Evaluation of Data Center Network Security based on Next-Generation Firewall

Andi Jehan Alhasan, Nico Surantha
Computer Science Department, BINUS Graduate Program-Master of Computer Science, Jakarta, Indonesia

***Abstract*—This study aims to create a network security system that can mitigate attacks carried out by internal users and reduce attacks from internal networks. Further, a network security system is expected to overcome the difficulty of mitigating attacks carried out by internal users. The goal of this research is to analyze the effectiveness of the Next-Generation Firewall implemented to improve network security. The method used in this research is the comparison method with a test of TCP SYN attack, UDP flood attack, ICMP smurf attack, and DHCP starvation attack on a company network. From the experiment results, it can be concluded that the Next-Generation Firewall has significantly better performance for protecting mitigating attacks carried out by internal users on a company network. It can increase the security of data communication networks against threats from the internal networks.**

Keywords—Network security; next-generation firewall; TCP SYN attack; UDP flood attack; ICMP smurf attack

I. Introduction

Advances in IT technology today bring security concerns. So, it is crucial to secure network infrastructure [1]. Some widely used mechanisms to secure the network are firewall, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS). A firewall is a software or hardware-based network security system that controls incoming and outgoing network traffic by analyzing packets and determining whether packets are allowed through the firewall or not based on the rules created. The firewall works on Transmission Control Protocol/Internet Protocol (TCP/IP) [2]. Other mechanisms to secure the network are Intrusion Detection System (IDS), which can detect unauthorized attack activity, and Intrusion Prevention System (IPS), which can perform actions to prevent intrusion or attack on the network [3]. The purpose of using Firewall, IPS, or IDS is to protect the internal network from external attacks network and to protect firewall core network from internal attacks.

In the existing network topology, coal companies currently still use traditional firewall devices to provide network security for the company's data center network infrastructure. Traditional firewalls that are currently implemented in the company have not been able to prevent attacks from attackers originating from the local area network, such as DHCP Starvation attacks, TCP Syn Attacks, UDP Flood Attacks and, ICMP Smurf Attacks, to the coal company's core network firewall because traditional firewalls are currently only able to block data/traffic that passes in the form of ip addresses, ports, and protocols and cannot block specific data or detect the contents of data packets that pass through the network [18] [19]. Traditional Firewall rules and policies are not able to block these attacks due to the limitations of features in general in traditional enterprise firewall devices or other traditional firewall devices. The design of the Next Generation Firewall implementation on the pfSense firewall device is expected to be able to prevent attacks originating from the local area network to the core network firewall. The advantage of Next Generation Firewall compared to traditional firewalls is that it is able to provide network security functions by implementing packet blocking and a deep packet inspection feature against a number of malicious packets passing through the network. The Next Generation Firewall will periodically protect against new types of attacks that have not been identified by traditional firewalls. In this study, the Next Generation Firewall was integrated with an existing firewall that functions only as a router that currently exists in the company's network infrastructure.

Based on previous research papers that have been reviewed, previous research only used firewall, Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) devices to prevent SQL Injection attacks, OS Bash Injection Attacks, HTTP Traffic, DDoS attacks, Port Scanners, and Password Brute Force. There has been no research that focuses on preventing attacks from attackers on traditional firewalls, IPS and IDS such as DHCP Starvation attacks, TCP Syn Attacks, UDP Flood Attacks, and ICMP Smurf Attacks. So, our motivation in this research is to contribute by adding new methods of preventing or mitigating types of attacks, namely, DHCP Starvation attack, TCP Syn Attack, UDP Flood Attack, and ICMP Smurf Attack, from local area networks to firewall devices from the internal network.

In this study, a solution for preventing attacks from local area networks to the core network firewall infrastructure is the use of the Next Generation Firewall pfSense which is integrated with the existing firewall that functions as a router. In this study, it will be tested using Kali Linux (Nmap, Hping3) and Yersinia Tool as attackers and Next Generation Firewall pfSense along with its configuration as a prevention of these attacks.

II. Literature Review

Putra and Surantha previously have done research to design and implement vulnerability port Hypertext Transfer Protocol (HTTP), SQL Injection, and OS Bash Injection Attack on servers from internal network or inline mode with Damn Vulnerable Web App and Vega Vulnerability Scanner tools. The study integrated Cisco ISE Network Access Control, Cisco Identity Service Engine (ISE), and Intrusion Prevention System (IPS) on Cisco Firepower 8250 devices. In the study, the attack test was carried out on the windows server and then SQL Injection attack and OS Bash Injection Attack were performed on the server. The test results obtained that the integration of cisco ISE as Network Access Control (NAC) and Cisco Firepower 8250 devices as IPS can prevent attacks to HTTP ports, SQL Injection, and OS Bash Injection Attack the server from internal attacks. Compared to using only NAC devices because Cisco ISE devices can not prevent such attacks [4].

Erlacher and Dressler researched the implementation of Signature-based Network Intrusion Detection Systems using the Snort tool and in the research, they used Novel Flow-based Network Intrusion Detection Systems-Flow Information Export-based Signature-based Intrusion Detection System (NIDS FIXIDS). In the study, Tool Vermont (Versatile Monitoring Toolkit) served as a network monitoring toolkit and was combined with snort to prevent and detect attacks of massive HTTP traffic or high-speed traffic. The attack was tested using the Cisco Trex Traffic generator tool by sending high-speed HTTP traffic on a network that has been running NIDPS and FIXIDS. The test results improved methods for preventing and detecting a massive traffic attack on the network [5].

Other research by Bul'ajoul, James, and Shaikh researched the implementation of a Network Intrusion detection prevention system (NIDPS) using the Snort tool as NIDPS with a new Novel NIDPS architecture method. In the study, the snort tool that functioned as NIDPS could not prevent and detect attacks optimally when it received a huge traffic attack or high-speed traffic. Testing was done from Wincap, Flooder Packet, and Transmission Control Protocol (TCP) replay tools as attackers transmit TCP and User Datagram Protocol (UDP) traffic attacks. Testing with Novel NIDPS method architecture and integrating with Cisco Layer 3 switch resulted in better attack prevention and detection methods despite massive traffic attacks or high-speed traffic to internal networks [6].

Other research, which was conducted by Kaur and Singh, examined Web-Based attacks or attacks on a website on a network using deep learning-based system methods as hybrid intrusion detection and signature generation to prevent and detect attacks on the web. The prevention and detection of such attacks using D-Sign Architecture consist of Misuse Detection Engine, Anomaly Detection Engine, and Signature Generation Engine. In the study, the attack was tested by experimenting with attacks to a web with various HTTP traffic attacks. The results of D-Sign Architecture Implementation combined with Deep Recurrent Neural Network-based anomaly detection can produce better prevention and detection in the event of a known attack or a new attack on HTTP [7].

Duppa and Surantha did review and comparison testing traditional Intrusion Prevention System and Next-Generation Intrusion Prevention System. In the study, testing Next-Generation IPS to protect the network from attacks that take advantage of traditional IPS weaknesses, namely exploitation to HTTP Port or layer 7. Testing was done using Kali Linux as an attacker from inline or internal network mode with SQL Injection attack and malicious site exploit. The device used as NGIPS is Cisco Fire Power. From the penetration testing results, it can be concluded that Next-Generation IPS using the Cisco Firepower device can prevent SQL Injection attacks and malicious site exploit better than traditional IPS [8].

Ring and Landes researched the implementation using two methods, namely Unsupervised Port Scan Detection (UPDS) and Supervised Port Scan Detection (SPDS) in the research, to prevention of port scanning TCP and UDP protocols in a traffic network, such as scanning ports that open on Switch, Router, and Firewall devices. The scanning port was done in the research with the Nmap tool combined with Open Stack and NetFlow. The research compared the port scanning test algorithm with several TFDS, TRQ-SYN, UPDS, SPDS, and Webster. The test results obtained the results that UPDS and SPDS algorithms on the network can reduce or prevent an attacker from being able to scan open ports on the network or the user client [9].

Three-Tier Novel Architecture for Intrusion Detection and Prevention System in Software Defined Network was for prevention of DDoS attacks on a network. The research compared and tested Novel Three-Tier architecture with Intrusion Detection and Prevention SDN-IoT method to prevent replay attack, Mima attack, forgery attack, DDoS attack, on SDN network. From the test results, from the test results, it can be concluded that using Novel Three-Tier architecture for Intrusion Detection Prevention System (IDPS) can be guided from attacks on the system rather than the old Intrusion Detection and Prevention SDN-IoT [2].

Research conducted by Rengaraju and Ramanan researched the implementation of Intrusion Prevention System on Software Defined Networking network to secure Software-Defined Clouds (SDC) network as a controller for Denial-of-Service (DoS) and ICMP Flooding attack prevention. Attack testing was carried out with the hping3 tool. From the test results obtained, SDC Controller that serves as Access List (ACL) and IPS can prevent Denial-of-Service (DoS) and ICMP Flooding attacks with Signature-based method [10].

Research conducted by Karim and Handa researched Intrusion Detection System, which is increasingly a key element of system security that is used to identify the malicious activities in a computer network or system. Hybrid computing is one of the latest and an emerging area in the Information and Technology (IT) sector, which has given a different dimension to the organizations. Performance and security aspects and the major issues have to be addressed in Hybrid Computing. This research will attempt to give an overall idea about Hybrid computing, Intrusion, types of Intrusion Detection Systems, and earlier works done on Intrusion Detection System [11].

A global intrusion detection system composed by autonomous Internet-distributed detection systems was proposed. In our approach, distributed detection elements cooperate by sending information about a potential threatening flow that traverses its Autonomous System (AS). Distributed Intrusion Detection Systems (DIDS) use Border Gateway Protocol (BGP) updating capabilities in order to spread intrusion warning messages across Internet routing domain so as to notify the SIEM of the attack target. When an anomalous in-transit traffic is detected, the AS integrated IDS gathers all attributes of the anomalous flow in the extended BGP Network Layer Reachability Information (NLRI) field and advertises it towards the AS target of the intrusion. Then, the SIEM of the target AS can use such information set to manage related protection countermeasures [12] [13].

Other research by Choi and Allison is in the form of a review paper related to the methods used Intrusion Prevention System and Intrusion Detection System. IPDS performs attack prevention and detection using 2 algorithms, namely signature-based detection and anomaly detection. In the study, the authors emphasized the use of IDPS implementation in a small to Medium-size Enterprise in preventing and detecting attacks within computer networks [14].

This research was to analyze the effectiveness of the Next Generation Firewall that was implemented to secure IoT in smart house and company network. The method used in this research was the method of comparison with a test of DDoS attacks, phishing, and SQL Injection on both network, smart house network, and company network. From the results of experiment, it can be concluded that the Next Generation Firewall has significantly better performance for protecting smart house and company network and it can increase security of data communication networks against threats from the Internet [15].

Sri Lanka Institute of Information Technology Computing (Pvt) Ltd representatives presented research in 2016 on how to create a more secure network by integrating firewall capability and firewall technologies. The findings of the experiment prove that the suggested concept is capable of constructing a stable network. This study discussed how firewalls are used to shield infrastructure from outside intruders and how Virtual Private Networks (VPN) allow encrypted access to the corporate network over non secure public networks [16].

Other research by Kishan, Rami, and Lei researched the Traditional firewalls are incapable of coping with emerging threats such as targeted and data-focused attacks. This paper discusses a survey of the different types of current and next-generation firewalls, highlighting their potential functionalities. The different technologies implemented in Next-Generation Firewall (NGFW) for network security were highlighted. Additionally, the advantages of the next-generation firewalls were compared against the traditional firewalls. Also, in this paper, the primary network security goals, their recent emerging security threats, and their potential solutions to protect the network are discussed [17].

Most data centers still use traditional firewalls, Intrusion Prevention System (IPS), and Intrusion Detection System (IDS) to provide network security in data centers. Traditional firewalls, IPS, and IDS applied in this data center cannot detect attacks with different variants, such as TCP SYN attacks, UDP flood attacks, ICMP smurf attacks, and DHCP starvation attacks. By utilizing anomaly-based because traditional firewall, IPS, and IDS weaknesses only understand the identity of data passed based (IP address and port used) and unable to recognize deep packet inspection, unable to know what is in the data package of these attacks.

TABLE I. COMPARISON OF RESEARCH ON IPS, IDS AND FIREWALL

No	Reference	Research Topics	Method	Tools
1	Putra & Surantha, 2019	implementation Cisco ISE and IPS NAC to prevent SQL Injection attacks and OS Bash Injection Attack on servers.	Network Access Control and Intrusion Prevention System (IPS)	Cisco ISE and Cisco Firewall Firepower
2	Erlacher & Dressler, 2019	Implementation of Signature-based Network Intrusion Detection Systems to prevent HTTP Traffic attacks	Signature-based Network Intrusion Detection Systems	Snort, Tool Vermont, and Cisco Trex Traffic generator
3	Bul'ajoul, James, & Shaikh, 2019	Implementation of Network Intrusion detection prevention system (NIDPS) to prevent substantial traffic attacks or high-speed traffic on an internal network	Novel Network Intrusion Detection Systems architecture	Snort, tool Wincap, Flooder Packet, and TCP replay
4	Kaur & Singh, 2019	Research related to Web-Based Attack or attack on a website on a network	Arsitektur D-Sign, Deep Recurrent Neural Network-based anomaly detection	Open Web Application Security Project (OWASP)
5	Duppa & Surantha, 2019	Implementation of Next-Generation IPS Testing to prevent SQL Injection and Exploit Malicious Site attacks	Next Generation Intrusion Prevention System (NGIPS)	Cisco ISE and Cisco Firewall Firepower
6	Ring, Landes, & Hotho, 2018	Testing and prevention of port scanning to TCP and UDP protocols on traffic network for the prevention of port scanning on Switches, Routers, and Firewall	UPDS (Unsupervised Port Scan Detection) and SPDS (Supervised Port Scan Detection).	Nmap, Open Stack, and NetFlow
7	Ali & Yousaf, 2020	Intrusion Detection and Prevention System in Software Defined Network to prevent DDOS attacks on SDN network	Deep Learning Novel Three-Tier	Network simulator environment OMNeT++ 4.6
8	Choi & Allison, 2017	Review paper of attack prevention and detection using signature-based detection and anomaly detection algorithms in small and medium-sized enterprise network	Signature-based detection and anomaly detection of IDS, IPS	
9	Rengaraju & Ramanan, 2017	Implementation of Intrusion Prevention System in Software Defined Networking network for Denial-of-Service attack prevention.	Distributed Firewall with Intrusion Prevention System (IPS) for SDC	Software-Defined Clouds Controller
10	Soewito & Andhika, 2017	Analyze and implemented the effectiveness of the Next Generation Firewall to prevent DDoS attacks, phishing, and SQL Injection in bright house and the company network.	Next Generation Firewall	LOIC (Low Orbit Ion Canon) and NGFW Checkpoint
11	Tharaka, Silva, & Sharmila, 2016	Analyze firewall capacity and other firewall technologies such as packet filtering, network address translation, virtual private network, and proxy services.	Firewall	
12	Neupane, Rami, & Lei, 2018	A survey of the different types of current and next generation firewalls are discussed in details highlighting their potential functionalities.	Next Generation Firewall	Palo Alto Next Generation Firewall

Previous research on Literature Review or refer in the Table I used a firewall, IPS, and IDS devices to prevent SQL injection attacks, OS bash injection attacks, HTTP traffic, DDoS attacks, Port scanner, and passwords brute force only. No research focused on preventing attacks such as TCP SYN, UDP flood, ICMP smurf, and DHCP starvation attacks on firewall or router devices. Thus, the motivation of this research is to later contribute by adding prevention or mitigation with different variants types of attacks that currently often occur in network infrastructure in data centers that come from internal networks.

In this research, a solution was proposed to improve network security to prevent attacks on the company's infrastructure network and prevent attacks from internal networks to the company's core network infrastructure by using Next-Generation Firewall pfSense and Suricata tool.

III. Methodology

A. System Design

As summarized in Table II, the Next-Generation firewall used in this research was open source tool security software, namely pfSense with OS 2.5.1 series. Next-Generation firewall has been connected between the traditional firewall and core switches. The Next-Generation firewall pfSense was integrated with the traditional firewall with all segments in the network infrastructure. Pfsense was able to communicate with a traditional firewall as a router to perform the expected integration according to the objectives in this study. Switch access connected directly to the user's pc using layer 2 switch. Computers used as attackers were Asus type with Kali Linux OS.

Fig. 1 proposes a new topology using Next-Generation firewall pfSense connected to the network in inline mode. In this study, the device was integrated with the existing infrastructure. The integration done in this study was a physical and logical connection in which the traditional firewall as a router internet gateway and the Next-Generation firewall pfSense should be able to connect with existing infrastructure devices and then configure to integrate existing devices. Policy implementation and configuration will be carried out on the Next-Generation firewall pfSense to prevent TCP SYN attack, UDP flood attack, ICMP Smurf attack and DHCP Starvation Attack. To achieve the objectives in this study, a network security system that can reduce internal users who carry out attacks and reduce attacks from internal networks was created by using Next-Generation firewall pfSense.

In the existing network topology, the traditional firewall core network implemented as a router internet gateway, which runs Network Address Translation (NAT) service, Routing Default route, Domain Name System (DNS) Service, and service Dynamic Host Configuration Protocol (DHCP), aims to connect internal network clients to connect the internet safely and reliably. On the proposed added devices topology above, Next-Generation firewall devices implemented the Intrusion Prevention System (IPS) feature in inline mode to prevent attacks to the traditional firewall core network. On the access switch, VLAN and Port Security division are implemented to ensure that only clients' registered Media Access Control (MAC) address and VLAN in the switch can be connected to the network or the internet.

TABLE II. Existing and Proposed System Specifications

Tool	Vendor	OS Version	Function
RB1016-12G	Mikrotik	6.47.8	Traditional Firewall As Router Internet Gateway
PC with 2 LAN Card	PfSense	2.5.1	Next-Generation Firewall

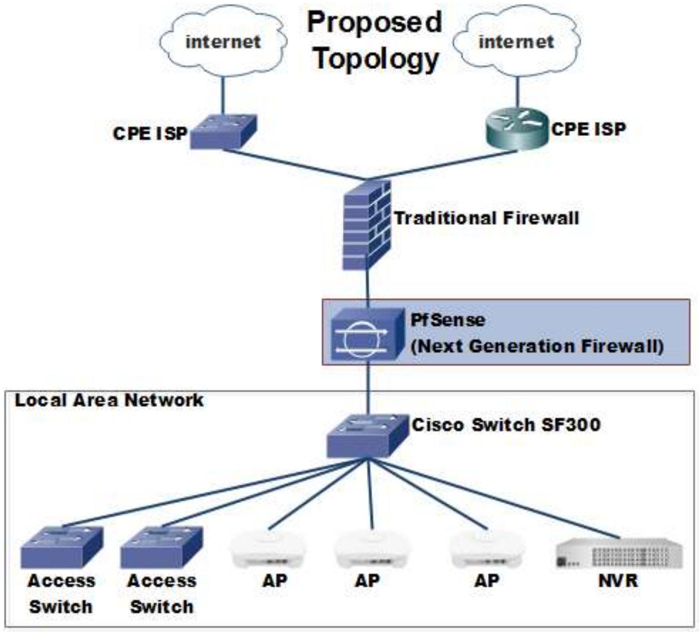


Fig. 1. Proposed Network Topology.

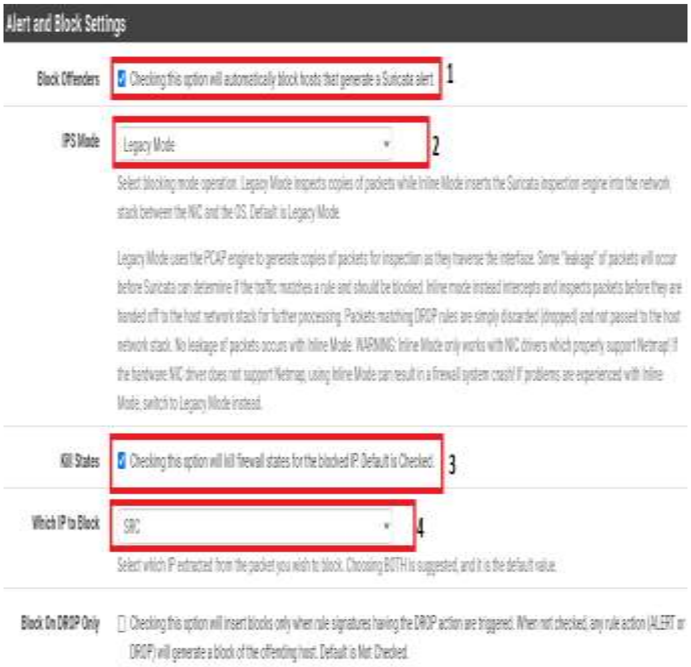
Table III presents existing configuration traditional firewall Mikrotik as router internet gateway, while Table IV and Fig. 2 present the configuration of the proposed Next-Generation Firewall Pfsense as intrusion prevention system for preventing TCP SYN attack, UDP flood attack, ICMP smurf attack, and DHCP starvation attack from an internal network.

TABLE III. Configuration of Traditional Firewall Mikrotik

Service	Configuration	Function
IP Address	ip address add address=192.168.10.1/24 network=192.168.1.0 interface=ether1	IP Gateway Local Area Network
DHCP Client	ip dhcp-client add interface=wlan1 use-peer-dns=yes use-peer-ntp=yes add-default-route=yes	Request Internet Connection to ISP
NAT	chain=srcnat action=masquerade out-interface=wlan1 log=no log-prefix=""	Translation from an internal network to external network/internet
Default Route	ip route add dst-address=0.0.0.0/0 gateway=192.168.1.1 distance=1	Routing packet to the internet from LAN
DHCP Server	Add address=192.168.10.0/24 gateway=192.168.10.1	Give out ip address to LAN

TABLE IV. CONFIGURATION OF PROPOSED NEXT-GENERATION FIREWALL PFSENSE FOR PREVENTING ATTACKS

Service	Configuration	Function
IP Address	Interface>LAN>IPv4 address 192.168.1.1, IPv4 subnet /24, description LAN	Default gateway LAN
	Interface>WAN>IPv4 address 192.168.10.2, IPv4 subnet /24, IPv4 gateway 192.168.10.1 description WAN	Connection to Traditional Firewall
Default Route	System>Routing>Gateways>add Interface WAN, address Family IPv4, Gateway 192.168.10.1	Connecting to Internet
NAT	Firewall>NAT>Outbond>Mode Automatic Outbound NAT	Translation from an internal network to external network/internet
DNS	System>General Setup>DNS Server 202.152.254.246	Translate domain names into IP Addresses
Suricata	Interface>Service>Suricata	Enable Mode IPS
Intrusion Prevention System	Interface>Edit>Enable Block Offenders	For the prevention of TCP SYN, UDP flood, ICMP smurf and DHCP starvation attack
	IPS Mode> Legacy Mode	
	Kill State > Enable	
	Which IP to Block > SRC	


Alert and Block Settings

Block Offenders ☑ Checking this option will automatically block hosts that generate a Suricata alert 1

IPS Mode: Legacy Mode 2

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Suricata inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Suricata can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! If the hardware NIC driver does not support Netmap, using Inline Mode can result in a firewall system crash! If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States ☑ Checking this option will kill firewall states for the blocked IP. Default is Checked. 3

Which IP to Block: SRC 4

Select which IP extracted from the packet you wish to block. Choosing BOTH is suggested, and it is the default value.

Block On DROP Only □ Checking this option will insert blocks only when rule signatures having the DROP action are triggered. When not checked, any rule action (ALERT or DROP) will generate a block of the offending host. Default is Not Checked.

Fig. 2. Enable Configuration IPS on pfSense using Suricata.

B. *Implementation and Testing*

In this research, implementation and testing were carried out to prove the solution given to overcome the existing problems. This implementation and testing were carried out using system design and infrastructure that has been integrated with the traditional firewall like a router internet gateway and Next-Generation firewall pfSense and Suricata as an Intrusion Prevention Systems. By configuring the traditional firewall and Next-Generation firewall pfSense, both systems can communicate and integrate to achieve the objectives of this research. Then, this test took place by trying to simulate an attack by connecting the user's laptop to the internal network. The attack operating system used the Kali Linux tool hping3 and additional tool Yersinia that acted as an attacker. In this study, the traditional firewall Mikrotik targeted the attack connected to the Next-Generation firewall pfSense. Then, the attacker would perform a TCP SYN attack, UDP flood attack, ICMP smurf attack, and DHCP starvation attack on the traditional firewall. Table V presents system specifications used for attack testing simulation and Fig. 3 is the attack testing topology used in this study.

In this test, the Next-Generation firewall pfsense was located in the middle of an inline configured network so that the traditional firewall could immediately decide on the package that has been checked. The package was analyzed by the Next-Generation firewall pfSense based on signatures or anomalies. If the package contains a crime or vulnerability, the Next-Generation firewall pfSense will immediately prevent it by blocking malicious packages. Then, the Next-Generation firewall pfSense can immediately prevent and quarantine the computer that is the source of the attack so that it no longer launched prolonged attacks on the network. In this test, a compliant user was an official network access condition with specific requirements. Attack testing employed several sample attacks, namely TCP SYN attack, UDP flood attack, ICMP smurf attack, and DHCP starvation attack, using tool Hping3 and Yersinia on Kali Linux OS.

TABLE V. SYSTEM SPECIFICATIONS USED FOR ATTACK TESTING SIMULATION

Perangkat	Vendor	OS Version	Function
RB951UI-2HND	Mikrotik	6.43.1	Traditional Firewall
Laptop with 2 LAN Card	Pfsense	2.5.1	Next-Generation Firewall
Notebook	Kali Linux	Kali Linux	Attacker

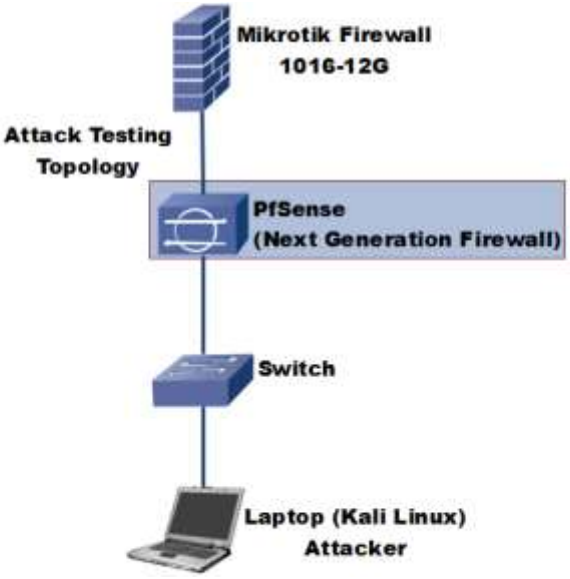


Fig. 3. Attack Testing Topology.

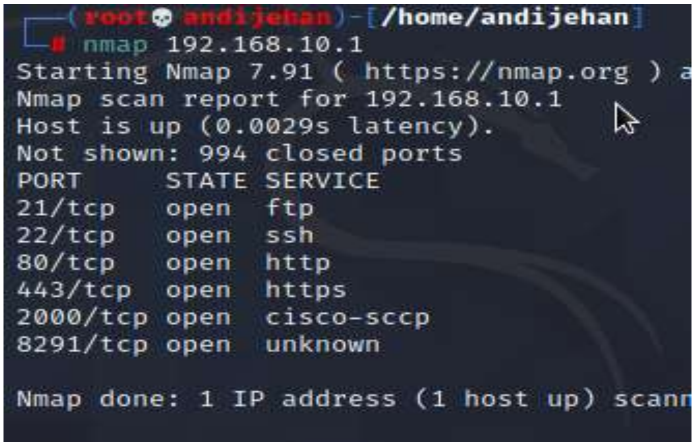
IV. Evaluation Result and Discussion

The Next-Generation firewall that was used in this study as Intrusion Prevention System was open-source pfSense and Suricata. Next-Generation firewall pfSense will connect traditional firewall Mikrotik device and cisco distribution switch. Integrating traditional firewall Mikrotik and Next-Generation firewall pfSense and Suricata as Intrusion Prevention System is expected to prevent an attack from an internal network to a traditional firewall core network.

Next-Generation firewall pfSense and Suricata will prevent attacks from internal networks to a traditional firewall core network as the purpose of this study expects. The following are the results of attack tests that have been done with the Next-Generation firewall pfSense and Suricata.

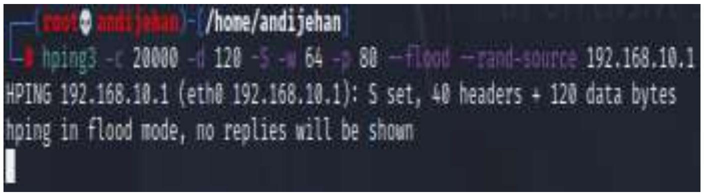
A. TCP Syn Attack

Based on the tests that have been done, users tried TCP SYN attacks using Kali Linux with the hping3 tool on the target traditional firewall Mikrotik. The first attacker performed a port scan that was available on target. The commonly used target is the 80/HTTP service, as shown in Fig. 4. Then, the attack used the command hping3 -c 20000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.10.1, as shown in Fig. 5, which aims to send the targeted attackers a large number of TCP SYN packets. Using only the traditional firewall Mikrotik, these attack attempts succeeded by exhausting traditional firewall resources and impacting performance. As shown in Fig. 6, these attacks can be performed because the traditional firewall Mikrotik cannot detect the TCP SYN attack pattern. However, using the enhancements of the Next-Generation firewall pfSense in this study, TCP SYN attack attempts were detected and blocked by pfSense. PfSense detects attack patterns and then blocks or prevents them before getting to the traditional firewall Mikrotik so that network performance becomes regular and smooth. As shown in Fig. 7, TCP SYN attacks can be mitigated by pfSense.



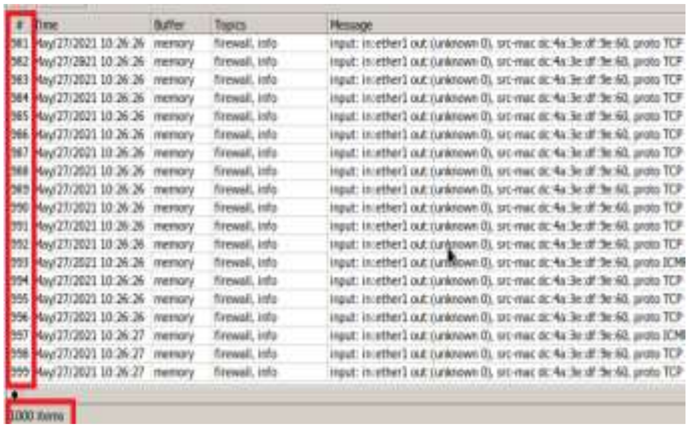
```
┌──(root💀andijehan)-[/home/andijehan]
└─# nmap 192.168.10.1
Starting Nmap 7.91 ( https://nmap.org ) a
Nmap scan report for 192.168.10.1
Host is up (0.0029s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
2000/tcp open  cisco-sccp
8291/tcp open  unknown

Nmap done: 1 IP address (1 host up) scann
```

Fig. 4. Scanning Available Ports on a Target.



```
┌──(root💀andijehan)-[/home/andijehan]
└─# hping3 -c 20000 -d 120 -S -w 64 -p 80 --flood --rand-source 192.168.10.1
HPING 192.168.10.1 (eth0 192.168.10.1): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

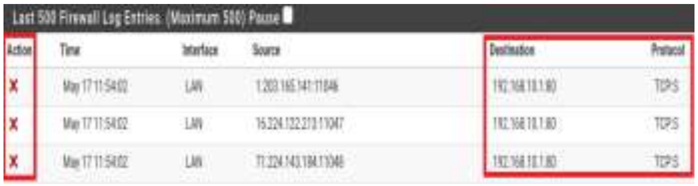
Fig. 5. Attacker Send Large Number TCP/SYN Packets.



#	Time	Buffer	Topics	Message
981	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
982	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
983	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
984	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
985	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
986	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
987	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
988	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
989	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
990	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
991	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
992	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
993	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto ICM
994	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
995	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
996	May/27/2021 10:26:26	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
997	May/27/2021 10:26:27	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto ICM
998	May/27/2021 10:26:27	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP
999	May/27/2021 10:26:27	memory	firewall, info	input: in:ether1 out:(unknown 0), src-mac dc:4a:3e:df:9e:60, proto TCP

1000 items

Fig. 6. TCP SYN Sent from Random Source Addresses.



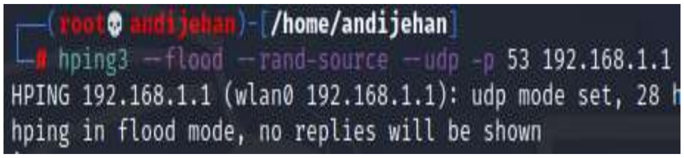
Last 500 Firewall Log Entries. (Maximum 500) Pause

Action	Time	Interface	Source	Destination	Protocol
✗	May 17 11:54:02	LAN	1.203.165.141:11846	192.168.10.1:80	TCP:S
✗	May 17 11:54:02	LAN	16.224.122.213:11047	192.168.10.1:80	TCP:S
✗	May 17 11:54:02	LAN	71.224.143.184:11048	192.168.10.1:80	TCP:S

Fig. 7. Result Log Blocked TCP SYN Attack by Pfsense.

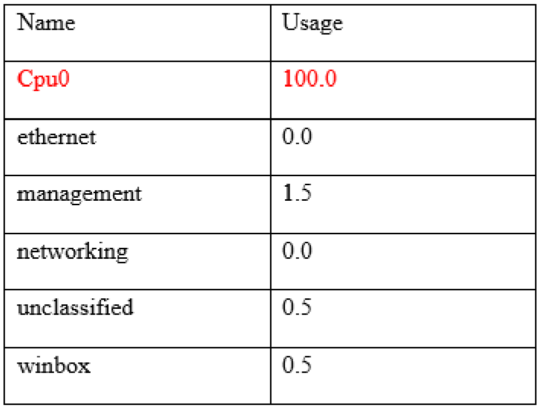
B. UDP Flood Attack

Based on the results of the second test, the UDP flood attack was carried out on a traditional firewall Mikrotik as a target by still using the hping3 tool, starting to attack the UDP 53 (DNS) protocol port with hping3, as seen in Fig. 8 using the CLI --flood --rand-source --UDP -p 53 192.168.10.1 command. This attack aimed to create and send many UDP datagrams from the pampered IP to the targeted traditional firewall Mikrotik. When the firewall receives this type of traffic, it cannot process each request and consume its bandwidth by sending ICMP "unreachable destination" packets. Using only a traditional firewall Mikrotik, these attack attempts succeeded by exhausting firewall resources and impacting performance. As shown in Fig. 9, using an additional device that was the Next-Generation firewall Pfsense in this study, UDP flood attack attempts were detected and blocked by pfSense. PfSense can detect attack patterns and then block or prevent them from getting to the traditional firewall Mikrotik so that network performance becomes regular and smooth. As shown in Fig. 10, the TCP SYN attack can be mitigated by pfSense.



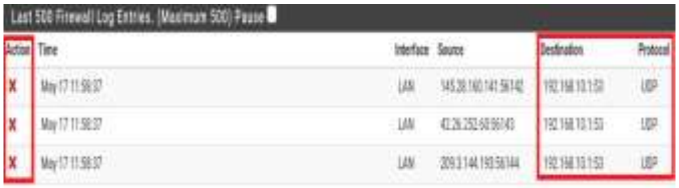
```
┌──(root💀 andijehan)-[/home/andijehan]
└─# hping3 --flood --rand-source --udp -p 53 192.168.1.1
HPING 192.168.1.1 (wlan0 192.168.1.1): udp mode set, 28 h
hping in flood mode, no replies will be shown
```

Fig. 8. Attacker UDP Protocol Port 53 (DNS).



Name	Usage
Cpu0	100.0
ethernet	0.0
management	1.5
networking	0.0
unclassified	0.5
winbox	0.5

Fig. 9. Exhausting the Resources CPU of the Traditional Firewall.

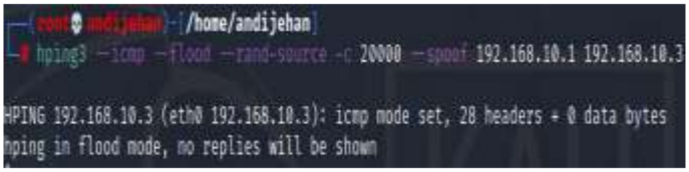


```
Last 500 Firewall Log Entries. (Maximum 500) Pause
Action Time                Interface Source                Destination       Protocol
X      May 17 11:58:37     LAN       145.28.160.141:56142  192.168.10.1:53   UDP
X      May 17 11:58:37     LAN       42.26.252.68:56143    192.168.10.1:53   UDP
X      May 17 11:58:37     LAN       209.3.144.193:56144   192.168.10.1:53   UDP
```

Fig. 10. Result Blocked UDP Flood Attack by Pfsense.

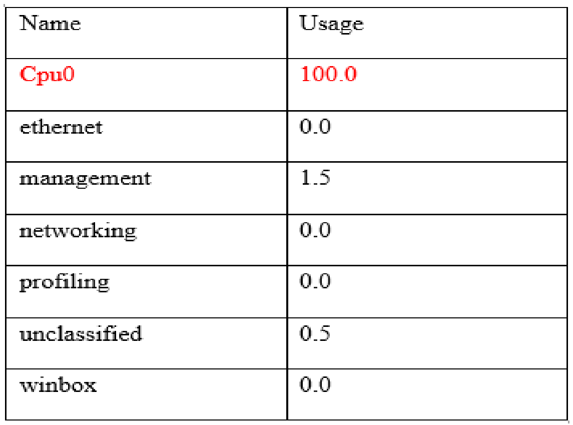
C. ICMP Smurf Attack

The third test was an ICMP smurf attack. This type of attack uses a large number of Internet Control Message Protocol (ICMP) ping firewall that targeted internet broadcast addresses, e.g., 192.168.1.255, using the command hping3 --Icmp --flood --rand-source -c 20000 --spoof 192.168.10.1 192.168.10.255. as seen in Fig. 11. This attack is aimed at all replies sent to the victim instead of the IP used for pinging. Using only a traditional firewall Mikrotik, this attack exhausts firewall resources and impacts performance, as shown in Fig. 12, because the traditional firewall cannot detect the pattern of ICMP smurf attack. However, using an enhancement that is the Next-Generation firewall Pfsense in this test, ICMP smurf attack attempt was detected and blocked by pfSense. PfSense can detect attack patterns and then block or prevent them from entering traditional firewalls so that network performance becomes regular and smooth. As shown in Fig. 13, the ICMP smurf attack can be mitigated by pfSense.



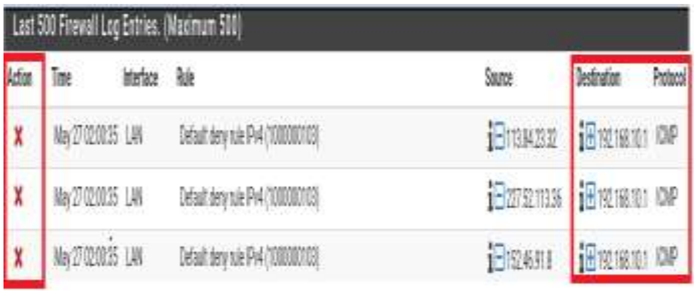
```
┌──(root💀 andijehan)-[/home/andijehan]
└─# hping3 --icmp --flood --rand-source -c 20000 --spoof 192.168.10.1 192.168.10.3

HPING 192.168.10.3 (eth0 192.168.10.3): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Fig. 11. Attacker Sends Large Number ICMP Packets.



Name	Usage
Cpu0	100.0
ethernet	0.0
management	1.5
networking	0.0
profiling	0.0
unclassified	0.5
winbox	0.0

Fig. 12. Exhausting the Resources CPU of the Traditional Firewall.

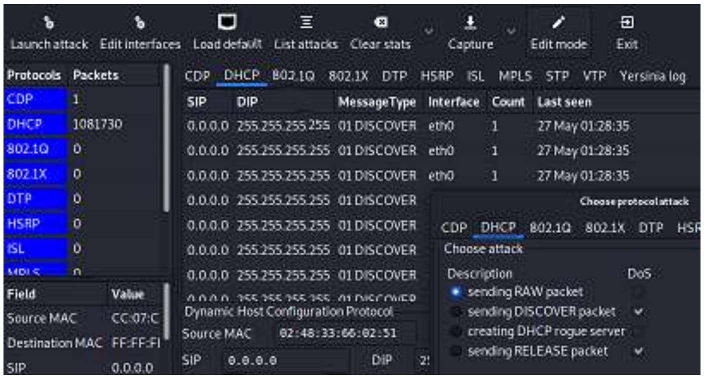


```
Last 500 Firewall Log Entries. (Maximum 500)
Action Time            Interface Rule                              Source         Destination   Protocol
X      May 27 02:00:35 LAN       Default deny rule IPv4 (1000000103) 113.84.23.32   192.168.10.1  ICMP
X      May 27 02:00:35 LAN       Default deny rule IPv4 (1000000103) 227.52.113.36  192.168.10.1  ICMP
X      May 27 02:00:35 LAN       Default deny rule IPv4 (1000000103) 152.46.91.8    192.168.10.1  ICMP
```

Fig. 13. Result Blocked ICMP Smurf Attack by Pfsense.

D. DHCP Starvation Attack

The last attack test was a DHCP hunger attack performed on a traditional firewall Mikrotik as a target using the Yersinia tool. As seen in Fig. 14, using a Mikrotik firewall, this attack can be detected and recognized so that DHCP hunger attacks do not make the traditional firewall Mikrotik down. Similarly, by using the additional Next-Generation firewall in this test, DHCP hunger strike attempts were detected and blocked by pfSense. PfSense can detect attack patterns and then block or prevent them from getting to the traditional firewall Mikrotik. As seen in Fig. 15, starvation attacks can be mitigated by traditional firewall Mikrotik and pfSense.



Protocols	Packets
CDP	1
DHCP	1081730
802.1Q	0
802.1X	0
DTP	0
HSRP	0
ISL	0
MPLS	0

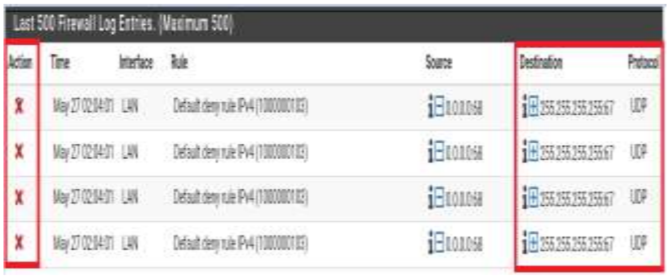
SIP	DIP	MessageType	Interface	Count	Last seen
0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	27 May 01:28:35
0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	27 May 01:28:35
0.0.0.0	255.255.255.255	01 DISCOVER	eth0	1	27 May 01:28:35
0.0.0.0	255.255.255.255	01 DISCOVER			
0.0.0.0	255.255.255.255	01 DISCOVER			
0.0.0.0	255.255.255.255	01 DISCOVER			
0.0.0.0	255.255.255.255	01 DISCOVER			
0.0.0.0	255.255.255.255	01 DISCOVER			

Field	Value
Source MAC	CC:07:C
Destination MAC	FF:FF:FI
SIP	0.0.0.0

Dynamic Host Configuration Protocol
Source MAC 02:48:33:66:02:51
SIP 0.0.0.0 DIP 2!

Description	DoS
● sending RAW packet	
○ sending DISCOVER packet	✓
○ creating DHCP rogue server	
○ sending RELEASE packet	✓

Fig. 14. DHCP Starvation Attack with Tool Yersinia.



Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	May 27 02:04:01	LAN	Default deny rule IPv4 (1000000103)	0.0.0.0:68	255.255.255.255:67	UDP
✗	May 27 02:04:01	LAN	Default deny rule IPv4 (1000000103)	0.0.0.0:68	255.255.255.255:67	UDP
✗	May 27 02:04:01	LAN	Default deny rule IPv4 (1000000103)	0.0.0.0:68	255.255.255.255:67	UDP
✗	May 27 02:04:01	LAN	Default deny rule IPv4 (1000000103)	0.0.0.0:68	255.255.255.255:67	UDP

Fig. 15. Result of Blocked DHCP Starvation Attack by Pfsense.

Table VI summarizes the results based on the completed tests in this study. It shows significantly different results from using a traditional firewall only or integrating a traditional firewall with a Next-Generation firewall pfSense. The expected test results in this study can be achieved using the proposed solution. The proposed solution demonstrated that the Next-Generation firewall pfSense can prevent attacks from internal users and can reduce attacks from internal networks based on the test scenarios that have been done. With additional devices, Next-Generation firewall pfSense can improve network security compared to traditional firewall Mikrotik only.

TABLE VI. RESULT COMPARISON

No	**Type Intrusion**	**Target**	**Result**	
			Firewall	**NGFW Pfsense (Proposed Solution)**
1	TCP Syn Attack	Vulnerable Firewall	Allowed	Blocked
2	UDP Flood Attack	Vulnerable Firewall	Allowed	Blocked
3	ICMP Smurf Attack	Vulnerable Firewall	Allowed	Blocked
4	DHCP Starvation Attack	Vulnerable Firewall	Blocked	Blocked

With the results of the tests that have been done in this research, the proposed solution is to integrate traditional firewall Mikrotik as a router with Next-Generation firewall pfSense that can mitigate against internal users who perform attacks from internal networks. Thus, network security with firewall system integration with a Next-Generation firewall can be increased compared to traditional firewall Mikrotik only.

V. CONCLUSION

Based on the test results conducted in this study, the proposed solution demonstrates that the Next-Generation firewall pfSense can prevent attacks from internal users and can reduce attacks from internal networks based on the test scenarios that have been done. With additional devices, the Next-Generation firewall pfSense can improve network security compared to traditional firewalls only. However, this study still has many limitations, especially on the type of attack tested. In this study, attack testing only targeted network devices with traditional firewall from internal networks only. It is recommended for further research to conduct attack testing from the public internet to the internal network in order to improve network security better.

ACKNOWLEDGMENT

The publication of this research is fully supported by Bina Nusantara University.

REFERENCES

[1] Abubakar, R., Aldegheishem, A., Majeed, M. F., Mehmood, A., Maryam, H., Alrajeh, N. A., ... & Jawad, M. (2020). An Effective Mechanism to Mitigate Real-Time DDoS Attack. IEEE Access, 8, 126215-126227.

[2] Ali, A., & Yousaf, M. M. (2020). Novel Three-Tier Intrusion Detection and Prevention System in Software Defined Network. IEEE Access, 8, 109662-109676.

[3] Alzahrani, S., & Hong, L. (2018). Generation of DDoS attack dataset for effective ids development and evaluation. Journal of Information Security, 9(4), 225-241.

[4] Putra, A. S., & Surantha, N. (2019). Internal Threat Defense using Network Access Control and Intrusion Prevention System. International Journal of Advanced Computer Science and Applications, Vol. 10, No. 9, 2019.

[5] Erlacher, F., & Dressler, F. (2020). On High-Speed Flow-based Intrusion Detection using Snort-compatible Signatures. IEEE Transactions on Dependable and Secure Computing.

[6] Bul'ajoul, W., James, A., & Shaikh, S. (2019). A New Architecture For Network Intrusion Detection And Prevention. IEEE Access, 7, 18558-18573.

[7] Kaur, S., & Singh, M. (2019). Hybrid intrusion detection and signature generation using Deep Recurrent Neural Networks. Neural Computing and Applications, 1-19.

[8] Duppa, G., & Surantha, N. (2019). Evaluation of network security based on next-generation intrusion prevention system. Telkomnika, 17(1), 39-48.

[9] Ring, M., Landes, D., & Hotho, A. (2018). Detection of slow port scans in flow-based network traffic. PloS one, 13(9), e0204507.

[10] Rengaraju, P., Ramanan, V. R., & Lung, C. H. (2017, August). Detection and prevention of DoS attacks in Software-Defined Cloud networks. In 2017 IEEE Conference on Dependable and Secure Computing (pp. 217-223). IEEE.

[11] Karim, H. A. R. A., Handa, S. S., & Murthy, M. R. (2017). A Methodical Approach to Implement Intrusion Detection System in Hybrid Network. International Journal of Engineering Science, 4817.

[12] Silva, R. S., & de Moraes, L. F. (2019). A cooperative approach with improved performance for global intrusion detection systems for internet service providers. Annals of Telecommunications, 74(3-4), 167-173.

[13] Silva, R. S., & Macedo, E. L. (2017, October). A cooperative approach for a global intrusion detection system for internet service providers. In 2017 1st cybersecurity in networking conference (CSNet) (pp. 1-8). IEEE.

[14] Choi, Y. B., & Allison, G. D. (2017). Intrusion Prevention And Detection In Small To Medium-Sized Enterprises. In SAIS 2017 Proceedings.

[15] Soewito, B., & Andhika, C. E. (2019, August). Next-generation firewall for improving security in company and IoT network. In 2019 International Seminar on Intelligent Technology and Its Applications (ISITIA) (pp. 205-209). IEEE.

[16] S.C. Tharaka, R.L.C. Silva, S. Sharmila, S.U.I. Silva, K.L.D.N. Liyanage, A.A.T.K.K. Amarasinghe, D. Dhammearatchi. (2016, April). High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies. International Journal of Scientific and Research Publications, Volume 6, Issue 4, pg. 504-508,April 2016, ISSN 2250-3153.

[17] Neupane, K., Rami, H., Lei, C., (2018). Next Generation Firewall for Network Security: A Survey. IEEE Access, 978-15386-6133-18.

[18] Barker, Keith., Scott Morris dan Kevin Wallace, CCNA Security 640-554, 2012.

[19] P. Oppenheimer and T.-D. N. Design, "Cisco Press," ISBN, vol. 1, pp. 57069-57870, 2011.