Journal of Artificial Intelligence and Engineering Applications

Website: https://ioinformatic.org/

15th October 2025. Vol. 5. No. 1; e-ISSN: 2808-4519

Design and Implementation of Network Security Using Fortinet Firewall at the Communication and Information Service of Central Lombok Regency

Muhammad Azami[1]*, I Putu Haryadi[2], Husain[3]

[1,2,3]Fakultas Teknik,· Bumigora University
muhammadamiy07@gmail.com[1*]

Abstract

In an increasingly complex digital era, government agencies such as the Communication and Information Service (Diskominfo) of Central Lombok Regency face serious challenges related to network security. This research aims to design and implement a Fortinet FortiGate firewall-based network security system, in order to detect and address cyber threats that have the potential to disrupt operations and public services. The method used is *the Network Development Life Cycle* (NDLC), which includes the stages of analysis, design, simulation, implementation, monitoring, and management. The system was tested using common attack scenarios such as *PortSscanning* and *Denial of Service* (DoS) with the help of tools such as *nmap, sqlmap* and *hping3*. The results show that the implementation of FortiGate, including features such as *Web Application Firewall* (WAF), *Intrusion Prevention System* (IPS) and *Antivirus*, is able to provide comprehensive protection and real-time response to threats. This study also shows that the Fortigate-based network security system is able to significantly improve the network security posture of the Communication and Information Service (Diskominfo) of Central Lombok Regency. This system provides multi-layered, reliable, and easy-to-manage protection, and is an important foundation in maintaining the sustainability of local government digital services.

Keywords*: Network Security, Fortinet Fortigate Firewall, WAF, IPS, Antivirus*

1. Introduction

The Central Lombok Communication and Information Service (Diskominfo) is a government agency that has an important role in information management and technology development. In addition, it also acts as a liaison between the government, the community and various other sectors through the use of information and communication technology. Currently, the Central Lombok Diskominfo has a local network connected to *Internet* Through *Internet Service Provider (ISP) Hypernet* with a speed of 650 Mbps. In addition, it has taken advantage of virtualization-based technology *VMWare* to manage *server* virtually, i.e. in the form of *Virtual Machine (VM)*. A computer network is a set of "interconnections" between two computers *autonomous* or more connected to wired or cordless transmission media (*wireless*) [1]. A computer network is a system consisting of computers that are designed to be able to share resources (printers, CPUs), communicate *(surel*, instant messaging), and can access information (browser *web*). The purpose of a computer network is to be able to request and provide services (*service)*, so that the party who requests/receives the service is called *client* and those who provide/send services are called *server* [2].

Fortinet is a network security service provider or *network security* was among the majority of the global fortune 100 companies in 2009 and is the security mainstay of many large companies. In addition, Fortinet also provides Solutions *smart security* without borders that aim to meet a high level of security and meet the needs of Fortinet users. Fortigate as a device, is responsible for ensuring the overall security of the network and acts as a gateway and router for LAN networks, so it does not require additional routers or load balancing devices if there is more than one WAN connection [3].

Web Application Firewall (WAF) acts as a shield between the user and the web application, where any incoming HTTP request is first examined against a set of security rules before being forwarded to the application. If the request is detected to contain an attack pattern such as *SQL Injection, Cross Site Scripting (XSS), Remote File Inclusion*, *or Command Injection*, then the WAF will automatically block the request, issue an alert, or log it in the log for further analysis. One of the main advantages of WAF is its ability to protect running systems without having to modify application code, making it an ideal solution for agencies or organizations that have limited development resources [4]. *Intrusion Prevention System* (IPS) is a network security system designed to actively detect and prevent cyberattacks before they can damage systems or steal data. IPS works by monitoring network traffic in real-time, analyzing each incoming and outgoing data packet, and identifying suspicious attack patterns based on database signatures, anomalous behavior, or predefined policies. IPS acts as an active layer of protection that is able to stop attacks in real-time, such as DDoS attacks, *exploit* against security loopholes (*vulnerability*), malware intrusion, as well as application-based attacks such as *SQL injection* or *cross-site scripting* (XSS). In addition, social studies also performs a recording function *(logging)*) for any incidents, notify administrators, and support stricter security policies in network systems [5]. *Antivirus* is security software designed to detect, prevent, and remove malicious software (*Malware*) from a computer system or network. *Antivirus* Acting as the first line of defense in the system *endpoint* (such as a computer, laptop, or server) to ensure that no malicious programs infect, steal, or corrupt important data. Moreover *Antivirus* It also provides real-time protection that continuously monitors system activity and network traffic to detect suspicious behavior [6].

This research aims to design and implement a Fortigate-based network security system at the Communication and Information Office of Central Lombok Regency as a preventive and responsive effort to various forms of cyber threats. The main objective of this research is to build a reliable network security system, by utilizing the advanced features of firewalls such as *Web Application firewall* (WAF), *Intrusion Prevention System* (IPS) and *Antivirus*. In addition, this study aims to test the effectiveness of the system through simulated cyberattacks such as *SQL Injection, port scanning*, and *Denial of Service* (Dos), with the help of tools such as *nmap, sqlmap* and *hping3* to see the extent to which firewalls can detect and handle threats automatically.

2. Research Method

The research method used in this study is the Network Development Life Cycle (NDLC) approach, a network system development model designed to facilitate the comprehensive and structured planning, design, and implementation of network security systems. NDLC consists of six main stages, namely Analysis, Design, Simulation, Implementation, Monitoring, and Management

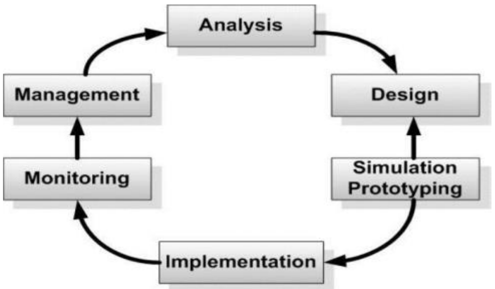


Fig 1: NDLC Method [7]

2.1. Stages of Analysis

The Analysis stage is the initial stage in which researchers analyze problems that arise, analyze user needs, and analyze network topology.

1. Stages of Data Collection
   The data collection methods used by the author in this thesis research are:
   a. Literature Studies, before raising the topic of this research, the author has conducted a literature study with various previous studies.
   b. Interviews are conducted with related parties involving the upper management structure down to the lower level/operator in order to obtain concrete and complete data.
   c. Observation, collecting data where the author collects data by direct observation on the object being studied.
   In addition, the author also conducts collection through the old network topology or before the fortigate firewall was implemented. The network topology before the fortigate firewall was implemented at the Central Lombok Communication and Information Service (Diskominfo) can be seen in figure 2

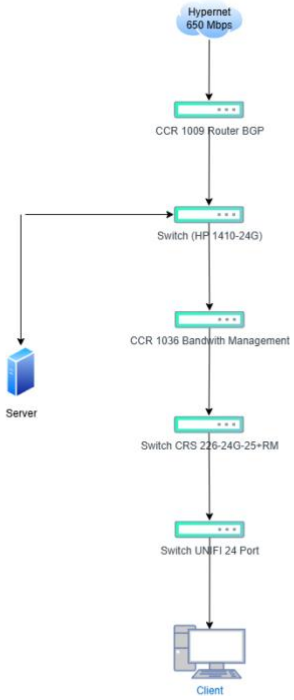


Fig. 2: Old Network Topology

Figure 2 shows the topology of the internet network starting from the main internet connection with a speed of 650 Mbps from Hypernet that enters the CCR 1009 MicroTik Router device configured using BGP (Border Gateway Protocol). From this router, the network is continued to the HP 1410-24G Switch, which serves as an initial distribution to other devices including the internal server. Servers connect directly to these switches to support on-premises services such as data storage or internal applications. Furthermore, the connection is forwarded to the CCR 1036 MicroTik Router which plays a role in bandwidth management, regulating and dividing network capacity to keep usage efficient. From there, the network is passed to the CRS 226-24G-25+RM MicroTik Switch, which is a smart switch for advanced distribution. Finally, the network gets to the UNIFI 24 Port Switch, which shares the connection with the clients, i.e. the user's computer in the network environment. This topology describes a well-organized network infrastructure, from internet service providers, network traffic management, to distribution to end users.

2. Data Analysis

The data analysis in this study was carried out qualitatively by observing that before using the Fortinet network security system, the network condition at Diskominfo still relies on manual security that is not able to detect threats automatically. This has resulted in several cyber incidents, including illegal access to online gambling sites that interfere with the institution's official services. The impact is felt directly by employees who have difficulty accessing the official website, so that work productivity decreases. In response to these issues, Fortinet's FortiGate began to be implemented from early 2024 using FortiGate 80F devices. The system is equipped with key features such as *Web Application Firewall* (WAF), *Intrusion Prevention System* (IPS), and *Antivirus*. These three features play an important role in automatically detecting and blocking various cyberattacks. The need for a network security system is considered very large because almost all public and internal services in Diskominfo have been digitized. Although integration with external monitoring systems has not been fully implemented, the current system is considered to be very adequate for internal operational needs.

Previous studies have generally highlighted the importance of implementing network security systems in various institutions, both government, educational, and private sector institutions. One trend that looks consistent is the use of *Next Generation Firewall* (NGF) technology such as Fortinet FortiGate which is able to integrate advanced security features such as *Intrusion Prevention System* (IPS), *Web Filtering, Antivirus*, and *Application Control* in one system. In addition, previous research shows that Fortinet's technology has been widely adopted with various approaches, both for access management, attack prevention, and network traffic efficiency. So the difference with what the author researched lies in a *comprehensive* and *empirical* approach, because in addition to designing and implementing, direct simulations of various types of cyber attacks are also carried out, such as *SQL injection, port scanning*, and *Denial of Servive* (DoS). This shows that the designed system is not only theoretical or preventive, but also capable of responding to real attacks automatically and adaptively.

2.2. Design Stage

This design stage will be carried out to design the topology design drawings of the interconnection network to be built. The design can be in the form of a topological structure, data access, wiring layout that will provide a clear picture of the project to be built.

1. Network Design

Here the author makes a network design at the Communication and Information Service (Diskominfo) of Central Lombok Regency, to ensure that all devices can connect and communicate optimally, support the application system used, and be protected from cyber threats. The network design can be seen in figure 3.

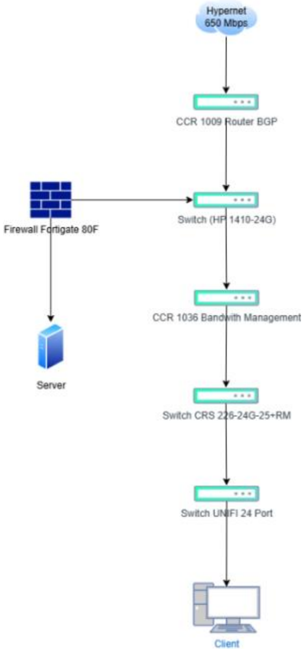


Fig. 3: Network Design

In figure 3, it illustrates the network topology of the Central Lombok Regency Diskominfo after the implementation of a security system using the FortiGate 80F firewall. The main internet connection comes from the Hypernet service provider with a speed of 650 Mbps, which first enters through a CCR 1009 router device configured using the Border Gateway Protocol (BGP) to manage the data traffic route. From the router, the network is forwarded to the HP 1410-24G switch which serves as the initial link and the main distribution point to the various network devices below. One of the important connections of this switch is to the FortiGate 80F firewall, which then connects directly to the internal server. The FortiGate 80F firewall acts as the network's main layer of defense, filtering and securing all incoming and outgoing data traffic. Any request that wants to access the server must first pass through this firewall, so that only legitimate and unsuspicious traffic is allowed. The internal server stores various important systems such as public information, personnel systems, and village websites. On the other main line, traffic is forwarded from the HP switch to CCR 1036, a bandwidth management device that is in charge of dividing and controlling the distribution of internet capacity to all network users to keep it efficient. Next, the data is forwarded to the CRS 226-24G-25+RM switch which serves to distribute the connection to the next switch, which is the UNIFI 24 Port, which then connects the network to the client computer in the work environment. This topological structure demonstrates a layered security (defense in depth) and systematic and efficient network management, with a combination of traffic regulation, separation of server access points, and protection from cyberattacks through the FortiGate firewall.

After the *implementation of the FortiGate firewall*, it shows a significant improvement in the security aspect of the network. The addition of *a firewall* component between *the router* and *the server* is an important step in strengthening the network's security posture. *Firewalls* function as gatekeepers that filter incoming and outgoing traffic, and can block suspicious access, filter based on IP, port, protocol, and detect attacks such as *SQL Injection*, *Denial of Service* (*Dos), Port Scanning*, and others.

2. System Design

   The design of the network security system at the Communication and Information Service of Central Lombok Regency has the main goal, namely to improve the security of information technology infrastructure as a whole. This system is designed to provide protection against various forms of cyber attacks that can disrupt public services, damage data, and threaten the continuity of organizational operations. The topology used in the test consists of three main elements: *the attacker client, the FortiGate firewall*, and the internal server of Diskominfo, as seen in figure 4.

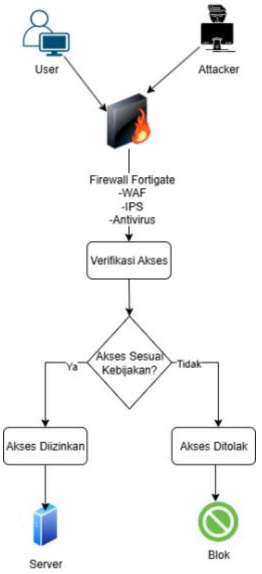


Fig 4: System Design

In figure 4, the flow starts from two directions from the source of the access request, namely the Attacker fund user. Each incoming access request will first go through a security system consisting of the Fortigate Firewall, which is equipped with *a Web Application Firewall* (WAF), *Intrusion Prevention System* (IPS), and *Antivirus*. These three features work together to *analyze and verify* whether the traffic is safe and in accordance with applicable policies. Next, the process enters the access verification stage. At this stage, the system will check if the access request complies with the security policies that have been configured in the firewall. If the request is appropriate, access will be allowed and forwarded to the server as a legitimate service. However, if the request does not match, the system will automatically reject and block such access as an attempt to mitigate the attack, for example from a suspicious IP or the type of traffic indicated as a threat.

2.3. Tahap Simulation Prototyping

This stage is to test and see the initial performance of the network to be built and as a percentage material and sharing with other work teams, but due to the limitations of the device only using tools to build the topology to be designed. In this study, the simulation was carried out by building a test network that resembles the network infrastructure of the Central Lombok Regency Communication and Information Office. *The network prototype* was built using a combination of hardware and virtual, involving key components such as FortiGate (both physical and virtual devices), web servers (targets), PC admins (system managers), and Kali Linux-based attacker devices.

At this stage, network security testing is also carried out by simulating several types of attacks to measure the effectiveness of firewalls in detecting and preventing these threats. The types of attacks that will be attempted on network security systems include:

1. Port Scanning with Nmap, this test is carried out to test whether suricata can detect port scanning activities that aim to find security gaps in the network.
2. Sql Injection with *Sqlmap, Sqlmap* works by sending various SQL payloads to the target *server* and monitoring the responses provided. If *the server* responds abnormally or returns database information, then the application is considered vulnerable to SQL injection. However, if the connection is rejected, a timeout occurs, or no exploitable parameters are found, then it can be concluded that the system has an effective defense mechanism.
3. Denial of Service with hping3, this test aims to find out how *FortiGate* responds to an attack that aims to disable the service by sending a large amount of network traffic at the same time.

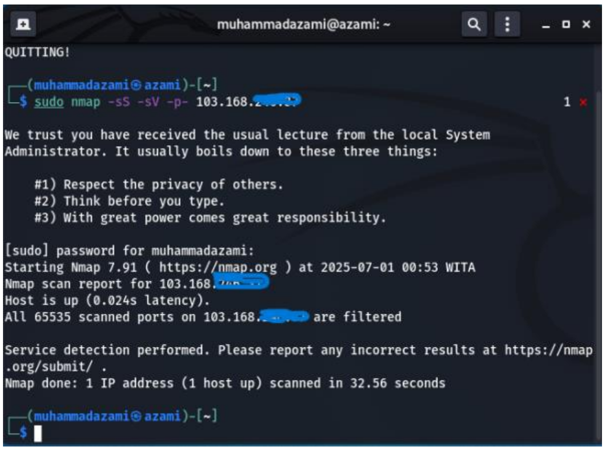
3. Results and Discussion

3.1 System Test Results

The results of the test of the applied network security system show that Fortinet's Fortigate-based defense mechanism is able to carry out its function effectively in distinguishing legal access from cyberattacks. The test is repeated for each of the three times of each attack, with two main scenarios: access from a *legal user* and an attack from an unauthorized party (*attacker*). During testing as *an attacker*, several types of attacks such as *port scanning* using *Nmap, SQL Injection* via *SQLMap*, and *Hping3* Denial of Service *(DoS) attacks* are launched on the server. As a result, FortiGate was able to detect all of these attacks accurately. On the other hand, when the test is carried out by a legitimate internal user *(legal user*), such as an employee of the Communication and Informatics Service who accesses the internal web application and email services, the system does not show any restrictions that hinder productivity. FortiGate allows traffic from internal IPs that have been configured as long as access is made in accordance with *predefined* rules.

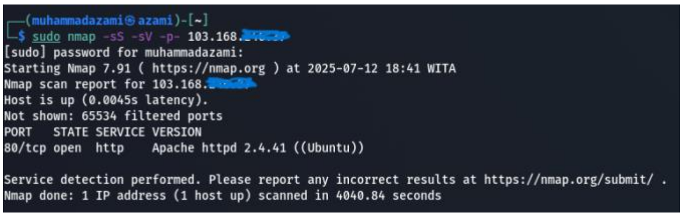
3.2 Security Test Results

1. Port Scanning Attack Testing (nmap)



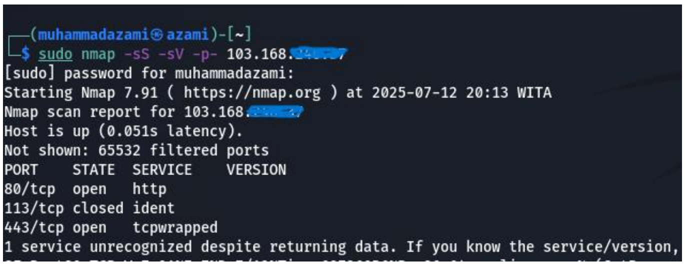
```
QUITTING!

┌──(muhammadazami㉿azami)-[~]
└─$ sudo nmap -sS -sV -p- 103.168.[redacted]                          1 ✗

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for muhammadazami:
Starting Nmap 7.91 ( https://nmap.org ) at 2025-07-01 00:53 WITA
Nmap scan report for 103.168.[redacted]
Host is up (0.024s latency).
All 65535 scanned ports on 103.168.[redacted] are filtered

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.56 seconds

┌──(muhammadazami㉿azami)-[~]
└─$ █
```

Fig. 5: First Test Results



```
┌──(muhammadazami㉿azami)-[~]
└─$ sudo nmap -sS -sV -p- 103.168.[redacted]
[sudo] password for muhammadazami:
Starting Nmap 7.91 ( https://nmap.org ) at 2025-07-12 18:41 WITA
Nmap scan report for 103.168.[redacted]
Host is up (0.0045s latency).
Not shown: 65534 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4040.84 seconds
```

Fig. 6: Second Test Results



```
┌──(muhammadazami㉿azami)-[~]
└─$ sudo nmap -sS -sV -p- 103.168.[redacted]
[sudo] password for muhammadazami:
Starting Nmap 7.91 ( https://nmap.org ) at 2025-07-12 20:13 WITA
Nmap scan report for 103.168.[redacted]
Host is up (0.051s latency).
Not shown: 65532 filtered ports
PORT    STATE  SERVICE    VERSION
80/tcp  open   http
113/tcp closed ident
443/tcp open   tcpwrapped
1 service unrecognized despite returning data. If you know the service/version,
```

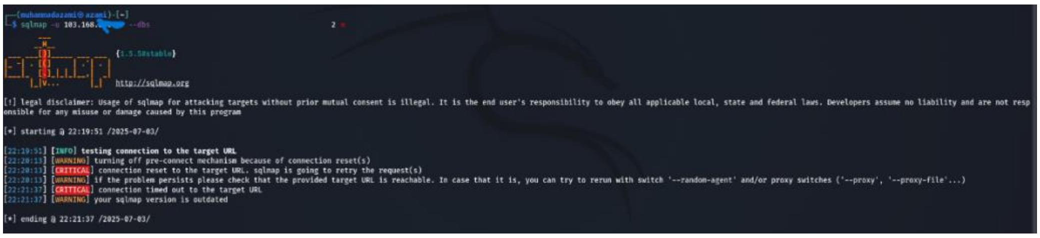
Fig. 7: Results of the Third Test

So after performing three port scanning attack tests, it can be concluded that there is one port that is open, namely port 80/tcp, and it shows port 113/tcp in a closed state and port 443/tcp appears as tcpwrapped which indicates that the system refuses further checks on that port. So that as many as 65534 other ports were detected in a "*filtered*" state, which indicates that the firewall or network security system has arranged that these ports do not respond to requests from outside, thus increasing system security. This indicates that the target system has been configured with a fairly good level of security, opening only the necessary ports and closing or filtering other ports to minimize the risk of outside attacks.

Table. 1: Port Scanning Attack Test Results

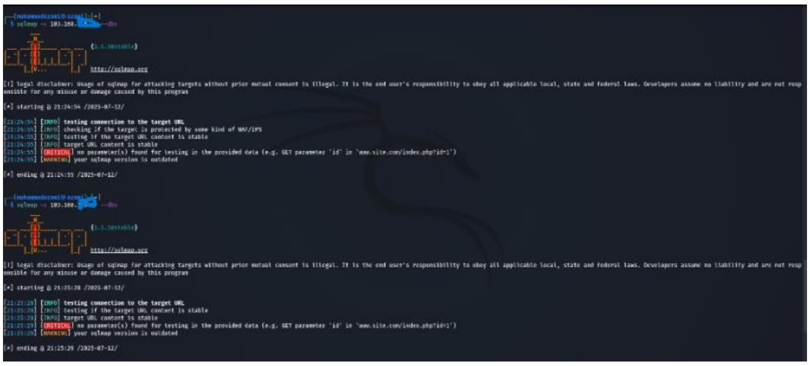
Yes	Types of Attacks	Tools Used	Parameter	Result	Information
1	Port Scanning	Nmap	Nmap -sS -sV -p- 103.168.*.*	All ports are *filtered*. No open ports were detected.	The system successfully blocked access.
2	Port Scanning	Nmap	Nmap -sS -sV -p- 103.168.*.*	Port 80/tcp	running HTTP services using *Apache* version 2.4.41 on *the Ubuntu* operating system.
3	Port Scanning	Nmap	Nmap -sS -sV -p- 103.168.*.*	Port 113/tcp dan port 443/tcp	Displayed port 113/TCP in the *closed* state and port 443/TCP appears as *TCPWRAPPED* indicating that the system declined further checks on that port,

2. Sql Injection Attack Testing (sqlmap)



```
┌──(muhammadazami㉿azami)-[~]
└─$ sqlmap -u 103.168.[redacted] --dbs                                2 ✘

                 {1.5.5#stable}

                 http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not resp
onsible for any misuse or damage caused by this program

[*] starting @ 22:19:51 /2025-07-03/

[22:19:51] [INFO] testing connection to the target URL
[22:20:13] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[22:20:13] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the request(s)
[22:20:13] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switches ('--proxy', '--proxy-file'...)
[22:21:37] [CRITICAL] connection timed out to the target URL
[22:21:37] [WARNING] your sqlmap version is outdated

[*] ending @ 22:21:37 /2025-07-03/
```

Fig. 8: First Test Results



```
┌──(muhammadazami㉿azam[redacted])-[~]
└─$ sqlmap -u 103.168.[redacted] --dbs

                 {1.5.5#stable}

                 http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not resp
onsible for any misuse or damage caused by this program

[*] starting @ 21:24:54 /2025-07-12/

[21:24:54] [INFO] testing connection to the target URL
[21:24:55] [INFO] checking if the target is protected by some kind of WAF/IPS
[21:24:55] [INFO] testing if the target URL content is stable
[21:24:55] [INFO] target URL content is stable
[21:24:55] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1')
[21:24:55] [WARNING] your sqlmap version is outdated

[*] ending @ 21:24:55 /2025-07-12/

┌──(muhammadazami㉿azam[redacted]
└─$ sqlmap -u 103.168.[redacted] --dbs

                 {1.5.5#stable}

                 http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not resp
onsible for any misuse or damage caused by this program

[*] starting @ 21:25:28 /2025-07-12/

[21:25:28] [INFO] testing connection to the target URL
[21:25:29] [INFO] testing if the target URL content is stable
[21:25:29] [INFO] target URL content is stable
[21:25:29] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1')
[21:25:29] [WARNING] your sqlmap version is outdated

[*] ending @ 21:25:29 /2025-07-12/
```

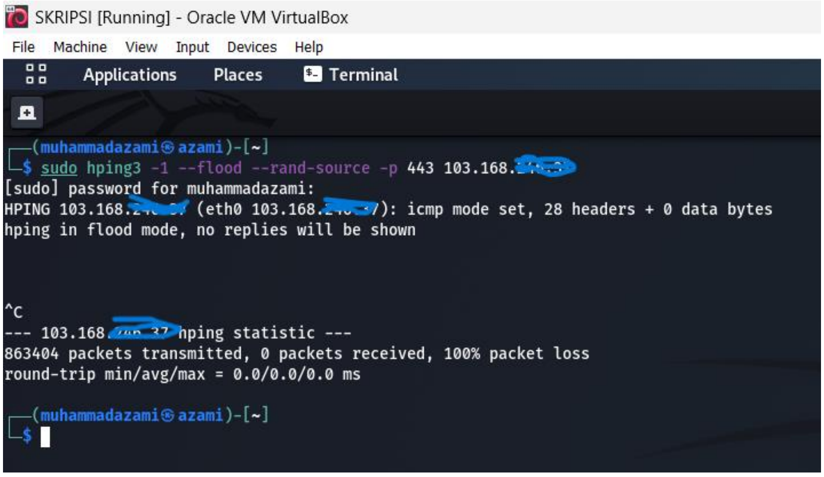
Fig. 9: Second and Third Test Results

After performing the test, the result displayed is that *the SQLMap* process fails to detect parameters that can be used for SQL Injection testing. It says *[CRITICAL] no parameter(s) found for testing,* which means the URL given doesn't have a parameter (e.g. ?id=1) that is typically used as an entry point for SQL Injection attacks. Because no GET or POST parameters were detected, SQLMap was unable to proceed with the testing process.

Table. 2: Sql Injection Attack Test Results

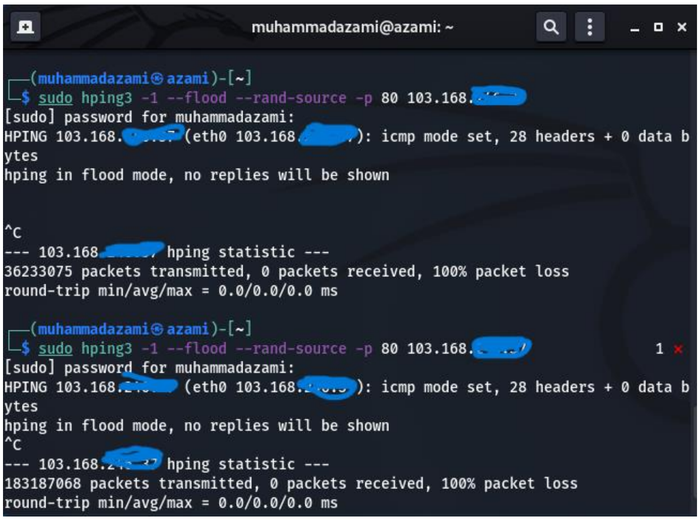
Yes	Types of Attacks	Tools Used	Parameter	Result	Information
1	Sql Injection	Sqlmap	sqlmap -u 103.168.*.* --dbs	The connection is *reset*, *timeout*. No exploitable parameters were found.	The system successfully detects and blocks SQLi attacks with WAF.
2	Sql Injection	Sqlmap	sqlmap -u 103.168.*.* --dbs	*[CRITICAL] no parameter(s) found for testing,*	*SQLMap* fails to detect the
3	Sql Injection	Sqlmap	sqlmap -u 103.168.*.* --dbs	*[CRITICAL] no parameter(s) found for testing,*	*SQLMap* fails to detect the

3. Testing Denial of Service Attacks (pping3)


SKRIPSI [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal

```
┌──(muhammadazami㉿azami)-[~]
└─$ sudo hping3 -1 --flood --rand-source -p 443 103.168.[redacted]
[sudo] password for muhammadazami:
HPING 103.168.[redacted] (eth0 103.168.[redacted]): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown


^C
--- 103.168.[redacted] hping statistic ---
863404 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(muhammadazami㉿azami)-[~]
└─$ █
```

Fig. 10: First Test Results



```
┌──(muhammadazami㉿azami)-[~]
└─$ sudo hping3 -1 --flood --rand-source -p 80 103.168.[redacted]
[sudo] password for muhammadazami:
HPING 103.168.[redacted] (eth0 103.168.[redacted]): icmp mode set, 28 headers + 0 data b
ytes
hping in flood mode, no replies will be shown

^C
--- 103.168.[redacted] hping statistic ---
36233075 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(muhammadazami㉿azami)-[~]
└─$ sudo hping3 -1 --flood --rand-source -p 80 103.168.[redacted]                1 ✕
[sudo] password for muhammadazami:
HPING 103.168.[redacted] (eth0 103.168.[redacted]): icmp mode set, 28 headers + 0 data b
ytes
hping in flood mode, no replies will be shown
^C
--- 103.168.[redacted] hping statistic ---
183187068 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

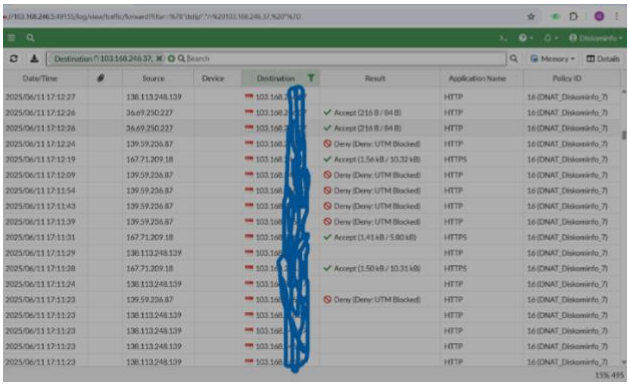
Fig. 11: Second and Third Test Results

Furthermore, the attack test scenario that the author carried out is a simulation of a Denial of Service (*DoS*) attack, this attack works by flooding the target with large *requests* or traffic, thus causing the target resources such as cpu, ram, or available services to be burdened with *requests* that flood the target. To carry out *a DoS* attack, the author uses *a Kali Linux tool* called "h*ping3", hping3 is one* of the *tools* that functions to carry out denial of service attacks.

Table 3: Results of Denial of Service (DOS) Attack Trials

Yes	Types of Attacks	Tools Used	Parameter	Result	Information
1	*Denial of Service*	*Hping3*	sudo hping3 -1 --flood --rand-source -p 443 103.168.*.*	Simulations show massive ICMP packet delivery. The system is able to withstand excessive traffic load and does not respond at all	Security systems successfully prevent or ignore such attacks.
2	*Denial of Service*	*Haping3*	sudo hping3 -1 --flood --rand-source -p 443 103.168.*.*	Simulations show massive ICMP packet delivery. The system is able to withstand excessive traffic load and does not respond at all	Security systems successfully prevent or ignore such attacks.
3	*Denial of Service*	*Hping3*	sudo hping3 -1 --flood --rand-source -p 443 103.168.*.*	Simulations show massive ICMP packet delivery. The system is able to withstand excessive traffic load and does not respond at all	Security systems successfully prevent or ignore such attacks.

3.3 Log Results on Fortigate



//103.168.246.5:49155/log/view/traffic/forward?filter=%7B"dstip":"=%20103.168.246.37,%20"%7D

Diskominfo

Destination ∩ 103.168.246.37, ✖ Search | Memory | Details

Date/Time		Source	Device	Destination	Result	Application Name	Policy ID
2025/06/11 17:12:27		138.113.248.139		103.168.[redacted]		HTTP	16 (DNAT_Diskominfo_7)
2025/06/11 17:12:26		36.69.250.227		103.168.[redacted]	✓ Accept (216 B / 84 B)	HTTP	16 (DNAT_Diskominfo_7)
2025/06/11 17:12:26		36.69.250.227		103.168.[redacted]	✓ Accept (216 B / 84 B)	HTTP	16 (DNAT_Diskominfo_7)
2025/06/11 17:12:24		139.59.236.87		103.168.[redacted]	⊘ Deny (Deny: UTM Blocked)	HTTP	16 (DNAT_Diskominfo_7)
2025/06/11 17:12:19		167.71.209.18		103.168.[redacted]	✓ Accept (1.56 kB / 10.32 kB)	HTTPS	16 (DNAT_Diskominfo_7)
2025/06/11 17:12:09		139.59.236.87		103.168.[redacted]	⊘ Deny (Deny: UTM Blocked)	HTTP	16 (DNAT_Diskominfo_7)
2025/06/11 17:11:54		139.59.236.87		103.168[redacted]	⊘ Deny (Deny: UTM Blocked)	HTTP	16 (DNAT_Diskominfo_7)
2025/06/11 17:11:43		139.59.236.87		103.168[redacted]	⊘ Deny (Deny: UTM Blocked)	HTTP	16 (DNAT_Diskominfo_7)
2025/06/11 17:11:39		139.59.236.87		103.168[redacted]	⊘ Deny (Deny: UTM Blocked)	HTTP	16 (DNAT_Diskominfo_7)
2025/06/11 17:11:31		167.71.209.18		103.168[redacted]	✓ Accept (1.41 kB / 5.80 kB)	HTTPS	16 (DNAT_Diskominfo_7)
2025/06/11 17:11:29		138.113.248.139		103.16[redacted]		HTTP	16 (DNAT_Diskominfo_7)
2025/06/11 17:11:28		167.71.209.18		103.16[redacted]	✓ Accept (1.50 kB / 10.31 kB)	HTTPS	16 (DNAT_Diskominfo_7)
2025/06/11 17:11:24		138.113.248.139		103.16[redacted]		HTTP	16 (DNAT_Diskominfo_7)
2025/06/11 17:11:23		139.59.236.87		103.16[redacted]	⊘ Deny (Deny: UTM Blocked)	HTTP	16 (DNAT_Diskominfo_7)
2025/06/11 17:11:23		138.113.248.139		103.168.[redacted]		HTTP	16 (DNAT_Diskominfo_7)
2025/06/11 17:11:23		138.113.248.139		103.168.[redacted]		HTTP	16 (DNAT_Diskominfo_7)
2025/06/11 17:11:23		138.113.248.139		103.168.[redacted]		HTTP	16 (DNAT_Diskominfo_7)
2025/06/11 17:11:23		138.113.248.139		103.168.[redacted]		HTTP	16 (DNAT_Diskominfo_7)

15% 495

Fig. 12: Log Results on Fortigate

Figure 12 shows network traffic log data filtered by *IP destination* 103.168.*.*. This data records all attempted access from various IP sources to a predetermined destination server, including the results of the security system's actions on that traffic. It is seen that FortiGate performs the identification and decision-making of each access request. Some IP addresses try to access the destination server via the HTTP or HTTPS protocol. The system then responds to these requests with two types of actions: *Accept* or *Deny* (*Blocked*). This rejection indicates that FortiGate's system successfully detects potential threats, such as suspicious traffic or attacks, and then blocks that access automatically. In addition, it is also seen that all system actions are performed under a firewall policy with ID 16 (DNAT_Diskominfo_7), which indicates that all traffic to IP 103.168.*.* is routed through a specific NAT policy configured for security and monitoring purposes. Legal activity such as from IP 167.71.209.18 or 136.69.250.227 is still accepted, with a recorded data size (byte), indicating legitimate traffic. While suspicious requests from IPs are consistently rejected. This proves that the FortiGate system is able to carry out access detection, prevention, and control functions based on the security profile that has been compiled, as well as support audits through clear and detailed logs.

4. Conclusion

Based on the results of the research conducted and the results of the tests that have been carried out, it can be concluded that the network security system designed and implemented using the Fortinet FortiGate device is able to provide protection against cyber threats that have the potential to disrupt the stability and integrity of the information system at the Communication and Information Service (Diskominfo) of Central Lombok Regency, such as *Sql Injection, Port Scanning* and *Denial of Service* (Two). This research has gone through systematic stages ranging from analyzing security needs, designing network topology, configuring firewall devices, to testing systems against simulated attacks such as *port scanning*, *SQL injection*, and *denial of service (DoS).* The test results prove that the system successfully detects, blocks, and responds to these threats effectively. The results of this study also show that the implementation of *Fortinet*'s network security technology is not only able to improve the reliability and stability of data communication infrastructure, but also strengthens the cybersecurity posture of government organizations such as the Communication and Information Office (Diskominfo) of Central Lombok Regency. The system also provides convenience for network administrators to monitor and manage incidents centrally and in real-time, so that responses to threats can be carried out quickly and efficiently. Thus, this system is worthy of being used as a model for strengthening network security in other local government agencies that face similar challenges in facing the digital era and increasing cyber threats.

References

[1] S. Aryanti, Khairil, and H. Aspriyono, "Development of a Mikrotik-Based Wifi Network Security System Using the Network Development Life Cycle (NDLC) Method," *Engineering*, vol. 17, no. 2, pp. 88–95, 2023, doi: 10.33369/teknosia.v17i2.31582.

[2] Nanang Sadikin & Mukhlis, "Implementation of Computer Network Security for Internet Access Using Key Security," *Information*, vol. 6, no. 1, pp. 20–27, 2020, [Online]. Available: https://maklumatika.i-tech.ac.id/index.php/maklumatika/article/view/77%0Ahttps://maklumatika.i-tech.ac.id/index.php/maklumatika/article/download/77/85

[3] F. R. Arbie and M. Raharjo, "Implementation of Network Security with the Security Profiles Method using Fortigate at the State Civil Apparatus Commission," *J. Inform. Terpadu*, vol. 10, no. 1, pp. 27–34, 2024, doi: 10.54914/jit.v10i1.1060.

[4] M. Annas, R. T. Adek, and Y. Afrillia, “Web Application Firewall (WAF) Design to Detect and Anticipate Hacking in Web-Based Applications,” *J. Adv. Comput. Knowl. Algorithms*, vol. 1, no. 3, pp. 52–58, 2024, doi: 10.29103/jacka.v1i3.16315.

[5] E. Dwi Setiawan, Ridwansyah, and M. Raharjo, "Designing Next-Generation Firewall Network Security Using Fortinet Routers at Pt. Alodokter Teknologi Solusi," *J. Inform. Terpadu*, vol. 9, no. 1, pp. 34–39, 2023, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[6] A. Riduan and N. Sadikin, "Firewall Design Using Fortigate at PT Swadharma Duta Data," *J. Information*, vol. 8, no. 1, pp. 90–98, 2021, [Online]. Available: https://maklumatika.i-tech.ac.id/index.php/maklumatika/article/view/122

[7] D. Prima Jaya, H. Aspriyono, and E. Suryana, "Implementation of Computer Network Security Using Fortigate as a Firewall at the Computer Lab of IAIN Bengkulu," *Gatotkaca J.*, vol. 2, no. 1, pp. 31–38, 2021, [Online]. Available: https://doi.org/10.37638/gatotkaca.2.1.31-38

[8] N. Bayu and A. Susila, "Application of Fortigate Technology in the Development of SSL-VPN-Based VPN Networks (Case Study: Ministry of PANRB)," *Log. J. Computing Science. and Educators.*, vol. 2, no. 1, pp. 153–159, 2023, [Online]. Available: https://journal.mediapublikasi.id/index.php/logic/article/view/2899

[9] N. Sadikin and M. Sari, "Implementation of Password Policy on Domain Security Policy Group Policy Object (GPO) of Active Directory Domain Services for Network Security in Windows Server," *J. Information*, vol. 10, no. 1, pp. 1–9, 2023, [Online]. Available: https://maklumatika.i-tech.ac.id/index.php/maklumatika/article/view/152

[10] A. T. Laksono and M. A. H. Nasution, "Implementation of Local Area Network Computer Network Security Using Access Control List in Company X," *J. Sist. Computer. and Inform.*, vol. 1, no. 2, p. 83, 2020, doi: 10.30865/json.v1i2.1920.

[11] F. P. Eka Putra, Amir Hamzah, W. Agel, and R. O. Firmansyah Kusuma, "Implementation of Mikrotik Network Security System Using Firewall Filtering and Port Knocking," *J. Inf. and Technology System.*, vol. 5, no. 4, pp. 82–87, 2024, doi: 10.60083/jsisfotek.v5i4.329.

[12] A. E. Syaputra *et al.*, *Computer Network Security*. 2025. [Online]. Available: https://repository.sadapenerbit.com/index.php/books/catalog/book/235

[13] D. Wicaksono, "Network Security System Firewall Using Firewall with Port Blocking and Firewall Filtering Methods," *JATISI (Tek Journal. Inform. and Sist. Information)*, vol. 9, no. 2, pp. 1380–1392, 2022, doi: 10.35957/jatisi.v9i2.2103.

[14] J. Education and M. Efendi, "Available online EISSN: 2502-471X DEVELOPMENT OF CISCO'S SIMULATION-BASED NETWORK SECURITY SYSTEM MODULE," pp. 399–408, 2016.

[15] N. Sadikin, "Implementation of Security Control on Information Technology Infrastructure to Prevent and Overcome Ransomware Malware for Enterprise Information Security," *J. Information*, vol. 10, no. 2, pp. 77–86, 2023, [Online]. Available: https://maklumatika.i-tech.ac.id/index.php/maklumatika/article/view/234

[16] R. Hendrawan, L. Widyawati, and O. Asroni, "Implementation of Multihomed Firewall Based on IDS and DMZ Technology Using PfSense," *J. Artif. Intell. Eng. Appl.*, vol. 4, no. 3, pp. 1823–1828, 2025, doi:10.59934/jaiea.v4i3.1028.

[17] S. Dewi, "Network Security Using VPN (Virtual Private Network) with PPTP (Point to Point Tunneling Protocol) Method at the Kertaraharja Ciamis Village Office," *EVOLUTION J. Science and Management.*, vol. 8, no. 1, pp. 128–139, 2020, doi: 10.31294/evolution.v8i1.7658.

[18] G. H. A. Kusuma, "Designing a Web Server Network Security System Scheme using Web Application Firewall and Fortigate to Prevent Data Leaks during the Covid-19 Pandemic," *J. Informatics Adv. ...*, vol. 2, no. 2, pp. 1–4, 2021, [Online]. Available: http://journal.univpancasila.ac.id/index.php/jiac/article/view/3259

[19] S. Parulian, D. A. Pratiwi, and M. Cahya Yustina, "Threats and Solutions to Cyber Attacks in Indonesia," *Telecommun. Networks, Electron. Comput. Technol.*, vol. 1, no. 2, pp. 85–92, 2021, [Online]. Available: http://ejournal.upi.edu/index.php/TELNECT/

[20] R. Yulianto and F. Aprilyani, "Computer Network Security System Using NDLC Method with Linux Zentyal at the Coordinating Ministry for Maritime Affairs," *J. Tek. Inform. Inter-National Statistics*, vol. VI, no. 2, pp. 79–86, 2020.

[21] Y. Mulyanto, E. S. Susanto, M. I. Akbar, and F. Idifitriani, "Computer Network Security Analysis Using Intrusion Detection System (IDS) and Firewall Methods," *Digit. Transform. Technol.*, vol. 3, no. 2, pp. 864–870, 2024, doi: 10.47709/digitech.v3i2.3402.

[22] K. Aziz, S. Zakir, W. Aprison, and L. Efriyanti, "Implementation of Network Security with Firewall Filtering Method Using Mikrotik at SMKN 3 Payakumbuh," *JATI (Journal of Mhs. Tek. Inform.*, vol. 8, no. 3, pp. 3343–3352, 2024, doi: 10.36040/jati.v8i3.9662.