Infotek : Jurnal Informatika dan Teknologi
Vol. 9 No. 1, Januari 2026
Hal.219-230

e-ISSN 2614-8773

DOI : 10.29408/jit.v9i1.32536 Link : https://dx.doi.org/10.29408/jit.v9i1.32536

Implementasi Sistem Monitoring Perangkat Rectifier dan AC Berbasis Jaringan VPN Menggunakan Mikrotik pada Ruang Server

Taufik Rahman[1*], Muhammad Farid Anfasa[2]
[1,2] Program Studi Teknik Informatika, Universitas Bina Sarana Informatika
*taufik@bsi.ac.id

Abstrak

Ruang server pada sektor telekomunikasi memerlukan sistem pemantauan yang andal untuk menjaga kontinuitas layanan, khususnya terhadap perangkat pendukung seperti rectifier dan air conditioner (AC) yang berperan penting dalam kestabilan daya dan suhu. Permasalahan yang sering terjadi adalah keterbatasan monitoring yang belum terintegrasi serta belum dapat diakses secara aman dari jarak jauh, sehingga berpotensi menimbulkan keterlambatan dalam deteksi gangguan. Penelitian ini bertujuan untuk mengimplementasikan sistem monitoring perangkat rectifier dan AC berbasis jaringan Virtual Private Network (VPN) menggunakan MikroTik pada ruang server. Metodologi penelitian meliputi tahapan identifikasi permasalahan, studi literatur, analisis kebutuhan sistem, perancangan topologi jaringan, implementasi VPN dan sistem monitoring, serta pengujian dan evaluasi kinerja jaringan. VPN dikonfigurasikan pada router MikroTik untuk menyediakan jalur komunikasi yang aman antara ruang server dan administrator jaringan. Pengujian dilakukan dengan membandingkan kondisi jaringan sebelum dan sesudah implementasi menggunakan parameter konektivitas dan kestabilan akses monitoring. Hasil penelitian menunjukkan bahwa sistem monitoring yang diusulkan mampu menyediakan pemantauan kondisi rectifier dan AC secara real-time dengan tingkat keamanan yang lebih baik. Implementasi VPN berbasis MikroTik terbukti mendukung konektivitas yang stabil dan aman, sehingga mempercepat proses deteksi dini gangguan dan meningkatkan keandalan operasional ruang server. Sistem ini diharapkan dapat menjadi solusi praktis dalam pengelolaan infrastruktur ruang server pada lingkungan telekomunikasi.

Kata kunci : Air Conditioner, Keamanan Jaringan, MikroTik, Monitoring, Rectifier, Remote Access,VPN

Abstract

Server rooms in the telecommunications sector require a reliable monitoring system to maintain service continuity, especially for supporting devices such as rectifiers and air conditioners (AC) which play an important role in power and temperature stability. A problem that often occurs is the limitation of monitoring that has not been integrated and cannot be accessed safely remotely, so it has the potential to cause delays in interference detection. This study aims to implement a monitoring system for rectifier devices and air conditioners based on the Virtual Private Network (VPN) network using MikroTik in the server room. The research methodology includes the stages of problem identification, literature study, system needs analysis, network topology design, VPN implementation and monitoring system, as well as testing and evaluating network performance. The VPN is configured on the MikroTik router to provide a secure communication path between the server room and the network administrator. The test was carried out by comparing the network conditions before and after implementation using connectivity parameters and monitoring access stability. The results of the study show that the proposed monitoring system is able to provide real-time monitoring of the condition of rectifiers and air conditioners with a better level of safety. MikroTik-based VPN implementations are proven to support stable and secure connectivity, thus speeding up the early detection process of interference and improving the operational reliability of server space. This system is expected to be a practical solution in managing server space infrastructure in telecommunication environments.

Keywords : Air Conditioner, MikroTik, Monitoring, Network Security, Rectifier, Remote Access, VPN.

Infotek : Jurnal Informatika dan Teknologi
Vol. 9 No. 1, Januari 2026
Hal.219-230

e-ISSN 2614-8773

DOI : 10.29408/jit.v9i1.32536 Link : https://dx.doi.org/10.29408/jit.v9i1.32536

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi (TIK) secara global telah mendorong peningkatan kebutuhan terhadap layanan data yang andal, berkelanjutan, dan beroperasi selama 24 jam. Infrastruktur pusat data dan ruang server menjadi komponen kritis dalam mendukung layanan tersebut, khususnya pada sektor telekomunikasi. Laporan internasional menyebutkan bahwa gangguan pada sistem catu daya dan sistem pendingin merupakan salah satu penyebab utama terjadinya downtime pusat data, dengan kontribusi signifikan terhadap kegagalan layanan jaringan[1]. Di tingkat nasional, operator telekomunikasi seperti PT Telkom Indonesia dituntut untuk menjaga kontinuitas layanan dengan memastikan perangkat pendukung ruang server, terutama rectifier sebagai penyedia daya DC dan air conditioner (AC) sebagai pengendali suhu, beroperasi secara optimal dan stabil.

Salah satu isu utama yang sering dihadapi adalah keterbatasan sistem monitoring yang bersifat real-time, terpusat, dan aman, khususnya pada ruang server yang tersebar di berbagai lokasi operasional. Monitoring yang masih dilakukan secara manual atau lokal berpotensi menyebabkan keterlambatan dalam mendeteksi gangguan pada rectifier maupun AC, sehingga meningkatkan risiko kerusakan perangkat dan penurunan kualitas layanan. Menurut Tanenbaum dan Wetherall, sistem jaringan modern memerlukan mekanisme monitoring yang terintegrasi dan dapat diakses secara jarak jauh untuk menjamin keandalan infrastruktur jaringan kritikal[2]. Oleh karena itu, dibutuhkan solusi monitoring berbasis jaringan yang tidak hanya andal, tetapi juga aman.

Penelitian sebelumnya telah banyak membahas sistem monitoring jaringan dan lingkungan ruang server. Beberapa penelitian memanfaatkan Internet of Things (IoT) untuk pemantauan suhu dan konsumsi energi guna meningkatkan efisiensi operasional pusat data[3]. Penelitian lain mengkaji penggunaan Network Monitoring System (NMS) seperti PRTG, Zabbix, dan The Dude dalam memantau perangkat jaringan dan trafik data[4]. Namun, sebagian besar penelitian tersebut lebih menitikberatkan pada monitoring trafik jaringan atau efisiensi energi, dan belum secara spesifik mengintegrasikan monitoring perangkat rectifier dan AC dengan mekanisme keamanan jaringan berbasis VPN, khususnya pada lingkungan operasional telekomunikasi.

Berdasarkan kajian tersebut, terdapat celah penelitian pada aspek implementasi sistem monitoring perangkat pendukung ruang server yang mengombinasikan keamanan jaringan dan pemantauan perangkat daya serta pendingin dalam satu sistem terintegrasi. Kebaruan penelitian ini terletak pada penerapan Virtual Private Network (VPN) menggunakan MikroTik sebagai media komunikasi yang aman untuk

Infotek : Jurnal Informatika dan Teknologi
Vol. 9 No. 1, Januari 2026
Hal.219-230

e-ISSN 2614-8773

DOI : 10.29408/jit.v9i1.32536 Link : https://dx.doi.org/10.29408/jit.v9i1.32536

monitoring perangkat rectifier dan AC secara real-time. Secara teori, VPN memungkinkan pembentukan jalur komunikasi privat di atas jaringan publik dengan menjamin kerahasiaan, integritas, dan autentikasi data[5]. MikroTik sebagai perangkat router menyediakan fitur VPN yang fleksibel dan efisien, sehingga banyak digunakan dalam implementasi jaringan skala perusahaan[6]. Fokus penelitian ini adalah mengimplementasikan sistem monitoring perangkat rectifier dan AC berbasis jaringan VPN menggunakan MikroTik pada ruang server, serta menganalisis peningkatan kinerja dan keamanan jaringan setelah implementasi. Hasil penelitian diharapkan dapat menjadi solusi praktis dalam meningkatkan keandalan operasional ruang server, mempercepat deteksi gangguan, dan mendukung pengelolaan infrastruktur telekomunikasi yang lebih aman dan efisien

2. Tinjauan Pustaka

2.1. Penelitian Terkait

Beberapa penelitian terdahulu yang relevan dengan topik monitoring perangkat berbasis jaringan VPN dan Mikrotik dalam lima tahun terakhir, antara lain:

- Sistem Monitoring Infrastruktur Jaringan dengan MikroTik dan Telegram Penelitian ini mengembangkan sistem monitoring jaringan infrastruktur menggunakan router MikroTik dengan notifikasi melalui Telegram untuk mendeteksi gangguan jaringan secara real-time. Studi ini memperlihatkan implementasi monitoring berbasis perangkat MikroTik untuk menjaga kestabilan sistem jaringan di lingkungan sekolah menengah kejuruan[7].

- Remote Sistem Informasi Manajemen VPN Remote Mikrotik Berbasis Codeigniter PHP Framework Di Desa Sawo. Studi ini merancang sistem manajemen remote VPN berbasis MikroTik dengan antarmuka yang memudahkan konfigurasi VPN bagi pengguna non-teknis sehingga mengurangi kesalahan pengaturan pada konfigurasi VPN dan meningkatkan efisiensi akses jaringan remote[8].

- Perancangan dan Implementasi VPN Menggunakan MikroTik (NDLC)
Penelitian ini menerapkan jaringan VPN berbasis MikroTik pada lingkungan kampus untuk meningkatkan keamanan dan stabilitas akses pengguna jarak jauh. Hasil penelitian menunjukkan peningkatan signifikan keamanan dan akses jaringan eksternal[9].

- Implementasi Keamanan Data pada Jaringan Router MikroTik Menggunakan VPN L2TP/IPSec Penelitian ini mengevaluasi efektivitas VPN L2TP/IPSec untuk keamanan data pada router MikroTik melalui pengujian serangan serta analisa QoS, menunjukkan peningkatan keamanan data di jaringan meskipun terjadi beberapa dampak pada performa jaringan[10].

Infotek : Jurnal Informatika dan Teknologi
Vol. 9 No. 1, Januari 2026
Hal.219-230

e-ISSN 2614-8773

DOI : 10.29408/jit.v9i1.32536 Link : https://dx.doi.org/10.29408/jit.v9i1.32536

- Sistem Monitoring Jaringan dengan Fitur The Dude MikroTik Penelitian ini mengoptimalkan fungsi *The Dude* pada MikroTik RouterOS untuk monitoring jaringan, mendeteksi kesalahan koneksi, dan mempermudah admin jaringan mengetahui letak gangguan dengan cepat[11].
- Penelitian oleh Fajri berjudul Perancangan Remote Site Mikrotik dengan VPN (PPPoE) Menggunakan Rest API di SMA Muhammadiyah 3 Padang. Penelitian ini merancang sistem VPN berbasis Mikrotik yang dikombinasikan dengan Rest API untuk meningkatkan keamanan, stabilitas. dan efisiensi jaringan internet di sekolah. Hasilnya, sistem mampu membatasi akses pengguna serta mempercepat konfigurasi jaringan[12].
- Penelitian oleh Amirulloh yang berjudul Pengembangan Trainer Air Conditioner Split Daya 1 PK Berbasis Internet of Things (IoT) merancang prototipe trainer AC dengan NodeMCU ESP8266 dan aplikasi Blynk. Sistem ini memungkinkan pemantauan dan pengendalian suhu jarak jauh dengan hasil uji fungsional mencapai 95%[13].
- Penelitian oleh Pratama dan Puspitasari yang berjudul Penerapan Protokol L2TP/IPSec dan Port Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP. Penelitian ini menawarkan solusi agar administrator dapat meremote router Mikrotik dari jaringan publik dengan aman menggunakan VPN berbasis L2TP/IPSec[14].
- Penelitian oleh Afifi Al-Atsari dan Suharjo yang berjudul Integrasi Server On-Premise dengan Server Cloud Menggunakan Cloud VPN dan Mikrotik Ipsec Untuk Peningkatan Keamanan Koneksi berhasil membangun VPN site-to-site untuk menghubungkan kantor cabang dengan tingkat keamanan data yang lebih baik[15].
- Penelitian oleh Prayogi Wicaksana yang berjudul Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec sebagai Keamanan Jaringan. Penelitian ini membuktikan bahwa penerapan VPN pada perangkat Mikrotik mampu meningkatkan keamanan jaringan dan mempercepat proses pertukaran data antar kantor[16].

2.2. Landasan Teori

1. Rectifier sebagai Perangkat Konversi Daya Rectifier adalah perangkat elektronik yang mengubah arus bolak-balik (AC) menjadi arus searah (DC) yang dibutuhkan oleh sistem seperti server atau peralatan telekomunikasi untuk menjaga stabilitas daya. Efisiensi dan pemantauan rectifier membantu kestabilan sistem operasi dan mencegah gangguan[17]

2. Virtual Private Network (VPN) VPN adalah teknologi untuk membangun koneksi aman antara dua titik jaringan melalui internet publik. Dengan enkripsi, VPN menjaga privasi dan integritas data antara remote client dan jaringan internal[18].

Infotek : Jurnal Informatika dan Teknologi
Vol. 9 No. 1, Januari 2026
Hal.219-230

e-ISSN 2614-8773

DOI : 10.29408/jit.v9i1.32536 Link : https://dx.doi.org/10.29408/jit.v9i1.32536

3. MikroTik RouterOS dan Fitur VPN MikroTik RouterOS menyediakan fitur VPN (L2TP, PPTP, IPSec) yang dapat dikonfigurasi untuk memberikan akses aman ke jaringan internal. Router ini banyak digunakan untuk skenario monitoring jaringan dan remote connectivity[9].

4. Konsep Real-Time Monitoring dan IoT Monitoring status perangkat secara konstan di jaringan modern sering menggunakan pendekatan IoT atau aplikasi NMS untuk real-time data, alert otomatis, dan pemantauan terpusat[19][20].

5. Pentingnya Redundansi dan Failover Dalam sistem kritikal seperti telekomunikasi, redundancy (cadangan) dan failover dibutuhkan untuk mengurangi downtime saat satu komponen gagal.

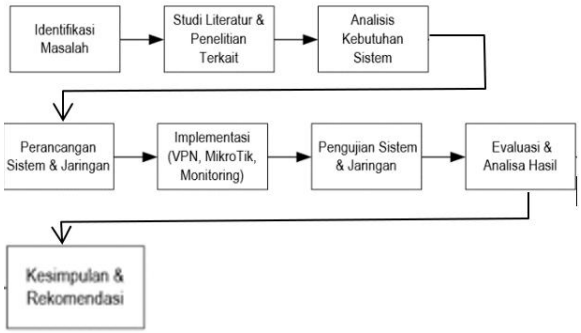
6. Reliability dan Maintainability dalam Sistem Monitoring Perangkat monitoring harus memiliki parameter reliability tinggi agar dapat menjadi acuan daya tahan komponen dan meminimalkan risiko kegagalan fungsi.

7. Topologi dan Segmentasi Jaringan Desain topologi jaringan harus mempertimbangkan segmentasi VLAN, routing, dan VPN untuk memastikan trafik monitoring tidak bercampur dengan trafik lain dan tetap aman.

8. Sistem Monitoring Jaringan Sistem monitoring jaringan adalah mekanisme yang digunakan untuk mengamati, mencatat, dan menganalisis kondisi perangkat serta kinerja jaringan secara real-time. Sistem monitoring memungkinkan administrator jaringan untuk mendeteksi gangguan lebih cepat, menjaga performa layanan, serta melakukan tindakan preventif terhadap potensi kerusakan. Dalam konteks ruang server, sistem monitoring berperan penting untuk memastikan perangkat kritikal seperti rectifier dan AC tetap berfungsi normal [9].

2.3. Tahapan Penelitian

Tahapan penelitian disusun secara sistematis untuk memastikan bahwa proses perancangan, implementasi, dan evaluasi sistem monitoring berjalan terstruktur serta dapat dipertanggungjawabkan secara ilmiah. Metodologi penelitian ini terdiri dari beberapa tahapan utama, mulai dari studi literatur hingga penarikan kesimpulan.



Gambar 1 Diagram Alir (Flowchart) Tahapan Penelitian

1. Identifikasi Masalah. Tahap awal dilakukan dengan mengidentifikasi permasalahan yang terjadi pada ruang server, khususnya terkait keterbatasan monitoring perangkat rectifier dan

Infotek : Jurnal Informatika dan Teknologi
Vol. 9 No. 1, Januari 2026
Hal.219-230

e-ISSN 2614-8773

DOI : 10.29408/jit.v9i1.32536 Link : https://dx.doi.org/10.29408/jit.v9i1.32536

AC yang belum terintegrasi serta belum dapat diakses secara aman dari jarak jauh.

2. Studi Literatur dan Penelitian Terkait. Peneliti mengkaji buku, jurnal ilmiah, dan penelitian terdahulu yang berkaitan dengan sistem monitoring jaringan, rectifier, sistem pendingin (AC), VPN, serta pemanfaatan MikroTik sebagai perangkat jaringan.

3. Analisis Kebutuhan Sistem. Pada tahap ini dilakukan analisis kebutuhan fungsional dan non-fungsional sistem, meliputi parameter monitoring (tegangan, suhu, status perangkat), kebutuhan keamanan jaringan, serta kebutuhan perangkat keras dan perangkat lunak.

4. Perancangan Sistem dan Jaringan. Tahap ini mencakup perancangan topologi jaringan usulan, skema VPN berbasis MikroTik, arsitektur sistem monitoring, serta alur komunikasi data antara perangkat rectifier, AC, dan server monitoring.

5. Implementasi Sistem

Implementasi dilakukan dengan konfigurasi VPN pada router MikroTik, instalasi sistem monitoring, integrasi perangkat rectifier dan AC, serta pengaturan server monitoring agar data dapat diakses secara real-time dan aman.

6. Pengujian Sistem dan Jaringan. Pengujian dilakukan untuk mengevaluasi konektivitas jaringan VPN, kestabilan sistem monitoring, akurasi data, serta keamanan akses. Pengujian menggunakan tools seperti *Ping*, *Traceroute*, dan Network Monitoring System.

7. Evaluasi dan Analisa Hasil. Data hasil pengujian dianalisis untuk mengetahui perbedaan kinerja sebelum dan sesudah implementasi, termasuk peningkatan keandalan monitoring dan keamanan jaringan

8. Kesimpulan dan Rekomendasi. Tahap akhir adalah penyusunan kesimpulan berdasarkan hasil evaluasi serta pemberian rekomendasi untuk pengembangan sistem monitoring ke depan

3. Metode Penelitian

3.1. Desain Penelitian

Desain penelitian yang digunakan adalah perancangan sistem monitoring perangkat rectifier dan air conditioner (AC) dengan memanfaatkan jaringan Virtual Private Network (VPN) berbasis mikrotik dan menerapkan topologi star. Pemilihan desain ini didasarkan pada kebutuhan untuk menciptakan sistem yang aman, andal, dan efisien dalam melakukan pemantauan perangkat secara real-time dan jarak jauh.

3.2. Lokasi Penelitian

Penelitian ini dilakukan di PT Telkom STO Bekasi, yang merupakan salah satu unit kerja operasional PT Telkom Indonesia di wilayah Bekasi. Lokasi ini dipilih karena memiliki ruang server yang berfungsi sebagai pusat pengelolaan data dan layanan telekomunikasi, sehingga memerlukan dukungan perangkat penunjang dengan tingkat keandalan tinggi.

Infotek : Jurnal Informatika dan Teknologi
Vol. 9 No. 1, Januari 2026
Hal.219-230

e-ISSN 2614-8773

DOI : 10.29408/jit.v9i1.32536 Link : https://dx.doi.org/10.29408/jit.v9i1.32536

4. Hasil dan Pembahasan

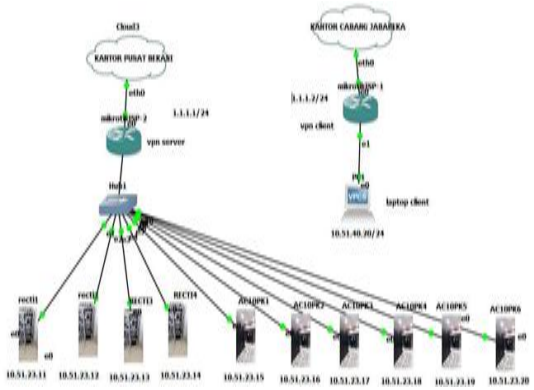
4.1. Hasil Penelitian

Hasil penelitian diperoleh melalui tahapan implementasi dan pengujian sistem monitoring perangkat rectifier dan air conditioner (AC) yang terintegrasi dengan jaringan VPN berbasis MikroTik pada ruang server. Implementasi dilakukan untuk menjawab permasalahan keterbatasan monitoring jarak jauh dan keamanan akses terhadap perangkat pendukung ruang server.

1. Implementasi Jaringan VPN Menggunakan MikroTik

Pada tahap ini, router MikroTik dikonfigurasikan untuk membangun koneksi Virtual Private Network (VPN) antara ruang server dan administrator jaringan. VPN berfungsi sebagai jalur komunikasi privat yang memungkinkan akses monitoring dari luar jaringan lokal tanpa membuka akses langsung ke jaringan internal. Hasil implementasi menunjukkan bahwa koneksi VPN dapat terhubung secara stabil dan memungkinkan administrator mengakses sistem monitoring secara aman.

Bukti empiris: perancangan jaringan usulan dilakukan secara sistematis agar sistem monitoring dapat berjalan dengan baik. Berdasarkan analisis kebutuhan, dirancang jaringan usulan dengan memanfaatkan Mikrotik RouterOS sebagai pusat pengelolaan jaringan dan VPN sebagai jalur komunikasi aman. Topologi yang digunakan adalah topologi hybrid yang mengintegrasikan LAN internal ruang server dengan VPN Mikrotik sehingga dapat diakses secara jarak jauh oleh teknisi.



Gambar 2 Skema Jaringan Usulan

Dalam jaringan usulan ini, perangkat rectifier dan air conditioner (AC) dipasangkan sensor untuk membaca parameter operasional (tegangan, arus, dan suhu). Data sensor dikirim ke dashboard monitoring berbasis web yang terhubung dengan router Mikrotik. Router kemudian mengamankan akses monitoring dengan konfigurasi VPN L2TP/IPSec, firewall, VLAN, serta autentikasi pengguna. Dengan rancangan ini, teknisi dapat melakukan monitoring real-time baik secara lokal melalui LAN maupun secara jarak jauh melalui VPN terenkripsi. Rancangan jaringan ini diharapkan dapat menjawab permasalahan utama, yaitu keterbatasan monitoring manual, absennya akses jarak jauh, serta kebutuhan keamanan data monitoring.

Infotek : Jurnal Informatika dan Teknologi
Vol. 9 No. 1, Januari 2026
Hal.219-230

e-ISSN 2614-8773

DOI : 10.29408/jit.v9i1.32536 Link : https://dx.doi.org/10.29408/jit.v9i1.32536

2. Implementasi Sistem Monitoring Rectifier dan AC

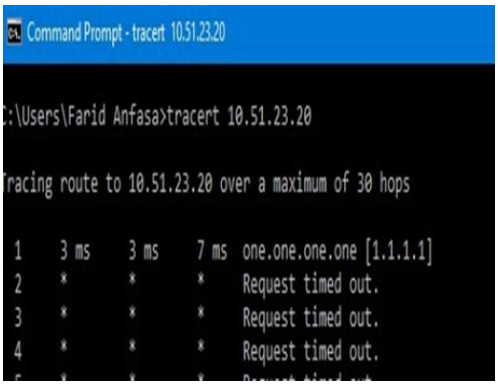
Sistem monitoring dikonfigurasikan untuk menampilkan informasi kondisi perangkat rectifier dan AC, seperti status perangkat, suhu ruang, dan parameter operasional lainnya. Data monitoring ditampilkan secara real-time melalui aplikasi monitoring yang terhubung ke jaringan internal ruang server.

3. Hasil Pengujian Jaringan Awal

Pengujian jaringan awal dilakukan sebelum implementasi VPN dan sistem monitoring terintegrasi. Pengujian menggunakan perintah *ping* dan *traceroute* menunjukkan bahwa akses monitoring hanya dapat dilakukan dari jaringan lokal, serta belum tersedia mekanisme keamanan tambahan untuk akses jarak jauh. Kondisi ini berpotensi menimbulkan risiko keamanan dan keterlambatan penanganan gangguan. Tes ping dilakukan dari komputer teknisi ke perangkat rectifier/AC melalui jaringan kantor cabang. Hasil: Ping tidak stabil, terdapat packet loss dan delay tinggi pada waktu tertentu.

Gambar 3. Tes Ping Dari Client Ke AC

Traceroute digunakan untuk melihat rute yang dilalui data menuju server monitoring. Temuan: Jalur yang dilalui mencakup beberapa hop internal yang turut menambah latensi koneksi.



Gambar 4 Tes *Traceroute*

Hasil pengujian awal mengindikasikan bahwa akses monitoring dari luar kantor masih belum memanfaatkan jalur aman seperti VPN, sistem monitoring belum terintegrasi dengan fitur notifikasi maupun alarm otomatis, serta jaringan belum dilengkapi dengan firewall atau mekanisme perlindungan lain sehingga rentan terhadap akses tidak sah. Selain itu, tidak adanya segmentasi VLAN menyebabkan seluruh perangkat tergabung dalam satu jaringan yang meningkatkan potensi risiko internal. Temuan ini menjadi dasar penting dalam perancangan sistem jaringan baru yang lebih terstruktur, aman, serta mampu mendukung pemantauan perangkat secara jarak jauh melalui VPN.

4. Hasil Pengujian Jaringan Akhir

Setelah implementasi VPN dan sistem monitoring, pengujian ulang dilakukan menggunakan tools yang sama. Hasil pengujian menunjukkan bahwa konektivitas jaringan tetap stabil, dan akses monitoring dapat dilakukan dari jarak jauh melalui

Infotek : Jurnal Informatika dan Teknologi
Vol. 9 No. 1, Januari 2026
Hal.219-230

e-ISSN 2614-8773

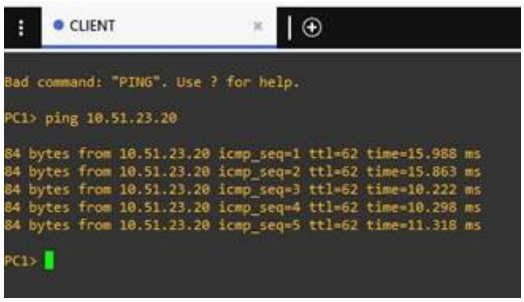
DOI : 10.29408/jit.v9i1.32536 Link : https://dx.doi.org/10.29408/jit.v9i1.32536

VPN. Tidak ditemukan kehilangan paket yang signifikan, serta waktu respon jaringan masih berada pada batas yang dapat diterima untuk kebutuhan monitoring.

5. Hasil Pengujian Jaringan Akhir

Setelah implementasi VPN dan sistem monitoring, pengujian ulang dilakukan menggunakan tools yang sama. Hasil pengujian menunjukkan bahwa konektivitas jaringan tetap stabil, dan akses monitoring dapat dilakukan dari jarak jauh melalui VPN. Tidak ditemukan kehilangan paket yang signifikan, serta waktu respon jaringan masih berada pada batas yang dapat diterima untuk kebutuhan monitoring.

Tes Ping dilakukan dari perangkat teknisi melalui koneksi VPN ke perangkat rectifer dan *AC*. Hasil: Respon koneksi sangat baik dengan rata-rata waktu 15 ms dan tanpa terjadi *packet loss*. Penggunaan VPN tidak memberikan dampak negatif terhadap latensi bila dibandingkan dengan koneksi lokal.

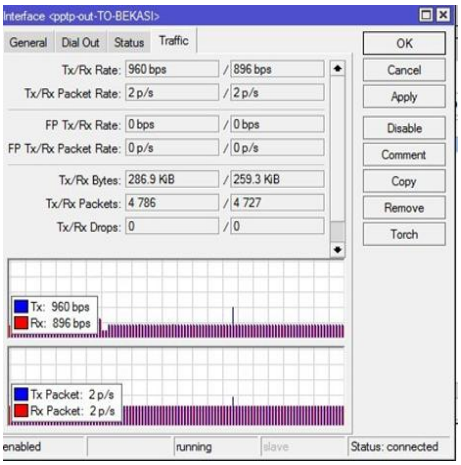


Gambar 5. Tes Ping Dari Client Ke AC

Kemudian tes traceroute untuk menunjukkan jalur koneksi ke server monitoring lebih optimal dengan hop minimal, membuktikan VPN Mikrotik mampu mempersingkat komunikasi ke jaringan internal.

Gambar 6. Tes Route Ke AC 10 pk no 6

Pemantauan Trafik dan *Bandwidth* (Mikrotik & PRTG). Lalu lintas data terpantau dalam kondisi stabil dan terkendali antara client VPN dan server monitoring. Tidak ditemukan hambatan.



Gambar 7. Cek Trafik dan Bandwidth

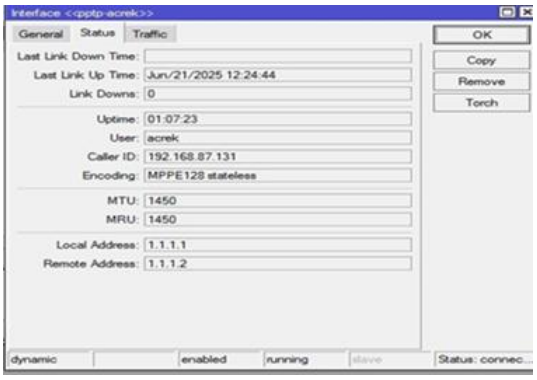
Pengujian sistem keamanan dilakukan melalui tes VPN dengan menggunakan protokol L2TP/IPSec. Hasil pengujian menunjukkan bahwa koneksi VPN berhasil terhubung dengan enkripsi aktif sehingga data yang ditransmisikan lebih aman. Selain itu, sistem hanya dapat diakses oleh pengguna yang memiliki kredensial serta alamat IP terdaftar, sehingga akses ke sistem monitoring

Infotek : Jurnal Informatika dan Teknologi
Vol. 9 No. 1, Januari 2026
Hal.219-230

e-ISSN 2614-8773

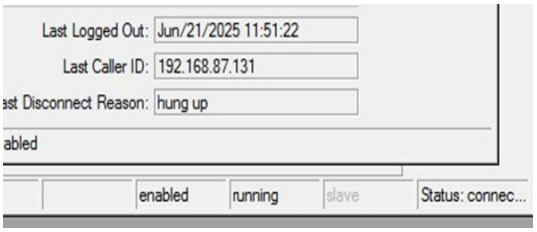
DOI : 10.29408/jit.v9i1.32536 Link : https://dx.doi.org/10.29408/jit.v9i1.32536

menjadi lebih terbatas dan terlindungi dari upaya penyusupan pihak yang tidak berwenang.



Gambar 8 Alamat IP Yang Terkoneksi

Akses ke jaringan internal berhasil dibatasi melalui aturan *firewall* di perangkat Mikrotik. Semua aktivitas terekam dalam sistem log, termasuk *login*, perubahan perangkat, dan koneksi VPN, sehingga mendukung keamanan dan proses audit.



Gambar 9 IP Yang Terkoneksi Ke VPN Server

4.2. Pembahasan

Berdasarkan hasil penelitian, implementasi sistem monitoring perangkat rectifier dan AC berbasis jaringan VPN menggunakan MikroTik terbukti mampu meningkatkan efektivitas dan keamanan pemantauan ruang server. Penggunaan VPN memberikan lapisan keamanan tambahan dengan membatasi akses hanya kepada pengguna yang terautentikasi, sehingga mengurangi risiko akses tidak sah ke jaringan internal. Integrasi sistem monitoring dengan jaringan VPN juga memberikan kemudahan bagi administrator jaringan dalam melakukan pemantauan secara real-time tanpa harus berada di lokasi ruang server. Hal ini berdampak pada percepatan proses deteksi dini terhadap potensi gangguan pada perangkat rectifier dan AC, yang sangat penting dalam menjaga stabilitas daya dan suhu ruang server. Dibandingkan dengan kondisi sebelum implementasi, sistem yang diusulkan menunjukkan peningkatan pada aspek aksesibilitas, keamanan, dan keandalan monitoring. Hasil ini sejalan dengan teori dan penelitian sebelumnya yang menyatakan bahwa monitoring terpusat dan berbasis jaringan aman dapat meningkatkan efisiensi pengelolaan infrastruktur jaringan dan perangkat kritikal.

Tabel 1. Perbandingan Hasil Evaluasi Jaringan

Aspek Uji	Sebelum Implementasi	Setelah Implementasi
Akses *Remote*	Tidak tersedia	VPN terenkripsi menggunakan Mikrotik tersedia
Monitoring *Real-Time*	Tidak akurat dan tidak stabil	*Real-time* dan terintegrasi dengan notifikasi
Keamanan Jaringan	Tidak ada *firewall/VPN*	*Firewall* dan *VPN* aktif dengan autentikasi
Logging Aktivitas	Tidak ada	Tersedia log lengkap pada Mikrotik

Infotek : Jurnal Informatika dan Teknologi
Vol. 9 No. 1, Januari 2026
Hal.219-230

e-ISSN 2614-8773

DOI : 10.29408/jit.v9i1.32536 Link : https://dx.doi.org/10.29408/jit.v9i1.32536

5. Kesimpulan

Penelitian ini membuktikan bahwa implementasi sistem monitoring perangkat rectifier dan air conditioner (AC) berbasis jaringan VPN menggunakan MikroTik di PT Telkom STO Bekasi mampu meningkatkan efektivitas pemantauan kondisi ruang server secara real-time dan aman. Penerapan VPN memungkinkan akses monitoring jarak jauh dengan tingkat keamanan yang lebih baik, sehingga mendukung deteksi dini terhadap potensi gangguan pada sistem daya dan pendingin. Kontribusi penelitian ini terletak pada integrasi sistem monitoring perangkat kritikal ruang server dengan mekanisme keamanan jaringan berbasis VPN dalam satu arsitektur yang aplikatif dan mudah diterapkan pada lingkungan operasional telekomunikasi. Sistem yang diusulkan dapat menjadi solusi praktis untuk meningkatkan keandalan operasional dan mengurangi risiko gangguan layanan. Namun demikian, penelitian ini masih terbatas pada pemantauan parameter dasar dan ruang lingkup implementasi yang terbatas. Pengembangan lebih lanjut diperlukan untuk menambahkan fitur analisis prediktif, otomatisasi notifikasi, serta pengujian pada skala jaringan yang lebih luas guna meningkatkan kinerja dan skalabilitas sistem

6. Daftar Pustaka

[1] A. Lawrence and L. Simon, “Annual Outage Analysis 2023,” Uptime Institute. [Online]. Available: https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[2] A. Tanenbaum, N. Feamster, and D. Wetherall, *Computer Networks, Global Edition, 6/E*. 2021. L. Zhao, S. Qu, J. Zeng, and Q. Zhao, “Energy-saving and management of telecom operators’ remote computer rooms using IoT technology,” *IEEE Access*, vol. 8, pp. 166197–166211, 2020, doi: 10.1109/ACCESS.2020.3022641.

[4] W. Odom, *CCNA 200-301 Official Cert Guide , Volume 1 , Second Edition*. Hoboken, New Jersey: Cisco Press, 2024.

[5] T. Copyright and W. Stallings, “C Ryptography and N Etwork S Ecurity :,” 2013.

[6] Emils, “Virtual Private Networks,” Atlassian Confluence 9.2.11. [Online]. Available: https://help.mikrotik.com/docs/spaces/ROS/pages/119144597/Virtual+Private+Networks

[7] B. Pratama, Zulhendra, A. Hadi, and L. Mursyida, “Development of Network Infrastructure Monitoring System at Vocational High School Using MikroTik and Telegram Integration,” *J. Hypermedia Technol. Learn.*, vol. 2, no. 2, pp. 194–208, 2024, doi: 10.58536/j-hytel.v2i3.133

[8] P. E and A. R. Adi, “Sistem Informasi Manajemen VPN Remote Mikrotik Berbasis Codeigniter PHP Framework Di Desa Sawo,” *J-Intech*, vol. 12, no. 02, pp. 340–352, 2024, doi: 10.32664/j-intech.v12i02.1468.

[9] N. P. Riyanto, F. A. Thariq, and M. Putra, “Perancangan Dan Implementasi Sistem Jaringan Server Dengan Vpn Berbasis Mikrotik Menggunakan Metode Network Development Life Cycle (NDLC),” vol. 32, no. 3, pp. 167–186, 2021, doi: https://doi.org/10.31539/intecoms.v8i1.13761.

[10] H. D. Nugroho and Y. Sutanto, “Implementasi Keamanan Data Pada

Infotek : Jurnal Informatika dan Teknologi
Vol. 9 No. 1, Januari 2026
Hal.219-230

e-ISSN 2614-8773

DOI : 10.29408/jit.v9i1.32536 Link : https://dx.doi.org/10.29408/jit.v9i1.32536

Jaringan Router MikroTik Menggunakan VPN L2TP Dan IPSec," *J. Electr. Electron. …*, vol. 4, no. 1, 2025, doi: https://doi.org/10.58991/at4tdq03.

[11] B. Purwanto and W. A. Dewa, "Sistem Monitoring Jaringan dengan Memanfaatkan Fitur The Dude Mikrotik Router Os," *J. Teknol. Informasi, Teor. Konsep dan Implentasi*, vol. 11, no. 1, pp. 33–37, 2020, doi: 10.36382/jti-tki.v11i1.488.

[12] A. F. Fajri, N. Novinaldi, A. P. Nanda, I. Isnardi, and E. Iswandy, "Perancangan Remote Site Mikrotik dengan VPN (PPPoE) Menggunakan Rest Api di SMA Muhammadiyah 3 Padang," *J. Pustaka Robot Sister (Jurnal Pus. Akses Kaji. Robot. Sist. Tertanam, dan Sist. Terdistribusi)*, vol. 2, no. 1, pp. 5–11, 2024, doi: 10.55382/jurnalpustakarobotsister.v2i1.378.

[13] M. A. Amirulloh, Basuki, F. S. Hadi, and D. A. R. Wati, "Pengembangan Trainer Air Conditioner Split Daya 1 PK Berbasis Internet of Things (IoT)," *J. Inform. Multimed. dan Tek.*, vol. 2, no. 1, pp. 1–6, 2025, doi: 10.71456/jimt.v2i1.1351.

[14] H. Pratama and N. F. Puspitasari, "Penerapan Protokol L2TP/IPSec dan Port Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP Implementation of L2TP / IPSec Protocol and Port Forwarding for Remote Mikrotik on Dynamic IP Networks," *Citec J.*, vol. 7, no. 1, pp. 51–62, 2020.

[15] H. A. Al-Atsari and I. Suharjo, "Integrasi Server On-Premise dengan Server Cloud Menggunakan Cloud VPN dan Mikrotik Ipsec Untuk Peningkatan Keamanan Koneksi," vol. 4, no. 11, pp. 1977–1996, 2023, doi: https://doi.org/10.46799/jsa.v4i11.757.

[16] P. Wicaksana, F. Hadi, and A. F. Hadi, "Perancangan Implementasi VPN Server Menggunakan Protokol L2TP dan IPSec Sebagai Keamanan Jaringan," *J. KomtekInfo*, vol. 8, no. 3, pp. 169–175, 2021, doi: 10.35134/komtekinfo.v8i3.128.

[17] F. M. Arianto, D. D. Maulana, and A. H. Zulfahmi, "Optimasi Rectifier Untuk Meningkatkan Kinerja Server Pada Pt.Garuda Media Telematika," *Elconika J. Tek. Elektro*, vol. 3, no. 1, pp. 15–21, 2024, doi: 10.33752/elconika.v3i1.8257.

[18] F. P. E. Putra, M. K. R.A, M. W. Ridho, and V. Huda, "Analisis Kinerja dan Keamanan Protokol PPTP dan L2TP/IPSec VPN pada Jaringan MikroTik," vol. 8, no. 2, pp. 334–344, 2025, doi: https://dx.doi.org/10.29408/jit.v8i2.30230.

[19] S. C. Prasath, N. Darwin, R. S. Ramkumar, S. Nithishkumar, and P. L. Somasundharam, "IoT-Powered UPS Battery Monitoring: Ensuring High availability and reliability for Critical Systems," *E3S Web Conf.*, vol. 399, pp. 1–8, 2023, doi: 10.1051/e3sconf/202339904007.

[20] F. P. E. Putra, M. Khairi, M. I. Hidayatullah, and I. Maulana, "Analisis Protokol Keamanan Jaringan dalam Era Internet of Things (IoT)," vol. 8, no. 2, pp. 356–366, 2025, doi: https://dx.doi.org/10.29408/jit.v8i2.30257