# ANALISIS METODE PENGAMANAN PADA PENGGUNAAN *FIREWALL* MIKROTIK UNTUK KEAMANAN JARINGAN KOMPUTER

SKRIPSI

Diajukan untuk memenuhi salah satu syarat untuk memperoleh gelar Sarjana Teknik, pada Program Studi S-1 Teknik Elektro


Oleh:

**Heru Purnama**

**1900194**

**PROGRAM STUDI TEKNIK ELEKTRO**

**DEPARTEMEN PENDIDIKAN TEKNIK ELEKTRO**

**FAKULTAS PENDIDIKAN TEKNOLOGI DAN KEJURUAN**

**UNIVERSITAS PENDIDIKAN INDONESIA**


**2023**

# ANALISIS METODE PENGAMANAN PADA PENGGUNAAN *FIREWALL* MIKROTIK UNTUK KEAMANAN JARINGAN KOMPUTER

Oleh:

Heru Purnama

skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Teknik pada Program Studi S1 Teknik Elektro


Universitas Pendidikan Indonesia
Februari 2023

**LEMBAR PENGESAHAN SKRIPSI**

**HERU PURNAMA**

**E.5051.1900194**

**ANALISIS METODE PENGAMANAN PADA PENGGUNAAN *FIREWALL* MIKROTIK UNTUK KEAMANAN JARINGAN KOMPUTER**

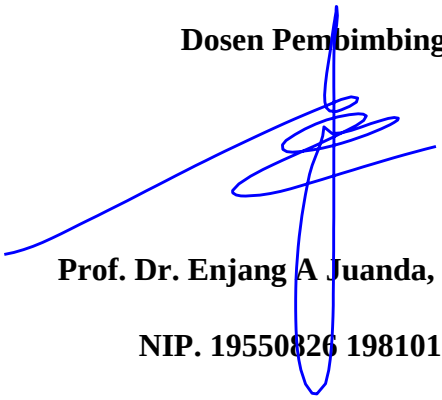
**Disetujui dan disahkan oleh pembimbing:**

**Dosen Pembimbing I**

**Dr. Siscka Elvyanti, M.T.**

**NIP. 19731122 200112 2 002**

**Dosen Pembimbing II**



**Prof. Dr. Enjang A Juanda, M.Pd, M.T.**

**NIP. 19550826 198101 1 001**

**Mengetahui,**

**Ketua Program Studi Teknik Elektro**

**Iwan Kustiawan, S.Pd.,M.T., Ph.D.**

**NIP. 19770908 200312 1 002**

## ABSTRAK

Serangan pada jaringan komputer menjadi lebih mudah dilakukan karena adanya ponsel pintar yang dapat melakukan berbagai hal pada jaringan tersebut, seperti melakukan observasi, menggunakan terminal, mengakses *database* dari jarak jauh, dan hal yang lain yang kegunaannya mendekati sistem operasi *Linux* yang dipasang di *desktop* pada umumnya. Untuk itu diperlukan suatu cara untuk mencegah atau meminimalisir dampak dari serangan keamanan siber dengan cara meningkatkan keamanan pada jaringan. Oleh karena itu, kemampuan *router* atau *server* dalam mencegah serangan harus optimal, salah satunya dengan memanfaatkan *firewall*. Arsitektur yang digunakan dalam percobaan ini meliputi *router*, jaringan *internal*, *server*, *Demilitarized Zone* (*DMZ*), dan *honeypot*. Metode yang diusulkan untuk mendapatkan performa *firewall* yang optimal dengan cara membandingkan setiap kemungkinan metode pengamanan jaringan pada *firewall*. Pada penelitian ini metode yang digunakan untuk mengamankan jaringan komputer menggunakan metode *Drop*, *Reject*, *Tarpit*, dan *redirect* ke *honeypot*, serta penggunaan konsep *DMZ*. Sedangkan untuk pengujian sistem, penelitian ini akan menggunakan metode *denial-of-service* terdistribusi menuju sistem. Setelah melalui proses ini, data dikumpulkan dan ditinjau untuk menemukan cara terbaik untuk menangani serangan dengan menggunakan *MCDM TOPSIS Entropy* dan *Critic*



**Kata kunci: Keamanan Jaringan, *Drop, Reject, Tarpit, redirect, honeypot, DMZ, MCDM, TOPSIS, Entropy, Critic.***



## ABSTRACT

*Attacks on computer networks have become more accessible because smartphones can do various things to the network, such as making observations, using terminals, accessing databases remotely, and others whose uses are close to the Linux operating system installed on a desktop in general. For that, we need a way to prevent or minimize the impact of cybersecurity attacks by increasing security on the network. Therefore, the ability of a router or server to handle attacks must be optimal, one of which is by utilizing a firewall. The architectures used in this experiment include routers, internal networks, servers, Demilitarized Zone (DMZ), and honeypots. The proposed method to get optimal firewall performance is to compare every possible security method on the firewall. In this research the method used to secure computer networks is by using the Drop, Reject, Tarpit, and redirect, and the use of the DMZ concept. As for system testing, this study will use the denial-of-service method to penetrate the system. After going through this process, the output* data *are collected and reviewed to get the best way to handle attacks by using MCDM TOPSIS Entropy and Critic.*



**Keywords: *Cyber Security, Drop, Reject, Tarpit, redirect, honeypot, DMZ, MCDM, TOPSIS, Entropy, Critic.***

## DAFTAR ISI

## DAFTAR PUSTAKA


2nd International Conference on Statistics, Mathematics, Teaching, and Research 2017. (2018). *Journal of Physics: Conference Series*, *1028*, 011001. https://doi.org/10.1088/1742-6596/1028/1/011001

*A New Trend of DDoS Attacks: Mobile Devices Are Becoming a New Generation of Botnets—Alibaba Cloud Community*. (n.d.). https://www.alibabacloud.com/blog/a-new-trend-of-ddos-attacks-mobile-devices-are-becoming-a-new-generation-of-botnets_595026

AL-Dhief, F. T., Sabri, N., Latiff, N. M. A., Albader, A., Mohammed, M. A., AL-Haddad, R. N., Salman, Y. D., Khanapi, M., Ghani, A., & Obaid, O. I. (n.d.). Performance Comparison between TCP and UDP Protocols in Different Simulation Scenarios. *International Journal of Engineering*.

Anthi, E., Williams, L., Javed, A., & Burnap, P. (2021). Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks. *Computers and Security*, *108*, 102352–102352. https://doi.org/10.1016/j.cose.2021.102352

Ceron, J. M., Scholten, C., Pras, A., & Santanna, J. (2020). MikroTik Devices Landscape, Realistic Honeypots, and Automated Attack Classification. *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, 1–9. https://doi.org/10.1109/NOMS47738.2020.9110336

Chakraborty, S. (2022). TOPSIS and Modified TOPSIS: A comparative analysis. *Decision Analytics Journal*, *2*, 100021. https://doi.org/10.1016/j.dajour.2021.100021

Chen, P. (2021). Effects of the entropy weight on TOPSIS. *Expert Systems with Applications*, *168*, 114186. https://doi.org/10.1016/j.eswa.2020.114186

Dabbagh, M., Ghandour, A. J., Fawaz, K., Hajj, W. E., & Hajj, H. (2011). Slow port scanning detection. *2011 7th International Conference on Information Assurance and Security (IAS)*, 228–233. https://doi.org/10.1109/ISIAS.2011.6122824

Dadheech, K., Choudhary, A., & Bhatia, G. (2018). De-Militarized Zone: A Next Level to Network Security. *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 595–600. https://doi.org/10.1109/ICICCT.2018.8473328

Fitri, N. R., Budi, A. H. S., Kustiawan, I., & Suwono, S. E. (2020). Low interaction honeypot as the defense mechanism against Slowloris attack on the web server. *IOP Conference Series: Materials Science and Engineering*, *850*(1), 012037. https://doi.org/10.1088/1757-899X/850/1/012037

*Hping3 | Kali Linux Tools*. (n.d.). https://www.kali.org/tools/hping3/

Huang, J., & China, P. R. (n.d.). *Combining Entropy Weight and TOPSIS Method for Information System Selection*.

Husain, Z. J. (2022a, October 6). Waspada Dengan Serangan Botnet Dan Cara Menghindarinya. *BSI UII*. https://bsi.uii.ac.id/waspada-serangan-botnet/

Husain, Z. J. (2022b, October 6). Waspada Dengan Serangan Botnet Dan Cara Menghindarinya. *BSI UII*. https://bsi.uii.ac.id/waspada-serangan-botnet/

Jaya, B., Yuhandri, Y., & Sumijan, S. (2020). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS). *Jurnal Sistim*

*Informasi Dan Teknologi*, *2*, 115–123. https://doi.org/10.37034/jsisfotek.v2i4.32

Khattab, S., Melhem, R., Mosse, D., & Znati, T. (n.d.). *Honeypot Back-propagation for Mitigating Spoofing Distributed Denial-of-Service Attacks*.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. *Computer*, *50*(7), 80–84. https://doi.org/10.1109/MC.2017.201

Kumar, S., & Rai, S. (n.d.). Survey on Transport Layer Protocols: TCP & UDP. *International Journal of Computer Applications*, *46*.

Madi, M., & Radovanovi, M. (n.d.). *RANKING OF SOME MOST COMMONLY USED NON- TRADITIONAL MACHINING PROCESSES USING ROV AND CRITIC METHODS*.

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39–53. https://doi.org/10.1145/997150.997156

Mokube, I., & Adams, M. (2007). Honeypots: Concepts, approaches, and challenges. *Proceedings of the 45th Annual Southeast Regional Conference*, 321–326. https://doi.org/10.1145/1233341.1233399

Moore, C. (2016). Detecting Ransomware with Honeypot Techniques. *2016 Cybersecurity and Cyberforensics Conference (CCC)*, 77–81. https://doi.org/10.1109/CCC.2016.14

Natsir, N., Pd, S., & Pd, M. (n.d.). *PAKET KEAHLIAN PEDAGOGIK*.

Nawrocki, D. N., & Harding, W. H. (1986). State-value weighted entropy as a measure of investment risk. *Applied Economics*, *18*(4), 411–419. https://doi.org/10.1080/00036848600000038

Osanaiye, O., Choo, K.-K. R., & Dlodlo, M. (2016). Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. *Journal of Network and Computer Applications*, *67*, 147–165. https://doi.org/10.1016/j.jnca.2016.01.001

Papathanasiou, J., & Ploskas, N. (2018). TOPSIS. In J. Papathanasiou & N. Ploskas, *Multiple Criteria Decision Aid* (Vol. 136, pp. 1–30). Springer International Publishing. https://doi.org/10.1007/978-3-319-91648-4_1

Parusa, M. S. (2021). *IMPLEMENTASI HONEYPOT UNTUK MENINGKATKAN SISTEM KEAMANAN SERVER PADA JURUSAN TEKNIK KOMPUTER*.

Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys*, *39*(1), 3. https://doi.org/10.1145/1216370.1216373

*Port Scanning and Reconnaissance with Hping3*. (n.d.). https://www.hackers-arise.com/post/port-scanning-and-reconnaissance-with-hping3

Porter, J. (2020, June 1). *Users discover wallpaper that can crash some Android phones*. The Verge. https://www.theverge.com/2020/6/1/21276658/android-phone-wallpaper-bug-crash-rgb-srgb-samsung-pixel

published, A. W. (2020, June 4). *A "cursed" wallpaper could crash your phone with its color profile [Update: A fix has been found]*. Android Central. https://www.androidcentral.com/cursed-wallpaper-could-crash-your-phone-its-color-profile

Rani, P. U., & Rao, D. V. P. (2011). A Novel Implementation of ARM based Design of Firewall to prevent SYN Flood Attack. *International Journal of Computer Trends and Technology*.

*The Difference Between Drop And Reject When Configuring A Firewall*. (n.d.). Retrieved March 11, 2023, from https://www.nstec.com/what-is-the-difference-between-drop-and-reject-in-firewall/

*Use tarpit vs drop for scripts blocking attackers | MTIN Consulting*. (2017, July 26). https://www.mtin.net/blog/use-tarpit-vs-drop-for-scripts-blocking-attackers/

Webb, J. (n.d.). *Network Demilitarized Zone (DMZ)*.

Yari, G., & Chaji, A. R. (2012). Maximum Bayesian entropy method for determining ordered weighted averaging operator weights. *Computers & Industrial Engineering*, *63*(1), 338–342. https://doi.org/10.1016/j.cie.2012.03.010

Zafar, S., Alamgir, Z., & Rehman, M. H. (2021). An effective blockchain evaluation system based on entropy-CRITIC weight method and MCDM techniques. *Peer-to-Peer Networking and Applications*, *14*(5), 3110–3123. https://doi.org/10.1007/s12083-021-01173-8