

## PENERAPAN TEKNOLOGI VPN L2TP DAN PROTOKOL AAA RADIUS PADA JARINGAN HOTSPOT

\*Aah Sumiah<sup>1)</sup>, Fitra Nugraha<sup>2)</sup>, Aji Permana<sup>3)</sup>

<sup>1)</sup>Manajemen Informatika, Fakultas Ilmu Komputer, Universitas Kuningan

<sup>2)</sup>Teknik Informatika, Fakultas Ilmu Komputer, Universitas Kuningan

<sup>3)</sup>Sistem Informasi, Fakultas Ilmu Komputer, Universitas Kuningan

E-mail: [\\*aah.sumiah@uniku.ac.id](mailto:*aah.sumiah@uniku.ac.id), [2fitra@uniku.ac.id](mailto:2fitra@uniku.ac.id), [3aji@uniku.ac.id](mailto:3aji@uniku.ac.id)

### *Abstrak*

Penggunaan hotspot portal sebagai autentikasi jaringan dan meningkatkan keamanan jaringan wireless lazim diterapkan dengan digabungkan dengan database Radius (Remote Authentication Dial-In User Service) sebagai sarana penyimpanan credential user yang dapat diakses oleh perangkat jaringan. Permasalahan terjadi ketika suatu perusahaan yang mempunyai jaringan intranet terpisahkan secara geografis dimana database radius user harus dijalankan di jaringan intranet masing masing, sehingga proses registrasi user yang sama harus dilakukan berulang kali di perusahaan cabang. Universitas Kuningan memiliki Kampus cabang yang secara geografis letak jarak lokasinya berbeda, maka diperlukan teknologi yang terpusat dan aman dalam melakukan pertukaran data. Pada penelitian ini, meneliti tentang penerapan teknologi VPN (Virtual Private Network) untuk menggabungkan dua atau lebih jaringan yang berbeda dengan penerapan keamanan pada komunikasi datanya. Database Radius akan disimpan di datacenter yang menggunakan ip public sehingga dapat diakses oleh kedua site yang terkoneksi menggunakan VPN, sehingga data user hotspot menjadi terpusat. Rancangan topologi berhasil disimulasikan menggunakan aplikasi vmware dan gns3 sebagai simulator perangkat jaringan berbasis mikrotik sesuai dengan perangkat yang digunakan di objek penelitian. Hasil yang didapatkan, tiap site yang terhubung menggunakan remote vpn l2tp dapat saling terhubung ke database radius yang berada di datacenter, serta dapat diautentikasi oleh hotspot login yang diaktifkan pada router mikrotik.

*Kata Kunci-- hotspot, L2tp VPN, Radius Database, proxy, Autentikasi*

### *Abstract*

*The use of portal hotspots as network authentication and enhancing wireless network security is commonly implemented by combining it with the Radius database (Remote Authentication Dial-In User Service) as a means of storing user credentials that can be accessed by network devices. Problems occur when a company that has an intranet network is geographically separated where the radius user database must be run on each intranet network, so that the same user registration process must be carried out repeatedly at branch companies. Kuningan University has branch campuses that are geographically located at different distances, so a centralized and secure technology is needed in exchanging data. In this study, the application of VPN (Virtual Private Network) technology was examined to combine two or more different networks with the application of security to data communications. The Radius database will be stored in a data center that uses a public IP so that it can be accessed by both sites connected using a VPN, so that the hotspot user data changes. The topology design was successfully simulated using the vmware and gns3 applications as a simulator for Mikrotik-based network devices according to the devices used in the research object. The results obtained, each site that is connected using remote vpn l2tp can be connected to each other to the radius database in the datacenter, and can be authenticated by a login hotspot that is activated on the Mikrotik router.*

*Keywords-- hotspot, L2tp VPN, Radius Database, proxy, Authentication*

## I. PENDAHULUAN

Perkembangan serta penerapan ilmu pengetahuan dan teknologi mempunyai dampak yang sangat penting dalam berbagai aspek kegiatan yang meliputi komunikasi nirkabel/wireless yang dimana telah menjadi kebutuhan dasar gaya hidup baru masyarakat. Jaringan internet nirkabel yang lebih dikenal dengan jaringan hotspot menjadi teknologi alternative yang lebih mudah diimplementasikan di lingkungan kerja seperti di perkantoran, industri, maupun akademik.

Dengan semakin banyaknya pengguna internet, maka banyak juga solusi dan permasalahan yang terjadi pada jaringan komputer. Seperti halnya yang terjadi di Kampus Universitas Kuningan, berdasarkan hasil riset dan wawancara dengan pihak Kampus terdapat sebuah permasalahan pada jarak Kampus pusat dan Kampus cabang yang berhubungan dengan penggunaan/pembuatan akun user hotspot. Universitas Kuningan memiliki Kampus cabang yang secara geografis letak jarak lokasinya berbeda, maka solusinya diperlukan teknologi yang terpusat dan aman dalam melakukan pertukaran data. Data tersebut akan tersimpan pada server di Kampus pusat dan diakses oleh client di Kampus cabang. Salah satu teknologi yang dapat digunakan adalah Virtual Private Network (VPN). Dikarenakan Universitas Kuningan memiliki 2 Kampus yang secara geografis letak jarak antara Kampus pusat dan Kampus cabang cukup berjauhan. Sehingga dalam pengoperasiannya kurang efektif karena harus membuat akun user dimasing-masing Kampus.

Dari latar belakang masalah tersebut, maka peneliti tertarik untuk melakukan kajian penelitian yang berjudul “PENERAPAN TEKNOLOGI VPN L2TP DAN PROTOKOL AAA RADIUS PADA JARINGAN HOTSPOT” agar dapat mengatasi permasalahan jaringan yang ada di Universitas Kuningan.

## II. METODE PENELITIAN

Penelitian yang dilakukan agar tersusun dengan rapi, dan tertata diperlukan tahapan-tahapan yang dipergunakan dalam melakukan penelitian adalah dengan metodologi sebagai berikut:

### A. Metode Pengumpulan Data.

Dalam metode pengumpulan data ini membahas tentang cara memperoleh data yang akan

dibutuhkan untuk penelitian. Metode pengumpulan data yang dilakukan peneliti untuk kelancara dalam penelitian adalah sebagai berikut:

#### 1. Studi Pustaka

Pada tahap ini melakukan proses pencarian literatur berupa jurnal ilmiah, website dan buku referensi, yang sesuai dengan topik penelitian. Dengan harapan peneliti mendapat banyak informasi yang bersangkutan dengan topik penelitian.

#### 2. Wawancara.

Pada tahap pengumpulan data ini wawancara ini dilakukan dengan cara mengadakan komunikasi langsung dengan pihak divisi jaringan Pusinfo Universitas Kuningan yang dapat memberikan informasi dan data-data yang diperoleh mengenai Infrastruktur Jaringan di Universitas Kuningan

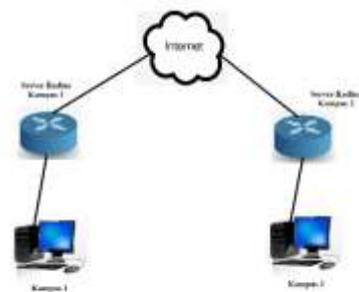
## B. Metode Pengembangan Perangkat Lunak

Model pengembangan sistem yang digunakan oleh peneliti yaitu Network Development Life Cycle (NDLC) yang terbagi dalam beberapa tahap, yaitu:

#### 1. Analisis

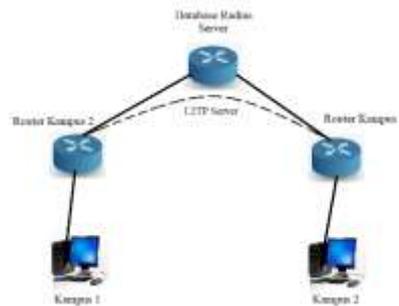
##### a. Topologi Jaringan

Pada tahap ini dibahas mengenai analisa perancangan VPN tunneling menggunakan protokol L2TP. Dalam analisa perancangan VPN ini nantinya akan terbagi menjadi beberapa bagian, yaitu LAN Kampus 1, LAN Kampus 2 dan network ISP/Internet. LAN Kampus 2 akan mengakses LAN Kampus 1 untuk keperluan file transfer melalui network ISP/Internet yang bertindak sebagai penyedia layanan internet.



**Gambar 1.1** Topologi Jaringan yang berjalan di Universitas Kuningan

Secara Topologi Kampus 1 dan Kampus 2 terhubung, tetapi pengelolaan jaringan router berbeda. Topologi diatas merupakan acuan yang akan digunakan oleh peneliti dalam membuat topologi untuk tunneling L2TP pada tugas akhir ini. Berikut adalah topologi jaringan yang diusulkan :



**Gambar 1.2** Topologi Jaringan yang diusulkan di Universitas Kuningan

Database radius server disimpan dirouter yang berada didata center internet dan digunakan sebagai sinyal ke database Radius Server. Router yang berada didata center internet tersebut digunakan juga sebagai L2TP Server dan digunakan sebagai penghubung antara Kampus 1 dan Kampus 2.

- b. Bisnis penggunaan jaringan yang sedang bejalan
  - 1) Alur registrasi user hotspot.
  - 2) Pihak pengelola Proses jaringan hotspot harus mendapatkan user untuk di Kampus 1 dan Kampus 2.
  - 3) Ketika user berpindah dari Kampus 1 dan Kampus 2 atau sebaliknya, user harus login ulang ke portal hotspot.

Hal tersebut terjadi karena :

  - Database user hotspot yang digunakan oleh jaringan Kampus 1 berbeda dengan database user hotspot Kampus 2.
  - Peralatan jaringan khususnya Router di Universitas Kuningan menggunakan Mikrotik.
- 2. Desain dan Perancangan
  - a. Simulasi Jaringan Usulan

Topologi dan konfigurasi jaringan yang akan peneliti usulkan untuk diterapkan di Kampus 1 dan Kampus 2 akan di simulasikan menggunakan software GNS3 sehingga hampir mendekati kondisi nyata ketika diterapkan.

- b. Testing
 

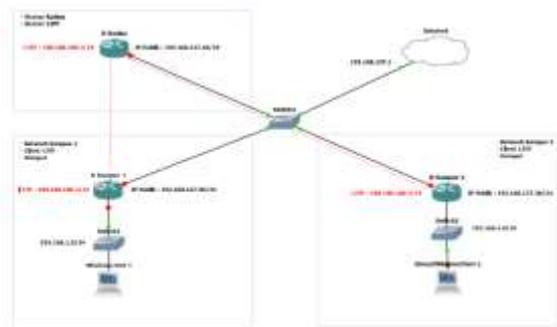
Testing akan dilakukan menggunakan simulator. Peneliti akan melakukan koneksi untuk implementasi jaringan di Universitas Kuningan dengan menggunakan software GNS3 yang mana aplikasi ini bertujuan untuk merancang jaringan sebelum di implementasikan ke Kampus 1 dan Kampus 2.
- c. Implementasi
 

Berdasarkan jaringan usulan simulasi dan hasil testing, maka hasil penelitian tersebut akan diusulkan untuk diterapkan. Sedangkan tahap implementasi peneliti melakukan percobaan VPN menggunakan metode L2TP antara Kampus 1 dan Kampus 2.

### III. HASIL DAN PEMBAHASAN

#### A. Perancangan Topology Jaringan Usulan

Berdasarkan perancangan jaringan yang telah disusun, berikut adalah perancangan topology jaringan usulan.



**Gambar 1.3** Perancangan Topologi Jaringan Usulan

#### B. Pengaturan IP Address

Setelah penyusunan topologi jaringan usulan maka diperlukan pengaturan IP Address pada masing-masing router untuk memudahkan dalam konfigurasi router. Berikut adalah table IP Address pada masing-masing router:

- 1. IP Address pada router Radius Server

Interfac	IP Address	Keterangan
e		

Ether1	192.168.137.10/24	IP ini didapat dari Internet
L2TP Server	100.100.100.1/24	IP L2TP untuk berkomunikasi dengan router kampus 1 dan router kampus 2

2. IP Address pada router Kampus 1

Interfac e	IP Address	Keterangan
Ether1	192.168.137.20/24	IP ini didapat dari Internet
Ether2	192.168.1.1/24	IP ini adalah IP DHCP Server untuk jaringan local di kampus 1
L2TP Client	100.100.100.2/24	IP L2TP untuk berkomunikasi dengan router radius

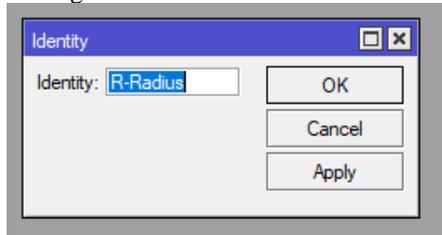
3. IP Address pada router Kampus 2

Interfac e	IP Address	Keterangan
Ether1	192.168.137.30/24	IP ini didapat dari Internet
Ether2	192.168.2.1/24	IP ini adalah IP DHCP Server untuk jaringan local di kampus 2
L2TP Client	100.100.100.3/24	IP L2TP untuk berkomunikasi dengan router radius

Untuk virtual personal computer tidak perlu mengatur IP Address karena akan mendapatkan IP DHCP dari router.

C. Konfigurasi Router

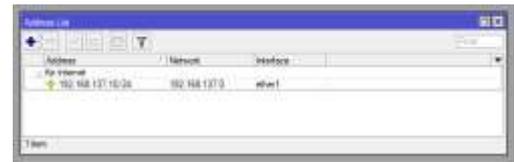
1. Konfigurasi Identitas



Gambar 1.3 Konfigurasi Identitas Router

Identitas router berguna untuk membedakan router satu dengan router yang lainnya.

2. Konfigurasi Identitas



Gambar 1.4 IP Address Router IP Address tersebut didapat langsung dari internet secara default

3. Pengaturan DNS



Gambar 1.5 Setting DNS

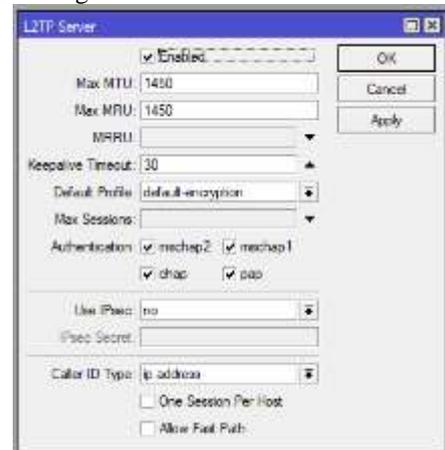
Untuk menyimpan informasi data domain dalam jaringan. Dengan adanya DNS, domain atau hostname yang ada akan ditranslate dan diterjemahkan dalam alamat IP sehingga dapat diakses.

4. Pengaturan Routing



Gambar 1.5 Pengaturan Routing

5. Konfigurasi L2TP Server



Gambar 1.5 Konfigurasi L2TP Server

Pengaturan PPP Secret agar router kampus 1 dan router kampus 2 dapat terhubung dengan router radius.



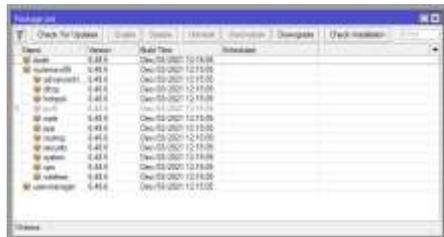
**Gambar 1.6** Pengaturan PPP Secret

6. Konfigurasi Radius



**Gambar 1.7** Setting Radius Server

7. Penambahan paket user manager pada router radius



**Gambar 1.8** Paket User Manager pada Router Radius

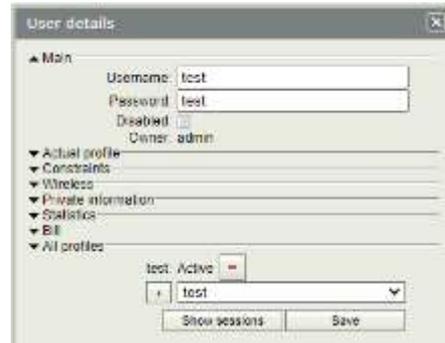
**D. Konfigurasi User Manager**

1. Konfigurasi Router



**Gambar 1.9** Konfigurasi User Manager

2. Konfigurasi User Hotspot



**Gambar 1.10** Konfigurasi User Hotspot

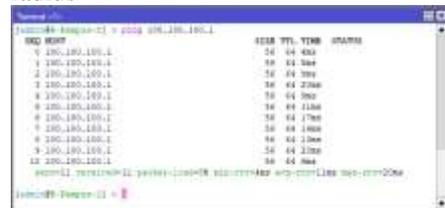
**E. Testing**

1. Ping dari router kampus 1 ke router radius melalui L2TP



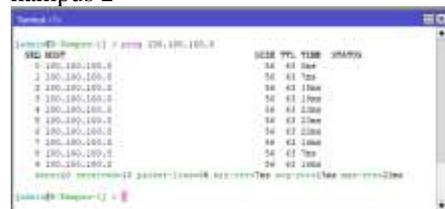
**Gambar 1.11** Testing Router Kampus 1 ke Router Kampus 2 melalui L2TP

2. Ping dari router kampus 2 ke router radius



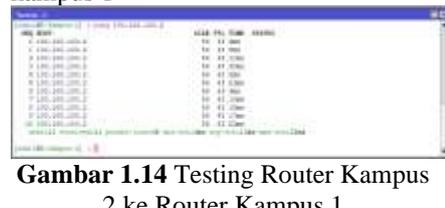
**Gambar 1.12** Testing Router Kampus 2 ke Router Radius

3. Ping dari router kampus 1 ke router kampus 2



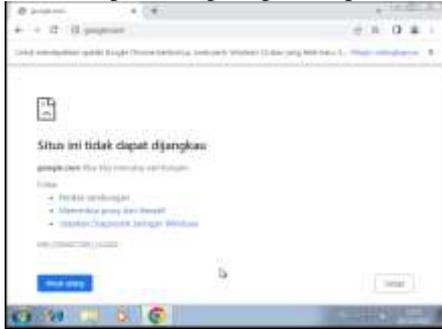
**Gambar 1.13** Testing Router Kampus 1 ke Kampus Router 2

4. Ping dari router kampus 2 ke router kampus 1



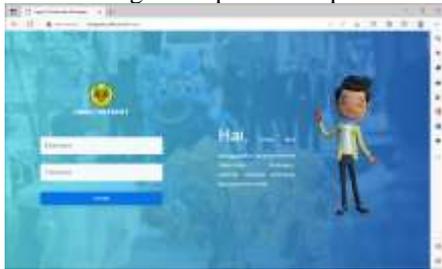
**Gambar 1.14** Testing Router Kampus 2 ke Router Kampus 1

5. Akses internet dari computer di jaringan local kampus 1 tanpa login hotspot



**Gambar 1.15** Akses Jaringan Lokal Kampus 1 tanpa login hotspot

6. Halaman login hotspot di computer 1



**Gambar 1.16** Halaman Login Hotspot di Komputer 1

7. Akses internet dari computer di jaringan local kampus 1 setelah login hotspot



**Gambar 1.17** Akses internet dari computer di jaringan local kampus 1 setelah login hotspot

#### IV. SIMPULAN

Setelah melakukan penelitian serta hasil pembahasan yang penulis uraikan pada bab-bab sebelumnya, maka dapat ditarik kesimpulan serta saran yang nantinya diharapkan berguna dan bermanfaat dalam penerapannya. Berikut kesimpulan dan saran yang dapat diambil dari penelitian ini:

1. Setelah dilakukan implementasi pada GNS3 dapat di simpulkan penggunaan protokol autentikasi pada AAA Radius server dan protokol VPN L2TP dapat mengatasi alur registrasi hotspot pada kedua kampus yang jaraknya berjauhan.

2. Proses pengujian Topologi Usulan dapat berjalan dengan lebih efektif dengan membuat Radius Terpusat yang menjadi penghubung antara Kampus 1 dan Kampus 2.
3. Penelitian selanjutnya diharapkan melakukan pengembangan sistem jaringan dari sisi jumlah perangkat pada kampus pusat maupun kampus cabang yang akan di jadikan pengujian.
4. Pada penelitian ini dapat dijadikan sebagai rujukan untuk mengembangkan tipe jaringan (topologi jaringan) dengan VPN lain seperti PPTP dan SSTP atau sejenisnya agar mendapat performa yang lebih baik.

#### DAFTAR PUSTAKA

- [1] A. H., Kamal, Suratno, & M. M. (2022). RANCANG BANGUN JARINGAN HOTSPOT BERBASIS MIKROTIK DI FAKULTAS TEKNIK UNIVERSITAS ISLAM MAKASSAR. *Teknologi Komputer*, 2, 89-95.
- [2] Ardianto, F., & Trianto. (2019). Jaringan Hotspot Radius (Remote Acces Dial-In User Service) Server Mikrotik Radius (Remote Acces Dial-In User Service) Hotspot Network Mikrotik Server (Vol. 2).
- [3] B. S., & Sutrisno. (2017). Layanan Jaringan Internet Pada Virtual Private Network (VPN) Menggunakan L2TP Untuk Peningkatan Keamanan Jaringan. *Information Communication & Technology*, 16, 1-6.
- [4] H. G., H. S., & M. G. (2018). PENGELOLAAN JARINGAN DENGAN ROUTER MIKROTIK UNTUK MENINGKATKAN EFEKTIFITAS PENGGUNAAN BANDWITH INTERNET (STUDI KASUS SMK KI HAJAR DEWANTORO KOTA TANGERANG). *Ilmu Komputer*, 3, 54-70.
- [5] H. K. (2017). Sistem Autentikasi Hotspot Menggunakan Radius Server Mikrotik Router. *INFORMATICS FOR EDUCATORS AND PROFESSIONALS*, 2, 43-50.
- [5] H. P., & Puspitasari, N. F. (2020). Penerapan Protokol L2TP/IPSec dan Port Forwarding untuk Remote Mikrotik pada Jaringan Dynamic IP. *Citec*, 7, 51-62.
- [6] Haeruddin, & Kelvin. (2022). Analisa Penggunaan VPN L2TP dan SSTP di Masa Pandemi Covid-19. *Ilmu Komputer dan Bisnis*, XIII, 105-114.

- [7] Maharani, & F. L. (2017). Penerapan Teknologi Virtual Private Network Pada Wan PT. Asuransi Jiwa Tugu Mandiri Jakarta. Indonesian Journal on Networking and Security, 7, 9-13.
- [8] Putra, Y. K., M. S., & Mahpuz. (2020). Penerapan Mikrotik Dalam Mengembangkan Infrastruktur Jaringan Pada Kantor Desa Rumbuk Kecamatan Sakra. Informatika dan Teknologi, 3, 182-193.
- [9] Rakhmah, S. N., Kuncoro, I. M., & H. H. (2019). Pengelolaan Jaringan Hotspot Menggunakan Mikrotik Routers OS pada PT Arsen Kusuma Indonesia. Infokar, 1, 15-22.
- [10] S. S., & Al-Malik, M. Z. (2021). VERIFIKASI FORMAL PROTOKOL AUTENTIKASI LINTAS REALM BERBASIS KUNCI PUBLIK. Sistem Komputer Musirawas, 6, 60-72.
- [11] Saragi, D. R., Nasution, Z. M., Sumarno, I. P., & F. A. (n.d.). IMPLEMENTASI KONFIGURASI HOTSPOT SERVER UNTUK AKSES INTERNET MENGGUNAKAN MIKROTIK ROUTER PADA DINAS LINGKUNGAN HIDUP PEMATANGSIANTAR. Device, 11, 13-20.
- [12] Sembiring, A. S. (2020). Penerapan Model Protokol Aaa (Authentication, Authorization, Accounting) Pada Keamanan Jaringan Komunikasi Wan (Wide Area. Multimedia dan Teknologi Informasi, 2, 19-29.
- [13] Sumarna, & A. M. (2020). Implementasi Virtual Private Network Menggunakan L2TP/IPsec pada BBPK Jakarta. Manajemen Sistem Informasi dan Teknologi, 11, 90-97