INDEXIA: Informatic and Computational Intelligent Journal
Vol.08, No.01, Mei 2026, hlm. 11-22
P-ISSN: 2657-0424
E-ISSN: 2657-0432

IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN OUTLINE VPN BERBASIS VPS SERVER DI RSUD XYZ

Dany Achmad Maulana[1], Muhammad Faishol Amrulloh[2]*
[1, 2] Program studi teknik informatika, Universitas Yudharta Pasuruan
Jl. Yudharta No. 07 (Pesantren Ngalah) Sengonagung Purwosari Pasuruan Jawa Timur
e-mail: danyachmad75@gmail.com[1)], faishol@yudharta.ac.id[2)]
* corresponding author

(Naskah masuk : 07 Agustus 2025 Diterima untuk diterbitkan : 10 September 2025)

ABSTRAK

Keamanan jaringan merupakan aspek krusial dalam pengelolaan sistem informasi di rumah sakit, terutama dalam melindungi data pasien dan rekam medis, RSUD XYZ saat ini belum menerapkan Virtual *Private Network* (VPN) untuk mengamankan koneksi jaringan internalnya. Penelitian ini bertujuan untuk *mengimplementasikan* sistem keamanan jaringan menggunakan *Outline* VPN berbasis VPS Server sebagai solusi untuk meningkatkan perlindungan data dan akses jaringan rumah sakit. Adapun metode yang digunakan pada penelitian ini adalah menggunakan Outline VPN berbasis VPS pada Server di RSUD, Implementasi dilakukan dengan merancang dan mengonfigurasi *Outline* VPN pada VPS, serta menguji efektivitasnya dalam mengenkripsi dan mengamankan koneksi jaringan. hasil dari penelitian ini adalah *Outline* VPN berbasis VPS Server berhasil meningkatkan keamanan jaringan RSUD dengan mengenkripsi seluruh lalu lintas data dan membatasi akses hanya bagi pengguna dengan kunci akses, adapun hasil kuesioner dari 10 responden menunjukkan tingkat efektivitas sebesar 86,6% yang termasuk kategori sangat baik, sehingga penerapan sistem ini dinilai efektif dalam melindungi data sensitif.

***Kata Kunci**: Keamanan jaringan, Virtual Private Network, VPS Server.*

ABSTRACT

Network security is a crucial aspect in managing information systems in hospitals, especially in protecting patient data and medical records, XYZ Regional General Hospital currently has not implemented a Virtual Private Network (VPN) to secure its internal network connections. This study aims to implement a network security system using a VPS Server-based Outline VPN as a solution to improve data protection and hospital network access. The method used in this study is to use a VPS-based Outline VPN on a Server at the Regional General Hospital, Implementation is carried out by designing and configuring Outline VPN on a VPS, and testing its effectiveness in encrypting and securing network connections. The results of this study are that the VPS Server-based Outline VPN successfully improves the security of the Regional General Hospital network by encrypting all data traffic and limiting access only to users with access keys, while the results of the questionnaire from 10 respondents showed an effectiveness level of 86,6% which is included in the very good category, so the implementation of this system is considered effective in protecting sensitive data.

***Keywords**: Network security, Virtual Private Network, VPS Server.*

I. PENDAHULUAN

Perkembangan teknologi informasi di sektor kesehatan telah mengubah cara rumah sakit dalam mengelola data pasien dan pelayanan medis. Hampir seluruh aktivitas rumah sakit kini terintegrasi dalam Sistem Informasi Manajemen Rumah Sakit (SIMRS), mulai dari pendaftaran pasien, penyimpanan rekam medis elektronik, manajemen obat, hingga laporan administrasi dan keuangan. Di RSUD XYZ, sistem informasi tersebut menjadi tulang punggung operasional sehari-hari, sehingga keandalan dan keamanannya sangat krusial. Data pasien dan rekam medis merupakan informasi yang bersifat pribadi, sensitif, serta dilindungi undang-undang. Jika data ini bocor atau disalahgunakan, tidak hanya merugikan pasien tetapi juga menurunkan kepercayaan masyarakat terhadap layanan rumah sakit.

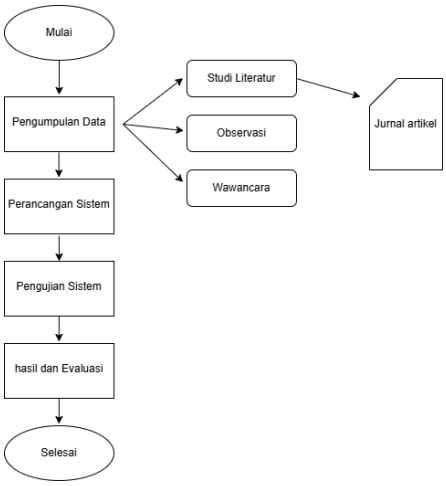
Hasil observasi dan studi kasus menunjukkan bahwa jaringan RSUD XYZ belum dilengkapi Virtual Private Network (VPN) sebagai lapisan pengamanan tambahan. Ketiadaan sistem VPN membuat lalu lintas data masih berjalan dalam bentuk yang rentan diakses oleh pihak tidak berwenang. Hal ini menimbulkan berbagai risiko, seperti potensi kebocoran data pasien, pencurian kredensial pengguna sistem, serta serangan sniffing dan man-in-the-middle attack yang memungkinkan peretas menyadap komunikasi jaringan. Realitas keamanan digital dalam dunia kesehatan di Indonesia menunjukkan bahwa ancaman nyata terhadap data pasien bukan sekadar teori. Misalnya, pada awal 2022, sekitar 6 juta data pasien yang mencakup hasil CT-scan, X-ray, tes COVID-19, serta informasi rumah sakit, dilaporkan bocor dan dijual secara online. Kondisi tersebut semakin berbahaya ketika staf rumah sakit mengakses sistem dari luar jaringan internal, misalnya untuk keperluan administratif jarak jauh, karena tanpa enkripsi pada lalu lintas data dapat dengan mudah diintersepsi. Jika masalah-masalah ini tidak segera diatasi, RSUD XYZ berisiko mengalami kebocoran data pasien maupun gangguan pada operasional sistem informasi rumah sakit.[1]

Untuk menjawab permasalahan tersebut, diperlukan solusi keamanan jaringan yang mampu melindungi lalu lintas data melalui proses enkripsi serta menyediakan kontrol akses yang lebih terstruktur. Salah satu teknologi yang dapat digunakan adalah Outline VPN berbasis Virtual Private Server (VPS). Outline VPN menawarkan konfigurasi yang sederhana, kompatibel dengan berbagai perangkat, serta memanfaatkan algoritma enkripsi yang kuat untuk menjaga kerahasiaan data. Selain itu, fitur manajemen berbasis access key memungkinkan administrator membatasi akses hanya kepada perangkat yang benar-benar berhak. Dengan dukungan VPS, sistem ini lebih fleksibel, mudah diatur, dan tidak bergantung pada layanan pihak ketiga yang berpotensi memiliki celah keamanan. Solusi ini juga memberikan keleluasaan bagi pihak rumah sakit untuk mengontrol sepenuhnya infrastruktur keamanannya secara mandiri. [2]

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada implementasi sistem keamanan jaringan menggunakan Outline VPN berbasis VPS Server di RSUD XYZ. Dengan menerapkan sistem ini, diharapkan rumah sakit mampu meningkatkan perlindungan data pasien dari risiko kebocoran maupun penyalahgunaan, menjaga kerahasiaan komunikasi jaringan internal maupun eksternal, serta mendukung kelancaran operasional SIMRS secara aman dan efisien. Penelitian ini juga diharapkan memberikan kontribusi nyata bagi pengembangan keamanan jaringan di lingkungan rumah sakit, sekaligus menjadi referensi bagi institusi kesehatan lain yang menghadapi permasalahan serupa dalam mengamankan data sensitif melalui pemanfaatan teknologi VPN berbasis VPS. [3]

II. METODE PENELITIAN

Penelitian ini menggunakan metode studi kasus dengan konsep studi kasus yang mendalam terhadap satu objek tertentu dalam jangka waktu tertentu, penelitian ini berfokus pada masalah keamanan jaringan RSUD dan penggunaan Outline VPN sebagai solusinya. Tahapan yang dilakukan yaitu tahap pengumpulan data, Merancang perangkat lunak, pengujian sistem, hasil dan evaluasi. Berikut adalah tahapan penelitian.[4]



Gambar 1. Tahapan Penelitian

A. Metode Pengumpulan Data

Sebelum pengolahan data, tahap awal melibatkan melakukan studi literatur dan melakukan wawancara dan observasi di lokasi penelitian untuk mendapatkan lebih banyak informasi tentang subjek penelitian yang berguna untuk melakukan penelitian atau mencari teori yang sesuai dengan masalah.[5]

1. Studi literatur

Studi literatur digunakan untuk mencari jurnal atau buku yang berkaitan dengan topik penelitian ini dengan tujuan mendapatkan referensi yang dapat digunakan dalam proses perancangan dan pembuatan sistem untuk memperdalam pemahaman tentang keamanan jaringan, VPN, dan VPS, serta memastikan bahwa penelitian ini memiliki kontribusi yang unik dan berbeda dari penelitian sebelumnya.

2. Observasi

Observasi dilakukan dengan cara mengunjungi lokasi secara langsung untuk melihat kondisi keamanan jaringan di RSUD XYZ sebelum dan sesudah penerapan Outline VPN berbasis VPS. Tinjauan ini dilakukan untuk memahami potensi ancaman keamanan, pola trafik jaringan, dan kemampuan VPN untuk meningkatkan keamanan data.

3. Wawancara

Wawancara dilakukan dengan salah satu staf it atau petugas yang menangani sistem keamanan jaringan yang ada di RSUD. Dilakukan wawancara untuk mendapatkan informasi tentang lokasi penelitian. Gambar dan Tabel

B. Analisis kebutuhan sistem

Dalam penelitian "Implementasi Sistem Keamanan Jaringan Menggunakan Outline VPN Berbasis VPS Server di RSUD XYZ", beberapa alat dan perangkat yang dibutuhkan meliputi perangkat keras (hardware) dan perangkat lunak (software) sebagai berikut:

1. Perangkat keras (hardware) Spesifikasi minimum:
   - Processor: Intel Core i5/AMD Ryzen 5 atau lebih tinggi
   - RAM: 8GB atau lebih
   - Storage: SSD 256GB atau lebih
   - OS: Windows/Linux/MacOS
2. Server VPS (Virtual Private Server) Penyedia VPS: Vultr, DigitalOcean, AWS, atau lainnya Spesifikasi minimum:
   - CPU: 1 vCPU atau lebih
   - RAM: 1GB atau lebih
   - Storage: 25GB SSD atau lebih
   - Bandwidth: 1TB atau lebih
3. Perangkat lunak (software)
   Software yang digunakan untuk implementasi VPN dan pengujian keamanan jaringan berikut beberapa software yang dibutuhkan:
   - Ubuntu/Debian Linux
   - Outline VPN Manager (untuk mengatur VPN di VPS)
   - Outline VPN Client (untuk koneksi VPN di perangkat pengguna)
   - Remote Desktop & SSH Client
   - PuTTY (Windows) / Terminal (Windows & Linux) Digunakan untuk mengakses dan mengelola VPS secara remote

C. Perancangan sistem

Dalam penelitian ini perancangan sistem dilakukan secara sistematis untuk memastikan bahwa solusi yang diterapkan efektif dalam meningkatkan keamanan jaringan rumah sakit.

1. Analisis kebutuhan sistem.
2. Instalasi dan konfigurasi vps dan Outline vpn.
3. Cara kerja dan penggunaan vpn.

Pengujian sistem

Pengujian sistem dalam penelitian ini sangat penting untuk memastikan bahwa VPN yang diimplementasikan benar-benar meningkatkan keamanan jaringan RSUD tanpa mengganggu performa dan kenyamanan pengguna. Pengujian dilakukan yang mencakup keamanan, kinerja, stabilitas jaringan,[6] kemudahan penggunaan. Adapun pengujian dilakukan dalam tiga aspek utama, yaitu pengujian enkripsi data, pengujian koneksi jaringan client-server, serta pengujian kecepatan akses internet sebelum dan sesudah menggunakan VPN.

1. Pengujian Enkripsi Data: Menggunakan Wireshark untuk menangkap paket data sebelum dan sesudah koneksi VPN diaktifkan.
2. Pengujian Koneksi Client–Server: Melihat apakah client dapat terhubung menggunakan access key yang telah dibuat.
3.Pengujian Kecepatan: Menggunakan Speedtest via web untuk membandingkan kecepatan download, upload, ping, dan jitter dalam kondisi VPN aktif dan nonaktif.

Rancangan Alur sistem

Pada tahap ini berfungsi untuk mengetahui skema perancangan alur sistem yang akan di terapkan pada penelitian ini yang dapat menghubungkan antara akses jaringan vpn server admin dan pengguna. Perancangan ini di mulai dari instalasi OS (operating system) menggunakan Ubuntu 22.04 LTS x 64 pada server vps, setelah Instalasi sistem operasi salin source code yang sudah di sediakan oleh Outline Manager untuk generate API key dari server VPS. [7]

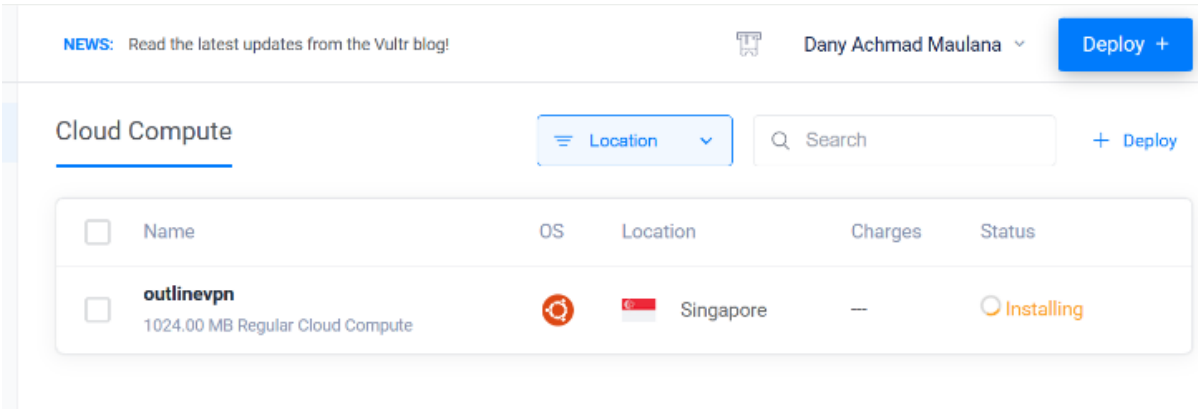
fungsi API sebagai jembatan pertukaran data antara server VPS dan Outline Manager sehingga Sistem aplikasi Outline Manager berhasil terkoneksi dengan server VPS maka akan ada (access key) atau kunci akses, fungsi kunci akses untuk manajemen perangkat yang akan di berikan akses koneksi ke VPN, kunci akses berbentuk API key yang dapat di pindah dari Outline Manager ke Outline client.[8]

III. HASIL DAN PEMBAHASAN

Implementasi Sistem

Pada bab ini menjelaskan implementasi sistem, hasil dari perancangan sistem yang berisi tentang langkah-langkah instalasi Outline VPN[9] di VPS hingga saling terkoneksi. Instalasi Outline VPN di VPS dimulai dengan menyediakan server virtual menggunakan layanan VPS seperti Vultr, kemudian menginstal sistem operasi berbasis Linux Ubuntu versi terbaru, untuk memastikan kompatibilitas dan keamanan. Setelah server siap, Memindahkan Script resmi Outline Manager yang akan digunakan untuk mengonfigurasi layanan VPN di VPS. [10]

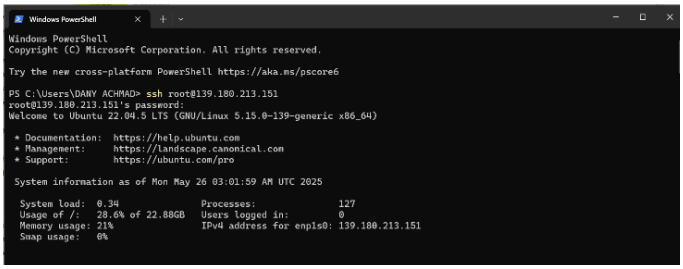
Setelah proses instalasi selesai, administrator dapat terkoneksi dengan server, mengelola koneksi dan membuat kunci akses untuk setiap pengguna guna untuk mengkoneksikan VPN,[11] memantau dan mengontrol trafik secara terpisah. Kemudian kunci akses ini dapat dibagikan kepada pengguna yang akan mengakses layanan VPN melalui aplikasi Outline Client, yang memungkinkan koneksi ke server VPN yang aman dan terenkripsi. tahap akhir yaitu pengujian sistem keamanan jaringan VPN dan koneksi jaringan.



Gambar 2. Instalasi Operating sistem

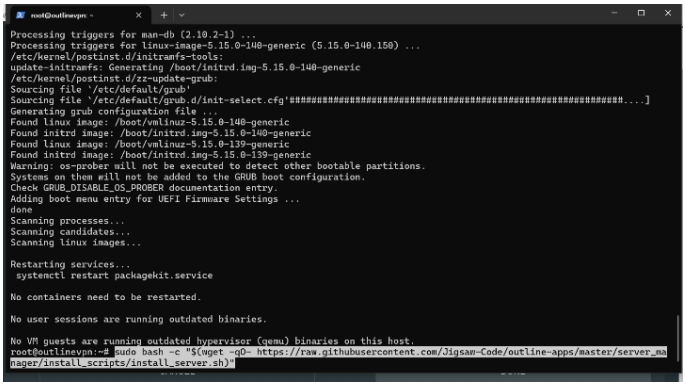
INDEXIA: Informatic and Computational Intelligent Journal
Vol.08, No.01, Mei 2026, hlm. 11-22
P-ISSN: 2657-0424
E-ISSN: 2657-0432

Setelah VPS dengan sistem operasi Ubuntu 22.04 LTS berhasil dibuat akan secara otomatis mendapatkan alamat IP publik, username (default: root), dan password root dari penyedia VPS.



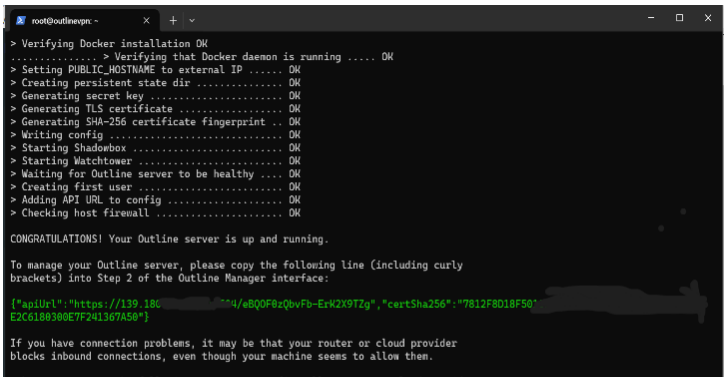
Gambar 3. Login ubuntu Server

Untuk login ke VPS menggunakan aplikasi SSH client. Di Windows, aplikasi populer yang digunakan adalah PuTTY, namun pada instalasi ini menggunakan Terminal Secure Shell, Tahap login memasukan IP Address VPS, Username: root Password root dengan ip server yang di gunakan saat ini 139.180.213.151 VPS menggunakan SSH Key, yang disiapkan saat instalasi sebelumnya.



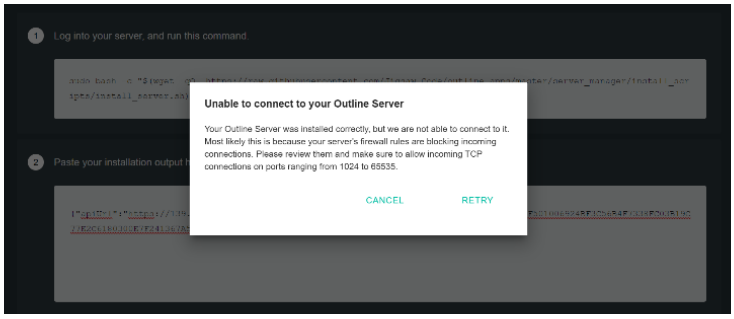
Gambar 4. Konfigurasi VPN Server

Instalasi Outline VPN Server dimulai setelah berhasil login ke VPS melalui koneksi SSH. administrator menjalankan perintah instalasi menggunakan skrip resmi dari Outline Manager yang sudah tersedia Skrip ini untuk mengunduh dan menginstal semua komponen yang diperlukan untuk menjalankan Outline Server, konfigurasi awal sistem dan pembuatan sertifikat keamanan.



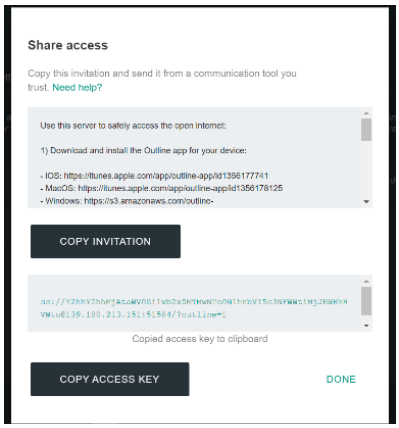
Gambar 5. API URL Outline Manager

Setelah Proses instalasi Outline VPN selesai, sistem akan menampilkan informasi konfigurasi server dalam bentuk API URL, alamat IP, port, serta SHA256 dari sertifikat keamanan. Informasi ini yang nantinya digunakan untuk menghubungkan Outline Manager ke Outline Server.

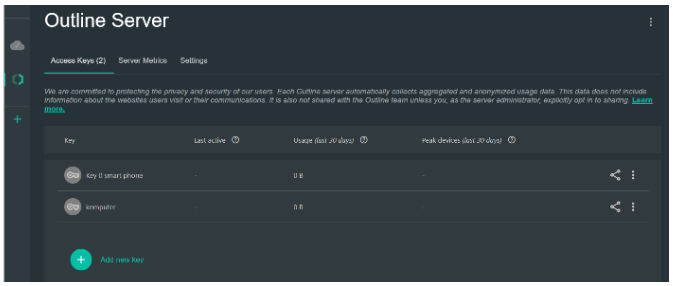


Gambar 6. Koneksi Outline Manager

Tautan API key tersebut, kemudian dimasukan ke dalam kolom input yang disediakan pada aplikasi Outline Manager. Setelah API key dimasukkan dengan benar, pengguna dapat menekan tombol "Connect" untuk memulai proses integrasi antara Outline Manager dan server. Jika koneksi berhasil, Outline Manager akan menampilkan antarmuka pengelolaan server VPN yang siap digunakan untuk konfigurasi lebih lanjut.



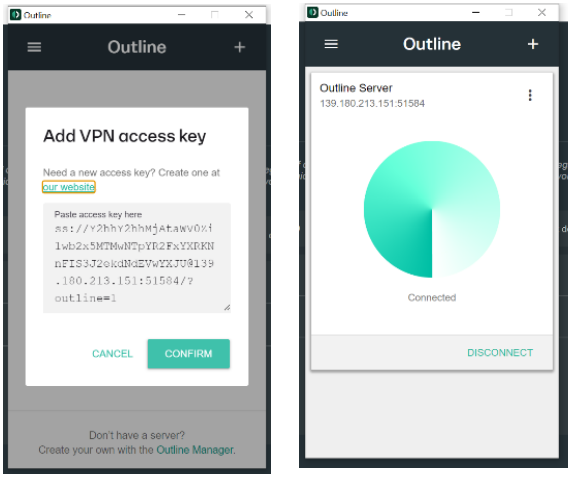
Gambar 7. Akses key Client



Gambar 8. Manajemen VPN

INDEXIA: Informatic and Computational Intelligent Journal
Vol.08, No.01, Mei 2026, hlm. 11-22
P-ISSN: 2657-0424
E-ISSN: 2657-0432

koneksi berhasil, Outline Manager akan menampilkan panel pengaturan server VPN. Melalui panel ini, pengguna dapat menambahkan access key untuk perangkat yang akan terhubung ke jaringan VPN, melihat statistik penggunaan data oleh setiap pengguna atau Client, serta mengatur akses, seperti membatasi atau menghapus access key yang sudah tidak digunakan.



Gambar 9. Koneksi Outline Client

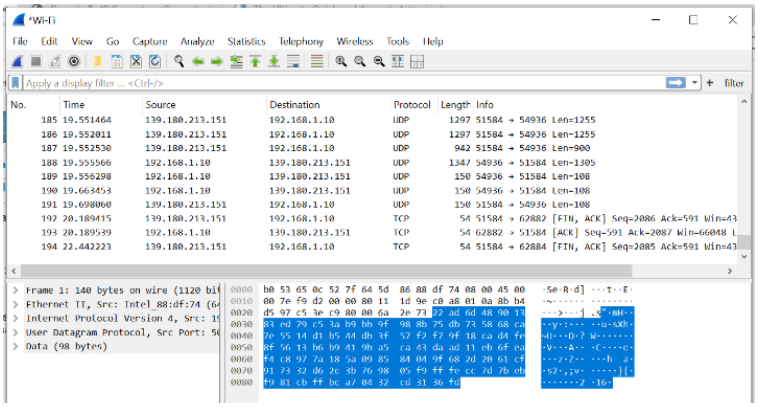
Setelah key access dibuat Outline Manager, selanjutnya menggunakan aplikasi Outline Client untuk menghubungkan perangkat pengguna ke server VPN. Untuk ini, pengguna hanya perlu menyalin link key access yang diberikan, lalu membuka aplikasi dan menempelkannya ke kolom yang tersedia. Untuk memulai koneksi, pengguna hanya perlu menekan tombol "Connect". Setelah proses selesai, perangkat akan terhubung secara instan ke jaringan VPN yang telah diatur. Selanjutnya, lalu lintas internet akan dienkripsi melalui server Outline yang telah ditetapkan.[12]

Hasil pengujian sistem

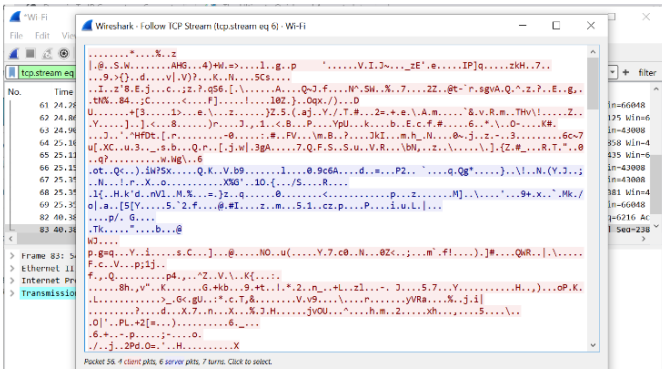
Pengujian merupakan tahap akhir penelitian pada sistem Outline VPN berbasis VPS yang di implementasikan di RSUD yang menunjukkan koneksi antara client dan server berhasil dilakukan dengan baik menggunakan access key yang telah dibuat melalui Outline Manager. Pengujian di gunakan untuk mengetahui bahwa lalu lintas data terenkripsi dengan baik atau tidak, sehingga tidak dapat dibaca secara langsung oleh pihak ketiga. Selain itu, apakah sistem berhasil membatasi akses hanya kepada pengguna yang memiliki kunci akses, dan administrator dapat dengan mudah mengelola melalui Outline Manager. menguji koneksi kecepatan setelah dan sesudah menggunakan VPN.
Catatan pengujian enkripsi:

- Outline VPN menggunakan enkripsi AES-256-GCM (default) yang sangat sulit untuk disadap atau dibuka tanpa kunci.
- Simulasi yang akan di uji tidak memecahkan enkripsi, tetapi hanya menunjukkan dampak perubahan penyadapan dengan dan tanpa VPN.

Pengujian Enkripsi pada gambar nomor 10 dilakukan setelah koneksi diamankan menggunakan Outline VPN atau VPN dalam posisi aktif, pengujian tahap ini menggunakan wireshark, seluruh lalu lintas data, termasuk protokol komunikasi, dialihkan melalui jalur terenkripsi dengan menggunakan kombinasi protokol TCP dan UDP, yang merupakan bagian dari implementasi Shadowsocks. Protokol yang digunakan adalah UDP (User Datagram Protocol) dan TCP (Transmission Control Protocol). Terlihat bahwa alamat sumber berasal dari IP publik (139.180.213.151) menuju IP lokal (192.168.1.10), dan data yang ditransfer dalam bentuk hex serta ASCII tidak dapat dibaca secara langsung karena terenkripsi.[13]



Gambar 10. Protokol TCP & UDP



Gambar 11. Packet Sniffing 2

Hasil tangkapan paket Wireshark ke dua pada gambar 11 saat mode VPN di aktifkan menunjukkan bahwa tampilan Follow TCP Stream di aplikasi Wireshark, yang digunakan untuk menganalisis lalu lintas jaringan. data yang terlihat merupakan hasil tangkapan komunikasi TCP antara client dan server dalam bentuk ASCII.Teks berwarna merah menandakan data yang dikirim oleh client (pengguna) ke server. Data ini sudah dalam bentuk terenkripsi atau tidak terbaca karena menggunakan protokol yang aman seperti (HTTPS) atau karena datanya berupa biner. Teks berwarna biru adalah data balasan dari server kepada client. Sama seperti sebelumnya, karena data tidak terbaca jelas, yang menujukan bahwa enkripsi berjalan dengan baik dan tidak memungkinkan penyadapan data secara langsung. Dengan dukungan kedua protokol tersebut, Outline VPN memastikan koneksi tetap stabil, dan aman, sehingga data sensitif seperti kredensial login maupun aktivitas pengguna tidak dapat diakses oleh pihak yang tidak berwenang meskipun berada di jaringan publik atau tidak aman.[14]

Pada tabel nomor 1 saat VPN dalam kondisi OFF, hasil tangkapan Wireshark menunjukkan bahwa data login seperti username dan password (uname=test&pass=passw123) dapat terlihat secara jelas, karena dikirim melalui protokol HTTP yang tidak memiliki enkripsi. Selain itu, permintaan halaman (GET /login.php HTTP/1.1) dan respon server (302 Found) juga dapat dibaca secara langsung.

Menandakan bahwa komunikasi antara client dan server sangat rentan terhadap penyadapan. Sebaliknya, ketika VPN dalam kondisi ON, seluruh lalu lintas data yang ditangkap oleh Wireshark berubah menjadi teks acak dan simbol tidak terbaca, dengan label seperti Encrypted Application Data untuk koneksi TCP atau payload dalam bentuk heksadesimal pada koneksi UDP. [15]Hal ini menunjukkan bahwa Outline VPN berhasil mengenkripsi seluruh komunikasi jaringan, sehingga informasi sensitif tidak dapat diakses atau dimata-matai, bahkan ketika dianalisis menggunakan tools seperti Wireshark.[16]

INDEXIA: Informatic and Computational Intelligent Journal
Vol.08, No.01, Mei 2026, hlm. 11-22
P-ISSN: 2657-0424
E-ISSN: 2657-0432

Tabel 1. Hasil pengujian enkripsi status VPN

NO	Status VPN	Protokol	Jenis data	Hasil tangkapan
1	OFF	HTTP	Username & Password	uname=test&passw123 (terlihat jelas)
2	OFF	TCP	HTTP Request	GET/login.php HTTP/1.1
3	OFF	TCP	HTTP Response	302 Found → redirect ke login.php
4	ON	TCP/UDP	Encrypted payload	Teks acak, simbol tidak terbaca (0x...)
5	ON	TCP	TLS Application	Encrypted Application Data (warna merah/biru)
6	ON	UDP	Shadowsocks Traffic	Payload terenkripsi dalam bentuk hex & ASCII

Tabel 2. Hasil Koneksi akses VPN

NO	Pengguna/perangkat	Status kunci akses	Hasil pengujian koneksi
1	Laptop A	Tidak ada	Gagal terhubung
2	Smartphone B	Ada	Berhasil terhubung
3	Laptop C	Kunci di hapus	Gagal terhubung
4	Smartphone D	Ada	Berhasil terhubung

Berdasarkan hasil implementasi sistem pada tabel nomor 2, Outline VPN berhasil membatasi akses jaringan hanya kepada pengguna yang memiliki kunci akses (access key). Hal ini ditunjukkan dengan uji coba koneksi, di mana perangkat yang tidak memiliki kunci tidak dapat terhubung ke jaringan VPN, sementara perangkat dengan kunci dapat terkoneksi dan mengakses internet secara aman. Selain itu, proses manajemen pengguna oleh administrator melalui aplikasi Outline Manager dapat dilakukan dengan mudah, seperti menambahkan, menghapus, atau membatasi akses pengguna hanya dalam beberapa klik.

Tabel 3. Hasil Uji jaringan

NO	Metode pengujian	Download (Mbps)	Upload (Mbps)	Ping (ms)	Jitter (ms)
1	VPN OFF	13.0	14.0	35	1
2	VPN ON	14.1	10.1	29	27
3	VPN OFF	14.1	13.6	21	2
4	VPN ON	14.5	9.1	65	31
5	VPN OFF	14.6	14.1	20	6
6	VPN ON	14.3	8.8	31	12

Pengujian kecepatan jaringan pada tabel nomor 3 dilakukan untuk mengetahui dampak penggunaan Outline VPN terhadap performa koneksi internet. Pengujian dilakukan menggunakan layanan speedtest untuk mengukur kecepatan unduh (download), unggah (upload), dan latency (ping), baik sebelum maupun sesudah koneksi VPN diaktifkan hasil data pengujian di tampilkan dalam bentuk tabel berikut spesifikasi layanan jaringan dan server VPN pada saat proses pengujian di lakukan, Sumber internet jaringan bandwidth 15Mbps server lokal, jenis VPS yang di gunakan yaitu Vultr, dengan prosesor CPU: 1 vCPU, RAM: 1GB dan kapasitas penyimpanan: SSD 25GB, Bandwidth: 1TB dengan lokasi VPS singapura.[17]

Untuk mengetahui sejauh mana perubahan suatu parameter setelah penggunaan Outline VPN, digunakan rumus untuk mengetahui nilai persentase nya dengan rumus sebagai berikut:

$$\frac{(\text{Nilai VPN ON} - \text{Nilai VPN OFF})}{(\text{Nilai VPN OFF}) \times 100\%}$$

Nilai VPN ON, di kurangi Nilai VPN OFF, di bagi Nilai VPN OFF, di kali seratus persen.
Keterangan:

- Nilai VPN ON = Rata-rata nilai saat VPN aktif
- Nilai VPN OFF = Rata-rata nilai saat VPN tidak aktif

1. Download speed
   - VPN OFF: 13.0, 14.1, 14.6 Mbps → rata-rata:
     13.0+14.1+14.6 ÷ 3 = 13.9 Mbps
   - VPN ON: 14.1, 14.5, 14.3 Mbps → rata-rata:
     14.1+14.5+14.3 ÷ 3 = 14.3 Mbps
     Hasil (14.3−13.9 ÷ 13.9) × 100% = 2.88%
2. Upload speed
   - VPN OFF: 14.0, 13.6, 14.1 Mbps → rata-rata:
     14.0 + 13.6 + 14.1 ÷ 3 = 13.9 Mbps
   - VPN ON: 10.1, 9.1, 8.8 Mbps → rata-rata:
     10.1 + 9.1 + 8.8 ÷ 3 = 9.33 Mbps
     Hasil (9.33 − 13.9 ÷ 13.9) × 100% = −32.85%
3. Ping
   - VPN OFF: 35, 21, 20 ms → rata-rata:
     35 + 21 + 20 ÷ 3 = 25.3 ms
   - VPN ON: 29, 65, 31 ms → rata-rata:
     29 + 65 + 31 ÷ 3 = 41.7 ms
     (41.7 − 25.3 ÷ 25.3) × 100% = 64.43%
4. Jitter
   - VPN OFF: 1, 2, 6 ms → rata-rata:
     1 + 2 + 6 ÷ 3 = 3.0 ms
   - VPN ON: 27, 31, 12 ms → rata-rata:
     27 + 31 + 12 ÷ 3 = 23.3 ms
     (23.3 − 3.0 ÷ 3.0) × 100% = 676.7%

Tabel 4. Hasil Kuisioner

Pertanyaan	Sangat Setuju	Setuju	Netral	Tidak Setuju	Sangat Tidak Setuju
VPN memberikan rasa aman dalam mengakses internet	50%	50%	0%	0%	0%
Data melalui VPN terlindungi	50%	40%	10%	0%	0%
Informasi login & data sensitif aman	60%	30%	10%	0%	0%
Kecepatan koneksi VPN memadai	50%	40%	10%	0%	0%
VPN jarang mengalami gangguan	40%	40%	10%	10%	0%
VPN tidak mempengaruhi kecepatan internet	20%	50%	10%	20%	0%
Proses koneksi VPN mudah	50%	40%	10%	0%	0%
Aplikasi VPN mudah dipahami	60%	30%	0%	10%	0%
Puas dengan kinerja VPN	60%	30%	10%	0%	0%
Bersedia merekomendasikan VPN	50%	40%	10%	0%	0%

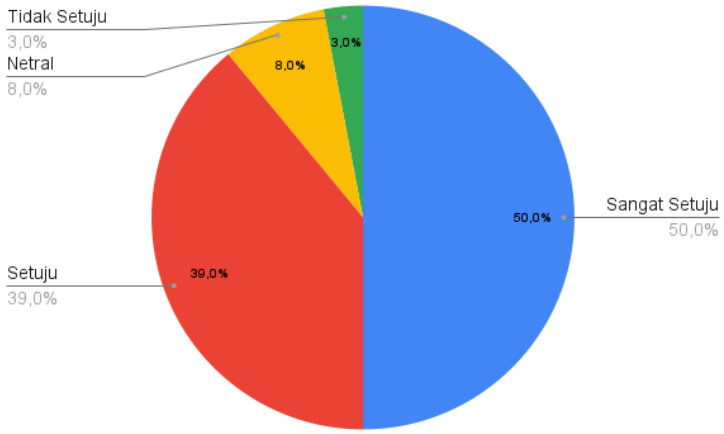
Berdasarkan hasil perhitungan rata-rata, penggunaan Outline VPN pada jaringan ini menunjukkan adanya peningkatan kecepatan download sebesar 2,88%, meskipun terjadi penurunan signifikan pada kecepatan upload sebesar 32,85%. Selain itu, nilai ping mengalami kenaikan sebesar 64,43%, yang mengindikasikan adanya peningkatan waktu respons akibat proses enkripsi dan perutean data. Jitter juga meningkat tajam sebesar 676,7%, menunjukkan fluktuasi koneksi yang lebih tinggi saat VPN diaktifkan terdapat penurunan peforma.[18]Berdasarkan data perbedaan kecepatan jaringan ini tidak terlalu mempengaruhi produktifitas pengguna, dikarenakan perbedaan letensi hanya sepersekian milidetik, speed upload dan download juga bisa di pengaruhi oleh Provider sumber internet dan spesifikasi server VPS. Meskipun terdapat penurunan pada aspek performa tertentu, penggunaan

INDEXIA: Informatic and Computational Intelligent Journal
Vol.08, No.01, Mei 2026, hlm. 11-22
P-ISSN: 2657-0424
E-ISSN: 2657-0432

Outline VPN tetap memberikan manfaat utama berupa peningkatan keamanan dan perlindungan data saat mengakses jaringan, khususnya dalam lingkungan RSUD yang rentan terhadap penyadapan.[19]

Untuk mengetahui efektiftas dari user experience kuesioner disebarkan kepada 10 responden untuk mengevaluasi penerapan Outline VPN berbasis VPS Server, Kuesioner terdiri dari 10 pernyataan dengan skala Likert (Sangat Setuju, Setuju, Netral, Tidak Setuju, sangat tidak setuju) karena total responden 10 orang, maka setiap 1 orang memiliki nilai 10% dari keseluruhan suara.Tabel berikut menyajikan rekapitulasi hasil jawaban responden:

Visualisasi data juga di tunjukan dalam bentuk Diagram lingkaran persentase untuk memudahkan dalam pembacaan data hasil kuisioner.



Gambar 12. Diagram lingkaran user experience

Hasil perhitungan setiap pertanyaan

- VPN memberikan rasa aman = 90%
- Data terlindungi = 88%
- Informasi login & data aman = 90%
- Kecepatan memadai = 88%
- Jarang gangguan = 82%
- Tidak mempengaruhi kecepatan = 74%
- Proses koneksi mudah = 88%
- Aplikasi mudah dipahami = 88%
- Puas dengan kinerja = 90%
- Bersedia merekomendasikan VPN = 88%

Berdasarkan hasil analisis dan perhitungan kuesioner di atas, diperoleh rata-rata efektivitas sebesar 86,6% yang termasuk dalam kategori sangat baik dan efektif. Hal ini menunjukkan bahwa penerapan VPN dinilai mampu memberikan keamanan data, kemudahan penggunaan, serta kepuasan pengguna secara menyeluruh, meski terdapat nilai persentase paling rendah 74% pada pengaruh kecepatan internet dan jaringan.

IV. KESIMPULAN

Hasil Penelitian dan pengujian menghasilkan beberapa kesimpulan sebagai berikut, Implementasi Outline VPN berbasis VPS Server berhasil dilakukan melalui tahapan instalasi dan konfigurasi server, pengaturan akses dengan Outline Manager, serta koneksi menggunakan Outline Client. Sistem ini mampu mengenkripsi seluruh lalu lintas data dan membatasi akses hanya kepada pengguna yang memiliki access key. Efektivitas sistem terbukti sangat baik, ditunjukkan oleh hasil uji enkripsi menggunakan wireshark yang melindungi data dari penyadapan, dan Adapun hasil dari kuesioner dengan tingkat efektivitas menunjukkan nilai rata-rata 86,6% dengan kategori sangat baik, yang menunjukkan bahwa penerapan VPN dinilai efektif dalam menjaga keamanan data dan memberikan kenyamanan penggunaan.

DAFTAR PUSTAKA

[1] A. F. Gentile, P. Fazio, dan G. Miceli, "A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios," *Telecom*, vol. 2, no. 4, hlm. 430–445, Nov 2021, doi: 10.3390/telecom2040025.

[2] F. A. Syaifuddin, D. A. Maulana, dan M. F. Amrulloh, "Analisis Keamanan Jaringan di Rumah Sakit Umum Daerah Bangil Menggunakan Firewall untuk Mencegah Serangan Brute Force dan Fraud," *Digit. Transform. Technol.*, vol. 4, no. 2, hlm. 895–902, Des 2024, doi: 10.47709/digitech.v4i2.5003.

[3] A. T. Permana dan A. F. Ramadhan, "Analisis Keamanan Jaringan Pada Layanan Wifi Dengan Menggunakan Wireshark," vol. 19, no. 1, 2025. https://ejournal.lppmunsap.org/index.php/infomans/article/view/820/1179

[4] M. Khofikur R.A, F. P. Eka Putra, Moh. W. Ridho G, dan V. Huda, "Analisis Kinerja dan Keamanan Protokol PPTP dan L2TP/IPSec VPN pada Jaringan MikroTik," *Infotek J. Inform. Dan Teknol.*, vol. 8, no. 2, hlm. 334–344, Jul 2025, doi: 10.29408/jit.v8i2.30230.

[5] H. Pribadi Fitrian, N. Alia Destiara, N. Elsa Destianti, dan G. Maddanil Khowat, "ANALISIS PENERAPAN TEKNOLOGI VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SOLUSI KEAMANAN DATA DI JARINGAN PUBLIK," *JATI J. Mhs. Tek. Inform.*, vol. 9, no. 1, hlm. 1559–1563, Jan 2025, doi: 10.36040/jati.v9i1.12712.

[6] T. B. Septiandoko, D. Desmulyati, dan A. Taufik, "Implementasi Jaringan Internet Site To Site VPN Dengan Metode IPSec Pada PT Telkom Akses," *Comput. Sci. CO-Sci.*, vol. 1, no. 1, hlm. 18–26, Jan 2021, doi: 10.31294/coscience.v1i1.138.

[7] A. A. Dharma dan F. H. Utami, "Implementasi Penggunaan Jaringan Intranet Menggunakan Linux Ubuntu Server". https://jurnal.unived.ac.id/index.php/jmi/article/view/6569/5056

[8] I. A. Laksono dan M. M. Alamin, "IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) BERBASIS MIKROTIK MENGGUNAKAN METODE PPTP PADA JARINGAN INTERNET DI FAKULTAS ILMU KOMPUTER UNUSIDA," vol. 9, no. 3, 2025. https://doi.org/10.36040/jati.v9i3.13582

[9] R. Subekti, "IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SOLUSI SECURITY SELAMA WORK FROM HOME".https://doi.org/10.28945/2441

[10] D. Novianto, Y. S. Japriadi, dan L. Tommy, "IMPLEMENTASI VIRTUAL PRIVATE NETWORK MENGGUNAKAN SSTP UNTUK KEAMANAN AKSES KE NETWORK ATTACHED STORAGE," vol. 10, no. 1, 2025. https://jurnal.univbinainsan.ac.id/index.php/jusim/article/view/2644/1375

[11] J. A. K. Parera, M. Dahoklory, C. Alyona, dan A. Lalaun, "IMPLEMENTASI VIRTUAL PRIVATE SERVER BERBASIS LINUX MENGGUNAKAN DIGITAL OCEAN SERTA UJI KECEPATAN JARINGAN SERVER CLOUD DI DESA RUTONG," vol. 15, 2024. https://doi.org/10.37639/jti.v15i3.384

[12] S. Wulandari, "Integrasi VPN (Virtual Private Network) dalam Sistem Jaringan Komputer untuk Keamanan Akses Data Jarak Jauh," *J. Inf. Technol.*, vol. 3, 2024. https://journals.itkes-ikabina.ac.id/index.php/JOIT/article/view/65/67

[13] J. L. Putra, L. Indriyani, dan Y. Angraini, "Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna".https://doi.org/10.31294/ijcit.v3i2.4677

[14] D. P. Kuswandono dan Z. Mutaqin, "PENGAMANAN AKSES JARAK JAUH JARINGAN INTERNET RUMAH DENGAN TEKNOLOGI VPN BERBASIS VPS," vol. 2, no. 1, 2024. https://banisalehjurnal.ubs.ac.id/index.php/tridi/article/view/60/31

[15] T. S. Ali, I. Santoso, A. S. Quiko, dan G. Santoso, "Pengaruh Virtual Private Network (VPN) Terhadap Keamanan dan Performa Akses Jaringan," vol. 01, no. 01, 2025. https://ejournal.utmj.ac.id/jarekom/article/download/903/505/3440

[16] S. M. Khaerullah dan D. Mustofa, "PENGGUNAAN WIRESHARK DALAM PENYADAPAN LALU LINTAS DATA BERPROTOKOL HTTP PADA JARINGAN WI-FI," *J. Ilm. IT CIDA*, vol. 10, no. 1, hlm. 19, Jul 2024, doi: 10.55635/jic.v10i1.203.

[17] N. Sobah dan M. F. Amrulloh, "Perancangan dan Implementasi Sistem Monitoring Jaringan di MA Darut Taqwa Berbasis Web yang Mengintegrasikan dengan API MikroTik," *BIOS J. Teknol. Inf. Dan Rekayasa Komput.*, vol. 4, no. 2, hlm. 42–53, Agu 2023, doi: 10.37148/bios.v4i2.75.

[18] A. A. Fikri, D. A. R. Wulandari, dan Y. A. Auliya, "Perancangan Detail Engineering Design Infrastruktur Jaringan Komputer RSUD X Kota Y," vol. 7, no. 3, 2022. https://doi.org/10.19184/isj.v7i3.35144

[19] M. G. Br Sitorus, N. Maria, dan Y. N. Safa, "Tinjauan Literatur Manajemen Risiko Cyber dalam Proyek: Identifikasi, Evaluasi, dan Mitigasi Ancaman," *J. Manaj. Inform. JAMIKA*, vol. 14, no. 2, hlm. 187–198, Jul 2024, doi: 10.34010/jamika.v14i2.12887.