BHATARA: Jurnal Multidisiplin
Vol. 3, No.1, Januari 2026, pp. 16-23, ISSN: 2476-9843

Analisis Keamanan Jaringan pada VLAN dengan Metode Firewall Security Port Menggunakan Telegram Bot sebagai Monitoring

Khabib Al Fatta[1], Hastari Utama[2], Joko Dwi Santoso[3], Pramudhita Ferdiansyah[3],
[1]Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta
[3]Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta
[2,3]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta

Jl. Ring Road Utara, Ngringin, Condongcatur, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55281

Coresponding e-mail: [1]khabibalfatta@students.amikom.ac.id

Abstrak

Perkembangan era digital meningkatkan kebutuhan akan keamanan jaringan, terutama pada lingkungan Virtual Local Area Network (VLAN). Penelitian ini bertujuan untuk menganalisis keamanan jaringan pada VLAN dengan menerapkan metode firewall security port dan memanfaatkan Telegram Bot sebagai sistem monitoring berbasis notifikasi real-time. Metode penelitian yang digunakan adalah SPDLC (Security Policy Development Life Cycle) dengan tahapan analisis, desain, implementasi, pengujian, dan evaluasi. Implementasi dilakukan menggunakan router Mikrotik dengan konfigurasi aturan firewall filter beraksi drop pada port tertentu, khususnya port FTP (21). Pengujian serangan DDoS dilakukan menggunakan software Ultraddos dengan mengirimkan 10.000 paket ke alamat IP target. Hasil penelitian menunjukkan bahwa firewall dengan aksi drop berhasil mencegah lonjakan CPU hingga 100% dan menghindari logout paksa pada perangkat. Selain itu, Telegram Bot berhasil mengirimkan notifikasi serangan dalam waktu kurang dari 5 detik setelah serangan terdeteksi, meningkatkan responsivitas administrator. Kesimpulan penelitian ini adalah integrasi firewall security port dan Telegram Bot efektif dalam melindungi jaringan VLAN dari serangan DDoS sekaligus menyediakan mekanisme monitoring yang cepat dan andal. Penelitian ini memberikan kontribusi praktis bagi pengembangan sistem keamanan jaringan yang responsif dan terdiferensiasi.

Kata Kunci: Keamanan jaringan, VLAN, firewall security port, Telegram Bot, monitoring real-time

Abstract

The development of the digital era increases the need for network security, especially in Virtual Local Area Network (VLAN) environments. This study aims to analyze network security in VLANs by implementing the firewall security port method and utilizing Telegram Bot as a real-time notification-based monitoring system. The research method used is SPDLC (Security Policy Development Life Cycle) with stages of analysis, design, implementation, testing, and evaluation. Implementation was carried out using a Mikrotik router with firewall filter rules configured to drop specific ports, particularly the FTP port (21). DDoS attack testing was conducted using Ultraddos software by sending 10,000 packets to the target IP address. The results show that the firewall with the drop action successfully prevented CPU spikes up to 100% and avoided forced logout on the device. Additionally, the Telegram Bot successfully sent attack notifications within less than 5 seconds after detection, improving administrator responsiveness. In conclusion, the integration of firewall security port and Telegram Bot is effective in protecting VLAN networks

from DDoS attacks while providing a fast and reliable monitoring mechanism. This research provides practical contributions to the development of responsive and differentiated network security systems.

Keywords: Network security, VLAN, firewall security port, Telegram Bot, real-time monitoring

1. Pendahuluan

Perkembangan teknologi informasi yang pesat telah membawa dampak signifikan terhadap efisiensi dan konektivitas dalam berbagai sektor, namun di sisi lain juga meningkatkan kerentanan terhadap ancaman keamanan jaringan (Dasmen et al., 2022). Jaringan komputer, sebagai infrastruktur penting dalam pertukaran data, terus menjadi sasaran serangan seperti *spoofing* dan *Distributed Denial of Service* (DDoS) yang dapat mengganggu ketersediaan layanan (Panjaitan & Syafari, 2019). Oleh karena itu, perlindungan jaringan melalui mekanisme keamanan yang andal dan responsif menjadi suatu kebutuhan yang mendesak, terutama dalam lingkungan Virtual Local Area Network (VLAN) yang membutuhkan isolasi logis dan pengamanan tambahan.

Salah satu pendekatan yang dinilai efektif dalam mengamankan jaringan adalah penerapan metode *firewall security port*, yang berfungsi untuk mengontrol akses berdasarkan port jaringan (Cahyawati et al., 2023). Metode ini tidak hanya membatasi akses tidak sah, tetapi juga dapat mencegah eksploitasi port yang rentan terhadap serangan DDoS dan intrusi. Namun, firewall saja belum cukup tanpa adanya sistem pemantauan yang mampu memberikan notifikasi real-time kepada administrator jaringan ketika terdeteksi ancaman. Di sinilah integrasi dengan sistem notifikasi otomatis seperti *Telegram Bot* dapat memberikan nilai tambah dalam kecepatan respons dan efisiensi pengawasan (Andriani & Sa'di, 2024).

Penelitian ini berfokus pada analisis keamanan jaringan pada VLAN dengan mengimplementasikan metode *firewall security port* pada perangkat Mikrotik, sekaligus memanfaatkan Telegram Bot sebagai media notifikasi serangan. Pendekatan ini diharapkan tidak hanya mampu memblokir akses ilegal, tetapi juga memberikan informasi langsung kepada administrator melalui pesan instan saat terjadi upaya pelanggaran keamanan. Dengan demikian, sistem keamanan menjadi lebih proaktif dan dapat mengurangi dampak serangan sebelum meluas. Berdasarkan tinjauan literatur, beberapa penelitian terdahulu telah menguji penerapan firewall berbasis port dan pemanfaatan bot Telegram untuk monitoring jaringan (Kusuma et al., 2020; Agusman et al., 2023). Namun, masih terbatasnya studi yang mengintegrasikan kedua metode tersebut secara spesifik dalam lingkungan VLAN dengan pengujian serangan DDoS secara real-time. Oleh karena itu, penelitian ini bertujuan untuk mengisi celah tersebut dengan melakukan simulasi serangan menggunakan tools seperti Ultraddos dan mengevaluasi efektivitas sistem yang dibangun.

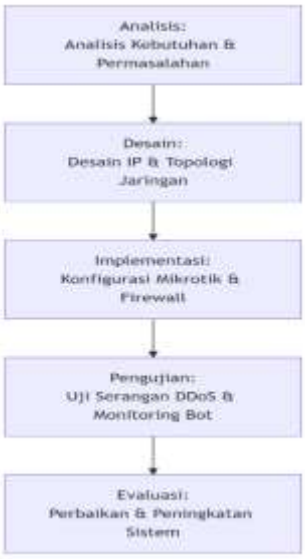
Secara keseluruhan, penelitian ini diharapkan dapat memberikan kontribusi praktis dalam pengembangan sistem keamanan jaringan yang lebih adaptif dan responsif. Hasil penelitian ini diharapkan menjadi acuan bagi pengelola jaringan dalam mengimplementasikan mekanisme firewall security port yang diperkuat dengan notifikasi real-time, khususnya dalam konteks lingkungan VLAN yang memerlukan tingkat keamanan dan pemantauan yang tinggi.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan SPDLC (Security Policy Development Life Cycle) sebagai kerangka metodologis utama. SPDLC merupakan metode pengembangan kebijakan keamanan yang terstruktur dan sistematis, yang terdiri atas fase-fase analisis, desain, implementasi, pengujian, dan evaluasi (Agusman et al., 2023). Pemilihan metode ini didasarkan pada kemampuannya dalam menyediakan alur yang jelas untuk merancang, menguji, dan menyempurnakan sistem keamanan jaringan secara iteratif. Metode ini juga telah banyak diterapkan dalam penelitian sejenis yang berfokus pada pengembangan sistem monitoring dan

keamanan jaringan berbasis notifikasi real-time (Purba & Simanjuntak, 2021). Dalam konteks penelitian ini, SPDLC digunakan untuk memandu proses mulai dari identifikasi kebutuhan keamanan, perancangan arsitektur jaringan VLAN, implementasi firewall security port pada Mikrotik, pengujian serangan menggunakan Ultraddos, hingga evaluasi efektivitas notifikasi yang dihasilkan oleh Telegram Bot. Dengan mengadopsi metode tersebut, penelitian ini bertujuan untuk memastikan bahwa setiap tahap pengembangan sistem dapat tercapai secara terukur, teruji, dan sesuai dengan tujuan analisis keamanan jaringan yang telah ditetapkan.

Penelitian ini menggunakan metode SPDLC (Security Policy Development Life Cycle) sebagai kerangka pengembangan sistem keamanan jaringan. Metode ini dipilih karena memberikan pendekatan yang terstruktur dan sistematis dalam merancang, mengimplementasikan, menguji, dan mengevaluasi kebijakan keamanan jaringan (Agusman et al., 2023). SPDLC terdiri atas lima tahapan utama yaitu analisis, desain, implementasi, pengujian, dan evaluasi. Alur penelitian ini digambarkan dalam Gambar 1.



Gambar 1. Alur Penelitian Berdasarkan Metode SPDLC

2.1. Analisis kebutuhan

Pada tahap ini, peneliti melakukan identifikasi kebutuhan perangkat keras dan perangkat lunak, serta menganalisis permasalahan keamanan yang mungkin terjadi pada jaringan VLAN. Analisis difokuskan pada kerentanan Mikrotik terhadap serangan dari alamat IP yang tidak dikenal. Solusi yang diusulkan adalah penerapan aturan firewall dengan aksi drop untuk menjaga stabilitas CPU Mikrotik (Dasmen et al., 2022). Hasil analisis kebutuhan dan permasalahan disajikan dalam Tabel 1 dan 2.

Tabel 1. Analisis Kebutuhan

Kategori	Spesifikasi
Hardware	ASUS X409JB, Intel Core i3, RAM 12 GB
Software	Mikrotik RouterOS, Winbox v3.40
Tools Uji Serangan	Ultraddos
Platform Monitoring	Telegram Bot API

Tabel 1 menunjukkan kebutuhan perangkat yang digunakan dalam penelitian, meliputi spesifikasi hardware dan software pendukung. Laptop ASUS X409JB dengan Intel Core i3 dan RAM 12 GB digunakan untuk konfigurasi dan pengujian. Mikrotik RouterOS dan Winbox v3.40 berfungsi sebagai sistem manajemen jaringan, sedangkan Ultraddos digunakan untuk simulasi serangan. Telegram Bot API dimanfaatkan sebagai platform monitoring notifikasi keamanan jaringan secara real-time.

Tabel 2. Analisis Permasalahan

Permasalahan	Rencana Solusi
Rentannya Mikrotik terhadap serangan dari IP tak dikenal	Menerapkan firewall dengan action drop untuk menjaga performa CPU.

Tabel 2 menjelaskan bahwa permasalahan utama berupa kerentanan Mikrotik terhadap serangan dari alamat IP yang tidak dikenal yang berpotensi membebani CPU. Untuk mengatasi hal tersebut, diterapkan aturan firewall dengan action drop guna memblokir trafik mencurigakan sebelum diproses lebih lanjut. Strategi ini bertujuan menjaga stabilitas performa router, meningkatkan keamanan jaringan VLAN, serta meminimalkan risiko gangguan layanan akibat serangan eksternal.

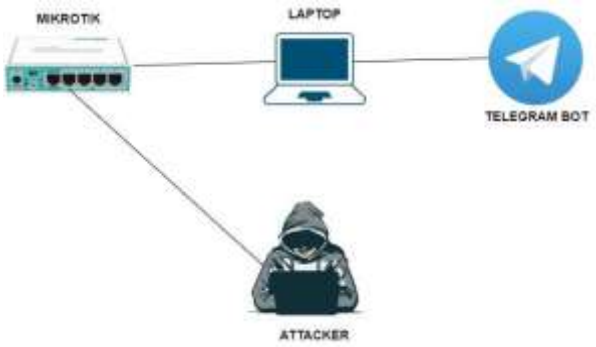
2.2. Perancangan desain topologi jaringan

Tahap desain meliputi perancangan topologi jaringan dan pengalokasian alamat IP. Jaringan dirancang dengan satu router Mikrotik yang terhubung ke internet melalui *interface* WLAN, serta VLAN yang dikonfigurasi pada *interface* ethernet. Tabel 3 menunjukkan rancangan alamat IP yang digunakan.

Tabel 3.Rancangan Alamat IP

Perangkat	Interface	Alamat IP	Subnet Mask
Router	WLAN1	192.168.113.195	255.255.255.0
Router	Ether2 (VLAN10)	192.168.10.1	255.255.255.0
Laptop	NIC	192.168.10.11	255.255.255.0

Topologi jaringan yang dirancang dapat dilihat pada Gambar 2.



Gambar 2. Topologi Jaringan

Arsitektur sistem keamanan jaringan pada Gambar 2melibatkan Mikrotik, laptop administrator, Telegram Bot, dan pihak penyerang. Mikrotik berfungsi sebagai pusat pengelolaan trafik jaringan, sementara laptop digunakan untuk konfigurasi dan monitoring. Telegram Bot dimanfaatkan sebagai media notifikasi kondisi router secara real-time. Attacker merepresentasikan sumber serangan dari IP tidak dikenal yang mencoba mengakses jaringan. Skema ini menunjukkan alur komunikasi serta titik masuk serangan yang menjadi fokus penerapan firewall.

2.3. Implementasi konfigurasi jaringan

Implementasi meliputi konfigurasi jaringan pada Mikrotik, meliputi:

a) Pengaturan alamat IP dan VLAN.
b) Konfigurasi NAT (*Network Address Translation*) untuk koneksi internet.
c) Penerapan aturan *firewall filter* dengan aksi *drop* pada port yang tidak diperlukan.
d) Konfigurasi Netwatch dan integrasi dengan Telegram Bot untuk notifikasi (Purba & Simanjuntak, 2021).

2.4. Pengujian

Pengujian dilakukan dengan mensimulasikan serangan DDoS menggunakan *software* Ultraddos dengan target IP 192.168.10.1 pada port FTP. Pengujian dilakukan dalam dua skenario: tanpa firewall aktif dan dengan firewall aktif. Notifikasi dikirim via Telegram Bot untuk memantau respons sistem (Andriani & Sa'di, 2024).

2.5. Evaluasi hasil

Evaluasi dilakukan dengan menganalisis hasil pengujian, termasuk performa CPU Mikrotik, jumlah paket yang diblokir, dan kecepatan notifikasi Telegram. Hasil evaluasi digunakan untuk menyempurnakan konfigurasi dan memberikan rekomendasi pengembangan sistem lebih lanjut.

3. Hasil dan Pembahasan

Bagian ini menyajikan hasil implementasi dan pengujian sistem keamanan jaringan pada VLAN yang telah dirancang berdasarkan metode SPDLC. Secara bertahap, dipaparkan proses konfigurasi jaringan menggunakan Mikrotik, penerapan aturan firewall security port dengan aksi drop, serta simulasi serangan DDoS menggunakan Ultraddos. Hasil pengujian kemudian dianalisis untuk mengevaluasi efektivitas firewall dalam melindungi jaringan dan menjaga stabilitas CPU, serta responsivitas sistem monitoring berbasis Telegram Bot dalam memberikan notifikasi serangan secara real-time (Andriani & Sa'di, 2024). Selain itu, dilakukan pembahasan komparatif antara kondisi jaringan tanpa firewall dan dengan firewall aktif, termasuk dampaknya terhadap lalu lintas paket, penggunaan CPU, dan keandalan notifikasi. Pembahasan ini juga mengaitkan temuan empiris dengan teori dan penelitian terdahulu untuk memberikan konteks yang lebih mendalam mengenai kontribusi penelitian dalam pengembangan sistem keamanan jaringan yang responsif dan terintegrasi (Purba & Simanjuntak, 2021).Implementasi sistem keamanan jaringan pada VLAN menggunakan metode firewall security port dengan monitoring berbasis Telegram Bot telah berhasil dilakukan sesuai dengan tahapan SPDLC. Hasil penelitian ini mencakup konfigurasi jaringan, hasil pengujian serangan, dan efektivitas notifikasi yang dihasilkan.

3.1. Hasil Konfigurasi Jaringan

Topologi jaringan yang dibangun terdiri atas satu router Mikrotik yang terhubung ke internet melalui antarmuka WLAN1, dengan VLAN10 dikonfigurasi pada antarmuka Ether2. Konfigurasi alamat IP sesuai dengan rancangan yang telah ditetapkan pada Tabel 3. Selain itu, aturan *firewall filter* dengan aksi *drop* telah diterapkan pada router untuk memblokir lalu lintas yang tidak sah, khususnya pada port yang berpotensi menjadi target serangan seperti port FTP (21). Konfigurasi NAT berhasil diimplementasikan sehingga seluruh host dalam VLAN dapat mengakses internet. Integrasi Telegram Bot dengan Mikrotik menggunakan fitur Netwatch juga berhasil dikonfigurasi untuk mengirimkan notifikasi saat terjadi perubahan status koneksi atau serangan.

3.2. Hasil Pengujian Serangan DdoS

Pengujian dilakukan menggunakan *software* Ultraddos dengan mengirimkan 10.000 paket ke alamat IP 192.168.10.1 pada port 21 (FTP). Pengujian dilaksanakan dalam dua skenario: tanpa firewall aktif dan dengan firewall aktif. Hasil pengujian dirangkum dalam Tabel 4.

Tabel 4 Hasil Pengujian Serangan DDoS

No	Skenario	Jumlah Paket Dikirim	IP Target	Port	Hasil
1	Tanpa firewall aktif	10.000	192.168.10.1	21	Terjadi *logout* pada Mikrotik, CPU mencapai 100%, lalu lintas tidak terpantau.
2	Dengan firewall aktif	10.000	192.168.10.1	21	Tidak terjadi *logout*, CPU stabil di bawah 50%, paket berhasil diblokir. Notifikasi Telegram terkirim.

Pada skenario tanpa firewall, serangan menyebabkan CPU Mikrotik mengalami *overload* dan mengakibatkan perangkat *logout* secara otomatis. Sebaliknya, dengan firewall yang diaktifkan, aturan *drop* berhasil memblokir paket serangan sehingga beban CPU tetap rendah dan koneksi jaringan tetap stabil.

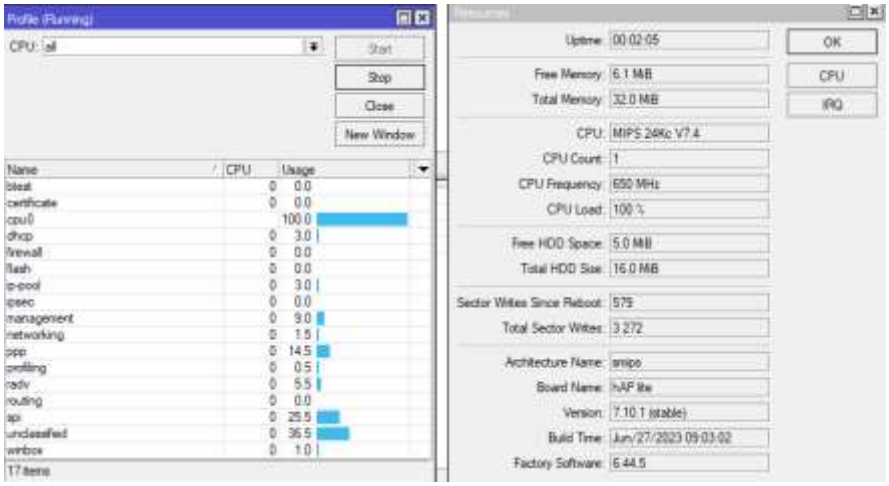
3.3. Hasil Monitoring dan Notifikasi Telegram Bot

Sistem monitoring berbasis Telegram Bot berhasil mengirimkan notifikasi real-time pada saat serangan terjadi dan berhenti. Notifikasi pertama dikirim ketika serangan terdeteksi, mencantumkan waktu, tanggal, dan alamat IP target. Notifikasi kedua dikirim ketika serangan berakhir. Waktu respons notifikasi rata-rata di bawah 5 detik setelah serangan terdeteksi oleh Netwatch. Contoh Notifikasi:

SERANGAN TERDETEKSI! IP: 192.168.10.1 | Tanggal: 03-05-2024 | Waktu: 22:11:36”
SERANGAN BERHENTI. IP: 192.168.10.1 | Tanggal: 03-05-2024 | Waktu: 22:12:31”

3.4. Data Performa Jaringan Selama Serangan

Selama serangan, firewall berhasil mencatat dan memblokir 44.243 paket dengan total 2.246,7 KiB data yang ditujukan ke port 21 seperti yang ditunjukkan pada Gambar 4.1. Data monitoring menunjukkan bahwa tanpa firewall, paket yang masuk tidak terdeteksi oleh sistem filter, sedangkan dengan firewall aktif, seluruh paket serahan tercatat dalam log firewall dan tidak sampai mengganggu layanan. Dengan demikian, hasil penelitian menunjukkan bahwa penerapan *firewall security port* dengan aksi *drop* efektif dalam mencegah dampak serangan DDoS pada jaringan VLAN, sementara Telegram Bot berperan sebagai sistem notifikasi yang cepat dan andal untuk meningkatkan responsibilitas administrasi jaringan.



Gambar 3. Hasil Monitoring Serangan

Hasil penelitian menunjukkan bahwa implementasi aturan *firewall security port* dengan aksi *drop* pada Mikrotik secara signifikan meningkatkan ketahanan jaringan VLAN terhadap serangan DDoS. Tanpa firewall aktif, serangan 10.000 paket yang ditujukan ke port FTP (21) menyebabkan *overload* CPU hingga 100% dan memicu *logout* paksa pada perangkat. Fenomena ini sesuai dengan temuan Dasmen dkk. (2022) yang menyatakan bahwa tanpa mekanisme pembatasan akses berbasis port, perangkat jaringan menjadi rentan terhadap eksploitasi lalu lintas masif. Sebaliknya, dengan firewall diaktifkan, aturan *drop* berhasil membuang paket-paket ilegal sebelum diproses lebih lanjut, sehingga beban CPU tetap stabil di bawah 50% dan tidak terjadi gangguan layanan. Hal ini membuktikan bahwa metode *firewall security port* tidak hanya berfungsi sebagai penyaring (*filter*), tetapi juga sebagai mitigasi *resource exhaustion* pada level perangkat (Purba & Simanjuntak, 2021).

Integrasi Telegram Bot sebagai sistem notifikasi memberikan dimensi responsif yang krusial dalam manajemen keamanan jaringan. Bot berhasil mengirimkan alert kurang dari 5 detik setelah Netwatch mendeteksi anomali lalu lintas, memungkinkan administrator untuk mengambil tindakan segera. Kecepatan ini lebih unggul dibandingkan sistem notifikasi berbasis email atau SMS yang memiliki latency lebih tinggi (Andriani & Sa'di, 2024). Notifikasi yang disertai informasi waktu, tanggal, dan alamat IP target juga meningkatkan akurasi respons, sehingga administrator dapat langsung mengidentifikasi sumber ancaman. Temuan ini sejalan dengan penelitian Agusman dkk. (2023) yang menekankan bahwa notifikasi real-time berbasis platform *messaging* populer seperti Telegram memperpendek siklus deteksi-respons (*detection-response cycle*) dalam pengawasan jaringan.

Dari sisi pengelolaan lalu lintas, firewall dengan aksi *drop* berhasil mencatat dan memblokir 44.243 paket serangan, sementara tanpa firewall, paket-paket tersebut tidak terpantau dalam log sistem. Ini menunjukkan bahwa selain fungsi proteksi, firewall juga berperan sebagai alat *auditing* yang memberikan visibilitas terhadap pola serangan. Namun, perlu dicatat bahwa konfigurasi *drop* pada port tertentu (seperti FTP) dapat berdampak pada layanan legitimate jika tidak diatur dengan cermat. Oleh karena itu, penerapan aturan firewall harus disertai analisis mendalam terhadap port-port kritis yang digunakan oleh layanan operasional (Cahyawati dkk., 2023).

Secara holistik, kombinasi *firewall security port* dan Telegram Bot menciptakan sistem keamanan *layered* yang tidak hanya bersifat preventif (melalui pemblokiran), tetapi juga detektif dan responsif (melalui notifikasi). Pendekatan ini sesuai dengan prinsip *defense in depth* yang direkomendasikan dalam pengembangan kebijakan keamanan jaringan (Purba & Simanjuntak, 2021). Meskipun demikian, penelitian ini memiliki keterbatasan pada lingkup pengujian yang hanya menggunakan satu jenis serangan (DDoS) dan satu port target. Penelitian lanjutan dapat menguji variasi serangan seperti *port scanning*, *brute force*, atau serangan *multi-vector* untuk mengukur ketahanan sistem secara lebih komprehensif.

4. Kesimpulan

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, penelitian ini menyimpulkan bahwa penerapan metode firewall security port dengan aksi *drop* pada lingkungan VLAN terbukti efektif dalam meningkatkan ketahanan jaringan terhadap serangan DDoS. Aturan firewall yang dikonfigurasi pada router Mikrotik berhasil mencegah lonjakan penggunaan CPU hingga 100% dan menghindari terjadinya *logout* paksa pada perangkat, yang sering kali menjadi dampak dari serangan *flooding* paket masif. Hal ini menunjukkan bahwa mekanisme pembatasan akses berbasis port tidak hanya berfungsi sebagai penyaring lalu lintas, tetapi juga sebagai pelindung stabilitas sumber daya perangkat jaringan. Selain itu, integrasi Telegram Bot sebagai sistem monitoring notifikasi real-time memberikan nilai tambah yang signifikan dalam meningkatkan responsivitas dan kesadaran (*awareness*) administrator jaringan. Bot berhasil mengirimkan alert dalam waktu kurang dari 5 detik setelah serangan terdeteksi, dilengkapi dengan informasi detail seperti alamat IP target, waktu, dan tanggal kejadian. Kemampuan ini mempersingkat siklus deteksi-respons dan memungkinkan tindakan mitigasi dapat dilakukan lebih cepat, sehingga mengurangi potensi dampak gangguan yang lebih luas. Secara keseluruhan, penelitian ini telah berhasil mendemonstrasikan bahwa pendekatan gabungan antara keamanan preventif berbasis firewall dan monitoring responsif berbasis bot dapat menciptakan lapisan pertahanan yang lebih komprehensif dalam lingkungan VLAN. Kombinasi ini tidak hanya mampu menangkal serangan secara teknis, tetapi juga memperkuat aspek manajerial melalui notifikasi yang terstruktur dan mudah diakses. Temuan ini memberikan kontribusi praktis bagi pengembangan sistem keamanan jaringan yang adaptif, khususnya dalam konteks jaringan dinamis yang memerlukan pengawasan terus-menerus dan respons yang cepat. Meskipun demikian, penelitian ini memiliki keterbatasan dalam hal ruang lingkup pengujian yang hanya berfokus pada serangan DDoS dengan satu vektor port. Oleh karena itu, implikasi dari temuan ini sekaligus membuka peluang untuk pengujian lebih lanjut dengan variasi serangan yang lebih kompleks, integrasi dengan sistem *intrusion detection* (IDS) yang lebih canggih, serta

pengembangan notifikasi yang bersifat *actionable* seperti perintah *auto-block* berbasis bot untuk menciptakan sistem keamanan yang semakin otonom dan proaktif.

Daftar Pustaka

1. Agusman, B., Mary, T., & Devegi, M. (2023). Perancangan sistem monitoring jaringan menggunakan Bot Telegram sebagai media notifikasi di SMK Negeri 3 Pariaman.
2. Andriani, R., & Sa'di, A. (2024). Implementasi notifikasi Bot Telegram pada sistem monitoring perangkat jaringan. *SISTEMASI: Jurnal Sistem Informasi*. http://sistemasi.ftik.unisi.ac.id
3. Cahyawati, R. K., Fadwa, F. K., Agustin, K. S. A., & Saputro, I. A. (2023). Perancangan keamanan jaringan menggunakan metode firewall security port. *Seminar Nasional AMIKOM Surakarta (SEMNASA)*.
4. Dasmen, R. N., Firmansyah, M. H., Khadafi, M., & Yolanda, T. (2022). Penerapan keamanan jaringan menggunakan metode firewall security port. *Decode: Jurnal Pendidikan Teknologi Informasi, 2*(1), 1–7. https://doi.org/10.51454/decode.v2i1.29
5. Kusuma, D., Darusalam, U., & Hidayatullah, D. (2020). Implementasi monitoring jaringan melalui aplikasi sosial media Telegram dengan Snort. *JIMP-Jurnal Informatika Merdeka Pasuruan, 5*.
6. Panjaitan, F., & Syafari, R. (2019). Pemanfaatan notifikasi Telegram untuk monitoring jaringan. *Jurnal SIMETRIS, 10*(2).
7. Purba, M. J., & Simanjuntak, A. G. P. (2021). Pengamanan Mikrotik RouterBoard dari serangan keamanan dengan notifikasi Bot Telegram. *Majalah Ilmiah METHODA, 11*(3), 241–246. https://doi.org/10.46880/methoda.Vol11No3.pp241-246
8. Putri, R. M., Zulkifli, I., & Fajri, R. M. (2023). Simulasi keamanan jaringan dengan metode network development life cycle menggunakan switch port security pada PT Pinus Merah Abadi.
9. Sudiatmika, I. P. G. A., Ariwanta, I. P. Y. A., & Melati, I. G. A. S. (2022). Mengoptimalkan keamanan jaringan komputer menggunakan Snort dan Telegram Bot yang terintegrasi dengan Mikrotik. *Journal of Computer System and Informatics (JoSYC), 3*(4), 247–256. https://doi.org/10.47065/josyc.v3i4.2037
10. Reza Abdullah, R., & Nurhayati, A. (2019). Monitoring sistem keamanan jaringan berbasis Telegram Bot pada local area network. *Journal of Informatics and Communications Technology, 1*(2), 45–53.