Teknik: Jurnal Ilmu Teknik dan Informatika
Volume 4 Nomor 2 Oktober 2024
e-ISSN: 2798-2513; p-ISSN: 2808-8751, Hal 01-08
DOI: https://doi.org/10.51903/teknik
Available online at: https://journal.stiestekom.ac.id/index.php/TEKNIK

Penerapan Teknologi SDN (Software-Defined Networking) untuk Meningkatkan Keamanan Jaringan Perusahaan

Puteri Ananda Khairunnisa[1], Norul Annisa[2], Jadiaman Parhusip[3]

[1]Universitas Palangka Raya, Palangka Raya, Indonesia
[2]Universitas Palangka Raya, Palangka Raya , Indonesia
[3] Universitas Palangka Raya, Palangka Raya , Indonesia
Email: puterianandа11@gmail.com[1], norulannisa107@gmail.com[2], parhusip.jadiaman@it.upr.ac.id[3]

Alamat Kampus: Jl. Yos Sudarso, Palangka, Kec. Jekan Raya, Kota Palangka Raya, Kalimantan Tengah 74874
Korespondensi Penulis: puterianandа11@gmail.com

Abstract. *Software-Defined Networking (SDN) is an innovative technology that provides network management with high error rates and adaptability. The purpose of this study is to investigate the application of SDN technology in improving corporate network security. This study uses secondary data from relevant scientific journals, analyzing the integration of Deep Packet Inspection (DPI) technology, Intrusion Prevention System (IPS), and network configuration automation to detect and prevent cyber threats. The results of the analysis show that the integration of DPI on the firewall can increase the threat detection rate by up to 25% compared to conventional firewalls, while IPS provides efficient protection against Distributed Denial of Service (DDoS) attacks. In addition, configuration configurations using Mikrotik and Python have succeeded in reducing human error by up to 50% and increasing operational efficiency. However, some technical challenges, such as decreased throughput, need to be optimized. This study concludes that SDN is an effective and flexible solution to improve corporate network security, while supporting cost and operational efficiency.*

Keywords: *SDN, DPI, IPS, Network Security, Automation*

Abstrak. Software-Defined Networking (SDN) merupakan teknologi inovatif yang menyediakan manajemen jaringan secara terpusat dengan tingkat fleksibilitas dan adaptabilitas yang tinggi. Tujuan penelitian ini adalah untuk menginvestigasi penerapan teknologi SDN dalam meningkatkan keamanan jaringan perusahaan. Penelitian ini menggunakan data sekunder dari jurnal ilmiah yang relevan, menganalisis integrasi teknologi Deep Packet Inspection (DPI), Intrusion Prevention System (IPS), dan otomatisasi konfigurasi jaringan guna mendeteksi serta mencegah ancaman siber. Hasil analisis menunjukkan bahwa penyatuan DPI pada firewall dapat meningkatkan tingkat deteksi ancaman hingga 25% dibandingkan dengan firewall konvensional, sementara IPS memberikan perlindungan efisien terhadap serangan Distributed Denial of Service (DDoS). Selain itu, otomatisasi konfigurasi menggunakan Mikrotik dan Python berhasil mengurangi kesalahan manusia hingga 50% dan meningkatkan efisiensi operasional. Walaupun begitu, beberapa tantangan teknis, seperti penurunan throughput, perlu dioptimalkan. Penelitian ini menyimpulkan bahwa SDN merupakan solusi yang efektif dan fleksibel untuk meningkatkan keamanan jaringan perusahaan, sekaligus mendukung efisiensi biaya dan operasional.

Kata kunci: SDN, DPI,IPS,Keamanan Jaringan,Otomasi

1. LATAR BELAKANG

Perkembangan teknologi informasi yang cepat telah mendorong kebutuhan akan jaringan yang lebih aman, fleksibel, dan efisien. Pada era digital ini, perusahaan

Received: September 11, 2024; Revised: September 18, 2024; Accepted: Oktober 12, 2024; Published: November 24, 2024;
*puterianandа11@gmail.com

menghadapi berbagai tantangan dalam mengelola infrastruktur jaringan mereka, terutama dalam hal keamanan dan skalabilitas. Salah satu solusi inovatif yang muncul adalah Software-Defined Networking (SDN). SDN memisahkan control plane dan data plane, memberikan fleksibilitas tinggi dalam pengelolaan jaringan secara terpusat dan mendukung berbagai kebutuhan bisnis.[1] [2]

Namun, jaringan tradisional memiliki keterbatasan dalam menghadapi ancaman keamanan, seperti Distributed Denial of Service (DDoS) dan malware. Firewall tradisional seringkali gagal mendeteksi ancaman tersembunyi di dalam lalu lintas data. Maka dari itu, integrasi teknologi keamanan modern seperti Deep Packet Inspection (DPI) dan Intrusion Prevention System (IPS) menjadi penting dalam meningkatkan perlindungan jaringan. DPI memungkinkan analisis mendalam terhadap paket data, sehingga dapat mendeteksi ancaman hingga tingkat aplikasi, sementara IPS mampu mencegah serangan secara real-time dengan memonitor lalu lintas jaringan.[3] [4] [5]

Selain itu, SDN menawarkan kemampuan untuk mengotomatisasi konfigurasi jaringan, yang secara signifikan mengurangi waktu dan biaya operasional. Implementasi teknologi seperti Python dan Mikrotik pada SDN telah terbukti meningkatkan efisiensi pengelolaan perangkat secara bersamaan, sehingga mengurangi potensi kesalahan manusia dalam konfigurasi.[6] [7] Dengan fleksibilitas ini, SDN tidak hanya memberikan solusi teknis tetapi juga mendukung pengembangan bisnis yang lebih adaptif terhadap perubahan teknologi

Penelitian ini bertujuan untuk mengeksplorasi penerapan teknologi SDN dalam meningkatkan keamanan jaringan perusahaan. Fokus utama penelitian ini adalah pada integrasi DPI dan IPS untuk mendeteksi ancaman keamanan, otomatisasi konfigurasi untuk efisiensi operasional, serta strategi pengelolaan serangan DDoS menggunakan API OpenFlow [5] [6] [8].

2. KAJIAN TEORITIS

2.1 Software-Defined Networking (SDN)

Software-Defined Networking (SDN) merupakan pendekatan baru dalam struktur jaringan yang memisahkan bagian kontrol dan pengolahan data, membolehkan pengelolaan jaringan secara sentral. Dengan teknologi ini, manajemen kebijakan jaringan menjadi lebih fleksibel, memudahkan integrasi perangkat yang beragam, serta mendukung terciptanya inovasi dalam jaringan.[1][2], SDN menggunakan protokol seperti OpenFlow untuk mengatur fungsi switch, sehingga memungkinkan jaringan untuk secara otomatis menyesuaikan diri dengan kebutuhan pengguna yang berubah[3]. Selain itu, SDN telah diterapkan secara luas dalam berbagai jenis jaringan, termasuk Wide Area Networks (WAN) dan Virtual Private Networks (VPN), guna menangani masalah-masalah seperti skala dan kompleksitas.[4][5]

2.2 Deep Packet Inspection (DPI)

Deep Packet Inspection (DPI) ialah teknologi keamanan jaringan yang memungkinkan firewall untuk menganalisis isi paket data secara menyeluruh, bukan hanya bagian headernya. DPI secara signifikan meningkatkan deteksi serangan seperti malware dan situs web berbahaya, dengan peningkatan deteksi hingga 25% dibandingkan firewall konvensional.[6] Penelitian telah menunjukkan bahwa integrasi DPI pada SDN memberikan lapisan perlindungan tambahan terhadap ancaman di tingkat aplikasi, sehingga menjadi solusi efektif untuk keamanan jaringan dalam lingkup perusahaan.[6][7]

2.3 Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) merupakan bagian dari sistem keamanan yang dapat mengidentifikasi, menganalisis, dan menghalangi serangan jaringan secara otomatis. Dalam jaringan SDN, IPS menggunakan arsitektur terpusat untuk memantau dan mengelola aliran data, sehingga dapat mencegah ancaman seperti Distributed Denial of Service (DDoS) secara real-time.[8] Namun, pengintegrasian IPS dalam SDN bisa berpotensi menurunkan throughput dan meningkatkan latensi jaringan.[4]

2.4 Otomasi Konfigurasi Jaringan

SDN mendukung otomatisasi konfigurasi jaringan, sangat bermanfaat bagi perusahaan dengan skala jaringan besar. Pemanfaatan Mikrotik dan Python untuk otomatisasi memungkinkan pengelolaan router secara simultan, mengurangi waktu konfigurasi hingga 50%, serta mengurangi risiko kesalahan manusia.[4][10] Ini memberikan efisiensi biaya yang signifikan dan mempercepat proses penyebaran jaringan.[4][5]

2.5 Penanganan Serangan DdoS

Penanganan serangan DDoS menjadi fokus utama dalam pengelolaan jaringan SDN. Teknologi OpenFlow pada SDN memungkinkan deteksi dan pemblokiran lalu lintas mencurigakan secara otomatis, memberikan perlindungan yang lebih baik dibandingkan jaringan tradisional.[9] Selain itu, integrasi IPS dengan SDN meningkatkan kemampuan mitigasi serangan pada lapisan aplikasi yang sulit dijangkau oleh firewall tradisional.[8][9]

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan analisis data sekunder, di mana informasi yang digunakan diperoleh dari jurnal ilmiah, artikel penelitian, dan laporan studi kasus yang relevan. Data sekunder ini mencakup hasil eksperimen dan simulasi yang telah dilakukan pada penelitian terdahulu tentang SDN, DPI, IPS, dan otomatisasi jaringan.

3.1 Pendekatan Penelitian

Penelitian ini menggunakan metode studi literatur untuk menganalisis penerapan teknologi Software-Defined Networking (SDN) dalam meningkatkan keamanan jaringan perusahaan. Data yang digunakan berasal dari penelitian sebelumnya yang membahas tentang arsitektur SDN, integrasi Deep Packet Inspection (DPI), Intrusion Prevention System (IPS), otomatisasi jaringan, dan penanganan serangan Distributed Denial of Service (DDoS).

3.2 Sumber Data

Data utama dalam penelitian ini diambil dari jurnal-jurnal ilmiah, artikel, dan laporan studi kasus yang relevan, termasuk:

a. Penerepan DPI pada firewall perusahaan untuk mendeteksi ancaman malware [6][7]
b. Integrasi IPS berbasis SDN untuk mitigasi serangan DdoS [8][9]
c. Otomatisasi konfigurasi jaringan menggunakan Mikrotik dan Python [4][5]
d. Teknologi SDWAN untuk failover dan pengelolaan lalu lintas jaringan yang optimal [10]

3.3 Prosedur Penelitian

a. Indentifikasi Masalah

Mengenali hambatan dalam manajemen dan keamanan jaringan konvensional, termasuk keterbatasan firewall dan kerentanan terhadap serangan siber.

b. Studi literatur

Melakukan analisis terhadap artikel dan penelitian terkait untuk memahami penerapan SDN dalam berbagai aspek keamanan jaringan, seperti DPI, IPS, dan manajemen DDoS.

c. Analisis dan Interpretasi

Memanfaatkan data dari artikel untuk: Melakukan evaluasi efektivitas DPI dalam meningkatkan deteksi ancaman, Mengukur keberhasilan IPS dalam mencegah serangan pada jaringan SDN.Mengevaluasi dampak otomatisasi konfigurasi pada efisiensi operasional perusahaan.

d. Simpulan dan Rekomendasi

Menyusun kesimpulan berdasarkan hasil analisis dan memberikan saran mengenai penerapan teknologi SDN dalam konteks perusahaan.

3.4 Instrumen Penelitian

Penelitian ini memanfaatkan data sekunder yang berasal dari berbagai jurnal ilmiah serta studi kasus guna merancang kerangka konseptual. Berikut adalah alat analisis yang digunakan yaitu,Penilaian efektivitas DPI dan IPS menggunakan parameter throughput, latensi, dan tingkat deteksi ancaman[7][9] Simulasi otomatisasi konfigurasi jaringan digunakan untuk mengukur efisiensi waktu dan mengurangi kesalahan manusia[4][5]

3.5 Validasi Data

Validasi dilakukan dengan membandingkan hasil penelitian dari berbagai sumber guna memastikan konsistensi dan relevansi data dengan tujuan penelitian. Sebagai

contoh, penelitian tentang DPI di SDN menunjukkan peningkatan deteksi ancaman hingga 25% dibandingkan dengan firewall tradisional[6][7]

4. HASIL DAN PEMBAHASAN

4.1 *Keunggulan Software-Defined Networking (SDN)*

SDN telah terbukti menjadi solusi yang efektif dalam mengatasi tantangan jaringan tradisional, terutama dalam hal fleksibilitas dan efisiensi operasional. Pemisahan *control plane* dan *data plane* memungkinkan pengelolaan jaringan secara terpusat dan independen dari perangkat keras tertentu.[1][2], Teknologi ini mendukung pengelolaan jaringan heterogen dengan berbagai vendor dan memberikan kemampuan adaptasi yang cepat terhadap perubahan kebutuhan jaringan.[3]

Hasil Studi:

Penelitian tentang penerapan SDN pada jaringan WAN mengungkapkan peningkatan efisiensi manajemen perangkat hingga 30%, terutama saat menghubungkan kantor cabang dan pusat menggunakan teknologi SDWAN.[4][5] Pengelolaan jaringan berbasis SDN memungkinkan pemantauan dan pengaturan secara real-time, sehingga meminimalkan risiko downtime akibat kesalahan konfigurasi.[1][4]

4.2 *Deep Packet Inspection (DPI)*

DPI merupakan teknologi keamanan yang memungkinan analisis mendalam terhadap paket data, memberikan perlindungan tambahan dibandingkan firewall tradisional dengan kemampuan menganalisis isi paket data untuk mendeteksi ancaman tersembunyi seperti malware yang sering luput dari firewall konvensional.

Hasil Studi:

Penerapan DPI pada firewall berbasis SDN berhasil meningkatkan tingkat deteksi ancaman hingga 25%[6], Studi menunjukkan bahwa teknologi DPI efektif dalam memblokir akses ke situs web berbahaya dan membatasi lalu lintas mencurigakan dengan efisiensi tinggi, walaupun ada potensi penurunan throughput jaringan[7].Integrasi DPI dalam jaringan SDN memberikan perlindungan tambahan terhadap ancaman pada lapisan aplikasi, menjadikannya pilihan ideal untuk perusahaan yang membutuhkan keamanan data tingkat tinggi. Meskipun demikian, optimalisasi kinerja jaringan menjadi tantangan yang perlu diatasi[6].

4.3 *Intrusion Prevention System (IPS)*

IPS di dalam jaringan SDN menyediakan kemampuan untuk mendeteksi dan mengatasi serangan secara otomatis. Dengan mengontrol aliran lalu lintas melalui SDN Controller, IPS dapat memantau dan memblokir serangan seperti Distributed Denial of Service (DDoS).

Hasil Studi:

Suatu penelitian menunjukkan bahwa pengintegrasian IPS pada SDN mampu mendeteksi hingga 97% ancaman yang terjadi di dalam jaringan perusahaan.[8] Walaupun efektif, proses deteksi ancaman oleh IPS dapat mengakibatkan penurunan throughput hingga 10% karena beban pemrosesan tambahan pada sistem.[8][9],IPS memberikan manfaat yang besar dalam mendeteksi dan mencegah ancaman jaringan secara real-time. Namun, perlu adanya optimisasi kinerja sistem guna mengurangi dampak negatif pada throughput jaringan.[8]

4.4 *Otomasi Konfigurasi Jaringan*

Teknologi SDN mendukung otomatisasi konfigurasi, yang secara signifikan mengurangi waktu dan biaya operasional. Dengan menggunakan Python dan Mikrotik, jaringan dapat dikonfigurasi secara bersamaan, mengurangi risiko kesalahan manusia.

Hasil Studi:

Penelitian menunjukkan bahwa otomatisasi konfigurasi jaringan dapat mengurangi waktu konfigurasi hingga 50% dibandingkan dengan metode manual[4][5], Pemanfaatan Python untuk otomatisasi pengaturan pada perangkat Mikrotik memungkinkan integrasi yang cepat antara kantor pusat dan cabang[4],Otomatisasi jaringan tidak hanya meningkatkan efisiensi operasional tetapi juga mempercepat respons terhadap perubahan kebutuhan bisnis. Teknologi ini menjadi solusi ideal bagi perusahaan yang ingin meningkatkan efisiensi tanpa mengabaikan keamanan jaringan.

4.5 *Penanganan Serangan DdoS*

Penanganan serangan DDoS memanfaatkan SDN menjadi salah satu aplikasi paling signifikan. SDN dapat mendeteksi dan memblokir lalu lintas mencurigakan secara otomatis berkat OpenFlow API.

Hasil Studi:

Penelitian membuktikan bahwa skema mitigasi DDoS berbasis OpenFlow berhasil menghalangi 95% serangan sebelum mencapai server utama[9][10]Teknologi ini memungkinkan identifikasi lalu lintas mencurigakan tanpa memengaruhi lalu lintas normal, meningkatkan stabilitas jaringan selama serangan terjadi[9] Penanganan serangan DDoS melalui SDN memberikan keunggulan yang tidak dimiliki oleh jaringan konvensional. Namun, implementasi ini memerlukan konfigurasi yang teliti agar deteksi tidak merugikan pengalaman pengguna dari lalu lintas yang sah[10].

5. KESIMPULAN DAN SARAN

Software-Defined Networking (SDN) merupakan teknologi inovatif yang memberikan solusi efektif untuk meningkatkan keamanan jaringan perusahaan. Dengan memisahkan *control plane* dan *data plane*, SDN memungkinkan pengelolaan jaringan secara terpusat, efisien, dan fleksibel. Integrasi teknologi seperti Deep Packet Inspection (DPI) dan Intrusion Prevention System (IPS) telah terbukti meningkatkan kemampuan deteksi dan pencegahan ancaman, termasuk serangan Distributed Denial of Service

(DDoS). Selain itu, otomatisasi konfigurasi jaringan melalui SDN dapat mengurangi kesalahan manusia dan biaya operasional, menjadikannya pilihan ideal untuk kebutuhan jaringan perusahaan modern.

Namun, peningkatan throughput akibat proses inspeksi masih menjadi tantangan yang memerlukan optimalisasi lebih lanjut. Oleh sebab itu, penelitian lanjutan diperlukan guna mengatasi hal tersebut dan menguji implementasi SDN pada jaringan berskala besar. Disarankan agar perusahaan mengintegrasikan SDN dengan teknologi berbasis kecerdasan buatan (AI) untuk mendeteksi ancaman lebih cepat dan otomatis, serta memberikan pelatihan kepada staf IT agar dapat memanfaatkan potensi teknologi ini secara maksimal dalam pengelolaan jaringan mereka.

DAFTAR REFERENSI

[1]. `F. Nisa and S. Ramadona, "Sistem Pencegahan Serangan Distributed Denial Of Service Pada Jaringan SDN," *Jurnal Sistim Informasi dan Teknologi*, vol. 5, no. 3, pp. 22–30, Aug. 2023. https://jsisfotek.org/index.php/JSisfotek/article/view/269

[2]. M. S. Bachtiar, N. Rahaningsih, and R. D. Dana, "Firewall Filtering Berbasis Deep Packet Inspection dalam Mendeteksi dan Mencegah Ancaman Malware," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 1, pp. 399–400, Feb. 2024. https://ejournal.itn.ac.id/index.php/jati/article/view/8387

[3]. M. A. Nugroho and N. A. Suwastika, "Perancangan Intrusion Prevention System pada Jaringan Software Defined Networks," *JUMANJI*, vol. 2, no. 1, pp. 1–16, Apr. 2018. https://jumanji.unjani.ac.id/index.php/jumanji/article/view/17

[4]. S. Hanadwiputra, S. Andri, and D. Prawinarko, "Implementasi Konsep Software Defined Networking (SDN) Wide Area Network (WAN) Pada Mikrotik Dengan Python 3," *JUPITER (Jurnal Teknologi Informatika & Komputer)*, vol. 4, no. 2, pp. 66–72, Aug. 2023. https://ojs.ibm.ac.id/index.php/jupiter/article/view/231

[5]. S. Hidayat and Y. Akbar, "Implementasi Failover VPN Kantor Pusat dan Cabang Menggunakan Teknologi SDWAN Dengan Strategi Best Quality," *JIMIK (Jurnal Indonesia: Manajemen Informatika dan Komunikasi)*, vol. 4, no. 3, pp. 1598–1608, Sep. 2023. doi: 10.35870/jimik.v4i3.386.

[6]. I. Hidayat and B. A. Perdana, "Arsitektur Software Defined Network: Implementasi Pada Small Network," *JJKK (Jurnal Jaringan Komputer dan Keamanan)*, vol. 1, no. 1, pp. 1–13, Feb. 2020. https://iitss.or.id/ojs/index.php/jjkk/article/view/16

[7]. R. Angellia, C. Iswahyudi, and P. Haryani, "Perancangan dan Simulasi Akses Jarak Jauh Menggunakan Teknologi VPN," *SCRIPT (Jurnal Sistem Informasi dan Komputer)*, vol. 12, no. 1, pp. 27–35, Jun. 2024. https://ejournal.akprind.ac.id/index.php/jarkom/article/view/4800

[8]. M. C. Anam, H. D. Septama, and R. A. Nama, "Pengaruh Penggunaan VLAN Pada Software Defined Network Berbasis Ryu Controller," *JITET (Jurnal Informatika dan Teknik Elektro Terapan)*, vol. 12, no. 1, pp. 372–373, Jan. 2024. https://journal.eng.unila.ac.id/index.php/jitet/article/view/3766

[9]. R. Fauzan and R. Rijayanti, "Analisis Keamanan Pendaftaran Akun Wi-Fi Pada Website Captive Portal," in *Konferensi Nasional Sistem Informasi (KNIS)*, Pangkalpinang, Mar. 2018, https://jurnal.atmaluhur.ac.id/index.php/knsi2018/article/view/536

[10]. Hanadwiputra, S. Andri, and D. Prawinarko, "Implementasi konsep software efined networking (SDN) wide area network (WAN) pada mikrotik dengan python 3," *JUPITER (Jurnal Teknologi Informatika & Komputer)*, vol. 4, no. 2, pp. 66–72, Aug. 2023. https://ojs.ibm.ac.id/index.php/jupiter/article/view/231