JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1387-1396

Arsitektur Perangkat Keras FortiGate: Manajemen Beban Kerja CPU dan Subsistem I/O pada Interfaces Port

Aldetia Farendi[1]

[1]Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Pamulang, Kota Tangerang Selatan, Indonesia
Email: [1]Aldetia121@gmail.com
(* : coressponding author)

Abstrak−FortiGate merupakan perangkat keamanan jaringan (firewall) yang kinerjanya sangat bergantung pada arsitektur perangkat keras, khususnya unit pemrosesan (CPU) dan subsistem masukan/keluaran (I/O). Penelitian ini bertujuan membahas arsitektur perangkat keras FortiGate dengan fokus pada manajemen beban kerja CPU serta peran subsistem I/O pada interfaces port. Pembahasan dilakukan dengan mengaitkan komponen perangkat keras FortiGate—seperti CPU, prosesor khusus (ASIC/Security Processing Unit), memori, dan interfaces port—dengan konsep dasar arsitektur komputer, meliputi pemrosesan instruksi, pembagian beban kerja, serta aliran data pada sistem I/O. Hasil pembahasan menunjukkan bahwa FortiGate mendistribusikan beban kerja antara CPU umum dan prosesor khusus untuk meningkatkan efisiensi pemrosesan paket, sementara subsistem I/O pada interfaces port berperan penting dalam menjaga kelancaran aliran data. Pemahaman terhadap arsitektur ini memberikan gambaran bagaimana perangkat keras bekerja dalam mendukung kinerja dan keamanan jaringan.

Kata Kunci: FortiGate, arsitektur perangkat keras, beban kerja CPU, subsistem I/O, interfaces port.

Abstract−*FortiGate is a network security appliance (firewall) whose performance is highly dependent on its hardware architecture, particularly the central processing unit (CPU) and the input/output (I/O) subsystem. This paper discusses the hardware architecture of FortiGate with a focus on CPU workload management and the role of the I/O subsystem on the interfaces port. The discussion links FortiGate hardware components—such as the CPU, dedicated processors (ASIC/Security Processing Unit), memory, and interfaces port—to fundamental computer architecture concepts, including instruction processing, workload distribution (offloading), and data flow within the I/O system. The results indicate that FortiGate does not rely solely on a general-purpose CPU; it also leverages dedicated processors to improve the efficiency of packet processing, while the I/O subsystem on the interfaces port plays a critical role in maintaining smooth inbound and outbound traffic. Understanding this architecture provides insight into how FortiGate hardware supports both performance and network security functions.*

Keywords: *FortiGate, hardware architecture, CPU workload, I/O subsystem, interfaces port.*

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah meningkatkan kebutuhan akan jaringan komputer yang cepat, stabil, dan aman. Infrastruktur jaringan modern tidak hanya dituntut mampu menyediakan layanan komunikasi data yang andal, tetapi juga harus mampu melindungi sistem dari berbagai ancaman keamanan siber yang semakin kompleks. Oleh karena itu, perangkat keamanan jaringan seperti firewall menjadi salah satu komponen penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data pada suatu jaringan komputer. Penggunaan Next Generation Firewall (NGFW) semakin banyak diterapkan karena mampu memberikan perlindungan yang lebih komprehensif dibandingkan firewall tradisional melalui fitur inspeksi paket, kontrol aplikasi, serta sistem pencegahan intrusi (Alhasan & Surantha, 2021; Grossi et al., 2024; Ismail et al., 2025).

Salah satu perangkat NGFW yang banyak digunakan pada lingkungan perusahaan maupun institusi adalah FortiGate. Perangkat ini tidak hanya berfungsi sebagai penyaring lalu lintas jaringan, tetapi juga mampu menjalankan berbagai layanan keamanan secara terintegrasi. Dalam operasionalnya, FortiGate harus memproses lalu lintas data yang masuk dan keluar melalui berbagai interfaces port secara real-time sehingga membutuhkan kemampuan pemrosesan yang tinggi untuk menjaga performa dan stabilitas jaringan (Prima Jaya et al., 2021).

Peningkatan jumlah pengguna, perangkat, serta volume lalu lintas data dapat menyebabkan beban kerja yang semakin besar pada perangkat jaringan. Apabila sumber daya pemrosesan tidak

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1387-1396

dikelola dengan baik, kondisi tersebut dapat menimbulkan bottleneck yang berdampak pada penurunan kinerja jaringan. Oleh karena itu, pemahaman mengenai pengelolaan beban kerja CPU dan mekanisme perpindahan data melalui subsistem input/output (I/O) menjadi aspek penting dalam mengevaluasi performa perangkat keamanan jaringan (Grossi et al., 2024; Sandi et al., 2025).

Beberapa penelitian sebelumnya telah membahas implementasi firewall untuk meningkatkan keamanan jaringan serta efektivitas Next Generation Firewall dalam mendeteksi dan mencegah berbagai jenis serangan jaringan. Hasil penelitian menunjukkan bahwa NGFW memiliki kemampuan yang lebih baik dibandingkan firewall tradisional karena mampu melakukan inspeksi paket secara lebih mendalam dan mendukung berbagai mekanisme keamanan tambahan. Namun demikian, penelitian yang secara khusus membahas hubungan antara arsitektur perangkat keras, manajemen beban kerja CPU, dan subsistem I/O pada perangkat FortiGate masih relatif terbatas (Alhasan & Surantha, 2021; Grossi et al., 2024; Ismail et al., 2025).

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk menganalisis arsitektur perangkat keras FortiGate-81F-POE dengan fokus pada manajemen beban kerja CPU dan subsistem I/O pada interfaces port. Analisis dilakukan untuk memahami bagaimana perangkat mengelola proses pemrosesan lalu lintas jaringan serta mekanisme perpindahan data yang mendukung kinerja sistem secara keseluruhan (Fortinet, 2023).

2. METODE

2.1 Jenis Penelitian

Teknik pengumpulan data dilakukan melalui observasi langsung terhadap perangkat FortiGate-81F-POE yang digunakan pada lingkungan home lab. Data diperoleh dengan mengakses antarmuka manajemen FortiOS untuk mengamati informasi yang berkaitan dengan penggunaan CPU, status memori, serta aktivitas interfaces port. Selain itu, dilakukan studi literatur terhadap dokumentasi resmi Fortinet dan beberapa penelitian terdahulu yang membahas firewall, Next Generation Firewall (NGFW), serta arsitektur perangkat jaringan guna mendukung analisis hasil observasi (Alhasan & Surantha, 2021; Fortinet, 2023).

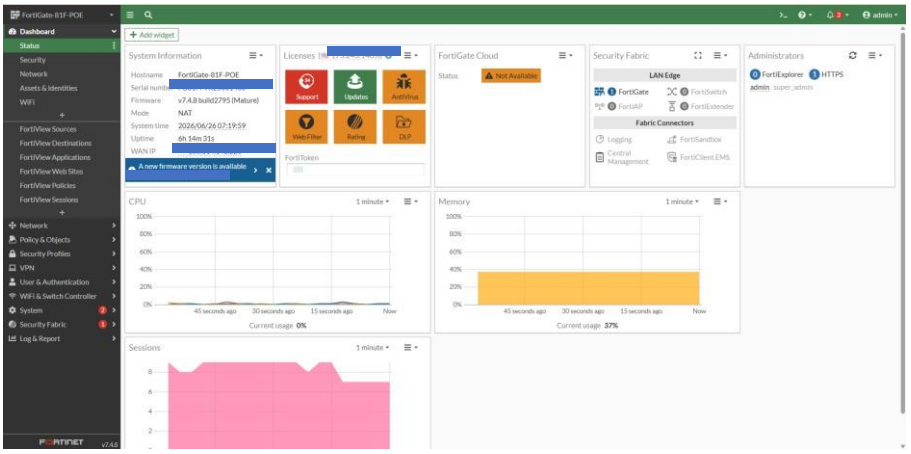
2.2 Objek Penelitian

Parameter yang diamati dalam penelitian ini terdiri atas dua aspek utama, yaitu manajemen beban kerja CPU dan subsistem input/output (I/O) pada interfaces port. Pengamatan pada CPU dilakukan dengan melihat informasi pemanfaatan sumber daya yang tersedia pada sistem FortiOS. Sementara itu, pengamatan subsistem I/O dilakukan dengan mengidentifikasi fungsi interfaces port, status koneksi, serta aliran lalu lintas data yang melewati masing-masing interface. Parameter tersebut dipilih karena berhubungan langsung dengan kinerja perangkat dalam memproses dan meneruskan paket data pada jaringan.

Tabel 1. Identitas Objek Penelitian

Parameter	Nilai
Perangkat	FortiGate-81F-POE
Versi FortiOS	v7.4.8 build2795
Lingkungan	Home lab (observasi langsung GUI/CLI)
Kondisi Topologi	Hanya uplink aktif, belum ada klien LAN untuk uji trafik

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1387-1396



Gambar 1. Analisis Data Berdasarkan Arsitektur Komputer

2.3 Teknik Pengumpulan Data

Dalam proses pengumpulan data beban kerja arsitektur (CPU dan memori), penelitian ini tidak menggunakan pengembangan algoritma khusus, melainkan menggunakan teknik **observasi langsung (*direct observation*)**. Data metrik kinerja diperoleh melalui mekanisme *system polling* bawaan dari sistem operasi FortiOS. Secara arsitektural, *kernel* dari sistem operasi akan secara berkala melakukan *polling* (pemeriksaan status) terhadap register prosesor dan alokasi memori fisik, lalu merepresentasikannya secara visual secara *real-time* pada GUI (Graphical User Interfaces) *Dashboard*. Penggunaan fitur *monitoring* bawaan perangkat ini dinilai paling valid untuk merepresentasikan status perangkat keras secara langsung tanpa memberikan beban (*overhead*) tambahan pada CPU dari aplikasi pihak ketiga. Adapun rincian tahapan pengumpulan data yang dilakukan adalah sebagai berikut:

1) **Verifikasi CLI**
   Untuk memperkuat data GUI, dilakukan verifikasi melalui CLI menggunakan perintah:
   - ***get system status*** — informasi model, firmware, mode operasi
   - ***get system performance status*** — CPU usage, memory usage, sessions

2) **Studi Literatur (data Sekunder)**
   Studi literatur dilakukan untuk memperoleh konsep dasar arsitektur komputer (CPU, memori, subsistem I/O) serta konsep terkait FortiGate. Sumber yang digunakan meliputi buku arsitektur komputer dan dokumentasi resmi Fortinet.

2.4 Parameter yang Diamati

Pemilihan parameter observasi disesuaikan dengan fokus penelitian, yaitu beban kerja prosesor dan subsistem antarmuka masukan/keluaran. Rincian parameter ditunjukkan pada Tabel 2.

Tabel 2 Parameter Observasi

Komponen	Parameter	Indikator	Sumber Data (GUI)
CPU	Beban kerja prosesor	Persentase *CPU usage*	*Dashboard widget CPU*
Memori	Beban operasional	Persentase *Memory usage*	*Dashboard widget Memory*
Subsistem I/O	Kategori antarmuka	Jenis *Interface* fisik/logis	*Network → Interfaces*
Subsistem I/O	Status jalur I/O	Status *Up/Down* dan IP	*Network → Interfaces*

2.5 Batasan Penelitian

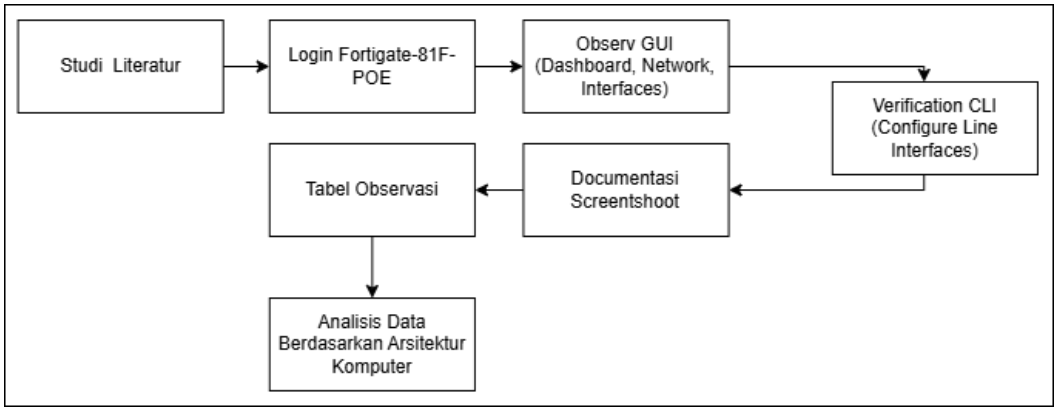
Penelitian ini dibatasi pada observasi kondisi perangkat dan status interfaces pada lingkungan pengujian home lab. Pengujian kinerja end-to-end secara aktif (seperti pengujian throughput atau latency) tidak dilakukan karena belum terdapat perangkat klien yang difungsikan untuk uji trafik pada

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1387-1396

sisi jaringan internal (LAN); entri klien DHCP yang tercatat pada interface internal hanya berasal dari perangkat administrator saat konfigurasi awal. Hasil observasi murni merepresentasikan beban kerja arsitektur sistem pada konfigurasi dasar.

2.6 Prosedur dan Alur Penelitian

Pelaksanaan penelitian dilakukan secara sistematis, dimulai dari tahapan inisialisasi *login* ke perangkat FortiGate, pemantauan indikator sistem melalui *Dashboard*, hingga identifikasi subsistem I/O pada menu *Interfaces*. Setelah data terkumpul, analisis dilakukan secara deskriptif dengan memetakan temuan parameter kerja ke dalam landasan teori arsitektur komputer. Seluruh tahapan prosedur pengumpulan hingga analisis data tersebut direpresentasikan secara visual melalui *flowchart* pada Gambar 2



Gambar 2. Alur pengumpulan data penelitian

3. ANALISA DAN PEMBAHASAN

Pada bagian ini dibahas hasil pengamatan yang telah dilakukan pada perangkat **FortiGate-81F-POE** di home lab, meliputi kondisi sistem, beban kerja CPU, serta subsistem I/O pada interfaces port. Pembahasan dikaitkan dengan konsep dasar arsitektur komputer, yaitu unit pemrosesan, memori, dan subsistem input/output.

3.1 Informasi Sistem dan Beban Kerja CPU

Berdasarkan hasil observasi pada perangkat FortiGate-81F-POE, sistem beroperasi dalam mode NAT. Pada saat pengambilan data, nilai CPU usage tercatat sebesar 1%, memory usage sebesar 38%, dan current sessions sebanyak 12 sesi aktif. Kondisi tersebut menunjukkan bahwa perangkat tidak mengalami beban pemrosesan yang tinggi sehingga sebagian besar sumber daya CPU masih tersedia untuk menangani lalu lintas jaringan yang masuk. Sementara itu, penggunaan memori yang lebih besar menunjukkan adanya alokasi sumber daya untuk penyimpanan informasi sesi, tabel koneksi, serta layanan sistem yang berjalan pada perangkat firewall.

Rendahnya utilisasi CPU menunjukkan bahwa perangkat masih memiliki kapasitas yang cukup untuk menangani peningkatan trafik jaringan. Hal ini sejalan dengan temuan Ibrahim et al. (2023) yang menyatakan bahwa dalam kondisi tanpa aktivitas trafik yang membanjiri firewall, penggunaan CPU FortiGate hanya berada pada rentang 0–2%, sedangkan pada saat menerima serangan DDoS penggunaan CPU dapat meningkat drastis hingga mendekati 100%.

Pada perangkat keamanan modern, pengelolaan sumber daya pemrosesan menjadi faktor penting karena berbagai fungsi keamanan seperti inspeksi paket, pengendalian aplikasi, dan pencegahan intrusi memerlukan proses komputasi yang berkelanjutan (Grossi et al., 2024; Ibrahim et al., 2023; Ismail et al., 2025).

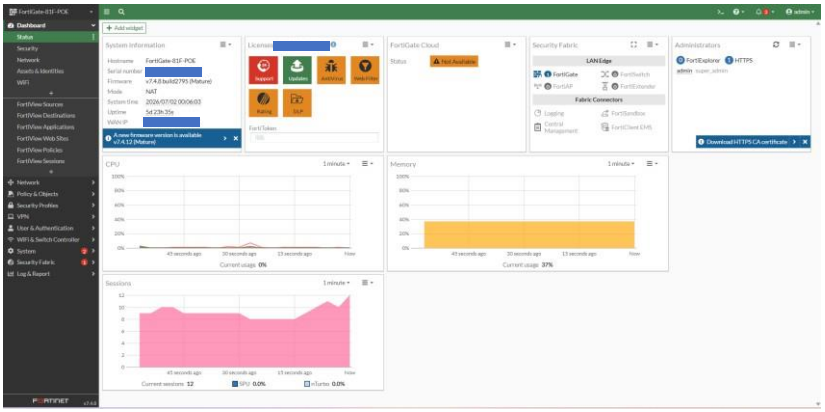
Selain CPU utama, FortiGate juga dilengkapi dengan teknologi akselerasi perangkat keras berupa Security Processing Unit (SPU) dan nTurbo. Berdasarkan hasil observasi, kedua komponen tersebut belum menunjukkan aktivitas pemrosesan yang signifikan sehingga nilai utilisasinya tercatat 0,0%. Keberadaan SPU dan nTurbo menunjukkan bahwa arsitektur FortiGate menerapkan

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1387-1396

pendekatan hardware acceleration untuk meningkatkan efisiensi pemrosesan paket jaringan. Pendekatan ini memungkinkan sebagian beban kerja yang umumnya diproses oleh CPU dialihkan ke prosesor khusus sehingga kinerja perangkat dapat dipertahankan ketika terjadi peningkatan lalu lintas jaringan maupun aktivasi fitur keamanan tingkat lanjut (Alhasan & Surantha, 2021; Fortinet, 2023; Grossi et al., 2024)

Tabel 3 Hasil Observasi Informasi Sistem dan Beban Kerja

Parameter	Nilai
Model/Hostname	FortiGate-81F-POE
Firmware	v7.4.8 build2795 (Mature)
Mode Operasi	NAT
CPU Usage	1%
Memory Usage	37%
Current Session	12
SPU Usage	0.0%
nTurbo Usage	0.0%



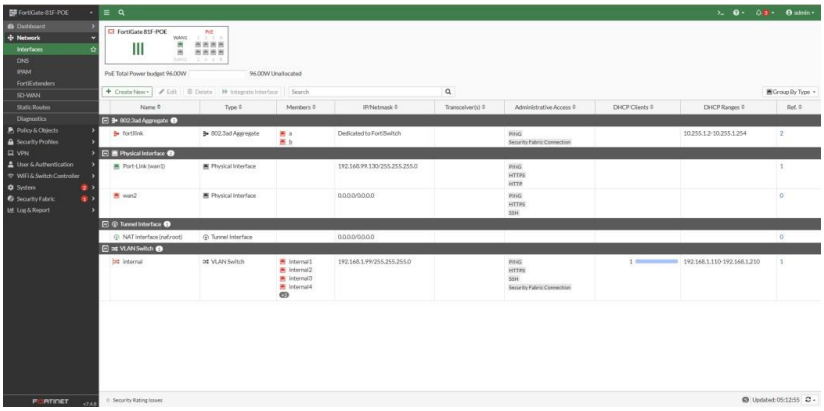
Gambar 4. Dashboard Fortigate 81F-POE

Untuk memperkuat data yang ditampilkan pada Dashboard, dilakukan verifikasi melalui CLI menggunakan perintah get system status dan get system performance status. Hasil verifikasi menunjukkan informasi model, firmware, dan mode operasi yang sesuai dengan Tabel 3, serta nilai CPU usage, memory usage, dan jumlah sesi yang konsisten dengan tampilan GUI, sehingga data observasi dinilai valid.

3.2 Subsistem I/O pada Interfaces Port

Pada FortiGate, subsistem I/O dapat diamati melalui menu Network → Interfaces karena pada bagian ini terlihat interfaces port yang digunakan untuk menerima dan mengirim data. Setiap interface berperan sebagai jalur masuk dan keluar paket data sehingga dapat dipandang sebagai implementasi subsistem input/output pada perangkat jaringan. Fungsi interfaces port jaringan sebagai media pertukaran data merupakan bagian penting dalam operasional firewall modern untuk mengendalikan lalu lintas jaringan yang masuk maupun keluar (Tomar & Bhile, 2021).

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1387-1396



Gambar 5 Interfaces network

Dari hasil pengamatan pada FortiGate-81F-POE, interface yang tersedia terbagi menjadi 4 jenis:

3.2.1 Interface fisik

Interfaces port fisik pada perangkat. Terdapat dua interface pada kategori ini, yaitu wan1 (Port-Link) yang berstatus aktif dengan alamat IP 192.168.99.130/255.255.255.0 dan berfungsi sebagai jalur uplink, serta wan2 yang berstatus tidak aktif karena tidak digunakan pada topologi saat ini.

3.2.2 802.3ad Aggregate

Interface fortilink yang merupakan gabungan (agregasi) dari dua port fisik (a dan b). Interface ini secara default dialokasikan untuk koneksi ke perangkat FortiSwitch dan menunjukkan bahwa FortiGate mendukung penggabungan beberapa jalur fisik menjadi satu jalur logis.

3.2.3 Tunnel Interface

Yaitu naf.root (NAT interface) yang merupakan interface virtual bawaan sistem. Interface ini tidak terikat pada port fisik dan dibuat otomatis oleh FortiOS untuk kebutuhan internal.

3.2.4 VLAN Switch

Yaitu interface internal yang menggabungkan beberapa port fisik (internal1–internal4) menjadi satu segmen jaringan dengan alamat IP 192.168.1.99/255.255.255.0. Interface ini menjalankan layanan DHCP dengan rentang alamat 192.168.1.110–192.168.1.210. Pada saat observasi tercatat 2 entri klien DHCP, yang merupakan sisa lease dari perangkat administrator saat proses konfigurasi awal, bukan klien aktif yang digunakan untuk pengujian trafik.

Hasil observasi dirangkum pada Tabel 4..

Tabel 4 Hasil Observasi Interfaces Port

Interface	Jenis	Status	IP/Netmask	Keterangan
wan1 (Port-Link)	Physical	Up	192.168.99.130/255.255.255.0	Jalur uplink aktif
wan2	Physical	Down	0.0.0.0/0.0.0.0	Tidak digunakan
fortilink	802.3ad Aggregate	Down	Dedicated to FortiSwitch	Agregasi port a dan b
naf.root	Tunnel	–	0.0.0.0/0.0.0.0	Interface virtual bawaan sistem

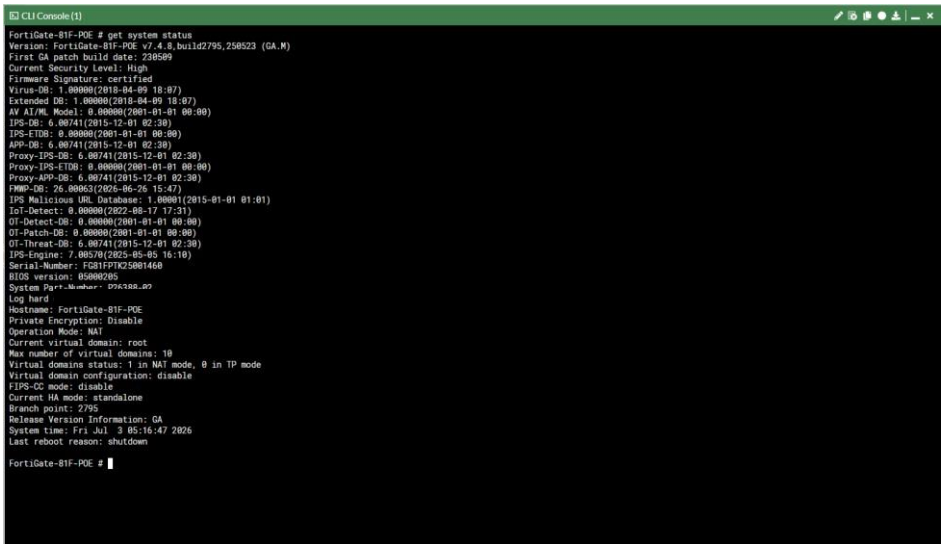
JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1387-1396

internal	VLAN Switch	Up	192.168.1.99/255.255.255.0	Gabungan port internal1–4, DHCP aktif (2 klien)

Dari hasil pengamatan tersebut terlihat bahwa subsistem I/O pada FortiGate tidak hanya terdiri atas port fisik, tetapi juga mencakup interface logis seperti agregasi, tunnel, dan VLAN switch yang dibangun di atas perangkat keras yang sama. Aliran data dari jaringan internal masuk melalui interface internal, kemudian diproses oleh sistem dan diteruskan keluar melalui interface wan1 sebagai jalur uplink. Kondisi ini menunjukkan bahwa kelancaran komunikasi data sangat dipengaruhi oleh interface yang aktif dan digunakan dalam proses pertukaran data. Sementara itu, interface yang tidak digunakan tetap tersedia sebagai cadangan untuk kebutuhan pengembangan jaringan di masa mendatang. Apabila volume trafik meningkat, interface aktif berpotensi menjadi titik hambatan (bottleneck) apabila kapasitas jalur komunikasi tidak seimbang dengan beban lalu lintas yang harus diproses (Sandi et al., 2025).

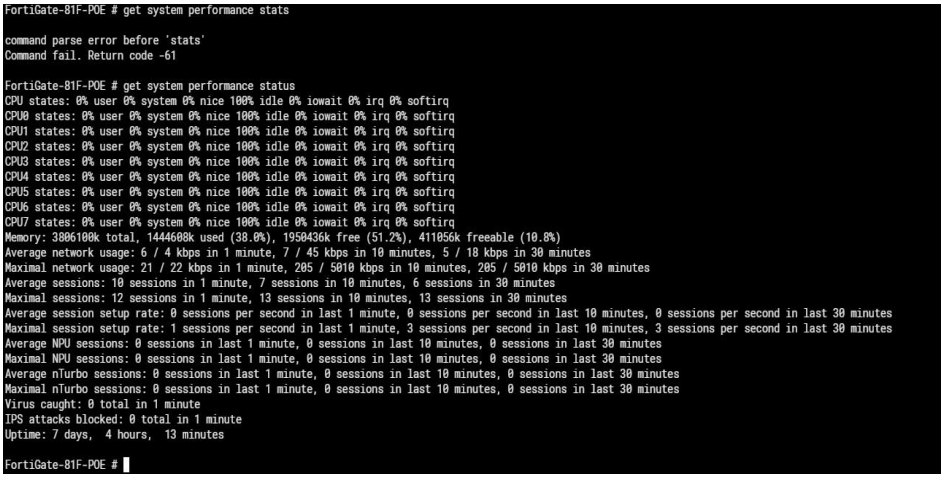
3.3 Verifikasi Data melalui CLI.

Sebagaimana dijelaskan pada metode penelitian, data yang ditampilkan pada GUI diverifikasi melalui *Command Line Interface* (CLI) untuk memastikan validitas hasil observasi. Verifikasi dilakukan menggunakan tiga perintah, yaitu *get system status* untuk informasi model, firmware, dan mode operasi; *get system performance* status untuk nilai CPU usage, memory usage, dan jumlah sesi; Hasil verifikasi ditunjukkan pada Gambar 6.



Gambar 6 Status perangkat

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1387-1396



Gambar 7 Hasil verifikasi get system performance status

Berdasarkan hasil verifikasi tersebut, informasi yang diperoleh melalui CLI menunjukkan nilai yang konsisten dengan tampilan pada Dashboard (Tabel 3) maupun menu Network → Interfaces (Tabel 4). Kesesuaian antara kedua sumber data ini menunjukkan bahwa hasil observasi valid, karena baik GUI maupun CLI membaca status yang sama dari sistem melalui mekanisme *polling* yang dilakukan oleh sistem operasi FortiOS terhadap kondisi perangkat keras.

3.4 Validasi Data Observasi.

Untuk memastikan validitas dan akurasi data yang diperoleh melalui antarmuka grafis (GUI) Dashboard dan menu Network → Interfaces, dilakukan verifikasi silang (cross-validation) menggunakan Command Line Interface (CLI) FortiOS. Langkah ini penting untuk menjamin bahwa metrik kinerja yang ditampilkan pada GUI sesuai dengan data internal sistem yang diakses secara langsung (Fortinet, 2023).

Proses validasi dilakukan dengan membandingkan nilai parameter pada Tabel 3 dan Tabel 4 terhadap output dari perintah CLI yang telah ditampilkan pada Gambar 6 dan Gambar 7 di bagian 3.3. Ringkasan perintah CLI yang digunakan untuk validasi ditunjukkan pada Tabel 5 berikut:

Tabel 5 Pemetaan Parameter Observasi terhadap Perintah Validasi CLI

Parameter Observasi	Perintah CLI	Fungsi Validasi
Model, Firmware, Mode Operasi	get system status	Memvalidasi identitas perangkat dan konfigurasi dasar
CPU Usage, Memory Usage, Session	get system performance status	Memvalidasi metrik kinerja sistem secara *real-time*

Berdasarkan output CLI pada **Gambar 7** (get system performance status), diperoleh data sebagai berikut:

Tabel 6 Perbandingan Nilai Parameter Observasi antara GUI dan CLI

Parameter	Nilai GUI (Tabel 3)	Nilai CLI	Status Validasi
CPU Usage	1%	~0-1% (idle 100%)	✓ Valid
Memory Usage	37%	39.8%	✓ Valid*
Current Session	12	12 sessions (last 1 min)	✓ Valid

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1387-1396

Selisih kecil pada memory usage disebabkan oleh perbedaan waktu pengambilan data (*timestamp*) antara GUI dan CLI, serta metode pembulatan yang berbeda. Nilai tersebut masih dalam rentang yang konsisten.

Output CLI pada Gambar 7 juga mengonfirmasi bahwa:

a. **CPU States** menunjukkan 100% idle pada semua core, yang konsisten dengan CPU usage rendah (1%) pada GUI
b. **Current Sessions** tercatat sebanyak 12 sesi pada menit terakhir, sesuai persis dengan nilai pada Tabel 3.
c. **Memory Usage** tercatat sekitar 39.8% (14440M used dari 20063M total), yang mendekati nilai 37% pada GUI.

Untuk validasi konfigurasi interface, perintah show system interface telah dijalankan untuk memverifikasi status, alamat IP, dan tipe setiap interface. Hasil verifikasi tersebut telah digunakan sebagai dasar pengisian Tabel 4 pada bagian 3.2, yang menunjukkan konsistensi antara konfigurasi sistem dan tampilan GUI.

Berdasarkan hasil validasi silang pada bagian ini, dapat disimpulkan bahwa seluruh data observasi yang digunakan dalam penelitian ini memiliki tingkat validitas yang tinggi dan merepresentasikan kondisi aktual perangkat FortiGate-81F-POE pada saat pengujian dilakukan.

4. KESIMPULAN

Berdasarkan hasil observasi dan analisis yang telah dilakukan pada perangkat FortiGate-81F-POE, dapat ditarik beberapa kesimpulan sebagai berikut:

a. Dari sisi beban kerja pemrosesan, hasil observasi menunjukkan bahwa pada kondisi konfigurasi dasar dengan trafik minimal, CPU usage tercatat sangat rendah (1%) sementara memory usage berada pada angka 37%. Kondisi ini menunjukkan karakteristik perangkat firewall yang bersifat stateful, di mana memori dialokasikan secara terus-menerus untuk mengelola tabel sesi dan data operasional sistem, sedangkan CPU hanya bekerja ketika terdapat paket yang perlu diproses. Hasil ini menunjukkan bahwa pada kondisi trafik minimal, beban kerja perangkat masih sangat rendah. Temuan tersebut berbeda dengan penelitian pada virtualized FortiGate yang memperlihatkan kenaikan konsumsi CPU dan memori secara signifikan saat firewall menghadapi trafik serangan, sehingga dapat disimpulkan bahwa utilisasi sumber daya sangat dipengaruhi oleh kondisi trafik dan skenario pengujian yang diterapkan (Ibrahim et al., 2023).
b. Arsitektur FortiGate tidak hanya mengandalkan CPU umum (general-purpose), tetapi juga dilengkapi prosesor khusus berupa SPU dan nTurbo sebagai komponen akselerasi perangkat keras. Nilai keduanya yang tercatat 0.0% pada saat observasi menunjukkan bahwa mekanisme hardware acceleration bersifat kondisional, yaitu baru aktif ketika terdapat trafik yang memenuhi kriteria offloading. Hal ini merepresentasikan konsep pembagian beban kerja antara prosesor umum dan prosesor khusus dalam arsitektur komputer.
c. Subsistem I/O pada FortiGate direalisasikan melalui interfaces port yang terdiri dari interface fisik (wan1, wan2) maupun interface logis (802.3ad aggregate, tunnel, dan VLAN switch). Hasil observasi menunjukkan bahwa satu perangkat keras dapat menyediakan banyak jalur I/O logis melalui konfigurasi, di mana kelancaran aliran data ditentukan oleh kombinasi antara kondisi jalur I/O yang aktif dan kapasitas pemrosesan sistem.
d. Hasil validasi silang antara data GUI dan CLI menunjukkan nilai yang konsisten dengan selisih minor akibat perbedaan waktu polling, sehingga data observasi yang digunakan dalam penelitian ini memiliki tingkat validitas yang dapat dipertanggungjawabkan.

Penelitian ini masih terbatas pada observasi kondisi perangkat dalam konfigurasi dasar tanpa pengujian trafik secara aktif. Oleh karena itu, penelitian selanjutnya dapat dikembangkan dengan melakukan pengujian kinerja end-to-end (seperti pengukuran throughput dan latency) menggunakan perangkat klien pada jaringan internal, serta pengamatan perilaku SPU dan nTurbo saat menangani trafik tinggi untuk membuktikan efektivitas mekanisme hardware acceleration secara empiris.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 4, No. 5 Tahun 2026
ISSN 3025-0919 (media online)
Hal 1387-1396

REFERENCES

Alhasan, A. J., & Surantha, N. (2021). Evaluation of Data Center Network Security based on Next-Generation Firewall.

ARCHITECTURES AND RULE SETS. *FUDMA Journal of Sciences (FJS) Vol. 9 No. 12, December 2025*, *2*(12), 306–312.

Fortinet. (2023). *FortiGate 80F Series Data Sheet*. https://www.fortinet.com/resources/data-sheets/fortigate-fortiwifi-80f-series

Grossi, M., Alfonsi, F., Prandini, M., & Gabrielli, A. (2024). Increasing the Security of Network Data Transmission with a Configurable Hardware Firewall Based on Field Programmable Gate Arrays. *Future Internet*, *16*(9). https://doi.org/10.3390/fi16090303

Ibrahim, M. M., Widjajarto, A., & Kurniawan, M. T. (2023). Implementasi dan Analisis Profil Sistem Pada Virtualisasi Fortigate Firewall Berdasarkan Metrik Sumber Daya Komputasi. *EProceedings of Engineering*, *10*(2), 1505–1511.

International Journal of Advanced Computer Science and Applications, *12*(9), 518–525. https://doi.org/10.14569/IJACSA.2021.0120958

Ismail, A. B., Hussaini, M. I., Abubakar, S. A., & Ahmad, A. (2025). EFFICACY AND LIMITATIONS OF FIREWALL CONFIGURATIONS IN PREVENTING NETWORK ATTACKS: A CONCEPTUAL REVIEW OF

Prima Jaya, D., Aspriyono, H., & Suryana, E. (2021). Implementasi Keamanan Jaringan Komputer Menggunakan Fortigate Sebagai Firewall pada Lab Komputer IAIN Bengkulu. *Gatotkaca Journal*, *2*(1), 31–38. https://doi.org/10.37638/gatotkaca.2.1.31-38

Sandi, T. A. A., Firmansyah, F., Raharjo, M., Watmah, S., & Putra, J. L. (2025). Analisa Performa VLAN Dengan Link Aggregation Control Protocol (LACP) Layer 3 Pada Kasus Penentuan Topologi. *INSANtek*, *6*(1), 19–27. https://doi.org/10.31294/insantek.v6i1.8751

Tomar, Y. S., & Bhile, N. (2021). First Line of Defense: Firewall. *Asian Journal of Research in Computer Science*, *12*(3), 25–32. https://doi.org/10.9734/ajrcos/2021/v12i330286