p-ISSN: 2252-3006
e-ISSN: 2685-2411

Implementation of Network Security Using Intrusion Prevention System (IPS) with Telegram Based Notification at PT Cyber Access Indonesia

Gede Angga Apriana[a1], I Nyoman Piarsa[a2]
[a]Information Technology Department, Faculty of Engineering, Udayana University, Bali, Indonesia
e-mail: [1]anggaapriana2002@gmail.com, [2]manpits@unud.ac.id

Abstrak

Keamanan jaringan menjadi aspek yang penting bagi sebuah perusahaan berbasis teknologi informasi seperti PT Cyber Akses Indonesia. Isu-isu ancaman keamanan marak terjadi seperti serangan brute force, malware hingga DDoS. Salah satu solusi yang diusulkan adalah Intrusion Prevention System (IPS) yang di mana ini bertugas untuk dapat mendeteksi serta mencegah serangan yang mencurigakan dengan notifikasi berbasis Telegram. Metode yang digunakan adalah Network Development Life Cycle (NDLC) dengan tahapan analisis hingga manajeman. Hasil dari pengujian menunjukkan bahwa konfigurasi keamanan IPS pada MikroTik mampu dapat mengidentifikasi dan memblokir serangan berdasarkan tingkat ancaman. Sistem notifikasi real-time melalui Bot Telegram sangat membantu administrator untuk merespon lebih cepat. Hasil analisis Quality of Service (QoS) juga menunjukkan bahwa penerapan keamanan IPS tidak menurunkan kualitas jaringan secara signifikan dengan nilai rata-rata QoS 3,5 yang memuaskan dari masing-masing parameter yang diuji seperti nilai throughput, packet loss, delay, dan juga jitter.

Kata kunci: *Keamanan jaringan, Intrusion Prevention System (IPS), Brute Force, DDoS, Notifikasi Keamanan, Quality of Service*, *NDLC*

Abstract

Network security is a crucial aspect for information technology-based companies such as PT Cyber Akses Indonesia. Security threats such as brute force attacks, malware, and DDoS are increasingly common. One proposed solution is the implementation of an Intrusion Prevention System (IPS), which functions to detect and prevent suspicious attacks while providing Telegram-based notifications. The methodology used is the Network Development Life Cycle (NDLC), covering stages from analysis to management. The results of the testing show that the IPS security configuration on MikroTik is capable of identifying and blocking attacks based on threat levels. The real-time notification system via Telegram Bot greatly assists administrators in responding more quickly. Quality of Service (QoS) analysis also indicates that the implementation of IPS security does not significantly degrade network performance, with an average QoS score of 3,5 across tested parameters such as throughput, packet loss, delay, and jitter.

Keywords : *Network security, Intrusion Prevention System (IPS), Brute Force, DDoS, Security Notification, Quality of Service, NDLC*

1. Introduction

The need for the internet has become an absolute necessity today, therefore an internet network needs security. the internet (interconnection networking) is an open global communication network that can connect many computer networks of various types and types using communications such as telephone, satellite and others [1].

Network security is an important aspect for a company, agency, or school that depends on the development of information technology, including PT Cyber Access Indonesia as a company engaged in information and communication technology (Internet Service Provider). Threats of attacks such as malware, hacking and DDoS can be financially detrimental and damage the company's reputation [2]. In overcoming these risks, one solution that can be applied is an Intrusion Prevention System (IPS) that functions to detect and prevent attacks automatically by analyzing network traffic. The integration of IPS security with Telegram notifications allows an

p-ISSN: 2252-3006
e-ISSN: 2685-2411

administrator to receive warning messages in real-time, so that they can immediately respond to existing threats.

This research in 2021 at STEI ITB discusses the design and implementation of a network security system using Snort as an IPS. The methods used are IDS and IPS by testing FTP services along with sniffer online mode on snort. The results show that the system successfully runs according to the configuration and methods used [2].

Research in 2017 from the University of Surabaya implemented IPS method using Snort and IP Tables on Linux OS. The stages include system analysis, device requirements, and test scenarios for attacks on the network. The results show that the configuration of Snort and IP Tables successfully blocks access from attackers and the system runs well [3].

Research in 2020 from Dehasen University Bengkulu discusses network security analysis using the concept of Intrusion Detection and Prevention System (IDPS). The methodology in this study includes analysis, design, implementation and system testing. The results show that IDPS is able to detect and prevent attacks such as port scanning, telnet access, and FTP on computer networks [4].

The implementation of an IPS-based security system with Telegram notifications at PT Cyber Akses Indonesia can be a strategic step in strengthening network security defenses, maintaining operational continuity, so as to maintain customer confidence in company services.

2. Research Method / Proposed Method

The research method used in this research is the Network Development Life Cycle (NDLC) which is an adaptation method of the System Development Life Cycle (SDLC). NDLC is used to plan, manage and optimize the development of computer network systems in a structured manner [5].

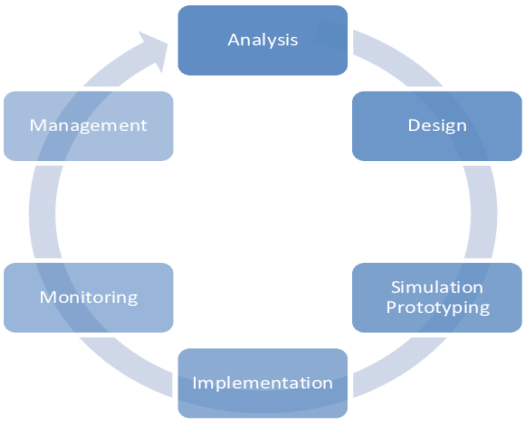

Figure 1. Research Method Network Development Life Cycle

Figure 1 shows the stages of the NDLC method used in this research, which consists of six stages analysis, design, simulation/prototyping, implementation monitoring and management. Each stage will be interrelated and form a sequential flow from analyzing needs to managing the network system as a whole.

2.1 Network Topology at PT Cyber Access Indonesia Company

Network topology is a method used to connect one computer to another, and can form a relationship structure between terminals in the network that can play a role in affecting the level of efficiency of the companys network [6]. The following is the network topology used in the existing internet network at PT Cyber Access Indonesia.

p-ISSN: 2252-3006
e-ISSN: 2685-2411

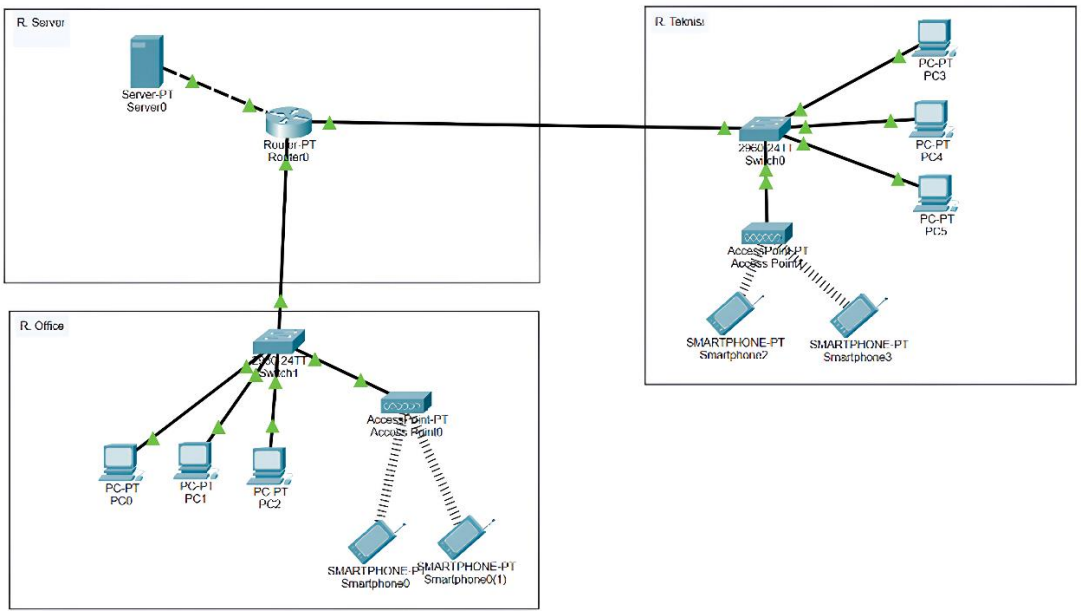

Figure 2. Network Topology PT Cyber Access Indonesia

Figure 2 above is the internet network topology design used at the PT Cyber Access Indonesia office. The picture above shows that PT Cyber Access Indonesia uses several network devices and also several different rooms, starting from the server room, office and technician room. The network devices used include 1 server, 1 router, 2 switches, and 2 access points in each room of the PT Cyber Access Indonesia office.

2.2 System Overview

Network security aims to be able to protect systems and data from hacking and threats such as Brute Forcce or DDoS. Integrated Intrusion Prevention System method through telegram notifications to automatically detect and prevent attacks. Here is an overview of the system

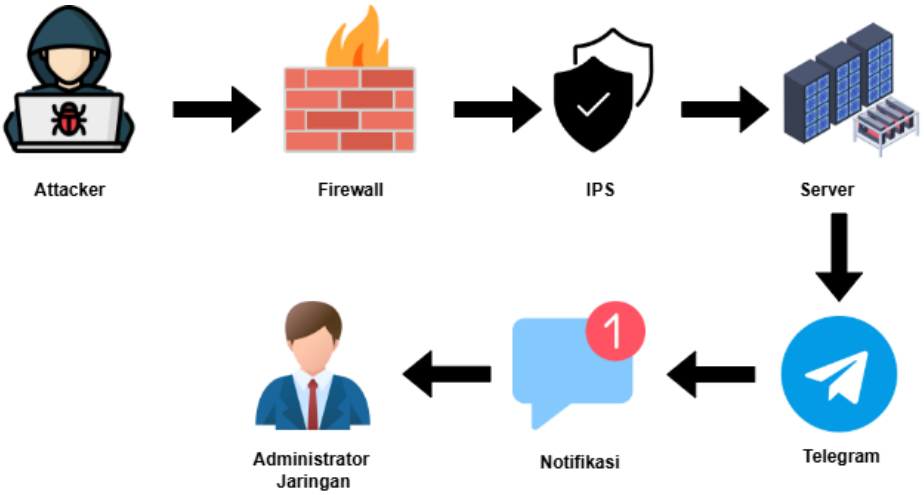

Figure 3. System Overview

Figure 3 shows an overview of the network security system using the Intrrusion Prevention System (IPS) with Telegram notifications. When an attacker tries to attack a server such as through DDoS, then network traffic is filtered by the firewall and IPS analyzes the traffic that passes through. If a threat is detected, the system will automatically send a notification to the network administrator via Telegram so that further action can be taken quickly.

3. Literature Study

Literature study is the process of collecting material from various scientific sources as a supporting theoretical basis in accordance with research related to the topic to be studied. This literature study can be quoted from books, scientific journals, articles and trusted sources that are relevant to the topic being studied.

3.1 Computer Network

A computer network is a collection of interconnections between two or more computers connected through wired or wireless connecting media. Its development began in the 1950s and now continues to develop into various types such as LAN, MAN and WAN [7].

3.2 Internet

The internet is a global communication network that can connect computer networks around the world, the internet makes it possible to communicate exchange information without limits. The main technology used is TCP/IP (Transmission Control Protocol/Internet Protocol) [8].

3.3 Network Security

Network security is an effort to prevent illegal access. Security technologies such as firewalls, VPN and IPS can be applied to address cyber threats. The goal is to be able to protect confidently, integrity an avaliability based on CIA principles [9].

3.4 IPS

Intrusion Prevention System (IPS) is a software/hardware-based technology used to monitor network traffic, detect suspicious activity and automatically prevent attacks. This IPS technology combines the functions of a firewall and Intrusion Detection System (IDS) by examining each incoming packet and blocking or allowing access based on threat identification [4].

3.5 IDS

Intrusion Detection System is a system that functions to monitor and analyze network traffic to detect suspicious activity. IDS can help administrators to take early preventive action. IDS is divided into two types, namely Host-Based (HIDS) and Network-Based (NIDS) [10].

3.6 Firewall

Firewall is a security system consisting of a number of components that are useful for limiting access rights between internal and external networks. Firewalls can provide optimal protection for data and devices on the network with the right configuration [11].

3.7 Telegram

Telegram is an instant messaging application and can be used for free via an internet connection. Telegram was founded by Pavel Durov and the first alpha version of Telegram was released in 2013, until now it has more than 950 million users. [12]

3.8 MikroTik

MikroTik is a Latvian company founded in 1996 that focuses on developing routers and wireless ISP systems. From 1997, MikroTik launched RouterOS, an operating system that provides stability and high flexibility control in data routing. MikroTik started producing its own hardware under the RouterBOARD brand in 2002 [13].

3.9 Brute Force

Brute force is an attack carried out by guessing a fan's password into a network system by trying various combinations of letters, numbers, or systematic dictionary data symbols repeatedly. This attack will target the login promt or password database [14].

3.10 DDoS

Distributed Denial of Service is an attack that aims to make the server slow until it does not function and cannot be accessed by other users. DDoS will attack by flooding the system until its resources are exhausted [3].

p-ISSN: 2252-3006
e-ISSN: 2685-2411

3.11 Quality of Service (QoS)

QoS is a method used to measure and assess the performance of a network so that services remain optimal based on certain parameters. QoS measurement parameters include throughput, packet loss, delay and jitter which refer to the TIPHON standard for evaluation [15].

Table 1. QoS Percentage and Value

Value	Precentage (%)	Indeks
3,8 - 4	95 – 100	Very Satisfactory
3 – 3,79	75 – 94,75	Satisfying
2 – 2,99	50 – 74,75	Less Satisfactory
1 – 1,99	25 – 49,75	Not Satisfactory

3.11.1 Throughput

Throughput is a parameter used to show how fast and slow data can be transmitted over a network. The greater the bandwidth, the higher the throughput value measured in units of bits per second (bps).

Table 2. Throughput Category

Category	Throughput (kbps)	Index
Very good	>2100	4
More	>1200 Kbps	3
Good	700-1200 Kbps	2
Medium	338 – 700 Kbps	1
Bad	0 – 338 Kbps	0

3.11.2 Packet Loss

Packet loss is a parameter that describes a situation where packet loss occurs during data transmission due to collision and congestion in the network.

Table 3. Packet Loss Category

Category	Packet Loss (%)	Index
Very Good	0% - 2%	4
Good	3% - 14%	3
Average	15% – 24%	2
Bad	>25%	1

3.11.3 Delay

Delay is a parameter that shows the length of time taken by data packets to reach the destination from the send point. Factors that affect delay include distance, transmission media and data processing time to the destination.

Table 4. Delay Category

Category	Delay (ms)	Index
Very Good	<150ms	4
Good	150ms - 300ms	3
Average	300ms - 450ms	2
Bad	> 450ms	1

3.11.4 Jitter

Jitter is the variation in time delay between packets sent in sequence. The occurrence of jitter is caused by differences in delay and high network traffic load (congestion).

Table 5. Jitter Category

Category	Jitter (ms)	Indeks
Very Good	0ms	4
Good	1ms - 75ms	3

p-ISSN: 2252-3006
e-ISSN: 2685-2411

Category	Jitter (ms)	Indeks
Average	76ms - 125ms	2
Bad	>125ms	1

4. Result and Discussion

After testing the 4 network security threat experiments, the results and discussion were obtained. The following are the results of the IPS security system and QoS calculations.

4.1 SSH Brute Force drop Implementation Results

The results of this SSH Brute Froce drop will refer to displaying the results of configuration actions that have been carried out in the previous stage which are useful for handling this type of Brute Force attack on the SSH protocol. The following below are the results.

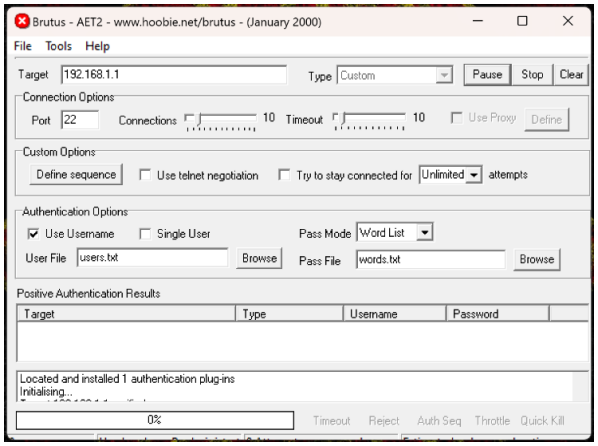

Figure 4. Brutus Testing Results After Implementation of IPS Firewall to Prevent SSH Brute Force

Figure 4 shows the results of testing brute force attacks using the Brutus AET2 application as an attacker against a server with IP 192.168.1.1 on port 22 SSH, with a timeout configuration of 10 seconds and user.txt and words.txt files as credential list files. After implementing IPS security rules on the firewall, this attack no longer generates recommendations from the server username and password, in contrast to the conditions before implementing IPS security where the application is still able to display detected credentials.

Figure 5. Telegram Bot Notification Results for SSH Brute Force Attacks

Figure 5 shows the results of an SSH Brute Force attack notification with a medium threat level sent by the Telgram Bot named Monitoring networkbot. This message will display complete

p-ISSN: 2252-3006
e-ISSN: 2685-2411

information containing the type of attack, time of occurrence, attacker IP and automatic action in the form of blocking access rights accompanied by adding the attacker IP to the blacklist for 30 days. This security notification feature helps network administrators respond to threats quickly and accurately.

4.2 Brute Force FTP Drop Implementation Results

The results of this FTP Brute Force drop will refer to the data results or the final results of an attempt to secure in thwarting or blocking FTP brute force attacks that try to break into the FTP server. Here are the results of the experiment in drop FTP Brute Force.

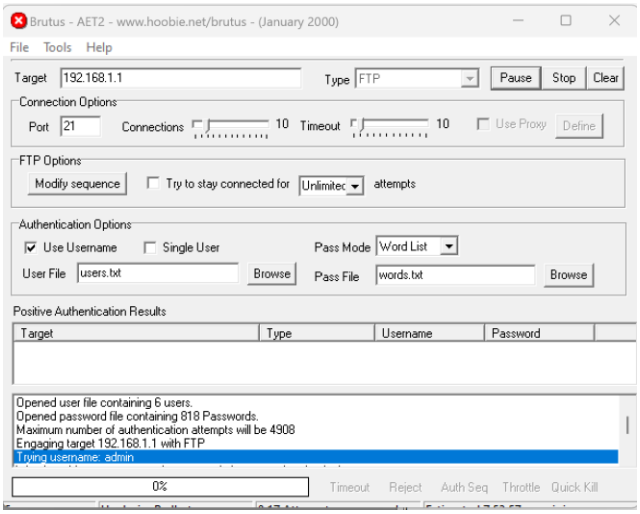

Figure 6. Brutus Testing Results After Implementation of IPS Firewall to Prevent FTP Brute Force

Figure 6 shows the results of testing a brute force attack using the Brutus AET2 application against an FTP server, with attacker IP 192.168.1.1 port 21 with a timeout configuration of 10 seconds and user.txt and words.txt files. This result is that after applying IPS rules to the firewall, brute force attacks no longer display username and password recommendations from the FTP server, this is different from conditions before IPS security where important credentials can still be detected.

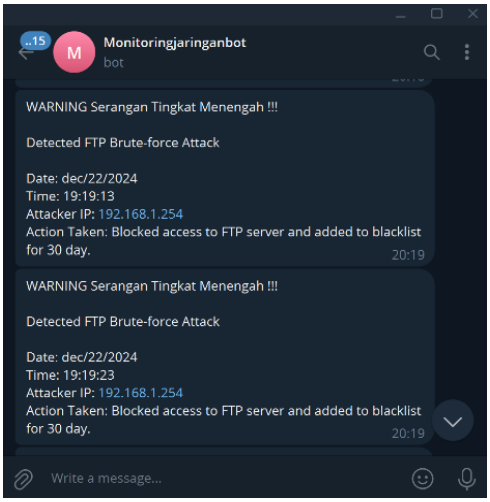

Figure 7. Telegram Bot Notification Results for FTP Brute Force Attack

Figure 7 shows the results of the FTP Brute Force attack notification with a medium threat level sent via Telegram Bot named Monitoringjaringanbot. This notification includes information on the type of attack, time of occurrence, attacker IP and is accompanied by an automatic action

p-ISSN: 2252-3006
e-ISSN: 2685-2411

of blocking access and adding the IP to the blacklist for 30 days. This feature makes it very easy for network administrators to respond to threats quickly and efficiently.

4.3 Results of TELNET Brute Force drop implementation

The results of this Telnet Brute Froce drop will refer to displaying the results of configuration actions that have been carried out in the previous stage which are useful for handling this type of Brute Force attack on the Telnet server protocol. Here below are the results .

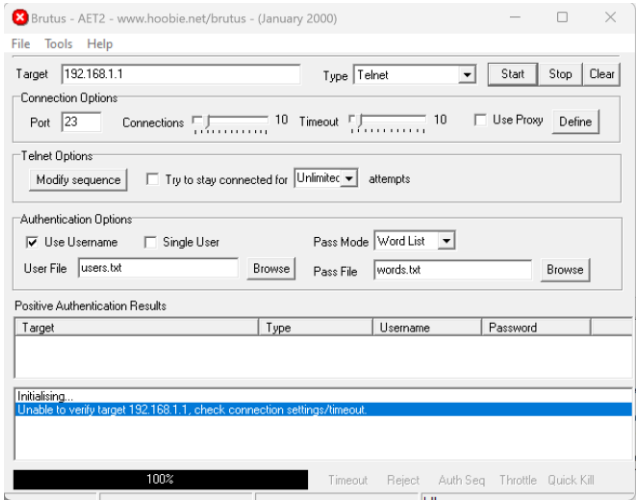

Figure 8. Brutus Testing Results After Implementation of IPS Firewall to Prevent TELNET Brute Force

Figure 8 above shows the results of testing the Telnet server brute force attack with IP 192.168.1.1 on port 23 carried out using the same Brutus AET2 application as used in SSH and FTP brute force testing by configuring a timeout of 10 seconds and user.txt and word.txt as username and password list files. After applying the IPS rule to the firewall, the results show that the test application no longer displays the username and password recommendations, this is different from before the application of the IPS rule where the credential data can still be detected.

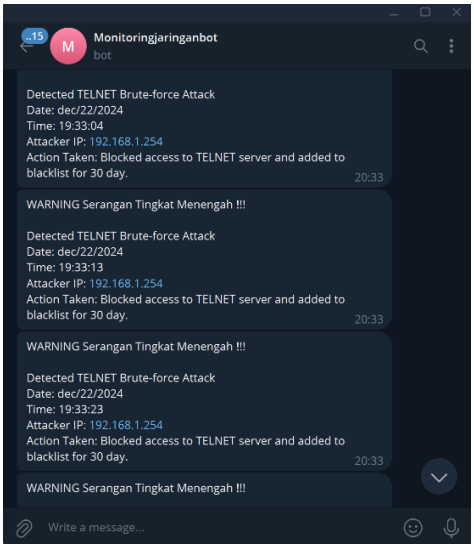

Figure 9. Telegram Bot Notification Results for Telnet Brute Force Attack

Figure 9 is a notification of a Telnet Brute Forse attack sent via Telegram Bot. This message notification contains important information such as the type of attack, the date when it happened, and the IP identity of the attacker who tried to access the server via port 23 Telnet.

p-ISSN: 2252-3006
e-ISSN: 2685-2411

The system will automatically block the IP for 30 days because it is classified as a low-level attack type. This notification helps administrators deal with threats quickly and effectively.

4.4 Drop Port Scanner Deployment Results

The results of this drop portscanner refer to an attempt to protect the server from attempted attackers by attacking through available ports. The following are the results of the drop portscanner experiment.

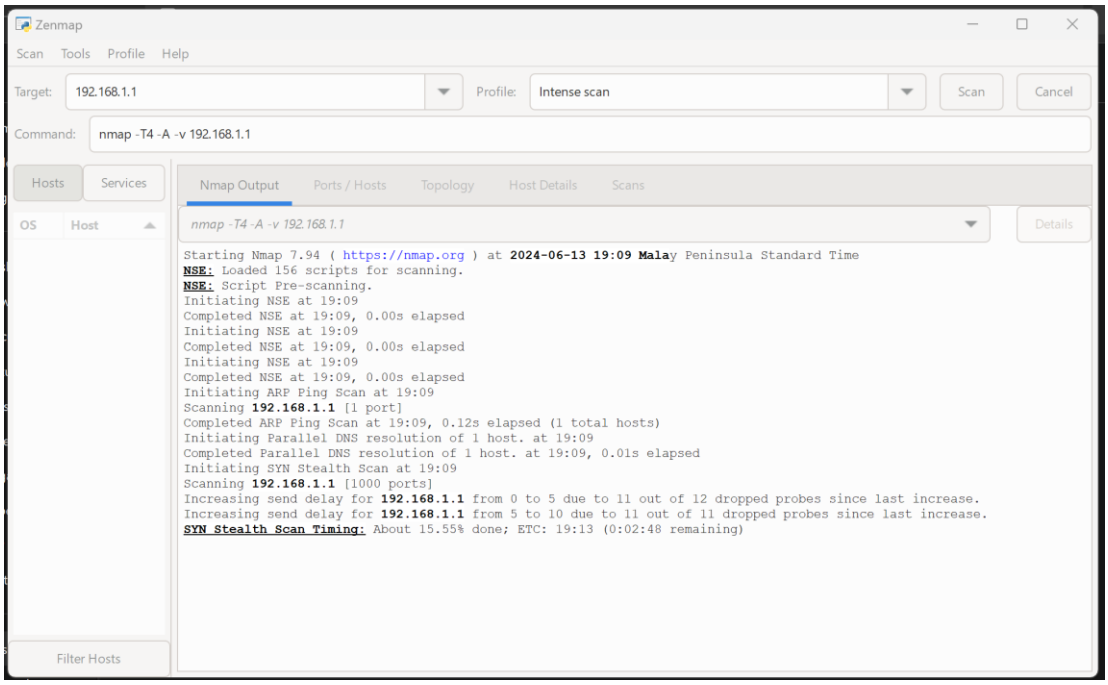

Figure 10. Results of Port Scannig Testing Using Zenmap After Implementation of drop PortScanner

Figure 10 shows the results of the port scanning test after applying the drop rule for PortScanner on the IPS firewall. This test was carried out on a server with IP 192.168.1.1 using the “intense scan” profile in the Zenmap application, after the application of IPS security the results showed no open ports on the server, which indicated that the security gap due to port scanning was effectively closed.

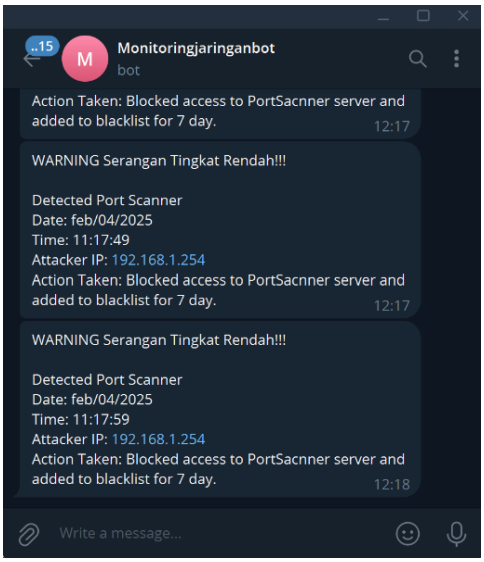

Figure 11.Telgram Bot Notification Results for PortScanner Attack

p-ISSN: 2252-3006
e-ISSN: 2685-2411

Figure 11 shows the Port Scanner attack notification sent via Telegram Bot. This message notification includes important information of the type of threat level, the type of attack, the date and time of the attack and also the IP of the attacker trying to scan for gaps in the server. This type of attack is classified as low-level, so the system will automatically block the IP for 7 days. This notification will make it easier for network administrators to take quick action against the potential threat..

4.5 DDoS drop Implementation Results

The results of this DDoS drop will refer to the results of the configurations that have been carried out in the previous subchapters. In this result will try to display information about DDoS attack attempts that are successfully handled and blocked, the following are the results of the DDoS drop experiment.

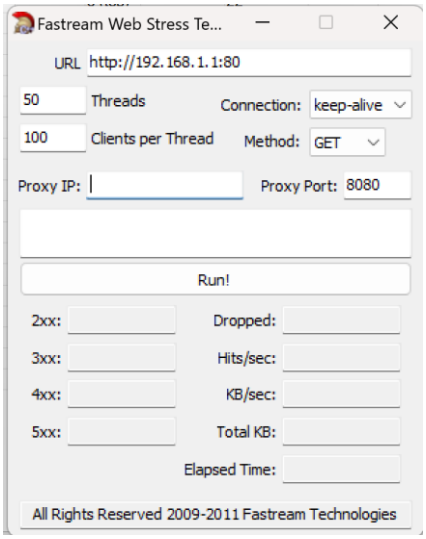

Figure 12. DDoS Attack Testing After Implementation of DDOS drop Rules

Figure 12 shows the display of the Faststream Web Stress Testing application used to test DDoS attacks after applying the DDoS drop rule on the IPS firewall. Testing is done with the same configuration as before, namely the target attack URL “http:192.168.1.1:80”, 50 threads, and 100 clients per thread using the GET method with a keep-alive connection. The test results when run will produce Telegram Bot-based security notifications to mitigate DDoS attacks.

Figure 13. Telegram Bot Notification Result for DDoS Attack

p-ISSN: 2252-3006
e-ISSN: 2685-2411

Figure 13. displays a notification of a high-level threat type DDoS attack through the Telegram Bot application. This notification contains information in the form of the type of attack, the date of the attack, and the IP address of the attacker who was detected trying to break into the server system through the DDoS attack method. This type of attack is a high-level threat, so the system will automatically block the attacker's IP for 1 year, making it easier for network administrators to handle quickly and effectively.

4.6 Quality of Service calculation results

Quality of Service analysis results are obtained based on the overall analysis results obtained from each parameter such as throughput, packet loss, delay and jitter. The results of this Quality of Service analysis are expected to be an illustration for the implementation of the internet network and security system of the company in the future, so that it can support the activities of the company from the use of internet services. The results of the Quality of Service analysis are as follows.

Tabel 6. QoS Results Before Security Implementation

Parameter	Value	Index	Category
Throughput (Kbps)	6518 Kbps	4	Very Good
Packet Loss (%)	4,05 %	3	Good
Delay (ms)	1,00 ms	4	Very Good
Jitter (ms)	1,00 ms	3	Good
Quality of Service		3,5	Satisfyng

Table 6 above is the result of the average QoS analysis on the internet network before the implementation of security. The analysis results obtained show that the quality of the internet network before the implementation of security is included in the satisfactory category, where the average throughput value is 6518 Kbps, packet loss 4.05%, delay 1.00 ms and jitter value 1.00 ms.

Tabel 7. QoS Results After Security Implementation

Parameter	Value	Index	Category
Throughput (Kbps)	4734 Kbps	4	Very Good
Packet Loss (%)	3,50 %	3	Good
Delay (ms)	1,60 ms	4	Very Good
Jitter (ms)	1,60 ms	3	Good
Quality of Service		3,5	Satusfyng

Table 7 above is the result of the average QoS analysis on the internet network after the implementation of security. The analysis results obtained show that the quality of the nternet network after the implementation of security is included in the satisfactory category, where the average throughput value is 4734 Kbps, packet loss 3.50%, delay 1.60 ms and jitter value 1.60 ms.

5. Conclusion

Based on the results and discussion, the implementation of a network security system based on the Intruison Prevention System (IPS) rule on MikroTik has proven effective in improving the security protection system against various cyber threats such as Port Scanner, Brute Force (SSH, FTP, TELNET), and DDoS. This system is able to detect and block attacks automatically, maintaining the stability and security of PT Cyber Access Indonesia's network. The integration of real-time notifications via Telegram Bot makes it easy for network administrators to respond to threats quickly and precisely, with complete information such as the type of attack, time and date of occurrence, attacker IP address and blocking duration. The combination of IPS rules and Telegram notifications is a solution for modern network security, and QoS analysis shows that this security implementation does not significantly degrade network quality, with an average satisfaction index of 3.5, indicating good system stability.

References

[1] A. Mohammad, "Pemanfaatan Instant Messenger Telegram Sebagai Alat Penyebaran Paham Radikal Di Indonesia," *J. Chem. Inf. Model.*, vol. 53, no. February, p. 2021, 2021, [Online]. Available: https://doi.org/10.1080/09638288.2019.1595750%0Ahttps://doi.org/10.1080/17518423.2017.1368728%0Ahttp://dx.doi.org/10.1080/17518423.2017.1368728%0Ahttps://doi.org/10.1016/j.ridd.2020.103766%0Ahttps://doi.org/10.1080/02640414.2019.1689076%0Ahttps://doi.org/

[2] H. Suhendi and W. D. Cahyo, "Perancangan Dan Implementasi Keamanan Jaringan Menggunakan Snort Sebagai Intrusion Prevention System (Ips) Pada Jaringan …," *Naratif J. Nas. Ris. …*, vol. 03, no. 02, pp. 60–68, 2021, [Online]. Available: https://naratif.sttbandung.ac.id/index.php/naratif/article/view/137%0Ahttps://naratif.sttbandung.ac.id/index.php/naratif/article/download/137/71

[3] Y. W. Pradipta, "IMPLEMENTASI INTRUSION PREVENTION SYSTEM (IPS) MENGGUNAKAN SNORT DAN IP TABLES BERBASIS LINUX," *J. Manaj. Inform.*, vol. 7, p. 282, 2017.

[4] H. Alamsyah, R. -, and A. Al Akbar, "Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System," *JOINTECS (Journal Inf. Technol. Comput. Sci.*, vol. 5, no. 1, p. 17, 2020, doi: 10.31328/jointecs.v5i1.1240.

[5] A. Putra Dwi and M. Alghozy Bey Ridho Thorriq, "Analisis dan Implementasi Keamanan Jaringan File Transfer Protocol (FTP) Menggunakan Intrusion Prevention System (IPS) pada Mikrotik," *Smart Comp Jurnalnya Orang Pint. Komput.*, vol. 11, no. 4, 2022, doi: 10.30591/smartcomp.v11i4.4263.

[6] R. Suwanto, I. Ruslianto, and M. Diponegoro, "Implementasi Intrusion Prevention System (IPS) Menggunakan Snort Dan IPTable Pada Monitoring Jaringan Lokal Berbasis Website," *J. Komput. dan Apl.*, vol. 07, no. 1, pp. 97–107, 2019.

[7] D. Susianto and A. Rachmawati, "Implementasi dan Analisis Jaringan Menggunakan Wireshark, Cain and Abels, Network Minner," *J. Cendikia*, vol. XVI, pp. 120–125, 2018.

[8] E. Juliyana and C. A. Nuraflah, "Peranan Internet Dalam Meningkatkan Citra Sma Swasta Budi Agung Medan," *Peran. Internet Dalam Meningkat. Citra Sma Swasta Budi Agung Medan*, vol. 3, no. 1, p. 13, 2020.

[9] A. Irfansyah, "5 Prinsip Kemanan Jaringan," *eduparx*, 2023. https://eduparx.id/blog/insight/5-prinsip-kemanan-jaringan/

[10] I. Ramadhan, "Monitoring Keamanan Jaringan Dengan Snort Ids Menggunakan Metode Forensic Jaringan (Studi Kasus: Cv.Triem Gunung Mas Sejahtera)," *J. Ilm. MIKA AMIK Al Muslim*, vol. 3, no. 1, pp. 13–18, 2019.

[11] F. Adhi Purwaningrum, A. Purwanto, E. Agus Darmadi, P. Tri Mitra Karya Mandiri Blok Semper Jomin Baru, and C. -Karawang, "Optimalisasi Jaringan Menggunakan Firewall," vol. 2, no. 3, pp. 17–23, 2018.

[12] Telegram, "Telegram FAQ," 2024. https://telegram.org/faq?setln=id (accessed Aug. 28, 2024).

[13] MikroTik, "About us," 2024. https://mikrotik.com/aboutus (accessed Aug. 28, 2024).

[14] S. Bahri, "Perancangan Keamanan Jaringan Untuk Mencegah Terjadinya Serangan Bruteforce Pada Router," *Indones. J. Educ. Comput. Sci.*, vol. 1, no. 3, pp. 136–147, 2023, doi: 10.60076/indotech.v1i3.239.

[15] D. Qadri, T. Y. Arif, and A. Azmi, "Analisis Tingkat Kinerja Jaringan Wireless Ieee 802.11N Menggunakan Mikrotik," *J. Komputer, Inf. Teknol. dan Elektro*, vol. 6, no. 2, pp. 21–26, 2021, doi: 10.24815/kitektro.v6i2.21848.