Jurnal SimanteC
Vol.xx, No.xx Juni 2022
P-ISSN : 2088-2130
E-ISSN : 2502-4884

ANALISIS PERFORMA VIRTUAL SOPHOS FIREWALL PADA IMPLEMENTASI NETWORK FUNCTION VIRTUALIZATION (NFV) MENGGUNAKAN HYPERVISOR VMWARE ESXI

ANALYSIS OF VIRTUAL SOPHOS FIREWALL PERFORMANCE IN NETWORK FUNCTION VIRTUALIZATION (NFV) IMPLEMENTATION USING VMWARE ESXI HYPERVISOR

Rizvan Dimas Saputra Ariyanto[1)], Agung Kridoyono[)]
[1,2]Prodi Informatika, Fakultas Teknik, Universitas 17 Agustus 1945 Surabaya
Jl. Semolowaru No.45 Surabaya
E-mail : [1*]rizvanariyanto@gmail.com, [2]akridoyono@gmail.com

ABSTRAK

Semakin maraknya kebutuhan masyarakat akan akses internet, menjadikan sebuah teknologi harus dapat berkembang pesat untuk memenuhi kebutuhan tersebut. Dibutuhkan kecanggihan dari suatu hardware dan proses yang berjalan didalam hardware tersebut guna mengelola dan memenuhi setiap permintaan yang dilakukan oleh pengguna ketika mengakses jaringan internet. Untuk itu dibutuhkan sebuah mesin virtual yang dapat meringkas pengadaan hardware pada suatu topology jaringan kedalam bentuk virtual device. Teknologi yang dapat digunakan ialah NFV (Network Function Virtualization). Hal tersebut sangat berbeda dengan penerapan traditional network function, dimana penerapan topologi jaringan sangat membutuhkan network hardware device dan cost operasional maupun pengadaan perangkat yang cukup tinggi. Serta konfigurasi dan integrasi network hardware device masih bersifat manual pada tiap perangkat dan kurang efektif. Untuk itu, sebelum menjalankan teknologi NFV dibutuhkan sebuah virtual machine atau hypervisor yang akan menjalankan fungsi virtualisasi. Untuk dapat mengetahui kelayakan fungsi dari teknologi NFV dibutuhkan sebuah pengujian yang mengacu pada QoS (Quality of Service) seperti pada parameter Throughput & Delay beserta analisa performa terhadap tingkat keamanan network server dalam menerapkan teknologi NFV.

Kata kunci : *hardware, NFV, QoS (Quality of Service), virtual, virtual machine.*

ABSTRACT

The increasingly widespread public need for internet access, making a technology must be able to develop rapidly to meet these needs. It takes the sophistication of a hardware and processes that run on the hardware to manage and fulfill every request made by the user when accessing the internet network. For that we need a virtual machine that can summarize the procurement of hardware in a network topology into the form of virtual devices. The technology that can be used is NFV (Network Function Virtualization). This is very different from the application of traditional network functions, where the application of network topology really requires network hardware devices and the operational costs as well as equipment procurement are quite high. And the configuration and integration of network hardware devices is still manual on each device and is less effective. For this reason, before running NFV technology, a virtual machine or hypervisor is needed that will perform the virtualization function. To be able to determine the feasibility of the function of NFV technology, a test that refers to QoS (Quality of Service) such as the Throughput & Delay parameters is needed along with a performance analysis of the security level of the network server in implementing NFV technology.

Keywords: *hardware, NFV, QoS (Quality of Service), virtual, virtual machine.*

PENDAHULUAN

Penyusunan sebuah topologi jaringan membutuhkan komposisi yang terdiri dari hardware dan software pembentuknya. Pengguna harus melakukan survei mendalam terhadap kebutuhan perangkat dan operasional yang akan dikeluarkannya ketika merancang sebuah topologi jaringan. Beberapa permasalahan pengguna ketika merancang sebuah topologi jaringan diantaranya adalah kebutuhan network hardware device yang terbilang cukup tinggi dalam perluasan jaringan, cost operasional dan pengadaan perangkat yang cukup tinggi, integrasi dan konfigurasi perangkat kurang efektif, migrasi perangkat dan konfigurasi cukup sulit dan dilakukan secara manual tiap network device, proses backup & restore konfigurasi perangkat dilakukan secara manual pada masing-masing perangkat, serta komponen network device rentan terserang malware karena manage device tidak terpusat. Sehingga dari permasalahan ini kami sebagai peneliti menerapkan teknologi virtualisasi atau disebut dengan *NFV (Network Function Virtualization)* [1]. Tujuan penerapan NFV adalah untuk meminimalisir penggunaan resource hardware yang akan digunakan dalam pembangunan suatu topologi jaringan. Hal tersebut dikarenakan NFV akan menjadikan kebutuhan network hardware device berubah menjadi bentuk virtual dengan fungsi yang masih sama seperti perangkat aslinya, lebih hemat dari segi cost operasional, maintenance maupun pengadaan perangkat, proses integrasi tiap perangkat akan menjadi terpusat pada suatu Hypervisor, serta backup & restore ketika migrasi perangkat cukup pada Hypervisor [2].

Hypervisor merupakan sebuah perangkat lunak yang berfungsi untuk menjembatani antara komunikasi hardware dengan komunikasi *virtual machine* [3]. Fungsi yang berjalan pada suatu Hypervisor yakni mengatur resource hardware pada suatu proses virtual machine yang berkaitan dengan CPU, RAM & storage. Pada penelitian ini kami menggunakan Hypervisor VMware ESXi untuk menjalankan fungsi yang ada pada teknologi NFV. VMware ESXi adalah sistem operasi berbasis Virtualization Technology yang diinstal pada sisi server dan digunakan untuk membentuk sebuah virtual machine yang berisi konfigurasi terkait dengan file, disk untuk membentuk seakan menjadi konfigurasi fisik sebuah hardware [4]. Virtual machine yang akan di install pada VMware ESXi adalah virtual Ubuntu server dan virtual Sophos firewall.

Dalam penelitian ini kami sebagai peneliti akan menguji dan implementasi terkait dengan performa dari virtual firewall. Sehingga pada hasil akhir penelitian dapat diketahui fungsional dan kualitas dari virtual firewall dengan membandingkan dengan hardware firewall. Hal tersebut dikarenakan dalam penerapan teknologi NFV, dibutuhkan sebuah tingkat keamanan yang tinggi untuk melindungi node jaringan agar suatu ancaman tidak dapat masuk dan menyerang sumber daya jaringan. Adanya teknologi NFV memungkinkan sebuah ancaman masuk kedalam jaringan telekomunikasi untuk menyerang sumber daya jaringan yang ada [5]. Maka dari itu dibutuhkan sebuah fungsi firewall yang nanti akan melakukan filtering keluar masuknya packet data pada topologi jaringan [6]. Firewall yang akan dilakukan pengujian performa dalam penelitian ini ialah virtual Sophos firewall, Sophos berfungsi untuk melindungi jaringan komputer dengan menerapkan filter rules dan action rules ketika suatu paket data keluar dan masuk jaringan client-server [7].

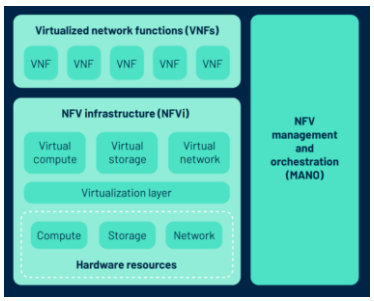
Dalam jaringan client-server diperlukan suatu server yang mampu memenuhi kebutuhan atau permintaan dari client. Untuk itu pada sisi VMware ESXi dilakukan instalasi virtual Ubuntu server, dimana nantinya akan melakukan pemenuhan kepada client terhadap permintaan layanan FTP *(File Transfer Protocol)* & remote SSH. Proses komunikasi antara client dan server dapat dilakukan dengan cara pengiriman dan

penerimaan file data dengan menjalankan protocol FTP. Sehingga proses remote transfer file data tidak dilakukan secara manual menggunakan *flashdisk* atau *hardisk* [8]. Ketika client mengirimkan permintaan kepada server untuk mengakses suatu file data, client harus melewati filtering rules terlebih dahulu yang terdapat pada firewall. Filtering yang dilakukan oleh firewall sesuai dengan filter rules yang sudah dibuat. Paket data yang bersifat baik dan sesuai dengan filter rules akan diperbolehkan untuk melewati jaringan. Namun paket data yang dianggap kurang baik akan dilakukan sebuah action *drop* sesuai dengan pengaturan pada filter rules [9].

Pengujian fungsional dan performa firewall sangat dibutuhkan dalam penerapan NFV, dikarenakan dengan pemilihan firewall yang baik maka akan menjadikan penerapan NFV lebih maksimal dan *secure*. Dalam penelitian ini, kami sebagai peneliti membandingkan 2 performa dan fungsional dari firewall berbasis virtual dan firewall berbasis hardware. Untuk virtual firewall yang akan diterapkan dalam pengujian adalah Sophos firewall, dan untuk hardware firewall menggunakan MikroTik firewall. Dalam melakukan pengujian terhadap performa firewall kami mengacu pada standarisasi TIPHON, yakni dengan melakukan pengujian terhadap performa *Quality of Service (QoS)* pada parameter *Throughput & Delay*. QoS merupakan parameter pengukuran untuk menentukan kualitas baik buruknya suatu topologi jaringan [10]. TIPHON (Telecommunications and Internet Protocol Harmonization Over Network) merupakan standar penilaian terhadap pengujian parameter QoS yang dikeluarkan oleh badan standarisasi ETSI (European Telecommunications Standards Institue) [11]. *Througphput* adalah salah satu parameter dalam Quality of Service (QoS) yang berfokus pada pengukuran durasi waktu yang dibutuhkan ketika suatu data dikirimkan melalui transmitter hingga suatu data dapat diterima oleh penerima (receiver) [12]. Sedangkan *Delay* merupakan besaran waktu yang dibutuhkan ketika proses pengiriman paket data dari suatu pengirim data (transmitter) menuju ke penerima data (receiver) [13]. Skema pengujian yang dilakukan adalah dengan melakukan pengiriman FTP antara client-server lalu disertai dengan burst packet berupa traffic size menggunakan tools *traffic generator* yakni D-ITG. D-ITG merupakan sebuah aplikasi client-server berbasis Command Line Interface (CLI) yang berguna untuk melakukan burst bandwidth terhadap proses pengiriman paket dan mengukur parameter QoS pada topologi jaringan yang sudah dirancang [14]. Traffic size yang akan dilewatkan pada D-ITG antara lain : 2 Mbps, 3 Mbps dan 4 Mbps. Percobaan pengujian yang dilakukan sebanyak 30 kali pada masing-masing firewall dengan disertai ketiga traffic size 2 Mbps, 3 Mbps dan 4 Mbps. Tujuannya yakni untuk memperoleh hasil yang valid dan tidak ambiguitas pada proses pengujian performa QoS firewall. Selain melakukan pengujian terhadap performa QoS firewall, peneliti juga melakukan pengujian terhadap fungsional virtual firewall dengan fungsi pembandingnya adalah MikroTik hardware firewall. Proses pengujian yang dilakukan adalah dengan menerapkan filtering rules dan action rules pada masing-masing fitur virtual Sophos firewall dan juga MikroTik firewall. Dengan menerapkan virtual Sophos firewall pada jaringan teknologi NFV, diharapkan dapat melakukan seleksi terhadap keluar masuknya packet data ketika komunikasi client-server. Serta dapat mengurangi resiko terjadinya ancaman keamanan lalu lintas data yang berasal dari client yang tidak dikenali oleh server [15].

METODE

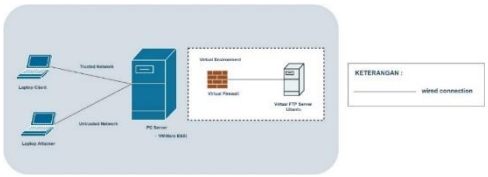
Metode yang digunakan dalam penelitian ini adalah metode virtualisasi dengan menggunakan literatur penelitian sebelumnya sebagai bahan perbandingan dan referensi. Metode virtualisasi yang diterapkan pada penelitian ini mengacu pada konsep NFV (Network Function Virtualization).



Gambar 1. Arsitektur NFV

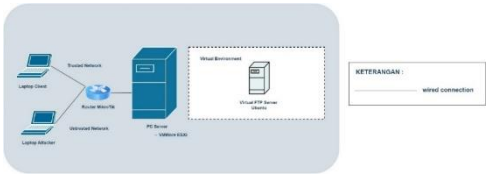
Dimana dalam pembentukannya NFV terdiri dari 3 kerangka komponen utama, yakni VNF (Virtualized Network Functions), NFVI (Network Functions Virtualization Infrastructure) & NFV-MANO (Network Functions Virtualization Management and Orchestration). VNF merupakan penerapan software base pada suatu fungsi jaringan dalam NFVI. Sedangkan NFVI merupakan seluruh komponen hardware dan software yang membentuk infrastruktur VNF. Terdapat 3 komponen penyusun NFVI, yakni hardware resources, virtualization layer dan virtualized resources. NFV-MANO merupakan sekumpulan blok fungsional dan repositori data yang digunakan untuk mengatur dan mengelola NFVI dan VNF.

Tahapan yang pertama dilakukan adalah dengan melakukan instalasi terhadap kebutuhan NFVI (Network Functions Virtualization Infrastructure) yang akan digunakan dalam penelitian, antara lain VMware ESXi (virtual machine), virtual Ubuntu Server 22.04, virtual Sophos firewall 18.5.1, laptop client, dan laptop attacker.



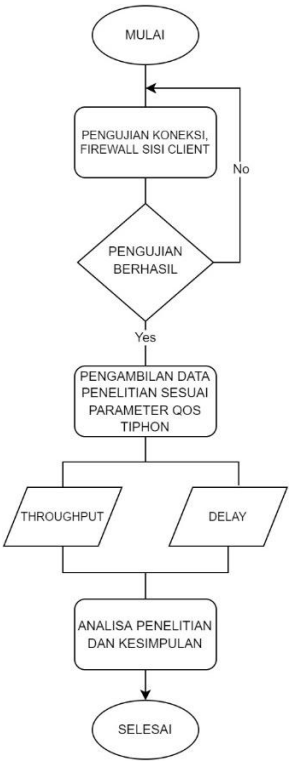
Gambar 2. Topologi Jaringan NFV *(Virtual Base)*

Gambar 2 merupakan bentuk topologi jaringan yang di implementasikan dalam penelitian ini. Terdapat 2 komponen VNF dalam penyusunnya, yakni virtual Sophos firewall dan virtual Ubuntu server. Dimana setelah melakukan instalasi sesuai dengan topologi tersebut, peneliti melanjutkan tahap konfigurasi masing-masing network function device, serta dilanjutkan dengan pengujian pada topologi jaringan NFV. Pengujian yang dilakukan adalah dengan mengacu pada parameter *QoS (Quality of Service)* dalam topologi jaringan NFV berdasarkan standar TIPHON dan parameter fungsional dari virtual Sophos firewall.



Gambar 3. Topologi Jaringan Conventional *(Hardware Base)*

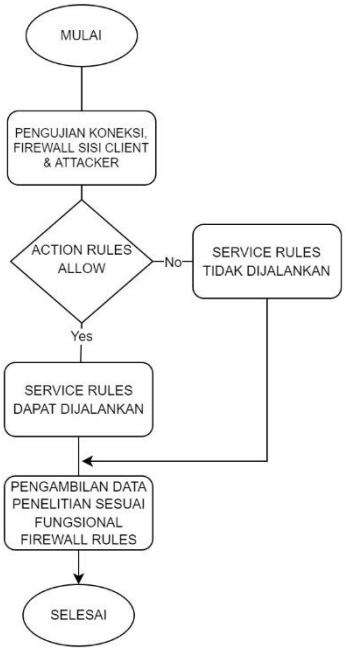
Gambar 3 merupakan bentuk topologi jaringan yang akan digunakan sebagai pembanding dengan topologi jaringan NFV pada penelitian ini. Tahapan yang dilakukan dalam topologi tersebut sama dengan topologi NFV, yakni melakukan instalasi network hardware device seperti MikroTik firewall dan laptop client-attacker, konfigurasi network device, dan pengujian topologi jaringannya.



Gambar 4. Flowchart Simulasi Pengujian *QoS (Quality of Service)*

Proses pengujian yang dilakukan terbagi menjadi 2 jenis. Pada gambar 4 merupakan tahapan yang dilakukan peneliti dalam melakukan pengujian

terhadap parameter *QoS (Quality of Service)* berdasarkan standarisasi TIPHON. Terdapat 2 *point* parameter yang akan diambil dalam pengujian ini, yakni *Throughput* dan *Delay*. Pengukuran dan pengambilan data parameter *QoS* dilakukan sebanyak 30 kali percobaan menggunakan network tools traffic generator yakni D-ITG. Pada D-ITG peneliti menambahkan aliran traffic size sebesar 2 Mbps, 3 Mbps dan 4 Mbps pada masing-masing percobaan.

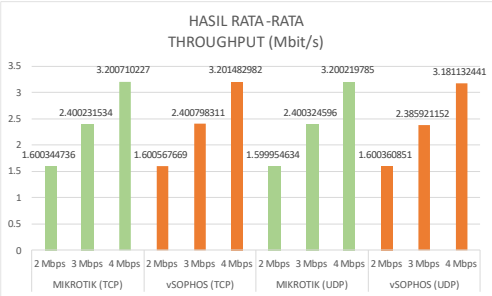


Gambar 5. Flowchart Simulasi Pengujian Fungsional Firewall

Gambar 5 merupakan tahapan simulasi pengujian terkait dengan fungsional dari virtual firewall device atau dalam hal ini virtual Sophos firewall. Dimana proses pengujiannya akan dilakukan dengan menambahkan *filter rules* dan *action rules* ketika client dan attacker melakukan komunikasi client-server dengan virtual server Ubuntu melewati firewall tersebut. Sehingga dalam proses pengujian ini peneliti akan mendapatkan hasil berkaitan dengan perbandingan fungsional antara virtual firewall dengan hardware firewall.

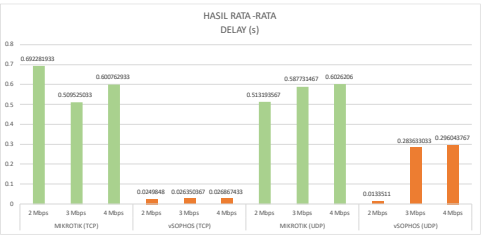
HASIL DAN PEMBAHASAN

Hasil dan pembahasan yang sudah dilakukan peneliti adalah pengambilan data pengujian *QoS* pada topologi jaringan NFV & topologi jaringan conventional berdasarkan protocol TCP UDP berdasarkan parameter *Throughput & Delay*, Fungsional virtual Sophos firewall dalam melakukan *blocking & accepting* packet data.



Gambar 6. Hasil Rata-rata Throughput

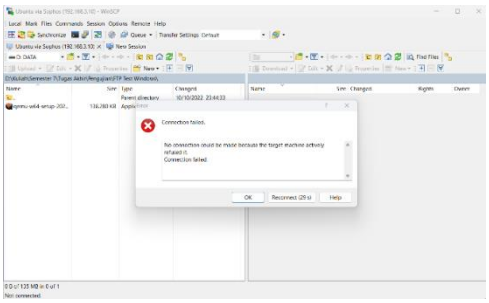
Pada gambar 6 merupakan hasil dari pengambilan data pengujian performa pada masing-masing topologi jaringan parameter Throughput, perbandingan antara MikroTik & vSophos firewall yang menerapkan protocol TCP dapat diketahui hasil rata-rata yang didapatkan dalam pengujian menunjukan bahwa Throughput pada vSophos firewall lebih tinggi dibandingkan dengan MikroTik firewall. Dengan perbedaan yang sangat kecil pada masing-masing pengujian traffic size nya. Sedangkan pada protocol UDP dapat diketahui hasil rata-rata yang didapatkan dalam pengujian menunjukan bahwa pada traffic size 2 Mbps vSophos firewall memiliki nilai Throughput yang lebih besar daripada MikroTik firewall. Namun pada traffic size 3 Mbps dan 4 Mbps MikroTik firewall memiliki nilai Throughput yang lebih besar daripada vSophos firewall.



Gambar 7. Hasil Rata-rata Delay

Pada gambar 7 perbandingan antara MikroTik & vSophos firewall yang

menerapkan protocol TCP & UDP dapat diketahui hasil rata-rata yang didapatkan dalam pengujian menunjukan bahwa nilai delay pada penerapan topologi *hardware base* yang menggunakan MikroTik firewall lebih tinggi daripada nilai delay pada penerapan topologi NFV vSophos firewall. Hal tersebut membuktikan bahwa penerapan topologi virtual memiliki nilai dan hasil delay yang lebih baik.



Gambar 8. Penerapan Blocking FTP Pada Client Tertentu Melalui Virtual Sophos Firewall

Pada gambar 8 pengujian terhadap fungsional virtual Sophos firewall berjalan dengan baik, hal tersebut dibuktikan dengan penambahan *filtering rules* dan *action rules* pada sisi virtual Sophos firewall yang menjadikan client tidak dapat menjalankan layanan *FTP (File Transfer Protocol)*.

SIMPULAN

Penerapan teknologi NFV dalam perancangan suatu topologi jaringan dapat menekan biaya operasional, maintenance & integrasi terhadap perangkat network hardware. Integrasi suatu komponen penyusun topologi jaringan dapat dilakukan dengan mudah pada teknologi NFV dikarenakan proses integrasinya dilakukan secara terpusat pada Hypervisor. Hasil pengujian *QoS (Quality of Service)* parameter *Throughput* yang didapatkan dari pengujian kedua firewall virtual Sophos dengan MikroTik menunjukkan hasil yang tidak jauh berbeda dan signifikan. Sedangkan, Hasil parameter *Delay* yang didapatkan dari pengujian kedua firewall virtual Sophos dengan MikroTik menunjukkan hasil pada Virtual Sophos Firewall lebih baik dibandingkan dengan MikroTik firewall baik dalam penerapan protocol TCP maupun UDP. Hal tersebut membuktikan bahwa penerapan topologi virtual (NFV) memiliki nilai dan hasil *Delay* yang lebih baik. Demikian juga dengan fungsional pada virtual Sophos firewall yang menunjukkan penerapan *filtering rules* dan *action rules* untuk *blocking* suatu client dapat berjalan dengan baik.

SARAN

Berdasarkan hasil penelitian yang sudah dicapai, maka terdapat beberapa saran perbaikan dalam penelitian selanjutnya guna melengkapi kekurangan yang ada pada penelitian saat ini dengan penggunaan virtual machine atau Hypervisor yang berbeda guna mendapatkan hasil pembanding ketika implementasi menggunakan Hypervisor selain VMware ESXi. Diperlukan juga penggunaan komponen network virtual device yang berbeda guna meningkatkan variasi dalam penerapan teknologi Network Function Virtualization (NFV). Selain itu, dibutuhkan penggunaan tools pengujian (traffic generator) yang berbeda guna membandingkan dengan hasil dari penelitian saat ini.

DAFTAR PUSTAKA

[1] D. Wiryatari, S. Raharjo, and E. Pramono, “Analisis Performansi Quality of service (QoS) Network Function Virtualization dengan Docker Container,” *J. FATEKSA J. ...*, pp. 10–16, 2021, [Online]. Available: https://uswim.e-journal.id/fateksa/article/view/236%0Ahttps://uswim.e-journal.id/fateksa/article/download/236/175

[2] R. F. Aswariza, D. Perdana, and R. M. Negara, “Analisis Throughput Dan Skalabilitas Virtualized Network Function VyOS Pada Hypervisor VMWare ESXi, XEN, DAN KVM,” *J. Infotel*, vol. 9, no. 1, p. 70, 2017, doi: 10.20895/infotel.v9i1.173.

[3] T. W. Caturiyanto, A. Setyanto, and E. Pramono, "Analisa Dan Perbandingan Performa Hypervisor ESXi, XEN, VMWARE Workstation Pro, Dan Virtualbox," *J. Inf. J. Penelit. dan Pengabdi. Masy.*, vol. 6, no. 2, pp. 40–44, 2020, doi: 10.46808/informa.v6i2.182.

[4] B. S. Panca, "Performance Analysis of NFS Protocol Usage on VMware ESXi Datastore," *J. Tek. Inform. dan Sist. Inf.*, vol. 3, no. 1, pp. 137–149, 2017, doi: 10.28932/jutisi.v3i1.584.

[5] A. T. Azzam, R. Munadi, and R. Mayasari, "Analisis Throughput dan High Availability Firewall sebagai Virtualized Network Function pada VMware ESXI," pp. 149–154, 2019.

[6] Y. Yanti and R. Effendi, "Analisa Sistem Keamanan Jaringan Komputer Firewall Menggunakan Shorewall Pada PT. Indofarma Global Medika," *J. TEKSAGRO*, vol. 1, no. 2, pp. 14–21, 2020.

[7] S. Sas, A. Simorangkir, and T. W. Harjanti, "Implementasi keamanan jaringan menggunakan perangkat lunak sophos xg firewall," vol. 7, no. 2, 2021.

[8] F. Nurrahman, "Implementasi Linux Ubuntu Server 18.04 Sebagai Server Sistem Informasi Akademik Pada Sekolah Tinggi Manajemen Informatika Dan Komputer Samarinda," *J. DiJITAC*, vol. 1, no. 1, pp. 55–77, 2020.

[9] F. Adhi Purwaningrum, A. Purwanto, E. Agus Darmadi, P. Tri Mitra Karya Mandiri Blok Semper Jomin Baru, and C. -Karawang, "Optimalisasi Jaringan Menggunakan Firewall," vol. 2, no. 3, pp. 17–23, 2018.

[10] H. Fahmi, "Analisis Qos (Quality of Service) Pengukuran Delay, Jitter, Packet Lost Dan Throughput Untuk Mendapatkan Kualitas Kerja Radio Streaming Yang Baik," *J. Teknol. Inf. dan Komun.*, vol. 7, no. 2, pp. 98–105, 2018.

[11] P. R. Utami, "Analisis Perbandingan Quality of Service Jaringan Internet Berbasis Wireless Pada Layanan Internet Service Provider (Isp) Indihome Dan First Media," *J. Ilm. Teknol. dan Rekayasa*, vol. 25, no. 2, pp. 125–137, 2020, doi: 10.35760/tr.2020.v25i2.2723.

[12] A. R. Maulana, H. Walidainy, M. Irhamsyah, F. Fathurrahman, and A. Bintang, "Analisis Quality of Service (Qos) Jaringan Internet Pada Website E-Learning Univiersitas Syiah Kuala Berbasis Wireshark," *J. Komputer, Inf. Teknol. dan Elektro*, vol. 6, no. 2, pp. 27–30, 2021, doi: 10.24815/kitektro.v6i2.22284.

[13] Aprianto Budiman, M. Ficky Duskarnaen, and Hamidillah Ajie, "Analisis Quality of Service (Qos) Pada Jaringan Internet Smk Negeri 7 Jakarta," *PINTER J. Pendidik. Tek. Inform. dan Komput.*, vol. 4, no. 2, pp. 32–36, 2020, doi: 10.21009/pinter.4.2.6.

[14] N. Iryani, A. D. Ramadhani, and M. K. Sari, "Analisis Performansi Routing OSPF menggunakan RYU Controller dan POX Controller pada Software Defined Networking," *J. Telekomun. dan Komput.*, vol. 11, no. 1, p. 73, 2021, doi: 10.22441/incomtech.v11i1.10187.

[15] M. I. S. Aryo Nur Utomo, ST, M.Kom1, "Implementasi Sistem Keamanan Server Menggunakan Honeypot Dan Raspberry Pi Terhadap Attacker," *J. Rekayasa Inf.*, vol. 7, no. 2, pp. 71–77, 2018.