JURNAL TEKNOLOGI REKAYASA INFORMASI DAN KOMPUTER
E-ISSN: 2797-1724, DOI: 10.30811/jtrik.v7i2.4297
Vol. 7 No. 2 2025 pp. 07-13

Firewall Implementation Using Port Knocking Method for Network and Server Security

Muhammad Fatahillah[1], Aswandi[1*], Anwar[1]

[1]Jurusan Teknologi Informasi dan Komputer, Politeknik Negeri Lhokseumawe, Indonesia

*Corresponding Author: aswandi@pnl.ac.id

Article info: Received 07/02,/2025, Revised 08/02/2025, Accepted 07/03/2025

Abstract

Along with the development of information technology, the use of computer networks is increasingly widespread and increasingly important for many organizations, many attacks are carried out by irresponsible people on open ports, thus making people who do not have access or interest be able to easily easy to control those ports. On the laboratory router 110 cloud computing, efforts are made to protect the network using the port knocking method to increase network security and prevent access from unauthorized parties, the problem is that ports often open or access without security which can make it easier for unauthorized users to enter the router. This study examines the port access service, testing is carried out on all ports and the results obtained are clients who do not knock ports, so access to the router is denied, otherwise clients who have knocked port access are given, the percentage value obtained from implementing the port knocking method firewall 100% successful in preventing unauthorized access. Testing against various attacks such as port scanning, DDoS, Brute force, and packet sniffing, the results of the experiments for each attack show that the firewall using the port knocking method succeeded in preventing all of these attacks with an attack failure percentage value of 100%, of all attacks tested by the firewall detects all attacker's Ip addresses and denies all access, along with entering these Ip addresses into the intruder's address list and the firewall successfully protects the network from attacks.

Keywords: Network Security, Port Knocking, Firewall, Port Scanning, DdoS, Packet Sniffing, Brute Force

1. Introduction

As with the development of information technology, the use of computer networks is increasingly widespread and increasingly important for many organizations and companies. In the use of networks computers can also pose a high security risk [1]. With so many security threats such as DDoS attacks, Hacking, Malware and so on, from some of these threats can result in significant losses for the organization or company. To prevent undesirable things, administrators' networks will install firewalls and perform several configurations for limit who can access the server. These configurations can include setting firewall rules, restricting access to certain ports, use of authentication, and other security measures that can minimize the risk of network attacks and maintain server security. One of the main focuses in computer network services is maintaining secure access on ports, a common problem is open ports or insecure access which can make it easier for unauthorized users to enter the server [2]. Therefore, the method is needed Port knocking, Port knocking is a security system that can perform the function of blocking unwanted access on the network. With using this technique, access to the port will be blocked by default and will only be opened when the user performs a series of connections or rules that match a certain pattern. This can prevent unwanted access and improve overall network security [3].

This research is related to previous research with the title "Analysis and Implementation of Firewall Using Port Knocking Method Based on Mikrotik RouterOS". Research This aims to secure the Mikrotik server network from this implementation provides a solution to the risk of someone who does not have authorization to enter the Mikrotik network server from irresponsible people responsible for being able to access the Mikrotik network server and also can provide ease of application access for administrators. The difference in this research is not using packet sniffing to determine the level of network security, whereas the research to be carried out uses packet sniffing for
network security traffic. The similarity of this research with the research that will be carried out lies in the use of

the same method, namely port knocking for security network [4].

This research is related to previous research with the title "Implementation of Network Security System On Mikrotik RB-951 Using Port Knocking Method". This research aims to secure the Mikrotik server network from this implementation provides a solution to the risk of someone who does not have authorization to enter the Mikrotik network server from irresponsible people responsible for being able to access the Mikrotik network server and also aims to find out that the Service port that has port knocking installed will be closed if performing a port scanning process. The difference in this research is not using packet sniffing to determine the level of network security, whereas the research to be carried out uses packet sniffing for network security traffic. The similarity of this research with the research that will be carried out lies in the use of the same method, namely port knocking for security network [5].

This research is related to previous research with the title "Effectiveness of using port methods blocking and port knocking". This research aims to secure Mikrotik server network from this implementation provides a solution to the risk someone who does not have authorization to enter the network server Mikrotik from irresponsible people who can access Mikrotik network server. The difference between this research and the research that will be carried out lies in the use of python software to launch attacks, whereas in the research to be carried out using linux and several types of attacks will be carried out. The similarity of this research with the research to be carried out lies in the use of the same method, namely port knocking for security network [6].

This research is related to previous research with the title "network security analysis using sniffing method and network security implementation on Mikrotik Router OS v6.48.3 using port knocking". This research aims to test security networks as eavesdropping with the sniffing method and using Wireshark and implement the port knocking method for network security on Mikrotik router os v6.48.3. The difference between this research and the research to be carried out lies in the case study, which previous research was located at Ubudiyah Indonesia University, while in the research to be carried out the case study is located at Politeknik Negeri Lhokseumawe. Similarity, this research with the research to be carried out lies in the use port knocking method [7].

2. Methods

This research uses the port knocking method to block unwanted network access. With this technique, port access will be blocked by default and only opened when a user performs a series of connections or rules that match a specific pattern. This can prevent unwanted access and improve overall network security.

2.1. Hardware Design

The design of the network topology where the port knocking method is implemented to prevent unauthorized access can be seen in Figure 1.

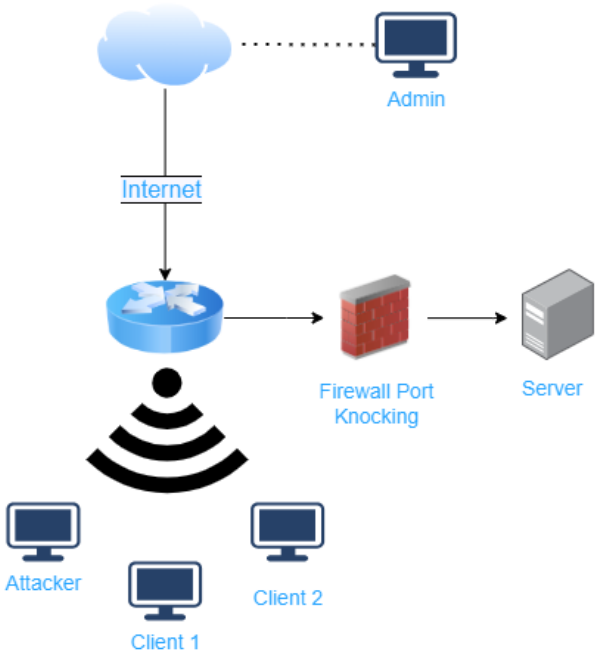

Figure 1. Network Topology

Based on the network topology in Figure 1, the local environment includes one Mikrotik routerboard configured with a port knocking firewall, an Ubuntu server, two Windows 10 clients, and one attacker attempting to access

the router.

On the public side, an administrator can access the server remotely. The router is configured to allow the local server to be accessed remotely via the public network. To enable communication between devices, configurations were implemented. In this research, port forwarding was configured on the router to allow remote access and control of the local server from the public network. Following this, the firewall was designed and configured using the port knocking method.

2.2. Firewall

A firewall is a model that can be effectively implemented on both hardware and software. Firewalls are used to limit or control who has access to a private network [8]. A firewall can be seen in Figure 2.

Figure 2. Firewall

2.3. Mikrotik

Mikrotik is an operating system and software that can turn a computer into a network router. Mikrotik's function is to address problems in a computer network, specifically for managing internet connections. This allows internet connections to be centralized and makes management easier [9]. Mikrotik can be seen in Figure 3.

Figure 3. Mikrotik

2.4. Putty

PuTTY is a software application that functions as an SSH, Telnet, and rlogin client. It's designed to provide remote server access via network protocols like Secure Shell (SSH), Telnet, and Remote Login (rlogin) [10]. PuTTY can be seen in Figure 4.

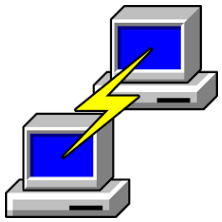

Figure 4. Putty

2.5. Port Knocking

Port knocking is a method for closing and opening specific ports that administrators can secure using a series of keys or codes. This method employs a specialized authentication system designed for client-server connections. Port knocking is a concept that hides a remote service, allowing a firewall to grant access to a port and its associated services only after the client successfully authenticates with the firewall [11].

2.6. Port Scanning

Port scanning is a technique used to scan ports on a computer network by using specialized software or tools to perform automated port scanning [12].

2.7. Brute Force

Brute force is an attack method that attempts all possible combinations to guess a password or encryption key used in a system. This attack is carried out with the hope of gaining illegal access to an account or sensitive data by trying every possibility in sequence.

If a brute force attack is successful, the attacker can gain illegal access to user accounts, systems, or or sensitive data. This can negatively impact data confidentiality, user privacy, or the integrity of the attacked system [13].

2.8. Distributed Denial of Service (DdoS)

This describes a type of cyber attack that aims to overwhelm a server or network by sending a large volume of requests or traffic, making it unable to serve legitimate requests. This DDoS attack is carried out using many distributed sources across the network to send massive traffic to the target, making it harder to track and stop the attack [14].

2.9. Packet Sniffing

Packet sniffing, also known as network analysis or packet capturing, is the process of intercepting packets flowing through a computer network. To perform packet sniffing, specialized applications are required. These applications capture each packet and sometimes analyze its contents based on RFC (Request for Comments) or other specifications. Depending on the network's structure (such as a hub or switch), the party performing the sniffing can access all or part of the traffic from a single machine on the network. Sniffing applications can also configure the network controller to operate in promiscuous mode to listen to all packets [15].

2.10. Knock

In the context of computer security, knocking refers to a technique or method used to secure access to network services by requiring users to perform a specific series of actions or send a correct sequence of packets before access to the service is granted [16].

3. Result and Discussions

3.1. Firewall Configuration Result

This research implements the port knocking method on a router firewall to enhance network and server security. Through this method, only clients that successfully perform the correct port knocking sequence are granted access to services or servers. The port knocking rules applied to the firewall can be seen in Figure 5.

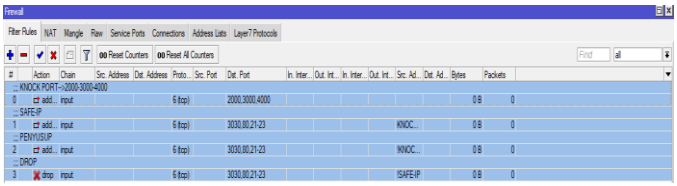

Figure 5. Port Knocking Rule

The administrator uses four (4) knocking rules to secure access to ports commonly open to the public. The administrator applies knocking to all ports provided by the laboratory's 110 cloud computing router, including Winbox (3030), FTP (21), SSH (22), Telnet (23), and WWW (80).

3.2. Service Access Testing

Service access testing was conducted to determine the firewall's response to accessing services provided by the router before and after performing port knocking. The results of the access testing can be seen in Table 1.

Table 1. Service Access Testing Result

No	Port Knocking	Service				Success Percentage	
		SSH WinBox	FTP	Telnet	WWW	Fail	Success

1	Before	Fail	Fail	Fail	Fail	Fail	100%	0%
2	After	Success	Success	Success	Success	Success	0%	100%

Based on Table 1, the firewall only permits access to services for clients that have performed port knocking correctly and completely. Access attempts by client IP addresses that do not perform port knocking will be added to the "Intruder" address list, and their access will be denied by the firewall.

3.3. Firewall Testing Against Nmap Port Scanning Attack

Nmap operates by sending a series of packets to a specified target and analyzing the responses. From these responses, Nmap can determine whether a port is open, closed, or even filtered. The results of the firewall's testing against port scanning attacks can be seen in Table 2.

Table 2. Port Scanning Attack Testing Result

No	Port Number	Attacker Ip address	Knocking Step	Knokcing Time Out	Attack Time	Total Success Knock	Success Attack Percentage	
							Fail	Success
1	21-80	192.168.20.111	4	1 hour	52.77 s	0	100%	0%
2	80-3030	192.168.20.111	4	1 hour	255.34 s	0	100%	0%
3	80-3030	192.168.20.111	4	1 hour	507.35 s	0	100%	0%

Based on Table 2, port scanning attacks against Mikrotik Routerboard LAB110 failed to scan existing ports or services. This confirms the effectiveness of the port knocking method in protecting the system from suspicious port scanning attempts.

3.4. Firewall Testing Against DDoS

A DDoS (Distributed Denial of Service) attack is a type of cyber attack where a group of attackers use numerous devices to simultaneously flood one or more targets with an extremely large volume of data traffic. The results of the firewall's testing against DDoS attacks can be seen in Table 3.

Table 3. DDoS Attack Testing Result

No	Attacker Ip address	Firewall Port knocking	Attack	Result	Attack Package	Success Attack Percentage	
						Fail	Success
1	192.168.20.250	Active	DDoS	Detected	Drop	100%	0%
2	192.168.20.251	Active	DDoS	Detected	Drop	100%	0%

Based on Table 3, it's evident that two attacker IP addresses were detected by the firewall filter and added to the "Penyusup" (Intruder) address list. The firewall successfully blocked packets from these attacks, with a total of 3300 packets rejected during the attack, amounting to 3300 bytes (B).

3.5. Firewall Testing Against Brute Force

Nmap brute force attacks are automated attempts to gain unauthorized access to systems or services by trying various password combinations using Nmap software. The attacker targets SSH, FTP, Telnet, and WWW services. The results of the firewall's testing against brute force attacks can be seen in Table 4.

Table 4. Brute Force Attack Testing Result

NO	Port Number	Attacker Ip address	Firewall Port knocking	Port Status	Success Attack Percentage	
					Fail	Success

1	SSH (22)	192.168.20.111	Active	Filtered	100%	0%
2	Telnet (23)	192.168.20.111	Active	Filtered	100%	0%
3	FTP (21)	192.168.20.111	Active	Filtered	100%	0%
4	WWW (80)	192.168.20.111	Active	Filtered	100%	0%

Based on Table 4 from the attack attempts, it shows that the Nmap brute force attack failed because the port knocking firewall caused the target service/port to be in a filtered status, and the firewall successfully secured the network against the attack.

3.6. Firewall Testing Against Packet Sniffing

Sniffing is the process of intercepting data packets on a computer network system. This involves monitoring and capturing all network traffic that passes through, regardless of the intended recipient. A significant detrimental impact of this is that an attacker can view sensitive information, such as usernames and passwords, within the data packets traveling across the computer network.

Table 5. Packet Sniffing Attack Testing Result

No	*Website*	*Port*	Protocol	Success Attack Percentage	
				Fail	Success
1	Pusbindiklatren.bappenas.go.id	80	HTTP	0%	100%
2	Webfig Mikrotik (192.168.2.254:8080)	80	HTTP	50%	50%
3	Paspor-gtk.simpkb.id	80	HTTPS	100%	0%

Based on the results from Table 5, it indicates that packet sniffing attacks will only be successful on HTTP websites. On HTTP websites, data such as passwords, personal information, and other sensitive data are sent in plain text, meaning user privacy is vulnerable to sniffing attacks. Conversely, on HTTPS websites, this data is encrypted and secure from hacking.

4. Conclusion

After conducting research on the implementation of a firewall using the Port Knocking method for network and server security, the following conclusions can be drawn:

a. Access Control Effectiveness: For service and port access, the firewall only permitted access to clients who successfully performed the port knocking sequence correctly and completely. Clients who failed to perform the knocking sequence were added to the "Intruder" address list and had their access denied by the firewall. All access attempts without proper port knocking were 100% unsuccessful.
b. Attack Detection and Mitigation: During testing against various attacks including port scanning, DDoS, and brute force, the firewall using the port knocking method successfully detected the attacker's IP addresses. These attacker IP addresses were added to the "Intruder" address list, and their access was subsequently denied by the firewall.
c. DDoS Attack Resilience: Specifically for DDoS attack testing, the firewall successfully detected the attacker's IP addresses and added them to the "Intruder" address list. It also successfully rejected packets from these attacks, with a total of 3300 packets being blocked during the assault, amounting to 3300 bytes (B).
d. Packet Sniffing Limitations: In packet sniffing attack testing, the firewall did not directly respond to the attack. This is because sniffing attacks do not target the firewall directly but rather the clients connected to the cloud computing laboratory network. Sniffing attacks were successful on HTTP web protocols (where data like passwords and personal information are sent in plain text), but unsuccessful on Mikrotik Webfig for capturing passwords, though usernames could still be found.

REFERENCES

[1] A. Amarudin, "Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking," *J. Teknoinfo*, vol. 12, no. 2, p. 72, 2018.

[2] S. Khadafi, S. Nurmuslimah, and F. K. Anggakusuma, "Implementasi Firewall Dan Port Knocking Sebagai Keamanan Data Transfer Pada Ftp Server Berbasiskan Linux Ubuntu Server," *J. Ilm. NERO*, vol. 4, no. 3, pp. 181–188, 2019.

[3] J. Al Amien, "Implementasi Keamanan Jaringan Dengan Iptables Sebagai Firewall Menggunakan Metode Port Knocking," *J. Fasilkom*, vol. 10, no. 2, pp. 159–165, 2020.

[4] Anita, "Analisis Dan Implementasi Firewall Menggunakan Metode Port Knocking Berbasis Mikrotik Routeros," 2018.

[5] M. Z. Rifqi, "Implementasi Sistem Keamanan Jaringan Pada Mikrotik RB-951 Menggunakan Metode Port Knocking," vol. 000, no. 0411, p. 586043, 2021.

[6] M. Wijaya, "Efektifitas Penggunaan Metode Port Blocking Dan Port Knocking Pada Sistem Keamanan Jaringan," no. 8.5.2017, pp. 2003–2005, 2022.

[7] R. Albar and R. O. Putra, "Sniffing Dan Implementasi Keamanan Jaringan Network Security Analysis Using the Method Sniffing and Implementation of Network Security on Microtik Router Os V6 . 48 . 3 Using Port Knocking Method," *J. Informatics Comput. Sci.*, vol. 8, no. 1, pp. 1–11, 2022.

[8] P. Teknova, "Memastikan Keamanan Jaringan dengan Teknologi Firewall," *profio.co.id*, 2020. https://profio.co.id/memastikan-keamanan-jaringan-dengan-teknologi-firewall/.

[9] E. Santi, "Pengertian Apa Itu Mikrotik, Jenis, dan Cara Setting yang Benar," *idwebhost.com*, 2022. https://idwebhost.com/blog/pengertian-apa-itu-mikrotik-fungsi-jenis-dan-cara-setting-yang-benar/.

[10] E. O. Choiri, "Apa Itu PuTTY, Fitur dan Cara Menggunakannya," *qwords.com*, 2022. https://qwords.com/blog/apa-itu-putty/.

[11] jurusan teknik mesin L. N. Ikhsanto, "Aplikasi Keamanan Jaringan Menggunakan Metode Port Knocking," vol. 21, no. 1, pp. 1–9, 2020.

[12] Y. Muhyidin, M. Hafid Totohendarto, E. Undamayanti, and S. Tinggi Teknologi Wastukancana, "Perbandingan Tingkat Keamanan Website Menggunakan Nmap Dan Nikto Dengan Metode Ethical Hacking Comparison of Website Security Levels Using Nmap and Nikto With Ethical Hacking Methods," *J. Teknol.*, pp. 1–10, 2020.

[13] Y. Mulyanto and A. A. Fari, "Analisis Keamanan Login Router Mikrotik dari Serangan Brute Force Menggunakan Metode Penetration Testing," *J. Inform. Teknol. dan Sains*, vol. 4, no. No.3, pp. 145–155, 2022.

[14] N. P. D. R. R. Ida Ayu Mas Putri Mahalini, Ida Bagus Kusuma, Dewantara, N. M. Mahardika, Listartha, I. M. E. Saskara, and G. A. Jude, "Analisis Kelayakan Tools Dengan Metode Penyerangan Distributed Denial of Service (Ddos) Menggunakan Fl00D3R, Ddos-Ripper, Dan Raven-Storm," *J. Teknol. Inf.*, vol. 6, no. 2, pp. 278–285, 2022.

[15] Y. Astuti, H. Aspriyono, and R. Zulfiandry, "Analysis of Wifi Network Security with Packet Sniffing Technique at RRI Bengkulu Public Broadcasting Institution," *Gatotkaca J.*, vol. 2, no. 2, pp. 163–172, 2021.

[16] M. A. Verdiana, I. M. A. D. Suarjaya, and A. A. K. A. C. Wiranatha, "Implementasi Algoritma PRNG pada Aplikasi Port Knocking Sebagai Perlindungan Server," *J. Ilm. Merpati (Menara Penelit. Akad. Teknol. Informasi)*, vol. 8, no. 3, p. 232, 2020.