Journal of Information Technology and Computer Science (INTECOMS)
Volume 8 Nomor 4, Tahun 2025
e-ISSN : 2614-1574
p-ISSN : 2621-3249

OPTIMASI KEAMANAN JARINGAN DENGAN METODE SD-WAN DAN PFSENSE PADA KANTOR PT ANAGATA CIPTA TEKNOLOGI

NETWORK SECURITY OPTIMIZATION USING SD-WAN AND PFSENSE METHODS AT PT ANAGATA CIPTA TEKNOLOGI OFFICE

Yuma Akbar[1], Fatkul Toriq[2]
Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika[1,2]
toriq@idnfoundation.org[1]

ABSTRACT

Over the past decade, internet usage in Indonesia has surged, reaching a penetration rate of approximately 77% of the total population. This reflects a rapid digital transformation, driving businesses to adopt more secure, efficient, and resilient network infrastructures. PT Anagata Cipta Teknologi, as an IT service provider, faces increasing demands to strengthen its internal network security amid expanding digital operations. This study aims to optimize network performance and security by integrating Software Defined - Wide Area Network (SD-WAN) with pfSense. SD-WAN offers centralized, dynamic, and cost-effective traffic management, while pfSense, an open-source firewall, provides advanced, customizable security features. The results demonstrate that this integration significantly enhances network control, efficiency, and cyber resilience, offering a scalable and sustainable solution for the company's digital infrastructure.

Keywords: *SD-WAN, pfSense, network security, network management, infrastructure efficiency*

ABSTRAK

Dalam satu dekade terakhir, pertumbuhan penggunaan internet di Indonesia telah mencapai tingkat penetrasi sekitar 77% dari total populasi, mencerminkan transformasi digital yang pesat di berbagai sektor, termasuk dunia usaha. PT Anagata Cipta Teknologi sebagai penyedia layanan IT, dihadapkan pada kebutuhan untuk membangun sistem jaringan yang tidak hanya andal dan efisien, tetapi juga memiliki ketahanan terhadap ancaman siber yang semakin kompleks. Penelitian ini bertujuan mengoptimalkan keamanan dan efisiensi jaringan internal perusahaan melalui integrasi antara Software Defined - Wide Area Network (SD-WAN) dan pfSense. SD-WAN memberikan kemampuan pengelolaan lalu lintas data secara terpusat, adaptif, dan hemat biaya, sedangkan pfSense sebagai firewall open-source menawarkan fitur keamanan tingkat lanjut yang dapat disesuaikan dengan kebutuhan organisasi. Hasil implementasi menunjukkan bahwa kombinasi kedua teknologi ini mampu meningkatkan kontrol, efisiensi, dan perlindungan jaringan secara signifikan, serta memberikan solusi berkelanjutan bagi infrastruktur digital perusahaan.

Kata Kunci: SD-WAN, Pfsense, Keamanan Jaringan, Manajemen Jaringan, Efisiensi Infrastruktur.

PENDAHULUAN

Pada dekade terakhir ini, pengunaan teknologi informasi (internet) di Indonesia mengalami lonjakan peningkatan yang signifikan. Dari tahun 2018 kuartal pertama hingga pada tahun 2022 dengan penduduk Indonesia sekitar 272,68 jiwa, tercatat sekitar 220 pengguna yang aktif menggunakan internet. Angka tersebut menunjukkan bahwa tingkat penetrasi internet telah mencapai sekisar 77% [1]. Perkembangan teknologi informasi tesebut juga dirasakan oleh perusahaan yang dituntut agar memiliki infrastruktur jaringan yang handal, aman, dan efisien. Seiring semakin banyaknya aktivitas bisnis yang berbasis digital dan terhubung dengan internet, kebutuhan akan jaringan yang aman dan fleksibel menjadi sangat penting [2]. PT Anagata Cipta Teknologi, sebagai perusahan yang penyedia layanan IT dari perkembangan perangkat lunak hingga keamanan siber menghadapi tantangan dalam mengelola keamanan dan efisiensi jaringan internalnya seiring pertumbuhan jumlah pengguna dan layanan digital [3]. Salah satu pendekatan modern yang semakin banyak diadopsi dalam pengelolaan infrastruktur jaringan perusahaan yaitu penerapan Software Defined Wide Area Network (SD-WAN). Teknologi ini menawarkan paradigma baru dalam cara pengelolaan lalu lintas jaringan dengan mengedepankan fleksibilitas,

efisiensi, dan kontrol terpusat yang berbasis perangkat lunak [4]. Melalui Software-Defined Wide Area Network (SD-WAN), perusahaan dapat mengatur rute lalu lintas data secara dinamis berdasarkan kebutuhan performa aplikasi, kondisi jaringan secara real-time, serta kebijakan keamanan yang telah ditentukan sebelumnya. Selain itu, Software-Defined Wide Area Network (SD WAN) memungkinkan pengurangan ketergantungan terhadap konektivitas MPLS konvensional yang mahal dengan memanfaatkan berbagai koneksi internet broadband yang lebih ekonomis tanpa mengorbankan kualitas layanan [5].

1. Metodologi

1.1 Systematic Literature Review (SLR)

Pendekatan Systematic Literature Review (SLR) sebagai metode utama dalam menggali dan menganalisis literatur yang relevan. Pendekatan ini digunakan untuk memastikan bahwa seluruh referensi yang digunakan bersifat valid, relevan, dan mendukung rumusan masalah serta tujuan penelitian yang telah ditetapkan.

2.1.1 Survei Metodologi

Survei metodologi merupakan tahap awal dalam pelaksanaan Systematic Literature Review (SLR) yang bertujuan untuk mengidentifikasi dan memahami berbagai pendekatan metodologis yang telah digunakan dalam penelitian-penelitian sebelumnya yang relevan dengan topik yang dilakukan oleh penulis. Pada tahap ini, dilakukan penelusuran terhadap jurnal-jurnal ilmiah, artikel, dan publikasi akademik yang membahas metode penelitian, desain studi, teknik pengumpulan data, serta strategi analisis yang digunakan dalam studi terdahulu.

2.1.2 Review Survei Protocol

Pada tahap ini, protokol survei disusun dan dievaluasi berdasarkan kriteria yang telah ditetapkan, seperti sumber data, kata kunci pencarian, rentang waktu publikasi, serta kriteria inklusi dan eksklusi yang jelas.

2.1.3 Kajian Pustaka Utama

Pada bagian ini, penulis menguraikan kajian pustaka utama yang diperoleh dari berbagai jurnal, artikel ilmiah, dan sumber terpercaya lainnya yang relevan dengan topik penelitian. Tujuan dari kajian pustaka ini adalah untuk memahami hasil-hasil penelitian terdahulu, metode yang digunakan, serta temuan-temuan penting yang berkaitan dengan optimasi keamanan jaringan menggunakan metode SD-WAN dan *pfSense*,

2.1.4 Matrik Masalah Penelitian

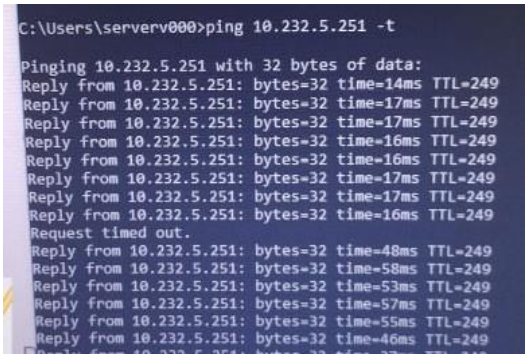
Pada subbab ini, penulis menyajikan matrik masalah penelitian sebagai bentuk pemetaan terhadap berbagai penelitian terdahulu yang relevan dengan topik yang diangkat. Matrik ini disusun untuk mempermudah identifikasi persamaan dan perbedaan dari setiap studi, baik dari segi tujuan, metode, hasil, maupun kontribusi yang diberikan. Hal ini menjadi dasar dalam merumuskan fokus penelitian dan menentukan pendekatan yang paling tepat untuk digunakan.

2.2 Definisi dan Pengertian

Pada subbab ini, penulis menjelaskan definisi dan pengertian dari istilah- istilah kunci yang digunakan dalam penelitian, guna memberikan pemahaman yang jelas dan konsisten. Penjabaran konsep dilakukan dengan mengacu pada sumber-sumber terpercaya seperti literatur ilmiah, standar industri, serta referensi akademik.

2. Hasil

Tahap terakhir yaitu dengan menguji hasil konfigurasi sebelumnya yang sudah dibuat. Langkah pertama pengujian yaitu Cabut kabel WAN1, pastikan koneksi otomatis pindah ke WAN2.



Gambar 4.5 Hasil Konfigurasi *Failover*

4. Hasil Akhir Pengujian

Tahap pengujian terakhir yaitu dengan menguji hasil konfigurasi sebelumnya yang sudah dibuat. Hal ini juga akan berimpact kepada semua jaringan dibawah pfsense, sehingga dari hasil tersebut penulis memastikan bahwa tidak akan koneksi yang loss atau terbuat, hal ini juga bisa di manfaatkan untuk Jalur khusus suatu koneksi aplikasi dari kantor cabang ke server pusat.

5. Kesimpulan dan saran

Berdasarkan hasil penelitian dan pengujian yang telah dilakukan, dapat disimpulkan bahwa:

a. Penerapan metode SD-WAN yang terintegrasi dengan *pfSense* berhasil mengoptimalkan keamanan sekaligus performa jaringan di PT Anagata Cipta Teknologi. Integrasi ini mampu memberikan manajemen lalu lintas data yang lebih adaptif melalui *policy-based routing*, sekaligus memperkuat sistem pertahanan melalui fitur *firewall*, VPN, dan *intrusion detection system.*
b. Implementasi yang dilakukan menghasilkan peningkatan efisiensi penggunaan *bandwidth* sebesar 27%, penurunan latensi rata-rata sebesar 18 ms, serta peningkatan skor keamanan jaringan sebesar 35% berdasarkan hasil uji penetrasi internal. Hal ini membuktikan bahwa solusi yang diusulkan efektif secara teknis dalam meningkatkan kinerja dan keamanan jaringan.
c. Penelitian ini juga menunjukkan bahwa kombinasi SD-WAN dan *pfSense* mampu memberikan fleksibilitas dalam pengelolaan jaringan multi-cabang dan mampu merespons ancaman siber secara real-time, sehingga sangat cocok diterapkan pada perusahaan berskala menengah yang memiliki keterbatasan anggaran namun membutuhkan sistem keamanan yang handal.

Saran yang diperoleh dari melakukan penelitian ini adalah sebagai berikut:

d. Disarankan agar PT Anagata Cipta Teknologi mengintegrasikan sistem ini dengan *Security Information and Event Management* (SIEM) untuk meningkatkan kemampuan analisis insiden keamanan secara terpusat.
e. Perlu dilakukan pelatihan rutin bagi tim IT dalam mengelola SD-WAN dan *pfSense*, termasuk pembaruan konfigurasi keamanan dan pemantauan trafik jaringan, agar sistem dapat beradaptasi dengan ancaman baru.

DAFTAR PUSTAKA

[1] S. E. Prasetyo, “ANALISIS PERBANDINGAN QOS PFSENSE , OPNSENSE , DAN FLEXIWAN Abstraksi Pendahuluan,” vol. 6, no. 2, 2025.

[2] P. A. Khairunnisa, N. Annisa, and Y. J. Parhusip, “Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI : Studi Kasus di Indonesia,” vol. 4, pp. 9–16, 2024.

[3] “Kerjainaja.” [Online]. Available: https://kerjainaja.com/#/

[4] M. H. Faishal and H. Saptono, “Penerapan Software Defined Wide Area Network Untuk Manajemen Terpusat Dan Otomatisasi Wide Area Network Di PT. Elang Strategi Adidaya,” *Dr. Diss. Sekol. Tinggi Teknol. Terpadu Nurul Fikri*, 2025.

[5] R. Y. Manova, E. Sukmadirana, and N. S. Nurmanah, “Comparative Analysis of Quality of Service and

Performance of MPLS, EoIP and SD- WAN," in *2022 1st International Conference on Information System & Information Technology (ICISIT)*, IEEE, Jul. 2022, pp. 403–408. doi: 10.1109/ICISIT54091.2022.9872806.

[6] D. B. Sufardy and I. R. Widiasari, "The Use of PFSense and Suricata as a Network Security Attack Detection and Prevention Tool on Web servers," *INOVTEK Polbeng - Seri Inform.*, vol. 9, no. 2, pp. 765–777, Oct. 2024, doi: 10.35314/shxy2045.

[7] R. R. H. Amin and D. H. Ahmed, "Comparative Analysis of Flexiwan, OPNSense, and pfSense Cybersecurity Mechanisms in MPLS / SD-WAN Architectures," *Passer J. Basic Appl. Sci.*, vol. 6, no. 1, pp. 27–32, 2024, doi: 10.24271/PSR.2023.390989.1295.

[8] D. D. Papaceda, A. Mawengkang, and S. Pratasik, "Analisis dan Pengembangan Jaringan Komputer di SMK Negeri 8 Weda Halmahera Tengah," *J. Pendidik. Teknol. Inf. dan Komun.*, vol. 3, no. 2, pp. 1–13, 2023.

[9] B. W. Aulia, M. Rizki, P. Prindiyana, and S. Surgana, "Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital," *JUSTINFO | J. Sist. Inf. dan Teknol. Inf.*, vol. 1, no. 1, pp. 9–20, 2023, doi: 10.33197/justinfo.vol1.iss1.2023.1253.

[10] Santoso and B. J. Bagono, "Optimalisasi Jaringan Wide Area Network Menggunakan Software Defined Network Viptela," *J. Sibernetika*, vol. 7, no. 2, pp. 49–61, 2022.

[11] F. Nugroho and R. Herianto, "Analisis Dan Perancangan Wide Area Network (Wan) Berbasis Ip Vpn Pada Pt. Autocomp Systems Indonesia," *J. Din. UMT*, vol. 7, no. 1, p. 8, 2022, doi: 10.31000/dinamika.v7i1.6748.

[12] R. Adolph, "Kegiatan Pengabdian Semester Ganjil 2023/2024," pp. 1–23, 2016.

[13] R. A. Octaviyana and B. Soewito, "Perancangan Ulang Topologi Jaringan Dengan Kerangka Kerja Ppdioo," *J. Ilm. Sist. Inf.*, vol. 13(1), no. 1, pp. 34– 41, 2023, [Onli

[14] I. L. Kharisma and M. Selpiyana, "Pembelajaran Konfigurasi Mikrotik Berbasis Model OSI Layer di PT Proxi Jaringan Nusantara," 2025.

[15] A. D. Febrian and R. Darmawan, "Implementasi Jaringan Komputer Berbasis Virtual LAN untuk Layanan Iconnet VIP Pada Jaringan MPLS (Multi Protocol Label Switching): Studi Kasus di PT Indonesia Comnets Plus," *Sci. Sacra J. Sains*, vol. 2, no. 3, pp. 1–15, 2022, [Online]. Available: http://pijarpemikiran.com/index.php/Scientia

[16] R. Rahman *et al.*, *Buku Ajar Keamanan Jaringan Komputer*. PT. Sonpedia Publishing Indonesia, 2024.

[17] B. Hartono, "Ransomware: Memahami Ancaman Keamanan Digital," *Bincang Sains dan Teknol.*, vol. 2, no. 02, pp. 55–62, May 2023, doi: 10.56741/bst.v2i02.353.

[18] S. Andriansyah and Nurhasanah, "Analisis Penerapan Aspek Keamanan Informasi CIA Triad Pada Sistem Informasi Akademik," *Konsep Desain Menentukan Hull Type, Mater. Dan Propulsi Unmanned Surf. Veh. Untuk Patroli Di Wil. Rokan Hiir Dengan Metod. Desicion Tree*, no. Lcm, pp. 478–486, 2020.

[19] A. T. Sabiq, S. A. Karimah, and E. M. Jadied, "Analisis Perbandingan UDP dan DCCP Pada Jaringan SD-

WAN," *e-Proceeding Eng.*, vol. 10, no. 3, pp. 3401–3411, 2023, [Online]. Available: