Sistem Keamanan *Work From Anywhere* Menggunakan VPN Generasi Lanjut

Haeruddin [a,1,*], Gautama Wijaya [a,2], Husnul Khatimah [a,3]

[a] Program Sarjana Teknologi Informasi, Universitas Internasional Batam, Jl. Gajah Mada, Baloi – Sei Ladi, Batam 29426, Indonesia
[1] haeruddin@uib.ac.id*; [2] gautama.wijaya@uib.ac.id; [3] 2032029.husnul@uib.edu;
* Koresponsendi penulis

ARTICLE INFO

Article history
Menerima 15 Agustus 2023
Revisi 27 Oktober 2023
Diterima 29 Oktober 2023

Kata Kunci
Jaringan
Keamanan
VPN
WFA
ZeroTier

ABSTRACT

Working remotely or what we know as Work From Anywhere is still a trend after the COVID-19 pandemic. Working from anywhere and anytime can increase productivity and reduce transportation costs, and is accompanied by fast internet support, good communication and collaboration platforms so this is very popular and in demand. When implementing WFA, it has its own challenges, namely data security. Not all organizations are supported by a reliable IT infrastructure that can protect employee data during WFA. One of the security system technologies that can be used during WFA is VPN. Currently there are many VPN protocols that can be used for WFA. However, in implementing a VPN network, there are several things that must be considered to ensure that the VPN network is successful and functional, such as security, choosing the right architecture, selecting technology and protocols, scalability, quality of service, management and monitoring, as well as security and privacy policies. ZeroTier is a next-generation VPN that is easy to configure, can support multiple devices, and uses an end-to-end connection, eliminating the need for a centralized VPN server. In implementing VPN ZeroTier the method used is the Network Development Life Cycle (NDLC). This methodology is used to plan, implement, and manage a VPN network with ZeroTier to function according to WFA needs.

1. Pendahuluan

Bekerja dari mana saja (*Work From Anywhere*) yang biasa disingkat WFA adalah istilah yang digunakan untuk menggambarkan lingkungan kerja di mana karyawan tidak harus bekerja di kantor tradisional atau tempat kerja fisik, tetapi memiliki kemampuan untuk bekerja dari mana saja dengan memilih lokasi yang mereka sukai, seperti rumah, ruang kerja bersama, kedai kopi, atau bahkan saat bepergian yang penting memiliki koneksi internet [1]. Bentuk pekerjaan seperti itu semakin populer dalam beberapa tahun terakhir, terutama sejak pandemi COVID-19 yang memaksa banyak perusahaan beralih ke pekerjaan jarak jauh. Manfaat bekerja dari mana saja mencakup peningkatan produktivitas dan kepuasan kerja, pengurangan waktu dan biaya perjalanan, serta kemampuan untuk berkolaborasi dengan tim yang beragam dari mana saja di dunia [2]. Meskipun pandemi COVID-19 telah berlalu dan menuju *Era New Normal*, tren bekerja jarak jauh masih menjadi populer dan diminati [3], [4]. Hal ini terjadi karena dukungan teknologi, seperti internet berkecepatan tinggi, komputasi awan, alat kolaborasi dan *platform* komunikasi yang memungkinkan bekerja jarak jauh [5].

Keamanan data saat bekerja secara jarak jauh menjadi sangat penting karena adanya potensi risiko tinggi yang harus dipertimbangkan. karyawan yang bekerja di tempat umum seperti di rumah, ruang kerja bersama, kedai kopi atau tempat umum lainnya dengan menggunakan jaringan WI-FI Publik memungkinkan penyusup melakukan pencurian data. Dalam laporan yang diterbitkan oleh *Global advisory and Accounting Networks*, masalah keamanan dunia maya menunjukkan bahwa hampir 65% organisasi mengumumkan bahwa mereka telah dilanggar atau terkena serangan dunia maya selama bekerja jarak jauh [6]. Hal ini dapat terjadi karena mereka tidak dapat menerapkan semua metode perlindungan keamanan informasi dalam menjaga informasi di kantor pada saat WFA. Disisi lain perusahaan mungkin tidak memperhitungkan kesiapan keamanan siber [7]. Kehilangan data saat bekerja jarak jauh berdampak pada individu dan perusahaan seperti kehilangan informasi penting, kerugian finansial, penurunan produktivitas, hilangnya kepercayaan dan reputasi, dan pelanggaran privasi dan kepatuhan. Oleh karena itu, penting untuk memikirkan apa saja cara untuk memastikan keamanan informasi jika terjadi WFA [8].

Salah satu teknologi untuk mengatasi keamanan data saat WFA adalah teknologi *Virtual Private Network* (VPN). VPN adalah teknologi yang digunakan untuk membuat koneksi aman dan terenkripsi antara perangkat yang terhubung ke internet dengan jaringan pribadi atau publik [9]. Dengan menggunakan VPN, data yang dikirimkan dan diterima antara perangkat pengguna dan server tujuan akan dienkripsi, sehingga melindungi informasi sensitif pengguna seperti kata sandi, data keuangan, atau informasi bisnis dari penyusup atau pihak yang tidak berwenang. Ada banyak jenis VPN yang dapat digunakan tergantung dari kebutuhan pengguna seperti *Remote Access* VPN, *Site-to-Site* VPN, SSL/TLS VPN, *IPsec* VPN, dan MPLS VPN [10]. Dalam mengimplementasikan jaringan VPN ada beberapa hal yang harus diperhatikan untuk memastikan jaringan VPN tersebut sukses dan fungsional seperti keamanan, pemilihan arsitektur yang tepat, pemilihan teknologi dan protokol, skalabilitas, kualitas layanan, manajemen dan pemantauan, serta kebijakan keamanan dan privasi.

ZeroTier adalah sebuah *platform* VPN yang dirancang untuk menyederhanakan konektivitas jaringan antar perangkat yang terhubung ke internet. Teknologi ini memungkinkan pengguna untuk membuat jaringan pribadi virtual yang aman di atas infrastruktur internet yang ada. Jaringan pribadi virtual ini menciptakan ruang terpisah dan terenkripsi di antara perangkat yang terhubung, baik di dalam jaringan lokal maupun jaringan publik, seperti internet. ZeroTier menggunakan pendekatan *peer-to-peer*, dimana setiap perangkat yang terhubung ke jaringan ZeroTier menjadi simpul (*node*) dalam jaringan tersebut. Simpul-simpul ini berkomunikasi langsung satu sama lain melalui enkripsi *end-to-end*, menghilangkan kebutuhan terkoneksi melalui VPN server pusat, dan mekanisme otentikasi kriptografi yang kuat untuk memverifikasi identitas dan mengenkripsi lalu lintas data. Setiap simpul dalam jaringan diberikan kunci pribadi unik untuk mengamankan komunikasi, memiliki fleksibel dan dapat digunakan di berbagai lingkungan. Ini mencakup konektivitas antar perangkat di jaringan lokal yang sama, perangkat yang berada di jaringan yang berbeda, atau bahkan perangkat yang berada di belakang *Firewall* atau *Network Address Translation* (NAT). ZeroTier menyediakan konsol manajemen sentral yang memungkinkan *Administrator* untuk mengelola dan mengatur VPN, mengelola pengguna, memberikan izin akses, dan melacak aktivitas jaringan dan kompatibel dengan berbagai *platform*, termasuk Windows, macOS, Linux, iOS, Android, dan bahkan perangkat keras seperti *router*, serta *open-source* dengan lisensi BSD.

Pada penelitian ini metode yang di gunakan mengimplementasikan sistem keamanan bekerja jarak jauh adalah *Network Development Life Cycle* (NDLC). Metodologi ini di gunakan untuk merencanakan, mengimplementasikan, dan mengelola jaringan VPN ZeroTier pada organisasi yang menerapkan WFA. Metode ini melibatkan serangkaian tahap yang terstruktur untuk memastikan jaringan berfungsi dengan baik dan memenuhi kebutuhan sistem keamanan bekerja jarak jauh.

2. Metode

Pada penelitian ini menggunakan metode *Network Development Life Cycle* (NDLC) yang menggunakan pendekatan sistematis dalam perencanaan, desain, implementasi, dan pemeliharaan. Metode NDLC pada penelitian ini akan membantu memastikan bahwa pengembangan jaringan VPN ZeroTier pada organisasi yang menerapkan WFA dilakukan dengan teratur, efisien, dan sesuai dengan kebutuhan peneltian ini [11]–[13]. Berikut ini adalah tahapan-tahapan NDLC yang akan diterapkan pada penelitian ini:

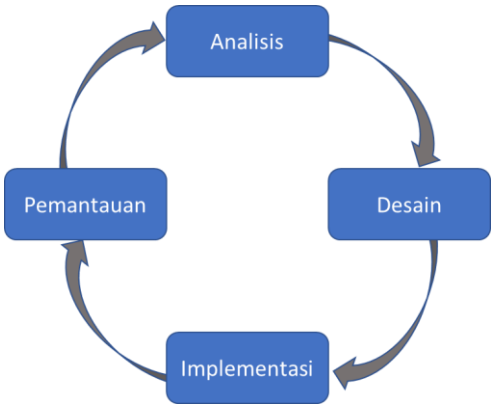

Fig.1. Siklus NDLC

2.1 Analisis

Pada tahapan ini akan dilakukan analisa kebutuhan jaringan meliputi perangkat keras dan perangkat lunak yang akan digunakan, perbandingan teknologi VPN yang ada dengan Zero Tier.

2.2 Desain

Pada tahapan ini akan merancangan topologi jaringan VPN menggunakan Zero Tier yang dapat digunakan untuk mendukung WFA yang dapat diterapkan oleh organisasi yang akan menetapkan WFA menggunakan tools https://app.diagrams.net/.

2.3 Implementasi

Pada tahapan ini melakukan implementasi Jaringan VPN menggunakan Zero Tier sesuai dengan topologi yang telah didesain ditahapan sebelumnya. Implementasi ini meliputi implementasi jaringan Zero Tier pada server (Linux Ubuntu Server), perangkat mobile (Android & iOS, Laptop (Windows), perangkat jaringan (Mikortik OS)

2.4 Monitoring

Setelah melakukan penerapan rancangan jaringan VPN menggunakan Zero Tier telah selesai dilakukan, penulis akan melakukan pemantauan dan pengujian terhadap bandwidth meliputi delay, packet lost dan jitter melalui koneksi jaringan Zero Tier yang telah diterapkan. Untuk mendefinisikan kategori QoS maka data yang didapatkan dari pengukuran tiga parameter terakhir dipotret dengan standar Telecomunication and Internet Protocol harmonization Over Network (TIPHON) [14], [15] seperti pada table 1-3 berikut ini.

Tabel 1. Tingkat kualitas *delay*

Kualitas	**Rentang *Delay* (D)**	**Index**
Buruk	>450ms	1
Sedang	300ms < D ≤ 450ms	2
Bagus	150ms < D ≤ 300ms	3
Sangat Bagus	<150ms	4

Tabel 2. Tingkat kualitas *packet lost*

Kualitas	Rentang *Packet Lost* (P)	Index
Buruk	15% < P ≤ 25%	1
Sedang	3% < P ≤ 15%	2
Bagus	0% < P ≤ 3%	3
Sangat Bagus	0%	4

Tabel 3. Tingkat kualitas *jitter*

Kualitas	Rentang *Jitter* (J)	Index
Buruk	125ms < J ≤ 225ms	1
Sedang	75ms < J ≤ 125ms	2
Bagus	0ms < J ≤ 75ms	3
Sangat Bagus	0ms	4

Pada tahapan ini juga akan dilakukan pengujian keamanan jaringan dengan menggunakan tool Wireshark untuk menangkap paket data yang melalui jaringan Zero Tier apakah dalam kondisi aman atau tidak.

3. Hasil dan Pembahasan

3.1 Analisis

Pada skenario implementasi jaringan WFA, dimana kita menggunakan satu server berbasis *cloud* di Amozon Web Service (AWS), jaringan kantor yang di lengkapi dengan router Mikrotik, dan komputer klien, serta perangkat pengguna yang menggunakan laptop dan *smartphone* yang WFA dari berbagai tempat.

Tabel 4. Kebutuhan Perangkat dan Spesifikasi

Nama Perangkat	Spesifikasi
Server AWS EC2	OS Ubuntu Server, CPU 2 Core, RAM 8 GB, SSD 50 GB
MikroTik RB 951 G	CPU: Atheros AR9344 600Mhz (5) 10/100/1000 Gigabit Ethernet Ports (1) USB 2.0 Port Memory: 128MB DDR2 onboard memory
Laptop	OS Windows, CPU core I7, RAM 16 GB
Smartphone	
Mi Foco F3	OS Android, CPU Snapdragon 870, RAM 8 GB, Storage 256GB

ZeroTier merupakan generasi lanjut VPN dan protocol VPN seperti OpenVPN, IPSec, PPTP, L2TP dapat dikategorikan sebagai tradisional VPN. Pada tabel 5 berikut ini merupakan perbandingan ZeroTier dengan Tradisonal VPN.

ZeroTier memiliki beberapa jenis lisensi mulai dasar, profesional, bisnis, dan edisi komunitas. Edisi dasar diperuntukkan kepada semua orang dengan satu admin, dengan 25 node dan jaringan tanpa batas, namun fitur ini tidak mendukung SSO bisnis, ini dapat digunakan secara gratis. Lisensi berikutnya Profesional yang berbayar dengan biaya per satu user admin 10 USD, dan harga 25 node 5 USD perbulan. Untuk kalangan bisnis harus menghubungi bagian penjualan. Selain itu ZeroTier menyediakan edisi terbuka dengan jumlah node, jaringan, dan admin tampa batas. Hanya saja layanan ini harus di hosting sendiri. Layanan Edisi Terbuka sangat cocok di gunakan di Perusahaan yang memiliki sumber daya manusia di bidang teknologi informasi yang dapat mengelola layanan ini secara mandiri.

Tabel 5. Perbandingan ZeroTier dan Tradisional VPN

Fitur	ZeroTier	Tradisional VPN
Jenis Jaringan	ZeroTier merupakan *software-defined networking* (SDN) yang membuat jaringan *overlay* virtual untuk menghubungkan perangkat dengan aman melalui internet. Ini berfungsi sebagai switch ethernet global yang memungkinkan komunikasi langsung antar perangkat seolah-olah berada dalam jaringan lokal yang sama.	VPN Tradisional membuat terowongan terenkripsi antara perangkat pengguna dan server VPN yang terletak di lokasi fisik yang berbeda. Ini akan menutupi alamat IP pengguna dan mengenkripsi lalu lintas di internet antara perangkat pengguna dan server.
Kemudahan Penggunaan	ZeroTier lebih mudah diatur dan digunakan. Pengguna dapat membuat akun, menginstal klien ZeroTier di perangkat mereka, bergabung dengan jaringan, dan mulai berkomunikasi dengan aman.	VPN biasanya memerlukan penginstalan perangkat lunak klien pada perangkat pengguna, dan pengguna harus terhubung ke server VPN tertentu untuk membuat koneksi yang aman
Skalabilitas	ZeroTier dirancang untuk efisiensi skalabilitas jaringan, sehingga cocok digunakan untuk jaringan pribadi kecil sampai jaringan dengan penyebaran yang besar dengan ribuan perangkat yang terhubung	VPN tradisional dapat menangani koneksi simultan dalam jumlah terbatas, dan beberapa penyedia mungkin memberlakukan pembatasan bandwidth atau penggunaan data
Kasus Penggunaan	ZeroTier sering digunakan untuk komunikasi perangkat ke-perangkat, akses jarak jauh, penerapan IoT yang aman, dan aplikasi game yang memerlukan koneksi latensi rendah.	VPN tradisional biasanya digunakan untuk melindungi privasi online, melewati pembatasan geografis, mengamankan koneksi Wi-Fi publik, dan mengaktifkan akses jarak jauh ke jaringan perusahaan
Kebutuhan Server	Terdesentralisasi -Tidak ada server khusus	Terpusat - Membutuhkan server VPN
Protokol	Hak milik	Berbagai protokol (OpenVPN, IPSec, PPTP, L2TP,dll.)
Ketersediaan	Tersedia untuk berbagai platform	Tersedia untuk berbagai platform

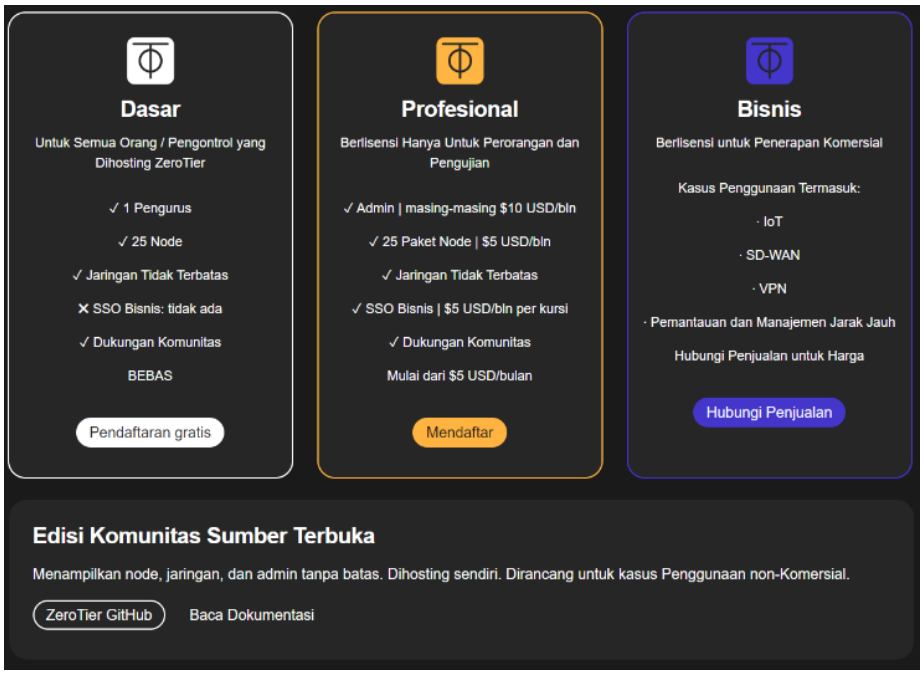

Fig. 2. Jenis Lisensi ZeroTier

3.2 Desain

Topologi yang dirancang pada penelitian ini mengikuti tren saat ini dimana data tidak lagi perpusat di pusat data yang berada di kantor melaikan data terdapat pada layanan cloud seperti AWS, Google, Microsof namun pada skenarion ini akan menggunakan server di layanan AWS.

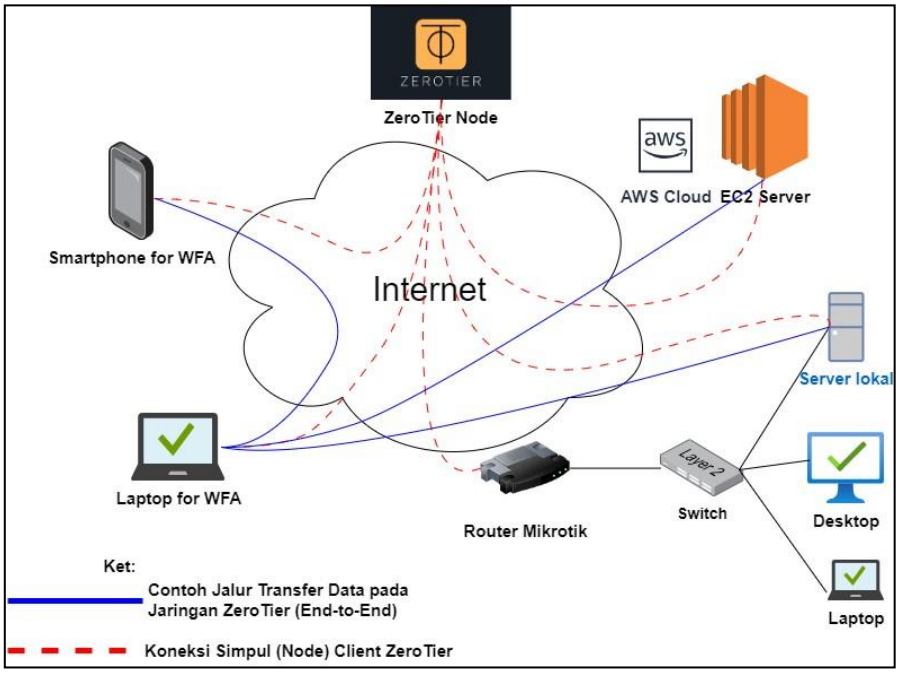

Fig. 3. Topologi Jaringan ZeroTier

Pada topologi gambar 3 dapat dilihat semua perangkat akan terhubung ke simpul ZeroTier dengan garis merah putus-putus seperti server, perangkat jaringan, perangkat pengguna. Setelah terkoneksi maka perangkat dapat berkomuniasi secara *end-to-end* yang di tandai dengan garis biru, tanpa harus melewati simpul ZeroTier.

3.3 Implementasi

Pada tahapan ini akan dilakukan konfigurasi ZeroTier pada server, laptop, smartphone, dan perangkat jaringan Mikrotik.

1. Konfigurasi Simpul ZiroTier

Pada penelitian ini menggunakan layanan dengan lisensi ZeroTier dasar 25 *node* yang berarti dapat membuat 25 jaringan yang berbeda dalam suatu organisasi. Tahap pertama *login* pada laman ZeroTier https://my.zerotier.com/, setelah berhasil login tahap berikutnya membuat jaringan seperti pada gambar 4 berikut ini.

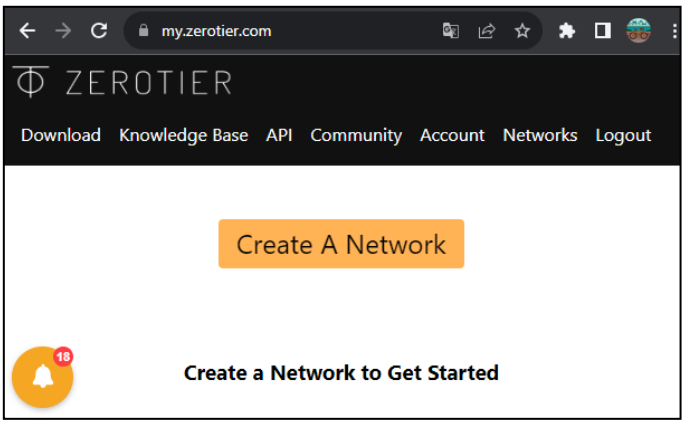

Fig.4. *Dashboard ZeroTier*

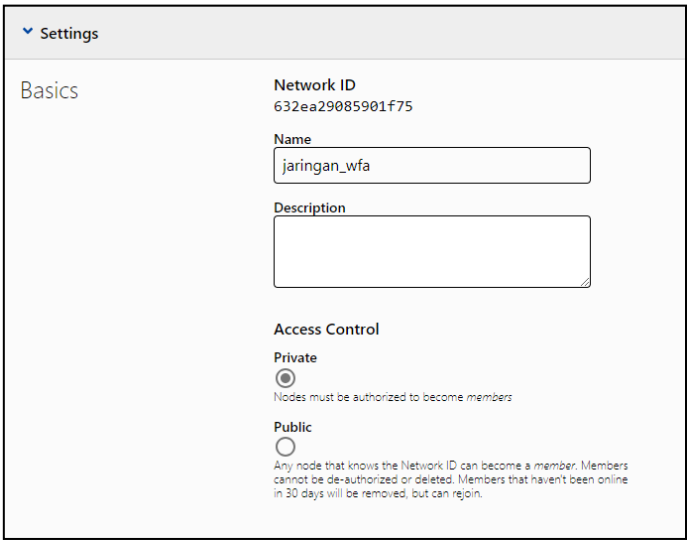

Fig.5. Konfigurasi *ZeroTier* Dasar

Pada gambar 5, tahapan pertama yang harus dilakukan yaitu memberikan nama pada jaringan yang di buat untuk mempermudah adminstrasi jaringan, setelah itu membuat *access* kontrol *Private* agar *user* yang terdaftar yang dapat menggunakan jaringan VPN ZeroTier ini.

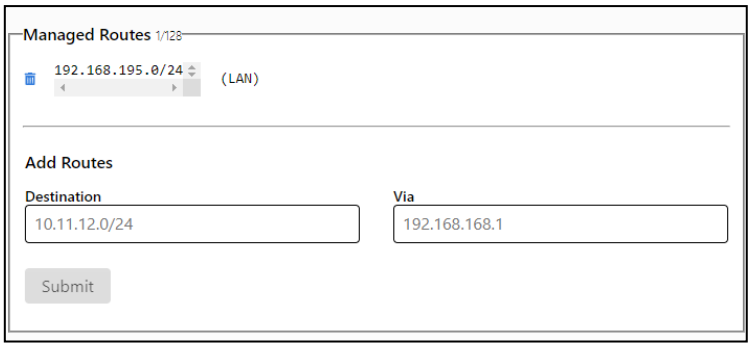

Fig. 6. Konfigurasi *Routing*

Pada gambar 6 merupakan konfigurasi routing, pada kasus ini disini hanya untuk menghubungan sesama jaringan lokal untuk WFA. Jaringan lokal yang di gunakan adalah 192.168.195.0/24. Tahapan berikutnya pengaturan IPv4 *Auto Assign.*

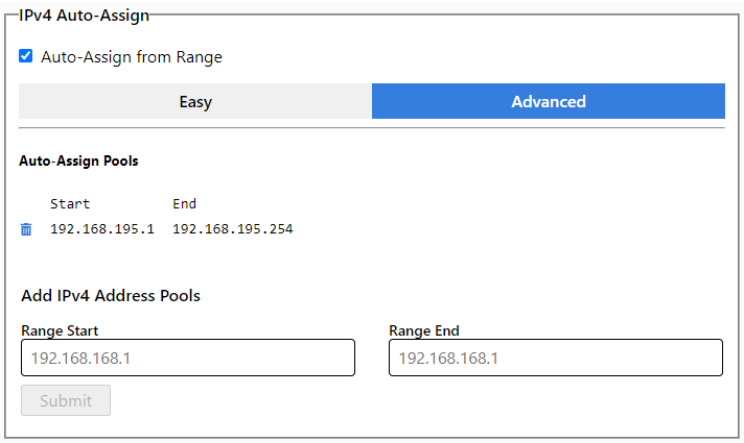

Fig.7. Pengaturan Pengalamatan IP Address Klien

Pengaturan pengalamatan secara otomatis ini di tujukan jika klien terhubung ke simpul ZeroTier maka akan mendapatkan Alamat IP Address secara otomati seperti pada gambar 7.

2. Konfigurasi ZeroTier Klien

Setelah membuat *node* pada ZeroTier tahap berikutnya adalah konfigurasi pada klien. Pada gambar 8 berikut ini adalah konfigurasi ZeroTier Klien menggunakan *smartphone*. Pengguna untuk terhubung ke simpul ZeroTier harus memasukkan kode Network ID dan *Add Network*.

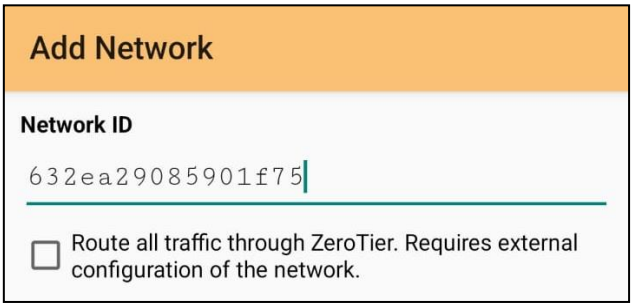

Fig.8. *Input Network* ID pada *client ZeroTier*

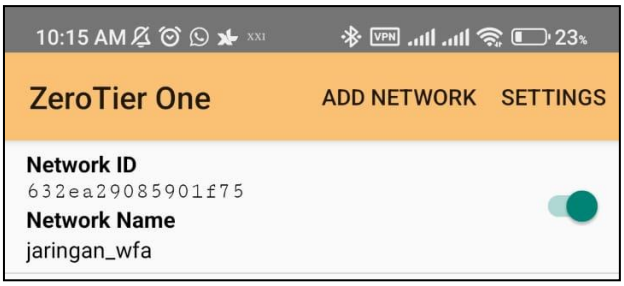

Fig.9. Terkoneksi ke Jaringan

Pada saat pertama kali pengguna terhubung ke simpul ZeroTier akan tertolak, karena Administrator belum memberikan akses. Pada gambar 10 merupakan tampilan administrator, pada bagian *Auth?* Administrator harus menceklis agar pengguna dapat terhubung.

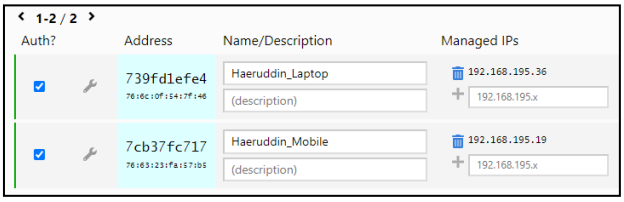

Fig.10. Memberikan hak akses ke pengguna

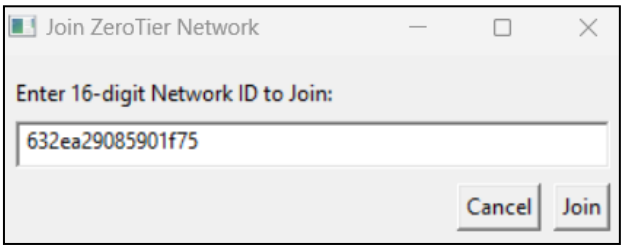

Fig.11. Terhubung ke ZeroTier pada Klien Windows

Untuk pengguna yang berbasis Windows tahapan yang dilakukan sama dengan pangguna smartphone, dengan cara membuka aplikasi ZeroTier klien, memasukkan *Network* ID jaringan yang akan digunakan, dan mendapatkan ijin dari Administrator.

```
root@ip-172-31-31-241:/home/ubuntu# zerotier-cli info
200 info f37f969b97 1.10.6 ONLINE
root@ip-172-31-31-241:/home/ubuntu# zerotier-cli join 632ea29085901f75
200 join OK
root@ip-172-31-31-241:/home/ubuntu# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
        inet 172.31.31.241  netmask 255.255.240.0  broadcast 172.31.31.255
        inet6 fe80::892:bfff:fe9c:dfdb  prefixlen 64  scopeid 0x20<link>
        ether 0a:92:bf:9c:df:db  txqueuelen 1000  (Ethernet)
        RX packets 268537  bytes 381105037 (381.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24011  bytes 17910753 (17.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

zt6ovtfd7q: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 2800
        inet 192.168.195.10  netmask 255.255.255.0  broadcast 192.168.195.255
        inet6 fe80::74ec:efff:fe13:b35  prefixlen 64  scopeid 0x20<link>
```

Fig.12. Konfigurasi ZeroTeir Klien di Ubuntu Server

Pada gambar 12 merupakan konfigurasi ZeroTier pada Ubuntu Server yang ada di AWS, sama dengan *Smarphone* atau *desktop* hanya melakukan entri *network* ID, dan persetujuan Administraor dan terhubung ke jaringan.

3.4 Pemantauan

1. Pengujian Koneksi
   Pengujian koneksi dari *host* yang terhubung di simpul ZeroTier secara keseluruhan dapat terhubung satu sama lain.

Tabel 6. Hasil tes koneksi menggunakan protokol ICMP

Source	Destination	Protokol	Status
192.168.195.10	192.168.195.11	ICMP	Berhasil
	192.168.195.12	ICMP	Berhasil
	192.168.195.13	ICMP	Berhasil
192.168.195.11	192.168.195.10	ICMP	Berhasil
	192.168.195.12	ICMP	Berhasil
	192.168.195.13	ICMP	Berhasil
192.168.195.12	192.168.195.10	ICMP	Berhasil
	192.168.195.11	ICMP	Berhasil
	192.168.195.13	ICMP	Berhasil
192.168.195.13	192.168.195.10	ICMP	Berhasil
	192.168.195.11	ICMP	Berhasil
	192.168.195.12	ICMP	Berhasil

2. Pengujian *Quality of Service*
   Dalam melakukan pengukuran *Quality of Service*, pengujian dilakukan mengirimkan data dari klien ke server melalui simpul ZeroTier di atas jaringan internet dengan menggunakan 4 parameter kapasitas *bandwaidth* mulai dari 5 Mbps, 10 Mbps, 15 Mbps, 20 Mbps, dan besar *file* yang dikirim adalah 5 Megabyte. Pada table 6 dapat di lihat hasil *packet loss*, *delay*, dan *jitter*.

Tabel 7. Hasil QoS

Bandwidth	Packet Loss	Delay	Jitter
5mb	0%	5,7ms	5,6ms
10mb	0%	5,5ms	5,4ms
15mb	0%	5,3ms	5,2ms
20mb	0%	5,4ms	7,3ms

Tabel 8. Rata-Rata Indeks Pada Hasil QoS

Bandwidth	Packet Loss	Delay	Jitter	Rata-Rata	Kategori
5mb	4	4	3	3,7	Memuaskan
10mb	4	4	3	3,7	Memuaskan
15mb	4	4	3	3,7	Memuaskan
20mb	4	4	3	3,7	Memuaskan

3. Pada tabel 8 merupakan rata-rata index QoS. Jika kita merujuk pada standar *Telecommunications and Internet Protocol Harmonization Over Networks* (TIPHON) dengan nilai *index* 3-3,79 memuasakan. Dari hasil yang didapatkan pada 8 di mana rata-rata index QoS adalah 3,7 yang berarti memuaskan.
4. Pengujian keamanan
   Pengujian keamanan menggunakan aplikasi Wireshark untuk menangkap paket pada jaringan VPN ZeroTier. Skenario pengujian dimana *user* melakukan ping ke salah satu *user* yang terkoneksi dengan simpul ZeroTier. Pada gambar 14 setelah dilakukan filter tidak ditemukan

komunikasi icmp jaringan yang menggunakan simpul ZeroTier. Hasil ini menunjukkan bahwa koneksi *end-to-end* ZeroTier aman.

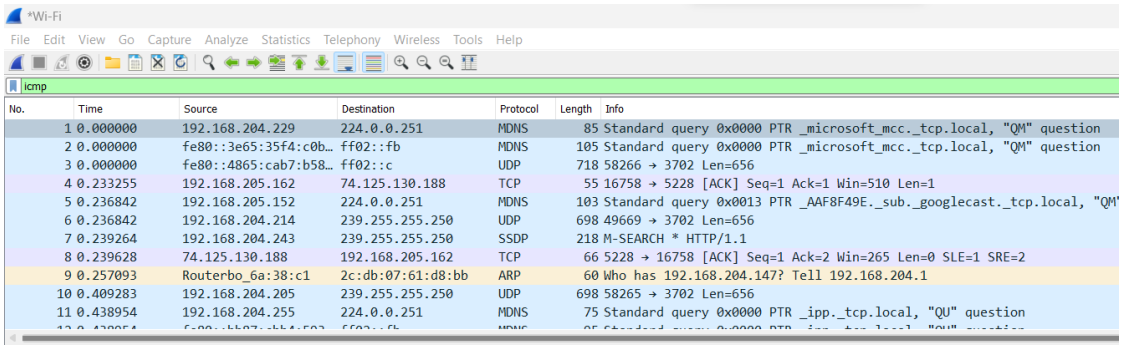

Fig.13. Hasil paket tangkapan Wireshark

5. Skalabilitas
   Pada jaringan ZeroTier dukungan jumlah klien tidak dibatasi, kecuali menggunakan simpul ZireTier yang di *hosting* oleh ZeroTier maka akan ada batasan segmen jaringan yaitu hanya mendukung 25 Network ID tanpa ada batasan pengguna. Jika ingin menggunakan lebih dari 25 *Network* ID harus menghosting secara pribadi untuk simpul ZireTier agar bebas biaya.

4. Kesimpulan

ZeroTier marupakan generasi lanjut VPN dan protocol VPN seperti OpenVPN, IPSec, PPTP, L2TP merupakan katergori Tradisional VPN. Dengan menggunakan ZeroTier maupun VPN lain merupakan solusi jaringan yang digunakan untuk mengamankan, menghubungkan, dan mengelola perangkat di berbagai lokasi yang berbeda. ZeroTier memiliki konfigurasi yang sederhana dan cepat untuk menghubungkan banyak perangkat diberbagai lokasi. Berbeda dengan tipe VPN yang lain harus memiliki keterampilan khusus untuk melakukan konfigurasi. ZeroTier menggunakan koneksi *end-to-end* sehingga ini juga bisa digunakan untuk keamanan antara perangkan dalan satu jaringan lokal yang sama. VPN tradisional menggunakan konsep Klien dan server, sehingga semua koneksi akan terpusat di server. Kemampuan server dan jumlah *bandwitdh* menentukan ketersediaan koneksi dan kecepatan jaringan. Berbeda dengan ZeroTier, kecepatan di tentukan dengan kapasitas masing masing pengguna. Karena menggunakan komunikasi end-to-end pada saat pengguna bertukar informasi atau data, Administror jaringan tidak dapat melakukan pemantauan trafik.

Daftar Pustaka

[1] N. Evika, K. Ni'mah, and W. E. Pujianto, "Efektifitas Work From Anywhere Pada Era Digital," *Jurnal Pendidikan Sosial Humaniora*, vol. 2, no. 3, pp. 18–33, 2023, doi: 10.30640/dewantara.v2i3.1305.

[2] P. (Raj) Choudhury, C. Foroughi, and B. Larson, "Work-from-anywhere: The productivity effects of geographic flexibility," *Strategic Management Journal*, vol. 42, no. 4, pp. 655–683, 2021, doi: https://doi.org/10.1002/smj.3251.

[3] I. Fronza, L. Corral, G. Iaccarino, L. Bartoli, and C. Pahl, "Work-From-Anywhere Skills: Aligning Supply and Demand Starting from High Schools," in *International Conference on Computer Supported Education, CSEDU - Proceedings*, Science and Technology Publications, Lda, 2022, pp. 327–337. doi: 10.5220/0010984300003182.

[4] D. L. Kusworo and M. N. K. Fauzi, "Work From Anywhere (WFA): Formulation of Policy Design for the Work System of State Civil Apparatus as Government Bureaucratic

Efficiency In The New Normal Era," *Pancasila and Law Review*, vol. 3, no. 2, pp. 127–136, Dec. 2022, doi: 10.25041/plr.v3i2.2769.

[5] W. Matli and S. F. Wamba, "Work from anywhere: inequalities in technology infrastructure distribution for digit workers," *Digital Transformation and Society*, vol. 2, no. 2, pp. 149–162, May 2023, doi: 10.1108/dts-08-2022-0042.

[6] G. N. Alotibi and A. Al Abdulwahid, "An Investigation of Cybersecurity Issues of Remote Work during the COVID-19 Pandemic in Saudi Arabia," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 1, pp. 47–53, 2023, doi: 10.14569/IJACSA.2023.0140106.

[7] G. Sebastian, "A descriptive study on cybersecurity challenges of working from home during COVID-19 pandemic and a proposed 8 step WFH cyber-attack mitigation plan," *IBIMA Business Review*, vol. 2021, 2021, doi: 10.5171/2021.589235.

[8] E. Kolomoets, "Ensuring information security in the field of remote work," in *Journal of Physics: Conference Series*, IOP Publishing Ltd, Mar. 2022. doi: 10.1088/1742-6596/2210/1/012008.

[9] A. Rosyidah and J. Mabe Parenreng, "Network Security Analysis Based on Internet Protocol Security Using Virtual Private Network (VPN)," vol. 03, p. 3, 2023, doi: 10.31763/iota.v3i3.613.

[10] M. A. Gunawan and S. Wardhana, "Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN (Virtual Private Network)," *Elektronika Kendali Telekomunikasi Tenaga Listrik Komputer*, vol. 6, no. 1, pp. 69–78, 2023.

[11] H. Haeruddin and K. Kelvin, "Analisa Penggunaan VPN L2TP dan SSTP di Masa Pandemi Covid-19," *Jurnal Ilmu Komputer dan Bisnis*, vol. 13, no. 1, pp. 105–114, May 2022, doi: 10.47927/jikb.v13i1.279.

[12] H. Haeruddin and E. Efendi, "Analisa Jaringan VPN MPLS L3 dan L2 Dimasa Pandemi COVID-2019 untuk Mendukung Work From Home," *Jurnal Ilmu Komputer dan Bisnis*, vol. XIII, no. 1, pp. 76–84, 2021.

[13] F. Hadinata, S. E. Prasetyo, and H. Haeruddin, "Analisa Penggunaan Jaringan ZeroTier di Masa Pandemi Covid-2019," *Jurnal Ilmu Komputer dan Bisnis*, vol. 13, no. 1, pp. 85–93, May 2022, doi: 10.47927/jikb.v13i1.276.

[14] G. Barovih, S. Surahmat, and F. Febrianty, "Analysis of Network Attached Storage Performance with NFS Protocol in Integrated Business Start-Up," *Sinkron*, vol. 8, no. 3, pp. 1299–1306, Jul. 2023, doi: 10.33395/sinkron.v8i3.12417.

[15] S. Budiyanto and D. Gunawan, "Comparative Analysis of VPN Protocols at Layer 2 Focusing on Voice over Internet Protocol," *IEEE Access*, 2023, doi: 10.1109/ACCESS.2023.3286032.