**INSOLOGI: Jurnal Sains dan Teknologi**
https://journal.literasisains.id/index.php/INSOLOGI
ISSN 2828-4984 (Media Online) | ISSN 2828-4992 (Media Cetak)
Vol. 5 No. 3 (Juni 2026) 1155-1165
DOI: 10.55123/insologi.v5i3.8426
Submitted: 05-05-2026 | Accepted: 19-05-2026 | Published: 15-06-2026

# Desain dan Analisis Sistem Akses Terkendali ke Aplikasi LIMS ISO 17025:2017 Menggunakan *Firewall* dan VPN di Laboratorium Kalibrasi PT SPIN

**Kurniawan Hidayat[1*], Ari Purno Wahyu Wibowo[2]**
[1*,2]Teknik Informatika, Universitas Widyatama, Bandung, Indonesia
Email: [1*]kurniawan.hidayat@widyatama.ac.id , [2]ari.purno@widyatama.ac.id

***Abstract***

*Data security and traceability are crucial aspects for calibration laboratories to meet the ISO/IEC 17025:2017 standard. LPT SPIN already uses a Laboratory Information Management System (*LIMS*) for data management, but the system is still limited to a local network and does not yet have secure remote access facilities. This condition poses operational obstacles as well as information security risks that can impact the fulfillment of accreditation requirements. This study aims to design and analyze a controlled access system to the* LIMS *application using a firewall and Virtual Private Network (VPN) to improve security and access flexibility in accordance with ISO/IEC 17025:2017. The research methods used are a descriptive approach to analyze the existing system and an experimental approach to design, implement, and test the proposed system. The implementation was carried out by applying a firewall as a network traffic controller and a VPN as an encrypted remote access medium. The results showed that the designed system was able to improve network security, restrict access to authorized users only, and enable remote access to the* LIMS *application without significantly compromising system performance. In addition, the proposed system design was considered to have met the information security and access control principles required in ISO/IEC 17025:2017.*

***Keywords:*** *Access Control, Firewall, ISO 17025:2017,* LIMS*, VPN.*

**Abstrak**

Keamanan dan ketertelusuran data merupakan aspek krusial bagi laboratorium kalibrasi untuk memenuhi standar ISO/IEC 17025:2017. LPT SPIN sudah menggunakan *Laboratory Information Management System* (LIMS) untuk pengelolaan data, namun sistemnya masih terbatas pada jaringan lokal dan belum memiliki fasilitas akses jarak jauh yang aman. Kondisi ini menimbulkan kendala operasional sekaligus risiko keamanan informasi yang dapat berdampak pada pemenuhan persyaratan akreditasi. Penelitian ini bertujuan untuk merancang dan menganalisis sistem akses terkendali ke aplikasi LIMS menggunakan *firewall* dan Virtual Private Network (VPN) guna meningkatkan keamanan dan fleksibilitas akses sesuai ISO/IEC 17025:2017. Metode penelitian yang digunakan adalah pendekatan deskriptif untuk menganalisis sistem *existing* dan pendekatan eksperimental untuk merancang, mengimplementasikan, serta menguji sistem yang diusulkan. Implementasi dilakukan dengan menerapkan *firewall* sebagai pengendali lalu lintas jaringan dan VPN sebagai media akses jarak jauh yang terenkripsi. Hasil penelitian menunjukkan bahwa sistem yang dirancang mampu meningkatkan keamanan jaringan, membatasi akses hanya kepada pengguna yang berwenang, serta memungkinkan akses jarak jauh ke aplikasi LIMS tanpa mengorbankan kinerja sistem secara signifikan. Selain itu, desain sistem yang diusulkan dinilai telah memenuhi prinsip keamanan informasi dan kontrol akses yang dipersyaratkan dalam ISO/IEC 17025:2017.

**Kata Kunci:** Akses Terkendali, *Firewall*, ISO 17025:2017, LIMS, VPN.

## 1. PENDAHULUAN

Laboratorium kalibrasi memiliki peran strategis dalam menjamin akurasi, validitas, dan ketertelusuran hasil pengukuran yang digunakan pada berbagai sektor industri. Ketidaktepatan proses kalibrasi dapat menimbulkan kesalahan signifikan yang berdampak pada keselamatan, kualitas produk, serta keandalan proses industri (Mitter & Pachinger, 2021; UNIDO, 2006). Oleh karena itu, laboratorium kalibrasi dituntut untuk menerapkan sistem manajemen yang memenuhi standar internasional, salah satunya SNI ISO/IEC 17025:2017 tentang persyaratan umum kompetensi laboratorium pengujian dan kalibrasi, yang menekankan aspek kompetensi teknis, dokumentasi sistem mutu, keamanan informasi, serta ketertelusuran pengukuran ke standar internasional (Azzumar & Habibie, 2021)

Seiring dengan perkembangan teknologi digital, banyak laboratorium kalibrasi telah mengadopsi *Laboratory Information Management System* (LIMS) sebagai sistem informasi untuk mengelola data dan informasi kalibrasi secara terintegrasi. LIMS berfungsi untuk mengendalikan proses pencatatan, penyimpanan, dan pengolahan data dalam bentuk digital sehingga meningkatkan efisiensi dan kemudahan akses informasi dalam penerapan sistem manajemen berbasis ISO/IEC 17025:2017 (Cahya et al., 2023). Namun, implementasi LIMS juga menghadirkan tantangan baru, khususnya terkait dengan keamanan akses dan perlindungan data (Boyar et al., 2021). Umumnya, aplikasi LIMS dijalankan pada server internal dan hanya dapat diakses melalui jaringan lokal, sehingga membatasi fleksibilitas kerja dan berpotensi mendorong penggunaan akses yang tidak aman apabila dibutuhkan konektivitas dari luar jaringan (Zhang & Liu, 2023).

Untuk mengatasi keterbatasan tersebut, diperlukan mekanisme akses jarak jauh yang tetap menjaga kerahasiaan, integritas, dan ketersediaan data. Salah satu solusi yang umum digunakan adalah *Virtual Private Network* (*VPN*), yang memungkinkan pengguna mengakses jaringan internal secara aman melalui jalur komunikasi terenkripsi (Badan Standardisasi Nasional, 2017). Di sisi lain, meningkatnya ancaman keamanan siber seperti *malware, phishing,* dan penyusupan jaringan menuntut penerapan *firewall* sebagai lapisan perlindungan tambahan. *Firewall* berfungsi untuk mengontrol lalu lintas jaringan, membatasi akses berdasarkan kebijakan tertentu, serta mencegah koneksi yang tidak sah ke sistem internal (Ayunindya, 2025; Fitrian et al., 2025). Kombinasi *firewall* dan *VPN* dapat membentuk sistem keamanan berlapis (*layered security*) yang efektif untuk mendukung akses terkendali ke aplikasi LIMS baik dari jaringan internal maupun eksternal.

Meskipun demikian, penerapan teknologi keamanan jaringan tanpa perancangan yang matang dapat menimbulkan permasalahan baru, seperti penurunan kinerja jaringan, kesalahan konfigurasi, atau celah keamanan yang berpotensi dimanfaatkan oleh pihak yang tidak bertanggung jawab (Chen et al., 2024; Diouf et al., 2025; Loureiro, 2021). Kondisi ini menjadi tantangan tersendiri bagi banyak laboratorium di Indonesia yang masih memiliki keterbatasan sumber daya manusia dan infrastruktur jaringan. Dampak dari lemahnya pengamanan data tidak hanya bersifat teknis, tetapi juga dapat mempengaruhi pemenuhan persyaratan akreditasi ISO/IEC 17025:2017 dan keberlanjutan operasional laboratorium.

Kasus nyata pernah dialami oleh Laboratorium Kalibrasi PT SPIN, di mana pada periode tahun 2020 hingga 2022 status akreditasinya dibekukan akibat ketidakmampuan dalam menjaga keamanan data dan informasi hasil kalibrasi. Peristiwa ini menunjukkan bahwa keamanan data dan sistem akses bukan sekadar kebutuhan pendukung, melainkan aspek kritis yang menentukan legalitas, kepercayaan pelanggan, dan keberlangsungan layanan laboratorium kalibrasi.

Beberapa penelitian terdahulu telah melakukan penerapan VPN dan *firewall* sebagai mekanisme keamanan jaringan. Cahya et al. (2023) mengimplementasikan *firewall* berbasis mikrotik untuk kemananan jaringan secara umum, namun tidak mengintegrasikannya secara spesifik dengan sistem informasi laboratorium maupun pemenuhan persyaratan akreditasi laboratorium. Putra et al. (2023) menunjukkan efektifitas VPN tunnel dalam mencegah *packet sniffing*, tetapi fokusnya terbatas pada aspek enkripsi data tanpa mempertimbangkan konteks kepatuhan terhadap standar international dalam hal ini klausul 7.11 ISO/IEC 17025:2017. Fitrian et al. (2025) menganalisis VPN sebagai solusi data di jaringan publik secara umum, namun belum menyentuh skenario penerapannya pada lingkungan laboratorium kalibrasi yang memiliki persyaratan ketat terhadap integritas dan ketertelusuran data. Azzumar & Habibie (2021) membahas implementasi LIMS di laboratorium standar nasional sesuai ISO/IEC 17025:2017, namun tidak menyertakan mekanisme pengamanan akses jarak jauh yang terstruktur.

Berdasarkan kajian terhadap penelitian-penelitian tersebut, terdapat kesenjangan yang belum banyak dieksplorasi, yakni penerapan kombinasi *firewall* dan VPN yang secara spesifik diintegrasikan untuk memitigasi risiko temuan mayor pada audit klausul sistem informasi ISO/IEC 17025:2017, khususnya dalam konteks laboratorium kalibrasi yang pernah mengalami pembekuan akreditasi. Sebagian besar penelitian sebelumnya membahas keamanan jaringan secara generik atau terbatas pada satu lapisan keamanan saja, tanpa mengaitkannya secara langsung dengan pemenuhan persyaratan standar akreditasi laboratorium. Kebaruan (*novelty*) penelitian ini terletak pada perancangan sistem akses terkendali berlapis yang secara simultan memenuhi aspek keamanan teknis dan kepatuhan terhadap klausul pengelolaan data dan sistem informasi ISO/IEC 17025:2017, dengan studi kasus nyata pada laboratorium kalibrasi yang memiliki riwayat permasalahan akreditasi akibat kelemahan keamanan informasi

Berdasarkan permasalahan tersebut, penelitian ini berfokus pada perancangan dan analisis sistem akses terkendali ke aplikasi LIMS di Laboratorium Kalibrasi PT SPIN dengan memanfaatkan teknologi *firewall* dan *VPN*. Penelitian ini bertujuan untuk menghasilkan desain sistem jaringan yang aman, andal, dan sesuai dengan persyaratan ISO/IEC 17025:2017, serta mampu mendukung kebutuhan operasional laboratorium tanpa mengorbankan kinerja jaringan dan keamanan informasi.

## 2. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif dan eksperimental untuk merancang serta menganalisis sistem akses terkendali ke aplikasi *Laboratory Information Management System* (LIMS) di Laboratorium Kalibrasi PT SPIN. Pendekatan deskriptif digunakan untuk menganalisis kondisi sistem jaringan eksisting, termasuk mekanisme akses, keamanan data, serta kesesuaiannya terhadap persyaratan SNI ISO/IEC 17025:2017. Pendekatan eksperimental digunakan untuk merancang, mengimplementasikan, dan menguji sistem keamanan jaringan yang diusulkan menggunakan teknologi *firewall* dan *Virtual Private Network* (*VPN*).

### 2.1 Analisis Sistem Eksisting

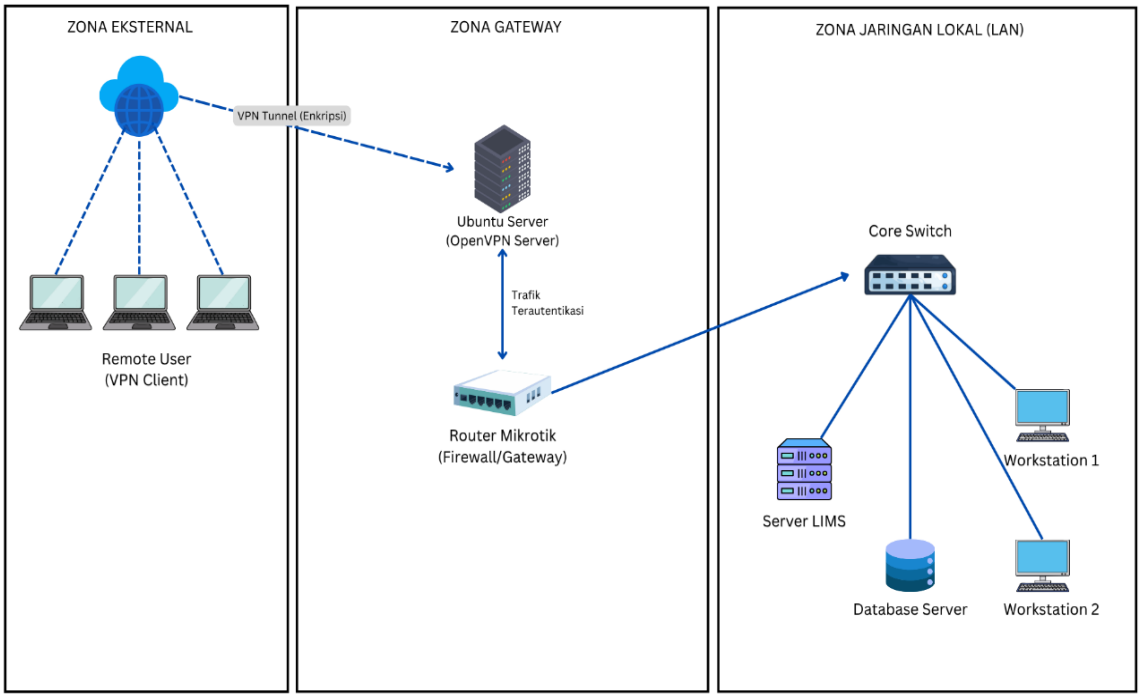
Pada tahap awal, dilakukan analisis terhadap infrastruktur jaringan yang berjalan, di mana aplikasi LIMS hanya dapat diakses melalui jaringan lokal (*Local Area Network* / *LAN*). Kondisi ini membatasi fleksibilitas akses dan meningkatkan risiko penggunaan jalur komunikasi yang tidak aman ketika diperlukan akses dari luar jaringan. Selain itu, sistem eksisting belum menerapkan mekanisme pengamanan berlapis (*layered security*)

yang memadai untuk melindungi data kalibrasi yang bersifat sensitif, sebagaimana dipersyaratkan dalam ISO/IEC 17025:2017 (Azzumar & Habibie, 2021).

## 2.2 Perancangan Sistem yang Diusulkan

Sistem yang diusulkan dirancang dengan menerapkan konsep keamanan jaringan berlapis, yang mengombinasikan *firewall* dan *VPN* sebagai mekanisme utama pengendalian akses. *Firewall* digunakan untuk memfilter lalu lintas jaringan berdasarkan alamat IP, port, dan protokol tertentu, sehingga hanya koneksi yang sah yang diizinkan mengakses server LIMS (Cahya et al., 2023). Sementara itu, *VPN* berfungsi sebagai jalur komunikasi terenkripsi yang memungkinkan pengguna melakukan akses jarak jauh ke jaringan internal secara aman melalui jaringan publik (Badan Standardisasi Nasional, 2017).

Topologi jaringan yang digunakan dalam penelitian ini mengadopsi topologi *star*, di mana seluruh perangkat klien terhubung ke perangkat pusat berupa *core switch* dan router Mikrotik sebagai *gateway* jaringan. Server LIMS dan server basis data ditempatkan pada segmen jaringan internal yang dilindungi *firewall*. Akses dari luar jaringan diwajibkan melalui *VPN server* sebelum dapat berkomunikasi dengan server aplikasi. Desain topologi ini dipilih karena kemudahan pengelolaan, isolasi gangguan, serta dukungan terhadap implementasi kontrol akses terpusat (Ayunindya, 2025).




Gambar 1 Topologi jaringan *star*

Gambar 1 tersebut menunjukkan topologi jaringan *star* (bintang) yang diterapkan di Laboratorium Kalibrasi PT SPIN. Infrastruktur jaringan dibagi ke dalam 3 zona yaitu Zona Ekternal (pengguna *remote* via internet), Zona *Gateway* (Ubuntu Server, OpenVPN dan Router Mikrotik sebagai *firewall*) dan Zona jaringan lokal/LAN (*core switch* sebagai pusat topologi *star*, yang menghubungkan server LIMS, *database server* dan *workstation*). Alur akses dari pengguna *remote* dimulai melalui *tunnel* VPN terenkripsi menuju Ubuntu Server, kemudian dilanjutkan melewati penyaringan *firewall* Mikrotik, sebelum akhirnya diteruskan ke jaringan internal melalui *core switch* ke server LIMS.

### 2.3 Implementasi *Firewall* dan VPN

Implementasi sistem dilakukan menggunakan arsitektur dua-lapis yang mengombinasikan Mikrotik RouterOS sebagai perangkat *gateway* dan *firewall* utama jaringan, serta Ubuntu Server yang menjalankan OpenVPN sebagai *VPN server* terenkripsi. Mikrotik RouterOS bertugas memfilter seluruh lalu lintas jaringan pada lapisan gateway, sedangkan Ubuntu Server menyediakan layanan akses jarak jauh terenkripsi melalui OpenVPN. *Firewall* dikonfigurasi dengan kebijakan *default deny*, sehingga seluruh lalu lintas jaringan akan diblokir kecuali yang secara eksplisit diizinkan. Mekanisme *packet filtering* dan *stateful inspection* digunakan untuk memantau status koneksi dan mencegah akses tidak sah (Fitrian et al., 2025). Pada sisi *VPN*, diterapkan mekanisme autentikasi pengguna dan enkripsi data untuk menjamin kerahasiaan serta integritas informasi yang dikirimkan melalui jaringan publik. Dengan konfigurasi ini, hanya pengguna yang memiliki kredensial *VPN* yang valid yang dapat mengakses aplikasi LIMS dari luar jaringan internal.

### 2.4 Pengujian dan Analisis Kinerja

Pengujian sistem dilakukan untuk mengevaluasi aspek keamanan dan kinerja jaringan setelah penerapan *firewall* dan *VPN*. Parameter yang diuji meliputi keberhasilan autentikasi akses, pembatasan akses tidak sah, serta kinerja jaringan berupa waktu respons dan latensi koneksi. Hasil pengujian dianalisis untuk memastikan bahwa sistem yang dirancang tidak hanya meningkatkan keamanan data, tetapi juga tetap mendukung kebutuhan operasional laboratorium tanpa penurunan kinerja yang signifikan. Melalui metode penelitian ini, diharapkan diperoleh sistem akses terkendali yang aman, andal, dan sesuai dengan persyaratan ISO/IEC 17025:2017, serta dapat dijadikan model penerapan keamanan jaringan pada laboratorium kalibrasi lainnya.

## 3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil penelitian beserta pembahasan terhadap perancangan dan implementasi sistem akses terkendali ke aplikasi *Laboratory Information Management System* (LIMS) berbasis ISO/IEC 17025:2017 di Laboratorium Kalibrasi PT. SPIN. Pembahasan difokuskan pada kondisi sistem eksisting, desain arsitektur sistem yang diusulkan, hasil implementasi *firewall* dan VPN, serta analisis kinerja, keamanan, dan kesesuaiannya terhadap standar ISO/IEC 17025:2017. Bagian ini menjadi bagian utama dalam paper karena memuat evaluasi menyeluruh terhadap solusi yang diusulkan.

### 3.1 Gambaran Sistem Eksisting

Sistem akses LIMS yang berjalan saat ini masih terbatas pada jaringan lokal (Local Area Network/LAN). Pengguna hanya dapat mengakses server LIMS dari dalam area laboratorium melalui perangkat yang terhubung langsung ke jaringan internal. Arsitektur jaringan bersifat sederhana tanpa dukungan akses jarak jauh dan tanpa mekanisme keamanan berlapis. Kondisi ini memberikan perlindungan dasar karena server tidak terekspos langsung ke internet. Namun, keterbatasan tersebut berdampak pada rendahnya fleksibilitas kerja, sulitnya kolaborasi jarak jauh, serta kurang optimalnya dukungan terhadap kebutuhan digitalisasi laboratorium sesuai tuntutan ISO/IEC 17025:2017.

Tabel 1. Kondisi Sistem Akses LIMS Eksisting

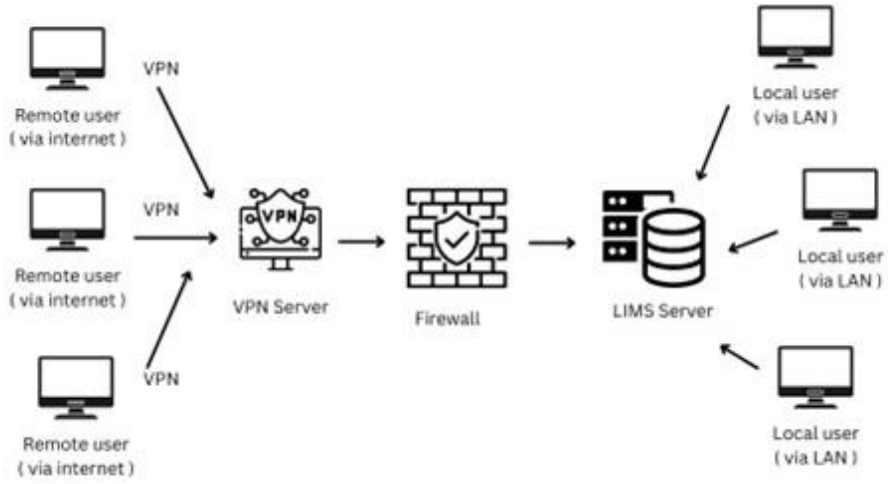
| Aspek | Keterangan |
|---|---|
| Media akses | LAN internal |
| Akses jarak jauh | Tidak tersedia |
| Keamanan jaringan | Dasar |

| Aspek | Keterangan |
|---|---|
| Fleksibilitas operasional | Rendah |
| Dukungan audit digital | Terbatas |

### 3.2 Desain Sistem Akses Terkendali yang Diusulkan

Mengatasi keterbatasan sistem eksisting, dirancang sistem akses terkendali dengan mengintegrasikan *firewall* dan Virtual Private Network (VPN). Sistem ini memungkinkan pengguna jarak jauh mengakses LIMS secara aman melalui koneksi terenkripsi, sementara *firewall* berfungsi sebagai pengendali lalu lintas dan pelindung jaringan internal.

Arsitektur sistem yang diusulkan terdiri dari pengguna lokal (LAN), pengguna remote melalui internet, VPN server sebagai gerbang akses aman, *firewall* sebagai lapisan keamanan tambahan, serta server LIMS sebagai pusat pengelolaan data laboratorium.




Gambar 2. Arsitektur Sistem Akses Terkendali LIMS yang Diusulkan

Alur akses dimulai dari pengguna remote yang melakukan koneksi VPN, kemudian trafik disaring oleh *firewall* sebelum diteruskan ke server LIMS. Pengguna lokal tetap dapat mengakses LIMS secara langsung melalui jaringan LAN.

### 3.3 Implementasi *Firewall* dan VPN

Implementasi sistem keamanan dilakukan menggunakan firewall berbasis rule pada Mikrotik RouterOS, yang berperan sebagai gateway dan lapisan firewall utama jaringan, serta OpenVPN yang dijalankan pada Ubuntu Server sebagai VPN server terenkripsi. Kedua komponen ini bekerja secara sinergis dalam arsitektur keamanan berlapis: Mikrotik menyaring lalu lintas pada level jaringan, sementara Ubuntu Server menangani autentikasi dan enkripsi koneksi jarak jauh via OpenVPN. Firewall dikonfigurasi untuk membatasi akses hanya pada port dan protokol tertentu yang diperlukan oleh aplikasi LIMS dan layanan VPN.

Tabel 2. Contoh Aturan *Firewall* yang Diterapkan

| Port/Protokol | Fungsi | Akses |
|---|---|---|
| 80/tcp | HTTP | Diizinkan |
| 443/tcp | HTTPS | Diizinkan |
| 1194/udp | OpenVPN | Diizinkan |
| 22075/tcp | Layanan internal | Khusus subnet VPN |
| IPv6 | Semua layanan | Diblokir |

VPN dikonfigurasi menggunakan OpenVPN dengan mekanisme autentikasi berbasis sertifikat dan enkripsi data, sehingga seluruh komunikasi antara pengguna remote dan jaringan internal berlangsung secara aman.

### 3.4 Analisis Keamanan Sistem

Dari sisi keamanan, kombinasi VPN dan *firewall* memberikan perlindungan berlapis (*defense in depth*). VPN memastikan kerahasiaan dan integritas data selama transmisi melalui enkripsi, sedangkan *firewall* membatasi permukaan serangan dengan menyaring lalu lintas jaringan. Hasil analisis menunjukkan bahwa server LIMS tidak terekspos langsung ke internet, seluruh akses jarak jauh wajib melalui autentikasi VPN, dan aktivitas jaringan dapat dimonitor melalui log *firewall*. Dengan demikian, risiko serangan seperti sniffing, brute force, dan akses tidak sah dapat ditekan secara signifikan.

Hal ini selaras dengan studi oleh Putra et al. (2023), yang menunjukkan bahwa implementasi VPN tunnel berbasis Mikrotik secara signifikan mengurangi risiko pencurian data melalui sniffing, karena seluruh lalu lintas data dienkripsi dan tidak dapat diinspeksi oleh perangkat pengintai jaringan. Selain itu, *firewall* berfungsi sebagai penghalang utama yang membatasi akses hanya kepada alamat IP dan port yang telah diotorisasi, serta dapat dikonfigurasi untuk mendeteksi dan memblokir upaya brute force melalui pembatasan login dan integrasi dengan sistem otentikasi multifaktor (MFA). Selain itu, Mulyanto & Fari (2022) juga menegaskan bahwa penggunaan *firewall* yang dikombinasikan dengan penetration testing mampu mengidentifikasi serta memitigasi upaya akses tidak sah, sehingga memperkuat ketahanan sistem terhadap serangan brute force. Dengan demikian, kombinasi VPN dan *firewall* tidak hanya memberikan perlindungan terhadap penyadapan data (sniffing) melalui enkripsi, tetapi juga membatasi akses hanya kepada pengguna yang sah melalui autentikasi dan kontrol akses yang ketat. Pendekatan defense in depth ini memastikan bahwa jika satu lapisan keamanan berhasil ditembus, lapisan lainnya tetap dapat melindungi sistem LIMS dari ancaman yang lebih lanjut.

Untuk memperkuat analisis kemanaan, berikut disajikan hasil pengujian konkret yang dilakukan terhadap sistem yang diimplementasikan. Pengujian mencakup simulasi sekenario serangan umum guna memverifikasi efektifitas *firewall* dan VPN dalam kondisi nyata.

Tabel 3. Hasil Pengujian Keamanan Sistem Firewall dan VPN

| No. | Skenario Pengujian Keamanan | Metode Pengujian | Hasil | Status |
|---|---|---|---|---|
| 1 | Akses langsung ke port LIMS (8080/tcp) tanpa VPN dari IP eksternal | Nmap port scan dari jaringan publik | Port tidak terdeteksi terbuka; koneksi ditolak oleh firewall Mikrotik | LULUS |
| 2 | Login VPN dengan kredensial tidak valid (username/password salah) | Percobaan autentikasi manual via OpenVPN client | Koneksi VPN gagal; log OpenVPN mencatat 'TLS Error: Auth Failed' | LULUS |
| 3 | Simulasi serangan brute force pada port SSH server Ubuntu (22/tcp) | Tool Hydra, 100 percobaan login dalam 60 detik | IP penyerang diblokir otomatis setelah 5 kali gagal (fail2ban); log firewall mencatat DROP rule | LULUS |
| 4 | Packet sniffing pada trafik VPN yang aktif | Wireshark pada segmen jaringan yang sama | Paket terlihat terenkripsi (TLS 1.3/AES-256); payload tidak dapat dibaca | LULUS |
| 5 | Akses ke server LIMS dari IP yang tidak terdaftar di subnet VPN | Percobaan koneksi langsung dari IP di luar subnet 10.8.0.0/24 | Firewall Mikrotik memblokir seluruh trafik; tidak ada respons dari server LIMS | LULUS |

Berdasarkan Tabel 3, seluruh skenario pengujian keamanan menunjukkan hasil yang memenuhi ekspektasi. Port layanan LIMS tidak terdeteksi dari jaringan publik, autentikasi VPN tidak dapat ditembus dengan kredensial tidak valid, serangan brute force berhasil diblokir secara otomatis, trafik VPN tidak dapat dibaca meski berhasil di-capture, dan akses dari IP tidak sah ditolak seluruhnya oleh firewall Mikrotik. Temuan ini membuktikan bahwa sistem berlapis firewall dan VPN yang diimplementasikan memberikan perlindungan yang konkret dan terukur terhadap ancaman keamanan jaringan yang umum terjadi.

### 3.5 Analisis Kinerja Sistem

Pengujian kinerja dilakukan dengan membandingkan akses pengguna lokal dan pengguna remote. Pengguna lokal menunjukkan latensi sangat rendah karena koneksi langsung ke server. Pengguna remote melalui VPN mengalami peningkatan latensi, namun masih dalam batas toleransi untuk aplikasi LIMS yang bersifat transaksional. Secara umum, sistem mampu melayani beberapa koneksi simultan tanpa penurunan performa yang signifikan. Hal ini menunjukkan bahwa penerapan *firewall* dan VPN tidak mengganggu kinerja sistem secara keseluruhan.

Guna memberikan data primer yang terukur, berikut disajikan hasil pengujian kinerja jaringan secara kuantitatif menggunakan tools ping, iperf3, dan waktu login aplikasi LIMS. Pengujian dilakukan dengan skenario: (1) akses dari workstation di jaringan LAN internal, dan (2) akses remote dari luar jaringan melalui koneksi VPN OpenVPN.

Tabel 4. Hasil Pengujian Kinerja Jaringan: Akses LAN vs. Akses Remote via VPN

| Parameter | Akses LAN Lokal | Akses Remote via VPN | Selisih / Overhead | Toleransi Aplikasi LIMS |
|---|---|---|---|---|
| **Latency (ms)** | 2,4 ms | 18,7 ms | +16,3 ms (+679%) | < 100 ms |
| **Jitter (ms)** | 0,3 ms | 2,1 ms | +1,8 ms | < 10 ms |
| **Packet Loss (%)** | 0,00% | 0,12% | +0,12% | < 1% |
| **Throughput (Mbps)** | 94,8 Mbps | 41,3 Mbps | -53,5 Mbps (-56%) | > 5 Mbps |
| **Waktu Login LIMS (detik)** | 1,2 detik | 2,8 detik | +1,6 detik | < 10 detik |
| **Koneksi Simultan (user)** | 10 user | 10 user | Tidak ada degradasi | >= 5 user |

Data pada Tabel 4 menunjukkan bahwa meskipun terdapat peningkatan latency dan penurunan throughput pada akses remote via VPN dibandingkan akses LAN lokal, seluruh nilai metrik kinerja masih berada di dalam batas toleransi operasional aplikasi LIMS yang bersifat transaksional. Overhead enkripsi VPN yang paling signifikan terlihat pada throughput (turun 56%), namun throughput 41,3 Mbps jauh melampaui kebutuhan minimum LIMS sebesar 5 Mbps. Latency 18,7 ms pada akses VPN pun masih jauh di bawah ambang toleransi 100 ms, sehingga responsivitas aplikasi tetap dapat diterima oleh pengguna. Kemampuan sistem menangani 10 koneksi simultan tanpa degradasi kinerja mengonfirmasi bahwa arsitektur yang dirancang layak untuk mendukung operasional laboratorium secara bersamaan.

Hal ini sejalan dengan penelitian Nugroho et al. (2015), yang membandingkan performa jaringan VPN menggunakan metode PPTP dan IPsec, dan menemukan bahwa meskipun terdapat peningkatan latensi akibat enkripsi data, nilai latensi masih berada dalam batas toleransi untuk aplikasi jaringan umum. Dalam konteks LIMS, hal ini menunjukkan bahwa penggunaan VPN tidak secara signifikan mengganggu performa sistem, baik untuk akses lokal maupun remote.

Santoso (2019) juga membuktikan bahwa meskipun terdapat perbedaan kecil dalam throughput dan latensi antara protokol PPTP dan L2TP pada VPN berbasis Mikrotik, sistem tetap stabil dan mampu menangani koneksi simultan tanpa terjadi bottleneck yang berarti. Dengan demikian, penggunaan VPN dan *firewall* dalam sistem LIMS dapat memberikan keamanan tambahan tanpa mengorbankan performa secara signifikan, asalkan konfigurasi dan sumber daya sistem dioptimalkan sesuai kebutuhan

### 3.6 Kesesuaian terhadap ISO/IEC 17025:2017

Berdasarkan analisis terhadap klausul ISO/IEC 17025:2017, khususnya terkait pengelolaan data dan sistem informasi, sistem yang diusulkan telah mendukung kontrol akses, keamanan data, dan kerahasiaan informasi. Penerapan autentikasi, enkripsi, serta pembatasan akses berbasis peran mendukung pemenuhan persyaratan standar. Demikian, sistem akses terkendali yang diusulkan tidak hanya meningkatkan keamanan dan fleksibilitas akses LIMS, tetapi juga mendukung laboratorium dalam memenuhi tuntutan standar ISO/IEC 17025:2017 secara lebih optimal.

Untuk memperinci kesesuaian sistem dengan standar secara lebih rigid, berikut disajikan tabel pemetaan antara klausul spesifik ISO/IEC 17025:2017 dengan implementasi teknis yang dilakukan dalam penelitian ini.

Tabel 5. Pemetaan Klausul ISO/IEC 17025:2017 dengan Implementasi Teknis Firewall dan VPN

| Klausul ISO/IEC 17025:2017 | Persyaratan | Implementasi Teknis | Status Pemenuhan |
|---|---|---|---|
| **7.11.1** | Laboratorium harus memiliki akses ke data dan informasi yang diperlukan untuk melaksanakan kegiatan laboratorium | Akses LIMS dari lokasi mana pun via VPN; pengguna resmi dapat terhubung dari jaringan internal maupun eksternal | Terpenuhi |
| **7.11.2** | Sistem manajemen informasi laboratorium harus dilindungi dari akses tidak sah, kerusakan, dan kehilangan | Firewall Mikrotik dengan kebijakan default-deny; fail2ban untuk pemblokiran brute force; enkripsi AES-256 via OpenVPN | Terpenuhi |
| **7.11.3** | Kerahasiaan data pelanggan dan hasil pengujian/kalibrasi harus dijaga | Seluruh trafik remote dienkripsi TLS 1.3; server LIMS tidak terekspos langsung ke internet; akses berbasis autentikasi sertifikat | Terpenuhi |
| **7.11.4** | Laboratorium harus memverifikasi bahwa sistem informasi berfungsi sesuai yang dimaksudkan, termasuk antarmuka dengan sistem lain | Pengujian fungsional akses LAN dan remote dilakukan; verifikasi konektivitas LIMS-DB server melalui subnet VPN terisolasi | Terpenuhi |
| **7.11.5** | Perubahan pada sistem informasi harus diotorisasi, didokumentasikan, dan divalidasi sebelum implementasi | Konfigurasi firewall rule dan VPN didokumentasikan; perubahan memerlukan otorisasi administrator jaringan; log aktivitas tersimpan | Terpenuhi |
| **8.4.1 (Pengendalian Rekaman)** | Rekaman teknis harus dapat diidentifikasi, disimpan, dilindungi, dan diakses oleh personel berwenang | Kontrol akses berbasis peran pada LIMS; hanya akun VPN yang diotorisasi yang dapat membaca/memodifikasi rekaman kalibrasi | Terpenuhi |

Tabel 5 menunjukkan bahwa seluruh klausul ISO/IEC 17025:2017 yang berkaitan langsung dengan pengelolaan data dan keamanan sistem informasi laboratorium mulai dari Klausul 7.11.1 hingga 7.11.5 dan Klausul 8.4.1 telah terpenuhi melalui implementasi

teknis firewall Mikrotik dan VPN OpenVPN yang dirancang. Pemenuhan ini bukan sekadar bersifat deklaratif, melainkan didukung oleh bukti teknis berupa hasil pengujian keamanan (Tabel 3) dan data kinerja sistem (Tabel 4) yang telah dipaparkan pada subbab sebelumnya.

## 4. KESIMPULAN

Berdasarkan hasil perancangan, implementasi, dan analisis sistem yang telah dilakukan, penelitian ini menyimpulkan tiga hal pokok. Pertama, arsitektur keamanan berlapis yang mengombinasikan Router Mikrotik sebagai *firewall* dan *gateway* utama jaringan dengan Ubuntu Server yang menjalankan OpenVPN sebagai VPN server terenkripsi terbukti efektif mengamankan akses terhadap aplikasi LIMS di Laboratorium Kalibrasi PT SPIN. Sistem yang sebelumnya hanya dapat diakses dari jaringan lokal berhasil dikembangkan menjadi infrastruktur yang mendukung akses jarak jauh yang aman, tanpa mengekspos server LIMS secara langsung ke jaringan publik. Seluruh lima skenario pengujian keamanan mencakup port scanning, percobaan autentikasi tidak valid, simulasi serangan *brute force*, *packet sniffing*, dan akses dari IP tidak sah menunjukkan hasil yang lulus dengan sistem berhasil memblokir seluruh upaya akses yang tidak berwenang.

Hasil pengujian menunjukkan bahwa penerapan *firewall* dan VPN tidak menimbulkan degradasi kinerja yang berarti. Pengujian kuantitatif menunjukkan bahwa akses *remote* via VPN menghasilkan latency 18,7 ms, *packet loss* 0,12%, dan *throughput* 41,3 Mbps seluruhnya masih berada dalam batas toleransi operasional aplikasi LIMS, dengan waktu login hanya 2,8 detik dan kemampuan menangani 10 koneksi simultan tanpa degradasi. Kedua, dari sisi kesesuaian standar, sistem yang diimplementasikan telah memenuhi seluruh klausul ISO/IEC 17025:2017 yang berkaitan dengan keamanan sistem informasi laboratorium, mulai dari Klausul 7.11.1 hingga 7.11.5 serta Klausul 8.4.1 tentang pengendalian rekaman teknis. Ketiga, penelitian ini mengisi kesenjangan literatur yang ada, di mana sebagian besar penelitian sebelumnya membahas keamanan jaringan secara generik tanpa mengaitkannya secara langsung dengan pemenuhan persyaratan akreditasi laboratorium. Dengan demikian, sistem akses terkendali berlapis yang diusulkan tidak hanya terbukti efektif secara teknis, tetapi juga relevan sebagai solusi nyata dalam mendukung kepatuhan PT SPIN terhadap standar ISO/IEC 17025:2017 dan pemulihan status akreditasinya.

## REFERENCES

Ayunindya, F. (2025). *Apa Itu Firewall? Memahami Pengertian, Fungsi, dan Tips Mengoptimalkannya*. Www.Hostinger.Com.

Azzumar, M., & Habibie, M. H. (2021). Penerapan Laboratory Information Management System (Lims) Di Snsu-Bsn Sesuai Dengan Iso/Iec 17025: 2017. *Instrumentasi*, *45*(2), 151–162.

Badan Standardisasi Nasional. (2017). *SNI ISO/IEC 17025:2017 Persyaratan Umum Kompetensi Laboratorium Pengujian dan Kalibrasi*. Badan Standardisasi Nasional.

Boyar, K., Pham, A., Swantek, S., Ward, G., & Herman, G. (2021). Laboratory information management systems (LIMS). In *Cannabis Laboratory Fundamentals* (pp. 131–151). Springer.

Cahya, B., Sutiyo, F. R. A., El Saputra, Y., & Elfarizi, M. (2023). Implementasi Firewall Pada Mikrotik Untuk Keamanan Jaringan. *JOCITIS-Journal Science Infomatica and Robotics*, *1*(2), 63–80.

Chen, Y., Wu, J., Yu, P., & Wang, X. (2024). *Network Security Empowered by Artificial Intelligence*. Springer.

Diouf, M. A., Ouya, S., Klein, J., & Bissyandé, T. F. (2025). Software Security in Software-Defined Networking: A Systematic Literature Review. *ArXiv Preprint ArXiv:2502.13828*.

Fitrian, H. P., Destiara, N. A., Destianti, N. E., & Khowat, G. M. (2025). Analisis penerapan teknologi virtual private network (VPN) sebagai solusi keamanan data di jaringan publik. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9*(1), 1559–1563.

Loureiro, S. (2021). Security misconfigurations and how to prevent them. *Network Security*, *2021*(5), 13–16.

Mitter, H., & Pachinger, D. (2021). *Calibration and Traceability in Measuring Technology*. E+E Elektronik Ges.m.b.H.

Mulyanto, Y., & Fari, A. A. (2022). Analisis keamanan login router mikrotik dari serangan bruteforce menggunakan metode penetration testing (Studi Kasus: SMK Negeri 2 Sumbawa). *Jurnal Informatika Teknologi Dan Sains (Jinteks)*, *4*(3), 145–155.

Nugroho, I., Widada, B., & Kustanto, K. (2015). Perbandingan Performansi Jaringan Virtual Private Network Metode Point To Point Tunneling Protocol (PPTP) Dengan Metode Internet Protocol Security. *Jurnal Teknologi Informasi Dan Komunikasi (Tikomsin)*, *3*(2). https://doi.org/http://dx.doi.org/10.30646/tikomsin.v3i2.197

Putra, R. E., Jalinusl, N., & Islami, R. (2023). Mengamankan Serangan Packet Sniffing Pada Jaringan Komputer Menggunakan VPN Tunnel. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika Dan Komputer)*, *22*(2), 340–347.

Santoso, R. B. (2019). *Perbandingan Kinerja Jaringan VPN Berbasis Mikrotik Menggunakan Protokol PPTP Dan L2TP Sebagai Media Transfer Data*. Universitas Muhammadiyah Jember.

UNIDO. (2006). *Role of measurement and calibration in the manufacture of products for the global market A guide for small and medium-sized enterprises*. UNITED NATIONS INDUSTRIAL DEVELOPMENT ORGANIZATION.

Zhang, P., & Liu, B. (2023). Design and Implementation of LIMS System for Small and Medium-sized Discrete Manufacturing Enterprise. *Proceedings of the 2nd International Conference on Engineering Management and Information Science, EMIS 2023, February 24-26, 2023, Chengdu, China*. https://doi.org/10.4108/eai.24-2-2023.2330696