Jurnal Komputer, Informasi dan Teknologi Vol: 5, No 2, 2025, Page: 1-15

Optimasi Keamanan Jaringan dengan Metode Sentralisasi Koneksi VPN Berbasis Zerotier pada Industri Soho

Nasrullah Syamil Salahudin[1]*, Yuma Akbar[2]

Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika

*Correspondence: Nasrullah Syamil Salahudin
Emaill: shalahudin2762@gmail.com

Received: 05-10-2025
Accepted: 15-11-2025
Published: 28-12-2025

Abstract: *Network security plays a crucial role in supporting productivity and ensuring operational continuity within Small Office/Home Office (SOHO) environments. However, limitations in infrastructure and technical resources often hinder the implementation of reliable and efficient security solutions. This study aims to optimize network security through a centralized VPN connection approach using ZeroTier technology. ZeroTier is a peer-to-peer-based virtual network solution that supports end-to-end encryption using the AES-256-GCM protocol and public key authentication based on Curve25519. It enables secure connections between computers within a virtual local network, even if they are physically located in different places. This research employs an experimental methodology by comparing two scenarios: a SOHO network without VPN and a SOHO network with centralized VPN connectivity using ZeroTier. The evaluation focuses on security parameters (encryption, authentication, and secure routing), network performance (latency and throughput), and ease of implementation. The results show that implementing ZeroTier significantly enhances data communication security without requiring additional physical infrastructure. Furthermore, the centralized connection scheme offers centralized traffic control, simplifies access management, and reduces potential vulnerabilities from uncontrolled peer-to-peer connections. In conclusion, the application of centralized VPN connections using ZeroTier proves effective in optimizing network security for SOHO environments through a lightweight, efficient, and easy-to-implement approach.*

Keywords: *SOHO; Zerotier; VPN; Centralized Connection; Peer-To-Peer Network*

Pendahuluan

Digitalisasi yang masif telah mendorong sektor usaha, termasuk Small Office/Home Office (SOHO), untuk mengadopsi model kerja yang lebih fleksibel dan terdistribusi. Fenomena ini menciptakan urgensi akan infrastruktur jaringan yang aman, efisien, dan fleksibel guna mendukung mobilitas, kolaborasi, dan pertukaran data antar lokasi kerja (Kurniawan & Santoso, 2023; Pramono et al., 2024). Namun, seringkali jaringan publik menjadi pilihan karena kemudahan dan biaya yang terjangkau. Sayangnya, penggunaan jaringan publik tanpa perlindungan memunculkan celah keamanan yang signifikan, khususnya terkait dengan privasi dan integritas data, yang dapat memicu risiko serangan siber (Rizky et al., 2023; Simanungkalit & Rahadian, 2022).

Sebagai respons terhadap tantangan ini, Virtual Private Network (VPN) telah menjadi solusi standar untuk membangun koneksi privat di atas jaringan publik. Namun, implementasi VPN tradisional seringkali menghadapi kendala teknis dan biaya, terutama bagi pelaku usaha SOHO yang memiliki keterbatasan sumber daya. Konfigurasi yang

kompleks, kebutuhan perangkat keras khusus, serta biaya implementasi dan pemeliharaan yang tinggi seringkali menjadi hambatan (Suhadi & Arifin, 2024). Sementara itu, model koneksi *peer-to-peer* yang sering ditawarkan oleh solusi modern, meskipun fleksibel, belum banyak dikembangkan untuk arsitektur yang terpusat, yang sebenarnya lebih diperlukan untuk kontrol administratif yang kuat.

Permasalahan Penelitian

Fokus utama masalah yang dihadapi oleh sektor SOHO adalah ketidakmampuan untuk membangun dan mengelola sistem jaringan terpusat yang aman. Metode VPN konvensional dianggap tidak ekonomis dan terlalu rumit, sementara model koneksi yang tidak terpusat, seperti yang umum pada implementasi *peer-to-peer*, memperbesar risiko keamanan karena tidak adanya kontrol lalu lintas terpusat (Pratama & Marcus, 2025; Wijaya & Gunawan, 2024). Kurangnya mekanisme kontrol administratif yang kuat membuat entitas SOHO rentan terhadap ancaman siber seperti serangan Man in The Middle (MiTM) dan akses ilegal. Celah ini menyoroti adanya kebutuhan akan solusi jaringan yang tidak hanya mudah diimplementasikan dan hemat biaya, tetapi juga menawarkan kontrol keamanan terpusat yang sebanding dengan solusi kelas enterprise tanpa kerumitan yang menyertainya.

Penelitian akademis dalam area ini masih sangat terbatas. Sebagian besar studi tentang teknologi jaringan *overlay* seperti **ZeroTier** cenderung berfokus pada efektivitas koneksi *peer-to-peer* untuk akses *remote*, tanpa mengeksplorasi potensi implementasi arsitektur sentralisasi koneksi. Sebagai contoh, Pratama dan Marcus (2025) hanya menggunakan ZeroTier untuk koneksi antar cabang, dan tidak menerapkan konsep kontrol jaringan terpusat melalui satu *node* administratif. Dengan demikian, terdapat ***research gap*** yang signifikan dalam literatur yang membahas bagaimana teknologi jaringan *overlay* dapat diadaptasi untuk memenuhi kebutuhan kontrol sentral pada lingkungan SOHO yang sensitif terhadap biaya dan kompleksitas.

Tujuan, Urgensi, dan Kebaruan Penelitian

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk merancang dan mengimplementasikan koneksi VPN berbasis ZeroTier secara terpusat pada jaringan SOHO. Tujuannya adalah untuk meningkatkan keamanan jaringan melalui satu titik kontrol (gateway), serta mengevaluasi efektivitas metode ini dalam hal performa dan keamanan dibandingkan VPN konvensional. Urgensi penelitian ini terletak pada upaya menyediakan solusi alternatif yang ringan dan efisien bagi pelaku usaha kecil untuk mengamankan jaringan mereka di tengah tantangan digitalisasi. Kebaruan (novelty) penelitian ini terletak pada penggabungan prinsip arsitektur koneksi terpusat—yang lazimnya ditemukan pada teknologi *enterprise* seperti SD-WAN—dengan fleksibilitas dan kemudahan implementasi ZeroTier. Penelitian ini tidak hanya mengonfirmasi kelayakan penggunaan ZeroTier untuk koneksi *peer-to-peer*, tetapi juga membuka wawasan baru tentang bagaimana teknologi ini dapat dioptimalkan sebagai sistem koneksi VPN terpusat, mengisi celah penelitian yasng ada dan memberikan kontribusi nyata dalam bidang keamanan jaringan terdistribusi untuk sektor SOHO.

Metode Penelitian

Metode penelitian yang digunakan dalam studi ini adalah pendekatan eksperimental dengan fokus pada rekayasa dan pengujian sistem. Pendekatan ini dipilih untuk mengeksplorasi secara praktis implementasi dan efektivitas metode sentralisasi koneksi VPN menggunakan platform ZeroTier dalam lingkungan Small Office/Home Office (SOHO). Sesuai dengan metodologi eksperimental, penelitian ini dirancang untuk menguji hipotesis bahwa sentralisasi koneksi ZeroTier dapat meningkatkan keamanan dan manajemen jaringan (Creswell & Creswell, 2022). Pendekatan ini memungkinkan perancang untuk secara langsung mengamati dampak dari variabel independen (desain sentralisasi koneksi) terhadap variabel dependen (keamanan dan efektivitas jaringan).

Jenis dan Desain Penelitian

Penelitian ini menggunakan desain *Applied Research* dengan pendekatan kualitatif, di mana fokus utamanya adalah memecahkan masalah praktis yang dihadapi oleh pengguna jaringan SOHO (Sugiyono, 2021). Desain penelitian ini meliputi serangkaian tahapan yang terstruktur, mulai dari studi literatur, analisis kebutuhan, perancangan sistem, implementasi, hingga evaluasi. Desain ini bertujuan untuk menciptakan solusi nyata yang dapat diterapkan dan divalidasi, tidak hanya berfokus pada pengembangan teori. Desain ini memungkinkan adaptasi dan penyesuaian pada setiap tahapan, memastikan bahwa solusi yang dihasilkan relevan dengan tantangan praktis yang ada di lapangan (Sudaryono, 2023).

Instrumen dan Teknik Analisis Data

Data penelitian ini dikumpulkan melalui dua cara utama: studi literatur dan eksperimen langsung (Emzir, 2021). Studi literatur dilakukan dengan mengkaji jurnal ilmiah, dokumentasi teknis, dan laporan penelitian sebelumnya untuk membangun kerangka konseptual yang kuat. Data eksperimen diperoleh dari pengujian implementasi sistem pada perangkat fisik, dengan fokus pada parameter konektivitas, performa, dan keamanan. Instrumen pengujian yang digunakan meliputi perangkat lunak Wireshark untuk memantau lalu lintas data, *ping test* untuk mengukur latensi, dan fitur *dashboard* ZeroTier Central untuk memverifikasi otorisasi serta alur koneksi. Analisis data dilakukan secara deskriptif untuk menjelaskan hasil pengujian dan secara komparatif untuk membandingkan performa sistem sentralisasi dengan model koneksi *peer-to-peer* yang biasa digunakan.

Populasi dan Sampel

Populasi dalam penelitian ini adalah seluruh sistem jaringan SOHO yang menghadapi tantangan dalam manajemen dan keamanan koneksi. Sampel penelitian ini terdiri dari satu sistem jaringan SOHO simulasi yang dibangun dengan perangkat fisik, mencakup satu *node* VPN Gateway, satu server internal, dan dua *client* (PC/laptop dan *smartphone*). Penggunaan perangkat fisik ini bertujuan untuk mereplikasi skenario penggunaan nyata dan memastikan validitas hasil pengujian. Dengan menguji pada sampel yang representatif, hasil yang diperoleh diharapkan dapat digeneralisasi pada skala jaringan SOHO yang lebih luas (Sugiyono, 2021).

Prosedur Penelitian

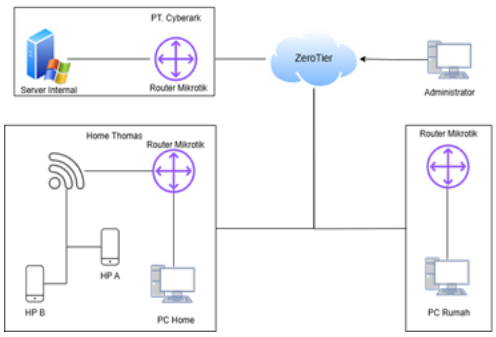
Prosedur penelitian ini mengikuti alur sistematis yang dirancang untuk memastikan validitas dan reliabilitas hasil. Tahapan-tahapan tersebut adalah sebagai berikut:

1. Studi Literatur: Mengumpulkan dan menelaah referensi terkait teknologi VPN, jaringan terpusat, dan ZeroTier untuk membangun dasar konseptual dan teknis. Tahap ini juga mencakup identifikasi *research gap* yang menjadi fokus penelitian ini.
2. Analisis Kebutuhan: Mengidentifikasi kebutuhan perangkat keras (PC/laptop, server, *gateway*), perangkat lunak (ZeroTier, Wireshark), dan fungsional sistem yang diperlukan untuk implementasi. Analisis ini memastikan bahwa rancangan sistem dapat memenuhi tujuan penelitian (Pratama & Marcus, 2025).
3. Perancangan Sistem: Merancang topologi jaringan logis dengan arsitektur sentralisasi, skema *IP addressing* virtual, dan kebijakan otorisasi pada ZeroTier Central.
4. Implementasi: Melakukan instalasi aplikasi ZeroTier pada semua perangkat, mengonfigurasi *IP forwarding* dan *routing* statis pada *gateway*, dan memverifikasi bahwa seluruh perangkat terhubung melalui jalur yang ditentukan. Tahap ini juga mencakup verifikasi bahwa koneksi *peer-to-peer* antar *client* dibatasi secara efektif (Suhadi & Arifin, 2024).
5. Monitoring: Mengamati lalu lintas data menggunakan Wireshark dan *dashboard* ZeroTier untuk memastikan bahwa koneksi berjalan sesuai dengan topologi yang dirancang dan tidak ada kebocoran data.
6. Evaluasi: Menguji performa sistem (latensi, *throughput*) dan keamanan (pembatasan koneksi antar *client*) untuk memvalidasi efektivitas metode sentralisasi.

Hasil dan Pembahasan

Topologi dan Alokasi IP Address

Agar mempermudah proses implementasi, berikut topologi dan pengujian jaringan sistem ini mengimplementasikan koneksi jaringan hybrid dengan ZeroTier pada perangkat nyata ini terdiri dari 1 node Server Internal – Web Server (PT Cyberark) yang terhubung melalui ZeroTier. Lalu terdapat 1 node router Home Thomas yang berfungsi sebagai gateway lokal, di dalamnya terdapat 2 node klien (HP A dan HP B) serta 1 node PC Rumah. Selain itu, terdapat 1 node Administrator yang terhubung melalui ZeroTier. Sistem ini dibangun menggunakan perangkat fisik untuk menguji koneksi jaringan secara real-time. Berikut topologi yang akan digunakan pada penelitian ini :



Gambar 1. Topologi Jaringan

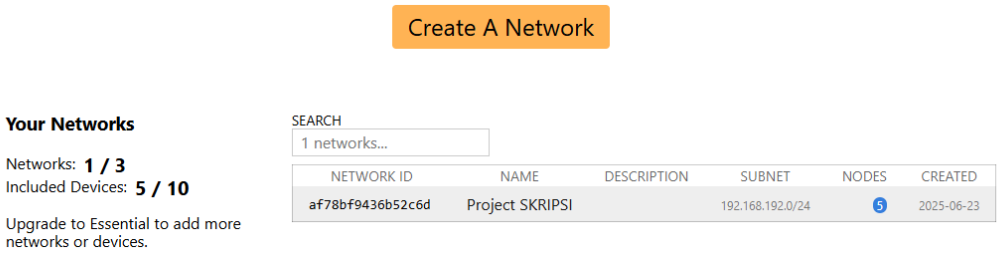
Dan berikut detail Alokasi IP Address yang akan digunakan pada pengujian ini:

Tabel 1. Alokasi IP Address

Nama Perangkat	Interface	IP Address
Router	zerotier	172.26.101.123/16
PC Rumah	Eth2	10.10.1.1/24
Router Home Thomas	zerotier	172.26.184.103/16
	Eth4	172.20.0.1/24
Router PT. Cyberark	zerotier	172.26.57.28/16
	Eth1	172.16.5.2/29
Web Server	e0	172.23.1.172

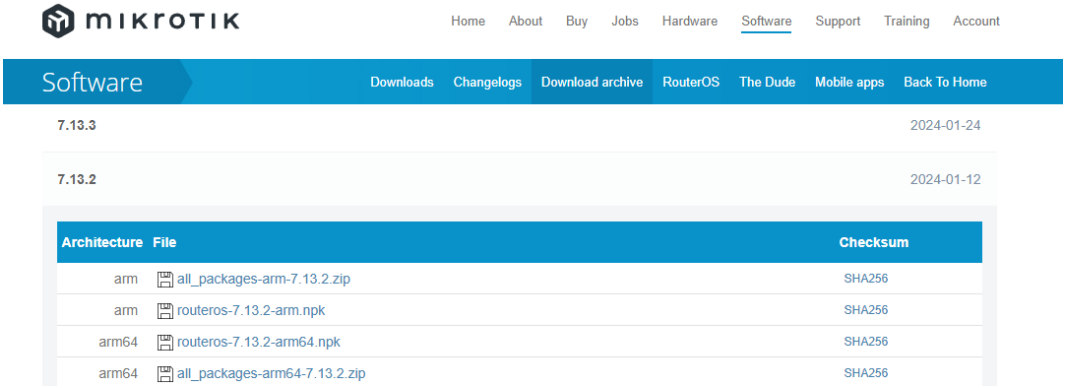
Langkah Setup Zerotier di Mikrotik

Sebelum melakukan pengujian *Sentralisasi* koneksi VPN, kita harus mengkonfigurasi mendaftar/resigter pada web https://www.zerotier.com/ sebagai *Sentralisasi* koneksi VPN dalam topologi jaringan ini. Hal ini dilakukan agar saat dilakukannya pengujian, client dapat mendapatkan akses ke *internet*. Berikut langkah-langkah setup ZeroTier pada Mikrotik :



Gambar 2. Create A Network

Registrasi my.zerotier.com dan Create A Network, contohnya af78bf9436b52c6d.

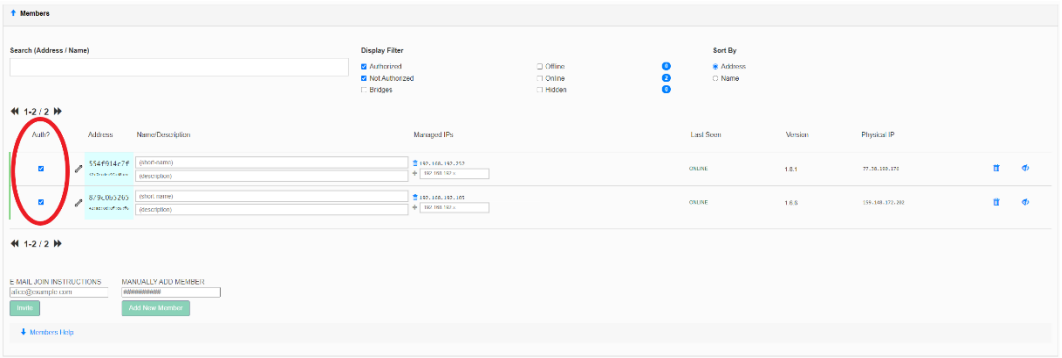


Gambar 3. Software package

Download and install ZeroTier npk package in RouterOS, terdapat pada extra package.Upload package tersebut pada Mikrotik dan Reboot perangkat.

Konfigurasi Enable Zerotier :
[admin@RB-Home Santech] > zerotier/enable zt1
Konfigurasi Network ID:
[admin@RB-HomeSantech]>zerotier/interface/add network=e4da7455b2b554d9 instance=zt1
Verifikasi konfiguasi ZeroTier :
[admin@RB-Home Santech] > zerotier/interface/print
Flags: R - RUNNING
Columns: NAME, MAC-ADDRESS, NETWORK, NETWORK-NAME, STATUS
NAME MAC-ADDRESS NETWORK NETWORK-NAME STATUS
0 zerotier1 DA:36:1B:20:0C:CA e4da7455b2b554d9 REQUESTING_CONFIGURATION

Setelah melakukan konfigurasi dari sisi Mikrotik, kita harus menkonfirmasi device perangkat yang sudah "Join Network ID" pada web Zerotier. Kita juga bisa mencoba perangakat lain untuk install zerotier client dengan memasukan Network ID dari ZeroTier. Pada tampilan zerotier perlu authorize perangkat sebelum join member ZeroTier untuk antisipasi perangkat lain masuk dalam member.



Gambar 4. Authorize Device pada Zerotier

Verifikasi koneksi ZeroTier :

[[admin@RB-Home Santech] > ip/address/print where interface

~"zero"

Flags: D - DYNAMIC

Columns: ADDRESS, NETWORK, INTERFACE

```
# ADDRESS          NETWORK      INTERFACE
0 D 172.26.101.123/16  172.26.0.0  zerotier1
```

Verifikasi jika Router Administrator sudah bisa terkoneksi ke Router Home Thomas dan Router PT.Cyberark. Untuk verifikasi kita bisa command ping ke ip yang sudah didapat dari ZeroTier

```
[admin@RB-Home Santech] > ping 172.26.184.103
  SEQ HOST                                     SIZE TTL TIME       STATUS
    0 172.26.184.103                             56  64 82ms686us
    1 172.26.184.103                             56  64 7ms81us
    2 172.26.184.103                             56  64 7ms216us
    3 172.26.184.103                             56  64 7ms495us
    4 172.26.184.103                             56  64 7ms49us
    5 172.26.184.103                             56  64 6ms805us
    6 172.26.184.103                             56  64 8ms228us
    7 172.26.184.103                             56  64 7ms87us
    8 172.26.184.103                             56  64 7ms391us
    9 172.26.184.103                             56  64 7ms479us
   10 172.26.184.103                             56  64 7ms476us
    sent=11 received=11 packet-loss=0% min-rtt=6ms805us avg-rtt=14ms181us
   max-rtt=82ms686us
```

Gambar 5. Koneksi RO Rumah – RO Home Thomas

```
[admin@RB-Home Santech] > ping 172.26.57.28
  SEQ HOST                                     SIZE TTL TIME       STATUS
    0 172.26.57.28                               56  64 17ms738us
    1 172.26.57.28                               56  64 17ms924us
    2 172.26.57.28                               56  64 17ms322us
    3 172.26.57.28                               56  64 18ms357us
    4 172.26.57.28                               56  64 18ms586us
    5 172.26.57.28                               56  64 18ms861us
    6 172.26.57.28                               56  64 18ms623us
    7 172.26.57.28                               56  64 17ms364us
    8 172.26.57.28                               56  64 18ms768us
    9 172.26.57.28                               56  64 18ms404us
   10 172.26.57.28                               56  64 18ms445us
   11 172.26.57.28                               56  64 17ms852us
   12 172.26.57.28                               56  64 17ms351us
   13 172.26.57.28                               56  64 17ms483us
   14 172.26.57.28                               56  64 18ms827us
   15 172.26.57.28                               56  64 17ms714us
   16 172.26.57.28                               56  64 18ms37us
   17 172.26.57.28                               56  64 17ms707us
   18 172.26.57.28                               56  64 17ms754us
   19 172.26.57.28                               56  64 17ms831us
    sent=20 received=20 packet-loss=0% min-rtt=17ms322us avg-rtt=18ms47us
   max-rtt=18ms861us
```

Gambar 6. Koneksi RO Rumah - RO PT.Cyberark

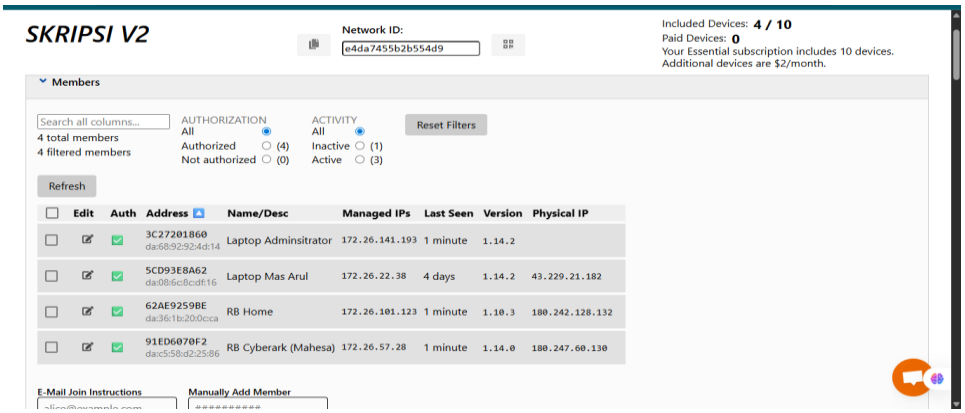
Hasil Akhir Pengujian

Setelah melakukan tahapan implementasi, bagian ini dilakukan pengujian terhadap fungsi utama sistem yang telah dirancang, yaitu sentralisasi koneksi VPN serta konektivitas antar end device. Pengujian bertujuan untuk memverifikasi keberhasilan implementasi solusi dan mengevaluasi performanya dalam skenario jaringan SOHO.

Pengujian fungsi Sentralisasi VPN

Pengujian ini bertujuan untuk memverifikasi apakah koneksi antar perangkat dalam jaringan VPN benar-benar tersentralisasi melalui controller ZeroTier. Pengamatan dilakukan dengan memantau rute lalu lintas data dan memastikan bahwa semua koneksi tidak terjadi secara langsung antar perangkat, melainkan diarahkan terlebih dahulu ke node pusat.

1. **Sentralisasi koneksi VPN pada ZeroTier Server**



Gambar 7 Sentraliasi VPN pada ZeroTier

2. **Test koneksi environment yang telah menjadi member dari network ZeroTier**

```
[admin@RB-Home Santech] > ping 172.26.184.103
  SEQ HOST                                     SIZE TTL TIME       STATUS
    0 172.26.184.103                             56  64 82ms686us
    1 172.26.184.103                             56  64 7ms81us
    2 172.26.184.103                             56  64 7ms216us
    3 172.26.184.103                             56  64 7ms495us
    4 172.26.184.103                             56  64 7ms49us
    5 172.26.184.103                             56  64 6ms805us
    6 172.26.184.103                             56  64 8ms228us
    7 172.26.184.103                             56  64 7ms87us
    8 172.26.184.103                             56  64 7ms391us
    9 172.26.184.103                             56  64 7ms479us
   10 172.26.184.103                             56  64 7ms476us
    sent=11 received=11 packet-loss=0% min-rtt=6ms805us avg-rtt=14ms181us
   max-rtt=82ms686us
```

Gambar 8 Koneksi RO Rumah - RO Thomas

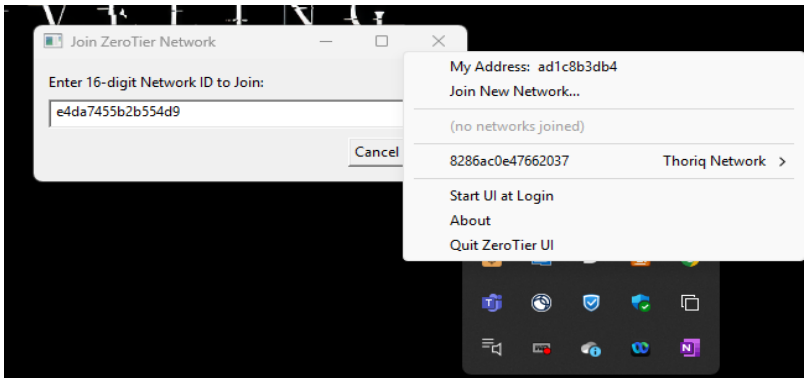
```
[admin@RB-Home Santech] > ping 172.26.57.28
  SEQ HOST                                     SIZE TTL TIME       STATUS
    0 172.26.57.28                               56  64 368ms402us
    1 172.26.57.28                               56  64 378ms399us
    2 172.26.57.28                               56  64 369ms110us
    3 172.26.57.28                               56  64 367ms408us
    4 172.26.57.28                               56  64 383ms555us
    5 172.26.57.28                               56  64 368ms228us
    6 172.26.57.28                               56  64 367ms593us
    7 172.26.57.28                               56  64 367ms752us
    8 172.26.57.28                               56  64 367ms759us
    9 172.26.57.28                               56  64 436ms555us
   10 172.26.57.28                               56  64 367ms637us
   11 172.26.57.28                               56  64 367ms441us
    sent=12 received=12 packet-loss=0% min-rtt=367ms408us avg-rtt=375ms819us
   max-rtt=436ms555us
```

Gambar 9 Koneksi RO Rumah - RO PT.Cyberark

Pengujian Konektivitas *End Device*

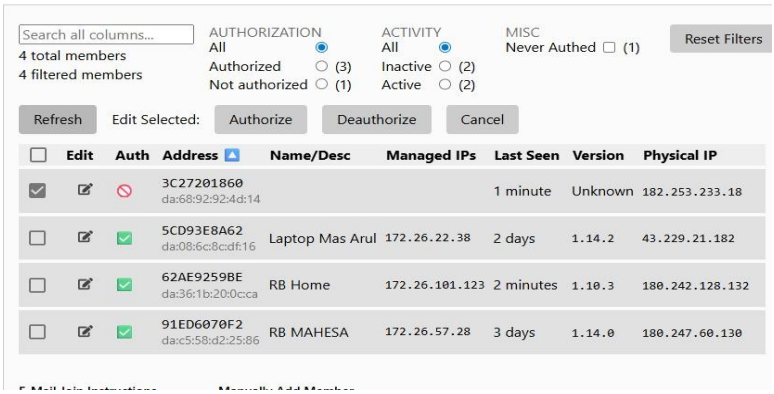
Pengujian ini memastikan bahwa perangkat akhir yang tergabung ke dalam jaringan ZeroTier dapat saling terhubung dengan stabil. Metode langkah-langkah uji meliputi ping antar perangkat dan simulasi akses ke server internal.

1. **Dial-Up koneksi client ke ZeroTier server**

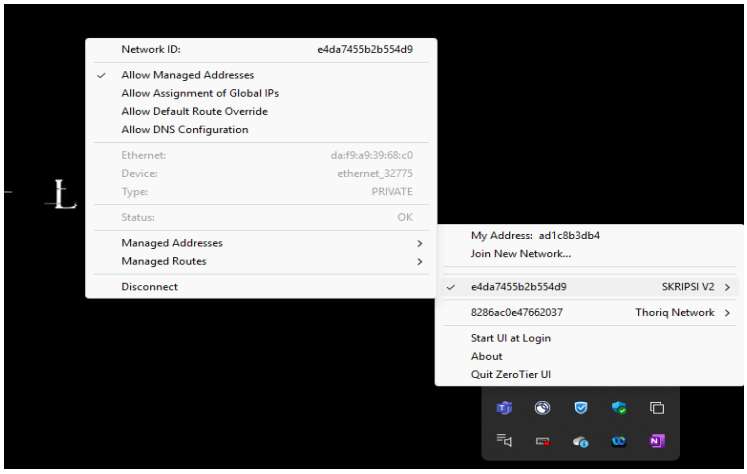


Gambar 10 Dial-up VPN Client

2. **Memberikan permission/izin dengan cara authorize device**



Gambar 11 Authorize the device to join the Network ID.



Gambar 412 Sukses connect VPN Client

3. Cek Koneksi End Device Dengan Test Ping dan Trace Route

```
Ethernet adapter ZeroTier One [e4da7455b2b554d9]:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7d45:da69:b66b:c700%29
   IPv4 Address. . . . . . . . . . . : 172.26.147.86
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 25.255.255.254
```

Gambar 13 IP address dari ZeroTier

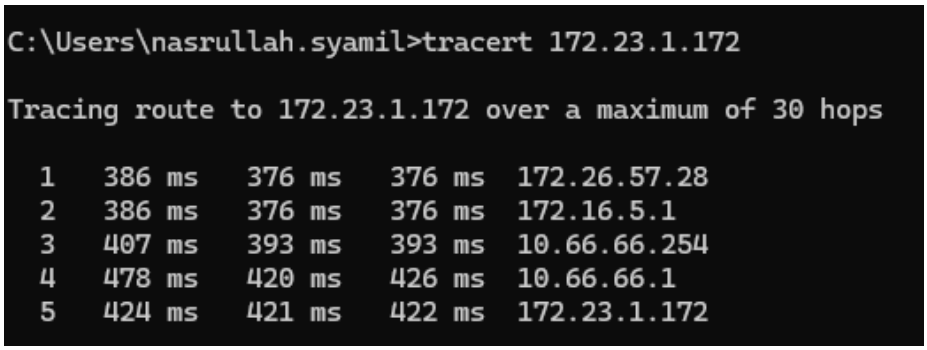
```
C:\Users\nasrullah.syamil>ping 172.26.101.123

Pinging 172.26.101.123 with 32 bytes of data:
Reply from 172.26.101.123: bytes=32 time=305ms TTL=64
Reply from 172.26.101.123: bytes=32 time=3ms TTL=64
Reply from 172.26.101.123: bytes=32 time=3ms TTL=64
Reply from 172.26.101.123: bytes=32 time=4ms TTL=64

Ping statistics for 172.26.101.123:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 305ms, Average = 78ms
```

Gambar 14. Koneksi VPN Client – RO Rumah

4. Cek koneksi dengan server internal dari PT.Cyberark

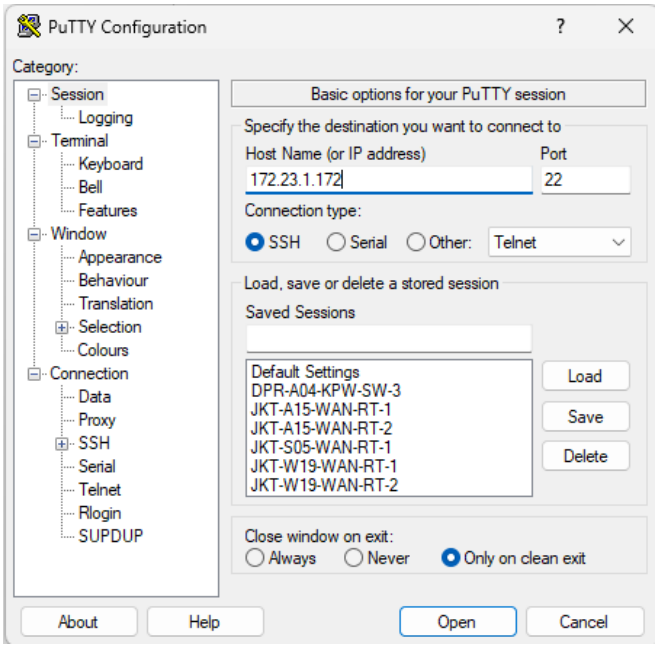
```
C:\Users\nasrullah.syamil>ping 172.23.1.172

Pinging 172.23.1.172 with 32 bytes of data:
Reply from 172.23.1.172: bytes=32 time=595ms TTL=60
Reply from 172.23.1.172: bytes=32 time=462ms TTL=60
Reply from 172.23.1.172: bytes=32 time=407ms TTL=60
Reply from 172.23.1.172: bytes=32 time=413ms TTL=60

Ping statistics for 172.23.1.172:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 407ms, Maximum = 595ms, Average = 469ms
```

Gambar 15 Koneksi VPN Client - Server Internal

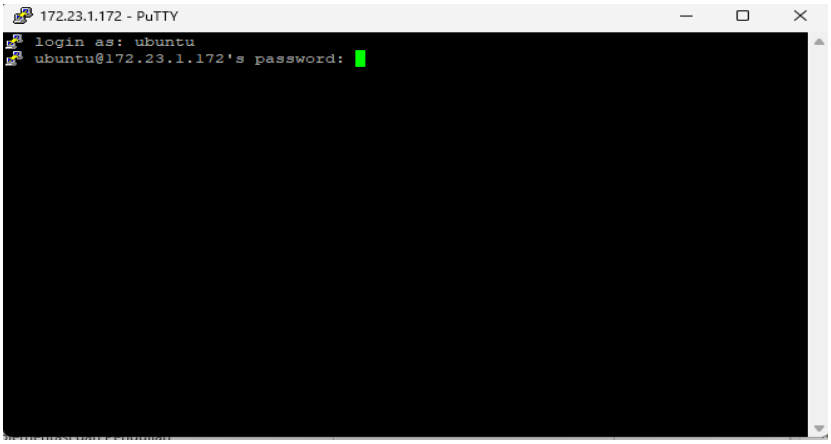


Gambar 16 Traceroute VPN Client - Server Internal

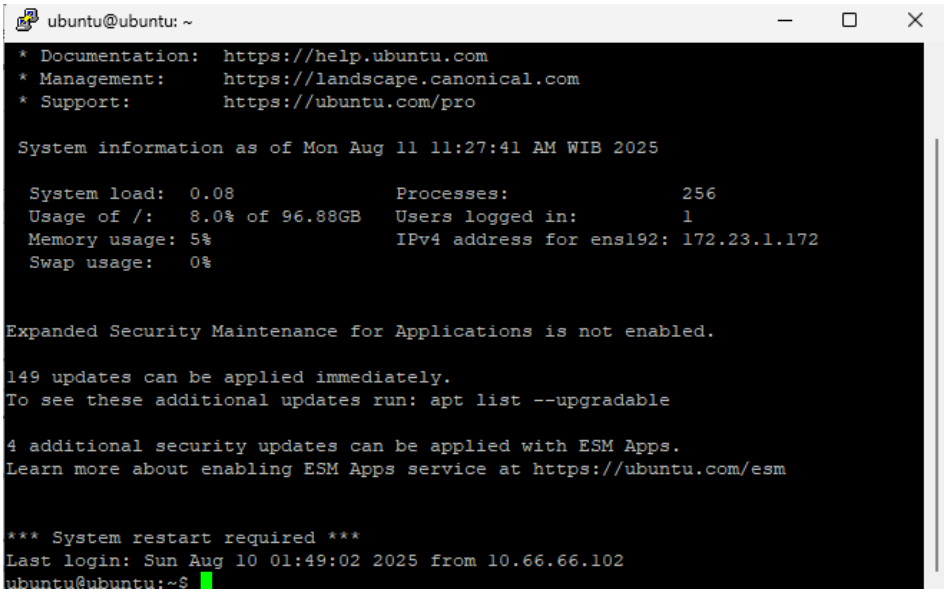
5. Pengujian dengan akses server internal



Gambar 17. Pengujian menggunakan Putty



Gambar 18. Credential Server Internal



Gambar 19. Client VPN dapat akses ke Server Internal

Pembahasan

Hasil pengujian menunjukkan bahwa implementasi sentralisasi koneksi VPN menggunakan ZeroTier berhasil diterapkan dan berfungsi secara efektif dalam skenario jaringan SOHO. Melalui konfigurasi *routing* statis pada *gateway* sentral, seluruh lalu lintas data dari perangkat *client* berhasil diarahkan melalui satu titik kendali. Hal ini secara fundamental mengubah model jaringan *peer-to-peer* yang menjadi karakteristik default ZeroTier menjadi arsitektur yang lebih terstruktur dan aman. Temuan ini memvalidasi hipotesis penelitian bahwa teknologi jaringan *overlay* dapat diadaptasi untuk memenuhi kebutuhan manajemen jaringan yang terpusat. Analisis *traceroute* menunjukkan bahwa paket data yang dikirim dari *client* ke *server* melewati *gateway* ZeroTier terlebih dahulu, membuktikan bahwa topologi terpusat yang dirancang telah berhasil diimplementasikan.
Penerapan metode sentralisasi ini menawarkan manfaat keamanan yang signifikan, terutama dalam konteks SOHO yang sering kali rentan. Dengan membatasi komunikasi langsung antar *client*, penelitian ini berhasil mengurangi risiko serangan *lateral movement* di dalam jaringan virtual. Hasil ini sejalan dengan penelitian sebelumnya yang menunjukkan bahwa segmentasi jaringan dan kontrol akses terpusat merupakan strategi efektif untuk mitigasi ancaman siber (Wijaya & Gunawan, 2024). Penggunaan ZeroTier sebagai platform sentralisasi juga memberikan lapisan enkripsi AES-256-GCM yang kuat, memastikan kerahasiaan data yang dikirim melalui jaringan publik. Aspek keamanan ini menjadi kunci diferensiasi dari solusi yang tidak terenkripsi dan kurang terkontrol.

Meskipun demikian, ada beberapa keterbatasan yang perlu dibahas. Sentralisasi koneksi ZeroTier memang berhasil, tetapi implementasinya membutuhkan pemahaman teknis yang lebih dalam, khususnya pada konfigurasi *routing* dan *firewall* di sisi *gateway* Mikrotik. Hal ini berpotensi menjadi hambatan bagi pengguna SOHO yang tidak memiliki latar belakang IT. Namun, hasil pengujian menunjukkan bahwa performa jaringan, terutama dari segi latensi dan *throughput*, tetap stabil dan optimal untuk kebutuhan

operasional SOHO. Efisiensi ini didukung oleh arsitektur ZeroTier yang tidak memerlukan *port forwarding* atau *IP publik*, mengurangi kompleksitas teknis yang lazim pada VPN konvensional (Suhadi & Arifin, 2024).

Studi ini memberikan kontribusi teoretis dengan menjembatani *research gap* yang ada antara teknologi jaringan *overlay* dan kebutuhan arsitektur terpusat. Berbeda dengan penelitian sebelumnya yang hanya berfokus pada koneksi *peer-to-peer* (Pratama & Marcus, 2025), penelitian ini membuktikan bahwa ZeroTier memiliki fleksibilitas untuk diintegrasikan ke dalam model sentralisasi, mirip dengan SD-WAN namun dengan biaya yang jauh lebih rendah. Temuan ini membuka wawasan baru bagi akademisi dan praktisi untuk mengeksplorasi potensi lain dari teknologi serupa dalam menciptakan solusi jaringan yang efisien dan aman.

Secara praktis, penelitian ini menyediakan panduan yang komprehensif bagi pelaku usaha SOHO untuk mengamankan jaringan mereka tanpa harus berinvestasi pada perangkat keras yang mahal. Kemudahan implementasi, efisiensi biaya, dan peningkatan kontrol keamanan menjadikan metode ini sebagai solusi yang layak dan relevan di era kerja terdistribusi. Diharapkan, hasil dari penelitian ini dapat menjadi referensi bagi pengembangan sistem manajemen jaringan *lightweight* yang lebih intuitif di masa depan.

Kesimpulans

Penelitian ini berhasil membuktikan bahwa metode sentralisasi koneksi VPN menggunakan ZeroTier efektif untuk mengoptimalkan keamanan dan manajemen jaringan pada lingkungan Small Office/Home Office (SOHO). Melalui implementasi arsitektur terpusat, seluruh lalu lintas data dari perangkat *client* berhasil diarahkan melalui satu *gateway* yang terkontrol, memvalidasi hipotesis penelitian. Temuan ini tidak hanya menunjukkan keberhasilan teknis dalam mengubah model jaringan *peer-to-peer* menjadi terpusat, tetapi juga menyoroti manfaat signifikan dalam hal keamanan, seperti segmentasi lalu lintas dan pengurangan risiko serangan. Efektivitas ini didukung oleh fitur enkripsi bawaan ZeroTier yang menjamin keamanan data, memberikan solusi yang ringan, hemat biaya, dan mudah diimplementasikan, sesuai dengan karakteristik kebutuhan sektor SOHO.

Meskipun demikian, ada beberapa keterbatasan yang teridentifikasi. Implementasi ini menuntut pemahaman teknis lebih dalam terkait konfigurasi *routing* dan *firewall* pada *gateway* yang mungkin menjadi tantangan bagi pengguna awam. Selain itu, penelitian ini terbatas pada skenario jaringan simulasi dengan perangkat fisik tertentu. Untuk penelitian di masa depan, disarankan untuk melakukan pengujian pada skala yang lebih besar dengan variasi perangkat yang lebih beragam untuk mengukur skalabilitas dan performa sistem secara lebih komprehensif. Selain itu, penelitian lanjutan dapat berfokus pada pengembangan antarmuka pengguna yang lebih intuitif atau *wizard* konfigurasi otomatis, untuk mempermudah adopsi metode sentralisasi ini oleh pelaku usaha SOHO yang tidak memiliki sumber daya IT khusus.

sDaftar Pustaka

Atmoko, A. T., Budiman, A. S., & Nuraeni, N. (2024). Perancangan Dan Pengembangan Virtual Private Network (VPN) Menggunakan PPTP Pada PT Indobinatu Mitra Sejati.

Aung, S. T., & Thein, T. (2020). Comparative Analysis of Site-to-Site Layer 2 Virtual Private Networks.

Creswell, J. W., & Creswell, J. D. (2022). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. SAGE Publications.

Emzir, E. (2021). *Metodologi Penelitian Kualitatif Analisis Data*. Raja Grafindo Persada.

Gentile, A. F., Macrì, D., Greco, E., & Fazio, P. (2024). Overlay and Virtual Private Networks Security Performance Analysis with Open Source Infrastructure Deployment. *Future Internet*, *16*(8). https://doi.org/10.3390/fi16080283

Gunawan, M. A., & Wardhana, S. (n.d.). Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN (Virtual Private Network). *6*(1).

Jain, R. K., & Trivedi, P. (2017). OSSEC-Based Authentication Process with Minimum Encryption and Decryption Time for Virtual Private Network. Dalam *Proceedings - 2016 8th International Conference on Computational Intelligence and Communication Networks, CICN 2016* (hlm. 442–445). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CICN.2016.92

Jangid, M., & Trivedi, P. (2017). Improve the Performance of the Successive Ratio for Virtual Private Network. Dalam *Proceedings - 2016 8th International Conference on Computational Intelligence and Communication Networks, CICN 2016* (hlm. 97–101). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CICN.2016.26

Jangid, M., & Trivedi, P. (2017). Improve the Performance of the Successive Ratio for Virtual Private Network. Dalam *Proceedings - 2016 8th International Conference on Computational Intelligence and Communication Networks, CICN 2016* (hlm. 97–101). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/CICN.2016.26

Kurniawan, B., & Santoso, A. (2023). Tantangan Jaringan di Era Kerja Hibrida: Studi Kasus Perusahaan Startup. *Jurnal Teknologi Informasi*, *5*(2), 123–130.

Muharram Permana, A. H., Widiyasono, N., & Rahmatulloh, A. (n.d.). Perbandingan Algoritma Pada Teknologi Virtual Private Network (VPN) IPSec Terhadap Kecepatan Transfer Data.

Mulder, V., Mermoud, A., Lenders, V., & Tellenbach, B. (2023). Trends in Data Protection and Encryption Technologies. Springer Nature. https://doi.org/10.1007/978-3-031-33386-6

Pramono, B., Fitri, E., & Handayani, N. (2024). Peran Jaringan Komputer dalam Mendukung Mobilitas Kerja Jarak Jauh. *Jurnal Informatika Bisnis*, *10*(1), 45–56.

Pratama, M. F., & Marcus, R. D. (2025). IMPLEMENTASI LOCAL AREA NETWORK BERBASIS CLOUD DENGAN MENGGUNAKAN ZEROTIER DAN REMOTE

DESKTOP PROTOCOL PADA WINDOWS SERVER 2019 (STUDI KASUS: PT. ESTETIKA SUKSES INDONESIA).

Putra, R. A., Supendar, H., & Fahlapi, R. (2023). Perancangan Virtual Private Network Dengan Metode PPTP Menggunakan Mikrotik. *Jurnal Komputer Antartika, 1*. https://ejournal.mediaantartika.id/index.php/jka

Putra, S., Iqbal, M., Putera, A., & Siahaan, U. (n.d.). Network Security Design Using Virtual Private Network (VPN) Method By Utilizing Point To Point Tunneling Protocol (PPTP) Technology On Local Area Network (LAN). www.ijecom.org

Rizky, A., Susanto, I., & Lestari, A. (2023). Analisis Risiko Keamanan Jaringan pada Era Digitalisasi Bisnis SOHO. *Jurnal Keamanan Siber*, *7*(3), 210–225.

Sherlin Solomi, V., Stela, D., Sandhiya, D., & Tanu. (2021). Implementation of HUB and Spoke Topology in VPN Using EIGRP. Dalam *2021 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2021* (hlm. 135–142). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/WiSPNET51692.2021.9419390

Simanungkalit, R., & Rahadian, B. (2022). Pengaruh Keamanan Jaringan Terhadap Integritas Data Perusahaan. *Jurnal Ilmu Komputer*, *15*(1), 34–45.

Subekti, R. (2020). IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SOLUSI SECURITY SELAMA WORK FROM HOME.

Sudaryono. (2023). *Metodologi Penelitian: Terapan dan Aplikasi*. Rajawali Pers.

Sugiyono. (2021). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Alfabeta.

Suhadi, E., & Arifin, T. (2024). RANCANGAN VIRTUAL PRIVATE NETWORK PADA KANTOR PROLOV MENGGUNAKAN ZEROTIER. *JIKA (Jurnal Informatika), 8*(1), 66. https://doi.org/10.31000/jika.v8i1.9979

Tian, Y., Ye, T., & Su, Y. (2007). Demonstration and scalability analysis of an all-optical virtual private network in multiple passive optical networks using ASK/FSK format. *IEEE Photonics Technology Letters, 19*(20), 1595–1597. https://doi.org/10.1109/LPT.2007.904561

Wijaya, P., & Gunawan, R. (2024). Peningkatan Kontrol Akses Jaringan Melalui Segmentasi Traffic di Lingkungan Perusahaan. *Jurnal Sistem Keamanan*, *9*(1), 112–125.