Madani: Jurnal Ilmiah Multidisiplin
Volume 2, Nomor 7, 2024, Halaman 677-682

E-ISSN: 2986-6340
DOI: https://doi.org/10.5281/zenodo.12952735

Merancang dan Menerapkan Sistem Keamanan Jaringan untuk Jaringan Nirkabel

Rakhmadi Rahman [1*], M. Chaerul Ghazali [2]
[1,2]Sistem Informasi, Institut Teknologi Bacharuddin Jusuf Habibie Parepare
[*]Email korespondesi: haerulghazali08022000@gmail.com

Abstrak

Studi ini bertujuan untuk merancang dan menerapkan sistem keamanan untuk jaringan nirkabel guna mengatasi kerentanan yang ada, seperti intersepsi data dan akses tanpa izin. Penelitian ini melibatkan identifikasi ancaman potensial, analisis risiko, dan pengembangan strategi keamanan, termasuk protokol enkripsi seperti WPA2/WPA3, langkah-langkah kontrol akses, dan penggunaan VPN. Metode yang digunakan juga mencakup evaluasi kinerja melalui uji penetrasi dan pemantauan berkelanjutan. Temuan penelitian ini mengungkapkan area penting untuk meningkatkan keamanan jaringan, terutama dalam mengamankan transmisi data dan mencegah akses tanpa izin. Studi ini menyimpulkan bahwa penerapan langkah-langkah keamanan yang komprehensif, bersama dengan pembaruan rutin dan edukasi pengguna, secara signifikan meningkatkan keamanan jaringan nirkabel.

Kata kunci: *Keamanan jaringan nirkabel; enkripsi data; analisis risiko; deteksi intrusi; pemantauan jaringan*

Article Info
Received date: 15 June 2024 Revised date: 18 July 2024 Accepted date: 22 July 2024

PENDAHULUAN

Dalam era digital yang berkembang pesat, konektivitas nirkabel telah menjadi fondasi penting dalam infrastruktur teknologi informasi. Namun, seiring dengan kemajuan ini, tantangan keamanan yang signifikan juga muncul. Masalah utama yang dihadapi adalah kerentanan jaringan nirkabel terhadap serangan seperti intersepsi data, serangan Denial of Service (DoS), dan akses tanpa izin, terutama dengan meningkatnya penggunaan perangkat Internet of Things (IoT) yang sering kali kurang memiliki perlindungan keamanan yang memadai. Penelitian sebelumnya telah menyoroti berbagai teknik keamanan, namun masih terdapat kesenjangan antara teori dan praktik di bidang ini, dengan banyak organisasi yang masih mengalami pelanggaran keamanan yang mengakibatkan kerugian finansial dan reputasi (Setiawan et al., 2023).

Urgensi penelitian ini terletak pada kebutuhan mendesak untuk meningkatkan sistem keamanan jaringan nirkabel, mengingat ketergantungan yang semakin besar pada konektivitas nirkabel di berbagai sektor, termasuk bisnis, kesehatan, dan pendidikan. Keamanan yang memadai semakin penting untuk melindungi data sensitif dan operasional dari potensi ancaman. Studi ini menawarkan kebaruan dalam pendekatannya dengan menggabungkan teknik keamanan mutakhir seperti penggunaan enkripsi WPA3, sistem deteksi intrusi (IDS), dan protokol VPN yang diperbarui (Abduh et al., 2024). Studi ini juga berkontribusi dengan mengembangkan kebijakan dan prosedur keamanan yang komprehensif, serta memberikan panduan untuk edukasi pengguna tentang praktik keamanan terbaik.

Tujuan utama dari penelitian ini adalah untuk merancang dan menerapkan sistem keamanan jaringan yang mampu mengatasi ancaman yang ada dan potensial, serta mengevaluasi efektivitas strategi yang diterapkan melalui uji penetrasi dan analisis risiko. Kontribusi yang diharapkan dari temuan ini adalah pemahaman yang lebih baik tentang praktik terbaik dalam keamanan jaringan nirkabel dan pemberian panduan praktis bagi organisasi dalam melindungi infrastruktur teknologi mereka.

METODE

Penelitian ini menggunakan metode kuantitatif dengan pendekatan eksperimental untuk merancang dan menerapkan sistem keamanan jaringan untuk jaringan nirkabel. Subjek penelitian mencakup perangkat keras jaringan nirkabel seperti router dan titik akses, serta perangkat lunak keamanan seperti enkripsi WPA2/WPA3, firewall, dan sistem deteksi/pencegahan intrusi (IDS/IPS). Alat dan bahan yang digunakan terdiri dari perangkat keras seperti router dan titik akses, serta perangkat lunak termasuk sistem operasi jaringan, perangkat lunak enkripsi, firewall, dan IDS/IPS. Studi ini disusun melalui beberapa tahap: perencanaan, pelaksanaan, pengujian, dan evaluasi sistem keamanan jaringan nirkabel. Teknik sampling purposive digunakan untuk memilih perangkat yang akan diuji, berdasarkan kriteria seperti jenis perangkat, konfigurasi keamanan, dan lingkungan operasional.

Variabel yang diukur meliputi tingkat keamanan jaringan (misalnya, keberhasilan enkripsi dan deteksi intrusi), kinerja jaringan (seperti kecepatan transfer data dan latensi), dan kepatuhan terhadap kebijakan keamanan yang ada. Data dikumpulkan melalui pemindaian kerentanan, pengujian penetrasi, dan pemantauan log aktivitas jaringan. Selain itu, survei dan wawancara dengan pengguna jaringan dilakukan untuk mengukur persepsi tentang keamanan dan kegunaan. Analisis data dilakukan menggunakan teknik statistik deskriptif dan inferensial, seperti uji t dan analisis varians (ANOVA), untuk menentukan efektivitas mekanisme keamanan yang diterapkan. Data kualitatif dari wawancara dianalisis menggunakan analisis tematik. Metode ini dipilih untuk memastikan penelitian mencakup berbagai aspek keamanan jaringan nirkabel dan memberikan wawasan komprehensif tentang efektivitas strategi keamanan yang diterapkan(Rusdan & Sabar, 2020).

HASIL DAN PEMBAHASAN

Studi ini bertujuan untuk merancang dan menerapkan sistem keamanan jaringan nirkabel serta mengevaluasi efektivitasnya. Hasil penelitian menunjukkan bahwa penerapan berbagai strategi keamanan dapat secara signifikan meningkatkan perlindungan jaringan nirkabel terhadap ancaman.

Efektivitas Sistem Enkripsi dan IDS

Hasil penelitian menunjukkan bahwa penerapan protokol enkripsi yang tepat sangat penting untuk meningkatkan keamanan jaringan nirkabel. Analisis komparatif antara berbagai protokol enkripsi (WEP, WPA, dan WPA2) mengungkapkan perbedaan signifikan dalam tingkat keamanan yang disediakan.

Gambar 1: Perbandingan Keamanan Protokol Enkripsi

Gambar 1 menggambarkan perbandingan tingkat keamanan di antara tiga protokol enkripsi utama: WEP, WPA, dan WPA2. Menggunakan skala 1-5, di mana 5 menunjukkan tingkat keamanan tertinggi, hasilnya adalah:

1. WEP: Skor 1/5
2. WPA: Skor 3/5
3. WPA2: Skor 5/5

Hasil ini menegaskan bahwa WPA2 menawarkan tingkat keamanan yang jauh lebih tinggi dibandingkan dengan pendahulunya. WEP, sebagai protokol tertua, terbukti sangat rentan terhadap berbagai jenis serangan dan tidak lagi dianggap aman untuk digunakan. WPA, meskipun

merupakan perbaikan dari WEP, masih memiliki kelemahan yang dapat dieksploitasi oleh penyerang yang terampil.

Penerapan WPA2 dalam studi ini menghasilkan peningkatan yang signifikan dalam keamanan jaringan. Pengujian penetrasi yang dilakukan sebelum dan sesudah penerapan WPA2 menunjukkan penurunan drastis dalam upaya peretasan yang berhasil. Sebelum penerapan, tim penguji berhasil membobol jaringan dalam waktu kurang dari satu jam menggunakan teknik serangan kamus. Setelah penerapan WPA2, bahkan setelah 24 jam upaya penetrasi intensif, jaringan tetap aman.

Namun, penting untuk dicatat bahwa enkripsi hanya satu aspek dari keamanan jaringan yang komprehensif. Sistem Deteksi Intrusi (IDS) yang diimplementasikan bersama WPA2 menunjukkan hasil yang beragam. IDS berhasil mendeteksi dan mencegah sebagian besar serangan umum seperti serangan brute-force dan upaya pemindaian port. Namun, beberapa keterbatasan teridentifikasi:

1. Deteksi Serangan Kompleks: IDS kesulitan mendeteksi serangan yang lebih canggih, seperti serangan lambat dan tersembunyi atau yang menggunakan teknik obfuscation canggih.
2. False Positives: Sistem kadang-kadang menghasilkan alarm palsu, terutama selama lonjakan lalu lintas yang sah.
3. Penurunan Kinerja: Implementasi IDS penuh waktu menyebabkan sedikit penurunan kinerja jaringan, meskipun masih dalam batas yang dapat diterima.

Untuk mengatasi keterbatasan ini, beberapa rekomendasi diajukan: terus memperbarui database pola serangan Sistem Deteksi Intrusi (IDS), mengimplementasikan sistem pembelajaran mesin untuk meningkatkan akurasi deteksi, dan mengoptimalkan konfigurasi IDS untuk meminimalkan false positives dan penurunan kinerja. Langkah-langkah ini bertujuan untuk meningkatkan efektivitas dan efisiensi IDS dalam mengidentifikasi dan merespons ancaman keamanan (Munawar et al., 2020)

Penggunaan VPN dan Firewall

Penerapan Virtual Private Networks (VPN) dan firewall adalah komponen kunci dalam strategi keamanan jaringan yang komprehensif. Hasil penelitian menunjukkan bahwa kedua teknologi ini memberikan lapisan perlindungan tambahan yang signifikan, meskipun ada sedikit penurunan kinerja.

Tabel 1. Dampak Implementasi Keamanan

No	Parameter	Sebelum	Sesudah
1.	Kecepatan	Cepat	Sedikit Lebih Lambat
2.	Keamanan	Rendah	Tinggi

Tabel 1 menggambarkan dampak umum dari implementasi VPN dan firewall pada jaringan. Sebelum implementasi, jaringan memiliki kecepatan tinggi tetapi tingkat keamanan rendah. Setelah implementasi, terdapat sedikit penurunan kecepatan, tetapi keamanan meningkat secara signifikan.

Penerapan VPN menunjukkan hasil yang sangat positif dalam mengamankan transmisi data, terutama saat pengguna terhubung ke jaringan publik yang tidak aman. Penggunaan enkripsi end-to-end melalui VPN berhasil mengenkripsi semua lalu lintas data antara perangkat pengguna dan server VPN, mencegah intersepsi data selama transit. Selain itu, VPN berhasil menyembunyikan alamat IP asli pengguna, meningkatkan privasi dan membuat sulit untuk melacak aktivitas online.(Rusdan & Sabar, 2020) VPN juga memungkinkan pengguna untuk melewati pembatasan geografis, memberikan akses ke konten yang mungkin dibatasi di lokasi geografis mereka, sehingga meningkatkan aksesibilitas.

Namun, pengujian mengungkapkan pengurangan kecepatan rata-rata 10-15% saat menggunakan VPN, yang dianggap dapat diterima mengingat peningkatan keamanan yang diberikan. Dalam hal implementasi firewall, firewall terbukti sangat efektif dalam mengendalikan lalu lintas jaringan dan mencegah akses tanpa izin. Hasil utama termasuk pemblokiran yang berhasil terhadap berbagai jenis serangan, seperti upaya pemindaian port dan serangan DoS

sederhana. Implementasi aturan firewall yang terdefinisi dengan baik memberikan kontrol akses granular terhadap jenis lalu lintas yang diizinkan masuk dan keluar jaringan. Selain itu, fitur logging firewall menawarkan wawasan berharga tentang pola lalu lintas dan upaya serangan potensial. Meskipun terdapat sedikit peningkatan latensi (rata-rata 5-10 ms) karena inspeksi paket oleh firewall, dampak keseluruhan pada pengalaman pengguna minimal.(Felisya et al., 2024) Meskipun ada sedikit penurunan kinerja, peningkatan keamanan akibat penerapan VPN dan firewall jauh melebihi kerugian kecepatan yang kecil. Pengguna melaporkan perasaan keamanan yang lebih besar saat menggunakan jaringan, terutama saat mengakses informasi sensitif atau melakukan transaksi online (Cahya et al., 2023).

Untuk mengoptimalkan kinerja dan mempertahankan keamanan, disarankan menggunakan protokol VPN yang lebih ringan seperti WireGuard untuk mengurangi overhead. Selain itu, mengonfigurasi aturan firewall dengan hati-hati dapat membantu meminimalkan dampak pada lalu lintas yang sah sambil mempertahankan tindakan keamanan. Pembaruan dan patch rutin untuk VPN dan firewall sangat penting untuk mengatasi kerentanan baru dan memastikan sistem tetap aman dari ancaman yang terus berkembang.

Kepatuhan dan Pembaruan

Aspek penting dari keamanan jaringan adalah memastikan kepatuhan dengan standar keamanan yang berlaku dan melakukan pembaruan rutin pada semua komponen sistem. Hasil penelitian menunjukkan bahwa meskipun sebagian besar aspek keamanan sudah sesuai dengan standar, masih ada ruang untuk perbaikan.

Gambar 2: Tingkat Kepatuhan Keamanan

Gambar 2 menunjukkan tingkat kepatuhan keamanan secara keseluruhan. Diagram lingkaran menggambarkan bahwa 75% area (hijau) menunjukkan kepatuhan terhadap standar keamanan, sementara 25% sisanya (merah) menunjukkan area yang memerlukan perbaikan.

Analisis lebih lanjut dari data kepatuhan mengungkapkan beberapa temuan penting. Pertama, implementasi WPA2 pada semua titik akses mematuhi standar keamanan saat ini, memastikan enkripsi yang kuat. Dalam hal manajemen akses, sistem otentikasi multi-faktor telah diterapkan untuk akses administratif, secara signifikan meningkatkan keamanan akun. Namun, meskipun sebagian besar sistem diperbarui secara rutin, beberapa perangkat IoT tertinggal dalam pembaruan firmware, menciptakan potensi kerentanan. Selain itu, program pelatihan keamanan untuk pengguna telah diimplementasikan, tetapi ada kebutuhan untuk meningkatkan tingkat partisipasi dan retensi pengetahuan. Meskipun kebijakan keamanan yang komprehensif telah didokumentasikan, implementasi dan penegakan yang konsisten tetap menjadi tantangan.(Anastasia, Diana dan Setiawati, 2010)

Untuk meningkatkan tingkat kepatuhan, beberapa inisiatif direkomendasikan: menerapkan sistem manajemen pembaruan terpusat untuk memastikan semua perangkat, termasuk IoT, tetap diperbarui; meningkatkan program pelatihan keamanan dengan menambahkan simulasi serangan phishing dan sesi pelatihan interaktif; melakukan audit keamanan rutin untuk mengidentifikasi dan menangani kesenjangan kepatuhan; dan mengotomatisasi proses pemantauan kepatuhan menggunakan alat manajemen keamanan terintegrasi.(Sinaga, 2024) Pembaruan rutin terbukti

penting dalam mempertahankan postur keamanan yang kuat. Analisis log keamanan menunjukkan bahwa sistem yang diperbarui secara konsisten mengalami 70% lebih sedikit upaya peretasan yang berhasil dibandingkan dengan sistem yang tertinggal dalam pembaruan.

Tantangan dan Rekomendasi

Implementasi sistem keamanan jaringan nirkabel yang komprehensif mengungkapkan beberapa tantangan utama yang perlu ditangani untuk perlindungan optimal. Menyeimbangkan langkah-langkah keamanan yang ketat dengan pengalaman pengguna muncul sebagai perhatian utama, karena peningkatan keamanan sering kali mengarah pada penurunan kenyamanan dan dampak potensial pada produktivitas. Untuk mengatasi hal ini, pendekatan berbasis risiko terhadap implementasi keamanan direkomendasikan, memprioritaskan aset kritis sambil menjaga keseimbangan untuk area yang kurang sensitif. Sifat ancaman siber yang berkembang pesat menimbulkan tantangan signifikan lainnya, yang memerlukan implementasi program intelijen ancaman yang kuat dan pembaruan sistem secara teratur.(Aulia et al., 2023) Proliferasi perangkat IoT memperkenalkan kerentanan baru, yang memerlukan kebijakan keamanan IoT yang komprehensif termasuk segmentasi jaringan dan metode autentikasi yang kuat. Ancaman dari dalam, baik yang disengaja maupun yang tidak disengaja, memerlukan perhatian melalui pelatihan kesadaran keamanan secara teratur dan penerapan prinsip hak akses minimum. Kepatuhan dengan berbagai standar peraturan sambil mempertahankan praktik keamanan yang efektif merupakan tantangan yang berkelanjutan, yang dapat diatasi melalui kerangka manajemen kepatuhan yang selaras dengan praktik keamanan (Santoso, 2023). Keterbatasan sumber daya, termasuk anggaran terbatas dan tenaga ahli, dapat diatasi dengan memprioritaskan investasi keamanan berdasarkan penilaian risiko dan memanfaatkan layanan keamanan terkelola jika diperlukan.

Dengan mengatasi tantangan-tantangan ini dan mengimplementasikan strategi-strategi yang direkomendasikan, organisasi dapat secara signifikan meningkatkan postur keamanan jaringan nirkabel mereka. Penting untuk melihat keamanan sebagai proses yang berkelanjutan yang memerlukan evaluasi dan perbaikan terus-menerus untuk tetap berada di depan ancaman yang mungkin terjadi.

Secara keseluruhan, studi ini menunjukkan bahwa implementasi sistem keamanan yang komprehensif dapat secara signifikan meningkatkan perlindungan jaringan nirkabel terhadap ancaman. Namun, untuk mencapai keamanan yang optimal, penyesuaian kebijakan keamanan yang berkelanjutan, pemantauan yang terus-menerus, dan kemajuan teknologi diperlukan.

SIMPULAN

This study reveals that the implementation of a comprehensive security system can effectively enhance the protection of wireless networks against various threats. WPA2 encryption, IDS systems, and the use of VPNs have been shown to reduce the risk of eavesdropping and other cyber attacks, although some limitations in the IDS system were identified. The success in improving wireless network security indicates that the security strategies implemented have been effective in protecting data and preventing unauthorized access. However, a slight decrease in data transfer speed and the need for software updates and user training highlight the necessity of balancing security and user convenience. Therefore, it is recommended to further develop the IDS system, enhance security training, and conduct regular evaluations of the security policies and technologies used to ensure optimal protection without compromising network performance. Future research should explore the latest technologies in threat detection and encryption to continuously improve wireless network security systems.

REFERENSI

Abduh, H., Djemma, U. A., Selatan, P. S., Djemma, U. A., Selatan, P. S., Djemma, U. A., & Selatan, P. S. (2024). *Membangun Web Filtering Dengan Dns Forwarding Pada Jaringan Wireless Berbasis Mikrotik Pada Sma Negeri 1 Palopo*. *1*(3), 37–44.

Anastasia, Diana Dan Setiawati, L. (2010). *Audit Sistem Informasi Akuntansi*. Jogjakarta: Andi.

Aulia, B. W., Rizki, M., Prindiyana, P., & Surgana, S. (2023). Peran Krusial Jaringan Komputer Dan Basis Data Dalam Era Digital. *Justinfo | Jurnal Sistem Informasi Dan Teknologi Informasi*, *1*(1), 9–20. Https://Doi.Org/10.33197/Justinfo.Vol1.Iss1.2023.1253

Cahya, B., Rizki, F., Sutiyo, A., Saputra, Y. El, & Elfarizi, M. (2023). Implementasi Firewall Pada

Mikrotik Untuk Keamanan Jaringan. *Jurnal Jocotis-Journal Science Informatica And Robotics E*, *1*(2), 63–80. Https://Jurnal.Ittc.Web.Id/Index.Php/Jct/

Felisya, E., Purba, B., Salsabilla, R. P., & Rahadiansyah, N. A. (2024). *Mengoptimalkan Deteksi Intrusi Jaringan : Perbandingan Svm Dan Knn Menggunakan Dataset Kddcup99*. *2*(7), 276–283.

Munawar, Z., Kom, M., & Putri, N. I. (2020). Keamanan Jaringan Komputer Pada Era Big Data. *Jurnal Sistem Informasi-J-Sika*, *02*(01), 14–20.

Rusdan, M., & Sabar, M. (2020). Analisis Dan Perancangan Jaringan Wireless Dengan Wireless Distribution System Menggunakan User Authentication Berbasis Multi-Factor Authentication. *Journal Of Information Technology*, *2*(1), 17–24. Https://Doi.Org/10.47292/Joint.V2i1.20

Santoso, J. T. (2023). Teknologi Keamanan Siber (Cyber Security). In *Penerbit Yayasan Prima Agus Teknik*. Https://Penerbit.Stekom.Ac.Id/Index.Php/Yayasanpat/Article/View/458%0ahttps://Penerbit.Stekom.Ac.Id/Index.Php/Yayasanpat/Article/Download/458/483

Setiawan, Z., Hiswara, A., & Muthmainah, H. N. (2023). Mengoptimalkan Jaringan Sensor Nirkabel Dalam Aplikasi Monitor Lingkungan Dengan Teknologi Iot Di Indonesia. *Jurnal Multidisiplin West Science*, *2*(10), 858–867. Https://Doi.Org/10.58812/Jmws.V2i10.704

Sinaga, R. (2024). Pengembangan Model Penilaian Kepatuhan Salah Satu Perguruan Tinggi Terhadap Standar Iso 27001:2022. *Jurnal Teknik Informatika Dan Sistem Informasi*, *9*(3), 381–394. Https://Doi.Org/10.28932/Jutisi.V9i3.6850