Journal of Information System and Technology, Vol. 05 No. 03, Des 2024, pp. 15-24
ISSN : 2775-0272
DOI : 10.37253/joint.v5i3.9986

Contents list available at https://journal.uib.ac.id/
JOINT
(Journal of Information System and Technology)
journal homepage: https://journal.uib.ac.id/index.php/joint/

Optimalisasi Keamanan Jaringan Di Era Digital menggunakan Metode *Zero Trust*

Haeruddin[1], Stefanus Eko Prasetyo[2], dan Ari Wahyuni Kaharuddin[3]
1,2,3 Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Internasional Batam
E-mail: haeruddin@uib.ac.id[1], stefanus@uib.ac.id[2], 2132054.ari@uib.edu[3]

Abstract

In the digital era, computer networks serve as a crucial foundation for various aspects of life, including business and education. Network security, encompassing data confidentiality, integrity, and availability, is a critical factor in protecting against cyber threats. Universitas Internasional Batam (UIB) *faces challenges such as intrusion and hacking, necessitating additional security measures. To address these challenges, the implementation of Zero Trust Network Access (ZTNA) supported by Virtual Private Network (VPN) and Multi-Factor Authentication (MFA) has become a highly relevant strategy. ZTNA ensures that every request for network access is evaluated individually, without assuming trust in any entity, thereby enhancing the necessary security layers. This study employs the Network Development Life Cycle (NDLC) method to design and develop a ZTNA network at UIB using the ZeroTier platform. The process includes network and security requirements analysis, ZTNA architecture design, implementation across various devices, and MFA integration with Google Authenticator. Monitoring and Quality of Service (QoS) testing using iPerf were also conducted to ensure the system's effectiveness. The research findings demonstrate that ZeroTier effectively facilitates direct communication with high-quality service, while the enhanced security provided by MFA makes it a reliable and secure solution for the exchange of sensitive data in the dynamic and complex environment of the university.*
***Keywords**: MFA, networking, security, VPN, zero trust, zerotier*

Abstrak

Di era digital, jaringan komputer berfungsi sebagai fondasi penting bagi berbagai aspek kehidupan, termasuk bisnis dan pendidikan. Keamanan jaringan, yang meliputi kerahasiaan, integritas, dan ketersediaan data, merupakan faktor krusial dalam melindungi terhadap ancaman siber. Universitas Internasional Batam (UIB) menghadapi tantangan seperti penyusupan dan peretasan, sehingga memerlukan langkah keamanan tambahan. Untuk mengatasi tantangan ini, penerapan *Zero Trust Network Access* (ZTNA) dengan bantuan *Virtual Private Network* (VPN) dan *Multi-Factor Authentication* (MFA) menjadi strategi yang sangat relevan. ZTNA memastikan bahwa setiap permintaan akses ke jaringan dievaluasi secara individual, tanpa mengasumsikan kepercayaan terhadap entitas mana pun, sehingga meningkatkan lapisan keamanan yang diperlukan. Penelitian ini menggunakan metode *Network Development Life Cycle* (NDLC) untuk merancang dan mengembangkan jaringan ZTNA di UIB dengan menggunakan *platform* ZeroTier. Proses ini meliputi analisis kebutuhan jaringan dan keamanan, desain struktur ZTNA, implementasi pada berbagai perangkat, dan integrasi MFA dengan Google Authenticator. Pemantauan dan pengujian *Quality of Service* (QoS) menggunakan iPerf juga dilakukan untuk memastikan efektivitas sistem. Hasil penelitian menunjukkan bahwa ZeroTier mampu efektif memfasilitasi komunikasi langsung dengan kualitas layanan tinggi, sementara peningkatan keamanan melalui MFA menjadikannya solusi yang andal dan aman untuk pertukaran data sensitif dalam lingkungan universitas yang dinamis dan kompleks.
Katakunci: jaringan, keamanan, MFA, VPN, *zero trust, zerotier*

I. PENDAHULUAN

Di era digital yang terus berkembang ini, jaringan komputer telah menjadi fondasi penting bagi hampir setiap aspek kehidupan, baik dalam dunia bisnis, pendidikan, hiburan, maupun interaksi sosial. Hampir semua aspek kehidupan kita saat ini bergantung pada konektivitas dan pertukaran data yang disediakan oleh jaringan komputer [1]. Keamanan jaringan biasanya dianggap sebagai produk dari berbagai elemen. Meskipun elemen-elemen ini dapat bervariasi tergantung pada konteks, terdapat tiga aspek utama dalam konsep keamanan jaringan: kerahasiaan, integritas, dan ketersediaan [2]. Keamanan siber dalam jaringan merupakan elemen penting yang bertujuan untuk melindungi data dan sistem dari berbagai ancaman serangan siber.

Salah satu masalah utama dalam keamanan jaringan adalah penetrasi ilegal oleh pihak yang tidak berwenang. Ini mencakup upaya peretasan yang bertujuan mencuri informasi penting atau merusak sistem [3]. Selain itu, serangan *Distributed Denial of Service* (DdoS) menjadi ancaman serius, di mana server atau jaringan dibanjiri permintaan palsu sehingga tidak dapat diakses [4]. Ancaman siber juga dapat muncul dari *malware* seperti virus, *worm*, atau *trojan horse*, yang merusak sistem dan mencuri data [5]. Sering kali, pengguna yang tidak berhati-hati atau tidak terlatih menjadi celah keamanan dengan tindakan seperti mengklik tautan atau lampiran berbahaya dalam email. Ancaman keamanan jaringan tidak hanya berasal dari luar, tetapi juga bisa timbul dari dalam jaringan sendiri, menambah kompleksitas masalah keamanan [6].

Di lingkungan Universitas Internasional Batam (UIB), keamanan jaringan menjadi aspek penting mengingat kompleksitas informasi yang ada. Pengelola jaringan di UIB sering dihadapkan pada serangkaian tantangan keamanan seperti penyusupan jaringan. Penyusup biasanya mencoba memalsukan identitas atau hak akses untuk mendapatkan akses ke sumber daya yang kemudian berpotensi merusak sistem, mencuri data sensitif, dan mengganggu operasional jaringan. Selain itu, serangan *brute force* juga kerap terjadi di area kampus. Serangan ini melibatkan upaya masuk ke sistem dengan mencoba berbagai kombinasi kata sandi atau kunci enkripsi hingga berhasil [7]. Contoh nyata dari tantangan ini adalah penyerangan terhadap situs cbt.uib.ac.id (*Computer-Based Test*/CBT), yang merupakan website untuk ujian berbasis komputer oleh mahasiswa UIB. Situs ini berhasil diretas dan diubah menjadi situs judi *online*, menyebabkan kerusakan dan gangguan yang signifikan. Insiden ini menegaskan pentingnya penerapan langkah-langkah keamanan tambahan untuk mencegah terjadinya insiden serupa di masa depan.

Pada setiap universitas, terdapat pusat data yang berfungsi sebagai tempat penyimpanan dan pengelolaan server untuk berbagai aplikasi, seperti sistem manajemen siswa, sistem informasi keuangan, sistem manajemen infrastruktur IT, dan lainnya [8]. Dengan menerapkan sistem otentikasi pada setiap server, administrator dapat menjalankan aktivitas sehari-hari mereka dengan lebih aman dan terjamin keamanannya. Penerapan sistem otentikasi yang kokoh pada setiap server juga memastikan bahwa hanya pengguna yang sah yang memiliki akses yang tepat ke data sensitif dan aplikasi penting universitas. Langkah-langkah keamanan tambahan ini menjadi kunci dalam menjaga integritas dan ketersediaan sistem informasi universitas, yang pada gilirannya mendukung kelancaran operasional dan memberikan perlindungan optimal terhadap data sensitif mahasiswa dan staf.

Salah satu pendekatan yang dapat diterapkan adalah *Zero Trust Network Access* (ZTNA), yaitu model keamanan siber yang menekankan perlindungan aset dan data dengan prinsip bahwa kepercayaan tidak dapat diberikan secara otomatis dan harus dievaluasi secara terus-menerus [9]. Infrastruktur ini bergantung pada solusi seperti *Privileged Access Management* (PAM), yang membatasi akses berwenang melalui otentikasi dan otoritas akun. Dalam ZTNA, jika seorang pengguna membutuhkan akses ke suatu server, pengguna tidak diberikan izin secara langsung melainkan harus meminta otoritas sebelum akhirnya mendapatkan persetujuan [10]. *Zero Trust* juga melibatkan beberapa tahapan untuk mengotentikasi pengguna, termasuk *Multi-Factor Authentication* (MFA) yang harus mengikuti pedoman Assurance Level 2 dari Institute Nasional Standar dan Teknologi (NIST) [11]. Mengingat kondisi akses jarak jauh yang semakin penting, baik untuk mahasiswa yang belajar dari rumah maupun staf yang bekerja secara *remote*, implementasi ZTNA di UIB menjadi semakin beralasan. Langkah ini akan membantu melindungi data sensitif dan

merespon lebih efektif terhadap ancaman serangan siber yang kompleks.

Ada beberapa metode dalam menyiapkan lingkungan *Zero Trust*, salah satunya adalah menggunakan VPN (*Virtual Private Network*) dengan MFA (*Multi-Factor Authentication*). Metode ini menambahkan lapisan keamanan ekstra dengan menggunakan enkripsi untuk data dalam transit dan mengharuskan pengguna menyediakan berbagai bentuk autentikasi. Hal ini membantu mencegah akses tidak sah ke jaringan. Metode ini sangat berguna bagi pengguna jarak jauh yang perlu mengakses sumber daya atau data sensitif di luar perimeter jaringan. Dalam menerapkan VPN dengan MFA, terdapat banyak cara dan vendor yang tersedia, seperti *platform OpenVPN*, *OpenConnect*, dan *ZeroTier* [12].

Salah satu *platform* yang unggul yaitu *ZeroTier*, perangkat lunak *open source* yang dikembangkan oleh *ZeroTier, Inc*., yang berfungsi sebagai VPN dan *Software-Define Wide Area Network* (SD-WAN) [13]. *ZeroTier* menciptakan jaringan *peer-to-peer* (P2P) terenkripsi yang menghubungkan perangkat dimanapun mereka berada [14]. Proses implementasi ZTNA dengan *ZeroTier* dimulai dengan pembuatan jaringan virtual, melibatkan instalasi dan konfigurasi perangkat lunak *ZeroTier* pada semua perangkat yang membutuhkan akses ke jaringan. Setiap perangkat yang berusaha bergabung dengan jaringan harus melewati proses otentikasi, yang didukung oleh *ZeroTier* dengan MFA, menambahkan lapisan keamanan ekstra. MFA yang digunakan untuk mendukung lingkungan *zero trust* pada *ZeroTier* yaitu dengan menggunakan *Google Authenticator*. *Google Authenticator* berperan sebagai tambahan keamanan dengan mengirim *One-Time Password* (OTP) saat server diakses [15].

[12] Dalam penelitian yang dilakukan oleh Yacob pada tahun 2023 mengeksplorasi penerapan *Zero Trust* dalam sistem berbasis *cloud* menggunakan *GitLab* yang di-*hosting* oleh *Docker*. Pendekatan ini menggabungkan kunci GPG dan *OpenID Connect* untuk autentikasi dan kontrol akses, menghasilkan lapisan keamanan yang kuat dan memastikan integritas data. Sementara itu, penelitian oleh [16] Paavo pada tahun 2020 menjelaskan prinsip kerja arsitektur *Zero Trust* dan implementasinya dalam lingkungan laboratorium virtualisasi menggunakan *ZeroTier* dan *VirtualLab*. Penelitian ini berhasil membangun jaringan simulasi yang menunjukkan kepraktisan *Zero Trust* dalam lingkungan pendidikan dan pengujian, meskipun tidak mencantumkan hasil dari keberhasilan dalam mengimplementasikan *Zero Trust*. Selain itu, penelitian oleh [17] membahas solusi keamanan VPN bagi individu yang bekerja jarak jauh menggunakan *ZeroTier*. Pengujian QoS menunjukkan hasil yang memuaskan dengan rata-rata indeks 3,7, dan penilaian keamanan menggunakan *Wireshark* mengonfirmasi keamanan koneksi *end-to-end ZeroTier*. Namun, dari penelitian sebelumnya penggunaan *platform ZeroTier* sebagai solusi untuk *Zero Trust Network* masih kurang ditemui, selain itu belum ada yang menerapkan metode VPN + MFA sebagai solusi dalam penerapan *Zero Trust Network*. Oleh karena itu, penelitian ini bertujuan untuk mengeksplorasi dan mengimplementasikan penggunaan *ZeroTier* bersama dengan MFA sebagai metode untuk memperkuat keamanan *Zero Trust Network*, serta mengevaluasi efektivitasnya dalam lingkungan jaringan yang kompleks.

II. METODE PENELITIAN

Penelitian pada studi ini melibatkan metode *Network Development Life Cycle* (NDLC). NDLC merupakan metode yang digunakan dalam pengembangan dan perancangan jaringan komputer. Metode ini mencakup serangkaian langkah sistematis dan terstruktur, mulai dari analisis kebutuhan, desain, pembuatan prototipe, implementasi, pemantauan hingga pengelolaan. Pada tahap desain akan dilakukan sebuah pemetaan apa saja yang akan dilakukan dalam implementasi *Zero Trust* dengan menggunakan *platform ZeroTier*. Setelah itu langkah yang dilakukan adalah dengan melakukan implementasi dan mengoperasikan mekanisme yang sudah dibuat.

A. Analisis

Dalam penelitian ini, analisis kebutuhan jaringan dan keamanan akan dilakukan dengan menyelidiki jenis perangkat yang digunakan di lingkungan kampus, mengevaluasi metode otentikasi yang diterapkan, serta merancang strategi enkripsi data yang sesuai untuk implementasi ZTNA menggunakan *ZeroTier*. Hal ini akan melibatkan survei mendalam terhadap infrastruktur jaringan dan perangkat yang digunakan di UIB, serta penilaian terhadap

kebutuhan keamanan yang spesifik. Selain itu, akan dilakukan evaluasi terhadap berbagai opsi otentikasi, termasuk MFA, serta pemilihan dan konfigurasi strategi enkripsi data yang sesuai dengan standar keamanan yang relevan.

B. Desain

Pada tahap desain, akan dirancang struktur umum ZTNA yang akan diimplementasikan melalui *platform ZeroTier* guna mendukung jaringan nol kepercayaan di lingkungan kampus. Meskipun berfokus pada implementasi sampel atau bagian kecil dari sistem keamanan di UIB, proses ini tetap melibatkan perencanaan struktural yang cermat. Ini menitikberatkan pada aspek-aspek kritis seperti integrasi dengan infrastruktur kampus, konfigurasi kebijakan akses, dan penyesuaian optimal dengan kebutuhan pengguna. Desain ini bertujuan menciptakan landasan yang solid untuk implementasi ZTNA yang efektif.

C. Implementasi

Pada tahap implementasi, penerapan ZTNA menggunakan *ZeroTier* sesuai dengan desain topologi sebelumnya yang akan dijalankan. Proses implementasi ini mencakup penyesuaian jaringan *ZeroTier* pada server (Linux Ubuntu Server), perangkat *mobile* (Android & iOS), laptop (Windows), dan perangkat jaringan (Mikrotik OS). Untuk meningkatkan tingkat keamanan, penerapan MFA pada *ZeroTier* akan melibatkan integrasi dengan *Google Authenticator* yang memberikan lapisan keamanan tambahan dengan memverifikasi identitas pengguna melalui metode otentikasi ganda, seperti kode penggunaan sekali atau perangkat otentikasi, memastikan bahwa akses ke jaringan *ZeroTier* hanya diberikan kepada pengguna yang sah dan terotorisasi.

D. *Monitoring*

Setelah berhasil menerapkan rancangan jaringan ZTNA dengan *ZeroTier*, langkah selanjutnya adalah melakukan pemantauan dan pengujian. Pemantauan ini meliputi pemantauan sistem keamanan untuk mendeteksi dan mencegah potensi ancaman, sementara pengujian *Quality of Service* (QoS) dilakukan untuk mengevaluasi kualitas layanan jaringan yang. QoS merupakan teknik mengukur dan mengelola kualitas jaringan dengan mengatur parameter penting seperti *throughput*, *jitter*, dan *packet loss*, agar layanan sesuai dengan standar yang diinginkan [18]. Kategori QoS ditentukan berdasarkan pengukuran *throughput*, *jitter*, dan *packet loss*, yang mengacu pada standar *Telecomunication* and *Internet Protocol Harmonization Over Network* (TIPHON) [19].

Tabel 1. *Standar Quality of Service*

Nilai	Presentase (%)	Indeks
3,8 – 4	95 – 100	Sangat Memuaskan
3 – 3,79	75 – 94,75	Memuaskan
2 – 3,79	50 – 74,75	Kurang Memuaskan
1 – 1,99	25 – 49,75	Tidak Memuaskan

Tabel 2. Standar *Throughput*

Category	*Throughput*	Indeks
Buruk	0 Mbps - 338 kbps	0
Kurang Baik	338 kbps - 700 kbps	1
Cukup Baik	700 kbps - 1200 kbps	2
Baik	1,2 Mbps – 2,1 Mbps	3
Sangat Baik	>2,1 Mbps	4

Tabel 3. Standar *Packet Loss*

Category	*Packet Loss*	Indeks
Kurang Baik	15% - 25%	1
Cukup Baik	3% - 15%	2
Baik	0% - 3%	3
Sangat Baik	0%	4

Tabel 4. Standar *Jitter*

Category	*Jitter*	Indeks
Kurang Baik	125 – 255 ms	1
Cukup Baik	75 – 125 ms	2
Baik	0 – 75 ms	3
Sangat Baik	0 ms	4

III. HASIL DAN PEMBAHASAN

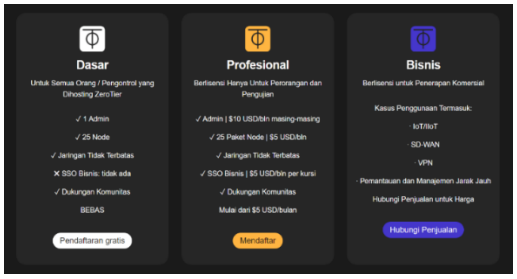
A. Analisis

Dalam skenario penerapan jaringan *Zero Trust* ini, dimulai dengan menggunakan satu server, jaringan lokal yang dilengkapi dengan router Mikrotik, dan komputer klien. Di samping itu, terdapat juga perangkat eksternal seperti

laptop dan *smartphone* yang terhubung melalui internet.

Sebelum melakukan perbaikan atau peningkatan pada sistem, memahami kondisi awal dari kinerja yang ada sangatlah penting. Hal ini mencakup pengukuran performa jaringan seperti latensi, keandalan koneksi, serta evaluasi keamanan dan kemampuan akses terhadap sumber daya.

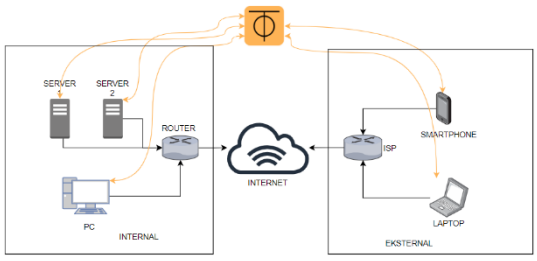
ZeroTier merupakan layanan berbasis *open source* yang terinspirasi oleh solusi seperti BeyondCorp. Sebagai perangkat lunak berbasis *open source*, *ZeroTier* tersedia secara gratis dan tidak memerlukan pembayaran lisensi jika digunakan untuk proyek non-komersial. *ZeroTier* dipilih sebagai solusi dalam bagian praktis dari penelitian ini karena kompatibel dengan berbagai perangkat dan penggunaannya dalam penelitian eksperimental tidak menghasilkan biaya tambahan. Berikut merupakan jenis-jenis lisensi yang ada pada layanan *ZeroTier*.



Gambar 1. Lisensi yang ada pada *ZeroTier*

B. Desain

Tahap selanjutnya dalam proses NDLC yaitu tahap perancangan yang akan menjadi fondasi untuk tahap selanjutnya, yaitu implementasi. Desain ini merupakan perancangan dari sistem simulasi yang akan digunakan untuk implementasi ZTNA. Topologi desain yang dimaksud sebagai berikut:



Gambar 2. Topologi Jaringan *ZeroTier*

Pada Gambar 2, terlihat semua perangkat terhubung ke node *ZeroTier*. Gambar tersebut menunjukkan perangkat dari jaringan internal dan jaringan eksternal, yang merupakan jaringan berbeda. Dengan terhubungnya setiap perangkat ke *node ZeroTier*, antar klien dapat terhubung dan berkomunikasi satu sama lain secara efektif, terlepas dari apakah mereka berada di jaringan internal atau eksternal.

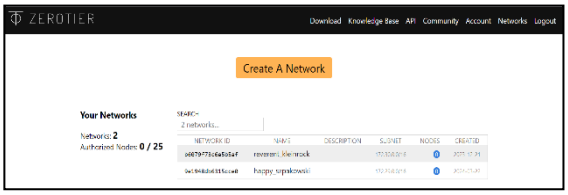
Gambar 3. *Flowchart* Koneksi SSH dengan *Google Authenticator*

Pada Gambar 3, menggambarkan proses SSH pada server. Proses SSH dengan *Google Authenticator* dimulai dengan klien melakukan koneksi SSH ke server. Klien menghubungi server melalui protokol SSH menggunakan *port* 22. Pada tahap ini, koneksi TCP/IP diinisiasi antara klien dan server. Setelah koneksi dibuat, klien dan server menjalankan protokol *Handshake* SSH untuk bertukar kunci kriptografi. Kunci publik dipertukarkan antara klien dan server, memastikan bahwa komunikasi selanjutnya bersifat terenkripsi dan aman dari penyadapan. Setelah saluran komunikasi aman dibentuk, server meminta pengguna untuk melakukan otentikasi. Pengguna diminta untuk memasukkan OTP yang dihasilkan oleh aplikasi *Google Authenticator*. Server kemudian memverifikasi OTP tersebut. Jika OTP yang dimasukkan oleh pengguna sesuai, otentikasi berhasil dan server memberikan akses kepada klien untuk memulai sesi SSH. Namun, jika OTP tidak valid, server akan menolak akses ke klien, dan proses otentikasi akan berakhir atau pengguna diminta untuk mencoba menghubungkan server kembali.

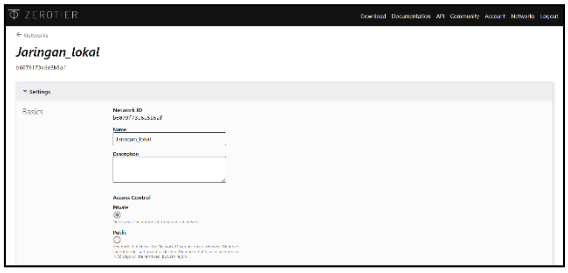
C. Implementasi

a) Konfigurasi *ZeroTier*

Langkah awal dalam implementasi *ZeroTier* yaitu mendaftar akun di *ZeroTier*. Dalam akun tersebut, pengguna dapat membuat satu atau lebih jaringan untuk digunakan oleh setiap *end-user*, sehingga mereka dapat berkomunikasi satu sama lain. Setelah berhasil masuk ke laman *ZeroTier* https://my.zerotier.com/, setelah berhasil *login* tahap berikutnya yaitu membuat jaringan seperti Gambar 4.

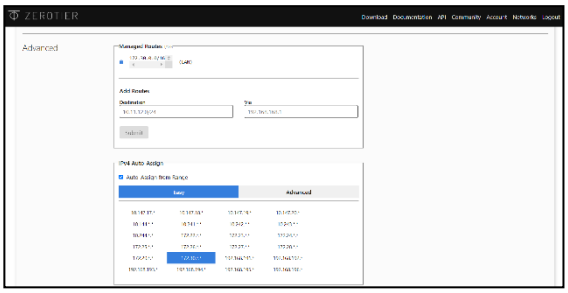


Gambar 4. *Dashbord ZeroTier*



Gambar 5. Konfigurasi Jaringan

Pada Gambar 5 dilakukan konfigurasi dasar seperti penetapan nama jaringan dan kontrol akses. Penetapan nama jaringan membantu dalam identifikasi, sedangkan kontrol akses memastikan keamanan dan pengelolaan akses pengguna ke jaringan. Di bagian pengaturan dasar juga terdapat *Network ID* yang nantinya akan didaftarkan pada setiap perangkat.

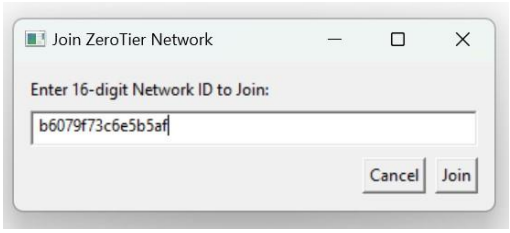


Gambar 6. Konfigurasi IP

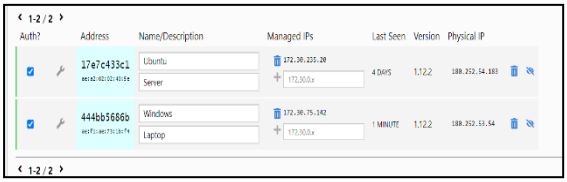
Pada Gambar 6 menggambarkan proses konfigurasi *routing* dan pengaturan *IPv4 Auto-Assign*. Pada langkah ini, jaringan lokal yang digunakan memiliki alamat 172.30.0.0/16, dan pengaturan IPv4 dilakukan dengan *mode 'easy'*. Dengan cara ini, setiap klien yang tersambung ke node *ZeroTier* akan secara otomatis mendapatkan alamat IP. Pengaturan ini bertujuan untuk mempermudah manajemen jaringan dan menjamin setiap perangkat memperoleh alamat IP tanpa perlu konfigurasi manual.

b) Penambahan Klien ke dalam *ZeroTier*

Setelah konfigurasi dasar pada *ZeroTier*, tahap berikutnya yaitu menambahkan klien dengan menggunakan *Network ID*. Pada Gambar 7, ditunjukkan proses penambahan *Network ID* menggunakan Windows. Pengguna dapat memasukkan kode *Network ID* dan mengklik *'Join'* untuk bergabung dengan jaringan *ZeroTier*.

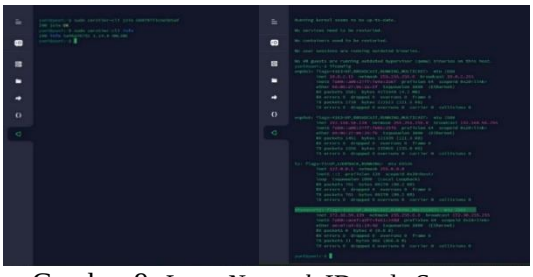


Gambar 7. *Input Network ID* pada Windows



Gambar 8. Authentikasi Klien

Setiap klien yang ditambahkan harus melakukan authentikasi untuk mendapatkan hak akses yang diberikan oleh *Administrator*. Cara melakukan authentikasi yaitu dengan mencentang bagian *'Auth'*. Pada Gambar 8, terlihat bahwa perangkat yang terdaftar telah dicentang, menandakan bahwa perangkat tersebut telah diauthentikasi dan menerima alamt IP.



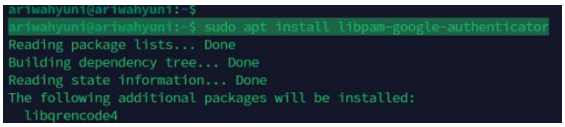
Gambar 9. *Input Network ID* pada Server

Selanjutnya adalah konfigurasi *Network ID* menggunakan server Ubuntu. Pada Gambar 9, terlihat bahwa setelah menambahkan *Network ID*, status yang diberikan adalah *'online'*. Dengan status ini, ketika memeriksa alamat IP, perangkat akan menerima IP dari *ZeroTier*. Proses ini memastikan bahwa

server Ubuntu berhasil terhubung ke jaringan *ZeroTier* dan siap berkomunikasi dengan perangkat lain yang juga terhubung ke jaringan tersebut.

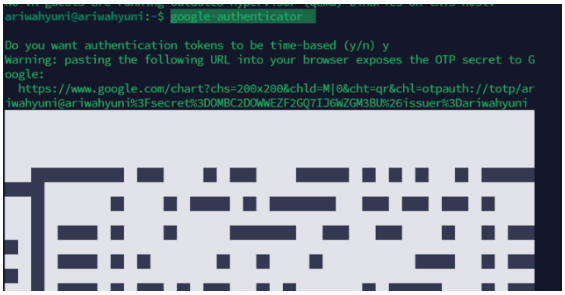
c) Penerapan *Zero Trust Network*

Setelah menambahkan klien ke dalam jaringan *ZeroTier*, tahap berikutnya adalah menerapkan konsep jaringan *Zero Trust*. Pengintegrasian jaringan *Zero Trust* ini dilakukan dengan menggunakan MFA *dari Google Authenticator* untuk meningkatkan keamanan dan memastikan bahwa hanya pengguna yang terauthentikasi dengan benar yang dapat mengakases sumber daya jaringan.



Gambar 10. *Install Google Authenticator*

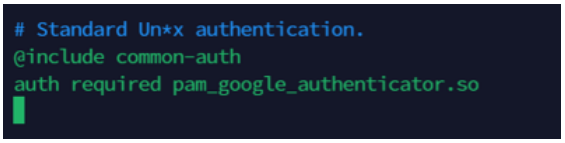
Langkah pertama dalam menerapkan jaringan *Zero Trust* yaitu dengan menginstal *Google Authenticator* pada server. Gambar 10 menunjukkan perintah yang digunakan untuk melakukan instalasi *Google Authenticator*. Perintah ini akan meng-*install* modul PAM (*Pluggable Authentication Module*) menggunalan *Google Authenticator.*



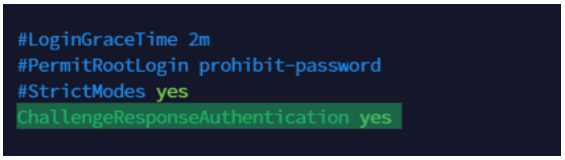
Gambar 11. Konfigurasi *Google Authenticator*

Langkah selanjutnya adalah mengkonfigurasi *Google Authenticator* pada server. Seperti yang ditunjukkan pada Gambar 11, perintah '*google-autheticator'* digunakan untuk menampilkan kode QR dan kode rahasia. Kode ini dapat dipindai oleh aplikasi *Google Authenticator* di perangkat seluler.

Langkah berikutnya adalah melakukan konfigurasi pada file '*/etc/pam.d/sshd*' seperti pada Gambar 12, dengan menambahkan baris *'auth required pam_google_authenticator.so*'. Baris ini bertujuan untuk mengaktifkan modul PAM *Google Authenticator* sebagai bagian dari proses autentikasi pada layanan SSH.



Gambar 12. Konfigurasi *File* '/etc/pam.d/sshd'



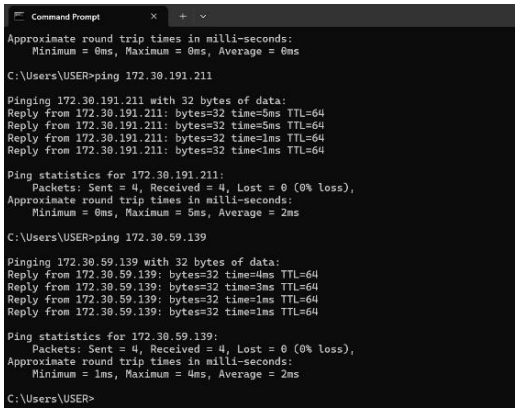
Gambar 13. Konfigurasi *File* '/etc/ssh/sshd_config'

Pada Gambar 13, dilakukan konfigursi pada *file '/etc/ssh/sshd_config'* dengan menambahkan baris '*ChallengeResponseAuthentication yes*'. Penambahan baris ini bertujuan agar server SSH meminta respon dari klien untuk autentikasi tambahan selain menggunakan kata sandi, seperti kode verifikasi (OTP) dari aplikasi *Google Athenticator.*

D. Monitoring

a) Pengujian Koneksi

Pengujian koneksi ini bertujuan untuk memastikan bahwa setiap *host* yang terhubung pada setiap *node ZeroTier* dapat saling terhubung. Pada Gambar 14, metode yang digunakan dalam pengujian ini adalah dengan menggunakan *'ping'*, di mana ICMP *Echo Request* dikirimkan ke alamat IP target.



Gambar 14. Uji Koneksi Menggunakan 'ping'

Tabel 5. Hasil Pengujian Koneksi

Source	***Destination***	***Protocol***	***Status***
172.30.59.139	172.30.191.211	ICMP	*Success*
	172.30.75.142	ICMP	*Success*
172.30.191.211	172.30.59.139	ICMP	*Success*
	172.30.75.142	ICMP	*Success*
172.30.75.142	172.30.59.139	ICMP	*Success*
	172.30.191.211	ICMP	*Success*

b) Pengujian *Quality of Service*

Dalam melakukan pengukuran kualitas layanana (*Quality of Service*), perhitungan dilakukan dengan menggunakan data berukuran 5MB, 10MB, 15MB, dan 20MB yang akan dikirimkan dari server ke klien melalui aplikasi *iPerf*. Penggunaan ukuran data yang bervariasi ini bertujuan untuk mengevaluasi kinerja jaringan dalam kondisi yang berbeda, sehingga dapat memberikan gambaran yang lebih detail. Hasil dari pengujian ini dapat dilihat pada Tabel 5 yang mencangkup *throughput, packet loss, dan jitter.*

Tabel 6. Hasil Pengujian QoS

Bandwith	***Throughput***	***Packet Loss***	***Jitter***
5MB	4,768 Mbps	0%	0,209 ms
10MB	9,52 Mbps	0%	0,069 ms
15MB	14,32 Mbps	0%	0,144 ms
20MB	19,04 Mbps	0%	0,071 ms

Tabel 7. Hasil Indeks QoS

Bandwith	***Throughput***	***Packet Loss***	***Jitter***	***Rata-rata***	***Kategori***
5MB	4	4	4	4	Sangat Baik
10MB	4	4	4	4	Sangat Baik
15MB	4	4	4	4	Sangat Baik
20MB	4	4	4	4	Sangat Baik

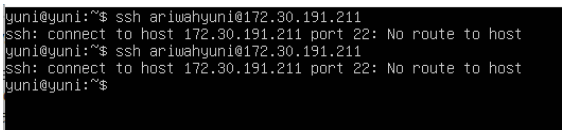
Berdasarkan Tabel 7, dan standar dari *Telecommunication and Internet Protocol Harmonization Over Network* (TIPHON), hasil pengujian menunjukkan bahwa indeks rata-rata untuk *Throughput, Packet Loss,* dan *Jitter* mencapai angka 4, yang termasuk dalam kategori sangat baik. Hasil ini menunjukkan bahwa performa jaringan yang diuji memiliki kualitas yang sangat tinggi, memenuhi standar yang ditetapkan untuk koneksi telekomunikasi dan internet. Indeks ini mencerminkan kemampuan jaringan dalam mempertahankan kualitas layanan yang optimal, dengan tingkat kehilangan paket dan *jitter* yang minimal, serta *throughput* yang stabil.

c) Pengujian Keamanan SSH

Pada pengujian kali ini, akan dilakukan pengujian dengan melakukan SSH pada setiap server. Pengujian ini akan terbagi menjadi dua IP, di mana satu IP merupakan anggota dari jaringan *ZeroTier* dan yang lainnya bukan anggota jaringan *ZeroTier*. Kedua IP ini akan melakukan SSH ke server yang merupakan anggota dari jaringan *ZeroTier*. Dalam percobaan ini, kedua IP yang akan diuji sudah mengetahui kode OTP yang akan dikirimkan oleh *Google Authenticator*. Tujuan pengujian ini adalah untuk mengetahui apakah IP yang bukan anggota dari jaringan *ZeroTier* dapat melakukan SSH dan masuk ke dalam server meski sudah mengetahui kode OTP.

Gambar 15. SSH ke Sesama Jaringan *ZeroTier*

Pada Gambar 15, dapat dilihat bahwa IP yang merupakan anggota dari jaringan *ZeroTier*, yaitu 172.30.59.139, dapat melakukan SSH dan masuk ke dalam server dengan menggunakan kode OTP yang dikirimkan oleh *Google Authenticator*. Hasil ini menunjukkan bahwa anggota jaringan *ZeroTier* memiliki akses yang berhasil ke server melalui metode autentikasi yang aman, sesuai dengan pengujian yang telah direncanakan. Hal ini mengonfirmasi bahwa konfigurasi jaringan dan mekanisme autentikasi berfungsi dengan baik.



Gambar 16. SSH ke Berbeda Jaringan *ZeroTier*

Sementara itu, pada Gambar 16. dapat dilihat bahwa IP yang bukan merupakan anggota dari jaringan *ZeroTier*, yaitu 192.168.56.134, tidak dapat melakukan SSH. *Output* yang dihasilkan menunjukkan pesan *'No route to host'*, yang berarti tidak ada jalur untuk mencapai *host* tersebut. Hal ini menunjukkan bahwa IP yang bukan anggota dari jaringan *ZeroTier* tidak memiliki akses untuk melakukan SSH ke server, sesuai dengan pengujian yang direncanakan.

IV. KESIMPULAN

Hasil penelitian mengenai jaringan *ZeroTier* menegaskan kemampuannya dalam memfasilitasi komunikasi langsung antara pengguna yang terhubung dalam jaringan yang sama. Evaluasi *Quality of Service* menunjukkan bahwa jaringan ini mampu memberikan kualitas layanan yang tinggi, dengan indeks rata-rata mencapai angka 4. Ini menandakan kemampuan jaringan *ZeroTier* dalam menangani lalu lintas data dengan baik, tanpa gangguan atau jeda yang signifikan. Selain itu, langkah-langkah keamanan, seperti penggunaan *Multi-Factor Authentication* (MFA), memberikan tambahan perlindungan terhadap akses yang tidak sah atau penyalahgunaan klien yang melakukan *remote*, seperti SSH. Dengan demikian, jaringan *ZeroTier* dapat dianggap sebagai solusi yang andal dan aman untuk keperluan komunikasi dan pertukaran data, dengan peningkatan keamanan yang signifikan melalui MFA.

V. DAFTAR PUSTAKA

[1] N. A. Santoso, K. B. Affandi, and R. D. Kurniawan, "Implementasi Keamanan Jaringan Menggunakan Port Knocking," *Jurnal Janitra Informatika dan Sistem Informasi*, vol. 2, no. 2, pp. 90–95, Oct. 2022, doi: 10.25008/janitra.v2i2.156.

[2] F. Novianto, "Evaluasi keamanan informasi E-Government menggunakan model defense in depth," *Cyber Security dan Forensik Digital*, vol. 3, no. 1, pp. 14–19, 2020.

[3] V. T. Aditya, "Manajemen Ancaman dan Keamanan Jaringan melalui Penggunaan Firewall dengan Mikrotik pada PT Dinamika Mediakom," 2023. [Online]. Available: dspace.uii.ac.id/123456789/48937

[4] S. Wani, M. Imthiyas, H. Almohamedh, K. M. Alhamed, S. Almotairi, and Y. Gulzar, "Distributed denial of service (Ddos) mitigation using blockchain—a comprehensive insight," Feb. 01, 2021, *MDPI AG*. doi: 10.3390/sym13020227.

[5] W. Qiang, L. Yang, and H. Jin, "Efficient and Robust Malware Detection Based on Control Flow Traces Using Deep Neural Networks," *Comput Secur*, vol. 122, p. 102871, Nov. 2022, doi: 10.1016/j.cose.2022.102871.

[6] K. S. Robbani and A. H. Reksoprodjo, "Perlindungan infrastruktur informasi kritikal nasional sektor ketenagalistrikan

dari ancaman siber critical national information infrastructure protection on electricity sector from cyber threats," 2020. doi: https://doi.org/10.33172/pa.v6i1.531.

[7] Y. Mulyanto and A. Algi Fari, "Analisis keamanan login router mikrotik dari serangan bruteforce menggunakan metode penetration testing (Studi Kasus: SMK Negeri 2 Sumbawa)," *Jurnal Informatika, Teknologi dan Sains*, vol. 4, no. 3, pp. 145–155, Aug. 2022, doi: 10.51401/jinteks.v4i3.1897.

[8] W. Yustika, N. Tusa, diah Siregar, V. Aprinilova Barus, M. Abiyyu Alwansyah Hasibuan, and J. Manajemen, "SURPLUS : JURNAL EKONOMI DAN BISNIS Peranan Sistem Database Di Dalam Sistem Informasi Manajemen Pada UINSU (Universitas Islam Negeri Sumatera Utara)," *SURPLUS : JURNAL EKONOMIDANBISNIS*, vol. 1, no. 2, pp. 188–196, 2023.

[9] A. Wylde, "Zero trust: Never trust, always verify," in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, IEEE, Jun. 2021, pp. 1–4. doi: 10.1109/CyberSA52016.2021.9478244.

[10] D. D'Silva and D. D. Ambawade, "Building A Zero Trust Architecture Using Kubernetes," in *2021 6th International Conference for Convergence in Technology, I2CT 2021*, Institute of Electrical and Electronics Engineers Inc., Apr. 2021. doi: 10.1109/I2CT51068.2021.9418203.

[11] L. Miller and T. George, *Zero Trust Privilege For Dummies*, Special Edition. Hoboken: John Wiley & Sons, Inc, 2019.

[12] T. Yacob, "Säkra känslig data i molnet: En ny era av säkerhet med Zero Trust principer Securing Sensitive Data in the Cloud: A New Era of Security Through Zero Trust Principles," 2023.

[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] J. Piispanen, "Evaluation report on integration demonstration Document Identification Dissemination Level PU Lead Participant JAMK Lead Author Contributing Beneficiaries Related Deliverables," 2019.

[15] M. Taifur and I. Akhand, "Development of a Multilevel Authentication System for Data Center Administration," 2019.

[16] T. Paavo, "Zero Trust-arkkitehtuuri Opinnäytetyö Tieto-ja viestintätekniikka 2020," 2020.

[17] H. Haeruddin, G. Wijaya, and H. Khatimah, "Sistem keamanan work from anywhere menggunakan VPN generasi lanjut," *JITU : Journal Informatic Technology And Communication*, vol. 7, no. 2, pp. 102–113, Nov. 2023, doi: 10.36596/jitu.v7i2.1086.

[18] M. Sadar and W. Syafitri, "Guntoro, Evaluasi Performance Jaringan Internet Kampus Menggunakan Quality Of Service (QoS) EVALUASI PERFORMANCE JARINGAN INTERNET KAMPUS MENGGUNAKAN QUALITY OF SERVICE (QOS)," *SEMASTER: Seminar Nasional Teknologi Informasi & Ilmu Komputer*, vol. 1, no. 1, pp. 280–290, 2020, doi: https://doi.org/10.31849/semaster.v1i1.6139.

[19] 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.