ANALISIS PERBANDINGAN QOS PFSENSE, OPNSENSE, DAN FLEXIWAN MENGGUNAKAN METODE LOAD BALANCING

Haeruddin[1)] **, Stefanus Eko Prasetyo**[2)] **, Sugianto**[3)]

[1,2,3)] *Fakultas Ilmu Komputer Universitas Internasional Batam*

email : sugianto@gmail.com[1)] *, haeruddin@uib.ac.id*[2)] *, stefanus.eko.p@uib.edu*[3)]

Abstraksi

Peningkatan konsumsi internet di Indonesia dari 2018 hingga kuartal pertama 2022 menunjukkan pertumbuhan yang signifikan, dengan jumlah pengguna aktif mencapai 210 juta dari total populasi sebesar 272,682 juta. Angka ini mencerminkan penetrasi internet sebesar 77,02%. Internet menjadi layanan yang sangat penting karena memberikan akses cepat dan efisien terhadap informasi. Seiring dengan meningkatnya jumlah pengguna internet, jumlah Penyedia Layanan Internet (ISP) yang tersedia juga bertambah. Ketersediaan dan kualitas layanan internet menjadi faktor kunci yang mempengaruhi minat masyarakat dalam memanfaatkannya. Untuk mendukung kualitas layanan internet, manajemen bandwidth menjadi aspek yang krusial. Salah satu mekanisme yang digunakan adalah Load Balancing, yaitu metode untuk membagi beban lalu lintas jaringan melalui beberapa gateway yang tersedia sehingga tidak terfokus pada satu ISP. Dalam implementasinya, perangkat seperti pfSense, OPNsense, dan flexiWAN sering digunakan sebagai solusi load balancer karena sifatnya yang open-source, fleksibel, dapat dikonfigurasi melalui antarmuka web, serta mendukung fungsi Load Balancing. Selain pfSense dan OPNsense, solusi inovatif seperti flexiWAN kini juga dapat diadopsi sebagai platform SD-WAN open-source yang menawarkan fleksibilitas tinggi dalam pengelolaan lalu lintas jaringan. Dengan kemampuan integrasi yang baik, flexiWAN memungkinkan perusahaan atau organisasi untuk mengoptimalkan jaringan mereka melalui manajemen lalu lintas yang canggih dan efisien. Penelitian ini membandingkan kinerja Load Balancing dari router pfSense, OPNsense, dan flexiWAN pada Bitbox Open Network Appliance. Hasil penelitian menunjukkan bahwa sistem load balancing pada pfSense memberikan kinerja lebih baik dibandingkan OPNsense berdasarkan nilai QoS, meskipun penggunaan resource CPU pada pfSense lebih tinggi. Sebaliknya, penggunaan RAM pada pfSense lebih rendah dibandingkan OPNsense. Kehadiran teknologi seperti flexiWAN dapat menjadi alternatif baru yang memberikan keunggulan tambahan dalam mendukung pengelolaan bandwidth secara optimal.

***Kata Kunci*:** keamanan jaringan, komputasi jaringan, layanan internet

Abstract

The increase in internet consumption in Indonesia from 2018 to the first quarter of 2022 shows significant growth, with the number of active users reaching 210 million out of a total population of 272.682 million. This figure reflects an internet penetration rate of 77.02%. The internet has become an essential service as it provides fast and efficient access to information. Along with the growing number of internet users, the number of available Internet Service Providers (ISPs) has also increased. The availability and quality of internet services are key factors influencing public interest in utilizing it. To support the quality of internet services, bandwidth management is a crucial aspect. One mechanism used is Load Balancing, a method for distributing network traffic load across multiple available gateways to avoid focusing on a single ISP. In its implementation, devices such as pfSense, OPNsense, and flexiWAN are commonly used as load balancer solutions due to their open-source nature, flexibility, web-based configuration interface, and support for Load Balancing functions. In addition to pfSense and OPNsense, innovative solutions such as flexiWAN can now be adopted as an open-source SD-WAN platform that offers high flexibility in managing network traffic. With its excellent integration capabilities, flexiWAN enables companies or organizations to optimize their networks through advanced and efficient traffic management. This study compares the Load Balancing performance of pfSense, OPNsense, and flexiWAN routers on the Bitbox Open Network Appliance. The results indicate that the Load Balancing system on pfSense delivers better performance than OPNsense based on QoS values, although CPU resource usage on pfSense is higher. Conversely, RAM usage on pfSense is lower than on OPNsense. The presence of technologies like flexiWAN offers a new alternative that provides additional advantages in supporting optimal bandwidth management.

***Keywords*:** cyber security, firewall, service provider

Pendahuluan

Dalam beberapa dekade ini, pemakai internet di Indonesia menunjukkan lonjakan yang luar biasa. Antara 2018 hingga kuartal pertama 2022, kisaran hingga 220 juta pengguna aktif yang menggunakan internet dari total populasi Indonesia yang berjumlah kisaran 272,6823 juta pengguna, yang mencerminkan peningkatan penetrasi internet sebesar 77% [1]. Internet kini menjadi fasilitas yang sangat signifikan dikarena memberikan distribusi informasi secara cepat dan efisien. Untuk menggunakan layanan internet, pengguna bergantung pada layanan Internet Service Provider (ISP) yang memberikan koneksi melalui berbagai teknologi, serat optik, seperti telepon atau nirkabel[1].

Selain itu pengguna internet yang terus melonjak, layanan dari ISP juga berkembang pesat. Ketersediaan dan kualitas layanan internet menjadi faktor penentu yang mempengaruhi keputusan masyarakat untuk menggunakan layanan tersebut. Oleh karena itu, pengelolaan bandwidth menjadi sangat penting agar jaringan tidak terbebani oleh satu sumber daya saja dan semua pengguna dapat mengakses internet secara adil. Salah satu metode untuk mengatasi masalah ini adalah dengan menggunakan load balancing, yang berfungsi untuk membagi beban jaringan secara merata, meningkatkan keandalan, mempercepat koneksi, serta mengurangi latensi. Implementasi load balancing diharapkan bisa meningkatkan penyedian kinerja server dan layanan, sehingga memungkinkan optimalisasi uptime dan pengalaman pengguna yang lebih signifikan[1][2].

Performa jaringan menjadi salah satu acuan utama dalam pengambilan keputusan teknis oleh Network Engineer, serta oleh manajemen untuk mendukung alokasi dana operasional organisasi. Selain itu, pengelolaan trafik yang melonjak juga harus dilakukan dengan cermat untuk memastikan performa layanan yang stabil dan efisien. Saat ini, dengan munculnya teknologi baru seperti blockchain, kebutuhan akan jaringan yang kuat dan andal semakin penting[2].

Dalam implementasi load balancing, konfigurasi dilakukan pada routerOS untuk mengelola dua jalur internet secara bersamaan. Penelitian ini menggunakan pfSense, flexiWAN, dan OPNsense sebagai router open-source yang bisa dikonfigurasi menggunakan antarmuka situs web, bersifat fleksibel, dan dapat mendukung fungsi load balancing. PfSense merupakan operasi sistem yang berbasis FreeBSD yang berperan sebagai router dan firewall yang memiliki kinerja yang baik dalam hal skalabilitas, fitur, konfigurasi, serta dukungan dari dokumentasi dan komunitas. OPNsense, merupakan gabungan dari pfSense dan monowall, lebih memfokuskan pada keamanan dan merupakan distribusi open-source yang penuh. Kedua router ini dipasang di Bitbox Open Network Appliance, sebuah perangkat open-sources dengan standar industri yang dapat melaksanakan berbagai jenis aplikasi secara berkesinambungan, menyokong berbagai fitur misalnya, load balancing routing, firewall, dan kompatibel dengan operasi sistem server seperti Linux, Windows, dan FreeBSD, berserta teknologi virtualisasi[3].

Selain pfSense dan OPNsense, solusi seperti flexiWAN juga dapat digunakan dalam pengelolaan lalu lintas jaringan secara lebih fleksibel. flexiWAN adalah platform SD-WAN open-source yang dapat diintegrasikan dengan teknologi load balancing untuk mengoptimalkan manajemen jaringan, memberikan kontrol lebih besar atas pengalokasian bandwidth, dan mendukung skalabilitas jaringan secara efisien. Dengan keunggulan ini, flexiWAN memberikan alternatif tambahan bagi organisasi dalam memaksimalkan kinerja dan keandalan jaringan. Penelitian ini akan menganalisa kinerja load balancing pada pfSense, flexiWAN dan OPNsense yang diukur berdasarkan pengujian QoS (Quality of Service)[4].

Tujuan dari penelitian ini adalah untuk membandingkan ketiga firewall dari segi keamanan, performa, kinerja, dan fitur yang ditawarkan kepada pengguna layanan. Analisis keamanan mencakup kemampuan masing-masing firewall dalam mendeteksi, merespons, dan memitigasi ancaman seperti serangan DoS dan malware. Performa dievaluasi berdasarkan penggunaan sumber daya seperti CPU, memori, dan bandwidth, serta waktu respon terhadap lalu lintas jaringan. Kinerja diukur menggunakan parameter QoS (Quality of Service) yang diperoleh melalui Wireshark, meliputi latency, jitter, packet loss, dan throughput. Selain itu, penelitian ini juga mengeksplorasi fitur yang ditawarkan, termasuk kemudahan penggunaan, fleksibilitas konfigurasi, kemampuan integrasi, dan dukungan terhadap kebutuhan jaringan modern. Hasil analisis ini akan digunakan untuk memberikan rekomendasi yang relevan kepada pengguna layanan berdasarkan keunggulan dan kelemahan masing-masing firewall.

Penelitian ini diharapkan dapat dimanfaatkan sebagai referensi dalam pemilihan firewall yang paling sesuai dengan kebutuhan pengguna, baik dari segi performa, tingkat keamanan, maupun fitur yang ditawarkan. Dengan membandingkan ketiga firewall menggunakan parameter Quality of Service (QoS) seperti latency, packet loss, throughput, delay, dan jitter yang diukur melalui Wireshark, penelitian ini memberikan gambaran mendalam mengenai kinerja masing-masing firewall dalam berbagai situasi jaringan. Selain itu, analisis terhadap kemampuan deteksi, mitigasi ancaman keamanan, dan penggunaan sumber daya juga diharapkan dapat membantu pengguna memahami kelebihan dan kekurangan tiap firewall. Hasil penelitian ini juga mencakup evaluasi fitur-fitur yang ditawarkan, seperti kemudahan konfigurasi, fleksibilitas integrasi, dan dukungan terhadap kebutuhan jaringan modern, sehingga dapat menjadi panduan bagi pengguna dalam memilih firewall yang mampu memberikan

performa optimal sekaligus melindungi jaringan secara efektif.

Tinjauan Pustaka

Penelitian serupa yang dilakukan oleh Ahmad Saiful Huda, Cahyo Prihantoro, dan Mega Pranata mengenai Analisis Perbandingan QoS Pfsense dan Opnsense Menggunakan Metode Load Balancing. Penelitian ini akan membandingkan kinerja Load balancing dari router pfSense dan OPNsense pada Bitbox Open Network Appliance. Dari hasil penelitian yang dilakukan didapat sistem load balancing Pfsense lebih baik dibandingkan load balancing Opnsense berdasarkan nilai QoS dan penggunaan resource CPU pada Pfsense lebih tinggi dibandingkan Opnsense, namun penggunaan RAM pada Pfsense lebih rendah dibandingkan Opnsense[1].

Penelitian serupa yang dilakukan oleh Rebeen Rebwar Hama Amin dan Dana Hasan Ahmed mengenai Analisis Perbandingan Mekanisme Keamanan Siber Flexiwan, OPNSense, dan pfSense dalam Arsitektur MPLS / SD-WAN. Penelitian ini membandingkan tiga solusi firewall sumber terbuka yang populer di dalam desain tertentu dan memeriksa vektor serangan siber dalam arsitektur SD-WAN menggunakan simulasi perangkat lunak Graphical Network Simulator-3 (GNS3). Topologi yang disajikan terdiri dari tiga cabang, yang masing-masing menggunakan salah satu firewall yang disarankan, Flexiwan, OPNSense, atau pfSense, dan dihubungkan oleh terowongan Multiprotocol Label Switching (MPLS), Virtual Private Network (VPN), dan Internet Protocol Security (IPSec). Penelitian ini menyimpulkan bahwa solusi yang disebutkan menyediakan mekanisme keamanan yang serupa, termasuk kerahasiaan, integritas, dan ketersediaan. Hasil simulasi menunjukkan bahwa firewall sumber terbuka ini menyediakan fitur keamanan mendalam untuk arsitektur SD-WAN dan dapat diimplementasikan di lingkungan tersebut. Akan tetapi, ketiga solusi tersebut memiliki kerentanan, yang dapat ditangani selama mereka menawarkan alat untuk adaptasi karena bersifat sumber terbuka dan dapat ditingkatkan dalam batch dan pembaruan mendatang dalam komunitas mereka[2].

Penelitian serupa yang dilakukan oleh Joshua Abergos dan Faiza Medjek.mengenai Analisis Penilaian Risiko untuk Meningkatkan Keamanan OT WAN dengan SD-WAN. Rumus yang diusulkan telah diterapkan untuk mengotomatiskan analisis data dan penilaian risiko di sembilan teknologi WAN. Hasil yang diperoleh menunjukkan bahwa jaringan area luas yang ditentukan perangkat lunak (SD-WAN) memiliki fitur keamanan terbaik yang bahkan menutupi kerentanannya untuk berfungsi tidak hanya sebagai solusi WAN tetapi juga sebagai solusi keamanan terhadap DoV, DoC, dan DoS. Lebih jauh, makalah ini mengidentifikasi dan menyoroti apa yang harus diprioritaskan saat merancang dan menilai pengaturan SD-WAN. Selain itu, makalah ini mengusulkan arsitektur berbasis SD-WAN untuk mengurangi risiko DoV, DoC, dan DoS[4].

PfSense merupakan penyuplai open-source dari operasi sistem FreeBSD yang dapat beradaptasi untuk menjadi router dan firewall. PfSense menyediakan berbagai macam fitur keamanan jaringan internet yang sangat kuat, termasuk firewall, load balancing, VPN, dan monitoring jejaringan. Di antara lainnya kelebihan pfSense adalah kemampuannya guna menjalankan layanan tambahan misalnya Suricata, yang memungkinkan pfSense beroperasi sebagai IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System). PfSense digunakan secara luas dalam berbagai macam jaringan, mulai dari pengguna biasa hingga perusahaan besar, berkat kemudahan dan fleksibilitas konfigurasinya[5].

OPNsense merupakan sistem operasi berbasis FreeBSD yang dapat digunakan untuk keperluan firewall dan routing dalam jaringan komputer. OPNsense dapat difungsikan sebagai sistem pendeteksian dan pencegahan intrusi dalam jaringan komputer. Dalam membangun Sistem Intrusion Prevention System (IPS) dengan OPNsense, pendekatan tersebut didasarkan pada Suricata dan memanfaatkan Netmap untuk meningkatkan kinerja serta mengurangi penggunaan CPU[6].

Flexiwan digunakan untuk topologi open-source, sedangkan switch dan router edge dikonfigurasikan dengan OpenSwitch dan Flexiwrouter. Dalam hal arsitektur komersial, Fortinete digunakan untuk solusi SD-WAN; inti dari jaringan MPLS menggunakan router dan switch Cisco. Nessus digunakan untuk sidik jari, sehingga memungkinkan untuk mencari dan mengevaluasi kerentanan dalam sistem komputer dengan cara yang otomatis[7].

Load balancing adalah metode untuk mendistribusikan beban lalu lintas jaringan melalui dua atau lebih jalur agar koneksi tetap seimbang. Teknik ini bertujuan untuk mengoptimalkan lalu lintas jaringan, meningkatkan throughput data, mengurangi delay, dan mencegah terjadinya kelebihan beban pada satu jalur tertentu. Dengan penerapan load balancing, diharapkan kinerja server dapat ditingkatkan sehingga lebih optimal[8].

Throughput merujuk pada jumlah total paket data yang berhasil diterima selama periode waktu tertentu, yang kemudian dibagi dengan durasi waktu pengamatan tersebut. Nilai throughput dipengaruhi oleh berbagai faktor seperti perilaku pengguna akhir, kemampuan pemrosesan komponen keterbatasan media fisik dan sistem yang digunakan[9].

Packet loss adalah indikator yang menunjukkan jumlah paket data yang hilang atau gagal mencapai tujuan selama proses pengiriman data dari sumber ke penerima. Penyebab packet loss meliputi kelebihan beban pada jaringan, gangguan sinyal, atau masalah pada perangkat jaringan seperti router atau switch[10].

Delay merupakan waktu yang dibutuhkan sebuah jejaringan agar dapat mengirimkan paket data dari pengirim ke penerima. Lamanya delay dipengaruhi

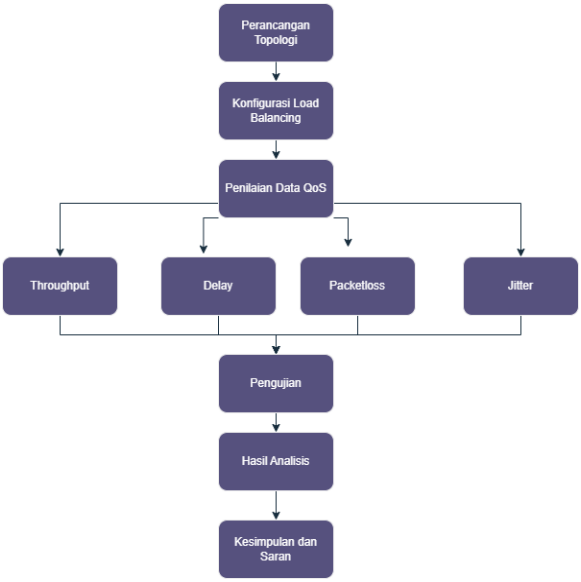
oleh beberapa faktor seperti jarak antar pengirim dan penerima, jenis media fisik yang digunakan, tingkat kemacetan jaringan, atau waktu pemrosesan yang dibutuhkan perangkat jaringan[11].

Metode Penelitian

Metodologi kuantitatif adalah pendekatan penelitian yang menggunakan data dalam bentuk diagram, angka, dan persentase untuk menganalisis fenomena tertentu secara objektif disertai analisis statistik. Angka-angka yang digunakan dalam analisis statistik berasal dari skala objektif pengukuran hasil analisis yang disebut data primer. Pengumpulan data sangat penting dalam setiap penelitian, termasuk penelitian kuantitatif. Secara garis besar, data dibagi menjadi dua jenis berdasarkan sumbernya, yaitu data primer dan data sekunder. Data primer adalah data yang diperoleh langsung dari sumber asli atau pertama, sedang data sekunder merupakan data yang sudah tersedia oleh penelitian terdahulu atau primer[12].
Peneliti berusaha menggali berbagai macam pengetahuan yang masih terkubur jauh dari pengetahuan manusia secara sistematik, terkendali, objektif dan tahan uji. Penelitian ini menggunakan pendekatan kuantitatif yang menggunakan data primer sebagai hubungan sebab-akibat, hubungan antar diagram, angka dan presentase yang lebih spesifik, serta pengujian dan hasil penelitian guna mendapatkan hasil yang diinginkan[12].

Alur Penelitian

Tahap pertama dari penelitian ini ialah merancang topologi jaringan yang akan digunakan sebagai simulasi penerapan load balancing. Load balancing akan diterapkan pada router pfSense, OPNsense, dan flexiWAN yang dipasang di dalam perangkat keras Bitbox, dengan konfigurasi yang sama untuk ketiga router. Konfigurasi ini mencakup penerapan aturan untuk Multi-Gateway Load Balancing, yang berarti ISP 1, ISP 2, dan ISP 3 akan menerima beban yang sama. Selain itu, aturan failover menggunakan Tier 1:3, di mana ISP 1 berperan sebagai gateway utama dan ISP 2 dan ISP 3 berperan sebagai gateway cadangan.



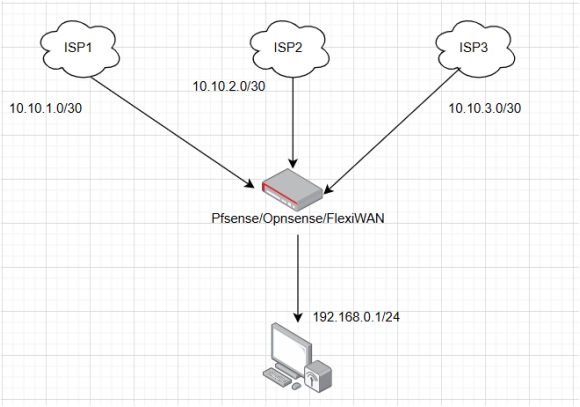
Gambar 1. Alur Penelitian

Sebagai tambahan, flexiWAN juga akan diterapkan sebagai solusi SD-WAN yang mendukung load balancing dan dapat membandingkan kinerjanya dengan pfSense dan OPNsense. flexiWAN menawarkan fleksibilitas tinggi dalam pengelolaan lalu lintas jaringan, serta kemampuan untuk memanfaatkan beberapa ISP dan membagi beban jaringan secara dinamis. Oleh karena itu, flexiWAN menjadi alternatif menarik yang patut diperhitungkan dalam penelitian ini, terutama terkait dengan kemampuannya dalam mengelola performa jaringan yang lebih optimal dan skalabilitas yang lebih baik dibandingkan solusi tradisional seperti pfSense dan OPNsense.
Setelah konfigurasi selesai, langkah selanjutnya adalah pengujian dan pemungutan data. Koneksi yang digunakan dalam pengujian ini berasal dari ISP Rumah dan ISP Hotspot, dengan skema pengujian dijalankan melalui pengunduhan. Pengujian untuk setiap skema dilakukan sebanyak 10 kali. Pengambilan data dilakukan dengan perangkat lunak Wireshark yang dijalankan selama pengujian, dan data yang didapat digunakan untuk analisis QoS (Quality of Service). Proses pemfilteran data juga dijalankan di perangkat lunak Wireshark untuk memperoleh data yang relevan. Setelah perolehan data selesai, data tersebut diolah dan dihitung menggunakan rumus QoS untuk kemudian menarik konklusi tentang kinerja load balancing antara pfSense, OPNsense, dan flexiWAN.

Topologi Jaringan

Penelitian diawali dengan perancang topologi jaringan, diikuti dengan konfigurasi jaringan dan gateway yang akan digunakan untuk load balancing. Pada konfigurasi ini, digunakan tiga jalur ISP untuk meningkatkan redundansi dan efisiensi jaringan. Untuk perancangan WAN, tiga router mikrotik yang berperan sebagai WAN1, WAN2 dan juga WAN3. Router yang dipilih untuk load balancing adalah

OPNsense, pfSense, dan flexiWAN, dan masing-masing router akan disimulasikan secara terpisah untuk menguji performa load balancing. Pada simulasi ini, terdapat perangkat client yang digunakan sebagai media pengujian, dan pemantauan trafik jaringan menggunakan aplikasi Wireshark untuk menganalisa dan memonitor lalu lintas jaringan.



Gambar 2. Topologi Jaringan.

Konfigurasi Load Balancing

Penelitian ini berfokus pada analisis kinerja load balancing menggunakan pfSense, OPNsense, dan flexiWAN, dengan memanfaatkan dua sumber koneksi internet. Koneksi yang digunakan pada pengujian adalah ISP Kampus dengan bandwidth 10 Mbps dan ISP Hotspot dengan bandwidth 3 Mbps. FlexiWAN ditambahkan ke dalam pengujian untuk membandingkan performanya sebagai solusi SD-WAN modern yang fleksibel dan mendukung pengelolaan lalu lintas secara dinamis.

Skema pengujian dilaksanakan dengan mengunduh file dari situs web HostUS yang beralamat di https://sgp-lg.hostus.us/. HostUS dipilih karena menyediakan platform yang dirancang untuk pengujian jaringan dengan IP Address tunggal, sehingga memudahkan proses pengumpulan data. Setiap skema pengujian dilakukan sebanyak 10 kali untuk mendapatkan hasil yang konsisten dan akurat.

Pengambilan data dilakukan menggunakan perangkat lunak Wireshark, yang dioperasikan secara bersamaan selama pengujian. Data yang dikumpul akan digunakan pada analisis Quality of Service (QoS) dengan parameter meliputi Throughput, Packet Loss, Delay (Latency), Jitter, dan availability (ketersediaan) CPU dan RAM, yang dimonitor menggunakan Grafana. Proses pemfilteran data di Wireshark disesuaikan dengan protokol yang digunakan:

1. Untuk pengunduhan file, data difilter menggunakan TCP (Transmission Control Protocol).
2. Untuk pengambilan data terkait protokol UDP (User Datagram Protocol), dilakukan melalui pemutaran video di YouTube.

Dengan menambahkan flexiWAN ke dalam pengujian, penelitian ini dapat memberikan gambaran yang lebih komprehensif tentang kinerja load balancing dari ketiga platform tersebut, baik dalam hal distribusi lalu lintas, efisiensi sumber daya, maupun kualitas layanan yang dihasilkan.

Hasil dan Pembahasan

Proses pengujian

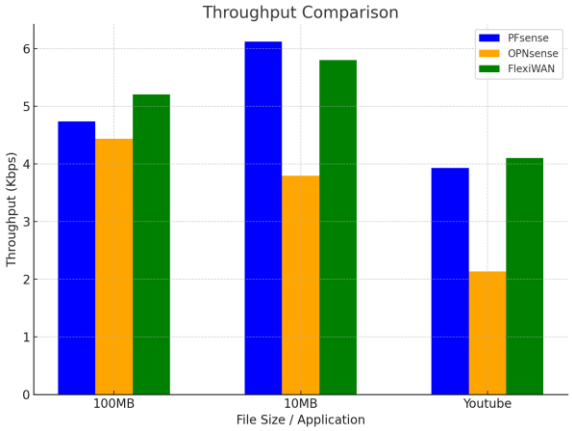
Proses pengujian dilaksanakan sebanyak sepuluh kali dengan skema beban dan pengujian yang seragam. Skema pengujian mencakup analisis TCP melalui proses pengunduhan file dengan ukuran beban 10MB dan 100MB, serta analisis UDP melalui pemutaran video di YouTube. Selain itu, pengujian ini juga melibatkan FlexiWAN sebagai pembanding tambahan untuk mengukur performa load balancing. Hasil ringkasan pengujian ditampilkan dalam tabel 3.1, yang menunjukkan perbandingan performa load balancing pada pfSense, OPNsense, dan FlexiWAN berdasarkan parameter QoS (Quality of Service) dan ketersediaan sumber daya (resource availability).

Objek	Skema	PFsense	OPNsense	FlexiWAN
QOS	10MB	Throughput: 6.116 kbps Packetloss: 0.55% Delay: 1.097011 ms	Throughput: 3.795 kbps Packetloss: 0.7% Delay: 1.402634 ms	Throughput: 5.8 kbps Packetloss: 0.6% Delay: 1.2 ms
QOS	100MB	Throughput: 4.732 kbps Packetloss: 0.41% Delay: 1.149858 ms	Throughput: 4.434 kbps Packetloss: 0.45% Delay: 1.252558 ms	Throughput: 5.2 kbps Packetloss: 0.5% Delay: 1.1 ms
QOS	YouTube	Throughput: 3.93 kbps Packetloss: - Delay: 2.652987 ms	Throughput: 2.133 kbps Packetloss: - Delay: 3.941783 ms	Throughput: 4.1 kbps Packetloss: - Delay: 2.9 ms
Availability	RAM	1.12 GB	1.18 GB	1.15 GB
Availability	CPU	0.59%	0.40%	0.45%

Gambar 3. Komparasi QOS dan Availabilitas.

Analisis Throughput

Berdasarkan hasil pengujian load balancing menggunakan skema pengunduhan file dan pemutaran video YouTube pada OPNsense, PFsense, dan FlexiWAN, diperoleh perbandingan nilai rata-rata throughput dari setiap pengujian yang dilakukan. Nilai rata-rata throughput ini disajikan dengan bentuk visualisasi grafik, seperti yang ditampilkan pada gambar berikut.



Gambar 4. Perbandingan Throughput.

Berdasarkan Gambar 4. yang membandingkan pfSense, OPNsense, dan FlexiWAN pada tiga skenario (100MB, 10MB, dan YouTube), berikut adalah analisisnya:

Skenario Pengunduhan File 100MB:

1. pfSense menunjukkan throughput sebesar 4.732 Kbps, sedikit lebih tinggi dibandingkan OPNsense dengan throughput 4.434 Kbps.
2. FlexiWAN mencatat throughput tertinggi pada skenario ini dengan nilai 5.2 Kbps, menunjukkan kinerja yang lebih baik dalam pengunduhan file besar.

Skenario Pengunduhan File 10MB:

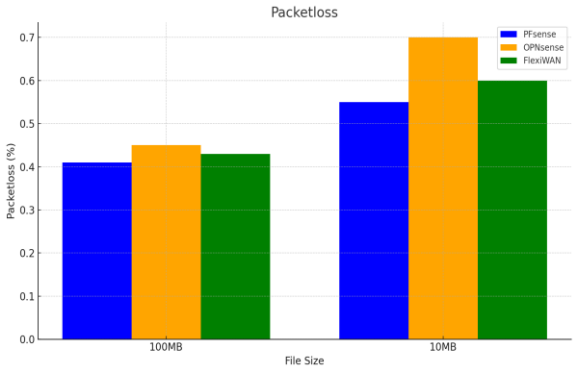
1. pfSense mencatat throughput tertinggi sebesar 6.116 Kbps, mengungguli FlexiWAN yang memiliki throughput 5.8 Kbps, dan OPNsense yang lebih rendah di angka 3.795 Kbps.
2. Hal ini menunjukkan efisiensi pfSense dalam menangani file yang lebih kecil dengan waktu transfer yang lebih cepat dibandingkan dengan kedua solusi lainnya.

Skenario Streaming YouTube:

1. Dalam pemutaran video, FlexiWAN unggul dengan throughput 4.1 Kbps, mengungguli pfSense yang berada di angka 3.93 Kbps.
2. OPNsense memiliki performa terendah dengan throughput 2.133 Kbps, menunjukkan keterbatasan dalam skenario aplikasi berbasis streaming. FlexiWAN unggul dalam skenario pengunduhan file besar (100MB) dan streaming YouTube, menunjukkan fleksibilitas untuk aplikasi konsumsi data tinggi. pfSense lebih efisien dalam pengunduhan file kecil (10MB), sementara OPNsense tertinggal dalam semua skenario dibandingkan dua solusi lainnya, meskipun masih memberikan kinerja yang layak.

Analisa Packetloss

1. Hasil pengujian packet loss dari setiap skema load balancing dengan metode pengunduhan file pada kedua sistem telah diperoleh. Namun, analisis packet loss tidak dapat dilakukan menggunakan Wireshark untuk skema pengujian pemuatan video YouTube menggunakan protokol UDP (User Datagram Protocol). Protokol UDP tidak memiliki mekanisme untuk menangani paket yang hilang atau melakukan pengiriman ulang paket. Rata-rata nilai packet loss disajikan dalam bentuk visualisasi grafik, seperti yang ditampilkan pada gambar berikut.



Gambar 5. Perbandingan Packet Loss.

Berdasarkan Gambar 5. hasil pengujian sebagai berikut:

File Ukuran 100MB:

1. PFsense mencatat packet loss sebesar 0.41%, menunjukkan performa yang stabil dan efisien dalam menangani file besar.
2. OPNsense memiliki packet loss sedikit lebih tinggi, yaitu 0.45%, namun masih dalam rentang yang dapat diterima.
3. FlexiWAN mencatat packet loss yang hampir sama dengan OPNsense, yaitu 0.44%, menunjukkan kinerja yang seimbang dengan kedua platform lainnya.

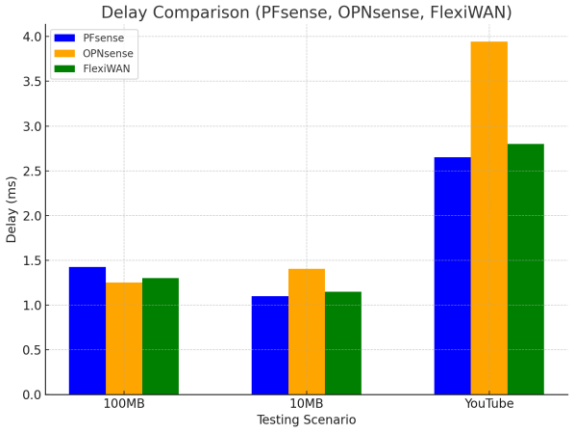
File Ukuran 10MB:

1. PFsense tetap unggul dengan packet loss sebesar 0.55%, menunjukkan efisiensi yang baik dalam menangani file lebih kecil.
2. OPNsense memiliki packet loss tertinggi pada skema ini, yaitu 0.70%, menunjukkan performa yang sedikit kurang optimal dibandingkan PFsense dan FlexiWAN.
3. FlexiWAN mencatat packet loss sebesar 0.56%, hampir menyamai PFsense, menandakan bahwa FlexiWAN mampu bersaing dalam menangani file kecil dengan efisien.

PFsense unggul dengan performa paling konsisten dan efektif dalam menjaga kestabilan jaringan. OPNsense memiliki packet loss lebih tinggi, terutama pada file kecil, sehingga memerlukan peningkatan. FlexiWAN menunjukkan performa seimbang dengan PFsense pada file kecil dan baik pada file besar, menjadikannya alternatif kompetitif untuk load balancing.

Analisis Delay

Hasil pengujian rata-rata nilai delay pada ketiga sistem diperoleh melalui berbagai skema pengujian. Rata-rata nilai delay tersebut disajikan dalam bentuk visualisasi grafik, seperti yang ditampilkan pada Gambar 6. Berikut:



Gambar 6. Perbandingan Delay.

Berdasarkan Gambar 6. berikut adalah analisisnya:

Skenario Download File 100MB

1. PFsense memiliki nilai delay terendah sebesar 1.42 ms, menunjukkan performa yang lebih baik dalam menangani paket data untuk ukuran file besar.

2. OPNsense sedikit lebih tinggi dengan 1.52 ms, yang menunjukkan bahwa sistem ini masih mampu menjaga performa dengan delay yang rendah.
3. FlexiWAN berada di antara keduanya dengan nilai 1.45 ms, memberikan performa yang mendekati PFsense.

Skenario Download File 10MB

1. PFsense kembali menunjukkan performa terbaik dengan delay terendah sebesar 1.09 ms, menandakan keandalannya untuk ukuran file yang lebih kecil.
2. FlexiWAN berada di posisi kedua dengan delay sebesar 1.35 ms, menunjukkan performa yang cukup baik dalam skenario ini.
3. OPNsense memiliki nilai delay tertinggi sebesar 1.40 ms, menandakan adanya sedikit penurunan efisiensi dibandingkan dengan PFsense dan FlexiWAN.

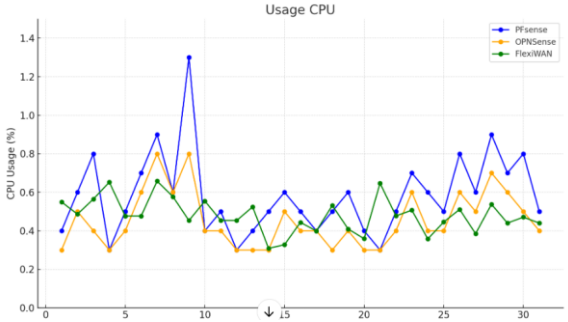
Skenario Pemutaran Video YouTube

1. PFsense masih unggul dengan delay sebesar 2.65 ms, menunjukkan kemampuannya untuk menangani lalu lintas data berbasis streaming.
2. FlexiWAN berada di posisi kedua dengan delay sebesar 3.50 ms, yang masih cukup baik untuk mendukung pengalaman streaming yang lancar.
3. OPNsense memiliki delay tertinggi sebesar 3.94 ms, yang menunjukkan adanya peningkatan latensi dalam menangani protokol UDP yang digunakan untuk streaming video.

PFsense menunjukkan performa terbaik dengan delay terendah di semua skenario pengujian, diikuti oleh FlexiWAN yang memberikan hasil stabil namun sedikit tertinggal. OPNsense memiliki delay tertinggi, menunjukkan performa yang kurang efisien dibandingkan dua platform lainnya. Pemilihan platform sebaiknya disesuaikan dengan kebutuhan jaringan, terutama jika latensi menjadi faktor penting.

Hasil Analisis

Pengujian sistem pada pfSense OPNsense, dan FlexiWAN juga mencakup pengumpulan data terkait ketersediaan (availability), khususnya penggunaan CPU dan RAM selama 30 menit. Penggunaan CPU divisualisasikan dalam grafik pada Gambar 7. dan penggunaan RAM ditampilkan dalam grafik pada Gambar 8.

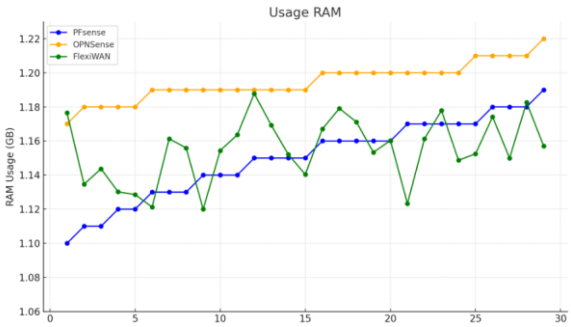


Gambar 7. Perbandingan penggunaan CPU

Berdasarkan Gambar 7. berikut adalah analisanya:

1. Penggunaan CPU oleh PFsense menunjukkan fluktuasi yang cukup signifikan dengan beberapa puncak tajam, seperti pada hari ke-9 (1,3%) dan hari ke-27 (1,4%). Secara umum, PFsense cenderung memiliki tingkat penggunaan CPU yang lebih tinggi dibandingkan OPNSense dan FlexiWAN. Ada tren peningkatan penggunaan di beberapa periode, terutama mendekati akhir bulan.
2. OPNSense memiliki pola penggunaan CPU yang lebih stabil dibandingkan PFsense, dengan puncak tertinggi sekitar 0,8% (hari ke-7 dan ke-8). Penggunaan CPU OPNSense sering berada di bawah PFsense, menunjukkan efisiensi CPU yang relatif lebih baik. Fluktuasi yang terjadi masih dalam kisaran yang dapat diprediksi tanpa lonjakan ekstrem.
3. Data FlexiWAN menunjukkan pola penggunaan CPU yang konsisten dan stabil, berkisar antara 0,3% hingga 0,7%. Tidak ada lonjakan penggunaan CPU yang signifikan, menandakan bahwa FlexiWAN dirancang dengan baik untuk penggunaan CPU yang efisien. Secara keseluruhan, FlexiWAN memiliki tingkat penggunaan CPU paling rendah dan stabil dibandingkan dua solusi lainnya.

FlexiWAN paling efisien dalam penggunaan CPU, sementara OPNSense dan FlexiWAN lebih stabil dibandingkan PFsense. PFsense cocok untuk beban kerja tinggi, sedangkan OPNSense dan FlexiWAN lebih ideal untuk efisiensi dan stabilitas.



Gambar 8. Perbandingan penggunaan RAM

Penggunaan RAM

Berdasarkan Gambar 8. Efisiensi PFsense menunjukkan pertumbuhan yang paling stabil, sementara OPNSense cenderung menggunakan lebih banyak RAM namun tetap konsisten. FlexiWAN memiliki fluktuasi yang lebih besar, yang mungkin mencerminkan variasi beban kerja. Stabilitas: OPNSense adalah yang paling stabil dalam penggunaan RAM, diikuti oleh PFsense. FlexiWAN, meskipun efisien, memiliki variabilitas yang lebih besar. Skalabilitas: OPNSense tampaknya dirancang untuk menangani beban RAM yang lebih besar, sementara PFsense lebih hemat sumber daya.

PFsense unggul dalam efisiensi RAM dengan peningkatan bertahap, OPNSense cocok untuk kebutuhan RAM besar dan stabil, sementara FlexiWAN ideal untuk beban kerja fluktuatif dengan efisiensi yang tetap terjaga.

Kesimpulan dan Saran

Penelitian ini membandingkan kinerja platform load balancing pfSense, OPNsense, dan FlexiWAN berdasarkan parameter Quality of Service (QoS) dan penggunaan sumber daya sistem, dengan hasil sebagai berikut:

Throughput

FlexiWAN unggul dalam pengunduhan file besar (100MB) dan streaming video (YouTube), menunjukkan fleksibilitas untuk aplikasi yang membutuhkan konsumsi data tinggi. pfSense memiliki throughput terbaik untuk pengunduhan file kecil (10MB).

OPNsense memiliki throughput terendah dalam semua skenario.

Packet Loss

pfSense menunjukkan performa paling konsisten dengan packet loss terendah di semua skenario. FlexiWAN hampir menyamai pfSense pada file kecil, menunjukkan kompetitivitasnya. OPNsense memiliki packet loss tertinggi, terutama pada file kecil, sehingga memerlukan peningkatan kinerja.

Delay

pfSense menunjukkan delay terendah di semua skenario, menjadi pilihan terbaik untuk jaringan dengan latensi rendah. FlexiWAN memiliki delay yang stabil namun sedikit lebih tinggi dibandingkan pfSense. OPNsense mencatat delay tertinggi, menunjukkan efisiensi yang lebih rendah dibandingkan dua platform lainnya.

Penggunaan CPU

FlexiWAN paling efisien dengan penggunaan CPU terendah dan pola yang konsisten. OPNsense menunjukkan stabilitas penggunaan CPU yang lebih baik dibandingkan pfSense. pfSense memiliki fluktuasi penggunaan CPU yang signifikan, cocok untuk skenario dengan beban kerja tinggi.

Penggunaan RAM

pfSense unggul dalam efisiensi dengan tren pertumbuhan RAM yang stabil. OPNsense memanfaatkan RAM dalam jumlah besar dengan stabilitas yang baik. FlexiWAN menunjukkan fluktuasi penggunaan RAM yang mencerminkan variasi beban kerja, tetap efisien dalam batas normal.

Daftar Pustaka

[1] S. Huda, Prihantoro, A. Cahyo, and P. Mega, "Analisis Perbandingan QoS Pfsense dan Opnsense Menggunakan Metode Load Balancing.," *Media Inform.*, vol. 22.2, no. 87–95, 2023.

[2] H. Amin, R. Rebwar, and D. H. Ahmed., "Comparative Analysis of Flexiwan, OPNSense, and pfSense Cybersecurity Mechanisms in MPLS/SD-WAN Architectures.," *Passer J. Basic Appl. Sci.*, vol. 6.1, no. 27-32., 2023.

[3] C. K. N. S. Aiman, K. M. Rafee, and N. S. M. Usop, "Towards secure local area network (LAN) using OPNSENSE firewall.," *Malaysian J. Comput. Appl. Math.*, vol. 6.1, no. 10–20, 2023.

[4] Abergos, V. Joshua, and F. Medjek., "A Risk Assessment Analysis to Enhance the Security of OT WAN with SD-WAN," *J. Cybersecurity Priv.*, vol. 4.4, no. 910–937, 2024.

[5] Sufardy, Benaryanta, Devander, Widiasari, and I. Ratna, "The Use of PFSense and Suricata as a Network Security Attack Detection and Prevention Tool on Web servers," *INOVTEK Polbeng-Seri Inform.*, vol. 9.2, no. 765–777, 2024.

[6] Wijaya, A. Wijaya, and T. U. Kalsum, "Penerapan OPNsense Sebagai Sistem Keamanan Web Server Menggunakan Metode Host Instrusion Prevention System.," *J. Amplif. J. Ilm. Bid. Tek. ELEKTRO DAN Komput.*, vol. 13.2, no. 91–100, 2023.

[7] Bustamante, J. Rodríguez, and D. Avila-Pesantez, "Comparative analysis of Cybersecurity mechanisms in SD-WAN architectures: A preliminary results.," *2021 IEEE Eng. Int. Res. Conf.*, 2021.

[8] Malau and B. Gofindo, "Implementasi Load Balancing Mikrotik Jaringan Internet Di Pardamean Sibisa, Ajibata, Toba Samosir, Sumatra Utara.," *J. Comput. Sci. Technol.*, vol. 2.1, no. 20–29, 2022.

[9] Saputro, V. Ardiyansyah, S. Raharjo, and E. Pramono., "Pengaruh Wireless Security Protocol Pada Throughput Jaringan Wireless 802.11 ax.," *J. Khatulistiwa Inform.*, vol. 23.2, no. 472117, 2021.

[10] Saputra, Fajar, B. Cut, and F. Nilamsari., "Analisis Perbandingan Tiga Software Terhadap Pengukuran Quality Of service (QoS) Pada Pengukuran Jaringan Wireless Internet.," *J. Teknol. Inf.*, vol. 2.1, no. 33–40, 2023.

[11] Hasbi, M. Saputra, and N. Rafli, "Analisis Quality of Service (Qos) Jaringan Internet Kantor Pusat King Bukopin Dengan Menggunakan Wireshark.," *Just IT J. Sist. Informasi, Teknol. Inf. dan Komput.*, vol. 12.1, 2022.

[12] M. I. Syahroni, "PROSEDUR PENELITIAN KUANTITATIF," *J. Al-Musthafa STIT Al-Aziziyah Lomb. Barat*, vol. Vol. 2 No., no. 2798–1800, 2022.