Jurnal Publikasi Ilmu Komputer dan Multimedia

E-ISSN: 2808-8999
P-ISSN: 2808-9375

Evaluasi Kinerja High Availability Firewall pfSense Menggunakan CARP pada Jaringan Lokal

Ade Frihadi [1], Silviana Windasari[2*], Abdurohman[3]

[1,2*] **Department of Electrical Engineering, Faculty of Engineering,Universitas Sains Indonesia, Indonesia**
[3] **Graduate School of Electrical Engineering, School of Bioscience, Technology and Innovation (SBTI), Atma Jaya Catholic University of Indonesia, Jakarta, Indonesia**

email : ade.frihadi@lecturer.sains.ac.idsilviana.windasari@lecturer.sains.ac.id*, kang.abdurohman@gmail.com[3]

Abstract: The availability of network services is a crucial factor in supporting organizational activities, particularly in environments that rely on continuous network connectivity. Disruptions to firewall devices can cause the entire network service to stop, as firewalls function as the central point for security enforcement and traffic management. One solution to address this issue is the implementation of a High Availability (HA) mechanism. This study aims to evaluate the performance of a High Availability system on a pfSense firewall using the Common Address Redundancy Protocol (CARP) in a local network environment. The research method employed is an experimental approach by deploying two pfSense devices configured in a master–backup scheme. Testing was conducted by simulating failures on the primary firewall and measuring network performance parameters, including failover time, packet loss, delay, and connection stability during the service transition process. The results show that the implementation of CARP on the pfSense firewall is capable of performing automatic failover with relatively short service switching time and minimal network disruption. Network connectivity can be well maintained, particularly for TCP-based services, indicating that this High Availability system is effective in improving the reliability and availability of local networks. This study is expected to serve as a reference for implementing pfSense-based redundant firewall systems in small- to medium-scale network environments.

Keywords: PfSense; High Availability; CARP; Firewall; Failover

Diterima: 11 Februari 2026
Direvisi: 16 Februari 2026
Diterima: 18 Februari 2026
Diterbitkan: 28 Februari 2026
Versi sekarang: Januari 2026

Abstrak: Ketersediaan layanan jaringan merupakan faktor penting dalam mendukung aktivitas organisasi, khususnya pada lingkungan yang bergantung pada konektivitas jaringan secara terus-menerus. Gangguan pada perangkat firewall dapat menyebabkan terhentinya seluruh layanan jaringan karena firewall berperan sebagai titik sentral pengamanan dan pengaturan trafik. Salah satu solusi untuk mengatasi permasalahan tersebut adalah penerapan mekanisme High Availability (HA). Penelitian ini bertujuan untuk mengevaluasi kinerja sistem High Availability pada firewall pfSense menggunakan Common Address Redundancy Protocol (CARP) dalam lingkungan jaringan lokal. Metode penelitian yang digunakan adalah metode eksperimental dengan membangun dua perangkat pfSense yang dikonfigurasikan dalam skema master–backup. Pengujian dilakukan dengan mensimulasikan kegagalan pada firewall utama dan mengukur parameter kinerja jaringan berupa waktu failover, packet loss, delay, dan stabilitas koneksi selama proses perpindahan layanan. Hasil pengujian menunjukkan bahwa implementasi CARP pada firewall pfSense mampu melakukan proses failover secara otomatis dengan waktu perpindahan layanan yang relatif singkat dan gangguan jaringan yang minimal. Koneksi jaringan dapat dipertahankan dengan baik, terutama pada layanan berbasis TCP, sehingga sistem High Availability ini efektif dalam meningkatkan keandalan dan ketersediaan jaringan lokal. Penelitian ini

diharapkan dapat menjadi referensi dalam penerapan firewall redundan berbasis pfSense pada lingkungan jaringan skala kecil hingga menengah.

Kata kunci: PfSense; High Availability; CARP; Firewall; Failover

1. Pendahuluan

Perkembangan teknologi informasi telah mendorong meningkatnya kebutuhan akan infrastruktur jaringan yang andal dan selalu tersedia. Hampir seluruh aktivitas organisasi, baik pada sektor pendidikan, pemerintahan, maupun bisnis, bergantung pada jaringan komputer sebagai media pertukaran data dan akses layanan digital [1], [2]. Ketergantungan tersebut menuntut sistem jaringan memiliki tingkat ketersediaan yang tinggi agar layanan tetap dapat diakses secara berkelanjutan. Firewall merupakan salah satu komponen utama dalam arsitektur jaringan komputer yang berfungsi sebagai pengaman sekaligus pengatur lalu lintas data antara jaringan internal dan jaringan eksternal [3], [4], [5]. Seluruh trafik jaringan umumnya melewati perangkat firewall sebelum diteruskan ke jaringan internal. Kondisi ini menjadikan firewall sebagai titik kritis dalam sistem jaringan. Apabila firewall mengalami gangguan, maka seluruh layanan jaringan dapat terhenti secara keseluruhan. Pada banyak implementasi jaringan skala kecil hingga menengah, firewall masih diterapkan menggunakan satu perangkat tunggal. Arsitektur tersebut menimbulkan permasalahan single point of failure, yaitu kondisi ketika kegagalan satu perangkat menyebabkan sistem tidak dapat beroperasi [3], [5], [6]. Dampak dari kegagalan firewall dapat berupa terputusnya koneksi internet, terganggunya akses aplikasi internal, serta terhambatnya aktivitas operasional organisasi. Untuk mengatasi permasalahan tersebut, konsep High Availability (HA) diterapkan sebagai solusi peningkatan keandalan sistem jaringan. High Availability bertujuan menjaga ketersediaan layanan dengan meminimalkan waktu henti (downtime) melalui penggunaan perangkat cadangan yang dapat mengambil alih fungsi utama secara otomatis [6], [7]. Dengan adanya mekanisme HA, sistem jaringan diharapkan tetap dapat beroperasi meskipun terjadi gangguan pada perangkat utama.

PfSense merupakan sistem operasi firewall berbasis open source yang banyak digunakan karena stabilitas, fleksibilitas, serta kelengkapan fitur yang dimilikinya. pfSense mendukung berbagai layanan jaringan seperti firewall stateful, NAT, VPN, serta manajemen trafik [8], [9]. Selain itu, pfSense juga menyediakan fitur High Availability yang dapat diimplementasikan menggunakan Common Address Redundancy Protocol (CARP). CARP merupakan protokol redundansi yang memungkinkan beberapa perangkat jaringan berbagi satu alamat IP virtual. Dalam mekanisme ini, satu perangkat berperan sebagai master yang aktif melayani trafik, sedangkan perangkat lainnya berfungsi sebagai backup [10], [11], [12]. Ketika perangkat master mengalami gangguan, perangkat backup secara otomatis mengambil alih alamat IP virtual sehingga layanan jaringan tetap dapat diakses oleh pengguna tanpa perlu konfigurasi ulang. Meskipun fitur High Availability berbasis CARP telah tersedia pada pfSense, implementasinya pada jaringan lokal masih memerlukan evaluasi kinerja secara kuantitatif. Evaluasi tersebut penting untuk mengetahui seberapa cepat proses failover berlangsung dan sejauh mana gangguan jaringan terjadi selama proses perpindahan layanan. Oleh karena itu, penelitian ini dilakukan untuk mengevaluasi kinerja High Availability firewall pfSense menggunakan CARP berdasarkan parameter waktu failover, packet loss, delay, dan stabilitas koneksi jaringan.

2. Tinjauan Literatur

2.1. Firewall Jaringan

Firewall merupakan sistem keamanan jaringan yang berfungsi untuk mengontrol lalu lintas data yang masuk dan keluar berdasarkan aturan tertentu. Firewall digunakan untuk melindungi jaringan internal dari akses tidak sah serta berbagai ancaman jaringan [4]. Secara umum, firewall dapat diimplementasikan dalam bentuk perangkat keras, perangkat lunak, maupun kombinasi keduanya. Firewall modern umumnya bersifat stateful, yaitu mampu

memantau status koneksi jaringan sehingga hanya paket data yang sesuai dengan status koneksi yang diizinkan untuk melewati sistem [13]. Dengan kemampuan ini, firewall dapat memberikan tingkat keamanan yang lebih tinggi dibandingkan firewall stateless yang hanya memeriksa header paket. Dalam arsitektur jaringan, firewall ditempatkan sebagai gerbang utama antara jaringan internal dan jaringan eksternal. Oleh karena itu, keberlangsungan operasional firewall sangat menentukan ketersediaan layanan jaringan secara keseluruhan [14].

2.2 Konsep High Availability

High Availability (HA) merupakan konsep perancangan sistem yang bertujuan untuk menjaga layanan tetap tersedia dengan meminimalkan waktu henti akibat kegagalan sistem [15]. HA dicapai melalui penggunaan perangkat redundan yang mampu mengambil alih fungsi sistem utama secara otomatis. Parameter utama dalam High Availability meliputi:

- Mean Time Between Failure (MTBF)
- Mean Time To Repair (MTTR)
- tingkat availability sistem

Secara matematis, tingkat ketersediaan sistem dapat dinyatakan sebagai berikut [16]:

$$Availability = \frac{MTBF}{MTBF+MTTR}\ X\ 100\% \quad (1)$$

Semakin kecil nilai MTTR dan semakin besar MTBF, maka tingkat ketersediaan sistem akan semakin tinggi.

2.3 PfSense sebagai Firewall Open Source

PfSense merupakan sistem operasi firewall dan router berbasis FreeBSD yang bersifat open source. pfSense banyak digunakan pada jaringan skala kecil hingga enterprise karena memiliki stabilitas tinggi dan dukungan fitur yang lengkap [17].

Beberapa fitur utama pfSense antara lain:

- Stateful firewall
- Network Address Translation (NAT)
- Virtual Private Network (VPN)
- Traffic shaping
- High Availability

Kemampuan High Availability pada pfSense menjadikannya solusi alternatif yang ekonomis dibandingkan perangkat firewall komersial [18], [19].

2.4 Common Address Redundancy Protocol (CARP)

Common Address Redundancy Protocol (CARP) merupakan protokol redundansi layer-3 yang dikembangkan untuk menyediakan mekanisme alamat IP virtual pada beberapa

perangkat jaringan [20]. CARP memungkinkan dua atau lebih perangkat berbagi satu alamat IP yang sama.

Dalam implementasinya, CARP menggunakan konsep:

- Master → perangkat aktif
- Backup → perangkat cadangan

Pemilihan master dilakukan berdasarkan nilai advertisement interval dan skew. Apabila perangkat master berhenti mengirimkan iklan CARP, maka perangkat backup secara otomatis mengambil alih peran sebagai master [21]. CARP banyak digunakan pada firewall berbasis FreeBSD karena stabilitas dan kemampuannya dalam melakukan failover secara cepat.

2.5 Sinkronisasi State (pfsync)

Proses failover tidak memutus koneksi yang sedang aktif, pfSense menggunakan mekanisme sinkronisasi state yang dikenal sebagai pfsync. Mekanisme ini berfungsi untuk menyinkronkan tabel koneksi dan status NAT antar firewall master dan backup. Dengan adanya pfsync, koneksi TCP yang sedang berlangsung dapat tetap dipertahankan ketika terjadi perpindahan layanan. Hal ini sangat penting terutama pada layanan berbasis web dan aplikasi internal.

2.6 Parameter Kualitas Layanan Jaringan

Evaluasi kinerja jaringan umumnya dilakukan dengan mengukur beberapa parameter Quality of Service (QoS), antara lain:

- Delay

  Merupakan waktu tempuh paket data dari pengirim ke penerima.

- PacketLoss

  Menunjukkan persentase paket yang hilang selama transmisi data.

- Throughput

  Menunjukkan jumlah data yang berhasil dikirim dalam satuan waktu.

Dalam penelitian ini, fokus pengukuran diarahkan pada delay dan packet loss karena kedua parameter tersebut paling terpengaruh saat proses failover berlangsung.

2.7 Penelitian Terkait

Beberapa penelitian sebelumnya telah membahas implementasi High Availability pada firewall. Penelitian oleh Ramadhan [20] melakukan implementasi CARP pada pfSense dan menyimpulkan bahwa mekanisme tersebut mampu meningkatkan ketersediaan jaringan. Penelitian lain oleh Fattahilah [7] menunjukkan bahwa firewall redundan mampu mengurangi downtime secara signifikan dibandingkan firewall tunggal. Namun, sebagian besar penelitian masih berfokus pada aspek implementasi tanpa melakukan pengukuran detail terhadap waktu failover dan stabilitas koneksi secara kuantitatif. Oleh karena itu, penelitian ini difokuskan pada evaluasi kinerja CARP melalui pengujian langsung pada jaringan lokal.

3. Metode

3.1. Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan metode eksperimental, yaitu dengan melakukan pengujian langsung terhadap sistem jaringan yang dibangun. Pendekatan eksperimental dipilih karena mampu memberikan gambaran nyata mengenai kinerja sistem High Availability ketika terjadi gangguan pada perangkat utama. Eksperimen dilakukan dengan membangun dua perangkat firewall pfSense yang dikonfigurasikan dalam skema master–backup. Selanjutnya dilakukan simulasi gangguan untuk mengamati proses failover serta dampaknya terhadap kualitas layanan jaringan.

3.2. Lingkungan dan Perangkat Penelitian

3.2.1. Perangkat Keras

Perangkat keras yang digunakan dalam penelitian ini adalah satu unit laptop yang digunakan sebagai media virtualisasi untuk menjalankan seluruh komponen jaringan. Spesifikasi perangkat keras ditunjukkan pada Tabel 1.

Tabel 1. Spesifikasi Perangkat Keras

No	Perangkat	Spesifikasi
1	Laptop	Intel Core i7 3,04 GHz
2	Memori	RAM 8 GB
3	Media Penyimpanan	HDD 500 GB

Laptop digunakan sebagai host system yang menjalankan beberapa mesin virtual, termasuk firewall pfSense master, firewall pfSense backup, dan perangkat client.

3.2.2. Perangkat Lunak

Perangkat lunak yang digunakan dalam penelitian ini ditunjukkan pada Tabel 2.

Tabel 2. Spesifikasi Perangkat Lunak

No	Perangkat Lunak	Keterangan
1	Oracle VirtualBox	Platform virtualisasi
2	pfSense Community Edition	Versi 2.8.0
3	Sistem Operasi Client	Windows/Linux
4	Wireshark	Monitoring trafik jaringan
5	Command Prompt	Pengujian koneksi

Penggunaan teknologi virtualisasi memungkinkan simulasi lingkungan jaringan dilakukan secara fleksibel tanpa memerlukan perangkat fisik tambahan, sehingga proses pengujian dapat dikontrol dengan lebih baik.

3.3. Arsitektur dan Topologi Jaringan

3.3.2. Arsitektur Sistem Jaringan

Arsitektur jaringan yang digunakan dalam penelitian ini dirancang menggunakan konsep High Availability dengan dua firewall pfSense yang dikonfigurasikan dalam skema master–backup. Sistem dibangun pada lingkungan virtualisasi menggunakan Oracle VirtualBox, sehingga seluruh perangkat jaringan direpresentasikan dalam bentuk mesin virtual.

Setiap firewall pfSense memiliki tiga antarmuka jaringan, yaitu:

1. Interface WAN

   Digunakan sebagai jalur koneksi ke jaringan eksternal atau internet.
2. Interface LAN

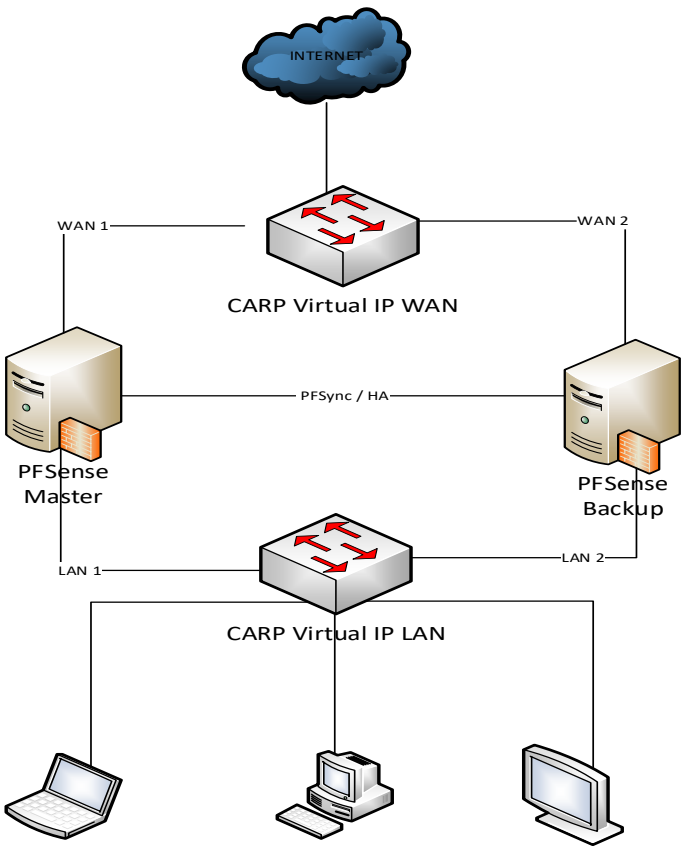
   Digunakan sebagai jalur komunikasi ke jaringan internal dan client.
3. Interface SYNC

   Digunakan khusus untuk proses sinkronisasi state koneksi (pfsync) dan pertukaran informasi CARP antar firewall.

Client jaringan menggunakan Virtual IP (VIP) yang dihasilkan oleh mekanisme CARP sebagai default gateway. Dengan demikian, client tidak terpengaruh oleh perubahan status firewall aktif ketika terjadi proses failover.

3.3.3. Topologi Jaringan

Topologi jaringan High Availability pada jaringan lokal yang diterapkan pada penelitian ini ditunjukkan pada Gambar 1.



Gambar 2. Topologi High Availability Firewall pfSense Menggunakan CARP

Pada kondisi normal, firewall pfSense master berperan sebagai perangkat aktif yang melayani seluruh lalu lintas jaringan. Firewall pfSense backup berada dalam kondisi siaga dan terus menerima sinkronisasi state dari firewall master melalui interface SYNC. Ketika firewall master mengalami gangguan, firewall backup secara otomatis mengambil alih peran master

dan mengaktifkan Virtual IP, sehingga client tetap dapat mengakses jaringan tanpa perubahan konfigurasi.

4. Hasil dan Pembahasan

4.1 . Hasil Pengujian Waktu Failover

Pengujian waktu failover dilakukan untuk mengetahui kecepatan perpindahan layanan dari firewall pfSense master ke firewall pfSense backup ketika terjadi gangguan. Pengujian dilakukan dengan beberapa skenario gangguan yang telah ditentukan pada tahap metodologi. Hasil pengujian waktu failover ditunjukkan pada Tabel 3.

Tabel 3. Hasil Pengujian Waktu Failover

No	Skenario Gangguan	Waktu Failover (detik)
1	Pemutusan koneksi WAN master	1,8
2	Shutdown firewall master	2,6
3	Restart service firewall	1,4
4	Disconnect interface LAN	2,1
Rata-rata		1,97

Berdasarkan hasil pengujian, rata-rata waktu failover yang diperoleh adalah sebesar 1,97 detik. Nilai tersebut menunjukkan bahwa mekanisme CARP mampu melakukan perpindahan layanan secara cepat tanpa memerlukan konfigurasi ulang pada sisi client.

4.2 . Analisis Packet Loss

Packet loss diukur menggunakan pengujian ICMP (ping) secara terus-menerus dari sisi client menuju gateway jaringan. Pengukuran dilakukan sebelum, saat, dan setelah proses failover berlangsung. Hasil pengujian menunjukkan bahwa packet loss hanya terjadi pada saat transisi failover. Rata-rata packet loss yang tercatat berada pada rentang 1–2%, dan kembali normal setelah firewall backup aktif sepenuhnya. Nilai tersebut masih berada dalam batas toleransi jaringan lokal, sehingga tidak memberikan dampak signifikan terhadap kualitas layanan jaringan.

4.3 . Analisis Delay

Delay diukur berdasarkan waktu respon paket ICMP dari client ke gateway. Pada kondisi normal, delay rata-rata berada pada kisaran 2–3 ms. Namun saat proses failover berlangsung, delay mengalami peningkatan sementara hingga mencapai 15–20 ms. Peningkatan delay tersebut bersifat sementara dan terjadi akibat proses pemilihan master CARP serta sinkronisasi state firewall. Setelah proses failover selesai, nilai delay kembali mendekati kondisi normal.

4.4 . Stabilitas Koneksi Jaringan

Stabilitas koneksi diamati melalui kontinuitas pengiriman paket dan keberlangsungan sesi koneksi jaringan. Hasil pengamatan menunjukkan bahwa koneksi jaringan hanya mengalami gangguan singkat selama proses failover. Penggunaan mekanisme pfsync pada pfSense memungkinkan sinkronisasi state koneksi antara firewall master dan backup, sehingga sesi komunikasi dapat dipertahankan dengan baik. Hal ini sangat membantu dalam menjaga layanan berbasis TCP tetap aktif selama proses perpindahan layanan.

6. Kesimpulan

Hasil penelitian menunjukkan bahwa implementasi High Availability menggunakan CARP pada firewall pfSense mampu meningkatkan keandalan jaringan lokal secara signifikan. Waktu failover yang relatif singkat dengan rata-rata waktu perpindahan layanan sebesar 1,97 detik menunjukkan bahwa sistem mampu meminimalkan downtime ketika terjadi gangguan pada firewall utama. Packet loss dan peningkatan delay hanya terjadi sementara saat proses failover berlangsung dan kembali normal setelah firewall backup aktif. Temuan ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa mekanisme redundansi firewall dapat meningkatkan tingkat ketersediaan jaringan secara keseluruhan. Penggunaan virtualisasi tidak memengaruhi validitas hasil karena simulasi dilakukan secara terkontrol dan konsisten. Dengan biaya implementasi yang relatif rendah dan berbasis perangkat lunak open source, pfSense dengan CARP menjadi solusi yang efektif bagi organisasi skala kecil hingga menengah yang membutuhkan sistem jaringan andal tanpa investasi perangkat mahal.

Saran untuk penelitian selanjutnya pengujian dapat diperluas pada aplikasi real-time seperti VoIP dan video conference untuk mengetahui dampak failover secara lebih spesifik, mengimplementasikan skenario multi-WAN untuk mengevaluasi kinerja High Availability pada jaringan yang lebih kompleks dan evaluasi performa dapat dilakukan dengan membandingkan pfSense dengan perangkat firewall lain guna memperoleh hasil yang lebih komprehensif.

Referensi

[1] E. Tabaku and E. Duçi, "Optimizing High Availability in Educational Systems Using Xen Paravirtualization," *J. Educ. Soc. Res.*, vol. 15, no. 2, pp. 205–225, 2025, doi: 10.36941/jesr-2025-0054.

[2] M. Tornatore, T. Gomes, C. Mas-Machuca, S. Ayoubi, E. Oki, and C. Assi, "Guest Editors' Introduction: Special Section on Design and Management of Reliable Communication Networks," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 3, pp. 2455–2459, 2021, doi: 10.1109/TNSM.2021.3103145.

[3] C.-S. Chao, "Developing a Feasible Firewall System with Parallel Rule Allocation Optimization for High Service Availability under Large-Scale Network Attacks," in *2023 IEEE 5th Eurasia Conference on IOT, Communication and Engineering (ECICE)*, 2023, pp. 56–60. doi: 10.1109/ECICE59523.2023.10383082.

[4] F. P. E. Putra, M. Dafid, and I. Syafi'i, "Firewall Implementation as a Computer Network Security Strategy for Data Protection," *Brill. Res. Artif. Intell.*, vol. 5, no. 1, pp. 291–297, 2025, doi: 10.47709/brilliance.v5i1.6162.

[5] A.-D. Tudosi, D. G. Balan, and A. D. Potorac, "Secure network architecture based on distributed firewalls," in *2022 International Conference on Development and Application Systems (DAS)*, 2022, pp. 85–90. doi: 10.1109/DAS54948.2022.9786092.

[6] A. I. Al-Darrab and A. M. A. Rushdi, "Multi-State Reliability Evaluation of Local Area Networks," in *2021 National Computing Colleges Conference (NCCC)*, 2021, pp. 1–6. doi: 10.1109/NCCC49330.2021.9428843.

[7] N. R. Fattahilah, F. Nurfadila, and Y. Setiawan, "High Availability's Implementation on the Fortigate Firewall Using SD-WAN Zone and HA Cluster Active-Passive," *Indones. J. Multidiscip. Sci.*, vol. 2, no. 11, pp. 3937–3952, 2023, doi: 10.55324/ijoms.v2i11.622.

[8] D. Kreculj, Đ. Dihovični, N. Ratković Kovačević, M. Gaborov, and M. Zajeganović, "pfSense Router and Firewall Software," pp. 132–137, 2023, doi: 10.15308/sinteza-2023-132-137.

[9] V. Henriques and M. Tanner, "a S Ystematic L Iterature R Eview of a Gile and," *Interdiscip. J. Information, Knowl. Manag.*, vol. 12,

pp. 53–73, 2017.

[10] R. Nur, Z. Saharuna, I. Irmawati, I. Irawan, and R. Wahyuni, "Gateway Redundancy Using Common Address Redundancy Protocol (CARP)," *IJITEE (International J. Inf. Technol. Electr. Eng.*, vol. 2, no. 3, p. 71, 2019, doi: 10.22146/ijitee.43701.

[11] M. S. F. Ramadhan and Nendi, "Penerapan Redundancy Firewall Pfsense Menggunakan Metode Carp Dengan Pfsync Dan Xmlrpc Sync," *J. Indones. Manaj. Inform. dan Komun.*, vol. 4, no. 3, pp. 1704–1713, 2023, doi: 10.35870/jimik.v4i3.394.

[12] A.-D. Tudosi, A. Graur, D. G. Balan, and A. D. Potorac, "Automatic Directory Service Integration in Distributed Firewall Resources: A Study of Scripting and LDAP Integration with pfSense," in *Advances in Digital Health and Medical Bioengineering*, H.-N. Costin, R. Magjarević, and G. G. Petroiu, Eds., Cham: Springer Nature Switzerland, 2024, pp. 400–411.

[13] M. Caprolu, S. Raponi, and R. Di Pietro, "Fortress: an efficient and distributed firewall for stateful data plane sdn," *Secur. Commun. Networks*, vol. 2019, no. 1, p. 6874592, 2019.

[14] A. T. Azzam, R. Munadi, and R. Mayasari, "Performance analysis of firewall as virtualized network function on VMware ESXi hypervisor," *J. Infotel*, vol. 11, no. 1, pp. 29–35, 2019.

[15] N. R. Fattahilah, F. Nurfadila, and ..., "High Availability's Implementation on the Fortigate Firewall Using SD-WAN Zone and HA Cluster Active-Passive," *Indones. …*, 2023, [Online]. Available: https://ijoms.internationaljournallabs.com/index.php/ijoms/article/view/622

[16] P. Alavian, Y. Eun, K. Liu, S. M. Meerkov, and L. Zhang, "The (α, β)-precise estimates of MTBF and MTTR: Definition, calculation, and observation time," *IEEE Trans. Autom. Sci. Eng.*, vol. 18, no. 3, pp. 1469–1477, 2020.

[17] P. SenthilKumar and M. Muthukumar, "A study on firewall system, scheduling and routing using pfsense scheme," in *2018 International conference on intelligent computing and communication for smart world (I2C2SW)*, IEEE, 2018, pp. 14–17.

[18] K. C. Patel and P. Sharma, "A Review paper on pfsense-an Open source firewall introducing with different capabilities & customization," *IJARIIE*, vol. 3, pp. 2395–4396, 2017.

[19] D. Kumar and M. Gupta, "Implementation of firewall & intrusion detection system using pfSense to enhance network security," *Int. J. Electr. Electron. Comput. Sci. Eng.*, vol. 1, pp. 1222–2454, 2018.

[20] M. S. F. Ramadhan, "PENERAPAN REDUNDANCY FIREWALL PFSENSE MENGGUNAKAN METODE CARP DENGAN PFSYNC DAN XMLRPC SYNC," *J. Indones. Manaj. Inform. dan Komun.*, vol. 4, no. 3, pp. 1704–1713, 2023.

[21] R. Nur, Z. Saharuna, I. Irmawati, I. Irawan, and R. Wahyuni, "Gateway redundancy using common address redundancy protocol (CARP)," *IJITEE (International J. Inf. Technol. Electr. Eng.*, vol. 2, no. 3, pp. 71–77, 2019.