Perancangan Keamanan Jaringan Menggunakan *Metode Firewall Security Port*

Relita Kurnia Cahyawati[1], Fadilla Fadwa Kusuma Agustin*[2], Kinanti Sekar Arum[3], Indrawan Ady Saputro[4]
[1234]Program Studi S1 informatika STMIK Amikom Surakarta
[1234]Sukoharjo, Indonesia
Email: [1]relita.10257@mhs.amikomsolo.ac.id,
[2]fadilla.10322@mhs.amikomsolo.ac.id, [3]kinanti.10236@mhs.amikomsolo.ac.id,
[4]indrawanadys@dosen.amikomsolo.ac.id

Abstract

Network security design is a very important aspect in maintaining the integrity, confidentiality, and availability of data in an organization. One common method used in network security design is the implementation of firewalls with a focus on securing ports. The purpose of this research is to develop an effective network security system using the firewall security port method. This method includes identifying and restricting access to critical ports within the network with the intent of preventing unauthorized access and protecting the system from potential external threats. Through active monitoring of port traffic, firewalls have the ability to detect and respond to possible attacks. This research will explore the optimal firewall configuration, taking into account the specific needs of the organization and network characteristics. In addition, the study will evaluate the impact of firewall implementation on network performance and interconnection between business units. It is hoped that the results of this study can provide practical guidelines for efficient and effective network security design by utilizing the firewall security port method. The conclusion of this study is expected to be the basis for organizations in implementing appropriate and proactive security measures in the face of evolving threats in the network environment.

Keywords: *Firewall, Security, Networking*

Abstraksi

Perancangan keamanan jaringan merupakan aspek yang sangat penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data dalam suatu organisasi. Salah satu metode umum yang digunakan dalam desain keamanan jaringan adalah penerapan firewall dengan fokus pada pengamanan port. Tujuan dari penelitian ini adalah untuk mengembangkan sistem keamanan jaringan yang efektif dengan menggunakan metode firewall security port. Metode ini mencakup mengidentifikasi dan membatasi akses ke port penting dalam jaringan dengan tujuan mencegah akses tidak sah dan melindungi sistem dari potensi ancaman eksternal. Melalui pemantauan aktif terhadap lalu lintas port, firewall memiliki kemampuan untuk mendeteksi dan merespons kemungkinan serangan. Penelitian ini akan mengeksplorasi konfigurasi firewall yang optimal, dengan

mempertimbangkan kebutuhan spesifik organisasi dan karakteristik jaringan. Selain itu, penelitian ini akan mengevaluasi dampak penerapan firewall terhadap kinerja jaringan dan interkoneksi antar unit bisnis. Hasil penelitian ini diharapkan dapat memberikan pedoman praktis perancangan keamanan jaringan yang efisien dan efektif dengan memanfaatkan metode port keamanan firewall. Kesimpulan dari penelitian ini diharapkan dapat menjadi dasar bagi organisasi dalam menerapkan langkah-langkah keamanan yang tepat dan proaktif dalam menghadapi ancaman yang terus berkembang di lingkungan jaringan.

Kata Kunci: *Firewall, Keamanan, Jaringan*

1. PENDAHULUAN

Keamanan jaringan merupakan fondasi yang krusial dalam menghadapi pesatnya perkembangan teknologi saat ini. Dalam era di mana konektivitas digital semakin mendalam, keamanan jaringan menjadi pilar utama untuk melindungi data sensitif, mencegah serangan *cyber*, dan memastikan integritas sistem. Tanpa keamanan jaringan yang kokoh, risiko ancaman keamanan seperti peretasan, pencurian data, dan serangan *malware* dapat mengancam kelangsungan operasional dan privasi informasi, menunjukkan bahwa keberlanjutan teknologi kita sangat tergantung pada ketangguhan sistem keamanan jaringan. Oleh karena itu, menggarisbawahi urgensi perlindungan jaringan bukan hanya sebagai prioritas, melainkan sebagai suatu keharusan esensial dalam menghadapi dinamika perkembangan teknologi yang terus berkembang.

Dalam era informasi yang semakin maju, di mana jaringan komputer menjadi elemen kritis dalam memfasilitasi komunikasi, pertukaran data, dan akses ke sumber daya digital, keamanan jaringan menjadi sebuah aspek yang tak terelakkan. Seiring dengan perkembangan teknologi, tantangan keamanan dalam lingkungan jaringan juga semakin kompleks dan beragam [1].

Ancaman-ancaman seperti serangan *malware*, peretasan, dan akses tidak sah terus meningkat, mengakibatkan dampak serius seperti pencurian data sensitif, kerugian finansial, dan kerusakan reputasi [2]. Dalam menghadapi kompleksitas tantangan keamanan ini, keberadaan sistem keamanan jaringan menjadi sangat penting [3]. Salah satu komponen utama dalam sistem keamanan jaringan adalah *firewall* [4]. *Firewall* berperan sebagai pencegah dan pengidentifikasi terhadap pengguna yang tidak sah yang berusaha memasuki jaringan komputer.

Firewall adalah sebuah sistem atau perangkat yang berperan sebagai garis pertahanan pertama dalam perlindungan sistem [5]. Keamanan jaringan adalah suatu sistem yang dirancang untuk melindungi integritas, kerahasiaan, dan ketersediaan data di dalam jaringan komputer. Dalam konteks ini, integritas merujuk pada keutuhan data, kerahasiaan berkaitan dengan privasi informasi, dan ketersediaan mengacu pada ketersediaan layanan dan sumber daya jaringan [6]. Dengan meningkatnya serangan terhadap jaringan, penggunaan teknologi keamanan telah menjadi suatu keharusan [7].

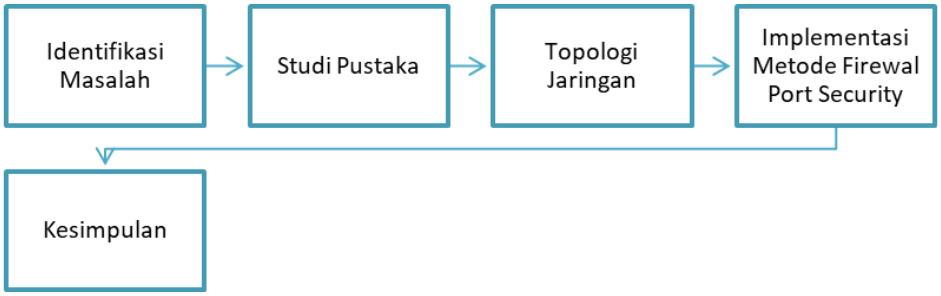
Keamanan jaringan tidak hanya melibatkan perangkat keras (*hardware*) dan perangkat lunak (*software*), tetapi juga melibatkan praktik-praktik keamanan yang efektif [8].

Penelitian tentang implementasi virtualisasi Paloalto *firewall* yang bertujuan untuk mendapatkan fungsi profil sistem pada *firewall* di mana bekerja sebagai filter yang menganalisis dan mengatur lalu lintas data yang masuk dan keluar dari jaringan [9].Penelitian lainnya menjelaskan bahwa *firewall* dapat membatasi akses ke *port-port* tertentu yang digunakan untuk berkomunikasi dengan berbagai layanan dan aplikasi [10]. *Firewall* juga digunakan untuk melindungi, membatasi maupun menolak jaringan pribadi dengan jaringan luar yang berbahaya [11]. Menerapkan metode *firewall security port* setidaknya dapat mengantisipasi suatu permasalahan dalam sistem jaringan komputer [12]. Penelitian ini bertujuan untuk menganalisis efektivitas penggunaan *firewall* dalam melindungi jaringan dari serangan. Selain itu, penelitian ini juga bertujuan untuk mencari cara-cara untuk meningkatkan keamanan jaringan dengan memanfaatkan teknologi *firewall* yang ada.

Hasil dari penelitian ini memberikan pemahaman yang lebih mendalam tentang peran *firewall* dalam melindungi jaringan dari berbagai ancaman keamanan. Selain itu, penelitian ini juga diharapkan dapat memberikan rekomendasi untuk meningkatkan keamanan jaringan dengan memanfaatkan metode *firewall security port*.

2. METODE PENELITIAN

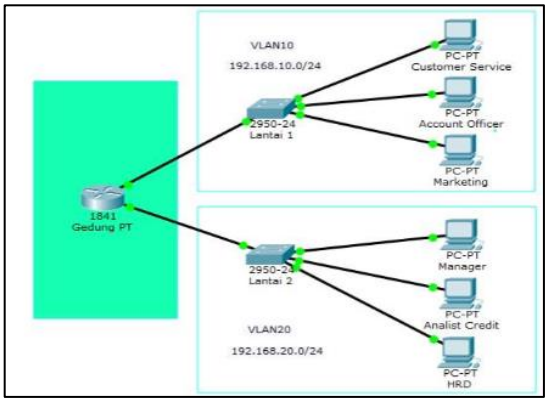
Metode penelitian dalam penelitian ini pada gambar 1, menyajikan landasan teoritis yang melibatkan aspek keamanan jaringan, topologi jaringan, dan implementasi metode *firewall port security*. Pemahaman mendalam tentang konsep keamanan dan topologi menjadi landasan penting bagi eksperimen yang dilakukan. Pemilihan topologi jaringan yang tepat diidentifikasi sebagai faktor kunci untuk meningkatkan efektivitas *firewall port security*. Mengidentifikasi potensi titik rentan dalam topologi jaringan membantu mengoptimalkan upaya keamanan dan meningkatkan daya tahan terhadap ancaman *cyber*. Fokus utama penelitian terletak pada implementasi langkah-langkah, konfigurasi, dan pengujian metode *firewall port security* dalam lingkungan jaringan simulasi. Proses analisis data mencakup evaluasi metrik keamanan yang dipilih dan identifikasi pola serangan, sementara bagian kesimpulan merangkum temuan utama dan memberikan arah untuk penelitian selanjutnya serta rekomendasi untuk perbaikan dalam penerapan keamanan jaringan.



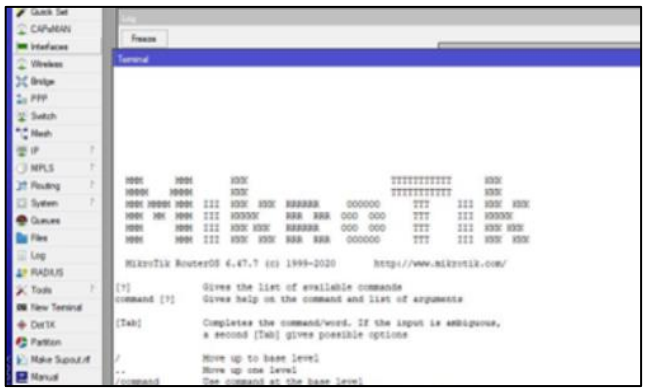
Gambar 1. Metode Penelitian

3. HASIL DAN PEMBAHASAN

Tahap awal dalam membuat topologi *firewall security port* yaitu dengan membuat perancangan dengan dua perangkat, satu PC dan satu laptop, dapat diimplementasikan untuk meningkatkan keamanan jaringan pada skala kecil. Pada topologi ini, perangkat PC dan laptop dihubungkan ke *router* atau *switch* sebagai pusat pengaturan jaringan. *Firewall security port* ditempatkan di antara *router* atau *switch* dan perangkat PC serta laptop. Konfigurasi *firewall* akan mengatur lalu lintas *port* yang diperbolehkan atau diblokir, sehingga hanya lalu lintas yang dianggap aman yang dapat melewati *firewall* dan mencapai perangkat akhir. Implementasi ini juga memungkinkan pemantauan yang lebih baik terhadap aktivitas jaringan serta memberikan kontrol yang lebih besar terhadap akses ke *port-port* tertentu. Berikut ini gambar topologi simulasi jaringan terlihat pada gambar 2 dan tampilan Mikrotik terlihat pada gambar 3.

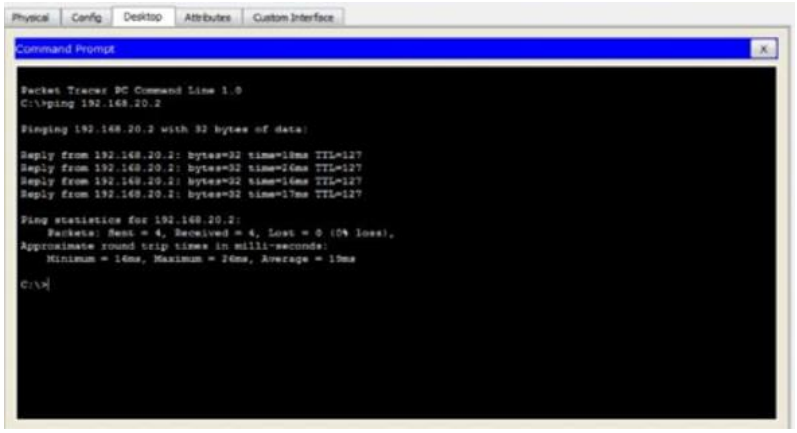


Gambar 2. Topologi Simulasi Jaringan



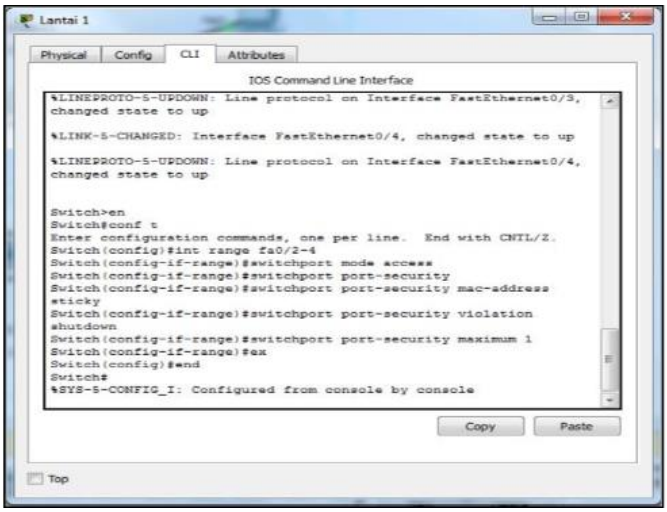
Gambar 3. Tampilan Awal Mikrotik

Simulasi jaringan awal sebelumnya sudah dikonfigurasi (*routing*, *switching*) seluruh perangkat agar jaringan dapat terhubung dan juga menerapkan VLAN pada setiap *switch*. Tetapi *switch* yang dikonfigurasi belum menggunakan *security port*. Untuk pengujian tes ini menggunakan pengiriman Pesan/Data pada setiap PC yang terhubung ke *router* dan juga *test ping* dari PC CS Lantai1 Ke PC *Manager* Lantai 2, untuk memastikan proses jaringan telah terhubung pada gambar 4.



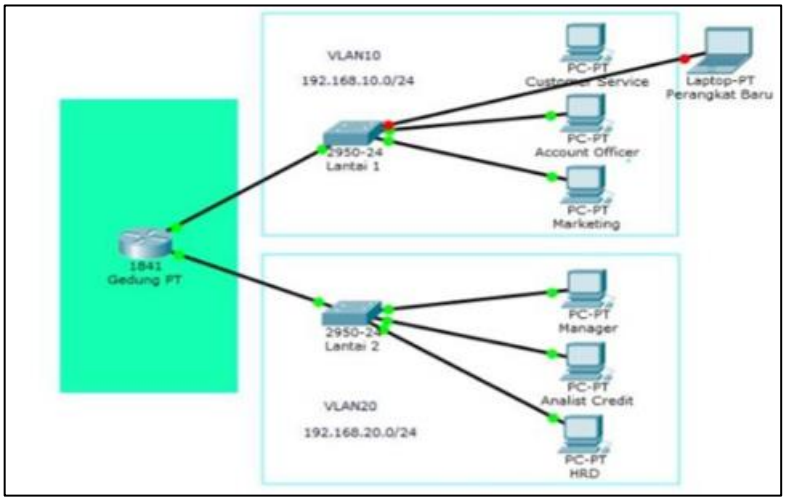
Gambar 4. Test Jaringan

Jika semua perangkat sudah terhubung, selanjutnya menerapkan *port security*. Penerapan keamanan jaringan ini menggunakan *security port* pada setiap *switch* menggunakan cara konfigurasi yang sama. Hanya melakukan perintah *mac-address port security sticky* pada gambar 5.



Gambar 5. Konfigurasi

Untuk tes, menggunakan satu Laptop perangkat baru. Kemudian satu kabel koneksi PC yang terhubung ke *switch* di cabut dan disambungkan ke perangkat baru serta mengonfigurasi/memasukkan alamat IP yang sama pada gambar 6.



Gambar 6. Koneksi Perangkat Baru

Pada lantai 1 *port* yang tersambung ke perangkat baru berwarna merah yang artinya, akses jaringan pada perangkat tersebut tidak terkoneksi walaupun mengonfigurasi alamat IP yang sama, karena jika ada perangkat yang tidak dikenal terkoneksi tidak sesuai dengan *mac-address*nya maka port pada *switch* akan otomatis mati.

4. KESIMPULAN

Penelitian ini mengevaluasi efektivitas metode *firewall security port* dalam melindungi jaringan dari ancaman keamanan. Hasil analisis menunjukkan bahwa *firewall* berbasis port ini berhasil mengurangi risiko serangan dari luar yang mengincar layanan jaringan tertentu. Kesimpulannya, penggunaan *firewall security port* yang cermat dapat menjadi aspek penting dalam upaya melindungi integritas dan kerahasiaan jaringan.

DAFTAR PUSTAKA

[1] A. Novrianto, B. Asmanto, and D. Irawan, "Perancangan Sistem Informasi Jaringan Lan (Local Area Network) Pada Laboratorium Komputer Smp Negeri 2 Sekampung Lampung Timur," *J. Mhs. Sist. Inf.*, vol. 3, no. 2, pp. 46–53, 2022, doi: 10.24127/jmsi.v3i2.2150.

[2] E. Soesanto, A. Romadhon, B. Dwi Mardika, and M. Fahmi Setiawan, "Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File," *SAMMAJIVA J. Penelit. Bisnisdan Manaj.*, vol. 1, no. 2, p. 186, 2023.

[3] O. Rivaldi and N. L. Marpaung, "Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata," *INOVTEK Polbeng - Seri Inform.*, vol. 8, no. 1, p. 141, 2023, doi: 10.35314/isi.v8i1.3269.

[4] D. Wicaksono, "Firewall Sistem Keamanan Jaringan Menggunakan Firewall dengan Metode Port Blocking dan Firewall Filtering," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 2, pp. 1380–1392, 2022, doi: 10.35957/jatisi.v9i2.2103.

[5] R. N. Dasmen, M. Hendra Firmansyah, M. Khadafi, and Tri Yolanda, "Penerapan Keamanan Jaringan Menggunakan Metode Firewall Security Port," *Decod. J. Pendidik. Teknol. Inf.*, vol. 2, no. 1, pp. 1–7, 2022, doi: 10.51454/decode.v2i1.29.
[6] R. Permana, D. Ramadhani, and I. Lestari, "Proteksi Keamanan Jaringan Komputer di Sekolah Menengah Kejuran Al-Madani Pontianak," *Int. J. Nat. Sci. Eng.*, vol. 3, no. 1, p. 37, 2019, doi: 10.23887/ijnse.v3i1.22175.
[7] A. S. Waskita and H. Sidik, "Diplomasi Siber Indonesia dalam Penyelenggaraan Capacity Building on National Cybersecurity Strategy Workshop 2019," *Padjadjaran J. Int. Relations*, vol. 5, no. 2, p. 142, 2023, doi: 10.24198/padjir.v5i2.41337.
[8] N. Tamsir *et al.*, *Keamanan Sistem Informasi*. Bandung: Indie Press, 2023.
[9] N. M. M. Listyawati, A. Widjajarto, and M. T. Kurniawan, "Implementasi dan Analisis Profil Sistem Pada Virtualisasi Paloalto Firewall Berdasarkan Metrik Sumber Daya Komputasi," *J. Sist. Komput. dan Inform.*, vol. 4, no. 1, p. 112, 2022, doi: 10.30865/json.v4i1.4780.
[10] S. Sutiman and A. Gunawan, "Firewall Port Security Switch Untuk Keamanan Jaringan Komputer Menggunakan Cisco Router 1600S Pada Pt. Tirta Kencana Tata Warna Sukabumi," *CONTEN Comput. Netw. Technol.*, vol. 1, no. 1, pp. 13–22, 2021, doi: 10.31294/conten.v1i1.402.
[11] A. Khoumsi, M. Erradi, and W. Krombi, "A formal basis for the design and analysis of firewall security policies," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 1, pp. 51–66, 2018, doi: https://doi.org/10.1016/j.jksuci.2016.11.008.
[12] L. Azharuddin and T. Nurhastuti, "Perancangan dan Implementasi Sistem Keamanan Jaringan dengan Port Security Menggunakan Switch CISCO di PT. Citra Solusi Pratama," *J. Teknol. Inf.*, vol. 9, no. 1, pp. 56–68, 2023, doi: 10.52643/jti.v9i1.3175.