

IMPLEMENTASI VPN MENGGUNAKAN PROTOKOL L2TP UNTUK PENGELOLAAN NAS (*NETWORK ATTACHED STORAGE*) PADA STB

Dimas Zaldiyanto¹⁾, Subektiningsih^{*1)} Irma Rofni Wulandari²⁾

¹⁾ Informatika, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta

²⁾ Sistem Informasi, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta

Email: dimaszaldiyanto@students.amikom.ac.id¹⁾, subektiningsih@amikom.ac.id^{*2)}, rofni@amikom.ac.id³⁾

Abstrak- Mengimplementasikan Virtual Private Network (VPN) dalam pengendalian jarak jauh *Network Attached Storage* (NAS) menggunakan protokol L2TP pada Router Mikrotik. Penelitian ini menggunakan perangkat bekas, Set Top Box HG680P yang diubah menjadi server NAS sebagai alternatif yang lebih ekonomis dan ramah lingkungan dibandingkan membeli server NAS konvensional. Implementasi VPN L2TP melalui Mikrotik memfasilitasi akses jarak jauh dengan tingkat keamanan yang terjamin. Pengujian dilakukan dengan menggunakan dua perangkat, Laptop dan Smartphone yang digunakan untuk mengakses dan mentransfer data melalui jaringan VPN. Hasil pengujian menunjukkan bahwa implementasi VPN berhasil memfasilitasi akses dari berbagai lokasi dan transfer data dengan performa yang baik. Pada pengujian dengan kecepatan *download* 50 Mbps dan *upload* 10 Mbps terhadap ukuran file dari 50 Mb hingga 1000 Mb. Hasil pengujian menggunakan VPN memberikan kecepatan rata-rata dari semua transfer file adalah 15,12Mb/s dengan rata-rata waktu transfer adalah 4 menit 14 detik. Pengujian juga dilakukan dengan memutus koneksi VPN pada Mikrotik. Tidak terhubungnya VPN pada Mikrotik menjadikan browser gagal untuk mengakses situs, karena VPN tidak dapat mengakses informasi pada Server NAS. Oleh sebab itu, VPN sangat berperan sebagai jembatan untuk dapat mengakses Server NAS di luar jaringan lokal. Pada manajemen akses dilakukan pembatasan pada setiap user untuk meningkatkan keamanan pada saat akses atau berbagai file pada server NAS kepada orang lain. Tujuannya supaya pengguna mempunyai batasan akses, hanya dapat mengakses bagian yang telah ditentukan saja. Penelitian ini diharapkan dapat memberikan kontribusi dalam mengembangkan solusi jaringan yang aman, ekonomis, dan efisien, terutama dalam memanfaatkan perangkat bekas untuk pengelolaan data.

Kata Kunci: VPN; NAS; L2TP; Mikrotik; STB

Abstract- *Implementing Virtual Private Network (VPN) in remote Network Attached Storage (NAS) control using L2TP protocol on Mikrotik Router. This study uses a used device, Set Top Box HG680P, converted into a NAS server as a more economical and environmentally friendly alternative to buying a conventional NAS server. Implementation of L2TP VPN via Mikrotik facilitates remote access with guaranteed security levels. Testing was carried out using two devices, a Laptop and a Smartphone, which were used to access and transfer data via a VPN network. The test results showed that the VPN implementation successfully facilitated access from various locations and data transfer with good performance. In testing, the download speed was 50 Mbps, and the upload speed was 10 Mbps for file sizes from 50 Mb to 1000 Mb. The test results using VPN gave an average speed of all file transfers of 15.12Mb/s with an average transfer time of 4 minutes 14 seconds. Testing was also carried out by disconnecting the VPN connection on Mikrotik. The unconnected VPN on Mikrotik causes the browser to fail to access the site because the VPN cannot access information on the NAS Server. Therefore, VPNs play an important role as a bridge to access the NAS server outside the local network. In access management, restrictions are imposed on each user to increase security when accessing or sharing files on the NAS server with others. The goal is for users to have access restrictions, only being able to access the specified parts. This research is expected to contribute to developing secure, economical, and efficient network solutions, especially in utilizing used devices for data management.*

Keywords: VPN; NAS; L2TP; Mikrotik; STB

1. PENDAHULUAN

Penggunaan sumber daya teknologi yang digunakan secara efisien dan efektif menjadi sangat penting. Namun pesatnya perkembangan teknologi ini banyak menghasilkan perangkat elektronik yang menjadi usang tidak terpakai. Seperti *Set Top Box* (STB), dengan memanfaatkan STB bekas ini yang dapat diubah menjadi Server NAS. Pemanfaatan ini dapat memberikan solusi untuk mengurangi limbah elektronik serta memberikan alternatif yang ekonomis untuk penggunaan rumah atau bisnis kecil dibanding membeli server NAS konvensional. Dalam upaya meningkatkan pemanfaatan teknologi yang ada, maka dilakukan upaya mengubah *Smart Tv Box* (STB) yang sudah tidak terpakai menjadi Sistem operasi Linux [1] sehingga memungkinkan STB berfungsi dengan efektif. Penggunaan *Network Attached Storage* (NAS) menjadi salah satu solusi untuk pengaksesan data yang lebih fleksibel dan efisien, karena data akan disimpan secara terpusat dan dapat diakses melalui jaringan lokal yang sama [2]. Namun, tantangan muncul ketika membutuhkan akses data di luar jaringan yang berbeda. Penggunaan *Virtual Private Network* (VPN) menjadi salah satu solusi yang efektif untuk dapat mengakses NAS dari berbagai lokasi [3]. Pemanfaatan Mikrotik sebagai *Gateway* VPN memfasilitasi akses jarak jauh yang aman, memperluas fungsi STB menjadi lebih dari penyimpanan lokal. Dukungan Protokol *Layer 2 Tunneling Protocol* (L2TP), menjadikan Mikrotik dapat mengamankan koneksi antara pengguna dan NAS [4]. Data sensitif dapat diakses dengan aman dari berbagai lokasi [5]. Solusi ini tidak hanya mengurangi biaya,

namun mengatasi permasalahan limbah elektronik, sekaligus memberikan wawasan baru dalam pemanfaatan teknologi yang berkelanjutan.

Berbagai Penelitian yang dilakukan seperti oleh [6] Penelitian ini mengukur kinerja STB (Set Top Box) sebagai perangkat penyimpanan *cloud* dan menilai sejauh mana perangkat ini dapat diandalkan sebagai solusi penyimpanan *digital*. Hasil penelitian menunjukkan bahwa STB dapat berfungsi sebagai penyimpanan *cloud* dengan performa cukup baik untuk penggunaan sehari-hari, meskipun terdapat beberapa keterbatasan dalam transfer data. Penelitian ini melibatkan pengujian Kinerja STB dalam berbagai skenario penyimpanan dan transfer data untuk mendapatkan gambaran lengkap tentang kemampuan perangkat ini. Penulis menyarankan untuk mengeksplorasi peningkatan kinerja STB dengan menambahkan fitur atau komponen yang lebih canggih guna meningkatkan fungsionalnya sebagai perangkat penyimpanan *cloud* yang lebih handal. Penelitian Berikutnya dilakukan Oleh Jurnal [7] Penelitian ini membahas mengubah STB bekas menjadi mini *server* hemat biaya, yang dapat digunakan menjadi penyimpanan data pribadi dan berbagi file antar pengguna dengan memanfaatkan perangkat lunak *Server Samba*. Pengujian dilakukan mentransfer sebuah dokumen melalui jaringan dengan hasil tanpa ada kendala antara *client* dan *server*. dari penelitian ini menunjukkan bahwa STB bekas dapat diandalkan sebagai *mini server* dengan performa yang cukup baik. Penelitian ini mencakup perubahan Sistem Operasi STB ke Linux Armbian, pengaturan *Samba Server*. Namun *server* ini tidak ada manajemen bandwidth menyebabkan pengujian 3 perangkat tidak terbagi secara merata menyebabkan terjadinya kecepatan *Upload* maupun *Download* saling berebut. Maka pada penelitian selanjutnya disarankan untuk meningkatkan manajemen bandwidth pada STB yang digunakan untuk dapat memaksimalkan kerjanya.

Penelitian yang dilakukan Oleh [1] Penelitian ini membahas Analisis mengenai sistem *E-Learning* berbasis Moodle yang berjalan di server STB (Set Top Box) FiberHome HG680P, Tujuan dari penelitian ini adalah untuk menguji seberapa baik kinerja STB dalam mendukung platform *E-Learning*, terutama untuk skala kecil sampai menengah. Hasil Penelitian menunjukkan bahwa perangkat ini dapat menjalankan Moodle dengan performa yang cukup baik pada beban rendah, meskipun terjadi penurunan kinerja ketika beban meningkat. Metode yang digunakan dalam penelitian ini melibatkan pengujian langsung terhadap performa STB sebagai *server Moodle*, dengan fokus pengukuran pada waktu respon dan kecepatan akses di berbagai tingkat beban. Penelitian selanjutnya disarankan untuk mengeksplorasi penggunaan STB FiberHome HG680P sebagai *cloud storage* atau *Network Attached Storage (NAS)*. Penelitian yang dilakukan oleh [2] Membahas untuk menyediakan solusi penyimpanan data yang terpusat dan efisien di SMAN 1 Denpasar, diketahui bahwa pengelolaan data masih belum efektif dengan penggunaan Flash disk dan Harddisk yang rentan terhadap serangan virus serta resiko kehilangan data. maka penulis jurnal mengimplementasikan server NAS menggunakan OMV (Open Media Vault) pada Raspberry Pi 4. Hasil dari implementasi ini berhasil meningkatkan efisiensi pengelolaan data di SMAN 1 Denpasar serta mengurangi resiko kehilangan data karena data tidak disimpan secara terpusat. dengan mendapatkan hasil transfer data rata-rata 2,46 MB/s untuk transfer melalui Wireless dan 10 MB/s untuk transfer file melalui kabel LAN.

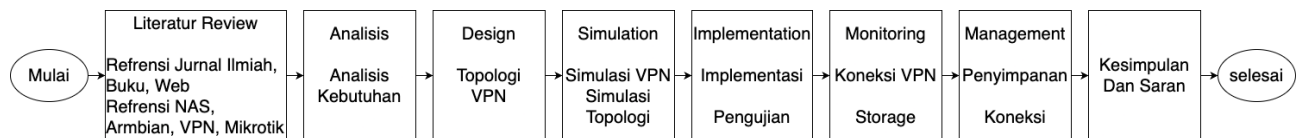
STB (Set Top Box) menggunakan FiberHome HG680P yang mempunyai 2 GB RAM dan mempunyai Processor Quad Core Cortex A7, FiberHome HG680P ini memiliki *Port Ethernet* 100MB dan 2 Slot USB dapat kita hubungkan dengan *Hard Drive* Eksternal untuk media penyimpanan NAS [8]. Mikrotik adalah sebuah perusahaan yang berasal dari Latvia, yang berfokus pada pengembangan perangkat keras dan perangkat lunak jaringan komputer, sistem operasi yang digunakan oleh perangkat Mikrotik adalah RouterOS yang berbasis Linux, RouterOS dapat menjadi network router mendukung VPN server, yang akan kita gunakan pada penelitian ini[9]. VPN (Virtual Private Network) dapat digambarkan yang berfungsi sebagai terowongan virtual yang menghubungkan satu jaringan ke jaringan lainnya dan mengenkripsi koneksi antara dua jaringan, yang dapat memungkinkan pengguna yang memiliki izin hak akses untuk mengakses data dalam jaringan tersebut dengan aman [10]. L2TP (*Layer 2 Tunneling Protocol*) adalah protokol yang digunakan untuk membentuk VPN (*Virtual Private Network*) melalui internet, L2TP yang merupakan pengembangan dari protokol PPTP dan L2F, menggunakan mekanisme keamanan dan enkripsi yang sama dengan PPTP sebagai kunci autentikasi [11]. NAS (*Network Attached Storage*) adalah server yang menggunakan sistem operasi khusus yang memungkinkan banyak pengguna untuk menyimpan dan mengakses data dari satu lokasi terpusat. NAS sangat berguna karena memudahkan penyimpanan dan berbagi data secara aman dan efisien yang memungkinkan berbagai platform dapat mengakses ke file NAS seperti Komputer, Smartphone yang terhubung dalam sebuah jaringan yang sama[12]. OMV (*Open Media Vault*) adalah perangkat lunak berbasis *Open Source* yang dirancang khusus untuk NAS (*Network Attached Storage*) generasi terbaru, yang berbasis pada sistem operasi Linux Debian. Perangkat lunak ini menyediakan berbagai layanan akses data, termasuk SSH, FTP, SMB/CIFS, server media DAAP, RSync, dan client BitTorrent. *Open Media Vault* Memiliki struktur modular yang memungkinkan penambahan fitur melalui sistem *plugin* [13].

VPS (*Virtual Private Server*) adalah layanan server fisik yang membagi hardware untuk dapat digunakan menjadi beberapa *hosting server* [14]. Salah satu fasilitas layanan dari VPS memiliki IP Publik yang dapat diakses langsung dari Internet tanpa perantara. Dengan adanya IP Publik ini dapat dimanfaatkan untuk menjadi server VPN. CHR (*Cloud Hosted Router*) merupakan RouterOS yang dirancang untuk beroperasi di mesin virtual, CHR mendukung arsitektur 64-bit x86 dan kompatibel dengan hypervisor seperti Hyper-V, VirtualBox, VMware, dan KVM. Yang membedakan dengan RouterOS adalah kecepatan yang dapat diakses. Salah satu penggunaan CHR adalah melakukan Interkoneksi antar jaringan LAN melalui Internet [15]. WinBox merupakan aplikasi yang dikembangkan oleh MikroTik untuk mengelola router Mikrotik RouterOS yang berbasis GUI (*Graphical User Interface*), dengan adanya WinBox, dapat memudahkan untuk mengkonfigurasi pengaturan Manajemen *Bandwidth*, Konfigurasi VPN, pengaturan *Firewall* dan Pemantauan Jaringan, dengan cara yang lebih mudah dibandingkan dengan menggunakan *Command Line (CLI)*[16]. Dalam penelitian

ini akan dilakukan pemanfaatan STB bekas sebagai sarana penyimpanan terpusat dengan menerapkan VPN supaya dapat diakses di luar jaringan lokal, sehingga tidak terbatas pada cakupan area.

2. METODOLOGI PENELITIAN

Metode penelitian diperlukan supaya tahap penelitian yang dilakukan sesuai dengan rencana yang telah ditentukan, seperti sajian pada Gambar 1. Dalam Penelitian ini memiliki 8 Prosedur langkah penelitian diantaranya adalah (1) Literatur Review (2) Analisis (3) Simulation (4) Implementation (5) Monitoring (6) Management, dan (7) Kesimpulan Dan Saran. Langkah ini akan dijelaskan di bawah ini.



Gambar 1. Alur Penelitian

2.1 Alur Penelitian

Pada *literatur review* dari penelitian yang selanjutnya dilakukan oleh Jurnal [17] Tujuan dari jurnal ini adalah untuk merancang dan mengimplementasikan solusi penyimpanan *cloud* yang aman dan efisien dengan memanfaatkan perangkat lunak *Open Source FreeNas*, dan memastikan data dapat diakses secara aman melalui *Tunneling*. Hasil penelitian dari jurnal tersebut menunjukkan bahwa sistem yang dirancang mampu menyediakan layanan penyimpanan *cloud* yang aman, Jurnal ini melibatkan perancangan, implementasi dan pengujian sistem *cloud storage* dengan simulasi skenario akses dan keamanan melalui *tunneling*, Penulis menyarankan untuk penelitian selanjutnya mengeksplorasi peningkatan kinerja dan keamanan sistem dengan menggunakan teknologi *tunneling* yang lebih maju dan dapat menambahkan fitur tambahan lainnya untuk meningkatkan efisiensi sistem. Penelitian yang selanjutnya dilakukan oleh [18] Melakukan perbandingan kinerja QoS (*Quality Of Service*) menggunakan berbagai protokol VPN (Virtual Private Network), seperti PPTP, L2TP, SSTP, dan IPSEC, penelitian ini bertujuan untuk menilai dan membandingkan kinerja QoS dari masing-masing protokol VPN tersebut dalam di bidang keamanan dan efisiensi jaringan. Hasil penelitian menunjukkan dari keempat Protokol yang telah di uji. Protokol L2TP dan IPSEC memiliki *Throughput* yang lebih unggul, maka itu penulis menjadikan sebuah referensi karena pada penelitian ini berfokus pada *Throughput* yang akan digunakan nantinya. Kemudian pada metode yang digunakan penelitian ini melibatkan pengujian langsung dan analisis perbandingan terhadap setiap protokol VPN dalam kondisi jaringan yang berbeda. Pada penelitian selanjutnya disarankan untuk mengeksplorasi implementasi protokol-protokol tersebut dalam skenario jaringan yang lebih kompleks atau pada berbagai jenis perangkat untuk mendapatkan pemahaman yang lebih mendalam mengenai kinerja QoS yang optimal.

2.2 Analisis

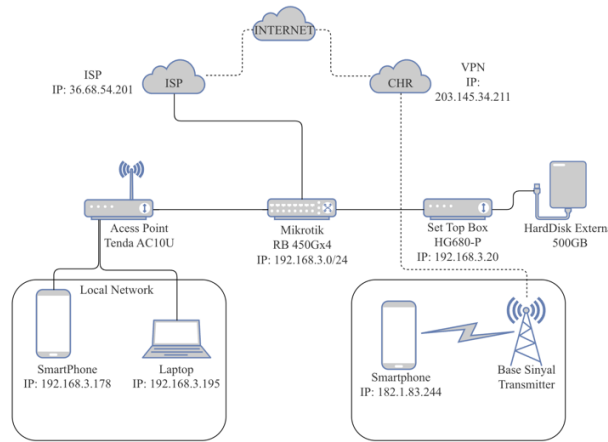
Pada tahap Analisis ini peneliti menggunakan STB yang tidak terpakai untuk digunakan sebagai server, sebab STB ini mempunyai daya yang cukup kecil hanya 12Watt, Peneliti menggunakan Hard Disk 3.5 inch dengan kapasitas 500GB sebagai media penyimpanan utama NAS, namun STB ini memiliki output daya sebesar 5Volt 500 Mili Ampere saja. Jika mengandalkan daya dari *slot* USB saja. Dapat merusak *Port* USB pada STB, untuk menjaga Harddisk tetap optimal dengan pemberian daya yang cukup maka peneliti menggunakan *Hard Disk Enclosure* yang mempunyai *Power External*. Penggunaan Mikrotik merupakan peran penting pada penelitian ini, Mikrotik dapat digunakan sebagai penghubung antara VPN dengan STB. Dengan ini pengguna dapat mengakses langsung dengan cara mengetikkan IP VPN di browser, cara ini lebih efektif dibanding dengan harus menghubungkan *device* dengan VPN terlebih dahulu untuk dapat mengakses NAS pada luar jaringan. Dengan adanya penelitian ini peneliti berharap dapat menjadi kontribusi penggunaan limbah elektronik secara maksimal.

2.2.1 Alat Dan Bahan

Pada Penelitian Ini menggunakan 4 Perangkat yaitu: Laptop Macbook Pro M1, Smartphone Iphone 15 Pro Max, Mikrotik RB 450Gx4, Dan Set Top Box HG680P. Peneliti Juga Menggunakan Internet Provider (ISP) dari Indihome yang memiliki kecepatan 50Mb/s Download, Dan 10Mb/s Upload sebagai koneksi Utama pada penelitian ini, dan Menggunakan Provider Data Seluler Telkomsel yang digunakan pada koneksi Smartphone. Dalam melakukan Implementasi Pada Penelitian memerlukan beberapa *software*. Berikut merupakan Perangkat Lunak yang digunakan pada Penelitian ini Seperti: Balena Etcher, Browser Brave, Cisco Packet Tracer, PhotoSync, Termius, Dan WinBox.

2.3 Design

Penulis menggunakan *Visual Paradigm Online* untuk menggambarkan Desain Topologi yang digunakan. Pada langkah awal memastikan Mikrotik terhubung dengan ISP untuk terhubung kedalam Internet dilanjutkan penyambungan koneksi VPN yang telah dibuat, kemudian mengatur IP pada STB menjadi Statik agar tidak berubah oleh DHCP, dengan *device* yang saling terhubung ini dapat memungkinkan mengakses server NAS melalui jaringan lokal, maupun di luar jaringan lokal. Agar lebih mudah memahami topologi yang digunakan dapat dilihat pada Gambar 2 di bawah ini.



Gambar 2. Topologi Jaringan

Dalam memudahkan untuk membaca IP yang digunakan pada topologi di Gambar 2, maka Tabel 1 menyajikan daftar IP yang digunakan dalam masing-masing perangkat.

Tabel 1. Daftar Alamat IP Pada Topologi

| No | Nama Device | IP | Gateway |
|----|---------------------|----------------|----------------|
| 1 | VPN | 203.145.34.211 | 203.145.34.211 |
| 2 | ISP Indihome | 36.68.54.201 | 118.98.115.70 |
| 3 | Mikrotik RB450Gx4 | 192.168.2.1 | 192.168.1.1 |
| 4 | Tenda AC10U | 192.168.3.11 | 192.168.2.1 |
| 5 | Smartphone | 192.168.3.178 | 192.168.2.1 |
| 6 | Laptop | 192.168.3.195 | 192.168.2.1 |
| 7 | Set Top Box HG680-P | 192.168.3.20 | 192.168.3.1 |

Pada Tahap Berikutnya Seperti Simulation, Implementation, Monitoring, Management akan di bahas pada Sub Bab Hasil Dan Pembahasan.

3. HASIL DAN PEMBAHASAN

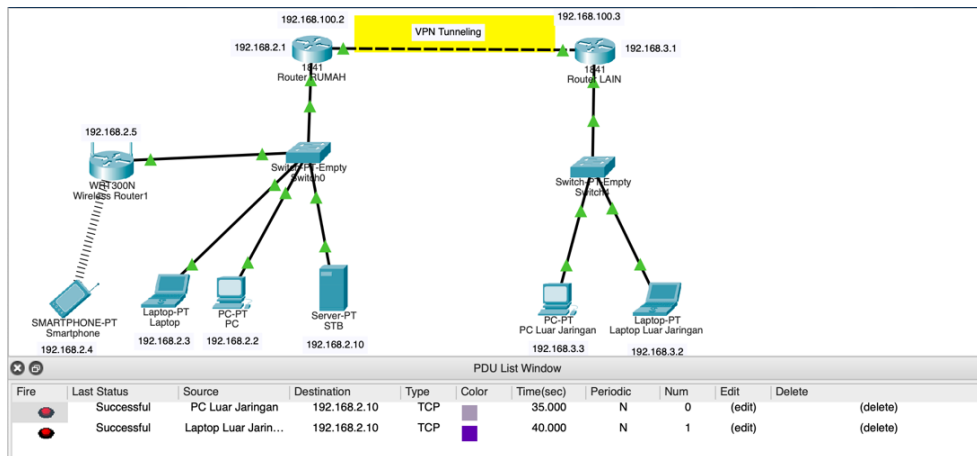
Pada tahap ini akan melakukan Implementasi penggunaan Set Top Box sebagai NAS Server pengujian akan dilakukan melalui koneksi lokal dan pengujian melalui koneksi VPN. Yang dimulai dari tahap Simulasi dengan menggunakan Cisco Packet Tracer, Kemudian Memasuki tahap Implementation yaitu penerapan kedalam Perangkat Keras, Kemudian Tahap Monitoring yang di lakukan adalah Memonitoring Koneksi VPN, Dan Memonitoring Penyimpanan Pada NAS. Dan pada Tahap Terakhir sebelum Kesimpulan Dan Saran yaitu Tahap Management, pada Tahap Management adalah untuk mengatur Hak pada setiap User yang akan Ditentukan.

3.1 Simulation

Pada tahap simulasi ini peneliti akan mensimulasikan topologi yang digunakan pada Aplikasi. Cisco Packet Tracer merupakan sebuah aplikasi yang di kembangkan oleh perusahaan Cisco Systems, Aplikasi ini digunakan sebagai simulasi topologi jaringan yang digunakan pada penelitian ini sebelum diimplementasikan ke perangkat nyata, Aplikasi ini dapat diunduh melalui situs resminya Cisco. Dengan menjalankan simulasi VPN (*Virtual Private Network*) dan Simulasi Tanpa VPN dapat memastikan berjalan tanpa adanya kendala. Peneliti melakukan pengujian menggunakan objek PC dan Laptop yang seolah olah berada di luar jaringan lokal.

3.1.1 Simulasi Menggunakan VPN

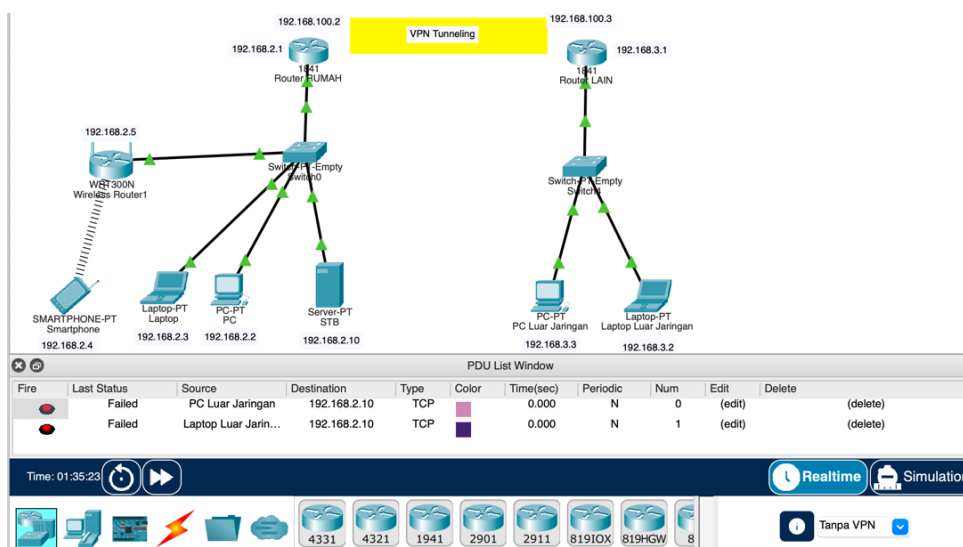
PC yang mempunyai alamat IP 192.168.3.3 dan Laptop dengan alamat IP 192.168.3.2 yang disimulasikan berbeda jaringan tersebut mencoba untuk mengakses server STB lokal yang memiliki IP 192.168.2.10 melalui koneksi VPN yang telah dikonfigurasi, Hasil dari simulasi ini menunjukkan bahwa PC dan Laptop yang berada di luar jaringan berhasil terhubung ke server STB tanpa adanya kendala. Gambar 3 Merupakan Tampilan simulasi pengujian menggunakan VPN.



Gambar 3. Simulasi VPN Menggunakan Cisco Packet Tracer

3.1.2 Simulasi Tanpa Menggunakan VPN

Untuk membuktikan bahwa koneksi VPN dapat membantu untuk mengakses Server di luar jaringan lokal. Maka Peneliti mensimulasikan untuk mencoba mengakses Server STB tanpa menggunakan VPN. Dan dapat dilihat pada Gambar 4 dibawah, tanpa adanya jembatan koneksi VPN, PC dan Laptop maupun koneksi di luar jaringan lokal tidak dapat untuk mengakses server STB. Setelah tahap simulasi ini dilakukan, langkah selanjutnya maka peneliti akan mengimplementasikan ke perangkat fisik.



Gambar 4. Simulasi Tanpa VPN Menggunakan Cisco Packet Tracer

3.1 Implementasi

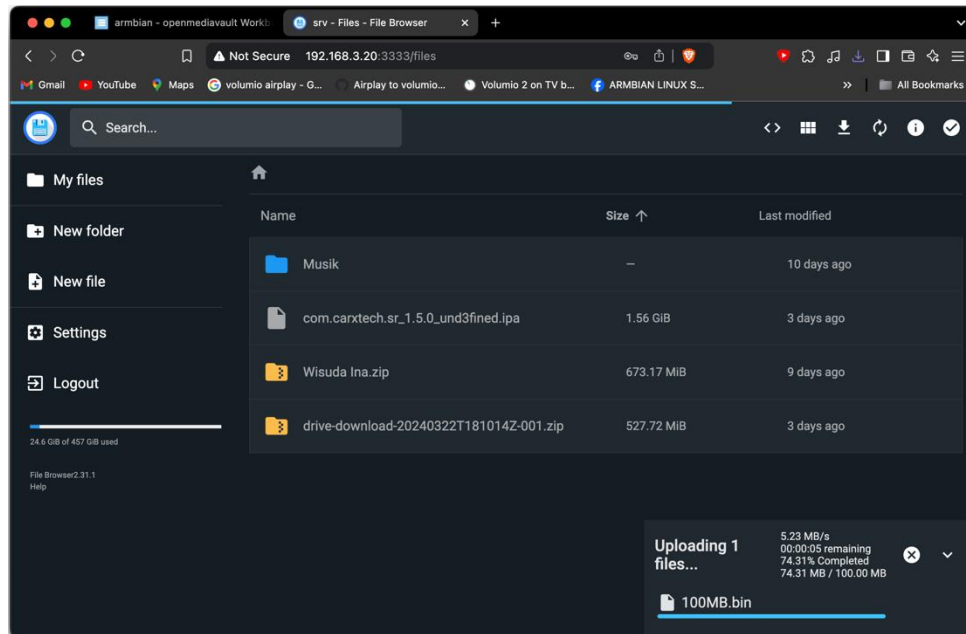
Pada Tahap Implementasi Peneliti akan melakukan penerapan ke alat fisik yaitu mengubah sistem operasi pada STB yang akan digunakan dari berbasis Android menjadi berbasis Linux Armbian dan mengkonfigurasi layanan NAS (Network Attached Storage), peneliti menggunakan OMV (Open Media Vault) sebagai layanan NAS. Diikuti dengan pembuatan server VPS yang akan digunakan, peneliti menggunakan CHR sebagai sistem operasi pada server VPS untuk digunakan sebagai server VPN. Dengan dilanjutkan untuk menghubungkan antara VPN dengan perangkat jaringan lokal seperti STB dan Mikrotik. Pada tahap Implementasi ini akan melakukan Perubahan Sistem Operasi pada STB (Set Top Box) dengan cara burning kartu SD menggunakan Aplikasi Balena Etcher diikuti dengan instalasi OMV (Open Media Vault) dan dilanjutkan pengujian pada server NAS baik dengan koneksi lokal maupun melalui koneksi VPN.

3.2 Pembahasan

Pada Tahap ini Peneliti akan melakukan Pengujian pada Server STB untuk menyediakan layanan NAS melalui jaringan lokal dan melalui *Tunnel* VPN. Pada langkah awal pengujian ini dilakukan pada jaringan lokal diikuti dengan tahap pengujian menggunakan VPN. pada pengujian ini Peneliti menggunakan 2 Device yaitu 1 Laptop untuk melakukan akses file NAS, dan 1 *Smartphone* untuk melakukan pengujian sebagai *backup* foto di luar jaringan lokal. Dan setelah pengujian File yang telah di lakukan Peneliti Telah Mencatat Hasil sebagai Berikut:

3.2.1 Pengujian Transfer File Pada Layanan NAS Melalui Koneksi Lokal

Open media Vault menyediakan antarmuka website untuk mengakses *file* dan mengelola *file*, dengan mengakses alamat IP dan dilanjutkan *Port* yang digunakan, pada browser <http://192.168.3.20:3333>. Pada pengujian, *file* yang dilakukan memiliki ukuran sebesar 50MB, 100MB, 200MB, 300MB, 400MB, 500MB, 600MB, 700MB, 800MB, 900MB, dan 1GB hasil pengujian ditunjukkan pada tabel 2 menunjukkan total waktu yang ditempuh masing-masing file.



Dan Gambar 5 Merupakan Tampilan pada NAS berbasis Web.

Gambar 5. Tampilan Web File Manager OMV

Tabel 2. Total Waktu Transfer File Pada Koneksi Lokal

| No | Ukuran File | Min | Rata - Rata | Max | Total Waktu |
|----|-------------|------------|-------------|------------|------------------|
| 1 | 50MB | 13,60 Mb/s | 24,24 Mb/s | 32,80 Mb/s | 0 Menit 10 Detik |
| 2 | 100MB | 12,72 Mb/s | 36,56 Mb/s | 50,40 Mb/s | 0 Menit 18 Detik |
| 3 | 200MB | 12,80 Mb/s | 39,04 Mb/s | 46,32 Mb/s | 0 Menit 37 Detik |
| 4 | 300MB | 08,16 Mb/s | 42,48 Mb/s | 53,36 Mb/s | 0 Menit 53 Detik |
| 5 | 400MB | 11,60 Mb/s | 45,6 Mb/s | 58,16 Mb/s | 1 Menit 06 Detik |
| 6 | 500MB | 11,76 Mb/s | 45,84 Mb/s | 52,64 Mb/s | 1 Menit 26 Detik |
| 7 | 600MB | 11,60 Mb/s | 52,08 Mb/s | 61,52 Mb/s | 1 Menit 25 Detik |
| 8 | 700MB | 11,60 Mb/s | 49,84 Mb/s | 69,44 Mb/s | 1 Menit 49 Detik |
| 9 | 800MB | 09,52 Mb/s | 61,20 Mb/s | 71,36 Mb/s | 1 Menit 40 Detik |
| 10 | 900MB | 09,60 Mb/s | 59,28 Mb/s | 69,76 Mb/s | 1 Menit 55 Detik |
| 11 | 1000MB | 16,00 Mb/s | 51,52 Mb/s | 69,76 Mb/s | 2 Menit 40 Detik |

Dari pengujian pada Tabel 2 yang telah dilakukan peneliti mencatat waktu transfer yang telah dilakukan pada pengujian menggunakan koneksi lokal, kecepatan transfer pada NAS mendapat kecepatan maksimal hingga 71,36Mb/s dan dari seluruh pengujian yang telah di lakukan peneliti mendapatkan hasil rata-rata kecepatan pada 46,16Mb/s kecepatan ini masih sangat nyaman digunakan untuk melakukan akses file baik *Upload* maupun *Download* pada server NAS.

3.2.2 Pengujian Melalui Koneksi VPN

Pada Tahap ini Pengujian yang dilakukan adalah menggunakan koneksi VPN. NAS akan diakses di luar jaringan lokal, Pengujian dilakukan pada Laptop untuk mencoba mengakses File NAS. Pada pengujian, *file* yang dilakukan memiliki ukuran yang sama seperti pengujian pada koneksi lokal yaitu sebesar 50MB, 100MB, 200MB, 300MB, 400MB, 500MB, 600MB, 700MB, 800MB, 900MB, dan 1GB. Dari pengujian yang telah dilakukan, Peneliti mencantumkan hasil

pada tabel 3 yang menunjukkan total waktu dari masing-masing file yang telah di *Upload* ke dalam Server NAS. Pengujian memiliki perbedaan waktu dengan menggunakan koneksi lokal. Hal tersebut dipengaruhi oleh faktor kecepatan Internet yang dimiliki Peneliti, Kecepatan yang dimiliki oleh peneliti yaitu Download 50Mbps dan Upload 10Mbps hal ini akan sangat berpengaruh pada saat melakukan Upload maupun Download file, Untuk penggunaan pribadi maupun skala rumahan hal ini masih dalam batas toleransi.

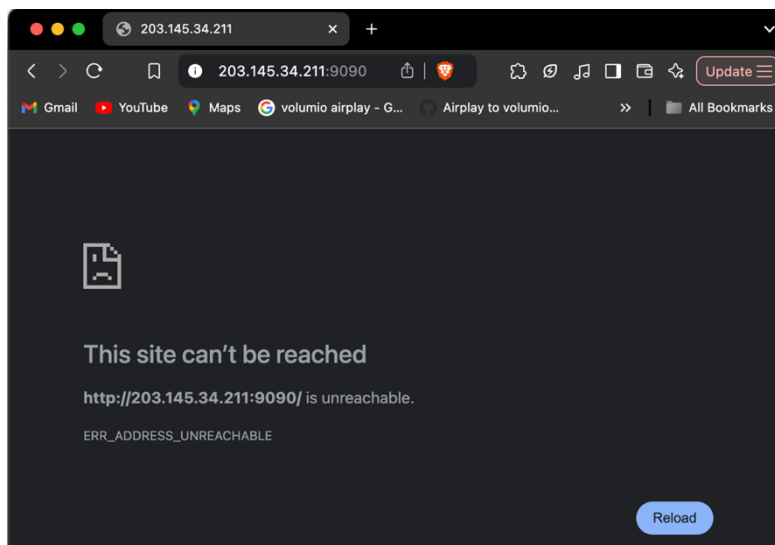
Tabel 3. Total Waktu Transfer File Menggunakan VPN

| No | Ukuran File | Min | Rata - Rata | Max | Total Waktu |
|----|-------------|-----------|-------------|------------|------------------|
| 1 | 50Mb | 1,04 Mb/s | 11,12 Mb/s | 17,04 Mb/s | 0 Menit 29 Detik |
| 2 | 100Mb | 6,40 Mb/s | 12,08 Mb/s | 18,56 Mb/s | 1 Menit 08 Detik |
| 3 | 200Mb | 1,84 Mb/s | 13,44 Mb/s | 19,52 Mb/s | 1 Menit 57 Detik |
| 4 | 300Mb | 5,68 Mb/s | 11,52 Mb/s | 19,76 Mb/s | 3 Menit 23 Detik |
| 5 | 400Mb | 6,88 Mb/s | 16,16 Mb/s | 22,80 Mb/s | 3 Menit 18 Detik |
| 6 | 500Mb | 0,88 Mb/s | 14,80 Mb/s | 24,64 Mb/s | 4 Menit 26 Detik |
| 7 | 600Mb | 5,92 Mb/s | 17,92 Mb/s | 25,76 Mb/s | 4 Menit 25 Detik |
| 8 | 700Mb | 3,92 Mb/s | 18,72 Mb/s | 29,12 Mb/s | 4 Menit 55 Detik |
| 9 | 800Mb | 6,40 Mb/s | 16,96 Mb/s | 24,32 Mb/s | 6 Menit 15 Detik |
| 10 | 900Mb | 1,04 Mb/s | 15,36 Mb/s | 25,76 Mb/s | 7 Menit 39 Detik |
| 11 | 1000Mb | 5,44 Mb/s | 18,24 Mb/s | 30,16 Mb/s | 7 Menit 38 Detik |

Dari pengujian Tabel 3 yang telah dilakukan dengan menggunakan koneksi VPN yang diakses melalui di luar jaringan lokal dengan bantuan Hotspot pada *Smartphone*. Peneliti menguji pada file dengan ukuran 50MB hingga 1GB, hasil pengujian yang telah dilakukan peneliti mencatat masing-masing kecepatan pada setiap file, Hasil yang didapat dengan pengujian melalui VPN memberikan kecepatan maksimal 30,16Mb/s dan peneliti juga menghitung kecepatan rata-rata dari semua file yang didapat adalah 15,12Mb/s, Kecepatan ini dipengaruhi oleh ISP yang dimiliki pada peneliti, ketika melakukan transfer file kedalam NAS melalui VPN, maka koneksi yang digunakan bergantung pada kecepatan ISP yang dimiliki, berbeda jika melalui koneksi lokal yang mengandalkan kekuatan Router untuk dapat melewati *Traffic* tersebut. Hasil pengujian menggunakan VPN memberikan rata-rata waktu transfer adalah 4 menit 14 detik.

3.2.3 Pengujian Akses Tanpa VPN

Pada Tahap ini, Peneliti melakukan pengujian dengan memutus koneksi VPN pada Mikrotik, langkah ini bertujuan untuk memahami bagaimana NAS diakses di luar jaringan lokal tanpa adanya jembatan yang diberikan oleh VPN untuk dapat terhubung ke dalam jaringan Internet. Langkah Awal dengan membuka *Tab Interfaces* pada aplikasi Winbox, diikuti dengan *Disable Profile* VPN yang telah terhubung pada Mikrotik. Hasil Pengujian Dengan Tidak Terhubungnya VPN pada Mikrotik, NAS Gagal untuk diakses, dikarenakan VPN tidak dapat mengakses informasi pada Server NAS, Hal tersebut ditunjukkan pada Gambar 6. Yang merupakan Tampilan tidak dapat dijangkau pada Browser ketika Mikrotik tidak Dihubungkan dengan VPN. Dari pengujian ini dapat disimpulkan VPN sangat Berperan penting pada penelitian ini sebagai jembatan untuk dapat mengakses Server NAS di luar jaringan Lokal.



Gambar 6. Tampilan Situs Tidak Dapat Dijangkau Pada Browser

3.3 Monitoring

Pada tahap monitoring, peneliti melakukan pemantauan yang menyeluruh untuk memastikan bahwa perangkat jaringan lokal terhubung dengan VPN secara optimal. Pemantauan ini tidak hanya terfokus pada koneksi VPN saja, tetapi juga mencakup beberapa aspek penting lainnya seperti *CPU Utilization*, *File System*, *Memory*, *Network Interfaces*, *Monitoring Suhu Pada HDD*, *Uptime*, *System Information*. Peneliti memonitor penggunaan penyimpanan untuk memastikan kapasitas storage yang telah terpakai serta yang masih tersedia. Selain itu, pemantauan juga dilakukan terhadap penggunaan *bandwidth* untuk memastikan bahwa transmisi data melalui VPN berjalan efisien tanpa adanya kendala atau gangguan yang signifikan. Melalui pemantauan ini, peneliti dapat mengidentifikasi dan mengatasi potensi masalah secara langsung, sehingga menjamin kinerja dan kestabilan sistem selama penelitian berlangsung.

3.4 Management

Pada tahap Manajemen penulis melakukan pengaturan hak akses untuk setiap pengguna yang diberikan hak akses pada NAS. Hal ini bermaksud untuk memastikan keamanan data yang efisiensi penggunaan sistem sesuai dengan kebutuhan masing-masing pengguna. Sebagai contoh pengguna A hanya diberikan hak akses untuk melihat *file* saja. Berarti pengguna A tidak dapat mengubah, menghapus ataupun menambahkan *file* pada sistem NAS, melainkan hanya memiliki akses untuk melihat dan menyalin *file* yang tersedia. Selanjutnya pengguna B diberikan hak akses yang lebih luas, yaitu dapat memodifikasi isi *file* beserta melihat semua *file* yang ada di NAS. Dan pengguna C diberikan akses yang lebih spesifik saja, yaitu hanya dapat mengakses folder tertentu yang telah dilakukan, pengguna C dapat melakukan memodifikasi *file* dan menambahkan file pada NAS, tetapi hanya folder tertentu saja. Pada Tabel 4 dibawah merupakan tabel hak akses pada masing-masing user, dengan melakukan pembatasan pada setiap *user* dapat meningkatkan keamanan pada saat ingin berbagi *file* pada server NAS kepada orang lain, pengguna tidak perlu khawatir akan *file* penting diakses oleh user lain, karena setiap *user* hanya dapat mengakses yang telah ditentukan saja.

Tabel 4. Hak User

| Nama User | Folder Data | Folder Foto | Folder Musik |
|-----------|--------------|--------------|--------------|
| User-A | Read | Read | Read |
| User-B | Read / Write | Read / Write | Read / Write |
| User-C | No | No | Read / Write |

KESIMPULAN

Berdasarkan Hasil dari “Implementasi VPN Untuk Pengendalian Jarak Jauh NAS Menggunakan Protokol L2TP Melalui Mikrotik” yang dilakukan oleh peneliti, maka dapat diambil kesimpulan bahwa penelitian ini telah berhasil memanfaatkan STB sebagai *mini server* untuk menjalankan layanan NAS menggunakan OMV. Tahap yang dilakukan adalah dengan mengubah sistem operasi Android TV menjadi Linux Armbian. Selanjutnya, sistem tersebut dihubungkan dengan *Harddisk Eksternal* untuk difungsikan sebagai media penyimpanan utama NAS. VPN dengan protokol L2TP diterapkan supaya server NAS dapat diakses di luar jaringan lokal. Dalam mengkoneksikan jaringan luar membutuhkan gateway VPN yang memanfaatkan Mikrotik. Peran Mikrotik juga melakukan *Port Forwarding* untuk mengarahkan alamat IP publik yang dimiliki pada VPN ke IP lokal STB sehingga pengguna dapat mengakses NAS dengan menggunakan IP publik VPN. Pengujian akses NAS dilakukan menggunakan Laptop dan *Smartphone*, menggunakan koneksi Lokal dan VPN, Hasil pengujian menunjukkan Laptop dan *Smartphone* berhasil mengakses *file* NAS di luar jaringan lokal. Pengujian dilakukan dengan cara transfer *file* kedalam server NAS. Ukuran *file* yang diuji bervariasi, yaitu dari 50MB hingga 1GB. Parameter pengujian adalah waktu dan kecepatan transfer *File*. Hasilnya adalah kecepatan transfer *file* melalui VPN cenderung lebih lambat dibandingkan dengan menggunakan jaringan lokal, yaitu dengan rata-rata sebesar 15,12Mb/s. Dalam pengujian dinyatakan bahwa pengujian pada *File* 1GB membutuhkan waktu 7 Menit 38 Detik pada VPN, dan membutuhkan waktu 2 Menit 40 Detik pada koneksi lokal. Pada penelitian selanjutnya untuk meningkatkan keandalan dan keamanan penyimpanan data dapat menambahkan dukungan penggunaan RAID (*Redundant Array of Independent Disks*). Menerapkan konfigurasi RAID, menjadikan data dapat disalin secara otomatis dari satu disk ke disk lainnya, sehingga resiko kehilangan data karena kerusakan perangkat keras dapat diminimalkan.

REFERENCES

- [1] “ANALISIS PERFORMA E-LEARNING BERBASIS MOODLE BERJALAN DI SERVER RENDAH BIAYA STB FIBERHOME HG680-P.”
- [2] N. Sri, J. Kusuma, G. Sastrawangsa, I. Puritan, and W. Adh, “Rancang Bangun Server Network Attached Storage (NAS) Sebagai Penyimpanan Data Terpusat Studi Kasus SMAN 1 Denpasar.”
- [3] D. P. Kuswandono, “DESIGN PENGAMANAN AKSES JARAK JAUH JARINGAN RUMAH DENGAN TEKNOLOGI VPN (VIRTUAL PRIVATE NETWORK) BERBASIS DI CLOUD VPS (VIRTUAL PRIVATE SERVER),” 2018.

- [4] M. A. Gunawan and S. Wardhana, “Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN (Virtual Private Network),” vol. 6, no. 1.
- [5] A. Purnama Sari and N. Kemala, “PERANCANGAN JARINGAN VIRTUAL PRIVATE NETWORK BERBASIS IP SECURITY MENGGUNAKAN ROUTER MIKROTIK,” vol. 7, no. 2, 2020.
- [6] R. Patuke, A. Mulyanto, and R. Takdir, “PENGUKURAN KINERJA SET TOP BOX (STB) SEBAGAI PENYIMPANAN CLOUD,” vol. 2, no. 1, 2022.
- [7] M. F. Ardiansyah, T. M. Diansyah, R. Liza, and D. Redaksi, “Attribution-ShareAlike 4.0 International Some rights reserved Cloud Computing Penggunaan Set top box Bekas untuk Dimanfaatkan sebagai Cloud Server INFORMASI ARTIKEL A B S T R A K.”
- [8] M. Nasrulloh, “PEMANFAATAN SET TOP BOX SMART TV HG680P UNTUK AKSES INTERNET MURAH BAGI PELAJAR DESA SUNGAI BELIDA PADA MASA PANDEMI COVID-19,” May 2023.
- [9] B. Cahya, F. Rizki, A. Sutiyo, Y. El Saputra, and M. Elfarizi, “IMPLEMENTASI FIREWALL PADA MIKROTIK UNTUK KEAMANAN JARINGAN,” 2023. [Online]. Available: <https://jurnal.itcc.web.id/index.php/jct/>
- [10] M. Rafii and N. Wicaksana, “Perancangan Virtual Private Network Layer 2 Tunneling Protocol (L2TP) Berbasis Mikrotik,” vol. 1, no. 1, 2022, [Online]. Available: <https://jurnal.netplg.com/>
- [11] M. A. Gunawan and S. Wardhana, “Implementasi dan Perbandingan Keamanan PPTP dan L2TP/IPsec VPN (Virtual Private Network),” vol. 6, no. 1, 2023.
- [12] W. Wijaya, F. Panjaitan, S. Rizal, and M. Ulfa, “Perbandingan Kinerja Sistem Operasi Network Attached Storage: Studi Kasus Truenas dan Xigmanas,” *Jurnal Indonesia : Manajemen Informatika dan Komunikasi*, vol. 5, no. 1, pp. 255–261, Jan. 2024, doi: 10.35870/jimik.v5i1.468.
- [13] I. B. Putu, W. Politeknik, and N. Denpasar, “Rancang Bangun Media Storage Berbasis Armbian Menggunakan Orange-Pi dan Open media vault,” *PATRIA ARTHA Technological Journal* •, vol. 5, no. 1, 2021.
- [14] D. P. Kuswandono, “DESIGN PENGAMANAN AKSES JARAK JAUH JARINGAN RUMAH DENGAN TEKNOLOGI VPN (VIRTUAL PRIVATE NETWORK) BERBASIS DI CLOUD VPS (VIRTUAL PRIVATE SERVER),” 2018.
- [15] A. Purnama Sari and N. Kemala, “PERANCANGAN JARINGAN VIRTUAL PRIVATE NETWORK BERBASIS IP SECURITY MENGGUNAKAN ROUTER MIKROTIK,” vol. 7, no. 2, 2020.
- [16] Y. Mendrofa and R. Fauzi, “IMPLEMENTASI KEAMANAN JARINGAN MENGGUNAKAN PORT KNOCKING,” *JURNAL COMASIE*, 2023.
- [17] S. Pangestu and I. R. Widiyasari, “Perancangan Cloud Storage Menggunakan Freenas Melalui Jalur Tunneling,” *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 9, no. 2, 2022.
- [18] “Analisis Perbandingan Kinerja QOS Dengan Metode PPTP, L2TP, SSTP Dan IPSEC Pada Jaringan VPN Dengan Menggunakan Mikrotik Pada Kantor Badan Perwakilan Dan Kependudukan Keluarga Berencana Nasional (BKKBN) Pekanbaru”.