Optimal Filter Assignment Policy Against Distributed Denial of Service Attack on Router Mikrotik

Salkin Lutfi[1], *Amal* Khairan[2], *Yasir* Muin[3*] , *Munazat* Salmin[4]

[1,2,3,4] Informatics Engineering, Faculty of Engineering, Universitas Khairun, Ternate, Indonesia

Abstract. Information technology is currently one of the things that almost all universities widely adopt. The development of information technology requires universities to manage potential resources effectively and efficiently. as stated in the regulation of the Minister of Research, Technology, and Higher Education Number 62 of 2017 concerning the governance of information technology in the university environment that is to support the achievement of increasing access, relevance, quality of higher education, innovation, and strengthening governance and accountability of a university. The consequence of the application of information technology is the emergence of information security risks, the threat of this attack is a concern that every university must be wary of to secure network infrastructure from these attacks. Open access provides great potential for everyone to commit crimes against network infrastructure. as explained that computer network security is part of a system that is very important to be maintained, for that it is necessary to make efforts that can be made by the party responsible for securing the University X network from DDoS attacks. the method used to secure the network infrastructure makes a filtering policy to block DDoS attacks, the results obtained from the application according to the filter rules applied to the proxy device successfully block DDoS attacks.

Keywords: DDoS Attack, Vulnerability, Penetration Testing, Network Security

1 Introduction

Information technology is currently one of the things that are widely adopted by almost all universities [andi Suryadi]. The development of information technology requires universities to manage potential resources effectively and efficiently [1]. as stated in the regulation of the Minister of Research, Technology, and Higher Education Number 62 of 2017 concerning the governance of information technology in the university environment that to support the achievement of increasing access, relevance, quality of higher education, innovation and strengthening governance and accountability of a university [2]. The consequence of the application of information technology (ICT) is the emergence of information security risks [3]. Security issues become a focus for every university to secure assets or network infrastructure from the threat of cyber-attacks.

Various attacks that occur in the internet world often have an adequate impact, with a variety of types of attacks. Citing data from a report from Kaspersky Lab, an attack that has a fairly large impact is a Distributed Denial of Service (DDoS) attack. The increase in the number of attacks reached 31 percent when compared to 2020 [4]. Distributed Denial of Service or DDoS attack is a cyber-attack that occurs due to flooding of the Internet network by fake traffic (Internet traffic) on servers, systems, or the network itself. This attack is carried out using several host computers so that the attacked website can no longer be accessed due to not being able to manage all traffic [5]. The threat of this attack is a concern that every university must be aware of to secure network infrastructure from these attacks.

University x is a state university located in Ternate, North Maluku, which has a fairly complex network infrastructure that is used to provide operational services in each unit to openly access information systems and other resources. Open access provides great potential for everyone to commit crimes on network infrastructure. as explained that computer network security is part of a system that is very important to be maintained, for that there need to be efforts that can be made by the party responsible for securing the network from DDoS attacks. Based on these problems, the action taken to secure the network infrastructure from the threat of cyber-attacks is to create a filter/blocking policy that can optimize DDoS attacks.

2 Research Methods

The research was conducted based on the flow in Figure 1

* Corresponding author : yasirmuin@unkhair.ac.id

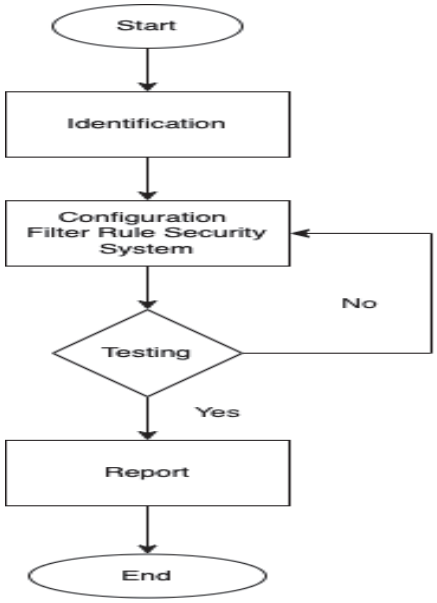

Fig 1 Flow Chart

2.1 Identification

Identification is the initial process to determine and identify network security system problems in the existing conditions of Khairun University. the identification process is carried out in two processes, namely observation and identification of network devices. Observations were made to collect data about the condition of network infrastructure and network security systems used by the university. while the identification of network devices is carried out to determine directly the network security that is implemented on the MikroTik router device. Both processes are carried out to obtain references that can be used as data to solve problems following the research problem.

2.2 Configuration Filter Rule Security System

This step is an explanation of how the rule configuration is done to prevent DDoS attacks. This security rule filtering system is implemented on the proxy router firewall by applying several parameters, namely, creating a rule to capture all new connections made and forwarding to a special firewall chain, secondly regulating the number of packets that pass through the network based on time, thirdly identifying packets that exceed capacity. following the specified then entered into the address list as an anomaly alert, then the detected anomaly will be deleted because it is considered as an attacking threat.

2.3 Testing

The testing process is carried out to test the functionality of the application of the DDoS attack rule filter on the Mikrotik router device to determine the success of the rule implementation. testing using one of the DDoS attacks tools to try to flood the router device with anomalous traffic so that the proxy CPU load performance cannot work optimally. the testing process will show how the filtering rule that is applied will block the traffic, and be included in the address list as an attack message.

2.4 Report

Reporting is the process of documenting the results of security system testing that contains information about information from test results and results from router devices that record all test activities

3 Result and Discussion

In the section is the implementation of filter rules for the prevention of DDoS attacks. There are two stages in the process including

3.1 Configiration Filter Rules

Preventing and reducing DDoS attacks against Mikrotik router devices, it can be done using several steps.

1. Address List
   DDoS attacks come from many sources and it is a much easier way to block connections using an Address List. Identify the source of the malicious IP Address (eg 1.1.1.1 and 2.2.2.2) and create an Address List:

```
/IP firewall address-list add address=200.100.10.0/24
list=Blackhole add
```

2. Filter Prerouting
   To resist attacks, we will filter or downgrade connections to the source of the attack. The further the router has to process bad traffic the harder it will work. The Prerouting process is a great place to block traffic on the device itself if we don't have blackholing configured with the ISP provider, create a Prerouting filter rule using the Blackhole Address List we just created and Action Drop:

```
/ip firewall raw add chain=prerouting src-address-
list=Blackhole action=drop place-before=0
```

When a new malicious IP address is detected, it will be added to the Address List

3. blocking DDoS Attack
   to block incoming attacks on router devices, we can do the command below:

```
/IP firewall filter
add action=jump chain=forward connection-
state=new jump-target=detect-DDoS
add action=return chain=detect-DDoS DST-
limit=32,32,src-and-dest-addresses/10s
```

```
add action=add-DST-to-address-list address-
list=ddosed address-list-timeout=10m chain=detect-
DDoS
```

```
add action=add-src-to-address-list address-
list=ddoser address-list-timeout=10m chain=detect-
DDoS
add action=drop chain=forward connection-state=new
DST-address-list=ddosed src-address-list=ddoser
```

Explanation:

- First, we will capture all the new connections made and pass them to the custom firewall chain.
- Then for each pair of source and destination IP addresses, we will set a limit for the number of packets per second (PPS) and their reset timer and then pass control back to the chain from which the jump occurred.
- Once we have a packet that exceeds the apps we've specified, we add the source and target to the Address List.
- Then we drop all packets flowing through the router if their IP matches the Address List

3.2 Testing

The testing process is the final stage to test the functionality of the implementation of the filter rule security system into the Mikrotik router device. the test is carried out using the mikrotiksploit tool which functions as a DDoS attack.

1. Testing before implementing the security system.
   The test results before the implementation of the security system on the Mikrotik router device can be seen in Figure 2.

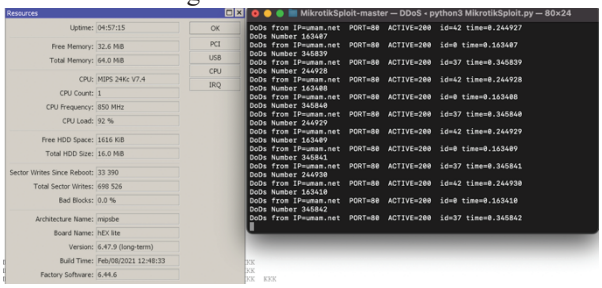

Fig. 2. Testing DDoS Attack

In Figure 2 it can be seen that the test before the filtering rule was applied for the security system gave a very significant impact on the Mikrotik router device performance, namely an increase of up to 92 percent, of course, this poses a big risk to the network infrastructure of the university.

2. Testing after implementation of security system
   The testing process after applying the filtering rule gives quite expected results. We can see this from the performance of the filtering rule which can block DDoS Attack attacks that enter the Mikrotik router device, thus making the CPU load performance of the device stable. we can see this in Figure 2.

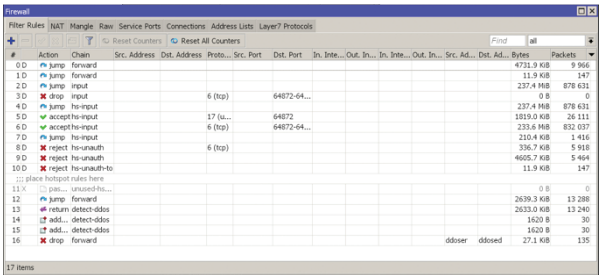

Fig. 3. Filter Fule Active

Figure 3 shows that the filter rule configuration for the DDos Attack attack block is successfully marked by the number of packets recorded by the filter increases when the attack is active. the attack blocking process provides the CPU load performance of the proxy router be stable compared to before the security system was implemented. CPU load presentation can be seen in figure 4.

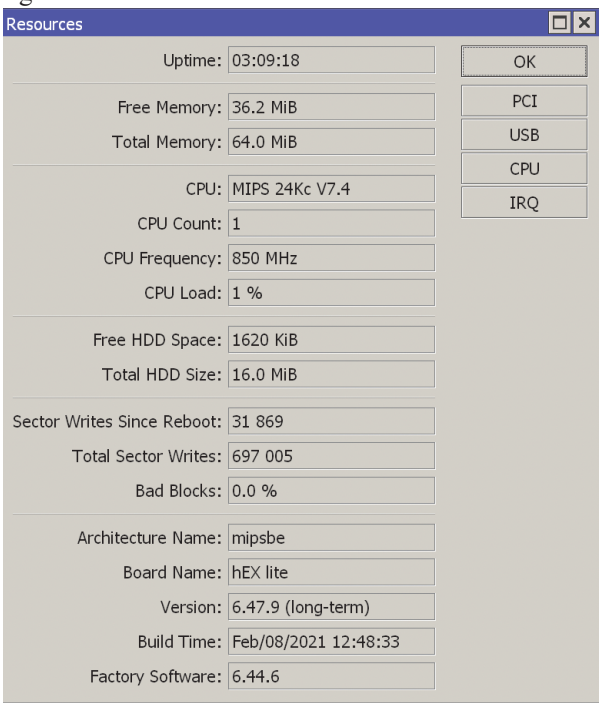

Fig. 4. CPU Load Performance

3.3 Report

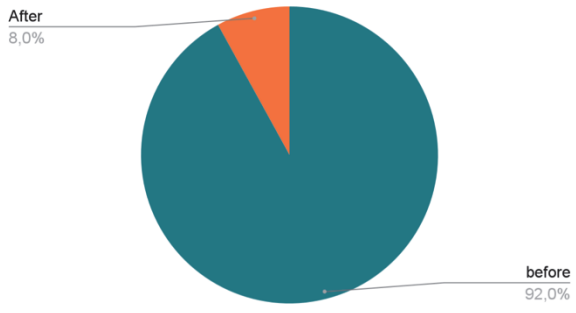

Fig. 5. Implementation of Security System

The graph above shows a presentation of the test results before and after the implementation of the security system on the router device.

Description

1. Before
   The presentation of the test was carried out before the implementation of the security system on the Mikrotik router, the results of the DDoS Attack attack gave a fairly large impact on the performance of the CPU load, and the increase continued to increase during the test. the results obtained from this test reached 92%.
2. After
   test presentations after the implementation of security systems give smaller results than before. implementation gives an 8.0% yield. This means that it has succeeded in blocking incoming DDoS attacks on the router device, thus making CPU Load performance stable.

4 Conclusion

Information technology is currently a thing that is widely adopted by almost all universities. The development of information technology requires universities to manage potential resources effectively and efficiently. The consequence of the application of information technology (ICT) is the emergence of information security risks. Security issues become a focus for every university to secure assets or network infrastructure from the threat of cyber-attacks. The threat of this attack is a concern that every university must be aware of to secure network infrastructure from these attacks. With these problems, the action taken to secure the network infrastructure from the threat of cyber-attacks is to create a filter/blocking policy that can optimize DDoS attacks. the method used to secure the attack there are several stages including identification, namely the process to determine and identify the existing condition of network infrastructure can be in the form of observation and or checking the security used. the second is the configuration of the security rule to block attacks to secure the network, the third test at this stage is a process to test the network security system that has implemented the security rule. The results obtained in the application of the security rule successfully block DDoS Attack attacks, this can be shown from the normal CPU Load presentation when compared to before the presentation security rule CPU Load reached 98%.

References

[1]. B. Sutomo, M. A. Saputra, D. Stmik, D. Wacana, M. Lampung, and S. Wacana, “Perancangan Tata Kelola Teknologi Informasi Pada Perguruan Tinggi Dengan Menggunakan Framework Cobit 5 Studi Kasus : Stmik Dharma Wacana Metro.” [Online]. Available: http://ojs.stmikdharmawacana.ac.id

[2]. “Permen Ristekdikti No. 62 Tahun 2017 tentang Tata Kelola Teknologi Informasi Di Lingkungan Kementerian Riset, Teknologi, Dan Pendidikan Tinggi [JDIH BPK RI].” https://peraturan.bpk.go.id/Home/Details/140999/permen-ristekdikti-no-62-tahun-2017 (accessed Aug. 15, 2022).

[3]. Asriyanik, A., & Prajoko, P. (2018). Pengembangan Aplikasi Penilaian Risiko Keamanan Informasi Berbasis Iso 27005 Menggunakan Metode Prototyping. *SANTIKA is a scientific journal of science and technology*, ***8*(2),** 813-822.

[4]. “DDoS attacks hit a record high in Q4 2021 | Kaspersky.https://www.kaspersky.com/about/press-releases/2022_ddos-attacks-hit-a-record-high-in-q4-2021 (accessed Aug. 15, 2022)

[5]. https://www.biznethome.net/blog/sedikit-mengenal-ddos-attack-yang-bisa-menyerang-website.