www.bircu-journal.com/index.php/birci
Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
Budapest Institute

Nunukan State Court's Computer Network Security Improvement Using Centralized Next-Generation Firewall

Victor Parlindungan Sitorus[1], Suzzana Lamria Siregar[2]
[1,2]*Universitas Gunadarma, Indonesia*
victorparlindungansitorus@gmail.com, ssiregar@staff.gunadarma.ac.id

Abstract

The Nunukan District Court currently uses technology and information systems to improve services to the community. However, the use of technology and information systems is not accompanied by the application of technology and information system security. This makes the Nunukan District Court vulnerable to attacks and threats such as viruses, phishing, DDoS and others. To overcome this, in this research, a design was made for the implementation of the Next-Generation Firewall which functions to protect information technology and systems in the Nunukan District Court from threats and attacks on technology and information systems. From the results of tests conducted at the Nunukan District Court, the Next-Generation Firewall can prevent attacks and threats carried out in testing. Not only that, this study also found an increase in network performance at the Nunukan District Court. Several features were implemented, such as web filters, antivirus, IPS and antiDDoS, which were seen to be able to prevent attacks and threats to the information system used at the Nunukan District Court. The implementation of the applied design also makes the firewall resource device at the Nunukan District Court unburdened because it offloads the security scanning function to the NGFW device in the cloud which causes an increase in internet access performance.

Keywords
technology and system information security; next-generation firewall; computer network

I. Introduction

The use of technology in the public service sector makes public services faster. Previously difficult to access public information can now be accessed directly using the help of the internet. Many government agencies publish information to the public over the internet, by ensuring data security against all kinds of attacks against all attacks/threats.

In line with the Supreme Court's goal of establishing a modern judicial system in Indonesia, the court has now utilized Information and Communication Technology (ICT)/Internet to improve the quality of legal services throughout Indonesia. But the use of information technology and systems cannot be separated from data security threats/attacks. According to data from the State Cyber and Password Agency, from January 2020 to April 2020 there were 88,414,296 cyberattacks consisting of 56% Trojan activity, 43% information retrieval, 1% attacks on web-based applications, and lain attacks such as attacks using exploit kits and on other networks.

The court's reliance on the internet and the vulnerability of court information technology and systems to cyberattacks is what underlies the implementation of research entitled "Improved Computer Network Security Using a Centralized Next-Generation Firewall (NGFW". The selection of Next-Generation Firewall (NGFW) as the main solution of this study is because NGFW uses Application Specific Integrated Circuit (ASIC) components that have a much higher IP packet processing capacity performance

compared to ordinary *firewalls* that still use Central Processing Unit (CPU) components and have application awareness, identity awareness, Intrusion Prevention System (IPS), antivirus functions and dynamic web filters. (Patil and Mohurle 2017).

Given the extent of the problems raised in the background above, the author restricted the problem in subsequent research. The main problems in this study, only limited to:

a. The court that was used as the object of research was the Nunukan District Court, North Kalimantan.
b. The research was conducted using NGFW devices that are already available in the cloud and firewalls in the Nunukan District Court.
c. Security testing is only performed on web filter features, antivirus, Intrusion Prevention System, AntiDDoS, and internet network performance.

The purpose of this study was the design of a security system for the Court using a centralized Next-Generation Firewall (NGFW) system. In this design effort, this research is aimed at identifying threats / attacks on the security of technology and information systems and the risks faced by the Internal and External Networks of the Court and presenting a form of court computer network design that utilizes a centralized Next-Generation Firewall (NGFW).

II. Review of Literature

NGFW devices are designed to check HTTP packets, analyze SQL commands to check whether a query falls into a category that is considered acceptable or has a possible threat/attack. In order to be categorized as a Next-Generation Firewall, a system must have the following 5 aspects (Chakravarthi, 2016):

a. Non-screwive, in-line, bump-in-the-wire (BITM) capability, where Next-Generation Firewall devices can be implemented on existing network systems, where Next-Generation Firewalls can filter traffic channels of activity between *hosts*;
b. Intrusion Prevention System (IPS) based on integrated signatures, which can determine the type of attack, stop the attack and make a report of the event that occurred;
c. Ability to enter information from outside the Next-Generation Firewall, including index-based settings, whitelists, and boycott mechanisms (IP tires);
d. Secure Socket Layer (SSL) system to perform deeper checks on encrypted data packets using secure socket layer (SSL) or transport layer security (TLS) security protocols;
e. Recognizable application proof using signature from a predefined application, *payload* check, and *header* inspection.

In information technology security, there are 3 aspects of security that are considered important that include *Confidentiality*, *Integrity*, and *Availability* which are also known as the CIA triad (Labone Maxime, 2020). Confidentiality is an aspect of security that restricts access to information, where only people who have obtained permission can access certain information. Confidentiality is defined by the ISO 27000 stkorbanr as a property whose information is not available or disclosed to individuals, entities, or processes (ISO, 2018). One of the attacks on *confidentiality* is phishing with a very form like a fake website. In the act of phishing attacks, attackers or often known as phishers use tactics and strategies in designing phishing websites (Mohammad, Thabtah and McCluskey. 2015). *Integrity* refers to the level of trust in information, trust in this case includes accuracy and consistency of existing information. Therefore, there is a need for protection against information from

modifications by unauthorized parties. Some attacks on *integrity* are SQL injection and Cross-site Scripting (XSS). A form of SQL Injection attack is a hacker technique for executing malicious SQL queries on database servers that can be run through web-based applications to access databases containing sensitive information (Yunuhs, Brohan, Surin, Najib and Liang, 2016) while Cross-site Scripting (XSS) attacks are attacks involving the injection of malicious code into web-based applications from untrusted sources (Ayeni, Sahalu and Adeyanju, 2018). The concept *of availability* of information means that the information is always provided when needed for people who have permission for the information. So that when needed by *the user*, data / information can be quickly accessed and used. One of the most critically anticipated attacks on *the availability* of information is Distributed Denial of Service (DDoS). DoS and DDoS attacks are designed to make a machine or network resource unavailable to its users (Smith and Simpson, 2016). In addition, the factor of human negligence can also result in availability and indirectly impact other components. Another factor is the factor of natural disasters, although rare but the impact caused is sometimes quite large. *Backups* are needed to prevent data loss when computers are attacked by "disasters" (Andry and Honni, 2017).

Various threats and attacks on information system technology can lead to the disclosure of sensitive and confidential information. The fundamental difference between a threat and an attack is that the threat is a constant danger to information integrity, while an attack is a real act of breaching security. An information system security attack is any action that targets a computer in an information system, infrastructure, computer network or personal computer device, using a variety of methods to steal, alter and damage data or information systems. Network attacks can be grouped into two main categories: passive attacks and active attacks (Khan and Hasan, 2018). Passive attacks are relatively rare from a classification perspective, but can be carried out relatively easily, especially if traffic is not encrypted (Kiernet, Bouzefrane and Thoniel, 2015). An active attack is a type of network exploit in which an attacker can modify or change content and impact system resources. This will cause harm to the victims. Attackers will carry out passive attacks to gather information before they start carrying out active attacks. The attacker tried to disrupt and break into the system. The victims will get information about active attacks. This type of attack will threaten its integrity and availability (Eian, Lim, Yeap, Yeo and Fatima, 2020).

To prevent threats and security in information technology and systems, several technologies were developed such as Intrusion Prevention System (IPS), *web filtering*, *antivirus* network, and Virtual Private Network (VPN). Intrusion Prevention System (IPS) is a device or software on computer network security that serves to detect attack activity and threats and prevent the impact of attack activity and information system technology security threats (Sergey, 2016). IPS blocks specific data packets, connections, or hosts from entering the trusted network by stopping the connection from the data packet or providing the event information to the administrator. Intrusion Prevention System (IPS) is divided into three categories, namely application-based IPS, host-based IPS and network-based IPS (Labonne, 2020). Web filters are designed to improve network security and productivity, but as with anything else, they must be applied correctly in order to function properly (Baishya and Kakoty 2019). By using web content filtering, administrators can control access to web content by blocking web pages that contain specific words or patterns. This helps prevent access to pages with dubious material. Administrators can specify perl's regular words, phrases, patterns, wildcards, and expressions to match the content on the web page. Administrators can use multiple *web content filtering* lists and select the best content filtering list for each *web filter* profile (Fortinet, 2020). Antivirus

was developed to detect and remove computer viruses. Modern antivirus can protect a system from Browser Helper Objects (BHOs), browser *hijackers*, *ransomware*, *keylogger*, *backdoors*, *rootkits*, *trojans*, *horses*, *worms*, malicious LSPs, *dialers*, *fraud tools*, *adware* and *spyware* (Rosenberg, 2017). Unlike antivirus in general that is installed on a computer, network antivirus runs on a system that is integrated with a computer network. Although antiviruses on *hosts* provide strong protection for *hosts*, they also face problems. The first problem is the use problem. The use of antivirus causes *non-trivial overhead*. It usually takes several hours to scan *the host* (Hsu, Lee, Luo and Chang, 2019). A Virtual Private Network (VPN) is an encrypted network connection between private networks over a public network (Zeeshan, 2018). With encryption technology, data security becomes more secure. Although there are parties who can intercept data that passes through the internet and even the VPN line itself, but not necessarily able to read the data, because the data has been scrambled. In its implementation, there are currently 2 modes that can be used, namely *site-to-site* and *remote-access*.

III. Research Method

A frame of mind is needed to do a study in order to run well and in accordance with the goal. Based on figure 1, the initial ledge of this study is to identify problems that exist in the object of research. Before conducting the identification process, first select the research topic to focus research. The next activity is to analyze the system in the Nununukan District Court and the main Next-Generation Firewall system located in the *cloud*. The results of the analysis will be used as guidelines in identifying problems and finding solutions.

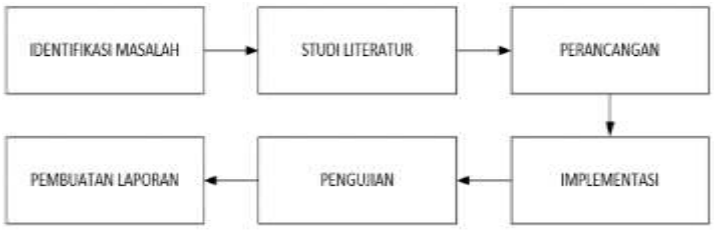

Figure 1. *Research framework of mind*

Identification of the problem is carried out to find the problem that occurred in the Nunukan District Court. At this stage, problems were found in the security of technology and information. To find out the existing problems, several stages are carried out:

a. System analysis running
   Perform analysis on the network system that is running to find out the function of the system as a whole
b. Make observations and tests
   Conducted observations and tests conducted on May 20, 2021. The first application carried out was an experiment to download a virus on the WINCAR website. Furthermore, the dos attack test was carried out towards the Nunukan District Court website.

The design is carried out with the results of the identification analysis of the problem that has been done. At this stage, the design of features and network designs will be applied. The design made is a topology that will be applied to the Nunukan District Court. At this stage, a draft access rights were also created that would be applied to firewall

devices in the Nunukan District Court and The Next-Generation Firewall in the cloud. At this stage of design is also determined security features that will be applied such as web filters, antivirus, and antiDDoS as well as security profiles that will be applied.

At the implementation stage, implementation is carried out to integrate firewall devices located in the Nunukan District Court and Next-Generation Firewall located in the cloud. The Next-Generation Firewall device that is used is the FortiGate 50E located in the Nunukan District Court, serves as a firewall and antiDDoS and FortiGate 200E which serves to carry out the security scanning process.

The testing phase is carried out with the aim of ensuring the system is made in accordance with the results of analysis and design and produce a conclusion whether the system is in accordance with the expected. For that, a testing method is needed that becomes a size or parameter so that conclusions can be drawn so that the system has indeed run according to the purpose. Some of the tests conducted include:

1. Antivirus testing is done by trying to download viruses to see if NGFW can block.
2. Web filter testing is done by trying to access the website by entering the blocking category on the web filter to see if NGFW can prevent users from accessing websites that fall into the block category.
3. DDoS attacks are carried out by conducting DDoS attacks using Canon's High-Orbit ION application towards the Nunukan District Court website to see if NGFW can prevent DoS-type attacks.
4. Sniffing is done using the wire shark application to see if the VPN protocol is used whether it has used the TLS 1.3 protocol.

IV. Discussion

The Nunukan District Court currently uses an internet network with a dedicated speed of 50 Mbps which serves to synchronize the case tracing information system (SIPP) application database to the network of high courts and the Supreme Court, to support online hearings, as well as supporting the operational activities of employees and judges. Currently network topology does not follow the standard hierarchy of three-layer networks. This is due to the absence of a vibrating capacity switch device that can divide the network according to the standard hierarchy of three-layer networks. As a result of the non-implementation of *the three-layer* network standard hiearki, the servers cannot be confirmed with other networks. Figure 2 shows the system currently running, where there is a router device that only acts as a *packet forwarder* and *bridging* without filtering access to the servers.

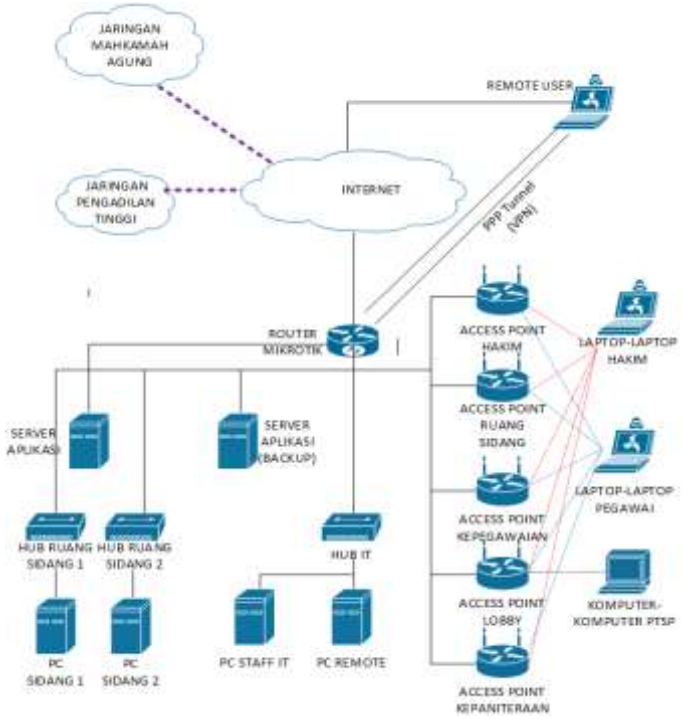

Figure 2. *Network system underway in Nunukan District Court*

4.1 Identification of Attacks and Threats

The nunukan district court computer network currently has not implemented computer network security so a solution is needed, namely the implementation of a Next-Generation Firewall that is useful to protect servers and devices such as laptops, personal computers, and smart devices from information system security threats and attacks such as viruses, exploits and others. As proof, an experiment was conducted that downloaded the EICAR TEST-VIRU virus on the wicar.org website. Figure 3 shows the results of testing security mechanisms by downloading a virus. It can be seen that the virus is downloaded, indicated by the complete download status.

Figure 3. *Testing security mechanisms by downloading a virus*

The second test was to conduct a TCP flood attack from within the nunukan district court's computer network of the Nunukan District Court website hosted on one of the hosting service providers. The test was conducted using Canon's High Orbit Ion application flooding the http://pn-nunukan.go.id website service with TCP SYN on port 80. The result obtained from the attempted attack for 30 minutes, the hosting service provider

where the Nunukan District Court website blocked the public IP of the Nunukan District Court which caused all access from the Nunukan District Court to the website http://pn-nunukan blocked, it can be seen from figure 4.

Figure 4. *Nunukan District Court website page when accessed after conducting TCP flood testing in the direction of http://pn-nunukan.go.id*

4.2 Network Design

To solve the existing problems, a new network design was created in the Nunukan District Court. In figure 5, there are several additions of Next-Generation Firewall devices installed in the Nunukan District Court and in the cloud as well as the separation of the network of servers from the network of employees and judges. In the image there are 2 lines that represent the type of application or *website* to be addressed. The purple line indicates the type of application or website belonging to the Supreme Court. The green line indicates the type of application or *website* other than that of the Supreme Court. The main purpose of creating this design is to segment the server-server computer network with the computer network of employees and judges. The next goal is to be able to divide *traffic* towards the Supreme Court application or website with traffic that is general or traffic other than towards the Supreme Court application or *website*. All *this traffic* will be scanned by the Next-Generation Firewall FortiGate 200E device located in the *cloud*.

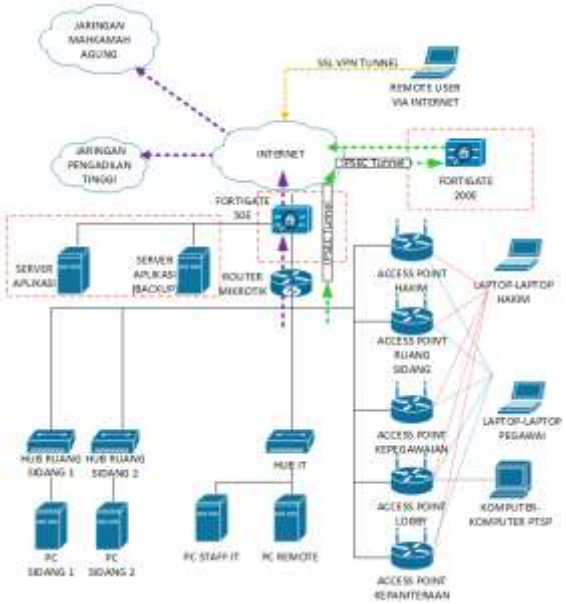

Figure 5. *Design the Nunukan District Court network using a centralized Next-Generation Firewall*

4.3 Access Rule Assignment

Communication is the process of delivering messages by someone to other people to tell, change attitudes, opinions or behavior either directly orally or indirectly through the media (Hasbullah, et al: 2018)**.** To regulate the flow of communication between the network of employees, judges, and guests towards the server network and the internet network, then the rules of access rules are made. This access rule will later be applied in the Next-Generation Firewall located in the Negeri Nunukan Court and the Next-Generation Firewall central which is in the cloud. After identifying the sub network address in the Nunukan District Court, information was obtained about the IP addresses located in the Nunukan District Court which was indicated by table 1.

Table 1. Subnet address information of each section

No	Section Name	Subnet Address
1	Sub. Planning, Information Technology and Reporting (PTIP) Section	192.168.10.0/24
2	Server/DMZ	192.168.3.0/24
3	Sub. Staffing Section	192.168.22.0/24
4	Courtroom	192.168.21.0/24
5	Clerkship	192.168.24.0/24
6	Judge	192.168.20.0/24
7	Public IP (Online SIPP server)	36.x.x.x/30

From the information that has been obtained, access rules are made that will be implemented in the Next-Generation Firewall in the Nunukan District Court and the Next-Generation Firewall central which is in the cloud.

4.4 Security Layer Assignment

Implementing security is the main goal of this research. In this section, it is explained about what security measures will be applied along with a list of implementations of security features on each subnetwork located in the Nunukan District Court. In this study, some security features that will be applied include Intrusion Prevention System (IPS), *network-based antivirus*, and *web filters*.

The first security feature is the Intrusion Prevention System (IPS) which functions to scan and block activities that are considered suspicious and dangerous on the computer network such as activities to exploit the weaknesses of an operating system to find backdoors. The second security feature is network-based antivirus that serves to scan viruses by scanning all network connections that pass through the Next-Generation Firewall FortiGate device and matching the signature on the virus database on the Next-Generation Firewall FortiGate device.

The next security feature is that web filters are useful for filtering all internet website connections by category. So when the website visited is categorized as an ineligible website or a prohibited website, then NGFW will carry out the blocking process.

4.5 Testing

The first test is to perform a DoS attack. To implement the DoS policy, knowledge is needed about the average session on the company's computer network or agency because if there is a policy installation error, the NGFW device will block the legitimate connection. By using dos policy, administrators can control the number of sessions generated from

each connection on the network using dos policy to prevent broadcast sessions which are the main element in any DoS type attack.

To test whether a DoS policy can stop a DoS-based attack such as tcp_flood or udp_flood. So, in the Next-Generation Firewall court, dos policy is applied by using a threshold of as many sessions as previously obtained. After the DoS policy is implemented, then testing is carried out using Canon's High Orbit Ion application which is a stress testing application and DoS for the network. Figure 6 shows the test results where NGFW can prevent the attack by clear-_session that is, removing the session from the IP address that is considered an anomaly from the session table.

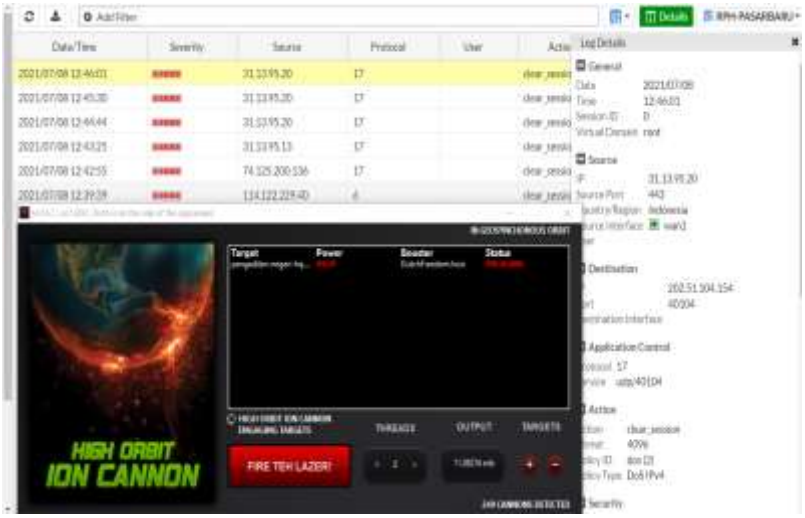

Figure 6. *Test results using Canon's High Orbit Ion*

It looks like NGFW can block *Antivirus testing* is done by downloading the EICAR virus testing file developed by the European Institute for Computer Antivirus Research. The scenario of this test is a computer using the internal finger of the branch court trying to download the eicar file obtained downloaded at the https://secure.eicar.org/eicar_com.zip address. Figure 7 shows the results of the test where an NGFW device in the cloud can stop the test computer from downloading a virus file. Here are the logs proving that NGFW FortiGate court HQ has blocked the activity.

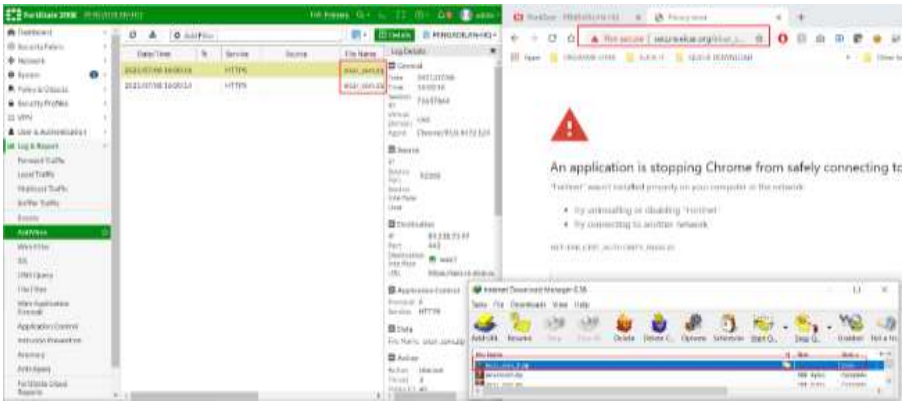

Figure 7. *Antivirus test results*

To test whether the IPS function is running or not, testing is carried out by running a malicious High Orbit Ion Cannon application that performs Denial-of-Service attacks from the direction of the internal network towards the test server on the internet. From the

results of these tests, NGFW can stop DoS attack activity from devices located on the court's internal network. This is evidenced in figure 8 by the log of the attack activity carried out.

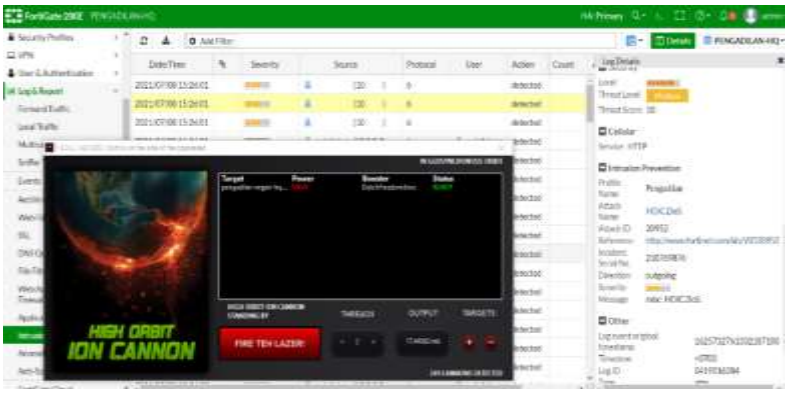

Figure 8. *IPS function test results*

To test whether the function of the Web Filter is running well, a website that contains gambling elements is carried out. From the test results shown in figure 9, it was obtained that the solution applied can block the request towards the website casino.netbet.com even if the user's device connectivity can ping, proving that in the network layer, users can access the casino.netbet.com but because there are rules for blocking websites with gambling categories, the website cannot be accessed.

Figure 9. *Web filter function test results*

In network performance testing, there was a very significant improvement. Testing is done by pinging the detik.com. From the test results, there was an increase in network performance by 27%. PING testing from the Nunukan District Court directly to detik.com located on the internet, the average latency that occurs is 61ms medium While when internet traffic is rushed through the tunnel towards the NGFW level in the *cloud* with security features (IPS, Web Filter, and Antivirus in an active state), the average latency obtained is 48ms.

The next test is to test how fast the time to access the website. The study is done by accessing the website detik.com and then measuring how fast the website opens. From the results of these tests, there was a very significant improvement. Testing showed the use of the internet network directly from branching, the travel time to access the website detik.com until it opened perfectly was 3.25 seconds. Meanwhile, when internet traffic is rushed through the IPSEC tunnel towards the NGFW device of the HQ court, the travel time of detik.com website access is 1.31 seconds. From the data, it can be concluded that there is an increase of 59.68% in website access time.

4.6 Final Conclusion

By using the Next-Generation Firewall that has been implemented in the Nunukan District Court, there are many aspects of improving. The results of the study are displayed in table 2 which shows excellent improvement. The Nunukan District Court Network, which initially did not have a security system to protect its technology and information systems, currently has a Next-Generation Firewall that protects the Nunukan District Court from threats and attacks on information technology and systems.

Table 2. Comparison before and after using NGFW is centralized.

Measurement	**NGFW no-distribution**	**Distributed** NGFW	**Change**
Average *latency*	61 ms	48 ms	Increased *latency* performance by 27%
Average website access time	3.25 seconds	1.31 seconds	Increased average website access time by 59.68%
Security Layer	Network Layer (Layer 3)	Application Layer (Layer 7)	100%
VPN	PPTP (unencrypted)	SSL-VPN (TLS v1.3) TLSv dan IPSEC	100%
NGFW security features	Nothing	IPS, Antivirus, Web Filter, WAF	100%

V. Conclusion

From the results of research conducted in the Nunukan District Court, the following conclusions were obtained:

1. Based on identification and testing conducted by the Nunukan District Court, it is susceptible to viral infections. The use of antivirus on servers and computers that are not always updated causes servers and computers to be vulnerable to viruses. The Nunukan Court did not have the tools to prevent attacks from local networks due to infected servers and computers infected with malicious software trying to send malicious connections to the Nunukan State Pengadilan website which caused the website hosting provider to block the public IP address belonging to the Nunukan District Court.
2. Some of the features that apply are web filters, antivirus, IPS and antiDDoS, seen to prevent attacks and attacks on information systems used in the Nunukan District Court. The implementation of the applied design also makes the firewall resource device in Nunukan State Court unencumbered because it is done offload security scanning function to the NGFW barrier in the cloud which causes an increase in internet access performance.

References

Andry, J.F., Honni. (2017). Using Backup and Restore Automation from Disaster in University Information Systems. Advances in Social Science, Education and Humanities Research.134.1-5

Ayeni, B. K., Sahalu, J. B., & Adeyanju, K. R. (2018). Detecting Cross-Site Scripting in Web Applications Using Fuzzy Inference System. 2018. 1-10

Baishya, A., Kakoty, S. (2019). A Review on Web Content Filtering, Its Technique and Prospects. International Journal of Computer Science Trends and Technology (IJCST). 7(3). 37-40

Chakravarthi, Maoj R. (2016). Next-Generation Firewall-A Review. International Journal of Computer Science and Information Technology. 1. 1212-1215

Eian, I.C.; Lim, K.Y., Yeap, M.X.L., Yeo, H.Q., Z, Fatima. (2020). Wireless Networks: Active and Passive Attack Vulnerabilities and Privacy Challenges. Preprints 2020

Fortinet. (2020). FortiOS Cookbook Version 6.2.0. [Online]. Available at: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/725397/web-content-filter [Accessed 06 August 2021]

Hasbullah, Hatta, M., and Arifin, Z. (2018). Communication Pattern of Wilayatul Hisbah, Lhokseumawe City in Implementing Amar Makruf Nahi Mungkar. *Budapest International Research and Critics Institure Journal*, Vol. 1, No. 4, 194-205.

Hsu, F., Lee C., Luo T., Chang T., Wu. (2019). A Cloud-Based Real-Time Mechanism to Protect End Hosts against Malware. Applied Science. 9(18). 3748

Khan, R., Hasan M. (2018). Network Threats, Attacks and Securityy Measures: A Review. International Journal of Advanced Research in Computer Science. 8(8).116-120

Kiernet, C., Bouzefrane, S., Thoniel P., (2015). Digital Identity Management. Elsevier. 95-135

Labonne, M. (2020). Anomaly-based Network Intrusion Detection Using Machine Learning.Perancis: Institut Polytechnique de Paris.

Mohammad, R.M., Thabtah, F., McCluskey, L. (2015). Tutorial and Critical Analysis of Phising Websites Methods. Computer Science Review. 17. 1-24

Patil, M dan Savita Mohurle. (2017). The Empirical Study of the Evolution of the Next Generation Firewalls. International Journal of Trend in Scientific Research and Development (IJTSRD). 1(5). 193-196

Rosenberg, J. (2017). Embeded Security. United State: Draper Laboratory, Cambridge

Sergey, B. (2016). Intrusion Detection System and Intrusion Prevention System with Snort provided by Security Onion. Finand: Xamk University of Applied Sciences

Smith, D. J., Simpson, K.G.L. (2020). The Safety Critical Handbook (Fifth Edition). Oxford: Butterworth-Heinemann.

Yunuhs, M.A.M.Y., Brohan, M.Z., Nawi, Z.M., Surin, E.S.M., Najib, N.A.M., Liang, C.W. (2016). Review of SQL Injection: Problems and Prevention. The international Journal on Informatics Visualization. 2. 215-219

Zeeshan, A. (2018). Virtual Private Network in Theory and Practice. Atlanta: Schoolar's Press.