Jurnal Indonesia : Manajemen Informatika dan Komunikasi
www.journal.amikindonesia.ac.id/jimik/ Vol 4 No 3, September (2023)
E-ISSN: 2723-7079, P-ISSN: 2776-8074

PENERAPAN *REDUNDANCY FIREWALL PFSENSE* MENGGUNAKAN METODE *CARP* DENGAN *PFSYNC* DAN *XMLRPC SYNC*

Muhammad Syahrul Fattah Ramadhan [1*], Nendi [2]

[1*,2] Program Studi Teknik Informatika, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Kota Jakarta Timur, Daerah Khusus Ibukota Jakarta, Indonesia

Email: fth.syahrul@gmail.com [1*]

Histori Artikel:
Dikirim 23 Juli 2023; *Diterima dalam bentuk revisi* 19 Agustus 2023; *Diterima* 25 Agustus 2023; *Diterbitkan* 10 September 2023.

Abstrak

Penggunaan teknologi informasi (TI) telah tumbuh pesat di berbagai sektor, seperti bisnis, industri, pendidikan, layanan kesehatan, dan pemerintahan. Dengan semakin tingginya ketergantungan pada TI, penting bagi organisasi untuk memastikan ketersediaan sistem yang tinggi pada firewall menjadi semakin penting. Ketika firewall mengalami masalah atau tidak tersedia, jaringan komputer dapat terkena serangan siber seperti DoS (Denial of Service), Port Scaning dan sebagainya. Sehingga mengakibatkan kerugian finansial, reputasi, dan kepercayaan pelanggan. Di sisi lain, ketersediaan sistem yang tinggi pada firewall dapat membantu organisasi memenuhi persyaratan regulasi, menjaga kepercayaan pelanggan, dan meningkatkan efisiensi operasional. Metode yang digunakan dalam penelitian ini yaitu metode Network Development Life Cycle (NDLC), yang terdiri dari enam tahap, yaitu Analysis, Design, Simulation Prototyping, Implementation, Monitoring, dan Management. Dari hasil pengujian dapat disimpulkan bahwa setelah dilakukan pengujian selama 10 kali dengan metode CARP. Dengan kondisi mengirimkan 30 packet lalu node Master mati, metode ini memiliki rata-rata paket terima sekitar 27.2 packet, lalu downtime disekitar 2.8 detik dan dengan packet loss sekitar 9.2%. Dengan hasil tersebut membuat metode CARP ini memiliki Availability yang tinggi terhadap kegagalan sistem atau jaringan.

Kata Kunci: CARP; Redundancy; PFSENSE.

Abstract

The use of information technology (IT) has grown rapidly in various sectors, such as business, industry, education, healthcare, and government. With the increasing dependence on IT, it is important for organizations to ensure high availability of the firewall system. When the firewall experiences problems or is unavailable, computer networks can be vulnerable to cyber attacks such as DoS (Denial of Service), Port Scanning, and others, resulting in financial loss, reputation damage, and loss of customer trust. On the other hand, high availability of the firewall system can help organizations meet regulatory requirements, maintain customer trust, and improve operational efficiency. The method used in this research is the Network Development Life Cycle (NDLC), which consists of six stages: Analysis, Design, Simulation Prototyping, Implementation, Monitoring, and Management. From the test results, it can be concluded that after testing 10 times with the CARP method, sending 30 packets and then the master node dies, this method has an average of 27.2 packets received, downtime of around 2.8 seconds, and packet loss of around 9.2%. These results make the CARP method have high availability against system or network failures.

Keyword: CARP; Redundancy; PFSENSE.

1. Pendahuluan

Penggunaan teknologi informasi (TI) telah tumbuh pesat di berbagai sektor, seperti bisnis, industri, pendidikan, layanan kesehatan, dan pemerintahan. Dengan semakin tingginya ketergantungan pada TI, penting bagi organisasi untuk memastikan ketersediaan sistem yang tinggi pada *firewall* menjadi semakin penting. Ketika *firewall* mengalami masalah atau tidak tersedia, jaringan komputer dapat terkena serangan siber seperti DoS (*Denial of Service*), *Port Scaning* dan sebagainya [1], [2]. Sehingga mengakibatkan kerugian finansial, reputasi, dan kepercayaan pelanggan. Di sisi lain, ketersediaan sistem yang tinggi pada *firewall* dapat membantu organisasi memenuhi persyaratan regulasi, menjaga kepercayaan pelanggan, dan meningkatkan efisiensi operasional.

Firewall adalah sebuah perangkat keamanan jaringan yang berfungsi untuk melindungi jaringan komputer dari serangan yang tidak diinginkan. *Pfsense* adalah salah satu *firewall open source* yang berbasis *FreeBSD*, yang populer digunakan untuk mengamankan jaringan komputer dengan fitur yang lengkap [3]. Dalam penerapan firewall pada jaringan komputer, ketersediaan dan keandalan sangat penting. Jika *firewal*l mengalami masalah, maka seluruh jaringan akan terkena dampaknya. Oleh karena itu, penerapan redundancy pada *firewall* menjadi sangat penting untuk memastikan ketersediaan dan keandalan jaringan. *Firewall Pfsense* memberikan solusi *redundancy firewall* dengan fitur CARP (*Common Address Redundancy Protocol*), fitur ini digunakan untuk menjadikan dua node *firewall* untuk berperan sebagai master dan slave [4][5]. Mekanisme CARP dilengkapi dengan fitur Pfsync dan XMLRPC sync yang membuat proses *redundancy firewall* lebih seamless, fitur Pfsync ini digunakan sebagai *Synchronize States* untuk mengirimkan pesan update antara node master dan slave melalui *Pfsync Protocol* (IP Protocol 240). Dan dilengkapi dengan fitur XMLRPC sync sebagai *Configuration Synchronization* untuk menyinkronasi setiap konfigurasi terbaru pada node master ke node slave sehingga jika node master down maka konfigurasi terbaru masih berjalan pada node slave [6].

Metode CARP ini dikembangkan oleh *OpenBSD*, dalam proses perkambangannya sebenarnya CARP ini tidak ada paten karena sifatnya *Open Source*. Oleh karena itu CARP tidak mempunyai protocol resmi yang terdaftar pada IEFT (*Internet Engineering Task Force*). Sehingga dalam proses komunikasi CARP ini menggunakan protocol dari VRRP (*Virtual Router Redundancy Protocol*) yang menggunakan IP Protocol 112 [7].

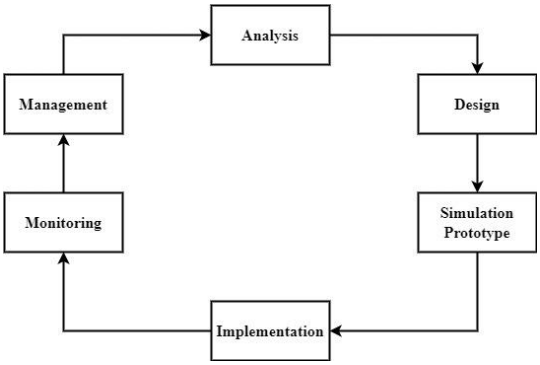
Dalam Penelitian berkaitan dengan Implementasi dan pengujian performa VRRP, lalu jika dibandingkan dengan FHRP, HSRP, GLBP [8]–[19], dapat disimpulkan bahwa metode VRRP memiliki kinerja dan *availability* yang baik ketika terjadinya kegagalan sistem. Oleh sebab itu karena CARP dan VRRP menggunakan IP Protocol 112 yang berarti sama seharusnya CARP memiliki kinerja dan availability yang baik. Dan dalam buku "*Mastering pfSense Second Edition Manage*, *secure*, and *monitor your on-premise and cloud network with pfSense* 2.4" [6], dijelaskan lengkap mengenai *firewall pfsense* dan menjelaskan sistem *redundancy* dengan metode CARP yang dilengkapi fitur pfsync dan XMLRPC Sync, sehingga menambah keunggulan redundancy CARP ini dibandingkan metode VRRP.

Dalam penelitian terkait Implementasi dan pengujian *firewall pfsense* [3][4],[20]–[23], dapat disimpulkan bahwa Implemetasi *firewall pfsense* selain *redundancy*, dapat menjadi sistem IDS (*Intrusion Detection System*) yang digunakan untuk deteksi dan monitoring anomali trafik seperti *DoS*, *Port Scanning*, dan sebagainya. Selain itu pfsense mendukung sistem *Failover* dan *Loadbalance*, Dengan adanya fitur ini dapat meningkatkan *Throughtput* dan kinerja pada jaringan. Metode yang digunakan dalam penelitian ini yaitu metode *Network Development Life Cycle* (NDLC), yang terdiri dari enam tahap, yaitu *Analysis*, *Design*, *Simulation Prototyping*, *Implementation*, *Monitoring*, dan *Management*. Kemudian Penelitian ini dilakukan berbasis simulasi laboratorium, dan bukan studi kasus pada jaringan suatu organisasi atau perusahaan. Penelitian ini bertujuan untuk mengetahui Penerapan *Redundancy Firewall* menggunakan metode CARP dengan Pfsync dan XMLRPC Sync pada platform firewall Pfsense. Simulasi ini akan dilakukan dengan aplikasi simulator PNET-LAB, dan diharapkan hasil penelitian ini dapat memberikan gambaran untuk guna menjadikan sistem jaringan organisasi atau perusahaan yang handal.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1704-1713
DOI : https://doi.org/10.35870/jimik.v4i3.394

2. Metode Penelitian

Metode yang digunakan dalam penelitian ini yaitu metode *Network Development Life Cycle* (NDLC), yang terdiri dari enam tahap, yaitu *Analysis*, *Design*, *Simulation Prototyping*, *Implementation*, *Monitoring*, dan *Management*. Untuk Penjelasan mengenai masing-masing tahapan adalah sebagai berikut:



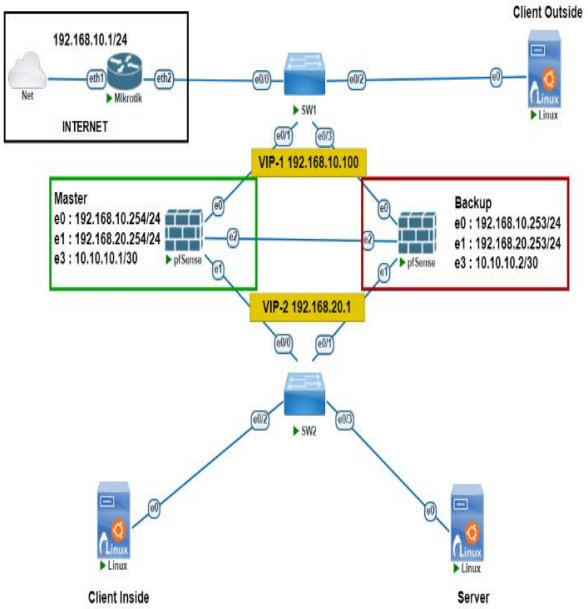
Gambar 1. Metode *NDLC*

1) Analysis

Pada tahap ini, dilakukan identifikasi dan analisa masalah yang ingin diselesaikan, yaitu mengimplementasi *Redundancy Firewall pfsense* menggunakan metode CARP dengan pfsync dan XMLRPC Sync. Dengan menghubungkan 2 *firewall* dengan mode *Master* dan *Backup*. Ketika *firewall Master* mendapat gangguan berupa kerusankan *Hardware* atau pun infrastruktur jaringan nya putus maka system akan berpindah ke *firewall Backup*. Pada tahap ini juga dijelaskan solusi yang dapat diambil dan diimplementasikan untuk menyelesaikan masalah tersebut.

2) Desain

Topologi jaringan yang akan digunakan dalam pengujian jaringan sistem Redundancy Firewall pfsense dengan menggunakan metode CARP dengan pfsync dan XMLRPC Sync terdiri dari 1 node router sebagai Internet Gateway dan difungsikan sebagai Zone Internet. Lalu terdapat 2 node firewall pfsense yang akan dikonfigurasi sebagai firewall Master and Backup. Dan terdapat 2 node switch untuk menghubungkan Zone Internet dan Zone Inside. Untuk pengujian terdapat 3 node client terdiri dari Client Outside, Inside dan Server.



Gambar 2. Topologi Jaringan

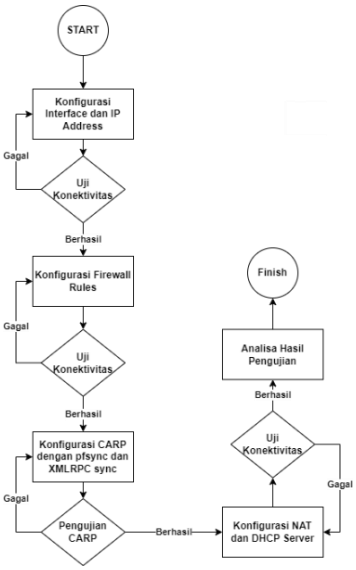
Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1704-1713
DOI : https://doi.org/10.35870/jimik.v4i3.394

Tabel 1. Alokasi IP Address

Nama Perangkat	Interface	IP Address
Router	eth1	192.168.100.245/24
	eth2	192.168.10.1/24
pfsense-Master	e0	192.168.10.254/24
	e1	192.168.20.254/24
	e2	10.10.10.1/30
	VIP-1	192.168.10.100
	VIP-2	192.168.20.1
pfsense-Backup	e0	192.168.10.253/24
	e1	192.168.20.253/24
	e2	10.10.10.2/30
Client Outside	e0	DHCP Client
Client Inside	e0	DHCP Client
Server	e0	DHCP Client

3) Simulation Prototype

Pada tahap simulasi, untuk membangun prototipe sistem *Redundancy Firewall pfsense* dengan menggunakan metode CARP dengan pfsync dan XMLRPC Sync, bisa dilakukan dengan bantuan simulator jaringan seperti PNET Lab. berdasarkan data yang telah dikumpulkan pada tahap-tahap sebelumnya. pada tahap ini dapat menjadi ajuan tindakan yang akan dilakukan pada tahap implementasi.



Gambar 3. Implementasi Rancangan

4) Implementasi

Berdasarkan tahap simulasi *prototype* yang telah dibuat, tahap implementasi untuk merealisasi simulasi yang sudah dilakukan pada tahap sebelumnya. Untuk memastikan bahwa sistem *redundancy* berjalan dengan baik dan sesuai dengan rancangan. Berikut ini skema pengujian yang akan dilakukan:

a) Pengujian fungsi *Redundancy Master-Backup*

Pengujian ini bertujuan untuk memverifikasi fungsi *redundancy firewall Master* dan *Backup* berjalan dengan normal. Dan untuk melihat proses perpindahan antara *firewall Master* ke *Backup* dapat menggunakan *wireshark*.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1704-1713
DOI : https://doi.org/10.35870/jimik.v4i3.394

b) Pengujian Konektivitas *End Device*

Pengujian ini bertujuan untuk memverifikasi konektivitas *end device*, Ketika saat proses *redundancy firewall* berlangsung. Hasil dari pengujian ini dapat mengetahui berapa waktu *downtime* yang terjadi serta mengetahui *persentase packet loss* pada *end device*.

5) *Monitoring*

Monitoring dilakukan setelah implementasi system rancangan selesai. Tahap ini dilakukan untuk menentukan sistem *Redundancy Firewall* pfsense dengan menggunakan metode CARP dengan pfsync dan XMLRPC Sync berfungsi dengan baik dengan kinerja yang optimal sesuai keinginan dan tujuan awal, dan dapat mengidentifikasi mengatasi masalah yang mungkin terjadi.

6) *Management*

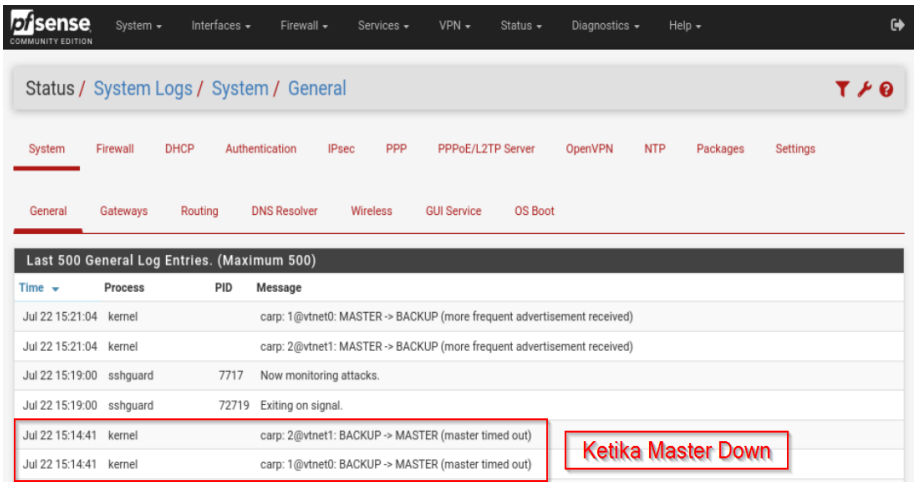
Pada tahap akhir ini, Manajemen merupakan salah satu aspek yang mendapatkan perhatian khusus, terutama dalam pembuatan kebijakan dan pengaturan yang bertujuan untuk memastikan sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung secara berkelanjutan dan mempertahankan unsur keandalannya.

3. Hasil dan Pembahasan

Setelah melakukan tahapan implementasi, selanjutnya akan dilakukan pengujian. Ada dua jenis pengujian dalam Penerapan *Redundancy Firewall pfsense* menggunakan Metode CARP dengan pfsync dan XMLRPC Sync, yaitu Pengujian fungsi *Redundancy Master-Backup* dengan Metode CARP dan Pengujian Konektivitas *End Device*.

1) Pengujian fungsi *Redundancy Master-Backup*

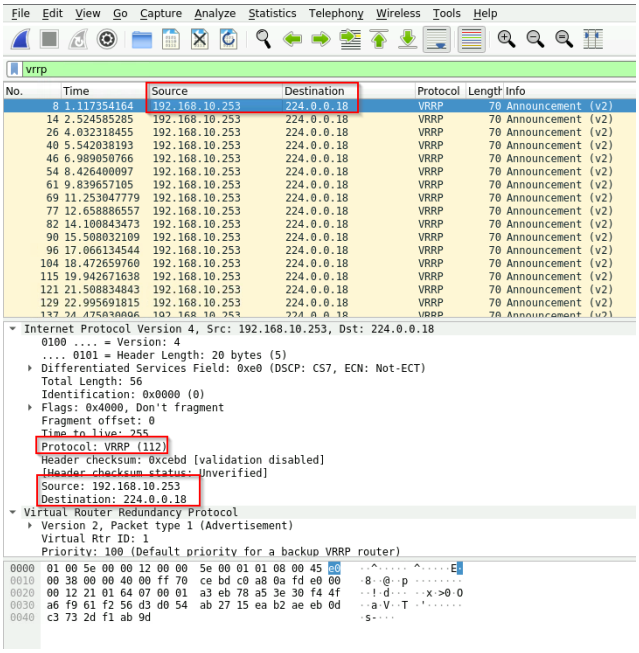
Pengujian ini bertujuan untuk memverifikasi fungsi *redundancy firewall Master* dan *Backup* berjalan dengan normal. Dan untuk melihat proses perpindahan antara *firewall Master* ke *Backup* dapat menggunakan Aplikasi *Wireshark*. Ketika pengujian node Master dibuat down agar sistem *redundancy* dapat berjalan sehingga dapat melihat proses perpindahan sistem jaringannya. Ketika node Master mati, maka sistem node Backup yang akan berjalan. Ini dapat diverifikasi melalui menu "Status" > "*System Logs*".



Gambar 4. Ketika Master Down

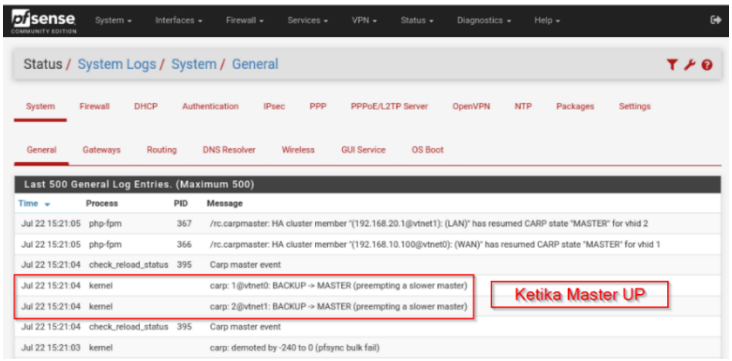
Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1704-1713
DOI : https://doi.org/10.35870/jimik.v4i3.394

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
www.journal.amikindonesia.ac.id/jimik/ Vol 4 No 3, September (2023)
E-ISSN: 2723-7079, P-ISSN: 2776-8074



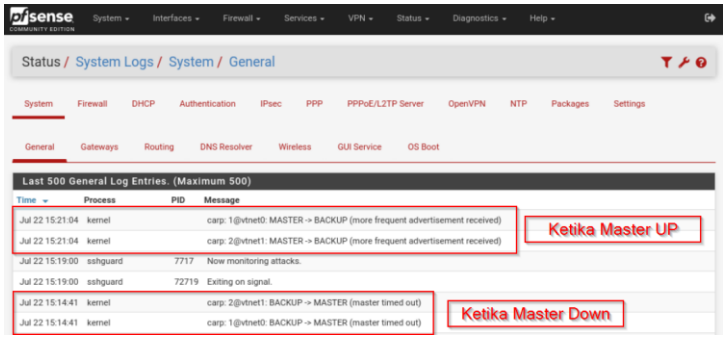
Gambar 5. *Wireshark Trafik* CARP

Dapat diperhatikan dalam gambar 4, didalam log node Backup menampilkan proses Ketika *node Backup* berubah menjadi *node Master* untuk menggantikan *node Master* yang sebelumnya telah mati. Bisa diperhatikan pada gambar 5, pada informasi protocol yang digunakan adalah 112. Dan pada *Source*: 192.168.10.253, Destination: 224.0.0.18, dengan informasi ini membuktikan bahwa sistem yang sedang berjalan saat ini berasal dari node Backup. Karena trafik ini melalui multicast maka dari itu *Destination Address* ke IP multicast. Ketika *node Master* kembali menyala, maka sistem akan merubah *node Backup* yang saat ini berjalan sebagai Master akan dirubah sebagai *Backup* kembali. Kita masuk ke *log pfsense Master*, disini muncul informasi proses perubahan status *Backup* menjadi Master Kembali.

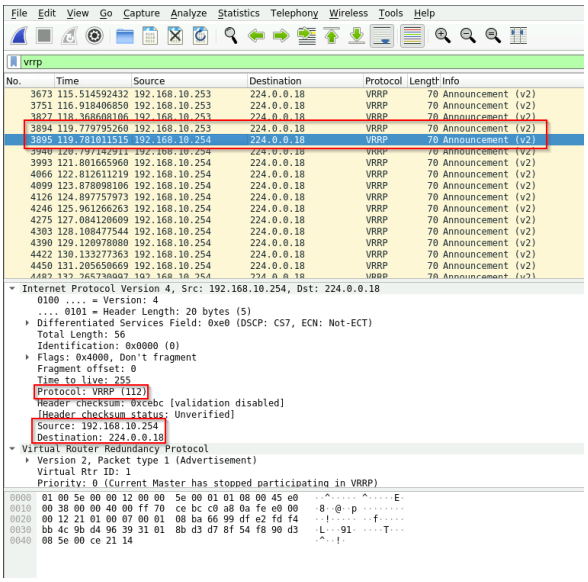


Gambar 6. Ketika *Master UP*

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1704-1713
DOI : https://doi.org/10.35870/jimik.v4i3.394



Gambar 7. *Log node Backup*



Gambar 8. Proses perpindahan system

Pada gambar 8, memuat informasi log pada node Backup Ketika Master menyala dan mati. Didalam log tersebut diperlihatkan ketika Master mati maka *node Backup* menjadi Master, namun ketika *node Master* menyala maka *node Backup* beralih menjadi *Backup* kembali.
Saat proses perpindahan sistem dari node Backup ke Master, bisa diperlihatkan pada gambar 8, hasil dari aplikasi Wireshark bahwa ketika node Backup yang berjalan maka trafik melalui *Source*: 192.168.10.253. Namun Ketika node Master yang kembali mengambil alih sistem maka *source Address* berubah menjadi *Source*: 192.168.10.254.

2) Pengujian Konektivitas *End Device*

Pada tahap pengujian konektivitas ini, dilakukan dengan mematikan node Master, lalu menggunakan perintah ping pada Client Inside dengan mengirim 30 packet yang diulangi selama 10 kali testing. Berikut perintah untuk pengetesan ping :
Terminal : Ping -c 30 google.com

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1704-1713
DOI : https://doi.org/10.35870/jimik.v4i3.394

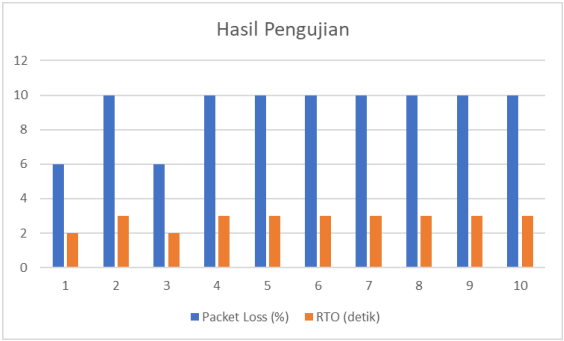
```
eve@Linux-Desktop:~$ ping -c 30 google.com
PING google.com (64.233.170.139) 56(84) bytes of data.
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=1 ttl=54 time=18.6 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=2 ttl=54 time=17.4 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=3 ttl=54 time=17.2 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=4 ttl=54 time=17.7 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=5 ttl=54 time=17.4 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=6 ttl=54 time=17.7 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=9 ttl=54 time=17.8 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=10 ttl=54 time=17.5 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=11 ttl=54 time=17.4 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=12 ttl=54 time=17.5 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=13 ttl=54 time=17.8 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=14 ttl=54 time=17.7 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=15 ttl=54 time=19.3 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=16 ttl=54 time=17.3 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=17 ttl=54 time=18.0 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=18 ttl=54 time=17.0 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=19 ttl=54 time=17.7 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=20 ttl=54 time=17.7 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=21 ttl=54 time=17.4 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=22 ttl=54 time=17.3 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=23 ttl=54 time=16.9 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=24 ttl=54 time=17.5 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=25 ttl=54 time=17.1 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=26 ttl=54 time=16.9 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=27 ttl=54 time=17.3 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=28 ttl=54 time=16.9 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=29 ttl=54 time=17.5 ms
64 bytes from sg-in-f139.1e100.net (64.233.170.139): icmp_seq=30 ttl=54 time=17.6 ms

--- google.com ping statistics ---
30 packets transmitted, 28 received, 6% packet loss, time 29099ms
rtt min/avg/max/mdev = 16.946/17.592/19.377/0.506 ms
eve@Linux-Desktop:~$
```

Gambar 9. Testing Ping

Tabel 2. Hasil Pengujian

Batch Testing	Packets Sent	Packets Received	Packet Loss (%)	RTO (detik)
1	30	28	6	2
2	30	27	10	3
3	30	28	6	2
4	30	27	10	3
5	30	27	10	3
6	30	27	10	3
7	30	27	10	3
8	30	27	10	3
9	30	27	10	3
10	30	27	10	3
Average		27.2	9.2	2.8



Gambar 10. Statistik Pengujian

Dari hasil pengujian diatas, dapat disimpulkan bahwa setelah dilakukan pengujian selama 10 kali dengan metode CARP. Dengan kondisi mengirimkan 30 packet lalu *node Master* mati, metode ini memiliki rata-rata paket terima sekitar 27.2 packet, lalu downtime disekitar 2.8 detik dan dengan packet loss sekitar 9.2%. Dengan hasil tersebut membuat metode CARP ini memiliki Availability yang tinggi terhadap kegagalan jaringan.

4. Kesimpulan

Berdasarkan hasil penelitian dan analisis data yang telah dilakukan, dapat disimpulkan bahwa *Sistem Rendundancy Firewall Pfsense* menggunakan metode CARP dengan pfsync dan XMLRPC Sync ini

Jurnal Indonesia : Manajemen Informatika dan Komunikasi, Volume 4 No 3, September (2023), pp. 1704-1713
DOI : https://doi.org/10.35870/jimik.v4i3.394

memiliki kinerja dan *Availability* yang bagus. Pertama, didalam fitur CARP ini memiliki fitur pfsync dan XMLRPC Sync yang tidak ada pada sistem redundancy yang sejenis seperti VRRP dan HSRP. fitur ini dapat membuat dua sistem *firewall* dapat saling *backup* dengan *seamless* tanpa adanya miss konfigurasi. Terlebih lagi pfsense ini adalah *opensource firewall* yang dapat digunakan oleh organisasi atau instansi apapun secara gratis, dan kita bisa memakai semua fitur didalamnya. Kedua, perlu diingat bahwa Metode ini dikembangkan oleh *OpenBSD*, dalam proses perkambangannya sebenarnya CARP ini tidak ada paten karena sifatnya *Open Source*. Oleh karena itu CARP tidak mempunyai protocol resmi yang terdaftar pada IEFT (*Internet Engineering Task Force*). Sehingga dalam proses komunikasi CARP ini menggunakan protocol dari VRRP yang menggunakan IP Protocol 112. Ketiga, dari hasil penelitian ini dapat menyimpulkan bahwa metode CARP ini memiliki kinerja dan *Availability* yang bagus. Selama 10 kali pengujian, dengan mengirimkan 30 packet secara berulang, hasilnya 27.2 packet diterima, lalu dengan *downtime* sekitar 2.8 detik dan dengan packetloss sekitar 9.2%. Hasil pengujian ini cukup untuk menunjukan kehandalan metode CARP ini.

5. Daftar Pustaka

[1] Sholihan, A. W. N., Mukti, A. R., Suryayusra, S., & Dasmen, R. N. Implementation of Network Security and Anticipating Attackers Using pfSense Firewall. *CESS (Journal of Computer Engineering, System and Science)*, *8*(1), 175-183.

[2] Arman, M., & Rachmat, N. (2020). Implementasi sistem keamanan web server menggunakan pfsense. *Jusikom: Jurnal Sistem Komputer Musirawas*, *5*(1), 13-23.

[3] Azzam, A. T., Munadi, R., & Mayasari, R. (2019). Analisis Throughput dan High Availability Firewall sebagai Virtualized Network Function pada VMware ESXI. *Prosiding SENIATI*, *5*(2), 149-154.

[4] Attebury, G., & Ramamurthy, B. (2006, June). Router and firewall redundancy with OpenBSD and CARP. In *2006 IEEE International Conference on Communications* (Vol. 1, pp. 146-151). IEEE. DOI: 10.1109/ICC.2006.254719.

[5] Nur, R., Saharuna, Z., Irmawati, I., Irawan, I., & Wahyuni, R. (2019). Gateway redundancy using common address redundancy protocol (CARP). *IJITEE (International Journal of Information Technology and Electrical Engineering)*, *2*(3), 71-77. DOI: https://doi.org/10.22146/ijitee.43701.

[6] Zientara, D. (2018). *Mastering pfSense: Manage, secure, and monitor your on-premise and cloud network with pfSense 2.4*. Packt Publishing Ltd.

[7] PM, C., Megha, K. R., Sushmitha, M., & Baliga, S. Comparative Analysis of HSPR, VRRP and GLPB Network Redundancy Protocols.

[8] Machdi, A. R. (2019). ANALYZING MIKROTIK BASED VRRP (VIRTUAL ROUTER REDUNDANCY PROTOCOL) IMPLEMENTATION ON HOMEGRID NETWORKS. *Journal of Science Innovare*, *2*(01), 13-18. DOI: 10.33751/jsi.v2i01.1524.

[9] Julia, I. R., Suseno, H. B., Wardhani, L. K., Khairani, D., Hulliyah, K., & Muharram, A. T. (2020, October). Performance evaluation of first hop redundancy protocol (FHRP) on VRRP, HSRP, GLBP with routing protocol BGP and EIGRP. In *2020 8th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-5). IEEE. DOI: 10.1109/CITSM50537.2020.9268799.

[10] Suprijatmono, D., & Siswadi, A. (2019). Implementasi First Hop Redundancy Protocol (FHRP) Pada Jaringan Data Untuk Meningkatkan Availibility Pada Pelanggan. *SAINSTECH: JURNAL PENELITIAN DAN PENGKAJIAN SAINS DAN TEKNOLOGI*, *29*(2). DOI: https://doi.org/10.37277/stch.v29i2.339.

[11] Pamungkas, W. H. (2018). Perancangan Jaringan Redundancy Link Menggunakan Konsep HSRP dan Etherchannel (Studi Kasus PT. Telkom Area Palangkaraya). *Metik Jurnal*, *2*(1), 75-83.

[12] Akmaludin, A. (2019). *Evaluasi kinerja hot standby router protocol (Hsrp) dan gateway load b alancing protocol (Glbp) untuk layanan video streaming* (Bachelor's thesis, Fakultas Sains dan Teknologi Universitas Islam Negeri Syarif Hidayatullah Jakarta).

[13] Sastra, R. (2019). Analisa Kinerja Kualitas Layanan (QoS) Virtual Router Redudancyp Protocol (VRRP) Menggunakan Mikrotik Routerboard. *Jurnal Teknik Informatika*, *5*(1), 1-5. DOI: https://doi.org/10.51998/jti.v5i1.301.

[14] Rodiah, R. (2020). IMPLEMENTASI HIGH AVAILABILITY UNTUK PENGURANGAN WAKTU DOWNTIME PADA JARINGAN DENGAN PROTOKOL HIGH AVAILABILITY FIRST HOP REDUDANCY PROTOCOL (FHRP). *Jurnal Ilmiah Informatika Komputer*, *25*(2), 147-159. DOI: http://dx.doi.org/10.35760/ik.2020.v25i2.2982.

[15] Kuswanto, H., & Rahman, T. (2019). Failover Gateway Menggunakan Protokol Virtual Router Redundancy Protocol (VRRP) pada Mikrotik Router. *JUSTIN (Jurnal Sistem dan Teknologi Informasi)*, *7*(1), 60-66.

[16] Santoso, A., Wahyuddin, M. I., & Aningsih, A. (2020). Backcup Router Network Optimization to Prevent Link Failure Using the Virtual Router Redundancy Protocol (VRRP) Method: Backcup Router Network Optimization to Prevent Link Failure Using the Virtual Router Redundancy Protocol (VRRP) Method. *Jurnal Mantik*, *4*(1), 276-282.

[17] Raharjo, M., Pernando, F., & Fauzi, A. (2019). Perancangan Performansi Quality Of Service Dengan Metode Virtual Routing Redudancy Protocol (VRRP). *Jurnal Teknik Komputer AMIK BSI*, *5*(1), 87-92.

[18] Danhieux, P. (2004). CARP-the free fail-over protocol. *GSEC, Practical v1. 4b, SANS Institute*, 1-16.

[19] Fauzi, R., & Yuliadi, Y. (2019, November). Penerapan Load Balancing pada Router pfSense berbasis FreeBSD. In *Prosiding Seminar Nasional Ilmu Sosial dan Teknologi (SNISTEK)* (No. 2, pp. 169-174).

[20] "Dwiyatno, S., Andriani, W. A., & Sari, A. P. (2020, March). Implemetation of Snort IPS Using PfSense as Network Forensic in Smk XYZ. In *1st International Multidisciplinary Conference on Education, Technology, and Engineering (IMCETE 2019)* (pp. 186-192). Atlantis Press.