PERANCANGAN NEXT-GENERATION FIREWALL (NGFW) TERINTEGRASI DENGAN SIEM

SKRIPSI

CORNELIUS YULI ROSDIANTO

2207421059

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER POLITEKNIK NEGERI JAKARTA
2026

PERANCANGAN NEXT-GENERATION FIREWALL (NGFW) TERINTEGRASI DENGAN SIEM

SKRIPSI

Dibuat untuk Melengkapi Syarat-Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik

CORNELIUS YULI ROSDIANTO

2207421059

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN
JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER POLITEKNIK NEGERI JAKARTA
2026

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Cornelius Yuli Rosdianto

NIM : 2207421059

Jurusan/Program Studi : Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan

Judul Skripsi : Perancangan Next-Generation Firewall (NGFW) Terintegrasi Dengan SIEM

Menyatakan dengan sebenarnya bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 9 Juni 2026

Yang membuat pernyataan

Cornelius Yuli Rosdianto

NIM. 2207421059

LEMBAR PENGESAHAN

Skripsi ini diajukan oleh

Nama	: Cornelius Yuli Rosdianto
NIM	: 2207421059
Jurusan/Program Studi	: Teknik Informatika dan Komputer / Teknik Multimedia
Judul Skripsi	: Perancangan Next-Generation Firewall (NGFW) Terintegrasi Dengan SIEM

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Senin., Tanggal 22, Bulan ..Juni....., Tahun 2026 dan dinyatakan **LULUS.**

Disahkan oleh

Pembimbing I : Iik Muhamad Malik Matin, S.Kom, M.T. (.....)

Penguji I : Ayu Rosyida Zain, S.ST, M.T (.....)

Penguji II : Fachroni Arbi Murad, S.Kom., M.Kom (.....)

Penguji III : Chandra Wirawan, S.Kom.,M.Kom. (.....)

Mengetahui:
Jurusan Teknik Informatika dan Komputer
Ketua

Dr. Anita Hidayati, S.Kom., M.Kom.
NIP. 197908032003122003

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Esa atas segala rahmat, karunia, dan penyertaan-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Perancangan Next-Generation Firewall (NGFW) Terintegrasi Dengan SIEM" dengan baik. Dalam proses penyusunan skripsi ini, penulis memperoleh banyak bantuan, dukungan, arahan, serta masukan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan terima kasih kepada:

- Tuhan Yang Maha Esa atas kesempatan dan kemudahan yang diberikan sehingga penulisan skripsi ini dapat diselesaikan tepat waktu.
- Bapak Iik Muhamad Malik Matin, S.Kom, M.T., selaku Dosen Pembimbing, yang telah memberikan arahan dan masukan selama proses penyusunan skripsi.
- Kedua orang tua dan keluarga yang senantiasa memberikan doa, dukungan, serta motivasi kepada penulis.
- Teman-teman penulis terkhusus TMJ dan rekan-rekan selama kegiatan magang yang telah memberikan dukungan dan inspirasi selama proses penyusunan skripsi.

Penulis menyadari bahwa skripsi ini masih memiliki berbagai keterbatasan dan kekurangan. Oleh karena itu, kritik serta saran sangat diterima. Semoga skripsi ini dapat memberikan manfaat dan menambah wawasan bagi pembaca

Depok, 09 Juni 2026

Cornelius Yuli Rosdianto

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini :

Nama	: Cornelius Yuli Rosdianto
NIM	: 2207421059
Jurusan/Program Studi	: Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul :

Perancangan Next-Generation Firewall (NGFW) Terintegrasi Dengan SIEM

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyatan ini saya buat dengan sebenarnya.

Depok, ...9...Juni....2026

Yang menyatakan

(Cornelius Yuli Rosdianto)

NIM. 2207421059

PERANCANGAN NEXT-GENERATION FIREWALL (NGFW) TERINTEGRASI DENGAN SIEM

ABSTRAK

Peningkatan jumlah serangan siber menuntut organisasi untuk menerapkan sistem keamanan yang mampu mendeteksi, mencegah, dan memantau aktivitas berbahaya secara efektif. Namun, solusi keamanan komersial seperti Next-Generation Firewall (NGFW) dan Security Information and Event Management (SIEM) umumnya memerlukan biaya implementasi dan lisensi yang tinggi. Oleh karena itu, penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan berbasis open source menggunakan pfSense sebagai NGFW yang diintegrasikan dengan Suricata IPS, Zenarmor, dan Wazuh SIEM. Implementasi dilakukan pada lingkungan cloud Microsoft Azure menggunakan Virtual Machine. Suricata digunakan untuk mendeteksi dan memblokir serangan berbasis signature, sedangkan Zenarmor digunakan untuk menerapkan Application Control dan Web Control. Seluruh log keamanan diintegrasikan ke dalam Wazuh SIEM. Hasil penelitian menunjukkan bahwa sistem berhasil diimplementasikan dan diintegrasikan dengan baik. Pada pengujian SQL Injection dan Port Scanning, Suricata IPS mampu mendeteksi dan memblokir aktivitas serangan sebelum mencapai Web Server. Zenarmor juga berhasil memblokir akses menuju domain berbahaya dan website yang dibatasi berdasarkan kebijakan keamanan. Hasil pengujian Quality of Service (QoS) menunjukkan bahwa implementasi NGFW menyebabkan penurunan throughput dari 919,7 Mbps menjadi 879,3 Mbps atau sebesar 4,4% pada kondisi normal. Sementara itu nilai delay meningkat dari 1,533 ms menjadi 1,648 ms, jitter meningkat dari 0,017 ms menjadi 0,021 ms, sedangkan packet loss tetap berada pada 0%. Hasil tersebut menunjukkan bahwa implementasi sistem keamanan memberikan dampak terhadap kualitas layanan jaringan dan namun tetap berada pada kategori Sangat Bagus berdasarkan standar TIPHON.

Kata Kunci: Next-Generation Firewall, pfSense, Zenarmor, Wazuh, SIEM

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi informasi dan komunikasi di Indonesia telah mengalami peningkatan dalam beberapa dekade terakhir. Hal ini mengubah cara masyarakat dalam berinteraksi, belajar, dan menjalankan pekerjaannya sehari-hari. Berdasarkan data BPS pada hasil pendataan Survei Sosial Ekonomi Nasional (Susenas) 2024, jumlah pengguna internet terus meningkat secara konsisten setiap tahunnya. Pada tahun 2023, tercatat 69,21 persen penduduk Indonesia telah mengakses Internet dan meningkat pada 2024 menjadi 72,28 persen. Peningkatan ini mengindikasikan bahwa penggunaan internet tidak hanya sekadar fasilitas tambahan, melainkan telah menjadi kebutuhan primer yang menopang kehidupan sehari-hari.

Peningkatan dan transformasi ini tidak hanya membawa kemajuan dan kemudahan bagi banyak orang, namun juga membawa risiko dan ancaman baru dengan ikut berkembangnya serangan siber. Pada tahun 2024, Microsoft melaporkan bahwa pelanggan mereka menerima 600 juta serangan setiap harinya. Serangannya mulai dari ransomware, phising, hingga DDoS yang meningkat setiap tahunnya. Peningkatan serupa dilaporkan oleh Check Point pada laporan Q3 2024 yang mencatat jumlah serangan pada perusahaan meningkat 75% dari periode 2023 dan meningkat 15% dari kuartal sebelumnya.

Penggunaan firewall merupakan salah satu mekanisme untuk mengatasi banyaknya serangan dan melindungi aset organisasi. Firewall tradisional menggunakan teknik *packet filtering* yang bekerja pada Layer 3 (*Network*) dan Layer 4 (*Transport*) dari model OSI, di mana pemblokiran trafik dilakukan berdasarkan alamat IP sumber, alamat IP tujuan, dan port yang digunakan. Tujuannya adalah untuk memblokir trafik menuju alamat IP yang sudah diketahui *malicious* ataupun untuk membatasi akses dari internet menuju internal. Meskipun efektif, teknik ini memiliki keterbatasan dalam mendeteksi serangan modern ataupun kompleks. Penyerang sering kali menyisipkan *payload* berbahaya menggunakan port umum misalnya port 80 atau 443 yang biasanya digunakan organisasi untuk keperluan bisnis sehingga

diizinkan oleh firewall. Akibatnya serangan tersebut dapat masuk tanpa terdeteksi ataupun terblokir. Firewall tradisional tidak memiliki visibilitas terhadap isi paket, sehingga tidak mampu mengenali *malware* atau *payload* yang tersembunyi di balik lalu lintas jaringan yang tampak normal.

Untuk mengatasi kekurangan itu, banyak organisasi menggunakan firewall yang lebih modern atau NGFW. NGFW memiliki kemampuan *Deep Packet Inspection* (DPI) yang memungkinkan inspeksi paket hingga ke Layer 7 (*Application*). Selain mendeteksi pola serangan melalui *Intrusion Prevention System* (IPS), NGFW juga mampu mengidentifikasi aplikasi yang digunakan pengguna melalui fitur *Application Control* serta mengendalikan akses ke situs web berdasarkan kategori melalui fitur *Web Control.* Hal tersebut semakin penting karena serangan siber modern tidak berhenti pada tahap eksploitasi awal. Setelah berhasil memperoleh akses ke sistem, penyerang umumnya melakukan aktivitas lanjutan seperti mengunduh *malware*, memasang *backdoor*, melakukan komunikasi dengan *Command and Control* (C2) server, ataupun memanfaatkan aplikasi *remote access* untuk mempertahankan akses ke sistem korban. Selain firewall, organisasi juga memerlukan visibilitas mengenai apa yang terjadi di dalam jaringan untuk melakukan respons insiden yang efektif. Untuk itu NGFW perlu diintegrasikan dengan SIEM. *Security Information and Event Management* (SIEM) mampu menyatukan dan mengolah data log dari berbagai infrastruktur TI. Log dari perangkat keamanan diintegrasikan ke dalam satu dashboard untuk dilakukan analisis lanjutan oleh tim keamanan organisasi.

Namun, beberapa penelitian terkait masih berfokus pada fungsi deteksi dan monitoring serangan. Matin et al. (2025) berhasil membangun sistem deteksi dan monitoring menggunakan tools *open-source*, namun implementasi yang dilakukan masih terbatas pada proses deteksi dan pemantauan ancaman tanpa mekanisme pencegahan secara langsung. Hal serupa ditemukan pada penelitian Hafizh (2024) yang mengintegrasikan Snort dengan SIEM untuk melakukan monitoring keamanan jaringan, namun sistem yang dibangun hanya berfungsi mendeteksi serangan yang terjadi. Berbeda dengan kedua penelitian tersebut, Wiguna (2024) mengimplementasikan mekanisme *blacklist* IP setelah serangan terdeteksi. Meskipun mampu melakukan pemblokiran, arsitektur yang digunakan

menyebabkan adanya jeda waktu sehingga paket atau payload berbahaya masih dapat mencapai server target sebelum proses *blacklist* IP berhasil dilakukan. Sementara itu, Sulaiman, Seta, dan Falih (2021) berhasil mengembangkan sistem yang mampu merespons serangan secara otomatis, namun pengujiannya masih terbatas pada perangkat printer dan belum terintegrasi dengan SIEM sehingga aktivitas keamanan yang terjadi belum dapat dipantau secara terpusat.

Sebagai pembeda dari penelitian sebelumnya, penelitian ini mengimplementasikan sistem keamanan jaringan berbasis *open-source* menggunakan pfSense yang dikonfigurasi sebagai *Next-Generation Firewall* (NGFW) melalui integrasi Suricata dan Zenarmor, serta dihubungkan dengan platform SIEM Wazuh. Sistem yang dibangun tidak hanya digunakan untuk mendeteksi aktivitas serangan, tetapi juga merespon serangan melalui fitur *Intrusion Prevention System* (IPS) yang bekerja secara inline sehingga paket berbahaya dapat diblokir sebelum mencapai server tujuan. Selain itu, Zenarmor digunakan untuk menerapkan fitur *Application Control* dan *Web Control* sehingga akses aplikasi maupun situs web dapat dikendalikan sesuai kebijakan yang ditetapkan. Log dan aktivitas keamanan dari perangkat yang digunakan juga dikirim ke Wazuh untuk memudahkan proses monitoring dan analisis keamanan jaringan secara terpusat.

1.2 Perumusan Masalah

Melalui latar belakang tersebut, maka rumusan masalahnya adalah:

1. Bagaimana merancang NGFW berbasis Suricata dan Zenarmor yang berjalan pada *virtual machine* di *cloud*.
2. Bagaimana mengintegrasikan NGFW dengan SIEM sehingga serangan ataupun aktivitas jaringan yang ada dapat dipantau.
3. Bagaimana kemampuan NGFW dalam mendeteksi ataupun memblokir trafik *malicious*.

1.3 Batasan Masalah

Penelitian ini berfokus pada:

1. SIEM yang digunakan terbatas pada Wazuh SIEM
2. Integrasi pada SIEM Wazuh terbatas pada DVWA sebagai Web Server dan firewall pfSense serta komponen didalamnya.

3. Implementasi dilakukan pada lingkungan *cloud* menggunakan Virtual Machine Microsoft Azure.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Merancang sistem solusi keamanan menggunakan Suricata dan Zenarmor pada lingkungan *Cloud*.
2. Mengintegrasi sistem NGFW yang telah dibangun dengan SIEM
3. Melakukan evaluasi kemampuan NGFW dalam mendeteksi dan memblokir trafik malicious ataupun tidak sesuai dengan aturan

1.4.2 Manfaat

Adapun manfaat dari penelitian ini adalah sebagai berikut.

1. Manfaat Bagi Penulis: Memperdalam pemahaman teknis mengenai implementasi perangkat keamanan, khususnya dalam mengonfigurasi dan integrasi antara NGFW dan SIEM.
2. Manfaat Bagi Akademis: Menambah literatur di bidang Keamanan Jaringan, khususnya sebagai referensi mengenai efektivitas penggunaan perangkat lunak *open-source*.
3. Manfaat Bagi Masyarakat Umum: Memberikan rekomendasi solusi keamanan siber NGFW.

1.5 Sistematika Penulisan

Adapun sistematika penulisan dari laporan ini adalah sebagai berikut

A. BAB I PENDAHULUAN

   Bab I ini menjelaskan latar belakang penelitian, perumusan masalah, batasan, tujuan, dan manfaat penelitian, serta sistematika penulisan.

B. BAB II TINJAUAN PUSTAKA

   Bab II berisikan penjelasan mengenai landasan teori atau kajian ilmu yang berhubungan dengan berbagai pokok pikiran topik penyusunan skripsi ini yang relevan dari sumber yang valid.

C. BAB III METODE PENELITIAN

Bab III berisi penjelasan mengenai rancangan penelitian, tahapan penelitian, dan objek penelitian.

D. BAB IV HASIL DAN PEMBAHASAN

Bab IV berisi proses perancangan sistem, topologi, serta penyajian data hasil pengujian beserta analisis atau evaluasi terhadap performa sistem keamanan.

E. BAB V PENUTUP

Bab V berisikan mengungkapkan kesimpulan secara singkat yang menjawab rumusan masalah berdasarkan hasil penelitian, serta menyajikan saran dari hasil temuan untuk pengembangan penelitian selanjutnya

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat diambil kesimpulan sebagai berikut:

1. Sistem keamanan berbasis *Next-Generation Firewall* (NGFW) berhasil diimplementasikan menggunakan pfSense yang diintegrasikan dengan Suricata IPS dan Zenarmor pada lingkungan *Cloud* Azure. Sistem yang dibangun menempatkan NGFW sebagai *gateway* utama sehingga seluruh trafik baik masuk ataupun keluar akan melewati proses inspeksi dan filtering sebelum diteruskan menuju tujuan.
2. Integrasi antara pfSense, Suricata, Zenarmor, dan Wazuh berhasil dilakukan. Log keamanan yang dihasilkan oleh Suricata dapat dikirimkan menggunakan Syslog-ng, sedangkan log Zenarmor berhasil diintegrasikan menggunakan *script* python yang membaca data dari database internal Zenarmor. Seluruh log dikumpulkan pada Wazuh SIEM sehingga *alert* dapat dipantau secara terpusat.
3. Berdasarkan pengujian ancaman eksternal, sistem mampu mendeteksi dan memblokir berbagai aktivitas serangan seperti port *scanning* dan SQL Injection sebelum mencapai Web Server. Pada pengujian SQL Injection, seluruh *request malicious* berhasil diblokir dan tidak ditemukan aktivitas serangan yang tercatat pada Web Server melalui Wazuh Agent HIDS.
4. Hasil pengujian serangan harian menunjukkan bahwa Web Server yang terhubung langsung ke internet menerima berbagai aktivitas mencurigakan setiap hari, mulai dari koneksi yang berasal dari alamat IP dengan reputasi buruk hingga *request* yang mengandung *payload* yang terindikasi sebagai upaya eksploitasi. Seluruh aktivitas tersebut berhasil dimonitor dan *request* berbahaya berhasil diblokir oleh sistem keamanan.

6.2 Saran

Adapun beberapa saran yang dapat dilakukan pada penelitian selanjutnya, antara lain:

1. Penelitian selanjutnya dapat menggunakan SIEM lain baik berbasis komersial ataupun *open source* untuk dapat dibandingkan kemampuan serta performa sistem.
2. Integrasi sistem keamanan dapat diperluas dengan menambahkan sumber log lain seperti WAF maupun NDR.
3. Implementasi dapat dilakukan pada lingkungan jaringan yang berbeda misalnya pada lingkungan on-premises, untuk mengetahui kemampuan sistem dalam menangani trafik yang lebih besar.
4. Penelitian selanjutnya dapat melakukan evaluasi terhadap performa dan efektivitas implementasi NGFW berbasis *open source* serta membandingkannya dengan solusi NGFW komersial.

DAFTAR PUSTAKA

Ang, S., Huy, S. & Janarthanan, M., 2025, 'Utilizing IDS and IPS to Improve Cybersecurity Monitoring Process', *Journal of Cyber Security and Risk Auditing*, 2025(3), 77.

Badan Pusat Statistik, 2024, *Statistik Telekomunikasi Indonesia 2024*, BPS, Badan Pusat Statistik.

Bezas, K. & Filippidou, F., 2023, 'Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs)', *Comparative Analysis of Open Source Security Information & Event ManagementSystems (SIEMs)*, 12, 444–468.

Gupta, P., 2024, *Review of Next-Generation Firewalls*.

Liang, J. & Kim, Y., 2022, *Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall*, *2022 IEEE 12th Annual Computing and Communication Workshop and Conference, CCWC 2022*, 752–759, Institute of Electrical and Electronics Engineers Inc.

Manzoor, J., Waleed, A., Jamali, A.F. & Masood, A., 2024, 'Cybersecurity on a budget: Evaluating security and performance of *open-source* SIEM solutions for SMEs', *PLOS ONE*, 19(3 March).

Muhamad Malik Matin, I., Kurniawan, A., Rosyida Zain, A., Agustin, M., Informatika dan Komputer, T. & Negeri Jakarta, P., 2023, 'Sistem Monitoring Keamanan Pada Data Center Berbasis Security Information And Event Management (Siem) Dengan Wazuh dan IDS', *Journal of Innovative and Creativity*, 5(1), 2025.

Open Information Security Foundation (OISF), 2026, *Suricata User Guide*.

Patil, M. & Mohurle, S., 2017, 'The Empirical Study of the Evolution of the Next Generation Firewalls', *International Journal of Trend in Scientific Research and Development*, 1(5), 193–196.

Satilmis, H., Akleylek, S. & Yuce Tok, Z., 2025, 'Development of Various Stacking Ensemble-Based HIDS Using ADFA Datasets', *IEEE Open Journal of the Communications Society*, 6, 1170–1189.

Sulaiman, F.S., Seta, H.B. & Falih, N., 2021, *Exploitation Prevention on Network Printer with Signature-Based Suricata on PfSense*, *Proceedings - 3rd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2021*, 35–39, Institute of Electrical and Electronics Engineers Inc.

Wazuh, 2024, *Wazuh Documentation*.

Wiguna, R., 2024, *Analisis Implementasi dan Integrasi Suricata dengan Scirius dan ntopng untuk Pendeteksian dan Pemblokiran Serangan pada Server dengan Notifikasi WhatsApp*.

Wiradyaksa, I.D., Putri, D.H., Iqbal, R.M., Astari, N.H., Karna, N. & Dewanta, F., 2024, *Design and Implementation of Automated Web Application Firewall, Rate Limiting, and Intrusion Detection System for Cyber Defense*, *2024 8th International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2024*, 256–261, Institute of Electrical and Electronics Engineers Inc.

Zenarmor, 2024, *What is Web Filtering? Types, Benefits, Challenges and Best Practices*.

Zenarmor, 2026, *Welcome to the Zenarmor User Guide*.

DAFTAR RIWAYAT HIDUP

Cornelius Yuli Rosdianto, lahir pada tahun 2004, merupakan anak kedua dari tiga bersaudara. Penulis menyelesaikan pendidikan menengah pertama di SMPN 1 Cikarang Barat dan pendidikan menengah atas di SMAN 4 Tambun Selatan. Pada tahun 2022, penulis melanjutkan pendidikan di Program Studi Teknologi Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta. Selama menempuh pendidikan, penulis memiliki minat pada bidang jaringan komputer dan keamanan siber.