ANALISIS IMPLEMENTASI FIREWALL HARDWARE FORTINET PADA INFRASTRUKTUR JARINGAN DI RSKIA SADEWA YOGYAKARTA

Muhammad Zufar Arsalan, Arridho Ramadhan Firdaus*
Program Studi Teknologi Informasi, Universitas 'Aisyiyah Yogyakarta
Jl. Siliwangi (Ring Road Barat) No. 63, Nogotirto, Gamping, Sleman,
Daerah Istimewa Yogyakarta, Indonesia
arridhoramadhanfirdaus@unisayogya.ac.id

ABSTRAK

Keamanan jaringan merupakan aspek penting dalam operasional rumah sakit karena berkaitan langsung dengan perlindungan data medis serta keberlangsungan layanan sistem informasi. RSKIA Sadewa Yogyakarta menerapkan firewall hardware Fortinet sebagai solusi pengamanan jaringan untuk mengendalikan lalu lintas data dan meminimalkan potensi ancaman keamanan. Penelitian ini bertujuan untuk menganalisis implementasi firewall hardware Fortinet pada infrastruktur jaringan di RSKIA Sadewa Yogyakarta. Metode penelitian yang digunakan adalah metode kualitatif deskriptif dengan pendekatan studi kasus melalui observasi infrastruktur jaringan, analisis konfigurasi firewall, serta pemantauan trafik jaringan menggunakan sistem monitoring Prometheus dan Grafana. Hasil penelitian menunjukkan bahwa penerapan firewall Fortinet mampu meningkatkan keamanan dan stabilitas jaringan. Namun demikian, masih diperlukan optimalisasi pengelolaan bandwidth dan segmentasi jaringan agar kinerja jaringan rumah sakit dapat berjalan lebih efisien dan optimal.

Kata kunci: *Firewall, Fortinet, Keamanan Jaringan, Infrastruktur Jaringan, Rumah Sakit*

1. PENDAHULUAN

Teknologi informasi memiliki peran yang sangat penting dalam mendukung operasional rumah sakit, khususnya dalam pengelolaan sistem informasi dan jaringan komputer. Infrastruktur jaringan yang andal dan aman dibutuhkan untuk menunjang berbagai layanan digital seperti sistem rekam medis elektronik, sistem administrasi rumah sakit, serta layanan informasi pasien. Ketergantungan terhadap sistem jaringan menjadikan aspek keamanan jaringan sebagai faktor krusial dalam menjaga kualitas pelayanan kesehatan.

Lingkungan rumah sakit menyimpan dan mengelola data yang bersifat sensitif sehingga rentan terhadap berbagai ancaman keamanan jaringan, seperti akses tidak sah, serangan malware, serta gangguan layanan jaringan. Oleh karena itu, diperlukan sistem keamanan jaringan yang mampu mengendalikan lalu lintas data dan melindungi jaringan dari ancaman eksternal. Firewall merupakan salah satu komponen utama dalam sistem keamanan jaringan yang berfungsi sebagai pengendali dan penyaring lalu lintas data berdasarkan kebijakan keamanan tertentu.

Firewall hardware banyak digunakan pada jaringan berskala menengah hingga besar karena memiliki performa dan stabilitas yang lebih baik dibandingkan firewall berbasis perangkat lunak. Salah satu perangkat firewall hardware yang banyak diterapkan adalah Fortinet, yang menyediakan fitur keamanan komprehensif seperti pengaturan kebijakan akses jaringan, inspeksi paket data, serta perlindungan terhadap berbagai jenis serangan jaringan.

RSKIA Sadewa Yogyakarta telah menerapkan firewall hardware Fortinet sebagai bagian dari sistem keamanan jaringan rumah sakit. Namun, diperlukan analisis untuk mengetahui sejauh mana efektivitas implementasi firewall tersebut dalam menjaga keamanan dan stabilitas jaringan. Oleh karena itu, penelitian ini dilakukan untuk menganalisis implementasi firewall hardware Fortinet pada infrastruktur jaringan di RSKIA Sadewa Yogyakarta.

2. TINJAUAN PUSTAKA

2.1. Keamanan Jaringan

Keamanan jaringan merupakan upaya untuk melindungi sistem jaringan dari ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan data. Pada lingkungan rumah sakit, keamanan jaringan menjadi sangat penting karena berkaitan langsung dengan data medis pasien yang bersifat rahasia [1].

2.2. Firewall

Firewall adalah perangkat keamanan jaringan yang berfungsi mengontrol lalu lintas data antara jaringan internal dan eksternal berdasarkan aturan keamanan tertentu. Firewall digunakan untuk mencegah akses tidak sah serta meminimalkan risiko serangan jaringan [2].

2.3. Firewall Hardware Fortinet

Firewall hardware Fortinet merupakan perangkat keamanan jaringan yang dirancang untuk menangani lalu lintas jaringan secara terpusat dengan performa tinggi. Fortinet menyediakan fitur keamanan seperti filtering paket data, pengaturan kebijakan keamanan, serta perlindungan terhadap serangan jaringan [3], [6].

2.4. Monitoring Jaringan

Monitoring jaringan merupakan proses pemantauan kondisi jaringan secara berkala untuk memastikan jaringan berjalan dengan stabil dan optimal. Monitoring memungkinkan administrator

jaringan mendeteksi gangguan dan melakukan evaluasi performa jaringan secara real-time [5].

2.5. Prometheus dan Grafana

Prometheus merupakan sistem monitoring berbasis time-series yang digunakan untuk mengumpulkan data metrik jaringan, sedangkan Grafana digunakan untuk menampilkan data tersebut dalam bentuk visualisasi dashboard yang informatif dan mudah dipahami [5].

2.6. Penelitian Terkait

Beberapa penelitian menunjukkan bahwa penerapan firewall hardware mampu meningkatkan keamanan dan efisiensi jaringan. Konikiewicz dan Markowski [2] menyatakan bahwa firewall hardware memiliki keunggulan performa dibandingkan firewall software, sedangkan Putra et al. [3] menunjukkan efektivitas firewall Fortinet dalam menjaga keamanan data jaringan

3. METODE PENELITIAN

3.1. Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi kasus. Metode ini dipilih untuk memperoleh pemahaman mendalam mengenai penerapan firewall hardware Fortinet pada infrastruktur jaringan rumah sakit secara nyata dan kontekstual.

3.2. Tahapan Penelitian

Tahapan penelitian diawali dengan proses mulai melalui identifikasi infrastruktur jaringan di RSKIA Sadewa Yogyakarta. Pada tahap ini dilakukan pemetaan perangkat jaringan, topologi jaringan, serta posisi firewall Fortinet dalam sistem jaringan. Tahap selanjutnya adalah analisis konfigurasi firewall Fortinet yang meliputi pengaturan kebijakan keamanan, aturan akses jaringan, serta mekanisme pengendalian lalu lintas data.

Gambar 1. Alur Penelitian Implementasi Firewall Fortinet

Setelah analisis konfigurasi dilakukan, tahap berikutnya adalah monitoring trafik jaringan menggunakan Prometheus dan Grafana untuk mengamati kondisi jaringan secara real-time, termasuk lalu lintas data masuk dan keluar serta penggunaan bandwidth. Data hasil monitoring kemudian dianalisis untuk mengevaluasi efektivitas implementasi firewall Fortinet dalam menjaga keamanan dan stabilitas jaringan. Tahapan penelitian diakhiri dengan proses selesai, yaitu penarikan kesimpulan dan penyusunan rekomendasi perbaikan jaringan.

Berdasarkan alur penelitian pada Gambar 1. Tahapan penelitian diawali dengan identifikasi infrastruktur jaringan yang bertujuan untuk mengetahui kondisi perangkat jaringan, topologi jaringan, serta posisi firewall Fortinet dalam sistem jaringan RSKIA Sadewa Yogyakarta. Tahap selanjutnya adalah analisis konfigurasi firewall Fortinet yang meliputi pengaturan kebijakan keamanan, aturan akses jaringan, dan mekanisme pengendalian lalu lintas data. Setelah konfigurasi dianalisis, dilakukan monitoring trafik jaringan untuk mengamati kondisi jaringan secara real-time, termasuk lalu lintas data masuk dan keluar serta penggunaan bandwidth. Data hasil monitoring kemudian dianalisis untuk mengevaluasi efektivitas implementasi firewall Fortinet, yang selanjutnya digunakan sebagai dasar dalam penarikan kesimpulan penelitian.

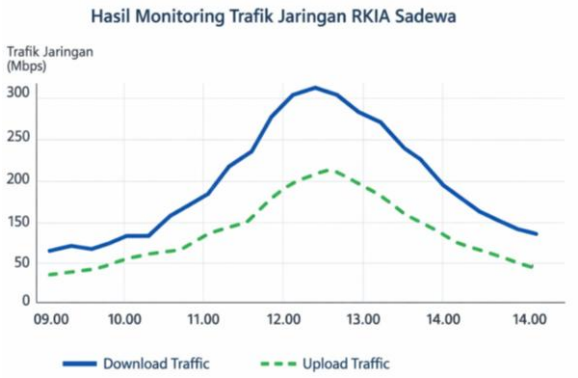
4. HASIL DAN PEMBAHASAN

4.1. Implementasi Firewall Fortinet

Firewall Fortinet diterapkan sebagai perangkat utama pengendali lalu lintas data pada jaringan RSKIA Sadewa Yogyakarta. Penerapan kebijakan keamanan dilakukan untuk membatasi akses jaringan dan mencegah potensi ancaman keamanan.

4.2. Monitoring Trafik Jaringan

Hasil monitoring menggunakan Prometheus dan Grafana menunjukkan bahwa lalu lintas jaringan berada dalam kondisi stabil dan terkontrol. Data monitoring membantu administrator jaringan dalam mengevaluasi penggunaan bandwidth serta mendeteksi potensi gangguan jaringan.

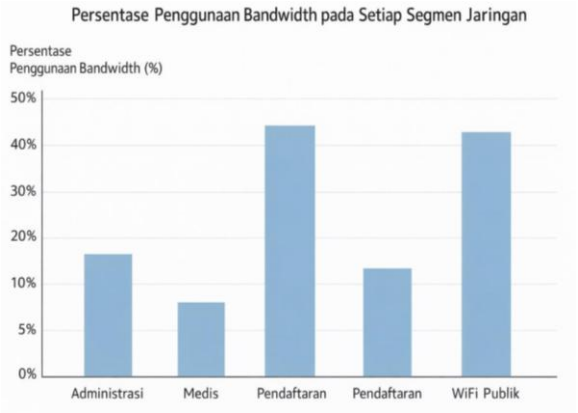


Gambar 2. Grafik Trafik Jaringan

Selain monitoring trafik secara umum, dilakukan pula analisis terhadap penggunaan bandwidth pada beberapa segmen jaringan. Hasil analisis penggunaan bandwidth ditunjukkan pada Gambar 2.

Berdasarkan Gambar 2. Terlihat bahwa segmen jaringan medis dan WiFi publik memiliki tingkat penggunaan bandwidth yang relatif tinggi dibandingkan segmen lainnya. Hal ini disebabkan oleh tingginya aktivitas pertukaran data, seperti akses sistem informasi medis, komunikasi internal, serta penggunaan internet oleh pengguna internal dan publik.

Kondisi tersebut menunjukkan bahwa meskipun firewall Fortinet telah mampu mengamankan lalu lintas data jaringan, masih diperlukan pengaturan lanjutan seperti penerapan Quality of Service (QoS) dan pemisahan segmen jaringan yang lebih optimal. Tujuannya adalah untuk memastikan bahwa layanan kritis rumah sakit tetap mendapatkan prioritas bandwidth yang memadai tanpa terganggu oleh aktivitas jaringan lain.



Gambar 3. Monitoring Penggunaan Bandwidth Jaringan

Berdasarkan hasil monitoring dan analisis jaringan yang dilakukan, dapat disimpulkan bahwa implementasi firewall Fortinet di RKIA Sadewa Yogyakarta telah berfungsi dengan baik sebagai sistem pengamanan jaringan. Firewall mampu mengontrol lalu lintas data serta membantu menjaga stabilitas jaringan selama jam operasional.

Namun demikian, hasil analisis juga menunjukkan bahwa masih terdapat beberapa aspek yang perlu ditingkatkan, terutama dalam hal pengelolaan bandwidth dan pemisahan segmen jaringan. Dengan optimalisasi konfigurasi firewall, penerapan manajemen bandwidth, serta segmentasi jaringan yang lebih baik, diharapkan kinerja dan keamanan jaringan rumah sakit dapat semakin meningkat.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa implementasi firewall hardware Fortinet pada infrastruktur jaringan RSKIA Sadewa Yogyakarta mampu meningkatkan keamanan dan stabilitas jaringan. Firewall Fortinet berperan penting dalam mengendalikan lalu lintas data serta membantu mencegah potensi ancaman keamanan jaringan. Dukungan sistem monitoring jaringan menggunakan Prometheus dan Grafana juga memudahkan administrator jaringan dalam melakukan pemantauan dan evaluasi kondisi jaringan secara real-time.

Meningkatkan kinerja jaringan secara optimal, disarankan agar dilakukan pengelolaan bandwidth yang lebih baik serta penerapan segmentasi jaringan yang lebih terstruktur. Optimalisasi konfigurasi firewall dan penerapan Quality of Service (QoS) diharapkan dapat meningkatkan efisiensi penggunaan jaringan, khususnya untuk layanan kritis rumah sakit. Penelitian selanjutnya dapat mengkaji pengujian performa jaringan secara kuantitatif untuk memperoleh hasil yang lebih terukur.

DAFTAR PUSTAKA

[1] A. Alshamrani, S. Myneni, and A. Chowdhary, “Network security monitoring and analysis using firewall and intrusion detection systems,” *IEEE Access*, vol. 8, pp. 123456–123468, 2020.

[2] M. H. Alsharif, M. K. Hasan, and J. Kim, “Network traffic monitoring and analysis for healthcare systems,” *Sensors*, vol. 21, no. 12, pp. 1–18, 2021.

[3] F. R. Arbie and M. Raharjo, “Implementasi keamanan jaringan menggunakan Fortigate,” *Jurnal Informatika Terpadu*, vol. 10, no. 1, pp. 27–34, 2024.

[4] D. B. Radityo and A. Rustianto, “Peningkatan efisiensi jaringan internet menggunakan firewall Fortigate,” *Journal of Digital Business and Technology Innovation (DBESTI)*, vol. 2, no. 1, pp. 96–102, 2025.

[5] F. P. E. Putra, M. Dafid, and I. Syafi’i, “Firewall implementation as a computer network security strategy for data protection,” *Brilliance: Research of Artificial Intelligence*, vol. 5, no. 1, pp. 291–299, 2025.

[6] A. Kumar and R. Singh, “Network security architecture in healthcare information systems,” *International Journal of Information Security Science*, vol. 9, no. 2, pp. 45–56, 2020.

[7] S. Behl, “Cybersecurity challenges in healthcare digital transformation,” *Journal of Healthcare Informatics Research*, vol. 5, no. 3, pp. 215–229, 2021.

[8] L. Zhang, Y. Wang, and X. Chen, “Firewall performance evaluation in enterprise networks,” *International Journal of Network Management*, vol. 31, no. 4, pp. 1–12, 2021.

[9] R. P. Mahajan and A. Verma, "Security assessment of firewall systems in hospital networks," *Journal of Medical Systems*, vol. 46, no. 5, pp. 1–10, 2022.

[10] T. H. Nguyen and D. Kim, "Network security management using hardware firewall in healthcare environments," *Applied Sciences*, vol. 13, no. 2, pp. 1–15, 2023.