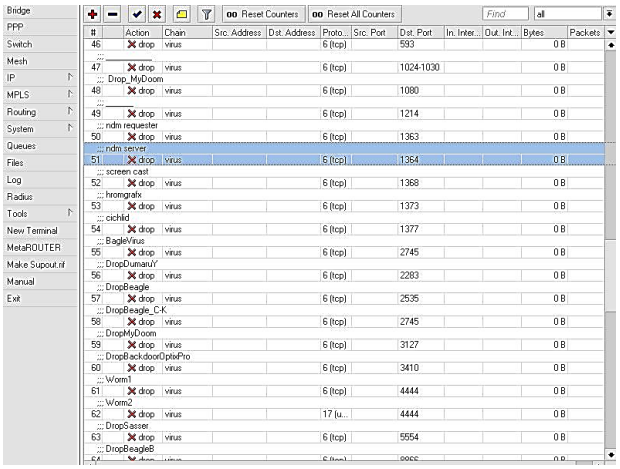

Figure 4. Firewall for Drop Viruses

The company where the research was conducted leased bandwidth at PT Telkom. Then the company rents back the bandwidth to schools and Internet cafes. The company makes PPPoE Server on the Mikrotik router then shares it through the Grid antenna so that schools and Internet Cafes can access the internet (see Figure 5).

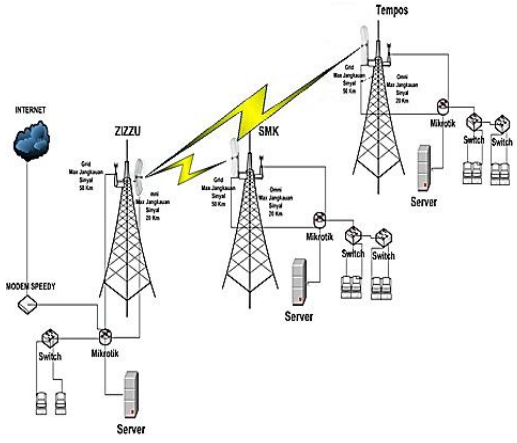

Figure 5. Network Topology

Provide Firewall Management Application to Anticipate DDoS attacks consisting of several main menus: home, apf, DDoS, rules, logs, system, and Logout menus. The following is the look at the Firewall Management Application to Anticipate DDoS Attacks:

After the Admin has successfully entered the login process, the Admin will be directed to the Application's home menu, where there is information about the Server and other package information on the home menu (see Figure 6).

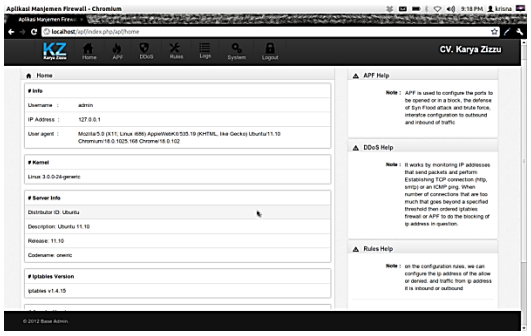

Figure 6. Home menu in the application program

The Admin uses the APF menu to set general and advance configurations. The General Admin can configure such as APF mode, blocking ports, defense, and interface settings used as data entry and exit. Advance the Admin can configure the ports that will be opened or allowed (see Figure 7).

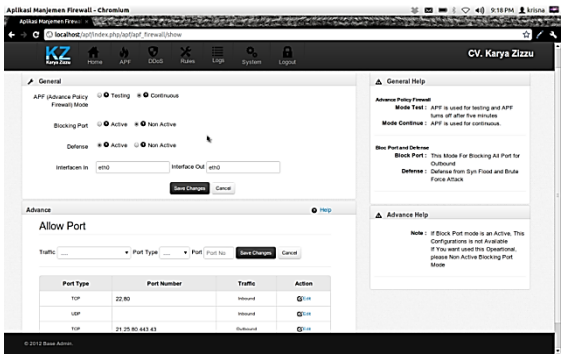

Figure 7. APF menu in the application program

Add Allow the Port form located in the APF page in the Admin's advanced configuration to add ports to be opened (see Figure 8).

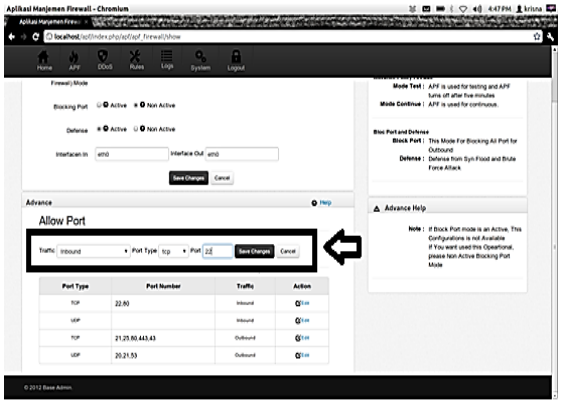

Figure 8. Menu Add Allow Port

The Admin uses the DDoS menu to set the anti-DDoS configuration. Admin can configure such as time-frequency, blocking the port, defense, and interface settings that are used as data entry and exit lines. Advance Admin can configure the ports to be opened or allowed (see Figure 9).

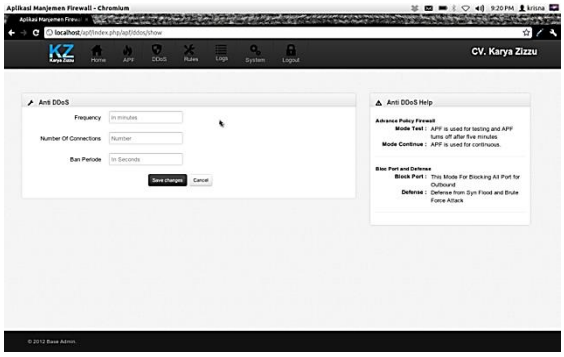

Figure 9. DDos Menu

Display the add rules form found in the Rules menu. used by the Admin to set the IP and Port that will be canceled or allow. The appearance of the additional rules form is as shown in Figure 10.

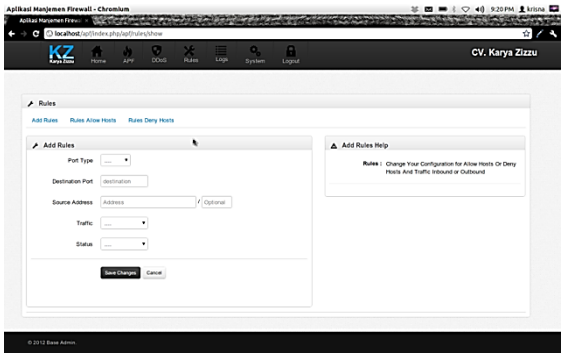

Figure 10. Add Rules Menu

The Deny Hosts Edit Rules form found on the Rules Deny the Admin uses hosts page to change the IP, protocol, Port, and traffic that will be denied access to the Server. The menu of the Edit Rules Deny Hosts is as shown in Figure 11.

Figure 11. Edit Rules Deny Hosts Menu

Display the log menu is a display that will display the IP blacklisted. The figure of the menu logs is as shown in Figure 12.

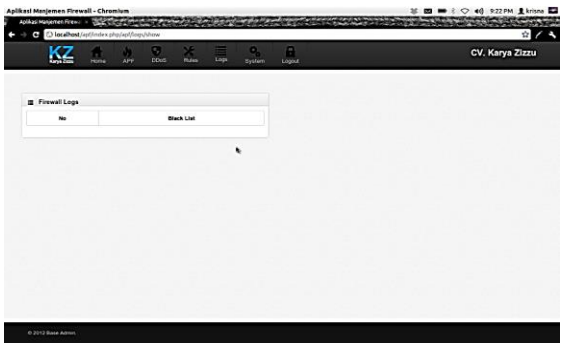

Figure 12. Menu Logs in the application program

The results of testing an application program built using the NDLC method are as follows: the Firewall Management Application can be used to open or close access to specific ports of data packets passing through the network so that they can find out what activities are intruders entering the network to the company's server machines, and can limit and monitor the

number of connections established by client computers so that they can easily observe attacks with DDoS attack techniques, Firewall Management Applications can also allow or deny specific IP addresses through port channels desired by Administrators, as a way to secure network connections connected to them. The Server, and from this application can generate a script address list that can be integrated into a Mikrotik router and implemented as a firewall can do a Drop-Address list on the network experiencing problems

4. CONCLUSION

The conclusions from research with application development to anticipate DDoS attacks on server machines and make observations of the running system are as follows: Management Application Firewall can be used to open or close access to certain ports of data packets that pass through the network to find out the activities of intruders that enter the network leading to the company's server engine; Application Management Firewall can limit and monitor the number of connections formed by Client computers to easily observe attacks with DDoS attack techniques; Firewall Management Applications can allow or reject specific IP Addresses via the port-channel desired by the Administrator to secure network connections connected to the Server, and the Application developed produces a script list of addresses in the Mikrotik router and can do a Drop-address list on an experiencing network. Securing servers from DDoS attacks without setting up a firewall on the router device and automating the monitoring of DDoS attack activity from outside the Server are the novelties of this study that have not been available in previous studies. The implications of the results of this study are the configuration of several firewall applications that exist for router devices no longer needs to be done separately, but the configuration is done through an integrated application program to secure the network efficiently. For further research, it is necessary to integrate the security of network systems and computer servers with mobile control systems.

REFERENCES

[1] A. Roohi, M. Adeel, and M. A. Shah, "DDoS in IoT: A roadmap towards security countermeasures," *ICAC 2019 - 2019 25th IEEE Int. Conf. Autom. Comput.*, no. September, pp. 1–6, 2019.

[2] A. Lohachab and B. Karambir, "Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks," *J. Commun. Inf. Networks*, vol. 3, no. 3, pp. 57–78, 2018.

[3] S. Chakraborty, P. Kumar, and B. Sinha, "A study on ddos attacks, danger and its prevention," *Int. J. Res. Anal. Rev.*, vol. 6, no. 2, pp. 10–15, 2019.

[4] A. Colella and C. M. Colombini, "Amplification DDoS attacks: Emerging threats and defense strategies," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8708, pp. 298–310, 2014.

[5] K. Zeb, O. Baig, and M. K. Asif, "DDoS attacks and countermeasures in cyberspace," *2015 2nd World Symp. Web Appl. Networking, WSWAN 2015*, 2015.

[6] J. Kaur Chahal, A. Bhandari, and S. Behal, "Distributed Denial of Service Attacks: A Threat or Challenge," *New Rev. Inf. Netw.*, vol. 24, no. 1, pp. 31–103, 2019.

[7] G. Booch, "Object Oriented Analysis & Design with Application," *Br. J. Hosp. Med. (Lond).*, vol. 75, no. 4, pp. 237-Unknown, 2006.

[8] M. Siekkinen, G. Urvoy-Keller, E. W. Biersack, and D. Collange, "A root cause analysis toolkit for TCP," *Comput. Networks*, vol. 52, no. 9, pp. 1846–1858, 2008.

[9] B. R. Mcree, "Security analysis with Wireshark," *ISSA J.*, no. November, pp. 39–43, 2006.

[10] J. Biskup, *Security in Computing Systems Original source of these lecture notes Security in Computing Systems Security in Computing Systems*, Fourth. Verlag Berlin Heidelberg: Springer, 2011.

[11] A. Rodriguez, J. Gatrell, J. Karas, and R. Peschke, *TCP / IP Tutorial and Overview*, Seventh Ed. NC: IBM Corporation, 2001.

[12] A. Uprit, "Network Security Using Linux/Unix Firewall," *Int. J. Res. Comput. Sci.*, vol. 2, no. 4, pp. 77–79, 2011.

[13] S. Suehring and R. Ziegler, *Linux Firewalls*, Third. Indiana: Novell Press, 2006.

[14] J. M. Kizza, *Guide to Computer Network Security - Fourth Edition*. 2017.

[15] L. Wang, Z. Wang, C. Yang, L. Zhang, and Q. Ye, "Linux kernels as complex networks: A novel method to study evolution," *IEEE Int. Conf. Softw. Maintenance, ICSM*, pp. 41–50, 2009.

[16] J. E. Goldman and P. Rawles, *Applied Data Communications: A Business-Oriented Approach*, 4/E. John Wiley and Sons, Inc., 2011.