CoMBInES
CONFERENCE ON MANAGEMENT, BUSINESS, INNOVATION, EDUCATION AND SOCIAL SCIENCES

Volume 4 No 1 (2024)

Received : Dec 12, 2023
Accepted : Dec 20, 2023
Published : Mar 28, 2024

Conference on Management, Business, Innovation, Education and Social Science
https://journal.uib.ac.id/index.php/combines

Analisis Perbandingan VPN Tunnel antara ngrok Edge Cloud vs Public IP Address menggunakan Open VPN

Gautama Wijaya[1], Tony Tan[2], Haeruddin[3], Stefanus Eko Prasetyo[4], Sun Pho[5]
Email : [1]gautama.wijaya@uib.ac.id, [2]tony@uib.ac.id

[1-5]Department of Information Technology, Universitas Internasional Batam, Batam, Indonesia

Abstrak

Ngrok adalah sebuah platform yang menyediakan solusi yang memungkinkan aplikasi pada jaringan pribadi untuk diakses melalui internet. Layanan ini menggunakan teknologi reserve proxy, yang membuat IP publik tidak diperlukan. Memanfaatkan kelebihan dari platform ngrok dan mengombinasikan dengan OpenVPN menghasilkan solusi layanan VPN baru tanpa memerlukan IP Publik. Artikel ini akan membahas solusi VPN yang diusulkan yang menggabungkan ngrok dan OpenVPN. Solusi ini membuat layanan VPN tanpa IP Public Static, yang diperlukan ketika menyediakan Layanan VPN. Untuk memastikan kualitas solusi yang diusulkan, artikel ini mendemonstrasikan, menguji, dan menganalisis QoS parameter pada VoIP. Hasil penelitian mengungkapkan bahwa menggabungkan kedua teknologi ini tidak mempengaruhi kinerja layanan VPN dan ngrok dapat digunakan sebagai pengganti IP Publik pada penyediaan layanan VPN.

Kata Kunci: openvpn, VPN, ngrok, QOS, VoIP.

Pendahuluan

Network tunneling merupakan koneksi virtual poin-to-poin yang dibuat antara dua perangkat jaringan melalui jaringan publik atau pribadi (Risdianto and Rumani 2011). Memanfaatkan tunneling dapat memberikan banyak manfaat kepada pengguna, seperti menyembunyikan alamat IP address, membuat jaringan yang aman dan terenkripsi (Shuai, Qianli, and Xing 2016). Teknologi tunneling digunakan untuk menyambungkan jaringan jarak jauh dengan aman melalui internet, seperti dalam kasus Jaringan Pribadi Virtual (VPN). Pada VPN, tunneling dibuat antara perangkat pengguna dan server VPN, memungkinkan pengguna mengakses internet dengan aman dan pribadi. Tunneling juga dapat digunakan untuk melewati batasan atau untuk menyediakan akses aman ke sumber daya jarak jauh.

Tunnel Broker adalah salah satu mekanisme tunnel yang dinamis, diaktifkan berdasarkan permintaan pengguna (Angelo 2019). membuat tunneling antara jaringan diperlukan Internet Protocol (IP), ini adalah protokol yang digunakan untuk mengkomunikasikan data melalui jaringan packet-switched menggunakan Internet Protocol Suite (Risdianto and Rumani 2011). IP adalah protokol utama di Lapisan Internet dari Internet Protocol Suite dan mempunyai tugas mengirimkan paket dari host sumber ke host tujuan berdasarkan alamat IP-nya. Dengan begitu

paket yang sudah di encapsulates dapat dikirim dari pengguna ke VPN server untuk membentuk tunneling (Pohl and Schotten 2017).

ngrok Edge Cloud merupakan platform yang mengizinkan aplikasi yang berada di jaringan local dapat digunakan oleh pengguna dari internet (Wang et al. 2022), (Narvios et al. 2022). Ngrok mengunakan teknologi reverse proxy yang didistribusikan secara global yang mengamankan, melindungi, dan mempercepat aplikasi dan layanan jaringan, terlepas dari lokasinya. Dengan menggabungkan komponen seperti reverse proxy, load balancer, gateway API, firewall, dan perlindungan DDoS. Pada tools ini tidak bergantung pada environment yang digunakan sehingga dapat berkerja pada berbagai jenis sistem operasi.

Pada artikel membahas tentang Performance analysis dan pengembangan layanan Virtual Private Network (VPN). pengembangan yang dimaksud adalah mengombinasikan OpenVPN dengan ngrok edge cloud. memanfaatkan kemampuan dari ngrok edge cloud yang dapat mengizinkan layanan diakses dari internet tanpa memiliki IP Public. Dengan begitu ngrok tersebut dapat menjadi tunnel broker bagi pengguna dengan layanan OpenVPN. untuk mendapatkan informasi yang komprehensif tentang performance dari kombinasi keduanya pada penelitian ini juga melakukan komparasi antara VPN menggunakan IP Public dan ngrok. Pada artikel ini menggunakan metode penelitian eksperimental dengan melakukan pengujian terhadap kedua model VPN tersebut pada voice over internet protocol (VoIP). Menggunakan penggujian tersebut dapat diperoleh analisis kualitas layanan dengan parameter delay, jitter, throughput dan packet loss (Ubedilah, Budiyanto, and Silalahi 2022). Dengan begitu dapat memberikan informasi yang komprehensif tentang kemampuan dari model yang diajukan.

TEKNOLOGI

1. VoIP

VoIP adalah singkatan dari *Voice over Internet Protocol,* sebuah teknologi yang memungkinkan komunikasi suara dan multimedia ditransmisikan melalui Internet daripada saluran telepon tradisional. VoIP mengubah sinyal suara analog menjadi paket data digital dan mengirimkannya melalui jaringan komputer (Tomás and Bidet 2023). Teknologi ini telah merevolusi komunikasi, sehingga memungkinkan untuk melakukan panggilan suara dan video, mengirim pesan, dan berbagi konten multimedia melalui Internet dengan biaya yang jauh lebih rendah dibandingkan layanan telepon tradisional. SIP adalah singkatan dari *Session Initiation Protocol*, yang merupakan protokol pensinyalan yang digunakan untuk memulai, memelihara, dan mengakhiri sesi real-time yang melibatkan video, suara, pesan, dan aplikasi serta layanan komunikasi lainnya melalui jaringan (Kapoor et al. 2023). Ini adalah komponen kunci dari jaringan VoIP. Ini digunakan untuk membuat dan mengelola panggilan suara dan video, pesan instan, dan aplikasi komunikasi lainnya.

2. Open VPN

OpenVPN adalah teknologi open source yang memiliki protokol *tunneling* paling aman yang menawarkan dua mode dasar: yang berjalan sebagai VPN *Layer* 2 dan *Layer* 3. *Tunnel OpenVPN* juga dapat mengangkut *Ethernet Frames*, paket IPX, dan *Windows Network Browsing packets* (NETBIOS), masalah umum di sebagian besar perusahaan membutuhkan solusi VPN. Setelah OpenVPN membuat *tunneling*, firewall di perusahaan dapat melindungi laptop apa pun, meskipun itu bukan *environments* lokal. OpenVPN dapat dikonfigurasi sebagai layanan TCP atau UDP, server, atau klien dan dapat menggunakan semua rule daripada firewall, batasan, mekanisme penerusan, dan konsep seperti NAT. OpenVPN memungkinkan autentikasi

pengguna yang aman menggunakan kunci publik (statis), dan nama pengguna dan kata sandi. OpenVPN adalah VPN tipe SSL yang menggunakan Kode Autentikasi Pesan berbasis Hash (HMAC) dengan algoritma hashing SHA1 untuk memastikan integritas isi paket (Manishankar, Saito, and Reed n.d.),(Tschorsch n.d.).

3. ngrok Edge Cloud

Gambar 1. Terminating TLS connections (ngrok.com)

ngrok Cloud Edge merupakan platform yang memungkinkan aplikasi pada jaringan privat diakses dari internet melalui platform tersebut. Dengan begitu, pengguna dengan sumber daya IT yang terbatas dapat dengan mudah mengakses aplikasi yang dibuatnya. Ngrok memiliki sekumpulan domain, alamat TCP, dan modul untuk menyediakan layanan tersebut. Dengan teknologi ini, dimungkinkan untuk memanipulasi kecepatan dan paket data yang keluar dari platform (Sarah et al. 2020). Gambar menunjukkan transmisi paket data hingga mencapai jaringan pribadi atau aplikasi di jaringan pribadi. Berikut ini adalah fitur-fitur yang disediakan platform ini (ngrok):

1. *Zero-knowledge TLS*
2. *Firewall*
3. *Encryption*
4. *Load balancing*
5. *Security*

Tabel 1. Conference on Management Combines (Font Tahoma 10 Bold)

No	Manajemen	Teknologi	Conference
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

Sumber : Combines

Tinjauan Pustaka

VPN merupakan alat penting dalam menyediakan jaringan yang aman dan andal untuk mengakses informasi (Wahanani, Idhom, and Mandyartha 2021). Aplikasi ini digunakan untuk mengamankan data pada saat proses transmisi dengan mengenkripsi paket data (Harchay, Berguiga, and Massaoudi 2022). terdapat banyak solusi VPN yang memudahkan perusahaan dalam menyediakan layanan ini. Zerotier adalah solusi VPN yang cara kerjanya sama dengan SASE Framework, Layanan ini menggunakan *Next generation network virtualization* dengan mengkombinasikan VPN dan SD-WAN. Dengan begitu, pengguna dapat terhubung dan berbagi data melalui jaringan yang disediakan oleh platform (Goethals et al. 2019), (Hadinata, Prasetyo, and Haeruddin 2022). Solusi selanjutnya, SoftEther adalah aplikasi open-source yang menyediakan akses jarak jauh VPN dan situs-ke-situs Layanan VPN. Penggunaan aplikasi ini

dapat memudahkan IT dalam mengelola sumber daya. kelebihan lain dari VPN ini adalah kemampuannya mendukung *Dynamic DNS* dan *NAT Traversal* (Kuroda 2017).

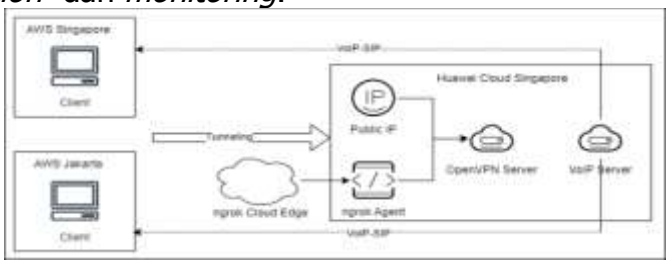
Solusi berikutnya adalah *framework Secure Access Service Edge* (SASE), yang menggabungkan teknologi *Software-defined networking in a wide area network* (SD-WAN) dan fungsi keamanan *cloud-native* (Nguyen et al. 2021). Kombinasi keduanya menghasilkan layanan VPN yang andal untuk perusahaan. Kombinasi kedua teknologi ini membuat layanan VPN mampu mengamankan jaringan dengan mengidentifikasi pengguna, perangkat, dan aplikasi (Deshpande 2021). Manfaatnya pada sumber daya IT adalah mengurangi biaya, pengeluaran, memelihara infrastruktur yang kompleks dan terfragmentasi (Bendicho and Bendicho 2023), (Brouwer and Groenewegen n.d.). Banyak penyedia layanan VPN saat ini menggunakan kerangka *Secure Access Service Edge* (SASE). Hal ini memungkinkan pengguna untuk berlangganan layanan dengan berbagai model langganan dan pembayaran.

Menurut penelitian (Budiyanto and Gunawan 2023), untuk mengukur kualitas dari layanan VPN dapat menggunakan aplikasi VoIP. Hal ini karena proses enkripsi yang komplek pada VPN dapat memberikan dampak yang buruk terhadap layanan VoIP. Menurut penelitian (Mohammed and Ali 2013),(H. et al. 2017),(Ramadhan, Firdausi, and Budiyanto 2017) dampak yang ditimbulkan dari penggunaan VPN dapat dianalisa menggunakan standard QoS menurut ITU (International Telecommunication Union) standards, termasuk *delay, jitter, throughput dan packet loss*. Dengan menganalisa parameter tersebut dapat memberikan informasi tentang kualitas dari layanan VPN yang disediakan.

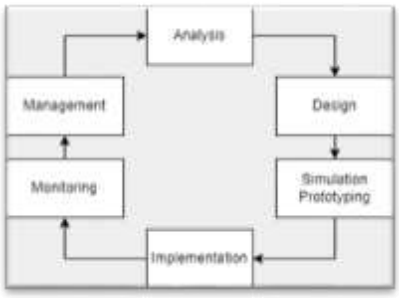
VPN merupakan layanan yang umum saat ini dibutuhkan oleh semua pengguna untuk mengamakan data dan informasi, akan tetapi tidak semua pengguna dapat menyediakan layanan tersebut secara mandiri akibat dari keterbatasan sumber daya. Pada artikel ini membahas tentang penelitian OpenVPN yang mengkombinasikan dengan ngrok Cloud Edge. Memanfaatkan fleksibilitas dan kelebihan masing-masing teknologi dapat membuat penyediaan layanan VPN model baru tanpa membutuhkan *IP Public static* atau *IP Public Dynamic*. Untuk mengukur kualitas dari model yang diajukan tersebut pada penelitian ini menggunakan metode eksperimental dengan menggunakan analisa QoS pada VoIP . Dengan begitu dapat memberikan informasi yang komprehensif terhadap model VPN yang diajukan.

Metodologi Penelitian

pada penelitian ini penulis menggunakan metode *Network Development Life Cycle* (NDLC). NDLC merupakan metode yang digunakan untuk mengembangkan dan mengimplementasikan sistem jaringan (Haeruddin and Kelvin 2022). Pada NDLC terdapat 6 tahapan, namum pada penelitian ini menerapkan 5 tahapan penelitian yaitu *design, simulation protyping, implementation* dan *monitoring*.



Gambar 2. Experiment network topology



Gambar 3. Network Development Cycle Life

Berikut ini merupakan penjelasan setiap tahapan NDLC yang dilakukan pada penelitian ini:

Pada tahap "*analysis*", Pada tahapan ini penulis melakukan analisa terhadap kebutuhan dan solusi layanan cloud yang sudah tersedia saat ini, untuk menentukan solusi dan metode evaluasi terhadap model VPN baru yang diajukan.

Pada tahap "*design*", Berdasarkan data dari tahapan sebelumnya, pada tahapan ini penulis membuat desain jaringan topologi, serta eksperimen untuk menguji kemampuan dari VPN yang diajukan. Gambar 3 merupakan desain yang dibuat dan di uji pada penelitian ini.

Tahap berikutnya adalah "*implementation*" pada tahapan ini, penulis akan mengimplementasi racangan toplogi yang sudah didesain sebelumnya. Untuk menguji VPN, pada tahapan ini penulis menggunakan 2 penyedia layanan cloud yang berbeda untuk memastikan data keluar menuju ke internet.

Tahap terakhir dilakukan adalah penulis akan melakukan pemantauan dan pengujian terhadap parameter yang telah ditentukan. Dengan melakukan pemantauan kedua jaringan OpenVPN yaitu *IP Public* dan ngrok yang dimulai dengan Packet Loss, Throughput, Delay, Jitter.

1. Experiment Environment

Tabel 1. Experiment Environment Specification

No	Nama	Spesifikasi	Lokasi
1	VOIP Server	CPU = 2 CORE, RAM = 4GB, *Storage* HDD = 40 GB,sistem Operasi = Linux	HUAWEI CLOUD *Region Singapore*
2	OpenVPN Server	CPU = 2 CORE, RAM = 4GB, *Storage* HDD = 40 GB, Network = 300 Mbps ,sistem Operasi = Linux	HUAWEI CLOUD *Region Singapore*
3	Client 1	CPU = 2 CORE, RAM = 4GB, *Storage* HDD = 40 GB,sistem Operasi = Windows Server	AWS *Region Singapore*
4	Client 2	CPU = 2 CORE, RAM = 4GB, *Storage* HDD = 40 GB,sistem Operasi = Windows Server	AWS *Region* Jakarta

Pada Tabel 1 merupakan *environments* akan digunakan pada *Experiment network topology*. Untuk mendapatkan informasi komprehensif mengenai kemampuan dari kedua layanan VPN tersebut, pada penelitian ini menggunakan dua (2) penyedia layanan Cloud. kedua penyedia layanan cloud tersebut yaitu Huawei Cloud dan AWS Cloud hal ini bertujuan untuk memastikan client menggunakan jaringan internet untuk terhubung ke layanan VPN. selain memisahkan kedua *environment* pada cloud yang berbeda, pada penelitian ini juga

memanfaatkan keuntungan cloud dengan menempatkan kedua client di region yang berbeda yaitu singapore dan indonesia (jakarta) untuk informasi pembagian client terdapat pada Tabel 1.

2. Skenario Pengujian

Pada bab ini akan membahas tentang scenario yang digunakan untuk menguji model VPN yang diajukan. Berdasarkan gambar 2 terdapat dua model VPN yang akan digunkan pada penelitian ini. Kedua model VPN tersebut akan di uji dengan menggunakan VoIP dengan cara menghubungi antara *client* 1 dan *client* 2 secara bergantian sebanyak 10 kali, untuk durasinya 60 menit setiap komunikasi. Berikut ini dua scenario yang akan digunakan pada penelitian ini.

1. Skenario 1: Openvpn + *IP Public*
2. Skenario 2: Openvpn + ngrok Edge Cloud

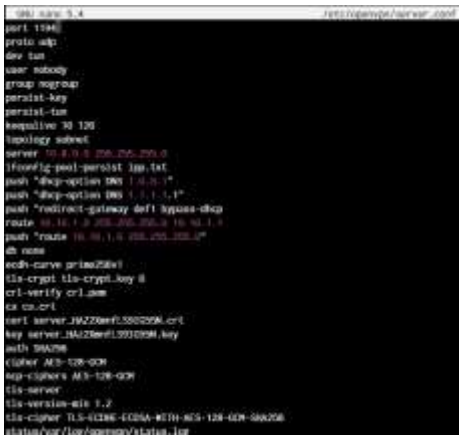
3. Pengumpulan data

Untuk memastikan kemampuan dari layanan VPN yang diusulkan, artikel ini menggunakan metode *sniffing* paket dengan menangkap semua *traffic* yang melewati *TAP-Windows Adapter interface* (Yan 2023). Setelah data di*capture*, data tersebut akan disimpan dalam bentuk file bertipe pcap. Untuk mendukung kegiatan pada tahap ini, gunakan tool wireshark. Alat perangkat lunak gratis ini dapat membantu dengan kemampuan *packet-sniffing*, menangkap aktivitas, *analytics*, dll. Dalam percobaan ini, perangkat lunak ini dipasang di *environments* VOIP Server (Adjardjah et al. 2023). Ini digunakan untuk menangkap semua paket jaringan dan menganalisisnya.

4. VPN Configuration

1. OpenVPN + *IP Public*

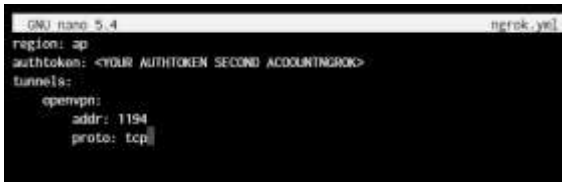
Setelah OpenVPN Server berhasil diimplementasi hingga OpenVPN telah diaplikasikan ke server, seperti yang terlihat pada Gambar 4 menghubungkan OpenVPN ke server menggunakan *IP Public*.



Gambar 4. OpenVPN + IP Public Configuration

2. OpenVPN + ngrok Edge Cloud

Seperti yang terlihat pada gambar 5a konfigurasi khusus pada file ngrok.yml untuk melakukan *tunneling* pada OpenVPN ke server menggunakan protocol tcp, selanjutnya pada gambar 5b menambahkan konfigurasi pada openvpn, setelah semua konfigurasi pada OpenVPN Server selesai, seperti pada yang terlihat gambar 5c bahwa dashboard dari ngrok TCP Url yang dihasilkan ngrok Cloud Edge akan digunakan sebagai akses poin openvpn.



(a)

(b)

(c)

Gambar 5. OpenVPN + ngrok Configuration

5. Quality of Service Parameter (QoS)

QoS adalah kemampuan untuk meningkatkan kualitas layanan jaringan dengan mengatur *throughput, packet loss, jitter, dan delay*. Penelitian ini berfokus pada pedoman standar ITU-T.G.1010 yang menetapkan nilai-nilai spesifik agar pengalaman pengguna terhadap QoS terasa baik. Jaringan, baik kabel maupun nirkabel, rentan terhadap gangguan yang dapat merugikan performanya. Beberapa parameter yang digunakan untuk menilai performa jaringan serta batasan nilai dari standar ITU-T.G.1010 dapat membantu dalam memahami hal ini (Balafif and Aini 2022).

1. Delay

Delay adalah waktu yang diperlukan oleh data untuk sampai dari sumber ke tujuan. Faktor-faktor yang mempengaruhi *delay* termasuk jarak, hambatan fisik, dan waktu pemrosesan. Kategori *Delay* dihitung menggunakan persamaan (1). Dimana *Delay* dihitung dengan membagi waktu pengamatan (Lo) dengan total paket yang diterima (∑ PR). Tabel 2 memberikan klasifikasi delay.

$$Delay = \frac{\text{Lo}}{\sum \text{PR}} \qquad (1)$$

Tabel 2. Delay

Kategori *Delay*	Besar *Delay*	Indeks
Sangat Bagus	<150 ms	4
Bagus	150 s/d 300 ms	3
Sedang	300 s/d 450 ms	2
Buruk	>450 ms	1

2. Jiiter

Jitter merupakan fluktuasi dalam waktu antrean, durasi pemrosesan data, dan interval untuk mereview ulang paket di tahap akhir perjalanan. Pengukuran kualitas layanan (QoS) untuk kategori *Jitter* diuraikan dalam persamaan (2). Di sini, *Jitter* dihitung dengan membagi total Variasi *Delay* (∑ DV) dengan total paket yang diterima (∑ PR). Tabel 3 menggambarkan klasifikasi jitter.

$$Jitter = \frac{\sum \mathrm{DV}}{\sum \mathrm{PR}} \qquad (2)$$

Tabel 3. Jitter

Kategori *Jitter*	*Jitter* (ms)	Indeks
Sangat Bagus	0 ms	4
Bagus	0 s/d 75 ms	3
Sedang	75 s/d 125 ms	2
Buruk	125 s/d 225 ms	1

3. Packet loss

Packet loss merupakan indikator jumlah paket data yang hilang karena konflik atau kepadatan pada jaringan. Perhitungan Kualitas Layanan (QoS) untuk kategori *Packet Loss* didefinisikan dalam persamaan (3). Dimana *Packet Loss* adalah hasil bagi antara jumlah paket yang dikirim dan diterima (SDP-RDP) dengan jumlah paket yang dikirim (SDP). Tabel 4 menggambarkan klasifikasi *packet loss*.

$$Packet\ Loss = \frac{\mathrm{SDP-RDP}}{\mathrm{SDP}} \qquad (3)$$

Tabel 4. Packet Loss

Kategori *Packet Loss*	*Packet Loss*	Indeks
Sangat Bagus	0 %	4
Bagus	3 %	3
Sedang	15 %	2
Buruk	25 %	1

4. Throughput

Throughput merupakan jumlah total paket yang berhasil tiba di tujuan dalam rentang waktu tertentu, dibagi dengan durasi waktu tersebut. Perhitungan Kualitas Layanan (QoS) untuk kategori *Throughput* didasarkan pada persamaan (4), di mana *throughput* didefinisikan sebagai hasil bagi antara jumlah paket yang diterima (RDP) dengan durasi pengamatan (Lo). Pengukuran *throughput* dilakukan dalam satuan bit per detik. Tabel 5 memaparkan klasifikasi *throughput*.

$$Throughput = \frac{\text{RDP}}{\text{Lo}} \qquad (4)$$

Tabel 5. Throughput

Kategori *Throughput*	*Throughput*	Indeks
Sangat Bagus	> 1200 Kbps	4
Bagus	700-1200 Kbps	3
Sedang	338-700 Kbps	2
Buruk	0-338 Kbps	1

Hasil dan Pembahasan

Pada bagian ini akan membahas hasil ekperimen yang dilakukan dengan mengumpulkan QoS parameter seperti *delay, packet loss, jitter* dan *throughput*. Setelah nilai dari QoS parameter tersebut terkumpul akan dilakukan perbandingan antara kedua skenario pengujian dan perbandingan dengan nilai standard QoS yang mengacu pada ITU-T.G.1010.

1. OpenVPN + *IP Public*

Pada tabel 6 merupakan nilai parameter QoS yang dikumpulkan pada eksperimen skenario pertama Openvpn + *IP Public.*

Tabel 6. Hasil eksperimen skenario 1 OpenVPN + IP Public

Information	*Call*	*Delay* (ms)	*Throughput* (Kbps)	*Packet Loss* (%)	*Jitter* (ms)
Average Singapore to Jakarta		5.101	209.7	0.04	6.5885
Singapore to Jakarta	1	4.93 ms	176 Kbps	0.03%	5.195ms
	2	4.94 ms	176 Kbps	0.03%	5.65ms
	3	4.95 ms	176 Kbps	0.06%	5.085ms
	4	4.97 ms	175 Kbps	0.03%	5.395ms
	5	4.53 ms	564 Kbps	0.05%	5.785ms
	6	4.92 ms	177 Kbps	0.04%	5.35ms
	7	6.84 ms	128 Kbps	0.07%	16.29ms
	8	4.95 ms	176 Kbps	0.03%	5.25ms
	9	4.98 ms	175 Kbps	0.03%	5.84ms
	10	5 ms	174 Kbps	0.03%	6.045ms

Information	*Call*	*Delay* (ms)	*Throughput* (Kbps)	*Packet Loss* (%)	*Jitter* (ms)
Average Jakarta to Singapore		5.1	167	0.39	6.5682
Jakarta to Singapore	1	4.94 ms	172 Kbps	0.03%	4.46ms
	2	4.94 ms	172 Kbps	0.04%	5.56ms
	3	4.95 ms	172 Kbps	0.04%	5.695ms
	4	4.96 ms	171 Kbps	0.03%	5.4ms
	5	4.53 ms	173 Kbps	0.05%	5.785ms
	6	4.92 ms	173 Kbps	0.04%	5.342ms
	7	6.83 ms	124 Kbps	0.07%	16.31ms
	8	4.95 ms	172 Kbps	0.03%	5.25ms
	9	4.98 ms	171 kbps	0.03%	5.835ms
	10	5 ms	170 Kbps	0.03%	6.045ms
Average		5.1005	188.35	0.215	6.57835

Pengumpulan data telah dilakukan dengan hasil yang ditunjukkan pada Tabel 6. Hasil *packet loss* menunjukkan angka 0.215 % berdasarkan standard QoS pada tabel 4, hasil tersebut dikategorikan sebagai "Sangat Bagus" ini menginformasikan jumlah paket yang hilang pada saat proses transmisi sangat kecil.

Hasil *delay* menghasilkan rata-rata 5.1005 ms selama 10 kali percobaan, dikategorikan sebagai "Sangat Bagus" berdasarkan kategori *delay*. Hal ini menunjukkan bahwa *delay* yang dialami oleh paket yang ditransmisikan rendah.

Hasil *jitter* menunjukkan rata-rata 6.57835 ms bahwa *jitter* yang didapat selama 10 kali percobaan, hal ini dikategorikan "Baik" berdasarkan standard QoS kategori *jitter* pada Tabel 3.

Hasil *throughput* selama 10 kali percobaan menunjukkan rata-rata 188.35 Kbps berdasarkan standard QoS dikategorikan "Buruk". Hal terjadi karena pada *network* hanya fokus mentransfer paket data VoIP.

Berdasarkan nilai parameter QoS pada skenario OpenVPN + *IP Public* menunjukkan aspek positif pada parameter *packet loss* dengan nilai 0.215 % kategori "Sangat Bagus", *delay* 5.1005 ms kategori "Sangat Bagus", dan *jitter* dengan nilai 6.57835 ms kategori "Bagus", namun pada *throughput* dengan nilai 188.35 Kbps kategori "Buruk".

2. OpenVPN + Ngrok

Pada Tabel 7 merupakan nilai paramater QoS yang dikumpulkan pada eksperimen skenario kedua Openvpn + ngrok

Tabel 7. Hasil eksperimen skenario 2 OpenVPN + ngrok

Information	*Call*	*Delay* (ms)	*Throughput* (Kbps)	*Packet Loss* (%)	*Jitter* (ms)
Average Singapore to Jakarta		4.947	175.6	0.009	5.9511
Singapore to Jakarta	1	4.97 ms	175 Kbps	0.01%	6.365ms
	2	4.93 ms	176 Kbps	0.01%	6.09ms
	3	4.93 ms	176 Kbps	0.01%	6.06ms
	4	4.95 ms	175 Kbps	0.00%	6.115ms
	5	4.92 ms	177 Kbps	0.01%	5.785ms
	6	4.94 ms	176 Kbps	0.01%	6.01ms
	7	4.94 ms	176 Kbps	0.01%	6.045ms
	8	4.96 ms	175 Kbps	0.01%	5.51ms
	9	4.94 ms	176 Kbps	0.01%	5.49ms
	10	4.99 ms	174 Kbps	0.01%	6.04ms

Information	*Call*	*Delay* (ms)	*Throughput* (Kbps)	*Packet Loss* (%)	*Jitter* (ms)
Average Jakarta to Singapore		4.945	171.7	0.009	5.9473
Jakarta to Singapore	1	4.96 ms	171 Kbps	0.01%	6.36ms
	2	4.93 ms	172 Kbps	0.01%	6.087ms
	3	4.93 ms	172 Kbps	0.01%	6.06ms
	4	4.95 ms	172 Kbps	0.00%	6.11ms
	5	4.92 ms	173 Kbps	0.01%	5.77ms
	6	4.94 ms	172 Kbps	0.01%	6.005ms
	7	4.94 ms	172 Kbps	0.01%	6.04ms
	8	4.95 ms	171 Kbps	0.01%	5.505ms
	9	4.94 ms	172 Kbps	0.01%	5.485ms

	10	4.99 ms	170 Kbps	0.01%	6.051ms
Average		4.946	173.65	0.009	5.9492

Table 7 menunjukkan *throughput*, *delay*, *packetloss*, dan *jitter* dari hasil pengujian eksperimental OpenVPN + Ngrok, dengan pengujian sebanyak sepuluh kali telphone.

Hasil *packet loss* menunjukkan angka rata-rata 0.009 % yang dikategorikan sebagai "Sangat Bagus". Kategori tersebut menunjukan bahwa kombinasi kedua teknologi juga dapat mentransmisikan paket dengan baik ke tujuan. Hal tersebut menunjukan karakteristik yang positif untuk layanan VPN.

Delay yang dihasilkan rata-rata 4.946 ms selama 10 kali percobaan, hal ini dikategorikan "Sangat Bagus" berdasarkan standard kategori *delay*. Kategori yang di dapat pada parameter ini menunjukan bahwa kombinasi dari kedua teknologi tersebut tidak menyebabkan peningkatan yang signitifikan terhadap waktu pengiriman paket data,

Jitter yang dihasilkan rata-rata 5.9492 ms selama 10 kali percobaan, yang dikategorikan "Bagus" berdasarkan standard kategori *jitter*. hal mengimplikasikan kombinasi openvpn dan ngrok yang menggunakan teknologi *reserve proxy* tidak mengganggu atau menyebabkan variasi pengiriman menjadi lebih buruk. Hal ini sangat penting VoIP dalam menjadi transmisi yang konsisten dan lancar pada jaringan VoIP.

Throughput yang dihasilkan rata-rata sebesar 173.65 Kbps selama 10 kali percobaan, hal ini dikategorikan "Buruk" berdasarkan standard kategori *throughput*. Penyebab utama nilai *throughput* yang kecil, karena pada jaringan hanya fokus dalam proses mentransmisikan paket data VoIP.

Tabel 8. SYSTEM ANALYSIS

Skenario	*Delay* (ms)	*Throughput* (Kbps)	*Packet Loss* (%)	*Jitter* (ms)
1. OpenVPN + *IP Public*	5.1005	188.35	0.215	6.57835
2. OpenVPN + Ngrok	4.946	173.65	0.009	5.9492

Pada Tabel 8 merupakan perbandingan nilai rata-rata parameter QoS antara skenario 1 Openvpn+*IP Public* dan skenario 2 OpenVPN + ngrok.

pada parameter "*Delay*" skenario 2 mendapatkan nilai yang lebih baik dengan nilai rata-rata *delay* adalah 4.946 ms. Berdasarkan standard QoS ITU pada Tabel 2 dikategorikan sangat bagus (< 150 ms). Sedangkan perbedaan nilai *delay* antara skenario 1 dan 2 hanya terpaut 0.1545 ms. Terdapat banyak faktor yang dapat menyebabkan nilai *value delay* naik, diantaranya adalah jarak, komputer *hardware* dan waktu proses.

Pada parameter "*Throughput*" skenario 1 lebih ungul dengan nilai rata-rata *throughput* 188.35. sedangkan nilai *throughput* skenario 2 adalah 173.65. selisih antara kedua skenario adalah 14,6 kbps. Kedua skenario mendapatkan kategori buruk karena *throughput* yang dihasilkan berada pada rentang 0-338 Kbps berdasarkan standard QoS ITU *throughput* Tabel 5. Penyebab kedua skenario mendapat nilai buruk pada parameter ini, karena jaringan hanya fokus untuk mentransmisikan paket data VoIP.

Pada parameter "*Packet Loss*" skenario 2 mendapatkan nilai rata-rata 0.009. nilai *packet loss* jauh lebih dari pada skenario 1. berdasarkan standard QoS ITU untuk *packet loss* mendapatkan kategori "Bagus" (3%).

pada parameter "*Jitter*" skenario 2 mendapatkan nilai 5.9492 ms, nilai tersebut lebih rendah dari pada skenario 1. Berdasarkan standard QoS ITU *jitter* yang nilai *jitter* skenario 1 mendapatkan kategori bagus (0 s/d 75 ms).

Berdasarkan hasil analisa yang terdapat pada tabel 8 menunjukan perbandingan parameter QoS kedua model VPN yang digunakan dalam penelitian. Hasilnya skenario 2 Openvpn + ngrok dapat dikombinasikan dengan VPN. kombinasi kedua teknologi tersebut menghasilkan model VPN baru yang tidak membutuhkan *IP Public*. kombinasi keduanya juga memberikan manfaat pada proses penyediaan layanan VPN yang *flexibel* dan murah. Penggunaan ngrok pada layanan VPN tidak memberikan dampak yang buruk pada layanan VPN.

Kesimpulan

Hasil pengembangan layanan VPN yang diajukan telah berhasil di implementasi dan diuji menggunakan metode penelitian NDLC. Hasil penelitian terdapat pada tabel 8, skenario 2 yang menjadi objek dari penelitian ini mendapatkan nilai parameter *delay* 4.946 ms, *throughput* 173.65, *packet loss* 0.009% dan *jitter* 5.9492 ms. berdasarkan standard QoS dan perbandingan antara skenario, kombinasi openvpn dan ngrok tidak memberikan dampak yang buruk terhadap layanan VPN. Dengan begitu ngrok dapat digunakan sebagai penganti publik IP dalam hal penyediaan layanan VPN yang murah dan *flexibel*.

Acknowledgments

Penulis mengucapkan terima kasih kepada Universitas Internasional Batam atas dukungannya.

Daftar Pustaka

Adjardjah, Winfred, Franklin Kumassah, Dawood Mohammed Abdallah, and John Awuah Addor. 2023. "Performance Evaluation of VoIP Analysis and Simulation." *Journal of Engineering Research and Reports* 25(7): 176–91.

Angelo, Raymond. 2019. "Secure Protocols And Virtual Private Networks: An Evaluation." *Issues in Information Systems* 20(3).

Balafif, Sabri, and Ikhda Qurrata Aini. 2022. "Analysis of Computer Network Performance on Communication and Informatics Office of West Sumbawa Regency Using Quality of Service Method." *Journal of Information Systems and Informatics* 4(4): 992–1007.

Bendicho, Carlos, and Daniel Bendicho. 2023. "Techno-Economic Assessment in Communications: New Challenges." In *Intelligent Computing*, Lecture Notes in Networks and Systems, ed. Kohei Arai. Cham: Springer Nature Switzerland, 134–50. https://link.springer.com/10.1007/978-3-031-37963-5_11 (October 14, 2023).

Brouwer, Marius, and Anand Groenewegen. "Cloud Access Security Brokers (CASBs) Characterization of the CASB Market and Its Alignment with Corporate Expectations Commissioned by KPMG Netherlands."

Budiyanto, Setiyo, and Dadang Gunawan. 2023. "Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice Over Internet Protocol." *IEEE Access* 11: 60853–65.

Deshpande, Dr. Aniket. 2021. "Relevance of Zero Trust Network Architecture Amidts and It's Rapid Adoption Amidts Work From Home Enforced by COVID-19." *Psychology and Education Journal* 58(1): 5672–77.

Goethals, Tom, Dwight Kerkhove, Bruno Volckaert, and Filip De Turck. 2019. "Scalability Evaluation of VPN Technologies for Secure Container Networking." In *2019 15th International Conference on Network and Service Management (CNSM)*, Halifax, NS, Canada: IEEE, 1–7. https://ieeexplore.ieee.org/document/9012673/ (October 13, 2023).

H., Mahdi et al. 2017. "Simulation and Analysis of Quality of Service (QoS) Parameters of Voice over IP (VoIP) Traffic through Heterogeneous Networks." *International Journal of Advanced Computer Science and Applications* 8(7). http://thesai.org/Publications/ViewPaper?Volume=8&Issue=7&Code=ijacsa&SerialNo=32 (October 20, 2023).

Hadinata, Frans, Stefanus Eko Prasetyo, and Haeruddin Haeruddin. 2022. "Analisa Penggunaan Jaringan ZeroTier di Masa Pandemi Covid-2019." *Jurnal Ilmu Komputer dan Bisnis* 13(1): 85–93.

Harchay, Ahlem, Abdelwahed Berguiga, and Ayman Massaoudi. 2022. "An Enhanced Traffic Split Routing Heuristic for Layer 2 and Layer 1 Services." *International Journal of Advanced Computer Science and Applications* 13(1). http://thesai.org/Publications/ViewPaper?Volume=13&Issue=1&Code=IJACSA&SerialNo=90 (October 12, 2023).

Kapoor, Maya et al. 2023. "Detecting VoIP Data Streams: Approaches Using Hidden Representation Learning." *Proceedings of the AAAI Conference on Artificial Intelligence* 37(13): 15519–27.

Kuroda, Toshikazu. 2017. "A Combination of Raspberry Pi and SoftEther VPN for Controlling Research Devices via the Internet." *Journal of the Experimental Analysis of Behavior* 108(3): 468–84.

Manishankar, Karthik, Patricia Saito, and Ben Reed. "Bridging Web Authentication to OpenVPN."

Mohammed, Hussein A, and Adnan Hussein Ali. 2013. "Effect of Some Security Mechanisms on the Qos VoIP Application Using OPNET." *International Journal of Current Engineering and Technology*.

Narvios, Wilen Melsedec O. et al. 2022. "Utilizing Web Page for Electrical Load Control and Power Monitoring." In Manila, Philippines, 050005. https://pubs.aip.org/aip/acp/article/2827140 (October 20, 2023).

"Ngrok \textbar Unified Application Delivery Platform for Developers." https://ngrok.com/ (December 13, 2023).

Nguyen, Van-Linh et al. 2021. "Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges." *IEEE Communications Surveys & Tutorials* 23(4): 2384–2428.

Pohl, Frederic, and Hans Dieter Schotten. 2017. "Secure and Scalable Remote Access Tunnels for the IIoT: An Assessment of openVPN and IPsec Performance." In *Service-Oriented and Cloud Computing*, Lecture Notes in Computer Science, eds. Flavio De Paoli, Stefan Schulte, and Einar Broch Johnsen. Cham: Springer International Publishing, 83–90. https://link.springer.com/10.1007/978-3-319-67262-5_7 (September 4, 2023).

Ramadhan, Eko, Ahmad Firdausi, and Setiyo Budiyanto. 2017. "Design and Analysis QoS VoIP Using Routing Border Gateway Protocol (BGP)." In *2017 International Conference on Broadband Communication, Wireless Sensors and Powering (BCWSP)*, , 1–4.

Risdianto, Aris Cahyadi, and R. Rumani. 2011. "IPv6 Tunnel Broker Implementation and Analysis for IPv6 and IPv4 Interconnection." In *2011 6th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, , 139–44.

Sarah, Annisa et al. 2020. "Learning IoT: Basic Experiments of Home Automation Using ESP8266, Arduino and XBee." In *2020 IEEE International Conference on Smart Internet of Things (SmartIoT)*, Beijing, China: IEEE, 290–94. https://ieeexplore.ieee.org/document/9192394/ (October 20, 2023).

Shuai, Yang, Zhang Qianli, and Li Xing. 2016. "A Tunnel Broker Based IPv6 Access System for a Small Scale Network with IPv4 Upstream." In *2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference*, , 206–10.

Tomás, Livia, and Ophélie Bidet. 2023. "Conducting Qualitative Interviews via VoIP Technologies: Reflections on Rapport, Technology, Digital Exclusion, and Ethics." *International Journal of Social Research Methodology*: 1–13.

Tschorsch, Florian. "OpenVPN TLS-Crypt-V2 Key Wrapping with Hardware Security Modules."

Ubedilah, Setiyo Budiyanto, and Lukman Medriavin Silalahi. 2022. "Analysis QoS VoIP Using GRE + IPSec Tunnel and IPIP Based on Session Initiation Protocol." In *2022 5th International Conference of Computer and Informatics Engineering (IC2IE)*, , 47–54.

Wahanani, Henni Endah, Mohammad Idhom, and Eka Prakarsa Mandyartha. 2021. "Analysis of Streaming Video on VPN Networks Between OpenVPN and L2TP/IPSec." In *2021 IEEE 7th Information Technology International Seminar (ITIS)*, , 1–5.

Wang, Yutan, Chi Wei, Haowei Sun, and Aili Qu. 2022. "Design of Intelligent Detection Platform for Wine Grape Pests and Diseases in Ningxia." *Plants* 12(1): 106.

Yan, Xiaodan. 2023. "Deep Learning-Based Efficient Analysis for Encrypted Traffic." *Applied Sciences* 13(21): 11776.